

RobustOS Pro Software Manual



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



#### **About this Document**

This document provides web interface information of the RobustOS Pro based gateway products, including gateway configuration and operation.

**Related Products** 

EG5100, EG5101, LG5100, EG5120, EV8100

Copyright©2023 Guangzhou Robustel Co., Ltd. All rights reserved.

#### **Trademarks and Permissions**

Orobustel & robust OSS are trademarks of Guangzhou Robustel Co., Ltd.. All other trademarks and trade

names mentioned in this document are the property of their respective owners.

#### Disclaimer

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

#### **Technical Support**

Tel: +86-20-82321505 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	Firmware Version	<b>Document Version</b>	Change Description
August 5, 2022	2.0.0	1.0.0	Initial release.
May 22, 2023	2.1.0	2.1.0	Added support for RobustOS Pro V2.1.0
September 14,	2.1.1 or newer	2.1.1	Added support for EG5101, EV8100
2023	version		

# Contents

Chapter 2	1 I	ntroduction	7
Chapter 2	2 I	nitial Configuration	8
2.1	F	PC Configuration	8
2.2	F	Factory Default Settings	11
2.3	F	Factory Reset	11
2.4	L	Log in the Device	12
2.5	(	Control Panel	13
Chapter 3	3 N	WebUI Descriptions	14
3.1	[	Dashboard	14
	3.1.1	Overview	14
	3.1.2	Modem	15
	3.1.3	Ethernet	15
	3.1.4	Internet Status	16
	3.1.5	LAN Status	16
	3.1.6	System Resource	
	3.1.7	System Information	17
	3.1.8	Cellular Status	17
	3.1.9	RCMS Status	
3.2	I	nterface	19
	3.2.1	Ethernet	19
	3.2.2	Cellular	20
	3.2.3	Bridge	26
	3.2.4	Wi-Fi	27
	3.2.5	CAN	36
	3.2.6	5 USB	
	3.2.7	′ VLAN	37
	3.2.8	DI/DO	
	3.2.9	Serial Port	43
	3.2.1	0 Bluetooth (Optional)	
	3.2.1	1 LoRa (Supported in LG5100)	
3.3	1	Network	
	3.3.1	WAN	60
	3.3.2	LAN	64
	3.3.3	Route	67
	3.3.4	Policy Route	68
	3.3.5	Firewall	70
	3.3.6	QoS	76
3.4	F	Packet Forwarders (Supported in LG5100)	
	3.4.1	Basic Station	
	3.4.2	UDP Forwarder	81
3.5	١	/PN	
	3.5.1	IPsec	
	3.5.2	OpenVPN	91
	3.5.3	GRE	100

# 10 robustel

	3.5.4	РРТР	102
	3.5.5	L2TP	106
	3.5.6	DMVPN	109
3.6	Serv	ices	113
	3.6.1	Syslog	113
	3.6.2	Event	115
	3.6.3	NTP	119
	3.6.4	SMS	121
	3.6.5	Email	122
	3.6.6	DDNS	123
	3.6.7	VRRP	125
	3.6.8	SSH	127
	3.6.9	GPS	127
	3.6.10	RCMS	131
	3.6.11	Voice call (Supported in EV8100)	134
	3.6.12	SNMP	139
	3.6.13	Captive Portal	144
	3.6.14	Web Server	146
	3.6.15	Advanced	147
3.7	Syst	em	148
	3.7.1	Debug	148
	3.7.2	Certificate Manager	149
	3.7.3	Resource Graph	153
	3.7.4	App Center	158
	3.7.5	Tools	158
	3.7.6	Flash Manager	161
	3.7.7	Service Management	164
	3.7.8	Profile	164
	3.7.9	User Management	166
	3.7.10	Debian Management	168
	3.7.11	Role Management	170
Chapter 4	4 Con	figuration Examples	172
4.1	Cell	ılar	172
	4.1.1	Cellular APN Manual Setting and Cellular Dial-up.	172
	4.1.2	SMS Remote Control	175
4.2	VPN	Configuration Examples	178
	4.2.1	IPsec VPN	178
	4.2.2	OpenVPN	182
	4.2.3	GRE VPN	185
Chapter !	5 Intro	oductions for CLI	188
5.1	Wha	at Is CLI	188
5.2	How	<i>i</i> to Configure the CLI	189
5.3	Com	imands Reference	189
5.4	Quio	k Start with Configuration Examples	190
Exar	mple 1: S	how current version	190
Exar	mple 2: C	LI for setting Cellular	190

# 10 robustel

Glossary
----------

# Chapter 1 Introduction

This software manual, used for all the RobustOS Pro based gateway products, provides web interface information (configuration and operation).

Please refer to the specific chapter accordingly, as hardware configurations or interfaces may vary from product to product.

Related Product	EG5100	EG5101	LG5100	EG5120	EV8100							
SIM card Slots	2	2	2	2	2							
Ethernet ports	2	1	2	2	2							
Console ports	-	-	-	-	-							
HDMI	-	-	-	-	-							
POE-PD	*	-	*	-	-							
Wi-Fi	*	-	-	*	*							
Bluetooth	*	-	-	*	*							
GNSS	*	-	-	*	-							
DI/DO	4	-	4	4	5							
Relay Output	-	-	-	-	-							
RS232	$\checkmark$			$\checkmark$								
RS485	$\checkmark$			$\checkmark$								
RS422	-	-	-	-	-							
USB	$\checkmark$											
CAN	*	-	-	-								
Docker		-	$\checkmark$	$\checkmark$								
FXS	-	-	-	-								

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

# **About RobustOS Pro**

RobustOS Pro is developed by Robustel based on Debian 11 (bullseye), a common Linux operating system with enhanced cybersecurity, advanced GUI and docker container supported. It will be more convenient for customers to develop and deploy edge computing applications by themselves according to their needs, supporting programming languages such as C, C++, Python, Java, Node.js etc., and the latest common APPs including VPNs, SMS remote control and more can be downloaded in RCMS to fully meet the needs of fragmented IoT applications.

# **Chapter 2** Initial Configuration

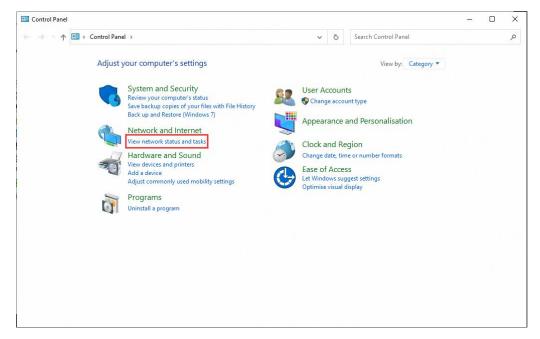
The device can be configured through your web browser that including Microsoft Edge, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows. It provides an easy and user-friendly interface for configuration. There are various ways to connect the device, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to 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 configurate a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

 Right-click "Windows LOGO" on the taskbar, select "Run", and type "Control" to launch the Control panel, then Click "View network status and tasks".





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

Network and Sharing Centre			
→ < ↑ Sontrol Pi	anel  → All Control Panel Items  → Network	and Sharing Centre 🗸 🖑	\$
Control Panel Home	View your basic network infor	mation and set up connections	
Change adapter settings	View your active networks		
Change advanced sharing settings	Network 8 Private network	Access type: Internet Connections: Ethernet 2	
Media streaming options	Physic lictwork		
	Network 13	Access type: No Internet access	
	Public network	Connections: 📮 Test LAN	
	Change your networking settings		
	Set up a new connection or n	etwork or VPN connection, or set up a router or access point.	
		or very connection, or set up a router or access point.	
	Troubleshoot problems Diagnose and repair network	problems or get troubleshooting information.	
See also			
Internet Options			

3. Click **Properties** in the window of **Network Connection status**.

General		
Connection -		
IPv4 Connec	ctivity:	Internet
IPv6 Connec	ctivity:	No Internet access
Media State	1	Enabled
Duration:		13 days 05:40:54
Speed:		1.0 Gbps
D <u>e</u> tails		
Activity		
	Sent —	— Received
		Received

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

Vetworking	Sharing			
Connect usi	ng:			
Intel(I	R) I211 Giga	bit Network Conne	ection	
			Conf	figure
This connec	tion uses the	e following items:		
🗹 💭 Clie	ent for Micros	soft Networks		^
🔽 🧶 File	and Printer	Sharing for Micros	oft Networks	
		Driver (NPCAP)		
Colores .				
	S Packet Sc	cheduler		
	S Packet So emet Protoci		(IPv4)	
Int.	emet Protoci	ol Version 4 (TCP/	COLORIDA COLORIDA	
	emet Protoci crosoft Netw	o <mark>l Version 4 (TCP/</mark> ork Adapter Multip	COLORIDA COLORIDA	~
	emet Protoci crosoft Netw	ol Version 4 (TCP/	COLORIDA COLORIDA	~
	emet Protoci crosoft Netw	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver	COLORIDA COLORIDA	~
	ernet Protoco crosoft Netwo crosoft LLDP	o <mark>l Version 4 (TCP/</mark> ork Adapter Multip	lexor Protocol	> erties
✓ Instal	emet Protoci crosoft Netwi crosoft LLDP	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver	lexor Protocol	
Instal	ernet Protoco crosoft Netwo crosoft LLDP II	ol Version 4 (TCP/ ork Adapter Multip P Protocol Driver <u>U</u> ninstall	lexor Protocol	erties
Instal	emet Protoci crosoft Netwicrosoft LLDP II n sion Control I	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver	Protocol	erties lefault
Instal I	emet Protoce crosoft Netw crosoft LLDP II n sion Control I a network pro	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver Uninstall Protocol/Internet F	Protocol Prop Protocol. The d	erties lefault
Instal I	emet Protoce crosoft Netw crosoft LLDP II n sion Control I a network pro	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver Uninstall Protocol/Internet F otocol that provide	Protocol Prop Protocol. The d	erties lefault
Instal I	emet Protoce crosoft Netw crosoft LLDP II n sion Control I a network pro	ol Version 4 (TCP/ ork Adapter Multip Protocol Driver Uninstall Protocol/Internet F otocol that provide	Protocol Prop Protocol. The d	erties lefault

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

nternet f	Protocol Version 4 (TCP/IPv4)	Propertie	25		×
General	Alternative Configuration				
this cap	n get IP settings assigned autor bability. Otherwise, you need to appropriate IP settings.				
<u>o</u>	btain an IP address automatical	ly			
	e the following IP address:				
<u>I</u> P ad	ddress:		¥.,		
Subr	net mask:		- 45	121	
Defa	ult gateway:				
	btain DNS server address autor	natically			
OUs	se the following DNS server add	resses:			
Prefe	erred DNS server:				
<u>A</u> lter	native DNS server:		10		
V	alidate settings upon exit			Advance	ed
			OK		Cancel



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

nternet Protocol Version 4 (TCP/IP	v4) Properties	×
General		
You can get IP settings assigned au this capability. Otherwise, you need for the appropriate IP settings.		
O Obtain an IP address automat	ically	
• Use the following IP address:		
IP address:	192.168.0.2	
Subnet mask:	255.255.255.0	
Default gateway:	192.168.0.1	
Obtain DNS server address au	Itomatically	
• Use the following DNS server a	addresses:	
Preferred DNS server:	8.8.8.8	
Alternative DNS server:		
Validate settings upon exit	Ad <u>v</u> anced.	•

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	See the information from the product label
ETH0	WAN mode or
	192.168.0.1/255.255.255.0, LAN mode
ETHn	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled

## 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 the 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, open a web browser such as Microsoft Edge, Google Chrome or Firefox, etc.
- 2. 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 <a href="http://192.168.0.1/">http://192.168.0.1/</a>, though the actual address may vary.

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

	🙆 Rot	uter Web Manager	×	+
$\leftarrow$	С	A Not secure	192.168.	0.1/auth/login.html

In the login page, enter the username and password, you can check the login information from the device's stick, and then click LOGIN. See the information on the product label for default username and password.
 Note: If enter the wrong password over 6 times, the user account will be locked for 5 minutes.



### 2.5 Control Panel

After logging in, the home page of the web interface is displayed, here take EG5120 for example.

Dashboard	System Uptime Internet Uptime 4h	CPU Temperature 48.0°C
E Interface	Modem	Ethernet
5 Network		
<sup>D</sup> VPN	SIM2 SIM1	ЕТНО ЕТН1
Services	Internet Status	Lan Status
> System	Active Link         wlan0           IP Address         172.16.24.41           Gateway         172.16.24.2           DNS         172.16.24.2 114.114.114.114	IP Address         192.168.0.1           MAC Address         34:FA:40:22:E4:D1
	System Resource	System Information
	3%         35%         5%           CPU Quad Core         RAM 668M/1920M         5%	Operating System         Debian GNU/Linux 11.2           System Time         Mon May 22 16:11:39 2023           Firmware Version         2.1.1.1 (562fa7af)           Hardware Version         1.1           Kernel Version         5.4.70-g31b8d9973           Serial Number         09070423020009
	Cellular Status	RCMS Status
	Modem Vendor     quectel       Modem Model     EG25       Network Registration     -       IMEI     865326068175382	RobustLink Status RobustelLink Last Connected RobustVPN Status RobustVPN Last Connected RobustVPN Virtual IP

From the homepage, users can find the model information and 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

① 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 <u>3.8.9 System > User</u> <u>Management</u>.

Control Panel			
Item	Description	lcon	
Save & Apply	The icon is in gray by default, and will turn red if any modifications on	(	
	configuration, then click to save the current configuration into device's flash	$\langle \rangle \langle \rangle$	
	and apply the modification on every configuration page, to make the	or	



	modification taking effect.	
Restart	Click to restart all the RobustOS Pro operating system based applications(applications controlled by ystem are not included), then switch to the login page.	Ç
Reboot	Click to reboot the device, then switch to the login page.	ලා
Logout	Click to log the current user out safely. After logging out, it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	Ð

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

- 1. Modify in one page;
- 2. Click Submit under this page;
- 3. Modify in another page;
- 4. Click Submit under this page;
- 5. Complete all modification;
- 6. Click  $\bigcirc$  for save and apply.

# **Chapter 3** WebUI Descriptions

## 3.1 Dashboard

### 3.1.1 Overview

System Uptime 4h	Internet Uptime 4h	CPU Temperature 48.0°C	Internet Traffic OMB	(Normal)	
System Uptime 4h	Internet Uptime 4h	Power Source External	Charging 4.048V	(EV8100)	
Item	Description				
System Uptime	Show the current amou	Show the current amount of time the router has been powered on.			
Internet Uptime	Show the current amou	Show the current amount of time the router has been connected to internet.			
CPU Temperature	Show the CPU tempera	Show the CPU temperature.			



Traffic	Show the amount of WWAN data traffic usage.
Power Source (EV8100	Show the current power source.
Only)	
Battery status (EV8100	Show the current battery status.
Only)	

### 3.1.2 Modem

#### This page shows the status of SIM card.

### Modem

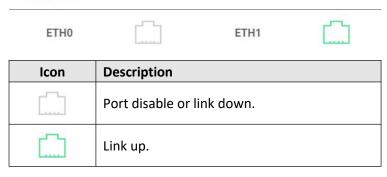


Item	Description
	Not connected.
	Weak signal.
.1	Medium signal.
.1	Strong signal.

## 3.1.3 Ethernet

This page shows the device's Ethernet status

#### Ethernet





### 3.1.4 Internet Status

This page shows the device's Internet status information.

#### Internet Status

Active Link	eth0
IP Address	172.16.19.22
Gateway	172.16.19.1
DNS	172.16.2.1 114.114.114.114

Item	Description
Active Link	Show the currently online link.
IP Address	Show the address of current link.
Gateway	Show the gateway address of the current link.
DNS	Show the current DNS server.

### 3.1.5 LAN Status

This page shows the device's LAN status

#### LAN Status

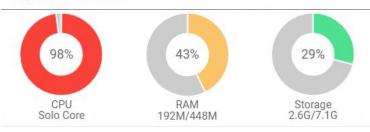
IP Address	192.168.0.1	
MAC Address	34:FA:40:0F:49:20	

Item	Description
IP Address	Show the IP address of the LAN.
MAC Address	Show the MAC address of the LAN.

### 3.1.6 System Resource

This page shows the device's system resources usage information. When the usage is more than 65%, the icon will be in Red. When the usage is between 30% and 65%, the icon will be in Yellow. When the usage is less than 30%, the icon will be in Green.







# 3.1.7 System Information

This page shows the device's system information.

#### System Information

Operation System	Debian GNU/Linux 11.2	
System Time	Tue May 9 17:57:53 2023	
Firmware Version	2.1.0 (8dc4bb15)	
Hardware Version	1.1	
Kernel Version	5.4.70-gd00acdc	
Serial Number	09070423020009	

Item	Description
Operating System	Show the operating system information.
System Time	Show the current system time.
Firmware Version	Show the firmware version running on the device.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of your device.

## 3.1.8 Cellular Status

This page shows the device's cellular status.

Modem Model	EG800Q-EU	
Network Registration	84	
RSRP(dBm)		
RSRQ(dB)		
SINR(dB)		
ENDC state	Inactive	

Item	Description
Modem Vendor	Show the radio module vendor information.
Network Registration	Show the current network registration information.
RSRP(dBm)	Show the current RSRP when you register to the 4G network.
RSRQ(dB)	Show the current RSRQ when you register to the 4G network.
SINR(dB)	Show the current SINR when you register to the 4G/5G network.
ENDC state	Show the ENDC state of 5G network.



### 3.1.9 RCMS Status

This page shows the device's cellular status.

RobustLink Status	Connected
RobustelLink Last Connected	2023-05-22 16:20:33
RobustVPN Status	Disconnected
RobustVPN Last Connected	Never
RobustVPN Virtual IP	
RobustVPN SubNet Address	

Item	Description
RobustLink Status	Show the status of RobustLink
RobustelLink Last Connected	Show the last connected times of RobustLink
RobustVPN Status	Show the status of RobustVPN
RobustVPN Last Connected	Show the last connected times of RobustVPN
RobustVPN Virtual IP	Show the virtual IP of RobustVPN
RobustVPN SubNet Address	Show the subnet address of RobustVPN



### 3.2 Interface

### 3.2.1 Ethernet

This section allows you to set the related parameters for Ethernet. There may be multiple Ethernet ports in the device. All Ethernet port in the device can be configured as either a WAN port or LAN port. The default settings of all Ethernet ports are lan0 and their default IP are 192.168.0.1/255.255.255.0. PoE could be supported in some devices.

#### Ports

	Status				
gs					
Port	MTU	MAC			
eth0	1500				Z
eth1	1500				
	Port eth0	gs Port MTU eth0 1500	gs Port MTU MAC eth0 1500	gs Port MTU MAC eth0 1500	gs Port MTU MAC eth0 1500

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

∧ Port Settings		
Name	port1	0
Port	eth0 v	
Port Speed	Auto v	
MTU	1500	0
MAC		0

Item	Description	Default
Name	Name of the port.	
Port	Show the editing port, read only.	
Port Speed	Select from "Auto", "10M-half", "10M-full", "100M-half", "100M-full", "1000M-half",	Auto
	"1000M-full".	
MTU	Enter the value of the maximum transmission unit(MTU).	1500
MAC	Specify the MAC address of the port.	
POE Enable	Click the toggle button to enable or disable the POE function. When POE function	
(Optional)	enabled, it will connect the POE voltage.	ON

**Status** 

Ports

∧ Port Status

Index

1

2

This section allows you to set the related parameters of Cellular. The device supports one cellular modem and two SIM slots, but only one SIM slot is activated at any time.

SIM1

ON

AT Debug

Primary Sim

Enable Auto Switching

Enable Auto Revert

### Cellular

Cellular

∧ General Settings

Item	Description	Default
Primary Sim	Select one Sim card as primary Sim card	SIM1
Enable Auto Switching	When auto switching is enabled, the SIM card will be automatically switched	ON
	to another one when there is SIM card error or connection error or ping fails	
	by default.	
Enable Auto Revert	When auto switching is enabled, the backup SIM card will be automatically	OFF
	switched to primary sim card when backup SIM card online time is greater	
	than revert interval time.	

OFF

?

?

?

V

Port

eth0

eth1

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

Status

Link

Up

Up

Status





Weak Signal	ON OFF ?	
While Roaming	ON OFF	

Item	Description	Default
Weak Signal	Switch to another SIM card when the signal is poor, only used for dual SIM	ON
	backup.	
While Roaming	Switch to another SIM card while roaming, only used for dual SIM backup.	OFF

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

Click 🗹 to configure its parameters in the pop-up window.

∧ General Settings				
Index	1			
SIM Card	SIM1 V			
Automatic APN Selection	ON OFF			
Enable APN for voice	ON OFF			
Phone Number				
PIN Code	0			
Extra AT Cmd	(			
Telnet Port	0			

# 10 robustel

мти	1500
Traffic Statistics	ON OFF
Billing Day	1
Enable IPv6	ON OFF

Item	Description	
Index	Indicate the ordinal of the list.	
SIM Card	Show the currently editing SIM card.	
Automatic APN Selection	Click the toggle button to enable/disable the "Automatic APN Selection"	ON
	option. After enabling, the device will recognize the access point name	
	automatically. Alternatively, users can disable this option and manually	
	add the access point name.	
Enable APN for voice	Click the toggle button to enable/disable the option.	OFF
	(Only EV8100 support)	
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	
Extra AT Cmd	Enter the AT commands used for cellular initialization.	
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet. 0	0
	means not supported.	
MTU	1280 - 1500	1500
Traffic Statistics	Traffic Statistics Click the toggle button to enable/disable the option.	
Billing Day	This option specifies the day of month for billing, the data traffic statistics will be	1
	recalculated from this day.	
Enable IPv6	Click the toggle button to enable/disable the option.	OFF

#### When the Automatic APN Selection is off, users can specify their own APN setting.

Automatic APN Selection	ON OFF
APN	internet
Username	
Password	
Authentication Type	None v

Item	Description	Default
Automatic APN Selection	Click the toggle button to enable/disable this option. Enable for AutoAPN	
	feature.	
APN	Enter the Access Point Name for cellular dial-up connection, provided by	internet
	local ISP.	
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null



Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Authentication Type	Select the authentication type. Select from "None", "CHAP", "PAP".	None
	None: None.	
	CHAP: Challenge-Handshake Authentication Protocol.	
	PAP: Password Authentication Protocol.	

