

RobustOS Software Manual



Guangzhou Robustel Co., Ltd. www.robustel.com



About this Document

This document provides web interface information of the RobustOS-based DTU, Router, and Gateway products, including function introduction and operation configuration.

Related Products

M1200, M1201 R1500, R1510, R1510 Lite, R1511, R1511P, R1520 R2010, R2011, R2110 R3000, R3000 Lite, R3000 Quad, R3000 LG, R3010 R5020, R5020 Lite R5010

Copyright©2024 Guangzhou Robustel Co., Ltd. All rights reserved.

Trademarks and Permissions

B robustel & robustels 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

The entire document cannot 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 mistaking use of this document.

Technical Support

Tel: 4009-897-791 Email: <u>support@robustel.com</u> Web: <u>www.robustel.com</u>





Document History

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

Date	Document Version	Firmware Version	Change Description
Aug. 1, 2022	V1.0.0	V5.0.0 or newer	1. Initial release.
Oct. 16, 2022	V1.1.0	V5.1.0 or newer	Added support for RobustOS V5.1.0 or newer.
Oct. 26, 2023	V5.2.0	V5.2.0 or newer	Added support for RobustOS V5.2.0 or newer.
July. 10, 2024	V5.3.0	V5.3.0 or newer	Added support for RobustOS V5.3.0 or newer.



Contents

1. Introduction	6
2. Initial Configuration	7
2.1 PC Configuration	7
2.2 Factory Default Settings	
2.3 Factory Reset	
2.4 Log in Your Device	
2.5 Control Panel	
3. WebUI Descriptions	14
3.1 Status	
3.1.1 System Information	14
3.1.2 Internet Status	
3.1.3 Modem Status	16
3.1.4 WiFi STA Status	
3.1.5 LAN Status	
3.2 Interface	
3.2.1 Link Manager	
3.2.2 LAN	
3.2.3 Ethernet	
3.2.4 Cellular	
3.2.5 Wi-Fi	
3.2.6 USB	69
3.2.7 DI/DO	
3.2.8 AI	75
3.2.9 Serial Port	76
3.2.10 Serial Redirector	
3.2.11 LoRa	
3.3 Packet Forwarders	
3.3.1 Basic Station	
3.3.2 Semtech UDP Forwarder	
3.4 Network	
3.4.1 Route	93
3.4.2 Firewall	94
3.4.3 IP Passthrough	
3.4.4 PPPoE Bridge	
3.5 VPN	
3.5.1 IPsec	
3.5.2 WireGuard	
3.5.3 OpenVPN	
3.5.4 GRE	
3.6 Services	
3.6.1 Syslog	
3.6.2 Event	
3.6.3 NTP	

10 robustel

3.6.4 SMS	
3.6.5 Email	147
3.6.6 DDNS	148
3.6.7 SSH	
3.6.8 Telephone	151
3.6.9 Ignition	153
3.6.10 GPS	153
3.6.11 Web Server	158
3.6.12 Advanced	159
3.6.13 Smart Roaming V2	
3.7 System	167
3.7.1 Debug	167
3.7.2 Update	
3.7.3 App Center	
3.7.4 Tools	
3.7.5 Profile	174
3.7.6 Access Control	
3.7.7 User Management	
3.7.8 Role Management	178
4. Configuration Examples	
4.1 Cellular	
4.1.1 Cellular Dial-Up	
4.1.2 SMS Remote Control	
4.2 VPN Configuration Examples	
4.2.1 IPsec VPN	
4.2.2 OpenVPN	190
4.2.3 GRE VPN	193
5. Introductions for CLI	
5.1 What Is CLI	
5.2 How to Configure the CLI	196
5.3 Commands Reference	197
5.4 Quick Start with Configuration Examples	
Example 1: Show the current version	197
Example 2: Update firmware via tftp	
Example 3: Set link-manager	
Example 4: Set Ethernet	199
Example 5: Set LAN IP address	
Example 6: CLI for setting Cellular	
Glossary	



1. Introduction

This software manual, used for all the RobustOS-based products including the DTU, Router, and Gateway products, provides web interface information (configuration and operation).

Please refer to the specific chapter accordingly, as hardware configurations or interfaces may vary on different models.

Related Product	M1200	M1201	R1510	R1510 Lite	R1511	R1520	R2010	R2011	R2110	R3000	R3000 Lite	R3000 Quad	R3000 LG	R3010	R5020	R5010
SIM Card	2	1	1	1	1	2	2	2	2	2	2	2	2	1	2	2
Ethernet	-	-	2	1	2	5	2	5	4	2	1	4	2	2	4	1
PoE PD	-	-	-	-	-	*	*	*	*	-	-	-	-	-	*	V
PoE PSE	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Wi-Fi	-	-	V	-	V	V	V	V	V	*	-	*	-	-	V	-
BLE	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-
GNSS	-	-	-	-	-	*	-	-	*	*	-	*	*	-	*	-
DI	2	-	V	-	-	V	V	-	V	2	-	-	2	-	V	-
DO	٧	-	٧	-	-	٧	V	-	٧	2	-	-	-	-	V	-
AI	-	-	-	-	-	٧	-	-	-	-	-	-	-	-	-	-
RS232	V	*	-	-	*	V	*	-	V	V	V	*	*	V	V	-
RS485	٧	*	-	-	*	٧	*	-	٧	٧	٧	*	*	٧	٧	-
USB Host	-	-	-	-	-	٧	-	-	٧	V	٧	٧	V	٧	V	V
RS422	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CAN	-	*	-	-	-	-	-	-	-	-	-	-	-	V	-	-
Voice (FXS)	-	-	-	-	-	-	-	-	-	-	-	-	-	V	-	-
MicroSD	-	-	-	-	-	-	-	-	٧	٧	-	٧	V	-	٧	-

Note: $\sqrt{}$ = *Supported, -* = *Unsupported, ** = *Optional*

About RobustOS

RobustOS is a Robustel self-developed and Linux-based operating system designed for Robustel devices. The RobustOS includes basic networking features and protocols providing customers excellent user experience. Meanwhile, Robustel offers a Software Development Kit (SDK) for partners and customers to allow additional customization by using C and C++. It also provides rich Apps to meet fragmented IoT market demands.



2. Initial Configuration

You can configure the device through the web browser, including Microsoft Edge, Google Chrome, Firefox, etc. A web browser is a standard application in the following operating systems: Ubuntu, macOS, Windows7/8/10/11, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the device, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC is equipped with an Ethernet port before connecting the device. 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 device. If you encounter any problems accessing the device 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 device.

2.1 PC Configuration

There are two ways to get an 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 device. Please refer to the steps below.

Here take **Windows 10** as an example. The configuration for Windows 7 newer is similar.

Find the Windows logo key

1.

(hereinafter referred to as Win key) of the keyboard, press Win + R, type

"Control" to run Control Panel. After opening the Control Panel, left-click on "View Network Status and Tasks".

Control Panel			100	×
$\leftrightarrow \rightarrow \cdots \uparrow$	> Control Panel >	✓ ♂ Search Control Panel		م
	Adjust your computer's settings	View by: Category 🔻		
	System and Security Review your computer's status Save backup copies of your files with File History Back up and Restore (Windows 7)	User Accounts Change account type Appearance and Personalisation		
	Network and Internet View network status and tasks Hardware and Sound View devices and printers Add a device	Clock and Region Change date, time or number formats Ease of Access		
	Adjust commonly used mobility settings Programs Uninstall a program	Let Windows suggest settings Optimise visual display		

2. After entering "Network and Sharing Center", click "Ethernet" connections status;

E Network and Sharing Centre				×
← → ✓ ↑ ¥ > Control Par	el > All Control Panel Items > Network and Sharing Centre	5 V		P
Control Panel Home	View your basic network information and set	t up connections		
Change adapter settings	View your active networks			
Change advanced sharing settings	Network 8 Private network	Access type: Internet Connections: Definition 2		
Media streaming options				
	Network 13	Access type: No Internet access		
	Public network	Connections: 📱 Test LAN		
	Change your networking settings			
	Set up a new connection or network Set up a broadband, dial-up or VPN connection,	or set up a router or access point.		
	Troubleshoot problems			
	Diagnose and repair network problems or get tro	ubleshooting information.		
See also				
Internet Options				
Windows Defender Firewall				

3. Click **Properties** in the window of **Local Area Connection status**.

eneral		
Connection —		
IPv4 Connec	tivity:	Internet
IPv6 Connec	tivity:	No Internet access
Media State:		Enabled
Duration:		13 days 05:40:54
Speed:		1.0 Gbps
D <u>e</u> tails		
	Sent —	Received
Activity	Sent — 828,675,176	— Received 2,751,829,674
Activity ———	828,675,176	all a

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



- 5. Two ways to configure the IP address of the computer.
 - (1) Auto obtain from the DHCP server, click "Obtain an IP address automatically";

	Protocol Version 4 (TCP/IPv4)				
General	Alternative Configuration				
this cap	n get IP settings assigned autor ability. Otherwise, you need to appropriate IP settings.				
<u>ام</u>	otain an IP address automatical	lly			
	e the following IP address:				
IP ac	ddress:		10	- e	
Subr	iet mask:		- 45	141	
Defa	ult gateway:				
	otain DNS server address autor	natically			
	e the following DNS server add				
Prefe	erred DNS server:				
<u>A</u> lter	native DNS server:		10		
V	alidate settings upon exit			Ad <u>v</u> an	ced
			ОК	_	Cancel



(2) Manually configure the PC with a static IP address on the same subnet as the device address, click and configure "Use the following IP address";

nternet Protocol Version 4 (TCP/	IPv4) Properties	×
General		
	automatically if your network supports eed to ask your network administrator	
O Obtain an IP address autom	atically	
• Use the following IP address	B	
IP address:	192.168.0.2	
Subnet mask:	255.255.255.0	
Default gateway:	192.168.0.1	
Obtain DNS server address a	automatically	
• Use the following DNS serve	r addresses:	
Preferred DNS server:	8.8.8.8	
Alternative DNS server:		
Ualidate settings upon exit	Ad <u>v</u> anced	
	OK Cance	4

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

2.2 Factory Default Settings

Before configuring your device, 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.
ETH1/2/3/4 ^(*)	192.168.0.1/255.255.255.0, LAN mode.
DHCP Server	Enabled

* There are differences in the number of ETH ports of different devices. For details, please refer to the product specification of the device.

2.3 Factory Reset

Function	Operation
Reboot	Press and hold the RST button for 2~5 seconds under the operating status.
Restore to default	Press and hold the RST button for 5 ~10 seconds under the operating status. The RUN
configuration	light flashes quickly, and then release the RST button, and the device will restore to the
	default configuration.
Restore to factory	Once the operation of restoring the default configuration is performed twice within one
configuration	minute, the device will restore to the factory default settings.



2.4 Log in Your Device

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

- 1. On your PC, launch a browser. e.g.: Microsoft Edge, Google Chrome, or Firefox, etc.
- From your web browser, type the IP address of the device into the address bar and press enter. The default IP address of the device is http://192.168.0.1/, though the actual address may vary.

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

	🙆 Ro	uter Web Manager	×	+
\leftarrow	С	▲ Not secure	192. <mark>16</mark> 8.	0.1/auth/login.html

3. On the login page, enter the username and password, choose the language, and then click **LOGIN**. Please check the information on the product label for the default username and password.

LE LE) robi	Jstel	
	1 admin		
	≙	_	
	LUGIN		



2.5 Control Panel

Brobuste Save & Apply | Reboot | Logout Username : admin ▲ It is strongly recommended to change the default password. Status Status System Information Device Model R1520-4L Global Interface System Uptime 0 days, 00:03:48 Network System Time Thu Jul 4 11:38:03 2024 (NTP not updated) VPN RAM Usage 68M Free/128M Total Services Firmware Version 5.3.0 (542cd9a) System Hardware Version 1.2 Kernel Version 4.9.152 Serial Number 05670123100510 A Internet Status Uptime Active IPv4 Link **IPv4 Address** IPv4 Gateway **IPv4 DNS** Active IPv6 Link **IPv6 Address** IPv6 Gateway IPv6 DNS ^ Modem Status Modem Model EG25 Registration Network Provider Network Type Signal Strength ~ WiFi STA Status BSSID Channel SSID RSSI A LAN Status IP Address 192.168.0.1/255.255.255.0 Active IPv6 Address Local IPv6 Address fe80::36fa:40ff:fe25:31f2/64 MAC Address 34:FA:40:25:31:F2 Copyright © 2024 Robustel Technologies. All rights reserved

After logging in, the home page of the web interface is displayed. Here take R1520 for example.

×

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

Using the default username and password to log in to the device, the page will pop up in the following tab

 \triangle It is strongly recommended to change the default password.

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

button to close the notification. To change your username and/or password, see 3.7.7 System > User

Management.

Orobustel	Save & Apply Reboot Logout Username : admin
igtarrow It is strongly recommended to change the default	password. ×
Status	

Control Panel		
Item	Description	Button
Save & Apply	Click to save the current configuration into the device's flash and apply	Save & Apply
	the modification on every configuration page, to modify taking effect.	
Reboot	Click to reboot the device. If the Reboot button is yellow, it means that	Reboot
	some completed configurations will take effect only after the reboot.	
Logout	Click to log the current user out safely. After logging out, it will switch to	Logout
	the login page. Shut down the web page directly without logout, the next	
	one can log in web on this browser without a password before timeout.	
Submit	Click to save the modification on the current configuration page.	Submit
Cancel	Click to cancel the modification on the current configuration page.	Cancel
Username	The name of the currently logged in account.	-

Note: The steps how to modify the configuration are as below:

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

3. WebUI Descriptions

3.1 Status

3.1.1 System Information

This page allows you to view the System Information, Internet Status, WiFi STA status, and LAN Status of your device.

System Information		
	Device Model	R1520-4L Global
	System Uptime	0 days, 00:01:05
	System Time	Tue Jun 18 16:26:02 2024 (NTP not updated)
	RAM Usage	64M Free/128M Total
	Firmware Version	5.3.0 (542cd9a)
	Hardware Version	1.2
	Kernel Version	4.9.152
	Serial Number	05670123100510

System Information		
Item	Description	
Device Model	Show model name of your device.	
System Uptime	Show device uptime.	
System Time	Show current system time.	
RAM Usage	Show free memory and the total memory.	
Firmware Version	Show firmware version running on the device.	
Hardware Version	Show current hardware version.	
Kernel Version	Show current kernel version.	
Serial Number	Show Serial Number of the device.	



3.1.2 Internet Status

∧ Internet Status	
Uptime	
Active IPv4 Link	
IPv4 Address	
IPv4 Gateway	
IPv4 DNS	
Active IPv6 Link	
IPv6 Address	
IPv6 Gateway	
IPv6 DNS	

This page shows the device's Internet status information.

Internet Status		
Item	Description	
Uptime	Show current amount of time the link has been connected.	
Active IPv4 Link	Show IPv4 currently used links: WWAN1, WWAN2, or WAN.	
IPv4 Address	Show IPv4 address of active link.	
IPv4 Gateway	Show IPv4 gateway address of active link.	
IPv4 DNS	Show IPv4 current DNS server address.	
Active IPv6 Link	Show IPv6 currently used links: WWAN1, WWAN2, or WAN.	
IPv6 Address	Show IPv6 address of active link.	
IPv6 Gateway	Show IPv6 gateway address of active link.	
IPv6 DNS	Show IPv6 current DNS server address.	



3.1.3 Modem Status

This page shows the device's Modem information.

 Modem Status 	
Modem Model	EG25
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	LTE
Signal Strength	16 (-81dBm)

Modem Status		
Item	Description	
Modem Model	Show model of cellular module.	
Registration	Show current network status.	
Network Provider	Show name of network provider.	
Network Type	Show current network service type.	
Signal Strength	Show the values of signal strength.	

3.1.4 WiFi STA Status

This page shows the basic information about WiFi stations.

∧ WiFi STA Status	
BSSID	20:65:8e:ba:51:91
Channel	60
SSID	Robustel-Visitor
RSSI	-67

WiFi STA Status		
Item	Description	
BSSID	Show the unique basic service identifier of the wireless access point the device is	
	connected to.	
Channel	Show the current channel number of the device connected to the wireless access	
	point, corresponding to the wireless channel.	
SSID	Show the service set identifier of the wireless access point the device is connected.	
RSSI	Show the wireless signal strength of the device connected to the wireless access	
	point, unit: dBm.	



3.1.5 LAN Status

This page shows the devices' LAN status

∧ LAN Status		
	IP Address	192.168.0.1/255.255.255.0
	Active IPv6 Address	
	Local IPv6 Address	fe80::36fa:40ff:fe25:31f2/64
	MAC Address	34:FA:40:25:31:F2

LAN Status		
Item	Description	
IP Address	Show IP address and the netmask of the LAN.	
Active IPv6 Address	Show active IPv6 address of the LAN.	
Local IPv6 Address	Show local IPv6 address of the LAN.	
MAC Address	Show MAC address of the LAN.	

3.2 Interface

3.2.1 Link Manager

This page allows you to manage link connections. The Link management function supports the selection of single/dual links. At the same time, each link supports the configuration of the link detection function to keep the network connection always online.

Link Manager	Status	
∧ General Setti	ngs	
	Primary Link	WWAN1 🤍 🍞
	Backup Link	None v
	Emergency Reboot	ON OFF ?

General Settings @ Link Manager		
Item	Description	Default
Primary Link	 Select from "WWAN1", "WWAN2", "WAN" or "WLAN". WWAN1: Select SIM1 as the primary wireless link. 	WWAN1
	WWAN2: Select SIM2 as the primary wireless link.	
	 WAN: Select WAN Ethernet port as the primary wired link. WLAN: Select WLAN as the primary wireless link. 	
	Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer	
	to <u>3.2.5 Wi-Fi</u> .	

General Settings @ Link Manager		
Item	Description	Default
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN", or "None".	None
	WWAN1: Select SIM1 as the backup wireless link.	
	 WWAN2: Select SIM2 as the backup wireless link. 	
	WAN: Select WAN Ethernet port as the backup wired link.	
	WLAN: Select WLAN as the backup wireless link.	
	Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer	
	to <u>3.2.5 Wi-Fi</u> .	
	None: No backup link.	
Backup Mode	Select from "Cold Backup", "Warm Backup", or "Load Balancing".	Cold
	Cold Backup: The inactive link is offline on standby.	Backup
	• Warm Backup: The inactive link is online on standby. It is not available	
	for dual SIM backup.	
	• Load Balancing: Use two links simultaneously. It is not available for dual	
	SIM backup.	
	Note: Backup Mode is available only Backup Link isn't None.	
Revert Interval	Specify number of minutes that elapses before the primary link is checked if	0
	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.	
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the	OFF
	whole system if no links are available.	

Note: Click ⑦ for help.

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

Index	Туре	Description	IPv4 Connection Type	IPv6 Connection Type	
1	WWAN1		DHCP	SLAAC	
2	WWAN2		DHCP	SLAAC	
3	WLAN		DHCP	SLAAC	
4	WAN		DHCP	SLAAC	

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

WWAN1/WWAN2

This window supports enabling or disabling IPV6 functionality. After disabling, IPV4 can still be used for networking. IPV6 is disabled by default.



Link Manager	
∧ General Settings	
Index	1
Туре	WWAN1 V
Description	
IPv6 Enable	OFF

The window is displayed below when enabling the "Automatic APN Selection" option.

∧ WWAN Settings	
Automatic APN Selection	ON OFF
Dialup Number	*99***1#
Authentication Type	Auto
PPP Preferred	ON OFF 7
Switch SIM By Data Allowance	ON OFF 0
Data Allowance	0
Billing Day	1

The window is displayed below when disabling the "Automatic APN Selection" option.

∧ WWAN Settings	
Automatic APN Selection	OFF
APN	internet
Username	
Password	•••••
Dialup Number	*99***1 #
Authentication Type	Auto
PPP Preferred	OFF 0
Switch SIM By Data Allowance	ON OFF 3
Data Allowance	0 7
Billing Day	1 🦻



Ping Detection Setti	ings		?
	Enable	ON OFF	
	IPV4 Primary Server	8.8.8.8	
	IPv4 Secondary Server	114.114.114	
	IPv6 Primary Server	2001:4860:4860::888	
	IPv6 Secondary Server	2400:3200::1	
	Interval	300	0
	Retry Interval	5	0
	Timeout	3	0
	Timeout unit	Second(s) v	
	Max Ping Tries	3	0
∧ Advanced Settings			
	NAT Enable	ON OFF	
	Conntrack Flush	ON OFF	
	Auto MTU For WWAN	ON OFF	
	Upload Bandwidth	10000	3
	Download Bandwidth	10000	

Overrided Primary DNS

Verbose Debug Enable

Debug Enable

Overrided Secondary DNS

Overrided IPv6 Primary DNS

Overrided IPv6 Secondary DNS

Link Settings (WWAN)			
Item Description		Default	
General Settings			
Index	Indicate ordinal of the list.		
Туре	Show type of the link.	WWAN1	
Description	Enter a description for this link.	Null	
IPv6 Enable	Click the toggle button to enable/disable the "IPv6 Enable" option. After enabling, IPV4 can still be used for networking.	OFF	

ON

OFF



Item	Description	Default
	WWAN Settings	
Automatic APN	Click the toggle button to enable/disable the "Automatic APN Selection"	ON
Selection	option. After enabling, the device will recognize the APN (Access Point	
	Name) automatically. Alternatively, you can disable this option and	
	manually add the APN (Access Point Name).	
APN	Enter APN (Access Point Name) for cellular dial-up connection, provided by	Internet
	the local ISP.	
Username	Enter username for cellular dial-up connection, provided by the local ISP.	Null
Password	Enter password for cellular dial-up connection, provided by the local ISP.	Null
Dialup Number	Enter dial-up number for the 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	Click the toggle button to enable/disable this option. After enabling, it will	OFF
Allowance	switch to another SIM when the data limit is reached.	
	Note: Only used for dual-SIM backup.	
Data Allowance	Set the monthly data traffic limitation. The system will record the data	0
	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.	
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated	1
	from that day.	
	Ping Detection Settings	1
Enable	Click the toggle button to enable/disable the ping detection mechanism, a	ON
	keepalive policy of the device.	
IPv4 Primary Server	The device will ping this primary address/domain name to check if the	8.8.8.8
	current IPv4 connectivity is active.	
IPv4 Secondary Server	The device will ping this secondary address/domain name to check if the	114.114.11
	current IPv4 connectivity is active.	4.114
IPv6 Primary Server	The device will ping this primary address/domain name to check if the	2001:4860:
	current IPv6 connectivity is active.	4860::8888
IPv6 Secondary Server	The device will ping this secondary address/domain name to check if the	2400:3200:
	current IPv6 connectivity is active.	:1
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping fails, the device will ping again every	5
	retry interval.	
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms).	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the	3
	max continuous ping tries reached.	
	Advanced Settings	



Link Settings (WWAN)			
Item	Description	Default	
Conntrack Flush	Click the toggle button to enable/disable clearing connection tracking	ON	
	information in the conntrack table when the link is established.		
	Note: This option is only available when "Enable NAT" is ON.		
Auto MTU For WWAN	Click the toggle button to enable/disable Auto MTU feature for WWAN.	ON	
MTU	Set the Maximum Transmission Unit.	1500	
	Note: MTU is available only "Auto MTU For WWAN" is OFF.		
Upload Bandwidth	Set upload bandwidth used for QoS, measured in kbps.	10000	
Download Bandwidth	Set download bandwidth used for QoS, measured in kbps.	10000	
Overrided Primary	Define primary IPv4 DNS server address used by the link.	Null	
DNS			
Overrided Secondary	Define secondary IPv4 DNS server address used by the link.	Null	
DNS			
Overrided IPv6	Define primary IPv6 DNS server address used by the link.	Null	
Primary DNS			
Overrided IPv6	Define secondary IPv6 DNS server address used by the link.	Null	
Secondary DNS			
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging	ON	
	information output.		
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose	OFF	
	debugging information output.		



WAN

For IPv4: The device will obtain IP automatically from DHCP server when applying "DHCP".

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	SLAAC V

The window is displayed below when choosing "Static" as IPv4 connection type.

