



G51-M5 Industrial 4G/5G Wireless Router

Product User Manual

V3.0

IOT SOLUTIONS



V3.0
<http://www.homtecsm2m.com>
May, 2025

Homtecs Technology always aims to provide customers with the most timely and comprehensive services. If you need any assistance, please feel free to contact our company. The contact information is as follows:

Shenzhen Homtecs Technology Co., Ltd

Address: 2A, Building F5, TCL Science Park International E-City, 1001 Zhongshan Yuan Road, Nanshan District, Shenzhen

Website: www.homtecsm2m.com

Phone: 86 755 2390 3495

If you need technical support or feedback on any issues in our technical documentation, please feel free to contact the following at any time:

Email: info@homtecsm2m.com

Phone: 86 755 2390 3495

Copyright © Shenzhen Homtecs Technology Company Limited 2012 ~ 2025

Without our written approval, anyone can't extract, copy whole or part of content of this file and can't spread out in any format.

Caution

Due to product updates or functional upgrading, we may renew the content of this file, and this file only for reference. All statement, information, suggestion etc. in this file does not compose any form of guarantee and we Homtecs reserves the right of final explanation.

Brand Statement



And other Homtecs Technology trademarks are all trademarks of Shenzhen Homtecs Technology Co., Ltd.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Attention

The products, services, or features you purchase are subject to the commercial contracts and terms of Homtecs Technology Company. All or part of the products, services, or features described in this document may not be within your scope of purchase or use. Unless otherwise agreed in the contract, Homtecs Technology makes no express or implied representations or warranties regarding the content of this document.

Due to product version upgrades or other reasons, the content of this document may be updated periodically. Unless otherwise agreed, this document is for use only and all statements, information, and recommendations in this document do not constitute any express or implied warranties.

Contents

1. Introduction	5
1.1. Overview	5
1.2. Model	5
1.3. Appearance	5
1.4. Accessories	6
1.5. How it works	6
1.6. Features	7
1.7. Technical indicators and specifications	8
1.8. Applications	9
1.8.1. Financial Industry Application	9
1.8.2. Vehicle Communication Industry Application	9
2. Hardware installation instructions	10
2.1. Installation Preparation	10
2.2. Schematic representation of the product panel	10
2.3. Product Indicator Description	11
2.4. Dimensional specification drawing	11
2.5. SIM card installation	12
2.6. Cable connections	12
2.7. Installation checks	12
3. Prepare for the configuration	13
3.1. Local connection configuration	13
3.2. Configuration checks	14
4. Configuration introduction	15
4.1. Establish a web configuration environment	15
4.2. System Status	16
5. Basic network configuration	17
5.1. WAN network configuration	17
5.2. Mobile network configuration	19
5.3. ICMP detection	22
5.4. LAN configuration	23
5.5. IPv6	24
5.6. VLAN	27
5.7. Link Schedule	29
5.8. DDNS	34
5.9. Routing	38
5.9.1. IPv4 Static Routing Table	38
5.9.2. IPV6 Static Routing Table	40
5.9.3. Policy Routing Table	41
5.9.4. OSPF	42
5.9.5. BGP	45
6. WLAN	48
6.1. Basic Settings	48
6.1.1. Wireless Client Mode	49
6.1.2. Wireless bridge mode	51
6.2. Multiple SSID	53
6.3. Wireless Survey	53
7. Advanced network configuration	54
7.1. IPv4 Port Forwarding	54
7.2. IPV6 Port Forwarding	56
7.3. Port Redirecting	60
7.4. DMZ	62
7.5. Port Mirror	63
7.6. IP Passthrough	64
7.7. Triggered	66
7.8. Captive Portal	71
7.9. Serial App2	72
7.10. GPS settings	75
7.11. UPnP/NAT-PMP	78
7.12. Bandwidth Control	79
7.13. VRRP	81

7.14. Static DHCP	88
8. Firewall	90
8.1. IP/URL Filtering	90
8.2. Keyword Filtering Settings / URL Filtering Settings / Access Filtering	92
8.3. Domain Filtering	93
9. VPN configuration	94
9.1. Wireguard	94
9.2. Zerotier	102
9.3. GRE	107
9.4. OpenVPN Client	109
9.5. OpenVPN Server	112
9.6. PPTP/L2TP server	118
9.7. L2TP/PPTP client	122
9.8. L2TPv3	125
9.9. IPSec	128
9.10. DMVPN	133
10. Administration	138
10.1. Identification	138
10.2. Time	138
10.3. Admin Access	139
10.4. HTTPS Certificate	140
10.5. Scheduled Reboot	141
10.6. SNMP	141
10.7. M2M Settings	143
10.8. DI/DO Settings	145
10.9. Configuration	150
10.10. Logging	152
10.11. Upgrade	153
10.12. Reboot	154
10.13. Logout	155
11. Tools	155
11.1. System log	155
11.2. Ping	156
11.3. Trace	156
11.4. WOL	157
11.5. Bandwidth	157
11.6. Traffic FigureTable	158
11.7. Factory reset via the RST button	158
12. Issues handling	159
12.1. Hardware issues	159
12.1.1. None of the indicators are on	159
12.1.2. SIM card connection issues	159
12.1.3. Network port connection issues	159
12.1.4. Antenna connection issues	160
12.2. Dial-up issues	160
12.2.1. Dial-up dropped	160
12.2.2. No signal display issues	160
12.2.3. SIM/UIM card could not be found	161
12.2.4. Communication signal is weak	161
12.3. VPN connection issues	161
12.3.1. VPN can't connect	161
12.3.2. The VPN can't communicate	162
12.4. WEB configuration operation issues	162
12.4.1. firmware upgrade failed	162
12.4.2. Forgot router password	163
12.4.3. Frequent reboot issues	163
12.5. Other issues	163
12.5.1. After modifying the IP address, I forgot to configure the Router and could not set it	163
12.5.2. Why is the network indicator not lit when connected to the PC after powering on?	163

1. Introduction.

1.1. Overview

G51-M5 industrial grade mobile 5G Router is an IoT wireless communication router that adopts the internationally recognized LTE/Sub6 5G mobile broadband network standard, providing customers with convenient and fast internet access or dedicated network transmission. It can be equipped with embedded Wi Fi modules or multiple LAN ports, providing customers with wired fixed network or wireless WLAN shared high-speed broadband connection for their terminals; Simultaneously supporting VPN (Wireguard, Zerotier, GRE, OpenVPN, IPSec, L2TP, PPTP, DMVPN) functions to build secure tunnels, widely used in industries such as finance, power, environmental protection, petroleum, transportation, and security.

It provides users with a web-based configuration interface and CLI command line configuration, which can be configured through a web browser or Telnet/SSL. It also provides users with an M2M terminal product management platform, which remotely manages all Router terminals. Users can monitor the status of all successfully connected terminals through the M2M platform, providing remote control, parameter configuration, and remote upgrade services.

This manual introduces the industrial grade Router series products to users, as well as how to install and configure the products, quickly guiding users to correctly install and configure basic parameters.

1.2. Model

This series of products adopts high-performance MIPS dual-core professional network communication processor, with embedded real-time operating system as the software support platform, to provide users with a safe, high-speed, stable and reliable 5G wireless routing network, and supports 4 Gigabit Ethernet interfaces and communication serial ports. There are a variety of models to choose from, and the following are the specific product model:

Model table 1-1:

HOMTECS	G51-M5W2				
Model	Network Bands	Wi-Fi	GPS	Ethernet port	Serial
G51-M5W2	5G :N1/N2/N3/N5/N7/N8/N12/N20/N25 /N28/N40/N41/N66/N71/N77/N78/N79 LTE FDD: B1/B3/B8 LTE TDD: B38/B39/B40/B41	optional	optional	4*LAN /1*WAN+3*LAN	RS232, RS485

Table 1- 1

1.3. Appearance

Appearance table 1-2:

Product series	G51-M5W2	
Appearance		



Figure 1-1 Appearance Introduction

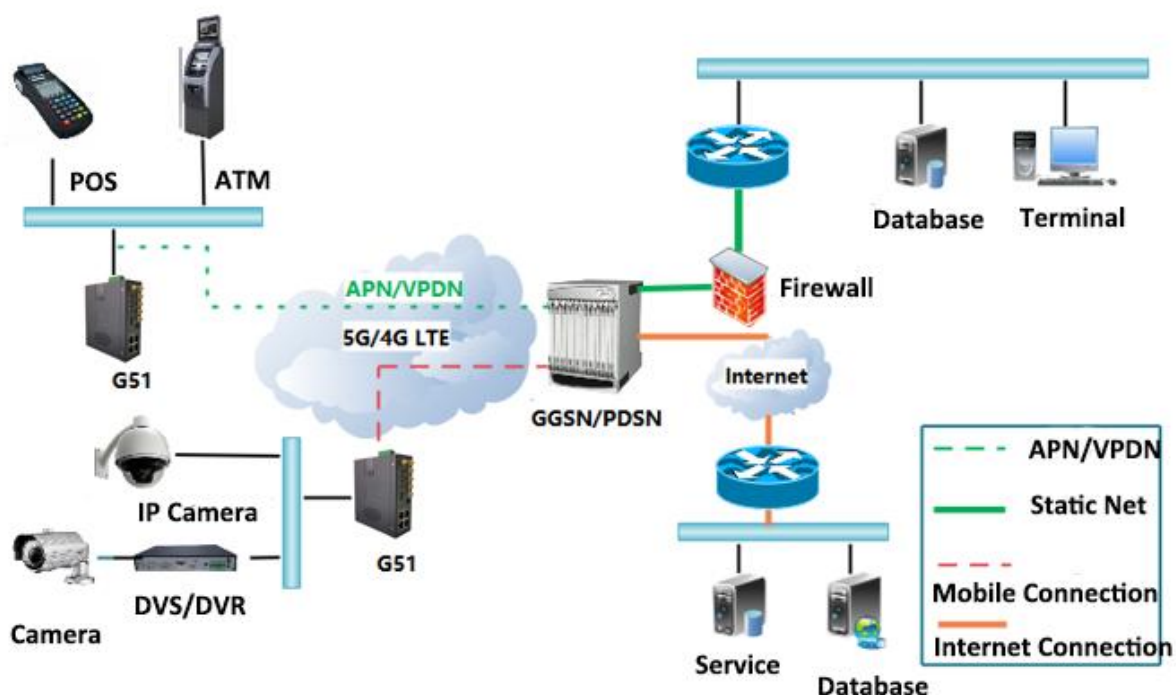
1.4. Accessories

Accessories Table 1-3:

Item	Quantity	Remark
G51 router	1	According to the user's order situation
4G/5G antennas	3	Assigned according to the network
WLAN antennas	2	When equipped with WLAN function
GPS antenna	1	When equipped with GPS function
Cable	1	Standard
Certificate	1	Standard
12V power adapter	1	Standard

Table 1- 3

1.5. How it works



Based on mobile wireless public or private networks, this series product builds wireless data tunnels on mature networks, which greatly reduces the cost of wireless data transmission in various industries.

1.6. Features

- Support Sub6 5G/FDD/TDD/TD-CDMA/WCDMA/EDVO and other networks, backward compatible with GPRS/EDGE/CDMA1x;
- Supports IEEE802.11b/g/n Wi Fi AP functionality, with extended support for Wi Fi clients, WDS bridging, and multiple authentication and encryption methods such as WEP, WPA/WPA2 Persistent/Enterprise, TKIP/AES, etc;
- Support virtual data and private networks (APN/VPDN);
- Support multiple on-demand dialing options, including scheduled up and down calls, voice or SMS controlled up and down calls, data triggered online calls, and idle link offline calls;
- Supports TCP/IP protocol stack and comprehensive network protocols such as Telnet, HTTP, SNMP, PPP, PPPoE, etc;
- PPP:
 - Support VPDN/APN function, which can easily and quickly access the virtual dial-up private network provided by mobile operators to protect your data security.
 - Supports PPPoE (Point to Point Protocol over Ethernet) protocol, which is a technology for forwarding PPP frames over Ethernet, especially suitable for ADSL.
 - Support CE and CCC certification.
 - Support connection detection and automatic repair. After the device is disconnected, it can be automatically reconnected to ensure stable online operation.
- Provide user-friendly interface configuration management, support Telnet/SSH/CLI configuration mode;
- Optional IPv6 protocol stack;
- Optional support for M2M terminal management platform;
- WDT watchdog design to maintain system stability;
- Can be customized and developed according to customer needs;
- Firewall function:
 - Support firewall packet filtering to filter out junk data for you, making the device more efficient.
 - Support Port Mapping, which enables access to specific port services from the Internet to machines within the local area network.
 - By holding virtual address mapping, the real IP can be hidden, making it convenient for your application.
 - The Demilitarized Zone (DMZ), also known as the "Demilitarized Zone" or "Isolation Zone".
 - Effectively solving the problem of external network being unable to access internal network servers after installing a firewall, while also effectively protecting the internal network.
 - Support MAC address binding, restrict access of internal network hosts, and provide more security guarantees.
- Management Platform:
 - Equipment remote management platform, which enables remote management of G51-M5 devices, supports remote parameter configuration, remote upgrade, remote log management, remote alarm management, information statistics and display, batch configuration, batch upgrade and other remote operations through the

management platform;

➤ Network tools:

- Provide PING and trace route to detect the connection status of the router;

1.7. Technical indicators and specifications

Router Interface Description

Interface	Describe	Remark
USIM	Plug in SIM card slot	
4G/5G	4G/5G antenna, SMA connector, 50 Ω	
WiFi	Wi-Fi antenna, SMA connector, 50 Ω	optional
GPS	GPS antenna, SMA connector, 50 Ω	optional
LAN	Ethernet downlink service interface, 1000Base TX, MDI/MDIX adaptive, Ethernet interface for connecting computers, switches, and hubs	Default: 1 * Console + 4*LAN/1*WAN+3*LAN
WAN	Ethernet uplink service interface, 1000Base TX, MDI/MDIX adaptive, upstream switch or router	WAN/LAN reuse
RST	Reset button, used to restore factory default settings (press and hold the button for 15 seconds after powering on)	
PWR	power interface	7.5~32V DC
RS232/RS485	Terminal block serial port, supporting RS-232 and RS-485 interfaces for data transmission	

Table 1- 4

Terminal block 1 (5PIN)			Terminal block 2		
1	DI1	input	1	V+	Positive pole of power input
2	DI2	input	2	V-	Negative pole of power input
3	GND	signal ground	3	GND	Signally
4	DO1	output	4	485A	485-A
5	DO2	output	5	485B	485-B
			6	GND	Signally
			7	TX	Serial port output
			8	RX	serial port input

Figure 1- 2

OTHERS:

Item	Parameter
Casing	Sheet metal shell
Weight	Approximately 467.2g
Working temperature	-20~+70℃
Product appearance	132×112×44mm
Storage temperature	-40~+85℃
relative humidity	<95% (no condensation)
Power consumption	When dialing 12V, the current is 730mA, and the standby current is 610mA

Table 1- 5

1.8. Applications

This series product is widely used in industries such as telecommunications, finance, information media, power, transportation, automotive and environmental protection, express cabinets, remote video surveillance, etc.

1.8.1. Financial Industry Application

G51 Router provides high security transmission protection for financial data through IPSec VPN and other methods, greatly reducing the risk of communication interruption caused by operator network failures. Its typical networking is shown in Figure 1-4:

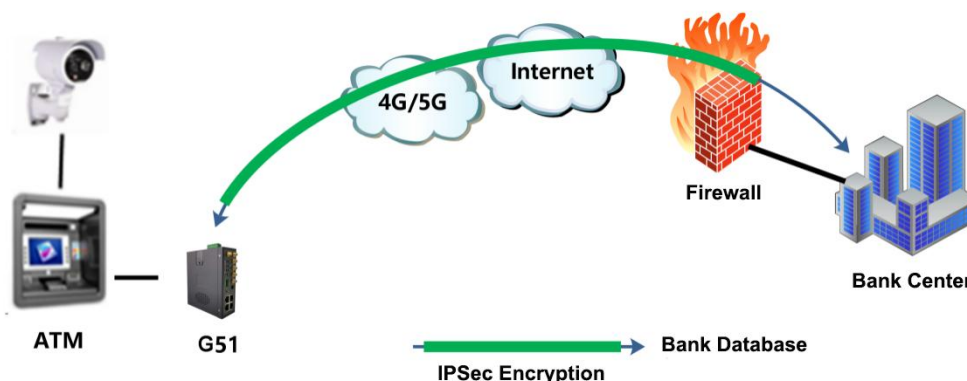


Figure 1-4 Schematic diagram of financial industry applications

1.8.2. Vehicle Communication Industry Application

G51 Router supports the transmission of in car videos. When in the parking lot, high-definition video data can be transmitted to nearby WLAN hotspots through WLAN, and then transmitted to the Internet through WLAN hotspots. During the driving process of the car, data can be transmitted to the video server through 4G/5G network communication. Its typical networking is shown in Figure 1-5:

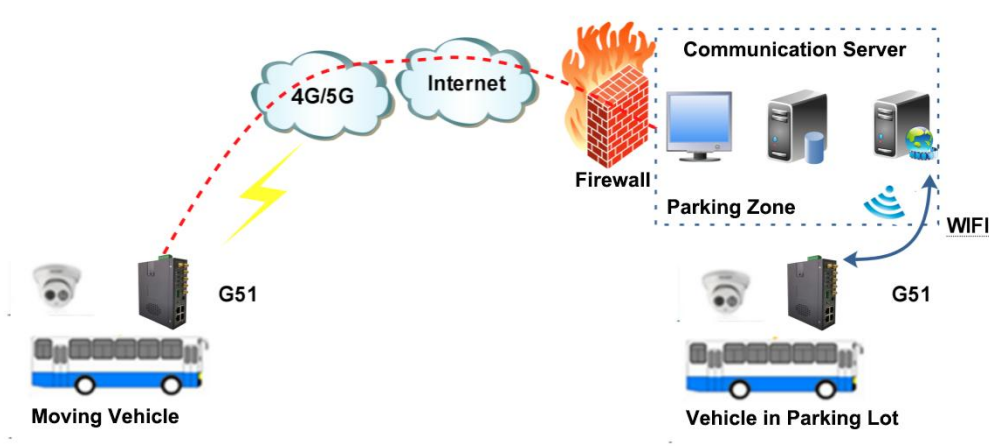


Figure 1-5 Application of Vehicle Communication Industry

2. Hardware installation instructions

2.1. Installation Preparation

Please confirm that G51 Router is within 4G/5G network coverage and there is no blocking on site.

Please provide the following conditions on site before installation:

- One PC
 - System: Windows XP/WIN7/WIN8/WIN10
 - CPU: PII 233 or higher
 - RAM: 32M or more
 - HDD: 6.4G or above
 - Ethernet port: : at least one (10M/100M/1000M)
 - IE version: 5.0 or later
 - Resolution: 640*480 or more
- A SIM card
 - Make sure that the card has data service enabled and is not down for arrears
- Power supply
 - 220V AC: Can be used with the DC power supply supplied with the product
 - 7.5~32V DC: ripple < 100 mV
- Fixed
 - Try to ensure that the router is placed on a horizontal plane and installed in an environment with low vibration frequency. When using industrial rails, the router can be attached to a chassis or rails equipped with rails (when installed on a moving vehicle or vibrating machine, it must be secured with an industrial rail).

2.2. Schematic representation of the product panel

G51 series products panel illustration

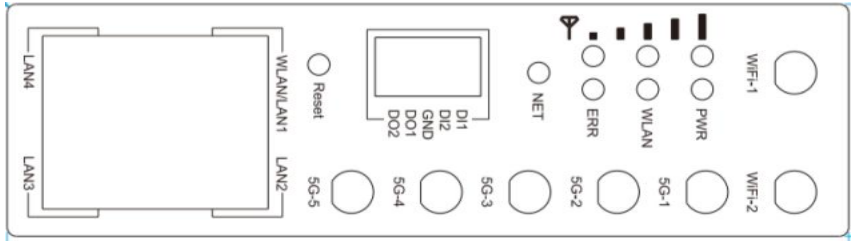
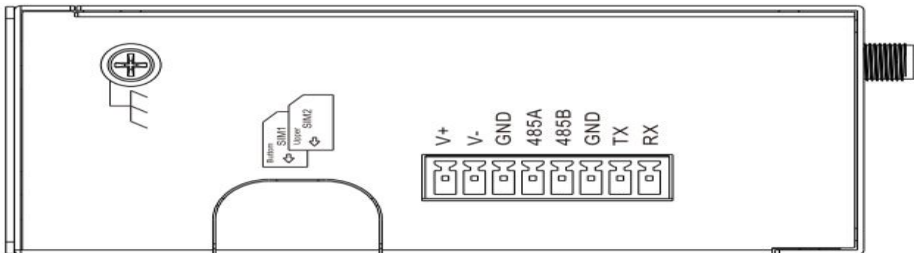
HOMTECS	G51 series
Front panel	
Side panels	

Table 2-1 Panel diagram

The antenna interfaces of the extended Wi-Fi and GPS function series products are different.

2.3. Product Indicator Description

Router Indicator Description

PWR	WLAN	ERR	Signal1	Signal2	Signal3	Light indication instructions
			Solid light	Solid light	Solid light	When it is a 4G/5G program, the 4G/5G is online and CSQ value is showed "CSQ >=18"
			Solid light	Solid light	Off	When it is a 4G/5G program, the 4G/5G is online and CSQ value is showed "10<CSQ<18"
			Solid light	Off	Off	When it is a 4G/5G program, the 4G/5G online CSQ value is showed "CSQ< = 10"
			The 2S flashing cycle flashes slowly, 1.5S is on, and 0.5S is off	Solid light	Solid light	When it is a 4G/5G program, the 3G is online and CSQ value is showed "CSQ>=18"
			The 2S flashing cycle flashes slowly, 1.5S is on, and 0.5S is off	Solid light	Off	When it is a 4G/5G program, the 3G is online and CSQ value is showed "10<CSQ<18"
			The 2S flashing cycle flashes slowly, 1.5S is on, and 0.5S is off	Off	Off	When it is a 4G/5G program, the 3G is online and CSQ value is showed "CSQ <= 10"
			0.5S flashing cycle flashes quickly, 0.25S on, 0.25S off			Registered in the network
	Solid light					The Wi-Fi is enabled, but there is no data transmission
	Flash					The Wi-Fi is enabled, and there is data transmission
	Off					Wi-Fi is disabled
		Off				Check that the SIM is OK
		Solid light				Failed to check the SIM
Solid light						The power supply is normal

Table 2-1

There is a difference in the indicator display of the extended single-mode dual-SIM product.

2.4. Dimensional specification drawing

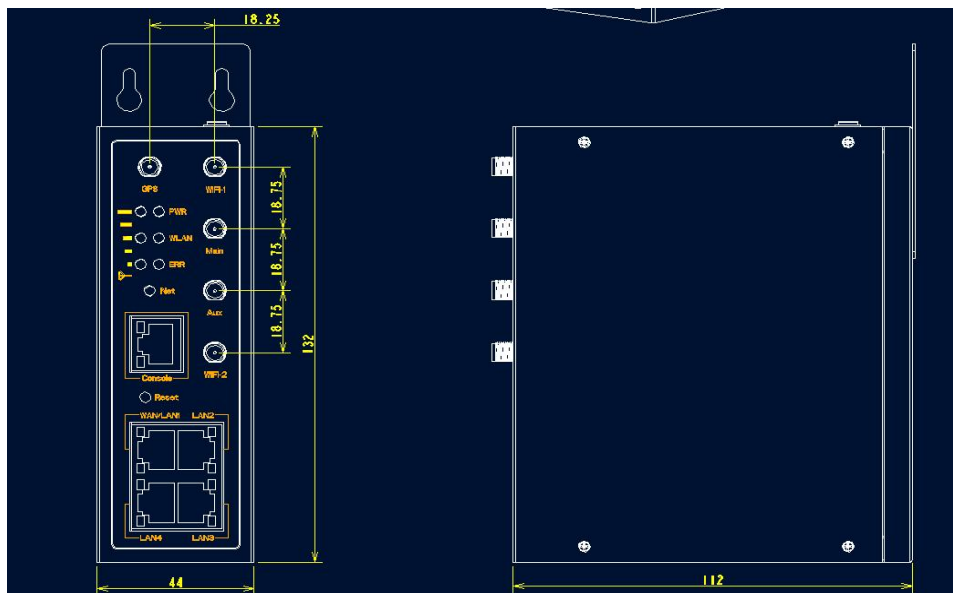


Figure 2-1 Dimensions of G51 series routers



The device supports a variety of installation methods: embedded integration, desktop placement, wall mounting and rail installation.

2.5. SIM card installation

Step 1: Open the card cover with a screwdriver.

Step 2: Insert the SIM into the card holder correctly.

2.6. Cable connections

After installing and fixing the device, follow the steps below to connect the router series.

1. Connect the 4G/5G antenna to the 4G/5G interface of the router, connect the Wi-Fi antenna to the WI FI interface of the router, and adjust the best position or pointing of the antenna.
2. Use an Ethernet cable to connect the LAN interface of the converter with the network card interface of the computer or the uplink interface of the switch or the uplink interface of the terminal equipment. The WAN interface is connected in the same mode as the LAN interface.
3. Connect the PWR connector of the circuit driver (the input of the power adapter is 12V/2A DC) and the power socket with the power adapter (or battery backup unit).
4. Press the switch of the power outlet.



Before connecting the cables, please disconnect the power of the router.

2.7. Installation checks

Before installing and preparing to power on, check if the SIM card is installed correctly.

Check the working status indicator light of the router after power on, and after power on the LAN port of the machine which connect to the lower level will light up, and the PWR light will light up, indicating that the system has started working normally.



WARNING

Be sure to connect the antenna before powering on to avoid partial impedance mismatch of the RF part, resulting in poor signal and inability to dial online.

Steps:

Step 1: Check if the antenna is installed correctly.

Step 2: Check if the SIM card is installed correctly and confirm that the SIM card is valid.

Step 3: G51 power supply

- After power is supplied, if the LAN port of the lower computer is connected to the G51, the Router has normal power supply.
- After a period of power, the router indicator lights up, indicating that the router system has been started.
- After the router indicator is on for a while, the .NET indicator lights up and flashes quickly, indicating that the router has found the module and started dialing. The router will have a .NET light on during dialing.



INSTRUCTIONS

For different modules, the router finds the module at different times, and the dial-up time is different due to different networks. So for different modules, the router dial-up and the time to get the IP address may be inconsistent, but the router dial-up process is strictly as described above.

3. Prepare for the configuration

3.1. Local connection configuration

Prerequisites

- The G51 Router has been powered.
- The G51 Router port has been connected via an Ethernet cable.

Specify the IP address mode

Step 1 Click "Start> Control Panel" in the window that opens, double-click "Network Connections", double-click "Network Connections" to open the "Local Connection Status" window, click "Properties", double-click Internet The protocol (TCP/IP) is shown in Figure 3-1

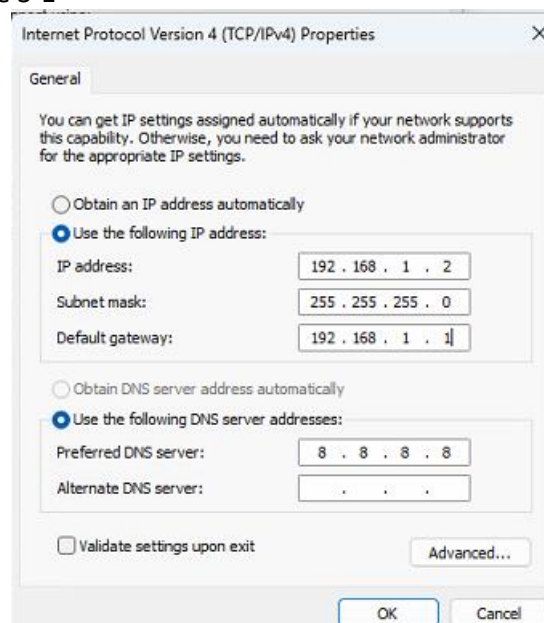


Figure 3-1 Internet Protocol (TCP/IP Properties Window).

Note: The IP address can be 192.168.1.x (where * represents any integer of 2~254).

Step 2: Click OK to complete the configuration.

DHCP automatically obtains IP addresses

The G51 Router has a built-in DHCP service that automatically assigns IP addresses to terminals connected to it based on pre-set parameters.

Step 1: Click "Start> Control Panel" in the window that opens, double-click "Network Connections" to open the "Local Connection Status" window, click "Properties", double click Internet Protocol (TCP/IP) as shown in Figure 3-2:

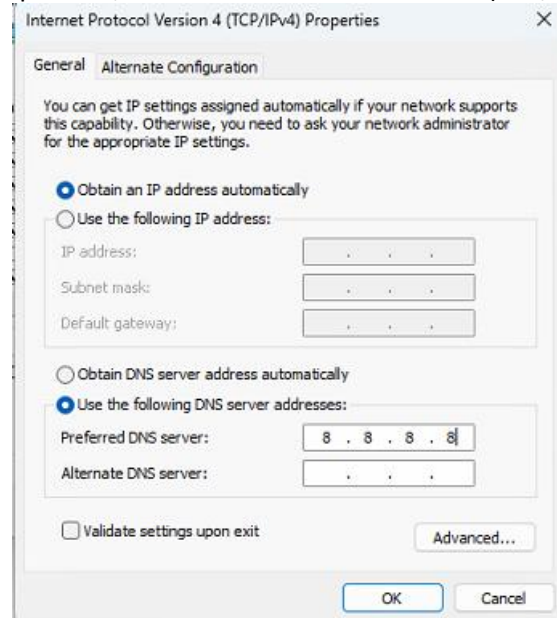


Figure 3-2 Internet Protocol (TCP/IP) Properties

Step 2: Click "OK" to complete the configuration.



The built-in DHCP service of the G51 Router is enabled at the factory, and the DHCP service is enabled until this function is configured.

3.2. Configuration checks

Step 1: Click "Start > Run" on your computer, enter the "cmd" command in the input box and press Enter. Open the Run window.

Step 2: Enter the command "ipconfig" in the "Run" window to configure the above two connections for the method "ipconfig". The IP address displayed in the window is different: the IP address displayed in Figure 3-3 is the IP address in Figure 3-3, as shown in Figure 3-4 shown; The IP address displayed in the configuration method of automatic IP acquisition by DHCP of the router is displayed as "2~51".'s random address.

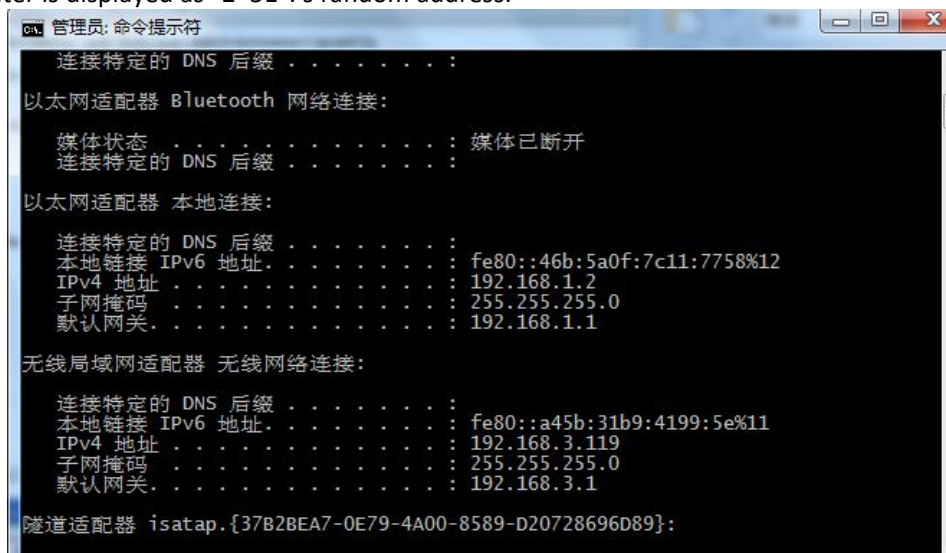


Figure 3-3 Specifies the result of 'ipconfig' IP address

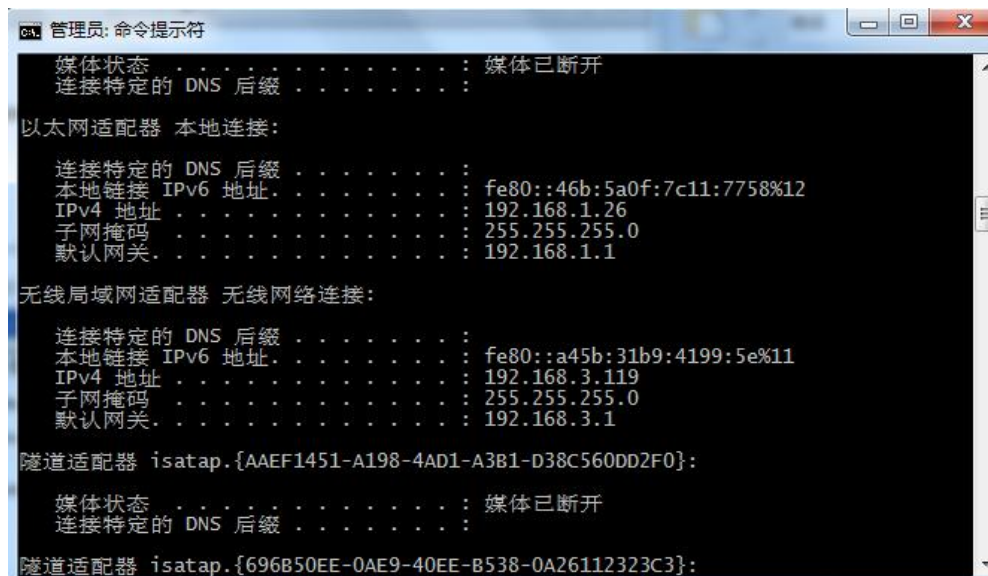


Figure 3-4 DHCP automatically obtains the result of 'ipconfig' IP address

Step 3: Enter the following command in the CLI window to check whether the connectivity is normal.

Ping 192.168.1.1

If the interface shown in Figure 3-5 is displayed, the local computer is properly connected to the G51 router.

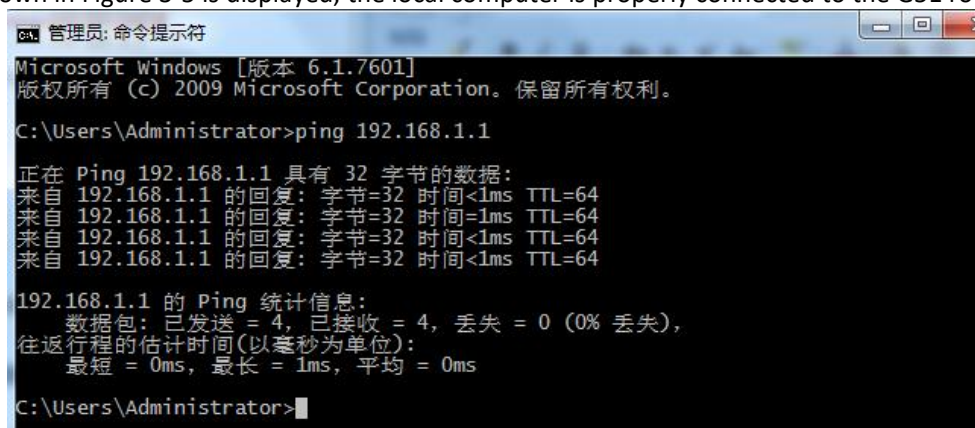


Figure 3-5 Connectivity Verification Results

4. Configuration introduction

4.1. Establish a web configuration environment

The Router can be configured through a local Ethernet interface. The default IP address set for the local Ethernet interface is 192.168.1.1, the subnet mask is 255.255.255.0. Perform the following steps to set up a web configuration environment:

1. Connect the LAN interface of the Router and the Ethernet interface of the computer with an Ethernet cable, the default computer can automatically obtain the IP address, and the IP address of the computer can also be fixed The format is: 192.168.1.xxx (where xxx represents any number between 2~254) and the subnet mask is 255.255.255.0.

2. Open the browser and enter "HTTP:192.168.1.1" in the address bar. In the login dialog box that appears, enter the username and password that you want to log in. The default username/password is admin/admin, as shown in Figure 4-1



Figure 4-1 Web Configuration Management User Authentication Page

4.2. System Status

You can query the status of the mobile network to learn about the "mobile network status" and "mobile network device information". In this way, the network and devices are healthy according to the relevant status.

LOG IN TO THE WEB CONFIGURATION PAGE OF THE ROUTER AND CLICK SYSTEM INFORMATION, AS SHOWN IN FIGURE 4-2

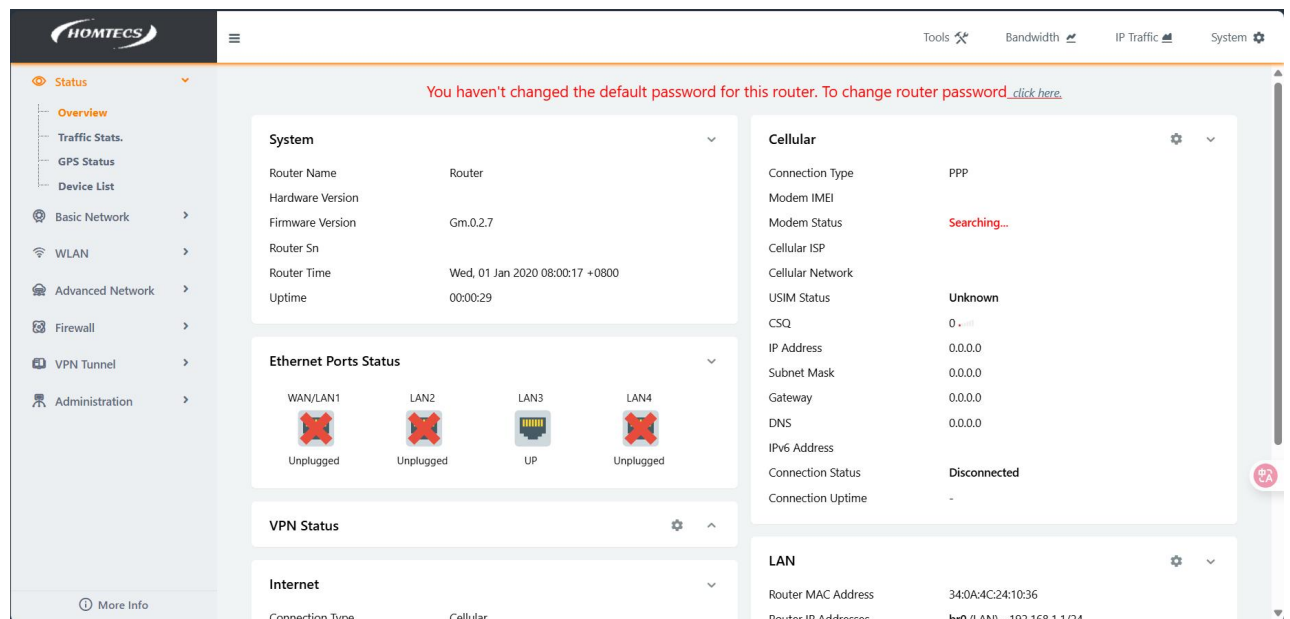


Figure 4-2 Screenshot of the Router status Table 4-1 of

the parameters on the Mobile Network Status page:

Parameter	Meaning
The name of the router	The current router name can be set in System Administration - System Identity
Hardware version	The current router hardware version
Firmware version	The version of the current router program
Router time	After networking, NTP actively aligns with the network time server, see Time Setting Parameters for details
Boot time	Displays the duration of the router when it is powered on
Total/Remaining Memory	The total memory of the router, and the remaining available memory
Connection type	The name of the current mobile network dial-up rule
Modem type	Mobile module model
IMEI	International Mobile Equipment Identification

Modem status	Check whether the module connection is normal
USIM status	Displays SIM card status
Signal strength	The signal strength of the wireless network, the value range: 1~31, if there is no signal, it will not be able to dial successfully.
IP address	The IP address assigned by the carrier obtained when the Router dials up.
Subnet mask	The carrier assignment that the Router gets when dialing up. 255.255.255.x
gateway	The address of the carrier-assigned gateway obtained when the Router dials the number.
Connection status	There are two states: connected and disconnected
Connection time	Displays the online duration of the Router after the dial-up is launched

Table 4-1

5. Basic network configuration



The web configuration interface is subject to change depending on the software version.

After entering the web configuration page, you can view the status of the router or change the router settings through the web configuration page. The following describes the common configurations.

5.1. WAN network configuration

In the navigation bar, select "Basic Configuration > WAN Network". On the page that opens, you can modify the parameters of configuring the WAN network. As shown in Figure 5-1:

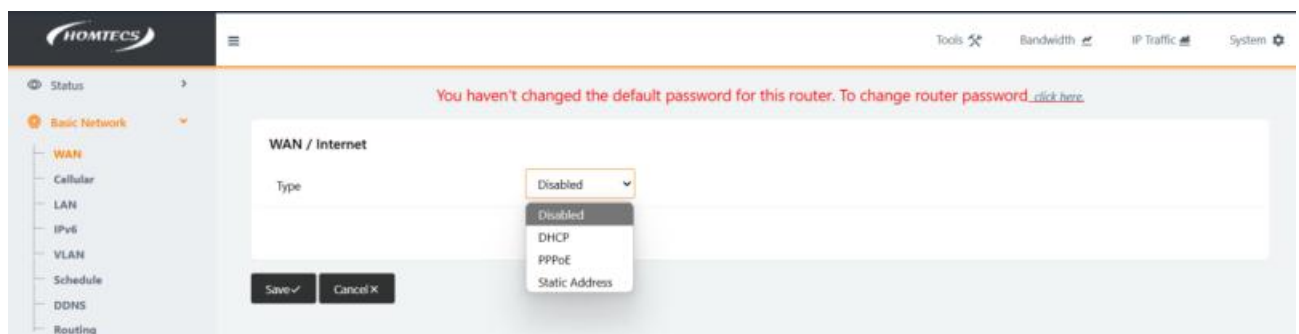


Figure 5-1 WAN connection type selection

According to the networking situation of the field application, select the Internet connection type provided by your ISP from the drop-down menu, including the following WAN connection types: PPPoE, static IP, dynamic address acquisition, and other WAN port access methods. As shown in Figure 5-2:

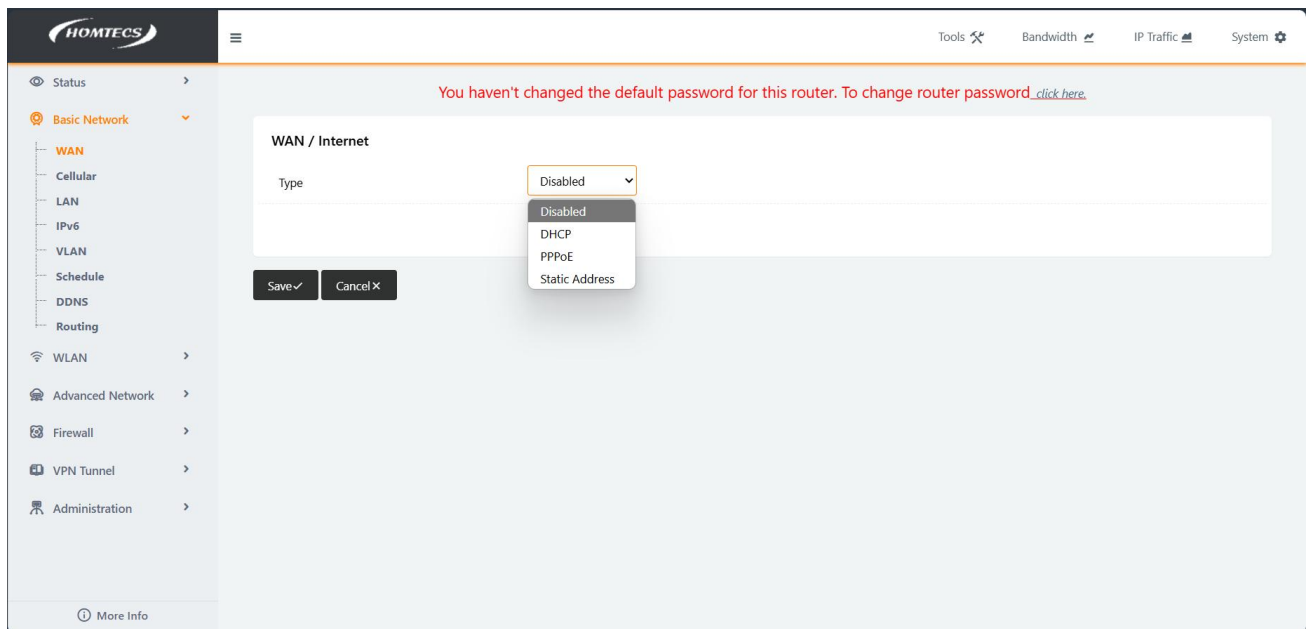


Figure 5-2 WAN Static Address Selection

Table 5-1 describes the WAN port connection type.

Parameter	Meaning	How to configure
Connection type	The type of connection for the WAN.	<p>The drop-down box contains:</p> <p>Static IP address: Manually configure IP addresses, gateways, and DNS information.</p> <p>DHCP :D the HCP client automatically obtains an IP address and accesses the Internet through WA.</p> <p>PPPoE: PPPoE dial-up to obtain IP addresses (dial- up to the Internet through ADSL).</p>
Displayed when Connection Type is set to Static IP		
IP	If Connection Type is set to Static IP, you need to set this parameter to Connection Type.	If Connection Type is set to Static IP, you need to set this parameter to Connection Type
Displayed when PPPoE is selected for Connection Type in the basic settings		
The name of the service	The PPPoE service name is usually used for identification and judgment between the client and the server, and is usually provided by the server, and is provided by the ISP when dialing up the ADSL number.	The general WORD type, up to 64 bytes, cannot be empty
Username/password	The username/password used for PPPoE dial-up is usually provided by the server, and by the ISP when dialing up ADSL.	In general, the maximum length of each WORD type and CODE type is 64 bytes, and none of them are empty

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Table 5-1

5.2. Mobile network configuration



- 1.The card authentication mode of most domestic operators is PAP, so the custom dialing option is configured as (separated by spaces) refuse-chap refuse-mschap refuse- mschap-v2; If it is a CHAP or other certification, you can adjust the corresponding parameters.
- 2.VPDN private network APN access point, user name and password need to be provided by the operator
- 3.Note that the APN private networks of China Unicom and China Mobile have dedicated APN access points, while China Telecom does not have APN access, only the user name and password are required
- 4.4G/5G LTE networks, whether TDD or FDD, the three major operators have a tendency to uniformly set APN as empty
- 5.If it is a public network card, the default authentication user name and password of China Telecom 3G are card, and the user name of a small number of cards needs to be configured to ctnet@mycdma.cn and the password to vnet.mobi
- 6.If it is a public network card, the APN of the mobile 3G network is CMNET, and some are CMWAP
- 7.If it is a public network card, the APN of China Unicom's 3G network is 3GNET, and some of it is 3GWAP

In the navigation bar, select Basic configuration > mobile networks. You can modify the relevant parameters of the mobile network, as shown in the following figure:

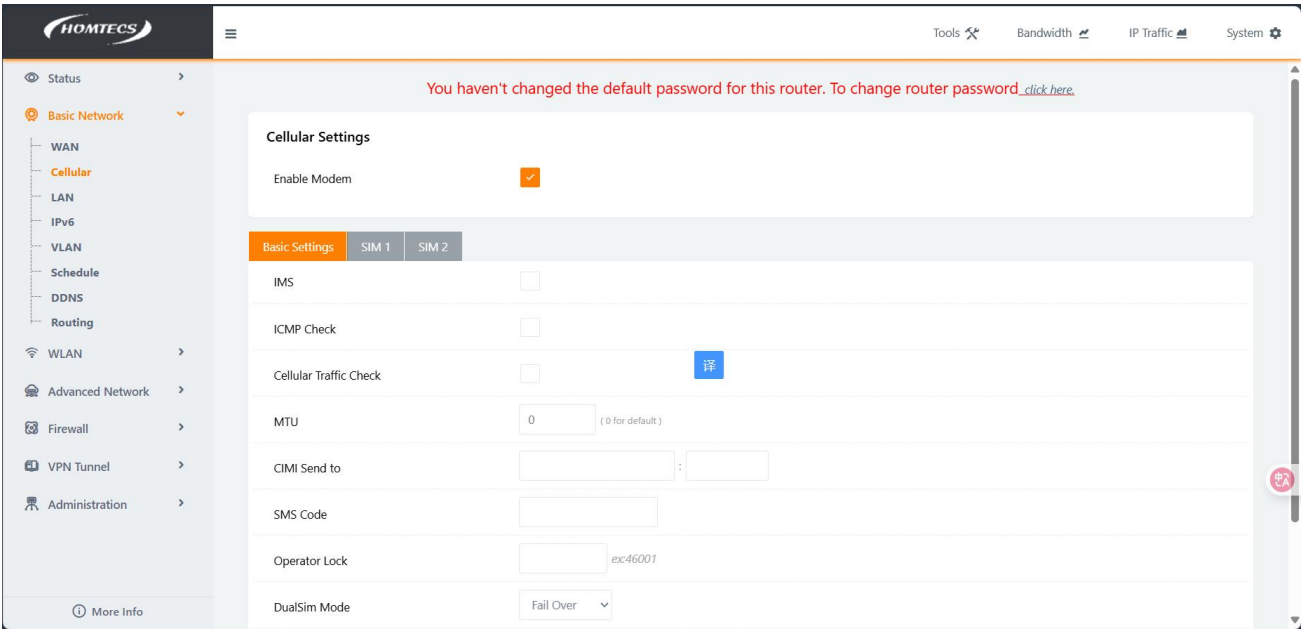


Figure 5-3

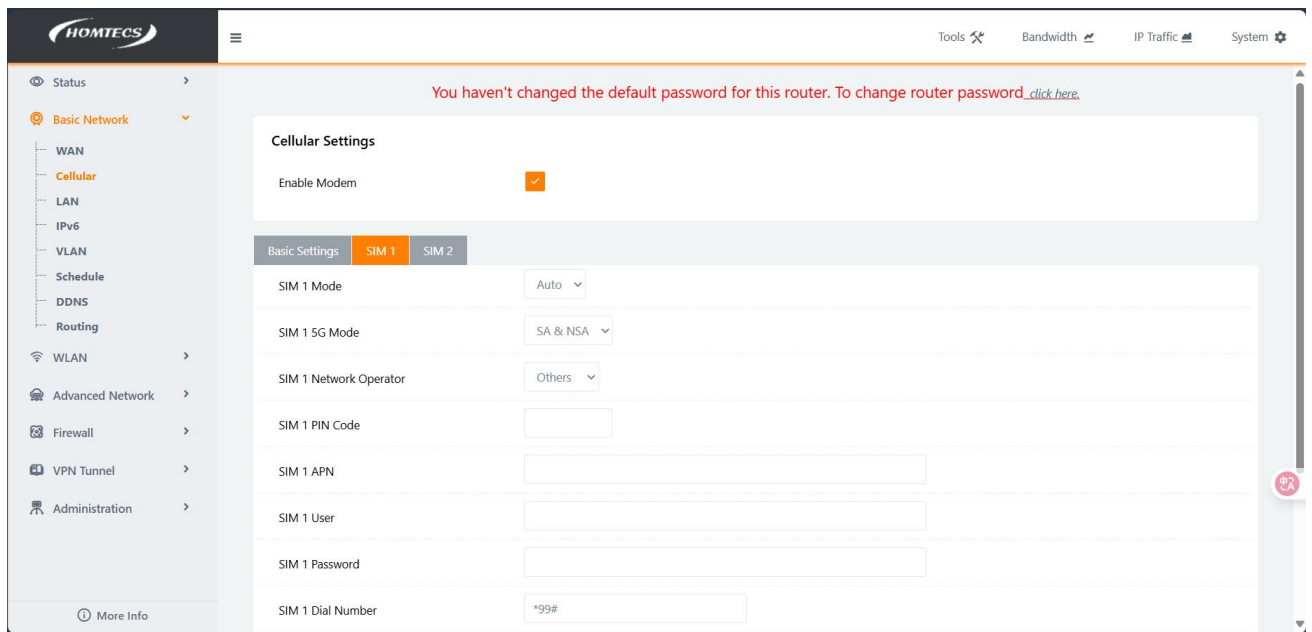


Figure 5-4

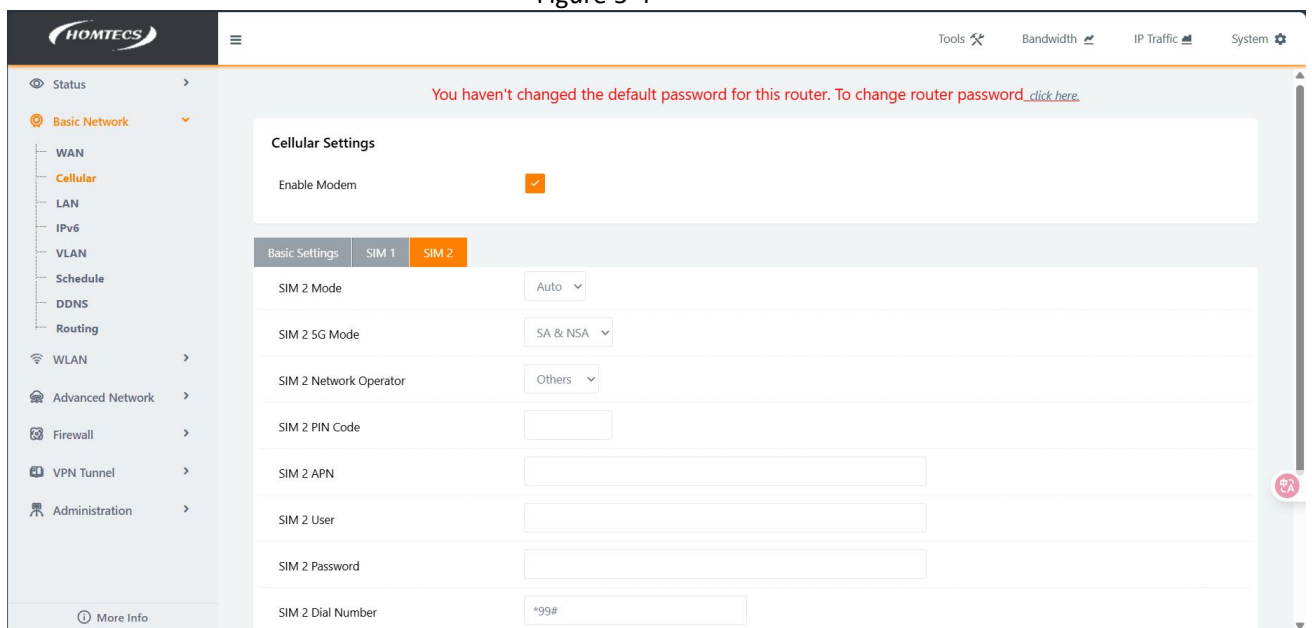


Figure 5-5 Screenshot of mobile network configuration

For details about the mobile network configuration parameters, see Table 5-2:

parameter	illustrate
Enable the module	means enabling or deactivating a wireless module; It is enabled by default
IMS	refers to the way the core network is accessed; It is off by default
Enable PPP mode	PPP dial-up mode is enabled and disabled by default
ICMP link detection	The ICMP link detection mechanism is enabled and disabled by default
Detect IP addresses	Refers to the IP address that needs to be detected by the link, and checks whether the host is reachable and whether the route is available
interval	The interval between the time interval at which the IP address was detected

parameter	illustrate
retry	After the detection fails, the exception handling action is performed after the number of consecutive failures is reached
ICMP RTT enabled	RTT (round-trip delay); It is off by default
RTT Threshold (Threshold)	The default value is 50ms, and exception handling operations are performed if the network delay exceeds 50ms. Range 50-2000ms
Exception handling	There are two actions that are performed when the number of retries is reached: reboot the system or redial
Traffic checks	Detect whether the Internet interface generates data traffic, if no traffic is generated within the detection time, perform exception handling and restart name redialing, which is disabled by default
Check the pattern	Rx, Tx, and Rx&Tx, that is, upstream and downstream data detection methods
Detection interval	The detection interval is used to determine whether the traffic rate increases compared with the previous time
Exception handling	Detect traffic and perform exception handling if there are no two changes to the previous comparison: reboot the system or redial
CIMI sent to	The TCP client sends two parameters, CCID and IMEI, to the service address and port, which are empty by default
SMS verification code	SMS verification code; For example, if the verification code is 1234, edit the SMS 1234 * reboot to send the routing SIM card, which is empty by default
Carrier lock- in	Lock your carrier's network number
Dual-SIM mode	There are four modes: automatic switching, card 1 only, card 2 only, backup mode Automatic switching: If card 1 fails to find the card, card 2 is switched, and card 2 fails to switch card 1 Automatic switching by default
SIM 1 network mode	Auto, 5G NR, 4G LTE (FDD/TDD), 3G (WCDMA/TD-SCDMA/HSPA), and 3G (CDMA 2000/CDMA 1x) are the default Auto
SIM 1 5G network standard SIM 2 5G network standard	SA&NSA, NSA, and SA are SA&NSA by default, and take effect only for 5G NR networks
SIM 1 network operator SIM 2 network operator	Others、Verizon; The default is Others, other carriers except Verizon

parameter	illustrate
SIM 1 Enable the lock band function SIM 2 enables the lock band function	Forced 5G NR, forced 4G LTE (FDD/TDD) will enable this function, and will be disabled by default. If this function is enabled, you can lock the band function
SIM 1 SA Band/NSA/LTE Band SIM 2 SA Band/NSA/LTE	Force 5G NR, open SIM 1/SIM 2 SA lock band setting; Force 4G LTE (FDD/TDD), open SIM 1/ SIM 2 LTE lock band setting;
SIM 1 PIN	Set a PIN for your SIM card
SIM 1 dialing number	The carrier's network access number
SIM 1 APN Access Point	Parameters of the service type provided by the carrier
SIM 1 username	PPP authentication username
SIM 1 password	PPP Authentication Password
SIM 1 authentication method	Default Auto, PAP, CHAP, MS-CHAP, MS-CHAPV2
SIM 1 Local IP	To obtain an IP address, the SIM service must be bound to the specified IP address

Table 5-2 Mobile Network configuration parameters

5.3. ICMP detection

The G51 Router not only supports this detection method, but also provides more reliable ICMP for abnormal phenomena such as false links in wireless networks, which are usually maintained by LCP and other methods Link detection function. ICMP detection mainly detects communication links through ping packet detection, and performs user-set actions when the link is abnormal to achieve rapid recovery of links and systems.

STEP 1: OPEN THE MOBILE NETWORK UNDER BASIC NETWORK ON THE WEB CONFIGURATION PAGE, AS SHOWN IN FIGURE 5-6.

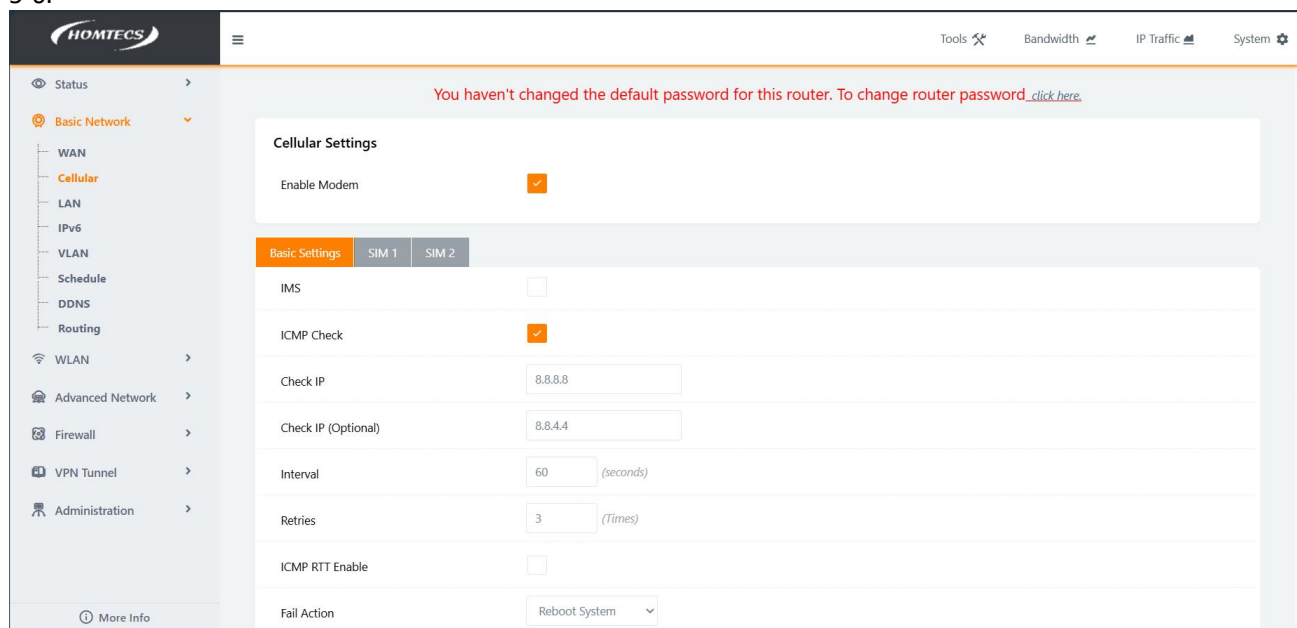


Figure 5-6 Mobile Network Configuration

Step 2: Configure ICMP detection service parameters

Parameter	Meaning	How to configure
Internet ICMP check	ICMP Detection Rule: enabled or disabled	Default parameter: Disabled
Detect IP address	TWO IP ADDRESSES ARE DETECTED, FIRST USE IP1 TO DETECT IF IT IS SUCCESSFUL, WAIT FOR THE NEXT TIME, AND IF THE TWO IP ADDRESSES FAIL TO PING ALTERNATELY, THE EXCEPTION HANDLING ACTION IS CARRIED OUT IF BOTH FAIL.	THE DEFAULT IP ADDRESS FOR EFFECTIVE PINGING IS 8.8.8.8
Detection interval	The detection interval and the maximum number of failures when the link is normal. When the maximum number of failures is reached, the ICMP rule executes the corresponding action tasks, such as modem redialing	Value range: 1~65535 (seconds). Default: 60 seconds
retry	Frequency setting	Value range: 1~1440 (times). Default: 3 (times)
ICMP RTT enabled	The RTT (Round-Trip Delay) feature is enabled	It is off by default
RTT Threshold (Threshold)	The highest value of network latency	The default value is 50ms, and exception handling operations are performed if the network delay exceeds 50ms. Range 50-2000ms
Exception handling	There are two ways to detect that the IP address is unreachable: reboot the system and redial	Default: Reboot the system

Table 5-3 ICMP detection parameters

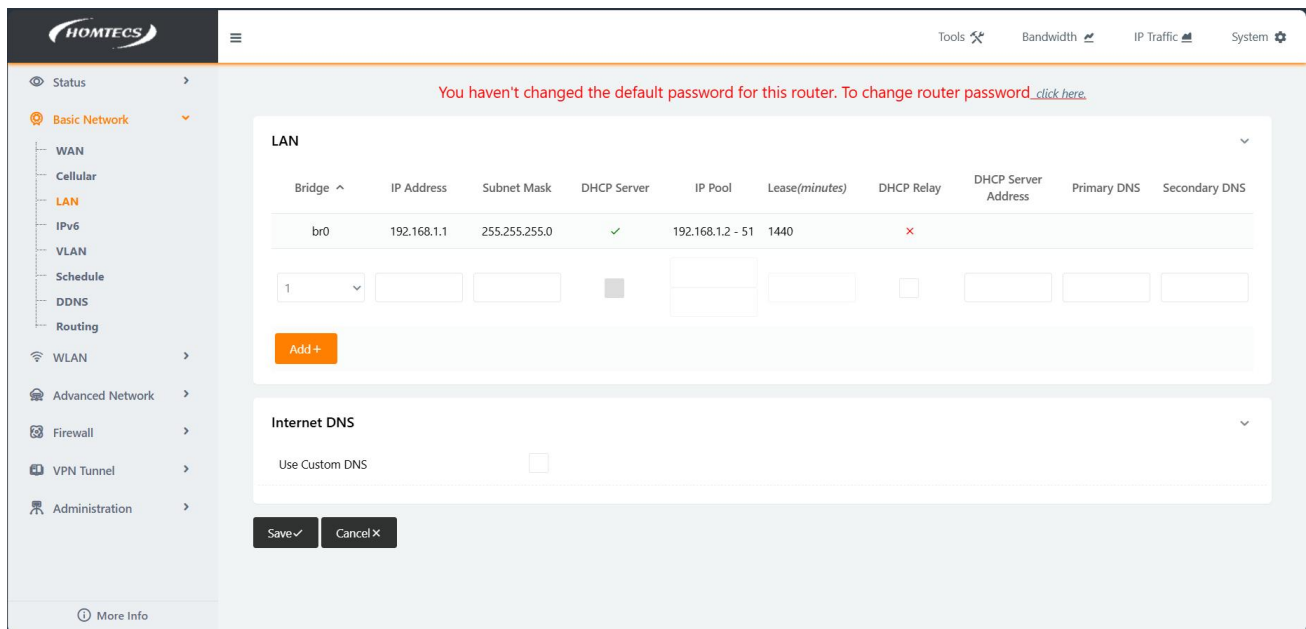
Step 3: Click Save to complete the addition of ICMP detection.



If an ICMP packet is abnormal, the ICMP packet is sent continuously according to the ICMP detection system, and if the destination address is unreachable, the backup address is detected. If the number of times the backup address is unreachable also reaches the number of retries, the exception handling operation is executed.

5.4. LAN configuration

In the navigation bar, select "Basic Configuration > Local Area Network". On the page that opens, you can modify the parameters of configuring the local area network, as shown in Figure 5-7



Figure

5-7 Screenshot of LAN configuration

Table 5-4 describes the parameters of LAN configuration

parameter	illustrate
Bridging	The default br0 parameter range of the interface is 0-4; LAN1-LAN4 network ports are used with VLANs
Router IP address	The IP address of the router, the default IP address is 192.168.1.1
Subnet mask	The mask address of the router, the default mask is 255.255.255.0
DHCP services	Dynamically assign IP services. Once the DHCP service is selected, the IP address range and lease options will appear below.
IP address ranges	IP addresses within the LAN range 2-254
lease	By default, the IP address automatically assigned by DHCP is valid at 1440
Added BR1-BR3	For details about how to use a VLAN with a VLAN, see VLAN Description
DHCP trunk	Enabled or disabled, disabled by default;
DHCP server address	The default is empty, format: A.B.C.D

Table 5-4 "Local Area Network" Configuration Parameters

After the configuration is completed, click the "Save Settings" button. After saving the configuration, the device will automatically restart for the corresponding configuration to take effect.

5.5. IPv6

IP is the abbreviation of Internet Protocol, while ipv6 is the sixth version of the Internet Protocol. It is a globally recognized next-generation Internet business application solution and the next-generation Internet protocol version formulated by the international standardization organization IETF to address the depletion of IPv4 addresses. It can provide massive network address resources and broad innovation space. Its number of addresses claims to be able to write an address for every grain of sand in the world.

The address length of IPv4 is 32 bits, and the number of addresses is 2^{32} , which is 4294967296; The length of ipv6 addresses is 128 bits, the number of addresses is 2^{128} , and there are about 3.4×10^{38} addresses. Because the number of ipv6 addresses is huge, it also greatly solves the problem of insufficient number of ipv6 network address resources. With the development of the Internet, IPv6 is needed as a support in emerging fields such as 5G, the Internet of Things, cloud computing, and driverless driving. The popularization of ipv6 is a general trend.

Step 1: Configure as follows, enable IPv6 penetration (default not enabled, device cannot obtain IPv6 address):

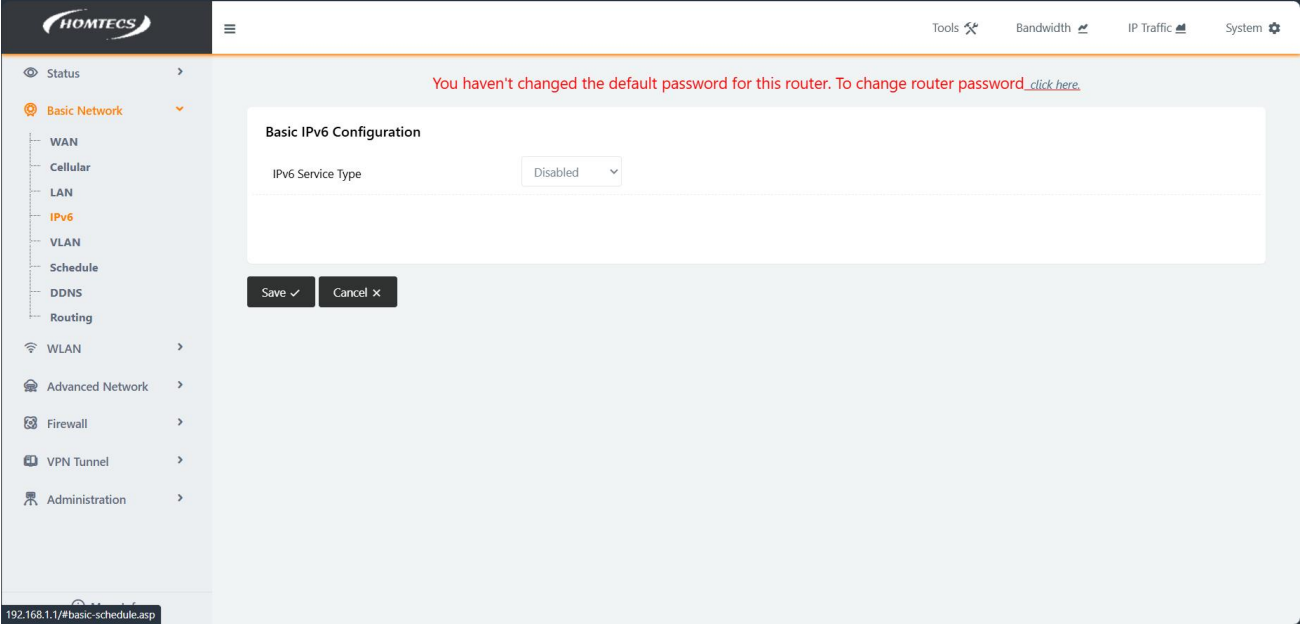


Figure 5-8

Step 2: After the module goes online, you can obtain the IPv 4 and IPv6 addresses, and the LAN will assign a RouterIPv6 address, through which you can access the router page locally, and the DNS and Router ipv automatically obtained by the local PC6 addresses are consistent:

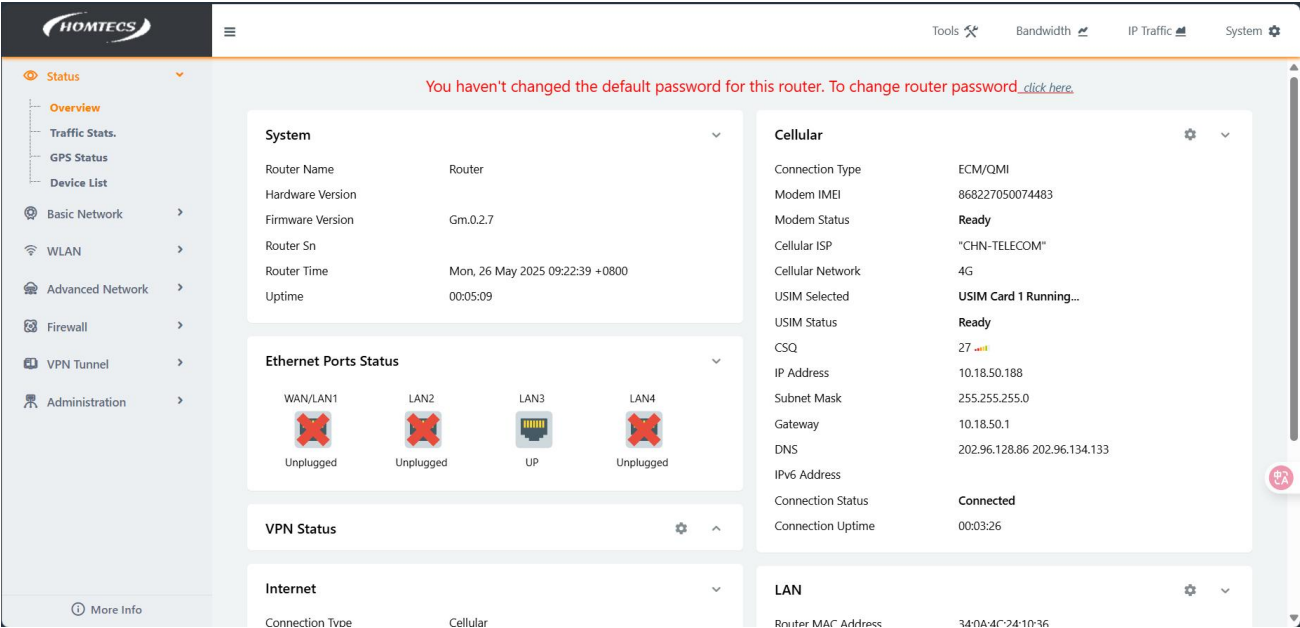


Figure 5-9

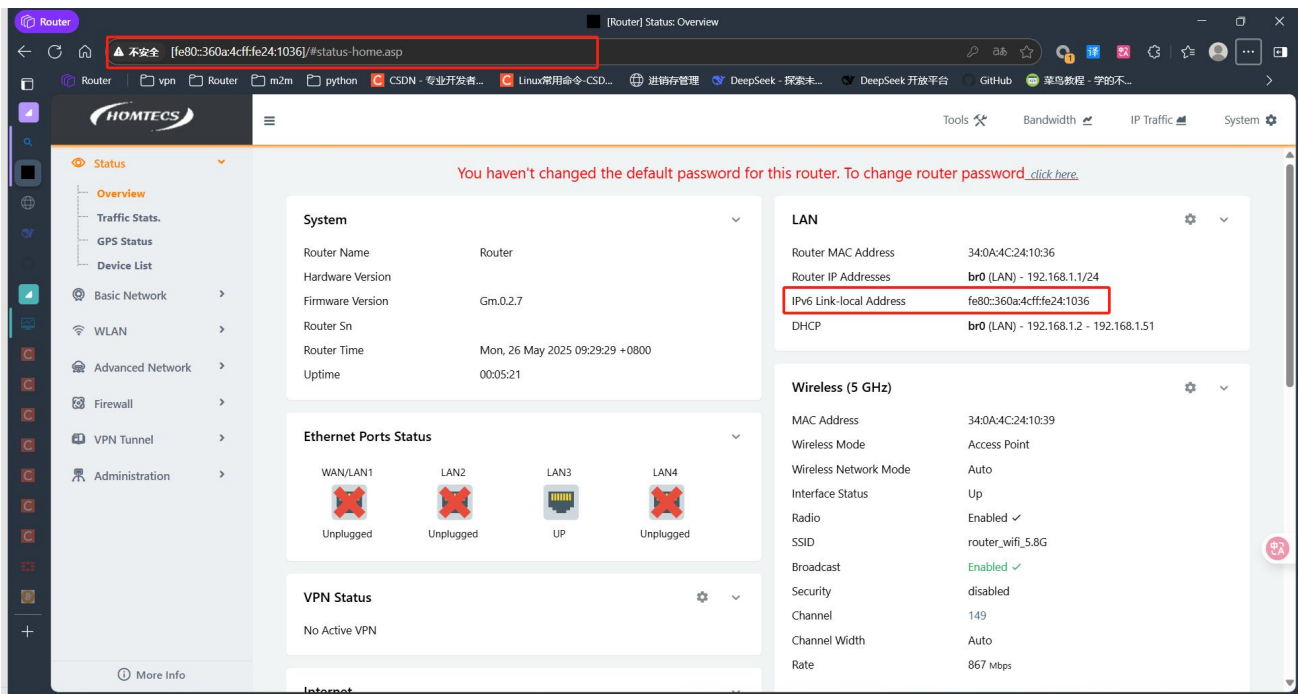


Figure 5-9

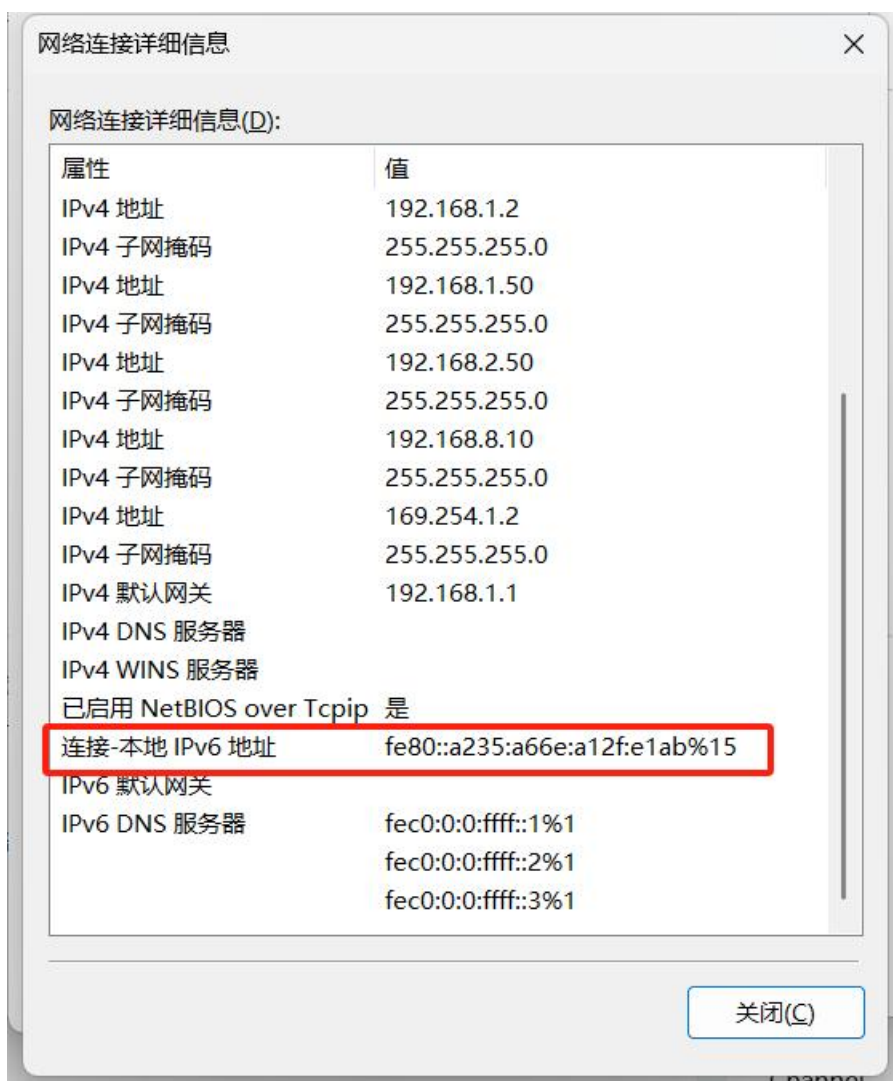


Figure 5-11

Step 3: Disconnect from other networks, use only the router to provide network to the PC, ping `www.baidu.com` and ping `baidu.com` respectively, the result is as follows:

```
15/01/2024 10:11.44 /home/mobaxterm ping baidu.com

正在 Ping baidu.com [39.156.66.10] 具有 32 字节的数据:
来自 39.156.66.10 的回复: 字节=32 时间=56ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=77ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=91ms TTL=47
来自 39.156.66.10 的回复: 字节=32 时间=445ms TTL=47

39.156.66.10 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 56ms, 最长 = 445ms, 平均 = 167ms

15/01/2024 10:19.04 /home/mobaxterm ping www.baidu.com

正在 Ping www.a.shifen.com [240e:ff:e020:9ae:0:ff:b014:8e8b] 具有 32 字节的数据:
来自 240e:ff:e020:9ae:0:ff:b014:8e8b 的回复: 时间=48ms
来自 240e:ff:e020:9ae:0:ff:b014:8e8b 的回复: 时间=47ms
来自 240e:ff:e020:9ae:0:ff:b014:8e8b 的回复: 时间=50ms
来自 240e:ff:e020:9ae:0:ff:b014:8e8b 的回复: 时间=34ms

240e:ff:e020:9ae:0:ff:b014:8e8b 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 34ms, 最长 = 50ms, 平均 = 44ms
```

Figure 5-12

5.6. VLAN

Virtual Local Area Network (VLAN) is a communication technology that logically divides a physical LAN into multiple broadcast domains. Compared with traditional LAN technology, VLAN technology is more flexible, and it has the following advantages: Reduced management overhead for moving, adding, and modifying network devices; It is possible to control broadcasting activities; It can improve the security of the network.

