



User Guide

R2010

Industrial Cellular Gateway
2 Eth + 2 SIM



robustOS



About This Document

This document provides hardware and software information of the Robustel R2010 Gateway, including introduction, installation, configuration and operation.

Copyright©2022 Guangzhou Robustel Co., Ltd..

All rights reserved.

Trademarks and Permissions

 &  are trademarks of Guangzhou Robustel Co., Ltd.. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

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

Technical Support

Tel: +86-20-82321505

Email: 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.

Regulatory and Type Approval Information

Table 1: Directives



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

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

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

Document History

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

Date	Firmware Version	Document Version	Descriptions
June 08, 2021		v.1.0.0	<ul style="list-style-type: none">• Initial release
December 25, 2021		v.1.0.1	<ul style="list-style-type: none">• Revised the company name• Revised Regulatory and Type Approval Information• Revised Disclaimer

Contents

Chapter 1	Product Overview.....	9
1.1	Key Features.....	9
1.2	Package Contents.....	9
1.3	Specifications.....	11
1.4	Dimensions.....	12
Chapter 2	Hardware Installation.....	13
2.1	PIN Assignment.....	13
2.2	1 x 3 3.5 mm Serial Port Definition.....	13
2.3	1 x 4 3.5 mm Serial Port Definition.....	13
2.4	LED Indicators.....	14
2.5	Reset Button.....	14
2.6	Ethernet Port.....	15
2.7	Insert or Remove SIM Card.....	15
2.8	Attach External Antenna (SMA Type).....	16
2.9	Mount the Gateway.....	17
2.10	Connect R2010 to a Computer.....	18
2.11	Power Supply.....	18
Chapter 3	Initial Configuration.....	19
3.1	Configure the Computer.....	19
3.2	Factory Default Settings.....	22
3.3	Log in the Gateway.....	22
3.4	Control Panel.....	23
Chapter 4	Gateway Configuration.....	25
4.1	Status.....	25
4.1.1	System Information.....	25
4.1.2	Internet Status.....	26
4.1.3	LAN Status.....	26
4.2	Interface.....	27
4.2.1	Link Manager.....	27
4.2.2	LAN.....	38
4.2.3	Ethernet.....	41
4.2.4	Cellular.....	43
4.2.5	Wi-Fi.....	错误! 未定义书签。
4.2.6	DI/DO.....	56
4.2.7	Serial Port.....	60
4.3	Network.....	64
4.3.1	Route.....	64
4.3.2	Firewall.....	65
4.3.3	IP Passthrough.....	72
4.4	VPN.....	73
4.4.1	IPsec.....	73
4.4.2	WireGuard.....	80
4.4.3	OpenVPN.....	83
4.4.4	GRE.....	96

4.5	Services.....	97
4.5.1	Syslog.....	97
4.5.2	Event.....	98
4.5.3	NTP.....	101
4.5.4	SMS.....	102
4.5.5	Email.....	103
4.5.6	DDNS.....	104
4.5.7	SSH.....	105
4.5.8	Web Server.....	106
4.5.9	Advanced.....	107
4.5.10	Smart Roaming.....	107
4.6	Edge2Cloud.....	111
4.6.1	Edge2Cloud.....	111
4.6.2	E2C Broker.....	112
4.7	System.....	113
4.7.1	Debug.....	113
4.7.2	Update.....	115
4.7.3	App Center.....	115
4.7.4	Tools.....	116
4.7.5	Profile.....	118
4.7.6	User Management.....	119
5	Configuration Examples.....	121
5.1	Cellular.....	121
5.1.1	Cellular Dial-Up.....	121
5.1.2	SMS Remote Control.....	123
5.2	VPN Configuration Examples.....	125
5.2.1	IPsec VPN.....	125
5.2.2	OpenVPN.....	129
5.2.3	GRE VPN.....	131
6	Introductions for CLI.....	133
6.1	What Is CLI.....	133
6.2	How to Configure the CLI.....	134
6.3	Commands Reference.....	135
6.4	Quick Start with Configuration Examples.....	135
	Glossary.....	141

Chapter 1 Product Overview

1.1 Key Features

The Robustel R2010 Industrial Dual SIM Cellular Gateway is a rugged, versatile 4G gateway with dual Ethernet ports, dual SIM single standby capability and a range of advanced functions for mission critical IoT or M2M applications.

The R2010 runs on Robustel's own Linux based Operating System, RobustOS. Developed entirely in-house, this gives way to a very high standard of technical support and high reliability. Robustel offers a Software Development Kit (SDK) to allow additional customization by using C, C++. It also provides rich Apps to meet fragmented IoT market demands.

1.2 Package Contents

Before installing your R2010 Gateway, verify the kit contents as following.

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

- 1 x Robustel R2010 Industrial Cellular Gateway



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



- 1 x 3-pin 3.5 mm male terminal block for RS232/RS485



- 1 x 4-pin 3.5 mm male terminal block for DIDO



- 2 x SMA-J cellular antenna (external)



- 2 x RP-SM-J Wi-Fi antenna (external)



Optional Accessories (sold separately)

- Ethernet cable



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



- DIN rail mounting kit



1.3 Specifications

Cellular Interface

- Number of antennas: 2 (MAIN + AUX) or 1 (MAIN)
- Connector: SMA-K, standard
- SIM: 2 (3.0 V & 1.8 V), standard

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

Wi-Fi Interface

- Number of antennas: 2 (Wi-Fi1 + Wi-Fi2)
- Connector: RP-SMA-K
- Standards: 802.11 b/g/n, 2 x 2 MIMO, supporting AP and Client modes
- Frequency bands: 2.4 GHz
- Security: WEP, WPA, WPA2
- Encryption: 68/128 AES, TKIP
- Data speed: 300 Mbps

Serial Interface

- Number of ports: 1 x RS485/RS232 (software configurable)
- Connector: 3-pin 3.5 mm female socket

DI/DO

- Number of ports: 1 x DI (wet contact), 1 x DO (wet contact)
- Connector: 1 x 4-pin 3.5 mm female connector
- Isolation: 3 KV DC
- Absolute maximum VDC: "V+" + 30 V DC (DI), 30V DC (DO)
- Maximum DI input current: 10 mA
- Maximum DO load current: 50 mA

Others

- 1 x RST button
- LED indicators: 1 x RUN, 1 x MDM, 1 x Wi-Fi, 3 x RSSI
- Built-in: Watchdog, Timer

Power Supply and Consumption

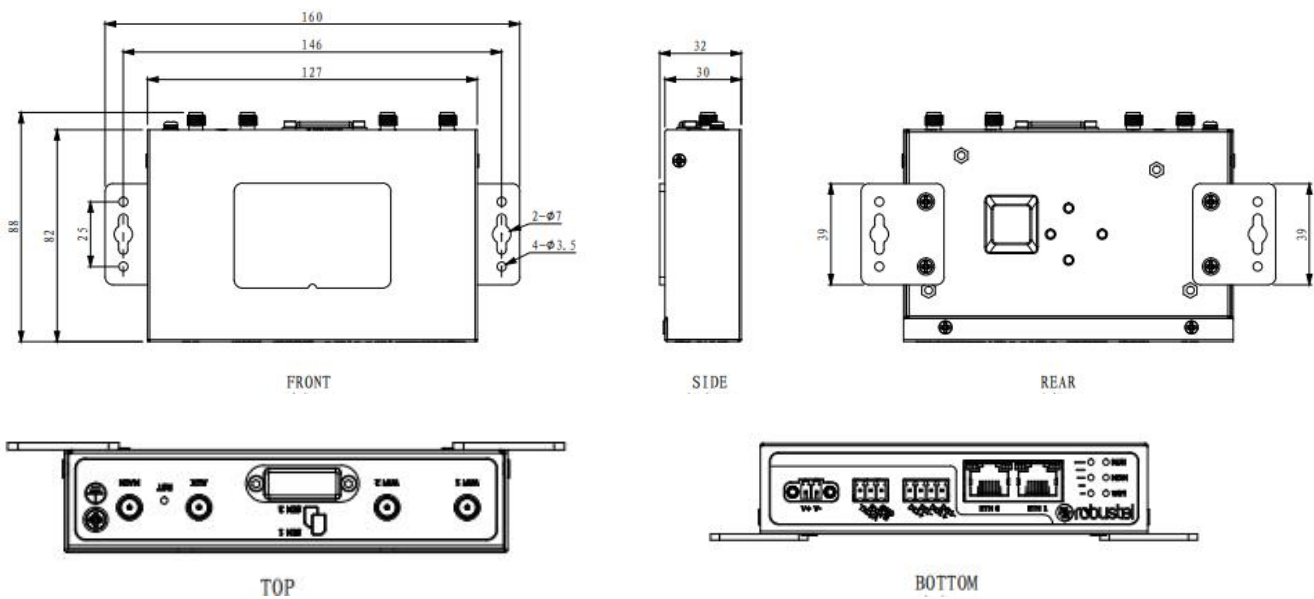
- Connector: 2-pin 3.5 mm female socket
- Input voltage: 9 to 36 V DC
- Power consumption: Idle: 200 mA@12 V
Data link: 580 mA (peak) @12 V

Physical Characteristics

- Ingress protection: IP30

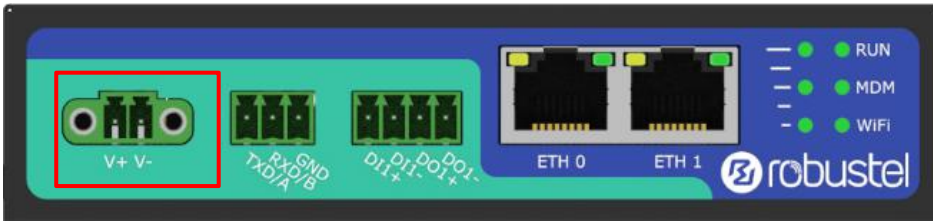
- Housing & Weight: Metal, 350 g
- Dimensions: 127 x 82 x 30 mm
- Installations: Desktop, wall mounting and DIN rail mounting (wall mounting kit and DIN rail mounting kit requires additional purchase.)
- Operation temperature: $-40\sim+75\text{ }^{\circ}\text{C}$
- Storage temperature: $-40\sim+85\text{ }^{\circ}\text{C}$
- Relative humidity: $5\sim95\% \text{ RH}$

1.4 Dimensions



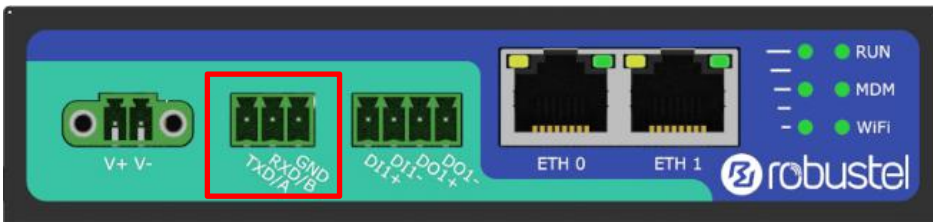
Chapter 2 Hardware Installation

2.1 PIN Assignment



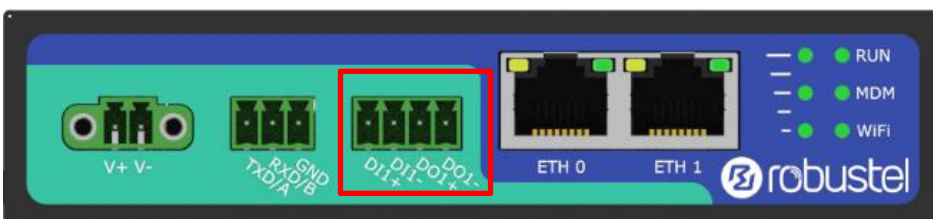
PIN	Descriptions	Notes
1	V+	Positive
2	V-	Negative

2.2 1 x 3 3.5 mm Serial Port Definition



PIN	Descriptions	Notes
1	TXD/A	RS232 data sending/RS485_A. See software configuration mode for specific definitions
2	RXD/B	RS232 data receiving/RS485_B. See software configuration mode for specific definitions
3	GND	Ground

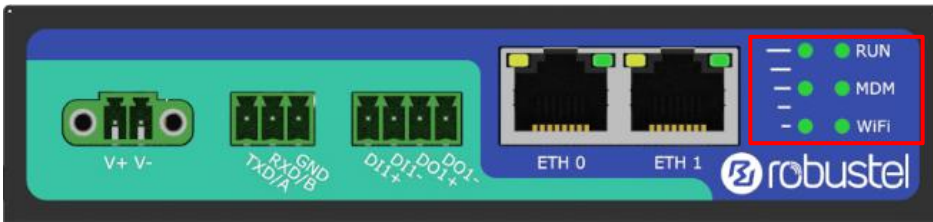
2.3 1 x 4 3.5 mm Serial Port Definition



PIN	Descriptions	Notes
1	DI1+	DI Positive
2	DI1-	DI Negative
3	DO1+	DO Positive
4	DO1-	DI Negative

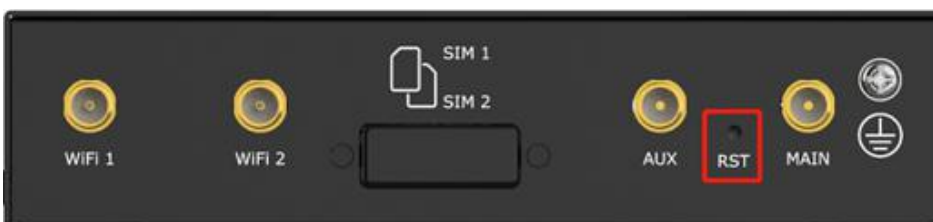
2.4 LED Indicators

The R2010 Gateway has been designed to be placed on a desktop. Below is the bottom view of the R2010.



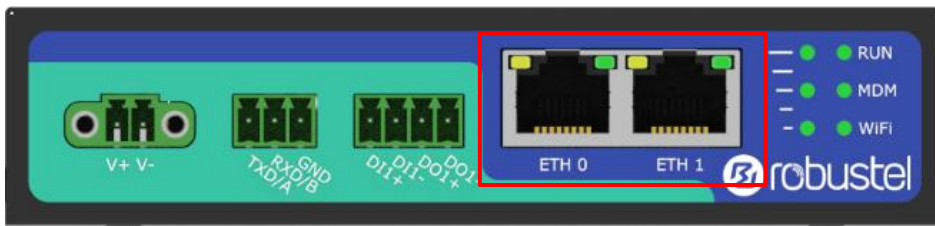
Name	Color	Status	Description
RUN	Green	On, solid	Gateway is powered on (System is initializing)
		On, blinking	Gateway starts operating
		Off	Gateway is powered off
MDM	Green	On, solid	Successful link connection
		On, blinking	Link connection is working
		Off	Link connection is not working
Wi-Fi	Green	On, solid	Backup card is being used
		Off	Main card is being used
RSSI	Green	Three lights on	Cellular module: high signal (20~31 dB)
		Two lights on	Cellular module: medium signal (10~19 dB)
		One light on	Cellular module: low signal (1~9 dB)
		Off	Module initializing or no signal

2.5 Reset Button



Function	Operation
Reboot	Press and hold the RST button for 2 to 7 seconds under the operating status.
Restore to factory default settings	Wait for 0~20 seconds after powering up the gateway, press and hold the RST button until all LEDs start blinking one by one, and release the button to return the gateway to factory defaults.

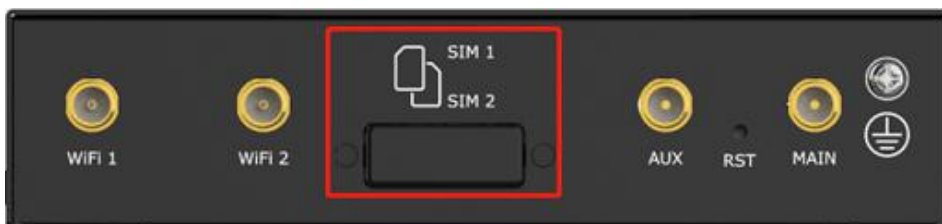
2.6 Ethernet Port

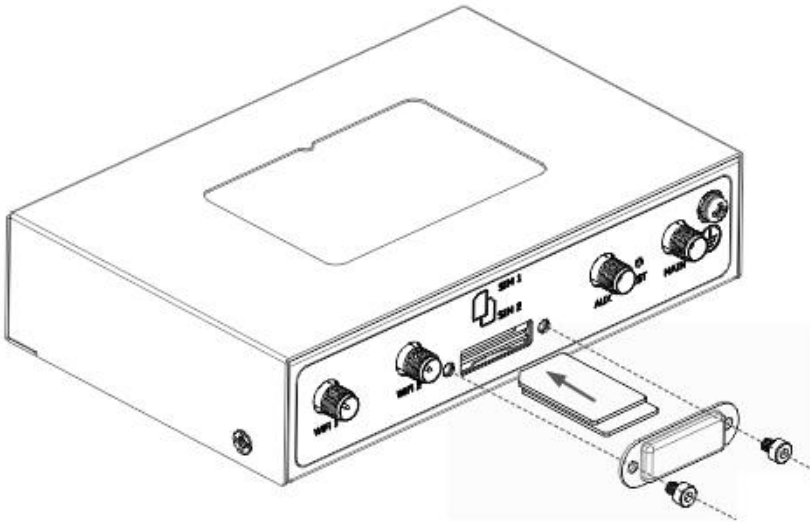


There are two Ethernet ports on R2010 Gateway, including ETH0 (WAN/LAN) and ETH1. Each has two LED indicators. The green one is a link indicator but the yellow one doesn't mean anything. For details about status, see the table below.