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	Static
IPv6 Connection Type	SLAAC
✓ WAN Settings	
A Static Address Settings A	
IP Address	
Gateway	
Primary DNS	
Secondary DNS	



The window is displayed below when choosing "PPPoE" as IPv4 connection type.

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	PPPoE v
IPv6 Connection Type	SLAAC
✓ WAN Settings	
∧ PPPoE Settings	
Username	
Password	
Authentication Type	Auto
PPP Expert Options	

For IPv6: The device will obtain IPv6 address/prefix automatically from SLAAC protocol when applying "SLAAC". And also can obtain an IPv6 address/prefix through the DHCPv6 protocol when applying "DHCPv6"

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	SLAAC

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	DHCPv6



The window is displayed below when choosing "Static" as IPv6 connection type.

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	Static
✓ WAN Settings	
A IPv6 Static Address Settings	
IPv6 Address	
IPv6 Gateway	
IPv6 Primary DNS	
IPv6 Secondary DNS	

The window is displayed below when choosing "PPPoE" as IPv6 connection type.

∧ General Settings	
Index	4
Туре	WAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP
IPv6 Connection Type	PPPoE
Address Mode	SLAAC V
∧ WAN Settings	
Data Allowance	200000
Traffic Statistics Reset Date	



? Ping Detection Settings Enable ON **IPV4 Primary Server** 8.8.8.8 **IPv4 Secondary Server** 1.2.4.8 **IPv6 Primary Server** 2001:4860:4860::8888 IPv6 Secondary Server 2400:3200::1 1 Interval 300 1 **Retry Interval** 5 3 ? Timeout **Timeout unit** Second(s) v 1 3 **Max Ping Tries**

Advanced Settings

NAT Enable	ON OF
Conntrack Flush	
мти	1500
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON ON
Verbose Debug Enable	OFF

Link Settings (WAN)		
Item	Description	Default
General Settings		
Index	Indicate ordinal of the list.	
Туре	Show type of the link.	WAN
Description	Enter a description for this link.	Null
IPv6 Enable	Click the toggle button to enable/disable the "IPv6 Enable" option.	OFF
IPv4 Connection Type	Select "DHCP", "Static" or "PPPoE".	DHCP



IPv6 Connection Type	Select "SLAAC", "DHCPv6", "Static" or "PPPoE".	SLAAC
Address Mode	When "IPv6 Connection Type" is set to "PPPoE", an "Address mode" setting	SLAAC
	item will automatically appear in the general settings. It supports selection	
	from a dropdown menu, allowing you to choose 'SLAAC' or 'DHCPv6'.	
	Static Address Settings	
IP Address	Set IP address with Netmask which can access the Internet.	Null
	IP address with Netmask, e.g., 192.168.1.1/24	
Gateway	Set gateway address of the WAN port.	Null
Primary DNS	Set primary DNS address.	Null
Secondary DNS	Set secondary DNS address.	Null
	IPv6 Static Address Settings	
IPv6 Address	Set a static IPv6 address, e.g., 2521:da8:202:10::20/64	Null
IPv6 Gateway	Set a IPv6 gateway address of the WAN port.	Null
IPv6 Primary DNS	Set a IPv6 primary DNS address.	Null
IPv6 Secondary DNS	Set a IPv6 secondary DNS address.	Null
	PPPoE Settings	
Username	Enter username provided by your Internet Service Provider.	Null
Password	Enter password provided by your Internet Service Provider.	Null
Authentication Type	Select from "Auto", "PAP" or "CHAP" as the local ISP requires.	Auto
PPP Expert Options	Enter PPP Expert options used for PPPoE dialup. You can enter some other	Null
	PPP dial strings in this field. Each string can be separated by a semicolon.	
	WAN Settings	1
Data Allowance	Set monthly data traffic limitation. The system will record the data traffic	200000
	statistics when data traffic limitation (MB) is specified. The traffic record	
	will be displayed in Interface > Link Manager > Status > WAN Data Usage	
	Statistics. 0 means disable data traffic record.	
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated	1
	from that day.	
	Ping Detection Settings	
Enable	Click the toggle button to enable/disable the ping detection mechanism, a	ON
	keepalive policy of the device.	
IPv4 Primary Server	The device will ping this primary address/domain name to check if the	8.8.8.8
	current connectivity is active.	
IPv4 Secondary Server	The device will ping this secondary address/domain name to check if the	114.114.11
	current connectivity is active.	4.114
IPv6 Primary Server	The device will ping the IPv6 secondaryd address/domain name to check if	2001:4860:
	the current connectivity is active. It can be configured to be empty, which	4860::8888
	means no ping detection will be performed.	
IPv6 Secondary Server	The device will ping the IPv6 secondaryd address/domain name to check if	2400:3200:
	the current connectivity is active. It can be configured to be empty, which	:1
	means no ping detection will be performed.	
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping fails, the device will ping again every	5
	retry interval.	
Timeout	Set ping timeout.	3



12 robuste



WLAN

The device will obtain IP address automatically from the WLAN AP when applied "DHCP" as the connection type. The specific parameter configuration of SSID is shown below.

Link Manager	
∧ General Settings	
Index	3
Туре	WLAN
Description	
IPv6 Enable	ON OFF
IPv4 Connection Type	DHCP
∧ WLAN Settings	
SSID	router
Connect to Hidden SSID	OFF
Password	
Data Allowance	200000 🝞
Traffic Statistics Reset Date	

The window is displayed below when choosing "Static" as IPv4 connection type.

Link Manager			
∧ General Settings			
	Index 3		
	Type WLAN	×.	
D	escription		
IP	v6 Enable OF	F	
IPv4 Conne	ction Type Static	×	
✓ WLAN Settings			
 Static Address Settings 			
I	P Address	?	
	Gateway		
Pri	mary DNS		
Secon	ndary DNS		

Ping Detection Settings		7
Enable	ON OT	
IPV4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114	
IPv6 Primary Server	2001:4860:4860::888	
IPv6 Secondary Server	2400:3200::1	
Interval	300	0
Retry Interval	5	0
Timeout	3	0
Timeout unit	Second(s)	
Max Ping Tries	3	1

Advanced Settings

NAT Enable	ON OFF
Conntrack Flush	
мти	1500
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Overrided IPv6 Primary DNS	
Overrided IPv6 Secondary DNS	
Debug Enable	ON OFF
Verbose Debug Enable	OFF

Link Settings (WLAN)				
Item	Default			
General Settings				
Index	Indicate ordinal of list.			
Туре	Show type of the link.	WLAN		
Description	Enter a description for this link.	Null		
IPv6 Enable	Click the toggle button to enable/disable this option.	OFF		

10 robustel







Upload Bandwidth	Enter upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter download bandwidth used for QoS, measured in kbps.	10000
Overrided Primary DNS	Define a primary DNS server address used by the link.	Null
Overrided Secondary	Define a secondary DNS server address for the link.	Null
DNS		
Overrided IPv6 Primary	Define a primary DNS server address used by the link.	Null
DNS		
Overrided IPv6	Define a secondary DNS server address for the link.	Null
Secondary DNS		
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging	ON
	information output.	
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose	OFF
	debugging information output.	



Status

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

Link Manag	jer i	Status		due' =	
Link Sta	tus				•••
Index	IPv4 Link	IPv6 Link	Status	Uptime	
1	WWAN1	NONE	Connected	0 days, 00:10:09	~

Click the right-most button **w**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.

Index	IPv4 Link	IPv6 Link	Statu	s Uptime	
1	WWAN1	NONE	Connec	ted 0 days, 00:10:09	^
			Index	1	
		IP	v4 Link	WWAN1	
		IP	v6 Link	NONE	
			Status	Connected	
		IPv4 In	terface	wwan	
		IPv6 In	terface	none	
			Uptime	0 days, 00:10:09	
		IPv4 A	ddress	10.149.72.11/255.255.255.248	
		IPv4 G	ateway	10.149.72.12	
			мти	1500	
		IP	v4 DNS	172.20.161.2 172.20.164.2	
		RX	Packets	4599	
		TX	Packets	2806	
		R	X Bytes	4599569	
		T	X Bytes	418388	



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

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

NUMB WAN Data Usage Statistics	0
WAN Monthly Stats	Clear

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

3.2.2 LAN

This section allows you to set the related parameters for the LAN port. There may be multiple Ethernet ports in the device, and at least one LAN port must be assigned as lan0 with its or their default IP 192.168.0.1/255.255.255.0.

Note:

- 1) R3000 Lite has only one Ethernet port which can only be assigned as LAN.
- 2) R1510 Lite has only one Ethernet port which can only be assigned as LAN.
- 3) R1511 Lite has only one Ethernet port which can only be assigned as LAN.

LAN

LAN	4	Multiple IP	Tagge	d VLAN	Status	
∧ Netwo	ork Setting	gs				?
Index	Interface	IPv4 Address	Netmask	VLAN ID		+
1	lan0	192.168.0.1	255.255.255.0	0		⊠ ×
^ DHCP	Static Lea	ise Settings				
Index	Interface	MAC	IPv4	Address		+

Note: The lan0 cannot be deleted.

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



∧ General Settings					
Index	1				
Interface	lan0 v				
IPv4 Address	192.168.0.1				
Netmask	255.255.255.0				
IPv6 Address Mode	Delegated				
IPv6 Address Allocation Type	SLAAC				
мти	1500				

The window is displayed below when choosing "Static" as IPv6 Address Mode.

∧ General Settings	
Index	1
Interface	lan0 v
IPv4 Address	192.168.0.1
Netmask	255.255.255.0
IPv6 Address Mode	Static
IPv6 Address Prefix	
NAT66	ON OFF
IPv6 Address Allocation Type	SLAAC
мти	1500

General Settings @ LAN						
Item	Item Description					
Index	Indicate ordinal of list.					
Interface	Show editing port. The lan1 is available only if it was selected by one of	lan0				
	ETH0~ETHn in Ethernet > Ports > Port Settings.					
IPv4 Address	Set IP address of the LAN port.	192.168.0.1				
Netmask	Set Netmask of the LAN port.	255.255.255.0				
IPv6 Address	Set IPV6 address mode. Options include "Delegated" or "Static".	SLAAC				
Mode						
IPv6 Address	Set IPV6 adress prefix.	Null				
Prefix						
NAT66	Click the toggle button to enable/disable this option.	ON				
IPv6 Address	Set IPV6 address allocation method. Options include "SLAAC", "DHCPv6" or	SLAAC				
Allocation	"Disabled".					

Туре		
MTU	Enter Maximum Transmission Unit.	1500

The window is displayed below when choosing "DHCPv6" as IPv6 Address Allocation.

∧ DHCPv6 Settings			
IPv6 Pool Start	1000	0	
IPv6 Pool End	2000	0	
Primary DNS			
Secondary DNS			
Lease Time	120	?	

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

∧ DHCPv4 Settings	
Enable	ON OFF
Mode	Server
IP Pool Start	192.168.0.2
IP Pool End	192.168.0.100
Subnet Mask	255.255.255.0
Gateway	
Primary DNS	
Secondary DNS	
WINS Server	
Lease Time	120
Advanced Settings	
Expert Options	
Debug Enable	ON OFF

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

Orobustel


DHCPv4 Settings	
Enable	ON OFF
Mode	Relay
DHCPv4 Server For Relay	

Advanced Settings		
	Debug Enable ON OFF	

LAN						
Item	Description	Default				
DHCPv4 Settings @ Server Mode						
Enable	Click the toggle button to enable/disable the DHCP function.	ON				
Mode	Select "Server" or "Relay".	Server				
	Server: Lease IP address to DHCP clients that have been					
	connected to LAN port					
	• Relay: The device can be a DHCP Relay, which will provide a relay					
	tunnel to solve the problem that DHCP Client and DHCP Server					
	are not in the same subnet					
DHCPv4 Server For	Define the DHCPv4 Server For Relay.	Null				
Relay @ Relay mode						
IP Pool Start	Define the beginning of the pool of IP addresses that will be leased to	192.168.0.2				
	DHCP clients.					
IP Pool End	Define the end of the pool of IP addresses that will be leased to DHCP	192.168.0.100				
	clients.					
Subnet Mask	Define the subnet mask of the IP address obtained by DHCP clients	255.255.255.0				
	from the DHCP server.					
Gateway	Define gateway address assigned by the DHCP server to the clients,	Null				
	which must be on the same network segment as the DHCP address					
	pool.					
Primary DNS	Define primary DNS server address assigned by the DHCP server to the	Null				
	clients.					
Secondary DNS	Define secondary DNS server address assigned by the DHCP server to	Null				
	the clients.					
WINS Server	Define Windows Internet Naming Service obtained by DHCP clients	Null				
	from DHCP server.					
Lease Time	Set a lease time in which the client can use the IP address obtained	120				
	from the DHCP server, measured in seconds.					
	DHCPv6 Settings					
IPv6 Pool Start	Define the beginning of the physical address pool of IP addresses that	1000				
	will be leased to DHCP clients.					



+

LAN						
Item	Description	Default				
IPv6 Pool End	Define the end of the physical address pool of IP addresses that will be	2000				
	leased to DHCP clients.					
Primary DNS	Define IPv6 primary DNS server address assigned by the DHCP server	Null				
	to the clients.					
Secondary DNS	Define IPv6 secondary DNS server address assigned by the DHCP	Null				
	server to the clients.					
Lease Time	Set a lease time in which the client can use the IPv6 address obtained	120				
	from the DHCP server, measured in seconds.					
	Advanced Settings					
Expert Options	Enter some other options of the DHCP server in this field.	Null				
	format: config-desc;config-desc, e.g. log-DHCP;quiet-DHCP					
Debug Enable	Click the toggle button to enable/disable this option. Enable DHCP	OFF				
	information output.					

A DHCP Static Lease Settings
 Index Interface MAC

IPv4 Address

You can click + to add a new MAC and IP from the pop-up window in DHCP Static Lease Settings.

LAN	ц =	
∧ General Settings		
Index	1	
Interface	lan0 v	
MAC		0
IPv4 Address		0
		Submit Close

LAN					
Item	Default				
General Settings					
MAC	Enter MAC address for static lease.	Null			
IPv4 Address	Enter IP address for static lease.	Null			

Multiple IP

LAI	N N	Multiple IP	Tagged VLAN	Status	
∧ Multip	ole IP Setti	ngs			
Index	Interface	IPv4 Address	Netmask		+



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

click 🗹 to edit the multiple IP of the LAN port.

Multiple IP		
∧ IP Settings		
Index	1	
Interface	lan0 v	
IPv4 Address		
Netmask		
		Submit Close

IP Settings					
Item Description Defau					
Index	Display index list.				
Interface	Show editing port.				
IPv4 Address	Set IP addresses of the LAN port.	Null			
Netmask	Set Netmask of the LAN port.	Null			

Tagged VLAN

LAN		Multiple I	P	Tagged VLAN	Status	
~ VLAN S	Settings					
Index	Enable	Interface	VID	IPv4 Address	Netmask	+

You may click + to add a VLAN to the LAN port or click \times to delete the VLAN of the LAN port. Now, click \square to edit the VLAN of the LAN port.

Tagged VLAN	
VLAN Settings	
Index	1
Enable	ON OFF
Interface	lan0 v
VID	100
IPv4 Address	
Netmask	
	Submit Close



VLAN Settings					
Item	Default				
Index	Display index list.				
Enable	Click the toggle button to enable/disable the Tagged VLAN function.	ON			
Interface	Show editing port.				
VID	Set VLAN ID of the LAN port. Values range from 1 to 4094	100			
IPv4 Address	Set IP address of the VLAN.	Null			
Netmask	Set Netmask of the VLAN.	Null			

Status

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

Index	Interface	IP A	ddress	Active IPv6	Address		
1	lan0		255.255.255	Active II vo	Address		~
∧ Conne	cted Device	es					
Index	IP A	ddress	MAC	Address	Interface	Inactive Time	
1	192.	168.0.7	20:7B:D2	2:BC:AC:81	lan0	0s	~
~ DHCP	Lease Tabl	e					
Index	IP A	ddress	MAC Addr	ess or IAID	Interface	Expired Time	
1	192.	168.0.7	20:7b:d	2:bc:ac:81	lan0	0 days, 01:21:45	~

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

∧ Interfa	ce Status		
Index	Interface	IP Address	Active IPv6 Address
1	lan0	192.168.0.1/255.255.255	^
		Index	1
		Interface	lan0
		IP Address	192.168.0.1/255.255.255.0
		Local IPv6 Address	fe80::36fa:40ff:fe25:31f2/64
		MAC Address	34:FA:40:25:31:F2
		RX Packets	32237
		TX Packets	31637
		RX Bytes	3729025
		TX Bytes	15431706

Connected Devices

Index	IP Address	MAG	C Address	Interface	Inactive Time	
1	192.168.0.7	20:7B:	D2:BC:AC:81	lan0	0s	^
		Index	1			
		IP Address	192.168.0.7			
		MAC Address	20:7B:D2:BC:A	AC:81		
		Interface	lan0			
∧ DHCP Lea	ise Table	Inactive Time	Os			
Index	IP Address	MAC Ad	dress or IAID	Interface	Expired Time	
		MAC Ad		Interface lan0	Expired Time 0 days, 01:21:45	^
Index	IP Address	MAC Ad	dress or IAID :d2:bc:ac:81		175	^
Index	IP Address	MAC Ad 20:7b Index	dress or IAID :d2:bc:ac:81		175	^
Index	IP Address 192.168.0.7	MAC Ad 20:7b Index	dress or IAID :d2:bc:ac:81 1 192.168.0.7	lan0	175	^
Index	IP Address 192.168.0.7	MAC Ad 20:7b Index IP Address	dress or IAID :d2:bc:ac:81 1 192.168.0.7	lan0	175	^

3.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There may be multi-Ethernet ports in the device. The ETHO in the device can be configured as either a WAN port or LAN port, while other Ethernet port(s) can only be configured as LAN ports. The default settings of all Ethernet ports are lan0 and their default IP is 192.168.0.1/255.255.255.0.

Note:

- 1) R3000 Lite has only one Ethernet port which can only be configured as LAN.
- 2) R1510 Lite has only one Ethernet port which can only be configured as LAN.
- 3) R1511 Lite has only one Ethernet port which can only be configured as LAN.

Ports		Status			
• Port Se	ettings				?
Index	Port	Port Assignment	Port Enable	Port Speed	
1	eth0	wan	true	Auto Negotiation	
2	eth1	lan0	true	Auto Negotiation	
3	eth2	lan0	true	Auto Negotiation	
4	eth3	lan0	true	Auto Negotiation	
5	eth4	lan0	true	Auto Negotiation	



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

Ports	Gaus & Linds Bake
A Port Settings	
Index	1
Port	eth0 v
Port Assignment	wan v 😨
Port Enable	ON OFF ?
Port Speed	Auto Negotiation v
VLAN Tag Enable	ON OFF
	Submit Close

Port Settings					
Item	Description	Default			
Index	Indicate ordinal of list.				
Port	Show editing port, read-only.				
Dort Assignment	Choose Ethernet port type, such as a WAN port or LAN port. When setting the	lan0			
Port Assignment	port as a LAN port, you can click the drop-down list to select "lan0" or "lan1".	lan0			
Port Enable	ort Enable or disable the port.				
Port Speed	Specify part speed	Auto			
(Optional)	Specify port speed.	Negotiation			
PoE Enable	Click to enable or disable the PoE function. When the PoE function is enabled,				
(Optional)	it will connect the POE voltage.	ON			
	Click the button to toggle VLAN identification on or off. It is only available	OFF			
VLAN Tag Enable	when the port allocation is set to wan.	OFF			

Advanced Settings			
	SFE Fast	OFF 😨	

Advanced Settings						
Item	Description	Default				
SFE Fast	Click the toggle button to enable/disable this feature.	OFF				
	SFE Fast can increase the ethernet port rate, but it affects QoS.					

Note: Only R5020 supports "SFE Fast ".

RobustOS Software Manual

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

Index	Port	Link	
1	eth0	Down	~
2	eth1	Down	~
3	eth2	Down	~
4	eth3	Down	~
5	eth4	Down	~

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

Index	Port	Link			
1	eth0	Down			~
2	eth1	Down			~
3	eth2	Down			~
4	eth3	Down			~
5	eth4	Down			^
			Index	5	
			Port	eth4	
			Link	Down	

3.2.4 Cellular

This section allows you to set the related parameters of Cellular. The device has 1 or 2 SIM card slots.

Cellul	lar	Status	AT Debug		
^ Advan	ced Cellula	r 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	6. 16. 16. 1	
∧ General Settings		
Index	1	
SIM Card	SIM1 v	
Phone Number)
PIN Code) 🤊
MCC+MNC Code) 🧿
Extra AT Cmd) 🤊
Telnet Port	0) 🧿
Waiting For Update APN	90	0
Monthly Sent SMS Limit	0) ?
SMS Billing Day	1) 🧿

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

∧ Cellular Network Settings	
Network Type	Auto 🗸 🦻
Band Select Type	All v 🖓
Manual Operator Selection	ON OFF
∧ Advanced Settings	
Debug Enable	ON OFF
Verbose Debug Enable	ON OFF
Timeout For Network Registration	0
Preferred Using CID3	ON OFF 0
Custom APN LIST Enable	
IMS	Auto 🗸 🖓

The window is displayed below when the Manual Operator Selection is set to "ON".

∧ Cellular Network Settings					
Network Type	Auto v 😨				
Band Select Type	All v 🦻				
Manual Operator Selection	ON OFF				
Primary PLMN					
Secondary PLMN					
Check Revert Interval	0 🦻				

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

Note:

1) There may be some differences in Band Settings due to the different cellular modules.

∧ Cellular Network Settings				
Network Type	Auto v 😨			
Band Select Type	Specify 🥑 😨			
Manual Operator Selection	ON OFF			



∧ Band Settings	
GSM 850	OFF OFF
GSM 900	Off OFF
GSM 1800	OFF
GSM 1900	OFF
WCDMA 800	OFF OFF
WCDMA 850	OFF OFF
WCDMA 900	OFF
WCDMA 1900	ON OFF
WCDMA 2100	ON OFF
WCDMA 1700	OFF
LTE Band 1	OFF
LTE Band 3	OFF OFF
LTE Band 5	OFF
LTE Band 7	OFF
LTE Band 8	OFF
LTE Band 20	OFF OFF
∧ Advanced Settings	
Debug Enable	ON DEF
Verbose Debug Enable	OH OFF
Timeout For Network Registration	0
Preferred Using CID3	OFF 0
Custom APN LIST Enable	
IMS	Auto v 😨

Cellular					
Item	em Description Defaul				
	General Settings				
Index	Indicate ordinal of list.				
SIM Card	Show currently editing SIM card. SIM1				
Phone Number	one Number Enter phone number of the SIM card. Null				
PIN Code	Enter a 4-8 character PIN code used for unlocking the SIM.	Null			



	Cellular	
Item	Description	Default
MCC+MNC Code	Enter 5-6 digits and semicolon endings must be used. Used to lock the device can only use the specified carrier SIM card.	Null
Extra AT Cmd	Enter AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Waiting For Update APN	The time interval for automatically updating the APN after connecting to the network. Unit: second	90
	The modem needs to support automatic update APN feature. e.g.: HL7618RD	
Monthly Sent	Enter the maximum number of SMS that can be sent per month, 0 means no	0
SMS Limit	limit.	
SMS Billing Day	Enter the date monthly to reset SMS count to zero.	1
	Cellular Network Settings	
Network Type Band Select 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", and "4G First". 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 Only: Only the 4G network is connected. 4G First: Connect to the 3G Network preferentially. 4G Only: Only the 4G network is connected. 2G First: Connect to the 4G Network preferentially. 4G Conly: Only the 4G network preferentially. 20 Click"?" Character in the menu for help to see the details. 21 Click"?" Character in the menu for help to see the details. 	Auto
Manual Operator	"Specify". Click the toggle button to enable/disable this option.	OFF
Selection		
Primary PLMN	Enter the primary operator.	Null
Secondary PLMN	Enter the secondary operator.	Null
Check Revert	Check to revert the time interval of the primary PLMN, 0 means disable to check.	0
Interval		
	Advanced Settings	1
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF
Timeout For Network Registration	The timeout is required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0



Cellular					
Item	Description	Default			
Preferred Using	Click the toggle button to enable/disable this option. Enable using APN3 to access	OFF			
CID3	the Internet. Some operators need to use APN3 to access the Internet normally,				
	just like Verizon and it can be turned on if necessary				
Custom APN LIST	Click the toggle button to enable/disable this option. Enable Custom APN LIST	ON			
Enable	feature				
IMS	Select from "Auto", "Enable" or "Disable".	Auto			
	Auto: The default setting at MBN file is used.				