#### When the APN for voice is on, users can configure their own voice APN in need.

Enable APN for voice APN for voice	Ins
▲ Cellular Network Settings	
Network Type	Auto v 🤅
Band Select Type	All v 🝞

This page allows you to configure cellular network settings. type and network band. You can specify a specific frequency band or network type for device.

**Note:** EG5120 does not support this feature.

Item	Description	Default
Network Type	Select the cellular network type, which is the network access order. Select	
	from "Auto", "2G Only", "3G Only", "4G Only", "5G Only".	
	Auto: Connect to the best signal network automatically	
	2G Only: Only the 2G network is connected	
	3G Only: Only the 3G network is connected	
	4G Only: Only the 4G network is connected	
	5G Only: Only the 5G network is connected	
	Note:	
	1) There may be some different optional network types due to the	
	different cellular module.	
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing	All
	"Specify".	
	Note:	
	There may be some differences in Band Setting due to the different cellular	
	module.	



∧ Advanced Settings				
Debug Enable	ON OFF			
Verbose Debug Enable	ON OFF			
Timeout For Network Registration	0	0		
Wireless Testing Mode	ON OFF			

Item	Description		
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging		
	information output.		
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose		
	debugging information output.		
Timeout For Network	The timeout required for the module to register to the network. Unit:	0	
Registration	seconds. 0 means the default setting is used.		
Wireless Testing Mode	Can only be turned on during laboratory testing when connected to	OFF	
	wireless tester! Must be turned off when connected to real network!		

### Status

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

Cellular	Status	s AT De	ebug		
Status					
Index	Modem Status	Modem Model	IMSI	Registration	
1	Ready	EG25	460015726101417	Registered to home network	

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

#### **RobustOS Pro Software Manual**

Cellular

Status

AT Debug

tatus					
Index	Modem Status	Modem Model	IMSI	Registration	
1	Ready	EG25	46001 0493	Registered to home network	
		Index	1		
		Modem Status	Ready		
		Modem Vendor	quectel		
		Modem Model	EG25		
		Current SIM	SIM1		
		Phone Number	+8613268		
		IMSI	46001 0493		
		ICCID	89860121 379743	3	
		Registration	Registered to home netw	ork	
		Network Provider	CHN-UNICOM		
		Network Type	LTE		
		Band	3		
		Signal Strength	24 (-65dBm)		
		RSRP	-101 dBm		
		RSRQ	-17 dB		
		SINR	-5 dB		
		Bit Error Rate	99		
		PLMN ID	46001		
		Local Area Code			
		Cell ID	6B20D02		
	1	Fracking Area Code	251B		
		Physical Cell ID	73		
		IMEI	8653260 382		
		Firmware Version	EG25GGBR07A08M2G_3	0 006 30 006	

Item	Description	
Index	Indicate the ordinal of the list.	
Modem Status	Show the status of the radio module.	
Modem Vendor	Show the vendor of the radio module.	
Modem Model	Show the model of the radio module.	
Current SIM	Show the SIM card that your router is using.	
Phone Number	Show the phone number of the current SIM.	
IMSI	Show the IMSI number of the current SIM.	
ICCID	Show the ICCID number of the current SIM.	
Registration	Show the current network status.	
Network Provider	Show the name of Network Provider.	



Item	Description
Network Type	Show the current network service type, e.g. WCDMA.
Band	Show the band information.
Signal Strength	Show the signal strength detected by the mobile.
RSRP	Show the current RSRP when you register to the 4G network.
RSRQ	Show the current RSRQ when you register to the 4G network.
SINR	Show the current SINR when you register to the 5G network.
Bit Error Rate	Show the current bit error rate.
PLMN ID	Show the current PLMN ID.
Local Area Code	Show the current local area code used for identifying different area.
Cell ID	Show the current cell ID used for locating the router.
Physical Cell ID	Show the current physical cell ID used for locating the router.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio
	module.
Firmware Version	Show the current firmware version of the radio module.

### AT Debug

This page allows you to send an AT command for device debugging.

Cellular	Status	AT Debug	<u>n. 4.</u>	
			 	_
∧ AT Debug				
Command				
Result				
				Send

# 3.2.3 Bridge

Bridge is used to create a single network consisting of multiple devices. The default bridge(br\_lan) interface is always available.

Settings		
Interfaces		
Interface	Description	+
br_lan	default bridge	Б×

10 robustel

Click + to add a new Bridge. The maximum count is **10**.

Click  $\times$  to delete the Bridge.

Click 🔽 to configure the Bridge's parameters in the pop-up window.

∧ Interfaces				
Interface	br_lan		?	
Description	default bridge			
Sub Interface	🗸 eth0	🗸 eth1		

Note: You should uncheck the eth0 of sub interface when set eth0 as WAN.

Item	Description	
Interface	The interface of Bridge.	
Description	The description of the Bridge.	
Sub Interface	Select and enable the related Ethernet port.	

### 3.2.4 Wi-Fi

This section allows you to configure the parameters of Wi-Fi AP mode. Router supports Wi-Fi AP or Client modes.

#### Mode

Mode	Radio	Status	
▲ General Settings			
		Mode	AP v ?

Item	Description			
Mode	Select the device's wireless mode, "AP" or "Client".			
	AP: Devices act as the center of the network and they provide wireless connectivity			
	to other devices.			
	Client: Client devices act as clients and they connect to an already existing Wi-Fi			
	network rather than creating their own network.			
	Note: The change of this option would cause wan link to restore default			
	configuration. You need to restart the whole device for changes to take effect.			



#### Radio

### **Radio Settings**

Wi-Fi can work on either 2.4 GHz or 5 GHz, but cannot support both concurrently.

2.4 GHz: 11bgn Mixed & 11b Only & 11g Only & 11n Only

5 GHz: 11an & 11a/an/ac

∧ Radio Settings	
Enable	ON OFF
Wireless Mode	11bgn Mixed v
Channel	Auto v 🕜

Item	Description	Default
Enable	Click the toggle button to enable/disable the Wi-Fi access point	OFF
	option.	
Wireless Mode	Select from "11bgn Mixed", "11b Only", "11g Only", "11n Only",	11bgn Mixed
	"11an" or "11a/ac/an".	
	• 11bgn Mixed: Mix IEEE 802.11b/g/n three agreements, for	
	backward compatibility.	
	• 11b only: IEEE 802.11b.	
	• 11g only: IEEE 802.11g.	
	• 11n only: IEEE 802.11n.	
	• 11a/an/ac: IEEE 802.11a/an/ac.	
	• 11an: IEEE 802.11an only.	
Channel	Select the frequency channel, including "Auto", "1", "2" "13",	Auto
	or "36", "40", "44", "48", "149", "153", "157", "161", "165".	
	• Auto: Router will scan all frequency channels until the best	
	one is found.	
	Others: Router will be fixed to work with this channel	
	1-2412 MHz.	
	2-2417 MHz.	
	3-2422 MHz.	
	4-2427 MHz.	
	5-2432 MHz.	
	6-2437 MHz.	
	7-2442 MHz.	
	8-2447 MHz.	
	9-2452 MHz.	
	10-2457 MHz.	
	11-2462 MHz.	
	12-2467 MHz.	
	13-2472 MHz.	



Item	Description	Default
	36-5180 MHz.	
	40-5200 MHz.	
	44-5220 MHz.	
	48-5240 MHz.	
	149-5745 MHz.	
	153-5765 MHz.	
	157-5785 MHz.	
	161-5805 MHz.	
	165-5825 MHz.	

## **Radio Advanced Settings**

∧ Radio Advanced Settings					
Beacon Interval	100	0			
DTIM Period	2	0			
RTS Threshold	2347	0			
Fragmentation Threshold	2346	0			
Enable WMM	ON OFF				
Enable Short GI					
Channel Width	20MHz	<ul> <li>✓ ⑦</li> </ul>			

Item	Description	Default
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon	100
	which is used for wireless network authentication.	
DTIM Period	Set the delivery traffic indication message period and the router AP will	2
	multicast the data according to this period.	
RTS Threshold	Set the "request to send" threshold. When the threshold set as 2347,	2347
	the router AP will not send detection signal before sending data. And	
	when the threshold set as 0, the router AP will send detection signal	
	before sending data.	
Fragmentation	Set the fragmentation threshold of a Wi-Fi AP. It is recommended that	2346
Threshold	you use the default value 2346.	
Enable WMM	Click the toggle button to enable/disable the Wi-Fi MultiMedia 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.	



Item	Description	Default
Channel Width	Select from "20MHz" or "40MHz".	Auto
(available on 11bgn	Note: 40 MHz channel width provides higher available data rate, twice	
Mixed/11b/11g/11n/	as many as 20 MHz channel width.	
11ac)		

### **Radio VAP Settings**

A Radio VAP Setting	s			
Enable	Broadcast SSID	SSID	Security Mode	+
	n access point. The maximum ure an access point, the secur		"Disabled".	
∧ General Settings				
	Enable	ON OFF		
	Interface	br_lan	v	
	Broadcast SSID	ON OFF		
	SSID	router		
	Security Mode	Disabled	V	

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



∧ General Settings	
Enable	ON OFF
Interface	br_lan v
Broadcast SSID	ON OFF
SSID	router
Security Mode	WPA-Personal v
WPA Version	Auto
Encryption	Auto
PSK Password	(
Group Key Update Interval	3600



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

▲ General Settings	
Enable	ON OFF
Interface	br_lan v
Broadcast SSID	ON OFF
SSID	router
Security Mode	WPA-Enterprise v
WPA Version	Auto v
Encryption	Auto
Radius Authentication Server Address	
Radius Authentication Server Port	1812
Radius Server Share Secret	
Group Key Update Interval	3600

Item	Description	Default
Name	Enter the name of the Wi-Fi access point.	
Enable	Click the toggle button to enable/disable the Wi-Fi access point	ON
	option.	
Interface	Select one interface.	br_lan
SSID	Enter the Service Set Identifier, the name of your wireless	
	network. The SSID of a client and the SSID of the AP must be	
	identical for the client and AP to be able to communicate with	
	each other. Enter 1 to 32 characters.	
Broadcast SSID	Click the toggle button to enable/disable the SSID being	ON
	broadcast. When enabled, the client can scan your SSID. When	
	disabled, the client cannot scan your SSID. If you want to connect	
	to the router AP, you need to manually enter the SSID of router	
	AP at Wi-Fi client side.	
Security Mode	Select from "Disabled", "WPA-Personal", "WPA-Enterprise".	Disabled
	Disabled: User can access the Wi-Fi without password	
	Note: It is strongly recommended for security purposes that	
	you do not choose this kind of mode.	
	WPA-Personal: Wi-Fi Protected Access only provides one	
	password used for Identity Authentication	
	WPA-Enterprise: Provides an authentication interface for	
	EAP which can be authenticated via Radius Authentication	



Item	Description	Default
	Server or other Extended Authentication	
WPA Version	Select from "Auto", "WPA" or "WPA2".	Auto
	• Auto: Router will choose automatically the most suitable	
	WPA version	
	WPA2 is a stronger security feature than WPA	
Encryption	Select from "Auto" or "AES".	Auto
	Auto: Router will choose automatically the most suitable	
	encryption	
	• 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	
PSK Password	Enter the Pre share key password. When router works as AP	Null
	mode, enter Master key to generate keys for encryption. A PSK	
	Password is used as a basis for encryption methods (or cipher	
	types) in a WLAN connection. The PSK Password should be	
	complicated and as long as possible. For security reasons, this	
	PSK Password should only be disclosed to users who need it, and	
	it should be changed regularly. Enter 8 to 63 characters.	
Group Key Update Interval	Enter the interval of group key update.	3600
Radius Authentication Server	Enter the address of radius authentication server.	Null
Address@WPA-Enterprise		
Radius Authentication Server	Enter the port of radius authentication server.	1812
Port@WPA-Enterprise		
Radius Server Share	Enter the shared secret of radius authentication server.	Null
Secret@WPA-Enterprise		

Advanced Setti	100	ł.
<ul> <li>Auvanceu Jetu</li> </ul>	<u> </u>	2

64
ON OFF (?)
none v

Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router's AP.	64
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option.	OFF
	When enabled, the router will isolate all connected wireless devices.	
Debug Level	Select from "verbose", "debug", "info", "notice", "warning" or	none
	"none".	



## **Radio ACL Settings**

▲ Radio ACL Settings	
Enable ACL	ON OFF
ACL Mode	Accept v 🕐

Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	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	
	Note: Router can only allow or deny devices which are included in	
	"Access Control List" at one time.	

#### **Radio Access Control List**

A Radio Acc	ess Control List		
Index	Description	MAC Address	+

Click + to add an access control point. The maximum count is **64**.

▲ Access Control List		
Index	1	)
Description		]
MAC Address		]

Item	Description	Default
Index	Indicate the ordinal of the list.	
Description	Enter a description for this access control list.	Null
MAC Address	MAC address of WiFi device	Null



### Status

#### This section allows you to view the status of AP.

Region	Radio	Status	•			
AP1 Status	;					
Index	Status	SSID	Channel	Channel Width	MAC Address	
1	COMPLETED	router	1	20	2c:3b:70:e9:7b:8f	
AP1 Assoc	iated Stations					
Index	MAC Address	Signal				
AP2 Status						
Index	Status	SSID	Channel	Channel Width	MAC Address	
1	COMPLETED	router_2	1	20	2c:3b:70:e9:7c:8f	
AP2 Assoc	iated Stations					
Index	MAC Address	Signal				
ΓA Status						
		SSID				
		IP Address				
		BSSID				
		WPA state				
		Key Mgmt				

#### Wi-Fi Client

Note: User can configure the device as Wi-Fi client by following steps. Before setting Wi-Fi Client, you need to <u>switch the Wi-Fi mode to Client</u> first.

Click <u>"Network> WAN>Link> Setting"</u>, click + to add a new WAN link, then configure the related parameters.



∧ Link Settings			
	Name	WWAN	0
	Туре	WIFI v	]
	Interface	wlan0 v	
	SSID	305	
	Password	•••••••	
	Description	default wan	
	Weight	0	?
	Firewall Zone	external v	

### 3.2.5 CAN

This section allows you to configure the parameters of CAN.

▲ General Settings			Set Dadu Tate	IUUK	
			Set Dadu Tate	IUUK	
▲ General Settings	∧ General Settings		set baud rate	100K v	
		A Ceneral Settings			

### 3.2.6 USB

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

USB	Key		
▲ General Settings			
	Enable USB	ON OFF	
	Enable Automatic Upgrade	ON OFF	

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 router when inserting a USB storage device with a	
	router firmware.	

∧ Key			
	USB Automatic Upgrade Key	Generate	
	USB Automatic Upgrade Key	Download	

Item	Description	Default
USB Automatic Upgrade Key	Click Generate to generate and click <b>Download</b> to download the key.	

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

# 3.2.7 VLAN

VLAN stands for Virtual LAN, allows splitting a single physical LAN into separate Virtual LANs, to reduce broadcast traffic on the LAN.

Setting	5			
-	16			
∧ Interfaces	;			
Name	Description	VLAN Tag		+

Click + to add a new Interface. The maximum count is **10**.

∧ Interfaces	
Name	
Description	
VLAN Tag	1
Parent Type	Ethernet v
Parent Interface	eth0 v



Item	Description	Default
Name	The name of VLAN.	Null
Description	Enter a description for this VLAN.	Null
VLAN Tag	Enter a tag for this VLAN.	1
Parent Type	Select from "Ethernet" or "Bridge".	Ethernet
Parent Interface	Select the related parent interface.	eth0

# 3.2.8 DI/DO

This section allows you to set the DI/DO parameters. The DI interface can be used for triggering alarm, while the DO can be used for controlling the slave device so as to do real-time monitoring. In some devices, users can configure the IO as DI or DO.

#### DIDO

DIDO	Statu	S			
_					
DIDO Settin	ngs				
Index	PHY Mode	Enable			
1	DI	false			C
2	DI	false			Ľ
3	DO	false			Ľ
4	DO	false			Z

Click to configure the parameters in the pop-up window.



#### DI

∧ General Settings	
Index	1
PHY Mode	DI
Enable	ON OFF
Mode	Counter v
Inversion	ON OFF
Threshold Value	0
Alarm On Content	Alarm On
Alarm Off Content	Alarm Off



Item	Description	Default
Index	Indicate the ordinal of the list.	
PHY Mode	DI, fixed, read only.	
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select from "ON-OFF" or "Counter".	Counter
	• ON-OFF: Alarm mode can be triggered at the DI access ON-OFF.	EV8100:
	Counter: Event counter mode	ON-OFF
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.	
Threshold Value	The threshold value is a unique parameter when the mode is <b>Count</b> . Set the	0
	threshold value to trigger the DI alarm when the count value reaches the	
	threshold value.	
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off

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

### DO

▲ General Settings	
Index	3
PHY Mode	DO v
Enable	ON OFF
Alarm On Action	Pulse v
Alarm Off Action	High Low Pulse
Initial State	Last v
Delay	0
Hold Time	0
Low-level Width	1000
High-level Width	1000
Triggered by DI	ON OFF
Alarm Source	NONE v

Item	Description	Default
Index	Indicate the ordinal of the list.	
PHY Mode	DO, fixed, read only.	



Item	Description	Default
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	<ul> <li>Digital Output initiates when there is an alarm. Selected from "High", "Low" or "Pulse".</li> <li>High: a high electrical level output</li> </ul>	High
	<ul> <li>Low: a low electrical level output</li> </ul>	
	<ul> <li>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered</li> </ul>	
Alarm Off	Digital Output initiates when alarm removed. Selected from "High", "Low" or "Pulse".	Low
Action	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	
Initial State	Specify the Digital Output status when powered on. Selected from "Last", "High" or "Low".	Last
	Last: DO's status will consist with the status of last power off	
	High: DO interface is in high electrical level	
	Low: DO interface is in low electrical level	
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a	0
(unit: 100ms)	"Delay". Enter from 0 to 3000 (0=generate pulse without delay).	
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action	0
(unit: s)	time reach 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 the low-level width. It is available when enabling Pulse as "Alarm On Action/Alarm	1000
(unit: ms)	Off Action". In Pulse Output mode, the selected digital output channel will generate a	
	square wave as specified in the pulse mode parameters. The low level widths are	
	specified here. Enter from 1000 to 3000.	
High-level	Set the high-level width. It is available when enabling Pulse as "Alarm On	1000
Width	Action/Alarm Off Action". In Pulse Output mode, the selected digital output channel	
(unit: ms)	will generate a 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



# **Relay Output**

∧ General Settings	
Index	3
PHY Mode	Relay v
Enable	ON OFF
Alarm On Action	Relay On v
Alarm Off Action	Relay Off v
Initial State	Relay On v
Delay	0
Hold Time	0
Triggered by DI	ON OFF
Alarm Source	NONE v

Item	Description	Default		
Index	Indicate the ordinal of the list.			
PHY Mode	Relay only on Relay Output device			
Enable	Click the toggle button to enable/disable this Relay Output.			
Alarm On Action	Relay Output initiates when there is an alarm.			
	Relay On: The relay will connect	On		
	Relay Off :The relay will disconnect			
Alarm Off	Relay Output initiates when alarm removed.	Relay		
Action	Relay On: The relay will connect	Off		
	Relay Off :The relay will disconnect			
Initial State	Specify the Relay Output status when powered on.	Relay		
	Relay On: The relay will connect	On		
	Relay Off :The relay will disconnect			
Delay	Set the delay time for DO alarm start-up. The first pulse will be generated after a	0		
(unit: 100ms)	"Delay". Enter from 0 to 3000 (0=generate pulse without delay).			
Hold Time	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action	0		
(unit: s)	time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds.			
	(0=keep on until the next action)			
Triggered by DI	Click the toggle button to enable/disable the relay output triggered by digital input.	ON		
Alarm Source	Digital output activation can be activated by this alarm.	None		



#### Status

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

A DI Status								
Index	Name	Level	Status	Count				
1	DI1	High	Alarm off					
2	DI2	High	Alarm off					
▲ Action Of	Clear							
		Co	ounter Alarm Of	DI 1	Clear			
		Co	ounter Alarm Of	DI 2	Clear			
▲ DO Status								
Index	Name	Level	Low-level W	idth Hi	gh-level Width			
1	D03	Low						
2	DO4	Low						
A DO Contro	bl							
			Level Of I	003	Toggle			
			Level Of [	004	Toggle			

# 3.2.9 Serial Port

This section allows you to set the serial port parameters. The device might support two serial ports, which might be configured as RS232or RS485 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 wired or wireless network, so as to realize the function of transparent data transmission.



# **Serial Port**

Index	Port	Enable	Туре	Baud Rate	Application Mode	
1	COM1	false	RS232	115200	Transparent	Ē
2	COM2	false	RS232	115200	Transparent	Г.

# Click to configure the parameters in the pop-up window.

∧ Serial Port Application Settings		
Index	1	
Port	COM1 v	
Enable	ON OFF	
Туре	RS232 v	
Baud Rate	[115200 v]	
Data Bits	8 v	
Stop Bits	[1v]	
Parity	None v	
Flow Control	None v	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Port	Show the current serial's name, read only. COM1	
Туре	Select from "RS232", "RS485".	
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" or "115200".	115200
Data Bits	Select from "7" or "8".	8
Stop Bits	Select from "1" or "2".	1
Parity	Select from "None", "Odd" or "Even".	None
Flow control	Select from "None", "Software" or "Hardware".	None



Default

50

1200

?

∧ Data Packing	

Packing Timeout

soon it reaches the specified length.

