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

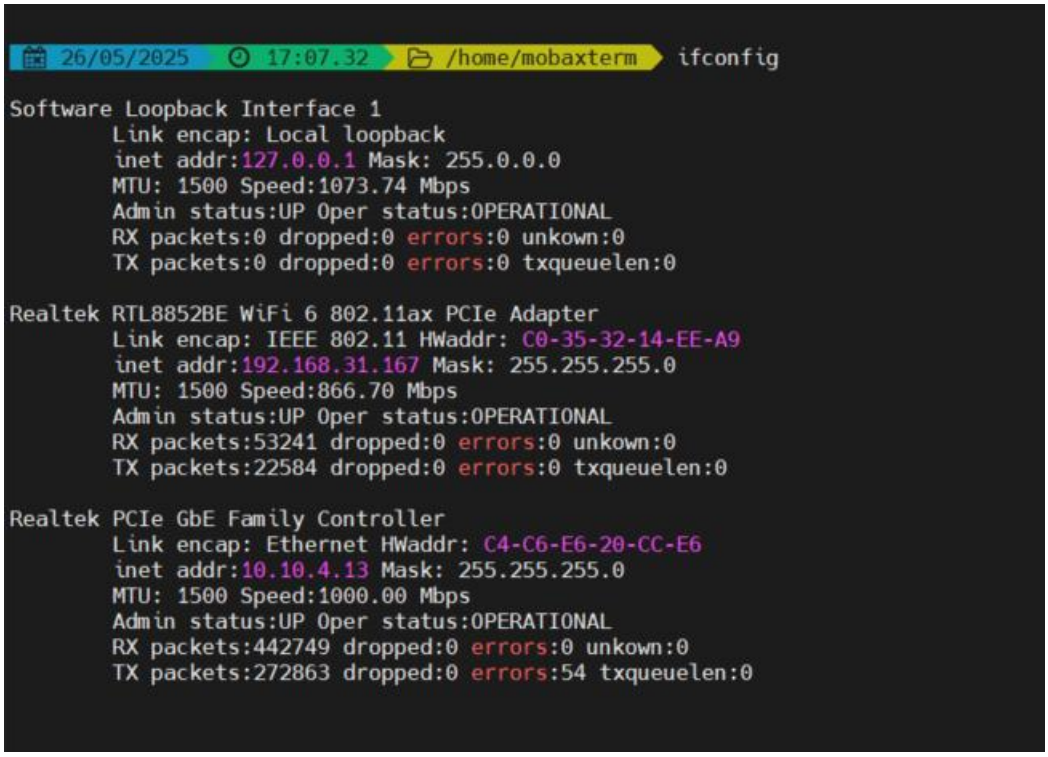


Figure 7-21

Step 2:

Open the routing web interface, select IP penetration in the advanced network, enable the IP penetration 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

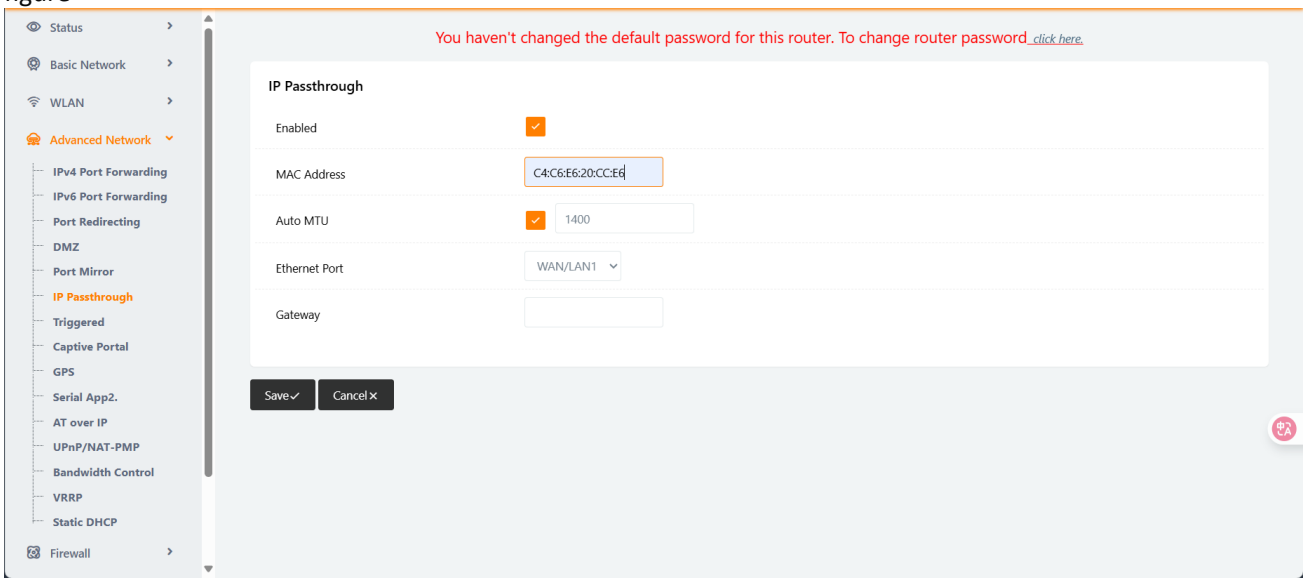
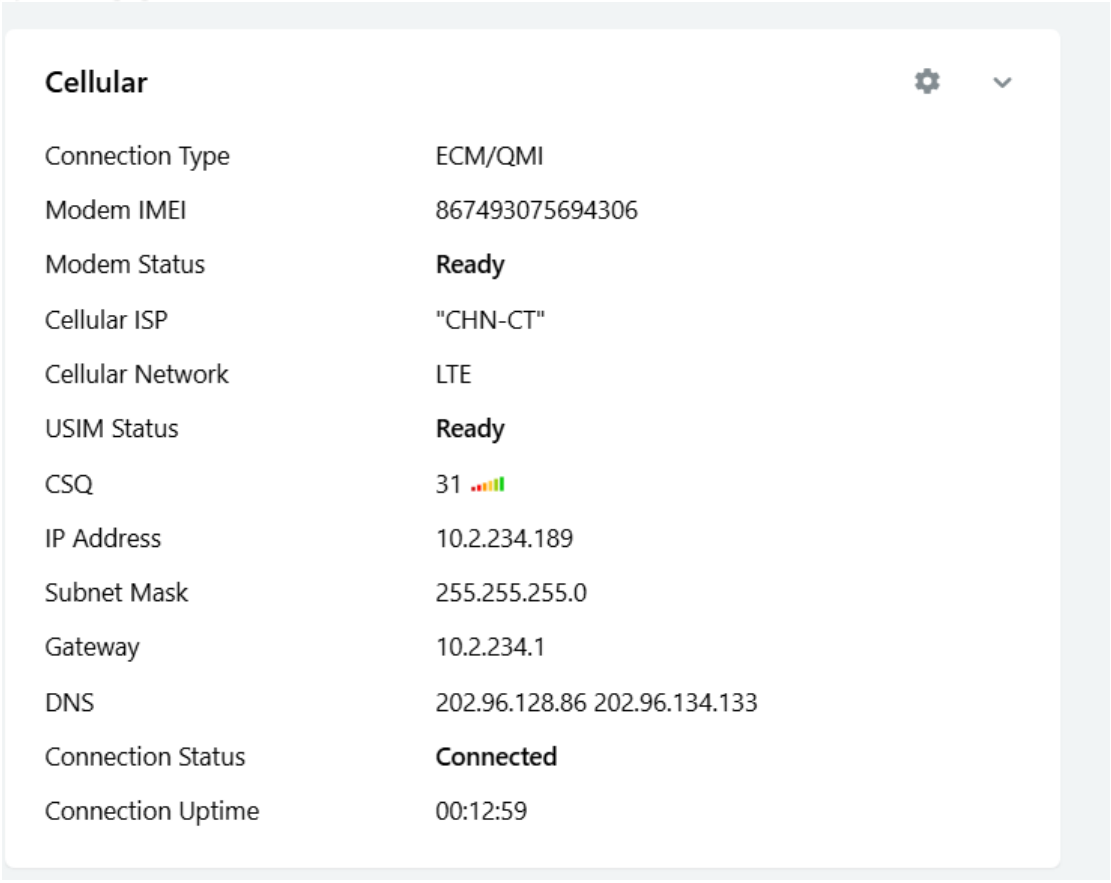


Figure 7-22 IP traversal configuration

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



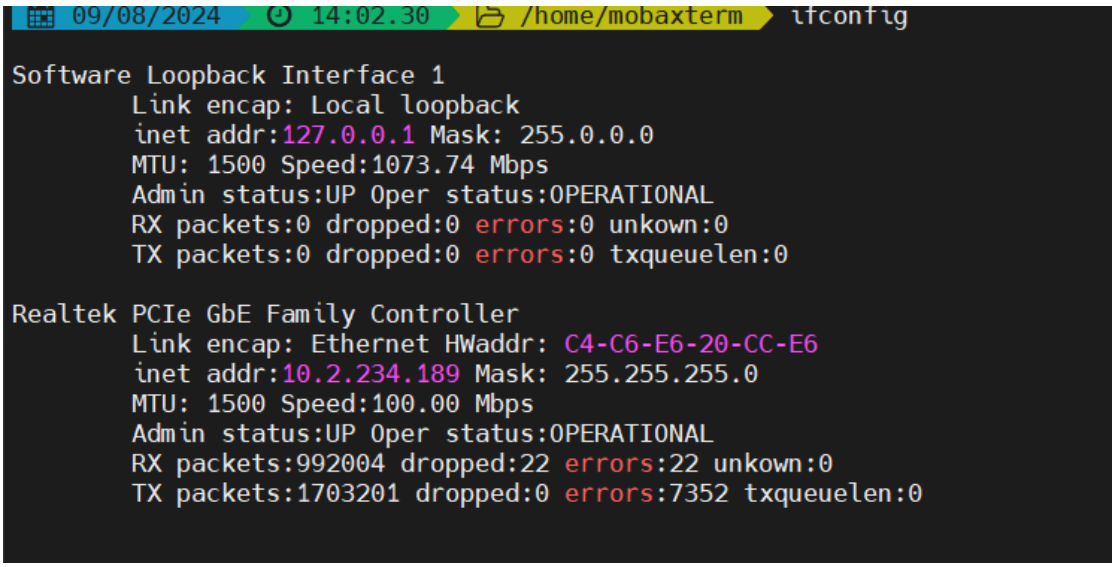


Figure 7-23 IP traversal

7.7. Triggered Port Forwarding

Triggered Port Forwarding. 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 > Port Trigger. On the page that opens, you can modify the parameters

related to the configuration port trigger function.

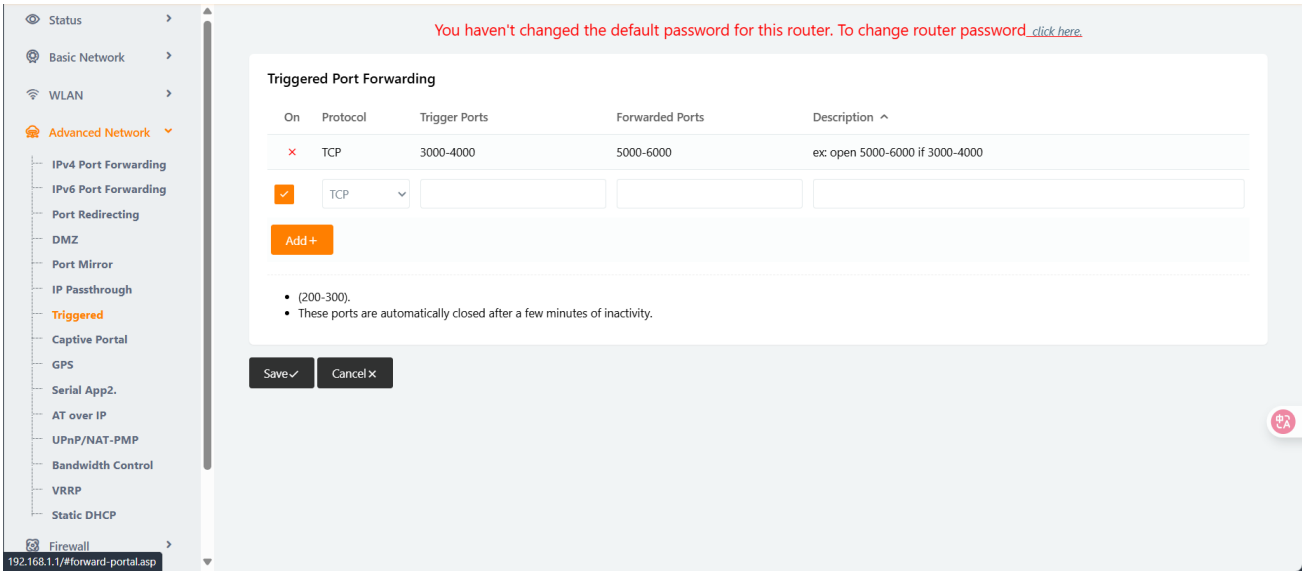
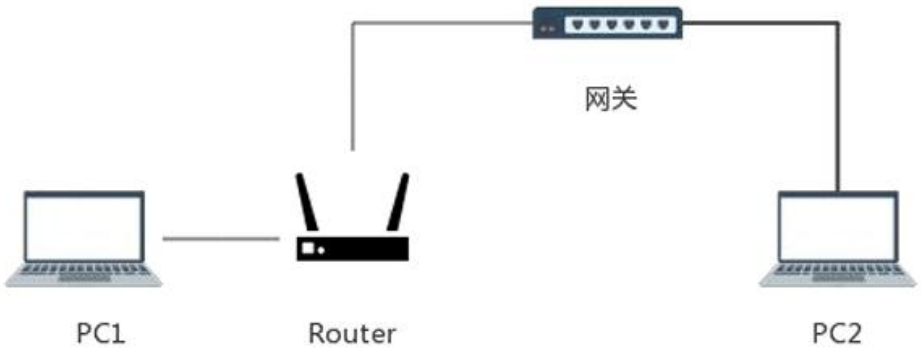


Figure 7-24 Port Triggering

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

Port trigger configuration example:

Step 1:



FTP (server:21) 192.168.10.94 192.168.10.95 FTP(client:8080)

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

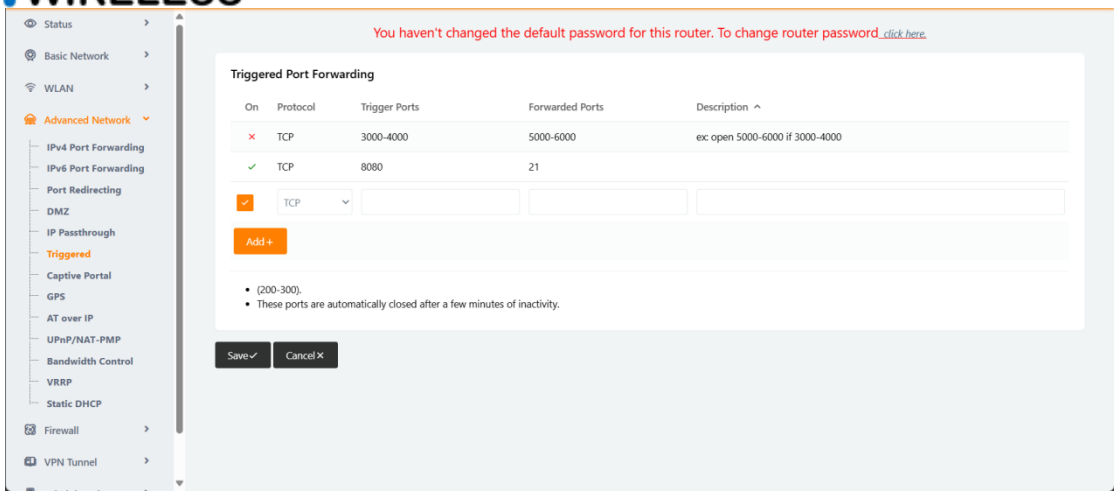


Figure 7-26 Port Trigger Configuration

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):

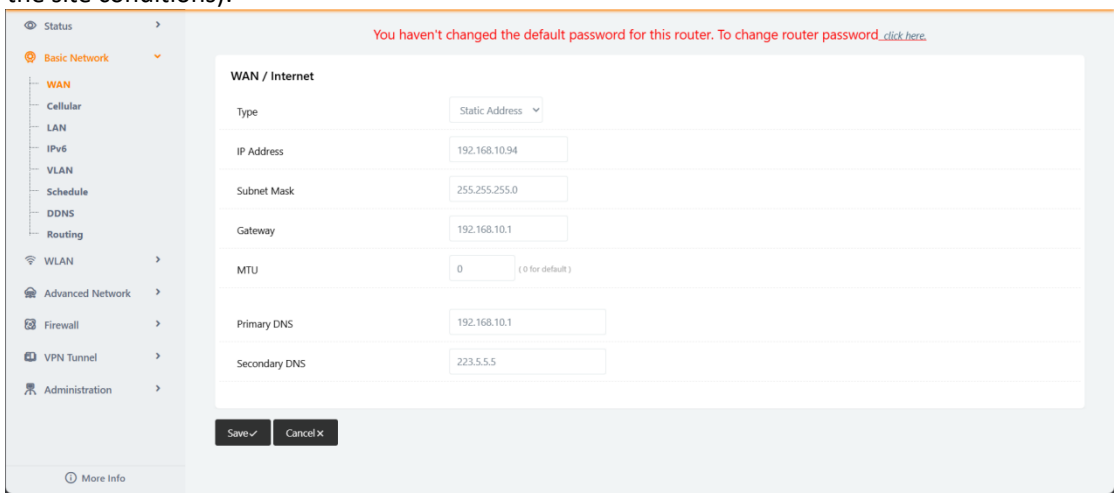


Figure 7-27 Static address settings

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

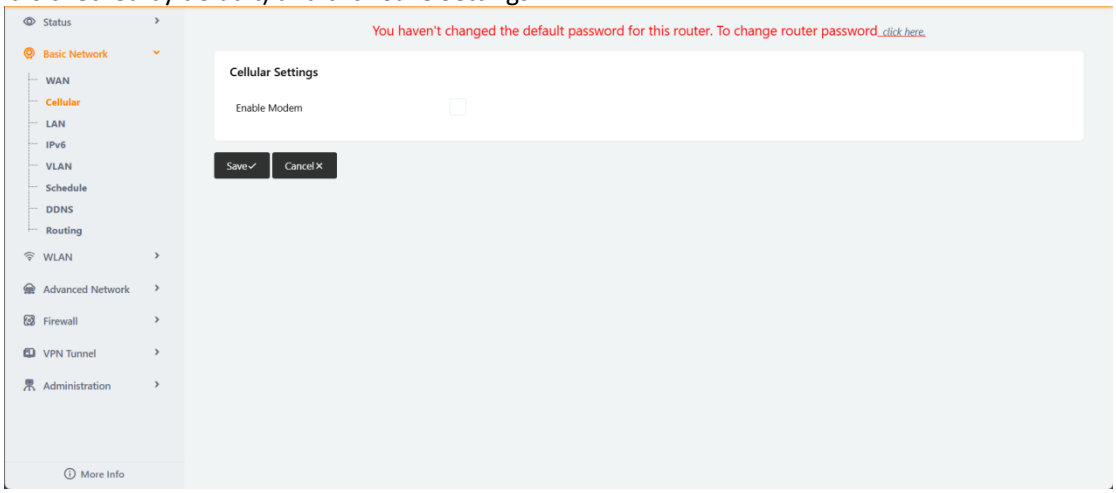


Figure 7-28 Mobile Network Settings

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:

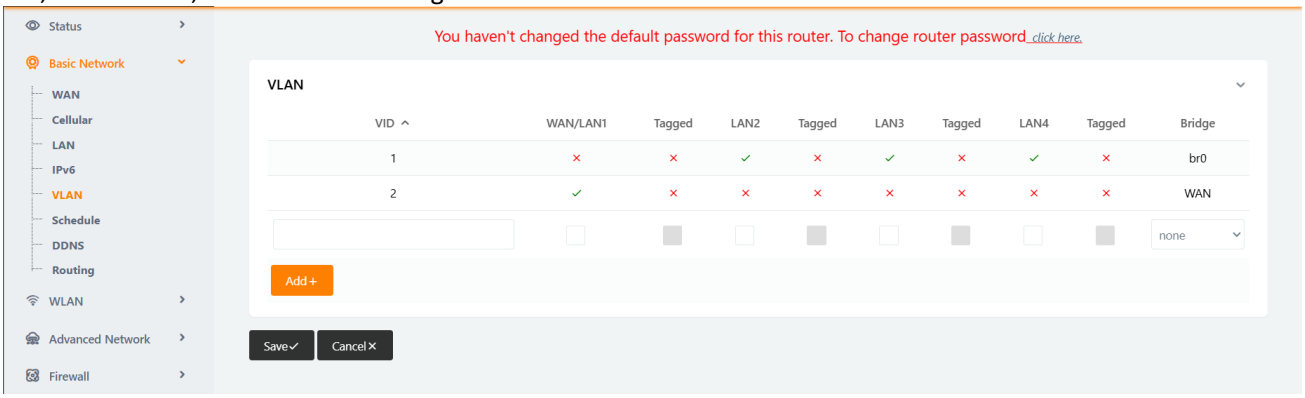


Figure 7-29 VLAN Settings

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

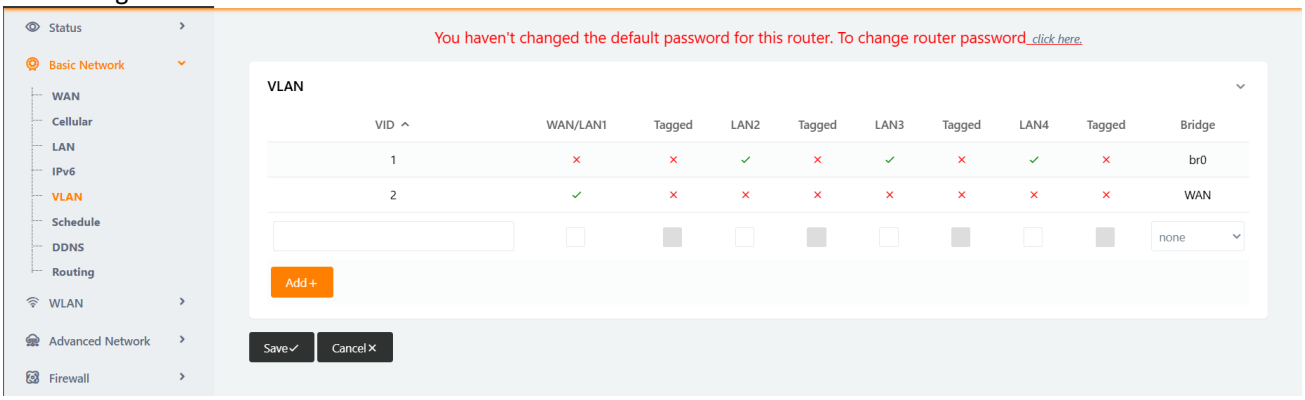


Figure 7-30 VLAN Settings

Step 5:

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

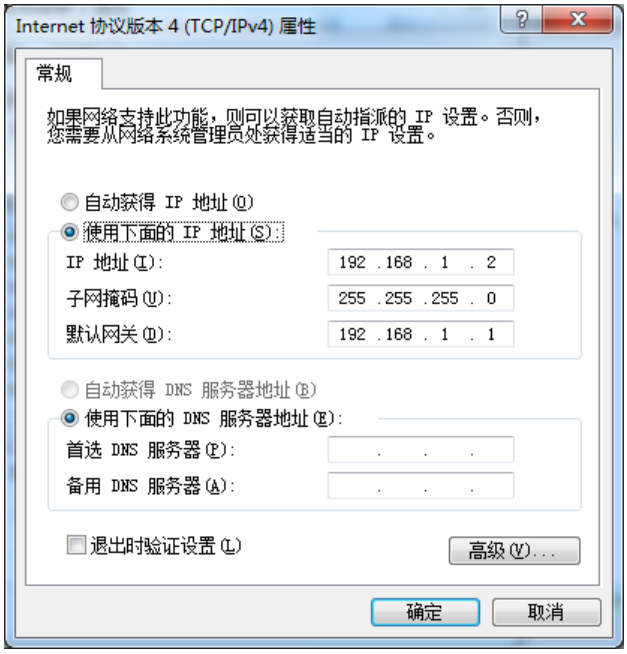


Figure 7-31 Local Connection Diagram

Step 6:

Open the TCP-UDP tool as the client (PC2 as the server)

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

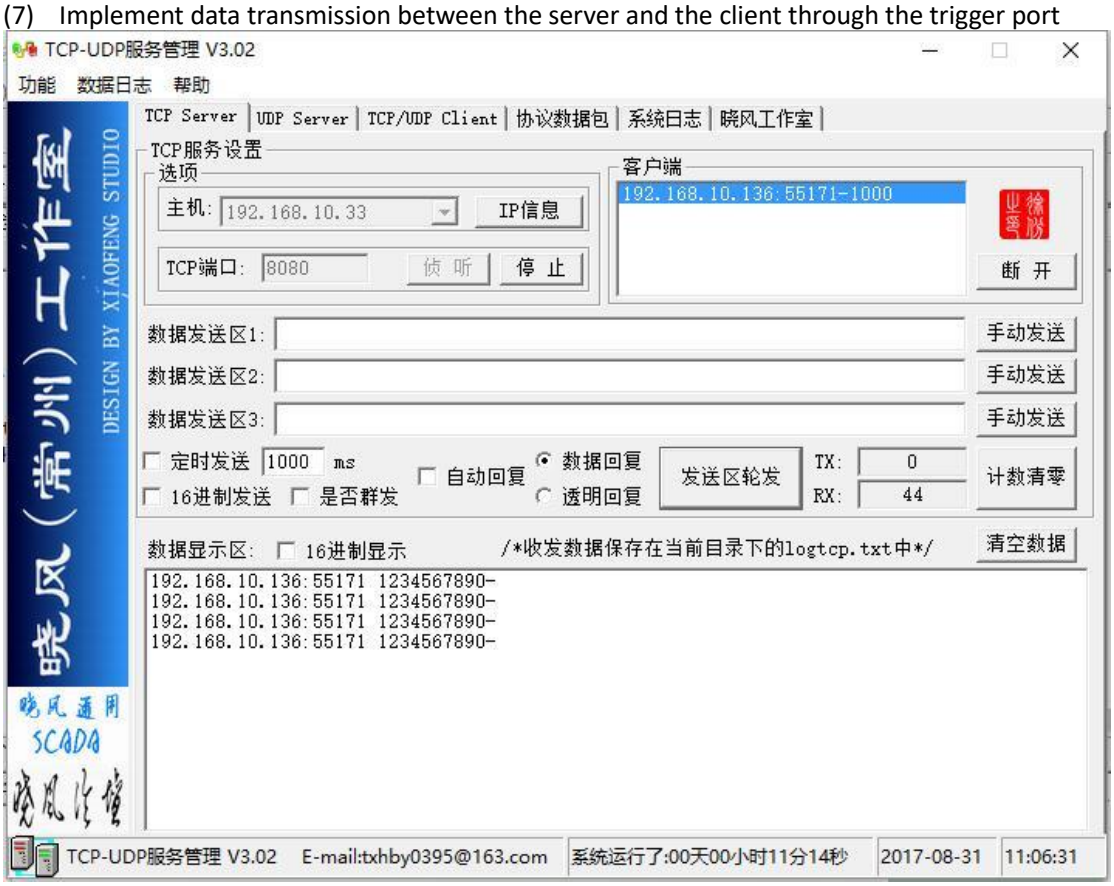


Figure 7-32 Data is sent and received from each other

Step 7:

PC1 Open FTP Easy Version Tool

(1) New User

(2) Configure user password and file path

(3) Click to save

(4) Click the start button

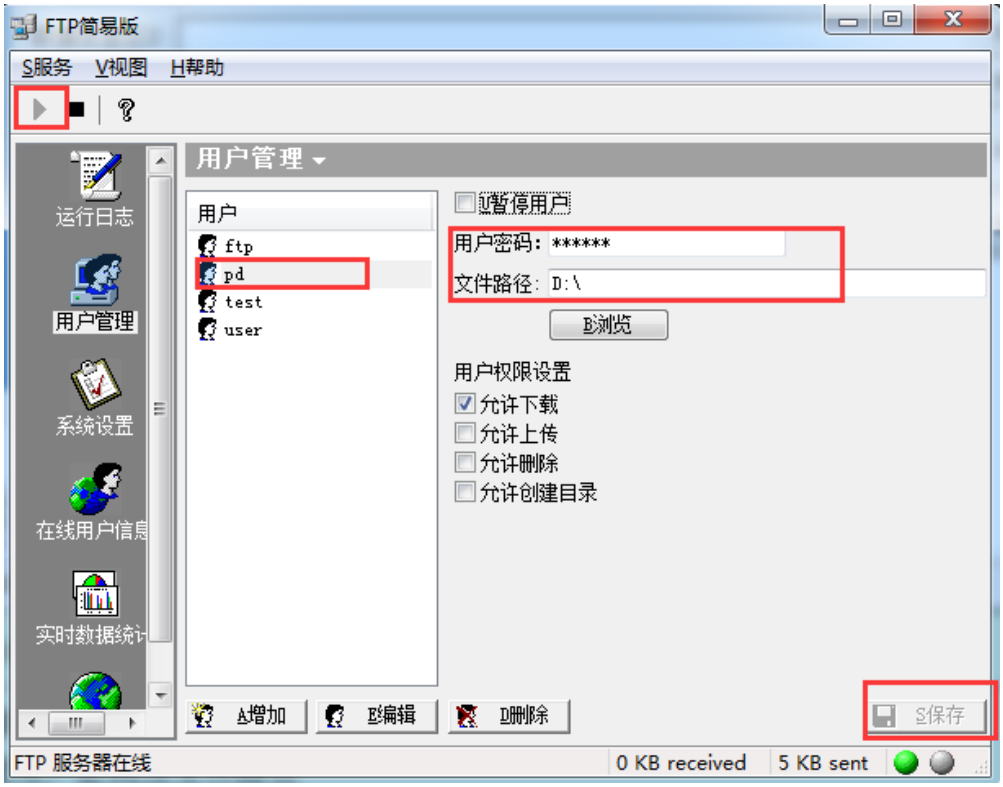


Figure 7-33 FTP Lite configuration

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. Portal advertising

WARNING

Both 5200 and 5500 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

In order to achieve the purpose of advertising push and business promotion.

