ZLWL IR5000 Series 4G Industrial Router Product Instruction Manual

CONTENTS

Without the written permission of the Company, no unit or individual shall excerpt or copy part or all of the contents of this document, and shall not be disseminated in any form.

Trademark Statement

And other trademarks are trademarks of Shenzhen ChiLink IoT Technology Co., Ltd.
ZLWL is our Chinese name: Zhi Lian Wu Lian
ChiLink is from China, Link the world.

All other trademarks or registered trademarks referred to in this document are the property of their respective owners.

Pay attention to

The products, services or features you purchase shall be subject to the commercial contracts and terms of Shenzhen ChiLink IoT Technology Co., Ltd., and all or part of the products, services or features described in this document may not be within the scope of your purchase or use. Except as otherwise agreed herein, Shenzhen ChiLink IoT Technology Co., Ltd. makes no representation or warranty, express or implied, regarding the contents of this document.

The content of this document may be updated from time to time due to product version upgrade or other reasons. Unless otherwise agreed, this document is intended as a guide to use only, and all statements, information and recommendations contained in this document do not constitute any warranty, express or implied.

Shenzhen ChiLink IoT Technology Co., Ltd.

Email:sales@chilinkiot.com
Http://www.szchilink.com
Http://www.chilinkiot.com
ChiLink is from China, Link the world.
Shenzhen Chilink IOT Technology CO., LTD.
Add:#518,#512,Block A,Famous Industrial Product Display
&Purchasing Center,Baoyuan Road,Baoan District,Shenzhen,China

Document Revision Records

Date	Version	Discription	Author
2015-5-15	V1.0	Initial Release	MC
2017-6-6	V1.1	Supplement/Amendment	MC/DHL
2019-10-8	V1.2	Update	MC/DHL
2021-9-18	V2.0	Update	MC/DHL

1.Product Description

Our router series adopts industrial design, adopts high-performance 32-bit embedded MIPS architecture dedicated network processor, embedded with industrial-grade, high-performance, multi-band mobile 3G/4G communication processing module. Support WCDMA, HSPA+, TD/FDD-LTE, EVDO (CDMA 2000), TD-SWCDMA, GSM and other high-speed mobile broadband network, to provide customers with convenient and fast Internet access or private network transmission, optional embedded Wi-Fi module or multi-LAN port. Provide customers with wired fixed network or wireless WLAN sharing high-speed broadband connection; At the same time, we provide customized advanced VPN (OpenVPN, IPSec) functions to build safe tunnels, which are widely used in finance, electric power, environmental protection, oil, transportation, security and other industries.

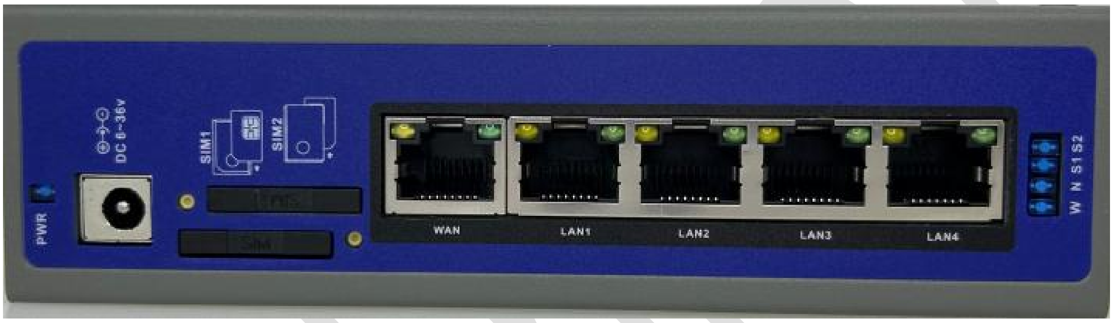
The Router series provides users with a Web-based configuration interface, making it very easy to configure and manage the Router. At the same time, the M2M terminal product management platform provides users with remote management of all Router terminals. Through the M2M platform, users can monitor the status of all terminals successfully connected to the platform, and provide remote control, parameter configuration and remote upgrade services.

This instruction manual introduces to the user how to install and configure the industrial grade Router, and guides the user to get started and use our products quickly after correctly installing the hardware and configuring the basic parameters.

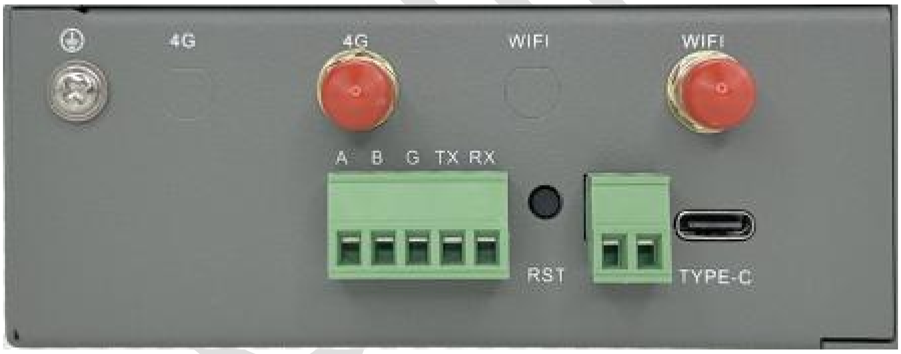
2.Device login and system status check

This chapter mainly introduces and instructs the customer how to judge the current network connection of the device through the state of each indicator light outside the device, and at the same time instructs the user how to connect to the routing device through the computer or other wireless terminals to set and view some parameters. The detailed description is as follows:

2.1Hardware interface



Front panel schematic diagram



Side panel schematic diagram

1) 2.4G WiFi: 2.4GHz frequency band WiFi SMA interface;

2) 4G Interface: SMA interface for 4G network antenna, which automatically downwardly compatible with 3G/2G network signals;

3) SIM1/SIM2: Dual SIM card slots, requiring installation of standard large SIM cards;

<SIM Card Installation Diagram>: When installing, place the SIM card with its chip circuit facing upward, aligning with the small triangle direction at the bottom of the card holder, then push the entire card slot upward to complete installation. (Note: Hot swapping of SIM cards is not supported. It is recommended to power off the device first before removing or inserting a SIM card to avoid damaging the SIM card);

4) SIM Card Ejection Button: Press here with a SIM card ejector pin or other sharp object to eject the SIM card holder;

5) LAN1-LAN4 Ports: Network ports for connecting LAN computers or other terminal devices;

6) WAN Port: Defaults to WAN port status; can be changed to LAN port use after modification;

7) RST: Reset button. When the device is powered on, press and hold this button for about 10 seconds, then release it. All lights will flash on and off once to indicate the completion of reset;

8) Serial Port 232/485: Select either one. The description of each terminal interface is as follows:

3.3V: Serial port power supply, generally no need to connect;

GND: Signal ground;

TX/B: 232/485 transmit signal;

RX/A: 232/485 receive signal;

9) POWER: Device power DC connector, supporting a wide DC voltage range of 7.5V~32V. The default power adapter is DC12V/1A;

2.2 Installation of SIM Card and Antenna

SIM Card Installation:

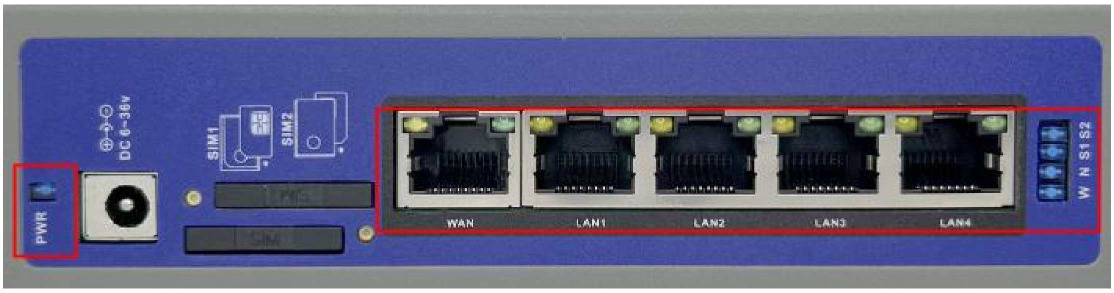
The device only supports the installation of standard Mini SIM cards. If a Nano/Micro SIM card is used, please install a card adapter first before use. When installing the SIM card as follows, press the ejection hole indicated by the blue arrow in the figure with another object, and the card holder will pop out automatically. When placing the card, ensure the SIM chip circuit faces upward, align the notch of the card with that of the card holder, and finally gently push the card holder back into place.

Installation of WiFi/4G Network Antennas:

As described above, the antennas are divided into WiFi antennas (2.4GHz) and 4G network antennas (compatible with 3G/2G). When using the device for the first time, please first remove the small red caps from the interfaces. Then, install the antennas by screwing them clockwise one by one as shown in the diagram (the antennas support bending at different angles).

By default, rod-shaped antennas are provided, which are compatible with both WiFi and mobile networks. When in use, please ensure that all antennas are properly connected.

2.3Explanation of Network Indicator Lights



Note: The IR5000 4G router supports single-mode dual-SIM mode.

In single-mode dual-SIM mode, both SIM1 and SIM2 can be inserted and used (dual SIM cards with single standby). The device prioritizes checking and using the SIM1 network: when the network of SIM1 is normal, it will consistently use the SIM1 network. If the dial-up of SIM1 network fails or is abnormal, the device will start switching to check the SIM2 network; when the SIM2 network is normal, it will consistently use the SIM2 network. If the SIM2 network is also abnormal, the device will continuously switch between checking SIM1 and SIM2 networks until a successful network connection is established.

Serial Number	**Dialing Status**	**SIM usage**	**NET indicator status**	**SIM status**	**network status**
1	Dialing Failed	No SIM	The green light flashes slowly, and finally goes out	SIM not inserted	not connected
2		Invalid or damaged SIM		Unplugged SIM Or SIM abnormal	
3		SIM installation error			
4	Dialing	SIM is normal	Flashes Quickly	simready	connecting
5	When SIM1 dial-up is successful	1<=Signal value (weak)<=10	S1 stays on steadily / S2 stays off steadily / N light flashes slowly		
6		11<signal value (general)<=20	S1 stays on steadily / S2 stays off steadily / N light		

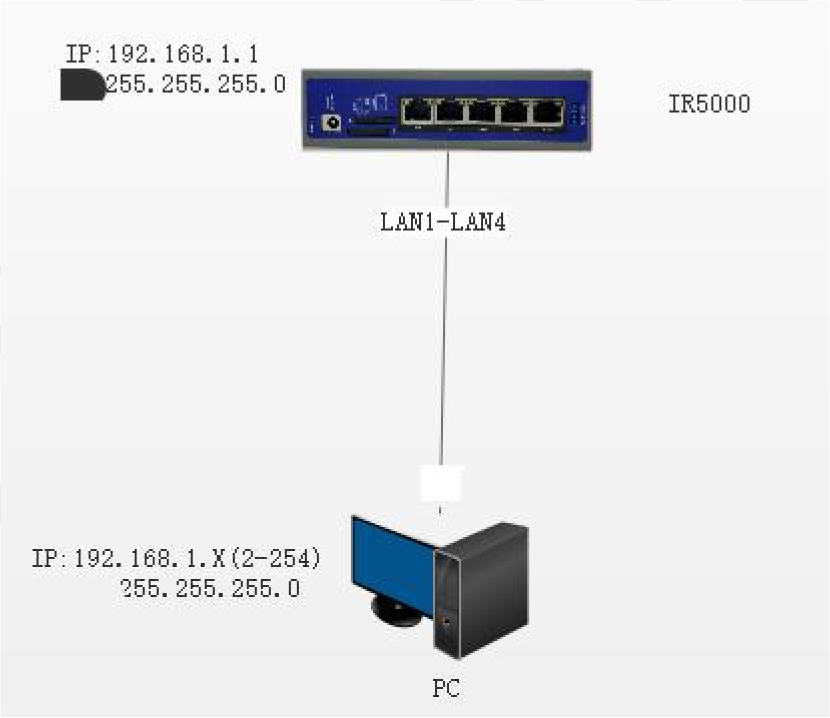
			flashes quickly	simready	connected
7		21<signal value (stronger)<=31	S1 stays on steadily / S2 stays off steadily / N light stays on steadily		
8	When SIM2 dial-up is successful	1<=Signal value (weak)<=10	S2 stays on steadily / S1 stays off steadily / N light flashes slowly		
9		11<signal value (general)<=20	S2 stays on steadily / S21stays off steadily / N light flashes quickly		
10		21<signal value (stronger)<=31	S2 stays on steadily / S1 stays off steadily / N light stays on steadily		

2.4 Web page login

The industrial router products of Chilink support users to view and set relevant product parameters with the login mode of Web terminal. The specific operations are as follows.

Step1: Hardware connection

Connect the router's LAN port to the computer. The computer's LAN card can set the automatic access address (or set the static IP address, but make sure it is on the same network as the router, otherwise you will not be able to log in to the router later. The default LAN address of the router is 192.168.1.1, and the netmask is 255.255.255.0）.



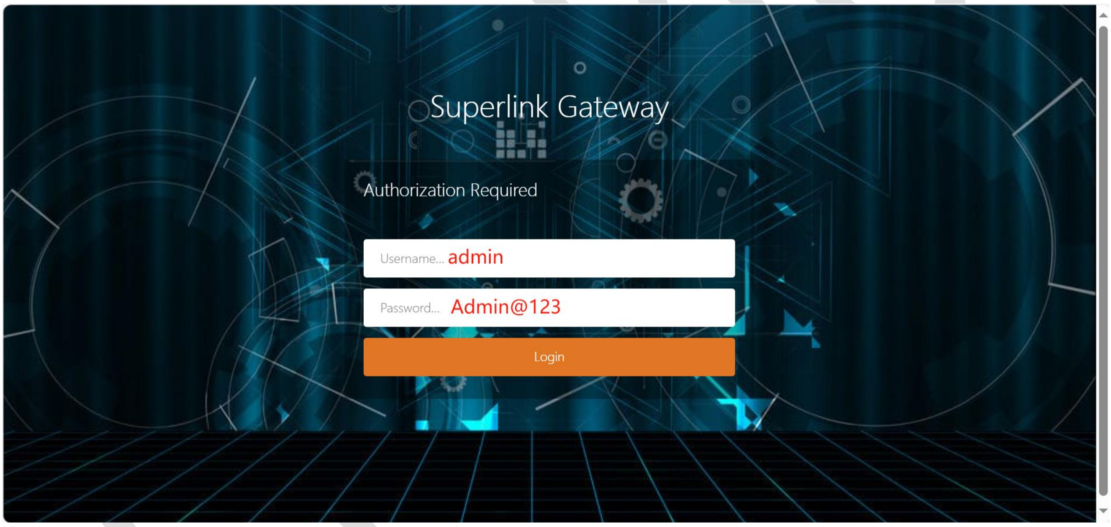
Device connection

Step 2: Check your computer's IP address

Open the computer's local connection and check whether the computer has obtained an IP address.

Step 3: Log on to the router Web using your browser

Open any browser, log in at the default address 192.168.1.1, enter the default user name/password admin/Admin@123(Factory pre-configuration can be customized according to user requirements.) (for the safety of the device, it is strongly recommended to change the default password when using the device, please refer to Section 7.2 "Management Rights" for details), and finally press Enter to enter the device Web page. As follows:



Superlink Gateway

Authorization Required

Username... admin

Password... Admin@123

3.System Status

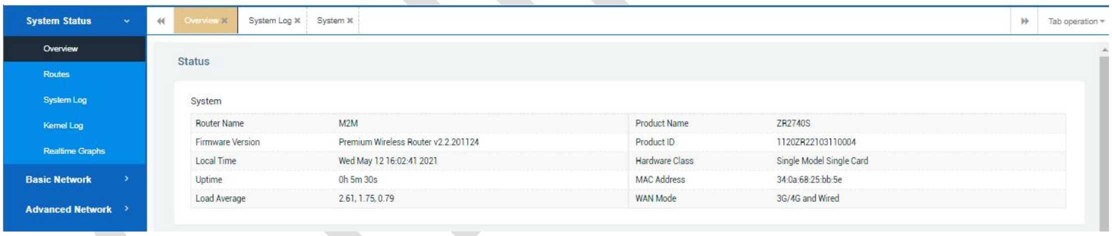
This chapter mainly instructs the user how to view the current status information of the routing device through this function, and make a preliminary judgment of the status of the current network access.

3.1 Overview

After logging in the router Web, click "System Status" -- "Overview". Here you can view some detailed information of the product, as follows:

3.1.1 Status bar

Here you can view the product system name, product model, product serial number, firmware version, hardware type (single module single card/dual module dual card), MAC address, WAN mode (wired mode/compatible mode /3G4G mode), load situation and other information.



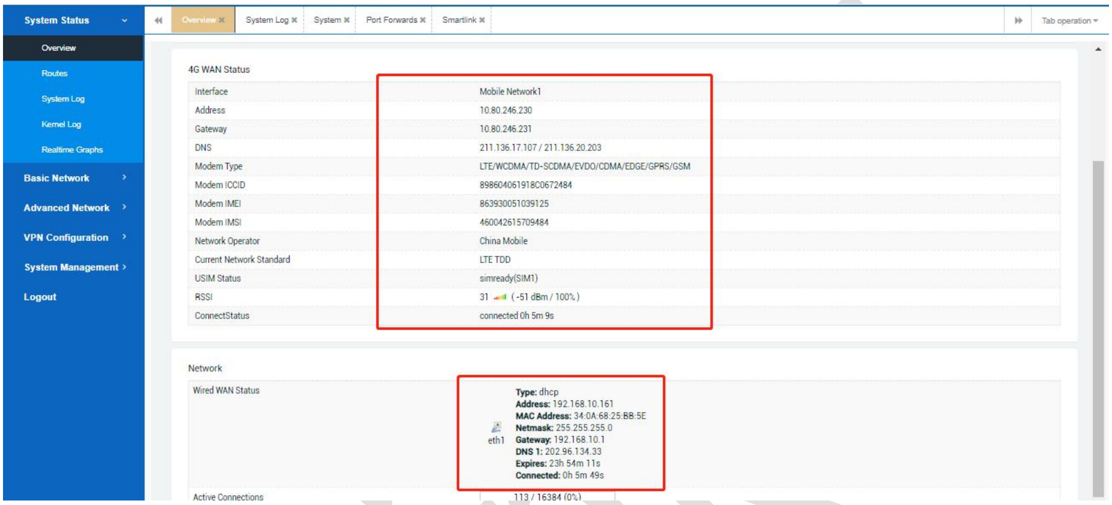
Status

System

Router Name	M2M	Product Name	ZR2740S
Firmware Version	Premium Wireless Router v2.2.201124	Product ID	1120ZR22103110004
Local Time	Wed May 12 16:02:41 2021	Hardware Class	Single Model Single Card
Uptime	0h 5m 30s	MAC Address	34:0a:68:25:bb:5e
Load Average	2.61, 1.75, 0.79	WAN Mode	3G/4G and Wired

3.1.2 Mobile WAN network and wired WAN status view

Here you can view the mobile network status details of the device, such as: SIM card insertion status and 3G/4G dialing details, 4G module identification, base station network received signal strength (RSSI) and the current network connection duration, etc.



4G WAN Status

Interface	Mobile Network1
Address	10.80.246.230
Gateway	10.80.246.231
DNS	211.136.17.107 / 211.136.20.203
Modem Type	LTE/WCDMA/TD-SCDMA/EVDO/CDMA/EDGE/GPRS/GSM
Modem ICCID	898604061918C0672484
Modem IMEI	863930051039125
Modem IMSI	460042615709484
Network Operator	China Mobile
Current Network Standard	LTE TDD
USIM Status	simready(SIM1)
RSSI	31 (-51 dBm / 100%)
ConnectStatus	connected 0h 5m 9s

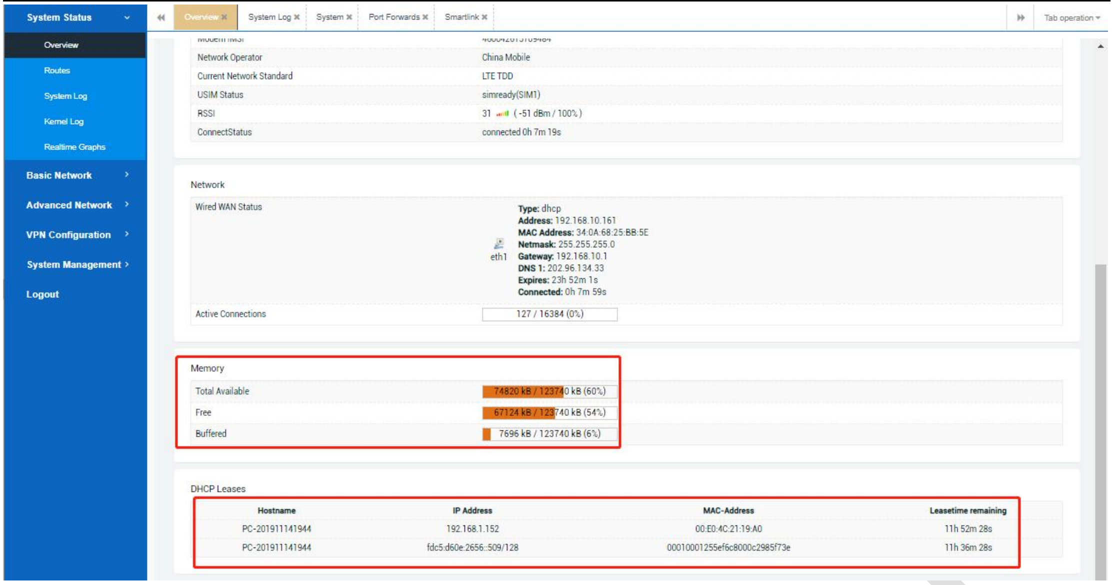
Network

Wired WAN Status	eth1	**Type:** dhcp **Address:** 192.168.10.161 **MAC Address:** 34:0A:68:25:BB:5E **Netmask:** 255.255.255.0 **Gateway:** 192.168.10.1 **DNS 1:** 202.96.134.33 **Expires:** 23h 54m 11s **Connected:** 0h 5m 49s
Active Connections		113 / 16384 (0%)

3.1.3 Memory usage and DHCP connection list

Here you can view the current memory usage of the device, including available memory, unused memory, buffers.

You can also view the list of devices connected to the DHCP server.



Modem IMSI	[illegible]
Network Operator	China Mobile
Current Network Standard	LTE TDD
USIM Status	simready(SIM1)
RSSI	31 (-51 dBm / 100%)
ConnectStatus	connected 0h 7m 19s

Network

Wired WAN Status	eth1 **Type:** dhcp **Address:** 192.168.10.161 **MAC Address:** 34:0A:68:25:BB:5E **Netmask:** 255.255.255.0 **Gateway:** 192.168.10.1 **DNS 1:** 202.96.134.33 **Expires:** 23h 52m 1s **Connected:** 0h 7m 59s
Active Connections	127 / 16384 (0%)

Memory

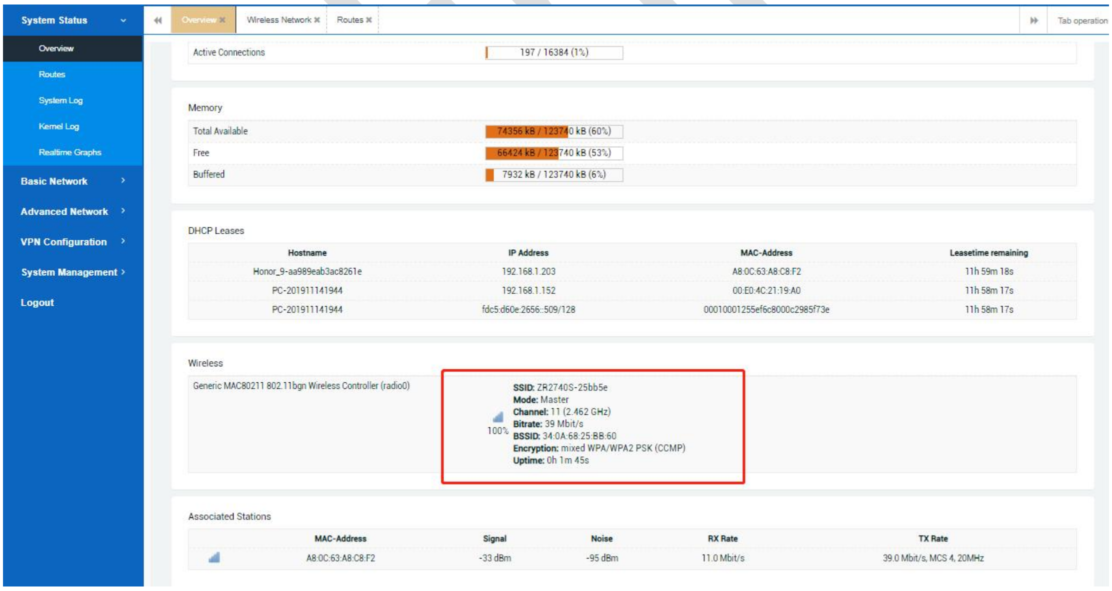
Total Available	74820 kB / 123740 kB (60%)
Free	67124 kB / 123740 kB (54%)
Buffered	7696 kB / 123740 kB (6%)

DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
PC-201911141944	192.168.1.152	00:E0:4C:21:19:A0	11h 52m 28s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 36m 28s

3.1.4 WiFi Access Point information

Here you can view the WiFi enabled status and working mode (AP/Client) of the device. At the same time, you can also check which wireless terminals are connected below, such as mobile phones, laptops, etc.



Active Connections	197 / 16384 (1%)

Memory

Total Available	74356 kB / 123740 kB (60%)
Free	66424 kB / 123740 kB (53%)
Buffered	7932 kB / 123740 kB (6%)

DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
Honor_9-aa989eab3ac8261e	192.168.1.203	A8:0C:63:A8:C8:F2	11h 59m 18s
PC-201911141944	192.168.1.152	00:E0:4C:21:19:A0	11h 58m 17s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 58m 17s

Wireless

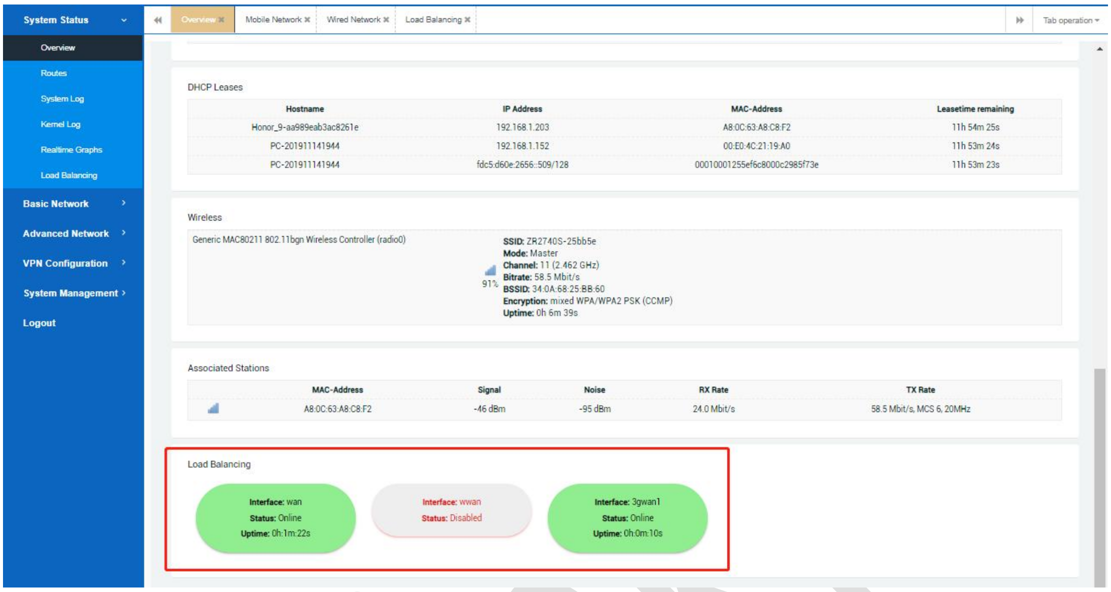
Generic MAC80211 802.11bgn Wireless Controller (radio0)	100% **SSID:** ZR2740S-25bb5e **Mode:** Master **Channel:** 11 (2.462 GHz) **Bitrate:** 39 Mbit/s **BSSID:** 34:0A:68:25:BB:60 **Encryption:** mixed WPA/WPA2 PSK (CCMP) **Uptime:** 0h 1m 45s

Associated Stations

	MAC-Address	Signal	Noise	RX Rate	TX Rate
	A8:0C:63:A8:C8:F2	-33 dBm	-95 dBm	11.0 Mbit/s	39.0 Mbit/s, MCS 4, 20MHz

3.1.5 Load Balancing (optional)

Here you can view the load balancing (MWAN3) interface status of the device (3G/4G mobile WAN and wired WAN), such as online or offline.



DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
Honor_9-aa989eab3ac8261e	192.168.1.203	A8:0C:63:A8:C8:F2	11h 54m 25s
PC-201911141944	192.168.1.152	00:E0:4C:21:19:A0	11h 53m 24s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 53m 23s

Wireless

Generic MAC80211 802.11bgn Wireless Controller (radio0)

SSID: ZR2740S-25bb5e
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: 58.5 Mbit/s
BSSID: 34:0A:68:25:BB:60
Encryption: mixed WPA/WPA2 PSK (CCMP)
Uptime: 0h 6m 39s

Associated Stations

MAC-Address	Signal	Noise	RX Rate	TX Rate
A8:0C:63:A8:C8:F2	-46 dBm	-95 dBm	24.0 Mbit/s	58.5 Mbit/s, MCS 6, 20MHz

Load Balancing

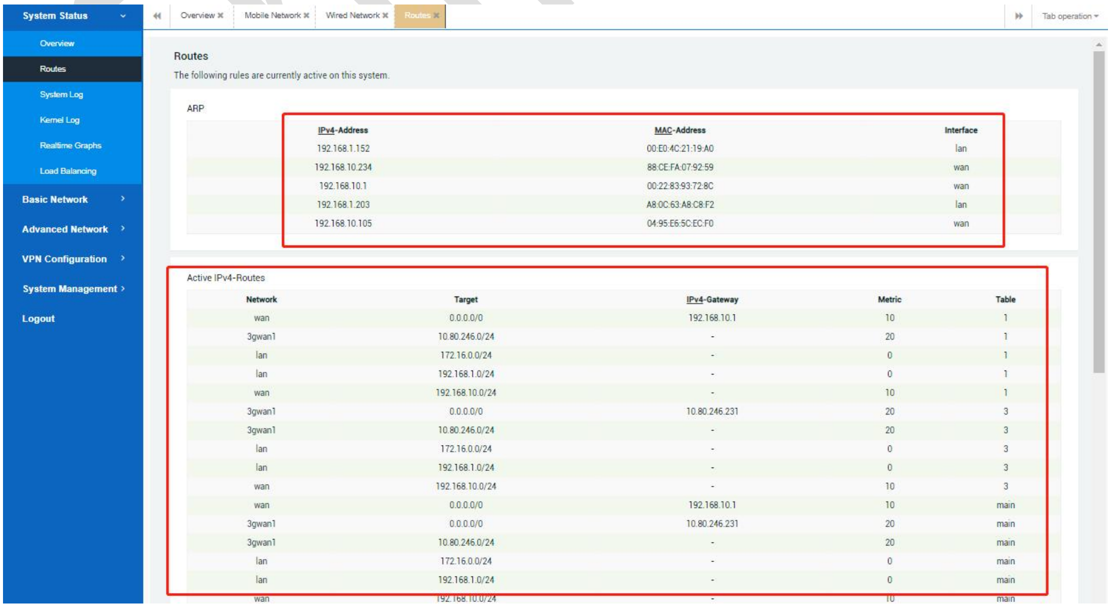
Interface: wan
Status: Online
Uptime: 0h:1m:22s

Interface: wwan
Status: Disabled

Interface: 3gwan1
Status: Online
Uptime: 0h:0m:10s

3.2 Routing Table

Here you can view the current host address list information through the ARP list; All active IPv4 and IPv6 routing links can be viewed at the same time as follows.



Routes

The following rules are currently active on this system.

ARP

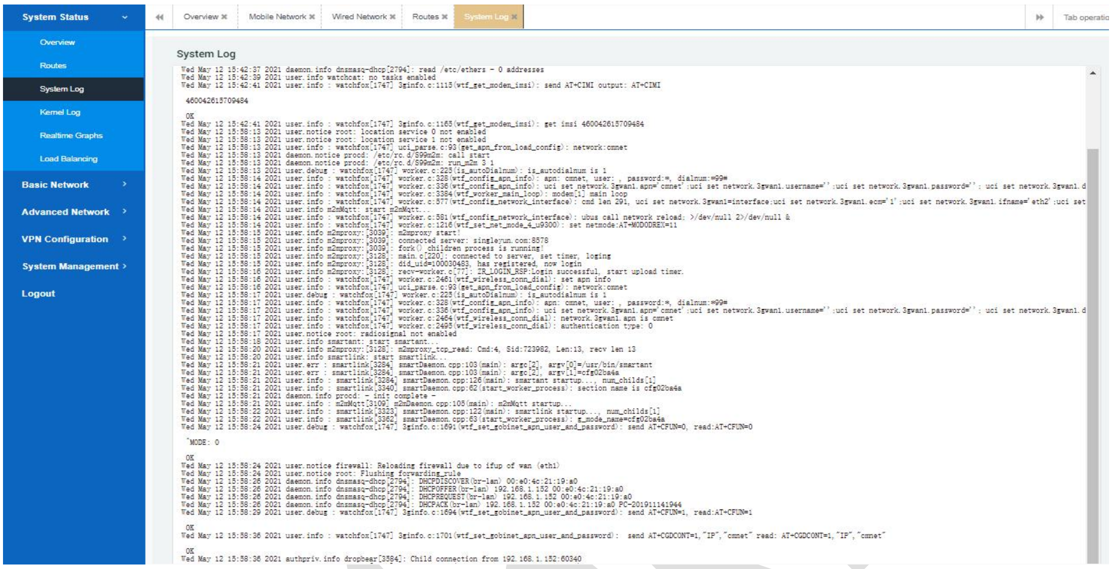
IPv4-Address	MAC-Address	Interface
192.168.1.152	00:E0:4C:21:19:A0	lan
192.168.10.234	88:CE:FA:07:92:59	wan
192.168.10.1	00:22:83:93:72:8C	wan
192.168.1.203	A8:0C:63:A8:C8:F2	lan
192.168.10.105	04:95:E6:5C:EC:F0	wan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	192.168.10.1	10	1
3gwan1	10.80.246.0/24	-	20	1
lan	172.16.0.0/24	-	0	1
lan	192.168.1.0/24	-	0	1
wan	192.168.10.0/24	-	10	1
3gwan1	0.0.0.0/0	10.80.246.231	20	3
3gwan1	10.80.246.0/24	-	20	3
lan	172.16.0.0/24	-	0	3
lan	192.168.1.0/24	-	0	3
wan	192.168.10.0/24	-	10	3
wan	0.0.0.0/0	192.168.10.1	10	main
3gwan1	0.0.0.0/0	10.80.246.231	20	main
3gwan1	10.80.246.0/24	-	20	main
lan	172.16.0.0/24	-	0	main
lan	192.168.1.0/24	-	0	main
wan	192.168.10.0/24	-	10	main

3.3 System Log

Here you can view the log details of the current function modules of the device. When there is an abnormal operation of the device, we can locate the on-site problems of the customer according to the log.

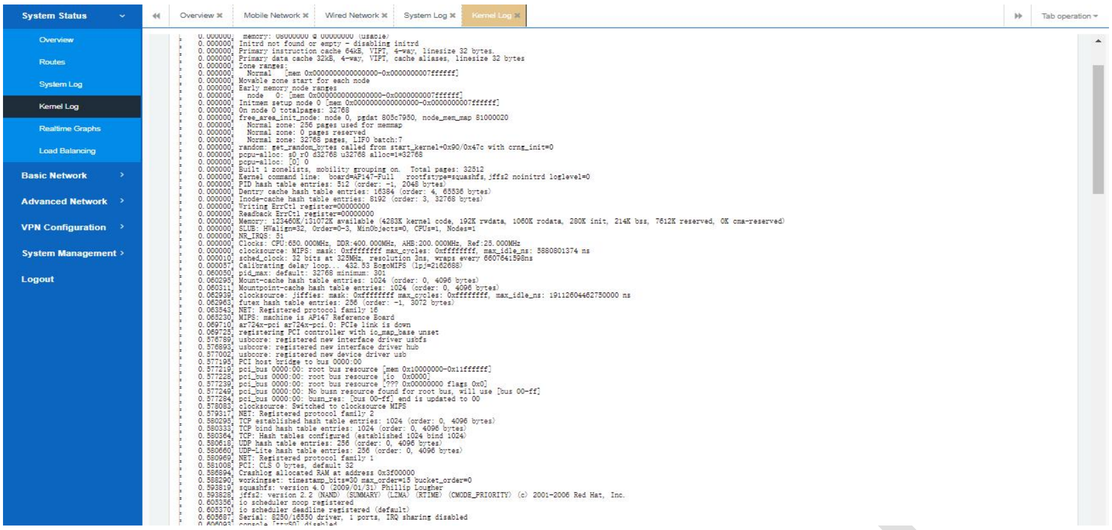


System Log

```
Wed May 12 15:42:37 2021 daemon.info dnsmasq-dhcp[2794]: read /etc/ethers - 0 addresses
Wed May 12 15:42:39 2021 user.info watchcat: no tasks enabled
Wed May 12 15:42:41 2021 user.info : watchfox[1747] 3ginfo.c:1115(wtf_get_modem_imsi): send AT+CIMI output: AT+CIMI

 460042615709484

 OK
Wed May 12 15:42:41 2021 user.info : watchfox[1747] 3ginfo.c:1165(wtf_get_modem_imsi): get imsi 460042615709484
Wed May 12 15:58:13 2021 user.notice root: location service 0 not enabled
Wed May 12 15:58:13 2021 user.notice root: location service 1 not enabled
Wed May 12 15:58:13 2021 user.info : watchfox[1747] uci_parse.c:93(get_apn_from_load_config): network:cmnet
Wed May 12 15:58:13 2021 daemon.notice procd: /etc/rc.d/S99m2m: call start
Wed May 12 15:58:13 2021 daemon.notice procd: /etc/rc.d/S99m2m: run_m2m 3 1
Wed May 12 15:58:13 2021 user.debug : watchfox[1747] worker.c:225(is_autoDialnum): is_autodialnum is 1
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:328(wtf_config_apn_info): apn: cmnet, user: , password:*, dialnum:*99#
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:336(wtf_config_apn_info): uci set network.3gwan1.apn='cmnet';uci set network.3gwan1.username='';uci set network.3gwan1.password=''; uci set network.3gwan1.d
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:3384(wtf_worker_main_loop): modem[1] main loop
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:577(wtf_config_network_interface): cmd len 291, uci set network.3gwan1=interface;uci set network.3gwan1.ecm='1';uci set network.3gwan1.ifname='eth2';uci set
Wed May 12 15:58:14 2021 user.info m2mMqtt: start m2mMqtt...
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:581(wtf_config_network_interface): ubus call network reload; >/dev/null 2>/dev/null &
Wed May 12 15:58:14 2021 user.info : watchfox[1747] worker.c:1216(wtf_set_net_mode_4_u9300): set netmode:AT+MODODREX=11
Wed May 12 15:58:15 2021 user.info m2mproxy:[3039]: m2mproxy start!
Wed May 12 15:58:15 2021 user.info m2mproxy:[3039]: connected server: singleyun.com:8578
Wed May 12 15:58:15 2021 user.info m2mproxy:[3039]: fork() children process is running!
Wed May 12 15:58:15 2021 user.info m2mproxy:[3128]: main.c[220]: connected to server, set timer, loging
Wed May 12 15:58:15 2021 user.info m2mproxy:[3128]: did_uid=100030483, has registered, now login
Wed May 12 15:58:16 2021 user.info m2mproxy:[3128]: recv-worker.c[77]: ZR_LOGIN_RSP:Login successful, start upload timer.
Wed May 12 15:58:16 2021 user.info : watchfox[1747] worker.c:2461(wtf_wireless_conn_dial): set apn info
Wed May 12 15:58:16 2021 user.info : watchfox[1747] uci_parse.c:93(get_apn_from_load_config): network:cmnet
Wed May 12 15:58:17 2021 user.debug : watchfox[1747] worker.c:225(is_autoDialnum): is_autodialnum is 1
Wed May 12 15:58:17 2021 user.info : watchfox[1747] worker.c:328(wtf_config_apn_info): apn: cmnet, user: , password:*, dialnum:*99#
Wed May 12 15:58:17 2021 user.info : watchfox[1747] worker.c:336(wtf_config_apn_info): uci set network.3gwan1.apn='cmnet';uci set network.3gwan1.username='';uci set network.3gwan1.password=''; uci set network.3gwan1.d
Wed May 12 15:58:17 2021 user.info : watchfox[1747] worker.c:2464(wtf_wireless_conn_dial): network.3gwan1.apn is cmnet
Wed May 12 15:58:17 2021 user.info : watchfox[1747] worker.c:2495(wtf_wireless_conn_dial): authentication type: 0
Wed May 12 15:58:17 2021 user.notice root: radiosignal not enabled
Wed May 12 15:58:18 2021 user.info smartant: start smartant...
Wed May 12 15:58:20 2021 user.info m2mproxy:[3128]: m2mproxy_tcp_read: Cmd:4, Sid:723982, Len:13, recv len 13
Wed May 12 15:58:20 2021 user.info smartlink: start smartlink...
Wed May 12 15:58:21 2021 user.err : smartlink[3284] smartDaemon.cpp:103(main): argc[2], argv[0]=/usr/bin/smartant
Wed May 12 15:58:21 2021 user.err : smartlink[3284] smartDaemon.cpp:103(main): argc[2], argv[1]=cfg02ba4a
Wed May 12 15:58:21 2021 user.info : smartlink[3284] smartDaemon.cpp:126(main): smartant startup..., num_childs[1]
Wed May 12 15:58:21 2021 user.info : smartlink[3340] smartDaemon.cpp:62(start_worker_process): section name is cfg02ba4a
Wed May 12 15:58:21 2021 daemon.info procd: - init complete -
Wed May 12 15:58:21 2021 user.info : m2mMqtt[3109] m2mDaemon.cpp:105(main): m2mMqtt startup...
Wed May 12 15:58:22 2021 user.info : smartlink[3323] smartDaemon.cpp:122(main): smartlink startup..., num_childs[1]
Wed May 12 15:58:22 2021 user.info : smartlink[3362] smartDaemon.cpp:63(start_worker_process): g_mode_name=cfg02ba4a
Wed May 12 15:58:24 2021 user.debug : watchfox[1747] 3ginfo.c:1691(wtf_set_gobinet_apn_user_and_password): send AT+CFUN=0, read:AT+CFUN=0

 ^MODE: 0

 OK
Wed May 12 15:58:24 2021 user.notice firewall: Reloading firewall due to ifup of wan (eth1)
Wed May 12 15:58:24 2021 user.notice root: Flushing forwarding_rule
Wed May 12 15:58:26 2021 daemon.info dnsmasq-dhcp[2794]: DHCPDISCOVER(br-lan) 00:e0:4c:21:19:a0
Wed May 12 15:58:26 2021 daemon.info dnsmasq-dhcp[2794]: DHCPOFFER(br-lan) 192.168.1.152 00:e0:4c:21:19:a0
Wed May 12 15:58:26 2021 daemon.info dnsmasq-dhcp[2794]: DHCPREQUEST(br-lan) 192.168.1.152 00:e0:4c:21:19:a0
Wed May 12 15:58:26 2021 daemon.info dnsmasq-dhcp[2794]: DHCPACK(br-lan) 192.168.1.152 00:e0:4c:21:19:a0 PC-201911141944
Wed May 12 15:58:29 2021 user.debug : watchfox[1747] 3ginfo.c:1694(wtf_set_gobinet_apn_user_and_password): send AT+CFUN=1, read:AT+CFUN=1

 OK
Wed May 12 15:58:36 2021 user.info : watchfox[1747] 3ginfo.c:1701(wtf_set_gobinet_apn_user_and_password):  send AT+CGDCONT=1,"IP","cmnet" read: AT+CGDCONT=1,"IP","cmnet"

 OK
Wed May 12 15:58:36 2021 authpriv.info dropbear[3584]: Child connection from 192.168.1.152:60340
```

3.4 Kernel Log

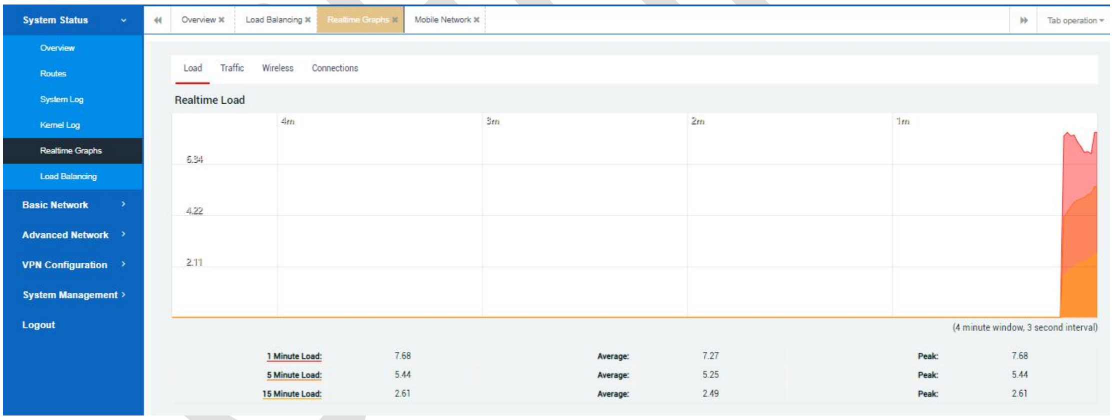
Here you can view the device background system driver interface startup information, when there are some device connection or startup abnormalities, you can use these logs to further locate customer field problems.



```
[    0.000000]  memory: 08000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
[    0.000000] Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
[    0.000000] Zone ranges:
[    0.000000]   Normal   [mem 0x0000000000000000-0x0000000007ffffff]
[    0.000000] Movable zone start for each node
[    0.000000] Early memory node ranges
[    0.000000]   node   0: [mem 0x0000000000000000-0x0000000007ffffff]
[    0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x0000000007ffffff]
[    0.000000] On node 0 totalpages: 32768
[    0.000000] free_area_init_node: node 0, pgdat 805c7950, node_mem_map 81000020
[    0.000000]   Normal zone: 256 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 32768 pages, LIFO batch:7
[    0.000000] random: get_random_bytes called from start_kernel+0x90/0x47c with crng_init=0
[    0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[    0.000000] pcpu-alloc: [0] 0
[    0.000000] Built 1 zonelists, mobility grouping on.  Total pages: 32512
[    0.000000] Kernel command line:  board=AP147-Full   rootfstype=squashfs,jffs2 noinitrd loglevel=0
[    0.000000] PID hash table entries: 512 (order: -1, 2048 bytes)
[    0.000000] Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
[    0.000000] Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
[    0.000000] Writing ErrCtl register=00000000
[    0.000000] Readback ErrCtl register=00000000
[    0.000000] Memory: 123460K/131072K available (4283K kernel code, 192K rwdata, 1060K rodata, 280K init, 214K bss, 7612K reserved, 0K cma-reserved)
[    0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[    0.000000] NR_IRQS: 51
[    0.000000] Clocks: CPU:650.000MHz, DDR:400.000MHz, AHB:200.000MHz, Ref:25.000MHz
[    0.000000] clocksource: MIPS: mask: 0xffffffff max_cycles: 0xffffffff, max_idle_ns: 5880801374 ns
[    0.000010] sched_clock: 32 bits at 325MHz, resolution 3ns, wraps every 6607641598ns
[    0.000057] Calibrating delay loop... 432.53 BogoMIPS (lpj=2162688)
[    0.060050] pid_max: default: 32768 minimum: 301
[    0.060295] Mount-cache hash table entries: 1024 (order: 0, 4096 bytes)
[    0.060311] Mountpoint-cache hash table entries: 1024 (order: 0, 4096 bytes)
[    0.062939] clocksource: jiffies: mask: 0xffffffff max_cycles: 0xffffffff, max_idle_ns: 19112604462750000 ns
[    0.062963] futex hash table entries: 256 (order: -1, 3072 bytes)
[    0.063543] NET: Registered protocol family 16
[    0.065230] MIPS: machine is AP147 Reference Board
[    0.069710] ar724x-pci ar724x-pci.0: PCIe link is down
[    0.069725] registering PCI controller with io_map_base unset
[    0.576789] usbcore: registered new interface driver usbfs
[    0.576893] usbcore: registered new interface driver hub
[    0.577002] usbcore: registered new device driver usb
[    0.577195] PCI host bridge to bus 0000:00
[    0.577219] pci_bus 0000:00: root bus resource [mem 0x10000000-0x11ffffff]
[    0.577228] pci_bus 0000:00: root bus resource [io  0x0000]
[    0.577239] pci_bus 0000:00: root bus resource [??? 0x00000000 flags 0x0]
[    0.577249] pci_bus 0000:00: No busn resource found for root bus, will use [bus 00-ff]
[    0.577284] pci_bus 0000:00: busn_res: [bus 00-ff] end is updated to 00
[    0.578083] clocksource: Switched to clocksource MIPS
[    0.579317] NET: Registered protocol family 2
[    0.580295] TCP established hash table entries: 1024 (order: 0, 4096 bytes)
[    0.580333] TCP bind hash table entries: 1024 (order: 0, 4096 bytes)
[    0.580364] TCP: Hash tables configured (established 1024 bind 1024)
[    0.580618] UDP hash table entries: 256 (order: 0, 4096 bytes)
[    0.580660] UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
[    0.580969] NET: Registered protocol family 1
[    0.581008] PCI: CLS 0 bytes, default 32
[    0.586894] Crashlog allocated RAM at address 0x3f00000
[    0.588290] workingset: timestamp_bits=30 max_order=15 bucket_order=0
[    0.593819] squashfs: version 4.0 (2009/01/31) Phillip Lougher
[    0.593828] jffs2: version 2.2 (NAND) (SUMMARY) (LZMA) (RTIME) (CMODE_PRIORITY) (c) 2001-2006 Red Hat, Inc.
[    0.605356] io scheduler noop registered
[    0.605370] io scheduler deadline registered (default)
[    0.605687] Serial: 8250/16550 driver, 1 ports, IRQ sharing disabled
[    0.606093] console [ttyS0] disabled
```

3.5 Real-time information

Here you can view the device load in real time (such as the load details in the 1st, 5th and 15th minutes), the upstream and downstream real-time traffic situation of different network interfaces, the signal and noise situation of WIFI and the link of other activities.

