

# R3000

Industrial Dual SIM Cellular VPN Router 2 Eth + 1 RS232 + 1 RS485 + 1 USB Host





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



#### **About This Document**

This document provides hardware and software information of the Robustel R3000 Router, including introduction, installation, configuration and operation.

Copyright©2022 Guangzhou Robustel Co., Ltd. All rights reserved.

**Trademarks and Permissions** 

B CODUSTE, CODUSTOS are trademarks of Guangzhou Robustel Co., Ltd.. All other trademarks and trade

names mentioned in this document are the property of their respective owners.

#### Disclaimer

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

Technical Support Tel: +86-20-82321505 Email: <u>support@robustel.com</u> Web: <u>www.robustel.com</u>

#### **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.
- When used, the device needs a suitable environment.
  - 1. If indoors, it needs to be provided an indoor enclosure.
  - 2. If outdoors, it needs to be provided a rain proof enclosure.
- RF exposure statements
  - 1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
  - 1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
  - 2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

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

#### Using the Router in Vehicle

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

#### **Protecting Your Router**

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

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



#### **Regulatory and Type Approval Information**

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

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

Name of	Hazardo	us Substa	nces							
the Part	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	0	0	0	0	-	-	-	-	-	-
Circuit modules	0	0	0	ο	ο	0	0	0	ο	0
Cables and cable assemblie s	0	0	0	0	0	0	0	0	0	0
Plastic and polymeric parts	0	0	0	0	0	0	0	0	0	0

o:

Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.

X:

Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in RoHS2.0.

-:

Indicates that it does not contain the toxic or hazardous substance.

#### **Document History**

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

Date	Firmware Version	Document Version	Change Description
Mar. 27, 2017	3.0.0	v.4.0.0	Initial release
Jul. 17, 2017	3.0.0	v.4.0.1	<ul> <li>Updated pictures in Chapter 2</li> <li>Updated OpenVPN configuration in Chapter 4.3.2</li> <li>Other minor editorial changes</li> </ul>
Jul. 20, 2017	3.0.0	v.4.0.2	Updated the description of DI/DO interface
Aug. 11, 2017	3.0.0	v.4.0.4	Added the new model R3000-NU to the ordering information
Feb.26, 2018	3.0.5	v.4.0.8	Updated firmware
Jun. 29, 2018	3.0.5	v.4.0.9	Revised the company name
Jan. 29, 2019	3.0.5	v.4.0.15	<ul><li> Revised the certifications</li><li> Revised the Frequency bands of Wifi</li></ul>
Jul. 22, 2019	3.0.5	v.4.1.0	<ul> <li>Revised the description of enclosure</li> <li>Revised the Regulatory and Type Approval Information</li> </ul>
Sep. 23, 2019	3.0.5	v.4.1.1	Revised the Approvals
Oct. 23, 2019	3.0.5	v.4.1.2	<ul><li>Added the DNP3 Transparent to Serial port</li><li>Added the Storage Temperature</li></ul>
Nov. 26, 2019	3.0.5	v.4.1.3	Revised the description of Update firmware via tftp
Feb. 28, 2020	3.0.5	v.4.1.4	<ul> <li>Revised the screenshot of ROS interface;</li> <li>Revised the parameter description;</li> <li>Added the related information of IPv6;</li> <li>Revised the Regulatory and Type Approval Information</li> <li>Delete the information in Key features</li> <li>Delete the information of Software in Specifications</li> <li>Delete the information of APP Center in Specifications</li> <li>Delete the information of Approvals in Specifications</li> <li>Delete the Ordering information</li> <li>Added the information of USB key</li> <li>Revised the information of IPsec VPN gateway address</li> <li>Revised the maximum count of filtering</li> <li>Revised the connector information of WiFi</li> </ul>
Aug. 6, 2020	3.0.5	v.4.1.5	<ul><li>Interface</li><li>Revised the Pin Assignment in chapter 2.1</li></ul>



			<ul> <li>Revised the serial port configuration example in chapter 4.1.4</li> <li>Revised the serial port configuration example in chapter 4.1.5</li> <li>Added the serial port configuration example in chapter 4.1.6</li> </ul>
Dec. 25, 2021	3.0.5	v.4.1.6	<ul> <li>Revised the company name</li> <li>Revised Regulatory and Type Approval Information</li> <li>Revised Disclaimer</li> </ul>



### Contents

Chapter 1	Product Overview	
1.1	Key Features	
1.2	Package Contents	
1.3	Specifications	
1.4	Dimensions	14
1.5	Warning	
Chapter 2	Hardware Installation	16
2.1	PIN Assignment	
2.2	LED Indicators	17
2.3	USB Interface	
2.4	Reset Button	19
2.5	Ethernet Ports	
2.6	Insert or Remove SIM Card/Micro SD Card	21
2.7	Attach External Antenna (SMA Type)	22
2.8	Mount the Router	
2.9	Ground the Router	
2.10	Connect the Router to a Computer	24
2.11	Power Supply	25
Chapter 3	Initial Configuration	26
3.1	Configure the PC	
3.2	Factory Default Settings	
3.3	Log in the Router	
3.4	Control Panel	
3.5	Status	
3.6	Interface > Link Manager	
3.7	Interface > LAN	50
3.8	Interface > Ethernet	
3.9	Interface > Cellular	
3.10	Interface > WiFi	
3.11	Interface > USB	69
3.12	Interface > DI/DO	
3.13	Interface > Serial Port	74
3.14	Network > Route	
3.15	Network > Firewall	
3.16	Network > IP Passthrough	
3.17	VPN > IPsec	86
3.18	VPN > OpenVPN	
3.19	VPN > GRE	
3.20	Services > Syslog	
3.21	Services > Event	
3.22	Services > NTP	
3.23	Services > SMS	
3.24	Services > Email	
3.25	Services > DDNS	

# Ørobustel

3.26	5	Serv	ices > SSH	118
3.27	7	Serv	ices > GPS	119
3.28	3	Services > Web Server		123
3.29	)	Serv	ices > Advanced	124
3.30	)	Syste	em > Debug	126
3.31	-	Syste	em > Update	127
3.32	2 !	Syste	em > App Center	128
3.33	3	Syste	em > Tools	129
3.34	L :	Syste	em > Profile	131
3.35	5	Syste	em > User Management	133
Chapter 4	4	Conf	iguration Examples	135
4.1		Inter	face	135
	4.1.1	L	Console Port	135
	4.1.2	2	Digital Input	135
	4.1.3	3	Digital Output	136
	4.1.4	ŀ	1*RS-232+1*RS-485	136
	4.1.5	5	2*RS-232	136
	4.1.6	5	2*RS-485	137
4.2		Cellu	lar	138
	4.2.1	. Cel	lular Dial-Up	138
	4.2.2	2 SM	S Remote Control	140
4.3		Netv	vork	142
	4.3.1	L	IPsec VPN	142
	4.3.2	<u>)</u>	OpenVPN	147
	4.3.3	3	GRE VPN	149
Chapter !	5	Intro	ductions for CLI	152
5.1	,	Wha	t Is CLI	152
5.2	I	How	to Configure the CLI	154
5.3	3 Commands Reference		154	
5.4		Quic	k Start with Configuration Examples	155
Glossary	•••••	•••••		162

# **Chapter 1 Product Overview**

### **1.1 Key Features**

The Robustel Industrial Dual SIM Cellular VPN Router (R3000) is a rugged cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

R3000 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, C++. It also provides rich Apps to meet fragmented IoT market demands.

### **1.2** Package Contents

Before installing your R3000 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 R3000 Industrial Dual SIM Cellular VPN Router (GPS/WiFi optional)









With WiFi and GPS

Only with GPS

Only with WiFi

Without WiFi and GPS

• 1 x 3-pin 5 mm male terminal block with lock for power supply





• 1 x 7-pin 3.5 mm male terminal block with lock for serial port, I/O and console port



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



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

#### **Optional Accessories** (sold separately):

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





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





• Wall mounting kit



• 35 mm DIN rail mounting kit



• Ethernet cable



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



### **1.3 Specifications**

#### **Cellular Interface**

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA-K
- SIM: 2 (3.0 V & 1.8 V)
- Standards: GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE
   GSM: max DL/UL = 9.6/2.7 Kbps
   GPRS: max DL/UL = 86 Kbps
   EDGE: max DL/UL = 236.8 Kbps
   WCDMA/TD-SCDMA: max DL/UL = 2.8 Mbps/384 Kbps



EVDO: max DL/UL = 5.4 Mbps/14.7 Kbps HSPA+: max DL/UL = 21/5.76 Mbps, fallback to 2G DC-HSPA+: max DL/UL = 42/5.76 Mbps, fallback to 2G FDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/3G TDD LTE: max DL/UL = 100/50 Mbps, fallback to 2G/3G

#### **Ethernet Interface**

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

#### WiFi Interface (Optional)

- Number of antennas: 1
- Connector: RP-SMA-K
- Standards: 802.11a/b/g/n, supporting AP and Client modes
  - Frequency bands: 2.4 GHz

5 GHz

- Security: Open ,WPA, WPA2, WEP
- Encryption: AES, TKIP, WEP64
- Data speed: Up to 150 Mbps

•	Receiving sensitivi	ty: 1 M	-97 dBm (< 8% PER)
	(+/- 1 dBm)	54 Mbps	-76.5 dBm (< 10% PER)
		MCS7 (20 MHz)	-72 dBm (< 10% PER)
		MCS7 (40 MHz)	-69 dBm (< 10% PER)

#### **GPS/GLONASS Interface** (Optional)

- Number of antennas: 1
- Connector: SMA female with 50 ohms impedance
- Tracking sensitivity: GPS: greater than -148 dBm

GLONASS: greater than -140 dBm

• Horizontal position accuracy: GPS: 2.5 m

GLONASS: 4.0 m

• Protocol: NMEA-0183 V2.3

#### **Serial Interface**

- Number of ports: 1 x RS-232 and 1 x RS-485, The hardware is configurable as 2 x RS-485 or 2 x RS-232
- Connector: 7-pin 3.5 mm female socket with lock
- ESD protection: ±15 KV
- Baud rate: 300 bps to 230400 bps
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)

#### DI/DO

- Type: 2 x DI (dry contact) + 2 x DO (wet contact), 4 x DI, 4 x DO, 3 x DI + 1 x DO or 3 x DO + 1 x DI
- Connector: 7-pin 3.5 mm female socket with lock



- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: "V+" +5V DC (DI), 30V DC (DO)
- Absolute maximum ADC: 300 mA

#### Others

- 1 x RST button
- 1 x Micro SD interface
- 1 x USB 2.0 host up to 480 Mbps
- 1 x CLI interface
- LED indicators 1 x RUN, 1 x PPP, 1 x USR, 1 x RSSI, 1 x NET, 1 x SIM

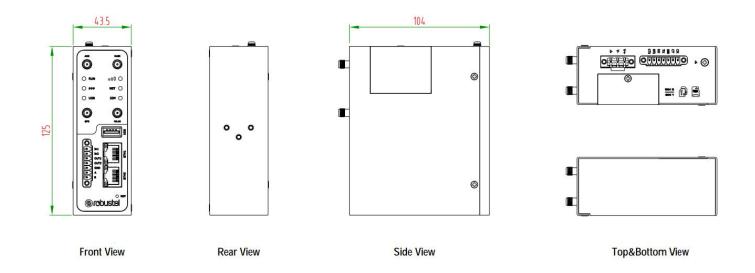
#### Power Supply and Consumption

- Connector: 3-pin 5 mm female socket with lock
- Input voltage: 9 to 60V DC
- Power consumption: Idle: 100 mA@12 V;Data link: 400 mA (peak) @12 V

#### **Physical Characteristics**

- Ingress protection: IP30
- Housing & Weight: Metal, 570 g
- Dimensions: 125 x 104 x 43.5 mm
- Installations: Desktop, wall mounting or 35 mm DIN rail mounting

### 1.4 Dimensions



#### 1.5 Warning

WARNING - EXPLOSION HAZAD. DO NOT REMOVE OR REPLACE WHILE CIRCUIT IS LIVE UNLESS THE AREA IS FREE OF

IGNITIBLE CONCENTRATIONS.

AVERTISSEMENT — RISQUE D'EXPLOSION. NE PAS RETIRER OU REMPLACER LORSQUE LE CIRCUIT EST SOUS TENSION, À MOINS QUE LE MILIEU SOIT LIBRE DE SUBSTANCES INFLAMMABLES CONCENTRÉES.

# **Chapter 2 Hardware Installation**

### 2.1 PIN Assignment







IN1 IN2

GN

PIN	Debug	RS-232	Direction
1	CR		$R3000 \leftarrow Device$
2	СТ		$R3000 \rightarrow Device$
3	GND	GND	
4		TXD	$R3000 \rightarrow Device$
5		RXD	$R3000 \leftarrow Device$
6		RTS	$R3000 \rightarrow Device$
7		CTS	R3000 ← Device
	AA71		('

Note: When the device is configured as 2\*RS-485, the pin is defined as follows:

PIN	Debug	RS-485	Direction
4		Data+(A)	$R3000 \rightarrow Device$
5		Data- (B)	$R3000 \leftarrow Device$

PIN	Power
8	Positive
9	Negative
10	GND

PIN	DI/DO	RS-485	Direction
11	Input 1		$R3000 \leftarrow Device$
12	Input 2		$R3000 \leftarrow Device$
13	Output 1		$R3000 \rightarrow Device$
14	Output 2		$R3000 \rightarrow Device$
15	GND		
16		Data+(A)	$R3000 \leftrightarrow Device$
17		Data- (B)	$R3000 \leftrightarrow Device$

PIN	DI/DO	RS-232	Direction
11	Input 1		R3000 ← Device
12	Input 2		R3000 ← Device
13	Output 1		$R3000 \rightarrow Device$
14	Output 2		$R3000 \rightarrow Device$
15	IO_GND		
16		TXD	$R3000 \leftrightarrow Device$
17		RXD	$R3000 \leftrightarrow Device$
3		GND	

Note: When PIN16/PIN17 is configured as RS-232, the GND of RS-232 should be connected to PIN3.

AUX	MAIN
O RUN	•11 •
• ррр	NET 🔵
USR	SIM 🔵
GPS	WLAN
	nd all all all all all all all all all al
Ini Ini In2 OUTI OUTI GND	ETHI
B B	ETHO
@ rot	oustel



### 2.2 LED Indicators



Name	Color	Status	Description
RUN	Green	On, fast blinking	Router is powered on
		(250 mSec blink time)	(System is initializing)
		On, blinking	Router starts operating
		(500 mSec blink time)	
		Off	Router is powered off
РРР	Green	On, solid	Link connection is working
		Off	Link connection is not working
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, solid	High Signal strength (21-31) is available
•••	Yellow	On, solid	Medium Signal strength (11-20) is available
	Red	On, solid	Low Signal strength (1-10) is available
		Off	No signal
NET	Green	On, solid	Connection to 4G network is established
	Yellow	On, solid	Connection to 3G network is established



	Red	On, solid	Connection to 2G network is established
		Off	Connection to network is not established or establishing
SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used

Note: You can choose the display type of USR LED. For more details, please refer to 3.29 Service > Advanced.

### 2.3 USB Interface



Function	Operation
Firmware	USB interface is used for batch firmware upgrading, but cannot
upgrade	be used for sending or receiving data from slave devices which
	connected to it. You can insert a USB storage device into the
	router's USB interface, such as a U disk or a hard disk. If there
	have a supported configuration file or a router firmware in this
	USB storage device, the router will automatically update the
	configuration file or the firmware. For more details, see 3.11
	Interface > USB.



### 2.4 Reset Button



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

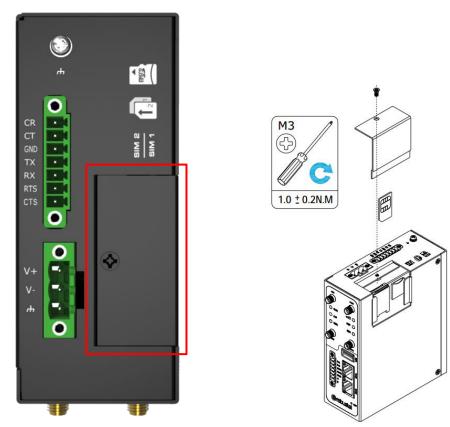
### 2.5 Ethernet Ports



There are two Ethernet ports on R3000 Router, including ETH0 and ETH1. Each Ethernet port has two LED indicators. The yellow one is a link indicator, while the green one is a speed indicator. 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
Speed indicator	On, solid	100 Mbps mode
	Off	10 Mbps mode

### 2.6 Insert or Remove SIM Card/Micro SD Card



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

#### • Insert SIM card/Micro SD 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/SD card slot.
- 3. To insert SIM card/Micro SD 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/Micro SD 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/SD card slot.
- 3. To remove SIM card/Micro SD 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.

### 2.7 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the router's antenna connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance. **Note:** Recommended torque for tightening is 0.35 N.m.

### 2.8 Mount the Router

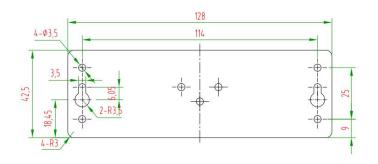
The router can be placed on a desktop or mounted to a wall or a 35 mm DIN rail. **Note:** 

When used, the device needs a suitable environment.

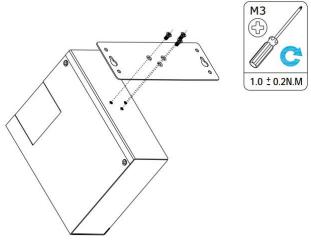
- 1. If indoors, it needs to be provided an indoor enclosure.
- 2. If outdoors, it needs to be provided a rain proof enclosure.

#### Two methods for mounting the router

1. Wall mounting (measured in mm)

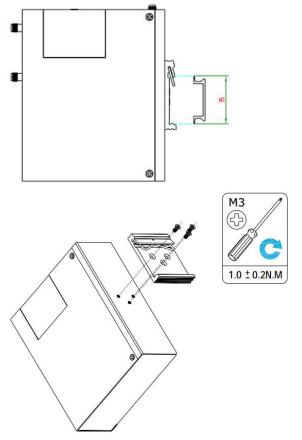






Use 3 pcs of M3\*4 flat head Phillips screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall. **Note:** Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.

2. DIN rail mounting (measured in mm)



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.



### 2.9 Ground the Router

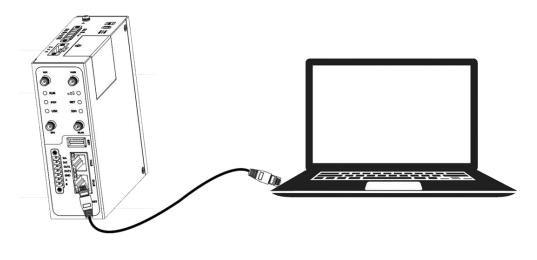
Router grounding helps prevent the noise effect due to electromagnetic interference (EMI). Connect the router to the site ground wire by the ground screw before powering on.

