

# RobustOS Software Manual

## About this Document

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

## Related Products

*M1200, M1201*

*R1500, R1510, R1510 Lite, R1511, R1511P, R1520*

*R2000, R2000 Dual, R2000 Ent, R2010, R2011, R2110*


*R3000, R3000 Lite, R3000 Quad, R3000 LG, R3010*

*R5020*

**Copyright©2022 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

The entire document cannot be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to change without notice due to continued progress in methodology, design, and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the mistaking use of this document.

## Technical Support

Tel: +86-20-82321505

Email: [support@robustel.com](mailto:support@robustel.com)

Web: [www.robustel.com](http://www.robustel.com)



**Document History**

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

Date	Document Version	Change Description
August 1, 2022	v.1.0.0	Initial release.

## Contents

<b>1. Introduction.....</b>	<b>6</b>
<b>2. Initial Configuration .....</b>	<b>7</b>
2.1 PC Configuration .....	7
2.2 Factory Default Settings .....	10
2.3 Factory Reset .....	10
2.4 Log in Your Device .....	11
2.5 Control Panel .....	12
<b>3. WebUI Descriptions .....</b>	<b>14</b>
3.1 Status.....	14
3.1.1 System Information .....	14
3.1.2 Internet Status .....	15
3.1.3 Modem Status .....	15
3.1.4 LAN Status.....	16
3.2 Interface .....	16
3.2.1 Link Manager .....	16
3.2.2 LAN .....	28
3.2.3 Ethernet.....	33
3.2.4 Cellular.....	35
3.2.5 Wi-Fi.....	41
3.2.6 USB .....	54
3.2.7 DI/DO.....	55
3.2.8 AI.....	60
3.2.9 Serial Port .....	61
3.2.10 LoRa .....	66
3.3 Packet Forwarders.....	69
3.3.1 Basic Station .....	69
3.3.2 Semtech UDP Forwarder .....	71
3.4 Network.....	76
3.4.1 Route .....	76
3.4.2 Firewall .....	78
3.4.3 IP Passthrough .....	88
3.5 VPN.....	88
3.5.1 IPsec.....	88
3.5.2 WireGuard .....	99
3.5.3 OpenVPN .....	101
3.5.4 GRE .....	113
3.6 Services .....	115
3.6.1 Syslog.....	115
3.6.2 Event.....	116
3.6.3 NTP .....	120
3.6.4 SMS.....	121
3.6.5 Email .....	123
3.6.6 DDNS.....	124

3.6.7	SSH.....	126
3.6.8	Telephone.....	127
3.6.9	Ignition.....	129
3.6.10	GPS.....	129
3.6.11	Web Server.....	134
3.6.12	Advanced.....	135
3.6.13	Smart Roaming V2.....	136
3.7	System.....	143
3.7.1	Debug.....	143
3.7.2	Update.....	144
3.7.3	App Center.....	144
3.7.4	Tools.....	146
3.7.5	Profile.....	149
3.7.6	User Management.....	151
<b>4.</b>	<b>Configuration Examples.....</b>	<b>152</b>
4.1	Cellular.....	152
4.1.1	Cellular Dial-Up.....	152
4.1.2	SMS Remote Control.....	155
4.2	VPN Configuration Examples.....	157
4.2.1	IPsec VPN.....	157
4.2.2	OpenVPN.....	161
4.2.3	GRE VPN.....	164
<b>5.</b>	<b>Introductions for CLI.....</b>	<b>166</b>
5.1	What Is CLI.....	166
5.2	How to Configure the CLI.....	167
5.3	Commands Reference.....	167
5.4	Quick Start with Configuration Examples.....	168
	<b>Example 1: Show the current version.....</b>	<b>168</b>
	<b>Example 2: Update firmware via tftp.....</b>	<b>168</b>
	<b>Example 3: Set link-manager.....</b>	<b>168</b>
	<b>Example 4: Set Ethernet.....</b>	<b>170</b>
	<b>Example 5: Set LAN IP address.....</b>	<b>170</b>
	<b>Example 6: CLI for setting Cellular.....</b>	<b>171</b>
	<b>Glossary.....</b>	<b>174</b>

# 1. Introduction

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

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

Related Product	M1200	M1201	R1510	R1510 Lite	R1511	R1520	R2000	R2000 Dual	R2000 Ent	R2010	R2011	R2110	R3000	R3000 Lite	R3000 Quad	R3000 LG	R3010	R5020
SIM Card	2	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	1	2
Ethernet	-	-	2	1	2	5	2	5	5	2	5	4	2	1	4	2	2	4
PoE PD	-	-	-	-	-	*	*	-	*	*	*	*	-	-	-	-	-	*
PoE PSE	-	-	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-
Wi-Fi	-	-	√	-	√	√	*	√	√	√	√	√	*	-	*	-	-	√
BLE	-	-	-	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-
GNSS	-	-	-	-	-	*	-	-	-	-	-	*	*	-	*	*	-	*
DI	2	-	√	-	-	√	-	√	-	√	-	√	2	-	-	2	-	√
DO	√	-	√	-	-	√	-	-	-	√	-	√	2	-	-	-	-	√
AI	-	-	-	-	-	√	-	-	-	-	-	-	-	-	-	-	-	-
RS232	√	*	-	-	*	√	-	-	*	*	-	√	√	√	*	*	√	√
RS485	√	*	-	-	*	√	-	-	*	*	-	√	√	√	*	*	√	√
USB Host	-	-	-	-	-	√	-	-	√	-	-	√	√	√	√	√	√	√
RS422	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CAN	-	*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	-
Voice (FXS)	-	-	-	-	-	-	-	-	*	-	-	-	-	-	-	-	√	-
MicroSD	-	-	-	-	-	-	-	-	-	-	-	√	√	-	√	√	-	√

Note: √ = Supported, - = Unsupported, \* = Optional

## About RobustOS

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


## 2. Initial Configuration

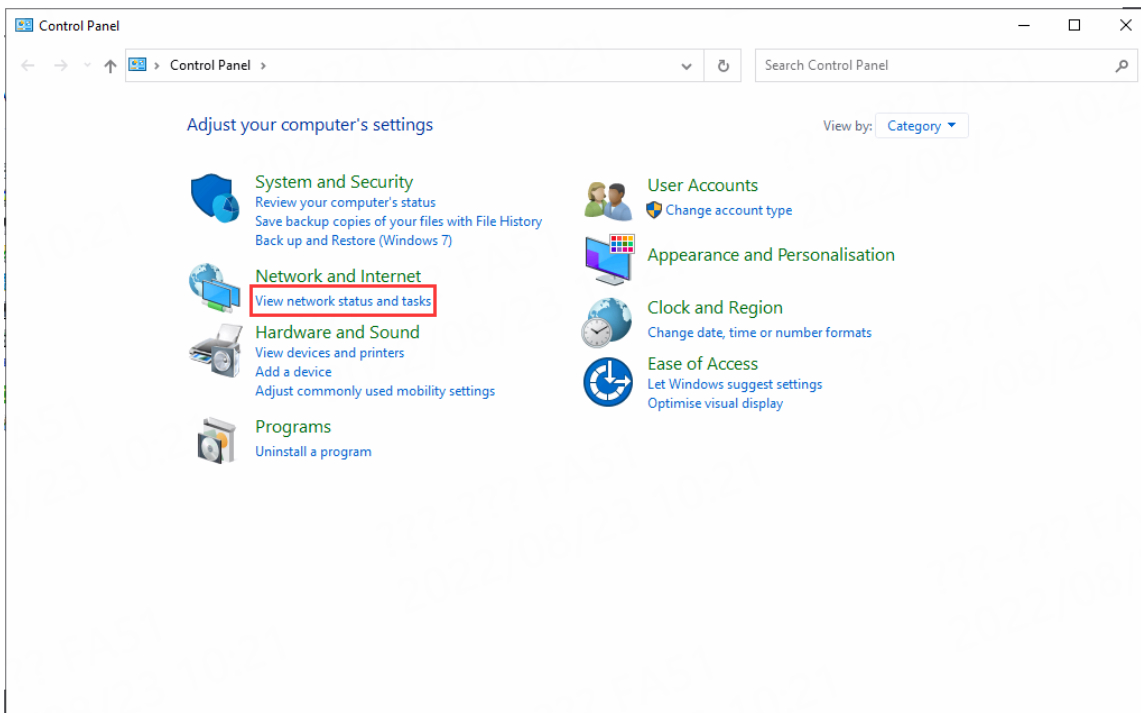
You can configure the device through the web browser, including Microsoft Edge, Google Chrome, Firefox, etc. A web browser is a standard application in the following operating systems: Ubuntu, macOS, Windows7/8/10/11, etc. It provides an easy and user-friendly interface for configuration. There are various ways to connect the device, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC is equipped with an Ethernet port before connecting the device. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the device. If you encounter any problems accessing the device web interface, it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the device.

### 2.1 PC Configuration

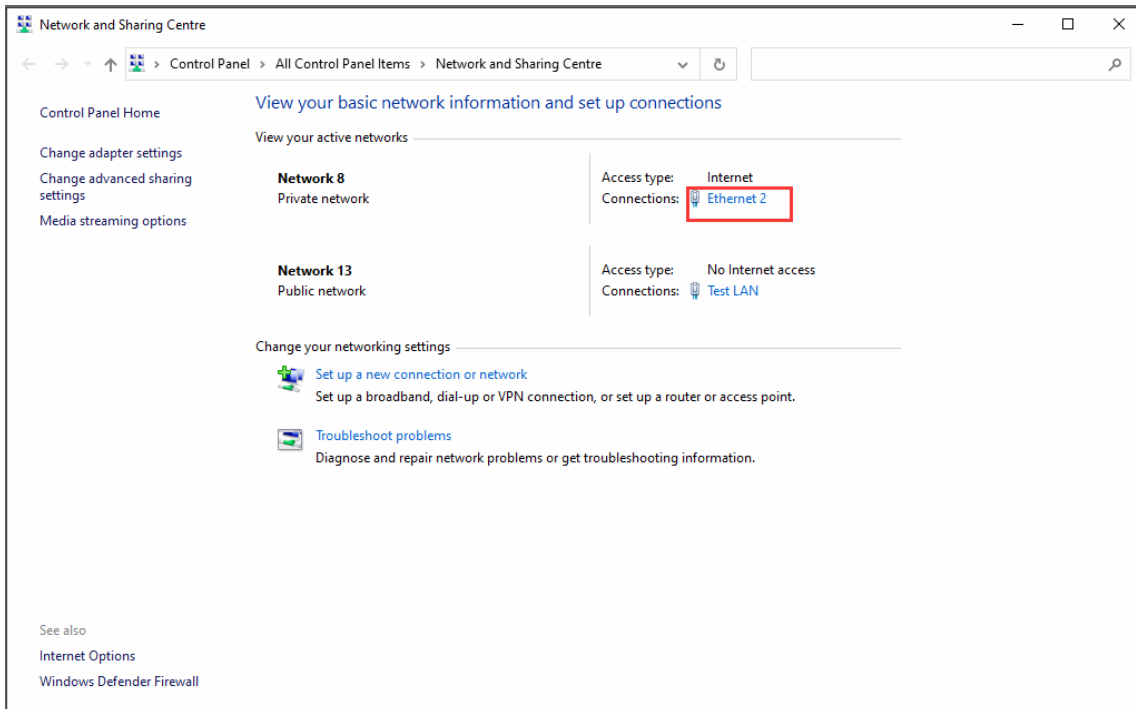
There are two ways to get an IP address for the computer. One is to obtain an IP address automatically from “Local Area Connection”, and another is to configure a static IP address manually within the same subnet of the router. Please refer to the steps below.

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

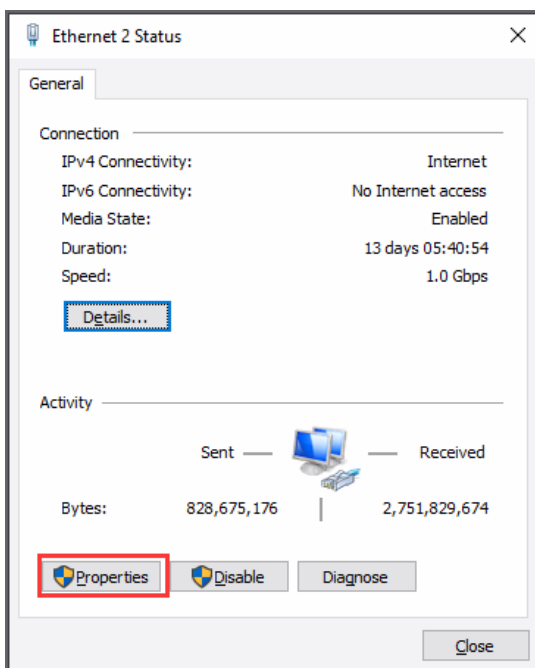
1. Find the Windows logo key  (hereinafter referred to as Win key) of the keyboard, press **Win + R**, type "**Control**" to run **Control Panel**. After opening the Control Panel, left-click on "**View Network Status and Tasks**".



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

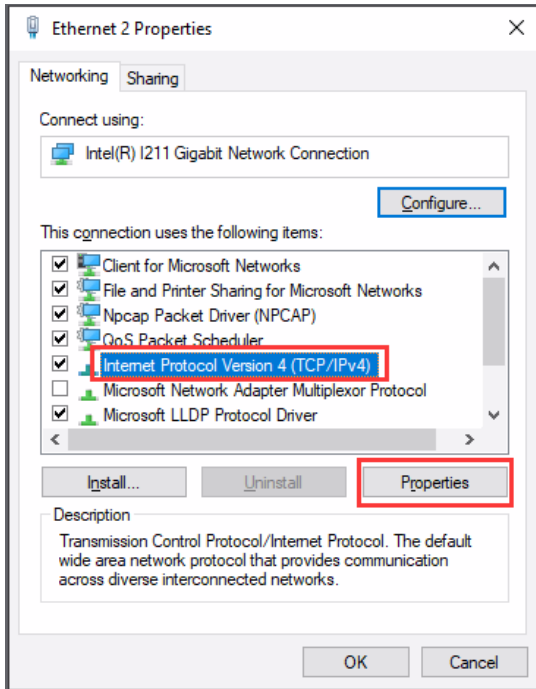


3. Click **Properties** in the window of **Local Area Connection status**.



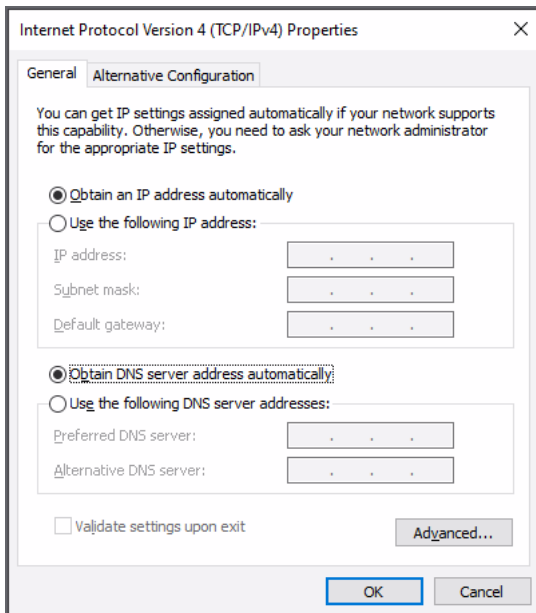


4. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

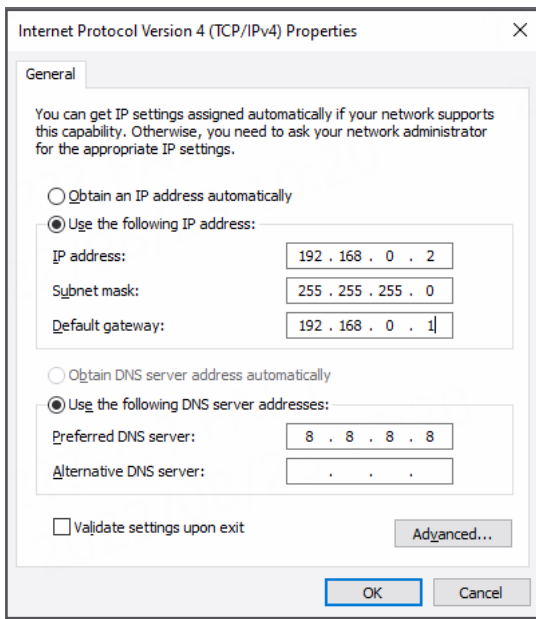


5. Two ways to configure the IP address of the computer.

(1) Auto obtain from the DHCP server, click "**Obtain an IP address automatically**";



(2) Manually configure 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.

## 2.2 Factory Default Settings

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

Item	Description
Username	admin
Password	admin
ETH0	WAN mode or 192.168.0.1/255.255.255.0, LAN mode.
ETH1/2/3/4(*)	192.168.0.1/255.255.255.0, LAN mode.
DHCP Server	Enabled

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

## 2.3 Factory Reset

Function	Operation
Reboot	Press and hold the RST button for 2~5 seconds under the operating status.
Restore to default 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.

## 2.4 Log in Your Device

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

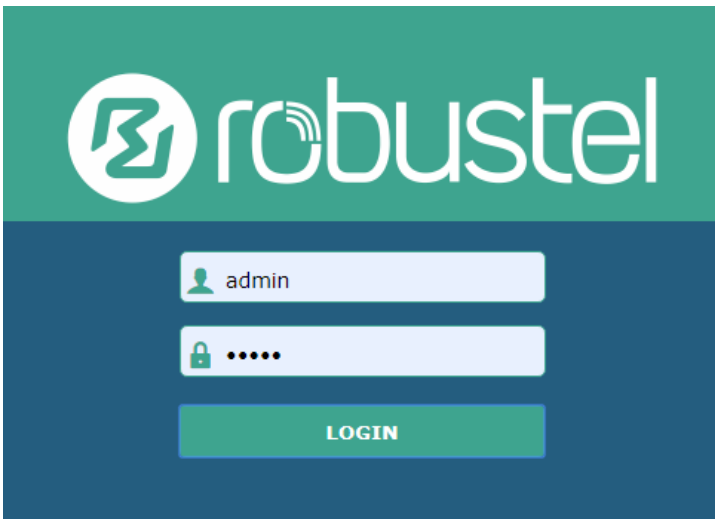
1. On your PC, launch a browser. e.g.: Microsoft Edge, Google Chrome or Firefox, etc.
2. From your web browser, type the IP address of the device into the address bar and press enter. The default IP address of the device is <http://192.168.0.1/>, though the actual address may vary.

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



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

**Note:** If enter the wrong username or password over 6 times, the login web will be locked for 5 minutes.



## 2.5 Control Panel

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



The screenshot displays the RobustOS web interface control panel. The top navigation bar includes the Robustel logo, the text "Save & Apply | Reboot | Logout", and a "Status" tab. A left sidebar contains menu items: Status, Interface, Network, VPN, Services, and System. The main content area is divided into four sections:

- System Information:**

Device Model	R1520-4L(V)
System Uptime	2 days, 23:12:53
System Time	Tue Jan 3 23:12:20 2017 (NTP not updated)
RAM Usage	72M Free/128M Total
Firmware Version	5.0.0 (e13067be)
Hardware Version	1.1
Kernel Version	4.9.152
Serial Number	[REDACTED]
- Internet Status:**

Active Link	
Uptime	
IP Address	
Gateway	
DNS	
- Modem Status:**


Modem Model	EG25
Registration	
Network Provider	
Network Type	
Signal Strength	
- LAN Status:**

IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:1A:1F:1E


At the bottom of the interface, a copyright notice reads: "Copyright © 2022 Robustel Technologies. All rights reserved."

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






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

 It is strongly recommended to change the default password. 




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

 button to close the notification. To change your username and/or password, see [3.6.6 System > User](#)

[Management.](#)

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

**Note:** The steps of how to modify configuration are as below:

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

## 3. WebUI Descriptions

### 3.1 Status

#### 3.1.1 System Information

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

^ System Information	
<b>Device Model</b>	R1520-4L(V)
<b>System Uptime</b>	0 days, 00:00:46
<b>System Time</b>	Sun Jan 1 00:00:11 2017 (NTP not updated)
<b>RAM Usage</b>	75M Free/128M Total
<b>Firmware Version</b>	5.0.0 (4ba3a3c7)
<b>Hardware Version</b>	1.1
<b>Kernel Version</b>	4.9.152
<b>Serial Number</b>	

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

### 3.1.2 Internet Status

This page shows the router's Internet status information.

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

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

### 3.1.3 Modem Status

This page shows the router's Modem information.

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

Modem Status	
Item	Description
Modem Model	Show model of the radio module.
Registration	Show current network status.
Network Provider	Show name of the Network Provider.
Network Type	Show current network service type, e.g., GPRS.
Signal Strength	Show the values of signal strength.

### 3.1.4 LAN Status

This page shows the routers' LAN status

**^ LAN Status**

**IP Address**    192.168.0.1/255.255.255.0

**MAC Address**    34:FA:40:0A:A4:2A

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

## 3.2 Interface

### 3.2.1 Link Manager

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

Link Manager
Status

**^ General Settings**

**Primary Link**    WWAN1 v ?

**Backup Link**    None v ?

**Emergency Reboot**    ON OFF ?

General Settings @ Link Manager		
Item	Description	Default
Primary Link	Select from "WWAN1", "WWAN2", "WAN" or "WLAN". <ul style="list-style-type: none"> <li>WWAN1: Select SIM1 as the primary wireless link.</li> <li>WWAN2: Select SIM2 as the primary wireless link.</li> <li>WAN: Select WAN Ethernet port as the primary wired link.</li> <li>WLAN: Select WLAN as the primary wireless link.</li> </ul> <i><b>Note:</b> WLAN link is available only if enable Wi-Fi as Client mode, please refer to <a href="#">3.2.5 Wi-Fi</a>.</i>	WWAN1



General Settings @ Link Manager		
Item	Description	Default
Backup Link	Select from "WWAN1", "WWAN2", "WAN", "WLAN", or "None". <ul style="list-style-type: none"> <li>WWAN1: Select SIM1 as the backup wireless link.</li> <li>WWAN2: Select SIM2 as the backup wireless link.</li> <li>WAN: Select WAN Ethernet port as the backup wired link.</li> <li>WLAN: Select WLAN as the backup wireless link.</li> </ul> <i>Note: WLAN link is available only if enable Wi-Fi as Client mode, please refer to <a href="#">3.2.5 Wi-Fi</a>.</i> <ul style="list-style-type: none"> <li>None: No backup link.</li> </ul>	None
Backup Mode	Select from "Cold Backup", "Warm Backup", or "Load Balancing". <ul style="list-style-type: none"> <li>Cold Backup: The inactive link is offline on standby.</li> <li>Warm Backup: The inactive link is online on standby.</li> <li>Load Balancing: Use two links simultaneously.</li> </ul> <i>Note: Backup Mode is available only Backup Link isn't None.</i>	Cold Backup
Revert Interval	Specify number of minutes that elapses before the primary link is checked if a backup link is being used in cold backup mode. 0 means disable checking. <i>Note: Revert interval is available only under the cold backup mode.</i>	0
Emergency Reboot	Click the toggle button to enable/disable this option. Enable to reboot the whole system if no links are available.	OFF

**Note:** Click for help.

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

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

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

## WWAN1/WWAN2

**Link Manager**

**^ General Settings**

Index

Type

Description

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

^ WWAN Settings

<b>Automatic APN Selection</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>Dialup Number</b>	<input type="text" value="*99***1#"/>		
<b>Authentication Type</b>	<input type="text" value="Auto"/> v		
<b>PPP Preferred</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>
<b>Switch SIM By Data Allowance</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>
<b>Data Allowance</b>	<input type="text" value="0"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	
<b>Billing Day</b>	<input type="text" value="1"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	

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

^ WWAN Settings

<b>Automatic APN Selection</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>APN</b>	<input type="text" value="internet"/>		
<b>Username</b>	<input type="text"/>		
<b>Password</b>	<input type="password" value="....."/>		
<b>Dialup Number</b>	<input type="text" value="*99***1#"/>		
<b>Authentication Type</b>	<input type="text" value="Auto"/> v		
<b>PPP Preferred</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>
<b>Switch SIM By Data Allowance</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>
<b>Data Allowance</b>	<input type="text" value="0"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	
<b>Billing Day</b>	<input type="text" value="1"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	

^ Ping Detection Settings ?

