



Software Manual

MG460

Software Manual

robust **OS** Pro

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

MG460

Copyright©2025 Guangzhou Robustel Co., Ltd.

All rights reserved.

Trademarks and Permissions

 robustel &  robustOS 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: support@robustel.com

Web: www.robustel.com

Document History

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

Date	Firmware Version	Document Version	Change Description
June 17, 2024	2.1.3	1.0.0	Initial release.
December 23, 2024	2.1.7	1.0.1	<ol style="list-style-type: none">1. Separated HBT and ALF into two tabs in BAM.2. Removed IPV6-related features.3. Added a multi-destination address option in Traffic Rules.4. Included a VPN toggle option in DIDO.5. Added COM1/2 options for the USR light in the Advanced Configuration.6. Changed GPS to GNSS on the web interface.7. Added an Overridden DNS option on the WAN interface.

Contents

Chapter 1 Initial Configuration	6
1.1 PC Configuration	6
1.2 Factory Default Settings	9
1.3 Factory Reset	9
1.4 Log in the Device	10
1.5 Control Panel	11
Chapter 2 WebUI Descriptions	13
2.1 Dashboard	13
2.1.1 Overview	13
2.1.2 Modem	13
2.1.3 Ethernet	14
2.1.4 Internet Status	14
2.1.5 LAN Status	14
2.1.6 System Resource	15
2.1.7 System Information	15
2.1.8 Cellular Status	16
2.1.9 RCMS Status	16
2.2 Interface	17
2.2.1 Ethernet	17
2.2.2 Cellular	18
2.2.3 Bridge	24
2.2.4 Wi-Fi	24
2.2.5 USB	25
2.2.6 VLAN	26
2.2.7 DI/DO	27
2.2.8 Serial Port	30
2.2.9 BAM	37
2.3 Network	40
2.3.1 WAN	40
2.3.2 LAN	44
2.3.3 Route	46
2.3.4 Policy Route	48
2.3.5 Firewall	49
2.3.6 QoS	56
2.4 VPN	58
2.4.1 IPsec	58
2.4.2 OpenVPN	66
2.4.3 GRE	74
2.4.4 PPTP	76
2.4.5 L2TP	80
2.4.6 DMVPN	83
2.5 Services	88
2.5.1 Syslog	88
2.5.2 Event	89

- 2.5.3 NTP 94
- 2.5.4 SMS 95
- 2.5.5 Email 97
- 2.5.6 DDNS 98
- 2.5.7 VRRP 100
- 2.5.8 SSH 101
- 2.5.9 GNSS 101
- 2.5.10 RCMS 105
- 2.5.11 SNMP 109
- 2.5.12 Web Server 113
- 2.5.13 Advanced 113
- 2.6 System 115
 - 2.6.1 Debug 115
 - 2.6.2 Certificate Manager 118
 - 2.6.3 Resource Graph 122
 - 2.6.4 App Center 127
 - 2.6.5 Tools 127
 - 2.6.6 Flash Manager 131
 - 2.6.7 Service Management 132
 - 2.6.8 Profile 133
 - 2.6.9 User Management 134
 - 2.6.10 DEB Management 136
 - 2.6.11 Role Management 137
- Chapter 3 Configuration Examples 141**
 - 3.1 Cellular 141
 - 3.1.1 Cellular APN Manual Setting and Cellular Dial-up 141
 - 3.1.2 SMS Remote Control 143
 - 3.2 VPN Configuration Examples 146
 - 3.2.1 IPsec VPN 146
 - 3.2.2 OpenVPN 150
 - 3.2.3 GRE VPN 153
- Chapter 4 Introductions for CLI 156**
 - 4.1 What Is CLI 156
 - 4.2 How to Configure the CLI 157
 - 4.3 Commands Reference 157
 - 4.4 Quick Start with Configuration Examples 158
 - Example 1: Show current version 158
 - Example 2: CLI for setting Cellular 158
- Chapter 5 Glossary 161**

Chapter 1 Initial Configuration

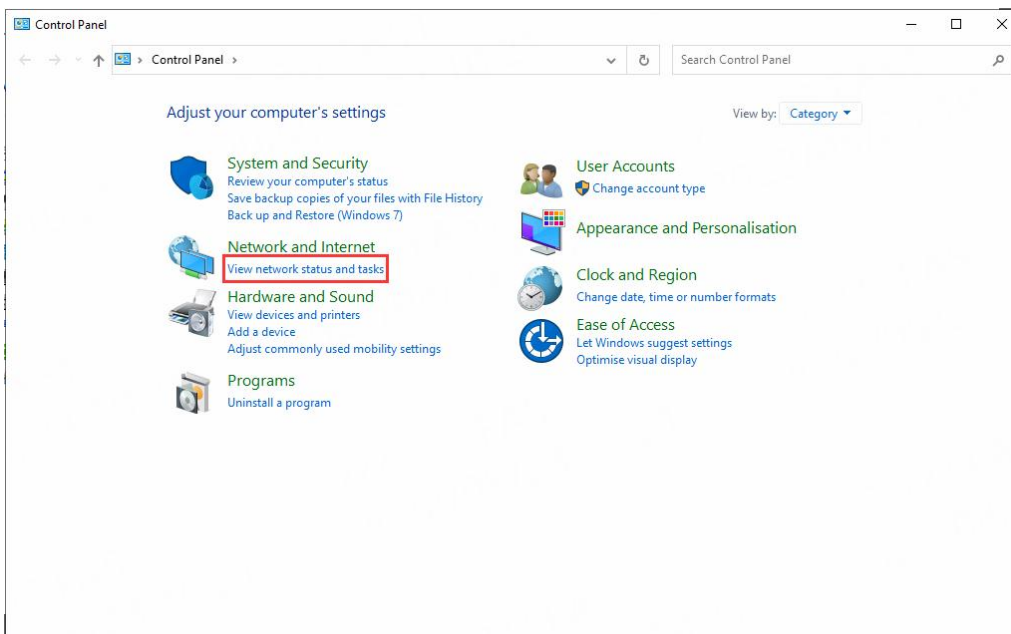
The device can be configured through your web browser that including Microsoft Edge, Chrome and Firefox, etc. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows. It provides an easy and user-friendly interface for configuration. There are various 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.

1.1 PC Configuration

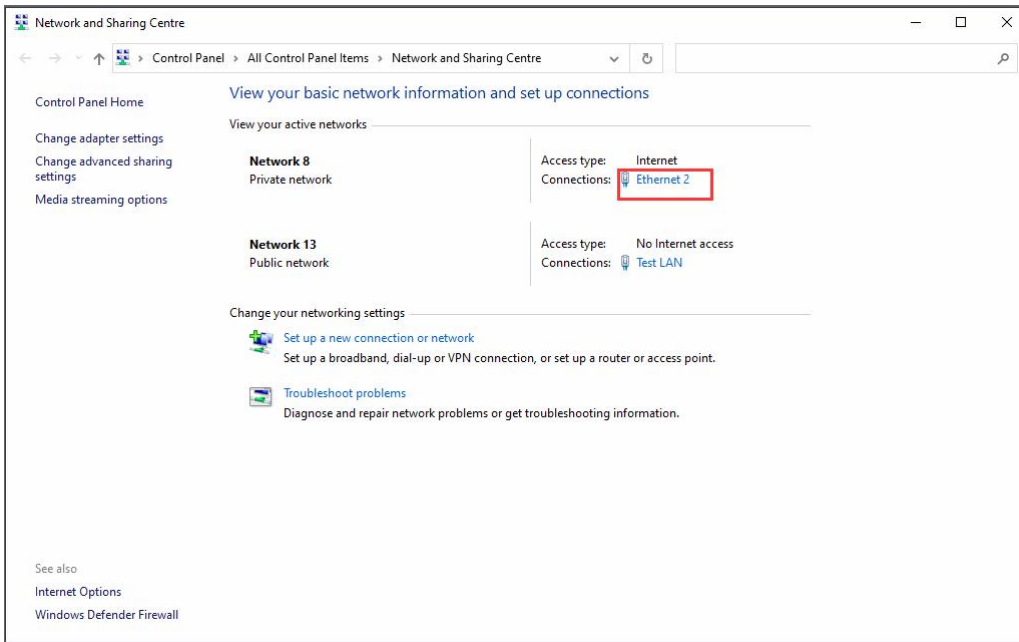
There are two ways to get an IP address for the computer. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

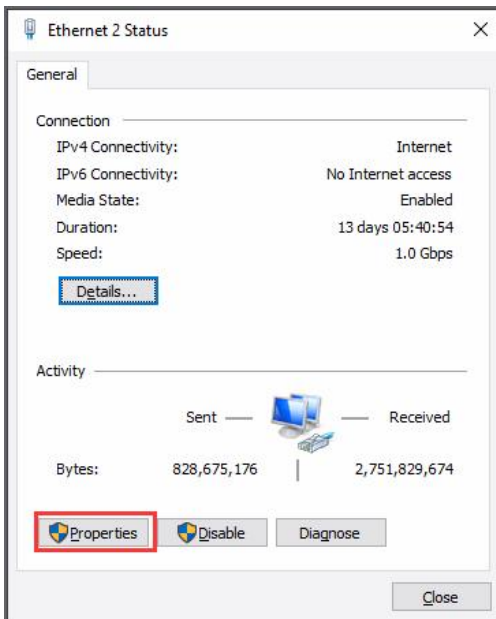
1. Right-click “**Windows LOGO**” on the taskbar, select “**Run**”, and type “**Control**” to launch the Control panel, then Click “**View network status and tasks**”.



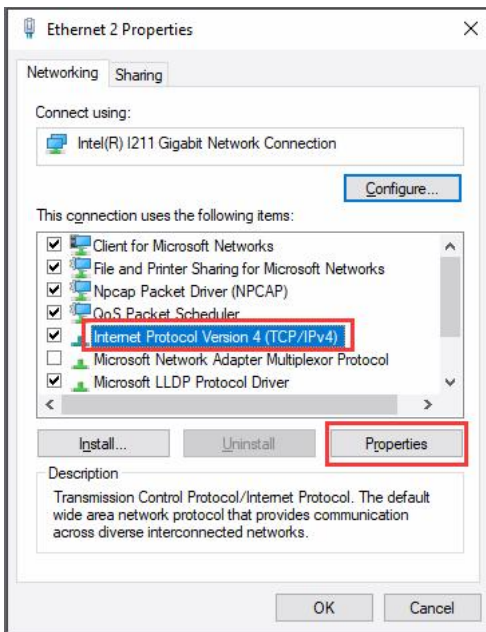
2. After entering "Network and Sharing Center", click "Ethernet" connections status.



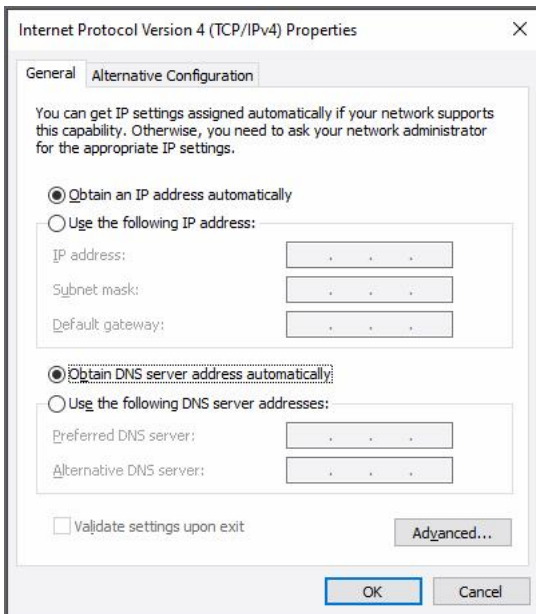
3. Click **Properties** in the window of Network Connection status.



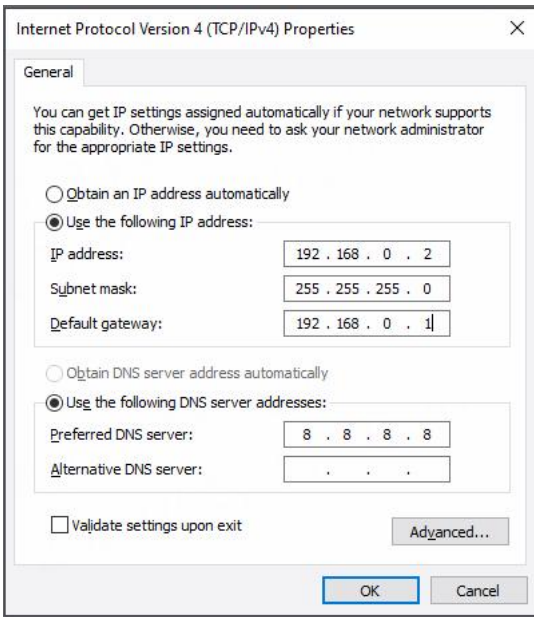
4. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



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



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



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

1.2 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
ETHn	192.168.0.1/255.255.0.0, LAN mode
DHCP Server	Enabled

1.3 Factory Reset

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

1.4 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 <https://192.168.0.1/24>, 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.



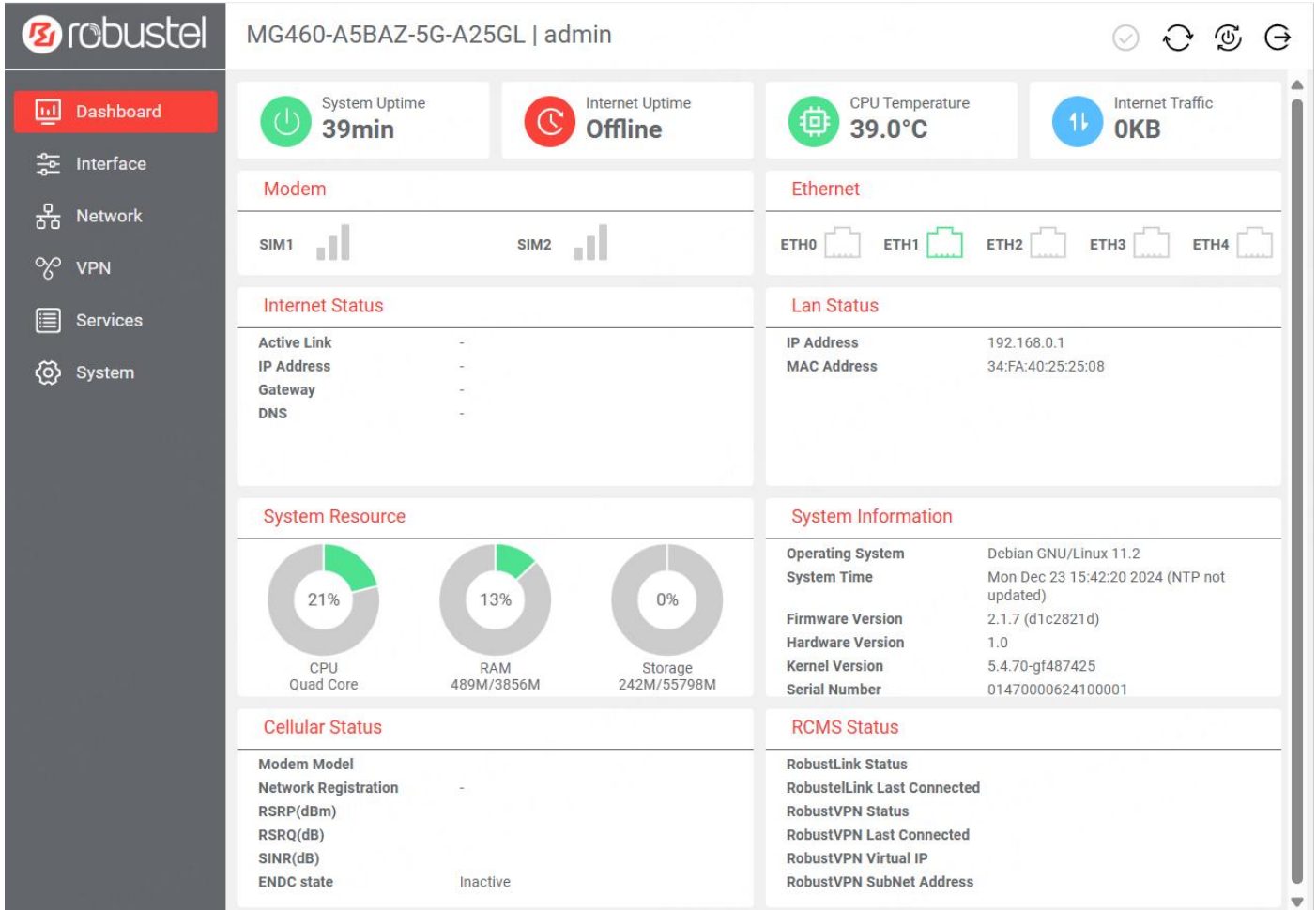
3. In the login page, enter the username and password, you can check the login information from the device's stick, and then click **LOGIN**. See the information on the product label for default username and password.

Note: If enter the wrong password over 6 times, the user account will be locked for 5 minutes.








1.5 Control Panel




After logging in, the home page of the web interface is displayed.



From the homepage, users can find the model information and perform operations such as saving the configuration, restarting the device , and logging out.