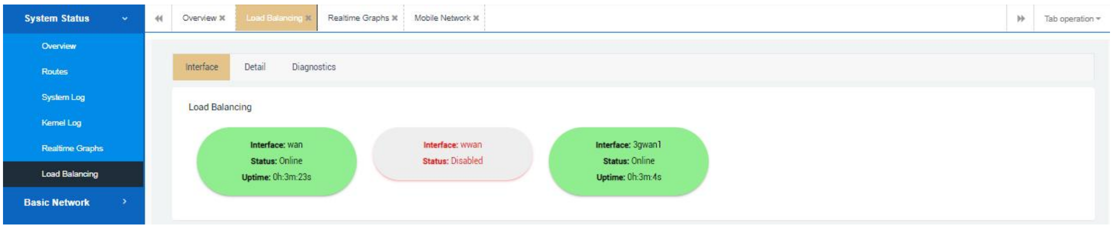


1 Minute Load:	7.68	Average:	7.27	Peak:	7.68
5 Minute Load:	5.44	Average:	5.25	Peak:	5.44
15 Minute Load:	2.61	Average:	2.49	Peak:	2.61

3.6 Load balancing

1）Interfaces

Here you can check the current online and offline status of each interface（WAN for wired WAN, WWAN for wifi client, 3gwan1 for 3/4G mobile network） of the system after the load balancing function is enabled (the system does not open load balancing by default, if you need to use it, please place an order and comment).



Load Balancing

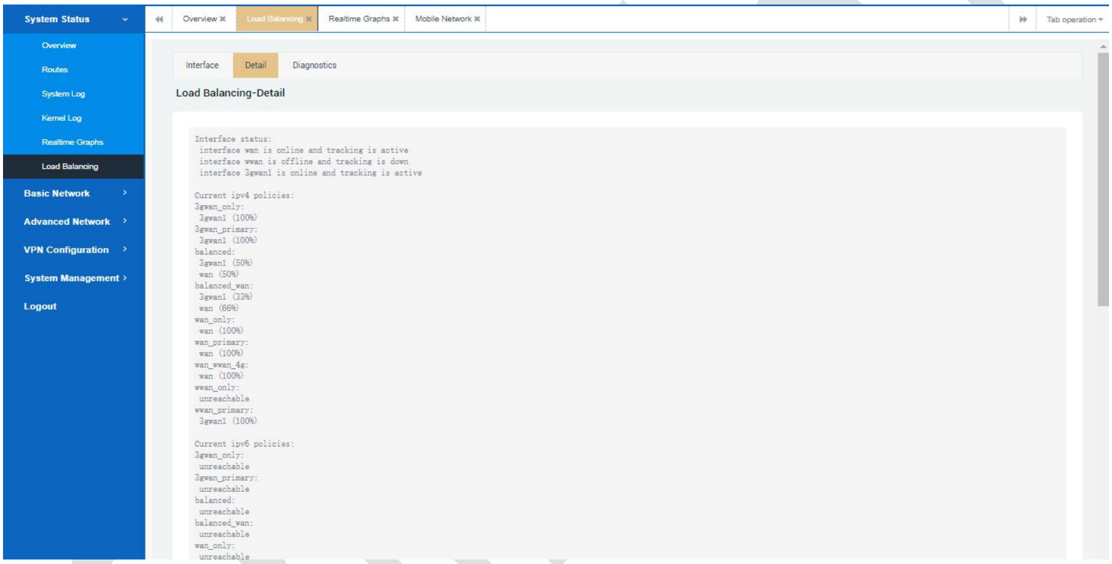
Interface: wan
Status: Online
Uptime: 0h:3m:23s

Interface: wwan
Status: Disabled

Interface: 3gwan1
Status: Online
Uptime: 0h:3m:4s

2）Detail

Here is a detailed view of the current load-balancing IPv4 / IPv6 policy rule status) .

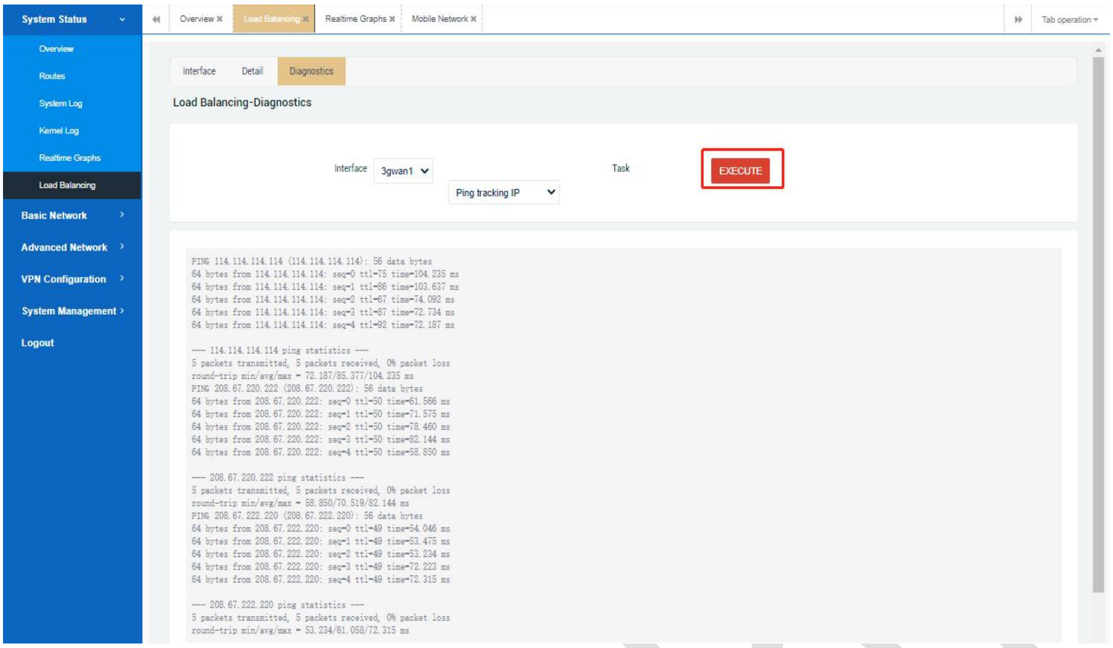


Load Balancing-Detail

```
Interface status:
 interface wan is online and tracking is active
 interface wwan is offline and tracking is down
 interface 3gwan1 is online and tracking is active

Current ipv4 policies:
3gwan_only:
 3gwan1 (100%)
3gwan_primary:
 3gwan1 (100%)
balanced:
 3gwan1 (50%)
 wan (50%)
balanced_wan:
 3gwan1 (33%)
 wan (66%)
wan_only:
 wan (100%)
wan_primary:
 wan (100%)
wan_wwan_4g:
 wan (100%)
wwan_only:
 unreachable
wwan_primary:
 3gwan1 (100%)

Current ipv6 policies:
3gwan_only:
 unreachable
3gwan_primary:
 unreachable
balanced:
 unreachable
balanced_wan:
 unreachable
wan_only:
 unreachable
```

3）Diagnosis

Here, the system WAN or 3GWAN1 interface can be respectively tested for connectivity to confirm whether the current network is normal and available.



Load Balancing-Diagnostics

Interface: 3gwan1

Task: Ping tracking IP

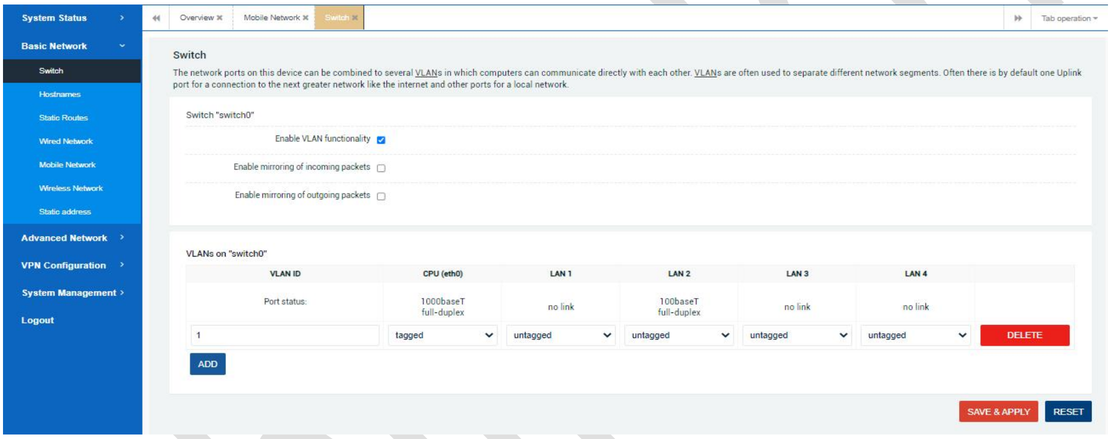
```
PING 114.114.114.114 (114.114.114.114): 56 data bytes
64 bytes from 114.114.114.114: seq=0 ttl=75 time=104.235 ms
64 bytes from 114.114.114.114: seq=1 ttl=86 time=103.637 ms
64 bytes from 114.114.114.114: seq=2 ttl=67 time=74.092 ms
64 bytes from 114.114.114.114: seq=3 ttl=87 time=72.734 ms
64 bytes from 114.114.114.114: seq=4 ttl=92 time=72.187 ms

--- 114.114.114.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 72.187/85.377/104.235 ms
PING 208.67.220.222 (208.67.220.222): 56 data bytes
64 bytes from 208.67.220.222: seq=0 ttl=50 time=61.566 ms
64 bytes from 208.67.220.222: seq=1 ttl=50 time=71.575 ms
64 bytes from 208.67.220.222: seq=2 ttl=50 time=78.460 ms
64 bytes from 208.67.220.222: seq=3 ttl=50 time=82.144 ms
64 bytes from 208.67.220.222: seq=4 ttl=50 time=58.850 ms

--- 208.67.220.222 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 58.850/70.519/82.144 ms
PING 208.67.222.220 (208.67.222.220): 56 data bytes
64 bytes from 208.67.222.220: seq=0 ttl=49 time=54.046 ms
64 bytes from 208.67.222.220: seq=1 ttl=49 time=53.475 ms
64 bytes from 208.67.222.220: seq=2 ttl=49 time=53.234 ms
64 bytes from 208.67.222.220: seq=3 ttl=49 time=72.223 ms
64 bytes from 208.67.222.220: seq=4 ttl=49 time=72.315 ms

--- 208.67.222.220 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 53.234/61.058/72.315 ms
```

4. Basic Network

This chapter mainly introduces several different external network access scenarios supported by our router, including wired WAN network, WIFI client network, 4G mobile dial up network, etc. The following mainly introduces the use of these specific configuration methods.

4.1 Switch

This part can divide the device into VLAN to divide the system network into different network segments. The details are brief.



Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Switch "switch0"

Enable VLAN functionality ☑

Enable mirroring of incoming packets ☐

Enable mirroring of outgoing packets ☐

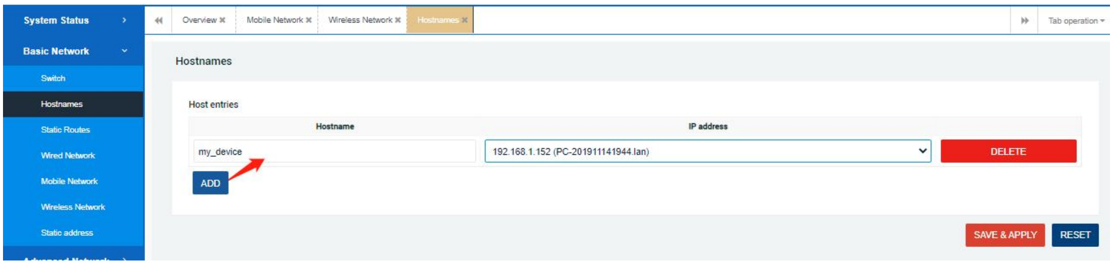
VLANs on "switch0"

VLAN ID	CPU (eth0)	LAN 1	LAN 2	LAN 3	LAN 4	
Port status:	1000baseT full-duplex	no link	100baseT full-duplex	no link	no link	
1	tagged	untagged	untagged	untagged	untagged	DELETE

4.2 Hostnames

Here, by clicking the "add" button, you can customize the host name of the device connected to the router based on their different IP address.

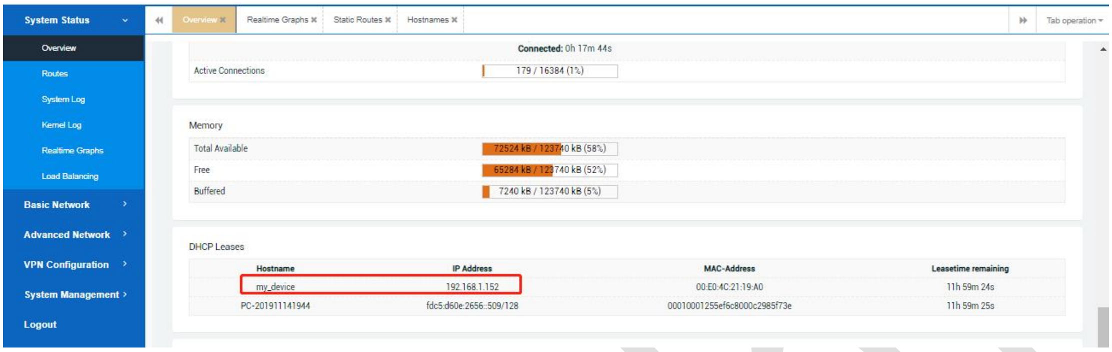
Example configuration: Customize a host named 'my_device' for the computer with IP address 192.168.1.152 connected to the router. You can see this host information in the System State Overview section.



Hostnames

Host entries

Hostname	IP address
my_device	192.168.1.152 (PC-201911141944.lan)



Connected: 0h 17m 44s

Active Connections 179 / 16384 (1%)

Memory

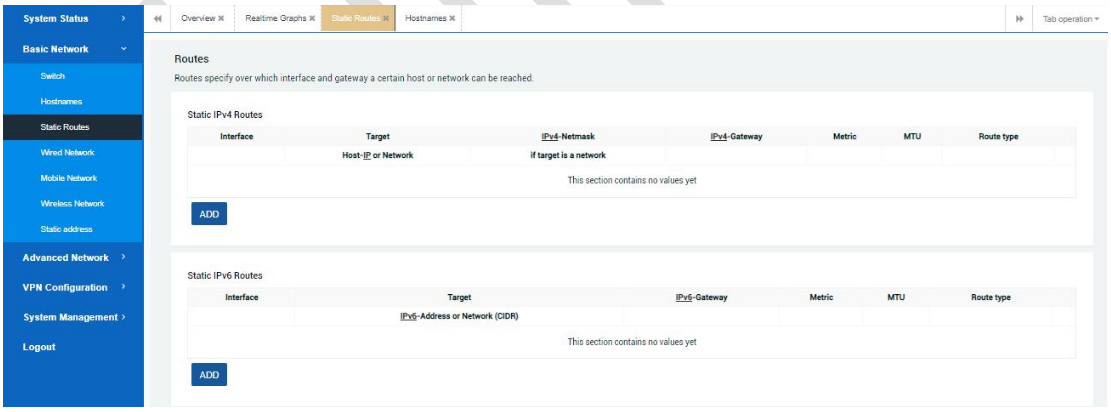
Total Available	72524 kB / 123740 kB (58%)
Free	65284 kB / 123740 kB (52%)
Buffered	7240 kB / 123740 kB (5%)

DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
my_device	192.168.1.152	00:E0:4C:21:19:A0	11h 59m 24s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 59m 25s

4.3 Static Routing

This section allows you to view all the current IPv4 / IPv6 dynamic routing tables of the system; You can also create a static routing table (mainly IPv4) by clicking the "Add" button to set up communication with the specified target network.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Route type
	Host-IP or Network	if target is a network				

This section contains no values yet

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	Route type
	IPv6-Address or Network (CIDR)				

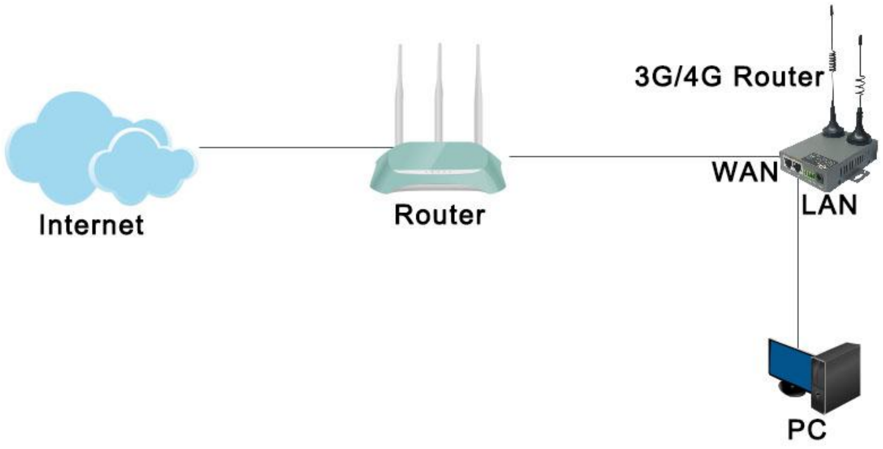
This section contains no values yet

4.4 Wired Network

This chapter mainly introduces several different network configuration modes of wired WAN in routing system, including dynamic WAN address, static WAN address, and PPPOE broadband dial-up mode.

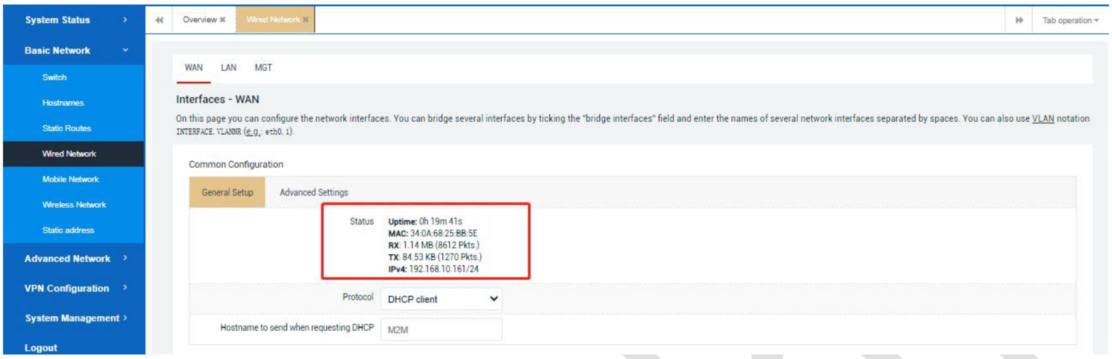
4.4.1 WAN Interface

Cable WAN network mode is to point to by a line bridge connecting mode connect a router's WAN port to another (superior) the router LAN port and make itself has the capability of network access (supervisor should pay attention to union of two router LAN network cannot be completely the same, otherwise result in network conflicts, you can change any of a router LAN address to avoid conflict).



4.4.1.1 DHCP Client

As shown in the figure below, the system defaults to the working mode of "DHCP client", that is, after accessing the superior router network, it will automatically obtain the IP address to access the Internet.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Common Configuration

Status
Uptime: 0h 19m 41s
MAC: 34:0A:68:25:BB:5E
RX: 1.14 MB (8612 Pkts.)
TX: 84.53 KB (1270 Pkts.)
IPv4: 192.168.10.161/24

Protocol: DHCP client

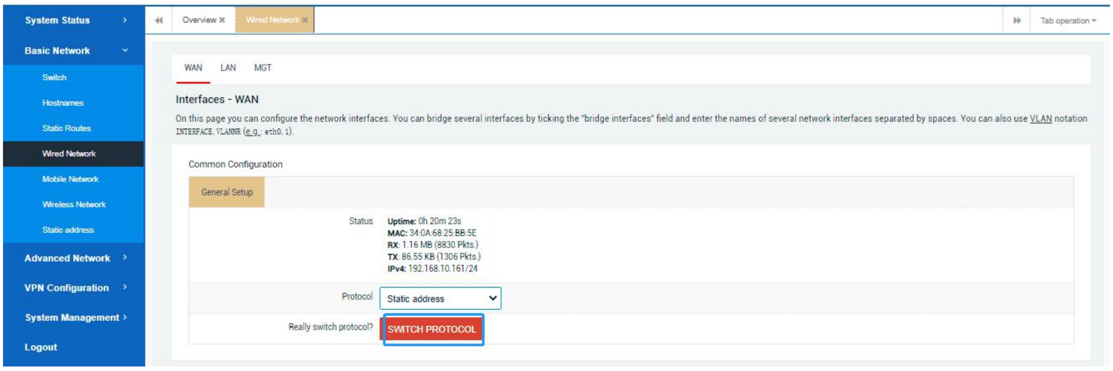
Hostname to send when requesting DHCP: M2M

4.4.1.2 Static(wan) address

In addition to automatic WAN access, you can also set the static IP address (must be set to the same network segment as the router above, the mask must be the same, the gateway address and the DNS address also need to be set; For example, the parent router network is 192.168.10.0/24, and the gateway address is 192.168.10.1).

The configuration is as follows:

Select "Basic Network" -- "Wired Network" -- "WAN" -- "General Setup", select the protocol as "Static Address", then switch the protocol and set IP address, subnet mask, gateway address and DNS server, and save the application.



Interfaces - WAN

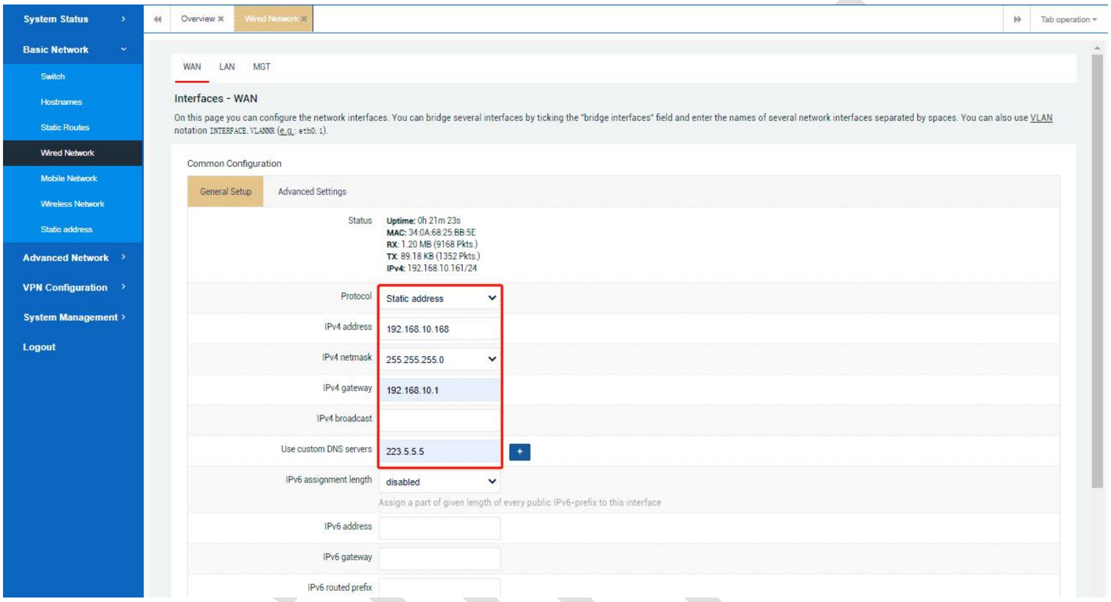
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Common Configuration

Status: **Uptime:** 0h 20m 23s
MAC: 34:0A:68:25:BB:5E
RX: 1.16 MB (8830 Pkts.)
TX: 86.55 KB (1306 Pkts.)
IPv4: 192.168.10.161/24

Protocol: Static address

Really switch protocol?



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Common Configuration

Status: **Uptime:** 0h 21m 23s
MAC: 34:0A:68:25:BB:5E
RX: 1.20 MB (9168 Pkts.)
TX: 89.18 KB (1352 Pkts.)
IPv4: 192.168.10.161/24

Protocol: Static address

IPv4 address: 192.168.10.168

IPv4 netmask: 255.255.255.0

IPv4 gateway: 192.168.10.1

IPv4 broadcast:

Use custom DNS servers: 223.5.5.5

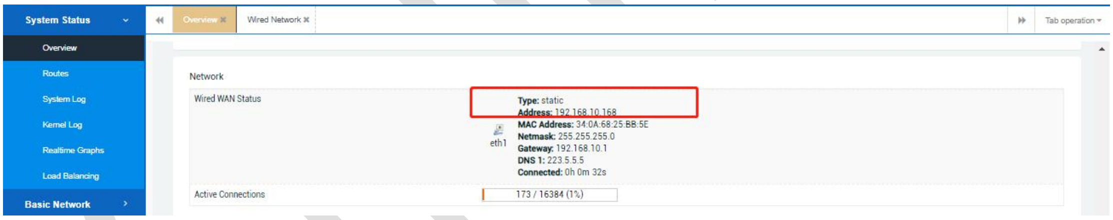
IPv6 assignment length: disabled

Assign a part of given length of every public IPv6-prefix to this interface

IPv6 address:

IPv6 gateway:

IPv6 routed prefix:



Network

Wired WAN Status: **Type:** static
Address: 192.168.10.168
MAC Address: 34:0A:68:25:BB:5E
Netmask: 255.255.255.0
Gateway: 192.168.10.1
DNS 1: 223.5.5.5
Connected: 0h 0m 32s

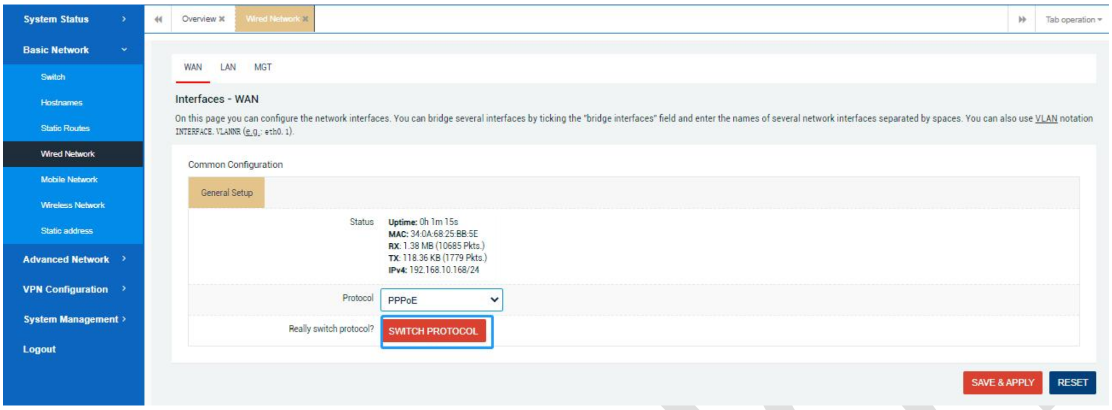
Active Connections: 173 / 16384 (1%)

4.4.1.3 PPPoE dial-up

This method mainly refers to using a broadband account assigned by a carrier or other ISP network provider to access the Internet.

Configuration actions:

Select "Basic Network" -- "Wired Network" -- "WAN" -- "General Setup" and select the protocol as "PPPoE". After switching the protocol, fill in the corresponding PAP/CHAP user name and password, and save the application.



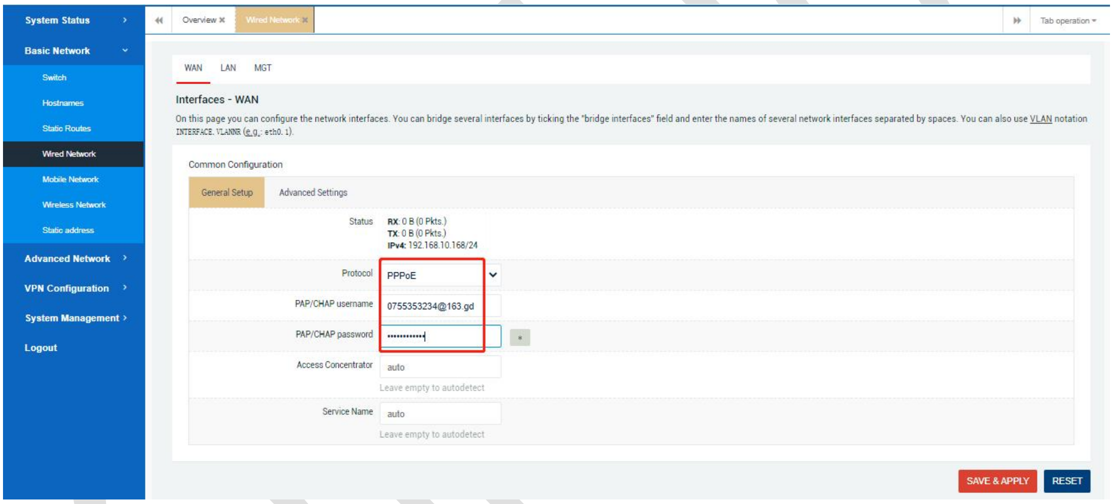
Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status: Uptime: 0h 1m 15s
MAC: 34:0A:68:25:BB:5E
RX: 1.38 MB (10685 Pkts.)
TX: 118.36 KB (1779 Pkts.)
IPv4: 192.168.10.168/24

Protocol: PPPoE

Really switch protocol? SWITCH PROTOCOL



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status: RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 192.168.10.168/24

Protocol: PPPoE

PAP/CHAP username: 0755353234@163.gd

PAP/CHAP password: ••••••••••••

Access Concentrator: auto
Leave empty to autodetect

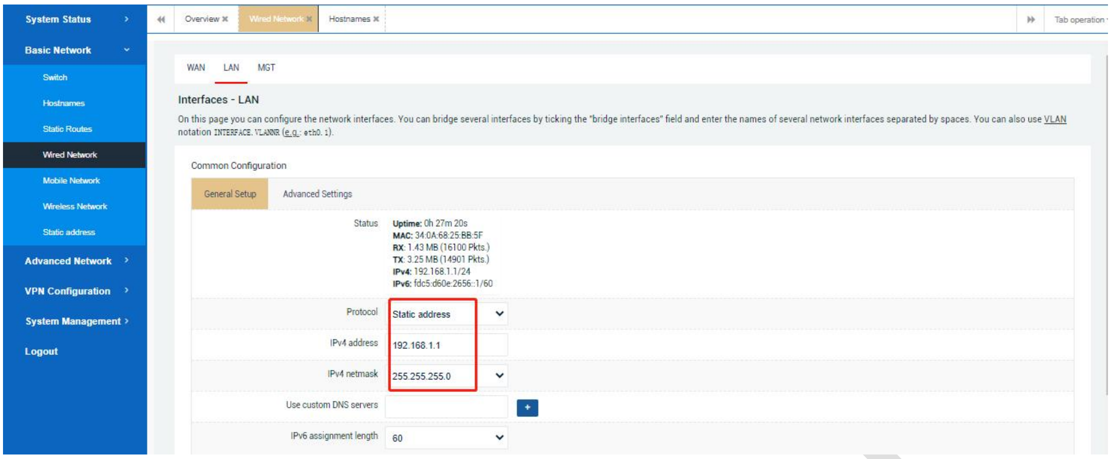
Service Name: auto
Leave empty to autodetect

4.4.2 LAN Interface

The router gateway IP address is 192.168.1.1 by default. You can also set the DHCP server configuration here.

1）**LAN address modification**

The default router LAN gateway IP address is 192.168.1.1, netmask 255.255.255.0. You can use the image below to change the IP address and netmask and save the application, and then use the new address to access the router configuration page.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: **Uptime:** 0h 27m 20s
MAC: 34:0A:68:25:BB:5F
RX: 1.43 MB (16100 Pkts.)
TX: 3.25 MB (14901 Pkts.)
IPv4: 192.168.1.1/24
IPv6: fdc5:d60e:2656::1/60

Protocol: Static address

IPv4 address: 192.168.1.1

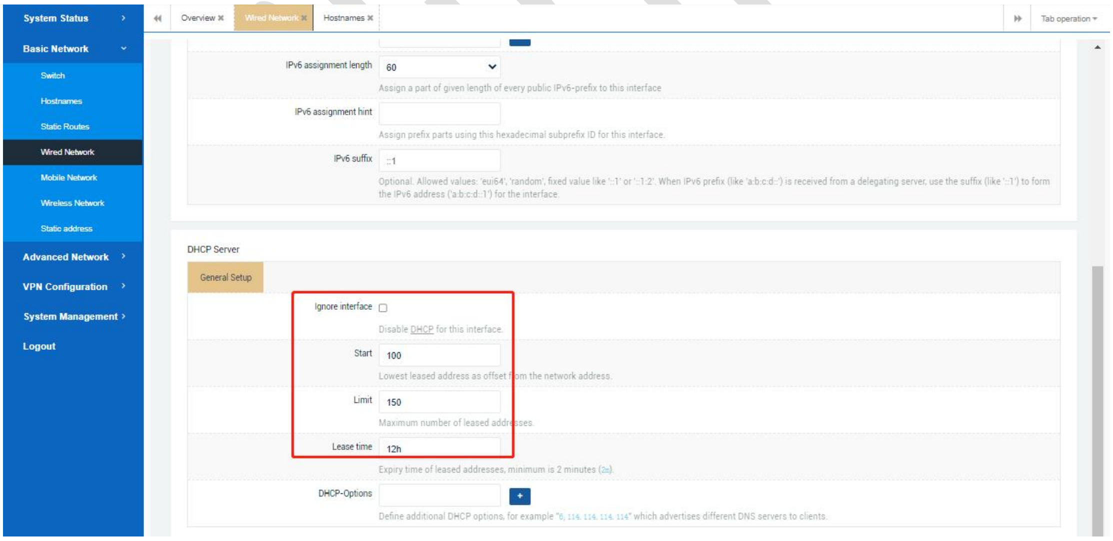
IPv4 netmask: 255.255.255.0

Use custom DNS servers:

IPv6 assignment length: 60

2）DHCP server configuration

The router DHCP server is enabled by default. You can also set the starting address of the address pool, the maximum number of addresses, the expiration date of the address lease, and the use of specific DNS server addresses. Of course, you can turn it off if you need to.



IPv6 assignment length: 60
Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint:
Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 suffix: ::1
Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.

DHCP Server

Ignore interface ☐
Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

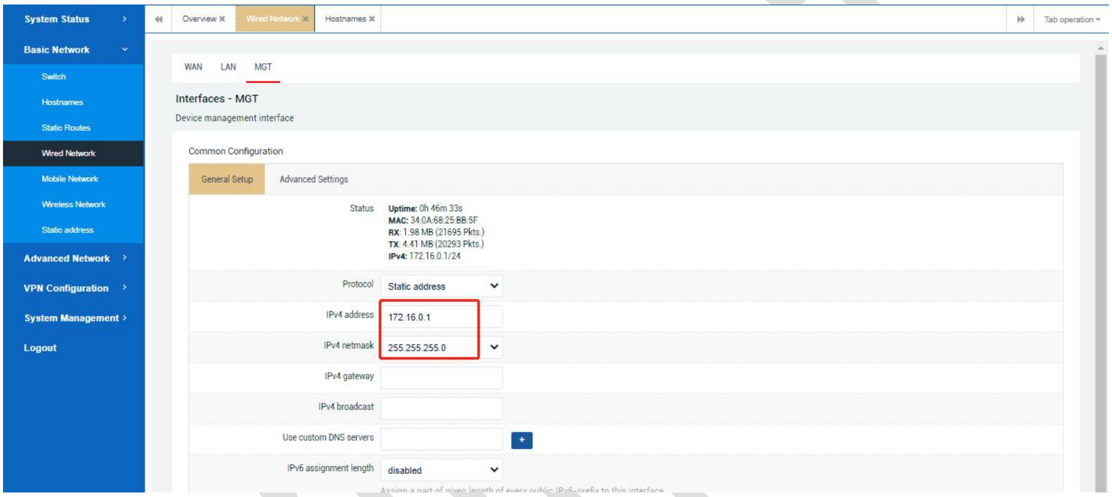
Lease time: 12h
Expiry time of leased addresses, minimum is 2 minutes (2m).

DHCP-Options:
Define additional DHCP options, for example "6,114.114.114.114" which advertises different DNS servers to clients.

4.4.3 MGT Interface

This interface is used as an alternate address (usually when the LAN port gateway address is forgotten or the current network address is used in conflict).

After connecting the computer to the router LAN port with a network cable, it is necessary to manually configure the IP with the same network segment as the MGT management address (the default is 172.16.0.1). Then enter 172.16.0.1 in the browser to log in to the router.



Interfaces - MGT

Device management interface

Common Configuration

Status: **Uptime:** 0h 46m 33s **MAC:** 34:0A:68:25:BB:5F **RX:** 1.98 MB (21695 Pkts.) **TX:** 4.41 MB (20293 Pkts.) **IPv4:** 172.16.0.1/24

Protocol	Static address
IPv4 address	172.16.0.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	disabled

Assign a part of given length of every public IPv6-prefix to this interface

4.5 Mobile network

3G/4G wireless router is a kind of wireless communication equipment for the Internet of Things, which supports international standard FDD-LTE, TDD-LTE, WCDMA (HSPA+), CDMA2000 (EVDO), TD-Scdma GSM (GPRS/EDGE)/CDMA 2G/ The 3G/4G mobile broadband network standard provides users with convenient and fast high-speed network transmission functions.

Here we mainly introduce two different dialing methods of mobile network and the configuration and use of accessing APN and VPDN network. At present, our company's 5-mode and 7-mode full Netcom 3G/4G router equipment supports all operators' network standards. Actually, it depends on the type of router modem selected by the user and the local operator's network support.

4.5.1 DHCP Dial (Single-mode dual-SIM)

By default, the device uses DHCP dialing, which is also the preferred module dialing method supported by most module manufacturers. This method has fast dialing speed and strong compatibility. This way of dialing generally does not need to manually configure the SIM card APN information. When dialing, the device will automatically recognize the different APN information of the operator (note that some IoT cards or VPDN private network cards need to manually configure the APN information, user name and password, otherwise the dialing will fail).

Specific operation: select "Basic Network" --- "Mobile Network" --- "3GWAN1" --- "Basic Settings", select "Protocol".

The main dialing parameters are described as follows:

【Protocol】: Optional DHCP client / PPP mode dial-up;

【Hostname sent when requesting DHCP】: Default is M2M;

【Pre-configured APN before CM dial-up】: Enabled by default. Common APN information will be pre-configured before CM dial-up to be compatible with common APNs of various operators.

【SIM default APN】: Enabled by default. The system's pre-configured APN information will be used before SIM dial-up. If custom APN information is required, select "Disable", then fill in the custom SIM APN information, as well as the SIM PAP/CHAP username and password.

【PIN】: SIM card PIN code; the default setting is sufficient, and generally no additional configuration is needed;

【Network type】: Default is "Auto"; you can manually select "Auto 4G/3G/2G" mode;

【SIM frequency locking】: After selecting a specific network type, you can lock the corresponding supported frequency bands to ensure dial-up and network access on the specified frequency bands.

【SIM card mode】: You can lock the device's card reading mode to SIM1, SIM2, dual-card backup, or GNSS (no card reading, only GPS usage);

【SIM smart card】: Disabled by default. If Guangdong Yika or SDK-free cards need to be used, select the corresponding option for dial-up.

【SIM operator mode】: Default is "Auto"; you can manually lock the operator to China Mobile, China Unicom, or China Telecom.

【SIM IP protocol】: Default is IPv4, dialing only to IPv4 addresses. You can manually select IPv4/IPv6 or IPv6 to dial to IPv4 and IPv6 addresses, or only to IPv6 addresses.

【APN】: Network access point required by the operator’s SIM card, generally required for IoT cards;

【PAP/CHAP username】: Username authentication required for dial-up, to be filled in according to specific circumstances;

【PAP/CHAP password】: Password authentication required for dial-up, to be filled in according to specific circumstances;

【Authentication type】: Including CHAP/PAP authentication;

【SIM card type】: Default is "Public network card"; you can manually select the card type as "Public network card" or "Private network card".

【SIM-C-IMSI】: Disabled by default; you can manually enable this function and configure C-IMSI.

【SIM card detection strategy】: You can manually select the SIM detection strategy as RSSI signal, Ping delay, or a hybrid strategy of both.

【RSSI signal】: Set the RSSI signal threshold; if the signal is lower than this value, the dial-up connection will be judged as interrupted.

【Ping delay】: Set the Ping address and Ping delay threshold; if the Ping detection delay exceeds the threshold, the dial-up connection will be judged as interrupted. Unit: milliseconds.

【Hybrid strategy】: Both RSSI signal and Ping delay are used; if either strategy condition is met, the dial-up connection will be judged as interrupted.

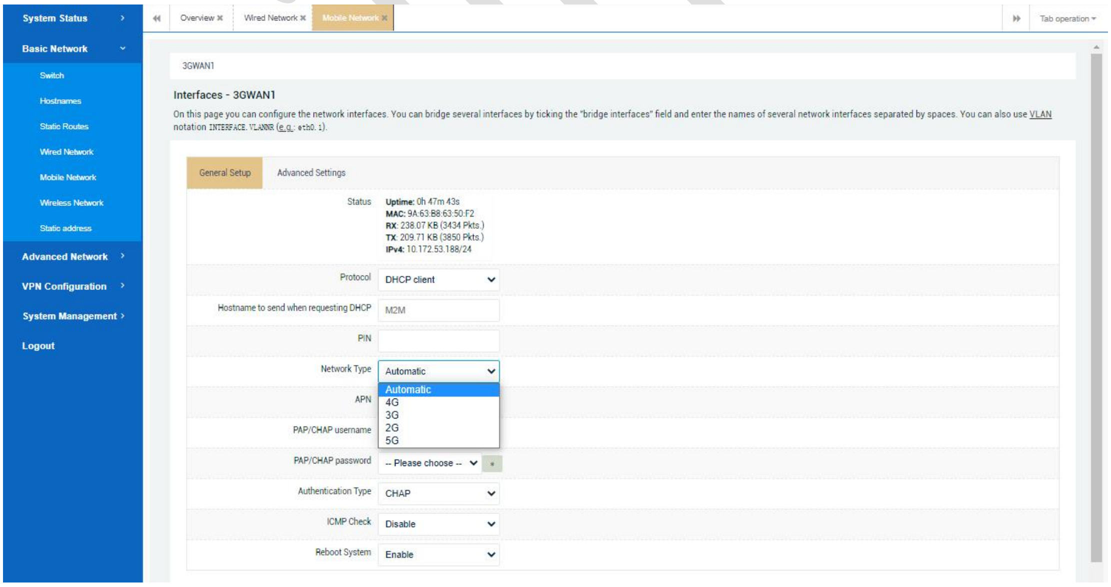
【Network disconnection restart】: Mobile network connectivity detection; disabled by default, to be configured according to specific circumstances;

【PCIe dial-up】: Disabled by default; when enabled, the SIM dial-up method will be PCIe dial-up;

4.5.1.1 Auto network (default)

The default network mode of the mobile network of the device is "automatic" mode, that is, the device will automatically identify the matching network according to the overlay network mode, signal strength, and network mode supported by the SIM card used by the surrounding operator base stations. If there is a 4G signal around, it will automatically match the 4G network first; when there is no 4G network, it will automatically recognize and switch to the 3G network; when the 3G network signal is poor or there is no network, it will automatically switch to the 2G network.