Packing Length 1200

Item	Description
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the
	data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the
	field. The unit is milliseconds.
	Note: Data will also be sent as specified by the packet length even when data is not
	reaching the interval timeout in the field.
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of
	data that is allowed to accumulate in the serial port buffer before sending. When a
	packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as

50

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

▲ Server Setting				
	Application Mode	Transparent	v	
	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		

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



∧ Server Setting		
Application Mode	Transparent	v
Protocol	UDP	v
Local IP		
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 Gateway 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 as follows:

∧ Server Setting			
	Application Mode	Modbus RTU Gateway	
	Protocol	TCP Server v	
	Local IP		]
	Local Port		]

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



∧ Server Setting		
Application Mode	Modbus RTU Gateway v	
Protocol	UDP v	
Local IP		
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 Gateway 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 Gateway	
	Protocol	TCP Server v	
	Local IP		
	Local Port		

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

▲ Server Setting		
Application Mode	Modbus ASCII Gateway v	
Protocol	UDP v	
Local IP		
Local Port		
Server Address		
Server Port		

Item	Description	Default
Application	Select from "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway".	Transp
Mode	Transparent: Device will transmit the serial data transparently	arent
	Modbus RTU Gateway: Device will translate the Modbus RTU data to Modbus	
	TCP data and sent out, and vice versa	
	• Modbus ASCII Gateway: Device will translate the Modbus ASCII data to Modbus	
	TCP data and sent out, and vice versa	
Protocol	Select from "TCP Client", "TCP Server", or "UDP".	ТСР
	• TCP Client: Device works as TCP client, initiate TCP connection to TCP server.	Client
	Server address supports both IP and domain name	
	• TCP Server: Device works as TCP server, listening for connection request from	
	TCP client	
	UDP: Device works as UDP client	
Server Address	Enter the address of server which will receive the data sent from device's serial port.	Null
	IP address or domain name will be available.	
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @	Enter device's LAN IP which will forward to the internet port of device.	Null
Transparent		



Item	Description	Default
Local Port @	Enter the port of device's LAN IP.	Null
Transparent		
Local IP @	Enter the local IP of under Modbus mode.	Null
Modbus		
Local Port @	Enter the local port of under Modbus mode.	Null
Modbus		

#### Status

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

Serial Por	t	Status			
Serial Po	rt Status				
Index	Туре	ТХ	RX	Connection Status	
1	RS232	0B	0B		
2	RS232	0B	0B		

# **3.2.10** Bluetooth (Optional)

This section allows you to set the Bluetooth parameters. Bluetooth can scan for other nearby Bluetooth devices.

#### General

Status			
_	_	_	
Enable	ON OFF		
Verbose Debug Enable	ON OFF		
Clear Interval	60	(?)	
	Enable Verbose Debug Enable	Enable ON OFF ? Verbose Debug Enable ON OFF ?	Enable ON OFF ? Verbose Debug Enable ON OFF ?

Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Verbose Debug	Click the toggle button to enable/disable this option. Enable for	OFF
Enable	verbose debugging information output.	
Clear Interval	Enter the interval of Bluetooth scan result clearify.	60
	unit:second	
	valid range:5-3600	

#### Status

ts Clear		
ts	Clear	

Click Clear to clear scan results

You can view scan results in the scan column.

#### **RobustOS Pro Software Manual**



Index	MAC	Name		RAW Data		RSSI		
1	23D542E5452F	(unknown)	1EFF0600010F	20028F5026A2BD63	3221C6CF	-99		
2	7E2FC52A2621	(unknown)	02010607	FFFCE806EEEF3C03	020016	-103		
3	37A59DE7A336	(unknown)	1EFF0600010F	20023ABD0EA095D	5361721F	-82		
4	4383A12E809C	(unknown)	1EFF4C000719	9010E2002F98F0200	059BDA3	-97		
5	45DAEF4F92C7	(unknown)	02011A020A08	80CFF4C001007351	F6FD2814	-91		
6	3F746D777121	(unknown)	02011A0DFF4	4C001608C1003BCF	631475D5	-92		
7	248FEE485581	(unknown)	1EFF0600010920222DD45D389589F631710			-97		
8	EA95C8FC7BB1	(unknown)	07FF4C0012020001			-92		
9	C77877D985B3	(unknown)	07FF4C0012023200		-84			
ican iBe	acon							
Index	MAC		UUID	Major M	inor RSSI	at 1m	RSSI	
ican Edo	lystone				-			
Index	MAC	Name	RSSI	Туре	Da	ata		
can EL/	A							

# 3.2.11 LoRa (Supported in LG5100)

This section allows you to set the LoRaWAN parameters. It is only for the LG5100.

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

#### RobustOS Pro Software Manual

General Settings	RF Settings	Filter Settings	s Status		
_					
▲ General Settings	Default	Gateway ID			
			34FA40FFFE214CC0		
	User Defined Gateway		ON OFF		
	User Defined (	Gateway ID	1234567890ABCDEF	(?)	
			Conorol Cottingo		

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		123456
Gateway ID	Enter Gateway ID.	7890AB
		CDEF

# **RF Settings**

General Settings	RF Settings Filter Settin	gs Status	
∧ SX1302 Board Sett	ings		
	Supported Frequency	CN470	v
	Full duplex	ON	
A SX1302 RF Chain0	Settings		
	Chain0 Enable	ON OFF	
	RF Frequency	470700000	
	RSSI Offset	-223	
	TX Enable	ON OFF	
	TX Min Frequency	47000000	
	TX Max Frequency	472700000	

10 robustel



▲ SX1302 RF Chain1 Settings	
Chain1 Enable	ON OFF
RF Frequency	471500000
RSSI Offset	-223
TX Enable	ON OFF

RF Settings					
Item	Description	Default			
	SX1302 Board Settings				
Support Frequency	Display support 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; RU868: RF Chain 0:869000000,RF Chain 1:864500000, 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. CN470: RF Chain 0:470700000,RF Chain 1: 471500000, 470.5,470.7,470.9,471.1,471.3,471.5,471.7,471.9.	Followed your device's model			
Full duplex	Enabled/Diasbled Full duplex mode.	OFF			
	SX1302 RF Chain 0 Settings				
Chain 0 Enable	Enabled/Diasbled Chain 0.	ON			
RF Frequency	Set frequency of RF link 0.	Followed your device's model			
RSSI Offset	Set RSSI offset of RF link 0.	-223			
TX Enable	Enabled/Disabled TX mode	ON			
TX Min Frequency	Set TX Minimum frequency of RF link 0.	Followed your device's model			
TX Max Frequency	Set TX Maximum frequency of RF link 0.	Followed your device's model			
SX1302 RF Chain 1 Settings					
Chain 0 Enable	Enabled/Diasbled Chain 0.	ON			
RF Frequency	Set frequency of RF link 1.	Followed your device's model			
RSSI Offset	Set RSSI offset of RF link 0.	-223			
TX Enable	Enabled/Disabled TX mode	OFF			
TX Min Frequency	Set TX Minimum frequency of RF link 1.	Followed your device's model			
TX Max	Set TX Maximum frequency of RF link 1.	Followed your device's			



RF Settings				
Item	Description	Default		
SX1302 Board Settings				
Frequency		model		

#### You can enable multi channels on this setting.

∧ SX1302 №	∧ SX1302 Multi Channels Settings			
Index	RF Chain	IF Frequency	+	
1	RF Chain 0	-400000	Σ×	
2	RF Chain 1	0	区 ×	

Click 🗹 to edit the RF Chain settings, here takes RF Chain 0 for example.

∧ Multi Channels Settings	
Index	1
Enable	ON OFF
RF Chain	RF Chain 0 v
IF Frequency	-400000

General Settings				
Item	Description	Default		
Index	Indicate the ordinal of the list.			
Enable	Click the toggle button to enable/disable this option.	ON		
RF Chain	Select the RF Chain			
15 fra	Enter center frequency in the range -500000-500000 in Hz. The offset between the			
IF frequency	center frequency of a particular channel and the center frequency of RF link 0/1.	0		

SX1302 Standard Channel Settings	
Enable	ON OFF
RF Chain	RF Chain 0 v
IF frequency	0
Bandwidth	500KHz v
Spread Factor	SF9 v

SX1302 Standard Channel Settings			
Item	Description	Default	



SX1302 Standard Channel Settings				
Item	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.			

<ul> <li>SX1302 FSK Channel Settings</li> </ul>				
	Enable	ON OFF		
	RF Chain	RF Chain 0	v	
	IF frequency	0		
	Bandwidth	500KHz	v	
	Datarate	250000		

SX1302 Standard Channel Settings		
Item	em 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
Datarate	Enter the datarate.	250000



# **Filter Settings**

General Settings	RF Settings	Filter Settings	Status		
∧ LoRa Filter Setting	gs				
		LoRa Filter ON	OFF		
2					
<ul> <li>Whitelist DevEUIs</li> </ul>					?
Index	DevEUI				+

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

Click + to add a whitelist rule.

∧ Whitelist Rules	
Index	1
DevEUI	

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



#### Status

∧ Basic		
	Model	
∧ RF package received		
CR	C Errors	
Du	plicates	
Join Du	plicates	
Join R	equests	
Total	Packets	
RF Packets R	leceived	
RF Packets Receive	ed State	
RF Packets For	rwarded	

∧ RF package sent	
Duplicates Acked	
Packets Acked	
Total Join Responses	
Join Responses Dropped	
Total Packets	
Packets Dropped	
RF Packets Sent to Concentrator	
RF Packets Sent Errors	



# ∧ Center Frequency

RF Chain 0 Frequency

RF Chain 1 Frequency

木 LoRa Mu	lti Datarate Channe	els	
Index	RF Chain	IF frequency	

#### LoRa Standard Channel

RF Chain	
IF frequency	
Bandwidth	
Spread Factor	

#### FSK Standard Channel

RF Chain		Cu
IF frequency		
Bandwidth		
Data Rate		

Status		
Item	Description	
	Basic	
Model	Show LoRa module model.	
	RF Package 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	
RF Packets Forwarded	Packets that CRC verified are sent from gateway to server.	
	Packets sent	
Duplicates Acked	Show the value of duplicate RF response packets sent.	
Packets Acked	Show the value of RF response packets sent.	



Status				
Item	Description			
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.			
RF Packets Sent to	Show the value of RF packets sent to concentrator.			
Concentrator				
RF Packets Sent Errors	Show the value of RF packets sent error.			
	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	Data Rate of FSK Standard Channel.			



# 3.3 Network

# 3.3.1 WAN

WAN stands for Wide Area Network, provides connectivity to the internet. You can configure WAN based on Ethernet, Cellular modem or Wi-Fi(if supported).

#### Link

Link	3	Status				
Settings						
Name	Туре	Description	Weight	Firewall Zone		+
Cellular	Modem	Backup WAN	0	external		:C×
Wired	Ethernet	default wan	0	external		:IC×
					Submit	Cancel

Click 🕂 to add a new WAN link.

Click  $\times$  to delete the link.

Press to drag the WAN link into the required order to switch between WAN connections, the topper one has higher priority.

Click 🚺 to edit the link.

Users can manage link connections in this section. It provides four types of connectivity interface to internet including Modem, Ethernet, VLAN and Wi-Fi.



∧ Link Settings	
Name	WWAN 3
Туре	Modem v
Interface	wwan
Description	default wan
Weight	0
Firewall Zone	external v

▲ Link Settings	
Name	WAN
Туре	Ethernet v
Interface	eth1 v
Description	
Weight	0 3
Firewall Zone	external v

#### **Note:** You should uncheck the eth0 of sub interface on **<u>Bridge</u>** section when set eth0 as WAN.

∧ Link Settings	
Name	
Туре	VLAN V
Interface	V
Description	
Weight	0
Firewall Zone	external v



∧ Link Settings	
Name	
Туре	WIFI v
Interface	wlan0 v
SSID	router
Password	
Description	
Weight	0
Firewall Zone	external v

#### Note: Before setting the WIFI link type, you should <u>config the Wi-Fi to Client mode</u>.

Item	Description	Default
Name	The name of link.	
Туре	The types of connectivity.	
	Modem: connected by cellular network.	
	Ethernet: connected by Ethernet wired network.	
	VLAN: connected by VLAN network.	
	Wi-Fi: connected by Wi-Fi network.	
Interface	Set the related interface.	
	If the type is Modem, please see the 3.2.2 Cellular.	
	If the type is Ethernet, please see the <b>3.2.1 Ethernet.</b>	
	If the type is VLAN, please see the <b><u>3.2.7 VLAN</u></b> .	
Description	The description of the link.	
SSID	The name of Wi-Fi network.	
Password	The Password of Wi-Fi network.	
Weight	The weight of this link among all links. 0 means not involved.	
Firewall Zone	The chosen set of firewall rules, please see the <b>3.3.5 Firewall</b> .	

▲ IPv4 Settings			
	IPv4 Connection Type	DHCP	v ?
∧ IPv6 Settings			
	IPv6 Connection Type	Auto	v

Item	Description	Default
IPv4 Connection Type	The type of IPv4 connection.	DHCP



Item	Description	Default	
	• DHCP.		
	• PPPoE.		
	Manual.		
	Disable.		
	Enter the parameters accordingly.		
	*Note: IPv6 over PPPoE is not supported now, so disabling IPv6 if		
	choosing PPPoE here.		
IPv6 Connection Type	The type of IPv6 connection.	Auto	
	Auto.		
	Manual.		
	Disable.		
	Enter the parameters accordingly.		

∧ Health Detection Settings		?
Enable	ON OFF	
IPv4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114	
IPv6 Primary Server	2001:4860:4860::8888	
IPv6 Secondary Server	2400:3200:baba::1	
Interval	30	0
Timeout	3	0
Reconnect Tries	3	0
Recover Tries	3	0

Item	Description	Default
Enable	Toggle the button to enable the health detection function	ON
IPv4 Primary Server	IPv4 Primary Server	8.8.8.8
IPv4 Secondary Server	IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	IPv6 Secondary Server	2400:3200:baba::1
Interval	Seconds to send next ping	30
Timeout	Seconds to wait for ping response	3
Reconnect Tries	Reconnect this link in case of sequential probes are	3
	unsuccessful.	
Recover Tries	Recovery this link in case of sequential probes are	3
	successful.	



#### Status

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

Link	Stat				
ink Status					
Interface	Status	MAC Address	IPv4 Address	IPv6 Address	
eth1	Connected	34:FA:40:0D:8E:2F	172.16.19.22		
wwan	Disconnected				

# 3.3.2 LAN

A Local Area Network (LAN) connects network devices together, such as Ethernet or Bridge, in a logical Layer-2 network. The default link(br\_lan) is always available.

#### Link

Link		Status		
∧ Settings	-		-	
Name	Туре	Description	Firewall Zone	+
LAN1	Bridge	default lan	internal	Ц×
9				

Click 🕂 to add a new LAN link.

Click  $\times$  to delete the LAN link.

Click 🗹 to edit the LAN link.

Users can manage link connections in this section. It provides three types of connectivity interface to internet including Bridge, Ethernet and VLAN.



∧ Link Settings		
Name	LAN1	?
Туре	Bridge v	
Interface	br_lan v	
Description	default lan	
Firewall Zone	internal v	

Item	Description	Default
Name	The name of the LAN link.	
Туре	The types of connectivity. Select from "Bridge", "Ethernet" and "VLAN".	Bridge
	Bridge: connected by Bridge network.	
	Ethernet: connected by Ethernet wired network.	
	VLAN: connected by VLAN network.	
Interface	Set the related interface.	
	If the type is Bridge, please see the <b><u>3.2.3 Bridge.</u></b>	
	If the type is Ethernet, please see the <b><u>3.2.1 Ethernet.</u></b>	
	If the type is VLAN, please see the <b><u>3.2.7 VLAN.</u></b>	
Description	The description of the link.	
Firewall Zone	The chosen set of firewall rules, please see the <b>3.3.5 Firewall.</b>	internal

∧ ip4 Settings			
IPv4 Address	192.168.0.1/24	+	
∧ DHCPv4 Settings			
IP Pool Start	192.168.0.2		
IP Pool End	192.168.0.100		
Primary DNS			
Secondary DNS			
Lease Time	120	(?)	

Item	Description	Default
IPv4 Address	Enter the IPv4 address with netmask.	192.168.0.1/24
IP Pool Start	The start IP address in pool.	192.168.0.2
IP Pool End	The end IP address in pool.	192.168.0.100
Primary DNS	Enter the primary DNS.	Null



Item	Description	Default
Secondary DNS	Enter the secondary DNS.	Null
Lease Time	The lease time in minute.	120

▲ IPv6 Settings			
	Address Mode	Delegated v	
▲ IPv6 Settings			
	Address Mode	Static v	
	NAT66	ON OFF	
2 A	IPv6 Address	fd00::1/64	
Item	Description		Default
Address Mode	Delegated or Statio	2.	Delegated
NAT66	IPv6-to-IPv6 Netwo	ork Address Translation. On or Off in static mode.	OFF
IPv6 Address	Enter the IPv6 add	ress with 64-bit network prefix in static mode.	fd00::1/64

#### Status

This window allows you to view the status of LAN link.

nterface	MAC Address	IPv4 Address	IPv6 Address	
br lan	34:FA:40:05:9E:CE	192.168.0.1	fe80::a56d:577b:36	

connec	ted Devices				
Index	IP Address	MAC Address	Interface	Inactive Time	
1	192.168.0.2	7C:8A:E1:8C:97:04	br_lan	Os	
2	fe80::41c4:e5d0:39	7C:8A:E1:8C:97:04	br_lan	178s	

Index IP Address MAC Address Interface Expired Time	NDHCP Lea	se Table				
	Index	IP Address	MAC Address	Interface	Expired Time	

# 3.3.3 Route

Routes ensure that network traffic finds its path to a destination network. Static routes are fixed routing entries in routing table.

# **Static Route**

∧ Static Route

Static Ro	oute	Status				
Static Ro	ute Table					
Index	Description	Destination	Netmask	Gateway	Interface	+

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

Item	Description	Default
Index	Indicate the ordinal of the list.	
Description	Enter a description for this static route.	Null
Destination	Enter the IP address of destination host or destination network.	Null
Netmask	Enter the Netmask of destination host or destination network.	Null
Gateway	Define the gateway of the destination.	Null
Metric	Enter the Metric value. Metrics help the gateway choose the best route	0
	among multiple feasible routes to a destination. The route will go in the	
	direction of the gateway with the lowest metric value.	
MTU	Enter the MTU value, 1280~1500.	1500

September 14, 2023

Index	1	
Description		
Destination		
Netmask		
Gateway		
Metric	0	
MTU	1500	
Interface	br_lan v	



Item	Description	Default
Interface	Choose the corresponding port of the link that you want to configure.	br_lan

#### Status

This window allows you to view the status of route.

tatic Rout	e Stat	tus				
Route Tab	le					
Index	Destination	Netmask	Gateway	Interface	Metric	
1	0.0.0	0.0.0	172.16.19.1	eth1	100	
2	0.0.0.0	0.0.0.0	10.182.244.189	wwan	200	
3	10.182.244.188	255.255.255.252	0.0.0.0	wwan	200	
4	172.16.19.0	255.255.255.0	0.0.0.0	eth1	100	
5	192.168.0.0	255.255.255.128	0.0.0.0	br_lan	425	

# 3.3.4 Policy Route

In this window, you can manage the outbound route based on the IP address, port number in the packet.

# **Policy Route**

Policy Rou				
Match sett	tings			

Click + to add a policy route. The maximum count is **20**.



^	Match	setti	ng

A Match Settings		
Index	1	
Name		
Protocol	TCP v	]
Hooks	PREROUTING	
Source Address		?
Source Port		0
Source MAC		0
Destination address		0
Destination port		0

Item	Description	Default
Index	Indicate the ordinal of the list.	
Name	Name of Policy Route.	
Protocol	The type of network protocol. Select from "Any",	TCP-UDP
	"TCP","UDP","TCP-UDP","ICMP" and "IGMP".	
Hooks	Fixed setting.	
Sources Address	Enter the source IP address.	
Source Port	Enter the source port in TCP/UDP type.	
Source MAC	Enter the source mac address.	
Destination Address	Enter the destination IP address.	
Destination Port	Enter the destination port in TCP/UDP type.	

∧ Route rules		
	Destination	
	Netmask	
	Gateway	
	Interface	br_lan v

Item	Description	Default
Destination	Enter the IP address of destination host or destination network.	
Netmask	Enter the Netmask of destination host or destination network.	
Gateway	Define the gateway of the destination.	
Interface	Choose the corresponding port of the link that you want to configure.	br_lan

# 3.3.5 Firewall

Firewall makes use of Linux iptables to control inbound and outbound traffic.

#### **General Setting**

General Settings	Port Forwards	Traffic Rules	Custom Rules	Status	
▲ General Settings					
	Enable SYN-floo	d protection	ON OFF		
		Input	ccept	V	
		Output	ccept	V	
		Forward	Prop	v	

Item	Description	Default
Enable SYN-flood protection	Countermeasures to protect against SYN flood attacks, click the	ON
	toggle button to enable/disable.	
Input	Default action of the Input chain if a packet does not match any	Accept
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Output	Default action of the Output chain if a packet does not match any	Accept
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Forward	Default action of the Forward chain if a packet does not match any	Drop
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Note: The general setting is use	ed as a default firewall setting unless specified.	

nes				(
Name	Input	Output	Forward	-
external	Drop	Accept	Drop	
internal	Accept	Accept	Accept	Z

Zone is a set of firewall rules, users can define their own firewall zone.



# Click + to add one firewall zone. The maximum count is **50**

▲ Zones		
Name	external	
Input	Drop v	
Output	Accept v	
Forward	Drop v	
Masquerading	ON OFF	
MSS clamping	ON OFF	

Item	Description	Default
Name	The name of the firewall zone.	
Input	Default action of the Input chain if a packet does not match any	Drop
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Output	Default action of the Output chain if a packet does not match any	Accept
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Forward	Default action of the Forward chain if a packet does not match any	Drop
	exist rule on that chain.	
	Accept: Packet gets to continue to the next chain.	
	Drop: Packet is stopped and deleted.	
Masquerading	Click the toggle button to enable/disable. MASQUERADE is an	ON
	iptables target that can be used instead of the SNAT (source NAT)	
	target when the external IP of the network interface is not known at	
	the moment of writing the rule (when the interface gets the	
	external IP dynamically).	
MSS clamping	Click the toggle button to enable/disable. MSS clamping is a	ON
	workaround used to change the maximum segment size (MSS) of all	
	TCP connections passing through links with an MTU lower than the	
	Ethernet default of 1500.	