Status

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

statu	IS AT De	bug		
Î.				
Modem Status	Modem Model	IMSI	Registration	
SIM not detected	EG25			1
age Statistics				
CTM1	CMC Monthly State	Clove		
SIMI	. SPIS MONITINY STATS	Clear		
	Modem Status SIM not detected sage Statistics	Modem Status Modem Model SIM not detected EG25 Gage Statistics	Modem Status Modem Model IMSI SIM not detected EG25	Modem Status Modem Model IMSI Registration SIM not detected EG25

For R5020, R5020Lite, R2110(CAT6) can display CA status information.

Cel	Cellular Status AT		AT De	bug			
∧ Stat	us						
Index	Modem Sta	atus Moder	m Model	IMSI	Reg	jistration	
1	Ready	RM50	00Q-AE 4	454031022833865	Re	gistered	~
^ Carr	ier Aggregatio	n Status					?
Index	CA Component	Band	RSRP(dBm	n) RSRQ(dB)	RSSI(dBm)	SINR(dB)	
1	PCC	LTE BAND 3	-101	-12	-69	0	~
^ SMS	Usage Statisti	cs					?
		SIM1 SMS Mo	nthly Stats	Clear			
		SIM2 SMS Mo	nthly Stats	Clear			

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



and a second second								
Index			Model	1510	IMSI		egistration	
1	Ready	RM50	0Q-AE		3102283386	5	Registered	
			Index	1				
		Modem	Status	Ready				
		Modem	Model	RM500	Q-AE			
		Curre	ent SIM	SIM1				
		Phone N	lumber					
			IMSI	45403	1022833865			
			ICCID	89852	0310202833	8658F		
		Regis	tration	Regist	ered			
		Network P	rovider	CHN-C	т			
		Netwoi	k Type	LTE				
		END	C Stats	Inactiv	/e			
			Band	3				
		Signal St	trength	23 (-6	7dBm)			
			RSRP	-100 c	IBm			
			RSRQ	-13 dE	3			
			SINR	11 dB				
		PI	LMN ID	46011				
		Local Are	a Code					
			Cell ID	D2175	32			
			IMEI	86719	7050524921			
		Firmware \	/ersion	RM500	QAEAAR11A	03M4G_01.001	.01.001	
		Physical	Cell ID	62				
		Tracking Are	a Code	754D				
Carri	er Aggregation	Status						
ndex	CA Component	Band	RSRP(c	lBm)	RSRQ(dB)	RSSI(dBm)	SINR(dB)	
1	PCC	LTE BAND 3	-10	1	-12	-69	0	

Clear

SIM2 SMS Monthly Stats



Status			
Item	Description		
Index	Indicate ordinal of list.		
Modem Status	Show status of radio module.		
Modem Model	Show model of radio module.		
Current SIM	Show SIM card that your device is using.		
Phone Number	Show phone number of current SIM.		
	Note: This option will be displayed if entered manually in Cellular >SIM1/SIM2 >		
	General Settings > Phone Number.		
IMSI	Show IMSI number of current SIM.		
ICCID	Show ICCID number of current SIM.		
Registration	Show current network status.		
Network Provider	Show name of the Network Provider.		
Network Type	Show current network service type, e.g., GPRS.		
ENDC Stats	Show current ENDC status.		
5G Architecture	Show current 5G type. SA or NSA. This option is only displayed on 5G products.		
Band	Show band of the current network.		
Signal Strength	Show signal strength. (Only valid for 2/3/4G network, please refer to RSRP for 5G network)		
RSRP	Show Reference Signal Received Power value. (Only valid for 4G or 5G networks)		
RSRQ	Show Reference Signal Received Quality Value. (Only valid for 4G or 5G networks)		
PLMN ID	Show current PLMN ID.		
Local Area Code	Show current local area code used for identifying the different areas.		
Cell ID	Show current cell ID used for locating the device.		
IMEI	Show IMEI (International Mobile Equipment Identity) number of the radio module.		
Firmware Version	Show current firmware version of cellular module.		
SINR	Show signal to interference plus noise ratio. (Only for 4G network or 5G network)		
Physical Cell ID	Show Physical Cell ID.		
Tracking Area Code	Show Tracking Area Code.		

∧ Carrier Aggregation Status							7	
Index	CA Component	Band	RSRP(c	lBm)	RSRQ(dB)	RSSI(dBm)	SINR(dB)	
1	PCC	LTE BAND 3	-82	1	-10	-50	4	^
			Index	1				
		CA Con	nponent	PCC				
			Band	LTE E	AND 3			
		RSR	P(dBm)	-82				
		RS	GRQ(dB)	-10				
		RSS	GI(dBm)	-50				
		SI	ENR(dB)	4				



Carrier Aggregation Status				
Item	Description			
Index	Indicate ordinal of list.			
CA Component	Show individual components involved in carrier aggregation.			
Band Show the frequency band (Band) of the carrier.				
RSRP(dBm) Show Reference Signal Received Power value.				
RSRQ(dB) Show Reference Signal Received Quality value.				
RSSI(dBm) Show Received Signal Strength Indicator value.				
SINR(dB) Show signal to interference plus noise ratio.				

SIM1 SMS Monthly Stats Clear SIM2 SMS Monthly Stats Clear

SMS Usage Statistics					
Item	Description				
SIM1 SMS Monthly Stats	Click the button Clear to manually clear the accumulated number of SMS sent using SIM1.				
SIM2 SMS Monthly Stats	Click the button Clear to manually clear the accumulated number of SMS sent using SIM2.				

AT Debug

This section allows you to do the AT Debug.

Cellular	Status	AT Debug	
∧ AT Debug			
Command			
Result			<u></u>
			Send



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

3.2.5 Wi-Fi

This section allows you to configure the parameters of two Wi-Fi modes. The device supports both Wi-Fi AP or Client modes and defaults as AP.

Wi-Fi AP

Configure Device as Wi-Fi AP

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

2.4GHz WI-FI Only

WiFi	Access Point	Advanced		ACL	Status
∧ General Setti	ngs				
		Mode	AP	v 😨	
		Region	SE	0	

Note: Only R3000 Series support Mode options.

2.4GHz and 5GHz Wi-Fi

WiFi	Access Point 2.4G	Access Po	oint 5G	Status	EAP Cert
General Se	ttings				
		Region	SE	0	

Note:

- 1) Only R2110 and R5020 support both 2.4GHz and 5GHz.
- 2) R2110/R5020 series/R151x series/1520/R201X series devices now support running WiFi AP and WiFi Client modes at the same time. The WLAN interface is added by default in link management, and there is no need to select the working mode here.

Access Point 2.4G

Click the **Access Point 2.4G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as "Disabled".



∧ General Settings	
Enable	ON OFF
Wireless Mode	11bgn Mixed v
Bandwidth	20MHz 🤍 😨
Channel	auto v
SSID	RBT-834A-2.4G
Broadcast SSID	ON OFF
Security Mode	Disabled v 😨

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

∧ General Settings	
Enable	ON OFF
Wireless Mode	11bgn Mixed v
Bandwidth	20MHz v
Channel	Auto v 😨
SSID	RBT_25FD_2G_test
Broadcast SSID	ON OFF
Security Mode	WPA-Personal v
WPA Version	WPA/WPA2 v
Encryption	AES v
PSK Password	
Group Key Update Interval	3600



The window is displayed below while setting "WEP" as the security mode.

∧ General Settings	
Enable	OFF
Wireless Mode	11bgn Mixed v
Bandwidth	20MHz V 😯
Channel	auto v
SSID	RBT-834A-2.4G
Broadcast SSID	ON OFF
Security Mode	WEP V
WEP Кеу	••••••••

The window is displayed below while setting "EAP-TLS" as the security mode. *Note:*

(1) Only R2110/R5020/R5020Lite supports "EAP-TLS" security mode.

∧ General Settings	
Enable	ON OFF
Wireless Mode	11bgn Mixed v
Bandwidth	20MHz v
Channel	Auto v 😨
SSID	RBT_25FD_2G_test
Broadcast SSID	ON OFF
Security Mode	EAP-TLS v 😨
Radius Authentication Server Address	0.0.0.0
Radius Authentication Server Port	1812
Radius Server Share Secret	······ (?)

General Settings @ Access Point 2.4G				
Item Description Default				
Enable Click the toggle button to enable/disable the Wi-Fi access		OFF		

General Settings @ Access Point 2.4G		
Item	Description	Default
Wireless Mode	 Select from "11bgn Mixed", "11b only", "11g only", and "11n only". 11bgn Mixed: mix three protocols for backward compatibility 11b only: IEEE 802.11b, 11 Mbps 11g only: IEEE 802.11g, 54 Mbps 	11bgn Mixed
	 11n only: IEEE 802.11n, 450 Mbps 	
Channel	 The channel that different bandwidths can choose is as follows. Auto: The device will scan all frequency channels until the best one is found. The frequency of 1~13 channels of 20MHz bandwidth available channel: 1-2412 MHz 2-2417 MHz 2-2427 MHz 2-2432 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 12-2467 MHz 2-2417 MHz 2-2472 MHz The frequency of 1~13 channels of 40MHz bandwidth available channel: 1-2412 MHz 2-2417 MHz 2-2417 MHz 2-2417 MHz 2-2417 MHz 2-2417 MHz 2-2417 MHz 3-2422 MHz 4-2427 MHz 2-2417 MHz 3-2422 MHz 4-2427 MHz 2-2417 MHz 3-2422 MHz 4-2427 MHz 3-2422 MHz 4-2427 MHz 3-2422 MHz 4-2427 MHz 3-2422 MHz 3-2427 MHz 3-2427 MHz 	Auto



General Settings @ Access Point 2.4G		
Item	Description	Default
SSID	Enter SSID (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.	RBT-XXXX-2.4G
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 device AP, you need to manually enter the SSID of the device AP on the Wi-Fi client side.	ON
Security Mode	 Select "Disabled", "WPA-Personal", "WPA-Enterprise", "WEP", "EAP-TLS". Disabled: The user can access the Wi-Fi without a password Note: It is strongly recommended for security purposes that you do not choose this kind of mode. WPA-personal: Wi-Fi access protection. Only one password is provided for identity authentication WEP: Wired Equivalent Privacy provides encryption for wireless device's data transmission WPA-Enterprise: Each user who connects to the network is required to provide a personal username and password, digital certificate, or other credentials for authentication. Note: This option is available for some models, R3000 EAP-TLS: An advanced authentication protocol for strong authentication and security based on the Transport Layer Security (TLS) protocol. Note: Only R2110/R5020/R5020Lite supports WiFi EAP-TLS authentication method. 	Disabled

General Settings @ Access Point 2.4G		
Item	Description	Default
WPA Version	 Select from "WPA/WPA2", "WPA" or "WPA2" or "WPA3". WPA/WPA2: The device will automatically choose the most suitable WPA version WPA: The early Wi-Fi security standard uses the TKIP (Temporal Key Integrity Protocol) encryption protocol to protect data transmission and provide a certain degree of data protection. WPA2: WPA2 is an upgraded version of WPA, using a more powerful encryption protocol AES (Advanced Encryption Standard), and providing more advanced data protection. WPA3: WPA3 is a further improvement of WPA2, using stronger password cracking protection, increasing the security of public wireless networks, and improving the method of password selection. Note: R2110/R5020 series/R151X series/R1520/R201X series support WPA3 	WPA/WPA2
Encryption	 Select from "TKIP" or "AES". TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP Note: The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode. 	AES
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
Radius Authentication	Enter the Radius authentication server address.	0.0.0.0
Server Address		
Radius Authentication	Enter the Radius authentication server port.	1812
Server Port		
Radius Server Share Secret	Enter the Radius server shared password, limited to 8 to 128 characters.	Null
Group Key Update Interval	Enter the time of group key renewal.	3600
WEP Кеу	Enter WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null



Advanced Settings		
Max Associated Stations	64	
Beacon Interval	100	0
DTIM Period	2	0
Channel Width	Auto	∨ 🦻
Enable Short GI	ON 017 7	
Enable AP Isolation	OM OFF 7	
Debug Level	None	v

Advanced Settings @ Access Point 2.4G		
Item	Description	Default
Max Associated Stations	Set the maximum number of clients allowed to access the device's	0
	AP. (Value 0 means without limitation)	
Beacon Interval	Set the interval of time in which the device AP broadcasts a beacon	100
	which is used for wireless network authentication.	
DTIM Period	Set delivery traffic indication message period, and the device AP will	2
	multicast the data according to this period.	
Channel Width	Select device channel width, "20 MHz" or "40 MHz"	Auto
	<i>Note:</i> 40 MHz channel width provides twice the data rate	
	available over a single 20 MHz channel; the data transfer rate	
	of 80MHz bandwidth is 4 times greater than that of a single	
	20Mhz bandwidth.	
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval	ON
	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.	
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option.	OFF
	When enabled, the device will isolate all connected wireless devices.	
	The wireless devices can't access each other.	
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", or	none
	"none".	

∧ ACL Settings	
Enable ACL	OFF
ACL Mode	Accept 🤍

ACL Settings @ Access Point 2.4G		
Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select "Accept" or "Deny".	Accept
	 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: The device can only allow or deny devices included in the "Access Control List" at one time. 	

∧ Access Control List			
Index	Description	MAC Address	+

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

Access Point 2.4G	
Access Control List	
Index Description MAC Address	
	Submit Close

Access Control List @ Access Point 2.4G		
Index Indicate ordinal of list		
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null



Access Point 5G

Click the **Access Point 5G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as "Disabled".

∧ General Settings	
Enable	OR
Wireless Mode	11an v
Bandwidth	20MHz 🤍 🕜
Channel	36 🗸
SSID	RBT-834A-5G
Broadcast SSID	ON OFF
Security Mode	Disabled v 😨

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

∧ General Settings	
Enable	ON OFF
Wireless Mode	11a/an/ac v
Bandwidth	80MHz V 🝞
Channel	44 🗸 🧭
SSID	RBT_25FD_5G_test
Broadcast SSID	ON OFF
Security Mode	WPA-Personal 🗸 🧭
WPA Version	WPA/WPA2
Encryption	AES
PSK Password	
Group Key Update Interval	3600



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

∧ General Settings	
Enable	ONOFF
Wireless Mode	11an v
Bandwidth	20MHz V
Channel	36 v 🦻
SSID	RBT-834A-5G
Broadcast SSID	ON OFF
Security Mode	WEP V
WEP Кеу	

The window is displayed below while setting "EAP-TLS" as the security mode. *Note:*

(1) Only R2110/R5020/R5020Lite supports "EAP-TLS" security mode.

∧ General Settings	
Enable	ON OFF
Wireless Mode	11a/an/ac v
Bandwidth	80MHz v 🝞
Channel	44 v 😨
SSID	RBT_25FD_5G_test
Broadcast SSID	ON OFF
Security Mode	EAP-TLS V
Radius Authentication Server Address	0.0.0.0
Radius Authentication Server Port	1812
Radius Server Share Secret	()

General Settings @ Access Point 5G		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF



	General Settings @ Access Point 5G	
Item	Description	Default
Wireless Mode	 Select from "11an", or "11a/an/ac". 11an: Compatible IEEE 802.11a, 54 Mbps and IEEE 802.11n, 300Mbps 11a/an/ac: Compatible IEEE 802.11a, 54 Mbps, IEEE802.11n 300 Mbps and 802.11ac, 867 Mbps 	11an
Bandwidth	Select from "20MHz", "40MHz" or "80MHz". Note : 40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20 MHz bandwidth.	20MHz
Channel	The optional channels for bandwidths are as below. • The frequency of 36~165 channels of 20MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 161–5805 MHz 165–5825 MHz 161–5805 MHz 165–5825 MHz 161–5805 MHz 40–5200 MHz 44–5220 MHz 44–5220 MHz 149–5745 MHz 153–5765 MHz 161–5805 MHz 161–5805 MHz 165–5825 MHz 161–5805 MHz 165–5825 MHz 165–5825 MHz 165–5825 MHz 165–5826 MHz 40–5200 MHz 44–5220 MHz 44–5220 MHz 44–5220 MHz 44–5220 MHz 4	36



General Settings @ Access Point 5G		
Item	Description	Default
	Note: All available channels of 5GHz Wi-Fi on different	
	bandwidths are listed above. Web parameters should be	
	configured due to the different available channels in different	
	countries and areas.	
SSID	Enter SSID (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	RBT-XXXX-5G
	each other. Enter 1 to 32 characters.	
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	ON
	to connect to the device AP, you need to manually enter the	
	SSID of the device AP on the Wi-Fi client side.	
Security Mode	Select "Disabled", "WPA-Personal", "WPA-Enterprise",	Disabled
	"WEP", "EAP-TLS".	
	• Disabled: The user can access the Wi-Fi without a	
	password	
	<i>Note</i> : It is strongly recommended for security purposes that	
	you do not choose this kind of mode.	
	WPA-personal: Wi-Fi access protection. Only one	
	password is provided for identity authentication	
	WEP: Wired Equivalent Privacy provides encryption for	
	wireless device's data transmission	
	• WPA-Enterprise: Each user who connects to the network	
	is required to provide a personal username and	
	password, digital certificate, or other credentials for	
	authentication.	
	Note: This option is available for some models, R3000	
	• EAP-TLS: An advanced authentication protocol for strong	
	authentication and security based on the Transport Layer	
	Security (TLS) protocol.	
	Note: Only R2110/R5020/R5020Lite supports WiFi	
	EAP-TLS authentication method.	

General Settings @ Access Point 5G		
Item	Description	Default
WPA Version	 Select from "WPA/WPA2", "WPA" or "WPA2" or "WPA3". WPA/WPA2: The device will automatically choose the most suitable WPA version WPA: The early Wi-Fi security standard uses the TKIP (Temporal Key Integrity Protocol) encryption protocol to protect data transmission and provide a certain degree of data protection. WPA2: WPA2 is an upgraded version of WPA, using a more powerful encryption protocol AES (Advanced Encryption Standard), and providing more advanced data protection. WPA3: WPA3 is a further improvement of WPA2, using stronger password cracking protection, increasing the security of public wireless networks, and improving the method of password selection. Note: R2110/R5020 series/R151X series/R1520/R201X series support WAP3 	WPA/WPA2
Encryption	 Select from "TKIP" or "AES". TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP Note: The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode. 	AES
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
@WPA-Personal		
Group Key Update Interval @WPA-Personal	Enter the time of group key renewal.	3600
WEP Key @WEP	Enter 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
Radius Authentication Server Address @EAP-TLS	Enter the Radius authentication server address.	0.0.0.0
Radius Authentication Server Port @EAP-TLS	Enter the Radius authentication server port.	1812



General Settings @ Access Point 5G		
Item Description Default		
Radius Server Share Secret	Enter the Radius server shared password, limited to 8 to 128	Null
@EAP-TLS	characters.	

Advanced Settings		
Max Associated Stations	0	?
Beacon Interval	100	0
DTIM Period	2	0
RTS Threshold	2347	0
Fragmentation Threshold	2346	0
Transmit Power	Max v	
Enable WMM	ON OFF	
Enable Short GI	ON OFF ?	
Enable AP Isolation	OR OFF	
Debug Level	none v	

Advanced Settings @ Access Point 5G		
Item	Description	Default
Max Associated Stations	Set the maximum number of clients allowed to access the device's	0
	AP. (Value 0 means without limitation)	
Beacon Interval	Set the interval of time in which the device AP broadcasts a beacon	100
	which is used for wireless network authentication.	
DTIM Period	Set delivery traffic indication message period and the device AP will	2
	multicast the data according to this period.	
RTS Threshold	Set "request to send" threshold. When the threshold is set as 2347,	2347
	the device AP will not send a detection signal before sending data.	
	And when the threshold is set as 0, the device AP will send a	
	detection signal before sending data.	
Fragmentation Threshold	Set fragmentation threshold of a Wi-Fi AP. It is recommended that	2346
	you use the default value 2346.	
Transmit Power	Select from "Max", "High", "Medium" or "Low".	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval	ON
	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.	
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option.	OFF



Advanced Settings @ Access Point 5G		
Item Description Default		Default
	When enabled, the device will isolate all connected wireless devices.	
	The wireless devices cannot access each other.	
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", or	none
	"none".	

ACL Settings

Enable ACL OFF ACL Mode Accept Image: Constraint of the second s			
ACL Settings @ Access Point 5G			
Item	Description	Default	
Enable ACL	Click the toggle button to enable/disable this option.	OFF	
ACL Mode	Select from "Accept" or "Deny".	Select from "Accept" or "Deny". Accept	
	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		
	<i>Note</i> : The device can only allow or deny devices that are included in the		
	"Access Control List" at one time.		

Access Control List Index Description MAC Address

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

Access Point 5G	
Access Control List	
Index	1
Description	
MAC Address	
	Submit Close

Access Control List @ Access Point 5G			
Index	Indicate ordinal of list.		
Description	Enter a description for this access control list.	Null	
MAC Address	Add a MAC address here.	Null	



Status

WiFi	Access	s Point Adv	vanced	ACL	Status	
AP Stat	tus					
		Statu	s COMPLET	ED		
		Channe	el 1			
		Channel Widt	h 20 MHz			
		MAC Addres	s 34:FA:40	:0E:F7:94		
^ Associa	ated Stations					
Index	MAC Address	IP Address	Name	Connected Time	Signal	

Note: Wi-Fi is off by default. Follow the steps below to enable it and set the device as Wi-Fi client.

EAP Cert

This section support EAP certificate settings and viewing certificate file information.

WiFi	Access Point	2.4G Access Poi	nt 5G	Status	EAP Cert	
~ EAP-TLS	6 Certificate Setting	IS				?
	РКС	S#12 Certificate	Choose	File No file chosen		
∧ Certifica	ate Files					
Index	File Name	File Size		Modification Ti	me	

EAP Cert			
Index	Indicate ordinal of list.		
PKCS#12 Certificate	Click the button Choose File to select the local PKCS#12 certificate		
	file, and click the button 💿 to import the certificate file.		

This section allows you to view the status of AP.



Wi-Fi Client

Note: This part of the content only applies to the R3000 series.

Configure Device as Wi-Fi Client

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

WiFi	Status			
∧ General Setti	ngs			
	Mode	Client	▼ 🦻	
	Region	SE	0	

Then a "WLAN" column will appear under the Interface list.

	Status		
Status	NULAN Status	;	
Interface		Status	Disconnected
Link Manager		Uptime	
LAN			
Ethernet		IP Address	
Cellular		Gateway	
WiFi		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
WLAN		DNS	
USB			
DIDO		MAC Address	
Serial Port		Channel	

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

~ WLAN Settings		
	SSID	router
	Connect to Hidden SSID	OFF
	Password	

Click Interface > WLAN to configure the parameters of Wi-Fi Client after setting the mode as Client. Please remember to click Save & Apply > Reboot after finishing the configuration, so that the configuration can take effect.



Status			
∧ WLAN Status			
	Status	Connected	
	Uptime	0 days, 00:00:17	
	IP Address	192.168.1.128/255.255.255.0	
	Gateway	192.168.1.253	
	DNS	172.16.0.1 202.96.209.6	
	MAC Address	00:23:a7:a4:13:e4	

3.2.6 USB

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

USB	Кеу	
∧ General Settings	5	
	Enable USB	ON OFF
	Enable Automatic Upgrade	OFF

Key

This section allows you to generate the key for the USB.

USB	Кеу	
^ Key		
	USB Automatic Upgrade Ke	Generate

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



USB Automatic Update		
Kev	Click Generate to generate a key, and click Download to download the key.	
Ney		

Note: In the process of USB auto upgrade, when using the USB auto-upgrade function, when the running light appears, it means the upgrade is in progress. When the running light stops and the USR light is on, it means the upgrade is complete. After upgrading, the device will not restart automatically. If there is no running light effect, it means that there is an abnormality, and it does not enter into the automatic upgrade process.

