

# Robustel GoRugged R2000

Dual SIM Industrial Cellular VPN Router

For GPRS/EDGE/UMTS/HSPA+/4G LTE Networks

## User Guide

Document Name:	<b>User Guide</b>
Firmware:	<b>1.2.2</b>
Date:	<b>2016-04-18</b>
Status:	<b>Confidential</b>
Doc ID:	<b>RT_UG_R2000_v.1.2.2</b>



## **About This Document**

This document describes hardware and software of Robustel R2000, Dual SIM Industrial 2G/3G/4G Router.

**Copyright© Guangzhou Robustel Technologies Co., Limited  
All Rights Reserved.**

## **Trademarks and Permissions**

Robustel are trademark of Guangzhou Robustel Technologies Co., Limited.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **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 revision 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 Contact Information**

Tel: +86-020-23354618

Fax: +86-020-82321505

E-mail: [support@robustel.com](mailto:support@robustel.com)

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

**Important Notice**

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

**Safety Precautions****General**

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
  1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
  1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
  2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your 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 route 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/EC	Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)	
2012/19/EU	Directive 2012/19/EU the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE)	

**Table 2:** Standards of the Ministry of Information Industry of the People’s Republic of China

SJ/T 11363-2006	“Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products” (2006-06).	
SJ/T 11364-2006	<p>“Marking for Control of Pollution Caused by Electronic Information Products” (2006-06).</p> <p>According to the “Chinese Administration on the Control of Pollution caused by Electronic Information Products” (ACPEIP) the EPUP, i.e., Environmental Protection Use Period, of this product is 20 years as per the symbol shown here, unless otherwise marked. The EPUP is valid only as long as the product is operated within the operating limits described in the Hardware Interface Description.</p> <p>Please see <a href="#">Table 3</a> for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.</p>	

**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)
Metal Parts	o	o	o	o	o	o
Circuit Modules	x	o	o	o	o	o
Cables and Cable Assemblies	o	o	o	o	o	o
Plastic and Polymeric parts	o	o	o	o	o	o

o:  
Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

x:  
Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.

**Revision History**

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

Release Date	Firmware Version	Doc Version	Details
2015-09-7	1.1.0	V1.0.0	First Release
2015-10-08	1.1.0	V1.0.1	Update section: Selection and Ordering Data (Operating Environment)
2015-11-10	1.1.0	V1.1.1	Increase section: wifi specification and WiFi function explain Modify section: change logo
2015-12-01	1.1.0	V1.1.2	Modify section: Selection and Ordering Data (modify R2000-3P frequency band)
2015-12-15	1.2.0	V1.2.0	Update section: Status, Link manager, LAN, Ethernet, Cellular, WiFi, WLAN, Route, Device Configuration, SMS remote control, CLI
2016-02-18	1.2.0	V1.2.1	Update section: Reset button
2016-04-18	1.2.0	V1.2.2	Modify section: delete R2000-3H type and description; increase SNMP description; modify detective to certificate in Regulatory and Type Approvals section.

## Contents

Chapter 1	Product Concept.....	8
1.1	Overview .....	8
1.2	Packing List .....	9
1.3	Specifications .....	10
1.4	Dimensions.....	13
1.5	Selection and Ordering Data .....	13
Chapter 2	Installation.....	14
2.1	Overview .....	14
2.2	LED Indicators.....	15
2.3	Reset Button.....	16
2.4	Ethernet Port.....	16
2.5	Install SIM Card.....	16
2.6	Connect the External Antenna .....	17
2.7	Ground the Router .....	17
2.8	Mount the Router .....	17
2.9	Power Supply.....	18
Chapter 3	Configure Settings over Web Browser .....	19
3.1	Configuring PC in Windows 7 .....	19
3.2	Factory Default Settings .....	22
3.3	Login Router .....	22
3.4	Control Panel.....	23
3.5	Status.....	25
3.6	Interface->Link Manager .....	28
3.7	Interface->LAN .....	37
3.8	Interface->Ethernet.....	42
3.9	Interface->Cellular.....	42
3.10	Interface->WiFi (Optional) .....	45
WiFi AP .....		45
3.11	Interface->WLAN (Optional).....	50
WiFi Client .....		50
3.12	Network->Route .....	52
3.13	Network->Firewall.....	54
3.14	VPN->IPSec .....	57
3.15	VPN->OpenVPN.....	64
3.15	VPN->GRE .....	71
3.16	Services->Syslog .....	72
3.17	Services->Event .....	73
3.18	Services->NTP.....	76
3.19	Services->SMS .....	77
3.20	Services->DDNS.....	78
3.21	Services->VRRP.....	79
3.22	Services->SSH .....	80

3.23	Services->Robustlink (optional APP) .....	81
3.24	Services->Web Server.....	83
3.25	Services->SNMP (optional APP) .....	84
3.26	Services->Advanced .....	87
3.27	System->Debug .....	88
3.28	System->Update .....	89
3.29	System->APP Center.....	90
3.30	System->Tools.....	91
3.31	System->Profile .....	94
3.32	System->Device Configuration .....	95
3.33	System->User Management.....	95
Chapter 4	Configuration Examples .....	97
4.1	Cellular .....	97
4.1.1	Cellular Dial-Up.....	97
4.1.2	SMS Remote Control.....	99
4.2	Network.....	101
4.2.1	IPSEC VPN .....	101
4.2.2	OPENVPN .....	105
4.2.3	GRE VPN.....	108
Chapter 5	Introductions for CLI.....	110
5.1	What's CLI.....	110
5.2	How to Configure the CLI .....	111
5.3	Commands Reference .....	117
Glossary	.....	118



# Chapter 1 Product Concept

## 1.1 Overview

Robustel GoRugged R2000 is an enterprise-class cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

- Dual SIM redundancy for continuous cellular connections; supports 2G/3G/4G.
- Various interfaces: 2xLAN/ 1xLAN, 1xWAN.
- WAN: static, PPPOE and DHCP client.
- Multiple links backup and ICMP detection.
- VPN tunnel: IPSec/ OpenVPN/GRE.
- Auto reboot via SMS/ Timing.
- Flexible Management methods: Web/SMS/CLI.
- Firmware upgrade via Web/CLI/SMS.
- Advanced Firewall: filtering, port mapping, DMZ.
- Support DDNS.
- Support VRRP.
- Support SNMP report events which include system startup, system reboot, system time update etc.
- Wide range input voltages from 9 to 26 VDC.
- The metal enclosure can be mounted on a DIN-rail, on the wall or be put on desktop.
- Built-in Watchdog, Timer

## 1.2 Packing List

Check your package to make sure it contains the following items:

- Robustel R2000 Router



- 3-pin pluggable terminal block for power connector x 1



- CD with user guide x 1

**Note:** Please notify your sales representative if any of the above items are missing or damaged.

Optional accessories (can be purchased separately):

- Cellular SMA antenna (3G/4G)



- RP-SMA Wi-Fi antenna (Stubby antenna or Magnet antenna optional)

*Stubby antenna*

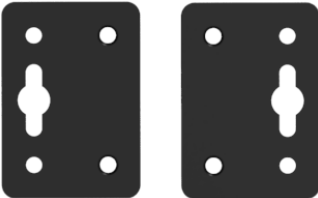
*Magnet antenna*



- Ethernet cable x 1



- Wall Mounting Kit x2



- 35mm Din-Rail mounting kit



- AC/DC Power Supply Adapter (12VDC, 1.5A) x 1 (EU, US, UK, AU plug optional)



## 1.3 Specifications

### Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS/HSPA+/FDD LTE
- FDD LTE: max. 150/50 Mbps (DL/UL)
- TDD LTE: max.112/10 Mbps (DL/UL)
- DC-HSPA+: 42/5.76 Mbps (DL/UL)
- HSPA+: max. 21.6/5.76 Mbps (DL/UL)
- EDGE: 236.8 kbps (DL/UL)

- GPRS: 85.6 kbps (DL/UL)
- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female(1xMAIN and 1xAUX)

### **Ethernet Interface**

- Number of Ports: 2xLAN or 1 x LAN, 1xWAN (10/100Mbps)
- Magnet Isolation Protection: 1.5KV

### **WLAN Interface (Optional)**

- Standards: 802.11b/g/n, support AP and Client mode
- Data speed: 2\*2 MIMO,300Mbps
- Frequency Band: 2.412 - 2.485 GHz
- Security: WEP, WPA, WPA2
- Encryption: 64/128 AES, TKIP
- Antenna Interface: RP-SMA Female

### **System**

- Reset button
- LED Indicators: RUN, PPP, USB, 3 x RSSI

### **CPU & Memory**

- CPU: 535MHz
- SDRAM: 64MB
- FLASH: 16MB

### **Software**

- Network protocols: PPP, TCP, UDP, DHCP, ICMP, NAT, DMZ, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, SNTP, Telnet, SNMP, etc.
- VPN tunnel: IPSec/OpenVPN/GRE
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, SMS

### **Power Supply and Consumption**

- Power Supply Interface: 3.5mm terminal block
- Input Voltage: 9 to 26 VDC
- Power Consumption: Idle: 100 mA @ 12 V

Data Link: 500 mA (peak) @ 12 V

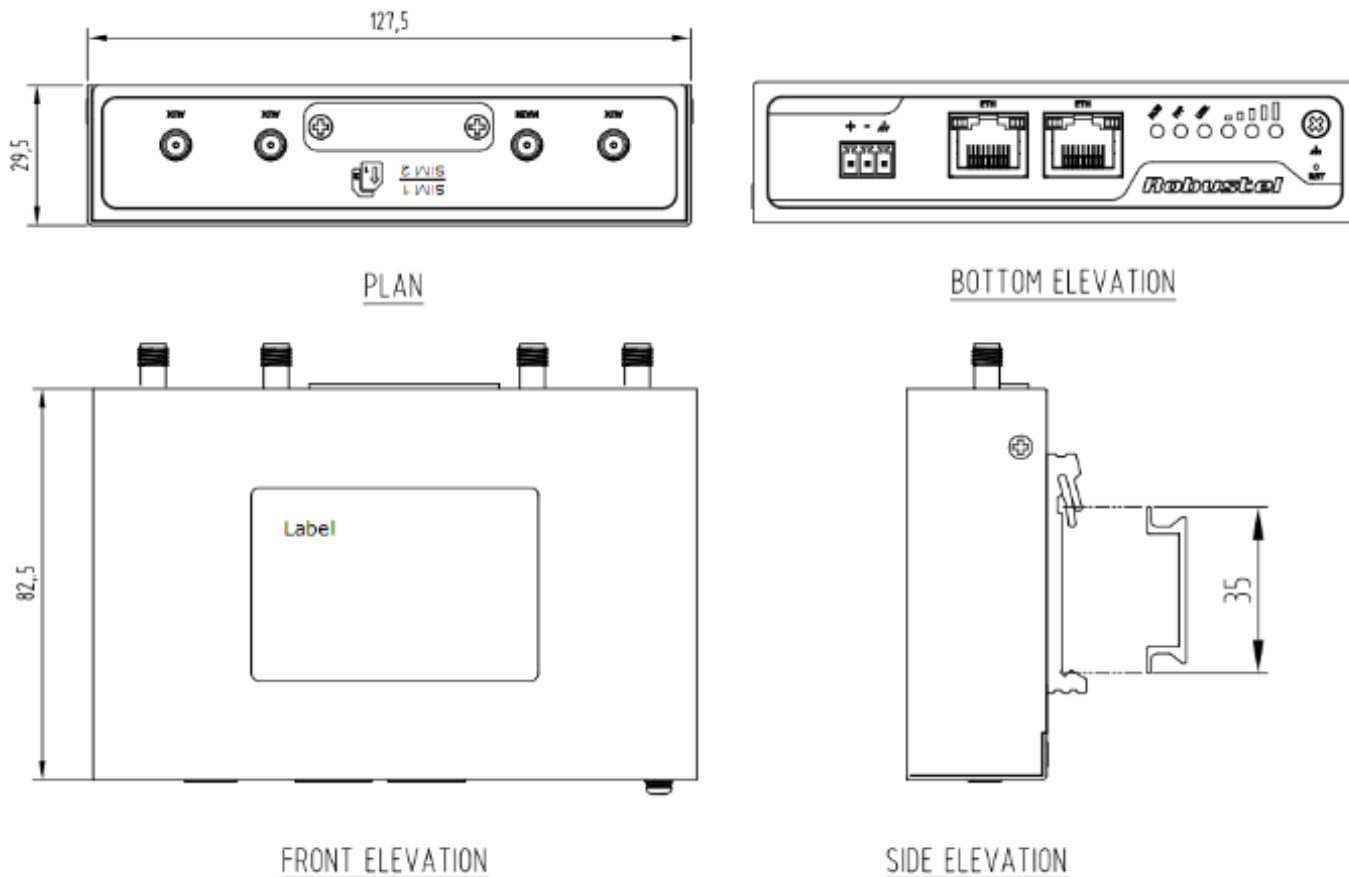
### **Physical Characteristics**

- Housing & Weight: Metal, 300g
- Dimension: (L x W x H): 127.5mm x 82.5mm x 29.5mm
- Installation: 35mm Din-Rail or wall mounting or desktop

### **Regulatory and Type Approvals**

- Approval & Certificate: CE, R&TTE, RoHS, WEEE
- EMI : EN 55022 (2006/A1: 2007) Class B
- EMC: EN 61000-4-2 (ESD) Level 3, EN 61000-4-3 (RS) Level 4  
EN 61000-4-4 (EFT) Level 3, EN 61000-4-5 (Surge) Level 3  
EN 61000-4-6 (CS) Level 3, EN 61000-4-8 Level 4

## 1.4 Dimensions



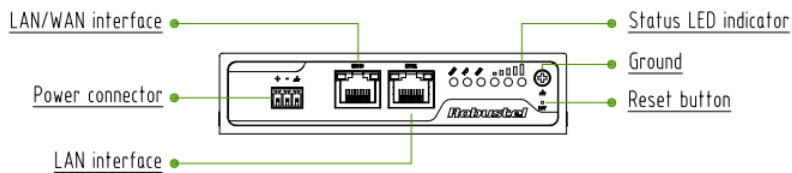
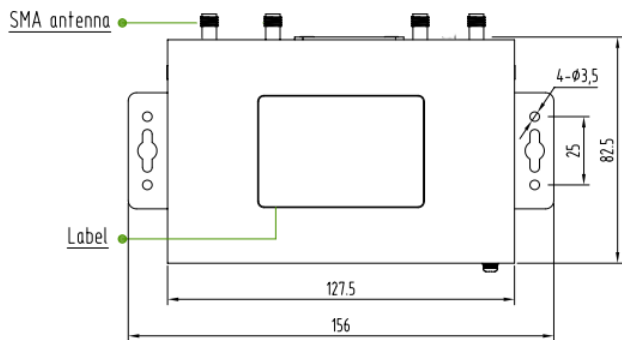
## 1.5 Selection and Ordering Data

Model No.	Frequency band	Operating Environment
R2000-3P	HSPA+: 2100/900 MHz or 2100/900/850 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz	-20 to +65°C/ 5 to 95% RH
R2000-4L	LTE FDD: B1, B2, B3, B4, B5, B7, B8, B20 LTE TDD: B38, B39, B40, B41 UMTS/DC-HSPA+/HSPA+/HSPA: 2100/1900/850/900/1800 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz	-20 to +65°C/ 5 to 95% RH


# Chapter 2 Installation

## 2.1 Overview

As shown in the following figures, R2000 router has two Ethernet ports (2xLAN or 1xLAN+1xWAN) and two cellular SIM card slots.



## 2.2 LED Indicators

Name	Color	Status	Function
RUN	Green	Blinking	Router is ready.
		On	Router is starting.
		Off	Router is power off.
PPP	Green	Blinking	PPP Indicator: Null
		On	PPP Indicator: PPP connection is up.
		Off	PPP Indicator: PPP connection is down.
USR	Green	Blinking	SIM: using backup SIM card. NET: register to a low level network.
		Off after blinking	SIM: working fine. NET: working fine.
		Light up	OpenVPN: OpenVPN is connected. IPSec: IPSec is connected. GRE: GRE is connected.
		Off after lighting up	OpenVPN: OpenVPN is disconnected. IPSec: IPSec is disconnected. GRE: GRE is disconnected.
	Green	On	Signal level: 21-31 (Perfect signal level).
	Yellow	On	Signal level: 11-20 (Average signal level).
	Red	On	Signal level: 1-10 (Exceptional signal level).
	When the network is disconnected, those three signal LEDs are designed as a binary combination code to indicate a series of error report. (Green Yellow Red) On: 1 Off: 0 001 AT command failed 010 no SIM card detected 011 it need to enter the PIN code 100 it need to enter the PUK code 101 registration failed 110 something wrong happened in the module		

**Note:** User can select display status of USR LED. For details please refer to 3.20 Service->Advanced section.



## 2.3 Reset Button

Function	Operation
Reboot	Push the button for 2~7 seconds under working status.
Restore to factory default setting	Power on the router, wait 5 seconds, and then keep pressing the "RST" button until six LEDs start to blink one by one circularly. Please release the pressing operation within 5 seconds. In this time the router loads default successfully.

## 2.4 Ethernet Port

There are two Ethernet ports in R2000 router, ETH1 is the LAN interface and ETH0 can be the LAN or WAN interface. The eth0 factory default is as LAN interface. Each Ethernet port has two LED indicators. The yellow one is **Link indicator** and the green one doesn't mean anything. There are three status of Link indicator. Please refer to the form below.

Indicator	Status	Description
Link Indicator	Off	Connection is down.
	On	Connection is up.
	Blink	Data is being transmitted

## 2.5 Install SIM Card

- **Remove slot cover**

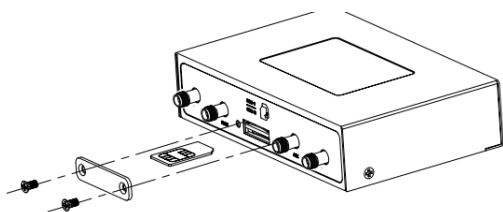
1. Make sure power supply is disconnected.
2. Use a screwdriver to unscrew the screw on the cover, and then remove the cover, you could find the SIM Card slots.

- **Inserting SIM Card**

3. Insert the SIM card, and you need press the card with your fingers until you hear "a cracking sound". Then use a screwdriver to screw the cover.

- **Removing SIM Card**

4. Make sure router is power off.
5. Press the card until you hear "a cracking sound", when the card will pop up to be pulled out.



