



User Guide

R1520

Industrial Dual SIM Cellular VPN Router



robustOS

Guangzhou Robustel LTD
www.robustel.com

Please note: R1520 is the general name of series products, and the model of this device is R1520-4L Global.


About This Document

This document provides hardware and software information of the Robustel High-speed intelligent LTE router R1520, including introduction, installation, configuration and operation.

Copyright©2020 Guangzhou Robustel LTD

All rights reserved.

Trademarks and Permissions

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

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

Name of the Part	Hazardous Substances									
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)	(DEHP)	(BBP)	(DBP)	(DIBP)
Metal parts	o	o	o	o	—	—	—	—	—	—
Circuit modules	o	o	o	o	o	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o	o	o	o	o
<p>o: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in RoHS2.0.</p> <p>X: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part <i>might exceed</i> the limit requirement in RoHS2.0.</p> <p>—: Indicates that it does not contain the toxic or hazardous substance.</p>										

Document History

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

Date	Firmware Version	Document Version	Change Description
Jun. 11, 2020	3.1.0	v 1.0.0	Initial release

Contents

Chapter 1	Product Overview	10
1.1	Introduction.....	10
1.2	Package Contents	10
1.3	Specifications	13
1.4	Dimensions.....	14
Chapter 2	Hardware Installation.....	15
2.1	Definition of Power Interface	15
2.2	Interface Definition of 2 * 3 3.5mm	15
2.3	Interface Definition of 2 * 4 3.5mm	16
2.4	LED indicator	17
2.5	USB Interface.....	18
2.6	Reset Button.....	19
2.7	Ethernet Ports	19
2.8	Insert or Remove SIM Card	20
3.2	Attach External Antenna (SMA Type)	21
3.3	Mount the Router	22
3.4	Connect the Router to a Computer.....	24
3.5	Power Supply.....	24
3.6	DI/DO Interface	25
3.7	AI Interface	26
Chapter 3	Initial Configuration	27
3.1	Configure the PC.....	27
3.2	Factory Default Settings	30
3.3	Log in the Router	30
3.4	Control Panel	31
Chapter 4	Router Configuration.....	33
4.1	Status.....	33
4.1.1	System Information	33
4.1.2	Internet Status	34
4.1.3	LAN Status.....	34
4.2	Interface	35
4.2.1	Link Manager	35
4.2.2	LAN	46
4.2.3	Ethernet	50
4.2.4	Cellular	51
4.2.5	WiFi.....	57
4.2.6	USB	65
4.2.7	DI/DO	66
4.2.8	AI.....	70
4.2.9	Serial Port	72
4.3	Network.....	77
4.3.1	Route	77
4.3.2	Firewall	79
4.3.3	IP Passthrough	84

4.4	VPN.....	85
4.4.1	IPsec.....	85
4.4.2	OpenVPN	93
4.4.3	GRE	106
4.5	Services	107
4.5.1	Syslog.....	107
4.5.2	Event.....	108
4.5.3	NTP	112
4.5.4	SMS.....	113
4.5.5	Email.....	114
4.5.6	DDNS.....	115
4.5.7	SSH.....	117
4.5.8	GPS (Optional)	117
4.5.9	Web Server	123
4.5.10	Advanced	124
4.6	System	125
4.6.1	Debug.....	125
4.6.2	Update	126
4.6.3	App Center.....	126
4.6.4	Tools.....	127
4.6.5	Profile.....	130
4.6.6	User Management	132
Chapter 5	Configuration Examples.....	134
5.1	Cellular	134
5.1.1	Cellular Dial-Up.....	134
5.1.2	SMS Remote Control.....	136
5.2	VPN Configuration Example	138
5.2.1	IPsec VPN	138
5.2.2	OpenVPN	142
5.2.3	GRE VPN.....	144
Chapter 6	Introductions for CLI.....	146
6.1	What Is CLI.....	146
6.2	How to Configure the CLI	148
6.3	Commands Reference	148
6.4	Quick Start with Configuration ExampleS	149
Glossary.....		156

Chapter 1 Product Overview

1.1 Introduction

The Robustel industrial dual SIM cellular VPN router (R1520) is a rugged cellular router can support 2G, 3G, and 4G LTE Cat 4 networks. It provides high-speed wireless network bandwidth for devices through wireless connections to ensure stable wireless network connections.

R1520 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 customized user experience, which is more diverse, convenient, and practical. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C. It also provides rich Apps to meet fragmented IoT market demands.

1.2 Package Contents

Before installing your R1520 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 R1520 High-speed intelligent LTE router



- 1 x 2-pin 3.5 mm male terminal block with lock for power supply



- 1 x 2*4-pin 3.5 mm male terminal block for serial port



- 1 x 2*3-pin 3.5 mm male terminal block for DI/DO/AI interface



- 1 x SMA-J cellular antenna (rubber antenna)



- 1 x RP-SMA-J WiFi antenna (rubber antenna)



- Ethernet cable



- 1 x SIM Card Sticker



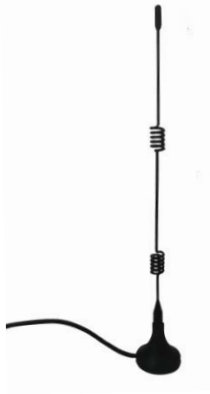
Optional Accessories (sold separately)

- SMA-J cellular antenna (rubber antenna or Magnet antenna is optional)

rubber antenna
Magnet antenna



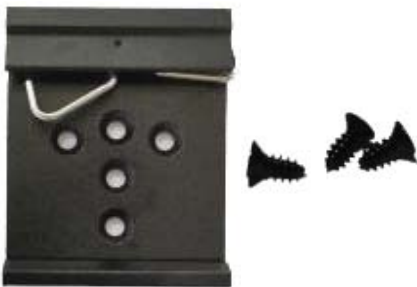
- RP-SMA-J WiFi antenna (rubber antenna or Magnet antenna is optional)
rubber antenna Magnet antenna



- SMA-J GPS antenna (Magnetic or adhesive is optional)



- 35 mm DIN Rail mounting kit



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



1.3 Specifications

Cellular Interface

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA-K
- SIM: 2 , Standard SIM or eSIM
- Standards: FDD LTE/TDD LTE, backward compatible to 2G/3G

Ethernet Interface

- Number of ports: 5 x 10/100 Mbps (It can be configured as 5x LAN or 4 x LAN + 1 x WAN)
- ETH0 port: supports 802.3at PD function
- Magnet isolation protection: 1.5 KV

WiFi Interface

- Number of antennas: 2 (WiFi1 + WiFi2)
- Connector: RP-SMA-K
- Standards: 802.11b/g/n, 2*2 MIMO, supports AP and Client modes
- Frequency bands: 2.4GHz
- Security: Open、WPA、WPA2、WEP
- Encryption: AES、TKIP、WEP64
- Data speed: Maximum rate is 300 Mbps

GPS Interface (Optional, depending on the cellular module)

- Number of antennas: 1
- Connector: SMA-K, 50 ohm characteristic impedance
- Positioning technology: GPS, QZSS, GLONASS, Galileo, BeiDou

Serial Interface

- Number of ports: 1 x RS-232 and 1 x RS-485
- Connector: 2 *4-pin 3.5 mm female socket
- ESD protection: ± 8 KV Air
- RS-232: Tx/D, Rx/D, RTS, CTS, SGND
- RS-485: Data+ (A), Data- (B)

DI/DO

- Type: 1 x DI (wet contact) + 1 x DO (wet contact)
- Connector: 2*3-pin 3.5 mm female socket
- Isolation: 3KVDC
- Absolute maximum : "V+" + 30 V DC (DI, 30 V DC (DO)
- Maximum input current of DI: 10 mA
- Maximum input current of DO: 100 mA

Analog Input

- Type: 1 x AI
- Connector: 2*3-pin 3.5 mm female socket(Shared with DI / DO)

- Measuring range: 4 ~ 20mA / 0 ~ 24V

Others

- 1 x Reset button (Tact Switch)
- 1 x 480 Mbps high-speed USB 2.0 interface (host mode), Type A, 5V / 500 mA
- LED indicators - 1 x RUN, 1 x Modem, 1 x USR, 1 x WiFi, 1 x RSSI

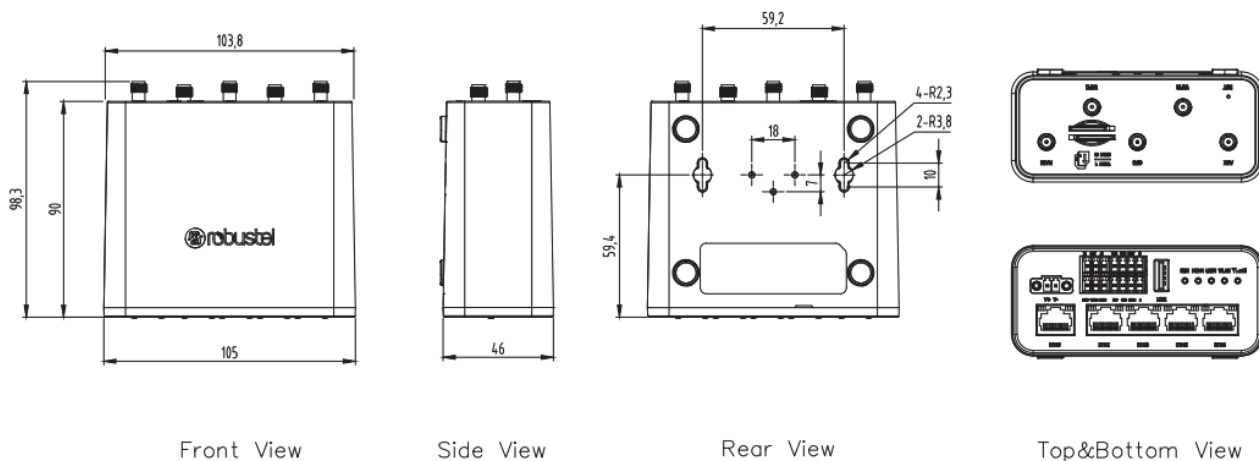
Power Supply and Consumption

- Connector: 2-pin 3.5 mm female socket with lock
- Input voltage: 9 to 36V DC
- Power consumption: Idle: 100 mA@12 V;
Data link: 1000 mA (peak) @12 V

Physical Characteristics

- Ingress protection: IP30
- Housing & Weight: Plastic, 250 g
- Dimensions: 105mm (length) x 90mm(width) x 46mm(thickness)
- Installations: Desktop, wall mounting or DIN rail mounting (Wall mounting and Din rail mounting installation requires additional installation accessories)
- Operating Temperature: -25~+70 °C
- Storage Temperature: -40~+85 °C
- Relative Humidity: 5~95% RH

1.4 Dimensions



Chapter 2 Hardware Installation

2.1 Definition of Power Interface



PIN	Description	Note
1	V+	Positive
2	V-	Negative

2.2 Interface Definition of 2 * 3 3.5mm



PIN	DI	DO	AI	Note
1	IN		--	Digital input positive
2	--	OUT	--	Digital output positive
3	--	--	AI	Analog input
4	IGND	--	--	Digital input negative
5	--	OGND	--	Digital output negative
6	--	--	AGND	Analog input signal ground

2.3 Interface Definition of 2 * 4 3.5mm



PIN	RS-232	RS-485	Note
1	TXD	--	Router → Device
2	RTS	--	Router → Device
3	--	GND	RS485 signal ground
4		B	RS485 Data+ (B)
5	RXD	--	Router ← Device
6	CTS	--	Router ← Device
7	SGND	--	RS232 signal ground
8	--	A	RS485 Data+ (A)

2.4 LED indicator

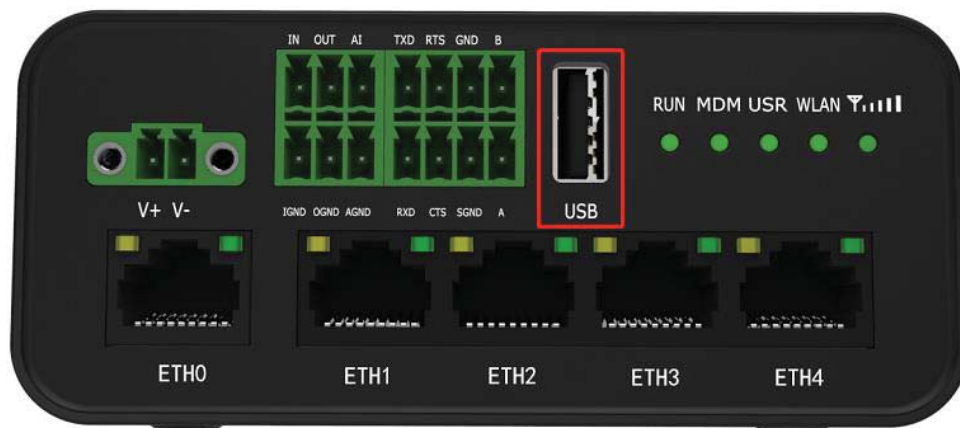


Name		Color	Status	Description
RUN		Green	On, solid	Router is powered on (System is initializing)
			On, blinking	Router starts operating
			Off	Router is powered off
MDM		Green	On, solid	Link connection is working
			On, blinking	Data is sent and received.
			Off	Link connection is not working
USR	USR-OpenVPN	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
RSSI		Green	On, solid	Signal level: Best signal level Wireless module : 21-31 dB (High Signal strength)
		Green	On, blinking	Signal level: Average signal level Wireless module : 11-20 dB (Medium Signal strength)
		Green	Off	Signal level: Abnormal signal level Wireless module : 1-10 dB (Low Signal strength)
		Green	Off	No signal
WLAN		Green	On, solid	WiFi is enabled and working properly
		Green	Off	WiFi is disabled or not working properly

Note: 1. click Services > Advanced > system > System Settings > Custom LED Indicator type to set the display type of USR LED.

2. When the LEDs start blinking one by one, the WLAN indicator will not turn on and off.

2.5 USB Interface



Function	Operation
Firmware upgrade	The USB interface can be used for batch firmware upgrades, but it cannot send or receive data with slave devices connected to the USB interface. The user can insert a USB storage device, such as a U disk or a hard disk, at the USB interface. If there is a configuration file or router firmware in the USB storage device, the router will automatically update the configuration file or firmware. For details, please refer to "4.2.6 USB".

2.6 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 0~20 seconds after powering up the router, press and hold the RST button with a pointed bar until all five LEDs start blinking one by one, and release the button to return the router to factory defaults.

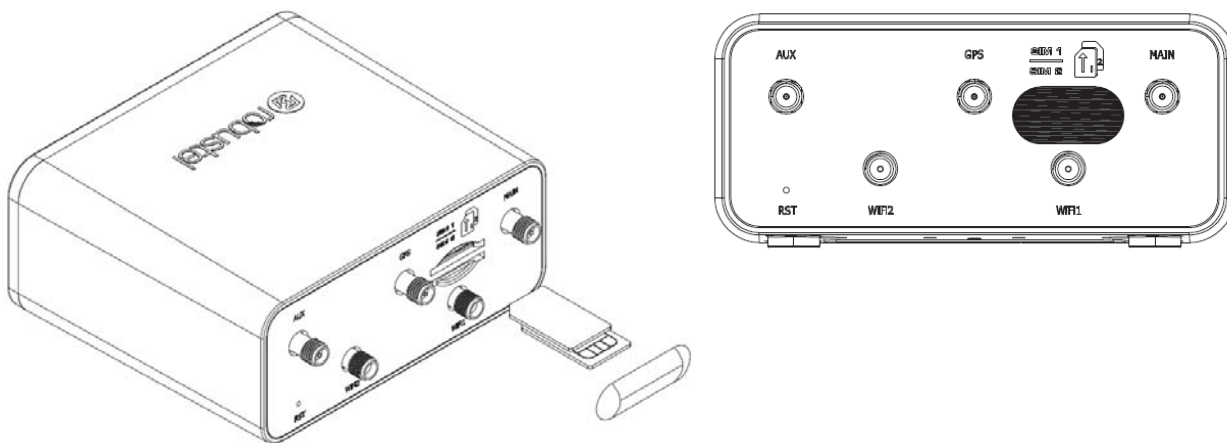
2.7 Ethernet Ports



There are five Ethernet ports on R1520, including ETH0 (POE), ETH1, ETH2, ETH3 and ETH4. Each has two LED indicators. The green one is a link indicator but the yellow one doesn't mean anything. For details about status, see the table below.

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

2.8 Insert or Remove SIM Card



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

- **Insert SIM card**

1. Make sure router is powered off.
2. To insert SIM card, press the card with finger until you hear a click.
3. After the SIM card is inserted, attach the SIM card sticker to the card slot.

- **Remove SIM card**

1. Make sure router is powered off.
2. Tear the SIM card sticker from the slot.
3. To remove SIM card, press the SIM card with finger until you hear a click and it pops out and then take out the card.

