



robustel | 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©2020Guangzhou 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 <a href="#">Table 3</a> 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:</p> <p>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:</p> <p>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>-:</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><li>• Attach External Antenna (SMA Type)</li><li>• </li></ul>
27 Apr., 2020	3.0.0	v.3.1.1	<ul style="list-style-type: none"><li>• Revised the picture instructions of Attach External Antenna (SMA Type)</li></ul>

## Contents

	<b>Chapter 1 Product</b>	<b>Overview</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.....	17
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
<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 inthe 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



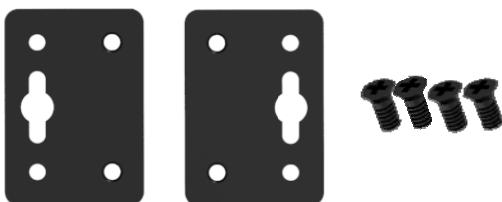
- 1 x *Quick Start Guide* with download link of other documents or tools



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

### Optional Accessories (sold separately)

- Wall mounting kit



- 35mm DIN rail mounting kit



- Ethernet cable



- AC/DC power adapter (12VDC, 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)

### 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: 1.5KV

### 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

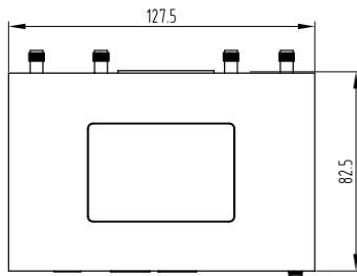
### Power Supply and Consumption

- Connector: 3-pin 3.5mm female socket
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 100 mA@12 V  
Data link: 500 mA (peak)@12 V

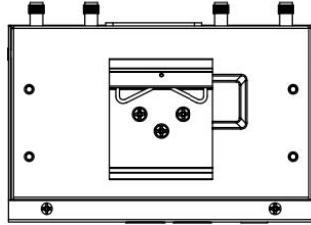
### Physical Characteristics

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

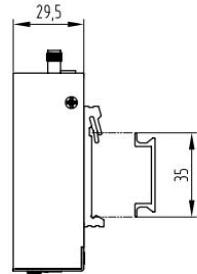
## 1.4 Dimensions



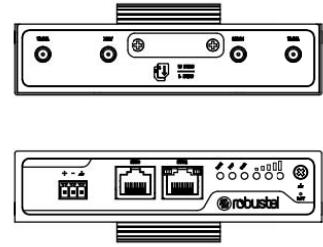
Front View



Rear View



Side View



Top&Bottom View



# 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	<p>When the network is disconnected, those three signal LEDs are designed as a binary combination code to indicate a series of error report.</p> <p>Blinking: 1    Off: 0</p> <p>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</p>

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

## 2.3 Reset Button

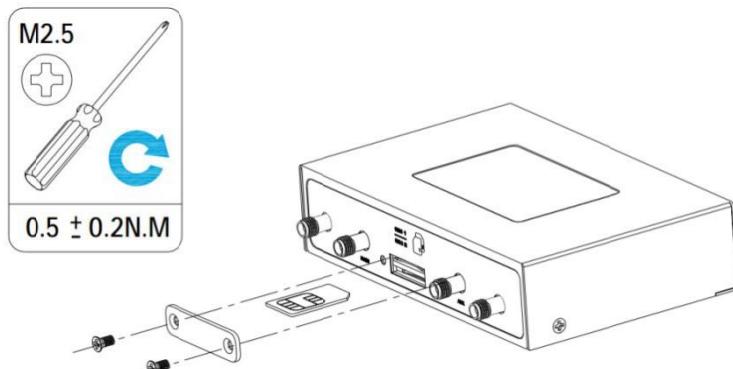
Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 3 seconds after powering up the router, press and hold the RST button until all six LEDs start blinking one by one, and release the button to return the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

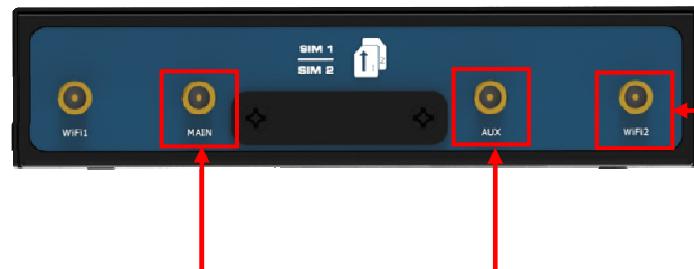
1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40°C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget 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.



Both WiFi1 and WiFi2 are RP-SMA-K antennas used for WLAN connection, but WiFi antennas are not divided into main and auxiliary antennas

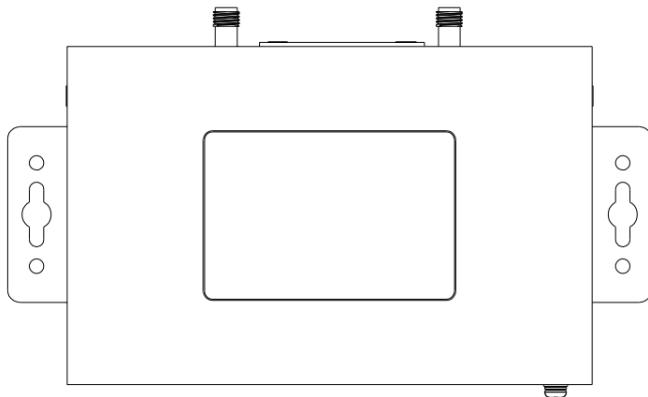
Both MAIN and AUX are SMA-J antennas used to connect to the cellular network. If only one antenna is used, it must be connected to the MAIN antenna

## 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

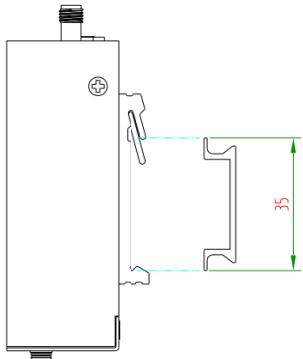
- Wall mounting(measured in mm)



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.