<b>Enable</b>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<b>Primary Server</b>	<input type="text" value="8.8.8.8"/>		
<b>Secondary Server</b>	<input type="text" value="114.114.114.114"/>		
<b>Interval</b>	<input type="text" value="300"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	
<b>Retry Interval</b>	<input type="text" value="5"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	
<b>Timeout</b>	<input type="text" value="3"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	
<b>Timeout unit</b>	<input type="text" value="Second(s)"/> v		
<b>Max Ping Tries</b>	<input type="text" value="3"/>	<input style="font-size: 10px; border: none; border-radius: 50%;" type="button" value="?"/>	

^ Advanced Settings

**NAT Enable**  ON  OFF

**Auto MTU For WWAN**  ON  OFF

**MTU**  ?

**Upload Bandwidth**  ?

**Download Bandwidth**

**Overridden Primary DNS**

**Overridden Secondary DNS**

**Debug Enable**  ON  OFF

**Verbose Debug Enable**  ON  OFF

Link Settings (WWAN)		
Item	Description	Default
<b>General Settings</b>		
Index	Indicate ordinal of the list.	--
Type	Show type of the link.	WWAN1
Description	Enter a description for this link.	Null
<b>WWAN Settings</b>		
Automatic APN Selection	Click the toggle button to enable/disable the “Automatic APN Selection” option. After enabling, the device will recognize the APN (Access Point Name) automatically. Alternatively, you can disable this option and manually add the APN (Access Point Name).	ON
APN	Enter APN (Access Point Name) for cellular dial-up connection, provided by the local ISP.	Internet
Username	Enter username for cellular dial-up connection, provided by the local ISP.	Null
Password	Enter password for cellular dial-up connection, provided by the local ISP.	Null
Dialup Number	Enter dial-up number for the cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Preferred	The PPP dial-up method is preferred.	OFF
Switch SIM By Data Allowance	Click the toggle button to enable/disable this option. After enabling, it will switch to another SIM when the data limit is reached. <b>Note:</b> Only used for dual-SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in <b>Interface &gt; Link Manager &gt; Status &gt; WWAN Data Usage Statistics</b> . 0 means disable data traffic record.	0
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated from that day.	1

Link Settings (WWAN)		
Item	Description	Default
<b>Ping Detection Settings</b>		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	The router will ping this primary address/domain name to check if the current IPv4 connectivity is active.	8.8.8.8
Secondary Server	The router will ping this secondary address/domain name to check if the current IPv4 connectivity is active.	114.114.114.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms).	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
<b>Advanced Settings</b>		
NAT Enable	Click the toggle button to enable/disable Network Address Translation.	ON
Auto MTU For WWAN	Click the toggle button to enable/disable Auto MTU feature for WWAN.	ON
MTU	Set the Maximum Transmission Unit. <b>Note:</b> MTU is available only "Auto MTU For WWAN" is OFF.	1500
Upload Bandwidth	Set upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Set download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define primary IPv4 DNS server address used by the link.	Null
Specify Secondary DNS	Define secondary IPv4 DNS server address used by the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

## WAN

The router will obtain IP automatically from DHCP server when apply "DHCP".

**Link Manager**

^ **General Settings**

Index

Type  v

Description

Connection Type  v

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

### ^ General Settings

Index	<input type="text" value="3"/>
Type	<input type="text" value="WAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="Static"/>

### ^ WAN Settings

Data Allowance	<input type="text" value="0"/>	<input type="text" value="?"/>
Billing Day	<input type="text" value="1"/>	<input type="text" value="?"/>

### ^ Static Address Settings

IP Address	<input type="text"/>	<input type="text" value="?"/>
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	

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

### ^ General Settings

Index	<input type="text" value="3"/>
Type	<input type="text" value="WAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="PPPoE"/>

### ^ WAN Settings

Data Allowance	<input type="text" value="0"/>	<input type="text" value="?"/>
Billing Day	<input type="text" value="1"/>	<input type="text" value="?"/>

### ^ PPPoE Settings

Username	<input type="text"/>	
Password	<input type="text"/>	
Authentication Type	<input type="text" value="Auto"/>	
PPP Expert Options	<input type="text"/>	<input type="text" value="?"/>

**^ Ping Detection Settings** ?

Enable  ON  OFF

Primary Server

Secondary Server

Interval  ?

Retry Interval  ?

Timeout  ?

Timeout unit  v

Max Ping Tries  ?

**^ Advanced Settings**

NAT Enable  ON  OFF

MTU

Upload Bandwidth  ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable  ON  OFF

Verbose Debug Enable  ON  OFF

Link Settings (WAN)		
Item	Description	Default
<b>General Settings</b>		
Index	Indicate ordinal of the list.	--
Type	Show type of the link.	WAN
Description	Enter a description for this link.	Null
Connection Type	Select from "DHCP", "Static" or "PPPoE".	DHCP
<b>Static Address Settings</b>		
IP Address	Set IP address with Netmask which can access the Internet. IP address with Netmask, e.g., 192.168.1.1/24	Null
Gateway	Set gateway address of the WAN port.	Null
Primary DNS	Set primary DNS address.	Null
Secondary DNS	Set secondary DNS address.	Null
<b>PPPoE Settings</b>		
Username	Enter username provided by your Internet Service Provider.	Null
Password	Enter password provided by your Internet Service Provider.	Null

Authentication Type	Select from “Auto”, “PAP” or “CHAP” as the local ISP required.	Auto
PPP Expert Options	Enter PPP Expert options used for PPPoE dialup. You can enter some other PPP dial strings in this field. Each string can be separated by a semicolon.	Null
<b>WAN Settings</b>		
Data Allowance	Set monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will be displayed in <b>Interface &gt; Link Manager &gt; Status &gt; WAN Data Usage Statistics</b> . 0 means disable data traffic record.	0
Billing Day	Specify monthly billing day. The data traffic statistics will be recalculated from that day.	1
<b>Ping Detection Settings</b>		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	The router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	The router will ping this secondary address/domain name to check if the current connectivity is active.	114.114.114.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms)	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
<b>Advanced Settings</b>		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter Maximum Transmission Unit.	1500
Upload Bandwidth	Enter upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define primary IPv4 DNS server address used by the link.	Null
Specify Secondary DNS	Define secondary IPv4 DNS server address for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

## WLAN

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

### Link Manager

#### ^ General Settings

Index	<input type="text" value="4"/>
Type	<input type="text" value="WLAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="DHCP"/>

#### ^ WLAN Settings

SSID	<input type="text" value="router"/>
Connect to Hidden SSID	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Password	<input type="text"/>

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

### ^ General Settings

Index	<input type="text" value="4"/>
Type	<input type="text" value="WLAN"/>
Description	<input type="text"/>
Connection Type	<input type="text" value="Static"/>

### ^ Static Address Settings

IP Address	<input type="text"/>	
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	



### ^ Ping Detection Settings ?

Enable  ON  OFF

Primary Server

Secondary Server

Interval  ?

Retry Interval  ?

Timeout  ?

Timeout unit  v

Max Ping Tries  ?

### ^ Advanced Settings

NAT Enable  ON  OFF

MTU

Upload Bandwidth  ?

Download Bandwidth

Overridden Primary DNS

Overridden Secondary DNS

Debug Enable  ON  OFF

Verbose Debug Enable  ON  OFF

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

IP Address	Enter IP address with Netmask which can access the Internet, e.g., 192.168.1.1/24.	Null
Router	Enter IP address of the Wi-Fi AP.	Null
Primary DNS	Set primary DNS address.	Null
Secondary DNS	Set secondary DNS address.	Null
<b>Ping Detection Settings</b>		
Enable	Click the toggle button to enable/disable the ping detection mechanism, a keepalive policy of the router.	ON
Primary Server	The router will ping this primary address/domain name to check if the current connectivity is active.	8.8.8.8
Secondary Server	The router will ping this secondary address/domain name to check if the current connectivity is active.	114.114.14.114
Interval	Set ping interval.	300
Retry Interval	Set ping retry interval. When ping failed, the router will ping again every retry interval.	5
Timeout	Set ping timeout.	3
Timeout Unit	Set ping timeout unit. Second(s) or Millisecond(ms)	Second
Max Ping Tries	Set max ping tries. Switch to another link or take emergency action if the max continuous ping tries reached.	3
<b>Advance Settings</b>		
NAT Enable	Click the toggle button to enable/disable the Network Address Translation option.	ON
MTU	Enter Maximum Transmission Unit.	1500
Upload Bandwidth	Enter upload bandwidth used for QoS, measured in kbps.	10000
Download Bandwidth	Enter download bandwidth used for QoS, measured in kbps.	10000
Specify Primary DNS	Define a primary DNS server address used by the link.	Null
Specify Secondary DNS	Define a secondary DNS server address for the link.	Null
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF

## Status

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

Link Manager		Status		
<b>^ Link Status</b> <span style="float: right;">...</span>				
Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:00:50	10.33.245.89/255.255.255.252

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



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

Link Manager		Status		
<b>^ Link Status</b> <span style="float: right;">...</span>				
Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:00:03	10.33.245.89/255.255.255.252
			<b>Index</b>	1
			<b>Link</b>	WWAN1
			<b>Status</b>	Connected
			<b>Interface</b>	wwan
			<b>Uptime</b>	0 days, 00:00:03
			<b>IP Address</b>	10.33.245.89/255.255.255.252
			<b>Gateway</b>	10.33.245.90
			<b>MTU</b>	1500
			<b>DNS</b>	120.80.80.80 221.5.88.88
			<b>RX Packets</b>	3
			<b>TX Packets</b>	3
			<b>RX Bytes</b>	656
			<b>TX Bytes</b>	700

**^ WWAN Data Usage Statistics** ?

WWAN1 Monthly Stats Clear  
WWAN2 Monthly Stats Clear

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

**^ WAN Data Usage Statistics** ?

WAN Monthly Stats Clear

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

### 3.2.2 LAN

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

**Note:**

- 1) R3000 Lite has only one Ethernet port which can only be assigned as LAN.
- 2) R2000 Lite has only one Ethernet port which can only be assigned as LAN.
- 3) R1510 Lite has only one Ethernet port which can only be assigned as LAN.

### LAN

LAN	Multiple IP	Tagged VLAN	Status	
<b>^ Network Settings</b> <span style="float: right;">?</span>				
Index	Interface	IP Address	Netmask	VLAN ID
1	lan0	192.168.0.1	255.255.255.0	0
				<span style="font-size: 2em;">+</span> <span style="font-size: 2em;">✕</span>

**Note:** The lan0 cannot be deleted.

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

**LAN**

**^ General Settings**

	<b>Index</b>	<input type="text" value="1"/>
<b>IPv4</b>	<b>Interface</b>	<input type="text" value="lan0"/> v
	<b>IP Address</b>	<input type="text" value="192.168.0.1"/>
	<b>Netmask</b>	<input type="text" value="255.255.255.0"/>
	<b>MTU</b>	<input type="text" value="1500"/>

General Settings @ LAN		
Item	Description	Default
Index	Indicate ordinal of list.	--
Interface	Show editing port. The lan1 is available only if it was selected by one of ETH0~ETHn in <b>Ethernet &gt; Ports &gt; Port Settings</b> .	lan0
IPv4 Address	Set IP address of the LAN port.	192.168.0.1
Netmask	Set Netmask of the LAN port.	255.255.255.0
MTU	Enter Maximum Transmission Unit.	1500

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

**^ DHCP Settings**

<b>Enable</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
<b>Mode</b>	<input type="text" value="Server"/> v
<b>IP Pool Start</b>	<input type="text" value="192.168.0.2"/>
<b>IP Pool End</b>	<input type="text" value="192.168.0.100"/>
<b>Subnet Mask</b>	<input type="text" value="255.255.255.0"/>

**^ DHCP Advanced Settings**

<b>Gateway</b>	<input type="text"/>
<b>Primary DNS</b>	<input type="text"/>
<b>Secondary DNS</b>	<input type="text"/>
<b>WINS Server</b>	<input type="text"/>
<b>Lease Time</b>	<input type="text" value="120"/> ?
<b>Static Lease</b>	<input type="text"/> ?
<b>Expert Options</b>	<input type="text"/> ?
<b>Debug Enable</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

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

^ DHCP Settings

Enable  ON  OFF

Mode Relay v

DHCP Server For Relay

^ DHCP Advanced Settings

Debug Enable  ON  OFF

LAN		
Item	Description	Default
<b>DHCP Settings</b>		
Enable	Click the toggle button to enable/disable the DHCP function.	ON
Mode	Select from “Server” or “Relay”. <ul style="list-style-type: none"> <li>Server: Lease IP address to DHCP clients which have been connected to LAN port</li> <li>Relay: The router can be a DHCP Relay, which will provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet</li> </ul>	Server
IPv4 Pool Start	Define the beginning of the pool of IP addresses that will be leased to DHCP clients.	192.168.0.2
IPv4 Pool End	Define the end of the pool of IP addresses that will be leased to DHCP clients.	192.168.0.100
Subnet Mask	Define the subnet mask of the IP address obtained by DHCP clients from the DHCP server.	255.255.255.0
DHCP Server for Relay	Enter the IP address of the DHCP relay server.	Null
<b>DHCP Advanced Settings</b>		
Gateway	Define gateway address assigned by the DHCP server to the clients, which must be on the same network segment as the DHCP address pool.	Null
Primary DNS	Define primary DNS server address assigned by the DHCP server to the clients.	Null
Secondary DNS	Define secondary DNS server address assigned by the DHCP server to the clients.	Null
WINS Server	Define Windows Internet Naming Service obtained by DHCP clients from DHCP sever.	Null
Lease Time	Set lease time in which the client can use the IP address obtained from the DHCP server, measured in seconds.	120
Static lease	Bind a lease to correspond to an IP address via MAC address. format: MAC, IP; MAC, IP;..., e.g. FF:ED:CB:A0:98:01,192.168.0.200	Null
Expert Options	Enter some other options of the DHCP server in this field. format: config-desc;config-desc, e.g. log-DHCP;quiet-DHCP	Null

LAN		
Item	Description	Default
Debug Enable	Click the toggle button to enable/disable this option. Enable DHCP information output.	OFF

## Multiple IP

LAN
Multiple IP
Tagged VLAN
Status

^ Multiple IP Settings

Index	Interface	IP Address	Netmask	
				+

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

**Multiple IP**

^ IP Settings

Index

Interface  v

IP Address

Netmask

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

## Tagged VLAN

LAN
Multiple IP
Tagged VLAN
Status

^ VLAN Settings

Index	Enable	Interface	VID	IP Address	Netmask	
						+

You may click **+** to add a VLAN to the LAN port or click **X** to delete the VLAN of the LAN port. Now, click **✎** to edit the VLAN of the LAN port.

**Tagged VLAN**

^ **VLAN Settings**

**Index**

**Enable** ON OFF

**Interface**  v

**VID**

**IP Address**

**Netmask**

Submit
Close

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



## Status

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

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

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

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

### 3.2.3 Ethernet

This section allows you to set the related parameters for Ethernet. There may be multi-Ethernet ports in the device. The ETH0 in the device can be configured as either a WAN port or LAN port, while other Ethernet port(s) can only be configured as LAN ports. The default settings of all Ethernet ports are lan0 and their default IP is 192.168.0.1/255.255.255.0.

Note:

- 1) R2000 Dual can supply power to the behind device via ETH1~ETH4(enable the POE in Ports settings).
- 2) R3000 Lite has only one Ethernet port which can only be configured as LAN.
- 3) R2000 Lite has only one Ethernet port which can only be configured as LAN.
- 4) R1510 Lite has only one Ethernet port which can only be configured as LAN.

Ports		Status	
<b>^ Port Settings</b>			
Index	Port	Port Assignment	Port Enable
1	eth0	lan0	true
2	eth1	lan0	true
3	eth2	lan0	true
4	eth3	lan0	true
5	eth4	lan0	true

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

**Ports**

**^ Port Settings**

Index:

Port:

Port Assignment:

Port Enable:  ON  OFF

Note: R3000 Quad/R2110/R5020 does not support the "Port Enable" feature.

Port Settings		
Item	Description	Default
Index	Indicate ordinal of list.	--
Port	Show editing port, read-only.	--
Port Assignment	Choose Ethernet port type, such as a WAN port or LAN port. When setting the port as a LAN port, you can click the drop-down list to select from "lan0" or "lan1".	lan0
Port Enable	eth0: When the WAN switch to LAN, this function needs to reboot to take effect. eth1: Enable or disable the port	ON
POE Enable (Optional)	Click to enable or disable the POE function. When the POE function is enabled, it will connect the POE voltage.	ON

## Status

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



Ports			Status
<b>^ Port Status</b>			
Index	Port	Link	
1	eth0	Down	
2	eth1	Down	
3	eth2	Down	
4	eth3	Up	


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

Ports			Status
<b>^ Port Status</b>			
Index	Port	Link	
1	eth0	Down	
2	eth1	Down	
3	eth2	Down	
4	eth3	Up	
		<b>Index</b>	4
		<b>Port</b>	eth3
		<b>Link</b>	Up

### 3.2.4 Cellular

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

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

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

**Cellular**

^ **General Settings**

Index	<input type="text" value="1"/>	
SIM Card	<input type="text" value="SIM1"/> v	
Phone Number	<input type="text"/>	
PIN Code	<input type="text"/>	?
MCC+MNC Code	<input type="text"/>	?
Extra AT Cmd	<input type="text"/>	?
Telnet Port	<input type="text" value="0"/>	?
Waiting For Update APN	<input type="text" value="90"/>	?

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

^ **Cellular Network Settings**

Network Type	<input style="border: 2px solid red;" type="text" value="Auto"/> v	?
Band Select Type	<input type="text" value="All"/> v	?

^ **Advanced Settings**

Debug Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
Verbose Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	
Timeout For Network Registration	<input type="text" value="0"/>	?
Preferred Using CID3	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?

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

Note:

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

^ **Cellular Network Settings**

Network Type	<input type="text" value="Auto"/> v	?
Band Select Type	<input style="border: 2px solid red;" type="text" value="Specify"/> v	?

### ^ Band Settings

GSM 850	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 1800	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
GSM 1900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 800	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 850	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 1900	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 2100	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
WCDMA 1700	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 1	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 3	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 5	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 7	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 8	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
LTE Band 20	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

### ^ Advanced Settings

Debug Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Verbose Debug Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF
Timeout For Network Registration	<input type="text" value="0"/>
Preferred Using CID3	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF

Cellular		
Item	Description	Default
<b>General Settings</b>		
Index	Indicate ordinal of list.	--
SIM Card	Show currently editing SIM card.	SIM1
Phone Number	Enter phone number of the SIM card.	Null
PIN Code	Enter a 4-8 characters PIN code used for unlocking the SIM.	Null
MCC+MNC Code	Enter 5-6 digits and semicolon endings must be used. Used to lock the device can only use the specified carrier SIM card.	Null
Extra AT Cmd	Enter AT commands used for cellular initialization.	Null

Cellular		
Item	Description	Default
Telnet Port	Specify the Port listening of telnet service, used for AT over Telnet.	0
Waiting For Update APN	The time interval for automatically updating the APN after connecting to the network. Unit: second The modem needs to support automatic update APN feature. e.g.: HL7618RD	90
Cellular Network Settings		
Network Type	Select the cellular network type, which is the network access order. Select from "Auto", "2G Only", "2G First", "3G Only", "3G First", "4G Only", and "4G First". <ul style="list-style-type: none"> <li>Auto: Connect to the best signal network automatically.</li> <li>2G Only: Only the 2G network is connected.</li> <li>2G First: Connect to the 2G Network preferentially.</li> <li>3G Only: Only the 3G network is connected.</li> <li>3G First: Connect to the 3G Network preferentially.</li> <li>4G Only: Only the 4G network is connected.</li> <li>4G First: Connect to the 4G Network preferentially.</li> </ul> <p><b>Note:</b></p> <p>1) There may be some different optional network types due to the different cellular modules.</p> <p>2) Click "?" Character in the menu for help to see the details.</p>	Auto
Band Select Type	Select from "All" or "Specify". You may choose certain bands if choosing "Specify".	All
Advanced Settings		
Debug Enable	Click the toggle button to enable/disable this option. Enable debugging information output.	ON
Verbose Debug Enable	Click the toggle button to enable/disable this option. Enable verbose debugging information output.	OFF
Timeout For Network Registration	The timeout is required for the module to register to the network. Unit: seconds. 0 means the default setting is used.	0
Preferred Using CID3	Click the toggle button to enable/disable this option. Enable using APN3 to access the Internet. Some operators need to use APN3 to access the Internet normally, just like Verizon and it can be turned on if necessary	OFF

## Status

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

Cellular	Status	AT Debug										
<b>^ Status</b> <table border="1"> <thead> <tr> <th>Index</th> <th>Modem Status</th> <th>Modem Model</th> <th>IMSI</th> <th>Registration</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Ready</td> <td>EG25</td> <td><div style="width: 100px; height: 10px; background-color: #ccc;"></div></td> <td>Registered to home network</td> </tr> </tbody> </table>			Index	Modem Status	Modem Model	IMSI	Registration	1	Ready	EG25	<div style="width: 100px; height: 10px; background-color: #ccc;"></div>	Registered to home network
Index	Modem Status	Modem Model	IMSI	Registration								
1	Ready	EG25	<div style="width: 100px; height: 10px; background-color: #ccc;"></div>	Registered to home network								

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

Cellular
Status
AT Debug

^ Status

Index	Modem Status	Modem Model	IMSI	Registration
1	Ready	EG25		Registered to home network

**Index** 1

**Modem Status** Ready

**Modem Model** EG25

**Current SIM** SIM1

**Phone Number**

**IMSI**

**ICCID**

**Registration** Registered to home network

**Network Provider** CHN-UNICOM

**Network Type** LTE

**Band** 3

**Signal Strength** 23 (-67dBm)

**RSRP** -97 dBm

**RSRQ** -8 dB

**Bit Error Rate** 99

**PLMN ID** 46001

**Local Area Code** 251B

**Cell ID** 6074702

**IMEI**

**Firmware Version** EG25GGBR07A07M2G\_01.001.01.001

**SINR** 21 dB

**Physical Cell ID** 83

Status	
Item	Description
Index	Indicate ordinal of list.
Modem Status	Show status of radio module.
Modem Model	Show model of radio module.
Current SIM	Show the SIM card that your router is using.
Phone Number	Show phone number of current SIM. <b>Note:</b> This option will be displayed if entered manually in <b>Cellular &gt;SIM1/ SIM2 &gt; General Settings &gt; Phone Number.</b>
IMSI	Show IMSI number of current SIM.
ICCID	Show ICCID number of current SIM.

Status	
Item	Description
Registration	Show current network status.
Network Provider	Show name of the Network Provider.
Network Type	Show current network service type, e.g., GPRS.
Band	Show band of the current network.
Signal Strength	Show signal strength. (Only valid for 2/3/4G network, please refer to RSRP for 5G network)
RSRP	Show Reference Signal Received Power value. (Only valid for 4G or 5G networks)
RSRQ	Show Reference Signal Received Quality value. (Only valid for 4G or 5G networks)
Bit Error Rate	Show current bit error rate.
PLMN ID	Show current PLMN ID.
Local Area Code	Show current local area code used for identifying the different areas.
Cell ID	Show current cell ID used for locating the router.
IMEI	Show IMEI (International Mobile Equipment Identity) number of the radio module.
Firmware Version	Show current firmware version of cellular module.
SINR	Show signal to interference plus noise ratio. (Only for 4G network or 5G network)
Physical Cell ID	Show Physical Cell ID.

## AT Debug

This section allows you to do the AT Debug.

Cellular
Status
AT Debug

^ AT Debug

**Command**

**Result**

AT Debug		
Item	Description	Default
Command	Enter AT command that you want to send to the cellular module in this text box.	Null
Result	Show AT command responded by the cellular module in this text box.	Null
<input style="background-color: #2c5e8c; color: white; padding: 2px 5px; border: none;" type="button" value="Send"/>	Click the button to send AT command.	--



## 3.2.5 Wi-Fi

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

### Wi-Fi AP

#### Configure Router as Wi-Fi AP

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

#### 2.4GHz Wi-Fi Only

WiFi	Access Point	Advanced	ACL	Status
<b>^ General Settings</b>				
Mode <input type="text" value="AP"/> ?				
Region <input type="text" value="SE"/> ?				

