



User Guide

R2000 Ent

Industrial Dual Module Cellular VPN Router with Voice
5 Eth + 1 Voice/RS-232/RS-485 + 1 USB Host



robustOS

Guangzhou Robustel LTD
www.robustel.com


About This Document

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

Copyright©2019 Guangzhou Robustel LTD.

All rights reserved.

Trademarks and Permissions

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

Disclaimer

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

Technical Support

Tel: +86-20-29019902

Fax: +86-20-82321505

Email: support@robustel.com

Web: www.robustel.com

Important Notice

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

Safety Precautions

General

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

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

Using the Router in Vehicle

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

Protecting Your Router

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

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

Regulatory and Type Approval Information

Table 1: Directives



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

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


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

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

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	o	o	o	o	o	o
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o
<p>o: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.</p> <p>X: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part <i>might exceed</i> the limit requirement in RoHS2.0.</p>										

Document History

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

Date	Firmware Version	Doc Version	Change Description
19 Apr.,2017	3.0.0	v.1.0.0	Initial release
21 Aug.,2017	3.0.0	v.1.0.1	<ul style="list-style-type: none"> • Noted that only SIM1 support voice function • Added more information about RJ11 connector • Corrected weight from 750 g to 695 g • Updated LED Indicators table in Chapter 2.1 • Added certifications information • Added avg power information • Other minor editorial changes
28 Jun.,2018	3.0.0	v.1.0.2	Revised the company name
30 Jan., 2019	3.0.0	v.1.0.3	Revised the certifications Revised the Frequency bands of Wifi
26 Mar., 2019	3.0.0	v.1.0.4	<ul style="list-style-type: none"> • Revised the English grammar • Added the description of Supporting GSM and VoLTE(optional) for voice traffic • Revised the Regulatory and Type Approval Information
17 Sep., 2019	3.0.0	v.1.0.5	<ul style="list-style-type: none"> • Revised the Regulatory and Type Approval Information • Revised the Approvals

Contents

Chapter 1	Product Overview	10
1.1	Key Features	10
1.2	Package Contents	11
1.3	Specifications	13
1.4	Dimensions.....	16
1.5	Ordering Information	16
Chapter 2	Hardware Installation.....	17
2.1	LED Indicators.....	17
2.2	RJ11 Interface.....	19
2.3	USB Interface.....	20
2.4	Reset Button.....	20
2.5	Ethernet Port.....	21
2.6	Insert or Remove SIM Card	21
2.7	Attach External Antenna (SMA Type).....	22
2.8	Mount the Router	23
2.9	Ground the Router	24
2.10	Connect the Router to a Computer.....	25
2.11	Power Supply.....	25
Chapter 3	Initial Configuration	26
3.1	Configure the PC.....	26
3.2	Factory Default Settings	29
3.3	Log in the Router	29
3.4	Control Panel	30
3.5	Status.....	31
3.6	Interface > Link Manager	33
3.7	Interface > LAN.....	44
3.8	Interface > Ethernet	49
3.9	Interface > Cellular	50
3.10	Interface > WiFi	54
3.11	Interface > USB.....	62
3.12	Interface > Serial Port (Optional)	63
3.13	Network > Route	67
3.14	Network > Firewall	68
3.15	Network > IP Passthrough	72
3.16	VPN > IPsec.....	72
3.17	VPN > OpenVPN	79
3.18	VPN > GRE	87
3.19	Services > Syslog.....	88
3.20	Services > Event.....	89
3.21	Services > NTP	92
3.22	Services > SMS.....	94
3.23	Services > Email.....	95
3.24	Services > DDNS	96

3.25	Services > SSH.....	97
3.26	Services > Telephone (Optional).....	98
3.27	Services > Web Server	99
3.28	Services > Advanced.....	100
3.29	System > Debug.....	102
3.30	System > Update	103
3.31	System > App Center	104
3.32	System > Tools	105
3.33	System > Profile.....	107
3.34	System > User Management	109
Chapter 4	Configuration Examples.....	111
4.1	Cellular	111
4.1.1	Cellular Dial-Up.....	111
4.1.2	SMS Remote Control.....	113
4.2	Network.....	115
4.2.1	IPsec VPN	115
4.2.2	OpenVPN	119
4.2.3	GRE VPN.....	121
Chapter 5	Introductions for CLI.....	123
5.1	What Is CLI.....	123
5.2	How to Configure the CLI	124
5.3	Commands Reference	130
Glossary		131

Chapter 1 Product Overview

1.1 Key Features

The Robustel Industrial Dual Module Cellular VPN Router with Voice (R2000 Ent) provides fast and reliable Internet connectivity, enhanced voice capabilities – making it perfect to respond to and manage any device, anytime and anywhere.

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

- Voice channel/RS-232/RS-485 (choose one only) shared across an RJ11 port
- Voice call and data transmission being used simultaneously, depending upon your ISP network
- Supports GSM and VoLTE(optional) for voice traffic
- Embedded dual-module supports two SIM cards online simultaneously
- The feature Link Manager supports configuration of Cellular WAN, Ethernet WAN, WiFi link backup and ICMP detection
- The option *Backup Mode* supports cold, warm and load balancing
- WAN port supports PD feature – compatible with 802.3at.
- WiFi supports AP mode and Client mode
- RobustOS + SDK + App
- IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Management and maintenance via Web/CLI/SMS/SNMP/RobustLink Cloud
- Auto reboot via SMS/Timing
- Including built-in software watchdog
- Desktop and easy wall or DIN rail mounting options

1.2 Package Contents

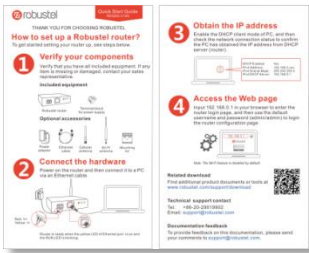
Before installing your R2000 Ent Router, verify the kit contents as following.

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

- 1 x Robustel R2000 Ent Industrial Dual Module Cellular VPN Router with Voice



- 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



- L-type screwdriver



- Ethernet cable



- RJ11 to RJ11 phone connectivity cable



- AC/DC power adapter (12V DC, 1.0 A; EU/US/UK/AU plug optional)



1.3 Specifications

Cellular Interface

- Number of antennas: 4 (MAIN1 + AUX1 + MAIN2 + AUX2)
- Connector: SMA female
- 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
 - 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: 4 x LAN + 1 x WAN (10/100 Mbps)
- WAN port: Supports 802.3 at PD feature (optional)
- Magnet isolation protection: 4 KV

WiFi Interface

- Number of antennas: 2 (WiFi1 + WiFi2)
- Connector: RP-SMA male

- Standards: 802.11b/g/n, supports AP and Client modes
- Frequency bands: 2.4 GHz
- Security: WEP, WPA, WPA2
- Encryption: 64/128 AES, TKIP
- Data speed: 2*2 MIMO, up to 300 Mbps
- RF output power:

802.11b	19 dBm
(+/- 1 dBm) 802.11g	19 dBm
802.11n (20 MHz)	18 dBm
802.11n (40 MHz)	17 dBm
- Receiving sensitivity:

802.11b	-93 dBm
(+/- 1 dBm) 802.11g	-90 dBm
802.11n (20 MHz)	-88 dBm
802.11n (40 MHz)	-85 dBm

Voice Interface

- Number of ports: 1 x Voice call (only SIM1 support)
- Connector: RJ11 (also be used for landline telephone's power supply)
- Standards: ITU Q.512 (SLIC)
 - ITU K.20 (overcurrent and overvoltage protection)
- Subscriber line interface circuit (SLIC)
 - Ring voltage: 40 to 90 Vpk configurable
 - Ring frequency: 20 to 25 Hz
 - Ring waveform: sine wave
 - Maximum ringer load: 5 ringer equivalence numbers (RENs)
 - On-hook voltage (tip/ring): -46 to -56V
 - Off-hook current: 18 to 20 mA
 - Terminating impedance: configurable

Serial Interface

- 1 x RS-232/RS-485 with an RJ11 interface
- 1 x USB 2.0 host up to 480 Mbps

Others

- 1 x Reset button (RST)
- LED indicators - 1 x RUN, 1 x NET1, 1 x NET2, 1 x RSSI1, 1 x RSSI2, 1 x USR
 - 5 x LINK of Ethernet interface, including WAN, ETH1, ETH2, ETH3 and ETH4

Software (Basic features of RobustOS)

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, HTTPs, DNS, ARP, RIP, OSPF, NTP, SMTP, Telnet, VLAN, SSH2, etc.
- VPN tunnel: IPsec, OpenVPN, GRE
- Firewall: DMZ, anti-DoS, Filtering (IP/Domain name/MAC address), Port Mapping, Access Control
- Management: Web, CLI, SMS
- Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU Gateway

App Center (Available Apps for RobustOS)

- Apps*: L2TP, PPTP, DMVPN, RobustVPN, VRRP, QoS, Captive Portal, WLAN Multi AP, SNMP, Language, RobustLink
- *Request on demand. For more Apps please visit www.robustel.com.

Power Supply and Consumption

- Connector: 2.1 mm DC Jack socket
Input voltage: 9 to 36V DC
- Power consumption: Idle: 350 mA@12 V
Data link: 500 mA (peak) @12 V
- PD feature: WAN port support
Input voltage: 48 to 57V DC

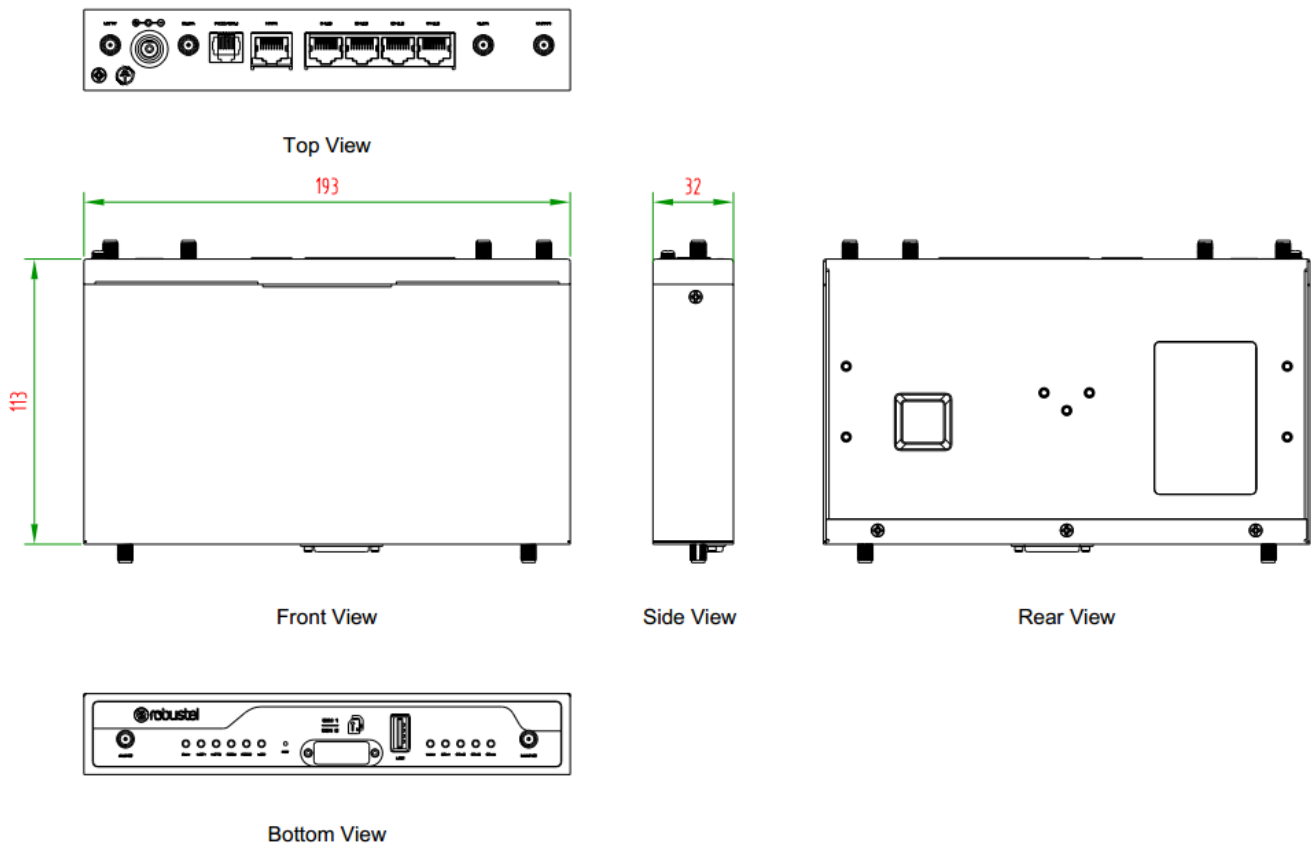
Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Metal, 695 g
- Dimensions: 193 x 113 x 32 mm
- Installations: Desktop, wall mounting or 35 mm DIN rail mounting

Approvals

- Regulatory: CE, RCM
- Environmental: RoHS2.0, WEEE

1.4 Dimensions



1.5 Ordering Information

Model	R2000-E4L1	R2000-E4L2
Module Number	Single module	Dual module
Antenna Number	2	4
Air Interface	GSM/GPRS/EDGE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/TD-SCDMA/CDMA (CDMA 1X/EVDO)/FDD LTE/TDD LTE	
Frequency Bands	AU: B1/B3/B5/B7/B8/B28, B40 EU: B1/B3/B7/B8/B20/B28/B31, B38/B40 US: B2/B4/B5/B13/B17/B25, B41 JP: B1/B3/B8/B9/B18/B19/B21/B28, B41 CN: B1/B3, B38/B39/B40/B41	
4G*	WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+: B1/B2/B5/B6/B8/B9/B19 TD-SCDMA: B34/B39 CDMA (CDMA 1X/EVDO): R0/A BC0/BC1/BC10	
3G	WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+: B1/B2/B5/B6/B8/B9/B19 TD-SCDMA: B34/B39 CDMA (CDMA 1X/EVDO): R0/A BC0/BC1/BC10	
2G	850/900/1800/1900 MHz	
Operating Environment	-25 to +70 °C/5 to 95% RH	

*For more information about 4G frequency bands in different countries, please contact your Robustel sales representative.