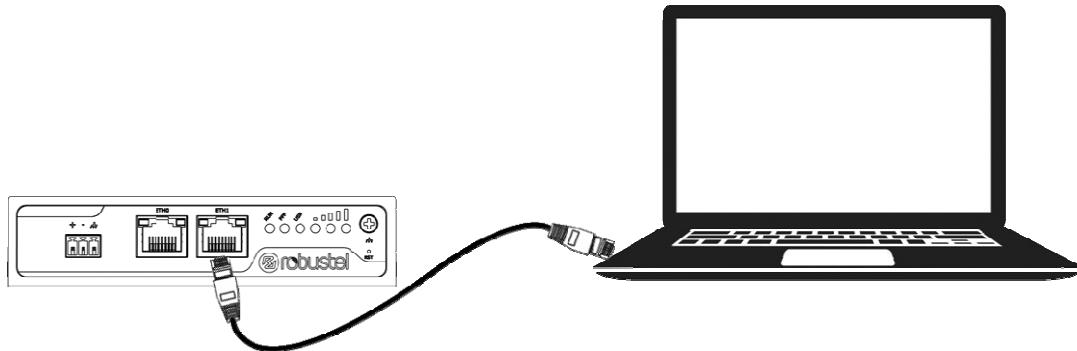
**Note:** Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

## 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

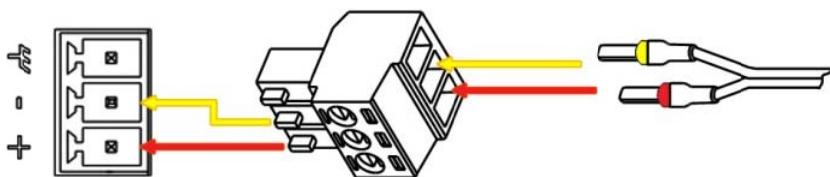


Connect an Ethernet cable to the port marked ETH0 or ETH1 at the bottom of the router, and connect the other end of the cable to your computer.

## 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.



# Chapter 3 Initial Configuration

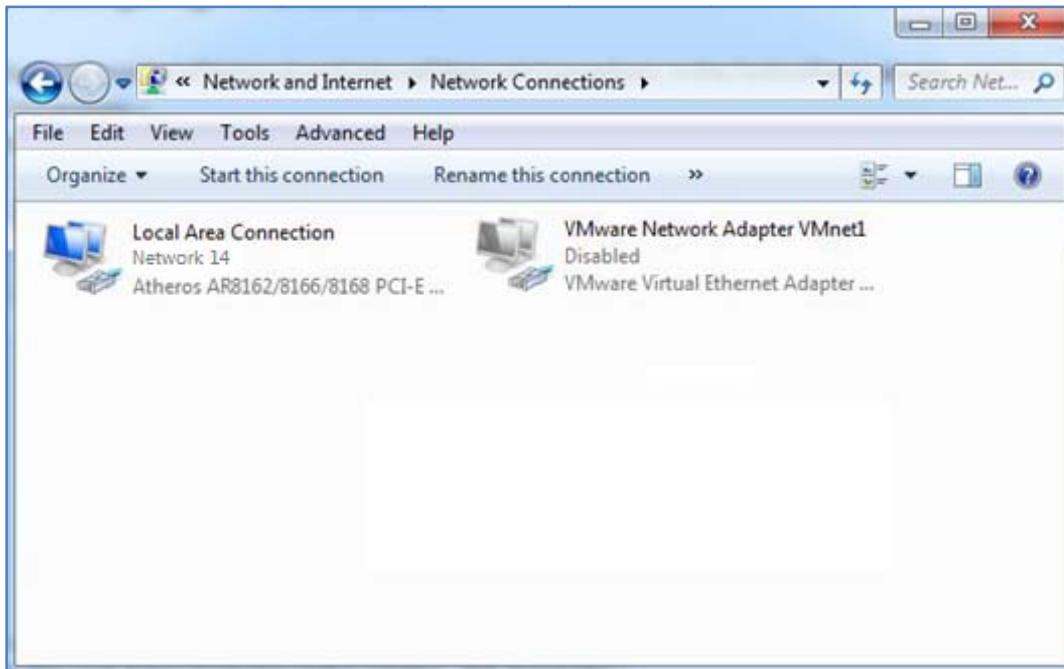
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

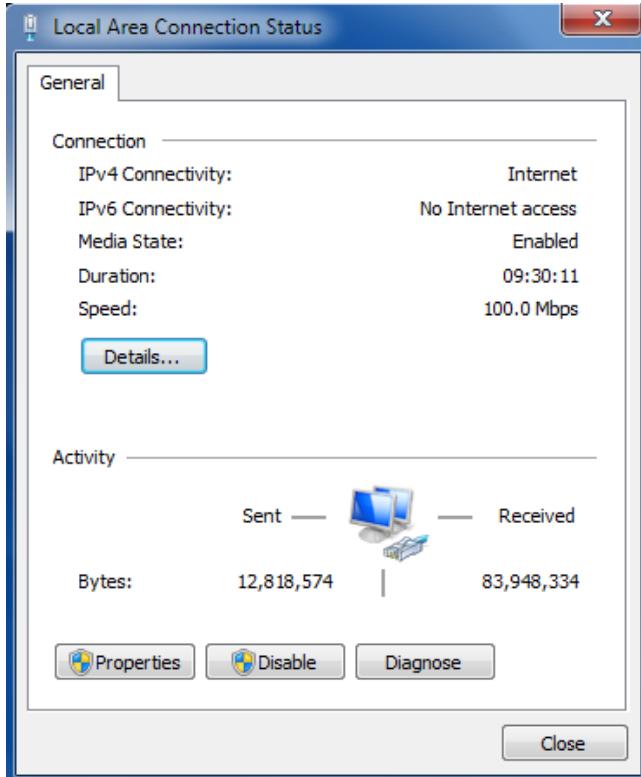
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

