



User Guide

R3000 LG

Industrial LoRaWAN Gateway

Low Power Consumption & Long Range Communication



robustOS

Guangzhou Robustel LTD
www.robustel.com

About This Document

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

Copyright©2019 Guangzhou Robustel LTD

All rights reserved.

Trademarks and Permissions

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

Disclaimer

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

Technical Support

Tel: +86-20-29019902

Fax: +86-20-82321505

Email: support@robustel.com

Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the gateway is used in a normal manner with a well-constructed network, the gateway 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 gateway, or for failure of the gateway to transmit or receive such data.

Safety Precautions

General

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

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

Using the Gateway in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the gateway.
- The driver or operator of any vehicle should not operate the gateway while driving.
- Install the gateway by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the gateway.
- The gateway 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 gateway is powered by the vehicle's main battery. The battery may be drained after extended period.

Protecting Your Gateway

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

- Do not expose the gateway 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 gateway. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the gateway. Do not use the gateway under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the gateway only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

FCC Caution:

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter

Regulatory and Type Approval Information

Table 1: Directives

2011/65/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 Table 3 for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.</p>

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.

Document History

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

Date	Firmware Version	Document Version	Change Description
16 Oct., 2017	1.0.0	v.1.0.0	Initial release
20 Dec., 2017	1.0.0	v.1.0.1	Updated model and certification info Added the image for GPS antenna
10 Apr., 2018	1.0.0	v.1.0.2	Added new LoRa standard 433-434 MHz (Europe) Updated LoRa interface information
28 Jun., 2018	1.0.0	v.1.0.3	Revised the company name
19 Jul., 2018	1.0.0	v.1.0.4	Revised the product name
29 Jan., 2019	1.0.0	v.1.0.5	Revised the certifications
27 Feb., 2019	1.0.0	v.1.0.6	<ul style="list-style-type: none"> • Revised the Max transmitted power of Lora interface • Revised the description of Max sensitivity • Revised the English Grammar
14 Mar., 2019	1.0.0	v.1.0.7	Added the FCC Statement

Contents

Chapter 1	Product Overview	10
1.1	Key Features	10
1.2	Package Contents	11
1.3	Specifications	13
1.4	Dimensions.....	15
1.5	Ordering Information	16
Chapter 2	Hardware Installation.....	17
2.1	PIN Assignment	17
2.2	LED Indicators.....	18
2.3	USB Interface.....	19
2.4	Reset Button.....	20
2.5	Ethernet Port.....	21
2.6	Insert or Remove SIM Card/Micro SD Card	22
2.7	Attach External Antenna (SMA Type).....	23
2.8	Mount the Gateway	24
2.9	Ground the Gateway	25
2.10	Power Supply.....	26
Chapter 3	Initial Configuration	27
3.1	Configure the PC.....	27
3.2	Factory Default Settings	30
3.3	Log in the Gateway	30
3.4	Control Panel.....	31
3.5	Status.....	32
3.6	Interface > Link Manager	34
3.7	Interface > LAN.....	42
3.8	Interface > Ethernet	47
3.9	Interface > Cellular	48
3.10	Interface > USB.....	52
3.11	Interface > DI	53
3.12	Interface > Serial Port.....	55
3.13	Interface > LoRa.....	60
3.14	Network > Route	64
3.15	Network > Firewall	66
3.16	Network > IP Passthrough.....	71
3.17	VPN > IPsec.....	71
3.18	VPN > OpenVPN	78
3.19	VPN > GRE	86
3.20	Services > Syslog.....	87
3.21	Services > Event.....	88
3.22	Services > NTP	91
3.23	Services > SMS.....	92
3.24	Services > Email.....	93
3.25	Services > DDNS	94
3.26	Services > SSH.....	95

3.27	Services > GPS	96
3.28	Services > Web Server	99
3.29	Services > Advanced	100
3.30	System > Debug	102
3.31	System > Update	103
3.32	System > App Center	103
3.33	System > Tools	104
3.34	System > Profile	106
3.35	System > User Management	107
Chapter 4	Configuration Examples.....	109
4.1	Interface	109
4.1.1	Console Port	109
4.1.2	Digital Input	110
4.1.3	RS-232	110
4.2	Cellular	111
4.2.1	Cellular Dial-Up.....	111
4.2.2	SMS Remote Control.....	113
4.3	Network.....	115
4.3.1	IPsec VPN	115
4.3.2	OpenVPN	119
4.3.3	GRE VPN	121
Chapter 5	Introductions for CLI.....	123
5.1	What Is CLI.....	123
5.2	How to Configure the CLI	124
5.3	Commands Reference	130
Glossary.....		131

Chapter 1 Product Overview

1.1 Key Features

Robustel R3000 LG is an industrial-grade LoRaWAN gateway, integrated with LoRaWAN wireless communication technology and cellular network technology, to provide users with wireless long-distance data transmission services. R3000 LG allows access to various types of LoRa application nodes, and supports wired Ethernet and wireless 4G/3G access to the cloud platform, mainly for LoRaWAN data transmission between LoRa node and cloud platform.

LPWAN technology is a type of RF Technology designed for low cost and mostly battery operated end devices and sensors. LoRaWAN is a MAC level protocol that uses LoRa Radio Technology as its physical layer. One can create both public and private networks with LoRaWAN. The LoRa Alliance has created a fully open LoRaWAN standard allowing the creation of star based LPWAN networks where end devices and sensors communicate with gateways connected to a cloud based (or on premise) LoRaWAN Network server. All communications are fully 128-bit AES encrypted, bidirectional and end devices can register onto the network over the air.

- Supports global LoRaWAN frequency bands
- Compatible with LoRaWAN and private protocols
- Compatible with any LoRaWAN cloud server
- Up to 8 channels supports receive data simultaneously
- Supports Packet Forwarder Version 2.2.1 and Packet Forwarder Protocol Version 1
- RobustOS + SDK
- TPH6700 Housing optional
- Backhaul option supports 3G, 4G and Ethernet
- Supports dual SIM
- Robust industrial design (9 to 60V DC, -40 to +75 °C)

1.2 Package Contents

Before installing your R3000 LG, verify the kit contents as following.

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

- 1 x Robustel R3000 LG Industrial LoRaWAN Gateway



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



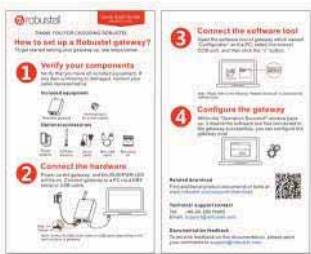
- 1 x 7-pin 3.5 mm male terminal block with lock for serial and console port



- 1 x 4-pin 3.5 mm male terminal block for digital input interface



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



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

Optional Accessories (sold separately)



- RP-SMA LoRa stubby antenna



- GPS antenna



- Wall mounting kit



- 35 mm DIN rail mounting kit



- Ethernet cable



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



1.3 Specifications

LoRa Interface

- Number of antennas: 1
- Connector: SMA female with 50 ohms impedance
- Standards: 902-928 MHz (North America)
- Max transmitted power: +13 dBm
- Max sensitivity: -142 dBm
- Reception capacity: Supports 8 channels, and each channel can receive data simultaneously
Supports 0.5 MHz bandwidth demodulation
- Communication range: 5 km

Cellular Interface

- Number of antennas: 2 (MAIN + AUX)
- Connector: SMA female
- SIM: 2 (3.0 V & 1.8 V)
- Standards: WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/FDD LTE
WCDMA: max DL/UL = 2.8 Mbps/384 Kbps
HSPA+: max DL/UL = 21/5.76 Mbps
DC-HSPA+: max DL/UL = 42/5.76 Mbps
FDD LTE: max DL/UL = 100/50 Mbps, fallback to 3G

Ethernet Interface

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

GPS/GLONASS Interface (Optional)

- Number of antennas: 1
- Connector: SMA female with 50 ohms impedance
- Acquisition sensitivity: GPS: greater than -148 dBm
GLONASS: greater than -145 dBm
- Navigation sensitivity: GPS: greater than -163 dBm
GLONASS: greater than -157 dBm
- Tracking sensitivity: GPS: greater than -165 dBm
GLONASS: greater than -161 dBm
- Horizontal position accuracy: GPS: 2.5 m
GLONASS: 2.6 m
- Protocol: NMEA-0183 v4.10

Serial Interface

- Number of ports: 1 x RS-232
- Connector: 7-pin 3.5 mm female socket with lock
- ESD protection: ±15 KV
- Baud rate: 300 bps to 230400 bps
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- RS-232: TxD, RxD, RTS, CTS, GND

Digital Input

- Number of ports: 2 x DI (dry contact)
- Connector: 4-pin 3.5 mm female socket
- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: "V+" +5V DC (DI)
- Absolute maximum ADC: 300 mA

Others

- 1 x RST button
- 1 x Micro SD interface
- 1 x USB 2.0 host up to 480 Mbps
- 1 x CLI interface
- LED indicators - 1 x RUN, 1 x MODEM, 1 x USR, 1 x RSSI, 1 x NET, 1 x SIM
- Built-in RTC, Watchdog, Timer

Software (Basic features of RobustOS)

- LoRaWAN protocols: V1.0 Class A/Class C and V1.0.2 Class A/Class C
- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, HTTPS, DNS, ARP, BGP, RIP, OSPF, NTP, SMTP, Telnet, VLAN, SSH2, DDNS, etc.
- VPN tunnel: IPsec, OpenVPN, GRE
- Firewall: DMZ, anti-DoS, Filtering (IP/Domain name/MAC address), Port Mapping, Access Control
- Management: Web, CLI, SMS
- Serial port: Transparent, TCP Client/Server, UDP, Modbus RTU Gateway

App Center (Available Apps for RobustOS)

- Apps*: L2TP, PPTP, DMVPN, RobustVPN, VRRP, QoS, SNMP, Language, RobustLink

*Request on demand. For more Apps please visit www.robustel.com.

Power Supply and Consumption

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

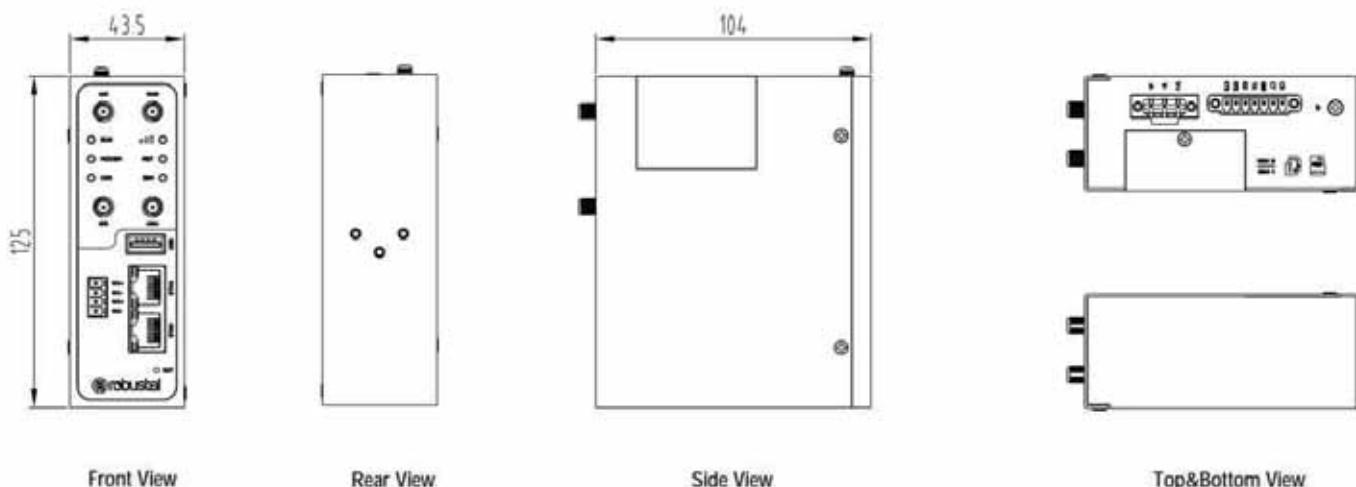
Physical Characteristics

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

Approvals

- Regulatory: CE (433MHz), CE (868MHz), RCM (915MHz)
- Environmental: RoHS, WEEE
- EMI: EN 55032: 2012/AC: 2013 (CE&RE) Class B
- EMS : IEC 61000-4-2 (ESD) Contact Level 2; Air Level 3
IEC 61000-4-3 (RS) Level 2
IEC 61000-4-4 (EFT) Level 2
IEC 61000-4-5 (Surge) Level 3
IEC 61000-4-6 (CS) Level 2

1.4 Dimensions



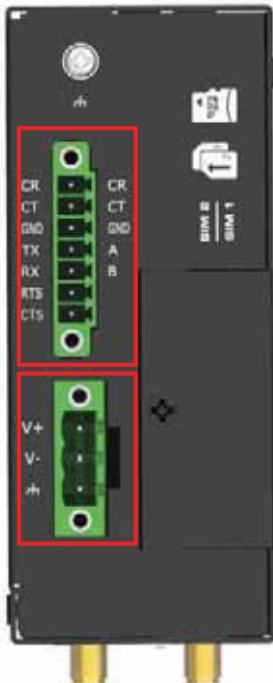
1.5 Ordering Information

Model	R3000-LG4LA
Gateway Type	LTE Gateway
Serial Port Type	RS-232
Air Interface	WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+ /FDD LTE
Frequency Bands	
4G*	B2/B4/B12
3G	B2/B5
Operating Environment	-40 to +75 °C 5 to 95% RH

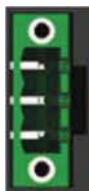
*For more information about 4G frequency bands in different countries, please contact your Robustel sales representative.

Chapter 2 Hardware Installation

2.1 PIN Assignment



PIN	Debug	RS-232	Direction
1	CR	--	Gateway ← Device
2	CT	--	Gateway → Device
3	GND	GND	--
4	--	TXD	Gateway → Device
5	--	RXD	Gateway ← Device
6	--	RTS	Gateway → Device
7	--	CTS	Gateway ← Device



PIN	Polarity
8	Positive
9	Negative
10	GND



PIN	DI	Direction
1	DI1+	Gateway ← Device
2	DI1-	Gateway ← Device
3	DI2+	Gateway ← Device
4	DI2-	Gateway ← Device

2.2 LED Indicators

The R3000 LG has been designed to be placed on a desktop. Below is the front view of the R3000 LG.



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

	Yellow	On, solid	Connection to 3G network is established
	Red	On, solid	Connection to 2G network is established
	/	Off	Connection to network is not established or establishing
SIM	Green	On, blinking	Backup card is being used
		Off	Main card is being used

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

2.3 USB Interface



Function	Operation
Firmware upgrade	USB interface is used for batch firmware upgrading, but cannot be used for sending or receiving data from slave devices which connected to it. You can insert a USB storage device into the gateway's USB interface, such as a U disk or a hard disk. If there have a supported configuration file or a gateway firmware in this USB storage device, the gateway will automatically update the configuration file or the firmware. For more details, see 3.10 Interface > USB .

2.4 Reset Button



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

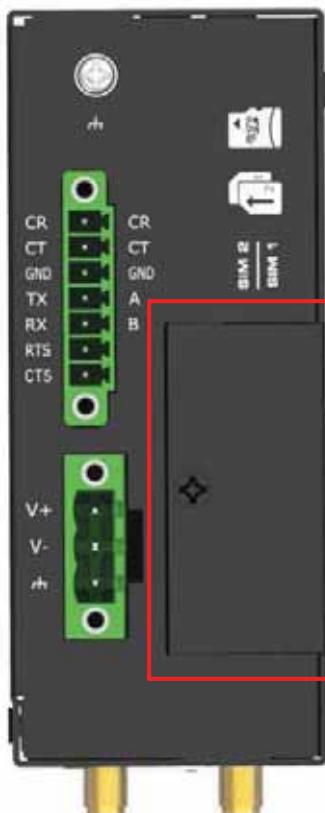
2.5 Ethernet Port



There are two Ethernet ports on R3000 LG, including ETH0 and ETH1. Each Ethernet port has two LED indicators. The yellow one is a link indicator, while the green one is a speed indicator. For details about status, see the table below.

Indicator	Status	Description
Link indicator	On, solid	Connection is established
	On, blinking	Data is being transferred
	Off	Connection is not established
Speed indicator	On, solid	100 Mbps mode
	Off	10 Mbps mode

2.6 Insert or Remove SIM Card/Micro SD Card



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

- **Insert SIM card/Micro SD card**

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

- **Remove SIM card/Micro SD card**

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

Note:

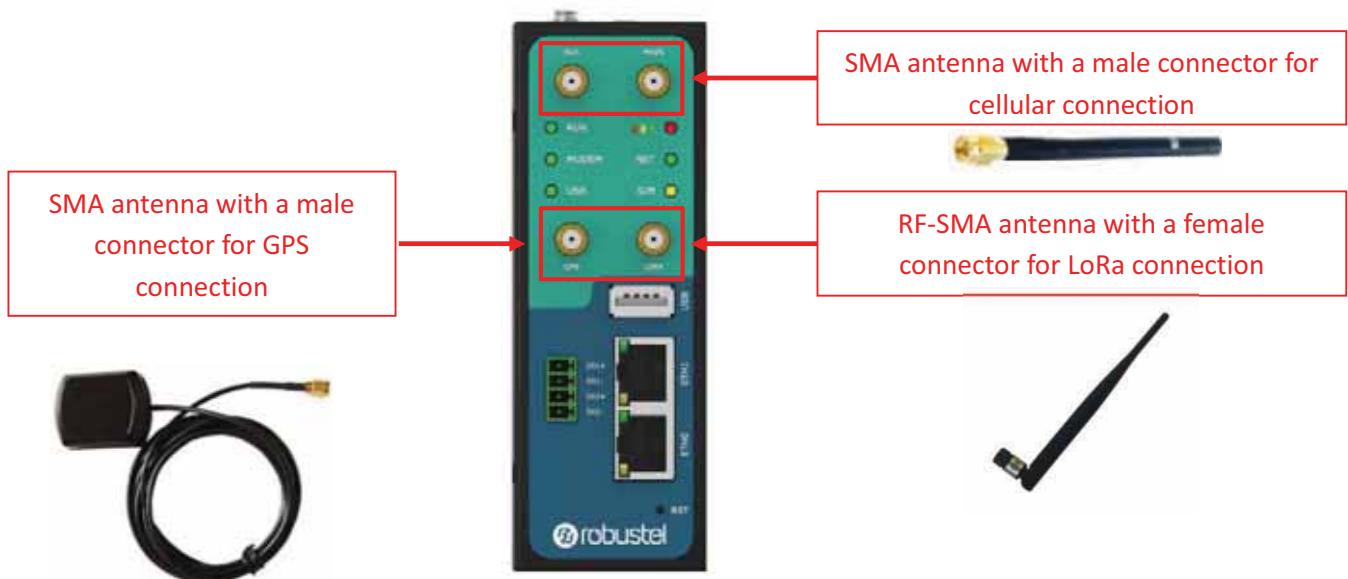
1. Recommended torque for inserting is 1.0 N.m, and the maximum allowed is 1.2 N.m.
2. Use the specific card when the device is working in extreme temperature (temperature exceeding 40 °C), because the regular card for long-time working in harsh environment will be disconnected frequently.
3. Do not forget to twist the cover tightly to avoid being stolen.

4. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
5. Do not bend or scratch the card.
6. Keep the card away from electricity and magnetism.
7. Make sure gateway is powered off before inserting or removing the card.

2.7 Attach External Antenna (SMA Type)

Attach an external SMA antenna to the gateway's antenna connector and twist tightly. Make sure the antenna is within the correct frequency range provided by the ISP and with 50 Ohm impedance.

Note: Recommended torque for tightening is 0.35 N.m.

