

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:4c9f: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

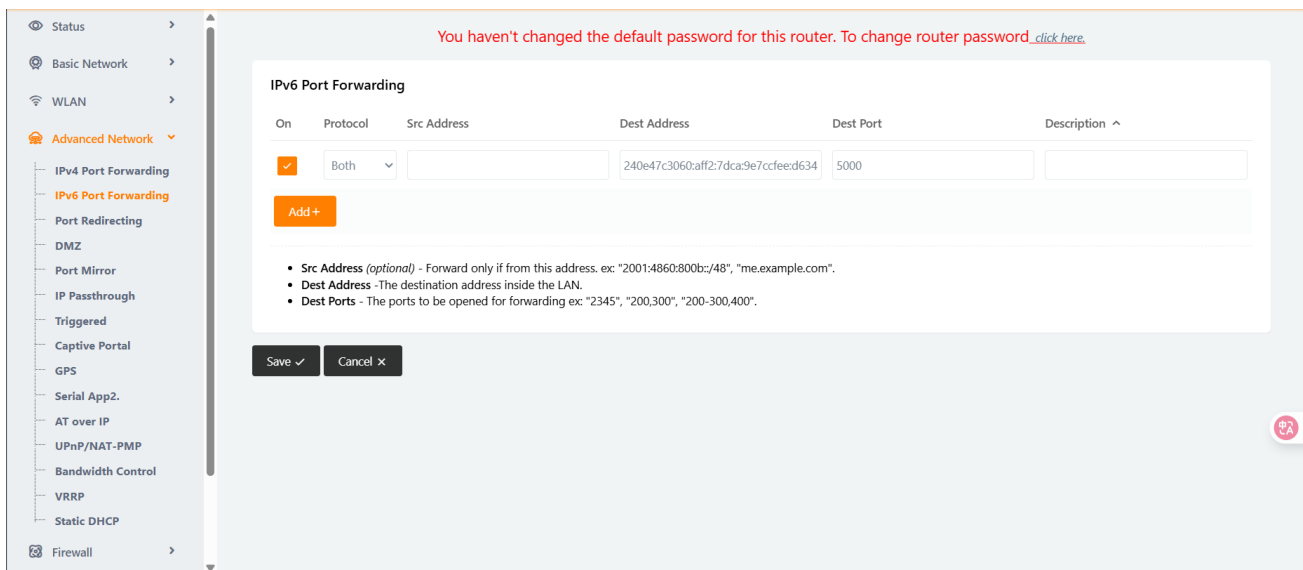


Figure 7-8

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

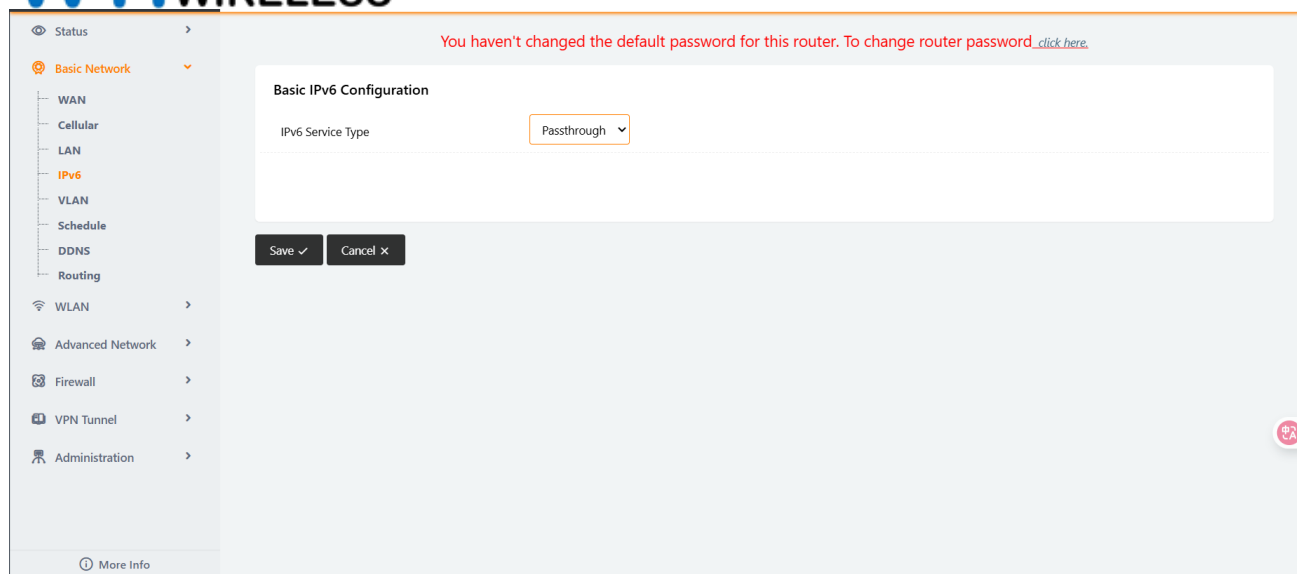


Figure 7-9

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

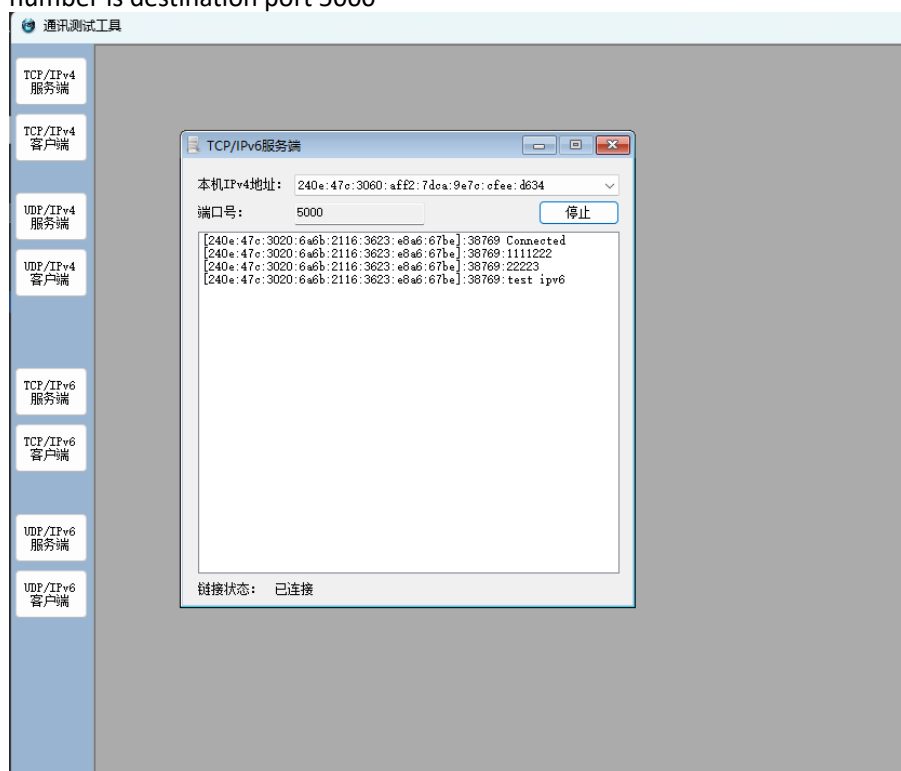


Figure 7-10

Step 4: On the PC 2 connected to Router 2, open the TCP client and use the temporary ipv6 address of the server and the destination port 5000 to connect. Port forwarding is normal.

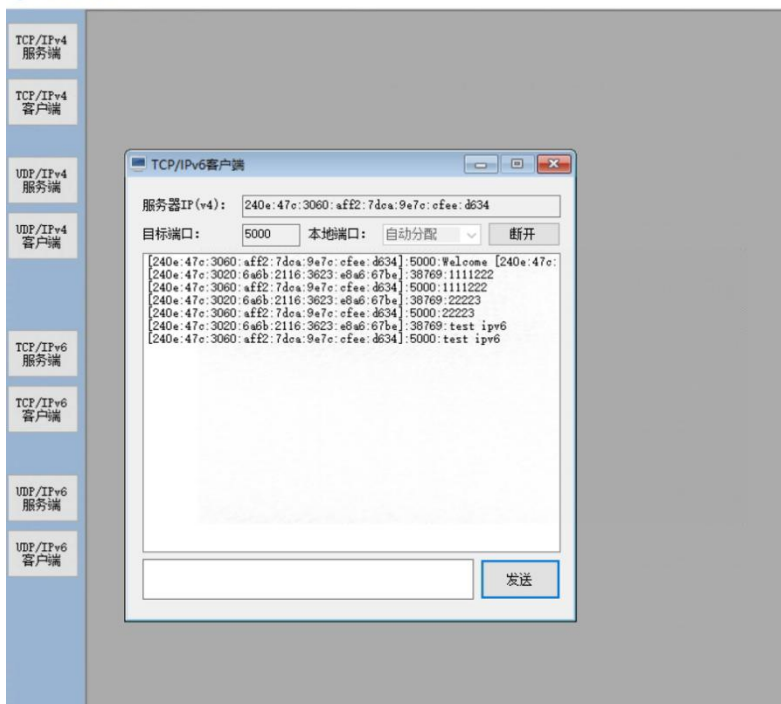


Figure 7-11

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

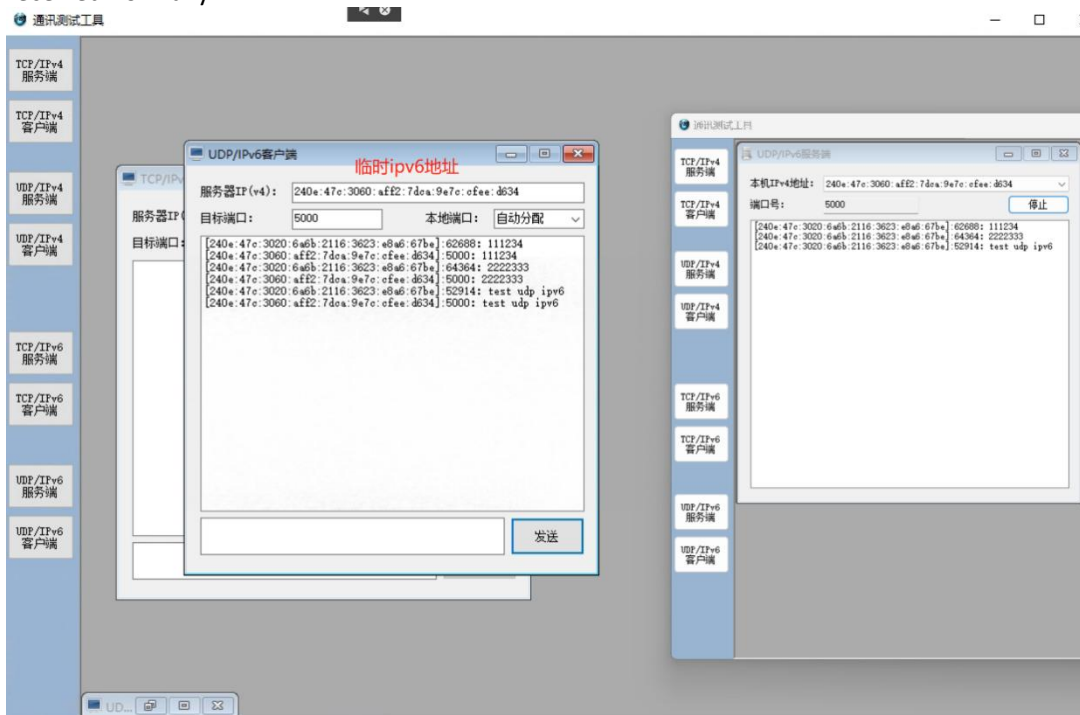


Figure 7-12

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.