Control Panel		
Item	Description	Icon
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 and apply the modification on every configuration page, to make the modification taking effect.	 or 
Restart	Click to restart all the RobustOS Pro operating system based applications(applications controlled by 11system are not included), then switch to the login page.	
Reboot	Click to reboot the device, then switch to the login page.	
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.	

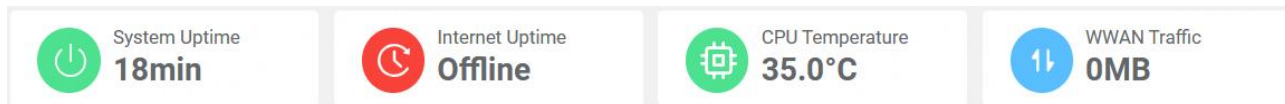
Note: The steps of how to modify configuration are as bellow:

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

Chapter 2 WebUI Descriptions

2.1 Dashboard

2.1.1 Overview







Item	Description
System Uptime	Show the current amount of time the router has been powered on.
Internet Uptime	Show the current amount of time the router has been connected to internet.
CPU Temperature	Show the CPU temperature.
Traffic	Show the amount of WWAN data traffic usage.

2.1.2 Modem

This page shows the status of SIM card.

Modem







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

2.1.3 Ethernet

This page shows the device’s Ethernet status

Ethernet

ETH0		ETH1	
------	---	------	---

Icon	Description
	Port disable or link down.
	Link up.

2.1.4 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.

2.1.5 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.

2.1.6 System Resource

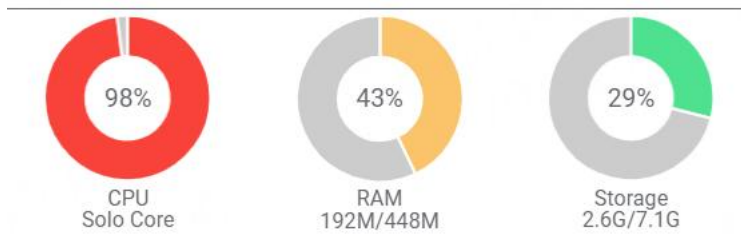
This page shows the device’s system resources usage information.

When the usage is more than 95%, the icon will be in **Red**.

When the usage is between 80% and 95%, the icon will be in **Yellow**.

When the usage is less than 80%, the icon will be in **Green**.

System Resource



2.1.7 System Information

This page shows the device’s system information.

System Information

Operating System	Debian GNU/Linux 11.2
System Time	Mon Jun 19 05:06:53 2023 (NTP not updated)
Firmware Version	2.1.3 (4f342e97)
Hardware Version	1.3
Kernel Version	5.4.70-gf9f5f4701
Serial Number	12000923120010

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.

2.1.8 Cellular Status

This page shows the device’s cellular status.

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

Item	Description
Modem Vendor	Show the radio module vendor information.
Modem Model	Show the model of the radio module.
Network Registration	Show the current network registration information.
IMEI	Show the IMEI (International Mobile Equipment Identity) number of the radio module.
IMSI	Show the IMSI (International Mobile Subscriber Identity) number of the current SIM.

2.1.9 RCMS Status

This page shows the device’s RCMS status.

RCMS 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

2.2 Interface

2.2.1 Ethernet

This section allows you to set the related parameters for Ethernet. There are 5 Ethernet ports in the device. The ETH0 is the WAN port, and others are the LAN port.

Ports

Ports			Status																								
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #333; color: white; padding: 2px 5px; margin-bottom: 5px;"> ^ Port Settings </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 20%;">Name</th> <th style="width: 20%;">Port</th> <th style="width: 20%;">MTU</th> <th style="width: 40%;"></th> </tr> </thead> <tbody> <tr> <td>port1</td> <td>eth0</td> <td>1500</td> <td style="text-align: right;"></td> </tr> <tr> <td>port2</td> <td>eth1</td> <td>1500</td> <td style="text-align: right;"></td> </tr> <tr> <td>port3</td> <td>eth2</td> <td>1500</td> <td style="text-align: right;"></td> </tr> <tr> <td>port4</td> <td>eth3</td> <td>1500</td> <td style="text-align: right;"></td> </tr> <tr> <td>port5</td> <td>eth4</td> <td>1500</td> <td style="text-align: right;"></td> </tr> </tbody> </table> </div>				Name	Port	MTU		port1	eth0	1500		port2	eth1	1500		port3	eth2	1500		port4	eth3	1500		port5	eth4	1500	
Name	Port	MTU																									
port1	eth0	1500																									
port2	eth1	1500																									
port3	eth2	1500																									
port4	eth3	1500																									
port5	eth4	1500																									

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

Ports

^ Port Settings

Name ?

Port v

Enable Ethernet ON OFF ?

Port Speed v

MTU ?

Item	Description	Default
Name	Name of the port.	--
Port	Show the editing port, read only.	--
Enable Ethernet	Click the toggle button to enable/disable the Ethernet port.	ON

Port Speed	Select from “Auto”, “10M-half”, “10M-full”, “100M-half”, “100M-full”, “1000M-half”, “1000M-full”.	Auto
MTU	Enter the value of the maximum transmission unit(MTU).	1500

Status

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

Ports
Status

^ Port Status

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

2.2.2 Cellular

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.

Cellular

Cellular
Status
AT Debug

^ General Settings

Primary Sim ?

SIM1

v

Enable Auto Switching ?

ON

OFF

?

Enable Auto Revert ?

ON

OFF

?

Revert Interval ?

30

?

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 to another one when there is SIM card error or connection error or ping fails by default.	ON
Enable Auto Revert	When auto switching is enabled, the backup SIM card will be automatically switched to primary sim card when backup SIM card online time is greater than revert interval time.	OFF
Revert Interver	Duaction of auto revert, the unit is minuts.	30

^ Additional Switching Rules

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 backup.	ON
While Roaming	Switch to another SIM card while roaming, only used for dual SIM backup.	OFF

^ Advanced Cellular Settings

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

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

^ General Settings

Index

SIM Card

Automatic APN Selection ON OFF

Phone Number

PIN Code

Extra AT Cmd

Telnet Port

Item	Description	Default
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” 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.	ON
Phone Number	Enter the phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
Extra AT Cmd	Enter the AT commands used for cellular initialization.	Null
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet. 0 means not supported.	0

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

Automatic APN Selection ON OFF

APN

Username

Password

Authentication Type v

Item	Description	Default
APN	Enter the Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	Enter the username for cellular dial-up connection, provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection, provided by local ISP.	Null
Authentication Type	Select the authentication type. Select from “None”, “CHAP”, “PAP”. <ul style="list-style-type: none"> • None: None. • CHAP: Challenge-Handshake Authentication Protocol. • PAP: Password Authentication Protocol. 	None

Cellular Network Settings

Network Type v ?

Band Select Type 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.

Item	Description	Default
Network Type	Select the cellular network type, which is the network access order. Select	Auto

	<p>from “Auto”, “2G Only”, “3G Only”, “4G Only”, “5G Only”.</p> <ul style="list-style-type: none"> • 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 <p><i>Note:</i> 1) There may be some different optional network types due to the different cellular module.</p>	
Band Select Type	<p>Select from “All” or “Specify”. You may choose certain bands if choosing “Specify”.</p> <p><i>Note:</i> There may be some differences in Band Setting due to the different cellular module.</p>	All

^ Advanced Settings

Debug Enable ON OFF

Verbose Debug Enable ON OFF

RSSI Threshold ?

RSRP Threshold ?

Timeout For Network Registration ?

Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable for debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable for verbose debugging information output.	OFF
RSSI Threshold	Is used to judge whether the signal is too weak to switch SIM, unit: dbm.	-87
RSRP Threshold	Is used to judge whether the signal is too weak to switch SIM, unit: dbm.	-105
Timeout For Network Registration	The timeout required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	150

Status

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

Cellular **Status** AT Debug

^ 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.

Cellular **Status** AT Debug

^ Status				
Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EG25	46001[REDACTED]0493	Registered to home network
<p>Index 1</p> <p>Modem Status Ready</p> <p>Modem Vendor quectel</p> <p>Modem Model EG25</p> <p>Current SIM SIM1</p> <p>Phone Number +8613268[REDACTED]</p> <p>IMSI 46001[REDACTED]0493</p> <p>ICCID 89860121[REDACTED]379743</p> <p>Registration Registered to home network</p> <p>Network Provider CHN-UNICOM</p> <p>Network Type LTE</p> <p>Band 3</p> <p>Signal Strength 24 (-65dBm)</p> <p>RSRP -101 dBm</p> <p>RSRQ -17 dB</p> <p>SINR -5 dB</p> <p>Bit Error Rate 99</p> <p>PLMN ID 46001</p> <p>Local Area Code</p> <p>Cell ID 6B20D02</p> <p>Tracking Area Code 251B</p> <p>Physical Cell ID 73</p> <p>IMEI 8653260 [REDACTED]382</p> <p>Firmware Version EG25GGBR07A08M2G_30.006.30.006</p>				

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.
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

^ AT Debug

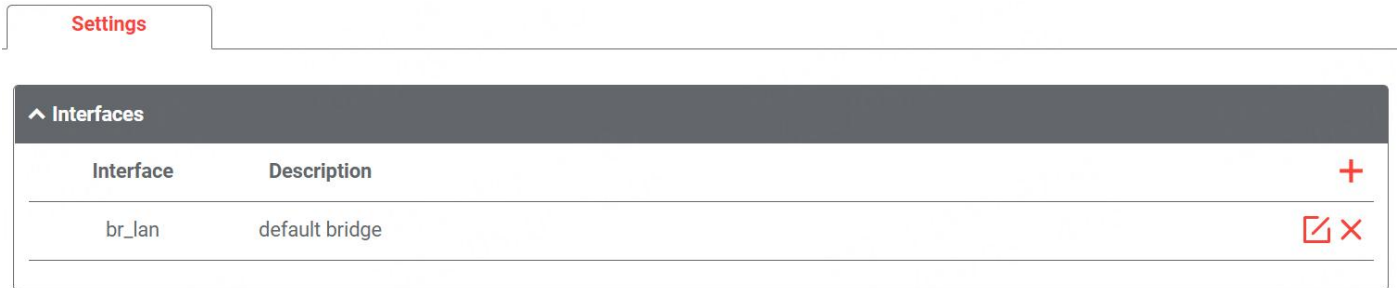
Command

Result

Send

2.2.3 Bridge

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



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

Click **X** to delete the Bridge.

Click **☑** to configure the Bridge’s parameters in the pop-up window.



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

2.2.4 Wi-Fi

This router cannot support WiFi AP mode, User can configure the device as Wi-Fi client by following steps.

Click [“Network> WAN>Link> Setting”](#), click **+** to add a new WAN link, then configure the related parameters.

^ Link Settings

Name ?

Type v

Interface v

SSID

Password

Description

Weight ?

Firewall Zone v

2.2.5 USB

This section allows you to configure the USB parameters. The router has two USB Host type A and one USB OTG type C ports available, the router's USB interface can be used to upgrade firmware and upgrade configuration. The users can disable all the USB ports for safety if needed.

USB

Key

^ USB Host Setting

Enable USB1 Host ON OFF ?

Enable USB2 Host ON OFF ?

Enable Automatic Upgrade ON OFF ?

^ USB OTG Settings

Enable USB3 OTG ON OFF ?

Item	Description	Default
Enable USB1 Host	Click the toggle button to enable/disable the USB1 Host option.	OFF
Enable USB2 Host	Click the toggle button to enable/disable the USB2 Host option.	OFF
Enable Automatic Upgrade	Click the toggle button to enable/disable this option. Enable to automatically update the firmware of the router when inserting a USB storage device with a router firmware.	OFF
Enable USB3 OTG	Click the toggle button to enable/disable the USB3 OTG option, to access to the microSD embedded.	OFF

^ Key

USB Automatic Upgrade Key	Generate
USB Automatic Upgrade Key	Download

Item	Description	Default
USB Automatic Upgrade Key	Click Generate to generate and click Download 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 USB 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.

2.2.6 VLAN

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

[Settings](#)

^ Interfaces

Name	Description	VLAN Tag	
			+

Click [+](#) to add a new Interface. The maximum count is **10**.

^ Interfaces

Name	<input type="text"/>	?
Description	<input type="text"/>	
VLAN Tag	<input type="text" value="1"/>	
Parent Type	<input type="text" value="Ethernet"/>	v
Parent Interface	<input type="text" value="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

2.2.7 DI/DO





This section allows you to set the DI/Relay output parameters.

DIDO

DIDO

Status

^ DIDO Settings

Index	PHY Mode	Enable	
1	DI	false	
2	DI	false	
3	Relay	false	
4	Relay	false	

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

DI

^ General Settings

Index	<input style="width: 100%;" type="text" value="1"/>
PHY Mode	<input style="width: 100%;" type="text" value="DI"/>
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Mode	<input style="width: 100%;" type="text" value="ON-OFF"/>
Inversion	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Alarm On Content	<input style="width: 100%;" type="text" value="Alarm On"/>
Alarm Off Content	<input style="width: 100%;" type="text" value="Alarm Off"/>
VPN Toggle	<input style="width: 100%;" type="text" value="Disable"/> ?

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". <ul style="list-style-type: none"> ON-OFF: Alarm mode can be triggered at the DI access ON-OFF. Counter: Event counter mode 	ON-OFF
Inversion	The count is divided into a rising edge count of the level or a falling edge count. If the current rising edge count, the reverse edge is the falling edge count.	OFF
Threshold Value	The threshold value is a unique parameter when the mode is Count . Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show the content when alarm on.	Alarm On
Alarm Off Content	Show the content when alarm off.	Alarm Off
VPN Toggle	Select from "Disable", "OpenVPN", "RVPN" to enable the VPN option by DI	Disable

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

Relay Output

^ General Settings

Index	<input type="text" value="3"/>
PHY Mode	<input style="border: 1px solid #ccc;" type="text" value="Relay"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Alarm On Action	<input style="border: 1px solid #ccc;" type="text" value="Relay On"/>
Alarm Off Action	<input style="border: 1px solid #ccc;" type="text" value="Relay Off"/>
Initial State	<input style="border: 1px solid #ccc;" type="text" value="Relay On"/>
Delay	<input style="border: 1px solid #ccc;" type="text" value="0"/> ?
Hold Time	<input style="border: 1px solid #ccc;" type="text" value="0"/> ?
Triggered by DI	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Alarm Source	<input style="border: 1px solid #ccc;" type="text" value="NONE"/>

Item	Description	Default
Index	Indicate the ordinal of the list.	--
PHY Mode	Relay only on Relay Output device	Relay
Enable	Click the toggle button to enable/disable this Relay Output.	OFF
Alarm On Action	Relay Output initiates when there is an alarm. Selected from "High", "Low" or "Pulse". <ul style="list-style-type: none"> Relay On: The relay will connect Relay Off :The relay will disconnect 	Relay On
Alarm Off Action	Relay Output initiates when alarm removed. Selected from "High", "Low" or "Pulse". <ul style="list-style-type: none"> Relay On: The relay will connect Relay Off :The relay will disconnect 	Relay Off
Initial State	Specify the Relay Output status when powered on. Selected from "Last", "High" or "Low". <ul style="list-style-type: none"> Relay On: The relay will connect Relay Off :The relay will disconnect 	Relay On
Delay (unit: 100ms)	Set the delay time for DO alarm start-up. The first pulse will be generated after a "Delay". Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set the hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reach this specified time, DO will stop the action. Enter from 0 to 3000 seconds. (0=keep on until the next action)	0
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.