**Note:**

1. *Recommended torque for inserting is 0.5N.m and the maximum torque is 0.7N.m.*
2. *Please use the specific M2M SIM card when the device works in extreme temperature (temperature exceeding 0-40 °C), because the long-time working of regular SIM card in harsh environment (temperature exceeding 0-40 °C) may increase the possibility of SIM card failure.*
3. *Don't forget screw the cover for again-theft.*
4. *Don't touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
5. *Don't bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
6. *Make sure router is power off before inserting or removing your SIM card.*

## 2.6 Connect the External Antenna

Connect router with an external antenna connector. Make sure the antenna is within correct frequency range and is screwed tightly. **Recommended torque for mounting is 0.35N.m**

## 2.7 Ground the Router

Grounding and wire router helps limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground by screwing to the grounding surface before connecting devices.

**Note:** *This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.*

## 2.8 Mount the Router

The router may be placed on a horizontal surface such as a desktop, mounted on a DIN-rail, or mounted on the wall.

- **Two ways of mounting the router**

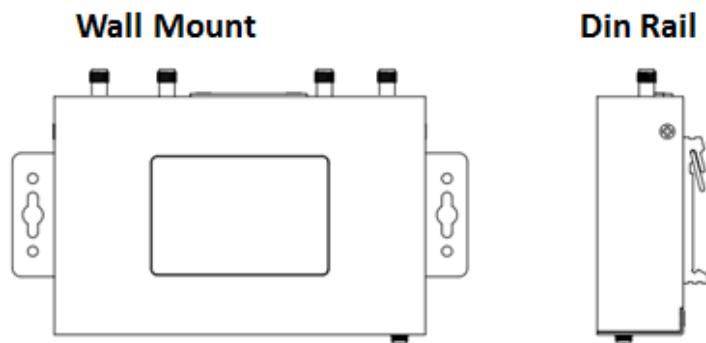
1. Use 4 pcs of M2.5 screw to fix the router on the two metal plates.  
And then use 2 pcs of M2.5 countersunk head cross recess screws with point-end to mount the router with two metal plates on the wall.

**Recommended torque for mounting is 0.5N.m and the maximum torque is 0.7N.m.**

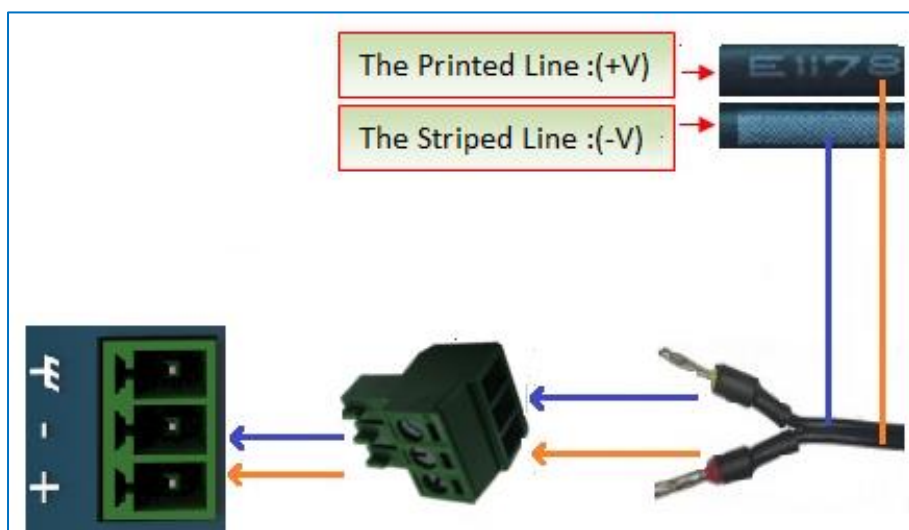
2. Mount the router on a DIN rail with 3 pcs of M3 countersunk head cross recess screws, and then hang the DIN-Rail on the holder.

You need to choose a standard holder. **Recommended torque for mounting is 1.0N.m and the maximum torque is 1.2N.m.**

**Note:** *When mounting the unit on a DIN-rail, make sure that it is oriented with the metal springs on top.*



## 2.9 Power Supply



The power supply range is 9 to 26 VDC.

**Note:** Please take care about the polarity, and do not make reverse connection. There are two lines connecting to the power supply adapter, as it illustrates on the power supply adapter label, the line printed with letters needs to be connected with the positive polarity, and the striped line needs to be connected with the negative polarity.

## Chapter 3 Configure Settings over Web Browser

The router can be configured through your web browser that include IE 8.0 or above, Chrome and Firefox. 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.

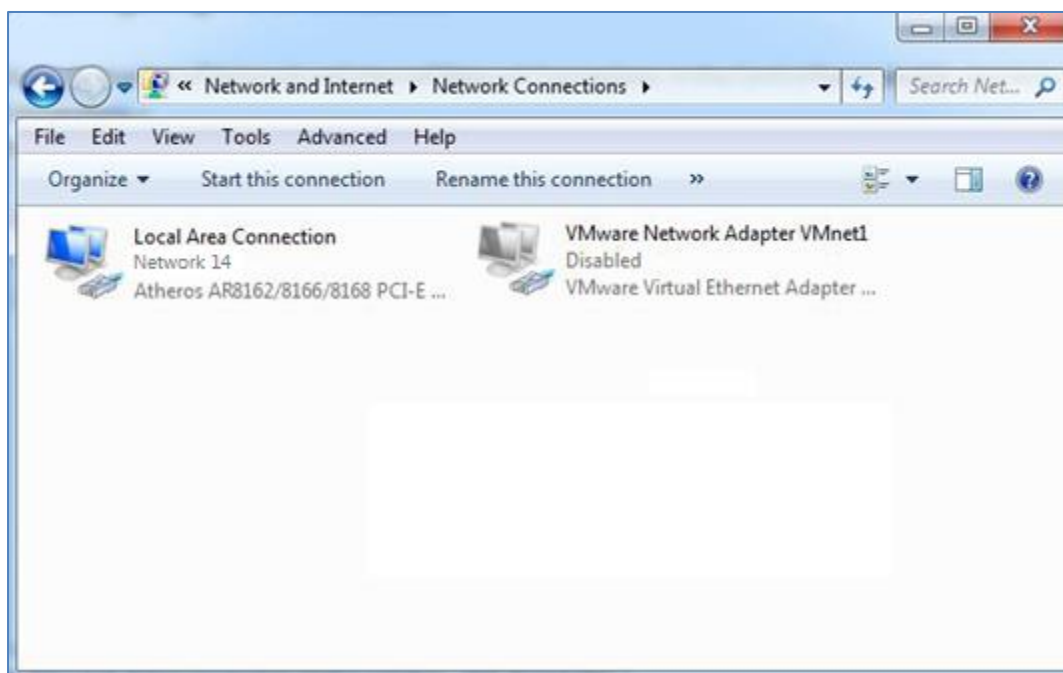
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the router.

### 3.1 Configuring PC in Windows 7

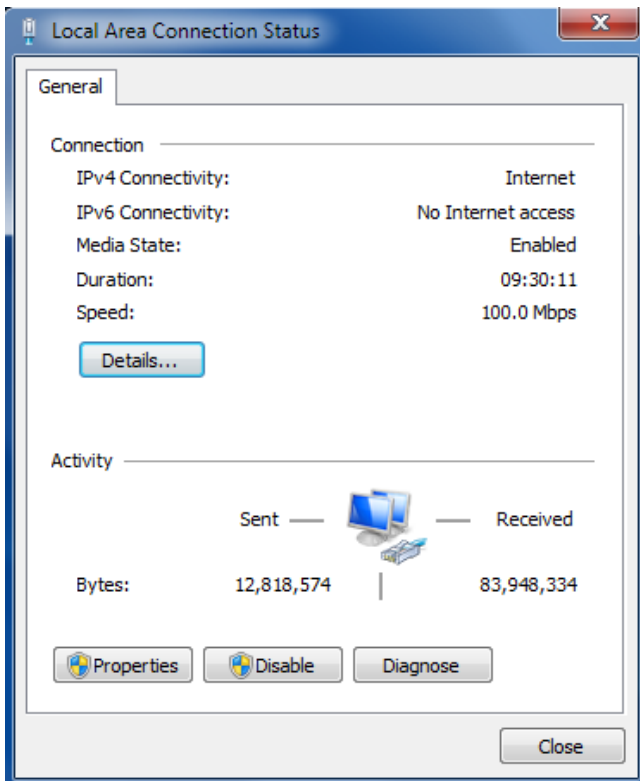
There are two methods to obtain IP address for the PC, one is automatically obtain IP address from DHCP server, and another is manually configured static IP address within the same subnet of R2000 router.

The configuration for windows system is similar.

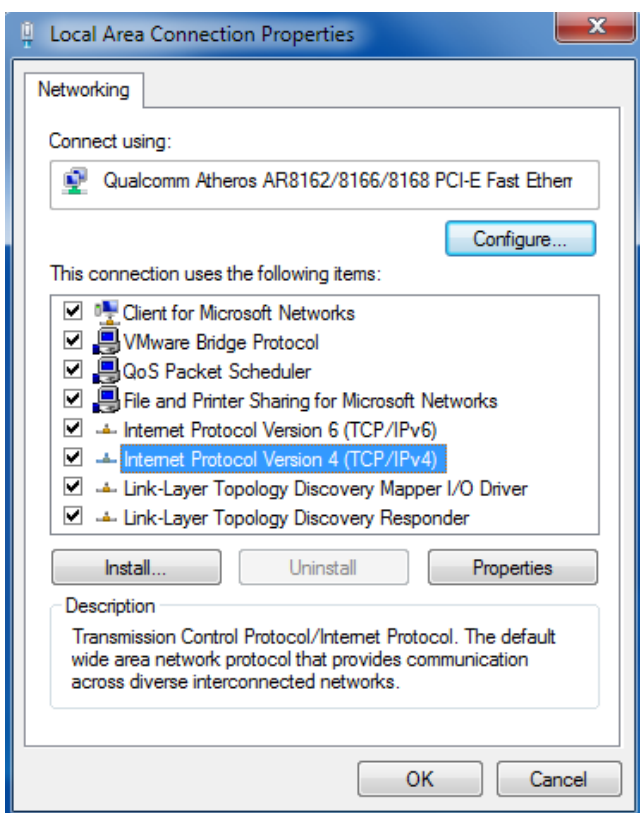
1. Go to *Start \Control Panel \Network and Internet\Network Connections*. Double-click *Local Area Connection*.



2. In the *Local Area Connection Status* window, click *Properties*.

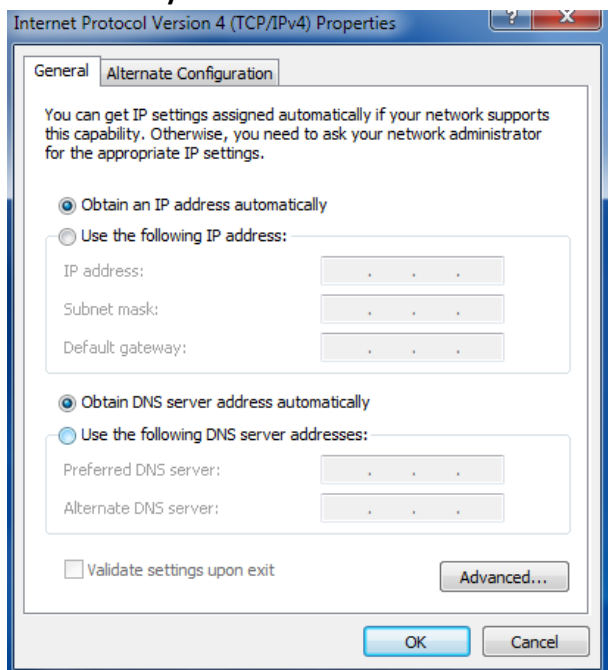


3. Select *Internet Protocol (TCP/IP)* and click *Properties*.

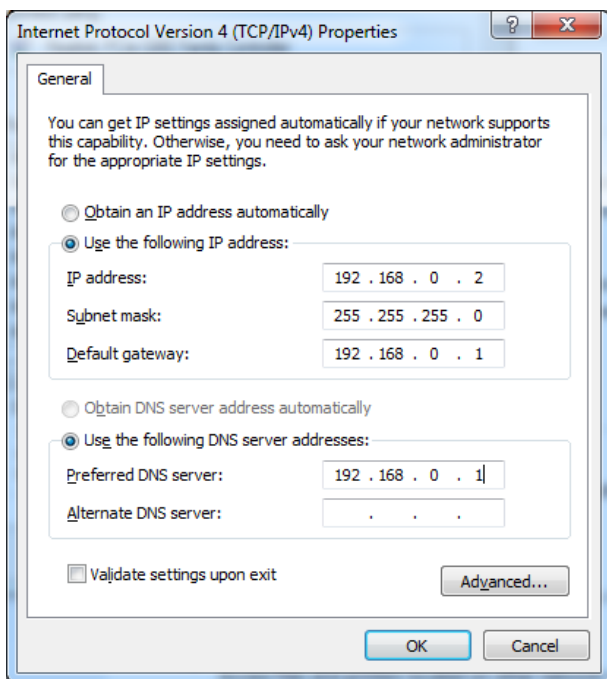


4. Configure the IP address of PC.

**Automatically obtain IP address from DHCP server**



**Manually configured static IP address within the same subnet of R2000 router**



5. Click *OK* to finish the configuration.

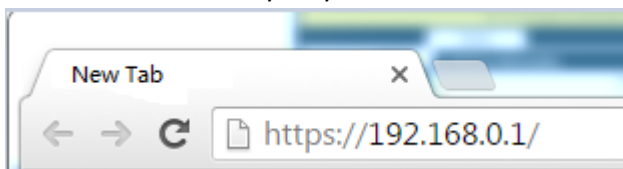
### 3.2 Factory Default Settings

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

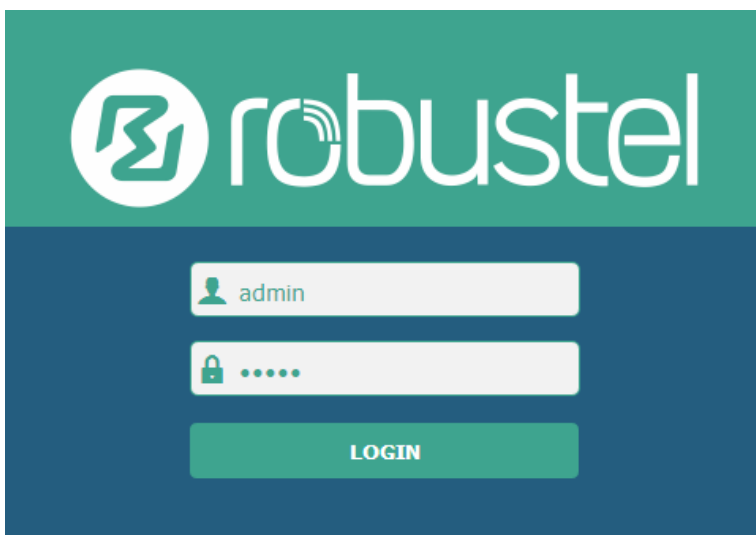
Item	Description
Username	admin
Password	admin
eth0	192.168.0.1/255.255.255.0, LAN
eth1	192.168.0.1/255.255.255.0, LAN
DHCP Server	Enabled

### 3.3 Login Router

1. On the PC, open a web browser such as Internet Explorer.
2. In the browser's address bar, enter the IP address of the Router. The default IP address is 192.168.0.1, though the actual address may vary.





3. Input the username and password and login the R2000. If enter the wrong username or password six times, the login web will be locked for 5 minutes.



### 3.4 Control Panel

After logging in the R2000, the home page of the R2000 router's web interface is displayed, just like the screenshot below.

This section allows users to save configuration, reboot router, logout. When you are first time to login R2000, there will be a pop-up tab “ It is strongly recommended to change the default password.”, click  to close the pop-up tab. And if you want to change the password, please refer to **3.27 System -> User Management** section.



The screenshot shows the Robustel web interface. At the top right, there are links for "Save & Apply", "Reboot", and "Logout". A yellow notification bar at the top contains a warning icon and the text "It is strongly recommended to change the default password." with a close button (x). The left sidebar contains navigation tabs: Status, Interface, Network, VPN, Services, and System. The main content area is titled "Status" and is divided into two sections: "System Information" and "Cellular Information".



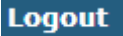

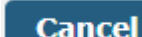
System Information	
Device Model	R2000
System Uptime	0 days, 00:05:34
System Time	Wed Dec 16 10:12:28 2015
Firmware Version	1.2.0 (Rev 399)
Hardware Version	1.0
Kernel Version	3.10.49
Serial Number	15090140040008




Cellular Information	
Modem Status	Ready
Model	ME909s-821
Firmware Version	11.617.00.00.00
IMEI	867223020050860
SIM Status	SIM2 using, total 1 SIMs
Network Registration	Registered to home network
Network Operator	CHN-UNICOM

Copyright © 2015 Robustel Technologies. All rights reserved.



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. When the Reboot button is in yellow, it means that some completed configurations will take effect only by reboot.	
Logout	Click to exit safely, then 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 submit the modification on current configuration page.	
Cancel	Click to cancel the modification on current configuration page.	

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

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

### 3.5 Status

This section displays the router’s status, which shows you a number of helpful information such as System Information, Cellular Information, Internet Status and LAN Status.

#### System Information

**^ System Information**

<b>Device Model</b>	R2000
<b>System Uptime</b>	0 days, 00:05:34
<b>System Time</b>	Wed Dec 16 10:12:28 2015
<b>Firmware Version</b>	1.2.0 (Rev 399)
<b>Hardware Version</b>	1.0
<b>Kernel Version</b>	3.10.49
<b>Serial Number</b>	15090140040008

System Information	
Item	Description
Device Model	Show the model name of this device.
System Uptime	Show how long the router has been working since power on.
System Time	Show the current system time.
Firmware Version	Show the current firmware version.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of this device.

**Cellular Information**

^ Cellular Information	
<b>Modem Status</b>	Ready
<b>Model</b>	ME909s-821
<b>Firmware Version</b>	11.617.00.00.00
<b>IMEI</b>	867223020050860
<b>SIM Status</b>	SIM2 using, total 1 SIMs
<b>Network Registration</b>	Registered to home network
<b>Network Operator</b>	CHN-UNICOM
<b>Network Type</b>	LTE
<b>Signal Strength</b>	19 (-75dBm)

Cellular Information	
Item	Description
Modem Status	Show the status of modem. There are 8 different status: 1. Initializing 2. Modem not found 3. No response 4. SIM not detected 5. SIM PIN required 6. SIM PUK required 7. Register failed 8. Ready
Modem Model	Show the current radio module type.
Firmware Version	Show the current radio firmware version.
IMEI	Show the IMEI number of the radio module.
SIM Status	Show the SIM card which the router works with currently: SIM1 or SIM2. And show the total SIM cards in the router.
Network Registration	Show the status of Registration. There are 6 different status: 1. Not registered, search stopped 2. Registered to home network 3. Not registered, searching 4. Registration denied 5. Unknown 6. Registered, roaming
Network Provider	Show the current network provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the current signal strength.