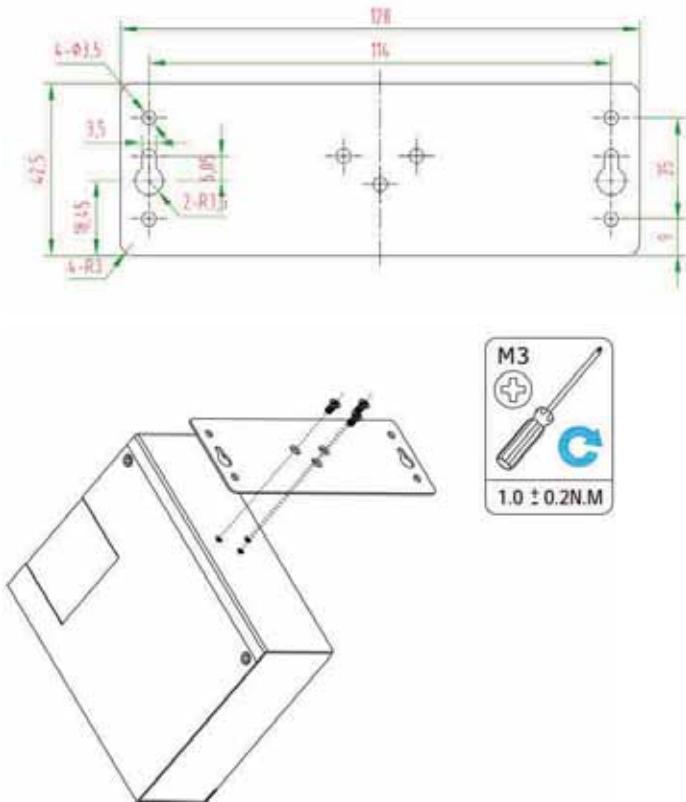


2.8 Mount the Gateway

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

Two methods for mounting the gateway

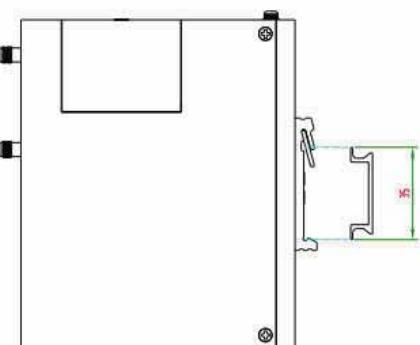
- Wall mounting (measured in mm)

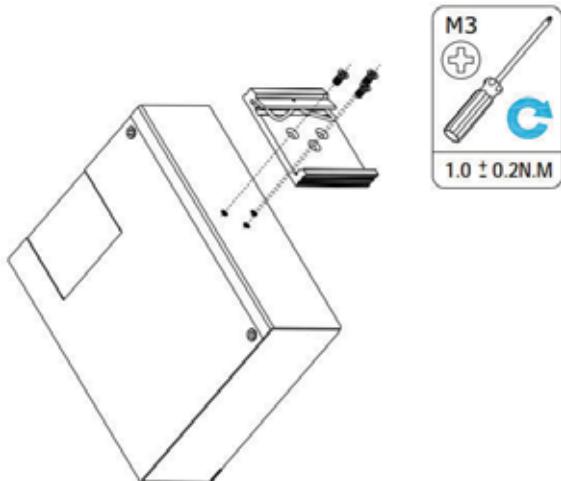


Use 3 pcs of M3*4 flat head Phillips screws to fix the wall mounting kit to the gateway, and then use 2 pcs of M3 drywall screws to mount the gateway associated with the wall mounting kit on the wall.

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

- DIN rail mounting (measured in mm)

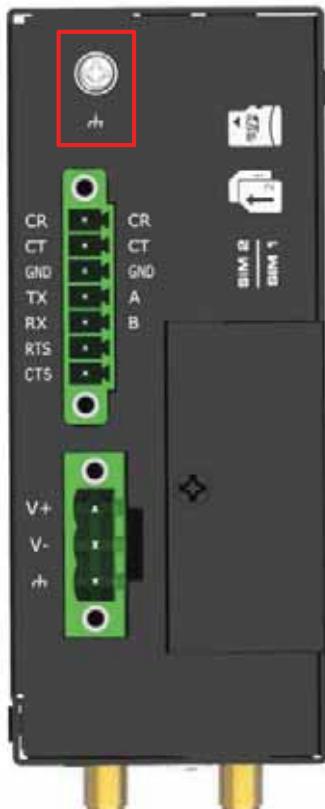




Use 3 pcs of M3*6 flat head Phillips screws to fix the DIN rail to the gateway, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

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

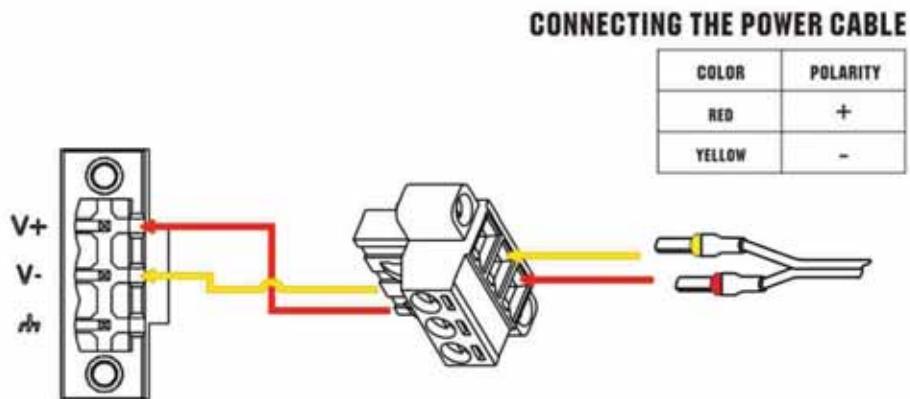
2.9 Ground the Gateway



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

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

2.10 Power Supply



R3000 LG supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Note: The range of power voltage is 9 to 60V DC.

Chapter 3 Initial Configuration

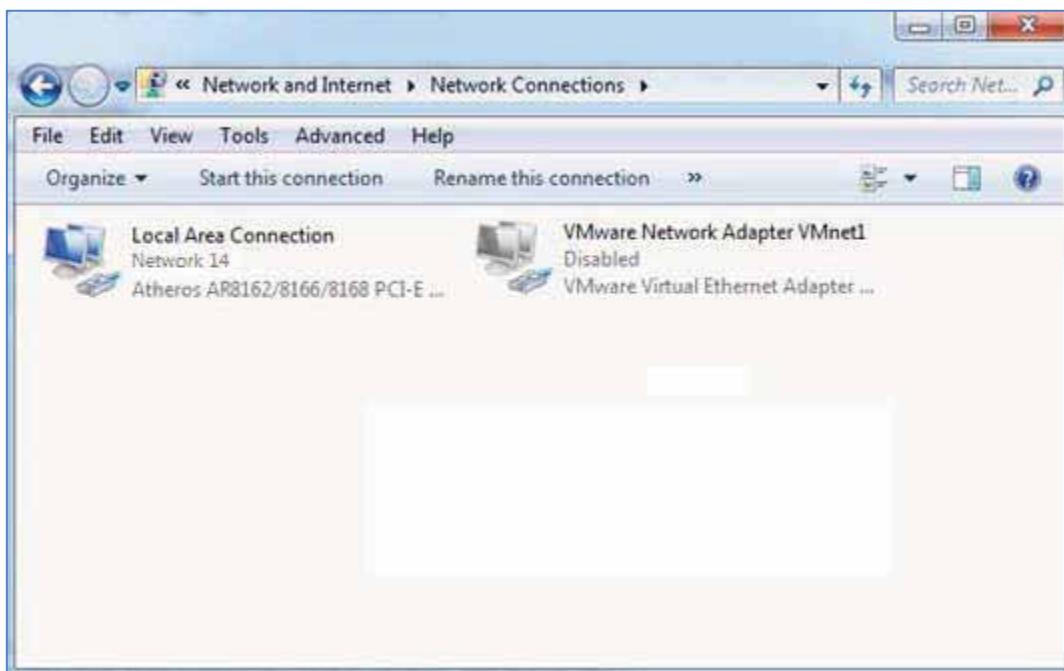
The gateway can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the gateway, 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 gateway. 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 gateway. If you encounter any problems accessing the gateway 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 gateway.

3.1 Configure the PC

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

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

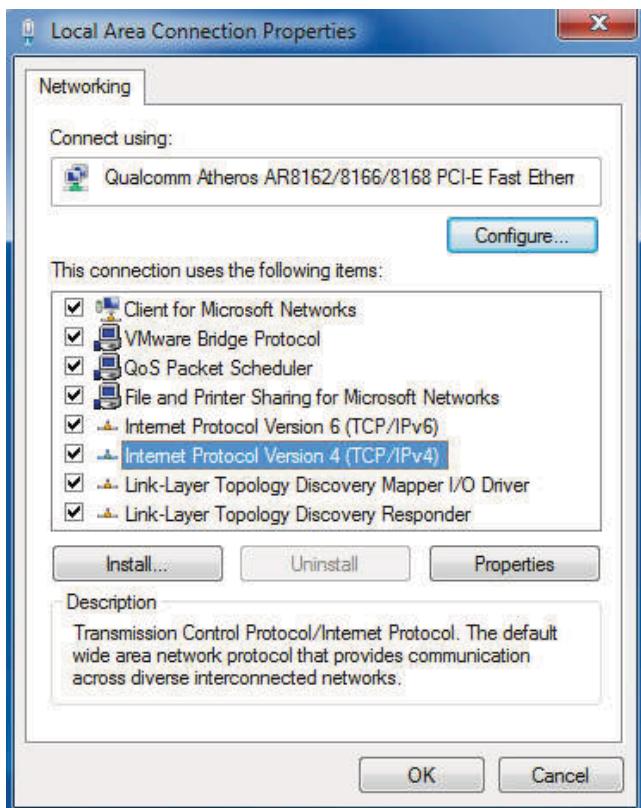
1. Click Start > Control panel, double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.



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

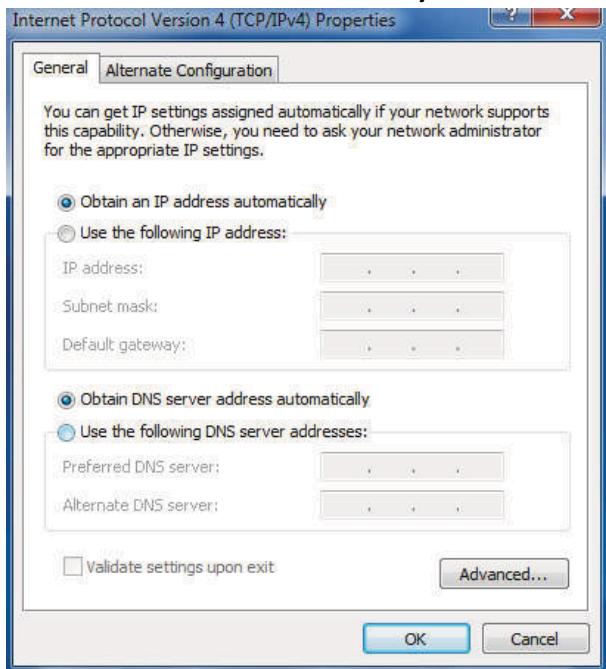


3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



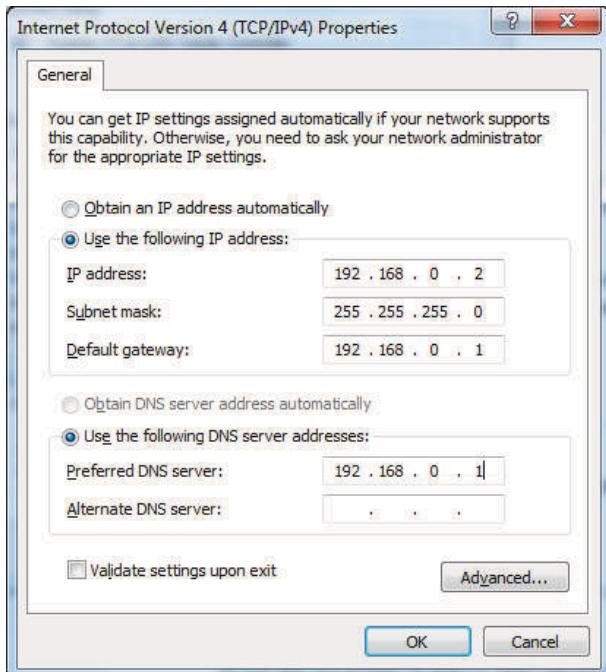
4. Two ways for configuring the IP address of PC.

Obtain an IP address automatically:



Use the following IP address:

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



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

3.2 Factory Default Settings

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

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

3.3 Log in the Gateway

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

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

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

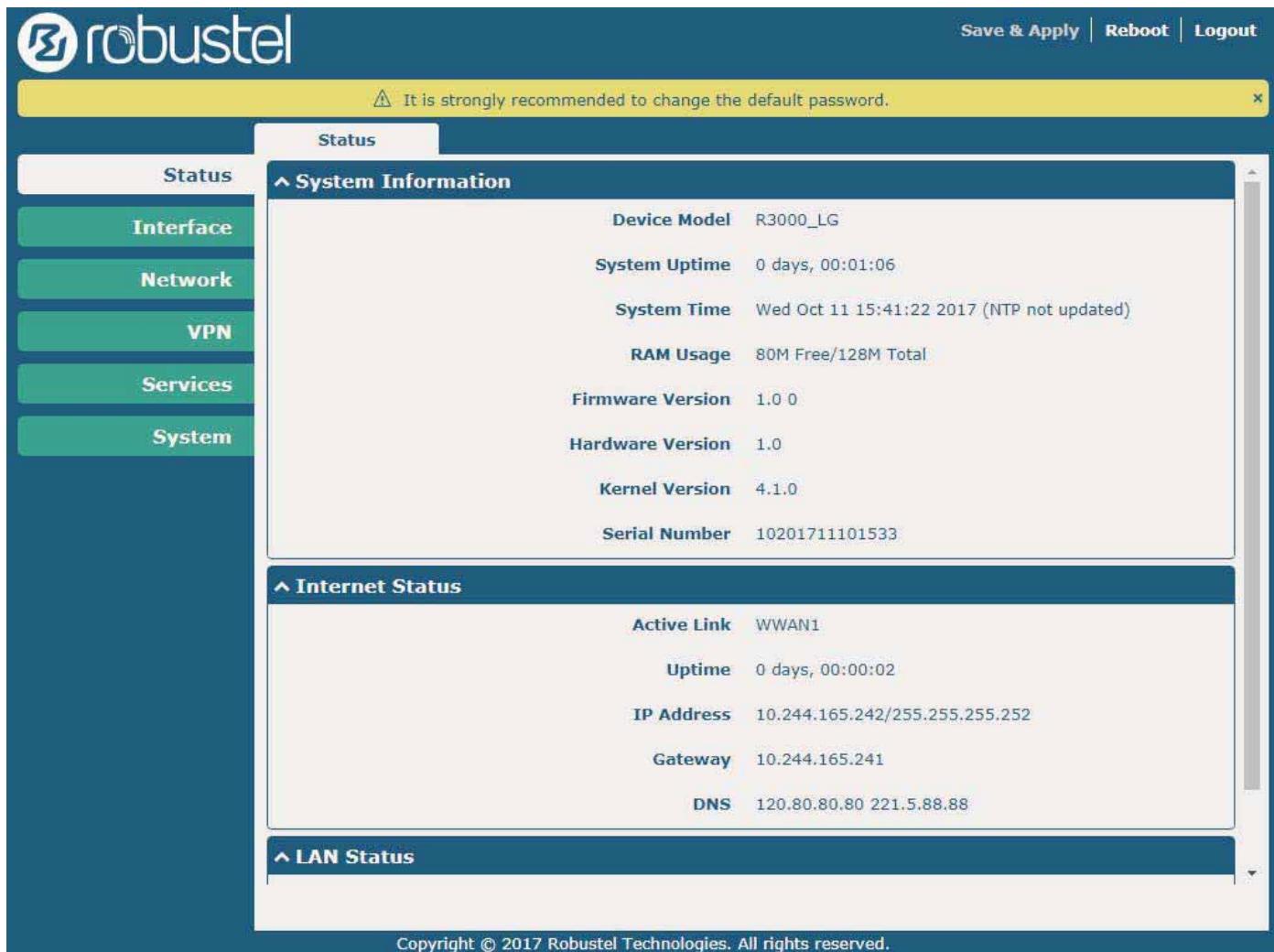


3. In the login page, enter the username and password, choose language and then click **LOGIN**. The default username and password are “admin”.

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

3.4 Control Panel

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



System Information

- Device Model: R3000_LG
- System Uptime: 0 days, 00:01:06
- System Time: Wed Oct 11 15:41:22 2017 (NTP not updated)
- RAM Usage: 80M Free/128M Total
- Firmware Version: 1.0.0
- Hardware Version: 1.0
- Kernel Version: 4.1.0
- Serial Number: 10201711101533

Internet Status

- Active Link: WWAN1
- Uptime: 0 days, 00:00:02
- IP Address: 10.244.165.242/255.255.255.252
- Gateway: 10.244.165.241
- DNS: 120.80.80.80 221.5.88.88

LAN Status

Copyright © 2017 Robustel Technologies. All rights reserved.

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

⚠ It is strongly recommended to change the default password.

It is strongly recommended for security purposes that you change the default username and/or password. To change your username and/or password, see **3.35 System > User Management**.

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

	login web on this browser without a password before timeout.	
Submit	Click to save the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

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

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

3.5 Status

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

System Information

System Information	
Device Model	R3000_LG
System Uptime	0 days, 00:01:06
System Time	Wed Oct 11 15:41:22 2017 (NTP not updated)
RAM Usage	80M Free/128M Total
Firmware Version	1.0.0
Hardware Version	1.0
Kernel Version	4.1.0
Serial Number	10201711101533

System Information	
Item	Description
Device Model	Show the model name of your device.
System Uptime	Show the current amount of time the gateway has been connected.
System Time	Show the current system time.
RAM Usage	Show the free memory and the total memory.

Firmware Version	Show the firmware version running on the gateway.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.

Internet Status

Internet Status	
Active Link	WWAN1
Uptime	0 days, 00:00:02
IP Address	10.244.165.242/255.255.255.252
Gateway	10.244.165.241
DNS	120.80.80.80 221.5.88.88

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

LAN Status

LAN Status	
IP Address	192.168.0.109/255.255.255.0
MAC Address	34:FA:40:0A:BE:E8

LAN Status	
Item	Description
IP Address	Show the IP address and the Netmask of the gateway.
MAC Address	Show the MAC address of the gateway.

3.6 Interface > Link Manager

This section allows you to setup the link connection.



Link Manager **Status**

General Settings

Primary Link	WWAN1	?
Backup Link	WWAN2	?
Backup Mode	Cold Backup	?
Revert Interval	0	?
Emergency Reboot	OFF	?

General Settings @ Link Manager		
Item	Description	Default
Primary Link	Select from "WWAN1", "WWAN2" or "WAN". <ul style="list-style-type: none"> WWAN1: Select to make SIM1 as the primary wireless link WWAN2: Select to make SIM2 as the primary wireless link WAN: Select to make WAN as the primary wired link Note: WAN link is available only if enable eth0 as WAN port in Interface > Ethernet > Ports > Port Settings. 	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", "WAN" or "None". <ul style="list-style-type: none"> WWAN1: Select to make SIM1 as backup wireless link WWAN2: Select to make SIM2 as backup wireless link WAN: Select to make WAN as the primary wired link Note: WAN link is available only if enable eth0 as WAN port in Interface > Ethernet > Ports > Port Settings. None: Do not select any backup link 	WWAN2
Backup Mode	Select from "Cold Backup", "Warm Backup" or "Load Balancing". <ul style="list-style-type: none"> Cold Backup: The inactive link is offline on standby Warm Backup: The inactive link is online on standby Load Balancing: Use two links simultaneously Note: R3000 LG do not support warm backup and load balancing in the situation of two WWAN links. 	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. Note: Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

Note: Click  for help.