^ DI Status				
Index	Name	Level	Status	Count
1	DI1	High	Alarm off	
2	DI2	High	Alarm off	

^ Action Of Clear	
Counter Alarm Of DI 1	Clear
Counter Alarm Of DI 2	Clear

^ DO Status					
Index	Name	Relay Action	Level	Low-level Width	High-level Width
1	Relay1	Off	Low		
2	Relay2	Off	Low		

^ DO Control	
Level Of Relay1	Toggle
Level Of Relay2	Toggle

2.2.8 Serial Port

This section allows you to set the serial port parameters. The device supports two serial ports, which might be configured as RS232 or RS422 or 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

Serial Port Settings					
Index	Port	Enable	Type	Baud Rate	Application Mode
1	COM1	false	RS232	115200	Transparent
2	COM2	false	RS232	115200	Transparent

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

Serial Port Application Settings

Index:

Port:

Enable: ON OFF

Type:

Baud Rate:

Data Bits:

Stop Bits:

Parity:

Flow Control:

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Port	Show the current serial's name, read only.	COM1
Type	Select from "RS232", "RS422" "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

^ Data Packing

Packing Timeout	<input style="width: 90%;" type="text" value="50"/>	?
Packing Length	<input style="width: 90%;" type="text" value="1200"/>	

Item	Description	Default
Packing Timeout	Set the packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. The unit is milliseconds. Note: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.	50
Packing Length	Set the packet length. The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as soon it reaches the specified length.	1200

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

^ Server Setting

Application Mode	<input style="width: 90%;" type="text" value="Transparent"/>	v
Protocol	<input style="width: 90%;" type="text" value="TCP Client"/>	v
Server Address	<input style="width: 90%;" type="text"/>	
Server Port	<input style="width: 90%;" type="text"/>	

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

^ Server Setting

Application Mode	<input style="width: 90%;" type="text" value="Transparent"/>	v
Protocol	<input style="width: 90%;" type="text" value="TCP Server"/>	v
Local IP	<input style="width: 90%;" type="text"/>	
Local Port	<input style="width: 90%;" type="text"/>	

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

^ Server Setting

Application Mode	<input style="width: 90%;" type="text" value="Transparent"/>
Protocol	<input style="width: 90%;" type="text" value="UDP"/>
Local IP	<input style="width: 90%;" type="text"/>
Local Port	<input style="width: 90%;" type="text"/>
Server Address	<input style="width: 90%;" type="text"/>
Server Port	<input style="width: 90%;" type="text"/>

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

^ Server Setting

Application Mode	<input style="width: 90%;" type="text" value="Modbus RTU Gateway"/>
Protocol	<input style="width: 90%;" type="text" value="TCP Client"/>
Server Address	<input style="width: 90%;" type="text"/>
Server Port	<input style="width: 90%;" type="text"/>

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

^ Server Setting

Application Mode	<input style="width: 90%;" type="text" value="Modbus RTU Gateway"/>
Protocol	<input style="width: 90%;" type="text" value="TCP Server"/>
Local IP	<input style="width: 90%;" type="text"/>
Local Port	<input style="width: 90%;" type="text"/>

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

^ Server Setting

Application Mode	<input style="border: 1px solid #ccc;" type="text" value="Modbus RTU Gateway"/>
Protocol	<input style="border: 1px solid #ccc;" type="text" value="UDP"/>
Local IP	<input style="border: 1px solid #ccc;" type="text"/>
Local Port	<input style="border: 1px solid #ccc;" type="text"/>
Server Address	<input style="border: 1px solid #ccc;" type="text"/>
Server Port	<input style="border: 1px solid #ccc;" type="text"/>

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

^ Server Setting

Application Mode	<input style="border: 1px solid #ccc;" type="text" value="Modbus ASCII Gateway"/>
Protocol	<input style="border: 1px solid #ccc;" type="text" value="TCP Client"/>
Server Address	<input style="border: 1px solid #ccc;" type="text"/>
Server Port	<input style="border: 1px solid #ccc;" type="text"/>

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

^ Server Setting

Application Mode	<input style="border: 1px solid #ccc;" type="text" value="Modbus ASCII Gateway"/>
Protocol	<input style="border: 1px solid #ccc;" type="text" value="TCP Server"/>
Local IP	<input style="border: 1px solid #ccc;" type="text"/>
Local Port	<input style="border: 1px solid #ccc;" type="text"/>

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

^ Server Setting

Application Mode	<input style="border: 1px solid #ccc;" type="text" value="Modbus ASCII Gateway"/>
Protocol	<input style="border: 1px solid #ccc;" type="text" value="UDP"/>
Local IP	<input style="border: 1px solid #ccc;" type="text"/>
Local Port	<input style="border: 1px solid #ccc;" type="text"/>
Server Address	<input style="border: 1px solid #ccc;" type="text"/>
Server Port	<input style="border: 1px solid #ccc;" type="text"/>

Item	Description	Default
Application Mode	Select from "Transparent", "Modbus RTU Gateway" or "Modbus ASCII Gateway". <ul style="list-style-type: none"> Transparent: Device will transmit the serial data transparently 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 	Transparent
Protocol	Select from "TCP Client", "TCP Server", or "UDP". <ul style="list-style-type: none"> TCP Client: Device works as TCP client, initiate TCP connection to TCP server. 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 	TCP Client
Server Address	Enter the address of server which will receive the data sent from device's serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter device's LAN IP which will forward to the internet port of device.	Null

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

Status

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

Serial Port **Status**

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

2.2.9 BAM

This section allows you to set the BAM(Bridge Alarm Management) parameters.

HBT

Interface/BAM

Bridge Alert Management (BAM)

HBT

ALF

Status

^ General Settings

Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Interface	<input type="text" value="br_lan"/> v
Server IP address/domain	<input type="text"/>
Server Port	<input type="text"/>
Message Quantity	<input type="text" value="1"/>
Period	<input type="text" value="10sec"/> v ?

Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Interface	Set the message outgoing interface	br_lan
Server IP address/domain	Set the Server IP address and domain	Null
Server Port	Set the Server port	Null
Message Quantity	Set the message quantity	1
Period	Set the heart beat peride	10sec

ALF

Interface/BAM

Bridge Alert Management (BAM)

HBT **ALF** Status

^ General Settings

Enable ON OFF

Interface v

Server IP address/domain

Server Port

Message Quantity

Period v ?

Action ON OFF ?

Item	Description	Default
Enable	Click the toggle button to enable or disable the function.	OFF
Interface	Set the message outgoing interface	br_lan
Server IP address/domain	Set the Server IP address and domain	Null
Server Port	Set the Server port	Null
Message Quantity	Set the message quantity	1
HBT period	Set the heart beat period	10sec
Action	Click the toggle button to enable or disable the function. ON: Send ALF message when VPN session is connected. OFF: Do not send ALF message.	ON

Status

Interface/BAM

Bridge Alert Management (BAM)

HBT ALF **Status**

^ HBT

Sending counter

Index	IP Address

^ ALF

Sending counter

Index	IP Address

You can view detailed information [here](#).

2.3 Network

2.3.1 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

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). To switch between WAN connections, please drag the WAN interfaces into the required order.

Link

Status

^ Settings

Name	Type	Description	Weight	Firewall Zone	+
WWAN	Modem(4G/5G)	default wan	0	external	⋮ ↗ ✕

^ Advanced DNS Settings

Overrided DNS Enable ON OFF ?

Overrided Primary DNS

Overrided Secondary DNS

Click + to add a new WAN link.

Click ✕ 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	<input type="text" value="WWAN"/>	?
Type	<input type="text" value="Modem"/>	v
Interface	<input type="text" value="wwan"/>	v
Description	<input type="text" value="default wan"/>	
Weight	<input type="text" value="0"/>	?
Firewall Zone	<input type="text" value="external"/>	v

^ Link Settings

Name	<input type="text" value="WAN"/>	?
Type	<input type="text" value="Ethernet"/>	v
Interface	<input type="text" value="eth1"/>	v
Description	<input type="text"/>	
Weight	<input type="text" value="0"/>	?
Firewall Zone	<input type="text" value="external"/>	v

^ Link Settings

Name	<input type="text"/>	?
Type	<input type="text" value="VLAN"/>	v
Interface	<input type="text"/>	v
Description	<input type="text"/>	
Weight	<input type="text" value="0"/>	?
Firewall Zone	<input type="text" value="external"/>	v

^ Link Settings

Name	<input type="text"/>	?
Type	<input type="text" value="WIFI"/>	v
Interface	<input type="text" value="wlan0"/>	v
SSID	<input type="text" value="router"/>	
Password	<input type="text"/>	
Description	<input type="text"/>	
Weight	<input type="text" value="0"/>	?
Firewall Zone	<input type="text" value="external"/>	v

Item	Description	Default
Name	The name of link.	--
Type	The types of connectivity. <ul style="list-style-type: none"> 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 2.2.2 Cellular . If the type is Ethernet, please see the 2.2.1 Ethernet . If the type is VLAN, please see the 2.2.6 VLAN .	--
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 2.3.5 Firewall .	--

^ IPv4 Settings

IPv4 Connection Type	<input type="text" value="DHCP"/>	?
----------------------	-----------------------------------	---

Item	Description	Default
IPv4 Connection Type	The type of IPv4 connection. <ul style="list-style-type: none"> DHCP. PPPoE. Manual. Disable. Enter the parameters accordingly.	DHCP

^ Health Detection Settings ?

Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
IPv4 Primary Server	<input type="text" value="8.8.8.8"/>
IPv4 Secondary Server	<input type="text" value="1.2.4.8"/>
Interval	<input type="text" value="300"/> ?
Timeout	<input type="text" value="5"/> ?
Reconnect Tries	<input type="text" value="3"/> ?
Recover Tries	<input type="text" value="3"/> ?

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
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 unsuccessful.	3
Recover Tries	Recovery this link in case of sequential probes are successful.	3

Advanced DNS Settings

^ Advanced DNS Settings

Overridden DNS Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Overridden Primary DNS	<input type="text"/>
Overridden Secondary DNS	<input type="text"/>

Item	Description	Default
Enable	Toggle the button to enable the overridden DNS function	OFF
Overridden Primary DNS	Define a primary DNS server address used by the link	NULL
Overridden Secondary DNS	Define a secondary DNS server address for the link	NULL

Status

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

Link **Status**



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


2.3.2 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	Type	Description	Firewall Zone	
LAN1	Bridge	default lan	internal	+
				 

Click  to add a new LAN link.

Click  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	<input type="text" value="LAN1"/>	?
Type	<input type="text" value="Bridge"/>	v
Interface	<input type="text" value="br_lan"/>	v
Description	<input type="text" value="default lan"/>	
Firewall Zone	<input type="text" value="internal"/>	v

Item	Description	Default
Name	The name of the LAN link.	--
Type	The types of connectivity. Select from "Bridge", "Ethernet" and "VLAN". <ul style="list-style-type: none"> Bridge: connected by Bridge network. Ethernet: connected by Ethernet wired network. VLAN: connected by VLAN network. 	Bridge
Interface	Set the related interface. If the type is Bridge, please see the 2.2.3 Bridge . If the type is Ethernet, please see the 2.2.1 Ethernet . If the type is VLAN, please see the 2.2.6 VLAN .	--
Description	The description of the link.	--
Firewall Zone	The chosen set of firewall rules, please see the 2.3.5 Firewall .	internal

^ ip4 Settings

IPv4 Address	<input type="text" value="192.168.0.1/24"/>	+
--------------	---	---

^ DHCPv4 Settings

IP Pool Start	<input type="text" value="192.168.0.2"/>	
IP Pool End	<input type="text" value="192.168.0.100"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	
Lease Time	<input type="text" value="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

Status

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

Network/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
Status

^ Interface Status

Interface	MAC Address	IPv4 Address
br_lan	34:FA:40:25:25:08	192.168.0.1

^ Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	192.168.0.75	00:E0:4C:68:00:59	br_lan	0s

2.3.3 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
Status

^ Static Route Table

Index	Description	Destination	Netmask	Gateway	Interface	+

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

^ Static Route

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Destination	<input type="text"/>
Netmask	<input type="text"/>
Gateway	<input type="text"/>
Metric	<input type="text" value="0"/>
MTU	<input type="text" value="1500"/>
Interface	<input style="border-bottom: none; border-right: none; border-top: none; border-left: none; width: 100%;" type="text" value="br_lan"/> v

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 among multiple feasible routes to a destination. The route will go in the direction of the gateway with the lowest metric value.	0
MTU	Enter the MTU value, 1280~1500.	1500
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.

Static Route
Status

^ Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	0.0.0.0	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

2.3.4 Policy Route

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

Policy Route

Policy Route

^ Match settings

Index	Name	Protocol	Source Address	Destination address	Interface	+

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

^ Match settings

Index	<input style="width: 90%;" type="text" value="1"/>	
Name	<input style="width: 100%;" type="text"/>	
Protocol	<input style="border-bottom: 1px solid #ccc;" type="text" value="TCP"/> v	
Hooks	<input style="border-bottom: 1px solid #ccc;" type="text" value="PREROUTING"/> v	
Source Address	<input style="width: 95%;" type="text"/>	?
Source Port	<input style="width: 95%;" type="text"/>	?
Source MAC	<input style="width: 95%;" type="text"/>	?
Destination address	<input style="width: 95%;" type="text"/>	?
Destination port	<input style="width: 95%;" type="text"/>	?

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", "ICMP" and "IGMP".	TCP-UDP
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

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

2.3.5 Firewall

Firewall makes use of Linux iptables to control inbound and outbound traffic, the router has already been configured to meet IEC61162-460 requirements.

General Setting

General Settings | Port Forwards | Traffic Rules | Custom Rules | Status

^ General Settings

Enable DOS protection ON OFF

Duration of direct connection ?

Input

Output

Forward

^ Zones ?

Name	Input	Output	Forward	
external	Drop	Accept	Drop	
internal	Accept	Accept	Drop	

Item	Description	Default
Enable DOS protection	click the toggle button to enable/disable.	ON
Duration of direct connection	<ul style="list-style-type: none"> The duration(hour) of direct connection Each rule is valid for four hours	4
Input	Default action of the Input chain if a packet does not match any exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Accept
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Drop

Note: The general setting is used as a default firewall setting unless specified.

^ Zones ?				
Name	Input	Output	Forward	+
external	Drop	Accept	Drop	
internal	Accept	Accept	Accept	

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	<input type="text" value="external"/>
Input	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Drop"/> v
Output	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Accept"/> v
Forward	<input style="border: none; border-bottom: 1px solid #ccc;" type="text" value="Drop"/> v
Masquerading	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
MSS clamping	<input checked="" type="checkbox"/> ON <input type="checkbox"/> 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 exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Drop
Output	Default action of the Output chain if a packet does not match any exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Accept
Forward	Default action of the Forward chain if a packet does not match any exist rule on that chain. <ul style="list-style-type: none"> Accept: Packet gets to continue to the next chain. Drop: Packet is stopped and deleted. 	Drop
Masquerading	Click the toggle button to enable/disable. MASQUERADE is an 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).	ON
MSS clamping	Click the toggle button to enable/disable. MSS clamping is a 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.	ON

^ DMZ Settings

Enable DMZ ON OFF

Host IP Address

Source IP Address ?

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.	OFF
Host IP Address	Enter the IP address of the DMZ host on your internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any	Null

	addresses.	
Destination IP Address	Set the address which the DMZ host can talk to . Null means for any addresses.	Null

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

Port Forwards

General Settings

Port Forwards

Traffic Rules

Custom Rules

Status

^ Port Forwards 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 + to add one. The maximum count is **50**.

Port Forwards Rules

Index	<input type="text" value="1"/>
Name	<input type="text"/>
IPv4 Source Address	<input type="text"/> +
Protocol	TCP-UDP v
Source zone	external v
External Port	<input type="text"/> ?
Destination zone	external v
Internal IP Address	<input type="text"/>
Internal port	<input type="text"/> ?

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. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
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 zone.	external
External Port	Match incoming traffic directed at the given destination port or port range on this host. Select a configured zone.	Null
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 Forwards **Traffic Rules** Custom Rules Status

Traffic Rules

Index	Name	Address Family	Protocol	Source zone	Action	+

This window allows you to view the traffic rules.

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

^ Traffic Rules

Index	<input type="text" value="1"/>
Name	<input type="text"/>
Address Family	<input type="text" value="IPv4"/> v
Protocol	<input type="text" value="TCP-UDP"/> v
Source zone	<input type="text" value="device_output"/> v
IPv4 Source Address	<input type="text"/> ?
Source Port	<input type="text"/> ?
Source MAC	<input type="text"/> ?
Output zone	<input type="text" value="any_forward"/> v
IPv4 Destination Address	<input type="text"/> + ?
Destination port	<input type="text"/> ?
Action	<input type="text" value="Drop"/> v

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	The name of the rule.	Null
Address family	Select "IPv4" as your application required.	IPv4
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.	device_output
IPv4 Source Address	The IPv4 address or network segment used by connecting hosts. The rule will apply only to hosts that connect from IP addresses specified in this field.	Null
Source Port	Port number(s) used by the connecting host. 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.	Null
Source MAC	MAC address of connecting hosts. 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.	Null
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
Multi-Destination Option	Click + to add more destination address, the max quantity is 20	Null
Destination port	The port number to which the incoming connection will be redirected.	Null
Action	Select from "Accept", or "Drop" as your application required.	Null

Custom Rules

General Settings Port Forwards Traffic Rules **Custom Rules** Status

^ Custom Iptables 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:

Name:

Family:

Rule: ?

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Name	Enter a description for this.	Null
Family	Select the "IPv4" 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.

General Settings Port Forwards Traffic Rules Custom Rules **Status**

```

^ IPv4 Filter
 0  0  ACCEPT  tcp  --  *  *  0.0.0.0/0  0.0.0.0/0  tcp dpt:22
12 562 ACCEPT  tcp  --  *  *  0.0.0.0/0  0.0.0.0/0  tcp dpt:80
 0  0  ACCEPT  tcp  --  *  *  0.0.0.0/0  0.0.0.0/0  tcp dpt:443
 0  0  ACCEPT  icmp --  *  *  0.0.0.0/0  0.0.0.0/0  icmp type 8
 0  0  ACCEPT  all  --  *  *  0.0.0.0/0  0.0.0.0/0  ctstate DNAT
86 10647 zone_internal_src_ACCEPT all -- *  *  0.0.0.0/0  0.0.0.0/0

Chain zone_internal_output (1 references)
pkts bytes target  prot opt in  out  source  destination
 28 6776 output_internal_rule all -- *  *  0.0.0.0/0  0.0.0.0/0
 28 6776 zone_internal_dest_ACCEPT all -- *  *  0.0.0.0/0  0.0.0.0/0

Chain zone_internal_src_ACCEPT (1 references)
pkts bytes target  prot opt in  out  source  destination
86 10647 ACCEPT  all  --  br_lan *  0.0.0.0/0  0.0.0.0/0  ctstate NEW,UNTRACKED
Chain zone_internal_src_DROP (0 references)

```

2.3.6 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

Upload Bandwidth

Download Bandwidth

ON
OFF

?