At present, we can pop up the following three pages:

The page is a simple pop-up page with an image ad, please see the renderings below. On this page, users can click the "Agree to the following terms" button and can directly access the Internet normally.

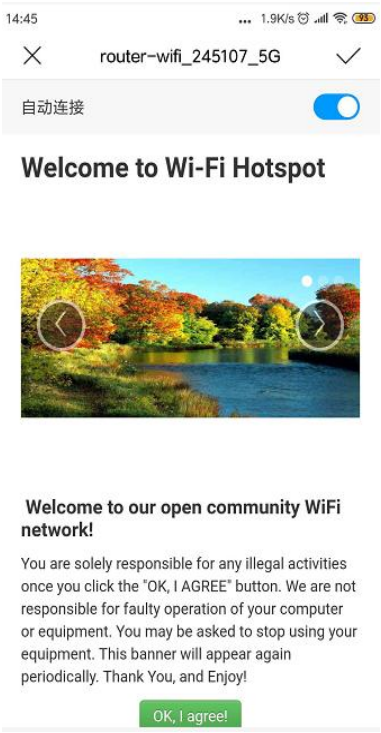


Figure 7-34

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.

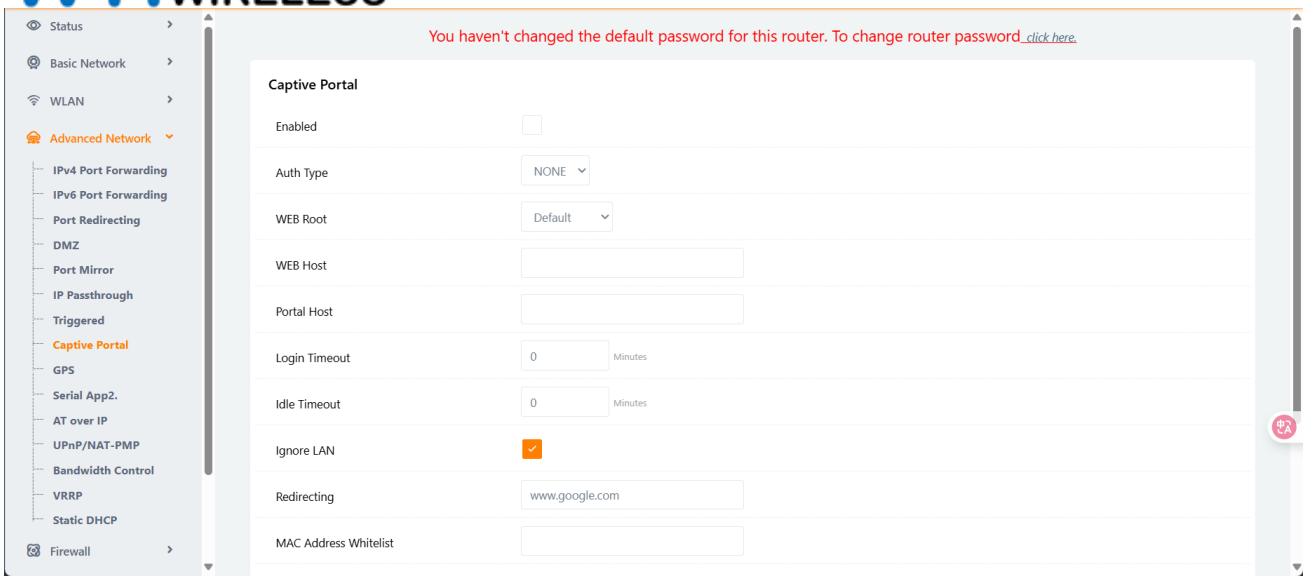


Figure 7-35

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

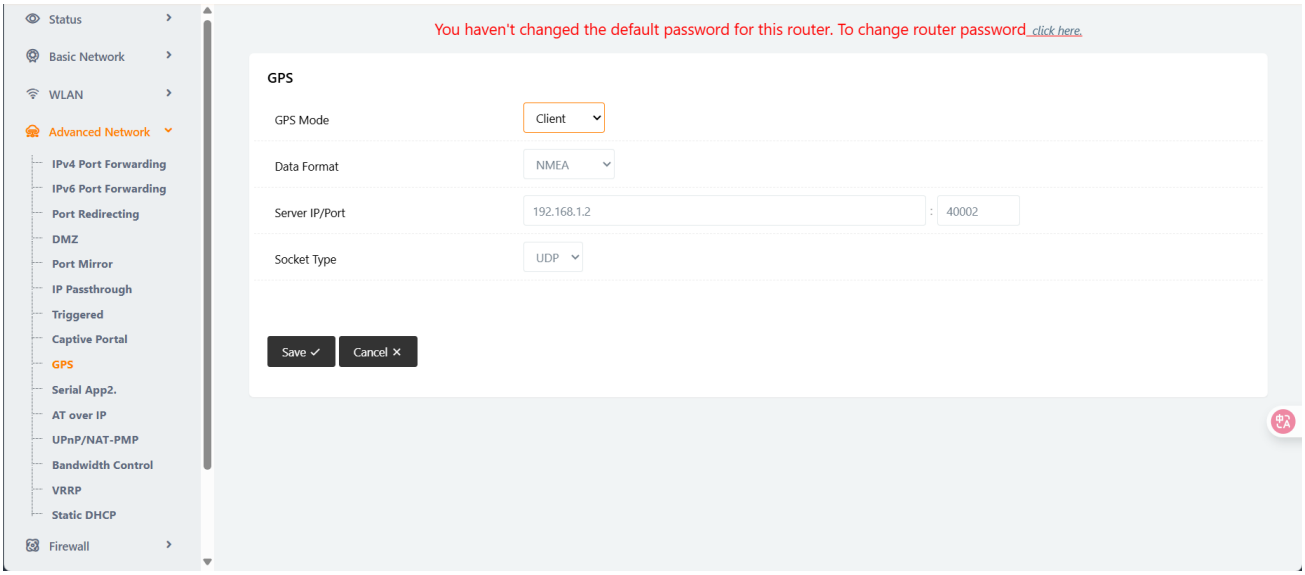


Figure 7-41

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

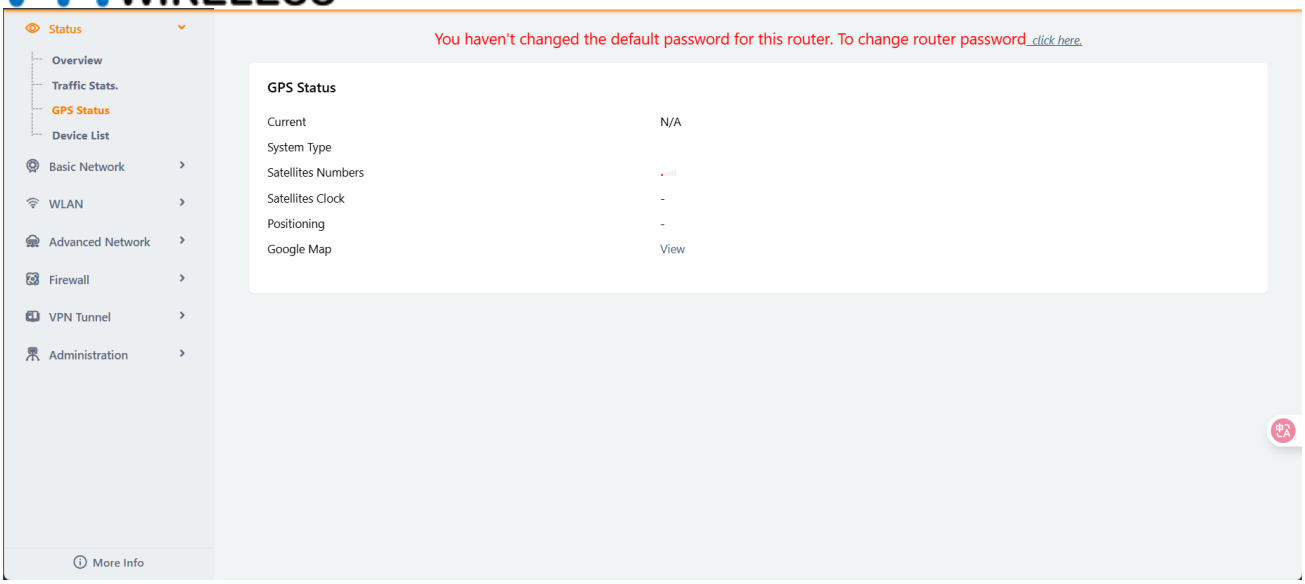


Figure 7-42

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.

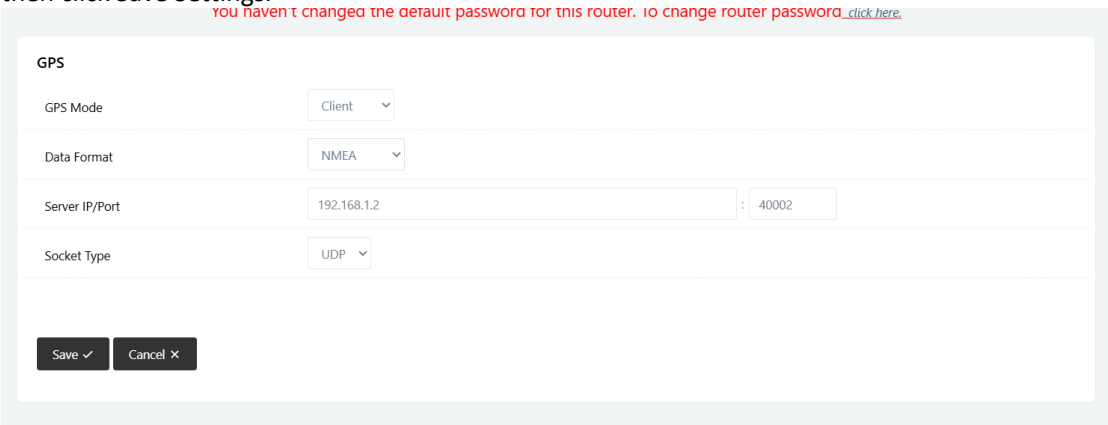


Figure 7-43 GPS configuration

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:

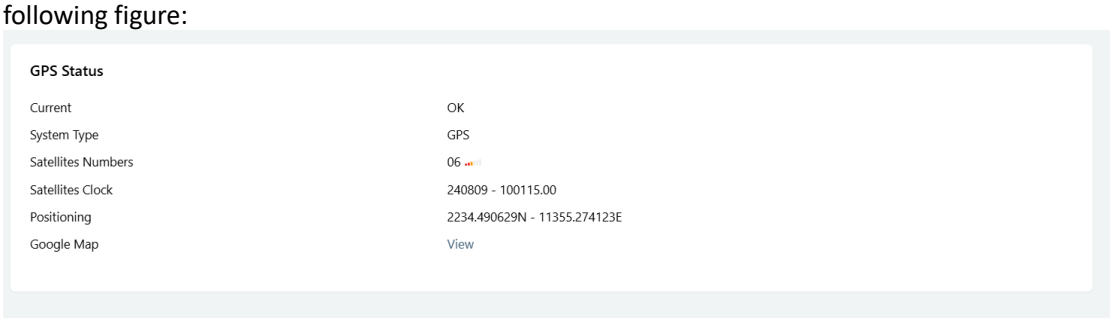


Figure 7-45 GPS status display

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.

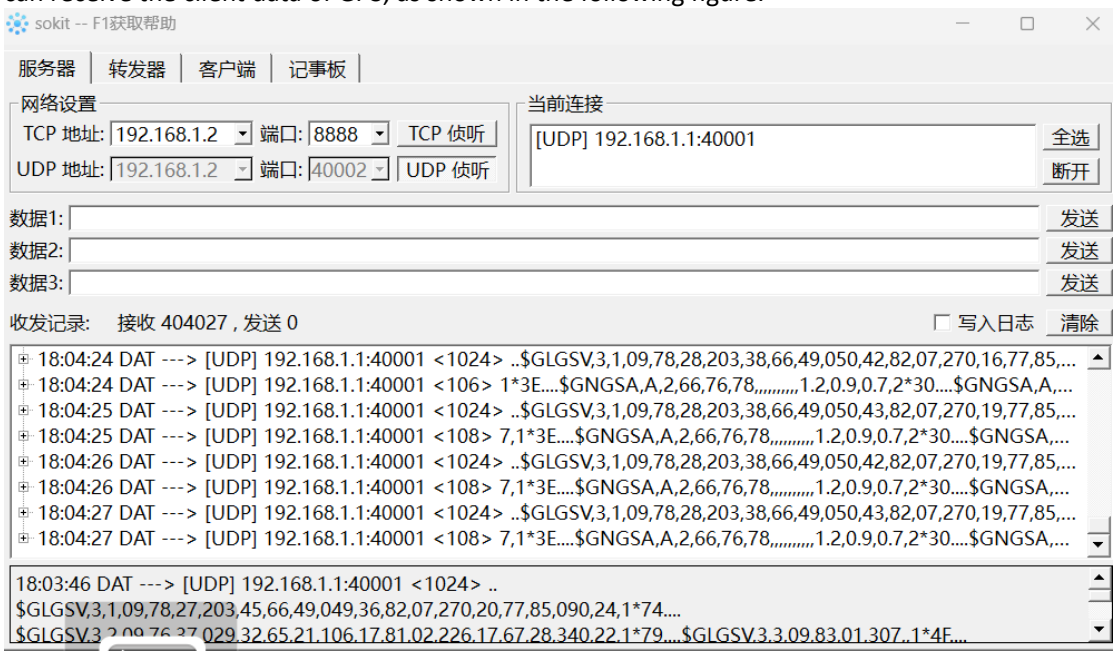


Figure 7-46 TCP-UDP receives GPS packets

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 5200, click Save

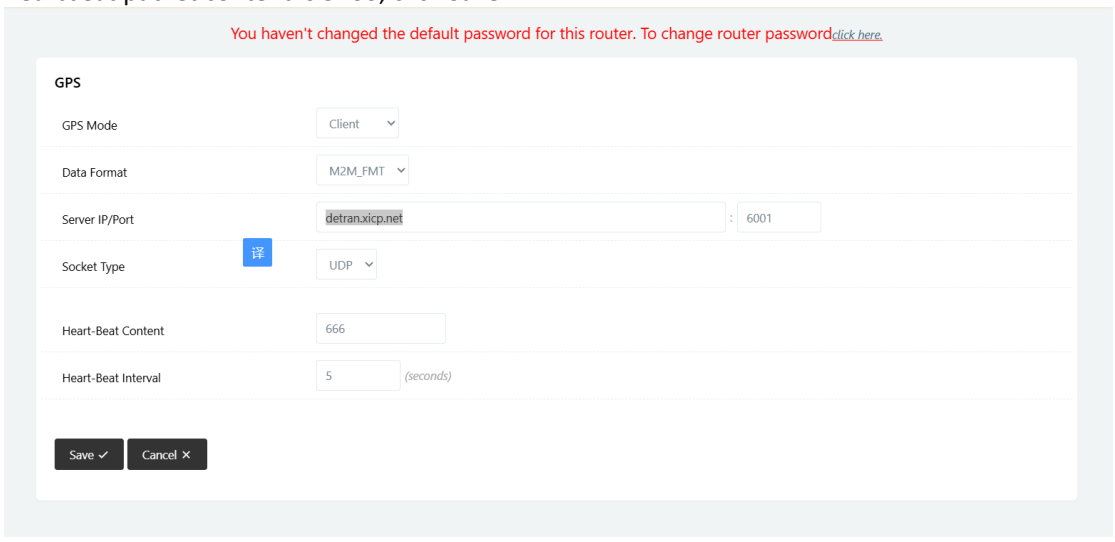


Figure 7-47 GPS configuration

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

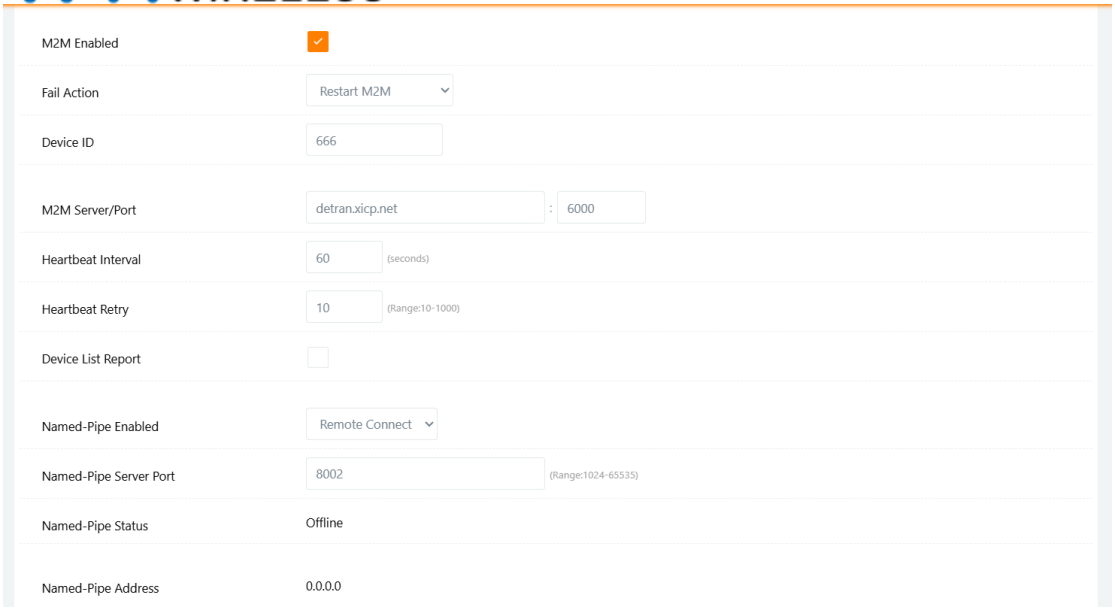


Figure 7-48 M2M Platform Management Settings

Step 3:

Log in to the Detran 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

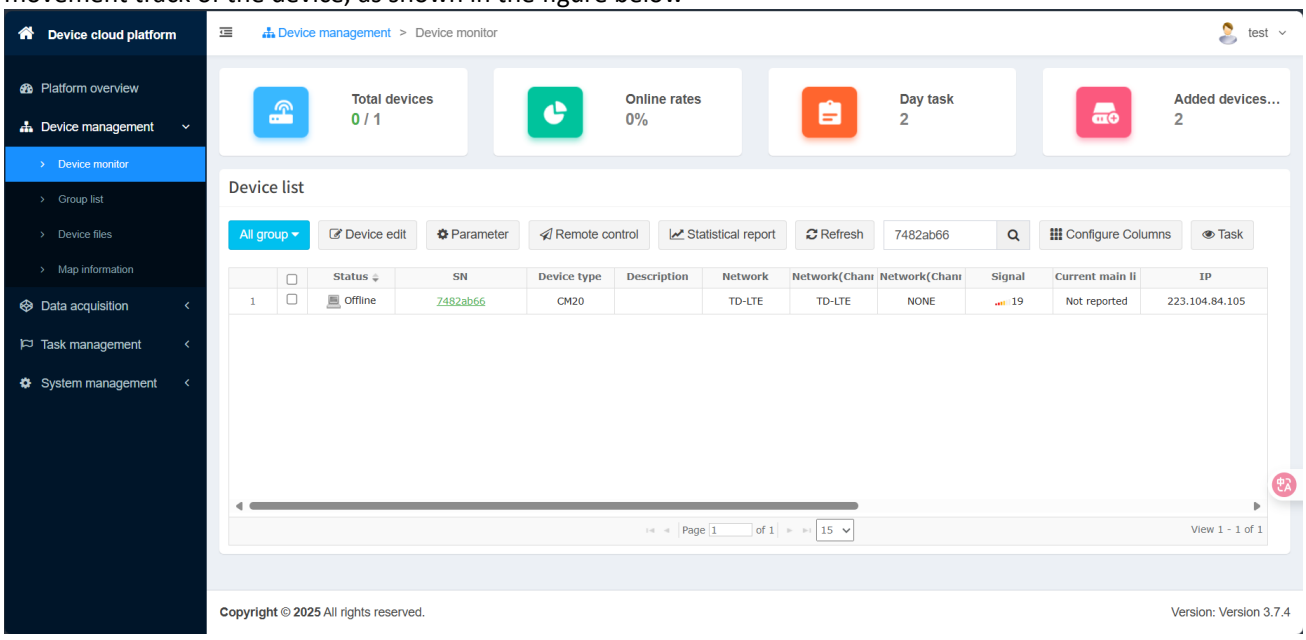


Figure 7-49

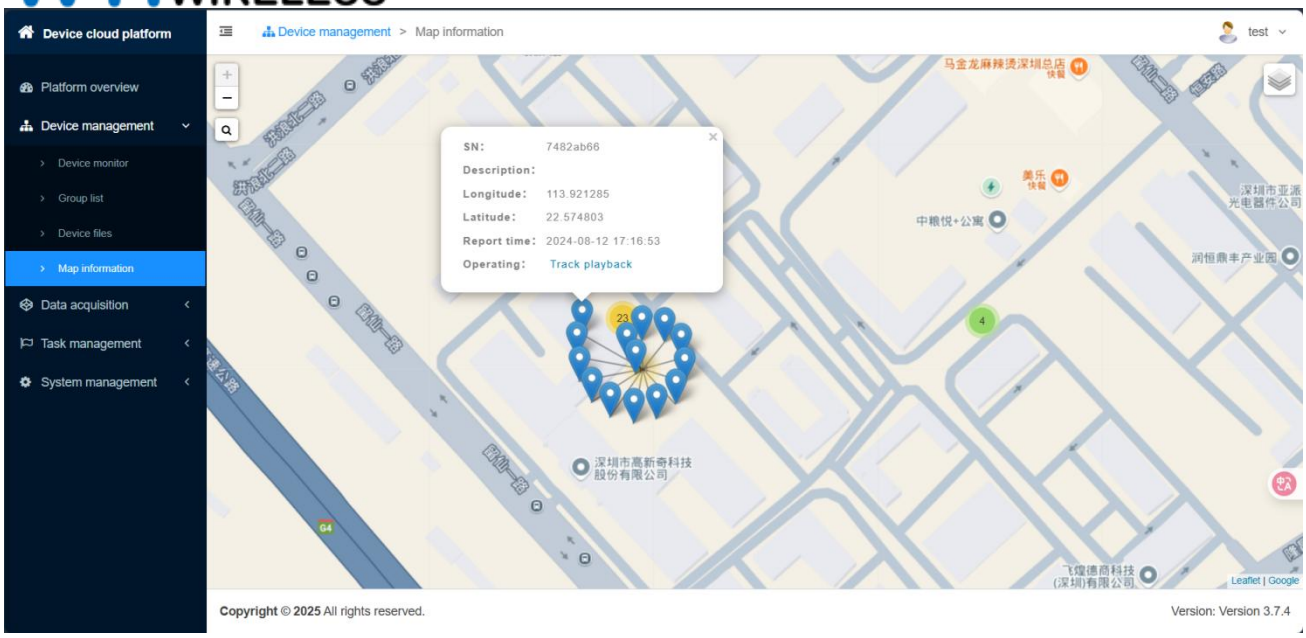
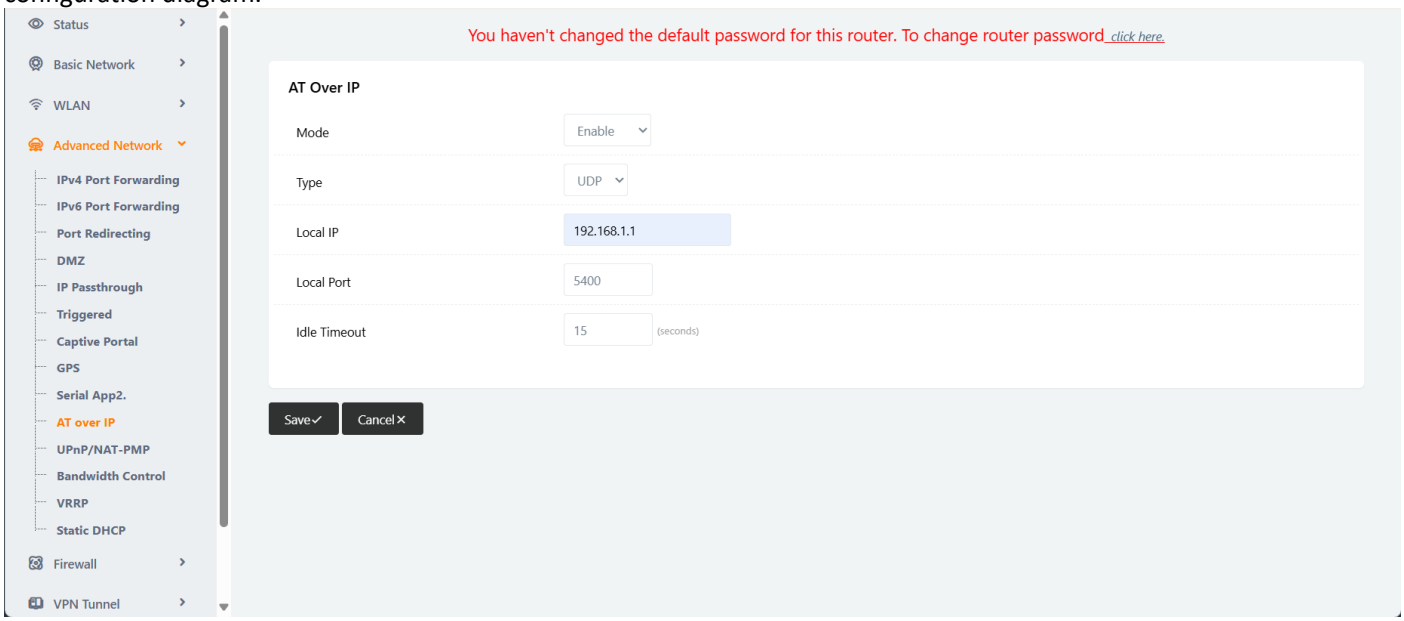


Figure 7-50 Platform device trajectory display

7.10. AT over IP

At over IP can be understood as querying module commands by specifying the IP and port number, as shown in the configuration diagram.