3.2.7 DI/DO

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

DI

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

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

DI	
∧ General Settings	
Index	1
Enable	OFF
Mode	ON-OFF V
Inversion	OFF
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off



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

DI	
∧ General Settings	
Index	1
Enable	ON OFF
Mode	Counter
Inversion	ON OFF
Time interval for clearing DI counts	0
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off

General Settings @ DI				
Item	Description	Default		
Index	Indicate ordinal of list.			
Enable	Click the toggle button to enable/disable the digital input function.	OFF		
Mode	Select "ON-OFF" or "Counter".			
	• ON-OFF: Alarm mode can be triggered at the DI access ON-OFF.			
	Counter: Event counter mode.			
Inversion	The count is divided into a rising edge count of the level or a falling edge	OFF		
	count. If the current rising edge count, the reverse edge is the falling edge			
	count.			
Time interval for	Input to set the DI count clearing timer. The possible value range is 0~2880,	0		
clearing DI counts	unit: minutes; 0 means not to use this function.			
Threshold Value	The threshold value is a unique parameter when the mode is counted. Set the	0		
	threshold value to trigger the DI alarm when the count value reaches the			
	threshold value.			
Alarm On Content	Show content when the alarm is on.	Alarm On		
Alarm Off Content	Show content when the alarm is off.	Alarm Off		

Note: It defaults to a high alarm while turning to a low alarm after enabling the "Inversion" button.

DO

DI	DI DO		Status			
^ DO Set	tings					
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 below.



DO	
∧ General Settings	
Index	1
Enable	ONOFF
Alarm On Action	High
Alarm Off Action	Low
Initial State	Last
Delay	0
Hold Time	0
Alarm Source	DI1 Alarm v

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

DO	
∧ General Settings	
Index	1
Enable	OFF
Alarm On Action	Pulse
Alarm Off Action	Low
Initial State	Last
Delay	0 🥘
Hold Time	0 🧿
Low-level Width	1000
High-level Width	1000 🦻
Alarm Source	DI1 Alarm V


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



	General Settings @ DO		
Item	Description	Default	
Index	Indicate ordinal of list.		
Enable	Click the toggle button to enable/disable this DO.	OFF	
Alarm On Action	 The mon Action Digital Output initiates when there is an alarm. Selected from "High", "Low" or "Pulse". 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. 		
Alarm Off Action	 Digital Output initiates when the alarm is removed. Selected from "High", "Low" or "Pulse". 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". Last: DO's status will consist of the status of the last power off. High: DO interface is at a high electrical level. Low: DO interface is at a low electrical level. 	Last	
Delay (unit: 100ms)	Set 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	Set hold time of DO status (Alarm On Action/Alarm Off Action). When the action time	0	



General Settings @ DO				
Item	Description	Default		
(unit: s)	reaches this specified time, DO will stop the action. Enter from 0 to 3000 seconds.			
	(0: keep on until the next action)			
Low-level Width	Set low-level width. It is available when enabling Pulse as "Alarm On Action/Alarm Off	1000		
(unit: ms)	Action". In Pulse Output mode, the selected digital output channel will generate a			
	square wave as specified in the pulse mode parameters. The low-level widths are			
	specified here. Enter from 1000 to 3000.			
High-level	Set high-level width. It is available when enabling Pulse as "Alarm On Action/Alarm	1000		
Width	Off Action". In Pulse Output mode, the selected digital output channel will generate a			
(unit: ms)	square wave as specified in the pulse mode parameters. The high-level widths are			
	specified here. Enter from 1000 to 3000.			
Alarm Source	Digital output activation can be activated by this alarm.	None		

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

DI		DO		Status	
Index	Level	Status	Count		
1	High	Alarm off			×
2	High	Alarm off			~
^ Action	Of Clear		· China i		
		Cour	nter Alarm	Of DI 1 Clear	
		Cour	nter Alarm	Of DI 2 Clear	
∧ DO Stat	us				
Index	Level	Low	-level Widt	h High-level Width	
1	Closed	d			×
2	Closed	ł			~
へ DO Con	trol				
			Level	Of DO1 Toggle	
			Level	Of DO2 Toggle	



3.2.8 AI

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

1) R1520 supports an AI interface.

AI		Status		
AI Set	tings			
Index	Enable	Input Type	Interval	
1	false	Voltage	5	

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

AI	
∧ General Settings	
Index	1
Enable	OFF
Input Type	Voltage 🦳 🧭
Min Threshold	3
Max Threshold	20
Interval	5 🦻

The window is displayed below when the "input type" is "Current".

AI		
∧ General Settings		
Index	1	
Enable	OT	
Input Type	Current	9
Min Threshold	4	0
Max Threshold	16	0
External Resistance	1200	0
Interval	5	0
		Submit Close



AI (Analog Input)				
Item	Description	Default		
Index	Indicate ordinal of list.			
Enable	Click the switch button to "ON" to turn on the analog input function.	OFF		
	Select "Voltage" or "Current".			
Input type	Voltage: The data collected is voltage.	Voltage		
	Current: The data collected is Current.			
Min Threshold @Voltage	Set minimum voltage threshold. When the voltage collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: V.	3		
Max Threshold @Voltage	Set maximum voltage threshold. When the voltage collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: V.	20		
Min Threshold @Current	Set minimum current threshold. When the current collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	4		
MaxThreshold @Current	Set maximum current threshold. When the current collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	16		
External Resistance	Set the value of the external resistance. Unit: ohm.	1200		
Interval	Collect latest data every few seconds.	5		

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

AI		Status		
AI Stat	us			
Index	Туре	Min Threshold	d Max Threshold Value	
1	voltage	3	20	
			Index 1	
			Type voltage	
		Min Thr	hreshold 3	
		Max Thi	hreshold 20	

3.2.9 Serial Port

This section allows you to set the serial port parameters. The device might support two serial ports, COM1 and COM2, which can be configured as two COM1 or two COM2 according to requirements. The serial data can be converted into IP data or through IP data into serial data, and then the data can be transmitted through a wired or wireless



network, to realize the function of transparent data transmission.

Note:

1) The serial ports of R2010 and R3000-Quad can be configured as RS232 or RS485.

Port Type	Serial Port	Status		
∧ General Setti	ngs			
	Serial Port	Type RS485	v	

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

Serial P	ort	Statu	IS		
∧ Serial I	Port Setti	ings			
Index	Port	Enable	Baud Rate	Application Mode	
1	COM1	false	115200	Transparent	
2	COM2	false	115200	Transparent	

Click the right-most S button of COM1 as below.

Serial Port				
Serial Port Application Settings				
Index	1			
Port	COM1 V			
Enable	OFF			
Baud Rate	115200 V			
Data Bits	8 V			
Stop Bits				
Parity	None			
Flow Control	None			
∧ Data Packing				
Packing Timeout	50 🕜			
Packing Length	1200			

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

∧ Server Setting	
Application Mode	Transparent
Protocol	TCP Client v
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Transparent v
Protocol	TCP Server v
Local IP	
Local Port	
Serial Keep Alive	0

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

∧ Server Setting	
Application Mode	Transparent
Protocol	UDP v
Local IP	
Local Port	
Server Address	
Server Port	

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 Gatewa v
Protocol	TCP Client v
Server Address	
Server Port	

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



Server Setting	
Application Mode	Modbus RTU Gatewa v
Protocol	TCP Server v
Local IP	
Local Port	
Serial Keep Alive	0

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 Gatewa v
Protocol	UDP v
Local IP	
Local Port	
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Modbus ASCII Gatev v
Protocol	TCP Client v
Server Address	
Server Port	

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

∧ Server Setting	
Application Mode	Modbus ASCII Gatev v
Protocol	TCP Server v
Local IP	
Local Port	
Serial Keep Alive	0

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
Local IP	
Local Port	
Server Address	
Server Port	

Serial Port					
Item Description					
	Serial Port Application Settings				
Index	Indicate ordinal of list.				
Port	Show 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".				
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".				
Data Packing					
Packing Timeout	Set packing timeout. The serial port will queue the data in the buffer and send the	50			
	data to the Cellular WAN/Ethernet WAN/ WLAN when it reaches the Interval Timeout				
	in the field. The unit is milliseconds.				
	<i>Note</i> : Data will also be sent as specified by the packet length even when data is not				
	reaching the interval timeout in the field.				



Serial Port			
Item	Description	Default	
Packing Length	Set packet length. The Packet length setting refers to the maximum amount of data	1200	
	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		
	as it reaches the specified length.		
	Server Settings		
Item	Description	Default	
Application	Select from "Transparent", "Modbus RTU Gateway", or "Modbus ASCII Gateway".	Transp	
Mode	• Transparent: The device will transmit the serial data transparently.	arent	
	• Modbus RTU Gateway: The device will translate the Modbus RTU data to Modbus		
	TCP data and send it out, and vice versa.		
	Modbus ASCII Gateway: The device will translate the Modbus ASCII data to		
	Modbus TCP data and send it out, and vice versa.		
Protocol	Select "TCP Client", "TCP Server", or "UDP".	ТСР	
	• TCP Client: Device works as a TCP client, and initiates a TCP connection to the	Client	
	TCP server. The server address supports both IP and domain name.		
	• TCP Server: Device works as a TCP server, listening for a connection request from		
	a TCP client.		
	UDP: Device works as a UDP client.		
Server Address	Enter the address of the server which will receive the data sent from the device's	Null	
	serial port. IP address or domain name will be available.		
Server Port	Enter a specified port of the server which is used for receiving the serial data.	Null	
Serial Keep Alive	Enter the keep-alive time, the value range is 0~18000, unit: second. When the serial	0	
	port or TCP no data is detected within the set time, all TCP client connections will be		
	actively disconnected. 0 means this function is not enabled.		
Local IP @		Null	
Transparent	Enter the device's LAN IP which will forward to the internet port of the device.		
Local Port @		Null	
Transparent	Enter port of the device's LAN IP.		
Local IP @		Null	
Modbus	Enter local IP under Modbus mode.		
Local Port @		Null	
Modbus	Enter local port under Modbus mode.		

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

Serial P	ort	Status				
∧ Serial Port Status list						
Index	Туре	ТХ	RX	Connection Status		
1	RS232	OB	0B			
2	RS485	0B	0B			



Status		
Item Descriptions		
ТХ	Send Data to Serial Port.	
RX	Received Data from Serial Port.	

3.2.10 Serial Redirector

This section allows you to redirect the Serial Port to Telnet. It is only for the R1520.

Redirect	tor	Status	
∧ Serial I	Port Sett	ings	7
Index	Port	Baud Rate Telnet Port	+

Click "Redirector" column to configure the Serial Redirector.

Click to select serial port and baud rate corresponding the device of serial port had connected, then input the correct Telnet port you expect to redirect.

Redirector	
∧ General Settings	
Index	1
Port	COM1 V
Baud Rate	115200 V
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Telnet Port	88
	Submit Close

Click the "Status" column to view redirection status.

Redirect	tor	Status	
^ Redire	ctor Port	Status	
Index	Port	Status	

3.2.11 LoRa

This section allows you to set the LoRaWAN parameters. It is only for the R3000-LG.

Click "General Settings" to configure the Gateway ID. Here is an example below.

General Settings	RF Settings	Filter Se	ttings	Status	
∧ General Settings					
Default Gateway ID			34FA40F	FFE052762	
User Defined Gateway ID Enable		ON 💿	F		
User Defined Gateway ID		1234567	7890ABCDEF		

General Settings		
Item	Description	Default
Default	Set default gateway ID, or you could define the Gateway ID with a unique 64-bit	Null
Gateway ID	sequence by yourself.	
User Defined		OFF
Gateway ID	Click the toggle button to enable/disable this option.	
Enable		
User Defined		Null
Gateway ID	Enter Gateway ID.	

RF Settings

General Settings	RF Settings	Filter Settings	Status
∧ RF Power Setti	ngs		
	RF Powe	er Limit No Limit	
∧ RF Chain Settin	gs		
-	Supported Fre	equency 863 870	V
	Frequencies	Options User-define	ne v 😨
	RF Chain 0 Fre	equency 86850000	0
	RF Chain 1 Fre	quency 86750000	00

RF Settings		
Item	Description	Default
RF Power Settings		
RF Power Limit	Display RF power limit.	No Limit



RF Settings		
Item	Description	Default
	RF Power Settings	
	RF Chain Settings	
Support	Display support frequency.	863 870
Frequency		805 870
	Set link frequency.	
	EU868:	
	868.1,868.3,868.5,867.1,867.3,867.5,867.7,867.9,	
	STD 868.3 and FSK 868.8;	
Frequencies	RU868:	User-define
Options	RF Chain 0:869000000,RF Chain 1:864500000,	User-define
	868.9,869.1,869.3,864.1,864.3,864.5,864.7,864.9;	
	KZ868:	
	RF Chain 0:865300000,RF Chain 1:867500000,	
	865.1,865.3,865.5,867.1,867.3,867.5,867.7,867.9.	
RF Chain 0	Set frequency of RF link 0.	868500000
Frequency		
RF Chain 1	Sat fraguancy of PE link 1	86750000
Frequency	Set frequency of RF link 1.	867500000

∧ LoRa Multi Datarate Channels Settings Index RF Chain IF frequency

Click+to Add LoRa Multi Datarate Channels Settings.

A LoRa Multi Datarate Channels Settings		
Index	1	
RF Chain	RF Chain 0 v	
IF frequency	0	

LoRa Multi Datarate Channels Settings@RF Settings		
Item	Description	Default
Index	Indicate ordinal of list.	1
RF Chain	Select RF Chain.	RF Chain 0
	Enter center frequency in the range -500000-500000 in Hz. The offset	
IF frequency	between the center frequency of a particular channel and the center	0
	frequency of RF link 0/1.	



A LoRa Standard Channel Settings			
Enable	ONOFF		
RF Chain	RF Chain 0		
IF frequency	0		
Bandwidth	500KHz		
Spread Factor	SF9		

LoRa Standard Channel Settings@RF Settings		
ltem	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Select RF Chain.	RF Chain 0
	Enter center frequency in the range -500000-500000 in Hz. The offset	
IF frequency	between the center frequency of a particular channel and the center 0	
	frequency of RF link 0/1.	
Bandwidth	Select optional bandwidth in KHz.	500KHz
Spread Factor	Enter an optional spreading factor. A high spreading factor corresponds	SF9
	to a low rate, and a low spreading factor corresponds to a high rate.	

Filter Settings

This section is used to modify LoRa filter settings.

General Settings	RF Settings	Filter Set	tings	Status	
∧ LoRa Filter S	∧ LoRa Filter Settings				
		LoRa Filter	ON OFF		
∧ Whitelist DevEUIs			0		
Index	DevEUI				+

Filter Settings		
Item	Description	Default
LoRa Filter	Click the toggle button to enable/disable this option.	OFF

Click to add a whitelist rule.

∧ Whitelist Rules	
Index	1
DevEUI	



Whitelist Rules@Filter Settings		
Item	Description	Default
Index	Display table number. 1	
DevEUI Enter DevEUI for device. Null		

This section allows you to check the status of LoRa interface.

General Settings	RF Settings	Filter Se	ettings	Status
∧ Basic	100 ⁷⁷			
		Model	SX1301	
∧ RF package rec	eived			
		CRC Errors	0	
		Duplicates	0	
	Join	Duplicates	0	
	Joi	n Requests	0	
	То	tal Packets	0	
	RF packe	ts received	0	
	RF packets rec	eived State	CRC_OK:	0.00%, CRC_FAIL: 0.00%, NO_CRC: 0.00%
	RF packets	forwarded	0 (0 bytes	3)
∧ Packets sent				
	Duplic	ates Acked		
	Pac	kets Acked		
	Total Join	Responses		
	Join Response	es Dropped		
	То	tal Packets		
	Packe	ts Dropped		



^ Cente	r Frequency		
RF Chain 0 Frequency			
	RF Chain 1 Frequency		
∧ LoRa I	Multi Datarate	Channels	
Index	RF Chain	IF frequency	

A LoRa Standard Channel		
RF Chain		
IF frequency		
Bandwidth		
Spread Factor		

> FSK Standard Channel		
RF Chain		
IF frequency		
Bandwidth		
Data Rate		

Status			
Item	Description		
	Basic		
Model	Show LoRa module model.		
	Packets received		
CRC Errors	Show the value of RF packets received in error.		
Duplicates	Show the value of duplicate RF packets received.		
Join Duplicates	Show the value of duplicate RF join request packets received.		
Join Requests	Show the value of RF join request packets received.		
Total Packets	Show the value of RF packets received.		
RF Packets Received	Show count of data packets from node to gateway.		
RF Packets Received State	Show the RF packets receiving state.		
	CRC_OK: Percentage of CRC verification		
	CRC_Fail: Percentage of CRC verification failure		
	NO_CRC: Percentage of abnormal packets without CRC		
Packets sent			



Status			
Item	Description		
Duplicates Asked	Show the value of duplicate RF response packets sent.		
Packets Asked	Show the value of RF response packets sent.		
Total Join Responses	Show the value of duplicate RF join response packets sent.		
Join Responses Dropped	Show the value of failed RF join response packets.		
Total Packets	Show the value of RF packets sent.		
Packets Dropped	Show the value of RF dropped packets.		
	Center Frequency		
RF Chain 0 Frequency	Center frequency of LoRa channel 0.		
RF Chain 1 Frequency	Center frequency of LoRa channel 1.		
	LoRa Multi Datarate Channels		
RF Chain	Index of LoRa channel.		
IF Frequency	IF frequency of LoRa channel.		
	LoRa standard Channel		
RF Chain	Index of LoRa standard channel.		
IF frequency	IF frequency of LoRa standard channel.		
Bandwidth	Bandwidth of LoRa standard channel.		
Spread Factor	Spread Factor of LoRa standard channel.		
FSK Standard Channel			
RF Chain	Index of FSK Standard Channel.		
IF frequency	IF frequency of FSK Standard Channel.		
Bandwidth	Bandwidth of FSK Standard Channel.		
Data Rate Of FSK Standard Channel.			



3.3 Packet Forwarders

3.3.1 Basic Station

General Settings

General Settings	Status	Cert Manager
▲ Gateway Setting	S	
		Enable OFF
	TLS	S Enable OFF
	Server	Address 127.0.0.1
	Ser	ver Port 3001
	Verbose Debug	g Enable OFF
		General Settings

	General Settings				
	Gateway Settings				
Item	Item Description				
Enable	Enable application.	OFF			
TLS Enable	Enable TLS encrypted transmission.	OFF			
Server	Server address (e.g., 127.0.0.1)	127.0.0.1			
Address					
Server Port	Server port number.	3001			
Verbose	Click the toggle button to enable/disable this option. Enable verbose debugging	OFF			
Debug Enable	information output.				

Status

This section allows you to view the status of the basic station.

General Settings	Status	Cert Manager				
^ Basic						
		TC Status				
	Station Version					
	Package Version (Protocol)					
	HAL Libra	ary Version				
Item	Description					



TC Status	Platform connection status.			
Station Version	Application version.			
Package Version	Application package version.			
(Protocol)				
HAL Library				
Version	LoRaWAN HAL library version.			

Cert Manager

This section allows you to view and import the certification.

General Settings	Status	Cert Man	ager			
∧ CA File Impo	rt					?
		CA Cert	Choose F	File No file chosen	Import	
		Client Cert	Choose F	File No file chosen	Import	
		Client Key	Choose F	File No file chosen	Import	
∧ Certificate Fil	es					
Index Fi	le Name	File Size	l.	Modification Time		

Cert Manager				
CA File Import				
Item	Description	Default		
CA Cert	Server certificate.	Null		
Client Cert	The certificate is assigned by the server to the client.	Null		
Client Key	The server assigns the private key of the certificate to the client.	Null		

3.3.2 Semtech UDP Forwarder

General Settings

General Settings	Status	
∧ Gateway Setti	ings	
	Enable	ON OFF
	LoRaWan Public	ON OFF
	Server Address	127.00.1
	Server Uplink Port	1780
	Service Downlink Port	1782
	Keepalive Interval	10
	statistics Refresh Interval	300
	Push Timeout Millisecond	120
6	Verbose Debug Enable	ON OFF

	General Settings Gateway Settings				
Item	Description	Default			
Enable	Click the toggle button to enable/disable this option.	OFF			
LoRaWan Public	Click the toggle button to enable/disable this option.	ON			
Server Address	Set the Server address.	127.0.0.1			
Server Uplink		1700			
Port	UDP uplink connection port.	1780			
Service	LIDD downlink connection nort	1782			
Downlink Port	UDP downlink connection port.	1/82			
Keepalive	Time interval for obtaining downlink data	10			
Interval	Time interval for obtaining downlink data.	10			
Statistics	Statistical internal USI undeto internal	200			
Refresh Interval	Statistical interval, USI update interval.	300			
Push Timeout	Unlink data timogut	120			
Millisecond	Uplink data timeout.	120			
Verbose Debug	Click the toggle button to enable/disable this option. Enable verbose	OFF			
Enable	debugging information output.	OFF			

	Status
Item	Description
	Basic
Status	Show LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show version of Packet forwarder.
HAL Library Version	Show driver version of LoRaWAN chipset inside gateway.
	Uplink
RF packets forwarded	Packets that CRC verified are sent from gateway to server.
Push Data Datagrams Sent	Total quantity of packets sent from gateway to server, including RF packets
	forwarded and statistics packets.
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent:
	Downlink
Pull Data Sent	Show the number of keepalive packets sent to the server, and the percentage of
	acknowledged packets regarding the keepalive packet from the server.
Pull Resp Datagrams Received	Show packet counts and sizes that will be sent from server to gateway.

This section allows you to view the status of Semtech UDP Forwarder.



3.4 Network

3.4.1 Route

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

Static Route

Static R	oute	Status	· · · · · · · · · · · · · · · · · · ·				
^ Static	Route Table						7
Index	Description	Destination	Netmask/Prefi	Gateway	Interface	VID	+

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

Static Route		
∧ Static Route		n j
Index	1	
Description		
Destination		3
Netmask/Prefix Length		3
Gateway		3
Interface	wwan1 v	
VID	0	3
		Submit Close

Static Route				
Item	Description	Default		
Index	Indicate ordinal of list.			
Description	Enter a description for this static route.	Null		
Destination	Enter IP address of destination host or destination network.	Null		
Netmask/Prefix Length	Enter Netmask of destination host or destination network.	Null		
Device	Define device of destination.	Null		
Interface	Choose corresponding port of the link that you want to configure.	wwan		
VID	Ener VLAN ID. 0 means no VLAN ID.	0		

Static Ro	ute S	tatus				
^ Route 1	Table					
Index	Destination	Netmask/Prefix	Gateway	Interface	Metric	
1	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0	~
2	fe80::	64	::	lan0	256	~
3	fe80::	64	::	eth1	256	~
4	fe80::	64	::	eth1.1	256	~
5	fe80::	64	::	wan	256	~
6	fe80::	64	::	wwan	256	V
7	ff00::	8	::	lan0	256	~
8	ff00::	8	::	eth1	256	×
9	ff00::	8	::	eth1.1	256	~
10	ff00::	8	::	wan	256	~
11	ff00::	8	::	wwan	256	~

This window allows you to view the status of the device.

3.4.2 Firewall

This section allows you to set the firewall and its related parameters, including Filtering, NAT, and IPset. The filtering rules can be used to either accept or block certain users or ports from accessing your device. Click "**Network> Firewall> Filter**". The following information is displayed:

Filtering	NAT	Advanced	Custom Rules	Status
∧ General Settings				
	Enabl	e Filtering ON O	FF	
	Default Filter	ing Policy Accept	v 🦻	
	Remote In	put Policy Drop	V	
	Local In	put Policy Accept	v	



+

 Access Control Settings 	
Enable Remote SSH Access	OFF
Enable Local SSH Access	ON OFF
Enable Remote Telnet Access	ONDOFF
Enable Local Teinet Access	ON
Enable Remote HTTP Access	ONOFF
Enable Local HTTP Access	ON OFF
Enable Remote HTTPS Access	ON OFF
Enable Remote Ping Respond	ON OFF ?
Enable DOS Defending	ON OFF
Enable VPN NAT Traversal	OFF 😨
∧ Whitelist Rules	(?)

Index	Description	S

Filtering	
∧ Whitelist Rules	
Index Description Source Address	
∧ Filtering Rules	
Index Source Address Source Port Source M	AC Target Address Target Port Protocol +

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.