Note:

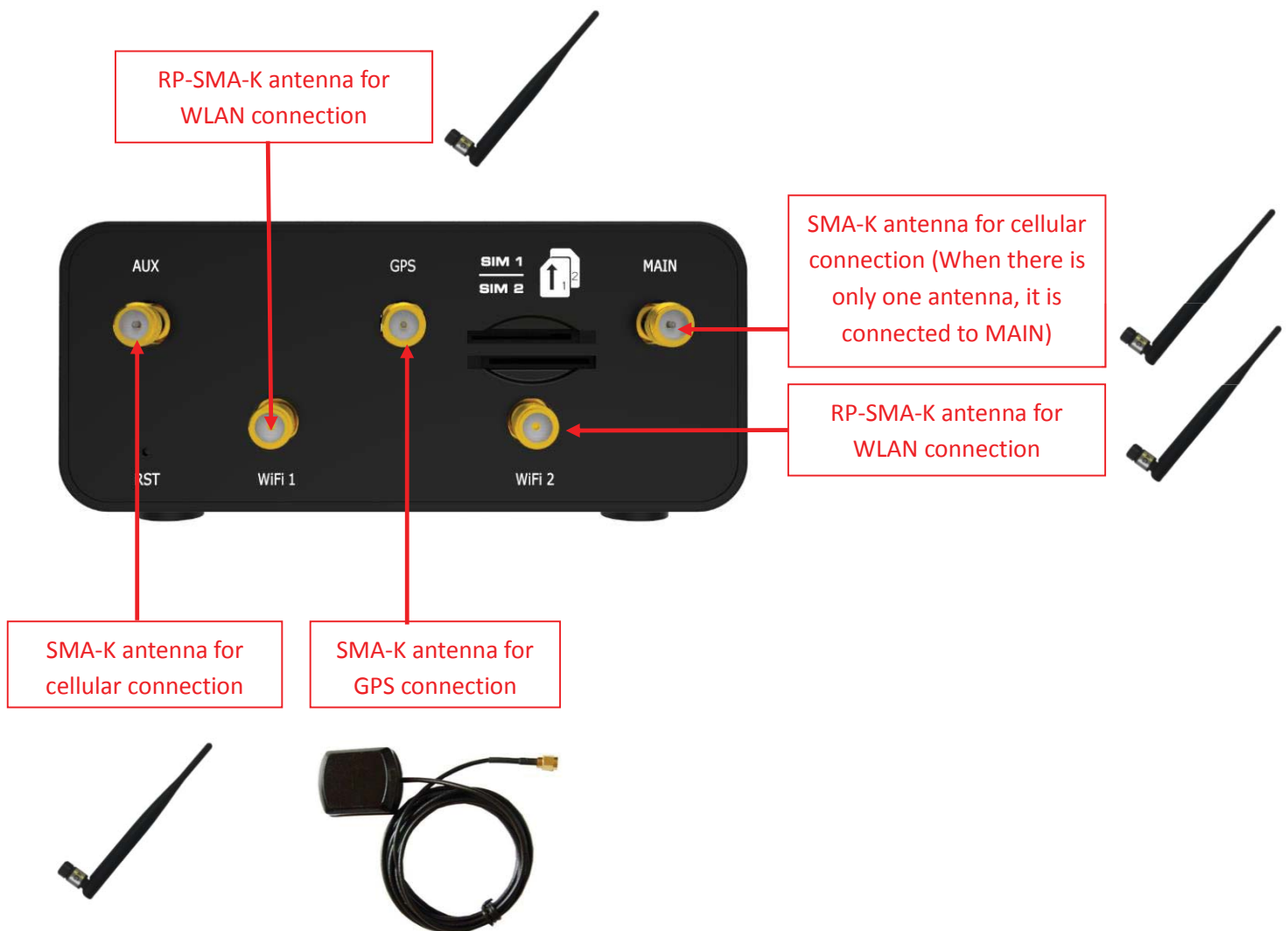
1. Use the specific M2M SIM card when the device is working in extreme temperature, because the regular card for long-time working in harsh environment will be disconnected frequently.
2. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.

3. Do not bend or scratch the card.
4. Keep the card away from electricity and magnetism.
5. Make sure router is powered off before inserting or removing the card.

2.9 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.

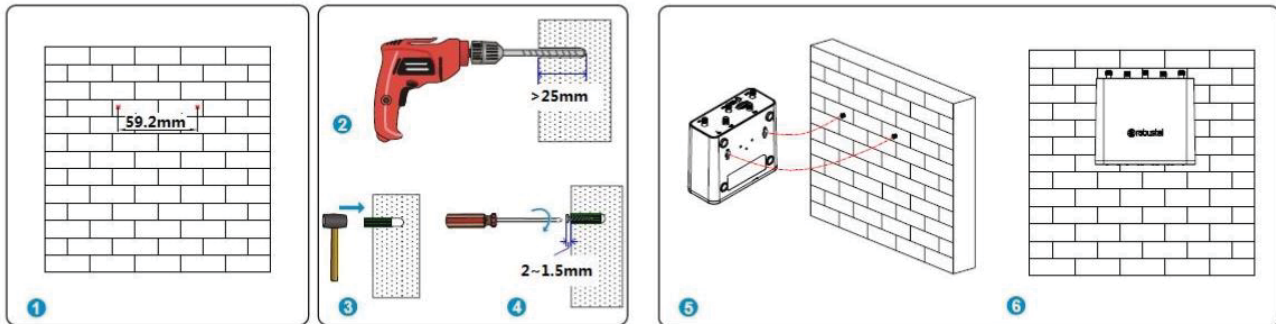


2.10 Mount the Router

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)

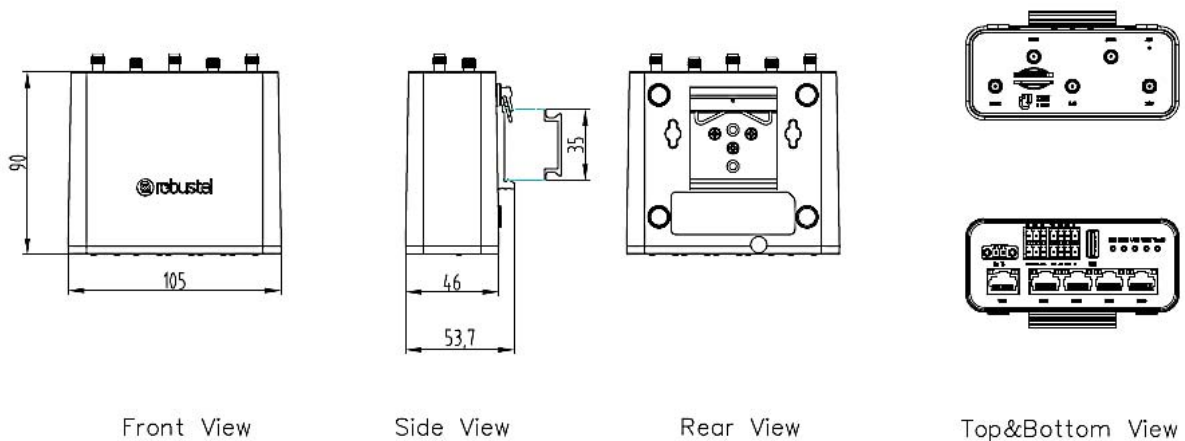


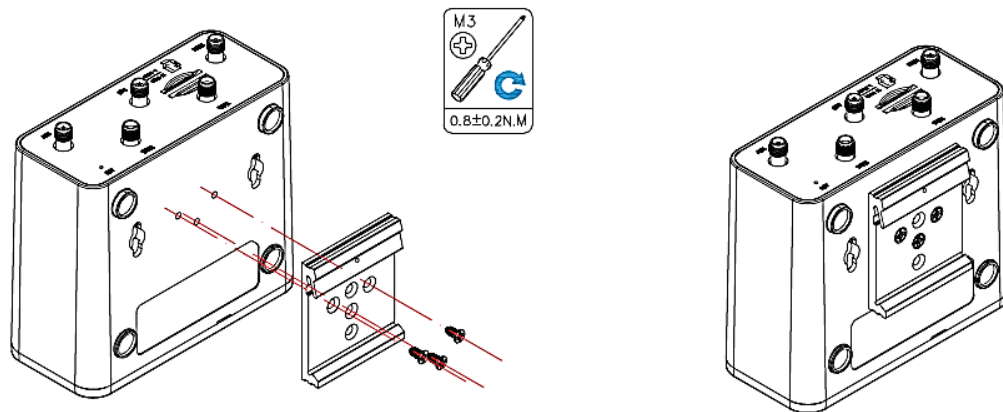
First, drill holes on the wall, the distance between the two holes is 60mm, then knock the expansion pipe into the wall with a rubber hammer, align the screw with the expansion pipe, insert the screw and reserve the corresponding length, and finally fix the product on the wall.

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

2. DIN rail mounting (measured in mm)

Option 1: Vertical installation

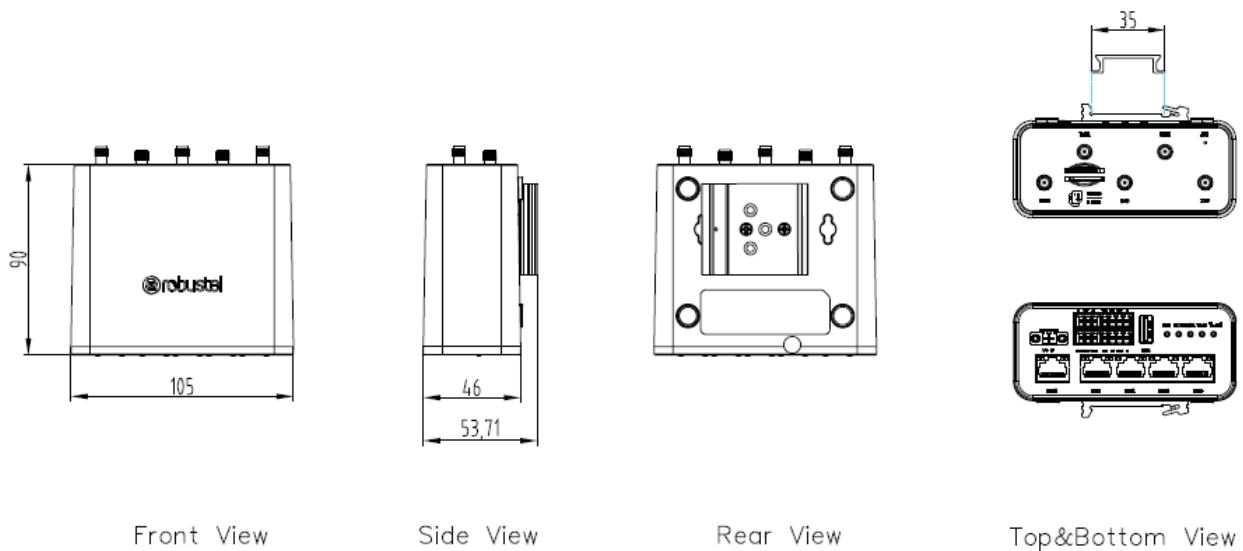


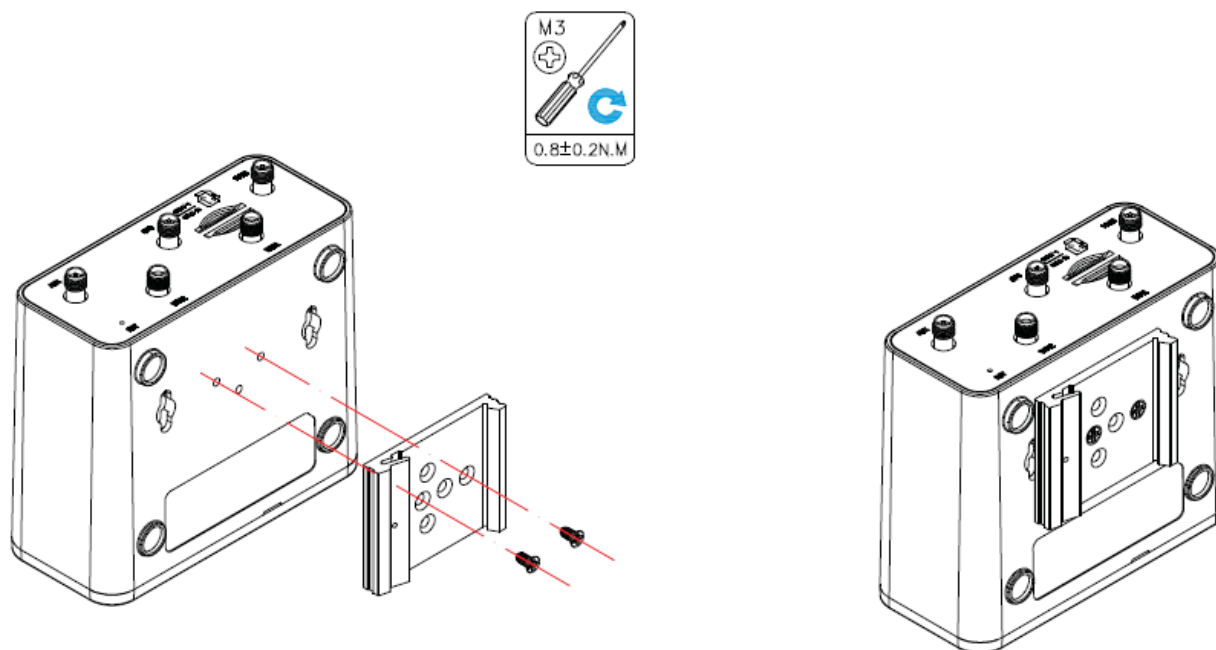


Use 3 pcs of M3*8 Black cross recessed countersunk head tapping screws to mount the router on the DIN rail, and then hang the DIN rail on the holder. You need to choose a standard holder.

Note: Recommended torque for mounting is 0.8 N.m, and the maximum allowed is 1.0 N.m.

Option 2: Horizontal installation





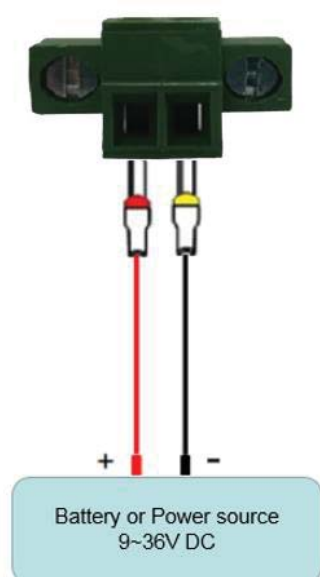
Use 3 pcs of M3*8 Black cross recessed countersunk head tapping screws to mount the router on the DIN rail, and then hang the DIN rail on the holder. You need to choose a standard holder.

Note: Recommended torque for mounting is 0.8 N.m, and the maximum allowed is 1.0 N.m.

2.11 Connect the Router to a Computer

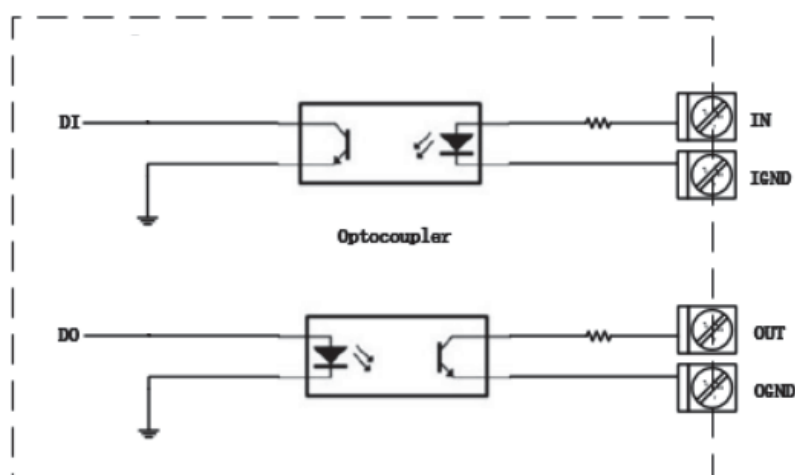
Connect the Ethernet port (ETH1 ~ ETH4) of the router to a PC with a standard crossover cable.

2.12 Power Supply



PIN	Description	Note
1	Power supply Positive	Connect the adapter or battery positive (red wire)
2	Power supply negative	Connect the adapter or battery negative (black wire)

2.13 DI/DO Interface



R1520 supports 1 channel DI and 1 channel DO, the internal schematic diagram is as shown above;

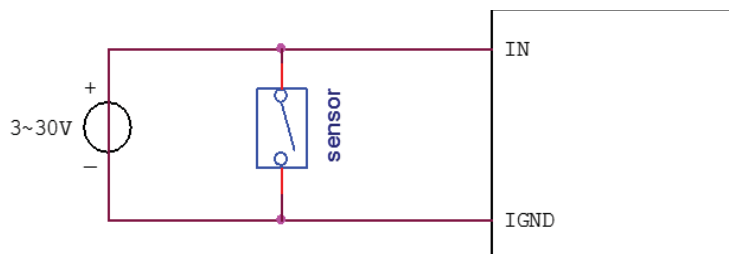
1. DI application

R1520 DI input is internally isolated by opt coupler, internal current-limiting design, within the working level of 0 ~ 30V, external input does not need current limiting, DI input logic level range is as follows:

Logic 1 level range: min 3.5 V to max 30 V;

Logic 0 level range: min 0 V to max 1 V;

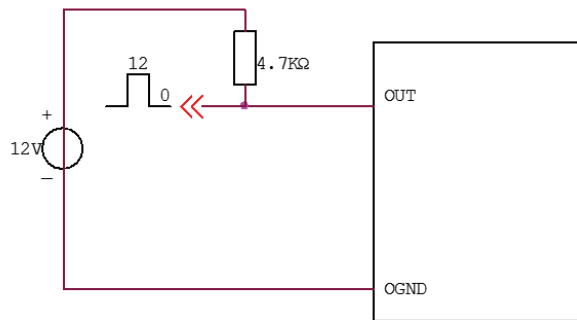
The application example is as follows:



2. DO application

R1520 DO output is internally isolated by opt coupler, OUT is OC gate output, Normal use requires external resistor pull-up, the pull-up voltage range is 3V ~ 30V (for actual use, please consult Robustel for selection of pull-up resistor);

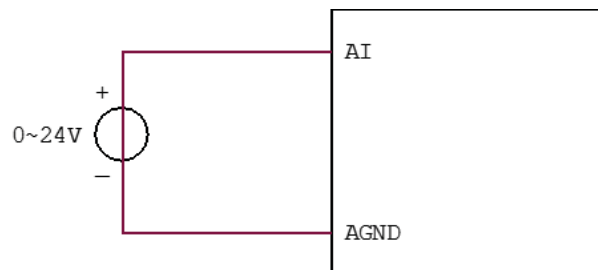
The application example is as follows:



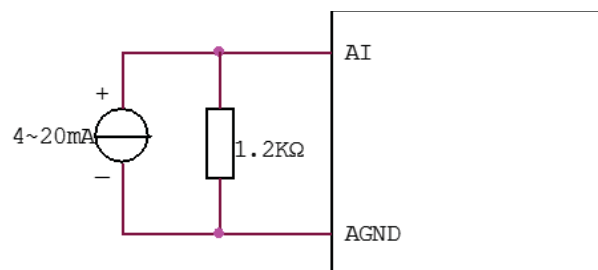
2.14 AI Interface

R1520 supports one channel AI interface for analog signal voltage and current measurement;

1. 0 ~ 24V voltage measurement, wiring as shown below:



2. 4 ~ 20mA current signal measurement requires an external parallel 1.2kohm resistor, wiring as shown below:



Chapter 3 Initial Configuration

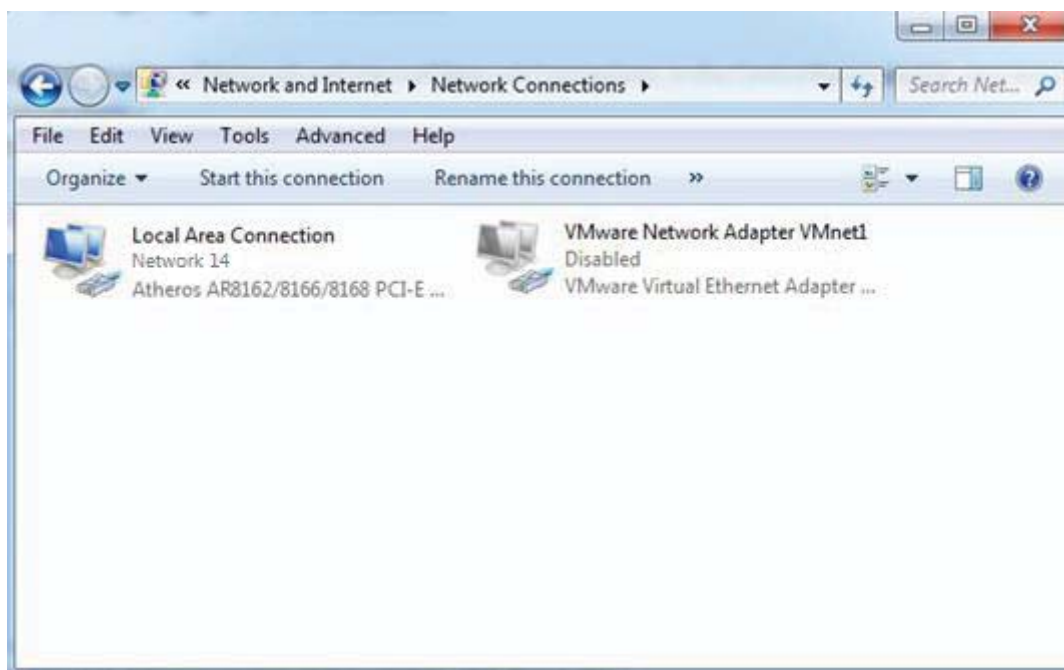
The router can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

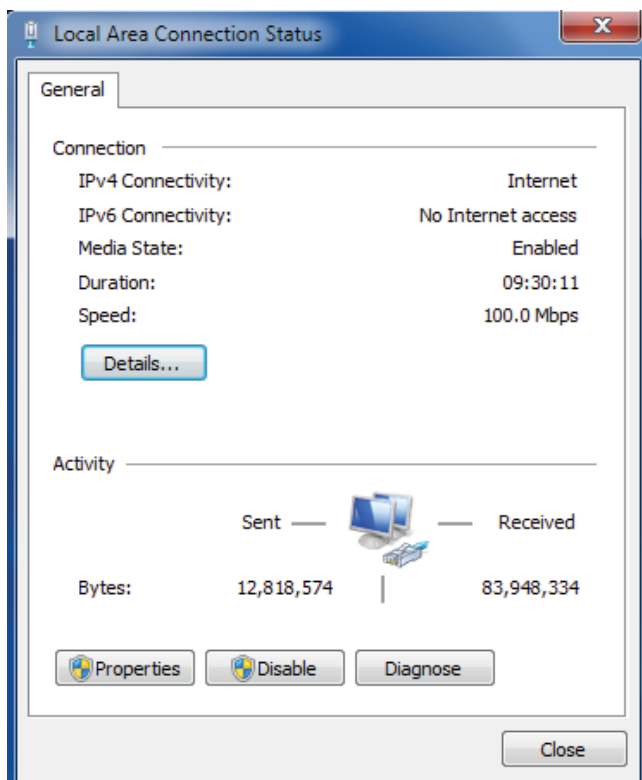
There are two methods to get IP address for the PC. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

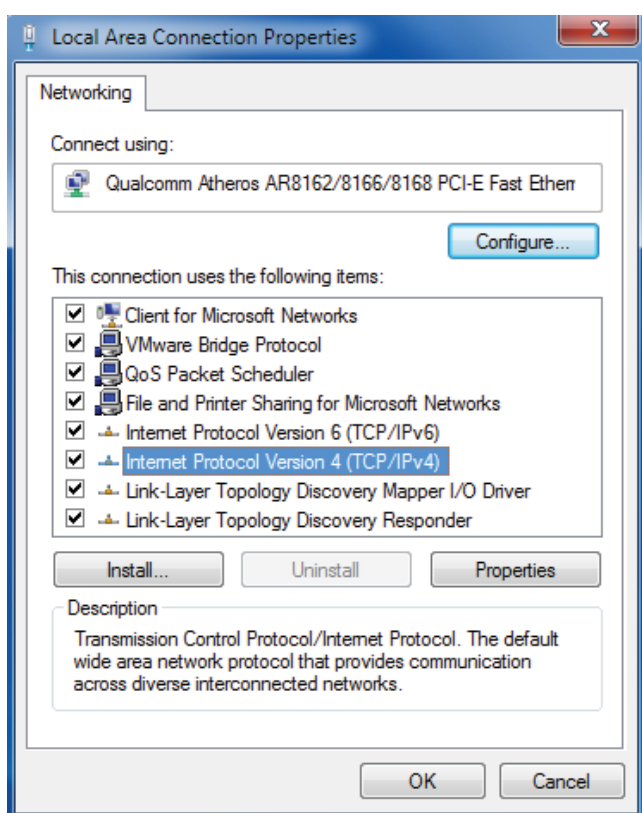
1. Click **Start > Control Panel**, double-click **Network and Internet**, and then double-click **Network Connections**.



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

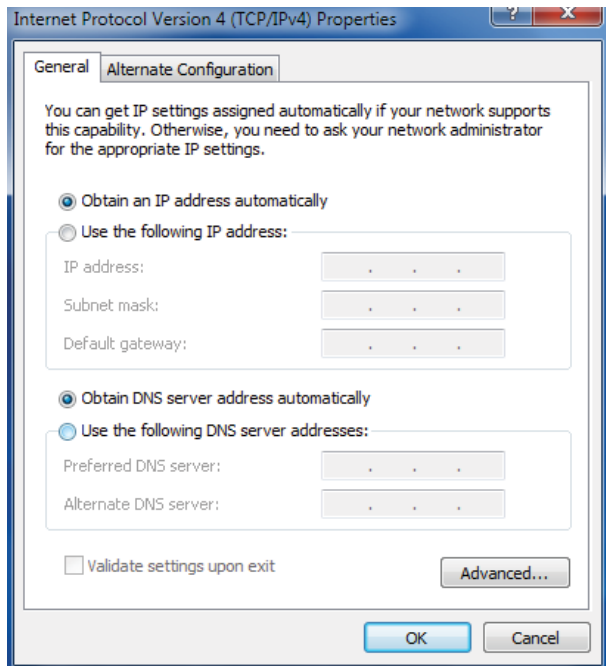


- Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



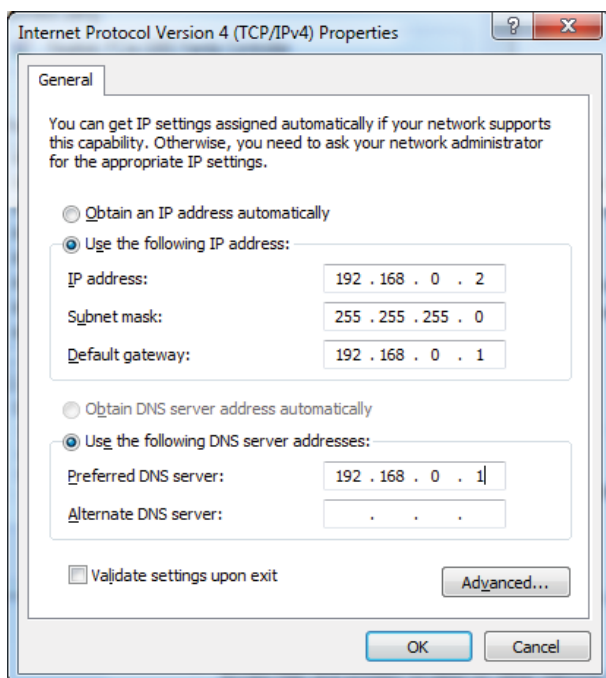
4. Two ways for configuring the IP address of PC

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



Use the following IP address:

(Configured a static IP address manually within the same subnet of the router, click and configure **"Use the following IP address"**)



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

3.2 Factory Default Settings

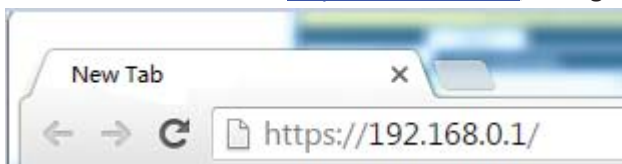
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
ETH0/POE	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

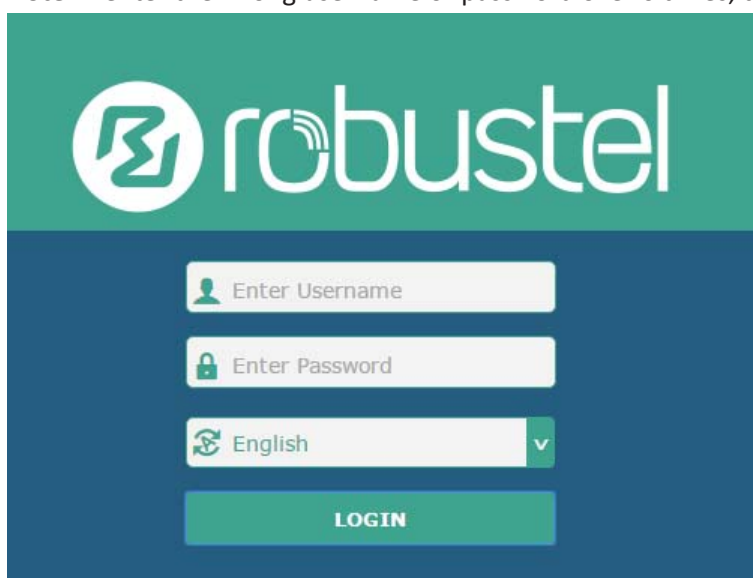
To log in to the management page and view the configuration status of your router, please follow the steps below.

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



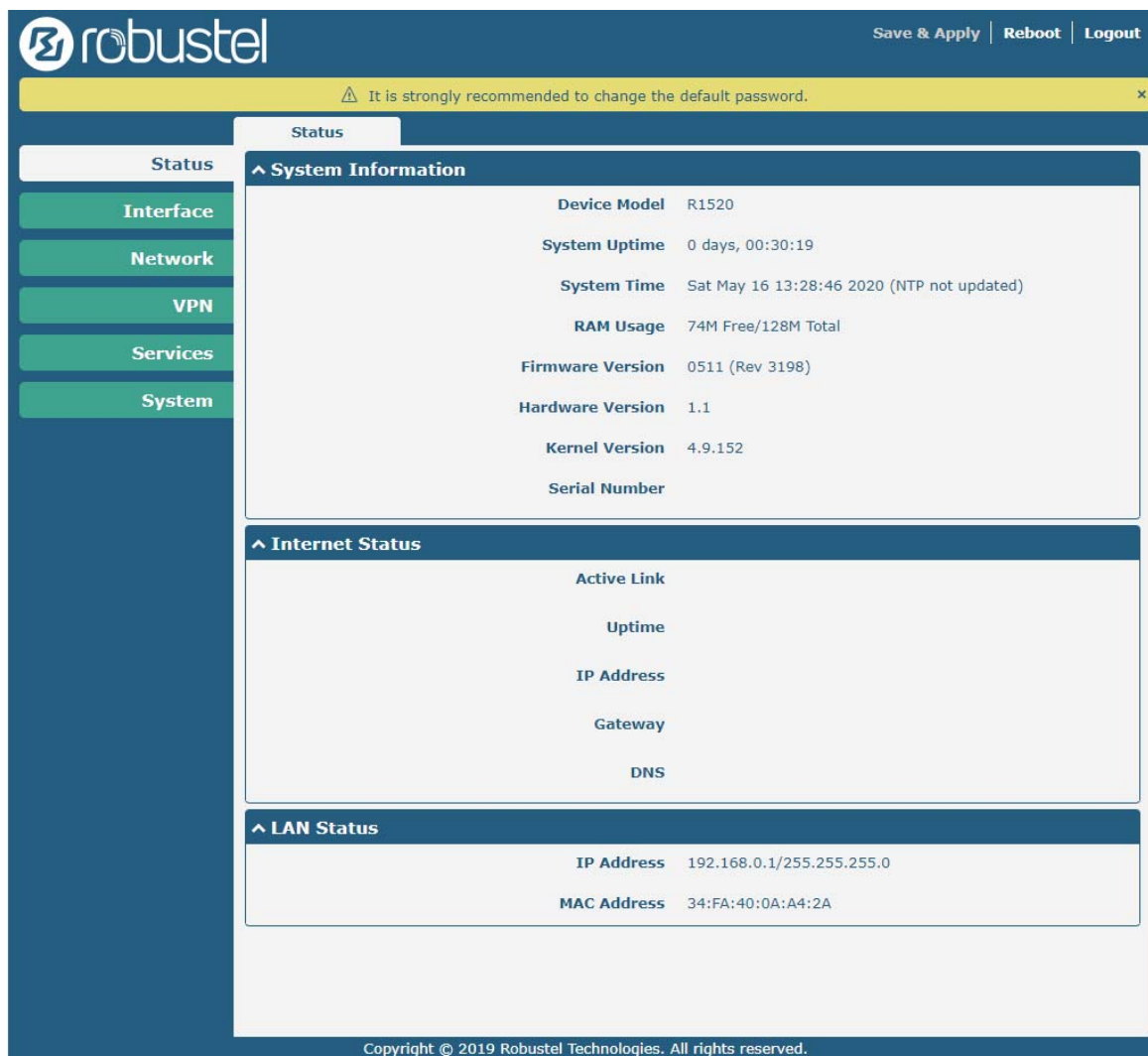
3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are “admin”.

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



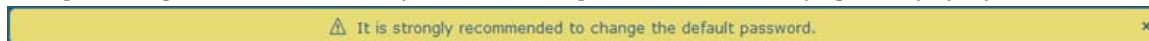
3.4 Control Panel

After successfully logging into the R1520 router, the home page is as shown in the figure below:





In the home page, the user can save the configuration, restart the router, log out, and so on.




Using the original username and 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.

Click the  to close the popup. To change your username and/or password, see **4.6.6 User Management**.

Control Panel		
Item	Description	Button
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification taking effect.	
Reboot	Click to reboot the router. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	

Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	
Submit	Click to save the modification on current configuration page.	
Cancel	Click to cancel the modification on current configuration page.	

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

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

Chapter 4 Router Configuration

4.1 Status

4.1.1 System Information

This section allows you to view the System Information of your Router.

^ System Information	
Device Model	R1520
System Uptime	0 days, 01:45:48
System Time	Sat May 16 14:44:15 2020 (NTP not updated)
RAM Usage	76M Free/128M Total
Firmware Version	0511 (Rev 3198)
Hardware Version	1.1
Kernel Version	4.9.152
Serial Number	

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, from which you can get information such as the router's time of delivery.

4.1.2 Internet Status

This section shows the Internet status information of your Router.

^ Internet Status	
Active Link	WWAN1
Uptime	0 days, 00:39:31
IP Address	10.122.74.11/255.255.255.248
Gateway	10.122.74.9
DNS	210.21.4.130 221.5.88.88

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

4.1.3 LAN Status

This section shows the router's LAN status information.

^ LAN Status	
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:0A:A4:2A

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.

4.2 Interface

4.2.1 Link Manager

This section allows you to setup the connection of Link Manager. Link manager is a network link backup function that provides mobile network and Ethernet link backups.

Link Manager

Status

^ General Settings

Primary Link

WWAN1

v

?

Backup Link

WWAN2

v

Backup Mode

Cold Backup

v

?

Revert Interval

0

?

Emergency Reboot

ON





OFF


?

General Settings @ Link Manager		
Item	Description	Default
Primary Link	Select from "WWAN1", "WWAN2", "WAN" or "WLAN". <ul style="list-style-type: none"> 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 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 4.2.5 WiFi .	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", "WAN" or "None". <ul style="list-style-type: none"> WWAN1: Select to make SIM1 as the backup wireless link WWAN2: Select to make SIM2 as the backup wireless link WAN: Select to make WAN 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 4.2.5 WiFi . <ul style="list-style-type: none"> None: Do not select any backup link 	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 Note: Warm backup mode is not available for dual SIM backup. <ul style="list-style-type: none"> 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/WAN/WLAN to enter the configuration window.

WWAN1/ WWAN2

Link Manager

^ General Settings

Index

1

Type

WWAN1

v

Description

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

^ WWAN Settings

Automatic APN Selection

ON

OFF

Dialup Number

*99***1#

Authentication Type

Auto

v

Switch SIM By Data Allowance

ON

OFF

?

Data Allowance

0

?

Billing Day

1

?

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

^ WWAN Settings

Automatic APN Selection
☐ ON ☒ OFF

APN

Username

Password

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

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. It can be null.	Null
WWAN Settings		

Link Settings (WWAN)		
Item	Description	Default
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
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 keep-alive 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
Ping Interval	Set the ping interval.	300
Ping Retry Interval	Set the ping retry interval. When ping failed, the router will ping again every retry interval.	5
Ping 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

Link Settings (WWAN)		
Item	Description	Default
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

3

Type

WAN

v

Description

Connection Type

DHCP

v

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

^ General Settings

Index

3

Type

WAN

v

Description

Connection Type

Static

v

^ Static Address Settings

IP Address

?

Gateway

Primary DNS

Secondary DNS

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

^ General Settings

Index Type Description Connection Type

^ WAN Settings

Data Allowance ?Billing Day ?

^ PPPoE Settings

Username Password Authentication Type PPP Expert Options ?

^ Ping Detection Settings

 ?Enable ☒ ON ☐ OFFPrimary Server Secondary Server Interval ?Retry Interval ?Timeout ?Max Ping Tries ?