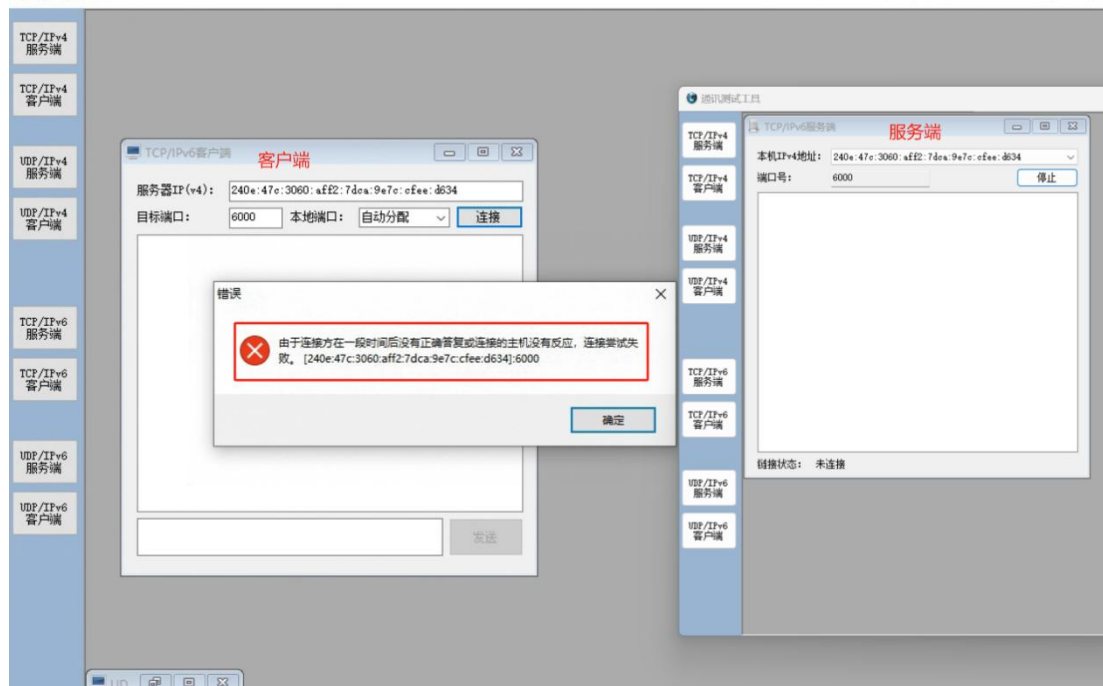


Figure 7-13

7.3. Port redirection settings

Port redirection 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.

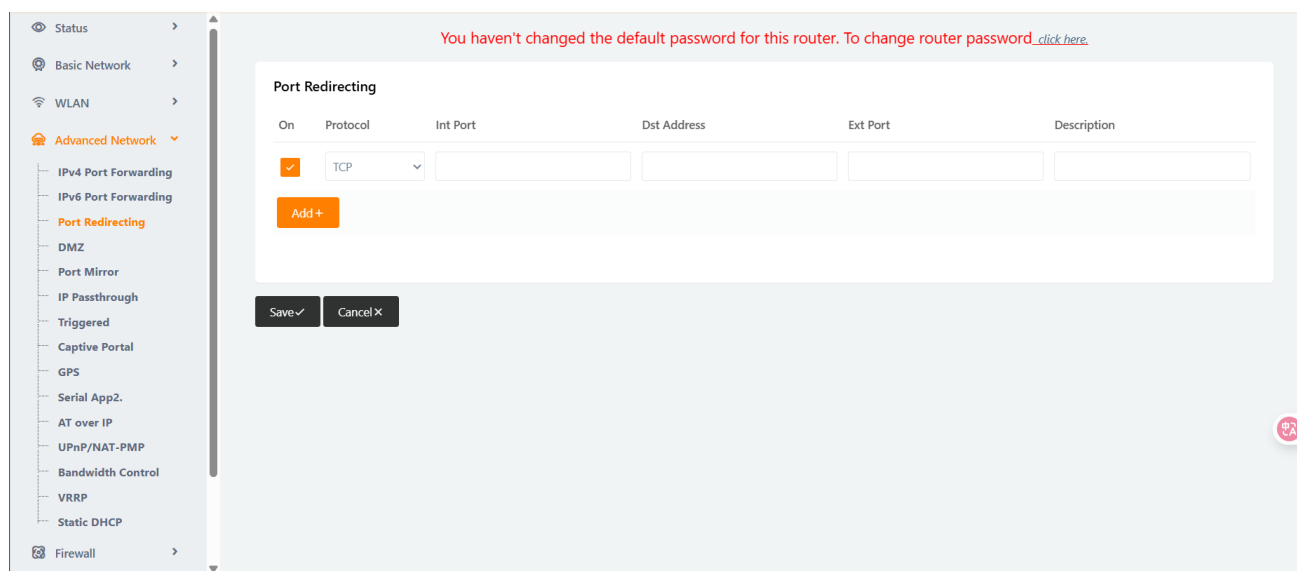


Figure 7-14

Description of Port Redirection configuration parameters

parameter	illustrate
enable	Tick/Unchecked
Protocol	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
Dst Address	Only redirect data from a set IP range
External port	The port that comes in from the WAN