∧ DMZ Settings		
Enable DMZ	ON OFF	
Host IP Address		]
Source IP Address		0
Destination IP Address		]

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

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

▲ Access Control Settings	
Enable SSH Access	ON OFF
Enable HTTP Access	ON OFF
Enable HTTPS Access	ON OFF
Enable Ping Respond	ON OFF ?

Item	Description	Default
Enable SSH Access	Click the toggle button to enable/disable this option. When enabled, the	OFF
	zone user can access the device via SSH.	
Enable HTTP Access	Click the toggle button to enable/disable this option. When enabled, the	OFF
	zone user can access the device via HTTP.	
Enable HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the	OFF
	zone user can access the device via HTTPS.	
Enable Ping Respond	Click the toggle button to enable/disable this option. When enabled, the	OFF
	device will reply to the Ping requests from other hosts on the zone.	



### **Port Forwards**

General Setting	gs	Port Forwards	Traffic Rules	Custom Rules	Status	
∧ Port Forwa	rds Rules	_	_	_	_	_
Index	Name	Protocol	Source zone	Destination zone		+

This window allows you to view the port forward rules. Port forwarding is a way of redirecting an incoming connection to another IP address, port or the combination of both.

click i to add one. The maximum count is <b>50</b>	Click 🗧	to add one.	The maximum	count is 50.
--	---------	-------------	-------------	--------------

▲ Port Forwards Rules		
Index	1	
Name		
IPv4 Source Address		+
Protocol	TCP-UDP v	
Source zone	external v	
External Port		0
Destination zone	external v	
Internal IP Address		
Internal port		0

Item	Description	Default
Index	Indicate the ordinal of the list.	
Name	Name of the rule.	Null
IPv4 Source Address	IP address or network segment used by connecting hosts.	Null
	The rule will apply only to hosts that connect from IP addresses specified	
	in this field.	
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP
Source zone	The zone to which the third party will be connecting. Select a configured	external
	zone.	
External Port	Match incoming traffic directed at the given destination port or port range	Null
	on this host. Select a configured zone.	
Destination zone	The zone to which the incoming connection will be redirected.	external
Internal IP Address	The IP address to which the incoming connection will be redirected.	Null
Internal Port	The port number to which the incoming connection will be redirected.	Null



### **Traffic Rules**

General Settings	Port Fo	orwards	Traffic Rules	Custom Rules	Status	
▲ Traffic Rules			_	_		_
Index	Name	Address Family	Protocol	Source zone	Action	+
5 <u></u>						

#### This window allows you to view the traffic rules.

#### Click + to add one. The maximum count is **50**.

▲ Traffic Rules		
Index	1	
Name		
Address Family	IPV4-IPV6 v	
Protocol	TCP-UDP v	
Source zone	device_output v	
IPv4 Source Address		0
IPv6 Source Address		
Source Port		1
Source MAC		?
Output zone	any_forward v	
IPv4 Destination Address		0
IPv6 Destination Address		
Destination port		0
Action	Drop v	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Name	The name of the rule.	Null
Address family	Select from "IPv4", "IPv6" or "IPv4-IPv6" as your application	IPv4-IPv6
	required.	
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP



Item	Description	Default
Source zone	The zone to which the third party will be connecting.	device_output
IPv4 Source Address	The IPv4 address or network segment used by connecting hosts.	Null
	The rule will apply only to hosts that connect from IP addresses	
	specified in this field.	
IPv6 Source Address	The IPv6 address or network segment used by connecting hosts.	Null
	The rule will apply only to hosts that connect from IP addresses	
	specified in this field.	
Source Port	Port number(s) used by the connecting host.	Null
	The rule will match the source port used by the connecting host with	
	the port number(s) specified in this field. Leave empty to make the	
	rule skip source port matching.	
Source MAC	MAC address of connecting hosts.	Null
	The rule will apply only to hosts that match MAC addresses specified	
	in this field. Leave empty to make the rule skip MAC address	
	matching.	
Output zone	The zone to which the incoming connection will be redirected.	any_forward
IPv4 Destination Address	The IP address to which the incoming connection will be redirected.	Null
IPv6 Destination Address	The IP address to which the incoming connection will be redirected.	Null
Destination port	The port number to which the incoming connection will be	Null
	redirected.	
Action	Select from "Accept", or "Drop" as your application required.	Null

### **Custom Rules**

General Settings	Port Forwa	ards	Traffic Rules	Custom Rules	Status		
∧ Custom Iptable	es Rules						
Index	Name	Family	Rule				+

This window allows you to view the custom rules.

Click + to add one. The maximum count is **50**.

∧ Custom Iptables Rule		
Index	1	
Name		
Family	IPv4 v	
Rule		0



Item	Description	Default
Index	Indicate the ordinal of the list.	
Name	Enter a description for this.	Null
Family	Select from "IPv4", "IPv6" or "IPv4-IPv6" as your application required.	IPv4
Rule	Users specify their own iptables rule in required format.	Null

#### Status

This window allows you to view the status of firewall.

eneral Settings	Port Forwards	Traffic Rules	Custom Rules	Status	
IPv4 Filter					
0 0 ACCEI		* 0.0.0.0/0	0.0.0/0	tcp dpt:22	
12 562 ACCE	T tcp *	* 0.0.0.0/0	0.0.0/0	tcp dpt:80	
0 0 ACCE	T tcp *	* 0.0.0.0/0	0.0.0/0	tcp dpt:443	
0 0 ACCE	T icmp *	* 0.0.0.0/0	0.0.0/0		
0 0 ACCE	T all *	* 0.0.0.0/0	0.0.0/0	ctstate DNAT	
86 10647 zone	internal_src_ACCEPT	all * *	0.0.0/0	0.0.0/0	
Chain zone_inter	al_output (1 referen	ices)			
pkts bytes targe	t prot opt in	out source	destination	1	
28 6776 output	t_internal_rule all	* *	0.0.0/0	0.0.0/0	
28 6776 zone	internal_dest_ACCEPT	all * *	0.0.0/0	0.0.0/0	
Chain zone_inter	al_src_ACCEPT (1 ref	erences)			
pkts bytes targe	t prot opt in	out source	destinatior	1	
00 10017 1000	T all br la	* 0000/0	0.0.0/0	ctstate NEW, UNTRACKED	

# 3.3.6 QoS

QoS provides the possibility to prioritize network traffic based on hosts, ports or services and limit download or upload speeds on a selected interface.

### **General Setting**

QoS				
▲ General Settings	_	_		_
	Enable QoS	ON OFF		
	Upload Bandwidth	10000	?	
	Download Bandwidth	10000	0	

Item	Description	Default
Enable QoS	Click the toggle button to enable or disable.	OFF
Upload Bandwidth	Enter a value for the upload bandwidth, the unit is kbit.	10000



Item	Description	Default
Download Bandwidth	Enter a value for the download bandwidth, the unit is kbit.	10000

# **Priority Definition**

Priority D	efinition				?
Index	Priority	Bandwidth	Borrow Spare Bandwidth		
1	Highest	20	true		
2	High	20	true		C
3	Normal	20	true		Ľ
4	Low	20	true		Ľ
5	Lowest	20	true		

# Click 🗹 to set the priority.

▲ Priority Definition	
Index	1
Priority	Highest     v
Bandwidth	20
Borrow Spare Bandwidth	ON OFF ?

Item	Description	Default
Bandwidth	Percentage of total bandwidth. The sum of bandwidth of all the priorities	20
	cannot be greater than 100.	
Borrow Spare Bandwidth	The traffic associated with this priority will borrow unused bandwidth	ON
	from other priorities when borrowing is enabled, and will be limited to	
	the specified bandwidth when borrowing is disabled.	

### **IPv4 QoS Rules**

IPv4 Q	oS Rules						
Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority	



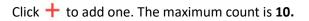
### Click + to add one. The maximum count is **10**.

∧ QoS Rules	
Index	1
Source Address	
Source Port	(
Source MAC	()
Target Address	()
Target Port	
Protocol	All v
Priority	Normal v

Item	Description	Default
Index	Indicate the ordinal of the list.	
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null
Target Address	The address of Host(s) to which data will be transmitted.	Null
Target Port	The port of Host(s) to which data will be transmitted.	Null
Protocol	Select from "All", "TCP", "UDP" or "ICMP" as your application required.	All
Priority	Select from "Highest", "High", "Normal", "Low" or "Lowest" as your	Normal
	application required.	

### **IPv6 QoS Rules**

ndex	Source Address	Source Port	Target Address	Target Port	Protocol	Priority	-





∧ QoS Rules
-------------

~ QUS Rules			
	Index	1	
	Source Address		0
	Source Port		<b>?</b>
	Source MAC		?
	Target Address		<b>?</b>
	Target Port		0
	Protocol	All	v
	Priority	Normal	v

Item	Description	Default
Index	Indicate the ordinal of the list.	
Source Address	The address of Host(s) from which data will be transmitted.	Null
Source Port	The port of Host(s) from which data will be transmitted.	Null
Source MAC	The MAC address of Host(s) from which data will be transmitted.	Null
Target Address	The address of Host(s) to which data will be transmitted.	Null
Target Port	The port of Host(s) to which data will be transmitted.	Null
Protocol	Select from "All", "TCP", "UDP" or "ICMP" as your application required.	All
Priority	Select from "Highest", "High", "Normal", "Low" or "Lowest" as your	Normal
	application required.	

# 3.4 Packet Forwarders (Supported in LG5100)

## 3.4.1 Basic Station

A LoRa Basic Station is a LoRaWAN device software implementation which provides this core functionality in terms of handling the packet flow, managing spectrum access and LNS backhaul connectivity, and more.

### **General Setting**

General Settings	Status	Cert Manag	ger		
∧ Gateway Settings					
		Enable	ONOFF		
		TLS Enable	ONOFF		
	S	erver Address	127.0.0.1		
		Server Port	3001		

Item	Description	Default
Enable	Enable application	OFF
TLS Enable	Enable TLS encrypted transmission	OFF
Server Address	Server address	127.0.0.1
Server Port	Server port	3001

#### Status

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

General Settings	Status	Cert Manager			
A Basia	_	_		_	
▲ Basic					
		TC Status			
	S	tation Version			
	Package Vers	sion (Protocol)			
	HAL L	ibrary Version			
Item	De	escription			
TC Status	P	atform connection stat	us		



Station Version	Application version
Package Version (Protocol)	Application package version
HAL Library Version	LoRaWAN HAL library version

### **Cert Manager**

General Settings	Status	Cert Mana	ger			
		_			_	
∧ CA File Import						?
		CA Cert	Choose File No file chosen	<u>1</u>		
		Client Cert	Choose File No file chosen	<u>1</u>		
		Client Key	Choose File No file chosen	<u>1</u>		

∧ Certificate	e Files			
Index	File Name	File Size	Modification Time	
-				

Cert Manager					
Item	Default				
	CA File Import				
CA Cert	Click "Choose File" to locate CA Cert file and then import this file into your				
	device.				
Client Cert	Click "Choose File" to locate Certificate file, and then import this file into				
	your device.				
Client Key	Click "Choose File" to locate Key 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			

# 3.4.2 UDP Forwarder

A Packet Forwarder is a program running on a device, that interacts:

- (1) With the LoRa chip, to receive and transmits LoRa packets;
- (2) With the network, to transmit them for applications.



### **General Setting**

General Settings Status			
▲ Gateway Settings			
	Enable	ON OFF	
Lo	rawan Public	ON OFF	
Se	erver Address	127.0.0.1	
Servi	er Uplink Port	1700	
Service [	)ownlink Port	1700	
Кеер	Alive Interval	5	
Sta	itistic Interval	30	
Push Timeou	t Millisecond	100	

Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Lorawan Public	Click the toggle button to enable or disable the function.	ON
Server Address	Set the LoRaWAN network server address.	127.0.0.1
Server Uplink	Set the uplink port to LoRaWAN network server	1700
Port		
Server Downlink	Set the downlink port to LoRaWAN network server.	1700
Port		
Keep Alive	Time interval for obtaining downlink data.	5
Interval		
Statistic Interval	Statistical interval, USI update interval.	30
Push Timeout	Uplink data timeout.	100
Millisecond		

#### Status

This section allows you to view the status of Packet forwarder.

General Settings

∧ Basic

10 robustel

Status

Status	
Packet Forwarder (Protocol)	

Push Data Acknowledged

HAL Library Version

▲ Uplink Push Data Datagrams Sent

∧ Downlink

Pull Data Sent

Pull Resp Datagrams Received

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			
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 Datagrasms Received	Show packet counts and size that will be sent from server to gateway.			



## 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.

#### General

General	Tunnel Status			
∧ General Settings				
	Keepalive	20	?	
	Optimize DH Exponent Size	ON OFF ?		
	Debug Enable	ONOFF		
	Enable Backup Gateway	ONOFF		

Item	Description	Default
Keepalive	Set the time to live in seconds. The router 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,	OFF
Optimize DH Size	when using dhgroup17 or dhgroup18, it helps to shorten the time to	
	generate the dh key.	
Dohug Frahla	Click the toggle button to enable/disable this option. Enable for IPsec VPN	OFF
Debug Enable	information output to the debug port.	
Enable Backup Gateway	Click the toggle button to enable/disable this option.	OFF

#### Tunnel

General	2	Tunnel	Status		
Funnel Se	ttings				



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

#### **General Setting**

▲ General Settings		
Index	1	
Enable	ON OFF	
Description		
Link Binding	wwan v	
Gateway		0
Protocol	ESP v	
Mode	Tunnel v	
Local Subnet		?
Remote Subnet		0
ІКЕ Туре	[IKEv1 v	
Negotiation Mode	Main v	
Initiation Mode	Always On v	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Link binding	Select the link to build IPSec.	Unbound
Gateway	Enter the address of remote side IPsec VPN server. 0.0.0.0 represents for any address.	Null
Mode	<ul> <li>Select from "Tunnel" and "Transport".</li> <li>Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it</li> <li>Transport: Used between end-stations or between an end-station and a router, if the router is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination</li> </ul>	Tunnel
Protocol	Select the security protocols from "ESP" and "AH".	ESP



	ESP: Use the ESP protocol	
	AH: Use the AH protocol	
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g.	Null
	192.168.1.0/24	
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g.	Null
	10.8.0.0/24	
ІКЕ Туре	Select from "IKEv1" and "IKEv2".	IKEv1
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1. If	Main
	the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE	
	negotiation mode must be aggressive. In this case, SAs can be established as	
	long as the username and password are correct.	
Initial Mode	Select from "Always On" and "On Demand".	Always On

### **Advanced Setting**

▲ Advanced Settings	
Enable Compression	ON OFF
Enable Forceencaps	ON OFF ?
Backup Gateway	(?)
Expert Options	

Item	Description	Default
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress	OFF
	the inner headers of IP packets.	
Enable Forceencaps	Force UDP encapsulation for ESP packets even if no NAT situation is	OFF
	detected. This may help to surmount restrictive firewalls.	
Backup Gateway	Backup Address of remote peer to initiate connection, empty means disable.	Null
Expert Options	Add more PPP configuration options here, format: config-desc; config-desc,	Null
	e.g. protostack=netkey; plutodebug=none	

## PHASE 1

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

∧ PHASE 1	
Encryption Algorithm	3DES v
Authentication Algorithm	SHA1 v
IKE DH Group	DHgroup2 v
Authentication Type	PSK v
PSK Secret	
Local ID Type	Default v
Remote ID Type	Default v
IKE Lifetime	86400

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

∧ PHASE 1	
Encryption Algorithm	3DES v
Authentication Algorithm	SHA1 v
IKE DH Group	DHgroup2 v
Authentication Type	CA v
Local Certificate	None
Remote Certificate(Optional)	None v
Private Key	None v
CA Certificate	None v
Private Key Password	
IKE Lifetime	86400

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

10 robustel

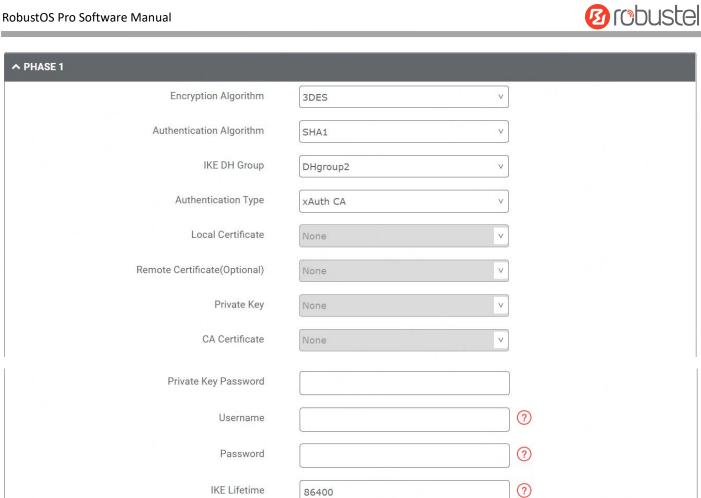
∧ PHASE 1		
Encryption Algorithm	3DES v	]
Authentication Algorithm	SHA1 v	]
IKE DH Group	DHgroup2 v	]
Authentication Type	PKCS#12 v	]
Remote Certificate(Optional)	None v	]
PKCS#12 Certificate	None v	]
Private Key Password		]
IKE Lifetime	86400	] ⑦

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

∧ PHASE 1		
Encryption Algorithm	3DES v	
Authentication Algorithm	SHA1 v	
IKE DH Group	DHgroup2 v	
Authentication Type	XAuth PSK v	
PSK Secret		
Local ID Type	Default v	
Remote ID Type	Default v	
Username		0
Password		?
IKE Lifetime	86400	0

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

10 robustel



Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128", "AES192" and "AES256".	3DES
	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", "SHA2 384" or "SHA2 512" .	MD5
Algorithm		
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14",	DHgroup2
	"DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18".	
Authentication Type	Select from "PSK", "CA", "xAuth PSK", "PKCS#12" and "xAuth CA" to be used in	PSK
	IKE negotiation.	
	PSK: Pre-shared Key	
	CA: Certification Authority	
	xAuth: Extended Authentication to AAA server	
	PKCS#12: Exchange digital certificate authentication	
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "Address", "FQDN" and "User FQDN" .	Default
	Default: Uses an IP address as the ID in IKE negotiation	
	• FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is	
	selected, type a name without any at sign (@) for the local security	



Item	Description	Default		
	router, e.g., test.robustel.com			
	• User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this			
	option is selected, type a name string with a sign "@" for the local			
	security router, e.g., test@robustel.com			
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation.	Default		
	Default: Uses an IP address as the ID in IKE negotiation			
	• FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is			
	selected, type a name without any at sign (@) for the local security			
	router, e.g., test.robustel.com			
	• User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this			
	option is selected, type a name string with a sign "@" for the local			
	security router, e.g., test@robustel.com			
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new	86400		
	SA. As soon as the new SA is set up, it takes effect immediately and the old			
	one will be cleared automatically when it expires.			
Private Key Password	Enter the private key under the "CA" and "xAuth CA" authentication types.			
Username	Enter the username used for the "xAuth PSK" and "xAuth CA" authentication			
	types.			
Password	Enter the password used for the "xAuth PSK" and "xAuth CA" authentication	Null		
	types.			

### PHASE 2

▲ PHASE 2		
Encryption Algorithm	3DES v	]
Authentication Algorithm	SHA1 v	]
PFS Group	PFS(N/A) v	]
SA Lifetime	28800	0
DPD Interval	30	] 📀
DPD Failures	150	] 🕐

Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128", "AES192"or "AES256" when you select "ESP"	3DES
	in "Protocol". Higher security means more complex implementation and	
	lower speed. DES is enough to meet general requirements. Use 3DES when	
	high confidentiality and security are required.	
Authentication	Select from "MD5", "SHA1", "SHA2 256" or "SHA2 512" to be used in SA	MD5
Algorithm	negotiation.	
PFS Group	Select from "PFS(N/A)", "DHgroup1", "DHgroup2", "DHgroup5",	DHgroup2



Item	Description	Default
	"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 the interval after which DPD is triggered if no IPsec protected packets is	30
	received from the peer. DPD is a Dead peer detection. DPD irregularly	
	detects dead IKE peers. When the local end sends an IPsec packet, DPD	
	checks the time the last IPsec packet was received from the peer. If the time	
	exceeds the DPD interval, it sends a DPD hello to the peer. If the local end	
	receives no DPD acknowledgment within the DPD packet retransmission	
	interval, it retransmits the DPD hello. If the local end still receives no DPD	
	acknowledgment after having made the maximum number of	
	retransmission attempts, it considers the peer already dead, and clears the	
	IKE SA and the IPsec SAs based on the IKE SA.	
DPD Failures	Set the timeout of DPD (Dead Peer Detection) packets.	150

#### Status

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

		Status					
Status		_	-	-	-	-	_
escription	Status	Uptime	_	_		_	_
			Status	Status	Status	Status	Status

# 3.5.2 OpenVPN

This section allows you to set the OpenVPN and the related parameters. OpenVPN is an open-source software application that creates secures point-to-point or site-to-site connections.



### **OpenVPN**

OpenVPN	Status					
▲ Tunnel Settings						
Index Enab	e Description	Mode P	eer Address			+
▲ Password Manage	•					
Index Us	ername					+
∧ Client Manage						
Index Enab	e Common Na	me Client IP	Address			+

### **Tunnel Setting**

Click to add an OpenVPN tunnel settings. The maximum count is 5. The configure page might vary when choosing different mode, and the **Authentication Type** might be fixed for using on specific mode. By default, the mode is "P2P". The window is displayed as 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	v
Authentication Type	None	v ?
Local IP	10.8.0.1	
Remote IP	10.8.0.2	
Keepalive Interval	20	0
Keepalive Timeout	120	0
TUN MTU	1500	
Max Frame Size		
Enable Compression	ON OFF	
Enable NAT	ON OFF	
Verbose Level	0	v 0
Advanced Settings		
Expert Options		0

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

∧ General Settings	
Index	1
Enable	ON OFF
Description	
Mode	Client v ?
Protocol	UDP v
Peer Address	
Peer Port	1194
Interface Type	TUN     v

Ørobustel

Authentication Type	None	v ?	
Renegotiation Interval	86400	?	
Keepalive Interval	20	?	
Keepalive Timeout	120	•	
TUN MTU	1500		
Max Frame Size			
Enable Compression	ON OFF		
Enable NAT	ON OFF		
Enable DNS overrid	ON OFF ?		
Verbose Level	0	v ?	