^ Advanced Settings

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

Link Settings (WAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link. It can be null.	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
Router	Set the router 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
WAN Settings		
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.	OFF
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day. If not set, traffic will not be counted.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keep-alive 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

4

Type

WLAN

v

Description

Connection Type

DHCP

v

^ WLAN Settings

SSID

router

Connect to Hidden SSID

OFF

Password

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

^ General Settings

Index

4

Type

WLAN

v

Description

Connection Type

Static

v

WLAN Settings

^ Static Address Settings

IP Address

?

Gateway

Primary DNS

Secondary DNS

R1520 does not support "PPPoE" WLAN connection types.

^ Ping Detection Settings

Enable

ON OFF

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Max Ping Tries

3

?

^ Advanced Settings

NAT Enable

ON OFF

MTU

1500

Upload Bandwidth

10000

?

Download Bandwidth

10000

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. It can be null.	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

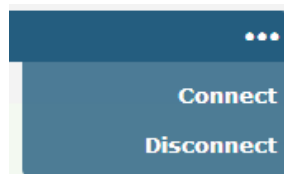
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	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.

Link Manager		Status		
^ Link Status				
Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 01:03:29	10.122.74.11..
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 Manager

Status

Link Status

Index

Link

Status

Uptime

IP Address

1

WWAN1

Connected

0 days, 01:03:29

10.122.74.11..

Index

1

Link

WWAN1

Status

Connected

Interface

wwan

Uptime

0 days, 01:03:29

IP Address

10.122.74.11/255.255.255.248

Gateway

10.122.74.9

DNS

210.21.4.130 221.5.88.88

RX Packets

42

TX Packets

46

RX Bytes

2962

TX Bytes

3568

2

WWAN2

Disconnected

^ WWAN Data Usage Statistics		?
WWAN1 Monthly Stats	Clear	
WWAN2 Monthly Stats	Clear	
^ WAN Data Usage Statistics		?
WAN Monthly Stats	Clear	

WWAN usage data statistics and WAN usage data statistics respectively count the packet flow of the cellular module and WAN.

Click the **Clear** button to clear the monthly data traffic usage statistics of SIM1 or SIM2. Data statistics will be displayed only if enable the Data Allowance function in **Interface > Link Manager > Link Settings > WWAN1/WWAN2/WAN Settings > Data Allowance** .

^ WWAN Settings

Automatic APN Selection ☒ ON ☐ OFF

Dialup Number *99***1#

Authentication Type Auto

Switch SIM By Data Allowance ☐ ON ☒ OFF ?

Data Allowance 0 ?

Billing Day 1 ?

^ WAN Settings

Data Allowance 0 ?

Billing Day 1 ?




4.2.2 LAN

This section allows you to set the related parameters for LAN port. When ETH0 is configured as WAN, the router has four LAN ports, ETH1, ETH2, ETH3, and ETH4. The ETH1, ETH2, ETH3 and ETH4 can freely choose from lan0, lan1, lan2 and lan3. When ETH0 is configured as LAN, the router has five LAN ports, ETH0, ETH1, ETH2, ETH3, and ETH4. The ETH0, ETH1, ETH2, ETH3 and ETH4 can freely choose from lan0, lan1, lan2, lan3 or lan4. Whether it is four LAN ports or five LAN ports, lan0 must be selected by at least one LAN port. The default settings of ETH1/ETH2/ETH3/ETH4 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN

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

LAN

^ General Settings

Index 1

Interface lan0

IP Address 192.168.0.1

Netmask 255.255.255.0

MTU 1500

General Settings @ LAN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Note: 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 the mode of DHCP 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 DHCP Relay, which will provide a relay tunnel to solve problem that DHCP Client and DHCP Server is not in a same subnet 	Server
IPv4 Pool Start	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.2
IPv4 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		
Router	Define the router assigned by the DHCP server to the clients, which must be on the same network segment with DHCP address pool.	Null
Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Secondary DNS	Define the secondary DNS server assigned by the DHCP server to the Override secondary DNS will override the automatically obtained DNS.	Null
WINS Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set the lease time which the client can use the IP address obtained from DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond an IP address via a MAC address. format: mac,ip;mac,ip;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for DHCP information output.	OFF

Multiple IP

LAN	Multiple IP	Status		
^ Multiple IP Settings				
Index	Interface	IP Address	Netmask	
1	lan0	10.0.0.1	255.255.255.0	 

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

Multiple IP

^ IP Settings

Index	<input type="text" value="1"/>
Interface	<input type="text" value="lan0"/> v
IP Address	<input type="text" value="10.0.0.1"/>
Netmask	<input type="text" value="255.255.255.0"/>

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

Status

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

LAN	Multiple IP	Status		
^ Interface Status				
Index	Interface	IP Address	MAC Address	
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:68:AC	
^ Connected Devices				
Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.5	D4:3A:65:05:FC:4A	lan0	0s
^ DHCP Lease Table				
Index	IP Address	MAC Address	Interface	Expired Time
1	192.168.0.5	d4:3a:65:05:fc:4a	lan0	0 days, 01:51:32


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

^ Interface Status				
Index	Interface	IP Address	MAC Address	
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:68:AC	
	Index	1		
	Interface	lan0		
	IP Address	192.168.0.1/255.255.255.0		
	MAC Address	34:FA:40:0B:68:AC		
	RX Packets	14470		
	TX Packets	12759		
	RX Bytes	2849614		
	TX Bytes	10657230		

4.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There are five Ethernet ports on R1520 Router, including ETH0, ETH1, ETH2, ETH3 and ETH4. ETH0 can be configured as the WAN port for the router to access the outer network or the LAN port for the lower end devices to connect with the router. ETH1, ETH2, ETH3 and ETH4 can only be configured as a LAN port for the lower device to connect to the router. The default factory settings of ETH0 is Wan. ETH1, ETH2, ETH3 and ETH4 are lan0, and the default IP is 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 the  button on the right-most of eth1 to change the port parameters in the port window that pops up.

Ports

^ Port Settings

Index

2

Port

eth1

Port Assignment

lan0

Ports

^ Port Settings

Index

2

Port

eth1

Port Assignment

lan0

Submit

Close

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

Click the status column to view the connection status of all Ethernet ports.

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


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

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

4.2.4 Cellular

This section allows you to set the related parameters of Cellular. The R1520 Router has two SIM card slot. When inserting a single SIM card for the first time, both Sim1 and sim2 slots are available.

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

Click the right most button  of SIM 1 to edit the parameters.

Cellular

^ General Settings

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

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

^ Cellular Network Settings

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

^ Advanced Settings

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

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

^ Cellular Network Settings

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

^ Band Settings

GSM 850

ON OFF

GSM 900

ON OFF

GSM 1800

ON OFF

GSM 1900

ON OFF

WCDMA 800

ON OFF

WCDMA 850

ON OFF

WCDMA 900

ON OFF

WCDMA 1900

ON OFF

WCDMA 2100

ON OFF

WCDMA 1700

ON OFF

LTE Band 1

ON OFF

LTE Band 3

ON OFF

LTE Band 5

ON OFF

LTE Band 7

ON OFF

LTE Band 8

ON OFF

LTE Band 20

ON OFF

^ 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	Set the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		
Network Type	Select from "Auto", "4G Only", "4G First". <ul style="list-style-type: none"> Auto: Connect to the best signal network automatically 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		

Cellular		
Item	Description	Default
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	EG25-G	460019372994937	Registered to home network

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

^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EG25-G	460019372994937	Registered to home network
Index 1				
Modem Status				
Modem Model EG25-G				
Current SIM SIM1				
Phone Number				
IMSI 460019372994937				
ICCID 89860118801079009362				
Registration Registered to home network				
Network Provider CHN-UNICOM				
Network Type LTE				
Band 3				
Signal Strength 19 (-75dBm)				
RSRP -107 dBm				
RSRQ -7 dB				
SINR 21 dB				
Bit Error Rate 99				
PLMN ID 46001				
Local Area Code 2507				
Cell ID 6074702				
IMEI 862107045897238				
Firmware Version EC20CEFAGR06A09M4G				

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: SIM1 or SIM2.
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 > General Settings > Phone Number .
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.

Status	
Item	Description
Band	Show the band of the current network.
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the current RSRP when you register to the 4G network.
RSRQ	Show the current RSRQ when you register to the 4G network.
SINR	Show the current SINR when you register to the 4G network.
EC/IO	Show EC/IO when registering to 3G networks.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Community ID	Show the current Community 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.

Click the "AT Debug" to detect the AT command.

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.	--

4.2.5 WiFi

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

WiFi AP

Configure Router as WiFi AP

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

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

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

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

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

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

General Settings @ Access Point 2G		
Item	Description	Default
Enable	Click the toggle button to enable/disable the WiFi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b only”, “11g only” and “11n only”. <ul style="list-style-type: none"> 11bgn Mixed: mix three protocols for backward compatibility 11b only: IEEE 802.11b, 11 Mbps~2.4GHz 11g only: IEEE 802.11g, 54 Mbps~2.4GHz 11n only: IEEE 802.11n, 300 Mbps 	11bgn Mixed
Channel	The channel that different bandwidth can choose is as follows. <ul style="list-style-type: none"> Auto: Router will scan all frequency channels until the best one is found 1~11channel of 20MHz bandwidth will be fixed to work with this channel: <ul style="list-style-type: none"> 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 The frequency of 3~9 channels of 40MHz bandwidth available channel: 	Auto

General Settings @ Access Point 2G		
Item	Description	Default
	3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz	
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	Select from “Disabled”, “WPA-Personal”, “WPA-Enterprise” or “WEP”. <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 access protection, only one password is provided for identity authentication WPA-Enterprise: Supports 802.1x RADIUS authentication. WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission 	Disabled
WPA Version	Select from “Auto”, “WPA” or “WPA2”. <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

General Settings @ Access Point 2G		
Item	Description	Default
Encryption	<p>Select from “TKIP” or “AES”.</p> <ul style="list-style-type: none"> TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication 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 <p>Note: The security mode will affect wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.</p>	AES
PSK Password	Enter the Pre share key password. Enter 8 to 63 characters.	Null
Radius Authentication Server Address	Enter the IP address of the Radius authentication server.	Null
Radius Authentication Server Port	Enter the port of the Radius authentication server.	1812
Radius Server Share Secret	Enter Radius to identify the server's Shared key.	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

^ Advanced Settings

Max Associated Stations

64

Beacon Interval

100

?

DTIM Period

2

?

RTS Threshold

2347

?

Fragmentation Threshold

2346

?

Transmit Rate

Auto

v

11N Transmit Rate

Auto

v

Transmit Power

Max

v

Channel Width

Auto

v

?

Enable Short GI

ON

OFF

?

Enable AP Isolation

ON

OFF

?

Debug Level

none

v

Advanced Settings @ Access Point		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router's AP. (0 value means no limit)	0
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set the delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS/CTS Threshold	Set the threshold of "request to send", which is the request to send a 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 data transfer rate or default to automatic.	Auto
11N Transmit Rate	Specify the data transfer rate in IEEE 802.11n WiFi mode or default to automatic.	Auto
Transmit Power	Select the transmit power level. Select from "Max", "High", "Medium" or "Low".	Max
bandwidth	Select from "20MHz" or "40MHz". Note: The 40MHz channel bandwidth provides an available data transfer rate that is more than twice that of a single 20MHz channel.	20MHZ
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.	OFF

Advanced Settings @ Access Point		
Item	Description	Default
	When enabled, the router will isolate all connected wireless devices. The wireless device cannot access the router directly via WLAN.	
Debug Level	Select from “verbose”, “deBug”, “info”, “notice”, “warning” or “none”.	none

^ General Settings

Enable ACL ☐ ON ☒ 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 Settings @ Access Point		
Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select 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 @ Access Point		
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		1			
Channel Width		20 MHz			
MAC Address		34:FA:40:09:D3:38			
^ Associated Stations					
Index	MAC Address	IP Address	Name	Connected Time	Signal

Note: WiFi is off by default. Follow the steps below to enable it and configure the router as WiFi client.

WiFi Client

Configure Router as WiFi Client

Click **Interface > WiFi > WiFi**, select “Client” as the mode and regarding the AP type to choose the related Client Band then click “Submit”.

WiFi
^ General Settings
Mode <input type="text" value="Client"/> ?
Region <input type="text" value="SE"/> ?

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

Status	Interface	WiFi
Link Manager	LAN	
Ethernet		
Cellular		
WiFi		

WiFi
^ General Settings
Mode <input type="text" value="Client"/> ?
Region <input type="text" value="SE"/> ?

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

WLAN Settings
SSID <input type="text" value="router"/>
Connect to Hidden SSID <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Password <input type="text"/>

Click **Interface > WLAN** to configure the parameters of WiFi Client after setting the mode as Client.

Status	
^ WLAN Status	
Status	Connected
Uptime	0 days, 00:02:40
IP Address	172.16.23.246/255.255.255.0
Gateway	172.16.23.1
DNS	172.16.23.2 114.114.114.114
MAC Address	34:fa:40:09:d3:38
^ Link Status	
Signal	-74 dBm
Noise	-95 dBm
Width	20 MHz
TX Bitrate	1.0 MBit/s
TX	2034 bytes (26 packets)
RX	662881 bytes (4446 packets)
^ WPA Status	
WPA State	COMPLETED
Frequency	2412
BSSID	20:65:8e:ba:56:60
SSID	Robustel
Mode	station
Key Management	WPA2-PSK
Pairwise Cipher	CCMP
Group Cipher	TKIP

Users can refresh the SSID scan results near the router. Click , and then click scan to refresh the surrounding SSID

^ Scan Results					...	?
Index	SSID	MAC Address	Frequency	Signal	Scan	
1	Robustel-Visitor	20:65:8E:BA:56:61	2412	-72 dBm		
2	DIRECT-mE-mix2s	C2:4C:2C:EB:0C:90	2412	-74 dBm		
3	Robustel	20:65:8E:BA:56:60	2412	-75 dBm		
4	router-203	00:23:A7:AB:64:F4	2422	-83 dBm		
5	OpenWrt	B8:27:EB:B6:C8:75	2462	-89 dBm		

4.2.6 USB

This section allows you to configure the USB parameters. The router's USB interface can be used to upgrade firmware

and upgrade configuration.

USB

Key

General Settings

Enable USB

ON OFF

Enable Automatic Upgrade

ON OFF

USB

Key

Key

USB Automatic Update Key

Generate

USB Automatic Update Key

Download

General Settings @ USB		
Item	Description	Default
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the router when inserting a USB storage device with a router firmware.	OFF
Key		
Item	Description	Default
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

Note: when using the USB automatic upgrade function, the LEDs start blinking one by one, it means that the upgrade is in progress. When LEDs stop blinking one by one, and the USER Indicators is on, it means that the upgrade is completed. After upgrading, the device will not restart automatically. If there is no LEDs start blinking one by one all the time, it means there is an exception, and it does not enter into the automatic upgrade process.

4.2.7 DI/DO

This section allows you to set the DI/DO parameters. Digital Input and Digital Output are the specific interfaces for R1520. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to realize real-time monitoring.

DI


DI

DO

Status

DI Settings

Index	Enable	Mode	Inversion
1	false	ON-OFF	false

Click the right-most  button of DI index 1 as below. The window is displayed as below when the default mode is “ON-OFF”.

DI

^ General Settings

Index

Enable

Mode

Inversion

Alarm On Content

Alarm Off Content

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

DI

^ General Settings

Index

Enable

Mode

Inversion

Threshold Value


Alarm On Content

Alarm Off Content

General Settings @ DI		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select from “ON-OFF” or “Counter”. <ul style="list-style-type: none"> ON-OFF: Alarm mode can be triggered at the DI access ON-OFF. Counter: Event counter mode 	ON-OFF
Inversion	The count is divided into a rising edge count of the level or a falling edge count. If the current rising edge count, the reverse edge is the falling edge count.	OFF
Threshold Value	The threshold value is a unique parameter when the mode is count. Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off

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

DO

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

Click  to enter the DO index 1, the configuration window is shown as below.

DO

^ General Settings

Index

1

Enable

☐ ON ☒ OFF

Alarm On Action

High

▼

Alarm Off Action

Low

▼

Initial State

Last

▼

Delay

0

?

Hold Time

0

?

Alarm Source

DI1 Alarm

▼

The window is displayed as below when choosing “Pulse” as the alarm on action.

DO

^ General Settings

Index

1

Enable

☐ ON ☒ OFF

Alarm On Action

Pulse

▼

Alarm Off Action

Low

▼

Initial State

Last

▼

Delay

0

?

Hold Time

0

?

Low-level Width

1000

?

High-level Width

1000

?

Alarm Source

DI1 Alarm

▼

The window is displayed as below when choosing “Pulse” as the alarm off action.

DO

^ General Settings

Index

Enable

ON

OFF

Alarm On Action

High

v

Alarm Off Action

Pulse

v

Initial State

Last

v

Delay

0

?

Hold Time

0

?

Low-level Width

1000

?

High-level Width

1000

?

Alarm Source

DI1 Alarm

v

General Settings @ DO		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> High: a high electrical level output Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered 	High
Alarm Off Action	Digital Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> High: a high electrical level output Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered 	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. <ul style="list-style-type: none"> Last: DO’s status will consist with the status of last power off High: DO interface is in high electrical level Low: DO interface is in low electrical level 	Last
Delay (unit: 100ms)	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
Low-level Width	Set the low-level width. It is available when enabling Pulse as “Alarm On Action/Alarm	1000

General Settings @ DO		
Item	Description	Default
(unit: ms)	Off Action". In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1000 to 3000.	
High-level Width (unit: ms)	Set the high-level width. It is available when enabling Pulse as "Alarm On Action/Alarm Off Action". In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1000 to 3000.	1000
Alarm Source	Digital output activation can be activated by this alarm.	DI1

Status


This window allows you to view the status of DI/DO interface. It can also clear the counter alarm of DI in here. Click **Clear** button to clear DI 1 or DI 2 monthly usage statistics info for counter alarm.