Table 7-1 Port Redirection Configuration Parameters

Port Redirection 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

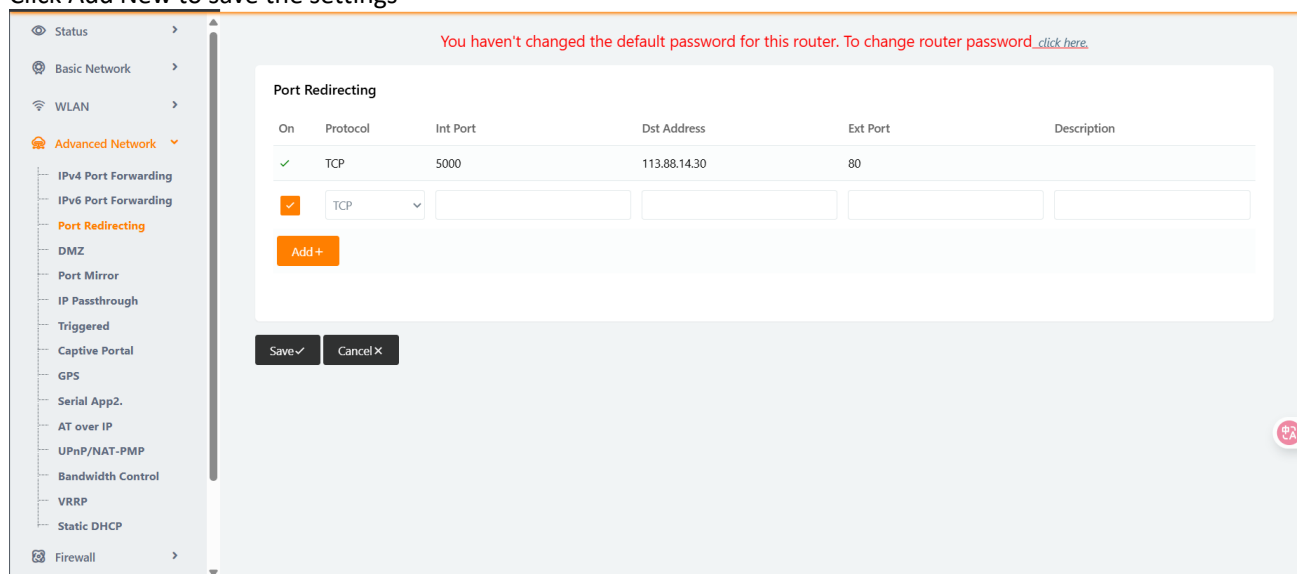


Figure 7-15 Port Redirection Configuration

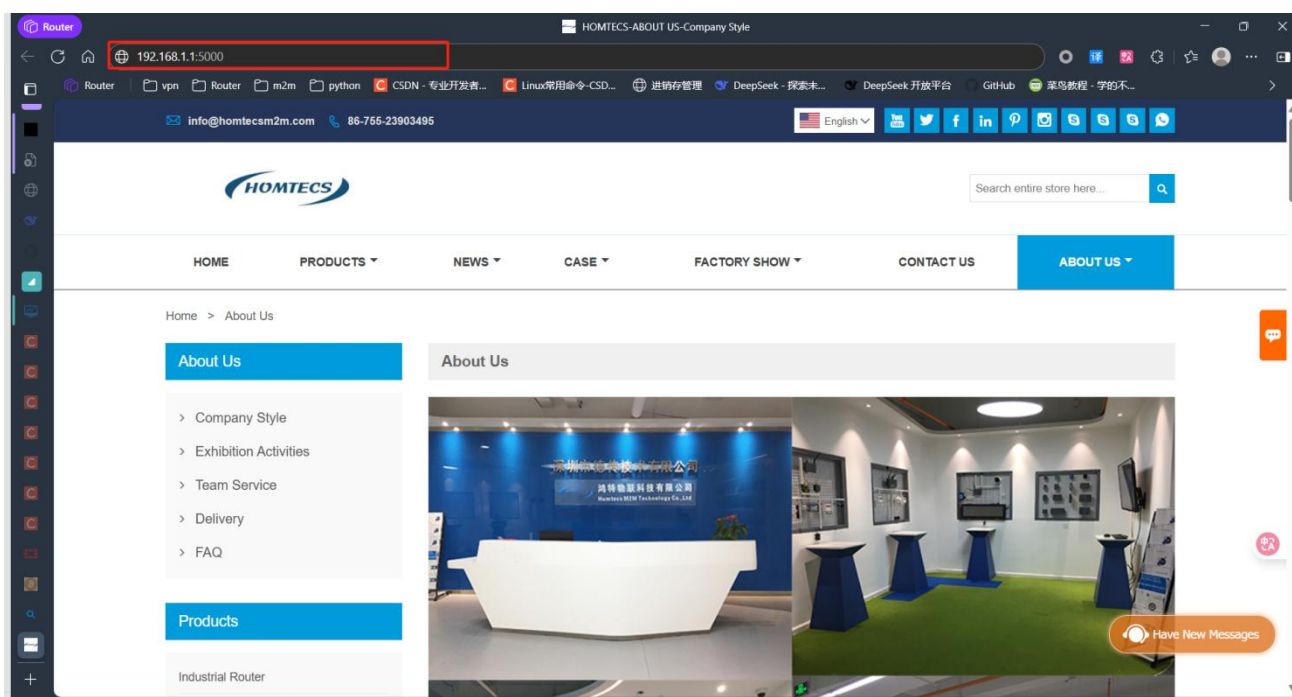


Figure 7-16 Redirect Service

7.4. DMZ settings

The space between two firewalls is called DMZ. Compared to the Internet, DMZ can provide higher security, but its security is lower than that of internal networks.

DMZ (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 <https://www.wtiwireless.com/>

buffer is located within a small network area between the internal and external networks of the enterprise. Some server facilities that must be made public, such as enterprise web servers, FTP servers, and forums, can be placed within this small network area. On the other hand, through such a DMZ area, the internal network is more effectively protected. Because of this type of network deployment, compared to general firewall solutions, it adds an additional barrier for attackers from the external network.

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.

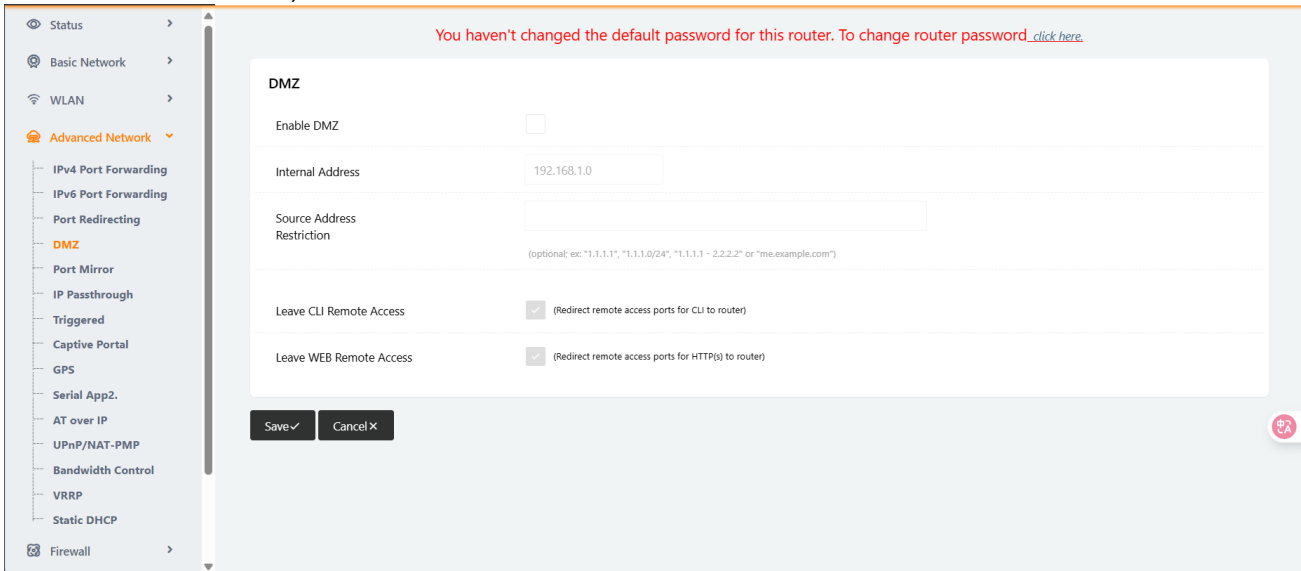


Figure 7-17 DMZ settings



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

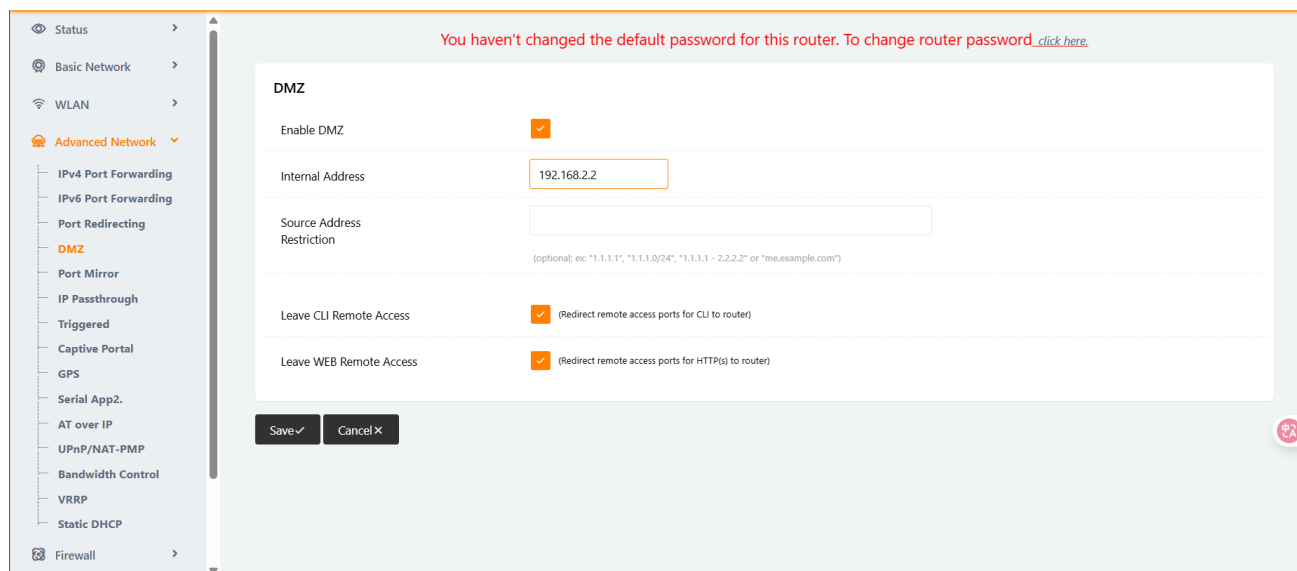


Figure 7-18 DMZ configuration

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

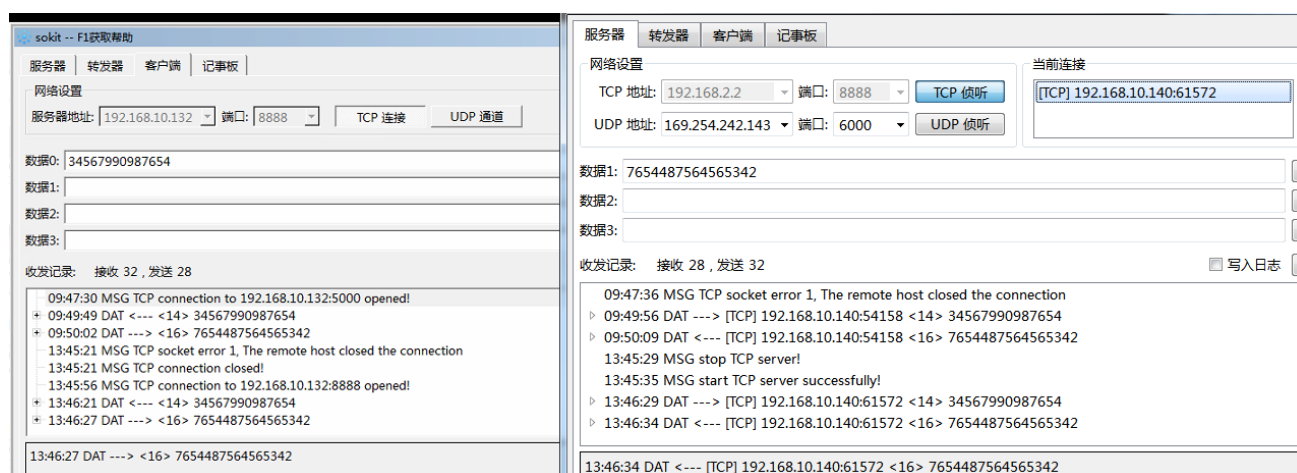
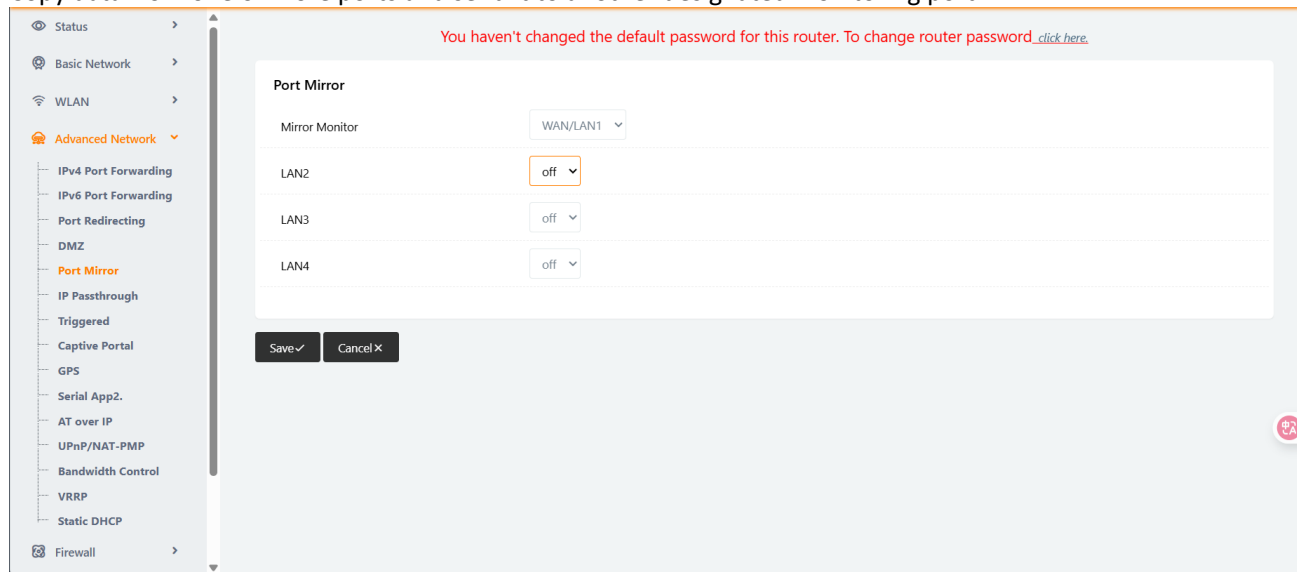


Figure 7-19 Data Sending and Receiving

7.5. Port Mirroring

Port mirroring, also known as port monitoring



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.