#### 2.4GHz and 5GHz Wi-Fi

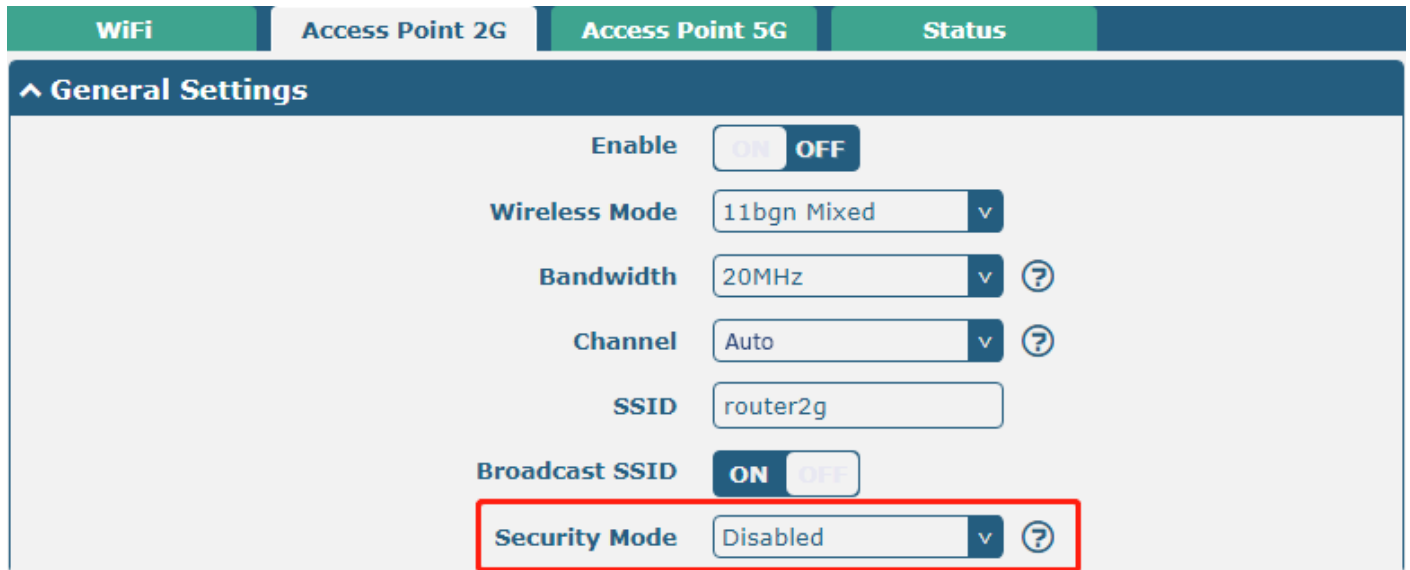
WiFi	Access Point 2G	Access Point 5G	Status
<b>^ General Settings</b>			
Mode <input type="text" value="AP"/> ?			
Region <input type="text" value="SE"/> ?			

#### Note:

- 1) Please remember to click **Save & Apply > Reboot** after finishing the configuration, the change would take effect.
- 2) Only R2110 and R5020 supports 2.4GHz and 5GHz.

## Access Point 2G

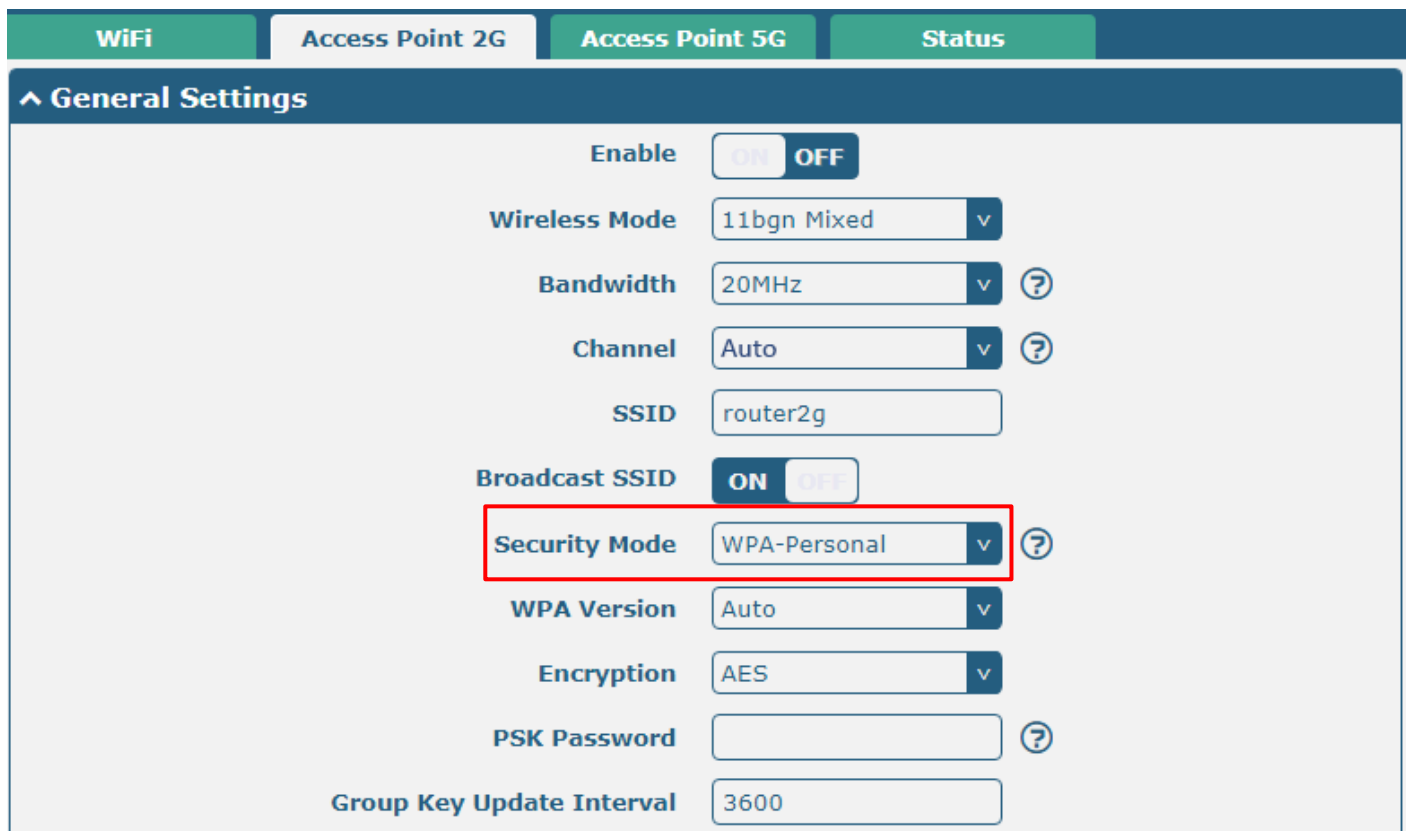
Click the **Access Point 2G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as “Disabled”.



The screenshot shows the configuration interface for the Access Point 2G. The 'Access Point 2G' tab is selected. Under 'General Settings', the 'Security Mode' dropdown menu is highlighted with a red box and is currently set to 'Disabled'. Other settings include: Enable (OFF), Wireless Mode (11bgn Mixed), Bandwidth (20MHz), Channel (Auto), SSID (router2g), and Broadcast SSID (ON).

WiFi	Access Point 2G	Access Point 5G	Status
<b>General Settings</b>			
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
Wireless Mode	11bgn Mixed		
Bandwidth	20MHz		
Channel	Auto		
SSID	router2g		
Broadcast SSID	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF		
Security Mode	Disabled		

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



The screenshot shows the configuration interface for the Access Point 2G with the 'Security Mode' dropdown menu highlighted by a red box and set to 'WPA-Personal'. Additional security settings are visible: WPA Version (Auto), Encryption (AES), PSK Password (empty), and Group Key Update Interval (3600).

WiFi	Access Point 2G	Access Point 5G	Status
<b>General Settings</b>			
Enable	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
Wireless Mode	11bgn Mixed		
Bandwidth	20MHz		
Channel	Auto		
SSID	router2g		
Broadcast SSID	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF		
Security Mode	WPA-Personal		
WPA Version	Auto		
Encryption	AES		
PSK Password			
Group Key Update Interval	3600		

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

**^ General Settings**

Enable  ON  OFF

Wireless Mode 11bgn Mixed

Bandwidth 20MHz

Channel Auto

SSID router2g

Broadcast SSID  ON  OFF

Security Mode WEP

WEP Key

General Settings @ Access Point 2G		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11bgn Mixed”, “11b only”, “11g only”, and “11n only”. <ul style="list-style-type: none"> <li>11bgn Mixed: mix three protocols for backward compatibility</li> <li>11b only: IEEE 802.11b, 11 Mbps</li> <li>11g only: IEEE 802.11g, 54 Mbps</li> <li>11n only: IEEE 802.11n, 450 Mbps</li> </ul>	11bgn Mixed
Bandwidth	Select from “20 MHz” or “40MHz”. <b>Note:</b> 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	20MHz
Channel	The channel that different bandwidths can choose is as follows. <ul style="list-style-type: none"> <li>Auto: The router will scan all frequency channels until the best one is found.</li> <li>The frequency of 1~13 channels of 20MHz bandwidth available channel:                             <ul style="list-style-type: none"> <li>1–2412 MHz</li> <li>2–2417 MHz</li> <li>3–2422 MHz</li> <li>4–2427 MHz</li> <li>5–2432 MHz</li> <li>6–2437 MHz</li> <li>7–2442 MHz</li> <li>8–2447 MHz</li> <li>9–2452 MHz</li> </ul> </li> </ul>	Auto

General Settings @ Access Point 2G		
Item	Description	Default
	10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz <ul style="list-style-type: none"> <li>The frequency of 1~13 channels of 40MHz bandwidth available channel:</li> </ul> 1–2412 MHz 2–2417 MHz 3–2422 MHz 4–2427 MHz 5–2432 MHz 6–2437 MHz 7–2442 MHz 8–2447 MHz 9–2452 MHz 10–2457 MHz 11–2462 MHz 12–2467 MHz 13–2472 MHz	
SSID	Enter SSID (Service Set Identifier), the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router2g
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of the router AP on the Wi-Fi client side.	ON
Security Mode	Select from “Disabled”, “WPA-Personal” or “WEP”. <ul style="list-style-type: none"> <li>Disabled: The user can access the Wi-Fi without a password</li> </ul> <p><b>Note:</b> <i>It is strongly recommended for security purposes that you do not choose this kind of mode.</i></p> <ul style="list-style-type: none"> <li>WPA-personal: Wi-Fi access protection, only one password is provided for identity authentication</li> <li>WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission</li> </ul>	Disabled
WPA Version	Select from “Auto”, “WPA” or “WPA2”. <ul style="list-style-type: none"> <li>Auto: Router will choose automatically the most suitable WPA version</li> <li>WPA2 is a stronger security feature than WPA</li> </ul>	Auto

General Settings @ Access Point 2G		
Item	Description	Default
Encryption	Select from "TKIP" or "AES". <ul style="list-style-type: none"> <li>TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication</li> <li>AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP</li> </ul> <p><b>Note:</b> The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.</p>	Auto
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time of group key renewal.	3600
WEP Key	Enter WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

^ **Advanced Settings**

**Max Associated Stations**  ?

**Beacon Interval**  ?

**DTIM Period**  ?

**Enable Short GI**  ON  OFF ?

**Enable AP Isolation**  ON  OFF ?

**Debug Level**  v

Advanced Settings @ Access Point 2G		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router's AP. (Value 0 means without limitation)	0
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set delivery traffic indication message period and the router AP will multicast the data according to this period.	2
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a	ON

Advanced Settings @ Access Point 2G		
Item	Description	Default
	long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless devices can't access each other.	OFF
Debug Level	Select from "verbose", "debug", "info", "notice", "warning", or "none".	none

^ ACL Settings

Enable ACL  ON  OFF

ACL Mode Accept v ?

^ Access Control List

Index	Description	MAC Address	+

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

Access Point 2G

^ Access Control List

Index

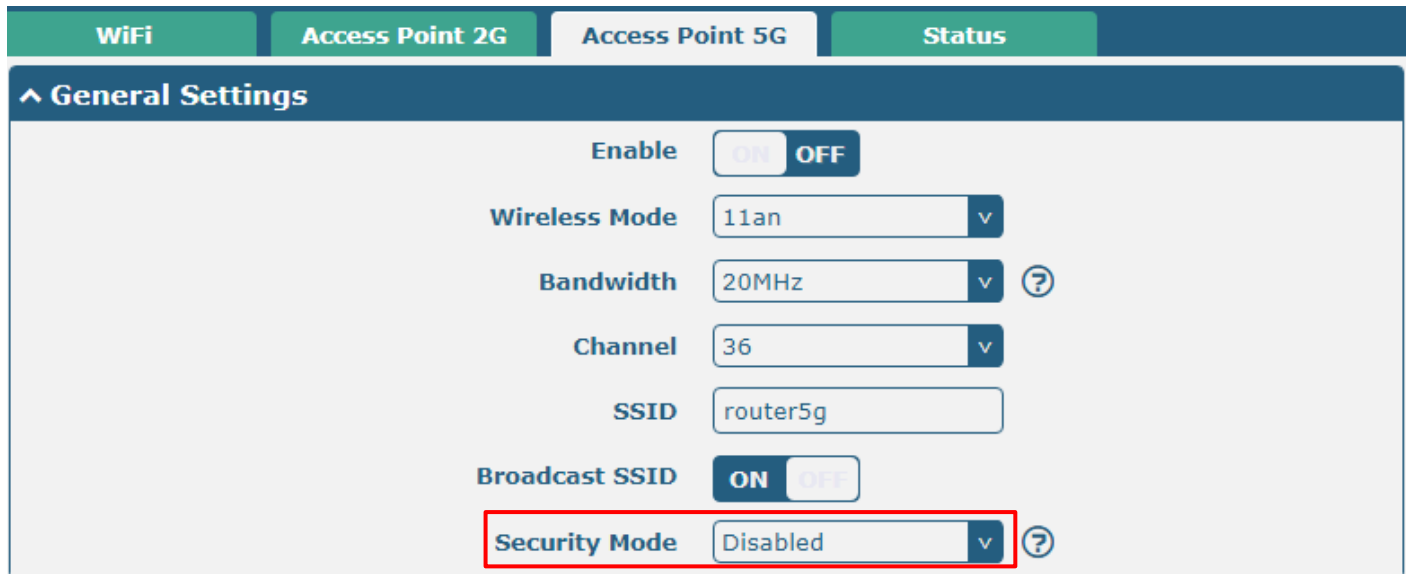
Description

MAC Address

ACL Settings @ Access Point 2G		
Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from "Accept" or "Deny". <ul style="list-style-type: none"> <li>Accept: Only the packets fitting the entities of the "Access Control List" can be allowed</li> <li>Deny: All the packets fitting the entities of the "Access Control List" will be denied</li> </ul> <p><b>Note:</b> The router can only allow or deny devices that are included in the "Access Control List" at one time.</p>	Accept
Access Control List @ Access Point 2G		
Index	Indicate ordinal of list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

## Access Point 5G

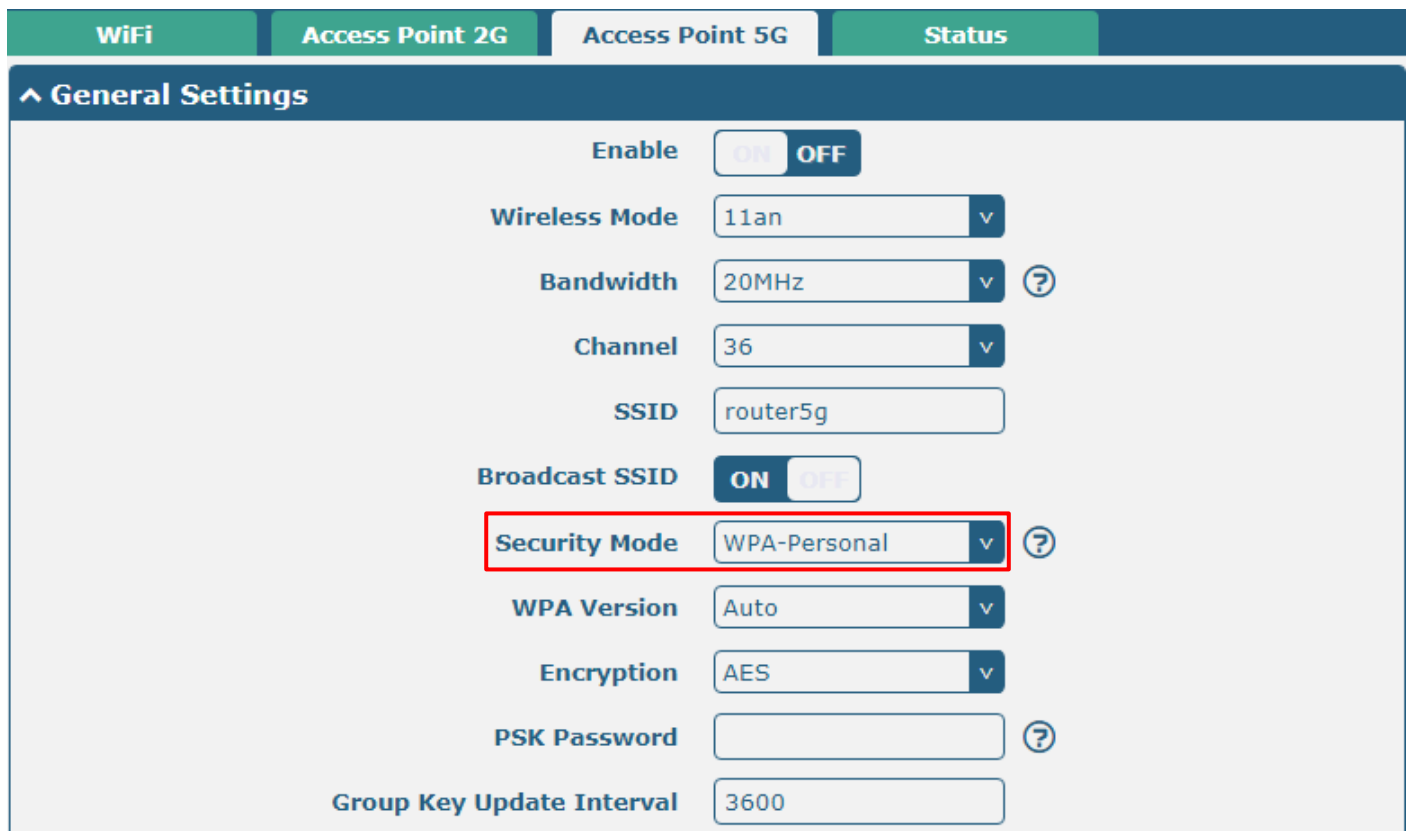
Click the **Access Point 5G** column to configure the parameters of Wi-Fi AP. By default, the security mode is set as “Disabled”.



The screenshot shows the 'Access Point 5G' configuration page. The 'Security Mode' dropdown menu is highlighted with a red box and is currently set to 'Disabled'. Other settings include: Enable (ON/OFF), Wireless Mode (11an), Bandwidth (20MHz), Channel (36), SSID (router5g), and Broadcast SSID (ON/OFF).

WiFi	Access Point 2G	Access Point 5G	Status
^ General Settings			
Enable	<input type="checkbox"/> ON <input type="checkbox"/> OFF		
Wireless Mode	11an v		
Bandwidth	20MHz v ?		
Channel	36 v		
SSID	router5g		
Broadcast SSID	<input type="checkbox"/> ON <input type="checkbox"/> OFF		
Security Mode	Disabled v ?		

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



The screenshot shows the 'Access Point 5G' configuration page with the 'Security Mode' dropdown menu highlighted by a red box and set to 'WPA-Personal'. Additional security settings are visible: WPA Version (Auto), Encryption (AES), PSK Password (empty), and Group Key Update Interval (3600).

WiFi	Access Point 2G	Access Point 5G	Status
^ General Settings			
Enable	<input type="checkbox"/> ON <input type="checkbox"/> OFF		
Wireless Mode	11an v		
Bandwidth	20MHz v ?		
Channel	36 v		
SSID	router5g		
Broadcast SSID	<input type="checkbox"/> ON <input type="checkbox"/> OFF		
Security Mode	WPA-Personal v ?		
WPA Version	Auto v		
Encryption	AES v		
PSK Password	?		
Group Key Update Interval	3600		

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

WiFi
Access Point 2G
Access Point 5G
Status

^ General Settings

Enable
 ON  OFF

Wireless Mode

11an
v

Bandwidth

20MHz
v
?

Channel

36
v

SSID

Broadcast SSID
 ON  OFF

Security Mode

WEP
v

?

WEP Key

?

General Settings @ Access Point 5G		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Wi-Fi access point option.	OFF
Wireless Mode	Select from “11an”, or “11a/an/ac”. <ul style="list-style-type: none"> <li>11an: Compatible IEEE 802.11a, 54 Mbps and IEEE 802.11n, 300Mbps</li> <li>11a/an/ac: Compatible IEEE 802.11a, 54 Mbps, IEEE802.11n 300 Mbps and 802.11ac, 867 Mbps</li> </ul>	11an
Bandwidth	Select from “20MHz”, “40MHz” or “80MHz”. <p><b>Note:</b> 40 MHz channel width provides twice the data rate available over a single 20 MHz channel; the data transfer rate of 80MHz bandwidth is 4 times greater than that of a single 20Mhz bandwidth.</p>	20MHz
Channel	The optional channels for bandwidths are as below. <ul style="list-style-type: none"> <li>The frequency of 36~165 channels of 20MHz bandwidth available channels:                             <ul style="list-style-type: none"> <li>36–5180 MHz</li> <li>40–5200 MHz</li> <li>44–5220 MHz</li> <li>48–5240 MHz</li> <li>149–5745 MHz</li> <li>153–5765 MHz</li> <li>157–5785 MHz</li> <li>161–5805 MHz</li> <li>165–5825 MHz</li> </ul> </li> <li>The frequency of 36~165 channels of 40MHz bandwidth available channels:</li> </ul>	36



General Settings @ Access Point 5G		
Item	Description	Default
	<p>36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz</p> <ul style="list-style-type: none"> <li>The frequency of 36~165 channels of 80MHz bandwidth available channels: 36–5180 MHz 40–5200 MHz 44–5220 MHz 48–5240 MHz 149–5745 MHz 153–5765 MHz 157–5785 MHz 161–5805 MHz 165–5825 MHz</li> </ul> <p><b>Note:</b> All available channels of 5GHz Wi-Fi on different bandwidths are listed above. Web parameters should be configured due to the different available channels in different countries and areas.</p>	
SSID	Enter SSID (Service Set Identifier), the name of your wireless network. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Enter 1 to 32 characters.	router5g
Broadcast SSID	Click the toggle button to enable/disable the SSID being broadcast. When enabled, the client can scan your SSID. When disabled, the client cannot scan your SSID. If you want to connect to the router AP, you need to manually enter the SSID of the router AP on the Wi-Fi client side.	ON
Security Mode	<p>Select from “Disabled”, “WPA-Personal”, or “WEP”.</p> <ul style="list-style-type: none"> <li>Disabled: The user can access the Wi-Fi without a password</li> </ul> <p><b>Note:</b> It is strongly recommended for security purposes that you do not choose this kind of mode.</p> <ul style="list-style-type: none"> <li>WPA-personal: Wi-Fi access protection, only one password is provided for identity authentication</li> <li>WEP: Wired Equivalent Privacy provides encryption for wireless device’s data transmission</li> </ul>	Disabled

General Settings @ Access Point 5G		
Item	Description	Default
WPA Version	Select from "Auto", "WPA" or "WPA2". <ul style="list-style-type: none"> <li>Auto: Router will choose automatically the most suitable WPA version</li> <li>WPA2 is a stronger security feature than WPA</li> </ul>	Auto
Encryption	Select from "TKIP" or "AES". <ul style="list-style-type: none"> <li>TKIP: Temporal Key Integrity Protocol (TKIP) encryption uses a wireless connection. TKIP encryption can be used for WPA-PSK and WPA 802.1x authentication</li> <li>AES: AES encryption uses a wireless connection. AES can be used for CCMP WPA-PSK and WPA 802.1x authentication. AES is a stronger encryption algorithm than TKIP</li> </ul> <p><b>Note:</b> The security mode will affect the wireless communication rate. Different wireless modes support different encryption modes. For example, 802.11n supports neither WEP security mode nor the TKIP algorithm. If they are used, the wireless communication rate will reduce to 54Mbps (802.11g mode). It is recommended to select AES in 802.11n mode.</p>	AES
PSK Password	Enter Pre-share key password. Enter 8 to 63 characters.	Null
Group Key Update Interval	Enter the time of group key renewal.	3600
WEP Key	Enter WEP key. The key length should be 10 or 26 hexadecimal digits depending on which WEP key is used, 64 digits or 128 digits.	Null

^ Advanced Settings

<b>Max Associated Stations</b>	<input type="text" value="0"/>	?
<b>Beacon Interval</b>	<input type="text" value="100"/>	?
<b>DTIM Period</b>	<input type="text" value="2"/>	?
<b>RTS Threshold</b>	<input type="text" value="2347"/>	?
<b>Fragmentation Threshold</b>	<input type="text" value="2346"/>	?
<b>Transmit Power</b>	<input type="text" value="Max"/>	v
<b>Enable WMM</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	
<b>Enable Short GI</b>	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF	?
<b>Enable AP Isolation</b>	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF	?
<b>Debug Level</b>	<input type="text" value="none"/>	v

Advanced Settings @ Access Point 5G		
Item	Description	Default
Max Associated Stations	Set the max number of clients allowed to access the router’s AP. (Value 0 means without limitation)	0
Beacon Interval	Set the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.	100
DTIM Period	Set delivery traffic indication message period and the router AP will multicast the data according to this period.	2
RTS Threshold	Set “request to send” threshold. When the threshold is set as 2347, the router AP will not send a detection signal before sending data. And when the threshold is set as 0, the router AP will send a detection signal before sending data.	2347
Fragmentation Threshold	Set fragmentation threshold of a Wi-Fi AP. It is recommended that you use the default value 2346.	2346
Transmit Power	Select from “Max”, “High”, “Medium” or “Low”.	Max
Enable WMM	Click the toggle button to enable/disable the WMM option.	ON
Enable Short GI	Click the toggle button to enable/disable the Short Guard Interval option. Short GI is a blank time between two symbols, providing a long buffer time for signal delay. Using the Short GI would increase 11% in data rates, but also result in higher packet error rates.	ON
Enable AP Isolation	Click the toggle button to enable/disable the AP isolation option. When enabled, the router will isolate all connected wireless devices. The wireless devices cannot access each other.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning”, or “none”.	none

**^ ACL Settings**

Enable ACL  ON  OFF

ACL Mode

**^ Access Control List**

Index	Description	MAC Address	
			+

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

**^ Access Control List**

Index

Description

MAC Address

ACL Settings @ Access Point 5G		
Item	Description	Default
Enable ACL	Click the toggle button to enable/disable this option.	OFF
ACL Mode	Select from "Accept" or "Deny". <ul style="list-style-type: none"> <li>Accept: Only the packets fitting the entities of the "Access Control List" can be allowed</li> <li>Deny: All the packets fitting the entities of the "Access Control List" will be denied</li> </ul> <i>Note: The router can only allow or deny devices that are included in the "Access Control List" at one time.</i>	Accept
Access Control List @ Access Point 5G		
Index	Indicate ordinal of list.	--
Description	Enter a description for this access control list.	Null
MAC Address	Add a MAC address here.	Null

## Status

This section allows you to view the status of AP.