Click + to add the whitelist rules.



Filtering	
∧ Filtering Rules	
Index	1
Description	
Invert Source Address	ON OFF 😨
Source Address	
Source MAC	
Invert Target Address	ON OFF 2
Target Address	
Protocol	All
Action	Drop
	Submit Close

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

∧ Filtering Rules	
Index	1
Description	
Invert Source Address	ON OFF 7
Source Address	
Source Port	
Source MAC	
Invert Target Address	ON OFF 7
Target Address	
Target Port	
Protocol	ТСР
Action	Drop

Filtering				
Item	Description	Default		
General Settings				
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON		



Filtering				
Item	Description	Default		
Default Filtering Policy Select from "Accept" or "Drop". • Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list • Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list				
Remote Input Policy	 Select from "Accept", "Drop" or "Reject". Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list Reject: Device will reject all the connecting requests except the hosts which fit the accepted filter list Reject: Device will reject all the connecting requests except the hosts which fit the accepted filter list, and a deny (terminate) packet is returned 	Drop		
Local Input Policy	 Select from "Accept", "Drop" or "Reject". Accept: Device will accept all the connecting requests except the hosts which fit the drop filter list Drop: Device will drop all the connecting requests except the hosts which fit the accepted filter list Reject: Device will reject all the connecting requests except the hosts which fit the accepted filter list, and a deny (terminate) packet is returned 	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 device 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 device locally via SSH.	ON		
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the device 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 device 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 device 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 device 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 device remotely via HTTPS.	ON		
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the device 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 device will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON		



	Filtering				
Item	Description	Default			
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 ordinal of 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 ordinal of list.				
Description	Enter a description for this filtering rule.	Null			
Invert Source Address	Enable to invert source address the user input	OFF			
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			
Invert Target Address	Enable to invert target address the user input	OFF			
Target Address	Enter target address which the access originator wants to access.	Null			
Target Port	Enter target port that the access originator wants to access.	Null			
Protocol	Select from "All", "TCP", "UDP", "ICMP", "ICMPv6" or "TCP-UDP".	All			
	Note : It is recommended that you choose "All" if you don't know which				
	protocol of your application to use.				
Action	Select from "Accept" or "Drop".	Drop			
	• Accept: When Default Filtering Policy is dropped, the device will				
	drop all the connecting requests except the hosts which fit this				
	accepted filtering list.				
	• Drop: When Default Filtering Policy is accepted, the device will				
	accept all the connecting requests except the hosts which fit this				
	drop filtering list.				

NAT

This section allows you to set the NAT related feature, including DMZ, Port Mapping, and NAT.

Filte	ering	NAT	Advanced	Cu	stom Rules	Status	
^ NAT	Helpers						
			SIP 0	OFF 😨			
^ DMZ	Settings						
		E	nable DMZ	OFF			
		Host	IP Address				
		Source	IP Address				
^ Port	Mapping Rule	s					?
Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol	+
^ NAT	Rules			ويناطون			?
Index	Description	Source Addres	s Out	Targe	t Address	NAT IP	+

NAT Helpers provide a pass-through for VoIP communications between the router's LAN and WAN. Click "**Network> Firewall> NAT> NAT Helpers**". The following information is displayed:

∧ NAT Helpers		
	SIP OFF ?	
·	NAT Helpers	

in the pers		
Item	Description	Default
SIP	Click the toggle button to enable/disable SIP ALG. It provide a pass-through for	OFF
	VoIP communications between the router's LAN and WAN.	

DMZ (Demilitarized Zone), also known as the demilitarized zone. It is a buffer between a non-secure system and a security 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> NAT> DMZ". The following information is displayed:

∧ DMZ Settings	
Enable DMZ	ON OFF
Host IP Address	
Source IP Address	()

July. 10, 2024





DMZ Settings				
Item	Description	Default		
Enable DMZ	Click the toggle button to enable/disable DMZ. DMZ host is a host on the	OFF		
	internal network that has all ports exposed, except those ports otherwise			
	forwarded.			
Host IP Address	Enter IP address of the DMZ host on your internal network. Support input for	Null		
	IPv6 addresses.			
Source IP Address	Set address which can talk to the DMZ host. Null means for any addresses.	Null		
	Support input for IPv6 addresses.			

Port mapping is defined manually in the device, 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> NAT> Port Mapping**" to display the following:

∧ Port M	lapping Rules	5					?
Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol	+

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

NAT		
∧ Port Mapping Rules		
Index	1	
Description		
Remote IP		0
Remote Port		0
Internet IP		0
Interface	unspecified v	
Internet Port		0
Local IP		
Local Port		0
Protocol	TCP-UDP v	
		Submit Close

Port Mapping Rules					
Item	Description	Default			
Index	Indicate ordinal of 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	Null			



Port Mapping Rules					
Item	Description	Default			
	means unlimited, And support input for IPv6 addresses. e.g.,				
	10.10.10/255.255.255.255 or 192.168.1.0/24.				
Remote Port	Specify the port of the host or network which can access the local IP	Null			
	address. Empty means unlimited.				
Internet IP	Enter Internet IP of the device which can be accessed by other hosts from	Null			
	the Internet.				
Interface	Choose corresponding port of the link that you want to configure.	Unspecified			
Internet Port	Enter Internet port of the device which can be accessed by other hosts	Null			
	from Internet.				
Local IP	Enter device's LAN IP which will forward to the Internet port of device.	Null			
	Support input for IPv6 addresses.				
Local Port	Enter port of device's LAN IP.	Null			
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP			

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

^ NAT	Rules					?
Index	Description	Source Address	Out	Target Address	NAT IP	+

Click 🕇 to add custom rules.

∧ NAT Settings				
Index	1			
Description				
Source Address		7		
Out	unspecified v			
Target Address		7		
NAT IP		?		
			Submit	Close

NAT Settings						
Item	Description	Default				
Index	Indicate ordinal of list.					
Description	Enter a description of this NAT rule.	Null				
Source Address	Enter source address in the format x.x.x.x or X:X:X:X:X:X:X, x.x.x.x/xx or X:X:X:X:X:X:X:X:X/xxx, x.x.x.x.x.x or X:X:X:X:X:X:X:X:X:X:X:X:X:X:X:X:X:X:X:	Null				
Out	Select output interface. Selecting unspecified means any output interface.	unspecified				



Target Address	Enter target address in the format x.x.x.x or X:X:X:X:X:X:X:X.	Null
NAT IP	Enter NAT address in the format x.x.x.x.	Null

Advanced

IP sets are a framework inside the Linux kernel, which can be administered by the IPset utility. Depending on the type, an IP set may store IP addresses, networks, (TCP/UDP) port numbers, MAC addresses, interface names, or combinations of them in a way, which ensures lightning speed when matching an entry against a set. Click "**Network> Firewall> Advanced**". The following information is displayed:

Filtering		NAT	Advan	ced	Custom Rule	s	Status
^ Advance	d Settings						
		Ena	able Ipset	ON OF	3		
		Default In	put Policy	Accept	v		
		MAC	List Name	mac		?	
		MAC L	ist Action	Drop	×		
		IP Port	List Name	ip-port		2	
		IP Port L	ist Action	Drop	v		
		Net	List Name	net		2	
		Net L	ist Action	Drop	V		
^ MAC List							⑦ +
Index	MAC						+
∧ IP Port L	.ist						?
Index Prot	tocol	IP	Port				+
∧ Net List							7
Index	Net						+

Advanced			
∧ MAC List			
Index	1)	
МАС)	
		Submit	Close

Click + to add a MAC list. The maximum count is **50**.





Click + to add an IP Port list. The maximum count is **50**.

Advanced			
∧ IP Port List			
Index	1		
Protocol	TCP		
IP			
Port		0	
		Submit	Close

Click + to add a Net list. The maximum count is **50**.

Advanced	
∧ Net List	
Index	1
Net	0
	Submit Close

Advanced					
Item	Description	Default			
General Settings					
Enable Ipset	Click the toggle button to enable/disable the lpset option.	ON			
Default Input Policy	Select from "Accept" or "Drop".	Accept			
	Accept: Device will accept all the input connecting requests				
	except the hosts which fit the drop list of MAC/ IP-Port/ Net.				
	Drop: Device will drop all the input connecting requests except				
	the hosts which fit the accepted list of MAC/ IP-Port/ Net.				
MAC List Name	Enter the name of the MAC list. It cannot support entering pure	mac			
	numbers.				
MAC List Action	Select from "Accept" or "Drop".	Drop			
	• Accept: When Default Input Policy is dropped, the device will drop				
	all the connecting requests except the hosts which fit this accepted				
	MAC list.				
	• Drop: When Default Input Policy is accepted, the device will accept				
	all the connecting requests except the hosts which fit this drop				
	MAC list.				
IP Port List Name	Enter name of the MAC list. It cannot support entering pure numbers.	ip-port			



Advanced				
Item	Description	Default		
IP Port List Action	Select from "Accept" or "Drop".	Drop		
	Accept: When Default Input Policy is dropped, the device will drop			
	all the connecting requests except the hosts which fit this			
	accepted IP Port list.			
	• Drop: When Default Input Policy is accepted, the device will accept			
	all the connecting requests except the hosts which fit this drop IP			
	Port list.			
Net List Name	Enter the name of the MAC list. It cannot support entering pure	net		
	numbers.			
Net List Action	Select from "Accept" or "Drop".	Drop		
	Accept: When Default Input Policy is dropped, the device will drop			
	all the connecting requests except the hosts which fit this			
	accepted Net list.			
	Drop: When Default Input Policy is accepted, the device will accept			
	all the connecting requests except the hosts which fit this drop Net			
	list.			
	MAC List			
Index	Indicate ordinal of the list.			
MAC address	Enter the MAC address. Format: XX:XX:XX:XX:XX:XX.	Null		
	IP Port list			
Index	Indicate ordinal of list.			
Protocol	Select from "TCP", or "UDP".	ТСР		
IP	Enter IP address. Format: x.x.x.x or X:X:X:X:X:X:X:X	Null		
Port	Enter port number.	Null		
	Net list			
Index	Indicate ordinal of list.			
Net	Enter domain name/ IP/ IP segment. Format: x.x.x.x or X:X:X:X:X:X:X,	Null		
	x.x.x.x/xx or X:X:X:X:X:X:X:X/xxx, or domain name.			

Custom Rules

This section allows you to add rules that define yourself. Click "**Network> Firewall> Custom Rule**" to display the following:

^ Custo	m Iptables Rules		(?)
Index	Description	Rule	+
^ Custo	m Ip6tables Rules		?
Index	Description	Rule	+

Click 🛨 to add custom rules. The maximum count is 5**0**.



Custom Rules	
∧ Custom Iptables Rule	
Index	1
Description	
Rule	

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

Custom Rules			
∧ Custom Ip6tables Rule			
Index	1		
Description			
Rule		0	
		Submit	Close

Custom Ip6tables Rules					
Item	Description	Default			
Index	Indicate ordinal of list.				
Description	Enter a description for these Custom Firewall Rules for IPv6.	Null			
Rule	Enter custom rules.	Null			

This section allows you to view the status of the device's firewall.



ndex	Packets	Target	Protocol	In	Out	Source	Destination	
1	1536	ACCEPT	all	lo	*	0.0.0/0	0.0.0/0	~
2	0	ACCEPT	tcp	lan+	*	0.0.0/0	0.0.0/0	~
3	0	DROP	tcp	lan+	35	0.0.0/0	0.0.0.0/0	~
4	1147	ACCEPT	tcp	lan+	*	0.0.0/0	0.0.0/0	~
5	0	ACCEPT	tcp	lan+	*	0.0.0/0	0.0.0/0	~
6	0	REJECT	tcp	*	se.	0.0.0/0	0.0.0/0	~
7	4	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0	~
8	0	DROP	tcp	*	*	0.0.0/0	0.0.0/0	N
9	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0/0	~
10	0	DROP	tcp	*	*	0.0.0/0	0.0.0/0	~
11	0	ACCEPT	icmp	*	35	0.0.0/0	0.0.0.0/0	~
12	0	DROP	icmp	*	*	0.0.0/0	0.0.0/0	~
13	0	ACCEPT	all	lo	*	::/0	::/0	~
14	0	ACCEPT	tcp	lan+	*	::/0	::/0	~
15	0	DROP	tcp	lan+	*	::/0	::/0	~
16	0	ACCEPT	tcp	lan+	*	::/0	::/0	1
17	0	ACCEPT	tcp	lan+	*	::/0	::/0	~
18	0	REJECT	tcp	*	*	::/0	::/0	~
19	0	ACCEPT	tcp	*	*	::/0	::/0	1
20	0	DROP	tcp	*	*	::/0	::/0	1
21	0	ACCEPT	tcp	312	*	::/0	::/0	1
22	0	DROP	tcp	34	*	::/0	::/0	1
23	0	ACCEPT	icmpv6	sk	*	::/0	::/0	
24	0	DROP	icmpv6	*	*	::/0	::/0	1

Forward							
Packets	Target	Protocol	In	Out	Source	Destination	
0	TCPMSS	tcp	*	*	0.0.0/0	0.0.0/0	~
0	TCPMSS	tcp	*	*	::/0	::/0	~
Output							
Packets	Target	Protocol	In	Out	Source	Destination	
Prerouting	g						
Packets	Target	Protocol	In	Out	Source	Destination	
Postroutin	ng						
Packets	Target	Protocol	In	Out	Source	Destination	
FIREWALI		OSTROUTI	NG			Same	
Packets	Target	Protocol	In	Out	Source	Destination	
FIREWALI	L_NAT_P	REROUTIN	G		gili		
Packets	Target	Protocol	In	Out	Source	Destination	
	Packets 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	PacketsTarget0TCPMSS0TCPMSSOutputTargetPacketsTargetPacketsTargetPacketsTargetFIREWALL_NAT_POPacketsTarget	PacketsTargetProtocol0TCPMSStcp0TCPMSStcp0TCPMSStcpOutputPacketsTargetPacketsTargetProtocolPostroutingProtocolProtocolPacketsTargetProtocolPacketsTargetProtocolFIREWALL_NAT_POSTROUTIIProtocolFIREWALL_NAT_PREROUTINProtocol	PacketsTargetProtocolIn0TCPMSStcp*0TCPMSStcp*0TCPMSStcp*OutputProtocolInPacketsTargetProtocolInPacketsTargetProtocolInPacketsTargetProtocolInPacketsTargetProtocolInPacketsTargetProtocolInFIREWALL_NAT_POSTROUTINGInInFIREWALL_NAT_PREROUTINGIn	PacketsTargetProtocolInOut0TCPMSStcp**0TCPMSStcp**0TCPMSStcp**Output***PacketsTargetProtocolInOutPrerouting****PacketsTargetProtocolInOutPostrouting****PacketsTargetProtocolInOutFIREWALL_NAT_POSTROUTING**PacketsTargetProtocolInOutFIREWALL_NAT_PREROUTING***	PacketsTargetProtocolInOutSource0TCPMSStcp**0.0.0.0/00TCPMSStcp**::/0Output**::/0PacketsTargetProtocolInOutSourcePrerouting**Source*PacketsTargetProtocolInOutSourcePacketsTargetProtocolInOutSourcePacketsTargetProtocolInOutSourceFIREWALL_NAT_POSTROUTINGInOutSourceFIREWALL_NAT_PREROUTINGInOutSource	PacketsTargetProtocolInOutSourceDestination0TCPMSStcp**0.0.0.0/00.0.0.0/00TCPMSStcp**::/0::/00TCPMSStcp**::/0::/0Output***::/0SourceDestinationPacketsTargetProtocolInOutSourceDestinationPacketsTargetProtocolInOutSourceDestinationPacketsTargetProtocolInOutSourceDestinationPacketsTargetProtocolInOutSourceDestinationFIREWALL_NAT_POSTROUTINGInOutSourceDestinationFIREWALL_NAT_PREROUTINGInOutSourceDestination



3.4.3 IP Passthrough

Click "Network > IP Passthrough > IP Passthrough" to enable or disable the IP Passthrough option.

IP Passthrough	
∧ General Setting	
	Enable OFF

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

Note:

- (1) The IP Passthrough function can only assign one network provider address.
- (2) To use this function, the main link needs to be set to WWAN, and the backup link needs to be set to None.

3.4.4 PPPoE Bridge

This section is used to set parameters related to the PPPoE bridging function. When this function is enabled, the downstream device can obtain the WWAN IP address through PPPoE dial-up.

Note: To use this function, the primary link needs to be set to WWAN and the backup link needs to be set to None. Click "**Network > PPPoE Bridge > PPPoE Bridge**" to configure the PPPoE bridge function.

PPPoE Bridge	Status				
∧ General Settir	ngs	<u>م</u>			
		Enable	ON OFF		
		Username		0	
		Password			

General Settings@PPPoE Bridge					
Item	Description	Default			
Enable	Enable/disable PPPoE bridging function.	OFF			
Username	Enter a custom username for authentication and obtaining an IP address.	NULL			
Password	Enter the password corresponding to the customized username for authentication and obtaining an IP address.	NULL			

Status

This section is used to view the status of PPPoE bridge.


PPPoE Bridge	Status	
^ Status		
	Status	
	Client IP Address	
	Client Connect Time	

Note: Click "Network > PPPoE Bridge > Status" to view the current application running status, client IP, and last connection duration.

3.5 VPN

3.5.1 IPsec

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

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

General

General	Tunnel	Stati	us	x509	
∧ General Settin	gs				
		Keepalive	20	7	
	Optimize DH Exp	onent Size	ON	F	
	Del	oug Enable	ON OF		
	Enable Backu	p Gateway	ON OF	F	



The window is displayed below when enabling "Enable Backup Gateway".



	General Settings @ General				
Item	Description	Default			
Keepalive	Set the time to live in seconds. The device sends keep-alive packets to the	20			
	NAT (Network Address Translation) server at regular intervals to prevent				
	the records on the NAT table from disappearing.				
	Click the toggle button to enable/disable this option. When enabled, when	OFF			
Optimize DH Size	using dhgroup17 or dhgroup18, it helps to shorten the time to generate				
	the DH key.				
Dahug Enabla	Click the toggle button to enable/disable this option. Enable IPsec VPN	OFF			
Debug Enable	information output to the debug port.				
	-1: Absolutely silent	-1			
	0: Very basic auditing logs, (e.g. SA up/SA down)				
Debuglovel	1: Generic control flow with errors, a good default to see whats going on				
Debug Level	2: More detailed debugging control flow				
	3: Including RAW data dumps in hex				
	4: Also include sensitive material in dumps, e.g. keys				
Enable Backup Gateway					
Monitor Interval	Enter Monitor Interval. Unit: second.	30			
Monitor Times	Enter number maxim of IPsec primary device not answered.	5			

Tunnel

Gener	al	Tunnel	Statu	s x5	09	
∧ Tunne	l Settings	3				
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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



∧ General Settings		
Index	1	
Enable	ON OFF	
Description		
Gateway		0
Backup Gateway		0
Mode	Tunnel	
Protocol	ESP v	
Local Subnet		3
Local Protoport		0
Remote Subnet		3
Remote Protoport		0
Link Binding	Unspecified v	?

	General Settings @ Tunnel	
Item	Description	Default
Index	Indicate ordinal of list.	
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter address of remote side IPsec VPN server. 0.0.0.0 represents any address,	Null
	e.g., 172.16.0.1 or 2001:1520::1	
Backup Gateway	Enter backup address of remote side IPsec VPN server. Empty means disable, e.g.,	Null
	172.16.0.2 or 2001:1520::2	
Mode	Select "Tunnel" and "Transport".	Tunnel
	• Tunnel: Commonly used between devices, or at an end-station to a device,	
	the device acting as a proxy for the hosts behind it.	
	• Transport: Used between end-stations or between an end-station and a	
	device, if the device is being treated as a host-for example, an encrypted	
	Telnet session from a workstation to a device, in which the device is the	
	actual destination.	
Protocol	Select the security protocols from "ESP" and "AH".	ESP
	• ESP: Use the ESP protocol.	
	AH: Use the AH protocol.	
Local Subnet	Enter local subnet's address with a mask protected by IPsec, e.g. 192.168.0.0/24;	Null
	192.168.1.0/24; 2001:1520:2222::/64, 0.0.0.0/0 or ::/0 means any subnet.	
Local Protoport	Enter protocol with port, e.g., tcp/443; udp/1701.	Null
	Local protoport and remote protoport must be the same if both are not empty.	
Remote Subnet	Enter remote subnet's address with a mask protected by IPsec, e.g.	Null



	10.8.0.0/24;10.8.1.0/24; 2001:3000:3333::/64, 0.0.0.0/0 or ::/0 means any	
	subnet.	
Remote Protoport	Enter protocol with port, e.g., tcp/443; udp/1701.	Null
	Local protoport and remote protoport must be the same if both are not empty.	
Link binding	Select link to build IPsec.	Unbound

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



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

∧ IKE Settings	
ІКЕ Туре	IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400 🦻



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

▲ IKE Settings	
ІКЕ Туре	[IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 Y
IKE DH Group	DHgroup2 V
Authentication Type	PKCS#12 V
Private Key Password	
IKE Lifetime	86400 🦻

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

∧ IKE Settings	
ІКЕ Туре	IKEv1 V
Negotiation Mode	Main v
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
IKE DH Group	DHgroup2
Authentication Type	xAuth PSK v
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400 😨



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



	IKE Settings	
Item	Description	Default
ІКЕ Туре	Select from "IKEv1" and "IKEv2".	IKEv1
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1.	Main
	If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE	
	negotiation mode must be aggressive. In this case, SA can be established as	
	long as the username and password are correct.	
Encrypt Algorithm	Select from "3DES", "AES128", "AES192" and "AES256" to be used in IKE	3DES
	negotiation.	
	• 3DES: Use 168-bit 3DES encryption algorithm in CBC mode.	
	• AES128: Use 128-bit AES encryption algorithm in CBC mode.	
	• AES128: Use 192-bit AES encryption algorithm in CBC mode.	
	• AES256: Use 256-bit AES encryption algorithm in CBC mode.	
Authentication	Select from "MD5", "SHA1", "SHA2 256", or "SHA2 512" to be used in IKE	SHA1
Algorithm	negotiation.	
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14",	DHgroup2
	"DHgroup15", "DHgroup16", "DHgroup17", or "DHgroup18" to be used in key	
	negotiation phase 1.	
Authentication Type	Select from "PSK", "CA", "xAuth PSK"," PKCS#12", and "xAuth CA" to be used	PSK
	in IKE negotiation.	
	PSK: Pre-shared Key.	
	CA: Certification Authority.	
	• xAuth: Extended Authentication to AAA server.	
	PKCS#12: Exchange digital certificate authentication.	



IKE Settings			
Item	Description	Default	
PSK Secret	Enter pre-shared key.	Null	
Local ID Type	 Select "Default", "Address", "FQDN" and "User FQDN" for IKE negotiation. Default: Uses an IP address as the ID in IKE negotiation. Address: Uses the local device or endpoint's IP address as the identifier in the IKE negotiation, e.g., 172.16.0.1 or 2001:1520::1. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any sign (@) for the local security device, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option if this option is selected, type a name string with a sign "@" for the local 	Default	
Remote ID Type	 security device, e.g., test@robustel.com. Select "Default", "Address", "FQDN" and "User FQDN" for IKE negotiation. Default: Uses an IP address as the ID in IKE negotiation. Address: Uses the remote device or endpoint's IP address as the identifier in the IKE negotiation, e.g., 192.168.10.1 or 2001:2110::1. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any sign (@) for the local security device, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security device, e.g., test." 	Default	
IKE Lifetime	Set lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as 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 private key under "CA" and "xAuth CA" authentication types.	Null	
Username	Enter username used for "xAuth PSK" and "xAuth CA" authentication types.	Null	
Password	Enter password used for "xAuth PSK" and "xAuth CA" authentication types.	Null	



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



✓ IKE Settings	
∧ SA Settings	
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
PFS Group	PFS(N/A)
SA Lifetime	28800
DPD Interval	30
DPD Failures	150 🕝



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

	Sec. 8 Locks 6
Tunnel	
∧ General Settings	
Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	AH
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	(
Link Binding	Unspecified v
∧ SA Settings	
Encryption Algorithm	3DES v
Authentication Algorithm	SHA1 v
PFS Group	PFS(N/A)
SA Lifetime	28800
DPD Interval	30
DPD Failures	150 🦻
∧ Advanced Settings	
Enable Compression	ON OFF
Enable Forceencaps	ON OFF 7
Conntrack Flush	ON OFF
Expert Options	



	SA Settings	
Item	Description	Default
Encrypt Algorithm	Select "3DES", "AES128", "AES192", or "AES256" when you select "ESP" in	3DES
	"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.	
Authentication	Select from "MD5", "SHA1", "SHA2 256", or "SHA2 512" to be used in SA	SHA1
Algorithm	negotiation.	
PFS Group	Select from "PFS(N/A)", "DHgroup1", "DHgroup2", "DHgroup5",	PFS(N/A)
	"DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18"	
	to be used in SA negotiation.	
SA Lifetime	Set the IPsec SA lifetime. When negotiating to set up IPsec SAs, IKE uses the	28800
	smaller one between the lifetime set locally and the lifetime proposed by	
	the peer.	
DPD Interval	Set interval after which DPD is triggered if no IPsec protected packets are	30
	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.	
DPD Failures	Set timeout of DPD (Dead Peer Detection) packets.	150
	Advanced Settings	
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress	OFF
	the inner headers of IP packets.	
Enable Forceencaps	Click the toggle button to enable/disable this option. After it is enabled,	OFF
	even if no NAT condition is detected, the UDP encapsulation of esp packets	
	is forced. This may help overcome restrictive firewalls.	
Conntrack Flush	Click the toggle button to enable/disable this option. Clear conntrack after	OFF
	establishing IPsec.	
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc,	Null
	e.g. protostack=netkey;plutodebug=none.	