?

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

Priority Definition

^ Priority Definition ?

Index	Priority	Bandwidth	Borrow Spare Bandwidth	
1	Highest	20	true	✕
2	High	20	true	✕
3	Normal	20	true	✕
4	Low	20	true	✕
5	Lowest	20	true	✕

Click to set the priority.

^ Priority Definition

Index:

Priority: v

Bandwidth: ?

Borrow Spare Bandwidth: ON OFF ?

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

IPv4 QoS Rules

^ IPv4 QoS Rules

Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority	
+							

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

^ QoS Rules

Index:

Source Address: ?

Source Port: ?

Source MAC: ?

Target Address: ?

Target Port: ?

Protocol: v

Priority: 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 application required.	Normal

2.4 VPN

2.4.1 IPsec

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

General

General
Tunnel
Status

^ General Settings

Keepalive

?

Optimize DH Exponent Size

ON

OFF

?

Debug Enable

ON

OFF

Enable Backup Gateway

ON

OFF

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

Tunnel

General **Tunnel** Status

^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+

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

General Setting

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Link Binding	<input type="text" value="wwan"/> v
Gateway	<input type="text"/> ?
Protocol	<input type="text" value="ESP"/> v
Mode	<input type="text" value="Tunnel"/> v
Local Subnet	<input type="text"/> ?
Remote Subnet	<input type="text"/> ?
IKE Type	<input type="text" value="IKEv1"/> v
Negotiation Mode	<input type="text" value="Main"/> v
Initiation Mode	<input type="text" value="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	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it 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 	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> ESP: Use the ESP protocol AH: Use the AH protocol 	ESP
Local Subnet	Enter the local subnet's address with mask protected by IPsec, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter the remote subnet's address with mask protected by IPsec, e.g. 10.8.0.0/24	Null
IKE Type	Select from "IKEv1" and "IKEv2".	IKEv1
Negotiation Mode	Select from "Main" and "Aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
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 the inner headers of IP packets.	OFF
Enable Forceencaps	Force UDP encapsulation for ESP packets even if no NAT situation is detected.This may help to surmount restrictive firewalls.	OFF
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, e.g. protostack=netkey; plutodebug=none	Null

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	v ?

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	v
Remote Certificate(Optional)	None	v
Private Key	None	v
CA Certificate	None	v
Private Key Password		
IKE Lifetime	86400	v ?

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

^ 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	?

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		?
Password		?
IKE Lifetime	86400	?

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

^ PHASE 1

Encryption Algorithm	<input type="text" value="3DES"/>	v
Authentication Algorithm	<input type="text" value="SHA1"/>	v
IKE DH Group	<input type="text" value="DHgroup2"/>	v
Authentication Type	<input type="text" value="xAuth CA"/>	v
Local Certificate	<input type="text" value="None"/>	v
Remote Certificate(Optional)	<input type="text" value="None"/>	v
Private Key	<input type="text" value="None"/>	v
CA Certificate	<input type="text" value="None"/>	v
Private Key Password	<input type="text"/>	
Username	<input type="text"/>	?
Password	<input type="text"/>	?
IKE Lifetime	<input type="text" value="86400"/>	?

Item	Description	Default
Encrypt Algorithm	Select from "3DES", "AES128", "AES192" and "AES256". <ul style="list-style-type: none"> 3DES: Use 168-bit 3DES encryption algorithm in CBC mode AES128: Use 128-bit AES encryption algorithm in CBC mode AES128: Use 192-bit AES encryption algorithm in CBC mode AES256: Use 256-bit AES encryption algorithm in CBC mode 	3DES
Authentication Algorithm	Select from "MD5", "SHA1", "SHA2 256", "SHA2 384" or "SHA2 512" .	MD5
IKE DH Group	Select from "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" .	DHgroup2
Authentication Type	Select from "PSK", "CA", "xAuth PSK", "PKCS#12" and "xAuth CA" to be used in IKE negotiation. <ul style="list-style-type: none"> PSK: Pre-shared Key CA: Certification Authority xAuth: Extended Authentication to AAA server PKCS#12: Exchange digital certificate authentication 	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from "Default", "Address", "FQDN" and "User FQDN" . <ul style="list-style-type: none"> 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 	Default

Item	Description	Default
	router, e.g., test.robustel.com <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> 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 	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key under the “CA” and “xAuth CA” authentication types.	Null
Username	Enter the username used for the “xAuth PSK” and “xAuth CA” authentication types.	Null
Password	Enter the password used for the “xAuth PSK” and “xAuth CA” authentication types.	Null

PHASE 2

^ PHASE 2

Encryption Algorithm	3DES	v
Authentication Algorithm	SHA1	v
PFS Group	PFS(N/A)	v
SA Lifetime	28800	?
DPD Interval	30	?
DPD Failures	150	?

Item	Description	Default
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192” or “AES256” when you select “ESP” in “Protocol”. Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256” or “SHA2 512” to be used in SA negotiation.	MD5
PFS Group	Select from “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 smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is 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.	30
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.

General
Tunnel
Status

^ IPsec Tunnel Status

Index	Description	Status	Uptime

2.4.2 OpenVPN

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

OpenVPN

OpenVPN

Status

^ Tunnel Settings

Index	Enable	Description	Mode	Peer Address	+

^ Password Manage

Index	Username		+

^ Client Manage

Index	Enable	Common Name	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	<input style="width: 100%;" type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input style="width: 100%;" type="text"/>
Mode	<input style="width: 100%;" type="text" value="P2P"/> ?
TLS Mode	<input style="width: 100%;" type="text" value="None"/> ?
Protocol	<input style="width: 100%;" type="text" value="UDP"/>
Peer Address	<input style="width: 100%;" type="text"/>

Peer Port	<input type="text" value="1194"/>
Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="None"/> v ?
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Verbose Level	<input type="text" value="0"/> v ?

^ Advanced Settings

Expert Options	<input type="text"/> ?
----------------	------------------------

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> v ?
Protocol	<input type="text" value="UDP"/> v
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v

Authentication Type	None	?
Renegotiation Interval	86400	?
Keepalive Interval	20	?
Keepalive Timeout	120	?
TUN MTU	1500	
Max Frame Size		
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
Verbose Level	0	?

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

^ General Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	
Mode	Server
Protocol	UDP
Listen IP Address	
Listen Port	1194
Interface Type	TUN

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

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

Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="None"/> ?
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Keepalive Interval	<input type="text" value="20"/> ?
Keepalive Timeout	<input type="text" value="120"/> ?
TUN MTU	<input type="text" value="1500"/>

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

Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="Preshared"/> ?
Pre-Share Key	<input type="text" value="None"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
Keepalive Interval	<input type="text" value="20"/> ?


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

Listen IP Address	<input type="text"/>
Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="Password"/> ?
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
Keepalive Interval	<input type="text" value="20"/> ?

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

Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="X509CA"/> ?
Root CA	<input type="text" value="None"/>
Certificate File	<input type="text" value="None"/>
Private Key	<input type="text" value="None"/>
Private Key Password	<input type="text"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="10.8.0.2"/>
Encrypt Algorithm	<input type="text" value="BF"/>

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

Listen Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<input type="text" value="X509CA Password"/> 
Root CA	<input type="text" value="None"/>
Certificate File	<input type="text" value="None"/>
Private Key	<input type="text" value="None"/>
Private Key Password	<input type="text"/>
Local IP	<input type="text" value="10.8.0.1"/>
Remote IP	<input type="text" value="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
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 server.	Null
Peer Port	Enter the end-to-end listener port or the listener port of the OpenVPN server.	1194
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 interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.	TUN
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA”, “X509CA password”. Note:None and Preshared types only used for P2P mode. It must to add account from the User Management, when using server mode with password authentication.	Null
Private Key Password	Enter the private key password under "X509CA" and "X509CA password" authentication.	Null
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES-128”, “AES-192” and	BF

Item	Description	Default
	"AES-256". <ul style="list-style-type: none"> BF: Use 128-bit BF encryption algorithm in CBC mode DES: Use 64-bit DES encryption algorithm in CBC mode DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode AES128: Use 128-bit AES encryption algorithm in CBC mode AES192: Use 192-bit AES encryption algorithm in CBC mode AES256: Use 256-bit AES encryption algorithm in CBC mode 	
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	Select the level of the output log and values from 0 to 11. <ul style="list-style-type: none"> 0: No output except fatal errors 1~4: Normal usage range 5: Output R and W characters to the console for each packet read and write 6~11: Debug info range 	0

^ Advanced Settings

Expert Options ?

Item	Description	Default
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ','.	Null

Client Management

^ Client Manage

Index	Enable	Common Name	Client IP Address	
				+

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Common Name	<input type="text"/> ?
Client IP Address	<input type="text"/>

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the switch button to enable/disable this option.	ON
Common Name	Specify a common name for the client.	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.

OpenVPN
Status

^ OpenVPN Tunnel Status

Index	Description	Status	Mode	Uptime	Local IPv4	Local IPv6

^ OpenVPN Client List

Index	Common Name	Real IP	Port	Virtual IPv4	Virtual IPv6

2.4.3 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 Settings

Index	Enable	Description	Remote IP Address	+

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

^ Tunnel Settings

Index

Enable

ON

OFF

Description

Remote IP Address

Local Virtual IP Address

Local Virtual Netmask/Prefix Length

?

Remote Virtual IP Address

Enable Default Route

ON

OFF

Enable NAT

ON

OFF

Secrets

Link Binding

wwan

v

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Enable	Click the toggle button to enable/disable this GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates data packets so that it can route packets of other protocols in an IP network.	ON
Description	Enter a description for this GRE tunnel.	Null
Remote IP Address	Set the remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set the local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask/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 the traffics of the router will go through the GRE VPN.	OFF

Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when router under NAT environment.	OFF
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
Status

^ GRE tunnel status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

2.4.4 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

Enable User LED

?

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

PPTP Server

General
PPTP Server
PPTP Client
Status

^ PPTP Server Settings

Enable PPTP Server ON OFF

Username ?

Password ?

Local IP

Start IP

End IP

Authentication pap v

Enable NAT ON OFF

Expert Options noaccomp nopcomp nodeflate nobsdcomp 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".	pap
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 separated by a ';' .	Null
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 Client** Status

PPTP Client 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: ?

Password: ?

Authentication: pap v

Enable NAT ON OFF
 All Traffic via This Interface ON OFF
 Remote Subnet
 Remote Subnet Mask
 Expert Options

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".	pap
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This Interface	Click the toggle button to enable/disable this function.	OFF
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 separated by a ';' .	Null

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 Server](#)
[PPTP Client](#)
[Status](#)

^ PPTP Server Status

Index	Remote IP Address	Uptime

^ PPTP Client Status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

2.4.5 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
 ON OFF ?

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

L2TP Server

General
L2TP Server
L2TP Client
Status

^ L2TP Server Settings

Enable L2TP Server
 ON OFF

Username ?

Password ?

Local IP

Start IP

End IP

Tunnel Secrets	<input type="text"/>
Authentication	<input type="text" value="pap"/>
Port	<input type="text" value="1701"/>
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Expert Options	<input type="text" value="noaccomp nopcomp nodeflate nobsdcomp r"/>
Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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”.	pap
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 separated by a ‘;’ .	Null
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 L2TP server. The maximum count is **20**.

^ Static Route

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Client IP	<input type="text"/> ?

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 Client** Status

^ L2TP Client Settings

Index	Enable	Description	Server Address	Authentication	Remote Subnet	Remote Subnet ...	
+							

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

^ L2TP Client Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Server Address	<input type="text"/>
Username	<input type="text"/> ?
Password	<input type="text"/> ?
Authentication	<input type="text" value="pap"/> v
Tunnel Secrets	<input type="text"/>
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
All Traffic via This Interface	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Expert Options	<input type="text" value="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".	pap
Tunnel Secrets	Enter the tunnel password.	Null
Enable NAT	Click the toggle button to enable/disable NAT.	ON
All Traffic via This Interface	Click the toggle button to enable/disable this function.	OFF
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 separated by a ';' .	Null

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
L2TP Server
L2TP Client
Status

^ L2TP Server Status

Index	Remote IP Address	Uptime

^ L2TP Client Status

Index	Description	Status	Local IP Address	Remote IP Address	Uptime

2.4.6 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 ON OFF

Description

DMVPN Type v

Link Binding v

Hub Address ?

GRE Settings

GRE Local IP Address ?

GRE HUB IP Address ?

GRE Netmask

GRE Secrets

GRE MTU

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: Single hub mode Dual-hub: Dual hub mode	Default
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

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

^ SA Settings

SA Encryption Algorithm	<input type="text" value="3DES"/>
SA Authentication Algorithm	<input type="text" value="SHA1"/>
PFS Group	<input type="text" value="PFS(N/A)"/>

^ Nhrp Settings

Enable Zebra VTY	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NHRP VTY	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Nhrp Holdtime(s)	<input type="text" value="7200"/>

Item	Description	Default
IKE Type	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 correct.	Main
Local ID Type	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 Algorithm	Select from "DES", "3DES" and "AES128" to be used in IKE negotiation. 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.	3DES
IKE Authen Algorithm	Select from "MD5" and "SHA1" to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
IKE DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be 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.	MODP1024_2
Authentication Type	Select Authentication Type	PSK
PSK Secrets	Enter PSK secret key.	Null
SA Encryption Algorithm	Select the SA Encryption Algorithm from "DES", "3DES", "AES 128", "AES 192", "AES 256".	3DES
SA Authentication Algorithm	Select the SA Authentication Algorithm from "MD5", "SHA1", "SHA2 256", "SHA2 512".	SHA1
PFS Group	Select the PFS Group.	PFS(N/A)

Status

The status bar allows to view DMVPN connection status.

DMVPN	Status	x509
-------	--------	------

^ DMVPN Status	
Status	
Uptime	

X509

^ X509 Settings ?

Local Certificate	<input type="button" value="Choose File"/> No file chosen ↑
Private Key	<input type="button" value="Choose File"/> No file chosen ↑
CA Certificate	<input type="button" value="Choose File"/> No file chosen ↑

^ Local Certificate

Index	File Name	File Size	Modification Time

^ Private Key

Index	File Name	File Size	Modification Time

^ CA Certificate

Index	File Name	File Size	Modification Time

x509		
Item	Description	Default
X509 Settings		
Root CA	Click "Choose File" to locate Root CA file and then import this file into your device.	--
Certificate File	Click "Choose File" to locate Certificate file, and then import this file into your device.	--
Private Key	Click "Choose File" to locate Private Key file, and then import this file into your device.	--
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

2.5 Services

2.5.1 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.

Syslog

^ Syslog Settings

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

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

Syslog

^ Syslog Settings

Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
Syslog Level	<input type="text" value="Debug"/>	v
Save Position	<input type="text" value="RAM"/>	v ?
Log to Remote	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
Add Identifier	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
Remote IP Address	<input type="text"/>	
Remote Port	<input type="text" value="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 high. The lower level will output more syslog in details.	Debug
Save Position	Select the save position from “RAM”, “NVM” or “Console”. The data will be cleared after reboot when choose “RAM”. Note: It's not recommended that you save syslog to NVM (Non-Volatile Memory)	NVM

	for a long time.	
Log to Remote	Click the toggle button to enable/disable this option. Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	ON
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add serial number to syslog message which used for loading Syslog to RCMS.	OFF
Remote IP Address	Enter the IP address of syslog server when enabling the “Log to Remote” option.	Null
Remote Port	Enter the port of syslog server when enabling the “Log to Remote” option.	514

2.5.2 Event

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

Event

Event

Notification

Query

^ General Settings

Signal Quality Threshold	<input style="width: 90%;" type="text" value="0"/>	?
Temperature Threshold	<input style="width: 90%;" type="text" value="0"/>	?
Estimated Remaining Flash Lifetime	<input style="width: 90%;" type="text" value="20%-30%"/>	v

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

Notification

Event **Notification** Query

^ Event Notification Group Settings

Index	Description	Send SMS	Send Email	DO Control	Save to NVM	
+						

Click button to add an Event parameters.

^ General Settings

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Send SMS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Send Email	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DO Control	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Save to NVM	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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 send notification to the specified phone numbers via SMS if event occurs. Set the related phone number in "3.21 Services > Email", and use ';' to separate each number.	OFF
Send Email	Click the toggle button to enable/disable this option. When enabled, the router will send notification to the specified email box via Email if event occurs. Set the related email address in "3.21 Services > Email".	OFF
DO Control	Click the toggle button to enable / disable this option. After it is turned on, the event router will send it to the corresponding DO in the form of Low / High level.	OFF
Save to NVM	Click the toggle button to enable/disable this option. Enable to save event to nonvolatile memory.	OFF

Event Selection ?