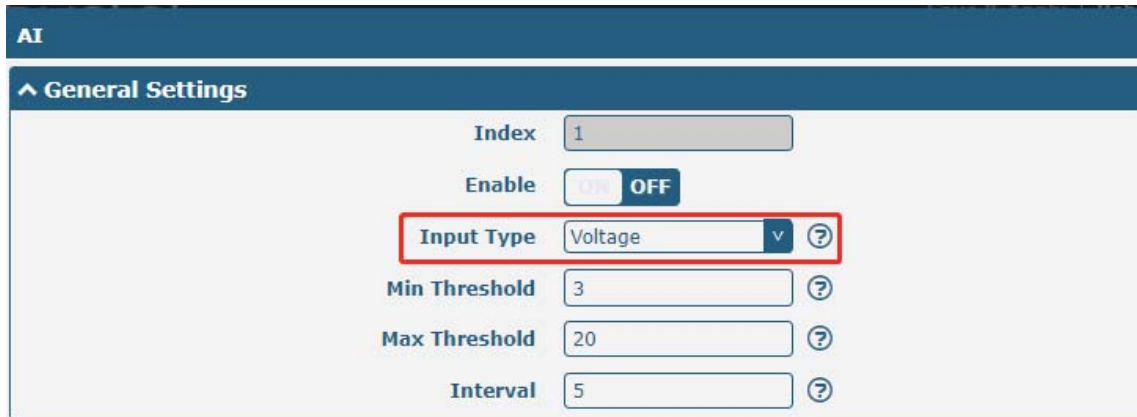
DI	DO	Status	
^ DI Status			
Index	Level	Status	Count
1	Low	Alarm off	
^ Action Of Clear			
Counter Alarm Of DI 1			Clear
^ DO Status			
Index	Level	Low-level Width	High-level Width
1	Low		
^ DO Control			
Level Of DO1			Toggle

4.2.8 AI

This section is used to set the parameters of analog input (AI). AI is a unique interface of R1520 router. The analog input is used to collect analog signals within a certain range, and is often used to collect continuously changing values such as voltage, current, temperature, and pressure of the sensor. The higher the accuracy of the ADC bits used for analog input, the finer the analog quantization and the more accurate the result.


AI	Status		
^ AI Settings			
Index	Enable	Input Type	Interval
1	false	Voltage	5

Click the right-most  button of DI index 1 as below. The window is displayed as below when the “input type” is “voltage”.



The screenshot shows the 'AI' settings window. Under the 'General Settings' tab, the 'Index' is set to 1. The 'Enable' switch is currently in the 'OFF' position. The 'Input Type' dropdown menu is highlighted with a red box and shows 'Voltage' selected. Below it, the 'Min Threshold' is set to 3, the 'Max Threshold' is set to 20, and the 'Interval' is set to 5. Each of these three fields has a help icon (question mark) to its right.

The window is displayed as below when the “input type” is “Current”.



This screenshot shows the same 'AI' settings window, but the 'Input Type' dropdown menu is now set to 'Current' and is highlighted with a red box. The 'Min Threshold' has changed to 4, the 'Max Threshold' has changed to 16, and the 'Interval' remains at 5. The 'Enable' switch is still 'OFF'.

AI (Analog Input)		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the switch button to "ON" to turn on the analog input function.	OFF
Input type	Select from "Voltage" or "Current". <ul style="list-style-type: none"> Voltage: The data collected is voltage Current: The data collected is Current 	Voltage
Min Threshold@Voltage	Set the minimum voltage threshold. When the voltage collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: V.	3
Max Threshold@Voltage	Set the maximum voltage threshold. When the voltage collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: V.	20
Min	Set the minimum current threshold. When the current collected by the AI interface is	4

AI (Analog Input)		
Item	Description	Default
Threshold@Current	less than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	
Min Threshold@Current	Set the maximum current threshold. When the current collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	16
Interval	Collect the latest data every few seconds.	5

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

AI	Status			
^ AI Status				
Index	Type	Min Threshold	Max Threshold	Value
1	voltage	3	20	
<div><div>Index</div><div>1</div></div>				
<div><div>Type</div><div>voltage</div></div>				
<div><div>Min Threshold</div><div>3</div></div>				
<div><div>Max Threshold</div><div>20</div></div>				

4.2.9 Serial Port

This section allows you to set the serial port parameters. The R1520 router supports two serial ports, COM1 and COM2. It can also be modified according to requirements and configured as two COM1 or two COM2. The serial data can be converted into IP data or through IP data into serial data, and then the data can be transmitted through wired or wireless network, so as to realize the function of transparent data transmission.

Serial Port	Status				
^ Serial Port Settings					
Index	Port	Enable	Baud Rate	Application Mode	
1	COM1	false	115200	Transparent	
2	COM2	false	115200	Transparent	

Click the right-most  button of COM1 as below.

Serial Port

Serial Port Application Settings

Index	<input type="text" value="1"/>
Port	<input type="text" value="COM1"/> v
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Baud Rate	<input type="text" value="115200"/> v
Data Bits	<input type="text" value="8"/> v
Stop Bits	<input type="text" value="1"/> v
Parity	<input type="text" value="None"/> v
Flow Control	<input type="text" value="None"/> v

Data Packing

Packing Timeout	<input type="text" value="50"/> ?
Packing Length	<input type="text" value="1200"/>

- In the "Server Settings" column, when "Transparent " is selected as the application mode and "TCP Client" as the protocol, the window is as follows:

Server Setting

Application Mode	<input type="text" value="Transparent"/> v
Protocol	<input type="text" value="TCP Client"/> v
Server Address	<input type="text"/>
Server Port	<input type="text"/>

When "Transparent " is selected as the application mode and "TCP Server" as the protocol, the window is as follows:

Server Setting

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

When "Transparent " is selected as the application mode and "UDP" is used as the protocol, the window is as follows:

^ 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"/>

- When “ModBus RTU Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:

^ Server Setting	
Application Mode	Modbus RTU Gateway v
Protocol	TCP Client v
Server Address	<input type="text"/>
Server Port	<input type="text"/>

When "ModBus RTU Gateway" is selected as the application mode and "TCP Server" as the protocol, the window is as follows:

^ Server Setting	
Application Mode	Modbus RTU Gateway v
Protocol	TCP Server v
Local IP	<input type="text"/>
Local Port	<input type="text"/>

When selecting "ModBus RTU Gateway" as the application mode and "UDP" as the protocol, the window is as follows:

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

- When “ModBus ASCII Gateway” is selected as the application mode and “TCP Client” as the protocol, the window is as follows:

^ Server Setting

Application Mode

Modbus ASCII Gatev v

Protocol

TCP Client v

Server Address

Server Port

When selecting "ModBus ASCII Gateway" as the application mode and "TCP Server" as the protocol, the window is as follows:

^ Server Setting

Application Mode

Modbus ASCII Gatev v

Protocol

TCP Server v

Local IP

Local Port

When selecting "ModBus ASCII Gateway" as the application mode and "UDP" as the protocol, the window is as follows:

^ Server Setting

Application Mode

Modbus ASCII Gatev v

Protocol

UDP v

Local IP

Local Port

Server Address

Server Port

Serial Port		
Item	Description	Default
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	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" or "115200".	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. The unit is milliseconds.	50

Serial Port		
Item	Description	Default
	Note: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200

Server Settings		
Item	Description	Default
Application Mode	Select from "Transparent", "Modbus RTU Router" or "Modbus ASCII Router". <ul style="list-style-type: none"> Transparent: Router will transmit the serial data transparently Modbus RTU Router: Router will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa Modbus ASCII Router: Router will translate the Modbus ASCII data to Modbus TCP data and sent out, and vice versa 	Transparent
Protocol	Select from "TCP Client", "TCP Server", or "UDP". <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 	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	RS232	0B	0B	
2	RS485	0B	0B	

4.3 Network


4.3.1 Route

This section allows you to set the static route. Static routes are routes based on destination addresses. Up to 20 static routes can be added to the router. Routing Information Protocol, or RIP (Route Information Protocol), is widely used in small networks with stable rate changes. The OSPF (Open Shortest Path First) protocol is used for decision routing within a single autonomous system and is suitable for large networks.

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

Static Route

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

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

Static Route	
^ Static Route	
Index	<input type="text" value="1"/>
Description	<input type="text"/>
Destination	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
Interface	<input type="text" value="wwan"/> 

Static Route		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this 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
Router	Define the router of the destination.	Null
Interface	Choose the corresponding port of the link that you want to configure.	wwan

Status

This window allows you to view the status of route.

Static Route		Status			
^ Route Table					
Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.122.74.9	wwan	0
2	10.122.74.8	255.255.255.248	0.0.0.0	wwan	0
3	172.16.0.0	255.255.0.0	0.0.0.0	lan0	0

4.3.2 Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping, Custom Rules, DMZ and Status. Filtering rules allow users to custom accept or discard a specified access source, filtering its IP address or MAC address.

Click "> firewall > filter" to display as follows:


Filtering

The filtering rules can be used to either accept or block certain users or ports from accessing your router.

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

Click **+** to add whitelist rules. The maximum count is 50.

Filtering	
^ Whitelist Rules	
Index	<input type="text" value="1"/>
Description	<input type="text"/>
Source Address	<input type="text"/> ⓘ

Click  to add filtering rules. The maximum count is 50. 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

1

Description

Source Address

?

Source MAC

?

Target Address

?

Protocol

All

v

Action

Drop

v

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

^ Filtering Rules

Index

1

Description

Source Address

?

Source Port

?

Source MAC

?

Target Address

?

Target Port

?

Protocol

TCP

v

Action

Drop

v

Filtering		
Item	Description	Default
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. Cannot be changed when filtering rules table is not empty. <ul style="list-style-type: none"> 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

Filtering		
Item	Description	Default
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	ON
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable Console	Click the toggle button to enable/disable this option. When enabled, the user can access the router via Console.	ON
Enable the vpn_nat traversal	Click the toggle button to enable/disable this option. When enabled, the router automatically modifies the IP address of the VPN header received by WAN/WWAN to the IP address of the device under LAN port and sends it out.	OFF
Whitelist Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Filtering Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	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

Filtering		
Item	Description	Default
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

Port mapping is defined manually in the router, and the data received from some ports in the public network are all forwarded to a port of an IP in the internal network. Click "network > firewall > port mapping" to display as follows:

Filtering	Port Mapping	Custom Rules	DMZ	Status		
^ Port Mapping Rules						
Index	Description	Internet Port	Local IP	Local Port	Protocol	+

Click  to add port mapping rules. The maximum rule count is 50.

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 to the local IP address. Empty means unlimited. e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Set the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router's LAN IP which will forward to the internet port of router.	Null


Port Mapping Rules		
Item	Description	Default
Local Port	Enter the port of router's LAN IP.	Null
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP

Custom Rules

Custom rules, that is, rules that you define yourself. Click "Network> Firewall> Custom Rules" to display as follows:

Filtering	Port Mapping	Custom Rules	DMZ	Status
^ Custom Iptables Rules				
Index	Description	Rule	+	

Click  to add custom rules. The maximum rule count is 50.


Custom Rules	
^ Custom Iptables Rule	
Index	<input type="text" value="1"/>
Description	<input type="text"/>
Rule	<input type="text"/> 

Custom firewall Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this custom rule.	Null
Rule	Specify one custom rule.	Null

DMZ

The DMZ, also known as the Demilitarized Zone, is being transformed into a large swath of land. It is to solve the problem that the access user of the external network cannot access the internal network server after installing the firewall, and set up a buffer between the non-secure system and the secure system. A DMZ host is an Intranet host that has open access to all ports except the occupied and forwarded ports to the specified address.

Click "> firewall > DMZ" to display the following:

Filtering	Port Mapping	Custom Rules	DMZ	Status
^ DMZ Settings				
Enable DMZ	<input type="button" value="ON"/> <input checked="" type="button" 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

Status

This window allows you to view the status of chain input, chain forward and chain output.

Filtering	Port Mapping	Custom Rules	DMZ	Status			
^ Chain Input							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
4	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	52	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
^ Chain Forward							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0
^ Chain Output							
Index	Packets	Target	Protocol	In	Out	Source	Destination

4.3.3 IP Passthrough

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

IP Passthrough

^ General Settings

Enable

ON OFF ?

If router enables the IP Pass-through, the terminal device (such as PC) will enable the DHCP Client mode and connect to LAN port of the router; and after the router dial up successfully, the PC will automatically obtain the IP address and DNS server address which assigned by ISP. To use this function, the main link needs to be set to WWAN, and the backup link needs to be set to None.

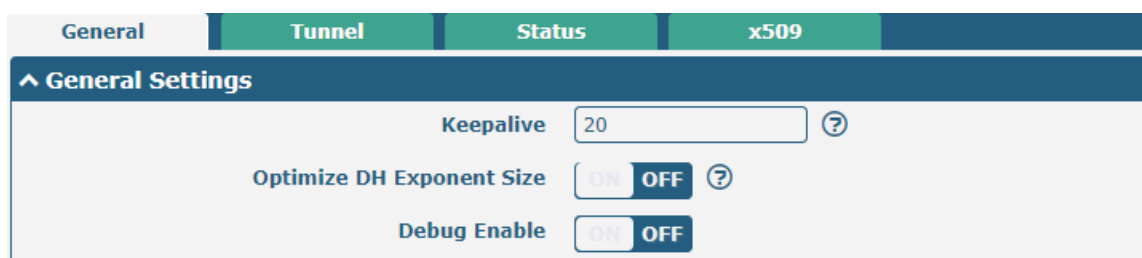
4.4 VPN

4.4.1 IPsec

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

Click **VPN > IPsec > general** to set IPsec parameters.

General



General Tunnel Status x509

^ General Settings

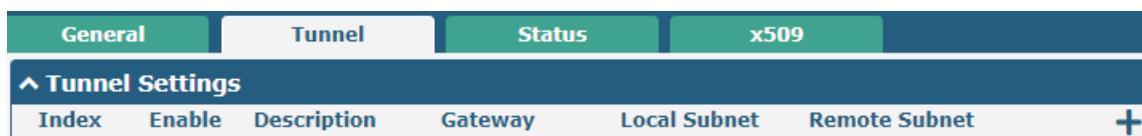
Keepalive ?

Optimize DH Exponent Size ?

Debug Enable

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

Tunnel



General Tunnel Status x509

^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+
-------	--------	-------------	---------	--------------	---------------	---

Click  to add IPsec tunnel settings. The maximum count is 6.

Tunnel

^ General Settings

Index

1

Enable

ON

OFF

Description

Gateway

?

Mode

Tunnel

v

Protocol

ESP

v

Local Subnet

?

Remote Subnet

?

Link Binding

Unspecified

v

?

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Router	Enter the address of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it Transport: Used between end-stations or between an end-station and a router, if the router 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
Link binding	Select the link to build Ipsec.	Unbound

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

^ IKE Settings

IKE Type	IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	PSK	v
PSK Secret	<input type="text"/>	
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

IKE Type	IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	CA	v
Private Key Password	<input type="text"/>	
IKE Lifetime	86400	?

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

^ IKE Settings

IKE Type	IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	PKCS#12	v
Private Key Password	<input type="text"/>	
IKE Lifetime	86400	?

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

^ IKE Settings

IKE Type

IKEv1

v

Negotiation Mode

Main

v

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

IKE DH Group

DHgroup2

v

Authentication Type

xAuth PSK

v

PSK Secret

Local ID Type

Default

v

Remote ID Type

Default

v

Username

?

Password

?

IKE Lifetime

86400

?

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

^ IKE Settings

IKE Type

IKEv1

v

Negotiation Mode

Main

v

Encryption Algorithm

3DES

v

Authentication Algorithm

SHA1

v

IKE DH Group

DHgroup2

v

Authentication Type

xAuth CA

v

Private Key Password

Username

?

Password

?

IKE Lifetime

86400

?

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

IKE Settings		
Item	Description	Default
	<ul style="list-style-type: none"> 3DES: Use 168-bit 3DES encryption algorithm in CBC mode AES128: Use 128-bit AES encryption algorithm in CBC mode AES128: Use 192-bit AES encryption algorithm in CBC mode AES256: Use 256-bit AES encryption algorithm in CBC mode 	
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from "PSK", "CA", "xAuth PSK", "PKCS#12" and "xAuth CA" to be used in IKE negotiation. <ul style="list-style-type: none"> PSK: Pre-shared Key CA: Certification Authority xAuth: Extended Authentication to AAA server PKCS#12: Exchange digital certificate authentication 	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: Uses an IP address as the ID in IKE negotiation FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com User FQDN: Uses 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 router, e.g., test@robustel.com 	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> Default: Uses an IP address as the ID in IKE negotiation FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security router, e.g., test.robustel.com User FQDN: Uses 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 router, 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.

Tunnel

^ General 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"/> ?
Mode	<input type="text" value="Tunnel"/> v
Protocol	<input type="text" value="ESP"/> v
Local Subnet	<input type="text"/> ?
Remote Subnet	<input type="text"/> ?
Link Binding	<input type="text" value="Unspecified"/> v ?

^ IKE Settings

^ SA Settings

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

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

Tunnel

^ General 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"/> ?
Mode	<input type="text" value="Tunnel"/> v
Protocol	<input type="text" value="AH"/> v
Local Subnet	<input type="text"/> ?
Remote Subnet	<input type="text"/> ?
Link Binding	<input type="text" value="Unspecified"/> v ?

▼ IKE Settings

▲ SA Settings

Authentication Algorithm

SHA1

▼

PFS Group

DHgroup2

▼

SA Lifetime

28800

?

DPD Interval

30

?

DPD Failures

150

?

▲ Advanced Settings

Enable Compression

ON

OFF

Enable Forceencaps

ON

OFF

?

Expert Options

?

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192” 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 “PFS(N/A)”, “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating to 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 a Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	30
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	150
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps		OFF

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

Status

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

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

x509

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

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

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5", or "Tunnel 6".	Tunnel 1
Local Certificate	Click on "Choose File" to locate the certificate file from local computer, and then import this file into your router.	--
Remote Certificate	Click on "Choose File" to locate the certificate file from remote computer, and then import this file into your router.	--
Private Key	Click on "Choose File" to locate the private key file.	--
CA Certificate	Click on "Choose File" to locate the correct CA certificate file.	--
PKCS#12 Certificate	Click on "Choose File" to locate the PKCS # 12 certificate file.	--

x509		
Item	Description	Default
X509 Settings		
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


4.4.2 OpenVPN

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

Click "**VPN > OpenVPN > OpenVPN**" to display as follows:

OpenVPN

OpenVPN		Status	x509
^ Tunnel Settings			
Index	Enable	Description	Mode
^ Password Manage			
Index	Username		
^ Client Manage			
Index	Enable	Common Name	Client IP Address

Click  to add OpenVPN tunnel settings. The maximum count is 5. By default, the mode is "P2P". The window is displayed as below when choosing "P2P" as the mode.