Chapter 2 Hardware Installation

2.1 LED Indicators

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



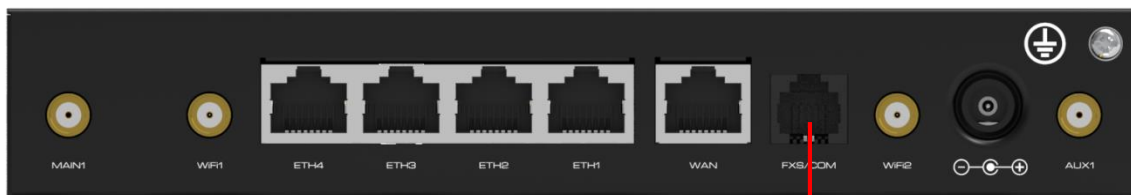
Name	Color	Status	Description
RUN	Green	On, fast blinking (250 mSec blink time)	Router is powered on (System is initializing)
		On, blinking (500 mSec blink time)	Router starts operating
		Off	Router is powered off
NET1 (Represents for the Module1)	Green	On, solid	Network is joined successfully by using the Module1 card and worked in an optimum one
		On, blinking	Network is joined successfully but worked in a lower-level than standard
		Off	Network is not joined or joining
NET2 (Represents for the Module2)	Green	On, solid	Network is joined successfully by using the Module2 card and worked in an optimum one
		On, blinking	Network is joined successfully but worked in a lower-level than standard
		Off	Network is not joined or joining
RSSI1 (Represents for the signal value of Module1)	Green	On, solid	High signal strength (21-31) is available
		On, slow blinking (1 sec blink time)	Medium signal strength (11-20) is available
		On, fast blinking	Low signal strength (1-10) is available
		Off	No signal
RSSI2 (Represents for the signal value of Module2)	Green	On, solid	High signal strength (21-31) is available
		On, slow blinking	Medium signal strength (11-20) is available
		On, fast blinking	Low signal strength (1-10) is available
		Off	No signal
USR-SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used
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
WAN/ETH1/ ETH2/ETH3/ ETH4	Green	On, solid	Connection is established
		On, blinking	Data is being transferred
		Off	Connection is not established

Note: You can choose the display type of USR LED. For more details, please refer to **3.28 Service > Advanced**.

2.2 RJ11 Interface

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



RJ11 Port
 (Shared by voice input
 /RS-232/RS-485)

PIN	Voice	Direction
1	NC	--
2	NC	--
3	RINGD/RDC	I/O
4	TIPD/TDC	I/O
5	NC	--
6	NC	--

PIN	RS-232	Direction
1	NC	--
2	GND	--
3	RXD	Router ← Device
4	TXD	Router → Device
5	GND	--
6	NC	--

PIN	RS-485	Direction
1	NC	--
2	GND	--
3	B	RS485_D-
4	A	RS485_D+
5	GND	--
6	NC	--

2.3 USB Interface



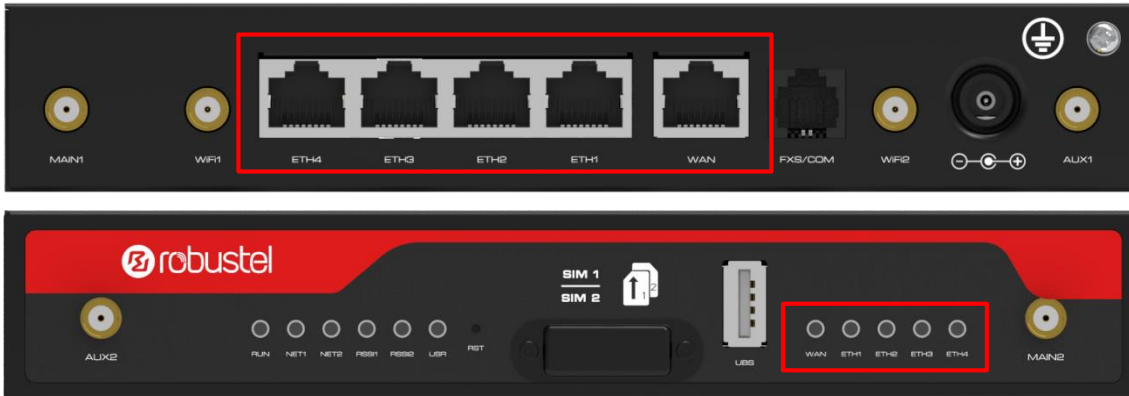
Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the router's USB interface, such as a U disk or a hard disk. If there have a supported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

2.4 Reset Button



Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 5 seconds after powering up the router, press and hold the RST button for about 16 seconds until all six LEDs start blinking one by one, and release the button to return the router to factory defaults.

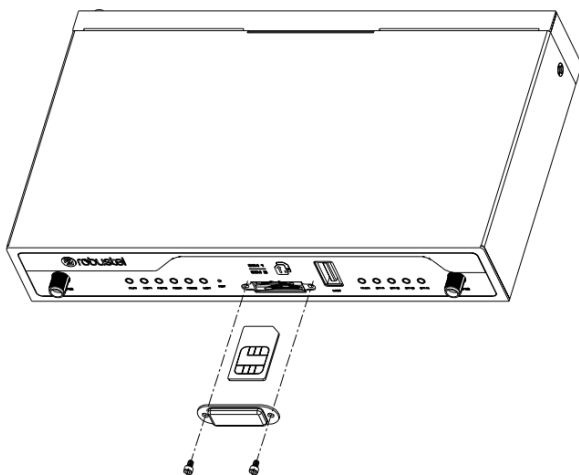
2.5 Ethernet Port



R2000 Ent Router has five Ethernet ports, including WAN, ETH1, ETH2, ETH3 and ETH4. And every Ethernet port corresponds to a specific LED indicator in the bottom view of the router (refer to the above figures). For details about status, see the table below.

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

2.6 Insert or Remove SIM Card



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

- **Insert SIM card**

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

- **Remove SIM card**

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

Note:

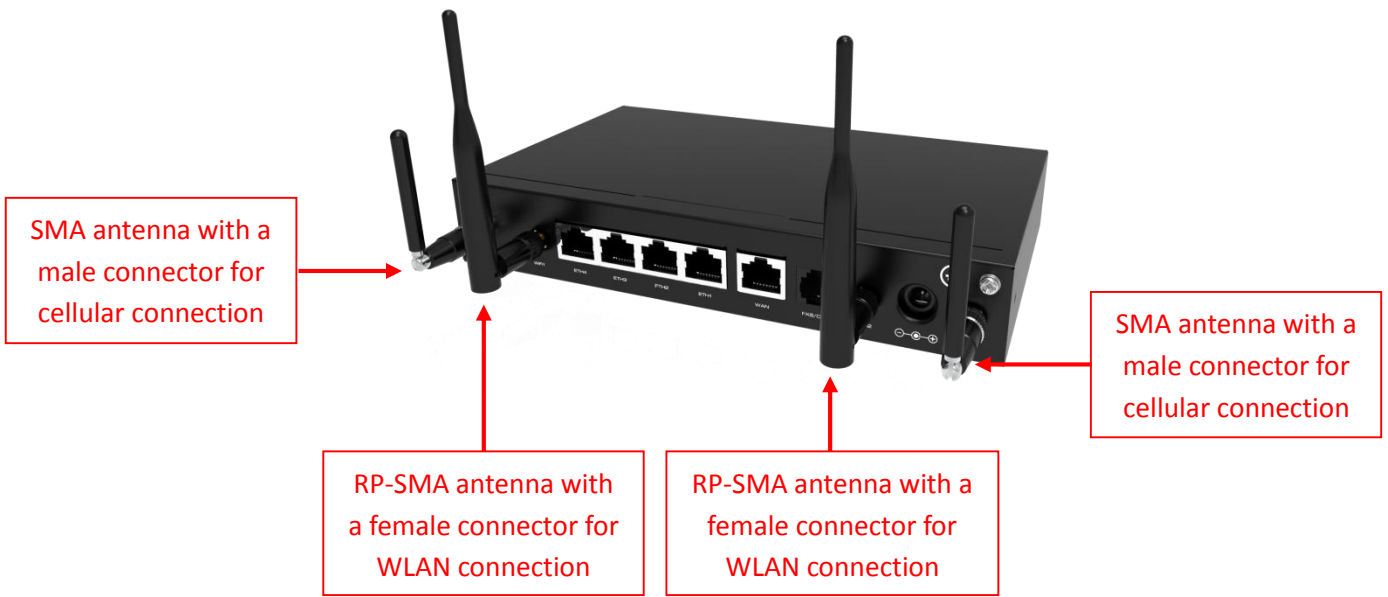
1. Recommended torque for inserting is 0.5 N.m, and the maximum allowed is 0.7 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not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



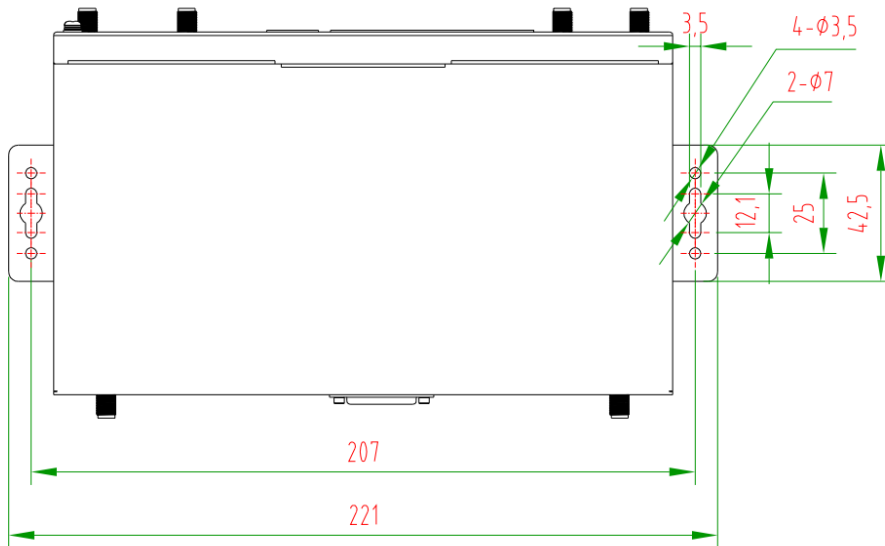


2.8 Mount the Router

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

Two methods for mounting the router

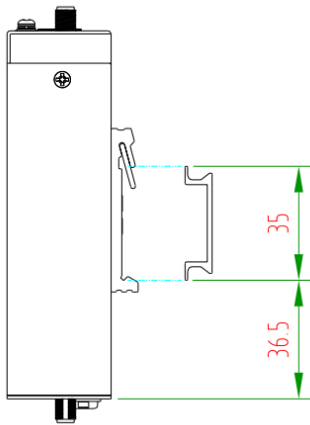
1. Wall mounting (measured in mm)



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

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

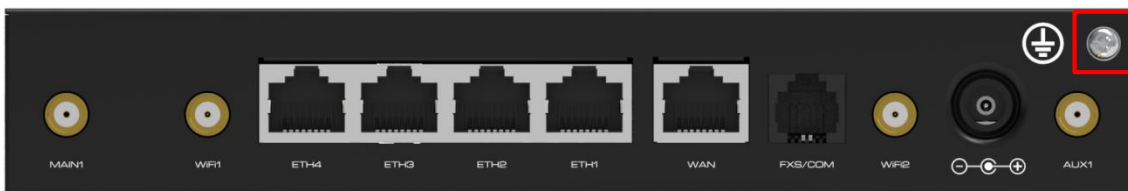
2. DIN rail mounting (measured in mm)



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.

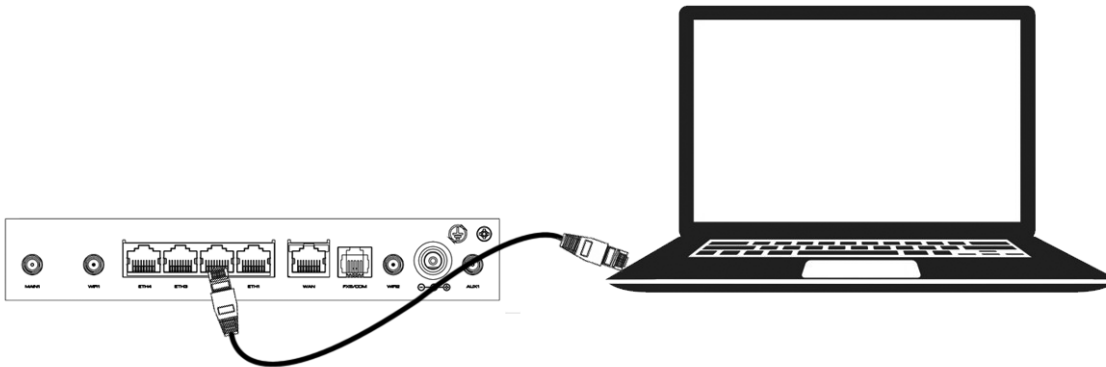
2.9 Ground the Router



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.

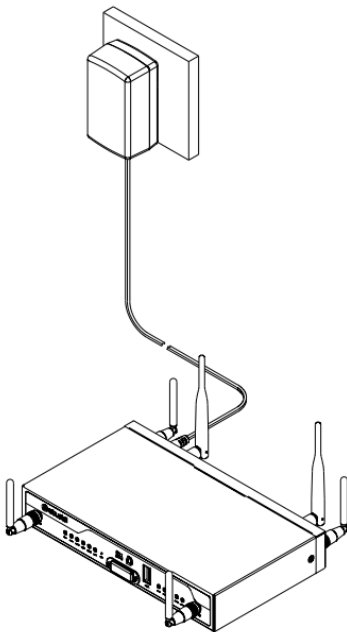
Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.

2.10 Connect the Router to a Computer



Connect an Ethernet cable to any port marked ETH1~4 at the top of the R2000 Ent Router, and connect the other end of the cable to your computer.

2.11 Power Supply



Use a DC Jack adapter to connect the router's power connector to the power supply.