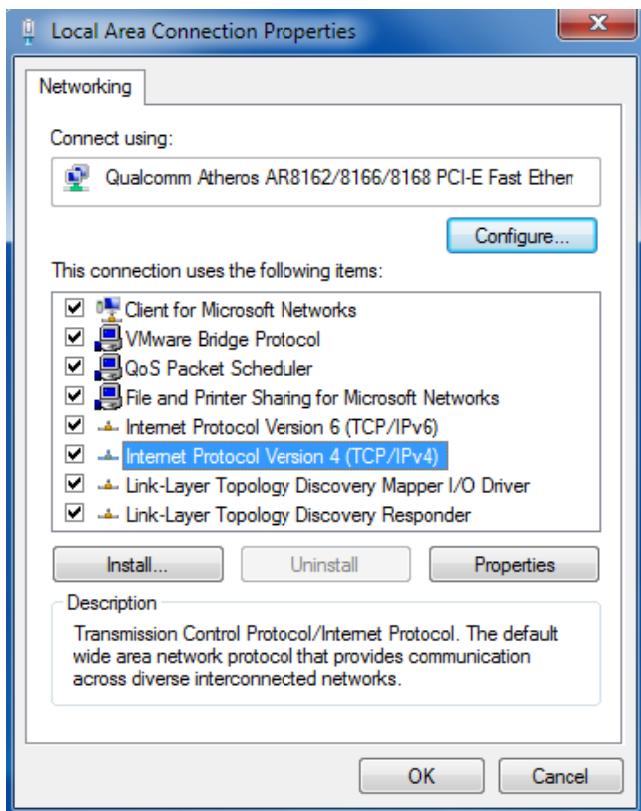
1. Click **Start>Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



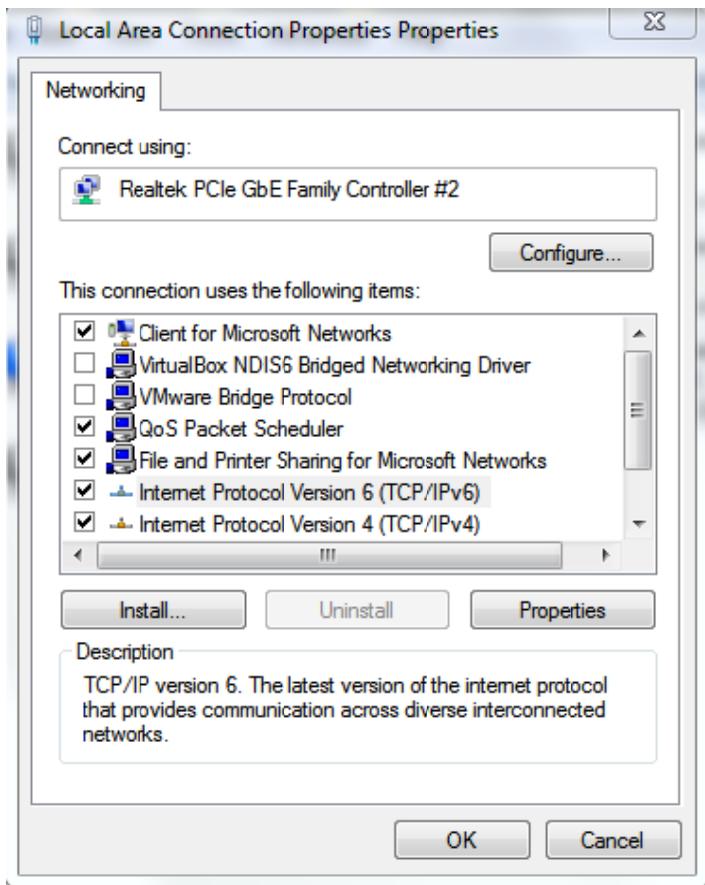
2. Click **Properties** in the window of **Local Area Connection Status**.



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

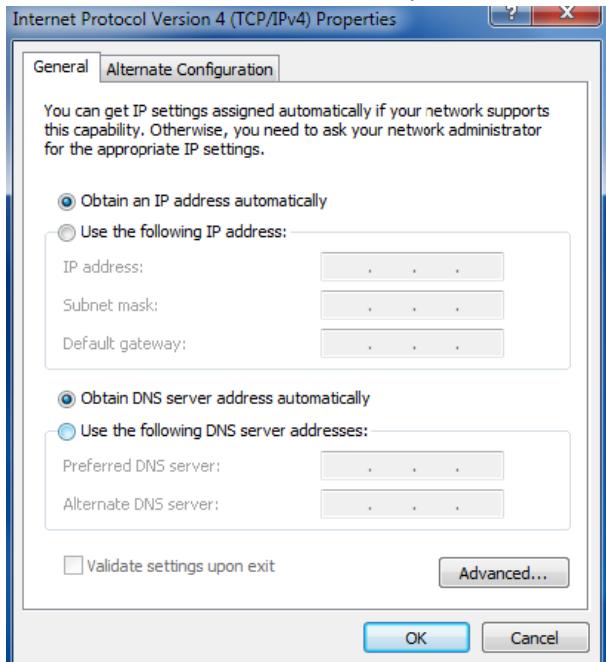


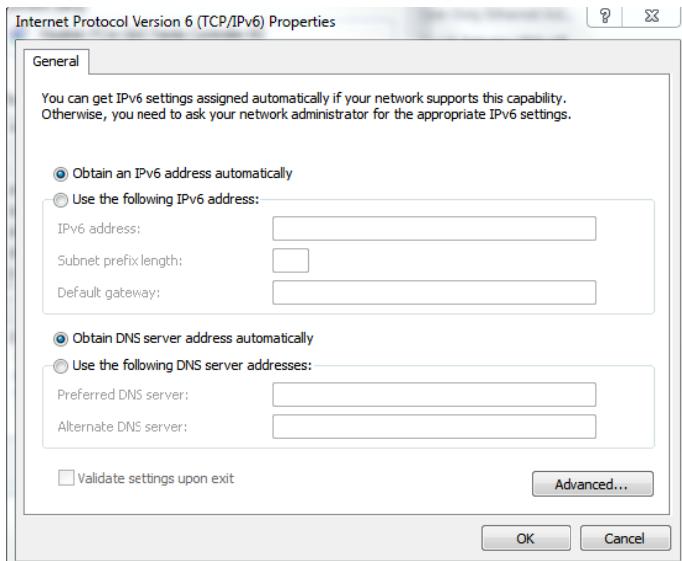
4. Choose **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.