Specific operation: select "Basic Network" --- "Mobile Network" --- "3GWAN1" --- "Basic Settings", select "Network Type", as follows:



3GWAN1

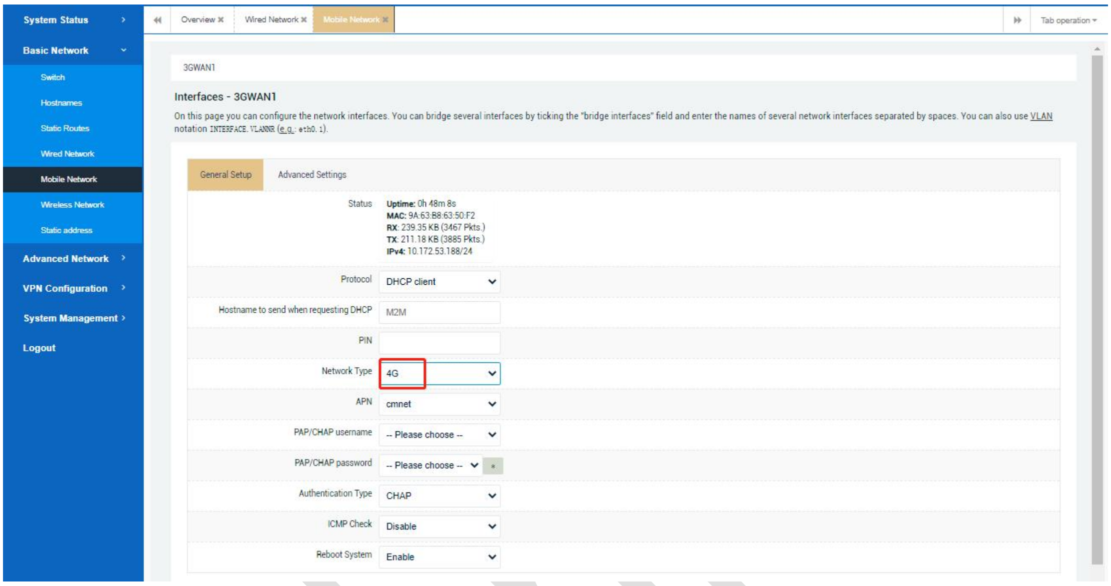
Interfaces - 3GWAN1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status	**Uptime:** 0h 47m 43s **MAC:** 9A:63:B8:63:50:F2 **RX:** 238.07 KB (3434 Pkts.) **TX:** 209.71 KB (3850 Pkts.) **IPv4:** 10.172.53.188/24
Protocol	DHCP client
Hostname to send when requesting DHCP	M2M
PIN	
Network Type	Automatic Automatic 4G 3G 2G 5G
APN	
PAP/CHAP username	
PAP/CHAP password	-- Please choose --
Authentication Type	CHAP
ICMP Check	Disable
Reboot System	Enable

4.5.1.2 Lock the network (4G/3G/2G)

Specific operation: select "Basic Network" --- "Mobile Network" --- "Basic Settings", change the "Network Type" to 4G" mode, and save the dial-up networking information ("System Status" --- "Overview" "---"3G WAN1 (mobile network) status"). As follows:

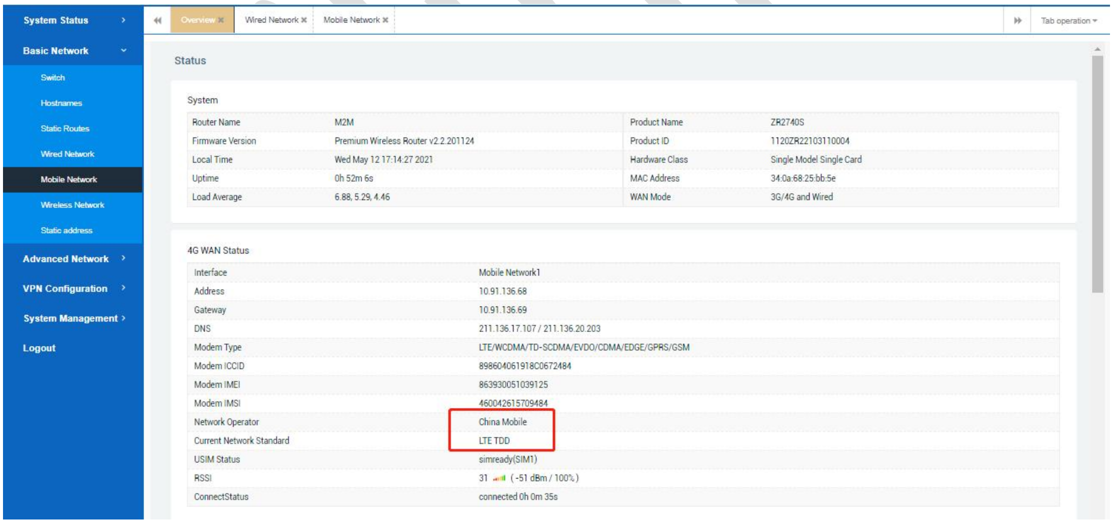


3GWAN1

Interfaces - 3GWAN1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status	**Uptime:** 0h 48m 8s **MAC:** 9A:63:B8:63:50:F2 **RX:** 239.35 KB (3467 Pkts.) **TX:** 211.18 KB (3885 Pkts.) **IPv4:** 10.172.53.188/24
Protocol	DHCP client
Hostname to send when requesting DHCP	M2M
PIN	
Network Type	4G
APN	cmnet
PAP/CHAP username	-- Please choose --
PAP/CHAP password	-- Please choose --
Authentication Type	CHAP
ICMP Check	Disable
Reboot System	Enable



Status

System

Router Name	M2M	Product Name	ZR2740S
Firmware Version	Premium Wireless Router v2.2.201124	Product ID	1120ZR22103110004
Local Time	Wed May 12 17:14:27 2021	Hardware Class	Single Model Single Card
Uptime	0h 52m 6s	MAC Address	34:0a:68:25:bb:5e
Load Average	6.88, 5.29, 4.46	WAN Mode	3G/4G and Wired

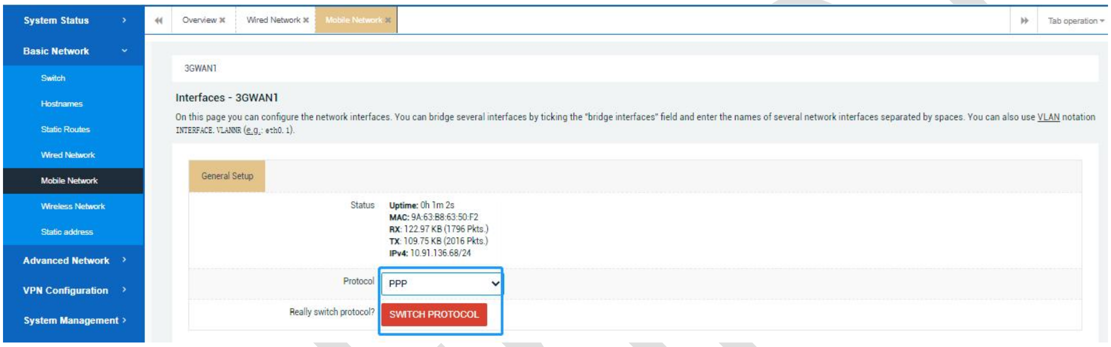
4G WAN Status

Interface	Mobile Network1
Address	10.91.136.68
Gateway	10.91.136.69
DNS	211.136.17.107 / 211.136.20.203
Modem Type	LTE/WCDMA/TD-SCDMA/EVDO/CDMA/EDGE/GPRS/GSM
Modem ICCID	898604061918C0672484
Modem IMEI	863930051039125
Modem IMSI	460042615709484
Network Operator	China Mobile
Current Network Standard	LTE TDD
USIM Status	simready(SIM1)
RSSI	31 (-51 dBm / 100%)
ConnectStatus	connected 0h 0m 35s

4.5.2 PPP Dial

The routing device itself also supports PPP dial-up mode, you can try to switch to use this dial-up mode. (This way of dialing generally does not need to manually configure the SIM card APN information. The device will automatically recognize the different APN information of the three major operators when dialing. Dialing failed).

Specific operation: select "Basic Network" --- "Mobile Network" --- "3GWAN1" --- "Basic Settings", select the protocol type "PPP" and confirm the replacement protocol. as follows:



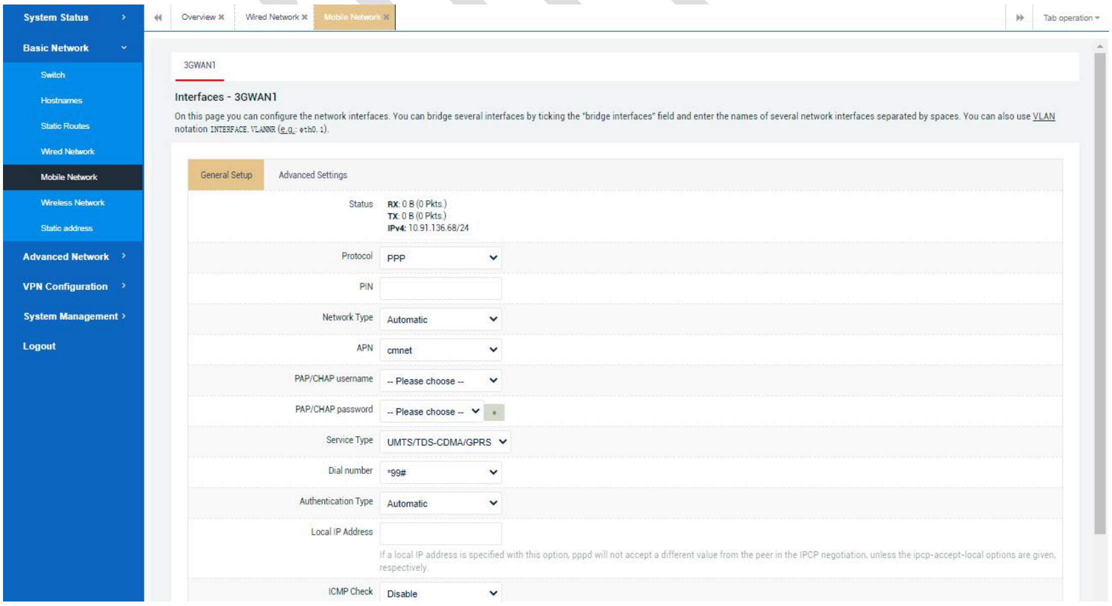
Interfaces - 3GWAN1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Status: **Uptime:** 0h 1m 2s
MAC: 9A:63:B8:63:50:F2
RX: 122.97 KB (1796 Pkts.)
TX: 109.75 KB (2016 Pkts.)
IPv4: 10.91.136.68/24

Protocol: PPP

Really switch protocol?



Interfaces - 3GWAN1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Status	**RX:** 0 B (0 Pkts.) **TX:** 0 B (0 Pkts.) **IPv4:** 10.91.136.68/24
Protocol	PPP
PIN	
Network Type	Automatic
APN	cmnet
PAP/CHAP username	-- Please choose --
PAP/CHAP password	-- Please choose --
Service Type	UMTS/TDS-CDMA/GPRS
Dial number	*99#
Authentication Type	Automatic
Local IP Address	 If a local IP address is specified with this option, pppd will not accept a different value from the peer in the IPCP negotiation, unless the ipcp-accept-local options are given, respectively.
ICMP Check	Disable

4.5.2.1 Automatic network

See for details 4.5.1.1

4.5.2.1 Lock the network (4G/3G/2G)

See for details 4.5.1.2

Notice:

1) For the use of APN IoT card or VPDN dedicated network card, please fill in the APN access point information and PAP/CHAP user name and password correctly, otherwise the system cannot complete dial-up networking.

2) For the VPDN private network card scenario, it is generally not allowed to access the external network. Please log in to the device page and find the "High

Level Network"---"Network Monitoring", turn off this function or modify the default ping address to be a valid and connectable other private network address, otherwise it will cause the device to periodically restart about 10 minutes.

4.6 Wireless Network

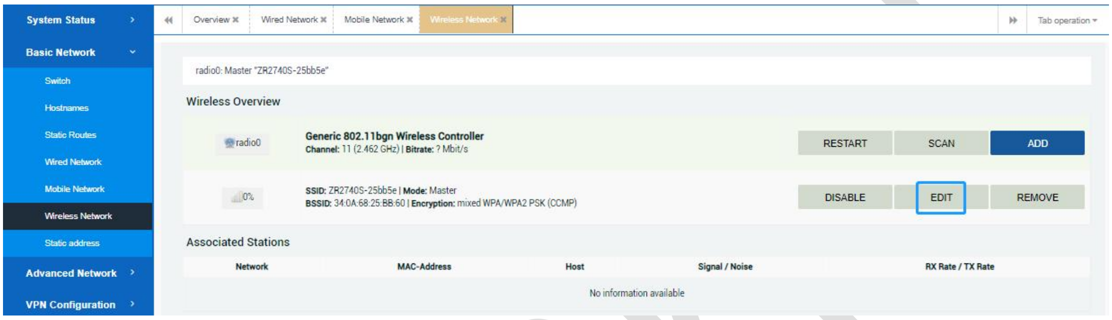
The following mainly introduces two commonly used wireless working modes.

Access point AP mode: This working mode is to use the router as a wireless transmitting point, which can provide mobile phones, laptops or other wireless terminals to connect to the Internet through wireless means (Wi-Fi has no password by default before V2.1, and it is strongly recommended for the safety of the device. Please set the WiFi password when the customer uses the device; after the V2.1 version, the default WiFi password is admin123(Factory pre-configuration can be customized according to user requirements.)).Specific operations such as 4.6.1。

Client mode: This mode refers to the use of the routing device as a wireless client, which can enable itself to have networking capabilities by searching and joining other wireless hotspots around it, that is, wireless bridging. Specific operations such as 4.6.2。

4.6.1 AP mode

Specific operation: select "Basic Network" --- "Wireless Network" --- "Wireless Overview" to check and confirm. as follows:



radio0: Master "ZR2740S-25bb5e"

Wireless Overview

radio0 Generic 802.11bgn Wireless Controller
Channel: 11 (2.462 GHz) | Bitrate: ? Mbit/s

0% SSID: ZR2740S-25bb5e | Mode: Master
BSSID: 34:0A:68:25:BB:60 | Encryption: mixed WPA/WPA2 PSK (CCMP)

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

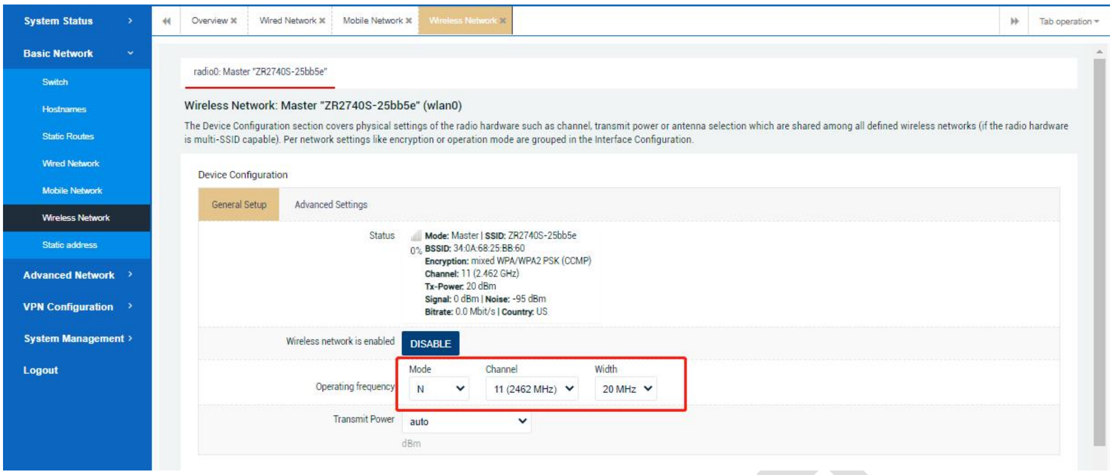
Click the Add button to add a WiFi interface, which can be used to configure the access point AP or client mode.

4.6.1.1 Device Configuration

Click the "Edit" button on the right of "Wireless Profile" and enter "Device Configuration" to configure the basic and advanced settings of wireless WiFi.

4.6.1.1.1 Basic Settings

Through the "Basic Settings" option, you can configure the wireless network (WiFi) switch, wireless channel selection and radio power adjustment, as follows;



radio0: Master "ZR2740S-25bb5e"

Wireless Network: Master "ZR2740S-25bb5e" (wlan0)

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

Device Configuration

Status 0% **Mode:** Master | **SSID:** ZR2740S-25bb5e
BSSID: 34:0A:68:25:BB:60
Encryption: mixed WPA/WPA2 PSK (CCMP)
Channel: 11 (2.462 GHz)
Tx-Power: 20 dBm
Signal: 0 dBm | **Noise:** -95 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

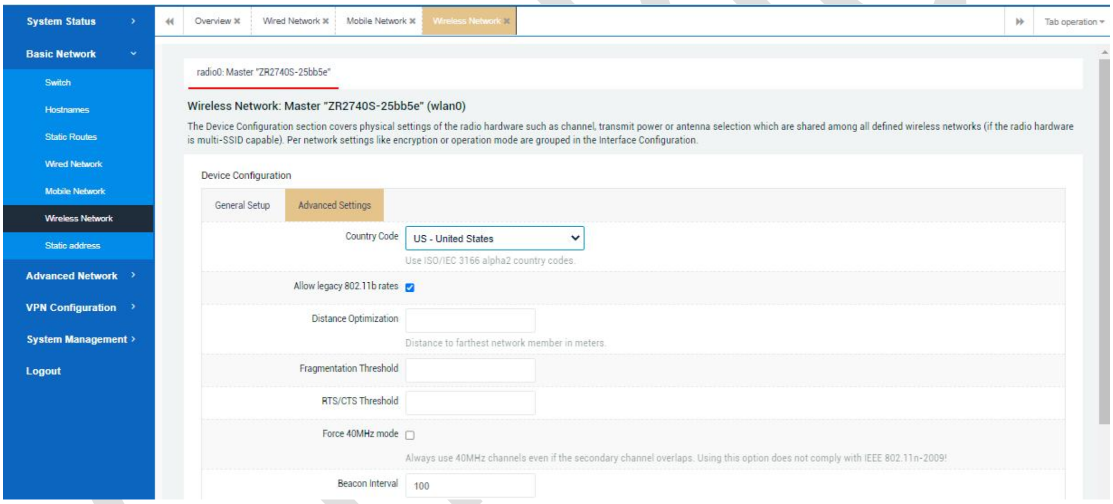
Wireless network is enabled

Operating frequency: Mode N; Channel 11 (2462 MHz); Width 20 MHz

Transmit Power: auto
dBm

4.6.1.1.2 Advanced Settings

Through the "advanced settings", you can set the country code, distance optimization and other settings. as follows:



radio0: Master "ZR2740S-25bb5e"

Wireless Network: Master "ZR2740S-25bb5e" (wlan0)

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

Device Configuration

Country Code: US - United States
Use ISO/IEC 3166 alpha2 country codes.

Allow legacy 802.11b rates ☑

Distance Optimization:
Distance to farthest network member in meters.

Fragmentation Threshold:

RTS/CTS Threshold:

Force 40MHz mode ☐
Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

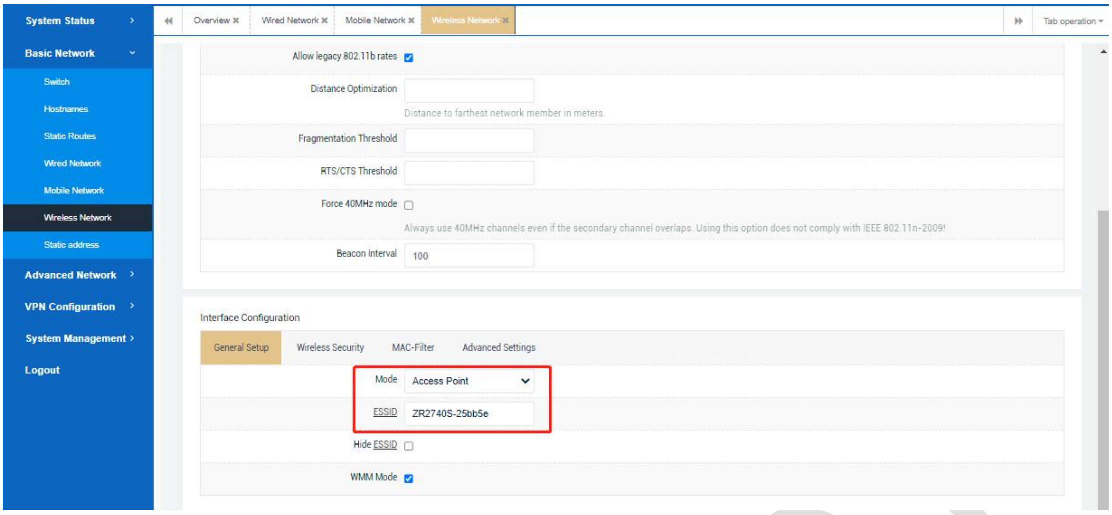
Beacon Interval: 100

4.6.1.2 Interface Configuration

Click the "Edit" button on the right of the wireless profile and then enter the "Interface Configuration".

4.6.1.2.1 Basic Settings

Through the "Basic Settings" option, you can set the WiFi mode, wireless ESSID (hotspot name), working mode, whether to hide the ESSID name, and enable WMM mode, etc. as follows:



Allow legacy 802.11b rates ☑

Distance Optimization

Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Force 40MHz mode □

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

Beacon Interval: 100

Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Mode: Access Point

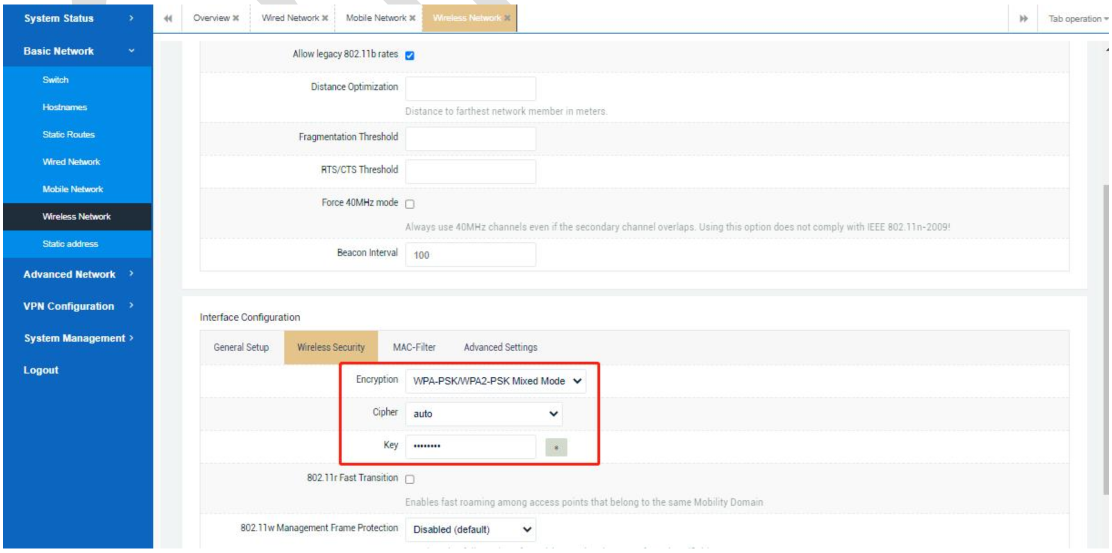
ESSID: ZR2740S-25bb5e

Hide ESSID □

WMM Mode ☑

4.6.1.2.1 WiFi Password Setting

Through the "Wireless Security" option, you can set the wireless encryption method (the new version defaults to WPA-PSK/WPA2 Mixed Mode mixed encryption), algorithm and secret key settings, etc. (the password is at least 8 digits, the default is Admin@123), and the rest of the settings are generally default That's it.



Allow legacy 802.11b rates ☑

Distance Optimization

Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Force 40MHz mode □

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

Beacon Interval: 100

Interface Configuration

General Setup | Wireless Security | MAC-Filter | Advanced Settings

Encryption: WPA-PSK/WPA2-PSK Mixed Mode

Cipher: auto

Key: ••••••••

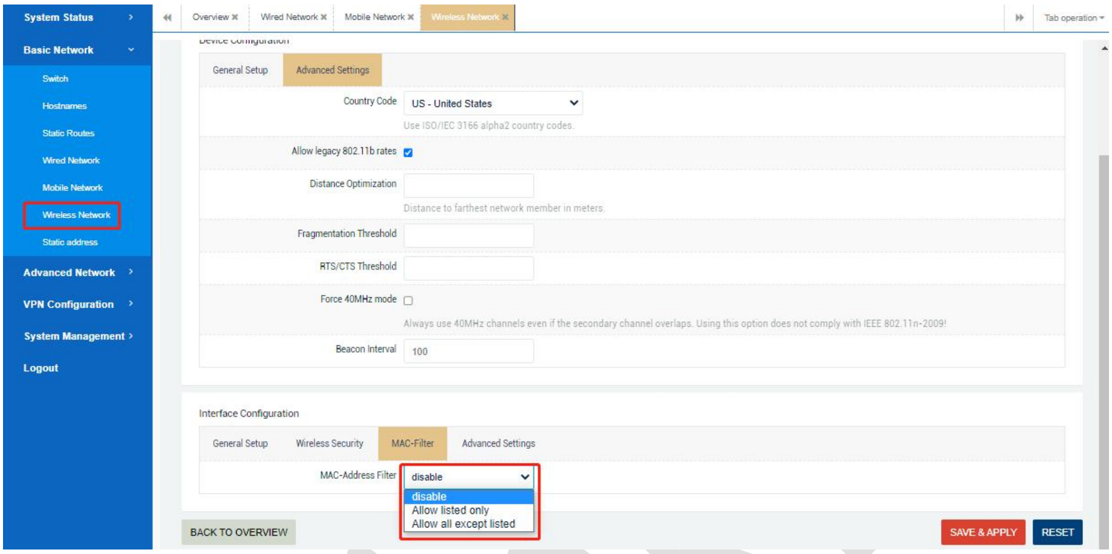
802.11r Fast Transition □

Enables fast roaming among access points that belong to the same Mobility Domain

802.11w Management Frame Protection: Disabled (default)

4.6.1.2.3 Black and white list settings

Through the "MAC filtering" option, you can set whether to enable MAC address filtering (disabled by default), "allow only in the list (whitelist: accessible)" or "only allow outside the list (blacklist: no access)". as follows:



Country Code: US - United States

Use ISO/IEC 3166 alpha2 country codes.

Allow legacy 802.11b rates ☑

Distance Optimization

Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Force 40MHz mode ☐

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

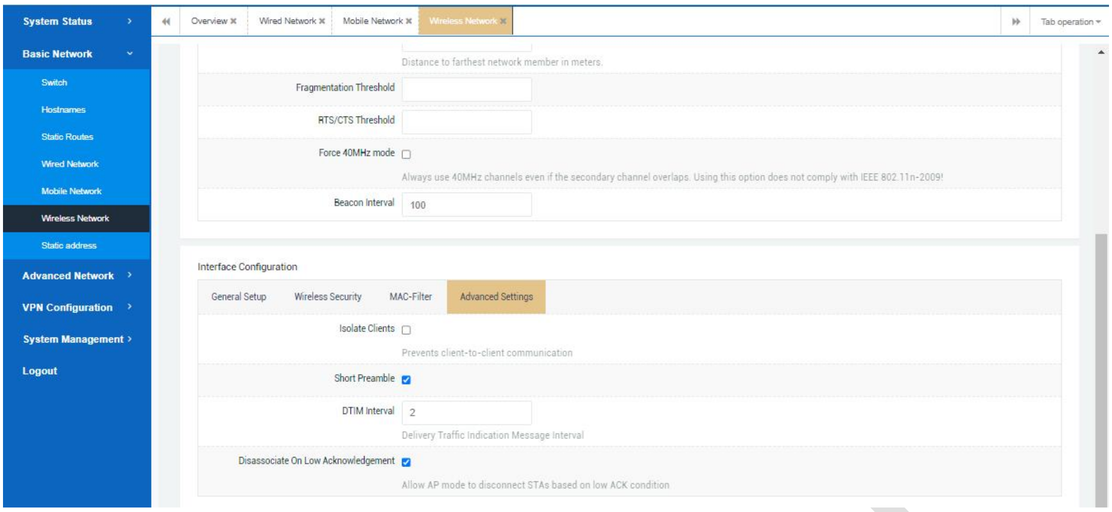
Beacon Interval: 100

MAC-Address Filter: disable

disable
Allow listed only
Allow all except listed

4.6.1.2.4 Advanced Settings

Through the "Advanced Settings" option, you can set whether to isolate the client, etc., as follows:



Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Force 40MHz mode □

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

Beacon Interval: 100

Interface Configuration

Isolate Clients □

Prevents client-to-client communication

Short Preamble ☑

DTIM Interval: 2

Delivery Traffic Indication Message Interval

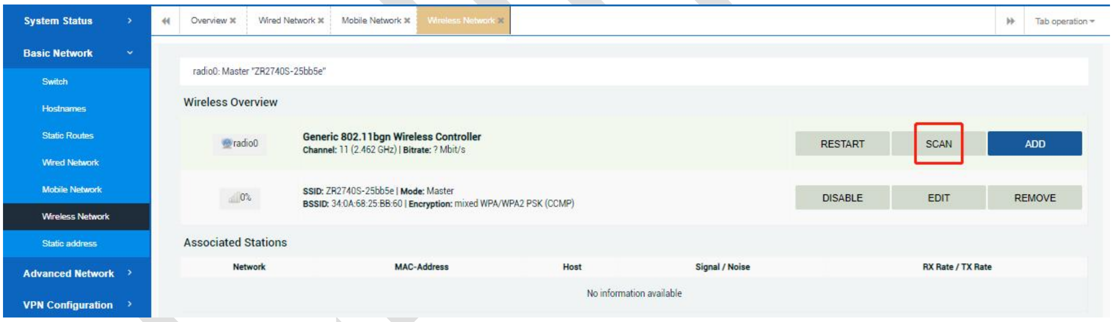
Disassociate On Low Acknowledgement ☑

Allow AP mode to disconnect STAs based on low ACK condition

4.6.2 Client Mode

You can scan to join other wireless hotspots and set the method of obtaining an IP address (DHCP (default) or static address). as follows:

1) Specific operation: Select "Basic Network" --- "Wireless Network" --- "Wireless Overview", click the "Scan" button on the right to start searching for other wireless hotspots around, as follows:



radio0: Master "ZR2740S-25bb5e"

Wireless Overview

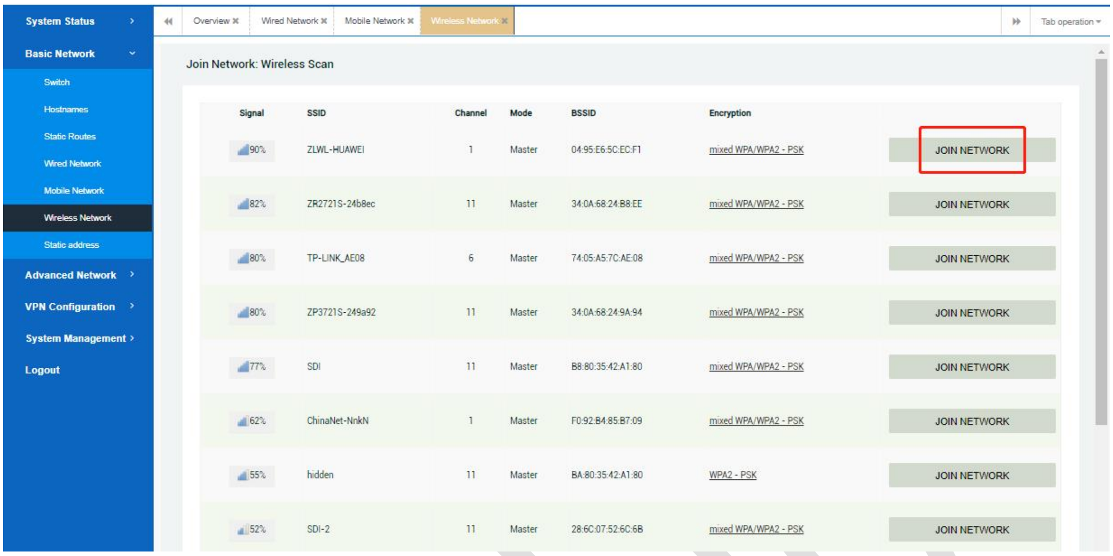
radio0 Generic 802.11bgn Wireless Controller
Channel: 11 (2.462 GHz) | Bitrate: ? Mbit/s

0% SSID: ZR2740S-25bb5e | Mode: Master
BSSID: 34:0A:68:25:BB:60 | Encryption: mixed WPA/WPA2 PSK (CCMP)

Associated Stations

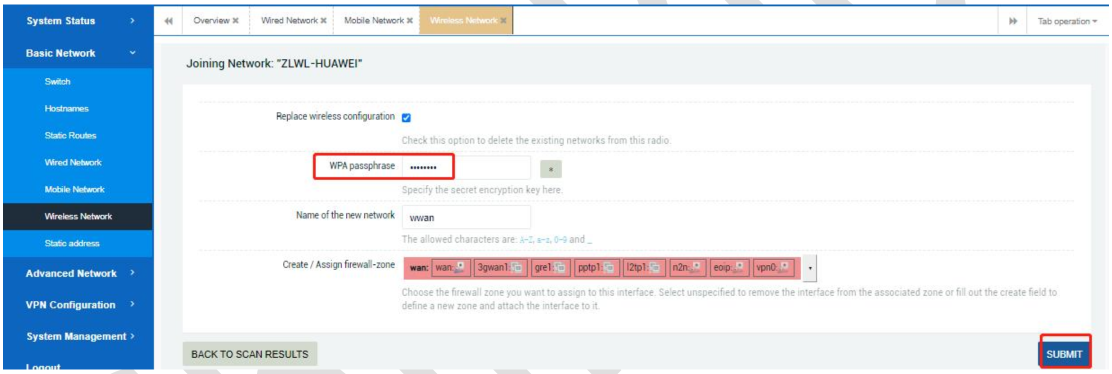
Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

2）Select the wireless hotspot that needs to be connected, click "join network", check "reset wireless configuration" and set the password of the wireless hotspot and the name of the new network (the default is sufficient), and finally click "submit", the page will jump Go to the "Interface Configuration" --- "Basic Settings" page (you can set the protocol (wireless IP address acquisition method) to DHCP (default) or static address method), the rest of the settings can be defaulted, and finally click "Save Application", as follows:



Join Network: Wireless Scan

Signal	SSID	Channel	Mode	BSSID	Encryption	
90%	ZLWL-HUAWEI	1	Master	04:95:E6:5C:EC:F1	mixed WPA/WPA2 - PSK	JOIN NETWORK
82%	ZR2721S-24b8ec	11	Master	34:0A:68:24:B8:EE	mixed WPA/WPA2 - PSK	JOIN NETWORK
80%	TP-LINK_AE08	6	Master	74:05:A5:7C:AE:08	mixed WPA/WPA2 - PSK	JOIN NETWORK
80%	ZP3721S-249a92	11	Master	34:0A:68:24:9A:94	mixed WPA/WPA2 - PSK	JOIN NETWORK
77%	SDI	11	Master	B8:80:35:42:A1:80	mixed WPA/WPA2 - PSK	JOIN NETWORK
62%	ChinaNet-NnkN	1	Master	F0:92:B4:85:B7:09	mixed WPA/WPA2 - PSK	JOIN NETWORK
55%	hidden	11	Master	BA:80:35:42:A1:80	WPA2 - PSK	JOIN NETWORK
52%	SDI-2	11	Master	28:6C:07:52:6C:6B	mixed WPA/WPA2 - PSK	JOIN NETWORK



Joining Network: "ZLWL-HUAWEI"

Replace wireless configuration ☑

Check this option to delete the existing networks from this radio.

WPA passphrase ••••••••

Specify the secret encryption key here.

Name of the new network: wwan

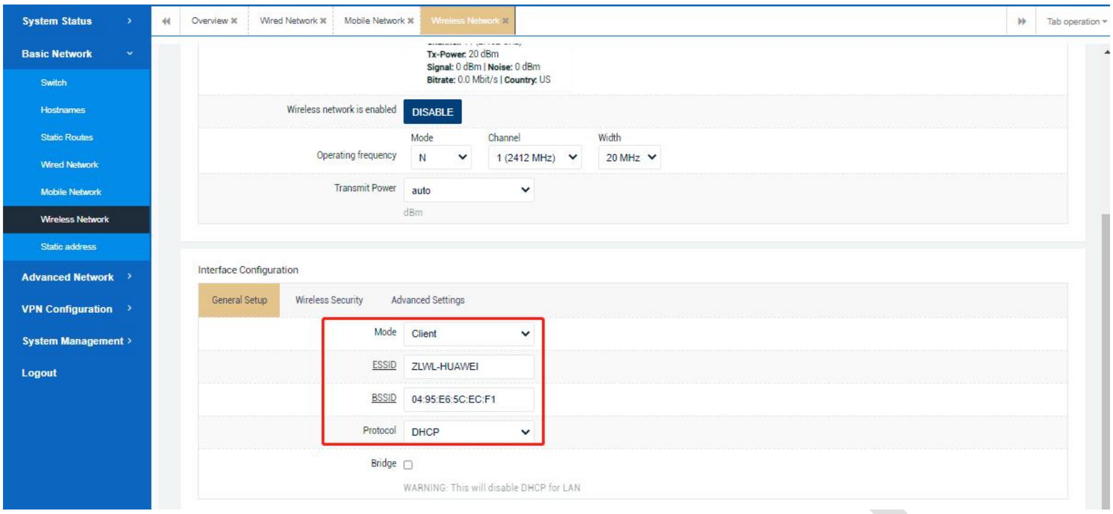
The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone: wan

Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it.

4.6.2.1 Client DHCP (default)

After filling in the password and submitting, jump to the WiFi interface configuration page, "Interface Configuration" --- "Basic Settings", the "Protocol" defaults to "DHCP", and then save the application.



Tx-Power: 20 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

Wireless network is enabled

Operating frequency: Mode N; Channel 1 (2412 MHz); Width 20 MHz

Transmit Power: auto dBm

Mode: Client

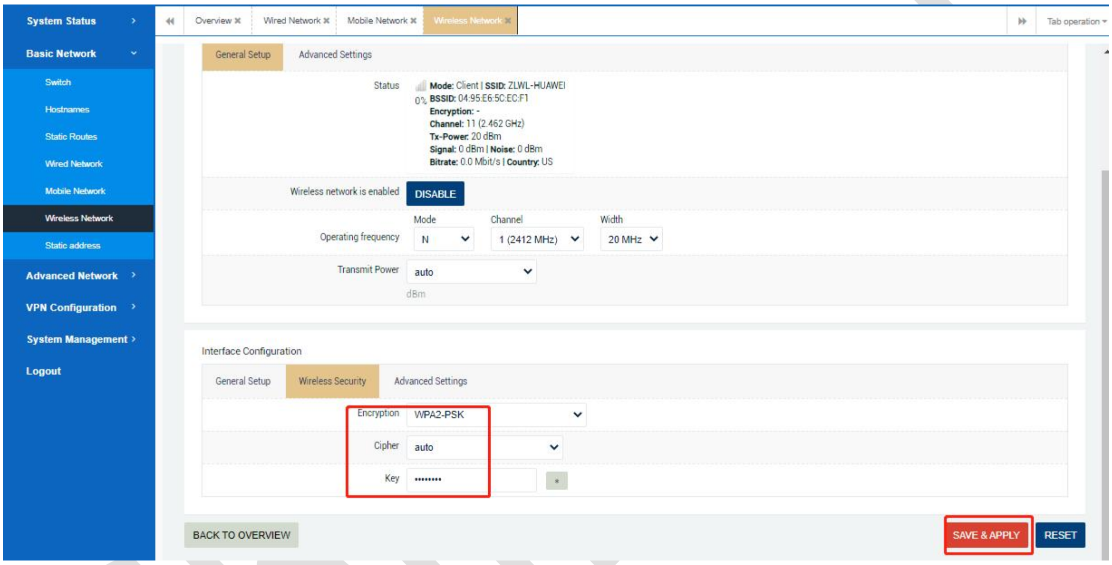
ESSID: ZLWL-HUAWEI

BSSID: 04:95:E6:5C:EC:F1

Protocol: DHCP

Bridge ☐

WARNING: This will disable DHCP for LAN



Status: 0% **Mode:** Client | **SSID:** ZLWL-HUAWEI
BSSID: 04:95:E6:5C:EC:F1
Encryption: -
Channel: 11 (2.462 GHz)
Tx-Power: 20 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

Wireless network is enabled

Operating frequency: Mode N; Channel 1 (2412 MHz); Width 20 MHz

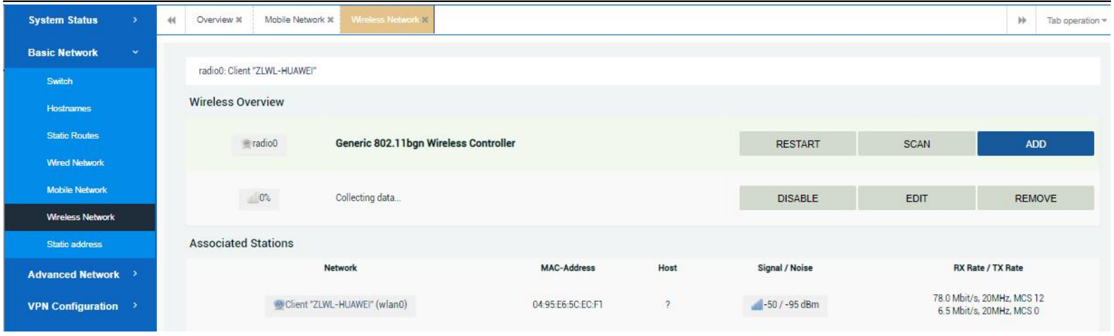
Transmit Power: auto dBm

Encryption: WPA2-PSK

Cipher: auto

Key: ••••••••

After clicking to save the application, select "System Status" --- "Overview" --- "Wireless" to check that the wireless client mode has been successfully connected at this time, as follows:



radio0: Client "ZLWL-HUAWEI"

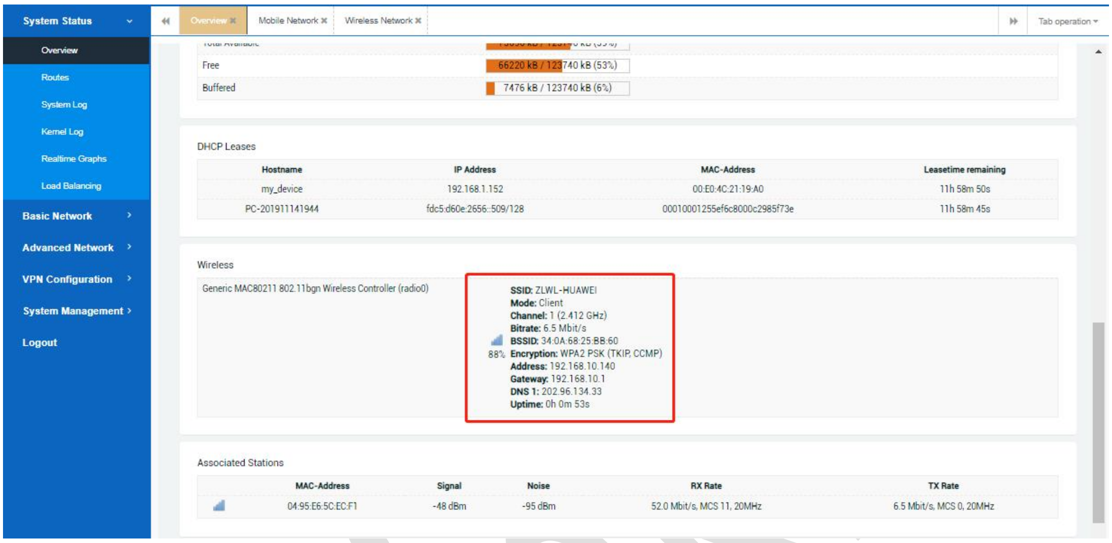
Wireless Overview

radio0 Generic 802.11bgn Wireless Controller

0% Collecting data...