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

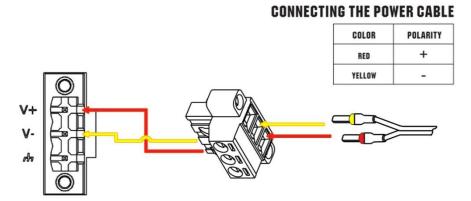


### 2.10 Connect the Router to a Computer

Connect an Ethernet cable to the port marked ETH0 or ETH1 at the front of the R3000 Router, and connect the other end of the cable to your computer.



### 2.11 Power Supply



R3000 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. The last step is to plug the power adapter into your socket. **Note:** The range of power voltage is 9 to 60V DC.

# **Chapter 3** Initial Configuration

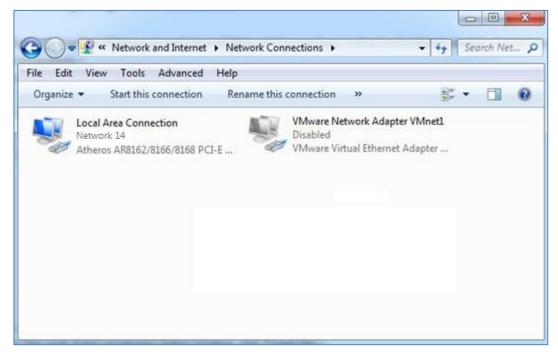
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

eneral		
Connection —		
IPv4 Connect	ivity:	Internet
IPv6 Connect	ivity:	No Internet access
Media State:		Enabled
Duration:		09:30:11
		100 0.00
Speed:		100.0 Mbps
Details	]	100.0 Mbps
Details	Sent —	100.0 Mbps
	Sent — 12,818,574	

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

Guaicomin Ame	ros AR8162/8166/816	58 PCI-E Fast Ether
		Configure
his connection uses t	200 2010 000 <b>#</b> 1666 200	
Client for Mici		
VMware Bridg		
🗹 📙 QoS Packet :		
	er Sharing for Microsoft	
	col Version 6 (TCP/IP)	and the second se
	col Version 4 (TCP/IP)	
	pology Discovery Map	
✓ ink-Layer 10	pology Discovery Res	ponder
	Uninstall	Properties
Install		
		· · · · · · · · · · · · · · · · · · ·
Description	Protocol/Internet Pro	tocol. The default

Select Internet protocol version 6 (TCP/IPv6), and click Properties.



Connect using	3 		omoan		
Realtek	PCIe GbE Fa	amily Controller	#2		
				Configure	
his connectio	on uses the fo	llowing items:			
Client	for Microsoft	Networks			
		Bridged Networ	king Drive	er	
	are Bridge Pro				Ξ
	Packet Sche				
🗹 📑 File a		aring for Micros		rks	-
J. Intern	at Dusta and M				
		2 T			
		ersion 6 (TCP/ ersion 4 (TCP/		+	-
		ersion 4 (TCP/		▶ Properties	•
<ul> <li>✓ Intern</li> <li></li> </ul>		ersion 4 (TCP/		▶ Properties	•
Inter     Install	et Protocol V	ersion 4 (TCP/	1Pv4)		-

4. Two ways for configuring the IP address of PC **Obtain an IP address automatically:** 

General	Alternate Configuration					
this cap	get IP settings assigned au ability. Otherwise, you need appropriate IP settings.					
Ob	otain an IP address automati	cally				
Us	e the following IP address: -					
IP ac	ldress:			2		
Subnet mask: Default gateway:						
		40	- 3	3		
o Ob	otain DNS server address aut	omatically				
- O Us	e the following DNS server a	ddresses:				
Prefe	erred DNS server:		97	a.		
Alter	nate DNS server:			•		
V	alidate settings upon exit			Adv	anced	. ]
						_



General		
	ned automatically if your network supports this r network administrator for the appropriate IPv	
Obtain an IPv6 address au	tomatically	
OUse the following IPv6 add	ress:	
IPv6 address:		
Subnet prefix length:		
Default gateway:		
Obtain DNS server address	automatically	
OUse the following DNS serv	er addresses:	
Preferred DNS server:		
Alternate DNS server:		
Validate settings upon ex	t	Advanced

#### Use the following IP address:

(Configured a static IP address manually within the same subnet of the router)

eneral				
	automatically if your network supports eed to ask your network administrator			
Obtain an IP address auton	natically			
Use the following IP addres	s:			
IP address:	192.168.0.2			
Subnet mask:	255 . 255 . 255 . 0			
Default gateway:	192.168.0.1			
Obtain DNS server address	automatically			
O Use the following DNS serve	er addresses:			
Preferred DNS server:	192 . 168 . 0 . 1			
Alternate DNS server:	e > a			
Validate settings upon exit	Advanced			

General		
	ed automatically if your network supports this capability. r network administrator for the appropriate IPv6 settings.	
🔘 Obtain an IPv6 address au	tomatically	
() Use the following IPv6 add	ress:	
IPv6 address:	2421:da8:202:10:e5d8:fe17:b400:d2e	
Subnet prefix length:	64	
Default gateway:	2421:da8:202:10:36fa:40ff:fe0c:e470	
Obtain DNS server address	automatically	
• Use the following DNS serv	er addresses:	
Preferred DNS server:		
Alternate DNS server:		
🔲 Vaļidate settings upon exit	Advanc	ed

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

### **3.2 Factory Default Settings**

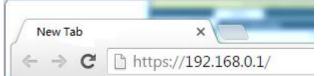
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
ETH0	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 and Firebox, etc.
- 2. From your web browser, type the IP address of the router into the address bar and press enter. The default IP address of the router is <a href="http://192.168.0.1/">http://192.168.0.1/</a>, though the actual address may vary.



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

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





### 3.4 Control Panel

After logging in, the home page of the R3000 Router's web interface is displayed, for example.

<b>Ø</b> robuste	el	Save & Apply   Reboot   Logout
	${\tilde{ A}}$ It is strongly recommended to change th	e default password. ×
	Status	
Status	∧ System Information	
Interface	Device Model	R3000-4L
Network	System Uptime	0 days, 00:24:35
VPN	System Time	Thu Nov 28 10:24:21 2019
	RAM Usage	79M Free/128M Total
Services	Firmware Version	3.3.0_20191124 (Rev 2935)
System	Hardware Version	1.2
	Kernel Version	4.1.0
	Serial Number	01870719090011
	∧ Internet Status	
	Uptime	0 days, 00:13:17
	Active IPv4 Link	WWAN1
	IPv4 Address	10.244.109.195/255.255.255.248
	IPv4 Gateway	10.244.109.193
	IPv4 DNS	120.80.80.80 221.5.88.88
	Active IPv6 Link	WWAN1
	IPv6 Address	2408:84f3:81d:daec: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 home page, users can perform operations such as saving configuration, restarting the router, and logging



out.

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

 $\underline{\mathbb{A}}$  . It is strongly recommended to change the default password.

Click 🔀 to close the popup. It is strongly recommended for security purposes that you change the default

username and/or password. To change your username and/or password, see 3.35 System > User Management.

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

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

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

### 3.5 Status

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



### **System Information**

▲ System Information	
Device Model	R3000-4L
System Uptime	0 days, 00:24:35
System Time	Thu Nov 28 10:24:21 2019
RAM Usage	79M Free/128M Total
Firmware Version	3.3.0_20191124 (Rev 2935)
Hardware Version	1.2
Kernel Version	4.1.0
Serial Number	01870719090011

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**

0 days, 00:13:17
WWAN1
10.244.109.195/255.255.255.248
10.244.109.193
120.80.80.80 221.5.88.88
WWAN1
2408:84f3:81d:daec:1e:10ff:fe1f:0/64
fe80::4e54:99ff:fe45:e5d5
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.	
IPIPv4 Address	Show the IPv4 address of current link.	
IPv4 Gateway	Show the IPv4 gateway of the current link.	
IPv4 DNS	Show the current IPv4 DNS server.	
IPv6 Link Description	Show the currently online link: WWAN1, WWAN2, WAN or WLAN.	
IPIPv6 Address	Show the IPv6 address of current link.	
IPv6 Gateway	Show the IPv6 gateway of the current link.	
IPv6 DNS	Show the current IPv6 DNS server.	

### LAN Status

∧ LAN Status	
IP Addres	s 192.168.0.1/255.255.0
Active IPv6 Addres	s 2121:da8:202:10:36fa:40ff:fe18:68a8/64
Inactive IPv6 Addres	5
MAC Addres	s 34:FA:40:18:68:A8

LAN Status		
Item	Description	
IP Address	Show the IPv4 address and the Netmask of the router.	
IPv6 Address	Shows the IPv6 address and prefix length obtained by the router along with the current backup link.	
Inactive IPv6 Address	Shows the IPv6 address and prefix length obtained by the router along with the current online link.	
MAC Address	Show the MAC address of the router.	

### 3.6 Interface > Link Manager

This section allows you to setup the link connection.

Link Manager	Status		
∧ General Settings			
	Primary Link	WWAN1 V	0
	Backup Link	WWAN2 V	
	Backup Mode	Cold Backup v	0
	Revert Interval	0	) 🤊
	Emergency Reboot	OFF 😨	

General Settings @ Link Manager		
Item	Description	Default
Primary Link	<ul> <li>Select from "WWAN1", "WWAN2", "WAN" or "WLAN".</li> <li>WWAN1: Select to make SIM1 as the primary wireless link</li> <li>WWAN2: Select to make SIM2 as the primary wireless link</li> <li>WAN: Select to make WAN Ethernet port as the primary wired link Note: WAN link is available only if enable eth0 as WAN port in Interface &gt; Ethernet &gt; Ports &gt; Port Settings.</li> <li>WLAN: Select to make WLAN as the primary wireless link Note: WLAN link is available only if enable WiFi as Client mode, please refer to 3.10 Interface &gt; WiFi.</li> </ul>	WWAN1
Backup Link	<ul> <li>Select from "None", "WWAN1", "WWAN2", "WAN" or "WLAN".</li> <li>None: Do not select any backup link</li> <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 backup wired link</li> <li>Note: WAN link is available only if enable eth0 as WAN interface in Interface &gt; Ethernet &gt; Ports &gt; Port Settings.</li> <li>WLAN: Select to make WLAN as the backup wireless link</li> </ul>	
Backup Mode	<ul> <li>refer to 3.10 Interface &gt; WiFi.</li> <li>Select from "Cold Backup", "Warm Backup" or "Load Balancing".</li> <li>Cold Backup: The inactive link is offline on standby</li> <li>Warm Backup: The inactive link is online on standby</li> <li>Note: Warm backup mode is not available for dual SIM backup.</li> <li>Load Balancing: Use two links simultaneously</li> </ul>	
Revert Interval	<ul> <li>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.</li> <li>Note: Revert interval is available only under the cold backup mode.</li> </ul>	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

Note: Click 🕝 for help.

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

∧ Link Settings					
Index	Туре	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 Con the right-most of WWAN1/WWAN2 to enter the configuration window.

#### WWAN1/WWAN2

Link Manager	
∧ General Settings	
Index	1
Туре	WWAN1 Y
Description	admin
IPv6 Enable	ON DEE

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

A WWAN Settings					
Automatic APN Selection	ON OFF				
Dialup Number	*99***1#				
Authentication Type	Auto				
Aggressive Reset	ON OF ?				
Switch SIM By Data Allowance	OFF 7				
Data Allowance	0 ⑦				
Billing Day					

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

∧ WWAN Settings	
Automatic APN Selection	OFF
APN	internet
Username	
Password	•••••
Dialup Number	<b>*99***</b> 1#
Authentication Type	Auto
PPP Preferred	OFF ⑦
Switch SIM By Data Allowance	OFF 7
Data Allowance	0 7
Billing Day	

∧ IPv6 LAN Settings	
Connection Type	Static
IPv6 Prefix	2521:da8:202:10::/64
IPv6 NAT Enable	ON DEF

▲ Ping Detection Settings		0
Enable	ON OT	
IPV4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114.114	
IPv6 Primary Server	2001:4860:4860::888	
IPv6 Secondary Server	2400:da00:2::29	
Interval	300	3
Retry Interval	5	3
Timeout	3	0
Max Ping Tries	3	0



∧ Advanced Settings	
IPv4 NAT Enable	ON OFF
Upload Bandwidth	10000 🧿
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON DEE
Verbose Debug Enable	OFF OFF

Link Settings (WWAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	
Туре	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
IPv6	Click the toggle button to enable / disable IPv6.	OFF
	WWAN Settings	·
Automatic APN	Click the toggle button to enable/disable the "Automatic APN Selection"	ON
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.	
APN	Enter the Access Point Name for cellular dial-up connection, provided by	internet
	local ISP.	
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	*99***1#
	ISP.	
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	Click the toggle button to enable/disable this option. After enabling, it will	OFF
Allowance	switch to another SIM when the data limit reached.	
	Note: Only used for dual SIM backup.	
Data Allowance	Set the monthly data traffic limitation. The system will record the data	0
	traffic statistics when data traffic limitation (MiB) is specified. The traffic	
	record will be displayed in Interface > Link Manager > Status > WWAN	
	Data Usage Statistics. 0 means disable data traffic record.	
Billing Day	Specify the monthly billing day. The data traffic statistics will be	1
	recalculated from that day.	
	IPv6 LAN Settings	1
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	ON
	keep-alive policy of the router.	
IPv4 Primary Server	Router will ping this primary address/domain name to check that if the	8.8.8.8
	current IPv4 connectivity is active.	
IPv4 Secondary Server	Router will ping this secondary address/domain name to check that if the	114.114.11
	current IPv4 connectivity is active.	4.114
IPv6 Primary Server	Router will ping this primary address/domain name to check that if the	2001:4860
	current IPv6 connectivity is active.	4860::8888
IPv6 Secondary Server	Router will ping this secondary address/domain name to check that if the	2400:da00
	current IPv6 connectivity is active.	2::29
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again	5
	every retry interval.	
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if	3
	the max continuous ping tries reached.	
	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 the Primary DNS server	Defines the primary IPv4 DNS server used by the link.	Null
Specify the Secondary DNS server	Defines the Secondary IPv4 DNS server used by the link.	Null
Specify the IPv6	Defines the primary IPv6 DNS server used by the link.	Null
Primary DNS server		
, Specify the IPv6	Defines the Secondary IPv6 DNS server used by the link.	Null
Secondary DNS server		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging	ON
	information output.	
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose	OFF
	debugging information output.	

## WAN

Router will obtain IP automatically from DHCP server if choosing "DHCP" as **IPv4 connection type**. Router will obtain IPv6 prefix automatically from DHCP server if choosing "SLAAC" as **IPv6 connection type**. The window is displayed as below.



Link Manager	A strain the second
∧ General Settings	
Index	3
Туре	WAN
Description	admin
IPv6 Enable	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			
Туре	WAN			
Description				
Connection Type	Static			
<ul> <li>Static Address Settings</li> </ul>	Static Address Settings			
IP Address	0			
Gateway				
Primary DNS				
Secondary DNS				

∧ General Settings	
Index	3
Туре	WAN
Description	admin
IPv6 Enable	OTTO
IPv4 Connection Type	Static
IPv6 Connection Type	Static
∧ Static Address Settings	
IP Address	
Gateway	
Primary DNS	
Secondary DNS	
NIPv6 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	3
Туре	WAN
Description	
Connection Type	PPPoE
∧ PPPoE Settings	
Username	
Password	
Authentication Type	Auto
PPP Expert Options	0
∧ General Settings	
Index	3
Туре	WAN
Description	admin
IPv6 Enable	OFF
IPv4 Connection Type	PPPoE
IPv6 Connection Type	PPPoE
Address Mode	SLAAC
∧ PPPoE Settings	
Username	
Password	
Authentication Type	Auto
PPP Expert Options	
▲ Ping Detection Settings	(?
Enable	
IPV4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::888
IPv6 Secondary Server	2400:da00:2::29
Interval	300 🦻
Retry Interval	5 3
Timeout	3
Max Ping Tries	3



▲ Advanced Settings	
IPv4 NAT Enable	ON OFF
мти	1500
Upload Bandwidth	10000 🧿
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON OFF
Verbose Debug Enable	ON OFF

Link Settings (WAN)		
Item	Description	Default
	General Settings	
Index	Indicate the ordinal of the list.	
Туре	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 IP" or "PPPoE".	DHCP
IPv6 connection type	Select from "SLAAC", "DHCPv6", "Static IP" or "PPPoE".	SLAAC
Address type	Select from "SLAAC"or "DHCPv6".	SLAAC
	IPv4 Static Address Settings	
IP Address	Set the IPv4 address with Netmask which can access the	Null
	internet.	
	IP address with Netmask, e.g. 192.168.1.1/24	
Gateway	Set the gateway of the IPv4 address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
	IPv6 Static Address Settings	
IPv6 Address	Set the IPv6 address with Netmask which can access the	Null
	internet.	
	IP address with Netmask, e.g. 2521:da8:202:10::20/64	
Gateway	Set the gateway of the IPv6 address in WAN port.	Null
IPv6 Primary DNS	Set the primary IPv6 DNS server used by the link.	Null
IPv6 Secondary DNS	Set the secondary IPv6 DNS server used by the link.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can	Null
	enter some other PPP dial strings in this field. Each string can be	



	separated by a semicolon.	
	IPv6 LAN Settings	
Connection type	Select the link to assign IPv6 prefixes to the LAN.	Delegated
IPv6 Prefix	Sets the static IPv6 prefix assigned by the link to the LAN.	Null
Enabled IPv6 NAT	Set up links to enable IPv6 NAT.	OFF
	Ping Detection Settings	
Enable	Click the toggle button to enable/disable the ping detection	ON
	mechanism, a keep-alive policy of the router.	
Primary Server	Router will ping this primary address/domain name to check that	8.8.8.8
	if the current IPv4 connectivity is active.	
Secondary Server	Router will ping this secondary address/domain name to check	114.114.114.114
	that if the current IPv4 connectivity is active.	
IPv6 Primary Server	Router will ping this primary address/domain name to check that	2001:4860:4860::888
	if the current IPv6 connectivity is active.	8
IPv6 Secondary Server	Router will ping this secondary address/domain name to check	2400:da00:2::29
	that if the current IPv6 connectivity is active.	2400.0000.229
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping	5
	again every retry interval.	
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency	3
	action if the max continuous ping tries reached.	
	Advanced Settings	
NAT Enable	Click the toggle button to enable/disable the Network Address	ON
	Translation option.	
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 the Primary	Defines the primary IPv4 DNS server for the link.	Null
DNS server		
Specify the Secondary	Defines the secondary IPv4 DNS server for the link.	Null
DNS server		
Specify the IPv6	Defines the primary IPv6 DNS server for the link.	Null
Primary DNS server		
Specify the IPv6	Defines the secondary IPv6 DNS server for the link.	Null
Secondary DNS server		
Debug Enable	Click the toggle button to enable/disable this option. Enable for	ON
	debugging information output.	
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for	OFF
	verbose debugging information output.	