**Internet Status**

**^ Internet Status**

**Active Link**    WWAN1

**Uptime**        0 days, 00:05:02

**IP Address**    10.151.84.17/255.255.255.252

**Gateway**       10.151.84.18

**DNS**            210.21.4.130 221.5.88.88

Internet Status	
Item	Description
Active Link	Show the current WAN link: WWAN1, WWAN2 or WAN.
Uptime	Show how long the current WAN have been working.
IP Address	Show the current WAN IP address.
Gateway	Show the current gateway.
DNS	Show the current primary DNS server and Secondary server.

**LAN Status**

**^ LAN Status**

**IP Address**    172.16.99.11/255.255.0.0

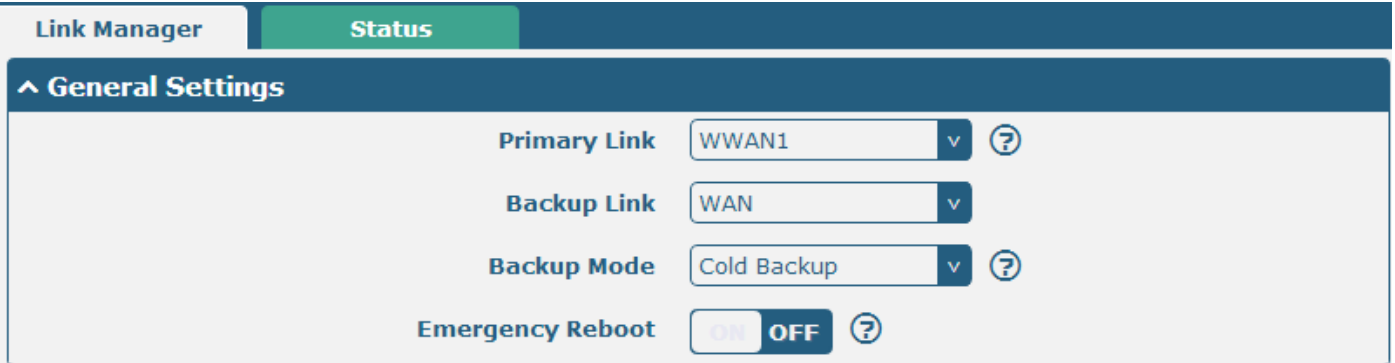
**MAC Address**   34:FA:40:04:AD:67

Router Information	
Item	Description
IP Address	Show the current IP Address and the Netmask.
MAC Address	Show the current MAC Address.

### 3.6 Interface->Link Manager

#### Link Manager

User can manage the link connection in this section.



Link Manager		
Item	Description	Default
Primary Link	Select from “WWAN1”, “WWAN2”, “WAN”, “WLAN”. <ol style="list-style-type: none"> <li>WWAN1: Select to make SIM1 as the primary wireless link. <b>Note:</b> insert SIM card please refer to the installation quick guide.</li> <li>WWAN2: Select to make SIM2 as the primary wireless link.</li> <li>WAN: Select to make WAN Ethernet port as the primary link. <b>Note:</b> WAN link available only if enable ETH0 as WAN interface in <b>System-&gt;Device Configuration-&gt;Advance Device Settings</b></li> <li>WLAN: Select to make WLAN as the router’s primary link. <b>Note:</b> WLAN link available only if enable R2000 as WiFi Client in <b>System-&gt;Device Configuration-&gt;Advance Device Settings</b></li> </ol>	WWAN1
Backup Link	Select from “None”, “WWAN1”, “WWAN2”, “WAN”, “WLAN”. <ol style="list-style-type: none"> <li>None: Do not select backup interface.</li> <li>WWAN1: Select to make SIM1 as backup wireless WAN.</li> <li>WWAN2: Select to make SIM2 as backup wireless WAN.</li> <li>WAN: Select to make WAN Ethernet port as the backup WAN. <b>Note:</b> WAN link available only if enable ETH0 as WAN interface in <b>System-&gt;Device Configuration-&gt;Advance Device Settings</b></li> <li>WLAN: Select to make WLAN as the router’s backup link. <b>Note:</b> WLAN link available only if enable R2000 as WiFi Client in <b>System-&gt;Device Configuration-&gt;Advance Device Settings</b></li> </ol>	None
Backup Mode	Cold backup: The inactive link is offline on standby. Warm backup: The inactive link is online on standby. Warm backup mode is not available for dual SIM backup.	Cold backup
Emergency Reboot	Enable to reboot the whole system if no links available.	OFF

**Note:** Click “?” for help.

**Link Setting** section allows user to configure the parameter of link connection, include the WWAN1/WWAN, WAN and WLAN.

It is recommended to enable Ping detection to keep router always online.

The Ping detection increases the reliability and also cost data traffic.

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

Click to enter the link configuration window.

### WWAN1/WWAN2

**Link Manager**

^ General Settings

Index

Type

Description

When enable “Automatic APN Selection”, the window will display just like the following screenshot.

^ WWAN Settings

**Automatic APN Selection**  ON  OFF

Dialup Number

Authentication Type

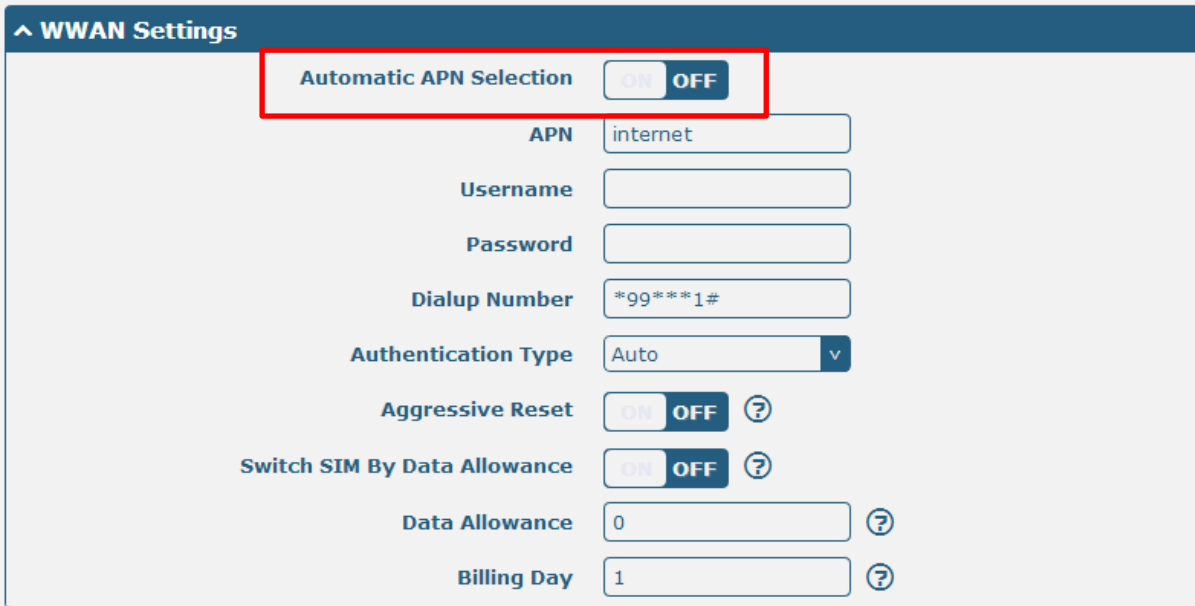
Aggressive Reset  ON  OFF ?

Switch SIM By Data Allowance  ON  OFF ?

Data Allowance  ?

Billing Day  ?

When disable “Automatic APN Selection”, the window will display just like the following screenshot.



WWAN Setting		
Item	Description	Default
<b>Automatic APN Selection ON</b>	ON: R2000 will recognize the access point name automatically.	ON
Dialup Number	Dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
Aggressive Reset	The module will be reset when the link become unreachable.	OFF
Switch SIM By Data Allowance	Switch to another SIM when reach data allowance, only use 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 display in <b>Link Manager-&gt;Status-&gt; WWAN Data Usage Statistics</b> section. 0 means disable data traffic record.	0
Billing Day	This option specifies the day of month for billing, the data traffic statistics will be recalculated from this day.	1
Redial Interval	Seconds to wait for redial.	10
<b>Automatic APN Selection OFF</b>	OFF: Select access point name manually.	/
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	User Name for cellular dial-up connection, provided by local ISP.	Null
Password	Password for cellular dial-up connection, provided by local ISP.	Null

^ Ping Detection Settings ?

Enable  ON  OFF

Primary Server

Secondary Server

Interval  ?

Retry Interval  ?

Timeout  ?

Max Ping Tries  ?

^ Advanced Settings

MTU

Overridden Primary DNS

Overridden Secondary DNS

Ping Detection Settings/Advanced Setting		
Item	Description	Default
Enable	To enable “ping detection”. It was a keepalive policy of R2000 router.	OFF
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.	Null
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Tmeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Overridden Primary DNS	Overridden DNS will override the automatically obtained DNS.	Null
Overridden Secondary DNS	Overridden DNS will override the automatically obtained DNS.	Null



**WAN**

**Link Manager**

^ **General Settings**

**Index**

**Description**

**Type**  v

**Connection Type**  v

When choose the WAN Connection Type as DHCP, R2000 will obtain IP automatically from DHCP server.

When choose the WAN Connection Type as Static.

^ **Static Address Settings**

**IP Address**  ?

**Gateway**

**Primary DNS**

**Secondary DNS**

<b>Static</b>		
Item	Description	Default
IP Address	Set the IP address with Netmask which can access the internet. IP address with netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the WAN IP.	Null
Primary DNS	Set the Primary DNS.	Null
Secondary DNS	Set the Secondary DNS.	Null

When choose the WAN Connection Type as PPPoE.

^ **PPPoE Settings**

**Username**

**Password**

**Authentication Type**  v

**PPP Expert Options**  ?

<b>PPPoE</b>		
Item	Description	Default
Username	Enter the username which was provided by your Internet Service Provider.	Null
Password	Enter the password which was provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" and "CHAP" as the local ISP required.	Auto

PPPoE		
Item	Description	Default
PPP Expert Options	PPP Expert options used for PPPoE dialup. You can enter some other PPP initialization strings in this field. Each string can be separated by a semicolon.	Null

^ Ping Detection Settings
?

**Enable**  ON  OFF

**Primary Server**

**Secondary Server**

**Interval**  ?

**Retry Interval**  ?

**Timeout**  ?

**Max Ping Tries**  ?

^ Advanced Settings

**MTU**

**Overridden Primary DNS**

**Overridden Secondary DNS**

Ping Detection Setting/Advance Setting		
Item	Description	Default
Enable	To enable “ping detection”. It was a keepalive policy of R2000 router.	OFF
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.	Null
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Overridden Primary DNS	Overridden DNS will override the automatically obtained DNS.	Null
Overridden Secondary DNS	Overridden DNS will override the automatically obtained DNS.	Null

**WLAN**

**Link Manager**

^ **General Settings**

**Index**

**Description**

**Type**  v

**Connection Type**  v

^ **WLAN Settings**

**SSID**

**Connect to Hidden SSID**  ON  OFF

**Password**

**Debug Level**  v

WLAN Setting		
Item	Description	Default
SSID	Enter SSID of the access point which R2000 want to connect. Input from 1 to 32 characters.	router
Connect to Hidden SSID	When R2000 works as Client mode and need to connect to any access point which has hidden SSID, you need to enable this feature.	OFF
Password	Enter access point's passphrase which it wants to connect to. Input from 8 to 63 characters.	Null
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", "none".	None

When choose the WLAN Connection Type as DHCP, R2000 will obtain IP automatically from the WLAN AP.  
 When choose the WLAN Connection Type as Static. Please enter the related parameter in the **Static Address Setting** window.

^ **Static Address Settings**

**IP Address**  ?

**Gateway**

**Primary DNS**

**Secondary DNS**

Static Address Setting		
Item	Description	Default
IP Address	Enter the IP address which was identified by the WiFi AP. IP address with netmask, e.g. 192.168.1.1/24	Null
Gateway	Enter the WiFi AP's IP address.	Null

Static Address Setting		
Item	Description	Default
Primary DNS	Enter the primary DNS server IP address.	Null
Secondary DNS	Enter the Secondary DNS server IP address.	Null

R2000 router cannot support PPPoE WLAN Connection Type.

^ Ping Detection Settings
?

Enable  ON  OFF

Primary Server

Secondary Server

Interval  ?

Retry Interval  ?

Timeout  ?

Max Ping Tries  ?

---

^ Advanced Settings

MTU


Overrided Primary DNS

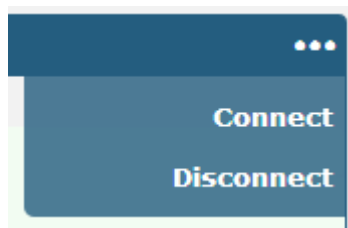
Overrided Secondary DNS

Ping Detection Setting/Advance Setting		
Item	Description	Default
Enable	To enable “ping detection”. It was a keepalive policy of R2000 router.	OFF
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.	Null
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Tmeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Overrided Primary DNS	Overrided DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Overrided DNS will override the automatically obtained DNS.	Null

Status

Link Manager		Status		
^ Link Status				
Index	Link	Status	Uptime	IP Address
1	WLAN	Connected	0 days, 00:00:10	192.168.1.12...

Click the button  which is in the top right of the Link Status window. Select the connection status of the current link.



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

^ Link Status				
Index	Link	Status	Uptime	IP Address
1	WLAN	Connected	0 days, 00:00:10	192.168.1.12...
		<b>Index</b>	1	
		<b>Link</b>	WLAN	
		<b>Status</b>	Connected	
		<b>Uptime</b>	0 days, 00:00:10	
		<b>IP Address</b>	192.168.1.123/255.255.255.0	
		<b>Gateway</b>	192.168.1.1	
		<b>DNS</b>	192.168.1.1	
		<b>RX Packets</b>	1200	
		<b>TX Packets</b>	399	
		<b>RX Bytes</b>	165023	
		<b>TX Bytes</b>	106140	

^ WWAN Data Usage Statistics	
SIM1 Monthly Stats	<b>Clear</b>
SIM2 Monthly Stats	<b>Clear</b>

Click  button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will display only if

enable the Data Allowance function in **Link Manager->Link Setting->WWAN Setting**.

### 3.7 Interface->LAN

This section allows user to set the LAN and the related parameters.

#### LAN

LAN	Multiple IP	VLAN Trunk	Status
<b>^ Network Settings</b> <span style="float: right;">?</span>			
Index	Interface	IP Address	Netmask
1	lan0	192.168.0.1	255.255.255.0
<span>+</span> <span>✎</span> <span>✕</span>			

Click ✎ to edit the configuration of the current LAN interface. Click ✕ to delete the current LAN interface.

Click + to add a new LAN interface. The maximum number of LAN interface is two.

**LAN**

**^ General Settings**

Index:

Interface:  v

IP Address:

Netmask:

MTU:

General Settings		
Item	Description	Default
Interface	Select lan0 or lan1. When eth0 used As WAN, lan1 is unavailable. And lan1 available only if it was selected by eth0 or eth1 in <b>Ethernet-&gt;Port Setting</b> section.	lan0
IP Address	Set the IP Address of the LAN interface.	192.168.0.1
Netmask	Set the Netmask of the LAN interface.	255.255.255.0
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500

When select DHCP Mode as Server, the window will display as the following screenshot.

^ DHCP Settings

**Enable**  ON  OFF

**Mode** Server v

**IP Pool Start** 192.168.0.2

**IP Pool End** 192.168.0.100

**Subnet Mask** 255.255.255.0

^ DHCP Advanced Settings

**Gateway**  

**Primary DNS**  

**Secondary DNS**  

**WINS Server**  

**Lease Time** 120 ?

**Expert Options**   ?

**Debug Enable**  ON  OFF

DHCP Server		
Item	Description	Default
Enable	Click the switch to show “ON” and to enable DHCP function.	ON
Mode	Server: Lease IP address to DHCP clients which connect to LAN. 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.	DHCP Server
IP Pool Start	Define the beginning of the pool of IP addresses which will lease to DHCP clients.	192.168 .0.2
IP Pool End	Define the end of the pool of IP addresses which will lease to DHCP clients.	192.168 .0.100
Subnet Mask	Define the Subnet Mask which the DHCP clients will obtain from DHCP server.	255.255 .255.0
Gateway	Define the Gateway which the DHCP clients will obtain from DHCP server.	Null
Primary DNS	Define the Primary DNS Server which the DHCP clients will obtain from DHCP server.	Null
Secondary DNS	Define the Secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null
WINS Server	Define the Windows Name Server which the DHCP clients will obtain from DHCP server.	Null
Lease Time	Define the time which the client can use the IP address which obtained from DHCP server.	120

DHCP Server		
Item	Description	Default
Expert Options	You can enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Enable this function; it will output the DHCP information to syslog.	OFF

When select DHCP Mode as Relay, the window will display as the following screenshot.

^ DHCP Settings

Enable  ON  OFF

Mode  v

DHCP Server For Relay

^ DHCP Advanced Settings

Debug Enable  ON  OFF

DHCP Server		
Item	Description	Default
DHCP Server for Relay	Enter the DHCP Relay server IP address.	Null
Debug Enable	Enable this function; it will output the DHCP information to syslog.	OFF

### Multiple IP

LAN Multiple IP VLAN Trunk Status

^ Multiple IP Settings

Index	Interface	IP Address	Netmask	
1	lan0	172.16.99.67	255.255.0.0	<span style="float: right;">+</span> <span style="float: right;">✎ ✕</span>

Click to edit the Multiple IP of the LAN interface. Click to delete the Multiple IP of the LAN interface.

Click to add a multiple IP to the LAN interface.

Multiple IP

^ IP Settings

Index

Interface  v

IP Address

Netmask



Multiple IP		
Item	Description	Default
Interface	Select lan0 or lan1. When eth0 used As WAN, lan1 is unavailable. And lan1 available only if it was selected by eth0 or eth1 in <b>Ethernet-&gt;Port Setting</b> section.	lan0
IP Address	Set the multiple IP Address of the LAN interface.	Null
Netmask	Set the multiple Netmask of the LAN interface.	Null

### VLAN Trunk

LAN
Multiple IP
VLAN Trunk
Status

^ VLAN Settings

Index	Enable	Interface	VID	IP Address	Netmask	+
-------	--------	-----------	-----	------------	---------	---

Click to add a VLAN. The maximum number of the VLAN is eight.