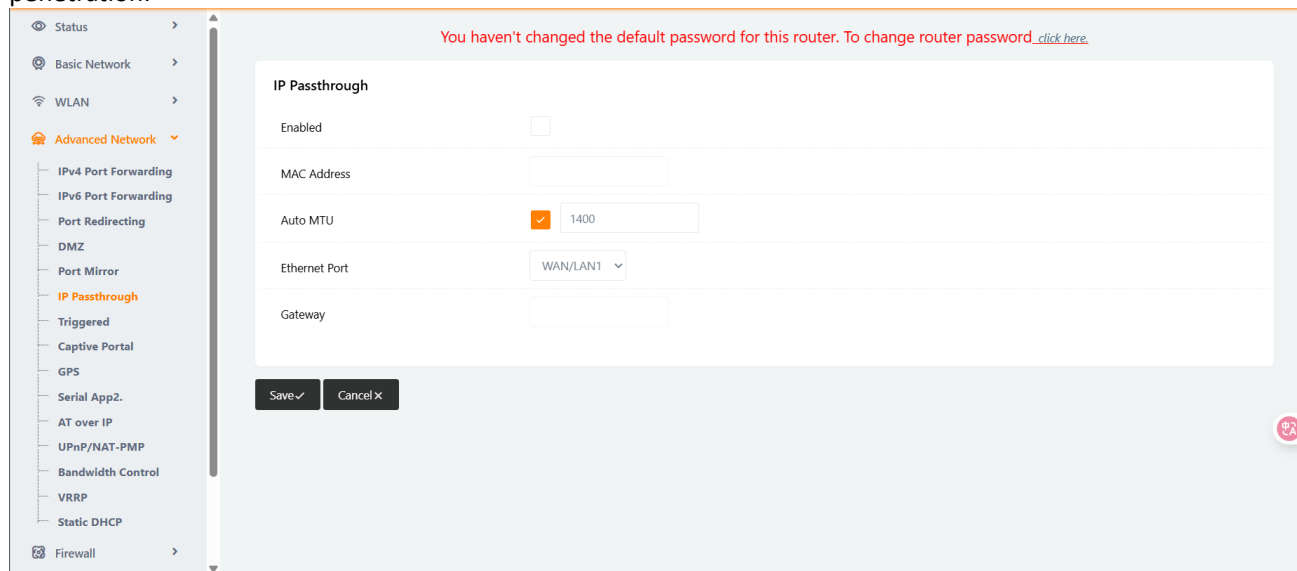


Figure 7-20

Description of the IP Penetration parameter

parameter	illustrate
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 Penetration Parameters

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

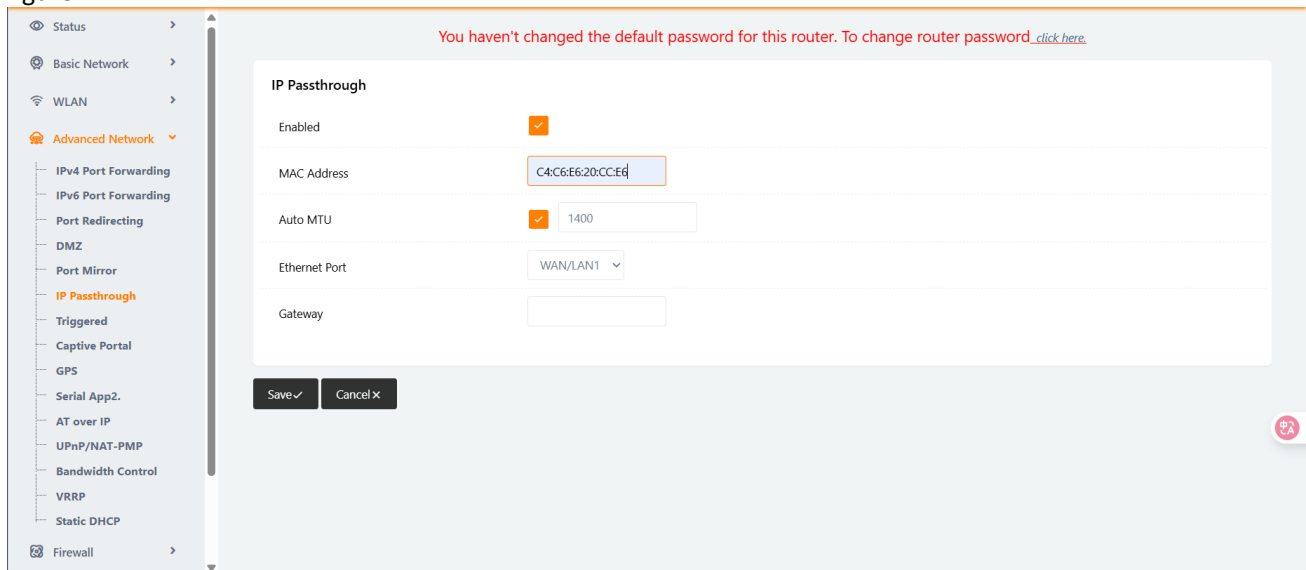
Realtek RTL8852BE WiFi 6 802.11ax PCIe Adapter
  Link encap: IEEE 802.11 HWaddr: C0-35-32-14-EE-A9
    inet addr:192.168.31.167 Mask: 255.255.255.0
    MTU: 1500 Speed:866.70 Mbps
    Admin status:UP Oper status:OPERATIONAL
    RX packets:53241 dropped:0 errors:0 unkown:0
    TX packets:22584 dropped:0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