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

2.7 Insert or Remove SIM Card





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

- **Insert SIM card**

1. Make sure the 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.
3. To insert SIM card, press the card with finger until you hear a click and then tighten the screws associated with the cover by using a screwdriver.
4. To put back the cover and tighten the screws associated with the cover by using a screwdriver.

- **Remove SIM card**

1. Make sure the 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.
3. To remove SIM 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. Use the specific M2M SIM 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.
2. Do not touch the metal of the card surface in case information in the card will lose or be destroyed.
3. Do not bend or scratch the card.
4. Keep the card away from electricity and magnetism.
5. Make sure gateway is powered off before inserting or removing the card.

2.8 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.



RP-SMA-K for Wi-Fi connection

SMA-K for cellular connection

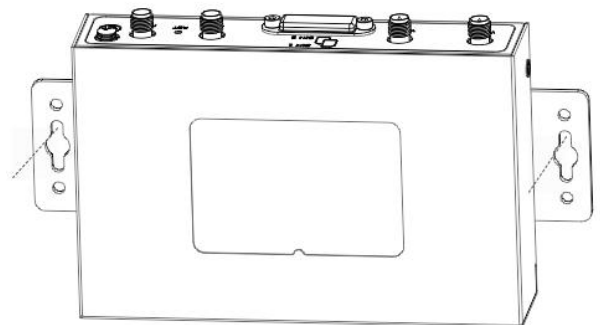
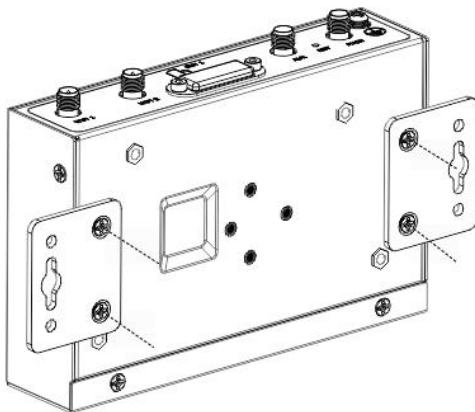


2.9 Mount the Gateway

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

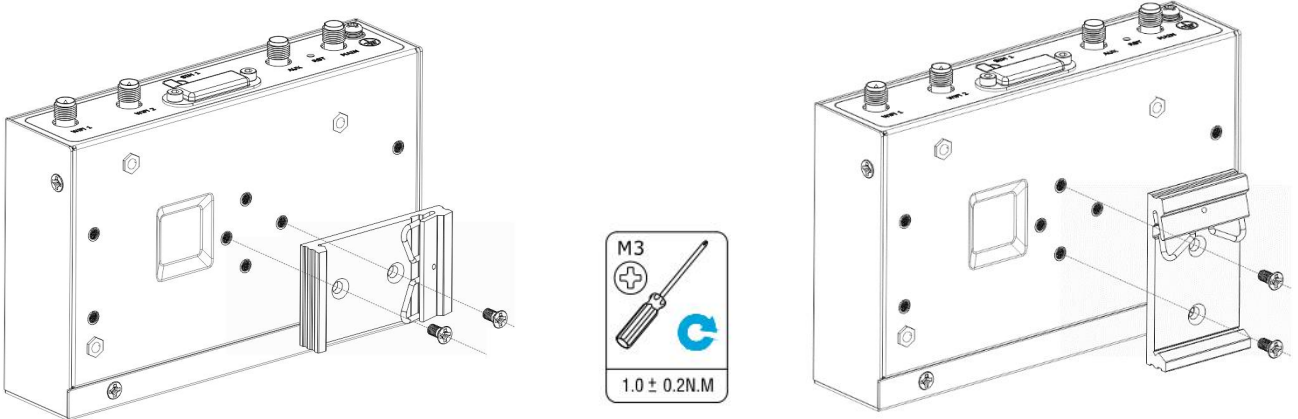
Two methods for mounting the gateway

- Wall mounting (measured in mm)



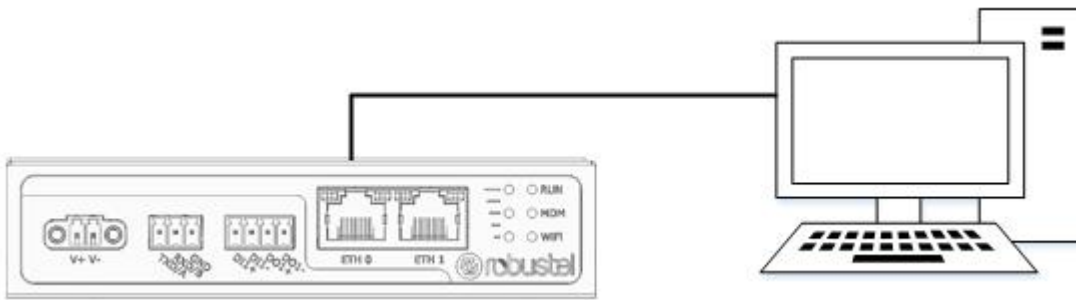
Use 4 pcs of M3 screws to fix the wall mounting kit to the gateway, and then use 2 pcs of M3 drywall screws to mount the gateway associated with the wall mounting kit on the wall.

- DIN rail mounting (measured in mm)



Use 3 pcs of M3 screws to fix the DIN rail to the gateway (as illustrations above shown, there are two mounting angles to choose from), and then hang the DIN rail on the mounting bracket.

2.10 Connect R2010 to a Computer

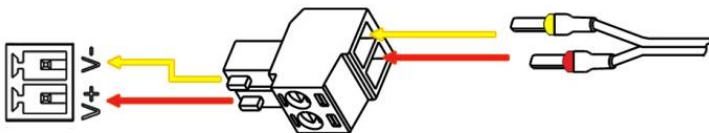


Connect the gateway's Ethernet port (ETH0~ETH1) to a PC with a standard Ethernet cable.

2.11 Power Supply

Power wiring diagram

Color	Descriptions
Red	+ Positive
Yellow	- Negative



The R2010 supports reverse polarity protection, but always refers to the illustration above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way. The last step is to plug the power adapter into your socket.

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

Chapter 3 Initial Configuration

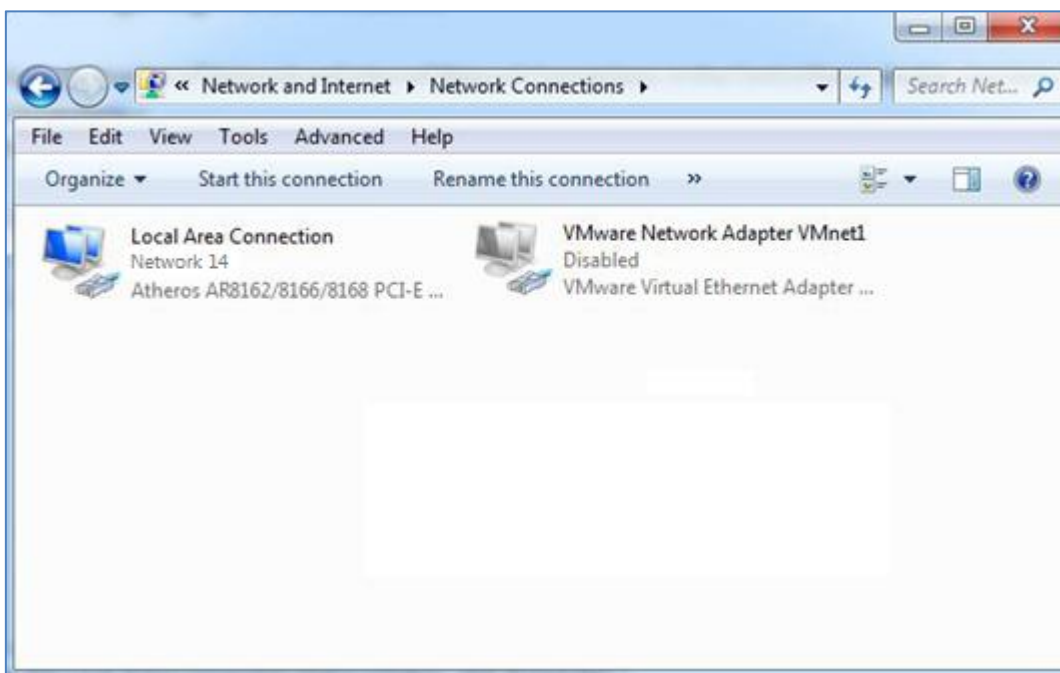
The gateway can be configured through your web browser that including IE 8.0 or above, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface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

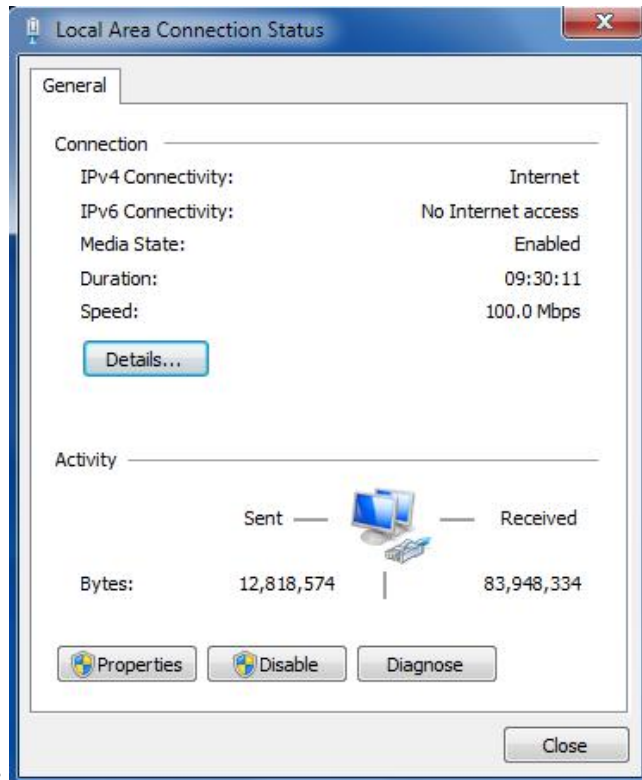
There are two methods to get IP address for the computer. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the gateway. Please refer to the steps below.

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**.

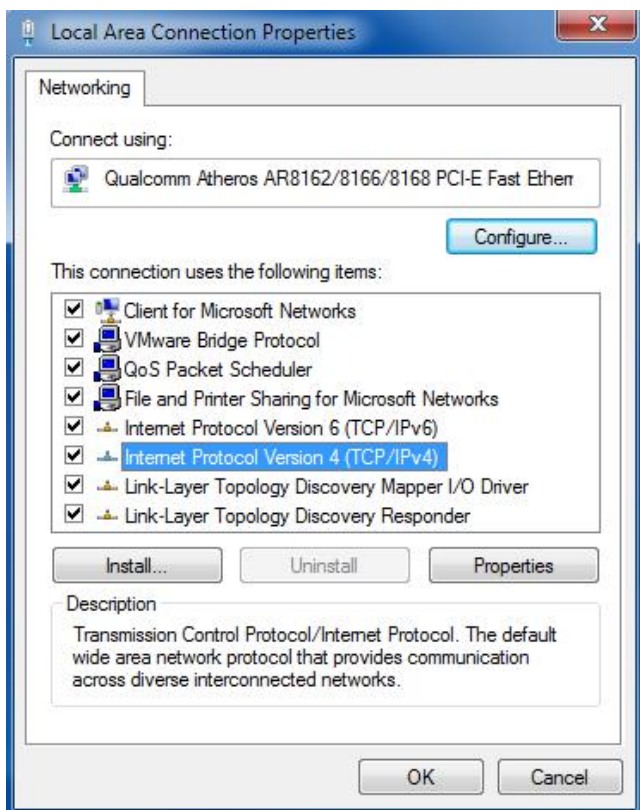


2. Click **Properties** in the window of **Local Area Connection**



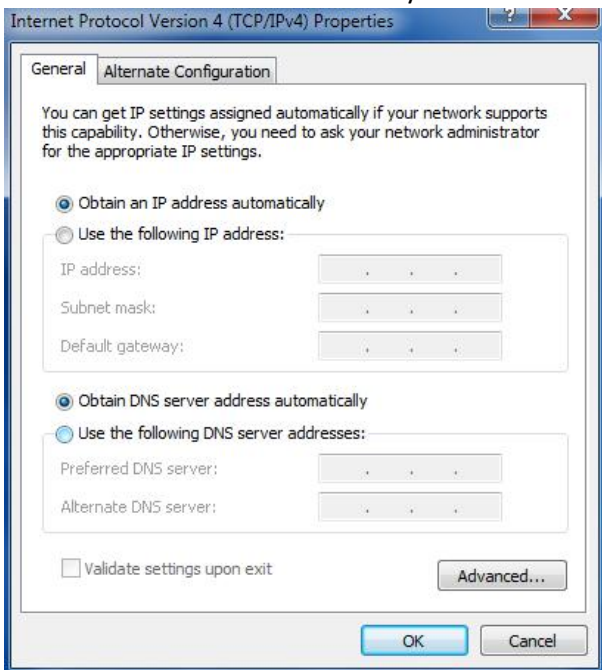
Status.

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

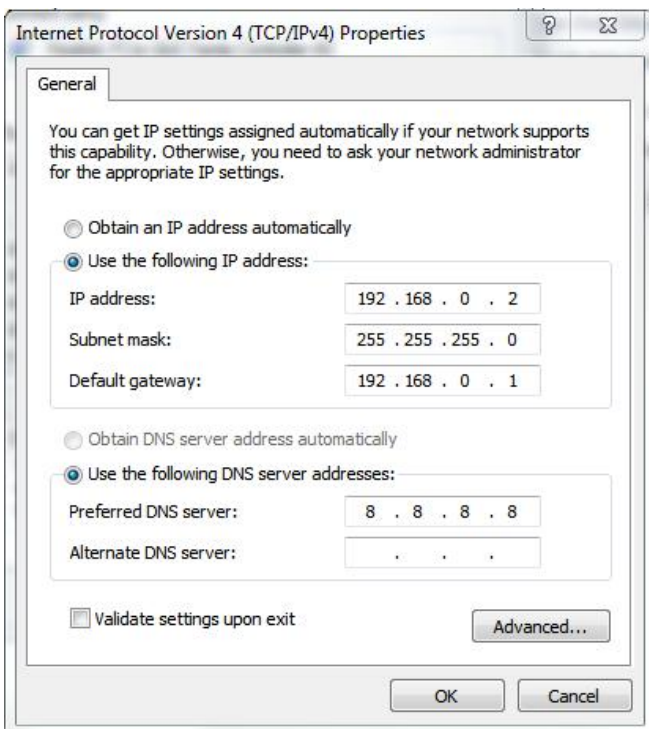


4. Two ways for configuring the IP address of computer.

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



Manually configure the PC with a static IP address on the same subnet as the gateway address, click and configure "**Use the following IP address**";



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

3.2 Factory Default Settings

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

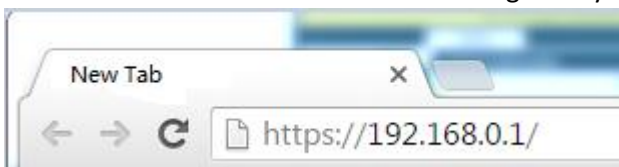
Item	Description
Username	admin
Password	admin
ETH0	WAN mode or 192.168.0.1/255.255.255.0, LAN mode
ETH1	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

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.

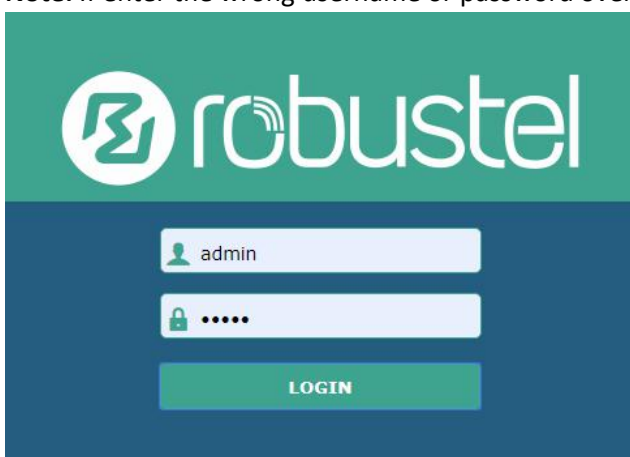
1. On your PC, open a web browser such as Internet Explorer, Google or Firefox, etc.
2. From your web browser, type the IP address of the gateway into the address bar and press enter. The default IP address of the gateway is <http://192.168.0.1/>, though the actual address may vary.