In the navigation bar, select “Basic Network >VLAN”. On the page, you can modify the parameters related to configuring a dynamic domain name. As shown in Figure 5-13

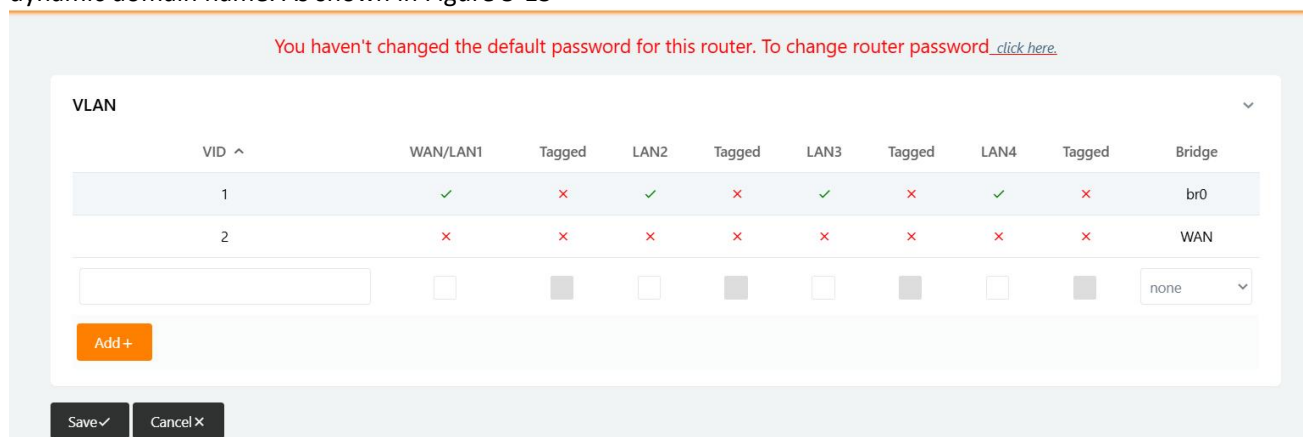


Figure 5-13

Table 5-5 VLAN parameter description

Parameter	Description
VID	Each VLAN switch port needs to be bound with a VID (VID range 0-15).
LAN1 、 LAN2 、 LAN3、 LAN4、 WAN	Corresponding to the physical interface of the routing device: 4 x LAN and 1 x WAN

Parameter	Description
Tagged	The data frames received from the trunk port (tagged and tagged) are tagged, and the data frames sent from the trunk port need to be tagged (regardless of the default VLAN).

Table 5-2

VLAN setting method

- 1. Each VLAN switch port needs to be bound with a VID. (VID range 0-15).
- 2. Each VLAN switch port falls into one of three categories: access and trunk
 - 2.1. Access port (equal to unchecked tagged - marked unchecked): the data frames received from such ports are not tagged, and the data frames sent from such ports are not tagged;
 - 2.2. Trunk port (equivalent to checking tagged-marked): the data frames received from such ports are tagged, and the data frames sent from such ports need to be tagged (regardless of the default VLAN);
 - 2.3. By default, the LAN port is br0 192.168.1.1, and three address segments can be added for different interfaces
- 3. By default, the LAN port is br0 192.168.1.1, and three address segments can be added for different interfaces.

You haven't changed the default password for this router. To change router password [click here.](#)

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address	Primary DNS	Secondary DNS
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440	✗			
1			<input type="checkbox"/>			<input type="checkbox"/>			

Add +

Internet DNS

Use Custom DNS ☐

Save ✓

Cancel ✕

Figure 5-14

- 4. Set up 3 LANs, one WAN is set as shown in the following figure, assign the WAN to VID 2, that is, bridge the WAN, and assign the other interfaces to the br0 interface

You haven't changed the default password for this router. To change router password [click here.](#)

VLAN

VID ^	WAN/LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
1	✗	✗	✓	✗	✓	✗	✓	✗	br0
2	✓	✗	✗	✗	✗	✗	✗	✗	WAN
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	none

Add +

Save ✓

Cancel ✕

Figure 5-15

- 5. After br1, br2, and br3 are added to the LAN, two LAN ports can be connected to VLANs with different IP segments, and the WAN ports are used independently as WAN ports, as shown in the following figure.

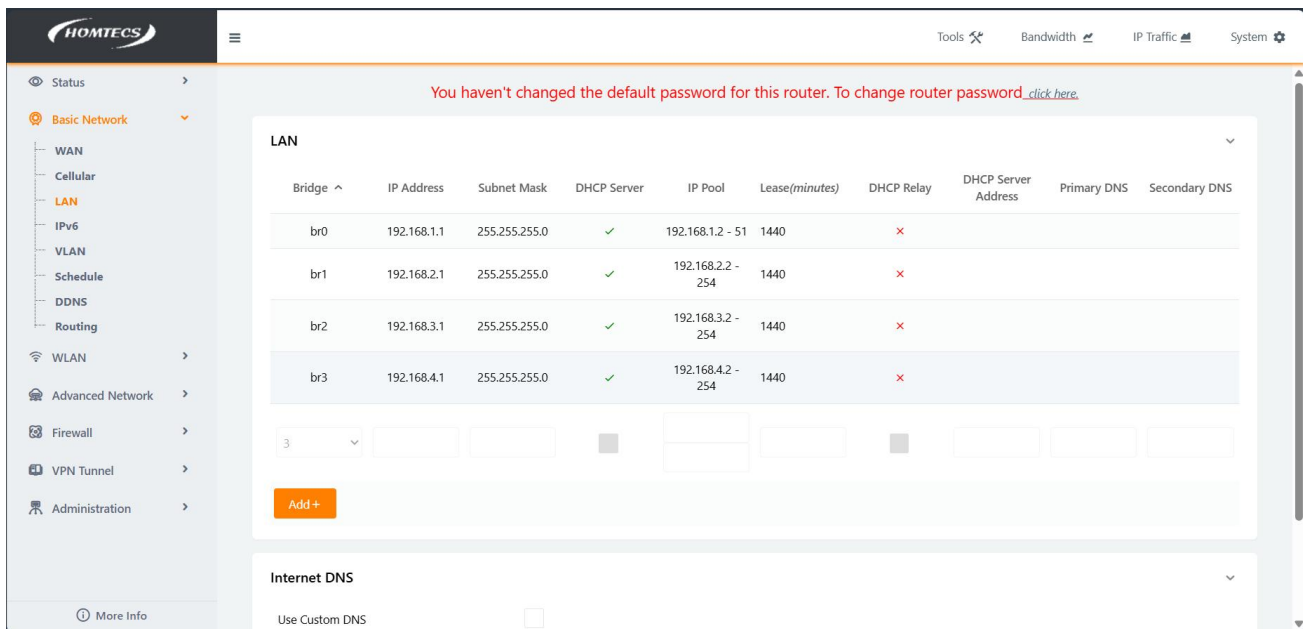


Figure 5-16

6. The 3 LAN ports and WAN ports are configured independently:

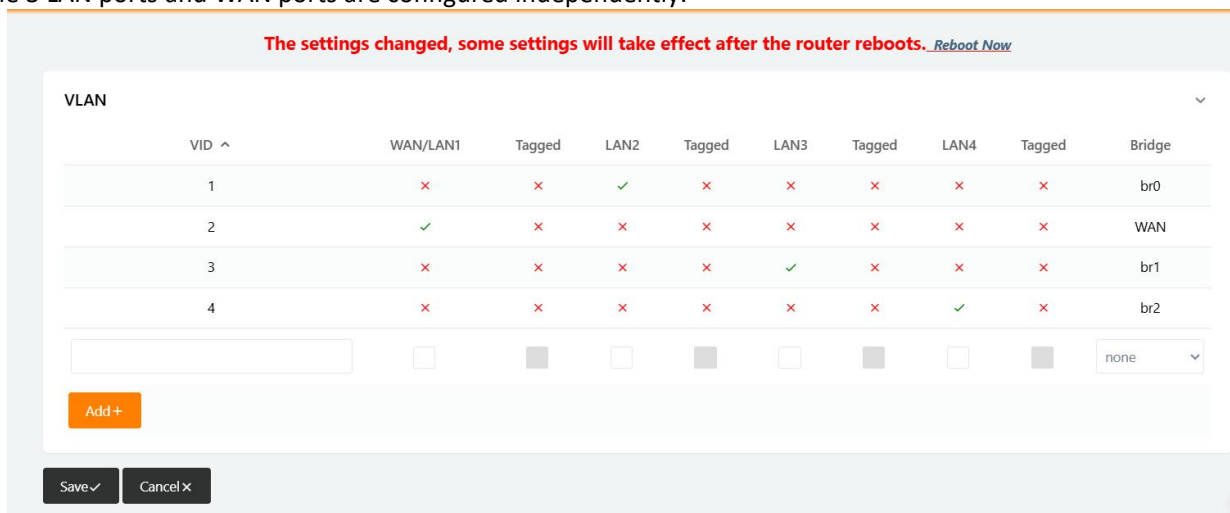


Figure 5-17

7. To label VLAN as trunk mode, the connected devices need to be set to the same VID of 1

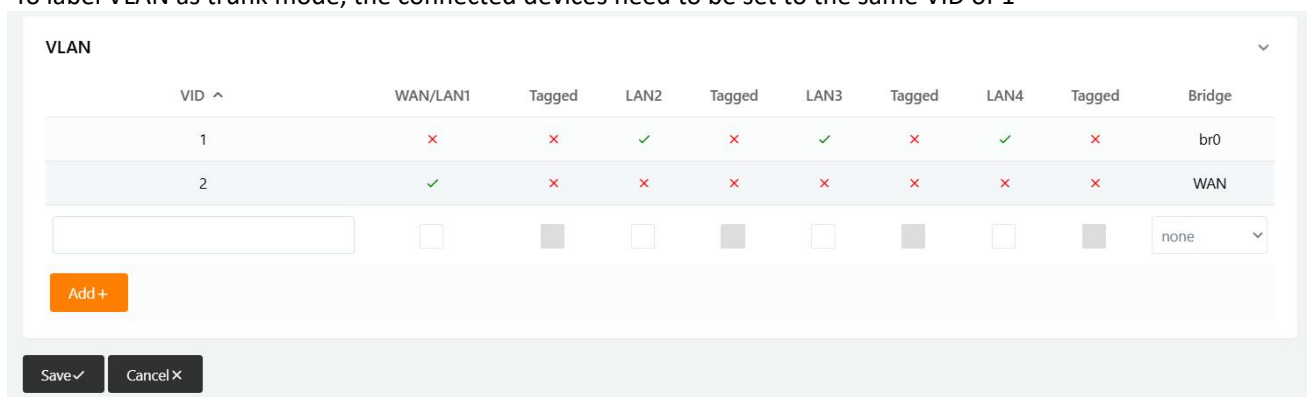


Figure 5-18

5.7. Link Schedule

In the navigation bar, choose Basic Network > Link Schedule. On the page that opens, you can configure the link scheduling WAN and 4G/5G backup mode, or both.



WARNING Only the version of 4G/5G and wired network backup has this function, which is subject to the version of the actual product.

Features:

1. ICMP link detection determines whether the link exists normally by IP address, and triggers the switching mechanism if the IP is not available if the IP is not available in the PING check.
2. The link scheduling strategy can be selected in BACKUP mode: if "WAN" is in link 1, the WAN network is the mainstay, and "modem" in link 2 is in standby. In BACKUP mode, when link 1 is online, link 1 is the main for 4G/5G networks, and link 2 is set in "WAN" for standby, and in BACKUP mode, when link 1 is online, link 1 is primary; When Link 1 fails after ICMP detection, it switches to Link 2. When Link 1 is restored after ICMP detection, it switches back to Link 1.
3. The link scheduling policy can be selected in FAILOVER mode, which means that link 1 and link 2 are backup mode for each other, and when link 1 is online, link 1 is the main link. After link 1 fails, it switches to link 2 after ICMP detection, and link 2 is the primary link. When link 1 takes effect again, link 2 remains the primary link and will not be switched back to link 1. After Link 2 fails, it switches to Link 1 after ICMP detection, and Link 1 is the primary link.
4. The WAN port supports DHCP automatic acquisition, static address, and PPPoE fixed network access, and the WAN needs to be enabled by default.

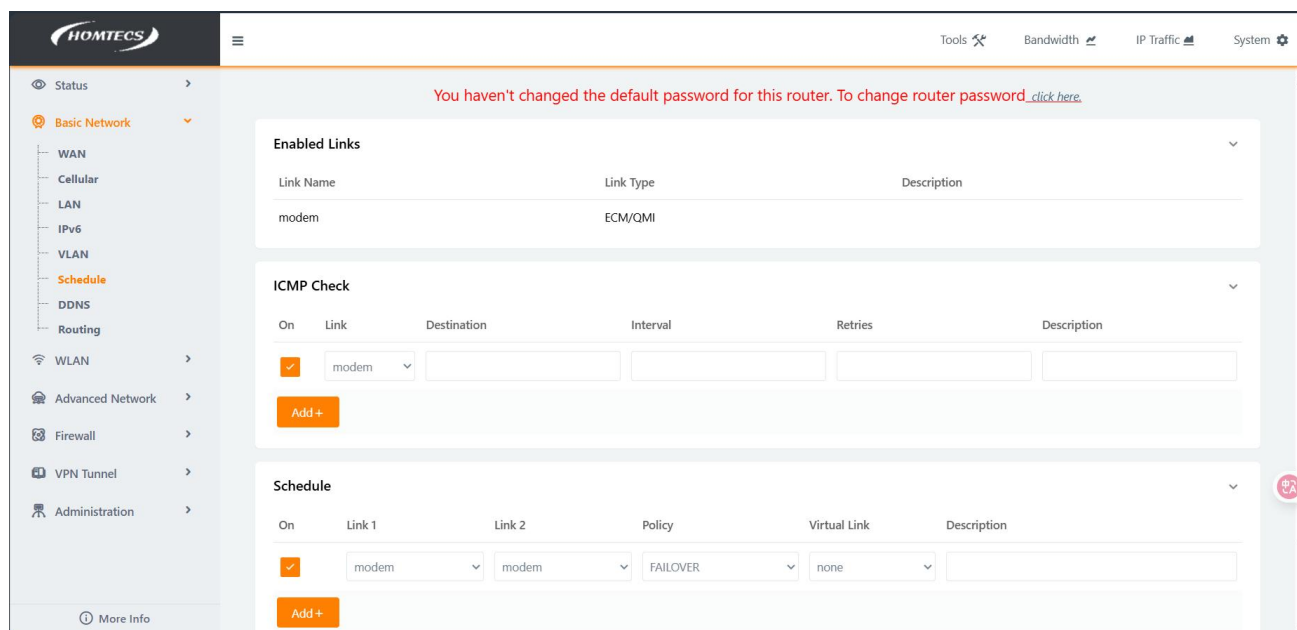


Figure 5-6

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Parameter	Description
ICMP Link Detection - Links	The default link name is modem, wan, sta, and sta2
ICMP Link Detection - Destination Address	Refers to the IP address or domain name that needs to be detected by the link, and whether the host is reachable and whether the route is available
ICMP Link Detection - Spacing	The interval between the time interval at which the IP address was detected
ICMP Link Detection - Retry	After the detection fails, the number of consecutive failures is toggled after the retry is reached
Link Scheduling - Link 1	The default link name is modem, wan, sta, and sta2
Link Scheduling - Link 2	The default link name is modem, wan, sta, and sta2

Link Scheduling - Policy	The link scheduling policy can be selected in the BACKUP mode: link 1 is WAN primary, link 2 is 4G/5G standby, or link 1 is 4G/5G primary, and link 2 is WAN. In the FAILOVER mode, link 1 and link 2 are backed up to each other
Virtual Link	virtual links; If there are less than two links, the default value is none. If there are more than two links, you need to combine the two links into a virtual link, vlink1 and vlink2, and then select the policy of vlink 1 and vlink2 as one link and the third link

Table 5-3

Link Schedule example:

Step 1:
In the navigation bar, select “Basic Network >WAN”. In the page that opens, select a static address from the drop-down box, set the parameters of the static address, and click Save Settings. As shown in the following figure (Note: The parameter configuration is an example, and the actual configuration needs to be configured according to the site situation):

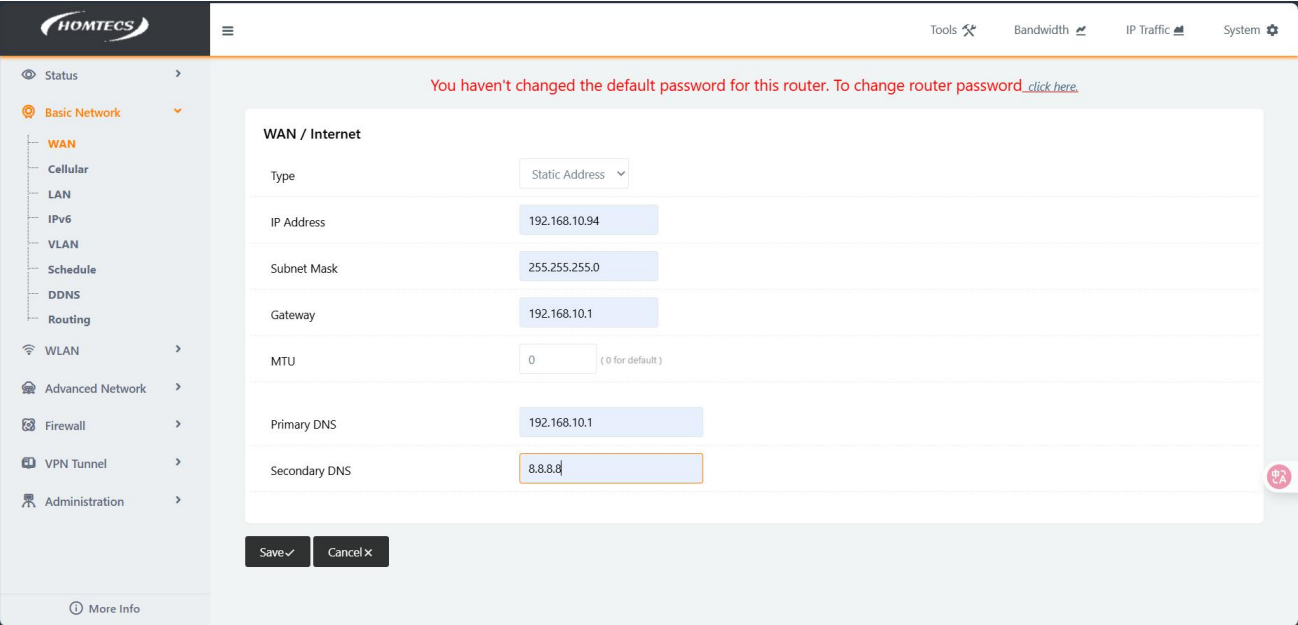


Figure 5-20 Static address settings

Step 2:
① In the navigation bar, select “Basic Network > VLAN”. On the page, remove the WAN with VID1 checked, and click OK, as shown in the following figure:

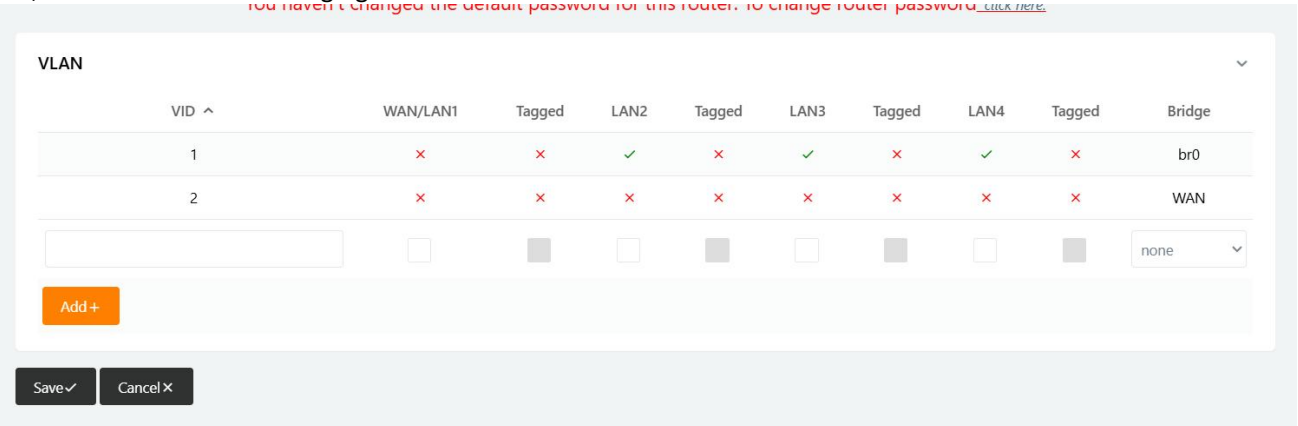


Figure 5-21

② In the VLAN page, add VID2, check WAN, click OK, and click Save Settings after the settings are complete, as shown in the following figure

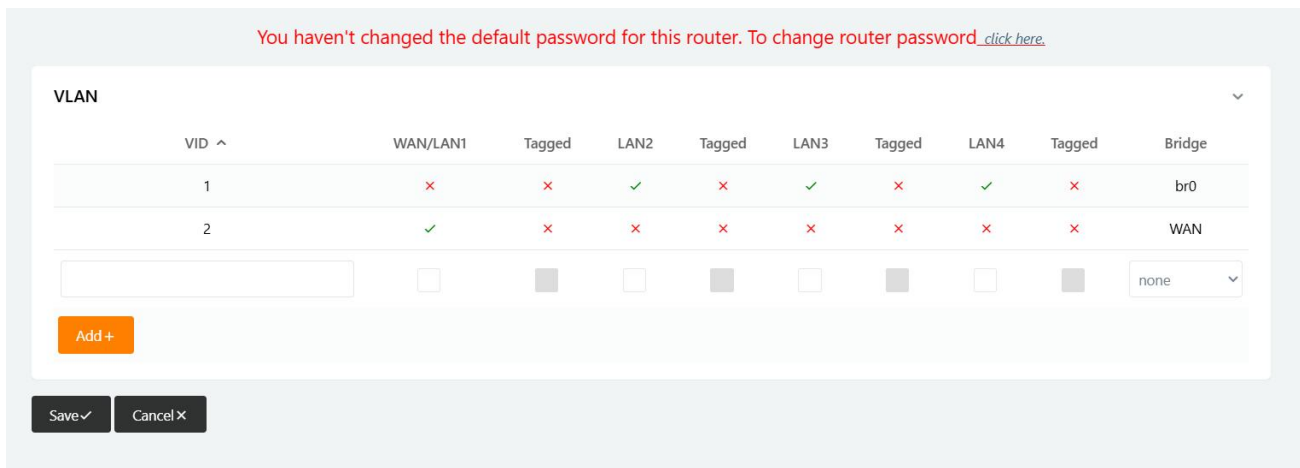


Figure 5-22 VLAN Settings

Step 3:

In the navigation bar, select “Status > Overview”. On the page, view the WAN network status and access the Internet, as shown in the following figure:

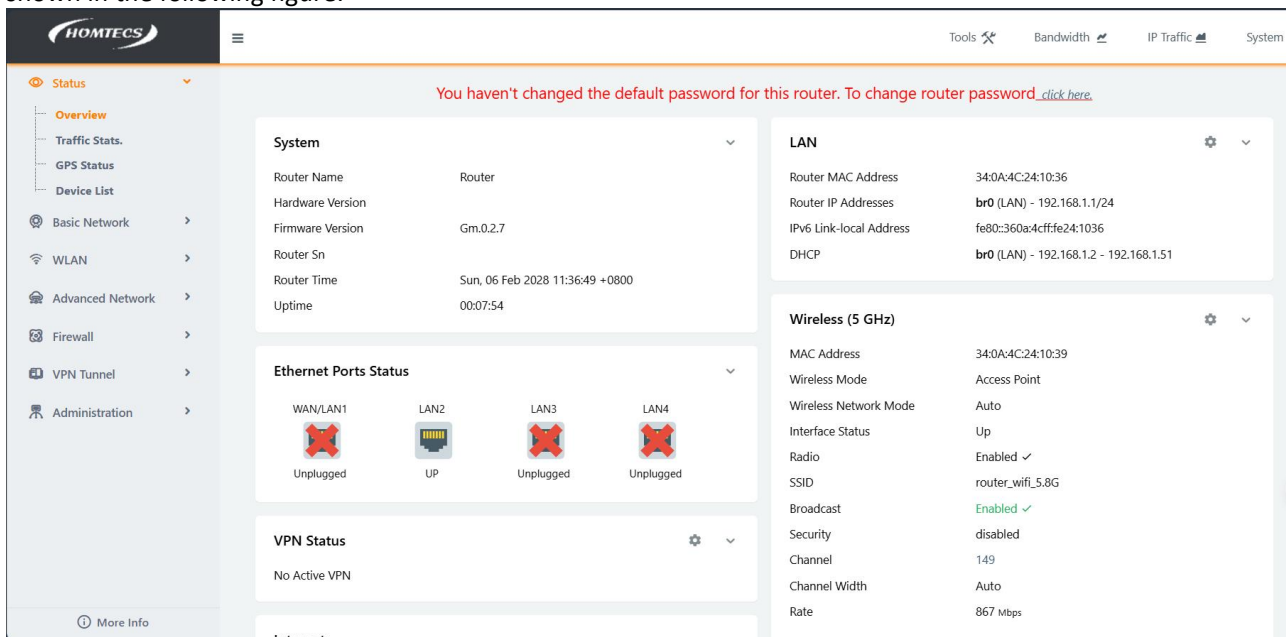


Figure 5-23 WAN network status

Step 4:

Turn on link scheduling in the basic network and configure ICMP link detection and link scheduling (Note: Link 1 is WAN; link 2 is modem), and the policy is backup; After the configuration is complete, click Save and wait for the device to restart.

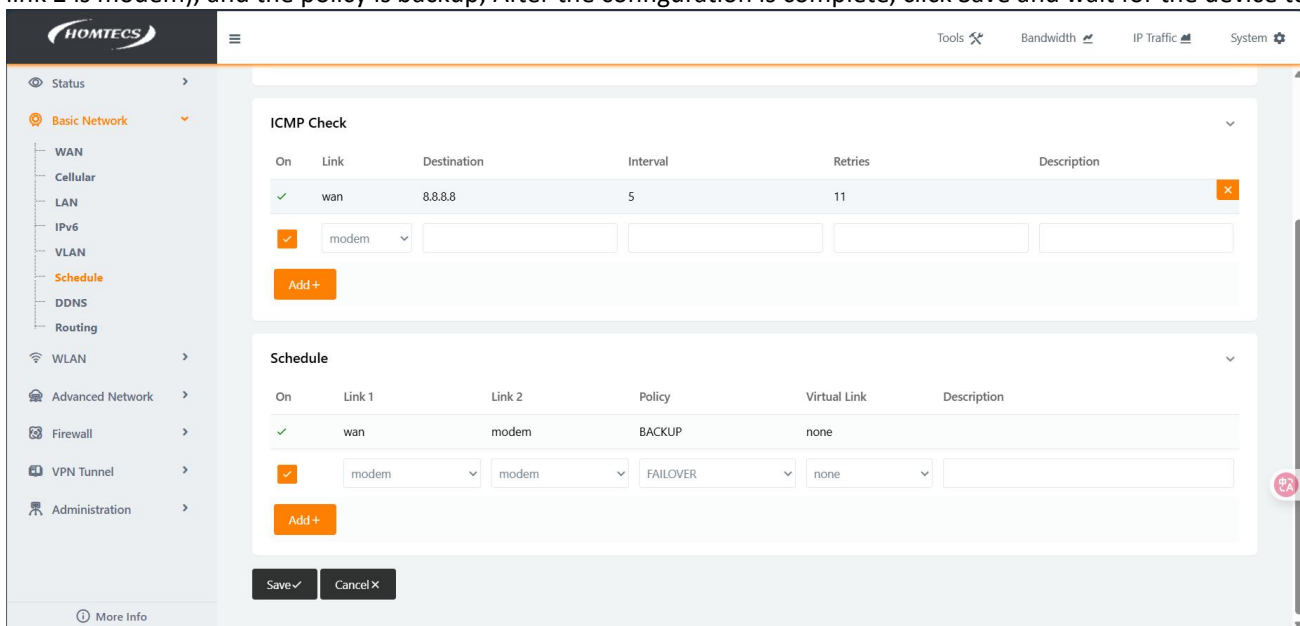


Figure 5-24 Link Schedule settings

Step 5:

Click System Information in Status page to view the WAN connection status (static Internet access is displayed if WAN is the

main), as shown in the following figure:

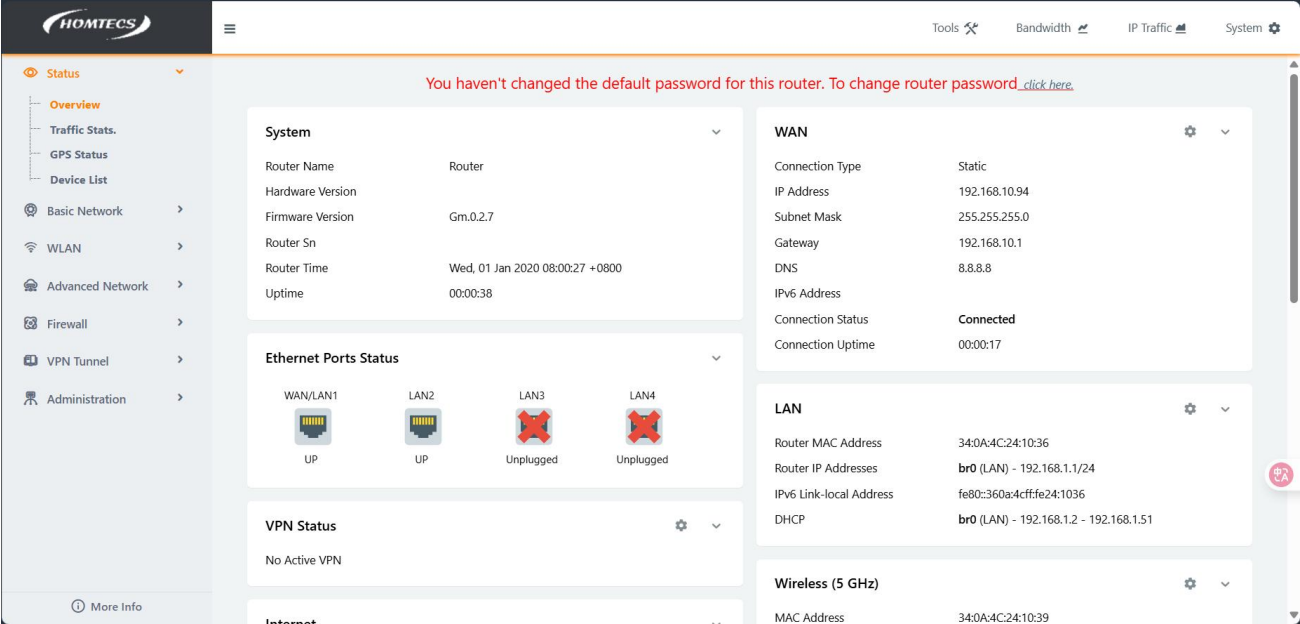


Figure 5-25 WAN Network Status

Step 6:
Disconnect the network cable of the WAN port and check the connection status of the WAN again (the card is online), as shown in the following figure:

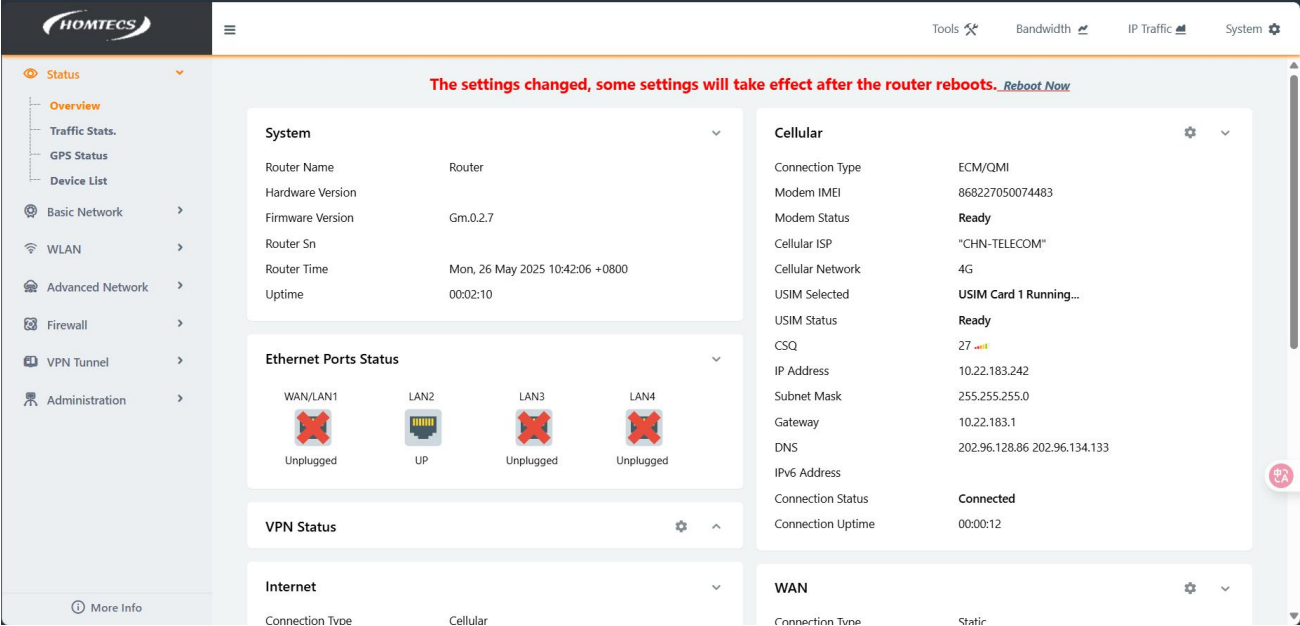


Figure 5-26 WAN network status

Step 7:
When you plug the network cable into the WAN port of the router again, check the WAN connection status (in this case, it is static Internet access), as shown in the following figure:

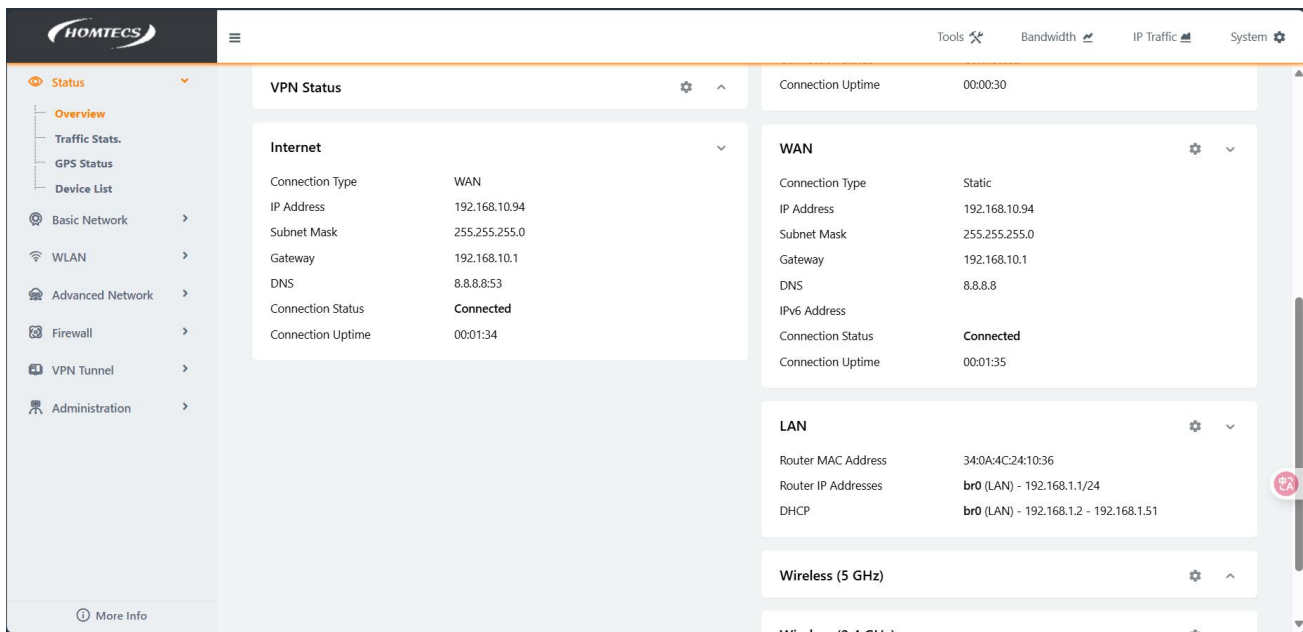


Figure 5-27 WAN networking

5.8. DDNS

DDNS is the abbreviation of Dynamic Domain Name System, and the DDNS protocol provides the corresponding query function between dynamic IP addresses and domain names. DDNS allows users to access the router's page from any PC that can connect to the public network through a domain name. Of course, the network corresponding to the SIM card used by the router must be a public network accessible address, so as to ensure that you can access the router by entering the domain name.

In the navigation bar, select “Basic Network > DDNS”. On the page, modify the parameters for configuring dynamic domain names. As shown in Figure 5-23, see Figure 5-23

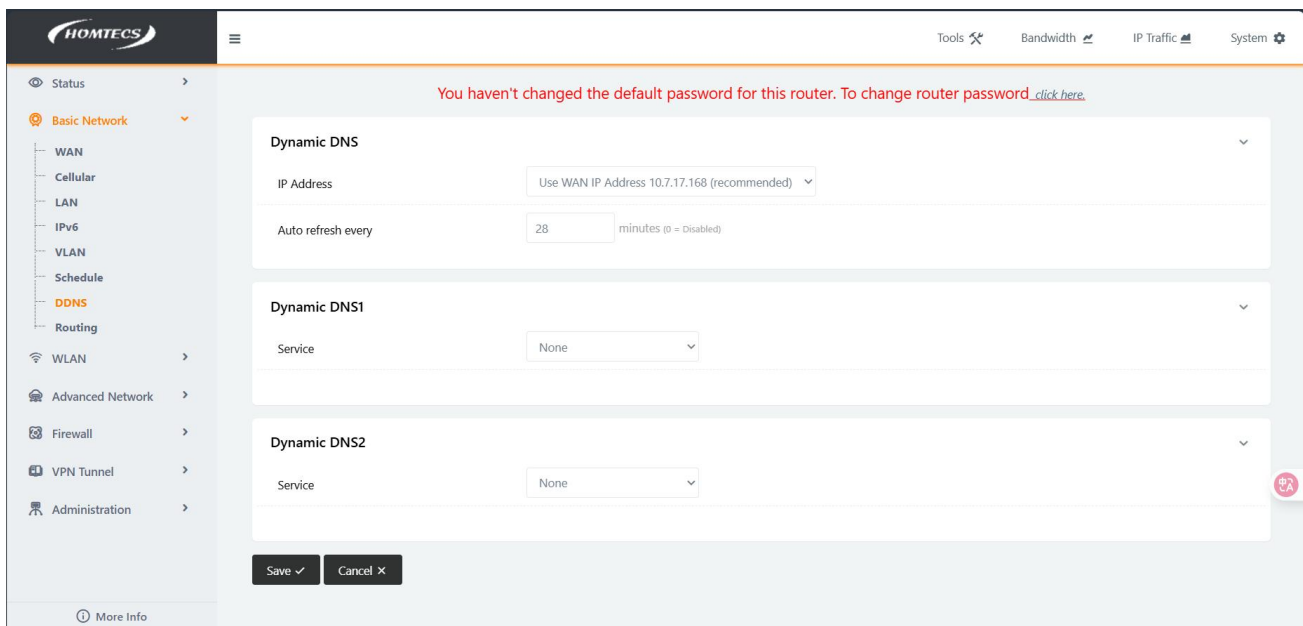


Figure 5-28 DDNS settings

Select the corresponding DDNS domain service provider from the drop-down list, such as 3322, and enter the state shown in Figure 5-29. Fill in the corresponding parameters and save.

You haven't changed the default password for this router. To change router password [click here](#).

Dynamic DNS

IP Address: Use WAN IP Address 10.7.17.168 (recommended)

Auto refresh every: 28 minutes (0 = Disabled)

Dynamic DNS1

Service: 3322

URL: <http://www.3322.org/>

Username:

Password:

Hostname:

Wildcard: ☐

MX:

Figure 5-29 DDNS settings

Description of the parameters for dynamic domain names

parameter	illustrate	How to configure
IP Address	The dynamic DNS service can change a dynamic IP address to any static Hostname, making it easily accessible from different locations on the Internet	The default value is the current interface address
Service Providers	The domain name applied for corresponds to the domain name provider option, and our company does not currently support the DDNS service of domain name providers outside the list	Drop-down options: 3322, miniDNS, etc
Service URL	The address provided by the domain name service provider	Click on the URL to enter the web page
Username/password	The username and password used to register the DDNS service provider domain name	General WORD type/CODE type, up to 64 bytes
The user's domain name	A domain name provided by a DDNS service provider, which corresponds to the IP of the router and usually accesses the IP of the router by accessing the domain name	The domain name obtained by following the steps

Table 5-7 Parameters for Dynamic Domain Names

After the configuration is complete, click the Save Settings button for the configuration to take effect



Domestic DDNS service provider: NO-IP.com (<https://www.NO-IP.com/>).

Foreign DDNS service providers: DNSEXIT (www.dnsexit.com), ZONEEDIT (www.zoneedit.com), DYNDNS (www.members.dyndns.org)

The IP address obtained from the SIM/UIM card service provider changes every time the router restarts. If you use the DDNS domain name you apply for when you remotely log in to the router, you can log in to the router page no matter how the modemIP address of the router changes.

Dynamic domain name configuration example:

- Preparations:
1. The telecom card must have a public network card IP, otherwise it must use the WAN wired public network IP mode
 2. Username: 5nre6hv@ddnskey.com Password: stone123
 3. Host name: all.ddnskey.com.net

Two links: before and after the power failure

Step 1:

To force 3G, turn on the mobile network of the basic network, select 3G (CDMA 2000/CDMA 1x) as the network mode of SIM1, and then click Save Settings to wait for restart. As shown in Figure 5-30

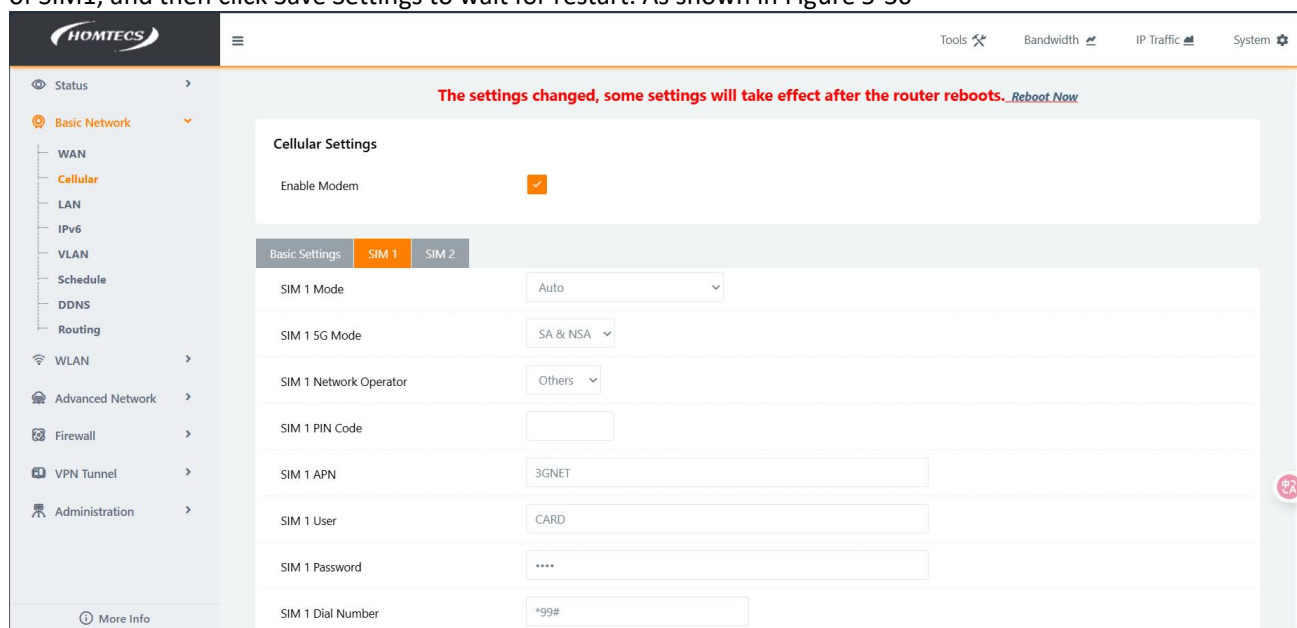


Figure 5-30 Mobile Network Configuration

Step 2:

Click the system information in the system status to view the status of the WAN network, at this time, China Telecom 3G is online, the public network address is obtained, and the Internet can be accessed, as shown in the following figure

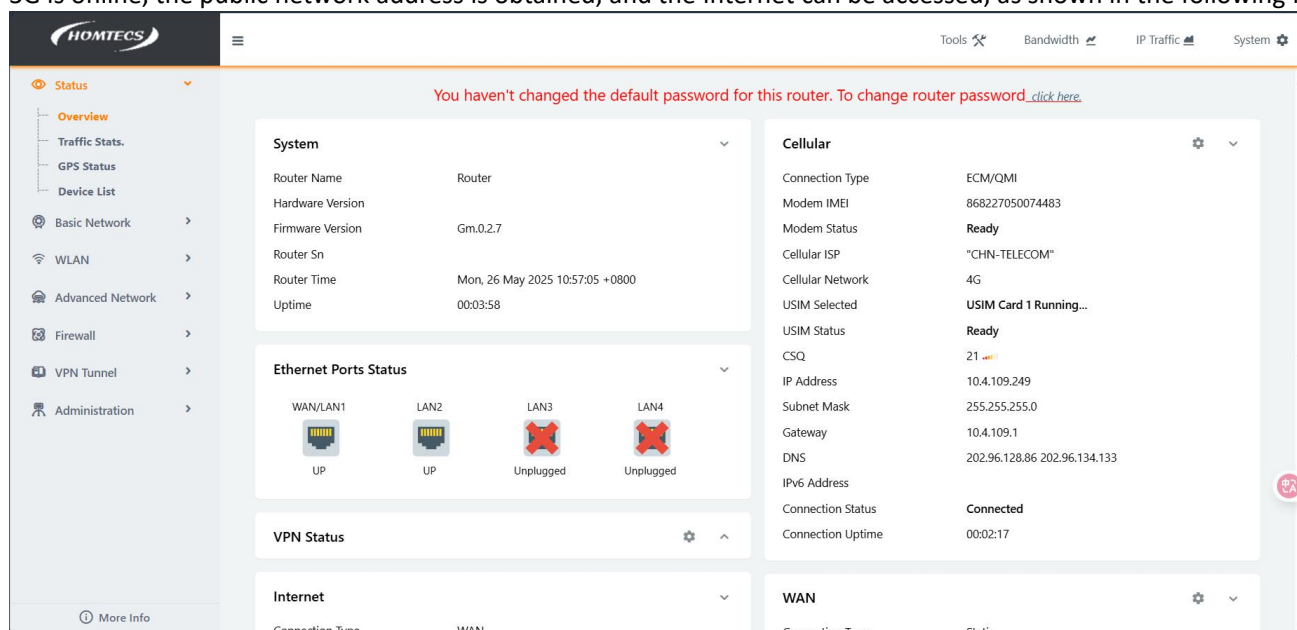


Figure 5-31 WAN network status

Step 3:

Click on the dynamic domain name in the basic network, and the automatic refresh setting will take 1 minute; Select dynamic domain name 1, select NO-IP.com as service provider, username: 5nre6hv@ddnskey.com, password: stone123, host name: all.ddnskey.com.net, and click Save Settings after the settings are complete.

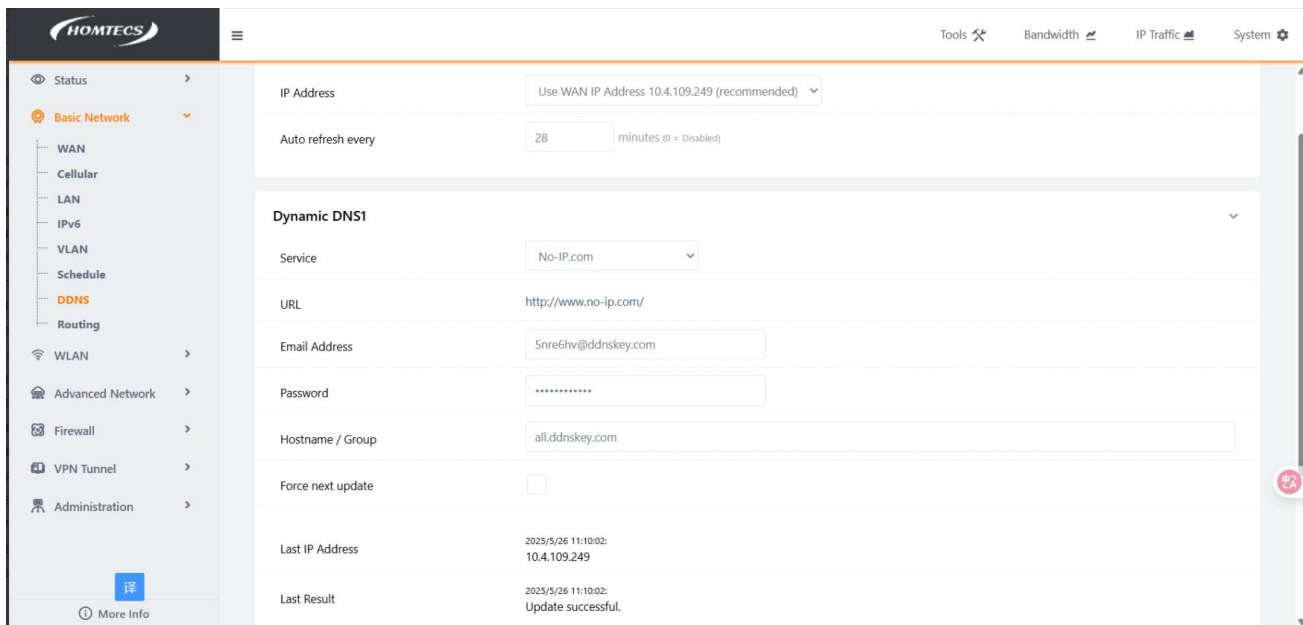


Figure 5-32 Dynamic domain name settings

Step 4:

Click the DDNS in the Basic Network to view the latest IP update status and open the administrator page to ping the host domain name, as shown in the following figure

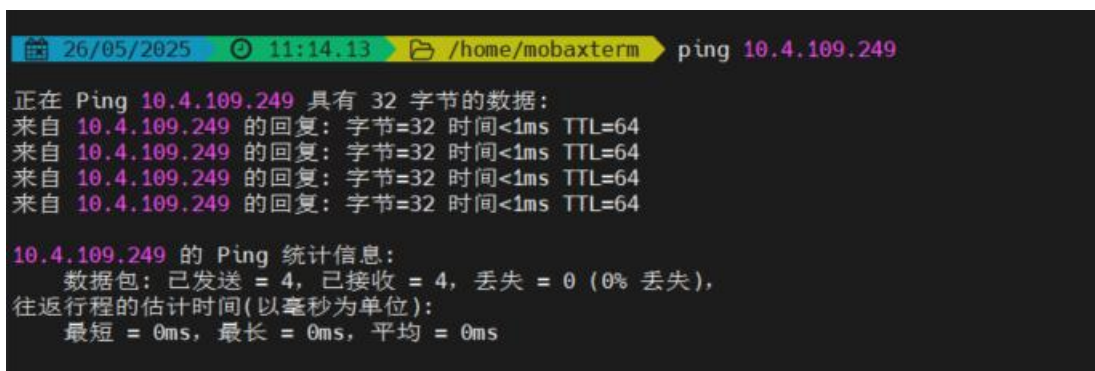
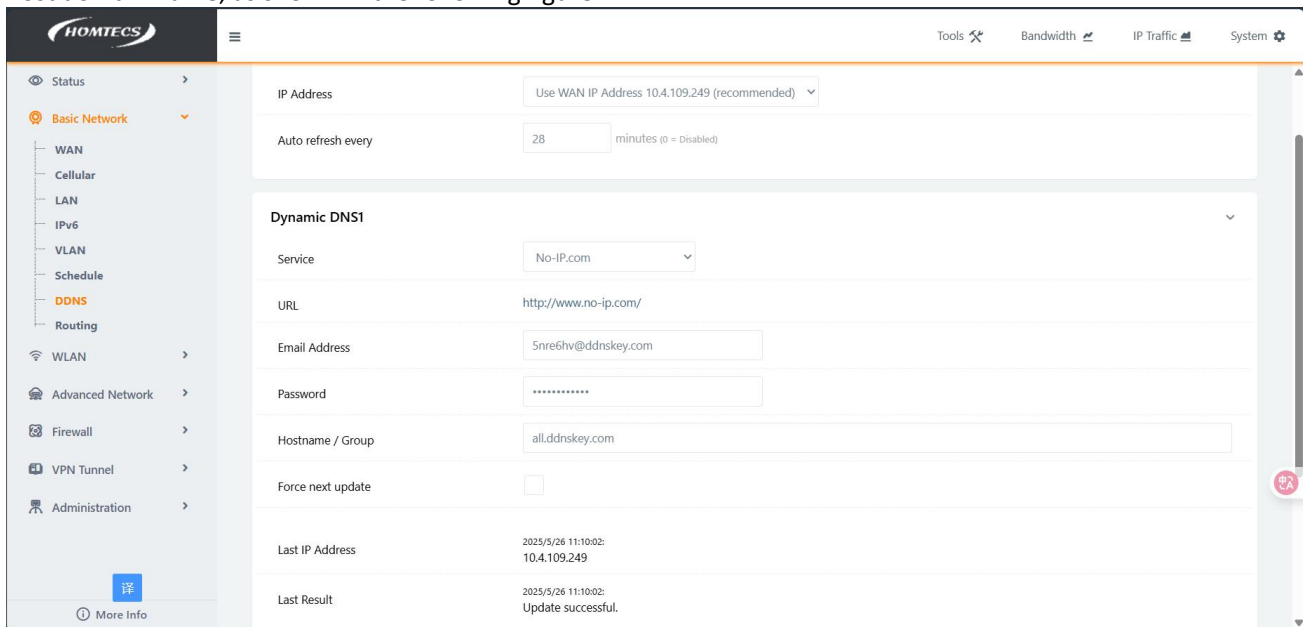


Figure 5-33 Ping the domain name

Step 5:

Result after power failure: The IP address resolved by the ping domain name will be automatically updated after each power failure

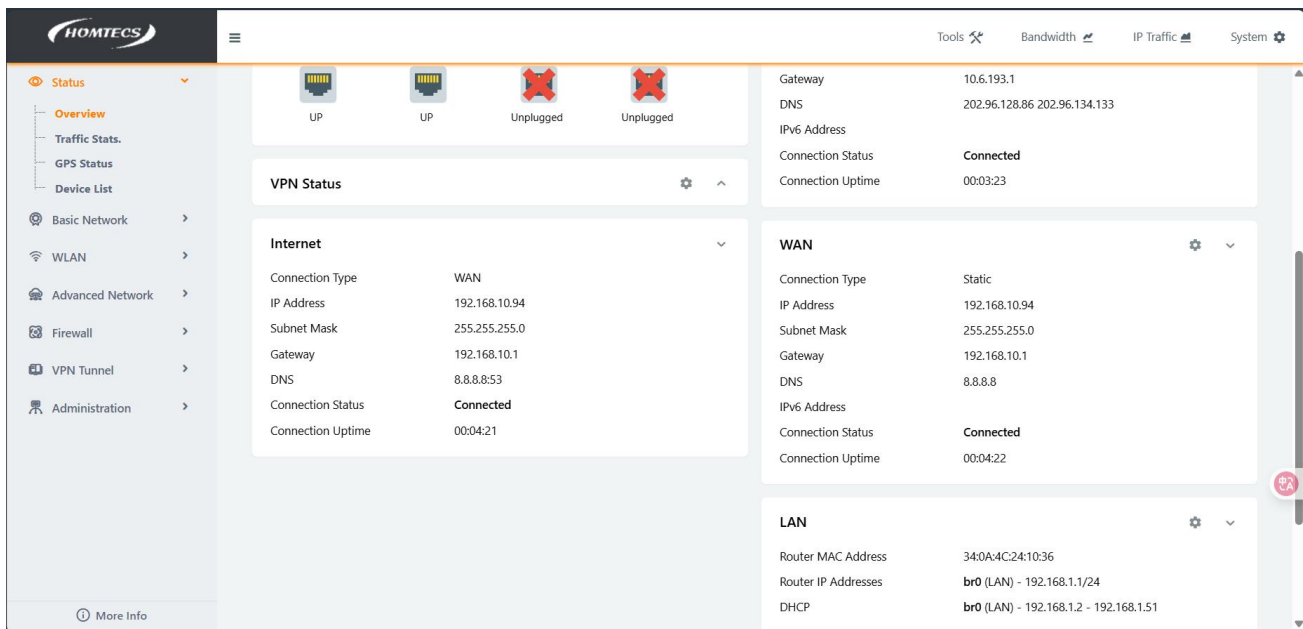


Figure 5-34 WAN Network Status

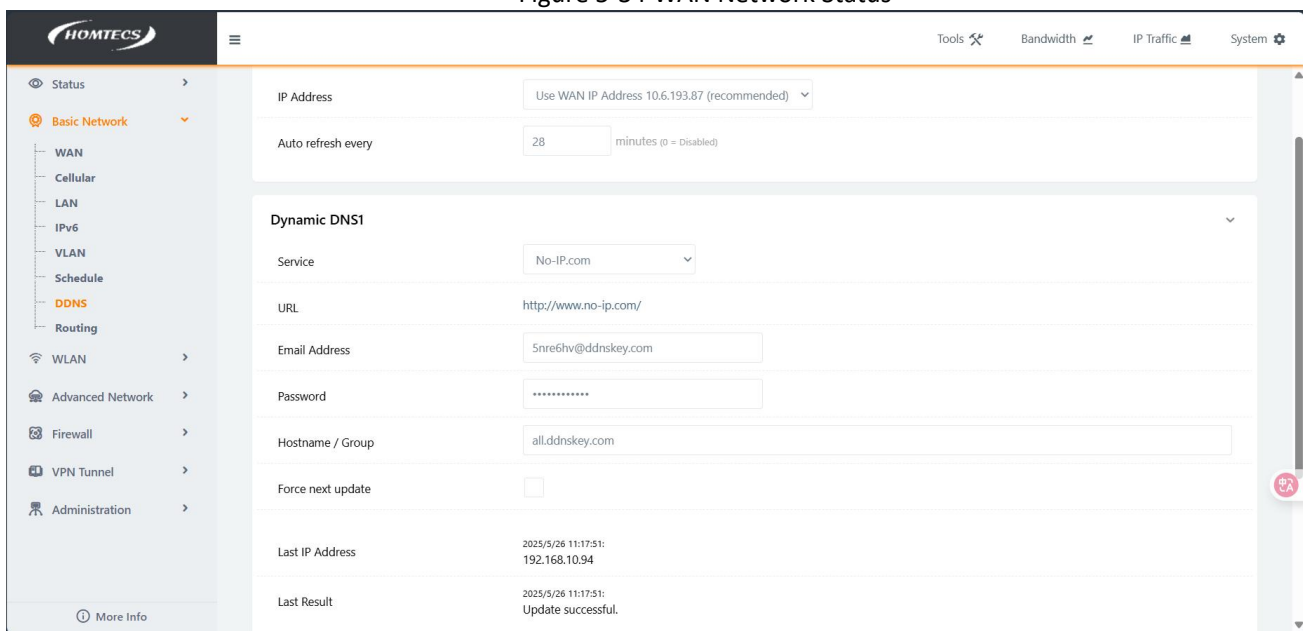


Figure 5-35 Domain name update status

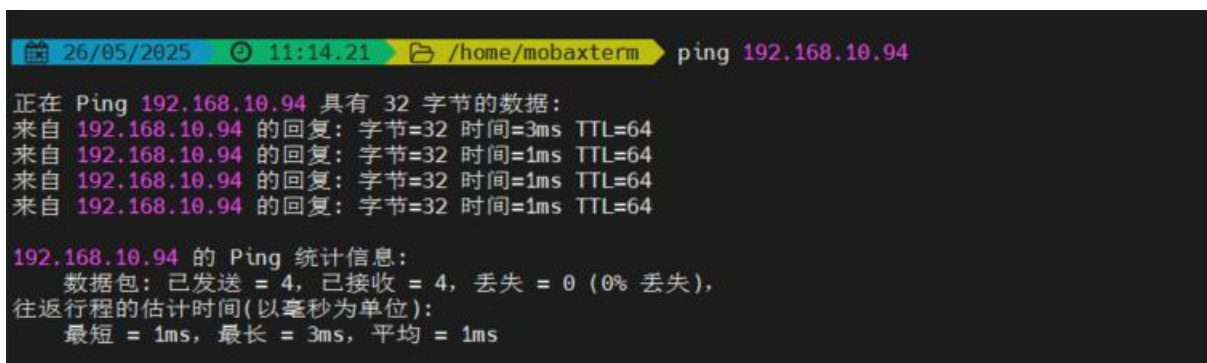


Figure 5-36 WAN Network Status

5.9. Routing

5.9.1. IPv4 Static Routing Table

The static route provides a specific forwarding path for the router to forward packets, which must be manually configured by the user. A static route is a route that uses the destination address as the basis for selection.

Step 1: select Routing in the Basic Network page, you can modify the IPv4 Static Routing Table parameters:

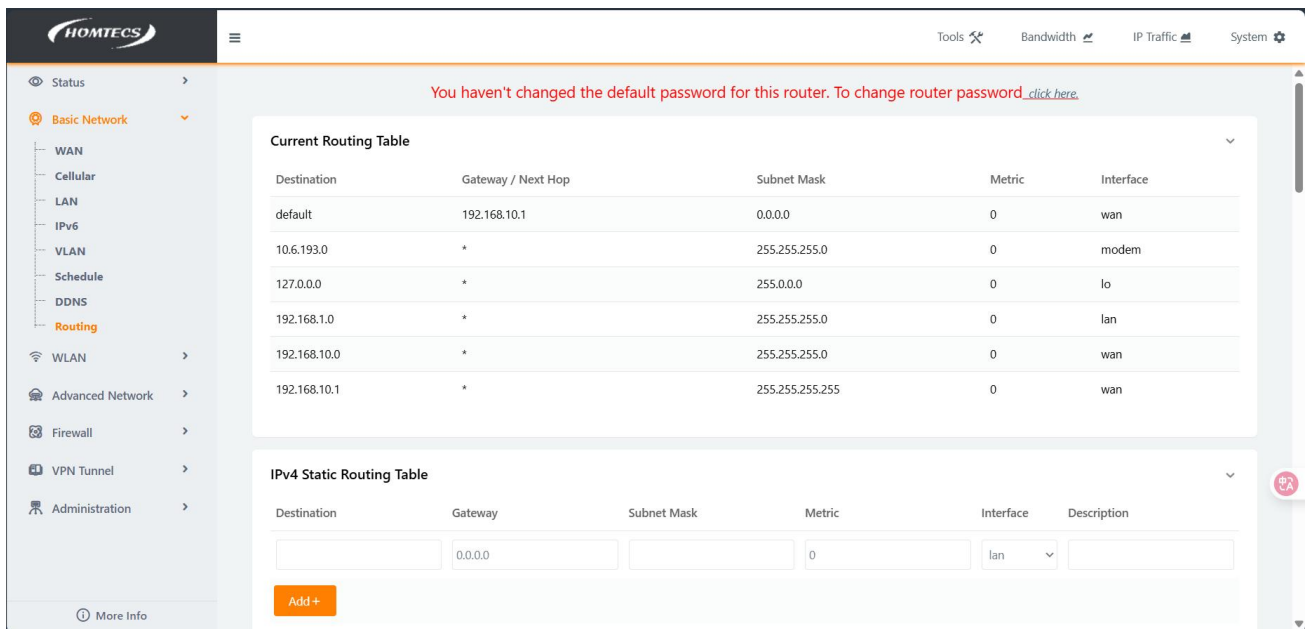


Figure 5-37 Routing settings

Step 2: Static routing parameter description

Parameter	Meaning	How to configure
Destination address	Set the destination address and the number of subnet mask digits for a static route	Enter the destination address and the number of bits of the subnet mask. Format: A.B.C.D/M
Gateway	Specify the next-hop IP address of a static route, that is, the port address of the neighboring router	Set it up as appropriate

Table 5-8 Static Routing settings

Step 3: Click Save to complete the static route settings.

Example configuration of a static route table:

Step 1:

Click Routing in Basic Network, configure the static route table settings, set the destination address to 192.168.10.0, set the subnet mask to 255.255.255.0, select LAN for the network interface, click Add, and click Save after the configuration is complete.

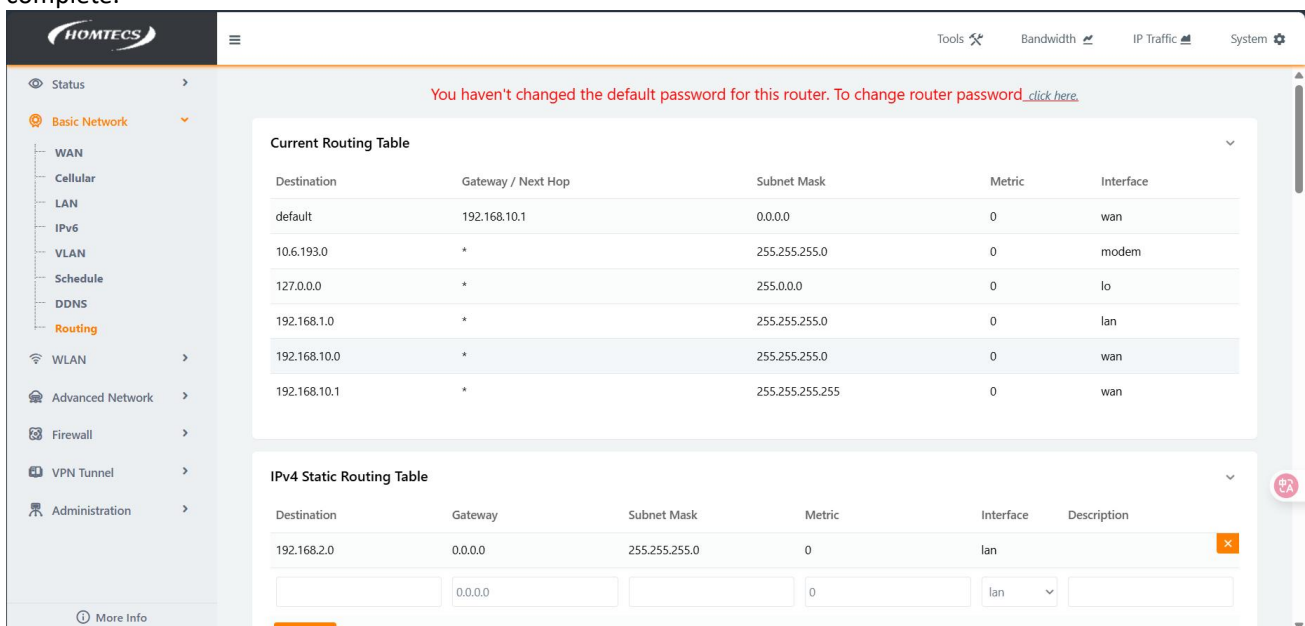


Figure 5-38 Static Route Configuration

Step 2:

After the save is complete, you can view the static route table in the current route table, and the static route table has taken effect.

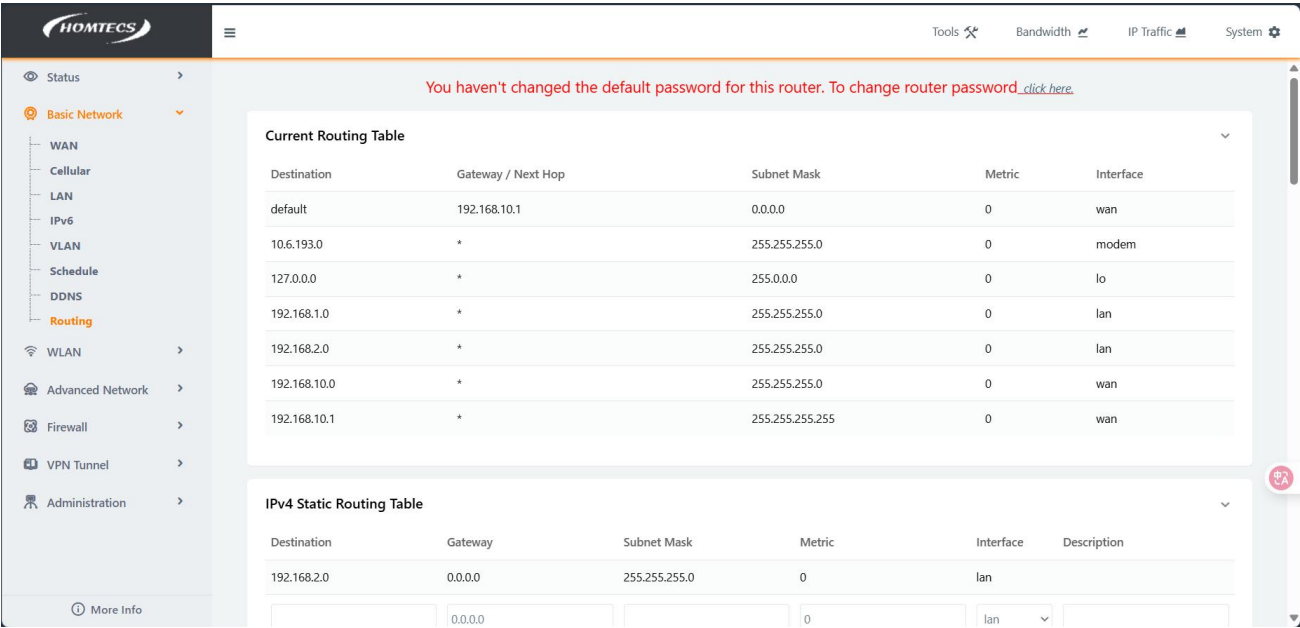


Figure 5-39 Static Routing Table

5.9.2. IPV6 Static Routing Table

Static route provides a specific forwarding path for the router to forward packets, which must be manually configured by the user. A static route is a route that uses the destination address as the basis for selection.

Step 1: select Routing in the Basic Network page, you can modify the IPv6 Static Routing Table parameters:

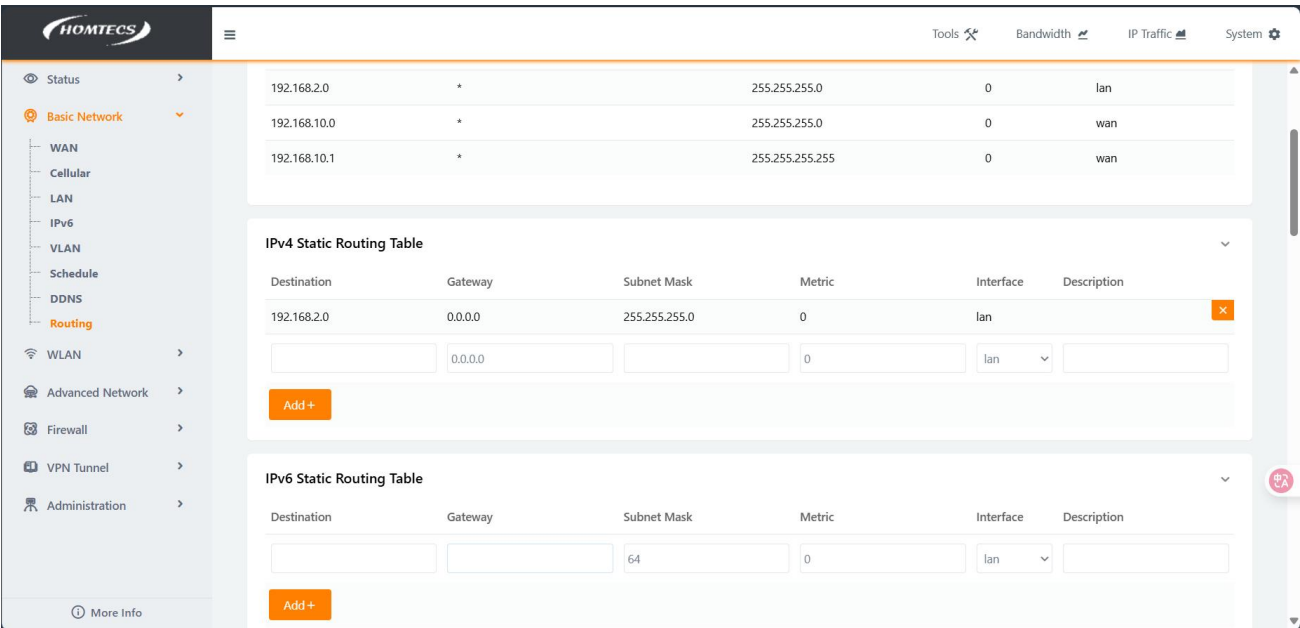


Figure 5-40

Step 2: Description of IPv6 Static Routing Parameters

Parameter	Meaning	How to configure
Destination address	Set the destination address and the number of subnet mask digits for a static route	Enter the destination address and the number of bits of the subnet mask. Format: AAAA:BBBB:CCCC:DDDD:EEEE:FFFF:GGGG:HHHH/64
gateway	Specify the next-hop IP address of a static route, that is, the port address of the neighboring router	Set it up as appropriate. The format is as follows:

Table 5-9 IPv6 Static Route Table

Step 3: Click Save to complete the static route settings.

IPv6 Static Route Table Configuration Example:

Step 1: Click Route in the Basic Network, configure the static route table settings, fill in the destination address, fill in the subnet mask, select LAN for the network interface, click Add, and click Save Settings after the configuration is complete.

Destination	Gateway	Subnet Mask	Metric	Interface	Description
fe80::a235:a66e:a12f:e1ab%15	fe80::6e3b:6bff:fe38:8293%15	64	1	lan	1

Figure 5-41

Step 2: After the IPV6 address is added, you need to restart the router for the configuration to take effect.

```

root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ip -6 route show
fe80::/64 dev eth2 proto kernel metric 256
fe80::/64 dev vlan1 proto kernel metric 256
fe80::/64 dev br0 proto kernel metric 256
fe80::/64 dev ra0 proto kernel metric 256
fe80::/64 dev rai0 proto kernel metric 256
fe80::/64 dev vlan2 proto kernel metric 256
fe80::/64 dev usb0 proto kernel metric 256
root@Router:/tmp/home/root#

```

Figure 5-42

5.9.3. Policy Routing Table

Policy Routing is a packet routing and forwarding mechanism that is more flexible than routing based on the destination network. The router will decide what to do with the packets that need to be routed through the route map, which determines the next- hop forwarding router for a packet.

Step 1: select Routing in the Basic Network page, you can modify the Policy Routing Table parameters, as shown in figure 5-43:

Figure 5-43 Policy Routing Table page

Step 2: Policy Routing Table parameter description

Parameter	Meaning
-----------	---------

Lan	Select the virtual network ports of PBR: VLAN1-VLAN16, AP, and AP2
modem	Module policy selection, such as Auto/Only/Primary/Secondary
wan	Select the policy of the WAN port, such as Auto/Only/Primary/Secondary
Sta	Sta (2.4GWiFi client) strategy selection, e.g. Auto/Only/Primary/Secondary
sta2	Sta2 (5.8GWiFi client) strategy selection, such as Auto/Only/Primary/Secondary

Table 5-10 Policy Routing Parameter Table

Note: Priority description of policy-based routing:

- ① Auto mode: the default value
- ② Priority size: Only>Primary>Secondary
- ③ When only mode is selected for one interface, only mode can be selected for other interfaces
- ④ When an interface selects the primary mode, other interfaces can only select the interface with a lower priority, and cannot select the primary mode at the same time
- ⑤ When an interface selects the secondary mode, one of the other interfaces can select the primary mode, while the others can only select the Auto mode

Step 3: Click Save Settings to save the PBR configuration

Example Policy Routing Table configuration:

Step 1: Click the route table settings of the Basic Network, configure the information of the policy route table, select vlan1 for lan, select only mode for modem, click Add, and save the setting:

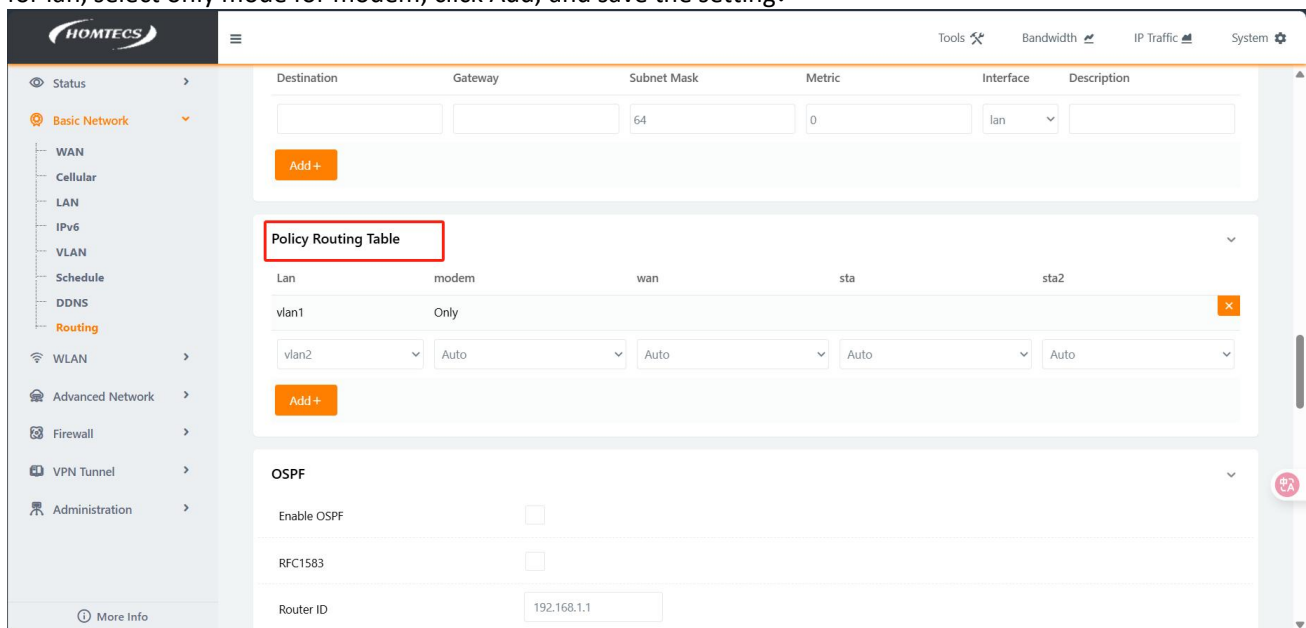


Figure 5-44 Policy Routing Table settings

Step 2: Enable modem and WAN online at the same time, and when the modem is switched to online modem, the routing device can access the public network normally. When switching to WAN online, the WAN cannot access the WAN because the PBR configuration only modem is used to access the Internet. Similarly, if STA and STA2 are also configured, you will not be able to access the Internet normally when switching to these two modes.