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

Chapter 3 Initial Configuration

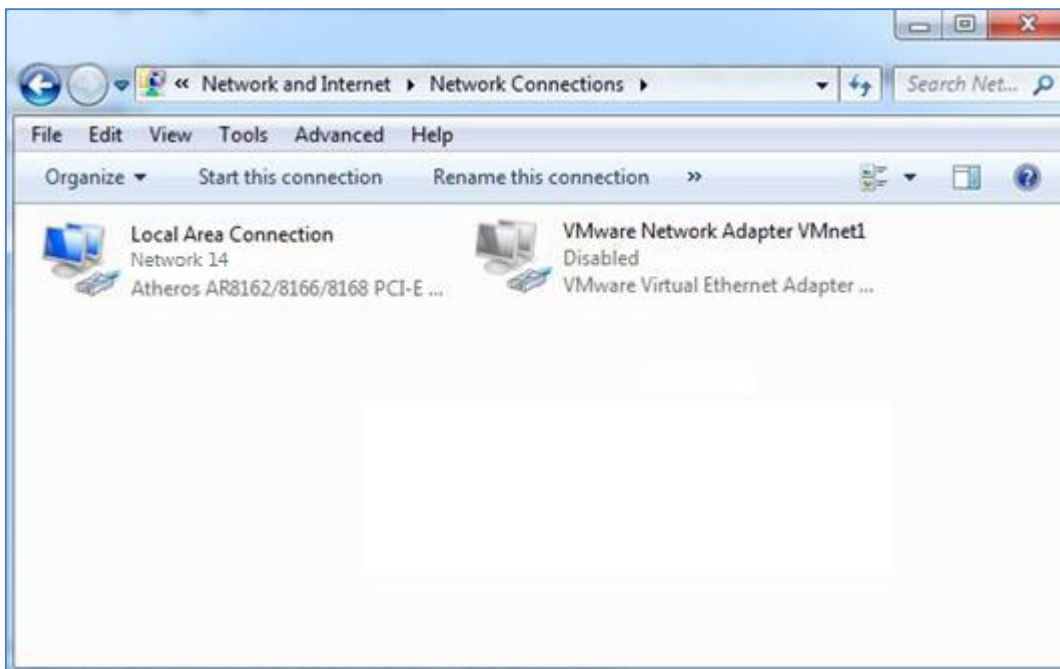
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

3.1 Configure the PC

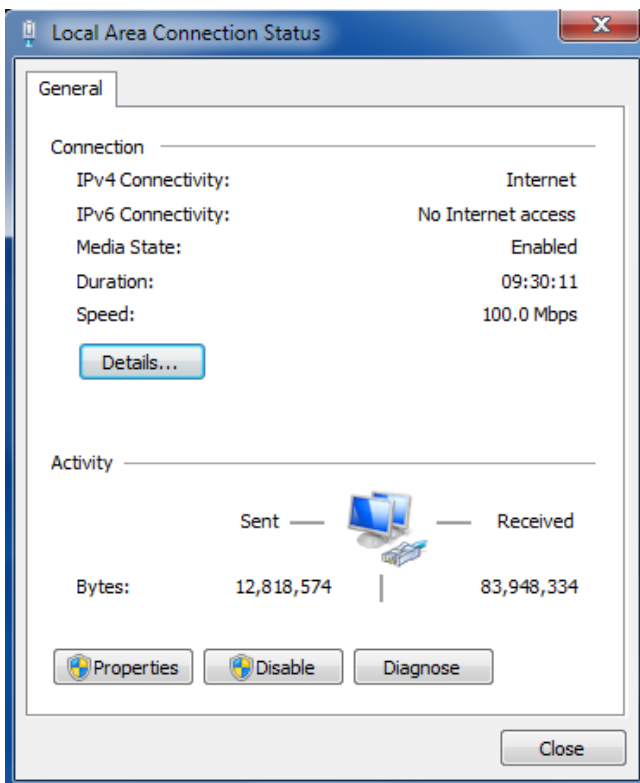
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

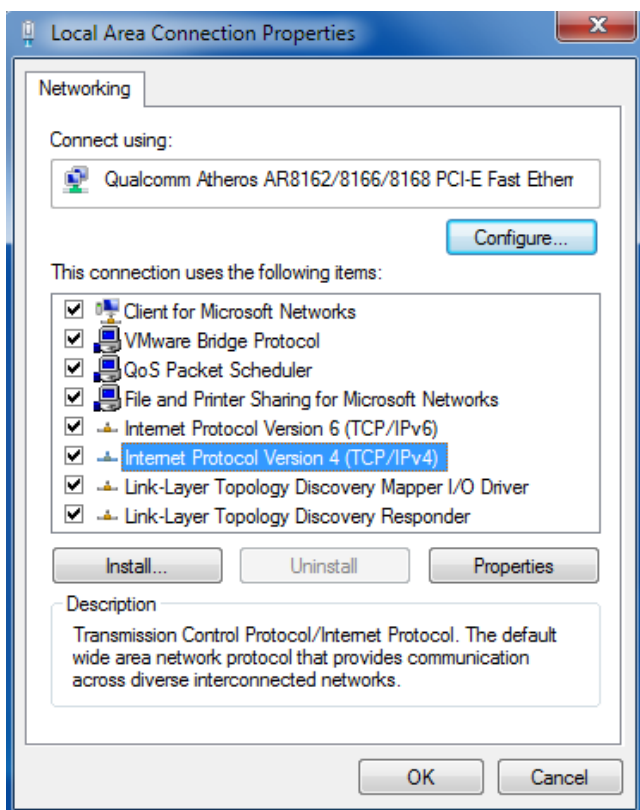
1. Click **Start > Control panel**, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



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

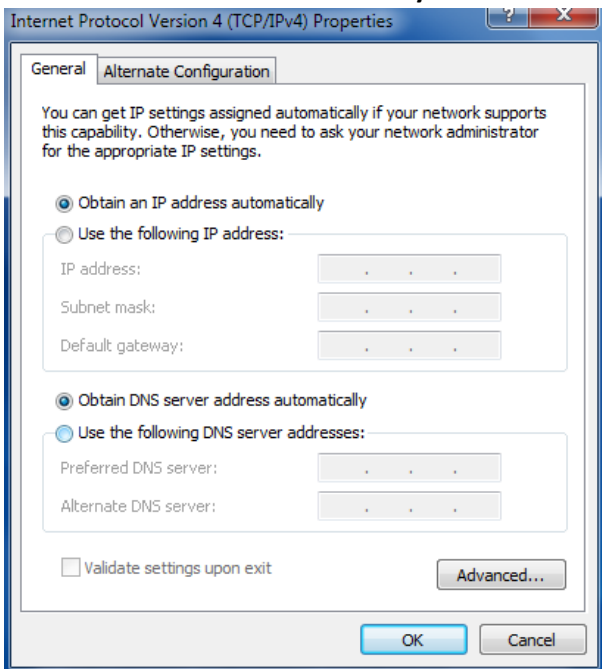


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



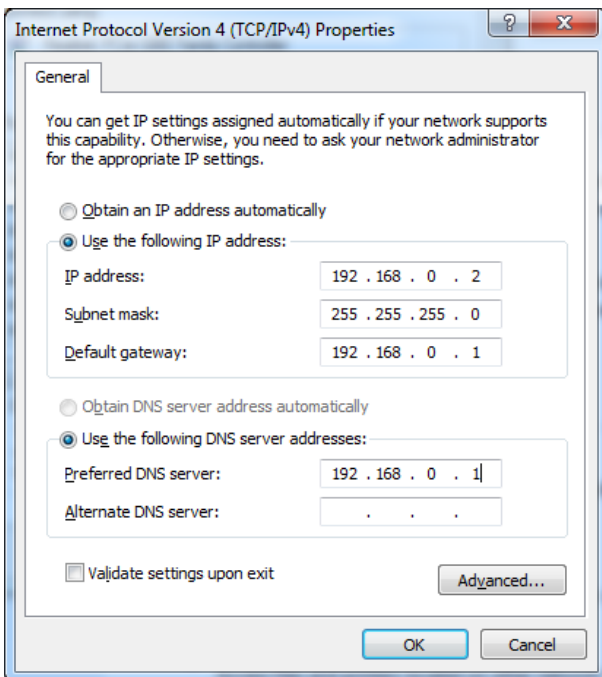
4. Two ways for configuring the IP address of PC.

Obtain an IP address automatically:



Use the following IP address:

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



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

3.2 Factory Default Settings

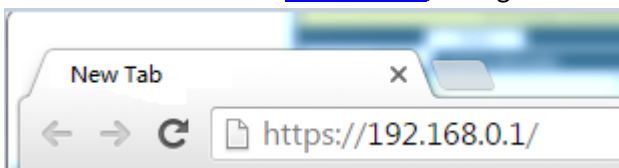
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
WAN	DHCP connection type by default, WAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
ETH2	192.168.0.1/255.255.255.0, LAN mode
ETH3	192.168.0.1/255.255.255.0, LAN mode
ETH4	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

3.3 Log in the Router

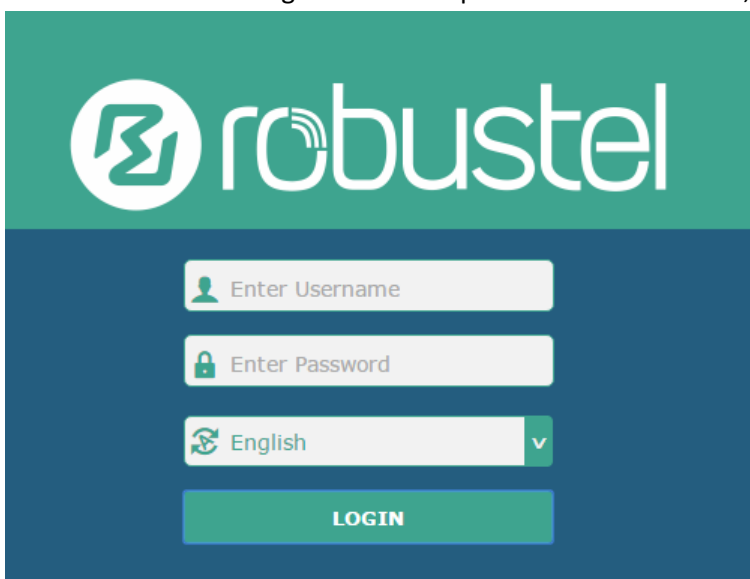
To log in to the management page and view the configuration status of your router, please follow the steps below.

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



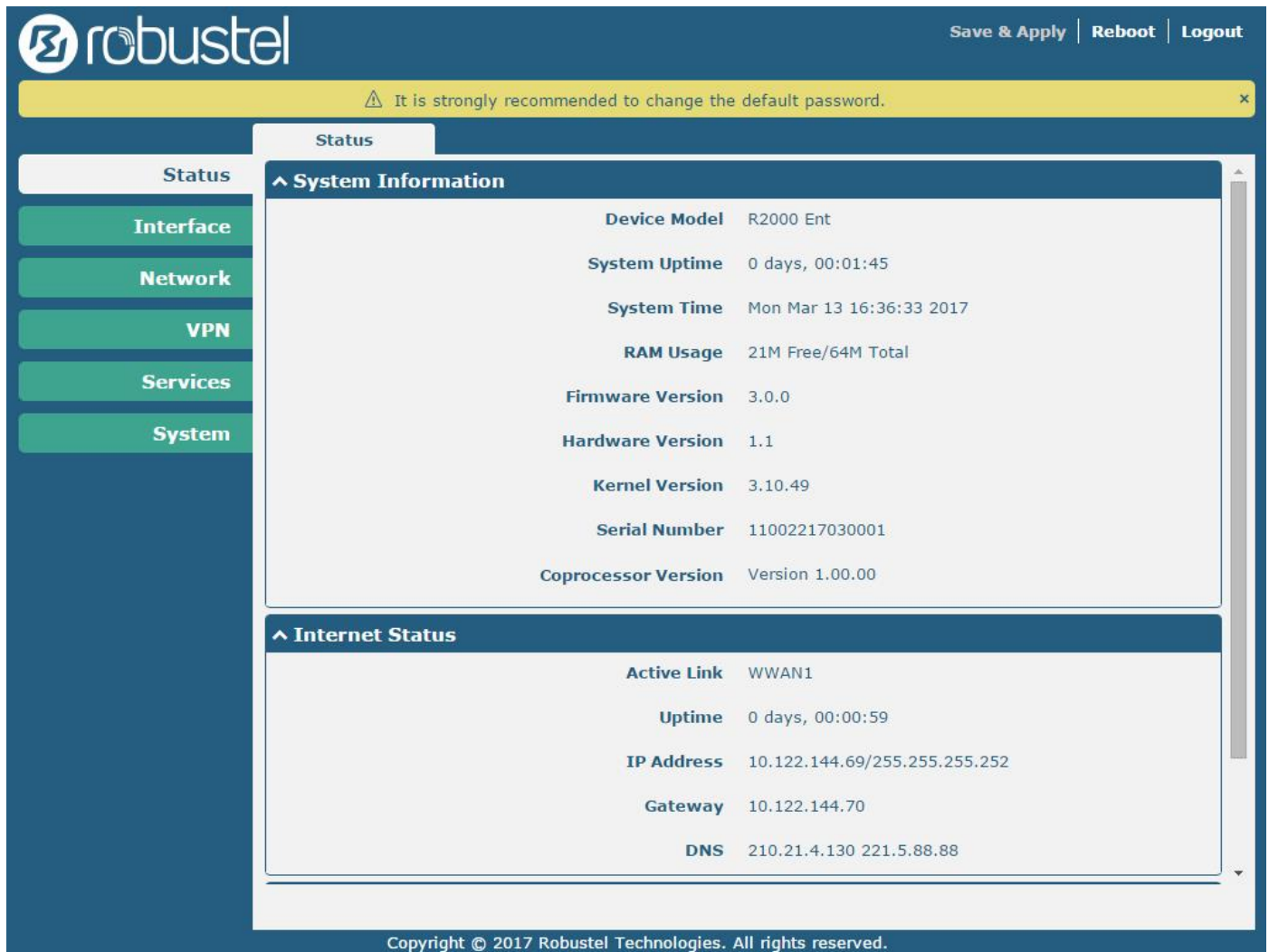
3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are "admin".

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




3.4 Control Panel



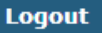
After logging in, the home page of the R2000 Ent Router's web interface is displayed, for example.



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



It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **3.34 System > User Management**.

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

	login web on this browser without a password before timeout.	
Submit	Click to save the modification on current configuration page.	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	R2000 Ent
System Uptime	0 days, 00:01:45
System Time	Mon Mar 13 16:36:33 2017
RAM Usage	21M Free/64M Total
Firmware Version	3.0.0
Hardware Version	1.1
Kernel Version	3.10.49
Serial Number	11002217030001
Coprocessor Version	Version 1.00.00

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.
Coprocessor Version	Show the coprocessor version of your device.

Internet Status

^ Internet Status	
Active Link	WWAN1
Uptime	0 days, 00:00:59
IP Address	10.122.144.69/255.255.255.252
Gateway	10.122.144.70
DNS	210.21.4.130 221.5.88.88

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

LAN Status

^ LAN Status	
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:06:DC:59

LAN Status	
Item	Description
IP Address	Show the IP address and the Netmask of the router.
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 ?

Backup Link ?

Backup Mode ?

Revert Interval ?

Emergency Reboot ON OFF ?

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

Note: Click  for help.

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

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

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

WWAN1/WWAN2

Link Manager

^ General Settings

Index

Type

Description

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

^ WWAN Settings

Automatic APN Selection ON OFF

Dialup Number

Authentication Type

Switch SIM By Data Allowance ON OFF ?

Data Allowance ?

Billing Day ?

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

^ WWAN Settings

Automatic APN Selection ON OFF

APN

Username

Password

Dialup Number

Authentication Type

Switch SIM By Data Allowance ON OFF ?