VLAN Trunk

^ VLAN Settings

Index

Enable  ON  OFF

Interface  v

VID

IP Address

Netmask

VLAN Trunk		
Item	Description	Default
Enable	Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Select lan0 or lan1. When eth0 used As WAN, lan1 is unavailable. And lan1 available only if it was selected by eth0 or eth1 in <b>Ethernet-&gt;Port Setting</b> section.	lan0
VID	Set the Tag ID of VLAN, values range from 1 to 4094.	100
IP Address, Netmask	Set the IP address, Netmask of VLAN interface	Null

### Status

This section shows the Ethernet port status and connected devices.

LAN	Multiple IP	VLAN Trunk	Status	
<b>^ Interface Status</b>				
Index	Interface	IP Address	MAC Address	
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:B9:E9	
2	lan1	172.16.99.68/255....	34:FA:40:0B:E6:46	
<b>^ Port Status</b>				
Index	Port	Link		
1	eth0	Down		
2	eth1	Up		
<b>^ Connected Devices</b>				
Index	IP Address	MAC Address	Interface	Inactive Time
1	172.16.3.16	D0:50:99:4D:F9:35	lan0	0s
<b>^ DHCP Lease Table</b>				
Index	IP Address	MAC Address	Interface	Expired Time

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

<b>^ Interface Status</b>			
Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:B9:E9
<b>Index</b> 1 <b>Interface</b> lan0 <b>IP Address</b> 192.168.0.1/255.255.255.0 <b>MAC Address</b> 34:FA:40:0B:B9:E9 <b>RX Packets</b> 0 <b>TX Packets</b> 0 <b>RX Bytes</b> 0 <b>TX Bytes</b> 0			
2	lan1	172.16.99.68/255....	34:FA:40:0B:E6:46

### 3.8 Interface->Ethernet

This section allow user to set the parameter of the Ethernet port. One port should be assigned to lan0 a least.

Ports		
^ Port Settings		
Index	Port	Port Assignment
1	eth0	lan1
2	eth1	lan0

Click  button, configure the port setting.

**Ports**

**^ Port Settings**

Index:

Port:

Port Assignment:

Ethernet		
Item	Description	Default
Index	The index of Ethernet port, cannot edit.	1 or 2
Port	eth0 or eth1 One port should be assigned to lan0 a least.	/
Port Assignment	Select lan0 or lan1. <b>Note:</b> When eth0 used As WAN, lan1 is unavailable. Please go to <b>System-&gt;Device Configuration</b> to enable eth0 used as WAN. And lan1 available only if it was selected by eth0 or eth1 in this field.	lan0


### 3.9 Interface->Cellular

This section allows users to set the Cellular WAN and the related parameters.

When it is the first time to insert single SIM card, SIM card 1 and SIM card 2 slots are available.

#### SIM

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

Click  to edit the parameters.

**Cellular**

^ **General Settings**

<b>Index</b>	<input type="text" value="1"/>
<b>SIM Card</b>	<input style="border: 1px solid #ccc; border-radius: 3px; width: 100%;" type="text" value="SIM1"/> v
<b>Phone Number</b>	<input type="text"/>
<b>Extra AT Cmd</b>	<input type="text"/> ?

When choose “Network Type type” is “Auto”;

^ **Cellular Network Settings**

<b>Network Type</b>	<input style="border: 1px solid #ccc; border-radius: 3px; width: 100%;" type="text" value="Auto"/> v ?
<b>Band Select Type</b>	<input style="border: 1px solid #ccc; border-radius: 3px; width: 100%;" type="text" value="All"/> v ?

When choose “band select type” is “Specify”.

^ **Cellular Network Settings**

<b>Network Type</b>	<input style="border: 1px solid #ccc; border-radius: 3px; width: 100%;" type="text" value="Auto"/> v ?
<b>Band Select Type</b>	<input style="border: 1px solid #ccc; border-radius: 3px; width: 100%;" type="text" value="Specify"/> v ?
<b>GSM 900</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>GSM 1800</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>WCDMA 850</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>WCDMA 900</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>WCDMA 1900</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>WCDMA 2100</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

Cellular		
Item	Description	Default
Index	Show the index of the SIM.	1
SIM Card	Set the current SIM card.	SIM1
Link Name	Set the current Link Name.	WWAN1
Phone Number	Define the phone number of the SIM card.	Null
Extra AT Cmd	AT commands used for cellular initialization.	Null
Network Type	Select from “Auto”, “2G Only”, “2G First”, “3G Only”, “3G First”, “4G Only”, “4G First”.	Auto
Band Select Type	Select from “All”, “Specify”. When select “Specify”, user can choose certain bands.	All

**Status**

This section allow user to check the cellular status information.

Cellular
Status

^ Cellular Information

<b>Modem Status</b>	Ready
<b>Current SIM</b>	SIM2
<b>Total SIMs</b>	1
<b>Phone Number</b>	145
<b>IMSI</b>	460010432615366
<b>ICCID</b>	89860114851074491267
<b>Network Registration</b>	Registered to home network
<b>Network Operator</b>	CHN-UNICOM
<b>Network Type</b>	WCDMA
<b>Signal Strength</b>	3 (-107dBm)
<b>Cell ID</b>	A50B,0148A989
<b>Model</b>	MU709s-6
<b>IMEI</b>	866430020015865
<b>Firmware Version</b>	11.652.61.00.00

Status	
Item	Description
Modem Status	Show the status of the radio module.
Current SIM	Show the SIM card which the router works with currently: SIM1 or SIM2.
Total SIMs	Show the number of SIM cards that is installed in the router.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the current signal strength.
Cell ID	Show the current cell ID, which can locate the router.
Modem Model	Show the model of the radio module.
IMEI	Show the IMEI number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

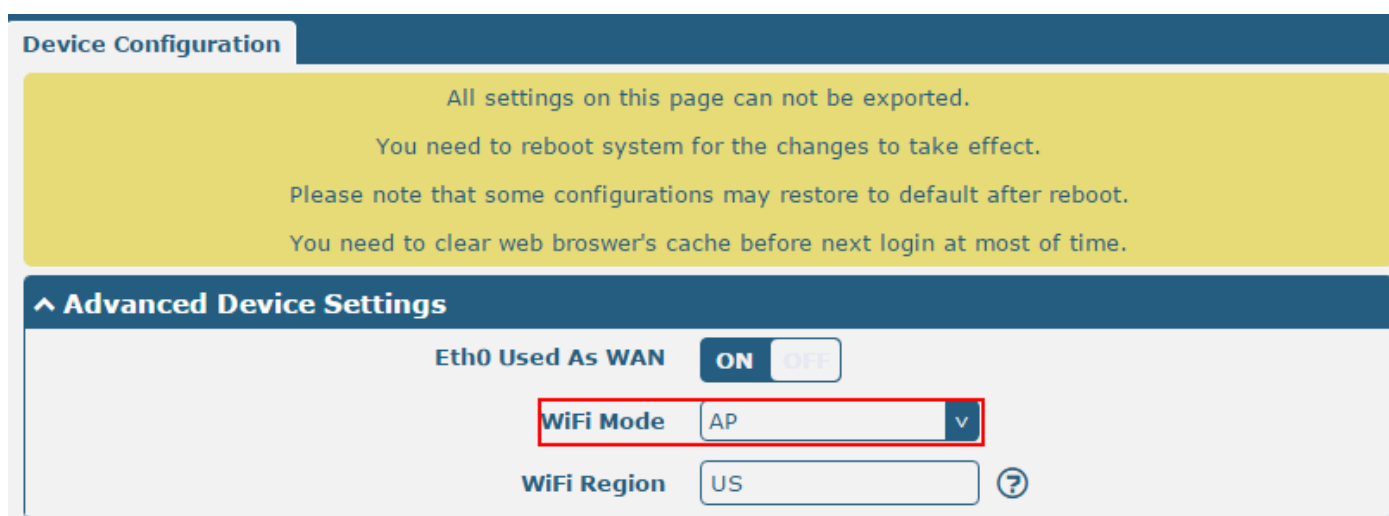
### 3.10 Interface->WiFi (Optional)

R2000 router support both WiFi AP and WiFi client. The factory default setting of R2000 is as WiFi AP. This section allow user to configure the parameters of WiFi AP.

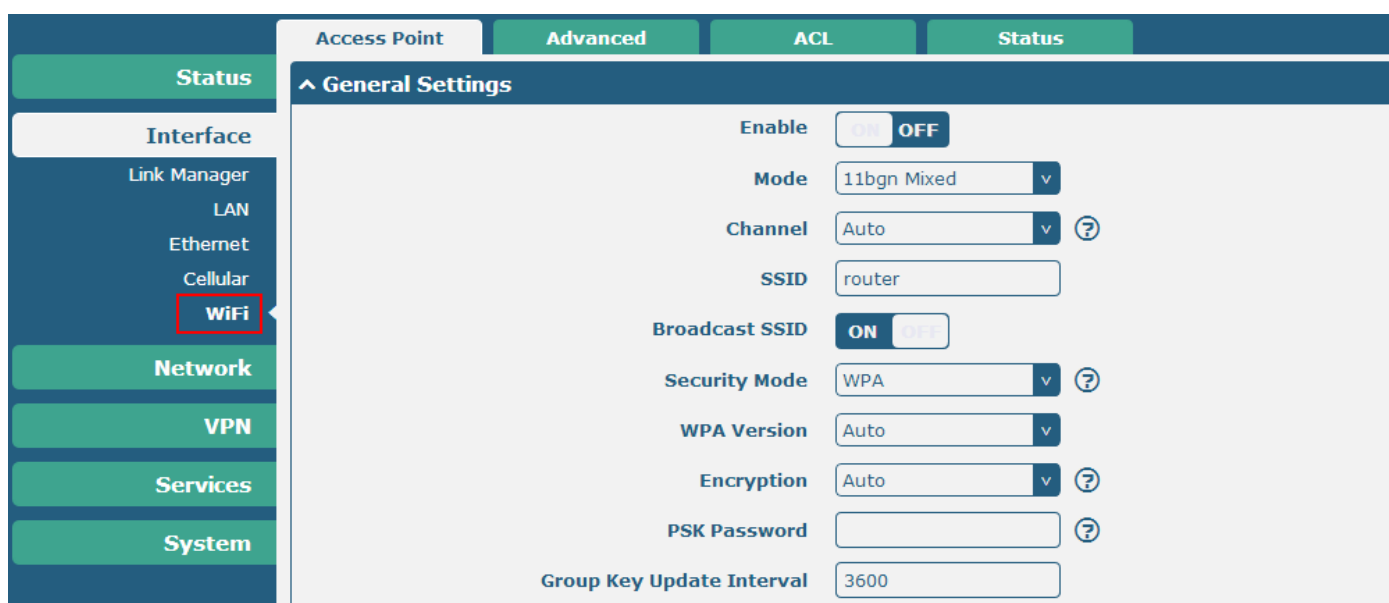
#### WiFi AP

##### Configure R2000 as a WiFi AP

Go to **System->Device Configuration**, select the WiFi mode as AP, click “Submit” and reboot the device to make the setting effect.



When R2000 router was set as a WiFi AP, we can find the WiFi item in the Interface menu. Just like the screenshot below.



Access Point		
Item	Description	Default
Enable	Click to "ON" side, enable the WiFi access point function.	OFF
Mode	Select from "11bgn Mixed", "11b only", "11g only" and "11n only". 11bgn Mixed: Three protocols mixed in order to backward compatibility 11b only: IEEE 802.11b, 11Mbit/s-- 2.4GHz 11g only: IEEE 802.11g, 54Mbit/s--2.4GHz 11n only: IEEE 802.11n, 300Mbps~600Mbps	11bgn Mixed
Channel	Select the frequency channel, which includes "Auto", "1", "2"..... "11". Auto: R2000 will scan all frequencies until it finds the best channel. 1~11: R2000 will be fixed to work with this channel. Following are the frequency of 1~ 11 channel. 1 - 2412 MHz 2 - 2417 MHz 3 - 2422 MHz 4 - 2427 MHz 5 - 2432 MHz 6 - 2437 MHz 7 - 2442 MHz 8 - 2447 MHz 9 - 2452 MHz 10 - 2457 MHz 11 - 2462 MHz 12 - 2467 MHz 13 - 2472 MHz	Auto
SSID	SSID (service set identifier) is the network name of the WiFi. 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. Input from 1 to 31 characters.	router
Broadcast SSID	Click "ON" to enable the SSID broadcasting. So that the client can scan the SSID. If you disable this feature, none of client could scan the SSID. If you want to connect to the router AP, you must need to enter the SSID of router AP at wifi client side manually.	ON
Security Mode	Select from "Disable", "WPA" and "WEP". Disable: User can access the WiFi without the password when disable security. WPA: Include WPA and WPA2. Personal versions of WPA (Wi-Fi Protected Access), also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. WEP: Wired Equivalent Privacy, provide encryption for wireless device's data transmission. It's not recommended to use WEP.	Disable

Access Point		
Item	Description	Default
WPA Version	Select from "Auto", "WPA" and "WPA2". Auto: R2000 will choose the most suitable selection automatically. WPA2 is a stronger security feature than WPA.	Auto
Encryption	Select from "Auto", "TKIP" and "AES". Auto: R2000 will choose the most suitable Encryption automatically. TKIP: Temporal Key Integrity Protocol (TKIP) encryption is used over the wireless link. TKIP encryption can be used with WPA-PSK and WPA with 802.1x authentication. It's not recommended to use TKIP encryption in 802.11n mode. AES: AES encryption is used over the wireless link. AES can be used WPA-PSK and WPA with 802.1x authentication. <b>Note:</b> AES is a stronger encryption algorithm than TKIP.	Auto
PSK Password	PSK password—Pre share key password. When R2000 works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Input from 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600



Access Point
Advanced
ACL
Status

**^ Advanced Settings**

<b>Max Associated Stations</b>	<input type="text" value="64"/>
<b>Beacon Interval</b>	<input type="text" value="100"/>
<b>DTIM Interval</b>	<input type="text" value="2"/>
<b>RTS Threshold</b>	<input type="text" value="2347"/>
<b>Fragmentation Threshold</b>	<input type="text" value="2346"/>
<b>Transmit Rate</b>	<input style="border: none; background-color: #e0e0e0; width: 100%;" type="text" value="Auto"/> <span style="float: right;">v</span>
<b>11N Transmit Rate</b>	<input style="border: none; background-color: #e0e0e0; width: 100%;" type="text" value="Auto"/> <span style="float: right;">v</span>
<b>Transmit Power</b>	<input style="border: none; background-color: #e0e0e0; width: 100%;" type="text" value="Max"/> <span style="float: right;">v</span>
<b>Channel Width</b>	<input style="border: none; background-color: #e0e0e0; width: 100%;" type="text" value="Auto"/> <span style="float: right;">v</span> <span style="float: right; font-size: 20px;">?</span>
<b>Enable WMM</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
<b>Enable Short GI</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF <span style="float: right; font-size: 20px;">?</span>
<b>Enable AP Isolation</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <span style="float: right; font-size: 20px;">?</span>
<b>Debug Level</b>	<input style="border: none; background-color: #e0e0e0; width: 100%;" type="text" value="none"/> <span style="float: right;">v</span>

Advanced		
Item	Description	Default
Max Associated Stations	Set the max number of association station to access the router AP.	64
Beacon Interval	Set the frequency of the router AP broadcast Beacon, which was used for wireless network synchronization.	100
DTIM Interval	DTIM (Delivery Traffic Indication Message), router AP will send the multicast traffic according to this interval.	2
RTS Threshold	Set RTS (request to send) threshold to 2347, router AP will never sent the signal before sending out data. Set RTS threshold to 0, router AP will send the signal once it sending out data.	2347
Fragmentation Threshold	Set the fragmentation threshold for WiFi AP data packet. Recommend remain at 2346.	2346
Transmit Rate	Set the transmit rate, you can choose Auto or specify a Transmit Rate.	Auto
11N Transmit Rate	Set the data transmit rate under the IEEE 802.11n WiFi mode. Select "Auto" or a specified transmit rate.	Auto
Transmit Power	Select from "Max", "High", "Medium" and "Low".	Max

Advanced		
Item	Description	Default
Channel Width	Select from "20MHz", "40MHz". 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	Auto
Enable WMM	Click "ON" to enable WMM.	ON
Enable Short GI	Click "ON" to enable Short GI (Short Guard Interval), short GI is a blank time between two symbols, it can provide a long buffer time to delay signal. Using the Short Guard Interval would provide an 11% increase in data rates, but also may result in higher packet error rates.	ON
Enable AP Isolation	Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", "none".	none

Access Point
Advanced
ACL
Status

^ General Settings

Enable ACL  ON  OFF

ACL Mode Accept v ?

^ Access Control List

Index	Description	MAC Address
<span style="color: white; font-weight: bold;">+</span>		

ACL

^ Access Control List

Index

Description

MAC Address

ACL		
Item	Description	Default
Enable ACL	Click to enable ACL (Access Control List).	Disable
ACL Mode	Select from "Accept" and "Deny". 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. <b>Note:</b> R2000 can only allow or deny devices which are included in "Access Control List" at one time.	Accept
Access Control List	Click " <span style="color: blue; font-weight: bold;">+</span> " to add MAC address.	Null

This section allow user to check the AP status and those WiFi client had connected to R2000 AP.

Access Point
Advanced
ACL
Status

**^ AP Status**

**Status** COMPLETED

**Channel** 6

**Channel Width** 20 MHz

**MAC Address** 34:FA:40:08:6A:B5

**^ Associated Stations**

Index	MAC Address	IP Address	Name	Connected Time	Signal
1	14:B9:68:71:E7:75			8	-71 dBm

### 3.11 Interface->WLAN (Optional)

R2000 router support both WiFi AP and WiFi client. The factory default setting of R2000 is as WiFi AP. This section allow user to configure the R2000 router as a WiFi client and set the related parameters.

#### WiFi Client

##### Configure R2000 as a WiFi client

Go to **System->Device Configuration**, select the WiFi mode as Client, click “Submit” and reboot the device to make the setting effect.

Device Configuration

All settings on this page can not be exported.

You need to reboot system for the changes to take effect.

Please note that some configurations may restore to default after reboot.

You need to clear web browser's cache before next login at most of time.

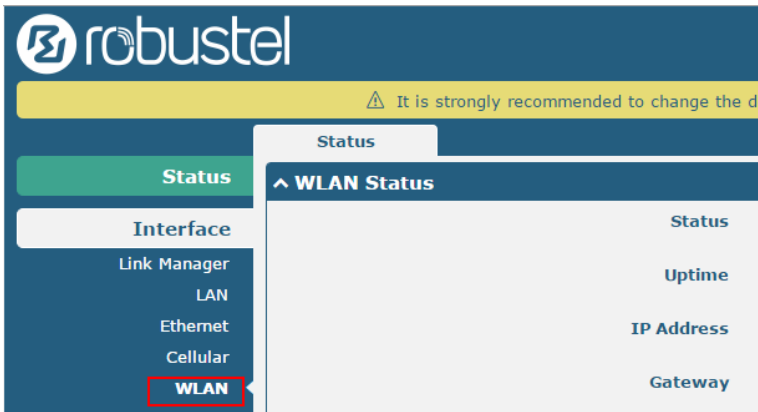
**^ Advanced Device Settings**

**Eth0 Used As WAN**  ON  OFF

**WiFi Mode**  v

**WiFi Region**  ?

After R2000 was configured successfully as a WiFi client, there will appear a WLAN tab in the Interface menu, just as the screenshot below.