5.9.4. OSPF

OSPF (Open Shortest Path First): is an interior gateway protocol (IGP) used between routers in a single autonomous system (AS). OSPF uses link-state technology, where routers send each other directly connected link information and link information it has to other routers. Each OSPF router maintains a database with the same AS topology, from which the shortest path is constructed to calculate the routing table, and when the topology changes, the OSPF protocol can quickly recalculate the path and only generate a small amount of routing protocol traffic. In addition, all OSPF routing packet

switching is validated.

Step 1: Open Basic Network and select Routing, as shown in figure 5-45

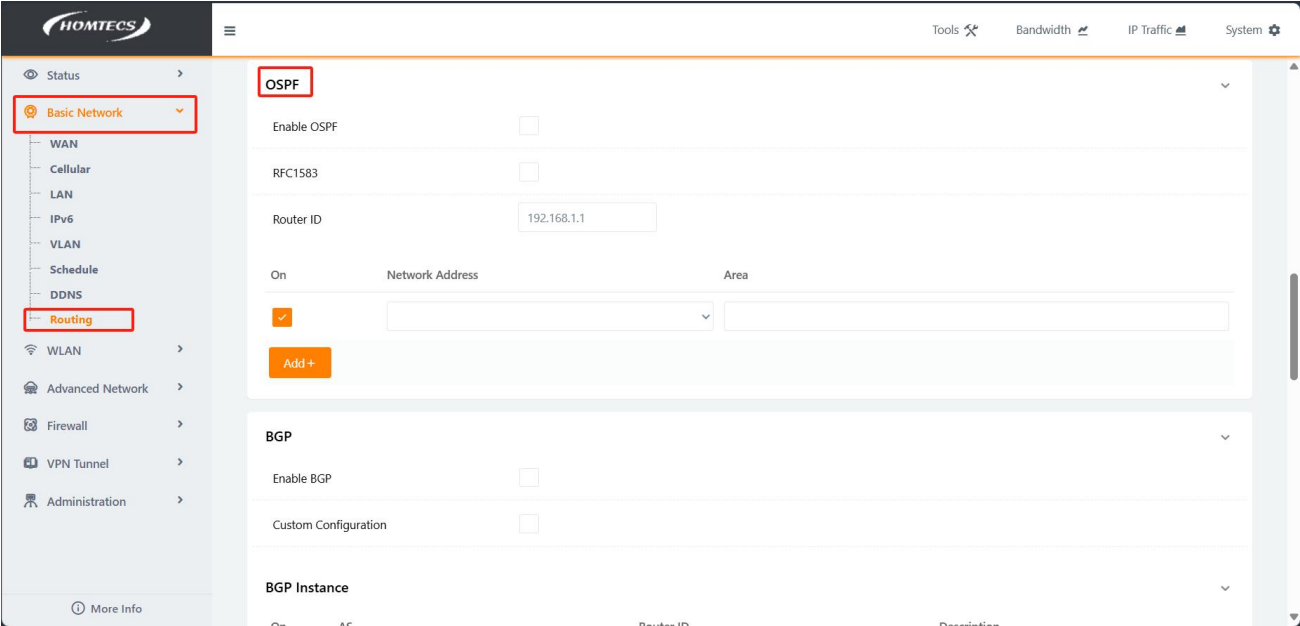


Figure 5-45 OSPF page

Step 2: OSPF parameter description

Parameter	Description	Parameter configuration
RFC1583	The preferred method of external routing	Enable or disable this feature
Router ID	The unique ID or ID of a route in a link	IP address or ID value
Network Address	Choice of network port, such as LAN/WAN	
Area	Assign a zone to the LAN/WAN	The zone values for LAN and WAN are configured to be different values

Table 5-11 OSPF parameters

OSPF configuration example:

Step 1: Enable OSPF, set the router ID to 192.168.1.1, the network address LAN, region 1, the network address WAN, region 0, and the wan port IP to 192.168.3.11, and save the settings

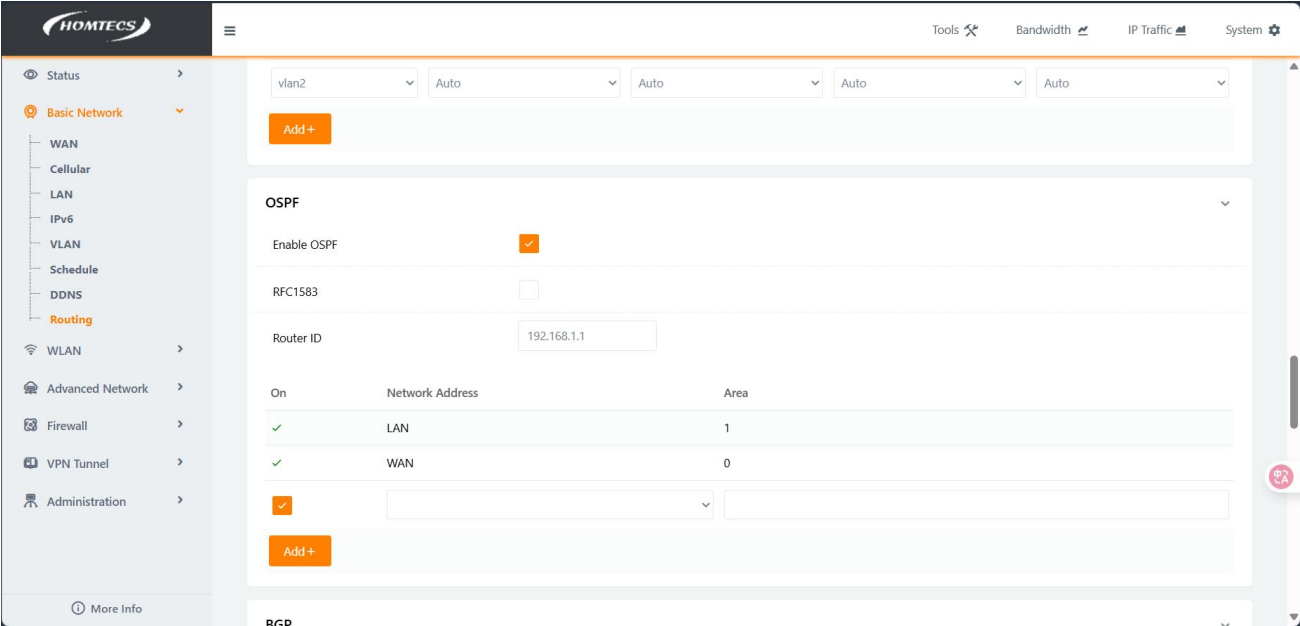


Figure 5-46 Screenshot of OSPF parameter configuration

Miscellaneous

Mode

Gateway

RIPv1 & v2

Disabled

DHCP Routes

☒

Spanning-Tree Protocol

☐

Figure 5-47 Other parameter configurations

Step 2: Configure the OSPF parameters of the other router, the router ID is 192.168.2.1, the network address is LAN, the region is 2, the network address is WAN, the region is 0, the WAN port IP is 192.168.3.12, and the two routers are interconnected through the WAN port

Basic Network

WAN

Cellular

LAN

IPv6

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

OSPF

Enable OSPF

☒

RFC1583

☐

Router ID

192.168.2.1

On

Network Address

Area

✓

LAN

2

✓

WAN

0

Add +

Figure 5-48 OSPF parameter configuration

Miscellaneous

Mode

Gateway

RIPv1 & v2

Disabled

DHCP Routes

☒

Spanning-Tree Protocol

☐

Figure 5-49 Other parameter configurations

Step 3: Route topology diagram

```

graph TD
    PC1[PC1  
192.168.1.2] -- area 1 --> R1[Router 1  
192.168.1.1]
    R1 -- "192.168.3.11" --> A0[area 0]
    A0 -- "192.168.3.12" --> R2[Router 2  
192.168.2.1]
    R2 -- area 2 --> PC2[PC2  
192.168.2.2]
  
```

Figure 5-50 Routing topology diagram

Step 4: View the routing tables of the two devices and ping the IP addresses of the peer subnets

Route1: (LAN ip address 192.168.1.1)

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.3.1	*	255.255.255.255	0	WAN
192.168.3.0	*	255.255.255.0	0	WAN
192.168.2.0	192.168.3.12	255.255.255.0	20	WAN
192.168.1.0	*	255.255.255.0	0	LAN
127.0.0.0	*	255.0.0.0	0	lo
default	192.168.3.1	0.0.0.0	0	WAN

Figure 5-51 shows the routing table

```
C:\Users\Administrator>ping 192.168.2.2 -t

正在 Ping 192.168.2.2 具有 32 字节的数据:
192.168.2.2 的回复: 字节=32 时间=6ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间<1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间<1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
192.168.2.2 的回复: 字节=32 时间=1ms TTL=62
```

Figure 5-52 IP detection

Route2: (LAN ip address 192.168.2.1)

Current Routing Table ▼				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
192.168.3.1	*	255.255.255.255	0	WAN
192.168.3.0	*	255.255.255.0	0	WAN
192.168.2.0	*	255.255.255.0	0	LAN
192.168.1.0	192.168.3.11	255.255.255.0	20	WAN
127.0.0.0	*	255.0.0.0	0	lo
default	192.168.3.1	0.0.0.0	0	WAN

Figure 5-53 shows the routing table

[illegible]

Figure 5-54 IP detection

5.9.5. BGP

Border Gateway Protocol (BGP) is an enhanced path vector routing protocol, and BGP is an external gateway protocol with rich policy control technologies, which mostly runs between ASs. Dynamic routing protocols can be divided into IGP and Interior Gateway Protocol (EGP) according to the scope of work. IGP works within the same AS and is mainly used to

discover and compute routes, and to exchange routing information within the AS. EGP works between AS and provides loop-free routing information exchange between ASs, while BGP is a type of EGP. One of the main tasks of BGP is to publish the network reachability information of the AS to other ASPs. The focus of BGP is not on the automatic discovery of network topology, but on selecting the best routes between ASs and controlling the propagation of routes. BGP uses TCP as its transport layer protocol (listening port number 179), which improves the reliability of the protocol and does not require a special mechanism to ensure the controllability of the connection. An AS is an IP network with the same routing policy under the jurisdiction of an entity, and each AS has a unique Autonomous System Number, which is assigned by IANA.

Step 1: Open the Basic Network, select Routing, and drop down the parameters to BGP Parameter Configuration

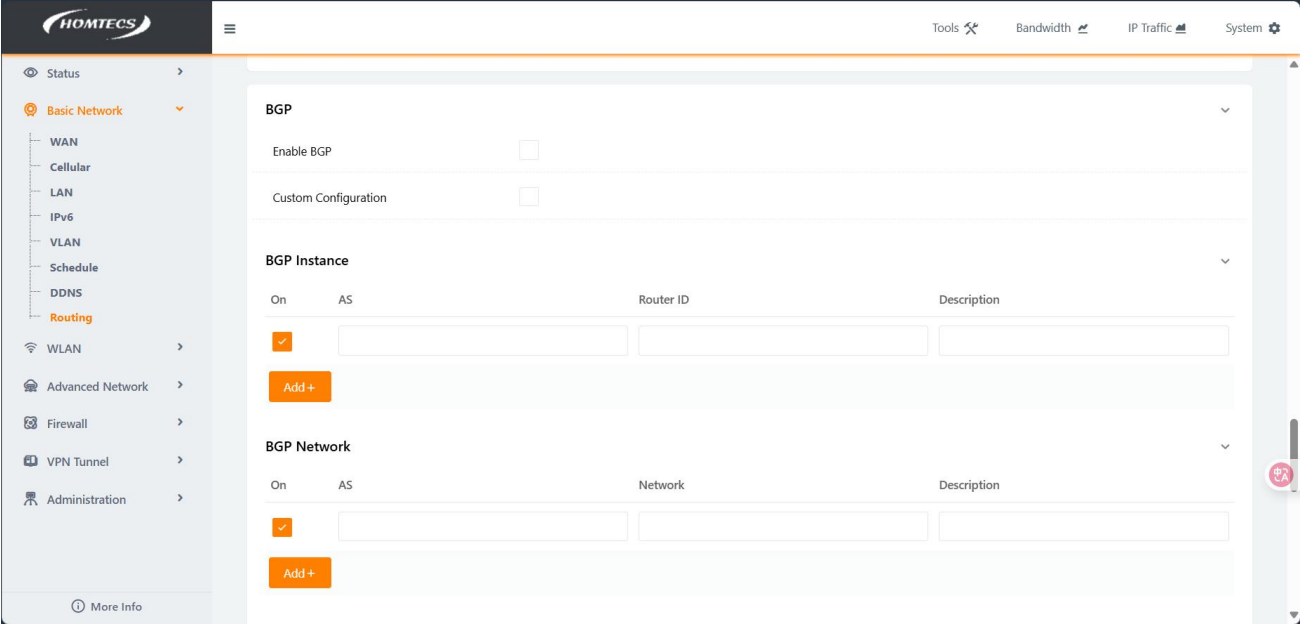


Figure 5-55

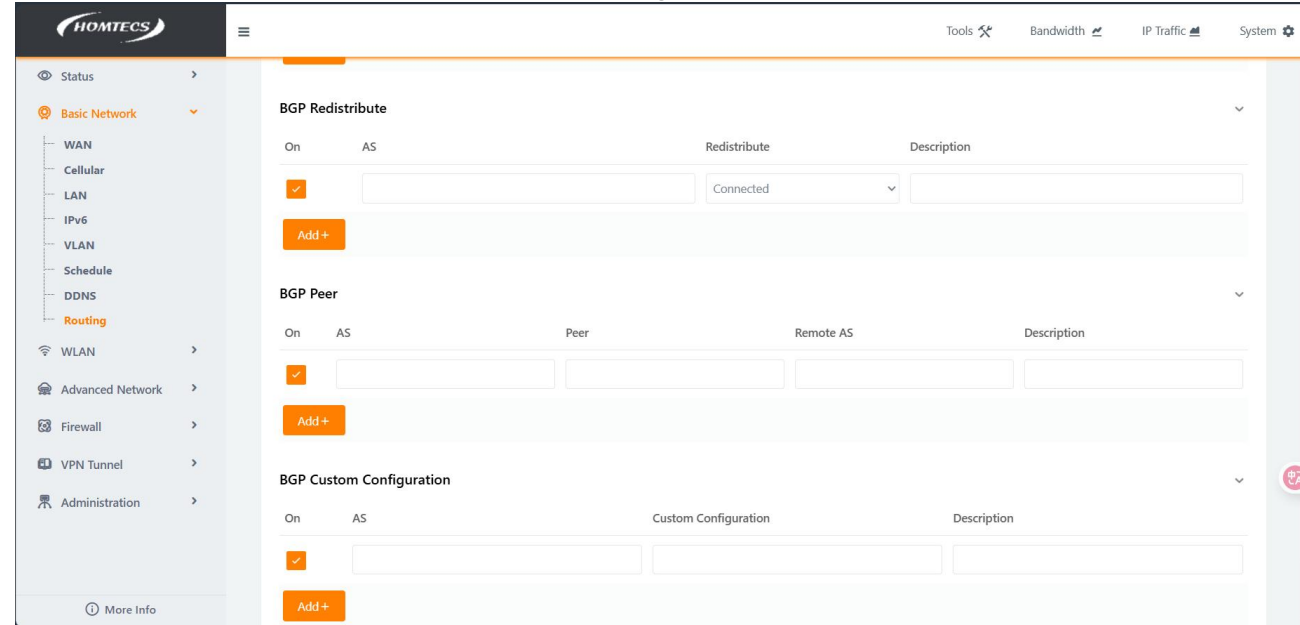


Figure 5-56

Step 2: BGP parameters

Parameter	Meaning	How to configure
Enable BGP	BGP enabled/disabled	Not enabled by default; Check to enable;
Customization options	User-configurable	Disabled by default; After enabled, the configuration information can be customized;
AS	Autonomous system number, unique	Range: 1-65535
The router ID of the BGP instance	The router ID of a BGP device, which is unique, is usually in the form of an IPv4 address, which is the IP of the BGP gateway	Format: A. B.C.D

Parameter	Meaning	How to configure
BGP network	The network address inside the B GP, which is distinguished from the router ID, is the network that will be broadcast by BGP	Format: A. B.C.D
BGP Redistribute	BGP redistribution	The default value is Connected; Optional Connected/Kernel/OSPF/RIP/Static
BGP Peer	Peer/peer BGP router ID	Format: A. B.C.D
Remote AS	The autonomous system number of the peer router, which is unique	Range: 1-65535
BGP customization options	Custom options for the corresponding autonomous system number	Self-configurable

Table 5-12

The configuration is as follows:

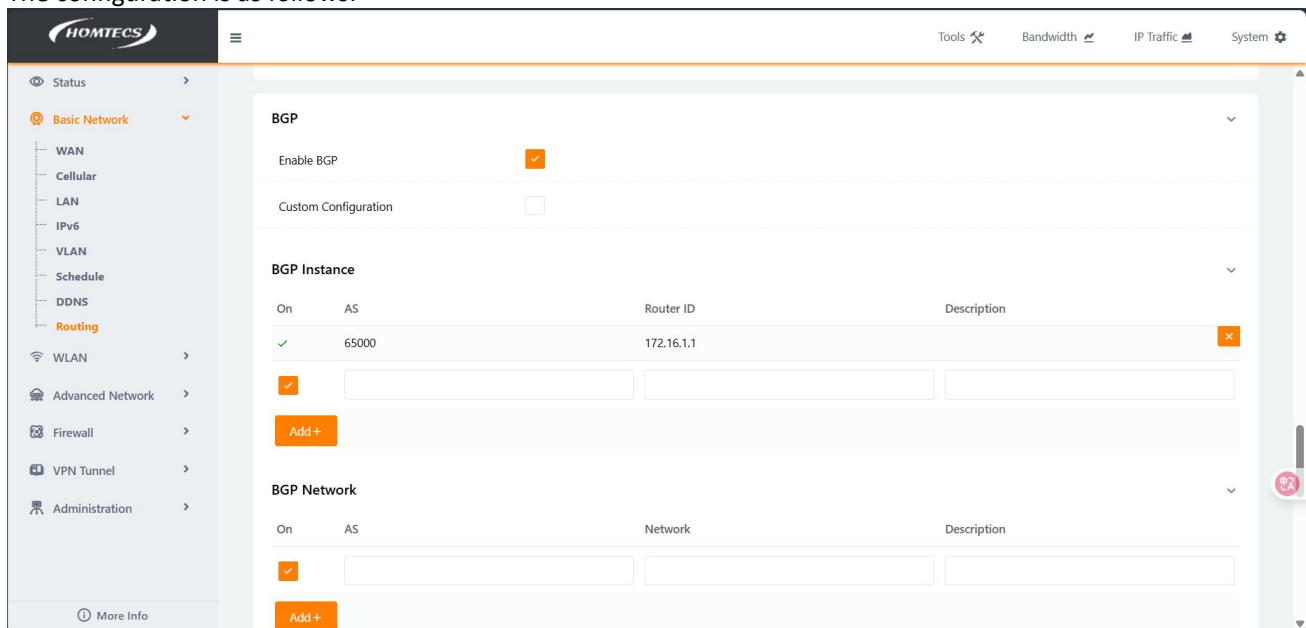


Figure 5-57

BGP Network

On	AS	Network	Description
<input checked="" type="checkbox"/>	65000	192.168.3.0/24	
<button>Add +</button>			

BGP Redistribute

On	AS	Redistribute	Description
<input checked="" type="checkbox"/>		Connected	
<button>Add +</button>			

Figure 5-58

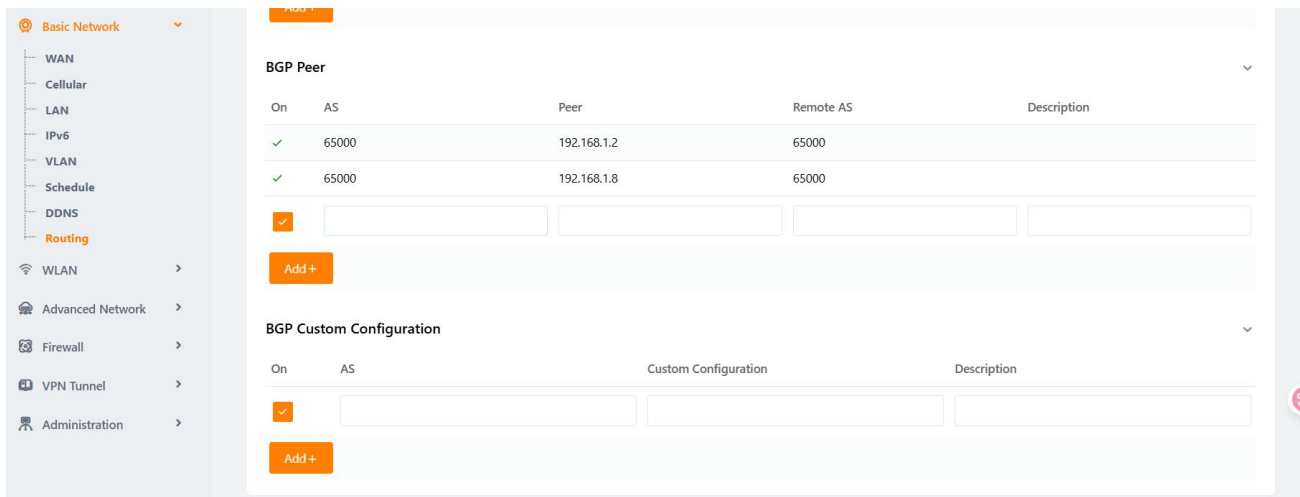


Figure 5-59

telnet enters the background and can ping the network address inside the peer BGP

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.1   0.0.0.0         UG        0      0      0   vlan2
10.36.84.32      0.0.0.0        255.255.255.252 U         0      0      0   usb0
127.0.0.0        0.0.0.0        255.0.0.0       U         0      0      0   lo
172.16.1.2       0.0.0.0        255.255.255.255 UH        20     0      0   dmvpn
172.16.1.3       172.16.1.2     255.255.255.255 UGH       20     0      0   dmvpn
172.16.1.8       0.0.0.0        255.255.255.255 UH        20     0      0   dmvpn
192.168.1.0      172.16.1.8     255.255.255.0   UG        20     0      0   dmvpn
192.168.2.0      172.16.1.2     255.255.255.0   UG        20     0      0   dmvpn
192.168.3.0      0.0.0.0        255.255.255.0   U         0      0      0   br0
192.168.10.0     0.0.0.0        255.255.255.0   U         0      0      0   vlan2
192.168.10.1     0.0.0.0        255.255.255.255 UH        0      0      0   vlan2

root@Router:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.365 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.082 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=1.285 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=1.133 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=1.229 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.082/1.218/1.365 ms

root@Router:/#
```

Figure 5-60

6. WLAN

6.1. Basic Settings

Select “WLAN>Basic Settings” in the navigation bar, you can modify and configure the basic parameters of Wi-Fi.



WARNING

The default WiFi password is set by the factory, and users can set or not set the WiFi password according to their own needs. The way to set the WiFi password is the last item in the “Basic Settings>Security Options”. Select the required encryption method from the drop-down list, and fill in the custom WiFi password, and save it.

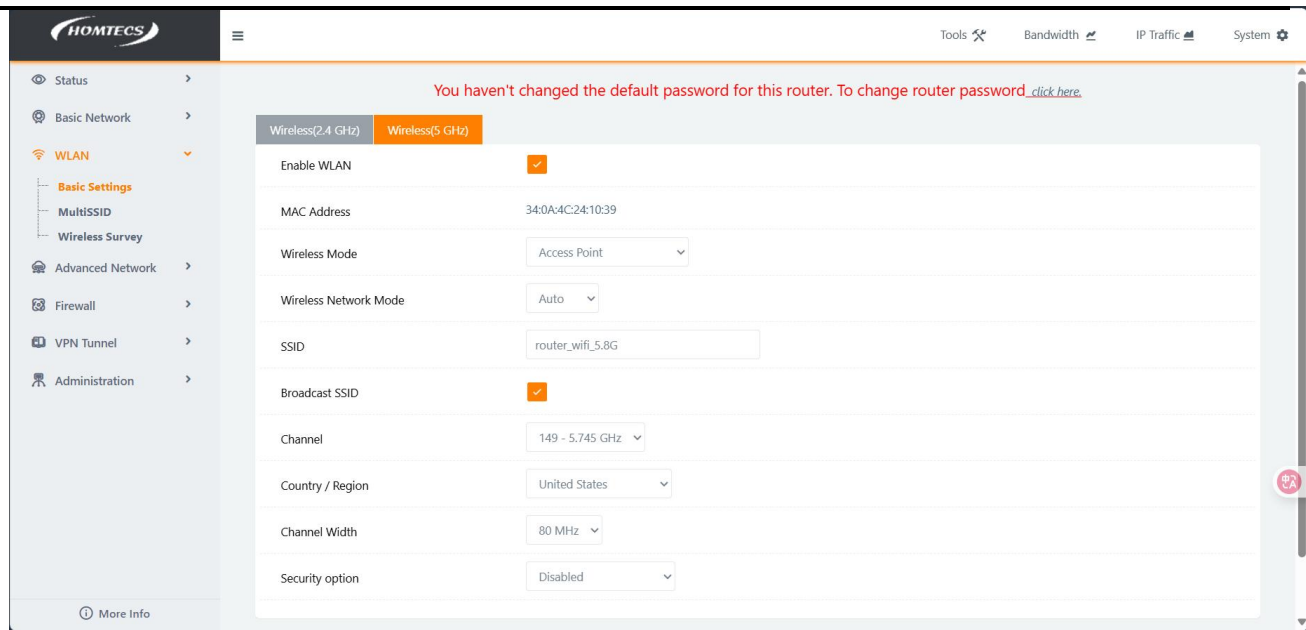


Figure 6-1 Screenshot of basic Wi-Fi parameters

Basic Settings parameters

Parameter	Meaning	How to configure
Enable WLAN	Turn on the wireless mode and the relevant Wi-Fi parameters can be set	button selection Enable Disable
Wireless Mode	Select the networking mode of the wireless network	The default AP working mode can also support clients
Wireless Network Mode	The router supports multiple protocols such as 11b/g/n.	Default Auto Only; or manually modify only 802.11g; B/G mix
SSID	The ID of the wireless network service set, which is the Router by default	Maximum 32 Bytes
Channel	Channels used by Wi-Fi	It is recommended to use the default value
Bandwidth	The bandwidth used by the wireless network	Support 20MHz, 40MHz, 80MHz
Security options	Configure the WLAN encryption mode so that it can be disable when encryption authentication is not required. WEP encryption is relatively easy to crack, so it is recommended to use WPA encryption	Drop-down box options: WEP 、 WPA 、 WPA-PSK 、 WPA2- PSK 、 WPA2 、 WPAPSK/WPA2PSK

Table 6-1 Basic Parameter Settings Configuration

6.1.1. Wireless Client Mode

Example of Wireless Client Mode settings:

Step 1: Open the WLAN settings, select the basic parameter settings, select the wireless client for wireless mode, the SSID name is consistent with the WiFi SSID name of the connected router, the security method and password must also be the same, then save the configuration and restart the router. The configuration is shown in the image:

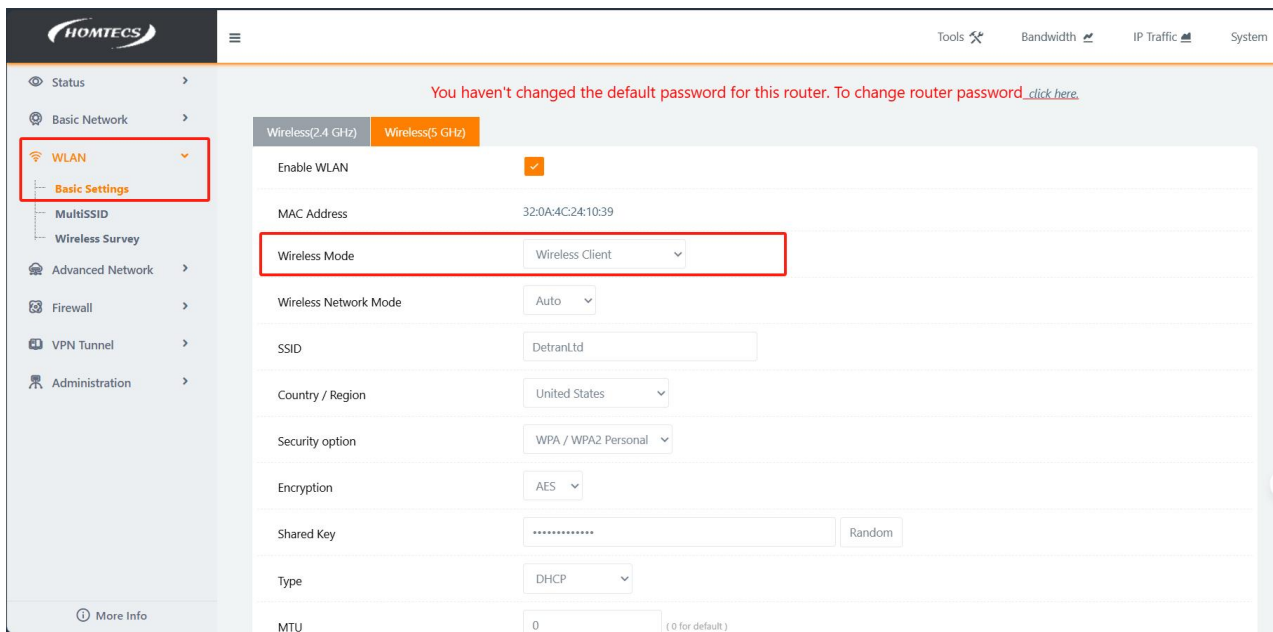


Figure 6-2 Wi-Fi Wireless Client Parameter Configuration

Step 2: Connect the WiFi antenna normally, and then check the connection status of the WiFi client on the status page, as shown in the figure:

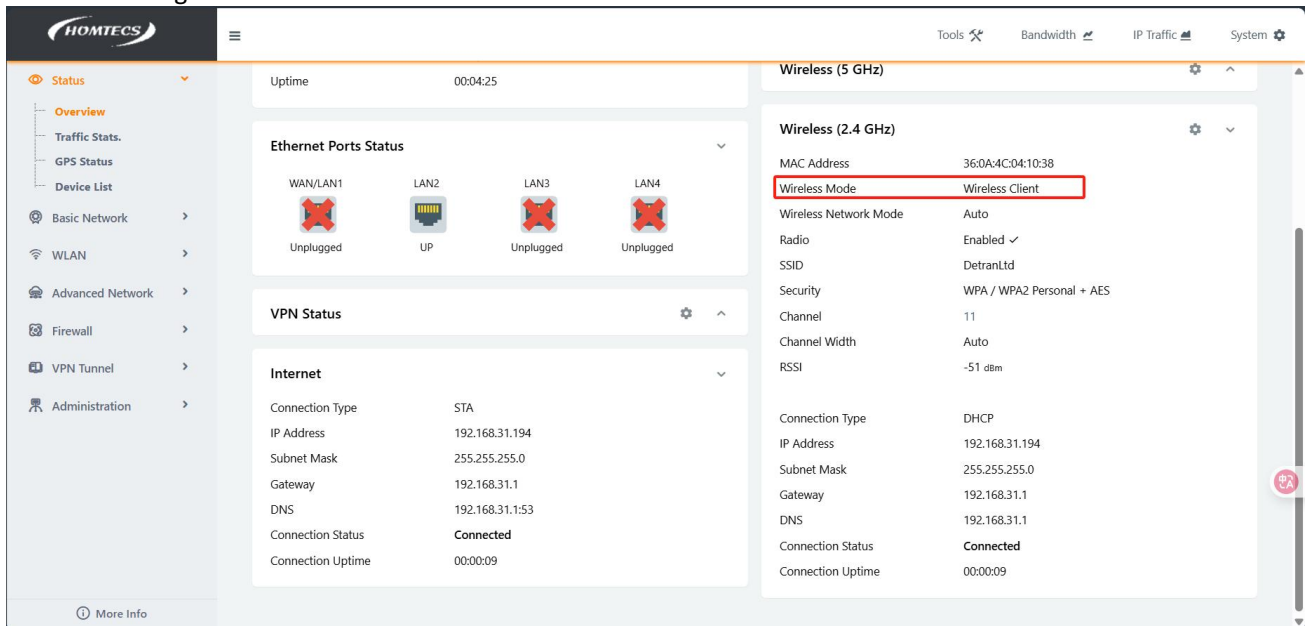


Figure 6-3 Wi-Fi Wireless Client Connection

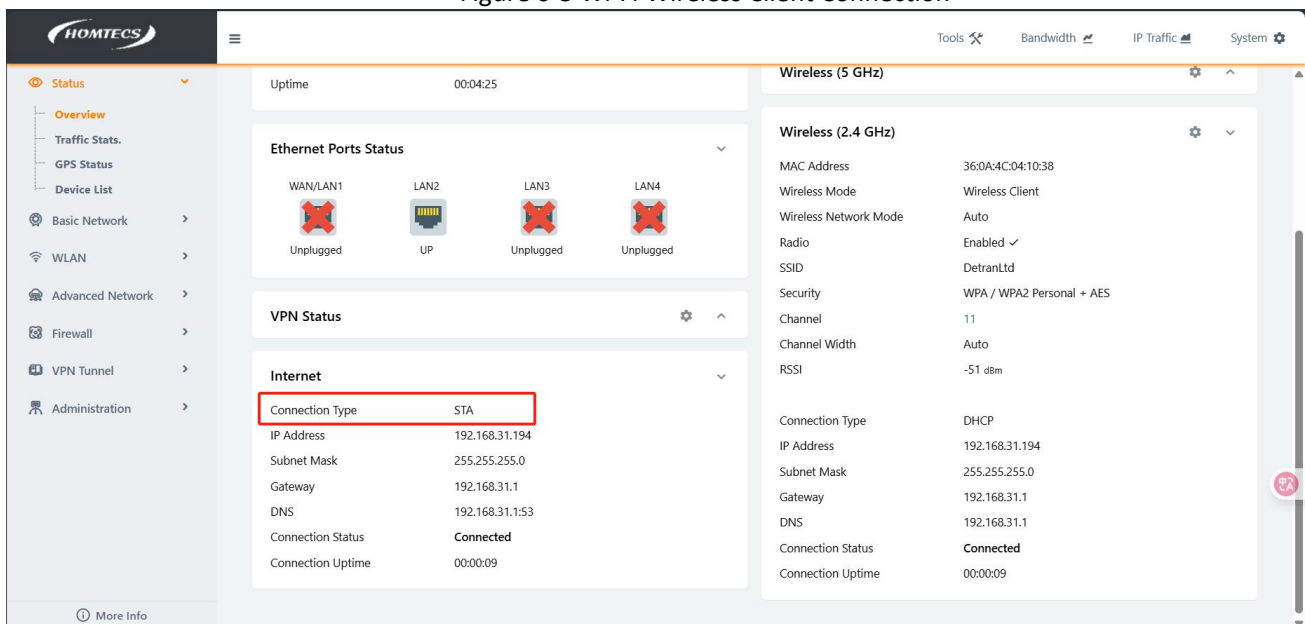


Figure 6-4 Wi-Fi Wireless Client Connection

Step 3: Check whether the device can access the Internet normally when the WiFi connected to the wireless client device can access the Internet normally

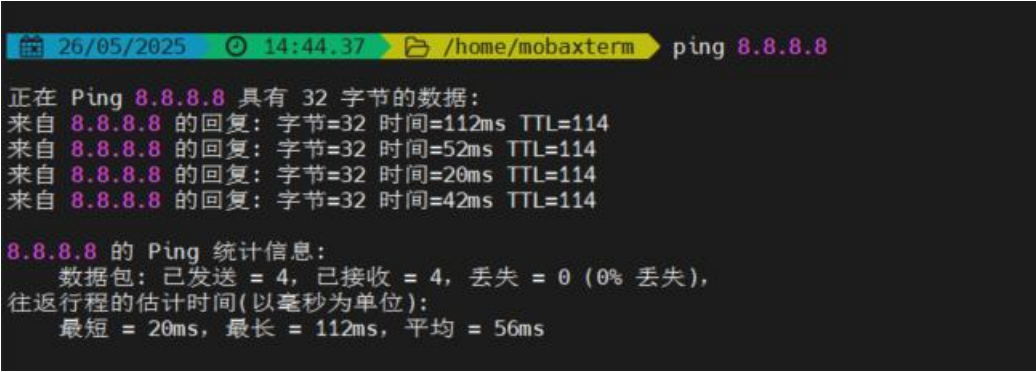


Figure 6-5 Internet access test

6.1.2. Wireless bridge mode

Wireless Bridging (WDS) Technology in the simplest network architecture, the Ethernet port of the bridge is connected to a hub or switch in the local area network, and the signal transmitting port is connected by a cable and antenna; In this way, the network system can be expanded.

Example wireless bridge mode configuration:

Step 1: Change the IP address of the LAN to 192.168.31.100 (which belongs to the same network segment as the bridged device), save the parameter configuration, and restart the router.

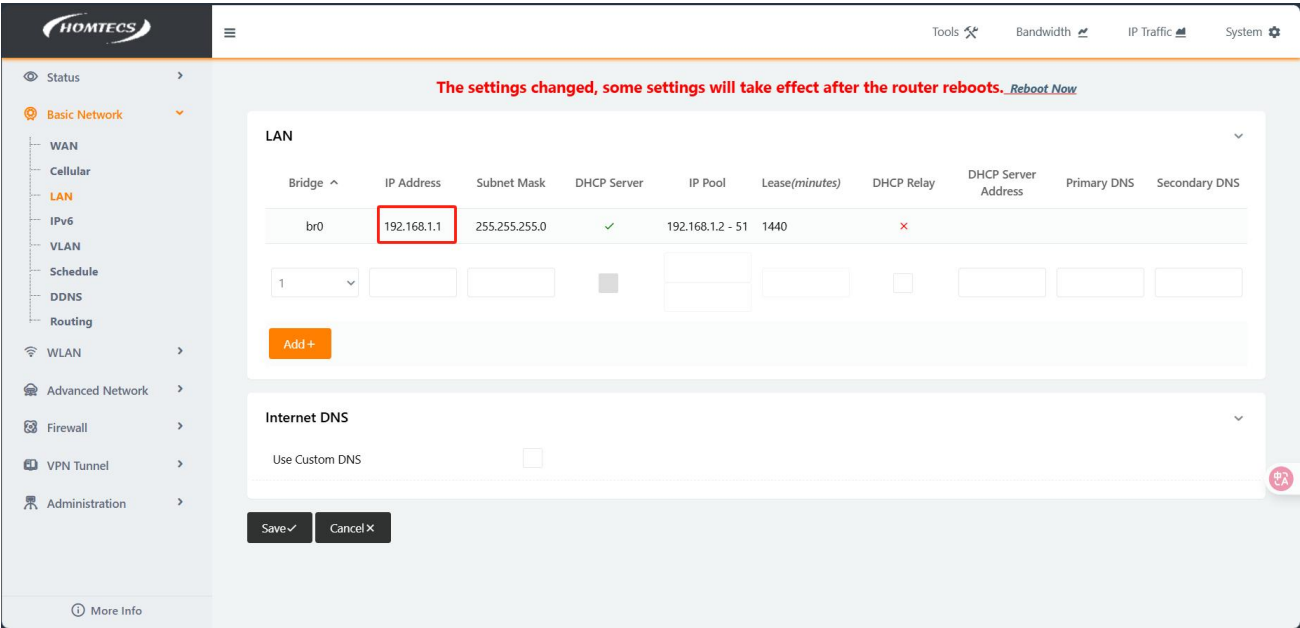


Figure 6-6 Screenshot of LAN parameter configuration

Step 2: Open the WLAN settings, configure the basic parameter settings, configure the wireless mode to the wireless bridge, the SSID and security mode and other configurations need to be consistent with the bridged device, and then save the parameters and restart the router

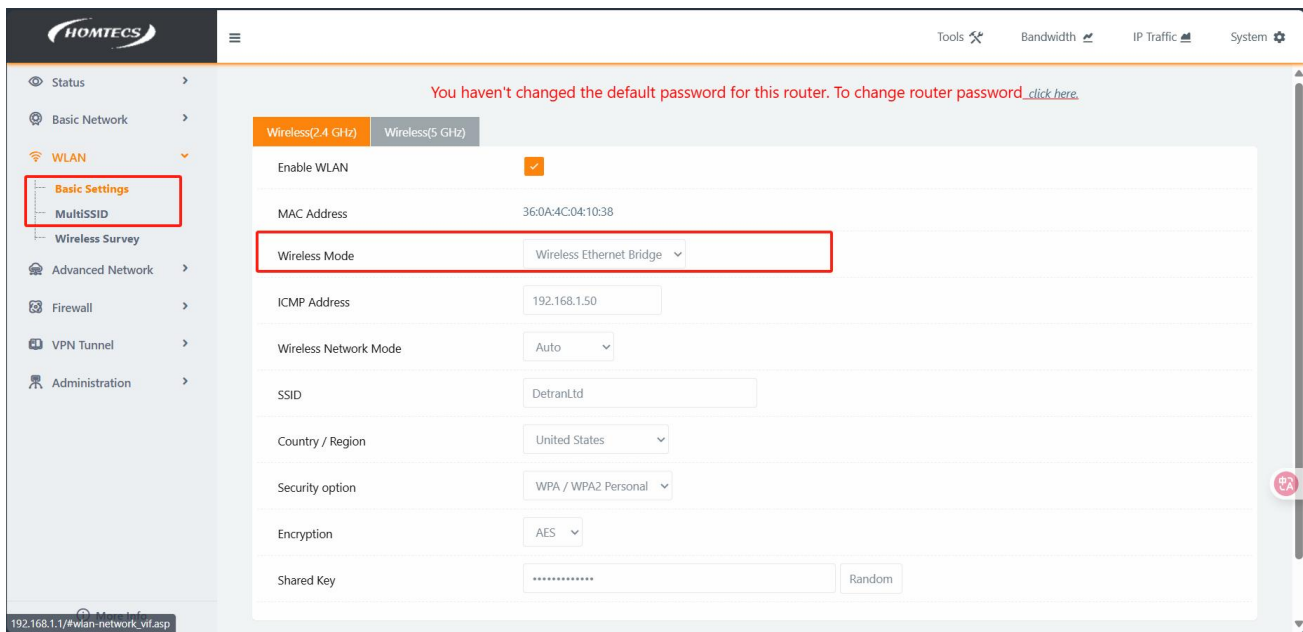


Figure 6-7 Screenshot of Wi-Fi wireless bridge parameter configuration

Step 3: Check the WLAN connection status on the web status home page of the router

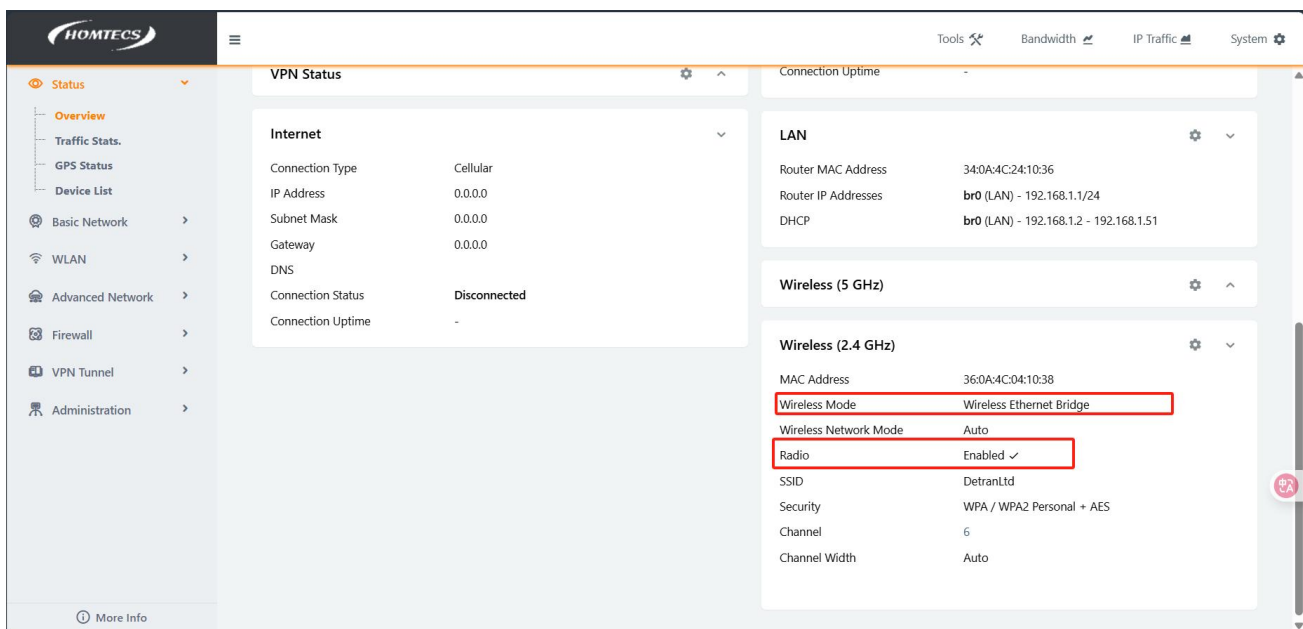


Figure 6-8 Wi-Fi wireless bridge connection

Step 4: Ping 192.168.31.1 (the gateway of the bridge device) and 114.114.114.114 (the accessible address of the Internet) respectively to check whether they can be pinged normally.

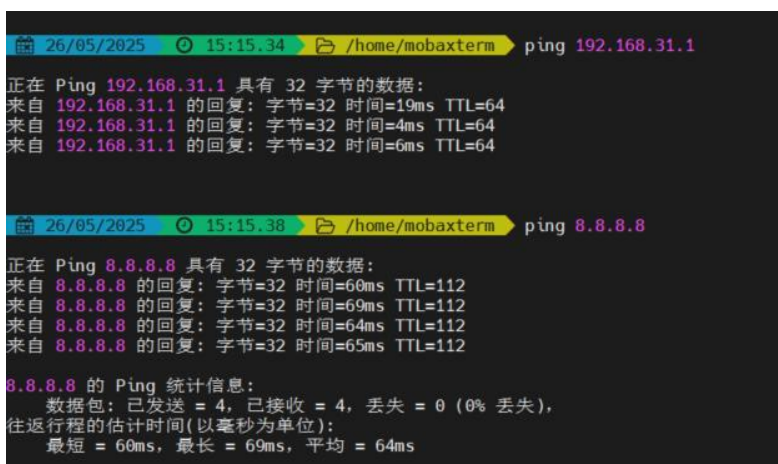


Figure 6-9 Screenshot of the Internet test

6.2. Multiple SSID

Multi-SSID is mainly used to allocate multiple WLANs, not just 2 WLANs, providing more connectivity options

Example for configuring multiple SSIDs:

Step 1: Open the WLAN settings, configure the multi-SSID, save the parameter settings, and restart the router after the configuration is complete

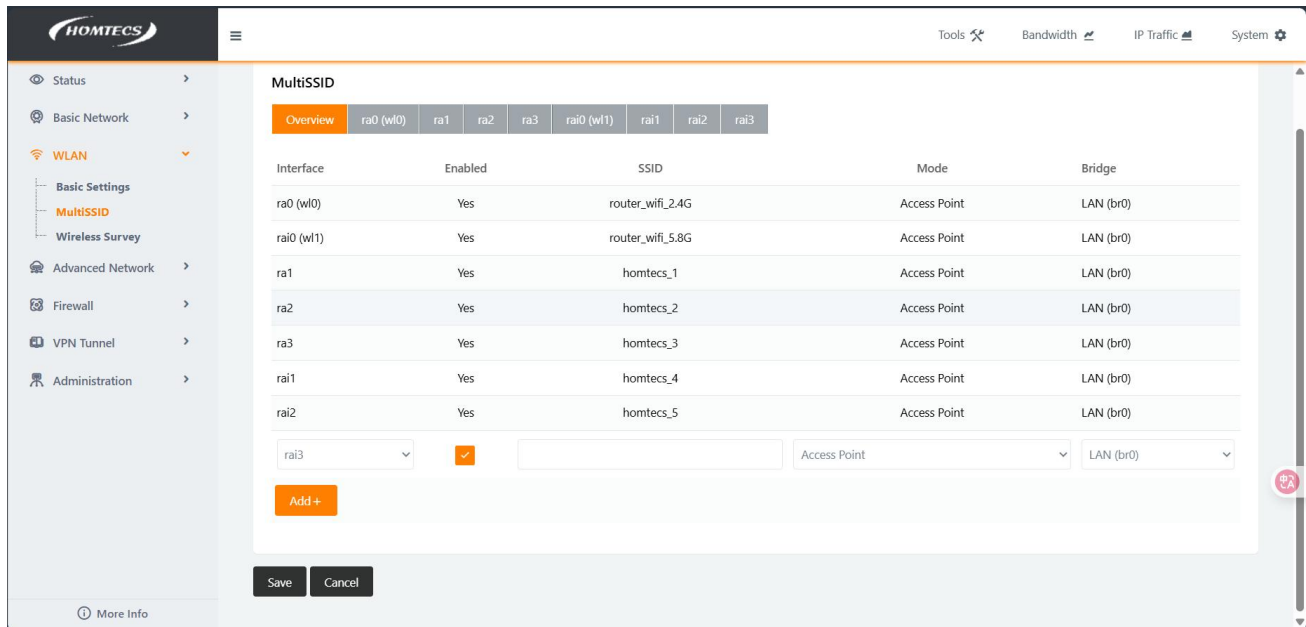


Figure 6-10 Configuring Wi-Fi parameters for multiple SSIDs is added

Step 2: Click on the web status home page of the router to check whether the information of the new Wi-Fi is normal (including the SSID name, MAC address, etc.), and other devices can be connected to WiFi normally.

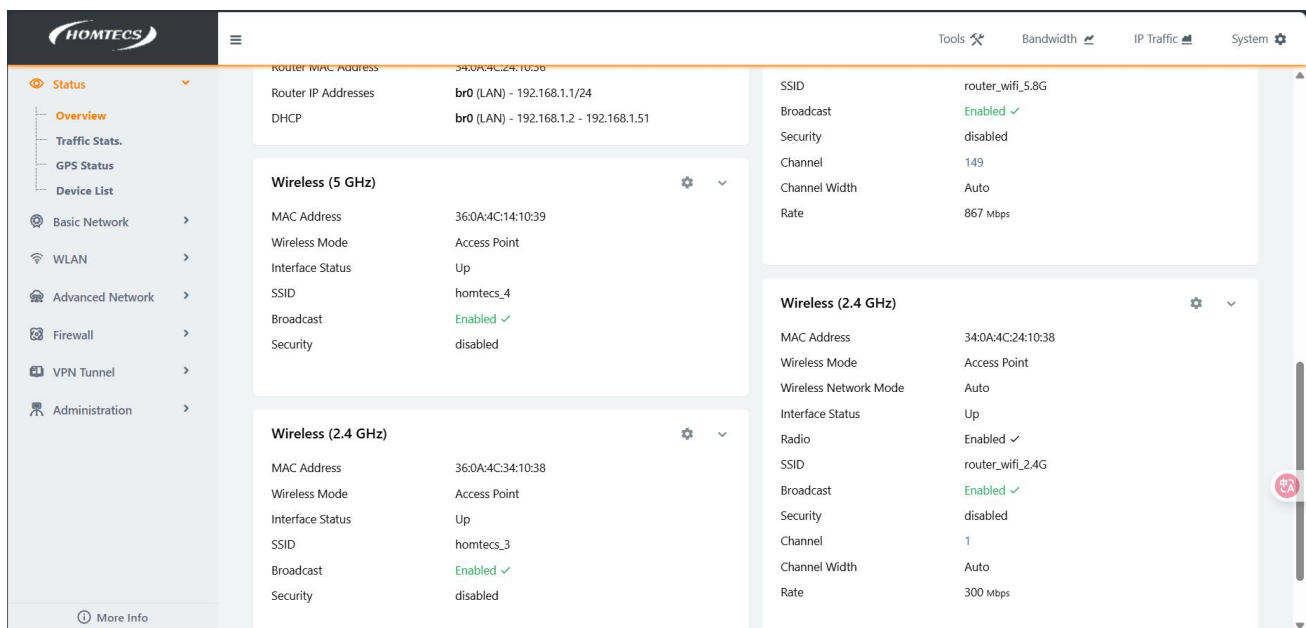


Figure 6-11 Screenshot of multiple SSIDs

6.3. Wireless Survey

In the navigation bar, select WLAN Configuration > Wireless Network Hunting. On the displayed page (Figure 6-13), you can search for information about the surrounding APs on a wireless network.

You haven't changed the default password for this router. To change router password, [click here](#).

Wireless Site Survey

Last Seen ^	Radio Band	SSID	BSSID	Channel	RSSI	Encryption
Mon 15:29:57 NEW (Det)	2.4G	router_wifi_2.4G	00:0C:43:28:80:E6	11	-58 dBm	OPEN/NONE
Mon 15:29:57 NEW (Det)	2.4G	DT_CHATGPT	04:D9:F5:B5:37:B8	2	-55 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	5G	DT_CHATGPT_5G	04:D9:F5:B5:37:BC	149	-56 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	2.4G	CU_AYHW	1C:94:68:71:D1:30	11	-58 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	5G	CU_AYHW_5G	1C:94:68:71:D1:31	56	-76 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	5G		1E:94:68:61:D1:30	56	-76 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	5G	SD-WAN2 (5G)	24:5E:BE:55:67:E8	161	-63 dBm	WPA2PSK/AES
Mon 15:29:57 NEW (Det)	2.4G	DetranLtd	24:CF:24:3E:6B:3F	6	-50 dBm	WPA2PSK/AES

192.168.1.1/#wlan/network_wifi.asp

Figure 6-13 Wireless network search

7. Advanced network configuration

7.1. IPv4 Port Forwarding

Port Forwarding is the act of forwarding a network port from one network node to another, allowing an external user to pass through an activated NAT router to a port at a private internal IP address (inside the LAN).

Source IP (optional): Only forwards data from a set IP range. Example: "1.2.3.4", "1.2.3.4 - 2.3.4.5", "1.2.3.0/24". "me.example.com".

External port : The port that should come in from WAN or 4G/5G VPN. Example: "2345", "200,300", "200-300,400"

Internal port (optional): If it is empty, it will automatically correspond to the external port. If the range of the inner port is different from the outer port, the internal port must be filled

Internal IP : Corresponding to the IP address in the local area network

In the navigation bar, select Advanced Network > IPv4 Port Forwarding. On the page that appears, you can modify the parameters for configuring port forwarding.

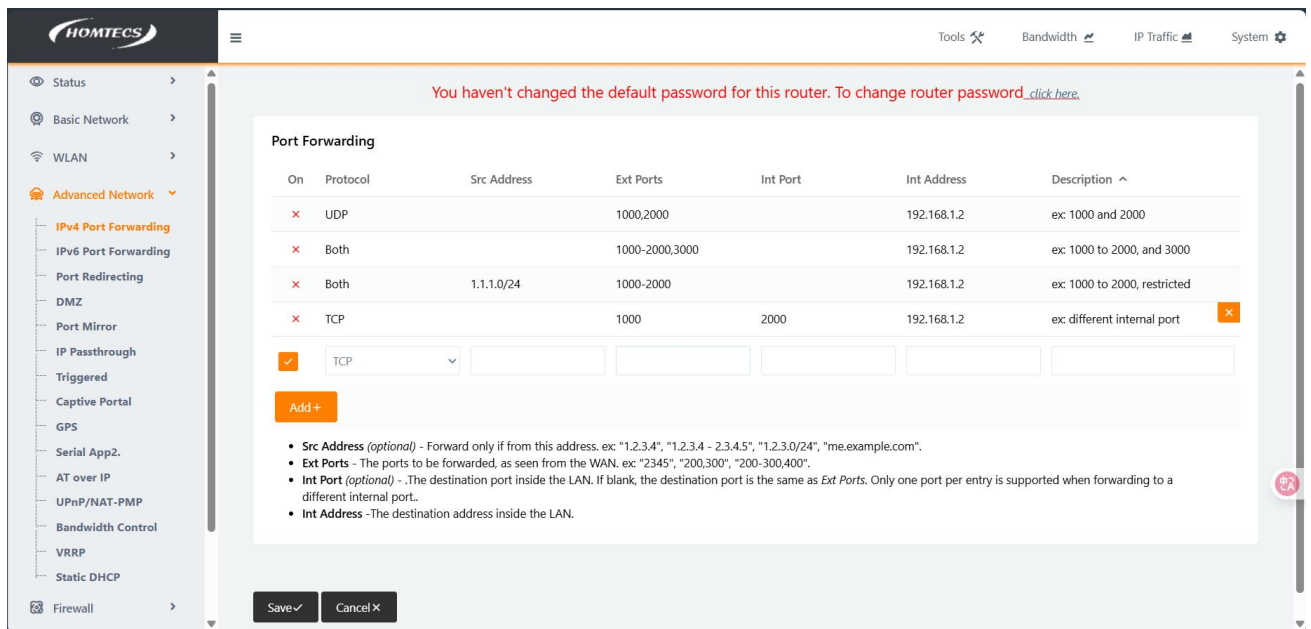


Figure 7-1 Port Forwarding

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Port Forwarding example:

Step 1:

Open the Routing web page, select Port Forwarding in Advanced Network, and configure port forwarding with 5000 ports on the external and internal ports. The internal IP address is 192.168.2.2, TCP protocol.

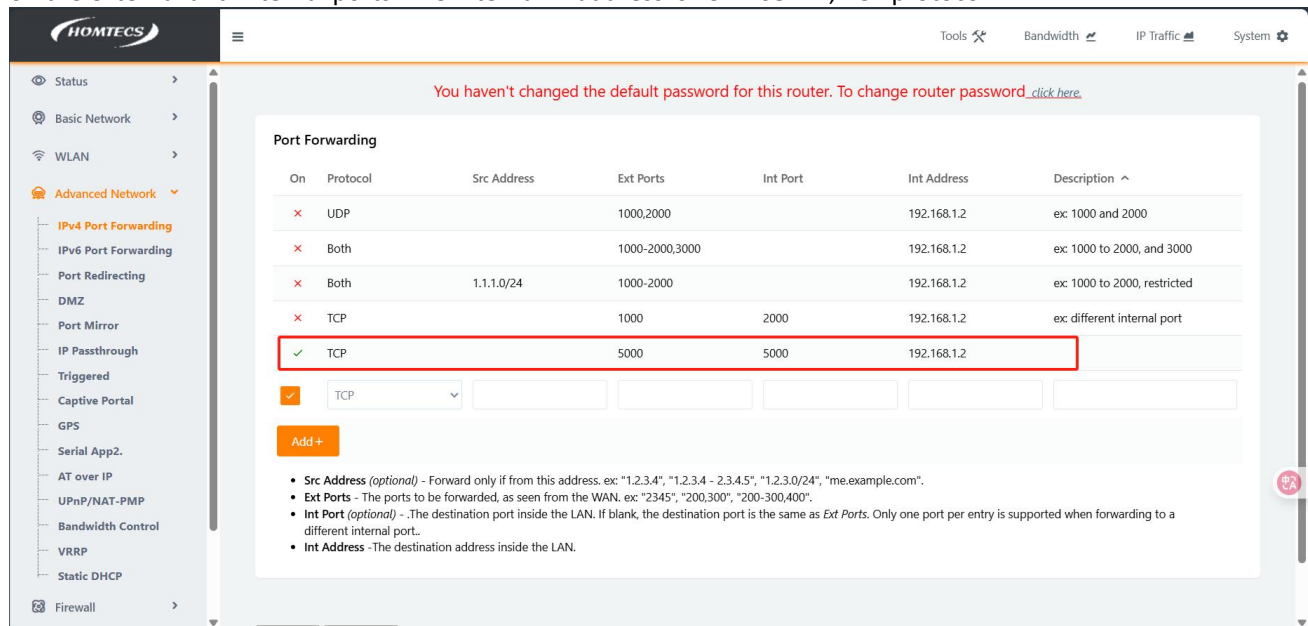


Figure 7-2 Port Forwarding Configuration

Step 2:

As the server, the local server uses the router to access the Internet and listens to the IP address and port 5000 of the local PC, and the client uses TCP to connect to the Internet IP address and port 5000 of the router.

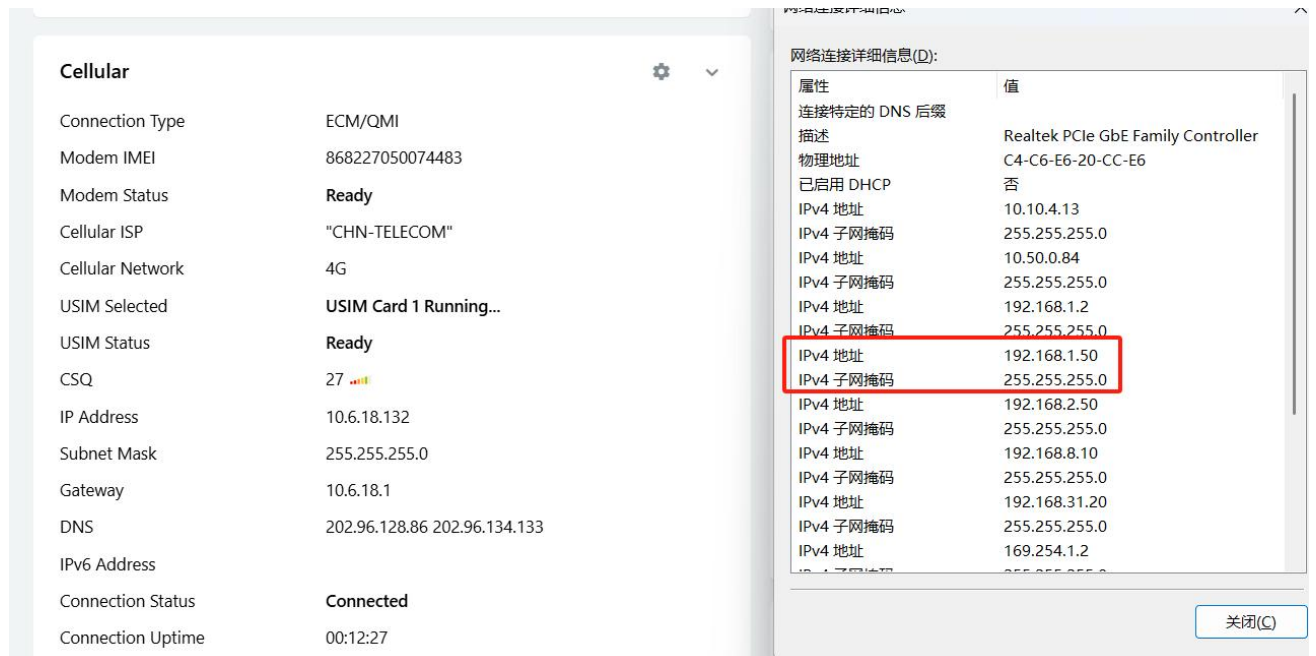


Figure 7-3 PC Setup

Step 3:

The server and the client can communicate with each other and send packets to each other

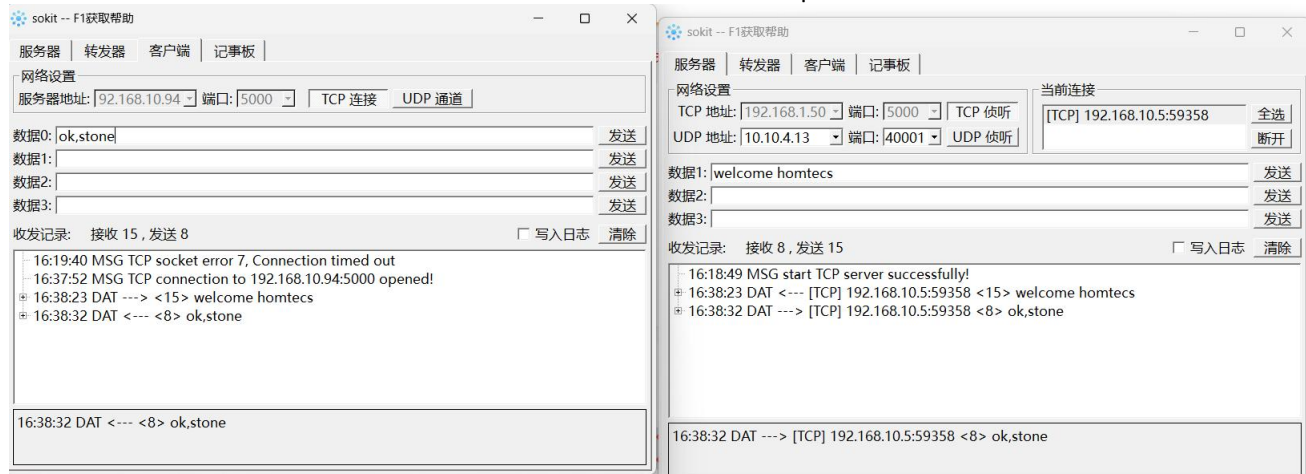


Figure 7-4 Data Transmission and Receiving

7.2. IPV6 Port Forwarding

Port Forwarding is the act of forwarding a network port from one network node to another, allowing an external user to pass through an activated NAT router to a port at a private internal IP address (inside the LAN).

Protocols - Support TCP, UDP and TCP/UDP

Source IP (optional) - Only forwards data from the specified IP range. For example: "2001:4860:800b::/48", "me.example.com".

Destination IP - The IP address within the corresponding local area network
Destination Port - Open **forwarding port**
For example: "2345", "200,300", "200-300,400"

In the navigation bar, select Advanced Network > IPv6 Port Forwarding. On the page that appears, you can modify the parameters for configuring port forwarding.

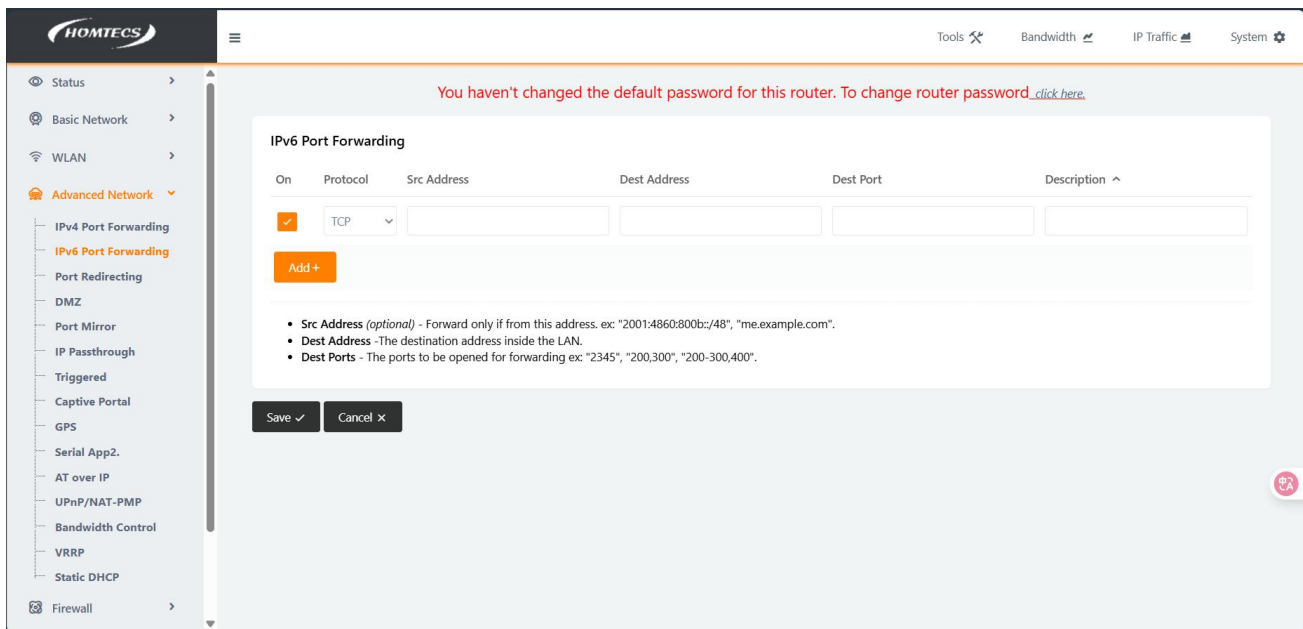


Figure 7-5

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Port forwarding example:

Step 1: Router1 opens the routing web interface, selects port forwarding in the advanced network, sets Protocol to Both, sets the source IP address to empty by default, sets the destination IP address to a temporary ipv 6 address automatically obtained by the local PC, and sets the destination port to 5 000 to save the parameter configuration. (using a telecom SIM card).

Mobile Network	
Connection Type	ECM/QMI
Modem IMEI	862430062451924
Modem State	Connected
Mobile Network	'CHN-CT'
USIM State	Ready
Signal Strength	31 dB
IP Address	10.29.55.189
IP Gateway	10.29.55.126
DNS Servers	106.38.128.68
IPv6 Address	240e:e107:ed0:0668::134.188 240e:e107:5::1
IPv6 Address	240e:e107:ed40:4668:: a109:f6b9:30f
Local Network	
Ethernet MAC Address	34.01.74:A8:C8 E0
LAN Interface	br0 (LAN) - 192.168.1.1/24
DHCP Lease	br0 (LAN) - 192.168.1.162 240e:e107:f602:aafe:rf82:e8: 2639

Figure 7-6

```

以太网适配器 以太网 2:

   连接特定的 DNS 后缀 . . . . . : 
   描述. . . . . : Intel(R) Ethernet Connection (23) I219-V
   物理地址. . . . . : 30-43-D7-EE-18-B1
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址 . . . . . : 240e:47c:3060:aff2::40b8:9b31( 首选)
   获得租约的时间 . . . . . : 2024年1月18日 14:18:27
   租约过期的时间 . . . . . : 2024年1月19日 2:18:27
   IPv6 地址 . . . . . : 240e:47c:3060:aff2:6a60:4fcc:7766:64b9( 首选)
   临时 IPv6 地址. . . . . : 240e:47c:3060:aff2:7dca:9e7c:cfee:d634( 首选)
   本地链接 IPv6 地址. . . . . : fe80::7091:8382:7706:97d4%18( 首选)
   IPv4 地址 . . . . . : 192.168.1.25( 首选)
   子网掩码 . . . . . : 255.255.255.0
   获得租约的时间 . . . . . : 2024年1月18日 15:19:54
   租约过期的时间 . . . . . : 2024年1月19日 15:19:54
   默认网关. . . . . : fe80::360a:74ff:fe82:6636%18
   . . . . . : fe80::360a:4cff:fe24:102%18
   . . . . . : 192.168.1.1
   DHCP 服务器 . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . : 305152983
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2B-D6-91-26-00-DE-AB-CA-78-CF
   DNS 服务器 . . . . . : 240e:47c:3060:aff2:360a:74ff:fe82:6636
   . . . . . : 192.168.1.1
   TCP/IP 上的 NetBIOS . . . . . : 已启用

```

Figure 7-7

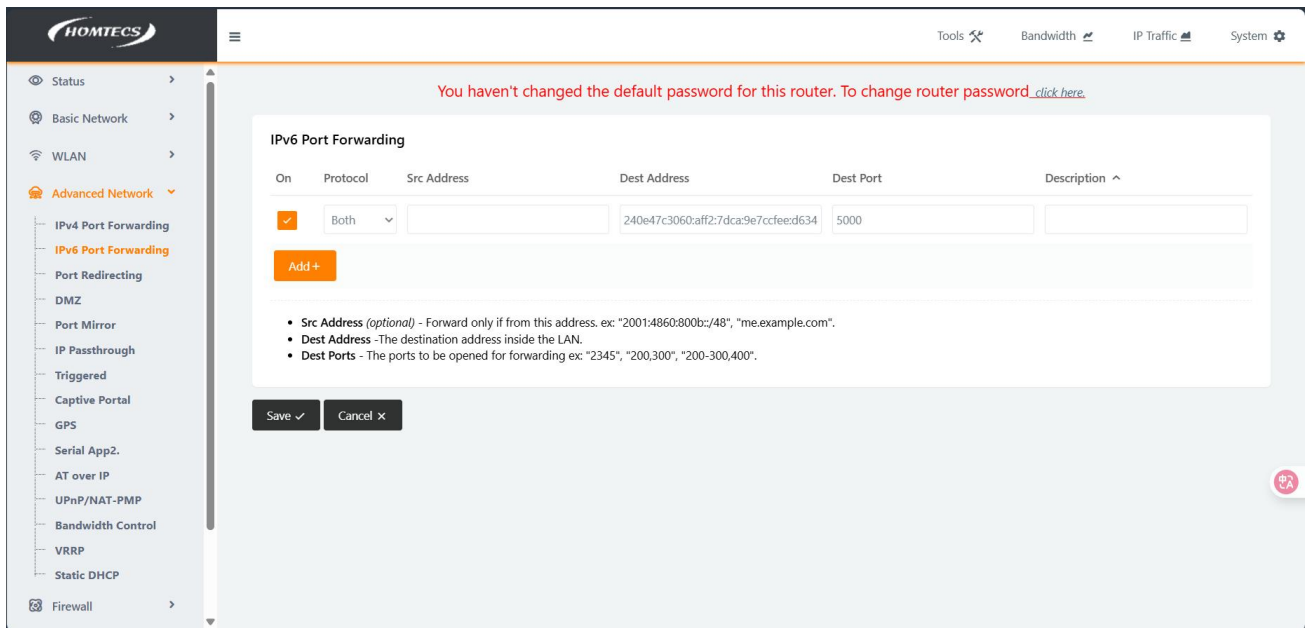


Figure 7-8

Step 2: The Router2 device uses the telecom SIM card to go online and enable IPv6 traversal

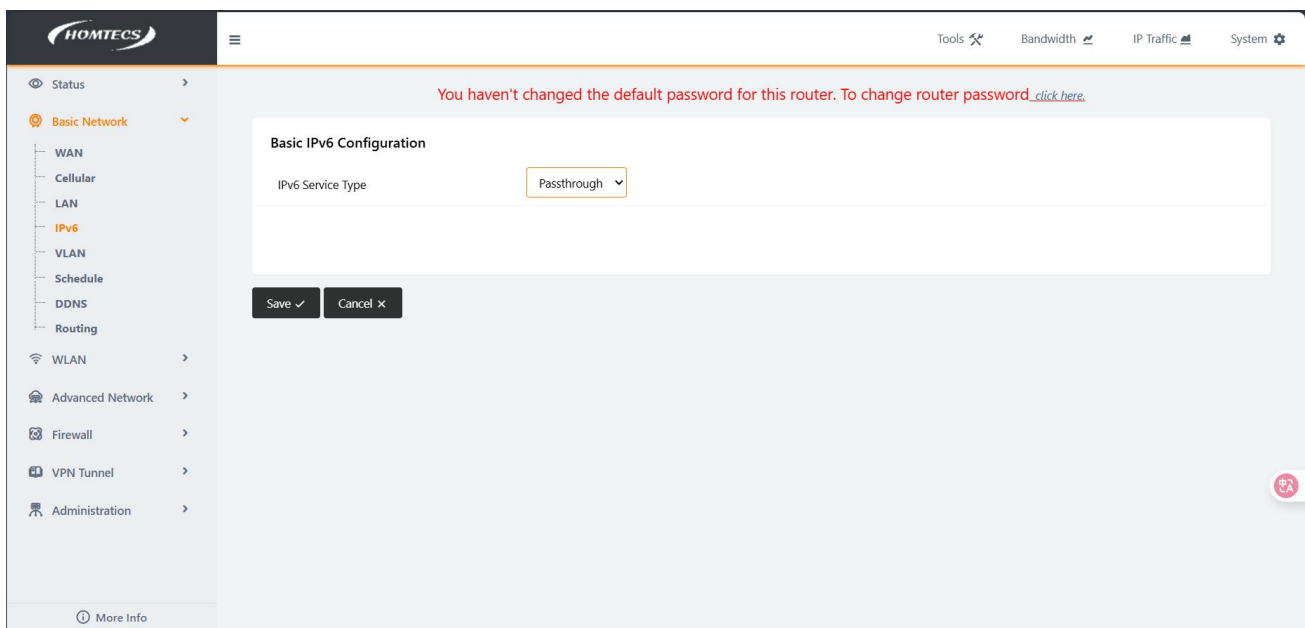


Figure 7-9

Step 3: PC 1 connected to Router1 enables the tcp service, the server address is a temporary ipv6 address, and the port number is destination port 5000

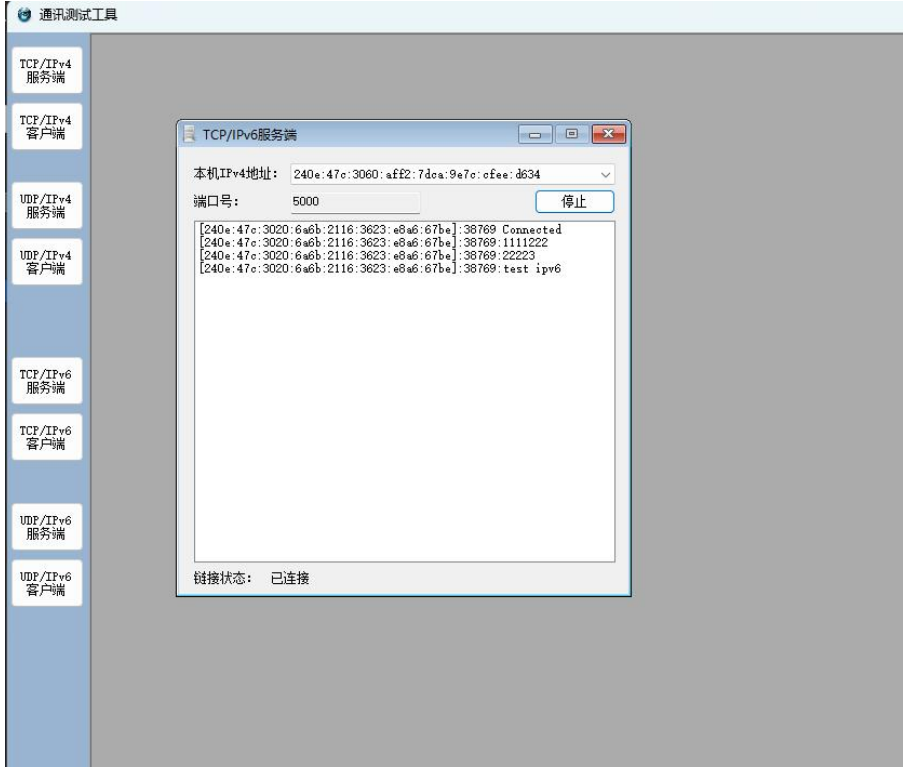


Figure 7-10

Step 4: On the PC 2 connected to Router 2, open the TCP client and use the temporary ipv 6 address of the server and the destination port 5000 to connect6. Port forwarding is normal.

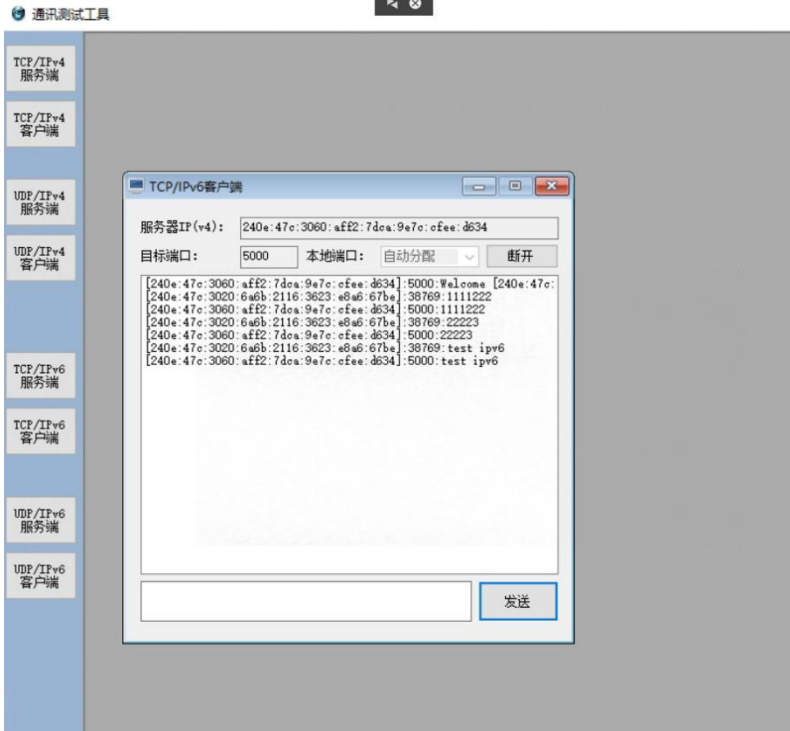


Figure 7-11

Step 5: PC1 and PC2 use the UDP protocol to communicate between the server and the client, and the data is sent and received normally

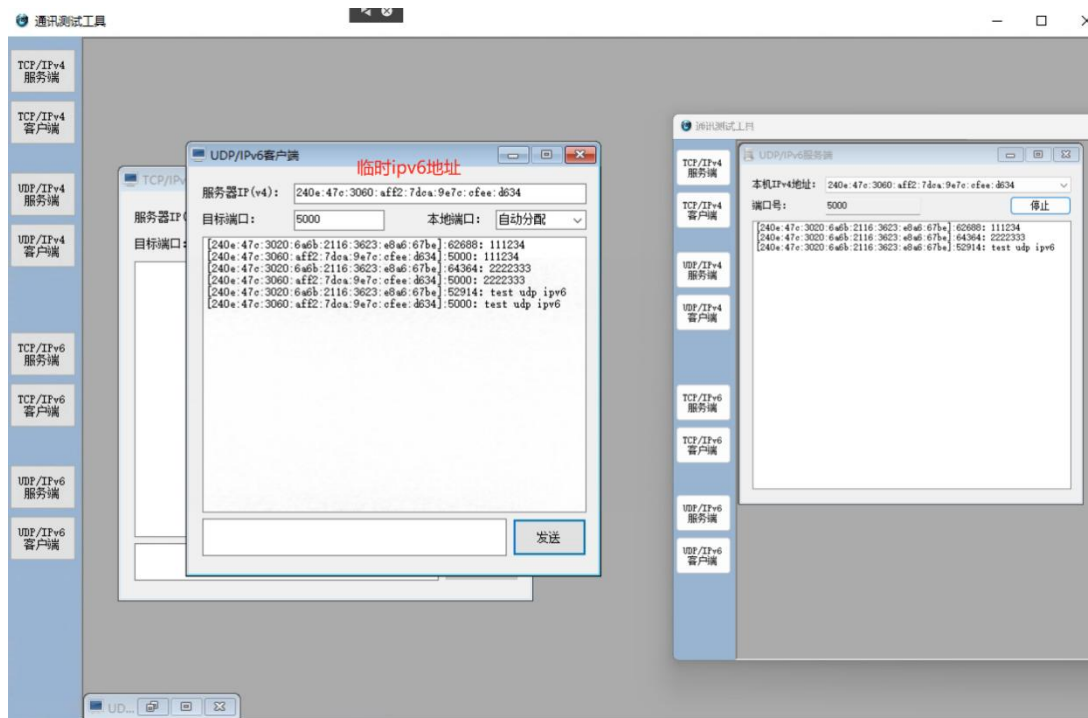


Figure 7-12

Step 6: When PC1 and PC2 enable TCP for the server and client respectively, and the IPv6 address is the same, but the port is inconsistent, the following error will be displayed: the connection fails, and normal data interaction cannot be performed.

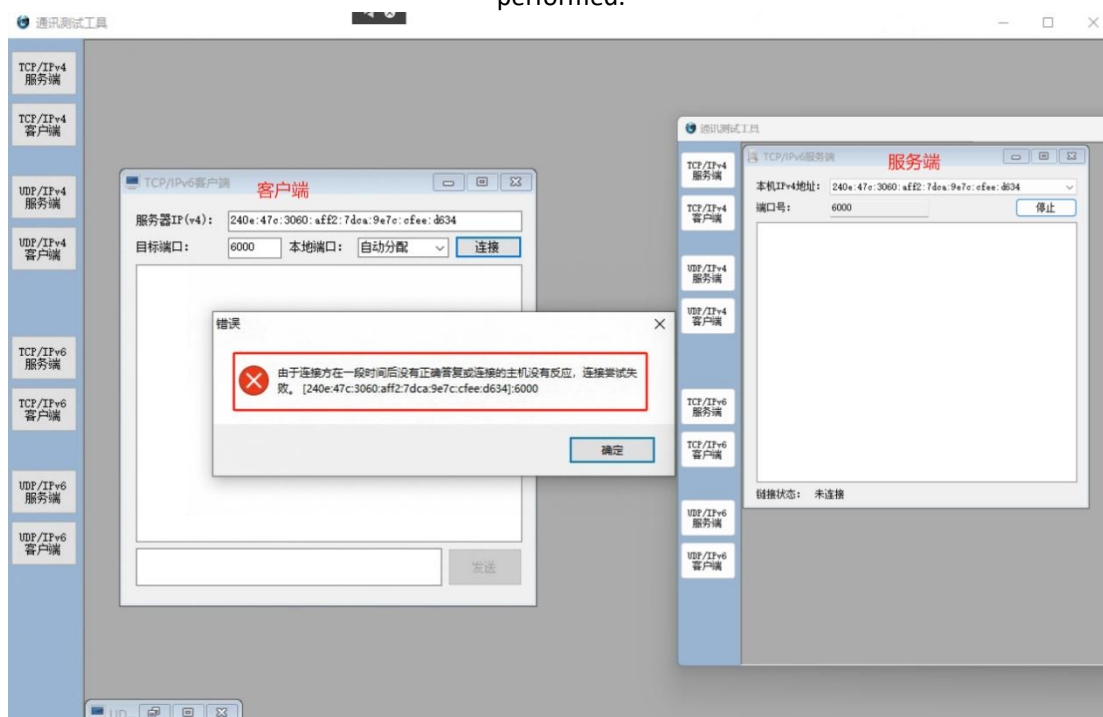


Figure 7-13

7.3. Port Redirecting

Port Redirecting is a feature of many firewalls that allows external users to connect to a specific IP address/port and to transport the firewall redirection to the appropriate internal server.

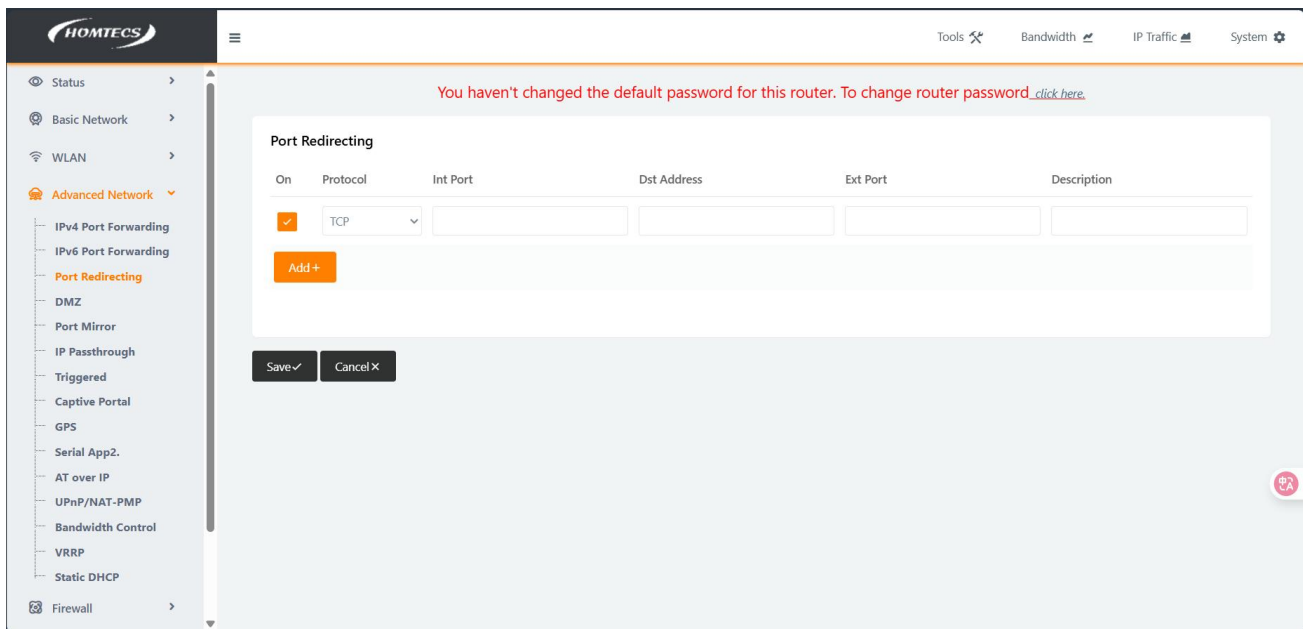


Figure 7-14

Description of Port Redirecting

Parameter	Description
enable	Tick/Unchecked
agreement	You can select three modes: TCP, UDP, TCP/UDP
Internal ports	If it is empty, it will automatically correspond to the external port. When the range of the inner port is different from the external port, the inner port must be populated
External IP	Only redirect data from a set IP range
External port	The port that comes in from the WAN

Table 7-1 Port Redirecting

Port Redirecting example:

Open the routing web interface, select Port Redirection for Advanced Network, set internal port 5000, external IP 113.88.14.30 external port 80, internal HTTP access 192.168.1.1:5000 redirect to external IP 113.88.14.30:80 web service. Click Add New to save the settings

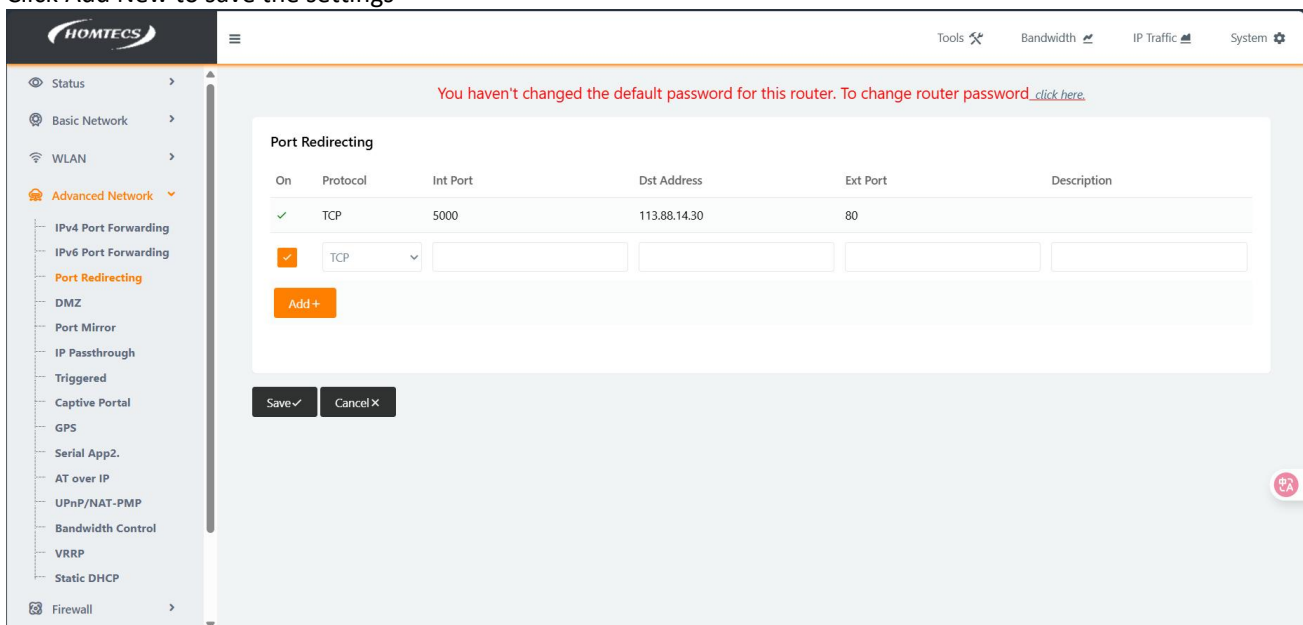


Figure 7-15 Port Redirecting

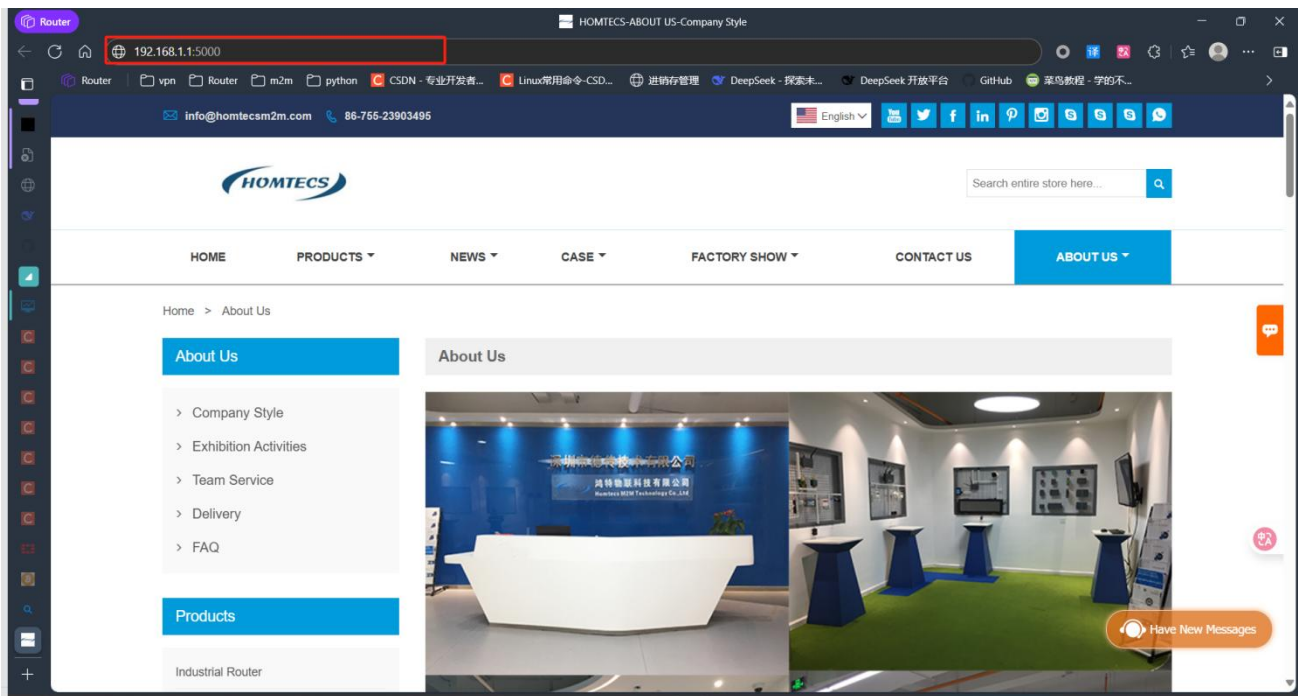


Figure 7-16 Redirect Service

7.4. DMZ

DMZ is the abbreviation of "demilitarized zone" in English, and the Chinese name is "quarantine zone" also known as "demilitarized zone". It is a buffer between the non- security system and the security system to solve the problem that the access users of the external network cannot access the internal network server after the firewall is installed. The buffer is located within a small network area between the internal and external networks of the enterprise.

In the navigation bar, select "Advanced Network >DMZ Settings". For example, if you need to map out the PC with the IP address of 192.168.1.119, then fill in the internal IP address of 192.168.1.119 and check Enable DMZ.

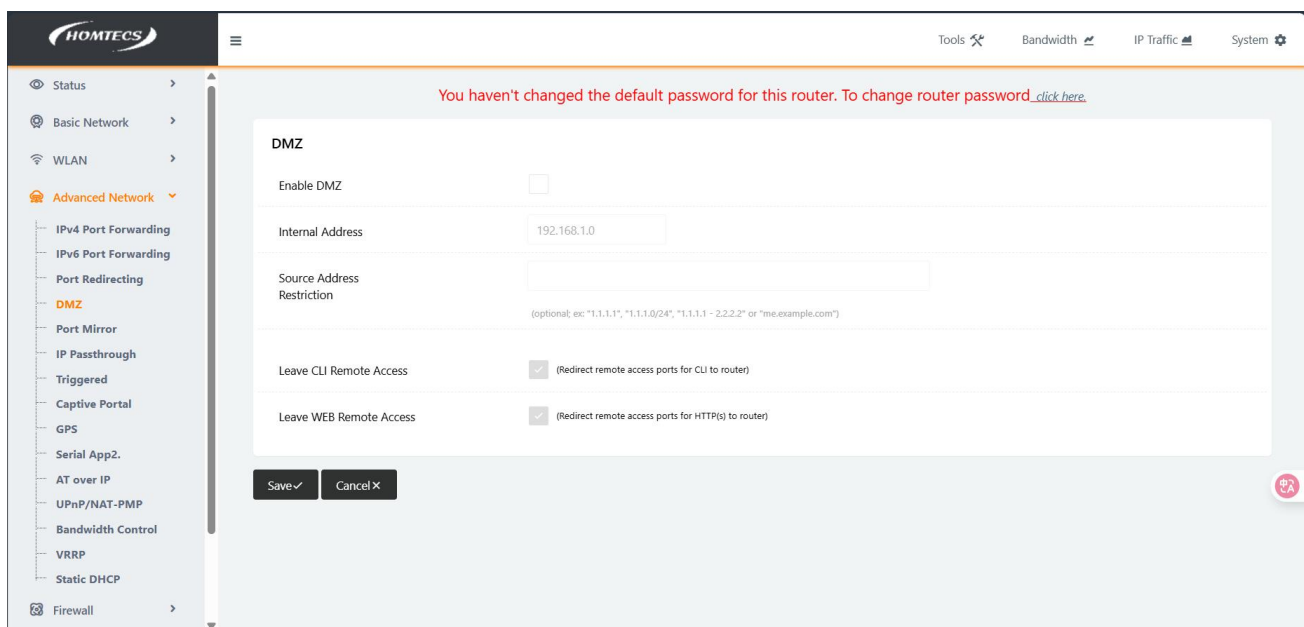


Figure 7-17 DMZ settings



WARNING

The DMZ feature allows a network terminal to be exposed to the Internet and thus use a specific service. The DMZ host forwards all ports to a computer at the same time. After clicking Enable, the PC or other terminal with the specified internal IP will be completely exposed to the public network. If you set up a DMZ host, all ports will be open to the Internet, which will take a lot of security risks, so you should only use it when necessary. When the DMZ host is set up,

all port mappings will point to the DMZ host, and port mappings to other computers will not work.

After the configuration is complete, click the Save Settings button for the configuration to take effect.

DMZ configuration example:

Step 1:

Open the web interface of the router, click DMZ settings in Advanced Network, start DMZ, fill in 192.168.2.2 for internal IP, and click Save settings

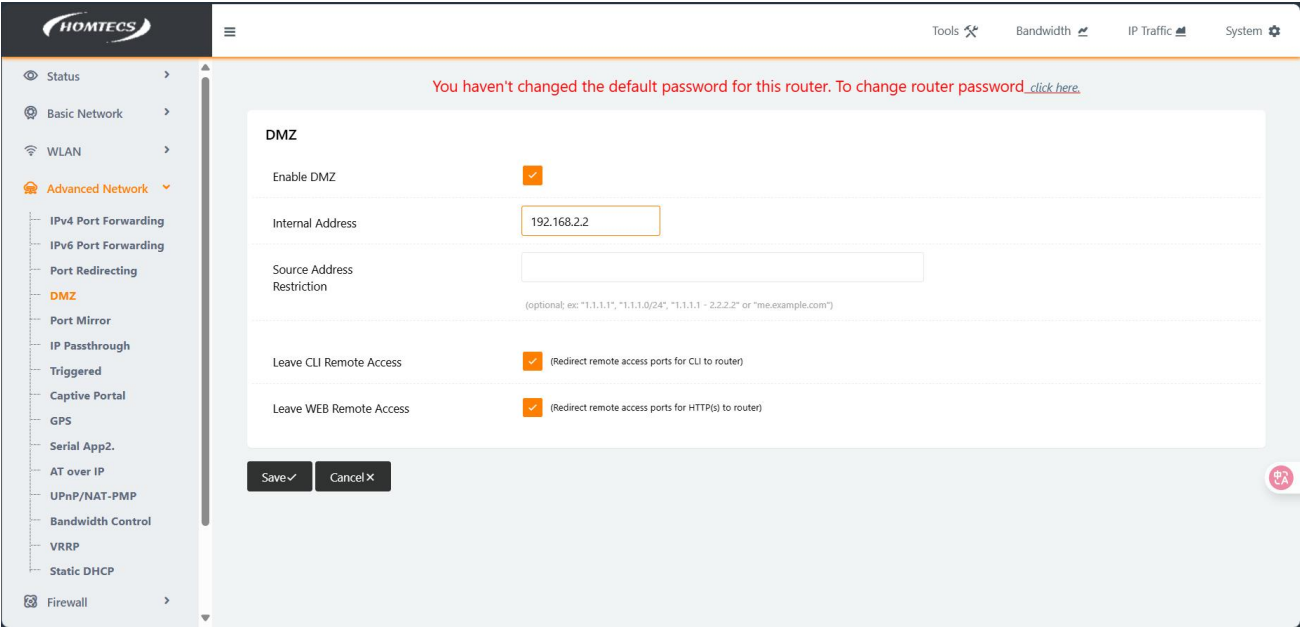


Figure 7-18 DMZ configuration

Step 2:

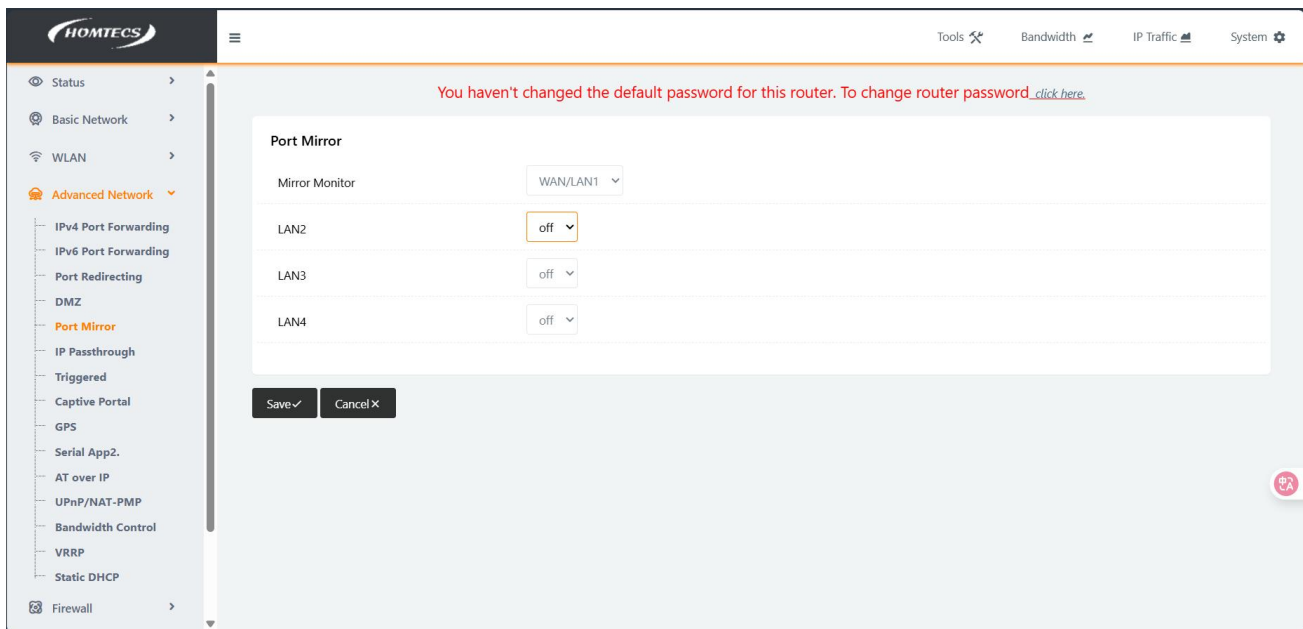
After you enter the internal IP address, you can connect to any port and connect the external IP address to the IP address of the router, and connect to the port that is the same as the internal IP address to connect to TCP or UDP and send packets to each other



Figure 7-19 Data Sending and Receiving

7.5. Port Mirror

Port Mirror, also known as port monitoring SPAN(Switched Port Analyzer), It is a network monitoring function of switches or routers, which serves to copy data from one or more ports and send it to another designated monitoring port.



7.6. IP Passthrough

When the computer is in the local area network, the computer nodes on the external network and the internal network need to connect and communicate, and sometimes the intranet penetration is not supported. In other words, the port can be mapped to allow computers on the external network to find computers on the internal network and improve the download speed.

Whether it is intranet penetration or other types of network penetration, it is a unified method to study and solve network penetration.

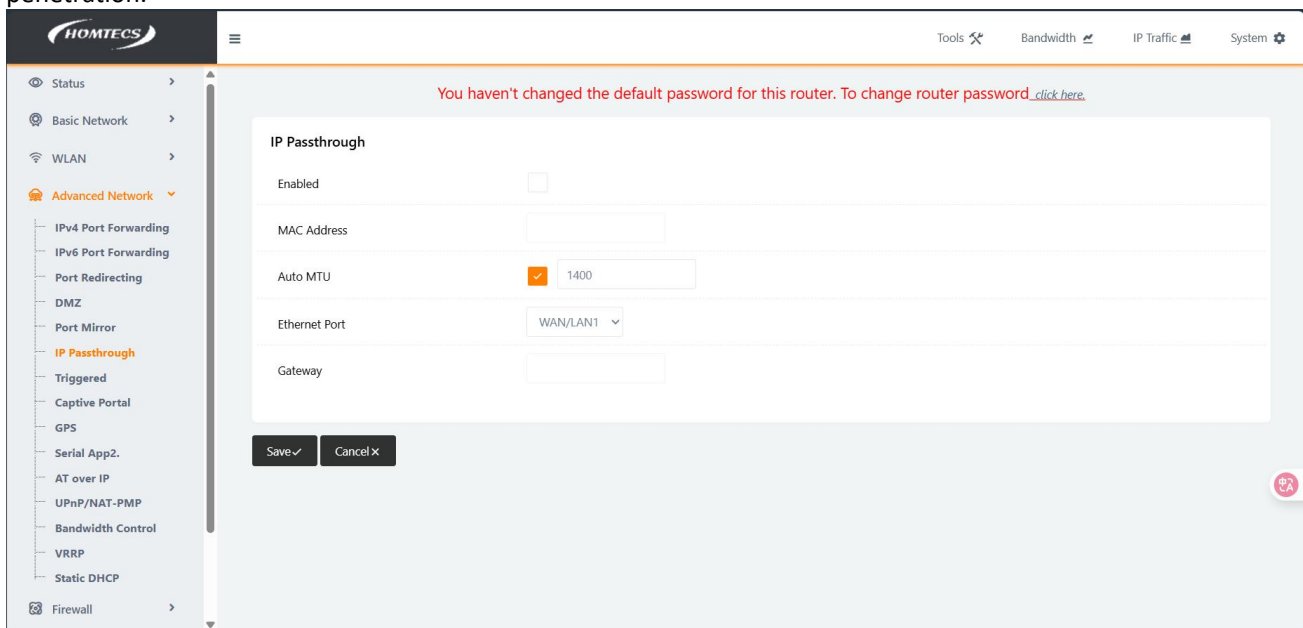


Figure 7-20

Description of the IP Passthrough

Parameter	Description
enable	Tick/Unchecked
MAC address	Enter the MAC address of the device to be penetrated
Auto MTU	MTU value setting; Default 1400
Ethernet Port	Specify whether the penetrated network port can access the Internet; Default WAN/LAN1
gateway	Specify the gateway address to be traversed

Table 7-2 IP Passthrough

Example of IP Passthrough:

Step 1:

Open the administrator: Command prompt (shortcut key win+R), enter cmd; Then enter ipconfig/all to find the MAC

address of the local connection

```
26/05/2025 17:07.32 /home/mobaxterm ifconfig

Software Loopback Interface 1
  Link encap: Local loopback
  inet addr:127.0.0.1 Mask: 255.0.0.0
  MTU: 1500 Speed:1073.74 Mbps
  Admin status:UP Oper status:OPERATIONAL
  RX packets:0 dropped:0 errors:0 unkown:0
  TX packets:0 dropped:0 errors:0 txqueuelen:0

Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
  Link encap: IEEE 802.11 HWaddr: C0-35-32-14-EE-A9
  inet addr:192.168.31.167 Mask: 255.255.255.0
  MTU: 1500 Speed:866.70 Mbps
  Admin status:UP Oper status:OPERATIONAL
  RX packets:53241 dropped:0 errors:0 unkown:0
  TX packets:22584 dropped:0 errors:0 txqueuelen:0

Realtek PCIe GbE Family Controller
  Link encap: Ethernet HWaddr: C4-C6-E6-20-CC-E6
  inet addr:10.10.4.13 Mask: 255.255.255.0
  MTU: 1500 Speed:1000.00 Mbps
  Admin status:UP Oper status:OPERATIONAL
  RX packets:442749 dropped:0 errors:0 unkown:0
  TX packets:272863 dropped:0 errors:54 txqueuelen:0
```

Figure 7-21

Step 2:
Open the routing web interface, select IP penetration in the advanced network, enable the IP Passthrough function, fill in step 1 to query the MAC address of the local connection, the router card is online, and click Save settings, as shown in the figure

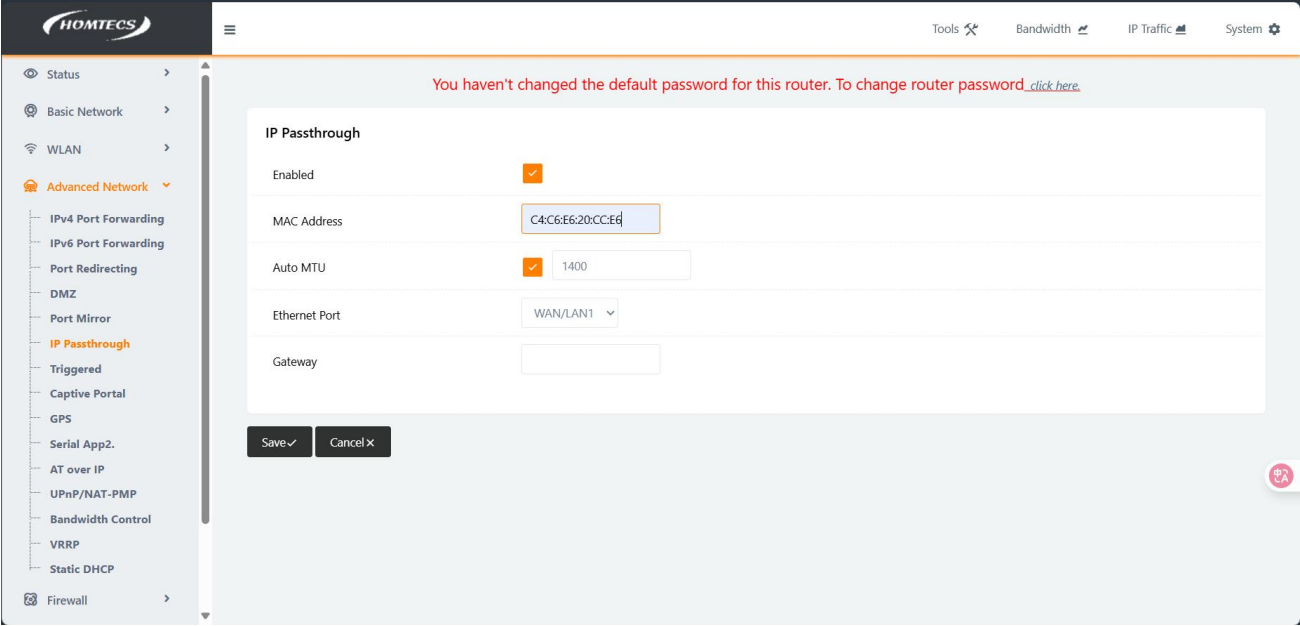



Figure 7-22 IP Passthrough settings

Step 3:
If you choose to automatically obtain the IP address and DNS server for your PC network connection, the PC can get the online IP of the card that has penetrated through and can access the Internet

Cellular	
Connection Type	ECM/QMI
Modem IMEI	867493075694306
Modem Status	Ready
Cellular ISP	"CHN-CT"
Cellular Network	LTE
USIM Status	Ready
CSQ	31 
IP Address	10.2.234.189
Subnet Mask	255.255.255.0
Gateway	10.2.234.1
DNS	202.96.128.86 202.96.134.133
Connection Status	Connected
Connection Uptime	00:12:59

```

09/08/2024 14:02:30 /home/mobaxterm tfconfig

Software Loopback Interface 1
  Link encap: Local loopback
  inet addr:127.0.0.1 Mask: 255.0.0.0
  MTU: 1500 Speed:1073.74 Mbps
  Admin status:UP Oper status:OPERATIONAL
  RX packets:0 dropped:0 errors:0 unknown:0
  TX packets:0 dropped:0 errors:0 txqueuelen:0

Realtek PCIe GbE Family Controller
  Link encap: Ethernet HWaddr: C4-C6-E6-20-CC-E6
  inet addr:10.2.234.189 Mask: 255.255.255.0
  MTU: 1500 Speed:100.00 Mbps
  Admin status:UP Oper status:OPERATIONAL
  RX packets:992004 dropped:22 errors:22 unknown:0
  TX packets:1703201 dropped:0 errors:7352 txqueuelen:0