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

∧ General Settings		
Index	1	
Enable	ON OFF	
Enable IPv6	ON OFF	
Description		
Mode	Server	v (?)
Protocol	UDP	v
Listen IP Address		
Listen Port	1194	
Interface Type	TUN	v



Listen IP Address		
Listen Port	1194	
Interface Type	TUN	v
Authentication Type	None	v ?
Enable IP Pool	ON OFF	
Client Subnet	10.8.0.0	
Client Subnet Netmask	255.255.255.0	
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	ON OFF	
Enable NAT	ON OFF	
Verbose Level	0	v ?



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

	Listen IP Address		
	Listen Port	1194	
	Interface Type	TUN	v
	Authentication Type	None	v 🕐
1. T P.+	Local IP	10.8.0.1	
	Remote IP	10.8.0.2	
	Keepalive Interval	20	<b>?</b>
	Keepalive Timeout	120	(?)
	TUN MTU	1500	

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

Listen Port	1194
Interface Type	TUN v
Authentication Type	Preshared v ?
Pre-Share Key	None v
Local IP	10.8.0.1
Remote IP	10.8.0.2
Encrypt Algorithm	BF v
Authentication Algorithm	SHA1 v
Keepalive Interval	20



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

Listen IP Address			
Listen Port	1194		
Interface Type	TUN	v	
Authentication Type	Password	v ?	
Local IP	10.8.0.1		
Remote IP	10.8.0.2		
Encrypt Algorithm	BF	v	
Authentication Algorithm	SHA1	v	
Keepalive Interval	20	0	

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

Listen Port	1194	
Interface Type	TUN v	
Authentication Type	X509CA v	0
Root CA	None v	
Certificate File	None v	
Private Key	None v	
Private Key Password		
Local IP	10.8.0.1	
Remote IP	10.8.0.2	
Encrypt Algorithm	BF v	

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

	_		
	Listen Port	1194	
	Interface Type	TUN	v
Auti	hentication Type	X509CA Password	v ?
	Root CA	None	v
	Certificate File	None	v
	Private Key	None	v
Privat	te Key Password		
	Local IP	10.8.0.1	
	Remote IP	10.8.0.2	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable this OpenVPN tunnel.	ON
Enable IPv6	Click the toggle button to enable/disable IPv6.	OFF
Description	Enter a description for this OpenVPN tunnel.	Null
Mode	Select from "P2P", "Client" or "Server".	P2P
TLS Mode	Select from "None", "Client" or "Server".	None
Protocol	Select from "UDP", "TCP-Client" or "TCP-Server".	UDP
Peer Address	Enter the end-to-end IP address or the domain of the remote OpenVPN	Null
	server.	
Peer Port	Enter the end-to-end listener port or the listener port of the OpenVPN	1194
	server.	
Listen IP Address	Enter the IP address or domain name.	Null
Listen Port Enter the listener port at this end.		1194
Interface Type	Select from "TUN", "TAP" which are two different kinds of device	TUN
	interface for OpenVPN. The difference between TUN and TAP device is	
	that a TUN device is a point-to-point virtual device on network while a	
	TAP device is a virtual device on Ethernet.	
Authentication Type	Select from "None", "Preshared", "Password", "X509CA", "X509CA	
	password".	
	Note:None and Preshared types only used for P2P mode. It must to add	Null
	account from the User Management, when using server mode with	
	password authentication.	
Private Key Password	Enter the private key password under "X509CA" and "X509CA	Null
	password" authentication.	
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2



Item	Description	Default
Encrypt Algorithm	<ul> <li>Select from "BF", "DES", "DES-EDE3", "AES-128", "AES-192" and</li> <li>"AES-256".</li> <li>BF: Use 128-bit BF encryption algorithm in CBC mode</li> <li>DES: Use 64-bit DES encryption algorithm in CBC mode</li> <li>DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode</li> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> </ul>	BF
Authentication Algorithm	Select from "MD5", "SHA1", "SHA256" or "SHA512".	SHA1
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set the keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
TUN MTU	Set the MTU for the tunnel.	1500
Max Frame Size	Sets the shard size of the data to be transmitted through the tunnel.	Null
Enable Compression	Click the switch button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of host behind router will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	<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		
	Expert Options	
Item	Description	Default
Expert Options	Enter some other options of OpenVPN in this field. Each expression can	Null
	be separated by a ';'.	

### **Client Management**

Client Ma	nage			
Index	Enable	Common Name	Client IP Address	



# Click + to add client information. The maximum count is **20**.

∧ General Settings	
Index	1
Enable	ON OFF
Common Name	()
Client IP Address	

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

#### Status

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

	Status					
anal Statua		_	_	_	_	_
	Status	Mode	Uptime	Local IPv4	Local IPv6	_
ent List						
Common	Name	Real IP	Port	Virtual IPv4	Virtual IPv6	
(	nnel Status escription ent List Common	nnel Status escription Status	nnel Status escription Status Mode ent List	nnel Status escription Status Mode Uptime ent List	nnel Status escription Status Mode Uptime Local IPv4 ent List	nnel Status escription Status Mode Uptime Local IPv4 Local IPv6 ent List

### 3.5.3 GRE

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



#### GRE

GRE		Status		
∧ Tunnel Se	ettings			
Index	Enable	Description	Remote IP Address	+

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

▲ Tunnel Settings	
Index	1
Enable	ON OFF
Description	
Remote IP Address	
Local Virtual IP Address	
Local Virtual Netmask/Prefix Length	
Remote Virtual IP Address	
Enable Default Route	ON OFF
Enable NAT	ON OFF
Secrets	
Link Binding	wwan

Item	Description	Default
Index	Indicate the ordinal of the 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
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask/Prefix	Set the local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set the remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all	OFF
	the traffics of the router will go through the GRE VPN.	



Enable NAT	Click the toggle button to enable/disable this option. This option must		
	be enabled when router under NAT environment.		
Secrets	Set the key of the GRE tunnel.	Null	
Link Binding	Set the specified interface of the GRE Tunnel	wwan	

#### Status

This section allows you to view the GRE tunnel status.

GRE	3	Status				
GRE tunn	el status					
Index	Description	Status	Local IP Address	Remote IP Address	Uptime	

## 3.5.4 PPTP

This section is used to set the parameters of PPTP, a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.

#### General

General	PPTP Server	PPTP Client	Status	
▲ General Settings				
	Enal	ole User LED	OFF ?	

Item	Description	Default
Enable User LED	Click the toggle button to enable/disable the user LED. If User LED is	OFF
	enable here, it will have a higher priority.	



#### **PPTP Server**

General	PPTP Server PPTP Clie	nt Status		
∧ PPTP Server Setting	gs			
	Enable PPTP Server	ON OFF		
	Username		0	
	Password		?	
	Local IP			
	Start IP			
	End IP			
	Authentication	рар	v	
	Enable NAT	ON OFF		
	Expert Options	noaccomp nopcomp nodeflate nob	sdcomp n	
	Debug Enable	ON OFF		

Item	Description	Default
Enable PPTP Server	Click the toggle button to enable/disable the PPTP server.	OFF
Username	Enter the name for PPTP server.	Null
Password	Enter the password for PPTP server.	Null
Local IP	IP address of this PPTP network interface.	Null
Start IP	PPTP IP address leases will begin from the address specified in this field.	Null
End IP	PPTP IP address leases will end with the address specified in this field.	Null
Authentication	Select from "pap", "chap", "mschap v1", "mschap v2".	рар
Enable NAT	Click the toggle button to enable/disable NAT.	ON
Expert Options	Enter some other options of PPTP in this field. Each expression can be	Null
	separated by a ';'.	
Debug Enable	Click the toggle button to enable/disable debug.	OFF

#### ∧ Static Route

Index Remote Subnet Remote Subnet ... Client IP

+

Click + to add a static route for PPTP server. The maximum count is **20**.



▲ Static Route	
Index	1
Description	
Remote Subnet	
Remote Subnet Mask	
Client IP	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Description	Enter a description for this static route.	Null
Remote Subnet	Enter the remote subnet's address.	Null
Remote Subnet Mask	Enter the remote mask of subnet address.	Null
Client IP	Enter the client IP, empty means anywhere.	Null

### **PPTP Client**

General		PPTP Server	PPTP Clie	ent	Status		
	ent Settings	-	_	_	-		_
Index	Enable	Description	Server Address	Authentication	Remote Subnet	Remote Subnet	+

Click + to add a PPTP client. The maximum count is **5**.

▲ PPTP Client Settings		
Index	1	]
Enable	ON OFF	
Description		]
Server Address		]
Username		0
Password		0
Authentication	pap v	]



Enable NAT	ON OFF	
All Traffic via This Interface	ONOFF	
Remote Subnet		
Remote Subnet Mask		
Expert Options	noaccomp nopcomp nodeflate nobsdcomp r	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable the PPTP client.	OFF
Server Address	Enter the IP address or hostname of a PPTP server.	
Username	Enter the name for PPTP server	Null
Password	Enter the password for PPTP server	Null
Authentication	Select from "pap", "chap", "mschap v1", "mschap v2".	рар
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This	Click the toggle button to enable/disable this function.	OFF
Interface		
Remote Subnet	Enter the remote subnet address.	Null
Remote Subnet	Enter the remote subnet address mask.	Null
Mask		
Expert Options	Enter some other options of PPTP in this field. Each expression can be	Null
	separated by a ';'.	

#### Status

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

General	PPTP Se	rver	PPTP Client	Status		
∧ PPTP Ser	ver Status					
Index	Remote IP Address	Uptir	ne			
	ent Status					
Index	Description S	tatus	Local IP Address	Remote IP Address	Uptime	
0						 

# 3.5.5 L2TP

L2TP is a tunneling protocol used to support virtual private networks. It is more secure than PPTP because it encapsulates the transferred data twice, but it is slower and uses more CPU power.

### General

General	L2TP Server L2TP Client Status			
		_		
▲ General Settings				
	Enable User LED OFF ?			
Item	Description	Default		
Enable User LED	Click the toggle button to enable/disable the user LED. If User LED is OFF			
	enable here, it will have a higher priority.			

### L2TP Server

General	L2TP Server L2T	P Client	Status		
∧ L2TP Server Setti	пле			 	
A L21P Server Setti	Enable L2TP Serv		OFF		
	Enable L21P Serv	Ver	OFF		
	Usernar	me		?	
	Passwo	ord		?	
	Local	IP			
	Start	IP			
	End	IP			

Tunnel Secrets		
Authentication	pap v	
Port	1701	
Enable NAT	ON OFF	
Expert Options	noaccomp nopcomp nodeflate nobsdcomp n	
Debug Enable	ON OFF	

Item	Description	Default
Enable L2TP Server	Click the toggle button to enable/disable the L2TP server.	OFF
Username	Enter the name for L2TP server	Null
Password	Enter the password for L2TP server	Null
Local IP	IP address of this L2TP network interface.	Null
Start IP	L2TP IP address leases will begin from the address specified in this field.	Null
End IP	L2TP IP address leases will end with the address specified in this field.	Null
Tunnel Secrets	Enter the tunnel password.	Null
Authentication	Select from "pap", "chap", "mschap v1", "mschap v2".	рар
Port	Enter the port of this tunnel.	1701
Enable NAT	Click the toggle button to enable/disable NAT.	OFF
Expert Options	Enter some other options of L2TP in this field. Each expression can be	Null
	separated by a ';'.	
Debug Enable	Click the toggle button to enable/disable debug.	OFF

#### ▲ Static Route

Index Remote Subilet Remote Subilet Chent in	Index	Remote Subnet	Remote Subnet	Client IP
--	-------	---------------	---------------	-----------

			-	
~	lic	k		

Click + to add a static route for L2TP server. The maximum count is **20**.

▲ Static Route	
Index	1
Description	
Remote Subnet	
Remote Subnet Mask	
Client IP	()

+

**12** robustel



Item	Description	Default
Index	Indicate the ordinal of the list.	
Description	Enter a description for this L2TP server.	Null
Remote Subnet	Enter the remote subnet address	Null
Remote Subnet Mask	Enter the remote subnet address mask	Null
Client IP	Enter the Client IP	Null

## **L2TP Client**

General		L2TP Server	L2TP Clie	ent Status			
L2TP Clie	ent Settings						
Index	Enable	Description	Server Address	Authentication Remo	te Subnet Remote Sub	net	+

Click + to add a L2TP client. The maximum count is 5.

▲ L2TP Client Settings						
Index	1					
Enable	ON OFF					
Description						
Server Address						
Username		0				
Password		0				
Authentication	pap v					
Tunnel Secrets						
Enable NAT	ON OFF					
All Traffic via This Interface	ON					
Remote Subnet						
Remote Subnet Mask		]				
Expert Options	noaccomp nopcomp nodeflate nobsdcomp r					



Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable the PPTP client.	OFF
Description	Enter a description for this L2TP client.	Null
Server Address	Enter the IP address or hostname of a L2TP server.	Null
Username	Enter the name for PPTP server	Null
Password	Enter the password for PPTP server	Null
Authentication	Select from "pap", "chap", "mschap v1", "mschap v2".	рар
Tunnel Secrets	Enter the tunnel password.	Null
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This	Click the toggle button to enable/disable this function.	OFF
Interface		
Remote Subnet	Enter the remote subnet address.	Null
Remote Subnet Mask	Enter the remote subnet address mask.	Null
Expert Options	Enter some other options of PPTP in this field. Each expression can be	Null
	separated by a ';'.	

### Status

The status bar allows to view L2TP connection status. Click on one of the rows and details of its link connection will be displayed below the current row.

General	L2	TP Server		L2TP Client	Status			
	_	_		_		_	_	
L2TP Ser	ver Status							
Index	Remote IP Add	ress	Uptime					
		_	-		_	_	_	_
▲ L2TP Clie	ent Status							
Index	Description	Status	Loca	I IP Address	Remote IP Address	Uptime		

# 3.5.6 DMVPN

DMVPN is a routing technique we can use to build a VPN network with multiple sites without having to statically configure all devices. It is a hub and spoke network, where the spokes will be able to communicate with each other directly without having to go through the hub.



### DMVPN

DMVPN	Status	x509			
DMVPN Settings					
		Enable DMVPN	ONOFF		
		Description			
		DMVPN Type	Default	v	
		Link Binding	eth0	v	
		Hub Address		(?	
	_	_	_		
∧ GRE Settings					
	GRE L	ocal IP Address		?	

GRE Local IP Address	
GRE HUB IP Address	()
GRE Netmask	
GRE Secrets	
GRE MTU	1436

Item	Description	Default
Enable	Click the toggle button to enable/disable the DMVPN client.	OFF
Description	Enter a description for DMVPN client.	Null
DMVPN Type	Select DMVPN Type	Default
	Default: Single hub mode	
	Dual-hub: Dual hub mode	
Link Binding	Select a link binding with DMVPN	Null
Hub Address	Enter the DMVPN hub address. e.g. 172.16.8.198	Null
GRE Local IP Address	Enter local tunnel address, e.g. 182.16.0.1	Null
GRE HUB IP Address	Enter hub tunnel address, e.g. 182.16.0.100	Null
GRE Netmask	Enter tunnel netmask.	Null
GRE Secrets	Enter GRE tunnel secret key.	Null
GRE MTU	Enter the maximum transmission unit.	1436



#### ∧ IKE Settings

the octaingo		
ІКЕ Туре	[IKEv1	×
Negotiation Mode	Main	v
Local ID Type	Default	v
IKE Encryption Algorithm	3DES	v
IKE Authentication Algorithm	SHA1	v
IKE DH Group	DHgroup2	v
Authentication Type	PSK	v
PSK Secret		

∧ SA Settings					
SA Encryption Algorithm	3DES	V			
SA Authentication Algorithm	SHA1	v			
PFS Group	PFS(N/A)	v			

∧ Nhrp Settings	
Enable Zebra VTY	ON OFF
Enable NHRP VTY	ON OFF
Nhrp Holdtime(s)	7200

Item	Description	Default
ІКЕ Туре	Select IKE Type	IKEv1
Negotiation Mode	Select from "Main" and "aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are	Main
Local ID Type	correct. Select from "ID", "FQDN" and "User FQDN" for IKE negotiation. "Default" stands for "Router's extern IP". ID: Uses custom string as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this	Default



Item	Description	Default
	option is selected, type a name string with an sign "@" for the local	
	security gateway, e.g., test@robustel.com.	
IKE Encryption	Select from "DES", "3DES" and "AES128" to be used in IKE negotiation.	3DES
Algorithm	DES: Uses the DES algorithm in CBC mode and 56-bit key.	
	3DES: Uses the 3DES algorithm in CBC mode and 168-bit key.	
	AES128: Uses the AES algorithm in CBC mode and 128-bit key.	
IKE Authen	Select from "MD5" and "SHA1" to be used in IKE negotiation.	MD5
Algorithm	MD5: Uses HMAC-SHA1.	
	SHA1: Uses HMAC-MD5.	
IKE DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be	MODP1024_2
	used in key negotiation phase 1.	
	MODP768_1: Uses the 768-bit Diffie-Hellman group.	
	MODP1024_2: Uses the 1024-bit Diffie-Hellman group.	
	MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	
Authentication Type	Select Authentication Type	PSK
PSK Secrets	Enter PSK secret key.	Null
SA Encryption	Select the SA Encryption Algorithm from "DES", "3DES", "AES 128", "AES	3DES
Algorithm	192", "AES 256".	
SA Authentication	Select the SA Authentication Algorithm from "MD5", "SHA1", "SHA2 256",	SHA1
Algorithm	"SHA2 512".	
PFS Group	Select the PFS Group.	PFS(N/A)

# Status

The status bar allows to view DMVPN connection status.

DMVPN	Status	x509	
A DMVPN Status			
		Status	
		Uptime	



### X509

へ X509 Setti	ngs				0
		Local Certificate	Choose File No file chosen		
		Private Key	Choose File No file chosen	<u>1</u>	
		CA Certificate	Choose File No file chosen	<b>↑</b>	
∧ Local Certi	ificate	_	_	_	_
Index	File Name	File Size	Modification Time		

∧ Private Key	y .			
Index	File Name	File Size	Modification Time	

∧ CA Certific	ate			
Index	File Name	File Size	Modification Time	

x509						
Item	Description	Default				
X509 Settings						
Local Certificate	Click "Choose File" to locate Local 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.					
CA Certificate	Click "Choose File" to locate CA 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				

# 3.6 Services

# 3.6.1 Syslog

This section allows you to set the syslog parameters. The system log of the router can be saved in the local, also

supports to be sent to remote log server and specified application debugging. By default, the "Log to Remote" option is disabled.

1000000000	-
Svs	log
0,3	iug

<ul> <li>Syslog Settings</li> </ul>				
	Enable	ON OFF		
	Syslog Level	Debug	v	
	Save Position	RAM	v ?	
	Log to Remote			

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

Syslog			
∧ Syslog Settings			
	Enable	ON OFF	
	Syslog Level	Debug	v
	Save Position	RAM	v 🧿
	Log to Remote		
	Add Identifier		
	Remote IP Address		
	Remote Port	514	

Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from "Debug", "Info", "Notice", "Warning" or "Error", which from low to	Debug
	high. The lower level will output more syslog in details.	
Save Position	Select the save position from "RAM", "NVM" or "Console". The data will be	RAM
	cleared after reboot when choose "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 to allow router	ON
	sending 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
	serial number to syslog message which used for loading Syslog to RCMS.	
Remote IP Address	Enter the IP address of syslog server when enabling the "Log to Remote" option.	Null



Remote Port	Enter the port of syslog server when enabling the "Log to Remote" option.	514

# 3.6.2 Event

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

#### Event

Event	Notification	Query				
		_	_	_		
∧ General Setting	S					
	Signal Quality	/ Threshold	0		(?)	
	Temperature	e Threshold	0		0	
	Estimated Remaining Fla	sh Lifetime	20%-30%		v	

Item	Description	Default
Signal Quality Threshold	Set the threshold for signal quality. Device will generate a log event	0
	when the actual threshold is less than the specified threshold. 0 means	
	disable this option.	
Temperature Threshold	Set the threshold for temperature. Device will generate a log event	0
	when the actual threshold is less than the specified threshold. 0 means	
	disable this option.	
Estimate Remaining Flash	Set the estimate of EMMC life. Device will generate a log event when	20%-30%
Lifetime	the actual estimate is in the specified parameter range.	

### Notification

cation Group	Settings					
Description	Send SMS	Send Email	DO Control	Save to NVM		
		ation Group Settings escription Send SMS				

Click + button to add an Event parameters.



▲ General Settings			
	Index	1	]
	Description		]
	Send SMS	ON OFF	
	Send Email	ON OFF	
	DO Control	ON OFF	
	Save to NVM	ON OFF	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will	OFF
	send notification to the specified phone numbers via SMS if event occurs. Set the	
	related phone number in "3.21 Services > Email", and use ';'to separate each	
	number.	
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will	OFF
	send notification to the specified email box via Email if event occurs. Set the related	
	email address in "3.21 Services > Email".	
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the	OFF
	event router 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 event to	OFF
	nonvolatile memory.	