## 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	4				
Туре	WLAN				
Description					
IPv6 Enable	OR OFF				
IPv4 Connection Type	DHCP				
∧ WLAN Settings					
SSID	router				
Connect to Hidden SSID	OFF				
Password					

The window is displayed as below when choosing "Static" as the IPv4 connection type.

∧ General Settings					
	Index	4			
	Туре	WLAN			
	Description				
	IPv6 Enable	OFF			
	IPv4 Connection Type	Static v			
✓ WLAN Settings					
∧ Static Address Setti	ngs				
	IP Address		0		
	Gateway				
	Primary DNS				
	Secondary DNS				

### R3000 Router does not support the **PPPoE** WLAN Connection Type.

▲ IPv6 LAN Settings	
Connection Type	Static
IPv6 Prefix	
IPv6 NAT Enable	OFF

▲ Ping Detection Settings		0
Enable	ON DIE	
IPV4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114	
IPv6 Primary Server	2001:4860:4860::888	
IPv6 Secondary Server	2400:da00:2::29	
Interval	300	3
Retry Interval	5	3
Timeout	3	3
Max Ping Tries	3	1
<ul> <li>Advanced Settings</li> </ul>		
IPv4 NAT Enable	ON OTT	
МТИ	1500	0
Upload Bandwidth	10000	7

ON

OFF

**Download Bandwidth** 

**Overrided Primary DNS** 

Verbose Debug Enable

**Debug Enable** 

**Overrided Secondary DNS** 

Overrided IPv6 Primary DNS

**Overrided IPv6 Secondary DNS** 

Link Settings (WLAN)					
Item	Default				
	General Settings				
Index	Indicate the ordinal of the list.				
Туре	Show the type of the link.	WLAN			
Description	Enter a description for this link.	Null			
Enable Ipv6	ov6 Click the toggle button to enable / disable IPv6. OFF				
IPv4 Connection Type	Pv4 Connection Type Select from "DHCP" or "Static".				
	WLAN Settings				
SSID	Enter a 1-32 characters SSID which your router wants to connect.	router			
	SSID (Service Set Identifier) is the name of your wireless network.				
Connect to Hidden	Click the toggle button to enable/disable this option. When	OFF			
SSID	router works as Client mode and needs to connect any access				
	point which has hidden SSID, you need to enable this option.				
Password	Enter an 8-63 characters password of the access point which your	Null			
	router wants to connect.				

10 robustel



	Static Address Settings	
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
	IPv6 LAN Settings	1
Connection type	Select the link to assign IPv6 prefixes to the LAN.	Delegated
IPv6 Prefix	Sets the static IPv6 prefix assigned by the link to the LAN.	Null
Enabled IPv6 NAT	Set up links to enable IPv6 NAT.	OFF
	Ping Detection Settings	1
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	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	2400:da00:2::29
Internel	that if the current IPv6 connectivity is active.	200
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		3
	Set the ping timeout.	
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency	3
	action if the max continuous ping tries reached.	
NAT Enable	Advance Settings Click the toggle button to enable/disable the Network Address	ON
	Translation option.	
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 the Primary DNS server	Defines the primary IPv4 DNS server for the link.	Null
Specify the Secondary DNS server	Defines the secondary IPv4 DNS server for the link.	Null
Specify the IPv6 Primary DNS server	Defines the primary IPv6 DNS server for the link.	Null
Specify the 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	OFF



verbose debugging information output.

### Status

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

Link Manag	jer 💦	Status			
Link Sta	tus				
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.

Index	IPv4 Link	IPv6 Link	Statu	ıs Uptime	
1	WWAN1	WWAN1	Connec	ted 0 days, 06:54	
			Index	1	
		IPv	4 Link	WWAN1	
		IPv	6 Link	WWAN1	
		3	Status	Connected	
		IPv4 Int	erface	wwan	
		IPv6 Int	erface	wwan	
		U	Iptime	0 days, 06:54:37	
		IPv4 Ad	ddress	10.37.98.229/255.255.255.252	
		IPv4 Ga	teway	10.37.98.230	
		IPv	4 DNS	120.80.80.80 221.5.88.88	
		IPv6 Ac	ddress	2408:84f3:1034:96f9:1e:10ff:fe1f:0/64	
		IPv6 Ga	teway	fe80::4e54:99ff:fe45:e5d5	
		IPv	6 DNS	2408:805d:8:: 2408:805c:4008::	
		RX Pa	ackets	712	
		TX Pa	ackets	979	
		RX	Bytes	47530	
		тх	Bytes	80258	
2	WWAN2	NONE	Disconn	ect	



∧ WWAN Data Usage Statistics		?
WWAN1 Monthly Stats	Clear	
WWAN2 Monthly Stats	Clear	

Click the **Clear** button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will be displayed

only if enable the Data Allowance function in Interface > Link Manager > Link Settings > WWAN Settings > Data Allowance.

# 3.7 Interface > LAN

This section allows you to set the related parameters for LAN port. There are two LAN ports on R3000 Router, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from Ian0 and Ian1, but at least one LAN port must be assigned as Ian0. The default settings of ETH0 and ETH1 are Ian0 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	N	Multiple IP	Sta	atus	
^ Netwo	ork Settir	ngs			7
Index	Interfac	e IPv4 Addre	Netmask	VLAN ID	+
1	lan0	192.168.0.1 2	255.255.255.0	0	⊠×⊇

### **Note:** Lan0 cannot be deleted.

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

LAN	
∧ General Settings	
Index	1
Interface	lan0 V
IPv4 Address	192.168.2.1
Netmask	255.255.255.0
IPv6 Address Allocation Type	SLAAC
MTU	1500 🧿

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



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

∧ DHCP Settings	
Enable	ON OFF
Mode	Server
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	0
Expert Options	0
Debug Enable	OFF

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

∧ DHCP Settings	
Enable	ON OFF
Mode	Relay
DHCP Server For Relay	
A DHCP Advanced Settings	
Debug Enable	ON OFF

LAN						
Item	Default					
	DHCP Settings					
Enable	able Click the toggle button to enable/disable the DHCP function. Of					
Mode	Mode Select from "Server" or "Relay".					
	Server: Lease IP address to DHCP clients which have been					
	connected to LAN port					
	• Relay: Router can be DHCP Relay, which will provide a relay					
	tunnel to solve problem that DHCP Client and DHCP Server is not					
	in a same subnet					
IP Pool Start	Define the beginning of the pool of IP addresses which will be leased	192.168.0.2				
	to DHCP clients.					
IP Pool End	Define the end of the pool of IP addresses which will be leased to	192.168.0.100				



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

# Multiple IP

LA	N	Multiple IP	Status	
∧ Multip	ole IP Setti	ngs		
Index	Interface	IP Address	Netmask	+

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

Multiple IP	
∧ IP Settings	
Index	1
Interface	lan0 v
IP Address	
Netmask	

**IP Settings** 



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

## **VLAN Trunk**

LAN		Multiple I	Р	VLAN Trunk	Status	
~ VLAN	Settings					
Index	Enable	Interface	VID	IP Address	Netmask	+

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

VLAN Trunk	
∧ VLAN Settings	
Index	1
Enable	ON OFF
Interface	lan0 v
VID	100
IP Address	
Netmask	

VLAN Trunk				
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 port.	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		
∧ Interfa	ice Status				
Index	Interface	IP Address	Active IPv6 Addre	55	
1	lan0	192.168.0.1/25	5.2 2121:da8:202:10:36	fa:	
Index	cted Device IPv4/IP	v6 Address	MAC Address	Interface	Inactive Time
1	192.1	68.0.59	D0:50:99:A9:2B:80	lan0	0s
∧ DHCP	Lease Tabl	e			
Index	IPv4/IP	v6 Address	MAC Address or IAID	Interface	Expired Time

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

∧ Connec	ted Devices					
Index	IPv4/IPv6 Address	MAG	C Address	Interface	Inactive Time	
1	192.168.0.59	D0:50:	99:A9:2B:80	lan0	0s	
		Index	1			
	IPv4/IPv	6 Address	192.168.0.59			
	MA	C Address	D0:50:99:A9:	2B:80		
		Interface	lan0			
	Inac	tive Time	0s			

## 3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on R3000 Router, including ETH0 and ETH1. The ETH0 on the router can be configured as either a WAN or a LAN port, while ETH1 can only be configured as a LAN port. By default, ETH0 and ETH1 are lan0, and their IP are 192.168.0.1/255.255.255.0. Since lan0 must be assigned to one port and WAN port must be assigned to the ETH0, there are four configurations. You can choose the appropriate configuration to fit your current needs. The specific port configurations are shown below.

Ports		Status	
∧ Port Se	ettings		2
Index	Port	Port Assignment	
1	eth0	lan0	
2	eth1	lan0	
∧ Port Se	ttings		2
Index	Port	Port Assignment	
1	eth0	lan0	
2	eth1	lan1	



Port Se	ettings		0
Index	Port	Port Assignment	
1	eth0	lan1	
2	eth1	lan0	
• Port Se	ettings		0
∧ Port Se Index	ettings Port	Port Assignment	7
		Port Assignment wan	() ()

This section introduces you to set the parameters of the WAN port.

Ports		Status	
∧ Port Se	ttings		0
Index	Port	Port Assignment	
1	eth0	wan	
2	eth1	lan0	

Click button of eth0 to configure its parameters. The port assignment can be changed by selecting from the drop

Ports	
∧ Port Settings	
Index	2
Port	eth1 v
Port Assignment	lan0 🤍 🍞

	Port Settings				
Item	tem Description				
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 a LAN port. When setting the lan0				
	port as a LAN port in Interface > LAN > LAN > Network Settings > General Settings,				
	you can click the drop-down list to select from "lan0" or "lan1".				



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

Ports		Status
A Port Sta	atus	
Index	Port	Link
1	eth0	Down
2	eth1	Up

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

Port Sta	ntus			
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 R3000 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.

Cellu	lar	Status	AT Debug		
^ Advan	ced Cellula	ar Settings			
Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	
2	SIM2		Auto	All	

### Click of SIM 1 to edit the parameters.

Cellular	
∧ General Settings	
Index	1
SIM Card	SIM1 V
Phone Number	
PIN Code	0
Extra AT Cmd	0
Telnet Port	0 7

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



∧ Cellular Network Settings	
Network Type	Auto 🔽 🕜
Band Select Type	All V 🖓
<ul> <li>Advanced Settings</li> </ul>	
Debug Enable	ON DEF
Verbose Debug Enable	OFF

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

∧ Cellular Network Settings	
Network Type	Auto 🤍 🧿
Band Select Type	Specify 🤍 🧿
∧ Band Settings	
GSM 850	OFF
GSM 900	OT OFF
GSM 1800	ON OFF
GSM 1900	ON OFF
WCDMA 850	ON OFF
WCDMA 900	ON OFF
WCDMA 1900	OH OFF
WCDMA 2100	OM OFF
LTE Band 1	ON OFF
LTE Band 2	OT OFF
LTE Band 3	ON OFF
LTE Band 4	ON OFF
LTE Band 5	OW OFF
LTE Band 7	ON OFF
LTE Band 8	OFF
LTE Band 20	OT OFF
	2

∧ Advanced Settings	
Debug Enable	ON OFF
Verbose Debug Enable	ON OFF

Cellular				
Item	Item Description Default			
General Settings				



	Cellular	
Item	Description	Default
Index	Indicate the ordinal of the list.	
SIM Card	Set the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
	Cellular Network Settings	
Network Type	<ul> <li>Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", "4G</li> <li>First".</li> <li>Auto: Connect to the best signal network automatically</li> <li>2G Only: Only the 2G network is connected</li> <li>2G First: Connect to the 2G Network preferentially</li> <li>3G Only: Only the 3G network is connected</li> <li>3G First: Connect to the 3G Network preferentially</li> <li>4G Only: Only the 4G network is connected</li> <li>4G First: Connect to the 4G Network preferentially</li> </ul>	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
	Advanced Settings	
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

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

Cellula	r Statu	IS AT	Debug	
Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	ME909s-120	460015006113059	Registered to home network

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

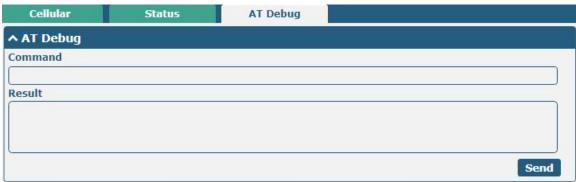
Cellular	Statu	IS AT	Debug		
∧ Status				l I	
Index Mo	dem Status			Registration	
1	Ready			Registered to home net	
		Index	1		
	1	Modem Status	Ready		
		Modem Model	ME909s-120		
		Current SIM	SIM1		
	P	hone Number			
		IMSI	460015006113059		
		ICCID	8986011880366995	52555	
		Registration	Registered to home network		
	Net	work Provider	CHN-UNICOM		
		Network Type	LTE		
		Band	1		
	Si	ignal Strength	25 (-63dBm)		
		RSRP	-90 dBm		
		RSRQ	-7.0 dBm		
		Bit Error Rate	99		
		PLMN ID	46001		
	Local Area Code				
	Cell ID				
		IMEI	867377024751079		
	Firn	nware Version	11.617.01.00.00		

Status				
Item	Description			
Index	Indicate the ordinal of the list.			
Modem Status	Show the status of the radio module.			
Modem Model	Show the model of the radio module.			
Current SIM	Show the SIM card that your router is using.			
Phone Number	Show the phone number of the current SIM.			
	Note: This option will be displayed if enter manually in Cellular > Advanced Cellular			
	Settings > SIM1/SIM2 > General Settings > Phone Number.			
IMSI	Show the IMSI number of the current SIM.			
ICCID	Show the ICCID number of the current SIM.			
Registration	Show the current network status.			
Network Provider	Show the name of Network Provider.			
Network Type	Show the current network service type, e.g. GPRS.			



Status			
Item	Description		
Registered band	Show the current frequency band.		
Signal Strength	Show the signal strength detected by the mobile.		
RSRP	Show the reference signal received power.		
RSRQ	Show the reference signal reception quality.		
Bit Error Rate	Show the current bit error rate.		
PLMN ID	Show the current PLMN ID.		
Local Area Code	Show the current local area code used for identifying different area.		
Cell ID	Show the current cell ID used for locating the router.		
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio		
	module.		
Firmware Version	Show the current firmware version of the radio module.		

### This page allows you to check the AT Debug.



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

## 3.10 Interface > WiFi

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

Note: Need to reboot to make configuration take effect if switching the AP and Client mode.

## WiFi AP

### **Configure Router as WiFi AP**

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



WiFi	Access Point	AC	L	Status	
∧ General Sett	ings				
		Mode	AP	v 7	
		Region	SE	0	

**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 Adv	anced	ACL	Status
∧ General Setting	s			
1	Enable	ON DEE	)	
	Band	2.4G	×.	
	Bandwidth	20MHz	×	
	Channe	Auto	v	
	SSIE	router999		
	Broadcast SSIE	OFF		
	Security Mode	Disabled	v 🦻	

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

WiFi	Access Point Adva	nced	ACL	Status
∧ General Setti	ngs			
	Enable			
	Band	2.4G	v	
	Bandwidth	20MHz	V	
	Channel	Auto	v	
	SSID	router999		
	Broadcast SSID	OFF		
	Security Mode	WPA-Personal	√ 😨	
	WPA Version	Auto	v	
	Encryption	Auto	v 😨	
	PSK Password		7	



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

WiFi	Access Point A	dvanced	ACL	Status
∧ General Settin	igs			
	Ena	ble ON O		
	Ba	and 2.4G	v	
	Bandwid	ith 20MHz	<b>v</b>	
	Chan	nel Auto	▼ ?	
	SS	ID router999		
	Broadcast SS			
	Security Mo	de WPA-Ente	rprise v 🧿	
	WPA Versi	ion Auto	×	
	Encrypt	ion Auto	v 🦻	
Radius	5 Authentication Server Addre	255		
Ra	dius Authentication Server P	ort 1812		
	Radius Server Share Sec	ret		

When "WEP" is selected as the security mode, the window is displayed as follows:

WiFi	Access Point	Advanced	ACL	Status
∧ General Settin	gs			
	E	nable ON DEF		
		Band 2.4G	v	
	Band	width 20MHz	V	
	Ch	annel Auto	v 😨	
		SSID router999		
	Broadcast	SSID OFF		
	Security	Mode WEP	v 😨	
	WE	P Key	0	

General Settings @ Access Point				
Item	Description	Default		
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF		
Band	Choose from "2.4G" or "5G".	2.4G		
Bandwidth	Select from "20MHz", "40MHz". 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	20MHz		
Channel	<ul> <li>Select the frequency channel, including "Auto", "1", "2" "13".</li> <li>Auto: Router will scan all frequency channels until the best one is found</li> <li>1~13: Router will be fixed to work with this channel Following are the frequency of 1~13 channel. 1: 2412 MHz</li> </ul>	Auto		



General Settings @ Access Point				
Item	Description	Default		
	2: 2417 MHz			
	3: 2422 MHz			
	4: 2427 MHz			
	5: 2432 MHz			
	6: 2437 MHz			
	7: 2442 MHz			
	8: 2447 MHz			
	9: 2452 MHz			
	10: 2457 MHz			
	11: 2462 MHz			
	12: 2467 MHz			
	13: 2472 MHz			
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of	router		
	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.			
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When	ON		
	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.			
Security Mode	Select from "Disabled", "WPA-Personal" or "WEP-Enterprise".	Disabled		
	<ul> <li>Disabled: User can access the WiFi without the password when disable</li> </ul>			
	security			
	<b>Note</b> : It is strongly recommended for security purposes that you do not			
	choose this kind of mode.			
	<ul> <li>WPA-Personal: WiFi access protection, only one password can be provided</li> </ul>			
	for identity authentication.			
	WPA-Enterprise: Wi-Fi secure network protection with RADIUS service.			
	<ul> <li>WEP: Wired Equivalent Privacy provides encryption for wireless device's</li> </ul>			
	data transmission.			
WPA Version	Select from "Auto", "WPA" or "WPA2".	Auto		
WIA VEISION	<ul> <li>Auto: Router will choose automatically the most suitable WPA version</li> </ul>	Auto		
	<ul> <li>WPA2 is a stronger security feature than WPA</li> </ul>			
Encryption	Select from "Auto", "TKIP" or "AES".	Auto		
Encryption	<ul> <li>Auto: Router will choose automatically the most suitable encryption</li> </ul>	Auto		
	<ul> <li>TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless</li> </ul>			
	connection. TKIP encryption can be used for WPA-PSK and WPA with			
	802.1x authentication.			
	<b>Note</b> : It's not recommended to use TKIP encryption in 802.11n mode.			
	<ul> <li>AES: AES encryption uses a wireless connection. AES can be used for</li> </ul>			
	WPA-PSK and WPA with 802.1x authentication. AES is a stronger			
	encryption algorithm than TKIP			
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null		
Radius	Address used by the RADIUS server.	Null		

Γ



General Settings @ Access Point				
Item	Description	Default		
Authentication				
server address				
Radius				
Authentication	Port used by the RADIUS server.	1812		
server port				
Radius	A trusted connection is established between the RADIUS client and the RADIUS			
Authentication	server, and the exchange of authentication messages is guaranteed by the	Null		
server shared key	shared key.			