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

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

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

WWAN1/WWAN2

Link Manager

General Settings

Index	1
Type	WWAN1
Description	

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

WWAN Settings

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

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

WWAN Settings

Automatic APN Selection	OFF
APN	internet
Username	
Password	
Dialup Number	*99***1#
Authentication Type	Auto
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

▲ Ping Detection Settings

Enable	<input checked="" type="button"/> ON <input type="button"/>
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300 <input type="button"/>
Retry Interval	5 <input type="button"/>
Timeout	3 <input type="button"/>
Max Ping Tries	3 <input type="button"/>

▲ Advanced Settings

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

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

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

WAN

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



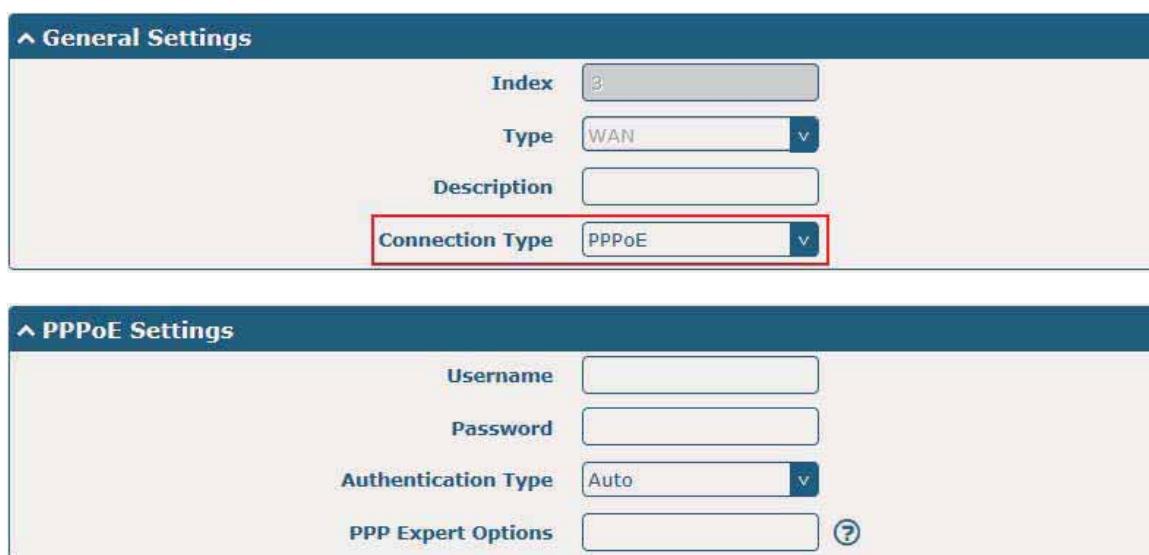
The screenshot shows the "Link Manager" interface with the "General Settings" tab selected. The "Type" field is set to "WAN". The "Connection Type" dropdown is set to "DHCP" and is highlighted with a red border.

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



The screenshot shows the "Link Manager" interface with the "General Settings" tab selected. The "Type" field is set to "WAN". The "Connection Type" dropdown is set to "Static" and is highlighted with a red border. Below it, the "Static Address Settings" section is visible, containing fields for IP Address, Gateway, Primary DNS, and Secondary DNS.

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



The screenshot shows the "Link Manager" interface with the "General Settings" tab selected. The "Type" field is set to "WAN". The "Connection Type" dropdown is set to "PPPoE" and is highlighted with a red border. Below it, the "PPPoE Settings" section is visible, containing fields for Username, Password, Authentication Type (set to Auto), and PPP Expert Options.

▲ Ping Detection Settings

Enable	<input checked="" type="button"/> ON 
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300 
Retry Interval	5 
Timeout	3 
Max Ping Tries	3 

▲ Advanced Settings

NAT Enable	<input checked="" type="button"/> ON 
MTU	1500
Upload Bandwidth	10000 
Download Bandwidth	10000
Overridden Primary DNS	
Overridden Secondary DNS	
Debug Enable	<input checked="" type="button"/> ON 
Verbose Debug Enable	<input type="button"/> OFF 

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

Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current connectivity is active.	114.114.11 4.114
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval. When ping failed, the gateway will ping again every retry interval.	5
Timeout	Set the ping timeout.	3
Max Ping Tries	Set the max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
Advanced Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Override primary DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Override secondary DNS will override the automatically obtained DNS.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

Status

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

Link Manager		Status			
^ Link Status					...
Index	Link	Status	Uptime	IP Address	
1	WWAN1	Connected	0 days, 00:10:46	10.244.165.2...	
2	WWAN2	Disconnected			

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



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

Link Status					...
Index	Link	Status	Uptime	IP Address	
1	WWAN1	Connected	0 days, 00:10:46	10.244.165.2...	Index 1 Link WWAN1 Status Connected Interface wwan Uptime 0 days, 00:10:46 IP Address 10.244.165.242/255.255.255.252 Gateway 10.244.165.241 DNS 120.80.80.80 221.5.88.88 RX Packets 10 TX Packets 24 RX Bytes 1216 TX Bytes 2270
2	WWAN2	Disconnected			

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

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

3.7 Interface > LAN

This section allows you to set the related parameters for LAN port. There are two LAN ports on R3000 LG, including ETH0 and ETH1. The ETH0 and ETH1 can freely choose from lan0 and lan1, but at least one LAN port must be assigned as lan0. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

LAN

By default, there is a LAN port (lan0) in the list. To begin adding a new LAN port (lan1), please configure ETH0 or ETH1 as lan1 first in **Ethernet > Ports > Port Settings**. Otherwise, the operation will be prompted as “List is full”.

LAN	Multiple IP	VLAN Trunk	Status
▲ Network Settings			
Index	Interface	IP Address	Netmask
1	lan0	192.168.0.109	255.255.255.0

Note: Lan0 cannot be deleted.

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

LAN										
▲ General Settings										
<table border="1"> <tr> <td>Index</td> <td>1</td> </tr> <tr> <td>Interface</td> <td>lan0</td> </tr> <tr> <td>IP Address</td> <td>192.168.0.109</td> </tr> <tr> <td>Netmask</td> <td>255.255.255.0</td> </tr> <tr> <td>MTU</td> <td>1500</td> </tr> </table>	Index	1	Interface	lan0	IP Address	192.168.0.109	Netmask	255.255.255.0	MTU	1500
Index	1									
Interface	lan0									
IP Address	192.168.0.109									
Netmask	255.255.255.0									
MTU	1500									

General Settings @ LAN		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Interface	Show the editing port. Lan1 is available only if it was selected by one of ETH0~ETH1 in Ethernet > Ports > Port Settings , and so on.	--
IP Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

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

^ DHCP Settings

Enable	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="ON"/>	<input style="background-color: white; border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none;" type="button" value="OFF"/>
Mode	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="Server"/>	
IP Pool Start	192.168.0.2	
IP Pool End	192.168.0.100	
Subnet Mask	255.255.255.0	

^ DHCP Advanced Settings

Gateway	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
Primary DNS	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
Secondary DNS	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
WINS Server	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
Lease Time	120 (?)
Static lease	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
Expert Options	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>
Debug Enable	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="ON"/> <input style="background-color: white; border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none;" type="button" value="OFF"/>

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

^ DHCP Settings

Enable	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="ON"/>	<input style="background-color: white; border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none;" type="button" value="OFF"/>
Mode	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="Relay"/>	
DHCP Server For Relay	<input style="width: 150px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/>	

^ DHCP Advanced Settings

Debug Enable	<input style="background-color: #0070C0; color: white; border: 1px solid #0070C0; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none; margin-right: 10px;" type="button" value="ON"/> <input style="background-color: white; border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; font-weight: bold; font-size: 10px; text-decoration: none;" type="button" value="OFF"/>
--------------	---

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

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

Multiple IP

LAN Multiple IP VLAN Trunk Status

▲ Multiple IP Settings

Index	Interface	IP Address	Netmask	
1	lan0	172.16.5.20	255.255.0.0	

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

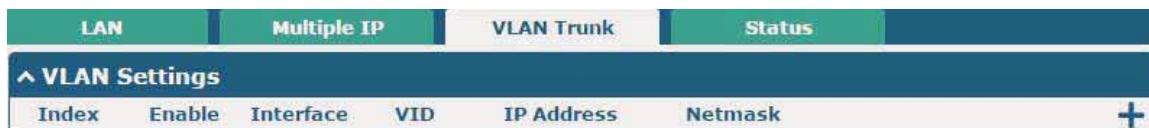
Multiple IP

▲ IP Settings

Index	<input type="text" value="1"/>
Interface	<input type="text" value="lan0"/>
IP Address	<input type="text" value="172.16.5.20"/>
Netmask	<input type="text" value="255.255.0.0"/>

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

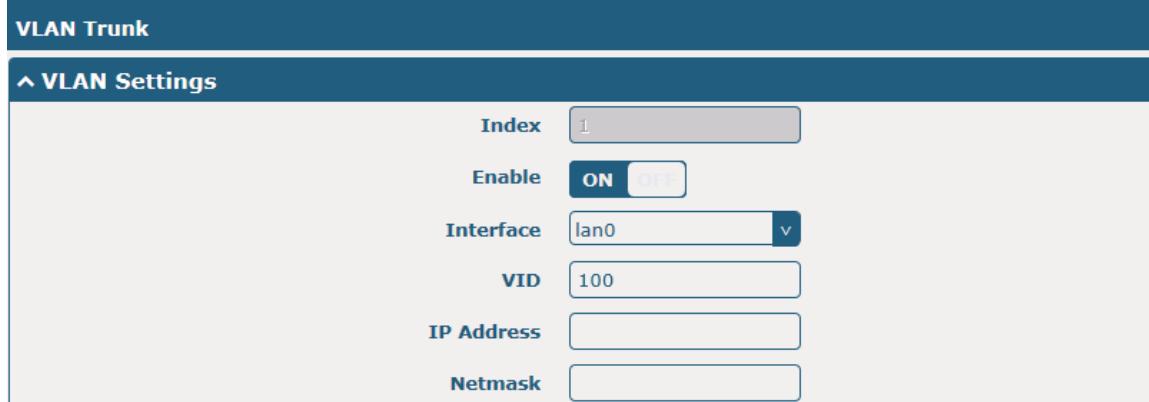
VLAN Trunk



The screenshot shows the VLAN Trunk configuration interface. At the top, there are four tabs: LAN, Multiple IP, VLAN Trunk (which is selected), and Status. Below the tabs, there is a sub-section titled "VLAN Settings" with the following fields:

- Index: A text input field containing "1".
- Enable: A toggle switch set to "ON".
- Interface: A dropdown menu set to "lan0".
- VID: A text input field containing "100".
- IP Address: An empty text input field.
- Netmask: An empty text input field.

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



The screenshot shows the VLAN Trunk configuration interface. At the top, there is a header "VLAN Trunk" and a sub-section titled "VLAN Settings" with the following fields:

- Index: A text input field containing "1".
- Enable: A toggle switch set to "ON".
- Interface: A dropdown menu set to "lan0".
- VID: A text input field containing "100".
- IP Address: An empty text input field.
- Netmask: An empty text input field.

VLAN Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this VLAN. Enable to make gateway can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Choose the interface which wants to enable VLAN trunk function. Select from "lan0" or "lan1" depends on your ETH0 and ETH1's corresponding LAN ports.	lan0
VID	Set the tag ID of VLAN and digits from 1 to 4094.	100
IP Address	Set the IP address of VLAN port.	Null
Netmask	Set the Netmask of VLAN port.	Null

Status

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

LAN	Multiple IP	VLAN Trunk	Status	
▲ Interface Status				
Index	Interface	IP Address	MAC Address	
1 lan0 192.168.0.109/255... 34:FA:40:0A:BE:E8				
▲ Connected Devices				
Index	IP Address	MAC Address	Interface	Inactive Time
1	172.16.1.23	D0:17:C2:8A:DB:F9	lan0	215s
2	192.168.0.10	D0:50:99:4D:F9:35	lan0	0s
3	172.16.5.160	68:F7:28:A1:AC:CF	lan0	12s
4	172.16.0.128	F8:32:E4:73:C3:2A	lan0	141s
5	172.16.5.212	34:97:F6:9E:07:BC	lan0	132s
6	172.16.5.181	1C:1B:0D:D1:97:97	lan0	19s
7	172.16.5.21	78:45:C4:35:13:44	lan0	39s
8	172.16.0.69	F8:32:E4:74:6E:9C	lan0	87s
9	172.16.1.47	48:8A:D2:18:B7:80	lan0	140s
10	172.16.2.5	70:8B:CD:4F:B1:1C	lan0	39s
11	172.16.2.15	D0:50:99:88:BD:28	lan0	101s
12	172.16.2.22	A4:1F:72:58:46:F7	lan0	0s
13	172.16.1.155	40:8D:5C:46:06:19	lan0	21s
14	172.16.0.119	B8:97:5A:95:80:87	lan0	35s
▲ DHCP Lease Table				
Index	IP Address	MAC Address	Interface	Expired Time

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

Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.109/255...	34:FA:40:0A:BE:E8
▲ Interface Status			
Index	1	Interface	lan0
IP Address	192.168.0.109/255.255.255.0	MAC Address	34:FA:40:0A:BE:E8
RX Packets	41776	TX Packets	1076
RX Bytes	5352897	TX Bytes	583289

3.8 Interface > Ethernet

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

Port Settings		
Index	Port	Port Assignment
1	eth0	lan0
2	eth1	lan0

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

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

Port Settings		
Index	Port	Port Assignment
1	eth0	wan
2	eth1	lan0

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

Ports	Status	
Port Settings		
Index	Port	Port Assignment
1	eth0	wan
2	eth1	lan0

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

Ports		
Port Settings		
<input type="text" value="1"/> Index	<input type="text" value="eth0"/> Port	<input type="text" value="lan0"/> Port Assignment
<input type="button" value="?"/>		

^ Port Settings

Index	1
Port	eth0
Port Assignment	wan lan0 lan1 wan
<input type="button" value="Submit"/> <input type="button" value="Close"/>	

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

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

Ports	Status
^ Port Status	
Index	Port
1	eth0
2	eth1
	Link
	Up
	Down

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

^ Port Status		
Index	Port	Link
1	eth0	Up
		Index 1
		Port eth0
		Link Up
2	eth1	Down

3.9 Interface > Cellular

This section allows you to set the related parameters of Cellular. The R3000 LG has two SIM card slots, but do not support two SIM cards online simultaneously due to its single-module design. If insert single SIM card at the first time, SIM1 slot and SIM2 slots are available.

Cellular	Status	AT Debug
^ Advanced Cellular Settings		
Index	SIM Card	Phone Number
1	SIM1	Auto
2	SIM2	Auto
		Network Type
		All
		Band Select Type
		All
		<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/>

Click  of SIM 1 to edit the parameters.

Cellular

General Settings

Index	1
SIM Card	SIM1
Phone Number	
PIN Code	
Extra AT Cmd	
Telnet Port	0

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

Cellular Network Settings

Network Type	Auto
Band Select Type	All

Advanced Settings

Debug Enable	ON
Verbose Debug Enable	OFF

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

Cellular Network Settings

Network Type	Auto
Band Select Type	Specify

Band Settings

GSM 850	 OFF
GSM 900	 OFF
GSM 1800	 OFF
GSM 1900	 OFF
WCDMA 850	 OFF
WCDMA 900	 OFF
WCDMA 1900	 OFF
WCDMA 2100	 OFF
LTE Band 1	 OFF
LTE Band 2	 OFF
LTE Band 3	 OFF
LTE Band 4	 OFF
LTE Band 5	 OFF
LTE Band 7	 OFF
LTE Band 8	 OFF
LTE Band 20	 OFF

Advanced Settings

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

Cellular		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
SIM Card	Show the currently editing SIM card.	SIM1
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Cellular Network Settings		
Network Type	Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", "4G First". <ul style="list-style-type: none">• Auto: Connect to the best signal network automatically• 2G Only: Only the 2G network is connected• 2G First: Connect to the 2G Network preferentially• 3G Only: Only the 3G network is connected• 3G First: Connect to the 3G Network preferentially• 4G Only: Only the 4G network is connected• 4G First: Connect to the 4G Network preferentially	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

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

Cellular	Status	AT Debug		
▲ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	MC7304	460012148626828	Registered to home network

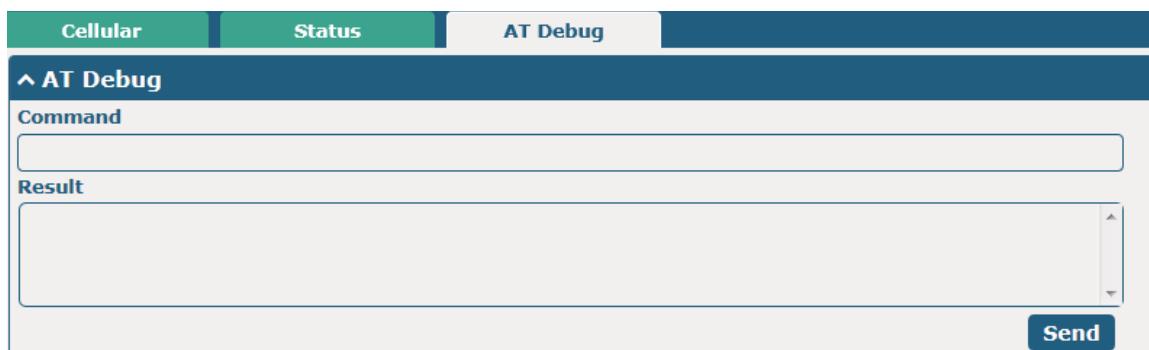
Click the row of status, the details status information will be displayed under the row.

▲ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	MC7304	460012148626828	Registered to home network
Index 1				
Modem Status Ready				
Modem Model MC7304				
Current SIM SIM1				
Phone Number				
IMSI 460012148626828				
ICCID 89860117851023142422				
Registration Registered to home network				
Network Provider				
Network Type LTE				
Signal Strength 24 (-65dBm)				
Bit Error Rate 99				
PLMN ID 46001				
Local Area Code FFFE				
Cell ID 06074702				
IMEI 356853052515535				
Firmware Version SWI9X15C_05.05.58.00 r27038 carmd-fwbuild1 2015/03/0...				

Status	
Item	Description
Index	Indicate the ordinal of the list.
Modem Status	Show the status of the radio module.
Modem Model	Show the model of the radio module.
Current SIM	Show the SIM card that your gateway is using.
Phone Number	Show the phone number of the current SIM. Note: This option will be displayed if enter manually in Cellular > Advanced Cellular Settings > SIM1/SIM2 > General Settings > Phone Number .
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the signal strength detected by the mobile.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.

Status	
Item	Description
Cell ID	Show the current cell ID used for locating the gateway.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

This page allows you to check the AT Debug.



The screenshot shows a user interface for AT Debug. At the top, there are three tabs: 'Cellular' (highlighted in green), 'Status', and 'AT Debug'. Below the tabs, the title '^ AT Debug' is displayed. Underneath the title, there are two text input fields: 'Command' (containing the AT command to be sent) and 'Result' (containing the response from the cellular module). A blue 'Send' button is located at the bottom right of the input area.

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

3.10 Interface > USB

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



The screenshot shows a user interface for General Settings @ USB. At the top, there are three tabs: 'USB' (highlighted in green), 'Key', and 'General Settings'. Below the tabs, the title '^ General Settings' is displayed. Underneath the title, there are two settings: 'Enable USB' (set to ON) and 'Enable Automatic Upgrade' (set to ON). Each setting has a corresponding toggle switch.

General Settings @ USB		
Item	Description	Default
Enable USB	Click the toggle button to enable/disable the USB option.	ON
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the gateway when inserting a USB storage device with a gateway firmware.	ON

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

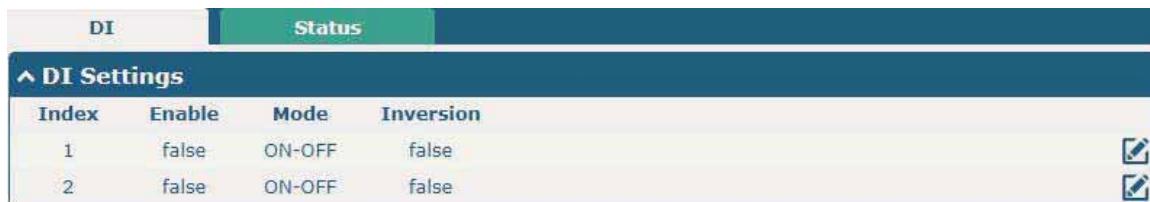


Key		
Item	Description	Default
USB Automatic Update Key	Click Generate to generate a key, and click Download to download the key.	--

3.11 Interface > DI

This section allows you to set the DI parameters. Digital Input interface is a specific interface for R3000 LG, which can be used for triggering alarm.