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
Client "ZLWL-HUAWEI" (wlan0)	04:95:E6:5C:EC:F1	?	-50 / -95 dBm	78.0 Mbit/s, 20MHz, MCS 12 6.5 Mbit/s, 20MHz, MCS 0



Free	66220 kB / 123740 kB (53%)
Buffered	7476 kB / 123740 kB (6%)

DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
my_device	192.168.1.152	00:E0:4C:21:19:A0	11h 58m 50s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 58m 45s

Wireless

Generic MAC80211 802.11bgn Wireless Controller (radio0)

88%

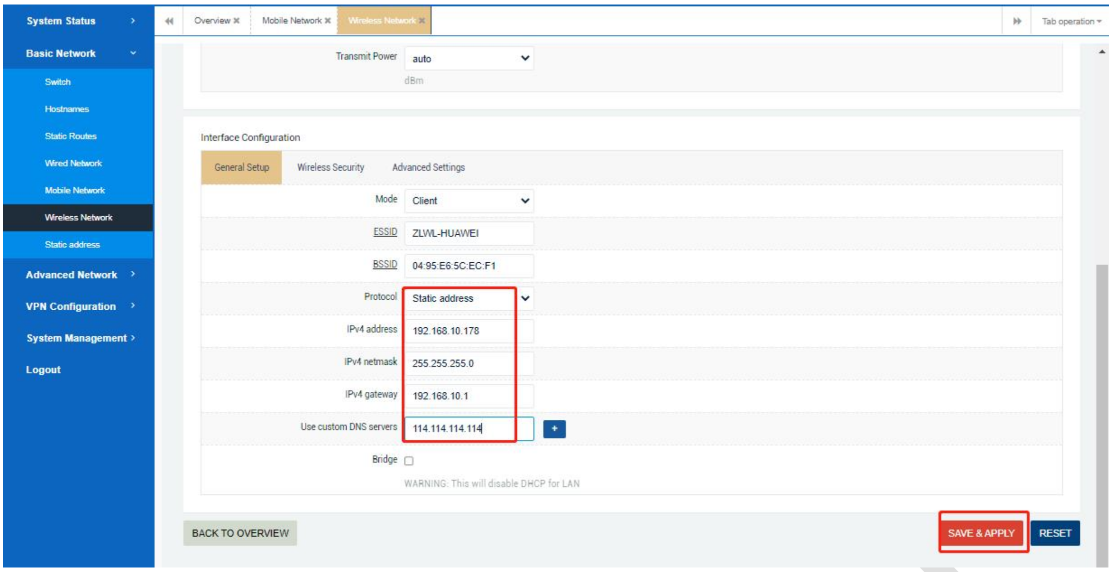
SSID: ZLWL-HUAWEI
Mode: Client
Channel: 1 (2.412 GHz)
Bitrate: 6.5 Mbit/s
BSSID: 34:0A:68:25:BB:60
Encryption: WPA2 PSK (TKIP, CCMP)
Address: 192.168.10.140
Gateway: 192.168.10.1
DNS 1: 202.96.134.33
Uptime: 0h 0m 53s

Associated Stations

	MAC-Address	Signal	Noise	RX Rate	TX Rate
	04:95:E6:5C:EC:F1	-48 dBm	-95 dBm	52.0 Mbit/s, MCS 11, 20MHz	6.5 Mbit/s, MCS 0, 20MHz

4.6.2.1 Client static address

You can scan to join WiFi, fill in the password and submit it, and then jump to the WiFi interface configuration page. In "Interface Configuration" --- "Basic Settings", select "Protocol" as "Static Address", and then enter the IP address, subnet mask, Save the application after the gateway and DNS server.

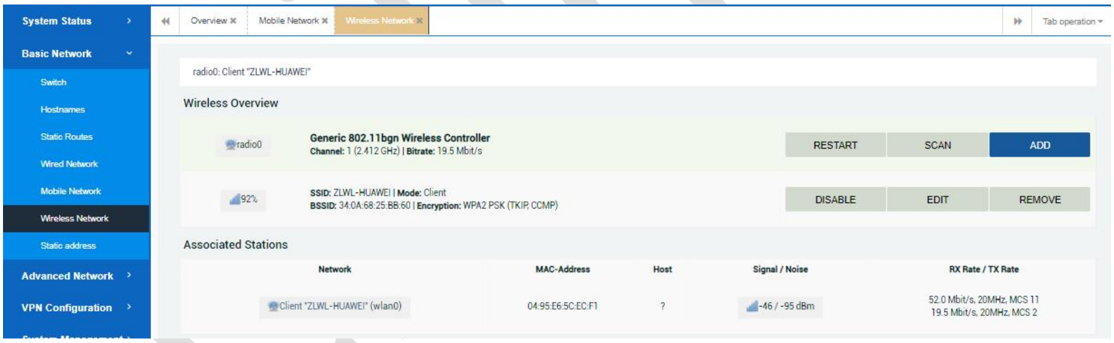


Transmit Power: auto
dBm

Interface Configuration

Mode: Client
ESSID: ZLWL-HUAWEI
BSSID: 04:95:E6:5C:EC:F1
Protocol: Static address
IPv4 address: 192.168.10.178
IPv4 netmask: 255.255.255.0
IPv4 gateway: 192.168.10.1
Use custom DNS servers: 114.114.114.114
Bridge: □
WARNING: This will disable DHCP for LAN

If you used "Protocol" as "DHCP" when scanning and joining before, now you need to change it to a static IP address. Specific operation: Select "Basic Network" --- "Wireless Network" --- "Wireless Profile", click the "Edit" button on the right, enter the interface configuration and select "Protocol" to change to "Static Address". After the configuration is as above:



radio0: Client "ZLWL-HUAWEI"

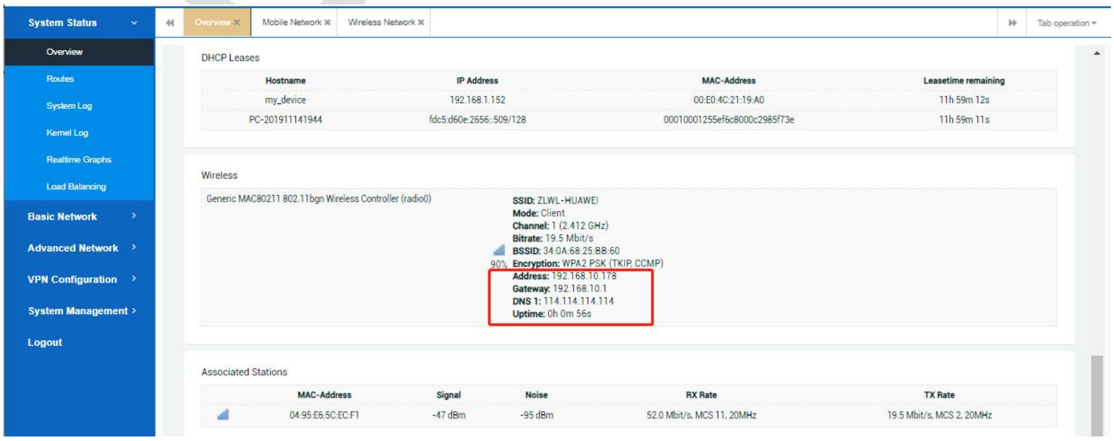
Wireless Overview

radio0 — **Generic 802.11bgn Wireless Controller**
Channel: 1 (2.412 GHz) | **Bitrate:** 19.5 Mbit/s

92% — **SSID:** ZLWL-HUAWEI | **Mode:** Client
BSSID: 34:0A:68:25:BB:60 | **Encryption:** WPA2 PSK (TKIP, CCMP)

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
Client "ZLWL-HUAWEI" (wlan0)	04:95:E6:5C:EC:F1	?	-46 / -95 dBm	52.0 Mbit/s, 20MHz, MCS 11 19.5 Mbit/s, 20MHz, MCS 2



DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
my_device	192.168.1.152	00:E0:4C:21:19:A0	11h 59m 12s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 59m 11s

Wireless

Generic MAC80211 802.11bgn Wireless Controller (radio0)

90%
SSID: ZLWL-HUAWEI
Mode: Client
Channel: 1 (2.412 GHz)
Bitrate: 19.5 Mbit/s
BSSID: 34:0A:68:25:BB:60
Encryption: WPA2 PSK (TKIP, CCMP)
Address: 192.168.10.178
Gateway: 192.168.10.1
DNS 1: 114.114.114.114
Uptime: 0h 0m 56s

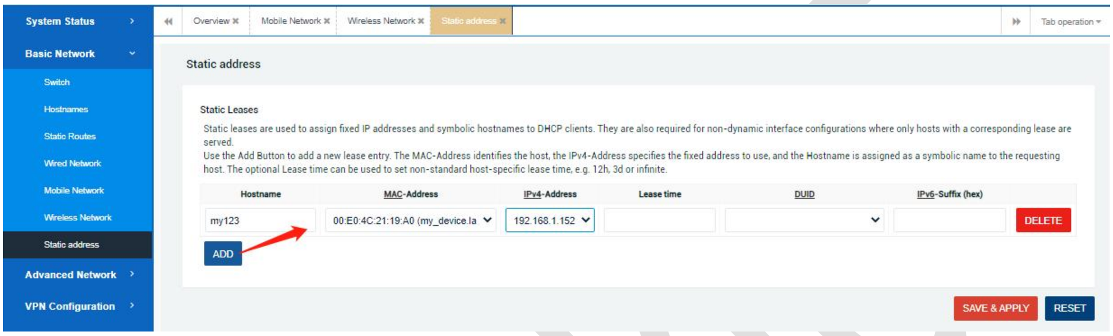
Associated Stations

	MAC-Address	Signal	Noise	RX Rate	TX Rate
	04:95:E6:5C:EC:F1	-47 dBm	-95 dBm	52.0 Mbit/s, MCS 11, 20MHz	19.5 Mbit/s, MCS 2, 20MHz

4.7 Static address

The static address function is used to assign a fixed IPv4 address to a host with a specified MAC address, that is, the host device MAC-IP binding, and it can also customize the device host name.

Select "Basic Network" --- "Static Address" and click the "Add" button to set the host name, MAC address, IPv4 address, lease period, etc., as follows:



Static address

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

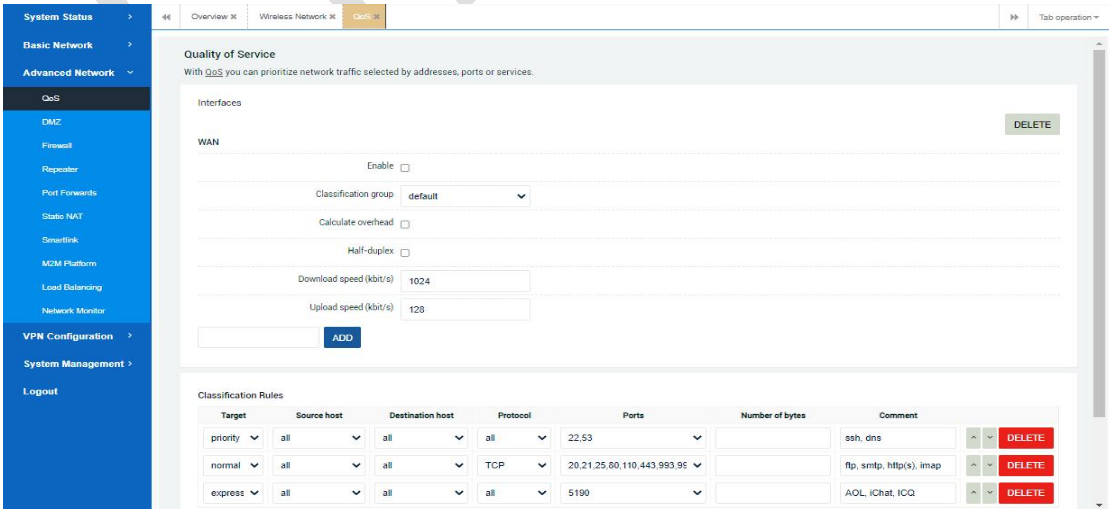
Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies the fixed address to use, and the Hostname is assigned as a symbolic name to the requesting host. The optional Lease time can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)	
my123	00:E0:4C:21:19:A0 (my_device.la	192.168.1.152				DELETE

5.Advanced Network

5.1 QoS

Here you can configure some specific QoS service quality rules, such as limiting the rate of each interface of the device or sorting different traffic data packets.



Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

WAN

Enable □

Classification group: default

Calculate overhead □

Half-duplex □

Download speed (kbit/s): 1024

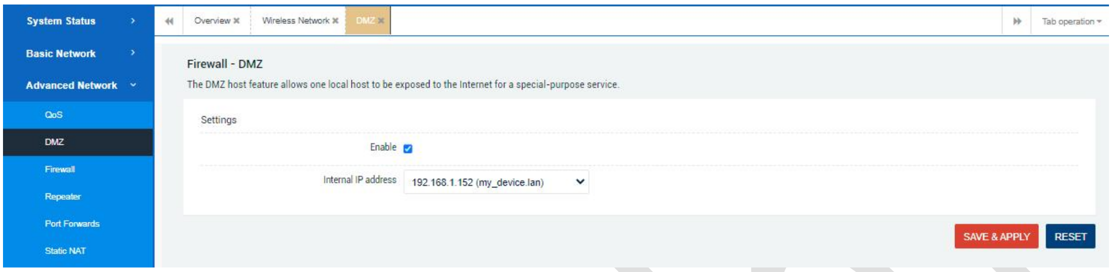
Upload speed (kbit/s): 128

Classification Rules

Target	Source host	Destination host	Protocol	Ports	Number of bytes	Comment	
priority	all	all	all	22,53		ssh, dns	DELETE
normal	all	all	TCP	20,21,25,80,110,443,993,9!		ftp, smtp, http(s), imap	DELETE
express	all	all	all	5190		AOL, iChat, ICQ	DELETE

5.2 DMZ

The network attributes used for the WAN interface of the routing device (such as with a public IP address) forward the full port of the external network to the internal network host behind the firewall, so that the internal service resources of the network can be accessed quickly and efficiently. Examples are as follows:



Firewall - DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service.

Settings

Enable ☑

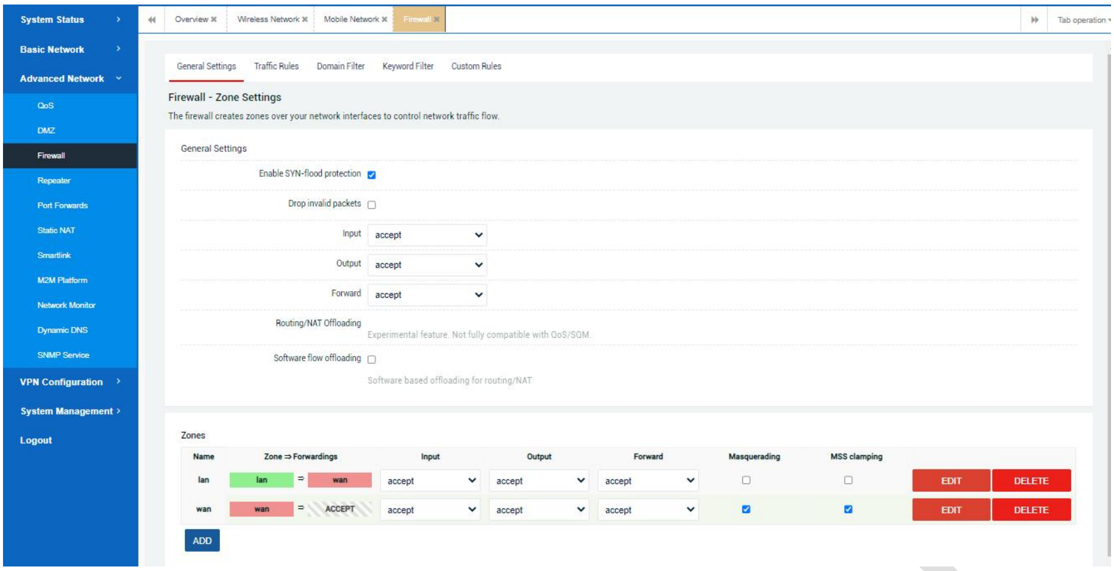
Internal IP address 192.168.1.152 (my_device.lan)

5.3 Firewall

The firewall configuration is used to set certain rules for the inbound and outbound traffic of the routing system so as to effectively protect the security of the system.

5.3.1 Basic Settings

It is mainly used to set the entry and exit data access rules of different interface areas of the routing system and set related SYN-flood defense, etc. It is generally defaulted and does not need to be changed.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection	☑
Drop invalid packets	□
Input	accept
Output	accept
Forward	accept
Routing/NAT Offloading	Experimental feature. Not fully compatible with QoS/SQM.
Software flow offloading	□ Software based offloading for routing/NAT

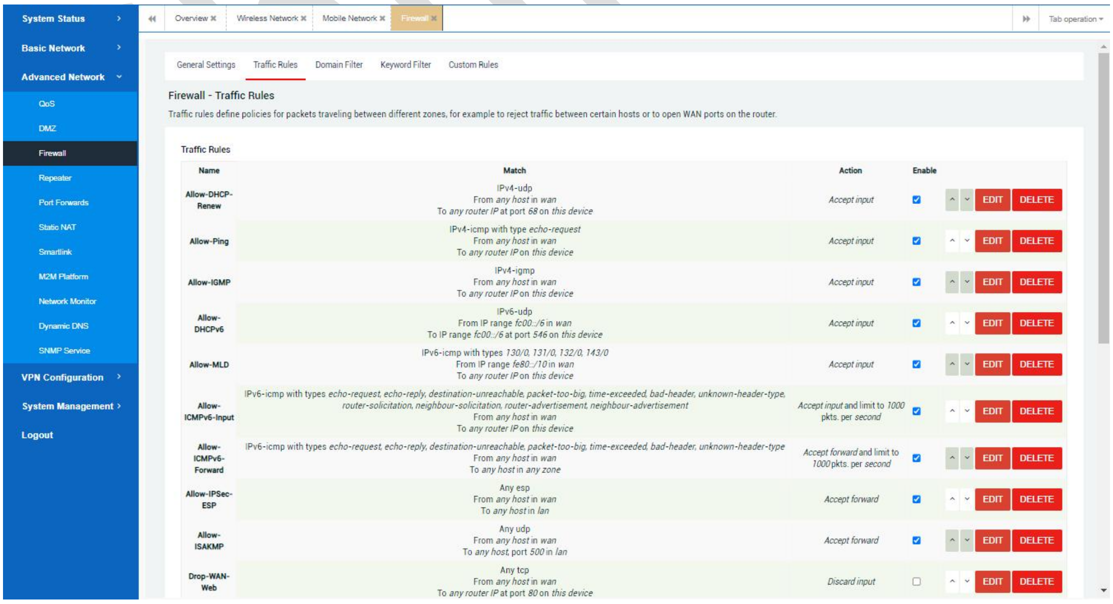
Zones

Name	Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan	lan ⇒ wan	accept	accept	accept	□	□	EDIT	DELETE
wan	wan ⇒ ACCEPT	accept	accept	accept	☑	☑	EDIT	DELETE

ADD

5.3.2 Communication rules

This is mainly used to define data packet transmission strategies between different areas, such as allowing or denying communication between some hosts. For details, you can also click "New Forwarding Rule" to add a user-defined communication rule policy, as follows:

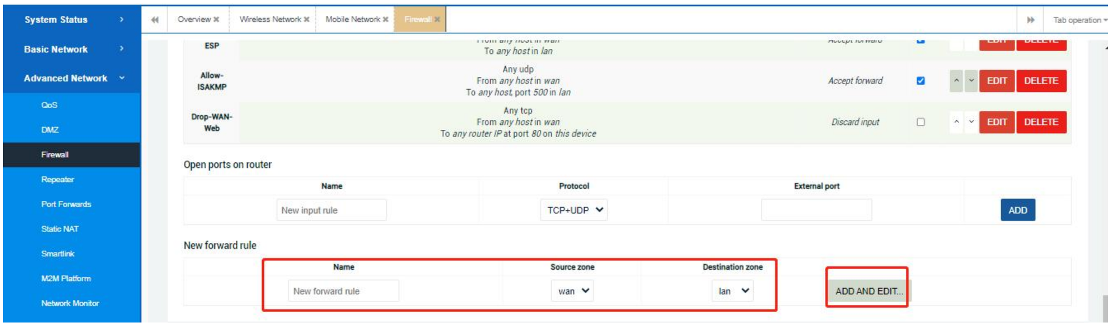


Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable			
Allow-DHCP-Renew	IPv4-udp From any host in wan To any router IP at port 68 on this device	Accept input	☑	^ ˅	EDIT	DELETE
Allow-Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input	☑	^ ˅	EDIT	DELETE
Allow-IGMP	IPv4-igmp From any host in wan To any router IP on this device	Accept input	☑	^ ˅	EDIT	DELETE
Allow-DHCPv6	IPv6-udp From IP range fc00::/6 in wan To IP range fc00::/6 at port 546 on this device	Accept input	☑	^ ˅	EDIT	DELETE
Allow-MLD	IPv6-icmp with types 130/0, 131/0, 132/0, 143/0 From IP range fe80::/10 in wan To any router IP on this device	Accept input	☑	^ ˅	EDIT	DELETE
Allow-ICMPv6-Input	IPv6-icmp with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	☑	^ ˅	EDIT	DELETE
Allow-ICMPv6-Forward	IPv6-icmp with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	☑	^ ˅	EDIT	DELETE
Allow-IPSec-ESP	Any esp From any host in wan To any host in lan	Accept forward	☑	^ ˅	EDIT	DELETE
Allow-ISAKMP	Any udp From any host in wan To any host, port 500 in lan	Accept forward	☑	^ ˅	EDIT	DELETE
Drop-WAN-Web	Any tcp From any host in wan To any router IP at port 80 on this device	Discard input	□	^ ˅	EDIT	DELETE



ESP	To *any host* in *lan*		
Allow-ISAKMP	Any udp From *any host* in *wan* To *any host*, port *500* in *lan*	*Accept forward*	☑
Drop-WAN-Web	Any tcp From *any host* in *wan* To *any router IP* at port *80* on *this device*	*Discard input*	□

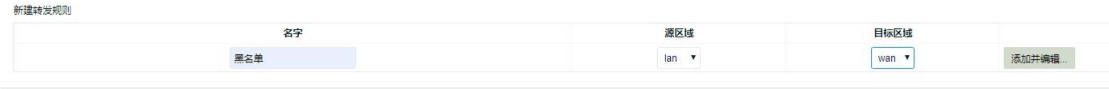
Open ports on router

Name	Protocol	External port	
New input rule	TCP+UDP		ADD

New forward rule

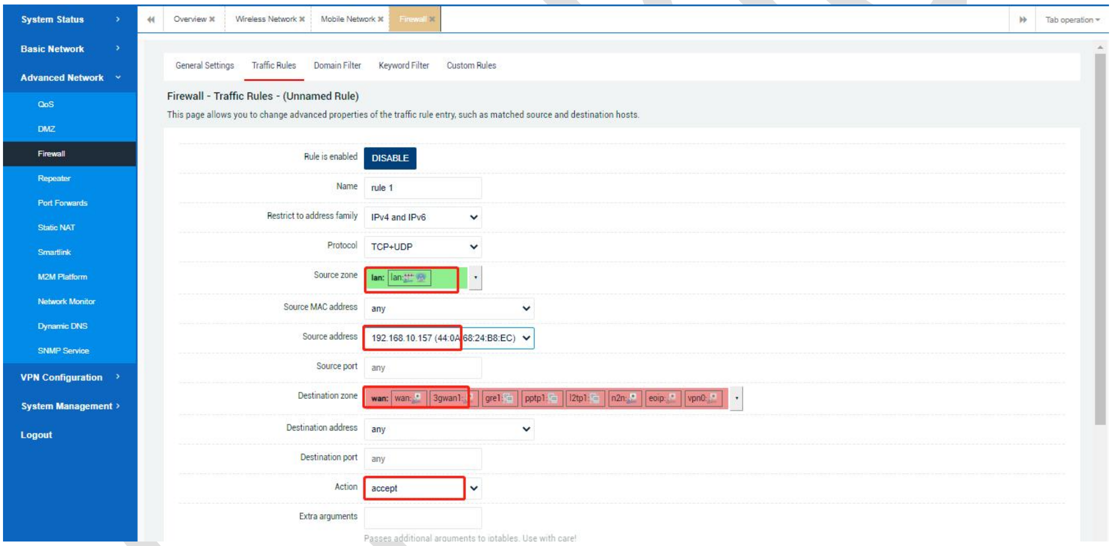
Name	Source zone	Destination zone	
New forward rule	wan	lan	ADD AND EDIT...

For example: create a new forwarding rule "blacklist" to restrict devices connected to the router from being able to access the Internet based on the MAC address. as follows:



新建转发规则

名字	源区域	目标区域	
黑名单	lan	wan	添加并编辑...



Firewall - Traffic Rules - (Unnamed Rule)

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	DISABLE
Name	rule 1
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Source zone	lan: lan:
Source MAC address	any
Source address	192.168.10.157 (44:0A:68:24:B8:EC)
Source port	any
Destination zone	wan: wan: 3gwan1: gre1: pptp1: l2tp1: n2n: eoip: vpn0:
Destination address	any
Destination port	any
Action	accept
Extra arguments	

Passes additional arguments to iptables. Use with care!

The parameters need to be set as follows, and the rest can be defaulted.

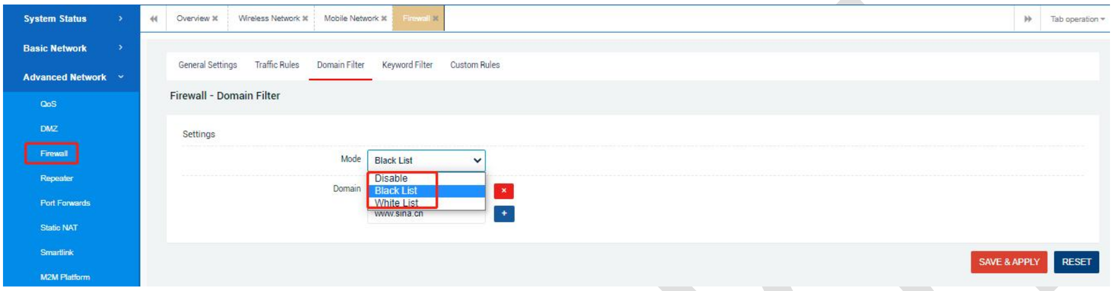
[Agreement]: Any;

[Source MAC address]: Access router LAN LAN host device MAC address, the example access router host MAC address is 00-50-56-2B-95-F0 (because the IP address will change directly);

[Action]: Reject;

5.3.3 Domain name filtering

Here you can set the black and white list of the network domain addresses to be accessed, thereby denying or allowing the router system to communicate with these addresses, as follows:



Firewall - Domain Filter

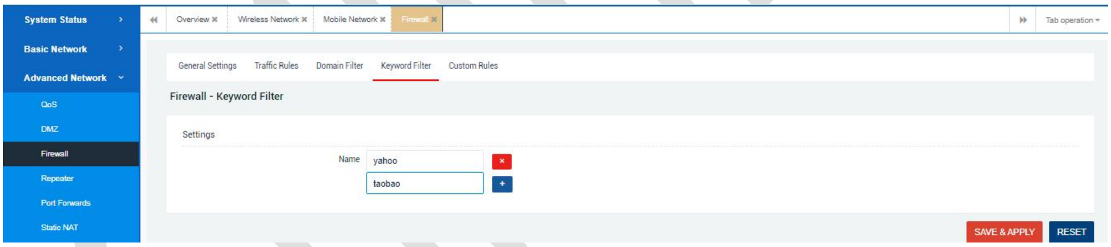
Settings

Mode: Black List

Domain: www.sina.cn

5.3.4 Keyword filtering

Here, you can configure keyword filtering to reject the routing system and certain specified network communications, as follows:



Firewall - Keyword Filter

Settings

Name: yahoo

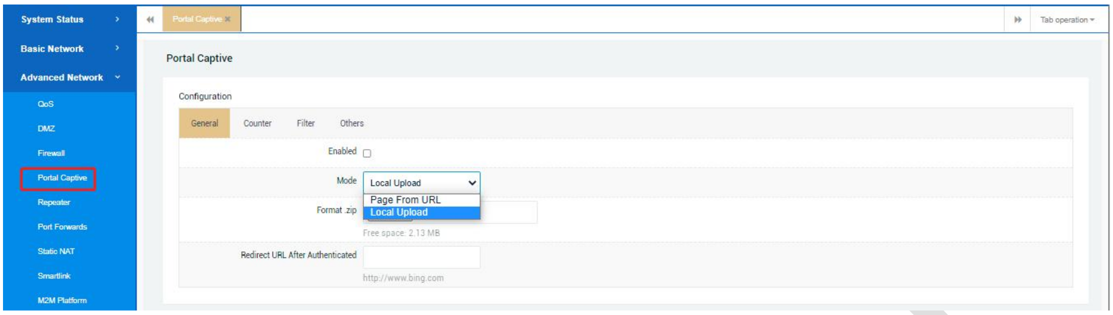
taobao

5.4 Portal authentication (optional)

This function is used to set advertising routing authentication parameters. Click "Advanced Network"-"Portal Authentication" to configure as follows:

5.4.1 General arrangement

You can configure whether it is enabled, the mode of obtaining advertisement files, and the redirection address after authentication.



Portal Captive

Configuration

Enabled □

Mode: Local Upload (Page From URL / Local Upload)

Format .zip

Free space: 2.13 MB

Redirect URL After Authenticated: http://www.bing.com

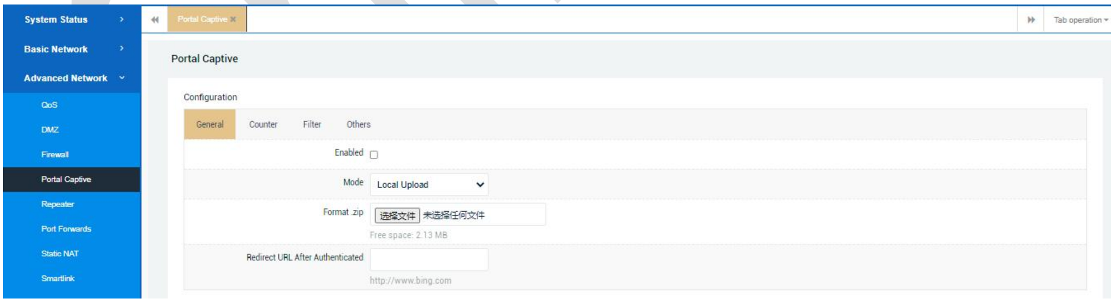
The configuration instructions are as follows:

[Enable] Check whether to enable the advertising routing function.

[Mode] You can choose the authentication file upload mode, which is uploaded locally by default.

[Jump address after authentication] The default is none, you can set it yourself.

5.4.1.1 Local Upload



Portal Captive

Configuration

Enabled □

Mode: Local Upload

Format .zip: 选择文件 未选择任何文件

Free space: 2.13 MB

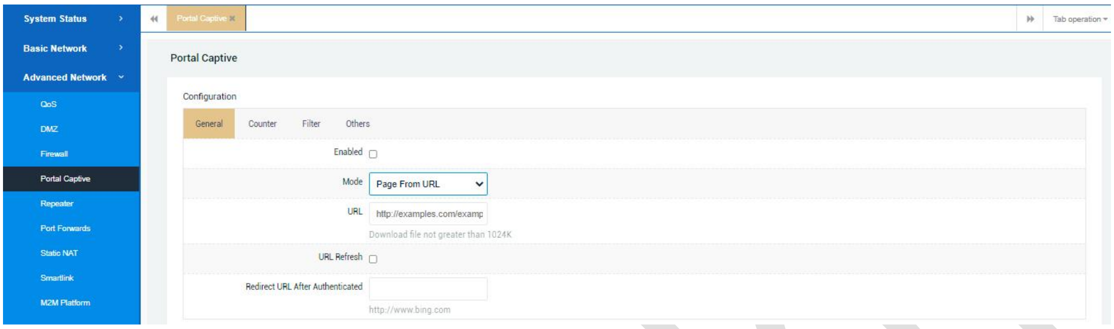
Redirect URL After Authenticated: http://www.bing.com

[Format] Upload a compressed package of certification files in *.zip format

5.4.1.2 Download file from URL server address

[Address] Fill in the URL server to store the htdocs advertisement file path (support http, https);

[Page update] means that when the htdocs advertisement file of the URL server changes, the advertising router will re-download the new htdocs file from the URL server. It is recommended to check it. After checking, the router background will check the server file every 5 minutes and update it synchronously.



Portal Captive

Configuration

Enabled □

Mode Page From URL

URL http://examples.com/examp

Download file not greater than 1024K

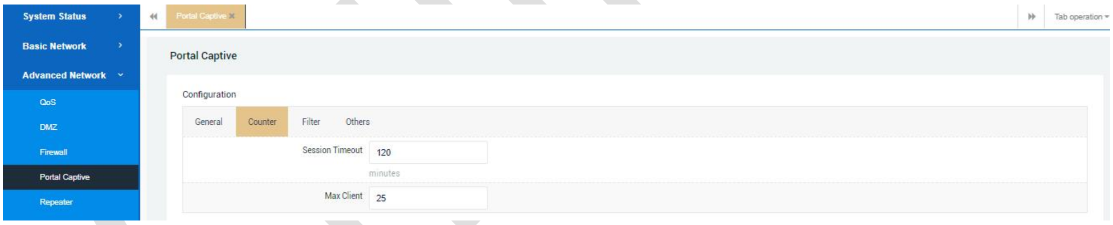
URL Refresh □

Redirect URL After Authenticated

http://www.bing.com

5.4.2 counter

It can be used to set the timeout period of connected devices and the maximum number of device connections.



Portal Captive

Configuration

Session Timeout 120

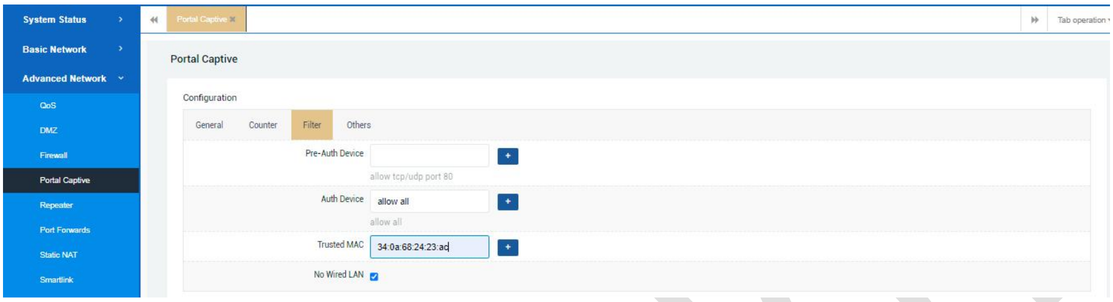
minutes

Max Client 25

[Session timeout] refers to the total time that wireless terminals such as mobile phones can connect to the router after WiFi access is authenticated. If this time is exceeded, the terminal will be disconnected and need to be re-authenticated. The default value is 120 minutes, which is 2 hours.

[Maximum number of customers] refers to the number of wireless terminals that support WiFi authentication for connecting to the router. When this value is exceeded, the newly added wireless terminal cannot pass the authentication. The default value is 25.

5.4.3 Filter



Pre-Auth Device: (empty)
allow tcp/udp port 80

Auth Device: allow all
allow all

Trusted MAC: 34:0a:68:24:23:ac

No Wired LAN ☑

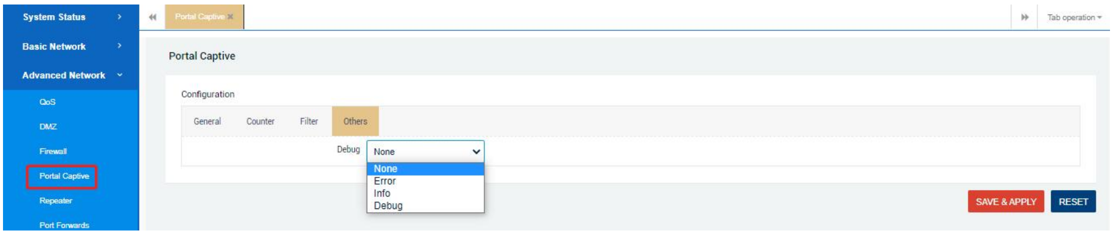
[Uncertified device] refers to a wireless terminal that is not connected to the router with WiFi certification or certification-free, and there are no restrictions on use by default.

[Authenticated device] refers to the network usage restrictions for wireless terminals after connecting to the route WiFi authentication, such as the restriction of the destination ip address or access port, all are allowed by default, and there is no restriction.

[Authentication-free device MAC address] means that after filling in the device's network card mac address, the wireless terminal does not need to be authenticated after connecting to the routed WiFi, and can directly access the network.

[Ignore wired devices] After checking, the system will ignore LAN access devices for authentication, and you can directly access the network.

5.4.4 other



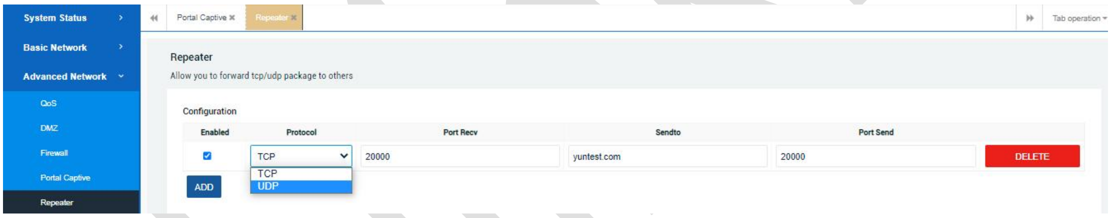
Portal Captive

Debug: None

[Debug] Switch to different log debugging sectors (none, error, information, debugging), the router system log will correspondingly display the corresponding log information;

5.5 Repeater

This function is used to forward TCP/UDP to other network locations. as follows:



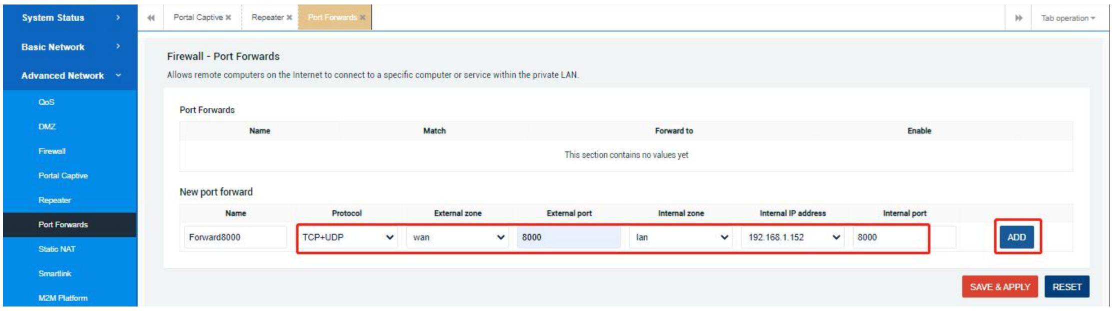
Repeater

Allow you to forward tcp/udp package to others

Enabled	Protocol	Port Recv	Sendto	Port Send
☑	TCP	20000	yuntest.com	20000

5.6 Port forwarding

This function is used to map the service resources of the internal host to the external access area of the device (usually a public IP address or an address that can be directly accessed), and at the same time makes the access to the internal service resources more secure. as follows:



Firewall - Port Forwards

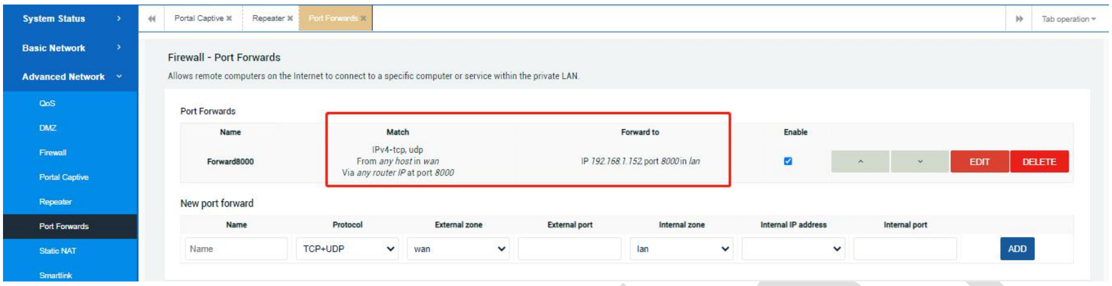
Allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable
This section contains no values yet			

New port forward

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
Forward8000	TCP+UDP	wan	8000	lan	192.168.1.152	8000



Firewall - Port Forwards

Allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable
Forward8000	IPv4-tcp, udp From *any host* in *wan* Via *any router IP* at port *8000*	IP *192.168.1.152*, port *8000* in *lan*	☑

New port forward

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
Name	TCP+UDP	wan		lan		

[Name]: The name of the custom rule;

[Agreement]: Select rule agreement, generally ALL;

[External area]: select WAN area;

[External port]: Fill in the port for forwarding access to the external area;

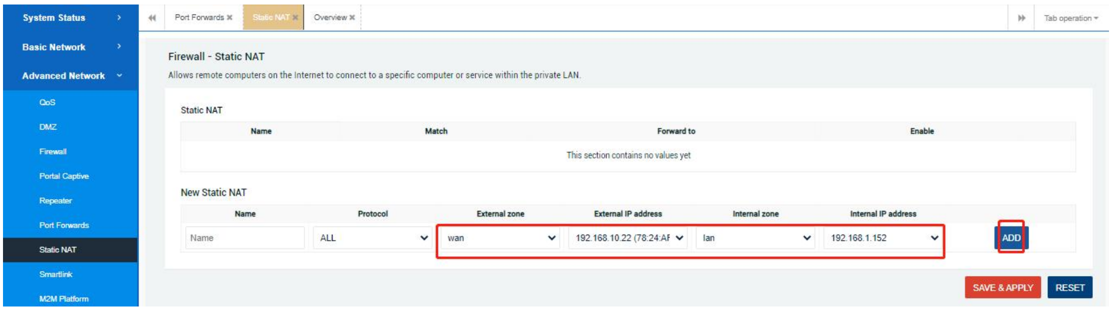
[Internal Area]: Select the area for internal forwarding, here is the LAN area;

[Internal address]: Fill in the internal host address after forwarding, which can be filled in specifically;

[Internal port]: Fill in the port forwarded and accessed by the internal host, which can be filled in specifically;

5.7 Static NAT

This function allows remote computers on the Internet to connect to specific computers or services in the internal network, and the device supports 1-to-1 or many-to-one static nat functions.



Firewall - Static NAT

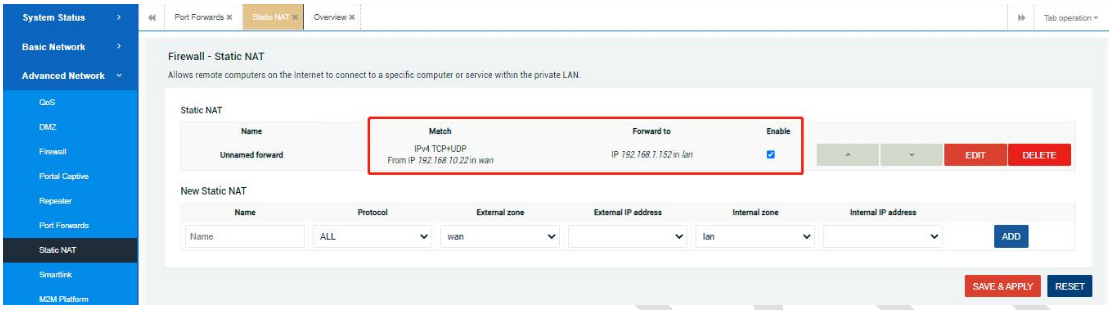
Allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Static NAT

Name	Match	Forward to	Enable
This section contains no values yet			

New Static NAT

Name	Protocol	External zone	External IP address	Internal zone	Internal IP address
Name	ALL	wan	192.168.10.22 (78:24:AF	lan	192.168.1.152



Firewall - Static NAT

Allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Static NAT

Name	Match	Forward to	Enable
Unnamed forward	IPv4 TCP+UDP From IP 192.168.10.22 in wan	IP 192.168.1.152 in lan	☑

New Static NAT

Name	Protocol	External zone	External IP address	Internal zone	Internal IP address
Name	ALL	wan		lan	

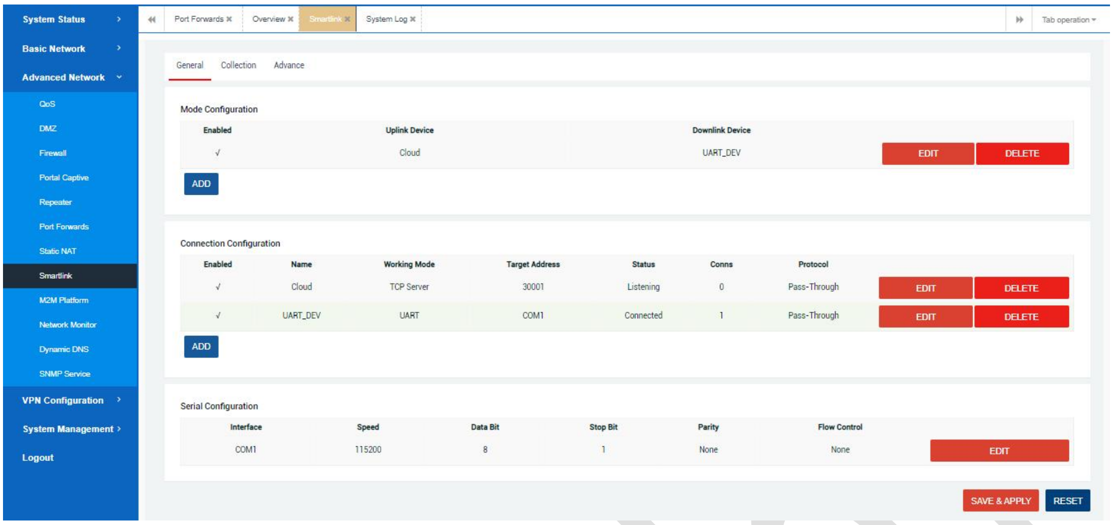
5.8 Smarklink

Smart IoT is composed of two parts: [General] and [Advanced].

[General] The interface mainly displays basic information such as user configuration mode configuration, connection configuration, and serial port configuration.

[Advanced] It mainly displays the advanced configuration of the serial port and other information.

5.8.1 General



Mode Configuration

Enabled	Uplink Device	Downlink Device		
√	Cloud	UART_DEV	EDIT	DELETE

ADD

Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol		
√	Cloud	TCP Server	30001	Listening	0	Pass-Through	EDIT	DELETE
√	UART_DEV	UART	COM1	Connected	1	Pass-Through	EDIT	DELETE

ADD

Serial Configuration

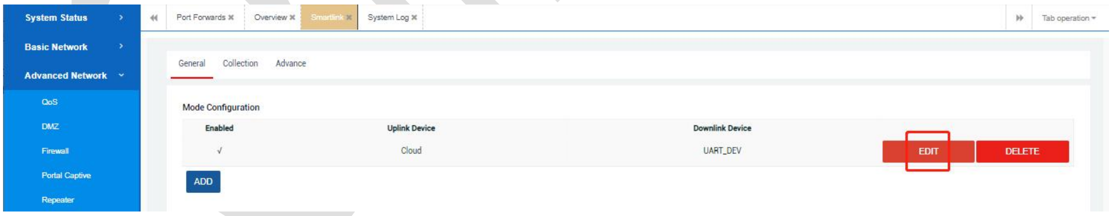
Interface	Speed	Data Bit	Stop Bit	Parity	Flow Control	
COM1	115200	8	1	None	None	EDIT

SAVE & APPLY RESET

5.8.1.1 Mode configuration

Click Add to create and use a new usage mode, and you can choose to use the created connection.