Status

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

Gener	al	Tunnel	Status	x509		
∧ IPSec	Tunnel Sta	tus				
Index	Description	Status	Uptime			
∧ Proxy	Identity St	atus				
index	Destination	gateway	Source address	Destination address	Stat	us Tunnel

x509

Users can upload the certificates for the IPsec tunnel in this section.

General		Funnel	Statu	5	x509		
^ X509 Se	ttings						?
		Tu	nnel Name	Tunnel 1	v		
		Local	Certificate	Choose	File No file chosen		
- 19 - Ba		Remote	Certificate	Choose	File No file chosen		
		P	rivate Key	Choose	File No file chosen		
		CA	Certificate	Choose	File No file chosen		
		PKCS#12	Certificate	Choose	File No file chosen		
^ Certifica	te Files						
Index	File Name		File Size		Modification Ti	me	

	x509					
Item	Description	Default				
	X509 Settings					
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3",	Tunnel 1				
	"Tunnel 4", "Tunnel 5", or "Tunnel 6".					
Local Certificate	Click "Choose File" to locate the certificate file from the local computer, and					
	then import this file into your device.					
Remote Certificate	Click "Choose File" to locate the certificate file from the remote computer,					
	and then import this file into your device.					
Private Key	Click "Choose File" to locate the private key file.					
CA Certificate	Click "Choose File" to locate the correct CA certificate file.					
PKCS#12 Certificate	Click "Choose File" to locate the PKCS # 12 certificate file.					
	Certificate Files					
Index	Indicate the ordinal of the list.					
Filename	Show imported certificate's name.	Null				



x509				
Item	Description	Default		
X509 Settings				
File Size	Show size of certificate file.	Null		
Last Modification	Show time of that last time to modify the certificate file.	Null		

3.5.2 WireGuard

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

WireGuard	Status	x50	9			
∧ General Setti	ngs					
	Enable	WireGuard	ONO	FF		
	P	rivate Key				
	Т	P Address			•	
	1	isten Port	51820			
		мти	1472			
	E	nable NAT	ON O	FF		

WireGuard@General Settings				
Item	tem Descriptions			
Enable WireGuard	Enable WireGuard Enable or disable WireGuard			
Private Key	Private Key Enter local private key. It can be generated automatically or imported manually via X509 settings, but it cannot be empty.			
IP Address	IP Address Enter IP address of the virtual interface. It cannot be empty.			
Listen Port	Enter virtual interface listen port. It cannot be empty.	51820		
MTU	Enter virtual interface slice size.	1472		
Enable NAT	Enable/disable 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	t Host	Endpoint Port		Allowed IPs		+
Click 🕂	to add peer sett	ing. The maximum	count is 20	•					
WireGu	ıard						.Anue.		
^ Peer	[.] Settings								
			Index	1					
		De	scription						
		P	ublic Key						
		Presh	ared Key						
		Endpo	oint Host						
		Endp	oint Port						
		Allo	owed IPs			?			
		Route Allo	owed IPs	ON					
		Persistent K	eepalive	0		?			
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~							Submit	Close	

WireGuard@Peer Settings							
Item	tem Descriptions						
	Peer Settings						
Index	Display index.						
Description	Enter peer descriptions.	Null					
Public Key	Enter public key and it cannot be empty.	Null					
Preshared Key	Enter pre-share key and it cannot be empty.	Null					
Endpoint Host	Enter peer IP address. A null value will not initiate a connection request.	Null					
Endpoint Port	Enter peer port. A null value will not initiate a connection request.	Null					
Allowed IPs	Enter allowed IP address, which cannot be empty.	Null					
Route Allowed IPs	Enable/disable feature. When enabled, routes will be created for the networks allowed for this peer. If the allowed network is 0.0.0/0, this peer will be set as the default route.	ON					
Persistent Keepalive	Enter interval of sending Persistent Keepalive messages, in seconds. 0 means disabling the feature.	0					



#### Status

The status bar allows you 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.

WireGu	ard	Status	x509			
∧ WireG	uard Tunnel S	Status				
Index	Description	Public Key	Virtual IP	Real IP	Port	Latest Handshake

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

WireGuard	Status	x509	
A X509 Settings			
	Р	rivate Key	Generate
	Р	rivate Key	Choose File No file chosen Import
		Public Key	Generate
		Config File	Generate
	(	Config File	Choose File No file chosen Import

	x509			
Item	Item Descriptions			
	X509 Settings			
Private Key	Click Generate button to generate a private key.			
Private Key	Click Choose File button to locate the private key from your computer, and then click Import button to import the private key.			
Public Key	Click Generate button to generate a public key.			
Config File	Click Generate button to generate a config file			
Config File	Click Choose File button to locate the config file from your computer, and then click Import button to import the config file.			

## 3.5.3 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. The device supports point-to-point and point-to-point connections.

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



## OpenVPN

OpenV	PN	Status	x509	
<b>∧</b> Tunne	l Settings	3		
Index	Enable	Description N	lode	+
∧ Passw	ord Mana	ige		l l
Index	Usern	ame		+
∧ Client	Manage			
Index	Enable	Common Name	Client IP Address	+

Click + to add OpenVPN tunnel settings. The maximum count is **5**. "Mode" is set "P2P" by default. The window is displayed below when choosing "P2P" as the mode.

∧ General Settings	
Index	1
Enable	ON OFF
Enable IPv6	ON OFF
Description	
Mode	P2P v 😨
TLS Mode	None v 🔊
Protocol	UDP v
Peer Address	
Peer Port	1194
Listen IP Address	
Listen Port	1194
Interface Type	TUN
Authentication Type	None v 😨



Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
τυν μτυ	1500
Max Frame Size	
Enable Compression	ON OFF
Enable NAT	ON OFF
Verbose Level	0 v 7

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

∧ General Settings	
Index	1
Enable	ON OFF
Enable IPv6	OFF
Description	
Mode	Auto v 🖓
Username	
Password	
Private Key Password	
Enable Client Status	ON OFF ?
Enable NAT	ON DEF



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

∧ General Settings		
Index	1	
Enable	ON OFF	
Description		
Mode	Client	7
Protocol	UDP v	
Peer Address		0
Peer Port	1194	Ĵ
Backup Address		0
Backup Port		Ĵ
Interface Type	TUN	
Authentication Type	None v	0
Renegotiation Interval	86400	0
Keepalive Interval	20	) 🤊
Keepalive Timeout	120	0
τυν μτυ	1500	
Max Frame Size		
Enable Compression	ON OFF	
Enable NAT	ON OFF	
Enable DNS overrid	ON OFF 2	
Verbose Level	0 ~	0

# 10 robustel

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

∧ General Settings			
	Index	1	
	Enable	ON OFF	
	Enable IPv6	ON	
	Description		
	Mode	Server	v 🦻
	Protocol	UDP	v
	Listen IP Address		0
	Listen Port	1194	
	Interface Type	TUN	v
	Authentication Type	None	⊻ 🧿
	Enable IP Pool	OFF	
	Client Subnet	10.8.0.0	0
	Client Subnet Netmask	255.255.255.0	0
	Renegotiation Interval	86400	0
	Max Clients	10	
	Keepalive Interval	20	0
	Keepalive Timeout	120	0
	TUN MTU	1500	
	Max Frame Size		
	Enable Compression	ON OFF	
	Enable Default Gateway	OFF	
	Enable NAT	ON OT	
	Verbose Level	0	v 0



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

∧ General Settings		
Index	1	
Enable	ON OFF	
Description		
Mode	Client v 🖓	
Protocol	UDP v	
Peer Address		
Peer Port	1194	
Backup Address		
Backup Port		
Interface Type	TUN	
Authentication Type	None 🧹 🥱	
Renegotiation Interval	86400	
Keepalive Interval	20	
Keepalive Timeout	120	
TUN MTU	1500	
Max Frame Size		
Enable Compression	ON OFF	
Enable NAT	ON OFF	
Enable DNS overrid	ON OFF 0	
Verbose Level	0 7	



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

∧ General Settings			
	Index	1	
	Enable	ON OFF	
	Description		
and a bar	Mode	Client v	1
	Protocol	UDP	
	Peer Address		3
	Peer Port	1194	
	Backup Address		3
	Backup Port		
	Interface Type	TUN	
	Authentication Type	Preshared v	0
	Encrypt Algorithm	BF v	
	Authentication Algorithm	SHA1 v	
	Renegotiation Interval	86400	1
	<b>Keepalive Interval</b>	20	1
	<b>Keepalive Timeout</b>	120	1
	TUN MTU	1500	
	Max Frame Size		
	Enable Compression	ON OFF	
	Enable NAT	ON OFF	
	Enable DNS overrid	OFF 😨	
	Verbose Level	0 v	7



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

∧ General Settings				
	Index	1	J	
	Enable	ON OFF		
	Description		]	
	Mode	Client	1	
	Protocol	UDP		
	Peer Address		0	
	Peer Port	1194	)	
		(1194		
	Backup Address		]	
	Backup Port		]	
	Interface Type	TUN v		
	Authentication Type	Password v	7	
	Username		]	
	Password		]	
	Encrypt Algorithm	BF		
A	uthentication Algorithm	SHA1 V		
	Renegotiation Interval	86400	) 🤊	
	Keepalive Interval	20	] 🤊	
	Keepalive Timeout	120	) 🤊	
	TUN MTU	1500	]	
	Max Frame Size		]	
	Private Key Password			
	Enable Compression	ON OFF		
	Enable NAT	ON OFF		
	Enable DNS overrid	OFF ?		
	Verbose Level	0	7	



Advanced Settings	
Enable HMAC Firewall	OFF 😨
Enable TLS Crypt	OFF
Enable PKCS#12	ONOFF
Expert Options	

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

∧ General Settings	
Index	
Enable	ON OFF
Description	
Mode	Client V
Protoco	UDP
Peer Address	
Peer Por	1194
Backup Address	
Backup Por	
Interface Type	TUN V
Authentication Type	: X509CA 🗸 🖓
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 V
Renegotiation Interva	86400
Keepalive Interva	20 🥱
Keepalive Timeou	t 120 🦻
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON OFF
Enable NA	ON DEF
Enable DNS overrid	OFF 😨
Verbose Leve	



Advanced Settings	
Enable HMAC Firewall	OFF 😨
Enable TLS Crypt	ON OFF
Enable PKCS#12	ON OFF
Expert Options	

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

∧ General Settings	
Index	1
Enable	ON OFF
Description	
Mode	Client v 🖓
Protocol	UDP v
Peer Address	
Peer Port	1194
Backup Address	0
Backup Port	
Interface Type	TUN
Authentication Type	X509CA Password v
Username	
Password	

	<b>B</b> robustel
v	
V	

Encrypt Algorithm	BF
Authentication Algorithm	SHA1 v
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120
TUN MTU	1500
Max Frame Size	
Private Key Password	
Enable Compression	ON OFF
Enable NAT	ON OFF
Enable DNS overrid	ON OFF 7
Verbose Level	0 V ?
Advanced Settings	
Enable HMAC Firewall	ON OFF 😨
Enable TLS Crypt	ON OFF
Enable PKCS#12	ONOFF
Expert Options	

General Settings @ OpenVPN				
Item	Default			
Index	Indicate ordinal of list.			
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON		
Enable IPv6	Click the toggle button to enable/disable IPv6 support for this OpenVPN tunnel. <i>Note</i> : "Client" mode does not support enabling IPv6.	OFF		
Description	Enter a description for this OpenVPN tunnel.	Null		
Mode	Select from "Auto", "P2P", "Client" or "Server".	P2P		
TLS Mode	Select from "None", "Client" or "Server". When TLS mode is       N         configuared as none, auth_type can confige preshared and none. But       Client and server can only for x509ca.			
Protocol	Select from "UDP", "TCP-Client", or "TCP-Server".	UDP		
Peer Address	Peer Address Enter end-to-end IP address or domain of remote OpenVPN server.			
Peer Port	Peer Port Enter end-to-end listener port or listener port of OpenVPN server.			
Backup Address       e.g. 172.12.0.2 or 2001:3000::2 or empty.         Note: Backup Address is available only "Mode" is Client.		Null		
Backup Port	Note: Backup port is available only "Mode" is Client.	Null		



General Settings @ OpenVPN				
Item	Description	Default		
Listen IP Address	Enter IP address or domain name, e.g., 192.168.20.1 or 2001:5020::100	Null		
	or empty			
Listen Port	Enter listener port at this end.	1194		
Interface Type	Select from "TUN", and "TAP" which are two different kinds of device	TUN		
	interfaces for OpenVPN. The difference between TUN and TAP devices			
	is that a TUN device is a point-to-point virtual device on the network			
	while a TAP device is a virtual device on Ethernet.			
Username	Enter username used for the "Password" or "X509CA Password"	Null		
	authentication type.			
Password	Enter password used for the "Password" or "X509CA Password"	Null		
	authentication type.			
Authentication Type	Select from "None", "Preshared", "Password", "X509CA", and "X509CA	None		
	Password".			
	<b>Note</b> : "None" and "Preshared" authentication types are only working			
	with P2P mode.			
	Click the toggle button to enable/disable this option. When enabled,			
Enable IP Pool	the client will obtain a virtual IP from the address pool.	OFF		
	<b>Note:</b> Enable IP Pool is available only "Mode" is Server.			
Local IP	Enter the local virtual IP.	10.8.0.1		
Remote IP	Enter the remote virtual IP.	10.8.0.2		
Local IPv6	Enter the local virtual IPv6.	2001:db8:1234:		
		:1		
Remote IPv6	Enter the remote virtual IPv6.	2001:db8:1234:		
		:2		
Prefix Length	Enter prefix length when enable "IPV6".	64		
Client Subnet	Client virtual IP network address.	10.8.0.0		
Client Subnet	Client virtual IP network address mask.	255.255.255.0		
Netmask				
IPv6 Client Subnet	Client virtual IPv6 network address.	2001:db8:1234:		
		:		
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES-128", "AES-192", and	BF		
	"AES-256".			
	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			
Authentication	Select from "MD5", "SHA1", "SHA256", "SHA384" or "SHA512".	SHA1		
Algorithm				
Max Clients	Set retention timeout. If the connection continues to timeout during			
	this time, the OpenVPN tunnel will be re-established.	10		
	Note: Max Clients is available only "Mode" is Server.			



	General Settings @ OpenVPN	
Item	Description	Default
Renegotiation	Set renegotiation interval. If the connection fails, OpenVPN will	86400
Interval	renegotiate when the renegotiation interval is reached.	
Keepalive Interval	Set a keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set keepalive timeout. Trigger OpenVPN restart after n seconds pass	120
	without reception of a ping or other packet from remote.	
TUN MTU	Set MTU for the tunnel.	1500
Max Frame Size	Set shard size of the data to be transmitted through the tunnel.	Null
Private Key Password	Enter private key password under "X509CA" and "X509CA password" authentication.	Null
Enable Compression	Click the switch button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable DNS override	Click the switch button to enable/disable this option. When enabled, DNS pushed by the server is received as the local DNS server.	OFF
Enable Bridge With LAN0	Click the toggle button to enable/disable this option. When enabled, the virtual interface can be bridged with Lan0. <b>Note:</b> Enable Bridge with LANO available only "Mode" is Client.	ON
Enable Default Gateway	Click the toggle button to enable/disable this option. When enabled, it will receive the gateway pushed by the server as the local gateway.	OFF
Enable Client Status	Click the toggle button to enable/disable this option. After the server is enabled, it can display the connected client status information.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of the host behind the device will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	<ul> <li>Select the level of the output log and values from 0 to 11.</li> <li>0: No output except fatal errors</li> <li>1~4: Normal usage range</li> <li>5: Output R and W characters to the console for each packet read and write</li> <li>6~11: Debug info range</li> </ul>	0
	Advanced Settings @ OpenVPN	
Item	Description	Default
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable TLS Crypt	Click the toggle button to enable/disable the TLS encryption protocol. TLS Crypt is an option for enhancing OpenVPN security, providing more advanced security.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standards, used to describe personal identity information.	OFF
Enable Client to Client @Server mode	Click the toggle button to enable/dsable this option.	OFF
Enable Dup Client	Click the toggle button to enable/dsable this option.	OFF

General Settings @ OpenVPN			
Item	Item Description		
@Server mode			
Enable IP Persist	Click the toggle button to enable/dsable this option.	ON	
@Server mode			
Expert Options	Enter some other options of OpenVPN in this field. Each expression can	Null	
	be separated by a ';'.		

## Status

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

OpenV	PN	Status	x50	09		
OpenV	PN Tunnel St	atus				
Index	Description	Status	Mode	Uptime	Local IP	Local IPv6
OpenV	PN Client Lis	t				
Index	Common I	Vame	Real IP	Port	Virtual IP	Virtual IPv6

### X509

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

OpenVPN	Statu	s x50	9		-	
^ X509 Set	tings					?
		Tunnel Name	Tunnel 1	· • ]		
		Mode	Client			
		Import Form	Default			
		Root CA	选择文件	未选择任何文件		
		Certificate File	选择文件	未选择任何文件		
		Private Key	选择文件	未选择任何文件		
		TLS-Auth Key	选择文件	未选择任何文件		
		TLS-Crypt Key	选择文件	未选择任何文件		
	р	KCS#12 Certificate	し、选择文件	未选择任何文件		
^ Certificat	e Files					
Index	File Name	File Siz	e	Modification Tin	ne	



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

## 3.5.4 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 GRE protocol: internal protocol encapsulation and private address encapsulation.

#### GRE



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



∧ Tunnel Settings	
Index	1
Enable	ON OFF
Description	
Bridge With LAN	ON OFF
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	ON OFF
Secrets	
МТ	1472
Link Binding	Unspecified 🗸

Tunnel Settings @ GRE			
Item	Description	Default	
Index	Indicate ordinal of list.		
Enable	Click the toggle button to enable/disable this GRE tunnel. GRE (Generic	ON	
	Routing Encapsulation) is a protocol that encapsulates data packets so		
	that it can route packets of other protocols in an IP network.		
Description	Enter a description for this GRE tunnel.	Null	
Bridge with LAN	Click the toggle button to enable/disable this option. When enabled, the	OFF	
	virtual interface can be bridged with lan0.		
Remote IP Address	Set remote real IP address of the GRE tunnel.	Null	
Local Virtual IP Address	Set local virtual IP address of the GRE tunnel.	Null	
Local Virtual Netmask	Set local virtual Netmask of the GRE tunnel.	Null	
Remote Virtual IP Address	Set remote virtual IP Address of the GRE tunnel.	Null	
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all	OFF	
	the traffic of the gateway will go through the GRE VPN.		
Enable NAT	Click the toggle button to enable/disable this option. This option must be	ON	
	enabled when the device is under a NAT environment.		
Secrets	Set key to the GRE tunnel.	Null	
MTU	Enter Maximum Transmission Unit.	1472	
Link Binding	Select link to build GRE.	Unbound	



#### Status

This section allows you to view the GRE tunnel status.

GRE		Status		
∧ GRE tu	nnel status	;		
Index	Description	Status	Local IP Address Remote IP Address	Uptime

## 3.6 Services

## 3.6.1 Syslog

This section allows you to set the Syslog parameters. The system log of the device can be saved the locally, and also supports be sent to remote log server and specified application debugging. By default, the "Log to Remote" option is disabled.

Syslog			
∧ Syslog Settings			
	Enable	ON DEF	
	Syslog Level	Debug	
	Save Position	RAM V	
	Log to Remote	OFF ?	

The window is displayed below when enabling the "Log to Remote" option.

Syslog		
∧ Syslog Settin	gs	
	Enable	ON OFF
	Syslog Level	Debug
	Save Position	RAM V 🖓
	Log to Remote	
	Add Identifier	OFF 0
	Remote IP Address	
	Remote Port	514



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 is from low	Debug
	to high. The lower level will output more Syslog in detail.	
Save Position	Select save position from "RAM", "NVM" or "Console". The data will be cleared	RAM
	after reboot when choosing "RAM".	
	<b>Note</b> : It's not recommended that you save Syslog to NVM (Non-Volatile Memory)	
	for a long time.	
Log to Remote	Click the toggle button to enable/disable this option. Enable the device to send	OFF
	Syslog to the remote Syslog server. You need to enter the IP and Port of the	
	Syslog server.	
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add	OFF
	a serial number to the Syslog message which is used for loading Syslog to	
	RobustLink.	
Remote IP Address	Enter IP address of the Syslog server when enabling the "Log to Remote" option.	Null
	Format: IPv4 address: x.x.x.x, IPv6 address: x:x:x:x:x:x, domain name: xxx.com	
Remote Port	Enter port of the Syslog server when enabling the "Log to Remote" option.	514

## 3.6.2 Event

This section allows you to set the event parameters. The event feature can send alerts by SMS or Email when certain system events occur.

## Notification

Notificat	ion	Event	Qu	ery		
∧ Event №	otification	Group Set	tings			
Index	Description	Send SMS	Send Email	<b>DO Control</b>	Save to NVM	+

Click + button to add an Event parameter.



## Notification

^ General Settings	
Index	1
Description	
Send SMS	ON OFF
Phone Number	()
Send Email	ON OFF
Email Addresses	(
DO Control	ON OFF
DO Index	DO1 v
DO Level	High
Save to NVM	ON OFF ?

General Settings @ Notification		
Item	Description	Default
Index	Indicate ordinal of list.	
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the device will	OFF
	send a notification to the specified phone numbers via SMS if an event occurs. Set	
	the related phone number in " <b>3.6.5 Services &gt; Email</b> ", and use ';' to separate each	
	number.	
Send Email	Click the toggle button to enable/disable this option. When enabled, the device will	OFF
	send a notification to the specified email box via email if an event occurs. Set the	
	related email address in "3.6.5 Services > Email".	
DO Control	Click the toggle button to enable/disable this option. After it is turned on, the event	OFF
	device will send it to the corresponding DO in the form of Low / High level.	
Save to NVM	Click the toggle button to enable/disable this option. Enable to save the event to	OFF
	nonvolatile memory.	

• Event Selection	(2)
System Startup	ON OFF
System Reboot	ON OFF
System Time Update	ON OFF
Configuration Change	ON
Cellular Network Type Change	ON OFF
Cellular Data Stats Clear	ON OFF
Cellular Data Traffic Overflow	ON OFF
Poor Signal Quality	ON OFF
Wan data traffic stats clear	ON OFF
Wan data traffic overflow	ON OFF
Link Switching	ON OFF
WAN Up	ON OFF
WAN Down	ON OFF
WLAN Up	ON OFF
WLAN Down	ON OFF
WWAN Up	ON OFF
WWAN Down	ON OFF
IPSec Connection Up	ON OFF
IPSec Connection Down	ON OFF
OpenVPN Connection Up	ON OFF
OpenVPN Connection Down	ON OFF
LAN Port Link Up	ON OFF
LAN Port Link Down	ON OFF
USB Device Connect	ON OFF
USB Device Remove	ON OFF
DDNS Update Success	ON OFF
DDNS Update Fail	ON OFF
Received SMS	ON OFF
SMS Command Execute	ON OFF
DI 1 ON	ON OFF
DI 1 OFF	ONOFF
DI 1 Counter Overflow	ON OFF





#### Event

This section allows you to set the event.