WiFi	Access Point	Advanced	ACL	Status
Advanced Set	ttings			
	Max Associated St	ations 64		
	Beacon In	terval 100	0	
	DTIM	Period 2	0	
	RTS Three	eshold 2347	7	
	Fragmentation Thre	eshold 2346	0	
	Transmi	t Rate Auto	×	
	Enable	WMM ON DEF	)	
	Enable Sh	ort GI ON OFF	) 🔊	
	Enable AP Iso	lation OFF	1	
	Debug	Level verbose	v	

Advanced Settings @Advanced				
Item	Description	Default		
Maximum number of access points	Set the maximum number of clients allowed to access the device AP. (A value of 0 means no limit)	64		
Signal interval	Sets the signal interval for the device AP to broadcast Beacon messages, which is used to declare the existence of a wireless network.	100		
DTIM cycle	Set the Delivery Traffic Indication Message period, that is, the period for delivering transmission instruction information. DTIM is used in the power saving mode. Device APs will multicast traffic based on this interval.	2		
RTS / CTS threshold	Set the Request To Send threshold, that is, the request to send threshold. When the threshold is set to 2347, the device AP does not send detection signals before sending data; when the threshold is set to 0, the device AP must send detection signals before sending data.	2347		
Fragmentation threshold	Set the packet threshold for WiFi AP packets. The recommended default is 2346.	2346		



Advanced Settings @Advanced				
Item	Description	Default		
Transmission rate	Data transfer rates can be automated or specified by default. Select from "Auto", "1Mbps", "2Mbps", "5.5Mbps", "6Mbps", "11Mbps", "12Mbps",	Auto		
	"18Mbps", "24Mbps", "36Mbps", "48Mbps", or "54Mbps".	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. It is			
the blank period between two symbols and provides buffer time for		ON		
	signal delay. Using a short guard interval can increase the data rate by			
	11%, but can also lead to higher packet error rates.			
Enable AP	Click the switch button to enable/disable the AP isolation option. When			
isolation	enabled, isolate all connected wireless devices, which cannot be	OFF		
	accessed directly through the WLAN.			
Commissioning	Select debug level. Select from "verbose," "debug," "info," "notice,"			
level	"warning," or "none."	none		

WiFi	Acces	s Point	ACL	Status	
∧ Genera	Settings				
		Enable /		OFF	
		ACL M	de Acce	pt 🔽 🦻	
^ Access	Control List				
Index	Description	MAC Address			+

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

ACL	
Access Control List	
Index	1
Description	
MAC Address	

ACL			
Item Description		Default	
	General Settings		
Enable ACL	Click the toggle button to enable ACL (Access Control List) option.	OFF	
ACL Mode	<ul> <li>Select from "Accept" or "Deny".</li> <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> <li>Note: Router can only allow or deny devices which are included in "Access Control List" at one time.</li> </ul>	Accept	



ACL				
Item	Description	Default		
	Access Control List			
Index	Indicate the ordinal of the list.			
Description	Enter a description for this access control list.	Null		
MAC Address	Add a MAC address here.	Null		

#### This section allows you to view the status of AP.

WiFi	Acces	s Point	Advar	nced	ACL	Status
AP Stat	tus					
		S	tatus	COMPLETED	)	
			SSID	router999		
		MAC Ad	dress	88:DA:1A:2	2A:65:9C	
^ Associa	ated Stations					
Index	MAC Address	IPv4 Address	IPv	ō Address	Name	Connected Time

Note: The WiFi function is turned off by default on the router. If you need to use it, please turn on WiFi according to the following steps and configure the router as a WiFi client.

## WiFi Client

### **Configure Router as WiFi client**

Click Interface > WiFi > WiFi, select "Client" as the mode and click "Submit > Save & Apply".

WiFi				
∧ General Setting	5			
	Mode	Client	v 😨	
	Region	SE	0	

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

	WiFi
Status	∧ General Settings
Interface	Mode Client V 🖓
Link Manager	Region SE
LAN	
Ethernet	
Cellular	
WiFi 🔦	
WLAN	

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



#### parameters of WLAN.

∧ WLAN Settings	
SSID	router
Connect to Hidden SSID	ON 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.

**Ø** robustel

Status	
∧ WLAN Status	
IPv4 Status	Connected
IPv6 Status	Connected
Uptime	0 days, 02:01:19
IPv4 Address	192.168.0.87/255.255.255.0
IPv4 Gateway	192.168.0.1
IPv4 DNS	192.168.0.1
IPv6 Address	2821:da8:202:10:8ada:1aff:fe2a:659c/64
IPv6 Gateway	fe80::36fa:40ff:fe18:68a8
IPv6 DNS	fe80::36fa:40ff:fe18:68a8
MAC Address	88:da:1a:2a:65:9c
∧ Link Status	
Signal	-9 dBm
TX Bitrate	65.0 MBit/s MCS 7
тх	15352 bytes (193 packets)
RX	40436 bytes (371 packets)
∧ WPA Status	
WPA State	COMPLETED
Frequency	2472
BSSID	88:da:1a:2a:65:7c
SSID	router888
Mode	station
Key Management	NONE
Pairwise Cipher	
Group Cipher	
∧ Scan Results	
Index SSID MAC Address	♥
1 router888 88:DA:1A:2A:65	:7C 2472 -37 dBm

This window allows you to scan for all the available SSIDs in your area and click one of those shown on the "Scan Results" list.

A Scan Resu	ilts				🕝
Index	SSID	MAC Address	Frequency	Signal	

Index	SSID	MAC Address	Frequency	Signal
1	Robustel-312-1	04:92:26:C7:3F:A8	2412	-63 dBm
2	Robustel-311	34:FA:40:07:D5:A2	2437	-67 dBm
3	mt7603e	34:FA:40:04:83:CA	2412	-73 dBm
4	AndroidAP	10:D0:7A:C4:54:EB	2437	-70 dBm
5	ChinaNet-Qg7u	CC:90:E8:1B:34:23	2467	-78 dBm
6	\x00\x00\x00\x00\x00\x	.\x00\x00\x00\x00		\X00\X00
7	ChinaNet-2.4G-F411	EC:8C:9A:B9:89:24	2462	-87 dBm
8	TP-LINK_041101	74:05:A5:51:29:A0	2437	-82 dBm
9	ChinaNet-TVYP	F0:92:B4:92:5C:69	2437	-78 dBm
10	ChinaNet-5605	C8:50:E9:E3:65:AE	2462	-85 dBm
11	HP-Print-00-LaserJet Pro	94:53:30:5A:51:E5	2437	-80 dBm
12	ChinaNet-6dfh	5C:09:79:4F:9F:F8	2457	-86 dBm
13	huxin	A8:0C:63:17:0A:F4	2412	-88 dBm
14	xiaofan	D8:C7:71:17:19:5C	2437	-86 dBm
15	router2g1	34:FA:40:07:CB:9B	2472	-46 dBm

# 3.11 Interface > USB

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

USB	Кеу	<u> </u>	
∧ General Sett	ings		
		Enable USB	ON OFF
Ena	ble Automatic Firmw	are Updating	ON OFF
USB	Кеу		
∧ Key			
	USB Automatic Upgrade Key		Generate

General Settings @ USB				
Item	Description	Default		
Enable USB	Click the toggle button to enable/disable the USB option.	ON		
Enable Automatic	Click the toggle button to enable/disable this option. Enable to automatically	ON		
Firmware Updating	update the firmware of the router when inserting a USB storage device with a			
	router firmware.			
	Кеу			
USB Automatic Update	Click Generate to generate a key.			
Кеу	It is used to verify the key file in the U disk. If it is consistent, it can be upgrade			
	d.			

10 robustel

# 3.12 Interface > DI/DO

This section allows you to set the DI/DO parameters. Digital Input and Digital Output are the specific interfaces for R3000. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

## DI

DI		DO		Status	
^ DI Set	tings				
Index	Enable	Mode	Inversion		
1	false	ON-OFF	false		6
2	false	ON-OFF	false		l.

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

DI	
∧ General Settings	
Index	1
Enable	ON OFF
Mode	ON-OFF v
Inversion	ON OFF
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off
	Submit Close

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

DI	
∧ General Settings	
Index	1.
Enable	OMOFF
Mode	Counter
Inversion	ON OFF
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off
	Submit Close

**General Settings** @ DI



Item	Description	Default		
Index	Indicate the ordinal of the list.			
Enable	Click the toggle button to enable/disable this DI.			
Mode	Select from "ON-OFF" or "Counter".			
	• ON-OFF: DI interface support ON and OFF mode (high or low level electrical)			
	trigger DI alarm. The mode default to ON, and OFF mode is available only			
	when enabling the inversion feature			
	ON—Under this mode, DI alarm status will be triggered to ON when DI			
	interface open from GND or input a high level electrical (logic 1), on the			
	contrary DI alarm status will be trigged to OFF when DI interface connect to			
	GND or input a low level electrical (logic 0)			
	OFF—Under this mode, DI alarm status will be triggered to ON when DI			
	interface connect to GND or input a low level electrical (logic 0), on the			
	contrary DI alarm status will be trigged to OFF when DI interface open from			
	GND or input a high level electrical (logic 1)			
	Counter: Event counter mode			
Inversion	Click the toggle button to enable/disable this option. Enable to set DI mode as OFF	OFF		
	mode.			
Threshold Value	Set the threshold vale. It will trigger alarm when event counter reaches this figure.	Null		
	After triggering alarm, DI will keep counting but not trigger alarm again. Enter 0 to			
	65535 digits. (0=will not trigger alarm)			
	<b>Note</b> : This option is only available when DI under the "Counter" mode.			
Alarm On Content	When the alarm is on, show its content.	Alarm		
		On		
Alarm Off	When the alarm is off, show its content.			
Content				

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

## DO

DI		DO	Status			
∧ DO Settings						
Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source	
1	false	High	Low	Last	DI1 Alarm	
2	false	High	Low	Last	DI1 Alarm	

Click 🗹 to enter the DO configuration window.



DO	
∧ General Settings	
Index	1
Enable	OFF
Alarm On Action	High
Alarm Off Action	Low
Initial State	Last
Delay	0 7
Hold Time	0 0
Alarm Source	DI1 Alarm v

## The window is displayed as below when choosing "Pulse" as the alarm on action.

DO	
∧ General Settings	
Index	1
Enable	OFF
Alarm On Action	Pulse
Alarm Off Action	Low
Initial State	Last
Delay	0 7
Hold Time	0 0
Low-level Width	10 🧿
High-level Width	10 7
Alarm Source	DI1 Alarm



### The window is displayed as below when choosing "Pulse" as the alarm off action.

DO	
∧ General Settings	
Index	1
Enable	OFF
Alarm On Action	High
Alarm Off Action	Pulse
Initial State	Last
Delay	0 ⑦
Hold Time	0 ⑦
Low-level Width	10 🧿
High-level Width	10 🧿
Alarm Source	DI1 Alarm v

DO		
Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from "High", "Low" or "Pulse".	High
	High: a high electrical level output	
	Low: a low electrical level output	
	• Pulse: Generates a square wave as specified in the pulse mode parameters when	
	triggered	
Alarm Off	Digital Output initiates when alarm removed. Selected from "High", "Low" or "Pulse".	Low
Action	High: a high electrical level output	
	Low: a low electrical level output	
	• Pulse: Generates a square wave as specified in the pulse mode parameters when	
	triggered	
Initial State	Specify the Digital Output status when powered on. Selected from "Last", "High" or "Low".	Low
	Last: DO's status will consist with the status of last power off	
	High: DO interface is in high electrical level	
	Low: DO interface is in low electrical level	
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a	0
	"Delay". Enter from 0 to 30000ms. (0=generate pulse without delay)	
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action	0
	time reach this specified time, DO will stop the action. Enter from 0 to 255 seconds.	
	(0=keep on until the next action)	
Low-level Width	Set the low-level width. It is available when enabling Pulse as "Alarm On Action/Alarm	10
	Off Action". In Pulse Output mode, the selected digital output channel will generate a	
	square wave as specified in the pulse mode parameters. The low level widths are	



DO		
Item	Description	Default
	specified here. Enter from 1 to 30000 ms.	
High-level	Set the high-level width. It is available when enabling Pulse as "Alarm On	10
Width	Action/Alarm Off Action". In Pulse Output mode, the selected digital output channel	
	will generate a square wave as specified in the pulse mode parameters. The high level	
	widths are specified here. Enter from 1 to 30000 ms.	
Alarm Source	Digital Output initiates according to different alarm source. Selected from "DI1 Alarm",	DI1
	"DI2 Alarm". DI1/DI2 Alarm: Digital Output triggers the related action when there is	Alarm
	alarm from Digital Input.	

### Status

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

DI		DO	Stat	us
∧ DI Stat	tus			
Index	Level	Status	Count	
1	High	Alarm off		
2	High	Alarm off		
Action	Of Clear	-		
		Cour	nter Alarm Of DI 1	Clear
		Cour	nter Alarm Of DI 2	Clear
∧ DO Sta	tus			
Index	Level	Low-level	Width High-level	Width
1	Low			
2	Low			
A DO Cor	ntrol			
			Level Of DO1	Toggl
			Level Of DO2	Toggl

# 3.13 Interface > Serial Port

This section allows you to set the serial port parameters. R3000 Router supports one COM1 and one COM2, also can be configured as either two COM1 or two COM2.

Serial P	ort	Statu	s		
^ Serial I	Port Setti	ngs			
Index	Port	Enable	Baud Rate	Application Mode	
1	COM1	false	115200	Transparent	
2	COM2	false	115200	Transparent	



Click the Month button on the most right of COM1, the pop-up window is as follows:

Serial Port	
∧ Serial Port Application Settings	
Index	1
Port	COM1 V
Enable	OT OFF
Baud Rate	115200 V
Data Bits	8 V
Stop Bits	
Parity	None
Flow Control	None
^ Data Packing	
Packing Timeout	50 🧿
Packing Length	1200
∧ Server Setting	
Application Mode	Transparent v
Protocol	TCP Client v
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Transparent
Protocol	TCP Client v
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Transparent v
Protocol	TCP Server v
Local IP	
Local Port	

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

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

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

▲ Server Setting	
Application Mode	Modbus RTU Gatewa v
Protocol	TCP Client v
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Modbus RTU Gatewa v
Protocol	TCP Server v
Local IP	
Local Port	

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

Application Mode	Modbus RTU Gatewa
Protocol	UDP
Local IP	
Local Port	
Server Address	
Server Port	

Serial Port					
Item Description Default					
Serial Port Application Settings					
Index Indicate the ordinal of the list					



	Serial Port					
Item	Description	Default				
	Serial Port Application Settings					
Index	Indicate the ordinal of the list.					
Port	Show the current serial's name, read only.					
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, OFF the serial port is not available.					
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", 1 "57600" , "115200" or "230400".					
Data Bits	Select from "7" or "8".	8				
Stop Bits	Select from "1" or "2".	1				
Parity	Select from "None", "Odd" or "Even".	None				
Flow control	Select from "None", "Software" or "Hardware".	None				
	Data Packing	.1				
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. <b>Note</b> : Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50				
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200				
	Server Settings					
Application Mode	<ul> <li>Select from "Transparent" or "Modbus RTU Gateway".</li> <li>Transparent: Router will transmit the serial data transparently</li> <li>Modbus RTU Gateway: Router will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa</li> </ul>	Transpare nt				
Protocol	<ul> <li>Select from "TCP Client", "TCP Server" and "UDP".</li> <li>TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name</li> <li>TCP Server: Router works as TCP server, listening for connection request from TCP client</li> <li>UDP: Router works as UDP client</li> <li>Robustlink: Router will automatically upload the serial data to Robustlink platform under the Robustlink protocol. Robustlink is a management platform from Robustel. This function only available when Router is connects to Robustlink</li> </ul>	TCP Client				
Server Address	Enter the address of server which will receive the data sent from router's serial port. IP address or domain name will be available.	Null				
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null				
Local IP @ Transparent	Enter router's LAN IP which will forward to the internet port of router.	Null				
Local Port @ Transparent	Enter the port of router's LAN IP.	Null				



Serial Port						
Item	Description	Default				
	Serial Port Application Settings					
Index	Indicate the ordinal of the list.					
Local IP @	Enter the local IP of under Modbus mode.	Null				
Modbus						
Local Port @	Enter the local port of under Modbus mode.	Null				
Modbus						

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

Serial P	ort	Status			
∧ Serial	Port Status	s list			
Index	Туре	ТХ	RX	Connection Status	
1	RS232	OB	OB		
2	RS485	OB	OB		

## 3.14 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 R	oute	Status				
∧ Static	Route Table					
Index	Description	Destination I	Netmask	Gateway	Interface	+
Click 🕂 t	o add static ro	oute. The maximur	m count is 20			
Static Ro	ute					
∧ Static	Route					
		I	Index 1		)	
		Descri	iption		)	
		Destin	nation		)	
		Neti	mask 🗌		)	
		Gate	eway		]	
		Inte	erface wwan	-v		
			S	tatic Route		
Item		Description	]			
Index		Indicate the	e ordinal of th	e list.		



Static Route					
Item	Description	Default			
Description	Enter a description for this route.	Null			
Destination	Enter the IP address of destination host or destination network.	Null			
Netmask/IPv6 address	Enter the Netmask of destination host or destination network.	Null			
Prefix Length					
Gateway	Define the gateway of the destination.	Null			
Interface	Choose the corresponding port of the link that you want to configure.	wwan1			

### Status

This window allows you to view the status of route.