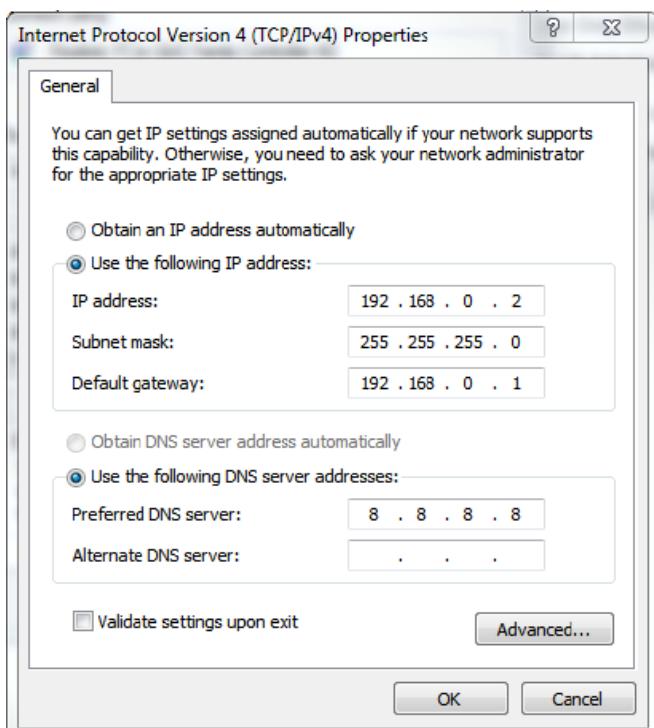
5. Two ways for configuring the IP address of PC.

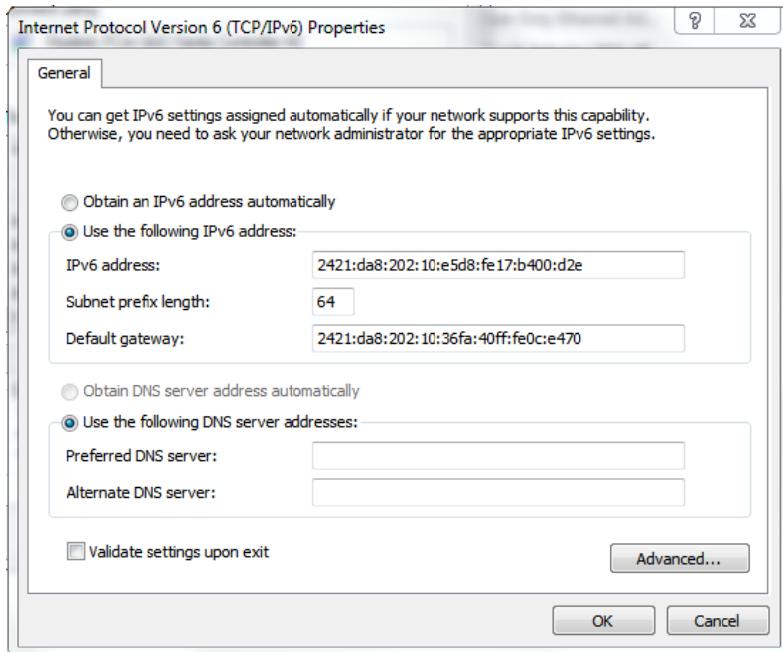
Obtain an IP address automatically from the DHCP server, click "**Obtain an IP address automatically**";





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.

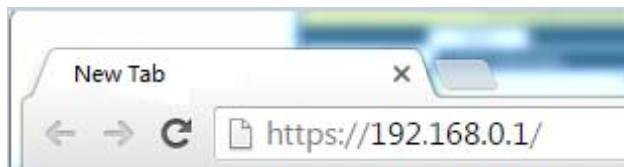
Item	Description
Username	admin
Password	admin
ETH0	192.168.0.1/255.255.255.0, LAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

## 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.

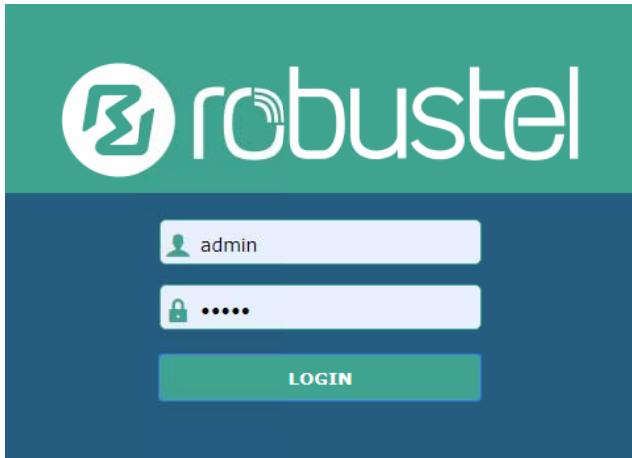
1. On your PC, open a web browser such as Internet Explorer, Google or Firebox, etc.
2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is <http://192.168.0.1/>, though the actual address may vary.

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



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

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



## 3.4 Control Panel

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



⚠ It is strongly recommended to change the default password.

Save & Apply | Reboot | Logout

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.

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.	<b>Save &amp; Apply</b>
Reboot	Click to reboot the router. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	<b>Reboot</b>
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.	<b>Logout</b>
Submit	Click to save the modification on current configuration page.	<b>Submit</b>
Cancel	Click to cancel the modification on current configuration page.	<b>Cancel</b>

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

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

## 3.5 Status

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



## System Information

System Information	
<b>Device Model</b>	R2000
<b>System Uptime</b>	0 days, 06:17:32
<b>System Time</b>	Thu Jul 6 17:28:51 2017
<b>RAM Usage</b>	17M Free/64M Total
<b>Firmware Version</b>	3.0.0
<b>Hardware Version</b>	1.0
<b>Kernel Version</b>	3.10.49
<b>Serial Number</b>	1111111111