Data Allowance ?

Billing Day ?

^ Ping Detection Settings
?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF

Link Settings (WWAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null
WWAN Settings		
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the access point name automatically. Alternatively, you can disable this option and manually add the access point name.	ON
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Dialup Number	Enter the dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. Note: Only used for dual SIM backup.	OFF

Link Settings (WWAN)		
Item	Description	Default
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in Interface > Link Manager > Status > WWAN Data Usage Statistics . 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
Upload Bandwidth	Set the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set the download bandwidth used for QoS, measured in kbps.	10000
Overridden Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overridden Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WAN

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

Link Manager

^ General Settings

Index	<input type="text" value="3"/>
Type	<input type="text" value="WAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="DHCP"/>

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

^ General Settings

Index	<input type="text" value="3"/>
Type	<input type="text" value="WAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="Static"/>

^ Static Address Settings

IP Address	<input type="text"/>	?
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	

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

^ General Settings

Index	<input type="text" value="3"/>
Type	<input type="text" value="WAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="PPPoE"/>

^ PPPoE Settings

Username	<input type="text"/>	
Password	<input type="text"/>	
Authentication Type	<input type="text" value="Auto"/>	
PPP Expert Options	<input type="text"/>	?

^ Ping Detection Settings ?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

MTU

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden 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.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from "DHCP", "Static" or "PPPoE".	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the IP address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null

Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.114.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overridden Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overridden Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WLAN

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

Link Manager

^ General Settings

Index	<input type="text" value="4"/>
Type	<input type="text" value="WLAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="DHCP"/>

^ WLAN Settings

SSID	<input type="text" value="Robustel"/>
Connect to Hidden SSID	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Password	<input type="password" value="....."/>

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

^ General Settings

Index	<input type="text" value="4"/>
Type	<input type="text" value="WLAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="Static"/>

^ Static Address Settings

IP Address	<input type="text"/>	
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	

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

^ Ping Detection Settings ?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

MTU

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF


Link Settings (WLAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WLAN
Description	Enter a description for this link.	Null
Connection Type	Select from "DHCP" or "Static".	DHCP
WLAN Settings		
SSID	Enter a 1-32 characters SSID which your router wants to connect. SSID (Service Set Identifier) is the name of your wireless network.	router
Connect to Hidden SSID	Click the toggle button to enable/disable this option. When router works as Client mode and needs to connect any access point which has hidden SSID, you need to enable this option.	OFF
Password	Enter an 8-63 characters password of the access point which your router wants to connect.	Null
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of WiFi AP.	Null
Primary DNS	Set the primary DNS.	Null

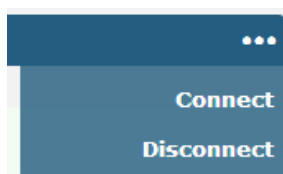
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.1 14.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overridden Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overridden Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

Status

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

Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:07:53	10.104.244.1..
2	WWAN2	Disconnected		

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



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

^ Link Status				
Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:07:53	10.104.244.1..
<p>Index 1</p> <p>Link WWAN1</p> <p>Status Connected</p> <p>Interface wwan1</p> <p>Uptime 0 days, 00:07:53</p> <p>IP Address 10.104.244.179/255.255.255.248</p> <p>Gateway 10.104.244.177</p> <p>DNS 210.21.4.130 221.5.88.88</p> <p>RX Packets 22</p> <p>TX Packets 26</p> <p>RX Bytes 2124</p> <p>TX Bytes 2690</p>				
2	WWAN2	Disconnected		

^ 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 four LAN ports on R2000 Ent Router, including ETH1~ETH4. The ETH1~ETH4 can freely choose from lan0~lan3, but at least one LAN port must be assigned as lan0. The default settings of ETH1~ETH4 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN

By default, there is a LAN port (lan0) in the list. To begin adding a new LAN port (lan1), please configure one of ETH1~ETH4 as lan1 first in **Ethernet > Ports > Port Settings**. Otherwise, the operation will be prompted as "List is full".

LAN	Multiple IP	VLAN Trunk	Status
^ Network Settings ?			
Index	Interface	IP Address	Netmask
1	lan0	192.168.0.1	255.255.255.0
+ ✎ ✕			

Note: Lan0 cannot be deleted.

You may click ✎ to edit the configuration of the LAN port, or click ✕ to delete the current LAN port. Now, click + to add a new LAN port. The maximum count is 4.

LAN

^ General Settings

Index:

Interface:

IP Address:

Netmask:

MTU:

General Settings @ LAN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Lan1 is available only if it was selected by one of ETH1~ETH4 in Ethernet > Ports > Port Settings .	lan0
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

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

^ DHCP Settings

Enable ON OFF

Mode Server v

IP Pool Start

IP Pool End

Subnet Mask

^ DHCP Advanced Settings

Gateway

Primary DNS

Secondary DNS

WINS Server

Lease Time ?

Static lease ?

Expert Options ?

Debug Enable ON OFF

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

^ DHCP Settings

Enable ON OFF

Mode Relay v

DHCP Server For Relay

^ DHCP Advanced Settings

Debug Enable ON OFF

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

LAN		
Item	Description	Default
IP Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
Gateway	Define the gateway assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Define the primary DNS server assigned by the DHCP server to the clients.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the clients.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF

Multiple IP

LAN	Multiple IP	VLAN Trunk	Status
^ Multiple IP Settings			
Index	Interface	IP Address	Netmask
1	lan0	172.16.99.44	255.255.0.0

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

Multiple IP

^ IP Settings

Index:

Interface:

IP Address:

Netmask:

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

VLAN Trunk

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

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

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

VLAN Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this VLAN. Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0", "lan1", "lan2" or "lan3" depends on your ETH1~ETH4'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	VLAN Trunk	Status	
^ Interface Status				
Index	Interface	IP Address	MAC Address	
1	lan0	192.168.0.1/255.2...	34:FA:40:02:C0:9A	
^ Connected Devices				
Index	IP Address	MAC Address	Interface	Inactive Time
1	172.16.2.15	D0:50:99:4D:F9:92	lan0	55s
2	172.16.1.23	D0:17:C2:8A:DB:F9	lan0	64s
3	172.16.5.25	34:DE:1A:F5:36:9C	lan0	162s
4	172.16.0.128	F8:32:E4:73:C3:2A	lan0	8s
5	172.16.5.232	1C:1B:0D:6C:2F:91	lan0	490s
6	172.16.5.108	48:D2:24:53:63:F6	lan0	3s
7	172.16.5.133	D0:50:99:8A:1E:B7	lan0	22s
8	172.16.5.169	3C:97:0E:F4:82:79	lan0	8s
9	172.16.5.178	D0:50:99:A9:09:1F	lan0	124s
10	172.16.5.76	D0:50:99:4D:F9:35	lan0	0s
11	172.16.5.200	00:E0:4C:03:0C:DD	lan0	1s
12	172.16.2.89	D0:50:99:51:C2:DE	lan0	818s
13	172.16.0.171	2C:56:DC:79:3D:D8	lan0	14s
^ DHCP Lease Table				
Index	IP Address	MAC Address	Interface	Expired Time

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

^ Interface Status			
Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:02:C0:9A
		Index	1
		Interface	lan0
		IP Address	192.168.0.1/255.255.255.0
		MAC Address	34:FA:40:02:C0:9A
		RX Packets	32342
		TX Packets	662
		RX Bytes	2904609
		TX Bytes	372319

3.8 Interface > Ethernet

This section allows you to set the related parameters for Ethernet. There are five Ethernet ports on R2000 Ent Router, including WAN, ETH1, ETH2, ETH3 and ETH4. The WAN on the router can only be configured as a WAN port, while ETH1~ETH4 can only be configured as LAN ports. The ETH1~ETH4 can freely choose from lan0~lan3, but at least one LAN port must be assigned as lan0. The default settings of ETH1~ETH4 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

Ports	Status	
^ Port Settings		
Index	Port	Port Assignment
1	eth0	wan
2	eth1	lan0
3	eth2	lan0
4	eth3	lan0
5	eth4	lan0

Click button of eth1 to configure its parameters. The port assignment can be changed by selecting from the drop down list.

Ports

^ Port Settings

Index:

Port:

Port Assignment:

^ Port Settings

Index:

Port:

Port Assignment:

- lan0
- lan1
- lan2
- lan3
- wan

Port Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Port	Show the editing port, read only.	--
Port Assignment	Choose the Ethernet port's type, as a WAN port or a LAN port. When setting the port as a LAN port in Interface > LAN > LAN > Network Settings > General Settings , you can click the drop-down list to select from "lan0", "lan1", "lan2" or "lan3".	lan0

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

Ports			Status
^ Port Status			
Index	Port	Link	
1	eth0	Down	
2	eth1	Down	
3	eth2	Down	
4	eth3	Up	
5	eth4	Down	

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

^ Port Status		
Index	Port	Link
1	eth0	Down
2	eth1	Down
3	eth2	Down
4	eth3	Up
<p style="text-align: right;"> Index 4 Port eth3 Link Up </p>		
5	eth4	Down

3.9 Interface > Cellular

This section allows you to set the related parameters of Cellular. The R2000 Ent’s embedded dual module supporting two SIM cards online simultaneously. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.

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

Click of SIM 1 to edit the parameters.

Cellular

^ General Settings

Index

SIM Card

Phone Number

PIN Code

Extra AT Cmd

Telnet Port

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

Cellular Network Settings

Network Type v ?

Band Select Type v ?

Advanced Settings

Debug Enable ON OFF

Verbose Debug Enable ON OFF

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

Cellular Network Settings

Network Type v ?

Band Select Type v ?

Band Settings

GSM 850	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 1800	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 1900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 850	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 1900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 2100	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 1	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 2	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 3	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 4	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 5	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 7	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 8	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 20	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

Advanced Settings

Debug Enable ON OFF

Verbose Debug Enable ON OFF

Cellular		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently 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	Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", "4G First". <ul style="list-style-type: none"> Auto: Connect to the best signal network automatically 2G Only: Only the 2G network is connected 2G First: Connect to the 2G Network preferentially 3G Only: Only the 3G network is connected 3G First: Connect to the 3G Network preferentially 4G Only: Only the 4G network is connected 4G First: Connect to the 4G Network preferentially 	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

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

Cellular	Status	AT Debug		
^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	ME909s-120	460065049045542	Registered to home network
2	Modem not found			

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

^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	ME909s-120	460065049045542	Registered to home network
<p>Index 1</p> <p>Modem Status Ready</p> <p>Modem Model ME909s-120</p> <p>Current SIM SIM1</p> <p>Phone Number</p> <p>IMSI 460065049045542</p> <p>ICCID 89860616090020638829</p> <p>Registration Registered to home network</p> <p>Network Provider CHN-UNICOM</p> <p>Network Type LTE</p> <p>Signal Strength 15 (-83dBm)</p> <p>Bit Error Rate 99</p> <p>PLMN ID 46001</p> <p>Local Area Code 2507</p> <p>Cell ID 06074702</p> <p>IMEI 867377021011030</p> <p>Firmware Version 11.617.01.00.00</p>				
2	Modem not found			

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.
Signal Strength	Show the signal strength detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.

Status	
Item	Description
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.

Cellular
Status
AT Debug

^ At Debug

Command

Result

Send

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

3.10 Interface > WiFi

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.

WiFi AP

Configure Router as WiFi AP

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

WiFi
Access Point
Advanced
ACL
Status

^ General Settings

Mode

AP
v
?

Region

SE
?

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

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

WiFi	Access Point	Advanced	ACL	Status
^ General Settings				
Enable <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID R2000 Ent				
Broadcast SSID <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Security Mode Disabled v ?				

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

^ General Settings				
Enable <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID R2000 Ent				
Broadcast SSID <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Security Mode WPA-Personal v ?				
WPA Version Auto v				
Encryption Auto v ?				
PSK Password				
Group Key Update Interval 3600				

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

^ General Settings				
Enable <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Wireless Mode 11bgn Mixed v				
Channel Auto v ?				
SSID R2000 Ent				
Broadcast SSID <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF				
Security Mode WPA-Enterprise v ?				
WPA Version Auto v				
Encryption Auto v ?				
Radius Authentication Server Address				
Radius Authentication Server Port 1812				
Radius Server Share Secret				
Group Key Update Interval 3600				

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

^ General Settings

Enable ON OFF

Wireless Mode v

Channel v ?

SSID

Broadcast SSID ON OFF

Security Mode v ?

WEP Key ?

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

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

General Settings @ Access Point		
Item	Description	Default
PSK Password	Enter the Pre share key password. When router works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812
Radius Server Share Secret	Enter the shared secret of radius authentication server.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

WiFi
Access Point
Advanced
ACL
Status

^ Advanced Settings

Max Associated Stations

Beacon Interval ?

DTIM Period ?

RTS Threshold ?

Fragmentation Threshold ?

Transmit Rate v

11N Transmit Rate v

Transmit Power v

Channel Width v ?

Enable WMM ON OFF

Enable Short GI ON OFF ?

Enable AP Isolation ON OFF ?

Debug Level v

Advanced Settings		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router’s AP.	64
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100

Advanced Settings		
Item	Description	Default
DTIM Period	Set the delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS Threshold	Set the “request to send” threshold. When the threshold set as 2347, the router AP will not send detection signal before sending data. And when the threshold set as 0, the router AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a WiFi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Specify the transmit rate or let it default to “Auto”.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let it default to “Auto”.	Auto
Transmit Power	Select from “Max”, “High”, “Medium” or “Low”.	Max
Channel Width	Select from “Auto”, “20MHz” or “40MHz”. Note: 40 MHz channel width provides higher available data rate, twice as many as 20 MHz channel width.	Auto
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning” or “none”.	none

WiFi | Access Point | **Advanced** | ACL | Status

^ General Settings

Enable ACL OFF

ACL Mode Accept v ?

^ 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

Description

MAC Address

ACL		
Item	Description	Default
General Settings		
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from "Accept" or "Deny". <ul style="list-style-type: none"> Accept: Only the packets fitting the entities of the "Access Control List" can be allowed Deny: All the packets fitting the entities of the "Access Control List" will be denied Note: Router can only allow or deny devices which are included in "Access Control List" at one time.	Accept
Access Control List		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

This section allows you to view the status of AP.