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

IP Passthrough

Enabled ☒

MAC Address

Auto MTU ☒ 1400

Ethernet Port

Gateway

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

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 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 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 unkown:0
  TX packets:1703201 dropped:0 errors:7352 txqueuelen:0
  
```

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.

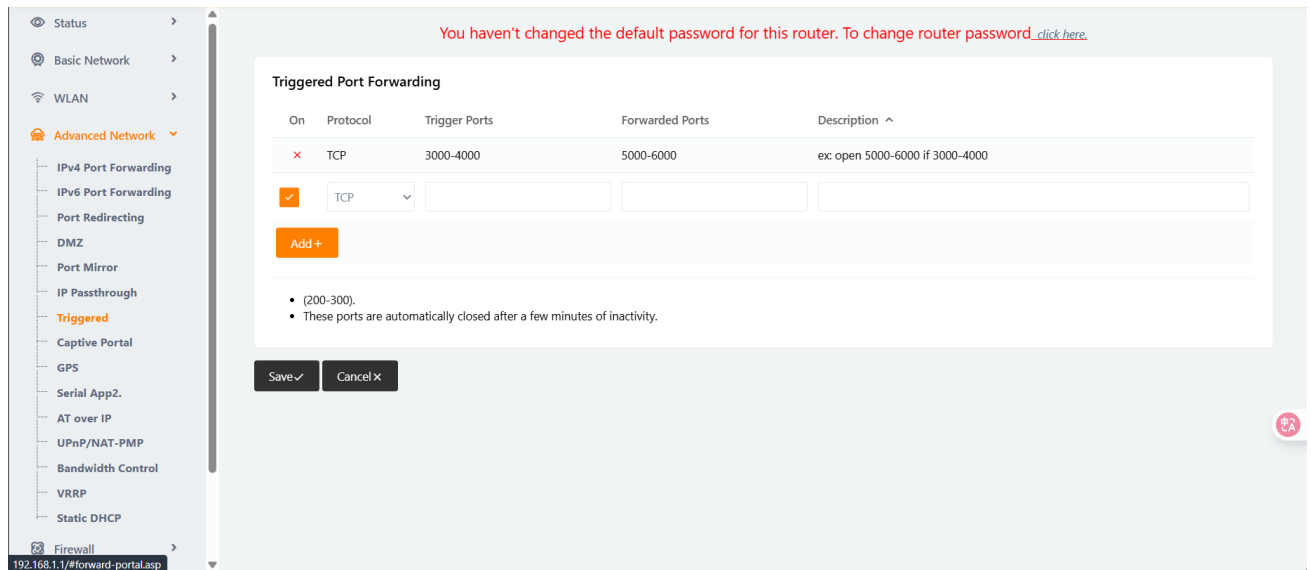


Figure 7-24 Port Triggering

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

Port trigger configuration example:

Step 1:

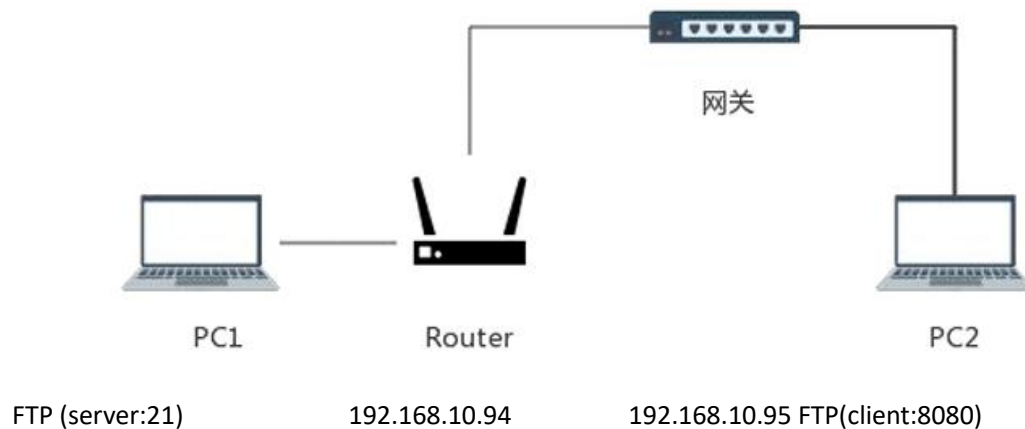


Figure 7-25 Triggering networking

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

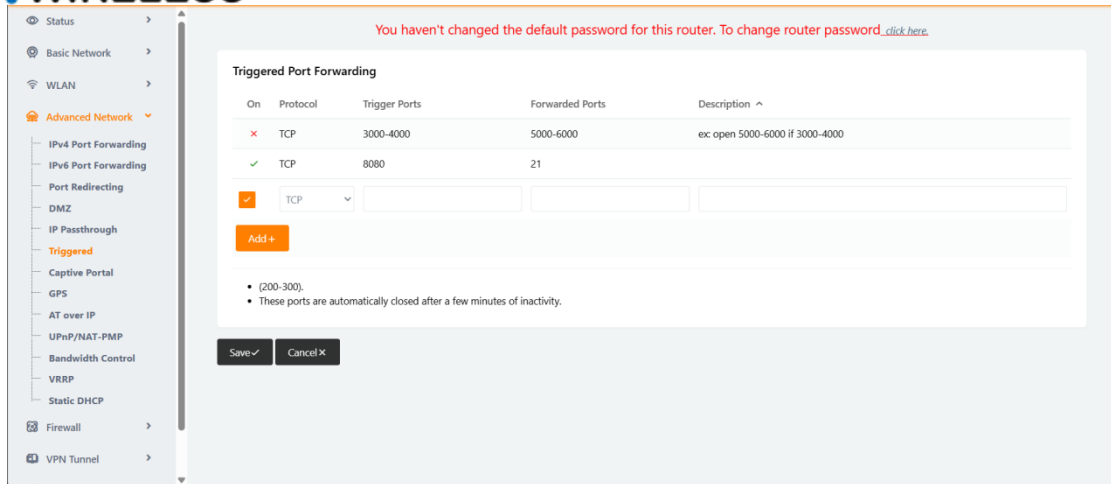


Figure 7-26 Port Trigger Configuration

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):

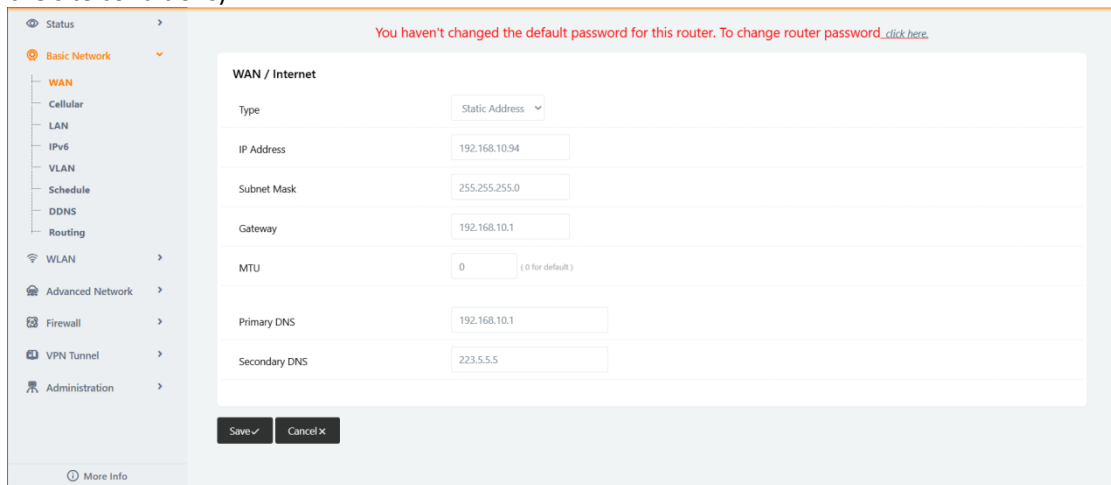


Figure 7-27 Static address settings

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

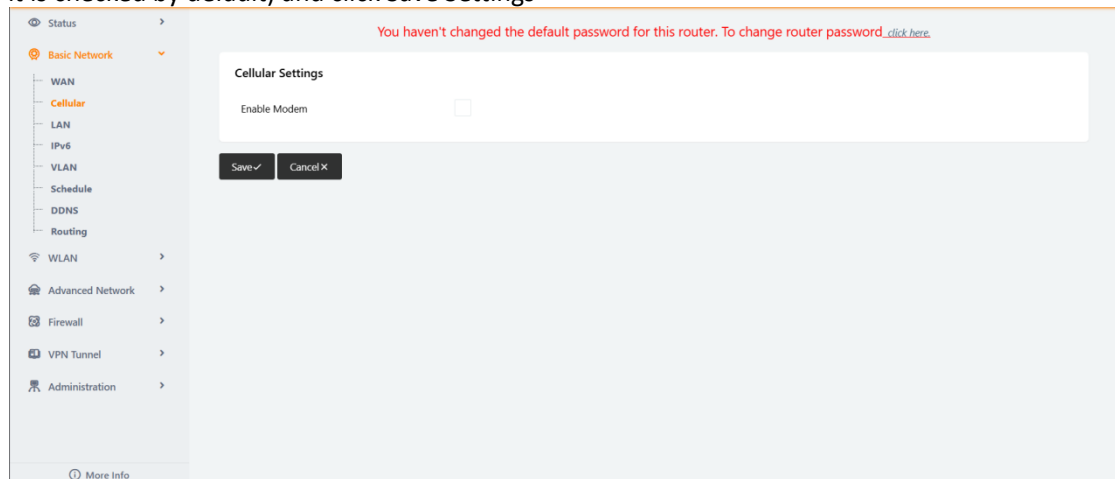


Figure 7-28 Mobile Network Settings

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:

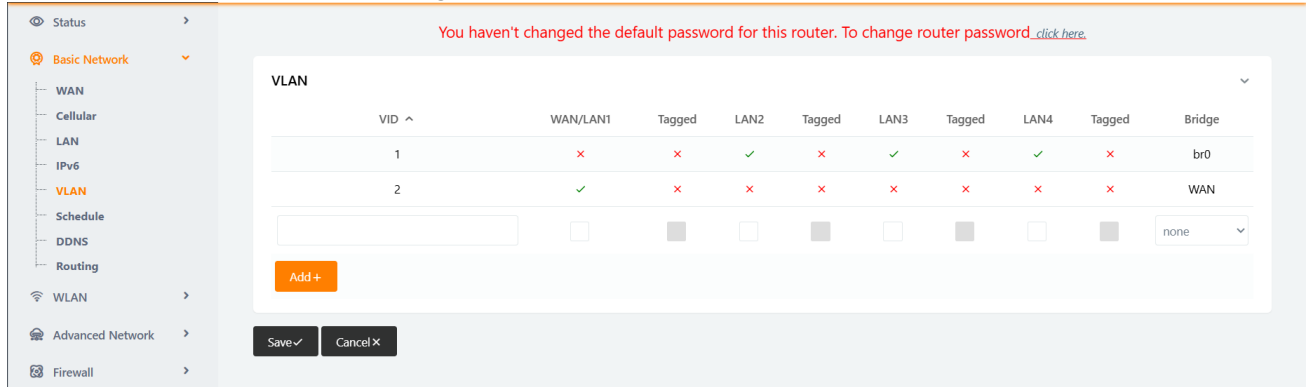


Figure 7-29 VLAN Settings

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

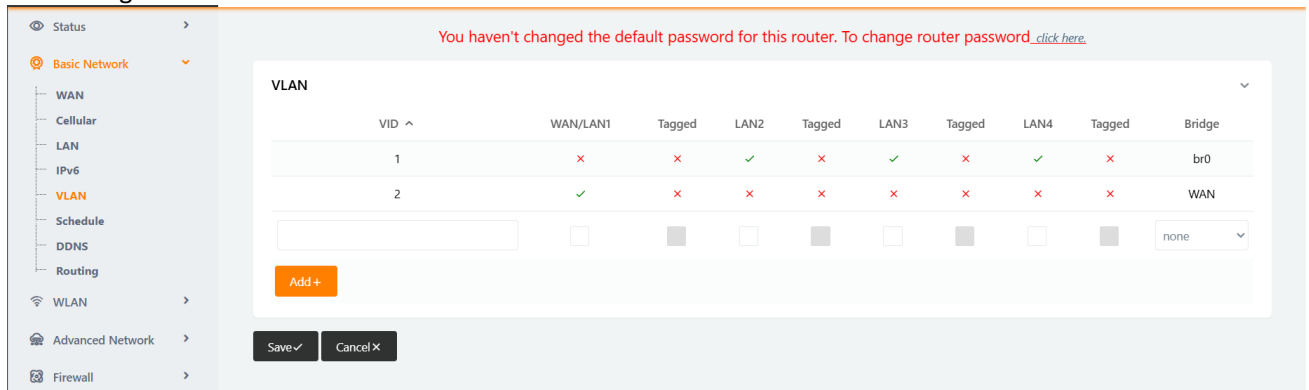


Figure 7-30 VLAN Settings

Step 5:

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

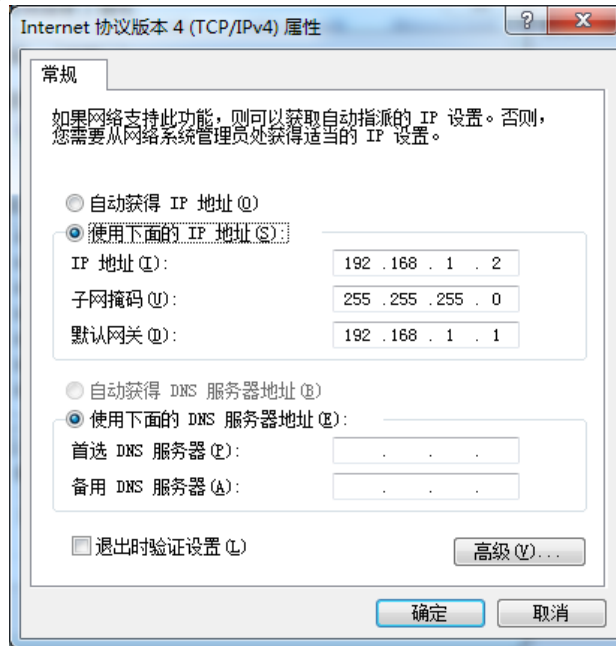


Figure 7-31 Local Connection Diagram

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

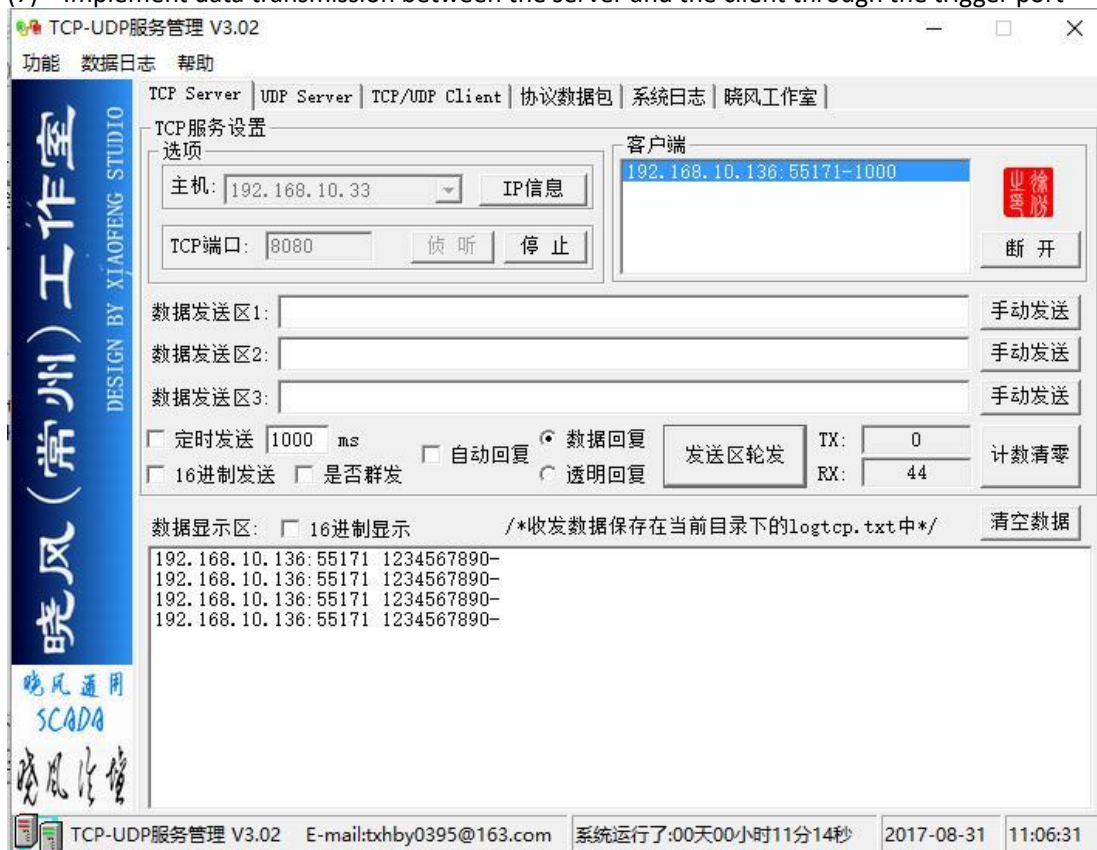


Figure 7-32 Data is sent and received from each other