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 6 times, the login web will be locked for 5 minutes.



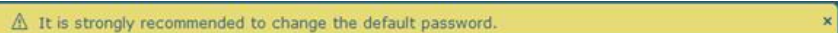
3.4 Control Panel

After logging in, the home page of the R2010 Gateway's web interface is displayed, for example.









From the homepage, users can perform operations such as saving the configuration, restarting the gateway, and logging out.

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






It is strongly recommended for security purposes that you change the default username and/or password. Click the

 button to close the popup. To change your username and/or password, see **4.6.6 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.	
Reboot	Click to reboot the gateway. If the Reboot button is yellow, it means that some completed configurations will take effect only after reboot.	
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	
Submit	Click to save the modification on current configuration page.	
Cancel	Click to cancel the modification on current configuration page.	

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

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

Chapter 4 Gateway Configuration

4.1 Status

4.1.1 System Information

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

^ System Information	
Device Model	R2010
System Uptime	0 days, 06:17:32
System Time	Wed Apr 14 18:00:32 2021 (NTP not updated)
RAM Usage	17M Free/64M Total
Firmware Version	3.0.0
Hardware Version	1.0
Kernel Version	3.10.49
Serial Number	111111111

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.

4.1.2 Internet Status

This page shows the gateway's Internet status information.

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

Internet Status	
Item	Description
Uptime	Show the current amount of time the link has been connected.
Active Link	Show the currently online link: WWAN1, WWAN2, or WAN.
IP Address	Show the address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current DNS server.

4.1.3 LAN Status

This page shows the gateways' LAN status

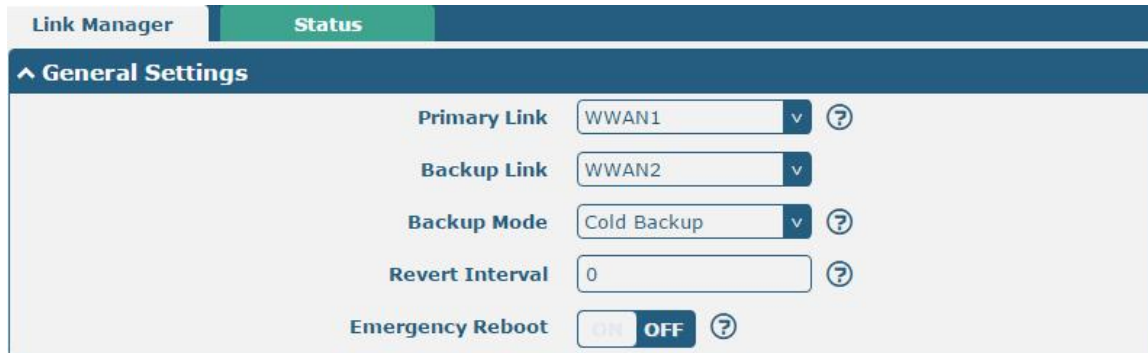
^ LAN Status	
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:0A:A4:2A

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

4.2 Interface

4.2.1 Link Manager

Users can manage link connections in this section. Link Manager is a link backup feature that provides mobile network and Ethernet link backup.



The screenshot shows the 'Link Manager' interface with a 'Status' tab selected. Under 'General Settings', the following options are visible:

- Primary Link:** WWAN1 (dropdown menu with a help icon)
- Backup Link:** WWAN2 (dropdown menu with a help icon)
- Backup Mode:** Cold Backup (dropdown menu with a help icon)
- Revert Interval:** 0 (input field with a help icon)
- Emergency Reboot:** OFF (toggle button with a help icon)

General Settings @ Link Manager		
Item	Description	Default
Primary Link	Select from "WWAN1", "WWAN2", "WAN" or "WLAN". <ul style="list-style-type: none"> WWAN1: Select to make SIM1 as the primary wireless link WWAN2: Select to make SIM2 as the primary wireless link WAN: Select to make WAN Ethernet port as the primary wired link WLAN: Select to make WLAN as the primary wireless link Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer to 4.2.5 Wi-Fi .	WWAN1
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN" 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 Ethernet port as the primary wired link WLAN: Select to make WLAN as the primary wireless link Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer to 4.2.5 Wi-Fi . <ul style="list-style-type: none"> None: Do not select any backup link 	None
Backup Mode	Select from "Cold Backup", "Warm Backup" or "Load Balancing". <ul style="list-style-type: none"> Cold Backup: The inactive link is offline on standby Warm Backup: The inactive link is online on standby Load Balancing: Use two links simultaneously 	Cold Backup
Revert Interval	Specify the number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. Note: Revert interval is available only under the cold backup mode.	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links available.	OFF

Note: Click  for help.

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

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

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

WWAN1/WWAN2

Link Manager

^ **General Settings**

Index:

Type:

Description:

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

^ **WWAN Settings**

Automatic APN Selection ON OFF

Dialup Number:

Authentication Type:

Switch SIM By Data Allowance: ON OFF ?

Data Allowance: ?

Billing Day: ?

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

^ WWAN Settings

Automatic APN Selection ON OFF

APN

Username

Password

Dialup Number

Authentication Type

PPP Preferred ON OFF ?

Switch SIM By Data Allowance ON OFF ?

Data Allowance ?

Billing Day ?

^ Ping Detection Settings
?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

Upload Bandwidth ?

Download Bandwidth

Overrided Primary DNS

Overrided Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF

Link Settings (WWAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WWAN1
Description	Enter a description for this link.	Null

Link Settings (WWAN)		
Item	Description	Default
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
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit reached. Note: Only used for dual-SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in Interface > Link Manager > Status > WWAN Data Usage Statistics . 0 means disable data traffic record.	0
Billing Day	Specify the monthly billing day. The data traffic statistics will be recalculated from that day.	1
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the gateway.	ON
Primary Server	Gateway will ping this primary address/domain name to check that if the current IPv4 connectivity is active.	8.8.8.8
Secondary Server	Gateway will ping this secondary address/domain name to check that if the current IPv4 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
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server used by the link.	Null

Link Settings (WWAN)		
Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WAN

Gateway will obtain IP automatically from DHCP server if choosing "DHCP".

Link Manager

^ **General Settings**

Index

Type

Description

Connection Type

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

^ **General Settings**

Index

Type

Description

Connection Type

^ **Static Address Settings**

IP Address ?

Gateway

Primary DNS

Secondary DNS

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

^ General Settings

Index

Type

Description

Connection Type

^ WAN Settings

Data Allowance ?

Billing Day ?

^ PPPoE Settings

Username

Password

Authentication Type

PPP Expert Options ?

^ Ping Detection Settings

 ?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

MTU

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF

Link Settings (WAN)		
Item	Description	Default
General Settings		
Index	Indicate the ordinal of the list.	--
Type	Show the type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from "DHCP", "Static" or "PPPoE".	DHCP
Static Address Settings		
IP Address	Set the IP address with Netmask which can access the Internet. IP address with Netmask, e.g. 192.168.1.1/24	Null
Gateway	Set the gateway of the IP address in WAN port.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
PPPoE Settings		
Username	Enter the username provided by your Internet Service Provider.	Null
Password	Enter the password provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP required.	Auto
PPP Expert Options	Enter the PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
WAN Settings		
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in Interface > Link Manager > Status > WWAN Data Usage Statistics . 0 means disable data traffic record.	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
MTU	Enter the Maximum Transmission Unit.	1500

Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary IPv4 DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary IPv4 DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

WLAN

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

Link Manager

^ **General Settings**

Index

Type v

Description

Connection Type v

^ **WLAN Settings**

SSID

Connect to Hidden SSID ON OFF

Password

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

^ **General Settings**

Index

Type v

Description

Connection Type v

v **WLAN Settings**

^ **Static Address Settings**

IP Address ?

Gateway

Primary DNS

Secondary DNS

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

^ PPPoE Settings

Username

Password

Authentication Type Auto v

PPP Expert Options ?

^ Ping Detection Settings
?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

MTU

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

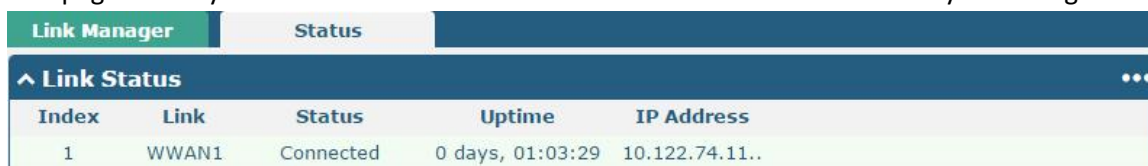
Verbose Debug Enable ON OFF

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


	wants to connect.	
Static Address Settings		
IP Address	Enter the IP address with Netmask which can access the Internet, e.g. 192.168.1.1/24	Null
Gateway	Enter the IP address of Wi-Fi AP.	Null
Primary DNS	Set the primary DNS.	Null
Secondary DNS	Set the secondary DNS.	Null
Ping Detection Settings		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the 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.	114.114.1 14.114
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
Advance Settings		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter the Maximum Transmission Unit.	1500
Upload Bandwidth	Enter the upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter the download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Defines the primary DNS server used by the link.	Null
Specify Secondary DNS	Defines the secondary DNS server for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF

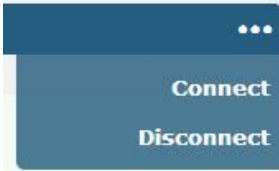
Status

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



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

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



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

Link Manager
Status

^ Link Status
...

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

Index 1

Link WWAN1

Status Connected

Interface wwan

Uptime 0 days, 01:03:29

IP Address 10.122.74.11/255.255.255.248

Gateway 10.122.74.9

DNS 210.21.4.130 221.5.88.88

RX Packets 42

TX Packets 46

RX Bytes 2962

TX Bytes 3568

^ WWAN Data Usage Statistics
?

WWAN1 Monthly Stats Clear

WWAN2 Monthly Stats Clear

Click the **Clear** button to clear SIM1 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**.

^ WAN Data Usage Statistics
?

WAN Monthly Stats Clear

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

4.2.2 LAN

This section allows you to set the related parameters for LAN port. There are two LAN ports on R2010 Gateway, 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

LAN	Multiple IP	Status			
^ Network Settings ?					
Index	Interface	IPv4 Address	Netmask	VLAN ID	
1	lan0	192.168.0.1	255.255.255.0	0	+ ✕

Note: Lan0 cannot be deleted.

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

LAN	
^ General Settings	
Index	<input type="text" value="1"/>
Interface	<input type="text" value="lan0"/> v
IPv4 Address	<input type="text" value="192.168.0.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
MTU	<input type="text" value="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 .	--
IPv4 Address	Set the IP address of the LAN port.	192.168.0.1
Netmask	Set the Netmask of the LAN port.	255.255.255.0
MTU	Enter the Maximum Transmission Unit.	1500

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

^ DHCP Settings

Enable ON OFF

Mode Server v

IP Pool Start

IP Pool End

Subnet Mask

^ DHCP Advanced Settings

Gateway

Primary DNS

Secondary DNS

WINS Server

Lease Time ?

Static Lease ?

Expert Options ?

Debug Enable ON OFF

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

^ DHCP Settings

Enable ON OFF

Mode Relay v

DHCP Server For Relay

^ DHCP Advanced Settings

Debug Enable ON OFF

LAN		
Item	Description	Default
DHCP Settings		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. <ul style="list-style-type: none"> Server: Lease IP address to DHCP clients which have been connected to LAN port Relay: 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
IPv4 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
IPv4 Pool End	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of DHCP relay server.	Null
DHCP Advanced Settings		
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	Status
^ Multiple IP Settings		
Index	Interface	IP Address
		Netmask
+		

You may click **+** to add a multiple IP to the LAN port, or click **X** to delete the multiple IP of the LAN port. Now, click **✎** 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"/> v
IP Address	<input type="text"/>
Netmask	<input type="text"/>

IP Settings		
Item	Description	Default
Index	Display the index 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

Status

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

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

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

^ Interface Status																			
Index	Interface	IP Address	MAC Address																
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:68:AC																
<table border="1"> <tbody> <tr> <td>Index</td> <td>1</td> </tr> <tr> <td>Interface</td> <td>lan0</td> </tr> <tr> <td>IP Address</td> <td>192.168.0.1/255.255.255.0</td> </tr> <tr> <td>MAC Address</td> <td>34:FA:40:0B:68:AC</td> </tr> <tr> <td>RX Packets</td> <td>14470</td> </tr> <tr> <td>TX Packets</td> <td>12759</td> </tr> <tr> <td>RX Bytes</td> <td>2849614</td> </tr> <tr> <td>TX Bytes</td> <td>10657230</td> </tr> </tbody> </table>				Index	1	Interface	lan0	IP Address	192.168.0.1/255.255.255.0	MAC Address	34:FA:40:0B:68:AC	RX Packets	14470	TX Packets	12759	RX Bytes	2849614	TX Bytes	10657230
Index	1																		
Interface	lan0																		
IP Address	192.168.0.1/255.255.255.0																		
MAC Address	34:FA:40:0B:68:AC																		
RX Packets	14470																		
TX Packets	12759																		
RX Bytes	2849614																		
TX Bytes	10657230																		

4.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There are two Ethernet ports on R2010 Gateway, including ETH0 and ETH1. The ETH0 on the gateway can be configured as either a WAN port or LAN port, also can be assigned as a PoE port, while ETH1 can only be configured as a LAN port. The default settings of ETH0 and ETH1 are lan0 and their default IP are 192.168.0.1/255.255.255.0.

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

Click button of eth0 to configure its parameters, and modify the port assignment parameters of eth0 in the pop-up window.

Ports

^ Port Settings

Index:

Port:

Port Assignment: ?

Port Enable: ON OFF ?

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 LAN port. When setting the port as a LAN port, you can click the drop-down list to select from "lan0" or "lan1".	lan0
Port Enable	eth0: When the WAN switch to LAN, this function needs to reboot to take effect. eth1: Enable or disable the port	true

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

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

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	Down
2	eth1	Up

Index 2

Port eth1

Link Up

4.2.4 Cellular

This section allows you to set the related parameters of Cellular. The R2010 has 2 SIM card slots.

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 on the right-most of SIM 1 to edit the parameters.

Cellular

^ General Settings

Index

SIM Card v

Phone Number

PIN Code ?

Extra AT Cmd ?

Telnet Port ?

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

^ Cellular Network Settings

Network Type v ?

Band Select Type v ?

^ Advanced Settings

Debug Enable ON OFF

Verbose Debug Enable ON OFF

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

^ Cellular Network Settings

Network Type v ?

Band Select Type v ?

^ Band Settings

GSM 900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 1800	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 1	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 3	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 5	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 8	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 34 (TDD)	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 38 (TDD)	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 39 (TDD)	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 40 (TDD)	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 41 (TDD)	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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
Timeout For Network Registration	<input type="text" value="0"/> ?

Submit
Close

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 the cellular network type, which is the network access order. 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

Cellular		
Item	Description	Default
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
Timeout For Network Registration	The timeout required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0

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	EC200T	460092070110283	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	EC200T	460019372994937	Registered to home network
Index 1				
Modem Status Ready				
Modem Model EC200T				
Current SIM SIM1				
Phone Number				
IMSI 460019372994937				
ICCID 89860118801079009362				
Registration Registered to home network				
Network Provider CHN-UNICOM				
Network Type LTE				
Band 3				
Signal Strength 19 (-75dBm)				
RSRP -107 dBm				
RSRQ -7 dB				
SINR 21 dB				
Bit Error Rate 99				
PLMN ID 46001				
Local Area Code 2507				
Cell ID 6074702				
IMEI 862107045897238				
Firmware Version EC200TCNHAR03A01M16__BETA_30694_0202				

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 > 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.

Status	
Item	Description
RSRP	Show the current RSRP when you register to the 4G network.
RSRQ	Show the current RSRQ when you register to the 4G network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the 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.

Cellular
Status
AT Debug

^ AT Debug

Command

Result

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
<input type="button" value="Send"/>	Click the button to send AT command.	--

4.2.5 Wi-Fi

This section allows you to configure the parameters of two Wi-Fi modes. Gateway supports both Wi-Fi AP or Client modes, and default as AP.

Wi-Fi AP

Configure Gateway as Wi-Fi AP

Click **Interface > Wi-Fi > Wi-Fi**, select **AP** as the mode and click **Submit**.