WiFi
Access Point
Advanced
ACL
Status

^ AP Status

Status COMPLETED

Channel 9

Channel Width 20 MHz

MAC Address 34:FA:40:01:CA:5E

^ Associated Stations

Index	MAC Address	IP Address	Name	Connected Time	Signal

WiFi Client

Configure Router as WiFi client

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

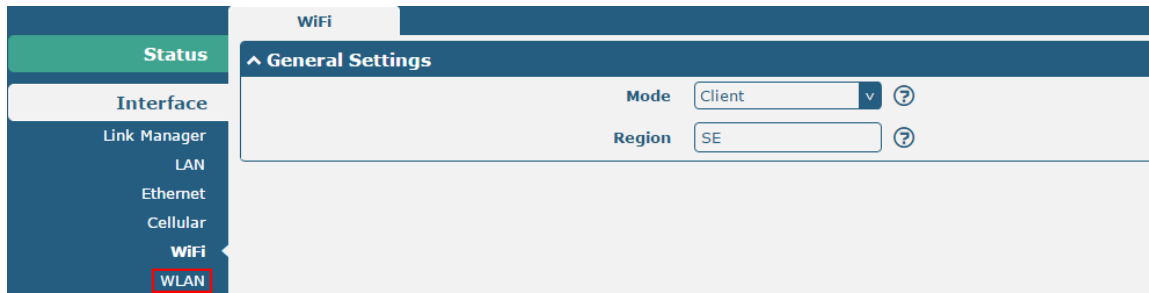
WiFi

^ General Settings

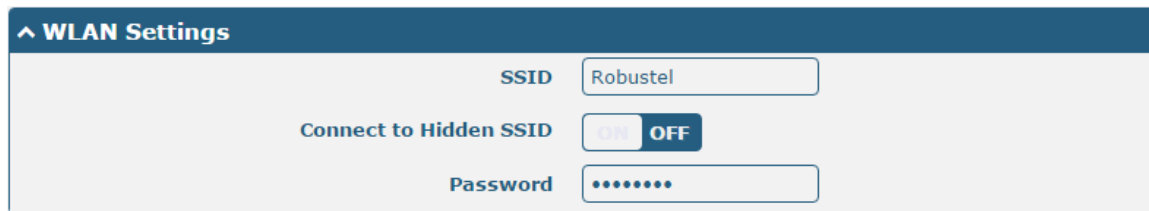
Mode v ?

Region ?

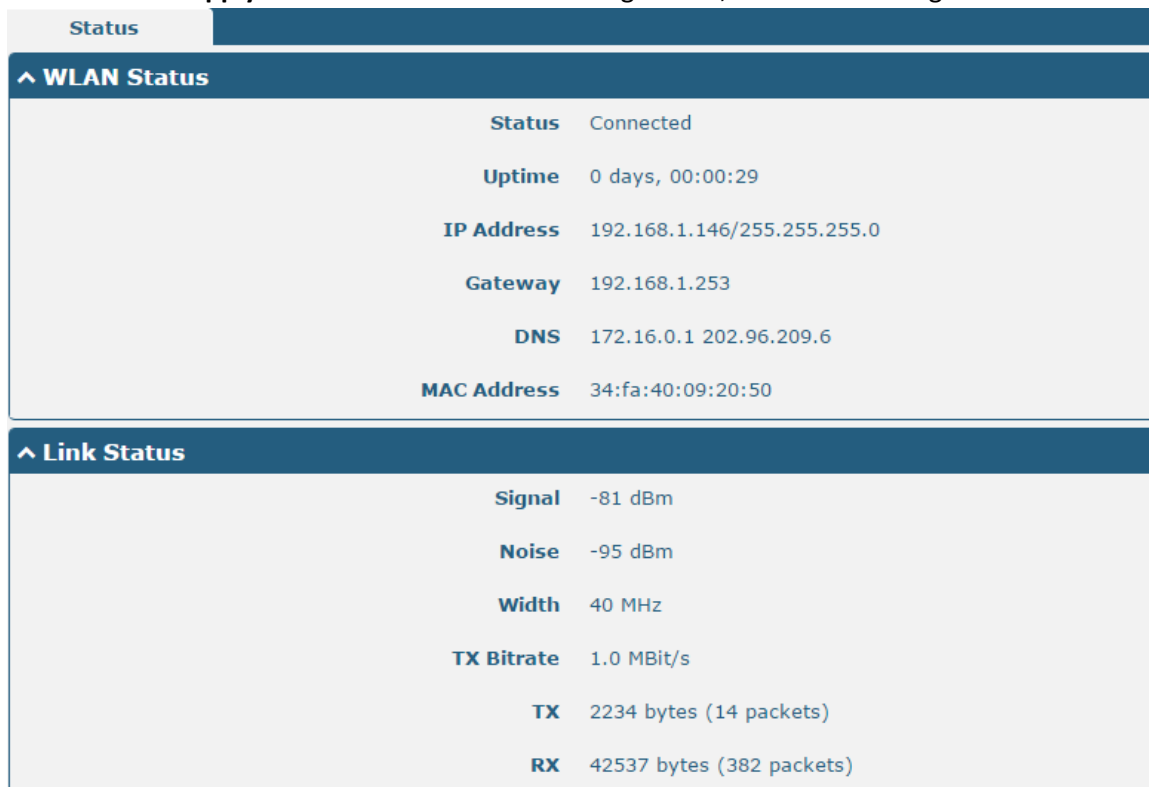
And then a “WLAN” column will appear under the Interface list.



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



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



^ WPA Status

WPA State COMPLETED

Frequency 2412

BSSID 3c:46:d8:23:5d:5a

SSID Robustel

Mode station

Key Management WPA2-PSK

Pairwise Cipher CCMP

Group Cipher CCMP

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

^ Scan Results ⋮

Index	SSID	MAC Address	Frequency	Signal	Scan
-------	------	-------------	-----------	--------	------

^ Scan Results ⋮

Index	SSID	MAC Address	Frequency	Signal
1	Chen	FE:2B:2A:84:79:8F	2462	61 dBm
2	appapp	68:A0:F6:E4:DF:1B	2427	65 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 Key

^ General Settings

Enable USB ON OFF

Enable Automatic Firmware Updating ON OFF

General Settings @ USB		
Item	Description	Default
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Firmware Updating	Click the toggle button to enable/disable this option. Enable to update automatically the router’s firmware when inserting a USB storage device with a router’s firmware.	ON

Router has the key for USB automatic update. User can generate the key in this page.

USB

Key

^ Key

USB Automatic Update Key
Generate

USB Automatic Update Key
Download

Key		
Item	Description	Default
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

3.12 Interface > Serial Port (Optional)

This section allows you to set the serial port parameters. R2000 Ent Router supports one voice input or one RS-232 or one RS-485 which is limited by the hardware on which it's installed. They shared across an RJ11 port. If your router has a serial port, this page is configurable.

Serial Port

Status

^ Serial Port Settings

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

Click the edit button of COM1.

Serial Port

^ Serial Port Application Settings

Index

Port

COM1
v

Enable

ON

OFF

Baud Rate

115200
v

Data Bits

8
v

Stop Bits

1
v

Parity

None
v

Flow Control

None
v

^ Data Packing

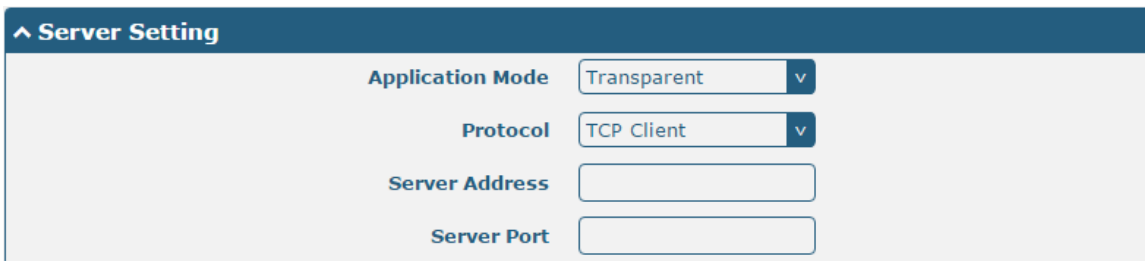
Packing Timeout

?

Packing Length

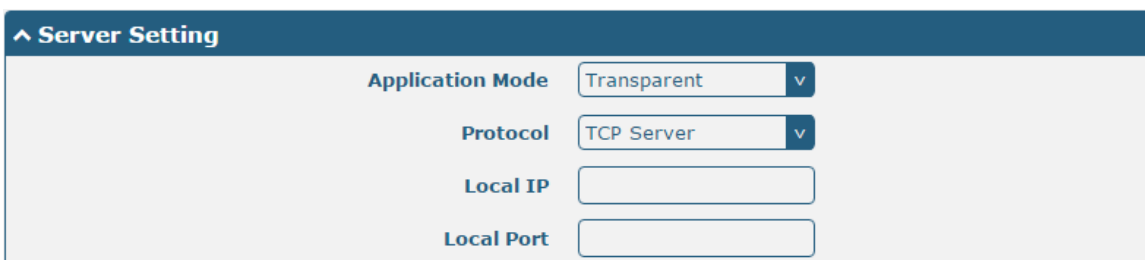
Serial Port		
Item	Description	Default
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud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

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



The screenshot shows a window titled "Server Setting" with a blue header. It contains four settings: "Application Mode" is set to "Transparent" (dropdown), "Protocol" is set to "TCP Client" (dropdown), "Server Address" is an empty text input field, and "Server Port" is an empty text input field.

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



The screenshot shows a window titled "Server Setting" with a blue header. It contains four settings: "Application Mode" is set to "Transparent" (dropdown), "Protocol" is set to "TCP Server" (dropdown), "Local IP" is an empty text input field, and "Local Port" is an empty text input field.

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

^ Server Setting

Application Mode	Transparent v
Protocol	UDP v
Local IP	<input type="text"/>
Local Port	<input type="text"/>
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

^ Server Setting

Application Mode	Transparent v
Protocol	Robustlink v

- 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	<input type="text"/>
Server Port	<input type="text"/>

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	<input type="text"/>
Local Port	<input type="text"/>

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

^ Server Setting

Application Mode	Modbus RTU Gatewa v
Protocol	UDP v
Local IP	<input type="text"/>
Local Port	<input type="text"/>
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

^ **Server Setting**

Application Mode Modbus RTU Gateway v

Protocol Robustlink v

Server Settings		
Item	Description	Default
Application Mode	Select from “Transparent” or “Modbus RTU Gateway”. <ul style="list-style-type: none"> Transparent: Router will transmit the serial data transparently Modbus RTU Gateway: Router will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa 	Transparent
Protocol	Select from “TCP Client”, “TCP Server”, “UDP” or “Robustlink”. <ul style="list-style-type: none"> TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name TCP Server: Router works as TCP server, listening for connection request from TCP client UDP: Router works as UDP client Robustlink: Router will automatically upload the serial data to Robustlink platform under the Robustlink protocol. Robustlink is a management platform from Robustel. This function only available when Router is connects to Robustlink 	TCP Client
Server Address	Enter the address of server which will receive the data sent from router’s serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port @ Transparent	Enter the port of router’s LAN IP.	Null
Local IP @ Modbus	Enter the local IP of under Modbus mode.	Null
Local Port @ Modbus	Enter the local port of under Modbus mode.	Null

Click the “Status” column to view the current serial port type.

Serial Port	Status			
^ Serial Port Status list				
Index	Type	Tx	Rx	Connection Status
1	RS485	0B	0B	

3.13 Network > Route

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

Static Route

Static Route
Status

^ Static Route Table

Index	Description	Destination	Netmask	Gateway	Interface	+
-------	-------------	-------------	---------	---------	-----------	---

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

Static Route

^ Static Route

Index

Description

Destination

Netmask

Gateway

Interface

wwan1 v

Static Route		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan1

Status

This window allows you to view the status of route.

Static Route
Status

^ Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	172.16.0.0	255.255.0.0	0.0.0.0	lan0	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

3.14 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
DMZ

^ General Settings

Enable Filtering ON OFF

Default Filtering Policy Accept v ?

^ Access Control Settings

Enable Remote SSH Access ON OFF

Enable Local SSH Access ON OFF

Enable Remote Telnet Access ON OFF

Enable Local Telnet Access ON OFF

Enable Remote HTTP Access ON OFF

Enable Local HTTP Access ON OFF

Enable Remote HTTPS Access ON OFF

Enable Remote Ping Respond ON OFF ?

Enable DOS Defending ON OFF

^ Filtering Rules

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

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

Filtering		
Item	Description	Default
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON

Click **+** to add a filtering rule. The maximum count is 20. The window is displayed as below when defaulting "All" or choosing "ICMP" as the protocol. Here take "All" as an example.

Filtering

^ **Filtering Rules**

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Source Address	<input type="text"/> ?
Source MAC	<input type="text"/> ?
Target Address	<input type="text"/> ?
Protocol	<input type="text" value="All"/> v
Action	<input type="text" value="Drop"/> v

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

^ Filtering Rules

Index

Description

Source Address ?

Source Port ?

Source MAC ?

Target Address ?

Target Port ?

Protocol v

Action v

Filtering Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter the target address which the access originator wants to access.	Null
Target Port	Enter the target port which the access originator wants to access.	Null
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP” or “TCP-UDP”. Note: It is recommended that you choose “All” if you don’t know which protocol of your application to use.	All
Action	Select from “Accept” or “Drop”. <ul style="list-style-type: none"> Accept: When Default Filtering Policy is drop, router will drop all the connecting requests except the hosts which fit this accept filtering list Drop: When Default Filtering Policy is accept, router will accept all the connecting requests except the hosts which fit this drop filtering list 	Drop

Port Mapping

Filtering
Port Mapping
DMZ

^ Port Mapping Rules

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	<input type="text" value="1"/>	
Description	<input type="text"/>	
Remote IP	<input type="text"/>	?
Internet Port	<input type="text"/>	?
Local IP	<input type="text"/>	
Local Port	<input type="text"/>	?
Protocol	<input type="text" value="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 the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router's LAN IP which will forward to the internet port of router.	Null
Local Port	Enter the port of router's LAN IP.	Null
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP

DMZ

Filtering | Port Mapping | DMZ

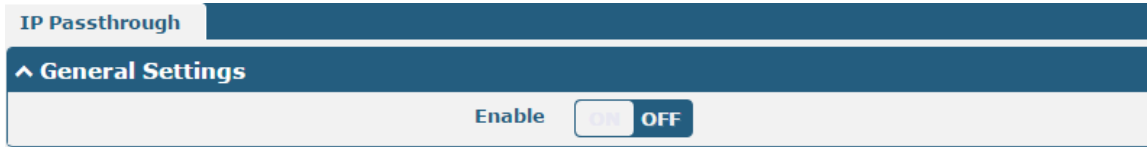
^ **DMZ Settings**

Enable DMZ	<input type="checkbox" value="ON"/> <input checked="" type="checkbox" value="OFF"/>	
Host IP Address	<input type="text"/>	
Source IP Address	<input type="text"/>	?