WiFi
Access Point 2G
Access Point 5G
Status

^ AP Status 2G

Status FAILED

Channel

Channel Width

MAC Address

^ Associated Stations 2G

Index	MAC Address	IP Address	Name	Connected Time	Signal

^ AP Status 5G

^ Associated Stations 5G

Index	MAC Address	IP Address	Name	Connected Time	Signal

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

## Wi-Fi Client

### Configure Router as Wi-Fi Client

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

The screenshot shows the 'WiFi' configuration page with the 'Status' tab selected. Under 'General Settings', the following options are visible:

- Mode:** Client (dropdown menu)
- Client Band:** 2.4G (dropdown menu)
- Region:** SE (text input)

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

The screenshot shows the 'Status' page with the 'WLAN Status' section expanded. The left sidebar shows the 'Interface' list with 'WLAN' highlighted. The main content area shows the following details for the WLAN interface:

- Status:** Disconnected
- Uptime:**
- IP Address:**
- Gateway:**
- DNS:**
- MAC Address:**
- Channel:**

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

The screenshot shows the 'WLAN Settings' page with the following configuration:

- SSID:** router
- Connect to Hidden SSID:** OFF
- Password:**

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

Status

^ WLAN Status

**Status** Connected

**Uptime** 0 days, 00:00:17

**IP Address** 192.168.1.128/255.255.255.0

**Gateway** 192.168.1.253

**DNS** 172.16.0.1 202.96.209.6

**MAC Address** 00:23:a7:a4:13:e4

### 3.2.6 USB

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

USB

Key

^ General Settings

**Enable USB**  ON  OFF

**Enable Automatic Upgrade**  ON  OFF

#### Key

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

USB

Key

^ Key

**USB Automatic Upgrade Key**

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

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

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

### 3.2.7 DI/DO

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

#### DI

DI	DO	Status	
<b>^ DI Settings</b>			
Index	Enable	Mode	Inversion
1	false	ON-OFF	false

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

DI

^ General Settings

Index

Enable  ON  OFF

Mode  v

Inversion  ON  OFF

Alarm On Content

Alarm Off Content

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

**DI**

^ **General Settings**

Index

Enable  ON  OFF

Mode  v

Inversion  ON  OFF

Threshold Value

Alarm On Content

Alarm Off Content

General Settings @ DI		
Item	Description	Default
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable the digital input function.	OFF
Mode	Select from “ON-OFF” or “Counter”. <ul style="list-style-type: none"> <li>ON-OFF: Alarm mode can be triggered at the DI access ON-OFF.</li> <li>Counter: Event counter mode.</li> </ul>	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 counted. Set the threshold value to trigger the DI alarm when the count value reaches the threshold value.	0
Alarm On Content	Show content when the alarm is on.	Alarm On
Alarm Off Content	Show content when the alarm is off.	Alarm Off

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

## DO

DI
DO
Status

^ **DO Settings**

Index	Enable	Alarm On Action	Alarm Off Action	Initial State	Alarm Source	
1	false	High	Low	Last	DI1 Alarm	

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



**DO**

**^ General Settings**

Index	<input type="text" value="1"/>
Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Alarm On Action	<input type="text" value="High"/> v
Alarm Off Action	<input type="text" value="Low"/> v
Initial State	<input type="text" value="Last"/> v
Delay	<input type="text" value="0"/> ?
Hold Time	<input type="text" value="0"/> ?
Alarm Source	<input type="text" value="DI1 Alarm"/> v

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

**DO**

**^ General Settings**

Index	<input type="text" value="1"/>
Enable	<input type="button" value="ON"/> <input type="button" value="OFF"/>
Alarm On Action	<input type="text" value="Pulse"/> v
Alarm Off Action	<input type="text" value="Low"/> v
Initial State	<input type="text" value="Last"/> v
Delay	<input type="text" value="0"/> ?
Hold Time	<input type="text" value="0"/> ?
Low-level Width	<input type="text" value="1000"/> ?
High-level Width	<input type="text" value="1000"/> ?
Alarm Source	<input type="text" value="DI1 Alarm"/> v

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

**DO**

^ **General Settings**

**Index**

**Enable**

**Alarm On Action**  v

**Alarm Off Action**  v

**Initial State**  v

**Delay**  ?

**Hold Time**  ?

**Low-level Width**  ?

**High-level Width**  ?

**Alarm Source**  v

General Settings @ DO		
Item	Description	Default
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable this DO.	OFF
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> <li>High: a high electrical level output.</li> <li>Low: a low electrical level output.</li> <li>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.</li> </ul>	High
Alarm Off Action	Digital Output initiates when the alarm is removed. Selected from “High”, “Low” or “Pulse”. <ul style="list-style-type: none"> <li>High: a high electrical level output.</li> <li>Low: a low electrical level output.</li> <li>Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.</li> </ul>	Low
Initial State	Specify the Digital Output status when powered on. Selected from “Last”, “High” or “Low”. <ul style="list-style-type: none"> <li>Last: DO’s status will consist of the status of the last power off.</li> <li>High: DO interface is in high electrical level.</li> <li>Low: DO interface is in low electrical level.</li> </ul>	Last
Delay (unit: 100ms)	Set delay time for DO alarm start-up. The first pulse will be generated after a “Delay”. Enter from 0 to 3000 (0=generate pulse without delay).	0
Hold Time (unit: s)	Set hold time of DO status (Alarm On Action/Alarm Off Action). When the action time reaches this specified time, DO will stop the action. Enter from 0 to 3000 seconds.	0

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

### Status

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

DI
DO
Status

^ DI Status

Index	Level	Status	Count
1	Low	Alarm off	

^ Action Of Clear

Counter Alarm Of DI 1 Clear

^ DO Status

Index	Level	Low-level Width	High-level Width
1	Low		

^ DO Control

Level Of DO1 Toggle

### 3.2.8 AI

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

Note:

1) R1520 support an AI interface.

AI	Status			
<b>^ AI Settings</b>				
Index	Enable	Input Type	Interval	
1	false	Voltage	5	

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

**AI**

**^ General Settings**

Index

Enable

**Input Type**

Min Threshold

Max Threshold

Interval

The window is displayed below when the “input type” is “Current”.

**AI**

**^ General Settings**

Index

Enable

**Input Type**

Min Threshold

Max Threshold

Interval

AI (Analog Input)		
Item	Description	Default
Index	Indicate ordinal of list.	--
Enable	Click the switch button to "ON" to turn on the analog input function.	OFF
Input type	Select from "Voltage" or "Current". <ul style="list-style-type: none"> <li>Voltage: The data collected is voltage.</li> <li>Current: The data collected is Current.</li> </ul>	Voltage
Min Threshold @Voltage	Set minimum voltage threshold. When the voltage collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: V.	3
Max Threshold @Voltage	Set maximum voltage threshold. When the voltage collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: V.	20
Min Threshold @Current	Set minimum current threshold. When the current collected by the AI interface is less than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	4
Min Threshold @Current	Set maximum current threshold. When the current collected by the AI interface is greater than the minimum voltage threshold, an event notification will be triggered. Unit: mA.	16
Interval	Collect latest data every few seconds.	5

### Status

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

AI
Status

**^ AI Status**

Index	Type	Min Threshold	Max Threshold	Value
1	voltage	3	20	
		<b>Index</b>	1	
		<b>Type</b>	voltage	
		<b>Min Threshold</b>	3	
		<b>Max Threshold</b>	20	

### 3.2.9 Serial Port

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

**Note:**

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

Port Type	Serial Port	Status
<b>^ General Settings</b>		
Serial Port Type	RS485 <input type="button" value="v"/>	

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

Serial Port	Status				
<b>^ Serial Port Settings</b>					
Index	Port	Enable	Baud Rate	Application Mode	
1	COM1	false	115200	Transparent	<input type="button" value="edit"/>
2	COM2	false	115200	Transparent	<input type="button" value="edit"/>

Click the right-most  button of COM1 as below.

<b>Serial Port</b>	
<b>^ Serial Port Application Settings</b>	
Index	<input type="text" value="1"/>
Port	COM1 <input type="button" value="v"/>
Enable	<input type="button" value="ON"/> <input checked="" type="button" value="OFF"/>
Baud Rate	115200 <input type="button" value="v"/>
Data Bits	8 <input type="button" value="v"/>
Stop Bits	1 <input type="button" value="v"/>
Parity	None <input type="button" value="v"/>
Flow Control	None <input type="button" value="v"/>
<b>^ Data Packing</b>	
Packing Timeout	<input type="text" value="50"/> <input type="button" value="help"/>
Packing Length	<input type="text" value="1200"/>

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

### ^ Server Setting

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

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

### ^ Server Setting

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

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

### ^ Server Setting

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

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

### ^ Server Setting

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

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

**^ Server Setting**

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

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

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

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

**^ Server Setting**

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

**Protocol**

**Local IP**

**Local Port**

**Server Address**

**Server Port**

Serial Port		
Item	Description	Default
<b>Serial Port Application Settings</b>		
Index	Indicate ordinal of list.	--
Port	Show current serial's name, read-only.	COM1
Enable	Click the toggle button to enable/disable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" or "115200".	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
<b>Data Packing</b>		
Packing Timeout	Set packing timeout. The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN/ WLAN when it reaches the Interval Timeout in the field. The unit is milliseconds. <i>Note: Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.</i>	50
Packing Length	Set 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
<b>Server Settings</b>		
Item	Description	Default
Application Mode	Select from "Transparent", "Modbus RTU Gateway", or "Modbus ASCII Gateway". <ul style="list-style-type: none"> <li>Transparent: The router will transmit the serial data transparently.</li> <li>Modbus RTU Gateway: The router will translate the Modbus RTU data to Modbus TCP data and send it out, and vice versa.</li> <li>Modbus ASCII Gateway: The router will translate the Modbus ASCII data to Modbus TCP data and send it out, and vice versa.</li> </ul>	Transp arent

Serial Port		
Item	Description	Default
Protocol	Select from "TCP Client", "TCP Server", or "UDP". <ul style="list-style-type: none"> <li>TCP Client: Router works as TCP client, initiates TCP connection to TCP server. The server address supports both IP and domain name.</li> <li>TCP Server: Router works as a TCP server, listening for a connection request from a TCP client.</li> <li>UDP: Router works as UDP client.</li> </ul>	TCP Client
Server Address	Enter address of the server which will receive the data sent from the router's serial port. IP address or domain name will be available.	Null
Server Port	Enter a specified port of the server which is used for receiving the serial data.	Null
Local IP @ Transparent	Enter router's LAN IP which will forward to the internet port of the router.	Null
Local Port @ Transparent	Enter port of the router's LAN IP.	Null
Local IP @ Modbus	Enter local IP under Modbus mode.	Null
Local Port @ Modbus	Enter local port under Modbus mode.	Null

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

Serial Port	Status															
<b>Serial Port Status list</b> <table border="1"> <thead> <tr> <th>Index</th> <th>Type</th> <th>TX</th> <th>RX</th> <th>Connection Status</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>RS232</td> <td>0B</td> <td>0B</td> <td></td> </tr> <tr> <td>2</td> <td>RS485</td> <td>0B</td> <td>0B</td> <td></td> </tr> </tbody> </table>		Index	Type	TX	RX	Connection Status	1	RS232	0B	0B		2	RS485	0B	0B	
Index	Type	TX	RX	Connection Status												
1	RS232	0B	0B													
2	RS485	0B	0B													

### 3.2.10 LoRa

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

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

General Settings	Status
<b>General Settings</b>	
Default Gateway ID	<input type="text" value="34FA40FFFE052762"/>
User Defined Gateway ID Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
User Defined Gateway ID	<input type="text" value="1234567890ABCDEF"/> <span>?</span>

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

## Status

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

General Settings
Status

^ Basic

Model

^ Packets received

CRC Errors  
Duplicates  
Join Duplicates  
Join Requests  
Total Packets

^ Packets sent

Duplicates Acked  
Packets Acked  
Total Join Responses  
Join Responses Dropped  
Total Packets  
Packets Dropped

**^ Center Frequency**

**RF Chain 0 Frequency**

**RF Chain 1 Frequency**

**^ LoRa Multi Datarate Channels**

Index	RF Chain	IF frequency
-------	----------	--------------

**^ LoRa Standard Channel**

**RF Chain**

**IF frequency**

**Bandwidth**

**Spread Factor**

**^ FSK Standard Channel**

**RF Chain**

**IF frequency**

**Bandwidth**

**Data Rate**

Status	
Item	Description
<b>Basic</b>	
Model	Show LoRa module model.
<b>Packets received</b>	
CRC Errors	Show the number of RF packets received in error.
Duplicates	Show the number of duplicate RF packets received.
Join Duplicates	Show the number of duplicate RF join request packets received.
Join Requests	Show the number of RF join request packets received.
Total Packets	Show the number of RF packets received.
<b>Packets sent</b>	
Duplicates Asked	Show the number of duplicate RF response packets sent.
Packets Asked	Show the number of RF response packets sent.
Total Join Responses	Show the number of duplicate RF join response packets sent.
Join Responses Dropped	Show the number of failed RF join response packets.
Total Packets	Show the number of RF packets sent.
Packets Dropped	Show the number of RF dropped packets.
<b>Center Frequency</b>	

Status	
Item	Description
RF Chain 0 Frequency	Center frequency of LoRa channel 0.
RF Chain 1 Frequency	Center frequency of LoRa channel 1.
LoRa Multi Datarate Channels	
RF Chain	Index of LoRa channel.
IF Frequency	IF frequency of LoRa channel.
LoRa standard Channel	
RF Chain	Index of LoRa standard channel.
IF frequency	IF frequency of LoRa standard channel.
Bandwidth	Bandwidth of LoRa standard channel.
Spread Factor	Spread Factor of LoRa standard channel.
FSK Standard Channel	
RF Chain	Index of FSK Standard Channel.
IF frequency	IF frequency of FSK Standard Channel.
Bandwidth	Bandwidth of FSK Standard Channel.
Data Rate	Data Rate of FSK Standard Channel.

### 3.3 Packet Forwarders

#### 3.3.1 Basic Station

General Settings
Status
Cert Manager

^ Gateway Settings

Enable ON OFF

TLS Enable ON OFF

Server Address

Server Port

General Settings		
Gateway Settings		
Item	Description	Default
Enable	Enable application.	OFF
TLS Enable	Enable TLS encrypted transmission.	OFF
Server Address	Server address (e.g., 127.0.0.1)	
Server Port	Server port number.	

## Status

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

General Settings
Status
Cert Manager

^ Basic

**TC Status**

**Station Version**

**Package Version (Protocol)**

**HAL Library Version**

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

This section allows you to view and import the certification.

General Settings
Status
Cert Manager

^ CA File Import ?

**CA Cert**  No file chosen Import

**Client Cert**  No file chosen Import

**Client Key**  No file chosen Import

^ Certificate Files

Index	File Name	File Size	Modification Time
Certificate Files			

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

### 3.3.2 Semtech UDP Forwarder

General Settings
RF Settings
Status

^ Gateway Settings

Enable ON OFF

LoRaWan Public ON OFF

Server Address

Server Uplink Port

Service Downlink Port

Keepalive Interval

statistics Refresh Interval

Push Timeout Millisecond

General Settings		
Gateway Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable this option.	OFF
LoRaWan Public	Click the toggle button to enable/disable this option.	ON
Server Address	Set the Server address.	127.0.0.1
Server Uplink Port	UDP uplink connection port.	1780
Service Downlink Port	UDP downlink connection port.	1782
Keepalive Interval	Time interval for obtaining downlink data.	10
Statistics Refresh Interval	Statistical interval, USI update interval.	300
Push Timeout Millisecond	Uplink data timeout.	120

## RF Settings

This section allows you to set the Radio Frequency.

General Settings
RF Settings
Status

^ RF Power Settings

**RF Power Limit**

^ RF Chain Settings

**Supported Frequency**

**Frequencies Options**  ?

**RF Chain 0 Frequency**

**RF Chain 1 Frequency**

^ LoRa Multi Datarate Channels Settings

Index	RF Chain	IF frequency	+
-------	----------	--------------	---

^ LoRa Standard Channel Settings

^ FSK Standard Channel Settings

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

RF Settings

^ LoRa Multi Datarate Channels Settings

**Index**

**RF Chain**

**IF frequency**

^ LoRa Multi Datarate Channels Settings

Index	RF Chain	IF frequency	+
1	RF Chain 0	0	✏ ✕
2	RF Chain 0	-400000	✏ ✕
3	RF Chain 0	-200000	✏ ✕
4	RF Chain 1	-400000	✏ ✕
5	RF Chain 1	-200000	✏ ✕
6	RF Chain 1	0	✏ ✕
7	RF Chain 1	200000	✏ ✕
8	RF Chain 1	400000	✏ ✕



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

^ LoRa Standard Channel Settings

Enable  ON  OFF

RF Chain RF Chain 0

IF frequency

Bandwidth 125KHz

Spread Factor SF7

Use FSK modulation instead of LoRa.

^ FSK Standard Channel Settings

Enable  ON  OFF

RF Chain RF Chain 0

IF frequency

Bandwidth 7.8KHz

Datarate

RF Settings		
Item	Description	Default
<b>RF Power Settings</b>		
RF Power Limit	Used to indicate the maximum transmit power limit for the current gateway. <ul style="list-style-type: none"> <li>No_Limit: Transmit power is not limited, depending on the transmit power value sent by the LoRaWAN server.</li> <li>EU_433: Maximum transmit power is limited to 10dbm or less.</li> <li>EU_868_870: Maximum transmit power is limited to 14dbm or less.</li> <li>CN_470_510: The maximum transmit power is limited to 17dbm or less.</li> <li>US_902_928: Maximum transmit power is limited to 26dbm or less.</li> <li>AU_915_928: Maximum transmit power limit below 26dbm.</li> <li>AS_923: Maximum transmit power is limited to 14dbm or less.</li> <li>KR_920_923: Maximum transmit power is limited to 23dbm or less.</li> <li>Max_Power: Use the maximum transmit power which is about 24.5dbm.</li> </ul> <p><i><b>Note:</b> The above options are not configurable and need to be set before delivery.</i></p>	No Limit
<b>RF Chain Settings</b>		
Supported Frequency	Choose supported frequency depending on the LoRaWAN module.	863 870

RF Settings		
Item	Description	Default
Frequencies Options	Select from "User-define", "EU868", "RU868", "KZ868".	User-define
RF Chain 0 Frequency	Enter central frequency of radio transceiver 0 which supports transmitting and receiving.	Null
RF Chain 1 Frequency	Enter center frequency of radio transceiver 1 which only supports receiving data from nodes.	Null
LoRa Multi Datarate Channels Settings		
Index	Indicate ordinal of list.	--
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	RF Chain 0
IF frequency	Enter IF frequency, measured in Hz. The offset between the central frequency of a specific channel and the central frequency of the chain is 0/1. E.g.: RF Chain 0, IF frequency: -20000. It means the central frequency of this channel should be 868300000=868500000-200000.	0
LoRa Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0
IF frequency	Enter IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of a specific channel and the center frequency of chain 0/1.	0
Bandwidth	Choose selectable bandwidth, measured in kHz.	500KHz
Spread Factor	Enter selectable spreading factor. The channel with a large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.	250000
FSK Standard Channel Settings		
Enable	Click the toggle button to enable/disable this option.	OFF
RF Chain	Choose Chain 0 or Chain 1 as RF Chain.	Chain 0
IF frequency	Enter IF frequency valued from -500000 to 500000, and measured in Hz. The offset between the center frequency of a specific channel and the center frequency of the chain is 0/1.	0
Bandwidth	Choose selectable bandwidth, measured in kHz.	500KHz
Datarate	Enter data rate valued from 500 to 250000 and measured in Bit.	250000

## Status

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

General Settings

RF Settings

Status

^ Basic

**Status**

**Packet Forwarder (Protocol)**

**HAL Library Version**

^ Uplink

**RF packets received**

**RF packets received State**

**RF packets forwarded**

**Push Data Datagrams Sent**

**Push Data Acknowledged**

^ Downlink

**Pull Data Sent**

**Pull Resp Datagrams Received**

**RF Packets Sent to Concentrator**

**RF Packets Sent Errors**

Status	
Item	Description
<b>Basic</b>	
Status	Show LoRaWAN status of your gateway.
Packet Forwarder (Protocol)	Show version of Packet forwarder.
HAL Library Version	Show driver version of LoRaWAN chipset inside gateway.
<b>Uplink</b>	
RF packets received	Show count of data packet from node to gateway.

Status	
Item	Description
RF packets received State	Show the RF packets receiving state. <ul style="list-style-type: none"> <li>CRC_OK: Percentage of CRC verification</li> <li>CRC_Fail: Percentage of CRC verification failure</li> <li>NO_CRC: Percentage of abnormal packets without CRC</li> </ul>
RF packets forwarded	Packets that CRC verified are sent from gateway to server.
Push Data Datagrams Sent	Total quantity of packets sent from gateway to server, including RF packets forwarded and statistics packets.
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent:
Downlink	
Pull Data Sent	Show the number of keepalive packets sent to the server, and the percentage of acknowledged packets regarding the keepalive packet from the server.
Pull Resp Datagrams Received	Show packet counts and size that will be sent from server to gateway.
RF Packets Sent to Concentrator	Show RF packet counts and size that will be sent from gateway to node.
RF Packets Sent Errors	Show RF packet counts that fail to be sent from server to node.

## 3.4 Network

### 3.4.1 Route

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

#### Static Route

Static Route		Status					
^ Static Route Table <span style="float: right;">?</span>							
Index	Description	Destination	Netmask	Gateway	Interface	VID	+

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

**Static Route**

^ **Static Route**

**Index**

**Description**

**Destination**

**Netmask**

**Gateway**

**Interface**  v

**VID**  ?

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

## Status

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

Static Route
Status

^ **Route Table**

Index	Destination	Netmask/Prefix Length	Gateway	Interface	Metric
1	0.0.0.0	0.0.0.0	192.168.10.1	wlan0	0
2	192.168.0.0	255.255.255.0	0.0.0.0	lan0	0
3	192.168.10.0	255.255.255.0	0.0.0.0	wlan0	0

### 3.4.2 Firewall

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

Filtering
NAT
Advanced
Custom Rules
Status

^ General Settings

Enable Filtering  ON  OFF

Default Filtering Policy Accept

^ Access Control Settings

Enable Remote SSH Access  ON  OFF

Enable Local SSH Access  ON  OFF

Enable Remote Telnet Access  ON  OFF

Enable Local Telnet Access  ON  OFF

Enable Remote HTTP Access  ON  OFF

Enable Local HTTP Access  ON  OFF

Enable Remote HTTPS Access  ON  OFF

Enable Remote Ping Respond  ON  OFF

Enable DOS Defending  ON  OFF

Enable VPN NAT Traversal  ON  OFF

^ Whitelist Rules

Index	Description	Source Address	+
			+

Click  to add the whitelist rules.