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

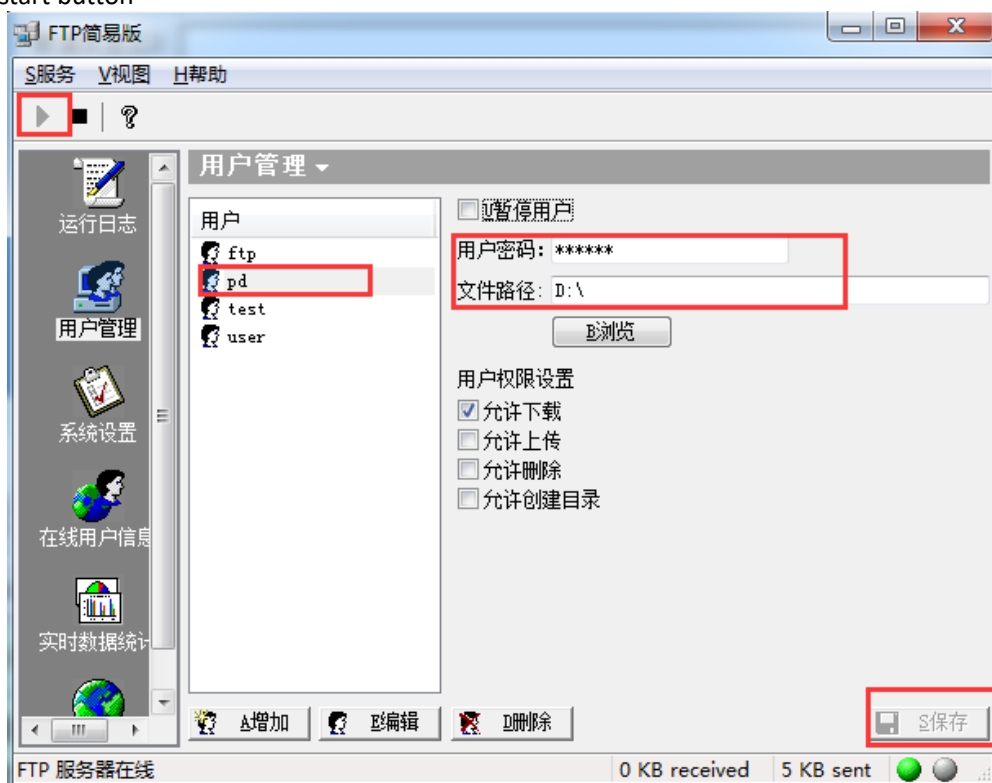


Figure 7-33 FTP Lite configuration

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



Both 5500 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 <https://www.wtiwireless.com/>

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.

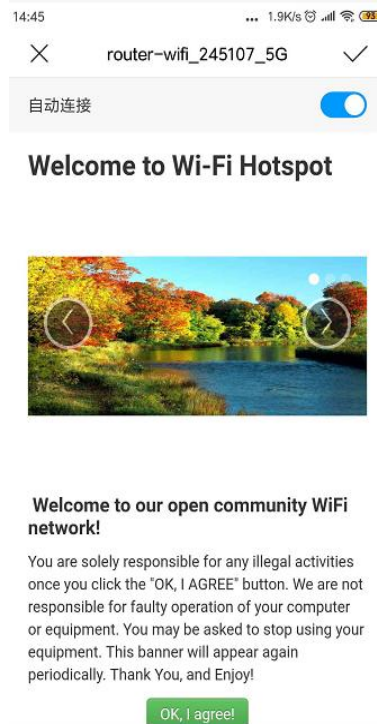


Figure 7-34

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.

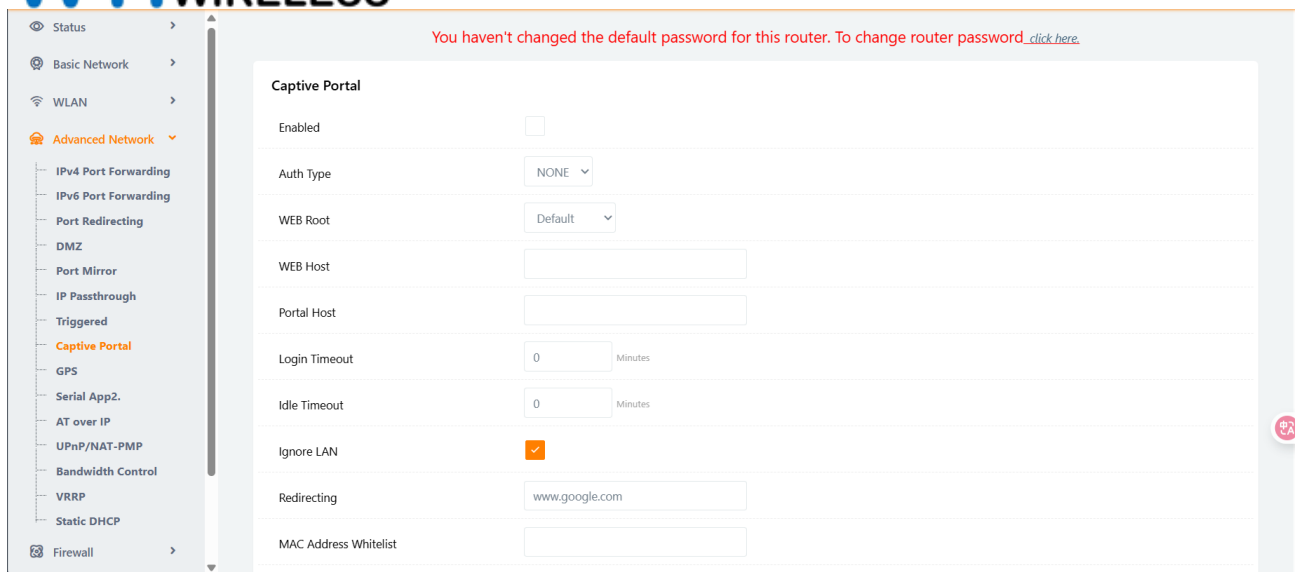


Figure 7-35

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. Serial to TCP/IP

In the navigation bar, select Advanced Network > Serial Port Application. On the page that opens, 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 setting.

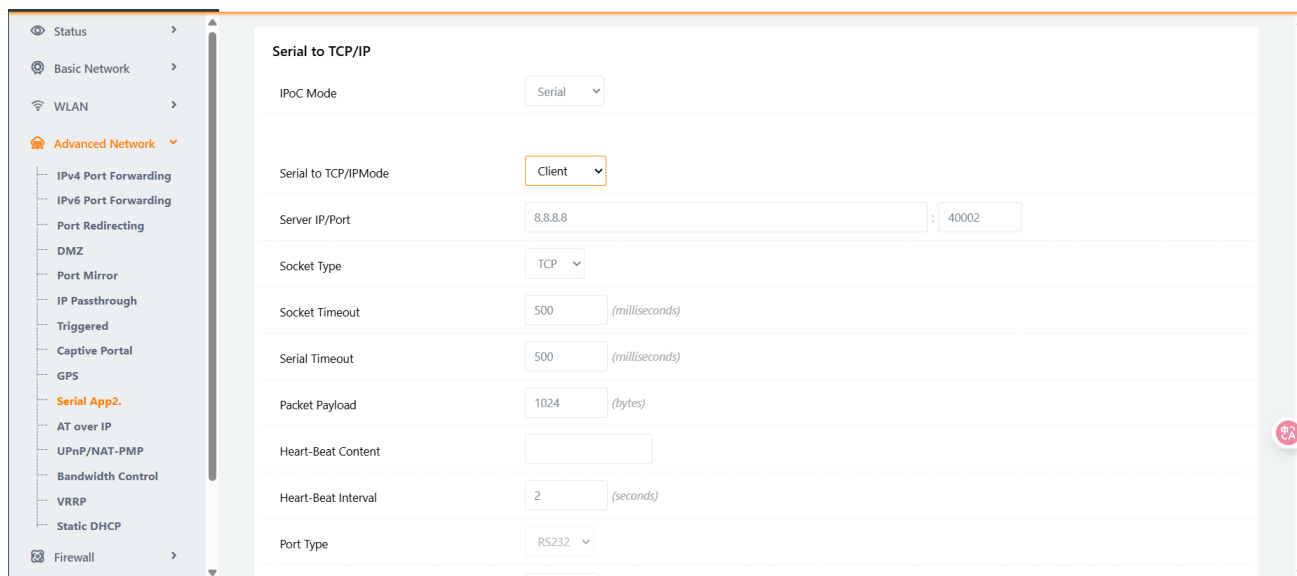


Figure 7-36

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
-----------	---------	------------------

parameter	meaning	How to configure
Server 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
Socket Type	TCP/UDP protocol is supported	Select TCP or UDP based on your application
Heart-Beat 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
Heart-Beat 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
Parity Bit	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

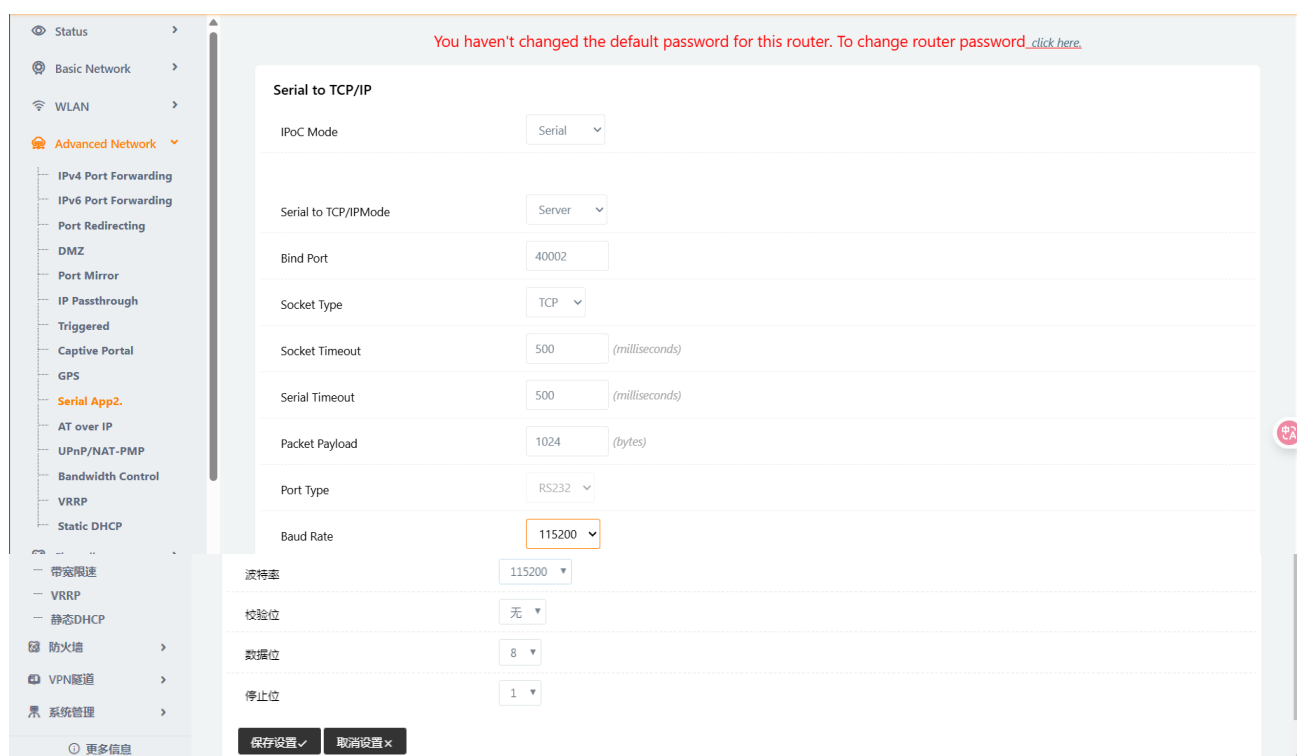
Table 7-3

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: 115500
4. Click Save settings



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

Serial to TCP/IP

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

Baud Rate: 115200

波特率: 115200

校验位: 无

数据位: 8

停止位: 1

保存设置 ✓ 取消设置 ✕

port, as

shown in the following figure:

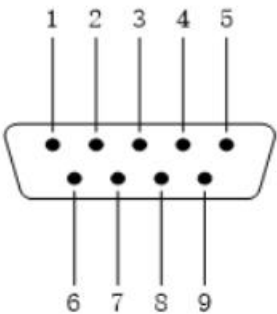