Route	: Table				
Index	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
1	0.0.0	0.0.0	10.37.98.230	wwan	0
2	10.37.98.228	255.255.255.252	0.0.0.0	wwan	0
3	192.168.2.0	255.255.255.0	0.0.0	lan0	0
4	2408:84f3:1034:9	64	::	wwan	256
5	2521:da8:202:10::	64		lan0	256
6	fe80::	64	::	lan0	256
7	fe80::	64		eth1	256
8	fe80::	64		wwan	256
9		0	fe80::4e54:99ff:fe	wwan	1024
10	ff02::1	128		lan0	0
11	ff02::1:ff1f:0	128	::	wwan	0
12	ff00::	8	::	lan0	256
13	ff00::	8	::	eth1	256
14	ff00::	8	::	wwan	256

# 3.15 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.

Filtering	Port Mapping	Custom F	Rules	DMZ	Status
∧ General Setti	ings				
	Enable	Filtering	ON OFF		
_	Default Filteri	ng Policy	Accept	v 🦻	
Access Contr	ol Settings				
	Enable Remote SS	H Access	OFF		
	Enable Local SS	H Access	ON OF		
	Enable Remote Telne	et Access	OM OFF		
	Enable Local Telne	et Access	ON DEF		
	Enable Remote HTT	P Access	OFF		
	Enable Local HTT	P Access	ON OFF		
	Enable Remote HTTP	S Access	ON OF		
	Enable Remote Ping	Respond	ON DE	0	
	Enable DOS D	efending	ON OF		
	Enable	Console	ON OFF	7	
	Enable VPN NAT	Fraversal	OFF	7	

∧ Whitelist Rules						?	
Index	Description	n Sou	Irce Address				+
∧ Filter	ing Rules						
Index S	ource Address S	ource Port	Source MAC	Target Address	Target Port	Protocol	+

# Click + to add whitelist:

Filtering	
∧ Whitelist Rules	
Index	1
Description	
Source Address	

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

Ørobustel



Filtering	
∧ Filtering Rules	
Index	1
Description	
Source Address	
Source MAC	
Target Address	
Protocol	
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	0
Target Address	0
Target Port	0
Protocol	ТСР
Action	Drop

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



		Filtering				
Item		Description	Default			
		the Internet user can access the router remotely via Telnet.				
Enable Local Teln	et Access	Click the toggle button to enable/disable this option. When enabled,				
		the LAN user can access the router locally via Telnet.				
Enable Remote H	TTP Access	Access Click the toggle button to enable/disable this option. When enabled,				
		the Internet user can access the router remotely via HTTP.				
Enable Local HTT	P Access	Click the toggle button to enable/disable this option. When enabled,	ON			
		the LAN user can access the router locally via HTTP.				
Enable Remote H	TTPS Access	Click the toggle button to enable/disable this option. When enabled,	ON			
		the Internet user can access the router remotely via HTTPS.				
Enable Remote P	ing Respond	Click the toggle button to enable/disable this option. When enabled,	ON			
	0	the router will reply to the Ping requests from other hosts on the				
		Internet.				
Enable DOS Defe	nding	Click the toggle button to enable/disable this option. When enabled,	ON			
		the router will defend the DOS. Dos attack is an attempt to make a				
		machine or network resource unavailable to its intended users.				
Enable Console		Click the toggle button to enable/disable this option.	ON			
Enable vpn nat tr	aversal					
		enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF			
		whitelist				
Index		Indicate the ordinal of the list.				
Description		Enter a description for this whitelist.				
Source Address		Defines if access is allowed from one or a range of IP addresses which				
		are defined by Source IP Address, or every IP addresses.				
	Destation	Filtering Rules				
Item	Description		Default			
Index		e ordinal of the list.				
Description		cription for this filtering rule.	Null			
Source Address		ccess is allowed from one or a range of IP addresses which are defined	Null			
		P Address, or every IP addresses.				
Source Port		access originator and enter its source port.	Null			
Source MAC	Enter the N	IAC address of the defined source IP address.	Null			
Target Address	Defines if a	ccess is allowed to one or a range of IP addresses which are defined by	Null			
	Target IP Ad	ddress, or every IP addresses.				
Target Port	Enter the ta	arget port which the access originator wants to access.	Null			
Protocol	Select from	n "All", "TCP", "UDP", "ICMP" or "TCP-UDP".				
	Note: It is r	t is recommended that you choose "All" if you don't know which protocol of				
	your applica	ation to use.				
Action	Select from	"Accept" or "Drop".	Drop			
	Accept	: When Default Filtering Policy is drop, router will drop all the				
	connec	cting requests except the hosts which fit this accept filtering list				
	Drop: \	When Default Filtering Policy is accept, router will accept all the				
			1			



### **Port Mapping**

Filteri	ng	Port Mapping	Custom Ru	les C	MZ	Status	
∧ Port M	lapping Rule	25					
Index	Description	Internet Port	Local IP	Local Port	Protocol		+

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

Port Mapping	
∧ Port Mapping Rules	
Index	1
Description	
Remote IP	
Internet Port	0
Local IP	
Local Port	0
Protocol	TCP-UDP v

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

Custom rules, that is, rules that you define yourself. Click Network> Firewall> Custom Rule and is displayed as follows:

Filteri	ng Port Mapp	ing Custom Rules	DMZ	Status
^ Custo	m Iptables Rules			
Index	Description	Rule		+
^ Custo	m Ip6tables Rules			
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	1
Description	
Rule	

Custom Iptables Rule				
Item	Description	Default		
Index	Indicate the ordinal of the list			
Description	Enter the description of the rule. Null			
Rule	Specify one Iptables rule.	Null		

### DMZ

Filtering	Port Mapping	Custom Rules	DMZ	Status
A DMZ Settings				
	E	nable DMZ		
	Host	IP Address		
	Source 1	IP Address	7	

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



#### Status

Filteri	ng	Port Map	ping	Custom R	ules	DMZ	Status
^ Chain	Input						
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	REJECT	tcp	*	*	0.0.0/0	0.0.0/0
2	52	ACCEPT	tcp	*	*	0.0.0/0	0.0.0.0/0
3	0	DROP	tcp		**	0.0.0/0	0.0.0.0/0
4	0	ACCEPT	tcp	*	*	0.0.0/0	0.0.0/0
5	0	DROP	tcp	**	*	0.0.0/0	0.0.0/0
6	0	ACCEPT	icmp	40	36	0.0.0/0	0.0.0/0
7	0	DROP	icmp	*	*	0.0.0/0	0.0.0/0
∧ Chain	Forward						
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	30	0.0.0/0	0.0.0/0
∧ Chain	Output						
Index	Packets	Target	Protocol	In	Out	Source	Destination

# **3.16** Network > IP Passthrough

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

IP Passthrough		
∧ General Settings		
	Enable OFF	

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

## 3.17 VPN > IPsec

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

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

General	Tunnel	Status	x509	
∧ General Settir	ıgs			
		Keepalive 20		3
	Optimize DH Exp	onent Size	OFF 😨	
	De	oug Enable	OFF	

### General

General Settings @ General			
Item	Description	Default	
Survival time	Set the survival time in seconds. The router sends keep-alive packets to a		
Survivartime	NAT (Network Address Translation) server at regular intervals to prevent	20	
	the records on the NAT table from disappearing.		
	Click the toggle button to enable / disable this option. When enabled,		
Optimize DH index size	when using dhgroup17 or dhgroup18, it helps to shorten the time to	OFF	
	generate dh keys.		
Debug Enable	Click the toggle button to enable/disable this option. Enable for IPsec VPN	OFF	
	information output to the debug port.		

### Tunnel

Gener	al	Tunnel	Statu	s x5	09	
	Settings					
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+



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

Tunnel	
∧ General Settings	
Index	1
Enable	ON OFF
Description	
Gateway	0
Mode	Tunnel
Protocol	ESP
Local Subnet	0
Remote Subnet	admin
Link Binding	Unspecified V

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 repres ents for any address.	Null
Mode	<ul> <li>Select from "Tunnel" and "Transport".</li> <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	<ul> <li>Select the security protocols from "ESP" and "AH".</li> <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.



ІКЕ Туре	[IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	(SHA1	V
IKE DH Group	DHgroup2	v
Authentication Type	PSK	v
PSK Secret		
Local ID Type	Default	v
Remote ID Type	Default	v
IKE Lifetime	86400	0

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

∧ IKE Settings	
ІКЕ Туре	IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	CA v
Private Key Password	
IKE Lifetime	86400

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

∧ IKE Settings	
ІКЕ Туре	IKEv1 v
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	PKCS#12
Private Key Password	
IKE Lifetime	86400

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



IKE Settings	
ІКЕ Туре	IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES v
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK v
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	
ІКЕ Туре	IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	xAuth CA v
Private Key Password	
Username	
Password	
IKE Lifetime	86400 3

IKE Settings			
Item	Description	Default	
ІКЕ Туре	Select from IKE v1 and IKE v2.	IKE v1	
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1.	Main	
	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.		
Authentication	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in IKE	SHA1	
Algorithm	negotiation.		
Encryption Algorithm	Select from "3DES", "AES128", "AES192" and "AES256" to be used in IKE	3DES	
	negotiation.		



	IKE Settings			
Item	Description			
	3DES: Use 168-bit 3DES encryption algorithm in CBC mode			
	AES128: Use 128-bit AES encryption algorithm in CBC mode			
	AES256: Use 256-bit AES encryption algorithm in CBC mode			
IKE DH Group	Select DH packets for IKE (Network Key Exchange) negotiation. Select	DHgroup2		
	from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15",			
	"DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation			
	phase 1.			
Authentication Type	Select from "PSK", "CA", "PKCS#12", "xAuth PSK" and "xAuth CA" to be used	PSK		
	in IKE negotiation.			
	PSK: Pre-shared Key			
	CA: Certification Authority			
	xAuth: Extended Authentication to AAA server			
PSK Secret	Enter the pre-shared key.	Null		
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation.	Default		
	<ul> <li>Default: Uses an IP address as the ID in IKE negotiation</li> </ul>			
	• FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is			
	selected, type a name without any at sign (@) for the local security			
	gateway, e.g., test.robustel.com.			
	<ul> <li>User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this</li> </ul>			
	option is selected, type a name string with a sign "@" for the local			
	security gateway, e.g., test@robustel.com.			
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation.	Default		
Nemote ib Type	<ul> <li>Default: Uses an IP address as the ID in IKE negotiation</li> </ul>	Derduit		
	<ul> <li>FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is</li> </ul>			
	selected, type a name without any at sign (@) for the local security			
	gateway, e.g., test.robustel.com.			
	<ul> <li>User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this</li> </ul>			
	option is selected, type a name string with a sign "@" for the local			
	security gateway, e.g., test@robustel.com.			
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	Null		
Osernanie		Null		
Password	types. Enter the password used for the "xAuth PSK" and "xAuth CA" authentication	Null		
1 8350010				
IKE Lifetime	types.	86400		
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a	86400		
	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.			

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

#### Robustel R3000 User Guide

∧ SA Settings		
Encrypt Algorithm	3DES V	
Authentication Algorithm	MD5 v	l .
PFS Group	DHgroup2 v	j .
SA Lifetime	28800	) 🔊
DPD Interval	60	0
DPD Failures	180	) 🔊
▲ General Settings		
Index	1	
Enable	ON DIT	
Description		
Gateway		0
Mode	Tunnel v	
Protocol	ESP	
Local Subnet		0
Remote Subnet		0
Link Binding	Unspecified v	0
✓ IKE Settings		
∧ SA Settings		
Encryption Algorithm	3DES v	
Authentication Algorithm	SHA1 V	
PFS Group	DHgroup2 v	
SA Lifetime	28800	0
DPD Interval	30	0
	<u></u>	

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

Ørobustel

Ørobustel

∧ General Settings	
Index	1
Enable	ON OFF
Description	
Gateway	
Mode	Tunnel
Protocol	AH
Local Subnet	0
Remote Subnet	
Link Binding	Unspecified V 🔇
✓ IKE Settings	
∧ SA Settings	
Authentication Algorithm	SHA1 V
PFS Group	DHgroup2 v
SA Lifetime	28800
DPD Interval	30
DPD Failures	150
∧ Advanced Settings	
Enable Compression	ON OFF
Enable Forceencaps	ON OFF ?

SA Settings				
Item	Description	Default		
Encrypt Algorithm	Select from "3DES", "AES128" or "AES256" when you select "ESP" in	3DES		
	"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.			
Authentication	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA	MD5		
Algorithm	negotiation.			
PFS Group	Select from "PFS (N/A) ","DHgroup1", "DHgroup2", "DHgroup5",	DHgroup2		
	"DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18"			
	to be used in SA negotiation.			
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKE uses the	28800		
	smaller one between the lifetime set locally and the lifetime proposed by			
	the peer.			
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is	60		



SA Settings				
Item	Description	Default		
	received from the peer. DPD is a Dead peer detection. DPD irregularly			
	detects dead IKE peers. When the local end sends an IPsec packet, DPD			
	checks the time the last IPsec packet was received from the peer. If the time			
	exceeds the DPD interval, it sends a DPD hello to the peer. If the local end			
	receives no DPD acknowledgment within the DPD packet retransmission			
	interval, it retransmits the DPD hello. If the local end still receives no DPD			
	acknowledgment after having made the maximum number of			
	retransmission attempts, it considers the peer already dead, and clears the			
	IKE SA and the IPsec SAs based on the IKE SA.			
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	OFF		
	the inner headers of IP packets.			
Enable Forced	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	OFF		
Encapsulation	is forced. This may help overcome restrictive firewalls.			
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc,	Null		
	e.g. protostack=netkey;plutodebug=none			

### Status

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

General Tunnel		Status	x509		
∧ IPSec	Tunnel Statu	5			
Index	Description	Status	Uptime		

#### x509

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

General	Т	innel Sta	tus	x509	
<b>× X</b> 509 Se	ttings				(7
		Tunnel Name	Tunnel 1	×	
		Local Certificate	Choose File	No file chosen	
		Remote Certificate	Choose File	No file chosen	
		Private Key	Choose File	No file chosen	
		CA Certificate	Choose File	] No file chosen	
		PKCS#12 Certificate	Choose File	No file chosen	
Certifica	te Files				
Index	File Name	File Siz	ze	Modification Time	



x509				
Item	Description	Default		
	X509 Settings			
Tunnel Name	Choose a valid tunnel.	Tunnel 1		
Local Certificate	Click on "Choose File" to upload a local 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	Null		
Remote Certificate	Click on "Choose File" to upload a remote certificate file from your computer, and then import this file into your router.	Null		
Private Key	Select the correct private key file to import into the router.	Null		
Root certificate	Select the root certificate file to import into the router.			
PKCS # 12 certificate	Select the PKCS # 12 certificate file to import into the router.			
Certificate Files				
Index	Indicate the ordinal of the list.			
File Name	Show the imported certificate's name.	Null		
File Size	Show the size of the certificate file.	Null		
Modification Time	Show the timestamp of that the last time to modify the certificate file.	Null		

# 3.18 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.

### OpenVPN

OpenV	PN	Status		x509			
∧ Tunne	Settings						
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

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



OpenVPN	A STAR BURGER AND A
∧ General Settings	
Index	1
Enable	ON OF
Enable IPv6	OM OFF
Description	
Mode	P2P V 😨
TLS Mode	None v
Protocol	UDP
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None 🤍 🍞
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Keepalive Interval	20
Keepalive Timeout	120 🤇
TUN MTU	1500
Max Frame Size	
Enable Compression	ON DEF
Enable NAT	OFF OFF
Verbose Level	0 7



### The window is displayed as below when choosing "Client" as the mode.

▲ General Settings	
Index	1
Enable	ON OFT
Description	
Mode	Client 🤍 🧿
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	None 🤍 🍞
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400
Keepalive Interval	20 3
Keepalive Timeout	120 🧿
TUN MTU	1500
Max Frame Size	
Enable Compression	ON OFF
Enable NAT	OM OFF
Enable DNS overrid	ON OFF ⑦
Verbose Level	0 2

10 robustel

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

	-
∧ General Settings	
Index	1
Enable	ON OFF
Enable IPv6	OT OFF
Description	
Mode	Server 🗸 🦻
Protocol	UDP V
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None 🤍 🤋
Enable IP Pool	OFF
Client Subnet	10.8.0.0
Client Subnet Netmask	255.255.255.0
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400 🧿
Max Clients	10
Keepalive Interval	20 🤇
Keepalive Timeout	120 🧿
TUN MTU	1500
Max Frame Size	
Enable Compression	ON OTT
Enable Default Gateway	ON OFF
Enable NAT	
	ON OFF
Verbose Level	0 7

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



OpenVPN			
∧ General Settings			
	Index	1	
	Enable	ON DIF	
	Description		
	Mode	Client	3
	Protocol	UDP	
	Peer Address		
	Peer Port	1194	
	Interface Type	TUN	
	Authentication Type	None v	3
	Encrypt Algorithm	BF	
Auth	entication Algorithm	SHA1 v	
Re	negotiation Interval	86400	3
	Keepalive Interval	20	3
	Keepalive Timeout	120	3
	TUN MTU	1500	
	Max Frame Size		
	Enable Compression	ON OTT	
	Enable NAT	OFF	
	Enable DNS overrid	OFF ?	
	Verbose Level	0	3

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



OpenVPN	
∧ General Settings	
Index	1
Enable	ON OFF
Description	
Mode	Client v 🧿
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	Preshared v 🤊
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Enable Compression	ON DEE
Enable NAT	OFF
Enable DNS overrid	OFF ?
Verbose Level	0 2

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



∧ General Settings	
Inde	x 1
Enabl	e on off
Descriptio	n
Mod	le Client 🤍 🤊
Protoco	DI UDP
Peer Addres	55
Peer Po	rt 1194
Interface Typ	e TUN V
Authentication Typ	e Password 🔽 😨
Usernam	e
Passwor	b
Encrypt Algorith	m BF
Authentication Algorith	m SHA1
Renegotiation Interva	al 86400 🧿
Keepalive Interva	al 20
Keepalive Timeou	it 120
TUN MT	U [1500
Max Frame Siz	e
Enable Compressio	n ON OFF
Enable NA	
Enable DNS overri	
Verbose Leve	
CIDOSC LEV	



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

∧ General Settings	
Index	1
Enable	ON DEE
Description	
Mode	Client V
Protocol	UDP V
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA 🗸 🤇
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400 🧿
Keepalive Interval	20 🧿
Keepalive Timeout	120 🧿
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON OF
Enable NAT	OFF OFF
Enable DNS overrid	OFF ?
Verbose Level	0 7



The suite descript disclosure de a hele	WINDOW ADDRESS WYFOOCA	Password" as the authentication type
i në window is dishlaved as heid	W When choosing XSU9LA	Passworn as the authentication type
The will dow is displayed as belo		assure as the authentication type

∧ General Settings	
Index	1
Enable	ON OFF
Description	
Mode	Client 🤍 🍞
Protocol	UDP
Peer Address	
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA Password V
Username	
Password	
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400
Keepalive Interval	20 🧿
Keepalive Timeout	120 🧿
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON OT
Enable NAT	ON OFF
Enable DNS overrid	OFF 😨
Verbose Level	0 2

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

∧ Advanced Settings	
Enable HMAC Firewall	OH OFF
Enable PKCS#12	OM OFF
Enable nsCertType	OM OFF
Expert Options	0

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



Advanced Settings	
Enable HMAC Firewall	OFF OFF
Enable Crl	OFF OFF
Enable Client To Client	Off OFF
Enable Dup Client	Off OFF
Enable IP Persist	ON OFF ?
Expert Options	