^ 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="P2P"/> v ⓘ
TLS Mode	<input type="text" value="None"/> v ⓘ
Protocol	<input type="text" value="UDP"/> v
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="None"/> v ⓘ
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/> v
Authentication Algorithm	<input type="text" value="SHA1"/> v
Keepalive Interval	<input type="text" value="20"/> ⓘ
Keepalive Timeout	<input type="text" value="120"/> ⓘ
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
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 “Auto” as the mode.

^ General Settings

Index

1

Enable

ON

OFF

Description

Mode

Auto

v

?

Private Key Password

Enable Client Status

ON

OFF

?

Enable NAT

ON

OFF

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

^ General Settings

Index

1

Enable

ON

OFF

Description

Mode

Client

v

?

Protocol

UDP

v

Peer Address

Peer Port

1194

Interface Type

TUN

v

Authentication Type

None

v

?

Encrypt Algorithm

BF

v

Authentication Algorithm

SHA1

v

Renegotiation Interval

86400

?

Keepalive Interval

20

?

Keepalive Timeout

120

?

TUN MTU

1500

Max Frame Size

Enable Compression

ON

OFF

Enable NAT

ON

OFF

Enable DNS overrid

ON

OFF

?

Verbose Level

0

v

?

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

^ General Settings

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

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

^ General Settings

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

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
Peer Address	
Peer Port	1194
Interface Type	TUN v
Authentication Type	Preshared v ?
Encrypt Algorithm	BF v
Authentication Algorithm	SHA1 v
Renegotiation Interval	86400 ?
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<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	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Client <input type="button" value="v"/> ?
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	Password <input type="button" value="v"/> ?
Username	
Password	
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Renegotiation Interval	86400 ?
Keepalive Interval	20 ?
Keepalive Timeout	120 ?
TUN MTU	1500
Max Frame Size	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Verbose Level	0 <input type="button" value="v"/> ?

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Client <input type="button" value="v"/> <input data-bbox="890 450 917 477" type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	
Peer Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA <input type="button" value="v"/> <input data-bbox="890 701 917 728" type="button" value="?"/>
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Renegotiation Interval	86400 <input data-bbox="890 857 917 884" type="button" value="?"/>
Keepalive Interval	20 <input data-bbox="890 907 917 934" type="button" value="?"/>
Keepalive Timeout	120 <input data-bbox="890 956 917 983" type="button" value="?"/>
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input data-bbox="778 1261 805 1288" type="button" value="?"/>
Verbose Level	0 <input type="button" value="v"/> <input data-bbox="890 1310 917 1337" type="button" value="?"/>

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

^ General Settings

Index
1

Enable
ON OFF

Description

Mode
Client

Protocol
UDP

Peer Address

Peer Port
1194

Interface Type
TUN

Authentication Type
X509CA Password

Username

Password

Encrypt Algorithm
BF

Authentication Algorithm
SHA1

Renegotiation Interval
86400

Keepalive Interval
20

Keepalive Timeout
120

TUN MTU
1500

Max Frame Size

Private Key Password

Enable Compression
ON OFF

Enable NAT
ON OFF

Enable DNS overrid
ON OFF

Verbose Level
0

^ Advanced Settings

Enable HMAC Firewall
ON OFF

Enable PKCS#12
ON OFF


Enable nsCertType
ON OFF

Expert Options

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

General Settings @ OpenVPN		
Item	Description	Default
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from "Auto", "P2P", "Client" or "Server".	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 listener port of the OpenVPN server.	1194
Listen IP Address	Enter the IP address or domain name.	Null
Listen Port	Enter the listener port at this end.	1194
Interface Type	Select from "TUN", "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
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
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". Note: "None" and "Preshared" authentication type are only working with P2P mode.	None
Enable IP Pool	Click the toggle button to enable / disable this option. When enabled, the client will obtain a virtual IP from the address pool.	OFF
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Client Subnet	Client virtual IP network address.	10.8.0.0
Client Subnet Netmask	Client virtual IP network address mask.	255.255.255.0
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES-128", "AES-192" and "AES-256". <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
Authentication Algorithm	Select from "MD5", "SHA1", "SHA256" or "SHA512".	SHA1
Max Clients	Set the retention timeout. If the connection continues to timeout during this time, the OpenVPN tunnel will be re-established.	10
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

General Settings @ OpenVPN		
Item	Description	Default
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
TUN MTU	Set the MTU for the tunnel.	1500
Max Frame Size	Sets the shard size of the data to be transmitted through the tunnel.	Null
Private Key Password	Enter the private key password under "X509CA" and "X509CA password" authentication.	Null
Enable Compression	Click the switch button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable DNS overrid	Click the switch button to enable/disable this option. When enabled, DNS pushed by the server is received as the local DNS server.	OFF
Enable Bridge With LAN0	Click the toggle button to enable / disable this option. When enabled, the virtual interface can be bridged with Lan0.	ON
Enable Default Gateway	Click the toggle button to enable / disable this option. When enabled, it will receive the gateway pushed by the server as the local gateway.	OFF
Enable Client Status	Click the toggle button to enable / disable this option. After the server is enabled, it can display the connected client status information.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log and values from 0 to 11. <ul style="list-style-type: none"> 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 @ 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

Click user password management  to add a user name and password. The maximum count is 20 as shown below.

OpenVPN

^ General Settings

Index

Username

Password

General Settings @ Password Manage		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Username	In server mode, configure the client's user name.	Null
Password	In server mode, configure the password for the client's username.	Null

Click client administration  to add client information, The maximum count is 20 as shown below.

OpenVPN

^ General Settings

Index

Enable

ON OFF

Common Name



Client IP Address

General Settings @ Client Manage		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the switch button to enable/disable this option.	ON
Common Name	Specify a common name for the client.	Null
Client IP Address	Specify the client's virtual IP address.	Null

Status

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

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

This section is used to locate the certificates such as CA.

OpenVPN
Status
x509

^ X509 Settings

Tunnel Name

Tunnel 1

▼

Mode

Client

▼

Root CA

Choose File

No file chosen

⬆

Certificate File

Choose File

No file chosen

⬆

Private Key

Choose File

No file chosen

⬆

TLS-Auth Key

Choose File

No file chosen

⬆

PKCS#12 Certificate

Choose File

No file chosen

⬆

^ Certificate Files

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

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

4.4.3 GRE

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

GRE

GRE
Status

^ Tunnel Settings

Index	Enable	Description	Remote IP Address
-------	--------	-------------	-------------------

+

Click  to add tunnel settings. The maximum count is 5.

GRE

^ Tunnel Settings

Index

Enable ON OFF

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask

Remote Virtual IP Address

Enable Default Route ON OFF

Enable NAT ON OFF

Secrets

Tunnel Settings @ GRE		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates data packets so that it can route packets of other protocols in an IP network.	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	OFF

	the traffics of the router will go through the GRE VPN.	
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
Secrets	Set the key of the GRE tunnel.	Null

Status

This section allows you to view the GRE tunnel status.

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

4.5 Services

4.5.1 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
<div>^ Syslog Settings</div> <div> <div>Enable</div> <div>ON OFF</div> </div> <div> <div>Syslog Level</div> <div>Debug v</div> </div> <div> <div>Save Position</div> <div>RAM v ?</div> </div> <div> <div>Log to Remote</div> <div>ON OFF ?</div> </div>

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

Syslog

^ Syslog Settings

Enable

☒ ON
 ☐ OFF

Syslog Level

v

Save Position

v
?

Log to Remote

☒ ON
 ☐ OFF
 ?

Add Identifier

☐ ON
 ☒ OFF
 ?

Remote IP Address

Remote Port

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 detail.	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 saving 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

4.5.2 Event

This section allows you to set the event parameters. Event feature provides an ability to send alerts by SNMP and RCMS when certain system events occur.

Event
Notification
Query

^ General Settings

Signal Quality Threshold

?


General Settings @ Event		
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. Router will generate a log event when	0

	the actual threshold is less than the specified threshold. 0 means disable this option.	
--	---	--

Event	Notification	Query
-------	--------------	-------

^ Event Notification Group Settings

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

Click  button to add an Event parameters.

Notification

^ General Settings

Index	1
Description	
Send SMS	<input type="checkbox"/> OFF
Send Email	<input type="checkbox"/> OFF
DO Control	<input type="checkbox"/> OFF
Save to NVM	<input 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
Wan data traffic stats clear	<input type="checkbox"/> OFF
Wan data traffic overflow	<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
DI 1 ON	<input type="checkbox"/> OFF
DI 1 OFF	<input type="checkbox"/> OFF
DI 1 Counter Overflow	<input type="checkbox"/> OFF
AI voltage low	<input type="checkbox"/> OFF
AI voltage high	<input type="checkbox"/> OFF
AI current low	<input type="checkbox"/> OFF
AI current high	<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 "4.5.4 Services > SMS", 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 "4.5.4 Services > Email".	OFF
Email Addresses	Enter the email addresses used for receiving event notification. Use a space to separate each address.	Null
DO Control	Click the toggle button to enable / disable this option. After opening, DO output is triggered.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

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

Event

Notification

Query

Save Position

RAM

Filtering

Apr 18 10:04:00, configuration change, via web manager

Apr 18 15:57:05, configuration change, via web manager

Apr 18 15:57:58, configuration change, via web manager

Apr 18 16:04:59, configuration change, via web manager

Apr 18 16:05:37, configuration change, via web manager

Apr 18 16:05:46, configuration change, via web manager

Apr 18 16:05:52, configuration change, via web manager

Apr 18 16:06:05, USB device remove

Apr 18 16:06:11, USB device connect

Apr 18 16:06:20, USB device remove

Apr 18 16:06:28, configuration change, via web manager

Apr 18 16:06:34, configuration change, via web manager

Apr 18 16:06:40, system time update

Apr 18 16:06:47, configuration change, via web manager

Apr 18 16:07:05, USB device connect

Apr 18 16:07:16, USB device remove

Apr 18 16:07:27, configuration change, via web manager

Apr 18 16:07:51, configuration change, via web manager

Apr 18 16:08:17, configuration change, via web manager

Apr 18 16:09:02, configuration change, via web manager

Apr 18 16:09:20, USB device connect

Apr 18 16:09:44, USB device remove

Apr 18 16:11:01, configuration change, via web manager

Apr 18 16:11:14, USB device connect

Apr 18 16:11:21, USB device remove

Apr 18 16:11:29, configuration change, via web manager

Apr 18 16:11:34, configuration change, via web manager

Apr 18 16:11:35, 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	Event will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

4.5.3 NTP

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

NTP

Status

^ Timezone Settings

Time Zone

UTC+08:00

Expert Setting

^ NTP Client Settings

Enable

ON

Primary NTP Server

pool.ntp.org

Secondary NTP Server

NTP Update Interval

0

^ NTP Server Settings

Enable

ON

NTP		
Item	Description	Default
Timezone Settings		
Time Zone	Click the drop down list to select the time zone you are in. EG, China: UTC + 08:00.	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. Eg, "~".	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) which NTP client synchronize the time from NTP server. Minutes wait for next update, and 0 means update only	0

	once.	
NTP Server Settings		
Enable	Click the toggle button to enable the NTP server option. Once enabled, the NTP client can synchronize with the router in time.	OFF

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

NTP

Status

^ Time

System Time

2018-04-18 16:15:12

PC Time

2018-04-18 16:16:37

Sync

Last Update Time

2018-04-18 16:11:35

4.5.4 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 **5.2.2 SMS Remote Control**.

SMS

SMS Testing

^ SMS Management Settings

Enable

ON OFF

Authentication Type

Password

v

?

Phone Number

?

SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. 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 authenticating, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be "cmd1; cmd2; ..." • Both: Use both the "Password" and "Phonenum" for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be "username: password; cmd1; cmd2; ..." 	Password
Phone Number	Set the phone number used for SMS management, and use ';' to separate each number.	Null

Note: It can be null when choose “Password” as the authentication type.

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

SMS

SMS Testing

^ SMS Testing

Phone Number

Message

Result

Send

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

4.5.5 Email

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

Email

^ Email Settings

Enable

ON

OFF

Enable TLS/SSL

ON

OFF

?

Enable STARTTLS

ON

OFF

Outgoing Server

Server Port

25

Timeout

10

?

Auth Login

ON

OFF

?

Username

Password

From

Subject

Email Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Email option.	OFF
Enable TLS/SSL	Click the toggle button to enable/disable the TLS/SSL option.	OFF
Enable STARTTLS	Click the toggle button to enable/disable the STARTTLS encrypted transmission method.	OFF
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Auth Login	Use username and password authentication	OFF
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

4.5.6 DDNS

This section allows you to set the DDNS parameters. DDNS, the full name of dynamic domain name server, is the dynamic domain name service. DDNS service allows you to map a dynamic IP address to a fixed domain name resolution service. Each time a user connects to the network, the client program will transmit the dynamic IP address

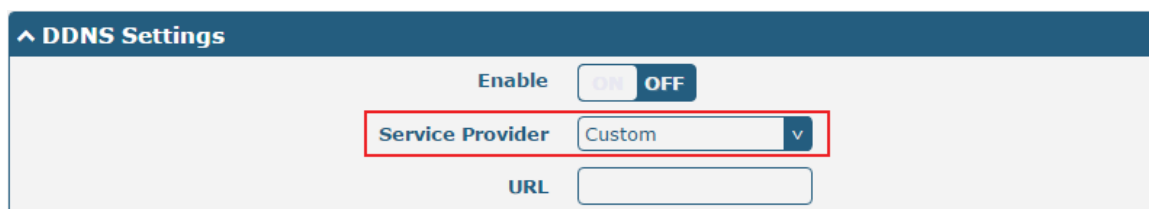
of the host to the server program located on the server host. The server program is responsible for providing DNS service and realizing dynamic domain name resolution, that is, DDNS service allows you to provide dynamic w for the host. An IP assigns a fixed domain name, and other users can access your host directly through this fixed domain name, rather than through the dynamic Wan IP address. The router's dynamic Wan IP address is assigned directly by the ISP.

Click **Service > DDNS** to set the parameters related to DDNS. and its service provider defaults to DynDNS.



The screenshot shows the 'DDNS' tab selected in the top navigation bar. Below it, the 'Status' tab is active. The 'DDNS Settings' section contains an 'Enable' toggle set to 'ON'. The 'Service Provider' dropdown menu is highlighted with a red box and shows 'DynDNS' selected. Below this are input fields for 'Hostname', 'Username', and 'Password'.

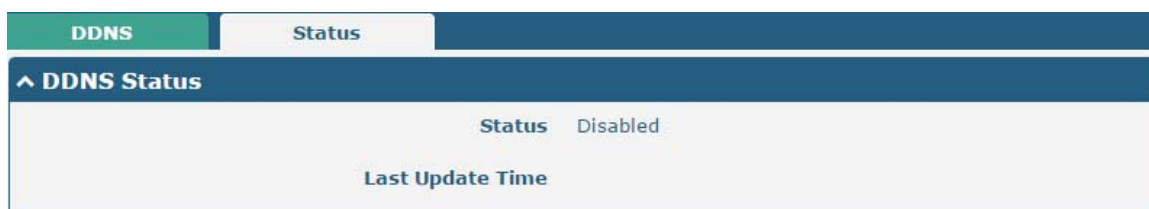
When service provider chose "Custom", the window is displayed as below.



The screenshot shows the 'DDNS Settings' section with the 'Service Provider' dropdown menu highlighted by a red box and set to 'Custom'. Below it is a 'URL' input field.

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

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



The screenshot shows the 'Status' tab selected in the top navigation bar. Below it, the 'DDNS Status' section displays 'Status' as 'Disabled' and 'Last Update Time' as empty.

DDNS Status

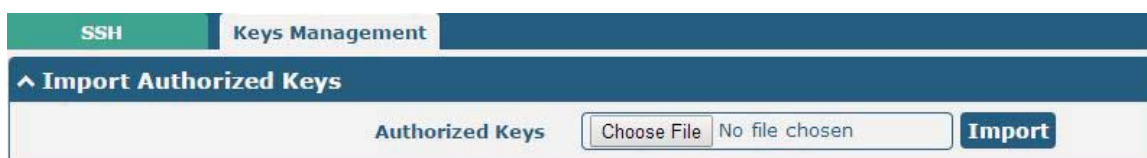
Item	Description
Status	Display the current status of the DDNS.
Last Update Time	Display the date and time for the DDNS was last updated successfully.

4.5.7 SSH

Router supports SSH password access and secret-key access.



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



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.

4.5.8 GPS (Optional)

This section allows you to configure the GPS parameters. The GPS function of the router can locate and obtain the location information of the device and report it to the designated server. R1520 does not have an independent GPS module. The positioning data comes from the cellular module. Whether the GPS function is supported depends on the cellular module.

GPS

Status

Map

^ General Settings

Enable GPS

ON OFF

Sync GPS Time

ON OFF

^ RS232 Report Settings

Report to RS232

ON OFF

Report GGA Sentence

ON OFF

Report VTG Sentence

ON OFF

Report RMC Sentence

ON OFF

Report GSV Sentence

ON OFF

^ GPS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	
							+

^ Advanced Settings

Add SN as GPSID

ON OFF ?

Self-define GPSID Prefix

?