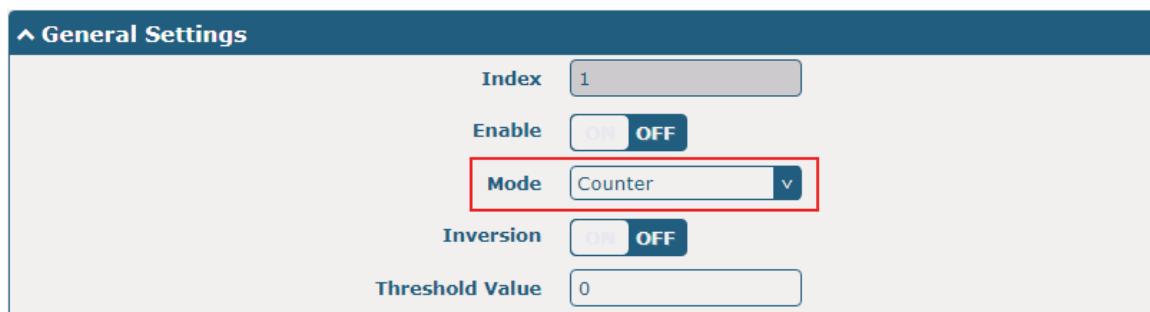
DI



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



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



General Settings @ DI		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DI.	OFF
Mode	<p>Select from “ON-OFF” or “Counter”.</p> <ul style="list-style-type: none"> ON-OFF: DI interface support ON and OFF mode (high or low level electrical) trigger DI alarm. The mode default to ON, and OFF mode is available only when enabling the inversion feature ON—Under this mode, DI alarm status will be triggered to ON when DI interface open from GND or input a high level electrical (logic 1), on the contrary DI alarm status will be triggered to OFF when DI interface connect to GND or input a low level electrical (logic 0) OFF—Under this mode, DI alarm status will be triggered to ON when DI interface connect to GND or input a low level electrical (logic 0), on the contrary DI alarm status will be triggered to OFF when DI interface open from GND or input a high level electrical (logic 1) <ul style="list-style-type: none"> Counter: Event counter mode 	ON-OFF
Inversion	Click the toggle button to enable/disable this option. Enable to set DI mode as OFF mode.	OFF
Threshold Value	<p>Set the threshold value. It will trigger alarm when event counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm again. Enter 0 to 65535 digits. (0=will not trigger alarm)</p> <p>Note: This option is only available when DI under the “Counter” mode.</p>	Null

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

Status

This window allows you to view the status of DO and DI interface. It also can clear the counter alarm of DI in here.

Click **Clear** button to clear DI1 or DI2 monthly usage statistics info for counter alarm.

DI Status

▲ DI Status

Index	Level	Status	Count
1	High	Alarm off	
2	High	Alarm off	

▲ Action Of Clear

Counter Alarm Of DI 1	Clear
Counter Alarm Of DI 2	Clear

3.12 Interface > Serial Port

This section allows you to set the serial port parameters. Serial port provides a way to transfer serial data to IP data, or vice versa, and transmit these data via wired or wireless network to achieve data transparent transmission. R3000 LG supports one RS-232 across a 7-pin 3.5 mm male socket with lock. Click the “Serial Port” column, and click the edit button of COM1.

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

Serial Port

^ Serial Port Application Settings

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

^ Data Packing

Packing Timeout	50	(?)
Packing Length	1200	

^ Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

Serial Port		
Item	Description	Default
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400",	115200

	“57600”, “115200” or “230400”.	
Data Bits	Select from “7” or “8”.	8
Stop Bits	Select from “1” or “2”.	1
Parity	Select from “None”, “Odd” or “Even”.	None
Flow control	Select from “None”, “Software” or “Hardware”.	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. Note: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200

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

Server Setting

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

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

Server Setting

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

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

Server Setting

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

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

Server Setting

Application Mode	Transparent
Protocol	Robustlink

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

Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	TCP Client
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

Server Setting

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

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

Server Setting

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

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

Server Setting

Application Mode	Modbus RTU Gatewa
Protocol	Robustlink

- The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Client” as the protocol.

Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	TCP Client
Server Address	<input type="text"/>
Server Port	<input type="text"/>

The window is displayed as below when choosing “Modbus ASCII Gateway” as the application mode and “TCP Server” as the protocol.

Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	TCP Server
Local IP	<input type="text"/>
Local Port	<input type="text"/>

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

Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	UDP
Local IP	<input type="text"/>
Local Port	<input type="text"/>
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

Server Setting

Application Mode	Modbus ASCII Gatev
Protocol	Robustlink

Server Settings		
Item	Description	Default
Application Mode	Select from “Transparent”, “Modbus RTU Gateway” or “Modbus ASCII Gateway”. <ul style="list-style-type: none"> Transparent: Gateway will transmit the serial data transparently Modbus RTU Gateway: Gateway will translate the Modbus RTU data to Modbus TCP data and sent out, and vice versa Modbus ASCII Gateway: 	Transparent

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

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

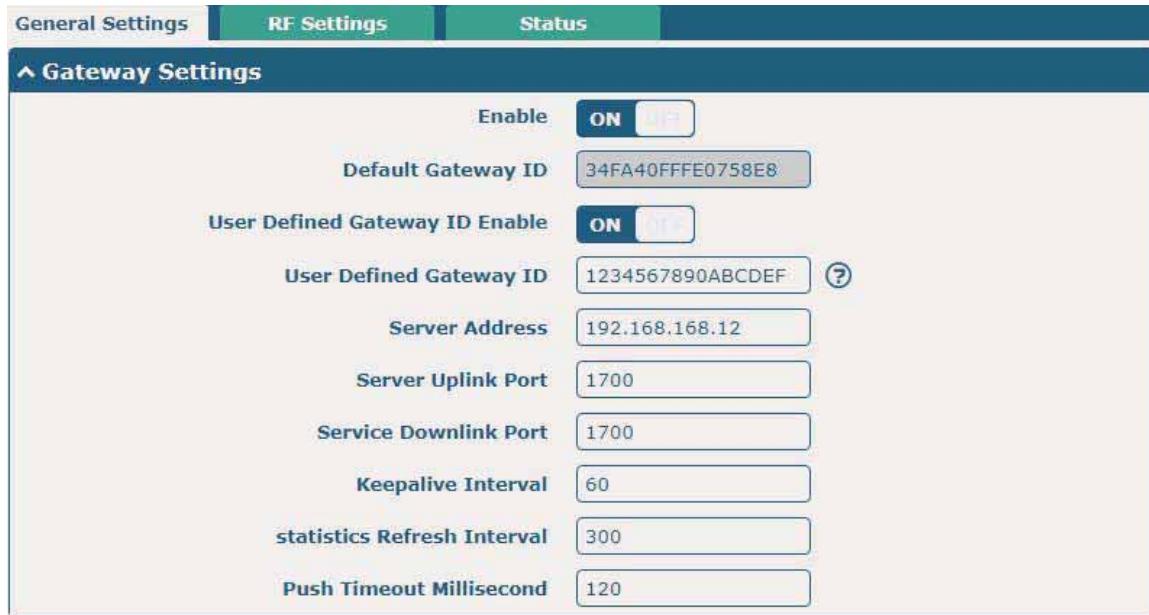
Serial Port	Status			
^ Serial Port Status				
Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	

3.13 Interface > LoRa

This section allows you to set the LoRaWAN parameters.

General Settings

Click “General Settings > Gateway Settings” to configure your node parameters. Here takes an example as below.



Gateway Settings	
Enable	<input checked="" type="checkbox"/>
Default Gateway ID	34FA40FFFE0758E8
User Defined Gateway ID Enable	<input checked="" type="checkbox"/>
User Defined Gateway ID	1234567890ABCDEF
Server Address	192.168.168.12
Server Uplink Port	1700
Service Downlink Port	1700
Keepalive Interval	60
Statistics Refresh Interval	300
Push Timeout Millisecond	120

Gateway Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the LoRaWAN forwarding of the gateway.	OFF
Default Gateway ID	Set the default gateway ID, or you could define the Gateway ID with a unique 64-bit sequence by yourself.	Null
User Defined Gateway ID Enable	Click the toggle button to enable/disable this option.	OFF
User Defined Gateway ID	Enter your defined Gateway ID.	Null
Server Address	Enter the remote IP of the LoRaWAN Server.	Null
Server Uplink Port	Enter the port of the LoRaWAN Server to upload data.	Null
Service Downlink Port	Enter the port of the LoRaWAN Server to send data to your gateway.	Null
Keepalive Interval	Enter the interval of keepalive packet which is sent from gateway to LoRaWAN server to keep the connection stable and alive.	Null
Statistics Refresh Interval	Enter the interval to refresh the statistics status of your gateway.	Null
Push Timeout Millisecond	Enter the timeout to wait for the response from server after the gateway sends data of mode, measured in ms.	Null

RF Settings

General Settings	RF Settings	Status								
▲ RF Power Settings <div style="display: flex; justify-content: space-between;"> RF Power Limit <div style="border: 1px solid #ccc; padding: 2px;">No Limit</div> </div>										
▲ RF Chain Settings <div style="display: flex; justify-content: space-between;"> Supported Frequency <div style="border: 1px solid #ccc; padding: 2px;">863 870</div> </div> <div style="display: flex; justify-content: space-between;"> RF Chain 0 Frequency <div style="border: 1px solid #ccc; padding: 2px;">868500000</div> </div> <div style="display: flex; justify-content: space-between;"> RF Chain 1 Frequency <div style="border: 1px solid #ccc; padding: 2px;">867500000</div> </div>										
▲ LoRa Multi Datarate Channels Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Index</th> <th>RF Chain</th> <th>IF frequency</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>RF Chain 0</td> <td>0</td> <td style="text-align: right; vertical-align: middle;"> + <input checked="" type="checkbox"/>X </td> </tr> </tbody> </table>			Index	RF Chain	IF frequency		1	RF Chain 0	0	+ <input checked="" type="checkbox"/> X
Index	RF Chain	IF frequency								
1	RF Chain 0	0	+ <input checked="" type="checkbox"/> X							

Click + to add a channel. The maximum count is 8.

RF Settings																																				
▲ LoRa Multi Datarate Channels Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Index</th> <th>RF Chain</th> <th>IF frequency</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>RF Chain 0</td> <td>1</td> </tr> <tr> <td></td> <td>RF Chain 0</td> <td>RF Chain 0</td> </tr> <tr> <td></td> <td>IF frequency</td> <td>0</td> </tr> </tbody> </table>	Index	RF Chain	IF frequency	1	RF Chain 0	1		RF Chain 0	RF Chain 0		IF frequency	0																								
Index	RF Chain	IF frequency																																		
1	RF Chain 0	1																																		
	RF Chain 0	RF Chain 0																																		
	IF frequency	0																																		
▲ LoRa Multi Datarate Channels Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Index</th> <th>RF Chain</th> <th>IF frequency</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>RF Chain 0</td> <td>0</td> <td style="text-align: right; vertical-align: middle;"> + <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>2</td> <td>RF Chain 0</td> <td>-400000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>3</td> <td>RF Chain 0</td> <td>-200000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>4</td> <td>RF Chain 1</td> <td>-400000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>5</td> <td>RF Chain 1</td> <td>-200000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>6</td> <td>RF Chain 1</td> <td>0</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>7</td> <td>RF Chain 1</td> <td>200000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> <tr> <td>8</td> <td>RF Chain 1</td> <td>400000</td> <td style="text-align: right; vertical-align: middle;"> <input checked="" type="checkbox"/>X </td> </tr> </tbody> </table>	Index	RF Chain	IF frequency		1	RF Chain 0	0	+ <input checked="" type="checkbox"/> X	2	RF Chain 0	-400000	<input checked="" type="checkbox"/> X	3	RF Chain 0	-200000	<input checked="" type="checkbox"/> X	4	RF Chain 1	-400000	<input checked="" type="checkbox"/> X	5	RF Chain 1	-200000	<input checked="" type="checkbox"/> X	6	RF Chain 1	0	<input checked="" type="checkbox"/> X	7	RF Chain 1	200000	<input checked="" type="checkbox"/> X	8	RF Chain 1	400000	<input checked="" type="checkbox"/> X
Index	RF Chain	IF frequency																																		
1	RF Chain 0	0	+ <input checked="" type="checkbox"/> X																																	
2	RF Chain 0	-400000	<input checked="" type="checkbox"/> X																																	
3	RF Chain 0	-200000	<input checked="" type="checkbox"/> X																																	
4	RF Chain 1	-400000	<input checked="" type="checkbox"/> X																																	
5	RF Chain 1	-200000	<input checked="" type="checkbox"/> X																																	
6	RF Chain 1	0	<input checked="" type="checkbox"/> X																																	
7	RF Chain 1	200000	<input checked="" type="checkbox"/> X																																	
8	RF Chain 1	400000	<input checked="" type="checkbox"/> X																																	

Use LoRa Standard channel to establish communication between nodes and gateway.

▲ LoRa Standard Channel Settings
<div style="display: flex; align-items: center;"> Enable <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;"> <input type="button" value="ON"/> OFF </div> </div> <div style="margin-top: 10px;"> RF Chain <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">RF Chain 0</div> </div> <div style="margin-top: 10px;"> IF frequency <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">0</div> </div> <div style="margin-top: 10px;"> Bandwidth <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">125KHz</div> </div> <div style="margin-top: 10px;"> Spread Factor <div style="border: 1px solid #ccc; padding: 2px; margin-left: 10px;">SF7</div> </div>

Use FSK modulation instead of LoRa.

FSK Standard Channel Settings

Enable	<input checked="" type="button"/> ON <input type="button"/> OFF
RF Chain	RF Chain 0
IF frequency	0
Bandwidth	7.8KHz
Datarate	500

RF Settings		
Item	Description	Default
RF Power Settings		
RF Power Limit	<p>Used to indicate the maximum transmit power limit for current gateway.</p> <ul style="list-style-type: none"> No_Limit: Transmit power is not limited, depending on the transmit power value sent by the LoRaWAN server EU_433: Maximum transmit power is limited to 10dbm or less EU_868_870: Maximum transmit power is limited to 14dbm or less CN_470_510: The maximum transmit power is limited to 17dbm or less US_902_928: Maximum transmit power is limited to 26dbm or less AU_915_928: Maximum transmit power limit below 26dbm AS_923: Maximum transmit power is limited to 14dbm or less KR_920_923: Maximum transmit power is limited to 23dbm or less Max_Power: Use the maximum transmit power which is about 24.5dbm <p>Note: The above options are not configurable and need to be set before delivery.</p>	No Limit
RF Chain Settings		
Supported Frequency	Choose the supported frequency depending on the LoRaWAN module.	863 870
RF Chain 0 Frequency	Enter the central frequency of radio transceiver 0 which supports transmitting and receiving.	Null
RF Chain 1 Frequency	Enter the center frequency of radio transceiver 1 which only supports receiving data from nodes.	Null
LoRa Multi Datarate Channels Settings		
Index	Indicate the ordinal of the list.	--
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	RF Chain 0
IF frequency	Enter the IF frequency, measured in Hz. The offset between the central frequency of specific channel and the central frequency of chain is 0/1. Eg: RF Chain 0, IF frequency: -20000. It means the central frequency of this channel should be 868300000=868500000-200000.	0
LoRa Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0

RF Settings		
Item	Description	Default
IF frequency	Enter the IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of specific channel and the center frequency of chain 0/1.	0
Bandwidth	Choose the selectable bandwidth, measured in KHz.	500KHz
Spread Factor	Enter the selectable spreading factor. The channel with large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.	250000
FSK Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0
IF frequency	Enter the IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of specific channel and the center frequency of chain is 0/1.	0
Bandwidth	Choose the selectable bandwidth, measured in KHz.	500KHz
Datarate	Enter the data rate valued from 500 to 250000 and measured in Bit.	250000

Status

Click “Status” to view your node status.

General Settings	RF Settings	Tx Gain Settings	Status										
▲ Basic <table border="1"> <tr> <td>Status</td> <td>Ready</td> </tr> <tr> <td>Packet Forwarder (Protocol)</td> <td>2.2.1 (1)</td> </tr> <tr> <td>HAL Library Version</td> <td>3.2.1</td> </tr> </table>				Status	Ready	Packet Forwarder (Protocol)	2.2.1 (1)	HAL Library Version	3.2.1				
Status	Ready												
Packet Forwarder (Protocol)	2.2.1 (1)												
HAL Library Version	3.2.1												
▲ Uplink <table border="1"> <tr> <td>RF packets received</td> <td>66</td> </tr> <tr> <td>RF packets received State</td> <td>CRC_OK: 86.36%, CRC_FAIL: 13.64%, NO_CRC: 0.00%</td> </tr> <tr> <td>RF packets forwarded</td> <td>57 (1029 bytes)</td> </tr> <tr> <td>Push Data Datagrams Sent</td> <td>158 (25231 bytes)</td> </tr> <tr> <td>Push Data Acknowledged</td> <td>100.00%</td> </tr> </table>				RF packets received	66	RF packets received State	CRC_OK: 86.36%, CRC_FAIL: 13.64%, NO_CRC: 0.00%	RF packets forwarded	57 (1029 bytes)	Push Data Datagrams Sent	158 (25231 bytes)	Push Data Acknowledged	100.00%
RF packets received	66												
RF packets received State	CRC_OK: 86.36%, CRC_FAIL: 13.64%, NO_CRC: 0.00%												
RF packets forwarded	57 (1029 bytes)												
Push Data Datagrams Sent	158 (25231 bytes)												
Push Data Acknowledged	100.00%												
▲ Downlink <table border="1"> <tr> <td>Pull Data Sent</td> <td>101 (100.00% acknowledged)</td> </tr> <tr> <td>Pull Resp Datagrams Received</td> <td>29 (5069 bytes)</td> </tr> <tr> <td>RF Packets Sent to Concentrator</td> <td>29 (398 bytes)</td> </tr> <tr> <td>RF Packets Sent Errors</td> <td>0</td> </tr> </table>				Pull Data Sent	101 (100.00% acknowledged)	Pull Resp Datagrams Received	29 (5069 bytes)	RF Packets Sent to Concentrator	29 (398 bytes)	RF Packets Sent Errors	0		
Pull Data Sent	101 (100.00% acknowledged)												
Pull Resp Datagrams Received	29 (5069 bytes)												
RF Packets Sent to Concentrator	29 (398 bytes)												
RF Packets Sent Errors	0												

Status	
Item	Description
Basic	
Status	Show the LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show the version of Packet forwarder.
HAL Library Version	Show the driver version of LoRaWAN chipset inside gateway.
Uplink	
RF packets received	Show the count of data packet from node to gateway.
RF packets received State	Show the RF packets receiving state. <ul style="list-style-type: none"> • CRC_OK: Percentage of CRC verification • CRC_Fail: Percentage of CRC verification failure • NO_CRC: Percentage of abnormal packets without CRC
RF packets forwarded	Packets that CRC verified are sent from gateway to server.
Push Data Datagrams Sent	The total quantity of packets sent from gateway to server, including the RF packets forwarded and statistics packets.
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent:
Downlink	
Pull Data Sent	Show the number of keepalive packets sent to the server, and percentage of acknowledged packet regarding the keepalive packet from the server.
Pull Resp Datagrams Received	Show the packet counts and size that will be sent from server to gateway.
RF Packets Sent to Concentrator	Show the RF packet counts and size that will be sent from gateway to node.
RF Packets Sent Errors	Show the RF packet counts that fail to be sent from server to node.

3.14 Network > Route

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

Static Route

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

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

Static Route

^ Static Route

Index	1
Description	
Destination	
Netmask	
Gateway	
Interface	lan0 

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

Status

This window allows you to view the status of route.

Static Route	Status				
^ Route Table					
Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	10.244.165.241	wwan	0
2	10.244.165.240	255.255.255.252	0.0.0.0	wwan	0
3	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0

3.15 Network > Firewall

This section allows you to set the firewall and its related parameters, including Filtering, Port Mapping and DMZ.