Configure the WiFi AP please go to the **Link Manager->WLAN** tab, and the way of configuration refer to the **3.6 Interface->Link Manager** section.

This section allows user to check the WLAN connection status. It includes WLAN status, Link status and WPA status.



**WPA Status**

WPA State: COMPLETED

Frequency: 2437

BSSID: 16:b9:68:71:e7:75

SSID: faye22222

Mode: station


Key Management: WPA2-PSK


Pairwise Cipher: CCMP


Group Cipher: CCMP

**Scan Results**

Index	SSID	MAC Address	Frequency	Signal
1	faye22222	16:B9:68:71:E7:75	2437	-65 dBm
2	3gRouter_AP	00:25:5E:B5:12:35	2437	-65 dBm
3	cfg_ap_ssid	54:36:9B:07:74:71	2422	-70 dBm
4	ABCD	14:CF:92:0A:1B:19	2457	-86 dBm
5	wlan	00:04:ED:BF:0A:3B	2412	-83 dBm

User can scan the surrounding SSIDs in this section. Please click , and then click "Scan" to scan the surrounding SSIDs.

**Scan Results** 

Index	SSID	MAC Address	Frequency	Signal
				


### 3.12 Network->Route


This section allows user to set the static route. (The maximum number of the static route is twenty.)

#### Static Route

Static Route | **Status**

**Static Route Table**

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

Click "" to add static routes, the maximum number of static routes is 20.

**Static Route**

^ **Static Route**

**Index**

**Description**

**Destination**

**Netmask**

**Gateway**

**Interface**

Submit
Close

Static Route		
Item	Description	Default
Index	Show the index of the static route.	1
Destination	Define the destination IP address.	Null
Netmask	Define the Netmask of the destination.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Select from "LAN", "WAN", "TUN"	LAN

**Status**

Static Route
Status

^ **Route Table**

Index	Destination	Netmask	Gateway	Interface	Metric
1	172.16.0.0	255.255.0.0	0.0.0.0	eth-br	0

### 3.13 Network->Firewall

This section allows users to set the Firewall and the related parameters, which includes “Filter”, “Port Mapping” and “DMZ”.

#### Filtering

Filtering

Port Mapping

DMZ

^ General Settings

Enable Filtering  ON  OFF

Default Filtering Policy  v ?

^ Access Control

Enable Remote SSH Access  ON  OFF

Enable Local SSH Access  ON  OFF

Enable Remote Telnet Access  ON  OFF

Enable Local Telnet Access  ON  OFF

Enable Remote HTTP Access  ON  OFF

Enable Local HTTP Access  ON  OFF

Enable Remote HTTPS Access  ON  OFF

Enable Remote Ping Respond  ON  OFF ?

Enable DOS Defending  ON  OFF

^ Filtering Rules

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

Click “+” to add filtering rules. (The maximum number of the filtering rule is twenty.)

**^ Filtering Rules**

**Index**

**Description**

**Source Address**  ?

**Source MAC**  ?

**Target Address**  ?

**Protocol**  v

**Action**  v

Filtering		
Item	Description	Default
Enable Filtering	Enable filtering rules.	ON
Default Filtering Policy	Select from "Accept" and "Drop". Accept: Router will accept all the connecting requests except the hosts which fit the filter list. Drop: Router will only reject the connecting requests from the hosts which fit the filter list.	accept
Enable Remote SSH Access	Enable to allow users to access the router remotely on the internet side via SSH.	OFF
Enable Local SSH Access	Enable to allow users to access the router on the local Ethernet via SSH.	ON
Enable Remote Telnet Access	Enable to allow users to access the router remotely on the internet side via Telnet.	OFF
Enable Local Telnet Access	Enable to allow users to access the router on the local Ethernet via Telnet.	ON
Enable Remote Http Access	Enable to allow users to access the router remotely on the internet side via Http.	OFF
Enable Local Http Access	Enable to allow users to access the router on the local Ethernet via Http.	ON
Enable Remote Https Access	Enable to allow users to access the router remotely on the internet side via Https.	ON
Enable Remote Ping Respond	Enable to make router reply the Ping requests from the internet side.	ON
Enable DOS Defending	Enable to defend dos attack. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Index	Show the index of the filtering rule or the MAC binding rule.	1
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 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



Filtering		
Item	Description	Default
Protocol	Select from "All", "TCP", "UDP", "ICMP", "TCP-UDP". If you don't know what kinds of protocol of your application, we recommend you select "ALL".	All
Action	Select from "Accept", "Drop".	Drop

### Port Mapping

Filtering
Port Mapping
DMZ

^ Port Mapping Rules

Index	Description	Internet Port	Local IP	Local Port	Protocol	
<span style="color: #0070C0;">+</span>						

Click "+" to add port mapping rules. (The maximum number of the port mapping rule is forty.)

^ Port Mapping Rules

<b>Index</b>	<input type="text" value="1"/>
<b>Description</b>	<input type="text"/>
<b>Internet Port</b>	<input type="text"/> <span style="color: #0070C0;">?</span>
<b>Local IP</b>	<input type="text"/>
<b>Local Port</b>	<input type="text"/> <span style="color: #0070C0;">?</span>
<b>Protocol</b>	<span style="border: 1px solid #0070C0; padding: 2px;">TCP-UDP</span> <span style="color: #0070C0;">v</span>

Port Mapping		
Item	Description	Default
Index	Show the index of the port mapping rule.	1
Internet Port	The port of the internet side which you want to forward to LAN side.	Null
Local IP	The device's IP on the LAN side which you want to forward the data to.	Null
Local Port	The device's port on the LAN side which you want to forward the data to.	Null
Protocol	Select from "TCP", "UDP" and "TCP-UDP".	TCP-UDP

## DMZ

Filtering
Port Mapping
DMZ

^ DMZ Settings

Enable DMZ  ON  OFF

Host IP Address

Source IP Address  ?

DMZ		
Item	Description	Default
Enable DMZ	Select to enable the DMZ function. 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 which on the internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

## 3.14 VPN->IPSec

This section allows users to set the IPSec and the related parameters.

### General

General
Tunnel
Status
x509

^ General Settings

Enable NAT Traversal  ON  OFF

Keepalive  ?

Debug Enable  ON  OFF

General		
Item	Description	Default
Enable NAT Traversal	Tick to enable NAT Traversal for IPSec. This item must be enabled when router under NAT environment.	ON
Keepalive	The interval that router sends packets to NAT box so that to avoid it remove the NAT mapping.	60
Debug Enable	Enable this function, and it will output IPSec information to the debug port.	OFF

**Tunnel**

General **Tunnel** Status x509

^ Tunnel Settings

Index	Enable	Description
-------	--------	-------------

+

Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)

^ Tunnel Settings

Index:

Enable:  ON  OFF

Description:

Gateway:  ?

Mode:  v

Protocol:  v

Local Subnet:  ?

Remote Subnet:  ?

Tunnel Settings		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable IPsec Tunnel.	ON
Description	Enter some simple words about the IPsec Tunnel.	Null
Gateway	Enter the address of remote side IPsec VPN server.	Null
Mode	Select from “Tunnel” and “Transport”. Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it. Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.	Tunnel
Protocol	Select the security protocols from “ESP” and “AH”. ESP: Uses the ESP protocol. AH: Uses the AH protocol.	ESP
Local Subnet	Enter IPsec Local Protected subnet’s address with mask, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter IPsec Remote Protected subnet’s address with mask, e.g. 10.8.0.0/24	Null

When choose "Authentication Type" to "PSK".

**^ IKE Settings**

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

When choose "Authentication Type" to "CA".

**^ IKE Settings**

<b>Negotiation Mode</b>	Main	▼
<b>Authentication Algorithm</b>	MD5	▼
<b>Encrypt Algorithm</b>	3DES	▼
<b>IKE DH Group</b>	MODP(1024)	▼
<b>Authentication Type</b>	CA	▼
<b>Private Key Password</b>	<input type="text"/>	
<b>IKE Lifetime</b>	86400	?

When choose “Authentication Type” to “xAuth PSK”.

**^ IKE Settings**

<b>Negotiation Mode</b>	<input type="text" value="Main"/>	<input type="button" value="v"/>
<b>Authentication Algorithm</b>	<input type="text" value="MD5"/>	<input type="button" value="v"/>
<b>Encrypt Algorithm</b>	<input type="text" value="3DES"/>	<input type="button" value="v"/>
<b>IKE DH Group</b>	<input type="text" value="MODP(1024)"/>	<input type="button" value="v"/>
<b>Authentication Type</b>	<input type="text" value="xAuth PSK"/>	<input type="button" value="v"/>
<b>PSK Secret</b>	<input type="text"/>	
<b>Local ID Type</b>	<input type="text" value="Default"/>	<input type="button" value="v"/>
<b>Remote ID Type</b>	<input type="text" value="Default"/>	<input type="button" value="v"/>
<b>Username</b>	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
<b>Password</b>	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
<b>IKE Lifetime</b>	<input type="text" value="86400"/>	<input style="float: right;" type="button" value="?"/>

When choose “Authentication Type” to “xAuth CA”.

**^ IKE Settings**

<b>Negotiation Mode</b>	<input type="text" value="Main"/>	<input type="button" value="v"/>
<b>Authentication Algorithm</b>	<input type="text" value="MD5"/>	<input type="button" value="v"/>
<b>Encrypt Algorithm</b>	<input type="text" value="3DES"/>	<input type="button" value="v"/>
<b>IKE DH Group</b>	<input type="text" value="MODP(1024)"/>	<input type="button" value="v"/>
<b>Authentication Type</b>	<input type="text" value="xAuth CA"/>	<input type="button" value="v"/>
<b>Private Key Password</b>	<input type="text"/>	
<b>Username</b>	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
<b>Password</b>	<input type="text"/>	<input style="float: right;" type="button" value="?"/>
<b>IKE Lifetime</b>	<input type="text" value="86400"/>	<input style="float: right;" type="button" value="?"/>

IKE Settings		
Item	Description	Default
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main

IKE Settings		
Item	Description	Default
Authentication Algorithm	Select from "MD5" and "SHA1" to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
Encrypt Algorithm	Select from "3DES", "AES128" and "AES256" to be used in IKE negotiation. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	3DES
IKE DH Group	Select from "MODP (1024)" and "MODP (1536)" to be used in key negotiation phase 1. MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
Authentication Type	Select from "PSK", "CA", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. xAuth: Extended Authentication to AAA server.	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "IP Address", "FQDN" and "User FQDN" for IKE negotiation. "Default" stands for "IP Address". IP Address: 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 gateway, 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 gateway, e.g., test@robustel.com.	Default
Remote ID Type	Select from "IP Address", "FQDN" and "User FQDN" for IKE negotiation. IP Address: 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 gateway, 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 gateway, e.g., test@robustel.com.	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key.	Null
Username	User name used for xAuth.	Null
Password	Password used for xAuth.	Null

When choose the “Tunnel Setting->General Setting->Protocol” to “ESP”.

**^ SA Settings**

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

When choose the “Tunnel Setting->Protocol” to “AH”.

**^ SA Settings**

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

**^ Advanced Settings**

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

SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256” when you select “ESP” in “Protocol”; Note: 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” and “SHA1”to be used in SA negotiation.	MD5
PFS Group	Select from “PFS (N/A)”, “MODP (1024)” and “MODP (1536)”. PFS (N/A): Disable PFS Group MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
SA Lifetime	Set the IPsec SA lifetime. Note: 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	60

SA Settings		
Item	Description	Default
	received from the peer. DPD: Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPSec packet, DPD checks the time the last IPSec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPSec SAs based on the IKE SA.	
DPD Failures	Set the timeout of DPD packets.	180
Advanced Settings		
Enable Compression	Tick to enable compressing the inner headers of IP packets.	OFF

**Status**

This section allow user to check the status of the IPSec tunnel.

General	Tunnel	Status	x509
<b>^ Tunnel Status</b>			
Index	Description	Status	Uptime

**x509**

User can upload the X509 certificate for the IPSec tunnel in this section.

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

x509		
Item	Description	Default
Tunnel Name	Select the name of the tunnel.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt	Null

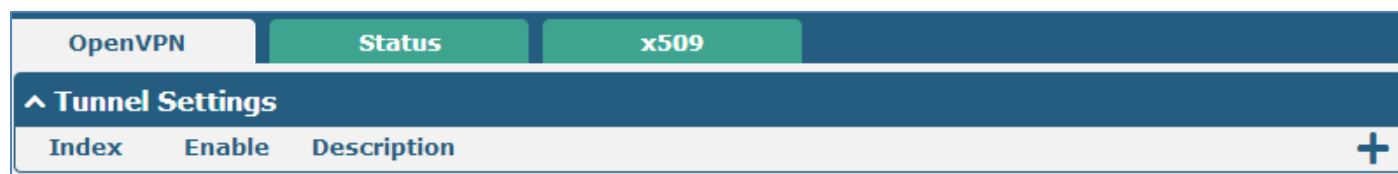


x509		
Item	Description	Default
	@private.key @crl.pem	
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

### 3.15 VPN->OpenVPN

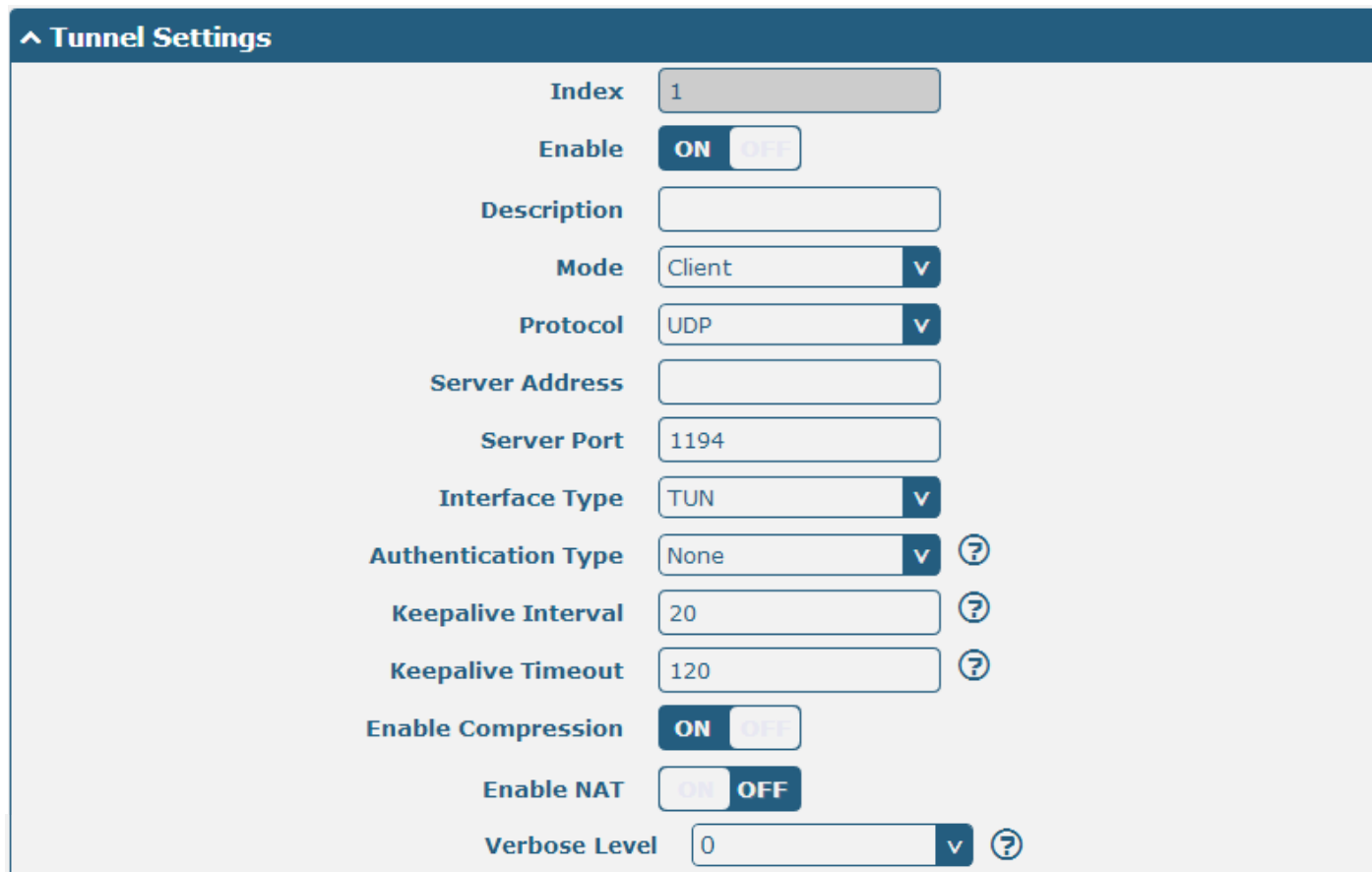
This section allows users to set the OpenVPN and the related parameters.

#### OpenVPN



Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)

When choose “Authentication Type” to “None”.



When choose "Authentication Type" to "Preshared".

**^ Tunnel Settings**

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

When choose "Authentication Type" to "Password".

**^ Tunnel Settings**

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

When choose "Authentication Type" to "X509CA".

**^ Tunnel Settings**

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

When choose “Authentication Type” to “X509CA Password”.