Filtering

^ Whitelist Rules

Index

Description

Source Address

**^ Filtering Rules**

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

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

**Filtering**

**^ Filtering Rules**

Index

Description

Source Address  ?

Source MAC  ?

Target Address  ?

**Protocol**  v

Action  v

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

**^ Filtering Rules**

Index

Description

Source Address  ?

Source Port  ?

Source MAC  ?

Target Address  ?

Target Port  ?

**Protocol**  v

Action  v

Filtering		
Item	Description	Default
<b>General Settings</b>		
Enable Filtering	Click the toggle button to enable/disable the filtering option.	ON
Default Filtering Policy	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list</li> <li>Drop: Router will drop all the connecting requests except the hosts which fit the accepted filter list</li> </ul>	Accept
<b>Access Control Settings</b>		
Enable Remote SSH Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via SSH.	OFF
Enable Local SSH Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via SSH.	ON
Enable Remote Telnet Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via Telnet.	OFF
Enable Local Telnet Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via Telnet.	OFF
Enable Remote HTTP Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTP.	OFF
Enable Local HTTP Access	Click the toggle button to enable/disable this option. When enabled, the LAN user can access the router locally via HTTP.	ON
Enable Remote HTTPS Access	Click the toggle button to enable/disable this option. When enabled, the Internet user can access the router remotely via HTTPS.	ON
Enable Remote Ping Respond	Click the toggle button to enable/disable this option. When enabled, the router will reply to the Ping requests from other hosts on the Internet.	ON
Enable DOS Defending	Click the toggle button to enable/disable this option. When enabled, the router will defend the DOS. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Enable VPN nat traversal	Click the toggle button to enable/disable this option. When enabled, enable NAT traversal for GRE / L2TP / PPTP VPN packets.	OFF
<b>Whitelist Rules</b>		
Index	Indicate ordinal of list.	--
Description	Enter a description for this whitelist rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
<b>Filtering Rules</b>		
Index	Indicate ordinal of list.	--
Description	Enter a description for this filtering rule.	Null
Source Address	Specify an access originator and enter its source address.	Null
Source Port	Specify an access originator and enter its source port.	Null
Source MAC	Specify an access originator and enter its source MAC address.	Null
Target Address	Enter target address which the access originator wants to access.	Null
Target Port	Enter target port that the access originator wants to access.	Null



Filtering		
Item	Description	Default
Protocol	Select from "All", "TCP", "UDP", "ICMP", "ICMPv6" or "TCP-UDP". <b>Note:</b> It is recommended that you choose "All" if you don't know which protocol of your application to use.	All
Action	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: When Default Filtering Policy is dropped, the router will drop all the connecting requests except the hosts which fit this accepted filtering list.</li> <li>Drop: When Default Filtering Policy is accepted, the router will accept all the connecting requests except the hosts which fit this drop filtering list.</li> </ul>	Drop

## NAT

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

Filtering
NAT
Advanced
Custom Rules
Status

^ DMZ Settings

Enable DMZ  ON  OFF

Host IP Address

Source IP Address  ?

^ Port Mapping Rules ?

Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol	+
-------	-------------	-----------	---------------	----------	------------	----------	---

^ NAT Rules ?

Index	Description	Source Address	Out	Target Address	NAT IP	+
-------	-------------	----------------	-----	----------------	--------	---

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

Click "Network> Firewall> NAT> DMZ". The following information is displayed:

^ DMZ Settings

Enable DMZ  ON  OFF

Host IP Address

Source IP Address  ?

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

Port mapping is defined manually in the router, and all data received from certain ports on the public network is forwarded to a certain port on a certain IP in the internal network. Click “**Network> Firewall> NAT> Port Mapping**” to display the following:

^ Port Mapping Rules <span style="float: right;">?</span>						
Index	Description	Remote IP	Internet Port	Local IP	Local Port	Protocol
<span>+</span>						

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

### NAT

^ Port Mapping Rules

<b>Index</b>	<input type="text" value="1"/>
<b>Description</b>	<input type="text"/>
<b>Remote IP</b>	<input type="text"/> <span style="float: right;">?</span>
<b>Remote Port</b>	<input type="text"/> <span style="float: right;">?</span>
<b>Internet IP</b>	<input type="text"/> <span style="float: right;">?</span>
<b>Interface</b>	<input type="text" value="unspecified"/> <span style="float: right;">v</span>
<b>Internet Port</b>	<input type="text"/> <span style="float: right;">?</span>
<b>Local IP</b>	<input type="text"/>
<b>Local Port</b>	<input type="text"/> <span style="float: right;">?</span>
<b>Protocol</b>	<input type="text" value="TCP-UDP"/> <span style="float: right;">v</span>

Port Mapping Rules		
Item	Description	Default
Index	Indicate ordinal of list.	--
Description	Enter a description for this port mapping.	Null
Remote IP	Specify the host or network which can access the local IP address. Empty means unlimited, e.g., 10.10.10.10/255.255.255.255 or 192.168.1.0/24.	Null
Remote Port	Specify the port of the host or network which can access the local IP address. Empty means unlimited.	Null
Internet IP	Enter Internet IP of the router which can be accessed by other hosts from	Null

Port Mapping Rules		
Item	Description	Default
	the Internet.	
Interface	Choose corresponding port of the link that you want to configure.	Unspecified
Internet Port	Enter Internet port of the router which can be accessed by other hosts from Internet.	Null
Local IP	Enter router's LAN IP which will forward to the Internet port of router.	Null
Local Port	Enter port of router's LAN IP.	Null
Protocol	Select from "TCP", "UDP" or "TCP-UDP" as your application required.	TCP-UDP

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

^ NAT Rules <span style="float: right;">?</span>						
Index	Description	Source Address	Out	Target Address	NAT IP	+

Click **+** to add custom rules.

**^ NAT Settings**

?

Index

Description

Source Address  ?

Out  v

Target Address  ?

NAT IP  ?

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

## Advanced

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

Filtering	NAT	Advanced	Custom Rules	Status
<b>^ Advanced Settings</b>				
Enable Ipset		<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF		
Default Input Policy		Accept <input type="button" value="v"/>		
MAC List Name		mac <input type="button" value="?"/>		
MAC List Action		Drop <input type="button" value="v"/>		
IP Port List Name		ip-port <input type="button" value="?"/>		
IP Port List Action		Drop <input type="button" value="v"/>		
Net List Name		net <input type="button" value="?"/>		
Net List Action		Drop <input type="button" value="v"/>		
<b>^ MAC List</b> <input type="button" value="?"/>				
Index	MAC	<input type="button" value="+"/>		
<b>^ IP Port List</b> <input type="button" value="?"/>				
Index	Protocol	IP	Port	<input type="button" value="+"/>
<b>^ Net List</b> <input type="button" value="?"/>				
Index	Net	<input type="button" value="+"/>		

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

Advanced	
<b>^ MAC List</b>	
Index	<input type="text" value="1"/>
MAC	<input type="text"/>
<input type="button" value="Submit"/> <input type="button" value="Close"/>	

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

**Advanced**

^ **IP Port List**

**Index**

**Protocol**  v

**IP**

**Port**  ?

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

**Advanced**

^ **Net List**

**Index**

**Net**  ?

<b>Advanced</b>		
<b>Item</b>	<b>Description</b>	<b>Default</b>
<b>General Settings</b>		
Enable Ipset	Click the toggle button to enable/disable the Ipset option.	ON
Default Input Policy	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: Router will accept all the connecting requests except the hosts which fit the drop list of MAC/ IP-Port/ Net.</li> <li>Drop: Router will drop all the connecting requests except the hosts which fit the accepted list of MAC/ IP-Port/ Net.</li> </ul>	Accept
MAC List Name	Enter the name of the MAC list. It cannot support entering pure numbers.	mac
MAC List Action	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: When Default Input Policy is dropped, the router will drop all the connecting requests except the hosts which fit this accepted MAC list.</li> <li>Drop: When Default Input Policy is accepted, the router will accept all the connecting requests except the hosts which fit this drop MAC list.</li> </ul>	Drop
IP Port List Name	Enter name of the MAC list. It cannot support entering pure numbers.	ip-port

Advanced		
Item	Description	Default
IP Port List Action	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: When Default Input Policy is dropped, the router will drop all the connecting requests except the hosts which fit this accepted IP Port list.</li> <li>Drop: When Default Input Policy is accepted, the router will accept all the connecting requests except the hosts which fit this drop IP Port list.</li> </ul>	Drop
Net List Name	Enter the name of the MAC list. It cannot support entering pure numbers.	net
Net List Action	Select from "Accept" or "Drop". <ul style="list-style-type: none"> <li>Accept: When Default Input Policy is dropped, the router will drop all the connecting requests except the hosts which fit this accepted Net list.</li> <li>Drop: When Default Input Policy is accepted, the router will accept all the connecting requests except the hosts which fit this drop Net list.</li> </ul>	Drop
MAC List		
Index	Indicate ordinal of the list.	--
MAC address	Enter the MAC address. Format: XX:XX:XX:XX:XX:XX.	Null
IP Port list		
Index	Indicate ordinal of list.	--
Protocol	Select from "TCP", or "UDP".	TCP
IP	Enter IP address.	Null
Port	Enter port number.	Null
Net list		
Index	Indicate ordinal of list.	--
Net	Enter domain name/ IP/ IP segment	Null

## Custom Rules

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

Filtering	NAT	Advanced	Custom Rules	Status
<b>^ Custom Iptables Rules</b>				
Index	Description	Rule	+	

Click  to add custom rules.

## Custom Rules

### ^ Custom Iptables Rule

Index

Description

Rule  ?

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

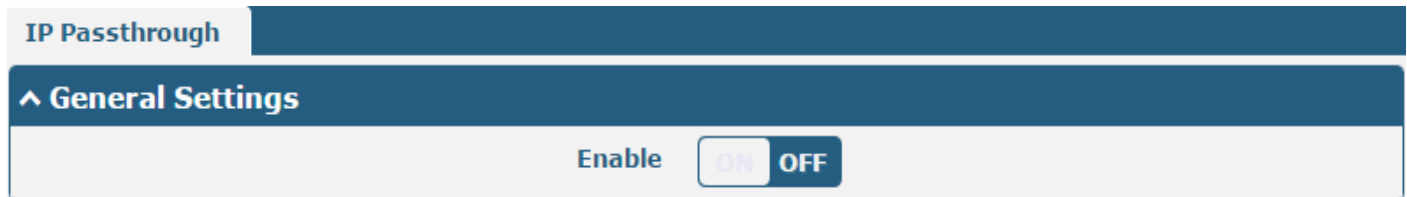
## Status

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

Filtering	NAT	Advanced	Custom Rules	Status			
<b>^ Chain Input</b>							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
2	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
3	0	DROP	all	*	*	0.0.0.0/0	0.0.0.0/0
4	0	DROP	tcp	lan+	*	0.0.0.0/0	0.0.0.0/0
5	0	REJECT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
6	69	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
7	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
8	0	ACCEPT	tcp	*	*	0.0.0.0/0	0.0.0.0/0
9	0	DROP	tcp	*	*	0.0.0.0/0	0.0.0.0/0
10	0	ACCEPT	icmp	*	*	0.0.0.0/0	0.0.0.0/0
11	0	DROP	icmp	*	*	0.0.0.0/0	0.0.0.0/0
<b>^ Chain Forward</b>							
Index	Packets	Target	Protocol	In	Out	Source	Destination
1	0	TCPMSS	tcp	*	*	0.0.0.0/0	0.0.0.0/0
<b>^ Chain Output</b>							
Index	Packets	Target	Protocol	In	Out	Source	Destination
<b>^ Chain Prerouting</b>							
Index	Packets	Target	Protocol	In	Out	Source	Destination
<b>^ Chain Postrouting</b>							
Index	Packets	Target	Protocol	In	Out	Source	Destination

### 3.4.3 IP Passthrough

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



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

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

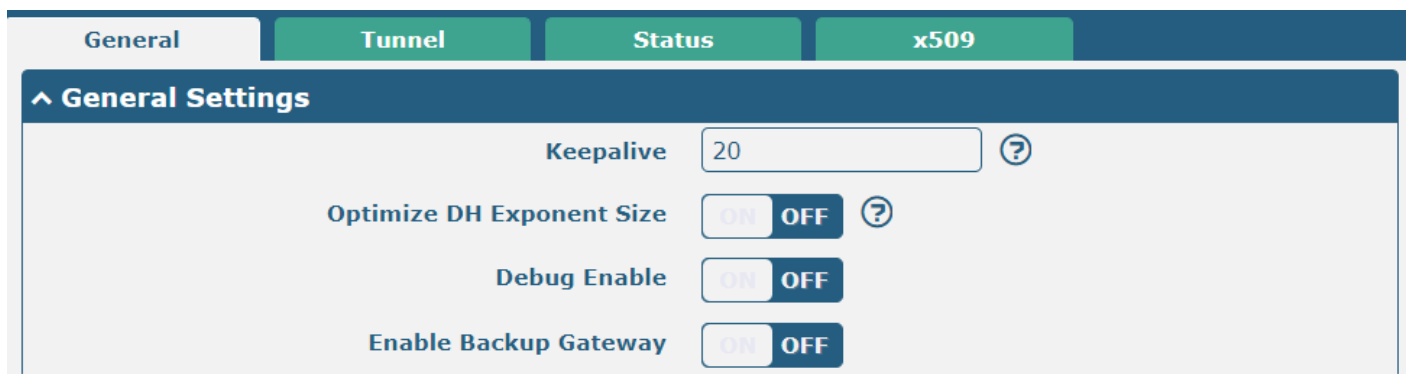
## 3.5 VPN

### 3.5.1 IPsec

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

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

#### General





The window is displayed as below when enabling “Enable Backup Gateway”.

The screenshot shows the configuration page for the 'x509' tunnel. The 'General Settings' section includes the following options:

- Keepalive: 20
- Optimize DH Exponent Size: OFF
- Debug Enable: OFF
- Enable Backup Gateway: ON** (highlighted with a red box)
- Monitor Interval: 30
- Monitor Times: 5

General Settings @ General		
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 IPsec VPN information output to the debug port.	OFF
Enable Backup Gateway		
Monitor Interval	Enter Monitor Interval. Unit: second.	30
Monitor Times	Enter number maxim of IPsec primary router not answered.	5

## Tunnel

The screenshot shows the 'Tunnel Settings' section with the following table structure:

Index	Enable	Description	Gateway	Local Subnet	Remote Subnet	+
-------	--------	-------------	---------	--------------	---------------	---

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

**^ General Settings**

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

General Settings @ Tunnel		
Item	Description	Default
Index	Indicate ordinal of list.	--
Enable	Click the toggle button to enable/disable this IPsec tunnel.	ON
Description	Enter a description for this IPsec tunnel.	Null
Gateway	Enter address of remote side IPsec VPN server. 0.0.0.0 represents any address.	Null
Backup Gateway	Enter backup address of remote side IPsec VPN server. Empty means disable.	Null
Mode	Select from "Tunnel" and "Transport". <ul style="list-style-type: none"> <li>Tunnel: Commonly used between routers, or at an end-station to a router, the router acting as a proxy for the hosts behind it.</li> <li>Transport: Used between end-stations or between an end-station and a router, if the router is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.</li> </ul>	Tunnel
Protocol	Select the security protocols from "ESP" and "AH". <ul style="list-style-type: none"> <li>ESP: Use the ESP protocol.</li> <li>AH: Use the AH protocol.</li> </ul>	ESP
Local Subnet	Enter local subnet's address with a mask protected by IPsec, e.g., 192.168.1.0/24.	Null
Local Protoport	Enter protocol with port, e.g., tcp/443; udp/1701. Local protoport and remote protoport must be the same if both are not empty.	Null
Remote Subnet	Enter remote subnet's address with a mask protected by IPsec, e.g., 10.8.0.0/24.	Null
Remote Protoport	Enter protocol with port, e.g., tcp/443; udp/1701. Local protoport and remote protoport must be the same if both are not empty.	Null
Link binding	Select link to build IPsec.	Unbound

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

**^ IKE Settings**

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

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

**^ IKE Settings**

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

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

**^ IKE Settings**

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

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

**^ IKE Settings**

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

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

### ^ IKE Settings

IKE Type	<input type="text" value="IKEv1"/>	v	
Negotiation Mode	<input type="text" value="Main"/>	v	
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	
<b>Authentication Type</b>	<input type="text" value="xAuth CA"/>	v	
Private Key Password	<input type="text"/>		
Username	<input type="text"/>		?
Password	<input type="text"/>		?
IKE Lifetime	<input type="text" value="86400"/>		?

IKE Settings		
Item	Description	Default
IKE Type	Select from “IKEv1” and “IKEv2”.	IKEv1
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPsec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SA can be established as long as the username and password are correct.	Main
Encrypt Algorithm	Select from “3DES”, “AES128”, “AES192” and “AES256” to be used in IKE negotiation. <ul style="list-style-type: none"> <li>3DES: Use 168-bit 3DES encryption algorithm in CBC mode.</li> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode.</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode.</li> <li>AES256: Use 256-bit AES encryption algorithm in CBC mode.</li> </ul>	3DES
Authentication Algorithm	Select from “MD5”, “SHA1”, “SHA2 256”, or “SHA2 512” to be used in IKE negotiation.	SHA1
IKE DH Group	Select from “DHgroup1”, “DHgroup2”, “DHgroup5”, “DHgroup14”, “DHgroup15”, “DHgroup16”, “DHgroup17”, or “DHgroup18” to be used in key negotiation phase 1.	DHgroup2
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK”, “PKCS#12”, and “xAuth CA” to be used in IKE negotiation. <ul style="list-style-type: none"> <li>PSK: Pre-shared Key.</li> <li>CA: Certification Authority.</li> <li>xAuth: Extended Authentication to AAA server.</li> <li>PKCS#12: Exchange digital certificate authentication.</li> </ul>	PSK
PSK Secret	Enter pre-shared key.	Null
Local ID Type	Select from “Default”, “FQDN” and “User FQDN” for IKE negotiation. <ul style="list-style-type: none"> <li>Default: Uses an IP address as the ID in IKE negotiation.</li> </ul>	Default

IKE Settings		
Item	Description	Default
	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>	
Remote ID Type	Select from "Default", "FQDN" and "User FQDN" for IKE negotiation. <ul style="list-style-type: none"> <li>Default: Uses an IP address as the ID in IKE negotiation.</li> <li>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.</li> <li>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.</li> </ul>	Default
IKE Lifetime	Set lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter private key under "CA" and "xAuth CA" authentication types.	Null
Username	Enter username used for "xAuth PSK" and "xAuth CA" authentication types.	Null
Password	Enter password used for "xAuth PSK" and "xAuth CA" authentication types.	Null

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

**Tunnel**

^ **General Settings**

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

v **IKE Settings**

^ **SA Settings**

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

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

**Tunnel**

^ **General Settings**

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

v **IKE Settings**

^ **SA Settings**

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"/>	?

^ **Advanced Settings**

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



SA Settings		
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.	SHA1
PFS Group	Select from "PFS(N/A)", "DHgroup1", "DHgroup2", "DHgroup5", "DHgroup14", "DHgroup15", "DHgroup16", "DHgroup17" or "DHgroup18" to be used in SA negotiation.	PFS(N/A)
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 interval after which DPD is triggered if no IPsec protected packets is received from the peer. DPD is Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPsec packet, DPD checks the time the last IPsec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgement within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgement 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 timeout of DPD (Dead Peer Detection) packets.	150
Advanced Settings		
Enable Compression	Click the toggle button to enable/disable this option. Enable to compress the inner headers of IP packets.	OFF
Enable Forceencaps	Click the toggle button to enable/disable this option. After it is enabled, even if no NAT condition is detected, the UDP encapsulation of esp packets is forced. This may help overcome restrictive firewalls.	OFF
Contrack Flush	Click the toggle button to enable/disable this option. Clear contrack after establishing IPsec.	OFF
Expert Options	Add more PPP configuration options here, format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none.	Null

## Status

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

General
Tunnel
Status
x509

**^ IPsec Tunnel Status**

Index	Description	Status	Uptime
-------	-------------	--------	--------

**^ Proxy Identity Status**

index	Destination gateway	Source address	Destination address	Status	Tunnel
-------	---------------------	----------------	---------------------	--------	--------

## x509

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

General
Tunnel
Status
x509

**^ X509 Settings** ?

**Tunnel Name**

**Local Certificate**  No file chosen

**Remote Certificate**  No file chosen

**Private Key**  No file chosen

**CA Certificate**  No file chosen

**PKCS#12 Certificate**  No file chosen

**^ Certificate Files**

Index	File Name	File Size	Modification Time
-------	-----------	-----------	-------------------

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

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

### 3.5.2 WireGuard

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

Click **“VPN> WireGuard”** to set the WireGuard parameters.

WireGuard
Status
x509

**^ General Settings**

**Enable WireGuard**  ON  OFF

**Private Key**

**IP Address**  ?

**Listen Port**

**MTU**

**Enable NAT**  ON  OFF

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

**Note:** Click for help.

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

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

**WireGuard**

**^ Peer Settings**

Index:

Description:

Public Key:

Preshared Key:

Endpoint Host:

Endpoint Port:

Allowed IPs:  ?

Route Allowed IPs:  ON  OFF ?

Persistent Keepalive:  ?

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

## Status

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

The interface shows a navigation bar with 'WireGuard', 'Status', and 'x509' tabs. Below it is a section titled 'WireGuard Tunnel Status' with a table header containing: Index, Description, Public Key, Virtual IP, Real IP, Port, Latest Handshake.