Filtering

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

Filtering	Port Mapping	Custom Rules	DMZ	Status																				
General Settings <div style="display: flex; justify-content: space-between;"> Enable Filtering <input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> Default Filtering Policy <input type="button" value="Accept"/> <input type="button" value="Drop"/> <input data-kind="parent" data-rs="2" type="button" value="?"/> </div>																								
Access Control Settings <table border="0"> <tr><td>Enable Remote SSH Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Local SSH Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Remote Telnet Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Local Telnet Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Remote HTTP Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Local HTTP Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Remote HTTPS Access</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Remote Ping Respond</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="parent" data-rs="2" type="button" value="?"/></td></tr> <tr><td>Enable DOS Defending</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/></td></tr> <tr><td>Enable Console</td><td><input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="ghost" type="button" value="?"/></td></tr> </table>					Enable Remote SSH Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Local SSH Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Remote Telnet Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Local Telnet Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Remote HTTP Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Local HTTP Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Remote HTTPS Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Remote Ping Respond	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="parent" data-rs="2" type="button" value="?"/>	Enable DOS Defending	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>	Enable Console	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="ghost" type="button" value="?"/>
Enable Remote SSH Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Local SSH Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Remote Telnet Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Local Telnet Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Remote HTTP Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Local HTTP Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Remote HTTPS Access	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Remote Ping Respond	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="parent" data-rs="2" type="button" value="?"/>																							
Enable DOS Defending	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/>																							
Enable Console	<input checked="" type="button" value="ON"/> <input type="button" value="OFF"/> <input data-kind="ghost" type="button" value="?"/>																							
Filtering Rules <table border="0"> <tr><td>Index</td><td>Source Address</td><td>Source Port</td><td>Source MAC</td><td>Target Address</td><td>Target Port</td><td>Protocol</td><td><input data-kind="parent" data-rs="2" type="button" value="+"/></td></tr> </table>					Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol	<input data-kind="parent" data-rs="2" type="button" value="+"/>												
Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol	<input data-kind="parent" data-rs="2" type="button" value="+"/>																	

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

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

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



The screenshot shows a configuration interface for 'Filtering Rules'. The 'Protocol' field is highlighted with a red box, indicating it is the current selection. Other fields include 'Index', 'Description', 'Source Address', 'Source MAC', 'Target Address', and 'Action'.

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

Filtering Rules

Index	1
Description	
Source Address	
Source Port	
Source MAC	
Target Address	
Target Port	
Protocol	TCP
Action	Drop

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

Port Mapping

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

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

Port Mapping

▲ Port Mapping Rules

Index	1
Description	
Remote IP	
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

Port Mapping Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of gateway which can be accessed by other hosts from internet.	Null
Local IP	Enter gateway's LAN IP which will forward to the internet port of gateway.	Null
Local Port	Enter the port of gateway's LAN IP.	Null
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP

Custom Rules

- [Filtering](#)
- [Port Mapping](#)
- [Custom Rules](#)
- [DMZ](#)
- [Status](#)

▲ Custom Iptables Rules

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

Click  to add custom rules. The maximum rule count is 40.

Custom Rules

▲ Custom Iptables Rule

Index	1
Description	
Rule	

Custom Iptables Rule		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this rule.	Null
Rule	Specify one iptables rule. e.g -I INPUT -s 192.168.0.2 -j ACCEPT	Null

DMZ

Filtering Port Mapping Custom Rules DMZ Status

▲ DMZ Settings

Enable DMZ OFF

Host IP Address

Source IP Address ?

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

Status

Click the "Status" column to view the

Filtering Port Mapping Custom Rules DMZ Status

▲ Chain Input

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	wwan	*	0.0.0.0/0	!10.244.165.242
2	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
4	0	DROP	tcp	wwan	*	0.0.0.0/0	0.0.0.0/0
5	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	50	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0

▲ Chain Forward

Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0

▲ Chain Output

Index	Packets	Target	Protocol	In	Out	Source	Destination

3.16 Network > IP Passthrough

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



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

3.17 VPN > IPsec

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

General



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

Tunnel

General	Tunnel	Status	x509							
▲ Tunnel Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Index</td> <td style="width: 10%;">Enable</td> <td>Description</td> <td>Gateway</td> <td>Local Subnet</td> <td>Remote Subnet</td> <td style="text-align: right; width: 10px;">+</td> </tr> </table>				Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+				

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

Tunnel																	
▲ General Settings <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">Index</td> <td style="width: 10%;">1</td> </tr> <tr> <td>Enable</td> <td>ON <input type="button" value="OFF"/></td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Gateway</td> <td></td> </tr> <tr> <td>Mode</td> <td>Tunnel</td> </tr> <tr> <td>Protocol</td> <td>ESP</td> </tr> <tr> <td>Local Subnet</td> <td></td> </tr> <tr> <td>Remote Subnet</td> <td></td> </tr> </table>		Index	1	Enable	ON <input type="button" value="OFF"/>	Description		Gateway		Mode	Tunnel	Protocol	ESP	Local Subnet		Remote Subnet	
Index	1																
Enable	ON <input type="button" value="OFF"/>																
Description																	
Gateway																	
Mode	Tunnel																
Protocol	ESP																
Local Subnet																	
Remote Subnet																	

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address of remote IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a gateway, in which the gateway is the actual destination 	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> ESP: Use the ESP protocol AH: Use the AH protocol 	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null

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

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

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

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

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

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

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

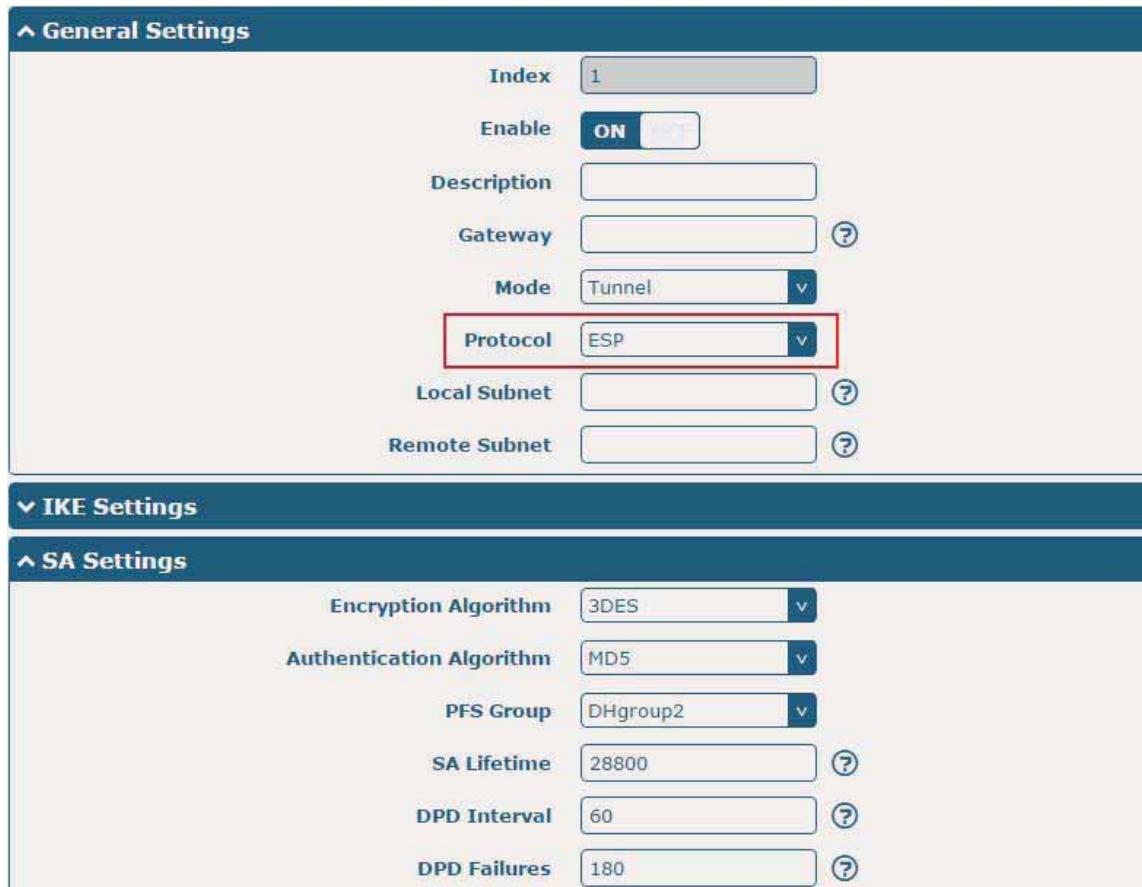
^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE Settings		
Item	Description	Default
IKE Type	Select from “IKEv1” or “IKEv2” as IKE version.	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in IKE negotiation.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256” to be used in IKE negotiation. <ul style="list-style-type: none"> • 3DES: Use 168-bit 3DES encryption algorithm in CBC mode • AES128: Use 128-bit AES encryption algorithm in CBC mode • AES256: Use 256-bit AES encryption algorithm in CBC mode 	3DES
IKE DH Group	Select from “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17” or “DHgroup18” to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. <ul style="list-style-type: none"> • PSK: Pre-shared Key • CA: x509 Certificate Authority • xAuth: Extended Authentication to AAA server 	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. <ul style="list-style-type: none"> • Default: Use an IP address as the ID in IKE negotiation • FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com • User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local 	Default

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

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



The screenshot shows the configuration interface for a tunnel. The **General Settings** section is open, displaying fields for Index (1), Enable (ON), Description, Gateway, Mode (Tunnel), Protocol (ESP, highlighted with a red box), Local Subnet, and Remote Subnet. The **IKE Settings** and **SA Settings** sections are also visible below.

General Settings	
Index	1
Enable	ON
Description	
Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Remote Subnet	

IKE Settings	
Encryption Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

SA Settings	
Encryption Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

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

General Settings

Index	1
Enable	ON <input type="button" value="OFF"/>
Description	
Gateway	
Mode	Tunnel <input type="button" value="▼"/>
Protocol	AH <input type="button" value="▼"/>
Local Subnet	
Remote Subnet	

IKE Settings

SA Settings

Authentication Algorithm	MD5 <input type="button" value="▼"/>
PFS Group	DHgroup2 <input type="button" value="▼"/>
SA Lifetime	28800 <input type="button" value="?"/>
DPD Interval	60 <input type="button" value="?"/>
DPD Failures	180 <input type="button" value="?"/>

Advanced Settings

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

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

SA Settings		
Item	Description	Default
	no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

Status

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

General	Tunnel	Status	x509
IPSec Tunnel Status			
Index	Description	Status	Uptime

x509

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

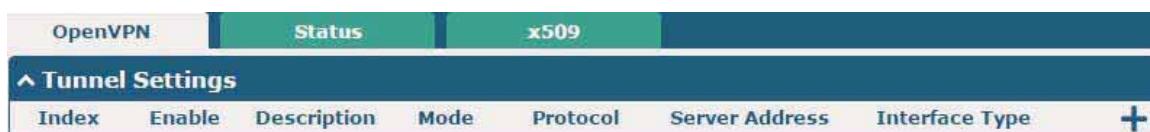
General	Tunnel	Status	x509
X509 Settings			
Tunnel Name	Tunnel 1	v	(?)
Certificate Files	Choose File	No file chosen	Upload
Certificate Files			
Index	File Name	File Size	Modification Time
x509			
Item	Description	Default	
X509 Settings			
Tunnel Name	Choose a valid tunnel.	Tunnel 1	
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your gateway. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null	

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

3.18 VPN > OpenVPN

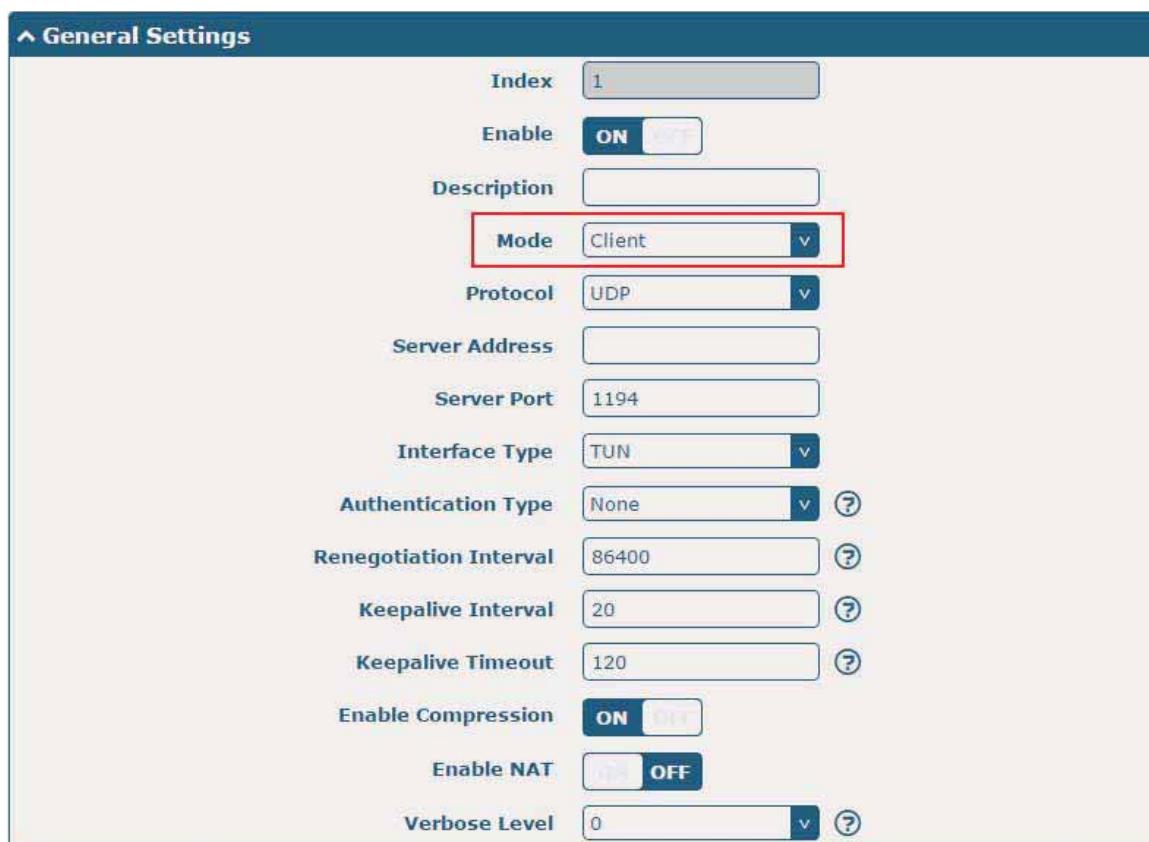
This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.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

OpenVPN



The screenshot shows the 'Tunnel Settings' tab of the OpenVPN configuration interface. The top navigation bar includes tabs for 'OpenVPN', 'Status', and 'x509'. Below the tabs, there is a header with columns: Index, Enable, Description, Mode, Protocol, Server Address, Interface Type, and a '+' button for adding new entries. The 'Mode' column for the first entry is highlighted with a red box.

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



The screenshot shows the 'General Settings' configuration window for a specific tunnel entry. The window contains the following fields:

- Index:** 1
- Enable:** ON
- Description:** (empty)
- Mode:** Client (highlighted with a red box)
- Protocol:** UDP
- Server Address:** (empty)
- Server Port:** 1194
- Interface Type:** TUN
- Authentication Type:** None (with a question mark icon)
- Renegotiation Interval:** 86400 (with a question mark icon)
- Keepalive Interval:** 20 (with a question mark icon)
- Keepalive Timeout:** 120 (with a question mark icon)
- Enable Compression:** ON
- Enable NAT:** OFF
- Verbose Level:** 0 (with a question mark icon)

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

General Settings

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

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

General Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

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

General Settings

Index	1
Enable	ON OFF
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON OFF
Enable NAT	ON OFF
Verbose Level	0

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

General Settings

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

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

General Settings

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

General Settings @ OpenVPN

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

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

Advanced Settings

Enable HMAC Firewall	<input type="button" value="ON"/> OFF
Enable PKCS#12	<input type="button" value="ON"/> OFF
Enable nsCertType	<input type="button" value="ON"/> OFF
Expert Options	<input type="text"/> ?

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

Status

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

OpenVPN	Status	x509
OpenVPN Tunnel Status		
Index	Description	Status
		Uptime
		Local IP

x509

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

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

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1

Certificate Files	Click on “Choose File” to locate the certificate file from your computer, and then import this file into your gateway. The correct file format is displayed as follows: @ca.crt @remote.crt @local.crt @private.key @crl.pem @client.p12	Null
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.19 VPN > GRE

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

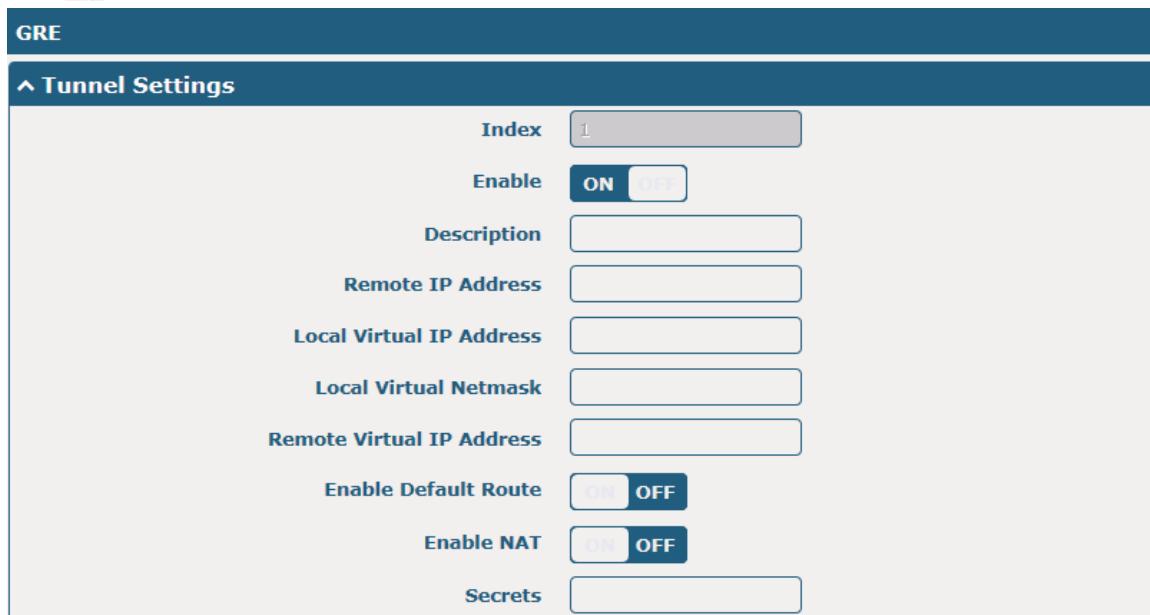
GRE



The screenshot shows the GRE Status interface with the following details:

- GRE** tab is selected.
- Status** tab is also present.
- Tunnel Settings** section is expanded.
- Header for the table: **Index**, **Enable**, **Description**, **Remote IP Address**.
- A blue plus icon (+) is located at the top right of the table area.

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



The screenshot shows the GRE configuration interface with the following details:

- GRE** tab is selected.
- Tunnel Settings** section is expanded.
- Form fields for setting up a tunnel:
 - Index**: Value 1.
 - Enable**: ON button is selected.
 - Description**: Empty input field.
 - Remote IP Address**: Empty input field.
 - Local Virtual IP Address**: Empty input field.
 - Local Virtual Netmask**: Empty input field.
 - Remote Virtual IP Address**: Empty input field.
 - Enable Default Route**: ON button is selected.
 - Enable NAT**: OFF button is selected.
 - Secrets**: Empty input field.

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

Status

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



The screenshot shows a navigation bar with 'GRE' and 'Status' tabs. Below is a detailed table for 'GRE tunnel status' with the following columns: Index, Description, Status, Local IP Address, Remote IP Address, and Uptime.