▲ Event Selection		?
System Startup	ON OFF	
System Reboot	ON OFF	
System Time Update	ON OFF	
Configuration Change	ON OFF	
Cellular Network Type Change	ON OFF	
Cellular Data Stats Clear	ON OFF	
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
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	ONOFF
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	ON OFF
DI 1 Counter Overflow	ON OFF
DI 2 ON	ON OFF
DI 2 OFF	ON OFF
DI 2 Counter Overflow	ON OFF
Excessive Temperature	ON OFF
Emmc Life Time Alert	ON OFF



Item	Description	Default
Event	Click the toggle button to enable this option to generate a log.	OFF

# Query

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

Event	Notification	Query				
▲ Event Details						
	Sa	ve Position	RAM	V		
		Filtering				
Mar 27 17:57:15 Mar 27 17:59:28 Mar 27 17:59:28 Mar 27 17:59:34 Mar 27 17:59:40 Mar 27 17:59:40 Mar 27 17:59:40 Mar 27 18:00:46 Mar 27 18:00:46 Mar 27 18:00:46 Mar 27 18:06:25 Mar 27 18:06:25 Mar 27 18:09:28 Mar 27 18:12:31 Mar 27 18:15:34 Mar 27 18:15:34	<pre>, switch link, from WWAN1 , switch link, from WWAN2 , LAN port link down, eth , LAN port link up, eth1 , LAN port link up, eth1 , LAN port link up, eth0 , LAN port link up, eth1 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN1 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN2 , switch link, from WWAN1 , switch link, from WWAN1</pre>	to WWAN1 O 1 1 to WWAN2 to WWAN2 to WWAN1 to WWAN2 to WWAN1 to WWAN2 to WWAN1 to WWAN2 to WWAN1			Clear	Refresh
Item	Description					Default
Save Position	RAM: Rand	ts' save posi lom-access r ·Volatile Me	•	NVM".		RAM
Filtering		• •	•	ls set by users. Click the follow box. Use "&" to		Null

# 3.6.3 NTP

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

more than one filter message, such as message1&message2.



#### NTP

NTP	Status					
∧ Timezone Settings	5					
	Time 2	Zone Asia-Sh	ianghai		v	
Item	Description					Default
Time Zone	Click the drop of	down list to sele	ect the time zo	one you are	in.	Asia-Shanghai

∧ NTP Client Settings	
Enable	ON OFF
Primary NTP Server	pool.ntp.org
Secondary NTP Server	
NTP Update Interval	0

Item	Description	Default
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
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) synchronizing the NTP client time with the	0
	NTP server's. Minutes wait for next update, and 0 means update only	
	once.	

∧ NTP Server Settings			
	Enable	ON OFF	

Item	Description	Default
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

#### Status

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

RobustOS Pro S	<b>Ø</b> robustel			
NTP	Status			
▲ Time				
		System Time	2022-05-07 16:27:05	
		PC Time	2022-05-07 16:27:07 Sync	
	las	t Undate Time	2022-05-07 08:48:25	

# 3.6.4 SMS

This section allows you to set SMS parameters. Device supports SMS management, and user can control and configure their devices by sending SMS. For more details about SMS control, refer to **4.1.2 SMS Remote Control**.

### SMS

SMS	SMS Testing				
∧ SMS Managem	ent Settings				?
	Enable	ON OFF			
	Authentication Type	Password	v ?	1	
	Phone Number		+	?	

Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option.	ON
	Note: 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 WEB manager for	
	authentication. For example, the format of the SMS should be "username:	
	password; cmd1; cmd2;"	
	Note: Set the WEB manager password in System > User Management section.	
	Phonenum: Use the Phone number for authentication, and user should set the	
	Phone Number that is allowed for SMS management. The format of the SMS	
	should be "cmd1; cmd2;"	
	Both: Use both the "Password" and "Phonenum" for authentication. User	
	should set the Phone Number that is allowed for SMS management. The	
	format of the SMS should be "username: password; cmd1; cmd2;"	
Phone Number	Set the phone number used for SMS management, and click $+$ to add new	Null
	phone number.	



**Note:** It can be null when choose "Password" as the authentication type.

### **SMS** Testing

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

SMS	SMS Testing			
∧ SMS Testing				
Phone Number				
		]		
Message				
Result				
				Send

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

# 3.6.5 Email

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

Email

▲ Email Settings			
	Enable	ON OFF	1a1
	Enable TLS/SSL	ON OFF	
	Enable STARTTLS	ON OFF	
	Outgoing Server		
	Server Port	25	
	Timeout	10	0
	Auth Login	ON OFF	
	Username		
	Password		
	From		
	Subject		

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

# 3.6.6 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, allows you whose ISP does not assign them a static IP address to use a domain

10 robustel

name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP. The service provider defaults to "DynDNS", as shown below.

### DDNS

DDNS		Status			
A DDNS Set	ttings				
Index	Enable	Service Provider	Hostname	Link Binding	+

Click<sup>+</sup> to add a new Dynamic Domain Name Server.

∧ DDNS Settings		
Index	1	
Enable	ON OFF	
Service Provider	DynDNS v	
Hostname		
Username		
Password	••••••	
Link Binding	wwan v	
Max Tries	3	0

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

∧ DDNS Settings	
Index	1
Enable	ON OFF
Service Provider	Custom v
URL	
Max Tries	3



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

### Status

The status bar allows to view DDNS connection status.

DDNS	Status		
∧ DDNS Status			
Index	Status	Last Update Time	

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

# 3.6.7 VRRP

This section allows you to set the VRRP parameters. VRRP stands for Virtual Router Redundancy Protocol, is a standard for device redundancy and failover that creates a virtual router with a floating IP address.



# **VRRP Settings**

∧ VRRP Settings	
Enable	ON OFF
Interface	br_lan v
Group ID	1
Priority	100
Interval	1
Virtual IP Address	

Item	Description	Default
Enable	Click the toggle button to enable/disable the VRRP option.	OFF
Interface	Selects which interface VRRP will operate on.	
Group ID	The Virtual Router Identifier. Routers with identical IDs will be grouped in the same VRRP cluster.	1
Priority	VRRP priority of the virtual router. Higher values equal higher priority.	100
Interval	Interval value in second, must be the same for all routing platforms in the VRRP group.	1
Virtual IP Address	Virtual IP address for the router's VRRP cluster.	Null

# **Ping Detection Settings**

∧ Ping Detection Settings			
Enabl	le	ON OFF	
Serve	er	8.8.8.8	
Interva	al	300	0

Item	Item Description	
Enable	Click the toggle button to enable/disable the option.	OFF
Server	The ping detection sever address.	8.8.8.8
Interval	Interval value for ping detection in second.	300



# 3.6.8 SSH

#### Device supports SSH password access and secret-key access.

SSH		
∧ SSH Settings		
	Enable	ON OFF
	Port	22
	Disable Password Logins	ON OFF
	Authorized Keys	None

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

# 3.6.9 GPS

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

#### GPS

GPS	Status	Мар			
∧ General Settings					
	1	Enable GPS	ON OFF		
	Sync	c GPS Time	ONOFF		



∧ RS232 Report Settings	1			
	Report to RS232	ONOFF		0.5
	Report GGA Sentence	ONOFF		
	Report VTG Sentence	ONOFF		
	Report RMC Sentence	ON		
	Report GSV Sentence	ONOFF		
∧ GPS Servers				
Index Enable	Protocol Local Address	Local Port Server Address	Server Port	+

Click<sup>+</sup> to add a new GPS Server. The maximum count is **5**.

∧ Server Settings	
Index	1
Enable	ON OFF
Protocol	TCP Client v
Server Address	
Server Port	
Send GGA Sentence	ON OFF
Send VTG Sentence	ONOFF
Send RMC Sentence	ON OFF
Send GSV Sentence	ON OFF

Item	Description	Default
Index	Indicate the ordinal of the list.	
Enable	Click the toggle button to enable/disable the server.	ON
Protocol	Select from "TCP Client", "TCP Server", "UDP".	TCP Client
Server Address	Server or local IP address.	Null
Server 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



Itom	Description			Default
	Self-define GPSID Prefix		0	
	Add SN as GPSID	ON OFF ?		
Advanced Setting	S			

Item	Description	Default
Add SN as GPSID	Click the toggle button to enable/disable this option.	OFF
Self-define GPSID Prefix	Self-define GPSIS Prefix, four upper case.	Null

### Status

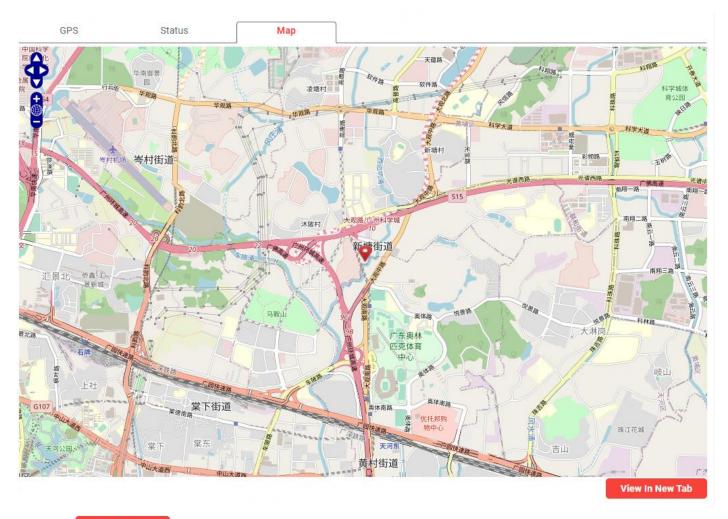
GPS	Status Map		
▲ GPS Status			
	Status	Standalone Fixed	
	UTC Time	2022-05-18 03:48:25	
	Last Fixed Time	2022-05-18 03:39:05 UTC	
	Satellites In Use	3	
	Satellites In View	GPS(10), Galileo(0), BeiDou(0), GLONASS(0)	
	Latitude	23.152445	
	Longitude	113.400612	
	Altitude	60.80 m	
	Speed	0.00 m/s	

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



### Мар

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 on the device and enable GPS in the GPS page.



Click the View In New Tab button to view in a new tab.



# 3.6.10 RCMS

This section allows you to set the RCMS parameters. Robustel Cloud Manager Service (RCMS) is a modular IoT cloud software platform compatible with all Robustel products.

### RCMS

RCMS	Event Selection Status	
∧ General Setting	S	
	Enable RCMS	ON OFF
	Enable RobustLink	ON OFF
	Enable RobustVPN	ON OFF
	Paho log detail enable	ON OFF
	RCMS Environment	RCMS Cloud International

Item	Description	Default
Enable RCMS	Click the toggle button to enable/disable this option.	OFF
Enable RobustLink	Click the toggle button to enable/disable this option.	OFF
Enable RobustVPN	Click the toggle button to enable/disable this option.	OFF
Paho log detail enable	Click the toggle button to enable/disable this option.	OFF
RCMS Environment	Select RCMS Environment	RCMS Cloud International
RCMS URL or IP	Enter IP Address or URL of RCMS server.	rcms-cloud.robust el.net
Port	Enter the Port of RCMS.	443

∧ Data Management				
	KeepAlive	600	v ?	
Dynamic Repo	ort Capture	60min	v ?	
Dynamic Rep	ort Upload	60min	v ?	
GPS Reportin	ng Settings	On GPS co-ordinate change	v ?	
GPS Distance	Threshold	20	?	



Item	Description	Default
KeepAlive	KeepAlive determines how long your device checks in with RCMS. A shorter KeepAlive will update RCMS more frequently but consume more data.	600
Dynamic Report Capture	Select the capture period of dynamic data is logged in the device	60min
Dynamic Report Upload	Select the upload period of dynamic data is update in the device	60min
GPS Reporting Settings	<ul> <li>Select GPS Reporting way:</li> <li>On GPS co-ordinate change - Report when GPS is updated</li> <li>Only with Dynamic Report - Collect and report in sync with the Data Collection Interval and Data Reporting Frequency</li> </ul>	On GPS co-ordinate change
GPS Distance Threshold	GPS data will be updated when the current position exceeds this value; Unit:meters Valid Range:10-10000	20

▲ Ping Settings			?
Enable Ping	ON OFF		
Primary Server	8.8.8.8		
Ping Timeout	5	?	
Ping Count	3	0	

Item	Description	Default
Enable Ping	Click the toggle button to enable/disable this option.	OFF
Primary Server	Enter the ping server.	8.8.8.8
Ping Timeout	Enter the time of waiting for a ping response. Unit: seconds	5
Ping Count	Enter the number of pings conducted to calculate average.	3



### **Event Selection**

RCMS	Event Selection Status		
Event Selection			
	System Startup	ON OFF	
	System Time Update	ON OFF	
	Cellular Network Type Change	ON OFF	
	Cellular Data Stats Clear	ON OFF	
	Cellular Data Traffic Overflow	ON OFF	
	Poor Signal Quality	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	ON OFF	
	DI 1 Counter Overflow	ON OFF	
	DI 2 ON	ON OFF	
	DI 2 OFF	ON OFF	
	DI 2 Counter Overflow	ON OFF	
	Excessive Temperature	ONOFF	



#### Status

RCMS Event Selection	Status		
▲ Connection Status			
R	obustLink Status Connected		
RobustLink	Last Connected 2023-05-30 13:54:59		
R	bustVPN Status		
RobustVPN	Last Connected Never		
Robi	istVPN Virtual IP		
RobustVPN	SubNet Address		
Item	Description		
RobustLink Status	Show the status of RobustLink		
RobustelLink Last Connected	Show the last connected times of RobustLink		
RobustVPN Status	Show the status of RobustVPN		
RobustVPN Last Connected Show the last connected times of RobustVPN			
RobustVPN Virtual IP	N Virtual IP Show the virtual IP of RobustVPN		
RobustVPN SubNet Address Show the subnet address of RobustVPN			

# 3.6.11 Voice call (Supported in EV8100)

This section allows you to set the Voice Call parameters. This allows you to customize and configure parameters related to voice calls, including the SIP protocol and VoLTE protocol.

### **Basic Setup**

▲ General Settings		
Enable Voice Call	ON OFF	
Log Level	Info v 🤇	e
Outgoing Calls Mode	SIP-First v	
Dial Timeout	6000	

Item	Description	Default
Enable Voice Call	Click the toggle button to enable/disable this option.	ON
Log Level	Select from "Trace", "Debug", "Info", "Warning", "Error", "Critical" or "Off"	Info



Outgoing Calls Mode	Select from "Block", "SIP-First", "SIP-Only" or "LTE-Only"	SIP-First
Dial Timeout	Unit: milliseconds.	6000

∧ Auto-Dialled			
Enable Auto-Di	alled ON OFF ?		
Auto-Dialled Nu	mber	(7)	
	Time 5000	(?)	

Item	Description	Default
Enable Auto-Dialled	Click the toggle button to enable/disable this option.	OFF
Auto-Dialled Number	The phone number to be called when Auto-Dialled is enabled.	
Time	The time in milliseconds for the call to be made when the user does	5000
	not dial after off-hooking.	5000

### SIP

∧ SIP Basic		
SIP Phone Number		
SIP Account		
Password		
SIP Server		0
Transport Protocol	UDP v	0
SIP Server Port	5060	3
Local Port	5060	0
Public Address		0
Enable SIP registration	ON OFF	
Registration Expire	300	
DTMF transmission	InBand v	

Item	Description	Default
SIP Phone Number	Enter the phone numberto identify the device uniquely for calls.	
SIP Account	Enter the registration username for the SIP account.	



Password	Enter the registration password.	
SIP Server	Enter the SIP Proxy server URL.	
Transport Portocol	Select the SIP signaling method. Select from "UDP", "TCP", "TLS" or "UDP+TCP".	UDP
SIP Server Port	Set the server port.	5060
Local Port	Set the local port.	5060
Public Address	Enter the public address.	
Enable SIP registration	Click the toggle button to enable/disable the registration by SIP calls.	ON
Registration Expire	Enter the re-registration timeout.	300
DTMF transmission	Set the DTMF transmission method. Select from "InBand", "RTP RFC2833" or "SIP INFO".	InBand

# **SIP Certificate**

∧ SIP Keys Settings				
CA Certif	îcate	选择文件 未选择任何文件	<u>^</u>	
Device Certif	licate	选择文件 未选择任何文件	<u>1</u>	
Device Private	e Key	选择文件 未选择任何文件	<u>*</u>	

∧ CA Certific	cate			
Index	File Name	File Size	Modification Time	

FI	le Name	File Size	Modification Time	

Idex	File Name	File Size	Modification Time	
------	-----------	-----------	-------------------	--



### VoLTE

∧ VoLTE Basic				
	DTMF transmission	InBand InBand RTP RFC2833	v	
Item	Description			Default
DTMF transmission	Select from "InBand	d" or "RTP RFC2833".		InBand

# Telephony

▲ Dial Tone		
Frequency 1	350	] ⑦
Frequency 2	440	] ⑦
Tone On Period	0	] 🧿
Tone Off Period	0	] 7

Item	Description	Default
Frequency 1	The frequency(Hz) of the first dial tone, 0 for no signal output.	350
Frequency 2	The frequency(Hz) of the second dial tone, 0 for no signal output.	440
Tone On Period	The duration(ms) of the dial tone active, 0 for disable dial tone only as off_duration > 0.	0
Tone Off Period	The duration(ms) of the dial tone inactive, 0 for continuous.	0

∧ Ringback Tone			
Frequency 1	480	0	
Frequency 2	440	?	
Tone On Period	2000	?	
Tone Off Period	4000	?	
Ringtone Cycle Gap	0	0	

Item	Description	Default
Frequency 1	The frequency(Hz) of the first ringback tone, 0 for no signal output.	480
Frequency 2	The frequency(Hz) of the second ringback tone, 0 for no signal output.	440

# 10 robustel

Tone On Period	The duration(ms) of the ringback tone active, 0 for disable ringback tone only as off_duration > 0.	2000
Tone Off Period	The duration(ms) of the ringback tone inactive, 0 for continuous.	4000
Ringtone Cycle Gap	The duration(ms) of the gap.	0

▲ Busy Tone		
Frequency 1	480	?
Frequency 2	620	?
Tone On Period	500	?
Tone Off Period	500	?

Item	Description	Default
Frequency 1	The frequency(Hz) of the first busy tone, 0 for no signal output.	480
Frequency 2	The frequency(Hz) of the second busy tone, 0 for no signal output.	620
Tone On Period	The duration(ms) of the busy tone active, 0 for disable busy tone only as off_duration > 0.	500
Tone Off Period	The duration(ms) of the busy tone inactive, 0 for continuous.	500

∧ Ringing		
Ring Frequency	25Hz v	
Ring Voltage(rms)	55V v	
Tone On Period	2000	0
Tone Off Period	4000	0
Ringtone Cycle Gap	0	] 🧿

Item	Description	Default
Ring Frequency	The frequency(Hz) of ringing. Select from "16Hz", "25Hz" or "50Hz".	25Hz
Ring Voltage(rms)	Select from"35V","45V","50V" or "55V".	55V
Tone On Period	The duration(ms) of the busy tone active.	2000
Tone Off Period	The duration(ms) of the busy tone inactive, 0 for continuous.	4000
Ringtone Cycle Gap	The duration(ms) of the gap.	0



∧ Other		
Line Impedance	600Ω  1000nF v	
RX Gain(dB)	-9	
TX Gain(dB)	-9	
Enable Polarity Reversal	ON OFF	

Item	Description	Default
Line Impendance	Select from "600 $\Omega$ ", "270 $\Omega$ +750 $\Omega$   150nF", "370 $\Omega$ +620 $\Omega$	
	310nF","220 $\Omega$ +820 $\Omega$   120nF", "600 $\Omega$   1000nF","200 $\Omega$ +680 $\Omega$	<b>600</b> Ω
	100nF" or "220 $\Omega$ +820 $\Omega$   115nF".	
RX Gain(dB)	Enter the RX Gain.	-9
TX Gain(dB)	Enter the TX Gain.	-9
Enable Polarity	Click the toggle button to enable/disable this option.	OFF
Reversal	OFF	

#### Status

This page allows you to view the status of SIP or VoLTE.

▲ Running Status		
Status	Running	
SIP Register	Account_Empty	
VoLTE Status		
Version	1.0.0 (4b39a46f)	

# 3.6.12 SNMP

This section allows you to set the SNMP parameters. Simple Network Management Protocol is a network management protocol used for collecting information and configuring network devices.



# **SNMP** Agent

SNMP Agent	SNMP Trap	VIBS			
∧ SNMP Agent Setti	ngs				
	Enable SNMP Age	nt	ONOFF		
	Pc	ort	161		
	OEM Enab	le	ONOFF		
	OEM Enterpri	se			
. 51 <sup>1</sup>	OEM Platfor	m			
	Versio	on	SNMPv3	v	
	Location In	fo			
	Contact In	fo			
	System Nan	ne			
	Authentication Algorith	im	MD5	v	
	Privacy Algorith	im	DES	v	

Item	Description	Default
Enable SNMP Agent	Click the toggle button to enable/disable this option.	OFF
Port	SNMP service's port.	161
OEM Enable	Click the toggle button to enable/disable this option.	OFF
OEM Enterprise	OEM enterprise information.	Null
OEM Platform	OEM platform information.	Null
Version	The SNMP version, select from "SNMPv3" or "SNMPv1v2v3".	SNMPv3
Location Info	System location information.	Null
Contact Info	System contact information.	Null
System Name	System name.	Null
Readonly Community Name	Access mode for current community.	Null
Readwrite	Access mode for current community.	NULL
Community Name		Null
Authentication	Select from "MD5", "SHA".	
Algorithm	MD5	
Privacy Algorithm	Select from "DES", "AES". DES	

Enable SNMP Trap ON OFF

SNMP Trap Setti	nas		
SNMP Agent	SNMP Trap	MIBS	

	Version	SNMPv3 v		
	Receiver Address			
	Receiver Port	162		
<ul> <li>SNMPv3 Authentication</li> </ul>				
	Username		]	
	Authentication Algorithm	MD5 v	]	
	Authentication Password			
	Privacy Algorithm	DES v	]	
	Privacy Password	[	Ĩ	

SNMP Trap Rules are alerts that trigger when certain user-specified events occur. When the trigger event happens,

Item	Description	Default
Enable SNMP Agent	Click the toggle button to enable/disable this option.	OFF
Receiver Address	Host name or IP address to transfer SNMP traffic to.	Null
Receiver Port	Trap host's port number.	162
User name	The user name access to SNMP.	Null
Authentication Algorithm	Select from "MD5", "SHA".	MD5
Authentication Password	Enter the authentication password.	Null
Privacy Algorithm	Select from "DES", "AES".	DES
Privacy Password	Enter the privacy password.	Null

Click the toggle button the enable or disable the related event.

the trap will notify known SNMP hosts.

**SNMP** Trap

# 10 robustel

?