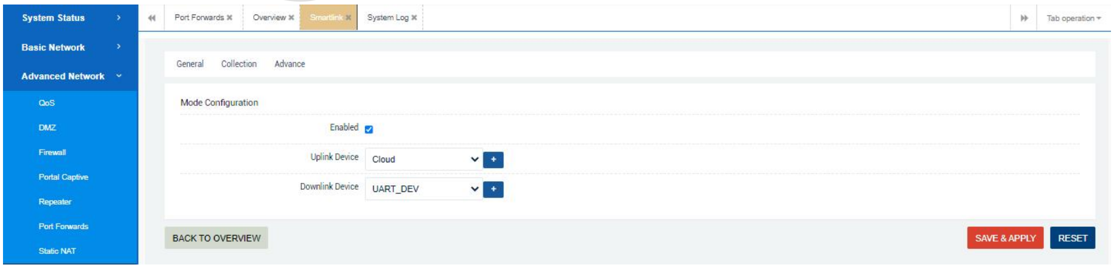
Note: Multiple modes cannot use the same working mode as the connection of the universal serial port. (The universal serial port is the physical COM port of the router device.)



Mode Configuration

Enabled	Uplink Device	Downlink Device		
√	Cloud	UART_DEV	EDIT	DELETE

ADD



Mode Configuration

Enabled ☑

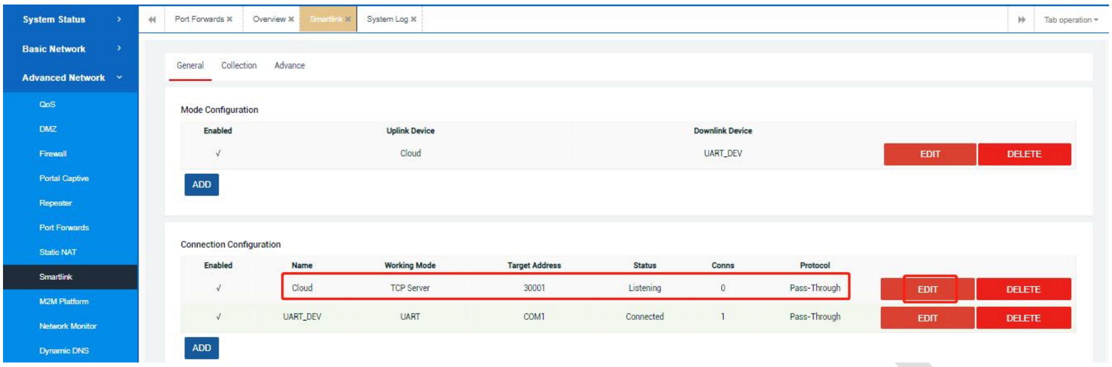
Uplink Device: Cloud +

Downlink Device: UART_DEV +

BACK TO OVERVIEW SAVE & APPLY RESET

5.8.1.2 Connection configuration

Uplink device settings:



Mode Configuration

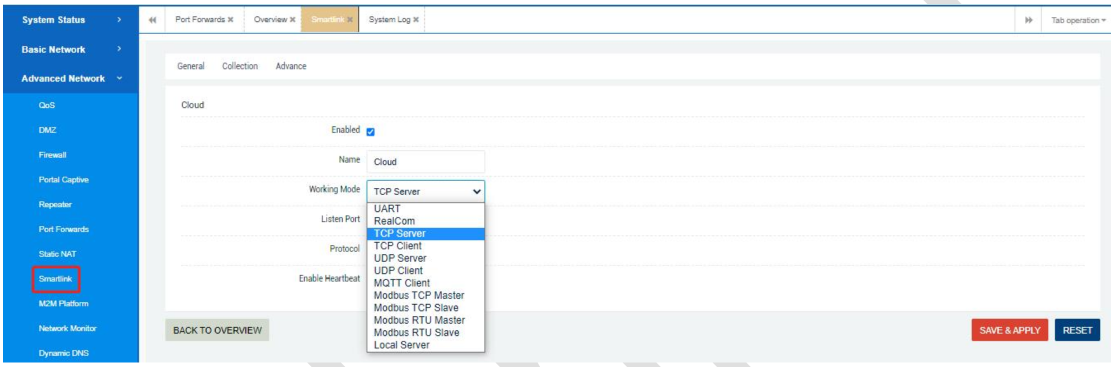
Enabled	Uplink Device	Downlink Device	
√	Cloud	UART_DEV	EDIT DELETE

ADD

Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol	
√	Cloud	TCP Server	30001	Listening	0	Pass-Through	EDIT DELETE
√	UART_DEV	UART	COM1	Connected	1	Pass-Through	EDIT DELETE

ADD



Cloud

Enabled ☑

Name: Cloud

Working Mode: TCP Server

Listen Port

Protocol

Enable Heartbeat

The parameter description is as follows:

[Enable]: After checking, enable the serial port function;

[Name]: It is empty by default and can be named;

[Work Agreement]: Choose the corresponding work mode according to actual needs;

[Monitor port]: TCP port, this item is related to the specific working mode;

[Protocol]: Transparent transmission mode;

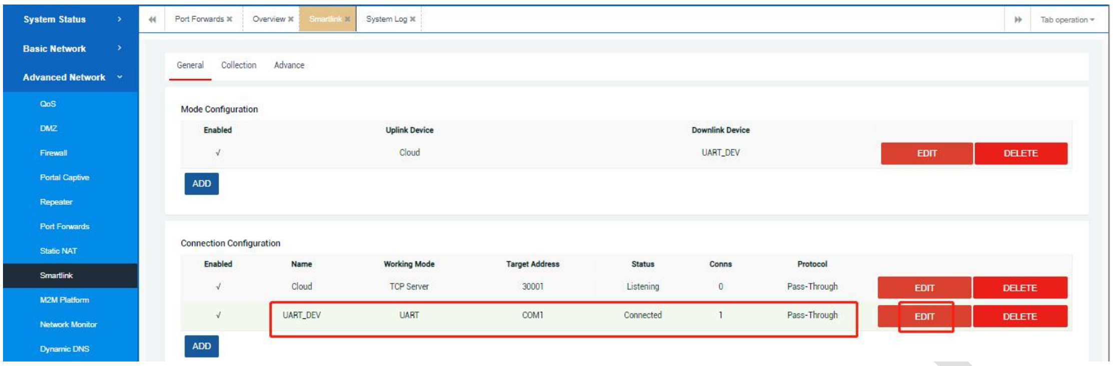
[Heartbeat]: Not checked by default;

[Heartbeat interval]: can be set specifically, the unit is second;

[Heartbeat content]: It can be set specifically, and the heartbeat content in the corresponding format must be filled in;

[Save and apply]: The configuration will take effect after saving and will be displayed in the general interface;

Downstream device settings:

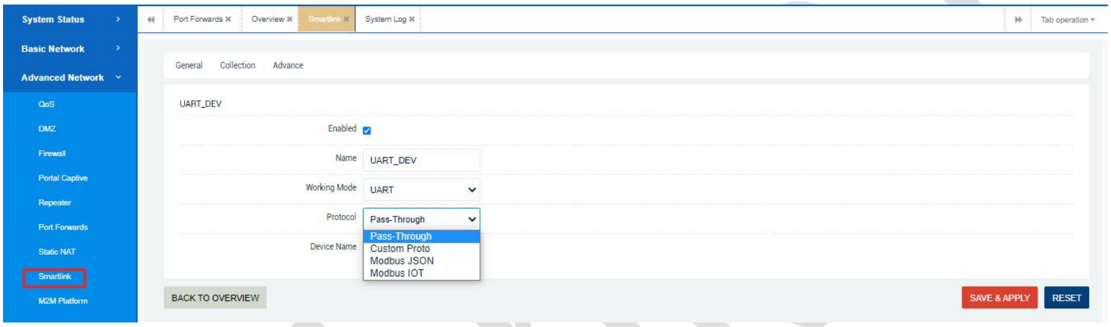


Mode Configuration

Enabled	Uplink Device	Downlink Device
√	Cloud	UART_DEV

Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol
√	Cloud	TCP Server	30001	Listening	0	Pass-Through
√	UART_DEV	UART	COM1	Connected	1	Pass-Through



UART_DEV

Enabled ☑

Name: UART_DEV

Working Mode: UART

Protocol: Pass-Through

Device Name

5.8.1.3 Serial port configuration

Click the edit button to enter the COM port configuration interface.

The interface parameters are described as follows:

[Baud rate]: The default is 115200, which can be set specifically;

[Data bit]: The default is 8, which can be set specifically;

[Stop bit]: The default is 1, which can be set specifically;

[Check Digit]: The default is NO, which can be set specifically;

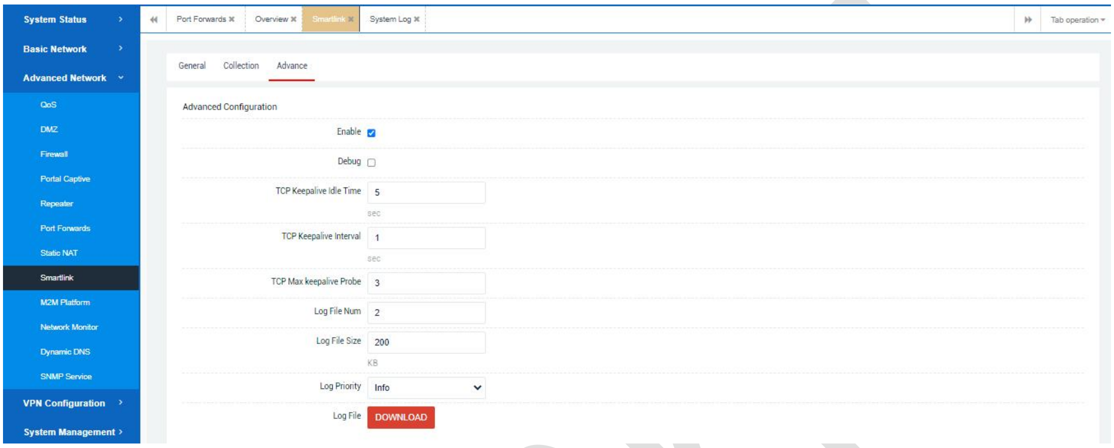
[Flow Control]: The default is NONE, which can be set specifically;

[Sub-packing interval]: The default is 60, which can be set specifically;

[Sub-package length]: The default is 1460, which can be set specifically;

5.8.2 advanced

Mainly configure the opening and closing of the Smartlink function, the opening and closing of debugging, the size, number, priority, download, etc. of log files. as follows:



Advanced Configuration

Enable ☑

Debug □

TCP Keepalive Idle Time: 5 sec

TCP Keepalive Interval: 1 sec

TCP Max keepalive Probe: 3

Log File Num: 2

Log File Size: 200 KB

Log Priority: Info

Log File: DOWNLOAD

The advanced parameters are described as follows:

[Open]: Smart IoT switch.

[Debug]: Not checked by default.

[TCP keep-alive idle time]: The default is 60s, which can be set specifically.

[TCP keep-alive detection interval]: The default is 3s, which can be set specifically.

[Maximum times of TCP keep-alive detection]: The default is 3 times, which can be set specifically.

[Number of retained log files]: The default is 2, which can be set specifically.

[Log file size]: The default is 200KB, and it is recommended not to exceed 3000KB.

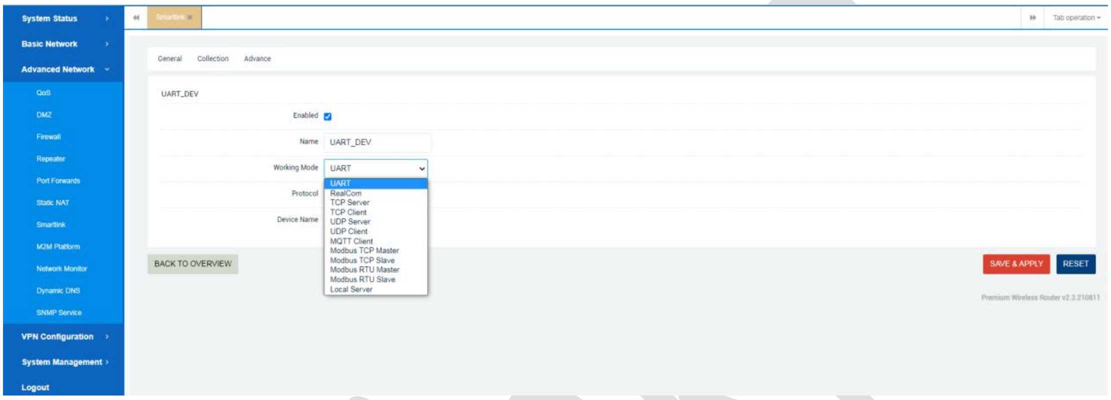
[Log Priority]: Default information, which can be selected specifically.

[Log file]: Download button.

5.8.3 Operating mode

Smartlink supports a total of 12 modes to meet the needs of different scenarios in the project. It can be flexibly configured according to the actual needs of the site. The general serial port mode is the physical COM port of the router.

Select "Advanced Network" --- "Smart IOT" --- "General" --- "Connection Configuration" --- "Edit", select "Work Mode". as follows:



UART_DEV

Enabled ☑

Name UART_DEV

Working Mode UART

- UART
- RealCom
- TCP Server
- TCP Client
- UDP Server
- UDP Client
- MQTT Client
- Modbus TCP Master
- Modbus TCP Slave
- Modbus RTU Master
- Modbus RTU Slave
- Local Server

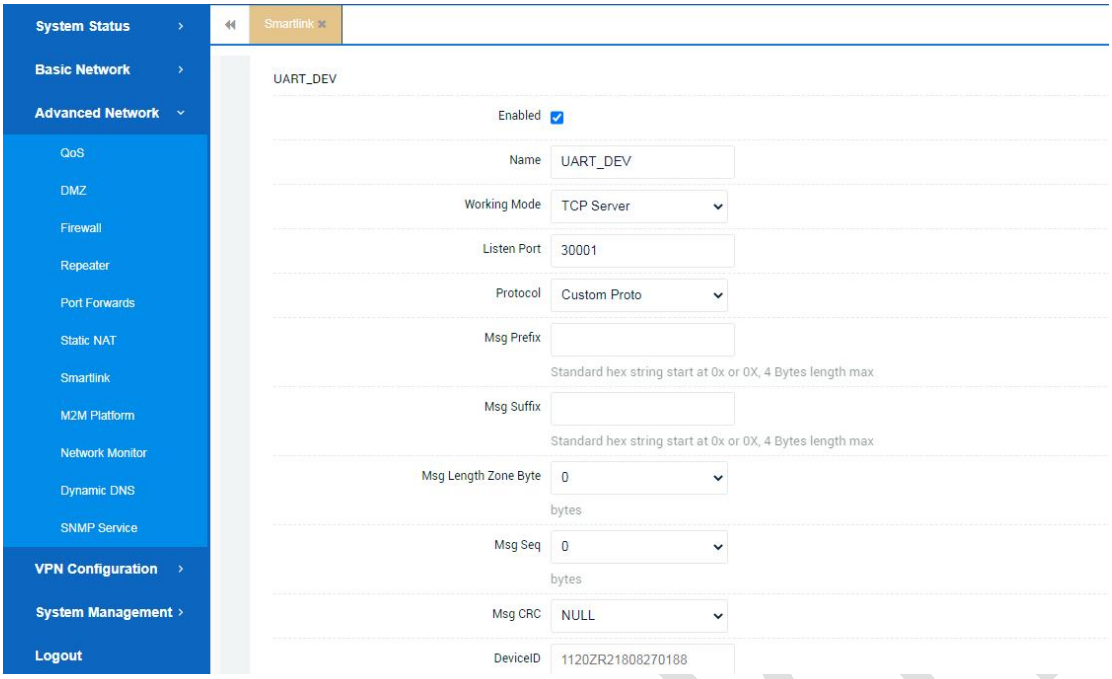
Protocol

Device Name

5.8.4 Custom protocol

Smartlink usage protocol supports the use of custom protocols to meet the needs of different scenarios. It can be flexibly configured according to the actual needs of the site.

Select "Advanced Network" --- "Smartlink" --- "General" --- "Connection Configuration" --- "Edit", select "Protocol". as follows:



UART_DEV

Enabled ☑

Name: UART_DEV

Working Mode: TCP Server

Listen Port: 30001

Protocol: Custom Proto

Msg Prefix:

Standard hex string start at 0x or 0X, 4 Bytes length max

Msg Suffix:

Standard hex string start at 0x or 0X, 4 Bytes length max

Msg Length Zone Byte: 0 bytes

Msg Seq: 0 bytes

Msg CRC: NULL

DeviceID: 1120ZR21808270188

[Message prefix]: a standard hexadecimal string starting with 0x or 0X, up to 4 bytes;

[Message length byte]: 0/1/2 byte setting can be set by yourself;

[Message sequence number]: default 0 byte, support 0/1/2 byte setting;

[Device ID]: ASCII and hexadecimal strings can be supported. If it is a hexadecimal string, it must be a standard hexadecimal string starting with 0x or 0X, and the maximum length is 16 bytes;

[CRC check]: The default is null, which can be set according to actual use;

[Message suffix]: a standard hexadecimal string beginning with 0x or 0X, maximum 4 bytes;

[Enable Heartbeat]: Heartbeat packet function settings, including two parameters, heartbeat content and heartbeat sending interval, which are not enabled by default.

5.8.5 Configuration example

5.8.5.1 TCP server

Example description

In the TCP server mode, the router configures an IP port number (monitoring the local port) as a TCP server, and passively waits for the remote host to connect. After the remote host initiates a connection request and establishes a connection with the router, the remote host can realize two-way transparent transmission through the network connection and the serial port. The remote host can read or send data to a serial device at the same time.

Example steps

Router (TCP server) parameters:

WAN port IP address: 192.168.10.122

Listening port: 6800

————————————————————————————————

Serial port configuration parameters:

Physical interface	Baud rate	Data bit	Stop bit	Parity bit	Flow control
COM1	115200	8	1	None	None

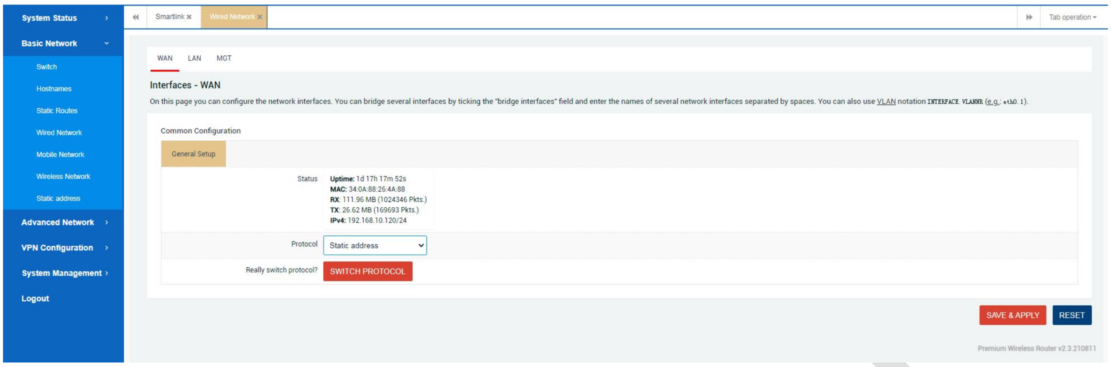
————————————————————————————————

Remote PC (TCP client) parameters:

IP address: 192.168.10.192

Step 1: Configure the WAN port IP address

Wired network>WAN>click protocol (select static address)>click to switch protocol



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

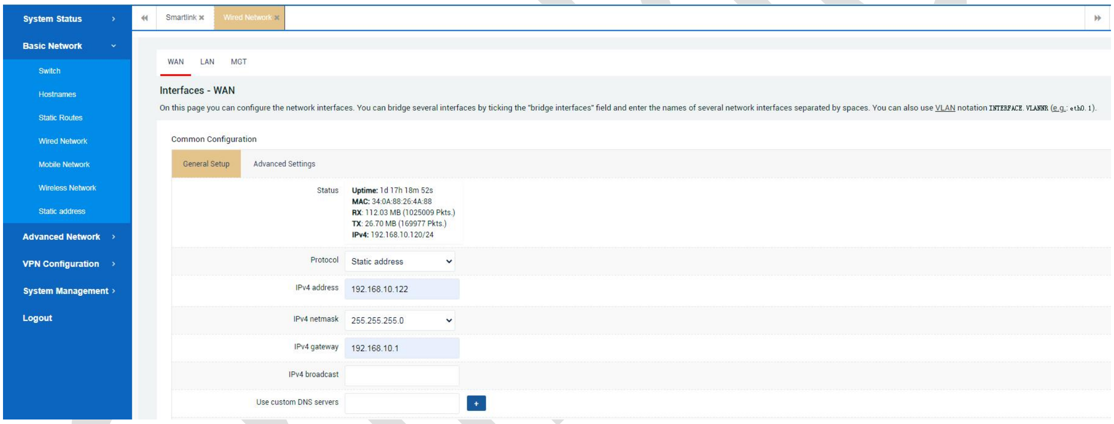
Common Configuration

Status: **Uptime:** 1d 17h 17m 52s
MAC: 34:0A:88:26:4A:88
RX: 111.96 MB (1024346 Pkts.)
TX: 26.62 MB (169693 Pkts.)
IPv4: 192.168.10.120/24

Protocol: Static address

Really switch protocol?

Configure the IPV4 address, subnet mask, and IPV4 gateway, and click the Save and Apply button in the lower right corner to save the configuration.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: **Uptime:** 1d 17h 18m 52s
MAC: 34:0A:88:26:4A:88
RX: 112.03 MB (1025009 Pkts.)
TX: 26.70 MB (169977 Pkts.)
IPv4: 192.168.10.120/24

Protocol: Static address

IPv4 address: 192.168.10.122

IPv4 netmask: 255.255.255.0

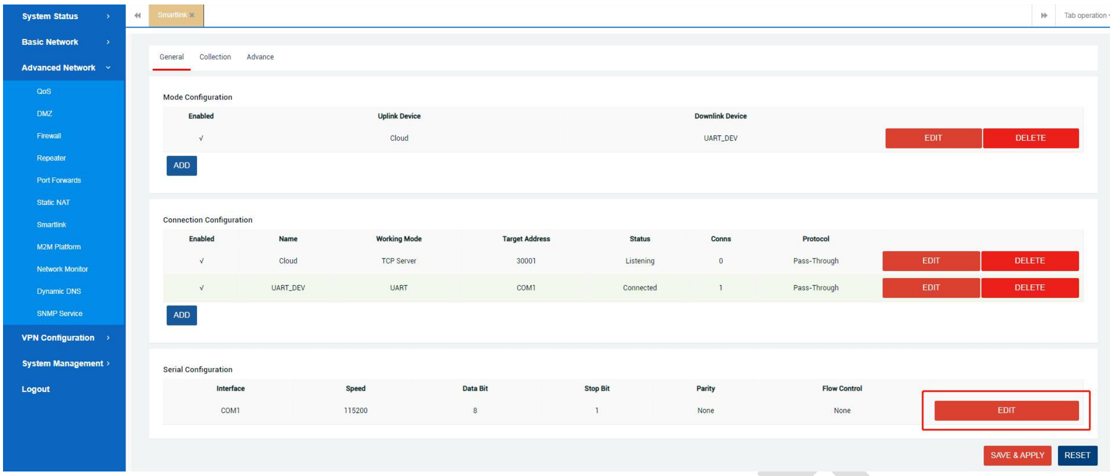
IPv4 gateway: 192.168.10.1

IPv4 broadcast:

Use custom DNS servers:

Step 2: Configure the serial port configuration

Smartlink> Click the "Edit" button of COM1. The serial port parameter can be configured.



Mode Configuration

Enabled	Uplink Device	Downlink Device		
√	Cloud	UART_DEV	EDIT	DELETE

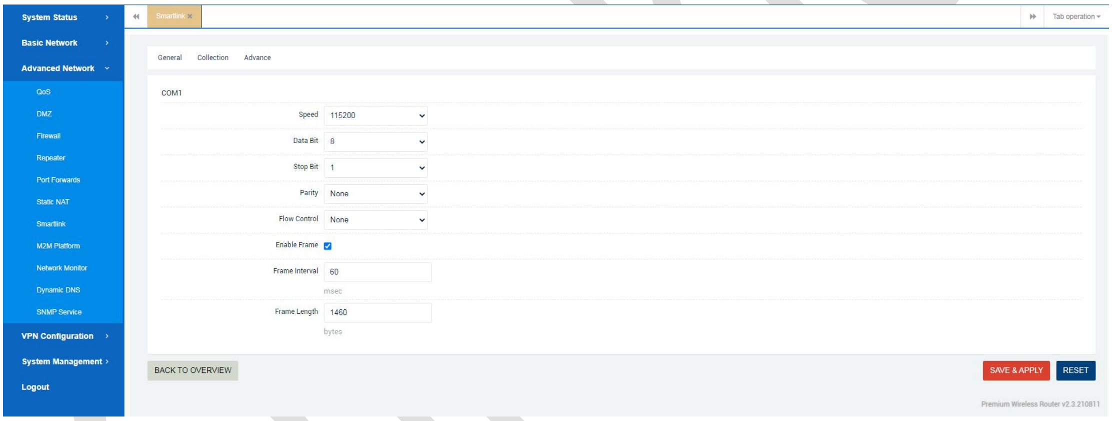
Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol		
√	Cloud	TCP Server	30001	Listening	0	Pass-Through	EDIT	DELETE
√	UART_DEV	UART	COM1	Connected	1	Pass-Through	EDIT	DELETE

Serial Configuration

Interface	Speed	Data Bit	Stop Bit	Parity	Flow Control	
COM1	115200	8	1	None	None	EDIT

Enter the configuration interface to modify the baud rate, data bit, stop bit and other parameters according to actual needs. The "Save and Apply" button in the lower right corner will save and take effect.



COM1

Speed	115200
Data Bit	8
Stop Bit	1
Parity	None
Flow Control	None
Enable Frame	☑
Frame Interval	60 msec
Frame Length	1460 bytes

5.8.5.2 TCP Client

Example description

In the TCP client mode, the router host IP and port number actively establish a TCP protocol connection with the remote PC, and the router can realize bidirectional transmission to the transparent mode through the network connection and the remote PC. The PC can send and receive data to a serial device at the same time.

Example steps

Router (TCP client) parameters:

WAN port IP address: 192.168.10.122

Server address: 192.168.10.192

Server port: 6800

——————————————————————————————

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

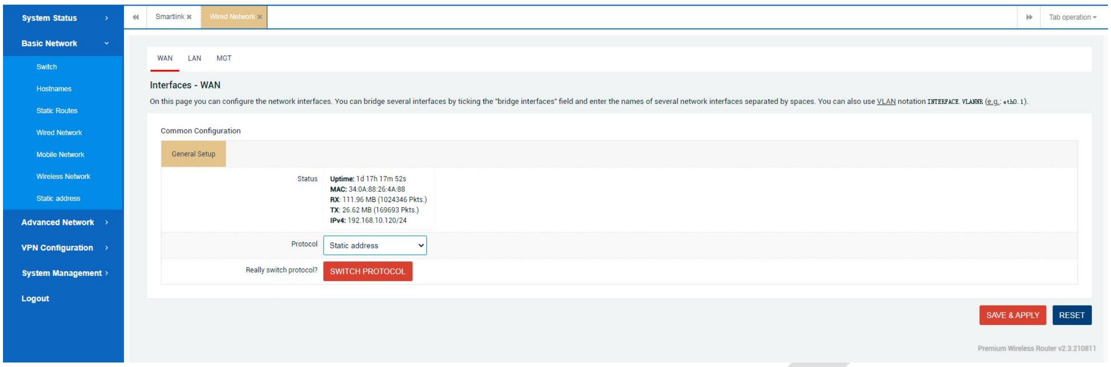
——————————————————————————————

PC (TCP server) parameters:

IP address: 192.168.10.192

Step 1: Configure the WAN port IP address

Wired network>WAN>click protocol (select static address)>click to switch protocol



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

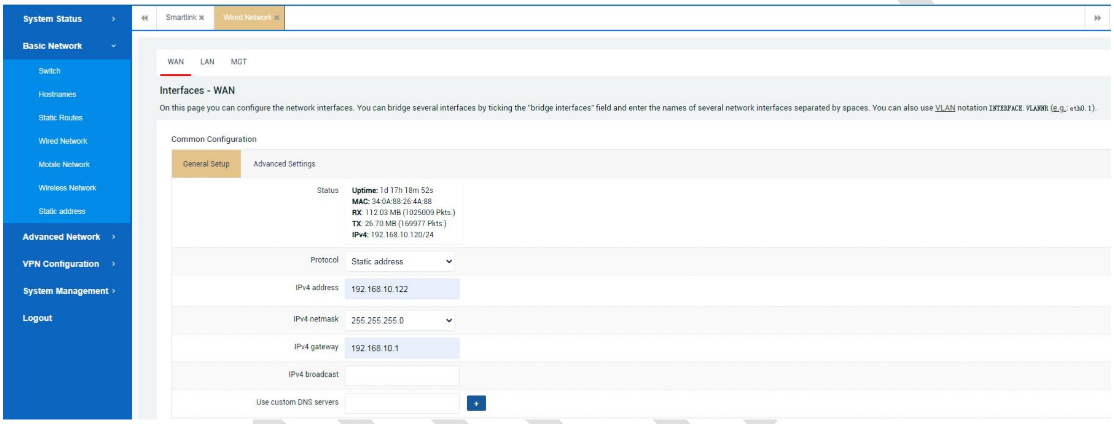
Status: **Uptime:** 1d 17h 17m 52s
MAC: 34:0A:88:26:4A:88
RX: 111.96 MB (1024346 Pkts.)
TX: 26.62 MB (169693 Pkts.)
IPv4: 192.168.10.120/24

Protocol: Static address

Really switch protocol?

Premium Wireless Router v2.3.210811

Configure IPV4 address, subnet mask, IPV4 gateway.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: **Uptime:** 1d 17h 18m 52s
MAC: 34:0A:88:26:4A:88
RX: 112.03 MB (1025009 Pkts.)
TX: 26.70 MB (169977 Pkts.)
IPv4: 192.168.10.120/24

Protocol: Static address

IPv4 address: 192.168.10.122

IPv4 netmask: 255.255.255.0

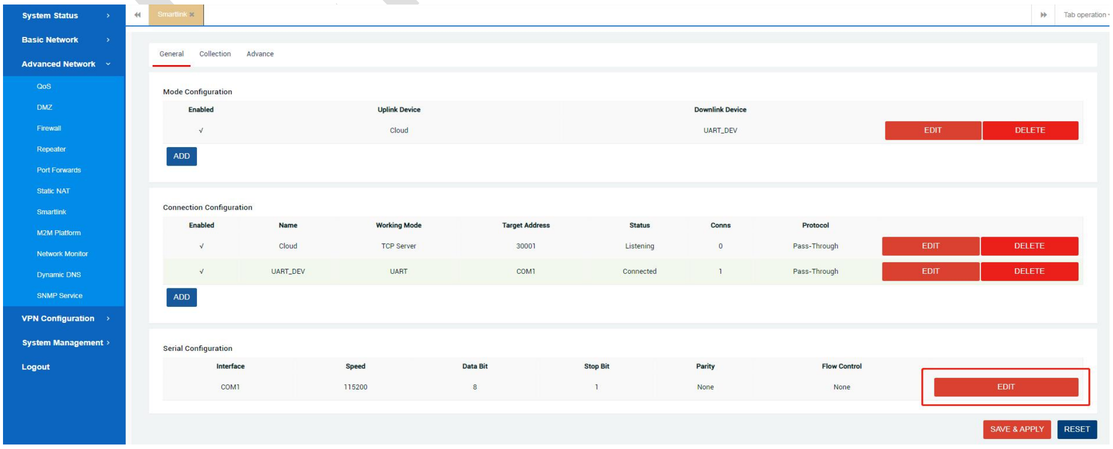
IPv4 gateway: 192.168.10.1

IPv4 broadcast:

Use custom DNS servers:

Step 2: Configure the serial port configuration

Smartlink> Click the edit button in the serial port configuration bar. The serial port parameter can be configured.



Mode Configuration

Enabled	Uplink Device	Downlink Device		
√	Cloud	UART_DEV	EDIT	DELETE

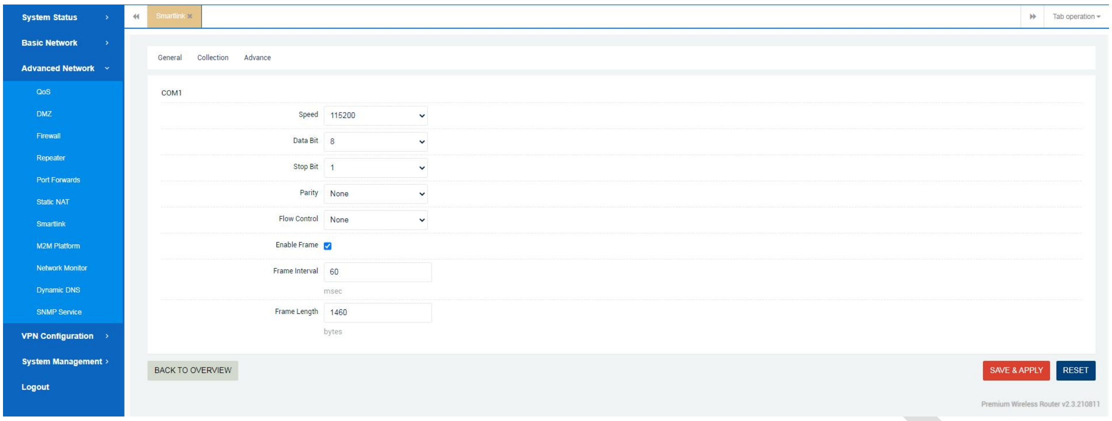
Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol		
√	Cloud	TCP Server	30001	Listening	0	Pass-Through	EDIT	DELETE
√	UART_DEV	UART	COM1	Connected	1	Pass-Through	EDIT	DELETE

Serial Configuration

Interface	Speed	Data Bit	Stop Bit	Parity	Flow Control	
COM1	115200	8	1	None	None	EDIT

Enter the configuration interface to modify the baud rate, data bit, stop bit and other parameters according to actual needs.



COM1

Speed: 115200

Data Bit: 8

Stop Bit: 1

Parity: None

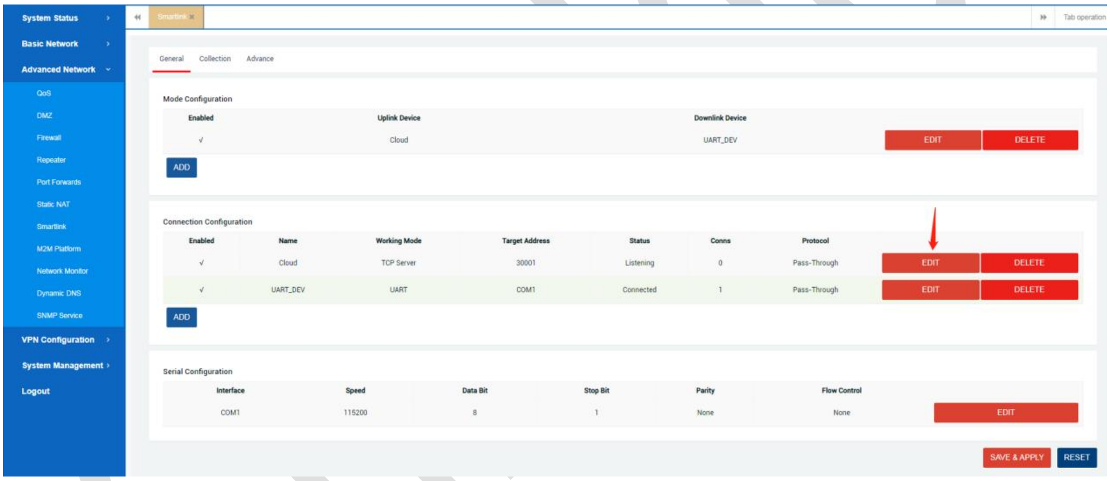
Flow Control: None

Enable Frame: ☑

Frame Interval: 60 msec

Frame Length: 1460 bytes

Step 3: Configure the server address and port for receiving data



Mode Configuration

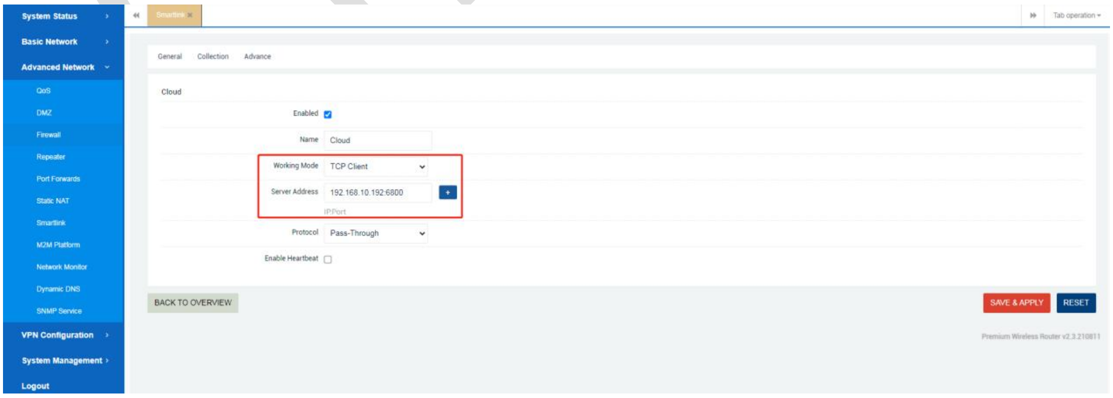
Enabled	Uplink Device	Downlink Device		
√	Cloud	UART_DEV	EDIT	DELETE

Connection Configuration

Enabled	Name	Working Mode	Target Address	Status	Conns	Protocol		
√	Cloud	TCP Server	30001	Listening	0	Pass-Through	EDIT	DELETE
√	UART_DEV	UART	COM1	Connected	1	Pass-Through	EDIT	DELETE

Serial Configuration

Interface	Speed	Data Bit	Stop Bit	Parity	Flow Control	
COM1	115200	8	1	None	None	EDIT



Cloud

Enabled: ☑

Name: Cloud

Working Mode: TCP Client

Server Address: 192.168.10.192:6800 (IP:Port)

Protocol: Pass-Through

Enable Heartbeat: □

5.8.5.3 UDP Server

Slightly (same as TCP server mode, the difference is that UDP server mode uses UDP protocol to build network connection)

5.8.5.4 UDP Client

Slightly (same as TCP client mode, the difference is that UDP client mode uses UDP protocol to build network connections)

5.8.5.5 Real serial port mode

Example description

In the real serial port mode, the router connects to the virtual serial port of the remote PC. The virtual serial port tool establishes a transparent network transmission connection between the host and the serial device in the operating system, and maps the router's serial port to the host's local virtual serial device according to the parameters such as the router IP address and serial number configured by the user to realize the real serial port and virtual Transparent transmission between serial ports.

Example steps

Router (real serial port) parameters:

WAN port IP address: 192.168.10.122

Router port: 30001 (fixed)

——————————————————————————

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

——————————————————————————

PC parameters:

IP address: 192.168.10.192

Step 1: Configure the WAN port ip address

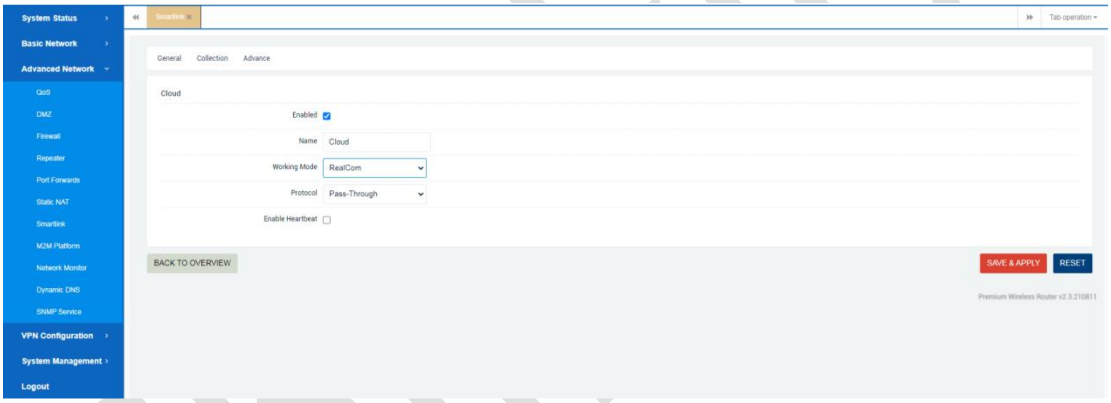
Omit (same as above)

Step 2: Configure the serial port configuration

Omit (same as above)

Step 3: Connection configuration

Configuration Enable check, name (can be empty), working mode selection: real serial port mode



Cloud

Enabled ☑

Name: Cloud

Working Mode: RealCom

Protocol: Pass-Through

Enable Heartbeat ☐

5.8.5.6 MQTT Client

Example description

Two MQTT clients are similar to the process of mailing letters between two people. One party publishes a message, and the other party receives the message after subscribing.

Example steps

————————————————————————————

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

——————————————————————————————

Serial port configuration parameters:

Physical interface Baud rate Data bit Stop bit Parity bit Flow control

COM1 115200 8 1 None None

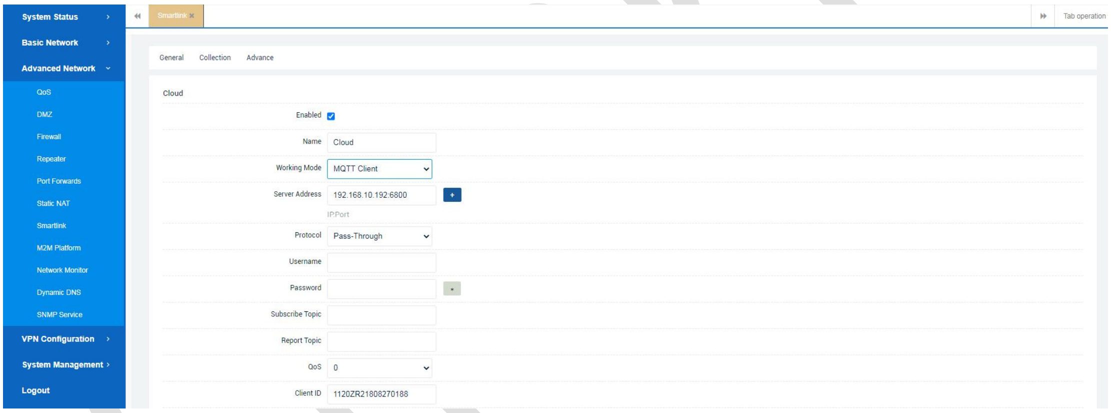
step 1:

Configure serial port configuration

Omit (same as above)

Step 2: Connection configuration

Configuration Enable check, name (can be empty), working mode selection: MQTT client



Cloud

Enabled ☑

Name: Cloud

Working Mode: MQTT Client

Server Address: 192.168.10.192:6800

IP:Port

Protocol: Pass-Through

Username:

Password:

Subscribe Topic:

Report Topic:

QoS: 0

Client ID: 1120ZR21808270188

[Server address] Fill in the MQTT server address and port (server address: port).

[Protocol] The default transparent transmission mode, you can choose by yourself;

[Username/Password] The MQTT server decides whether it is required or not. If there is, it needs to be filled in.

[Subscribe/Report Subject] The subject address for mutual communication can be set by yourself.

[Qos] Quality of service, the default is 0, you can choose to set 1, 2.

[Customer ID] Default device serial number.

[MQTT keep-alive period] MQTT keep-alive period, the default is 60 seconds.

[Device Mode] The default transparent transmission mode can be selected by yourself.

[Heartbeat] Check to enable.

[Heartbeat interval] The unit is second, which can be set by yourself.

[Heartbeat content] ASCII code and hexadecimal string can be set by yourself.

5.8.5.7 Modbus RTU to TCP master-slave communication

Please contact technical support to assist in debugging.

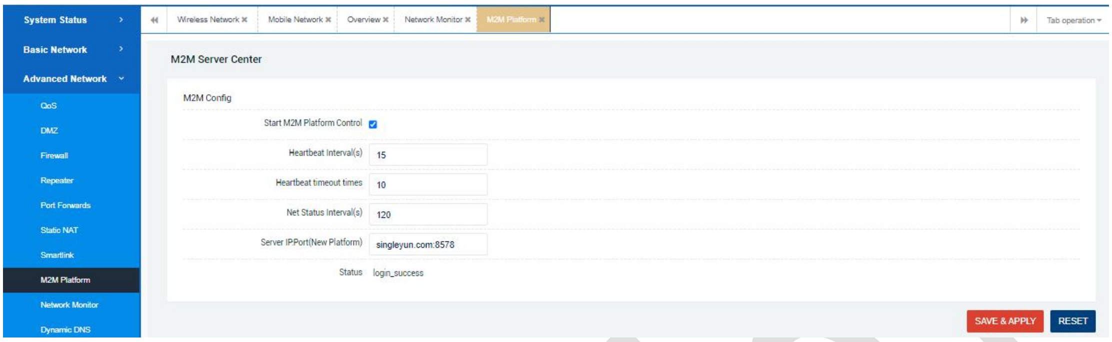
5.8.5.8 Modbus TCP master-slave communication

Please contact technical support to assist in debugging.

5.9 M2M Cloud platform

The user scenario of this function is: the router connects to the cloud server management platform through the Internet, and the user can realize remote view management of the router, remote firmware upgrade, remote configuration, log download and view without going to the site.

The functional parameters are described below:



M2M Server Center

M2M Config

Start M2M Platform Control ☑

Heartbeat Interval(s) 15

Heartbeat timeout times 10

Net Status Interval(s) 120

Server IP:Port(New Platform) singleyun.com:8578

Status login_success

[**Start M2M Platform Control**]： Enable or disable the platform connection；

[**Heartbeat Interval(s)**]： The heartbeat interval between the router client and server platform (default: 15s);

[**Heartbeat timeout times**]： The router client reports the number of failed heartbeat packets (if it exceeds this number, the router is considered to have failed to connect to the platform). The default is 10 times.

[**Net Status Interval(s)**]： The interval at which the router reports its online status to the server platform (default 120s).