Index	Description	Status	Local IP Address	Remote IP Address	Uptime
-------	-------------	--------	------------------	-------------------	--------

3.20 Services > Syslog

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



The screenshot shows the 'Syslog Settings' interface with the following configuration options:

- Enable: ON (button)
- Syslog Level: Debug (dropdown menu)
- Save Position: RAM (dropdown menu)
- Log to Remote: OFF (button)

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



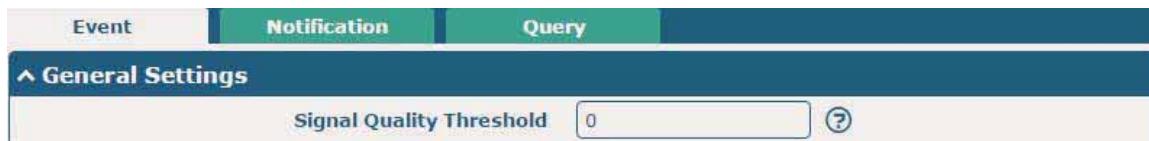
Syslog Settings

Enable	ON <input checked="" type="checkbox"/>
Syslog Level	Debug <input type="button" value="▼"/>
Save Position	RAM <input type="button" value="▼"/> <input type="button" value="?"/>
Log to Remote	ON <input checked="" type="checkbox"/> <input type="button" value="?"/>
Add Identifier	OFF <input type="checkbox"/> <input type="button" value="?"/>
Remote IP Address	<input type="text"/>
Remote Port	<input type="text"/> 514

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

3.21 Services > Event

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



General Settings

Signal Quality Threshold	<input type="text"/> 0 <input type="button" value="?"/>
--------------------------	---

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

Event **Notification** **Query**

▲ Event Notification Group Settings

Index Description Send SMS Send Email Save to NVM **+**

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

Notification

General Settings

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

Event Selection **?**

System Startup	<input type="checkbox"/> OFF
System Reboot	<input type="checkbox"/> OFF
System Time Update	<input type="checkbox"/> OFF
Configuration Change	<input type="checkbox"/> OFF
Cellular Network Type Change	<input type="checkbox"/> OFF
Cellular Data Stats Clear	<input type="checkbox"/> OFF
Cellular Data Traffic Overflow	<input type="checkbox"/> OFF
Poor Signal Quality	<input type="checkbox"/> OFF
Link Switching	<input type="checkbox"/> OFF
WAN Up	<input type="checkbox"/> OFF
WAN Down	<input type="checkbox"/> OFF
WWAN Up	<input type="checkbox"/> OFF
WWAN Down	<input type="checkbox"/> OFF
IPSec Connection Up	<input type="checkbox"/> OFF
IPSec Connection Down	<input type="checkbox"/> OFF
OpenVPN Connection Up	<input type="checkbox"/> OFF
OpenVPN Connection Down	<input type="checkbox"/> OFF
LAN Port Link Up	<input type="checkbox"/> OFF
LAN Port Link Down	<input type="checkbox"/> OFF
USB Device Connect	<input type="checkbox"/> OFF
USB Device Remove	<input type="checkbox"/> OFF
DDNS Update Success	<input type="checkbox"/> OFF
DDNS Update Fail	<input type="checkbox"/> OFF
Received SMS	<input type="checkbox"/> OFF
SMS Command Execute	<input type="checkbox"/> OFF
DI 1 ON	<input type="checkbox"/> OFF
DI 1 OFF	<input type="checkbox"/> OFF
DI 1 Counter Overflow	<input type="checkbox"/> OFF
DI 2 ON	<input type="checkbox"/> OFF
DI 2 OFF	<input type="checkbox"/> OFF
DI 2 Counter Overflow	<input type="checkbox"/> OFF

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

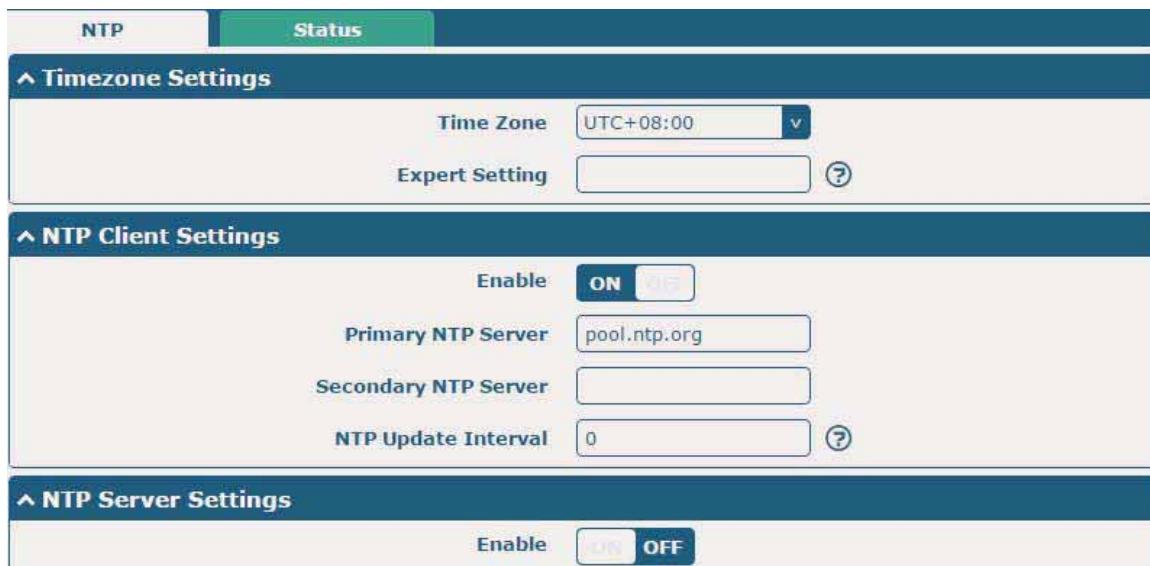
In the following window you can query various types of events record. Click **Refresh** to query filtered events while click **Clear** to clear the event records in the window.

Event	Notification	Query
▲ Event Details <div style="display: flex; justify-content: space-between;"> Save Position <div style="border: 1px solid #ccc; padding: 2px;">RAM</div> </div> <div style="margin-top: 5px;"> Filtering <input type="text"/> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> Oct 11 15:40:39, system startup Oct 11 15:40:41, LAN port link up, eth0 Oct 11 15:41:21, WWAN (cellular) up, WWAN1, ip=10.244.165.242 Oct 11 15:41:33, system time update </div> <div style="text-align: right; margin-top: 10px;"> Clear Refresh </div>		

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

3.22 Services > NTP

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



The screenshot shows the NTP configuration interface with three main sections:

- Timezone Settings:** Includes a dropdown for Time Zone (set to UTC+08:00) and an Expert Setting input field.
- NTP Client Settings:** Includes an Enable toggle (ON), Primary NTP Server (pool.ntp.org), Secondary NTP Server (empty), and NTP Update Interval (0).
- NTP Server Settings:** Includes an Enable toggle (OFF).

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

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

NTP	Status
▲ Time	
System Time 2017-10-11 16:56:27	
PC Time 2017-10-11 16:58:16 Sync	
Last Update Time 2017-10-11 15:41:33	

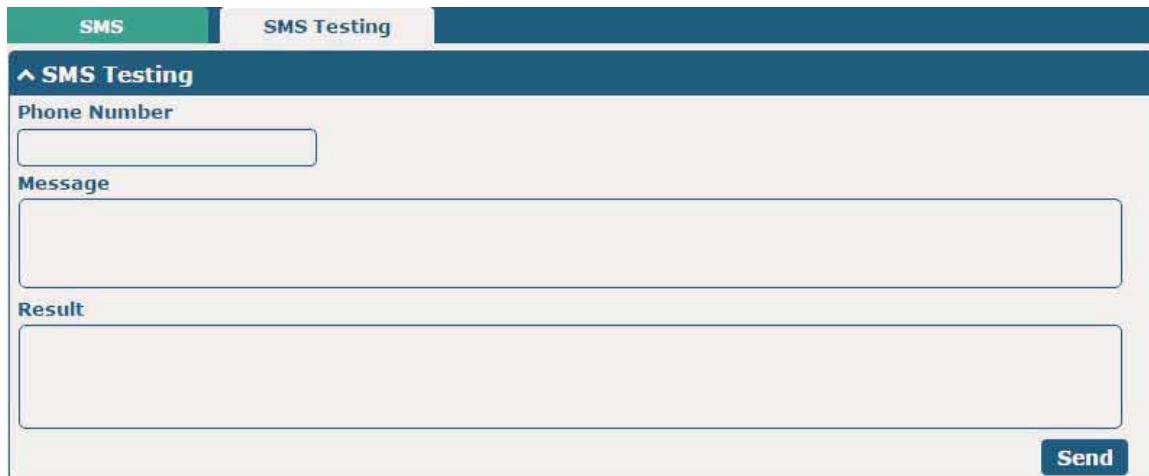
3.23 Services > SMS

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

SMS	SMS Testing
▲ SMS Management Settings	
Enable ON	
Authentication Type Password 	
Phone Number 	

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

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

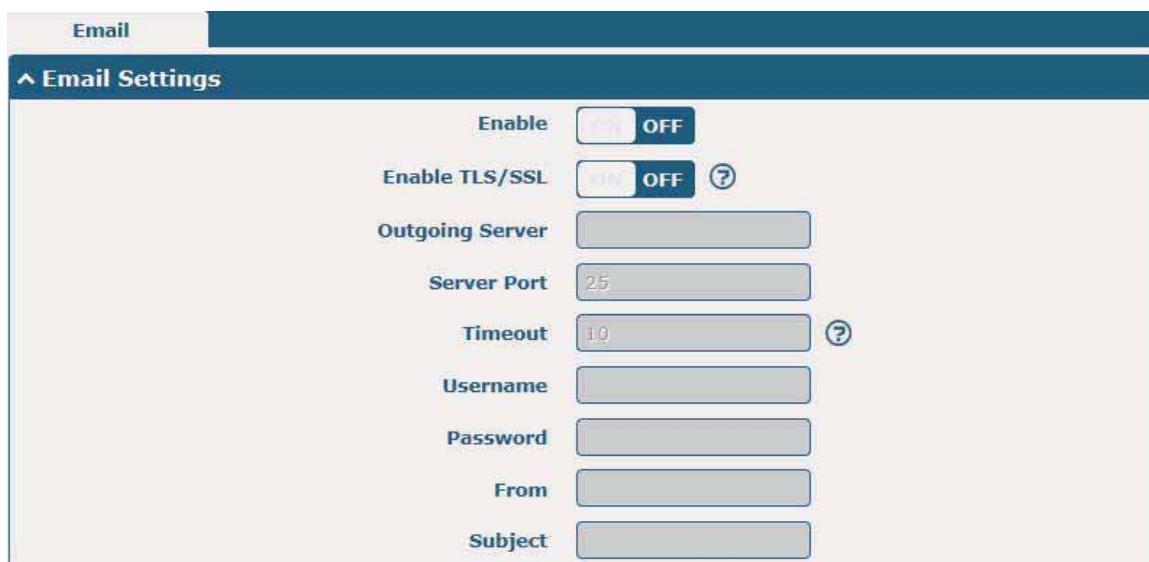


The screenshot shows the 'SMS Testing' section of the Robustel R3000 LG User Guide. It includes fields for 'Phone Number' and 'Message', and a 'Result' box where the test outcome will be displayed. A 'Send' button is located at the bottom right.

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

3.24 Services > Email

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



The screenshot shows the 'Email Settings' section of the Robustel R3000 LG User Guide. It includes fields for 'Enable', 'Enable TLS/SSL', 'Outgoing Server', 'Server Port', 'Timeout', 'Username', 'Password', 'From', and 'Subject'. The 'Enable' and 'Enable TLS/SSL' fields have toggle buttons.

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

Email Settings		
Item	Description	Default
Outgoing server	Enter the SMTP server IP Address or domain name.	Null
Server port	Enter the SMTP server port.	25
Timeout	Set the max time for sending email to SMTP server. When the server doesn't receive the email over this time, it will try to resend.	10
Username	Enter the username which has been registered from SMTP server.	Null
Password	Enter the password of the username above.	Null
From	Enter the source address of the email.	Null
Subject	Enter the subject of this email.	Null

3.25 Services > DDNS

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



The screenshot shows the 'DDNS' tab selected in the top navigation bar. Below it, the 'Status' tab is visible. The main area is titled 'DDNS Settings'. It contains the following fields:

- Enable:** A toggle switch set to 'OFF'.
- Service Provider:** A dropdown menu currently set to 'DynDNS'.
- Hostname:** An empty input field.
- Username:** An empty input field.
- Password:** An empty input field.

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



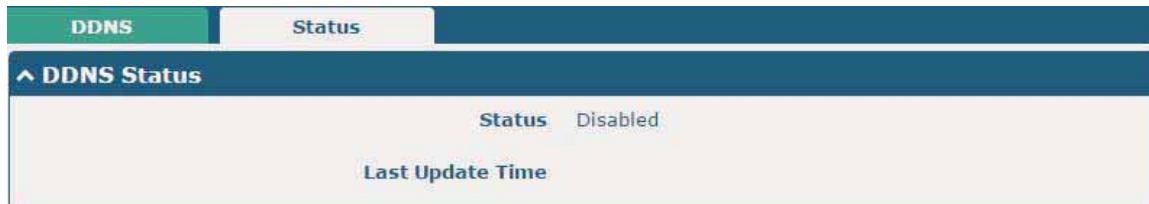
The screenshot shows the 'DDNS' tab selected in the top navigation bar. Below it, the 'Status' tab is visible. The main area is titled 'DDNS Settings'. It contains the following fields:

- Enable:** A toggle switch set to 'OFF'.
- Service Provider:** A dropdown menu currently set to 'Custom'.
- URL:** An empty input field.

DDNS Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. Note: the DDNS service only can be used after registered by	DynDNS

	Corresponding service provider.	
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null

Click “Status” bar to view the status of the DDNS.



The screenshot shows a navigation bar with "DDNS" and "Status" tabs. The "Status" tab is selected, displaying the "DDNS Status" section. It shows a "Status" field set to "Disabled". Below it is a "Last Update Time" field.

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

3.26 Services > SSH

Gateway supports SSH password access and secret-key access.



The screenshot shows a navigation bar with "SSH" and "Keys Management" tabs. The "SSH" tab is selected, displaying the "SSH Settings" section. It includes fields for "Enable" (ON), "Port" (22), and "Disable Password Logins" (OFF).

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

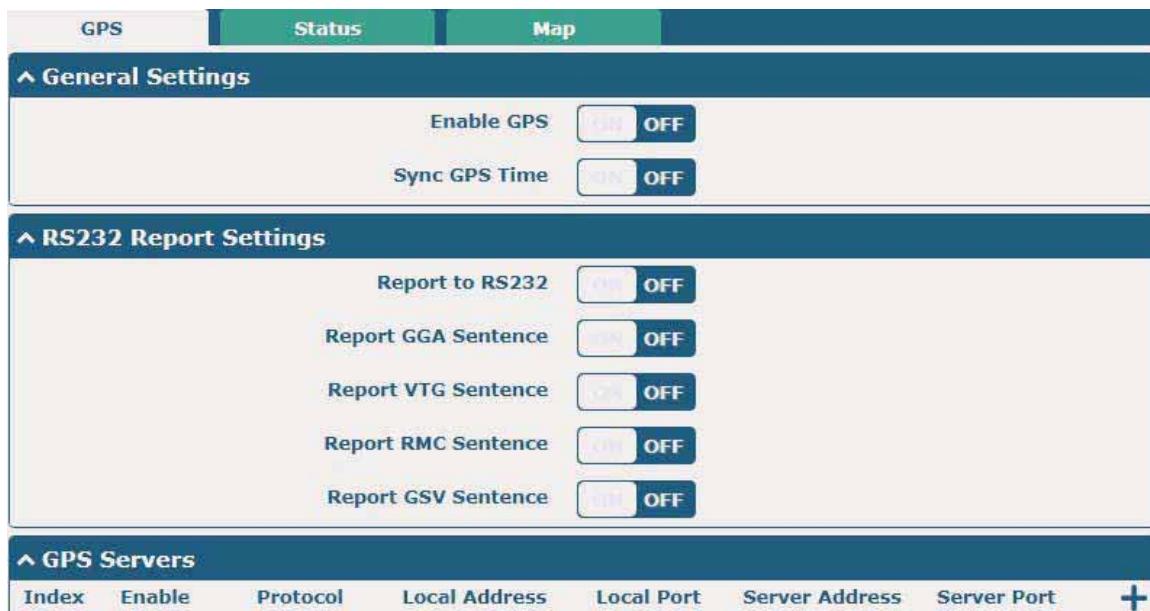


The screenshot shows a navigation bar with "SSH" and "Keys Management" tabs. The "Keys Management" tab is selected, displaying the "Import Authorized Keys" section. It has a "Authorized Keys" field with a "Choose File" button and a "No file chosen" message, and an "Import" button.

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

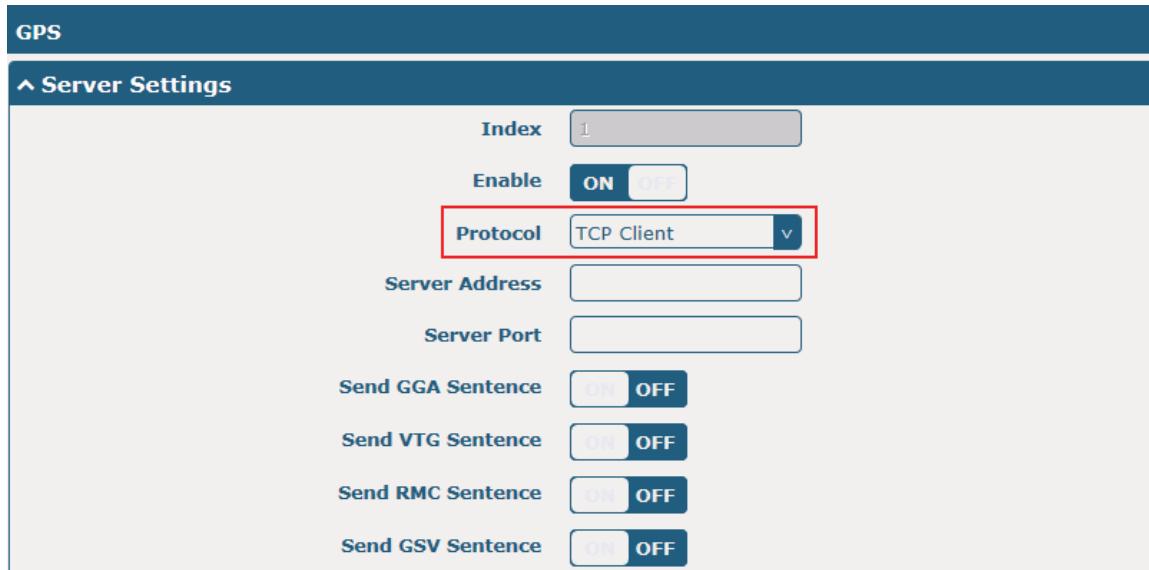
3.27 Services > GPS

This section allows you to set the GPS setting parameters.



GPS		
Item	Description	Default
General Settings		
Enable GPS	Click the toggle button to enable/disable the GPS option.	OFF
Sync GPS Time		OFF
RS232 Report Settings		
Report to RS232	Submit the GPS information via RS232.	OFF
Report GGA Sentence	Submit the GGA information.	OFF
Report VTG Sentence	Submit the VTG information.	OFF
Report RMC Sentence	Submit the RMC information.	OFF
Report GSV Sentence	Submit the GSV information.	OFF

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

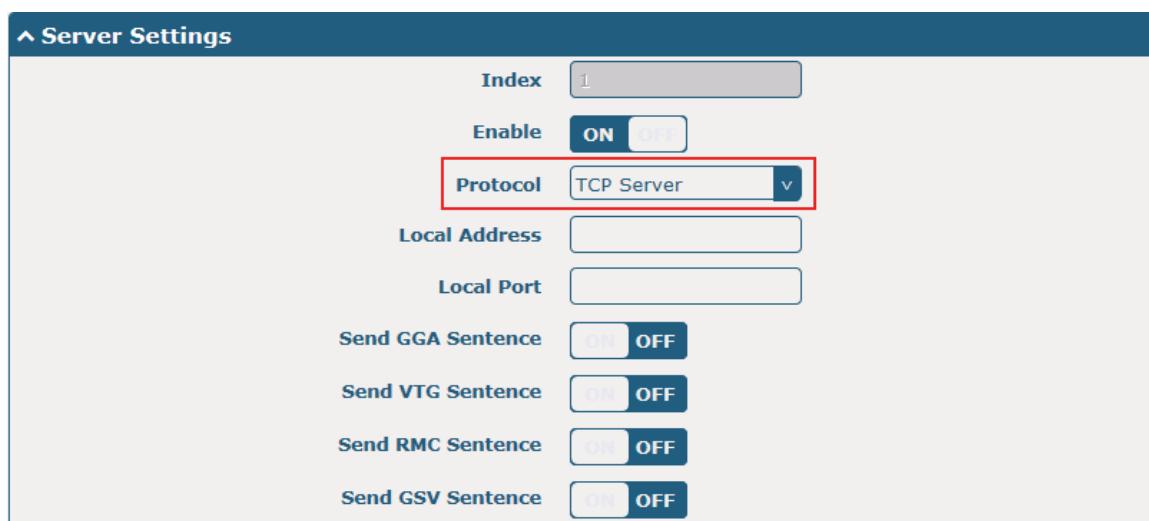


GPS

Server Settings

Index	1
Enable	ON OFF
Protocol	TCP Client
Server Address	[Input Field]
Server Port	[Input Field]
Send GGA Sentence	ON OFF
Send VTG Sentence	ON OFF
Send RMC Sentence	ON OFF
Send GSV Sentence	ON OFF

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



Server Settings

Index	1
Enable	ON OFF
Protocol	TCP Server
Local Address	[Input Field]
Local Port	[Input Field]
Send GGA Sentence	ON OFF
Send VTG Sentence	ON OFF
Send RMC Sentence	ON OFF
Send GSV Sentence	ON OFF

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



Server Settings

Index	1
Enable	ON OFF
Protocol	UDP
Server Address	[Input Field]
Server Port	[Input Field]
Send GGA Sentence	ON OFF
Send VTG Sentence	ON OFF
Send RMC Sentence	ON OFF
Send GSV Sentence	ON OFF

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

Click the "Status" column to view the current status.