Notification	Event Que	ery	
A General Settings			
	Signal Quality Threshold	0	] 🦻
	<b>RSRP</b> Threshold	0	0

General Settings @ Event		
Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. The device will generate a log event when the actual threshold is less than the specified threshold. 0 means disable this option.	0
RSRP Threshold	Set signal quality threshold. When the actual threshold is less than the specified RSRP threshold, the device will generate a log event. 0 disables this option. This option is only for 5G networks.	0

## Query

In the following window, you can query various types of event records.

Click **Refresh** to query filtered events.

Click **Clear** to clear the event records in the window.

Notification	Event	Query			
∧ Event Details					
	Sav	e Position RAM	×		
		Filtering			
Jan 01 00:00:08, Jan 01 00:00:08, Jan 01 00:00:08, Jan 01 02:06:08, Jan 01 02:06:08, Jan 01 02:06:08,	system startup LAN port link down, et LAN port link up, eth1 LAN port link down, et LAN port link down, et cellular data traffic cellular data traffic wan data traffic stats configuration change,	L :h2 stats clear, SIM1, stats clear, SIM2, s clear, TX=0KiB, R>	TX=0KiB, RX=0KiB		
				Clear	Refresh

Event Details				
Item	Description	Default		
Save Position	Select events' save position from "RAM" or "NVM".	RAM		
	RAM: Random-access memory.			
	NVM: Non-Volatile Memory.			
Filtering	Enter filtering messages based on the keywords set by users. Click the "Refresh"	Null		
	button, the filtered event will be displayed in the following box. Use "&" to separate			
	more than one filter message, such as message1&message2.			

## 3.6.3 NTP

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



NTP	Status	
∧ Timezone Sett	ings	
	Time Zone	UTC+08:00 V
	Expert Setting	
∧ NTP Client Set	tings	
	Enable	ON OFF
	Primary NTP Server	pool.ntp.org
	Secondary NTP Server	
	NTP Update Interval	0
	<b>Request network port</b>	default
NTP Server Se	ttings	
	Enable	ON OFF

NTP					
Item	m Description				
Time zone Settings					
Time Zone	Click the drop-down list to select the time zone you are in.	UTC +08:00			
Expert Setting Specify time zone with Daylight Saving Time in TZ environme		Null			
	format. The Time Zone option will be ignored in this case.				
NTP Client Settings					
Enable	Click the toggle button to enable/disable this option. Enable to	ON			
	synchronize time with the NTP server.				
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org			
	Format: ipv4 address: x.x.x.x,ipv6 address: x:x:x:x:x:x:x:x				
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null			
	Format: ipv4 address: x.x.x.x,ipv6 address: x:x:x:x:x:x:x:x				
NTP Update interval	Enter interval (minutes) synchronizing the NTP client time with the NTP	0			
	servers. Minutes wait for the next update, and 0 means update only				
	once.				
Request network port	Select Request network port from "default" or "LAN".	default			
NTP Server Settings					
Enable	Click the toggle button to enable/disable the NTP server option.	OFF			

### Status

This window allows you to view the current time of the device and also synchronize the device time.

Click Sync button to synchronize device time with the PC's time.


NTP	Status				
∧ Time					
	Sys	tem Time	2022-07-25 15:30:20		
		PC Time	2022-07-25 15:30:21	Sync	
	Last Upo	date Time	Not Updated		

### 3.6.4 SMS

This section allows you to set SMS parameters. The device supports SMS management, and users can control and configure their devices by sending SMS. For more details about SMS control, refer to <u>4.1.2 SMS Remote Control</u>.

SMS	SMS Testing		
SMS Management Settings			
	Enable	ON OFF	
	Authentication Type	Password v 🝞	
	Phone Number		
	Data Coding Scheme	GSM-7 V 🖓	

SMS Management Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option.	
	<b>Note</b> : If this option is disabled, the SMS configuration is invalid.	
Authentication Type	Select Authentication Type from "Password", "Phonenum" or "Both".	Password
	• Password: Use the same username and password as the WEB manager for	
	authentication. For example, the format of the SMS should be "username:	
	password; cmd1; cmd2;"	
	<b>Note:</b> Set WEB manager password in the <b>System &gt; User Management</b> section.	
	Phonenum: Use the Phone number for authentication, and the 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. The	
	user should set the Phone Number that is allowed for SMS management.	
	The format of the SMS should be "username: password; cmd1; cmd2;"	
Phone Number	Set phone number used for SMS management, and use '; 'to separate each	Null
	number.	
	<i>Note</i> : It can be null when choosing "Password" as the authentication type.	
Data Coding Scheme	Select Data Coding Scheme from "GSM-7" or "ucs2".	GSM-7



### **SMS** Testing

SMS

This section allows you to test the current SMS service whether is available.

∧ SMS Testing Phone Number	
Message	
Result	
	Send

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

10 robustel



### 3.6.5 Email

The email function supports sending the event notifications to the specified recipient by way of an email.

Email	0		
Email Setting	S		
	Enable	OFF	
	Enable TLS/SSL	OFF 7	
	Enable STARTTLS	OFF	
	Outgoing Server		
	Server Port	25	
	Timeout	10	0
	Auth Login	OFF 🕝	
	Username		
	Password		
	From		
	Subject		

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



### 3.6.6 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, and 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 device, which is assigned to you by your ISP.

#### DDNS

DDNS	Status	
∧ DDNS Settings		
	Enable	OFF
	Service Provider	DynDNS
	Hostname	
	Username	
	Password	
	Max Tries	3
	Custom Check IP	
	Enable Fake Address	OFF 😨

The service provider defaults to "DynDNS", as shown below.

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

DDNS	Status	
DDNS Setting	5	
	E	Enable OFF
	Service Pro	ovider Custom V
		URL
	Мах	c Tries 3
	Enable Fake Ad	idress OFF ⑦



When the "NO-IP" service provider is chosen, the window is displayed as below.

DDNS	Status	
A DDNS Settings		
	Enable	OFF
	Service Provider	NO-IP V
	Hostname	
	Username	
	Password	
	Max Tries	3
	Custom Check IP	0
	Enable Fake Address	OFF 😨

When the "3322" service provider is chosen, the window is displayed as below.

DDNS	Status		
> DDNS Settings			
	Enable	OFF	
	Service Provider	3322 V	
	Hostname		
	Username		
	Password		
	Max Tries	3	
	Custom Check IP		
	Enable Fake Address	OFF 😨	

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



Max tries	Enter maximum try times.	3
Custom Check IP	The function of Check IP Server is mainly used to check the current	Null
	public IP address. Null means using the default value.	NUII
Enable Fake Address	Click the toggle button to enable/disable this option. This option can	
	be used to fake an address update with a random address in the	OFF
	203.0.113.0/24 range, before updating with the actual IP address.	

#### Status

This section allows you to view the status of DDNS.

DDNS	Status	
∧ DDNS Status		
	Status	Disabled
	Last Update Time	

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

### 3.6.7 SSH

The device supports SSH password access and secret-key access.

SSH	Keys Management	
∧ SSH Settings		
	Enable	ON OFF
	Port	22
	Disable Password Logins	ON OFF

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



#### **Key Management**

This section allows you to import authorized Keys.

SSH	Keys Management		
∧ Import Au	thorized Keys		
	Authorized Keys	Choose File No file chose	en Import

Import Authorized Keys			
Item Description			
Authorized Keys Click "Choose File" to locate an authorized key from your PC, and then click "Import"			
	to import this key into your device.		
	<i>Note</i> : This option is valid when enabling the password logins option.		

### 3.6.8 Telephone

This section allows you to set the related parameters of the voice function. If your device has voice input, this page is configurable.

#### Note:

- 1) Whether or not voice calls and data transmission can be used simultaneously is dependent upon your ISP network.
- 2) R3010 support "Telephone" feature.

Telephone	Records			
∧ General Settin	gs			
	Wait Number Timeout	5	0	
	Digitmap			

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



### Records

This section allows you to view the call records.

Telep	hone	Records			
Call R	lecords				
		Filt	ering		
type out out	Phone Number 15917451884 13560328286	Start Time Jan 01 00:01:12 Jan 01 00:00:50	Duration 00:00:00 00:00:00		
out in out	15917451884 15917451884 15917451884	Mar 28 19:39:13 Mar 28 19:42:03 Mar 28 20:05:43	00:00:00 00:00:00 00:00:10		
out out out out	15917451884 15917451884 15917451884 15917451884	Mar 28 20:30:48 Mar 28 20:34:01 Jan 01 00:02:01 Jan 01 00:02:15	00:00:18 00:00:47 00:00:00 00:00:00		
out in	15917451884 15917451884	Mar 29 09:49:00 Mar 29 09:49:28	00:00:13 00:00:00		
				Clear	Refresh

General Settings				
tem Description				
Filtering	Set wait number timeout for the dial plan, measured in seconds.			
Clear	Click the button to clear the call record.			
Refresh	Click the button to refresh the call record.			



### 3.6.9 Ignition

This section is used to configure the parameters of Ignition. *Note: R5020 and R2110 support the ignition feature.* 

Ignition				
∧ General Settin	gs			
	Delay shutdown	60	0	
	Genera	I Settings		
Item	Description			Default
Delay shutdown Enter the time in seconds you want to delay power down. The timeout for delayed power down is 60 seconds to 3600 seconds.			60	

### 3.6.10 GPS

This section is used to configure parameters of GPS. The GPS feature of the device can locate and acquire the location information of the device and report it to the designated server.

GPS	Status	Мар	
A General Setting	gs		
	E	able GPS	
	Sync	GPS Time OFF	

~ KSZ3Z Report Settings	
Report to RS232	ON OFF
Report GGA Sentence	ONOFF
Report VTG Sentence	ON OFF
Report RMC Sentence	ON OFF
Report GSV Sentence	ON OFF
Report GNGSA Sentence	ON OFF
Report GNGNS Sentence	ON OFF
Report GLGSV Sentence	ON OFF

GPS			
Item	Description	Default	



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

^ GPS	Servers						
Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port	+

## Click + to add a new GPS Server.

GPS	
<ul> <li>Server Settings</li> </ul>	
Index	1
Enable	ON OFF
Protocol	TCP Client v
Server Address	
Server Port	
Send GGA Sentence	OFF
Send VTG Sentence	ONOFF
Send RMC Sentence	OFF
Send GSV Sentence	OFF
Send GNGSA Sentence	OFF
Send GNGNS Sentence	OR
Send GLGSV Sentence	OFF



Item	Description	Default
Index	Indicate ordinal of list.	
Enable	Click the toggle button to enable/disable the server.	ON
Protocol	Select from "TCP Client", "TCP Server", "UDP".	TCP Client
Server/Local Address	Server or local IP address. Format: IPv4 address: x.x.x.x, IPv6 address: x:x:x:x:x:x:x:x	Null
Server/Local Port	Server or local IP port.	Null
Send GGA Sentence	Click the toggle button to enable/disable this option.	OFF
Send VTG Sentence	Click the toggle button to enable/disable this option.	OFF
Send RMC Sentence	Click the toggle button to enable/disable this option.	OFF
Send GSV Sentence	Click the toggle button to enable/disable this option.	OFF
Send GNGSA Sentence	Click the toggle button to enable/disable this option.	OFF
Send GNGNS Sentence	Click the toggle button to enable/disable this option.	OFF
Send GLGSV Sentence	Click the toggle button to enable/disable this option.	OFF

Advanced Settings	
Remove CR and LF Character	ON OFF
Self-defined GPSID	None 🤍 🤕
Transmit interval	1

Item	Description	Default
Remove CR and LF Character	Enable to remove Carriage return Line Feed character	ON
Self-defined GPSID	The GPSID is appended to the NMEA message before transmit. You can choose "None", "Prefix", and "Suffix".	None
GPSID Header	Added GPSID Header. Usually using 7 upper case.	N/A
Append SN to GPSID	Enable to append SN to GPSID	OFF
Transmit interval	Enter the data reporting period. 0 means no data is uploaded.	1

#### Status

This section allows you to view the status of GPS.



∧ GPS Status	
Status	Not Fixed
UTC Time	
Last Fixed Time	
Satellites In Use	0
Satellites In View	GPS(0), Galileo(0), BeiDou(0), GLONASS(0)
Latitude	0.000000
Longitude	0.000000
Altitude	0.00 m
Speed	0.00 m/s

Item	Description
Status	Shows current GPS status of the device.
	Shows the UTC of a satellite.
UTC Time	<i>Note:</i> The UTC is the world's unified time, not local time.
Last Fixed Time	The time of the last successful positioning.
Satellites In Use	The number of satellites used.
Satellites In View	The number of visible satellites.
Latitude	Shows Latitude information of the device.
Longitude	Shows longitude information of the device.
Altitude	Shows height information of the device.
Speed	Shows speed information of the device.

#### MAP

The Map page displays the device's current coordinates and position on the map. To see the device's location on the map, make sure to attach the GPS antenna to the device and enable GPS on the GPS page.

# Ørobustel



### 3.6.11 Web Server

Web Server	Certificate Management				
∧ General Settings					
	HTTP Port	80	7		
	HTTPS Port	443	0		

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

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

### **Certificate Management**

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

Web Server	Certificate Management		
∧ Import Certi	ficate		
	Import Type	CA	
	HTTPS Certificate	Choose File No file chosen	Import

Import Certificate			
Item	Item Description Default		
Import Type	Select "CA" and "Private Key". CA		
	• CA: a digital certificate issued by the CA center.		
	Private Key: a private key file.		
HTTPS Certificate	Click "Choose File" to locate the certificate file from your PC, and then		



Import Certificate		
Item Description Default		
click "Import" to import this file into your device.		

### 3.6.12 Advanced

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

System	Reboot	
∧ System Settin	gs	
	Device Name	router 🦻
	User LED Type	None 🔽 🕝
		None
		SIM
		OpenVPN
		IPSec

System Settings				
Item	Description	Default		
Device Name	Set the name of this device to display the current device name in the browser tab	router		
	page. Valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.			
User LED Type	Specify display type of your USR LED. Select from "None", "OpenVPN" or "IPsec".	None		
	None: Meaningless indication and the LED is off.			
	SIM: USR indicator showing the sim status.			
	OpenVPN: USR indicator showing the OpenVPN status.			
	IPsec: USR indicator showing the IPsec status.			

#### Reboot

This section allows you to configure the reboot type.

System	n Re	boot			
^ Periodi	c Reboot Settin	gs			
		Periodic Reboot	0	0	
		Daily Reboot Time		0	
∧ Daily R	eboot Time List				
Index	Description	Daily Reboot Time			+

Click 🛨 to add daily reboot time. The maximum count is **5**.

Periodic Reboot Settings			
Item Description Defau		Default	



Periodic Reboot	Set reboot period of the device. 0 means disable. 0		
Daily Reboot Time	Set daily reboot time of device. You should follow the format as HH: MM, in 24h Null		
time frame, otherwise, the data will be invalid. Leave it empty means disable.			
Daily Reboot Time List			
Item Description Defau		Default	
Index	Indicate ordinal of list.		
Index Description	Indicate ordinal of list. Show description for Daily Reboot Time.	 Null	

## 3.6.13 Smart Roaming V2

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

∧ General Settings	
Smart Roaming Enable	OFF

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

^ Health Check	
Health Check Interval	5 🧿
RSSI Quality Check	
RSSI Threshold(2G)	-85
RSSI Threshold(3G)	-95
RSSI Threshold(4G)	-100 🧭
RSRP Quality Check	
RSRP Threshold(4G)	-100 🧭
RSRQ Quality Check	
RSRQ Threshold(4G)	-20
Network Delay Check	
RTT Timeout Threshold	3000
Packet Loss Rate Check	ON OFF ?
Packet Loss Rate Threshold	70 🧿



Health Check			
Item	Descriptions		
Health Check Interval	The health check interval for the current connection is 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.		
RSSI Quality Check	To enable/disable "RSSI Quality Check" feature.	ON	
RSSI Threshold (2G)	Signal strength threshold for 2G networks.	-85 dBm	
RSSI Threshold (3G)	Signal strength threshold for 3G networks.	-95 dBm	
RSSI Threshold (4G)	Signal strength threshold for 4G networks.	-100 dBm	
RSRP Quality Check	To enable/disable "RSRP Quality Check" feature.		
RSRP Threshold (4G)	The reference signal received power threshold for 4G networks.		
RSRQ Quality Check	To enable/disable "RSRQ Quality Check" feature.		
RSRQ Threshold (4G)	The reference signal receiving quality threshold for 4G networks.		
Network Delay Check	To enable/disable "Network Delay Check " feature.		
RTT Timeout Threshold	The reference signal received power threshold for 4G networks.		
Packet Loss Rate Check	Enable/disable "Packet Loss Rate Check" feature.		
Packet Loss Rate Threshold	Packet loss rate threshold value.		

∧ PING Settings	7
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
PING Timeout	5
Ping Tries	3

PING Settings		
Item	Descriptions	Default
Primary Server	The device pings primary address/domain name to detect if current connection is always alive.	8.8.8.8
Secondary Server	The device pings secondary address/domain name to detect if current	114.114.11
	connection is always alive.	4.114

PING Settings		
Item	Descriptions	Default
Ping Timeout	Set 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

<ul> <li>Advanced Settings</li> </ul>	
Use Degraded Network	ON OFF ?
Periodic Restart	0 ?
Daily Restart Time	
Preferred Operator List	

Advanced Settings		
Item	Descriptions	Default
Use Degraded Network	defined as a network that can be connected, but the network quality does not	
Periodic Restart	Set period of rebooting the "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 time point to restart "Smart Roaming" every day in the format of HH: MM (24-hour system). When this item is empty, it means to disable the timer reboot.	Null
Preferred Operator List	Set list of preferred operators by PLMN. If multiple operators are required, use semicolons to separate, e.g., 46000;46001	Null

∧ Status	?
State	Connected
Operator Selection Mode	Automatic
Time Since Last Network Scan Started	0 days, 00:10:04

Status		
Item	Descriptions	



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

A PLMN List
 Index PLMN Status RAT RSSI(dbm) RSRP(dbm) Latency(ms) Packet Loss(%) HealthCheck

## Preferred Operator List

Index PLMN

PLMN List		
Item	Descriptions	
Index	PLMN list index	
PLMN	PLMN = MCC + MNC, which 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 disconnected or does not meet the health check threshold), respectively.	
Preferred PLMN list		
Index	PLMN list index	
PLMN	PLMN = MCC + MNC, which is a combination of mobile country code and mobile network	



PLMN List		
Item	Descriptions	
	code.	

### Select

This section allows you to select the network.

Settings	Status	Select	Log	Speed Test	
∧ Operator S	elect				?
	User Specified Network	Selection	V		
			Forget RPLMN	Rescan Subm	je.
			Porget KPLMN	Kescan Subm	

Operator Select				
Item	Descriptions	Default		
User Specified	Select Specified Network.			
Network Selection				
Forget RPLMN	Forces deletion of all location information from the SIM.			
Rescan	Rescan operator list and this causes Smart Roaming to start again.			
Submit	Submit operator selected by the drop-down box.			

### Log

This section allows you to view the connection log.

Settings	Status	Select	Log	Speed Test
Connection	Log			
Time	Action	Method	Target Network	Outcome
Jul 22 17:25:02	Automatic network change	GUI	46001	Success
Jul 22 17:20:55	Automatic network change	GUI	46001	Success
Jul 22 15:28:35	Router initiated network change	GUI	46001	Success
Jul 22 14:47:01	Router initiated network change	GUI	46001	Success
Jul 22 14:35:26	Router initiated network change	GUI	46001	Success
Jul 22 14:28:50	Router initiated network change	GUI	46001	Success
Jul 22 14:27:31	Router initiated network change	GUI	46001	Success
Jul 22 14:25:15	Automatic network change	GUI	46001	Success
Jul 22 14:07:10	Automatic network change	GUI	46001	Success
Jul 22 01:03:25	Automatic network change	GUI	46001	Success
Jul 21 18:46:58	Automatic network change	GUI	46001	Success

#### Clear

Connection Log			
Clear	Click the button to clear the connection log.		



### Speed Test

This section allows you to test the network speed.

Settings	Status	Select		Log	Speed Test
∖ Speedtest					
Time	Action	Method	Network	Download	Upload
Jul 22 14:46:05	Speedtest	GUI		N/A	N/A

Speedtest

Clear

Speed Test		
Speedtest	Click the button to start the network speed test.	
Clear	Click the button to clear the speed test log.	



### 3.7 System

## 3.7.1 Debug

This section allows you to check and download the Syslog details. Click "Service > Syslog > Syslog Settings" to enable the Syslog.

Syslog		
^ Syslog Detai	ils	
		Log Level Debug v
		Filtering
		syslog.info syslogd started: BusyBox v1.34.1
2022-07-25 16:0 14:47:25 Jul 15		user.notice init[1]: r1520 version 5.0.0_rc1 (18d58ee9), built at
		user.notice eventd[924]: eventd started! uptime=36
		user.notice link_manager[933]: link manager started
		user.debug link_manager[933]: recv action connect from link_manager
		user.debug link_manager[933]: target link WWAN1, state Disconnected
		user.notice link_manager[933]: WWAN1 start connect
		user.info link_manager[933]: WWAN1 is not ready, waiting for
initialization	Live reacti	and this find the feet [soo]. While to not ready, hereing to
	2:51 router	daemon.err ntpdate[1034]: name server cannot be used: Temporary failure
in name resolut		
	· /	daemon.err ntpdate[1034]: no servers can be used, exiting
		user.notice ntpc_mgmt[1028]: ntp client synchronization failed. Reboot
in 1 minute.		
2022-07-25 16:0	2:52 router	user.notice modemd[1035]: modem service started
		user.notice smart roaming[1036]: smart roaming started
		Manual Refresh V Clear Refresh

A Syslog Files				
Index	File Name	File Size	Modification Time	
1	messages	9183	Mon Jul 25 16:05:52 2022	Ŧ

<ul> <li>System Diagnostic Data</li> </ul>	
System Diagnostic Data	Generate
System Diagnostic Data	Download

Syslog				
Item	Description	Default		
	Syslog Details			
Log Level	Select "Debug", "Info", "Notice", "Warn", and "Error" from low to high. The lower level will output more Syslog in detail.	Debug		
Filtering	Enter filtering messages 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	Manual		
	Seconds". You can select these intervals to refresh the log information displayed	Refresh		
	in the following box. If selecting "manual refresh", you should click the refresh			
	button to refresh the Syslog.			
Clear	Click the button to clear the Syslog.			
Refresh	Click the button to refresh the Syslog.			
	Syslog Files			
Syslog Files List	It can show at most 5 Syslog files in the list, the files' name ranges 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. When there is a problem with the			
	device, system diagnostic data can be generated and sent to a Robust technical			
	support representative for assistance.			

### 3.7.2 Update

This section allows you to upgrade the device system and implement system updates by importing and updating

firmware files. Import a firmware file from the PC to the device, 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.

Firmware Update	
∧ Firmware Update	
File	Choose File No file chosen Update

### 3.7.3 App Center

This section allows you to add some required or customized applications to the device. 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 device, 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 to the device again.

For more information about App, please refer t	to http://www.robustel.com/products/app-center/.
^ App Install	
File	Choose File No file chosen Install
App Usage	1.7MB Free/4.0MB Total

The successfully installed app will be displayed in the following list. Click  $\times$  to uninstall the app.

A Installed Apps						
Index	Name	Version	Status	Description		
1	vrrp	3.1.0	Stopped	VRRP Daemon	×	
2	dynamic_route	4.0.0	Stopped	Dynamic Route	×	
3	rcms	4.0.0	Stopped	rcms Client Connected to RCMS	×	

	App Center			
Item	Description	Default		
	App Install			
File	Click on "Choose File" to locate the App file from your PC, and then click Install to			
	import this file into your device.			
	<i>Note</i> : File format should be xxx.rpk, e.g., r1520-vrrp-5.0.0.rpk.			
	Installed Apps			
Index	Indicate ordinal of list.			
Name	Show name of App.	Null		
Version	Show version of App.	Null		
Status	Show status of App.	Null		
Description	Show description for App.	Null		

RT_SM_v.5.3.0

### 3.7.4 Tools

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

### Ping

This section allows you to use the Ping tools.