System Startup	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Reboot	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Time Update	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Configuration Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Network Type Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Stats Clear	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Traffic Overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Poor Signal Quality	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Wan data traffic stats clear	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Wan data traffic overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Link Switching	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

LAN Port Link Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN Port Link Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
USB Device Connect	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
USB Device Remove	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS Update Success	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DDNS Update Fail	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Received SMS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
SMS Command Execute	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 ON	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 OFF	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 1 Counter Overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 ON	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 OFF	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
DI 2 Counter Overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Excessive Temperature	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Emmc Life Time Alert	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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

Save Position RAM v

Filtering

```

Mar 27 17:54:12, switch link, from WWAN1 to WWAN2
Mar 27 17:57:15, switch link, from WWAN2 to WWAN1
Mar 27 17:59:28, LAN port link down, eth0
Mar 27 17:59:28, LAN port link down, eth1
Mar 27 17:59:34, LAN port link up, eth1
Mar 27 17:59:40, LAN port link up, eth0
Mar 27 17:59:40, LAN port link down, eth1
Mar 27 17:59:46, LAN port link up, eth1
Mar 27 18:00:18, switch link, from WWAN1 to WWAN2
Mar 27 18:00:46, LAN port link down, eth1
Mar 27 18:03:21, switch link, from WWAN2 to WWAN1
Mar 27 18:06:25, switch link, from WWAN1 to WWAN2
Mar 27 18:09:28, switch link, from WWAN2 to WWAN1
Mar 27 18:12:31, switch link, from WWAN1 to WWAN2
Mar 27 18:15:34, switch link, from WWAN2 to WWAN1
Mar 27 18:18:37, switch link, from WWAN1 to WWAN2
Mar 27 18:21:40, switch link, from WWAN2 to WWAN1
Mar 27 18:24:44, switch link, from WWAN1 to WWAN2
                    
```

Clear
Refresh

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

2.5.3 NTP

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

NTP

NTP
Status

^ Timezone Settings

Time Zone

Asia-Shanghai v

Item	Description	Default
Time Zone	Click the drop down list to select the time zone you are in.	UTC +08:00

^ 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 synchronize time with the NTP server.	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) synchronizing the NTP client time with the NTP server's. Minutes wait for next update, and 0 means update only once.	0

^ NTP 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 the NTP server option.	OFF
Primary NTP Server	Enter the primary NTP server	pool.ntp.org
Secondary NTP Server	Enter the secondary NTP server	Null
NTP Update Interval	Enter the NTP update interval, 0 means update only once.	0

^ 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.

NTP
Status

^ Time

System Time	2022-05-07 16:27:05
PC Time	2022-05-07 16:27:07 Sync
Last Update Time	2022-05-07 08:48:25

2.5.4 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 [3.1.2 SMS Remote Control](#).

SMS

SMS
SMS Testing

^ SMS Management Settings ?

Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Authentication Type	<input type="text" value="Password"/> ?
Phone Number	<input type="text"/> + ?

Item	Description	Default
Enable	Click the toggle button to enable/disable the SMS Management option. Note: If this option is disabled, the SMS configuration is invalid.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum” or “Both”. Password: Use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; ...” Note: Set the WEB manager password in System > User Management section. Phonenum: Use the Phone number for authentication, and user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; ...” Both: Use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd1; cmd2; ...”	Password
Phone Number	Set the phone number used for SMS management, and click + to add new phone number. Note: It can be null when choose “Password” as the authentication type.	Null

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.	--

2.5.5 Email

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

Email

^ Email Settings

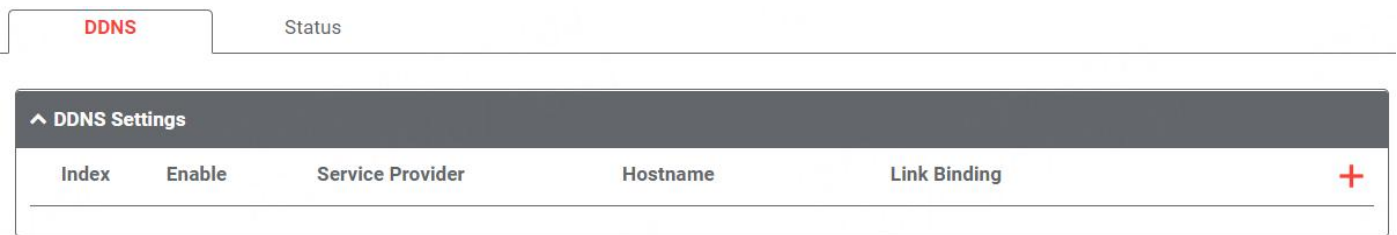
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
Enable TLS/SSL	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?	
Enable STARTTLS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
Outgoing Server	<input type="text"/>	
Server Port	<input type="text" value="25"/>	
Timeout	<input type="text" value="10"/>	?
Auth Login	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?	
Username	<input type="text"/>	
Password	<input type="text"/>	
From	<input type="text"/>	
Subject	<input type="text"/>	


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

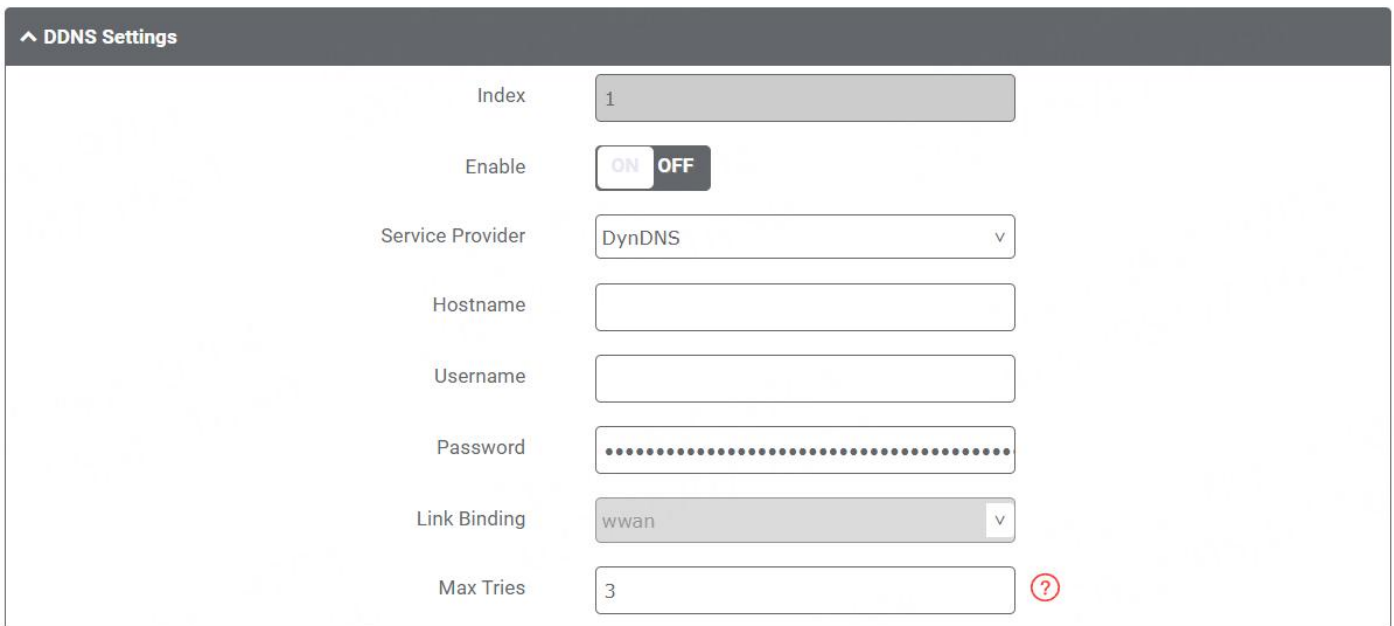
2.5.6 DDNS

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

DDNS



Click  to add a new Dynamic Domain Name Server.



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

^ DDNS Settings

Index	<input style="width: 100%;" type="text" value="1"/>
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Service Provider	<input style="width: 100%;" type="text" value="Custom"/> v
URL	<input style="width: 100%;" type="text"/>
Max Tries	<input style="width: 100%;" type="text" value="3"/> ?

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

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.

2.5.7 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	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Interface	<input type="text" value="br_Jan"/> v
Group ID	<input type="text" value="1"/>
Priority	<input type="text" value="100"/>
Interval	<input type="text" value="1"/> ?
Virtual IP Address	<input type="text"/>

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

Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Server	<input type="text" value="8.8.8.8"/>
Interval	<input type="text" value="300"/> ?

Item	Description	Default
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

2.5.8 SSH

Device supports SSH password access and secret-key access.

SSH

^ SSH Settings

Enable

ON
 OFF

Port

Disable Password Logins

ON
 OFF

Authorized Keys

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

2.5.9 GNSS

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

GNSS

GNSS
Status
Map

^ General Settings

Enable GNSS

ON
 OFF

Sync GNSS Time

ON
 OFF

^ RS232 Report Settings

Report to RS232	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Report GGA Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Report VTG Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Report RMC Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Report GSV Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

^ GNSS Servers

Index	Enable	Protocol	Local Address	Local Port	Server Address	Server Port
+						

Click + to add a new GNSS Server. The maximum count is 5.

^ Server Settings

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Protocol	TCP Client v
Server Address	
Server Port	
Send GGA Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Send VTG Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Send RMC Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Send GSV Sentence	<input type="checkbox"/> ON <input checked="" type="checkbox"/> 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/Local Address	Server or local IP address.	Null
Server/Local Port	Server or local IP port.	Null
Send GGA Sentence	Click the toggle button to enable/disable this option.	OFF
Send VTG Sentence	Click the toggle button to enable/disable this option.	OFF
Send RMC Sentence	Click the toggle button to enable/disable this option.	OFF
Send GSV Sentence	Click the toggle button to enable/disable this option.	OFF

^ Advanced Settings

Add SN as GNSSID ON OFF ?

Self-define GNSSID Prefix ?

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

Status

GNSS
Status
Map

^ GNSS Status

Status

UTC Time

Last Fixed Time

Satellites In Use

Satellites In View

Latitude

Longitude

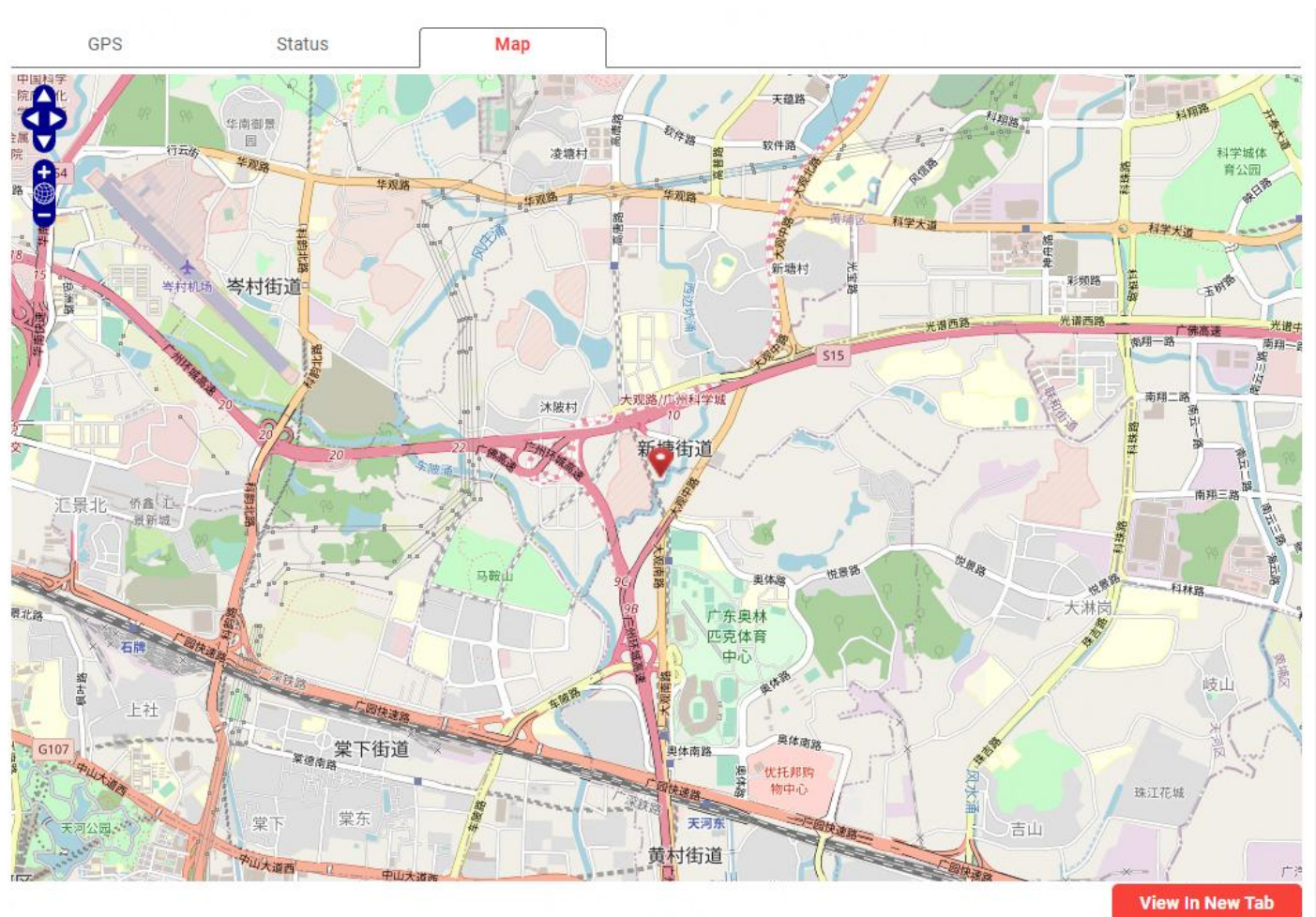
Altitude

Speed

Item	Description
Status	Shows the current GNSS status of the router.
UTC Time	Shows the UTC of satellite. Note: 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	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.

Map

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



Click the [View In New Tab](#) button to view in a new tab.

2.5.10 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 Settings

Enable RCMS	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable RobustLink	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable RobustVPN	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Paho log detail enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
RCMS Environment	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">RCMS Cloud International v</div>

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

^ Data Management

KeepAlive	<input style="width: 90%;" type="text" value="600"/> v ?
Dynamic Report Capture	<input style="width: 90%;" type="text" value="60min"/> v ?
Dynamic Report Upload	<input style="width: 90%;" type="text" value="60min"/> v ?
GPS Reporting Settings	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">On GPS co-ordinate change</div> v ?
GPS Distance Threshold	<input style="width: 90%;" type="text" value="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	600

	more data.	
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	Select GPS Reporting way: <ul style="list-style-type: none"> - On GPS co-ordinate change - Report when GPS is updated - Only with Dynamic Report - Collect and report in sync with the Data Collection Interval and Data Reporting Frequency 	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

Ping Timeout ?

Ping Count ?

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

Status

RCMS

Event Selection

Status

^ Connection Status	
RobustLink Status	Connected
RobustLink Last Connected	2023-05-30 13:54:59
RobustVPN Status	
RobustVPN Last Connected	Never
RobustVPN Virtual IP	
RobustVPN SubNet Address	

Item	Description
RobustLink Status	Show the status of RobustLink
RobustLink 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

2.5.11 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
MIBS

^ SNMP Agent Settings

Enable SNMP Agent	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Port	<input type="text" value="161"/>
OEM Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OEM Enterprise	<input type="text"/>
OEM Platform	<input type="text"/>
Version	<input type="text" value="SNMPv3"/> v
Location Info	<input type="text"/>
Contact Info	<input type="text"/>
System Name	<input type="text"/>
Authentication Algorithm	<input type="text" value="MD5"/> v
Privacy Algorithm	<input type="text" value="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		
Authentication Algorithm	Select from "MD5", "SHA".	MD5
Privacy Algorithm	Select from "DES", "AES".	DES

SNMP Trap

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

SNMP Agent
SNMP Trap
MIBS

^ SNMP Trap Settings

Enable SNMP Trap

ON
 OFF

Version

Receiver Address

Receiver Port

^ SNMPv3 Authentication

Username

Authentication Algorithm

Authentication Password

Privacy Algorithm

Privacy Password

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.

Event Selection ?

System Startup	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Reboot	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
System Time Update	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Configuration Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Network Type Change	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Stats Clear	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Cellular Data Traffic Overflow	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Poor Signal Quality	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Link Switching	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WWAN Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
IPSec Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
OpenVPN Connection Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN Port Link Up	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LAN Port Link Down	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

USB Device Connect	<input type="checkbox"/> ON <input type="checkbox"/> OFF
USB Device Remove	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DDNS Update Success	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DDNS Update Fail	<input type="checkbox"/> ON <input type="checkbox"/> OFF
Received SMS	<input type="checkbox"/> ON <input type="checkbox"/> OFF
SMS Command Execute	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 1 ON	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 1 OFF	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 1 Counter Overflow	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 2 ON	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 2 OFF	<input type="checkbox"/> ON <input type="checkbox"/> OFF
DI 2 Counter Overflow	<input type="checkbox"/> ON <input type="checkbox"/> OFF
Excessive Temperature	<input type="checkbox"/> ON <input type="checkbox"/> 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

SNMP MIBS	Generate
SNMP MIBS	Download

Item	Description	Default
MIBS	Click Generate to generate and click Download to download the device's MIB file.	--

2.5.12 Web Server

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

Web Server

^ General Settings

HTTP Port	<input style="width: 90%;" type="text" value="80"/>	?
HTTPS Port	<input style="width: 90%;" type="text" value="443"/>	?
HTTPS CA Certificate	<input style="width: 95%;" type="text" value="None"/> v	
HTTPS Private Keys	<input style="width: 95%;" type="text" value="None"/> v	

Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in router's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login router's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in router's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login 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.	443
HTTPS CA Certificate	Select one once the certification is imported, see 2.6.2 Certificate Manager .	
HTTPS Private Keys	Select one once the certification is imported, see 2.6.2 Certificate Manager .	