GPS Status

Status: Not Fixed

UTC Time: 2017-09-15 07:18:23

Last Fixed Time: 2017-09-14 12:36:58 UTC

Satellites In Use: 4

Satellites In View: 12

Latitude: 23.1534988

Longitude: 113.4013826

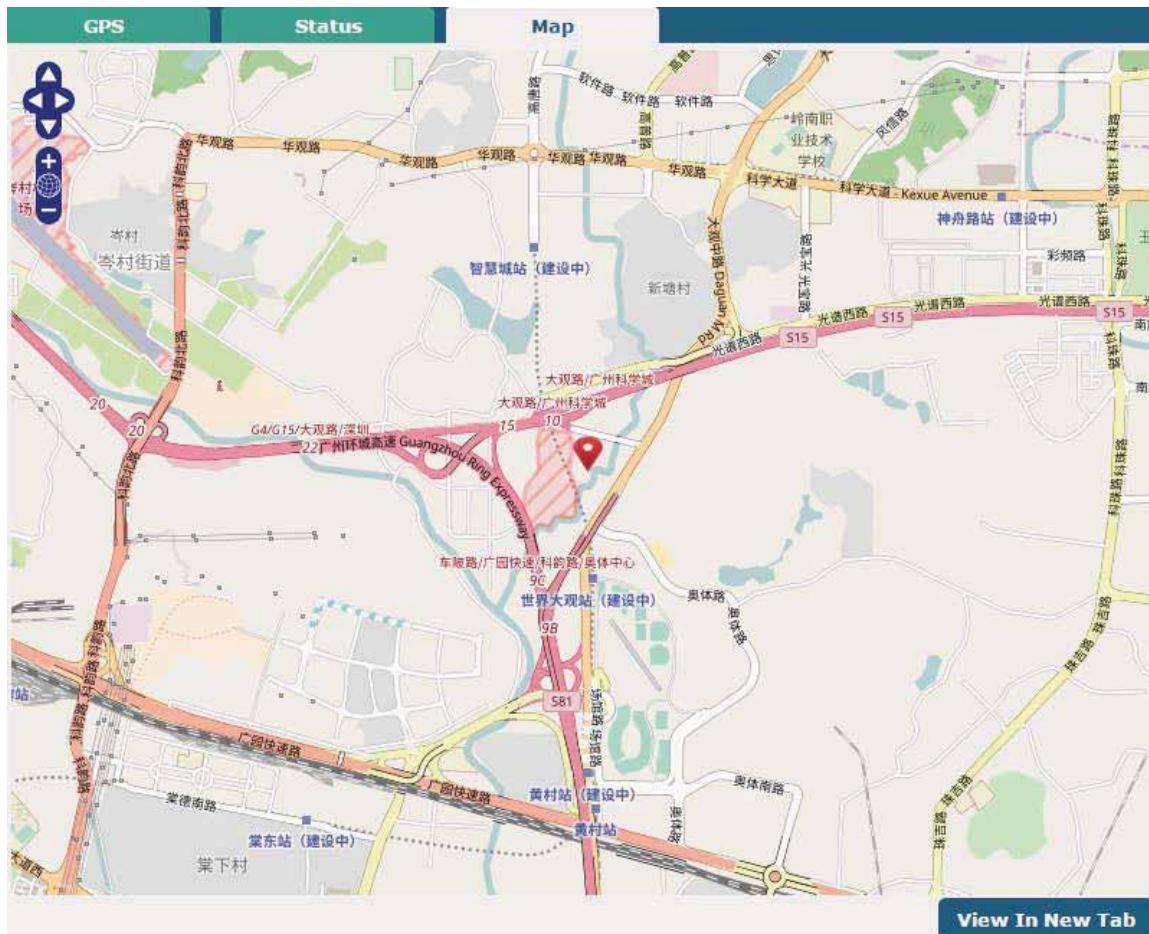
Altitude: 29.0 m

Speed: 1.947 m/s

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

GPS Status	
Item	Description
Speed	Show the horizontal speed of gateway.

Click “Map” column to view the current location of the gateway.



3.28 Services > Web Server

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

Web Server	Certificate Management
General Settings	
HTTP Port	<input type="text" value="80"/> ?
HTTPS Port	<input type="text" value="443"/> ?

General Settings @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in gateway'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 gateway with other HTTP Port number except 80, only adding that port number then you can login gateway's	80

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

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



The screenshot shows a 'Web Server' interface with a 'Certificate Management' tab selected. Under 'Import Certificate', the 'Import Type' dropdown is set to 'CA'. Below it, there is a 'HTTPS Certificate' field with a 'Choose File' button and a 'No file chosen' message, followed by an 'Import' button.

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

3.29 Services > Advanced

This section allows you to set the Advanced and parameters.



The screenshots show the 'System' configuration page. The first part shows 'System Settings' with 'Device Name' set to 'router' and 'User LED Type' set to 'None'. The second part shows the same settings with a red box highlighting the 'User LED Type' dropdown menu, which lists 'None', 'OpenVPN', and 'IPSec', with 'None' currently selected.

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



The screenshot shows the 'Periodic Reboot Settings' section of the web interface. It includes two input fields: 'Periodic Reboot' (set to 0) and 'Daily Reboot Time' (empty), each with a help icon (question mark).

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

3.30 System > Debug

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

Syslog

^ Syslog Details

Log Level: **Debug** ▾

Filtering: ?

```

Oct 11 16:46:28 router user.debug link_manager[732]: recv action ping_success from rping
Oct 11 16:46:28 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:46:28 router user.info link_manager[732]: WWAN1 ping test success
Oct 11 16:51:28 router user.debug link_manager[732]: WWAN1 (wwan) start ping test
Oct 11 16:51:28 router user.debug rping[2977]: start ping 8.8.8.8 (wwan)
Oct 11 16:51:29 router user.debug rping[2977]: PING 8.8.8.8 (8.8.8.8) from 10.244.165.242: 16 data bytes
Oct 11 16:51:29 router user.debug rping[2977]: 24 bytes from 8.8.8.8: seq=0 ttl=248 time=183.775 ms
Oct 11 16:51:29 router user.debug rping[2977]:
Oct 11 16:51:29 router user.debug rping[2977]: --- 8.8.8.8 ping statistics ---
Oct 11 16:51:29 router user.debug rping[2977]: 1 packets transmitted, 1 packets received, 0% packet loss
Oct 11 16:51:29 router user.debug rping[2977]: round-trip min/avg/max = 183.775/183.775/183.775 ms
Oct 11 16:51:29 router user.debug link_manager[732]: recv action ping_success from rping
Oct 11 16:51:29 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:51:29 router user.info link_manager[732]: WWAN1 ping test success
Oct 11 16:56:29 router user.debug link_manager[732]: WWAN1 (wwan) start ping test
Oct 11 16:56:29 router user.debug rping[3105]: start ping 8.8.8.8 (wwan)
Oct 11 16:56:29 router user.debug rping[3105]: PING 8.8.8.8 (8.8.8.8) from 10.244.165.242: 16 data bytes
Oct 11 16:56:29 router user.debug rping[3105]: 24 bytes from 8.8.8.8: seq=0 ttl=248 time=179.991 ms
Oct 11 16:56:29 router user.debug rping[3105]:
Oct 11 16:56:29 router user.debug rping[3105]: --- 8.8.8.8 ping statistics ---
Oct 11 16:56:29 router user.debug rping[3105]: 1 packets transmitted, 1 packets received, 0% packet loss
Oct 11 16:56:29 router user.debug rping[3105]: round-trip min/avg/max = 179.991/179.991/179.991 ms
Oct 11 16:56:29 router user.debug link_manager[732]: recv action ping_success from rping
Oct 11 16:56:29 router user.debug link_manager[732]: target link WWAN1, state Connected
Oct 11 16:56:29 router user.info link_manager[732]: WWAN1 ping test success

```

Manual Refresh ▾ **Clear** **Refresh**

^ Syslog Files

Index	File Name	File Size	Modification Time
1	messages	26328	Wed Oct 11 16:56:29 2017

^ System Diagnostic Data

System Diagnostic Data **Generate**

System Diagnostic Data **Download**

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

Refresh	Click the button to refresh the syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	--
System Diagnosing Data		
Generate	Click to generate the syslog diagnosing file.	--
Download	Click to download system diagnosing file.	--

3.31 System > Update

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

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



3.32 System > App Center

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

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



App Center				
Item	Description			Default
App Install				
File	Click on “Choose File” to locate the App file from your computer, and then click Install to import this file into your gateway.	--	--	--

App Center		
Item	Description	Default
Note: File format should be <i>xxx.rpk</i> , e.g. <i>R3000 LG-robustlink-1.0.0.rpk</i> .		
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

3.33 System > Tools

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

- Ping
- Traceroute
- Sniffer

^ Ping

IP Address	<input type="text"/>
Number of Request	<input type="text" value="5"/>
Timeout	<input type="text" value="1"/>
Local IP	<input type="text"/>

Start
Stop

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

Ping **Traceroute** **Sniffer**

▲ Traceroute

Trace Address

Trace Hops

Trace Timeout

Start **Stop**

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

Ping **Traceroute** **Sniffer**

▲ Sniffer

Interface

Host

Packets Request

Protocol

Status 

Start **Stop**

Capture Files			
Index	File Name	File Size	Modification Time
1	17-10-11_17-02-11.cap	24	Wed Oct 11 17:02:12 2017

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

3.34 System > Profile

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

Profile
Rollback

^ Import Configuration File

Reset Other Settings to Default
 OFF


Ignore Invalid Settings
 OFF


XML Configuration File

No file chosen

^ Export Configuration File

Ignore Disabled Features
 OFF


Add Detailed Information
 OFF


Encrypt Secret Data
 OFF


XML Configuration File

XML Configuration File

^ Default Configuration

Save Running Configuration as Default



Restore to Default Configuration

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

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



The screenshot shows the 'Configuration Rollback' section of the interface. It includes a 'Save as a Rollbackable Archive' button, a 'Save' button, and a help icon. Below this is the 'Configuration Archive Files' section with columns for Index, File Name, File Size, and Modification Time.

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

3.35 System > User Management

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

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



The screenshot shows the 'Super User Settings' section. It includes fields for New Username, Old Password, New Password, and Confirm Password, each with a help icon.

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

Super User Common User

^ Common User Settings

Index Role Username +

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

Common User

^ Common Users Settings

Index	<input type="text" value="1"/>
Role	<input type="text" value="Visitor"/>
Username	<input type="text"/>
Password	<input type="text"/>

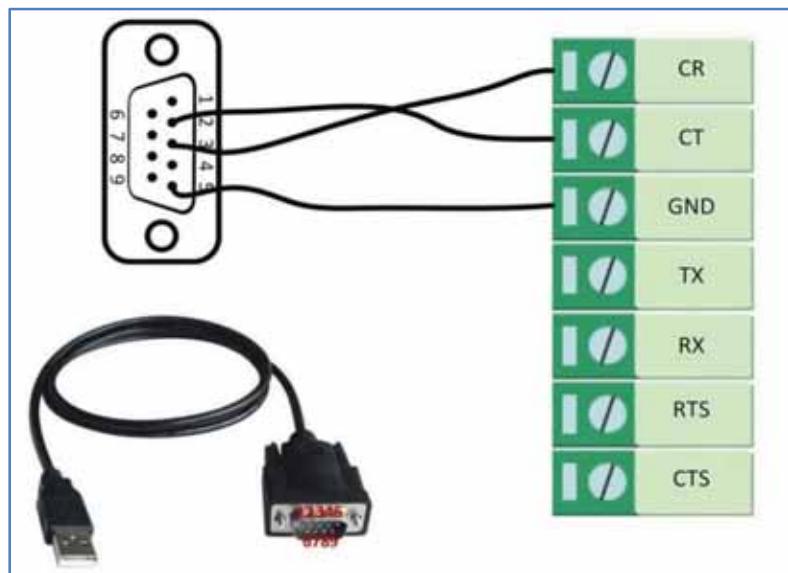
Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from “Visitor” and “Editor”. <ul style="list-style-type: none"> Visitor: Users only can view the configuration of gateway under this level Editor: Users can view and set the configuration of gateway under this level 	Visitor
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null

Chapter 4 Configuration Examples

4.1 Interface

4.1.1 Console Port

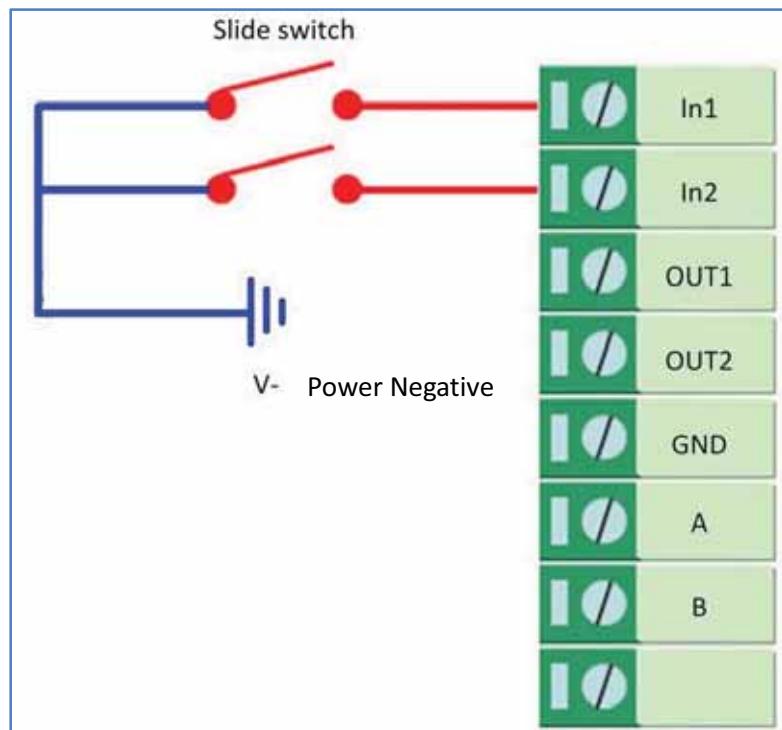
You can use the console port to manage the gateway via CLI commands, please refer to [Chapter 5 Introductions for CLI](#).



4.1.2 Digital Input

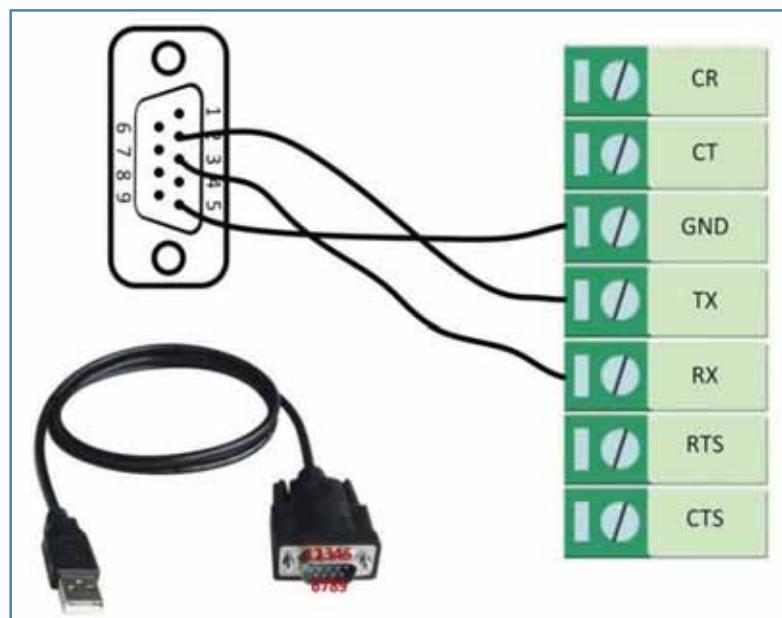
R3000 LG supports digital input with dry contact. Please check the connector interface of the gateway, you can easily find a mark "V-" at one pin of the power connector.

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



4.1.3 RS-232

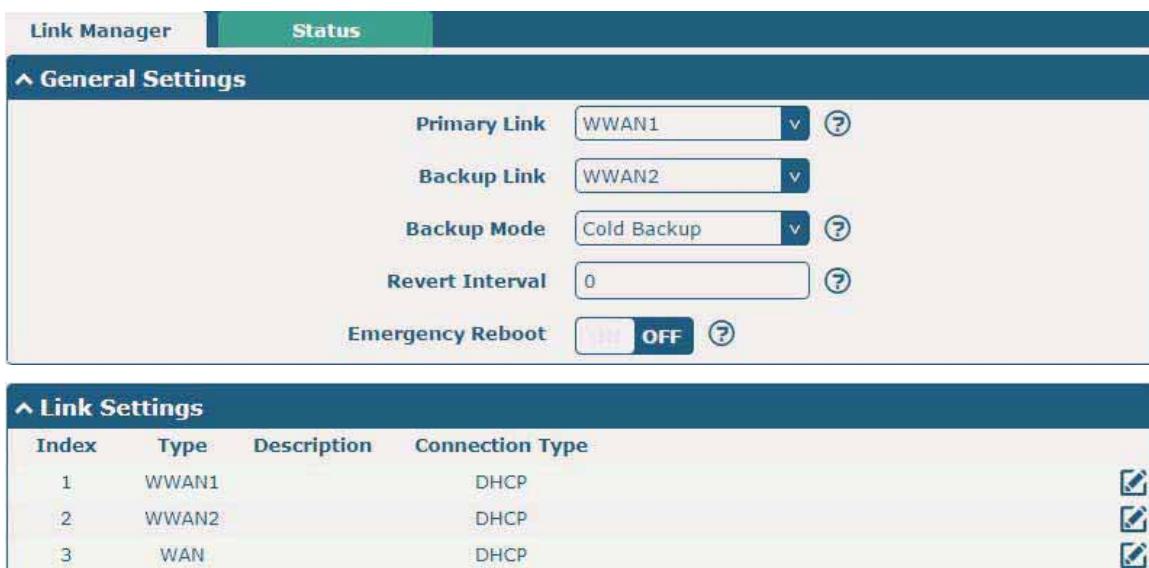
R3000 LG supports one RS-232 for serial data communication. Please refer to the connection diagram at the right side.



4.2 Cellular

4.2.1 Cellular Dial-Up

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



The screenshot displays the Robustel R3000 LG web-based configuration interface. It shows two main sections: "General Settings" and "Link Settings".

General Settings:

- Primary Link:** Set to "WWAN1".
- Backup Link:** Set to "WWAN2".
- Backup Mode:** Set to "Cold Backup".
- Revert Interval:** Set to "0".
- Emergency Reboot:** Set to "OFF".

Link Settings:

Index	Type	Description	Connection Type	Action
1	WWAN1		DHCP	<input checked="" type="checkbox"/>
2	WWAN2		DHCP	<input checked="" type="checkbox"/>
3	WAN		DHCP	<input checked="" type="checkbox"/>

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

Link Manager

General Settings

Index	<input type="text" value="1"/>
Type	<input type="text" value="WWAN1"/>
Description	

WWAN Settings

Automatic APN Selection	<input checked="" type="button" value="ON"/>
Dialup Number	<input type="text" value="*99****1#"/>
Authentication Type	<input type="text" value="Auto"/>
Switch SIM By Data Allowance	<input checked="" type="button" value="ON"/>
Data Allowance	<input type="text" value="0"/>
Billing Day	<input type="text" value="1"/>

Ping Detection Settings

Enable	<input checked="" type="button" value="ON"/>
Primary Server	<input type="text" value="8.8.8.8"/>
Secondary Server	<input type="text" value="114.114.114.114"/>
Interval	<input type="text" value="300"/>
Retry Interval	<input type="text" value="5"/>
Timeout	<input type="text" value="3"/>
Max Ping Tries	<input type="text" value="3"/>

Advanced Settings

NAT Enable	<input checked="" type="button" value="ON"/>
Upload Bandwidth	<input type="text" value="10000"/>
Download Bandwidth	<input type="text" value="10000"/>
Overridden Primary DNS	<input type="text"/>
Overridden Secondary DNS	<input type="text"/>
Debug Enable	<input checked="" type="button" value="ON"/>
Verbose Debug Enable	<input type="button" value="ON"/> <input checked="" type="button" value="OFF"/>

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

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

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

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

Cellular

General Settings

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

Cellular Network Settings

Network Type	<input type="button" value="Auto"/>
Band Select Type	<input type="button" value="All"/>

Advanced Settings

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

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

4.2.2 SMS Remote Control

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

An SMS command has the following structure:

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

SMS command Explanation:

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

please refer to **Chapter 5 Introductions for CLI**.