WiFi
Access Point
Advanced
ACL
Status

^ General Settings

Mode

Region

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

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



The screenshot shows the 'General Settings' section of the WiFi configuration page. The 'Security Mode' dropdown menu is highlighted with a red box and is currently set to 'Disabled'. Other settings include 'Enable' (OFF), 'Wireless Mode' (11bgn Mixed), 'Channel' (Auto), 'SSID' (router), and 'Broadcast SSID' (ON).

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

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



The screenshot shows the 'General Settings' section of the WiFi configuration page. The 'Security Mode' dropdown menu is highlighted with a red box and is now set to 'WPA-Personal'. Additional settings are visible, including 'WPA Version' (Auto), 'Encryption' (Auto), 'PSK Password', and 'Group Key Update Interval' (3600).

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

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

^ General Settings

Enable ON OFF

Wireless Mode

Channel ?

SSID

Broadcast SSID ON OFF

Security Mode ?

WPA Version

Encryption ?

Radius Authentication Server Address

Radius Authentication Server Port

Radius Server Share Secret

Group Key Update Interval

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

^ General Settings

Enable ON OFF

Wireless Mode

Channel ?

SSID

Broadcast SSID ON OFF

Security Mode ?

WEP Key ?

General Settings @ Access Point		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b Only”, “11g Only” or “11n Only”. <ul style="list-style-type: none"> 11bgn Mixed: Mix three agreements, for backward compatibility 11b only: IEEE 802.11b, 11Mbit/s~2.4GHz 11g only: IEEE 802.11g, 54Mbit/s~2.4GHz 11n only: IEEE 802.11n, 300Mbps~600Mbps 	11bgn Mixed

General Settings @ Access Point		
Item	Description	Default
Channel	<p>Select the frequency channel, including “Auto”, “1”, “2” “13”.</p> <ul style="list-style-type: none"> Auto: Gateway will scan all frequency channels until the best one is found 1~13 Gateway will be fixed to work with this channel Following are the frequency of 1~13 channel: 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz 	Auto
SSID	Enter the Service Set Identifier, the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	gateway
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the gateway AP, you need to manually enter the SSID of gateway AP at Wi-Fi client side.	ON
Security Mode	<p>Select from “Disabled”, “WPA-Personal”, “WPA-Enterprise” or “WEP”.</p> <ul style="list-style-type: none"> Disabled: User can access the Wi-Fi without password Note: It is strongly recommended for security purposes that you do not choose this kind of mode. WPA-Personal: Wi-Fi Protected Access only provides one password used for Identity Authentication WPA-Enterprise: Provides an authentication interface for EAP which can be authenticated via Radius Authentication Server or other Extended Authentication WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission 	Disabled
WPA Version	<p>Select from “Auto”, “WPA” or “WPA2”.</p> <ul style="list-style-type: none"> Auto: Gateway will choose automatically the most suitable WPA version WPA2 is a stronger security feature than WPA 	Auto

General Settings @ Access Point		
Item	Description	Default
Encryption	<p>Select from “Auto”, “TKIP” or “AES”.</p> <ul style="list-style-type: none"> Auto: Gateway will choose automatically the most suitable encryption TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication Note: It's not recommended to use TKIP encryption in 802.11n mode. AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP 	Auto
PSK Password	Enter the Pre share key password. When gateway works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the interval of group key update.	3600
Radius Authentication Server Address	Enter the address of radius authentication server.	Null
Radius Authentication Server Port	Enter the port of radius authentication server.	1812
Radius Server Share Secret	Enter the shared secret of radius authentication server.	Null
WEP Key	Enter the WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

^ Advanced Settings

Max Associated Stations

Beacon Interval ?

DTIM Period ?

RTS Threshold ?

Fragmentation Threshold ?

Transmit Rate v

11N Transmit Rate v

Transmit Power v

Channel Width v ?

Enable Short GI ON OFF ?

Enable AP Isolation ON OFF ?

Debug Level v

Advanced Settings		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the gateway's AP.	64
Beacon Interval	Set the interval of time in which the gateway AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set the delivery traffic indication message period and the gateway AP will multicast the data according to this period.	2
RTS/CTS Threshold	Set the "request to send" threshold. When the threshold set as 2347, the gateway AP will not send detection signal before sending data. And when the threshold set as 0, the gateway AP will send detection signal before sending data.	2347
Fragmentation Threshold	Set the fragmentation threshold of a Wi-Fi AP. It is recommended that you use the default value 2346.	2346
Transmit Rate	Set the transmit rate. You can choose Auto or specify a Transmit Rate, including 1Mbps, 2Mbps, 5.5Mbps, 6Mbps, 11Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, and 54Mbps, MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6 and MCS7.	Auto
11N Transmit Rate	Specify the transmit rate under the IEEE 802.11n mode or let is default to "Auto".	Auto
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Channel Width	Select from "Auto", "20MHz" or "40MHz". Note: 40 MHz channel width provides higher available data rate, twice as many as 20 MHz channel width.	Auto
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option.	OFF

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

WiFi
Access Point
Advanced
ACL
Status

^ General Settings

Enable ACL OFF

ACL Mode v ?

^ Access Control List

Index	Description	MAC Address
+		

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

ACL

^ Access Control List

Index

Description

MAC Address

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

This section allows you to view the status of AP.

WiFi	Access Point	Advanced	ACL	Status	
^ AP Status					
Status		FAILED			
Channel		6			
Channel Width		20 MHz			
MAC Address		34:FA:40:01:DE:02			
^ Associated Stations					
Index	MAC Address	IP Address	Name	Connected Time	Signal

Note: Wi-Fi function is disabled by factory default, if you need to use it, please enable Wi-Fi according to the following steps, and configure the device as Wi-Fi client.

Wi-Fi Client

Configure Gateway as Wi-Fi Client

Click **“Interface > Wi-Fi > Wi-Fi”**, select **“Client”** as the mode and click **“Submit”**.

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

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

Status	WiFi
Interface	^ General Settings
Link Manager	Mode <input type="text" value="Client"/> ?
LAN	Region <input type="text" value="SE"/> ?
Ethernet	
Cellular	
WiFi	
WLAN	

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

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

Click **"Interface > WLAN"** to configure the parameters of Wi-Fi Client after setting the mode as Client.

Status

^ WLAN Status

Status	Connected
Uptime	0 days, 00:02:40
IP Address	172.16.23.246/255.255.255.0
Gateway	172.16.23.1
DNS	172.16.23.2 114.114.114.114
MAC Address	34:fa:40:09:d3:38

^ Link Status

Signal	-74 dBm
Noise	-95 dBm
Width	20 MHz
TX Bitrate	1.0 MBit/s
TX	2034 bytes (26 packets)
RX	662881 bytes (4446 packets)

^ WPA Status

WPA State	COMPLETED
Frequency	2412
BSSID	20:65:8e:ba:56:60
SSID	Robustel
Mode	station
Key Management	WPA2-PSK
Pairwise Cipher	CCMP
Group Cipher	TKIP

This window allows you to scan for all available SSIDs in your area. Please click ... and then click "Scan" to refresh the surrounding SSID.

^ Scan Results ...


Index	SSID	MAC Address	Frequency	Signal	
1	Michael's	3C:46:D8:23:5D:5A	2437	58 dBm	Scan
2	Robustel-Client	34:FA:40:06:7F:8B	2412	58 dBm	
3	cfg_ap_ssid	00:23:A7:A3:F2:B8	2462	59 dBm	
4	Cao's	34:FA:40:09:E4:49	2437	67 dBm	
5	Anjiu	88:25:93:D4:CE:A2	2437	71 dBm	
6	FT-VIP	3C:8C:40:D4:47:90	2452	73 dBm	
7	FT	3C:8C:40:D4:47:91	2452	73 dBm	

4.2.6 DI/DO

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

DI

DI	DO	Status	
^ DI Settings			
Index	Enable	Mode	Inversion
1	false	ON-OFF	false

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

DI

^ General Settings

Index:

Enable: ON OFF

Mode: v

Inversion: ON OFF

Alarm On Content:

Alarm Off Content:

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

DI

^ General Settings

Index:

Enable: ON OFF

Mode: v

Inversion: ON OFF

Threshold Value:

Alarm On Content:

Alarm Off Content:

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

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

DO

DI	DO	Status												
^ DO Settings <table border="1"> <thead> <tr> <th>Index</th> <th>Enable</th> <th>Alarm On Action</th> <th>Alarm Off Action</th> <th>Initial State</th> <th>Alarm Source</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>false</td> <td>High</td> <td>Low</td> <td>Last</td> <td>DI1 Alarm</td> </tr> </tbody> </table>			Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source	1	false	High	Low	Last	DI1 Alarm
Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source									
1	false	High	Low	Last	DI1 Alarm									

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

DO

^ General Settings

Index:

Enable: ON OFF

Alarm On Action: v

Alarm Off Action: v

Initial State: v

Delay: ?

Hold Time: ?

Alarm Source: v

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

DO

^ **General Settings**

Index

Enable ON OFF

Alarm On Action

Alarm Off Action

Initial State

Delay ?

Hold Time ?

Low-level Width ?

High-level Width ?

Alarm Source

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

DO

^ **General Settings**

Index

Enable ON OFF

Alarm On Action

Alarm Off Action

Initial State

Delay ?

Hold Time ?

Low-level Width ?


High-level Width ?

Alarm Source

General Settings @ DO		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> High: a high electrical level output 	High

General Settings @ DO		
Item	Description	Default
	<ul style="list-style-type: none"> Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered 	
Alarm Off Action	Digital Output initiates when alarm removed. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> High: a high electrical level output Low: a low electrical level output Pulse: Generates a square wave as specified in the pulse mode parameters when triggered 	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. <ul style="list-style-type: none"> Last: DO’s status will consist with the status of last power off High: DO interface is in high electrical level Low: DO interface is in low electrical level 	Last
Delay (unit: 100ms)	Set the delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
Low-level Width (unit: ms)	Set the low-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Enter from 1000 to 3000.	1000
High-level Width (unit: ms)	Set the high-level width. It is available when enabling Pulse as “Alarm On Action/Alarm Off Action”. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Enter from 1000 to 3000.	1000
Alarm Source	Digital output activation can be activated by this alarm.	DI1

Status

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

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

4.2.7 Serial Port

This section allows you to set the serial port parameters. The R2010 gateway supports two serial ports, COM1 and COM2. It can also be modified according to requirements and configured as two COM1 or two COM2. The serial data can be converted into IP data or through IP data into serial data, and then the data can be transmitted through wired or wireless network, so as to realize the function of transparent data transmission.

Port Type	Serial Port	Status
^ General Settings		
Serial Port Type	RS485	v

Serial Port		
Item	Descriptions	Default
Serial Port Type	Support RS485 and RS232	RS485

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

Click the right-most button of COM1 as below.

Serial Port

^ **Serial Port Application Settings**

Index	<input type="text" value="1"/>
Port	<input style="border-bottom: 1px solid #ccc;" type="text" value="COM1"/> v
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Baud Rate	<input style="border-bottom: 1px solid #ccc;" type="text" value="115200"/> v
Data Bits	<input style="border-bottom: 1px solid #ccc;" type="text" value="8"/> v
Stop Bits	<input style="border-bottom: 1px solid #ccc;" type="text" value="1"/> v
Parity	<input style="border-bottom: 1px solid #ccc;" type="text" value="None"/> v
Flow Control	<input style="border-bottom: 1px solid #ccc;" type="text" value="None"/> v

^ **Data Packing**

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

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

^ **Server Setting**

Application Mode	<input style="border-bottom: 1px solid #ccc;" type="text" value="Transparent"/> v
Protocol	<input style="border-bottom: 1px solid #ccc;" type="text" value="TCP Client"/> v
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

^ **Server Setting**

Application Mode	<input style="border-bottom: 1px solid #ccc;" type="text" value="Transparent"/> v
Protocol	<input style="border-bottom: 1px solid #ccc;" type="text" value="TCP Server"/> v
Local IP	<input type="text"/>
Local Port	<input type="text"/>

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

^ **Server Setting**

Application Mode	<input style="border-bottom: 1px solid #ccc;" type="text" value="Transparent"/> v
Protocol	<input style="border-bottom: 1px solid #ccc;" type="text" value="UDP"/> v
Local IP	<input type="text"/>
Local Port	<input type="text"/>
Server Address	<input type="text"/>
Server Port	<input type="text"/>

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

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

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

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

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

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

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

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

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

^ **Server Setting**

Application Mode

Modbus ASCII Gatev v

Protocol

TCP Server v

Local IP

Local Port

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

^ **Server Setting**

Application Mode

Modbus ASCII Gatev v

Protocol

UDP v

Local IP

Local Port

Server Address

Server Port

Serial Port		
Item	Description	Default
Serial Port Application Settings		
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" or "115200".	115200
Data Bits	Select from "7" or "8".	8
Stop Bits	Select from "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow control	Select from "None", "Software" or "Hardware".	None
Data Packing		
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. The unit is milliseconds. 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

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: Gateway will translate the Modbus ASCII data to Modbus TCP data and sent out, and vice versa 	Transparent
Protocol	Select from "TCP Client", "TCP Server", or "UDP". <ul style="list-style-type: none"> TCP Client: 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 	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 list				
Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS485	0B	0B	

4.3 Network

4.3.1 Route

This section allows you to set the static route. Static 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/Prefix Length	Gateway	Interface	+

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

Static Route

^ Static Route

Index:

Description:

Destination:

Netmask/Prefix Length: ?

Gateway:

Interface: v

Static Route		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask/Prefix Length	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/Prefix Length	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	192.168.10.1	wlan0	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0
3	192.168.10.0	255.255.255.0	0.0.0.0	wlan0	0

4.3.2 Firewall

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

filtering rules can be used to either accept or block certain users or ports from accessing your gateway. Click **“Network> Firewall> Filter”**. The following information is displayed:

Filtering
Port Mapping
Custom Rules
DMZ
Status

^ General Settings

Enable Filtering ON OFF

Default Filtering Policy ?

^ Access Control Settings

Enable Remote SSH Access ON OFF

Enable Local SSH Access ON OFF

Enable Remote Telnet Access ON OFF

Enable Local Telnet Access ON OFF

Enable Remote HTTP Access ON OFF

Enable Local HTTP Access ON OFF

Enable Remote HTTPS Access ON OFF

Enable Remote Ping Respond ON OFF ?

Enable DOS Defending ON OFF

Enable Console ON OFF ?

Enable VPN NAT Traversal ON OFF ?

^ Whitelist Rules ?

Index	Description	Source Address	+

^ Filtering Rules

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

Click **+** to add the whitelist rules.

Filtering

^ Whitelist Rules

Index

Description

Source Address ?

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

Filtering

^ Filtering Rules

Index

Description

Source Address ?

Source MAC ?

Target Address ?

Protocol All v

Action v

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

^ Filtering Rules

Index

Description

Source Address ?

Source Port ?

Source MAC ?

Target Address ?

Target Port ?

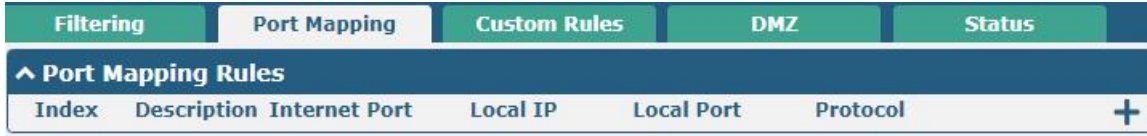
Protocol TCP v

Action v

Filtering		
Item	Description	Default
General Settings		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from “Accept” or “Drop”. <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
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

Filtering		
Item	Description	Default
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the 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.	OFF
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 debug port	Click the toggle button to enable / disable this option.	ON
Enable vpn nat traversal	Click the toggle button to enable / disable this option. When enabled, enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF
Whitelist Rules		
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Filtering Rules		
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", "ICMPv6" 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 is defined manually in the gateway, and all data received from certain ports on the public network is forwarded to a certain port on a certain IP in the internal network. Click **“Network> Firewall> Port Mapping”** to display the following:



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

Port Mapping

^ Port Mapping Rules

Index:

Description:

Remote IP: ?

Internet Port: ?

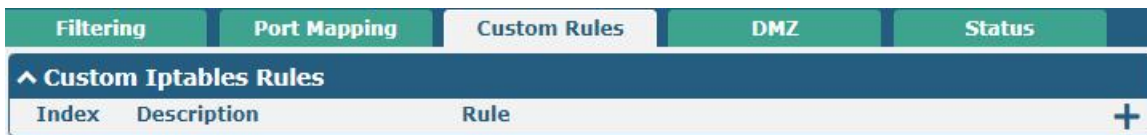
Local IP:

Local Port: ?

Protocol: v

Port Mapping Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g. 10.10.10.10/255.255.255.255 or 192.168.1.0/24	Null
Internet Port	Enter the internet port of 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, that is, rules that you define yourself. Click **“Network> Firewall> Custom Rule”** to display the following:



Click to add custom rules.