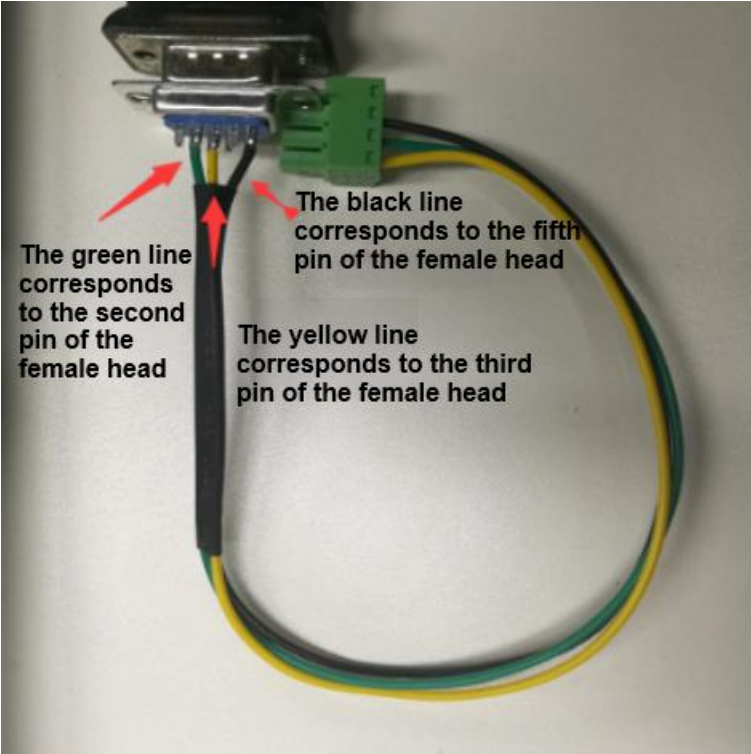


Figure 7-38

Terminal block 1 (4PIN)						
1	2	3	4	1Red line	VCC	+3.3V [Default N.C,open according to requirements]
				2Black line	GND	GND
				3Green line	TXD/485-B	RS232,OUTPUT: or 485-B
				4Yellow line	RXD/485-A	RS232,INPUT: or 485-A

Table 7-4 Terminal Wiring Diagram

Step 3:
View the COM port information on the computer

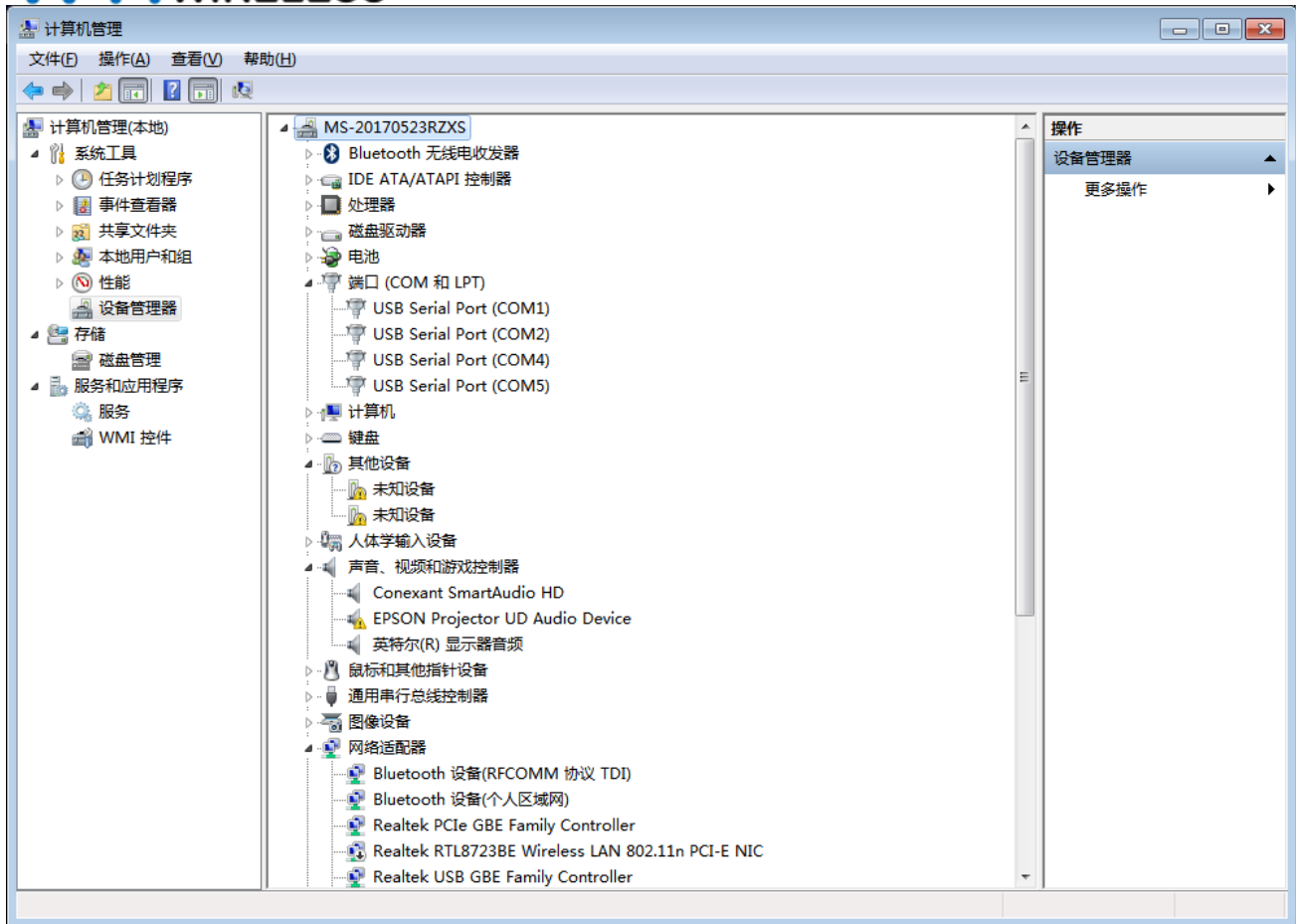


Figure 7-39 The COM port of a PC

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

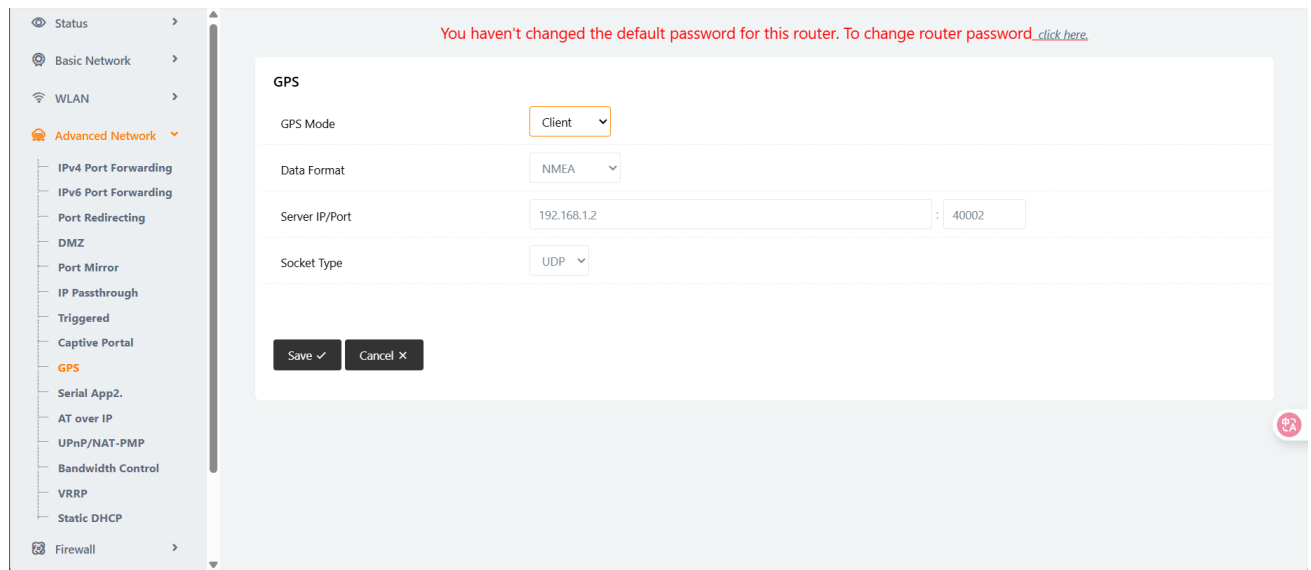


Figure 7-41

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

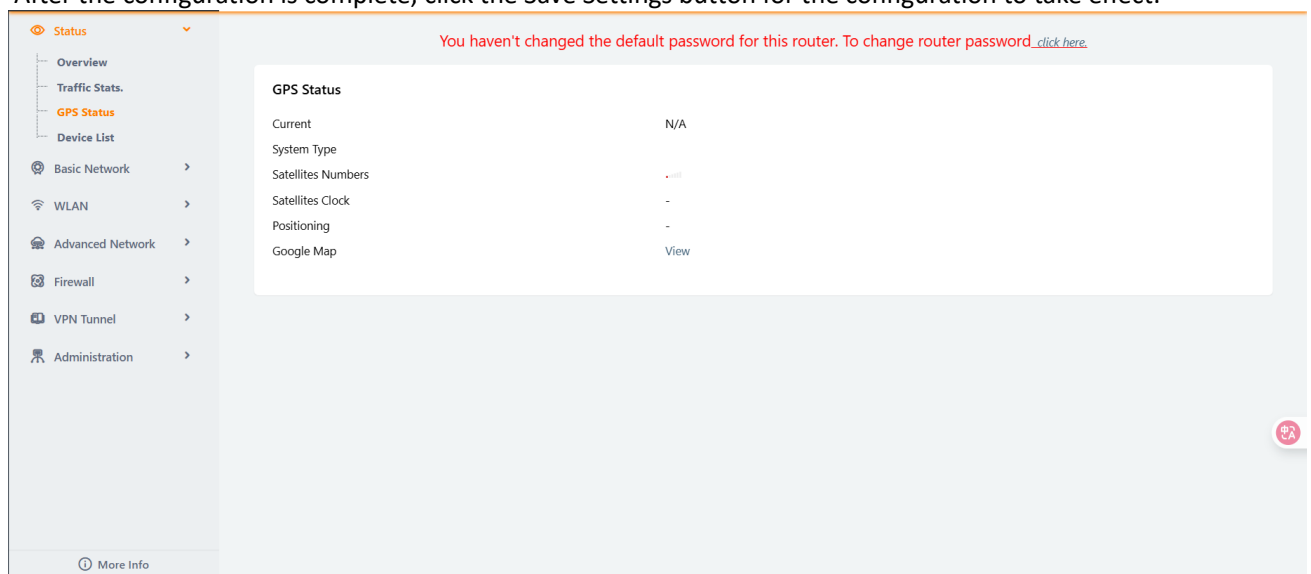


Figure 7-42

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.



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

GPS

GPS Mode

Client

Data Format

NMEA

Server IP/Port

192.168.1.2

:

40002

Socket Type

UDP

Save ✓

Cancel ✕

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:

GPS Status

Current	OK
System Type	GPS
Satellites Numbers	06
Satellites Clock	240809 - 100115.00
Positioning	2234.490629N - 11355.274123E
Google Map	View

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.

sokit -- F1获取帮助

服务器 | 转发器 | 客户端 | 记事板

网络设置

TCP 地址: 192.168.1.2

端口: 8888

TCP 侦听

UDP 地址: 192.168.1.2

端口: 40002

UDP 侦听

当前连接

[UDP] 192.168.1.1:40001

全选

断开

数据1:

数据2:

数据3:

发送

发送

发送

收发记录: 接收 404027, 发送 0

☐ 写入日志

清除

18:04:24 DAT ---> [UDP] 192.168.1.1:40001 <1024> ..\$GLGSV,3,1,09,78,28,203,38,66,49,050,42,82,07,270,16,77,85,...

18:04:24 DAT ---> [UDP] 192.168.1.1:40001 <106> 1*3E...\$GNGSA,A,2,66,76,78,.....1.2,0.9,0.7,2*30...\$GNGSA,A,...

18:04:25 DAT ---> [UDP] 192.168.1.1:40001 <1024> ..\$GLGSV,3,1,09,78,28,203,38,66,49,050,43,82,07,270,19,77,85,...