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	
<b>Uptime</b>	0 days, 00:00:40
<b>Active IPv4 Link</b>	WWAN1
<b>IPv4 Address</b>	10.161.3.12/255.0.0.0
<b>IPv4 Gateway</b>	10.0.0.1
<b>IPv4 DNS</b>	120.80.80.80 221.5.88.88
<b>Active IPv6 Link</b>	WWAN1
<b>IPv6 Address</b>	2408:84f3:2d:9e2c:1e:10ff:fe1f:0/64
<b>IPv6 Gateway</b>	fe80::4e54:99ff:fe45:e5d5
<b>IPv6 DNS</b>	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.
IPv6Address	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	
<b>IP Address</b>	192.168.0.1/255.255.255.0
<b>Active IPv6 Address</b>	2121:da8:202:10:36fa:40ff:fe18:68e3/64
<b>Inactive IPv6 Address</b>	
<b>MAC Address</b>	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	<input type="button" value="WWAN1"/> <span style="font-size: small;">?</span>
Backup Link	<input type="button" value="WWAN2"/> <span style="font-size: small;">?</span>
Backup Mode	<input type="button" value="Cold Backup"/> <span style="font-size: small;">?</span>
Revert Interval	<input type="text" value="0"/> <span style="font-size: small;">?</span>
Emergency Reboot	<input type="button" value="ON"/> <input type="button" value="OFF"/> <span style="font-size: small;">?</span>

General Settings @ Link Manager		
Item	Description	Default
Primary Link	<p>Select from “WWAN1”, “WWAN2”, “WAN” or “WLAN”.</p> <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 wiredlink <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	<p>Select from “WWAN1”, “WWAN2”, “WAN”, “WLAN” or “None”.</p> <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 wiredlink <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	<p>Select from “Cold Backup”, “Warm Backup” or “Load Balancing”.</p> <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> <p><b>Note:</b> R2000 do not support warm backup and load balancing in the situation of two WWAN links.</p>	Cold Backup
Revert Interval	<p>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.</p> <p><b>Note:</b> Revert interval is available only under the cold backup mode.</p>	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.

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	<b>ON</b>

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

**WWAN Settings**

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

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



### ▲ WWAN Settings

Automatic APN Selection	<input checked="checked" type="button"/> ON <input type="button"/> OFF
APN	internet
Username	
Password	*****
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	<input checked="checked" type="button"/> ON <input type="button"/> OFF <a href="#">?</a>
Switch SIM By Data Allowance	<input checked="checked" type="button"/> ON <input type="button"/> OFF <a href="#">?</a>
Data Allowance	0
Billing Day	1

### ▲ IPv6 LAN Settings

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

### ▲ Ping Detection Settings

Enable	<input checked="checked" type="button"/> ON <input type="button"/> 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	<input checked="checked" type="button"/> ON <input type="button"/> OFF
Upload Bandwidth	10000 <input type="button"/> ?
Download Bandwidth	10000 <input type="button"/>
Overriden Primary DNS	<input type="button"/>
Overriden Secondary DNS	<input type="button"/>
Overriden IPv6 Primary DNS	<input type="button"/>
Overriden IPv6 Secondary DNS	<input type="button"/>
Debug Enable	<input checked="checked" type="button"/> ON <input type="button"/> OFF
Verbose Debug Enable	<input type="button"/> ON <input checked="checked" type="button"/> OFF

Link Settings (WWAN)		
Item	Description	Default
<b>General Settings</b>		
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
<b>WWAN Settings</b>		
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
<b>IPv6 LAN Settings</b>		
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**.

**Link Manager**

**General Settings**

Index	3
Type	WAN
Description	admin
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	SLAAC

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

**General Settings**

Index	3
Type	WAN
Description	admin
IPv6 Enable	ON OFF
IPv4 Connection Type	Static
IPv6 Connection Type	Static

**Static Address Settings**

IP Address	
Gateway	
Primary DNS	
Secondary DNS	

**IPv6 Static Address Settings**

IPv6 Address	
IPv6 Gateway	
IPv6 Primary DNS	
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  IPv4 Connection Type  IPv6 Connection Type  Address Mode  

### PPPoE Settings

Username Password Authentication Type  PPP Expert Options  

### Ping Detection Settings

Enable  IPv4 Primary Server IPv4 Secondary Server IPv6 Primary Server IPv6 Secondary Server Interval  Retry Interval  Timeout  Max Ping Tries  

### Advanced Settings

IPv4 NAT Enable  MTU  Upload Bandwidth  Download Bandwidth Overridden Primary DNS Overridden Secondary DNS Overridden IPv6 Primary DNS Overridden IPv6 Secondary DNS Debug Enable  Verbose Debug Enable

Link Settings (WAN)		
Item	Description	Default
<b>General Settings</b>		
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
<b>IPv4 Static Address Settings</b>		
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
<b>IPv6 Static Address Settings</b>		
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
<b>PPPoE Settings</b>		
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
<b>IPv6 LAN Ping Settings</b>		
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
<b>Ping Detection Settings</b>		
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	<input type="text" value="3"/>
Type	<input type="text" value="WLAN"/>
Description	<input type="text"/>
IPv6 Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
IPv4 Connection Type	<input type="text" value="DHCP"/>

WLAN Settings

SSID	<input type="text" value="router"/>
Connect to Hidden SSID	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Password	<input type="text"/>

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

**General Settings**

Index	3
Type	WLAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	Static

**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
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**

<b>IPv4 NAT Enable</b>	<b>ON</b> <b>OFF</b>
<b>MTU</b>	1500
<b>Upload Bandwidth</b>	10000
<b>Download Bandwidth</b>	10000
<b>Overrided Primary DNS</b>	
<b>Overrided Secondary DNS</b>	
<b>Overrided IPv6 Primary DNS</b>	
<b>Overrided IPv6 Secondary DNS</b>	
<b>Debug Enable</b>	<b>ON</b> <b>OFF</b>
<b>Verbose Debug Enable</b>	<b>ON</b> <b>OFF</b>

**Link Settings (WLAN)**

Item	Description	Default
<b>General Settings</b>		
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
<b>WLAN Settings</b>		
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
<b>Static Address Settings</b>		
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
<b>IPv6 LAN Settings</b>		
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
<b>Ping Detection Settings</b>		
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.	114.114.1 14.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the current IPv6 connectivity is active.	2001:4860 :4860::888 8
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

#### Advance Settings

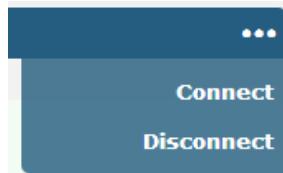
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary 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	
2	WWAN2	NONE	Disconnect...		