[**Server IP:Port(New Platform)**]： Server platform address and port configuration;

[**Status**]： The status of the router connecting to the cloud platform;

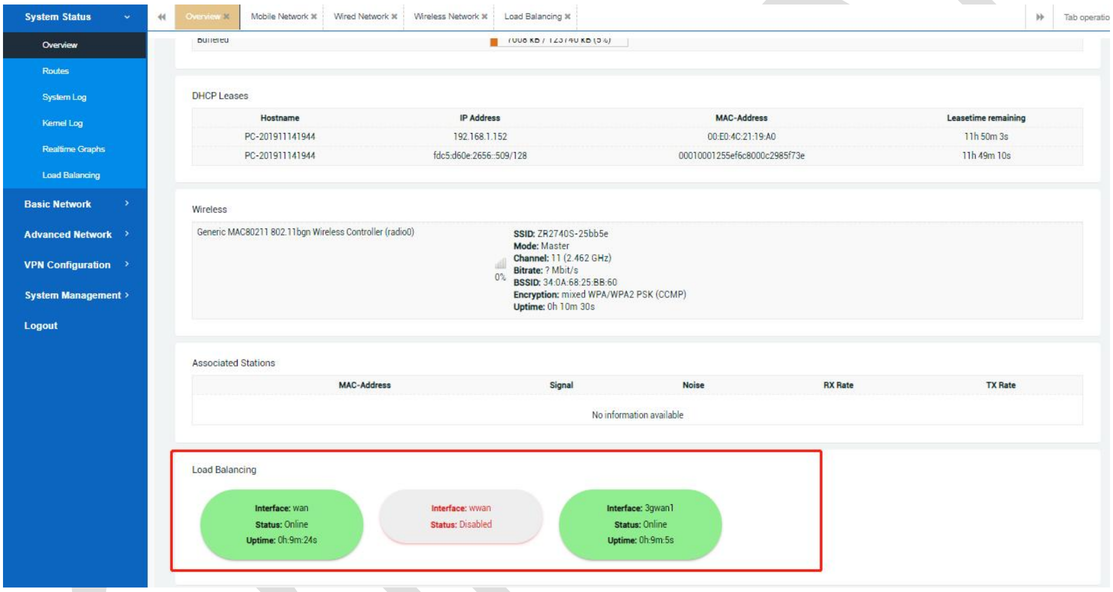
5.10 Load Balancing (optional)

The load balancing function (MWAN3) is mainly to deploy the interface traffic of different network interfaces of the router system (such as wired WAN, 3G/4G mobile network, WiFi client, etc.) according to certain policy rules, mainly including traffic balancing or switching backup.

The overall features of load balancing will be described below.

Note: For scenarios that use virtual private network functions (such as PPTP/2LTP/IPSEC, etc.), please turn off the device load balancing function to avoid causing the virtual private network to fail.

Load balancing is enabled by default in the system (different versions, different), select "System Status" --- "Overview" to view the real-time status of load balancing, as follows:



Buffered 7008 KB / 123740 KB (5%)

DHCP Leases

Hostname	IP Address	MAC-Address	Leasetime remaining
PC-201911141944	192.168.1.152	00:E0:4C:21:19:A0	11h 50m 3s
PC-201911141944	fdc5:d60e:2656::509/128	00010001255ef6c8000c2985f73e	11h 49m 10s

Wireless

Generic MAC80211 802.11bgn Wireless Controller (radio0)

0%

SSID: ZR2740S-25bb5e
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: ? Mbit/s
BSSID: 34:0A:68:25:BB:60
Encryption: mixed WPA/WPA2 PSK (CCMP)
Uptime: 0h 10m 30s

Associated Stations

MAC-Address	Signal	Noise	RX Rate	TX Rate
No information available				

Load Balancing

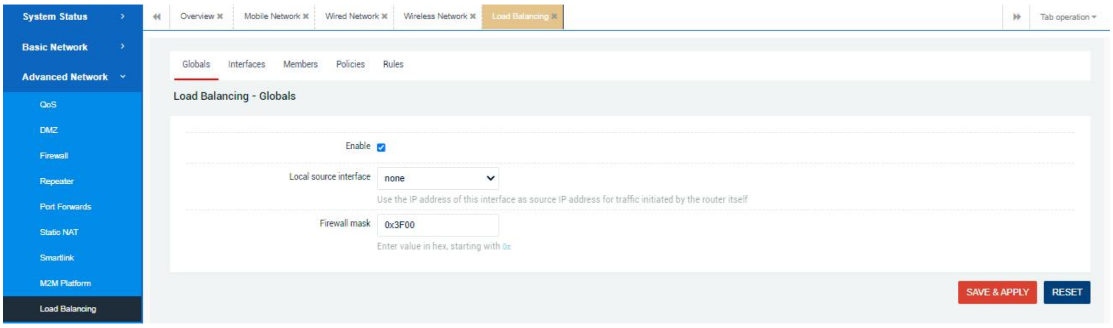
Interface: wan
Status: Online
Uptime: 0h:9m:24s

Interface: wwan
Status: Disabled

Interface: 3gwan1
Status: Online
Uptime: 0h:9m:5s

5.10.1 Global

Click the "Advanced Network" --- "Load Balancing" --- "Global" tab, which can be used to enable or disable the load balancing function (not enabled by default), as follows:



Load Balancing - Globals

Enable ☑

Local source interface: none

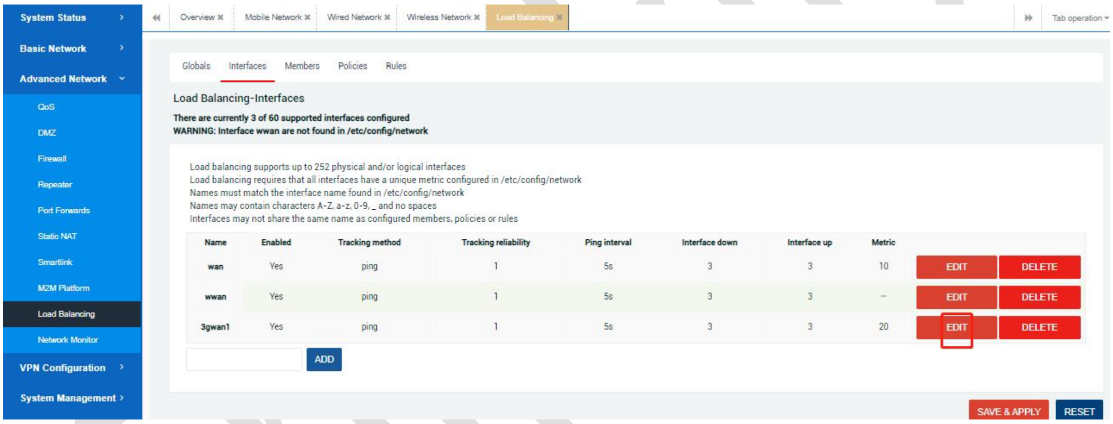
Use the IP address of this interface as source IP address for traffic initiated by the router itself

Firewall mask: 0x3F00

Enter value in hex, starting with 0x

5.10.2 Interface

Click the "Advanced Network" --- "Load Balancing" --- "Interface" tab to configure specific interface parameters. You can also add other interfaces by clicking the "Add" button in the lower left corner. After clicking "Edit", you can configure and modify the parameters as follows:

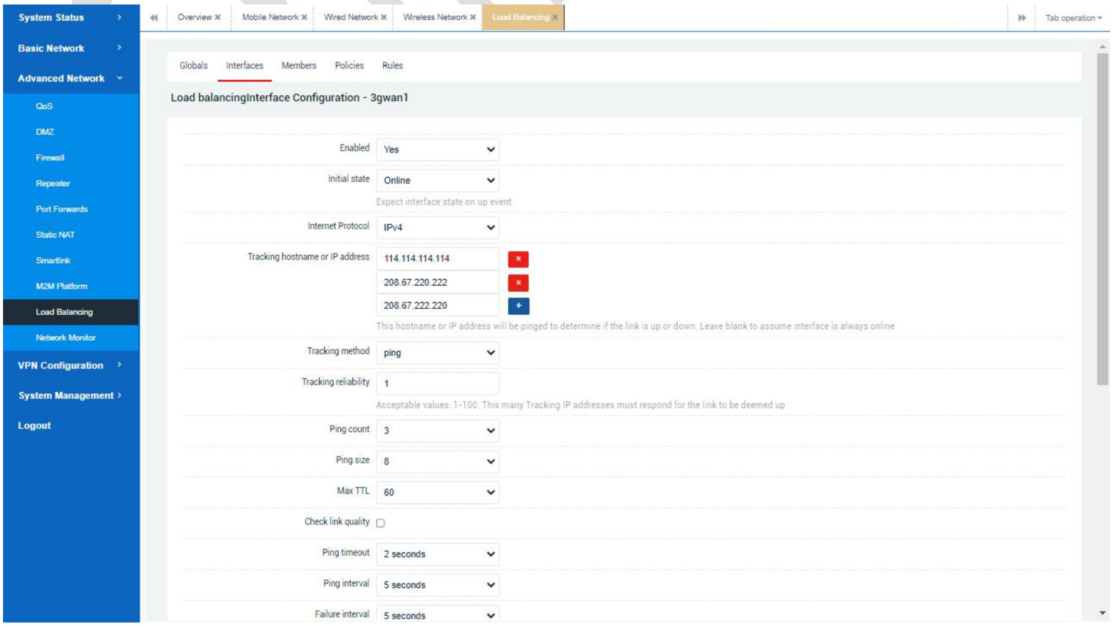


Load Balancing-Interfaces

There are currently 3 of 60 supported interfaces configured
WARNING: Interface wwan are not found in /etc/config/network

Load balancing supports up to 252 physical and/or logical interfaces
Load balancing requires that all interfaces have a unique metric configured in /etc/config/network
Names must match the interface name found in /etc/config/network
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Interfaces may not share the same name as configured members, policies or rules

Name	Enabled	Tracking method	Tracking reliability	Ping interval	Interface down	Interface up	Metric		
wan	Yes	ping	1	5s	3	3	10	EDIT	DELETE
wwan	Yes	ping	1	5s	3	3	–	EDIT	DELETE
3gwan1	Yes	ping	1	5s	3	3	20	EDIT	DELETE



Load balancingInterface Configuration - 3gwan1

Enabled: Yes

Initial state: Online

Expect interface state on up event

Internet Protocol: IPv4

Tracking hostname or IP address: 114.114.114.114 / 208.67.220.222 / 208.67.222.220

This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online

Tracking method: ping

Tracking reliability: 1

Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up

Ping count: 3

Ping size: 8

Max TTL: 60

Check link quality □

Ping timeout: 2 seconds

Ping interval: 5 seconds

Failure interval: 5 seconds

[Enable]: Whether to enable interface detection, it is enabled by default.

[Initial state]: Select the state of the interface during initial detection, such as online or offline.

[Internet Protocol]: Optional IPv4, IPv6, default IPv4.

[Tracked host or IP address]: Use ping to detect the destination host to determine whether the device's external network access is normal, and then to further determine whether the interface is online or offline, which is generally a public network or a valid IP.

[Tracking mode]: Ping mode is selected by default.

[Tracking reliability]: Specify how many IP addresses can be pinged when the interface will be considered online, and the default is one.

[Ping count]: the number of times of ping detection.

[Ping size]: The size of the data packet detected by ping, the default is 8 bytes.

[Ping timeout]: How long does it take to ping the external network or there is no response when it is considered as a timeout.

[Ping interval]: How often do you ping the destination host IP.

[Fault detection interval]: The ping interval during fault detection, the default is 5s.

[Failure Recovery Interval]: The ping interval during failure recovery, the default is 5s.

[Interface offline]: When the number of Ping failures reaches this value, the interface will be considered offline, 3 times by default.

[Interface online]: When the number of successful pings reaches this value, the interface that has been considered offline will be

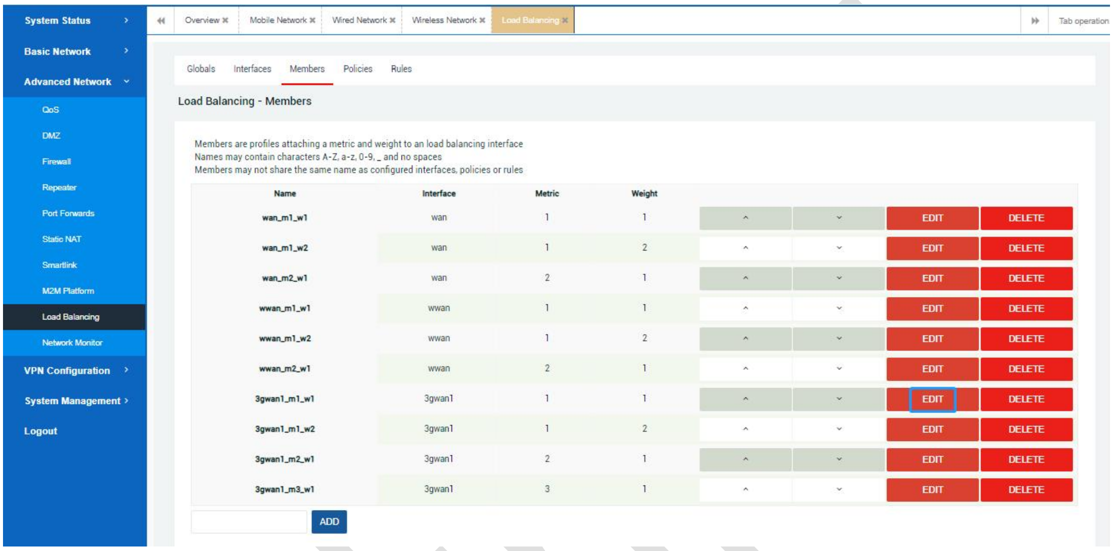
Go online again, 3 times by default.

[Refresh Interval Connection Table]: Refresh the global firewall connection tracking table when an interface event is triggered, which is enabled by default.

[Metrics]: Shows the metric of this interface in the configuration.

5.10.3 Member

Click the "Members" tab to view or add the members corresponding to each interface and configure different metric and weight. The system presets 6 member properties by default, as follows:

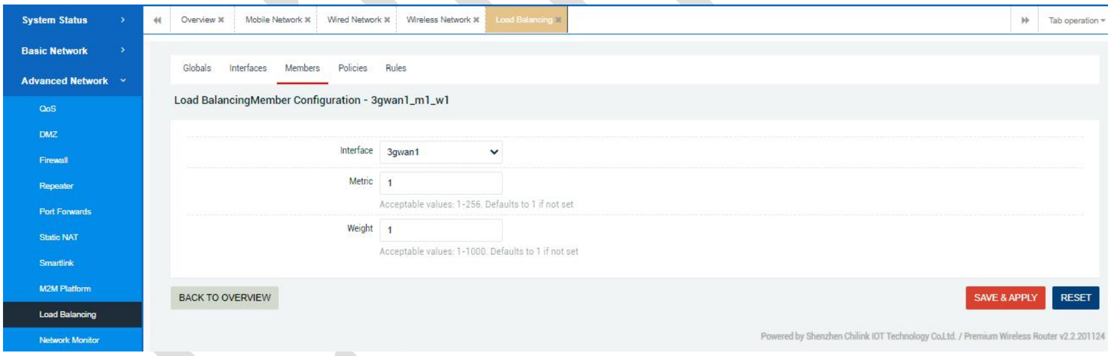


Load Balancing - Members

Members are profiles attaching a metric and weight to an load balancing interface
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Members may not share the same name as configured interfaces, policies or rules

Name	Interface	Metric	Weight				
wan_m1_w1	wan	1	1	˄	˅	EDIT	DELETE
wan_m1_w2	wan	1	2	˄	˅	EDIT	DELETE
wan_m2_w1	wan	2	1	˄	˅	EDIT	DELETE
wwan_m1_w1	wwan	1	1	˄	˅	EDIT	DELETE
wwan_m1_w2	wwan	1	2	˄	˅	EDIT	DELETE
wwan_m2_w1	wwan	2	1	˄	˅	EDIT	DELETE
3gwan1_m1_w1	3gwan1	1	1	˄	˅	EDIT	DELETE
3gwan1_m1_w2	3gwan1	1	2	˄	˅	EDIT	DELETE
3gwan1_m2_w1	3gwan1	2	1	˄	˅	EDIT	DELETE
3gwan1_m3_w1	3gwan1	3	1	˄	˅	EDIT	DELETE

ADD



Load BalancingMember Configuration - 3gwan1_m1_w1

Interface: 3gwan1

Metric: 1
Acceptable values: 1-256. Defaults to 1 if not set

Weight: 1
Acceptable values: 1-1000. Defaults to 1 if not set

BACK TO OVERVIEW

SAVE & APPLY

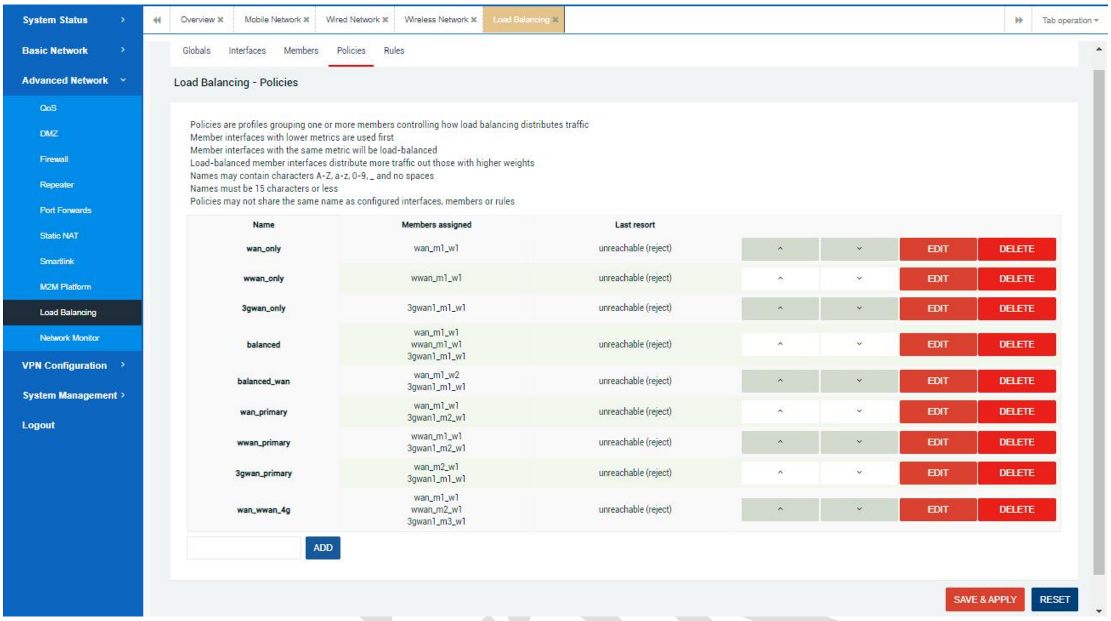
RESET

Powered by Shenzhen Chilink IOT Technology Co.Ltd. / Premium Wireless Router v2.2.201124

5.10.4 Strategy

This function is used to group members and tell MWAN how to distribute the traffic that uses this strategy in the "rule". Members with a lower metric will be used first, members with the same metric will load balance traffic, and members with a higher proportion will be allocated more traffic.

Click the "Strategy" tab to configure different policy rules based on the "Members" set in the previous step. There are 9 preset policies by default in the system, which are described as follows:



Load Balancing - Policies

Policies are profiles grouping one or more members controlling how load balancing distributes traffic
Member interfaces with lower metrics are used first
Member interfaces with the same metric will be load-balanced
Load-balanced member interfaces distribute more traffic out those with higher weights
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Names must be 15 characters or less
Policies may not share the same name as configured interfaces, members or rules

Name	Members assigned	Last resort				
wan_only	wan_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
wwan_only	wwan_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
3gwan_only	3gwan1_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
balanced	wan_m1_w1 wwan_m1_w1 3gwan1_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
balanced_wan	wan_m1_w2 3gwan1_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
wan_primary	wan_m1_w1 3gwan1_m2_w1	unreachable (reject)	^	˅	EDIT	DELETE
wwan_primary	wwan_m1_w1 3gwan1_m2_w1	unreachable (reject)	^	˅	EDIT	DELETE
3gwan_primary	wan_m2_w1 3gwan1_m1_w1	unreachable (reject)	^	˅	EDIT	DELETE
wan_wwan_4g	wan_m1_w1 wwan_m2_w1 3gwan1_m3_w1	unreachable (reject)	^	˅	EDIT	DELETE

5.10.4.1 wan_only

Refers to using only the wan wired network (ignoring whether the 3G/4G SIM card or wireless WiFi network is normal);

5.10.4.2 wwan_only

Refers to only using WiFi network (no matter whether the wan wired network, 3G/4G SIM card is normal or not, it is ignored);

5.10.4.3 3gwan_only

Refers to dial-up network using only 3G/4G SIM card (ignoring whether the wired wan network or wireless WiFi is normal);

5.10.4.4 balanced

Refers to the simultaneous use of wan wired network, wireless WiFi network and 3G/4G SIM card dial-up network; the default traffic ratio of the three is 1:1:1, which can be modified in detail;

5.10.4.5 balanced_wan

Refers to the simultaneous use of wan wired network and 3G/4G wireless SIM card dial-up network; the default traffic ratio between the two is wan:3gwan1=2:1, which can be modified in detail;

5.10.4.6 wan_primary

Refers to wan wired network priority, 3G/4G wireless SIM card dial-up network backup; when the wan cable is abnormal or faulty, the network automatically detects and switches to the 3G/4G wireless network, and after the wan network is restored, the network traffic is automatically detected and switched to wan cable .

5.10.4.7 wwan_primary

Refers to the wireless WiFi network priority, 3G/4G SIM card dial-up network backup; when the wireless WiFi is abnormal or faulty, the network automatically detects and switches to the 3G/4G network, and when the WiFi network is restored, the network traffic automatically detects and switches to the wireless WiFi.

5.10.4.8 3gwan_primary

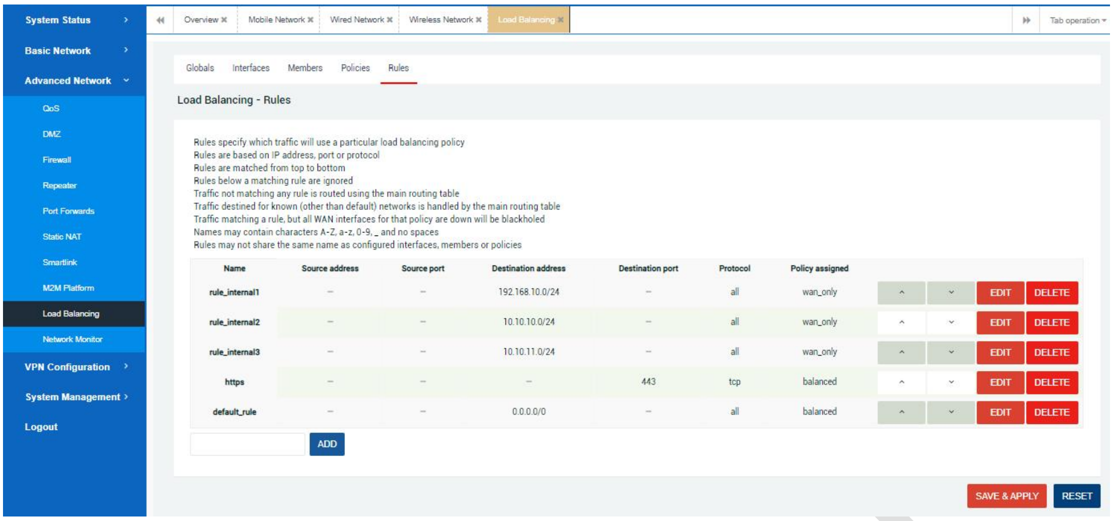
Refers to 3G/4G wireless dial-up network priority, wan wired network backup; when the 3G/4G dial-up network is abnormal or faulty, the network will automatically detect and switch to the wan wired network, and when the 3G/4G dial-up network is restored, the network traffic will automatically detect and switch again go back.

5.10.4.9 wan_wwan_4G

Refers to the wan wired network first, wireless WiFi backup, 3G/4G dial-up second; when the wan wired network is abnormal or faulty, the network automatically detects and switches to the wireless WiFi network, and when the wireless WiFi network is also abnormal or faulty, the network automatically detects and switches to 3G/4G dial-up network. At the same time, when the wireless WiFi network is restored, the network traffic is automatically detected and switched back, and when the wan wired network is also restored, the network traffic is automatically detected and switched back.

5.10.5 Rule

Click the "Rule" tab, the system will take effect according to the "policies" set in the previous step. The system default rule default_rule is balanced, that is, the wired WAN network and the 3G/4 wireless dial-up network can access traffic at the same time. Set other default_rule rules in the actual situation (6 strategies preset by the system can be selected. After selection, the 2 parameter allocation strategies shown below need to be modified to the selected strategy at the same time). as follows:



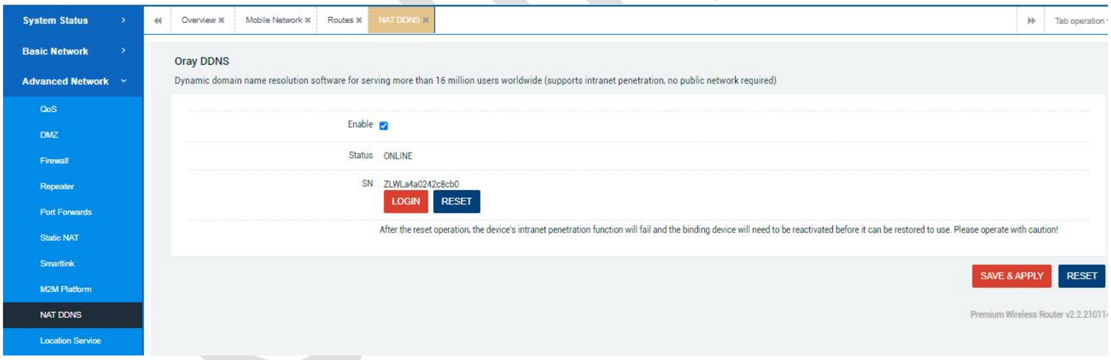
Load Balancing - Rules

Rules specify which traffic will use a particular load balancing policy
Rules are based on IP address, port or protocol
Rules are matched from top to bottom
Rules below a matching rule are ignored
Traffic not matching any rule is routed using the main routing table
Traffic destined for known (other than default) networks is handled by the main routing table
Traffic matching a rule, but all WAN interfaces for that policy are down will be blackholed
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Rules may not share the same name as configured interfaces, members or policies

Name	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned				
rule_internal1	–	–	192.168.10.0/24	–	all	wan_only	^	˅	EDIT	DELETE
rule_internal2	–	–	10.10.10.0/24	–	all	wan_only	^	˅	EDIT	DELETE
rule_internal3	–	–	10.10.11.0/24	–	all	wan_only	^	˅	EDIT	DELETE
https	–	–	–	443	tcp	balanced	^	˅	EDIT	DELETE
default_rule	–	–	0.0.0.0/0	–	all	balanced	^	˅	EDIT	DELETE

5.11Intranet penetration (optional)

The peanut shell software is embedded in the router device, which is mainly used for the peanut shell intranet penetration function, which is convenient for remotely accessing the equipment connected to the router through the account server registered on the peanut shell official website.



Oray DDNS

Dynamic domain name resolution software for serving more than 16 million users worldwide (supports intranet penetration, no public network required)

Enable ☑

Status ONLINE

SN ZLWLa4a0242c8cb0

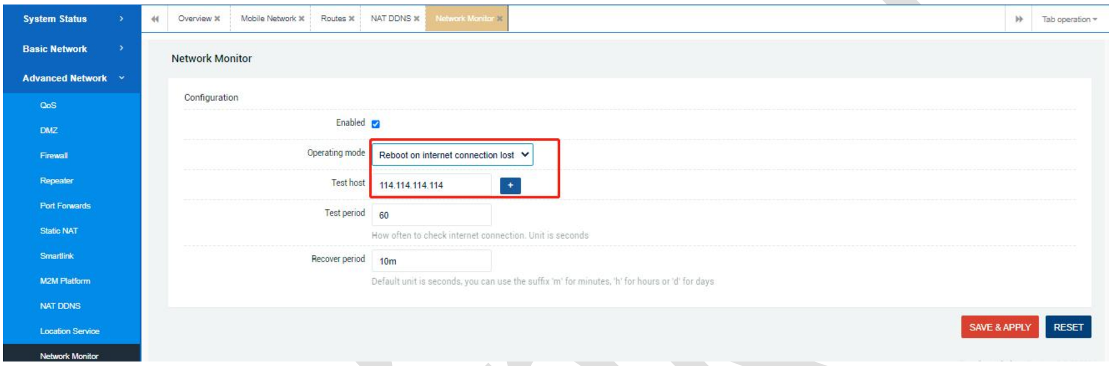
After the reset operation, the device's intranet penetration function will fail and the binding device will need to be reactivated before it can be restored to use. Please operate with caution!

5.12 Network Monitoring

This function (enabled by default in subsequent versions) periodically detects and judges the continuity of the device's own network by setting specific conditions (2 conditions), thereby performing specific actions (such as restarting, etc.). details as follows:

1）Restart after disconnection

This condition sets the device to periodically ping to detect the IP address of a specific network host (the default interval is 60s, and the period is 10min), and determines whether to restart the device by judging whether the network is on or off.



Network Monitor

Configuration

Enabled ☑

Operating mode: Reboot on internet connection lost

Test host: 114.114.114.114 +

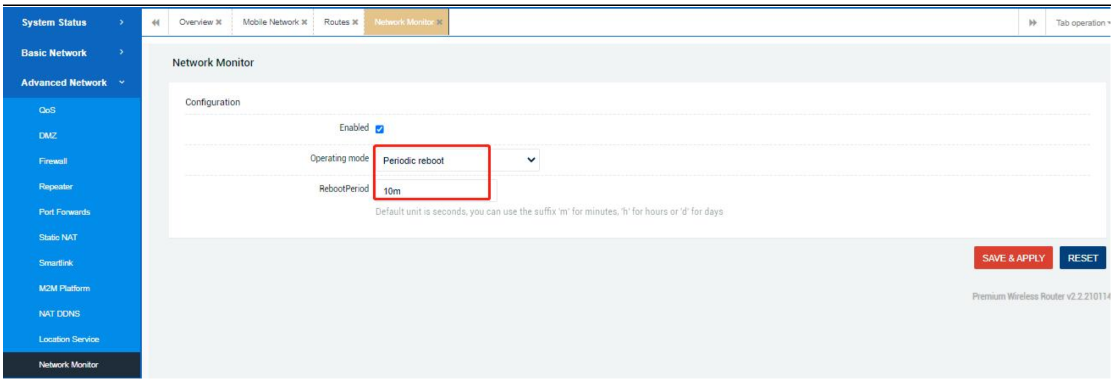
Test period: 60
How often to check internet connection. Unit is seconds

Recover period: 10m
Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

Note: For the scenario where the VPDN private network is used or the device's own network is not allowed to access the external network, you need to modify the ping host address to be a valid address, or disable the network monitoring function, otherwise the device will periodically restart abnormally.

2）Periodic restart

Set periodic/timed restart for the device (default is 10min).



Network Monitor

Configuration

Enabled ☑

Operating mode: Periodic reboot

RebootPeriod: 10m

Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

6.Virtual Private Network

This chapter mainly introduces several different virtual private network functions and simple configuration and use. The virtual private network function is generally used to build a remote local area network between the user's field device network and the server network or different device network with different data transmission methods (such as PPTP/L2TP) or encryption strength (such as IPSec/Openvpn) , To facilitate better and faster remote access and control of remote devices.

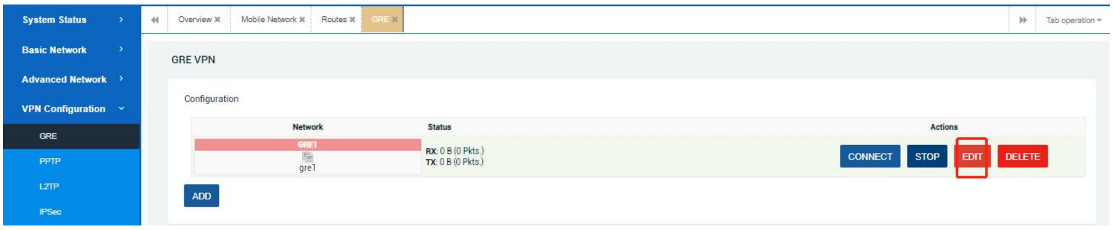
Note: For scenarios that use virtual private network functions (such as PPTP/2LTP/IPSEC, etc.), please turn off the device load balancing function to avoid causing the virtual private network to fail.

6.1 GRE Client

The premise of the main use scenario of the GRE network is that different nodes with access attributes of the public network or VPDN private network can realize mutual access communication between the subnet devices under the different nodes through the establishment of virtual tunnels.

1) Select "Virtual Private Network" --- "GRE" --- "GRE Tunnel", click the "Edit" button to proceed GRE related configuration, including tunnel source address, tunnel

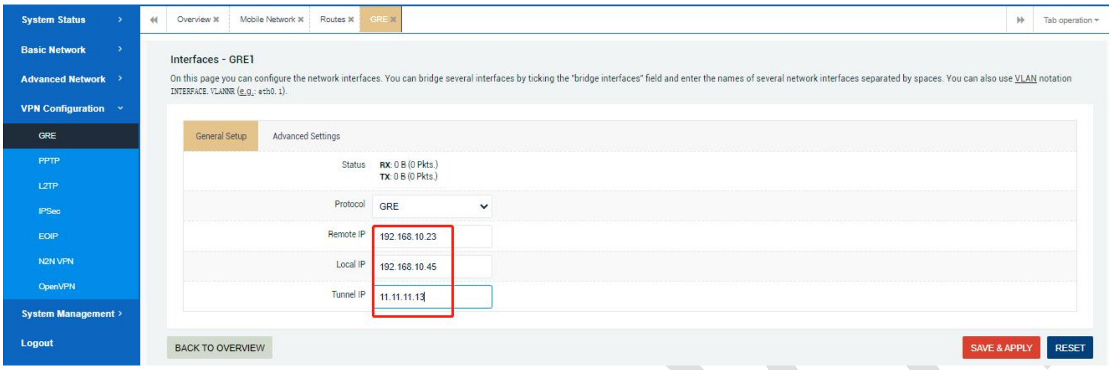
destination address, tunnel address, etc., are as follows:



GRE VPN

Configuration

Network	Status	Actions
GRE1 gre1	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	CONNECT STOP EDIT DELETE



Interfaces - GRE1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status: RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)

Protocol: GRE

Remote IP: 192.168.10.23

Local IP: 192.168.10.45

Tunnel IP: 11.11.11.13

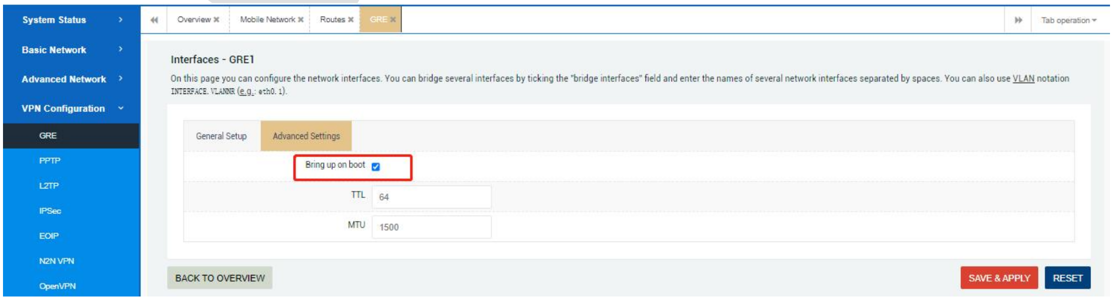
Among them, the description of each parameter is as follows:

[Tunnel destination address]: Fill in the public network IP address of the opposite router, this example is the LAN WAN port address 192.168.10.23;

[Tunnel source address]: Fill in the public network IP address of the local router, this example is the local LAN WAN port address 192.168.10.45;

[Tunnel Address]: Fill in the virtual tunnel IP address of the local router, here is 11.11.11.13 (the opposite tunnel address is 11.11.11.14) as an example;

2) Set up the "Autostart" service as follows:



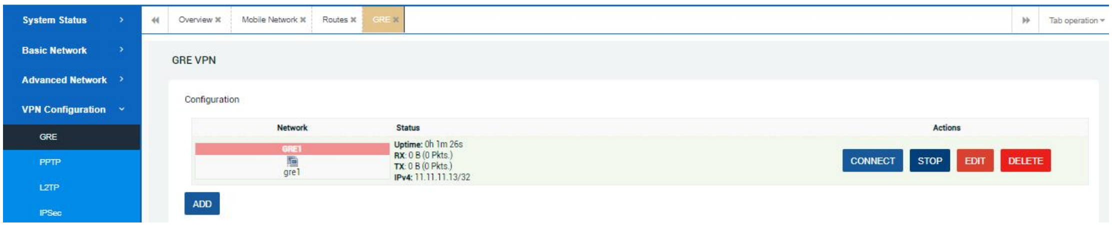
Interfaces - GRE1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Bring up on boot ☑

TTL: 64

MTU: 1500

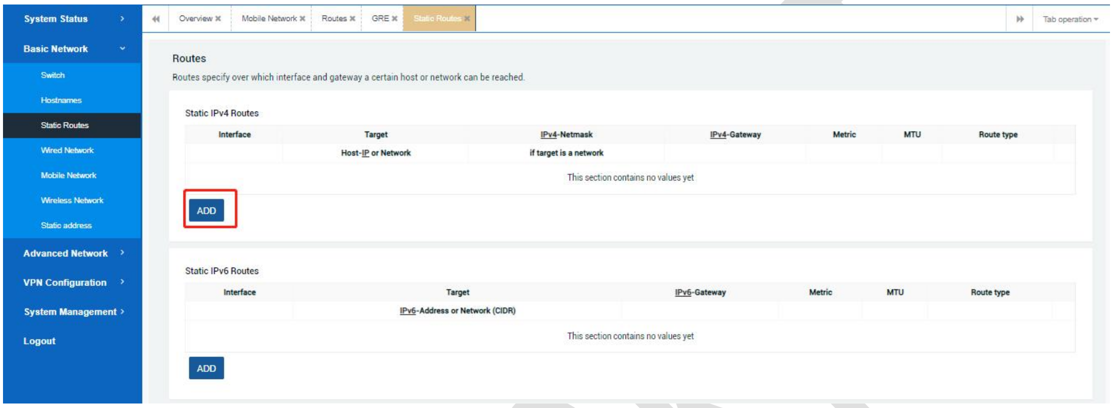


GRE VPN

Configuration

Network	Status	Actions
GRE1 gre1	Uptime: 0h 1m 26s RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.) IPv4: 11.11.11.13/32	CONNECT STOP EDIT DELETE

3) Take the local router subnet (192.168.3.0/24 as an example) to add the static routing table of the peer router network segment (take 192.168.4.0/24 as an example), as follows:



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

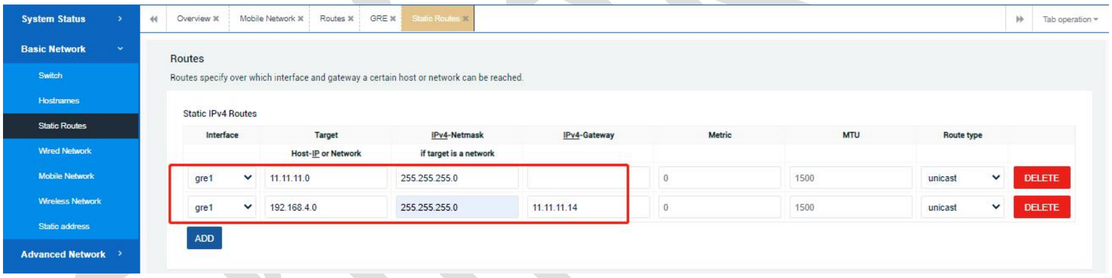
Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	Route type

This section contains no values yet

Static IPv6 Routes

Interface	Target IPv6-Address or Network (CIDR)	IPv6-Gateway	Metric	MTU	Route type

This section contains no values yet



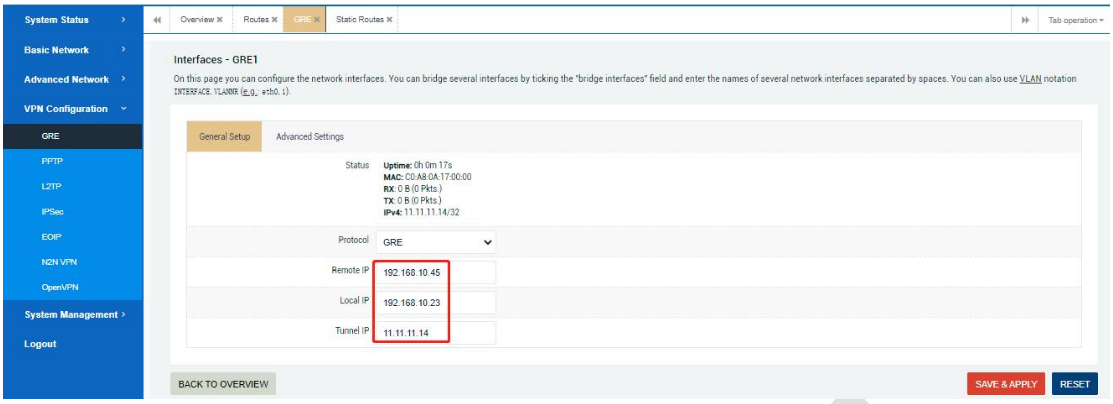
Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	Route type	
gre1	11.11.11.0	255.255.255.0		0	1500	unicast	DELETE
gre1	192.168.4.0	255.255.255.0	11.11.11.14	0	1500	unicast	DELETE

4) Configure the corresponding parameters for GRE on the other router at the opposite end, as follows:



Interfaces - GRE1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

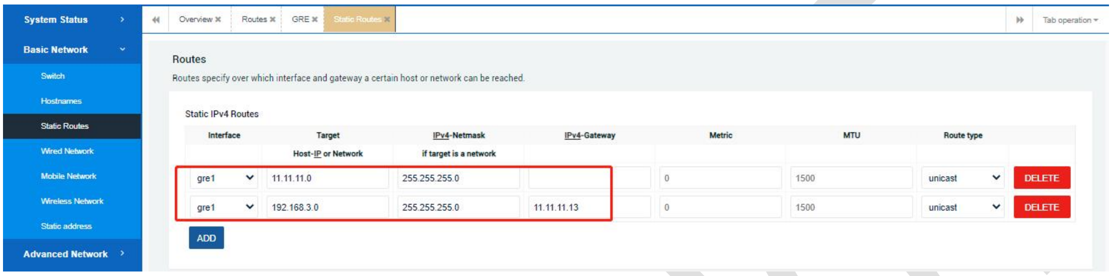
Status
Uptime: 0h 0m 17s
MAC: C0:A8:0A:17:00:00
RX: 0 B (0 Pkts.)
TX: 0 B (0 Pkts.)
IPv4: 11.11.11.14/32

Protocol: GRE

Remote IP: 192.168.10.45

Local IP: 192.168.10.23

Tunnel IP: 11.11.11.14



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	Route type	
	Host-IP or Network	if target is a network					
gre1	11.11.11.0	255.255.255.0		0	1500	unicast	DELETE
gre1	192.168.3.0	255.255.255.0	11.11.11.13	0	1500	unicast	DELETE

6.2 PPTP Client

The PPTP network is mainly used to connect different client router devices or PC computer clients to the VPN server through PPTP protocol dial-up configuration to achieve the following two main usage scenarios.