▲ Event Selection	
System Startup	ONOFF
System Reboot	ONOFF
System Time Update	ONOFF
Configuration Change	ONOFF
Cellular Network Type Change	ONOFF
Cellular Data Stats Clear	ONOFF
Cellular Data Traffic Overflow	ONOFF
Poor Signal Quality	ONOFF
Link Switching	ONOFF
WAN Up	ONOFF
WAN Down	ONOFF
WWAN Up	ONOFF
WWAN Down	ONOFF
IPSec Connection Up	ONOFF
IPSec Connection Down	ONOFF
OpenVPN Connection Up	ONOFF
OpenVPN Connection Down	ONOFF
LAN Port Link Up	ONOFF
LAN Port Link Down	ONOFF



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	ON OFF
DI 1 Counter Overflow	ON OFF
DI 2 ON	ON OFF
DI 2 OFF	ON OFF
DI 2 Counter Overflow	ON OFF
Excessive Temperature	ON OFF

### MIBS

MIB stands for Management Information Base, a MIB contains the variables that the managed device maintains and can be queried or set by the agent. The MIB defines the attributes of the managed device, including the name, status, access rights, and data type.

SNMP Agent	SNMP Trap	MIBS					
∧ SNMP MIBS							
	S	SNMP MIBS	Generate				
	s	SNMP MIBS	Download				
Item	Descripti	ion					Default
MIBS	Click Ge	nerate to g	generate and clic	Download	to download t	he device's	
	MIB file.						



# 3.6.13 Captive Portal

### **Captive Portal**

This section allows you to modify the parameters of Captive Portal.

Captive Portal is a web-based authentication setup that serves as a "login" page presented to users by network operators or devices before they can access the internet.

Captive Portal	Status		
∧ General Settings			
	Enable	ON OFF	
	Debug Enable	ON OFF	
	WAN Interface	wlan0 v	
	LAN Interface	VAP1 v	
	Platform	Custom v	
	Primary Radius Server		
	Secondary Radius Server		
	Authentication Port	1812	
	Accounting Port	1813	
	Radius Share Secret		0
	WWW Save Position	System v	
	Client Network	192.168.137.0	
	Client Netmask	255.255.255.0	
	Redirect URL		0

Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
Debug Enable	Click the toggle button to enable/disable debug mode. When debug	
	mode enabled, the captive portal running log will be displayed in	OFF
	syslog.	
WAN Interface	Select WAN Interface.	wlan0
LAN Interface	Select LAN Interface.	VAP1
Platform	Select a radius platform.	Custom



Primary Radius Server	Enter the Primary Radius Server.	Null
Secondary Radius Server	Enter the Secondary Radius Server.	Null
Authentication Port	Enter the Radius Server 's Authentication Port.	1812
Accounting Port	Enter the Radius Server 's Accounting Port.	1813
Radius Share Secret	Enter the Radius Share Secret, it is a security setting used in RADIUS servers and clients to establish a secure communication channel. Usually in 8 - 128 characters.	
WWW Save Position	Select the WWW Save Position, the WWW information will save in the specific position	System
Client Network	Enter the Client Network. If the client IP address is within the range, the RADIUS server assumes that the request comes from a trusted client and proceeds with the authentication process.	192.168.137.0
Client Netmask	Enter the Client Netmask. If the client Netmask is within the range, the RADIUS server assumes that the request comes from a trusted client and proceeds with the authentication process.	255.255.255.0
Redirect URL	Enter the Redirect URL. It will be redirected to this URL after authentication success	Null

UAM (Universal Access Method) is a technology used for user authentication and authorization in Wi-Fi networks. Here is the parameter settings for Captive Portal.

∧ UAM Settings	
UAM Secret	
UAMFORMAT	?
UAMPORT	3990
UAMUIPORT	4990
UAMDOMAINS Enable	ON OFF

Item	Description	Default
UAM Secret	Enter the UAM Secret. UAM Secret is a security key used in the	
	authentication process between a wireless access point and a RADIUS	Null
	server. Usually use 5 - 128 characters.	
UAM Format	UAM Format refers to the format of the web page that is presented	Null
	to users for authentication in UAM systems.	Null
UAM Port	The UAM Port is used to send authentication requests and responses	3990
	between the device and the authentication server.	3990
UAM UI Port	UAM UI Port is used to serve the authentication web page to the	4990
	user's browser, and to receive the user's authentication credentials.	4990
UAM Domains Enable	UAM Domain refers to the domain or subdomain that is used to host	
	the login or captive portal page for a user authentication and	OFF
	management system.	



Click the toggle button to enable/disable this option.

### Status

The status bar allows you to view Captive Portal associated stations status.

Captive Port	tal Stat	tus				
<ul> <li>Associate</li> </ul>	d Stations					
Index	MAC Address	IP Address	Inter State	Auth State	Login Name	
		ii Address	inter office		Login Hume	

# 3.6.14 Web Server

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

o1 o-w'				
General Settings				
	HTTP Port	80	(?	
	HTTPS Port	443	(?	
	HTTPS CA Certificate	None	v	
	HTTPS Private Keys	None	Y	

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

HTTPS CA Certificate	Select one once the certification is imported, see 3.7.2 Certificate Manager	
HTTPS Private Keys	Select one once the certification is imported, see 3.7.2 Certificate Manager	

# 3.6.15 Advanced

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

System	Reboot		
▲ System Settings			
а. 19 Ш.	Device Name	router	0
	User LED Type	None	v 🕜

Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid	router
	characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	
User LED Type	Specify the display type of your USR LED. Select from "None", "OpenVPN" or	None
	"IPsec".	
	None: Meaningless indication, and the LED is off	
	NET: show the network status	
	SIM:show the sim status.	
	OpenVPN: USR indicator showing the OpenVPN status	
	IPsec: USR indicator showing the IPsec status	
	RCMS: show the connect status of RCMS	

riodic Reboot S	Settings			
	Periodic Reboot	0	?	
	Daily Reboot Time		0	

Periodic Reboot Settings			
Item	Description	Default	
Periodic Reboot	Set the reboot period of the router. 0 means disable.	0	
Daily Reboot Time	Set the daily reboot time of the router. You should follow the format as HH:	Null	



	MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means	
	disable.	
Reboot When No	Click the toggle button to enable/disable this option.	OFF
Link Is Available		

# 3.7 System

# 3.7.1 Debug

#### 3.6.1 Debug

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

Syslog Details				
	Log Level	Debug	v	
	Filtering		(?)	
<pre>ppr 26 11:48:03 Router NetworkMan andle: 0xaaafb692780 upr 26 11:48:03 Router NetworkMan cc 1 -w 13 8.8.8' upr 26 11:48:04 Router NetworkMan upr 26 11:48:06 Router ModemManag /sys/devices/platform/soc@0/3080 upr 26 11:48:06 Router ModemManag /sys/devices/platform/soc@0/3080 upr 26 11:48:06 Router ModemManag /sys/devices/platform/soc@0/3080 upr 26 11:48:06 Router ModemManag /sys/devices/platform/soc@0/3080 upr 26 11:48:06 Router ModemManag upr 26 11:48:06 Router ModemManag /sys/devices/platform/soc@0/3080</pre>	ager[1738]: (info) ager[6427]: PING 8.8. ager[6427]: 64 bytes ager[6427]: 8.8.4 ager[6427]: 1 packet: ager[6427]: 1 the ager[1738]: (info) ager[1738]: (info) ager[1738]: (info) continuous success er[6373]: (info) [b: 0000. bus/30b50000.et] er[6373]: (info) [b: cono. bus/30b60000.et] er[6373]: (info) [b: cono. bus/30b60000.et]	<pre>[1682480883.9863] connectiv. 8.8 (8.8.8.8) from 172.16. from 8.8.8.8: icmp_seq=1 t 8.8 ping statistics s transmitted, 1 received, ' avg/max/mdev = 9.247/9.247/' [1682480884.0022] connectiv [1682480884.0023] device (e count: 13, continuous fail' ase-manager] couldn't check hernet': not supported by an ase-manager] couldn't check</pre>	ity: (eth0, IPv4, req 55) runn: 19.71 eth0: 56(84) bytes of o tl=113 time=9.25 ms 0% packet loss, time 0ms 9.247/0.000 ms ity: (eth0, IPv4, req 55) concl th0): concheck_update_state[] me count: 0 support for device nc1:0001:1': not supported by support for device ny plugin support for device ny plugin	ing '/bin/ping —I eth0 data. neck: primary ping IPv4], state: FULL, old

Item	Description	Default				
Log Level	Select from "Debug", "Info", "Notice", "Warn", "Error" which from low to high.	Debug				
	The lower level will output more syslog in detail.					
Filtering	Enter the filtering message based on the keywords. Use "&" to separate more	Null				
	than one filter message, such as "keyword1&keyword2".					
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 follow box. If selecting "manual refresh", you should click the refresh					
	button to refresh the syslog.					
Clear	Click the button to clear the syslog.					

Refresh	Click the button to refresh the syslog.	

∧ Syslog Journal File		
	System Journal File Generate	
	System Journal File Download	
Item	Description	Default
Item System Journal File	Description         Click Generate to generate and click Download to download the system	Default 

∧ System Diagnostic Data		
S	System Diagnostic Data Generate	
s	System Diagnostic Data Download	
Item	Description	Default
System Diagnostic Data	Click Generate to generate and click Download to download the system	
	diagnostic data.	

# 3.7.2 Certificate Manager

This section allows you to mange all of certificates here. If you want to manage a certificate for your custom application, you can manage it through Other tab.

### OpenVPN

OpenVPN	IPsec	SSH	Web	System Certificate	Other	
X509 Settings						?
		Root CA	Choose File No file choose	sen 🚺		
		Certificate File	Choose File No file choose	sen 🚺		
		Private Key	Choose File No file choose	sen 🚺		
		DH	Choose File No file choose	sen 🚺		
		TLS-Auth Key	Choose File No file choose	sen 🚺		
		CRL	Choose File No file choose	sen 🚹		

Ørobustel



TLS-Auth Key	Choose File No file chosen
CRL	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen
Pre-Share Key	Choose File No file chosen
Ovpn Config	Choose File No file chosen

Item	Description	Default
Root CA	Click on Choose File to locate the root ca file, and then click on $\triangle$ to	
	import this file into your device.	
Certificate File	Click on Choose File to locate the certificate file, and then click on 🗅 to	
	import this file into your device.	
Private Key	Click on Choose File to locate the Private Key file, and then click on 🗅 to	
	import this file into your device.	
DH	Click on Choose File to locate the DH file, and then click on 🗅 to import	
	this file into your device.	
TLS-Auth Key	Click on Choose File to locate the TLS-Auth Key file, and then click on 🗅 to	
	import this file into your device.	
CRL	Click on Choose File to locate the CRL file, and then click on 🗅 to import	
	this file into your device.	
PKCS#12 Certificate	Click on Choose File to locate the PKCS#12 Certificate file, and then click on	
	1 to import this file into your device.	
Pre-Share Key	Click on Choose File to locate the Pre-Share Key file, and then click on 1	
	to import this file into your device.	
Ovpn Config	Click on Choose File to locate the Ovpn Configy file, and then click on 1	
	to import this file into your device.	



### IPsec

OpenVPN	IPsec	SSH	Web	System Certificate	Other	
∧ X509 Settings						?
	Local	Certificate	Choose File No file chose	n 🗘		
	Remote	Certificate	Choose File No file chose	n 📩		
	F	Private Key	Choose File No file chose	n 📩		
	CA	Certificate	Choose File No file chose	n 📩		
	PKCS#12	Certificate	Choose File No file chose	n 🗘		
Itom	Description					ofault

Item	Description	Default
Local Certificate	Click on Choose File to locate the Local Certificate file, and then click on $ an$	
	to import this file into your device.	
Remote Certificate	Click on Choose File to locate the Remote Certificate file, and then click on	
	ᄎ to import this file into your device.	
Private Key	Click on Choose File to locate the Private Key file, and then click on $  begin{array}{c}  begin{array}{c} $	
	import this file into your device.	
CA Certificate	Click on Choose File to locate the CA Certificate file, and then click on $ alpha$	
	to import this file into your device.	
PKCS#12 Certificate	Click on Choose File to locate the PKCS#12 Certificate file, and then click on	
	1 to import this file into your device.	



### SSH

OpenVPN	IPsec	SSH	Web	System Certificate	Other	
▲ Authorized Keys Se	ttings					?
	Auth	orized Keys	hoose File No file chose	n 🗘		
▲ Authorized Keys						
Index Fil	e Name	File Size	Modification T	ime		
Item	Descriptio	n				Default
Authorized Keys	Click on	Choose File to loca	ite the Authorized	Keys file, and then c	lick on 🗘	

to import this file into your device.

### Web

OpenVPN	IPsec	SSH	Web	System Certificate	Other	
HTTPS Certified	icate Settings					?
		HTTPS Private Key	Choose File	]No file <mark>chosen</mark>	<u>1</u>	
		HTTPS CA Certificate	Choose File	] No file chosen	<b>_</b>	
HTTPS Privat	e Key					
Index	File Name	File Size		Modification Time		
1 <u>2</u>						

<b>^</b> HTTPS CA	Certificate			
Index	File Name	File Size	Modification Time	

Item	Description	Default
HTTPS Private Key	Click on $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	
	to import this file into your device.	
HTTPS CA Certificate	Click on Choose File to locate the Certificate file, and then click on 🗅 to	
	import this file into your device.	



### System Certificate

OpenVPN	IPsec	SSH	Web	System Certificate	Other
∧ Certificate Import					
		File	noose File No file cho	osen Import	
Item	Descriptio	on			Default
File	Click on	Choose File to loca	te the System ce	ertificate file, and then c	lick on
	📩 to im	port this file into y	our device.		

### Other

OpenVPN	IPsec	SSH	Web	System Certificate	Other	
へ Other Certificate	Settings					?
	Othe	er Certificate	hoose File No file o	chosen		

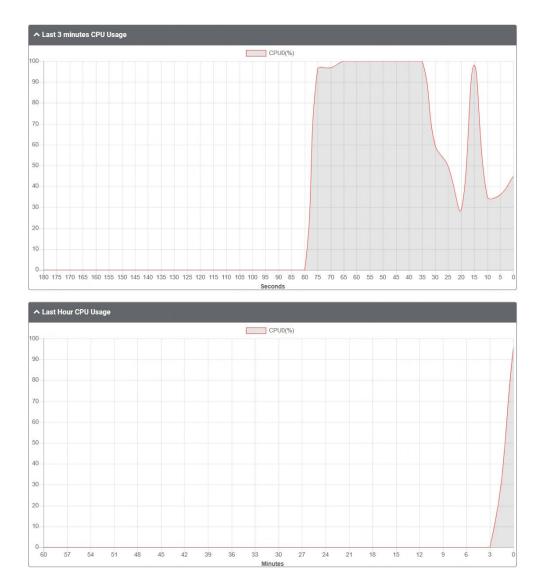
Item	Description	Default
Other Certificate	Click on Choose File to locate the Other Certificate file, and then click on	
	1 to import this file into your device.	

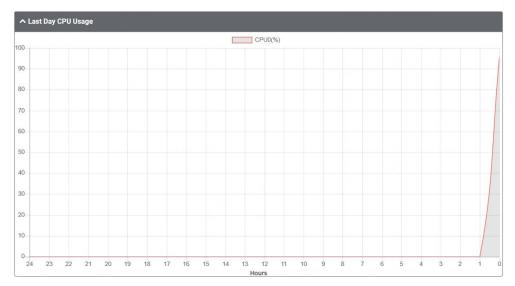
# 3.7.3 Resource Graph

This section allows you to view the system resource such as CPU usage or cellular signal strength in recent 3 minutes, last hour or last day.



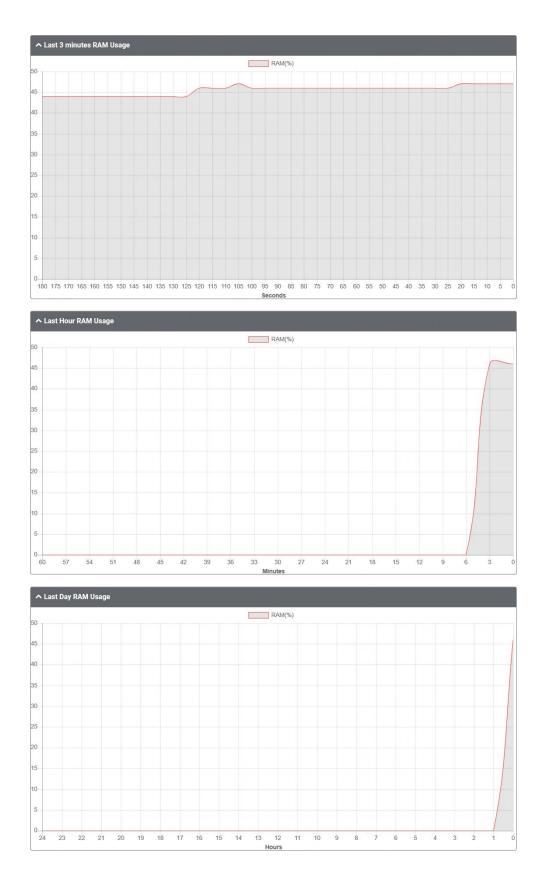
### **CPU Usage**







### **RAM Usage**

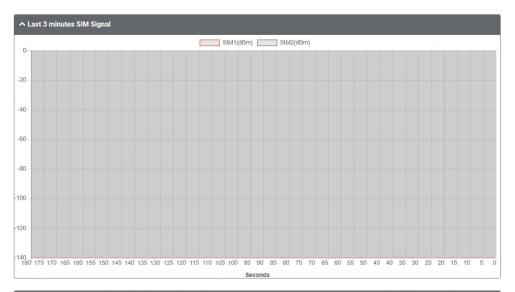


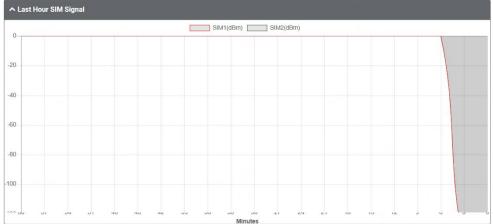
# SIM Traffic

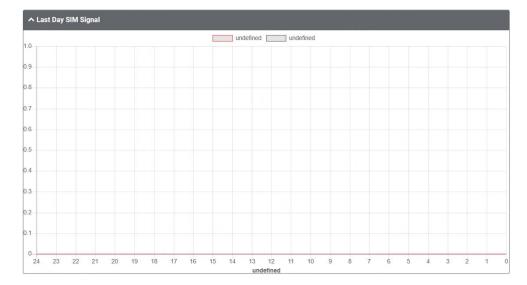




# SIM Signal







## 3.7.4 App Center

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

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

App Center		
	For more information about App, please refer to <a href="http://www.robustel.com/products/app-center/">http://www.robustel.com/products/app-center/</a> .	
∧ App Install		
	File Choose File No file chosen Install	
Item	Description	Default
File	Click on "Choose File" to locate the App file from your PC, and then click	
	Install to import this file into your device.	

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

↑ Installed Apps							
ndex	Name	Version	Status	Description			
1	linux-image-5.4.24-2.0.0	2.0.0	Running	Linux kernel, version 5.4.24-2.0.0	×		
2	rosp-core	2.0.0-1	Running	ros pro core deb	×		

Item	Description	Default
Index	Indicate the ordinal of the list.	
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the status of the App.	Null
Description	Show the description for this App.	Null

# 3.7.5 Tools

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



# Ping

Ping	Traceroute	Sniffer			
∧ Ping					
	IP Add	dress			
	Number of Rec	quest	5		
	Tim	neout	1		
	Inte	rface		v	
	1.00				Start Stop

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

### Traceroute

Ping	Traceroute	Sniffer			
• Traceroute					
	Tra	ice Address			
		Trace Hops	30		
	Tra	ice Timeout	1		
		Interface		~	

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

10 robustel



### Sniffer

Ping	Traceroute	Sniffer					
∧ Sniffer							
	Inter	rface	all	.v	·]		
		Host					
	Packets Rec	quest	1000				
	Pro	tocol	All	V	')		
	Si	tatus	0				
						Start	Stop

Item	Description	Default
Interface	Choose the interface according to your Ethernet configuration.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
Status	Show the current status of sniffer.	
Start	Click this button to start the sniffer.	
Chap	Click this button to stop the sniffer. Once you click this button, a new log file	
Stop	will be displayed in the following List.	

Capture	? Files			
Index	File Name	File Size	Modification Time	
1	22-05-09_13-45-11.cap	114101	Mon May 9 13:45:30 2022	₹×

Item	Description	Default
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find	
	the file from this Sniffer Traffic Data List and click ⊍ to download the log, click	
	× to delete the log file. It can cache a maximum of 5 files.	

# 3.7.6 Flash Manager

This section allows you to manage the device's flash memory life, you can easily check the flash status or thoughput



and start a period test on this section .

### Status

This page shows the flash status and data throughput details.

Status	Flash Memory Tests	
▲ Flash Status		0
-	Estimated Remaining Device Lifetime	90% - 100%
	Flash Total Erase Amount	303756.75 MB
	Total Blocks Erased	12273
	Block Size	24.75 MB
	Total Number of Blocks	3000
	Flash Avg Erase Count	18
	Flash Avg Erase Rate	<1%
	Flash Bad Block Count	7
	Increase Bad Block Count	0
	Power On Count	359 Times
	Reserved Block Consumption	Normal
	Capacity	14930 MB

Item	Today	Yesterday	Last 7 Days	Total	
Data Read(MB)	0	0	0	39040	
Data Write(MB)	128	0	128	76928	



# **Flash Memory Tests**

Status	Flash Memory Tests		
▲ Flash Memory Te	sts		
		Test Mode	scheduled v 🤇
		Start Time	mm/dd/yyyy:
		End Time	mm/dd/yyyy:
			Start Stop
		Flash N	Memory Tests @ Flash Manager
Item	Descriptio	on	
Test Mode	Manual:	When choo	sing 'manual', click 'start' to run a test, you can click 'stop' to end the
	test;		
	Schedule	<b>d</b> : Input the	e 'start' and 'end' time for a scheduled test.
	You can c	lick 'stop' bi	utton under whatever mode.
Start Time	Enter star	t time, forn	nat: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 12:00:00
End Time	Enter end	time, form	nat: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 18:00:00
	4		

You can click 🎽 to download the test log for viewing more information.