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

The interface shows 'X509 Settings' with three rows of controls:
 

- Private Key: **Generate** button
- Private Key:  No file chosen **Import** button
- Public Key: **Generate** button
- Config File: **Generate** button
- Config File:  No file chosen **Import** button

x509		
Item	Descriptions	Default
<b>X509 Settings</b>		
Private Key	Click <b>Generate</b> button to generate a private key.	--
Private Key	Click <input type="button" value="Choose File"/> button to locate the private key from your computer, and then click <b>Import</b> button to import the private key.	--
Public Key	Click <b>Generate</b> button to generate a public key.	--
Config File	Click <b>Generate</b> button to generate a config file	--
Config File	Click <input type="button" value="Choose File"/> button to locate the config file from your computer, and then click <b>Import</b> button to import the config file.	--

### 3.5.3 OpenVPN

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

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

## OpenVPN

OpenVPN	Status	x509		
<b>^ Tunnel Settings</b>				
Index	Enable	Description	Mode	+
<b>^ Password Manage</b>				
Index	Username			+
<b>^ Client Manage</b>				
Index	Enable	Common Name	Client IP Address	+

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

**^ General Settings**

Index:

Enable:  ON  OFF

Description:

Mode: P2P

TLS Mode:

Protocol:

Peer Address:

Peer Port:

Listen IP Address:

Listen Port:

Interface Type:

Authentication Type:

Local IP:

Remote IP:

Keepalive Interval:

Keepalive Timeout:

TUN MTU:

Max Frame Size:

Enable Compression:  ON  OFF

Enable NAT:  ON  OFF

Verbose Level:

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

**^ General Settings**

Index

Enable  ON  OFF

Description

Mode

Private Key Password

Enable Client Status  ON  OFF

Enable NAT  ON  OFF

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

**^ General Settings**

Index

Enable  ON  OFF

Description

Mode

Protocol

Peer Address

Peer Port

Interface Type

Authentication Type

Renegotiation Interval

Keepalive Interval

Keepalive Timeout

TUN MTU

Max Frame Size

Enable Compression  ON  OFF

Enable NAT  ON  OFF

Enable DNS overrid  ON  OFF

Verbose Level

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

**^ General Settings**

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



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

### ^ General Settings

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

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

### ^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="Preshared"/> <input type="button" value="v"/> <input type="button" value="?"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Renegotiation Interval	<input type="text" value="86400"/> <input type="button" value="?"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

### ^ General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="Password"/> <input type="button" value="v"/> <input type="button" value="?"/>
Username	<input type="text"/>
Password	<input type="text"/>
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"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

**^ General Settings**

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> <input type="button" value="v"/> <input type="button" value="?"/>
Protocol	<input type="text" value="UDP"/> <input type="button" value="v"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/> <input type="button" value="v"/>
Authentication Type	<input type="text" value="X509CA"/> <input type="button" value="v"/> <input type="button" value="?"/>
Encrypt Algorithm	<input type="text" value="BF"/> <input type="button" value="v"/>
Authentication Algorithm	<input type="text" value="SHA1"/> <input type="button" value="v"/>
Renegotiation Interval	<input type="text" value="86400"/> <input type="button" value="?"/>
Keepalive Interval	<input type="text" value="20"/> <input type="button" value="?"/>
Keepalive Timeout	<input type="text" value="120"/> <input type="button" value="?"/>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <input type="button" value="?"/>
Verbose Level	<input type="text" value="0"/> <input type="button" value="v"/> <input type="button" value="?"/>

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

**^ General Settings**

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Description	<input type="text"/>
Mode	<input type="text" value="Client"/> <span>?</span>
Protocol	<input type="text" value="UDP"/>
Peer Address	<input type="text"/>
Peer Port	<input type="text" value="1194"/>
Interface Type	<input type="text" value="TUN"/>
Authentication Type	<span style="border: 2px solid red; padding: 2px;"><input type="text" value="X509CA Password"/></span> <span>?</span>
Username	<input type="text"/>
Password	<input type="text"/>
Encrypt Algorithm	<input type="text" value="BF"/>
Authentication Algorithm	<input type="text" value="SHA1"/>
Renegotiation Interval	<input type="text" value="86400"/> <span>?</span>
Keepalive Interval	<input type="text" value="20"/> <span>?</span>
Keepalive Timeout	<input type="text" value="120"/> <span>?</span>
TUN MTU	<input type="text" value="1500"/>
Max Frame Size	<input type="text"/>
Private Key Password	<input type="text"/>
Enable Compression	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable NAT	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Enable DNS overrid	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <span>?</span>
Verbose Level	<input type="text" value="0"/> <span>?</span>

**^ Advanced Settings**

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

General Settings @ OpenVPN		
Item	Description	Default
Index	Indicate ordinal of 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 “Auto”, “P2P”, “Client” or “Server”.	P2P

General Settings @ OpenVPN		
Item	Description	Default
Protocol	Select from "UDP", "TCP-Client", or "TCP-Server".	UDP
Server Address	Enter end-to-end IP address or domain of remote OpenVPN server.	Null
Server Port	Enter end-to-end listener port or listener port of OpenVPN server.	1194
Listen IP Address	Enter IP address or domain name.	Null
Listen Port	Enter listener port at this end.	1194
Interface Type	Select from "TUN", and "TAP" which are two different kinds of device interfaces for OpenVPN. The difference between TUN and TAP devices is that a TUN device is a point-to-point virtual device on the network while a TAP device is a virtual device on Ethernet.	TUN
Username	Enter username used for the "Password" or "X509CA Password" authentication type.	Null
Password	Enter password used for the "Password" or "X509CA Password" authentication type.	Null
Authentication Type	Select from "None", "Preshared", "Password", "X509CA", and "X509CA Password". <b>Note:</b> "None" and "Preshared" authentication types are only working with P2P mode.	None
Enable IP Pool	Click the toggle button to enable/disable this option. When enabled, the client will obtain a virtual IP from the address pool. <b>Note:</b> Enable IP Pool is available only "Mode" is Server.	OFF
Local IP	Enter the local virtual IP.	10.8.0.1
Remote IP	Enter the remote virtual IP.	10.8.0.2
Client Subnet	Client virtual IP network address.	10.8.0.0
Client Subnet Netmask	Client virtual IP network address mask.	255.255.255.0
Encrypt Algorithm	Select from "BF", "DES", "DES-EDE3", "AES-128", "AES-192", and "AES-256". <ul style="list-style-type: none"> <li>BF: Use 128-bit BF encryption algorithm in CBC mode</li> <li>DES: Use 64-bit DES encryption algorithm in CBC mode</li> <li>DES-EDE3: Use 192-bit 3DES encryption algorithm in CBC mode</li> <li>AES128: Use 128-bit AES encryption algorithm in CBC mode</li> <li>AES192: Use 192-bit AES encryption algorithm in CBC mode</li> <li>AES256: Use 256-bit AES encryption algorithm in CBC mode</li> </ul>	BF
Authentication Algorithm	Select from "MD5", "SHA1", "SHA256" or "SHA512".	SHA1
Max Clients	Set retention timeout. If the connection continues to timeout during this time, the OpenVPN tunnel will be re-established. <b>Note:</b> Max Clients is available only "Mode" is Server.	10
Renegotiation Interval	Set renegotiation interval. If the connection failed, OpenVPN will renegotiate when the renegotiation interval is reached.	86400
Keepalive Interval	Set a keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Set keepalive timeout. Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120

General Settings @ OpenVPN		
Item	Description	Default
TUN MTU	Set MTU for the tunnel.	1500
Max Frame Size	Set shard size of the data to be transmitted through the tunnel.	Null
Private Key Password	Enter private key password under "X509CA" and "X509CA password" authentication.	Null
Enable Compression	Click the switch button to enable/disable this option. When enabled, this feature compresses the header of the IP packet.	ON
Enable DNS override	Click the switch button to enable/disable this option. When enabled, DNS pushed by the server is received as the local DNS server.	OFF
Enable Bridge With LAN0	Click the toggle button to enable/disable this option. When enabled, the virtual interface can be bridged with Lan0. <b>Note:</b> Enable Bridge with LAN0 available only "Mode" is Client.	ON
Enable Default Gateway	Click the toggle button to enable/disable this option. When enabled, it will receive the gateway pushed by the server as the local gateway.	OFF
Enable Client Status	Click the toggle button to enable/disable this option. After the server is enabled, it can display the connected client status information.	OFF
Enable NAT	Click the toggle button to enable/disable the NAT option. When enabled, the source IP address of the host behind the 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"> <li>0: No output except fatal errors</li> <li>1~4: Normal usage range</li> <li>5: Output R and W characters to the console for each packet read and write</li> <li>6~11: Debug info range</li> </ul>	0
Advanced Settings @ OpenVPN		
Item	Description	Default
Enable HMAC Firewall	Click the toggle button to enable/disable this option. Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Click the toggle button to enable/disable the PKCS#12 certificate. It is an exchange of digital certificate encryption standards, used to describe personal identity information.	OFF
Enable nsCertType	Click the toggle button to enable/disable nsCertType. Require that the peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	Enter some other options of OpenVPN in this field. Each expression can be separated by a ','.	Null

## Status

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

OpenVPN
Status
x509

**^ OpenVPN Tunnel Status**

Index	Description	Status	Mode	Uptime	Local IP
-------	-------------	--------	------	--------	----------

**^ OpenVPN Client List**

Index	Common Name	Virtual IP	Real IP	Port
-------	-------------	------------	---------	------

## X509

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

OpenVPN
Status
x509

**^ X509 Settings** ?

**Mode**  v

**Tunnel Name**  v

**Root CA**  ↑

**Certificate File**  ↑

**Private Key**  ↑

**TLS-Auth Key**  ↑

**PKCS#12 Certificate**  ↑

**^ Certificate Files**

Index	File Name	File Size	Modification Time
-------	-----------	-----------	-------------------

x509		
Item	Description	Default
<b>X509 Settings</b>		
Tunnel Name	Choose a valid tunnel. Select from "Tunnel 1", "Tunnel 2", "Tunnel 3", "Tunnel 4", "Tunnel 5", or "Tunnel 6".	Tunnel 1
Mode	The mode selected in Tunnel	Client
Root CA	Click "Choose File" to locate Root CA file and then import this file into your router.	--
Certificate File	Click "Choose File" to locate Certificate file, and then import this file into your router.	--
Private Key	Click "Choose File" to locate Private Key file, and then import this file into your router.	--
TLS-Auth Key	Click "Choose File" to locate TLS-Auth Key file, and then import this file into	--



x509		
Item	Description	Default
<b>X509 Settings</b>		
	your router.	
PKCS#12 Certificate	Click "Choose File" to locate the PKCS#12 Certificate file, and then import this file into your router.	--
<b>Certificate Files</b>		
Index	Indicate ordinal of list.	--
Filename	Show imported certificate's name.	Null
File Size	Show size of certificate file.	Null
Modification Time	Show timestamp of that the last time to modify the certificate file.	Null

### 3.5.4 GRE

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

#### GRE

GRE	Status					
<b>^ Tunnel Settings</b>						
Index	Enable	Description	Bridge With LAN	Interface	Remote IP Address	+

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

**GRE**

^ **Tunnel Settings**

**Index**

**Enable**  ON  OFF

**Description**

**Bridge With LAN**  ON  OFF

**Remote IP Address**

**Local Virtual IP Address**

**Local Virtual Netmask**

**Remote Virtual IP Address**

**Enable Default Route**  ON  OFF

**Enable NAT**  ON  OFF

**Secrets**

**Link Binding**  v ?

Tunnel Settings @ GRE		
Item	Description	Default
Index	Indicate ordinal of 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
Bridge with LAN	Click the toggle button to enable/disable this option. When enabled, the virtual interface can be bridged with lan0.	OFF
Remote IP Address	Set remote real IP address of the GRE tunnel.	Null
Local Virtual IP Address	Set local virtual IP address of the GRE tunnel.	Null
Local Virtual Netmask	Set local virtual Netmask of the GRE tunnel.	Null
Remote Virtual IP Address	Set remote virtual IP Address of the GRE tunnel.	Null
Enable Default Route	Click the toggle button to enable/disable this option. When enabled, all the traffics of the gateway will go through the GRE VPN.	OFF
Enable NAT	Click the toggle button to enable/disable this option. This option must be enabled when the router is under a NAT environment.	ON
Secrets	Set key to the GRE tunnel.	Null
Link Binding	Select link to build GRE.	Unbound

## 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	

## 3.6 Services

### 3.6.1 Syslog

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

Syslog

^ Syslog Settings

Enable

ON  OFF

Syslog Level

v

Save Position

v ?

Log to Remote

ON  OFF ?

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

Syslog

^ Syslog Settings

Enable

ON  OFF

Syslog Level

v

Save Position

v ?

Log to Remote

ON  OFF ?

Add Identifier

ON  OFF ?

Remote IP Address

Remote Port


Syslog Settings		
Item	Description	Default
Enable	Click the toggle button to enable/disable the Syslog settings option.	ON
Syslog Level	Select from "Debug", "Info", "Notice", "Warning", or "Error", which from low to high. The lower level will output more Syslog in detail.	Debug
Save Position	Select save position from "RAM", "NVM" or "Console". The data will be cleared after reboot when choosing "RAM". <b>Note:</b> <i>It's not recommended that you save Syslog to NVM (Non-Volatile Memory) for a long time.</i>	RAM
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.	OFF
Add Identifier	Click the toggle button to enable/disable this option. When enabled, you can add a serial number to the Syslog message which is used for loading Syslog to RobustLink.	OFF
Remote IP Address	Enter IP address of the Syslog server when enabling the "Log to Remote" option.	Null
Remote Port	Enter port of the Syslog server when enabling the "Log to Remote" option.	514

### 3.6.2 Event

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

#### Notification

Notification	Event	Query
<b>^ Event Notification Group Settings</b>		
Index	Description	Send SMS
		Send Email
		DO Control
		Save to NVM
+		

Click  button to add an Event parameter.

**Notification**

**^ General Settings**

Index	<input type="text" value="1"/>
Description	<input type="text"/>
Send SMS	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Phone Number	<input type="text"/> <span style="float: right;">?</span>
Send Email	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
Email Addresses	<input type="text"/> <span style="float: right;">?</span>
DO Control	<input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF
DO Index	<input type="text" value="DO1"/> <span style="float: right;">v</span>
DO Level	<input type="text" value="High"/> <span style="float: right;">v</span>
Save to NVM	<input type="checkbox"/> ON <input checked="" type="checkbox"/> OFF <span style="float: right;">?</span>

General Settings @ Notification		
Item	Description	Default
Index	Indicate ordinal of list.	--
Description	Enter a description for this group.	Null
Sent SMS	Click the toggle button to enable/disable this option. When enabled, the router will send a notification to the specified phone numbers via SMS if an event occurs. Set the related phone number in “3.6.5 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 a notification to the specified email box via email if an event occurs. Set the related email address in “3.6.5 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 the 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
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

## Event

This section allows you to set the event.

Notification
Event
Query

**^ General Settings**

Signal Quality Threshold  ?

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

## Query

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

Click Refresh to query filtered events.

Click Clear to clear the event records in the window.

Notification
Event
Query

**^ Event Details**

Save Position  v

Filtering

```

Jan 01 00:00:07, system startup
Jan 01 00:00:08, LAN port link down, eth0
Jan 01 00:00:08, LAN port link up, eth1
Jan 01 00:00:08, LAN port link down, eth2
Jan 01 00:00:08, LAN port link down, eth3
Jan 01 02:06:08, cellular data traffic stats clear, SIM1, TX=0KiB, RX=0KiB
Jan 01 02:06:08, cellular data traffic stats clear, SIM2, TX=0KiB, RX=0KiB
Jan 01 02:06:08, wan data traffic stats clear, TX=0KiB, RX=0KiB
Jan 01 02:06:09, configuration change, via web manager
                    
```

Clear
Refresh

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

### 3.6.3 NTP

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

NTP

Status

^ **Timezone Settings**

**Time Zone**

UTC+08:00

v

**Expert Setting**

?

^ **NTP Client Settings**

**Enable**

ON

OFF

**Primary NTP Server**

pool.ntp.org

0

default

^ **NTP Server Settings**

**Enable**

ON

OFF

NTP		
Item	Description	Default
<b>Time zone Settings</b>		
Time Zone	Click the drop-down list to select the time zone you are in.	UTC +08:00
Expert Setting	Specify time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
<b>NTP Client Settings</b>		
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 interval (minutes) synchronizing the NTP client time with the NTP servers. Minutes wait for the next update, and 0 means update only once.	0



Request network port	Select Request network port from “default” or “lan”.	default
NTP Server Settings		
Enable	Click the toggle button to enable/disable the NTP server option.	OFF

## Status

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

NTP
Status

^ Time

**System Time** 2022-07-25 15:30:20

**PC Time** 2022-07-25 15:30:21 Sync

**Last Update Time** Not Updated

## 3.6.4 SMS

This section allows you to set SMS parameters. The router supports SMS management, and users can control and configure their routers by sending SMS. For more details about SMS control, refer to [4.1.2 SMS Remote Control](#).

SMS
SMS Testing

^ SMS Management Settings ?

**Enable** ON OFF

**Authentication Type** Password ?

**Phone Number**  ?

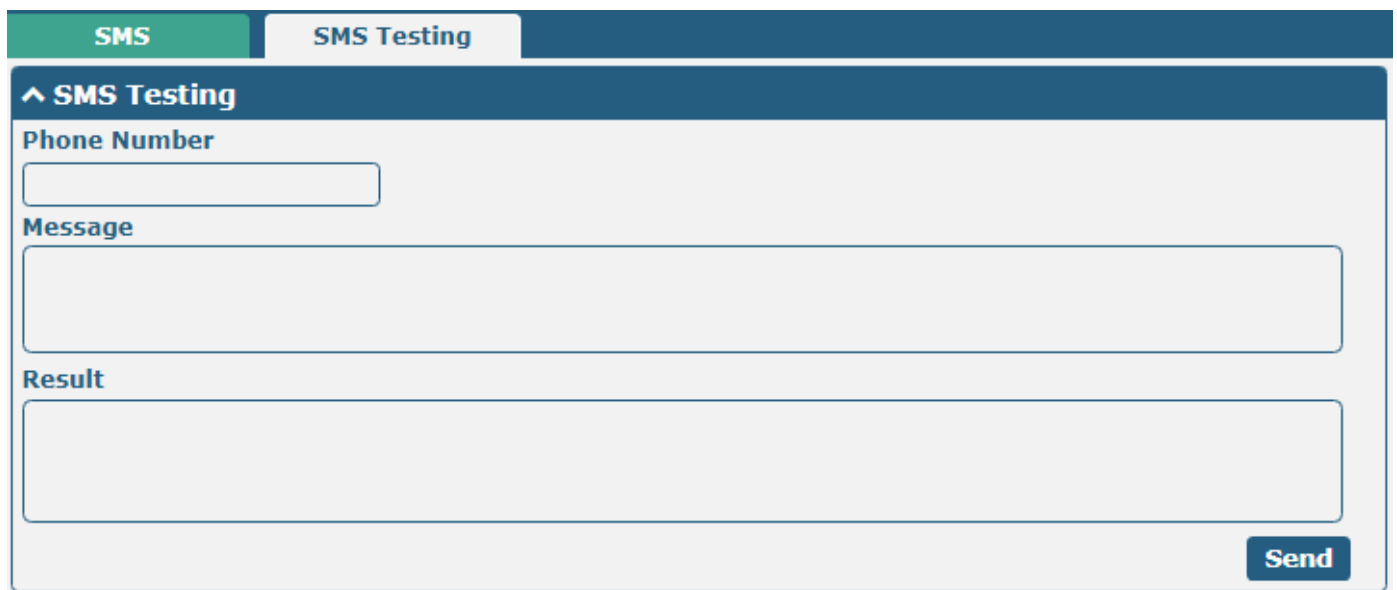
**Data Coding Scheme** GSM-7 ?


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

	user should set the Phone Number that is allowed for SMS management. The format of the SMS should be "username: password; cmd1; cmd2; ..."	
Phone Number	Set phone number used for SMS management, and use ';' to separate each number. <b>Note:</b> It can be null when choosing "Password" as the authentication type.	Null
Data Coding Scheme	Select Data Coding Scheme from "GSM-7" or "ucs2".	GSM-7

## SMS Testing

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



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

### 3.6.5 Email

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

Email
^ Email Settings

**Enable**  ON  OFF

**Enable TLS/SSL**  ON  OFF ?

**Enable STARTTLS**  ON  OFF

**Outgoing Server**

**Server Port**

**Timeout**  ?

**Auth Login**  ON  OFF ?

**Username**

**Password**

**From**

**Subject**

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

### 3.6.6 DDNS

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

#### DDNS

The service provider defaults to “DynDNS”, as shown below.

The screenshot shows the DDNS Settings interface. At the top, there are two tabs: "DDNS" and "Status", with "Status" being the active tab. Below the tabs is a header "DDNS Settings" with a caret icon. The main content area contains an "Enable" toggle set to "ON". Below this is a "Service Provider" dropdown menu, which is highlighted with a red box and currently shows "DynDNS". Underneath are input fields for "Hostname", "Username", and "Password". At the bottom, there is a "Max Tries" field set to "3" with a help icon to its right.

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

The screenshot shows the DDNS Settings interface with the "Service Provider" dropdown menu highlighted by a red box and set to "Custom". The "Enable" toggle is still "ON". The "URL" field is now visible below the "Service Provider" dropdown. The "Max Tries" field remains set to "3" with a help icon.

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

The screenshot shows the 'Status' tab of the DDNS Settings window. The 'Enable' toggle is set to 'OFF'. The 'Service Provider' dropdown menu is highlighted with a red box and shows 'NO-IP' selected. Below it are input fields for 'Hostname', 'Username', 'Password', and 'Max Tries' (set to 3).

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

The screenshot shows the 'Status' tab of the DDNS Settings window. The 'Enable' toggle is set to 'OFF'. The 'Service Provider' dropdown menu is highlighted with a red box and shows '3322' selected. Below it are input fields for 'Hostname', 'Username', 'Password', and 'Max Tries' (set to 3).

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

## Status

This section allows you to view the status of DDNS.

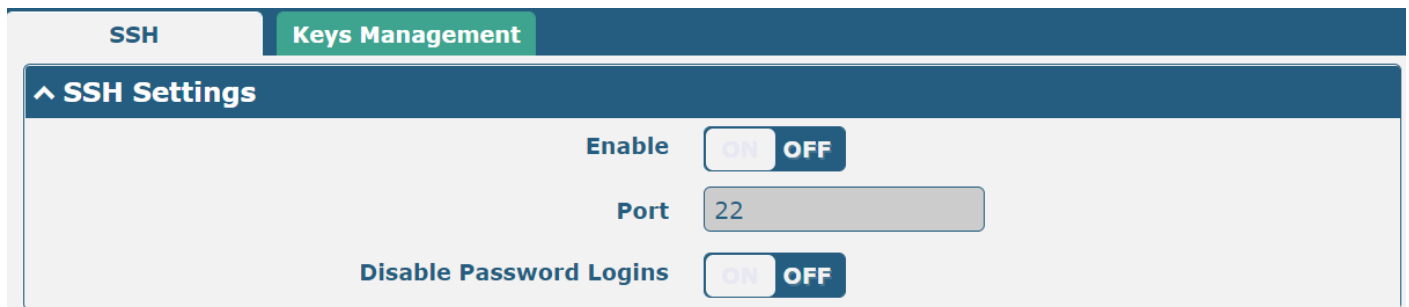


The screenshot shows a navigation bar with 'DDNS' and 'Status' tabs. Below it is a section titled '^ DDNS Status' containing two items: 'Status' with a value of 'Disabled' and 'Last Update Time'.

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

### 3.6.7 SSH

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

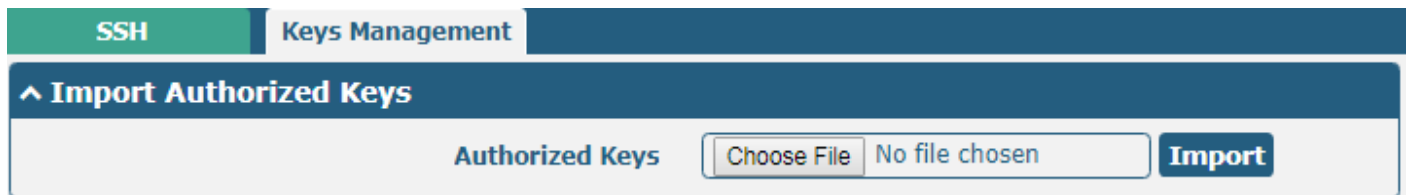


The screenshot shows a navigation bar with 'SSH' and 'Keys Management' tabs. Below it is a section titled '^ SSH Settings' containing three items: 'Enable' with a toggle set to 'OFF', 'Port' with a text input field containing '22', and 'Disable Password Logins' with a toggle set to 'OFF'.

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

## Key Management

This section allows you to import authorized Keys.



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

### 3.6.8 Telephone

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

**Note:**

- 1) Whether or not voice call and data transmission can be used simultaneously is dependent upon your ISP network.
- 2) R2000-Ent and R3010 support “Telephone” feature.



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

## Records

This section allows you to view the call records.

Telephone
Records

^ Call Records

Filtering

type	Phone Number	Start Time	Duration
out	15917451884	Jan 01 00:01:12	00:00:00
out	13560328286	Jan 01 00:00:50	00:00:00
out	15917451884	Mar 28 19:39:13	00:00:00
in	15917451884	Mar 28 19:42:03	00:00:00
out	15917451884	Mar 28 20:05:43	00:00:10
out	15917451884	Mar 28 20:30:48	00:00:18
out	15917451884	Mar 28 20:34:01	00:00:47
out	15917451884	Jan 01 00:02:01	00:00:00
out	15917451884	Jan 01 00:02:15	00:00:00
out	15917451884	Mar 29 09:49:00	00:00:13
in	15917451884	Mar 29 09:49:28	00:00:00

Clear
Refresh

General Settings		
Item	Description	Default
Filtering	Set wait number timeout for the dial plan, measured in seconds.	--
<span style="background-color: #004a7c; color: white; padding: 2px 5px; border-radius: 3px;">Clear</span>	Click the button to clear the call record.	--
<span style="background-color: #004a7c; color: white; padding: 2px 5px; border-radius: 3px;">Refresh</span>	Click the button to refresh the call record.	--



### 3.6.9 Ignition

This section is used to configure the parameters of Ignition.

**Note:** R5020 and R2110 support the ignition feature.

Ignition

^ General Settings

Delay shutdown

?