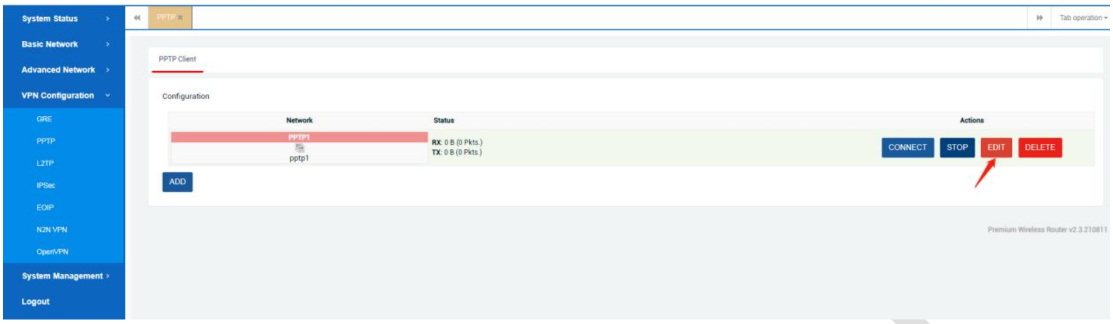
Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The schematic diagram is as follows:

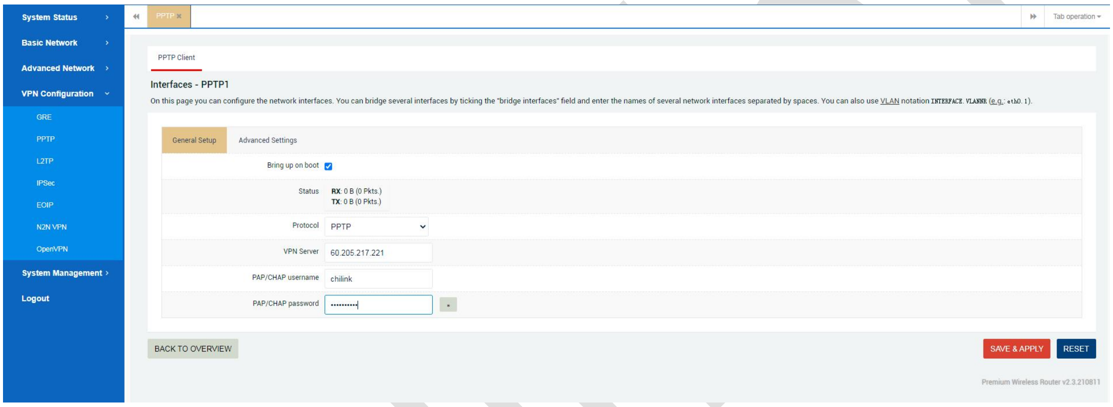
Specific operation: Select "Virtual Private Network" --- "PPTP" --- "PPTP Client", click the "Edit" button to configure specific parameters, as follows:

1) Select "Basic Settings" to start configuring server parameters and client account, password and other information, as follows:



Configuration

Network	Status	Actions
PPTP1 pptp1	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	CONNECT STOP EDIT DELETE



Interfaces - PPTP1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

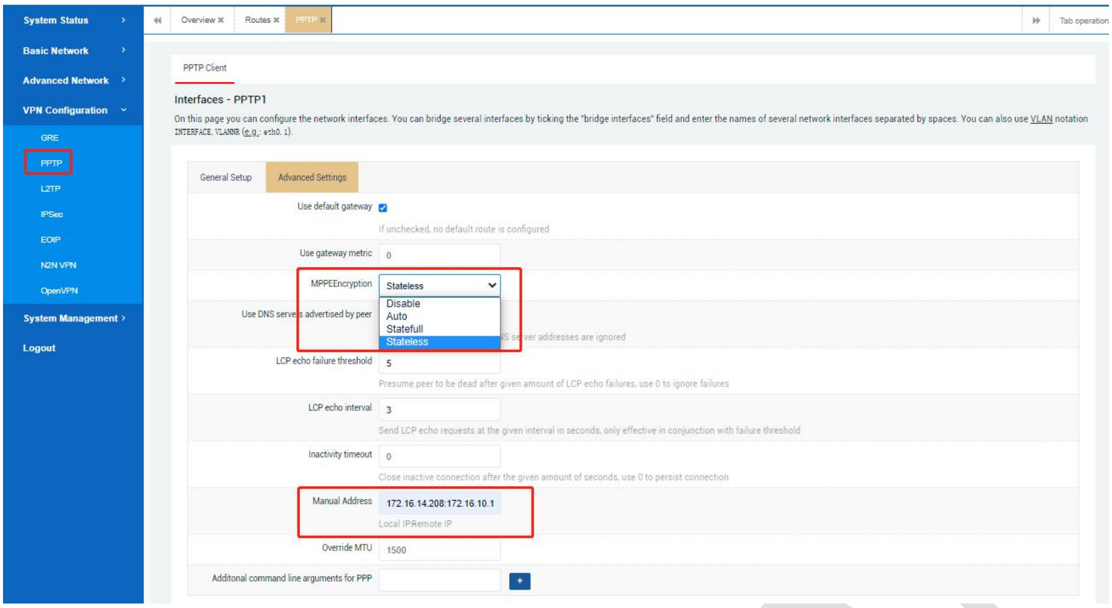
Bring up on boot	☑
Status	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)
Protocol	PPTP
VPN Server	60.205.217.221
PAP/CHAP username	chilink
PAP/CHAP password	••••••••••

[Startup]: After checking, the router will automatically start and connect to the PPTP service every time it restarts

[VPN server]: Fill in the IP address of the remote server, generally the public network IP address;

[PAP/CHAP username, password]: Fill in the client account and password assigned by the VPN server;

2）Select "Advanced Settings" to configure some specific advanced parameters, as follows:



Interfaces - PPTP1

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE. VLANNR (e.g.: eth0. 1).

Use default gateway ☑
If unchecked, no default route is configured

Use gateway metric: 0

MPPEEncryption: Stateless

Use DNS servers advertised by peer
…S server addresses are ignored

LCP echo failure threshold: 5
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval: 3
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout: 0
Close inactive connection after the given amount of seconds, use 0 to persist connection

Manual Address: 172.16.14.208:172.16.10.1
Local IP:Remote IP

Override MTU: 1500

Additonal command line arguments for PPP

[Use default gateway]: After checking, the router can automatically address the server terminal network;

[MPPE encryption]: Fill in the encryption type consistent with the VPN server, otherwise you may not be able to connect to the server;

[LCP response failure threshold]: LCP response times, the default is 5;

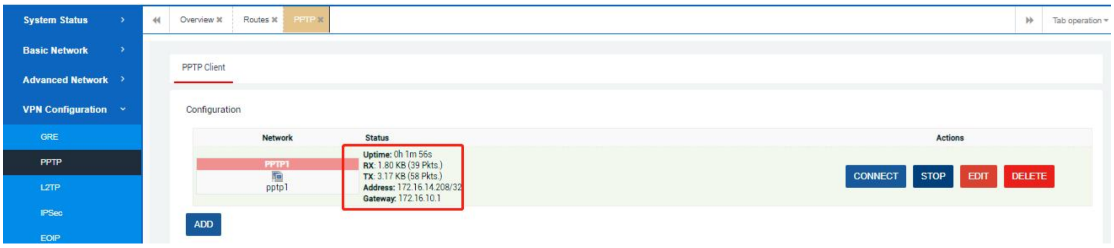
[LCP response interval]: LCP response interval, the default is 3s;

[Activity timeout]: Inactive connection control with the server, the default is 0, which means that continuous connection is supported;

[Manually assign address]: You can specify the VPN address; set the format 172.16.100.2 (client virtual IP): 172.16.100.1 (server gateway virtual IP);

[Additional parameters for PPP]: Customize PPP parameters, such as filling in the debugging command (debug) or specifying the client VPN IP address, etc. (If you need to specify the VPN address, the setting format: 172.16.100.2 (client virtual IP): 172.16. 100.1 (server gateway virtual IP));

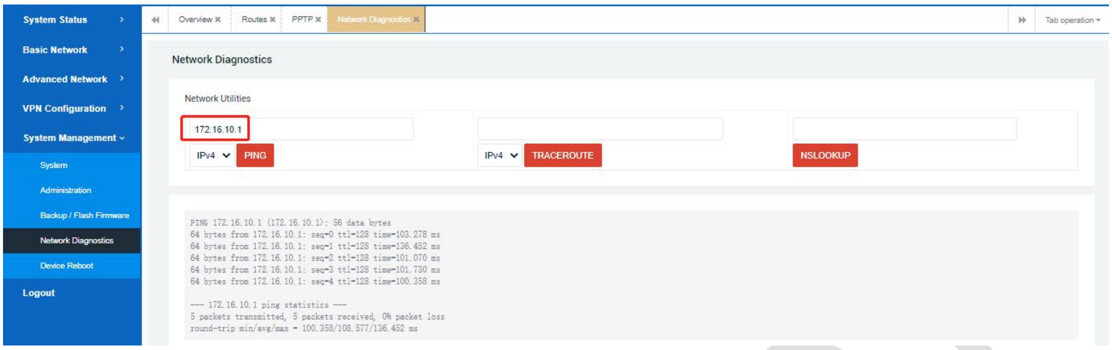
3）The PPTP client connects to the server successfully, as follows:



PPTP Client

Configuration

Network	Status	Actions
PPTP1 pptp1	**Uptime:** 0h 1m 56s **RX:** 1.80 KB (39 Pkts.) **TX:** 3.17 KB (58 Pkts.) **Address:** 172.16.14.208/32 **Gateway:** 172.16.10.1	CONNECT STOP EDIT DELETE



Network Diagnostics

Network Utilities

172.16.10.1 IPv4

```
PING 172.16.10.1 (172.16.10.1): 56 data bytes
64 bytes from 172.16.10.1: seq=0 ttl=128 time=103.278 ms
64 bytes from 172.16.10.1: seq=1 ttl=128 time=136.452 ms
64 bytes from 172.16.10.1: seq=2 ttl=128 time=101.070 ms
64 bytes from 172.16.10.1: seq=3 ttl=128 time=101.730 ms
64 bytes from 172.16.10.1: seq=4 ttl=128 time=100.358 ms

--- 172.16.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 100.358/108.577/136.452 ms
```

6.3 L2TP Client

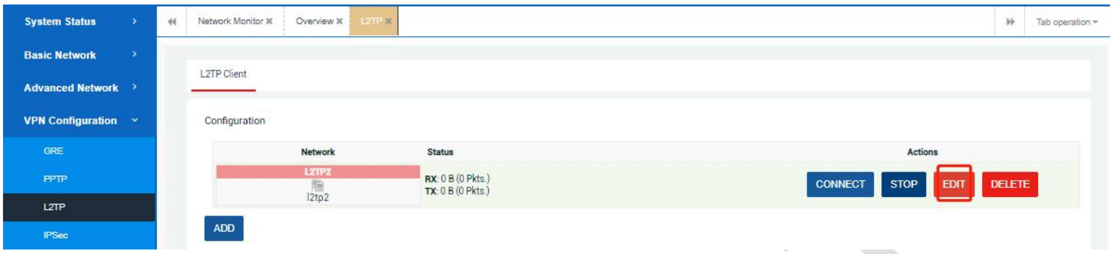
The L2TP network is also mainly used to connect different client router devices or PC computers to the VPN server through the L2TP protocol dial-up configuration to achieve the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The specific configuration is as follows:

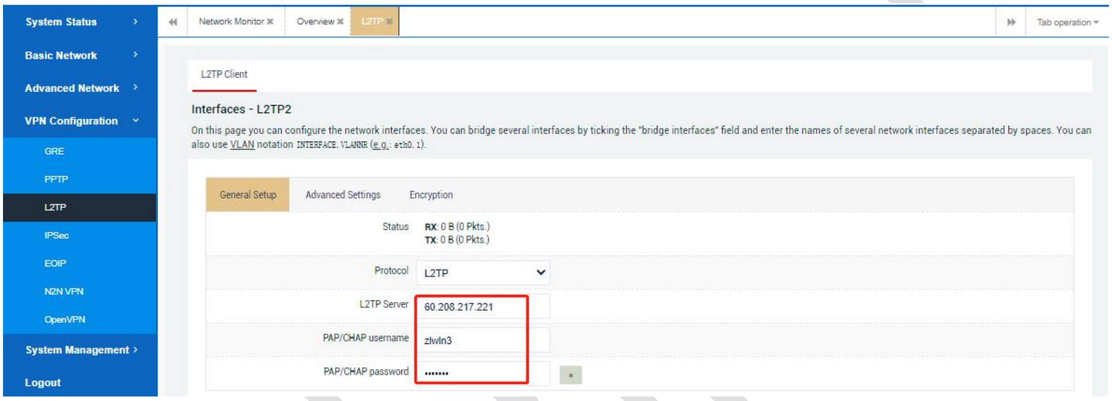
1）Select "Virtual Private Network" --- "L2TP" --- "L2TP Client", click the "Edit" button to perform "Basic Settings", and begin to configure server parameters and client account and password information, as follows:



L2TP Client

Configuration

Network	Status	Actions
L2TP2 l2tp2	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	CONNECT STOP EDIT DELETE



L2TP Client

Interfaces - L2TP2

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Status RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)

Protocol: L2TP

L2TP Server: 60.208.217.221

PAP/CHAP username: zlwln3

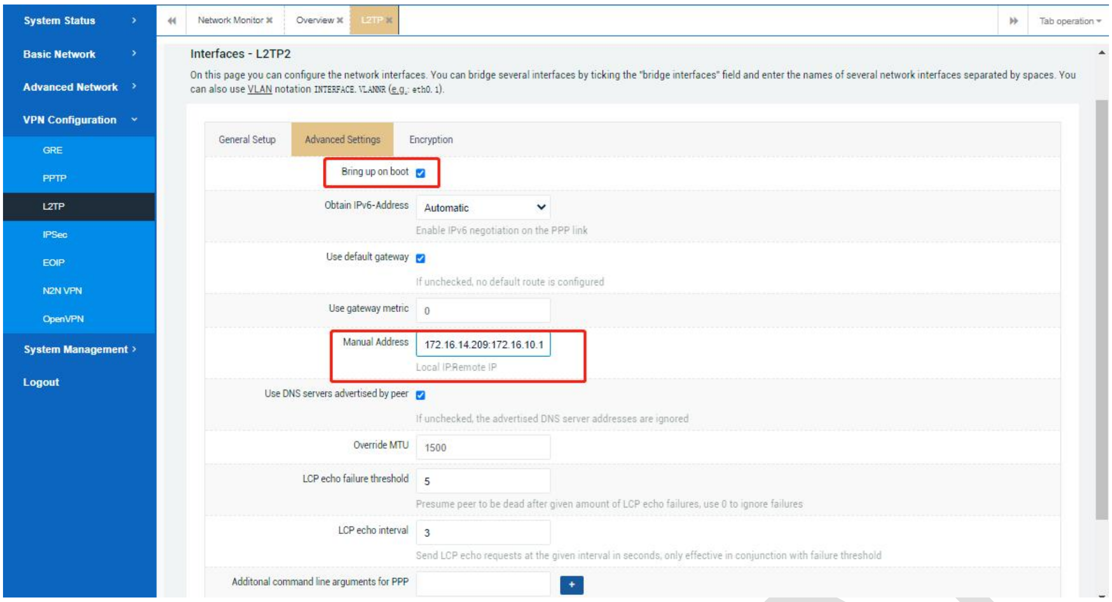
PAP/CHAP password: •••••••

[Protocol]: Default protocol type: L2TP;

[VPN server]: Fill in the IP address of the remote server, generally the public network IP address;

[PAP/CHAP username, password]: Fill in the client account and password assigned by the VPN server;

2）Select "Advanced Settings" to configure some specific advanced parameters, as follows:



Interfaces - L2TP2

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Bring up on boot ☑

Obtain IPv6-Address: Automatic
Enable IPv6 negotiation on the PPP link

Use default gateway ☑
If unchecked, no default route is configured

Use gateway metric: 0

Manual Address: 172.16.14.209:172.16.10.1
Local IP:Remote IP

Use DNS servers advertised by peer ☑
If unchecked, the advertised DNS server addresses are ignored

Override MTU: 1500

LCP echo failure threshold: 5
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval: 3
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Additonal command line arguments for PPP: +

[Startup]: After checking, the router will automatically start and connect to the L2TP service every time it restarts;

[Obtain IPv6 address]: The default is automatic, you can choose to disable or manually;

[Use default gateway]: After checking, the router can automatically address the server terminal network;

[Manually assign address]: You can specify the VPN address; set the format 172.16.100.2 (client address): 172.16.100.1 (VPN server gateway address);

[MPPE encryption]: Fill in the encryption type consistent with the VPN server, otherwise you may not be able to connect to the server;

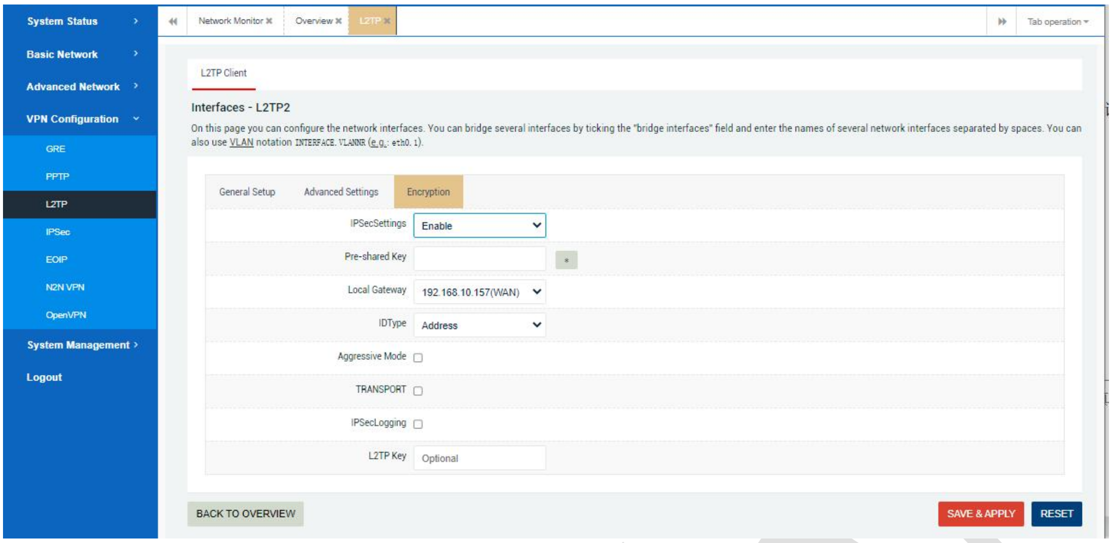
[LCP response failure threshold]: LCP response times, the default is 5;

[LCP response interval]: LCP response interval, the default is 3s;

[Response timeout]: Inactive connection control with the server, the default is 0, which means continuous connection is supported;

[Additional parameters for PPP]: Customize PPP parameters, such as debug, etc.;

3）Select "Encryption Method" to set whether IPSec configuration is enabled (default is none), and the L2TP key is as follows:

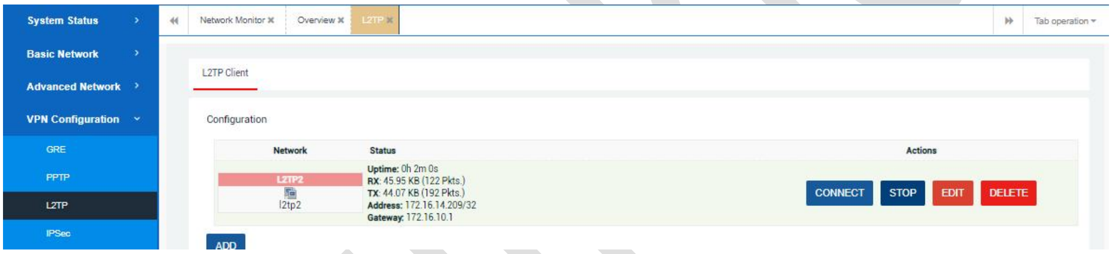


Interfaces - L2TP2

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

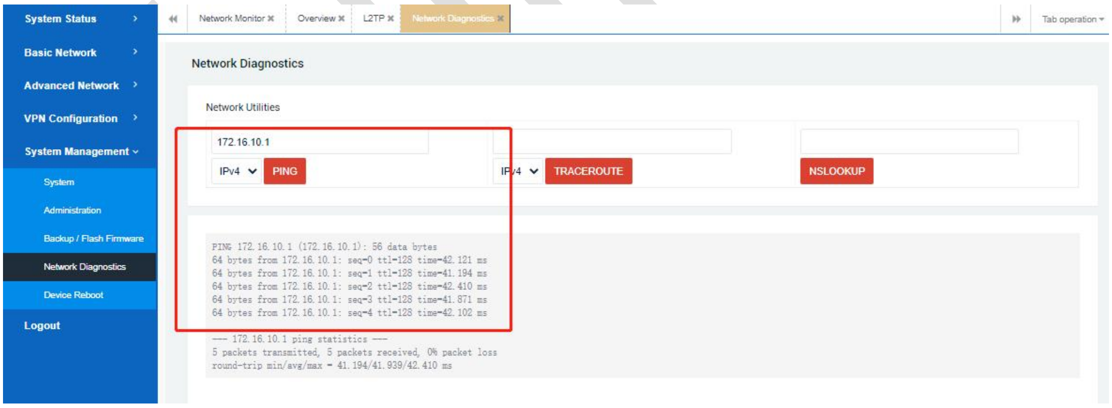
IPSecSettings	Enable
Pre-shared Key	
Local Gateway	192.168.10.157(WAN)
IDType	Address
Aggressive Mode	□
TRANSPORT	□
IPSecLogging	□
L2TP Key	Optional

4）The L2TP client connects to the server successfully, as follows:



Configuration

Network	Status	Actions
L2TP2 l2tp2	**Uptime:** 0h 2m 0s **RX:** 45.95 KB (122 Pkts.) **TX:** 44.07 KB (192 Pkts.) **Address:** 172.16.14.209/32 **Gateway:** 172.16.10.1	CONNECT STOP EDIT DELETE



Network Diagnostics

Network Utilities

172.16.10.1

```
PING 172.16.10.1 (172.16.10.1): 56 data bytes
64 bytes from 172.16.10.1: seq=0 ttl=128 time=42.121 ms
64 bytes from 172.16.10.1: seq=1 ttl=128 time=41.194 ms
64 bytes from 172.16.10.1: seq=2 ttl=128 time=42.410 ms
64 bytes from 172.16.10.1: seq=3 ttl=128 time=41.871 ms
64 bytes from 172.16.10.1: seq=4 ttl=128 time=42.102 ms

--- 172.16.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 41.194/41.939/42.410 ms
```

6.4 IPSec Client

The IPSec network is mainly used to connect different client router devices to the IPSec server through the IPSec protocol dial-up configuration so that the client router subnet devices and the server terminal network devices can communicate with each other at will.

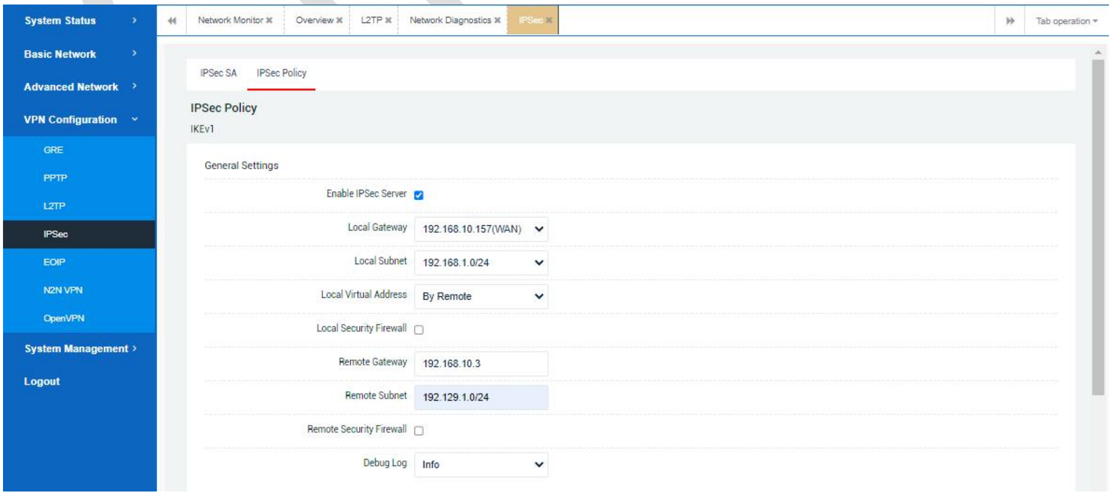
The specific configuration is as follows:

6.4.1 IPSec security strategy

The IPSec security strategy is mainly to set the server-related parameters, and configure the IKE/ESP security proposal, encryption algorithm, national secret SM3 algorithm and other parameter settings of phases 1 and 2 of the entire IPSEC communication.

6.4.1.1 Basic Settings

Select "Virtual Private Network" --- "IPSec" --- "IPSec Security Policy" --- "Basic Settings" to configure specific parameters. Examples are as follows:



IPSec Policy

IKEv1

General Settings

Enable IPSec Server ☑

Local Gateway: 192.168.10.157(WAN)

Local Subnet: 192.168.1.0/24

Local Virtual Address: By Remote

Local Security Firewall ☐

Remote Gateway: 192.168.10.3

Remote Subnet: 192.129.1.0/24

Remote Security Firewall ☐

Debug Log: Info

[Enable IPSec service]: Check whether to enable;

[Local Security Gateway]: Fill in the local 4G dial-up IP interface (3GWAN1), the example is the local interface WAN;

[Local Subnet Range]: Fill in the client's local subnet range;

[Local virtual address]: The default is assigned by the opposite end (you can also choose to customize);

[Local security firewall]: Device local client security firewall parameters, check whether to enable;

[Peer End Security Gateway]: Fill in the server-side gateway IP (usually the public network or domain name address);

[Range of terminal network]: Fill in the range of server terminal network;

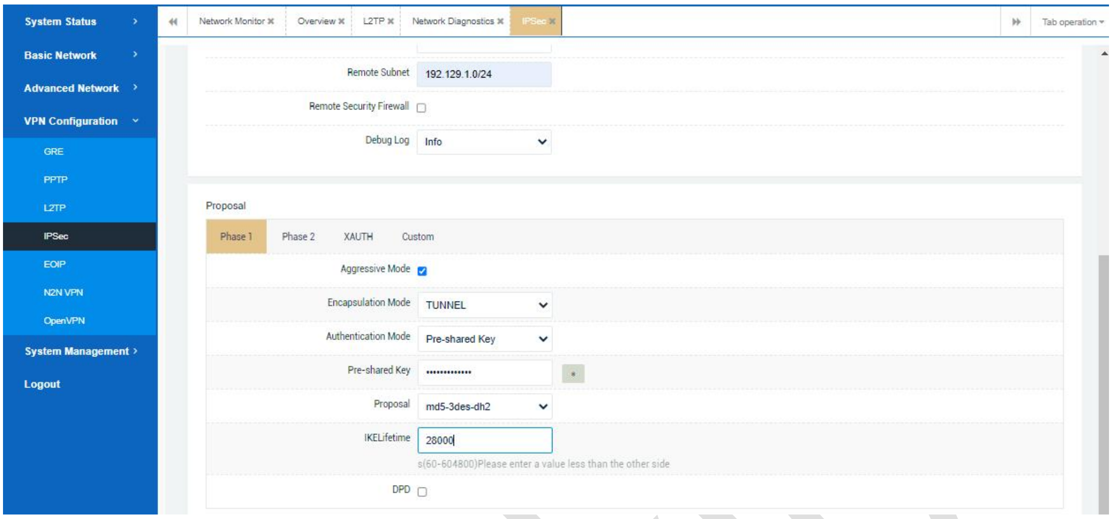
[Peer-end security firewall]: Device server-side security firewall parameters;

[Debug log]: After opening, you can view the specific connection debug log;

6.4.1.1 Security proposal

Select "Virtual Private Network" --- "IPSec" --- "IPSec Security Policy" --- "Basic Settings" drop down to "Security Proposal" to configure specific parameters, as follows:

Phase 1 configuration: Mainly configure parameters such as working mode (aggressive mode/main mode), encapsulation mode (tunnel/transmission mode), pre-shared key, security proposal, IKE lifetime, and DPD peer detection.



Remote Subnet: 192.129.1.0/24

Remote Security Firewall ☐

Debug Log: Info

Proposal

Phase 1 | Phase 2 | XAUTH | Custom

Aggressive Mode ☑

Encapsulation Mode: TUNNEL

Authentication Mode: Pre-shared Key

Pre-shared Key: ••••••••••••

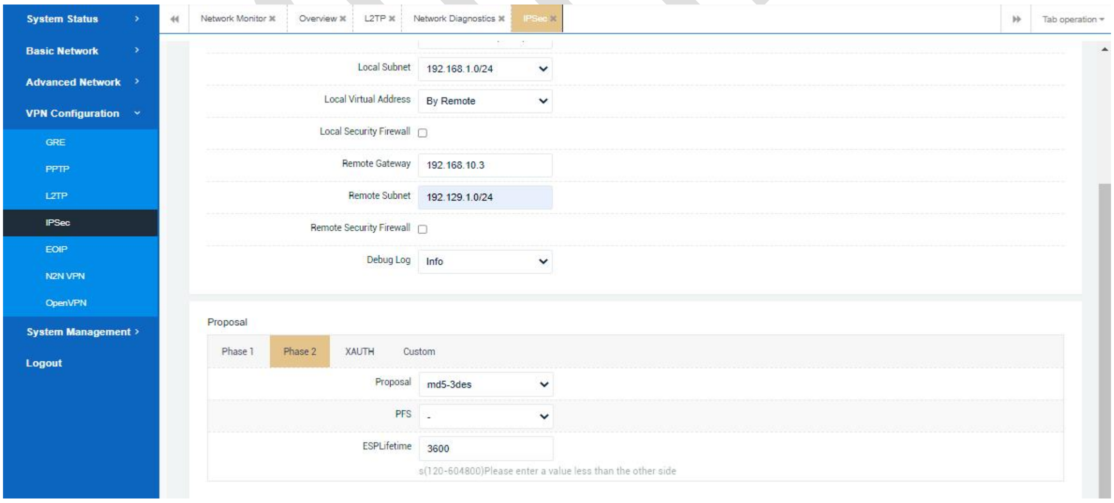
Proposal: md5-3des-dh2

IKELifetime: 28000

s(60-604800)Please enter a value less than the other side

DPD ☐

Phase 2 configuration: Mainly configure the security proposal, PFS parameters, and ESP lifetime of this phase.



Local Subnet: 192.168.1.0/24

Local Virtual Address: By Remote

Local Security Firewall ☐

Remote Gateway: 192.168.10.3

Remote Subnet: 192.129.1.0/24

Remote Security Firewall ☐

Debug Log: Info

Proposal

Phase 1 | Phase 2 | XAUTH | Custom

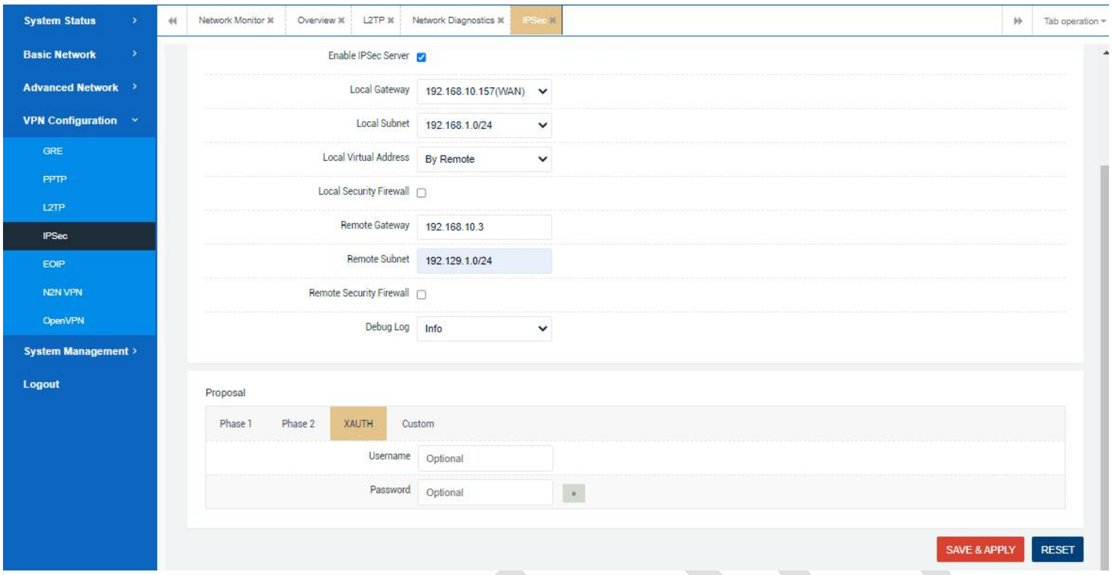
Proposal: md5-3des

PFS: -

ESPLifetime: 3600

s(120-604800)Please enter a value less than the other side

XAUTH (extended authentication) configuration: User name/password can be set.



Enable IPSec Server ☑

Local Gateway: 192.168.10.157(WAN)

Local Subnet: 192.168.1.0/24

Local Virtual Address: By Remote

Local Security Firewall □

Remote Gateway: 192.168.10.3

Remote Subnet: 192.129.1.0/24

Remote Security Firewall □

Debug Log: Info

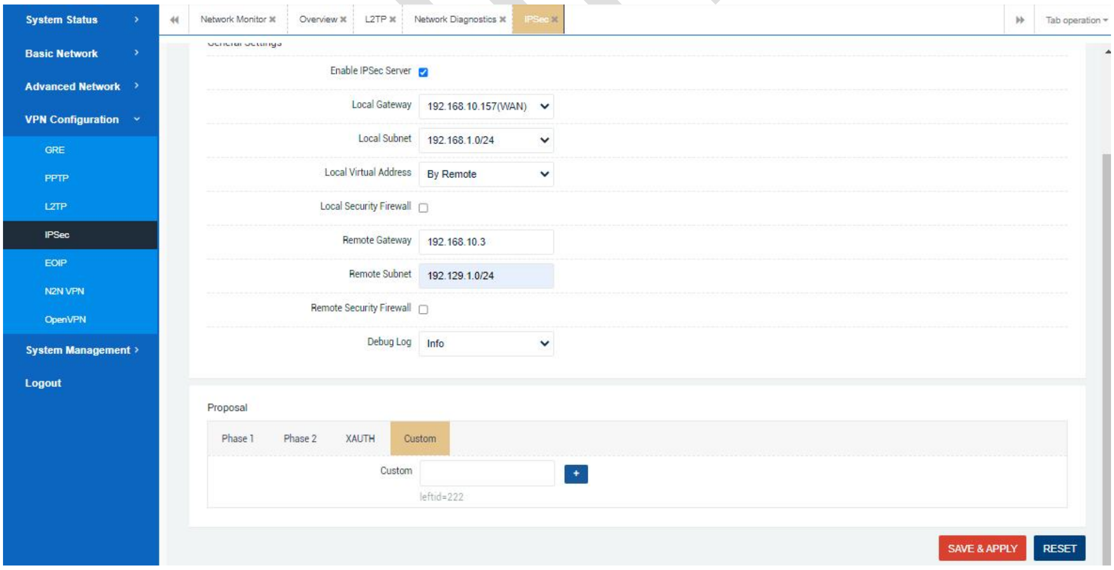
Proposal

Phase 1 | Phase 2 | XAUTH | Custom

Username: Optional

Password: Optional

Custom settings: If both ends of the server-side settings are based on FQIN name ID authentication, you can configure specific authentication parameters, such as leftid (client authentication ID name) and rightid (server authentication ID name).



General Settings

Enable IPSec Server ☑

Local Gateway: 192.168.10.157(WAN)

Local Subnet: 192.168.1.0/24

Local Virtual Address: By Remote

Local Security Firewall □

Remote Gateway: 192.168.10.3

Remote Subnet: 192.129.1.0/24

Remote Security Firewall □

Debug Log: Info

Proposal

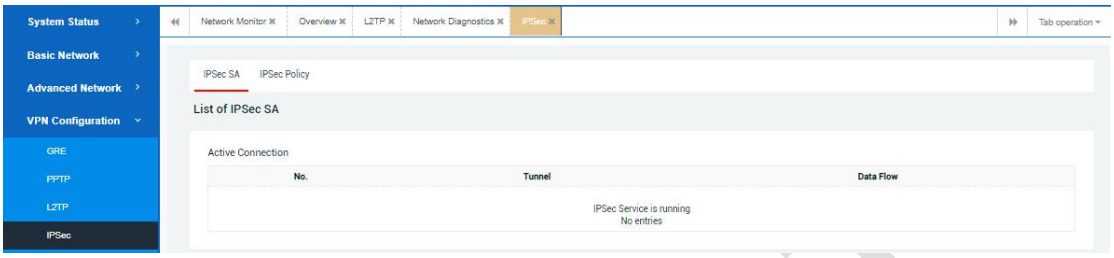
Phase 1 | Phase 2 | XAUTH | Custom

Custom: +

leftid=222

6.4.2 IPSec Security Alliance

Here you can view the tunnel establishment status and data flow at both ends of the IPSec. After the tunnel is successfully established, the following is as follows:



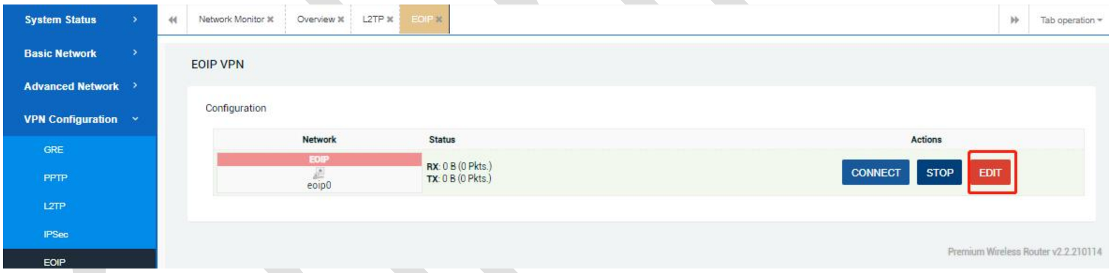
List of IPSec SA

Active Connection

No.	Tunnel	Data Flow
	IPSec Service is running No entries	

6.5 EOIP Client

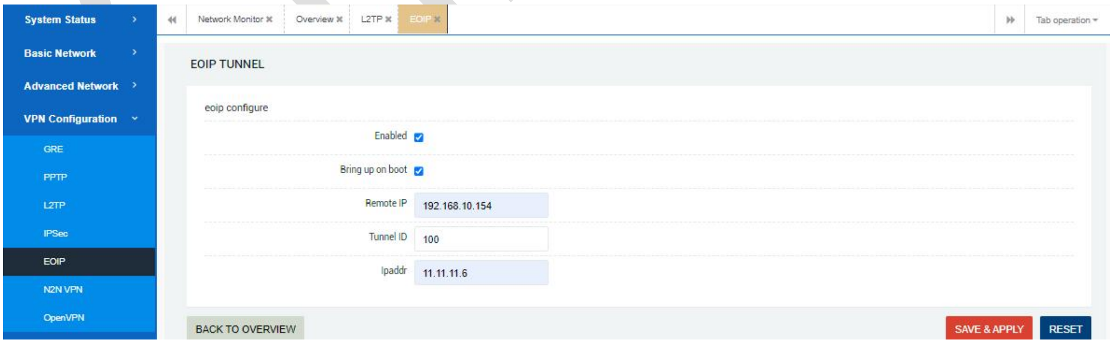
This function is similar to that used by the GRE VPN client, but the authentication parameter here is the tunnel ID (0-500), and the specific configuration refers to the use of GRE VPN. as follows:



EOIP VPN

Configuration

Network	Status	Actions
EOIP eoip0	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	CONNECT STOP EDIT



EOIP TUNNEL

eoip configure

Enabled	☑
Bring up on boot	☑
Remote IP	192.168.10.154
Tunnel ID	100
Ipaddr	11.11.11.6

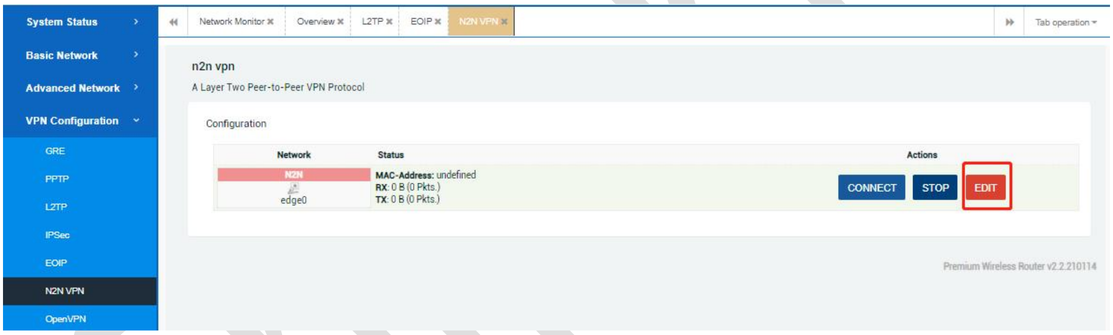
6.6 N2N VPN Client

The N2N network is mainly used to connect different client router devices or PC computer clients to the N2N super node server through the N2N protocol dial-up configuration to achieve the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The specific configuration is as follows:



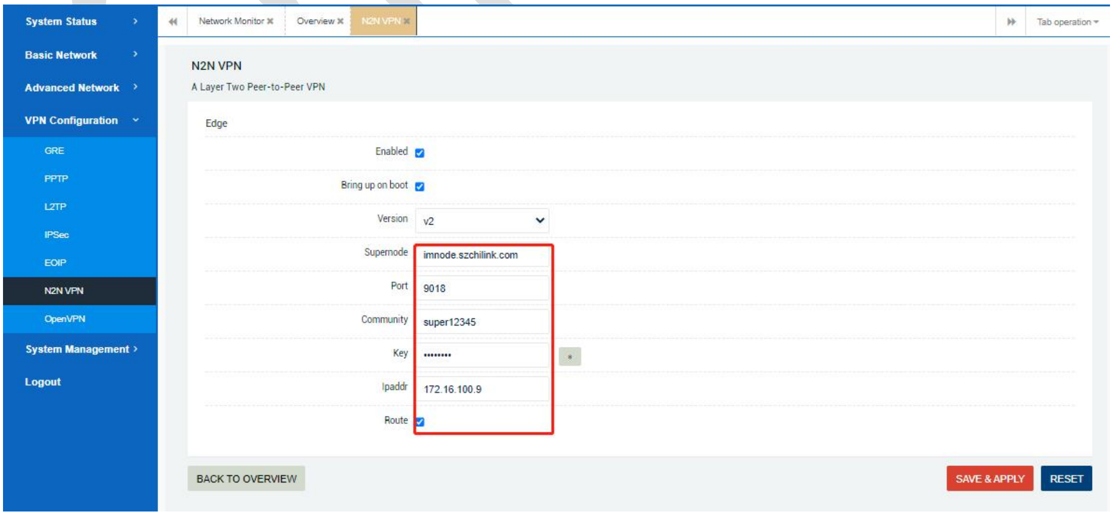
n2n vpn

A Layer Two Peer-to-Peer VPN Protocol

Configuration

Network	Status	Actions
N2N edge0	MAC-Address: undefined RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	CONNECT STOP EDIT

Premium Wireless Router v2.2.210114



N2N VPN

A Layer Two Peer-to-Peer VPN

Edge

Enabled ☑

Bring up on boot ☑

Version: v2

Supernode: imnode.szchilink.com

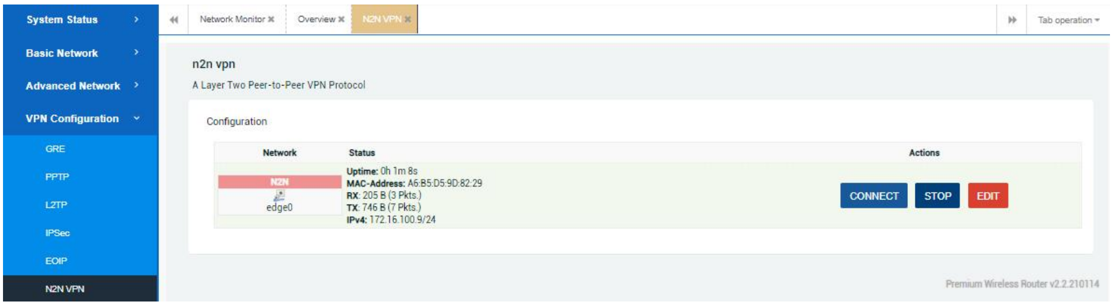
Port: 9018

Community: super12345

Key: ••••••••

Ipaddr: 172.16.100.9

Route ☑



n2n vpn

A Layer Two Peer-to-Peer VPN Protocol

Configuration

Network	Status	Actions
N2N edge0	**Uptime:** 0h 1m 8s **MAC-Address:** A6:B5:D5:9D:82:29 **RX:** 205 B (3 Pkts.) **TX:** 746 B (7 Pkts.) **IPv4:** 172.16.100.9/24	CONNECT STOP EDIT

Premium Wireless Router v2.2.210114

[Version]: Super node server optional protocol version V1 and V2;

[Super Node]: Fill in the IP address of the remote central server, generally the public network IP address;

[Port]: The service port of the super node server;

[Community]: N2N constitutes a point-to-point network identification name. Note: The names and passwords of the two client nodes must be exactly the same;

[Secret Key]: The verification password of the child node community network, the passwords of different nodes must be consistent;

[Address]: The virtual IP address in a peer-to-peer network, usually a private network;

[Routing and forwarding]: Used to automatically forward and access different sub-node routing networks;

6.7 OPEN VPN

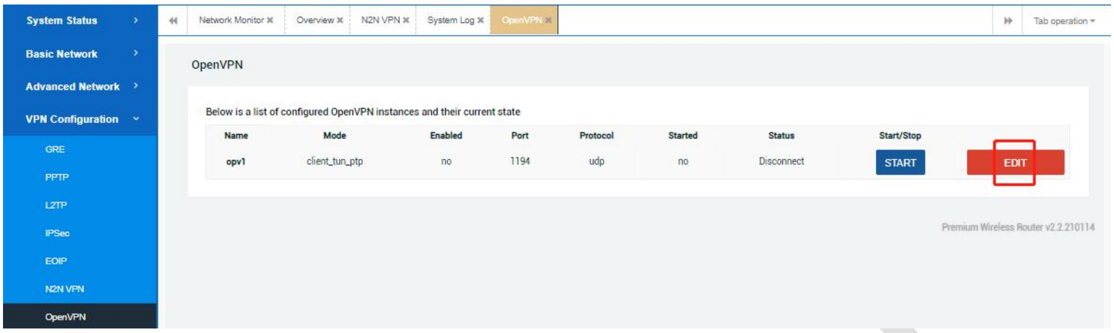
The OPEN VPN network is mainly used to connect different client router devices to the OPEN server after dialing through a specified protocol, so as to realize the following two main usage scenarios.

Scenario 1: The PC client can remotely access any subnet host in different router clients.

Scenario 2: Subnet hosts between client devices of different routers can communicate with each other at will.