Custom Rules

^ Custom Iptables Rule

Index

Description

Rule

Custom Firewall Rules		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this Custom Firewall Rules.	Null
Rule	Enter custom rules.	Null

DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a secure system that is set up to solve the problem that users who access the external network cannot access the internal network server after the firewall is installed. A DMZ host is an intranet host where all ports are open to the specified address except the ports that are occupied and forwarded.

Click **“Network> Firewall> DMZ”**. The following information is displayed:

Filtering
Port Mapping
DMZ

^ DMZ Settings

Enable DMZ ON 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

NAT setting, i.e. custom NAT rules. Click "**Network > Firewall > NAT**" to display the following.

The screenshot shows a web interface with tabs for Filtering, Port Mapping, Custom Rules, NAT, and Status. The NAT tab is active. Under 'DMZ Settings', there is a toggle for 'Enable DMZ' set to 'OFF', and input fields for 'Host IP Address' and 'Source IP Address'. Below this is a table header for 'NAT Settings' with columns: Index, Description, Source Address, Out, Target Address, and NAT IP. A plus sign icon is visible at the end of the table header.

Click to add custom rules.

The screenshot shows the 'NAT Settings' configuration form. It includes input fields for 'Index' (value: 1), 'Description', 'Source Address', 'Out' (dropdown menu: unspecified), 'Target Address', and 'NAT IP'. Each input field has a help icon (question mark). At the bottom right, there are 'Submit' and 'Close' buttons.

NAT Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description of this NAT rule.	Null
Source Address	Enter the source address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, or null to indicate any address.	Null
Out	Select the output interface. Selecting unspecified means any output interface.	unspecified
Target Address	Enter the target address in the format x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x.	Null
NAT IP	Enter the NAT address in the format x.x.x.x.	Null

Click **Status** to view the device’s firewall status.

Filtering	Port Mapping	Custom Rules	NAT	Status			
Chain Input							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	tcp	wlan0	*	0.0.0.0/0	0.0.0.0/0
4	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
5	6	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	5	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	tcp	wlan0	*	::/0	::/0
12	0	DROP	tcp	wlan0	*	::/0	::/0
13	0	DROP	tcp	wlan0	*	::/0	::/0
14	0	REJECT	tcp	*	*	::/0	::/0
15	0	ACCEPT	tcp	*	*	::/0	::/0
16	0	DROP	tcp	*	*	::/0	::/0
17	0	ACCEPT	tcp	*	*	::/0	::/0
18	0	DROP	tcp	*	*	::/0	::/0
19	0	ACCEPT	icmpv6	*	*	::/0	::/0
20	0	DROP	icmpv6	*	*	::/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
2	0	TCPMSS	tcp	*	*	::/0	::/0
Chain Output							
Index	Packets	Target	Protocol	In	Out	Source	Destination

4.3.3 IP Passthrough

Click “**Network > IP Passthrough > IP Passthrough**” to enable or disable the IP Passthrough option.



If gateway enables the IP Passthrough, 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.

Note: The IP Passthrough function can only assign one network provider address.

4.4 VPN

4.4.1 IPsec

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

Click **“Virtual Private Network> IPsec> General”** to set IPsec parameters.

General

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

Click **+** to add tunnel settings. The maximum count is 6.

Tunnel

^ **General Settings**

Index

Enable ON OFF

Description

Gateway ?

Mode v

Protocol v

Local Subnet ?

Remote Subnet ?

Link Binding v ?

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter the address or domain name of remote side IPsec VPN server.0.0.0.0 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
Link binding	Select from WWAN1, WWAN2, WAN, or WLAN.	Not bound

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

^ IKE Settings

IKE Type	IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	PSK	v
PSK Secret	<input type="text"/>	
Local ID Type	Default	v
Remote ID Type	Default	v
IKE Lifetime	86400	?

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

^ IKE Settings

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

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

^ IKE Settings

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

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

^ IKE Settings

IKE Type	IKEv1	v
Negotiation Mode	Main	v
Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	xAuth PSK	v
PSK Secret	<input type="text"/>	
Local ID Type	Default	v
Remote ID Type	Default	v
Username	<input type="text"/>	?
Password	<input type="text"/>	?
IKE Lifetime	86400	?

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

^ IKE Settings

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

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

IKE Settings		
Item	Description	Default
	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 	
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from "PSK", "CA", "PKCS#12", "xAuth PSK" and "xAuth CA" to be used in IKE negotiation. <ul style="list-style-type: none"> PSK: Pre-shared Key CA: x509 Certificate Authority xAuth: Extended Authentication to AAA server 	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> Default: Use an IP address as the ID in IKE negotiation FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com. 	Default
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> Default: Use an IP address as the ID in IKE negotiation FQDN: Use an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Use a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com. 	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.	Null
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication types.	Null

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

^ General Settings

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

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Gateway	<input type="text"/> ?
Mode	<input type="text" value="Tunnel"/> v
Protocol	<input type="text" value="AH"/> v
Local Subnet	<input type="text"/> ?
Remote Subnet	<input type="text"/> ?
Link Binding	<input type="text" value="Unspecified"/> v ?

^ IKE Settings

^ SA Settings

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

^ Advanced Settings

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

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.	SHA1
PFS Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	DHgroup2
SA Lifetime	Set the IPsec SA lifetime. When negotiating 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 no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPsec SAs based on the IKE SA.	30
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	180
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forced Encapsulation	Click the toggle button to enable / disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

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

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

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

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel.	Tunnel 1
Local Certificate	Click on “Choose File” to locate the certificate file from your computer, and then import this file into your gateway.	--
Peer Certificate	Select the peer certificate to import to the gateway.	--
Private Key	Select the correct private key file to import into the gateway.	--
Root Certificate	Select the root certificate file to import into the gateway.	--
PKCS#12 Certificate	Select the PKCS#12 certificate file to import into the route	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate’s name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

4.4.2 WireGuard

This section is used to set the parameters of WireGuard VPN, an open source SSL-based VPN system. The gateway's WireGuard feature can support both point-to-point and point-to-multipoint VPN channels.

Click “**Virtual Private Network > WireGuard > WireGuard**” to set the WireGuard parameters.

WireGuard@General Settings		
Item	Descriptions	Default
Enable WireGuard	Enable or disable WireGuard	OFF
Private Key	Enter the local private key. It can be generated automatically or imported manually via X509 settings, but cannot be empty.	Null
IP Address	Enter the IP address of the virtual interface. It cannot be empty.	Null
Listen Port	Enter the virtual interface listen port. It cannot be empty.	51820
MTU	Enter the virtual interface slice size.	1472
Enable NAT	Enable/disable the NAT feature. When enabled, the IP address will be converted to the interface virtual IP address.	ON

Note: click for help.

Peer Settings						
Index	Description	Public Key	Endpoint Host	Endpoint Port	Allowed IPs	
						+

Click to add peer setting. The maximum count is 20.

WireGuard

^ Peer Settings

Index

Description

Public Key

Preshared Key

Endpoint Host

Endpoint Port

Allowed IPs

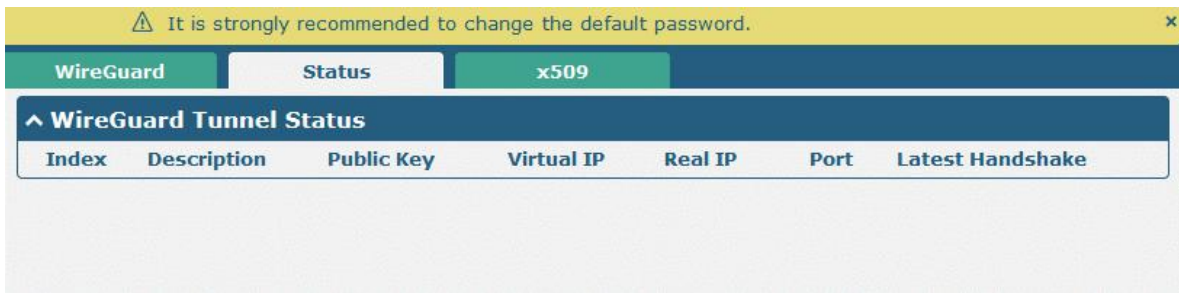
Route Allowed IPs ON OFF

Persistent Keepalive

WireGuard@Peer Settings		
Item	Descriptions	Default
Peer Settings		
Index	Display the index	--
Description	Enter peer descriptions. Can be empty.	Null
Public Key	Enter public key and it cannot be empty.	Null

WireGuard@Peer Settings		
Item	Descriptions	Default
Preshared Key	Enter preshared key and it cannot be empty.	Null
Endpoint Host	Enter the peer IP address. A null value will not initiate a connection request.	Null
Endpoint Port	Enter the peer port. A null value will not initiate a connection request.	Null
Allowed IPs	Enter the allowed IP address, which cannot be empty.	Null
Route Allowed IPs	Enable/disable the feature. When enabled, routes will be created for the networks allowed for this peer. If the allowed network is 0.0.0.0/0, this peer will be set as the default route.	ON
Persistent Keepalive	Enter the interval of sending Persistent Keepalive messages, in seconds. 0 means disabling the feature.	0


The status bar allows to view WireGuard's connection status. Click on one of the rows and details of its link connection will be displayed below the current row.



This section is used to generate or import private and public keys.



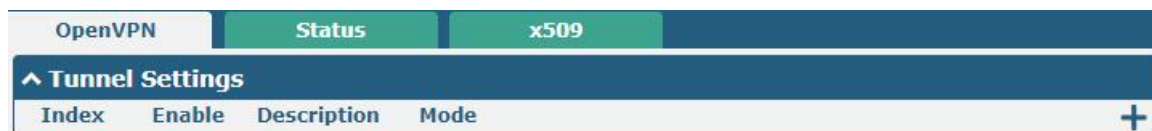
x509		
Item	Descriptions	Default
X509 Settings		
Private Key	Click Generate to generate private key; click Import to import the private key.	--
Private Key	Click Import to import the private key from the computer to the	--

x509		
Item	Descriptions	Default
	gateway.	
Public Key	Click  to generate public key.	--

4.4.3 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.

Click “**Virtual Private Network> OpenVPN> OpenVPN**”. The following information is displayed:



Click **+** to add tunnel settings. The maximum count is 6. By default, the mode is “P2P”.

General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="P2P"/> <input type="button" value="v"/> <input type="button" value="?"/>
TLS Mode	<input type="text" value="None"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="None"/> <input type="button" value="v"/> <input type="button" value="?"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="None"/> <input type="button" value="v"/> <input type="button" value="?"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Renegotiation Interval	<input type="text" value="86400"/> <input type="button" value="?"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

^ General Settings

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

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v ?
Protocol	<input type="text" value="UDP"/> v
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="None"/> v ?
Encrypt Algorithm	<input type="text" value="BF"/> v
Authentication Algorithm	<input type="text" value="SHA1"/> v
Renegotiation Interval	<input type="text" value="86400"/> ?
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="P2P"/> <input type="button" value="v"/> <input type="button" value="?"/>
TLS Mode	<input type="text" value="None"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="Preshared"/> <input type="button" value="v"/> <input type="button" value="?"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="P2P"/> <input type="button" value="v"/> <input type="button" value="?"/>
TLS Mode	<input type="text" value="None"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="Password"/> <input type="button" value="v"/> <input type="button" value="?"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="P2P"/> v ?
TLS Mode	<input type="text" value="None"/> v ?
Protocol	<input type="text" value="UDP"/> v
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/> v
Authentication Algorithm	<input type="text" value="SHA1"/> v
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable IPv6	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Description	<input type="text"/>
Mode	P2P <input type="button" value="v"/> <input type="button" value="?"/>
TLS Mode	None <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	1194
Listen IP Address	<input type="text"/>
Listen Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA Password <input type="button" value="v"/> <input type="button" value="?"/>
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Keepalive Interval	20 <input type="button" value="?"/>
Keepalive Timeout	120 <input type="button" value="?"/>
TUN MTU	1500
Max Frame Size	<input type="text"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	0 <input type="button" value="v"/> <input type="button" value="?"/>

^ Advanced Settings

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

^ Advanced Settings

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

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

^ **Advanced Settings**

Enable HMAC Firewall OFF

Enable Cri OFF

Enable Client To Client OFF

Enable Dup Client OFF

Enable IP Persist ON OFF ?

Expert Options ?

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

OpenVPN | Status | x509

^ **Tunnel Settings**

Index	Enable	Description	Mode	Protocol	Peer Address	Interface Type	+	
^ Password Manage								
Index	Username							+

Click Client Management + to add client information, as shown below:

OpenVPN

^ **General Settings**

Index

Enable ON OFF

Common Name ?

Client IP Address

Route ?

Push Route ?

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" or "Server".	P2P
TLS Mode	Select from "None", "Client" or "Server".	None
Protocol	Select from "UDP", "TCP-Client" or "TCP-Server".	UDP
Server Address	Enter the end-to-end IP address or the domain of the remote OpenVPN server.	Null
Server Port	Enter the end-to-end listener port or the listening port of the OpenVPN server.	1194

General Settings @ OpenVPN		
Item	Description	Default
Listening Address	Local server address.	Null
Listening Port	Local server port.	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
Authentication Type	Select from "None", "Preshared", "Password", "X509CA" and "X509CA Password". Note: "None" and "Preshared" authentication type are only working with P2P mode.	None
Enable IP Address Pool	Click the toggle button to enable / disable the IP address pool allocation function.	OFF
Starting Address	Defines the beginning of an IP address pool that assigns addresses to OpenVPN clients.	10.8.0.5
End Address	Defines the end of the IP address pool for assigning addresses to OpenVPN clients.	10.8.0.254
Client Network	Enter the client network IP.	10.8.0.0
Client Netmask	Enter the client netmask.	255.255.255.0
Username	Enter the username used for "Password" or "X509CA Password" authentication type.	Null
Password	Enter the password used for "Password" or "X509CA Password" authentication type.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES128", "AES192" and "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
Maximum Number of Clients	Set the maximum number of clients allowed to access the OpenVPN server.	10
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
MTU	Set the maximum transmission unit.	1500
Data Fragmentation	Set the maximum frame length.	Null

General Settings @ OpenVPN		
Item	Description	Default
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 Default Gateway	Standalone switch button to enable / disable the default gateway function. After enabling, push the local tunnel address as the default gateway of the peer device.	OFF
Receive DNS Push	Standalone switch button to enable / disable receiving DNS push function. After enabling, it is allowed to receive DNS information pushed by the peer.	OFF
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 @ OpenVPN		
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
Enable Crl	Click the toggle button to enable / disable the option. When enabled, client certificates can be revoked.	OFF
Enable Client to Client	Click the toggle button to enable / disable the option. When enabled, clients can communicate with each other.	OFF
Enable Dup Client	Click the toggle button to enable / disable the option. After being enabled, the tunnel IPs obtained by multiple clients are different, and the tunnel IP of the client and the tunnel IP of the server are interoperable.	OFF
Enable IP Address Hold	Click the toggle button to enable / disable the option. When enabled, the IP in the address pool is obtained automatically.	ON
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null
Advanced Settings @ User Password Management		
Username	Custom tunnel connection username.	Null

General Settings @ OpenVPN		
Item	Description	Default
Password	Custom tunnel connection password.	Null
Client Management		
Enable	Click the toggle button to enable / disable this option. When enabled, the client IP address can be managed.	OFF
Common Name	Set the certificate name.	Null
Client IP Address	Set a fixed client virtual IP.	Null
Route	Set client-side subnet.	Null
Push Route	Set server-side subnet.	Null

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

The screenshot shows the 'OpenVPN Status' page. It has tabs for 'OpenVPN', 'Status', and 'x509'. Under 'OpenVPN Tunnel Status', there is a table with columns: Index, Description, Status, Mode, Uptime, Local IP, and Local IPv6. Below that is the 'OpenVPN Client List' table with columns: Index, Common Name, Real IP, Port, Virtual IP, and Virtual IPv6.