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

OpenV	PN	Status		x509			
∧ Tunne	Settings						
Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type	+
^ Passw	ord Mana	ge					
Index	Usern	ame					+
∧ Client	Manage						]
Index	Enable	Common Nar	ne Clier	nt IP Address			+

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

OpenVPN	
∧ General Settings	
Index	1
Username	
Password	

Click Client Management 🛨 to add Client information, as shown

No. 2000 (2000) (2000)	
∧ General Settings	
Index	1
Enable	ON DEF
Common Name	0
Client IP Address	

General Settings @ OpenVPN			
Item Description Default			
Index	Indicate the ordinal of the list.		

be



General Settings @ OpenVPN		
Item	Description	Default
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable IPv6	Click the toggle button to enable/disable this OpenVPN tunnel to use ipv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from "P2P", "Client" or "Server".	Client
TLS Mode	Select from "None", "Client" or "Server".	None
Protocol	Select from "UDP", "TCP-Client" or "TCP-Server".	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
Listening address	Local server address.	Null
Listening port	Local server port.	1194
Interface Type	Select from "TUN", "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". <b>Note</b> : "None" and "Preshared" authentication type are only working with P2P mode.	None
Enable IP Address pool	Click the toggle button to enable / disable the IP address pool allocation function.	OFF
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for "Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and	BF
	<ul><li>"AES256".</li><li>BF: Use 128-bit BF encryption algorithm in CBC mode</li></ul>	
	<ul> <li>DES: Use 64-bit DES encryption algorithm in CBC mode</li> <li>DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode</li> </ul>	
	<ul> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> </ul>	



General Settings @ OpenVPN			
Item	Default		
	AES256: Use 256-bit AES encryption algorithm in CBC mode		
Renegotiation Set the renegotiation interval. If connection failed, OpenVPN with		86400	
Interval	renegotiate when the renegotiation interval reached.		
Maximum number of	Set the maximum number of clients allowed to access the OpenVPN	10	
clients	server.	10	
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20	
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass	120	
	without reception of a ping or other packet from remote.		
MTU	Set the maximum transmission unit.	1500	
Data Sharding	Set the maximum frame length.	Null	
Private Key Password	Enter the private key password under the "X509CA" and "X509CA	Null	
	Password" authentication type.		
Enable Compression	Click the toggle button to enable/disable this option. Enable to	ON	
	compress the data stream of the header.		
Enable Default	Standalone switch button to enable / disable the default gateway		
	function. After enabling, push the local tunnel address as the default	OFF	
Gateway	gateway of the peer device.		
Enable NAT	Click the toggle button to enable/disable the NAT option. When	OFF	
	enabled, the source IP address of host behind router will be disguised		
before accessing the remote OpenVPN client.			
	Standalone switch button to enable / disable receiving DNS push		
Receive DNS Push	function. After it is enabled, it is allowed to receive DNS information	OFF	
	pushed by the peer.		
Verbose Level	Select the level of the output log and values from 0 to 11.	0	
	O: No output except fatal errors		
	• 1~4: Normal usage range		
	• 5: Output R and W characters to the console for each packet read		
	and write		
	• 6~11: Debug info range		
	Advanced Settings @ OpenVPN		
Enable HMAC	Click the toggle button to enable/disable this option. Add an additional	OFF	
Firewall	layer of HMAC authentication on top of the TLS control channel to		
	protect against DoS attacks.		
Enable PKCS#12 Click the toggle button to enable/disable the PKCS#12 certificate. It is a		OFF	
exchange of digital certificate encryption standard, used to describe			
	personal identity information.		
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that peer	OFF	
certificate was signed with an explicit nsCertType designation of			
	"server".		
Enable Crl	Click the toggle button to enable / disable the option. When enabled,	OFF	
	client certificates can be revoked.		
Enable client to client	Click the toggle button to enable / disable the option. When enabled,	OFF	
	clients can communicate with each other.		



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

### Status

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

OpenV	PN	Status	x50	9		
∧ Open\	PN Tunnel St	atus				
Index	Description	Status	Mode	Uptime	Local IP	Local IPv6
∧ Open\	PN Client Lis	t				
Index	Common	Name	Real IP	Port	Virtual IP	Virtual IPv6

### x509

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

OpenVPN	Status x50	9	
∧ X509 Settings			0
	Tunnel Name	Tunnel 1	
	Mode	Client	
	Root CA	Choose File No file chosen	
	Certificate File	Choose File No file chosen	
	Private Key	Choose File No file chosen	
	TLS-Auth Key	Choose File No file chosen	
	PKCS#12 Certificate	Choose File No file chosen	

File Size

Index File Name

Modification Time

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

## 3.19 VPN > GRE

This section allows you to set the GRE and the related parameters. Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.

### GRE

GRE		Status	
∧ Tunne	Settings		
Index	Enable	Description Remote IP Address	+

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

10 robustel



GRE	
∧ Tunnel Settings	
Index	1
Enable	ON OFF
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask/Prefix Length	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	OFF
Secrets	
Link Binding	Unspecified 🤍

Tunnel Settings @ GRE		
Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP	Set the remote virtual IP Address of the GRE tunnel.	Null
Address/ IPv6 prefix		
length		
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all	OFF
	the traffics of the router will go through the GRE VPN.	
Enable NAT	Click the toggle button to enable/disable this option. This option must be	Disable
	enabled when router under NAT environment.	
Secrets	Set the key of the GRE tunnel.	Null
Link Dinding	Salact from "WAVAAANI1" "WAVAANI2" "WAVAANI" or "WAVAANI"	Not
Link Binding	Select from "WWAN1", "WWAN2", "WAN", or "WLAN".	bound

#### Status

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

GRE		Status			
∧ GRE tu	innel status				
Index	Description	Status	Local IP Address Remote IP Address	Uptime	

### 3.20 Services > Syslog

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

Syslog	
∧ Syslog Settings	
E	nable ON DEF
Syslog	Level Debug v
Save Po	sition RAM V
Log to Re	mote OFF

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

Syslog	
∧ Syslog Settings	
Enab	IE ON OFF
Syslog Lev	el Debug v
Save Positio	n RAM V 🤊
Log to Remot	e on off ?
Add Identifie	er Off OFF 7
Remote IP Addres	
Remote Po	rt 514

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

#### 3.21 Services > Event

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

Event	Notifica	tion Qu	ery				
∧ General	Settings						
	Signa	l Quality Threshold	0	0			
			General Sett	ings @ Event			
Item		Description					Default
Signal Qua	lity Threshold			uality. Router will ger	•		0
		the actual thresh this option.	hold is less th	an the specified thre	shold. U means di	sable	
Event	Notifica	tion Que	ery				
∧ Event No	otification Group	Settings					
Index [	Description Send S	MS Send Email	DO Control	Save to NVM	+		

#### Click + button to add an Event parameters.

Notification	
∧ General Settings	
Index	1
Description	
Send SMS	OMOFF
Send Email	OMOFF
DO Control	ON OFF
Save to NVM	OFF ?



∧ Event Selection	()
System Startup	OFF
System Reboot	OFF OFF
System Time Update	OW OFF
Configuration Change	ON OFF
Cellular Network Type Change	OH OFF
Cellular Data Stats Clear	COM OFF
Cellular Data Traffic Overflow	OFF
Poor Signal Quality	ON OFF
Link Switching	OFF OFF
WAN Up	OFF
WAN Down	Off OFF
WLAN Up	OFF
WLAN Down	OFF
WWAN Up	OFF
WWAN Down	OFF OFF
IPSec Connection Up	ON OFF
IPSec Connection Down	OH OFF
OpenVPN Connection Up	OFF
OpenVPN Connection Down	OFF
LAN Port Link Up	OFF
LAN Port Link Down	OFF
USB Device Connect	OFF
USB Device Remove	OFF
DDNS Update Success	ON OFF
DDNS Update Fail	OFF
Received SMS	OFF
SMS Command Execute	OFF
DI 1 ON	ON OFF
DI 1 OFF	OFF
DI 1 Counter Overflow	OFF
DI 2 ON	ON OFF
DI 2 OFF	ON OFF
DI 2 Counter Overflow	OFF OFF



	General Settings @ Notification		
Item	Description	Default	
Index	Indicate the ordinal of the list.		
Description	Enter a description for this group.	Null	
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will	OFF	
	send notification to the specified phone numbers via SMS if event occurs. Set the		
	related phone number in "3.24 Services > Email", and use ';'to separate each		
	number.		
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will	OFF	
	send notification to the specified email box via Email if event occurs. Set the related		
	email address in "3.24 Services > Email".		
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the		
DO CONTRO	event router will send it to the corresponding DO in the form of Low / High level.	OFF	
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to	OFF	
	nonvolatile memory.		

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

Event	Notification Query
∧ Event Detai	ls
▲ Event Detai Sep 11 19:00:53, Sep 11 19:00:55, Sep 11 19:00:55, Sep 11 19:00:55, Sep 11 19:01:06, Sep 11 19:01:16, Sep 11 19:47:25, Sep 11 19:47:25, Sep 11 19:47:26, Sep 11 19:47:26, Sep 11 19:47:26, Sep 11 19:47:24, Sep 11 19:47:41, Sep 11 19:47:42, Sep 11 19:47:44, Sep 11 19:48:50, Sep 11 19:48:51, Sep 11 19:48:51, Sep 11 19:48:51, Sep 11 19:48:51, Sep 11 19:48:52, Sep 11 19:48:52, Sep 11 19:48:54, Sep 11 19:49:04, Sep 11 19:49:05,	Is Save Position RAM ♥ Filtering system startup LAN port link down, eth0 LAN port link down, eth0 LAN port link up, eth1 WWAN (cellular) up, WWAN1, ip=10.189.43.25 system time update configuration change, link_manager restored to default after firmware updating configuration change, link_manager restored to default after firmware updating configuration change, link_manager restored to default after firmware updating configuration change, via web manager configuration change, via web manager WTAN (cellular) down, WTAN1 WTAN (cellular) down, WTAN1 WTAN (cellular) up, WWAN1, ip=10.189.43.25 configuration change, via web manager WTAN (cellular) down, WTAN1 WTAN (cellular) down, WTAN1
Sep 11 19:59:34, Sep 11 19:59:36, Sep 11 19:59:38, Sep 11 20:29:00,	configuration change, link_manager restored to default after firmware updating configuration change, via web manager
	Clear Refresh



	Event Details		
Item	Description	Default	
Save Position	Select the events' save position from "RAM" or "NVM".	RAM	
	RAM: Random-access memory		
	NVM: Non-Volatile Memory		
Filter Message	Event will be filtered according to the Filter Message that the user set. Click	Null	
	<b>Refresh</b> , the filtered event will be displayed in the follow box. Use "&" to		
	separate more than one filter message, such as message1&message2.		

### 3.22 Services > NTP

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

NTP	Status	
∧ Timezone Sett	ings	
	Time Zone	UTC+08:00 V
	Expert Setting	0
NTP Client Set	tings	
	Enable	ON OFF
	Primary NTP Server	pool.ntp.org
	Secondary NTP Server	
	NTP Update Interval	0 7
∧ NTP Server Se	ttings	
	Enable	OFF

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



NTP Server Settings				
Enable	Click the toggle button to enable the NTP server option.	OFF		

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

NTP	Status		
∧ Time			
	System Time	2019-12-31 10:48:42	
	PC Time	2019-12-31 10:48:44 <b>Sync</b>	]
	Last Update Time	2019-12-31 09:52:08	

### 3.23 Services > SMS

This section allows you to set SMS parameters. Router supports SMS management, and user can control and configure their routers by sending SMS. For more details about SMS control, refer to **4.2.2 SMS Remote Control**.

SMS	SMS Testing			
∧ SMS Manage	SMS Management Settings			
	Enable	ON OFF		
	Authentication Type	Password v		
Phone Number		0		

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

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

SMS	SMS Testing		
∧ SMS Testing			
Phone Number Message			
Message			
Result			
			Send

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

#### 3.24 Services > Email

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

Email	
∧ Email Settings	
Enable	OFF
Enable TLS/SSL	OFF ?
Enable STARTTLS	OFF
Outgoing Server	
Server Port	25
Timeout	10 🦻
Auth Login	OFF ?
Username	
Password	
From	
Subject	



Item	Description		
Enable	Click the toggle button to enable/disable the Email option.		
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF	
Enable STARTTLS	Click the toggle button to enable / disable STARTTLS encryption.	OFF	
Outgoing server	Enter the SMTP server IP Address or domain name.	Null	
Server port	Enter the SMTP server port.	25	
Timeout	Set the max time for sending email to SMTP server. When the server doesn't	10	
	receive the email over this time, it will try to resend.		
	If the mail server supports AUTH login, you must enable this button and set a	055	
Auth Login	username and password.	OFF	
Username	Enter the username which has been registered from SMTP server.	Null	
Password	Enter the password of the username above.	Null	
From	Enter the source address of the email.	Null	
Subject	Enter the subject of this email.	Null	

### 3.25 Services > DDNS

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

DDNS	Status	
DDNS Settings		
	Enable	OH OFF
	Service Provider	DynDNS
	Hostname	
	Username	
	Password	

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

A DDNS Settings		
	Enable	ON OFF
	Service Provider	Custom
	URL	

DDNS Settings			
Item	Description	Default	
Enable	Click the toggle button to enable/disable the DDNS option.	OFF	



Service Provider	Select the DDNS service from "DynDNS", "NO-IP" or "3322".	
	Note: the DDNS service only can be used after registered by	DynDNS
	Corresponding service provider.	
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click "Status" bar to view the status of the DDNS.

DDNS	Status	
∧ DDNS Status		
	Status	Disabled
	Last Update Time	

DDNS Status		
Item Description		
Status Display the current status of the DDNS.		
Last Update TimeDisplay the date and time for the DDNS was last updated successfully.		

### 3.26 Services > SSH

Router su	oports SSH	password	access a	nd secret-ke	v access.
nouter sup	pp0103 3311	puss	access a	na secret ke	y access.

SSH	Keys Management		
∧ SSH Settings			
		Enable	ON OFF
		Port	22
	Disable Passwo	ord Logins	OFF

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



SSH	Keys Management		
∧ Import Au	thorized Keys		
	Authorized Keys	Choose File No file chosen	Import

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

### 3.27 Services > GPS

This section allows you to set the GPS setting parameters.

GPS	Status	Мар	
∧ Genera	Settings		
	I	Enable GPS 0	PFF
	Syn	c GPS Time ON O	DFF
^ RS232	Report Settings		
	Repor	t to RS232 0	DFF
	Report GG/	Sentence o	DFF
	Report VTC	Sentence 0	DEE
	Report RMC	Sentence ON O	PFF
	Report GSV	Sentence on o	DFF
∧ GPS Sei	rvers		
Index E	nable Protocol Loc	al Address Local	Port Server Address Server Port 🕂

General Settings @ GPS				
Item	tem Description Default			
Enable GPS	Click the toggle button to enable/disable the GPS option. OFF			
Sync GPS Time	Click the toggle button to synchronize GPS time.	OFF		
	RS232 Report Settings			
Report to RS232	Click the toggle button to report to RS232.	OFF		
Report GGA	Click the taggle button to report CCA contance	OFF		
Sentence	Click the toggle button to report GGA sentence. OFF			
Report VTG	Click the toggle button to report VIC contence	OFF		
Sentence	Click the toggle button to report VTG sentence. OFF			
Report RMC	Click the taggle button to report DMC contenes			
Sentence	Click the toggle button to report RMC sentence. OFF			
Report GSV	Click the taggle button to report CCV contance			
Sentence	Click the toggle button to report GSV sentence.	OFF		



#### The window is displayed as below when choosing "TCP Client" as the protocol.

GPS	
∧ Server Settings	
Index	1
Enable	ON OFF
Protocol	TCP Client v
Server Address	
Server Port	
Send GGA Sentence	OFF
Send VTG Sentence	OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

The window is displayed as below when choosing "TCP Server" as the protocol.

GPS	
∧ Server Settings	
Index	1
Enable	ON OFF
Protocol	TCP Server v
Local Address	
Local Port	
Send GGA Sentence	OH OFF
Send VTG Sentence	ON OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

The window is displayed as below when choosing "UDP" as the protocol.



GPS	
∧ Server Settings	
Index	1
Enable	ON OFF
Protocol	UDP
Server Address	
Server Port	
Send GGA Sentence	OFF
Send VTG Sentence	OFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF

Server Settings			
Item	Description	Default	
Index	Indicate the ordinal of the list.		
Enable	Click the toggle button to enable/disable the GPS server	ON	
	settings.		
Protocol	Select from "TCP Client", "TCP Server" or "UDP".	TCP Client	
Server Address	Set the address of the TCP Client.	Null	
@TCP Client			
Server Port	Set the port of the remote TCP Server.	Null	
@TCP Client			
Local Address	Set the local address when the router set as a TCP Server.	Null	
Local Port	Set the local port when the router set as a TCP Server.	Null	
Server Address @ UDP	Set the address of the TCP Server.	Null	
Server Port @ UDP	Set the port of the remote TCP Server.	Null	
Send GGA Sentence	Send GGA information in NMEA format.	OFF	
Send VTG Sentence	Send VTG information in NMEA format.	OFF	
Send RMC Sentence	Send RMC information in NMEA format.	OFF	
Send GSV Sentence	Send GSV information in NMEA format.	OFF	

Click the "Status" column to view the status of the GPS.

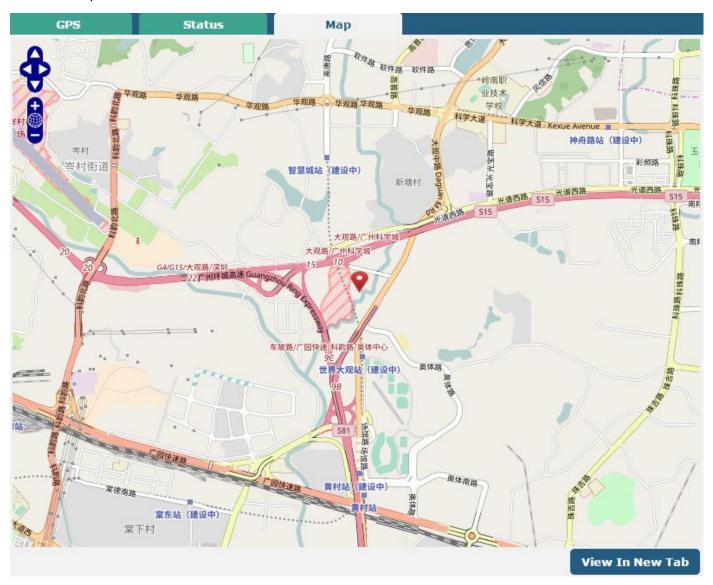


GPS	Status	Мар	
∧ GPS Status			
		Status	
		UTC Time	
	Las	st Fixed Time	
	Sat	ellites In Use	
	Sate	llites In View	
		Latitude	
		Longitude	
		Altitude	
		Speed	

	GPS Status		
Item Description			
Status	Show the GPS Status. GPS status includes: "NO Fix", "2D Fix" and "3D Fix".		
UTC Time	Show the UTC of satellites, which is world unified time, not local time.		
Last Fixed Time	Show the last positioning time.		
Satellites In Use	Show the satellite quantity in use.		
Satellite In View	View Show the satellite quantity in view.		
Latitude	Show the latitude status of router.		
Longitude	Show the longitude status of router.		
Altitude	Show the altitude status of router.		
Speed	Show the horizontal speed of router.		