The specific configuration is as follows:

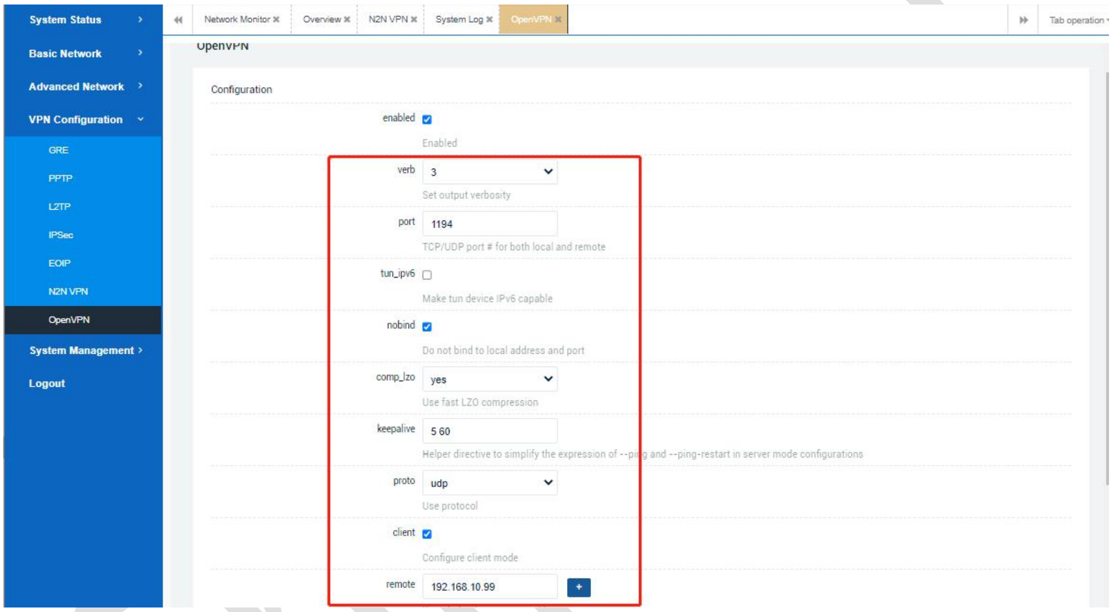
1）Select "Virtual Private Network" --- "OPEN VPN" to configure related parameters. The default interface examples are given as follows:



OpenVPN

Below is a list of configured OpenVPN instances and their current state

Name	Mode	Enabled	Port	Protocol	Started	Status	Start/Stop
opv1	client_tun_ptp	no	1194	udp	no	Disconnect	START



OpenVPN

Configuration

enabled ☑
Enabled

verb 3
Set output verbosity

port 1194
TCP/UDP port # for both local and remote

tun_ipv6 □
Make tun device IPv6 capable

nobind ☑
Do not bind to local address and port

comp_lzo yes
Use fast LZO compression

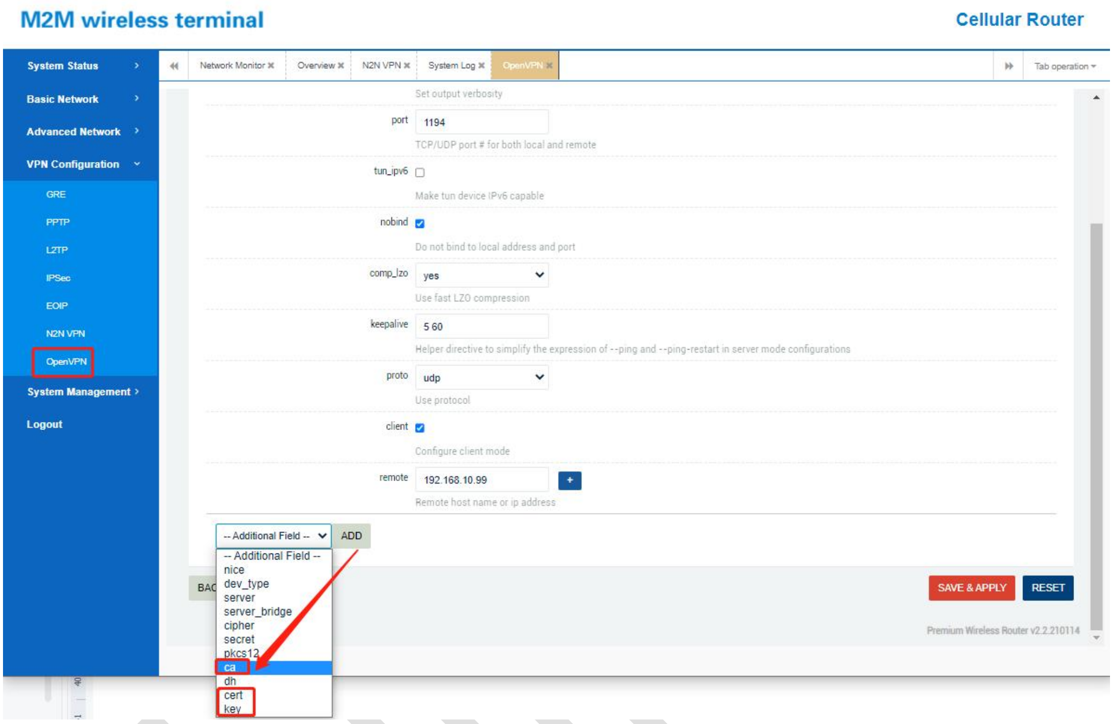
keepalive 5 60
Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations

proto udp
Use protocol

client ☑
Configure client mode

remote 192.168.10.99

2）Then click the "Add" button to add the openvpn client CA certificate, cert certificate, and key key certificate generated in advance on the server side one by one, and correctly configure the server IP address and port number, use protocol (default is udp), etc., and save the application The post-connection conditions are as follows:



M2M wireless terminal — Cellular Router

Set output verbosity

port: 1194 — TCP/UDP port # for both local and remote

tun_ipv6: ☐ — Make tun device IPv6 capable

nobind: ☑ — Do not bind to local address and port

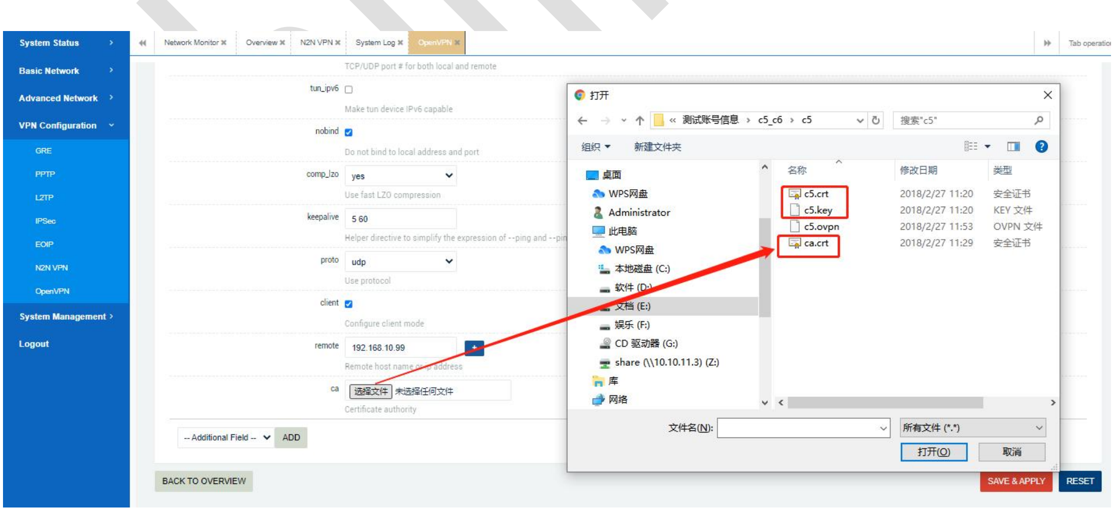
comp_lzo: yes — Use fast LZO compression

keepalive: 5 60 — Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations

proto: udp — Use protocol

client: ☑ — Configure client mode

remote: 192.168.10.99 — Remote host name or ip address

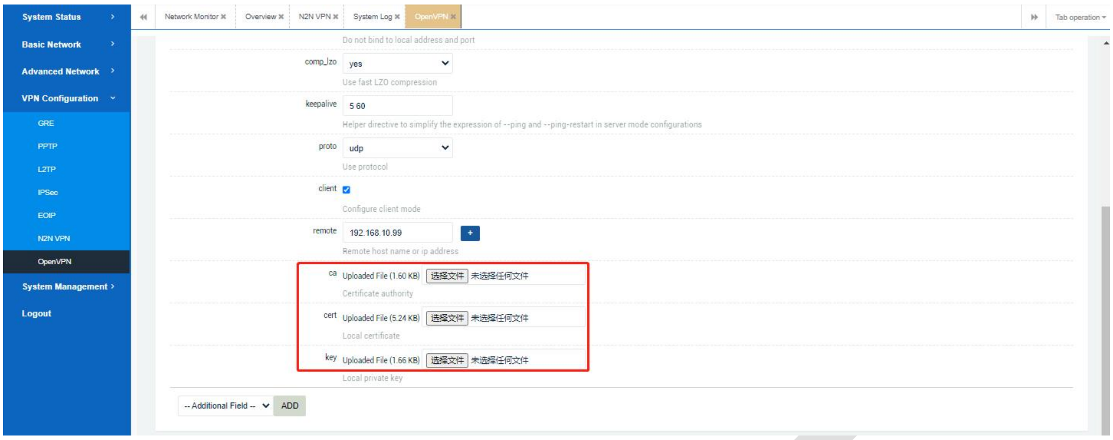


ca: 选择文件 未选择任何文件 — Certificate authority

打开

测试账号信息 › c5_c6 › c5

名称	修改日期	类型
c5.crt	2018/2/27 11:20	安全证书
c5.key	2018/2/27 11:20	KEY 文件
c5.ovpn	2018/2/27 11:53	OVPN 文件
ca.crt	2018/2/27 11:29	安全证书



Do not bind to local address and port

comp_lzo: yes
Use fast LZO compression

keepalive: 5 60
Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations

proto: udp
Use protocol

client: ☑
Configure client mode

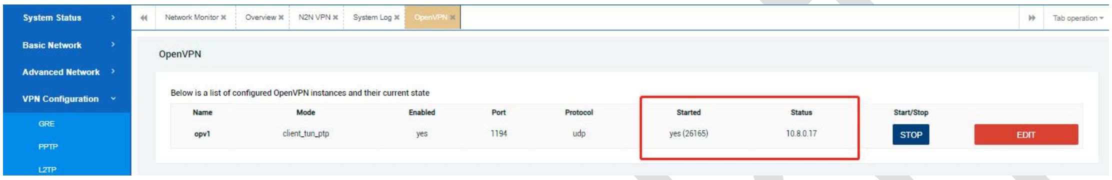
remote: 192.168.10.99 +
Remote host name or ip address

ca: Uploaded File (1.60 KB) 选择文件 未选择任何文件
Certificate authority

cert: Uploaded File (5.24 KB) 选择文件 未选择任何文件
Local certificate

key: Uploaded File (1.66 KB) 选择文件 未选择任何文件
Local private key

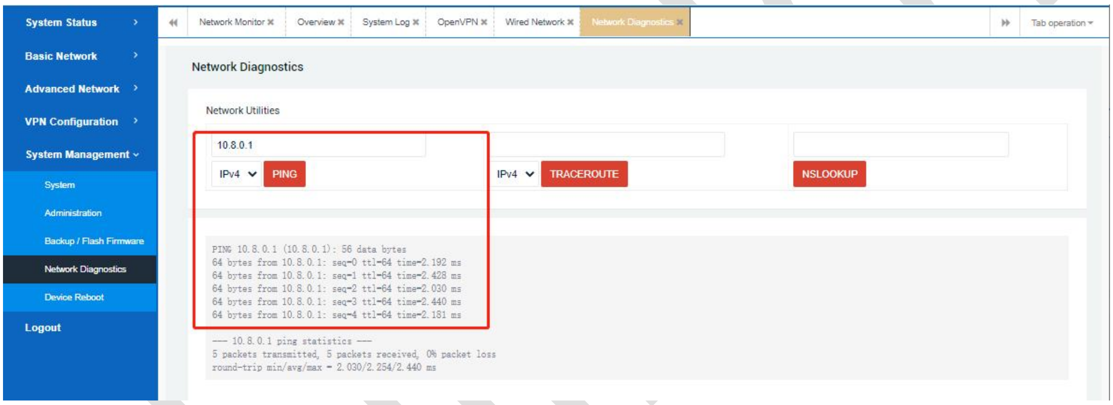
-- Additional Field -- ADD



OpenVPN

Below is a list of configured OpenVPN instances and their current state

Name	Mode	Enabled	Port	Protocol	Started	Status	Start/Stop	
opv1	client_tun_ptp	yes	1194	udp	yes (26165)	10.8.0.17	STOP	EDIT



Network Diagnostics

Network Utilities

10.8.0.1 IPv4 PING

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=64 time=2.192 ms
64 bytes from 10.8.0.1: seq=1 ttl=64 time=2.428 ms
64 bytes from 10.8.0.1: seq=2 ttl=64 time=2.030 ms
64 bytes from 10.8.0.1: seq=3 ttl=64 time=2.440 ms
64 bytes from 10.8.0.1: seq=4 ttl=64 time=2.181 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.030/2.254/2.440 ms
```

7.System Management

This chapter mainly introduces some system Settings of the router, such as system language, time zone, NTP server Settings and configuration of several network access modes.

At the same time, you can modify some system default management, such as login user name, password, shell background login access, etc. Finally, you can perform instant/timed restarts, firmware updates, configuration file backups, and more.

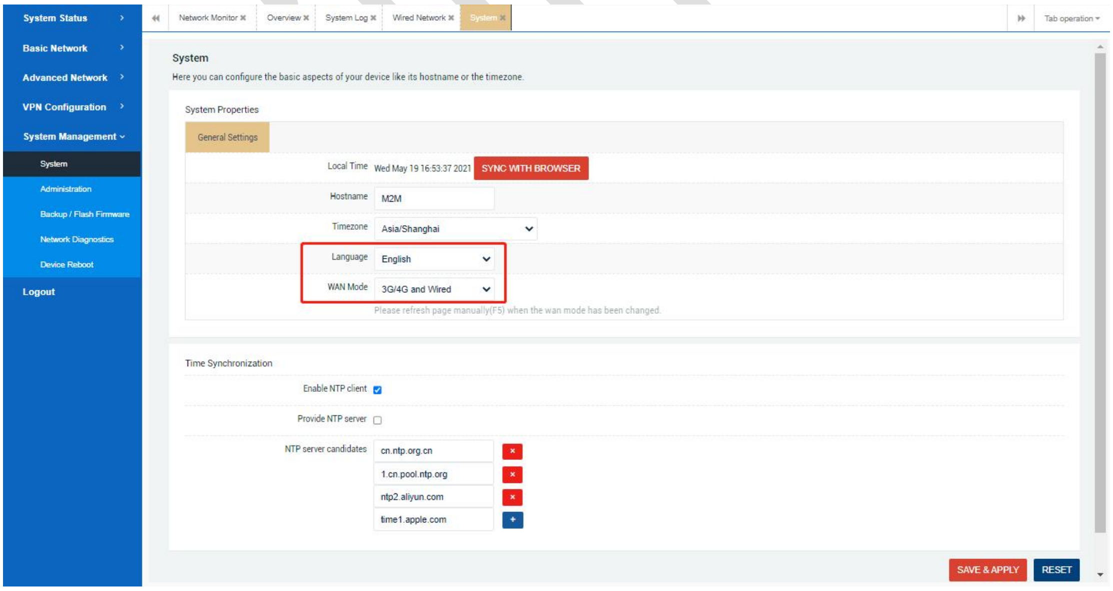
7.1 System

7.1.1 System property

In this section you can configure the system host name, time zone and language Settings, or change the WAN mode Settings, etc. You can also update the system local time by clicking "Synchronize Browser Time".

7.1.1.1 General Settings

As shown in the figure below, you can change the host name (M2M by default), time zone, language, etc.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Wed May 19 16:53:37 2021

Hostname: M2M

Timezone: Asia/Shanghai

Language: English

WAN Mode: 3G/4G and Wired

Please refresh page manually(F5) when the wan mode has been changed.

Time Synchronization

Enable NTP client ☑

Provide NTP server □

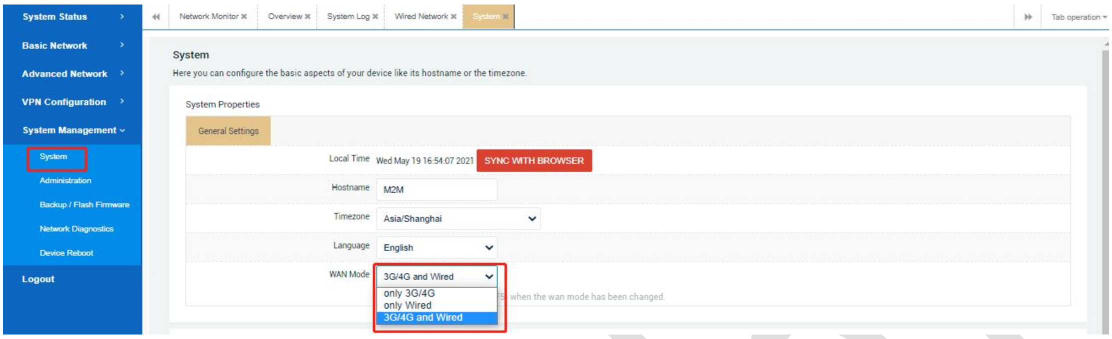
NTP server candidates: cn.ntp.org.cn, 1.cn.pool.ntp.org, ntp2.aliyun.com, time1.apple.com

7.1.1.2 Modification of WAN mode

The router supports three different "WAN modes", as described below:

7.1.1.2.1 3G/4G and Wired (default)

It means that the device supports both WAN port network access (cascaded to the LAN port of the upper router, and the network segment of the two routers cannot be the same) and 3G/4G mobile network.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Wed May 19 16:54:07 2021

Hostname: M2M

Timezone: Asia/Shanghai

Language: English

WAN Mode: 3G/4G and Wired

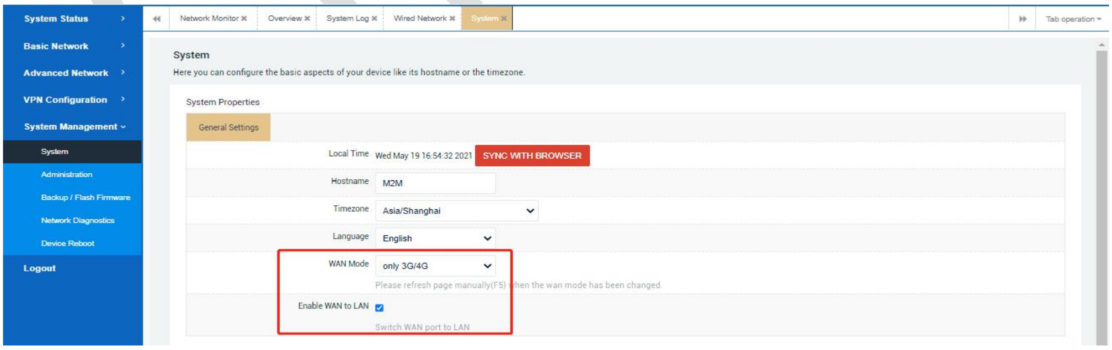
only 3G/4G
only Wired
3G/4G and Wired

…when the wan mode has been changed.

7.1.1.2.2 only 3G/4G

It means that the router only supports the SIM card mobile network and no longer supports the WAN network access (even if the WAN is connected to the superior network, it does not work);

You can further switch the WAN port to LAN by checking "WAN to LAN", so that you can connect to two user devices at the same time.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Wed May 19 16:54:32 2021

Hostname: M2M

Timezone: Asia/Shanghai

Language: English

WAN Mode: only 3G/4G

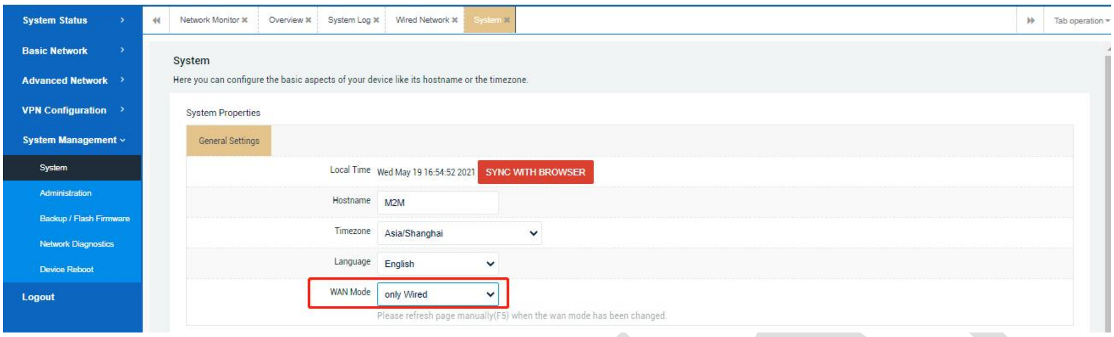
Please refresh page manually(F5) when the wan mode has been changed.

Enable WAN to LAN: ☑

Switch WAN port to LAN

7.1.1.2.3 Only Wired

It means that the router only supports wired WAN network access and no longer supports SIM card mobile network (it will not work even if the SIM card is inserted and the network is successfully connected).



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time: Wed May 19 16:54:52 2021

Hostname: M2M

Timezone: Asia/Shanghai

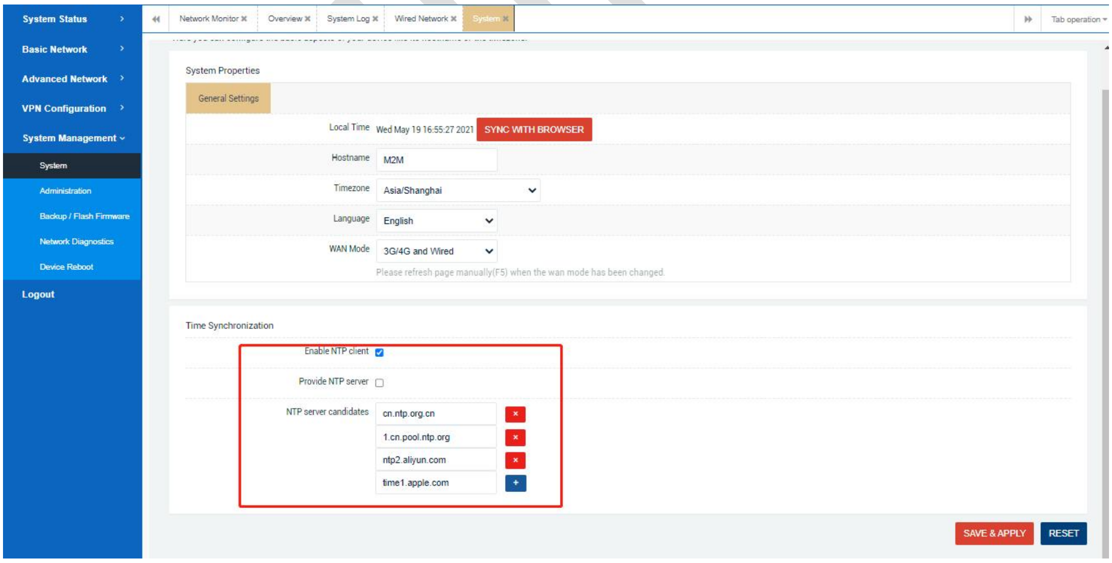
Language: English

WAN Mode: only Wired

Please refresh page manually(F5) when the wan mode has been changed.

7.1.2 Time synchronization

The router system supports the NTP network timing service, and the device has several default NTP servers. You can also customize to add or modify other NTP servers.



System Properties

Local Time: Wed May 19 16:55:27 2021

Hostname: M2M

Timezone: Asia/Shanghai

Language: English

WAN Mode: 3G/4G and Wired

Please refresh page manually(F5) when the wan mode has been changed.

Time Synchronization

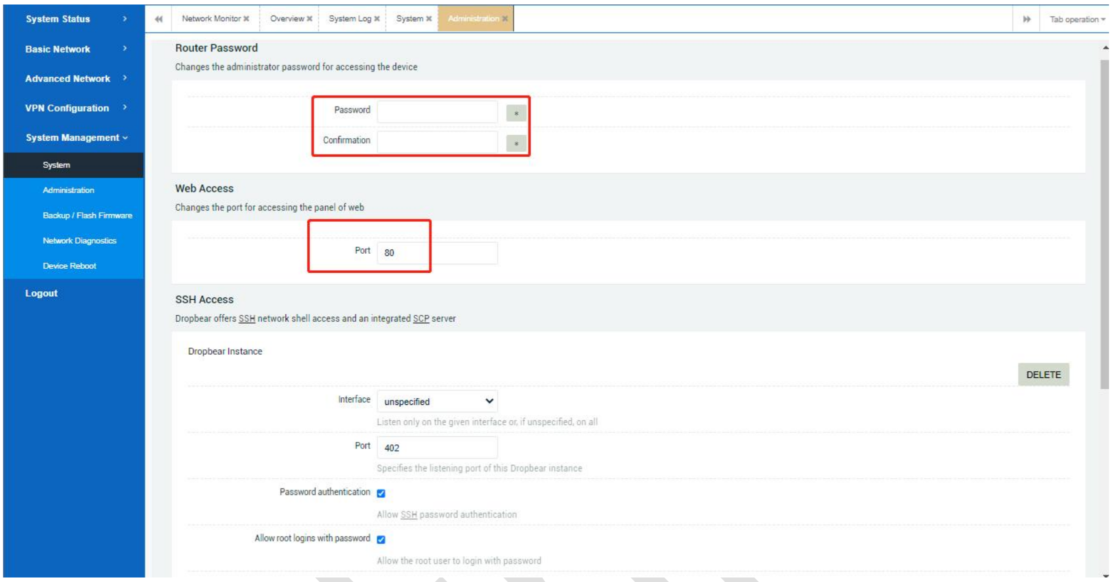
Enable NTP client ☑

Provide NTP server ☐

NTP server candidates: cn.ntp.org.cn, 1.cn.pool.ntp.org, ntp2.aliyun.com, time1.apple.com

7.2 Administration

In this chapter, you can modify the system's Web login password (default admin), Web access port (default 80), background SSH access (default LAN access, port 402) and other management permissions (in order to use the device safely, it is suggested that customers should change the default parameters when using the device).



Router Password

Changes the administrator password for accessing the device

Password:

Confirmation:

Web Access

Changes the port for accessing the panel of web

Port: 80

SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

Interface: unspecified

Listen only on the given interface or, if unspecified, on all

Port: 402

Specifies the listening port of this Dropbear instance

Password authentication: ☑

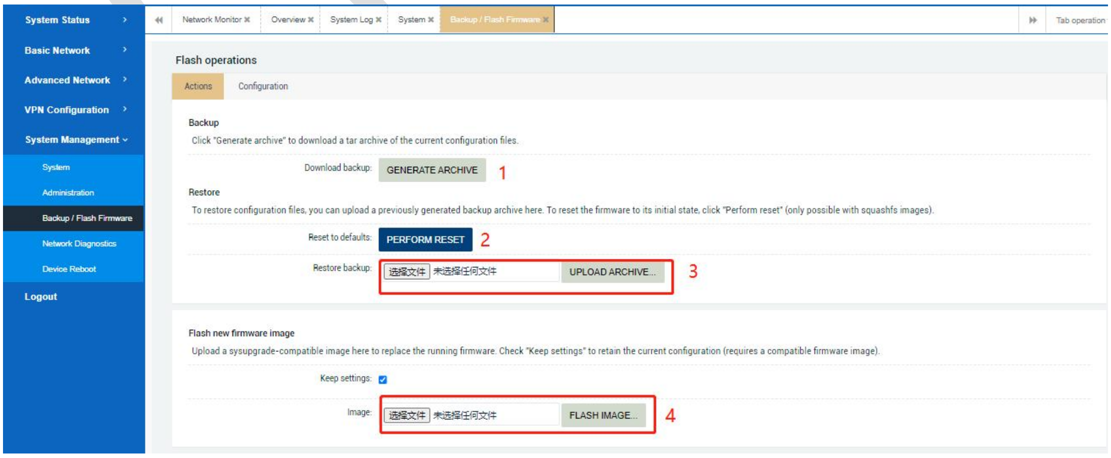
Allow SSH password authentication

Allow root logins with password: ☑

Allow the root user to login with password

7.3 Backup/flush Firmware

In this chapter, you can perform the following operations on the device system, such as firmware upgrade, backup parameters, reset, etc.



Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: GENERATE ARCHIVE

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults: PERFORM RESET

Restore backup: 未选择任何文件

Flash new firmware image

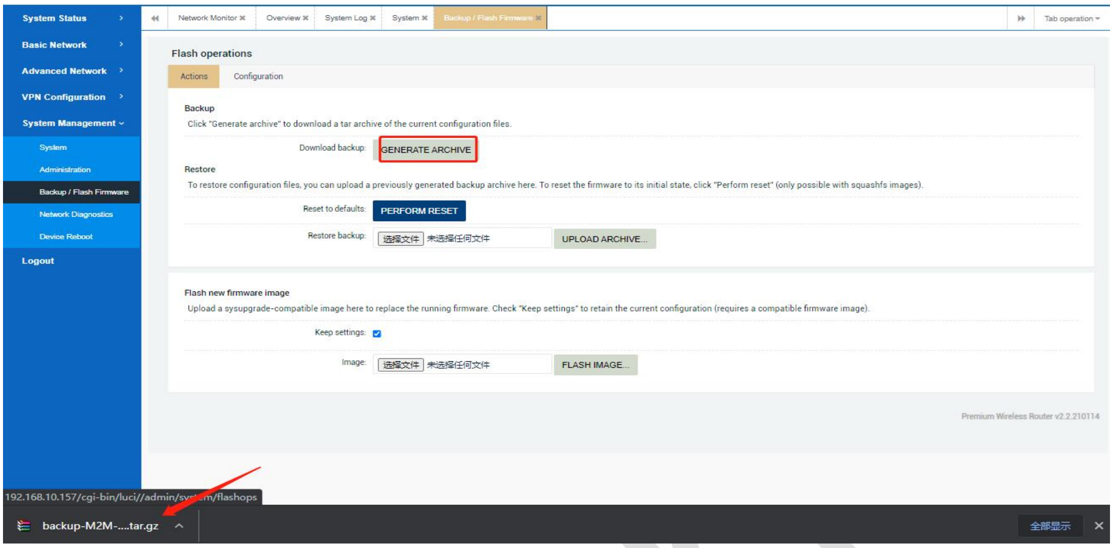
Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

Keep settings: ☑

Image: 未选择任何文件

7.3.1 Generate Archive

For this part, you can download some of the current configurations by clicking the ‘Generate Archive ‘ button of the router for backup so that you can use it for the next time.



Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: GENERATE ARCHIVE

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults: PERFORM RESET

Restore backup: 选择文件 未选择任何文件 UPLOAD ARCHIVE...

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

Keep settings: ☑

Image: 选择文件 未选择任何文件 FLASH IMAGE...

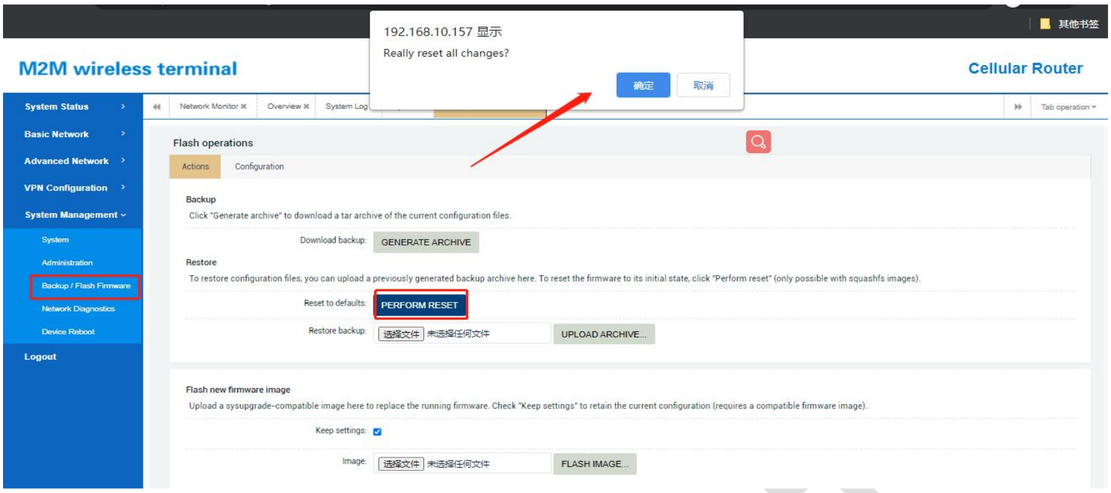
Premium Wireless Router v2.2.210114

192.168.10.157/cgi-bin/luci//admin/system/flashops

7.3.2 Perform Reset

The router system supports two ways to reset. Refer to the following instructions.

Method 1: Log in to the device Web page, and click "Execute Reset" to restore the routing system to the factory Settings. Please perform this operation carefully.



192.168.10.157 显示

Really reset all changes?

Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: GENERATE ARCHIVE

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults: PERFORM RESET

Restore backup: 选择文件 未选择任何文件

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

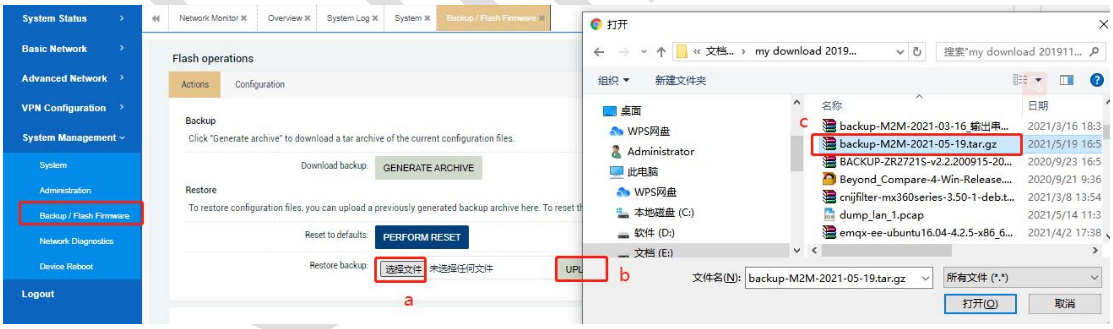
Keep settings: ☑

Image: 选择文件 未选择任何文件

Method 2: When the router is powered on, long press the black RST button for about 10 seconds and then release it (all the lights except the PWR power lamp are on and off to complete the reset).

7.3.3 Upload Archive

For this part, you can upload the backup configurations file by clicking the ‘Upload Archive ‘ button of the router so that you have no need to configure it again manual ly. It takes about 2-3 mins, so just be patient .You can handle it like below.



Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: GENERATE ARCHIVE

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset th

Reset to defaults: PERFORM RESET

Restore backup: 选择文件 未选择任何文件

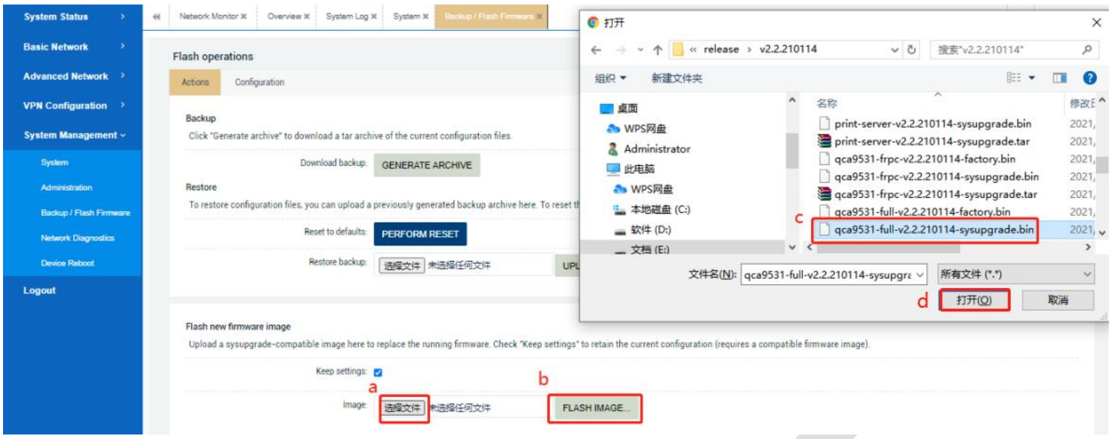
名称	日期
backup-M2M-2021-03-16_输出串...	2021/3/16 18:3
backup-M2M-2021-05-19.tar.gz	2021/5/19 16:5
BACKUP-ZR2721S-v2.2.200915-20...	2020/9/23 16:5
Beyond_Compare-4-Win-Release....	2020/9/21 9:36
cnijfilter-mx360series-3.50-1-deb.t...	2021/3/8 13:54
dump_lan_1.pcap	2021/5/14 11:3
emqx-ee-ubuntu16.04-4.2.5-x86_6...	2021/4/2 17:38

文件名(N): backup-M2M-2021-05-19.tar.gz

所有文件 (*.*)

7.3.4 Flash Image

For this part, you can upgrade the router device by clicking ‘Flash Image ’button. The upgrade process takes 2-3mins. Do not power off the device during this time, otherwise the upgrade will be abnormal and the system cannot be logged in again.



Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup:

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset th

Reset to defaults:

Restore backup: 选择文件 未选择任何文件

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires a compatible firmware image).

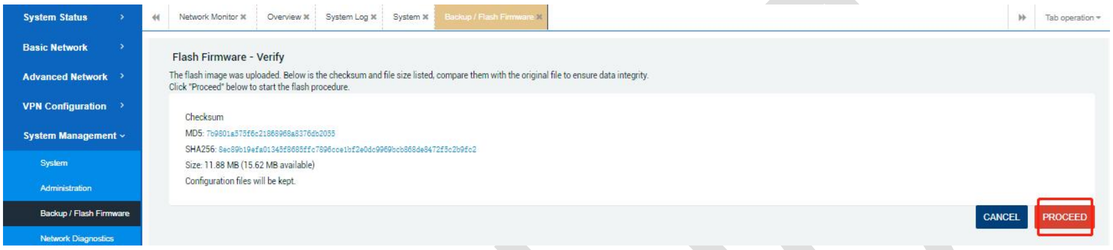
Keep settings: ☑

Image: 选择文件 未选择任何文件

名称	修改日
print-server-v2.2.210114-sysupgrade.bin	2021,
print-server-v2.2.210114-sysupgrade.tar	2021,
qca9531-frpc-v2.2.210114-factory.bin	2021,
qca9531-frpc-v2.2.210114-sysupgrade.bin	2021,
qca9531-frpc-v2.2.210114-sysupgrade.tar	2021,
qca9531-full-v2.2.210114-factory.bin	2021,
qca9531-full-v2.2.210114-sysupgrade.bin	2021,

文件名(N): qca9531-full-v2.2.210114-sysupgra

所有文件 (*.*)



Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

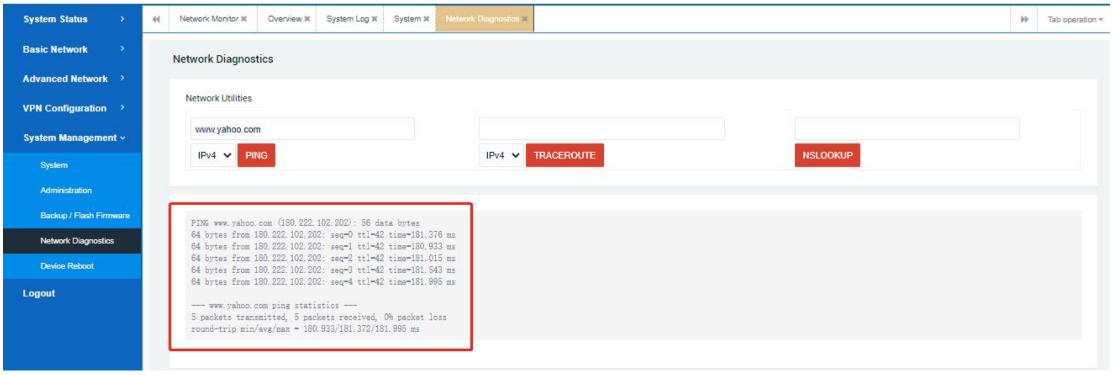
Checksum
MD5: 7b9801a575f6c21868968a8376db2055
SHA256: 8ec89b19efa01345f8685ffc7896cce1bf2e0dc9969bcb868de8472f5c2b9fc2
Size: 11.88 MB (15.62 MB available)
Configuration files will be kept.

Note: Select the "Keep settings" button, and the system will retain the user's original configuration parameters after upgrade. When upgrading firmware across versions, it is recommended not to check this option to prevent incompatible use of some system functions.

7.4 System diagnostics

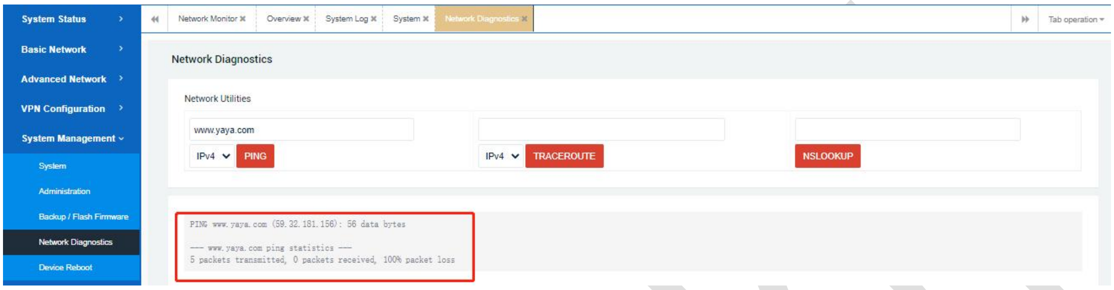
This chapter mainly introduces and instructs users how to confirm whether the router network is unblocked by using ‘ping’(to test whether the Internet is accessible) and ‘traceroute’ (to track and view the network routing table) tools.

In particular, if you can ping an external network address (such as www.yahoo.com) successfully, the network is reachable. Otherwise, it indicates that the current network is abnormal and cannot be connected to the Internet, which requires further investigation and processing.



www.yahoo.com

```
PING www.yahoo.com (180.222.102.202): 56 data bytes
64 bytes from 180.222.102.202: seq=0 ttl=42 time=181.376 ms
64 bytes from 180.222.102.202: seq=1 ttl=42 time=180.933 ms
64 bytes from 180.222.102.202: seq=2 ttl=42 time=181.015 ms
64 bytes from 180.222.102.202: seq=3 ttl=42 time=181.543 ms
64 bytes from 180.222.102.202: seq=4 ttl=42 time=181.995 ms

--- www.yahoo.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 180.933/181.372/181.995 ms
```



www.yaya.com

```
PING www.yaya.com (59.32.181.156): 56 data bytes

--- www.yaya.com ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

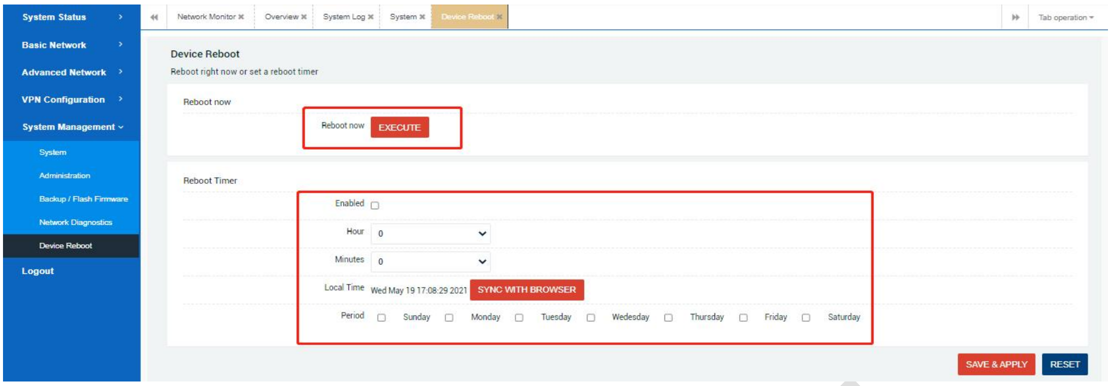
7.5 Device Reboot

7.5.1 Reboot now

Here you can restart the router immediately by clicking the Execute button if you need to.

7.5.2 Reboot timer

With this feature, you can set a specific time to restart the router system by date, hour, or minute.



Device Reboot

Reboot right now or set a reboot timer

Reboot now

Reboot now EXECUTE

Reboot Timer

Enabled □

Hour 0

Minutes 0

Local Time Wed May 19 17:08:29 2021 SYNC WITH BROWSER

Period □ Sunday □ Monday □ Tuesday □ Wedesday □ Thursday □ Friday □ Saturday

SAVE & APPLY RESET

8.Exit

Clicking the "Exit" button will automatically log you out of the current device's web page and return to the re-login state.

9. Overview of Router Open Ports

Port	Protocol	State	Service	Description
53	tcp	open	domain	DNS
80	tcp	open	http	Web Server
402	tcp	open	ssh	SSH for Dropbear
443	tcp	open	https	Web Server

Appendix: Network Abbreviations

The following abbreviations are only listed based on the current router system (the order is not limited), and hope to provide basic help for you to understand some network terms.

abbreviation	describe
Host network access related:	
M2M	Machine to Machine
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control Address
TTL	Time To Live
MTU	Maximum Transmission Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ARP	Address Resolution Protocol
Device/SIM card identification:	
IMEI	International Mobile EquIPment Identity
IMSI	International Mobile Subscriber Identity
ICCID	Integrate Circuit Card Identity
USIM	Universal Subscriber Identity Module
SIM	Subscriber Identity Module
APN	Access Point Name
Operator network standard:	
LTE	Long Term Evolution
TDD	Time Division Duplexing
TD-SCDMA	Time Division-Synchronous

	Code Division MultIPle Access
GSM/GPRS/EDGE	Global System for Mobile Communications General packet radio service Enhanced Data Rate for GSM Evolution
FDD	Frequency Division Duplexing
CDMA2000/HDR	Code Division MultIPle Access 2000 High Data Rate
CDMA	Code Division MultIPle Access
WCDMA/HSDPA/ HSUPA/HSPA+	Wideband Code Division MultIPle Access High Speed Downlink Packet Access High Speed Uplink Packet Access Enhenced High-Speed Packet Access
Common network domains:	
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
MGT	Management
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network
3GWAN1	3G/4G Wide Area Network
PPPoE	Point-to-Point Protocol Over Ethernet
PPP	Point to Point Protocol
Common network protocols:	
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol

	over SecureSocket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
PING	Packet Internet Groper
Wireless WiFi use and encryption:	
AP	Access Point
STA	Station
SSID	Service Set Identifier
ESSID	Extended Service Set Identifier
BSSID	Basic Service Set Identifier
WMM	Wi-Fi Multi Media
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA-PSK	WPA-Preshared Key
WPA2-PSK	WPA2-Preshared Key
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
Firewall related use:	
QoS	Quality of Service
DMZ	Demilitarized Zone
NAT	Network Address Translation
SNAT	Source Network Address Translation
DNAT	Destination Network Address Translation
UpNp	Universal Plug and Play
ACL	Access Control Lists
Positioning/timing service:	
GPS	Global Positioning System

LBS	Location Based Services
MCC	Mobile Country Code
MNC	Mobile Network Code
LAC	Location Area Code
CID	Cell ID
SID	System ID
NID	Network ID
BID	Base station ID
BD	BeiDou
NTP	Network Time Protocol
Virtual private network use:	
VPN	Virtual Private Network
VPDN	Virtual Private Dial Network
GRE	Generic Routing Encapsulation
PPTP	Point-to-Point Tunneling Protocol
L2TP	Layer 2 Tunneling Protocol
IPSec	Internet Protocol Security
EoIP	Ethernet over IP
N2N	Node to Node
LCP	Link Control Protocol
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
MPPE	Microsoft Point-to-Point Encryption
Algorithm and verification protocol:	
MD5	Message-Digest Algorithm
DES	Data Encryption Standard
3DES	TrIPle Data Encryption Algorithm

SHA	Secure Hash Algorithm
DH	Diffie-Hellman
SM3	/
IKE	Internet Key Exchange
DPD	Dead Peer Detection
PFS	Perfect Forward Secrecy
ESP	Encapsulating Security Payload
XAUTH	Extended Auth