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

The screenshot shows the 'X509 Settings' page. It has tabs for 'OpenVPN', 'Status', and 'x509'. The settings include: Tunnel Name (dropdown: Tunnel 1), Mode (dropdown: Client), Root CA (Choose File: No file chosen), Certificate File (Choose File: No file chosen), Private Key (Choose File: No file chosen), TLS-Auth Key (Choose File: No file chosen), and PKCS#12 Certificate (Choose File: No file chosen). Below is a 'Certificate Files' table with columns: Index, File Name, File Size, and Modification Time.

x509		
Item	Description	Default
X509 Settings		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5" or "Tunnel 6".	Tunnel 1
Tunnel mode	Select "P2P Mode", "Client Mode" or "Server Mode".	Client mode
Root certificate	Select the root certificate file to import into the gateway.	--
Certificate Files	Click on "Choose File" to locate the certificate file from your computer, and then import this file into your gateway.	--
Private Key	Select the private key file to import into the gateway.	--

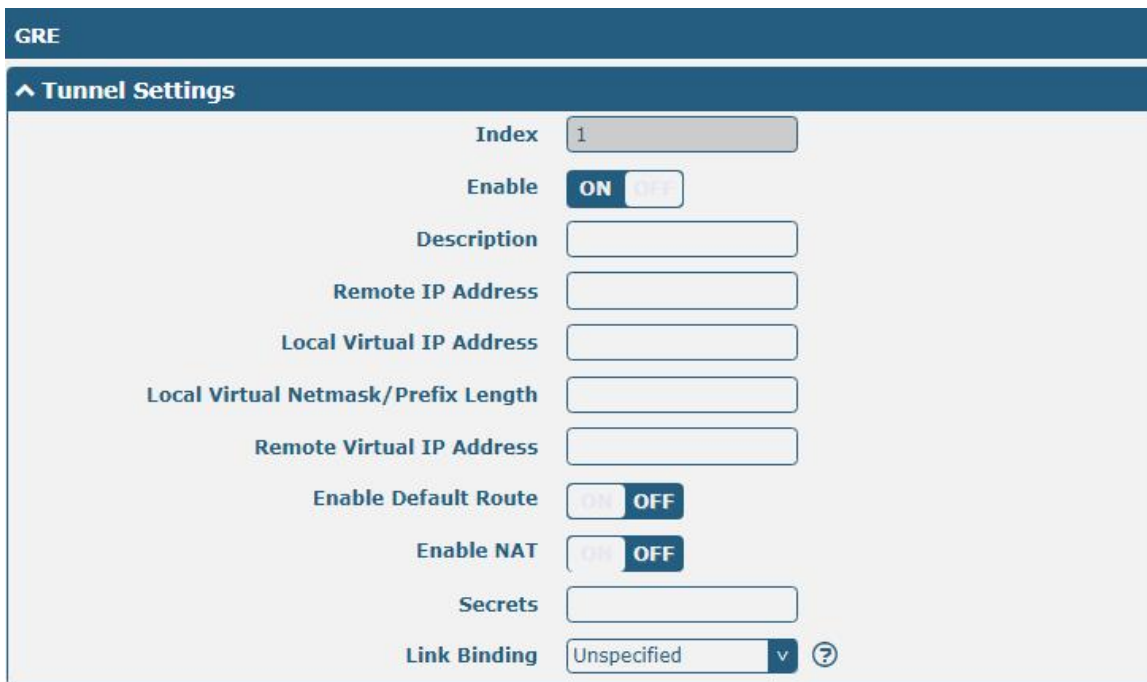
TLS-Auth Key	Select the TLS-Auth key file to import into the gateway.	--
PKCS # 12 Certificate	Select the PKCS # 12 certificate file to import into the gateway.	--
Certificate Files		
Index	Indicate the ordinal of the list.	--
Filename	Show the imported certificate's name.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

4.4.4 GRE

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



Click **+** to add tunnel settings. The maximum count is 6.



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
Link Binding	Select from "WWAN1", "WWAN2", "WAN", or "WLAN".	Not bound

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

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

4.5 Services

4.5.1 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.

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

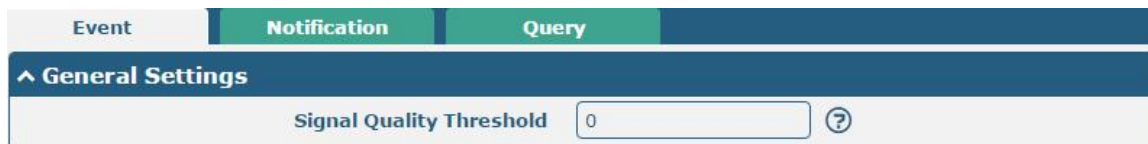
The window is displayed as below when enabling the “Log to Remote” option.

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

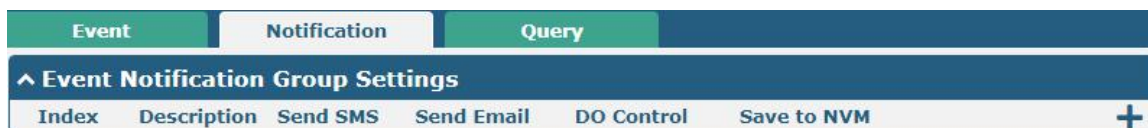
Syslog Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from "Debug", "Info", "Notice", "Warning" or "Error", which from low to high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from "RAM", "NVM" or "Console". The data will be cleared after reboot when choose "RAM". Note: It's not recommended that you save syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow 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


4.5.2 Event

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



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



Click  button to add an Event parameters.

Notification

^ General Settings

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Send SMS	<input type="checkbox"/> OFF
Send Email	<input type="checkbox"/> OFF
DO Control	<input type="checkbox"/> OFF
Save to NVM	<input type="checkbox"/> OFF ?

^ Event Selection ?

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

General Settings @ Notification		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the gateway will send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.21 Services > Email", and use ',' to separate each number.	OFF
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 "3.21 Services > Email".	OFF
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event gateway will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

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

Event
Notification
Query

^ Event Details

Save Position v

Filtering

```

Sep 11 19:00:53, system startup
Sep 11 19:00:55, LAN port link down, eth0
Sep 11 19:00:55, LAN port link up, eth1
Sep 11 19:01:06, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:01:16, system time update
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:25, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:26, configuration change, via web manager
Sep 11 19:47:41, configuration change, link_manager restored to default after firmware updating
Sep 11 19:47:42, configuration change, via web manager
Sep 11 19:47:42, WWAN (cellular) down, WWAN1
Sep 11 19:47:44, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:48:50, configuration change, via web manager
Sep 11 19:48:51, WWAN (cellular) down, WWAN1
Sep 11 19:48:52, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 19:49:04, configuration change, via web manager
Sep 11 19:49:05, WWAN (cellular) down, WWAN1
Sep 11 19:49:10, WLAN up
Sep 11 19:59:33, configuration change, link_manager restored to default after firmware updating
Sep 11 19:59:34, configuration change, via web manager
Sep 11 19:59:36, WLAN down
Sep 11 19:59:36, WWAN (cellular) up, WWAN1, ip=10.189.43.25
Sep 11 20:29:00, LAN port link down, eth1
Sep 11 20:34:06, LAN port link up, eth1
                    
```

Clear
Refresh

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

4.5.3 NTP

This section allows you to set the related NTP (Network Time Protocol) parameters.

NTP
Status

^ Timezone Settings

Time Zone

Expert Setting

^ NTP Client Settings

Enable ON OFF

Primary NTP Server

Secondary NTP Server

NTP Update Interval

^ NTP Server Settings

Enable ON OFF

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 computer’s time.



4.5.4 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 **5.2.2 SMS Remote Control**.



SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. Note: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum” or “Both”. <ul style="list-style-type: none"> • Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; ...” • 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.

SMS
SMS Testing

^ SMS Testing

Phone Number

Message

Result

SMS Testing		
Item	Description	Default
Phone Number	Enter the specified phone number which can receive the SMS from 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
<input type="button" value="Send"/>	Click the button to send the test message.	--

4.5.5 Email

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

Email

^ Email Settings

Enable ON OFF

Enable TLS/SSL ON OFF ?

Enable STARTTLS ON OFF

Outgoing Server

Server Port

Timeout ?

Auth Login ON OFF ?

Username

Password

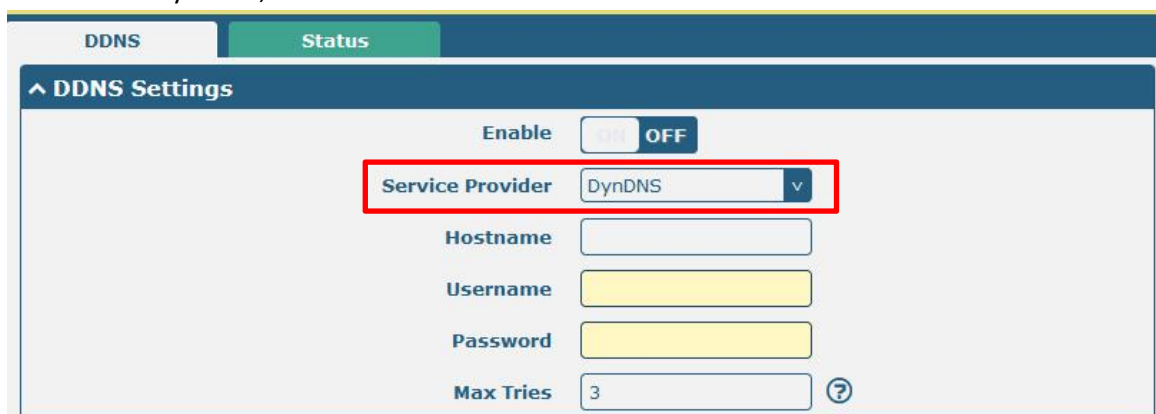
From

Subject

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

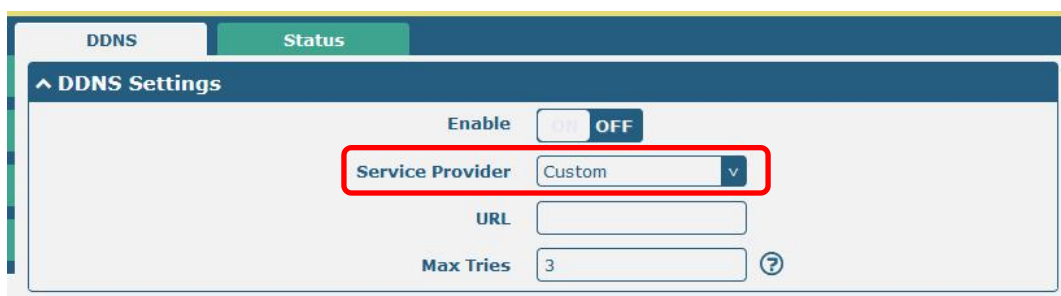
4.5.6 DDNS

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



The screenshot shows the DDNS Settings window. The 'Enable' toggle is set to OFF. The 'Service Provider' dropdown menu is highlighted with a red box and shows 'DynDNS' selected. Below it are input fields for 'Hostname', 'Username', and 'Password', and a 'Max Tries' field set to 3.

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



The screenshot shows the DDNS Settings window with 'Custom' selected in the 'Service Provider' dropdown menu, which is highlighted with a red box. The 'URL' field is now visible below the 'Service Provider' field. The 'Max Tries' field remains set to 3.

DDNS Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the DDNS option.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322” or “Custom”. Note: The DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the hostname provided by the DDNS server.	Null
Username	Enter the username provided by the DDNS server.	Null
Password	Enter the password provided by the DDNS server.	Null
URL	Enter the URL customized by user.	Null
Max tries	Enter the maximum tries times	3

DDNS
Status

^ DDNS Status

Status Disabled

Last Update Time

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

4.5.7 SSH

Gateway supports SSH password access and secret-key access.

SSH
Keys Management

^ SSH Settings

Enable ON OFF

Port

Disable Password Logins ON 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

SSH | Keys Management

^ Import Authorized Keys

Authorized Keys No file chosen

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

4.5.8 Web Server

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

Web Server | Certificate Management

^ General Settings

HTTP Port ?

HTTPS Port ?

General Settings @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in 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 Web Server.	80
HTTPS Port	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. Note: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.	443

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

Web Server | Certificate Management

^ Import Certificate

Import Type v

HTTPS Certificate No file chosen

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.	--

4.5.9 Advanced

This section allows you to set the Advanced and parameters.

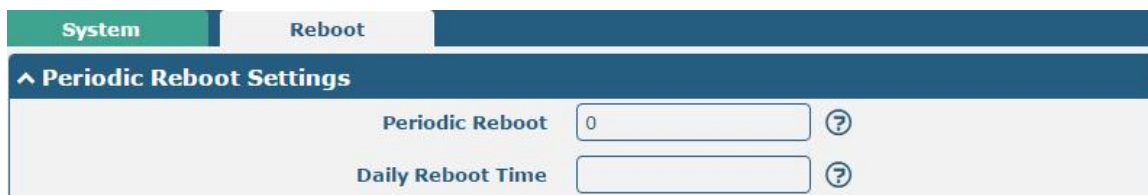


System | **Reboot**

^ System Settings

Device Name ?

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



System | **Reboot**

^ Periodic Reboot Settings

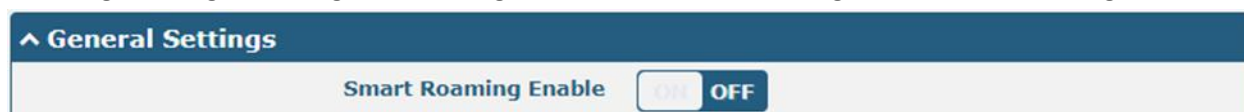
Periodic Reboot ?

Daily Reboot Time ?

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

4.5.10 Smart Roaming

Smarting roaming includes general settings, health check, PING settings and advanced settings.



^ General Settings

Smart Roaming Enable ON OFF

General Setting		
Item	Descriptions	Default
Smart Roaming Enable	Enable Smart Roaming	OFF

^ Health Check

Health Check Interval	<input type="text" value="5"/>	?
RSSI Quality Check	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
RSSI Threshold(2G)	<input type="text" value="-87"/>	?
RSSI Threshold(3G)	<input type="text" value="-87"/>	?
RSSI Threshold(4G)	<input type="text" value="-87"/>	?
RSRP Quality Check	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
RSRP Threshold(4G)	<input type="text" value="-105"/>	?
Network Delay Check	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
RTT Timeout Threshold	<input type="text" value="3000"/>	?
Packet Loss Rate Check	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
Packet Loss Rate Threshold	<input type="text" value="70"/>	?

Health Check		
Item	Descriptions	Default
Health Check Interval	The health check interval for the current connection in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Quality Check	To enable/disable the "RSSI Quality Check" feature.	ON
RSSI Threshold (2G)	Signal strength threshold for 2G networks.	-87 dBm
RSSI Threshold (3G)	Signal strength threshold for 3G networks.	-87 dBm
RSSI Threshold (4G)	Signal strength threshold for 4G networks.	-87 dBm
RSRP Quality Check	To enable/disable the "RSRP Quality Check" feature.	OFF
RSRP Threshold (4G)	The reference signal received power threshold for 4G networks.	-105 dBm
Network Delay Check	To enable/disable the "Network Delay Check" feature.	ON
RTT Timeout Threshold	The reference signal received power threshold for 4G networks.	3000 ms
Packet Loss Rate Check	To enable/disable the "Packet Loss Rate Check" feature.	ON
Packet Loss Rate Threshold	Packet loss rate threshold value.	70 %

^ PING Settings ?

Primary Server

Secondary Server

PING Timeout ?

Ping Tries ?

PING Settings		
Item	Descriptions	Default
Primary Server	The gateway pings the primary address/domain name to detect if the current connection is always alive.	8.8.8.8
Secondary Server	The gateway pings the secondary address/domain name to detect if the current connection is always alive.	114.114.114.114
Ping Timeout	Set the Ping timeout.	5 seconds
Ping Tries	The number of ping attempts per health check. Each ping attempt sends 3 ping messages by default, so the total number of ping messages sent per health check is (3 * number of ping attempts).	3 times

^ Advanced Settings
?

Use Degraded Network ON OFF ?

Periodic Restart ?

Daily Restart Time ?

Advanced Settings		
Item	Descriptions	Default
Use Degraded Network	To enable/disable the "Use degraded network" feature. A degraded network is defined as a network that can be connected, but the network quality does not meet the health check thresholds.	OFF
Periodic Restart	Set the period of rebooting "Smart Roaming" function in hours. 0 means no periodic reboot is enabled. Restarting "Smart Roaming" will re-find the available carrier network and reset the current status, because it takes a long time to search the available provider network, the reboot may take 3 to 5 minutes.	0
Daily Restart Time	Set the time point to restart "Smart Roaming" every day in the format of HH:MM (24-hour system). When this item is empty, it means disable the timer reboot.	Null

^ Status
?

State Inactive

Operator Selection Mode

Time Since Last Network Scan

Status	
Item	Descriptions
Status	Display the current status of "Smart Roaming". It includes Scanning, Connecting, Connected and Inactive status, which indicate that the network is searching for available network, connecting network, network is connected and the function is not started respectively.
Operator Selection Mode	Displays how the carrier network is currently selected. These include Automatic and Manual, which refer to automatic selection according to standard specifications and software selection based on network quality, respectively, and the software will cycle through the two methods.
Time Since Last Network Scan	Displays the time elapsed since the last search for available networks. A "Smart Roaming" reboot will refresh this time.