2.5.13 Advanced

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

System

Reboot

System Settings

Device Name ?

USR1 LED Type v ?

USR2 LED Type v ?

Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	460-gateway
USR LED Type	<ul style="list-style-type: none"> Specify the display type of your USR LED. Select from "None", "OpenVPN" or "IPsec", "SIM", "PPTP", "L2TP", "RCMS", "COM" . None: Meaningless indication, and the LED is off SIM: show the sim status. OpenVPN: USR indicator showing the OpenVPN status IPsec: USR indicator showing the IPsec status PPTP: USR indicator showing the PPTP status L2TP: USR indicator showing the L2TP status RCMS: show the connect status of RCMS COM1/2: show the connect status of Serial port 	OpenVPN

System

Reboot

Periodic Reboot Settings

Periodic Reboot ?

Daily Reboot Time ?

Emergency Reboot Settings

Reboot When No Link Is Available ON OFF ?

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

2.6 System

2.6.1 Debug

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

Syslog

Syslog
Netlog
VPNlog

```

Jun 19 10:40:37 460-gateway ModemManager[480143]: <info> [base-manager] modem for device
^/sys/devices/platform/32f10108.usb/38200000.dwc3/xhci-hcd.0.auto/usb1/1-1/1-1.3' successfully created
Jun 19 10:45:37 460-gateway ModemManager[480143]: opening device...
Jun 19 10:45:37 460-gateway ModemManager[480143]: [/dev/cdc-wdm0] Read max control message size from descriptors file: 4096
Jun 19 10:45:37 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30a20000.i2c': not supported by any plugin
Jun 19 10:45:37 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30be0000.ethernet': not supported by any plugin
Jun 19 10:45:37 460-gateway ModemManager[480143]: <warn> [modem0] couldn't query SIM slots: NoDeviceSupport
Jun 19 10:45:39 460-gateway mm_wrapper[2361]: [D] mmw_get_modem: found no modems!
Jun 19 10:45:41 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30a20000.i2c': not supported by any plugin
Jun 19 10:45:41 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30be0000.ethernet': not supported by any plugin
Jun 19 10:45:44 460-gateway mm_wrapper[2361]: [D] mmw_get_modem: found no modems!
Jun 19 10:45:44 460-gateway root[480253]: USB check status: host
Jun 19 10:45:46 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30a20000.i2c': not supported by any plugin
Jun 19 10:45:46 460-gateway ModemManager[480143]: <info> [base-manager] couldn't check support for device
^/sys/devices/platform/soc0/30800000.bus/30be0000.ethernet': not supported by any plugin
Jun 19 10:45:49 460-gateway ModemManager[480143]: <info> [modem0] state changed (unknown -> locked)
Jun 19 10:45:49 460-gateway ModemManager[480143]: <warn> [modem0] modem couldn't be initialized: Couldn't check unlock status: SIM not
inserted
Jun 19 10:45:49 460-gateway ModemManager[480143]: <info> [modem0] state changed (locked -> failed)
Jun 19 10:45:49 460-gateway mm_wrapper[2361]: [D] mmw_get_modem: found no modems!
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4296] manager: (cdc-wdm0): new Broadband device
(/org/freedesktop/NetworkManager/Devices/466)
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4309] device (cdc-wdm0): state change: unmanaged -> unavailable
(reason 'managed', sys-iface-state: 'external')
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4320] device (cdc-wdm0): modem state 'failed'
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4333] device (cdc-wdm0): old_state: unmanaged, state: unavailable,
concheck_now: false
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <warn> [1687142749.4334] device (cdc-wdm0): concheck_update_interval[IPv4]: applicable
interval is 0
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4334] device (cdc-wdm0): concheck_update_state[IPv4], state: NONE,
old state: UNKNOWN, dev state: unavailable, continuous success count: 0, continuous failure count: 1
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <warn> [1687142749.4337] device (cdc-wdm0): concheck_update_interval[IPv6]: applicable
interval is 0
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4337] device (cdc-wdm0): concheck_update_state[IPv6], state: NONE,
old state: UNKNOWN, dev state: unavailable, continuous success count: 0, continuous failure count: 1
Jun 19 10:45:49 460-gateway NetworkManager[1586]: <info> [1687142749.4343] modem-broadband[cdc-wdm0]: failed to retrieve SIM object: No
SIM object available
Jun 19 10:45:49 460-gateway modemd[479802]: Get modem path: /org/freedesktop/ModemManager1/Modem/0
Jun 19 10:45:49 460-gateway modemd[479802]: AT+GMM
Jun 19 10:45:50 460-gateway modemd[479802]: EG25
Jun 19 10:45:50 460-gateway modemd[479802]: AT+CGMR
Jun 19 10:45:50 460-gateway modemd[479802]: EG25GGBR07A08M2G
Jun 19 10:45:50 460-gateway modemd[479802]: AT+QGPS=1
Jun 19 10:45:50 460-gateway modemd[479802]: OK
Jun 19 10:45:50 460-gateway modemd[479802]: AT+QGPS?
Jun 19 10:45:50 460-gateway modemd[479802]: 1
Jun 19 10:45:50 460-gateway modemd[479802]: AT+QCFG="usbnet"
Jun 19 10:45:50 460-gateway modemd[479802]: "usbnet", 2
                    
```

Manual Refresh v

Clear

Refresh

Item	Description	Default
------	-------------	---------

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

^ Syslog Journal File

System Journal File
Generate

System Journal File
Download

Item	Description	Default
System Journal File	Click Generate to generate and click Download to download the system journal file.	--

^ System Diagnostic Data

System Diagnostic Data
Generate

System Diagnostic Data
Download

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

Netlog

Syslog	Netlog	VPNlog					
78	192.168.0.13	192.168.0.1	UDP	54277	53	2023-06-19 10:32:16	2023-06-19 10:32:46
79	192.168.0.13	192.168.0.1	UDP	51214	53	2023-06-19 10:32:16	2023-06-19 10:32:46
80	192.168.0.13	192.168.0.1	UDP	61033	53	2023-06-19 10:32:16	2023-06-19 10:32:48
81	192.168.0.13	192.168.0.1	UDP	63234	53	2023-06-19 10:32:16	2023-06-19 10:32:50
82	192.168.0.13	192.168.0.1	UDP	55044	53	2023-06-19 10:32:16	2023-06-19 10:32:46
83	192.168.0.13	192.168.0.1	UDP	51235	53	2023-06-19 10:32:16	2023-06-19 10:32:48
84	192.168.0.13	192.168.0.1	UDP	61180	53	2023-06-19 10:32:16	2023-06-19 10:32:47
85	192.168.0.13	192.168.0.1	UDP	49712	53	2023-06-19 10:32:16	2023-06-19 10:32:47
86	192.168.0.13	192.168.0.1	UDP	57387	53	2023-06-19 10:32:16	2023-06-19 10:32:46
87	192.168.0.13	192.168.0.1	UDP	57033	53	2023-06-19 10:32:16	2023-06-19 10:32:46
88	192.168.0.13	192.168.0.1	UDP	50445	53	2023-06-19 10:32:16	2023-06-19 10:32:47
89	192.168.0.13	192.168.0.1	UDP	49563	53	2023-06-19 10:32:16	2023-06-19 10:32:49
90	192.168.0.13	192.168.0.1	UDP	62820	53	2023-06-19 10:32:16	2023-06-19 10:32:46
91	192.168.0.13	192.168.0.1	UDP	54326	53	2023-06-19 10:32:16	2023-06-19 10:32:48
92	192.168.0.13	192.168.0.1	UDP	64357	53	2023-06-19 10:32:16	2023-06-19 10:32:47
93	192.168.0.13	192.168.0.1	UDP	52804	53	2023-06-19 10:32:16	2023-06-19 10:32:46
94	192.168.0.13	192.168.0.1	UDP	60909	53	2023-06-19 10:32:16	2023-06-19 10:32:47
95	192.168.0.13	192.168.0.1	UDP	62699	53	2023-06-19 10:32:16	2023-06-19 10:32:47
96	192.168.0.13	192.168.0.1	UDP	59098	53	2023-06-19 10:32:16	2023-06-19 10:32:47
97	192.168.0.13	192.168.0.1	UDP	54454	53	2023-06-19 10:32:16	2023-06-19 10:32:47
98	192.168.0.13	192.168.0.1	UDP	56096	53	2023-06-19 10:32:16	2023-06-19 10:32:49
99	192.168.0.13	192.168.0.1	UDP	56216	53	2023-06-19 10:32:16	2023-06-19 10:32:49
100	192.168.0.13	192.168.0.1	UDP	52434	53	2023-06-19 10:32:16	2023-06-19 10:32:47

100/page

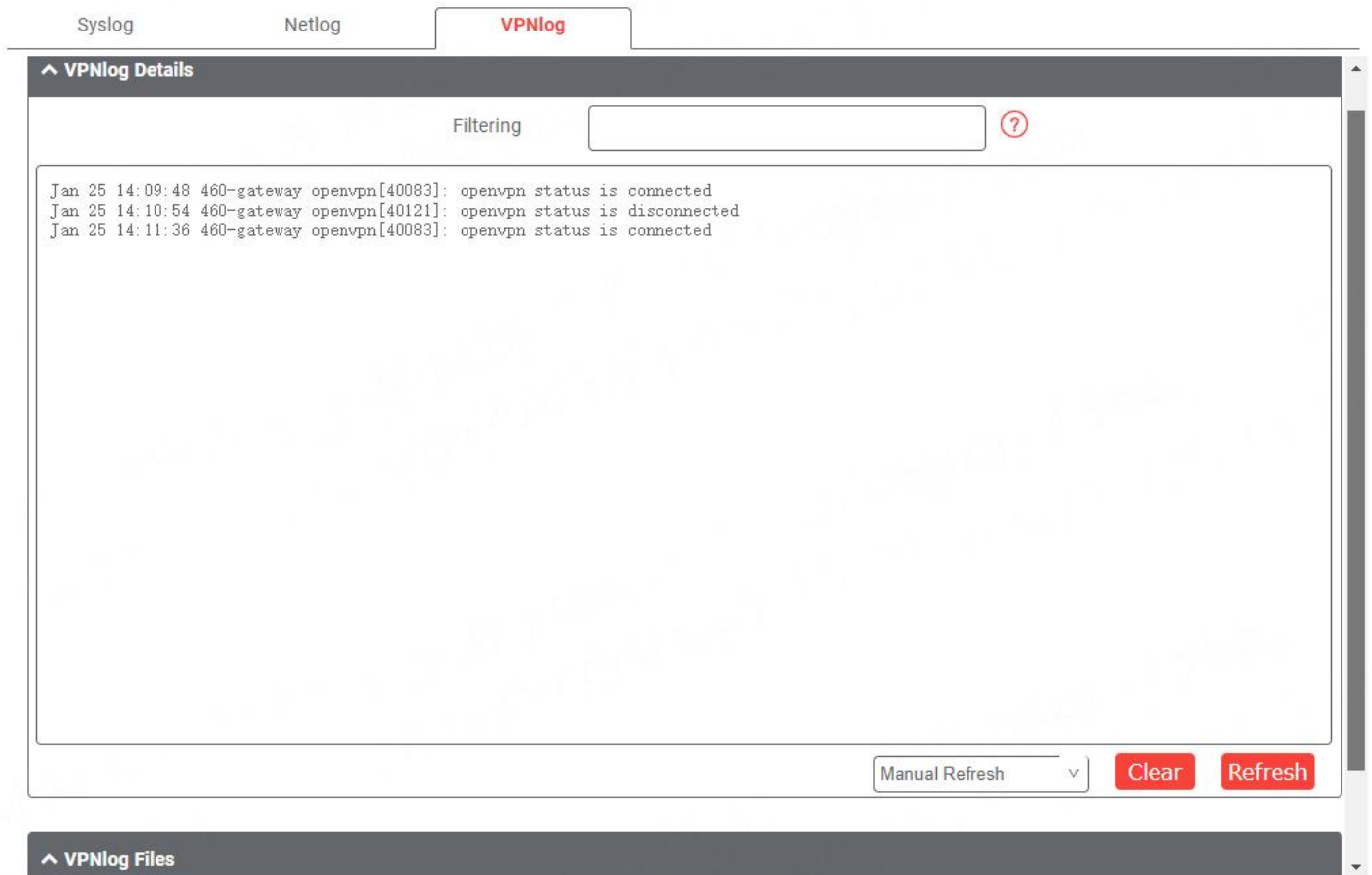
1/289

Jump

Prev

Next

VPNlog



The screenshot shows the VPNlog interface with three tabs: Syslog, Netlog, and VPNlog. The VPNlog tab is selected and displays the following log entries:

```
Jan 25 14:09:48 460-gateway openvpn[40083]: openvpn status is connected
Jan 25 14:10:54 460-gateway openvpn[40121]: openvpn status is disconnected
Jan 25 14:11:36 460-gateway openvpn[40083]: openvpn status is connected
```

The interface includes a 'Filtering' input field with a help icon, a 'Manual Refresh' dropdown menu, and 'Clear' and 'Refresh' buttons.

2.6.2 Certificate Manager

This section allows you to manage 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	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
Certificate File	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
Private Key	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
DH	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
TLS-Auth Key	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
CRL	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
TLS-Auth Key	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
CRL	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
PKCS#12 Certificate	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
Pre-Share Key	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>
Ovpn Config	<input type="button" value="Choose File"/> No file chosen <input style="float: right; width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/>

Item	Description	Default
Root CA	Click on <input type="button" value="Choose File"/> to locate the root ca file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	--
Certificate File	Click on <input type="button" value="Choose File"/> to locate the certificate file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	--
Private Key	Click on <input type="button" value="Choose File"/> to locate the Private Key file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	--
DH	Click on <input type="button" value="Choose File"/> to locate the DH file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	
TLS-Auth Key	Click on <input type="button" value="Choose File"/> to locate the TLS-Auth Key file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	--
CRL	Click on <input type="button" value="Choose File"/> to locate the CRL file, and then click on <input style="width: 20px; height: 20px; border: 1px solid #ccc; border-radius: 50%; background-color: #f00; color: white; text-align: center; line-height: 20px; vertical-align: middle;"/> to import this file into your device.	--

PKCS#12 Certificate	Click on <input type="button" value="Choose File"/> to locate the PKCS#12 Certificate file, and then click on to import this file into your device.	--
Pre-Share Key	Click on <input type="button" value="Choose File"/> to locate the Pre-Share Key file, and then click on to import this file into your device.	--
Ovpn Config	Click on <input type="button" value="Choose File"/> to locate the Ovpn Configy file, and then click on to import this file into your device.	--

IPsec

OpenVPN
IPsec
SSH
Web
System Certificate
Other

^ X509 Settings
?

Local Certificate	<input type="button" value="Choose File"/> No file chosen	
Remote Certificate	<input type="button" value="Choose File"/> No file chosen	
Private Key	<input type="button" value="Choose File"/> No file chosen	
CA Certificate	<input type="button" value="Choose File"/> No file chosen	
PKCS#12 Certificate	<input type="button" value="Choose File"/> No file chosen	

Item	Description	Default
Local Certificate	Click on <input type="button" value="Choose File"/> to locate the Local Certificate file, and then click on to import this file into your device.	--
Remote Certificate	Click on <input type="button" value="Choose File"/> to locate the Remote Certificate file, and then click on to import this file into your device.	--
Private Key	Click on <input type="button" value="Choose File"/> to locate the Private Key file, and then click on to import this file into your device.	--
CA Certificate	Click on <input type="button" value="Choose File"/> to locate the CA Certificate file, and then click on to import this file into your device.	--
PKCS#12 Certificate	Click on <input type="button" value="Choose File"/> to locate the PKCS#12 Certificate file, and then click on to import this file into your device.	--

SSH

OpenVPN IPsec **SSH** Web System Certificate Other

Authorized Keys Settings ?

Authorized Keys No file chosen

Authorized Keys

Index	File Name	File Size	Modification Time

Item	Description	Default
Authorized Keys	Click on <input type="button" value="Choose File"/> to locate the Authorized Keys file, and then click on to import this file into your device.	--

Web

OpenVPN IPsec SSH **Web** System Certificate Other

HTTPS Certificate Settings ?