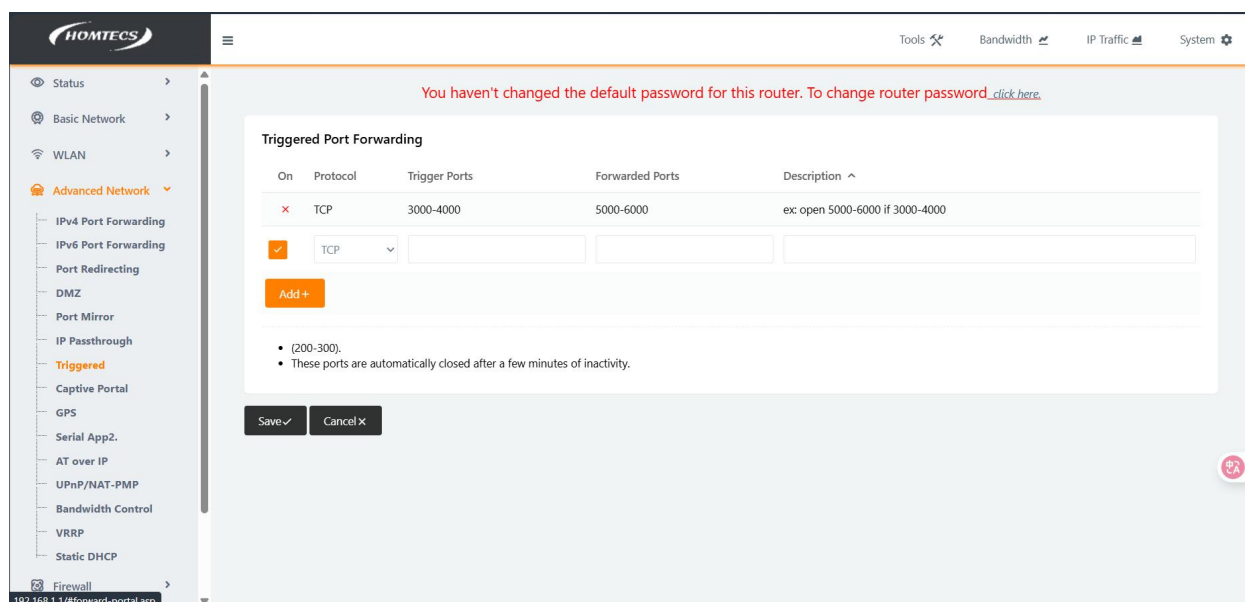
```

Figure 7-23 IP Passthrough

7.7. Triggered

The full name of Triggered is Port Triggering. In a computer network, when an application establishes an outward connection using a specific port (trigger port), the router forwards the external connection to a port specified internally (the forwarding port). Both the trigger port and the forwarding port can be a port range, such as 5000-6000. This is similar to port forwarding, but unlike port forwarding, forwarding is established after a certain amount of traffic is generated on the triggering port, that is, port forwarding occurs only after it is triggered. Once the trigger condition is not valid, the forwarding will also end.

In the navigation bar, select “Advanced Network > Triggered”. On the page that opens, you can modify the parameters related to the configuration port triggering function.



You haven't changed the default password for this router. To change router password [click here](#).

On	Protocol	Trigger Ports	Forwarded Ports	Description
<input checked="" type="checkbox"/>	TCP	3000-4000	5000-6000	ex: open 5000-6000 if 3000-4000

[Add +](#)

- (200-300).
- These ports are automatically closed after a few minutes of inactivity.

[Save](#) [Cancel](#)

Figure 7-24 Triggered

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Port trigger configuration example:

Step 1:

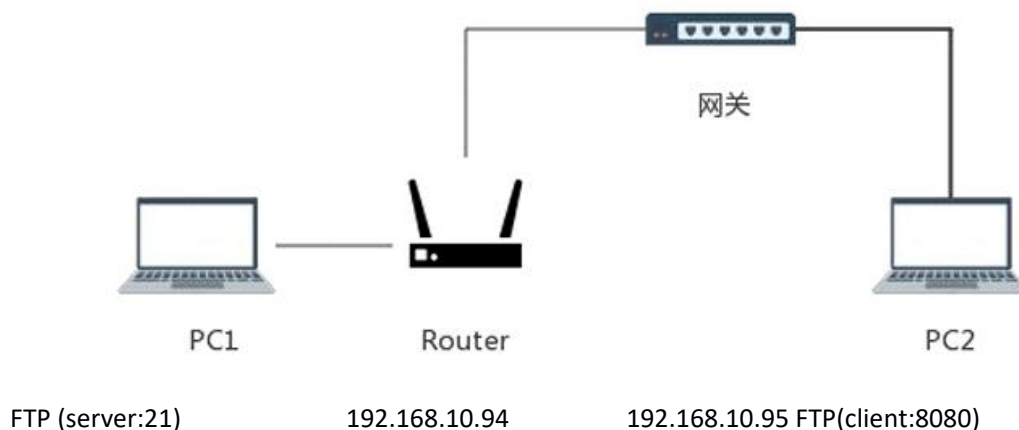


Figure 7-25 Triggering networking

- 1) Figure 7-25 Triggering networking
- 2) TURN ON THE ROUTER WEB SERVER
 - ① Turn on the port triggering feature in the router's advanced network Protocol: TCP
 - ② Trigger port: 8080
 - ③ Map ports: 21
 - ④ Click Add New and save the settings

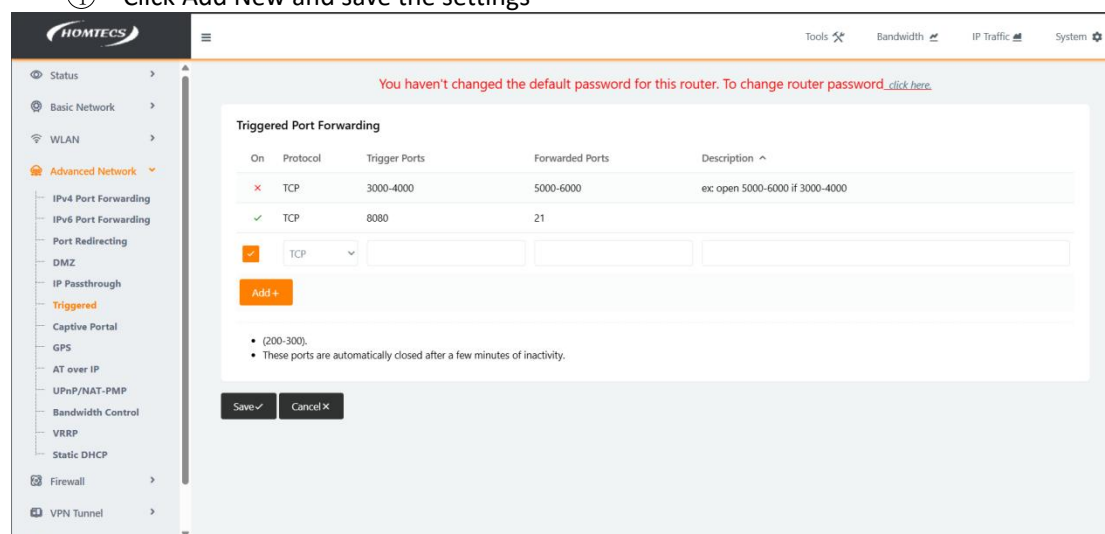


Figure 7-26 Triggered Configuration

Step 2:

In the navigation bar, select Basic Configuration > WAN Network. On the page that opens, select a static address from the drop-down box, configure the parameters of the static address, and click Save Settings. As shown in the figure below (Note: the configuration of measurement parameters is an example, and the actual configuration needs to be configured according to the site conditions):

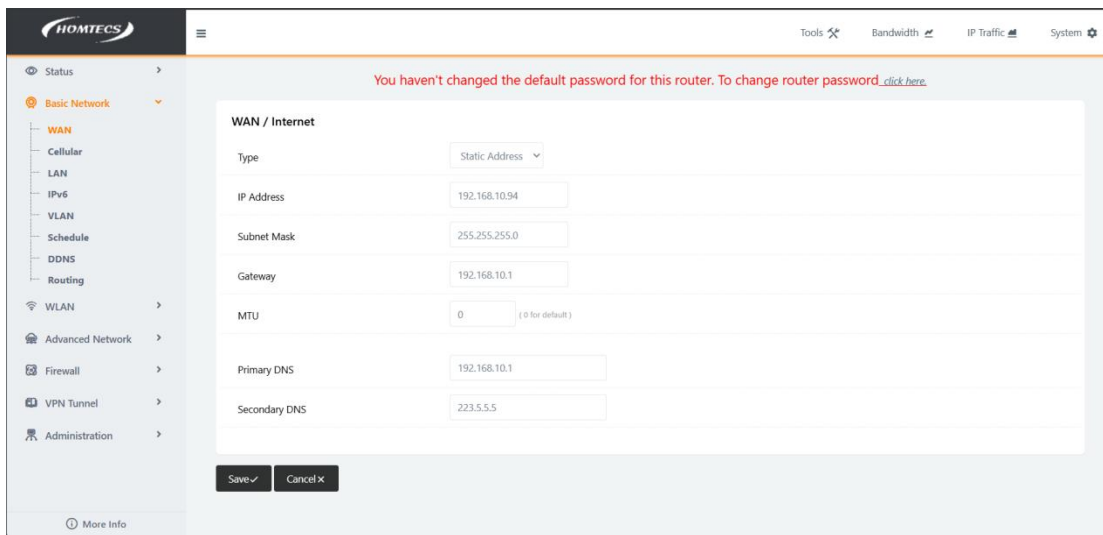


Figure 7-27 Static address settings

Step 3:

In the navigation bar, select Basic configuration > mobile networks. On the page that opens, uncheck the Enable module (Note: it is checked by default) and click Save Settings

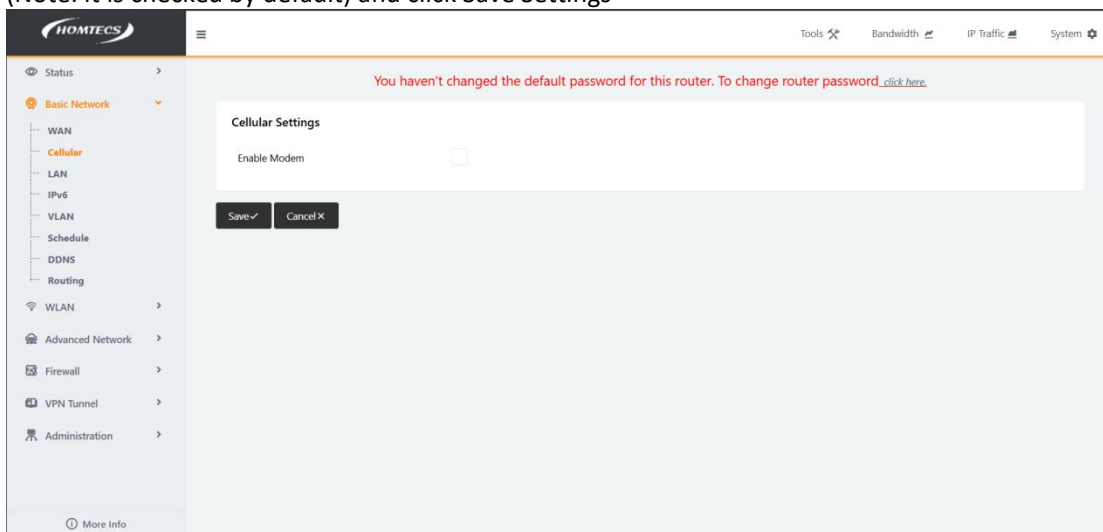


Figure 7-28 Mobile Network Settings

Step 4:

① In the navigation bar, select Basic Configuration > VLAN. In the page that opens, remove the WAN with VID1 checked, and click OK, as shown in the image:

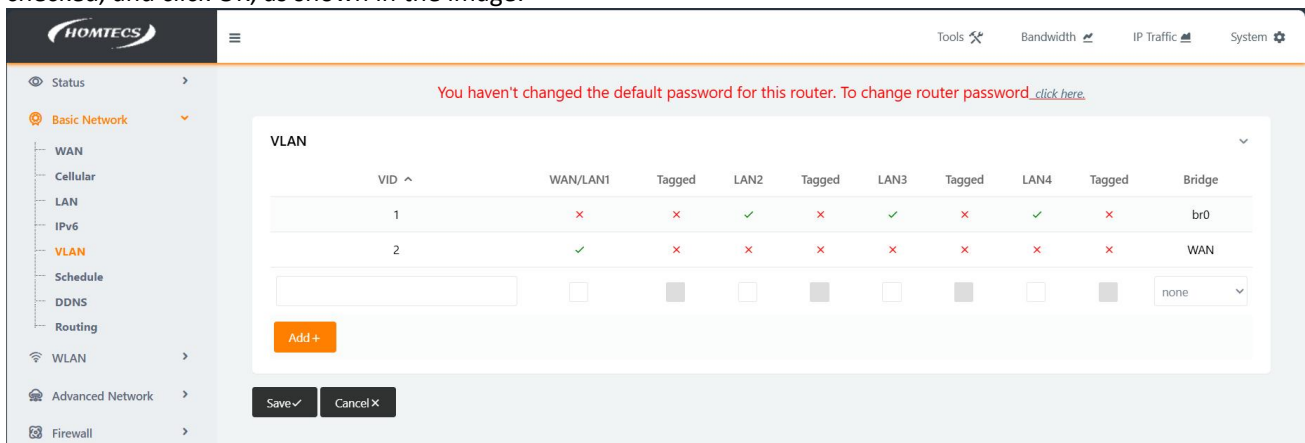


Figure 7-29 VLAN Settings

② In the VLAN page, add VID2, check WAN, click OK, and click Save Settings after the settings are completed, as shown in the figure

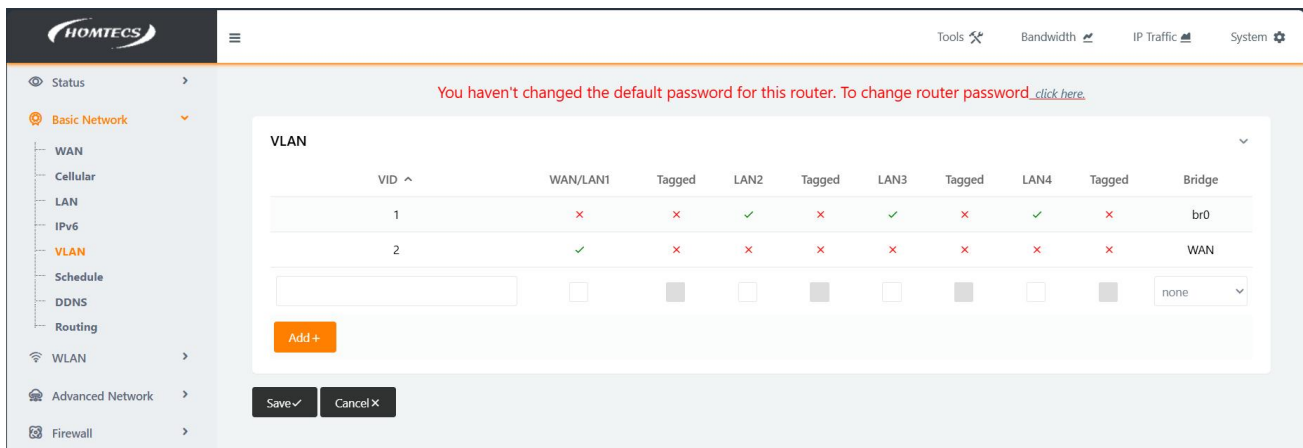


Figure 7-30 VLAN Settings

Step 5:

Configure a local connection gateway for PC1 (PC1 for PC1 with address 134).

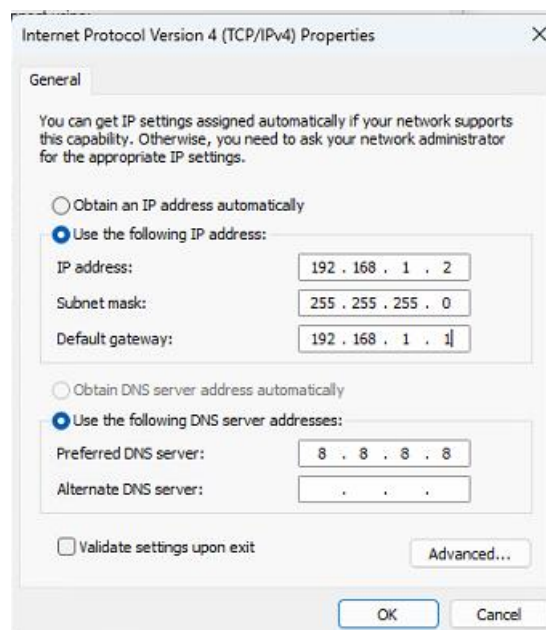


Figure 7-31 Local Connection Diagram

Step 6:

- (1) Open the TCP-UDP tool as the client (PC2 as the server) choose TCP-UDP Client
- (2) Host: 192.168.10.33 (PC2 host address)
- (3) Port 8080 (Router Configuration Trigger Port) Protocol: TCP
- (4) Click Connect
- (5) If the server is PC2, enable the TCP-UDP tool, set port 8080, and enable listening Implement data transmission between the server and the client through the trigger port
- (6) Figure 7-32 Data is sent and received from each other

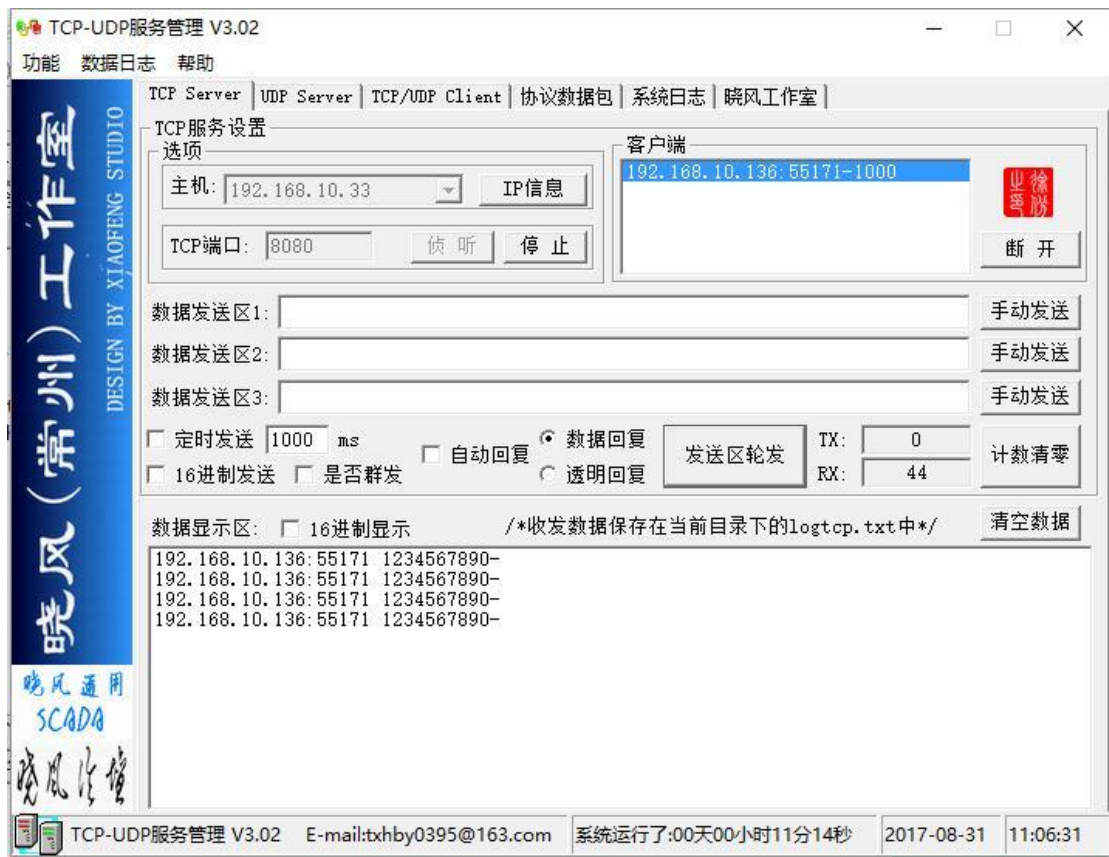


Figure 7-32 Data is sent and received from each other

Step 7:

PC1 Open FTP Easy Version Tool

(7) New User

(8) Configure user password and file path

(9) Click to save

(10) Click the start button



Figure 7-33 FTP Lite configuration

Step 8:

(1) Address: 192.168.10.136 (PC1 host address)

- (2) Username: pd (added user in FTP Simple Tool in PC1)
- (3) Password: 123123 (added user password in FTP Easy Tool in PC1)
- (4) Port: 21 (router port triggers the configured mapped port)
- (5) Click Connect
- (6) Get the file directory of PC1 (the directory in the file path of the FTP tool in PC1)

7.8. Captive Portal



WARNING

Both R series and G series routers are available in versions with portal advertising push function. The following settings are only valid for the version with the portal function.

Note: The pop-up page can be customized by the customer or we can customize the unique pop-up page according to the customer's requirements. In addition to forcing pop-up web pages, the portal function can also limit traffic and filter ports for access users. You can also set features such as login timeout, idle timeout, redirect homepage, whitelist, and more.

The Portal function will force a pre-configured function page to pop up when the user accesses the router and opens the browser to access the web page.

The page is a simple pop-up page with an image ad, please see the renderings below. On this page, when users click the "OK, I agree!" button and they can directly access the Internet normally.

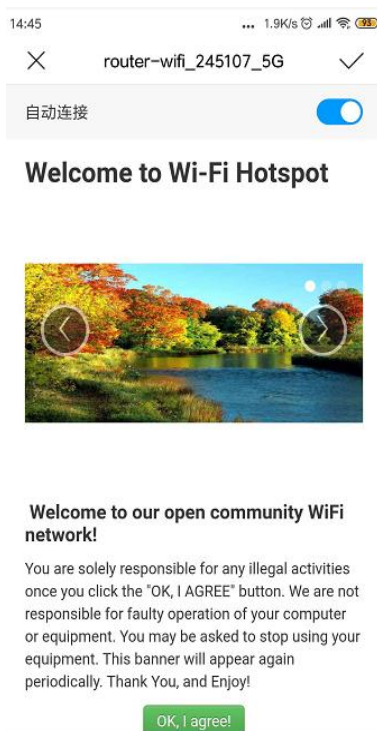


Figure 7-34

Here's how to set it up:

In the navigation bar, select "Advanced Network > Hotspot Push" to use the hotspot push function.

Redirect website <http://> : After the user authentication is completed, they will automatically be redirected to the configured web page.

Login service timeout: After the user authentication is passed, if the login time exceeds the time set here, the router will pop up the portal page again and the user needs to re-authenticate.

Terminal Idle Timeout: After the user authentication, if there is no data traffic within the specified time, the router will pop up the portal page again and require the user to re-authenticate.

Authentication-free MAC address: If the MAC address of the user's device is set here, the user will not pop up the portal page and can surf the Internet normally without authentication.

Terminal flow control: This service is used to control the uplink and downlink rates of a user after the user is authenticated.

[System Management] -----> [Storage Management] This page is used to send video files to the router so that the video in the router can be updated.

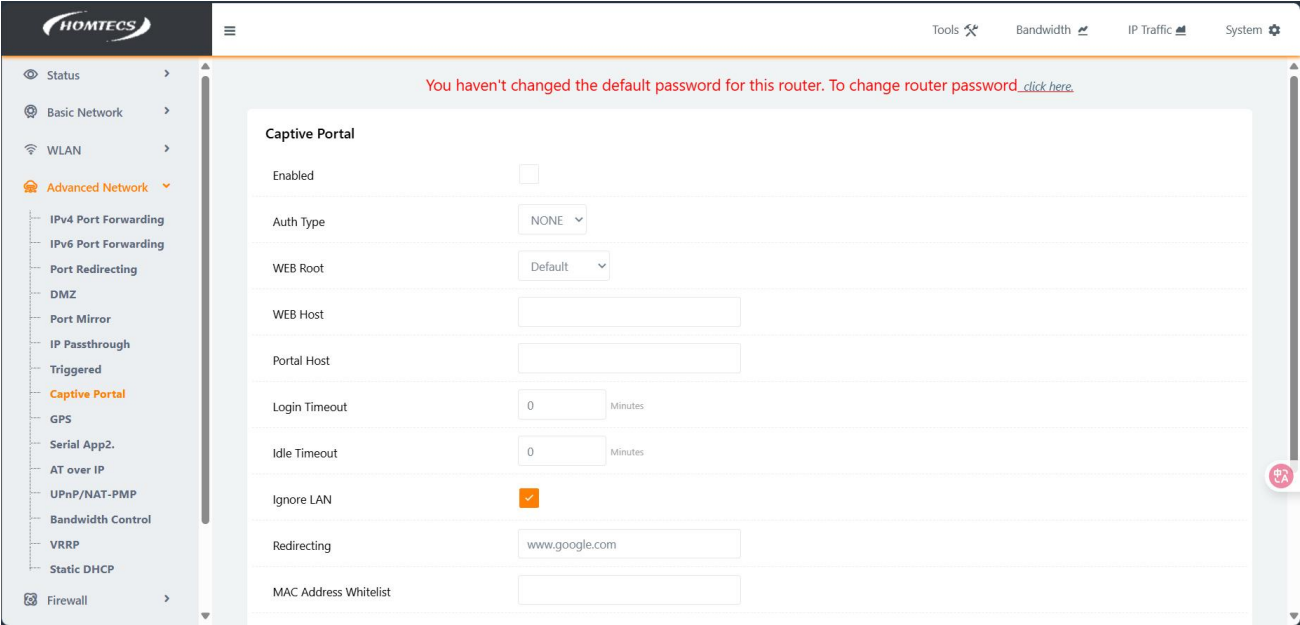


Figure 7-35

After the configuration is complete, click the Save Settings button, restart the configuration after the configuration is complete, and the portal pops up when the phone connects to the AP after going online.

7.9. Serial App2.

In the navigation bar, select Advanced Network > Serial App2. On the page, you can modify the parameters related to configuring the serial port application function.

The system defaults to the [Disabled] state, and you can select one of the working modes of [Server] and [Client] from the drop-down list. According to the current statistics, the vast majority of applications use the [client] working mode.

The following uses the [Client] mode as an example to illustrate the settings.

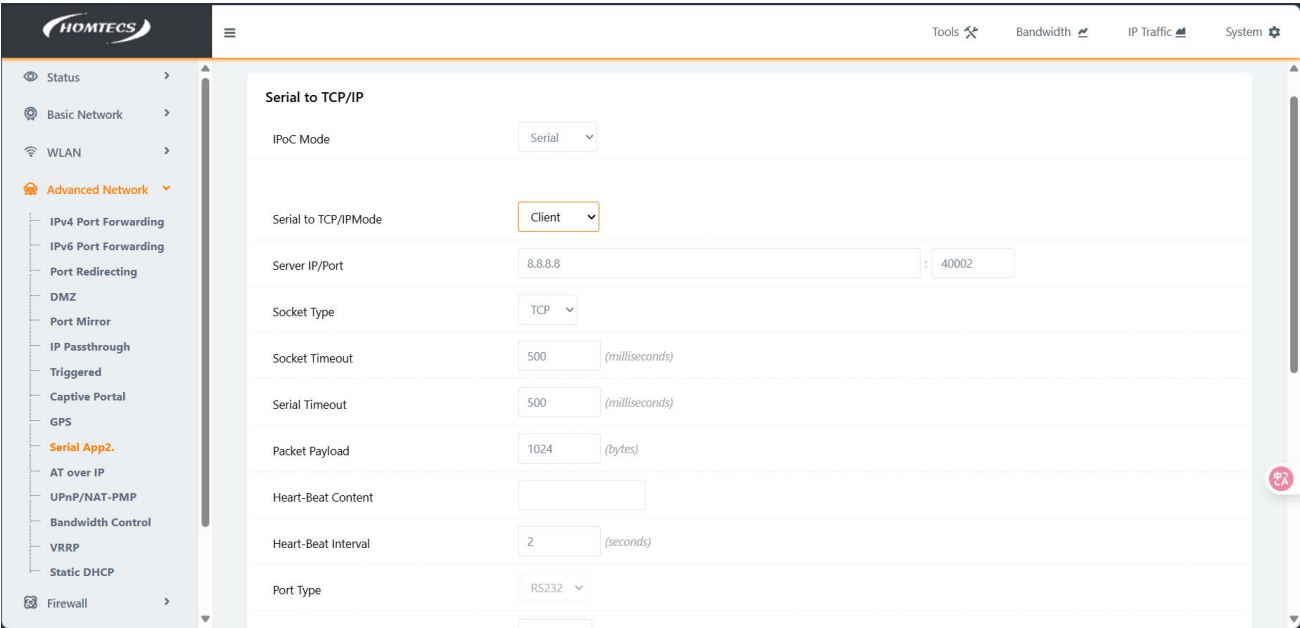


Figure 7-36

Select [Client] from the drop-down list to set the parameters of the serial port application client as shown in the table.

Parameter	Meaning	How to configure
Central host IP/port	Connect to the host IP/port of the hub	Enter the IP address of the monitoring server and the port on which it listens
Transmission Protocols	TCP/UDP protocol is supported	Select TCP or UDP based on your application
Link heartbeat packet content	Heartbeat data that maintains the link	It is used to monitor whether the device is online or not, and can be set by yourself
Link heartbeat packet interval	Heartbeat packet interval	It can be adjusted according to your own tolerance and business needs, and the default is every heartbeat every 2 seconds
Serial baud rate	Physical serial port communication settings	Fill in the baud rate of the connection between the lower computer and the serial port of the router
Check digit	None, odd, even	None by default and can be adjusted according to the field application
Data bits	5、6、7、8	Default 8, can be adjusted according to field application
Stop bits	1、2	Default 1, can be adjusted according to the field application

Table 7-3

Example of serial port application configuration:

Step 1:

Open the web interface of the router, click the serial port application in the advanced network, and set the serial port application parameters

1. Serial application network mode: client
2. Central host or IP address, port: 192.168.1.2 40002
3. Baud rate: 115200
4. Click Save settings

The screenshot shows the HOMTECS router's web interface. The 'Advanced Network' section is expanded, and the 'Serial App2' option is selected. The 'Serial to TCP/IP' configuration page is displayed. The configuration includes the following settings:

- IPoC Mode:** Serial
- Serial to TCP/IP Mode:** Server
- Bind Port:** 40002
- Socket Type:** TCP
- Socket Timeout:** 500 (milliseconds)
- Serial Timeout:** 500 (milliseconds)
- Packet Payload:** 1024 (bytes)
- Port Type:** RS232
- 波特率 (Baud Rate):** 115200
- 校验位 (Parity):** 无 (None)
- 数据位 (Data Bits):** 8
- 停止位 (Stop Bits):** 1

At the bottom of the configuration area, there are two buttons: '保存设置' (Save Settings) and '取消设置' (Cancel Settings).

Use the external terminal cable to connect the USB to serial port cable, and then connect the device terminal port, as shown in the following figure:

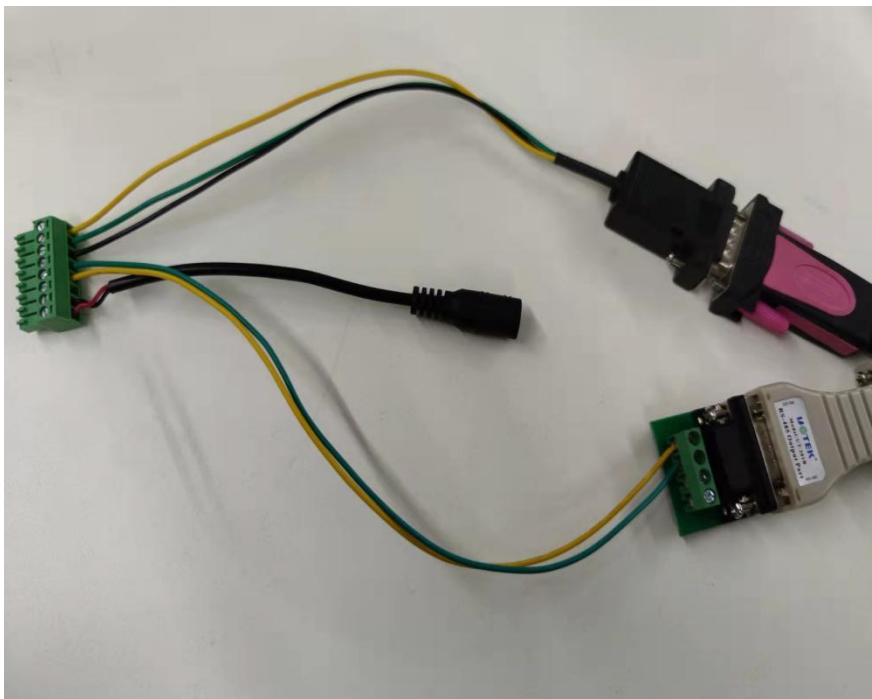


Figure 7-38

Terminal block 1(5PIN)			Terminal block 2		
1	DI1	INPUT	1	V+	Positive pole of power input
2	DI2	INPUT	2	V-	Negative pole of power input
3	GND	GND	3	GND	GND
4	DO1	OUTPUT	4	485A	485-A
5	DO2	OUTPUT	5	485B	485-B
			6	GND	GND
			7	TX	Serial port output
			8	RX	Serial port input

Table 7-4 Terminal Wiring Diagram

Step 3:

View the COM port information on the computer

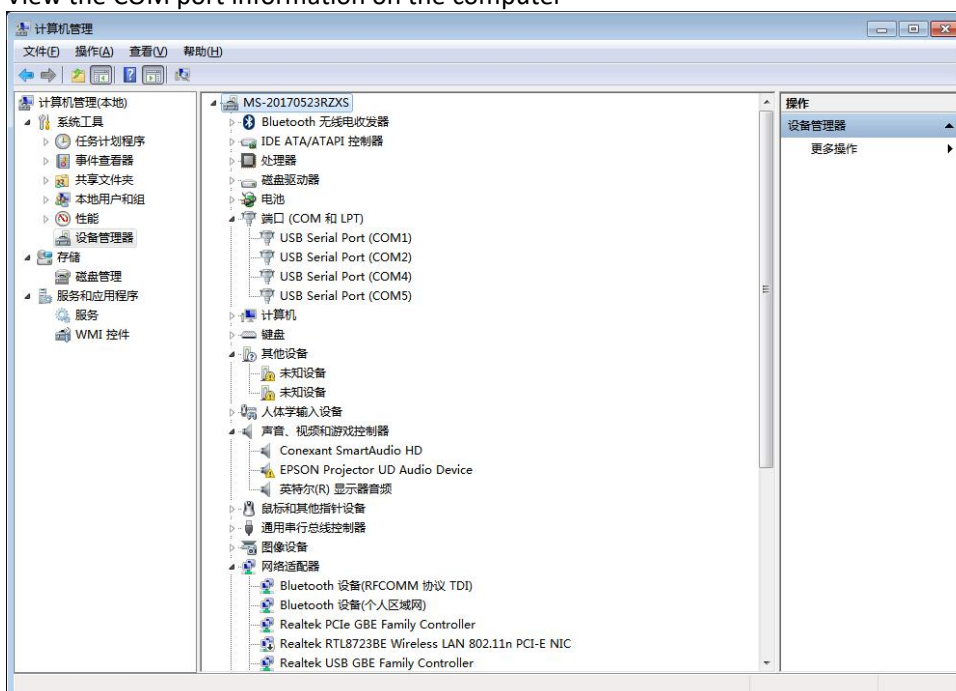


Figure 7-39 The COM port of a PC

Step 4:

Open the SSCOM tool and the TCP-UDP service management tool, select the TCP-UDP service management tool, select the server, host 192.168.1.2, port 40002, and click listen.

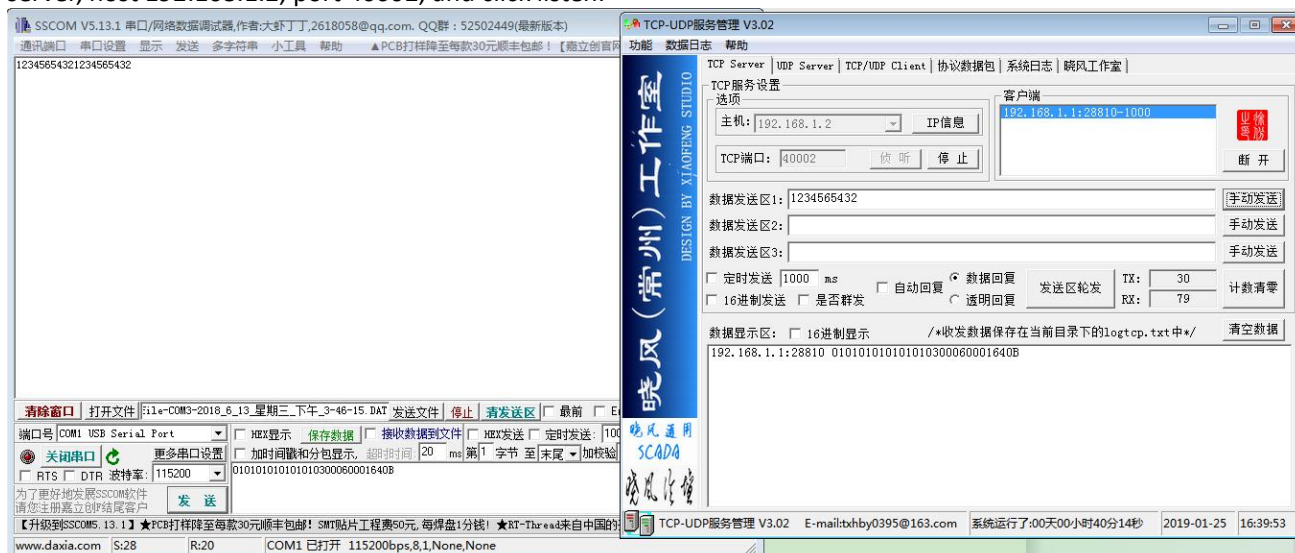


Figure 7-40 Data Transmission and Receiving

7.10. GPS settings

GPS (Global Positioning System) is used for the positioning of the geographical location of the device, which is generally used in conjunction with electronic maps and can be used to monitor moving vehicles or prevent theft.

Select "Advanced Network >GPS" in the navigation bar. In the page that opens, you can modify the relevant parameters of the configuration GPS setting function.

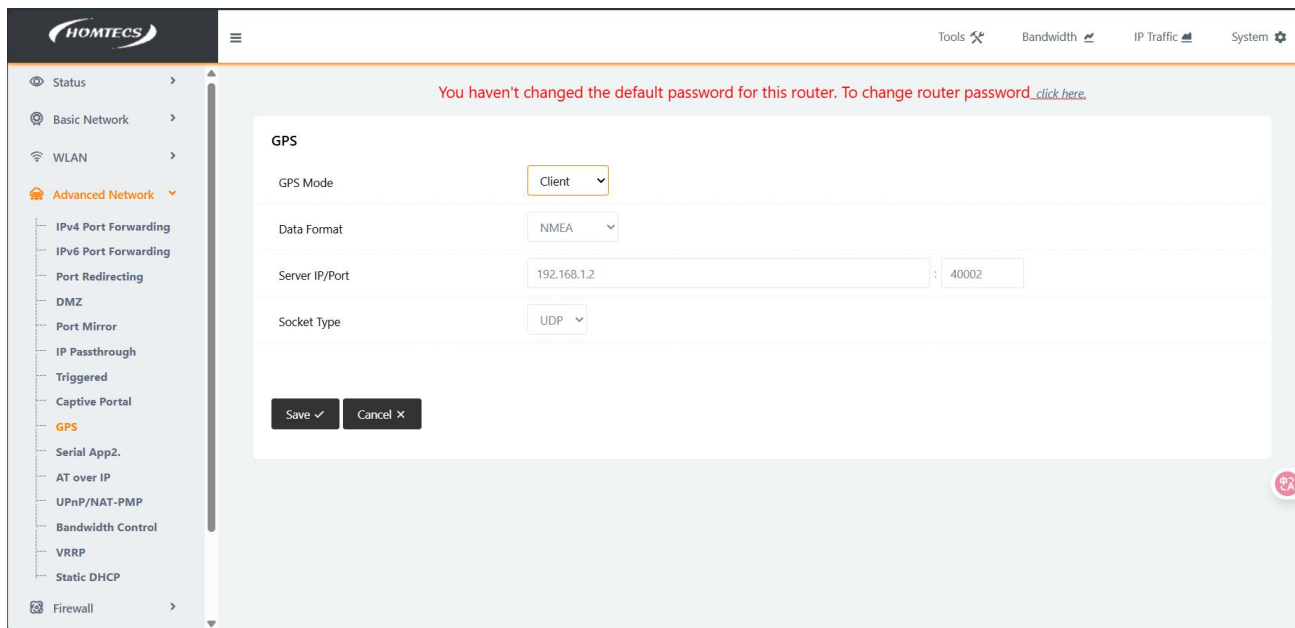


Figure 7-41

After the configuration is complete, click the Save Settings button for the configuration to take effect.

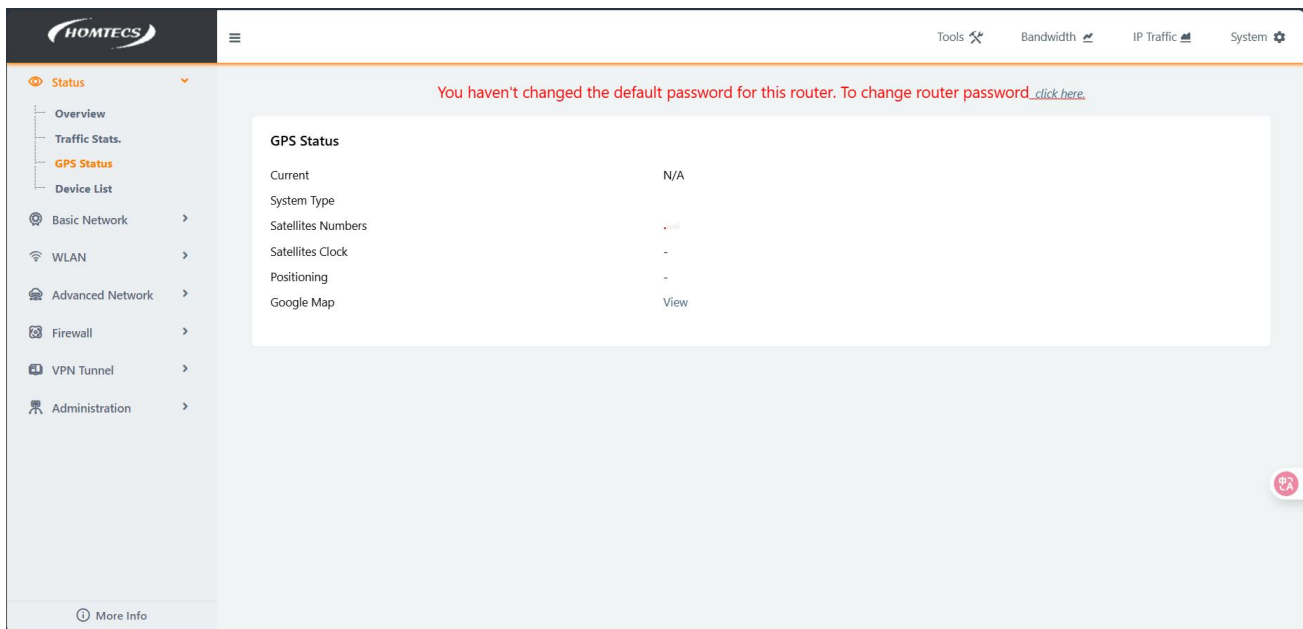


Figure 7-42

After the configuration is completed, the number of captured satellites, satellite time, and longitude and latitude information will be displayed in the GPS satellite status in the above figure. If the router is connected to the Internet, you can click the [Google Maps View] button to view the current location from the map.

Example of GPS setup:

Step 1:

Open the routing web interface, select GPS settings in Advanced Network, select Client for GPS network mode, and then click Save Settings.

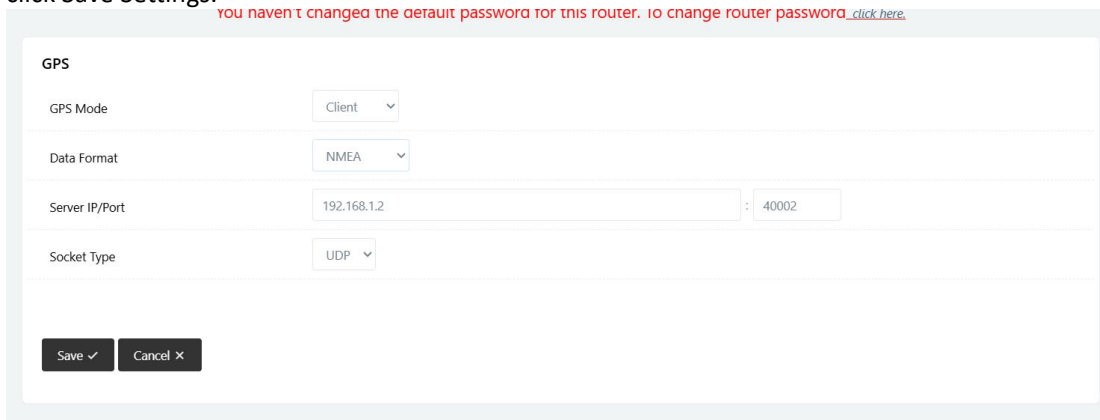


Figure 7-43 GPS configuration

Step 2:

Click GPS status in the system status to view the current GPS star search number and online status, as shown in the following figure:

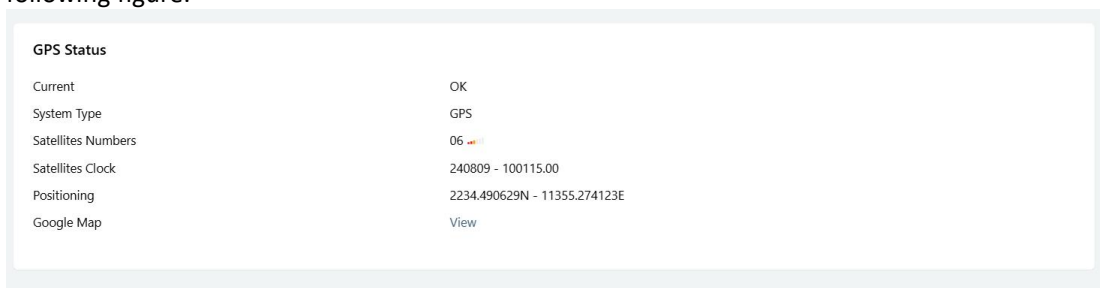


Figure 7-45 GPS status display

Step 3:

Open the sokit tool, select the server, the UDP address is 192.168.1.2, the port is 40002, click UDP listening, and you can receive the client data of GPS, as shown in the following figure.

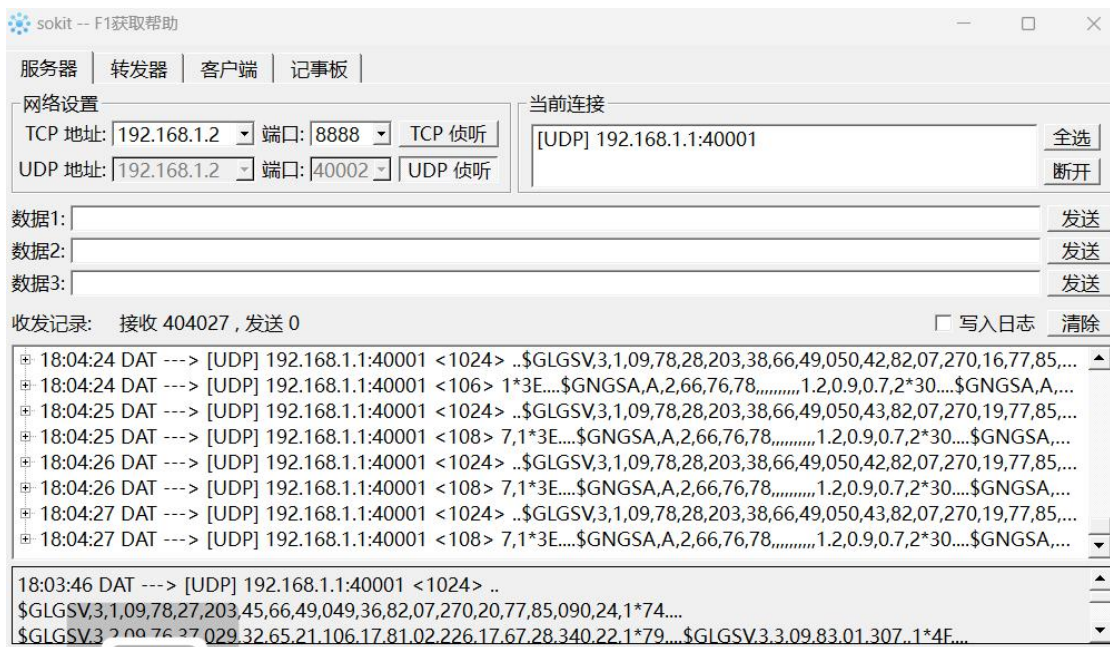


Figure 7-46 TCP-UDP receives GPS packets

Example of GPS tracks:

Step 1:

Click the router web interface, select the GPS settings in the advanced network, select the client for the GPS network mode, select the M2M_FMT for the data format, set the central host address to 120.78.189.220, port 6001, and the link heartbeat packet content is G51, click Save

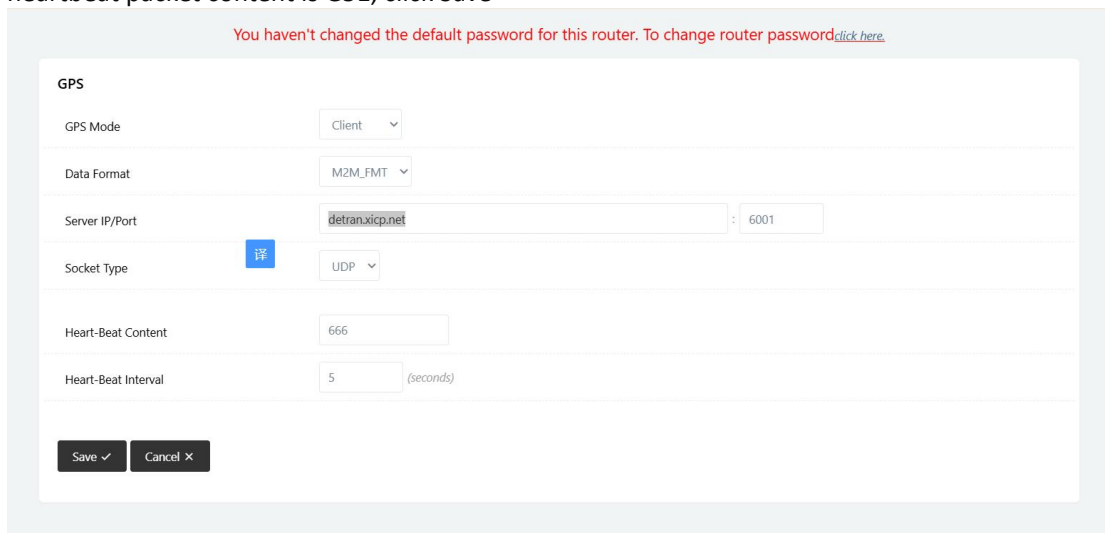


Figure 7-47 GPS configuration

Step 2:

Click M2M platform management in the system, enable M2M platform management, configure the M2M platform server to detran.xicp.net, set the port to 6000, and click Save settings

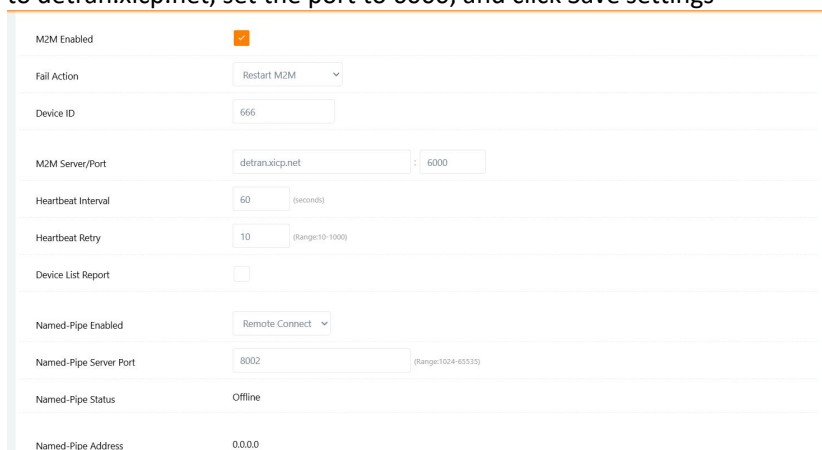


Figure 7-48 M2M Platform Management Settings

Step 3:

Log in to the Dechuan 3.0 platform <http://detran.xicp.net/m2m3.0>, view the serial number of the device, then copy the serial number, open the map information, paste the serial number in the search box, and click search to search for the movement track of the device, as shown in the figure below

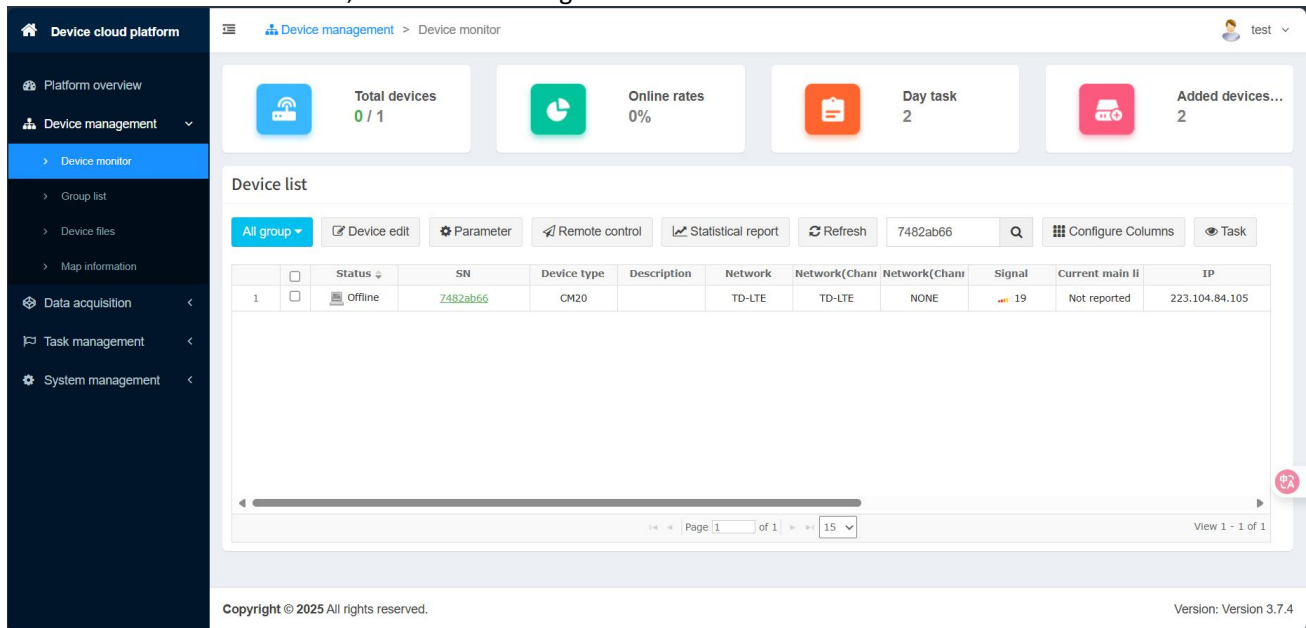


Figure 7-49

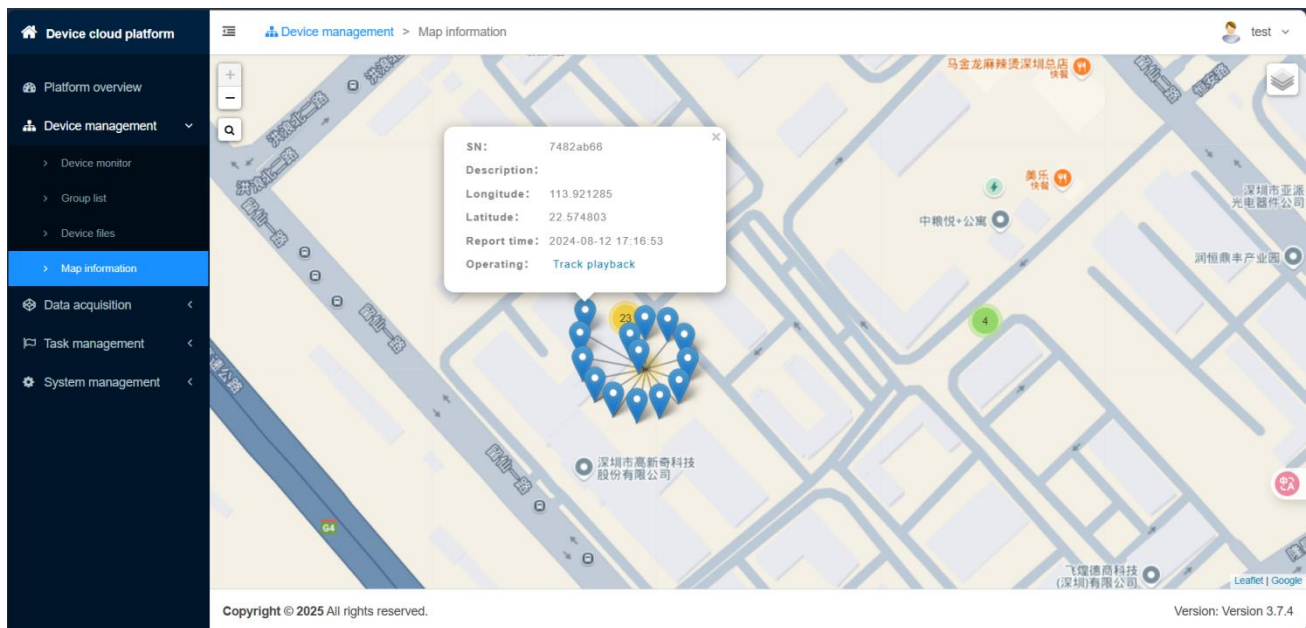


Figure 7-50 Platform device trajectory display

7.11. UPnP/NAT-PMP

Universal Plug and Play (UPnP) is universal plug and play, and cannot be simply understood as UPnP = "automatic port mapping". For an intranet computer, the UPnP function enables the NAT module of the gateway or router to do automatic port mapping, and the listening port is mapped from the gateway or router to the intranet computer. The network firewall module of the gateway or router starts opening this port to other computers on the Internet.

Step 1: Select "Advanced Network > UPnP/NAT-PMP" in the navigation bar. On the page that opens, you can modify the parameters for configuring UPnP.

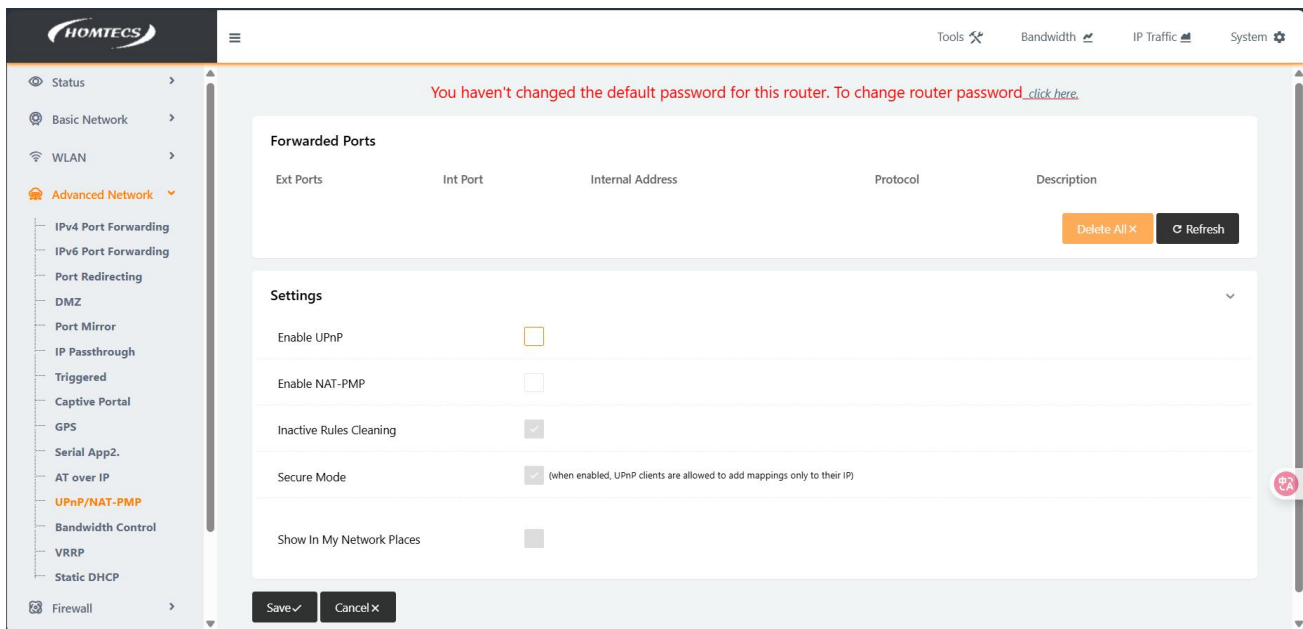


Figure 7-51

In the navigation bar, select Advanced Network >UPnP Settings. On the page that opens, you can modify the parameters related to configuring the UPnP setting function.

After the configuration is complete, click the Save Settings button for the configuration to take effect.

7.12. Bandwidth Control

Bandwidth Control can be used to provision network traffic, and some applications can bring convenience to users while taking up a large amount of network bandwidth. In order to ensure that all users in the LAN can use the network normally, you can use the bandwidth rate limiting function to limit the traffic of the specified host in the LAN.

Step 1: Select "Advanced Network > Bandwidth Control" in the navigation bar. On the page, you can modify the parameters for configuring bandwidth rate limiting.

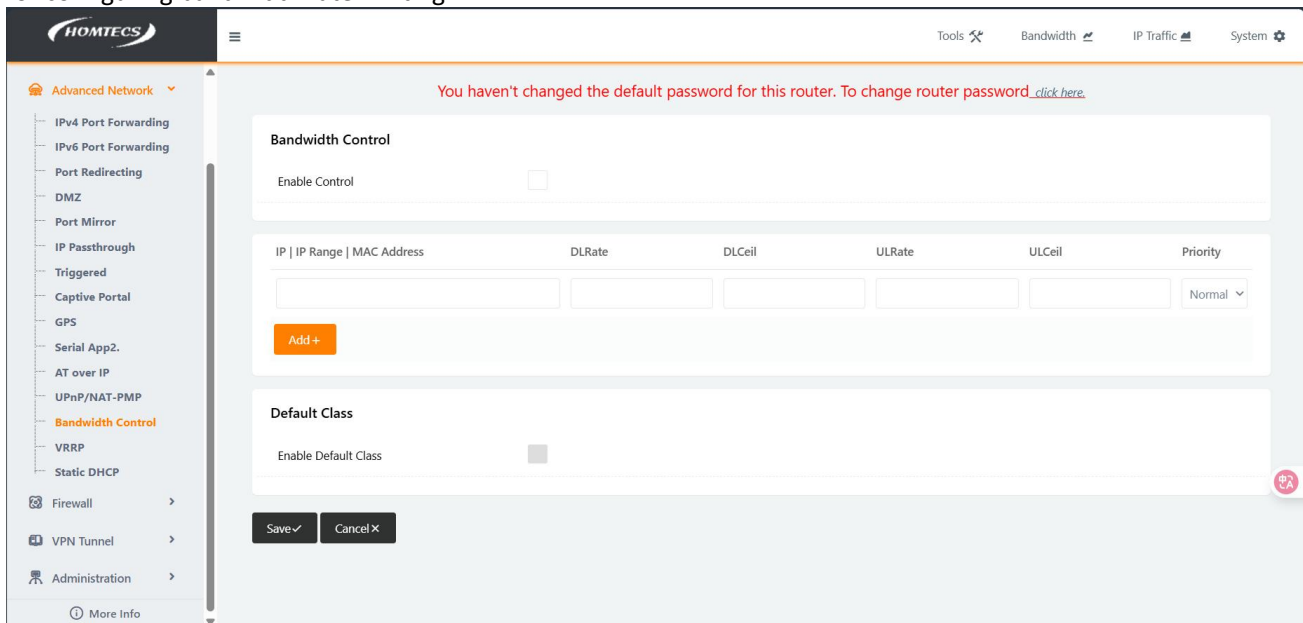


Figure 7-52

Bandwidth throttling example:

Step 1:

Open the web interface of the router, select Bandwidth Rate Limiting in Advanced Network, and enable Rate Limiting. The total download and total upload speed is 20000; The IP address is set to 192.168.1.2, and the download rate, maximum download rate, and upload rate are set to 8000. When you're done, click Save settings.

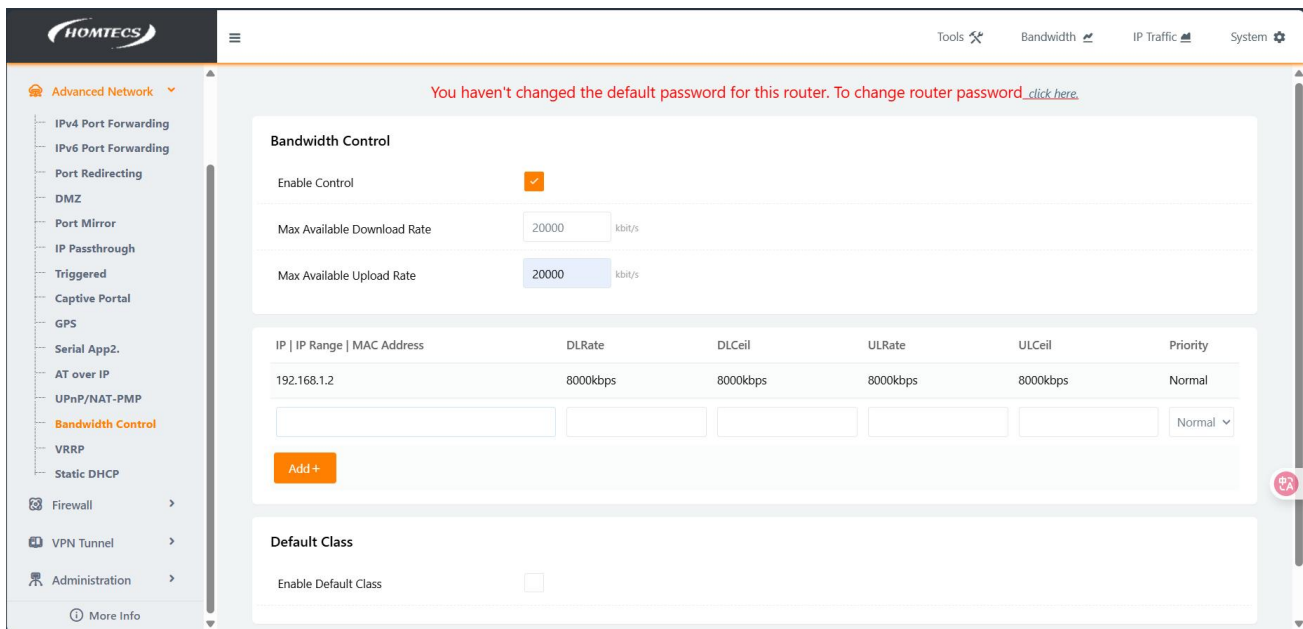


Figure 7-53 Bandwidth rate limiting configuration

Step 2:

Set the local connection on the PC side, the IP address is 192.168.1.2, the subnet mask is 255.255.255.0, and the default gateway is 192.168.1.1 (Note: The PC is supplied by the router, and the WiFi needs to be disconnected)

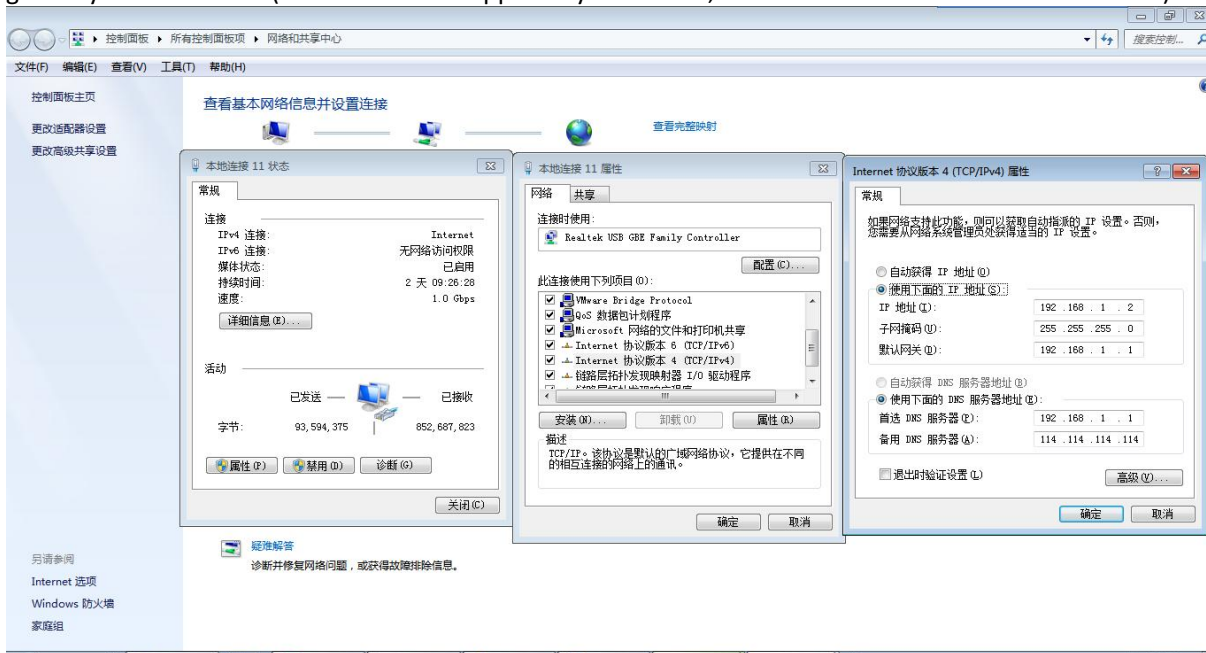


Figure 7-54 PC Local Connection Configuration

Step 3:

After opening the speed test URL of the <https://www.speedtest.net/zh-Hans> on the computer, click GO, the result is as follows, and the speed of the bandwidth is limited to less than 8000

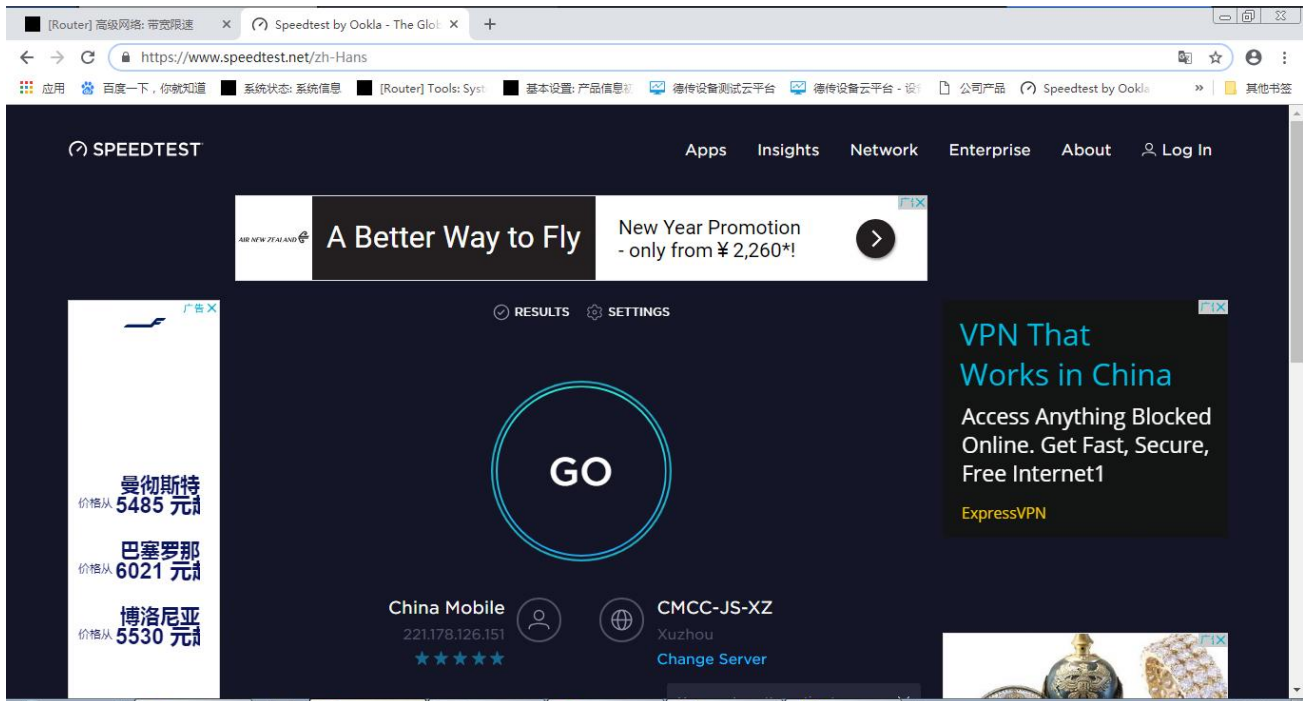


Figure 7-55



Figure 7-56 Speed test on the web interface

7.13. VRRP

Virtual Router Redundancy Protocol (VRRP) is a routing protocol proposed by the IETF to solve the phenomenon of single point failure of static gateways configured in local area networks, and a formal RFC2338 protocol standard has been launched in 1998. VRRP is widely used in edge networks, and its design goals are to support the transfer of IP data traffic failures without confusion in certain situations, to allow hosts to use a single router, and to maintain connectivity between routers in the event of a failure of the actual first-hop router.

Step 1: Select "Advanced Network > VRRP" in the navigation bar. On the page that appears, you can modify the parameters for configuring VRRP.

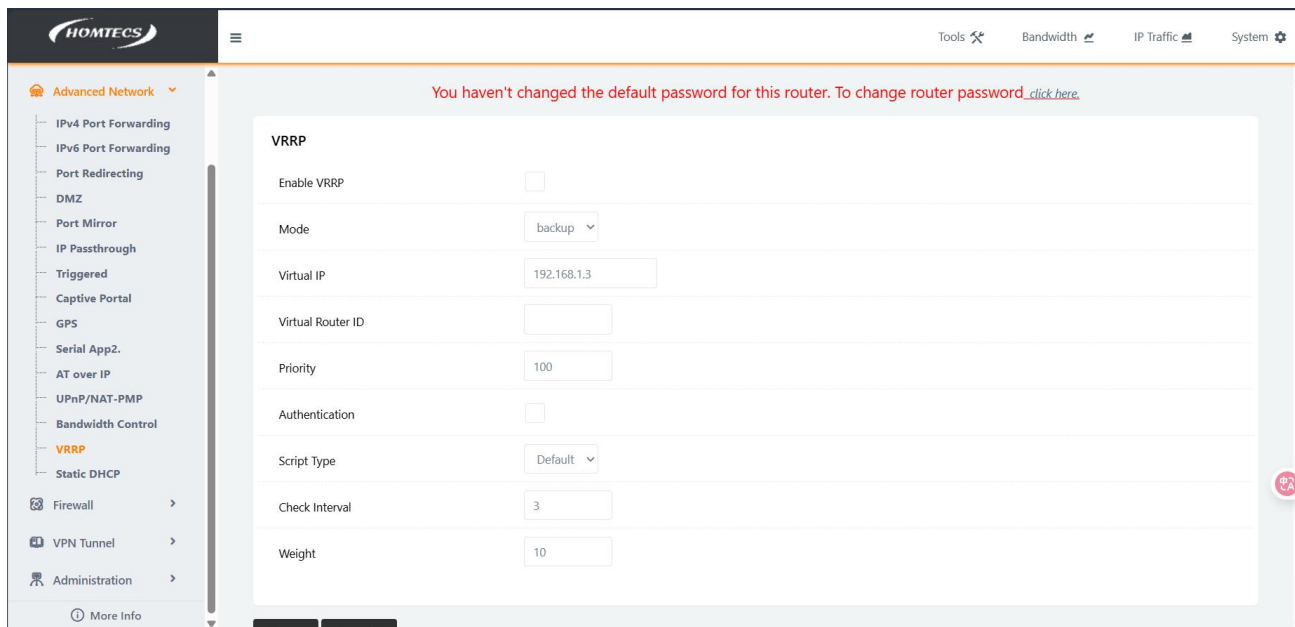


Figure 7-57

Example VRRP configuration:

1. The MAC addresses of the primary router and the standby router cannot be the same
2. Priority: The priority of the primary router is higher than that of the secondary
3. router Virtual IP address and virtual router ID: The two devices are set to be the same
4. Script type, detection interval, and weight: At present, ICMP detection is the detection of ICMP, which is to periodically ping an address to check whether the network is normal

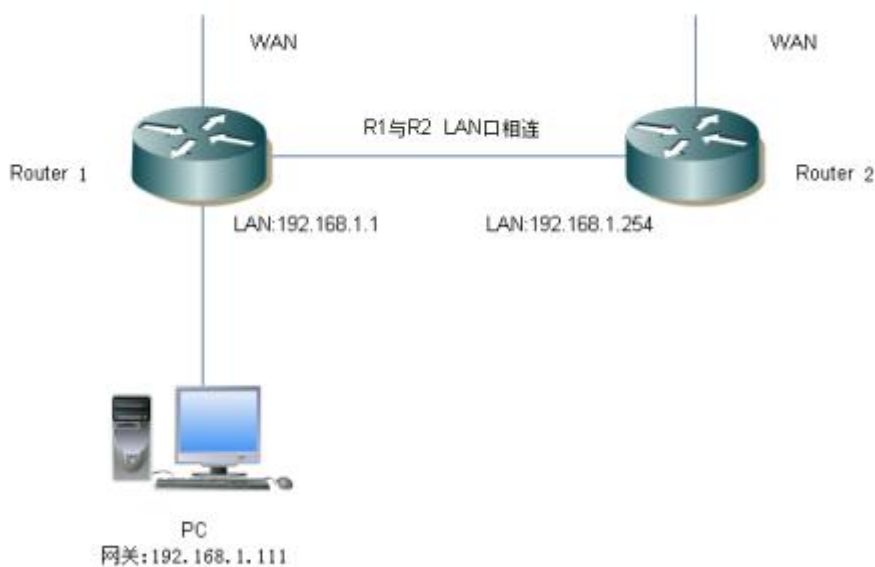


Figure 7-58 VRRP networking diagram

Primary Route Configuration (Router1).

Step 1:

LAN Configuration (Primary Routing Gateway is still 192.168.1.1)

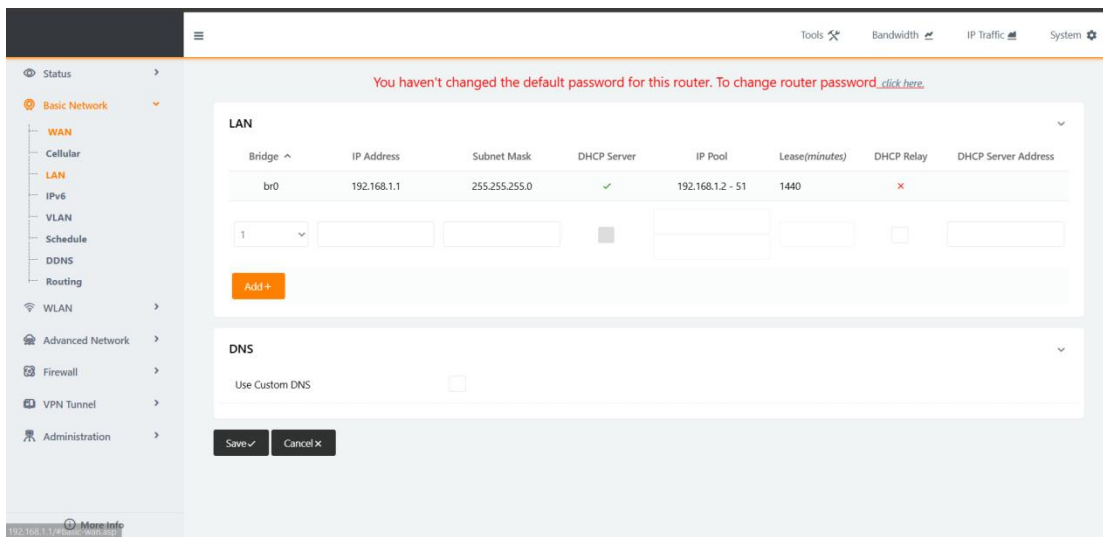


Figure 7-59 Local Area Network

Step 2:

In the navigation bar, select “Basic Network > WAN”. On the page, select a static address from the drop-down box, configure the parameters of the static address, and click Save Settings. As shown in the figure below (Note: the configuration of measurement parameters is an example, and the actual configuration needs to be configured according to the site conditions):

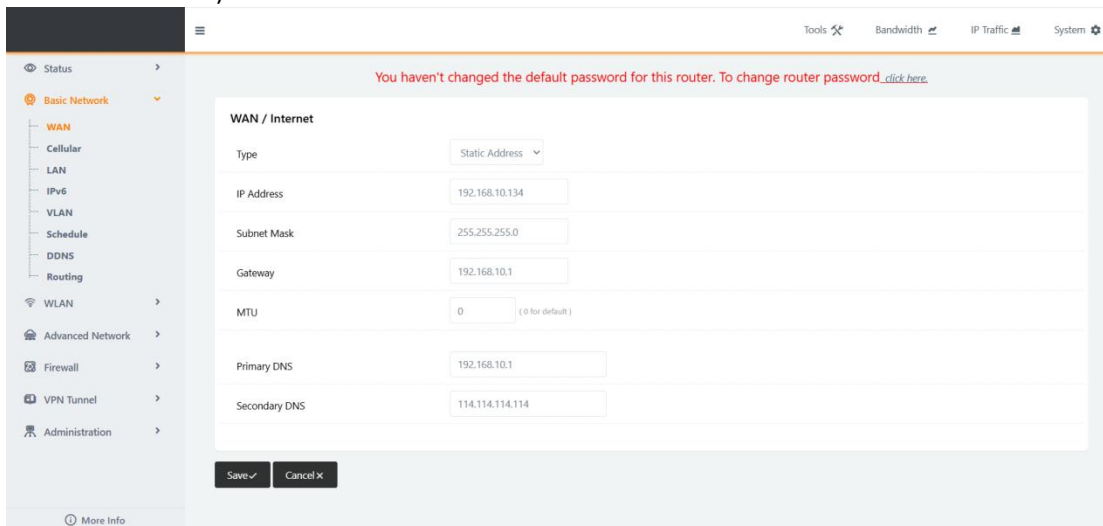


Figure 7-60 Static address settings

Step 3:

In the navigation bar, select Basic configuration > mobile networks. On the page that opens, uncheck the Enable module (Note: it is checked by default) and click Save Setting

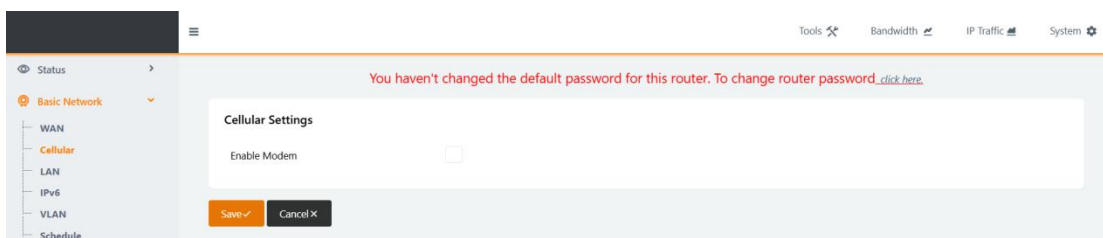


Figure 7-61 Mobile Network Settings

Step 4:

① In the navigation bar, select Basic Configuration > VLAN. In the page that opens, remove the WAN with VID1 checked, and click OK, as shown in the image:

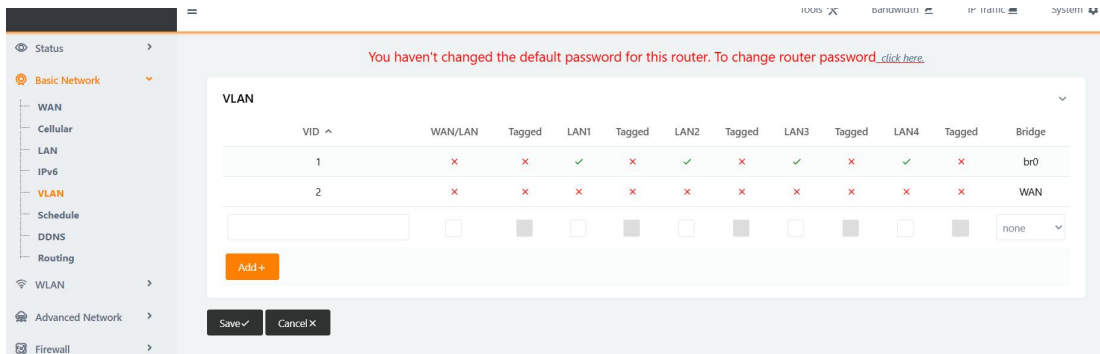


Figure 7-62 VLAN Setting

② In the VLAN page, add VID2, check WAN, click OK, and click Save Settings after the settings are completed, as shown in the figure

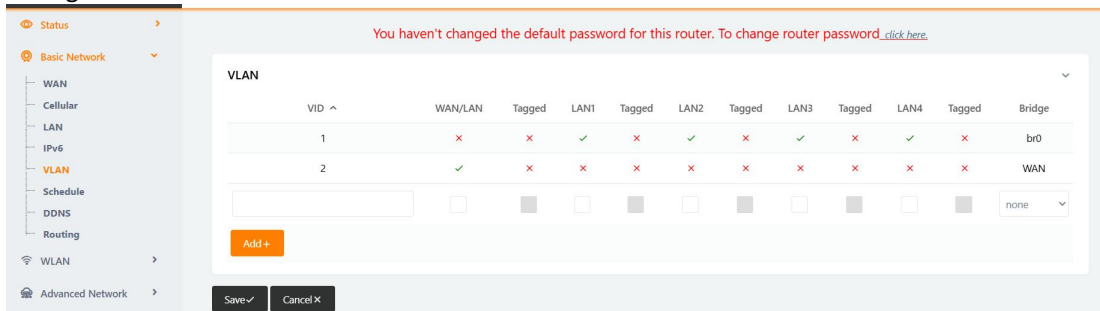


Figure 7-63 VLAN Settings

Step 5:

Configure VRRP and set the virtual IP address to 192.168.1.111 and set the same as the primary and standby THE ADDRESS IS: THE ADDRESS TO BE PINGED BY ICMP

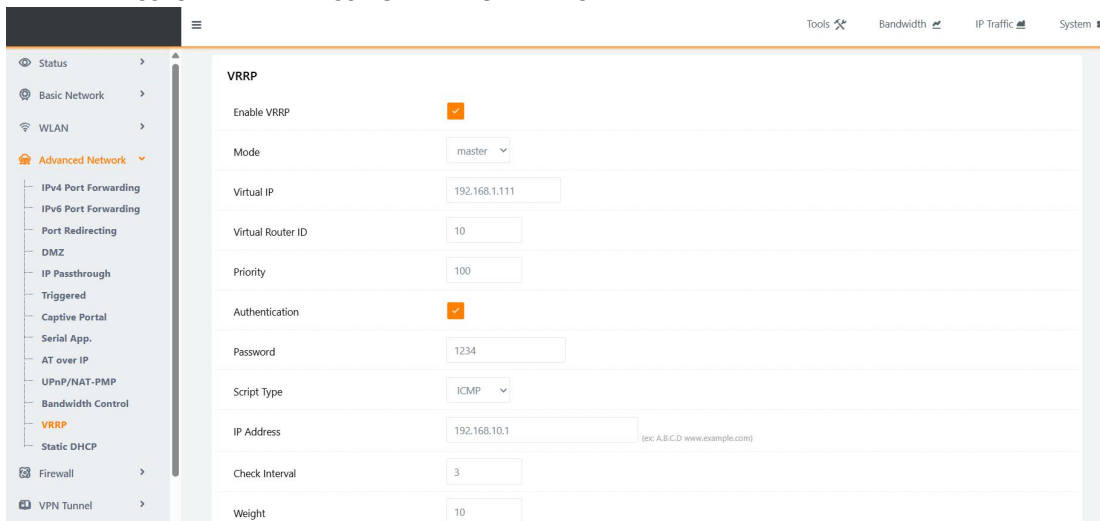


Figure 7-64 VRRP settings for the primary route

Step 6:

Select one of the active and standby computers to connect to the PC, and manually configure the address The following figure shows the configuration when the PC connects to the "main route", note: the gateway cannot write 192.168.1.1, but the virtual gateway address 192.168.1.111

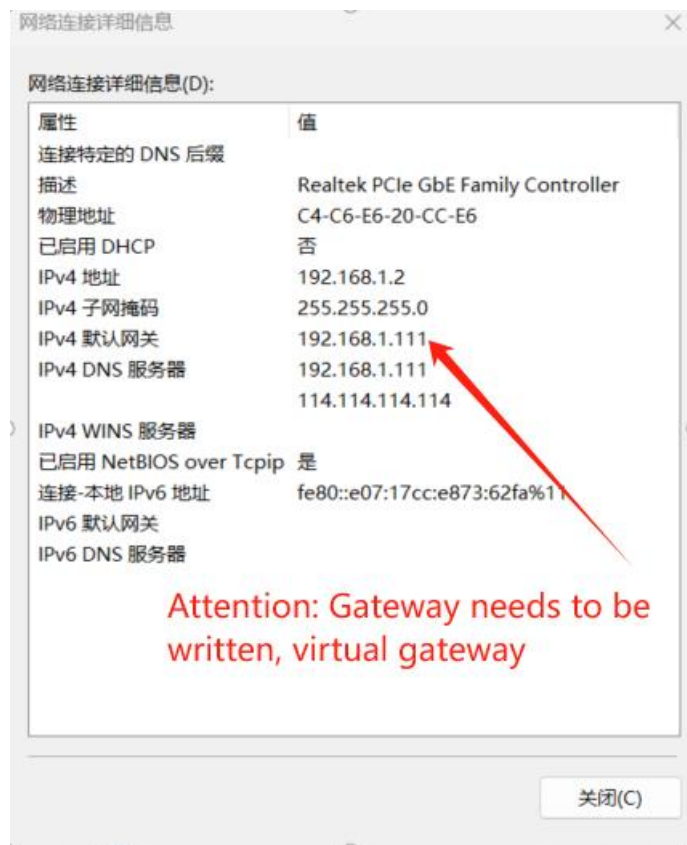


Figure 7-65 PC Local Connection Settings

Standby route configuration (Router2).

Step 1:

LAN Configuration (Changed to 192.168.1.254 for Standby Route Gateway)

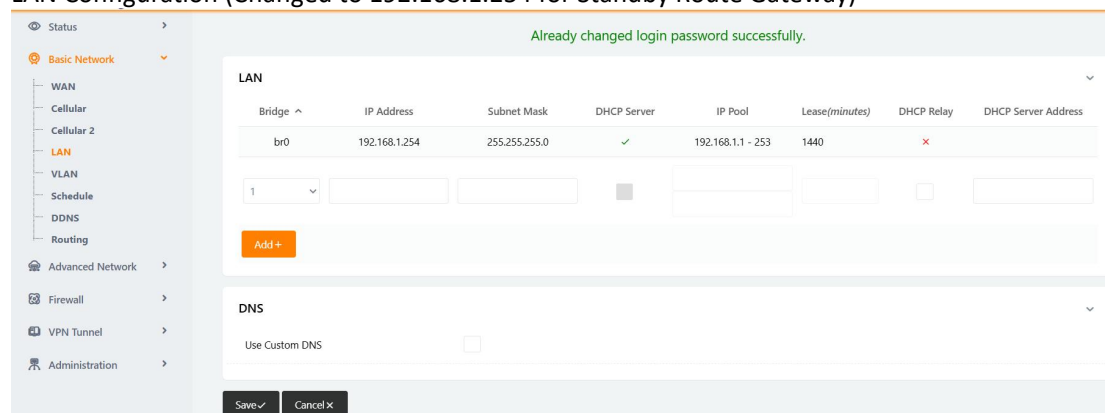


Figure 7-66 Standby LAN

Step 2:

In the navigation bar, select "Basic Network > WAN". On the page, select a static address from the drop-down box, configure the parameters of the static address, and click Save Settings. As shown in the figure below (Note: the configuration of measurement parameters is an example, and the actual configuration needs to be configured according to the site conditions):

Figure 7-67 Static address settings

Step 3:

In the navigation bar, select “Basic Network > Cellular”. On the page, uncheck the Enable module (Note: it is checked by default) and click Save Settings

Figure 7-68 Mobile Network Setup

Step 4:

① In the navigation bar, select “Basic Network > VLAN”. On the page, remove the WAN with VID1 checked, and click OK, as shown in the image:

VID ^	WAN/LAN	Tagged	LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
1	×	×	✓	×	×	×	×	×	×	×	br0
2	×	×	×	×	×	×	×	×	×	×	WAN

Figure 7-69 VLAN Settings

② In the VLAN page, add VID2, check WAN, click OK, and click Save Settings after the settings are completed, as shown in the figure

VID ^	WAN/LAN	Tagged	LAN1	Tagged	LAN2	Tagged	LAN3	Tagged	LAN4	Tagged	Bridge
1	×	×	✓	×	×	×	×	×	×	×	br0
2	✓	×	×	×	×	×	×	×	×	×	WAN
3											none

Figure 7-70 VLAN Setup

Step 5:

Configure the VRRP function for the standby route, as shown in the following figure

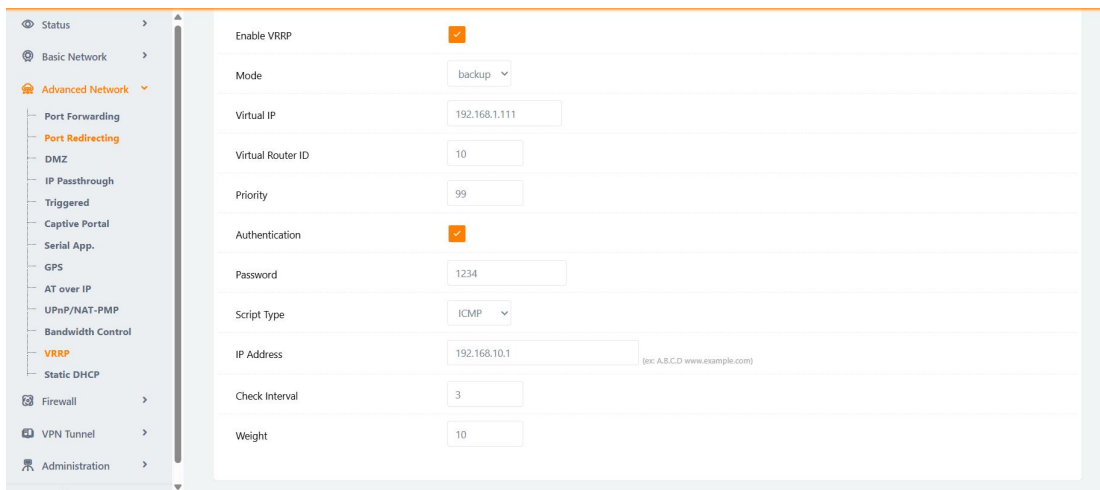


Figure 7-71 VRRP configuration of the standby route (R2).

❖ outcome

Instruction 1: `arp -d;`

Instruction 2: `arp -a----` to see which MAC address 192.168.1.111 matches with indicates which device provides the network

Phase 1: When both the active and standby WAN ports are present, the primary device (entering MASTER start) provides the network by default.

Phase 2: After the WAN port of the primary device is unplugged, the WAN port of the primary device will be switched to the secondary device (entering backup start) to provide the network.

Phase 3: After the WAN port of the master device is re-inserted, it switches to the main device (entering MASTER start) to provide the network.

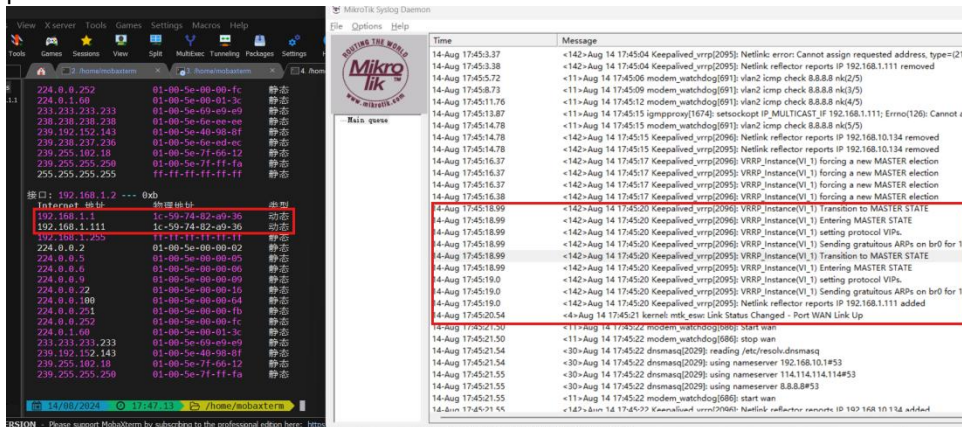


Figure 7-72: Both the primary and standby WAN ports are present

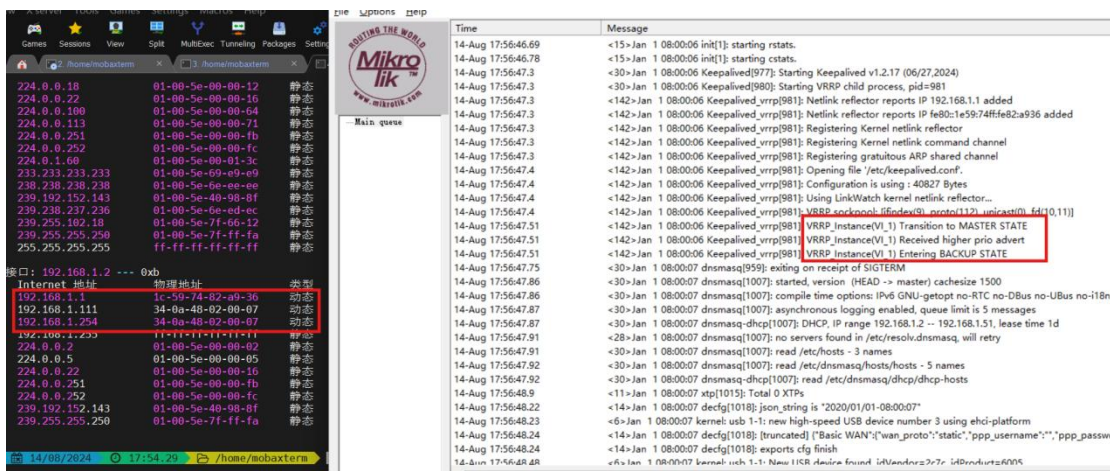


Figure 7-73: Unplug the WAN port of the primary device

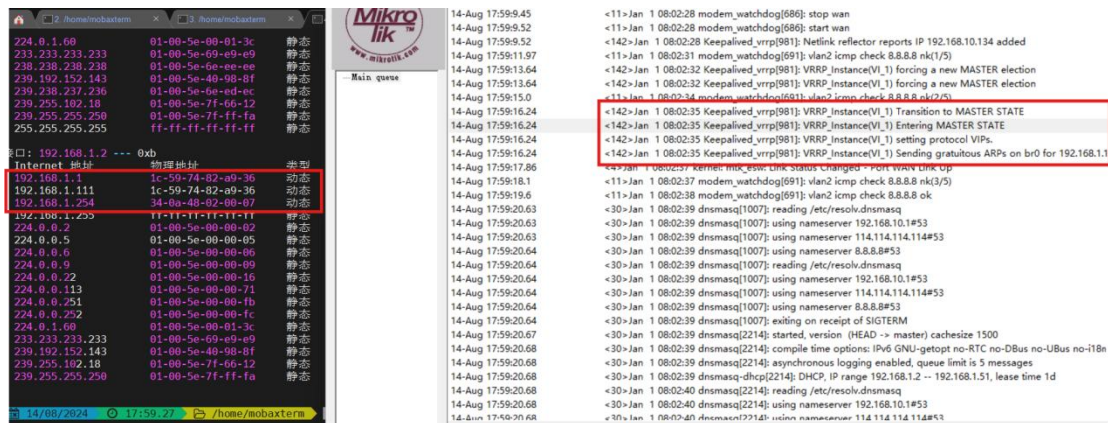


Figure 7-74 Replug the WAN port back into the main device

7.14. Static DHCP

Dynamic Host Configuration Protocol (DHCP) is a network protocol for local area networks. After the DHCP function is enabled, the lower computer can automatically obtain the dynamic IP.

Step 1: Select "Advanced Network > Static DHCP" in the navigation bar. On the page that opens, you can modify the parameters for configuring the static DHCP function.

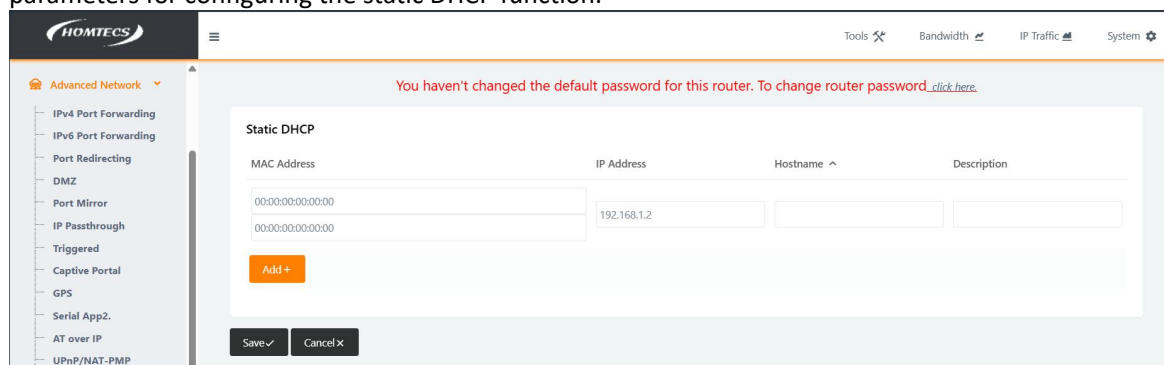


Figure 7-75

Step 2: Configure "DHCP Server Settings" The DHCP server settings parameters are shown in the table

The name of the parameter	meaning	How to configure
DHCP services	DHCP Service Enable button to enable/disable DHCP Service	button to select Settings: Enabled Disable
MAC	Configure the MAC address of the DHCP client that needs to specify the IP address of the DHCP acquisition IP	WORD TYPE MAC FORMAT For example, 00:1A:4D:34:B1:8E

Table 7-6 DHCP Server Settings

Step 3: Once the configuration is complete, click the "Save Settings" button for the configuration to take effect.

Static DHCP configuration example:

Step 1:

Open the administrator: Command prompt (shortcut key win+R), enter cmd; Then enter ipconfig/all to find the MAC address of the local connection

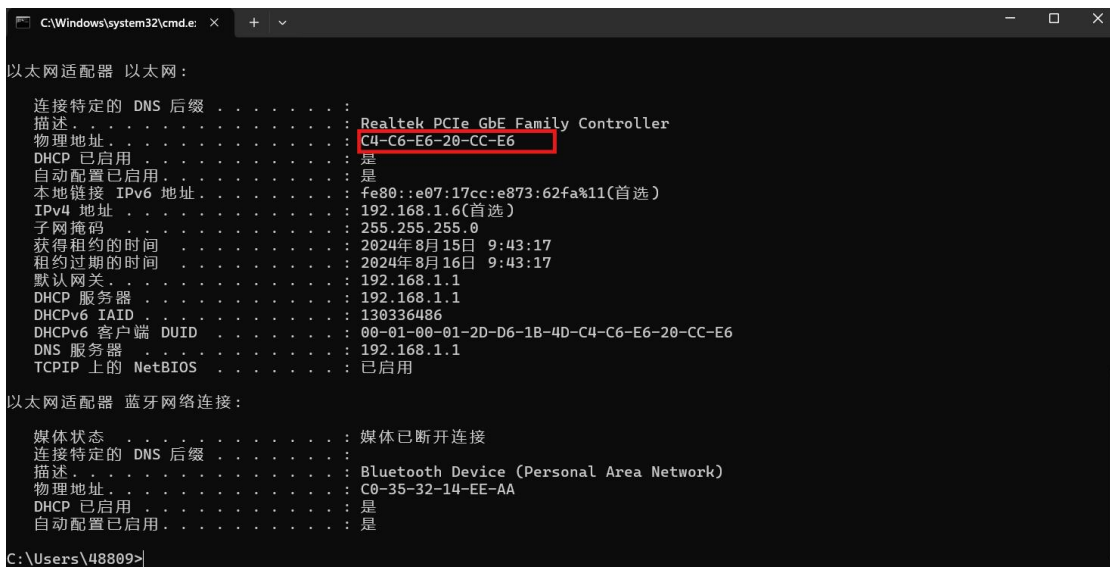


Figure 7-76 Administrator

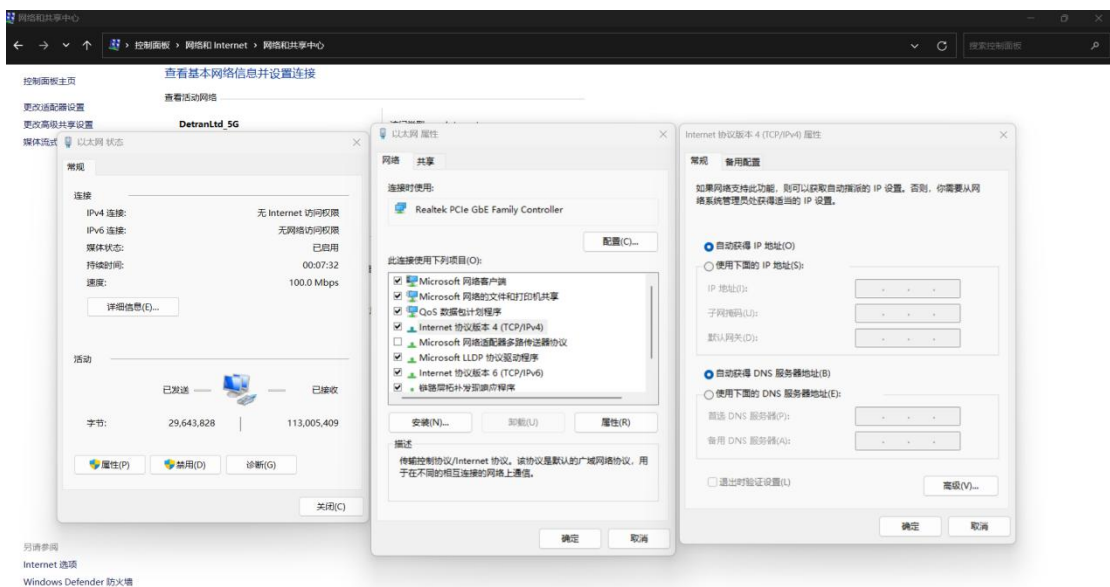


Figure 7-77 Automatic DHCP is enabled on the PC

Step 3:

Open the routing web interface, select static DHCP in the advanced network, and configure the MAC address (**Note: the MAC address filled in here is the MAC address queried in step 1**), the first of the two MAC address items can be set, and the second can be left unset, save the settings after the addition is completed

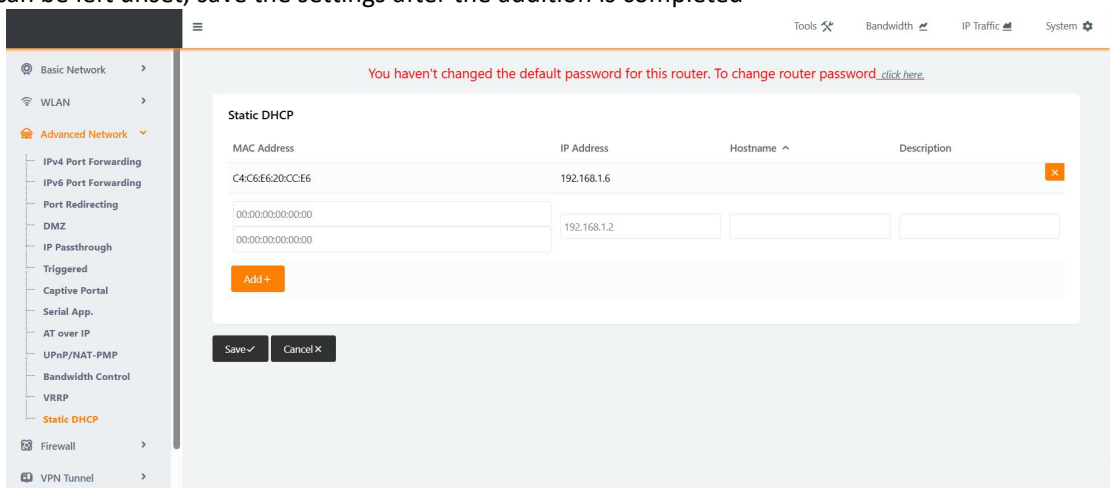


Figure 7-78 Static DHCP settings

Step 4:

Open the network and sharing center of the PC to view the details, and the IP address of the PC is the same as the

statically bound address (Note: If multiple PCs are bound, follow the method in step 1 to add the MAC address).

```
15/08/2024 10:16:51 /home/mobaxterm ifconfig

Software Loopback Interface 1
Link encap: Local loopback
inet addr:127.0.0.1 Mask: 255.0.0.0
MTU: 1500 Speed:1073.74 Mbps
Admin status:UP Oper status:OPERATIONAL
RX packets:0 dropped:0 errors:0 unkown:0
TX packets:0 dropped:0 errors:0 txqueuelen:0

Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
Link encap: IEEE 802.11 HWaddr: C0-35-32-14-EE-A9
inet addr:192.168.31.169 Mask: 255.255.255.0
MTU: 1500 Speed:1201.00 Mbps
Admin status:UP Oper status:OPERATIONAL
RX packets:819364 dropped:0 errors:0 unkown:0
TX packets:81267 dropped:0 errors:10 txqueuelen:0

Realtek PCIe GbE Family Controller
Link encap: Ethernet HWaddr: C4-C6-E6-20-CC-E6
inet addr:192.168.1.6 Mask: 255.255.255.0
MTU: 1500 Speed:100.00 Mbps
Admin status:UP Oper status:OPERATIONAL
RX packets:169204 dropped:0 errors:0 unkown:0
TX packets:133974 dropped:0 errors:148 txqueuelen:0
```

Figure 7-79 Binding static DHCP

8. Firewall

A firewall refers to a method of separating an intranet from a public access network, such as the Internet, and is an isolation technique. A firewall is an access control that is performed when two networks are in communication, allowing you to "consent" to data entering your network while keeping out data that you "deny", preventing hackers from accessing your network to the greatest extent.

8.1. IP/URL Filtering

The IP filtering module filters the incoming and outgoing IP packets based on the source address, destination address, port number, and other information in the headers of the IP packets, and allows or disables access to certain IP addresses.。

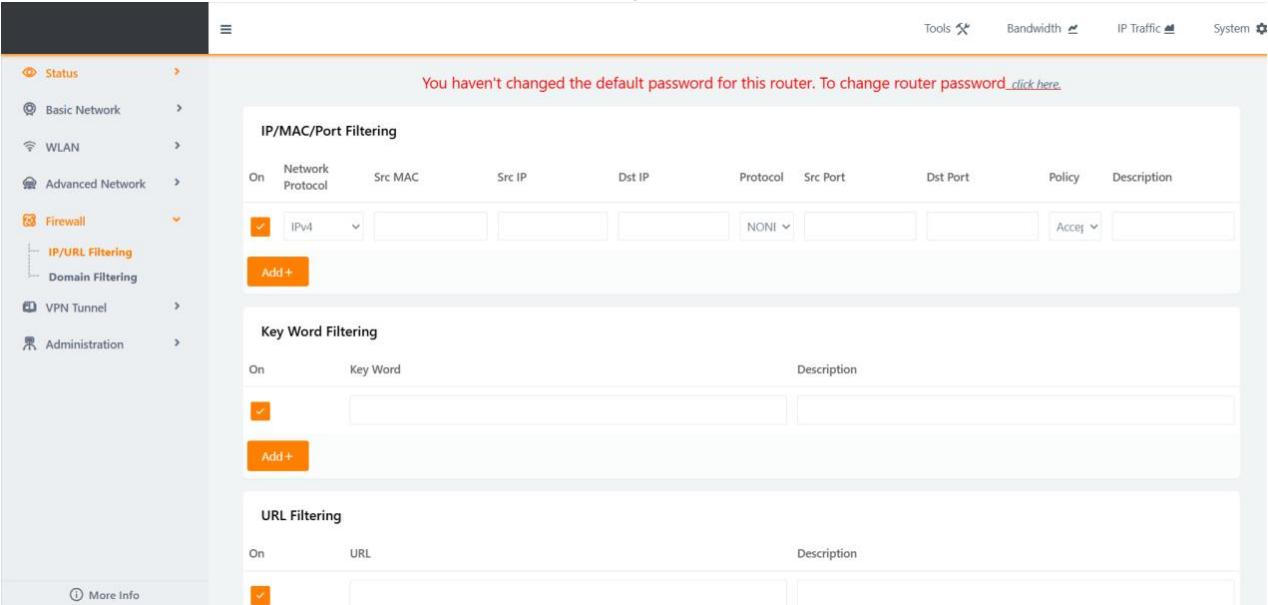


Figure 8-1

Example 1: Only one IP address is prohibited from accessing the Internet, and other IP addresses are allowed

IP/MAC/Port Filtering

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	IPv4	-	192.168.1.6	any/0	-	-	-	Drop	

☒ IPv4

 NONI

 Accept

Add +

Figure 8-2

As shown in Figure 8-2, if you configure a source IP address and select Discard as a policy, the IP address cannot access the Internet and other IP addresses can access the Internet normally

Example 2: Only one IP address is allowed to access the Internet, and others are prohibited

IP/MAC/Port Filtering

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	IPv4	-	any/0	any/0	-	-	-	Drop	
✓	IPv4	-	192.168.1.6	any/0	-	-	-	Accept	
✓	IPv4	-	any/0	192.168.1.6	-	-	-	Accept	

☒ IPv4

 NONI

 Accept

Add +

Figure 8-3

As shown in Figure 8-3, discard all IP addresses and MAC addresses, and then accept the source and destination of the specified IP address

Example 3: Only one MAC address is prohibited from accessing the Internet, and other addresses are allowed

IP/MAC/Port Filtering

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	IPv4	C4:C6:E6:20:CC:E6	any/0	any/0	-	-	-	Drop	

☒ IPv4

 NONI

 Accept

Add +

Figure 8-4

As shown in Figure 8-4, configure a source MAC address and select Discard as the policy

Example 4: Only one MAC address is allowed to access the Internet, and others are prohibited

IP/MAC/Port Filtering

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
✓	IPv4	-	any/0	any/0	-	-	-	Drop	
✓	IPv4	C4:C6:E6:20:CC:E6	any/0	any/0	-	-	-	Accept	
✓	IPv4	-	any/0	192.168.1.6	-	-	-	Accept	

☒ IPv4

 NONI

 Accept

Add +

Figure 8-5

As shown in Figure 8-5, the first one discards all IP addresses and MAC addresses, the second one accepts the specified MAC address, and the third one accepts the specified destination IP range

Example 5: Only one IP address is allowed, but others are forbidden

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	IPv4	-	any/0	any/0	-	-	-	Drop	<input type="text"/>
<input checked="" type="checkbox"/>	IPv4	-	any/0	192.168.1.6	-	-	-	Accept	<input type="text"/>
<input checked="" type="checkbox"/>	IPv4	-	192.168.1.6	any/0	-	-	-	Accept	<input type="text"/>

☒ IPv4

 NONE

 Accept

Add +

Figure 8-6

As shown in Figure 8-6, the first new source IP address and destination IP address can be discarded without entering the default IP address. Article 2 adds a designated destination IP for policy reception; Article 3 adds a designated source IP, and the policy selects to receive; After the configuration is saved, only 120.78.189.220 is allowed to be accessed, and other IP addresses cannot be accessed.

Example 6: Only one IP address is disallowed and others can be accessed

On	Network Protocol	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	IPv4	-	any/0	192.168.1.10	-	-	-	Drop	<input type="text"/>

☒ IPv4

 NONE

 Accept

Add +

Figure 8-7

As shown in Figure 8-7, the specified destination IP address is added and the policy is Discarded.

8.2. Keyword Filtering Settings / URL Filtering Settings / Access Filtering

1. Keyword filtering: Judge and filter the incoming and outgoing data of the keyword information configured by the user
2. URL filtering needs to filter the visited URLs according to the URLs and other information configured by the user
3. Access filtering needs to filter MAC, source IP, destination IP, port number and other information according to the user, and allow or prohibit access to certain IPs.

- Status
- Basic Network
- WLAN
- Advanced Network
- Firewall
 - IP/URL Filtering
 - Domain Filtering
- VPN Tunnel
- Administration

Tools Bandwidth IP Traffic System

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Add +

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Add +

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	NONE	<input type="text"/>	<input type="text"/>	Accept	<input type="text"/>

Add +

Figure 8-8

Example 1:

Key Word Filtering

On	Key Word	Description
<input checked="" type="checkbox"/>	baidu	
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Figure 8-9

Keyword filtering intercepts and discards the set content, does not support Chinese, spaces, numbers, English letters and symbols.

Example 2:

URL Filtering

On	URL	Description
<input checked="" type="checkbox"/>	www.jb1000.com/Article/Articleinfo.aspx?infoid=893923	http: //
<input checked="" type="checkbox"/>	www.wifilu.com/1666.html	https://
<input checked="" type="checkbox"/>	hlwksl.bokee.com/507180743.html	http: //
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Figure 8-10

URL filtering blocks and discards URLs and restricts only a URL address within a website.

Example 3:

Access filtering determines the IP protocol and port of the accessing router

Only certain IPs are allowed to access the device;

Access Filtering

On	Src MAC	Src IP	Dst IP	Protocol	Src Port	Dst Port	Policy	Description
<input checked="" type="checkbox"/>	-	any/0	any/0	-	-	-	Drop	
<input checked="" type="checkbox"/>	-	192.168.1.1	any/0	TCP	-	2323	Accept	
<input checked="" type="checkbox"/>	-	内部网络 192.168.1.6	any/0	TCP	-	80	Accept	
<input checked="" type="checkbox"/>	-	外部网络 13.107.139.11	any/0	TCP	-	80	Accept	
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	NONE	<input type="text"/>	<input type="text"/>	Accep	<input type="text"/>

Figure 8-11

8.3. Domain Filtering

Domain Filtering is a mechanism that allows certain domain names to be filtered for a specific range of domain names such as .com, .cn, .net, etc., allowing these domains to pass or not to pass.

Domain Filtering

On ☒

Default Policy

On	Domain	Description
<input checked="" type="checkbox"/>	www.baidu.com	
<input checked="" type="checkbox"/>	www.csdn.net	
<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Figure 8-12

For example, in Figure 8-12, configure blacklist domain name filtering, fill in www.qq.com and www.baidu.com respectively, PC only access the Internet through the router, PC can not access QQ and Baidu when opening the browser, but can access

other websites, on the contrary, the default policy is whitelist, then only access QQ and Baidu are allowed, and other websites cannot be accessed.

9. VPN configuration

Virtual Private Network (VPN) is a secure Internet-based local area network (LAN) that currently supports Wireguard/L2TP/PPTP/GRE/openvpn/IPSEC/L2TP V3/DMVPN are used separately.

9.1. Wireguard

WireGuard is an easy-to-configurable, fast, and secure open-source VPN that leverages the latest encryption technology. The goal is to provide a faster, simpler, and leaner general- purpose VPN that can be easily deployed on low-end devices like Raspberry Pi to high-end servers.

Since most other solutions like IPsec and OpenVPN were developed decades ago, realize that they are slow and difficult to configure and manage properly; Multi-platform support for Linux, Windows, macOS, BSD, iOS, and Android; Although wireguard is simple, it supports all the latest encryption technologies, such as the Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, and secure trusted fabrics; And because WireGuard runs in kernel space, it provides a secure network at high speeds.

Step 1: Select "VPN Tunnel >Wireguard" in the navigation bar as shown in the image, which contains both server and client modes

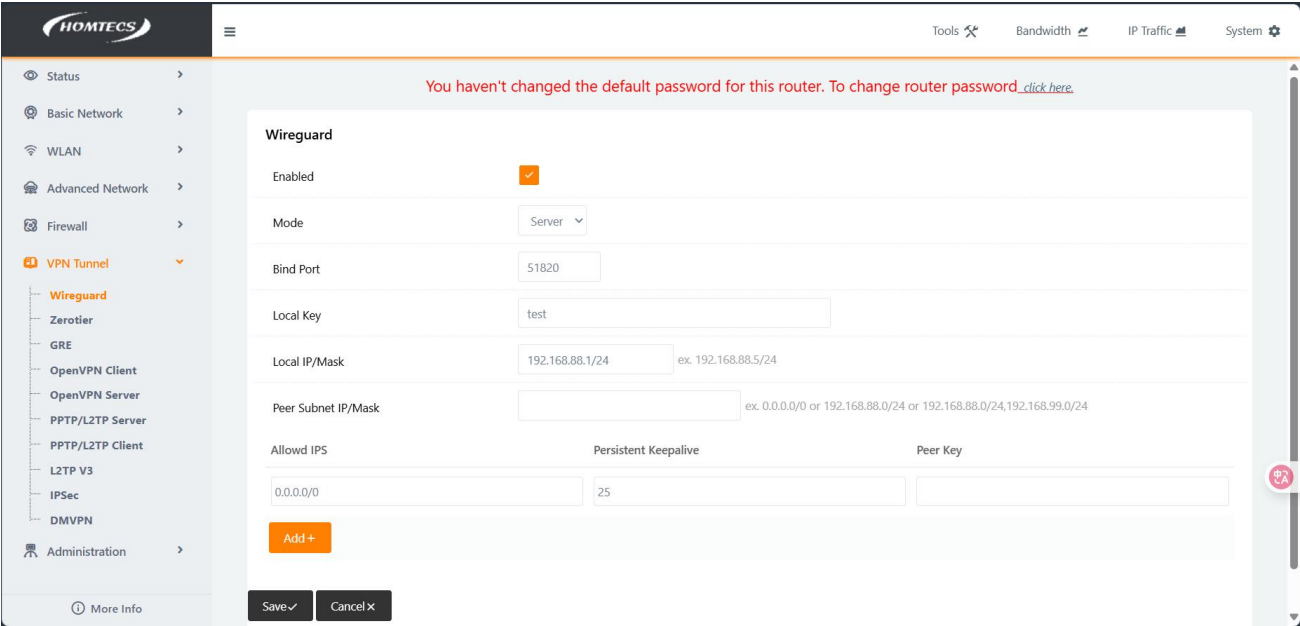


Figure 9-1

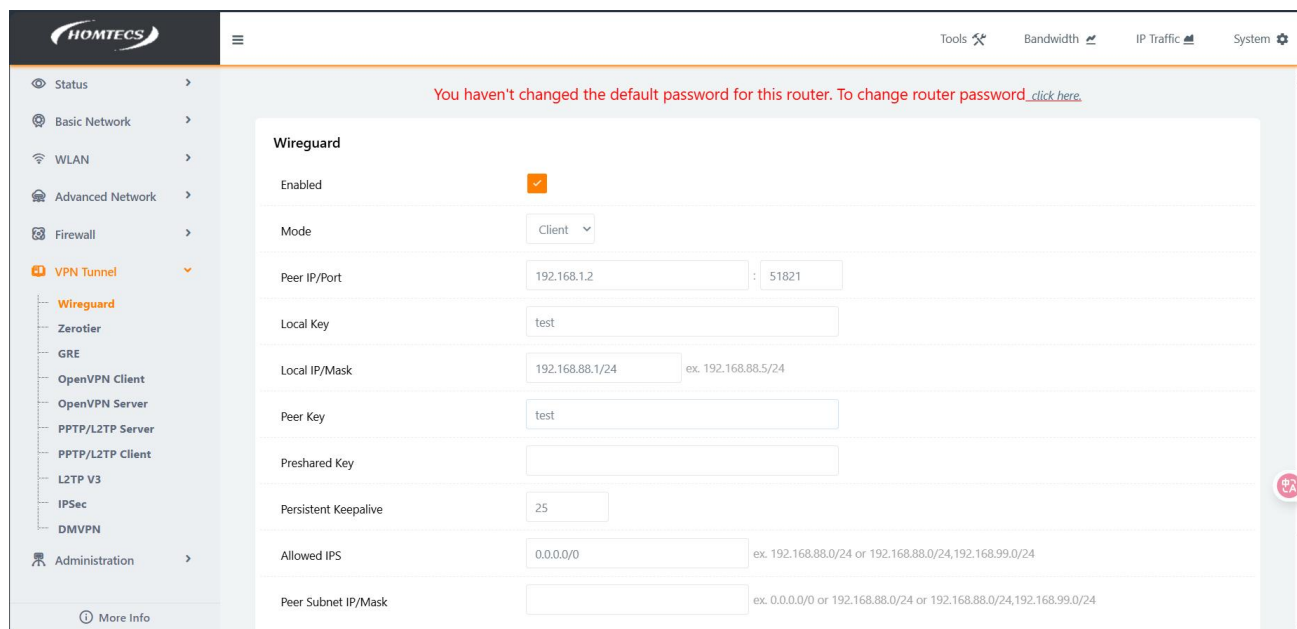


Figure 9-2

Step 2: Configure the wireguard parameter

Parameter	Meaning	How to configure
Enable Wireguard	Enable/disable the Wireguard feature	Click Enable to enable the feature
Network mode	There are two modes: server and client	Select the appropriate mode for each application
Local listening port	In server mode, the listening port of the server	The default is 51820
Local key	In server mode, the private key of the server	Default: test The server's private key is paired with the public key
Local address/mask	In server mode, one wireguardVPN subnet and mask of the server are supported	Format: A.B.C.D/M Default: 192.168.88.1/24
Peer subnet address/mask	In server mode, the client can have multiple WireGuard VPN subnets and masks	格式: A.B.C.D/M, E. F.G.H/N Default is empty
Allowd IPS	In server mode, the local subnet and mask of the client and the VPN subnet and mask of the client	格式: A.B.C.D/M, E. F.G.H/N Default: 0.0.0.0/0
Stay alive time	Every once in a while, it will be checked if the connection is dropped	Default: 25 Unit: seconds
Peer key	In server mode, the client's public key	Default is empty The client's private key is paired with the public key
Peer address/port	In client mode, the WAN port IP address and port number of the server	Port default: 192.168.1.2 Port default: 51821
Local key	In client mode, the private key of the client	Default: test It is paired with the public key set by the server
Local address/mask	In client mode, the VPN address and subnet of the client	Default: 192.168.88.1/24 The VPN address must be on the same network segment as the VPN address of the server, but the IP address is different
Peer key	In client mode, the server matches the public key	Default: test

Pre-shared key	The password of the client	Default is empty
Allowd IPS	In client mode, you can allow other IP addresses to access or connect to the device	Default: 0.0.0.0/0 The default setting means that all devices can access or connect
Peer subnet address/mask	In client mode, the local IP address of the server or the local IP address and subnet of other clients	Default is empty Format: A.B.C.D/M, E. F.G.H/N

Table 9-1 WireGuard parameters

Step 3: Set other parameters for server mode

You haven't changed the default password for this router. To change router password, [click here](#).

WAN / Internet

Type: Static Address

IP Address: 192.168.10.155

Subnet Mask: 255.255.255.0

Gateway: 192.168.10.1

MTU: 0 (0 for default)

Primary DNS: 192.168.10.1

Secondary DNS: 114.114.114.114

Figure 9-3

LAN

Bridge	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.1.1	255.255.255.0	✓	192.168.1.2 - 51	1440	✗	

1

Add +

DNS

Use Custom DNS: ☐

Figure 9-4

Step 4: Configure the wireguard parameter in server mode

You haven't changed the default password for this router. To change router password, [click here](#).

Wireguard

Enabled: ☒

Mode: Server

Bind Port: 51820

Local Key: ONFyuzEY5nNEkgOTyPsmYtuPD8fc9AU7nCS8pEIGY= Server private key

Local IP/Mask: 192.168.88.1/24 ex. 192.168.88.5/24

Peer Subnet IP/Mask: 192.168.3.0/24, 192.168.4.0/24 Server VPN tunnel address (note: cannot be the same as LAN port address)

Allowd IPS: 192.168.88.2/32, 192.168.3.0/24 subnet of Client 1

Persistent Keepalive: 25

Peer Key: xQWzK3nq9vUeqpkmldNzyFk1p/Sb6tbBNXhoc1F78yc= public key of Client 1

192.168.88.4/32, 192.168.4.0/24 subnet of Client 2

0.0.0.0/0 public key of Client 1

Add +

Figure 9-5

Step 5: Set other parameters in client mode
Route Client 1:

WAN / Internet

Type

Static Address

IP Address

192.168.10.125

Subnet Mask

255.255.255.0

Gateway

192.168.10.1

MTU

0

(0 for default)

Primary DNS

192.168.10.1

Secondary DNS

114.114.114.114

Figure 9-6

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.3.1	255.255.255.0	✓	192.168.3.2 - 254	1440	✗	

1

Add +

DNS

Use Custom DNS

Figure 9-7

Routing Client 2:

WAN / Internet

Type

Static Address

IP Address

192.168.10.127

Subnet Mask

255.255.255.0

Gateway

192.168.10.1

MTU

0

(0 for default)

Primary DNS

192.168.10.1

Secondary DNS

114.114.114.114

Figure 9-8

LAN

Bridge ^	IP Address	Subnet Mask	DHCP Server	IP Pool	Lease(minutes)	DHCP Relay	DHCP Server Address
br0	192.168.4.1	255.255.255.0	✓	192.168.4.2 - 254	1440	✗	

1

Add +

DNS

Use Custom DNS

Figure 9-9

Step 6: Configure the wireguard parameter of the client (the mask of the client must be set to /24, which cannot be in the same subnet range as /32 set by the server).

Route Client 1:

You haven't changed the default password for this router. To change router password [click here](#).

Wireguard

Enabled ☒

Mode: Client

Peer IP/Port: 192.168.10.155 : 51820 **Server WAN port IP/port**

Local Key: AAHE1BuHIpCgv/LGL9uKV5HFPZE1SHieqSiUjg830= **Client 1 Private Key**

Local IP/Mask: 192.168.88.2/24 ex. 192.168.88.5/24 **VPN tunnel address for client 1**

Peer Key: 6KVbpd/oz90D1zQ7og58trVfmdbjh+UFGX4c5oGZ4Gc= **Server public key**

Preshared Key:

Persistent Keepalive: 25

Allowed IPS: 0.0.0.0 ex. 192.168.88.0/24 or 192.168.88.0/24, 192.168.99.0/24

Peer Subnet IP/Mask: 192.168.1.0/24, 192.168.4.0/24 **Subnet of Client 2**

Figure 9-10

Routing Client 2:

You haven't changed the default password for this router. To change router password [click here](#).

Wireguard

Enabled ☒

Mode: Client

Peer IP/Port: 192.168.10.155 : 51821 **Server WAN port IP/port**

Local Key: CL64fgyfKuwYHf3yzjHfzLlU+YpMRoonUksZY= **Client 2 Private Key**

Local IP/Mask: 192.168.88.4/24 ex. 192.168.88.5/24 **VPN tunnel address for client 2**

Peer Key: 6KVbpd/oz90D1zQ7og58trVfmdbjh+UFGX4c5oGZ4Gc= **Server public key**

Preshared Key:

Persistent Keepalive: 25

Allowed IPS: 0.0.0.0 ex. 192.168.88.0/24 or 192.168.88.0/24, 192.168.99.0/24

Peer Subnet IP/Mask: 192.168.1.0/24, 192.168.3.0/24 **Subnet of Client 2**

Figure 9-11

Step 7: The connection is as follows

The telnet of the server enters the background and you can view the connection status and route table information