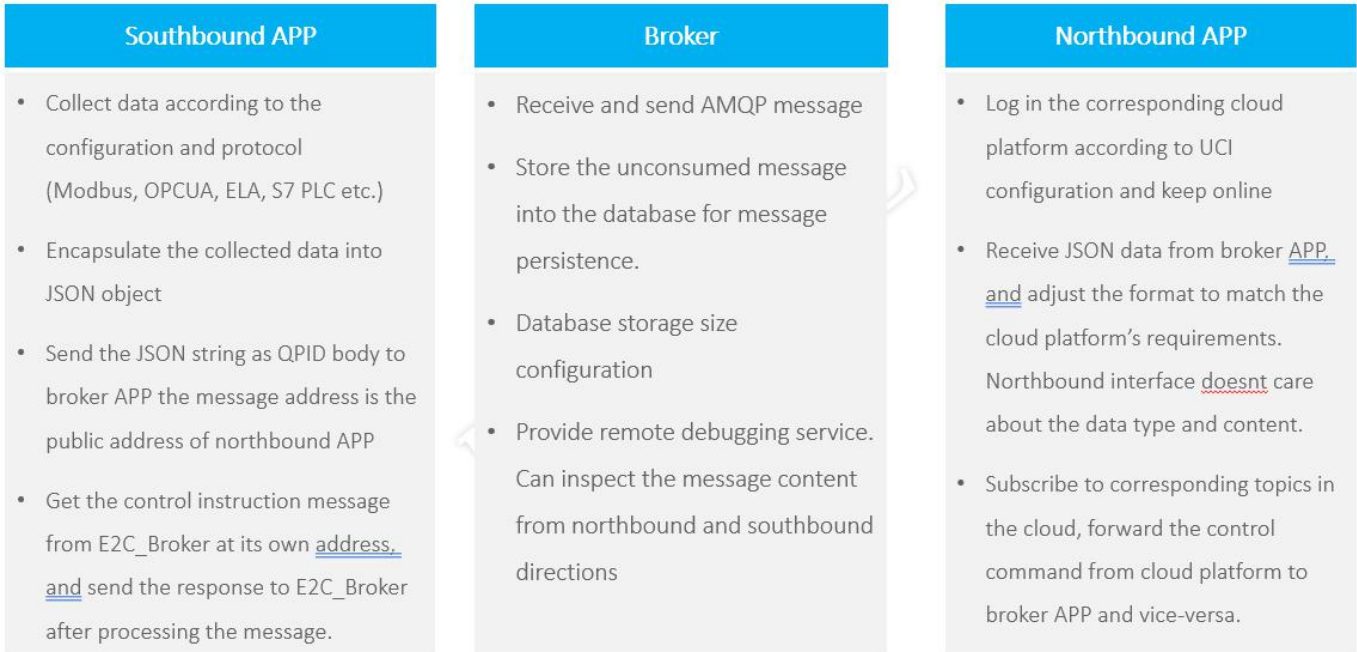
^ PLMN List ?								
Index	PLMN	Status	RAT	RSSI(dbm)	RSRP(dbm)	Latency(ms)	Packet Loss(%)	HealthCheck
PLMN List								
Item	Descriptions							
Index	PLMN list index							
PLMN	PLMN = MCC + MNC, that is, a combination of mobile country code and mobile network code.							
Status	The current network status, including Current, Visible, Forbidden, and Unknown, indicates the current use of this network, the available network, the forbidden network, and the unknown network, respectively.							
RAT (dbm)	Current wireless access technologies, including 2G/3G/4G.							
RSSI (dbm)	Current signal quality for 3G and 4G networks.							
RSRP (dbm)	Current reference signal reception power for 4G networks.							
Latency	Current network latency.							
Packet Loss (%)	Current network packet loss rate.							
Health Check	The current health check status, including Pending, Good, Degraded, and Failed, indicates that the current network has not yet been health checked; the network quality is good; the network is degraded; and the network quality is poor (including the network is disconnected or does not meet the health check threshold), respectively.							

4.6 Edge2Cloud

4.6.1 Edge2Cloud

Edge2Cloud (E2C) is a series of software collections running in the ROS operating system embedded in the Robustel Smart Gateway device, which can provide various functions of the IoT gateway at the hardware and software levels and solve the problem of data interfacing between traditional industrial device and the cloud platform.

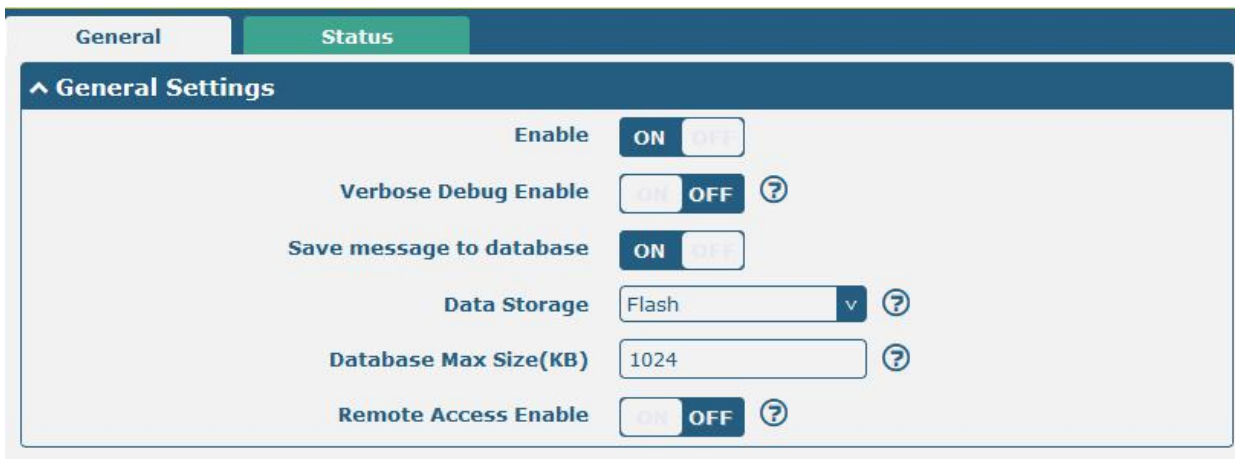
There are three types of E2C: Southbound APP, Northbound APP and Broker.



The latest ROS firmware has integrated E2C Broker, users can use the full functionality of Edeg2Cloud by choosing to install the corresponding Southbound APP and Northbound APP according to their needs.

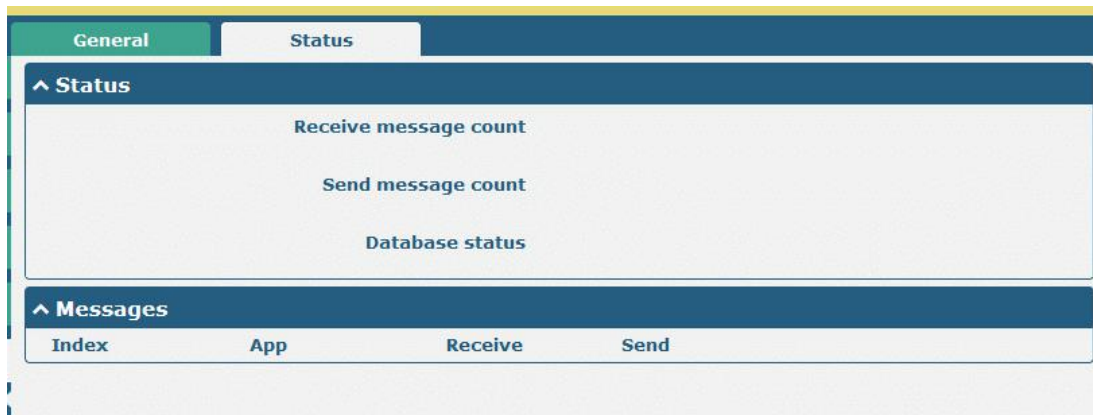
4.6.2 E2C Broker

This section is used to set E2C Broker parameters and view the operational status of E2C Broker. Click "**Edge2Cloud > E2C Broker**" to display the following.



E2C Broker Settings		
Item	Descriptions	Default
General Settings		
Enable	Enable or disable E2C Broker	OFF

Verbose Debug Enable	Enable or disable more detailed verbose debug	OFF
Save message to database	Whether the messages received by Broker are saved to the database.	ON
Data Storage	Database file storage area, optional: RAM, FLASH, SD-Card and USB-Storage.	FLASH
Database Max Size (kB)	The maximum size of the database file, in KB.	1024
Remote Access Enable	Whether to support sending and receiving messages through the web interface.	OFF



E2C Broker Status	
Item	Descriptions
Status	
Receive message count	The number of MQ messages received by Broker.
Send message count	Debugging of MQ messages sent by Broker.
Database status	Available means that the database is available and Space exceed means that the database capacity has reached the set maximum.
Messages	
App	Edge2Cloud southbound and northbound app name.
Receive	The number of messages received from the application.
Send	The number of messages sent to the reapplication.

4.7 System

4.7.1 Debug

This section allows you to check and download the syslog details. Click “**Service > Syslog > Syslog Settings**” to enable the syslog.

Syslog

^ Syslog Details

Log Level Debug v

Filtering ?

```

Sep 11 21:00:58 router user.debug rping[4655]: round-trip min/avg/max = 141.447/141.447/141.447 ms
Sep 11 21:00:58 router user.debug link_manager[3986]: rcv action ping_success from rping
Sep 11 21:00:58 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:00:58 router user.info link_manager[3986]: WWAN1 ping test success
Sep 11 21:05:58 router user.debug link_manager[3986]: WWAN1 (wwan) start ping test
Sep 11 21:05:58 router user.debug rping[4718]: start ping 8.8.8.8 (wwan)
Sep 11 21:05:59 router user.debug rping[4718]: PING 8.8.8.8 (8.8.8.8) from 10.18.11.133: 16 data bytes
Sep 11 21:05:59 router user.debug rping[4718]: 24 bytes from 8.8.8.8: seq=0 ttl=51 time=139.263 ms
Sep 11 21:05:59 router user.debug rping[4718]:
Sep 11 21:05:59 router user.debug rping[4718]: --- 8.8.8.8 ping statistics ---
Sep 11 21:05:59 router user.debug rping[4718]: 1 packets transmitted, 1 packets received, 0% packet loss
Sep 11 21:05:59 router user.debug rping[4718]: round-trip min/avg/max = 139.263/139.263/139.263 ms
Sep 11 21:05:59 router user.debug link_manager[3986]: rcv action ping_success from rping
Sep 11 21:05:59 router user.debug link_manager[3986]: target link WWAN1, state Connected
Sep 11 21:05:59 router user.info link_manager[3986]: WWAN1 ping test success
                    
```

Manual Refresh v
 Clear
Refresh

^ Syslog Files

Index	File Name	File Size	Modification Time
1	messages	77945	Wed Sep 11 21:05:59 2019

^ System Diagnostic Data

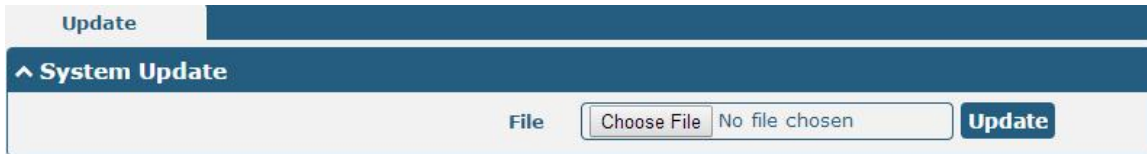
System Diagnostic Data
Generate

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.	--

4.7.2 Update

This section allows you to upgrade the gateway system and implement system update by importing and updating firmware files. Import a firmware file from the computer to the gateway, click **Update** and restart the device as prompted to complete the firmware update.

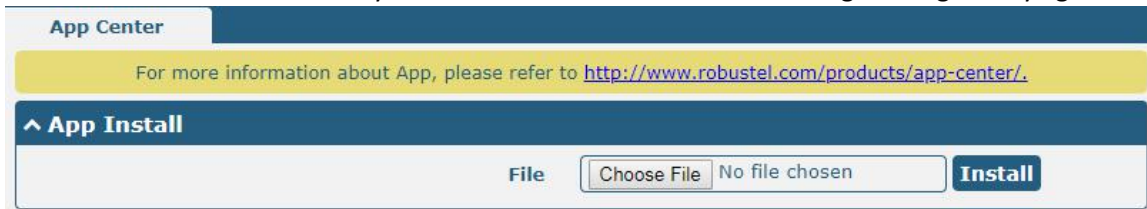
Note: To access the latest firmware file, please contact your technical support engineer.



4.7.3 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.



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

^ Installed Apps					
Index	Name	Version	Status	Description	
1	language_chinese	3.1.0	Stopped	Chinese language	X

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. Note: File format should be xxx.rpk, e.g. R2010-robustlink-1.0.0.rpk.	--
Installed Apps		
Index	Indicate the ordinal of the list.	--
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

4.7.4 Tools

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

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

Host

Packets Request

Protocol v

Status

Start **Stop**

^ Capture Files

Index	File Name	File Size	Modification Time
1	19-09-11_21-18-43.cap	52420	Tue Apr 13 17:15:24 2021

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

4.7.5 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 ON OFF

Ignore Invalid Settings ON OFF

XML Configuration File No file chosen

^ Export Configuration File

Ignore Disabled Features ON OFF

Add Detailed Information ON OFF

Encrypt Secret Data ON 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.	ON
XML Configuration File	Click on <input type="text" value="Choose File"/> to locate the XML configuration file from your computer, and then click <input type="button" value="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.	ON
XML Configuration File	Click Generate button to generate the XML configuration file, and click Export to export the XML configuration file.	--
Default Configuration		
Save Running Configuration as Default	Click Save button to save the current running parameters as default configuration.	--
Restore to Default Configuration	Click Restore button to restore the factory defaults.	--

Profile
Rollback

^ Configuration Rollback

Save as a Rollbackable Archive
Save
?

^ Configuration Archive Files

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

4.7.6 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.

Super User
Common User

^ Super User Settings

New Username ?

Old Password ?

New Password ?

Confirm Password

Super User Settings		
Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null
Old Password	Enter the old password of your 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 style="width: 80%;" type="text" value="1"/>
Role	<input style="border-bottom: 1px solid #ccc;" type="text" value="Visitor"/> v
Username	<input style="width: 80%;" type="text"/> ?
Password	<input style="width: 80%;" type="password"/> ?

Common User Settings		
Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from "Visitor" and "Editor". <ul style="list-style-type: none"> Visitor: Users only can view the configuration of 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

5 Configuration Examples

5.1 Cellular

5.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM card for Cellular Dial-up. Connect the 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 and “WWAN2” as the backup link, and set “Cold Backup” as the backup mode, then click “Submit”.

Link Manager
Status

^ General Settings

Primary Link ?





Backup Link


Backup Mode ?

Revert Interval ?

Emergency Reboot ON OFF ?

^ Link Settings

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

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

Link Manager

^ General Settings

Index

Type

Description

IPv6 Enable ON OFF

^ WWAN Settings

Automatic APN Selection ON OFF

Dialup Number

Authentication Type v

PPP Preferred ON OFF ?

Switch SIM By Data Allowance ON OFF ?

Data Allowance ?

Billing Day ?

^ Ping Detection Settings ?

Enable ON OFF

Primary Server

Secondary Server

Interval ?

Retry Interval ?

Timeout ?

Max Ping Tries ?

^ Advanced Settings

NAT Enable ON OFF

Upload Bandwidth ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable ON OFF

Verbose Debug Enable ON OFF

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

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

Cellular | **Status** | AT Debug

^ Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	
2	SIM2		Auto	All	

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

^ General Settings

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

^ Cellular Network Settings

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

^ Advanced Settings

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

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

5.1.2 SMS Remote Control

R2010 supports remote control via SMS. You can use following commands to get the status of the gateway, and set all the parameters of the gateway.

SMS command have the following structures:

1. Password mode—Username: **Password;cmd1;cmd2;cmd3; ...cmdn** (available for every phone number).
2. Phonenum mode-- **Password; cmd1; cmd2; cmd3; ... cmdn** (available when the SMS was sent from the phone number which had been added in 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. Username 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 **6.1 Introductions for CLI**.