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

3.15 Network > IP Passthrough

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

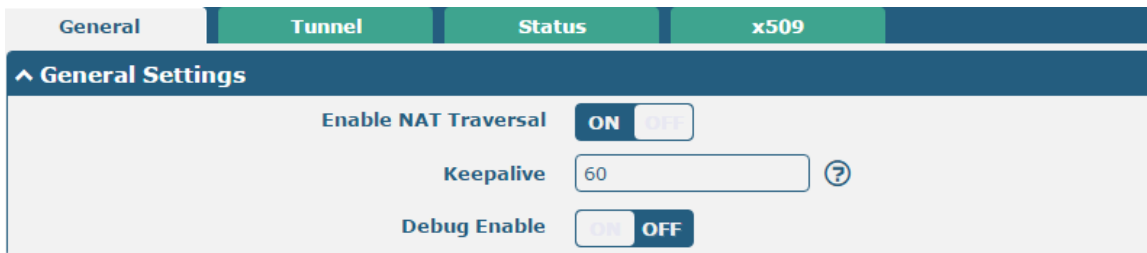


If router enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the router; and after the router dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP.

3.16 VPN > IPsec

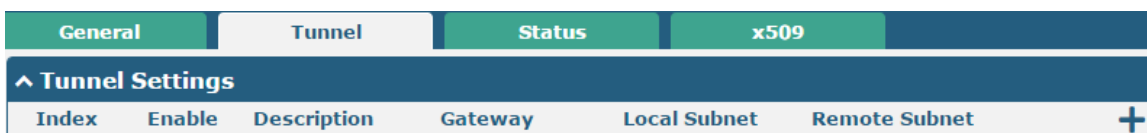
This section allows you to set the IPsec and the related parameters. Internet Protocol Security (IPsec) is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.

General



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

Tunnel



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

Tunnel

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode Tunnel v

Protocol ESP v

Local Subnet ?

Remote Subnet ?

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 of remote IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it 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 	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> ESP: Use the ESP protocol AH: Use the AH protocol 	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null

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

^ IKE Settings

Negotiation Mode	Main	v
Authentication Algorithm	MD5	v
Encryption Algorithm	3DES	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	?

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

^ IKE Settings

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

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

^ IKE Settings

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

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

^ IKE Settings

Negotiation Mode

Authentication Algorithm

Encryption Algorithm

IKE DH Group

Authentication Type

Private Key Password

Username ?

Password ?

IKE Lifetime ?

IKE Settings		
Item	Description	Default
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256” to be used in IKE negotiation. <ul style="list-style-type: none"> 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 	3DES
IKE DH Group	Select from “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. <ul style="list-style-type: none"> PSK: Pre-shared Key CA: x509 Certificate Authority xAuth: Extended Authentication to AAA server 	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. <ul style="list-style-type: none"> Default: Use an IP address as the ID in IKE negotiation FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security gateway, e.g., test@robustel.com. 	Default

IKE Settings		
Item	Description	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com. 	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

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

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

^ IKE Settings

^ SA Settings

Encryption Algorithm v

Authentication Algorithm v

PFS Group v

SA Lifetime ?

DPD Interval ?

DPD Failures ?

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

^ **General Settings**

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

v **IKE Settings**

^ **SA Settings**

Authentication Algorithm v

PFS Group v

SA Lifetime ?

DPD Interval ?

DPD Failures ?

^ **Advanced Settings**

Enable Compression ON OFF

Expert Options ?

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128" or "AES256" when you select "ESP" in "Protocol". Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA negotiation.	MD5
PFS Group	Select from "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	DHgroup 2
SA Lifetime	Set the IPsec SA lifetime. When negotiating set up IPsec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the	60

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

Status

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

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

x509

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

General	Tunnel	Status	x509
^ X509 Settings ?			
Tunnel Name		Tunnel 1 v	
Certificate Files		<input type="button" value="Choose File"/> <input type="text" value="No file chosen"/> <input type="button" value="Upload"/>	
^ Certificate Files			
Index	File Name	File Size	Modification Time

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

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

3.17 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



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

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	Client <input type="button" value="v"/>
Protocol	UDP <input type="button" value="v"/>
Server Address	<input type="text"/>
Server Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	None <input type="button" value="v"/> <input type="button" value="?"/>
Renegotiation Interval	86400 <input type="button" value="?"/>
Keepalive Interval	20 <input type="button" value="?"/>
Keepalive Timeout	120 <input type="button" value="?"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> <input type="button" value="?"/>

The window is displayed as below when choosing "P2P" as the mode.

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	P2P <input type="button" value="v"/>
Protocol	UDP <input type="button" value="v"/>
Server Address	<input type="text"/>
Server Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	None <input type="button" value="v"/> <input type="button" value="?"/>
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20 <input type="button" value="?"/>
Keepalive Timeout	120 <input type="button" value="?"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> <input type="button" value="?"/>

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Client v
Protocol	UDP v
Server Address	
Server Port	1194
Interface Type	TUN v
Authentication Type	None v ?
Renegotiation Interval	86400 ?
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 v ?

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Client v
Protocol	UDP v
Server Address	
Server Port	1194
Interface Type	TUN v
Authentication Type	Preshared v ?
Encrypt Algorithm	BF v
Renegotiation Interval	86400 ?
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="Password"/> v ?
Username	<input type="text"/>
Password	<input type="text"/>
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index

Enable ON OFF

Description

Mode

Protocol

Server Address

Server Port

Interface Type

Authentication Type

Username

Password

Encrypt Algorithm

Renegotiation Interval

Keepalive Interval

Keepalive Timeout

Private Key Password

Enable Compression ON OFF

Enable NAT ON OFF

Verbose Level

General Settings @ OpenVPN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from “P2P” or “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client” or “TCP-Server”.	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194
Interface Type	Select from “TUN” or “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN

General Settings @ OpenVPN		
Item	Description	Default
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. Note: “None” and “Preshared” authentication type are only working with P2P mode.	None
Username	Enter the username used for “Password” or “X509CA Password” authentication type.	Null
Password	Enter the password used for “Password” or “X509CA Password” authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES128”, “AES192” and “AES256”. <ul style="list-style-type: none"> BF: Use 128-bit BF encryption algorithm in CBC mode DES: Use 64-bit DES encryption algorithm in CBC mode DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode AES128: Use 128-bit AES encryption algorithm in CBC mode AES192: Use 192-bit AES encryption algorithm in CBC mode AES256: Use 256-bit AES encryption algorithm in CBC mode 	BF
Renegotiation Interval	Set the renegotiation interval. If connection failed, OpenVPN will renegotiate when the renegotiation interval reached.	86400
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Enter the private key password under the “X509CA” and “X509CA Password” authentication type.	Null
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the data stream of the header.	ON
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. <ul style="list-style-type: none"> 0: No output except fatal errors 1~4: Normal usage range 5: Output R and W characters to the console for each packet read and write 6~11: Debug info range 	0

^ **Advanced Settings**

Enable HMAC Firewall OFF

Enable PKCS#12 OFF

Enable nsCertType OFF

Expert Options ?

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

Status

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

^ **OpenVPN Tunnel Status**

Index	Description	Status	Uptime	Local IP
x509				

x509

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

^ **X509 Settings** ?

Tunnel Name v

Certificate Files +

^ **Certificate Files**

Index	File Name	File Size	Modification Time
x509			

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Certificate Files	Click on “Choose File” to locate the certificate file from your computer, and	Null

	<p>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 @client.p12</p>	
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.18 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



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



Tunnel Settings @ GRE		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the router will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null

Status

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

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

3.19 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	
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Syslog Level	Debug <input type="button" value="v"/>
Save Position	RAM <input type="button" value="v"/> <input type="button" value="?"/>
Log to Remote	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>

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

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

3.20 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.


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

this option.

Event Notification Query

^ Event Notification Group Settings

Index	Description	Send SMS	Send Email	Save to NVM	
					+

Click  button to add an Event parameters.

^ General Settings

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Send SMS	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Phone Number	<input type="text"/> ?
Send Email	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Email Addresses	<input type="text"/> ?
Save to NVM	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?

^ Event Selection ?

System Startup	<input type="checkbox"/> OFF
System Reboot	<input type="checkbox"/> OFF
System Time Update	<input type="checkbox"/> OFF
Configuration Change	<input type="checkbox"/> OFF
Cellular Network Type Change	<input type="checkbox"/> OFF
Cellular Data Stats Clear	<input type="checkbox"/> OFF
Cellular Data Traffic Overflow	<input type="checkbox"/> OFF
Poor Signal Quality	<input type="checkbox"/> OFF
Link Switching	<input type="checkbox"/> OFF
WAN Up	<input type="checkbox"/> OFF
WAN Down	<input type="checkbox"/> OFF
WLAN Up	<input type="checkbox"/> OFF
WLAN Down	<input type="checkbox"/> OFF
WWAN Up	<input type="checkbox"/> OFF
WWAN Down	<input type="checkbox"/> OFF
IPSec Connection Up	<input type="checkbox"/> OFF
IPSec Connection Down	<input type="checkbox"/> OFF
OpenVPN Connection Up	<input type="checkbox"/> OFF
OpenVPN Connection Down	<input type="checkbox"/> OFF
LAN Port Link Up	<input type="checkbox"/> OFF
LAN Port Link Down	<input type="checkbox"/> OFF
USB Device Connect	<input type="checkbox"/> OFF
USB Device Remove	<input type="checkbox"/> OFF
DDNS Update Success	<input type="checkbox"/> OFF
DDNS Update Fail	<input type="checkbox"/> OFF
Received SMS	<input type="checkbox"/> OFF
SMS Command Execute	<input type="checkbox"/> OFF

General Settings @ Notification		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.24 Services > Email", and use ';' to separate each number.	OFF
Phone Number	Enter the phone numbers used for receiving event notification. Use a semicolon (;) to separate each number.	Null
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in "3.24 Services > Email".	OFF
Email Address	Enter the email addresses used for receiving event notification. Use a space to	Null

	separate each address.	
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

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

Event
Notification
Query

^ Event Details

Save Position RAM v

Filtering

```

Mar 17 09:53:02, system startup
Mar 17 09:53:08, LAN port link down, eth1
Mar 17 09:53:08, LAN port link up, eth2
Mar 17 09:53:08, LAN port link down, eth3
Mar 17 09:53:08, LAN port link down, eth4
Mar 17 09:53:20, WWAN (cellular) up, WWAN1, ip=10.104.244.179
Mar 17 09:53:29, system time update
                    
```

Clear
Refresh

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

3.21 Services > NTP

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

NTP
Status

^ Timezone Settings

Time Zone

Expert Setting

?

^ NTP Client Settings

Enable
 ON OFF

Primary NTP Server

Secondary NTP Server

NTP Update Interval

?

^ NTP Server Settings

Enable
 ON OFF

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

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

NTP
Status

^ Time

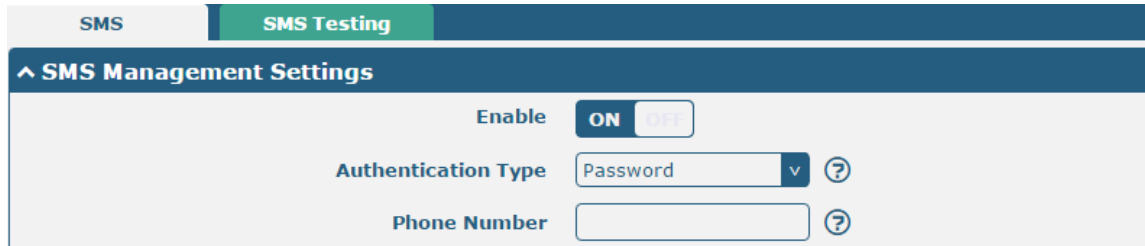
System Time
2017-03-17 11:48:00

PC Time
2017-03-17 11:49:01
Sync

Last Update Time
2017-03-17 09:53:29

3.22 Services > SMS

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



SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. Note: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum” or “Both”. <ul style="list-style-type: none"> • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; ...” Note: Set the WEB manager password in System > User Management section. • Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; ...” • Both: Use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd1; cmd2; ...” 	Password
Phone Number	Set the phone number used for SMS management, and use ‘;’ to separate each number.	Null

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

SMS

SMS Testing

^ SMS Testing

Phone Number

Message

Result

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
<input style="background-color: #004a7c; color: white; padding: 2px 10px; border: none; border-radius: 3px;" type="button" value="Send"/>	Click the button to send the test message.	--

3.23 Services > Email

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

Email

^ Email Settings

Enable ON OFF

Enable TLS/SSL ON OFF ?

Outgoing Server

Server Port

Timeout ?

Username

Password

From

Subject

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

Email Settings		
Item	Description	Default
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
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

3.24 Services > DDNS

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

The screenshot shows the 'DDNS Settings' form. At the top, there are tabs for 'DDNS' and 'Status'. Below the tabs is a header 'DDNS Settings'. The form contains an 'Enable' toggle set to 'OFF'. A red box highlights the 'Service Provider' dropdown menu, which is currently set to 'DynDNS'. Below this, there are input fields for 'Hostname', 'Username', and 'Password'.

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

The screenshot shows the 'DDNS Settings' form with the 'Service Provider' dropdown menu set to 'Custom'. A red box highlights this dropdown. Below the dropdown is an input field labeled 'URL'.

DDNS Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from "DynDNS", "NO-IP", "3322" or "Custom".	DynDNS

	Note: The DDNS service only can be used after registered by 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.

The screenshot shows a navigation bar with 'DDNS' and 'Status' tabs. Below it is a section titled '^ DDNS Status' containing a 'Status' indicator set to 'Disabled' and a 'Last Update Time' label.

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

3.25 Services > SSH

Router supports SSH password access and secret-key access.

The screenshot shows the 'SSH' settings page with a 'Keys Management' sub-tab. Under '^ SSH Settings', there are three controls: 'Enable' with a toggle set to 'ON', 'Port' with a text input field containing '22', and 'Disable Password Logins' with a toggle set to 'OFF'.

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

SSH | Keys Management

^ Import Authorized Keys

Authorized Keys No file chosen

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

3.26 Services > Telephone (Optional)

This section allows you to set the related parameters of voice function. R2000 Ent Router supports one voice input or one RS-232 or one RS-485 which is limited by the hardware on which it's installed. They shared across an RJ11 port. If your router has a voice input, this page is configurable. The R2000 Ent provides voice services via a standard RJ11 to RJ11 phone connectivity cable to make telephone calls.

Note: Whether or not voice call and data transmission can be used simultaneously is dependent upon your ISP network.

Telephone | Records

^ General Settings

Wait Number Timeout ?