WWAN Data Usage Statistics		?
WWAN1 Monthly Stats	<b>Clear</b>	
WWAN2 Monthly Stats	<b>Clear</b>	

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	
<b>▲ Network Settings</b>			
Index	Interface	IPv4 Address	Netmask
1	lan0	192.168.0.1	255.255.255.0

**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												
<b>▲ General Settings</b>												
<table> <tr> <td>Index</td> <td>1</td> </tr> <tr> <td>Interface</td> <td>lan0</td> </tr> <tr> <td>IPv4 Address</td> <td>192.168.2.1</td> </tr> <tr> <td>Netmask</td> <td>255.255.255.0</td> </tr> <tr> <td>IPv6 Address Allocation Type</td> <td>SLAAC</td> </tr> <tr> <td>MTU</td> <td>1500</td> </tr> </table>	Index	1	Interface	lan0	IPv4 Address	192.168.2.1	Netmask	255.255.255.0	IPv6 Address Allocation Type	SLAAC	MTU	1500
Index	1											
Interface	lan0											
IPv4 Address	192.168.2.1											
Netmask	255.255.255.0											
IPv6 Address Allocation Type	SLAAC											
MTU	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
IPv6Address 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	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Mode	Server
IP Pool Start	192.168.0.2
IP Pool End	192.168.0.100
Subnet Mask	255.255.255.0

**^ DHCP Advanced Settings**

Gateway	
Primary DNS	
Secondary DNS	
WINS Server	
Lease Time	120
Static Lease	
Expert Options	
Debug Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>

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

**^ DHCP Settings**

Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Mode	Relay
DHCP Server For Relay	

**^ DHCP Advanced Settings**

Debug Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
--------------	--

LAN		
Item	Description	Default
<b>DHCP Settings</b>		
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"/>
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	
1	ON	lan0	100			

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

VLAN Trunk

^ VLAN Settings

Index	Enable	Interface	VID	IP Address	Netmask
1	ON	lan0	100		

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	
<b>▲ Interface Status</b>			
Index	Interface	IP Address	Active IPv6 Address
1 lan0 192.168.0.1/255.2... 2221:da8:202:10:36fa:4...			
<b>▲ Connected Devices</b>			
Index	IPv4/IPv6 Address	MAC Address	Interface
1	192.168.0.59	D0:50:99:A9:2B:80	lan0
<b>▲ DHCP Lease Table</b>			
Index	IPv4/IPv6 Address	MAC Address or IAID	Interface
1	192.168.0.59	d0:50:99:a9:2b:80	lan0
<b>▲ DHCP Lease Table</b>			
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.

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

## 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	
<b>▲ Port Settings</b>		
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	1
Port	eth0
Port Assignment	lan0

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**

**^ 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

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.



The screenshot shows a web-based interface for AT Debug. At the top, there are three tabs: 'Cellular' (green), 'Status' (green), and 'AT Debug' (blue, indicating it is active). Below the tabs is a header 'AT Debug' with a back arrow icon. The main area is divided into two text boxes: 'Command' (top) and 'Result' (bottom). A blue 'Send' button is located at the bottom right of the interface.

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
<b>Send</b>	Click the button to send AT command.	--

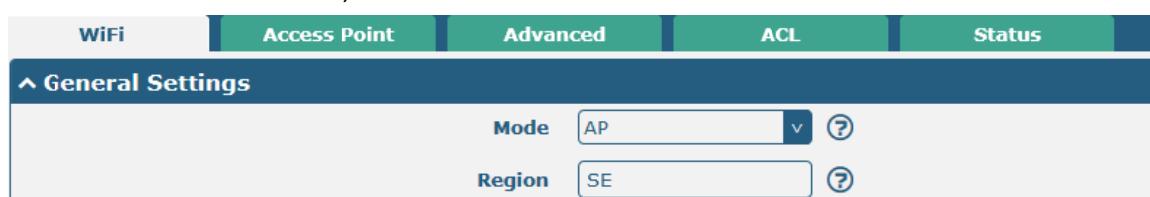
### 3.10 Interface > WiFi (Optional)

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”.



The screenshot shows the 'Access Point' configuration page. At the top, there are five tabs: 'WiFi' (gray), 'Access Point' (green, indicating it is active), 'Advanced' (gray), 'ACL' (gray), and 'Status' (gray). Below the tabs is a header 'General Settings' with a back arrow icon. The main area contains two settings: 'Mode' (set to 'AP') and 'Region' (set to 'SE'). Each setting has a help icon (a question mark inside a circle) to its right.

**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	ON <input type="button" value="OFF"/>			
Wireless Mode	11bgn Mixed <input type="button" value="v"/>			
Channel	Auto <input type="button" value="v"/> <input type="button" value="?"/>			
SSID	router			
Broadcast SSID	ON <input type="button" value="OFF"/>			
Security Mode	Disabled <input type="button" value="v"/> <input type="button" value="?"/>			

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

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

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

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



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

General Settings

Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Wireless Mode	11bgn Mixed
Channel	Auto
SSID	router
Broadcast SSID	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Security Mode	WEP
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”..... “11”. <ul style="list-style-type: none"> <li>• Auto: Router will scan all frequency channels until the best one is found</li> <li>• 1~11 Router will be fixed to work with this channel</li> </ul> Following are the frequency of 1~11channel: 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	Auto
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router

General Settings @ Access Point		
Item	Description	Default
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of router AP at WiFi client side.	ON
Security Mode	<p>Select from "Disabled", "WPA-Personal", "WPA-Enterprise" or "WEP".</p> <ul style="list-style-type: none"> <li>• <b>Disabled:</b> User can access the WiFi without password <b>Note:</b> It is strongly recommended for security purposes that you do not choose this kind of mode.</li> <li>• <b>WPA-Personal:</b> WiFi Protected Access only provides one password used for Identity Authentication</li> <li>• <b>WPA-Enterprise:</b> Provides an authentication interface for EAP which can be authenticated via Radius Authentication Server or other Extended Authentication</li> <li>• <b>WEP:</b> 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>• <b>Auto:</b> Router will choose automatically the most suitable WPA version</li> <li>• <b>WPA2</b> 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>• <b>Auto:</b> Router will choose automatically the most suitable encryption</li> <li>• <b>TKIP:</b> Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication <b>Note:</b> It's not recommended to use TKIP encryption in 802.11n mode.</li> <li>• <b>AES:</b> 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
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812