**^ Tunnel Settings**

<b>Index</b>	<input type="text" value="1"/>
<b>Enable</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
<b>Description</b>	<input type="text"/>
<b>Mode</b>	<input type="text" value="Client"/> ▼
<b>Protocol</b>	<input type="text" value="UDP"/> ▼
<b>Server Address</b>	<input type="text"/>
<b>Server Port</b>	<input type="text" value="1194"/>
<b>Interface Type</b>	<input type="text" value="TUN"/> ▼
<b>Authentication Type</b>	<input type="text" value="X509CA Password"/> ▼ <span style="float: right;">?</span>
<b>Username</b>	<input type="text"/>
<b>Password</b>	<input type="text"/>
<b>Encrypt Algorithm</b>	<input type="text" value="BF"/> ▼
<b>Keepalive Interval</b>	<input type="text" value="20"/> <span style="float: right;">?</span>
<b>Keepalive Timeout</b>	<input type="text" value="120"/> <span style="float: right;">?</span>
<b>Enable Compression</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
<b>Enable NAT</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>Verbose Level</b>	<input type="text" value="0"/> ▼ <span style="float: right;">?</span>

Tunnel Settings		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable OpenVPN tunnel.	ON
Description	Enter some simple words about the OpenVPN Tunnel.	Null
Mode	Select from “P2P”, “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client”.	UDP
Server Address	Enter the OpenVPN server address.	Null
Server Port	Enter the OpenVPN server port	1194
Interface Type	Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is this: a TUN device is a virtual IP point-to-point device and a TAP device is a virtual Ethernet device.	TUN

Tunnel Settings		
Item	Description	Default
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". "None" and "Preshared" type just work with p2p mode.	None
Local IP	When the "Mode" is "P2P". Define the local IP address of OpenVPN tunnel.	Null
Remote IP	When the "Mode" is "P2P". Define the remote IP address of OpenVPN tunnel.	Null
Username	User name used for Authentication Type "Password" or "X509CA Password".	Null
Password	Password used for Authentication Type "Password" or "X509CA Password".	Null
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "AES256". BF: Uses the BF algorithm in CBC mode and 128-bit key. DES: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES192: Uses the AES algorithm in CBC mode and 192-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	BF
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Password of Private Key for Authentication Type "X509CA"	Null
Enable Compression	Enable to compress the data stream.	ON
Enable NAT	Tick to enable NAT for OpenVPN. The source IP address of host behind R2000 will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log. Values range from 0 to 11. 0 -- No output except fatal errors. 1 to 4 -- Normal usage range. 5 -- Output R and W characters to the console for each packet read and write. 6 to 11 -- Debug info range	0

**^ Advanced Settings**

Enable HMAC Firewall
 ON  OFF

Enable PKCS#12
 ON  OFF

Enable nsCertType
 ON  OFF

Expert Options
 ?

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

Status

OpenVPN	Status	x509	
^ Tunnel Status			
Index	Description	Status	Uptime

x509

OpenVPN	Status	x509
^ X509 Settings <span style="float: right;">?</span>		
Tunnel Name		Tunnel 1 <span style="float: right;">v</span>
Certificate Files		Choose File No file chosen <span style="float: right;">↑</span>

^ Certificate Files			
Index	File Name	File Size	Last Modification

x509		
Item	Description	Default
Tunnel Name	Select the name of the Tunnel1 to Tunnel3. Because the maximum number of the tunnel is three.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

### 3.15 VPN->GRE

This section allows users to set the OpenVPN and the related parameters.

Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)

GRE		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates packets in order to route other protocols over IP networks.	ON
Description	Enter some simple words about the GRE Tunnel.	Null
Remote IP Address	Set remote IP Address of the virtual GRE tunnel.	Null
Local Virtual IP	Set local IP Address of the virtual GRE tunnel.	Null
Remote virtual IP	Set remote IP Address of the virtual GRE tunnel.	Null
Enable Default Route	All the traffics of R2000 router will go through the GRE VPN.	OFF
Enable NAT	Tick to enable NAT for GRE. The source IP address of host Behind R2000 will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

This section allow user to check the status of GRE tunnel.



### 3.16 Services->Syslog

This section allows users to set the syslog parameters.

Syslog

^ Syslog Settings

Enable ON OFF

Syslog Level Notice v

Save Position RAM v ?

Log to Remote ON OFF ?

^ Application Debug Control

Enable Modem Debug ON OFF

Enable Link Manager Debug ON OFF

Enable App Debug ON OFF ?

Syslog		
Syslog Settings		
Item	Description	Default
Enable	Click to enable Syslog setting.	OFF
Syslog Level	Select form “Debug”, “Info”, “Notice”, “Warning”, “Error” which from low to high. The lower level will output more syslog in detail.	Notice
Save Position	Select the save position from “RAM”, “NVM” and “Console”. Choose “RAM”, the data will be cleared after reboot. But it’s not recommended that saving syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Application Debug Control		
Enable Modem Debug	Click to enable router to debug Modem.	ON
Enable Link Manager Debug	Click to enable router to debug Link Manager.	ON
Enable APP Debug	Click to enable router’s debug control for all other applications.	ON

### 3.17 Services->Event

This section allows users to set the Event parameters.

Event
Notification
Query

**^ General Settings**

**Signal Quality Threshold**  ?

Event @ Event		
Item	Description	Default
Signal Quality Threshold	Router will generate log event when signal quality less than the threshold, 0 means disable.	0

Event
Notification
Query

**^ Event Notification Group Settings**

<b>Index</b>	<b>Description</b>	<b>Send SMS</b>	<b>Save to NVM</b>	+
--------------	--------------------	-----------------	--------------------	---

Click “+” button to add an Event parameters.

**Notification**

**^ Event Notification Group Settings**

<b>Index</b>	<input style="width: 150px;" type="text" value="1"/>
<b>Description</b>	<input style="width: 150px;" type="text"/>
<b>Send SMS</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
<b>Save to NVM</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <span style="float: right; font-size: 20px;">?</span>

**^ Event Selector**

**System Startup**  ON  OFF

**System Reboot**  ON  OFF

**System Time Update**  ON  OFF

**Configuration Change**  ON  OFF

**Cellular Network Type Change**  ON  OFF

**Cellular Data Stats Clear**  ON  OFF

**Poor Signal Quality**  ON  OFF

**Link Switching**  ON  OFF

**WWAN HS**  ON  OFF

Notification@ Event		
Item	Description	Default
Index	The index of event notification group.	1
Description	Enter some simple words to describe the Notify Group.	Null
Sent SMS	Click to enable router to send event notification SMS. Set the phone number that is used for receiving event notification, and use ';' to separate each number.	OFF
Save to NVM	Click to enable router to save event to nonvolatile memory.	OFF
Event Selector	Click to enable Event feature. There are numbers of R2000's main running event code you can select, such as "System Startup", "System Reboot", "System Time Update", etc.	OFF

Event
Notification
Query

^ Event Detail

**Save Position**

**Filter Message**

```
Feb 11 08:24:54, system startup
Feb 11 08:24:58, LAN port link up, port 1
Feb 11 08:25:12, WWAN (cellular) up, using SIM1
Feb 11 08:25:25, system time update
Feb 11 09:25:26, WWAN (cellular) down, using SIM1
Feb 11 09:25:39, WWAN (cellular) up, using SIM1
```

Clear
Refresh

Query @ Event		
Item	Description	Default
Save Position	Select the events' save position from "RAM", "NVM". 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

### 3.18 Services->NTP

This section allows users to set the NTP parameters.

NTP

Status

^ Timezone Settings

Time Zone

Expert Setting

?

^ NTP Client Settings

Enable

ON  OFF

Primary NTP Server

Secondary NTP Server

NTP Update Interval

?

^ NTP Server Settings

Enable

ON  OFF

Timezone Settings @ NTP		
Item	Description	Default
Time Zone	Select your local time zone.	UTC+08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Setting @ NTP		
Enable	Click to enable the router to synchronize time from NTP server. <b>Note:</b> R2000 doesn't have the RTC, so NTP client function must always be ON.	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, 0 means update only once.	0
NTP Server Setting @ NTP		
Enable	Click to enable the NTP server function of router.	OFF

The status part of NTP allows user to check the current time of R2000 and also synchronize the router time with PC.

Click Sync button to make the router time synchronize with PC.

NTP
Status

^ Time

**System Time** 2015-01-01 09:43:23

**PC Time** 2015-12-21 16:52:52 Sync

**Last Update Time** Not Updated

### 3.19 Services->SMS

This section allows users to set the SMS parameters.

SMS
SMS Testing

^ SMS Management Settings

**Enable** ON OFF

**Authentication Type** Password v ?

**Phone Number**  ?

SMS		
Item	Description	Default
Enable SMS Management	Click to enable SMS Management function.	ON
Authentication Type	<p>Select Authentication Type from “Password”, “Phonenum”, “Both”.</p> <p>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; ...”</p> <p><b>Note:</b> Set the WEB manager password in <b>System-&gt;User Management</b> section.</p> <p>Phonenum: use the Phone number for authenticating, user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; ...”</p> <p>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; ...”</p>	Password
Phone Number	Set the Phone Number that is allowed for SMS management, and use ‘;’ to separate each number.	Null

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

SMS
SMS Testing

^ SMS Testing

**Phone Number**

**Message**

**Result**

SMS Testing		
Item	Description	Default
Phone Number	Enter the specified phone number which will receive the SMS from R2000 router.	Null
Message	Enter the message that R2000 router will sent it to the specified phone number.	Null
Result	The result of the SMS test will display in the result box.	Null

### 3.20 Services->DDNS

This section allows users to set the DDNS parameters.

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

DDNS
Status

^ DDNS Settings

**Enable**  ON  OFF

**Service Provider**  v

**Hostname**

**Username**

**Password**

DDNS		
Item	Description	Default
Enable	Click to enable DDNS function.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322”. <b>Note:</b> the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the Host name of the DDNS server provided.	Null
Username	Enter the user name of the DDNS server provided.	Null
Password	Enter the password of the DDNS server provided.	Null

DDNS
Status

^ DDNS Status

Status

Last Update Time

Status		
Item	Description	Default
Status	Show current status of DDNS service.	Null
Last Update Time	Show the time that DDNS updated successfully at last time.	Null

### 3.21 Services->VRRP

This section allows users to set the VRRP parameters.

VRRP

^ VRRP Settings

**Enable**  ON  OFF

**Interface**  v

**Group ID**

**Priority**

**Interval**  ?

**Virtual IP Address**

VRRP		
Item	Description	Default
VRRP	VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN).Using VRRP, a virtual IP address can be specified manually.	Null



VRRP		
Item	Description	Default
Enable	Click to enable VRRP protocol.	OFF
Interface	Select from “lan0” and “lan1”.	lan0
Group ID	Specify which VRRP group of this router belong to.	1
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	120
Interval	The interval that master router sends VRRP packets to backup routers.	5
Virtual IP Address	A virtual IP address is shared among the routers, with one designated as the master router and the others as backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router)	192.168.0.1

### 3.22 Services->SSH

SSH
Keys Management

^ SSH Settings

Enable  ON  OFF

Port

Disable Password Logins  ON  OFF

SSH		
Item	Description	Default
Enable	Enable the function that user can access R2000 Router via SSH.	OFF
Port	Set the port of the SSH access.	22
Disable Password Logins	Switch to “ON” and disable password logins, so that user cannot access R2000 via SSH. In this situation, you should import the authorized key into R2000 in <b>Keys Management</b> part for accessing R2000. Switch to “OFF”, you can access R2000 via SSH normally.	OFF

SSH
Keys Management

^ Import Authorized Keys

Authorized Keys

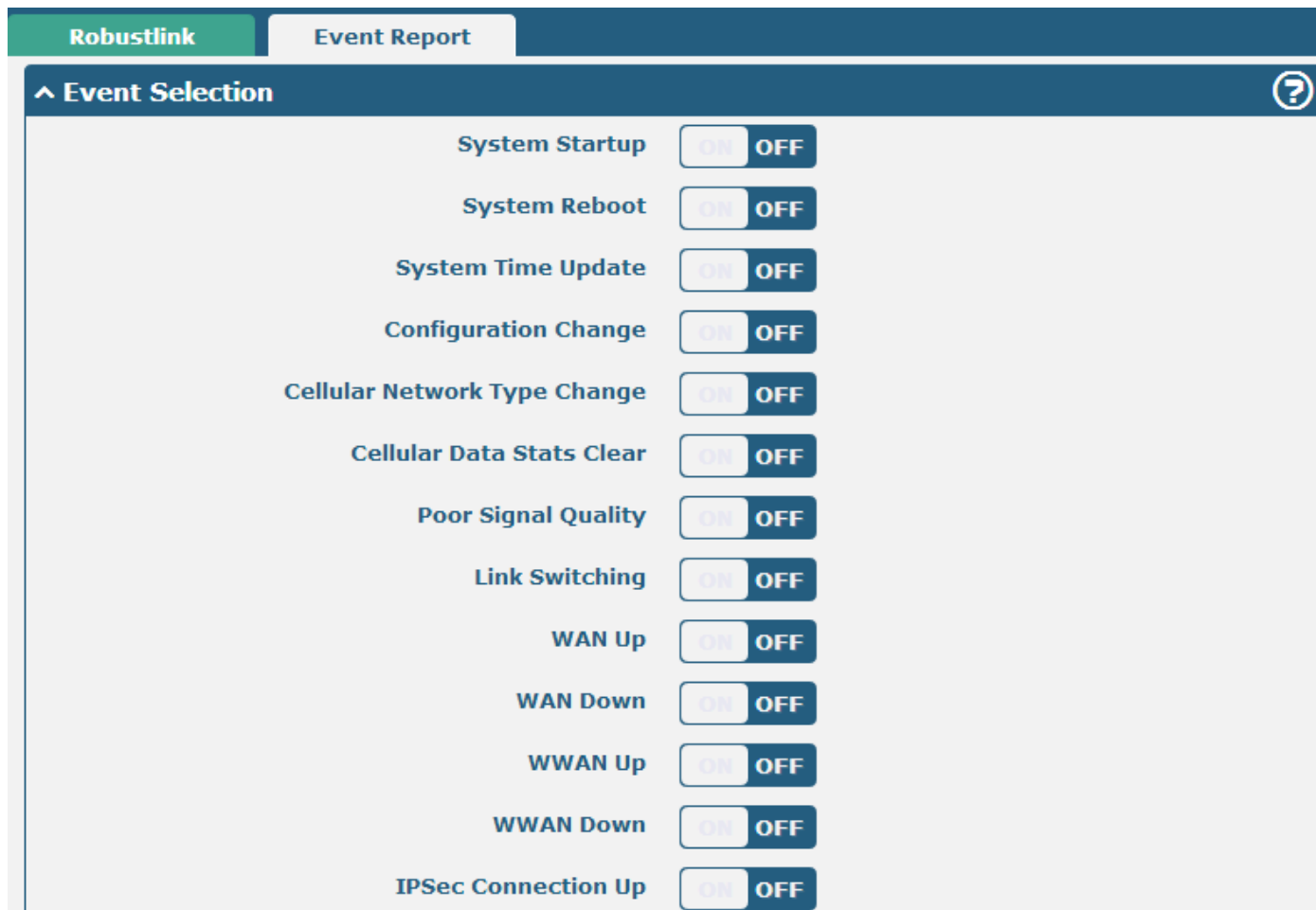
Keys Management	
Item	Description
Authorized Keys	<p>Effective when <b>SSH-&gt;Disable Password Logins</b> is “ON”.</p> <p>Select a key file from PC, then click <span style="background-color: #008080; color: white; padding: 2px 5px; border: 1px solid #ccc;">Import</span> button to import the key file in R2000. So that you can access R2000 via SSH without password.</p>

### 3.23 Services->Robustlink (optional APP)

Robustlink is a M2M management platform, which is developed independently by the Robustel Company. R2000 can be managed by Robustlink. User can set the relative parameters in this section. This function is as an APP which needs to install into R2000 in **System->APP Center** unit.

Robustlink		
Item	Description	Default
Enable	Switch to ON to enable the Robustlink.	
Server address	Enter IP address or domain name of RobustLink.	Null
Port	Enter port number of RobustLink.	31000
Password	Enter the password preset in RobustLink. Valid characters: a-z, A-Z, 0-9, @, ., -, #, \$, *. <i>Note: The passwords set in R2000 and RobustLink need to be the same.</i>	Null

R2000 support report the Event which has happened to Robustlink platform. In this section, user can select the events those will be reported to Robustlink.



Event Report	
Item	Description
Events	Switch "ON" to enable the event.

### 3.24 Services->Web Server

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

The screenshot shows the 'Web Server' configuration page with the 'Certificate Management' tab selected. Under the 'General Settings' section, there are two input fields: 'HTTP Port' with the value '80' and 'HTTPS Port' with the value '443'. Each field has a help icon (question mark) to its right.

Basic @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in R2000'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 R3000's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in R2000'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 R2000's Web Server. <b>Note:</b> <i>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.</i>	443
Login Timeout (s)	Enter the Login timeout you want to change in R3000's Web Server. After "Login Timeout", R3000 will force to log out the Web GUI and then you need to re-login again to Web GUI.	1800

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

The screenshot shows the 'Web Server' configuration page with the 'Certificate Management' tab selected. Under the 'Import Certificate' section, there is a dropdown menu for 'Import Type' set to 'CA'. Below it, there is a section for 'HTTPS Certificate' with a 'Choose File' button, the text 'No file chosen', and an 'Import' button.

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

### 3.25 Services->SNMP (optional APP)

This function is as an APP which needs to install into R2000 in **System->APP Center** unit. We can download the MIB file directly from web interface. And then we can manage the R2000 router via SNMP tool with the MIB file.

SNMP Agent
SNMP Trap
MIBS

**^ SNMP Agent Settings**

**Enable SNMP Agent**  ON  OFF

**Port**

**Version**

**Location Info**

**Contact Info**

**System Name**

**Readonly Community Name**

**Readwrite Community Name**

**Authentication Algorithm**

**Privacy Algorithm**

SNMP Agent @ SNMP		
Item	Description	Default
Enable SNMP Agent	Switch "ON" to enable SNMP Agent.	OFF
Port	UDP port for sending and receiving SNMP requests.	161
Version	Select from "SNMPv1", "SNMPv2" and "SNMPv3".	SNMPv3
Location Info	Enter the router's location info which will send to NMS (Network Management System).	null
Contact Info	Enter the router's contact info which will send to NMS	null

SNMP Agent @ SNMP		
Item	Description	Default
System name	Enter the router's system name which will send to NMS.	null
Readonly Community Name	Enter the community name which was allowed only to get the status of router.	null
Readwrite Community Name	Enter the community name which was allowed to get the status and set the configuration of router.	null
Authentication Algorithm	Select from "MD5" or "SHA". The authentication password default to be the login password of router. The Factory Default login password of router is "admin". We can change the password in <b>System-&gt; User Management</b> section. The authentication password must be the same as privacy password on NMS.	MD5
Privacy Algorithm	Select from "DES" or "AES". The privacy password default to be the login password of router. The Factory Default login password of router is "admin". We can change the password in <b>System-&gt; User Management</b> section. The privacy password must be the same as authentication password on NMS.	DES

SNMP Agent
SNMP Trap
MIBS

**^ SNMP Trap Settings**

**Enable SNMP Trap**  ON  OFF

**Version**  v

**Receiver Address**

**Receiver Port**

**^ SNMPv3 Authentication**

**Username**

**Authentication Algorithm**  v

**Authentication Password**

**Privacy Algorithm**  v

**Privacy Password**

^ Event Selection
?