# 3.7.7 Service Management

This section allows you to modify the network services manage way.

Service Management

▲ Settings		0
WAN	Managed by RobustOS Pro v	
LAN	Managed by RobustOS Pro v	
Firewall	Managed by RobustOS Pro v	
Route	Managed by RobustOS Pro v	
Policy Route	Managed by RobustOS Pro v	

Mode	View Status on RobustOS Pro	Configure via RobustOS Pro	Configure via Linux Shell
Managed By RobustOS Pro	v	v	x
Managed By Third-Party	x	x	v

## 3.7.8 Profile

This section allows you to import or export the configuration file, or rollback the device to a previous configuration.

### Profile

Profile	Rollback		
∧ Import Configur	ration File		
	Reset Other Settings to Default	ON OFF	
	Ignore Invalid Settings	ON OFF ?	
	XML Configuration File	Choose File No file chosen	
Item	Description		Default

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



Ignore Invalid Settings	Click the toggle button as "ON" to ignore invalid settings.	OFF
XML Configuration File	Click on Choose File to locate the XML configuration file from your PC, and	
	then click Import to import this file into your device.	

▲ Export Configuration File		
Ignore Disabled Features	ON OFF	
Add Detailed Information	ON OFF	
XML Configuration File	Generate	
XML Configuration File	Export	

Item	Description	Default
Ignore Disabled Features	Click the toggle button as "OFF" to ignore the disabled features.	OFF
Add Detailed Information	Click the toggle button as "On" to add detailed information.	OFF
Encrypt Secret Data	Click the toggle button as "ON" to encrypt the secret data.	ON
XML Configuration File	Click Generate button to generate the XML configuration file, and	
	click Export to export the XML configuration file.	

∧ Default Configuration	
Save Running Configuration as Default	Save ?
Restore to Default Configuration	Restore
Restore To Factory Default Configuration	Restore ?

Item	Description	Default
Save Running Configuration as Default	Click Save button to save the current running parameters as default	
	configuration.	
Restore to Default Configuration	Click Restore button to restore the defaults configuration.	
Restore to Factory Default Configuration	Click Restore button to restore the factory defaults configuration.	
	Note: The Linux file system will be restored to the initialization state.	



### Rollback

Profile	Rollback				
∧ Configurat	ion Rollback				
	Save as a Rollb	ackable Archive	ave		
∧ Configurat	ion Archive Files				
Index	File Name	File Size	Modification Time		

Item	Description	Default
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	View the related information about configuration archive files, including	
Files	name, size and modification time.	

### 3.7.9 User Management

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

Sudo User	Super User	Common User		
∧ Sudo User Setting	IS			?
	Ne	ew Username	?	
	(	Did Password	?	
	N	ew Password	0	
	Confi	rm Password		



Item	Descriptio	n	Default
New Username	Enter a ne	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9,	
	@,., -, #, \$	, and *.	
Old Password	Enter the	old password of your router. The default password please see the	Null
	product la	bel.	
New Password	Enter a ne	w password you want to create; valid characters are a-z, A-Z, 0-9,	Null
	@,., -, #, \$	@,., -, #, \$, and *.	
Confirm PasswordEnter the new password again to confirm.Nu		Null	
Sudo User Super User Common User		·	

∧ Super User Settings	()
New Username	
Old Password	()
New Password	()
Confirm Password	

Item	Description	Default
New Username	Enter a new username you want to create; valid characters are a-z, A-Z, 0-9,	Null
	@,., -, #, \$, and *.	
Old Password	Enter the old password of your router. The default password please see the	Null
	product label.	
New Password	Enter a new password you want to create; valid characters are a-z, A-Z, 0-9,	Null
	@,., -, #, \$, and *.	
Confirm Password	Enter the new password again to confirm.	Null

Sudo User	Super Us	er Common User	
Common User	Settings		(

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



▲ Common Users Settings	
Userld	
Role	Guest v
Username	
Password	

Item	Description	Default
Index	Indicate the ordinal of the list.	
Role	Select from "Guest" and "User".	
	Guest: Guest only can view the configuration of router under this level	
	• User: User can view and set the configuration of router under this level	
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z,	Null
	0-9, @, ., -, #, \$, and *.	

# 3.7.10 Debian Management

This section allows you to manage your own Debian packages.

Debian Management		
	_	
∧ Debian Package Management		
Apt Action	update	
Package Name		
Extra Parameters		0
	<u> </u>	Submit



Item	Description	Default	
Apt Action	Select from "update", "install", "clean", "remove", "show".		
	update: to update the apt.		
	Install: to install the apt.		
	Remove: to remove the apt.		
	Clean: to clean the apt.		
	Show: to show the apt list.		
Package Name	Enter the package name to implement.		
Extra Parameters	More parameters of 'apt' command, such as 'purge', etc. Null		

Role Management



# 3.7.11 Role Management

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

ettings		
Index	Role	
1	Guest	
2	User	

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

### Click dit Visitor/Editor permission.

∧ settings		
	Index	1
	Role	Guest v
	save and apply,reboot	ReadOnly v

∧ Network		and shares A
Firewall	ReadOnly v	
WAN	ReadOnly v	
Route	ReadOnly v	
QoS	ReadOnly v	
Policy Route	ReadOnly v	
LAN	ReadOnly v	

#### RobustOS Pro Software Manual

∧ System			
	Service Management	ReadOnly v	
	Flash Manager	ReadOnly v	
	DEB Management	ReadOnly v	
	Profile	ReadOnly v	
	Tools	ReadOnly v	
	App Center	ReadOnly v	
	Certificate Manager	ReadOnly v	
	Debug	ReadOnly v	
	User Management	ReadOnly v	

∧ Interface		
WiFi	ReadOnly v	
VLAN	ReadOnly v	
USB	ReadOnly v	
Serial Port	ReadOnly v	
Ethernet	ReadOnly v	
DIDO	ReadOnly v	
Cellular	ReadOnly v	
Bridge	ReadOnly v	

∧ VPN	
DMVPN	ReadOnly v
РРТР	ReadOnly
OpenVPN	ReadOnly
L2TP	ReadOnly
IPsec	ReadOnly
GRE	ReadOnly

**B**robustel



▲ Services			
	Captive Portal	ReadOnly	
	Web Server	ReadOnly	
	VRRP	ReadOnly	
	Syslog	ReadOnly	
	SSH	ReadOnly	
	SNMP	ReadOnly	
	SMS	ReadOnly	
	Advanced	ReadOnly	
	RCMS	ReadOnly	
	NTP	ReadOnly	
	GPS	ReadOnly	
	Event	ReadOnly	
	Email	ReadOnly	
	DDNS	ReadOnly	

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

#### Note:

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

# **Chapter 4** Configuration Examples

## 4.1 Cellular

# 4.1.1 Cellular APN Manual Setting and Cellular Dial-up.

This section shows you how to configure the APN for Cellular Dial-up. Connect the device correctly and insert the SIM card, then open the web configuration page. Under the homepage menu, click "Interface > Cellular > Cellular " to go



### to the cellular configuration page.

# Interface/Cellular

The router supports one cellular modem and two SIM slots, but only one SIM slot is activated at any time.

Cellular	Status AT De	bug		
▲ General Settings				
	Primary Sim	SIM1	× ?	
	Enable Auto Switching	ON OFF		
Additional Switchin	ng Rules			
	Weak Signal	ON OFF		
	While Roaming	ON OFF		

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

Click Click to set its parameters according to the current ISP.

∧ General Settings		
Index	1	
SIM Card	SIM1 v	
Automatic APN Selection	ON	
APN	internet	
Username		
Password		
Authentication Type	None v	
Phone Number		

# Ørobustel

PIN Code		0
Extra AT Cmd		0
Telnet Port	0	0

# Then Click <u>"Network> WAN> Link"</u> go to the WAN configuration page.

### Network/WAN

WAN stands for Wide Area Network, provides connectivity to the internet. You can config WAN based on Ethernet, Cellular modem or WiFi(if supported).

Link		Status			
Settings					
Name	Туре	Description	Weight	Firewall Zone	+
	WIFI	default wan	0	external	‼⊡×

Click + to add one link for cellular dial-up, select "Modem" as the link type, then click

to submit.

Submit

∧ Link Settings			
	Name	Cellular	0
	Туре	Modem	v
	Interface	wwan	v
	Description	Backup WAN	
	Weight	0	0
	Firewall Zone	external	v
<ul> <li>Health Detection Settings</li> </ul>			0
	Enable	ON OFF	
IDu/	1 Drimoni Sonior		Submit Close

After save and apply, the new cellular WAN link will take effect.

Link

Status



Name	Туре	Description	Weight	Firewall Zone	+
Wireless	WIFI	default wan	0	external	∷⊠×
Cellular	Modem	Backup WAN	0	external	‼⊠×

# 4.1.2 SMS Remote Control

EG51xx supports remote control via SMS. You can use following commands to get the status of the router, and set all the parameters of the router.

#### SMS command have the following structures:

- 1. Password mode—Username: Password;cmd1;cmd2;cmd3; ...cmdn (available for every phone number).
- 2. Phonenum mode-- **Password; cmd1; cmd2; cmd3; ... cmdn** (available when the SMS was sent from the phone number which had been added in router'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 router'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 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 configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

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

export the XML file.



# System/Profile

You can import, export configurations, or rollback to a previous configuration.

Profile	Rollback			
∧ Import Configura	ation File			
	Reset Other Settings to Default			
	Ignore Invalid Settings	ON OFF ?		
	XML Configuration File	Choose File No file chosen	Import	
▲ Export Configura	ation File			
	Ignore Disabled Features	ON OFF		
	Add Detailed Information	ON OFF ?		
	XML Configuration File	Generate		
	XML Configuration File	Export		

#### 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 commands packed in a single SMS.
- 4. E.g.

#### admin:admin;status system

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

#### SMS received:

firmware\_version = 2.0.0 firmware\_version\_full = "2.0.0 (60b55c0)" kernel\_version = 5.4.24-2.0.0 hardware\_version = 0.0 operation\_system = "Debian GNU/Linux 11.3"



device\_model = "" serial\_number = 2204190667030003 temperature\_interval = 53.0 uptime = "0 days, 00:12:06" system\_time = "Thu May 19 16:52:22 2022" ram\_usage = 392M/448M cpu\_usage = 392M/448M cpu\_usage = "22569s Idle/71405s Total /1 cpus" disk\_usage = 1.9G/7.1G **admin:admin;reboot** In this command, username is "admin", password is "admin", and the command is to reboot the Router. **SMS received:** OK

#### admin:admin;set firewall remote\_ssh\_access false;set firewall remote\_telnet\_access false

In this command, username is "admin", password is "admin", and the command is to disable the remote\_ssh and remote\_telnet access.

SMS received:

OK

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

#### SMS received:

ОК

ОК

ОК

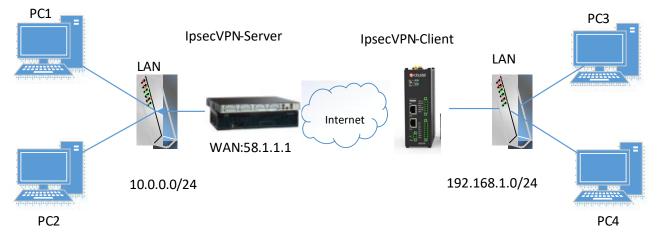
ОК



# 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).





### **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
                  Negate a command or set its defaults
  no
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
  kev
          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
               Configure IPSEC policy
  ipsec
  isakmp
               Configure ISAKMP policy
               Long term key operations
  kev
               Enter a crypto map
  map
Router(config) #crypto ipsec ?
  security-association Security association parameters
                        Define transform and settings
  transform-set
Router(config) #crypto ipsec transform-set Trans ?
  ah-md5-hmac AH-HMAC-MD5 transform
  ah-sha-hmac AH-HMAC-SHA transform
                ESP transform using 3DES(EDE) cipher (168 bits)
  esp-3des
  esp-aes
                ESP transform using AES cipher
                ESP transform using DES cipher (56 bits)
  esp-des
  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
```

### **IPsec VPN\_Client:**

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

# VPN/IPsec

IPsec is a suite of protocols for creating a secure tunnel between a host and a remote IP network across the Internet.

General		Tunnel	Status		
unnel Se	ettings				

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

∧ General Settings		
Index	1	
Enable	ON OFF	
Description	[IPsec1	]
Link Binding	wlan0 v	]
Gateway	58.1.1.1	] ⑦
Protocol	ESP v	]
Mode	Tunnel v	]
Local Subnet	192.168.1.0/24	?
Remote Subnet	0.0.0/24	0
ІКЕ Туре	IKEv1 v	]
Negotiation Mode	Main v	
Initiation Mode	Always On v	
▲ Advanced Settings		_
Enable Compression	ON OFF	
Enable Forceencaps	ON OFF ?	
Backup Gateway		] ⑦
Expert Options		] ⑦



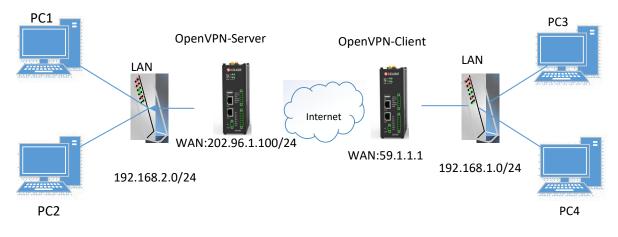
## ∧ PHASE 1

Encryption Algorithm	3DES	v	
Authentication Algorithm	SHA1	v	
IKE DH Group	DHgroup2	v	
Authentication Type	PSK	v	
PSK Secret			
Local ID Type	Default	v	
Remote ID Type	Default	v	
IKE Lifetime	86400	0	

#### ∧ PHASE 2 **Encryption Algorithm** 3DES V Authentication Algorithm SHA1 ٧ PFS Group PFS(N/A) ۷ ? SA Lifetime 28800 **DPD** Interval 0 30 2 **DPD** Failures 150

When finished, click Submit to submit and click  $\bigcirc$  for the configuration to take effect.

# 4.2.2 OpenVPN



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

### **OpenVPN\_Server:**

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

local 202.96.1.100 mode server port 1194 proto udp dev tun tun-mtu 1500 fragment 1500 ca ca.crt cert Server01.crt key Server01.key dh dh1024.pem server 10.8.0.0 255.255.255.0 ifconfig-pool-persist ipp.txt push "route 192.168.3.0 255.255.255.0" client-config-dir ccd route 192.168.1.0 255.255.255.0 keepalive 10 120 cipher BF-CBC comp-lzo max-clients 100 persist-key persist-tun status openvpn-status.log verb 3 Note: For more configuration details, please contact your technical support engineer.



### **OpenVPN\_Client:**

### Click "VPN > OpenVPN > OpenVPN" as below.

### VPN/OpenVPN

OpenVPN is an open-source VPN technology that creates secure point-to-point or site-to-site connections.

OpenVP	N	Status				
▲ Tunnel Se	ettings					
Index	Enable	Description	Mode	Peer Address		+

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

∧ General Settings		
Index	1	
Enable	ON OFF	
Description	client01	
Mode	Client v	0
Protocol	UDP v	
Peer Address	202.96.1.100	
Peer Port	1194	
Interface Type	TUN v	
Authentication Type	X509CA v	?



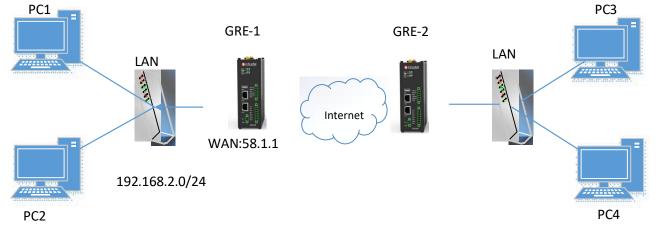
Root CA	None	v
Certificate File	None	v
Private Key	None	v
Private Key Password		
Encrypt Algorithm	BF	v
Authentication Algorithm	SHA1	v
Renegotiation Interval	86400	0
Keepalive Interval	20	0
Keepalive Timeout	120	0
TUN MTU	1500	
Max Frame Size	1400	
Enable Compression	ON OFF	
Enable NAT	ON OFF	
Enable DNS overrid	ON OFF ?	
Verbose Level	3	v 🕜

Advanced Settings Enable HMAC Firewall	ON OFF
Enable PKCS#12	ON OFF
Enable nsCertType	ON OFF
Expert Options	(
When finished, click Submit to submit a	nd click 🔗 for the configuration to take effect.



### 4.2.3 GRE VPN

**GRE VPN topology** 



### GRE-1:

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

### VPN/GRE

GRE stands for Generic Routing Encapsulation, is an IP packet encapsulation protocol that allows for networks and routes to be advertized from one network device to another.

GRE		Status	
Tunnel Se	ettings		

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



G	RE		
	Index	1	10
	Enable	ON OFF	
	Description	GRE-1	
	Remote IP Address	58.1.1.1	
	Local Virtual IP Address	10.8.0.1	
	Local Virtual Netmask/Prefix Length	255.255.255.0	
	Remote Virtual IP Address	10.8.0.2	
	Enable Default Route	ON OFF	
	Enable NAT	ON OFF	
	Secrets	••••	
		Submit	Close

When finished, click Submit to submit and click O for the configuration to take effect.



### GRE-2:

On the remote side, click + button and set the parameters of GRE-2 as below.

GRE					
	Index	1			
	Enable	ON OFF			
	Description	GRE-2			
	Remote IP Address	59.1.1.1			
	Local Virtual IP Address	10.8.0.2			
L	ocal Virtual Netmask/Prefix Length	255.255.255.0	?		
	Remote Virtual IP Address	10.8.0.1			
	Enable Default Route	ON OFF			
	Enable NAT	ON OFF			
	Secrets	•••••			
		A		Submit	Close

When finished, click Submit to submit and click Office for the configuration to take effect.

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

		GRE			
Index	1	Index	1		
Enable	ON OFF	Enable	ON OFF		
Description		ernal IP address of another GRE instance used <sup>Description</sup>	GRE-2		
Remote IP Address	58.1.1.1 to	establish the initial connection between peers. Remote IP Address	59.1.1.1		
Local Virtual IP Address	10.8.0.1	Local Virtual IP Address	10.8.0.2		
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	IP address of the remote GRE Tunnel network interface. Remote Virtual IP Address	10.8.0.1		
Enable Default Route	ON OFF	Enable Default Route	ON OFF	and a B	
Enable NAT	ON OFF	Enable NAT Used the same password for the GRE peers	ON OFF		
Secrets		Secrets	••••		
				Submit	Close



# **Chapter 5** Introductions for CLI

# 5.1 What Is CLI

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

#### **Route login:**

Router login: admin

Password: admin(could be different)

#

#### **CLI commands:**

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

# 5.2 How to Configure the CLI

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

# 5.3 Commands Reference

Commands	Syntax	Description
Debug	Debug parameters	Turn on or turn off debug function
Show	Show parameters	Show current configuration of each function, if we need to see all
		please using "show running "
Set	Set parameters	All the function parameters are set by commands set and add, the
Add	Add parameters	difference is that set is for the single parameter and add is for the list
		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 learn to configure it with some reference examples.

### Example 1: Show current version

```
# status system
firmware_version = 2.0.0
firmware_version_full = "2.0.0 (60b55c0)"
kernel_version = 5.4.24-2.0.0
hardware_version = 0.0
operation_system = "Debian GNU/Linux 11.3"
device_model = ""
serial_number = 2204190667030003
temperature_interval = 53.0
uptime = "0 days, 00:12:06"
system_time = "Thu May 19 16:52:22 2022"
ram_usage = 392M/448M
cpu_usage = "22569s Idle/71405s Total /1 cpus"
disk_usage = 1.9G/7.1G
#
```

## Example 2: CLI for setting Cellular

```
# show cellular all
primary_sim = sim1
auto switch = false
switch_by_signal = false
rssi_quality = -87
switch_while_roaming = false
sim {
    id = 1
     card = sim1
     phone_number = ""
     pin_code = ""
     extra_at_cmd = ""
    telnet_port = 0
     network_type = auto
     band_select_type = all
     band_settings {
         gsm 850 = false
         gsm_900 = false
         gsm_1800 = false
         gsm_1900 = false
```



wcdma\_800 = false wcdma\_850 = false wcdma\_900 = false wcdma\_1900 = false wcdma\_2100 = false wcdma\_1700 = false wcdma\_band19 = false lte\_band1 = false lte\_band2 = false Ite\_band3 = false lte\_band4 = false lte\_band5 = false lte\_band7 = false lte\_band8 = false Ite band13 = false lte\_band17 = false lte\_band18 = false lte\_band19 = false lte\_band20 = false Ite band21 = false lte\_band25 = false lte\_band28 = false lte\_band31 = false Ite\_band38 = false Ite\_band39 = false Ite\_band40 = false lte\_band41 = false debug\_enable = true verbose\_debug\_enable = false

```
# set(space+space)
```

}

}

ai	bridge	cellular	ddns	dido
dmvpn	email	ethernet	event	firewall
gps	gre	ipsec	l2tp	lan_links
ntp	openvpn	policy_router	pppoe_bridge	pptp
qos	rcms	reboot	route	serial_port
sms	snmp	ssh	syslog	system
Usb	syslog	user_management	vlan	vrrp
web_server	wan_links	web_server	wireless	

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



### # set cellular sim 1(space+?)

card	SIM Card
phone_number	Phone Number
pin_code	PIN Code
extra_at_cmd	Extra AT Cmd
telnet_port	Telnet Port
network_type	Network Type
band_select_type	Band Select Type
band_settings	Band Settings
telit_band_settings	Band Settings
debug_enable	Debug Enable
verbose_debug_enable	Verbose Debug Enable
# set cellular sim 1 phone_n	umber 18620435279
ОК	
<pre># config save_and_apply</pre>	

ОК

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



# Glossary

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



Abbr.	Description
LAN	local area network
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
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
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



Abbr.	Description
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 <sup>.</sup>	www.robustel.com	