General Settings		
Item	Description	Default
Delay shutdown	Enter the time in seconds you want to delay power down. The timeout for delayed power down is 60 seconds to 3600 seconds.	60

### 3.6.10 GPS

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

GPS
Status
Map

^ General Settings

Enable GPS
 ON  OFF

Sync GPS Time
 ON  OFF

^ RS232 Report Settings

Report to RS232
 ON  OFF

Report GGA Sentence
 ON  OFF

Report VTG Sentence
 ON  OFF

Report RMC Sentence
 ON  OFF

Report GSV Sentence
 ON  OFF

Report GNGSA Sentence
 ON  OFF


Report GNGNS Sentence
 ON  OFF

Report GLGSV Sentence
 ON  OFF

^ GPS Servers

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

GPS		
Item	Description	Default
<b>General Settings</b>		
Enable	Click the toggle button to ON to enable GPS.	OFF
Synchronized GPS Time	Click the toggle button to ON to synchronize GPS time.	OFF
<b>RS232 Report Data Settings</b>		
Reporting data through RS232	Reporting GPS Information by RS232.	OFF
Reporting GGA Sentence	Reporting GGA Sentence Information.	OFF
Reporting VTG Sentence	Reporting VTG Sentence Information.	OFF
Reporting RMC Sentence	Reporting RMC Sentence Information.	OFF
Reporting GSV Sentence	Reporting GSV Sentence Information.	OFF
Reporting GMGSA Sentence	Reporting VTG Sentence Information.	OFF
Reporting GNGNS Sentence	Reporting GNGNS Sentence Information.	OFF
Reporting GLGSV Sentence	Reporting GLGSV Sentence Information.	OFF

Click  to add a new GPS Server.

**GPS**

^ **Server Settings**

**Index**

**Enable**  ON  OFF

**Protocol** TCP Client v

**Server Address**

**Server Port**

**Send GGA Sentence**  ON  OFF

**Send VTG Sentence**  ON  OFF

**Send RMC Sentence**  ON  OFF

**Send GSV Sentence**  ON  OFF

**Send GNGSA Sentence**  ON  OFF

**Send GNGNS Sentence**  ON  OFF

**Send GLGSV Sentence**  ON  OFF

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

^ **Advanced Settings**

**Add SN as GPSID**     ON  OFF    ?

**Remove LF Character**     ON  OFF

**Self-define GPSID Prefix**        ?

Item	Description	Default
Add SN as GPSID	Click the toggle button to enable/disable this option. When enabled, the SN is appended to the NMEA message as a GPSID before transmission.	OFF
Remove LF Character	Click the toggle button to enable/disable this option.	ON
Self-define GPSID Prefix	Self-define GPSIS Prefix, four upper cases.	Null

## Status

This section allows you to view the status of GPS.

^ **GPS Status**

**Status**

**UTC Time**

**Last Fixed Time**

**Satellites In Use**

**Satellites In View**

**Latitude**

**Longitude**

**Altitude**

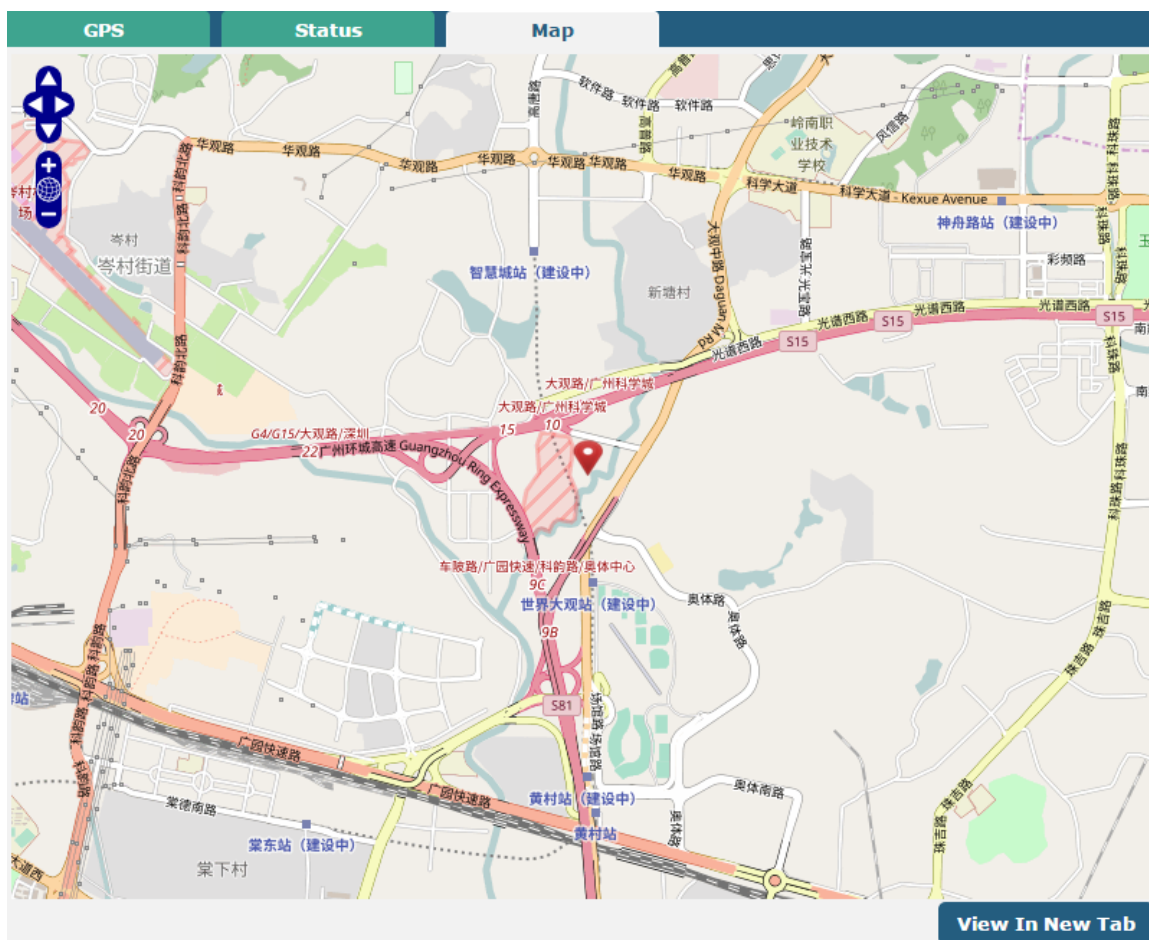
**Speed**

Item	Description
Status	Shows current GPS status of the router.
UTC Time	Shows the UTC of a satellite. <b>Note:</b> <i>The UTC is the world's unified time, not local time.</i>
Last Fixed Time	The time of the last successful positioning.
Satellites In Use	The number of satellites used.

Item	Description
Satellites In View	The number of visible satellites.
Latitude	Shows Latitude information of the router.
Longitude	Shows longitude information of the router.
Altitude	Shows height information of the router.
Speed	Shows 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 GPS antenna to the device and enable GPS on the GPS page.



### 3.6.11 Web Server

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

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

### Certificate Management

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

Import Certificate		
Item	Description	Default
Import Type	Select from “CA” and “Private Key”. <ul style="list-style-type: none"> <li>CA: a digital certificate issued by the CA center.</li> <li>Private Key: a private key file.</li> </ul>	CA
HTTPS Certificate	Click “Choose File” to locate the certificate file from your PC, and then	--

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

### 3.6.12 Advanced

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

System
Reboot

**^ System Settings**

**Device Name**

**User LED Type**

?

None

v
?

None

SIM

OpenVPN

IPSec

System Settings		
Item	Description	Default
Device Name	Set device name to distinguish different devices you have installed. Valid characters are a-z, A-Z, 0-9, @, ., -, #, \$, and *.	router
User LED Type	Specify display type of your USR LED. Select from "None", "OpenVPN" or "IPsec". <ul style="list-style-type: none"> <li>None: Meaningless indication and the LED is off.</li> <li>SIM: USR indicator showing the sim status.</li> <li>OpenVPN: USR indicator showing the OpenVPN status.</li> <li>IPsec: USR indicator showing the IPsec status.</li> </ul>	None

### Reboot

This section allows you to configure the reboot type.

System
Reboot

**^ Periodic Reboot Settings**

**Periodic Reboot**

**Daily Reboot Time**

?

?

Periodic Reboot Settings		
Item	Description	Default
Periodic Reboot	Set reboot period of the router. 0 means disable.	0
Daily Reboot Time	Set daily reboot time of 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

RT123\_SM\_v.1.0.0

1 August, 2022

135/176

### 3.6.13 Smart Roaming V2

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

**^ General Settings**

Smart Roaming Enable
 ON  OFF

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

**^ Health Check**

**Health Check Interval**  ?

**RSSI Quality Check**  ON  OFF ?

**RSSI Threshold(2G)**  ?

**RSSI Threshold(3G)**  ?

**RSSI Threshold(4G)**  ?

**RSRP Quality Check**  ON  OFF ?

**RSRP Threshold(4G)**  ?

**RSRQ Quality Check**  ON  OFF ?

**RSRQ Threshold(4G)**  ?

**Network Delay Check**  ON  OFF ?

**RTT Timeout Threshold**  ?

**Packet Loss Rate Check**  ON  OFF ?

**Packet Loss Rate Threshold**  ?

Health Check		
Item	Descriptions	Default
Health Check Interval	The health check interval for the current connection is in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Quality Check	To enable/disable "RSSI Quality Check" feature.	ON



Health Check		
Item	Descriptions	Default
Health Check Interval	The health check interval for the current connection is in minutes. If the health check fails, Smart Roaming will try to switch to another carrier network. Be careful not to set all check conditions to theoretically unattainable values.	5 Minutes
RSSI Threshold (2G)	Signal strength threshold for 2G networks.	-85 dBm
RSSI Threshold (3G)	Signal strength threshold for 3G networks.	-95 dBm
RSSI Threshold (4G)	Signal strength threshold for 4G networks.	-100 dBm
RSRP Quality Check	To enable/disable "RSRP Quality Check" feature.	OFF
RSRP Threshold (4G)	The reference signal received power threshold for 4G networks.	-100 dBm
RSRQ Quality Check	To enable/disable "RSRQ Quality Check" feature.	OFF
RSRQ Threshold (4G)	The reference signal receiving quality threshold for 4G networks.	-20 dBm
Network Delay Check	To enable/disable "Network Delay Check" feature.	OFF
RTT Timeout Threshold	The reference signal received power threshold for 4G networks.	3000 ms
Packet Loss Rate Check	Enable/disable "Packet Loss Rate Check" feature.	ON
Packet Loss Rate Threshold	Packet loss rate threshold value.	70

^ **PING Settings** ?

**Primary Server**

**Secondary Server**

**PING Timeout**  ?

**Ping Tries**  ?

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

PING Settings		
Item	Descriptions	Default
	health check is (3 * number of ping attempts).	

^ **Advanced Settings**

**Use Degraded Network** ON OFF ?

**Periodic Restart**  ?

**Daily Restart Time**  ?

**Preferred Operator List**  ?

Advanced Settings		
Item	Descriptions	Default
Use Degraded Network	To enable/disable "Use Degraded Network" feature. A degraded network is defined as a network that can be connected, but the network quality does not meet the health check thresholds.	OFF
Periodic Restart	Set period of rebooting the "Smart Roaming" function in hours. 0 means no periodic reboot is enabled. Restarting "Smart Roaming" will re-find the available carrier network and reset the current status because it takes a long time to search the available provider network, the reboot may take 3 to 5 minutes.	0
Daily Restart Time	Set time point to restart "Smart Roaming" every day in the format of HH: MM (24-hour system). When this item is empty, it means to disable the timer reboot.	Null
Preferred Operator List	Set list of preferred operators by PLMN. If multiple operators are required, use semicolons to separate, e.g., 46000;46001	Null

^ **Status**
?

**State** Connected

**Operator Selection Mode** Automatic

**Time Since Last Network Scan Started** 0 days, 00:10:04

Status	
Item	Descriptions
Status	Display current status of "Smart Roaming". It includes Scanning, Connecting, Connected, and Inactive status, which indicates that the network is searching for an available network, connecting network, network is connected and the function is not started respectively.

Status	
Item	Descriptions
Operator Selection Mode	Display which carrier network is currently selected. These include Automatic and Manual, which refer to automatic selection according to standard specifications and software selection based on network quality, respectively, and the software will cycle through the two methods.
Time Since Last Network Scan	Displays time elapsed since the last search for available networks. A "Smart Roaming" reboot will refresh this time.

^ PLMN List <span style="float: right;">?</span>								
Index	PLMN	Status	RAT	RSSI(dbm)	RSRP(dbm)	Latency(ms)	Packet Loss(%)	HealthCheck

^ Preferred Operator List	
Index	PLMN

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

## Select

This section allows you to select the network.

Settings
Status
Select
Log
Speed Test

^ Operator Select ?

User Specified Network Selection

Forget RPLMN
Rescan
Submit

Operator Select		
Item	Descriptions	Default
User Specified Network Selection	Select Specified Network.	--
<span style="background-color: #007060; color: white; padding: 2px 5px;">Forget RPLMN</span>	Forces deletion of all location information from the SIM.	--
<span style="background-color: #007060; color: white; padding: 2px 5px;">Rescan</span>	Rescan operator list and this causes Smart Roaming to start again.	--
<span style="background-color: #007060; color: white; padding: 2px 5px;">Submit</span>	Submit operator selected by the drop-down box.	--

## Log

This section allows you to view the connection log.

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

Connection Log		
<b>Clear</b>	Click the button to clear the connection log.	--

## Speed Test

This section allows you to test the network speed.

Settings
Status
Select
Log
Speed Test

^ Speedtest

Time	Action	Method	Network	Download	Upload
Jul 22 14:46:05	Speedtest	GUI		N/A	N/A

Speedtest
Clear

Speed Test		
<span style="background-color: #004a7c; color: white; padding: 2px 5px; border-radius: 3px;">Speedtest</span>	Click the button to start the network speed test.	--
<span style="background-color: #004a7c; color: white; padding: 2px 5px; border-radius: 3px;">Clear</span>	Click the button to clear the speed test log.	--

## 3.7 System

### 3.7.1 Debug

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

Syslog

^ Syslog Details

Log Level

Debug

Filtering?

```

2022-07-25 16:02:49 router syslog.info syslogd started: BusyBox v1.34.1
2022-07-25 16:02:49 router user.notice init[1]: r1520 version 5.0.0_rc1 (18d58ee9), built at
14:47:25 Jul 15 2022
2022-07-25 16:02:49 router user.notice eventd[924]: eventd started! uptime=36
2022-07-25 16:02:50 router user.notice link_manager[933]: link manager started
2022-07-25 16:02:50 router user.debug link_manager[933]: rcv action connect from link_manager
2022-07-25 16:02:50 router user.debug link_manager[933]: target link WWAN1, state Disconnected
2022-07-25 16:02:50 router user.notice link_manager[933]: WWAN1 start connect
2022-07-25 16:02:50 router user.info link_manager[933]: WWAN1 is not ready, waiting for
initialization
2022-07-25 16:02:51 router daemon.err ntpdate[1034]: name server cannot be used: Temporary failure
in name resolution (-3)
2022-07-25 16:02:52 router daemon.err ntpdate[1034]: no servers can be used, exiting
2022-07-25 16:02:52 router user.notice ntpc_mgmt[1028]: ntp client synchronization failed. Reboot
in 1 minute.
2022-07-25 16:02:52 router user.notice modemd[1035]: modem service started
2022-07-25 16:02:52 router user.notice smart_roaming[1036]: smart_roaming started
                
```

Manual Refresh

v

Clear

Refresh

^ Syslog Files

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

^ System Diagnostic Data

System Diagnostic Data

Generate

System Diagnostic Data

Download

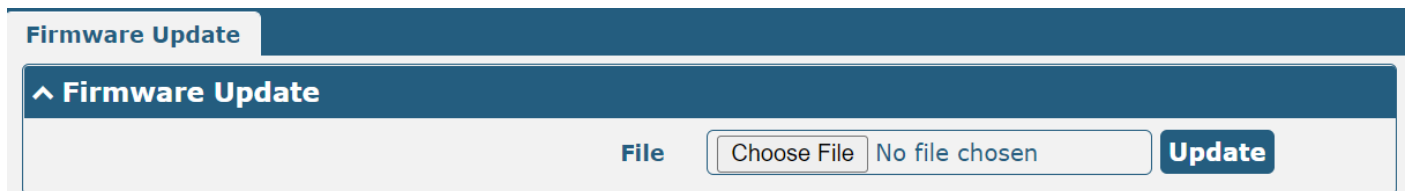
Syslog		
Item	Description	Default
Syslog Details		
Log Level	Select from “Debug”, “Info”, “Notice”, “Warn”, and “Error” from low to high. The lower level will output more Syslog in detail.	Debug
Filtering	Enter filtering message based on the keywords. Use “&” to separate more than one filter message, 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 following box. If selecting “manual refresh”, you should click the refresh button to refresh the Syslog.	Manual Refresh
<b>Clear</b>	Click the button to clear the Syslog.	--
<b>Refresh</b>	Click the button to refresh the Syslog.	--
Syslog Files		
Syslog Files List	It can show at most 5 Syslog files in the list, the files’ name ranges from message0 to message 4. And the newest Syslog file will be placed on the top of the list.	--
System Diagnosing Data		
<b>Generate</b>	Click to generate the Syslog diagnosing file. When there is a problem with the device, system diagnostic data can be generated and sent to a <b>Robust technical support representative</b> for assistance.	--

### 3.7.2 Update

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

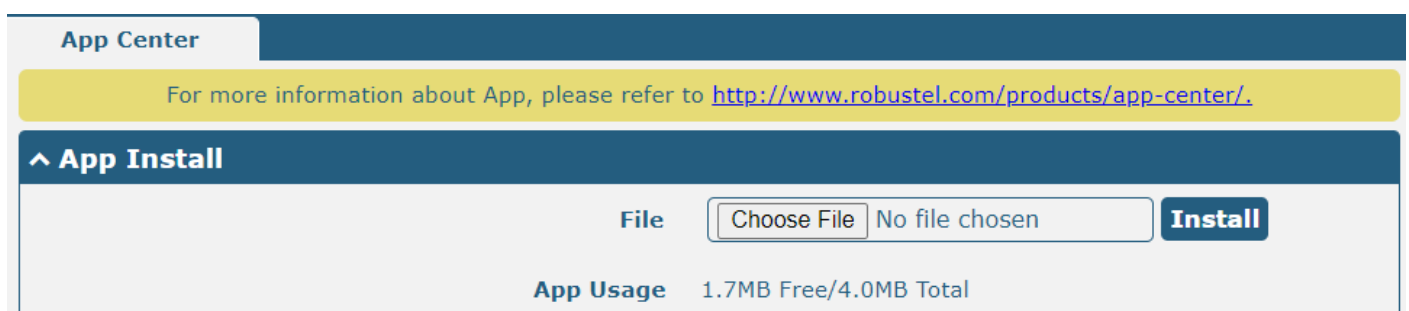
**Note:** To access the latest firmware file, please contact your technical support engineer.




### 3.7.3 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 to the router again.





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

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

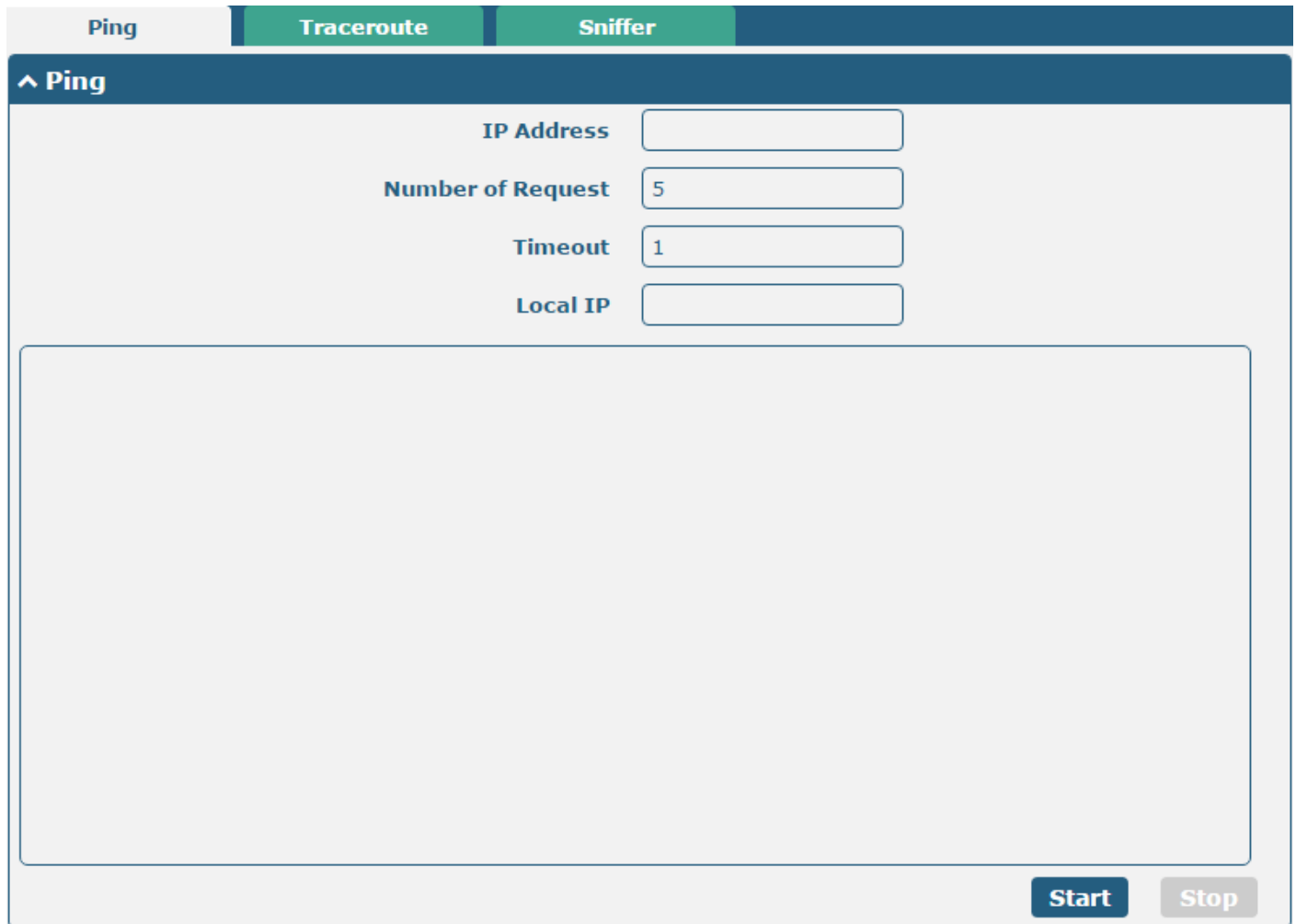
App Center		
Item	Description	Default
App Install		
File	Click on "Choose File" to locate the App file from your PC, and then click  to import this file into your router. <i>Note: File format should be xxx.rpk, e.g., r1520-vrrp-5.0.0.rpk.</i>	--
Installed Apps		
Index	Indicate ordinal of list.	--
Name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



### 3.7.4 Tools

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

#### Ping

This section allows you to use the Ping tools.



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

## Traceroute

This section allows you to use the Traceroute tools.

Ping
Traceroute
Sniffer

^ Traceroute

Trace Address

Trace Hops

Trace Timeout

Traceroute		
Item	Description	Default
Trace Address	Enter trace’s destination IP address or destination domain.	Null
Trace Hops	Specify max trace hops. The router will stop tracing if the trace hops have met the max value no matter whether destination has been reached or not.	30
Trace Timeout	Specify the timeout of Traceroute request.	1
<input style="background-color: #004a7c; color: white; padding: 2px 5px;" type="button" value="Start"/>	Click this button to start Traceroute request, and the log will be displayed in the following box.	--
<input style="background-color: #ccc; padding: 2px 5px;" type="button" value="Stop"/>	Click this button to stop Traceroute request.	--

## Sniffer

This section allows you to use the Sniffer tools.

Sniffer		
Item	Description	Default
Interface	Choose interface according to your Ethernet configuration.	All
Host	Filter packet that contains the specified IP address.	Null
Packets Request	Set packet number that the router can sniffer at a time.	1000
Protocol	Select from "All", "IP", "TCP", "UDP" and "ARP".	All
Status	Show current status of sniffer.	--
	Click the button to start sniffer.	--
	Click the button to stop the sniffer. Once you click this button, a new log file will be displayed in the following List.	--
Capture Files	Every time of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List click  to download the log and click  to delete the log file. It can cache a maximum of 5 files.	--

### 3.7.5 Profile

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

Profile
Rollback

**^ Import Configuration File**

Reset Other Settings to Default  ON  OFF ?

Ignore Invalid Settings  ON  OFF ?

XML Configuration File

**^ Export Configuration File**

Ignore Disabled Features  ON  OFF ?

Add Detailed Information  ON  OFF ?

Encrypt Secret Data  ON  OFF ?

XML Configuration File

**^ Default Configuration**

Save Running Configuration as Default  ?