System Startup  ON  OFF

System Reboot  ON  OFF

System Time Update  ON  OFF

Configuration Change  ON  OFF

Cellular Network Type Change  ON  OFF

Cellular Data Stats Clear  ON  OFF

Poor Signal Quality  ON  OFF

Link Switching  ON  OFF

SNMP Trap		
Item	Description	Default
Enable SNMP Trap	Switch "ON" to enable SNMP Trap feature.	Disable
Version	Select from "SNMPv1", "SNMPv2" and "SNMPv3".	SNMPv2
Receiver Address	Enter NMS (Network Management System) IP address.	Null
Receiver Port	Enter NMS port number	0
SNMPv3 Authentication		
Username	Set the username for NMS to receive the SNMP trap.	null
Authentication Algorithm	Select from "MD5" or "SHA".	MD5
Authentication Password	Set the authentication password for NMS to receive the SNMP trap.	null
Privacy Algorithm	Select from "DES" or "AES".	DES
Privacy password	Set the privacy password for NMS to receive the SNMP trap.	null
Event Selection		
Switch "ON" to enable the event. When the enabled event occurs, router will sent the related SNMP trap to NMS.		

SNMP Agent
SNMP Trap
MIBS

^ SNMP MIBS

SNMP MIBS Generate

SNMP MIBS Download

MIBS	
Item	Description
Generate	Click to generate the SNMP MIB file.
Download	Click to download the SNMP MIB file which is used to manage the R2000 router via SNMP tool.

### 3.26 Services->Advanced

This section allows users to set the Advanced and parameters.

System
Reboot
AT over Telnet

**^ System Settings**

Device Name

router

?

User LED Type

SIM

?

System @ Advanced		
Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed. Valid characters: a-z, A-Z, 0-9, ., -.	router
User LED Type	Select from "None", "SIM", "NET", "OpenVPN" and "IPSec".	SIM

System
Reboot
AT over Telnet

**^ 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

System
Reboot
AT over Telnet

**^ General Settings**

Enable

ON  OFF

Port

0

AT Cmd COM Port

ttyUSB0

v

AT over Telnet @ Advanced		
Item	Description	Default
Enable	Click to enable AT over Telnet function.	OFF
Port	Enter a specific port number to allow user sent AT command to this router over telnet.	0
AT Cmd COM Port	Select a COM port used for identifying the AT command.	ttyUSB0



### 3.27 System->Debug

This section allow user to check and download the syslog details.

Syslog

^ Syslog Details

Log Level

Debug ▼

Filtering

?

Manual Refresh ▼

Clear

Refresh

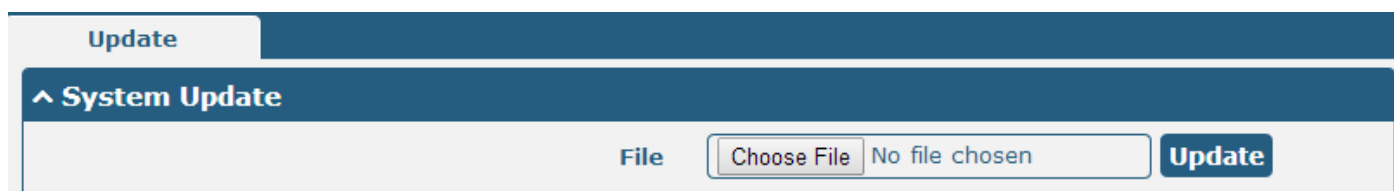
^ Syslog Files

Index	File Name	File Size	Last Modification
^ System Diagnostic Data			
	System Diagnostic Data	<div style="background-color: #005596; color: white; padding: 2px 5px; border-radius: 3px;">Generate</div>	
	System Diagnostic Data	<div style="background-color: #005596; color: white; padding: 2px 5px; border-radius: 3px;">Download</div>	

Syslog Details @ Syslog		
Item	Description	Default
Log Level	Select form "Debug", "Info", "Notice", "Warn", "Error" which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Log will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered log will be displayed in the follow box. Use "&" to	Null

	separate more than one filter message, such as “keyword1&keyword2”.	
Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds”and“30 Seconds”. User can select these intervals to refresh the log information displayed in the follow box. Select “manual refresh”, user should click the refresh button to refresh the syslog.	Manual Refresh
<b>Syslog Files List @ Syslog</b>		
Syslog Files List	It can show at most 5 syslog files in the list, the files’ name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	/
<b>System Diagnosing Data @ Syslog</b>		
Generate	Click to generate the syslog diagnosing file.	/
Download	Click to download system diagnosing file.	/

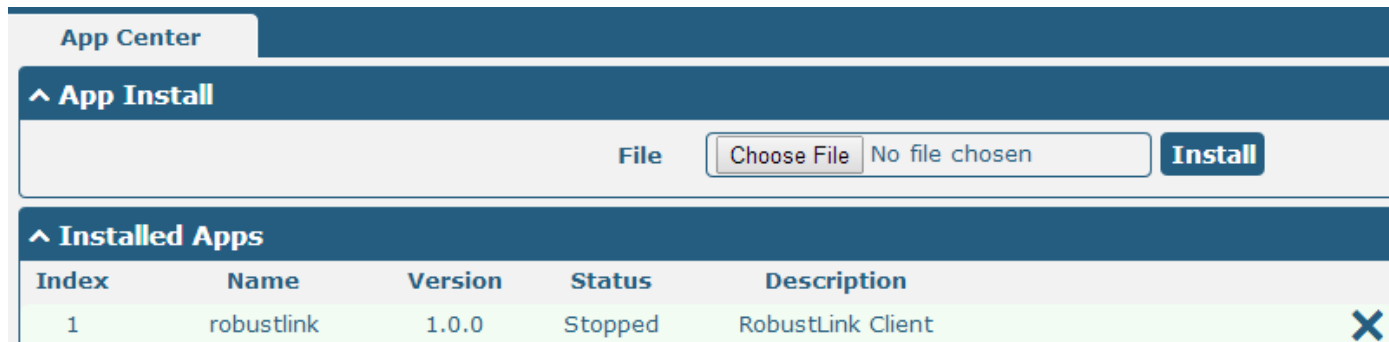
### 3.28 System->Update



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

### 3.29 System->APP Center

This section allow user to add a new function to R2000 router. And the new function will be in the form of an APP file which could be installed in R2000 router. In general, the App which had installed will display in **Service** section.



App Center		
Item	Description	Default
File	Choose the correct App file from your PC, and click <b>Install</b> button to import to R2000 router. File format: xxx.rpk, e.g. r2000-robustlink-1.0.0.rpk.	/
Install Apps	Those Apps which had installed in R2000 will be listed in <b>Installed Apps</b> .	Null
Index	Show the index of the App.	Null
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the Status of the App.	Null
Description	Show the description of the App.	Null

### 3.30 System->Tools

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

The screenshot shows a web-based interface for the 'Ping' tool. At the top, there are four tabs: 'Ping', 'At Debug', 'Traceroute', and 'Sniffer'. The 'Ping' tab is selected. Below the tabs, there is a header with an upward arrow and the text 'Ping'. The main area contains four input fields: 'IP Address' (empty), 'Number of Request' (value 5), 'Timeout' (value 1), and 'Local IP' (empty). Below these fields is a large, empty rectangular box intended for displaying the results of the ping command. At the bottom right of the interface, there are two buttons: a blue 'Start' button and a grey 'Stop' button.

Ping @ Tools		
Item	Description	Default
IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout	Specify 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
At Debug
Traceroute
Sniffer

**^ At Debug**

**Command**

**Result**

Send

At Debug @ Tools	
Item	Description
Command	Enter a At command in Command box, then click <span style="background-color: #004a7c; color: white; padding: 2px 5px; border-radius: 3px;">Send</span> button to send the At command to the cellular module.
Result	It will display the AT commands which respond from the cellular module in this box.

Ping
At Debug
Traceroute
Sniffer

**^ Traceroute**

Trace Address

Trace Hops

Trace Timeout

Start
Stop

Traceroute @ Tools		
Item	Description	Default
Trace Address	Enter the trace destination IP address or domain name.	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 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
At Debug
**Traceroute**
Sniffer

**^ Sniffer**

Interface

Host

Packets Request

Protocol

Status

Start Stop

**^ Capture Files**

Index	File Name	File Size	Last Modification	
1	14-01-01_09-56-26.cap	16682	Wed Jan 1 09:56:30 2014	

Sniffer @ Tools		
Item	Description	Default
Interface	Select form "All", "ETH1", and "ETH2": All: contain all the interface; ETH1: Ethernet interface1; ETH2: Cellular WAN.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
	Click this button to start the sniffer.	/
	Click this button to stop the sniffer. Once click the stop button, a new log file will be displayed in the follow List.	/
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click  to download the log, click  to delete the log file. It can cache a maximum of 5 files.	Null

### 3.31 System->Profile

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

Profile

^ Import Configuration File

Import Type

Keep Other Confgs v ?

XML Configuration File

Browse...

Import

^ Export Configuration File

Export Type

Full v ?

XML Configuration File

Generate

^ Factory Configuration

Factory Configuration

Restore

Import Configuration File @ Profile		
Import Type	Define what to do about the configs that is not contained in the imported file. There are two Import Types: Keep Other Confgs: Keep other configuration unchanged when import XML configuration file. Set Others To Default: Set other configuration to factory default when import XML configuration file.	Keep Other Confgs
XML Configuration File	Click "Browse" to select the XML file in your computer, and then click "Import" to import this file into your router.	
Export Configuration File @ Profile		
Export Type	There are four export Types : Essential: export the configuration file that only include enabled features. Essential && Detailed: export the configuration file that only include enabled features, and attach extra information such as <b>range</b> and <b>default</b> setting of those enable config option. Full: export the configuration file of all features; include both the enabled and disabled features. Full && Detailed: export the configuration file of all features, and attach extra information such as <b>range</b> and <b>default</b> setting of every config option.	Full
Export	Click "Export" and the configuration will be showed in the new popup browser window, then you can save it as a XML file.	
Factory Configuration @ Profile		
Restore	Click the "Restore" button to restore the router to factory default setting.	

### 3.32 System->Device Configuration

Enable or disable the WAN interface.

Device Configuration

All settings on this page can not be exported.

You need to reboot system for the changes to take effect.

Please note that some configurations may restore to default after reboot.

You need to clear web browser's cache before next login at most of time.

^ Advanced Device Settings

**Eth0 Used As WAN**

**WiFi Mode**  v

**WiFi Region**  ?

Advanced Device Settings		
Item	Description	Default
eth0 Used As WAN	Switch button to ON to configure eth0 as WAN interface. Switch button to OFF, it will disable the WAN interface, eth0 will recovery to be LAN interface.	OFF
WiFi Mode	Select from "Client" and "AP". WiFi AP: When enable the WiFi AP mode, R2000 could be accessed by the specified Clients. Please go to Interface->WiFi to configure the parameter of WiFi AP. WiFi Client: When enable the WiFi Client mode, R2000 can access the specified WiFi AP. Please go to Interface->WLAN to configure the parameter of WiFi Client.	Client
WiFi Region	Specify a two-letter country code which defined in ISO 3166-1 alpha-2 standard.	US

### 3.33 System->User Management

This section allows users to modify or add management user accounts.

Super User
Common User

^ Super User Settings

**Old Password**  ?

**New Password**  ?

**Confirm Password**  ?



Super User		
Item	Description	Default
Super User	One router has only one super user account. Under this account, user has the highest authority include modify, add and manage those user accounts.	/
Old Password	The old password of super user which default is "admin", valid characters: a-z, A-Z, 0-9, @, ., -, #, \$, *.	Null
New Password	Enter a new password for the super user, valid characters: a-z, A-Z, 0-9, @, ., -, #, \$, *.	Null
Confirm Password	Enter the new password again which had added in New Password item.	Null

Super User
Common User

^ Common Users Settings

Index	Role	Username
<span style="color: white; font-size: 24px;">+</span>		

Click the "+" button to add a new common user.

**Note:** One router has 5 common user accounts at most.

Common User

^ Common Users Settings

<b>Index</b>	<input style="width: 80%;" type="text" value="1"/>
<b>Role</b>	<input style="border-bottom: 1px solid #004a7c;" type="text" value="Visitor"/> <span style="font-size: 12px;">v</span>
<b>Username</b>	<input style="width: 80%;" type="text"/>
<b>Password</b>	<input style="width: 80%;" type="text"/>

Common User		
Item	Description	Default
Role	Select from "Visitor" and "Editor". 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. Valid characters: a-z, A-Z, 0-9, ., -.	Null
Password	Set the password which at least contains 5 characters. Valid characters: a-z, A-Z, 0-9, @, ., -, #, \$, *.	Null

# Chapter 4 Configuration Examples

## 4.1 Cellular

### 4.1.1 Cellular Dial-Up

This section shows users how to configure the primary and backup SIM card of Cellular Dial-up.

Interface-->Link Manager->General Setting

Select WWAN1 as Primary Link.

The screenshot shows the 'Link Manager' interface with the 'Status' tab selected. Under 'General Settings', 'Primary Link' is set to 'WWAN1', 'Backup Link' is 'None', and 'Emergency Reboot' is 'OFF'. Under 'Link Settings', a table lists two links:

Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP

Click to set the WWAN1's parameter according to the current ISP.

The screenshot shows the configuration for link index 1. Under 'General Settings', 'Index' is 1, 'Type' is WWAN1, and 'Description' is empty. Under 'WWAN Settings', 'Automatic APN Selection' is ON, 'Dialup Number' is \*99\*\*\*1#, 'Authentication Type' is Auto, 'Aggressive Reset' is OFF, 'Switch SIM By Data Allowance' is OFF, 'Data Allowance' is 0, and 'Billing Day' is 1.

^ Ping Detection Settings
?

Enable  ON  OFF

Primary Server

Secondary Server

Interval  ?

Retry Interval  ?

Timeout  ?

Max Ping Tries  ?

^ Advanced Settings

MTU

Overridden Primary DNS

Overridden Secondary DNS

The modifications will take effect after click “Submit” and “save and apply” button.

**Interface-->Cellular**

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

Click to set the SIM card’s parameter according to the application requirement.

Cellular

^ General Settings

Index

SIM Card  v

Phone Number

Extra AT Cmd  ?

^ Cellular Network Settings

Network Type  v ?

Band Select Type  v ?

The modifications will take effect after click “Submit” and “save and apply” button.

## 4.1.2 SMS Remote Control

R2000 supports remote control via SMS. User can use following commands to get the status of R2000, and set all the parameters of R2000.

There are three authentication types for SMS control. You can select from “Password”, “Phonenum” and “Both”.

### An SMS command has following structure:

1. Password mode—Username: Password;cmd1;cmd2;cmd3; ...cmdn (available every phone number).
2. Phonenum mode--cmd1; cmd2; cmd3; ... cmdn (available when the SMS was sent from the phone number which had been added in R2000's phone group).
3. Both mode-- Username: Password;cmd1;cmd2;cmd3; ...cmdn (available when the SMS was sent from the phone number which had been added in R2000's phone group).

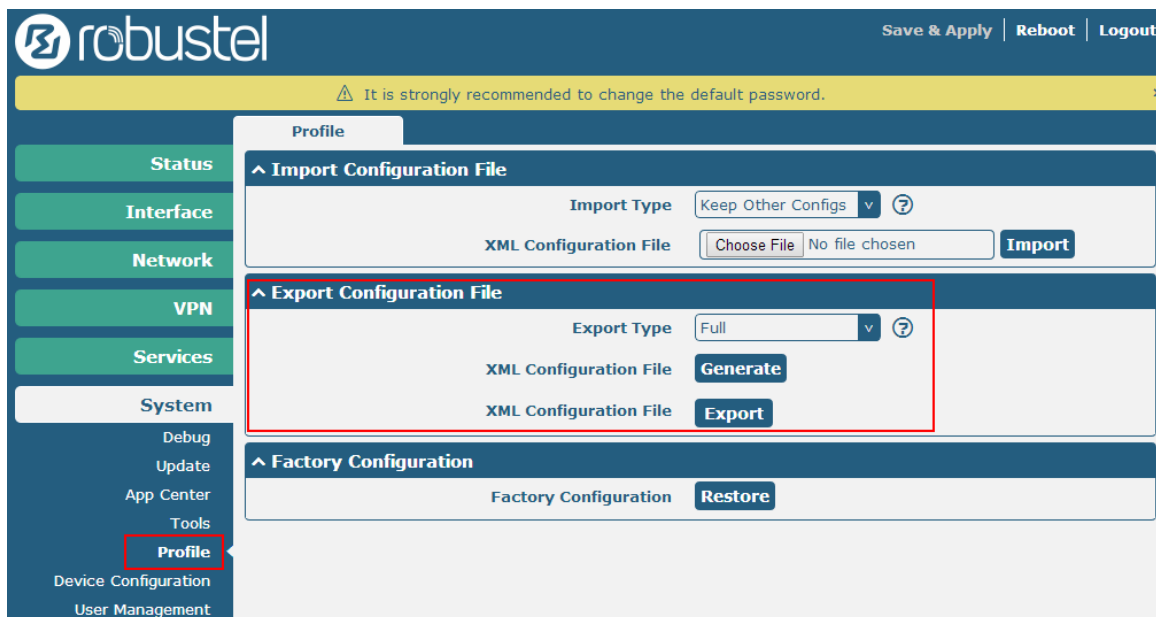
### SMS command Explanation:

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

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

Go to System->Profile->Export Configuration File, select Export type as **Full**, click **Generate** to generate

the XML file and then click **Export** to export the XML file.