Ping	Traceroute	Sniff	er	SpeedTest		
∧ Ping						
	1	P Address				
	Number	of Request	5			
		Timeout	1			
		Local IP				
					Start	Stop

Ping			
Item	Description	Default	
IP address	Enter the ping's destination IP address or destination domain. Support	Null	
	IPv4/IPv6 address or domain name, e.g. 10.10.10.10 or 2001:1520:1111::1		
Number of Requests	Specify number of ping requests.	5	
Timeout	Specify timeout of ping requests.	1	
Local IP	Specify local IP from cellular WAN, Ethernet WAN, or Ethernet LAN. Null stands	Null	
	for selecting a local IP address from these three automatically. Support		
	IPv4/IPv6 address, e.g. 10.10.10.10 or 2001:1520:1111::1		
Chart	Click the button to start a ping request, and the log will be displayed in the		
Start	following box.		



Stop	Click the button to stop the ping request.	
------	--------------------------------------------	--

### Traceroute

This section allows you to use the Traceroute tools.

Ping	Traceroute	Sniff	er	SpeedTest		
∧ Traceroute						
	Tra	ce Address				
		Trace Hops	30			
	Tra	ce Timeout	[1			
4						
					Start	Stop

Traceroute			
Item	Description	Default	
Trace Address	Enter trace's destination IP address or destination domain. Support IPv4/IPv6	Null	
	address or domain name, e.g. 10.10.10.10 or 2001:1520:1111::1		
Trace Hops	Specify max trace hops. The device will stop tracing if the trace hops have met	30	
	the max value no matter whether destination has been reached or not.		
Trace Timeout	Specify the timeout of Traceroute request.	1	
Colored and	Click this button to start Traceroute request, and the log will be displayed in		
Start	the following box.		
Stop	Click this button to stop Traceroute request.		





### Sniffer

This section allows you to use the Sniffer tools.

Pir	ng Tracerou	ite Sniff	fer	SpeedTest		
^ Sniffe	er					
		Interface	all	v		
		Host				
		Packets Request	1000			
		Protocol	All	v		
		Status	0			
					Start	Stop
^ Captu	ıre Files					
Index	File Name	File Siz	e	Modification Ti	ne	
1	23-10-25_17-55-04.cap	117568	3	Wed Oct 25 17:55:1	5 2023	OX

	Sniffer			
Item	Description	Default		
Interface	Choose interface according to your Ethernet configuration.	All		
Host	Filter packet that contains the specified IP address. Support IPv4/IPv6 address,	Null		
	e.g. 10.10.10 or 2001:1520:1111::1			
Packets Request	Set packet number that the device can sniffer at a time.	1000		
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All		
Status	Show current status of sniffer.			
Start	Click the button to start sniffer.			
Class	Click the button to stop the sniffer. Once you click this button, a new log file			
Stop	will be displayed in the following List.			
Capture Files	Every time of sniffer log will be saved automatically as a new file. You can find			
	the file from this Sniffer Traffic Data List click 💽 to download the log and			
	click 🗙 to delete the log file. It can cache a maximum of 5 files.			

# 10 robustel

### SpeedTest

This section allows you to use the SpeedTest tools.

Ping	Traceroute	Sniffer	SpeedTest	
∧ Speedtest				
	Numbe	r of threads 10		
	:	Specify URL		
				Start Stop
∧ Speedtest Log				
Time	Download	Upload		
Jan 1 00:18:38	N/A	N/A		
Jan 1 00:06:08	N/A	N/A		
Jan 1 00:02:17	N/A	N/A		
Jan 1 00:01:36	N/A	N/A		
				Clear

SpeedTest			
Item	Description	Default	
Number of threads	Expert setting item, enter the number of threads enabled when executing the	10	
	network speed test script. It is recommended to set it to 10.		
Host	Enter the speed test server URL that you specify to access during the test. If it	Null	
	is empty, the optimal server will be automatically selected.		
Start	Click this button to start the speed test, and the test information will be		
	displayed in real time in the upper window.		
Stop	Click this button to stop execution of the current test.		
Clear	Click this button to clear all test results in the network test log.		



### 3.7.5 Profile

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

Profile Rollback	
A Import Configuration File	
Reset Other Settings to Default	OFF ?
Ignore Invalid Settings	ON OFF 2
XML Configuration File	Choose File No file chosen Import
A Export Configuration File	
Ignore Disabled Features	ON OFF ?
Add Detailed Information	OFF ?
Encrypt Secret Data	ON OFF ?
XML Configuration File	Generate
∧ Default Configuration	
Save Running Configuration as Default	Save 😨
Restore to Default Configuration	Restore

Profile			
Item	Description	Default	
Import Configuration File			
Reset Other Settings to Default	Click the toggle button as "ON" to return other parameters to default settings.	OFF	
Ignore Invalid Settings	Click the toggle button as "OFF" to ignore invalid settings.	OFF	
XML Configuration File	Click on <u>Choose File</u> to locate the XML configuration file from your PC, and then click <b>Import</b> to import this file into your device.		
	Export Configuration File	1	
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	Click Save button to save the surrent running parameters as the default		
Configuration as	Click <b>Save</b> button to save the current running parameters as the default		
Default	configuration.		
Restore to Default	Click the button to rectare the factory defaults		
Configuration	Click the button to restore the factory defaults.		

### Rollback

This section allows you to roll back the configuration.

Profile	Rollback				
Configuration Rollback					
	Save as a Rollba	ckable Archive Sav	re 🕝		
∧ Configu	ration Archive Files			0	
Index	File Name	File Size	Modification Time		

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



### 3.7.6 Access Control

This section is used for settings related to device security access control management. If the same IP address enters an incorrect account or password a specified number of times, this IP will be restricted from accessing the device. It also provides the function of unblocking IP addresses in batches or individually.

**Note:** Before reaching the upper limit of incorrect login attempts, the accumulated number of errors will be cleared after successful login.

Security	Control		
∧ Security			?
	Enable	ON OFF	
	Incorrect Login Attempts	10	

Security@Access Control			
Item	Description	Default	
Enable	Enable/disable secure login access.	ON	
Incorrect Login	If the same IP address has been entered incorrectly for the specified number of	10	
Attempts	times, this IP will be restricted from accessing the device. The value range is		
	1~30.		

Secu	irity	Control				
~ Unbl	ock Settings					
		Unblo	ock All Unblock ?	e e e e e e e e e e e e e e e e e e e		
∧ Logiı	Attempts					?
∧ Logiı Index	Attempts Source Address	Source Port	Destination Address	Failed	Status	0

Control@Access Control			
Item	Description	Default	
Unblock All	Click the button Unblock enable/disable to release the IP addresses that have recorded restricted access on the device in batches.		

*Note:* Supports viewing all restricted access device IPs and unlocks IP restrictions individually.

### 3.7.7 User Management

This section allows you to change your username and password, and create or manage user accounts.



### **User Settings**

Admin	istrator Settings	7
Index	Username	
1	admin	
Comm	on User Settings	?
Index	Username Role	+

## Click Click

User Settings	
∧ Administrator Settings	
Username	admin
Old Password	ø
New Password	ø
Confirm Password	ø
	Submit Close

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

## Click + to Add a Common User.

<ul> <li>Common User Settings</li> </ul>		
Index	1	
Username		
Role	guest v	
Password		Ø
Confirm Password		ø



Common User Settings		
Item	Description	Default
Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, \$, and *.	Null
Role	Select common user role. Select from User or Guest	Gust
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9, @,., -, #, \$, and *.	Null
Confirm Password	Enter new password again to confirm.	Null

### 3.7.8 Role Management

This section is used to manage user roles and manage permissions for users in different roles.

Role Management		
<ul> <li>Settings</li> </ul>		0
Index	Role	
1	Guest	
2	User	

Role Names @ Role Management		
Item	Description	Default
Guest	Enter a guest name; valid characters are a-z, A-Z, 0-9, @,., -, #, \$, and *.	Guest
User	Enter a user name; valid characters are a-z, A-Z, 0-9, @,., -, #, \$, and *.	User

## Click 🗹 to edit Guest/User permission.

Role Management	
∧ settings	
Index	1
Role	Guest
save and apply,reboot	ReadOnly
∧ Interface	
Serial Port	ReadOnly
Cellular	ReadOnly
LAN	ReadOnly
Link Manager	ReadOnly
USB	ReadOnly
Ethernet	ReadOnly



∧ Network	
Firewall	ReadOnly
IP Passthrough	ReadOnly
Route	ReadOnly
~ VPN	
OpenVPN	ReadOnly
WireGuard	ReadOnly
GRE	ReadOnly
IPsec	ReadOnly

∧ Services	
Web Server	ReadOnly
DDNS	ReadOnly
Email	ReadOnly
Event	ReadOnly
GPS	ReadOnly
NTP	ReadOnly
Smart Roaming V2	ReadOnly
SMS	ReadOnly
SSH	ReadOnly
Syslog	ReadOnly
Advanced	ReadOnly

∧ System	
User Management	ReadOnly
Profile	ReadOnly
Tools	ReadOnly
App Center	ReadOnly
Update	ReadOnly
Debug	ReadOnly



User Permission @ Role Management	
Item	Description
None	Users have no permission to access or modify this setting.
ReadOnly	Users only have permission to read.
Read/Write	Users have permission to access or modify this setting.

#### Note:

- 1. When logging in with Guest/User, "Profile" is not available.
- 2. When the Guest "Save and apply, reboot" permission was set to "ReadOnly". After logging in as Guest, "save and apply", and "reboot" buttons will not be displayed.


# **4. Configuration Examples**

## 4.1 Cellular

# 4.1.1 Cellular Dial-Up

This section shows you how to configure the primary and backup SIM cards for Cellular Dial-up. Connect the device 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 Setting	js			
	Primary Link	WWAN1	v 7	
	Backup Link	None	v	
	Emergency Reboot	OFF	7	

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

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

Link Manager	
∧ General Settings	
Index	1
Туре	WWAN1 V
Description	



7		
∧ WWAN Settings		
Automatic APN Selection	ON OFF	
Dialup Number	*99***1#	)
Authentication Type	Auto	
PPP Preferred	ON OFF	
Switch SIM By Data Allowance	OFF ?	
Data Allowance	200000	0
Billing Day	1	) 🤊
A Ping Detection Settings		?
Enable	ON OFF	
Enable Primary Server	ON OFF 8.8.8.8	]
		)
Primary Server	8.8.8.8	] ] ] 🧿
Primary Server Secondary Server	8.8.8.8	) ) ) ?
Primary Server Secondary Server Interval	8.8.8.8       114.114.114       300	
Primary Server Secondary Server Interval Retry Interval	8.8.8.8 114.114.114 300 5	] 🧿
Primary Server Secondary Server Interval Retry Interval Timeout	8.8.8.8         114.114.114         300         5         3	] 🧿
Primary Server Secondary Server Interval Retry Interval Timeout Timeout unit	8.8.8.8 114.114.114 300 5 3 Second(s) v	] ⑦ ] ⑦

NAT Enable	ON OFF
Auto MTU For WWAN	ON OFF
Upload Bandwidth	10000
Download Bandwidth	10000
Overrided Primary DNS	
Overrided Secondary DNS	
Debug Enable	ON OFF
Verbose Debug Enable	OR OFF



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

Cellu	lar	Status	AT Debug		
^ Advan	ced Cellula	ar Settings			
Index	SIM Card	Phone Number	Network Type	Band Select Type	
1	SIM1		Auto	All	
2	SIM2		Auto	All	

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

Cellular		
∧ General Settings		
Index	1	
SIM Card	SIM1 v	
Phone Number		
PIN Code		0
MCC+MNC Code		0
Extra AT Cmd		0
Telnet Port	0	0
Waiting For Update APN	90	0
Cellular Network Settings		
Network Type	Auto	0
Band Select Type	All	3
Advanced Settings		
Debug Enable	ON OFF	
Verbose Debug Enable	ON OFF	
Timeout For Network Registration	0	0
Preferred Using CID3	ON OFF	



# 4.1.2 SMS Remote Control

R2011 supports remote control via SMS. You can use the following commands to get the status of the device, and set all the parameters of the device.

#### SMS commands 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 to the device'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 device's phone group).

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

#### SMS command Explanation:

- 1. Username and Password: Use the same username and password as the 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 <u>5.1 What Is CLI</u>.

**Note:** Download the configured XML file from the configured web browser. The format of the 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			
ヘ Import Confi	guration File			
	Reset Other Settings	s to Default	ON OFF	
	Ignore Inva	lid Settings	ON OFF	
	XML Config	uration File	Choose File No file chosen	Import
∧ Export Confi	guration File			
	Ignore Disable	ed Features	ON OFF	
Add Detailed Information		ON OFF		
Encrypt Secret Data		ON OFF ?		
XML Configuration File		Generate		
∧ Default Confi	iguration			
Save	Running Configuration	as Default	Save 🖓	
	Restore to Default Co	nfiguration	Restore	



#### XML command:

<lan>

<network max_entry_num="5">

<id>1</id>

<interface>lan0</interface>

<ip>172.16.24.24</ip>

<netmask>255.255.0.0</netmask>

<mtu>1500</mtu>

#### SMS cmd:

set lan network 1 interface lan0

set lan network 1 ip 172.16.24.24

set lan network 1 netmask 255.255.0.0

set lan network 1 mtu 1500

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

#### admin:admin;status system

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

#### SMS received:

hardware_version = 1.0

firmware_version = beta210618

firmware_version_full = "beta210618 (Rev 4250)"

kernel_version = 4.9.152

device_model = R2011

serial_number = ""

uptime = "0 days, 01:25:16"

system_time = "Tue Apr 21 17:09:04 2021"

ram_usage = "77M Free/128M Total"

#### admin:admin;reboot

In this command, the username is "admin", the password is "admin", and the command is to reboot the Device. **SMS received:** 

ОК

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

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

#### SMS received:

OK

ОК

# 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, the username is "admin", the password is "admin", and the command is to configure the LAN parameter.

SMS received:

ОК

ОК

ОК

ОК

## 4.2 VPN Configuration Examples

## 4.2.1 IPsec VPN

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



## **IPsec VPN_Client:**

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

Gener	al	Tunnel	Statu	s x5	09	
∧ Tunnel	Settings					
Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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



### Tunnel

and the second sec	
∧ General Settings	
Index	1
Enable	ON OFF
Description	
Gateway	
Backup Gateway	
Mode	Tunnel
Protocol	ESP
Local Subnet	
Local Protoport	
Remote Subnet	
Remote Protoport	
Link Binding	Unspecified v
∧ IKE Settings	
ІКЕ Туре	IKEv1 V

IKE Type	IKEv1 V
Negotiation Mode	Main
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1
IKE DH Group	DHgroup2
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400 3

∧ SA Settings	
Encryption Algorithm	3DES V
Authentication Algorithm	SHA1 V
PFS Group	DHgroup2 V
SA Lifetime	28800
DPD Interval	30 🦻
DPD Failures	150 🤇
Advanced Settings	
Enable Compression	OFF
Enable Forceencaps	OFF ?
Conntrack Flush	ON OFF
Expert Options	



## **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 from ISAKMP protection suite configuration mode
  exit
                 Set the Diffie-Hellman group
  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
               Long term key operations
  kev
  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 transform using AES cipher
  esp-aes
  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 0.0.0.255 192.168.1.0 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
```



The comparison between server and client is as below.



# 4.2.2 OpenVPN

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





## **OpenVPN_Server:**

Generate the relevant OpenVPN certificate on the server side firstly, and refer to the following commands to configure 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.

OpenV	PN	Status	x509		
∧ Tunne	l Settings				



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

OpenVPN	
∧ General Settings	
Index	1
Enable	ON DEF
Description	client01
Mode	Client v
Protocol	UDP
Peer Address	202.96.1.100
Peer Port	1194
Interface Type	TUN
Authentication Type	X509CA 7
Encrypt Algorithm	BF
Authentication Algorithm	SHA1 Y
Renegotiation Interval	86400
Keepalive Interval	20
Keepalive Timeout	120 🧿
TUN MTU	1500
Max Frame Size	1400
Private Key Password	•••••
Enable Compression	ON OFF
Enable NAT	ON OFF
Enable DNS overrid	OFF ?
Verbose Level	3 7
Advanced Settings	
Enable HMAC	Firewall OFF
Enable F	PKCS#12 OFF
Enable nst	CertType OFF
Expert	t Options



## 4.2.3 GRE VPN

**GRE VPN topology** 



### GRE-1:

The window is displayed below by clicking "VPN > GRE > GRE".

GRE		Status	
∧ Tunne	l Settings		
Index	Enable	Description Remote IP Address	+

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

GRE	
∧ Tunnel Settings	
Index	1
Enable	ON OFF
Description	
Bridge With LAN	ON OFF
Remote IP Address	59.1.1.1
Local Virtual IP Address	20.8.0.2
Local Virtual Netmask	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	ON OFF
Enable NAT	ON OFF
Secrets	•••••
Link Binding	Unspecified v 🕝
	Submit Close

## GRE-2:

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

GRE	
<ul> <li>Tunnel Settings</li> </ul>	
Index	1
Enable	ON OFF
Description	GRE-2
Bridge With LAN	ON OFF
Remote IP Address	59.1.1.1
Local Virtual IP Address	20.8.0.2
Local Virtual Netmask	255.255.255.0
Remote Virtual IP Address	10.8.0.2
Enable Default Route	ON OFF
Enable NAT	ONOFF
Secrets	•••••
Link Binding	Unspecified v 😨
<	Submit Close

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

GRE ▲ Tunnel Settings Tunnel Settings Index 1 Index 1 Enable ON ON Enable GRE-2 real public Description GRE-1 real public network IP address GRE-1 Description GRE-2 network IP address Remote IP Address GRE-1 real tunnrl IP address Remote IP Address 58.1.1.1 59.1.1.1 GRE-2 real tunnrl GRE-2 real tunnrl IP address Local Virtual IP Address 10.8.0.1 Local Virtual IP Address 10.8.0.2 IP address 0 Local Virtual Netmask/Prefix Length 255.255.255.0 Local Virtual Netmask/Prefix Length 255.255.255.0 **Remote Virtual IP Address** 10.8.0.2 Remote Virtual IP Address 10.8.0.1 GRE-1 real tunnrl Enable Default Route Enable Default Route OFF **IP** address OFF Enable NAT OFF Enable NAT OFF USE the same password for -----••••• Secrets Secrets USE the same password for GRE-1 and GRE-2 GRE-1 and GRE-2 Link Binding Unspecified v 7 Link Binding Unspecified

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



# **5. Introductions for CLI**

# 5.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the <u>SSH</u> or through a <u>Telnet</u> network connection. After establishing a Telnet or SSH connection with the device, enter the login account and password (default admin/admin) to enter the configuration mode of the device, as shown below.

### Route login:

Device login: admin

Password: admin

#### #

#### **CLI commands:**

#### #?

!	Comments
add	Add a list entry of configuration
add_preferred	smart roaming add preferred plmn list
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
delete_preferred	smart roaming remove all preferred operators
do	Set the level state of the do
exit	Exit from the CLI
force_rescan	smart roaming network rescan
forget_rplmn	smart roaming forget rplmn
help	Display an overview of the CLI syntax
ipsec_cert_get	Download IPSec certificate file via http or ftp
ovpn_cert_get	Download OpenVPN certificate file via http or ftp
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
saveConfig	Save Running Configuration as Default
select	smart roaming select operator
set	Set system configuration
show	Show system configuration
show_networks	show networks that scanf
speedtest	speedtest



status	Show running system information
tftp_upload_diagnostic	Generate diagnostic files and upload them using TFTP
tftpupdate	Update firmware or configuration file using tftp
traceroute	Print the route packets trace to network host
trigger	Trigger action
uninstall	Uninstall App
UploadConfig	Upload Current UCI Config to FTP Server
urlupdate	Update firmware via http or ftp
ver	Show version of firmware

# 5.2 How to Configure the CLI

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

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



# 5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug parameters	Turn on or turn off debug function
Show	Show parameters	Show the current configuration of each function.
Set	Set parameters	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
Add	Add parameters	parameter

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

# 5.4 Quick Start with Configuration Examples

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

## Example 1: Show the current version

# status system hardware_version = 1.0 firmware_version = beta210618 firmware_version_full = "beta210618 (Rev 4250)" kernel_version = 4.9.152 device_model = R2011 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 R2011-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new
firmware name
Download ing
Download success.
Upgrading
Upgrade success. //Update succeed



# reboot //Take effect after rebooting Rebooting... OK

# Example 3: Set link-manager

#### # set

# 301		
# 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(s	pace+?)	
primary link	Primary Link	
backup link	Backup Link	
backup_mode	BackSup Mode	
revert_interval	Revert Interval	
—		
emergency reboot	Emergency Reboot	
	Emergency Reboot Link Settings	
link	Link Settings	
link # set link_manager pri	Link Settings mary_link (space+?)	
link # set link_manager pri Enum Primary Link	Link Settings mary_link (space+?) (wwan1/wan)	//select "wwan1" as primary link
link # set link_manager pri Enum Primary Link # set link_manager pri	Link Settings mary_link (space+?) (wwan1/wan)	• • • • •
• • • =	Link Settings mary_link (space+?) (wwan1/wan) mary_link wwan1	//select "wwan1" as primary_link //setting succeed
link # set link_manager pri Enum Primary Link # set link_manager pri OK	Link Settings mary_link (space+?) (wwan1/wan) mary_link wwan1	• • •



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_overrided	Overrided Primary DNS	
dns2_overrided	Overrided Secondary DNS	
debug_enable	Debug Enable	
verbose_debug_enable	Verbose Debug Enable	
# set link_manager link 1 ty	/pe wwan1	
ОК		
# set link_manager link 1 w	wan (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 w	wan data_allowance 100	//enable cellular switch_by_data_traffic
ОК		//setting succeed
# set link_manager link 1 wwan billing_day 1		//setting specifies the day of the month for billing
ОК		// setting succeed
<pre># config save_and_apply</pre>		
ОК	<pre>// save and apply t</pre>	he current configuration, make your configuration effect

## Example 4: Set Ethernet

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

# 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
         device = ""
         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
             Multiple IP Address Settings
  multi ip
# set lan network 1(space+?)
  interface
            Interface
             IP Address
  ip
  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 the IP address for lan
                                                  //setting succeed
ОК
# set lan network 1 netmask 255.255.0.0
OK
#
•••
# config save_and_apply
                                         // save and apply the current configuration, make your configuration effect
OK
```



## **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
         Ite band1 = false
         Ite_band2 = false
         lte_band3 = false
         lte_band4 = false
         lte_band5 = false
         Ite band7 = false
         lte_band8 = false
         lte_band13 = false
         lte_band17 = false
         lte_band18 = false
         Ite band19 = false
         lte_band20 = false
         lte_band21 = false
         Ite_band25 = false
         Ite_band28 = false
         lte_band31 = false
         Ite_band38 = false
         Ite_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_manageme	nt web_server			
# set cellular	(space+?)						
sim SIM S	Settings						
# set cellular	sim(space+?)						
Integer Ir	ndex (11)						
	sim 1(space+?						
card		SIM Card					
phone_nu	mber	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					
	-	Band Settings					
telit_band_settings debug_enable		Debug Enable					
		Verbose Debug Enable					
# set cellular sim 1 phone_number 18620435279							
OK							
# config save	_and_apply						
ОК		// save and a	apply the current co	onfiguration, make your configuration effect			



# Glossary

Abbr.	Description
AC	Alternating Current
APN	Access Point Name
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
СНАР	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
LAN	local area network



Abbr.	Description
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
МО	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
РАР	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
РРТР	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
Тх	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
WAN	Wide Area Network

# Guangzhou Robustel Co., Ltd.

Add:	501, Building#2, 63 Yongan Road, Huangpu District,	
	Guangzhou, China 511350	
Email:	info@robustel.com	
Web:	www.robustel.com	