GPS		
Item	Description	Default
General Settings		
Enable	Click the toggle button to ON to enable GPS.	OFF
Synchronized GPS Time	Click the toggle button to ON to synchronize GPS time.	OFF
RS232 Report Data Settings		
Reporting data through RS232	Reporting GPS Information by RS232.	OFF
Reporting GGA Information	Reporting GGA Information.	OFF
Reporting VTG Information	Reporting VTG Information.	OFF
Reporting RMC Information	Reporting RMC Information.	OFF
Reporting GSV Information	Reporting GSV Information.	OFF

Click the Add button in the GPS server window, and its protocol is "TCP client" by default as shown below:

GPS

^ Server Settings

Index

1

Enable

ON OFF

Protocol

TCP Client

v

Server Address

Server Port

Send GGA Sentence

ON OFF

Send VTG Sentence

ON OFF

Send RMC Sentence

ON OFF

Send GSV Sentence

ON OFF

When "TCP server" is selected as the protocol, the window is displayed as follows:

GPS

^ Server Settings

Index

1

Enable

ON OFF

Protocol

TCP Server

v

Local Address

Local Port

Send GGA Sentence

ON OFF

Send VTG Sentence

ON OFF

Send RMC Sentence

ON OFF

Send GSV Sentence

ON OFF

When "UDP" is selected as the protocol, the window is displayed as follows:

GPS

^ Server Settings

Index

Enable ☒ ON ☐ OFF

Protocol

Server Address

Server Port

Send GGA Sentence ☐ ON ☒ OFF

Send VTG Sentence ☐ ON ☒ OFF

Send RMC Sentence ☐ ON ☒ OFF

Send GSV Sentence ☐ ON ☒ OFF

GPS Data Forwarding Settings

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to "ON" to enable the GPS data forwarding settings.	ON
Protocol	Select "TCP client", "TCP server" or "UDP" as the protocol. <ul style="list-style-type: none"> TCP Client: When the router acts as a TCP client, it starts up with the TCP server (GPS server). The address of the server supports both IP and domain name. TCP server: The router acts as a TCP server (GPS server) and listens for connection requests from TCP clients. UDP: Router as a UDP client. 	TCP Client
Server address @TCP client	Set the address of the TCP server.	Null
Server port @TCP client	Set the port of the remote TCP server	Null
Local address	Set the local address of the router as a TCP server.	Null
Local port	Set the local port of the router as a TCP server.	Null
Server address @UDP	Set the address of the TCP server	Null
Server port @UDP	Set the port of the remote TCP server.	Null
Send GGA information	Send GGA information in NMEA format	OFF
Send VTG information	Send VTG information in NMEA format	OFF
Send RMC information	Send RMC information in NMEA format	OFF

GPS Data Forwarding Settings		
Item	Description	Default
Send GSV information	Send GSV information in NMEA format	OFF

^ Advanced Settings

Add SN as GPSID 

Self-define GPSID Prefix 

Advanced Settings		
Item	Description	Default
Add SN as GPSID	Click the switch button to enable/disable this option. When enabled, SN is appended to the NMEA message as a GPSID before transmission.	OFF
Self-define GPSID Prefix	Customize the GPSID prefix with four uppercase letters	Null

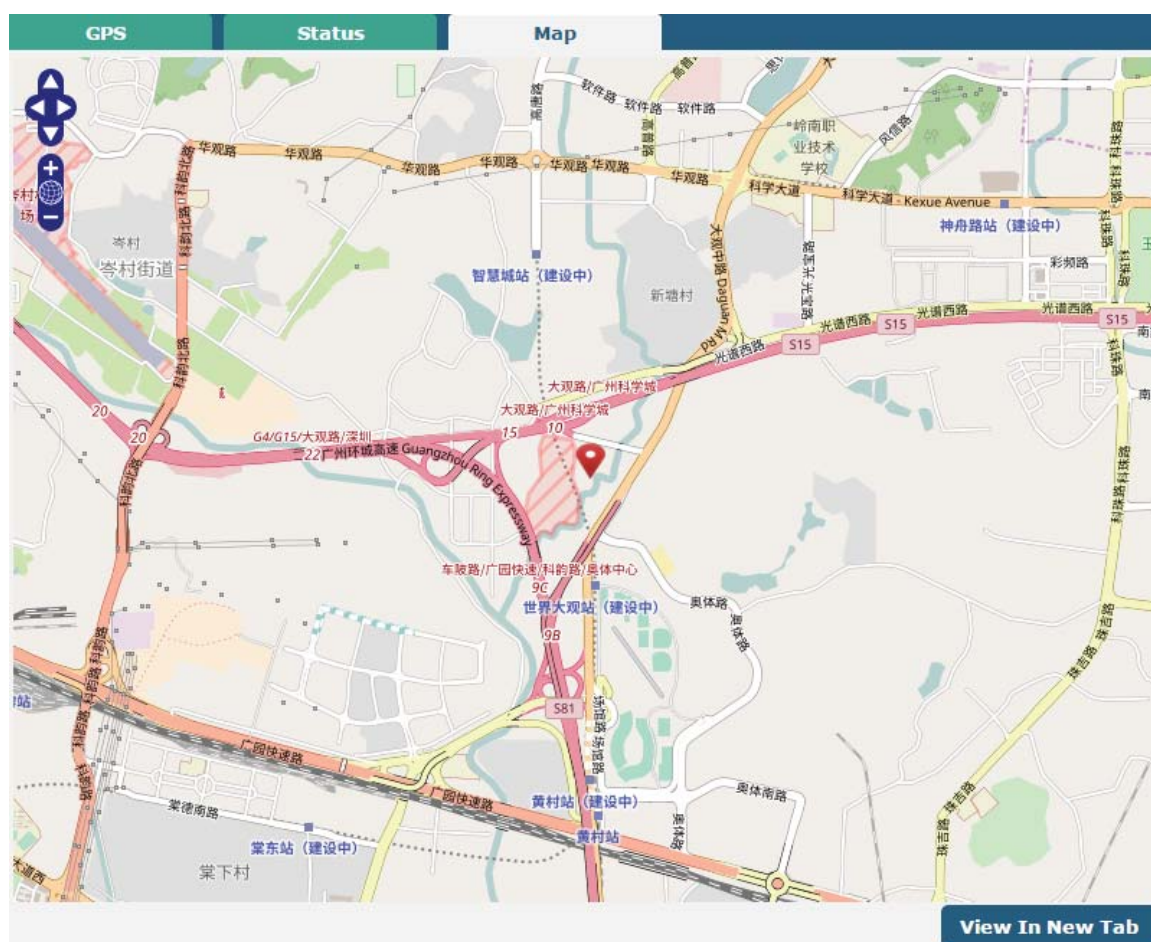
Click the "Status" column to view the current GPS status of the gateway;

GPS	Status	Map
^ GPS Status		
<div> <div>Status</div> <div>Not Fixed</div> </div>		
<div> <div>UTC Time</div> <div>2017-09-15 07:18:23</div> </div>		
<div> <div>Last Fixed Time</div> <div>2017-09-14 12:36:58 UTC</div> </div>		
<div> <div>Satellites In Use</div> <div>4</div> </div>		
<div> <div>Satellites In View</div> <div>12</div> </div>		
<div> <div>Latitude</div> <div>23.1534988</div> </div>		
<div> <div>Longitude</div> <div>113.4013826</div> </div>		
<div> <div>Altitude</div> <div>29.0 m</div> </div>		
<div> <div>Speed</div> <div>1.947 m/s</div> </div>		

GPS Status	
Item	Description
Status	Shows the current GPS status of the router.
UTC	Shows the UTC of satellite. Note: UTC is the world's unified time, not local time.
Final positioning time	The time of the last successful positioning.

GPS Status	
Item	Description
Number of satellites used	Number of satellites used
Number of visible satellites	Number of visible satellites
Latitude	Shows the Latitude information of the router.
Longitude	Shows the longitude information of the router.
Height	Shows the height information of the router.
Speed	Shows the speed information of the router.

Click the "Map" bar to view the current geographic positioning of the gateway.



4.5.9 Web Server

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

Web Server

Certificate Management

^ General Settings

HTTP Port

80

?

HTTPS Port

443

?

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

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

Web Server

Certificate Management

^ Import Certificate

Import Type

CA

v

HTTPS Certificate

Choose File

No file chosen

Import

Import Certificate		
Item	Description	Default
Import Type	Select from "CA" and "Private Key". <ul style="list-style-type: none"> 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.	--

4.5.10 Advanced

This section allows you to set the Advanced and parameters. Advanced router settings include system settings and restart.

System

Reboot

^ System Settings

Device Name

router

?

User LED Type

None

v

?

System

Reboot

^ System Settings

Device Name

router

?

User LED Type

None

None

SIM

OpenVPN

IPSec

?

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

System

Reboot

^ Periodic Reboot Settings

Periodic Reboot

0

?

Daily Reboot Time

?

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

4.6 System

4.6.1 Debug

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

Syslog

Syslog Details

Log Level

Debug

▼

Filtering

?

```

Feb 27 14:29:07 router user.debug link_manager[842]: target link WWAN1, state Connected
Feb 27 14:29:07 router user.info link_manager[842]: WWAN1 ping test success
Feb 27 14:29:23 router user.debug modemd[876]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A01807CBE54C163A883508F0A02806C83901A884C8BC18F0
A03804FEF6C11670D52A18F0C0480624B673A84254E1A53858F0A05806D4191CF4E13533A8F0A0680727960E0793C5305"
Feb 27 14:31:23 router user.debug modemd[876]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A01807CBE54C163A883508F0A02806C83901A884C8BC18F0
A03804FEF6C11670D52A18F0C0480624B673A84254E1A53858F0A05806D4191CF4E13533A8F0A0680727960E0793C5305"
Feb 27 14:33:23 router user.debug modemd[876]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A01807CBE54C163A883508F0A02806C83901A884C8BC18F0
A03804FEF6C11670D52A18F0C0480624B673A84254E1A53858F0A05806D4191CF4E13533A8F0A0680727960E0793C5305"
Feb 27 14:34:07 router user.debug link_manager[842]: WWAN1 (wwan) start ping test
Feb 27 14:34:07 router user.debug rping[16182]: start ping 8.8.8.8 (wwan)
Feb 27 14:34:07 router user.debug rping[16182]: PING 8.8.8.8 (8.8.8.8) from 10.122.74.11: 16 data bytes
Feb 27 14:34:07 router user.debug rping[16182]: 24 bytes from 8.8.8.8: seq=0 ttl=52 time=324.080 ms
Feb 27 14:34:07 router user.debug rping[16182]:
Feb 27 14:34:07 router user.debug rping[16182]: -- 8.8.8.8 ping statistics --
Feb 27 14:34:07 router user.debug rping[16182]: 1 packets transmitted, 1 packets received, 0% packet loss
Feb 27 14:34:07 router user.debug rping[16182]: round-trip min/avg/max = 324.080/324.080/324.080 ms
Feb 27 14:34:07 router user.debug link_manager[842]: rcv action ping_success from rping
Feb 27 14:34:07 router user.debug link_manager[842]: target link WWAN1, state Connected
Feb 27 14:34:07 router user.info link_manager[842]: WWAN1 ping test success
Feb 27 14:35:23 router user.debug modemd[876]: +CUSATP:
"D064810301250082028182850F80005500530049004D53615E9475288F0A01807CBE54C163A883508F0A02806C83901A884C8BC18F0
A03804FEF6C11670D52A18F0C0480624B673A84254E1A53858F0A05806D4191CF4E13533A8F0A0680727960E0793C5305"

```

Manual Refresh

▼

Clear

Refresh

Syslog Files

Index	File Name	File Size	Modification Time
1	messages	112612	Mon Feb 27 14:35:23 2017

System Diagnostic Data

System Diagnostic Data

Generate

System Diagnostic Data

Download

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

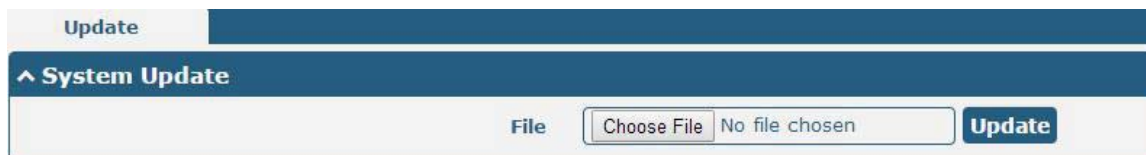
	selecting “manual refresh”, you should click the refresh button to refresh the syslog.
Clear	Click the button to clear the syslog.
Refresh	Click the button to refresh the syslog.
Syslog Files	
Syslog Files List	Only when logging is turned on in Services > system log > system log settings can log files be displayed in this list. The log generates a file with the size of 200K, which can display up to six system log files. Five files named messages0 ~ messages4 are old logs, and the latest system log file messages will be set at the top.
System Diagnosing Data	
Generate	Click to generate the syslog diagnosing file.
Download	Click to download system diagnosing file.

4.6.2 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.



The screenshot shows the 'Update' tab selected in the top navigation bar. Below it, the 'System Update' section is active. It features a 'File' label, a 'Choose File' button, a text field displaying 'No file chosen', and an 'Update' button.

4.6.3 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.



The screenshot shows the 'App Center' tab selected in the top navigation bar. Below it, a yellow banner provides a link for more information: <http://www.robustel.com/products/app-center/>. The 'App Install' section is active, featuring a 'File' label, a 'Choose File' button, a text field displaying 'No file chosen', and an 'Install' button.

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

^ Installed Apps				
Index	Name	Version	Status	Description
1	language_chinese	051101	Stopped	Chinese language

App Center		
Item	Description	Default
App Install		
Install to SD card	Click the toggle button to enable/disable the ability to install the app to the SD card.	OFF
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.	--
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
Location	Show the installation path.	Null
Description	Show the description for this App.	Null

4.6.4 Tools

This section provides users three tools: Ping, Traceroute and Sniffer. The Ping tool is used to detect the network connectivity of the router.

Ping
Traceroute
Sniffer

^ Ping

IP Address

Number of Request

Timeout

Local IP

Start
Stop

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

Ping
Traceroute
Sniffer

Traceroute

Trace Address

Trace Hops

Trace Timeout

Start Stop

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

Ping
Traceroute
Sniffer


Sniffer

Interface

Host



Packets Request







Protocol

Status 

Start Stop

Capture Files

Index	File Name	File Size	Modification Time	
1	18-04-18_16-17-29.cap	24	Wed Apr 18 16:17:30 2018	 

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. The grab file will be displayed in the window. Click  to download the grab file and click  to delete the grab file.	--
	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

4.6.5 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

ON OFF ?

Ignore Invalid Settings

ON OFF ?

XML Configuration File

Choose File No file chosen

Import

Export Configuration File

Ignore Disabled Features

ON OFF ?

Add Detailed Information

ON OFF ?

Encrypt Secret Data

ON OFF ?

XML Configuration File

Generate

Default Configuration

Save Running Configuration as Default

Save ?

Restore to Default Configuration

Restore

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

Ignore Invalid Settings	Click the toggle button as “ON” to ignore invalid settings.	ON
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 “ON” 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.	ON
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 Save button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore 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
-------	-----------	-----------	-------------------

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

4.6.6 User Management

This section allows you to change your username and password, and create or manage user accounts. One 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,If you do not want to change username, leave it blank. 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, \$, ., *, !, -	Null
Old Password	Enter the old password of your router. The default is "admin",5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, \$, ., *, !, -	Null
New Password	Enter a new password you want to create, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, \$, ., *, !, -	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". <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	Visitor
Username	Set the Username, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, \$, ., *, !, -	Null
Password	Set the password, 5-32 characters, valid characters: a-z, A-Z, 0-9, @, #, \$, ., *, !, -	Null

Chapter 5 Configuration Examples

5.1 Cellular

5.1.1 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 “Cold Backup” as the backup mode then click “Submit”.

Note: In the cold backup mode, when WWAN1 is the primary link, all data will be selected as WWAN1 for transmission, and WWAN2 will always be offline as the backup link; when WWAN1 is disconnected, the data will be switched to WWAN2 for transmission

Link Manager

Status

^ General Settings

Primary Link

WWAN1

v

?

Backup Link

WWAN2

v

Backup Mode

Cold Backup

v

?

Revert Interval

0

?





Emergency Reboot


ON

OFF

?

^ Link Settings

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

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

Link Manager

Status

^ General Settings

Index

1

Type

WWAN1

v

Description

^ WWAN Settings

Automatic APN Selection

ON OFF

Dialup Number

*99***1#

Authentication Type

Auto v

Switch SIM By Data Allowance

ON OFF ?

Data Allowance

0 ?

Billing Day

1 ?

^ Ping Detection Settings

?

Enable

ON OFF

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300 ?

Retry Interval

5 ?

Timeout

3 ?

Max Ping Tries

3 ?

^ Advanced Settings

NAT Enable

ON OFF

Upload Bandwidth

10000 ?

Download Bandwidth

10000

Overrided Primary DNS

Overrided 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 right most of edit button  of SIM1 to set its parameters according to your application request.

Cellular

^ General Settings

Index

1

SIM Card

SIM1

v

Phone Number

PIN Code

?

Extra AT Cmd

?

Telnet Port

0

?

^ Cellular Network Settings

Network Type

Auto

v

?

Band Select Type

All

v

?

^ Advanced Settings

Debug Enable

ON

OFF

Verbose Debug Enable

ON

OFF

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

5.1.2 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-- **Password;cmd1;cmd2;cmd3;... cmdn** (available when the SMS was sent from the phone number which had been added in R1520's phone group).
3. Both mode-- **Username:Password;cmd1;cmd2;cmd3;...cmdn** (available when the SMS was sent from the phone number).

Note: All command symbols must be entered in the English input half angle mode.

SMS command Explanation:

1. Password: The SMS control password defaults to the login password of the super user or the login password of the ordinary user who has read and write permissions.
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 6 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**, Select export type as "complete", 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 checked="" type="checkbox"/> ON <input 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 checked="" type="checkbox"/> ON <input 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>172.16.24.24</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS cmd:

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

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

4. E.g.

Password mode—**admin:admin;status system**

In this command, username is “admin”, password is “admin”, The control command is status system, and the function of the command is to get the system status.