Restore to Default Configuration

Profile		
Item	Description	Default
<b>Import Configuration File</b>		
Reset Other Settings to Default	Click the toggle button as “ON” to return other parameters to default settings.	OFF
Ignore Invalid Settings	Click the toggle button as “OFF” to ignore invalid settings.	OFF
XML Configuration File	Click on <span style="border: 1px solid #ccc; padding: 1px 5px;">Choose File</span> to locate the XML configuration file from your PC, and then click <span style="background-color: #004a7c; color: white; padding: 2px 5px;">Import</span> to import this file into your router.	--
<b>Export Configuration File</b>		
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 <span style="background-color: #004a7c; color: white; padding: 2px 5px;">Generate</span> button to generate the XML configuration file, and click <span style="background-color: #004a7c; color: white; padding: 2px 5px;">Export</span> to export the XML configuration file.	--

Default Configuration		
Save Running Configuration as Default	Click <b>Save</b> button to save the current running parameters as the default configuration.	--
Restore to Default Configuration	Click the button to restore the factory defaults.	--

## Rollback

This section allows you to roll back the configuration.

Profile
Rollback

^ **Configuration Rollback**

Save as a Rollbackable Archive Save ?

^ **Configuration Archive Files**

Index	File Name	File Size	Modification Time

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

### 3.7.6 User Management

This section allows you to change your username and password, and create or manage user accounts. One router has only one super user.

Super User

^ **Super User Settings** ?

**New Username**  ?

**Old Password**  ?

**New Password**  ?

**Confirm Password**

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

## 4. Configuration Examples

### 4.1 Cellular

#### 4.1.1 Cellular Dial-Up

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

Link Manager
Status





^ General Settings


Primary Link  ?

Backup Link

Emergency Reboot  ON  OFF ?

^ Link Settings

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

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

Link Manager

^ General Settings

Index

Type

Description



### ^ WWAN Settings

**Automatic APN Selection**  ON  OFF

**Dialup Number**

**Authentication Type**  v

**PPP Preferred**  ON  OFF ?

**Switch SIM By Data Allowance**  ON  OFF ?

**Data Allowance**  ?

**Billing Day**  ?

### ^ Ping Detection Settings ?

**Enable**  ON  OFF

**Primary Server**

**Secondary Server**

**Interval**  ?

**Retry Interval**  ?

**Timeout**  ?

**Timeout unit**  v

**Max Ping Tries**  ?

### ^ Advanced Settings

**NAT Enable**  ON  OFF

**Auto MTU For WWAN**  ON  OFF

**Upload Bandwidth**  ?

**Download Bandwidth**

**Overrided Primary DNS**

**Overrided Secondary DNS**

**Debug Enable**  ON  OFF

**Verbose Debug Enable**  ON  OFF

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

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

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

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

**Cellular**

^ **General Settings**

**Index**

**SIM Card**  v

**Phone Number**

**PIN Code**  ?

**MCC+MNC Code**  ?

**Extra AT Cmd**  ?

**Telnet Port**  ?

**Waiting For Update APN**  ?

^ **Cellular Network Settings**

**Network Type**  v ?

**Band Select Type**  v ?

^ **Advanced Settings**

**Debug Enable**

**Verbose Debug Enable**

**Timeout For Network Registration**  ?

**Preferred Using CID3**   ?

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

## 4.1.2 SMS Remote Control

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

### SMS commands have the following structures:

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

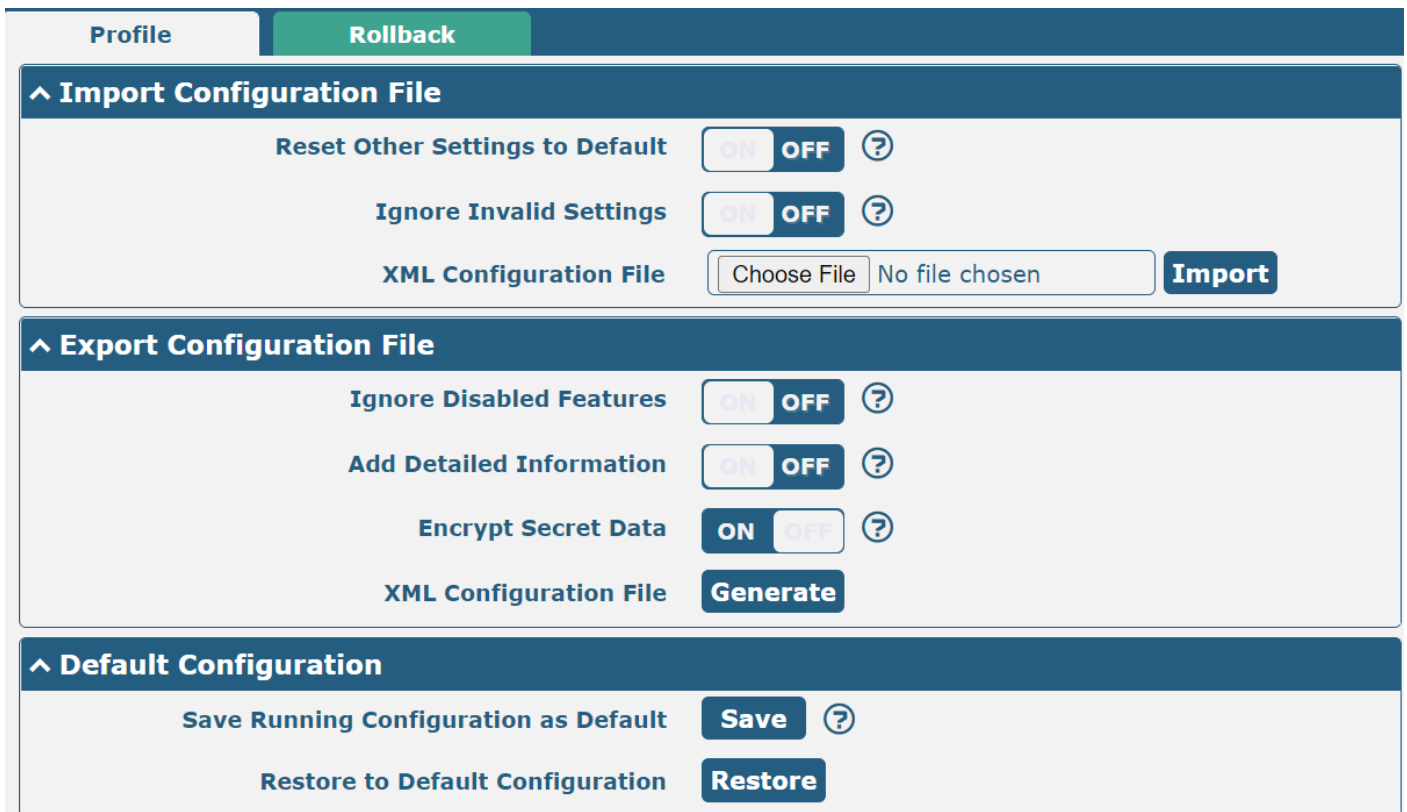
**Note: All command symbols must be entered in the half-angle mode of the English input method.**

### SMS command Explanation:

1. Username and Password: Use the same username and password as the WEB manager for authentication.
2. **cmd1, cmd2, cmd3 to cmdn**, the command format is the same as the CLI command, more details about CLI cmd please refer to [5.1 What Is CLI](#).

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

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



The screenshot shows a web interface with a top navigation bar containing 'Profile' and 'Rollback' tabs. Below this are three main sections:

- Import Configuration File:** Contains three settings: 'Reset Other Settings to Default' (OFF), 'Ignore Invalid Settings' (OFF), and 'XML Configuration File' (Choose File, No file chosen). An 'Import' button is at the bottom right.
- Export Configuration File:** Contains three settings: 'Ignore Disabled Features' (OFF), 'Add Detailed Information' (OFF), and 'Encrypt Secret Data' (ON). An 'XML Configuration File' section has a 'Generate' button.
- Default Configuration:** Contains two settings: 'Save Running Configuration as Default' (Save) and 'Restore to Default Configuration' (Restore).

**XML command:**

```
<lan>

<network max_entry_num="5">

<id>1</id>

<interface>lan0</interface>

<ip>172.16.24.24</ip>

<netmask>255.255.0.0</netmask>

<mtu>1500</mtu>
```

**SMS cmd:**

```
set lan network 1 interface lan0
```

```
set lan network 1 ip 172.16.24.24
```

```
set lan network 1 netmask 255.255.0.0
```

```
set lan network 1 mtu 1500
```

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

**admin:admin;status system**

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

**SMS received:**

```
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 21 17:09:04 2021"
ram_usage = "77M Free/128M Total"
```

**admin:admin;reboot**

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

**SMS received:**

```
OK
```

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

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

**SMS received:**

OK  
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, the username is “admin”, the password is “admin”, and the command is to configure the LAN parameter.

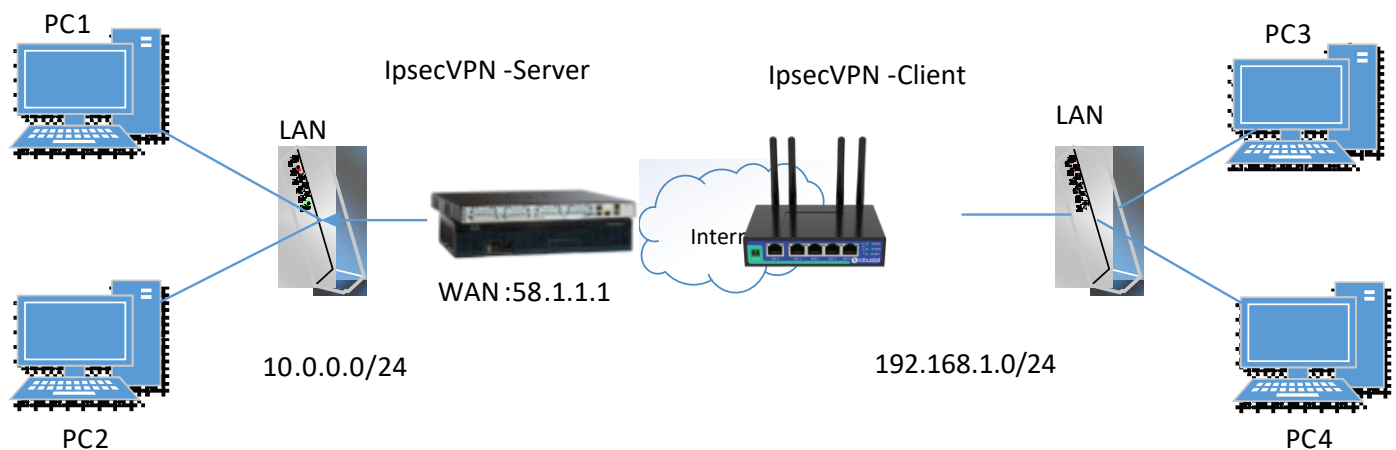
**SMS received:**

OK  
OK  
OK  
OK

## 4.2 VPN Configuration Examples

### 4.2.1 IPsec VPN

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



#### IPsec VPN\_Client:

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

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

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

## Tunnel

### ^ General Settings

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

### ^ IKE Settings

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

### ^ SA Settings

Encryption Algorithm	<input type="text" value="3DES"/>	v
Authentication Algorithm	<input type="text" value="SHA1"/>	v
PFS Group	<input type="text" value="DHgroup2"/>	v
SA Lifetime	<input type="text" value="28800"/>	?
DPD Interval	<input type="text" value="30"/>	?
DPD Failures	<input type="text" value="150"/>	?

### ^ Advanced Settings

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

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

## 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

```



The comparison between server and client is as below.

```

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
lifetime Set lifetime for ISAKMP security association
no Negate a command or set its defaults
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
ipsecc 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 (64 bits)
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)#exit
Router(config-if)#crypto map cry-map
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

```

**General Settings**

Index: 1

Enable:

Description:

Gateway: 58.1.1.1

Mode: Tunnel

Protocol: ESP

Local Subnet: 192.168.1.0/24

Remote Subnet: 0.0.0.0/24

Link Binding: Unspecified

**IKE Settings**

IKE Type: IKEv1

Negotiation Mode: Main

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

IKE DH Group: DHgroup2

Authentication Type: PSK

PSK Secret: \*\*\*\*\*

Local ID Type: Default

Remote ID Type: Default

IKE Lifetime: 86400

**SA Settings**

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

PFS Group: DHgroup2

SA Lifetime: 28800

DPD Interval: 30

DPD Failures: 150

**Advanced Settings**

Enable Compression:  OFF

Enable Forceencaps:  OFF

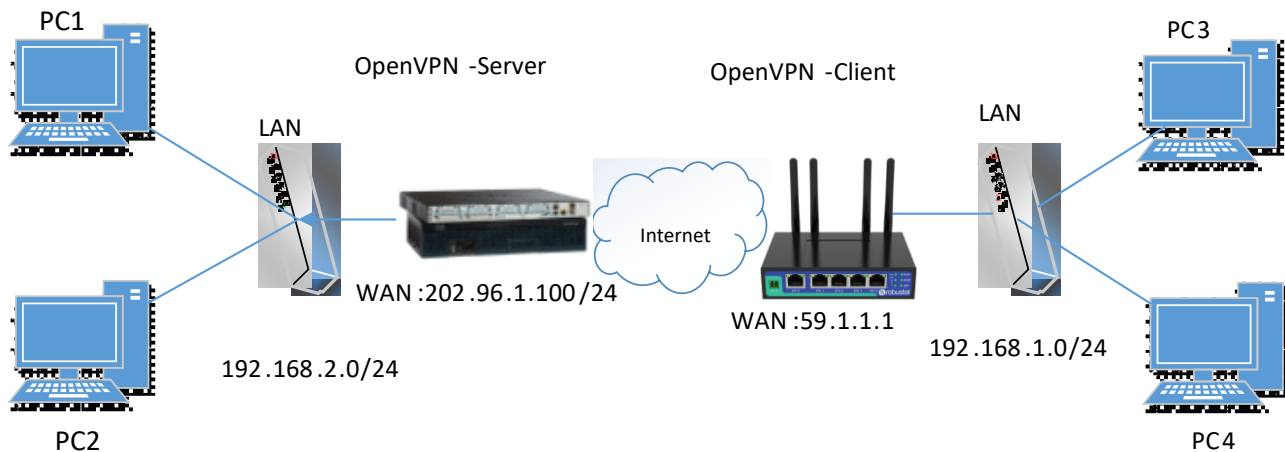
Expert Options:

Router IKE Settings should be consistent with service fees.

Router SA Settings should be consistent with service fees.

### 4.2.2 OpenVPN

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



## OpenVPN\_Server:

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

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

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

## OpenVPN\_Client:

Click “VPN > OpenVPN > OpenVPN” as below.



OpenVPN					
Status		x509			
^ Tunnel Settings					
Index	Enable	Description	Pr	Pe	Interface Type
+					

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

### OpenVPN

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

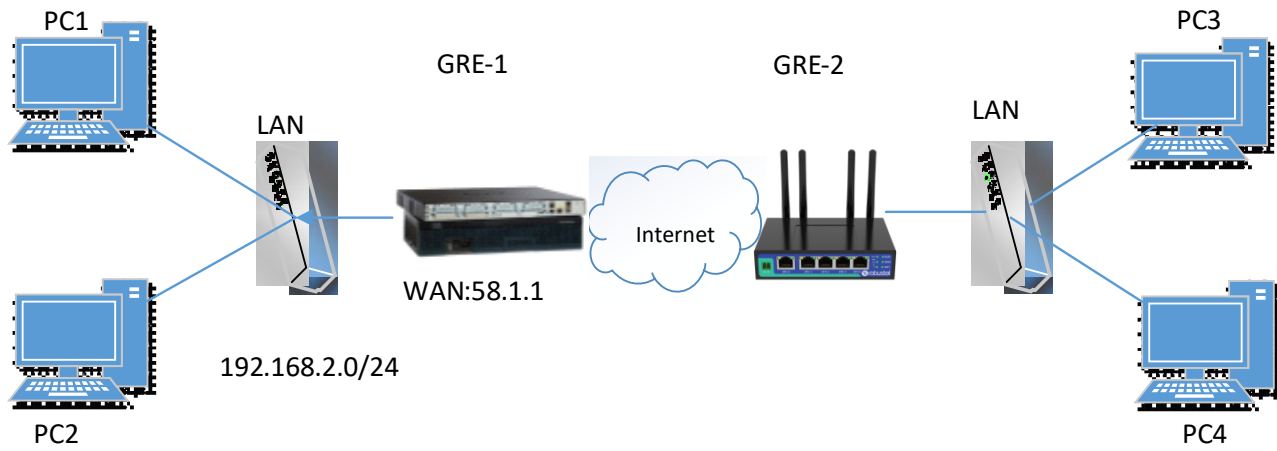
#### ^ Advanced Settings

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

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

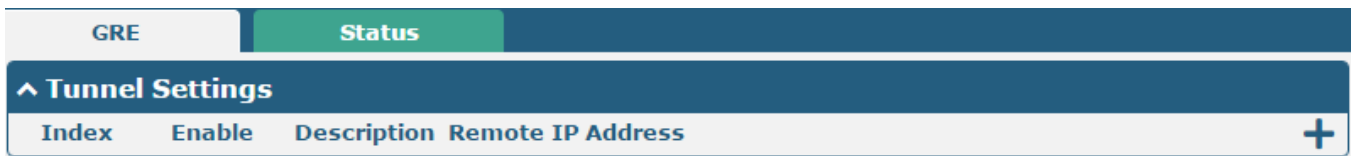
### 4.2.3 GRE VPN

GRE VPN topology



#### GRE-1:

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



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

GRE

^ Tunnel Settings

Index	Enable	Description	Remote IP Address
+			

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

GRE

^ Tunnel Settings

Index: 1

Enable: ON OFF

Description: [ ]

Bridge With LAN: ON OFF

Remote IP Address: 59.1.1.1

Local Virtual IP Address: 20.8.0.2

Local Virtual Netmask: 255.255.255.0

Remote Virtual IP Address: 10.8.0.2

Enable Default Route: ON OFF

Enable NAT: ON OFF

Secrets: [ ]

Link Binding: Unspecified [v] [?]

Submit Close

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

## GRE-2:

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

**GRE**

**^ Tunnel Settings**

Index: 1

Enable:  ON  OFF

Description: GRE-2

Bridge With LAN:  ON  OFF

Remote IP Address: 59.1.1.1

Local Virtual IP Address: 20.8.0.2

Local Virtual Netmask: 255.255.255.0

Remote Virtual IP Address: 10.8.0.2

Enable Default Route:  ON  OFF

Enable NAT:  ON  OFF

Secrets: .....

Link Binding: Unspecified

**Submit** **Close**

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

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

**GRE-1** **GRE-2**

**^ Tunnel Settings** **^ Tunnel Settings**

Index: 1

Enable:  ON  OFF

Description: GRE-1

Remote IP Address: 58.1.1.1

Local Virtual IP Address: 10.8.0.1

Local Virtual Netmask/Prefix Length: 255.255.255.0

Remote Virtual IP Address: 10.8.0.2

Enable Default Route:  ON  OFF

Enable NAT:  ON  OFF

Secrets: .....

Link Binding: Unspecified

GRE-1 real public network IP address

GRE-1 real tunnl IP address

GRE-2 real tunnl IP address

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

GRE-2 real public network IP address

GRE-2 real tunnl IP address

GRE-1 real tunnl IP address

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

## 5. Introductions for CLI

### 5.1 What Is CLI

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

#### Route login:

Router login: admin

Password: admin

#

#### CLI commands:

# ?

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

## 5.2 How to Configure the CLI

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

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

## 5.3 Commands Reference

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

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

## 5.4 Quick Start with Configuration Examples

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

### Example 1: Show the current version

```
# status system
hardware_version = 1.0
firmware_version = beta210618
firmware_version_full = "beta210618 (Rev 4250)"
kernel_version = 4.9.152
device_model = R2011
serial_number = ""
uptime = "0 days, 01:25:16"
system_time = "Tue Apr 15 17:09:04 2021"
ram_usage = "77M Free/128M Total"
```

### Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
  firmware  New firmware
  config    New configuration file
# tftpupdate firmware (space+?)
  filename  New file
# tftpupdate firmware filename R2011-firmware-sysupgrade-unknown.ruf host 192.168.100.99 //enter a new
firmware name
Downloading
Download success.
Upgrading
Upgrade success.          //Update succeed
# reboot                  //Take effect after rebooting
Rebooting...
OK
```

### Example 3: Set link-manager

```
# set
# set (space+?)
  cellular      Cellular
  ddns          DDNS
  dido          DIDO
  email         Email
  ethernet      Ethernet
  event         Event Management
```



firewall	Firewall
gre	GRE
ip_passthrough	IP Passthrough
ipsec	IPSec
lan	Local Area Network
link_manager	Link Manager
ntp	NTP
openvpn	OpenVPN
reboot	Automatic Reboot
route	Route
serial_port	Serial
sms	SMS
ssh	SSH
syslog	Syslog
system	System
user_management	User Management
web_server	Web Server

```
# set link_manager (space+?)
```

primary_link	Primary Link
backup_link	Backup Link
backup_mode	BackSup Mode
revert_interval	Revert Interval
emergency_reboot	Emergency Reboot
link	Link Settings

```
# set link_manager primary_link (space+?)
```

```
Enum Primary Link (wwan1/wan)
```

```
# set link_manager primary_link wwan1
```

```
//select "wwan1" as primary_link
```

```
OK
```

```
//setting succeed
```

```
#set link_manager link 1 (space+?)
```

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

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

#### Example 4: Set Ethernet

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

#### Example 5: Set LAN IP address

```
# show lan all
network {
  id = 1
  interface = lan0
  ip = 192.168.0.1
  netmask = 255.255.255.0
  mtu = 1500
  dhcp {
    enable = true
    mode = server
    relay_server = ""
    pool_start = 192.168.0.2
    pool_end = 192.168.0.100
    netmask = 255.255.255.0
    router = ""
```

```

    primary_dns = ""
    secondary_dns = ""
    wins_server = ""
    lease_time = 120
    static_lease = ""
    expert_options = ""
    debug_enable = false
}
vlan_id = 0
}
#
# set lan (space+?)
network      Network Settings
multi_ip     Multiple IP Address Settings
# set lan network 1(space+?)
interface    Interface
ip           IP Address
netmask      Netmask
mtu          MTU
dhcp         DHCP Settings
Vlan_id      VLAN ID
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.24.24           //set the IP address for lan
OK                                           //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
...
# config save_and_apply
OK                                           // save and apply the current configuration, make your configuration effect

```

## Example 6: CLI for setting Cellular

```

# show cellular all
sim {
    id = 1
    card = sim1
    phone_number = ""
    pin_code = ""
    extra_at_cmd = ""
    telnet_port = 0
    network_type = auto
    band_select_type = all
    band_settings {
        gsm_850 = false
        gsm_900 = false
    }
}

```

```
gsm_1800 = false
gsm_1900 = false
wcdma_800 = false
wcdma_850 = false
wcdma_900 = false
wcdma_1900 = false
wcdma_2100 = false
wcdma_1700 = false
wcdma_band19 = false
lte_band1 = false
lte_band2 = false
lte_band3 = false
lte_band4 = false
lte_band5 = false
lte_band7 = false
lte_band8 = false
lte_band13 = false
lte_band17 = false
lte_band18 = false
lte_band19 = false
lte_band20 = false
lte_band21 = false
lte_band25 = false
lte_band28 = false
lte_band31 = false
lte_band38 = false
lte_band39 = false
lte_band40 = false
lte_band41 = false
}
telit_band_settings {
    gsm_band = 900_and_1800
    wcdma_band = 1900
}
debug_enable = true
verbose_debug_enable = false
}
# set(space+space)
cellular      ddns          dido          email         ethernet
event        firewall      gre          ip_passthrough ipsec
l2tp         lan          link_manager ntp          openvpn
pptp         reboot      route       serial_port  sms
ssh          syslog      system      user_management web_server
# set cellular(space+?)
sim SIM Settings
# set cellular sim(space+?)
```

Integer Index (1..1)

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

card	SIM Card
phone_number	Phone Number
pin_code	PIN Code
extra_at_cmd	Extra AT Cmd
telnet_port	Telnet Port
network_type	Network Type
band_select_type	Band Select Type
band_settings	Band Settings
telit_band_settings	Band Settings
debug_enable	Debug Enable
verbose_debug_enable	Verbose Debug Enable

```
# set cellular sim 1 phone_number 18620435279
```

```
OK
```

```
...
```

```
# config save_and_apply
```

```
OK // save and apply the current configuration, make your configuration effect
```

# Glossary

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

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

**Guangzhou Robustel Co., Ltd.**

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

Email: [info@robustel.com](mailto:info@robustel.com)

Web: [www.robustel.com](http://www.robustel.com)