Click the "Map" column to view the current location of the router.



#### 3.28 Services > Web Server

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

Web Server	Certificate Management			
∧ General Sett	ings			
	HTTP Port	80	7	
	HTTPS Port	443	0	

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



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

#### This section allows you to import the certificate file into the route.

Web Server	Certificate Management	
∧ Import Certi	ficate	
	Import Type	CA
	HTTPS Certificate	Choose File No file chosen Import

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

### 3.29 Services > Advanced

This section allows you to set the Advanced and parameters.

System	Reboot			
∧ System Setting	js			
	Device Name	router	7	
	User LED Type	None	v	
System Setting	js			
	Device Name	router	0	
	User LED Type	None	v 😨	
		None OpenVPN IPSec		
		WiFi		



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

System	Reboot		
∧ Periodic Rebo	ot Settings		
	Periodic Reboot	0	
	Daily Reboot Time	0	

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

## 3.30 System > Debug

Syslog Details					
	Log Level	Debug	v		
	Filtering		0		
Sep 11 21:00:58 router user. debug rpin Sep 11 21:00:58 router user. debug lind Sep 11 21:00:58 router user. debug lind Sep 11 21:00:58 router user. debug lind Sep 11 21:05:58 router user. debug rpin Sep 11 21:05:59 router user. debug lind Sep 11 21:05:59 router user. debug lind	<pre>k_manager[3986]: 1 k_manager[3986]: 4 k_manager[3986]: W k_manager[3986]: W ng [4718]: start p: ng [4718]: Start p: ng [4718]: 24 bytes ng [4718]: 24 bytes ng [4718]: 8.8. ng [4718]: 1 packet ng [4718]: round-t1 k_manager[3986]: 4 k_manager[3986]: 4</pre>	ecv action ping arget link WWAN AN1 ping test s WAN1 (wwan) sta ng 8.8.8 (wwa .8.8 (8.8.8.8) sfrom 8.8.8.8: from 8.8.8.8: s transmitted, ip min/avg/max arget link WWAN	<pre>success from rp: [1, state Connects success art ping test m) from 10.18.11.133 seq=0 ttl=51 time stics</pre>	ng ed == 16 data bytes == 139.263 ms ed, 0% packet lo: =/139.263 ms ng	55
		Manual R	Refresh v	Clear R	efresh

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

^ Syslog	Files			
Index	File Name	File Size	Modification Time	
1	messages	77945	Wed Sep 11 21:05:59 2019	
∧ System	Diagnostic Data			
	System I	Diagnostic Data Ger	erate	

	Syslog				
Item	Description	Default			
Syslog Details					
Log Level	Select from "Debug", "Info", "Notice", "Warn", "Error" which from low to high.	Debug			
	The lower level will output more syslog in detail.				
Filtering	Enter the filtering message based on the keywords. Use "&" to separate more	Null			
	than one filter message, such as "keyword1&keyword2".				
Refresh	Select from "Manual Refresh", "5 Seconds", "10 Seconds", "20 Seconds" or "30	Manual			
	Seconds". You can select these intervals to refresh the log information displayed	Refresh			
	in the follow box. If selecting "manual refresh", you should click the refresh				
	button to refresh the syslog.				
Clear	Click the button to clear the syslog.				
Refresh	Click the button to refresh the syslog.				
	Syslog Files				
Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message0	/			
	to message 4. And the newest syslog file will be placed on the top of the list.				
	System Diagnosing Data				
Generate	Click to generate the syslog diagnosing file.	/			



Download

Click to download the generated system diagnostic data.

### 3.31 System > Update

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

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

Update			
∧ System Update			
	File	Choose File No file chosen	Update

Update				
Item	Description	Default		
System Update	Click Choose File button to select the correct firmware in your PC, and then	Null		
	click Update button to update. After updating successfully, you need to click			
	"save and apply", and then reboot the router to take effect.			

### **3.32** System > App Center

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

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

App Center	
For more information	bout App, please refer to http://www.robustel.com/products/app-center/.
App Install	
	File Choose File No file chosen Install

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

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

App Center				
Item	Description			
	App Install			
File	Click on "Choose File" to locate the App file from your computer, and then click			
	Install to import this file into your router.			
	Note: File format should be xxx.rpk, e.g. R3000-robustlink-1.0.0.rpk.			
	Installed Apps			
Index	Indicate the ordinal of the list.			
Name	Show the name of the App.	Null		
Version	Show the version of the App.	Null		
Status	Show the status of the App.	Null		
Description	Show the description for this App.	Null		

### 3.33 System > Tools

Ping	Traceroute Sr	iffer
∧ Ping		
	IP Address	
	Number of Reques	5
	Timeou	1
	Local II	
		Start Stop

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

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

Ping	Traceroute Snif	ier en
▲ Traceroute		
	Trace Address Trace Hops Trace Timeout	
		Start Stop

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

Pir	ng Tracerout	sniff	er		
∧ Sniff	er				
		Interface Host Packets Request Protocol Status	all 1000 All O	v v Start	Stop
^ Capte	ure Files				
Index	File Name	File Siz	e	Modification Time	i i i i i i i i i i i i i i i i i i i
1	19-09-11_21-18-43.cap	52420		Wed Sep 11 21:18:54 2019	<b>D</b> X

10 robustel



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

### 3.34 System > Profile

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

Profile	Rollback	
∧ Import Cor	ifiguration File	
	Reset Other Settings to Default	OFF 7
	Ignore Invalid Settings	OFF ?
	XML Configuration File	Choose File No file chosen Import
∧ Export Con	figuration File	
	Ignore Disabled Features	OFF 7
	Add Detailed Information	OFF 0
	Encrypt Secret Data	ON 🦳 🖗
	XML Configuration File	Generate
∧ Default Co	nfiguration	
Sav	ve Running Configuration as Default	Save 🕝
	Restore to Default Configuration	Restore

Profile			
Item Description			
Import Configuration File			
Reset Other Settings to	Click the toggle button as "ON" to return other parameters to default	OFF	
Default	settings.		
Ignore Invalid Settings	Click the toggle button as "OFF" to ignore invalid settings.	OFF	
XML Configuration File	Click on Choose File to locate the XML configuration file from your		



	computer, and then click Import to import this file into your router.	
	Export Configuration File	
Ignore Disabled Features	Click the toggle button as "OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as "On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as "ON" to encrypt the secret data.	OFF
XML Configuration File	Click Generate button to generate the XML configuration file.	
	Default Configuration	
Save Running	Save	
Configuration as Default	Click Save the current running parameters as default	
	configuration.	
Restore to Default	Click Restore to restore the factory defaults.	
Configuration		

Profile	Rollback				
^ Configu	∧ Configuration Rollback				
	Save as a Rollba	ckable Archive Save	• 7		
∧ Configu	ration Archive Files				
Index	File Name	File Size	Modification Time		

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

### 3.35 System > User Management

One router has only one super user who has the highest authority to modify, add and manage other common users.

Root	Super User Commo	n User		
∧ Super User Se	ttings			?
	New Username	admin	0	
	Old Password	•••••	0	
	New Password		7	
	Confirm Password			

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

Root		Super User	Common User	
∧ Commo	n User Se	ttings		
Index	Role	Username		+

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

Common User	
∧ Common Users Settings	
Index	1
Role	Visitor
Username	
Password	0

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

0-9, @, ., -, #, \$, and \*.

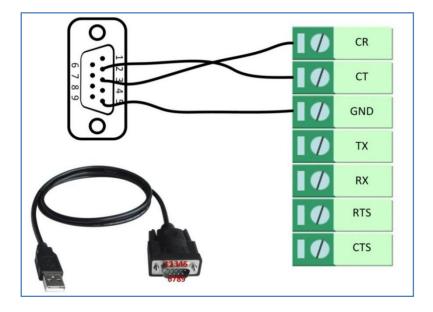


# **Chapter 4** Configuration Examples

### 4.1 Interface

### 4.1.1 Console Port

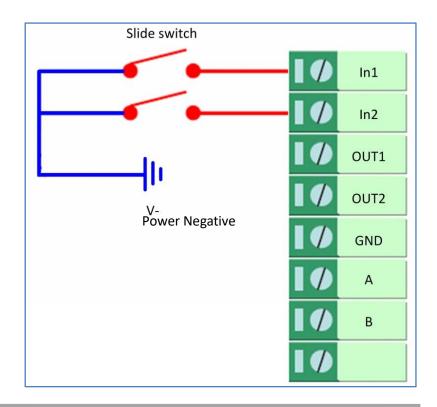
You can use the console port to manage the router via CLI commands, please refer to **Chapter 5 Introductions for CLI**.



### 4.1.2 Digital Input

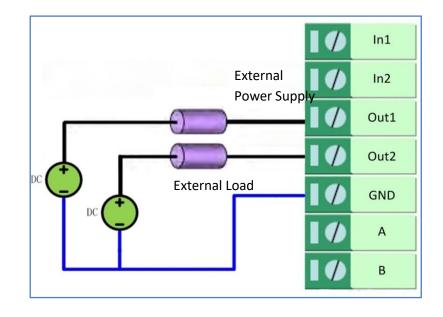
R3000 supports digital input with dry contact. Please check the connector interface of the router, you can easily find a mark "V-" at one pin of the power connector.

**Note:** Do not connect In1/In2 directly and do not slide the switch to the port marked "GND" on the terminal block. Otherwise, the DI cannot work properly.



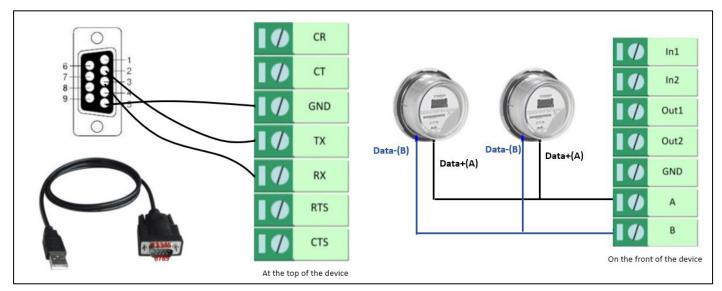
### 4.1.3 Digital Output

R3000 supports digital output with wet contact. Please refer to the right side figure to connect the negative pole of the power to the port marked "GND". The maximum output voltage, output current and output power of DO is 30V DC, 0.3 A and 0.3 W respectively. It means that the voltage difference between Out1, Out2 and GND cannot exceed to 30V DC; and the current value through Out1 and Out2 cannot exceed to 300 mA; while the output power dissipated by Out1 and Out2 cannot exceed to 0.3W. Otherwise, the DO will be damaged.



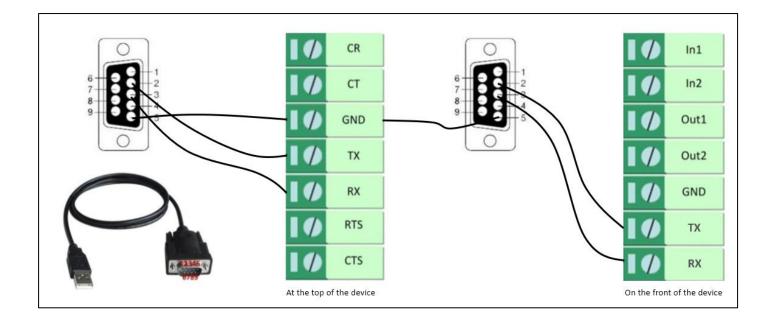
### 4.1.4 1\*RS-232+1\*RS-485

R3000 supports 1\*RS-232+1\*RS-485 for serial port data communication. Please refer to the connection diagram shown below.

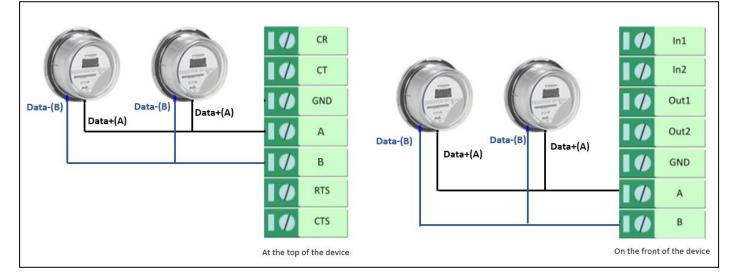


### 4.1.5 2\*RS-232

R3000 supports 2\*RS-232 for serial port data communication. Please refer to the connection diagram shown below.



#### 4.1.6 2\*RS-485



R3000 supports 2\*RS-485 for serial port data communication. Please refer to the connection diagram shown below.

### 4.2 Cellular

### 4.2.1 Cellular Dial-Up

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

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

Link Mar	nager	Status					
∧ Gener	al Setting	S					
			Primary Link	WWA	11	v 😨	
			Backup Link	WWA	12	v	
			Backup Mode	Cold E	Jackup	v 😨	
			Revert Interval	0		0	
		Em	ergency Reboot	ION .	OFF 😨		
∧ Link S	ettings						
Index	Туре	Description	IPv4 Connectio	n Type	IPv6 Conne	ection Type	
1	WWAN1	admin	DHCP		SLA	AAC	
2	WWAN2		DHCP		SLA	AAC	
3	WAN		DHCP		SLA	AAC	
4	WLAN		DHCP		SLA	AAC	

#### Click the Z of rightest of WWAN1 to set its parameters according to the current ISP.

Link Manager	
∧ General Settings	
Index	1
Туре	WWAN1 Y
Description	admin
IPv6 Enable	ON DEF



A WWAN Settings				
Automatic APN Selection	ON OFF			
Dialup Number	*99***1#			
Authentication Type	Auto			
PPP Preferred	OFF 7			
Switch SIM By Data Allowance	OFF 🕜			
Data Allowance	0 7			
Billing Day	1			

∧ IPv6 LAN Setting	S	
	Connection Type	Static v
	IPv6 Prefix	2521:da8:202:10::/64
	IPv6 NAT Enable	ON THE

▲ Ping Detection Settings		7
Enable	ON OFF	
IPV4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114	
IPv6 Primary Server	2001:4860:4860::888	
IPv6 Secondary Server	2400:da00:2::29	
Interval	300	0
Retry Interval	5	0
Timeout	3	0
Max Ping Tries	3	0
∧ Advanced Settings		
IPv4 NAT Enable	ON OTT	
Upload Bandwidth	10000	3
Download Bandwidth	10000	
Overrided Primary DNS		
Overrided Secondary DNS		
Overrided IPv6 Primary DNS		
Overrided IPv6 Secondary DNS		
Debug Enable	ON DEF	
Verbose Debug Enable	OFF	

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

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



Cellul	lar	Status	AT Debug		
^ Advan	ced Cellula	ar Settings			
Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	
2	SIM2		Auto	All	

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

Cellular	
∧ General Settings	
Index	1
SIM Card	SIM1 V
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0 7
∧ Cellular Network Settings	
Network Type	Auto 🤍 🧭
Band Select Type	All 🗸 🧭
∧ Advanced Settings	
Debug Enable	ON OFF
Verbose Debug Enable	ON OFF

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

### 4.2.2 SMS Remote Control

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

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

- 1. Password mode—Username: Password;cmd1;cmd2;cmd3; ...cmdn (available for every phone number).
- 2. Phonenum mode—**Password;cmd1; cmd2; cmd3; ... cmdn** (available when the SMS was sent from the phone number which had been added in R3000's phone group).
- 3. Both mode-- **Username: Password;cmd1;cmd2;cmd3; ...cmdn** (available when the SMS was sent from the phone number which had been added in R3000's phone group).

#### SMS command Explanation:

- 1. User name and Password: use the same username and password as WEB manager for authentication.
- 2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command, more details about CLI cmd please refer to **Chapter 5 Introductions for CLI**.