### XML command:

```
<lan>
<network max_entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.99.11</ip>
```

```
<netmask>255.255.0.0</netmask>
```

```
<mtu>1500</mtu>
```

**SMS cmd:**

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.99.11
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500
```

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

4. E.g.

**admin:admin;status system**

In this command, username is admin, password is admin, and the function of the command is getting the system status.

**SMS received:**

```
hardware_version = 1.0
firmware_version = "1.2.0 (Rev 399)"
kernel_version = 3.10.49
device_model = R2000
serial_number = 15090140040008
uptime = "0 days, 00:04:07"
system_time = "Tue Dec 22 15:02:36 2015"
```

**admin:admin;reboot**

In this command, username is admin, password is admin, and the command is reboot R2000.

**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 function of the command is disabling the remote\_ssh and remote\_telnet access.

**SMS received:**

```
OK
```

```
OK
```

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

In this command, username is admin, password is admin, and the function of those commands is configuring the LAN parameter.

**SMS received:**

```
OK
```

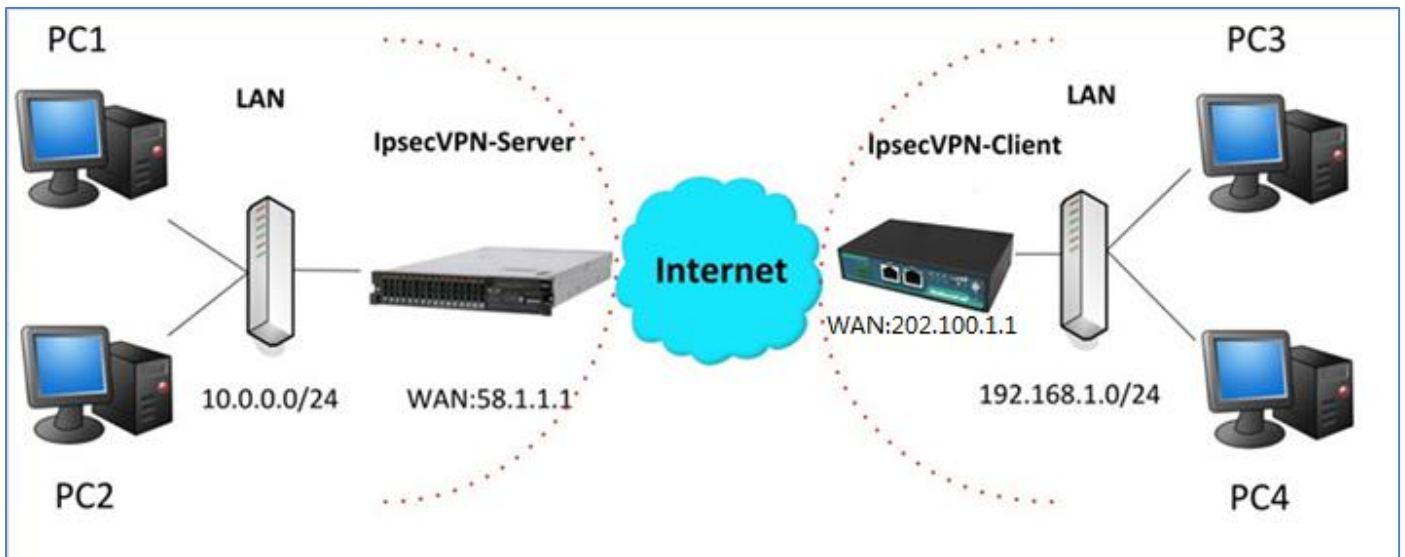
```
OK
```

```
OK
```

```
OK
```

## 4.2 Network

### 4.2.1 IPSEC VPN



**Note:** the configuration of server and client is as follows.

**IPSecVPN\_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

```

## IPSecVPN\_CLIENT:

### VPN--->IPSec--->Tunnel

General	Tunnel	Status	x509
<b>^ Tunnel Settings</b>			
Index	Enable	Description	+

Then click “”.

**Tunnel**

**^ Tunnel Settings**

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

**^ IKE Settings**

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

**^ SA Settings**

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





The modification will take effect after “Submit-->Save&Apply-->Reboot”.

The comparison between server and client is as following picture:

**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

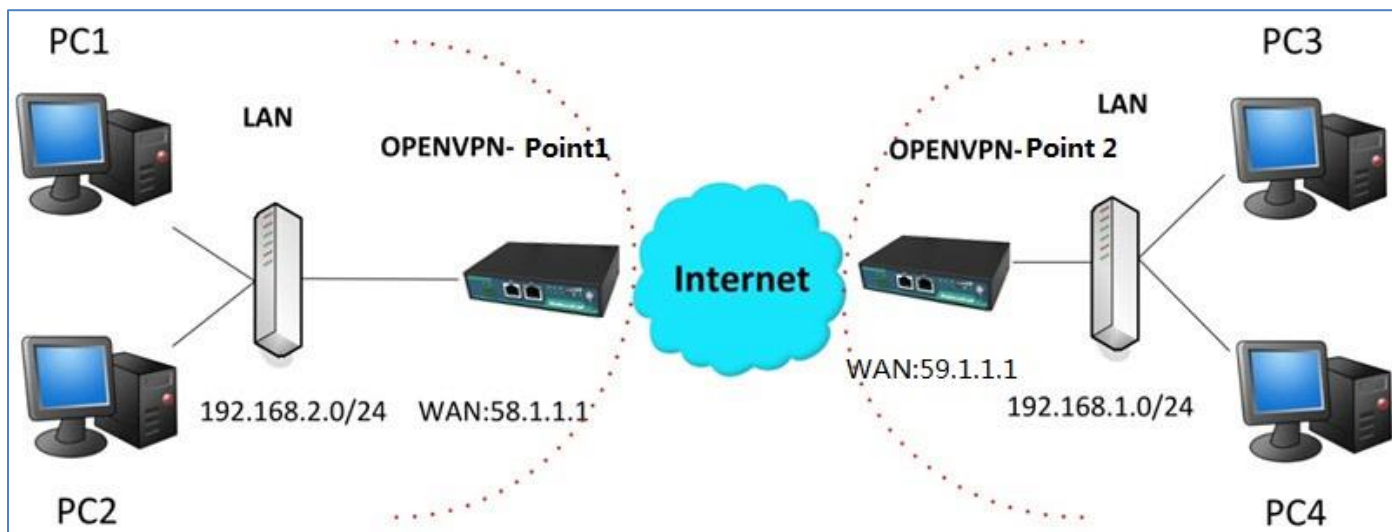
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
                    
```

**Client (R2000 Lite)**

IKE Setting in Client must be consistent with server.

SA Setting in Client must be consistent with server.

## 4.2.2 OPENVPN



**Note:** the configuration of two points is as follows.

### OPENVPN (p2p):

#### Point 1

VPN--->OpenVPN--->OpenVPN

OpenVPN	Status	x509
^ Tunnel Settings		
Index	Enable	Description

Click “+”.

**OpenVPN**

^ Tunnel Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="OpenVPN-Point 1"/>
Mode	<input type="text" value="P2P"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text" value="59.1.1.1"/>
Server 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"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF

^ Advanced Settings

Expert Options	<input type="text" value="route 192.168.1.0 255"/> ?
----------------	--

The modifications will take effect after click “Submit-->Save&Apply”.

## Point 2

VPN--->OpenVPN--->OpenVPN

OpenVPN	Status	x509
^ Tunnel Settings		
Index	Enable	Description

Click “”.

### OpenVPN

#### ^ Tunnel Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="OpenVPN-Point 2"/>
Mode	<input type="text" value="P2P"/> v
Protocol	<input type="text" value="UDP"/> v
Server Address	<input type="text" value="58.1.1.1"/>
Server 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="10.8.0.2"/>
Remote IP	<input type="text" value="10.8.0.1"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF

#### ^ Advanced Settings

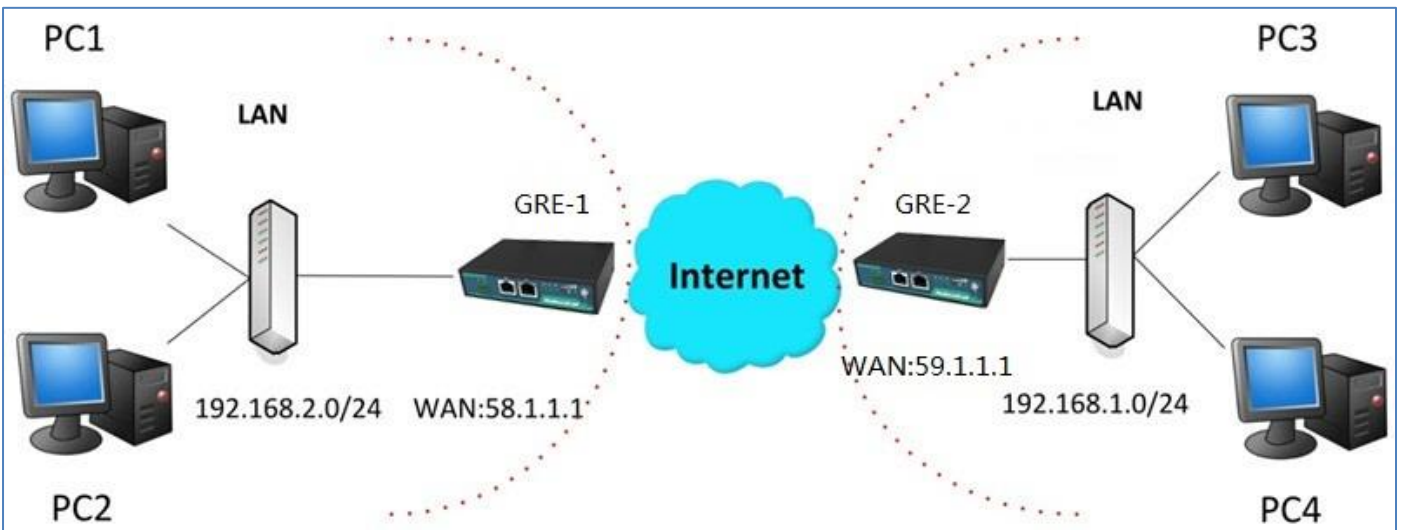
Expert Options	<input type="text" value="route 192.168.2.0 255"/> ?
----------------	--

The modifications will take effect after click "Submit-->Save&Apply".

The comparison between point 1 and point 2 is as following picture:

Point 1	point 2
<div style="background-color: #2c5e8c; color: white; padding: 5px;">OpenVPN</div> <div style="background-color: #2c5e8c; color: white; padding: 5px;">^ Tunnel Settings</div> <p style="margin-left: 20px;">Index: <input type="text" value="1"/></p> <p style="margin-left: 20px;">Enable: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p style="margin-left: 20px;">Description: <input type="text" value="OpenVPN-Point 1"/></p> <p style="margin-left: 20px;">Mode: <input type="text" value="P2P"/></p> <p style="margin-left: 20px;">Protocol: <input type="text" value="UDP"/></p> <p style="margin-left: 20px; color: red;">point 2 address</p> <p style="margin-left: 20px;">Server Address: <input type="text" value="59.1.1.1"/></p> <p style="margin-left: 20px;">Server Port: <input type="text" value="1194"/></p> <p style="margin-left: 20px;">Interface Type: <input type="text" value="TUN"/></p> <p style="margin-left: 20px;">Authentication Type: <input type="text" value="None"/></p> <p style="margin-left: 20px; color: red;">point 1 tunnel IP</p> <p style="margin-left: 20px;">Local IP: <input type="text" value="10.8.0.1"/></p> <p style="margin-left: 20px; color: red;">point 2 tunnel IP</p> <p style="margin-left: 20px;">Remote IP: <input type="text" value="10.8.0.2"/></p> <p style="margin-left: 20px;">Keepalive Interval: <input type="text" value="20"/></p> <p style="margin-left: 20px;">Keepalive Timeout: <input type="text" value="120"/></p> <p style="margin-left: 20px;">Enable Compression: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p style="margin-left: 20px;">Enable NAT: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <div style="background-color: #2c5e8c; color: white; padding: 5px;">^ Advanced Settings</div> <p style="margin-left: 20px;">Expert Options: <input type="text" value="route 192.168.1.0 255"/></p>	<div style="background-color: #2c5e8c; color: white; padding: 5px;">OpenVPN</div> <div style="background-color: #2c5e8c; color: white; padding: 5px;">^ Tunnel Settings</div> <p style="margin-left: 20px;">Index: <input type="text" value="1"/></p> <p style="margin-left: 20px;">Enable: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p style="margin-left: 20px;">Description: <input type="text" value="OpenVPN-Point 2"/></p> <p style="margin-left: 20px;">Mode: <input type="text" value="P2P"/></p> <p style="margin-left: 20px;">Protocol: <input type="text" value="UDP"/></p> <p style="margin-left: 20px; color: red;">point 1 address</p> <p style="margin-left: 20px;">Server Address: <input type="text" value="58.1.1.1"/></p> <p style="margin-left: 20px;">Server Port: <input type="text" value="1194"/></p> <p style="margin-left: 20px;">Interface Type: <input type="text" value="TUN"/></p> <p style="margin-left: 20px;">Authentication Type: <input type="text" value="None"/></p> <p style="margin-left: 20px; color: red;">point 2 tunnel IP</p> <p style="margin-left: 20px;">Local IP: <input type="text" value="10.8.0.2"/></p> <p style="margin-left: 20px; color: red;">point 1 tunnel IP</p> <p style="margin-left: 20px;">Remote IP: <input type="text" value="10.8.0.1"/></p> <p style="margin-left: 20px;">Keepalive Interval: <input type="text" value="20"/></p> <p style="margin-left: 20px;">Keepalive Timeout: <input type="text" value="120"/></p> <p style="margin-left: 20px;">Enable Compression: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p style="margin-left: 20px;">Enable NAT: <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <div style="background-color: #2c5e8c; color: white; padding: 5px;">^ Advanced Settings</div> <p style="margin-left: 20px;">Expert Options: <input type="text" value="route 192.168.2.0 255"/></p>

### 4.2.3 GRE VPN



### VPN--->GRE--->GRE

GRE	Status
^ Tunnel Settings	
Index	Enable
Description	Remote IP Address

Click “+”.

GRE-1:

The screenshot shows the configuration for GRE-1. The fields are: Index (1), Enable (ON), 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 (OFF), Enable NAT (OFF), and Secrets (\*\*\*\*\*). Red boxes highlight the Remote IP Address, Local Virtual IP Address, Remote Virtual IP Address, and Secrets fields.

The modifications will take effect after click “Submit-->Save&Apply”.

GRE-2:

The screenshot shows the configuration for GRE-2. The fields are: Index (1), Enable (ON), 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 (OFF), Enable NAT (OFF), and Secrets (\*\*\*\*\*). Red boxes highlight the Remote IP Address, Local Virtual IP Address, Remote Virtual IP Address, and Secrets fields.

The modifications will take effect after click “Submit-->Save&Apply”.

The comparison between point 1 and point 2 is as following picture:

The comparison shows two side-by-side screenshots of the Tunnel Settings page. The left side is labeled 'GRE-1' and the right side is labeled 'GRE-2'. Red boxes and text annotations highlight the differences: GRE-1 Remote IP Address (59.1.1.1) is labeled 'GRE-1 public IP'; GRE-1 Local Virtual IP Address (10.8.0.1) is labeled 'GRE-1 tunnel IP'; GRE-1 Remote Virtual IP Address (10.8.0.2) is labeled 'GRE-2 tunnel IP'; GRE-2 Remote IP Address (58.1.1.1) is labeled 'GRE-2 public IP'; GRE-2 Local Virtual IP Address (10.8.0.2) is labeled 'GRE-2 tunnel IP'; GRE-2 Remote Virtual IP Address (10.8.0.1) is labeled 'GRE-1 tunnel IP'; and the Secrets field is annotated with 'set the same secret as GRE-2' on both sides.

## Chapter 5 Introductions for CLI

### 5.1 What's CLI

The R2000 command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the [SSH](#) or through a [telnet](#) network connection.

#### Route login:

Router login: admin

Password: admin

#

#### CLI commands:

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

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

## 5.2 How to Configure the CLI

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

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

### 5.2.1 QuickStart with Configuration Examples

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

#### Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "1.2.0 (Rev 399)"
kernel_version = 3.10.49
device_model = R2000
serial_number = 15090140040008
uptime = "0 days, 00:04:07"
system_time = "Tue Dec 22 15:02:36 2015"
```

#### Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware    New firmware
# tftpupdate firmware (space+?)
  String    Firmware name
# tftpupdate firmware r2000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
```



Downloading

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

Flashing

Checking 100%

Decrypting 100%

Flashing 100%

Verifying 100%

Verify Success

upgrade success //update success

# config save\_and\_apply

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

### Example 3: Set link-manager

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

```

# set link_manager primary_link (space+?)
Enum Primary Link (wwan1/wwan2/wan/WiFi)
# set link_manager primary_link wwan1 //select "wwan1" as primary_link
OK //setting succeed

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

```

#### Example 4: Set LAN IP address

```

# show lan all
network {
    id = 1

```

```
interface = lan0
ip = 192.168.0.1
netmask = 255.255.255.0
mtu = 1500
dhcp {
    enable = true
    mode = server
    relay_server = ""
    pool_start = 192.168.0.2
    pool_end = 192.168.0.100
    netmask = 255.255.255.0
    gateway = ""
    primary_dns = ""
    secondary_dns = ""
    wins_server = ""
    lease_time = 120
    expert_options = ""
    debug_enable = false
}
}
multi_ip {
    id = 1
    interface = lan0
    ip = 172.16.99.11
    netmask = 255.255.0.0
}
#
# set lan
network    Network Settings
multi_ip   Multiple IP Address Settings
vlan       VLAN
# set lan network 1(space+?)
interface  Interface
ip         IP Address
netmask    Netmask
mtu        MTU
dhcp       DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.22           //set IP address for lan
OK                                           //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
```

```
...
# config save_and_apply
OK // save and apply current configuration, make you configuration effect
```

### Example 5: CLI for setting Cellular

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

```

band_gsm_850 = false
band_gsm_900 = false
band_gsm_1800 = false
band_gsm_1900 = false
band_wcdma_850 = false
band_wcdma_900 = false
band_wcdma_1900 = false
band_wcdma_2100 = false
band_lte_800 = false
band_lte_850 = false
band_lte_900 = false
band_lte_1800 = false
band_lte_1900 = false
band_lte_2100 = false
band_lte_2600 = false
band_lte_1700 = false
band_lte_700 = false
band_tdd_lte_2600 = false
band_tdd_lte_1900 = false
band_tdd_lte_2300 = false
band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet  cellular      ddns          dhcp          dns
event          firewall    ipsec        lan           link_manager
ntp            openvpn    reboot       route         serial_port
sms           snmp       syslog       system        user_management
vrrp

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

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

```

```

band_wcdma_900      WCDMA 900
band_wcdma_1900     WCDMA 1900
band_wcdma_2100     WCDMA 2100
band_lte_800        LTE 800 (band 20)
band_lte_850        LTE 850 (band 5)
band_lte_900        LTE 900 (band 8)
band_lte_1800       LTE 1800 (band 3)
band_lte_1900       LTE 1900 (band 2)
band_lte_2100       LTE 2100 (band 1)
band_lte_2600       LTE 2600 (band 7)
band_lte_1700       LTE 1700 (band 4)
band_lte_700        LTE 700 (band 17)
band_tdd_lte_2600   TDD LTE 2600 (band 38)
band_tdd_lte_1900   TDD LTE 1900 (band 39)
band_tdd_lte_2300   TDD LTE 2300 (band 40)
band_tdd_lte_2500   TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
...
# config save_and_apply
OK                                     // save and apply current configuration, make you configuration effect
    
```

### 5.3 Commands Reference

commands	syntax	description
Debug	<i>Debug parameters</i>	Turn on or turn off debug function
Show	<i>Show parameters</i>	Show current configuration of each function , if we need to see all please using “show running ”
Set	<i>Set 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	<i>Add parameters</i>	

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

# Glossary

Abbreviations	Description
AC	Alternating Current
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
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identification
IP	Internet Protocol
IPSec	Internet Protocol Security

Abbreviations	Description
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System



<b>Abbreviations</b>	<b>Description</b>
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
WAN	Wide Area Network