By executing the cmd command: telnet 192.168.1.1 5400, you can execute the query at command or modify the at parameter of the module, as shown in the figure

```
08/12/2023  13:44.28  /home/mobaxterm  telnet 192.168.1.1 5400
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
at
a
OK
t+at

ERROR
at+qcfg="usbnet"

+QCFG: "usbnet",0

OK
at+qgps?

+QGPS: 1

OK
Connection closed by foreign host.
```

7.11. UPnP settings

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" in the navigation bar. On the page that opens, you can modify the parameters for configuring UPnP.

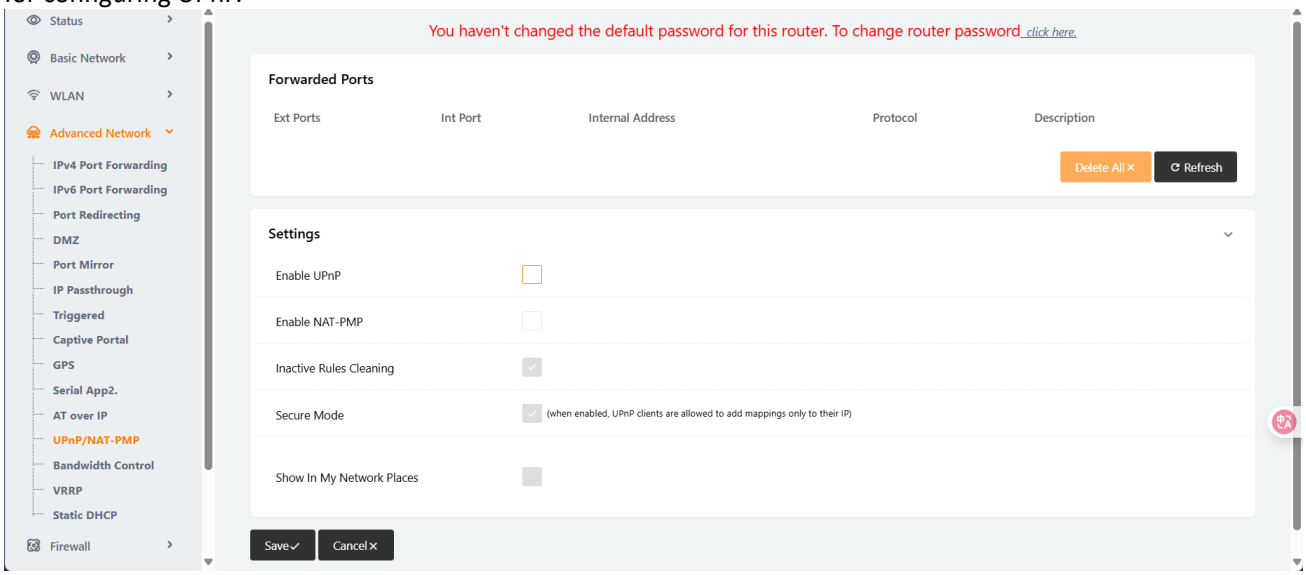


Figure 7-51

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 Rate Limiting" in the navigation bar. On the page that appears, you can modify the parameters for configuring bandwidth rate limiting.

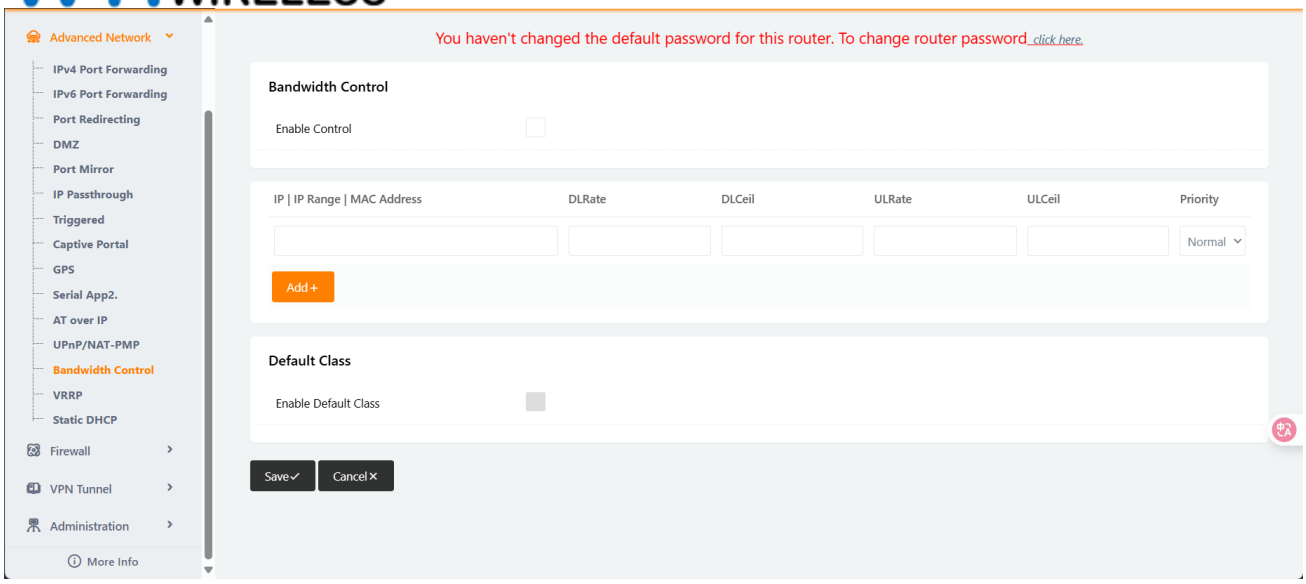


Figure 7-52

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.

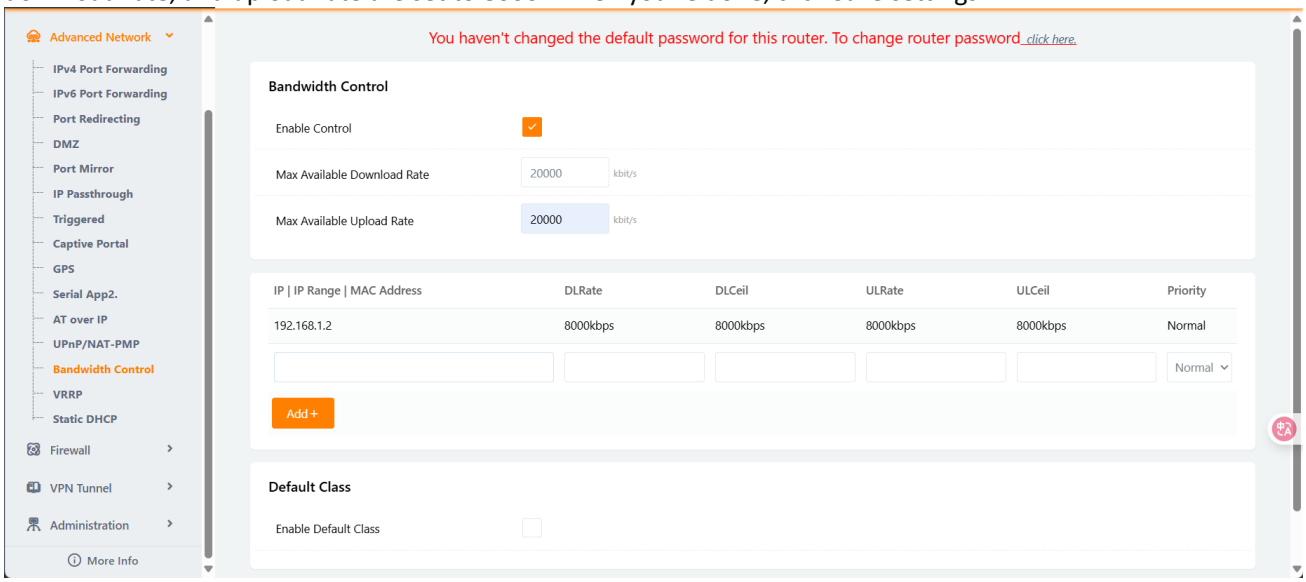


Figure 7-53 Bandwidth rate limiting configuration

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)

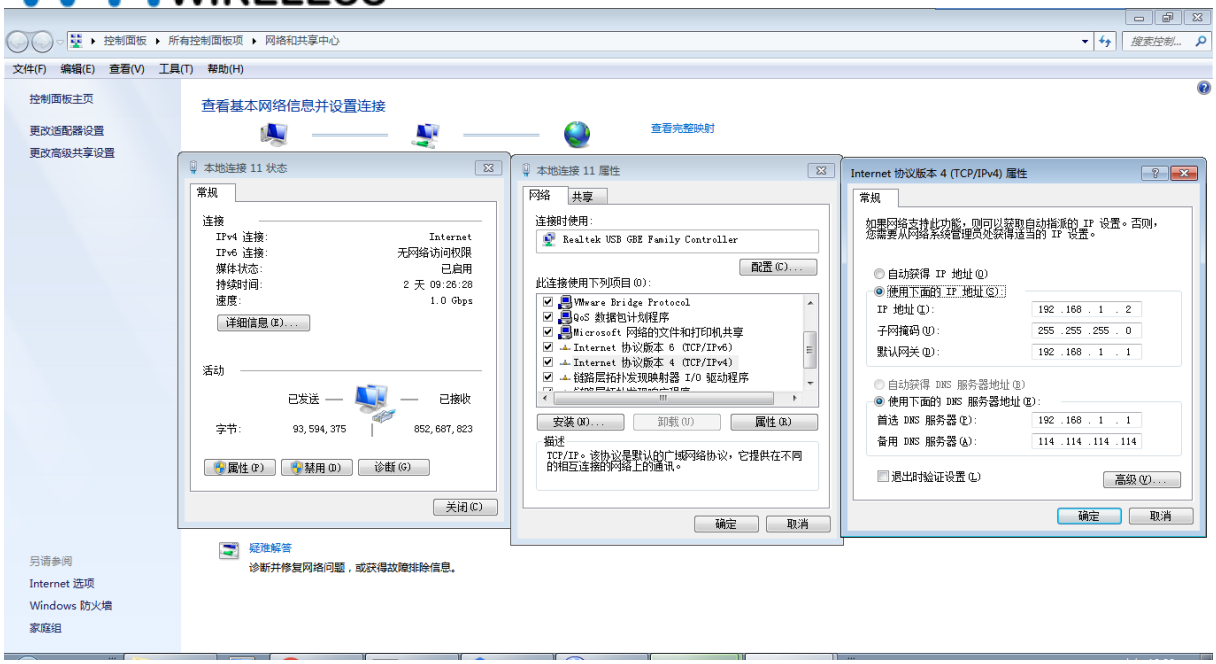


Figure 7-54 PC Local Connection Configuration

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

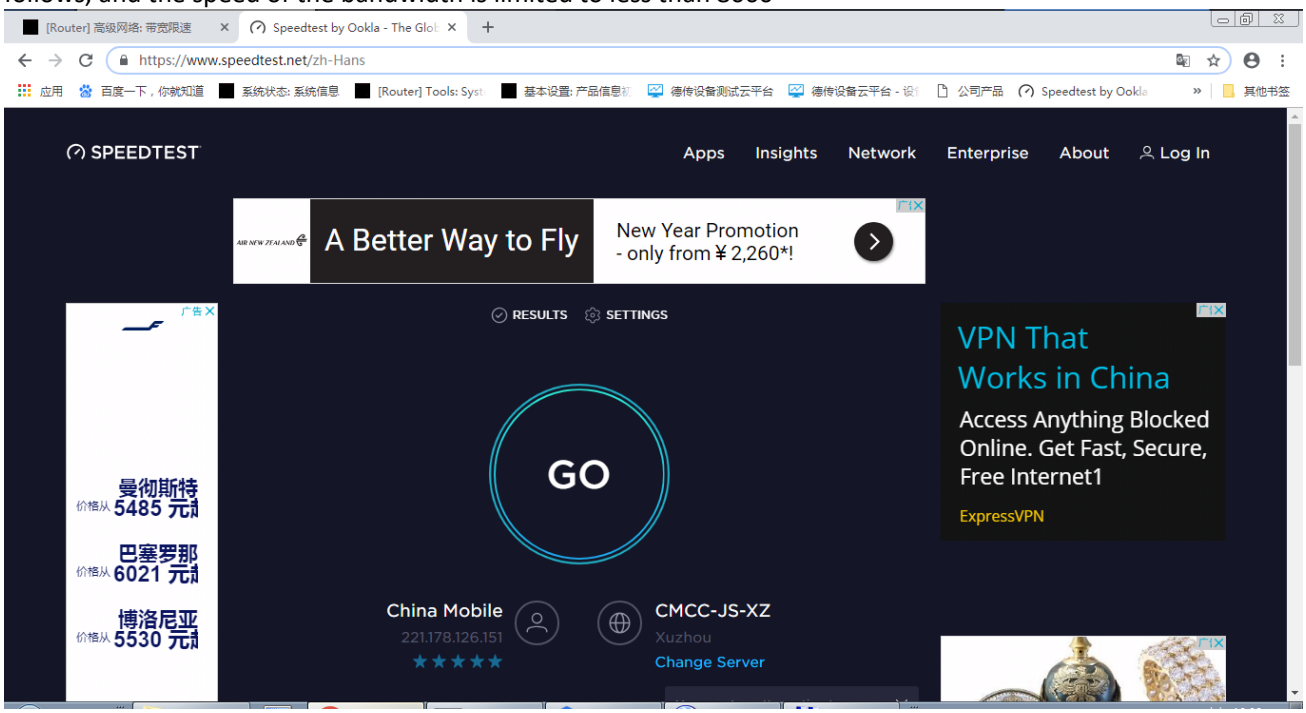


Figure 7-55



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.

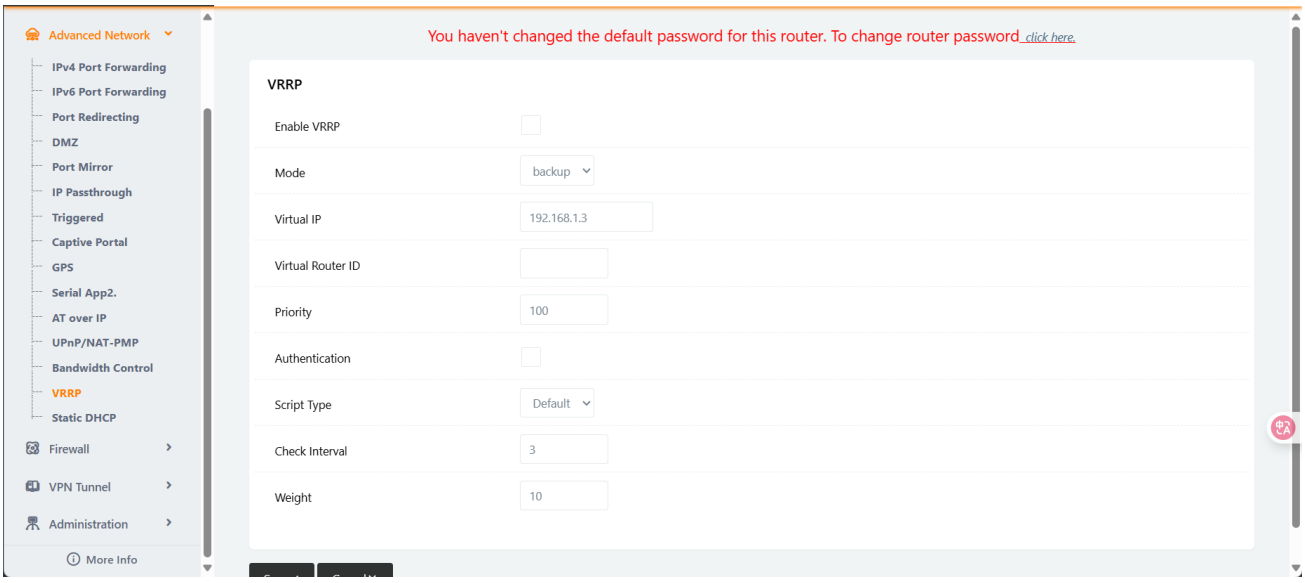


Figure 7-57

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

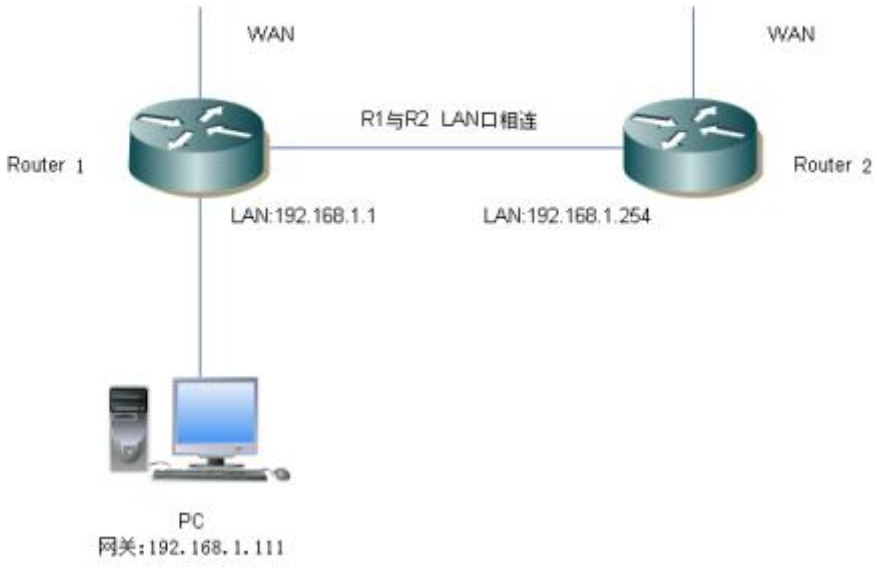


Figure 7-58 VRRP networking diagram

Primary Route Configuration (Router1).

Step 1:

LAN Configuration (Primary Routing Gateway is still 192.168.1.1)

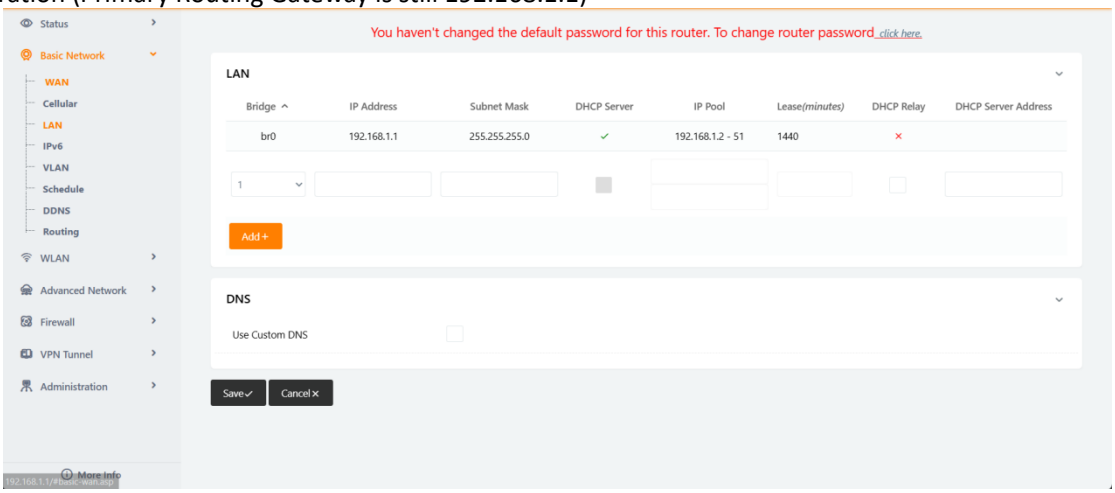


Figure 7-59 Local Area Network

Step 2:

In the navigation bar, select Basic 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):

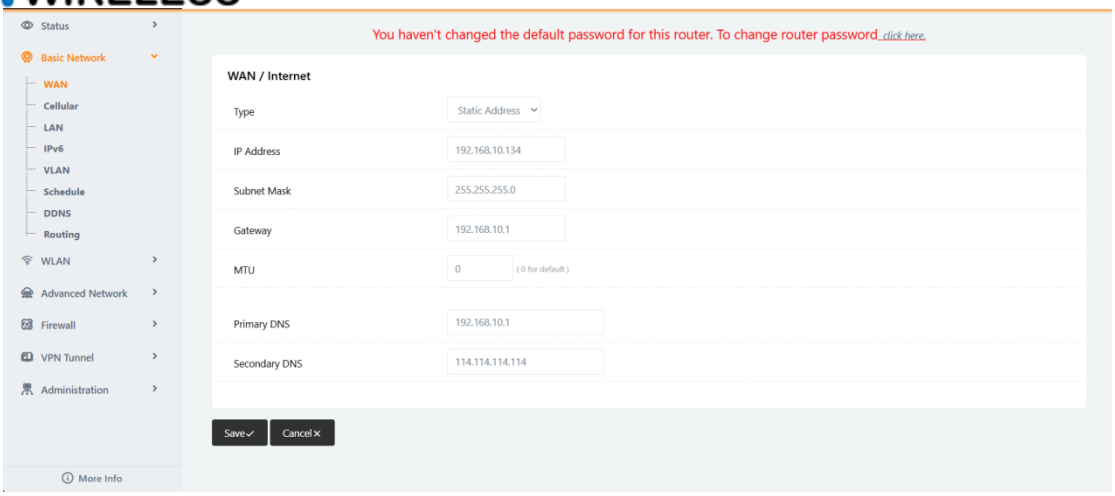


Figure 7-60 Static address settings

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

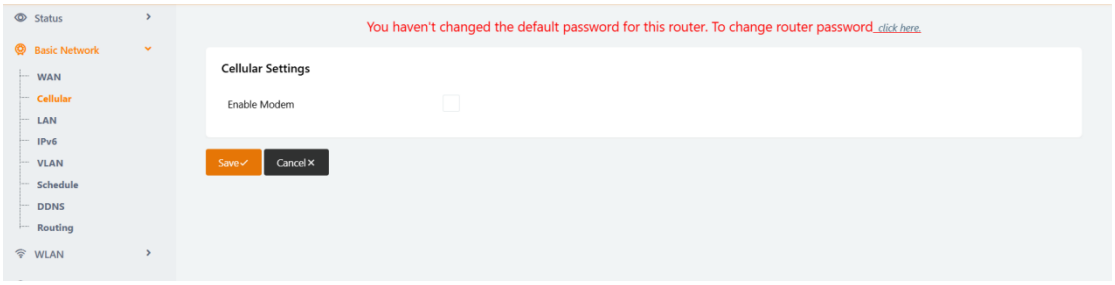


Figure 7-61 Mobile Network Settings

Step 4:

①In 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:

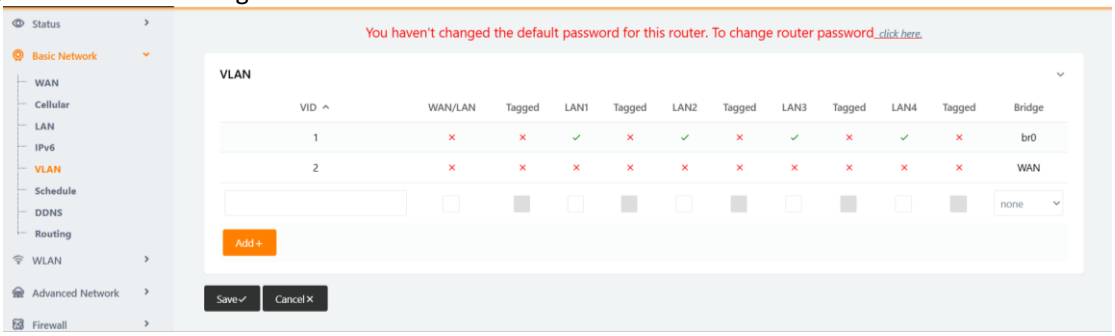


Figure 7-62 VLAN Setting

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

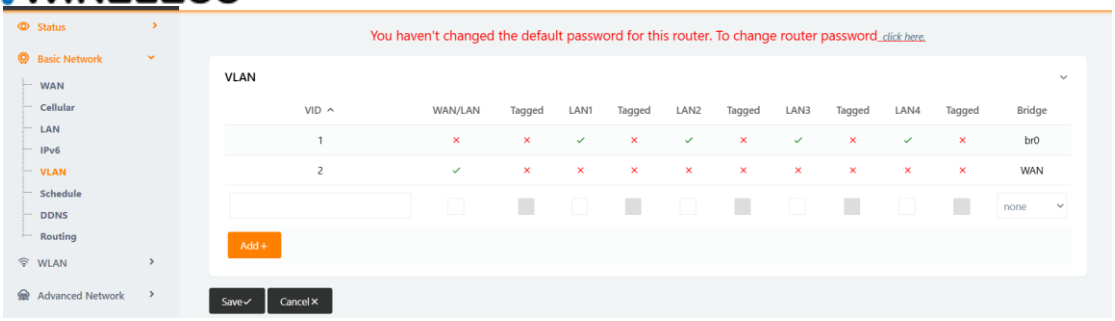


Figure 7-63 VLAN Settings

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

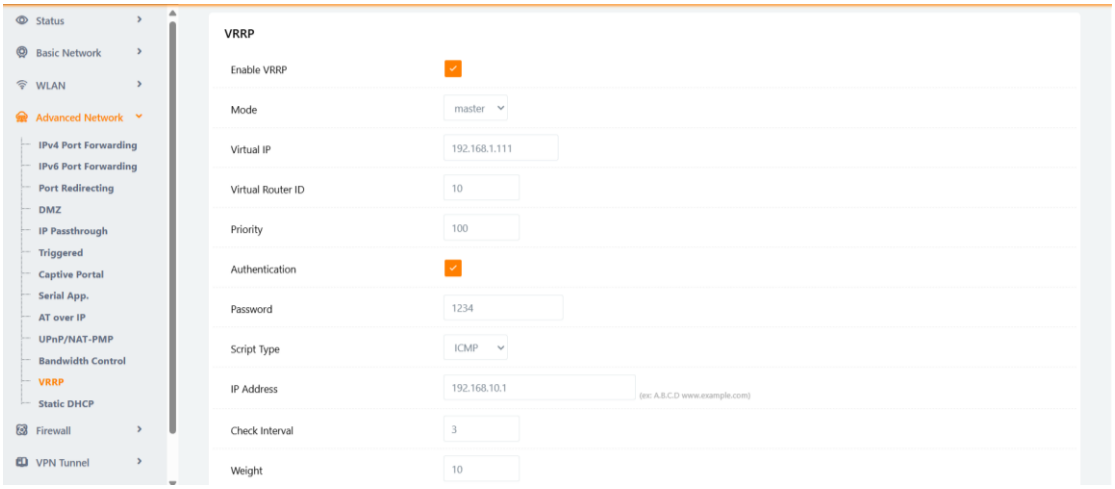


Figure 7-64 VRRP settings for the primary route

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)

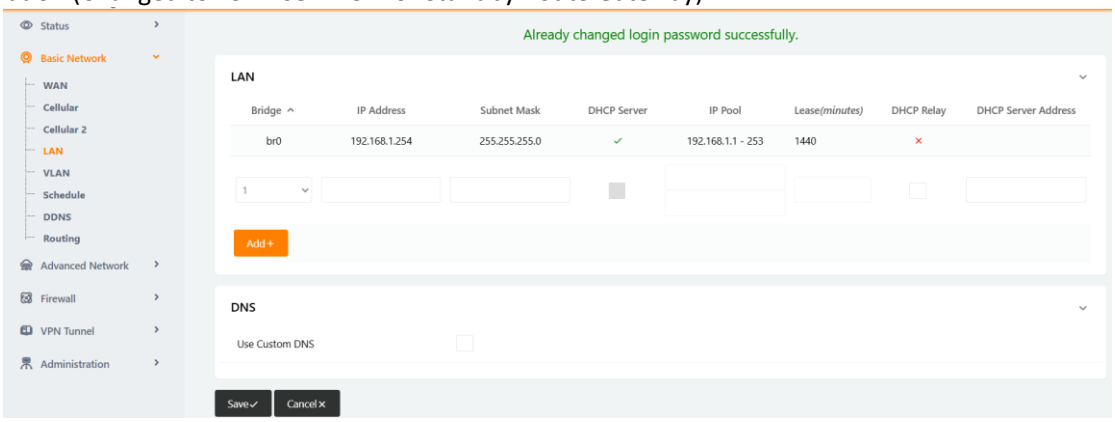


Figure 7-66 Standby LAN

Step 2:

In the navigation bar, select Basic 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):

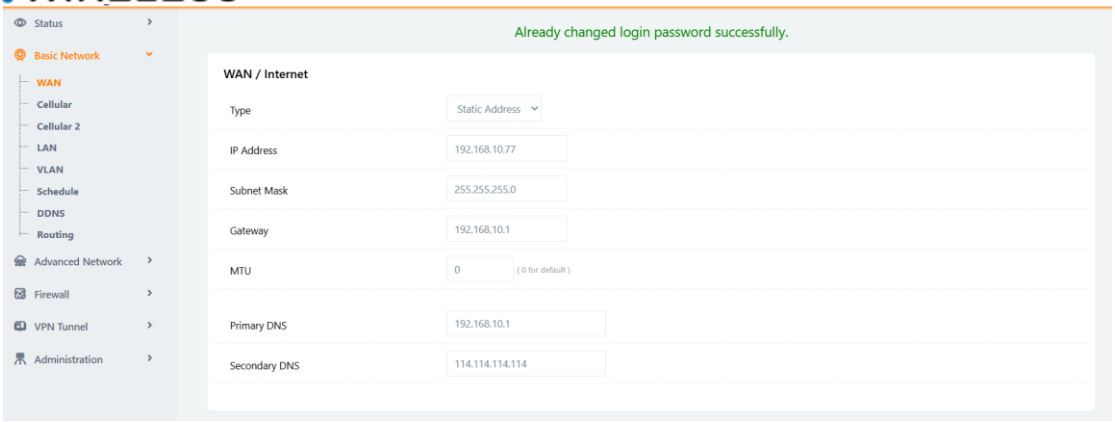


Figure 7-67 Static address settings

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

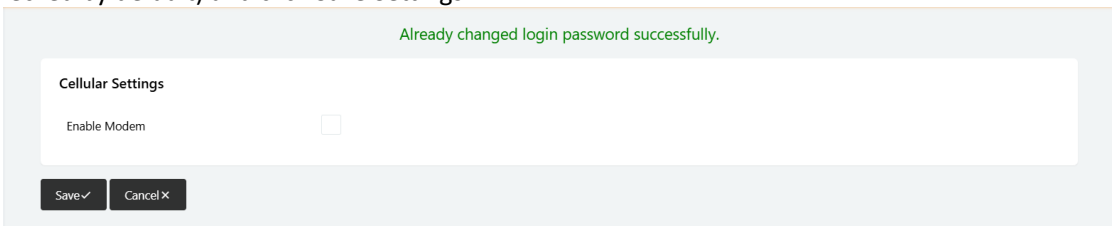


Figure 7-68 Mobile Network Setup

Step 4:

①In 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:

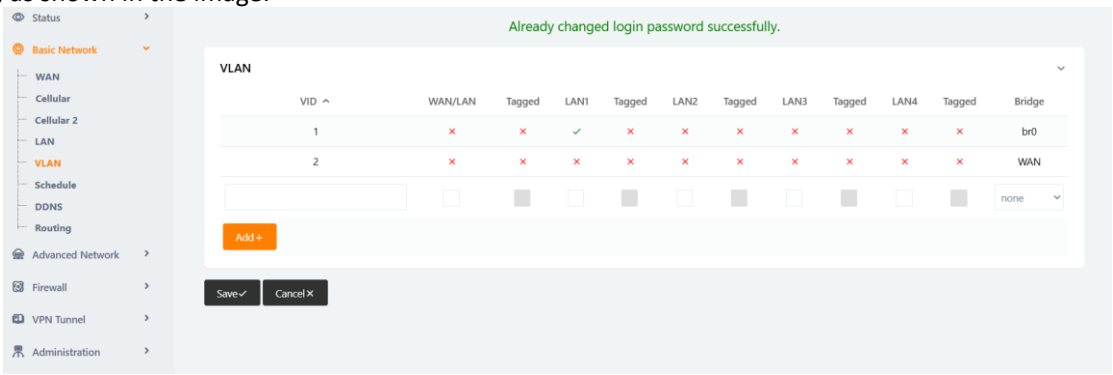


Figure 7-69 VLAN Settings

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

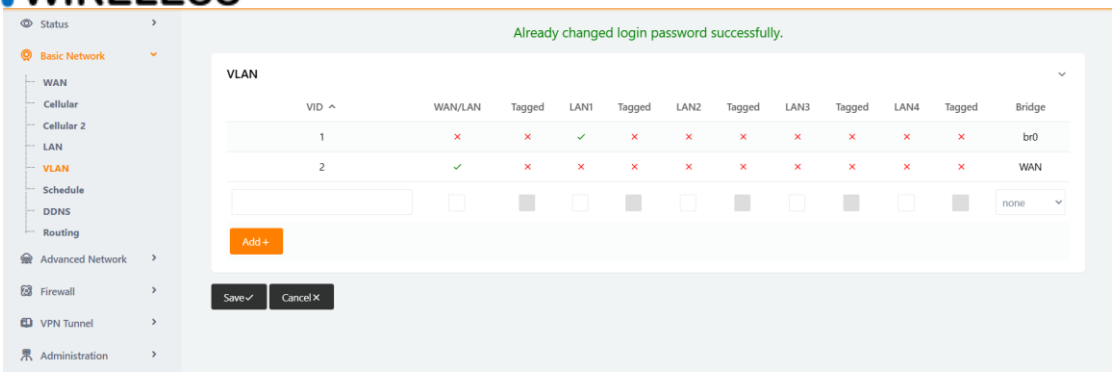


Figure 7-70 VLAN Setup

Step 5:

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

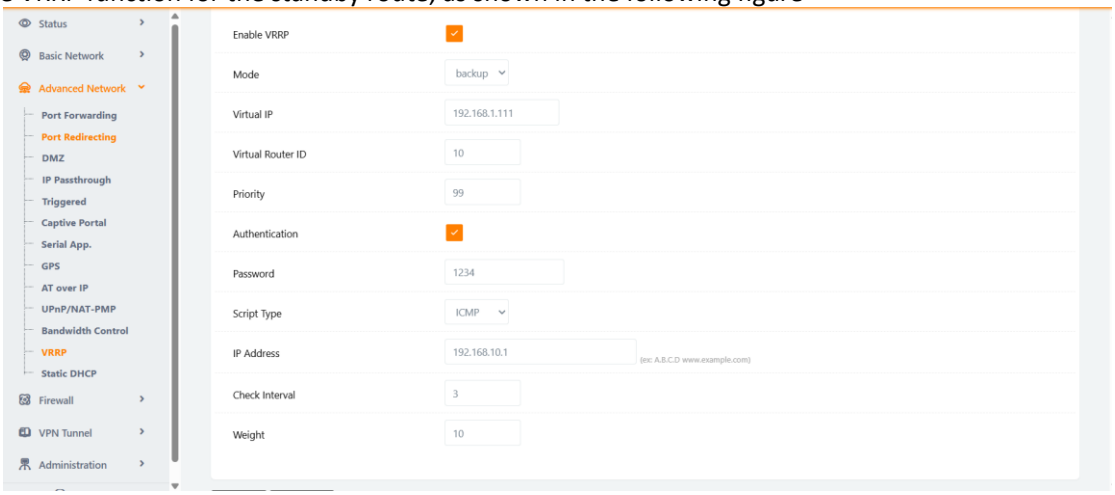


Figure 7-71 VRRP configuration of the standby route (R2).

❖ 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.

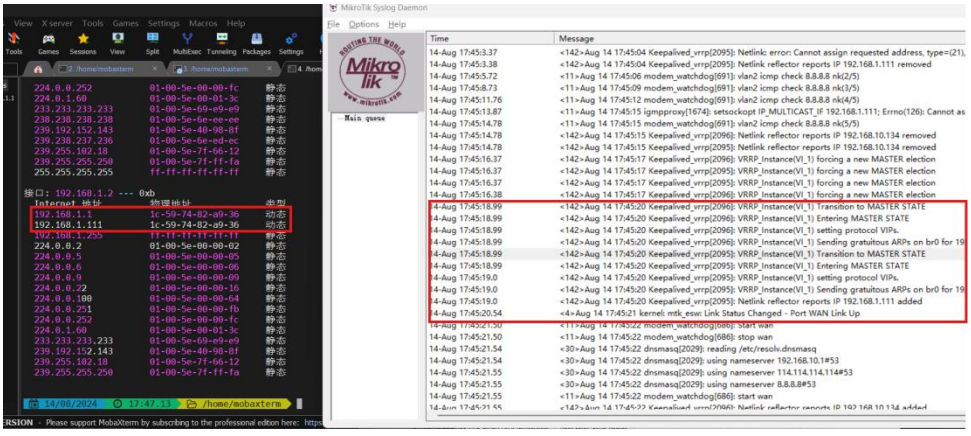


Figure 7-72: Both the primary and standby WAN ports are present

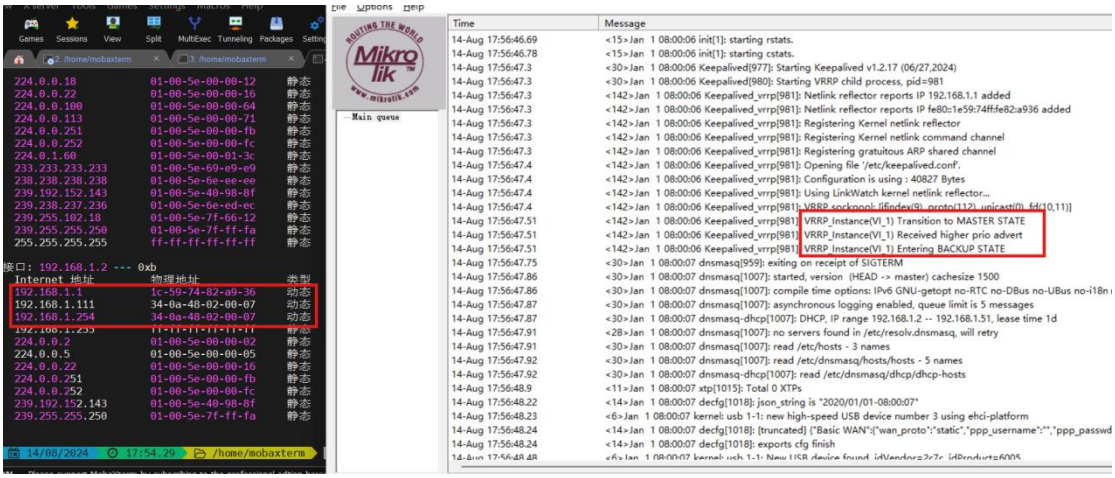


Figure 7-73: Unplug the WAN port of the primary device

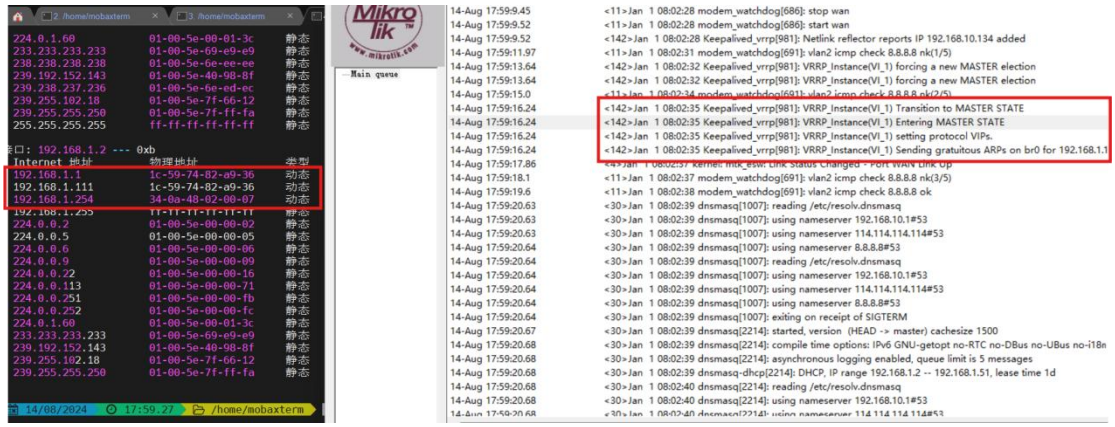


Figure 7-74 Replug the WAN port back into the main device

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.

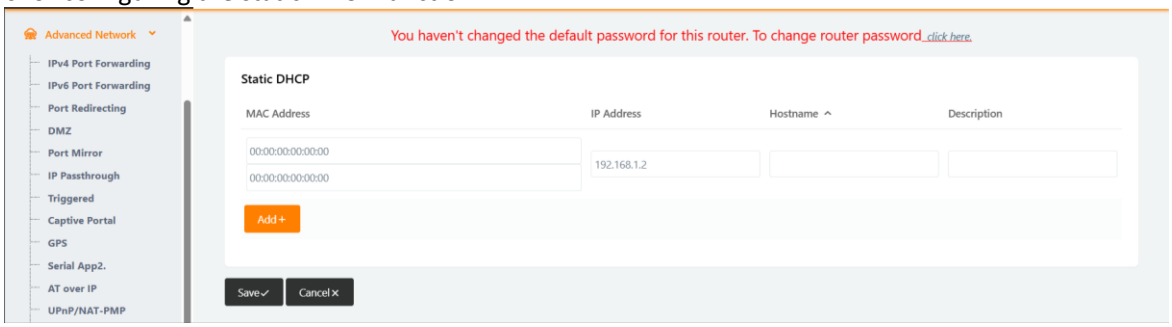


Figure 7-75

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

parameter	meaning	How to configure
DHCP service	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

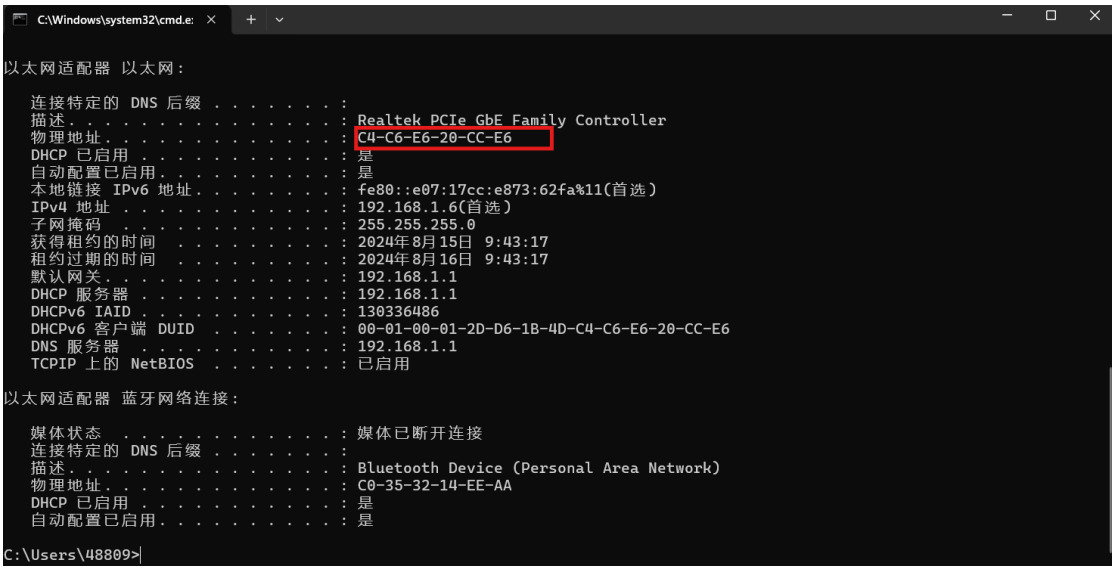


Figure 7-76 Administrator

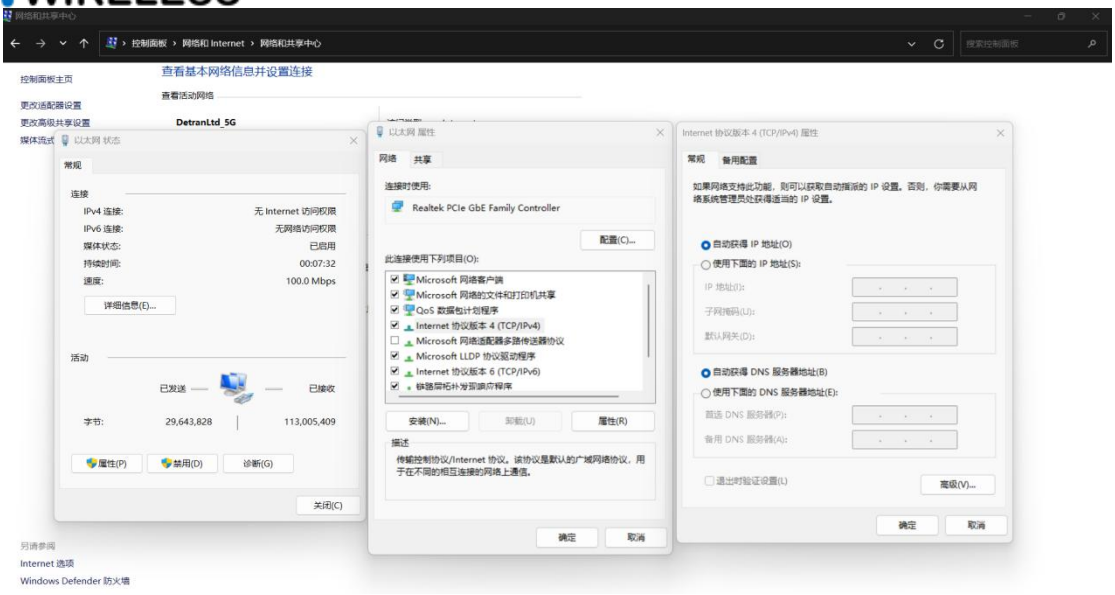


Figure 7-77 Automatic DHCP is enabled on the PC

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

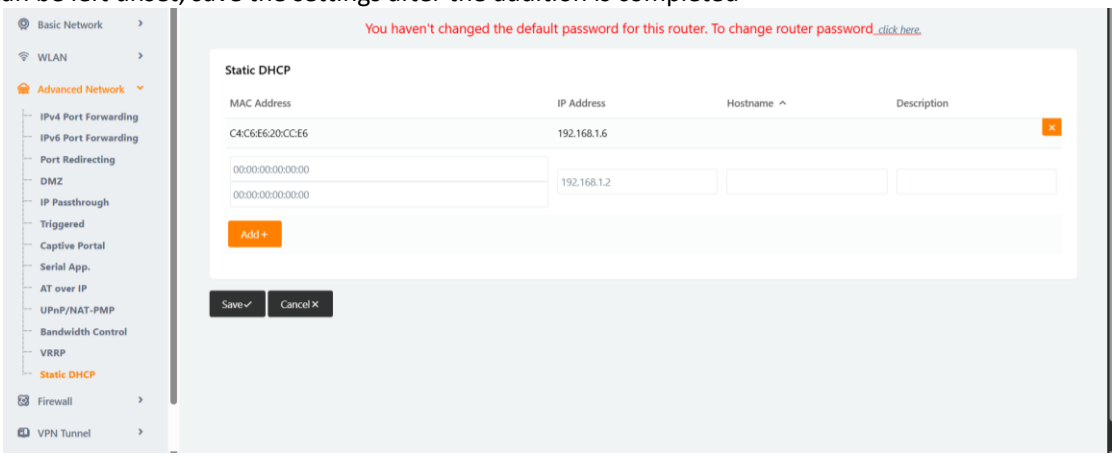


Figure 7-78 Static DHCP settings

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).

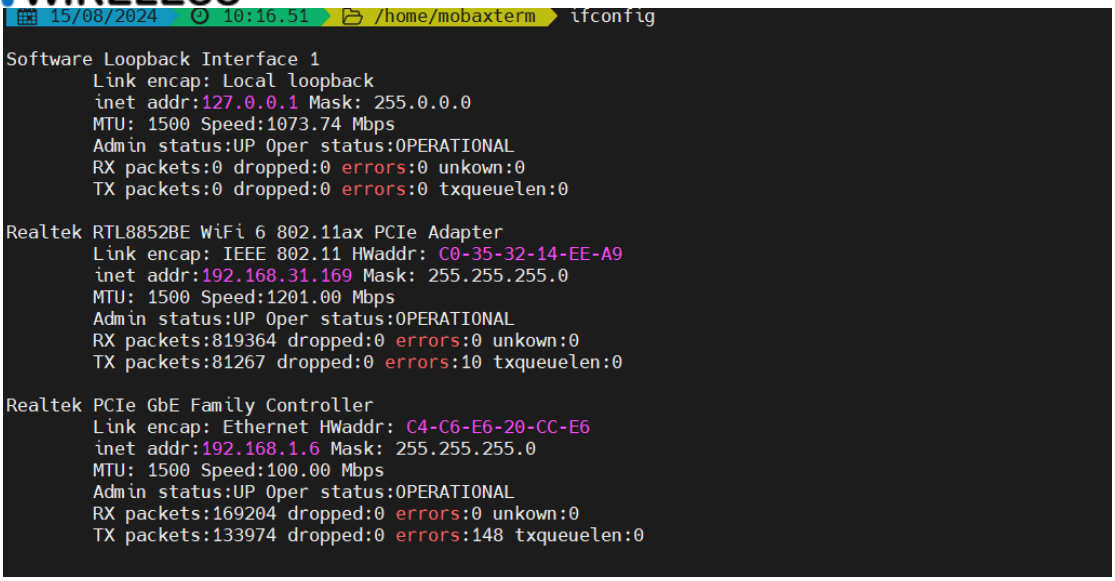


Figure 7-79 Binding static DHCP

8. Firewall

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.。

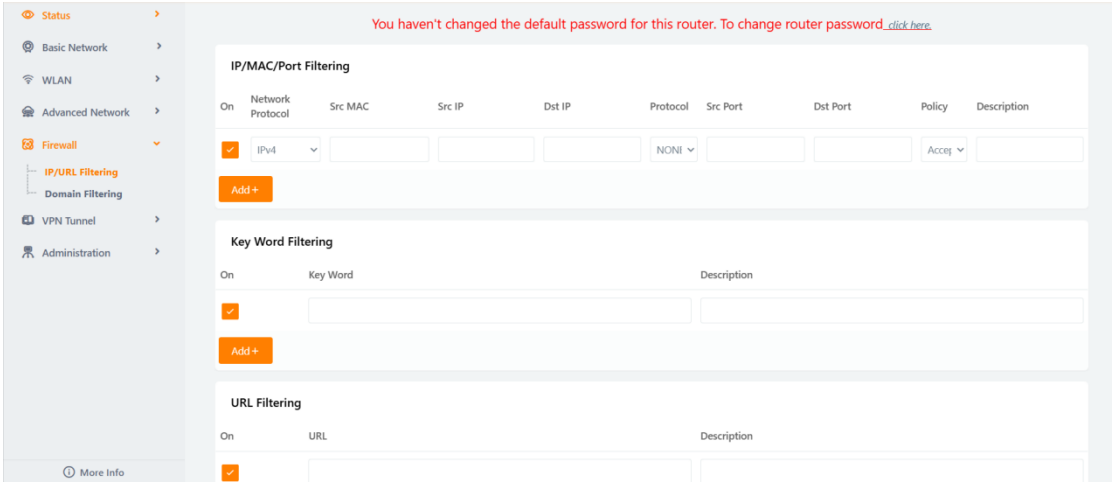


Figure 8-1

Configure the IP/MAC/Port filtering parameters as shown in the table

Parameter	Meaning	Configure
Source MAC	Configuration requires specifying the MAC address to allow or deny access.	WORD type MAC format e.g.00:1A:4D:34:B1:8E
Source IP	Configuration requires specifying the Source IP address to allow or deny access.	e.g.192.168.1.2
Destination IP	Configuration requires specifying the Destination IP address to allow or deny access.	e.g.192.168.10.70
Protocol	To enable data to travel from source to destination across a network, all participants in the communication must follow a common set of rules. This set of rules is called a protocol, which is ultimately defined by the format of the data packets transmitted over the network.	Select TCP, UDP, or ICMP based on the actual situation.
Source Port	Configuration requires specifying the Source Port to allow or deny access.	Configure the port based on the actual situation.
Destination port	Configuration requires specifying the Destination Port to allow or deny access.	Configure the port based on the actual situation.
Policy	Select "Accept" or "Drop" based on the actual situation.	Select "Accept" or "Drop" based on the actual situation.