Digitmap

General Settings @ Telephone		
Item	Description	Default
Wait Number Timeout	Set the wait number timeout for dial plan, measured in second.	5
Digitmap	Enter the digitmap used for matching the telephone number when making voice calls. When matched, the system will call this number immediately, and you don't need to wait for the dial-up timeout. This option is used for speed dialing.	Null

Telephone
Records

^ Call Records

Filtering

type	Phone Number	Start Time	Duration
out	15917451884	Jan 01 00:01:12	00:00:00
out	13560328286	Jan 01 00:00:50	00:00:00
out	15917451884	Mar 28 19:39:13	00:00:00
in	15917451884	Mar 28 19:42:03	00:00:00
out	15917451884	Mar 28 20:05:43	00:00:10
out	15917451884	Mar 28 20:30:48	00:00:18
out	15917451884	Mar 28 20:34:01	00:00:47
out	15917451884	Jan 01 00:02:01	00:00:00
out	15917451884	Jan 01 00:02:15	00:00:00
out	15917451884	Mar 29 09:49:00	00:00:13
in	15917451884	Mar 29 09:49:28	00:00:00

Clear
Refresh

Call Records		
Item	Description	Default
Filtering	Set the wait number timeout for dial plan, measured in second.	--
Clear	Click this button to clear the call record.	--
Refresh	Click this button to refresh the call record.	--

3.27 Services > Web Server

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

Web Server
Certificate Management

^ General Settings

HTTP Port

?

HTTPS Port

?

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

	except 80, only adding that port number then you can login router’s Web Server.	
HTTPS Port	<p>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.</p> <p>Note: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.</p>	443

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

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

3.28 Services > Advanced

This section allows you to set the Advanced and parameters.

System Settings		
Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	router
User LED Type	<p>Specify the display type of your USR LED. Select from “None”, “SIM”, “OpenVPN”, “IPSec” or “WiFi”.</p> <ul style="list-style-type: none"> None: Meaningless indication, and the LED is off SIM: USR indicator showing the SIM status OpenVPN: USR indicator showing the OpenVPN status IPSec: USR indicator showing the IPsec status WiFi: USR indicator showing the WiFi status <p>Note: For more details about USR indicator, see “2.1 LED Indicators”.</p>	None

System
Reboot

^ **Periodic Reboot Settings**

Periodic Reboot

?

Daily Reboot Time

?

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

3.29 System > Debug

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

Syslog
^ Syslog Details

Log Level

Filtering ?

```

Mar 17 11:46:15 router user.debug modemd[903]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A19807CBE54C163A883508F0A21806C83901A884C8BC18FO
A35804FEB6C11670D52A18F0C3680624B673A84254E1A53858F0A60806D4191CF4E13533A8F0A6280727960E0793C5305"
Mar 17 11:48:04 router user.debug link_manager[874]: WWAN2 (wwan2) init timeout
Mar 17 11:48:04 router user.debug link_manager[874]: rcv action disconnected from link_manager
Mar 17 11:48:04 router user.debug link_manager[874]: target link WWAN2, state Disconnected
Mar 17 11:48:04 router user.notice link_manager[874]: WWAN2 disconnected
Mar 17 11:48:04 router user.info link_manager[874]: there is no need to switch link (WWAN1:00 - WWAN2:30)
Mar 17 11:48:14 router user.debug modemd[903]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A19807CBE54C163A883508F0A21806C83901A884C8BC18FO
A35804FEB6C11670D52A18F0C3680624B673A84254E1A53858F0A60806D4191CF4E13533A8F0A6280727960E0793C5305"
Mar 17 11:48:40 router user.debug link_manager[874]: WWAN1 (wwan1) start ping test
Mar 17 11:48:40 router user.debug rping[12160]: start ping 8.8.8.8 (wwan1)
Mar 17 11:48:40 router user.debug rping[12160]: PING 8.8.8.8 (8.8.8.8) from 10.104.244.179: 16 data bytes
Mar 17 11:48:40 router user.debug rping[12160]: 24 bytes from 8.8.8.8: seq=0 ttl=52 time=375.349 ms
Mar 17 11:48:40 router user.debug rping[12160]:
Mar 17 11:48:40 router user.debug rping[12160]: --- 8.8.8.8 ping statistics ---
Mar 17 11:48:40 router user.debug rping[12160]: 1 packets transmitted, 1 packets received, 0% packet loss
Mar 17 11:48:40 router user.debug rping[12160]: round-trip min/avg/max = 375.349/375.349/375.349 ms
Mar 17 11:48:40 router user.debug link_manager[874]: rcv action ping_success from rping
Mar 17 11:48:40 router user.debug link_manager[874]: target link WWAN1, state Connected
Mar 17 11:48:40 router user.info link_manager[874]: WWAN1 ping test success
Mar 17 11:50:13 router user.debug modemd[903]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A19807CBE54C163A883508F0A21806C83901A884C8BC18FO
A35804FEB6C11670D52A18F0C3680624B673A84254E1A53858F0A60806D4191CF4E13533A8F0A6280727960E0793C5305"
                    
```

Manual Refresh
Clear
Refresh

^ Syslog Files

Index	File Name	File Size	Modification Time
1	messages	53532	Fri Mar 17 11:50:13 2017

^ System Diagnostic Data

System Diagnostic Data Generate

System Diagnostic Data Download

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

RT_UG_R2000 Ent_v.1.0.5
Confidential

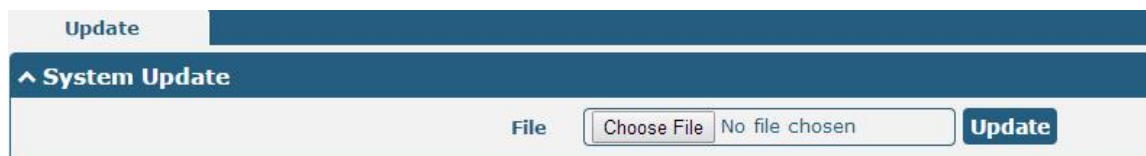
17 Sep., 2019

102/134

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 system diagnosing file.	--

3.30 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.

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

3.31 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.

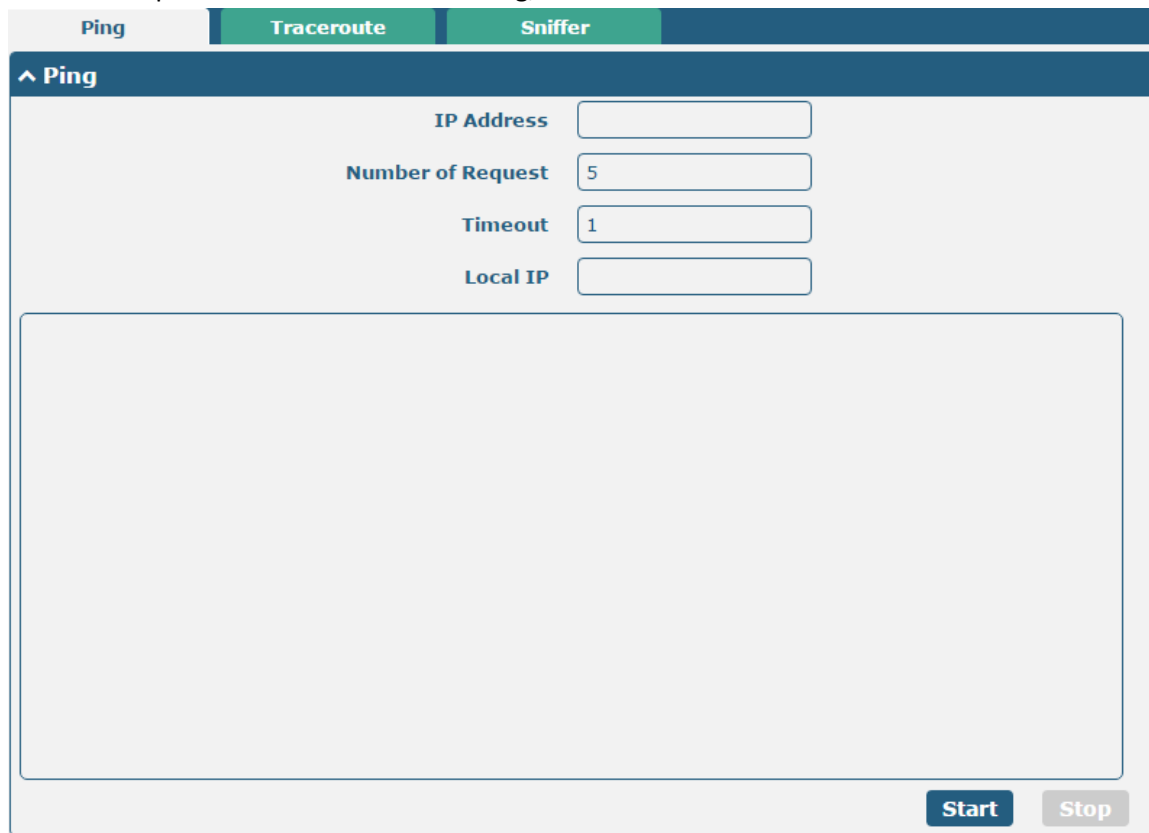
Note: After importing the applications to the router, the page display may have a slight delay due to the browser cache. It is recommended that you clear the browser cache first and log in the router again.





App Center		
Item	Description	Default
App Install		
File	Click on “Choose File” to locate the App file from your computer, and then click Install to import this file into your router. Note: File format should be xxx.rpk, e.g. R2000 Ent-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

3.32 System > Tools

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

Ping | Traceroute | Sniffer

Traceroute

Trace Address
 Trace Hops
 Trace Timeout

Start Stop

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

Ping | Traceroute | Sniffer

Sniffer

Interface v
 Host
 Packets Request
 Protocol v
 Status

Start Stop

Capture Files

Index	File Name	File Size	Modification Time
1	17-03-17_11-53-50.cap	24	Fri Mar 17 11:53:51 2017

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
	Click this button to start the sniffer.	--
	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click to download the log, click to delete the log file. It can cache a maximum of 5 files.	Null

3.33 System > Profile

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

Profile

Rollback

Import Configuration File

Reset Other Settings to Default OFF

Ignore Invalid Settings OFF

XML Configuration File No file chosen

Export Configuration File

Ignore Disabled Features OFF

Add Detailed Information OFF

Encrypt Secret Data OFF

XML Configuration File

XML Configuration File

Default Configuration

Save Running Configuration as Default

Restore to Default Configuration

Profile		
Item	Description	Default
Import Configuration File		
Reset Other Settings to Default	Click the toggle button as "ON" to return other parameters to default settings.	OFF

Ignore Invalid Settings	Click the toggle button as “OFF” to ignore invalid settings.	OFF
XML Configuration File	Click on 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, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click this button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click this button to restore the factory defaults.	--

Profile

Rollback

^ Configuration Rollback

Save as a Rollbackable Archive
Save
?

^ Configuration Archive Files

Index	File Name	File Size	Modification Time	
1	config1.tgz	2783	Fri Jan 1 00:00:09 2016	↺
2	config2.tgz	2760	Fri Jan 1 00:00:09 2016	↺
3	config3.tgz	2729	Fri Jan 1 00:00:09 2016	↺
4	config4.tgz	29	Fri Jan 1 00:00:09 2016	↺

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

3.34 System > User Management

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

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

Super User

Common User

^ Super User Settings

New Username

?

Old Password

?

New Password

?

Confirm Password

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

Super User

Common User

^ Common User Settings

Index	Role	Username	+

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

Common User

^ Common Users Settings

Index

Role

Visitor v

Username

?

Password

?

Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from "Visitor" and "Editor".	Visitor

	<ul style="list-style-type: none">• 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, 0-9, @, ., -, #, \$, and *.	Null

Chapter 4 Configuration Examples

4.1 Cellular

4.1.1 Cellular Dial-Up

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

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

The screenshot shows the 'Link Manager' interface with the 'Status' tab selected. It is divided into two main sections: 'General Settings' and 'Link Settings'.

General Settings:

- Primary Link: WWAN1
- Backup Link: WWAN2
- Backup Mode: Warm Backup
- Emergency Reboot: OFF

Link Settings:

Index	Type	Description	Connection Type	
1	WWAN1		DHCP	
2	WWAN2		DHCP	
3	WAN		DHCP	
4	WLAN		DHCP	

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

The screenshot shows the 'Link Manager' interface with the 'General Settings' tab selected for the WWAN1 link.

General Settings:

- Index: 1
- Type: WWAN1
- Description: (empty field)

^ WWAN Settings

Automatic APN Selection ON OFF

Dialup Number

Authentication Type v

Switch SIM By Data Allowance ON OFF ?

Data Allowance ?

Billing Day ?

^ Ping Detection Settings ?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF

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

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

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

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

Cellular

^ **General Settings**

Index	<input type="text" value="1"/>
SIM Card	<input style="border-bottom: 1px solid #ccc;" type="text" value="SIM1"/> v
Phone Number	<input type="text"/>
PIN Code	<input type="text"/> ?
Extra AT Cmd	<input type="text"/> ?
Telnet Port	<input type="text" value="0"/> ?

^ **Cellular Network Settings**

Network Type	<input style="border-bottom: 1px solid #ccc;" type="text" value="Auto"/> v ?
Band Select Type	<input style="border-bottom: 1px solid #ccc;" type="text" value="All"/> v ?