HTTPS Private Key No file chosen

HTTPS CA Certificate No file chosen

HTTPS Private Key

Index	File Name	File Size	Modification Time

HTTPS CA Certificate

Index	File Name	File Size	Modification Time

Item	Description	Default
HTTPS Private Key	Click on <input type="button" value="Choose File"/> to locate the Authorized Keys file, and then click on to import this file into your device.	--
HTTPS CA Certificate	Click on <input type="button" value="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 No file chosen

Item	Description	Default
File	Click on <input type="button" value="Choose File"/> to locate the System certificate file, and then click on to import this file into your device.	--

Other

OpenVPN IPsec SSH Web System Certificate **Other**

^ Other Certificate Settings ?

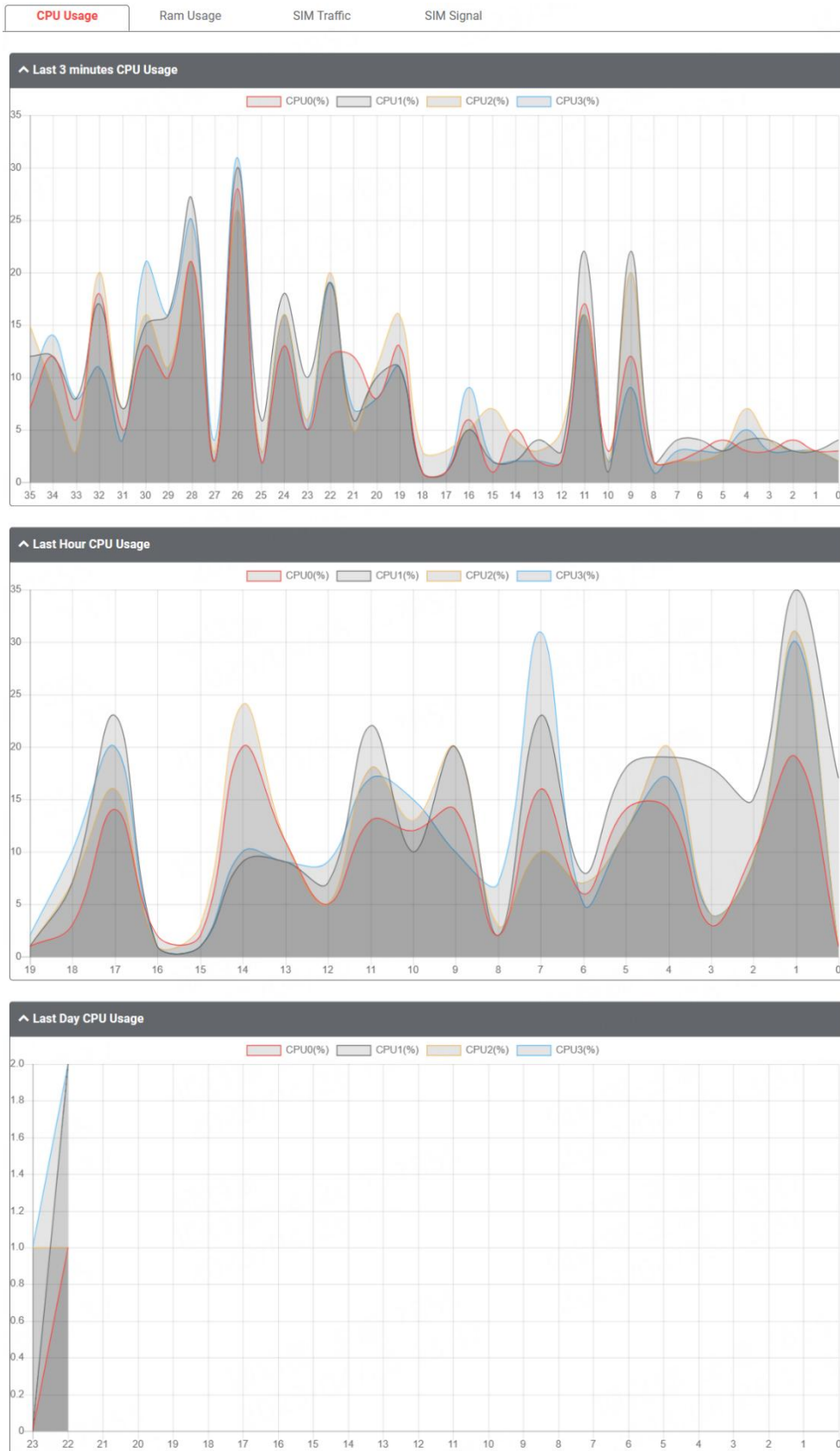
Other Certificate No file chosen

Item	Description	Default
Other Certificate	Click on <input type="button" value="Choose File"/> to locate the Other Certificate file, and then click on to import this file into your device.	--

2.6.3 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

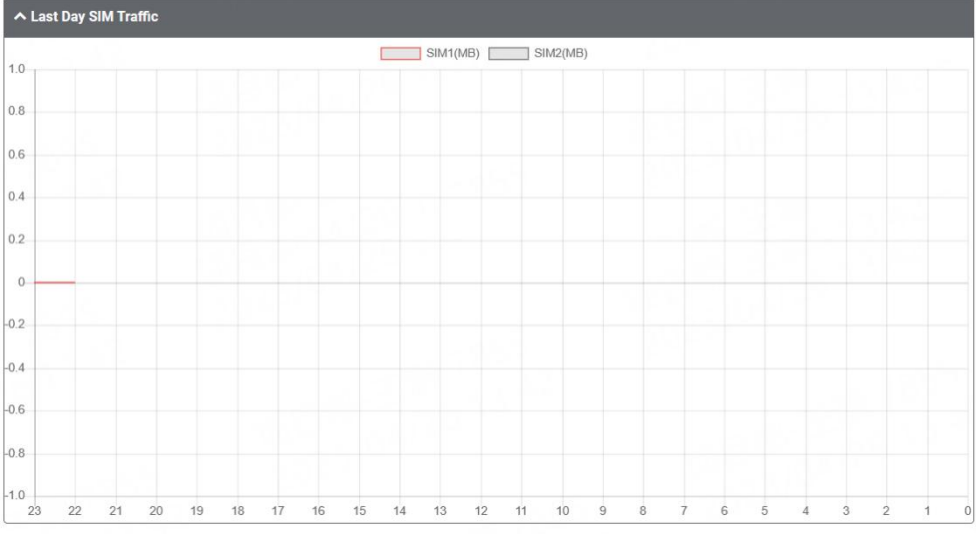
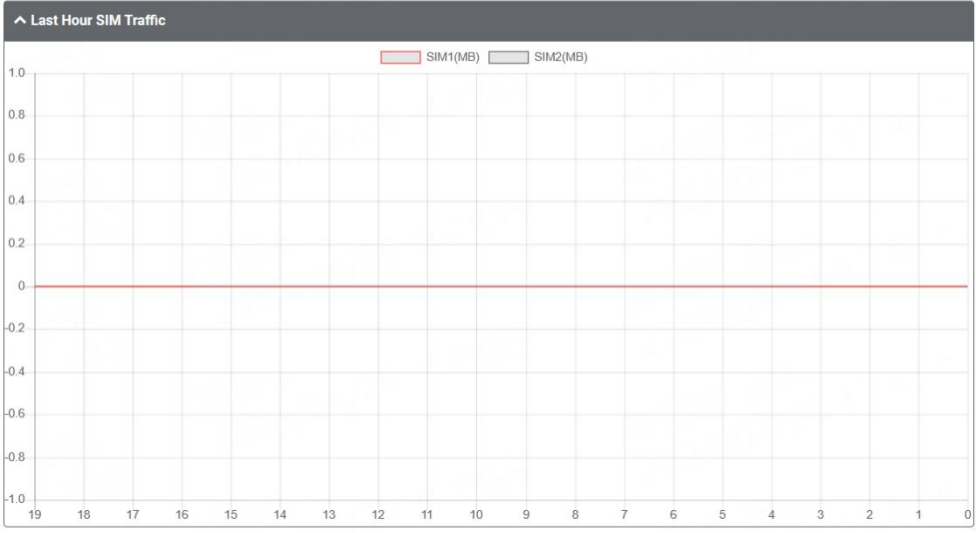
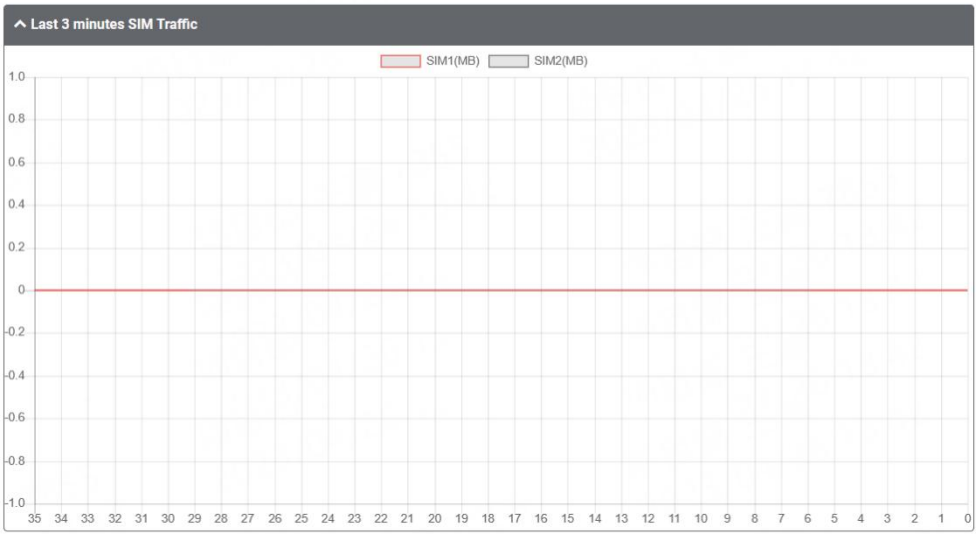


RAM Usage



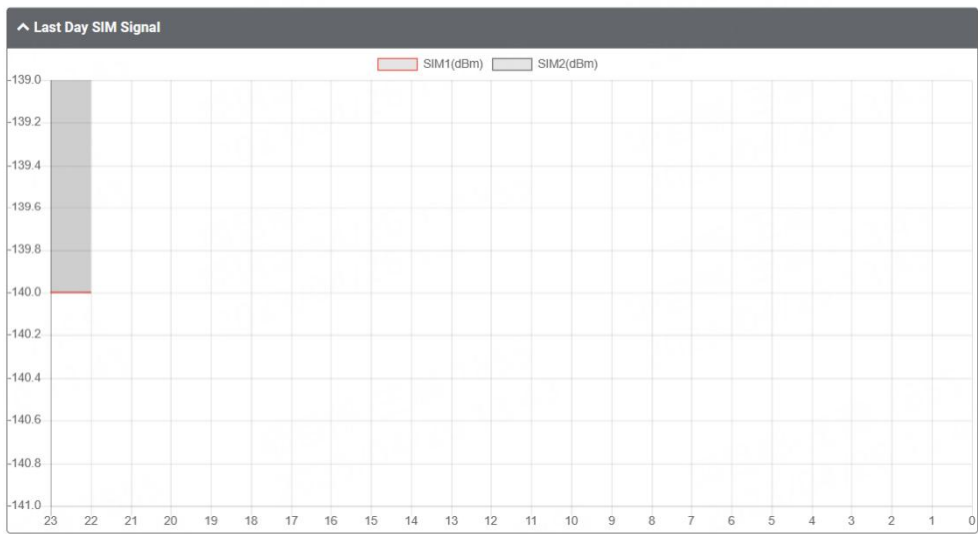
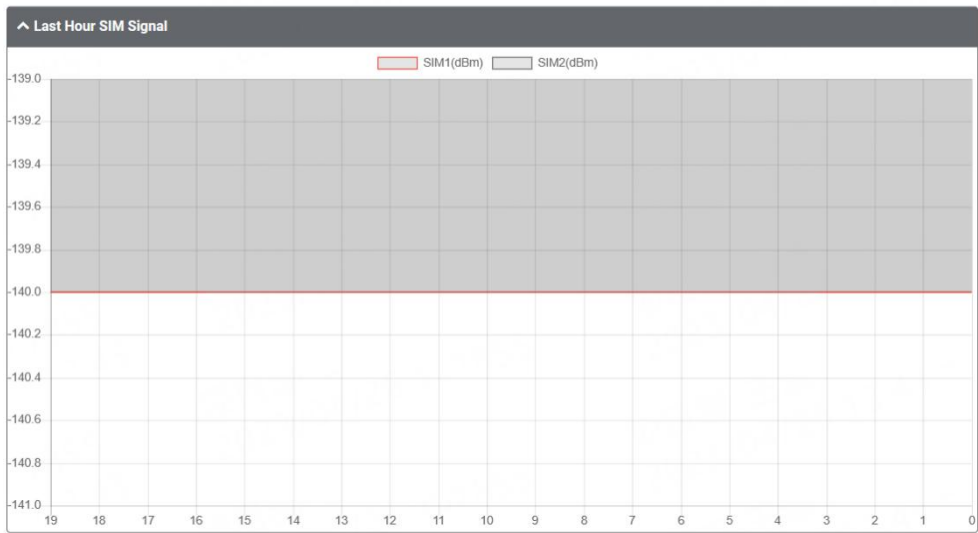
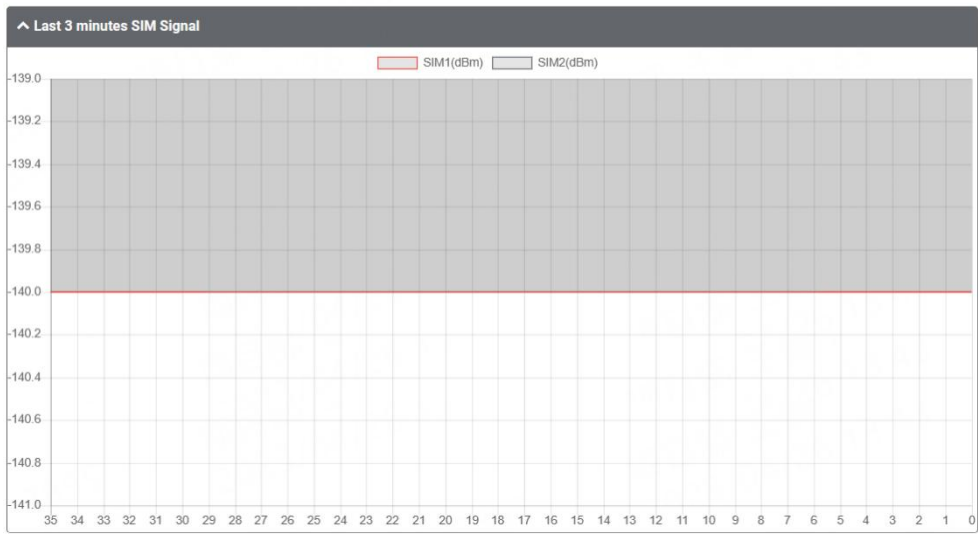
SIM Traffic

CPU Usage Ram Usage **SIM Traffic** SIM Signal



SIM Signal

CPU Usage Ram Usage SIM Traffic **SIM Signal**



2.6.4 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 <http://www.robustel.com/products/app-center/>.

^ 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 ✘ to uninstall the app.

^ Installed Apps

Index	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

2.6.5 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 Address

Number of Request

Timeout

Interface

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 stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	--
Stop	Click this button to stop ping request.	--

Traceroute

Ping
Traceroute
Sniffer

^ Traceroute

Trace Address

Trace Hops

Trace Timeout

Interface

Start
Stop

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 max value no matter the destination has been reached or not.	30
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 follow box.	--
Stop	Click this button to stop ping request.	--

Sniffer

Ping Traceroute **Sniffer**

^ Sniffer

Interface

Host

Packets Request

Protocol

Status

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.	--
	Click this button to start the sniffer.	--
	Click this button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--

^ Capture Files

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.	--

2.6.6 Flash Manager

This section allows you to manage the device’s flash memory life, you can easily check the flash status or throughput 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
?

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

^ Data Throughput

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 Tests

Test Mode ?

Start Time

End Time

Start
Stop

Flash Memory Tests @ Flash Manager	
Item	Description
Test Mode	Manual: When choosing 'manual', click 'start' to run a test, you can click 'stop' to end the test; Scheduled: Input the 'start' and 'end' time for a scheduled test. You can click 'stop' button under whatever mode.
Start Time	Enter start time, format: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 12:00:00
End Time	Enter end time, format: yyyy/mm/dd, hh/mm/ss. E.g. 2023/04/24, 18:00:00

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

2.6.7 Service Management

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

Service Management

^ Settings
?

WAN

LAN

Firewall

Route

Policy Route

Mode	View Status on RobustOS Pro	Configure via RobustOS Pro	Configure via Linux Shell
Managed By RobustOS Pro	√	√	X

Managed By Third-Party	X	X	√
------------------------	---	---	---

2.6.8 Profile

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

Profile

Profile
Rollback

^ Import Configuration File

Reset Other Settings to Default ON OFF ?

Ignore Invalid Settings ON OFF ?

XML Configuration File
 No file chosen Import

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

^ Configuration Rollback

Save as a Rollbackable Archive **Save** ?

^ Configuration Archive Files

Index	File Name	File Size	Modification Time

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

2.6.9 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.

The password need to be meet the requirement: 8-32 characters, must consist of at least three types of lowercase, uppercase, digit, and special characters.