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

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

Profile	Rollback	
∧ Import Conf	iguration File	
	Reset Other Settings to Default	OFF 7
	Ignore Invalid Settings	OFF 7
	XML Configuration File	Choose File No file chosen Import
∧ Export Confi	guration File	
	Ignore Disabled Features	OM OFF 7
	Add Detailed Information	он огг 🕜
	Encrypt Secret Data	OFF ?
	XML Configuration File	Generate
∧ Default Conf	iguration	
Save	Running Configuration as Default	Save 🕝
	Restore to Default Configuration	Restore

#### XML command:

```
<lan>
<network max_entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

#### SMS cmd:

set lan network 1 interface lan0 set lan network 1 ip 172.16.24.24 set lan network 1 netmask 255.255.0.0 set lan network 1 mtu 1500

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

#### admin:admin;status system

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

#### SMS received:

hardware\_version = 1.2



firmware\_version = "3.0.0" kernel\_version = 4.1.0 device\_model = R3000 serial\_number = 201612221052 uptime = "0 days, 00:40:21" system\_time = "Mon Feb 27 09:52:52 2017" **admin:admin;reboot** In this command, username is "admin", password is "admin", and the command is to reboot the Router. **SMS received:** OK

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

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

#### SMS received:

ОК

ОК

# admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

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

#### SMS received:

OK

ОК

ОК

ОК

# 4.3 Network

#### 4.3.1 IPsec VPN





The configuration of server and client is as follows.

IPsec VPN\_Server:

Cisco 2811:



Router>enable Router#config Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/Z. Router(config)#crypto isakmp policy 10 Router(config-isakmp)#? authentication Set authentication method for protection suite Set encryption algorithm for protection suite encryption exit Exit from ISAKMP protection suite configuration mode Set the Diffie-Hellman group group hash Set hash algorithm for protection suite lifetime Set lifetime for ISAKMP security association Negate a command or set its defaults no Router(config-isakmp) #encryption 3des Router(config-isakmp) #hash md5 Router(config-isakmp) #authentication pre-share Router(config-isakmp)#group 2 Router(config-isakmp) #exit Router(config) #crypto isakmp ? client Set client configuration policy enable Enable ISAKMP Set pre-shared key for remote peer kev policy Set policy for an ISAKMP protection suite Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0 Router(config) #crypto ? dynamic-map Specify a dynamic crypto map template ipsec Configure IPSEC policy Configure ISAKMP policy isakmp key Long term key operations map Enter a crypto map Router (config) #crypto ipsec ? security-association Security association parameters transform-set Define transform and settings Router(config) #crypto ipsec transform-set Trans ? ah-md5-hmac AH-HMAC-MD5 transform ah-sha-hmac AH-HMAC-SHA transform ESP transform using 3DES(EDE) cipher (168 bits) esp-3des ESP transform using AES cipher esp-aes esp-des ESP transform using DES cipher (56 bits) esp-md5-hmac ESP transform using HMAC-MD5 auth esp-sha-hmac ESP transform using HMAC-SHA auth Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac Router(config) #ip access-list extended vpn Router(config-ext-nacl) #permit ip 10.0.0.0.0.0.255 192.168.1.0 0.0.0.255 Router (config-ext-nacl) #exit Router(config) #crypto map cry-map 10 ipsec-isakmp % NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured. Router(config-crypto-map) #match address vpn Router(config-crypto-map) #set transform-set Trans Router(config-crypto-map)#set peer 202.100.1.1 Router(config-crypto-map) #exit Router(config) #interface fastEthernet 0/0

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

#### **IPsec VPN\_Client:**

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



General Tunnel		Tunnel	Statu	09		
∧ Tunne	l Settings					
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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

Tunnel		
∧ General Settings		
Index	1	]
Enable	ON DEE	
Description		)
Gateway		) 🔊
Mode	Tunnel	
Protocol	ESP	
Local Subnet		) 🔊
Remote Subnet		) 🔊
Link Binding	Unspecified v	0
∧ IKE Settings		
ІКЕ Туре	IKEv1 v	
Negotiation Mode	Main	
Encryption Algorithm	3DES V	
Authentication Algorithm	SHA1 V	
IKE DH Group	DHgroup2 v	
Authentication Type	PSK v	
PSK Secret	•••••	)
Local ID Type	Default	
Remote ID Type	Default	l in the second s
IKE Lifetime	86400	] 🤊
∧ SA Settings		
Encryption Algorithm	3DES V	
Authentication Algorithm	SHA1 v	
PFS Group	DHgroup2 v	
SA Lifetime	28800	) 🔊
DPD Interval	30	) 🔊
DPD Failures	150	) 🔊



∧ Advanced Settings	
Enable Compression	OFF OFF
Enable Forceencaps	GIN OFF 😨
Expert Options	

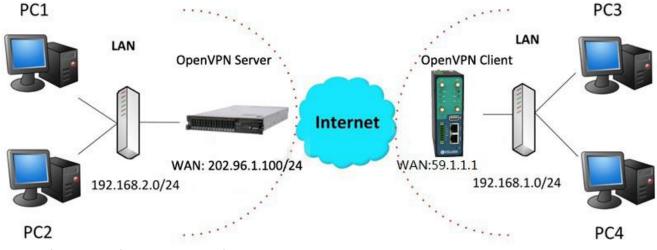
#### When finished, click **Submit > Save & Apply** for the configuration to take effect.

The comparison between server and client is as below.

Router>epable		
Routestconfig Server (Cisco 2811)	A General Settings	
Configuring from terminal, memory, or network [terminal]? Enter configuration commands, one per line. End with CNTL/E.	Index	1
Router(config)forypto isakmp policy 10 Router(config-isakmp)#?	Enable	ON
suthentication Set suthentication method for protection suite encryption Set encryption algorithm for protection suite	Description	
exit Exit from ISANNE protection suite configuration mode group Set the Diffie-Bellman group		
hash Set hash algorithm for protection suite	Gateway	58.1.1.1
no Nepate a compand or set its defaults	Mode	Tunnel
Router(config-laskmp)#encryption 3des Router(config-laskmp)fhash md5	Protocol	ESP v
Bouter(config-isakmp)fauthentication pre-share Bouter(config-isakmp)#group 2	Local Subnet	192.168.1.0/24
Router (config-isakup) fexit	Remote Subnet	0.0.0.0/24
Router(config)fcrypto isskmp ? client Set client configuration policy	Link Binding	
enable Enable ISAMMP key Set pre-shared key for remote peer		
policy Set policy for an ISANNP protection suite Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0	A IKE Settings	
	IKE Type	IKEV1
Routericonfigiforypto ? dynamic-map Specify a dynamic crypto map template Router IK	E Settings should Negotiation Mode	Main
	tent with service Encryption Algorithm	ades v
key Long term key operations	Authentication Algorithm	MD5
Router(config)#crypto ipsec ?	IKE DH Group	DHgroup2
security association Security association parameters transform-set Define transform and settings	Authentication Type	PSK
Router(config)#crypto ipsec transform-set Trans ? ah-md5-bmac AN-MMAC-MD5 transform	PSK Secret	[
ah-sha-hmac AR-SHAC-SHA transform esp-3des ESP transform using SDES(EDE) cipher (168 bits)		
esp-aes ESP transform using AES cipher	Local ID Type	Default
esp-des ESP transform using DES cipher (5% bits) esp-md5-hmac ESP transform using HMAC-HD5 auth	Remote ID Type	Default
Router(config)forypto ipsec transform-set Trans esp-2des esp-md5-hmac	IKE Lifetime	86400
	∧ SA Settings	
Router(config) #ip access-list extended vpn Router(config-ext-macl) #permit ip 10.0.0.0.0.0.0.255 192.168.1.0 0.0.0.255	Encryption Algorithm	3065
Router(config-ext-macl)#exit	Authentication Algorithm	MD5
	r SA Settings	DHgroup2
<ul> <li>NOTE: This new crypto map will remain disabled until a peer and a valid access list have been configured.</li> </ul>	the consistent with	
Router (config-orypto-map) fmatch address vpn Router (config-orypto-map) fest transform set Trans Router (config-orypto-map) fest transform set Trans	SA Lifetime	28800
Router(config-orypto-map)fset peer 202.100.1.1 Service Router(config-crypto-map)fexit	e rees. DPD Interval	30 30
source county cribes substance.	DPD Failures	150 3
Router(config)#interface fastSthermet 0/0	Advanced Settings	
Router(config-if)fip address 58.1.1.1 255.255.255.0 Bouter(config-if)for	Enable Compression	OFF
Router(config-if)#crypto map cry-map	Enable Forceencaps	
*Jan 3 07:16:26.705: VCRYPTO-6-ISARMP_ON_OFF: ISARMP is ON	Expert Options	
	Expert Options	U U

## 4.3.2 OpenVPN

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



The configuration of two points is as follows.

### **OpenVPN\_Server:**

Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server: local 202.96.1.100 mode server port 1194 proto udp dev tun tun-mtu 1500 fragment 1500 ca ca.crt cert Server01.crt key Server01.key dh dh1024.pem server 10.8.0.0 255.255.255.0 ifconfig-pool-persist ipp.txt push "route 192.168.3.0 255.255.255.0" client-config-dir ccd route 192.168.1.0 255.255.255.0 keepalive 10 120 cipher BF-CBC comp-lzo max-clients 100 persist-key persist-tun status openvpn-status.log

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

#### **OpenVPN\_Client:**

Click VPN > OpenVPN > OpenVPN as below.

OpenV	PN	Status		x509			
∧ Tunne	l Settings						
Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	+

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

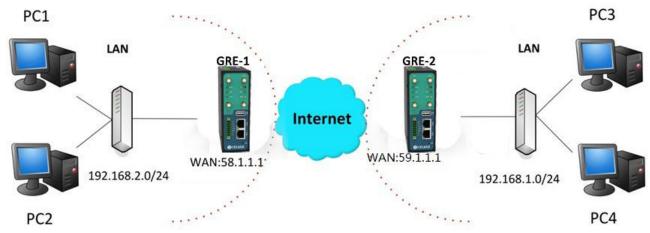
OpenVPN	n n. i. i. n.
∧ General Settings	
Index	1
Enable	ON DET
Description	client01
Mode	Client v
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA V
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interval	86400
Keepalive Interval	20 🦻
Keepalive Timeout	120 🥱
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	ON DEF
Enable NAT	OFF
Enable DNS overrid	OFF ?
Verbose Level	3 7





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

## 4.3.3 GRE VPN



The configuration of two points is as follows.

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



#### GRE-1:

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



∧ Tunnel Settings	
Index	1
Enable	ON DEF
Description	
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	•••••
Link Binding	Unspecified 🤍 🍞

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

GRE	
∧ Tunnel Settings	
Index	1
Enable	ON OFF
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0
Remote Virtual IP Address	10.8.0.1
Enable Default Route	ON OFF
Enable NAT	OR OFF
Secrets	•••••
Link Binding	Unspecified v

#### GRE-2:

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

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

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

#### Robustel R3000 User Guide



GRE			GRE			į
∧ Tunnel Settings	a		<ul> <li>Tunnel Settings</li> </ul>		100	
Index	1			Index	1	
Enable	ON			Enable	ON CON	GRE-2 real public
Description	GRE-1	GRE-1 real public net	work IP address	Description	GRE-2	network IP address
Remote IP Address	58.1.1.1	GRE-1 real tunnrl IP ac	dress Ren	note IP Address	59.1.1.1	
Local Virtual IP Address	10.8.0.1	GRE-2 real tunnrl IP ad	dress Local Vir	tual IP Address	10.8.0.2	GRE-2 real tunnrl
Local Virtual Netmask/Prefix Length	255.255.255.0	0	Local Virtual Netmasi	c/Prefix Length	255.255.255.0	
Remote Virtual IP Address	10.8.0.2		Remote Vir	tual IP Address	10.8.0.1	GRE-1 real tunnrl
Enable Default Route	OFF		Enable	e Default Route	OFF	IP address
Enable NAT	OFF			Enable NAT	OFF	USE the same
Secrets		USE the same passwo	rd for GRE-1 and GRE-2	Secrets	•••••	password for
Link Binding	Unspecified	0		Link Binding	Unspecified	GRE-1 and GRE-2

# **Chapter 5** Introductions for CLI

# 5.1 What Is CLI

The R3000 command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the <u>SSH</u> or through a <u>telnet</u> network connection.

File Edit View	r Tools Tab Window Help / 辰・ 〇	• • • 0 '
☐ telnet://192.1		
G To add the cu	rrent session, click on the left arrow button.	
1 New Session	× +	
outer login: ad	min	1
Password:	011)	
1	Comments	
add	Add a list entry of configuration	
clear	Clear statistics	
config	Configuration operation	
debug	Output debug information to the console	
del	Delete a list entry of configuration	
do	Set the level state of the do	
exit	Exit from the CLI	
help	Display an overview of the CLI syntax	
	Download OpenVPN certificate file via http or ftp	
ping	Send messages to network hosts	
reboot	Halt and perform a cold restart	
set	Set system configuration	E
show	Show system configuration	
status	Show running system information	
tftpupdate traceroute	Update firmware or configuration file using tftp	
urlupdate	Print the route packets trace to network host Update firmware via http or ftp	
ver	Show version of firmware	
ver		
П		
		-
Send text to th	e current tab only	. =
all send text to th	e current tab only	· -

#### Route login:

Router login: admin

Password: admin

#

#### CLI commands:

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

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



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

# 5.2 How to Configure the CLI

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

Commands /tips	Description	
? Typing a question mark "?" will show you the help information.		
	eg.	
	# config (Press '?')	
	config Configuration operation	
	# config (Press spacebar +'?')	
	commit Save the configuration changes and take effect	
	changed configuration	
	save_and_apply Save the configuration changes and take effect	
	changed configuration	
	loaddefault Restore Factory Configuration	
Ctrl+c	Press these two keys at the same time, except its "copy" function but also	
	can be used for "break" out of the setting program.	
Syntax error: The command is not	Command is not completed.	
completed		
Tick space key+ Tab key	It can help you finish you command.	
	Example:	
	# config (tick Enter key)	
	Syntax error: The command is not completed	
	# config (tick space key+ Tab key)	
	commit save_and_apply loaddefault	
#config commit	When your setting finished, you should enter those commands to make	
<pre># config save_and_apply</pre>	your setting take effect on the device.	
	Note: Commit and save_and_apply plays the same role.	
1		

# 5.3 Commands Reference

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

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

## 5.4 Quick Start with Configuration Examples

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

#### **Example 1: Show current version**

# status system hardware\_version = 1.2 firmware\_version = "3.0.0" kernel\_version = 4.1.0 device\_model = R3000 serial\_number = 201612221052 uptime = "0 days, 00:40:21" system\_time = "Mon Feb 27 09:52:52 2017"

### Example 2: Update firmware via tftp

# tftpupdate (space+?) firmware New firmware
# tftpupdate firmware (space+?)
String Firmware name
# tftpupdate firmware filename R3000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new
firmware name
Downloading
R3000-firmware-s 100%   **********************************
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success //update success
# config save_and_apply
OK // save and apply current configuration, make you configuration effect

#### Example 3: Set link-manager

# set	
# set	
at_over_telnet	AT Over Telnet
cellular	Cellular
ddns	Dynamic DNS
ethernet	Ethernet
event	Event Management

Robustel R3000 User Guide



Firewall	
GRE	
IPsec	
Local Area Network	
Link Manager	
NTP	
OpenVPN	
Automatic Reboot	
RobustLink	
Route	
SMS	
SNMP agent	
SSH	
Syslog	
System	
User Management	
VRRP	
Web Server	
Primary Link	
Backup Link	
Backup Mode	
Emergency Reboot	
Link Settings	
nary_link (space+?)	
wan1/wwan2/wan)	
nary_link wwan1	<pre>//select "wwan1" as primary_link</pre>
	//setting succeed
1	
Туре	
-	
-	
Overrided Secondary DNS	
1 type wwan1	
1 type wwan1	
1 type wwan1 1 wwan	
1 type wwan1 1 wwan Automatic APN Selection	
1 type wwan1 1 wwan	
ſ	GRE IPsec Local Area Network Link Manager NTP OpenVPN Automatic Reboot RobustLink Route SMS SNMP agent SSH Syslog System User Management VRP Web Server Primary Link Backup Mode Emergency Reboot Link Settings hary_link (space+?) wan1/wwan2/wan) hary_link wwan1 1 Type Description Connection Type WWAN Settings Static Address Settings PIPOE Settings PIPOE Settings PING Settings MTU Overrided Primary DNS



dialup\_number Dialup Number auth\_type Authentication Type aggressive\_reset **Aggressive Reset** switch\_by\_data\_allowance Switch SIM By Data Allowance data\_allowance Data Allowance billing\_day Billing Day # set link\_manager link 1 wwan switch\_by\_data\_allowance true OK # # set link\_manager link 1 wwan data\_allowance 100 //open cellular switch\_by\_data\_traffic ОК //setting succeed # set link manager link 1 wwan billing day 1 //setting specifies the day of month for billing OK //setting succeed ... # config save\_and\_apply OK // save and apply current configuration, make you configuration effect

#### **Example 4: Set Ethernet**

# set Ethernet port\_setting 2 port\_assignmEnt lan0
OK
# config save\_and\_apply
OK

//Set Table 2 (eth1) to lan0

//setting succeed

#### Example 5: Set LAN IP address

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



```
lease_time = 120
         expert_options = ""
         debug_enable = false
    }
}
multi_ip {
    id = 1
    interface = lan0
    ip = 172.16.24.24
     netmask = 255.255.0.0
}
#
# set lan
  network
                 Network Settings
  multi_ip
                 Multiple IP Address Settings
  vlan
                 VLAN
# set lan network 1(space+?)
  interface
                 Interface
                 IP Address
  ip
  netmask
                 Netmask
  mtu
                 MTU
                 DHCP Settings
  dhcp
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24
                                                  //set IP address for lan
                                                  //setting succeed
OK
# set lan network 1 netmask 255.255.0.0
OK
#
•••
# config save_and_apply
                                         // save and apply current configuration, make you configuration effect
ОК
```

## **Example 6: CLI for setting Cellular**

```
# show cellular all
sim {
    id = 1
    card = sim1
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
```



band\_gsm\_1900 = false band\_wcdma\_850 = false band\_wcdma\_900 = false band\_wcdma\_1900 = false band\_wcdma\_2100 = false band\_lte\_800 = false band\_lte\_850 = false band Ite 900 = false band\_lte\_1800 = false band\_lte\_1900 = false band\_lte\_2100 = false band\_lte\_2600 = false band\_lte\_1700 = false band\_lte\_700 = false band\_tdd\_lte\_2600 = false band\_tdd\_lte\_1900 = false band\_tdd\_lte\_2300 = false band\_tdd\_lte\_2500 = false sim { id = 2 card = sim2 phone\_number = "" extra\_at\_cmd = "" network\_type = auto band\_select\_type = all band\_gsm\_850 = false band\_gsm\_900 = false band gsm 1800 = false band\_gsm\_1900 = false band\_wcdma\_850 = false band\_wcdma\_900 = false band wcdma 1900 = false band\_wcdma\_2100 = false band\_lte\_800 = false band\_lte\_850 = false band\_lte\_900 = false band Ite 1800 = false band\_lte\_1900 = false band\_lte\_2100 = false band\_lte\_2600 = false band\_lte\_1700 = false band\_lte\_700 = false band\_tdd\_lte\_2600 = false band tdd Ite 1900 = false band\_tdd\_lte\_2300 = false

}



band_tdd_lt	:e_2500 = fa	lse		
}				
<pre># set(space+?)</pre>				
at_over_telnet	cellular	ddns	dhcp	dns
event	firewall	ipsec	lan	link_manager
ntp	openvpn	reboot	route	serial_port
sms	snmp	syslog	system	user_management
vrrp				
# set cellular(spa	ce+?)			
sim SIM Sett	ings			
# set cellular sim	(space+?)			
Integer Inde>	k (12)			
# set cellular sim	1(space+?)			
card	SI	M Card		
phone_numbe	er Ph	none Number		
extra_at_cmd	Ex	tra AT Cmd		
network_type	Ne	etwork Type		
band_select_ty	ype Ba	and Select Type		
band_gsm_850	0 GS	SM 850		
band_gsm_900	0 GS	5M 900		
band_gsm_180	00 GS	SM 1800		
band_gsm_190	00 GS	SM 1900		
band_wcdma_	850 W	CDMA 850		
band_wcdma_	900 W	CDMA 900		
band_wcdma_	1900 W	CDMA 1900		
band_wcdma_	2100 W	CDMA 2100		
band_lte_800	LT	E 800 (band 20)		
band_lte_850		E 850 (band 5)		
band_lte_900		E 900 (band 8)		
band_lte_1800		FE 1800 (band 3)		
band_lte_1900		E 1900 (band 2)		
band_lte_2100		E 2100 (band 1)		
band_lte_2600		E 2600 (band 7)		
band_lte_1700		E 1700 (band 4)		
band_lte_700		E 700 (band 17)		
band_tdd_lte_		DD LTE 2600 (band 38)		
band_tdd_lte_	-	DD LTE 1900 (band 39)		
band_tdd_lte_	-	DD LTE 2300 (band 40)		
band_tdd_lte_	-	DD LTE 2500 (band 41)		
	1 phone_nu	mber 18620435279		
ОК				
 # config cover one	ا میں ا			
# config save_and	apply	11	- +	onfiguration make you configuration official
ОК		// save and a	apply current c	onfiguration, make you configuration effect





# Glossary

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



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



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

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