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

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

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

XML command:

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

SMS cmd:

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

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

admin:admin;status system

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

SMS received:

```
hardware_version = 1.0
firmware_version = beta210414
firmware_version_full = "beta210414 (Rev 4034)"
kernel_version = 4.9.152
device_model = R2010
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 15 17:09:04 2021"
```

```
ram_usage = "77M Free/128M Total"
```

```
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 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500
```

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

SMS received:

OK

OK

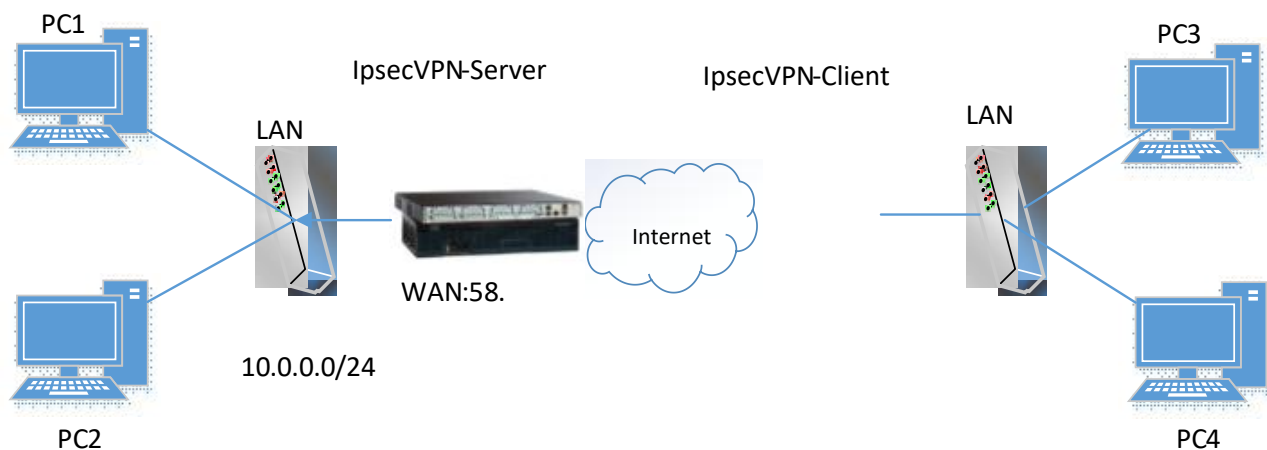
OK

OK

5.2 VPN Configuration Examples

5.2.1 IPsec VPN

IPsec VPN topology (server-side and client-side IKE and SA parameters must be configured the same).



IPsecVPN_Server:

Cisco 2811:

```

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

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

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

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

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

```

IPsec VPN_Client:

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

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

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

Tunnel

^ General Settings

Index:

Enable: ON OFF

Description:

Gateway: ?

Mode: v

Protocol: v

Local Subnet: ?

Remote Subnet: ?

Link Binding: v ?

^ IKE Settings

IKE Type: v

Negotiation Mode: v

Encryption Algorithm: v

Authentication Algorithm: v

IKE DH Group: v

Authentication Type: v

PSK Secret:

Local ID Type: v

Remote ID Type: v

IKE Lifetime: ?

SA Settings

Encryption Algorithm: 3DES

Authentication Algorithm: SHA1

PFS Group: DHgroup2

SA Lifetime: 28800

DPD Interval: 30

DPD Failures: 150

Advanced Settings

Enable Compression: OFF

Enable Forceencaps: OFF

Expert Options: []

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

The comparison between server and client is as below.

```

Router#enable
Router#conf t
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-IPSEC-MD5 transform
 ah-sha-hmac AH-IPSEC-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-aes-3des ESP transform using 3DES(EDE) cipher and AES 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
Router(config-if)#crypto map cry-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

```

Server (Cisco 2811)

Router IKE Settings

- Index: 1
- Enable: ON
- Description: []
- Gateway: 58.1.1.1
- Mode: Tunnel
- Protocol: ESP
- Local Subnet: 192.168.1.0/24
- Remote Subnet: 0.0.0.0/24
- Link Binding: Unspecified
- IKE Type: IKEv1
- Negotiation Mode: Main
- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- IKE DH Group: DHgroup2
- Authentication Type: PSK
- PSK Secret: ****
- Local ID Type: Default
- Remote ID Type: Default
- IKE Lifetime: 86400

Router SA Settings

- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- PFS Group: DHgroup2
- SA Lifetime: 28800
- DPD Interval: 30
- DPD Failures: 150

Advanced Settings

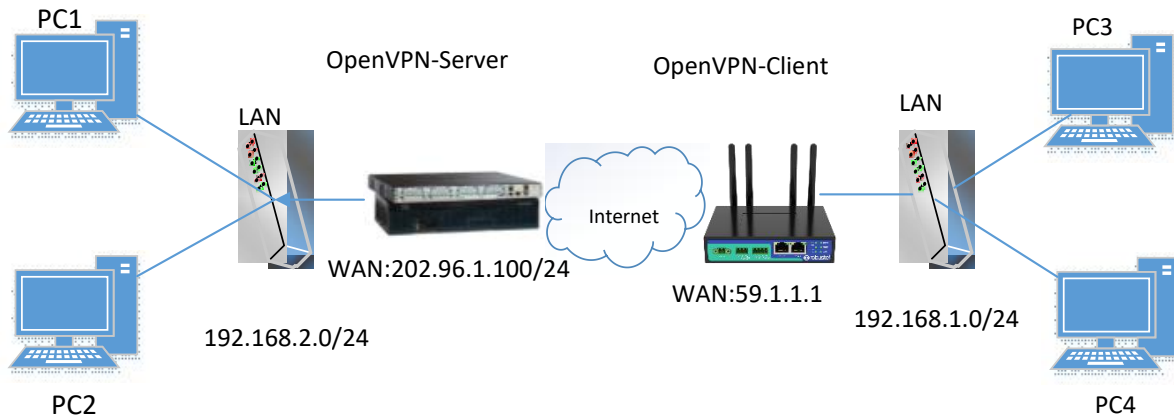
- Enable Compression: OFF
- Enable Forceencaps: OFF
- Expert Options: []

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

5.2.2 OpenVPN

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



OpenVPN_Server:

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

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

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

OpenVPN_Client:

Click “VPN > OpenVPN > OpenVPN” as below.

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

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

OpenVPN

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	client01
Mode	Client <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	UDP <input type="button" value="v"/>
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN <input type="button" value="v"/>
Authentication Type	X509CA <input type="button" value="v"/> <input type="button" value="?"/>
Encrypt Algorithm	BF <input type="button" value="v"/>
Authentication Algorithm	SHA1 <input type="button" value="v"/>
Renegotiation Interval	86400 <input type="button" value="?"/>
Keepalive Interval	20 <input type="button" value="?"/>
Keepalive Timeout	120 <input type="button" value="?"/>
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	3 <input type="button" value="v"/> <input type="button" value="?"/>

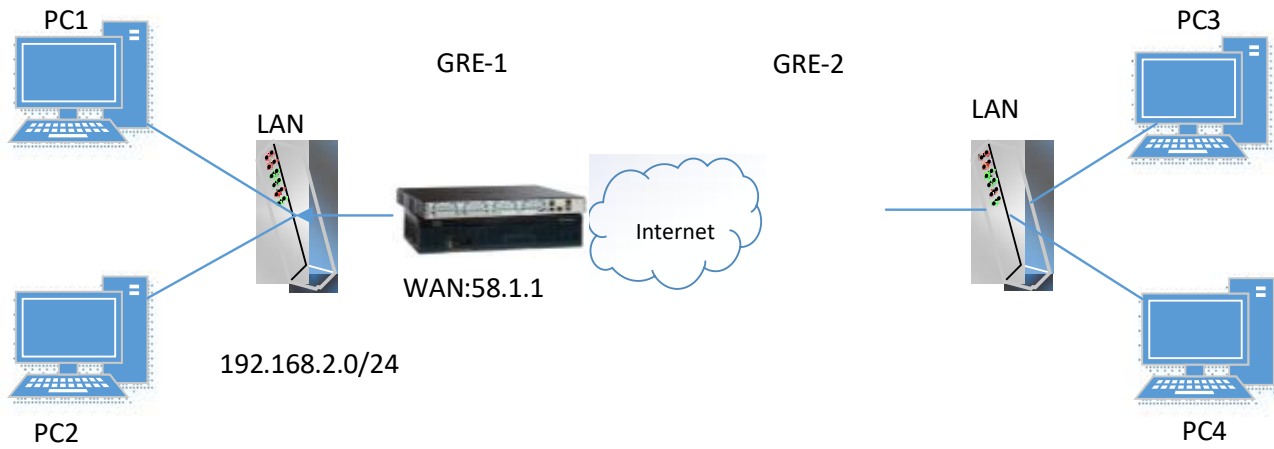
^ Advanced Settings

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

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

5.2.3 GRE VPN

GRE VPN topology



GRE-1:

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



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



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.

GRE

^ Tunnel Settings

Index

Enable ON OFF

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask/Prefix Length ?

Remote Virtual IP Address

Enable Default Route ON OFF

Enable NAT ON OFF

Secrets

Link Binding v ?

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

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

GRE	GRE
^ Tunnel Settings	^ Tunnel Settings
Index <input type="text" value="1"/>	Index <input type="text" value="1"/>
Enable <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	Enable <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description <input type="text" value="GRE-1"/>	Description <input type="text" value="GRE-2"/>
Remote IP Address <input type="text" value="58.1.1.1"/>	Remote IP Address <input type="text" value="59.1.1.1"/>
Local Virtual IP Address <input type="text" value="10.8.0.1"/>	Local Virtual IP Address <input type="text" value="10.8.0.2"/>
Local Virtual Netmask/Prefix Length <input type="text" value="255.255.255.0"/> ?	Local Virtual Netmask/Prefix Length <input type="text" value="255.255.255.0"/>
Remote Virtual IP Address <input type="text" value="10.8.0.2"/>	Remote Virtual IP Address <input type="text" value="10.8.0.1"/>
Enable Default Route <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	Enable Default Route <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	Enable NAT <input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets <input type="password" value="*****"/>	Secrets <input type="password" value="*****"/>
Link Binding <input type="text" value="Unspecified"/> v ?	Link Binding <input type="text" value="Unspecified"/> v ?

GRE-1 real public network IP address

GRE-1 real tunnlr IP address

GRE-2 real tunnlr IP address

GRE-2 real public network IP address

GRE-2 real tunnlr IP address

GRE-1 real tunnlr IP address

USE the same password for GRE-1 and GRE-2

USE the same password for GRE-1 and GRE-2

6 Introductions for CLI

6.1 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. After establishing a Telnet or SSH connection with the gateway, enter the login account and password (default admin/admin) to enter the configuration mode of the gateway, as shown below.

```
router login: admin
Password:
#
!           Comments
add        Add a list entry of configuration
clear      Clear statistics
config     Configuration operation
debug      Output debug information to the console
del        Delete a list entry of configuration
exit       Exit from the CLI
help       Display an overview of the CLI syntax
ovpn_cert_get Download OpenVPN certificate file via http or ftp
ping       Send messages to network hosts
reboot     Halt and perform a cold restart
set        Set system configuration
show       Show system configuration
status     Show running system information
tftpupdate Update firmware or configuration file using tftp
traceroute Print the route packets trace to network host
trigger    Trigger action
urlupdate  Update firmware via http or ftp
ver        Show version of firmware
```

```
#
```

Route login:

```
Gateway login: admin
```

```
Password: admin
```

```
#
```

CLI commands:

```
# ?
!           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
tracert	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

6.2 How to Configure the CLI

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

Commands /tips	Description
?	Typing a question mark “?” will show you the help information. eg. # config (Press ‘?’) config Configuration operation # config (Press spacebar +’?’) commit Save the configuration changes and take effect changed configuration save_and_apply Save the configuration changes and take effect changed configuration loaddefault Restore Factory Configuration
Ctrl+c	Press these two keys at the same time, except its “copy” function but also can be used for “break” out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
#config commit # config save_and_apply	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.

6.3 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 , if we need to see all please using "show running "
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.

6.4 Quick Start with Configuration Examples

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

Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = beta210414
firmware_version_full = "beta210414 (Rev 4034)"
kernel_version = 4.9.152
device_model = R2010
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 15 17:09:04 2021"
ram_usage = "77M Free/128M Total"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
firmware New firmware
config New configuration file
# tftpupdate firmware (space+?)
filename New file
# tftpupdate firmware filename ET8013-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new
firmware name
Downloading
Download success.
Upgrading
```

```
Upgrade success.      //Update succeed
# reboot              //Take effect after rebooting
Rebooting...
OK
```

Example 3: Set link-manager

```
# set
# set (space+?)
  cellular           Cellular
  ddns               DDNS
  dido              DIDO
  email             Email
  ethernet          Ethernet
  event            Event Management
  firewall          Firewall
  gre               GRE
  ip_passthrough    IP Passthrough
  ipsec            IPsec
  lan              Local Area Network
  link_manager      Link Manager
  ntp              NTP
  openvpn          OpenVPN
  reboot           Automatic Reboot
  route           Route
  serial_port      Serial
  sms             SMS
  ssh             SSH
  syslog          Syslog
  system          System
  user_management User Management
  web_server      Web Server

# set link_manager (space+?)
  primary_link      Primary Link
  backup_link       Backup Link
  backup_mode       BackSup Mode
  revert_interval   Revert Interval
  emergency_reboot  Emergency Reboot
  link              Link Settings
# set link_manager primary_link (space+?)
Enum Primary Link (wwan1/wan)
# set link_manager primary_link wwan1      //select "wwan1" as primary_link
OK                                          //setting succeed
#set link_manager link 1 (space+?)
  type              Type
```


desc	Description	
connection_type	Connection Type	
wwan	WWAN Settings	
static_addr	Static Address Settings	
pppoe	PPPoE Settings	
ping	Ping Settings	
nat_enable	NAT Enable	
mtu	MTU	
weight	Weight	
upload_bandwidth	Upload Bandwidth	
download_bandwidth	Download Bandwidth	
dns1_overridden	Overridden Primary DNS	
dns2_overridden	Overridden Secondary DNS	
debug_enable	Debug Enable	
verbose_debug_enable	Verbose Debug Enable	

```

# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan (space+?)
  auto_apn          Automatic APN Selection
  apn               APN
  username          Username
  password          Password
  dialup_number     Dialup Number
  auth_type         Authentication Type
  data_allowance    Data Allowance
  billing_day       Billing Day
# set link_manager link 1 wwan data_allowance 100           //enable cellular switch_by_data_traffic
OK                                                         //setting succeed
# set link_manager link 1 wwan billing_day 1                //setting specifies the day of month for billing
OK                                                         // setting succeed
...
# config save_and_apply
OK                                                         // save and apply current configuration, make you configuration effect

```

Example 4: Set Ethernet

```

# set Ethernet port_setting 2 port_assignment lan0         //Set Table 2 (eth1) to lan0
OK
# config save_and_apply                                   //setting succeed
OK

```

Example 5: Set LAN IP address

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
    netmask = 255.255.255.0
    mtu = 1500
    dhcp {
        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
        static_lease = ""
        expert_options = ""
        debug_enable = false
    }
    vlan_id = 0
}
#
# set lan (space+?)
network      Network Settings
multi_ip    Multiple IP Address Settings
# set lan network 1(space+?)
interface   Interface
ip          IP Address
netmask     Netmask
mtu         MTU
dhcp        DHCP Settings
Vlan_id     VLAN ID
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24           //set IP address for lan
OK                                           //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                           // save and apply current configuration, make you configuration effect
```

Example 6: CLI for setting Cellular

```
# show cellular all
sim {
    id = 1
    card = sim1
    phone_number = ""
    pin_code = ""
    extra_at_cmd = ""
    telnet_port = 0
    network_type = auto
    band_select_type = all
    band_settings {
        gsm_850 = false
        gsm_900 = false
        gsm_1800 = false
        gsm_1900 = false
        wcdma_800 = false
        wcdma_850 = false
        wcdma_900 = false
        wcdma_1900 = false
        wcdma_2100 = false
        wcdma_1700 = false
        wcdma_band19 = false
        lte_band1 = false
        lte_band2 = false
        lte_band3 = false
        lte_band4 = false
        lte_band5 = false
        lte_band7 = false
        lte_band8 = false
        lte_band13 = false
        lte_band17 = false
        lte_band18 = false
        lte_band19 = false
        lte_band20 = false
        lte_band21 = false
        lte_band25 = false
        lte_band28 = false
        lte_band31 = false
        lte_band38 = false
        lte_band39 = false
        lte_band40 = false
        lte_band41 = false
    }
    telit_band_settings {
```

```

    gsm_band = 900_and_1800
    wcdma_band = 1900
}
debug_enable = true
verbose_debug_enable = false
}
# set(space+space)
cellular      ddns      dido      email      ethernet
event         firewall  gre       ip_passthrough ipsec
l2tp          lan       link_manager ntp       openvpn
pptp          reboot    route     serial_port sms
ssh           syslog    system    user_management web_server
# set cellular(space+?)
sim SIM Settings
# set cellular sim(space+?)
Integer Index (1..1)

# set cellular sim 1(space+?)
card          SIM Card
phone_number  Phone Number
pin_code      PIN Code
extra_at_cmd  Extra AT Cmd
telnet_port   Telnet Port
network_type  Network Type
band_select_type Band Select Type
band_settings Band Settings
telit_band_settings Band Settings
debug_enable  Debug Enable
verbose_debug_enable Verbose Debug Enable
# set cellular sim 1 phone_number 18620435279
OK
...
# config save_and_apply
OK // save and apply current configuration, make you configuration effect

```

Glossary

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

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

Abbr.	Description
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.

Add: 501, Building 2, No. 63, Yong'an Avenue,
Huangpu District, Guangzhou, China 510660

Tel: 86-20-82321505

Email: support@robustel.com

Web: www.robustel.com