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

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



XML command:

```
<lan>
<network max_entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.7.29</ip>
<netmask>255.255.0.0</netmask>
<mtu>1500</mtu>
```

SMS cmd:

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.7.29
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 to get the system status.

SMS received:

```
hardware_version = 1.0
firmware_version = "1.0.0"
kernel_version = 4.1.0
```

```
device_model = R3000 LG
serial_number = 10201711101533
system_uptime = "0 days, 01:39:50"
system_time = "Wed Oct 11 17:20:07 2017"
```

admin:admin;reboot

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

SMS received:

OK

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

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

SMS received:

OK

OK

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;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 commands is to configure the LAN parameter.

SMS received:

OK

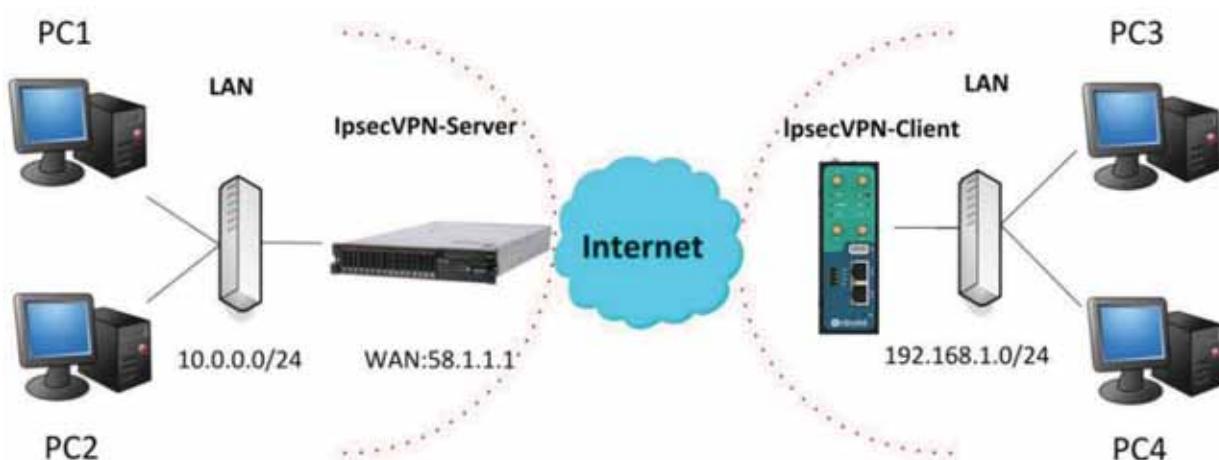
OK

OK

OK

4.3 Network

4.3.1 IPsec VPN



The configuration of server and client is as follows.

IPsec VPN_Server:**Cisco 2811:**

```

Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#
  authentication Set authentication method for protection suite
  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-MD5-MDS 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)#no shutdown
Router(config-if)#crypto map cry-map
*Jan  9 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

```

IPsec VPN Client:

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

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

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

Tunnel																					
▲ General Settings <table border="1"> <tr> <td>Index</td> <td>1</td> </tr> <tr> <td>Enable</td> <td>ON</td> </tr> <tr> <td>Description</td> <td></td> </tr> <tr> <td>Gateway</td> <td></td> </tr> <tr> <td>Mode</td> <td>Tunnel</td> </tr> <tr> <td>Protocol</td> <td>ESP</td> </tr> <tr> <td>Local Subnet</td> <td></td> </tr> <tr> <td>Remote Subnet</td> <td></td> </tr> </table>		Index	1	Enable	ON	Description		Gateway		Mode	Tunnel	Protocol	ESP	Local Subnet		Remote Subnet					
Index	1																				
Enable	ON																				
Description																					
Gateway																					
Mode	Tunnel																				
Protocol	ESP																				
Local Subnet																					
Remote Subnet																					
▲ IKE Settings <table border="1"> <tr> <td>IKE Type</td> <td>IKEv1</td> </tr> <tr> <td>Negotiation Mode</td> <td>Main</td> </tr> <tr> <td>Authentication Algorithm</td> <td>MD5</td> </tr> <tr> <td>Encryption Algorithm</td> <td>3DES</td> </tr> <tr> <td>IKE DH Group</td> <td>DHgroup2</td> </tr> <tr> <td>Authentication Type</td> <td>PSK</td> </tr> <tr> <td>PSK Secret</td> <td></td> </tr> <tr> <td>Local ID Type</td> <td>Default</td> </tr> <tr> <td>Remote ID Type</td> <td>Default</td> </tr> <tr> <td>IKE Lifetime</td> <td>86400</td> </tr> </table>		IKE Type	IKEv1	Negotiation Mode	Main	Authentication Algorithm	MD5	Encryption Algorithm	3DES	IKE DH Group	DHgroup2	Authentication Type	PSK	PSK Secret		Local ID Type	Default	Remote ID Type	Default	IKE Lifetime	86400
IKE Type	IKEv1																				
Negotiation Mode	Main																				
Authentication Algorithm	MD5																				
Encryption Algorithm	3DES																				
IKE DH Group	DHgroup2																				
Authentication Type	PSK																				
PSK Secret																					
Local ID Type	Default																				
Remote ID Type	Default																				
IKE Lifetime	86400																				

SA Settings

Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	DHgroup2
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

Advanced Settings

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

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

The comparison between server and client is as below.

Server (Cisco 2811)

```

Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication Set authentication method for protection suite
  encryption  Set encryption algorithm for protection suite
  exit        Exit from ISAKMP protection suite configuration mode
  group      Set the Diffie-Hellman group
  hash       Set hash algorithm for protection suite
  lifetime   Set lifetime for ISAKMP security association
  no         Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash 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     Get 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 ipsec ? 
  dynamic-map Specify a dynamic crypto map template
  ike       Configure IKE/ISAKMP policy
  isakmp   Configure ISAKMP policy
  key      Long term key operations
  map      Creates 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-IPsec-MD5 transform
  ah-sha-hmac AH-IPsec-SHA transform
  esp-3des ESP transform using 3DES(3DES) cipher (168 bits)
  esp-aes  ESP transform using AES cipher
  esp-3des ESP transform using DES cipher (64 bits)
  esp-md5-hmac ESP transform using HMAC-MD5 auth
  esp-sha-hmac ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
Router(config)#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 10.100.1.1
Router(config-crypto-map)#exit
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.1.1.1 255.255.255.0
Router(config-if)#no
Router(config-if)#crypto map cry-map
*Jan 3 07:14:26.701: %CRYPTO-6-ISAKMP_ON: ISAKMP is ON

```

Client (R3000 LG)

Tunnel

^ Tunnel Settings

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

^ IKE Settings

IKE Type	IKEv1
Negotiation Mode	Main
Authentication Algorithm	MD5
Encryption Algorithm	3DES
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	<input type="text"/>
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	66400

^ SA Settings

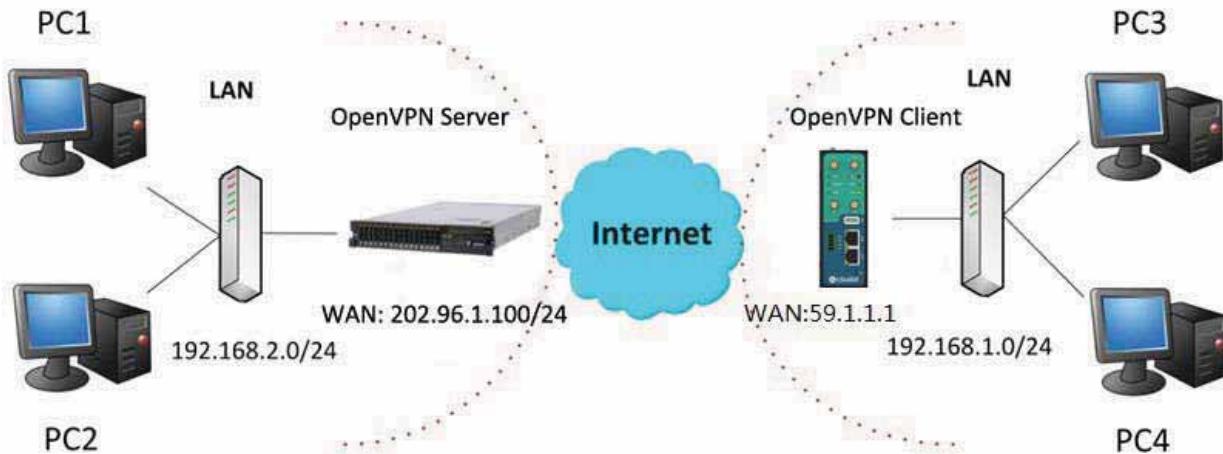
Encrypt Algorithms	3DES
Authentication Algorithms	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

Advanced Settings

Enable Compression	<input type="button"/> OFF
--------------------	----------------------------

4.3.2 OpenVPN

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



OpenVPN_Server:

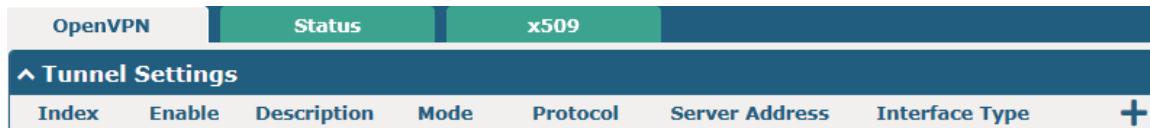
Generate relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configuration the Server:

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

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

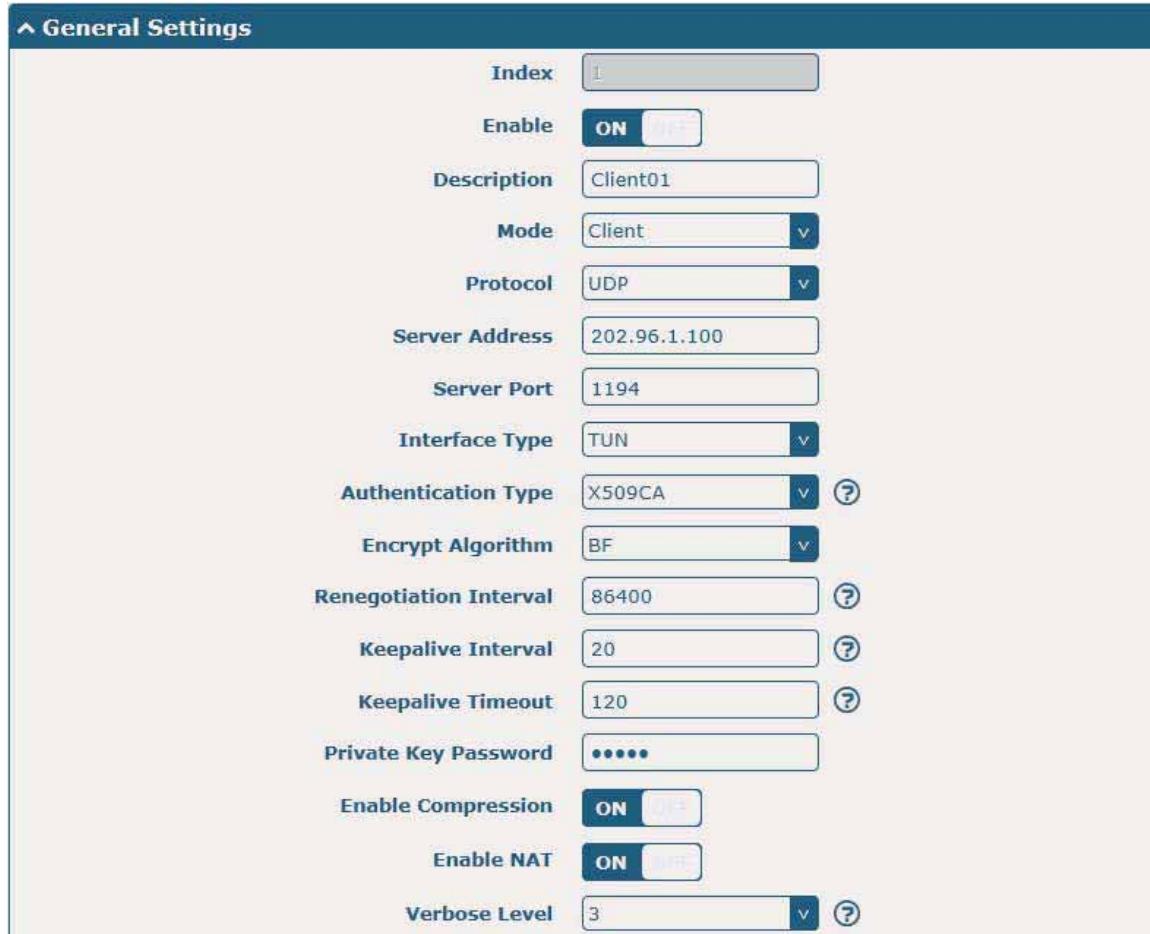
OpenVPN_Client:

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



Index	Enable	Description	Mode	Protocol	Server Address	Interface Type	
▲ Tunnel Settings							

Click  to configure the Client01 as below.



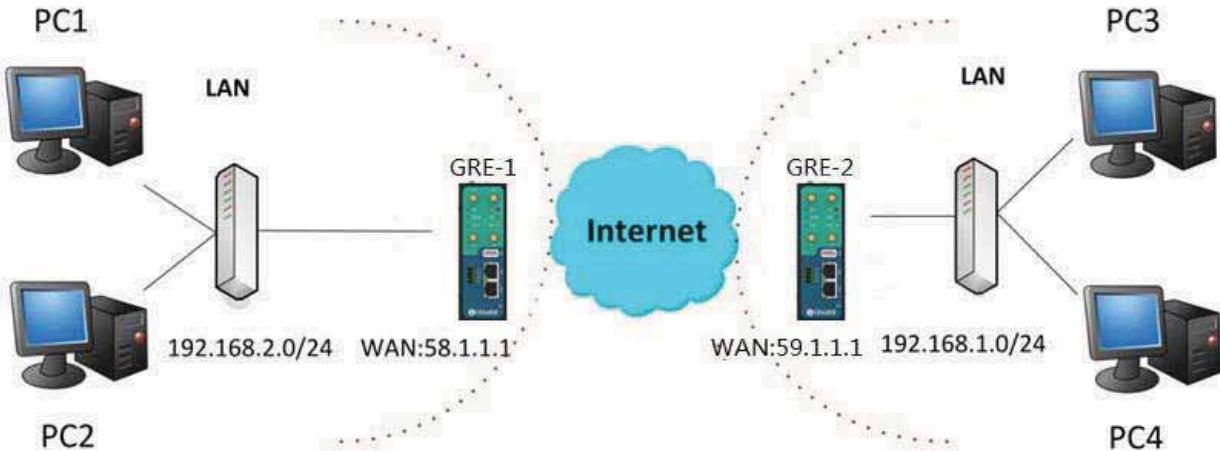
▲ General Settings	
Index	1
Enable	ON 
Description	Client01
Mode	Client 
Protocol	UDP 
Server Address	202.96.1.100
Server Port	1194
Interface Type	TUN 
Authentication Type	X509CA  
Encrypt Algorithm	BF 
Renegotiation Interval	86400 
Keepalive Interval	20 
Keepalive Timeout	120 
Private Key Password	*****
Enable Compression	ON 
Enable NAT	ON 
Verbose Level	3  



▲ Advanced Settings	
Enable HMAC Firewall	 OFF
Enable PKCS#12	 OFF
Enable nsCertType	 OFF
Expert Options	fragment 1500 

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

4.3.3 GRE VPN



The configuration of two points is as follows.

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

GRE	Status			
▲ Tunnel Settings				
Index	Enable	Description	Remote IP Address	

GRE-1:

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

Tunnel Settings

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

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

GRE-2:

Click  button and set the parameters of GRE-2 as below.

▲ Tunnel Settings

Index	1
Enable	<input checked="" type="button"/> ON <input type="button"/> OFF
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Remote Virtual IP Address	10.8.0.1
Enable Default Route	<input type="button"/> OFF
Enable NAT	<input type="button"/> OFF
Secrets	*****

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

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

GRE-1	GRE-2	
▲ Tunnel Settings	▲ Tunnel Settings	
Index	1	
Enable	<input checked="" type="button"/> ON <input type="button"/> OFF	
Description	GRE-1	
Remote IP Address	59.1.1.1	GRE-1 public IP
Local Virtual IP Address	10.8.0.1	GRE-1 tunnel IP
Remote Virtual IP Address	10.8.0.2	GRE-2 tunnel IP
Enable Default Route	<input type="button"/> OFF	
Enable NAT	<input type="button"/> OFF	set the same secret as GRE-2
Secrets	*****	

Chapter 5 Introductions for CLI

5.1 What Is CLI

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

Route login:

Gateway login: admin

Password: admin

#

CLI commands:

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

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

5.2 How to Configure the CLI

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

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

Quick Start with Configuration Examples

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

Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "1.0.0"
kernel_version = 4.1.0
device_model = R3000 LG
serial_number = 10201711101533
system_uptime = "0 days, 01:39:50"
system_time = "Wed Oct 11 17:20:07 2017"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
    firmware New firmware
# tftpupdate firmware (space+?)
    String Firmware name
# tftpupdate firmware R3000 LG-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware
name
Downloading
```

```
R3000 LG-firmware-s 100% |*****| 5018k 0:00:00 ETA
Flashing
Checking 100%
Decrypting 100%
Flashing 100%
Verifying 100%
Verify Success
upgrade success //update success
# config save_and_apply
OK // save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
# set
at_over_telnet      AT Over Telnet
cellular            Cellular
ddns                Dynamic DNS
ethernet            Ethernet
event               Event Management
firewall            Firewall
gre                 GRE
ipsec               IPsec
lan                 Local Area Network
link_manager        Link Manager
ntp                 NTP
openvpn             OpenVPN
reboot              Automatic Reboot
RobustLink          RobustLink
route               Route
sms                 SMS
snmp               SNMP agent
ssh                 SSH
syslog              Syslog
system              System
user_management     User Management
vrrp                VRRP
web_server          Web Server
# set link_manager
primary_link        Primary Link
backup_link          Backup Link
backup_mode          Backup Mode
emergency_reboot    Emergency Reboot
link                Link Settings
# set link_manager primary_link (space+?)
Enum   Primary Link (wwan1/wwan2/wan)
```

```

# set link_manager primary_link wwan1          //select "wwan1" as primary_link
OK
//setting succeed

# set link_manager link 1
type           Type
desc           Description
connection_type Connection Type
wwan           WWAN Settings
static_addr    Static Address Settings
pppoe          PPPoE Settings
ping           Ping Settings
mtu            MTU
dns1_overrided Overrided Primary DNS
dns2_overrided Overrided Secondary DNS

# set link_manager link 1 type wwan1
OK

# set link_manager link 1 wwan
auto_apn       Automatic APN Selection
apn            APN
username        Username
password        Password
dialup_number   Dialup Number
auth_type       Authentication Type
aggressive_reset Aggressive Reset
switch_by_data_allowance Switch SIM By Data Allowance
data_allowance  Data Allowance
billing_day     Billing Day

# set link_manager link 1 wwan switch_by_data_allowance true
OK

#
# set link_manager link 1 wwan data_allowance 100      //open cellular switch_by_data_traffic
OK
//setting succeed

# set link_manager link 1 wwan billing_day 1          //setting specifies the day of month for billing
OK
// setting succeed

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

```

Example 4: Set 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 = 172.16.7.29
    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	Debug <i>parameters</i>	Turn on or turn off debug function
Show	Show <i>parameters</i>	Show current configuration of each function
Set	Set <i>parameters</i>	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add <i>parameters</i>	

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

Glossary

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

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

Abbr.	Description
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel LTD

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

Tel: 86-20-29019902

Email: info@robustel.com

Web: www.robustel.com