^ **Advanced Settings**

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

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

4.1.2 SMS Remote Control

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

An SMS command has the following structure:

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

SMS command Explanation:

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

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

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

Profile	Rollback
^ Import Configuration File	
Reset Other Settings to Default	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Ignore Invalid Settings	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
XML Configuration File	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Import"/>
^ Export Configuration File	
Ignore Disabled Features	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Add Detailed Information	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Encrypt Secret Data	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
XML Configuration File	<input type="button" value="Generate"/>
^ Default Configuration	
Save Running Configuration as Default	<input type="button" value="Save"/> ?
Restore to Default Configuration	<input type="button" value="Restore"/>

XML command:

```
<lan >
<network max_entry_num="2" >
<id > 1</id >
<interface > lan0</interface >
<ip > 172.16.99.44</ip >
<netmask > 255.255.0.0</netmask >
<mtu > 1500</mtu >
```

SMS cmd:

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.99.44
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500
```

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

admin:admin;status system

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

SMS received:

```
hardware_version = 1.1
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000 Ent
serial_number = 11002217030001
uptime = "0 days, 00:01:45"
system_time = "Mon Mar 13 16:36:33 2017"
```

admin:admin;reboot

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

SMS received:

OK

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is “admin”, password is “admin”, and the command is to disable the remote_ssh and remote_telnet access.

SMS received:

OK

OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.44;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

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

SMS received:

OK

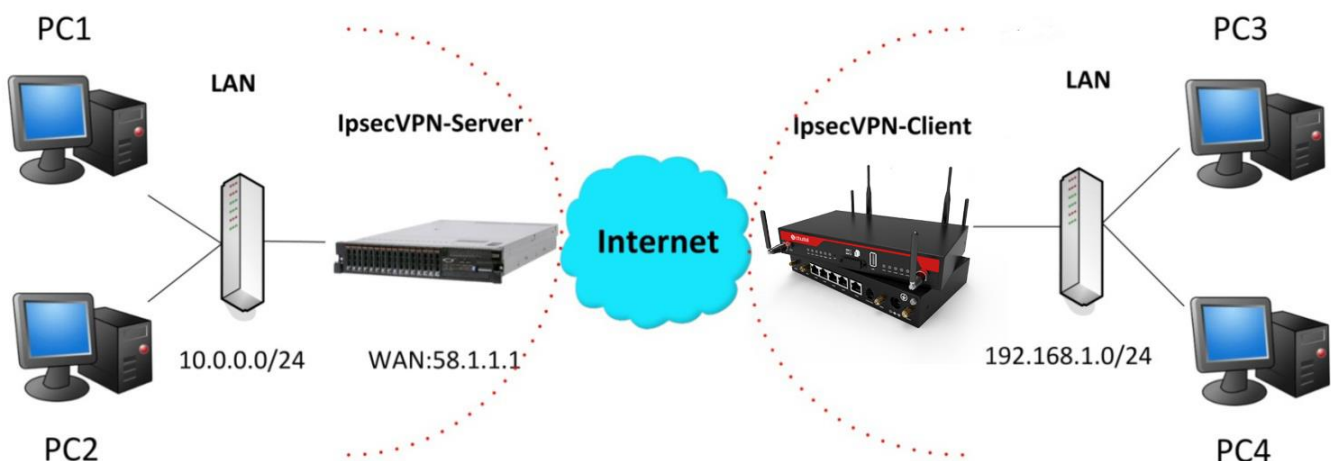
OK

OK

OK

4.2 Network

4.2.1 IPsec VPN



The configuration of server and client is as follows.

IPsec VPN_Server:

Cisco 2811:

```

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

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

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

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

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

```

IPsec VPN_Client:

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

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

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

Tunnel

^ General Settings

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

^ IKE Settings

Negotiation Mode v

Authentication Algorithm v

Encryption Algorithm v

IKE DH Group v

Authentication Type v

PSK Secret

Local ID Type v

Remote ID Type v

IKE Lifetime ?

^ SA Settings

Encrypt Algorithm	<input type="text" value="3DES"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
PFS Group	<input type="text" value="DHgroup2"/>	v	
SA Lifetime	<input type="text" value="28800"/>	?	
DPD Interval	<input type="text" value="60"/>	?	
DPD Failures	<input type="text" value="180"/>	?	

^ Advanced Settings

Enable Compression	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
Expert Options	<input type="text"/>	?	

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

The comparison between server and client is as below.

```

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

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

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

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

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

Server (Cisco 2811)

Client (R2000 Ent)

^ Tunnel Settings

Index	<input type="text" value="1"/>		
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF		
Description	<input type="text"/>		
Gateway	<input type="text" value="58.1.1.1"/>	?	
Mode	<input type="text" value="Tunnel"/>	v	
Protocol	<input type="text" value="ESP"/>	v	
Local Subnet	<input type="text" value="192.168.1.0"/>	?	
Remote Subnet	<input type="text" value="255.255.255.0"/>	?	

^ IKE Settings

Negotiation Mode	<input type="text" value="Main"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
Encrypt Algorithm	<input type="text" value="3DES"/>	v	
IKE DH Group	<input type="text" value="MODP(1024)"/>	v	
Authentication Type	<input type="text" value="PSK"/>	v	
PSK Secret	<input type="text" value="*****"/>		
Local ID Type	<input type="text" value="Default"/>	v	
Remote ID Type	<input type="text" value="Default"/>	v	
IKE Lifetime	<input type="text" value="86400"/>	?	

^ SA Settings

Encrypt Algorithm	<input type="text" value="3DES"/>	v	
Authentication Algorithm	<input type="text" value="MD5"/>	v	
PFS Group	<input type="text" value="MODP(1024)"/>	v	
SA Lifetime	<input type="text" value="28800"/>	?	
DPD Interval	<input type="text" value="60"/>	?	
DPD Failures	<input type="text" value="180"/>	?	

^ Advanced Settings

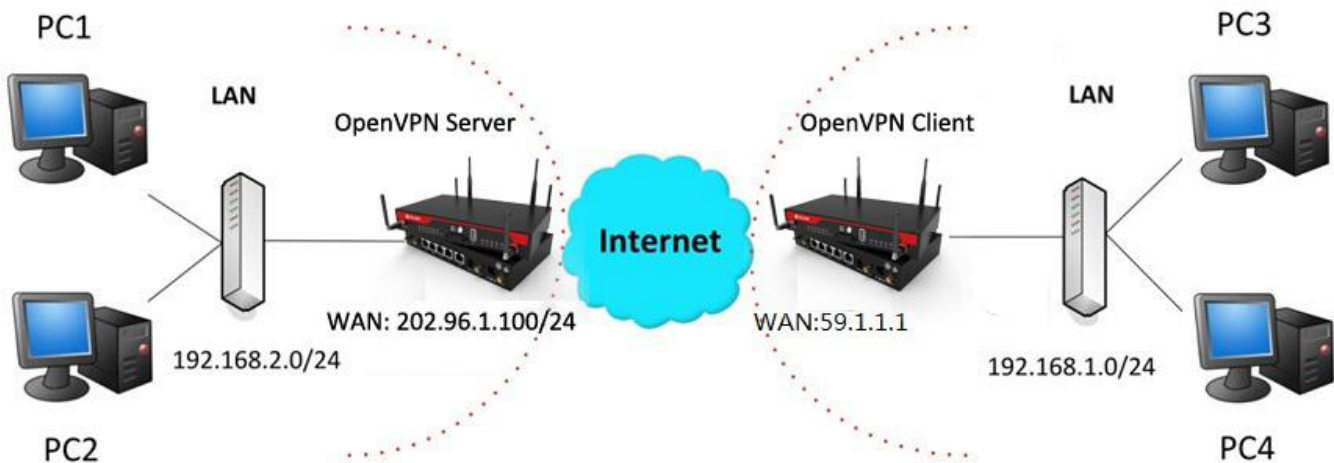
Enable Compression	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
--------------------	---------------------------------------------------------------------	--	--

IKE Setting in Client must be consistent with server.

SA Setting in Client must be consistent with server.

4.2.2 OpenVPN

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



OpenVPN_Server:

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

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

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

OpenVPN_Client:

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

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

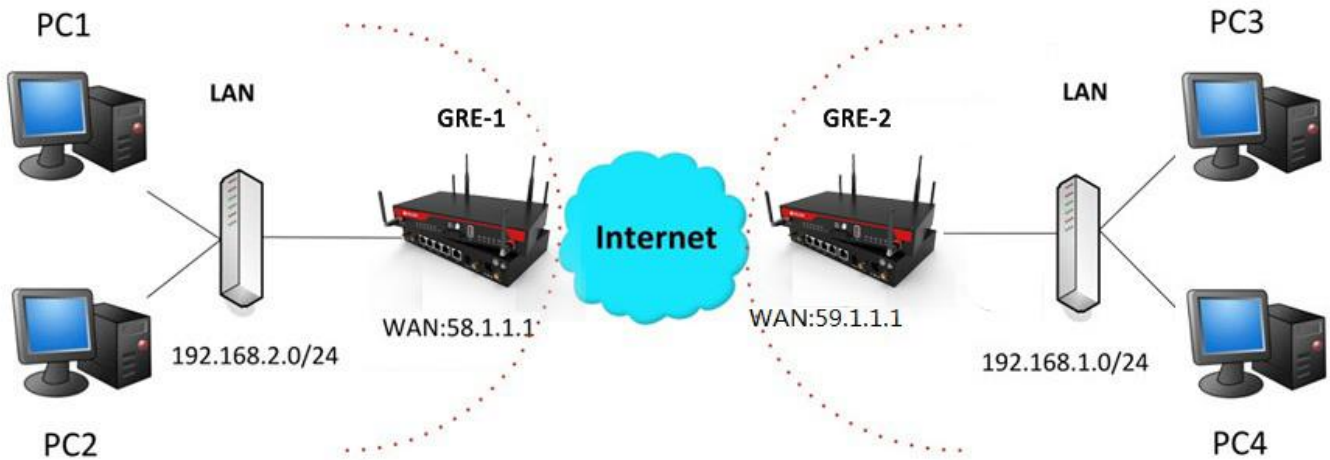
Click **+** to configure the Client01 as below.

^ General Settings	
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="Client01"/>
Mode	<input type="text" value="Client"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text" value="202.96.1.100"/>
Server Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Private Key Password	<input type="password" value="•••••"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Level	<input type="text" value="3"/> v ?

^ Advanced Settings	
Enable HMAC Firewall	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable PKCS#12	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable nsCertType	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Expert Options	<input type="text" value="fragment 1500"/> ?

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

4.2.3 GRE VPN



The configuration of two points is as follows.

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

GRE			
Status			
^ Tunnel Settings			
Index	Enable	Description	Remote IP Address
			+

GRE-1:

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

^ Tunnel Settings	
Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	GRE-1
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Remote Virtual IP Address	10.8.0.2
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	*****

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

GRE-2:

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

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

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

GRE-1	GRE-2
Remote IP Address: 59.1.1.1 (GRE-1 public IP)	Remote IP Address: 58.1.1.1 (GRE-2 public IP)
Local Virtual IP Address: 10.8.0.1 (GRE-1 tunnel IP)	Local Virtual IP Address: 10.8.0.2 (GRE-2 tunnel IP)
Remote Virtual IP Address: 10.8.0.2 (GRE-2 tunnel IP)	Remote Virtual IP Address: 10.8.0.1 (GRE-1 tunnel IP)
Enable NAT: OFF (set the same secret as GRE-2)	Enable NAT: OFF (set the same secret as GRE-1)
Secrets: *****	Secrets: *****

Chapter 5 Introductions for CLI

5.1 What Is CLI

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

Route login:

Router login: admin

Password: admin

#

CLI commands:

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

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

5.2 How to Configure the CLI

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

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

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 = 1.1
firmware_version = "3.0.0"
kernel_version = 3.10.49
device_model = R2000 Ent
serial_number = 11002217030001
uptime = "0 days, 00:01:45"
system_time = "Mon Mar 13 16:36:33 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware    New firmware
# tftpupdate firmware (space+?)
  String    Firmware name
# tftpupdate firmware R2000 Ent-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
```

Downloading

R2000 Ent-firmware-s 100% |*****| 5018k 0:00:00 ETA

Flashing

Checking 100%

Decrypting 100%

Flashing 100%

Verifying 100%

Verify Success

upgrade success //update success

config save_and_apply

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

Example 3: Set link-manager

set

set

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

```

# set link_manager primary_link (space+?)
Enum   Primary Link (wwan1/wwan2/wan)
# set link_manager primary_link wwan1           //select "wwan1" as primary_link
OK                                             //setting succeed
# set link_manager link 1
  type          Type
  desc          Description
  connection_type Connection Type
  wwan          WWAN Settings
  static_addr   Static Address Settings
  pppoe         PPPoE Settings
  ping         Ping Settings
  mtu          MTU
  dns1_overridden Overridden Primary DNS
  dns2_overridden Overridden Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
  auto_apn      Automatic APN Selection
  apn           APN
  username      Username
  password      Password
  dialup_number Dialup Number
  auth_type     Authentication Type
  switch_by_data_allowance Switch SIM By Data Allowance
  data_allowance Data Allowance
  billing_day   Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100           //open cellular switch_by_data_traffic
OK                                                         //setting succeed
# set link_manager link 1 wwan billing_day 1               //setting specifies the day of month for billing
OK                                                         // setting succeed
...
# config save_and_apply
OK                                                         // save and apply current configuration, make you configuration effect

```

Example 4: Set LAN IP address

```

# 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 = 172.16.99.44
    netmask = 255.255.0.0
}
#
# set lan
network      Network Settings
multi_ip     Multiple IP Address Settings
vlan         VLAN
# set lan network 1(space+?)
interface    Interface
ip           IP Address
netmask      Netmask
mtu          MTU
dhcp         DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.44           //set IP address for lan
OK                                           //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                           // save and apply current configuration, make you configuration effect
```

Example 5: CLI for setting Cellular

```
# show cellular all
sim {
    id = 1
    card = sim1
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
    band_wcdma_1900 = false
    band_wcdma_2100 = false
    band_lte_800 = false
    band_lte_850 = false
    band_lte_900 = false
    band_lte_1800 = false
    band_lte_1900 = false
    band_lte_2100 = false
    band_lte_2600 = false
    band_lte_1700 = false
    band_lte_700 = false
    band_tdd_lte_2600 = false
    band_tdd_lte_1900 = false
    band_tdd_lte_2300 = false
    band_tdd_lte_2500 = false
}
sim {
    id = 2
    card = sim2
    phone_number = ""
    extra_at_cmd = ""
    network_type = auto
    band_select_type = all
    band_gsm_850 = false
    band_gsm_900 = false
    band_gsm_1800 = false
    band_gsm_1900 = false
    band_wcdma_850 = false
    band_wcdma_900 = false
```



```

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

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

# set cellular sim 1(space+?)
  card                SIM Card
  phone_number        Phone Number
  extra_at_cmd        Extra AT Cmd
  network_type        Network Type
  band_select_type    Band Select Type
  band_gsm_850        GSM 850
  band_gsm_900        GSM 900
  band_gsm_1800       GSM 1800
  band_gsm_1900       GSM 1900
  band_wcdma_850      WCDMA 850
  band_wcdma_900      WCDMA 900
  band_wcdma_1900     WCDMA 1900
  band_wcdma_2100     WCDMA 2100
  band_lte_800        LTE 800 (band 20)
  band_lte_850        LTE 850 (band 5)
  band_lte_900        LTE 900 (band 8)
  band_lte_1800       LTE 1800 (band 3)

```

```

band_lte_1900      LTE 1900 (band 2)
band_lte_2100      LTE 2100 (band 1)
band_lte_2600      LTE 2600 (band 7)
band_lte_1700      LTE 1700 (band 4)
band_lte_700       LTE 700 (band 17)
band_tdd_lte_2600  TDD LTE 2600 (band 38)
band_tdd_lte_1900  TDD LTE 1900 (band 39)
band_tdd_lte_2300  TDD LTE 2300 (band 40)
band_tdd_lte_2500  TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
...
# config save_and_apply
OK                                     // save and apply current configuration, make you configuration effect

```

5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug <i>parameters</i>	Turn on or turn off debug function
Show	Show <i>parameters</i>	Show current configuration of each function.
Set	Set <i>parameters</i>	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add <i>parameters</i>	

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

Glossary

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

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

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

Guangzhou Robustel LTD

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

Web: www.robustel.com

Email: info@robustel.com

Tel: 86-20-29019902