```

21/08/2024 10:07:04 /home/mobaxterm telnet 192.168.1.1 2323
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Router login: root
Password:

root@Router:/tmp/home/root# wg
interface: wg0
  public key: 6KVbpd/oz90D1zQ7og58trVfmdbjh+UFGX4c5oGZ4Gc=
  private key: (hidden)
  listening port: 51820

peer: aQWzk3nq9vUeqpkmdINzyFk1p/SbeIbBhXHoc1F78yc=
  endpoint: 192.168.10.125:19880
  allowed ips: 192.168.88.2/32, 192.168.3.0/24
  latest handshake: 1 minute, 45 seconds ago
  transfer: 3.55 KiB received, 2.48 KiB sent
  persistent keepalive: every 25 seconds

peer: Mzto7A2ShKyslnNFDz+FsA6RRUng9cI8JqisLmwkGfK=
  endpoint: 192.168.10.127:3077
  allowed ips: 192.168.88.4/32, 192.168.4.0/24
  latest handshake: 1 minute, 55 seconds ago
  transfer: 69.77 KiB received, 26.40 KiB sent
  persistent keepalive: every 25 seconds

```

Client1

Client2

Figure 9-12

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.2.240.1     0.0.0.0         UG    0      0      0 usb0
10.2.240.0       0.0.0.0        255.255.255.0   U     0      0      0 usb0
10.2.240.1       0.0.0.0        255.255.255.255 UH    0      0      0 usb0
127.0.0.0        0.0.0.0        255.0.0.0       U     0      0      0 lo
192.168.1.0      0.0.0.0        255.255.255.0   U     0      0      0 br0
192.168.3.0      0.0.0.0        255.255.255.0   U     0      0      0 wg0
192.168.4.0      0.0.0.0        255.255.255.0   U     0      0      0 wg0
192.168.10.0     0.0.0.0        255.255.255.0   U     0      0      0 v1an2
192.168.88.0     0.0.0.0        255.255.255.0   U     0      0      0 wg0

```

Figure 9-13

In server mode, you can ping the vpn addresses, gateways, and subnet IPs of both clients on the PC side

```

root@Router:/tmp/home/root# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2): 56 data bytes
64 bytes from 192.168.88.2: seq=0 ttl=64 time=1.243 ms
64 bytes from 192.168.88.2: seq=1 ttl=64 time=1.002 ms
64 bytes from 192.168.88.2: seq=2 ttl=64 time=0.972 ms
64 bytes from 192.168.88.2: seq=3 ttl=64 time=0.963 ms
64 bytes from 192.168.88.2: seq=4 ttl=64 time=0.975 ms
64 bytes from 192.168.88.2: seq=5 ttl=64 time=1.004 ms
^C
--- 192.168.88.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.963/1.026/1.243 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=64 time=1.171 ms
64 bytes from 192.168.3.1: seq=1 ttl=64 time=0.975 ms
64 bytes from 192.168.3.1: seq=2 ttl=64 time=0.942 ms
64 bytes from 192.168.3.1: seq=3 ttl=64 time=0.943 ms
64 bytes from 192.168.3.1: seq=4 ttl=64 time=0.977 ms
^C
--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.942/1.001/1.171 ms

root@Router:/tmp/home/root# ping 192.168.3.195
PING 192.168.3.195 (192.168.3.195): 56 data bytes
64 bytes from 192.168.3.195: seq=0 ttl=127 time=1.566 ms
64 bytes from 192.168.3.195: seq=1 ttl=127 time=1.262 ms
64 bytes from 192.168.3.195: seq=2 ttl=127 time=1.276 ms
64 bytes from 192.168.3.195: seq=3 ttl=127 time=1.310 ms

```

Figure 9-14

```

root@Router:/tmp/home/root# ping 192.168.88.4
PING 192.168.88.4 (192.168.88.4): 56 data bytes
64 bytes from 192.168.88.4: seq=0 ttl=64 time=1.103 ms
64 bytes from 192.168.88.4: seq=1 ttl=64 time=0.984 ms
64 bytes from 192.168.88.4: seq=2 ttl=64 time=0.992 ms
64 bytes from 192.168.88.4: seq=3 ttl=64 time=0.988 ms
^C
--- 192.168.88.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.984/1.016/1.103 ms

root@Router:/tmp/home/root# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1): 56 data bytes
64 bytes from 192.168.4.1: seq=0 ttl=64 time=1.177 ms
64 bytes from 192.168.4.1: seq=1 ttl=64 time=2.672 ms
64 bytes from 192.168.4.1: seq=2 ttl=64 time=0.919 ms
64 bytes from 192.168.4.1: seq=3 ttl=64 time=0.973 ms
64 bytes from 192.168.4.1: seq=4 ttl=64 time=0.950 ms
^C
--- 192.168.4.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.919/1.338/2.672 ms

root@Router:/tmp/home/root# ping 192.168.4.195
PING 192.168.4.195 (192.168.4.195): 56 data bytes
64 bytes from 192.168.4.195: seq=0 ttl=127 time=1.599 ms
64 bytes from 192.168.4.195: seq=1 ttl=127 time=1.344 ms
64 bytes from 192.168.4.195: seq=2 ttl=127 time=1.298 ms
64 bytes from 192.168.4.195: seq=3 ttl=127 time=1.305 ms
^C
--- 192.168.4.195 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss

```

Figure 9-15

The telnet client enters the background and can view the connection status and route table information Client 1:


```

root@Router:/tmp/home/root# wg show
interface: wg0
  public key: aQWzk3nq9vUeqpkmdINzyFk1p/SbeIbBhXHoc1F78yc=
  private key: (hidden)
  listening port: 26277

peer: 6KVbpd/oz90D1zQ7og58trVFmdbjh+UFGX4c5oGZ4Gc=
  endpoint: 192.168.10.155:51820
  allowed ips: 0.0.0.0/0
  latest handshake: 1 minute, 36 seconds ago
  transfer: 4.43 KiB received, 6.20 KiB sent
  persistent keepalive: every 25 seconds
root@Router:/tmp/home/root#

```

Figure 9-16

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 192.168.10.1 0.0.0.0 UG 0 0 0 wlan2
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.3.0 0.0.0.0 255.255.255.0 U 0 0 0 br0
192.168.4.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0
192.168.10.0 0.0.0.0 255.255.255.0 U 0 0 0 wlan2
192.168.10.1 0.0.0.0 255.255.255.255 UH 0 0 0 wlan2
192.168.88.0 0.0.0.0 255.255.255.0 U 0 0 0 wg0

```

Figure 9-17

Client 1 can ping the VPN address, gateway and subnet IP address of the server (including the ping packet on the PC)

```

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.288 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=0.958 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.016 ms
64 bytes from 192.168.88.1: seq=4 ttl=64 time=1.079 ms
64 bytes from 192.168.88.1: seq=5 ttl=64 time=0.997 ms
^C
--- 192.168.88.1 ping statistics ---
5 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 0.958/1.067/1.288 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.000 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.933 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.966 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.935 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.933/0.998/1.156 ms

root@Router:/tmp/home/root# ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37): 56 data bytes
64 bytes from 192.168.1.37: seq=0 ttl=127 time=1.415 ms
64 bytes from 192.168.1.37: seq=1 ttl=127 time=1.301 ms
64 bytes from 192.168.1.37: seq=2 ttl=127 time=1.247 ms
64 bytes from 192.168.1.37: seq=3 ttl=127 time=1.285 ms
64 bytes from 192.168.1.37: seq=4 ttl=127 time=1.302 ms
^C

```

Server VPN address

Server subnet and gateway

Figure 9-18

Client 2:

```

root@Router:/tmp/home/root# wg
interface: wg0
  public key: Mzto7A2ShKyslnNFDz+Fsa6RRUng9cI8JqislmWkGFk=
  private key: (hidden)
  listening port: 47384

peer: 6KVbpd/oz90D1zQ7og58trVFmdbjh+UFGX4c5oGZ4Gc=
  endpoint: 192.168.10.155:51820
  allowed ips: 0.0.0.0/0
  latest handshake: 1 minute, 22 seconds ago
  transfer: 9.18 KiB received, 34.07 KiB sent
  persistent keepalive: every 25 seconds
root@Router:/tmp/home/root#

```

Figure 9-19

```

root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.1   0.0.0.0         UG    0      0          0 wlan2
127.0.0.0        0.0.0.0        255.0.0.0       U     0      0          0 lo
192.168.1.0      0.0.0.0        255.255.255.0   U     0      0          0 wg0
192.168.3.0      0.0.0.0        255.255.255.0   U     0      0          0 wg0
192.168.4.0      0.0.0.0        255.255.255.0   U     0      0          0 br0
192.168.10.0     0.0.0.0        255.255.255.0   U     0      0          0 wlan2
192.168.10.1     0.0.0.0        255.255.255.255 UH    0      0          0 wlan2
192.168.88.0     0.0.0.0        255.255.255.0   U     0      0          0 wg0

```

Figure 9-20

Client 2 can ping the VPN address, gateway and subnet IP address of the server (including the ping packet on the PC).

```

root@Router:/tmp/home/root# ping 192.168.88.1
PING 192.168.88.1 (192.168.88.1): 56 data bytes
64 bytes from 192.168.88.1: seq=0 ttl=64 time=1.288 ms
64 bytes from 192.168.88.1: seq=1 ttl=64 time=0.958 ms
64 bytes from 192.168.88.1: seq=2 ttl=64 time=1.016 ms
64 bytes from 192.168.88.1: seq=4 ttl=64 time=1.079 ms
64 bytes from 192.168.88.1: seq=5 ttl=64 time=0.997 ms
^C
--- 192.168.88.1 ping statistics ---
5 packets transmitted, 5 packets received, 16% packet loss
round-trip min/avg/max = 0.958/1.067/1.288 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.000 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.933 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.966 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.935 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.933/0.998/1.156 ms

root@Router:/tmp/home/root# ping 192.168.1.37
PING 192.168.1.37 (192.168.1.37): 56 data bytes
64 bytes from 192.168.1.37: seq=0 ttl=127 time=1.415 ms
64 bytes from 192.168.1.37: seq=1 ttl=127 time=1.301 ms
64 bytes from 192.168.1.37: seq=2 ttl=127 time=1.247 ms
64 bytes from 192.168.1.37: seq=3 ttl=127 time=1.285 ms
64 bytes from 192.168.1.37: seq=4 ttl=127 time=1.302 ms
^C

```

Figure 9-21

Client 1 or Client 2 pings the peer (including the PC side).

Client 1:

```

PING 192.168.88.4 (192.168.88.4): 56 data bytes
64 bytes from 192.168.88.4: seq=0 ttl=63 time=1.652 ms
64 bytes from 192.168.88.4: seq=1 ttl=63 time=1.594 ms
64 bytes from 192.168.88.4: seq=2 ttl=63 time=1.549 ms
64 bytes from 192.168.88.4: seq=3 ttl=63 time=1.576 ms
^C
--- 192.168.88.4 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.549/1.642/1.852 ms

root@Router:/tmp/home/root# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1): 56 data bytes
64 bytes from 192.168.4.1: seq=0 ttl=63 time=1.987 ms
64 bytes from 192.168.4.1: seq=1 ttl=63 time=1.638 ms
64 bytes from 192.168.4.1: seq=2 ttl=63 time=1.587 ms
^C
--- 192.168.4.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.587/1.737/1.987 ms

root@Router:/tmp/home/root# ping 192.168.4.195
PING 192.168.4.195 (192.168.4.195): 56 data bytes
64 bytes from 192.168.4.195: seq=0 ttl=126 time=2.962 ms
64 bytes from 192.168.4.195: seq=1 ttl=126 time=2.155 ms
64 bytes from 192.168.4.195: seq=2 ttl=126 time=2.112 ms
64 bytes from 192.168.4.195: seq=3 ttl=126 time=2.082 ms
^C
--- 192.168.4.195 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.082/2.327/2.962 ms

```

Figure 9-22

Client 2:

```

root@Router:/tmp/home/root# ping 192.168.88.2
PING 192.168.88.2 (192.168.88.2): 56 data bytes
64 bytes from 192.168.88.2: seq=0 ttl=63 time=1.901 ms
64 bytes from 192.168.88.2: seq=1 ttl=63 time=1.591 ms
64 bytes from 192.168.88.2: seq=2 ttl=63 time=1.667 ms
64 bytes from 192.168.88.2: seq=3 ttl=63 time=1.657 ms
^C
--- 192.168.88.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.591/1.704/1.901 ms

root@Router:/tmp/home/root# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: seq=0 ttl=63 time=1.912 ms
64 bytes from 192.168.3.1: seq=1 ttl=63 time=1.716 ms
64 bytes from 192.168.3.1: seq=2 ttl=63 time=1.705 ms
^C
--- 192.168.3.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.705/1.777/1.912 ms

root@Router:/tmp/home/root# ping 192.168.3.195
PING 192.168.3.195 (192.168.3.195): 56 data bytes
64 bytes from 192.168.3.195: seq=0 ttl=126 time=2.461 ms
64 bytes from 192.168.3.195: seq=1 ttl=126 time=2.211 ms
64 bytes from 192.168.3.195: seq=2 ttl=126 time=2.028 ms
^C
--- 192.168.3.195 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 2.028/2.233/2.461 ms

root@Router:/tmp/home/root#

```

Figure 9-23

9.2. Zerotier

ZeroTier is a software-defined networking (SDN) solution that enables users to create and manage virtual networks across physical devices and locations. It enables seamless connection of devices on the Internet, suitable for remote work, Internet of Things and other scenarios, providing secure and efficient network connectivity.

Step 1: Select "VPN Tunnel >Zerotier" in the navigation bar

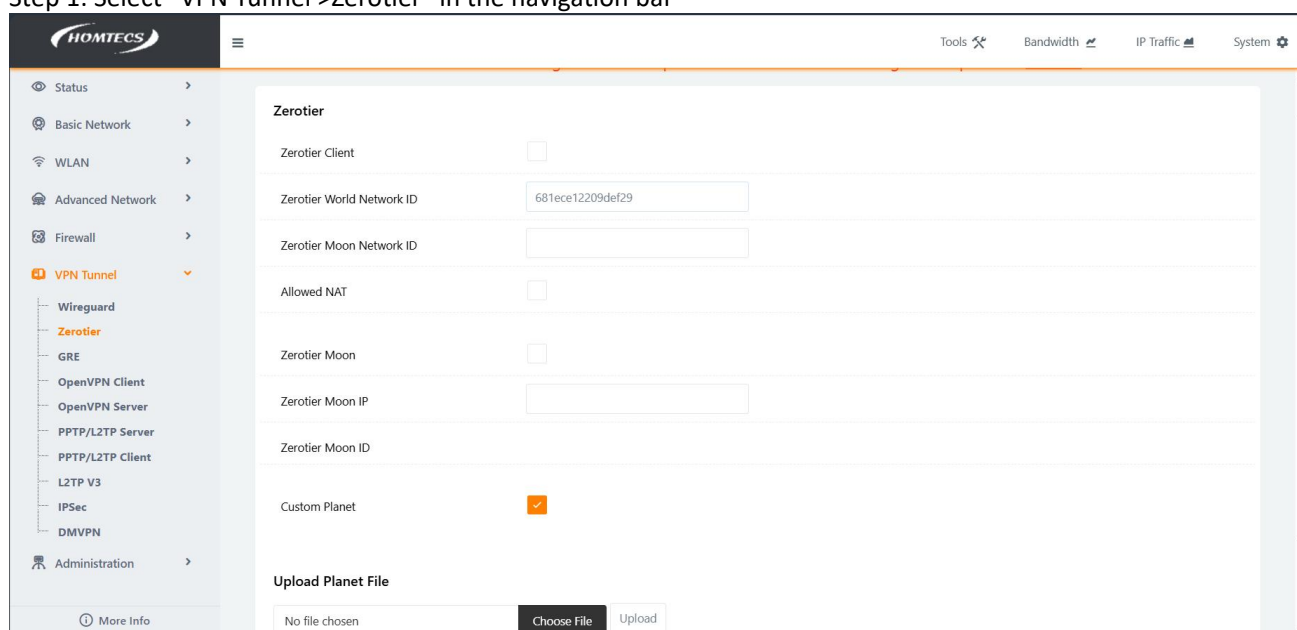


Figure 9-24

Zerotier Parameter Description:

The name of the parameter	meaning	How to configure
Enable Zerotier	Enable/disable the Zerotier feature	Click 'Enable' to enable the feature save to
Zerotier World Network ID	The network ID of the root node of the ZeroTier	
Zerotier Moon Network ID	This is the network ID of the ZeroTier proxy node	
	To enable this function, you need to use it in conjunction with the IP	

Automatically allow client NAT	management table of ZeroTier to allow access to other ZeroTier clients, and the IP address is the LAN CIDR block address of other ZeroTier clients. The gateway is the vpn address of the other ZeroTier client, and the IP address and gateway must correspond to the same route.	
Enable the ZeroTier Moon server	Enable/disable the Zerotier Moon server feature	Click 'Enable' to enable the feature save to
ZeroTier Moon Server IP	Enter the IP address of the Moonnode	
ZeroTier Moon server ID	Enter the ID of the Megaonnode	
Customize Planet	Enable/Disable indicates whether or not to use the custom Planet service	Click Enable to save to enable the feature
Upload the Planet file	Uploading a Planet file means uploading a Planet file on a custom server, and not uploading a file means that the official root node is used by default	

Table 9-2

Example of using a custom Planet:

Step 1: The first time you use a custom Planet, you need to import the Planet file, and you need to enable the custom Planet function, after importing the file, you need to re-save the settings to make the Planet file take effect, after the first import is successful, enter the background cd /tmp/etc/storage directory, you can view the Planet file, after the power is off and restarted, the Planet file has been written into the nvram parameter.

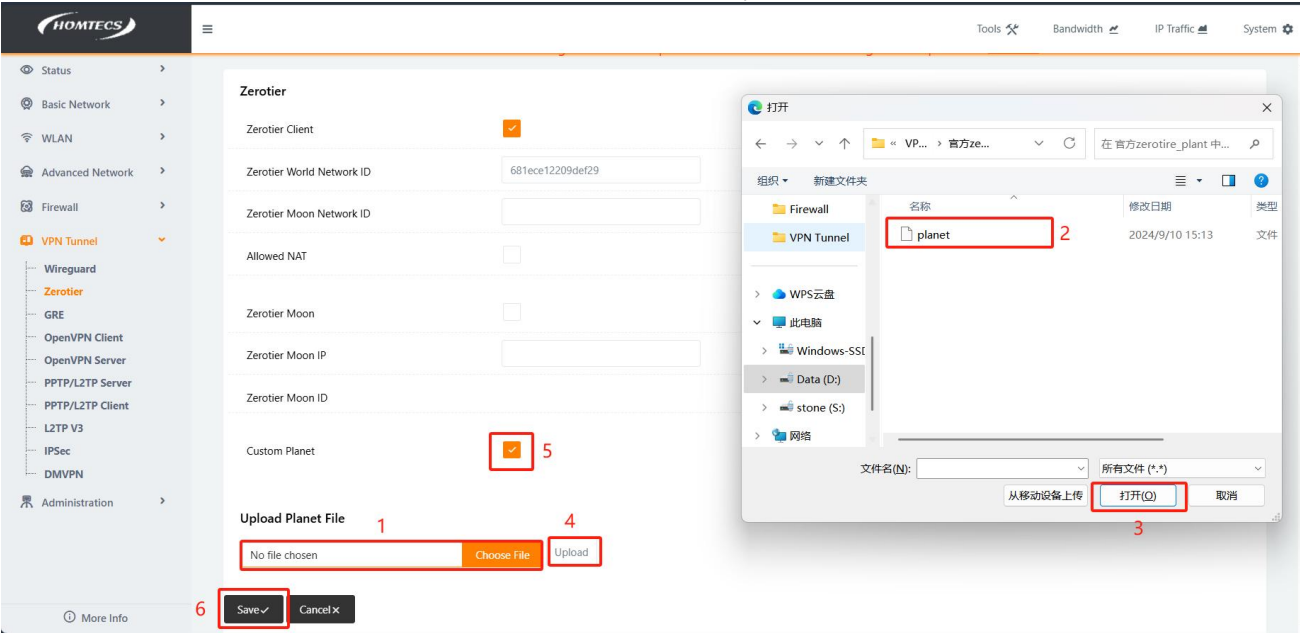


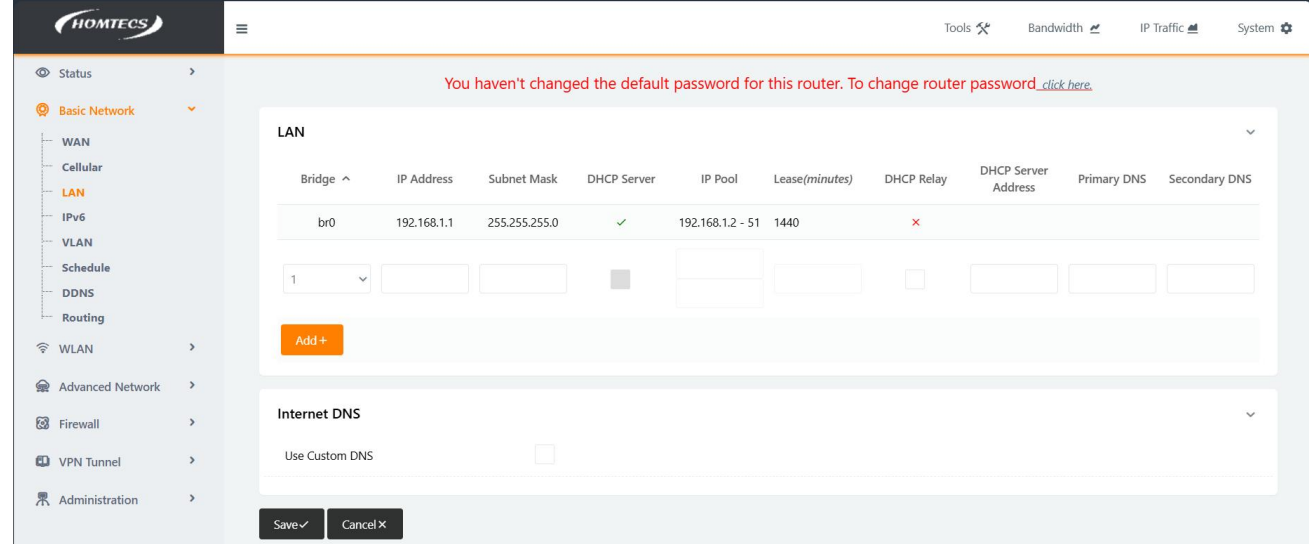
Figure 9-25

```
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# cd /tmp/etc/
root@Router:/tmp/etc# ls
TZ                dnsmasq          group            igmp.conf        iptables         openssl.cnf      resolv.conf      shadow          swanctl          zebra.conf
Wireless          dnsmasq.conf     gshadow          iproute2         ld.so.conf       passwd           resolv.dnsmasq  strongswan.conf  vpn              wg_cli_pub.key
cli.conf          ethertypes       hosts            ipsec.conf        moid             profile          rtpd.conf       strongswan.d     wg_cli_pub.key  wg_svr_pri.key
detran_cfg        fstab            hotplug2.rules  ipsec.secrets    mtab             protocols        services         strongswan.d     wg_cli_pub.key  wg_svr_pri.key
root@Router:/tmp/etc#
root@Router:/tmp/etc# cd storage/
root@Router:/tmp/etc/storage# ls
planet            zerotier-one
root@Router:/tmp/etc/storage#
root@Router:/tmp/etc/storage#
root@Router:/tmp/etc/storage#
```

Figure 9-26

Step 2: Use two routers, Router1 and Router2. Two PCs, PC1 and PC2; Router1 is connected to PC1, and Router2 is connected to PC2.

Router1 is configured as follows: the subnet address of PC1 is 192.168.1.25/24, and the gateway is 192.168.1.1



Figure

9-27

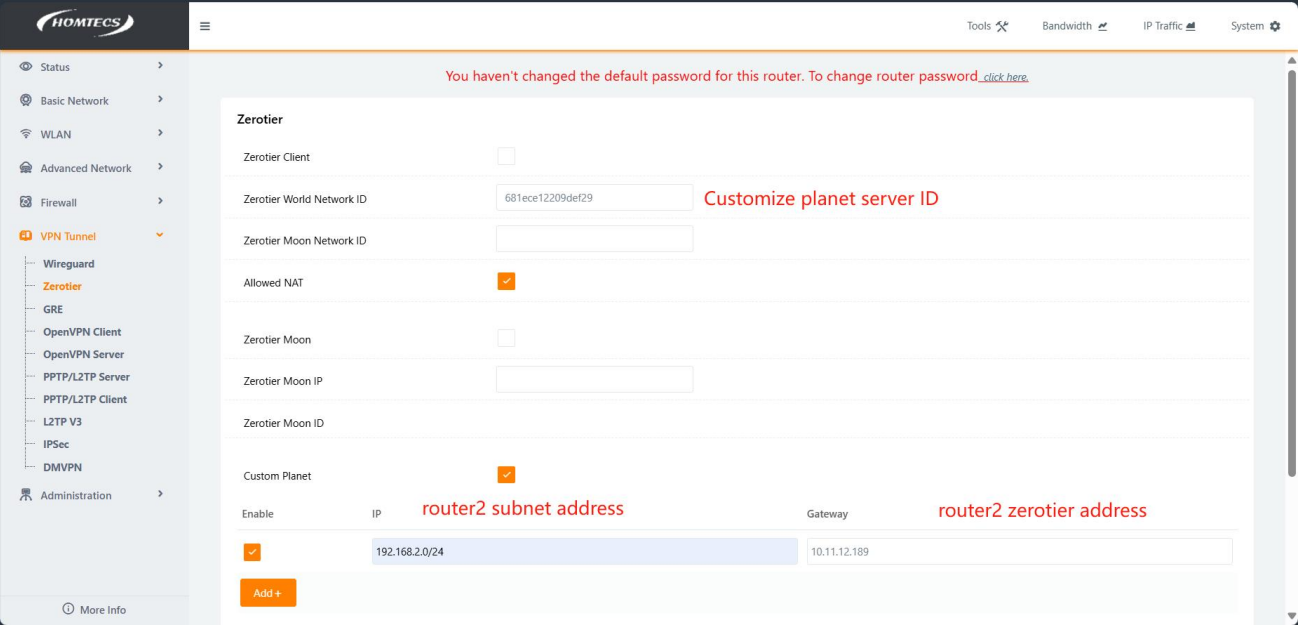


Figure 9-28

Router2 is configured as follows: PC2 has a subnet address of 192.168.2.35/24 and a gateway of 192.168.2.1

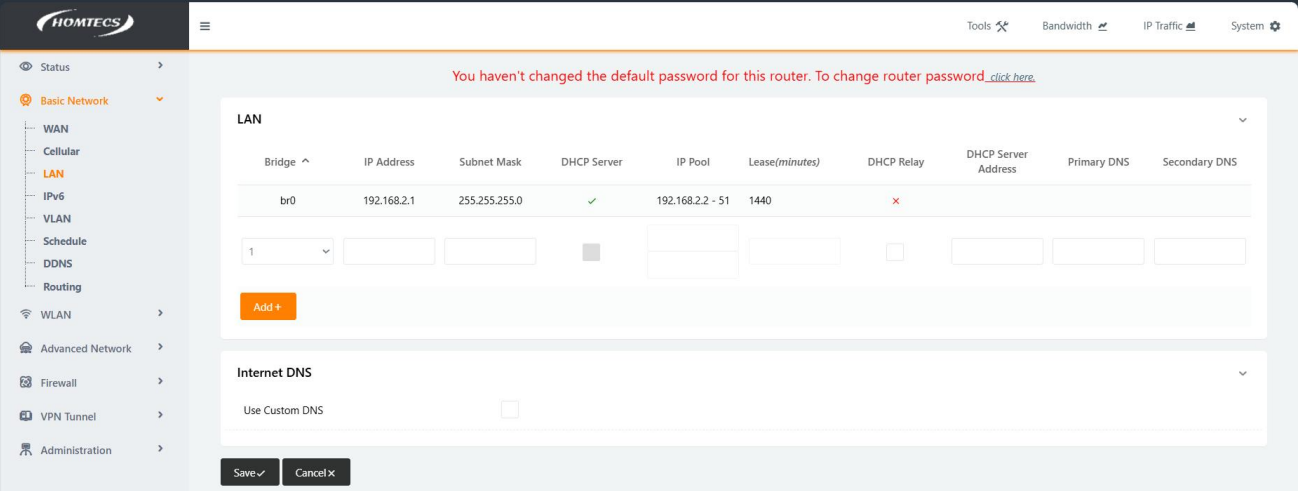


Figure 9-29

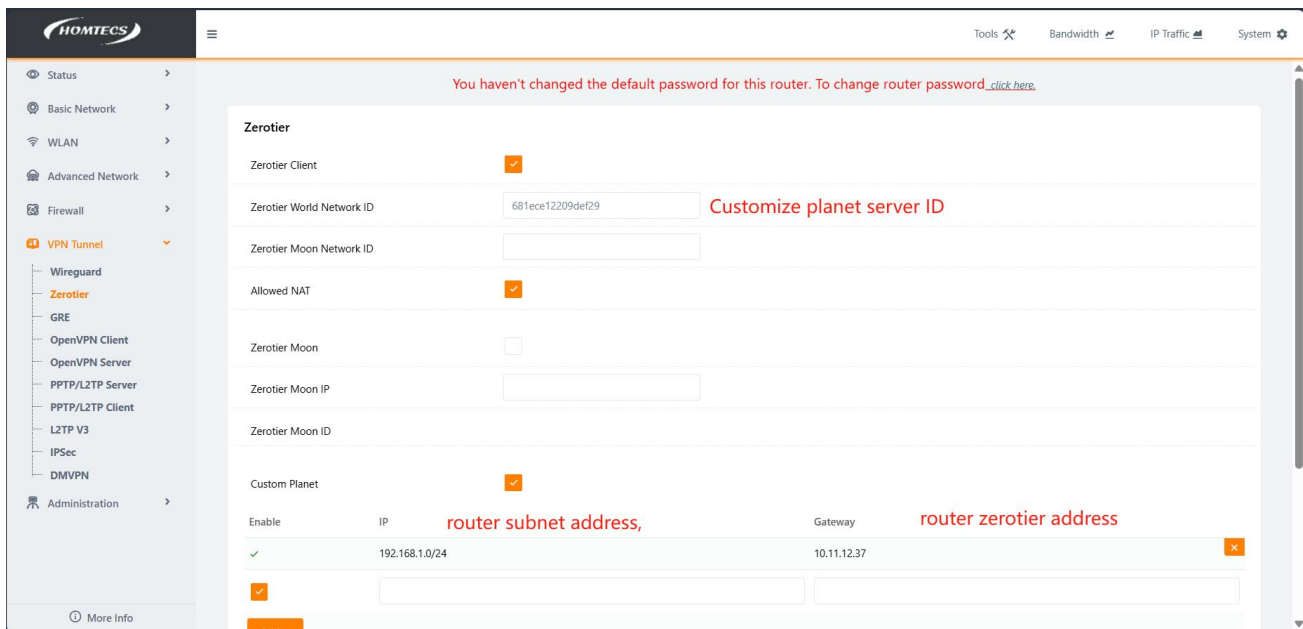


Figure 9-30

Step 3: Check the connection status

Enter the backend of Router1 and Router2 respectively, and ifconfig can also view and obtain the address

```
usb0      Link encap:Ethernet  HWaddr DE:07:B4:3D:02:30
          inet addr:10.66.55.31  Mask:255.255.255.192
          UP RUNNING NOARP MULTICAST  MTU:1400  Metric:1
          RX packets:78290  errors:0  dropped:0  overruns:0  frame:0
          TX packets:60320  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:92205309 (87.9 MiB)  TX bytes:6437284 (6.1 MiB)

vlan1     Link encap:Ethernet  HWaddr 34:0A:51:32:33:61
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:217012  errors:0  dropped:0  overruns:0  frame:0
          TX packets:21416  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17288035 (16.4 MiB)  TX bytes:7244639 (6.9 MiB)

ztpi7fh7ij Link encap:Ethernet  HWaddr 2A:C5:C6:CF:35:B8      Router1
          inet addr:10.11.12.37  Bcast:10.11.12.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:2800  Metric:1
          RX packets:1468  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1084  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:500
          RX bytes:1553048 (1.4 MiB)  TX bytes:125833 (122.8 KiB)

root@Router:/tmp/home/root#
```

Figure 9-31

```
usb0      Link encap:Ethernet  HWaddr 9E:C4:C8:48:22:D7
          inet addr:10.18.75.234  Bcast:10.18.75.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7794  errors:0  dropped:0  overruns:0  frame:0
          TX packets:18027  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2393128 (2.2 MiB)  TX bytes:4498395 (4.2 MiB)

vlan1     Link encap:Ethernet  HWaddr 30:3D:51:11:B2:55
          UP BROADCAST RUNNING ALLMULTI MULTICAST  MTU:1500  Metric:1
          RX packets:32689  errors:0  dropped:0  overruns:0  frame:0
          TX packets:13317  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3351346 (3.1 MiB)  TX bytes:3530408 (3.3 MiB)

ztpi7fh7ij Link encap:Ethernet  HWaddr 2A:5B:39:34:B1:59      Router2
          inet addr:10.11.12.189  Bcast:10.11.12.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:2800  Metric:1
          RX packets:1147  errors:0  dropped:0  overruns:0  frame:0
          TX packets:1466  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:500
          RX bytes:132091 (128.9 KiB)  TX bytes:1568220 (1.4 MiB)

root@Router:/tmp/home/root#
```

Figure 9-32

After NAT is configured, both devices can ping the peer gateway and subnet addresses on the PC and the router

Router1, PC1 ping:

```
root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=118.049 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=115.918 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=157.476 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=97.071 ms
64 bytes from 192.168.2.1: seq=4 ttl=64 time=95.434 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 95.434/116.789/157.476 ms

root@Router:/tmp/home/root# ping 192.168.2.35
PING 192.168.2.35 (192.168.2.35): 56 data bytes
64 bytes from 192.168.2.35: seq=0 ttl=127 time=131.753 ms
64 bytes from 192.168.2.35: seq=1 ttl=127 time=89.171 ms
64 bytes from 192.168.2.35: seq=2 ttl=127 time=69.050 ms
64 bytes from 192.168.2.35: seq=3 ttl=127 time=115.275 ms
64 bytes from 192.168.2.35: seq=4 ttl=127 time=112.699 ms
^C
--- 192.168.2.35 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 69.050/103.589/131.753 ms

root@Router:/tmp/home/root#
```

Router1

Figure 9-33

```
19/06/2024 10:23.27 /home/mobaxterm ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间=152ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=78ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=83ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=147ms TTL=63

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 78ms, 最长 = 152ms, 平均 = 115ms

19/06/2024 11:45.41 /home/mobaxterm ping 192.168.2.35

正在 Ping 192.168.2.35 具有 32 字节的数据:
来自 192.168.2.35 的回复: 字节=32 时间=97ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=102ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=76ms TTL=126
来自 192.168.2.35 的回复: 字节=32 时间=77ms TTL=126

192.168.2.35 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 76ms, 最长 = 102ms, 平均 = 88ms
```

PC1

Figure 9-34

Router2, PC2 ping:

```
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=95.862 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=72.544 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=122.445 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=58.510 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 58.510/87.340/122.445 ms

root@Router:/tmp/home/root# ping 192.168.1.25
PING 192.168.1.25 (192.168.1.25): 56 data bytes
64 bytes from 192.168.1.25: seq=0 ttl=127 time=152.327 ms
64 bytes from 192.168.1.25: seq=1 ttl=127 time=142.216 ms
64 bytes from 192.168.1.25: seq=2 ttl=127 time=76.966 ms
64 bytes from 192.168.1.25: seq=3 ttl=127 time=111.470 ms
64 bytes from 192.168.1.25: seq=4 ttl=127 time=698.566 ms
^C
--- 192.168.1.25 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 76.966/236.309/698.566 ms

root@Router:/tmp/home/root#
```

Router2

Figure 9-35

```

19/06/2024 11:50:09 /home/mobaxterm ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=70ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=506ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=145ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=67ms TTL=63

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 67ms, 最长 = 506ms, 平均 = 197ms

19/06/2024 11:50:29 /home/mobaxterm ping 192.168.1.25

正在 Ping 192.168.1.25 具有 32 字节的数据:
来自 192.168.1.25 的回复: 字节=32 时间=1408ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=463ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=78ms TTL=126
来自 192.168.1.25 的回复: 字节=32 时间=66ms TTL=126

192.168.1.25 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 66ms, 最长 = 1408ms, 平均 = 503ms

```

Figure 9-36

9.3. GRE

Tunneling technology is a way of passing data between networks through an interconnected network infrastructure. The logical path that the encapsulated packet travels through as it travels over the public Internet throughout the delivery process is called a tunnel. GRE (Generic Routing Encapsulation) specifies how one network protocol is used to encapsulate another. There are two main uses of the GRE protocol: internal protocol encapsulation and private address encapsulation.

Step 1: Select "VPN Tunnel > GRE" in the navigation bar, as shown in Figure 9-37

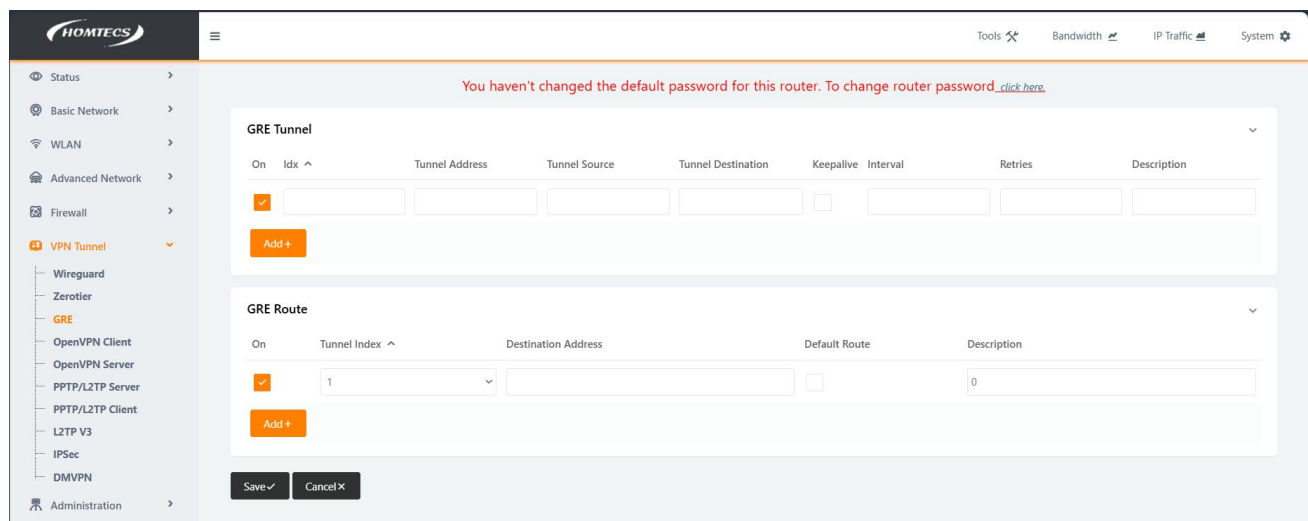


Figure 9-37

Step 2: GRE Mode Parameters

Parameter	Meaning	How to configure
Enable GRE	Enable/disable the IP Tunnel Service	Click Enable to enable the tunnel rule
Tunnel address	The virtual IP address of the local tunnel	Enter the virtual IP address of the local GRE tunnel. Format: Interface A.B.C.D
The source address of the tunnel	Set the IP address of the public network or WAN port of the machine	Enter the IP address of the external interface of the local network of the tunnel. Format: A.B.C.D
	The external interface IP address of	Enter the IP address of the external

The destination address of the tunnel	the tunnel peer network is usually the public IP (Internet) address, but it can also be the internal IP address of the enterprise	interface of the tunnel peer network Format: A.B.C.D. interface type
Destination address	Set the destination address of the peer	Format: A.B.C.D/M

Table 9-3 GRE Mode Parameter Configuration

Step 3: Once the configuration is complete, click the "Save Settings" button for the configuration to take effect.
Example:

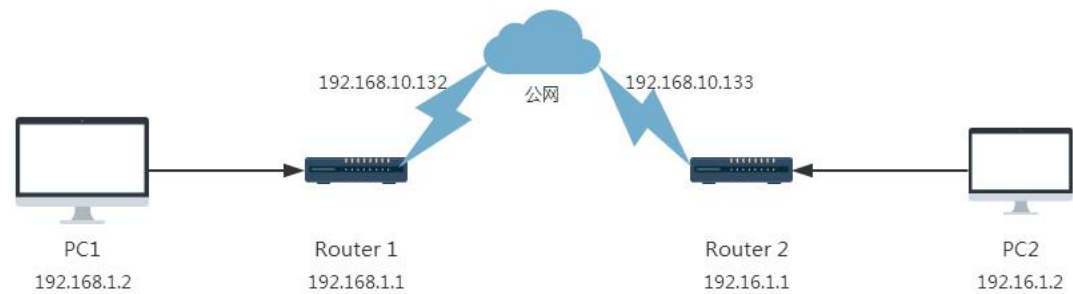


Figure 9-38

Router1 configuration:

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	3	192.168.1.1	192.168.10.69	192.168.10.67	✓	3	10	
✓								

Add +

GRE Route

On	Tunnel Index ^	Destination Address	Default Route	Description
✓	3	192.168.2.0/24	✓	0
✓	1			0

Add +

Figure 9-39

Router2 configuration:

GRE Tunnel

On	Idx ^	Tunnel Address	Tunnel Source	Tunnel Destination	Keepalive	Interval	Retries	Description
✓	3	192.168.2.1	192.168.10.67	192.168.10.69	✓	3	10	
✓								

Add +

GRE Route

On	Tunnel Index ^	Destination Address	Description
✓	3	192.168.1.0/24	
✓	1		

Add +

Figure 9-40

Router1 can be pinged from PC2

```
root@LTE_Quectel:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.828 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.661 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.642 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.629 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.636 ms
^C
```

Figure 9-41

Router1 can be pinged from PC2

```
23/08/2024 16:08.04 /home/mobaxterm ping 192.168.2.1

正在 Ping 192.168.2.1 具有 32 字节的数据:
来自 192.168.2.1 的回复: 字节=32 时间<1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=3ms TTL=63
来自 192.168.2.1 的回复: 字节=32 时间=1ms TTL=63

192.168.2.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 3ms, 平均 = 1ms
```

Figure 9-42

9.4. OpenVPN Client

OpenVPN is an application-layer VPN implementation based on the OpenSSL library, which is a virtual private tunnel that provides a secure data transmission between enterprises or between individuals and companies. OpenVPN allows a single point of participation in the establishment of a VPN using a shared key, e-certificate, or username/password for authentication.

- Step 1: Select "VPN Tunnel > OpenVPN Client" in the navigation bar.
- Step 2: Openvpn configuration is divided into four configurations

Basic settings

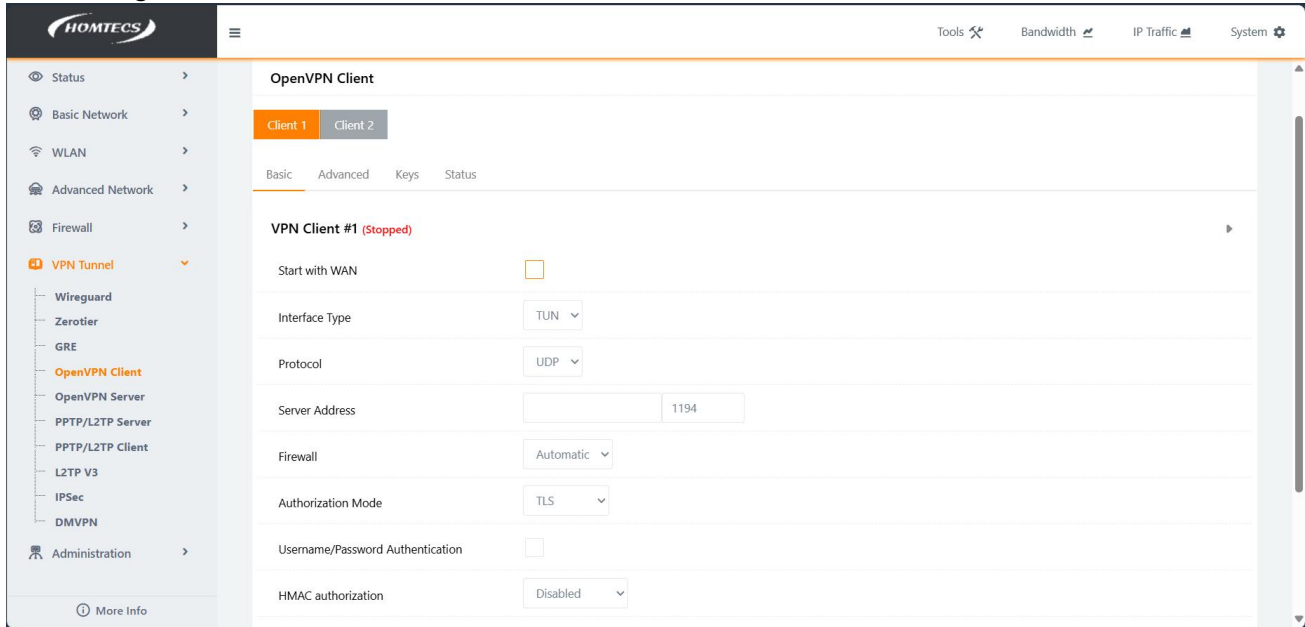


Figure 9-43

Basic Parameter Configuration Description:

Parameter	Meaning	How to configure
via the Internet	Whether the network is over a WAN port	Turn on or off
Interface type	The difference between TUN and TAP is that a TUN device is a point-to-point virtual appliance at the network layer, while TAP is a virtual appliance at the Ethernet link layer.	Drop-down to select TAP mode or TUN mode

	TAP mode: Openvpn bridging mode TUN mode: openvpn tunnel mode	
agreement	TCP mode or UDP mode	Select TCP mode or UDP mode from the drop-down list
Server address/port	Server subnet configuration, including IP address and port	You need to fill in the subnet address and port of the server. Format: A.B.C.D; port number
firewall	Firewall modes, including automatic and custom	Select Automatic or Custom from the drop-down list
Type of Certification	The authentication types include TLS, static key, and custom	Select TLS, static key, or custom from the drop-down drop-down
Username/password authentication	Whether to enable username/password authentication	Enabled or not enabled
Username	Appears when the username/password feature is enabled	Enter the username configured on the server
password	Appears when the username/password feature is enabled	Enter the password configured on the server
Only the username is authenticated	If the server does not have a password, it can be enabled without entering the password	Enable or disable
HMAC Certified	Hash message authentication: Default: Disabled, Bi- directional Incoming Outgoing	Enable or select one of the modes
The services are on the same subnet	Appears when TAP is selected for Interface Type	Enable or disable
Tunnel NAT is allowed	When the interface type is selected as TUN, click the toggle button to enable/disable the NAT (Network Address Translation) feature. When enabled, the host IP address behind the router will be encapsulated.	Enable or disable

Table 9-4 OpenVPN parameter configuration

Advanced settings:

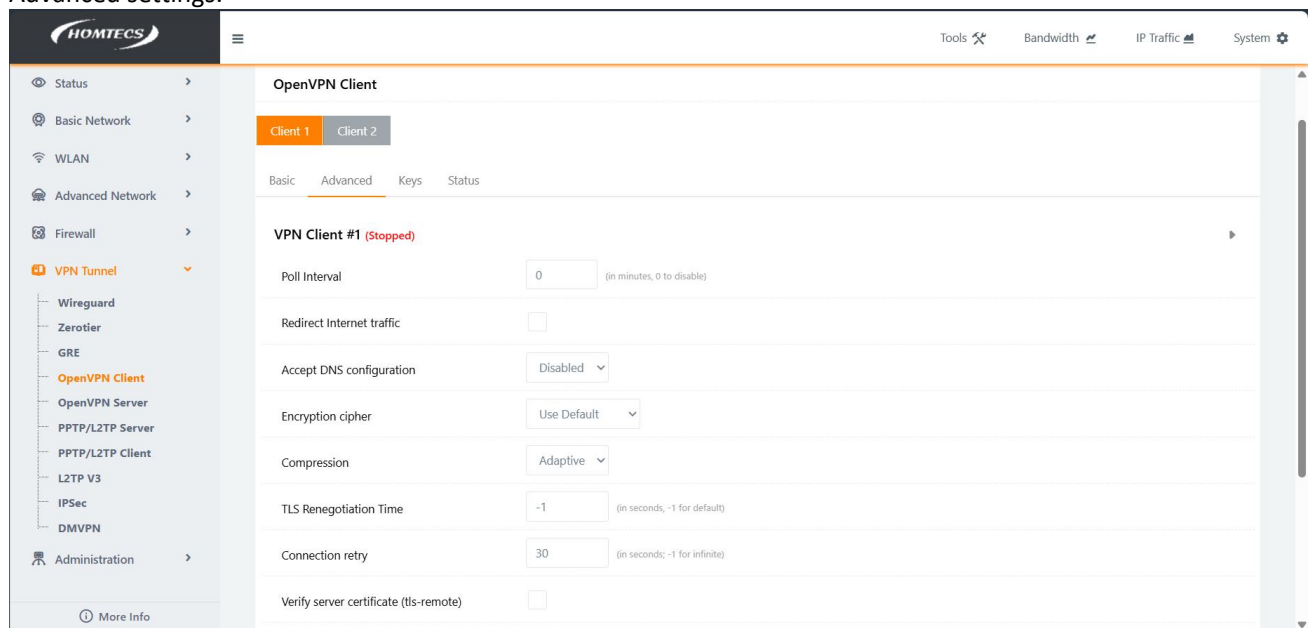


Figure 9-44

Advanced Setup Instructions:

Parameter	Meaning	How to configure
Polling interval	0 is not disabled and is in minutes	0 is not enabled, and 0 is enabled
Allowed is the default route	Whether to allow OpenVPN as the default route	Enable or disable

Receives the peer DNS configuration	4 种 对 端 DNS 配 置 ; disabled,relaxed,strict,exclusive	Select any one of the four modes from the drop down menu
Encryption algorithms	Choose from "BF", "DES", "DES-EDE3", "AES128", "AES192", and "AES256". BF:128-bit encryption algorithm using BF in CBC mode DES: Use DES's 64-bit encryption algorithm in CBC mode DES-EDE3: 192-bit encryption algorithm using 3DES in CBC mode AES128: Use AES's 128-bit encryption algorithm in CBC mode AES192: Use AES's 192-bit encryption algorithm in CBC mode AES256: Uses AES's 256-bit encryption algorithm in CBC mode	Select any one from the drop-down list
compress	4 种 压 缩 模 式 ; disabled , none , enabled , adaptive	
TLS renegotiation time	-1 is the default in seconds	-1 is the default Enter 0 or higher to enable
Number of reconnections	Set the number of reconnections of OpenVPN, -1 is an unlimited number of reconnections	-1 is an unlimited number of times, fill in the number above 0 as the number of reconnections, and the default is 30
Authentication server certificate	After checking the box, the common name input box appears	Enable or disable
Customization options	Reservation settings	

Table 9-5

Key Settings:

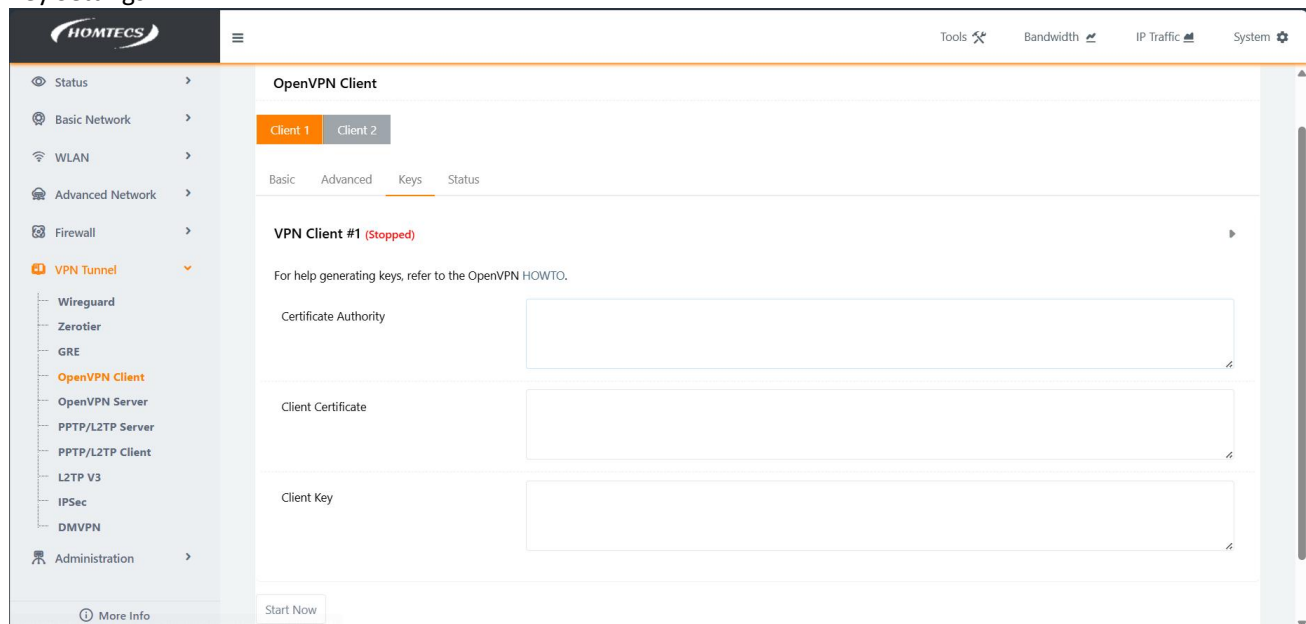


Figure 9-45

Key Setup Instructions:

Parameter	Meaning	How to configure
Certificate Authority	Configure the corresponding certificate authorization	Enter the corresponding authorization certificate
Client certificate	Configure the corresponding client certificate	Enter the corresponding client certificate
Client Secret	Configure the corresponding client	Enter the corresponding client

	secret	secret
--	--------	--------

Table 9-6

State:

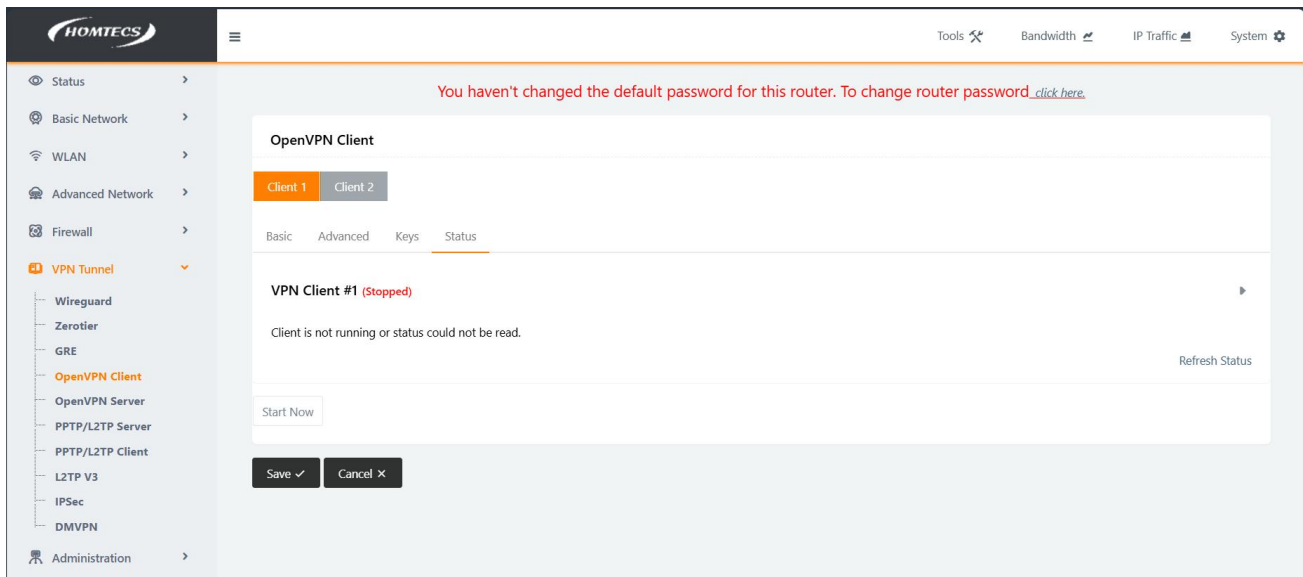


Figure 9-46

Status Description:

The name of the parameter	meaning	How to configure
Start now	Launch OpenVPN now	Enable or disable
Refresh the state	Manually refresh the OpenVPN link status	To click or not to click

Table 9-7

9.5. OpenVPN Server

OpenVPN is an application-layer VPN implementation based on the OpenSSL library, which is a virtual private tunnel that provides a secure data transmission between enterprises or between individuals and companies. OpenVPN allows a single point of participation in the establishment of a VPN using a shared key, e-certificate, or username/password for authentication.

Step 1: Select "VPN Tunnel > OpenVPN Server" in the navigation bar.

Step 2: Openvpn configuration is divided into four configurations

Basic setting

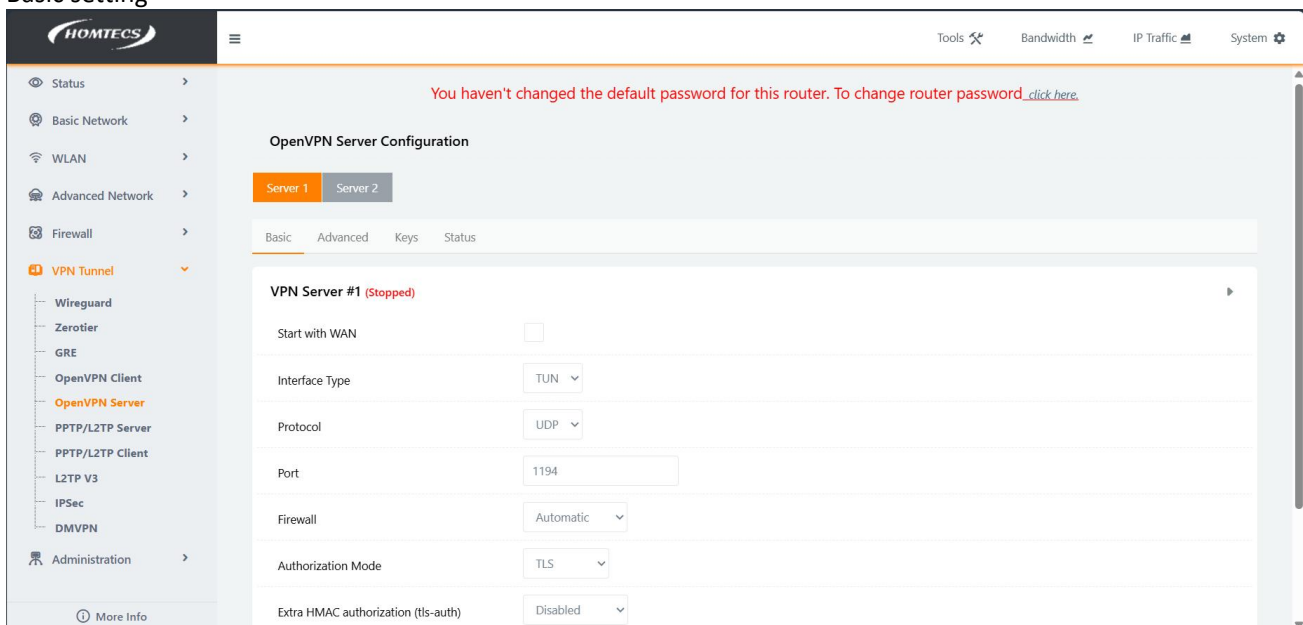


Figure 9-47

Basic Parameter Configuration Description:

Parameter	Meaning	How to configure
via the Internet	Whether the network is over a WAN port	Turn on or off
Interface type	The difference between TUN and TAP is that a TUN device is a point-to-point virtual appliance at the network layer, while TAP is a virtual appliance at the Ethernet link layer. TAP mode: Openvpn bridging mode TUN mode: openvpn tunnel mode	Drop-down to select TAP mode or TUN mode
agreement	TCP mode or UDP mode	Select TCP mode or UDP mode from the drop-down list
Server port	Server port configuration	The default port is 1194
firewall	Firewall modes, including automatic, External Only, and custom	Select automatic, External Only, or custom from the drop-down drop-down
Type of Certification	The authentication types include TLS, static key, and custom	Select TLS, static key, or custom from the drop-down drop-down
Additional HMAC certification	Hash message authentication: Default: Disabled, Bi-directional Incoming (0) Outgoing (1)	Enable or select one of the modes
VPN subnet/netmask	Server subnet address and mask assignment	Format: A.B.C.D/M Default: 10.8.0.0/24

Table 9-8 OpenVPN parameter configuration

Advanced settings:

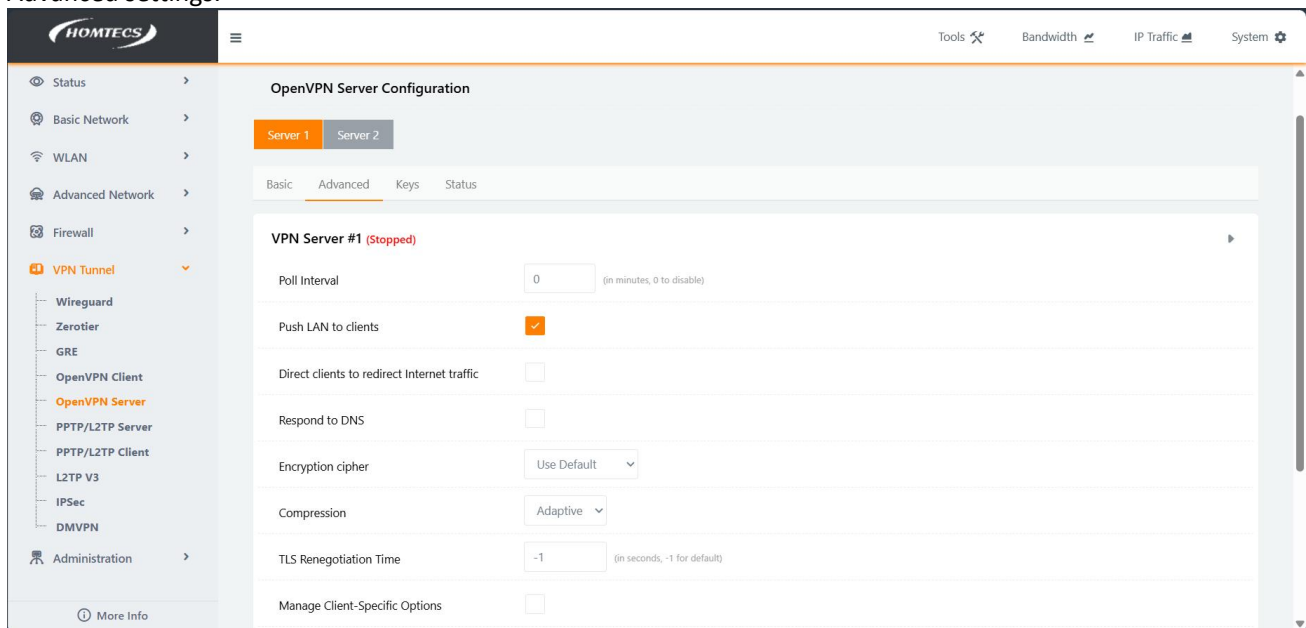


Figure 9-48

Advanced Setup Instructions:

Parameter	Meaning	How to configure
Polling interval	0 is not disabled and is in minutes	0 is disabled, and 0 or greater is enabled
Push the LAN to the client	Push the LAN port route of the server to the client	Enable or disable Enabled by default
Direct the client to redirect network traffic	The server responds to the DNS to the client	Enable or disable Not enabled by default
Respond to DNS	Whether the server will respond to DNS	Enable or disable Not enabled by default
		Enable or disable

Advertise DNS to clients	The server sends DNS to the client	Not enabled by default
Encryption algorithms	Choose from "BF", "DES", "DES-EDE3", "AES128", "AES192", and "AES256". BF: 128-bit encryption algorithm using BF in CBC mode DES: Use DES's 64-bit encryption algorithm in CBC mode DES-EDE3: uses the 192-bit encryption algorithm of 3DES in CBC mode AES128: Use AES's 128-bit encryption algorithm in CBC mode AES192: Use AES's 192-bit encryption algorithm in CBC mode AES256: Uses AES's 256-bit encryption algorithm in CBC mode	Select any one from the drop-down list
compress	4 种压缩模式: disabled, none, enabled, adaptive	Adaptive by default
TLS renegotiation time	-1 is the default in seconds	-1 is the default Enter 0 or higher to enable
Manage client-specific options	After enabled, you can configure whether clients or clients communicate with each other	Enable or disable Not enabled by default
Allow Client < - > Client	Whether client-to-client communication is allowed	Enable or disable Not enabled by default
Clients are allowed	configure which clients the server is allowed to push; Configurations include CommonName, subnet, netmask, and push	Enable or disable Not enabled by default
Allow user/authentication	When enabled, you can configure which users require authentication, The configuration includes a username and password	Enable or disable Not enabled by default
Customization options	Reservation settings	Default is empty

Table 9-9

Key Settings:

Figure 9-49

Key Setup Instructions:

Parameter	Meaning	How to configure
Certificate Authority	Configure certificate authority	Fill in the authorization certificate
Server-side certificates	Configure a server-side certificate	Enter the server certificate
Server key	Configure a server key	Enter the server key
Diffie Hellman parameters	Configure the DH parameter of the server	Enter the DH parameter of the server

Table 9-10

State:

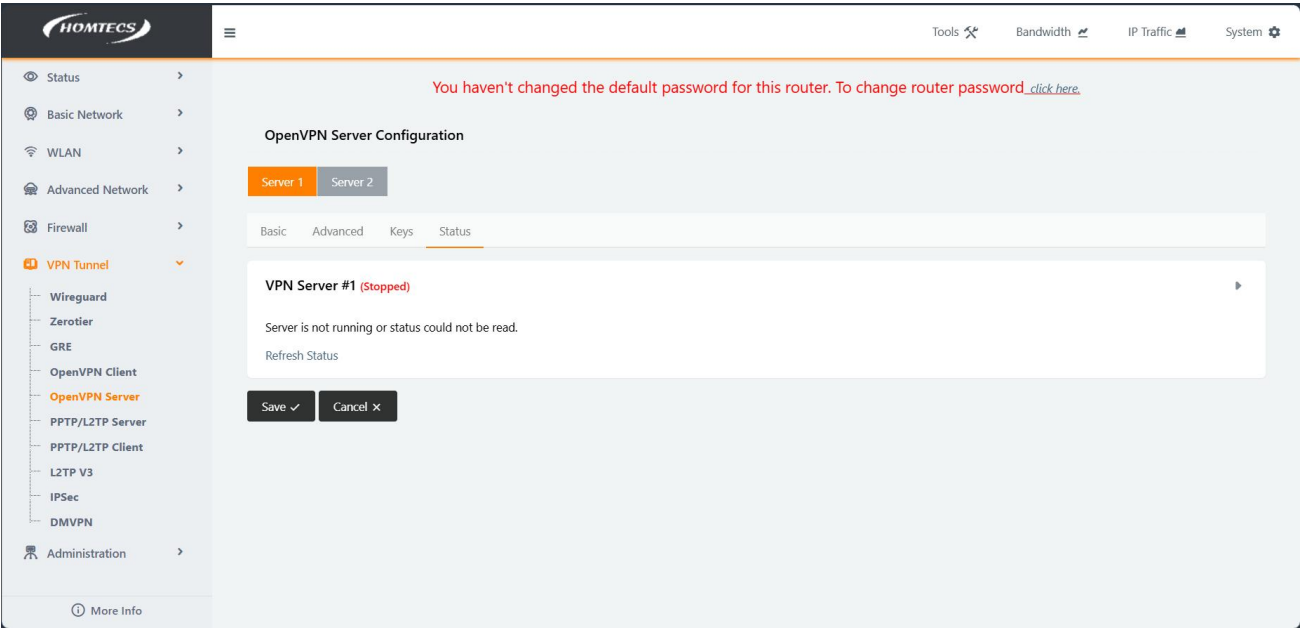


Figure 9-50

Status Description:

Parameter	Meaning	How to configure
Start now	Launch OpenVPN now	Enable or disable
Refresh the state	Manually refresh the OpenVPN link status	To click or not to click

Table 9-11

Example 1:

Example configuration of TUN-TCP

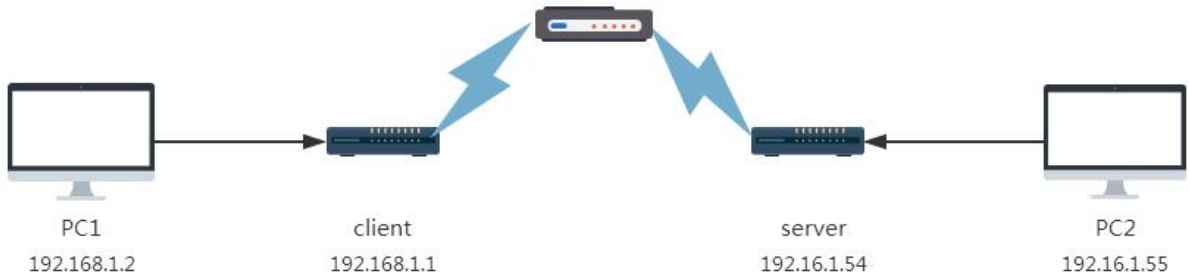


Figure 9-51

Server configuration:

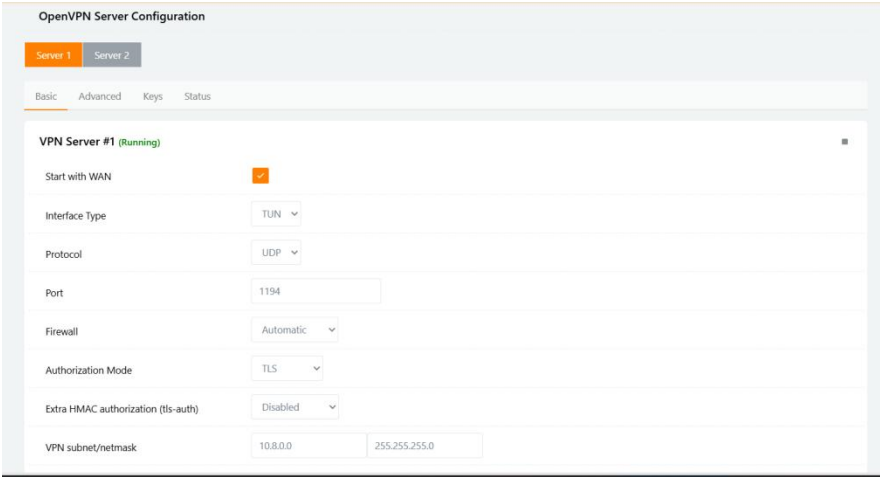


Figure 9-52

BasicAdvancedKeysStatus

VPN Server #1 (Running)

Poll Interval

0

(in minutes; 0 to disable)

Push LAN to clients

☒

Direct clients to redirect Internet traffic

☐

Respond to DNS

☐

Encryption cipher

Use Default

Compression

Adaptive

TLS Renegotiation Time

-1

(in seconds; -1 for default)

Manage Client-Specific Options

☐

Allow User/Pass Auth

☐

Custom Configuration

Figure 9-53

Client Configuration (check Allow Tunnel NAT):

OpenVPN Client

Client 1Client 2

BasicAdvancedKeysStatus

VPN Client #1 (Running)

Start with WAN

☒

Interface Type

TUN

Protocol

UDP

Server Address

192.168.10.69

1194

Firewall

Automatic

Authorization Mode

TLS

Username/Password Authentication

☐

HMAC authorization

Disabled

Figure 9-54

After the link is successful:

OpenVPN Server Configuration

Server 1Server 2

BasicAdvancedKeysStatus

VPN Server #1 (Running)

Data current as of Tue Sep 3 11:19:15 2024.

Client List

Common Name	Real Address	Virtual Address	Virtual IPv6 Address	Bytes Received	Bytes Sent	Connected Since	Connected Since (time_t)	Username	Client ID
client	192.168.10.70:50908	10.8.0.6		29301	29060	Tue Sep 3 09:11:22 2024	1725325882	UNDEF	0

Routing Table

Virtual Address	Common Name	Real Address	Last Ref
10.8.0.6	client	192.168.10.70:50908	Tue Sep 3 09:11:24 2024

General Statistics

Name	Value
Max bcst/mcast queue length	0

Refresh Status

Figure 9-55

Select Allow tunnel NAT, which can ping the same server IP address, but cannot ping the subnet IP address