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

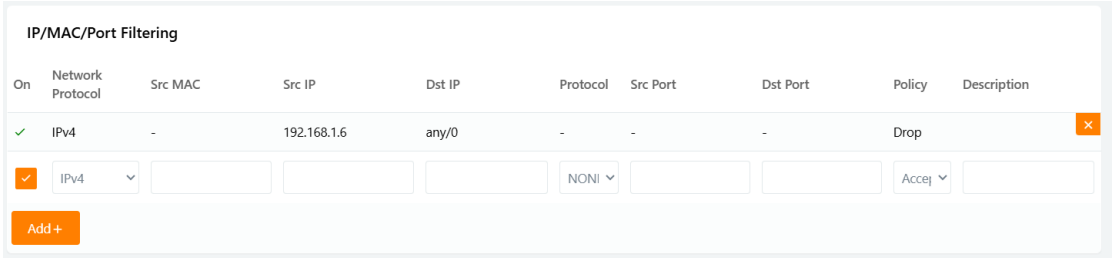


Figure 8-2

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

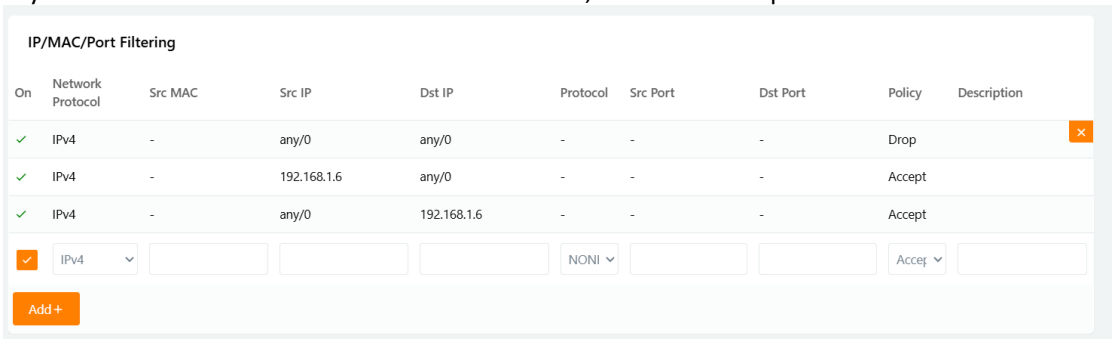


Figure 8-3

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 InteHow to configure

WORD type MAC format
For example, 00:1A:4D: 34: B1:8E
For example: 192.168.1.2
For example: 192.168.10.70
Choose TCP, UDP, ICMP according to the actual situation
Configure ports according to the actual situation
Configure ports according to the actual situation
Choose between receiving and discarding based on the actual situation addresses are allowed

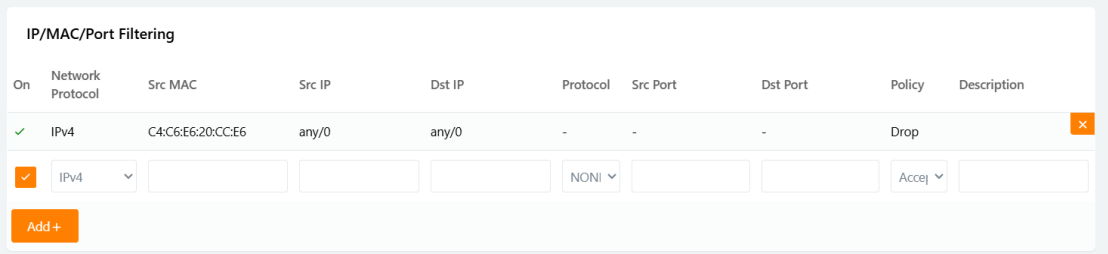


Figure 8-4

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

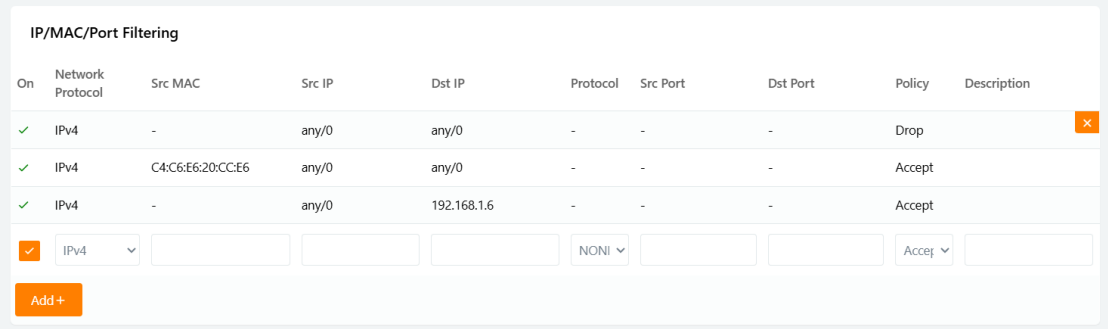


Figure 8-5

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

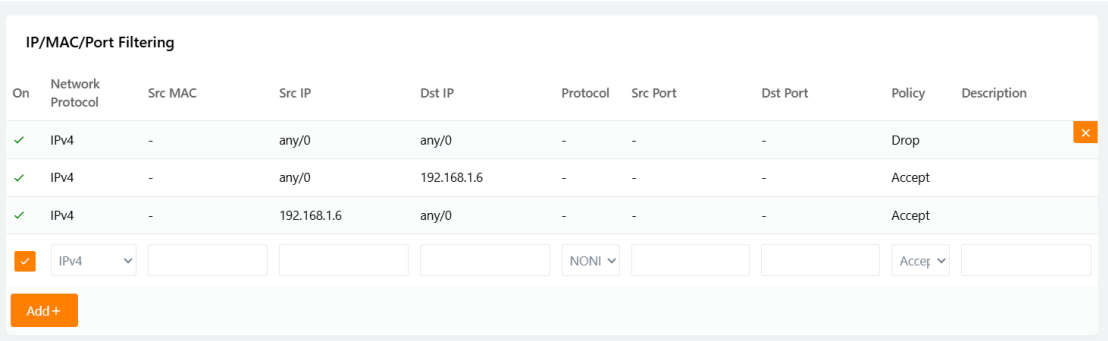


Figure 8-6

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

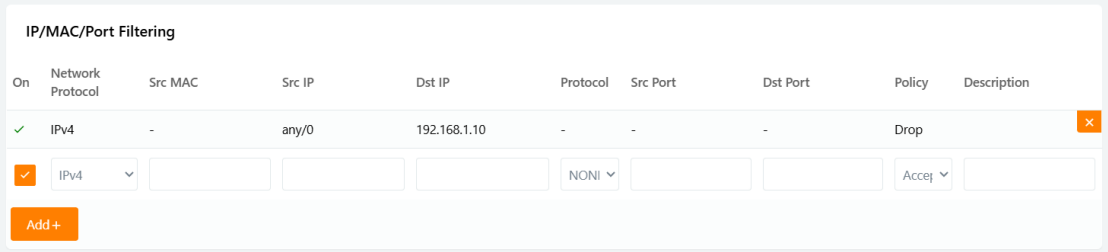


Figure 8-7

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.

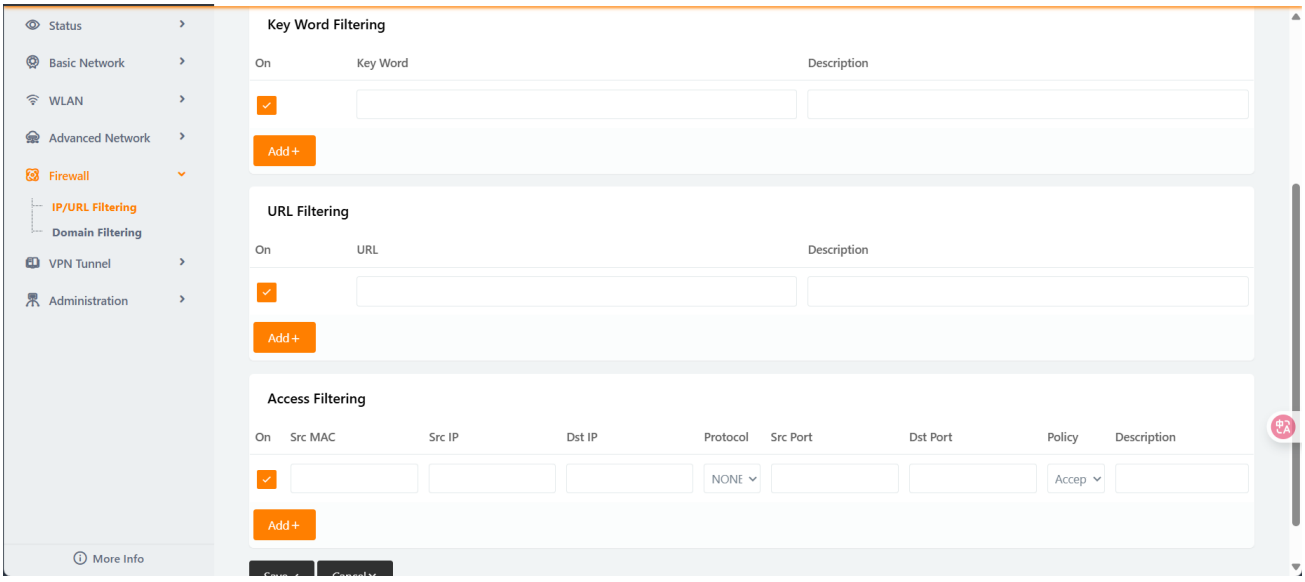


Figure 8-8

Example 1:

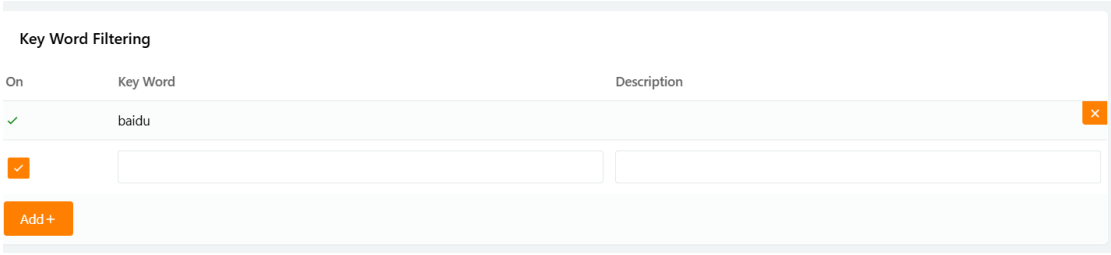


Figure 8–9

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

Example 2:

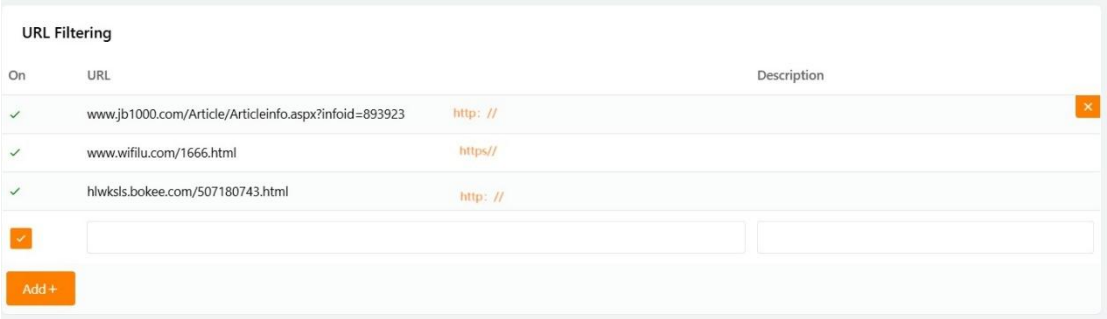


Figure 8–10

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;

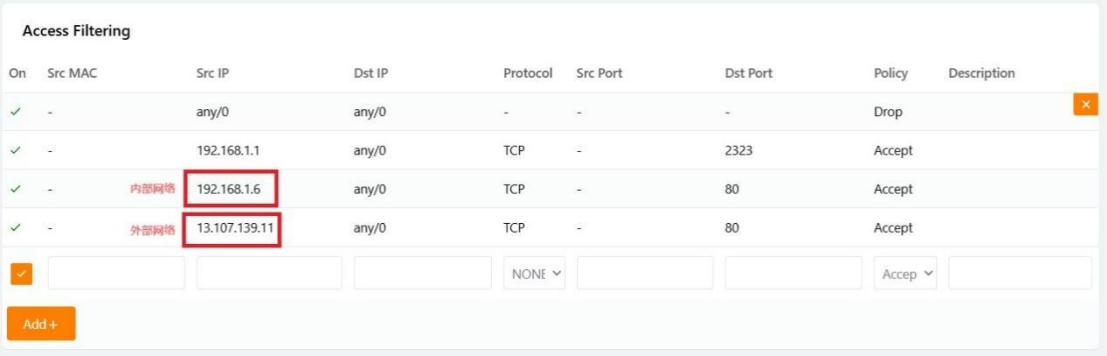


Figure 8–11

8.3. Domain name filtering

Domain name 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.

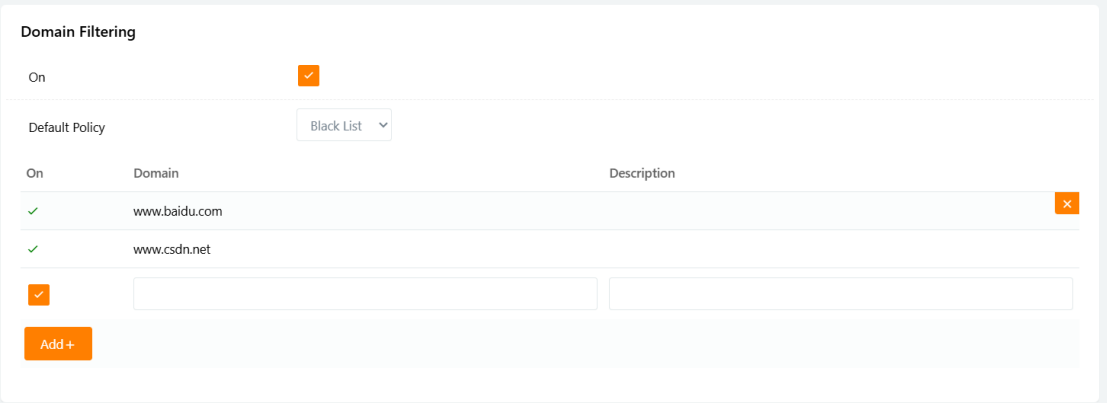


Figure 8-12

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/Zerotier/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

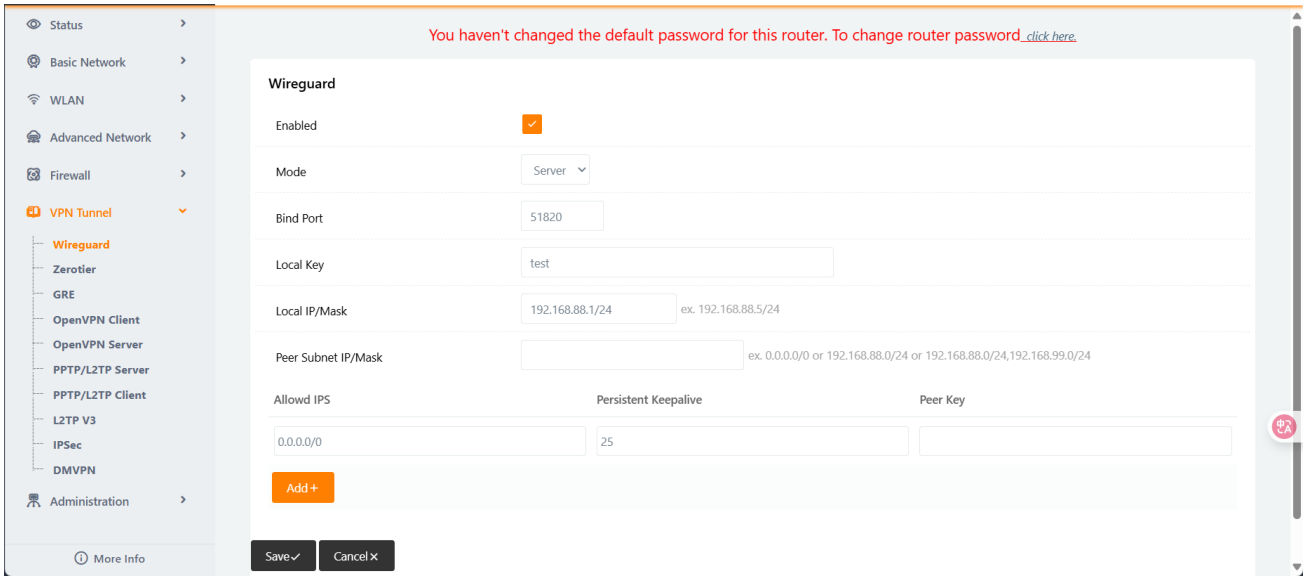


Figure 9-1

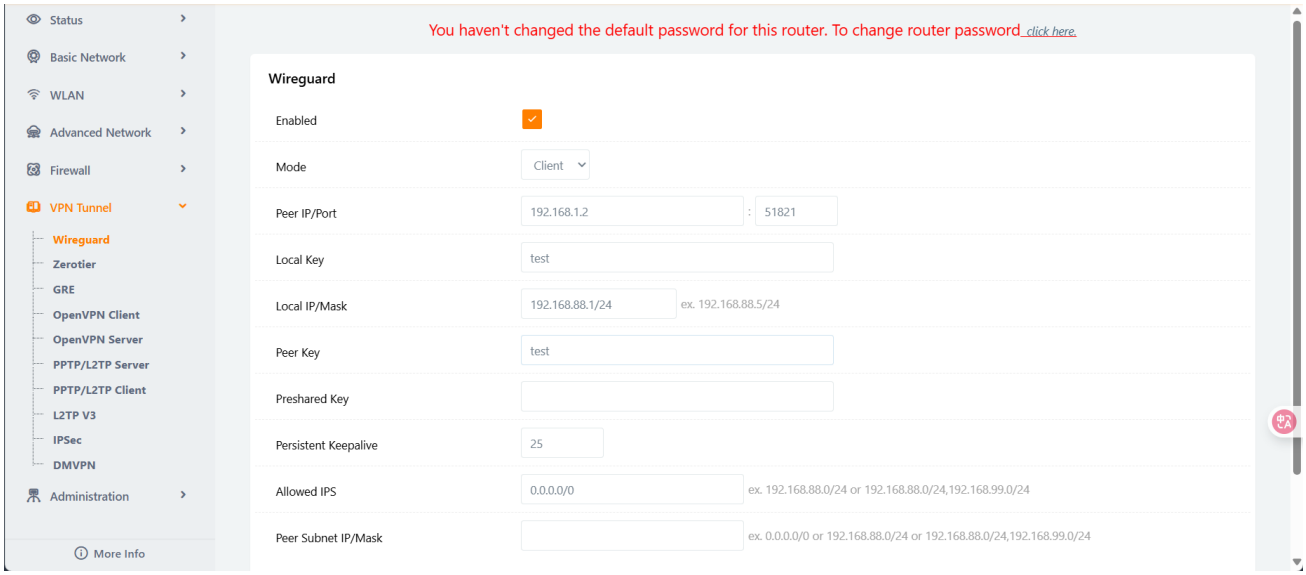


Figure 9-2

Step 2: Configure the wireguard parameter

The name of the parameter	meaning	How to configure
Enable Wireguard	Enable/disable the Wireguard feature	Click Enable to enable the feature
Mode	There are two modes: server and client	Select the appropriate mode for each application
Bind 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 IP/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 IP/Mask	In server mode, the clientcan 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
Persistent Keepalive	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 IP/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 IP/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
Preshared 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 IP/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

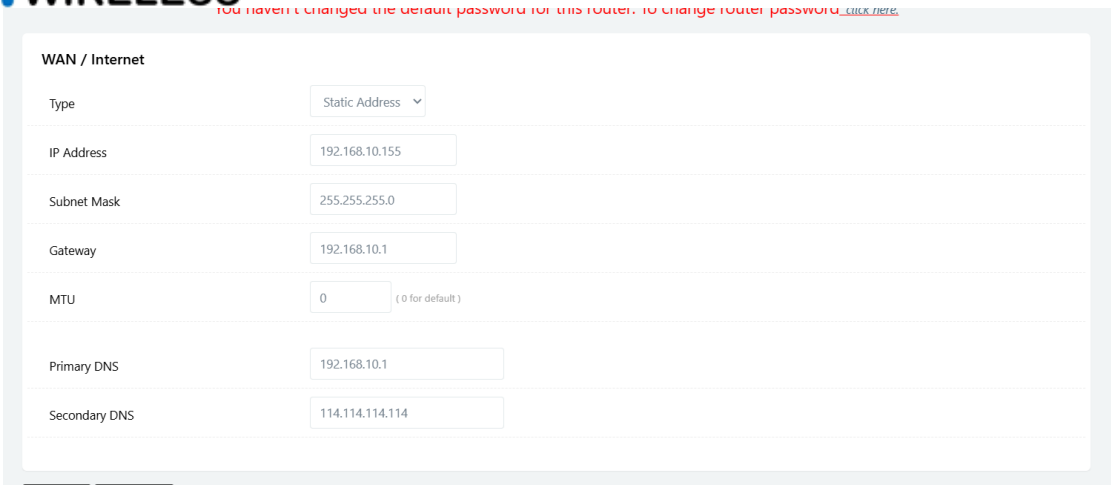


Figure 9-3

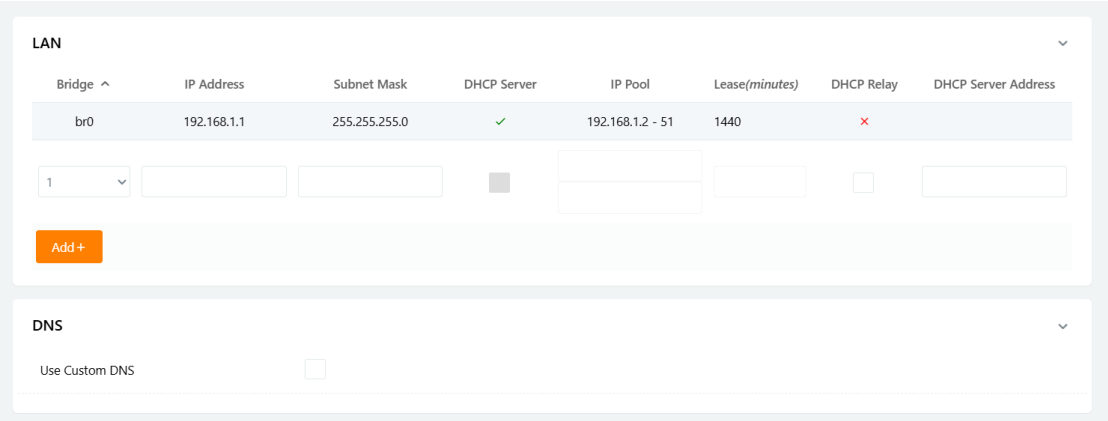


Figure 9-4

Step 4: Configure the wireguard parameter in server mode

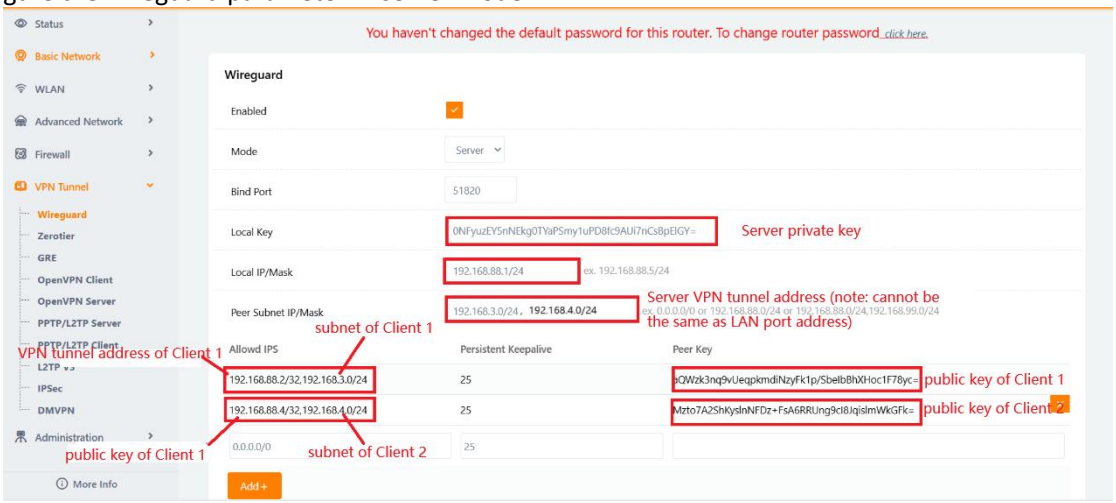


Figure 9-5

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

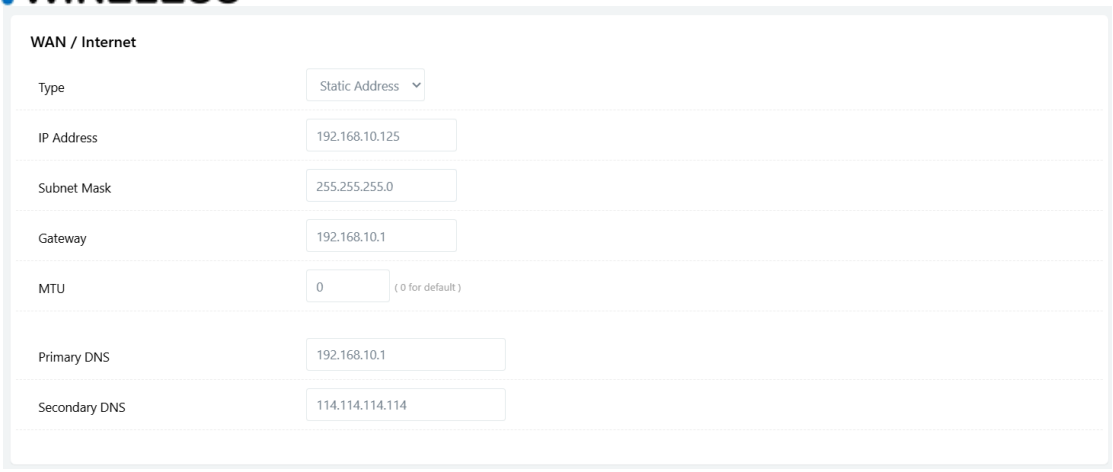


Figure 9-6

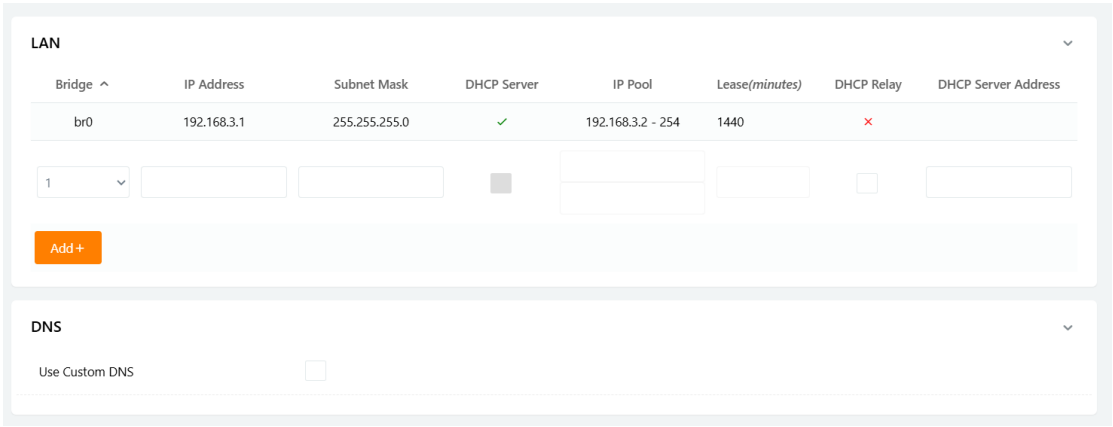


Figure 9-7

Routing Client 2:

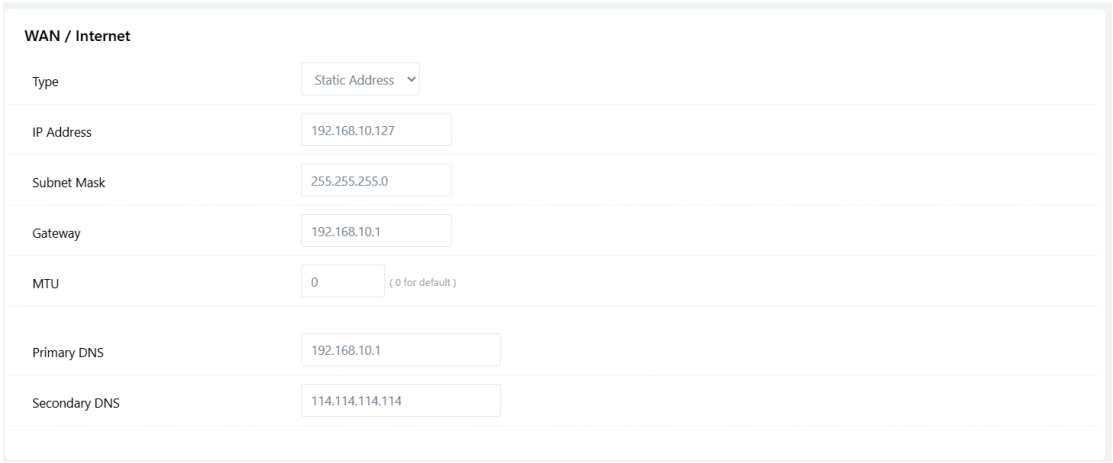


Figure 9-1

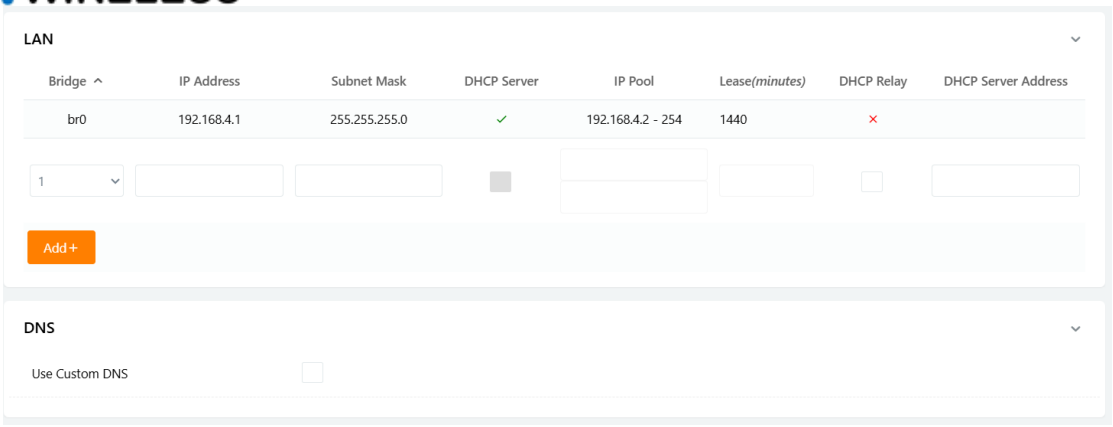


Figure 9-2

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:

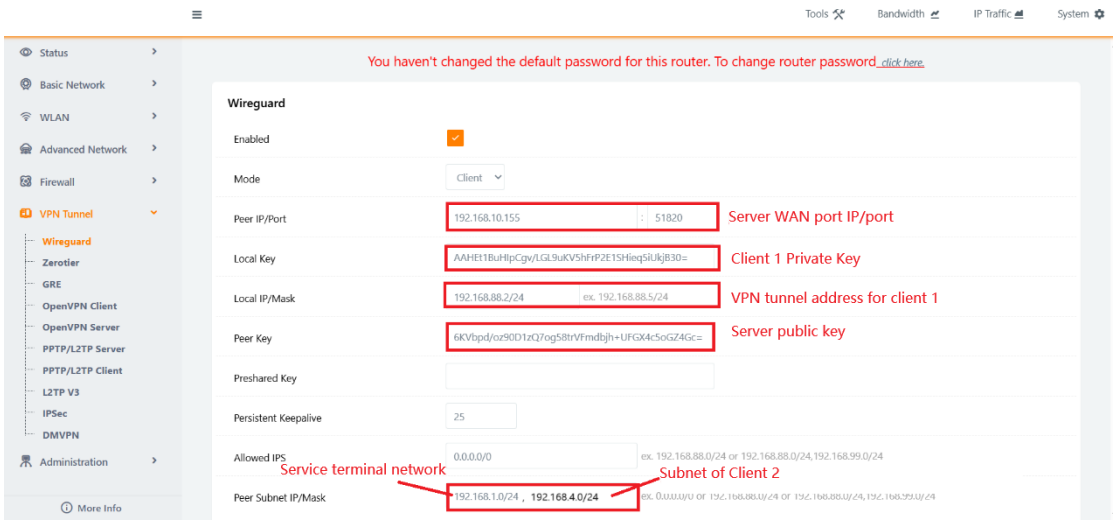


Figure 9-3

Routing Client 2:

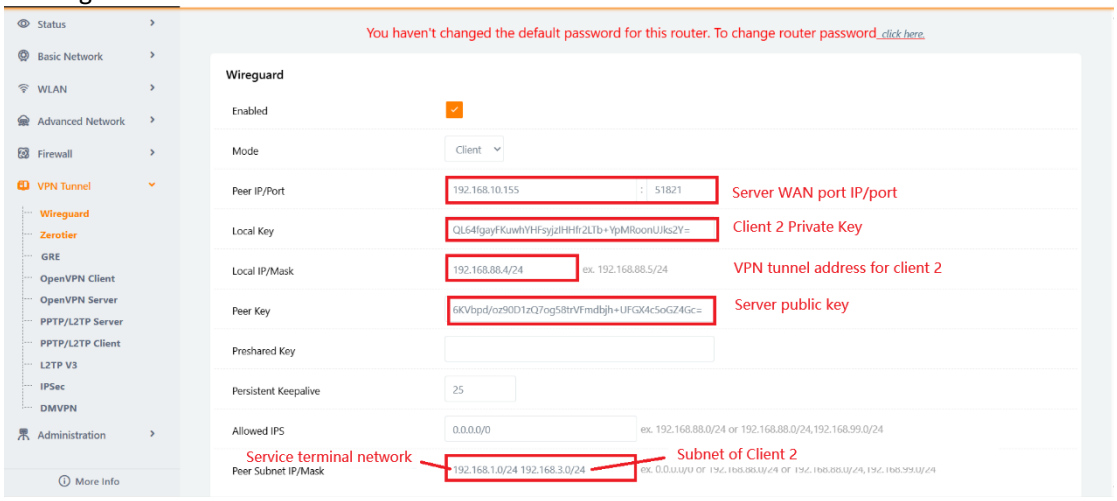


Figure 9-4

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

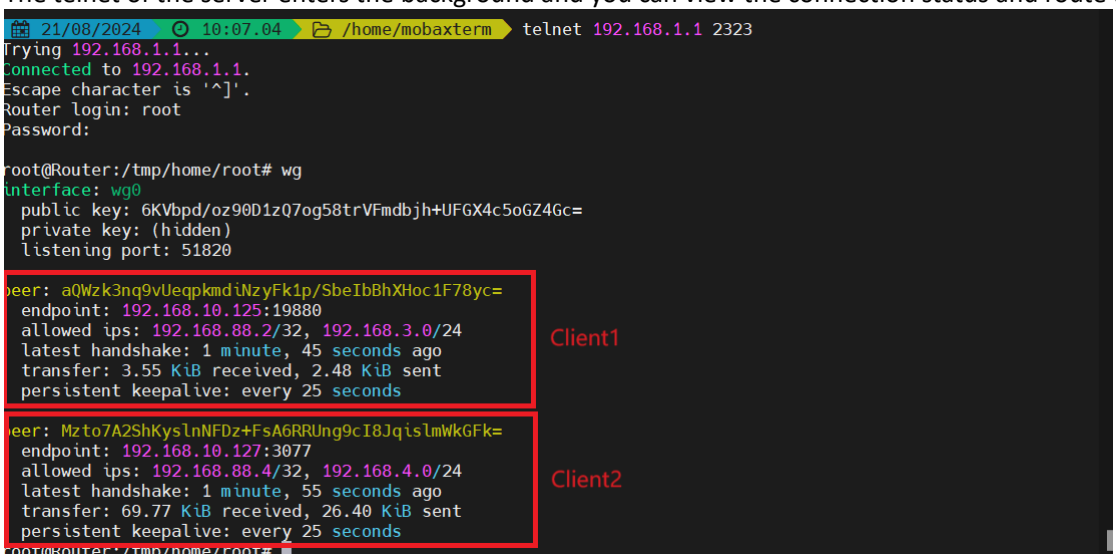


Figure 9-5

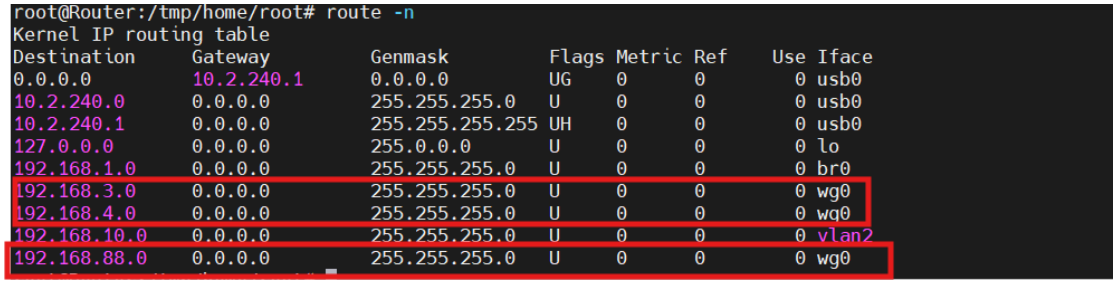


Figure 9-6

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

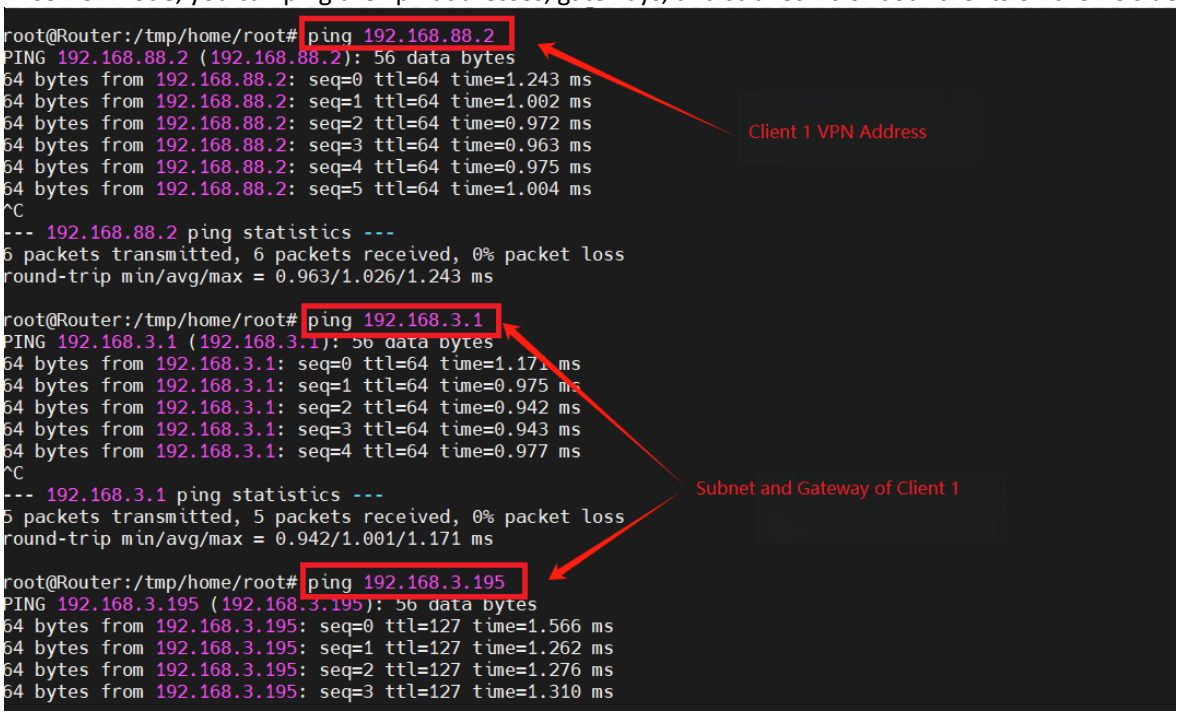


Figure 9-7

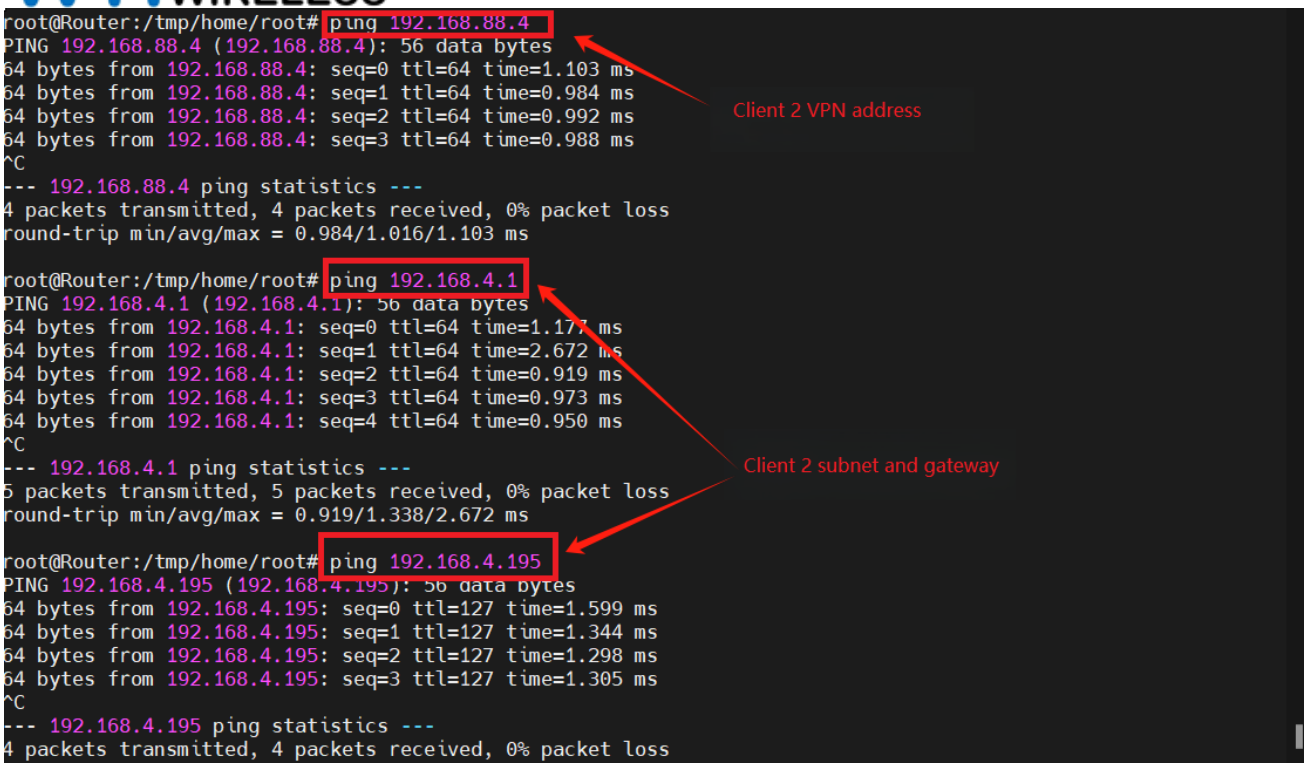


Figure 9-8

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



Figure 9-9

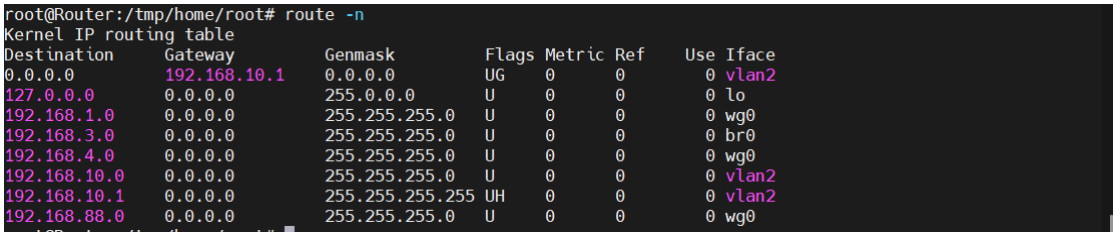


Figure 9-10

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

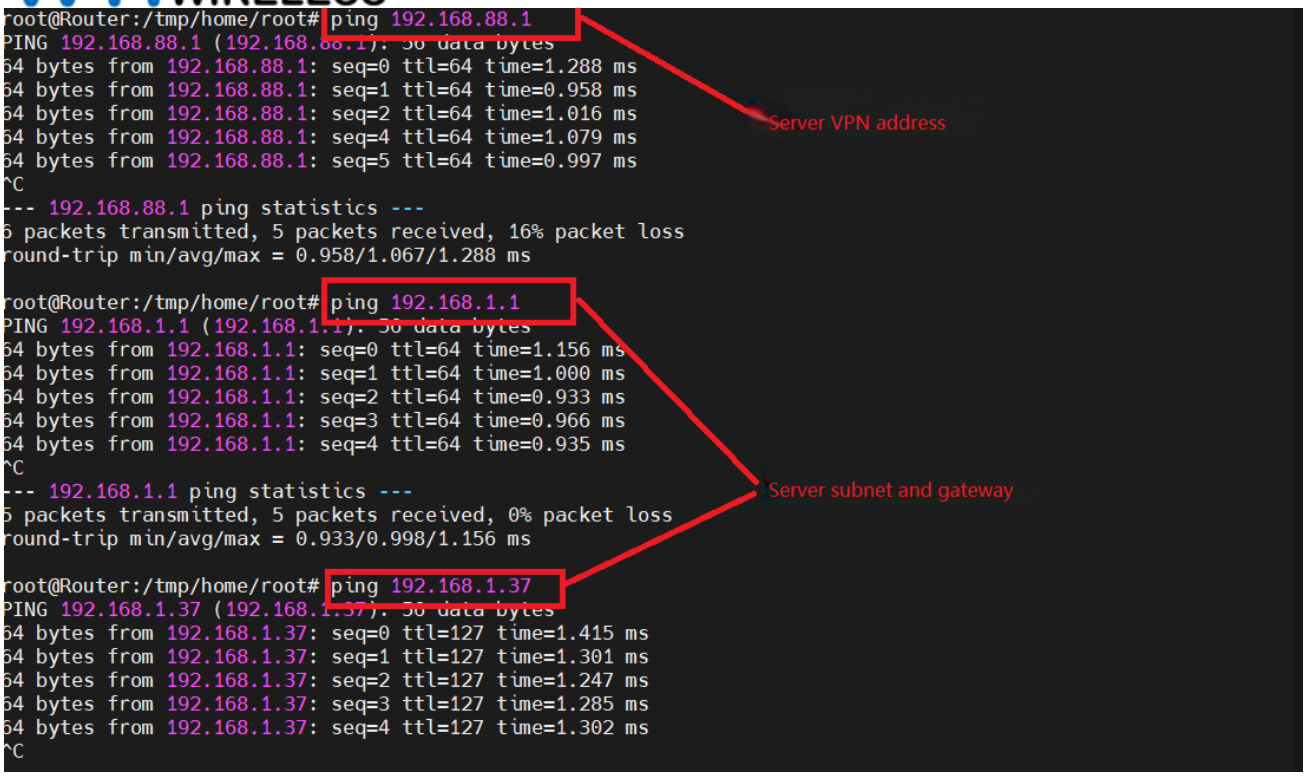


Figure 9-11

Client 2:



Figure 9-12

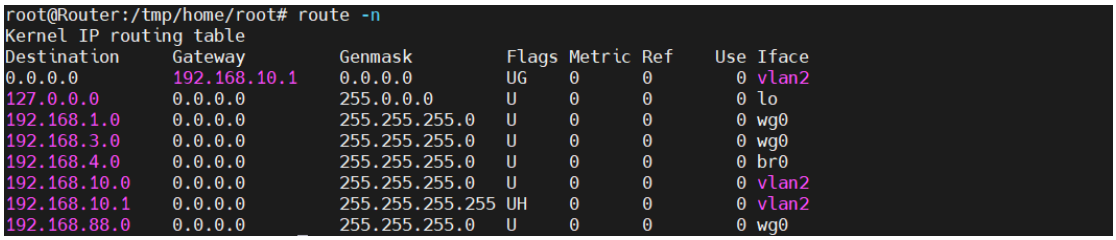


Figure 9-13

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

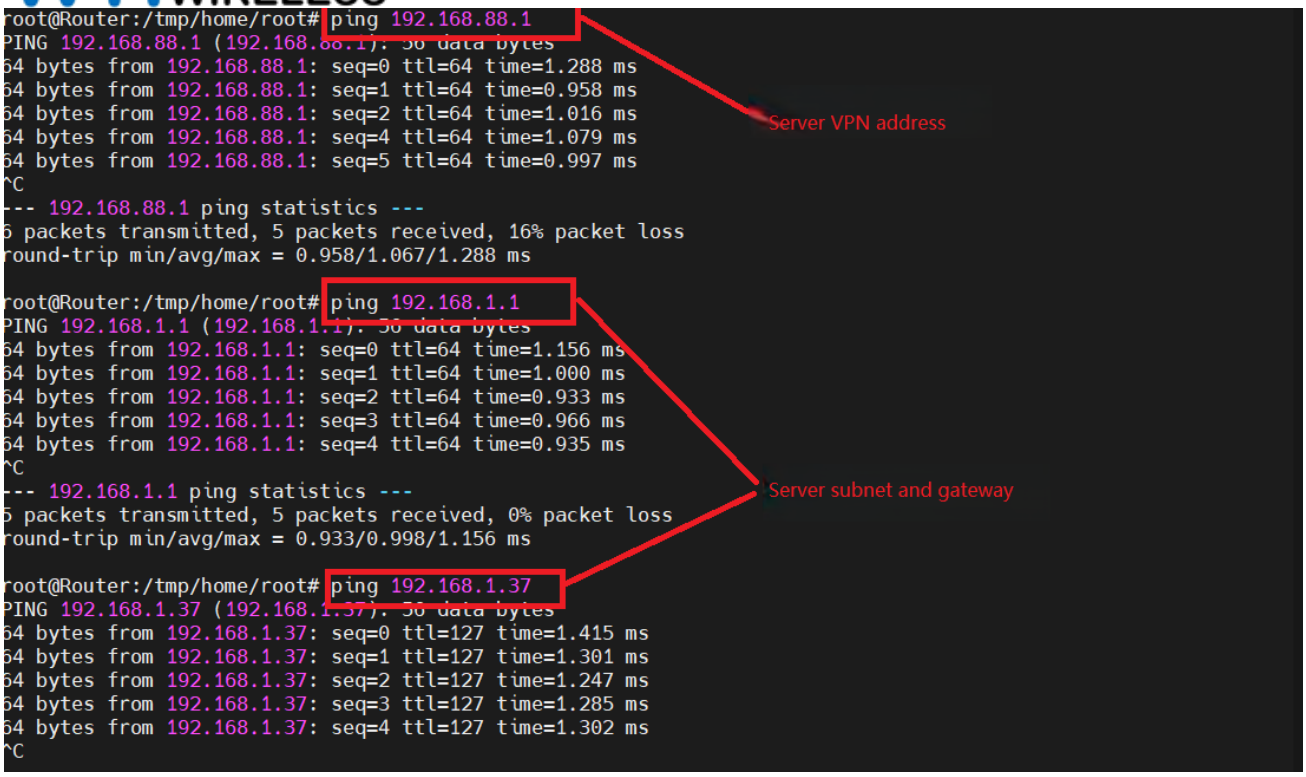


Figure 9-14

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

Client 1:

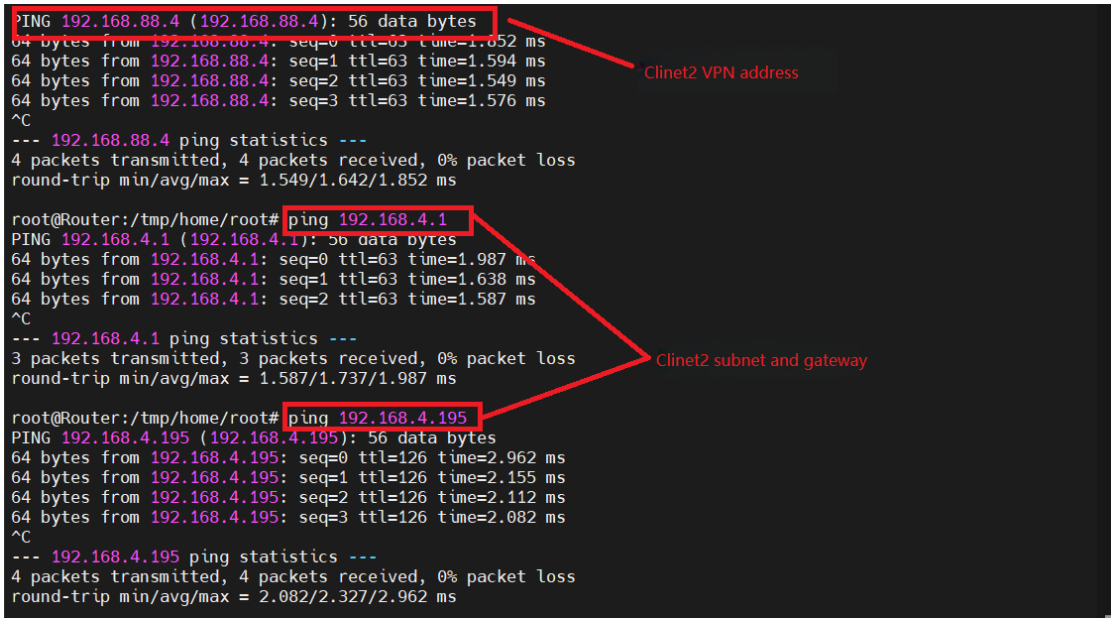


Figure 9-15

Client 2:

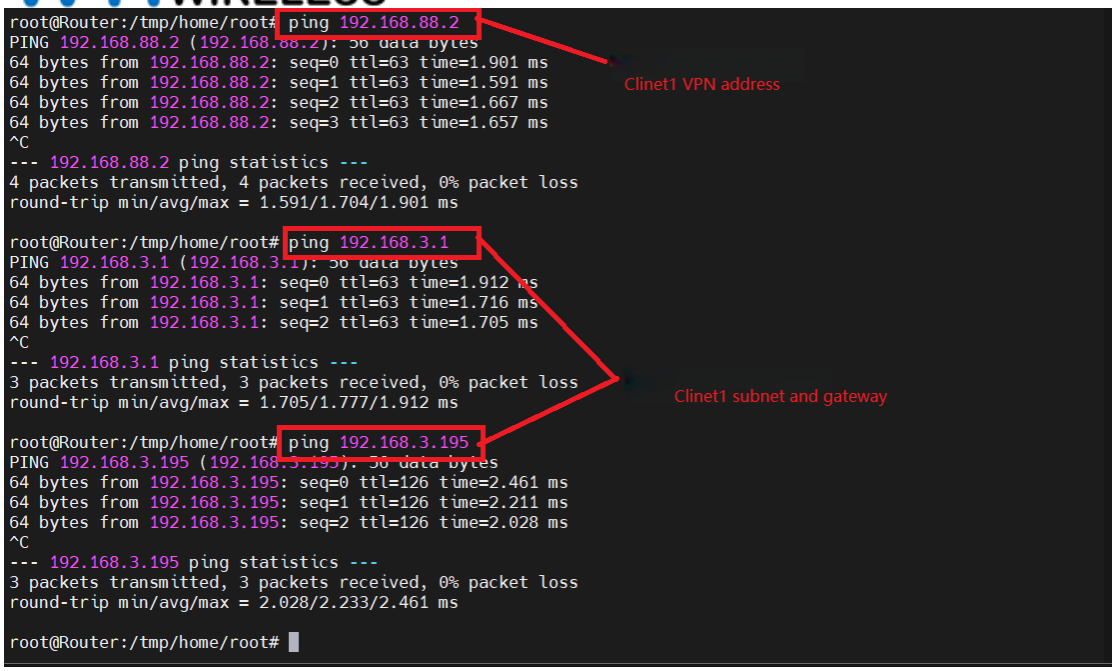


Figure 9-16

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

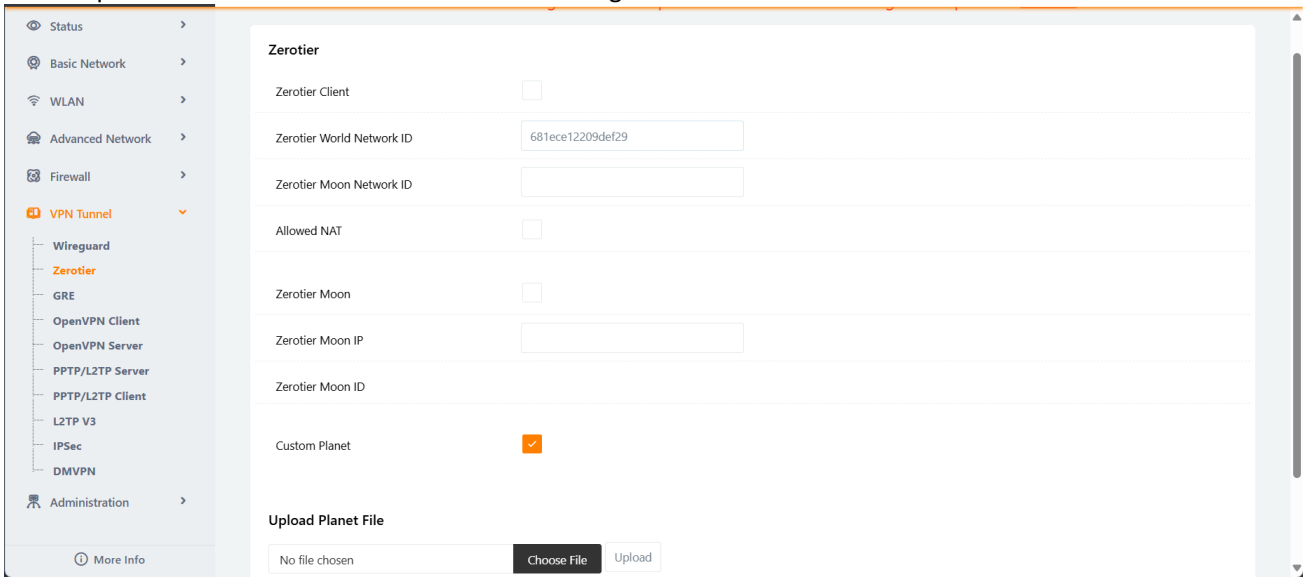


Figure 9-17

Zerotier Parameter Description:

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	

Automatically allow client NAT	To enable this function, you need to use it in conjunction with the IP 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 9-1

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.

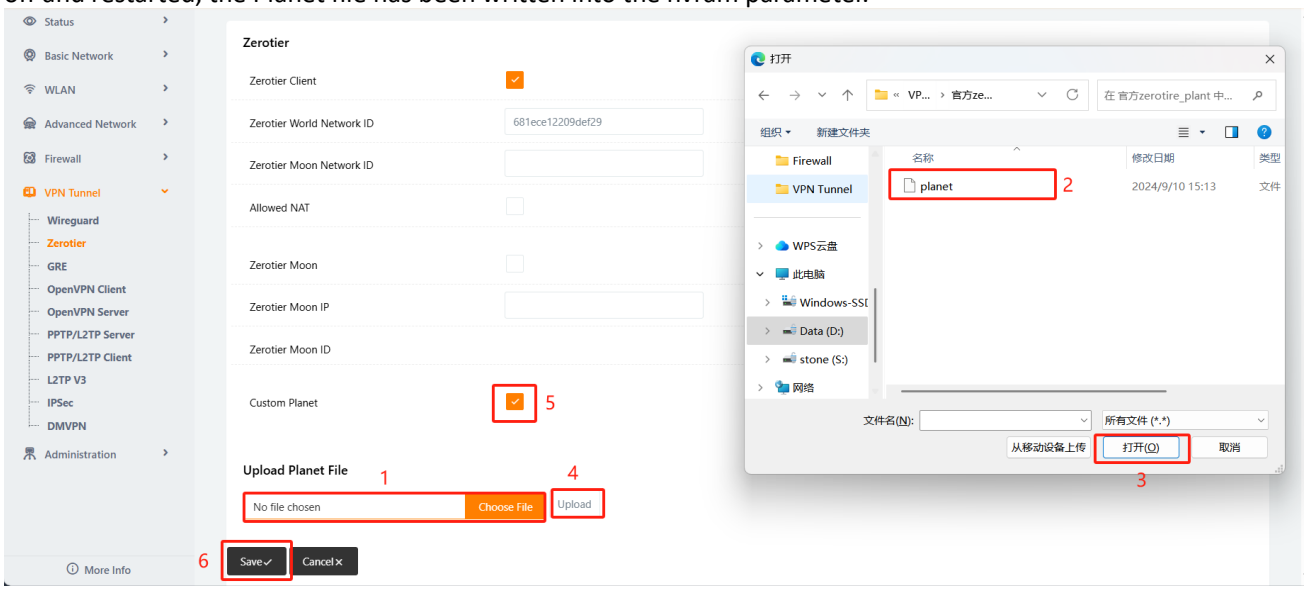


Figure 9-18



Figure 9-19

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

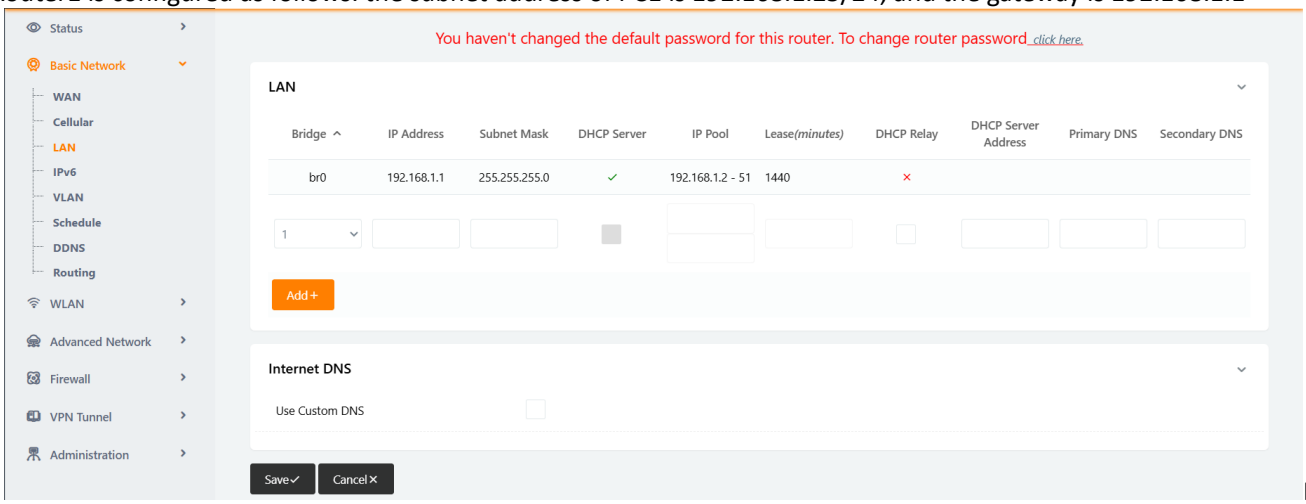


Figure 9-20

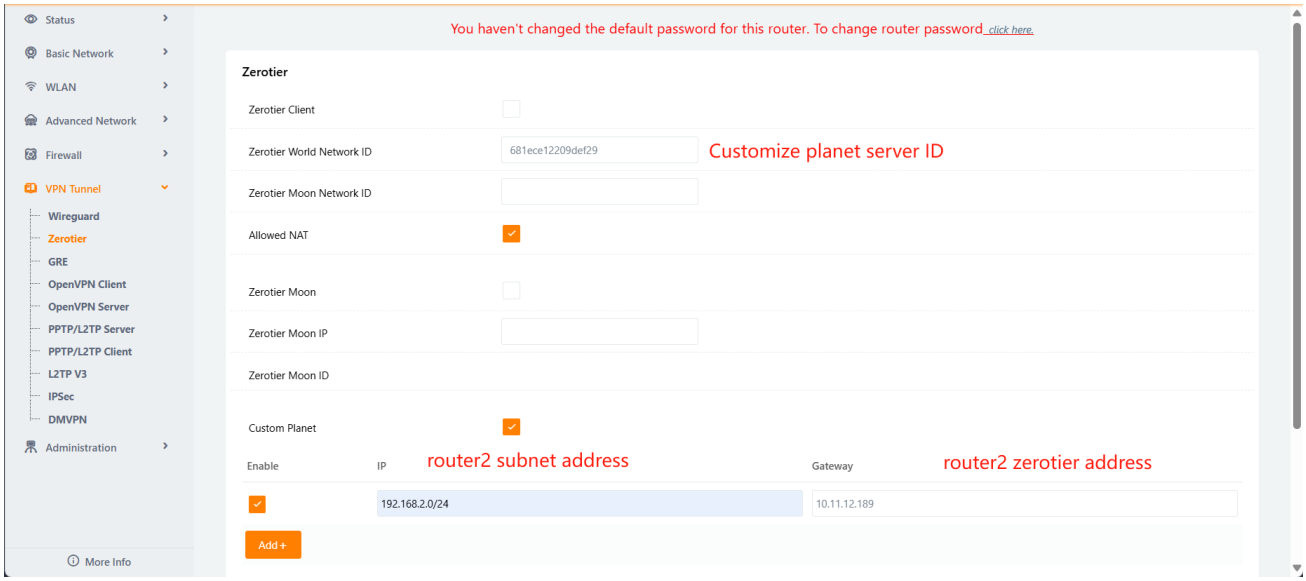


Figure 9-21

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

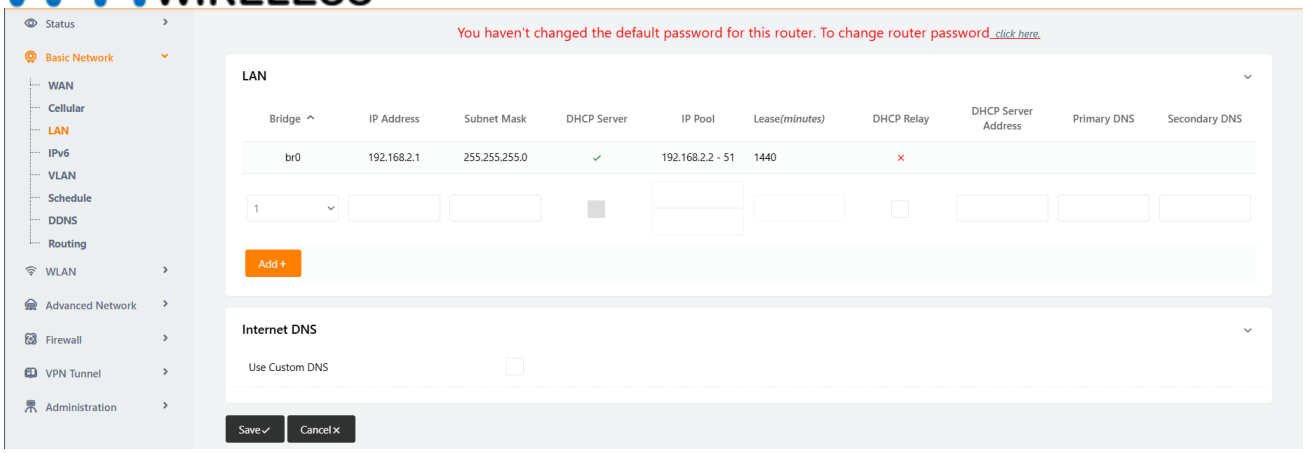


Figure 9-22

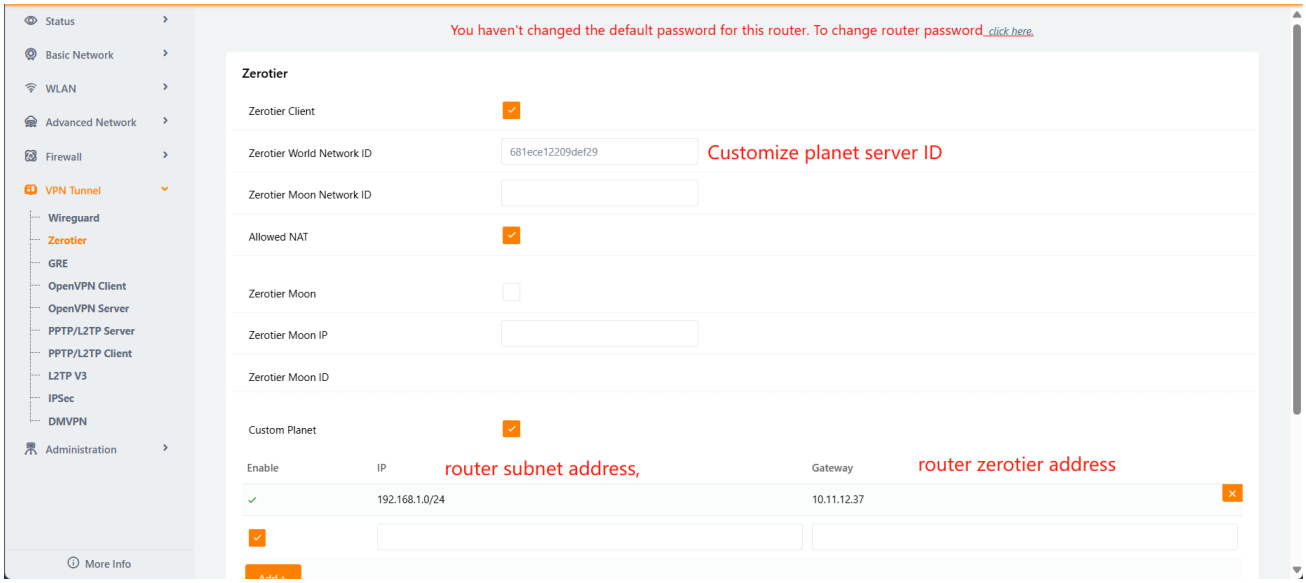


Figure 9-23

Step 3: Check the connection status

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

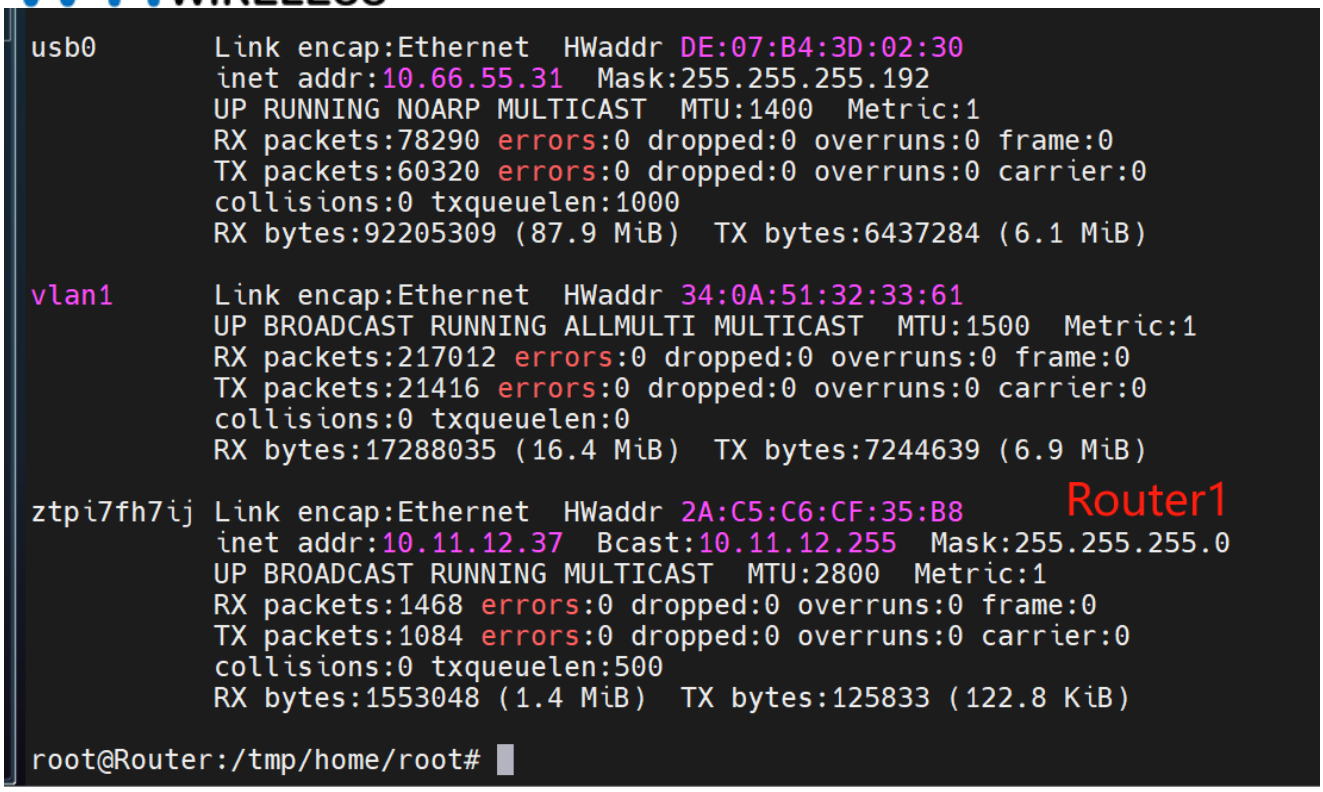


Figure 9-24

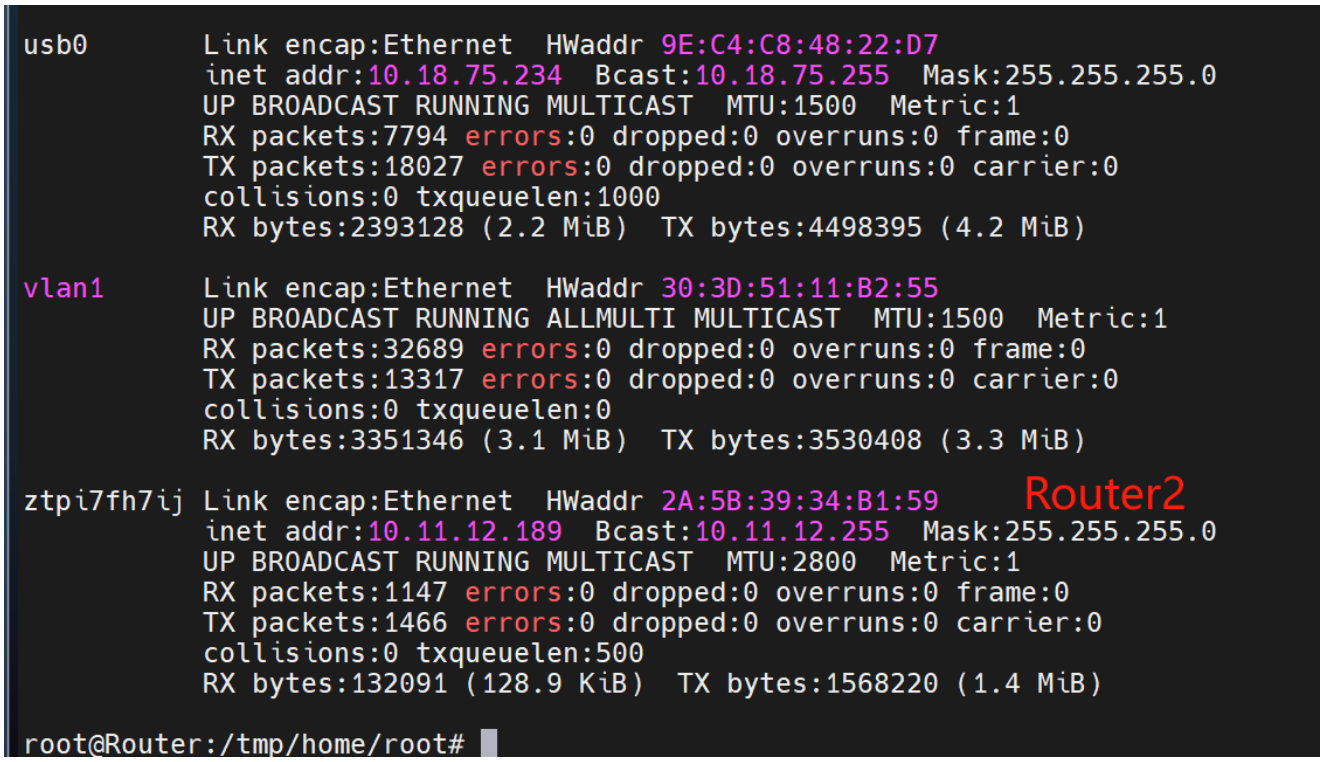


Figure 9-25

After NAT is configured, both devices can ping the peer gateway and subnet addresses on the PC and the router Router1, PC1 ping:

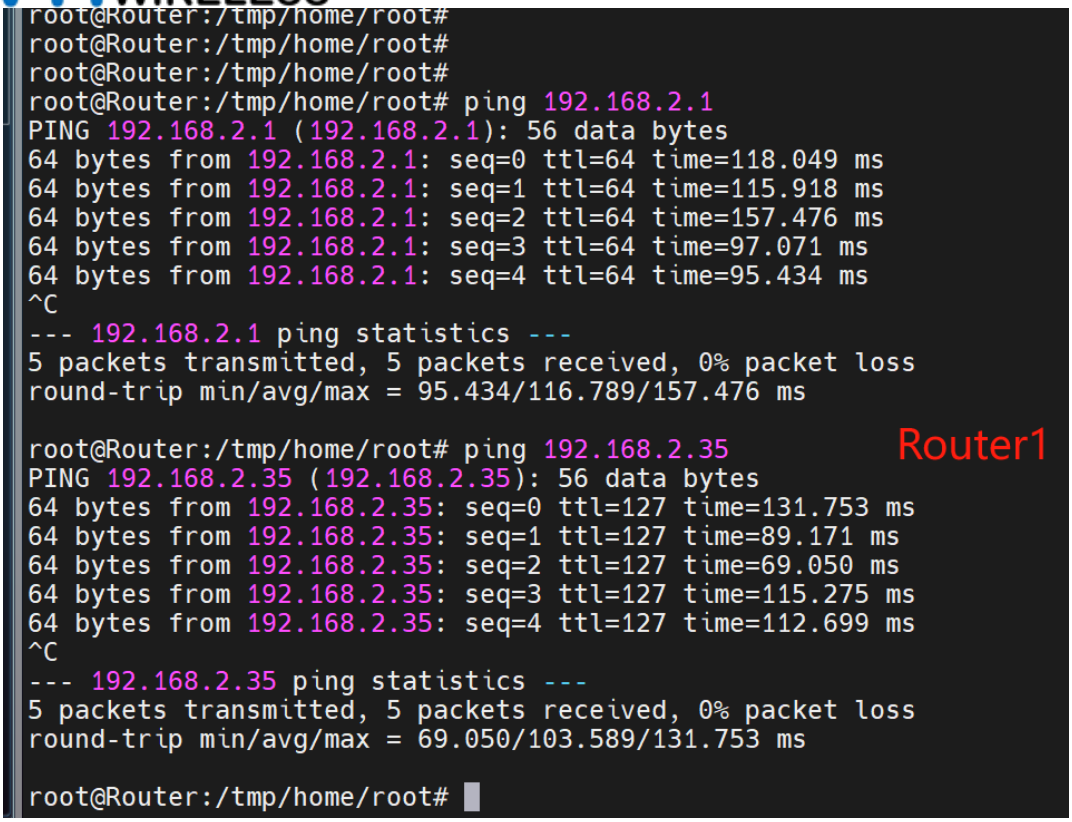


Figure 9-26

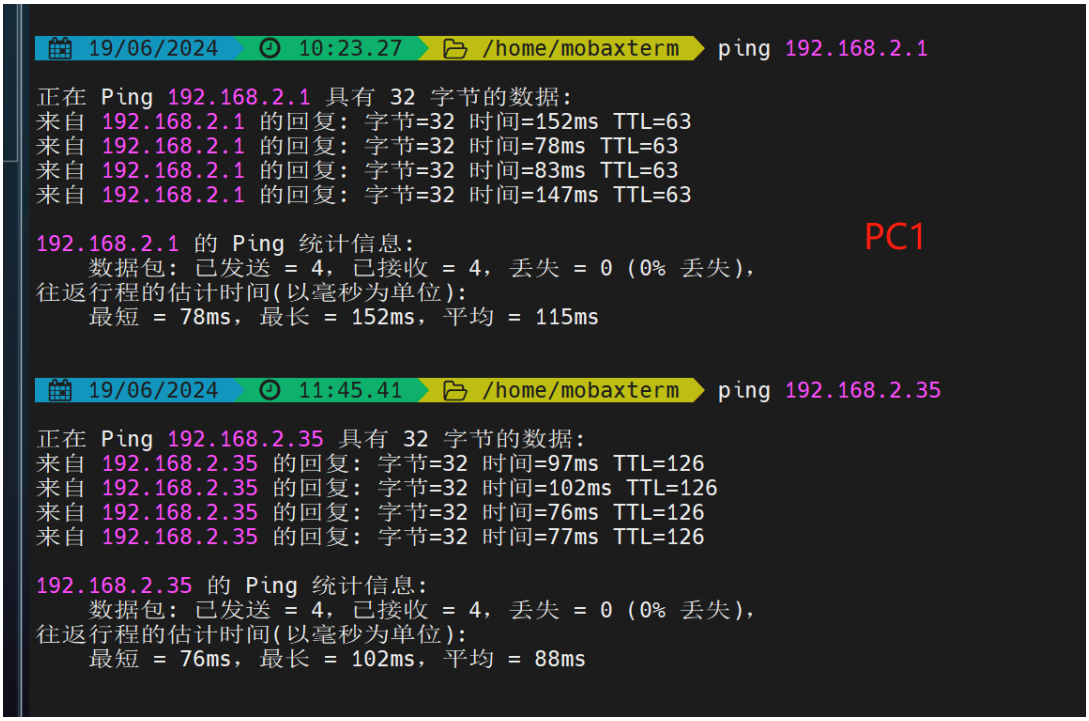


Figure 9-27

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 9-28

```
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
```

PC2

Figure 9-29

9.3. GRE setting

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 Settings" in the navigation bar, as shown in Figure 9-1

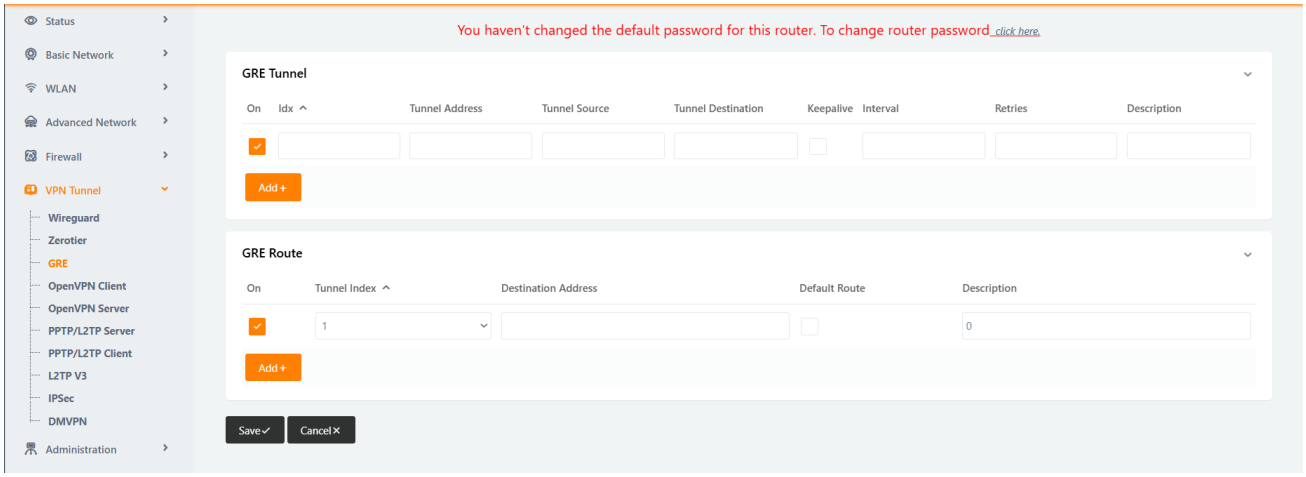


Figure 9-30

Step 2: GRE Mode Parameters

parameter	meaning	How to configure
ON/OFF GRE	ON/OFF 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
Tunnel Source	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
Tunnel Destination	The external interface IP address of the tunnel peer network is usually the public IP (Internet) address, but it can also be the internal IP address of the enterprise	Enter the IP address of the external 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 9-2 GRE Mode Parameter Configuration

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

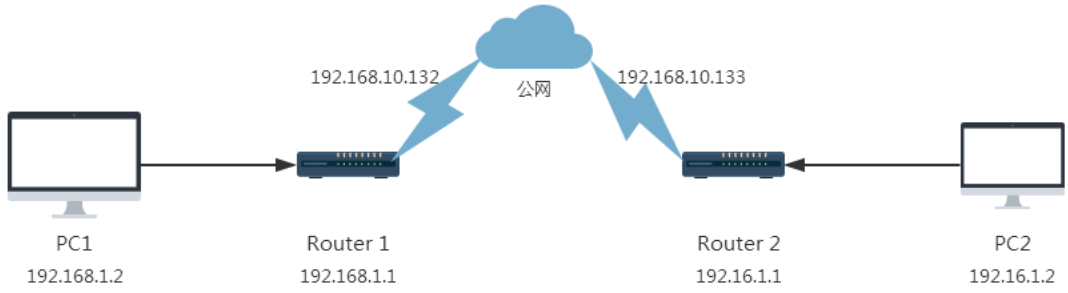


Figure 9-31

Router1 configuration:

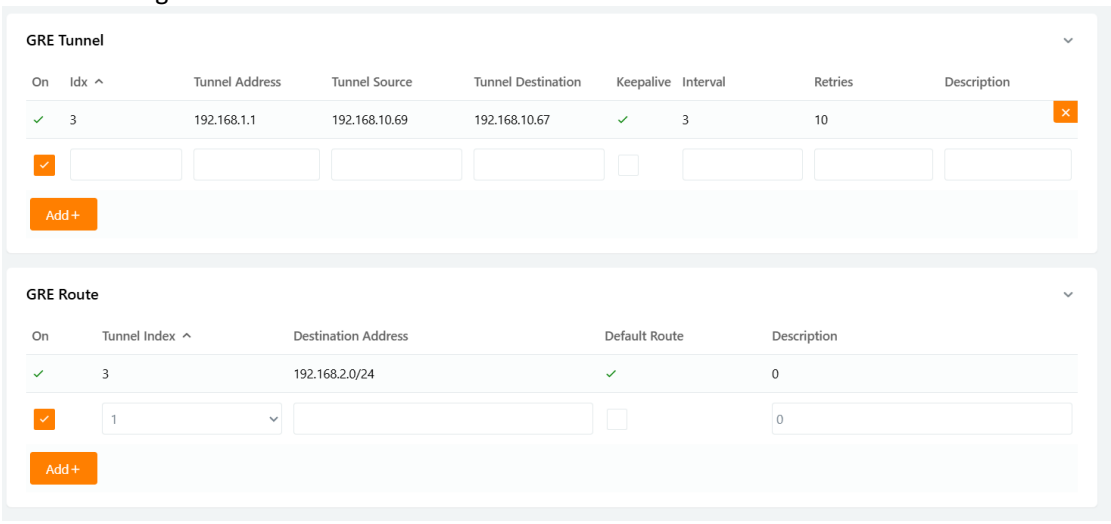


Figure 9-32

Router2 configuration:

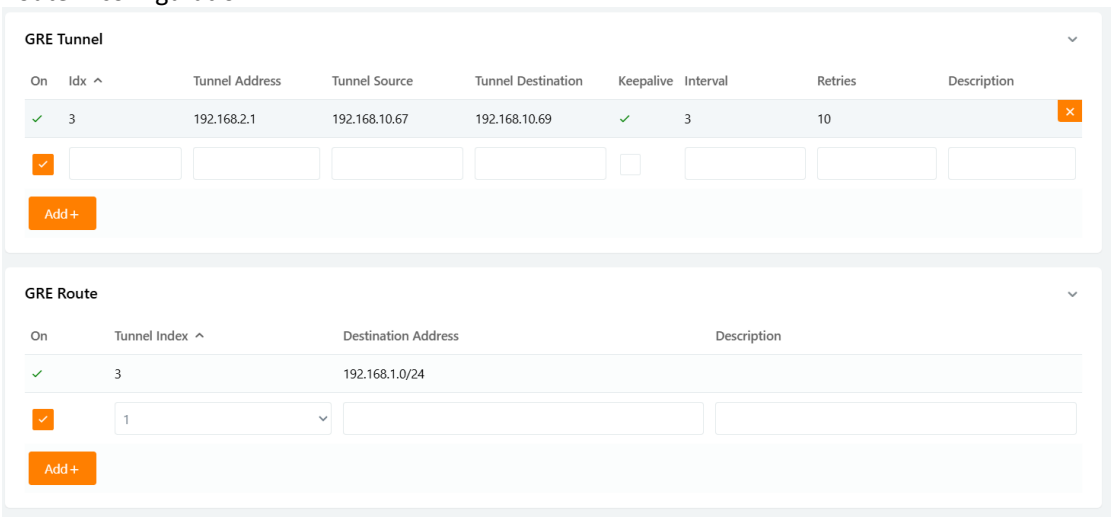


Figure 9-33

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 9-34

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 9-35

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

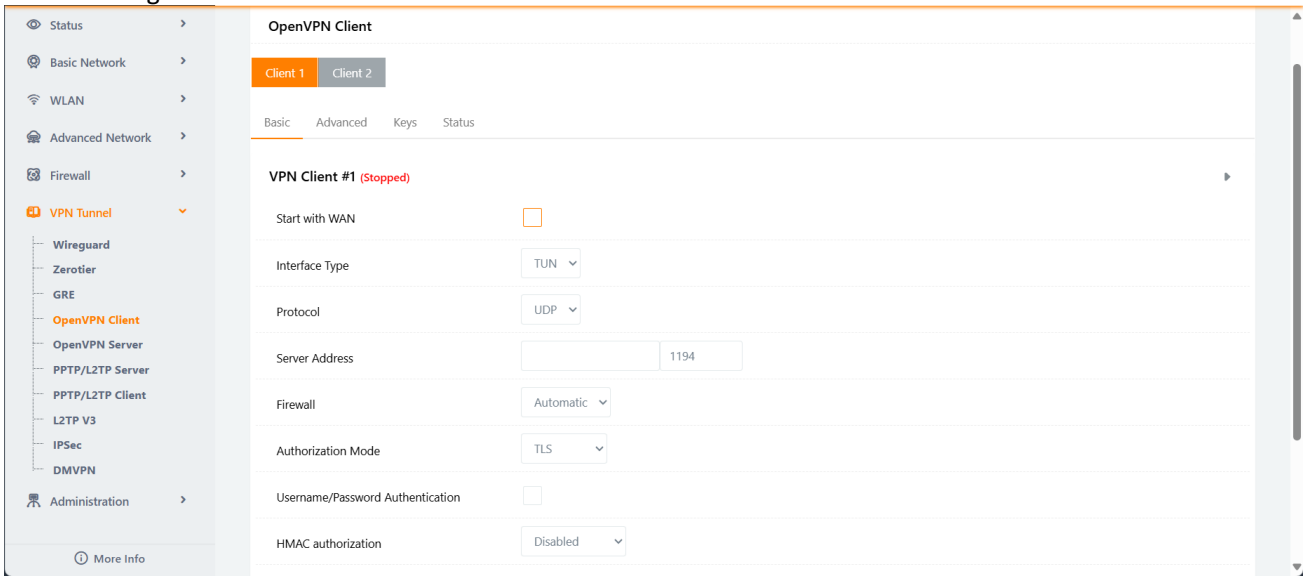


Figure 9-36

Basic Parameter Configuration Description:

The name of the parameter	meaning	How to configure
Start with WAN	Whether the network is over a WAN port	ON/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
Protocol	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
Authorization Mode	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
Username Authen. Only	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
Server is on the same subnet	Appears when TAP is selected for Interface Type	Enable or disable
Create NAT on tunnel	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 9-3 OpenVPN parameter configuration

Advanced settings:

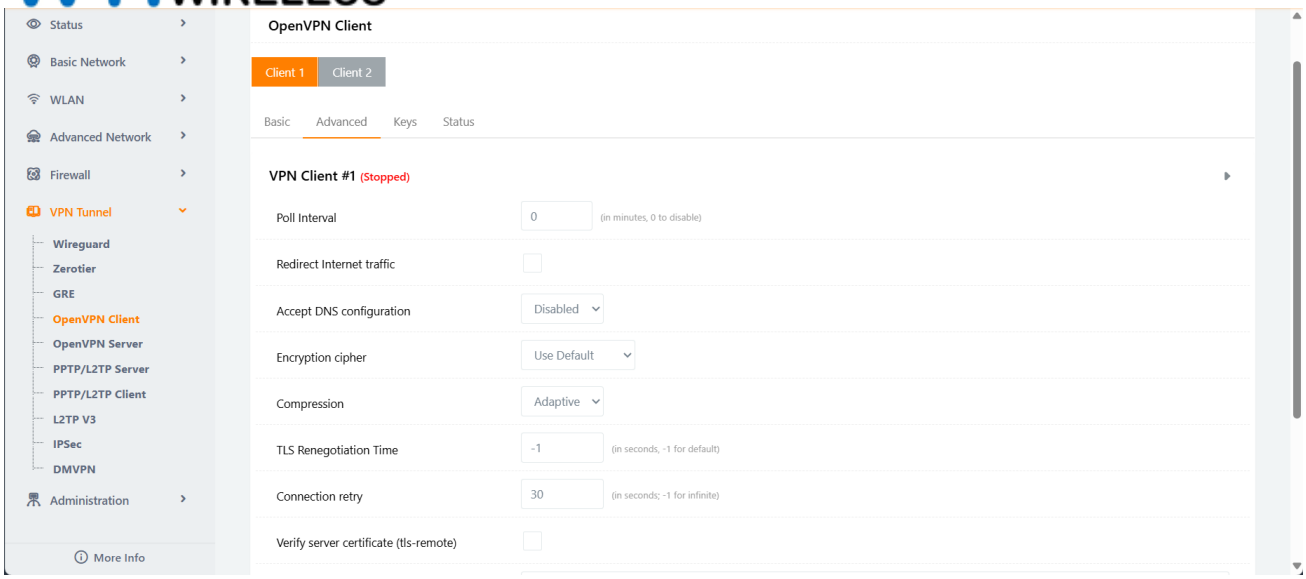


Figure 9-37

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
Redirect Internet traffic	Whether to allow OpenVPN as the default route	Enable or Disable
Receives the peer DNS configuration	4 types of end-to-end DNS configurations: disabled,relaxed,strict,exclusive	Select any one of the four modes from the dropdown menu
Encryption cipher	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
Compression	4 compression modes:disabled，none，enabled，adaptive	
TLS Renegotiation time	d-1 is the default in seconds	-1 is the default Enter 0 or higher to enable
Connection retry	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
Verify server certificate (tls-remote)	After checking the box, the common name input box appears	Enable or disable
Custom Configuration	Reservation settings	

Table 9-4

Keys:

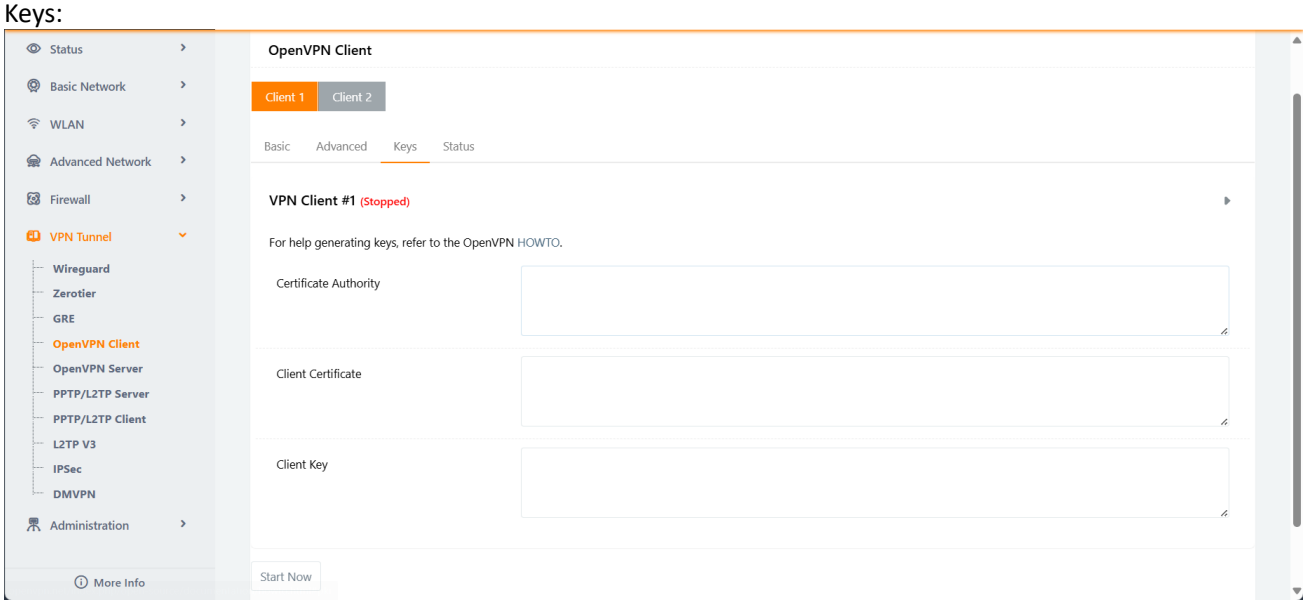


Figure 9-38

Key Setup Instructions:

The name of the 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 Key	Configure the corresponding client secret	Enter the corresponding client secret

Table 9-5

Status:

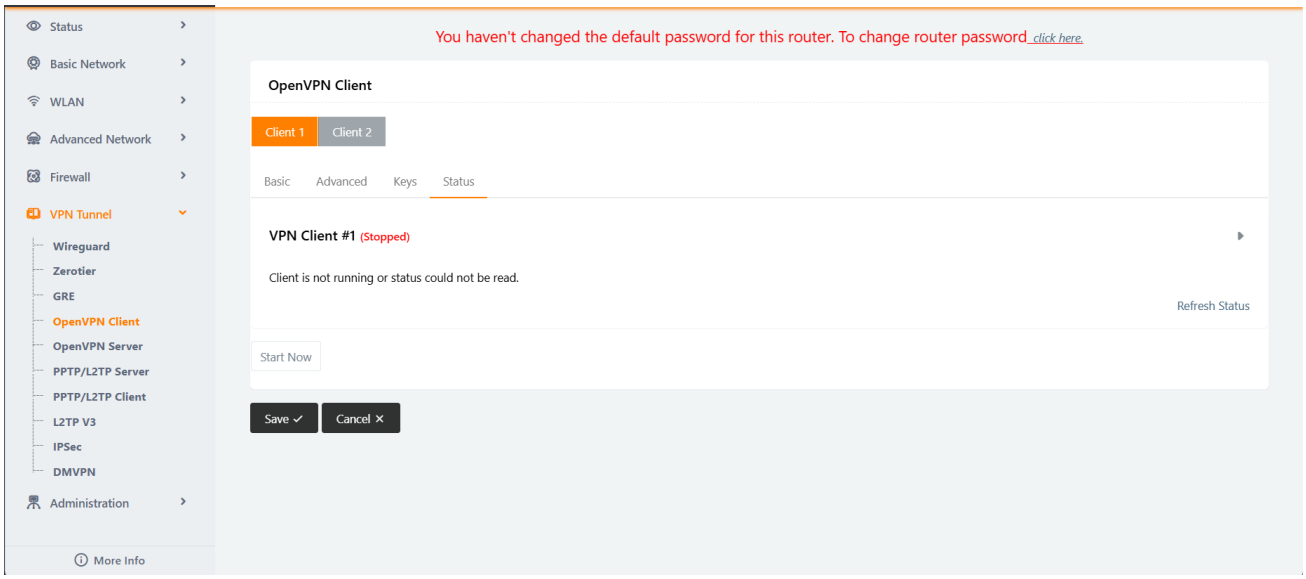


Figure 9-39

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 9-6

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

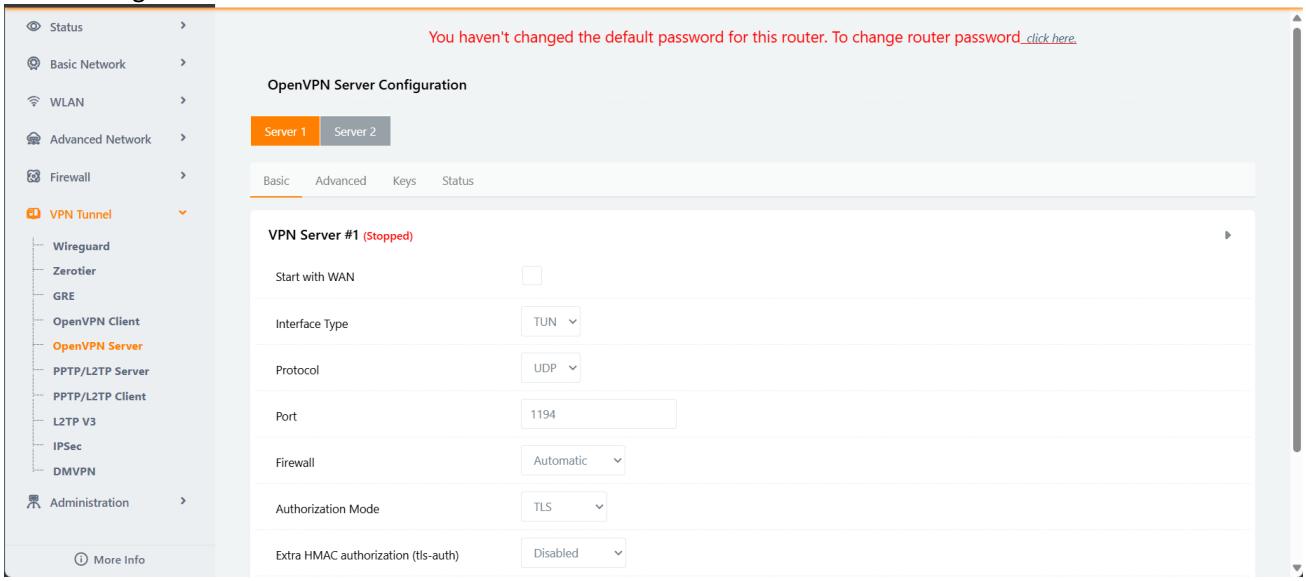


Figure 9-40

Basic Parameter Configuration Description:

parameter	meaning	How to configure
Start with WAN	Whether the network is over a WAN port	ON/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
Protocol	TCP mode or UDP mode	Select TCP mode or UDP mode from the drop-down list
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
Authorization Mode	The authentication types include TLS, static key, and custom	Select TLS, static key, or custom from the drop- down drop-down
Extra HMAC authorization	Hash message authentication: Default:	

(tls-auth)	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 9-7 OpenVPN parameter configuration

Advanced :

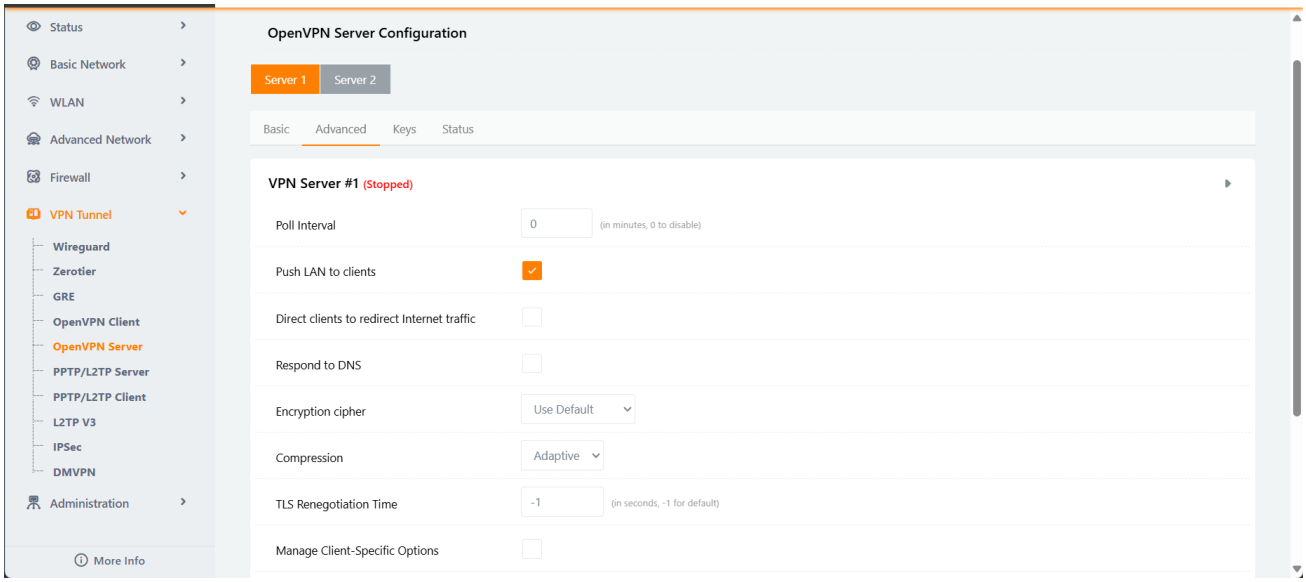


Figure 9-41

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
Advertise DNS to clients	The server sends DNS to the client	Enable or disable Not enabled by default
Encryption cipher	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
Compression	4 compression modes:disabled， none， enabled， adaptive	Adaptive by default