Special characters allowed: @, #, \$, ., *, !, -

Sudo User
Super User
Common User

^ Sudo User Settings ?

New Username	<input type="text"/>	?
Old Password	<input type="text"/>	?
New Password	<input type="text"/>	?
Confirm Password	<input type="text"/>	

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

Sudo User
Super User
Common User

^ Super User Settings ?

New Username	<input type="text"/>	?
Old Password	<input type="text"/>	?
New Password	<input type="text"/>	?
Confirm Password	<input type="text"/>	

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

Sudo User

Super User

Common User

^ Common User Settings ?

UserId	Role	Username

+

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

^ Common Users Settings

UserId

?

Role

v

Username

?

Password

?

Item	Description	Default
Index	Indicate the ordinal of the list.	--
Role	Select from "Guest" and "User". <ul style="list-style-type: none"> 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 	Guest
Username	Set the Username; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null
Password	Set the password which at least contains 5 characters; valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	Null

2.6.10 DEB Management

This section allows you to manage your own Debian packages.

DEB Management

^ DEB Package Management

Apt Action

v

Package Name

Extra Parameters

?



Item	Description	Default
------	-------------	---------

Apt Action	Select from “update”, “install”, “clean”, “remove”, “show”. <ul style="list-style-type: none"> • 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

2.6.11 Role Management

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

Role Management

^ Settings ?		
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  to edit Visitor/Editor permission.

^ settings

Index	<input type="text" value="1"/>
Role	<input type="text" value="Guest"/> v
save and apply,reboot..	<input type="text" value="ReadOnly"/> v

^ Network

Firewall	<input type="text" value="ReadOnly"/> v
WAN	<input type="text" value="ReadOnly"/> v
Route	<input type="text" value="ReadOnly"/> v
QoS	<input type="text" value="ReadOnly"/> v
Policy Route	<input type="text" value="ReadOnly"/> v
LAN	<input type="text" value="ReadOnly"/> v

^ System	
Service Management	ReadOnly <input type="text" value="v"/>
Flash Manager	ReadOnly <input type="text" value="v"/>
DEB Management	ReadOnly <input type="text" value="v"/>
Profile	ReadOnly <input type="text" value="v"/>
Tools	ReadOnly <input type="text" value="v"/>
App Center	ReadOnly <input type="text" value="v"/>
Certificate Manager	ReadOnly <input type="text" value="v"/>
Debug	ReadOnly <input type="text" value="v"/>
User Management	ReadOnly <input type="text" value="v"/>

^ Interface	
WiFi	ReadOnly <input type="text" value="v"/>
VLAN	ReadOnly <input type="text" value="v"/>
USB	ReadOnly <input type="text" value="v"/>
Serial Port	ReadOnly <input type="text" value="v"/>
Ethernet	ReadOnly <input type="text" value="v"/>
DIDO	ReadOnly <input type="text" value="v"/>
Cellular	ReadOnly <input type="text" value="v"/>
Bridge	ReadOnly <input type="text" value="v"/>

^ VPN	
DMVPN	ReadOnly <input type="text" value="v"/>
PPTP	ReadOnly <input type="text" value="v"/>
OpenVPN	ReadOnly <input type="text" value="v"/>
L2TP	ReadOnly <input type="text" value="v"/>
IPsec	ReadOnly <input type="text" value="v"/>
GRE	ReadOnly <input type="text" value="v"/>

^ Services

Captive Portal	<input type="text" value="ReadOnly"/>
Web Server	<input type="text" value="ReadOnly"/>
VRRP	<input type="text" value="ReadOnly"/>
Syslog	<input type="text" value="ReadOnly"/>
SSH	<input type="text" value="ReadOnly"/>
SNMP	<input type="text" value="ReadOnly"/>
SMS	<input type="text" value="ReadOnly"/>
Advanced	<input type="text" value="ReadOnly"/>
RCMS	<input type="text" value="ReadOnly"/>
NTP	<input type="text" value="ReadOnly"/>
GPS	<input type="text" value="ReadOnly"/>
Event	<input type="text" value="ReadOnly"/>
Email	<input type="text" value="ReadOnly"/>
DDNS	<input type="text" value="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 3 Configuration Examples

3.1 Cellular

3.1.1 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 Debug

^ General Settings

Primary Sim SIM1 v ?

Enable Auto Switching
 ON OFF ?


^ Additional Switching Rules

Weak Signal
 ON OFF ?

While Roaming
 ON OFF ?

^ Advanced Cellular Settings

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

Click  to set its parameters according to the current ISP.

^ General Settings

Index	<input type="text" value="1"/>
SIM Card	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="SIM1"/> v
Automatic APN Selection	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
APN	<input type="text" value="internet"/>
Username	<input type="text"/>
Password	<input type="password"/>
Authentication Type	<input style="border-bottom: 1px solid #ccc; border-right: 1px solid #ccc; border-left: 1px solid #ccc; border-top: 1px solid #ccc; width: 100%;" type="text" value="None"/> v
Phone Number	<input type="text"/>
PIN Code	<input type="text"/> ?
Extra AT Cmd	<input type="text"/> ?
Telnet Port	<input type="text" value="0"/> ?

Then Click [“Network> WAN> Link”](#) 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	Type	Description	Weight	Firewall Zone	+
Wireless	WIFI	default wan	0	external	⋮ ✎ ✕

Click + to add one link for cellular dial-up, select “Modem” as the link type, then click Submit to submit.

Link Settings

Name: Cellular

Type: Modem

Interface: wwan

Description: Backup WAN

Weight: 0

Firewall Zone: external

Health Detection Settings

Enable: ON OFF

IPv4 Primary Server: 0.0.0.0

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

Link	Status
------	--------

Settings

Name	Type	Description	Weight	Firewall Zone	
Wireless	WIFI	default wan	0	external	⋮ ↗ ✕
Cellular	Modem	Backup WAN	0	external	⋮ ↗ ✕

3.1.2 SMS Remote Control

MG460 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).
4. 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 [4.1 What Is CLI](#).

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

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

System/Profile

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

Profile

Rollback

^ Import Configuration File

Reset Other Settings to Default	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Ignore Invalid Settings	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
XML Configuration File	<input type="button" value="Choose File"/> No file chosen <input style="margin-left: 10px;" type="button" value="Import"/>

^ Export Configuration File

Ignore Disabled Features	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
Add Detailed Information	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF ?
XML Configuration File	<input style="background-color: red; color: white;" type="button" value="Generate"/>
XML Configuration File	<input style="background-color: red; color: white;" type="button" value="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 = "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

OK

admin:admin;set lan network 1 interface lan0;set lan network 1 ip 172.16.24.24;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

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

SMS received:

OK

OK

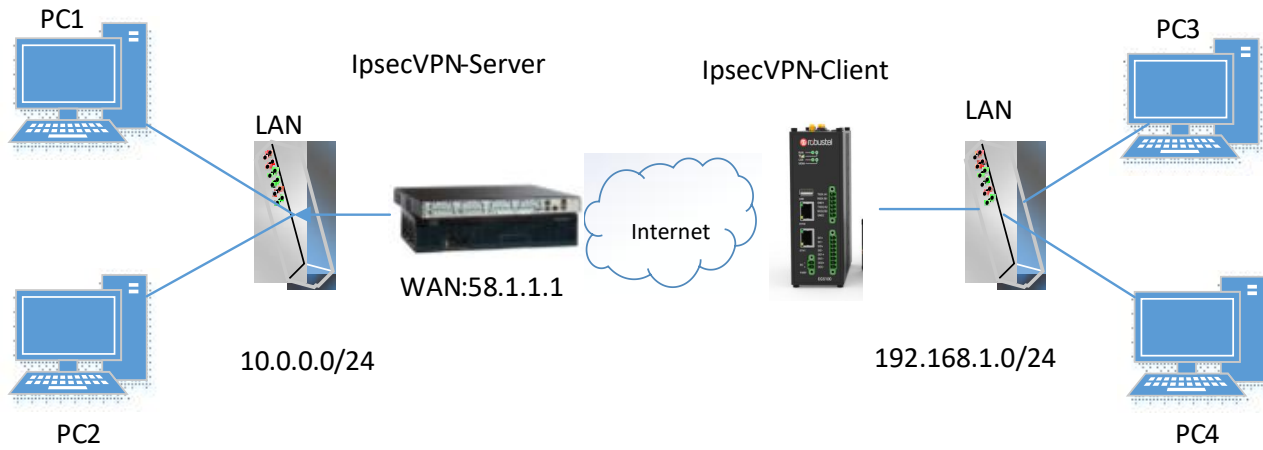
OK

OK

3.2 VPN Configuration Examples

3.2.1 IPsec VPN

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



IPsecVPN_Server:

Cisco 2811:

```

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

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

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

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

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

```

IPsec VPN_Client:

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

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

^ Tunnel Settings

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	
						+

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

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="IPsec1"/>
Link Binding	<input type="text" value="wlan0"/> v
Gateway	<input type="text" value="58.1.1.1"/> ?
Protocol	<input type="text" value="ESP"/> v
Mode	<input type="text" value="Tunnel"/> v
Local Subnet	<input type="text" value="192.168.1.0/24"/> ?
Remote Subnet	<input type="text" value="0.0.0.0/24"/> ?
IKE Type	<input type="text" value="IKEv1"/> v
Negotiation Mode	<input type="text" value="Main"/> v
Initiation Mode	<input type="text" value="Always On"/> v

^ Advanced Settings


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

^ PHASE 1

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

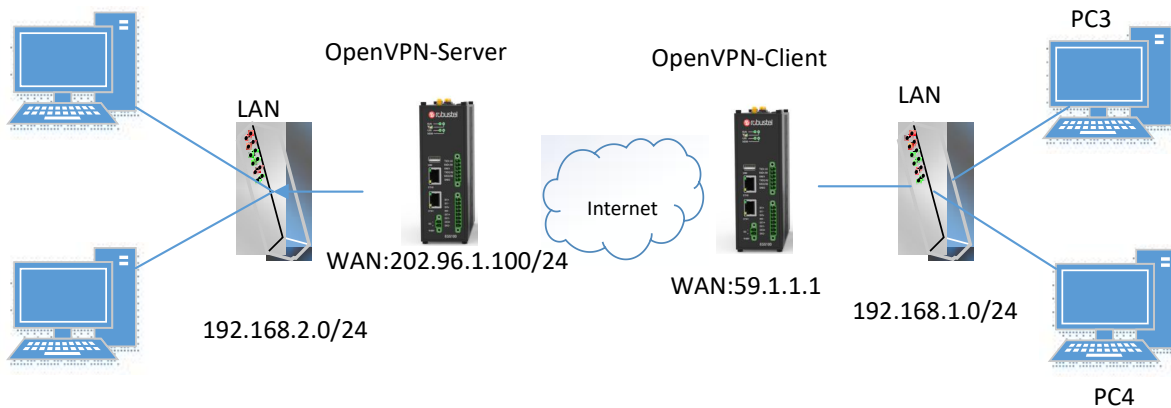
^ PHASE 2

Encryption Algorithm	<input type="text" value="3DES"/>	v
Authentication Algorithm	<input type="text" value="SHA1"/>	v
PFS Group	<input type="text" value="PFS(N/A)"/>	v
SA Lifetime	<input type="text" value="28800"/>	?
DPD Interval	<input type="text" value="30"/>	?
DPD Failures	<input type="text" value="150"/>	?

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

3.2.2 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.

OpenVPN
Status

^ Tunnel Settings

Index	Enable	Description	Mode	Peer Address	+

Click + to configure the Client01 as below.

^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="client01"/>
Mode	<input type="text" value="Client"/> v ?
Protocol	<input type="text" value="UDP"/> v
Peer Address	<input type="text" value="202.96.1.100"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> v
Authentication Type	<input type="text" value="X509CA"/> v ?

Root CA	<input type="text" value="None"/>	<input type="button" value="v"/>
Certificate File	<input type="text" value="None"/>	<input type="button" value="v"/>
Private Key	<input type="text" value="None"/>	<input type="button" value="v"/>
Private Key Password	<input type="password" value="••••"/>	
Encrypt Algorithm	<input type="text" value="BF"/>	<input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/>	<input type="button" value="v"/>
Renegotiation Interval	<input type="text" value="86400"/>	<input type="button" value="?"/>
Keepalive Interval	<input type="text" value="20"/>	<input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/>	<input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>	
Max Frame Size	<input type="text" value="1400"/>	
Enable Compression	<input checked="" type="checkbox" value="ON"/> <input type="checkbox" value="OFF"/>	
Enable NAT	<input checked="" type="checkbox" value="ON"/> <input type="checkbox" value="OFF"/>	
Enable DNS overrid	<input checked="" type="checkbox" value="ON"/> <input type="checkbox" value="OFF"/>	<input type="button" value="?"/>
Verbose Level	<input type="text" value="3"/>	<input type="button" value="v"/> <input type="button" value="?"/>

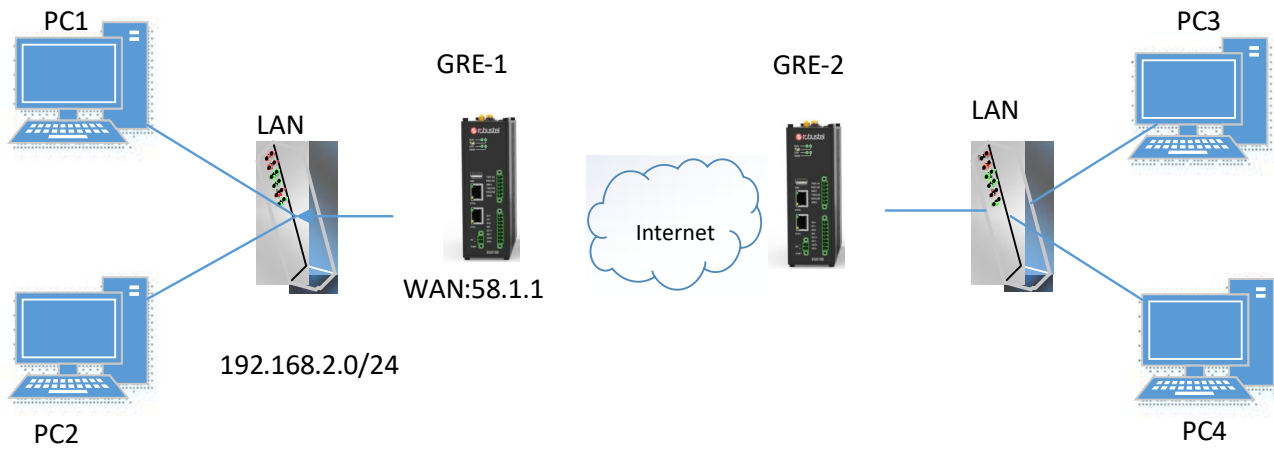
^ Advanced Settings

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

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

3.2.3 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 advertised from one network device to another.

GRE

Status

^ Tunnel Settings

Index	Enable	Description	Remote IP Address	+

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

GRE

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text" value="GRE-1"/>
Remote IP Address	<input type="text" value="58.1.1.1"/>
Local Virtual IP Address	<input type="text" value="10.8.0.1"/>
Local Virtual Netmask/Prefix Length	<input type="text" value="255.255.255.0"/> ?
Remote Virtual IP Address	<input type="text" value="10.8.0.2"/>
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets	<input type="text" value="...."/>

When finished, click to submit and click 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	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	GRE-2
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0 ?
Remote Virtual IP Address	10.8.0.1
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets

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

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

GRE	
Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> 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	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets

External IP address of another GRE instance used to establish the initial connection between peers.

IP address of the remote GRE Tunnel network interface.

Used the same password for the GRE peers

Index	1
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	GRE-2
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.2
Local Virtual Netmask/Prefix Length	255.255.255.0 ?
Remote Virtual IP Address	10.8.0.1
Enable Default Route	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Enable NAT	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Secrets

Chapter 4 Introductions for CLI

4.1 What Is CLI

Command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the [SSH](#) or through a [telnet](#) network connection. After establishing a Telnet or SSH connection with the 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

4.2 How to Configure the CLI

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

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

4.3 Commands Reference

Commands	Syntax	Description
Debug	Debug <i>parameters</i>	Turn on or turn off debug function
Show	Show <i>parameters</i>	Show current configuration of each function , if we need to see all please using “show running ”
Set	Set <i>parameters</i>	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add <i>parameters</i>	

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

4.4 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
lte_band3 = false
lte_band4 = false
lte_band5 = false
lte_band7 = false
lte_band8 = false
lte_band13 = false
lte_band17 = false
lte_band18 = false
lte_band19 = false
lte_band20 = false
lte_band21 = false
lte_band25 = false
lte_band28 = false
lte_band31 = false
lte_band38 = false
lte_band39 = false
lte_band40 = false
lte_band41 = false
}
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_number 18620435279
OK
...
# config save_and_apply
OK                                     // save and apply current configuration, make you configuration effect
```


Chapter 5 Glossary

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

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

Abbr.	Description
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Guangzhou Robustel Co., Ltd.

Add: 501, Building#2, 63 Yongan Road, Huangpu District,
Guangzhou, China 511350

Email: info@robustel.com

Web: www.robustel.com