SMS received:

```
hardware_version = 1.1
firmware_version = 3.1.0
firmware_version_full = "3.1.0 (Rev 3199)"
kernel_version = 4.9.152
device_model = R1520
serial_number = ""
uptime = "0 days, 00:02:55"
```

```
system_time = "Thu May 14 05:51:56 2020 (NTP not updated)"
```

```
ram_usage = "75M Free/128M Total"
```

```
admin:admin;reboot
```

In this command, username is "admin", password is "admin", and the command is to reBoot the R1520 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 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500
```

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

SMS received:

OK

OK

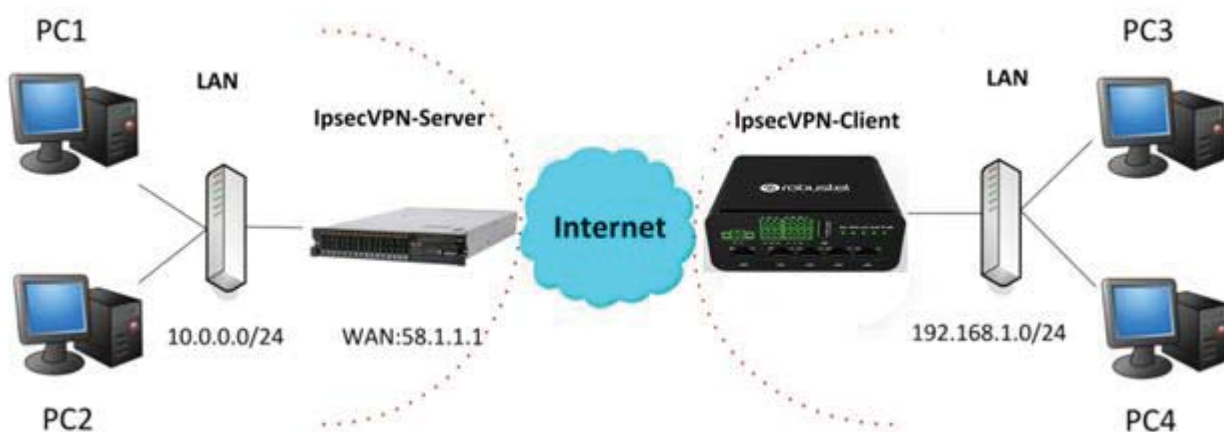
OK

OK

5.2 VPN Configuration Example

5.2.1 IPsec VPN

IPSec VPN sample topology (configuration of lke and SA parameters of server and client must be consistent):



IPsec VPN_Server:

Cisco 2811:

```

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

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

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

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

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

```

IPsec VPN_Client:

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

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

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

Tunnel

^ General Settings

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

^ IKE Settings

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

SA Settings

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

Advanced Settings

Enable Compression	ON	OFF	
Enable Forceencaps	ON	OFF	?
Expert Options		?	

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

The comparison between IPsec Server and Client is as below.

Server (Cisco 2811)

```

Router#enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
authentication  Set authentication method for protection suite
encryption      Set encryption algorithm for protection suite
exit            Exit from ISAKMP protection suite configuration mode
group           Set the Diffie-Hellman group
hash            Set hash algorithm for protection suite
lifetime        Set lifetime for ISAKMP security association
no             Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash sha1
Router(config-isakmp)#authentication gex-sha256
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp 7
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 7
security-association Security association parameters
transform-set Define transform and settings
Router(config)#crypto ipsec transform-set Tset1
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 (64 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 Tset1 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 Tset1
Router(config-crypto-map)#set peer 100.100.1.1
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)#no
Router(config-if)#crypto map cry-map
*Jan 8 07:16:24.785: %CRYPTO-4-ISAKMP_ON_OFF: ISAKMP is ON

```

Tunnel

Tunnel Settings

Index	
Enable	ON
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0
Remote Subnet	255.255.255.0

IKE Settings

Negotiation Mode	Main
Authentication Algorithms	MD5
Encrypt Algorithms	3DES
IKE DH Group	MODP(1024)
Authentication Type	PSK
PSK Secret	*****
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

SA Settings

Encrypt Algorithms	3DES
Authentication Algorithms	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

Advanced Settings

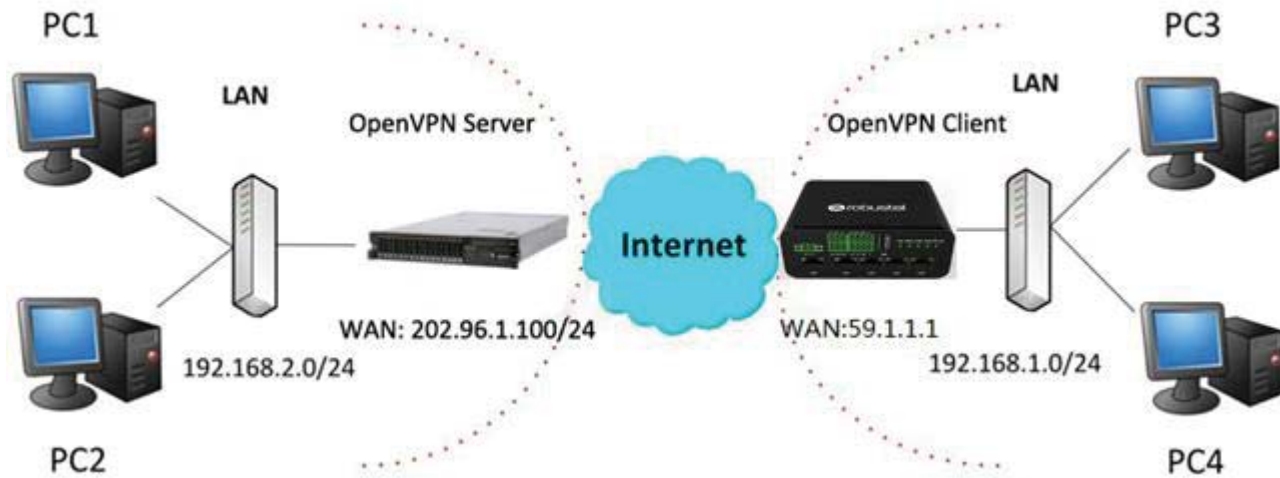
Enable Compression	OFF
--------------------	-----

IKE Setting in Client must be consistent with server.

SA Setting in Client must be consistent with server.

5.2.2 OpenVPN

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



The configuration of two points is as follows.

OpenVPN_Server:

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

```
local 202.96.1.100
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert Server01.crt
key Server01.key
dh dh1024.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.3.0 255.255.255.0"
client-config-dir ccd
route 192.168.1.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
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: 1

Enable: ☒ ON ☐ OFF

Description:

Mode: Client

Protocol: UDP

Peer Address:

Peer Port: 1194

Interface Type: TUN

Authentication Type: None

Encrypt Algorithm: BF

Authentication Algorithm: SHA1

Renegotiation Interval: 86400

Keepalive Interval: 20

Keepalive Timeout: 120

TUN MTU: 1500

Max Frame Size:

Enable Compression: ☒ ON ☐ OFF

Enable NAT: ☐ ON ☒ OFF

Enable DNS overrid: ☐ ON ☒ OFF

Verbose Level: 0

^ Advanced Settings

Enable HMAC Firewall: ☐ ON ☒ OFF

Enable PKCS#12: ☐ ON ☒ OFF

Enable nsCertType: ☐ ON ☒ OFF

Expert Options:

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

5.2.3 GRE VPN

GRE VPN example topology:



The configuration of two points is as follows.

GRE-1:

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

GRE			
Status			
^ Tunnel Settings			
Index	Enable	Description	Remote IP Address

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-2 as below.

^ Tunnel Settings

Index
1

Enable
ON OFF

Description
GRE-2

Remote IP Address
58.1.1.1

Local Virtual IP Address
10.8.0.2

Remote Virtual IP Address
10.8.0.1

Enable Default Route
ON OFF

Enable NAT
ON OFF

Secrets

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
<div> ^ Tunnel Settings </div> <div> Index 1 </div> <div> Enable ON OFF </div> <div> Description GRE-1 </div> <div> Remote IP Address 59.1.1.1 </div> <div> Local Virtual IP Address 10.8.0.1 </div> <div> Remote Virtual IP Address 10.8.0.2 </div> <div> Enable Default Route ON OFF </div> <div> Enable NAT ON OFF </div> <div> Secrets ***** </div>	<div> ^ Tunnel Settings </div> <div> Index 1 </div> <div> Enable ON OFF </div> <div> Description GRE-2 </div> <div> Remote IP Address 58.1.1.1 </div> <div> Local Virtual IP Address 10.8.0.2 </div> <div> Remote Virtual IP Address 10.8.0.1 </div> <div> Enable Default Route ON OFF </div> <div> Enable NAT ON OFF </div> <div> Secrets ***** </div>

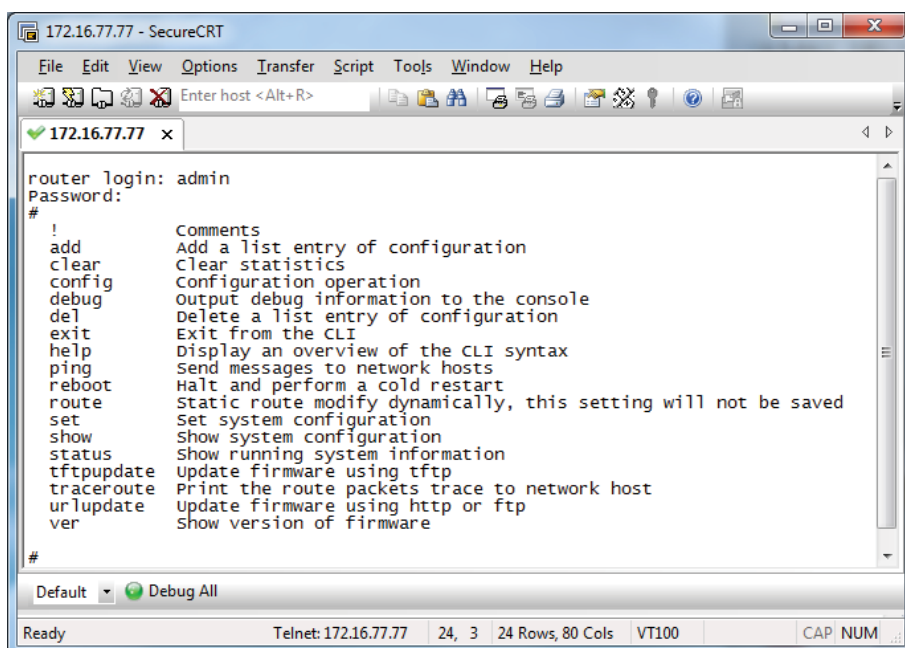
GRE-1 public IP: 59.1.1.1
GRE-1 tunnel IP: 10.8.0.1
GRE-2 tunnel IP: 10.8.0.2
GRE-2 public IP: 58.1.1.1
GRE-2 tunnel IP: 10.8.0.1
GRE-1 tunnel IP: 10.8.0.2

set the same secret as GRE-2
set the same secret as GRE-1

Chapter 6 Introductions for CLI

6.1 What Is CLI

The Command Line Interface (CLI) is a set of software interfaces that provide another way to configure device parameters. Users can connect to the router through SSH or telnet to configure CLI commands. After establishing a Telnet or SSH connection with the router, enter the login account and password (default admin/admin) to enter the router's configuration mode, as shown below.



Router login:

Router login: admin

Password: admin

#

CLI commands:

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

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ovpn_cert_get	Download OpenVPN certificate file via http or ftp

ping	Send messages to network hosts
reboot	Halt and perform a cold restart
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware or configuration file using tftp
traceroute	Print the route packets trace to network host
trigger	Trigger action
urlupdate	Update firmware via http or ftp
ver	Show version of firmware

6.2 How to Configure the CLI

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

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

6.3 Commands Reference

Commands	Syntax	Description
Debug	Debug <i>parameters</i>	enable on or disenable the 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: More detail about CLI command, please refer to “Command Line Interface Guide”.

6.4 Quick Start with Configuration ExampleS

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

Example 1: Show current version

```
# status system
hardware_version = 1.1
firmware_version = 3.1.0
firmware_version_full = "3.1.0 (Rev 3199)"
kernel_version = 4.9.152
device_model = R1520
serial_number = ""
uptime = "0 days, 00:06:51"
system_time = "Thu May 14 05:55:52 2020 (NTP not updated)"
ram_usage = "74M Free/128M Total"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
firmware New firmware
# tftpupdate firmware (space+?)
String Firmware name
# tftpupdate firmware r1520-firmware-3.1.0.ruf host 192.168.100.99 // enter a new firmware name
Downloading
r1520-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 // make you configuration effect after reboot
```

Example 3: Set link-manager

```
# set
# set (space+?)
ai AI
cellular Cellular
```

ddns	DDNS
dido	DIDO
email	Email
ethernet	Ethernet
event	Event Management
firewall	Firewall
gps	GPS
gre	GRE
ip_passthrough	IP Passthrough
ipsec	IPSec
lan	Local Area Network
link_manager	Link Manager
ntp	NTP
openvpn	OpenVPN
reboot	Automatic Reboot
route	Route
serial_port	Serial Port
sms	SMS
ssh	SSH
syslog	Syslog
system	System
usb	USB
user_management	User Management
web_server	Web Server
wifi	WiFi AP
# set link_management	
primary_link	Primary Link
Backup_link	Backup Link
Backup_mode	BackSup Mode
emergency_reBoot	Emergency ReBoot
link	Link Settings
# set link_management primary_link (space+?)	
Enum Primary Link (wwan1/wwan2/wan/wlan)	
# set link_management 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_overrided	Overrided Primary DNS
dns2_overrided	Overrided Secondary DNS

```
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
  auto_apn           Automatic APN Selection
  apn                APN
  username           Username
  password           Password
  dialup_numBer      Dialup NumBer
  auth_type          Authentication Type
  aggressive_reset    Aggressive Reset
  switch_By_data_allowance Switch SIM By Data Allowance
  data_allowance      Data Allowance
  Billing_day         Billing Day
# set link_manager link 1 wwan switch_By_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100           //open cellular switch_by_data_traffic
OK                                                         //setting succeed
# set link_manager link 1 wwan Billing_day 1                 //setting specifies the day of month for billing
OK                                                         //setting succeed
...
# config save_and_apply
OK                                                         //save and apply current configuration, make you configuration effect
```

Example 4: Set Ethernet

```
# set Ethernet port_setting 2 port_assignment lan0           //Set Table 2 (eth1) to lan0
OK
# config save_and_apply           //make you configuration effect
OK
```

Example 5: Set LAN IP address

```
# show lan all
network {
  id = 1
  interface = lan0
  ip = 192.168.0.1
  netmask = 255.255.255.0
  mtu = 1500
  dhcp {
```

```

    152umber = 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 = ""
    152umbe_enaBle = false
}
}
multi_ip {
    id = 1
    interface = lan0
    ip = 172.16.24.24
    netmask = 255.255.0.0
}
#
# set lan
network      Network Settings
multi_ip     Multiple IP Address Settings
vlan         VLAN
# set lan network 1(space+?)
interface    Interface
ip           IP Address
netmask      Netmask
mtu          MTU
dhcp         DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24           //set IP address for lan
OK                                           //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                           //save and apply current configuration, make you configuration
effect

```


Example 6: CLI for setting Cellular

```
# show cellular all
```

```
sim {  
    id = 1  
    card = sim1  
    phone_numBer = ""  
    extra_at_cmd = ""  
    network_type = auto  
    Band_select_type = all  
    Band_gsm_850 = false  
    Band_gsm_900 = false  
    Band_gsm_1800 = false  
    Band_gsm_1900 = false  
    Band_wcdma_850 = false  
    Band_wcdma_900 = false  
    Band_wcdma_1900 = false  
    Band_wcdma_2100 = false  
    Band_lte_800 = false  
    Band_lte_850 = false  
    Band_lte_900 = false  
    Band_lte_1800 = false  
    Band_lte_1900 = false  
    Band_lte_2100 = false  
    Band_lte_2600 = false  
    Band_lte_1700 = false  
    Band_lte_700 = false  
    Band_tdd_lte_2600 = false  
    Band_tdd_lte_1900 = false  
    Band_tdd_lte_2300 = false  
    Band_tdd_lte_2500 = false  
}  
sim {  
    id = 2  
    card = sim2  
    phone_numBer = ""  
    extra_at_cmd = ""  
    network_type = auto  
    Band_select_type = all  
    Band_gsm_850 = false  
    Band_gsm_900 = false  
    Band_gsm_1800 = false  
    Band_gsm_1900 = false  
    Band_wcdma_850 = false  
    Band_wcdma_900 = false  
    Band_wcdma_1900 = false
```

```

    Band_wcdma_2100 = false
    Band_lte_800 = false
    Band_lte_850 = false
    Band_lte_900 = false
    Band_lte_1800 = false
    Band_lte_1900 = false
    Band_lte_2100 = false
    Band_lte_2600 = false
    Band_lte_1700 = false
    Band_lte_700 = false
    Band_tdd_lte_2600 = false
    Band_tdd_lte_1900 = false
    Band_tdd_lte_2300 = false
    Band_tdd_lte_2500 = false
}
# set(space+?)
ai          AI
cellular    Cellular
ddns        DDNS
dido        DIDO
email       Email
ethernet    Ethernet
event       Event Management
firewall    Firewall
gps         GPS
gre         GRE
ip_passthrough IP Passthrough
ipsec       IPSec
lan         Local Area Network
link_manager Link Manager
ntp         NTP
openvpn     OpenVPN
reboot      Automatic Reboot
route       Route
serial_port Serial Port
sms         SMS
ssh         SSH
syslog      Syslog
system      System
usb         USB
user_management User Management
web_server  Web Server
wifi        WiFi AP
# 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
--------------	--------------

pin_code	PIN Code
----------	----------

extra_at_cmd	Extra AT Cmd
--------------	--------------

telnet_port	Telnet Port
-------------	-------------

network_type	Network Type
--------------	--------------

band_select_type	Band Select Type
------------------	------------------

band_settings	Band Settings
---------------	---------------

telit_band_settings	Band Settings
---------------------	---------------

debug_enable	Debug Enable
--------------	--------------

verbose_debug_enable	Verbose Debug Enable
----------------------	----------------------

```
OK
```

```
...
```

```
# config save_and_apply
```

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

Glossary

Abbr.	Description
AC	Alternating Current
AI	Analog Input
APN	Access Point Name of GPRS Service Provider Network
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
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 Identification
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
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Rubber antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct Current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio

Abbr.	Description
WAN	Wide Area Network

Guangzhou Robustel LTD

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

Tel: 86-20-29019902

Email: info@robustel.com

FCC/ISED Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

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

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

This device complies with Innovation, Science and Economic Development Canada licence-exempt RSS standard (s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le onjunc areil est conforme aux CNR d' l'innovation, la science et le développement économique Canada licables aux areils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

(1) l'areil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, onj si le brouillage est susceptible d'en compromettre le fonctionnement.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Tous les changements ou modifications non expressément approuvée par le responsable de la conformité pourrait vider l'utilisateur est habilité à exploiter l'équipemen.

ISED Radiation Exposure Statement:

This equipment complies with ISED RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

IC exposition aux radiations:

Cet yuipement est conforme avec ISED les limites d'exposition aux rayonnements dyinies pour un contr environnement.

Cet yetteur ne doit pas yre co-localisỹ ou fonctionner en conjonction avec une autre antenne ou yetteur. Cet yuipement doit yre install?et utilisỹvec une distance minimale de 20cm entre leradiateur & votre corps.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

This transmitter must not be coỹlocated or operating in conjunction with any other antenna or transmitter.

This equipment should be installed and operated with minimum distance 20cm between the radiator &you body.