```
03/09/2024 14:52.40 /home/mobaxterm ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 2ms, 平均 = 1ms

03/09/2024 14:53.06 /home/mobaxterm ping 192.168.1.37

正在 Ping 192.168.1.37 具有 32 字节的数据:
来自 192.168.1.37 的回复: 字节=32 时间=4ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=2ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=3ms TTL=126
来自 192.168.1.37 的回复: 字节=32 时间=2ms TTL=126

192.168.1.37 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 4ms, 平均 = 2ms
```

Figure 9-56

Client configuration (uncheck Allow Tunnel NAT):

Figure 9-57

If you do not select Allow tunnel NAT, you can ping the server IP address and the subnet IP address

TAP-TCP configuration example:

Server:

Figure 9-58

Client Configuration:

Client 1 Client 2

Basic Advanced Keys Status

VPN Client #1 (Running)

Start with WAN ☒

Interface Type TAP

Protocol UDP

Server Address 192.168.10.95 1194

Firewall Automatic

Authorization Mode TLS

Username/Password Authentication ☐

HMAC authorization Disabled

Server is on the same subnet ☒

Figure 9-59

After the link is successful, PC1 can ping the server gateway

```
06/09/2024 10:01:58 /home/mobaxterm ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3ms, 最长 = 5ms, 平均 = 3ms

06/09/2024 10:11:17 /home/mobaxterm ping 192.168.1.254

正在 Ping 192.168.1.254 具有 32 字节的数据:
来自 192.168.1.254 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.1.254 的回复: 字节=32 时间=4ms TTL=64

192.168.1.254 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 3ms, 最长 = 5ms, 平均 = 3ms
```

Figure 9-60

9.6. PPTP/L2TP server

PPTP is an extension of the End-to-End Protocol (PPP) that uses the authentication, compression, and encryption mechanisms provided by PPP, and PPTP can be automatically installed along with the TCP/IP protocol. PPTP and Microsoft End-to-End Encryption (MPPE) technology provide VPN services for encapsulating and encrypting confidential data. MPPE encrypts PPP frames with encryption keys generated by the MS-CHAP and MS-CHAP v2 authentication processes. In order to encrypt valid data contained in PPP frames, the VPN client must use the MS-CHAP, MS-CHAP v2 authentication protocol.

Step 1: Select "VPN Tunnel >PPTP/L2TP Server" in the navigation bar. The specific page is as follows:

HOMTECS VPN Tunnel

PPTP/L2TP Server

Enable ☐

Local IP Address/Netmask 192.168.1.1 / 255.255.255.0

Remote IP Address Range 172.19.0.1 - 172.19.0.6 (6)

Broadcast Relay Mode Disabled Enabling this may cause HIGH CPU usage

Protocol Type PPTP

Encryption MPPE-128

DNS Servers 0.0.0.0

0.0.0.0

WINS Servers 0.0.0.0

0.0.0.0

MTU 1450

Figure 9-61

HOMTECS VPN Tunnel

WINS Servers 0.0.0.0

0.0.0.0

MTU 1450

MRU 1450

Poptop Custom configuration

PPTP/L2TP User List

Username	Password	Static IP Address	Client Subnet Address	Client Subnet Mask
		172.19.0.		

Add +

Save ✓ Cancel ✕

»PPTP/L2TP Online

Figure 9-62

Step 2: PPTP/L2TP Server parameters

Parameters	Meaning	How to configure
Enable	Click Enable	enable
Local IP address/mask	The LAN port IP address and subnet of the router	Varies based on router LAN parameters
Remote IP address/mask	The VPN address of the server	The default value is 172.19.0.1-172.19.0.6
Broadcast relay mode	Trunk mode configuration	The default value is Disabled Disabled, LAN to VPN client, VPN clientto LAN, Both
Protocol Type	Protocol type	Default PTP PPTP/L2TP optional
Encryption	Data is encrypted against the VPN	Default MPPE-128 Optional MPPE-128/NONE
DNS server	The domain name resolution server settings of the VPN	Default 0.0.0.0, 0.0.0.0
WINS server	The VPN's domain name resolution server settings work based on the computer's NetBIOS name	Default 0.0.0.0, 0.0.0.0

MTU	The maximum transmission unit of data, which represents the outgoing traffic processing	Default 1450
MRU	The maximum transmission unit of data, which represents the incoming traffic processed	Default 1450
Poptop Customize the settings	User-defined	Default is empty
List of PPTP/L2TP users	/	/
Username	Username configuration for the server	Default is empty
password	Password configuration for the server	Default is empty
Static IP address	The VPN address assigned by the server to the client (within the range of remote IP addresses)	The default value is 172.19.0
The client subnet address	Subnet IP configuration of the client	Default is empty
Client subnet mask	The mask IP configuration of the client	Default is empty

Table 9-12 PPTP/L2TP server parameters

Step 3: Set the parameters as follows:

The screenshot shows the HOMTECS VPN Tunnel configuration interface. The left sidebar lists various network settings, with 'VPN Tunnel' expanded. The main panel displays the 'PPTP/L2TP Server' configuration. At the top, a red warning message states: 'You haven't changed the default password for this router. To change router password [click here](#).' Below this, the 'PPTP/L2TP Server' section is expanded, showing several configuration fields: 'Enable' (checked), 'Local IP Address/Netmask' (192.168.1.1 / 255.255.255.0), 'Remote IP Address Range' (172.19.0.1 - 172.19.0.6), 'Broadcast Relay Mode' (Disabled), 'Protocol Type' (PPTP), 'Encryption' (MPPE-128), 'DNS Servers' (0.0.0.0), and 'WINS Servers' (0.0.0.0). The bottom of the page has a 'More Info' link.

Figure 9-63

The screenshot shows the HOMTECS VPN Tunnel configuration interface, specifically the 'PPTP/L2TP User List' section. The left sidebar is the same as in Figure 9-63. The main panel shows the 'PPTP/L2TP Server' configuration from Figure 9-63, with additional fields for 'MTU' (1450) and 'MRU' (1450). Below the server settings, the 'PPTP/L2TP User List' section is expanded, showing a table with columns: 'Username', 'Password', 'Static IP Address', 'Client Subnet Address', and 'Client Subnet Mask'. The table contains one entry: 'homtecs123' with password 'Secret', static IP '172.19.0.2', client subnet '192.168.1.50', and client subnet mask '255.255.255.0'. There are 'Add +', 'Save', and 'Cancel' buttons at the bottom. A 'PPTP/L2TP Online' button is located at the bottom right.

Figure 9-64

Step 4: After the client is successfully connected, you can click the PPTP/L2TP online page at the bottom of the server configuration page to view the connection status

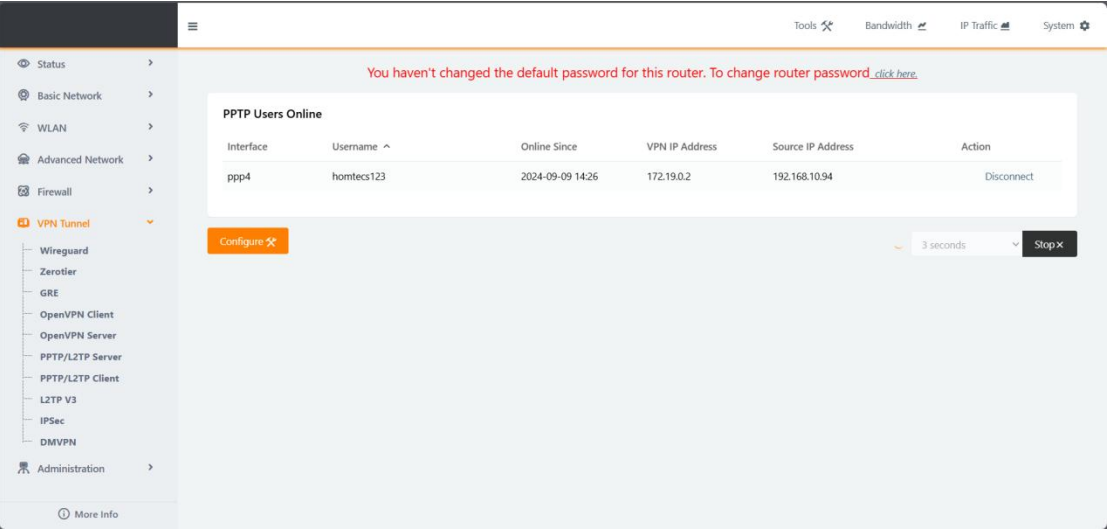


Figure 9-65

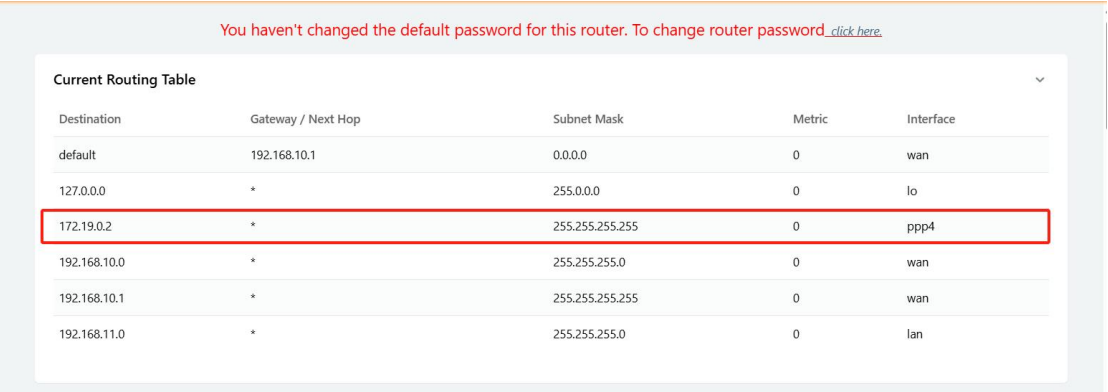


Figure 9-66

telnet enters the backend of the server and can ping the VPN address of the client

```
root@Router:/tmp/home/root#
root@Router:/tmp/home/root# ping 172.19.0.2
PING 172.19.0.3 (172.19.0.3): 56 data bytes
64 bytes from 172.19.0.3: seq=0 ttl=64 time=1.669 ms
64 bytes from 172.19.0.3: seq=1 ttl=64 time=1.442 ms
64 bytes from 172.19.0.3: seq=2 ttl=64 time=1.439 ms
64 bytes from 172.19.0.3: seq=3 ttl=64 time=1.444 ms
64 bytes from 172.19.0.3: seq=4 ttl=64 time=1.449 ms
^C
--- 172.19.0.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.439/1.488/1.669 ms
```

Figure 9-67

The client page is connected to the following link, and you can ping the IP address of the server



Figure 9-68

```

09/09/2024 14:26.47 /home/mobaxterm ping 192.168.11.1

正在 Ping 192.168.11.1 具有 32 字节的数据:
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63

192.168.11.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms

09/09/2024 14:31.40 /home/mobaxterm ping 192.168.11.1

正在 Ping 192.168.11.1 具有 32 字节的数据:
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63
来自 192.168.11.1 的回复: 字节=32 时间=1ms TTL=63

192.168.11.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms

```

Figure 9-69

9.7. L2TP/PPTP client

PPTP(Point to Point Tunneling Protocol) is a network technology that supports multi-protocol virtual private networks, and it is also a layer 2 protocol. Through this protocol, remote users can securely access the corporate network through the mainstream Windows operating system and other systems with point-to-point protocols, and can dial up to the local ISP to securely connect to the corporate network over the Internet.

L2TP (Layer Two Tunneling Protocol) is an abbreviation for Layer 2 Tunneling Protocol, which is a type of VPDN (Virtual Private Dial-up Network) technology, which is specially used for Layer 2 data channel transmission. L2TP provides a means of remote access access control, and its typical application scenario is that an employee of a company dials in to the company's local network access server (NAS) through PPP to access the company's internal network and obtain an IP address and access the network resources with the appropriate permissions. The employee dials in to the corporate network as securely and conveniently as they would on the corporate LAN.

L2TP protocol configuration:

Step 1: Select "VPN Tunnel > PPTP/L2TP Client" in the navigation bar. In the page that opens, you can select an L2TP client from the drop-down list and modify the relevant parameters.

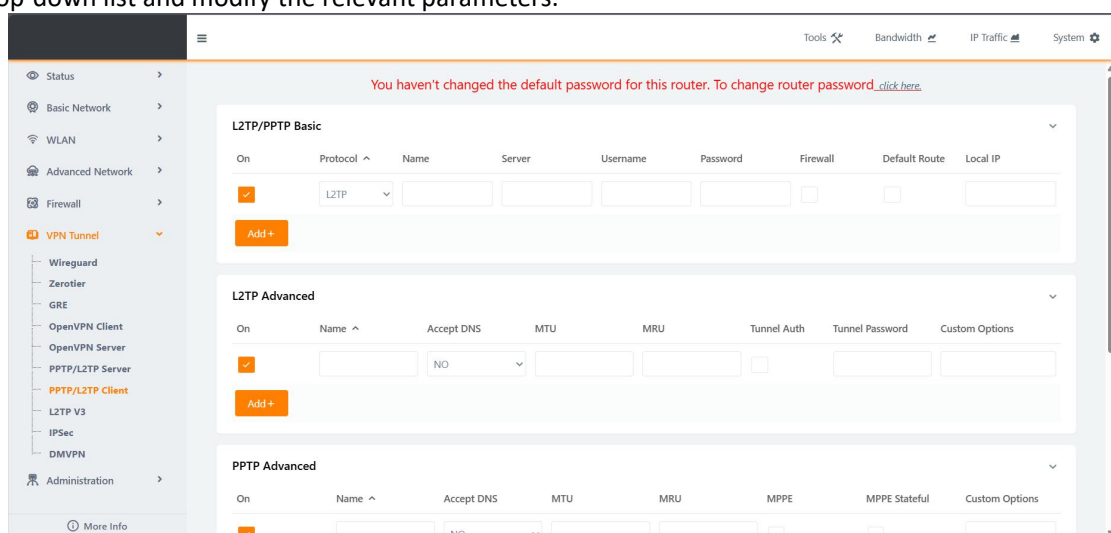


Figure 9-70

Step 2: L2TP description

Parameter	Meaning	How to configure
Enable	Click Enable	enable
Agreement	Select the client mode	Select L2TP/PPTP
name	Set the name of the client	Null
Server address	The IP address or domain name of the server used for access.	Fill in the IP address or domain name of the server
Username	A legitimate user who has been authorized to access the access server.	Fill in the username that the server has authorized
Password	The access server has authorized a valid user password.	Fill in the password that the server has authorized
Firewall	Set up a firewall	Tick/Unchecked
Default route	Set the default route	Tick/Unchecked
Local IP	Set the local IP address	Null
Receives the peer DNS	Accept L2TP Server to assign DNS addresses	YES/NO
MTU	Set the MTU parameters	1500
MRU	Set MRU parameters	1500
Tunnel authentication	Configure tunnel authentication	Tick/Unchecked
Tunnel password	Set a tunnel password	Null
Customize dialing options	Set up custom dialing content	Null

Table 9-13 L2TP configuration

PPTP protocol configuration:

Step 1: Select "VPN Tunnel >PPTP Client" in the navigation bar. In the page that opens, you can select an PPTP client from the drop-down list and modify the relevant parameters.

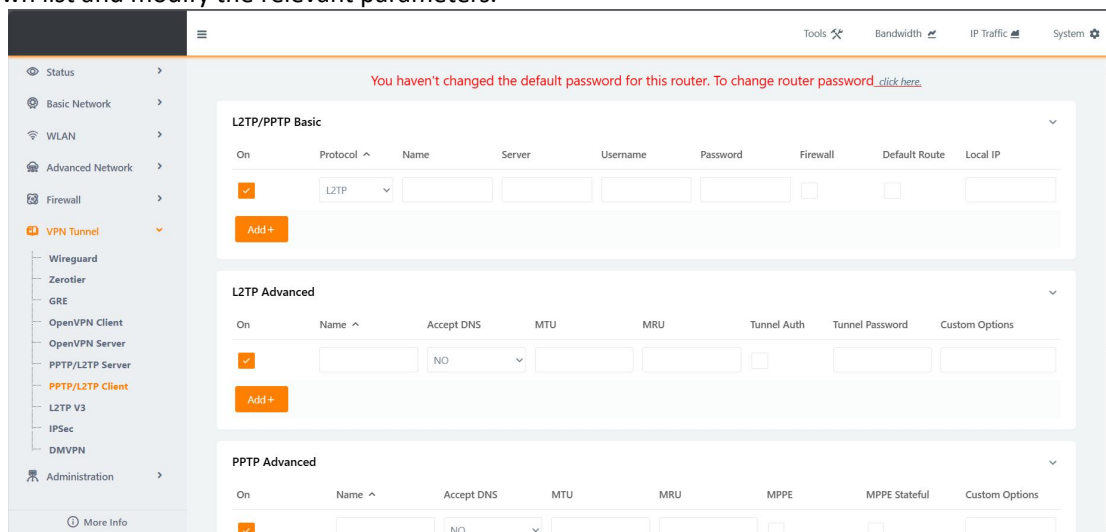


Figure 9-71

Step 2: PPTP parameters.

Parameter	Meaning	How to configure
Client-side mode	Select the client mode	L2TP or PPTP
Name	Set the name of the client	Null
Service address	The IP address or domain name of the server used for access.	Fill in the IP address or domain name of the server
Username	A legitimate user who has been authorized to access the access server.	Fill in the username that the server has authorized
Password	The access server has authorized a valid user password.	Fill in the password that the server has authorized
Firewall	Set up a firewall to allow the VPN to channel the NAT	Tick/unchecked
Default route	Set the default route for all data to go through VPN	Tick/Unchecked

Local IP	Set the local IP address of the specified VPN client	Null
Accept the peer DNS configuration	Accept the DNS Server Address assigned by the PPTP Server	Disable or enable
MTU	Set the MTU parameters	1500
MRU	Set MRU parameters	1500
MPPE encryption mode	Encryption options	Tick/Unchecked
MPPE connection status	Set the MPPE connection status	Tick/Unchecked
Customize dialing options	Set custom dialing options	If you need this option, you must contact our technical support

Table 9-14 VPN PPTP Parameter Configuration

Step 3: Save the settings and complete the VPN rule settings.

Example:

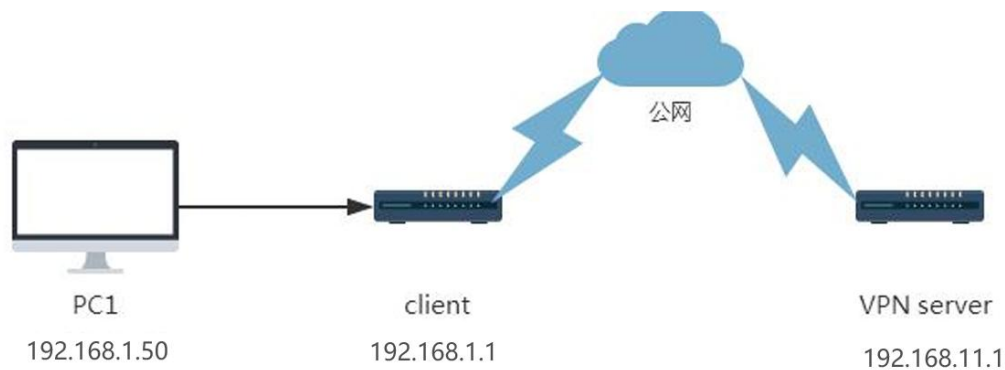


Figure 9-72

Configure PPTP, bring the router 4G/5G online, and link to the PPTP server

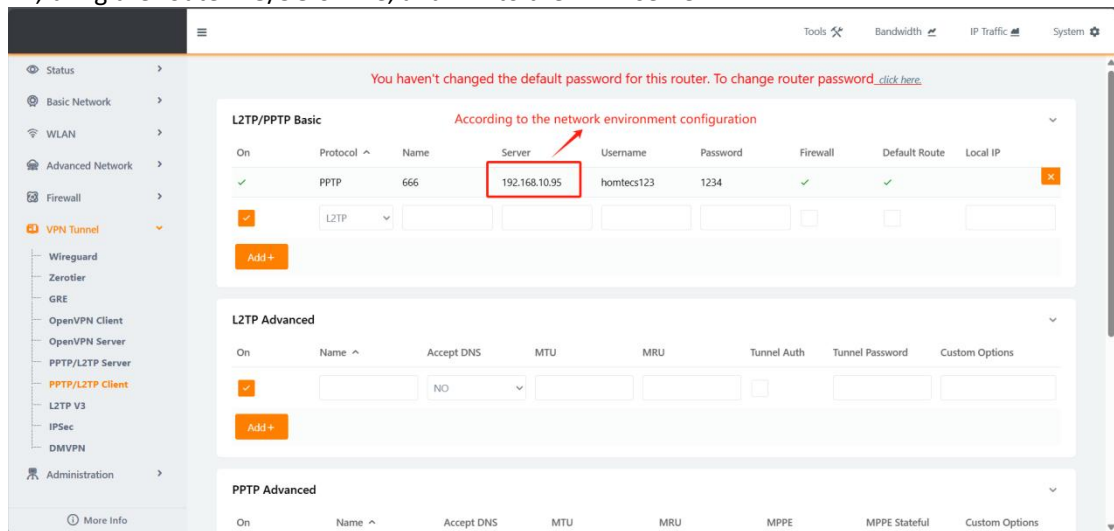


Figure 9-73

Configure PPTP, bring the router 4G/5G online, and link to the PPTP server

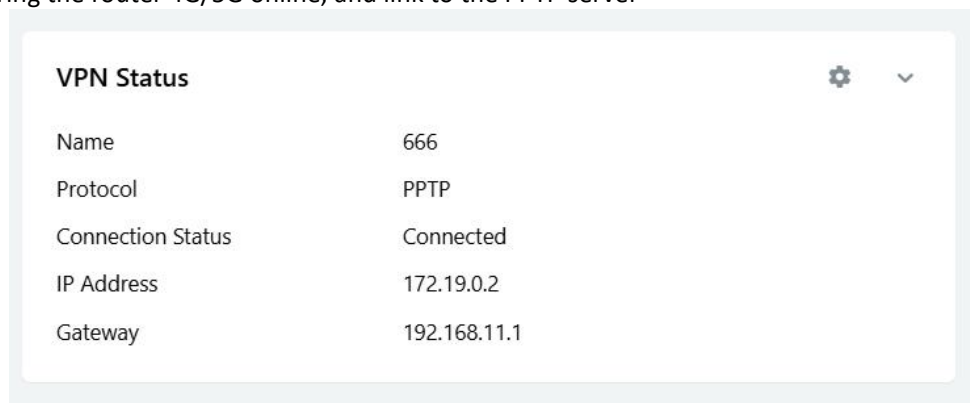


Figure 9-74

The PC can ping the PPTP server gateway through the router Internet access

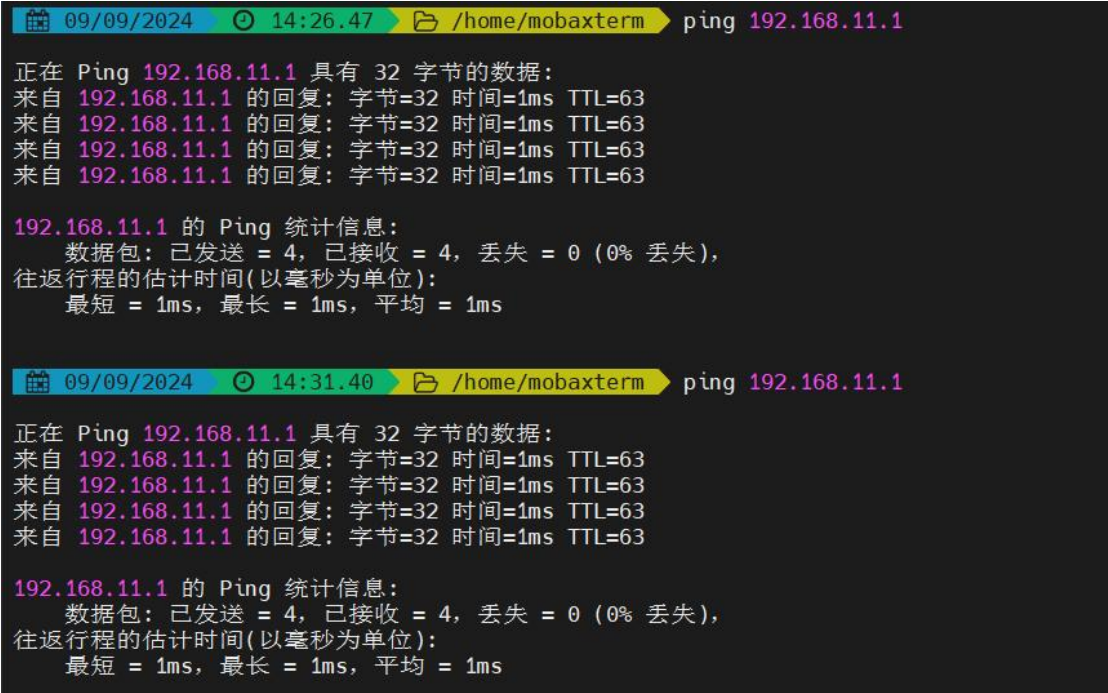


Figure 9-75

Example 2: Uncheck Default Route

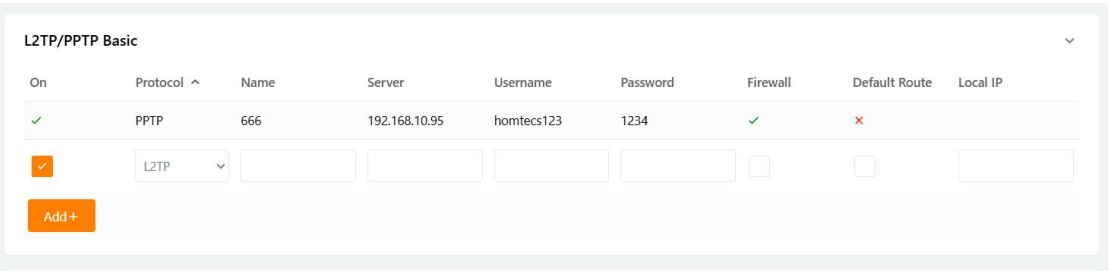


Figure 9-76

9.8. L2TPv3

L2TPv3 (Layer Two Tunneling Protocol - Version 3) is a Layer 2 tunneling technology that transparently transmits multiple Layer 2 packets (such as PPP, Ethernet, HDLC, and ATM) and transparently transmits Layer 2 access links on the user side in packet-switched networks. L2TPv3 is an L2VPN solution for IP-based networking. L2TPv3 is formerly Cisco's proprietary protocol, --- Universal Transport Protocol (UTI).

Step 1: Select "VPN Tunnel > L2TPv3" in the navigation bar.

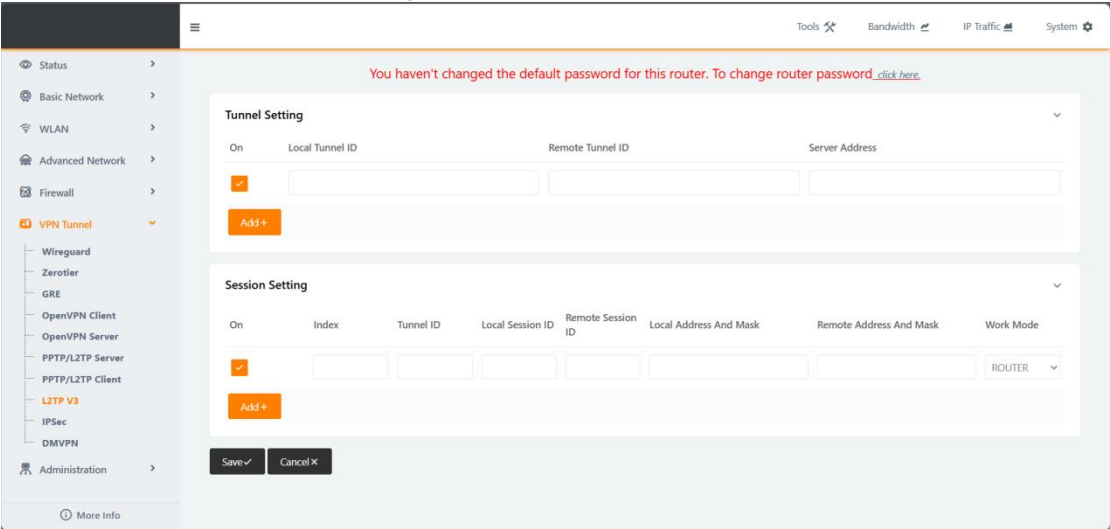


Figure 9-77

Step 2: L2TPv3 parameters

Parameter	Meaning	How to configure
Local tunnel ID	Local tunnel ID	Default is empty
ID of the peer tunnel	ID of the peer tunnel	Default is empty
Server address	The address of the peer WAN port	Default is empty Format: A.B.C.D,
Session setting sequence number	serial number	Default is empty
Session Setup Tunnel ID	Tunnel ID	Default is empty
Local session ID	Local session ID	Default is empty
The ID of the peer session	The ID of the peer session	Default is empty
Local tunnel address and mask	Local tunnel address and subnet	Format: A.B.C.D/M Default is empty
Peer tunnel address and mask	The address and subnet of the peer tunnel	Format: A.B.C.D/M Default is empty
Working mode	It is divided into routing, gateway and bridging	The route mode is selected by default

Table 9-15 L2TP V3 parameters

Step 3: Set the parameters as follows:

R1: local IP address 192.168.1.1/32, WAN port IP address 192.168.10.77

You haven't changed the default password for this router. To change router password [click here](#).

Tunnel Setting

On	Local Tunnel ID	Remote Tunnel ID	Server Address
<input checked="" type="checkbox"/>	1	1	192.168.10.95
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

[Add +](#)

Session Setting

On	Index	Tunnel ID	Local Session ID	Remote Session ID	Local Address And Mask	Remote Address And Mask	Work Mode
<input checked="" type="checkbox"/>	1	1	11	11	10.5.1.1/32	10.5.1.2/32	ROUTER
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	ROUTER

[Add +](#)

[Save](#) [Cancel](#)

Figure 9-78

R2: local IP address 192.168.2.1/32, WAN port IP address 192.168.10.169

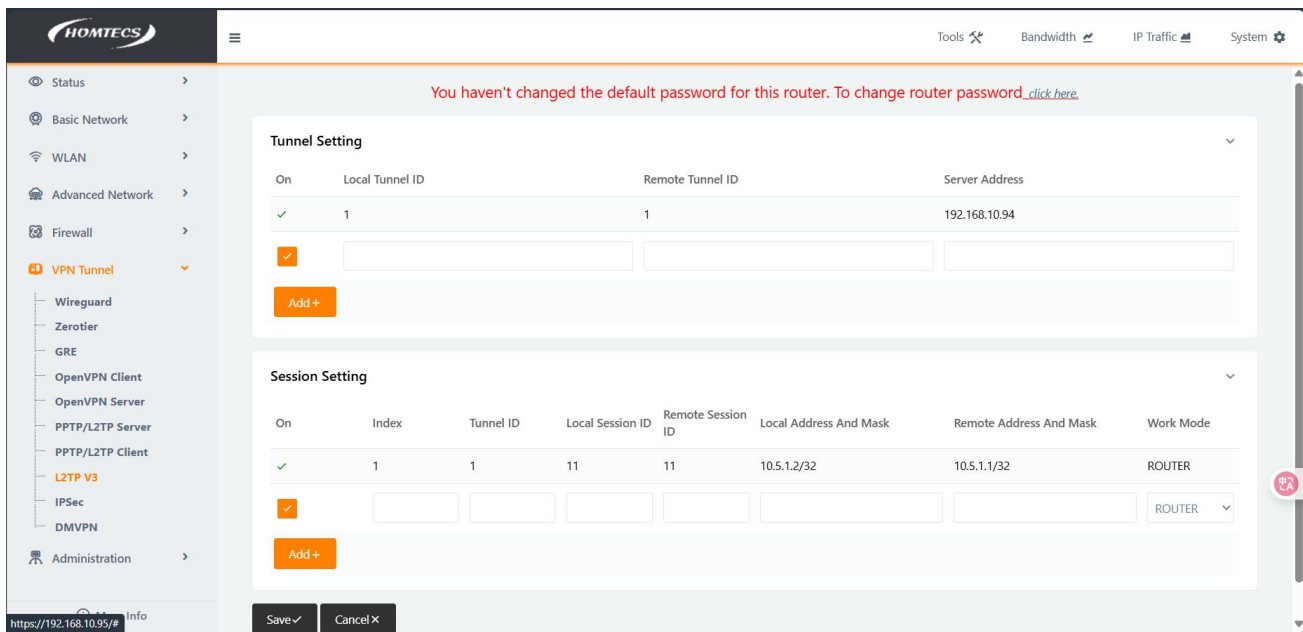


Figure 9-79

After the connection is established, you can view the information through the route tables of R 1 and R 2, and ping the tunnel address and gateway IP address of the peer end

R1 :

Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
10.4.168.0	*	255.255.255.0	0	modem
10.5.1.2	*	255.255.255.255	0	l2tpeth1
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	lan
192.168.2.0	*	255.255.255.255	0	l2tpeth1
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan

Figure 9-80

```

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.553 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.824 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.727 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.792 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.845 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.727/0.948/1.553 ms

root@Router:/tmp/home/root# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=0.324 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=0.252 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=0.232 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=0.293 ms
64 bytes from 192.168.2.1: seq=4 ttl=64 time=0.310 ms
^C
--- 192.168.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.232/0.282/0.324 ms

```

Figure 9-81

R2:

Current Routing Table				
Destination	Gateway / Next Hop	Subnet Mask	Metric	Interface
default	192.168.10.1	0.0.0.0	0	wan
10.5.1.1	*	255.255.255.255	0	l2tpeth1
127.0.0.0	*	255.0.0.0	0	lo
192.168.1.0	*	255.255.255.0	0	l2tpeth1
192.168.2.0	*	255.255.255.0	0	lan
192.168.10.0	*	255.255.255.0	0	wan
192.168.10.1	*	255.255.255.255	0	wan

Figure 9-82

```
root@Router:/tmp/home/root# ping 10.5.1.1
PING 10.5.1.1 (10.5.1.1): 56 data bytes
64 bytes from 10.5.1.1: seq=0 ttl=64 time=1.041 ms
64 bytes from 10.5.1.1: seq=1 ttl=64 time=0.829 ms
64 bytes from 10.5.1.1: seq=2 ttl=64 time=0.805 ms
64 bytes from 10.5.1.1: seq=3 ttl=64 time=0.818 ms
64 bytes from 10.5.1.1: seq=4 ttl=64 time=0.807 ms
^C
--- 10.5.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.805/0.860/1.041 ms

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=0.919 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.687 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.660 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.690 ms
^C
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.660/0.739/0.919 ms
```

Figure 9-83

9.9. IPSec

IPSec is a protocol built on top of the Internet Protocol (IP) layer that enables two or more hosts to communicate in a secure manner. IPSec is the long-term direction for secure networking. It provides proactive protection against attacks on private networks and the Internet through end-to-end security.

Step 1: Select "VPN Tunnel > IPSec" in the navigation bar.

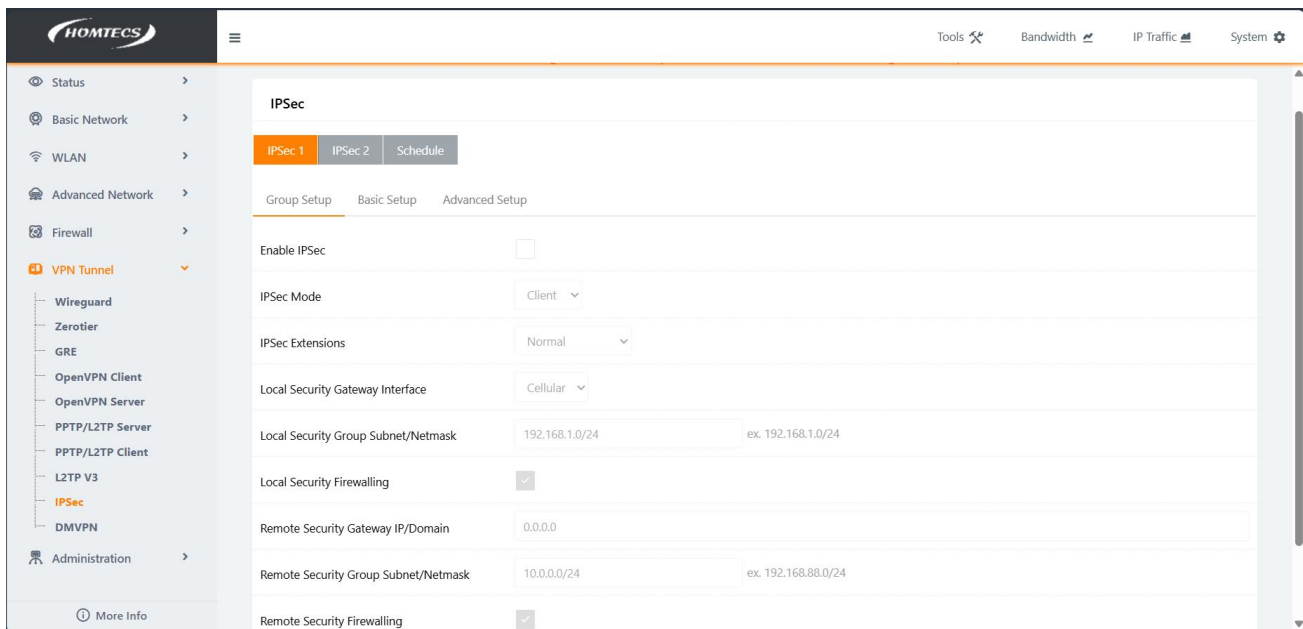


Figure 9-85

Step 2: This IPsec page is divided into two phases of configuration.

1. The first stage parameter configuration interface is shown in the following figure:

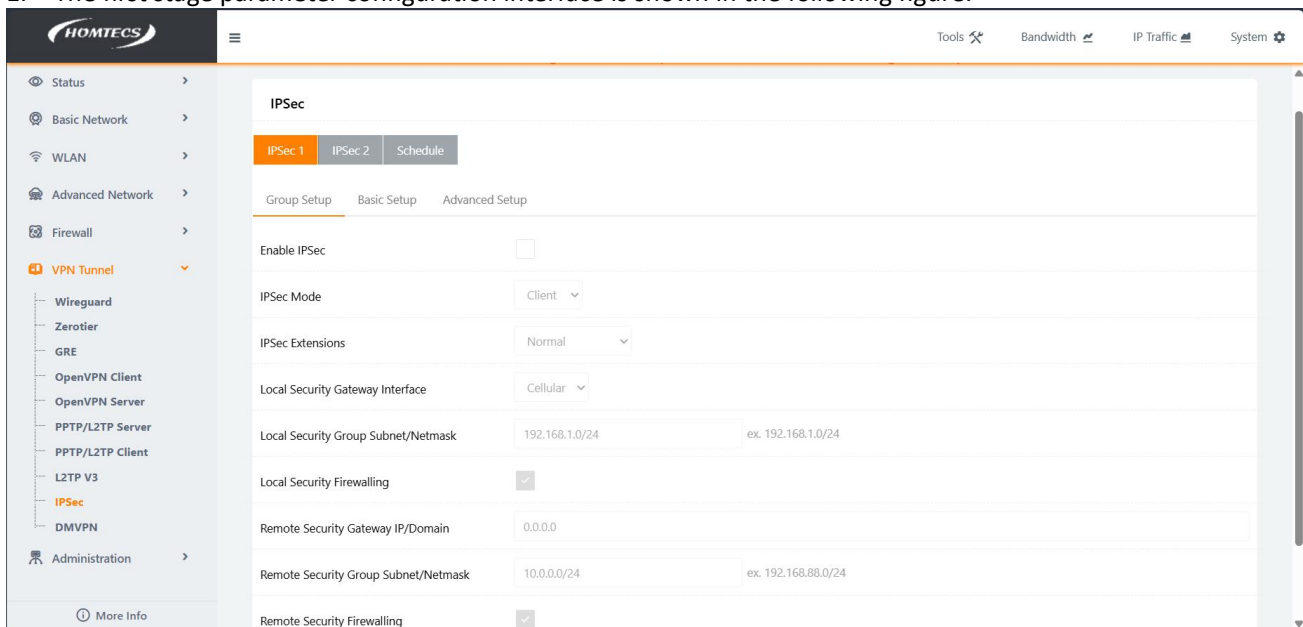


Figure 9-86

IPsec description of the first stage:

Parameter	Meaning	How to configure
Enable IPsec	Specifies whether to enable IPsec configuration	Enabled or not enabled
IPsec extension	Three IPsec networking methods: Normal IPsec/GRE Over IPsec/L2TP Over IPsec	Configure the networking mode of the server corresponding to the Yes
Local security group subnet	Local subnet configuration	You do not need to configure subnets in transmission mode, but you need to configure them in automatic and tunnel modes. Enter the local subnet address. Format: A.B.C.D/M,
On-premise security firewall	Whether the firewall is enabled	Enabled or not enabled
IP address/domain name of the remote security gateway	IPsec server IPO or domain name	

Remote security group subnet	Remote subnet configuration	You do not need to configure subnets in transmission mode, but you need to configure them in automatic and tunnel modes. Enter the remote subnet address. Format: A.B.C.D/M,
Remote Security Firewall	Whether the firewall is enabled	Enabled or not enabled

Table 9-16 IPSec Phase 1 Parameter Configuration

After the configuration is complete, click the Save Settings button for the configuration to take effect.

2. Figure 9-30 shows the parameters in the second stage.

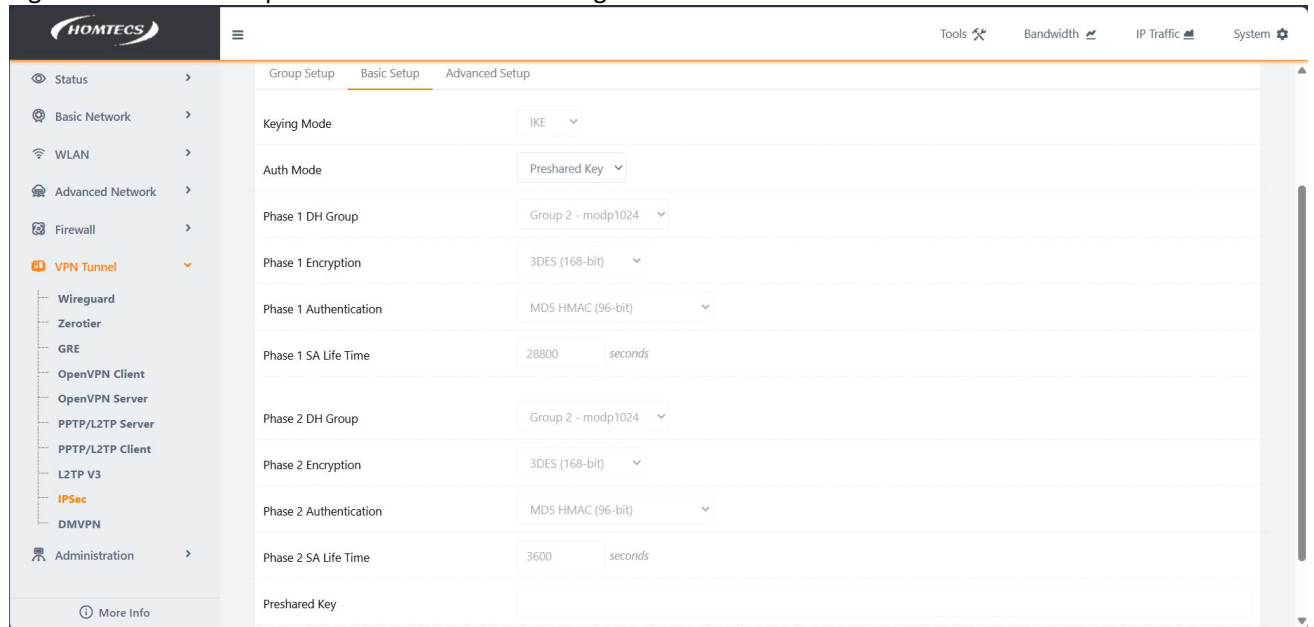


Figure 9-87

IPSec description of the second stage:

Parameter	Meaning	How to configure
DH Group	Use this setting when enabling perfect forward encryption. This setting is configured for the key length of the IPSec phase II SA negotiation	Select from the drop-down column Table Select the appropriate group name from the drop-down column Table
Encryption	Supports three encryption methods: des, 3des and aes	Select the drop-down column Table Select the appropriate group name from the drop-down column Table
SA Life Time	IPSec SA (IPSec Security Association) encryption lifetime	Fill in the appropriate key life cycle Value range: 120~86400 Unit: seconds

Table 9-17 IPSet Phase II parameters

Configuration example:

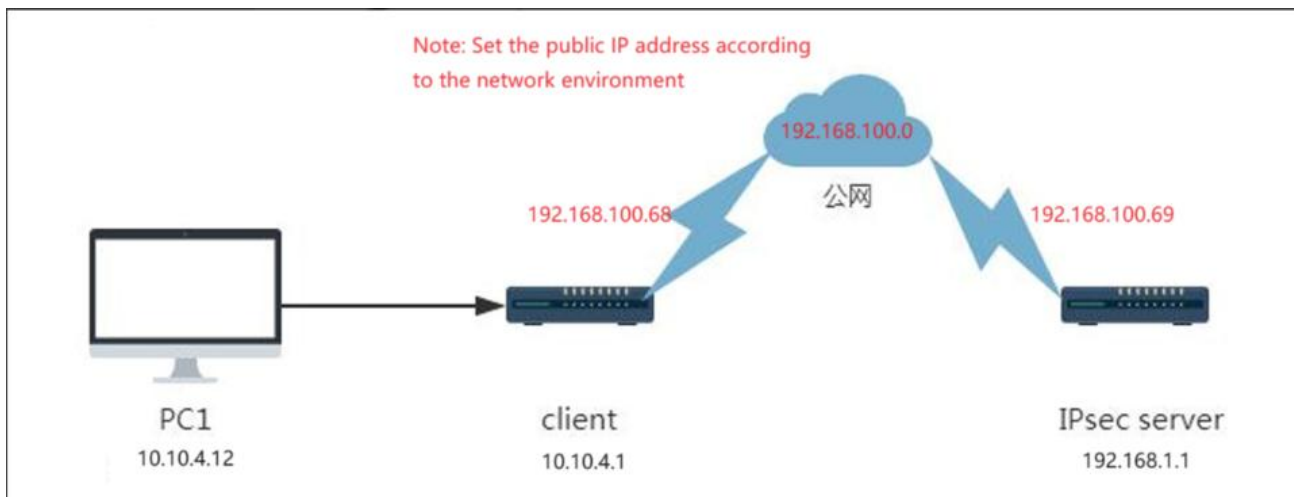


Figure 9-88

Group Setup:

IPSec

IPSec 1 | IPSec 2 | Schedule

Group Setup | Basic Setup | Advanced Setup

Enable IPSec ☒

IPSec Mode Server

IPSec Extensions Normal

Local Security Gateway Interface Cellular

Local Security Group Subnet/Netmask 192.168.1.0/24 ex. 192.168.1.0/24 Local LAN port IP

Local Security Firewalling ☒

Remote Security Gateway IP/Domain 0.0.0.0

Remote Security Group Subnet/Netmask 10.10.4.0/24 ex. 192.168.88.0/24 LAN IP of the remote device

Remote Security Firewalling ☒

Figure 9-89

Basic Setup:

Default parameters

Group Setup | Basic Setup | Advanced Setup

Keying Mode IKE

Auth Mode Preshared Key

Phase 1 DH Group Group 2 - modp1024

Phase 1 Encryption 3DES (168-bit)

Phase 1 Authentication MD5 HMAC (96-bit)

Phase 1 SA Life Time 28800 seconds

Phase 2 DH Group Group 2 - modp1024

Phase 2 Encryption 3DES (168-bit)

Phase 2 Authentication MD5 HMAC (96-bit)

Phase 2 SA Life Time 3600 seconds

Preshared Key

Figure 9-90

IPSec client:
Group Setup:

IPSec

IPSec 1IPSec 2

Group SetupBasic SetupAdvanced Setup

Enable IPSec

☒

IPSec Extensions

Normal

Local Security Gateway Interface

3G Cellular

Local Security Group Subnet/Netmask

10.10.4.0/24

ex. 192.168.1.0/24

Local Security Firewalling

☒

Remote Security Gateway IP/Domain

192.168.10.69

WAN port IP of remote device

Remote Security Group Subnet/Netmask

192.168.1.0/24

ex. 192.168.88.0/24 or 192.168.88.0/24,192.168.89.0/24

Remote Security Firewalling

☒

Note: The public IP address shown in the figure is set based on the current network environment

Basic Setup:

Default parameters

IPSec 1IPSec 2

Group SetupBasic SetupAdvanced Setup

Keying Mode

IKE with Preshared Key

Phase 1 DH Group

Group 2 - modp1024

Phase 1 Encryption

3DES (168-bit)

Phase 1 Authentication

MD5 HMAC (96-bit)

Phase 1 SA Life Time

28800

seconds

Phase 2 DH Group

Group 2 - modp1024

Phase 2 Encryption

3DES (168-bit)

Phase 2 Authentication

MD5 HMAC (96-bit)

Phase 2 SA Life Time

3600

seconds

Preshared Key

Advanced Setup:

Default parameters

IPSec 1IPSec 2

Group SetupBasic SetupAdvanced Setup

Aggressive Mode

Compress(IP Payload Compression)

Dead Peer Detection(DPD)

ICMP Check

IPSec Custom Options 1

IPSec Custom Options 2

IPSec Custom Options 3

IPSec Custom Options 4

After the configuration is completed and the connection is successful, the IP addresses of the client and server can ping each other, increasing the amount of incoming and outgoing traffic through Ipsec.

Client ping sever:

```

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=3ms TTL=127
来自 192.168.1.1 的回复: 字节=32 时间=1ms TTL=127

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 2, 丢失 = 2 (50% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 2ms, 平均 = 1ms

29/08/2024 11:47:28 /home/mobaxterm ping 192.168.1.1

```

VPN Status

VPN Mode	Openvpn Client1
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Connection Status	Disconnected
VPN Mode	Openvpn Client2
Local IP Address	0.0.0.0
Remote IP Address	0.0.0.0
Connection Status	Disconnected
IPSec 1	Connected
Phase 1 Status	11 seconds
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_MD5_96
IPSec Recv.	780 bytes
IPSec Send.	780 bytes

Sever ping client:

VPN Status

IPSec 1	Connected
Phase 1 Status	3 minutes
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_MD5_96/MODP_1024
IPSec Recv.	113782 Bytes
IPSec Send.	22207 Bytes

```

正在 Ping 10.10.4.1 具有 32 字节的数据:
来自 10.10.4.1 的回复: 字节=32 时间=1ms TTL=127
来自 10.10.4.1 的回复: 字节=32 时间=1ms TTL=127
来自 10.10.4.1 的回复: 字节=32 时间=11ms TTL=127
来自 10.10.4.1 的回复: 字节=32 时间=5ms TTL=127

10.10.4.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 1ms, 最长 = 11ms, 平均 = 4ms

29/08/2024 11:50:51 /home/mobaxterm

```

Note: The usage of IPSec server is based on data transmission between clients with limited access.

9.10. DMVPN

DMVPN is a highly scalable IPSec VPN solution, and the so-called high scalability refers to the solution suitable for large-scale deployment at the enterprise level, for example, for a network environment where an enterprise has hundreds of branch offices. Due to the limitations of the traditional IPSec VPN star network topology, the central site configuration is large, the traffic delay between branch sites is large, the maintenance cost is too large, and each branch site requires a fixed IP address, so the traditional IPSec is no longer applicable. DMVPN has simple configuration, good performance, supports dynamic IP addresses, provides a fully interconnected topology, zero packet loss, and supports multicast from branch structure to center. It consists of four basic components, namely mGRE, NHRP, Dynamic Routing Protocol, and IPSec.

Step 1: Select "VPN Tunnel>DMVPN" in the navigation bar.

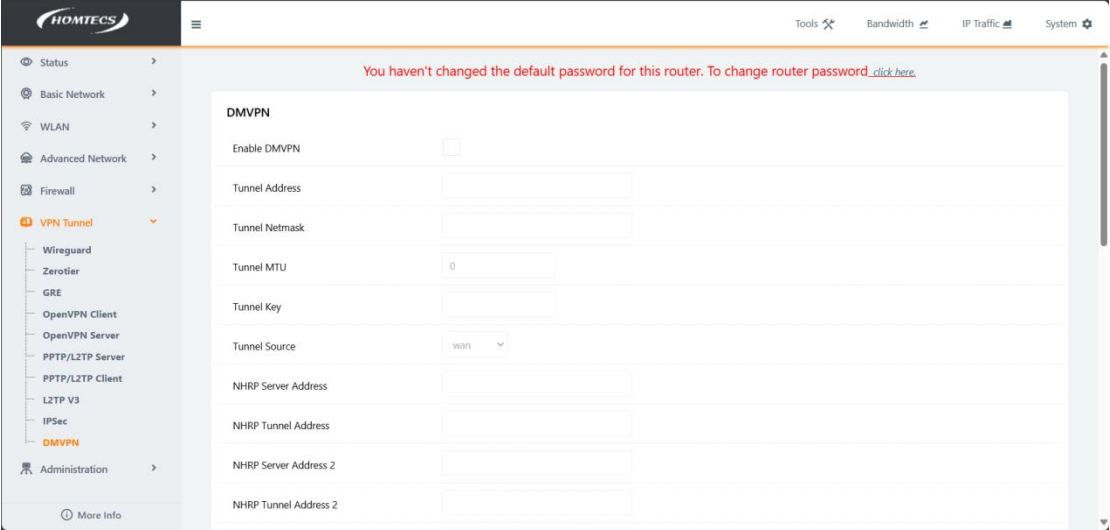


Figure 9-92

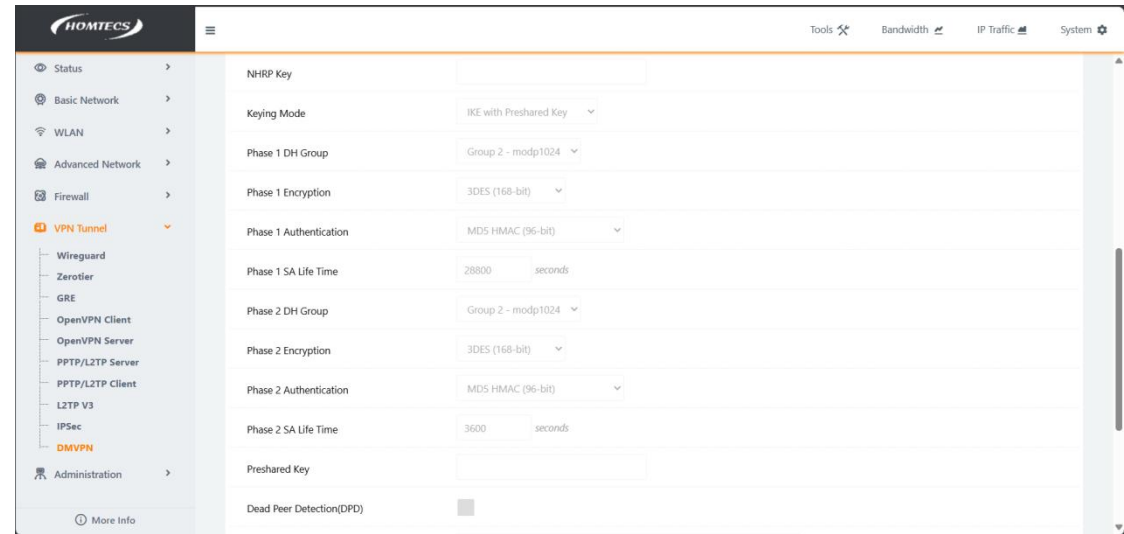
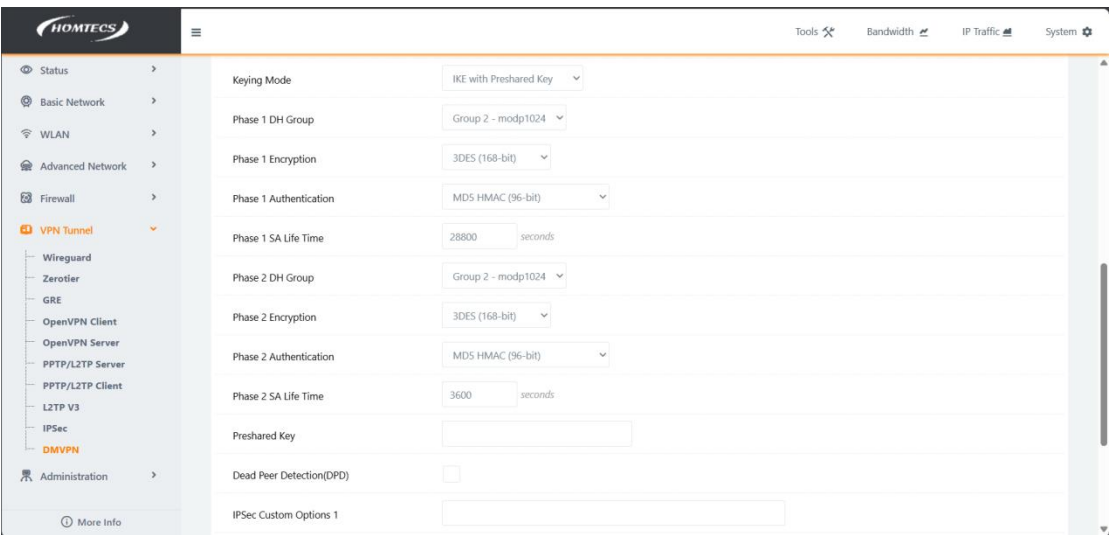


Figure 9-93



Step 2: The DMVPN parameters page is divided into two pages: DMVPN and BGP configuration:

DMVPN parameters are described as follows:

Parameter	Meaning	How to configure
Enable DMVPN	D Enabling and disabling MVPN	The default is disabled
Tunnel address	The tunnel address of the GRE	Default is empty; Format: A. B.C.D/M

Tunnel mask	Tunnel mask for GRE	Default is empty; Format: A. B.C.D/M
Tunnel MTU	GRE tunnel MTU value	The default is 0; Range: 0-2000
Tunnel key	GRE tunnel key	Default is empty;
The source address of the tunnel	Contains modem, wan, sta, sta2	Default: modem
Key mode	I KE/IKE v2 is supported	Default IKE
Stage 1/Stage 2 DH group	Group 1, Group2, Group5 are supported	Default Group2
Phase 1/Phase 2 Encryption Methods	Supports 3DES,AS-128, AES-192, AES-256	Default 3DES
Phase 1/Phase 2 Certification Methodology	Support NONE, MD5, SHA1, SHA2	Default MD5
Phase 1 SA is in force	The duration of the SA in Phase 1	The default is 28800 Unit: seconds Range: 1-86400
Phase 2 SA effective time	The duration of the SA in Phase 2	The default is 28800 Unit: seconds Range: 1-86400
Pre-shared key	The key of the IPSec must be the same as that of the server	Default is empty
DPD function	Enabling and disabling digital distortion detection	Default: Disabled
Detection cycle	The interval between the tests once	Default: 30 Unit: seconds Range: 1-86400
Detect timeout intervals	IPSec detection timeout period	Default: 150 Unit: seconds Range: 1-86400
IPSec Custom Options 1-4	IPSec custom content	Default is empty

Table 9-18 DMVPN parameters

Step 3:D configure the parameters on the MVPN page (including the BGP parameters on the Route Table Settings page).

HOMECS

Tools

Bandwidth

IP Traffic

System

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

Wireguard

Zerotier

GRE

OpenVPN Client

OpenVPN Server

PPTP/L2TP Server

PPTP/L2TP Client

L2TP V3

IPSec

DMVPN

Administration

More Info

You haven't changed the default password for this router. To change router password, [click here](#).

DMVPN

Enable DMVPN

Tunnel Address

172.16.1.2

Tunnel Netmask

255.255.255.0

Tunnel MTU

0

Tunnel Key

Tunnel Source

wan

NHRP Server Address

192.168.10.94

NHRP Tunnel Address

172.16.1.1

NHRP Server Address 2

NHRP Tunnel Address 2

Figure 9-94

HOMECS

Tools

Bandwidth

IP Traffic

System

Status

Basic Network

WLAN

Advanced Network

Firewall

VPN Tunnel

Wireguard

Zerotier

GRE

OpenVPN Client

OpenVPN Server

PPTP/L2TP Server

PPTP/L2TP Client

L2TP V3

IPSec

DMVPN

Administration

More Info

NHRP Tunnel Address 2

NHRP Key

Keying Mode

IKE with Preshared Key

Phase 1 DH Group

Group 2 - modp1024

Phase 1 Encryption

3DES (168-bit)

Phase 1 Authentication

MD5 HMAC (96-bit)

Phase 1 SA Life Time

28800

seconds

Phase 2 DH Group

Group 2 - modp1024

Phase 2 Encryption

3DES (168-bit)

Phase 2 Authentication

MD5 HMAC (96-bit)

Phase 2 SA Life Time

3600

seconds

Preshared Key

Force Peer Authentication (VPN)

Figure 9-95

HOMECS

Tools

Bandwidth

IP Traffic

System

Status

Basic Network

WAN

Cellular

LAN

IPv6

VLAN

Schedule

DDNS

Routing

WLAN

Advanced Network

Firewall

VPN Tunnel

Administration

More Info

BGP

Enable BGP

Custom Configuration

BGP Instance

On	AS	Router ID	Description
✓	65000	172.16.1.1	
✓			

Add +

BGP Network

On	AS	Network	Description
✓	65000	192.168.1.0	
✓			

Add +

Figure 9-96

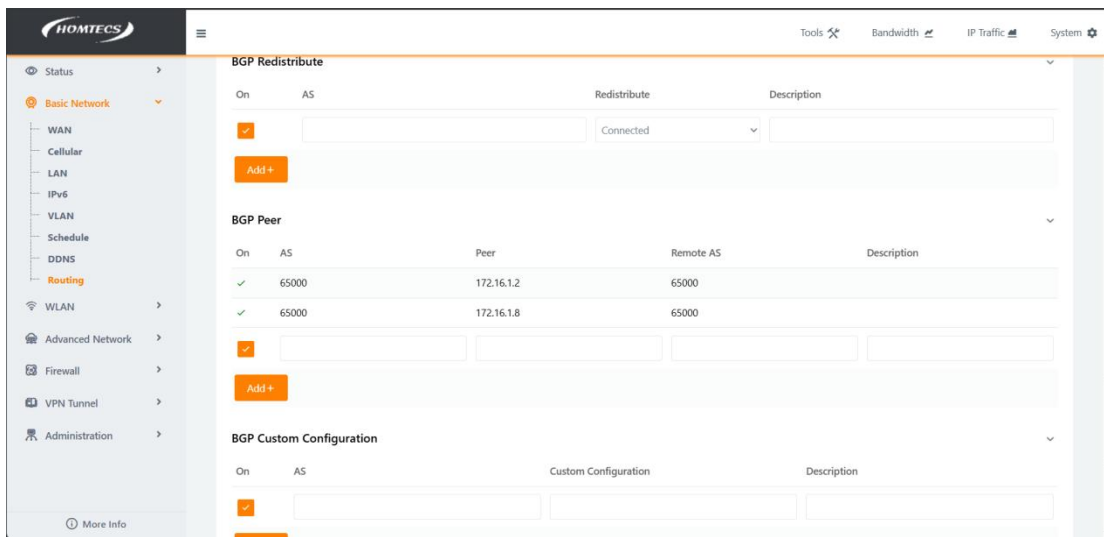


Figure 9-97

Step 4: After the configuration is complete, view the information about the route table, as follows:

R1

```

root@Router:/tmp/etc# route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.10.1   0.0.0.0         UG    0     0          0 vlan2
127.0.0.0        0.0.0.0        255.0.0.0       U     0     0          0 lo
172.16.1.0       172.16.1.2     255.255.255.0   UG    0     0          0 dmvpn
172.16.1.2       0.0.0.0        255.255.255.255 UH    0     0          0 dmvpn
192.168.1.0       0.0.0.0        255.255.255.0   U     0     0          0 br0
192.168.2.0       172.16.1.2     255.255.255.0   UG    20    0          0 dmvpn
192.168.10.0     0.0.0.0        255.255.255.0   U     0     0          0 vlan2
192.168.10.1     0.0.0.0        255.255.255.255 UH    0     0          0 vlan2
root@Router:/tmp/etc# ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1): 56 data bytes
64 bytes from 192.168.2.1: seq=0 ttl=64 time=1.748 ms
64 bytes from 192.168.2.1: seq=1 ttl=64 time=1.280 ms
64 bytes from 192.168.2.1: seq=2 ttl=64 time=1.412 ms
64 bytes from 192.168.2.1: seq=3 ttl=64 time=1.144 ms
^C
--- 192.168.2.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.144/1.396/1.748 ms
root@Router:/tmp/etc# ping 192.168.2.195
PING 192.168.2.195 (192.168.2.195): 56 data bytes
64 bytes from 192.168.2.195: seq=0 ttl=127 time=1.609 ms
64 bytes from 192.168.2.195: seq=1 ttl=127 time=1.492 ms
64 bytes from 192.168.2.195: seq=2 ttl=127 time=1.458 ms
64 bytes from 192.168.2.195: seq=3 ttl=127 time=1.383 ms
64 bytes from 192.168.2.195: seq=4 ttl=127 time=1.615 ms
^C
--- 192.168.2.195 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.383/1.511/1.615 ms
root@Router:/tmp/etc#

```

Figure 9-98

R2