General Settings @ Access Point		
Item	Description	Default
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
11N Transmit Rate	Auto
Transmit Power	Max
Channel Width	Auto
Enable WMM	ON <input type="button" value="OFF"/>
Enable Short GI	ON <input type="button" value="OFF"/>
Enable AP Isolation	ON <input type="button" value="OFF"/>
Debug Level	none

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 Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is	Auto

Advanced Settings		
Item	Description	Default
	default to "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  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
<b>General Settings</b>		
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> <li>Deny: All the packets fitting the entities of the "Access Control List" will be denied</li> </ul> <b>Note:</b> Router can only allow or deny devices which are included in "Access Control List" at one time.	Accept

ACL		
Item	Description	Default
<b>Access Control List</b>		
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
<b>AP Status</b>				
		<b>Status</b>	COMPLETED	
		<b>Channel</b>	6	
		<b>Channel Width</b>	20 MHz	
		<b>MAC Address</b>	34:FA:40:01:DE:02	
<b>Associated Stations</b>				
<b>Index</b>	<b>MAC Address</b>	<b>IP Address</b>	<b>Name</b>	<b>Connected Time</b>
				<b>Signal</b>

## WiFi Client

### Configure Router as WiFi Client

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

WiFi
<b>General Settings</b>
Mode <input type="button" value="Client"/> 
Region <input type="button" value="SE"/> 

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

WiFi
<b>Status</b>
<b>Interface</b>
Link Manager
LAN
Ethernet
Cellular
<b>WiFi</b>
<b>WLAN</b>

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



**WLAN Settings**

SSID	Robustel
Connect to Hidden SSID	<input checked="" type="button"/> ON <input type="button"/> OFF
Password	*****

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	
<b>WPA State</b>	COMPLETED
<b>Frequency</b>	2422
<b>BSSID</b>	88:da:1a:2a:69:bc
<b>SSID</b>	routerIpv63000
<b>Mode</b>	station
<b>Key Management</b>	WPA2-PSK
<b>Pairwise Cipher</b>	CCMP
<b>Group Cipher</b>	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**

<b>Index</b>	<input type="text" value="1"/>
<b>Description</b>	<input type="text"/>
<b>Destination</b>	<input type="text"/>
<b>Netmask/Prefix Length</b>	<input type="text"/> <a href="#">?</a>
<b>Gateway</b>	<input type="text"/>
<b>Interface</b>	<input type="text" value="wlan0"/> <a href="#">▼</a>

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			
<b>Route Table</b>					
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

### General Settings

Enable Filtering

Default Filtering Policy

### Access Control Settings

Enable Remote SSH Access

Enable Local SSH Access

Enable Remote Telnet Access

Enable Local Telnet Access

Enable Remote HTTP Access

Enable Local HTTP Access

Enable Remote HTTPS Access

Enable Remote Ping Respond

Enable DOS Defending

Enable Console

Enable VPN NAT Traversal

### Whitelist Rules

Index	Description	Source Address	<input type="button" value="?"/>
-------	-------------	----------------	----------------------------------

### Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol	<input type="button" value="+"/>
-------	----------------	-------------	------------	----------------	-------------	----------	----------------------------------

Click  to add the whitelist rules.

Filtering

### Whitelist Rules

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
Action	Drop

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
Action	Drop

Filtering		
Item	Description	Default
<b>General Settings</b>		
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
<b>Access Control Settings</b>		
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

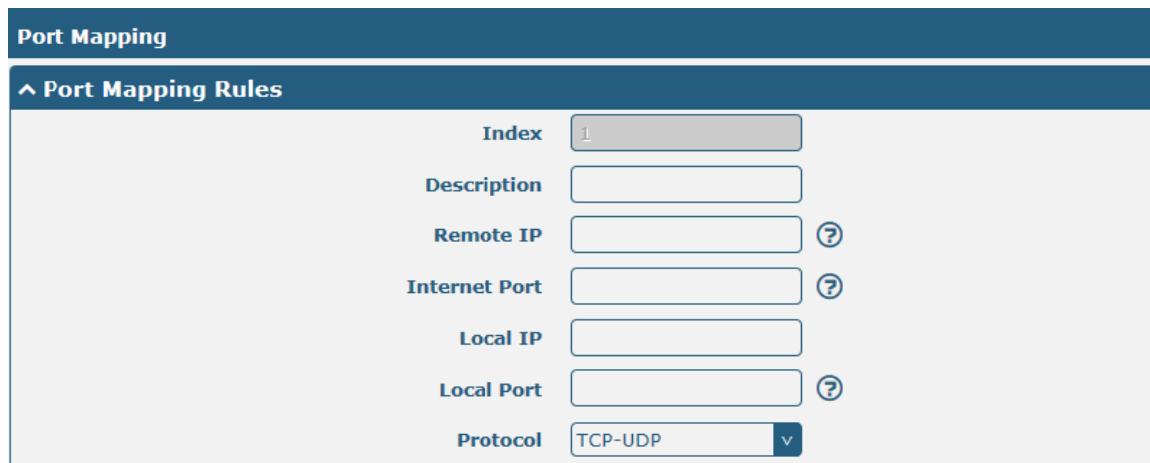
## Port Mapping

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:



Index	Description	Internet Port	Local IP	Local Port	Protocol
-------	-------------	---------------	----------	------------	----------

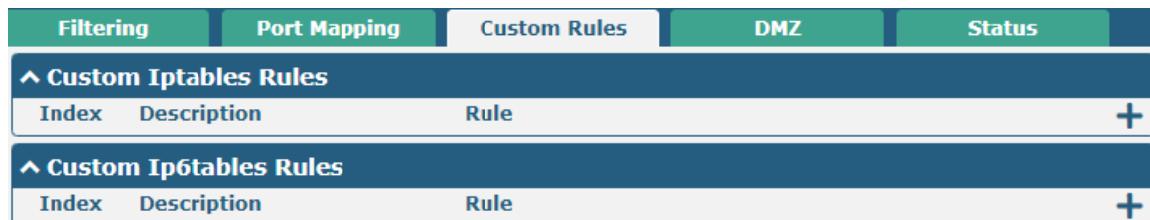
Click **+** to add port mapping rules. The maximum rule count is 40.



Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol
-------	-------------	-----------	---------------	----------	------------	----------

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:



Index	Description	Rule
-------	-------------	------

Index	Description	Rule
-------	-------------	------

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	<input type="text" value="1"/>
Description	<input type="text"/>
Rule	<input type="text"/> <a href="#">?</a>

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						
<b>DMZ Settings</b>								
<table border="1"> <tr> <td>Enable DMZ</td> <td><input checked="checked" type="button" value="ON"/> <input type="button" value="OFF"/></td> </tr> <tr> <td>Host IP Address</td> <td><input type="text"/></td> </tr> <tr> <td>Source IP Address</td> <td><input type="text"/> <a href="#">?</a></td> </tr> </table>			Enable DMZ	<input checked="checked" type="button" value="ON"/> <input type="button" value="OFF"/>	Host IP Address	<input type="text"/>	Source IP Address	<input type="text"/> <a href="#">?</a>
Enable DMZ	<input checked="checked" type="button" value="ON"/> <input type="button" value="OFF"/>							
Host IP Address	<input type="text"/>							
Source IP Address	<input type="text"/> <a href="#">?</a>							

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	
<b>Chain Input</b>									
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		
<b>Chain Forward</b>									
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		
<b>Chain Output</b>									
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
<b>General Settings</b>
Enable <input checked="" type="button"/> ON <input type="button"/> 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

General	Tunnel	Status	x509									
<b>General Settings</b> <table border="1"> <tr> <td>Keepalive</td> <td>20</td> <td>?</td> </tr> <tr> <td>Optimize DH Exponent Size</td> <td>ON OFF</td> <td>?</td> </tr> <tr> <td>Debug Enable</td> <td>ON OFF</td> <td></td> </tr> </table>				Keepalive	20	?	Optimize DH Exponent Size	ON OFF	?	Debug Enable	ON OFF	
Keepalive	20	?										
Optimize DH Exponent Size	ON OFF	?										
Debug Enable	ON OFF											

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 IPsecVPN information output to the debug port.	OFF

## Tunnel

General	Tunnel	Status	x509							
<b>Tunnel Settings</b> <table border="1"> <thead> <tr> <th>Index</th> <th>Enable</th> <th>Description</th> <th>Gateway</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>+</th> </tr> </thead> </table>				Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+				

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

<b>Tunnel</b>																			
<b>General Settings</b> <table border="1"> <tr> <td>Index</td> <td>1</td> </tr> <tr> <td>Enable</td> <td>ON OFF</td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Gateway</td> <td></td> </tr> <tr> <td>Mode</td> <td>Tunnel</td> </tr> <tr> <td>Protocol</td> <td>ESP</td> </tr> <tr> <td>Local Subnet</td> <td></td> </tr> <tr> <td>Remote Subnet</td> <td>admin</td> </tr> <tr> <td>Link Binding</td> <td>Unspecified</td> </tr> </table>		Index	1	Enable	ON OFF	Description		Gateway		Mode	Tunnel	Protocol	ESP	Local Subnet		Remote Subnet	admin	Link Binding	Unspecified
Index	1																		
Enable	ON OFF																		
Description																			
Gateway																			
Mode	Tunnel																		
Protocol	ESP																		
Local Subnet																			
Remote Subnet	admin																		
Link Binding	Unspecified																		

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	<p>Select from “Tunnel” and “Transport”.</p> <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	<p>Select the security protocols from “ESP” and “AH”.</p> <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.

**▲ IKE Settings**

<b>IKE Type</b>	IKEv1
<b>Negotiation Mode</b>	Main
<b>Encryption Algorithm</b>	3DES
<b>Authentication Algorithm</b>	SHA1
<b>IKE DH Group</b>	DHgroup2
<b>Authentication Type</b>	PSK
<b>PSK Secret</b>	
<b>Local ID Type</b>	Default
<b>Remote ID Type</b>	Default
<b>IKE Lifetime</b>	86400

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

**▲ IKE Settings**

<b>IKE Type</b>	IKEv1
<b>Negotiation Mode</b>	Main
<b>Encryption Algorithm</b>	3DES
<b>Authentication Algorithm</b>	SHA1
<b>IKE DH Group</b>	DHgroup2
<b>Authentication Type</b>	CA
<b>Private Key Password</b>	
<b>IKE Lifetime</b>	86400

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

**▲ IKE Settings**

<b>IKE Type</b>	IKEv1
<b>Negotiation Mode</b>	Main
<b>Encryption Algorithm</b>	3DES
<b>Authentication Algorithm</b>	SHA1
<b>IKE DH Group</b>	DHgroup2
<b>Authentication Type</b>	PKCS#12
<b>Private Key Password</b>	
<b>IKE Lifetime</b>	86400

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



### ▲ IKE Settings

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

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

### ▲ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
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 CertificateAuthority</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	ON <input type="button" value="OFF"/>
Description	
Gateway	
Mode	Tunnel <input type="button" value="v"/>
Protocol	ESP <input type="button" value="v"/>
Local Subnet	
Remote Subnet	
Link Binding	Unspecified <input type="button" value="v"/> <input type="button" value="?"/>

IKE Settings

SA Settings

Encryption Algorithm	3DES <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
PFS Group	DHgroup2 <input type="button" value="v"/>
SA Lifetime	28800 <input type="button" value="?"/>
DPD Interval	30 <input type="button" value="?"/>
DPD Failures	150 <input type="button" value="?"/>

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

General Settings

Index	1
Enable	ON <input type="button" value="OFF"/>
Description	
Gateway	
Mode	Tunnel <input type="button" value="v"/>
Protocol	AH <input type="button" value="v"/>
Local Subnet	
Remote Subnet	
Link Binding	Unspecified <input type="button" value="v"/> <input type="button" value="?"/>

IKE Settings



**SA Settings**

Authentication Algorithm	SHA1	<input type="button" value="v"/>
PFS Group	DHgroup2	<input type="button" value="v"/>
SA Lifetime	28800	<input type="button" value="?"/>
DPD Interval	30	<input type="button" value="?"/>
DPD Failures	150	<input type="button" value="?"/>

**Advanced Settings**

Enable Compression	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Enable Forceencaps	<input type="button" value="ON"/> <input type="button" value="OFF"/> <input type="button" value="?"/>
Expert Options	<input type="button" value="?"/>

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 are 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				
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".