```

root@Router:/tmp/home/root#
root@Router:/tmp/home/root# route -n
Kernel IP routing table
Destination        Gateway            Genmask           Flags Metric Ref    Use Iface
0.0.0.0            192.168.10.1      0.0.0.0           UG    0      0          0 vlan2
127.0.0.0          0.0.0.0           255.0.0.0         U      0      0          0 lo
172.16.1.0         172.16.1.1        255.255.255.0     UG    0      0          0 dmvpn
172.16.1.1         0.0.0.0           255.255.255.255   UH    0      0          0 dmvpn
192.168.1.0        172.16.1.1        255.255.255.0     UG    20     0          0 dmvpn
192.168.2.0        0.0.0.0           255.255.255.0     U      0      0          0 br0
192.168.10.0       0.0.0.0           255.255.255.0     U      0      0          0 vlan2
192.168.10.1       0.0.0.0           255.255.255.255   UH    0      0          0 vlan2

root@Router:/tmp/home/root# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.268 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=1.156 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=1.476 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=1.344 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=1.226 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.156/1.294/1.476 ms

root@Router:/tmp/home/root# ping 192.168.1.50
PING 192.168.1.50 (192.168.1.50): 56 data bytes
64 bytes from 192.168.1.50: seq=0 ttl=127 time=1.625 ms
64 bytes from 192.168.1.50: seq=1 ttl=127 time=1.568 ms
64 bytes from 192.168.1.50: seq=2 ttl=127 time=1.544 ms
64 bytes from 192.168.1.50: seq=3 ttl=127 time=1.554 ms
64 bytes from 192.168.1.50: seq=4 ttl=127 time=2.727 ms
^C
--- 192.168.1.50 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.544/1.803/2.727 ms

```

Figure 9-99

10. Administration

10.1. Identification

In the navigation bar, select “Administration > Identification”. On the page, you can modify the parameters of the identification. Identify the router, host name, and domain. If there are many network devices in the LAN, you can set the name of the router to distinguish it from other devices.

Figure 10-1

Description of Identification

Parameter	Description
The name of the router	The default value is Router, which can contain up to 32 English characters, and is displayed on the system status page after setting.
The name of the host	The default value is Router, with a maximum of 32 English characters, and the user-set name is displayed in the Windows LAN after setting.
Domain	The default value is empty, with a maximum of 32 English characters, and the domain name here is the domain of the WAN port, which is not required for general users.

Table 10-1 System Identity configuration parameters

After the configuration is complete, click the Save Settings button for the configuration to take effect.

10.2. Time

The G51 Router supports Network Time Protocol (NTP). When the NTP network is matched, the system time of the router corresponds to the actual time, and the functions such as task management are executed at the correct time. The specific steps are as follows.

Step 1: Select "Administration > Time" in the navigation bar.

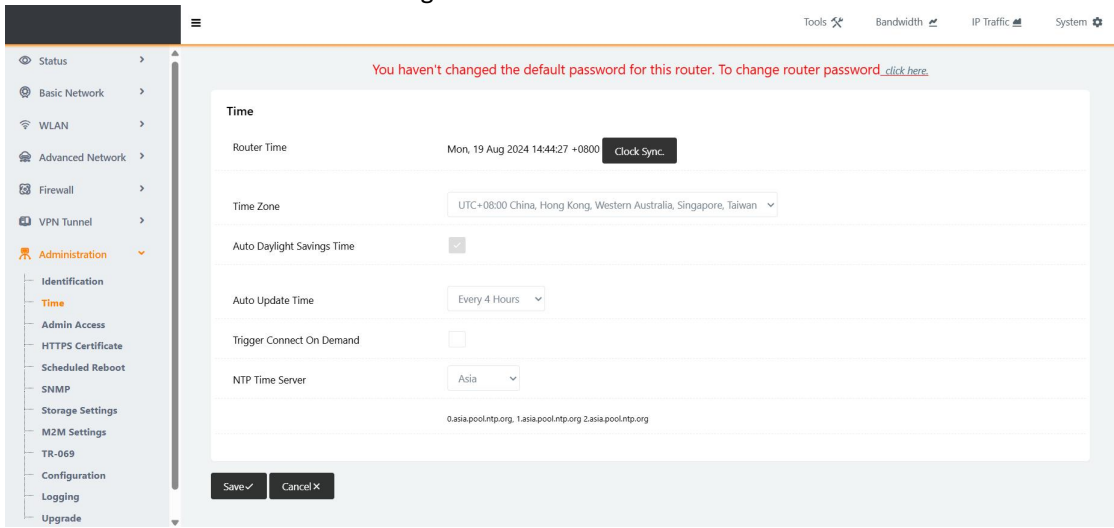


Figure 10-2 Screenshot of system time configuration

Step 2: Configure the system time parameters:

Parameter	Meaning	How to configure
time zone	The type of time synchronization for system time verification	drop-down list box selection
Automatic time synchronization	Set the time for automatic syncing	Select from the list box
Sync when needed	Sync time only when needed	Enabled or not enabled
NTP Network Time Server	NTP clock server	Select Default or ASIA

Table 10-2 Configure system time parameters

Step 3: Click Save to complete the system log parameter configuration.



WARNING

If you have internet access but the time update fails, try to select a different NTP time server.

10.3. Admin Access

In the navigation bar, select "Administration > Admin Access". On the page, you can modify the parameters related to the access settings.

On this page, you can configure some basic web access settings for your convenience.

The password setting option is to change the password of the system account admin.

Remote Access: Enable remote access, open the corresponding port, and save it.

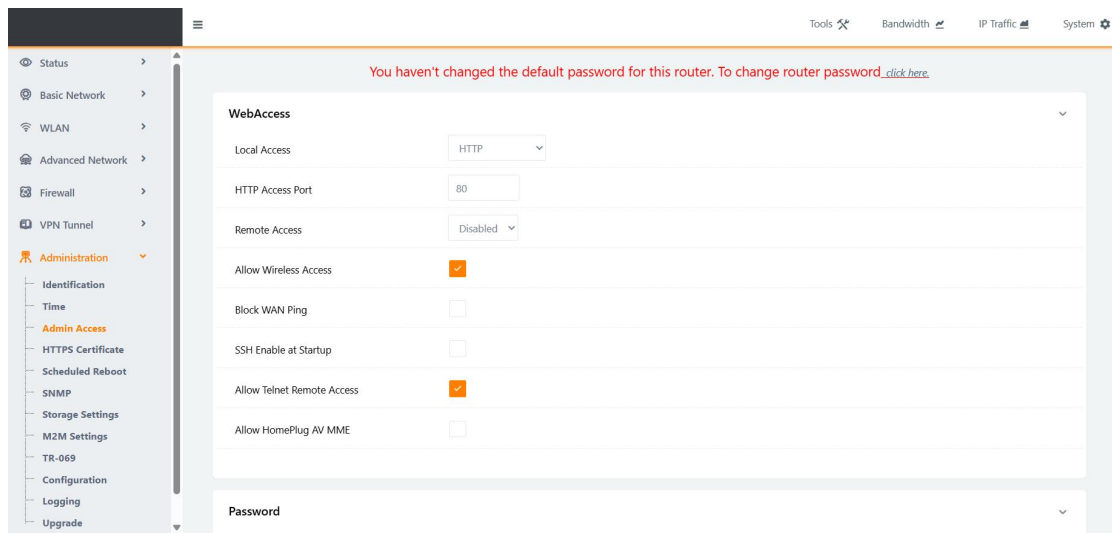


Figure 10-3 Screenshot of the configuration management configuration

Admin Access description

Parameter	Meaning	How to configure
Local access	SET LAN/HTTPS/HTTP&HTTPS TO LAN WEB ACCESS PROTOCOL	drop-down list box selection
HTTP access port	Default is 80	
Remote access	BY DEFAULT, HTTP/HTTPS/HTTP&HTTPS IS SELECTED FOR REMOTE WEB ACCESS PROTOCOLS SUCH AS WAN/MODEM/VPN	drop-down list box selection
Allow wireless access	WIFI CLIENT DEVICES ARE ALLOWED	Select Default or ASIA
WAN port is not pinged	EXTERNAL PINGS ARE TACITLY PROHIBITED	TICK: BAN PING; UNCHECKED: PING IS ALLOWED
SSH boot starts	SSH is not enabled by default	Check: On; Uncheck: Off
Enable Telnet remote access	Remote telnet access is not enabled by default	Check: On; Uncheck: Off

Table 10-3

After the configuration is complete, click the Save Settings button for the configuration to take effect.

10.4. HTTPS Certificate

In the navigation bar, select “Administration >HTTPS Certificate”. On the page, you can import and export HTTPS certificates and keys. As shown in the figure below 10-4

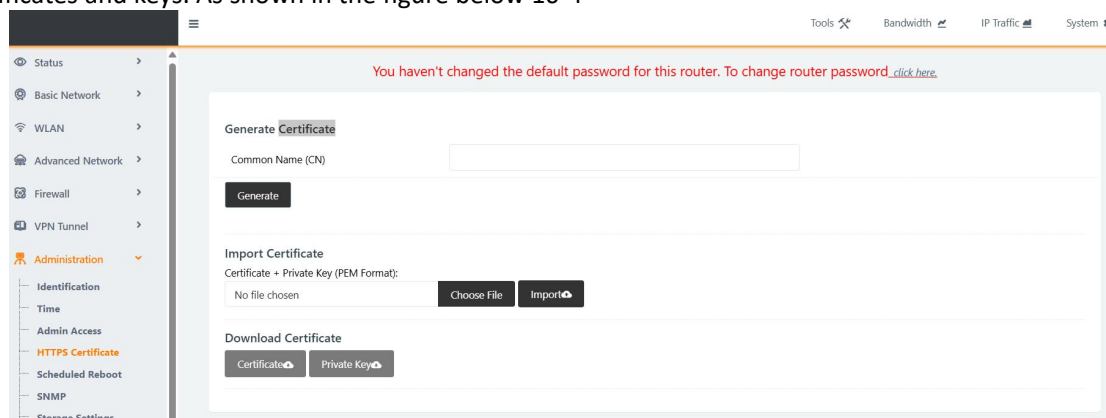


Figure 10-4

HTTPS Certificate parameters

Parameter	Meaning	How to configure
Generic name	The name of the generated certificate	Configure the name and click Generate
Import the certificate and private key	Import of certificates and keys	Put the certificate and key in one formatpem file and select the file to import

Certificate	Download the certificate	You need to import the certificate and key before you can download the certificate
Keys	Download the key	You need to import the certificate and key before you can download the key

Table 10-4 HTTPS Certificate parameters

10.5. Scheduled Reboot

In the navigation bar, select “Administration > Scheduled Reboot”. On the page, you can modify the parameters of the Scheduled reboot function.

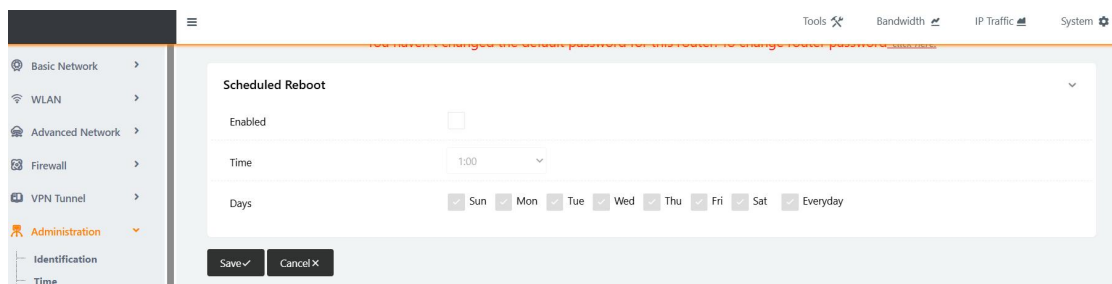


Figure 10-6

After the configuration is complete, click the Save Settings button for the configuration to take effect.

Example:

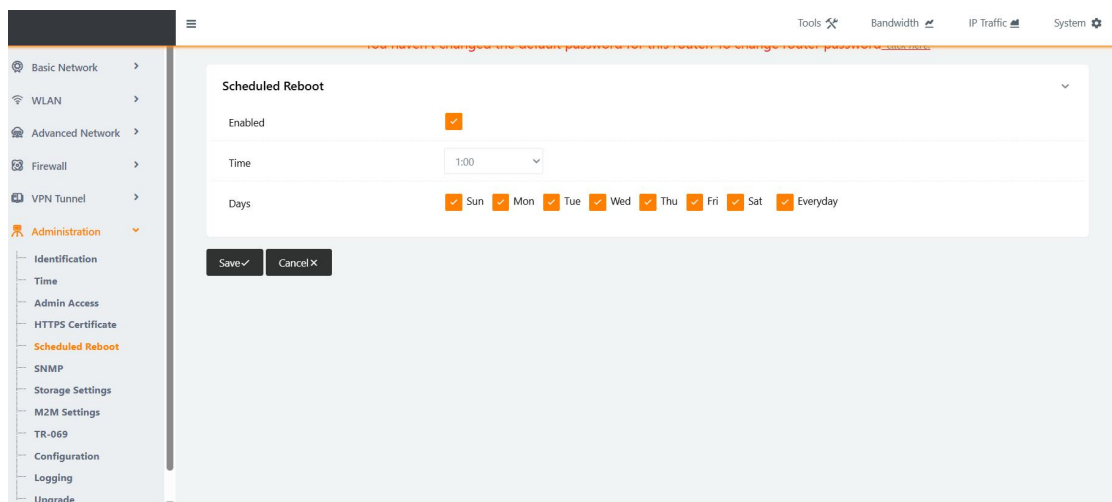


Figure 10-7

Tick "On" and set the drop-down time to 16:00

After synchronizing the device time, the device will automatically restart when it reaches 16:00

10.6. SNMP

After the Simple Network Management Protocol (SNMP) function is enabled, you can use SNMP management tools to remotely monitor devices and view their running status.

Step1: select “Administration > SNMP”. On the page, you can modify the parameters of the SNMP function. As shown in figure 10-8

You haven't changed the default password for this router. To change router password [click here](#).

SNMPP Settings

Enable SNMP	<input type="checkbox"/>
Port	161
Remote Access	<input type="checkbox"/>
Allowed Remote IP Address	<input type="text"/> (optional: e.g. "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")
System Name	router
Location	router
Contact	admin@router
RO Community	rocommunity
RW Community	rwcommunity

Figure 10-8

Step 2: SNMP parameters

Parameter	Meaning	How to configure
SNMP service	Use SNMP services	Radio button selection Enabled Disable
Service port	It is recommended that you configure the SNMP service listening port to 161 as the default end	Value range: 1~65535 Default: 161
Allows remote management of IPs	The server address reported by the router link status	Format: A.B.C.D. interface type

Table 10-5 SNMP parameter configuration

Example:

SNMPP Settings

Enable SNMP	<input checked="" type="checkbox"/>
Port	161
Remote Access	<input type="checkbox"/>
Allowed Remote IP Address	<input type="text"/> (optional: e.g. "1.1.1.1", "1.1.1.0/24", "1.1.1.1 - 2.2.2.2")
System Name	router
Location	router
Contact	admin@router
RO Community	rocommunity
RW Community	rwcommunity
SNMPv3 Authentication Type	NONE
SNMPv3 Privacy Type	NONE

Figure 10-9

You can use the MIB tool to query device data through SNMP

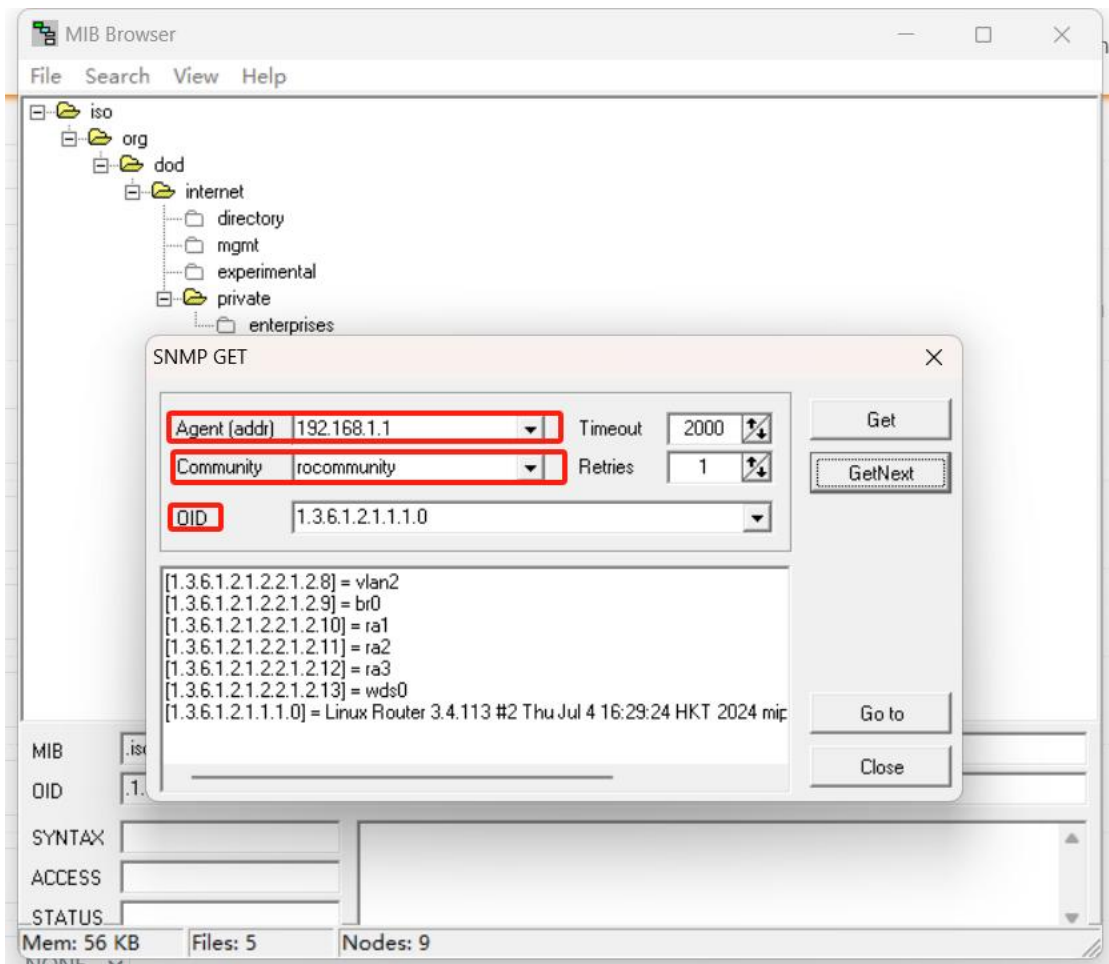


Figure 10-10

10.7. M2M Settings

Router communicates with the M2M (Machine-to-Machine) platform through the D&Com proprietary platform management protocol, which enables remote maintenance management and on-site network status monitoring and management, such as viewing device information, patch upgrades, firmware upgrades, Configure parameters to view the network signal strength, latency, and traffic of the device. The specific settings are as follows:

Step 1: Select "Administration>M2M Settings" in the navigation bar. On the page, you can modify the relevant parameters of the M2M platform management function to connect it with the management platform.

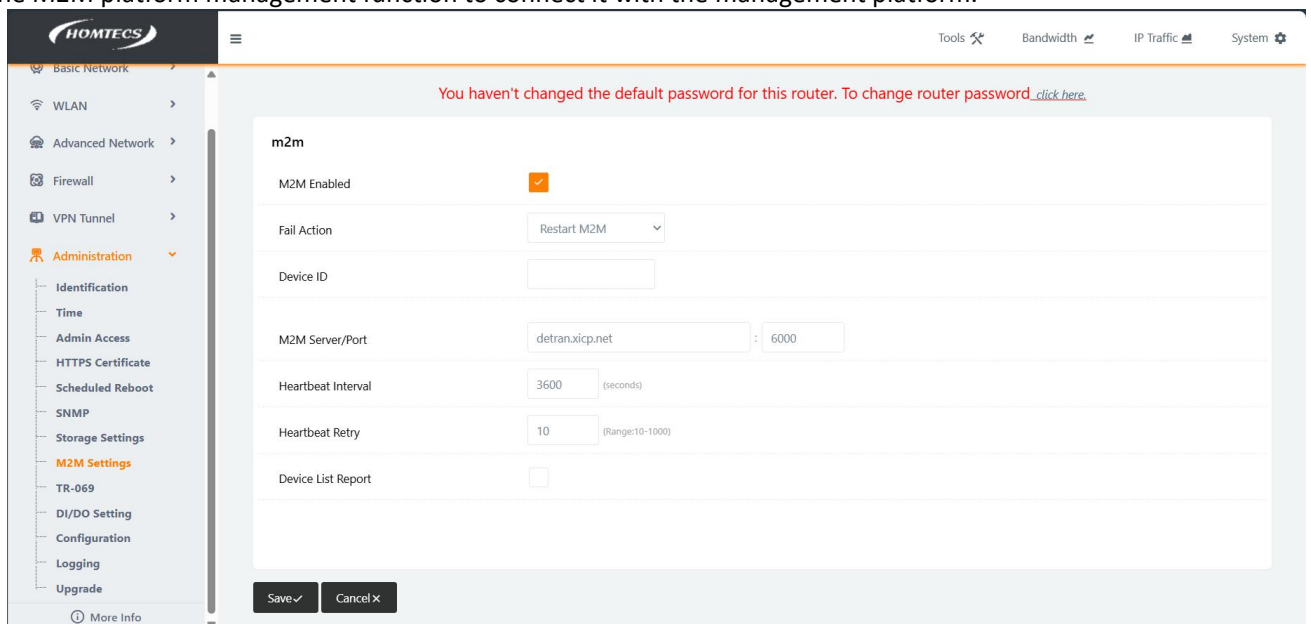


Figure 10-11

Step 2: M2M Settings description:

Parameter	Meaning	How to configure
Enable M2M platform management	To use M2M services, this function needs to be used with our M2M terminal management platform	Enabled or not enabled
Product ID	The device ID number, which can be edited into an easy-to-remember ID, so that the platform can see which terminal it corresponds to at a glance	WORD type, up to 64 bytes
Service port	The port number used by the WMMP service of the M2M platform server can be matched with the server	Value range: 1~65535
Heartbeat reporting frequency	In addition to the sending interval between the router and the M2M platform to maintain the connection, the heartbeat packet also contains the network status data of the router to update the real- time network status data of the M2M platform	Value range: 1~65535 Unit: seconds The default value is 60S
The number of heartbeat packet failures	The number of heartbeats that are retried after a heartbeat is sent	Default: 10 times
Device list reporting is enabled	Enable and disable the device list escalation feature	Disabled by default
Escalation mode	New Reports: Only the new device information is reported All Reports: Reports information about all devices	Default: Added escalation
The escalation interval of the device list	Escalation interval	Default: 0; Unit: seconds; Range: 0-3600

Table 10-6 M2M parameter configuration

Step 3: Once the configuration is complete, click the "Save" button for the configuration to take effect.

Example:

m2m

M2M Enabled

☒

Fail Action

Restart M2M

Device ID

homtecs-G51

M2M Server/Port

detran.xicp.net

:

6000

Heartbeat Interval

3600

(seconds)

Heartbeat Retry

10

(Range:10-1000)

Device List Report

☐

Figure 10-12

Log in to the platform to see the device information and operate on the device

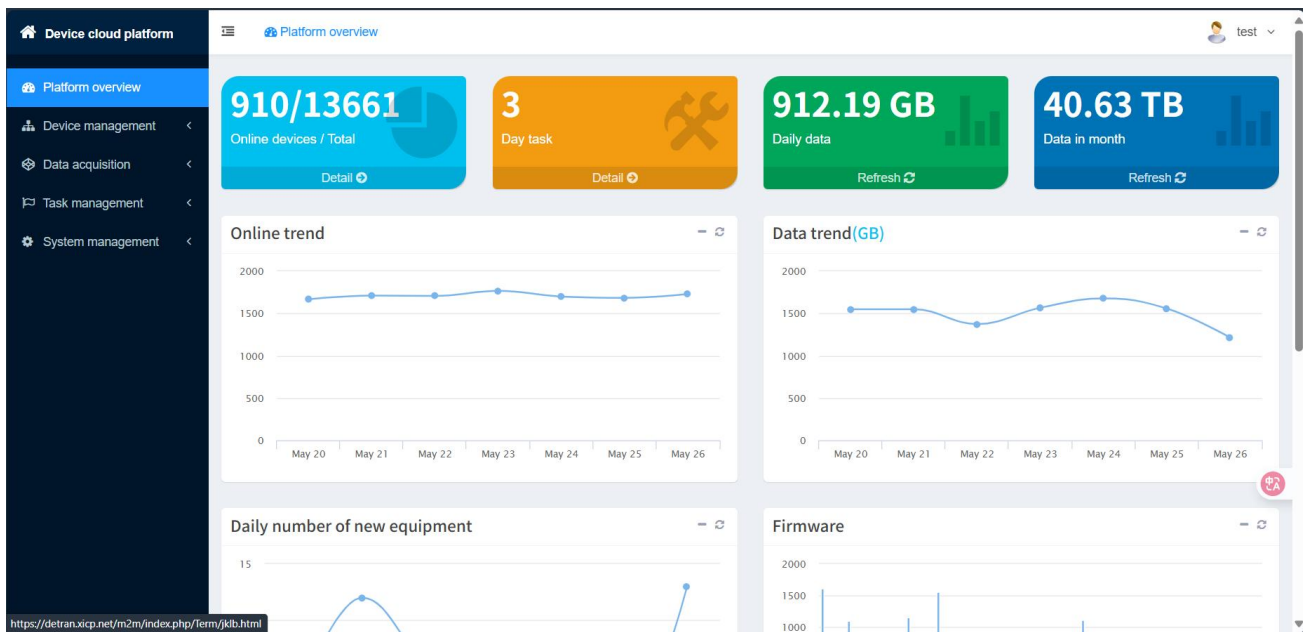


Figure 10-13

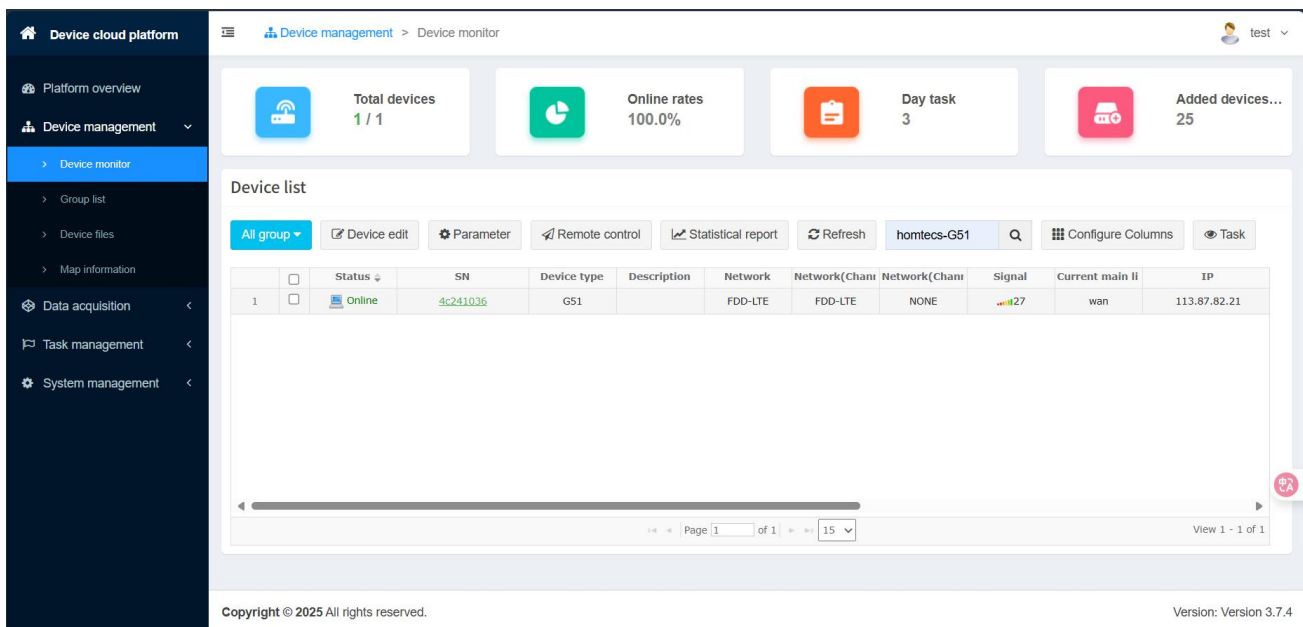


Figure 10-14

10.8. DI/DO Settings

Select “Administration > DI/DOutput” to use the IO port control function.

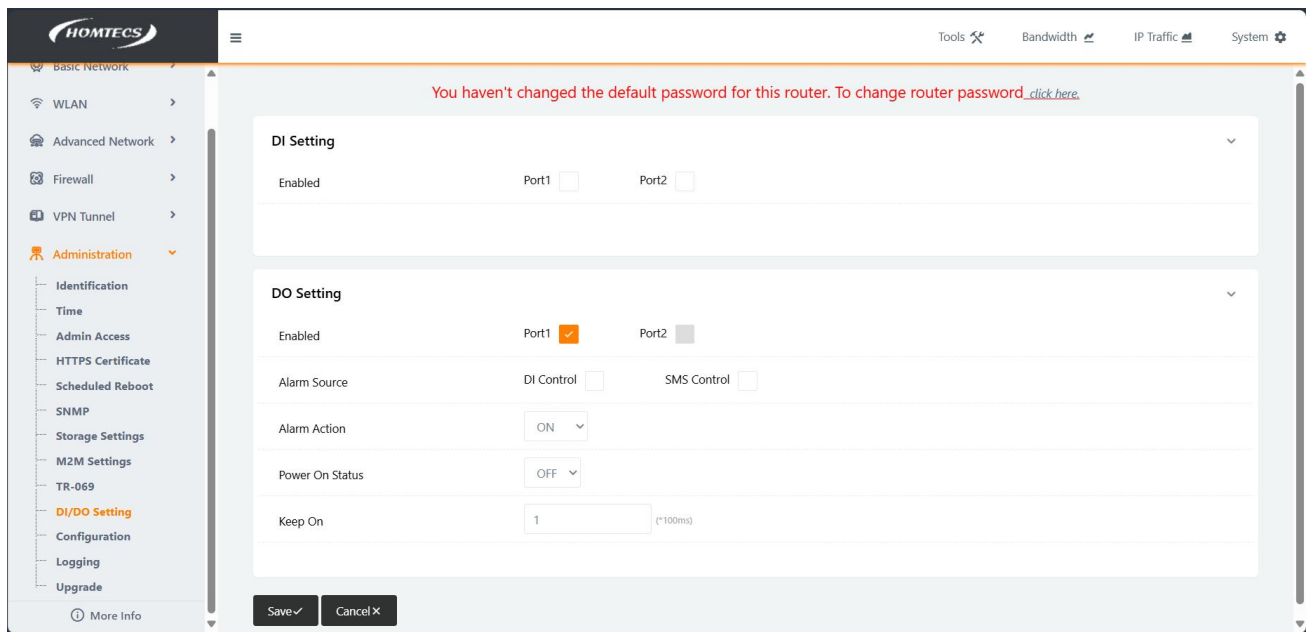


Figure 10-15

Configure the input pins, and the configuration page is as follows:

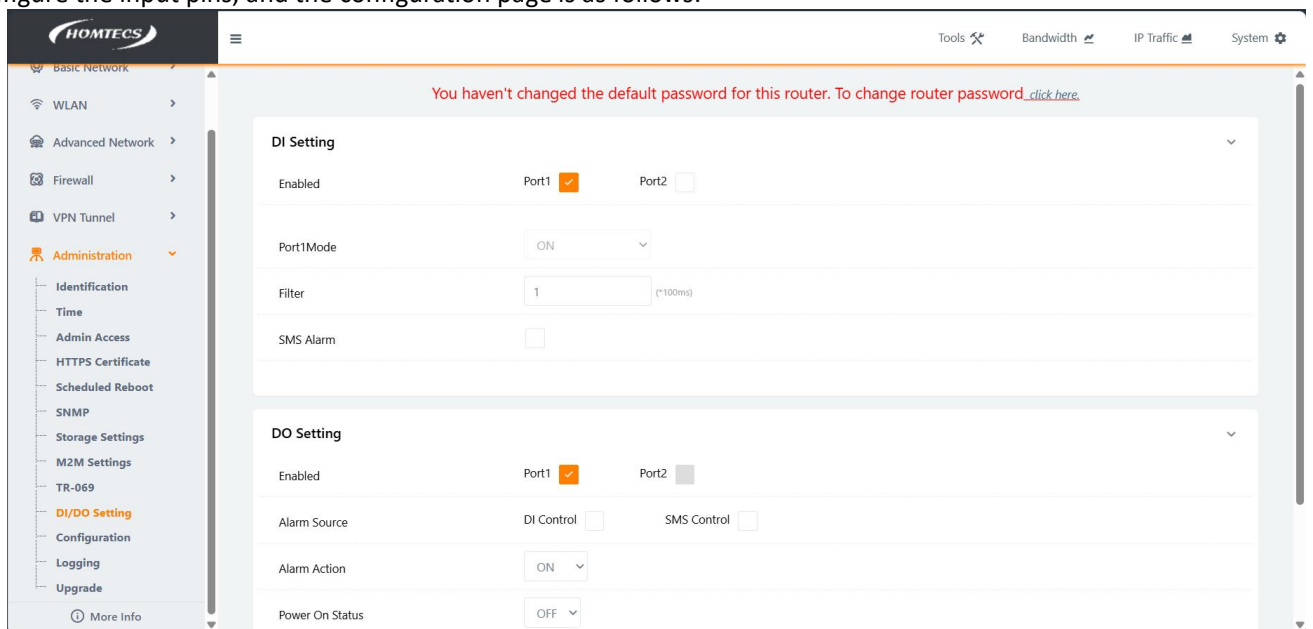


Figure 10-16

Description of the Input Management Configuration parameter:

parameter	illustrate	Default value
enable	With this pin, port 1 corresponds to IO1 on the appearance diagram, and port 2 corresponds to IO2 on the façade schematic.	Disable
Port mode	Three options: 'OFF', 'ON', 'EVENT_COUNTER' OFF: Triggers an event when connected to GND, and the external input is low; ON: Triggers an event when disconnected from GND, and the external input is high; EVENT_COUNTER: Enter the event counting mode.	OFF
Filter	Control switch jitter (1~100)*100ms For OFF and ON mode, the first and last detection are twice, and if both are at the same level, the alarm will be triggered. For EVENT_COUNTER mode, if the first and last values are not connected, a rising/falling	1

	edge is determined.	
Count triggering	The event count pattern works When the count reaches the specified value, an event alarm is triggered, and when the alarm event is triggered, the count continues, but no more alarms are triggered. Count does not begin until the set recovery time has elapsed. Input range: 0~100, 0 means that the alarm will not be triggered.	0
Count periods	The count should be valid for this period, after which it clears to 0 Input range: 0~30000, (0=means that the period is permanent, and any event triggered at any time can be effectively counted.))	0
Recovery count	The event count pattern works After the alarm is triggered by the counter, when to resume the recounting Input valid range: 0~30000 (*100ms) (0=no recovery count)	0
Trigger an event	The event count pattern works Two options: 'HI_TO_LO' and 'LO_TO_HI', the LO_TO_HI option means that when the connected IO port is pulled up, the trigger event count will be increased by one, and the HI_TO_LO option means that when the connected IO port is pulled up and released, the trigger event count will be increased by one.	LO_TO_HI
Counting begins	The event count pattern works. Currently, only the option 'POWER_ON' is supported. POWER_ON: This option means that the event count will start counting as soon as the feature is activated.	POWER_ON
SMS alerts	If this option is selected, an SMS message will be sent every time an alarm is triggered. Use this option with caution in the ON and OFF states. The persistent state is prone to trigger a large number of alarms.	0
The content of the text message	Enter the content of the SMS to be sent when the alarm is triggered, which is defined by the user. Maximum length: 70 ASCII visible characters Note: Since there may be sudden continuous alarm states in actual use, we have defined an SMS queue with a maximum length of 10, which means that if too many SMS sending requests are generated at the same time, we will only cache the first 10 SMS sending requests.	NULL
SMS receiving number 1	Phone number, SMS recipient	NULL
SMS receiving number 2	Phone number, SMS recipient	NULL

Table 10-7 Input Management Parameter Configuration

Configure the output pins on the following page:

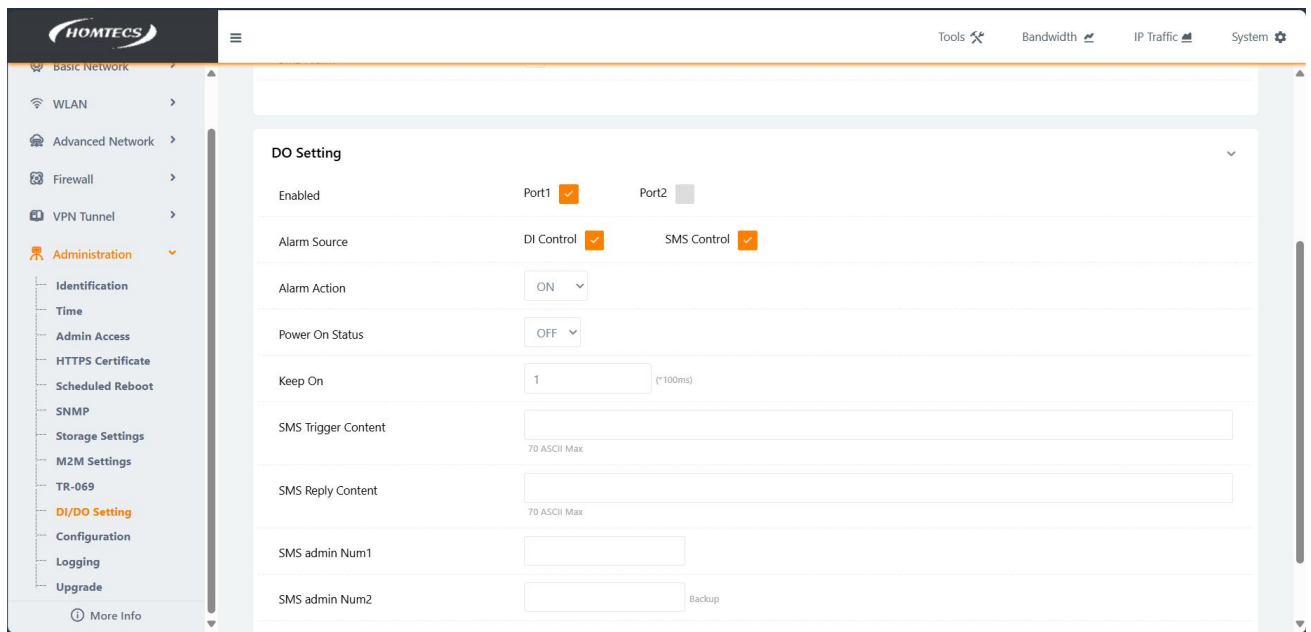




Figure 10-17

‘Output Management’ Configuration parameter description:

project	description	Default value
enable	Enable the pin	Disable
Alarm source	<p>It supports input pins, SMS control, and M2M platform alarm sources.</p> <p>When an alarm source is selected on the input pin, the alarm source port 1 and port 2 will output the corresponding waveform according to the user's selection.</p> <p>SMS controls the alarm source, triggers the output pin output when receiving a text message with specific content, and after the output pin output is completed, it replies to the previous SMS sender to specify the content.</p> <p>The M2M alarm source is not supported yet.</p>	BY Alarm
Trigger an action	<p>There are three options for the output pin to output when the alarm source triggers an event, 'OFF', 'ON', and 'Pulse'.</p> <p>OFF: Rising edge, output from low to high</p> <p>ON: Falling edge, output from high to low</p> <p>Pulse: When triggered, a pulse signal is generated, when the default state is ON, the pulse signal generated is a low level + high level continuous waveform, and when the default state is OFF, the generated pulse signal is a high level + low level continuous waveform.</p>	ON
Default state	<p>Specify the output status of the output pin when powering up, 'OFF', 'ON'</p> <p>OFF: logical 0.</p> <p>ON: logical 1.</p>	
duration	<p>When the trigger action option ON or OFF of the output pin is active, the input and output pins remain in this state for the length of time.</p> <p>When the default state is OFF and the trigger action is OFF, the output pin outputs one  Square wave, the duration value is the duration of the high level.</p> <p>When the default state is ON and the trigger action is ON,</p> <p>The output pin outputs one  Square wave, the duration value is the duration of the low level.</p>	



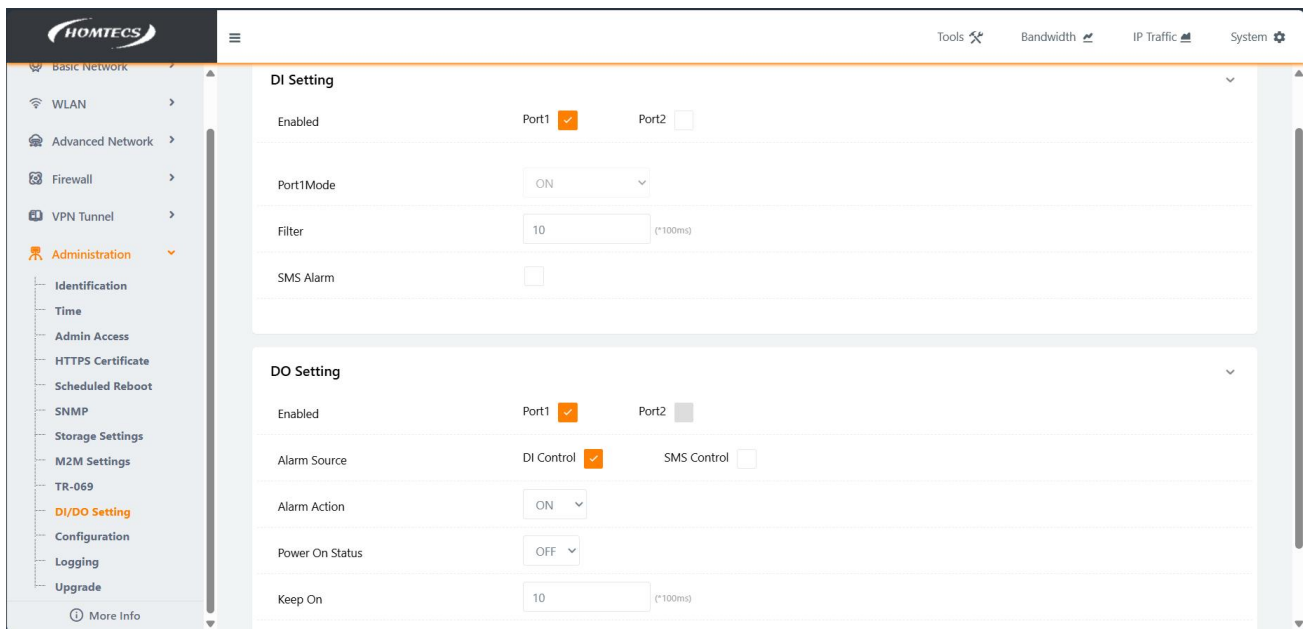
	<p>When the default state is OFF and the trigger action is ON, The output pin outputs one  square wave with a duration of high duration.</p> <p>When the default state is ON and the trigger action is OFF, The output pin outputs one  Square wave, which lasts for a low duration.</p> <p>The input range is 0~2550 (*100ms), (0 means always in a state state, use with caution).</p>	
Delay	<p>Valid when the Trigger Action option of the output pin is Pulse. After delaying the input time, the first square wave is generated Input valid range is 0~300(*100ms)</p>	0
Low level	<p>Valid when the Trigger Action option of the output pin is Pulse. Specifies the width of the square wave low level of 0 Input range: 1~300 (*100ms)</p>	10
High level	<p>Valid when the Trigger Action option of the output pin is Pulse. Specifies the width of the square wave high Input range: 1~300 (*100ms)</p>	10
Number of outputs	<p>Valid when the Trigger Action option of the output pin is Pulse. Specifies the number of pulses to be generated The input range is: 1~1000</p>	1
SMS alert content	<p>Triggers the output pin to output the content of the SMS waveform. The sender is one of the two numbers in the following options. Maximum length, 70 ASCII visible characters</p>	NULL
The content of the text message reply	<p>When the output pin outputs a waveform, it replies to the specified sender's content. Maximum length, 70 ASCII visible characters</p>	NULL
SMS Manager Number 1	The number of the SMS sender	NULL
SMS Manager Number 2	The number of the SMS sender	NULL

Table 10-8 Output Management Parameter Configuration

Example:

Step 1: Enable the input and output pin configuration; If you select Open Port 1 for the input pin configuration, the network mode will be locked to "ON" by default, and the filter image will be filled in "10"x100ms.

Step 2: Select Enable and Input Pin Control for the output pin configuration, select "ON" for alarm action, select "OFF" for default status, and set "10" x 100ms for duration.



Step 3: If a low level is inserted between the DI1 interface and the GND interface, the DI will not trigger an alarm and will not trigger the DO, and the DO will be in a low state at this time



Step 4: The DI1 interface and GND interface incoming change from low to high for 1 second, DI triggers an alarm and triggers DO for 1 time, and the DO is in a high state at this time, and the high state of DO lasts for 1 second each time, and then becomes low until the next time the DO is triggered



Step 5: If the DI1 interface and GND interface change from high to low, the DI will not trigger an alarm or DO, and the DO will be in a low state



10.9. Configuration

In the navigation bar, select “Administration > Configuration”. You can back up the configuration of the current router, restore the configuration of the router that was previously backed up, and restore to the factory settings.

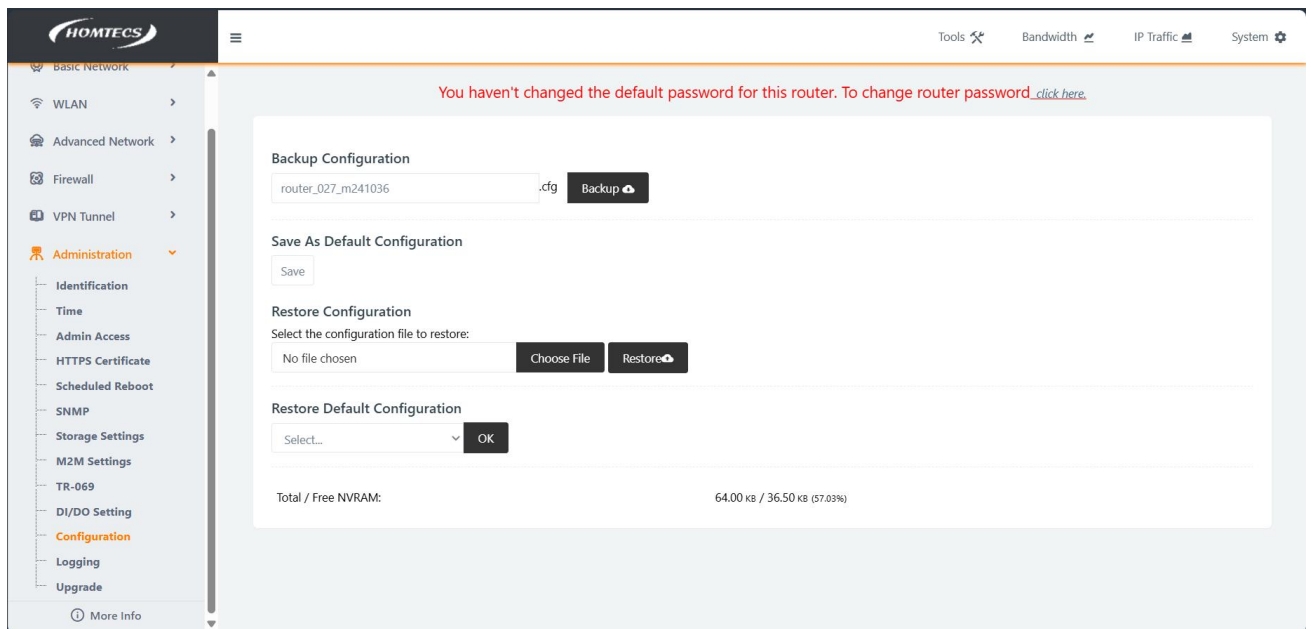


Figure 10-18



WARNING

Please choose carefully to back up and restore factory settings, once restored, all previous configurations will be invalid.

After the configuration is complete, click the “Save” button for the configuration to take effect.

Example:

To export the configuration file, click the backup button, and the browser can download the configuration file of the device at this time

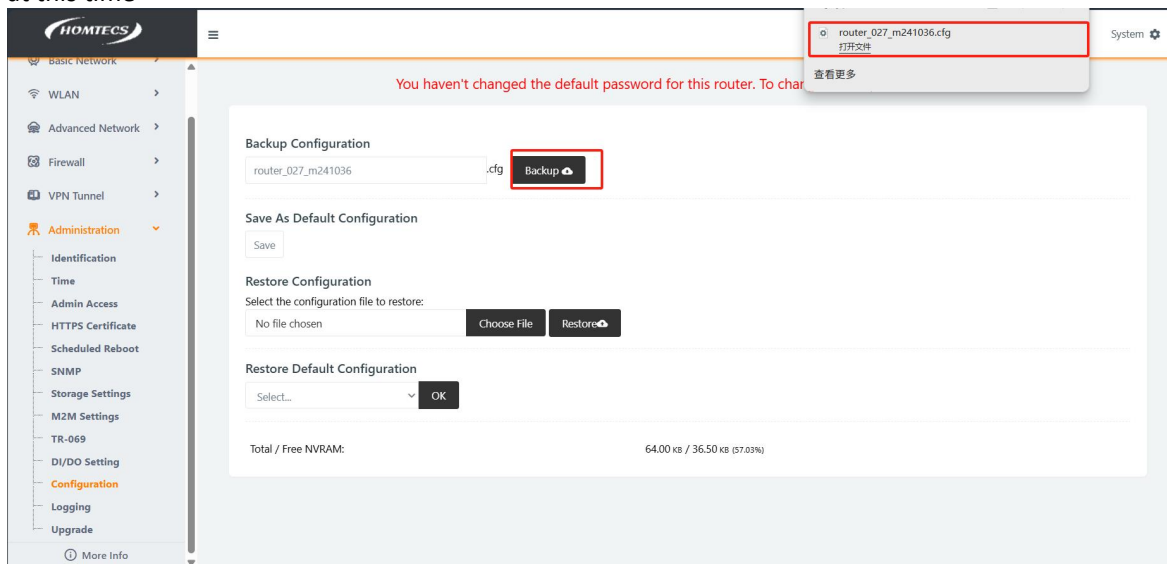


Figure 10-19

To import a profile:

Click "Select File" and go to the PC folder to select the configuration file you want to import

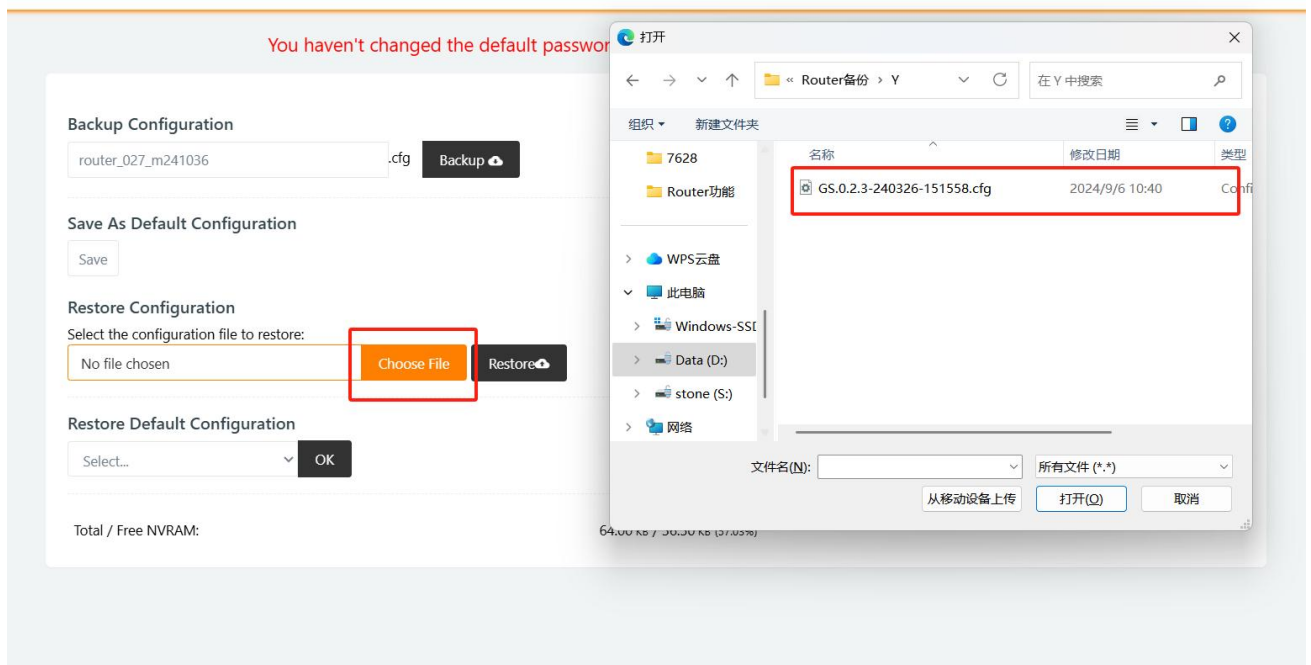


Figure 10-20

Click "Restore" and the system will automatically apply the profile and restart automatically

10.10. Logging

Local logs allow you to view system running and operation configurations on the Administration page. With this information, it is possible to find system anomalies and accurately locate problems.

Select "Administration > Logging" in the navigation bar as shown in figure 10-21:

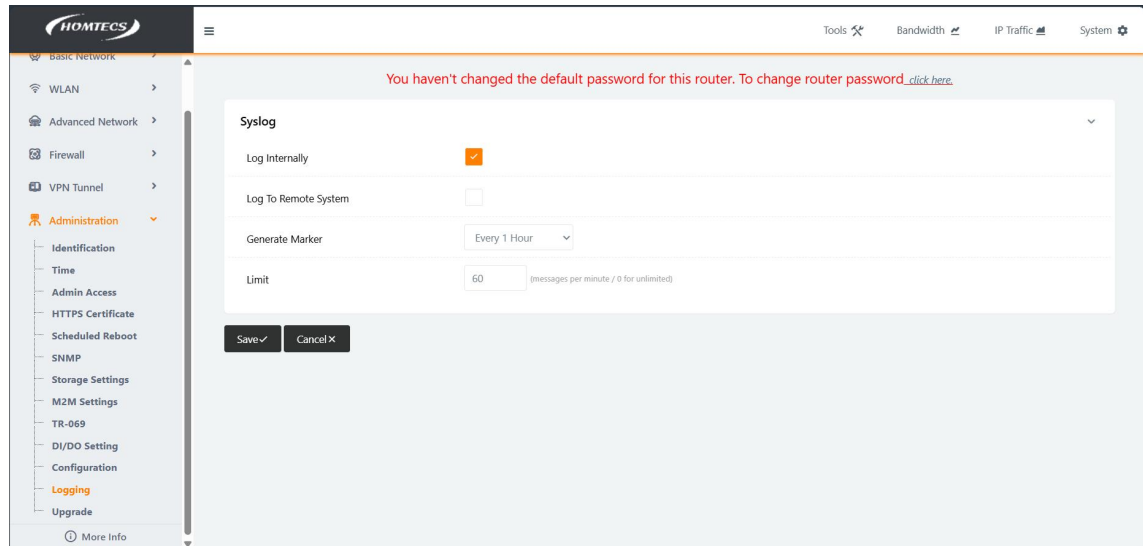


Figure 10-21

On the log configuration page, select the path (local or remote server) and the time when the logs are generated. Click Save Settings to take effect.

Configuration example:

Syslog

Log Internally

Log To Remote System

Host or IP Address / Port

192.168.1.50

:

514

Generate Marker

Every 1 Hour

Limit

60

(messages per minute / 0 for unlimited)

Save

Cancel

Figure 10-22

Select Record to remote system and enter the IP address and port

MikroTik Syslog Daemon			
File Options Help			
	Time	Message	IP
<div>ROUTING THE WORLD</div> <div>MikroTik</div> <div>www.mikrotik.com</div> <div>Main queue</div> <div>ipsec</div> <div>DI/DO</div> <div>n2n</div>	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: raid0: ==> main_virtual_jf_open	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.66	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.70	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: RtmpOSFileOpen(): Error 2 opening /etc/wireless/l1profile.dat	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: load l1profile succeed!	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: get_wdev_by_idx: invalid idx(0)	192.168.1.1
	27-May 17:55:20.71	<4>Jan 1 08:00:05 kernel: driver_owm():Try to Clear FW Own...	192.168.1.1
	27-May 17:55:21.39	<13>Jan 1 08:00:06 modem_watchdog[758]: Check Modem 1 USIM(1) Status (6/60)	192.168.1.1
	27-May 17:55:22.18	<6>Jan 1 08:00:06 kernel: usb 1-1: new full-speed USB device number 2 using xhci-hcd	192.168.1.1
	27-May 17:55:22.20	<6>Jan 1 08:00:06 kernel: usb 1-1: not running at top speed; connect to a high speed hub	192.168.1.1
	27-May 17:55:22.21	<15>Jan 1 08:00:06 hotplug[1040]: Attached USB device 1-1 (INTERFACE=null) PRODUCT=1782/4d00/2430	192.168.1.1
	27-May 17:55:22.22	<15>Jan 1 08:00:06 hotplug[1044]: Attached USB device 1-1:1.0 (INTERFACE=255/0/0 PRODUCT=1782/4d00/2430)	192.168.1.1
	27-May 17:55:22.24	<6>Jan 1 08:00:06 kernel: usb 1-1: New USB device found, idVendor=1782, idProduct=4d00	192.168.1.1
	27-May 17:55:22.25	<6>Jan 1 08:00:06 kernel: usb 1-1: Product: Gadget Serial	192.168.1.1
	27-May 17:55:22.25	<6>Jan 1 08:00:06 kernel: usb 1-1: Manufacturer: spreadtrum with dwc3-gadget	192.168.1.1
	27-May 17:55:23.38	<13>Jan 1 08:00:07 modem_watchdog[758]: Check Modem 1 USIM(1) Status (7/60)	192.168.1.1
	27-May 17:55:23.38	<13>Jan 1 08:00:08 modem_watchdog[758]: Check Modem 1 USIM(1) Status (8/60)	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: driver_owm():Success to clear FW Own	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[0]	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[1]	192.168.1.1
	27-May 17:55:23.68	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[2]	192.168.1.1
	27-May 17:55:23.69	<4>Jan 1 08:00:08 kernel: APWdsInitialize():WdsEntry[3]	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: RtmpOSFileOpen(): Error 2 opening /etc/Wireless/RT2860/RT2860_2G.dat	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: Open file "/etc/Wireless/RT2860/RT2860_2G.dat" failed!	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: E2pAccessMode=2	192.168.1.1
	27-May 17:55:23.74	<4>Jan 1 08:00:08 kernel: SSID[0]=router_wifi_5.8G, EdcalIdx=0	192.168.1.1
	27-May 17:55:23.75	<4>Jan 1 08:00:08 kernel: SSID[1]=router-wifi4, EdcalIdx=0	192.168.1.1

Figure 10-23

Open the remote log tool on the PC, and the tool automatically receives the log information sent by the device.

10.11. Upgrade

The Router supports local network system file upgrades, please make sure that you have obtained the target file for the system update and store the update file on the computer on the local area network.

In the navigation bar, select “Administration > Upgrade”. Click “Choose File” and select the upgrade package that needs to be updated, check “After flashing, erase all data in NVRAM memory”, and then click “Upgrade”. Do not power off during the upgrade process, do not disconnect the network cable, the upgrade can be completed in about 3 minutes. Wait patiently, and observe the RUN indicator of the device. If the RUN indicator is on, the program upgrade is successful. It is also possible to ping the address of the router on the PC at the same time (for example: ping 192.168.1.1 -t) If pinging is possible, the upgrade is successful, as shown in Figure 10-24.

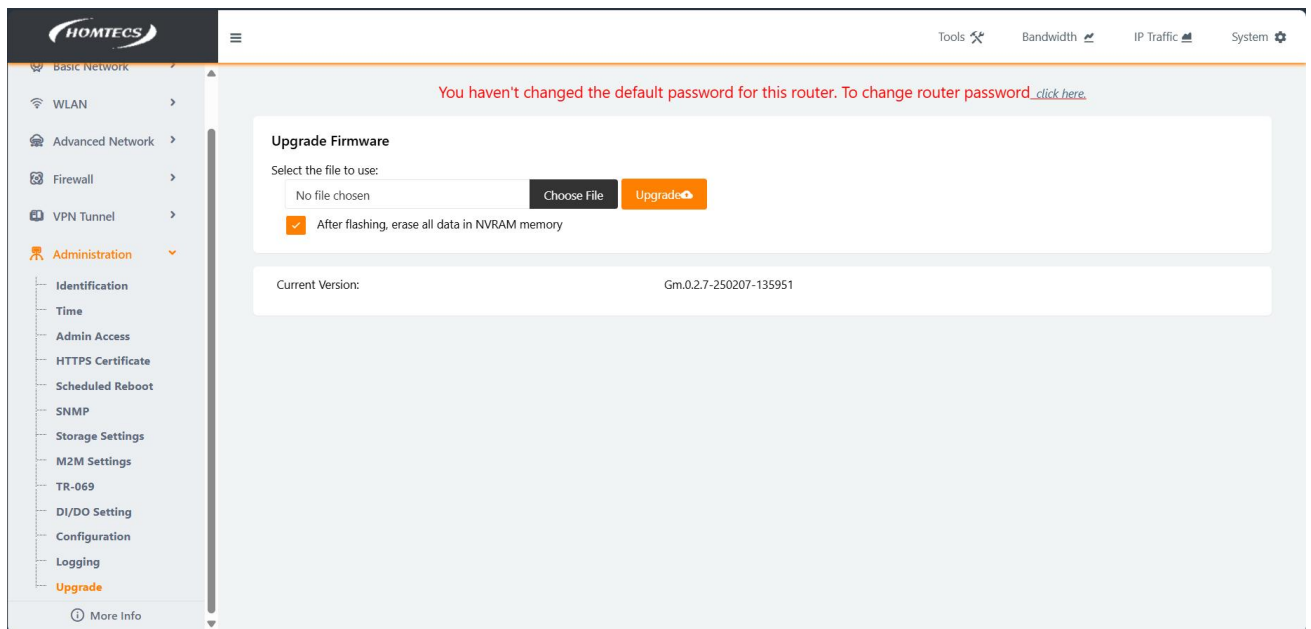


Figure 10-24 System Upgrade

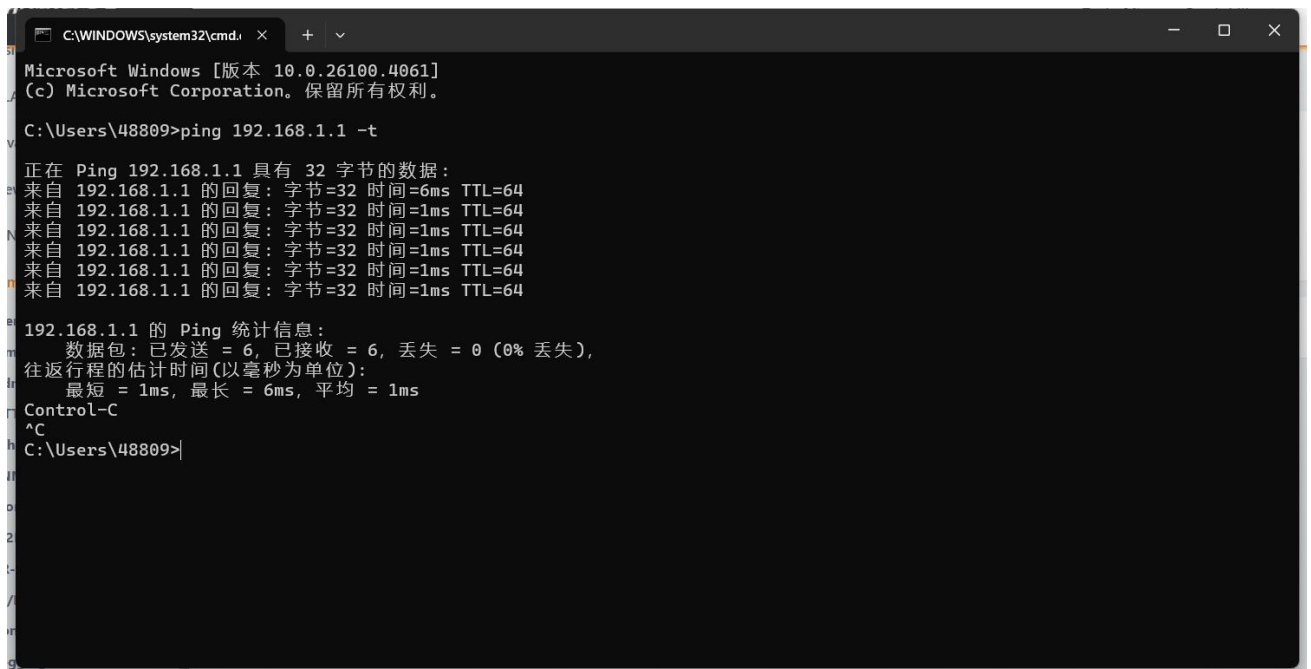


Figure 10-25 ping detection

10.12.Reboot

In the navigation bar, select “System > Reboot”. The Reboot dialog box pops up. If you don't want to reboot, you can select Cancel. If you select OK, the system will reboot, and the relevant update configurations made before will take effect after the restart.

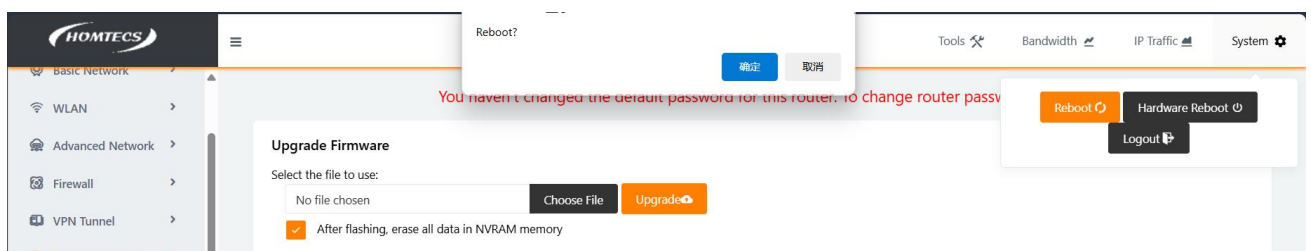


Figure 10-26

10.13. Logout

In the navigation bar, select “System > Logout”. The system will log you out directly, and then the system login screen will appear.

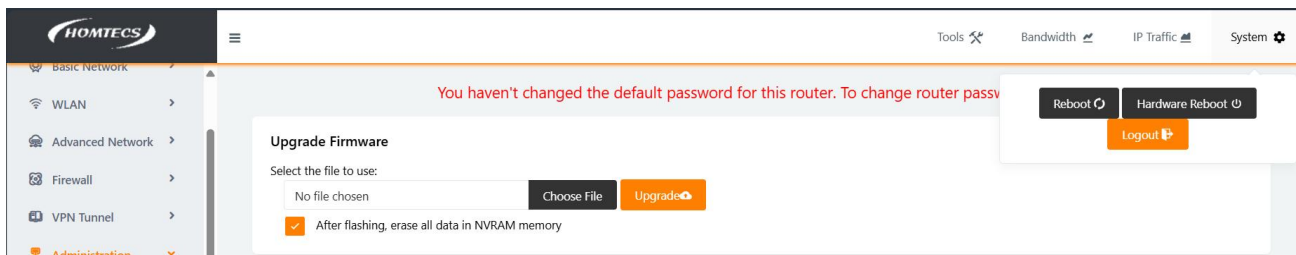


Figure 10-27

11. Tools

11.1. System log

System log is information that records hardware, software, and system problems in a system, while also monitoring events that occur in the system. It allows users to check why an error occurred or to look for traces left by the attacker when attacked. System logs include system logs, application logs, and security logs.

In the navigation bar, select “Tool > Log”, as shown in Figure 11-1

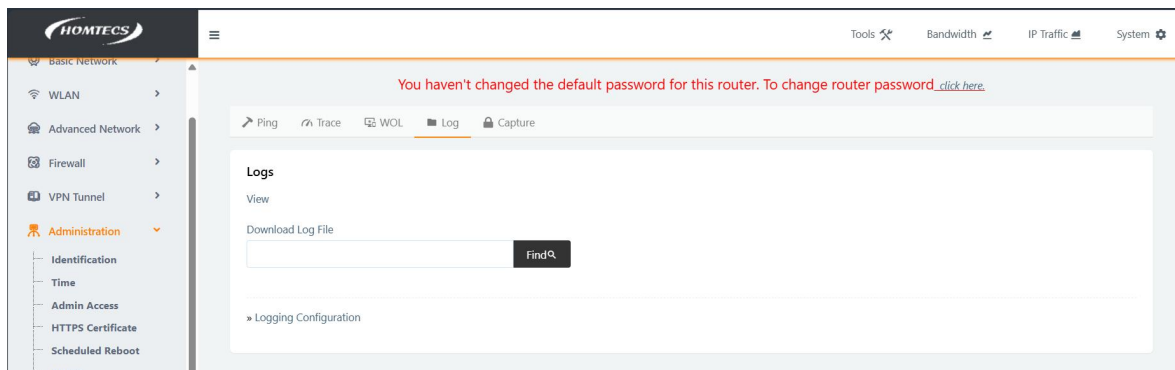


Figure 11-1

Step 1: Click View to observe the system log of the current router, as shown in the figure:

[illegible]

Figure 11-2 Log Status

Step 2: Download the log file to download the current log status to your computer.

Step 3: Click Log Settings and choose to log to the local system or the remote system.

Step 4: Once the configuration is complete, click the "Save" button for the configuration to take effect.

11.2. Ping

Ping is a command on Windows, Unix, and Linux. ping is also a communication protocol and is part of the TCP/IP protocol. You can use the ping command to check whether the network is connected, which can help us analyze and determine network faults.

In the navigation bar, select "Tool > Ping". On the page, enter the destination IP address to diagnose whether the router is connected to the network.

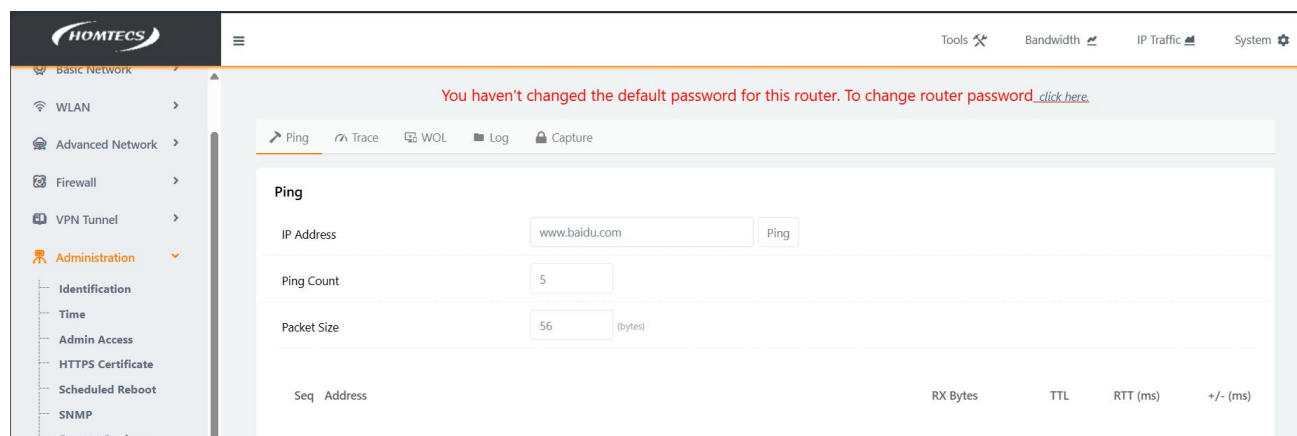


Figure 11-3

Wait a few moments for the test to complete and the test result is returned. If the destination IP address can be pinged, all packet loss indicates that the network is unreachable, and if the return is successful, the route is online.

11.3. Trace

Trace is a trace route utility that determines the path taken by an IP data gram to an access destination. The Trace command uses the IP Time-to-Live (TTL) field and an ICMP error message to determine the route from one host to other hosts on the network.

In the navigation bar, select "Tool > Trace". On the page, enter the destination IP address that the router is pursuing.

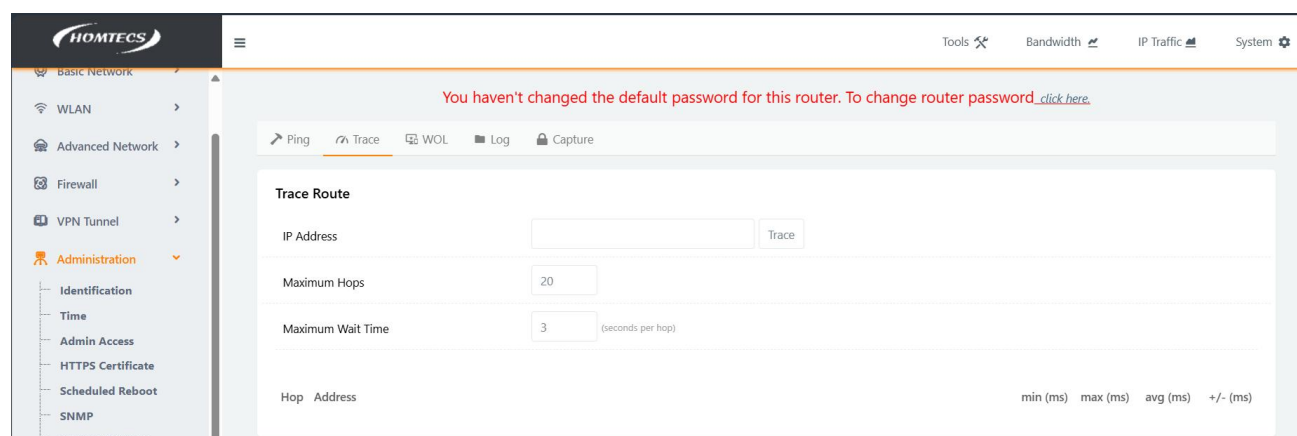


Figure 11-4

Wait a few moments, and when the trace is complete, the tracking result will be returned.

11.4. WOL

In the navigation bar, select "Tool > WOL". In the page that opens, fill in the MAC address list with the wake-up PC-MAC address to be used by the router to wake up the device.

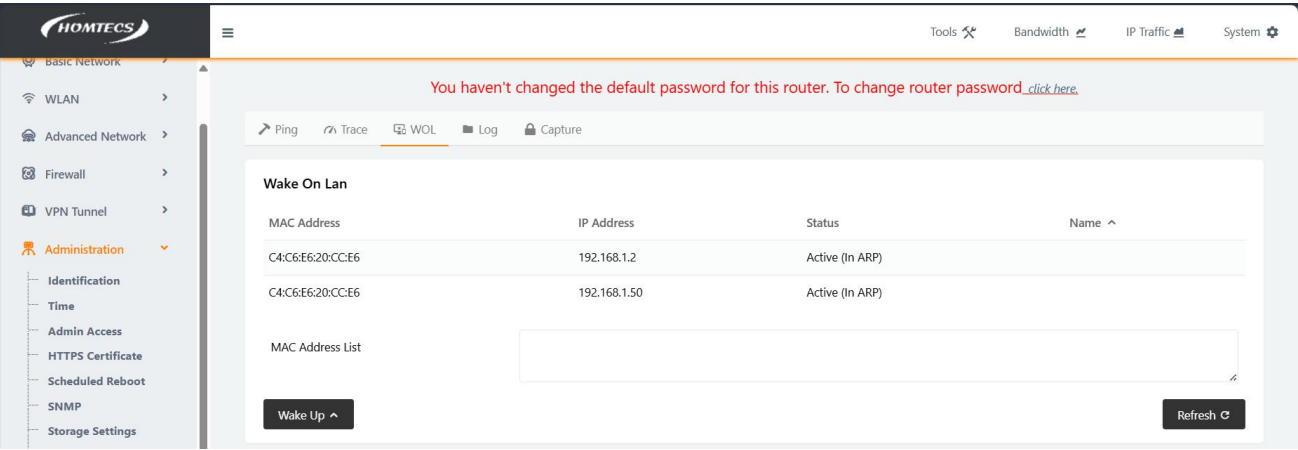


Figure 11-6

11.5. Bandwidth

There are many areas of bandwidth application, which can be used to identify the data transmission capacity of signal transmission, the amount of data passing through the link per unit time, and the display ability of the display.

1. In analog signal systems, it is also known as bandwidth, which refers to the amount of data that can be transmitted at a fixed time, that is, the ability to transmit data in the transmission pipeline. It is usually expressed in transmission cycles per second or hertz (Hz).
2. In digital devices, bandwidth refers to the amount of data that can pass through a link per unit of time. It is usually expressed in bps, which is the number of bits that can be transmitted per second.

In the navigation bar, select "Bandwidth". On the page, the real- time/last 24 hours/daily/weekly/monthly bandwidth information is displayed as shown in figure 11-7.

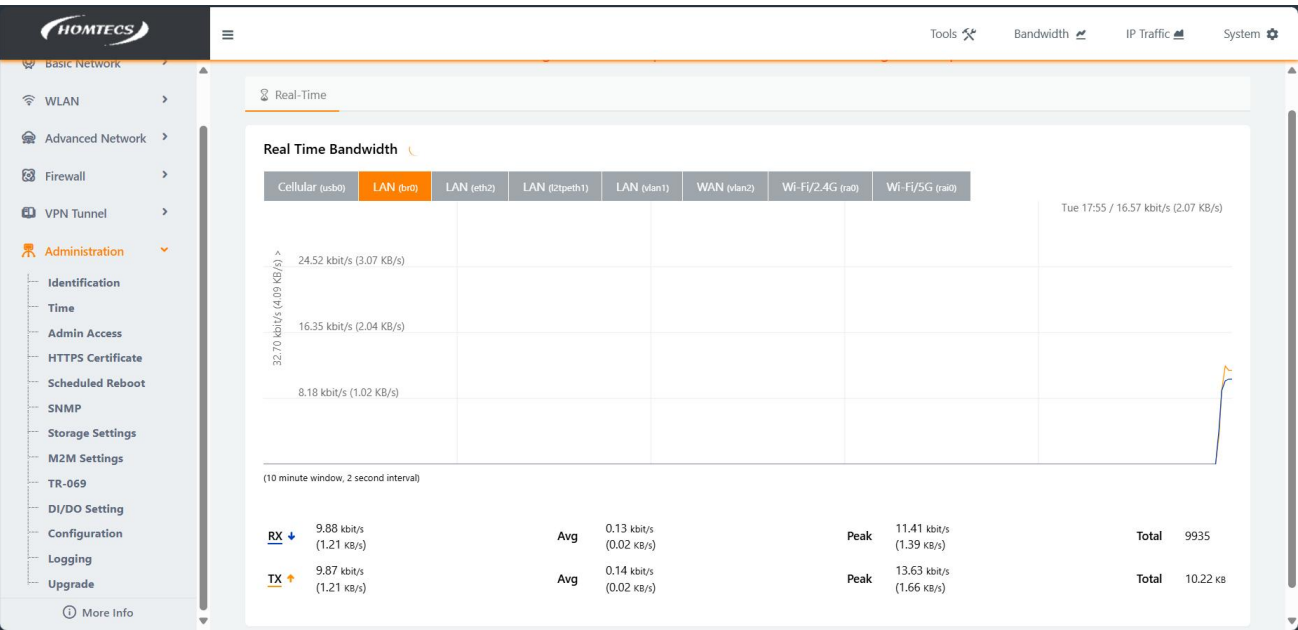


Figure 11-7

11.6. Traffic FigureTable

Traffic is a digital record, and router traffic records the number of bytes consumed by a device, and the units are B, KB, MB, and GB

Select "IP Traffic" in the navigation bar. In the page that opens, you can display real-time, last 24 hours, view graphs, transfer rate, and daily/monthly traffic information.

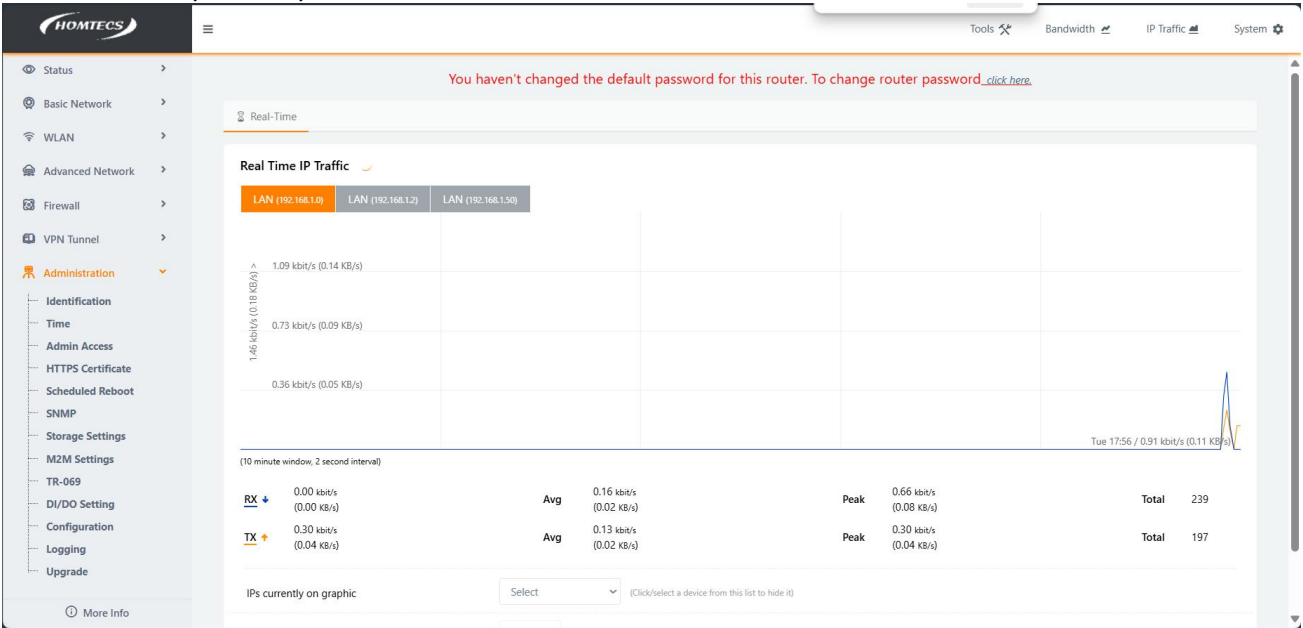


Figure 11-8

11.7. Factory reset via the RST button

If you forget your address or password and cannot log in to the WEB and other problems that require a factory reset, you can use the RST key to restore the factory settings.

1. RST button can be pressed and held with the tool for 30 seconds until the NET light stops flashing, and the system will automatically reboot and restore the factory settings to take effect.
2. After saving the parameters as the default configuration, the RST button can be pressed and held for 10 seconds, and the system will automatically restart and return to the saved default parameter values.

Default configuration of the system

Parameter	Default settings
LAN IP address	192.168.1.1
LAN subnet mask	255.255.255.0
DHCP server function	enable
Username	admin
Password	admin

Table 11-1 System Default Configuration



WARNING

When you do this, all configuration changes are cleared and you are restored to factory settings.

12. Issues handling

12.1. Hardware issues

12.1.1. None of the indicators are on

Problem phenomenon

None of the Router indicators are on.

Cause analysis

The possible causes are as follows:

The power supply does not meet the requirements

The power supply is not connected to the power port of the router

Solution

If the power supply does not meet the requirements, please make sure that the power supply range of the power supply is 5~36V.

If the power port of the router cannot be connected to the power supply, please plug the power cable into the power port.

12.1.2. SIM card connection issues

Problem phenomenon

The SIM card holder cannot be inserted properly.

Cause analysis

The possible causes are as follows:

The SIM card holder has been damaged

The SIM card is inserted in the wrong direction

Solution

If the SIM card holder is damaged, please contact our technical support engineer if you need to report for repair.

If the SIM card is inserted in the wrong direction, change and make sure that the SIM card is inserted into the card slot correctly.

12.1.3. Network port connection issues

Problem phenomenon

The LAN port indicator is not lit and the router page cannot be accessed.

Cause analysis

The possible causes are as follows:

The network cable is not installed correctly

The network cable is damaged

The PC NIC is working abnormally

Solution

If the network cable is installed incorrectly, please reinstall the network cable.

If the network cable is damaged, please replace the network cable.

If the network card on the PC side is working abnormally, please replace the network card.

12.1.4. Antenna connection issues

Problem phenomenon

The antenna does not fit properly

Cause analysis

possible causes are as follows:

The antenna does not meet the requirements of the accessories

The antenna connection is incorrect

Solution

If the antenna is installed incorrectly, replace the antenna that meets the requirements.

If the antenna is not connected correctly, please reconnect the antenna.

12.2. Dial-up issues

12.2.1. Dial-up dropped

Problem phenomenon

The Router is interrupted during dialing and fails to dial.

Cause analysis

possible causes are as follows:

The SIM card network type does not meet the requirements

The SIM card is in arrears

The power supply does not meet the requirements

Modem dialing configuration is incorrect

Solution

If the SIM card network type is incorrect, please replace the corresponding type of SIM card according to the module.

If the SIM card is in arrears, please go to the designated ISP to top up the SIM card.

If the power supply does not meet the requirements, please replace the power supply that meets the requirements.

If the modem dial-up configuration is incorrect, please refer to "Mobile Network" for correct configuration.

12.2.2. No signal display issues

Problem phenomenon

The Router mobile network status page is not displayed.

Cause analysis

possible causes are as follows:

The antenna connection is not normal The modem is not dialed on the line Modem disconnected

Solution

Reconnect the antenna as per the correct operation.

If the modem does not dial the number, see "Mobile Network".

If the modem is disconnected, please check whether there is a process in the application of the router that causes the router to go offline.

12.2.3. SIM/UIM card could not be found

Problem phenomenon

The Router mobile network status page shows that the SIM card could not be found.

Cause analysis

possible causes are as follows:

The SIM card is damaged

The SIM card is loose, the contact is not normal, or the installation is incorrect

Solution

If the SIM card is damaged or invalid, replace the SIM.

If the SIM card is loose, has abnormal contact, or is not installed correctly, please reinstall it.

12.2.4. Communication signal is weak

Problem phenomenon

The Router Mobile Network Status page shows no or poor signal.

Cause analysis

possible causes are as follows:

The antenna is not installed or damaged

The network coverage and signal strength of the area where the device is located are weak

Solution

Reconnect the antenna as per the correct operation.

If the antenna is damaged, replace the antenna.

If the network coverage and signal strength in the area where the device is located are weak, contact the network operator for a reasonable solution.

12.3. VPN connection issues

12.3.1. VPN can't connect

Problem phenomenon

The status page shows that the VPN could not connect

Cause analysis

The possible causes are as follows:

The interface used by the VPN connection is not working properly

The VPN configuration parameters are incorrect

The VPN peer server is not working properly

Solution

If the interface used by the VPN connection is not working properly, reconfigure the interface used correctly.

If the modem interface is not working properly, see Mobile Network.

If the VPN interface is not working properly, see VPN Configuration.

If the VPN configuration parameters are incorrect, see VPN Configuration.

If the VPN peer server is not working properly, check the configuration and working status of the VPN peer server.

12.3.2. The VPN can't communicate

Problem phenomenon

The VPN page shows that it is connected, but it is unable to communicate

Cause analysis

possible causes are as follows:

The route information configured in the routing table is incorrect The VPN peer server is incorrectly configured

Solution

If the route is incorrect, add the correct route

If the VPN peer server is incorrectly configured, change the configuration of the VPN peer server.

12.4. WEB configuration operation issues

12.4.1. firmware upgrade failed

Problem phenomenon

The firmware upgrade found that the upgrade was not successful

Cause analysis

possible causes are as follows:

The router restarts due to other functions during the upgrade The power supply does not meet the requirements

The model and format of the upgraded firmware are incorrect

The router loses power during the upgrade

Solution

If the upgrade fails due to the restart due to other functions during the upgrade, please disable the other functions and upgrade again.

If the power supply does not meet the requirements, replace the power supply that meets the requirements.

If the firmware version is incorrect, replace the firmware with the correct format and match the Router.

If the router is powered off during the upgrade, make sure that the router is powered normally during the upgrade.

12.4.2. Forgot router password

Problem phenomenon

I forgot my password when logging in to the router page

Cause analysis

The user has changed the password on the user management page

Solution

Step 1: The router is powered on

Step 2: Press and hold the RST reset button for about 15 seconds for the system to reboot successfully, otherwise try the operation again.

12.4.3. Frequent reboot issues

Check first:

Whether the module is normal.

Whether the Router is inserted into the SIM card.

Whether the SIM card is enabled for data service and whether it is shut down in arrears.

Whether the dialing parameter account/password is correct. Check if the signal is normal.

Check if the power supply voltage is normal.

12.5. Other issues

12.5.1. After modifying the IP address, I forgot to configure the Router and could not set it

The router is powered on, and the REST settings button can be restored by pressing and holding the REST settings button (until the system restarts).

12.5.2. Why is the network indicator not lit when connected to the PC after powering on?

When the PC and Router are directly connected through a network cable, please check whether the PC and Router are connected with a network crossover cable. Check if the network cable is normal.