18:04:25 DAT ---> [UDP] 192.168.1.1:40001 <108> 7,1*3E...\$GNGSA,A,2,66,76,78,.....1.2,0.9,0.7,2*30...\$GNGSA,...

18:04:26 DAT ---> [UDP] 192.168.1.1:40001 <1024> ..\$GLGSV,3,1,09,78,28,203,38,66,49,050,42,82,07,270,19,77,85,...

18:04:26 DAT ---> [UDP] 192.168.1.1:40001 <108> 7,1*3E...\$GNGSA,A,2,66,76,78,.....1.2,0.9,0.7,2*30...\$GNGSA,...

18:04:27 DAT ---> [UDP] 192.168.1.1:40001 <1024> ..\$GLGSV,3,1,09,78,28,203,38,66,49,050,43,82,07,270,19,77,85,...

18:04:27 DAT ---> [UDP] 192.168.1.1:40001 <108> 7,1*3E...\$GNGSA,A,2,66,76,78,.....1.2,0.9,0.7,2*30...\$GNGSA,...

18:03:46 DAT ---> [UDP] 192.168.1.1:40001 <1024> ..

\$GLGSV,3,1,09,78,27,203,45,66,49,049,36,82,07,270,20,77,85,090,24,1*74...

\$GLGSV,3,2,09,76,27,029,32,65,21,106,17,81,02,226,17,67,28,340,22,1*79...\$GLGSV,3,3,09,83,01,307,1*4E...

Figure 7-46 TCP-UDP receives GPS packets

Example of GPS tracks:

<https://www.wtiwireless.com/>

84 /

WTIwireless

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 5500, click Save

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

GPS Mode	Client
Data Format	M2M_FMT
Server IP/Port	detran.xicp.net : 6001
Socket Type	UDP
Heart-Beat Content	666
Heart-Beat Interval	5 (seconds)
Save ✓ Cancel ✕	

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

M2M Enabled	☒
Fail Action	Restart M2M
Device ID	666
M2M Server/Port	detran.xicp.net : 6000
Heartbeat Interval	60 (seconds)
Heartbeat Retry	10 (Range:10-1000)
Device List Report	☐
Named-Pipe Enabled	Remote Connect
Named-Pipe Server Port	8002 (Range:1024-65535)
Named-Pipe Status	Offline
Named-Pipe Address	0.0.0.0

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

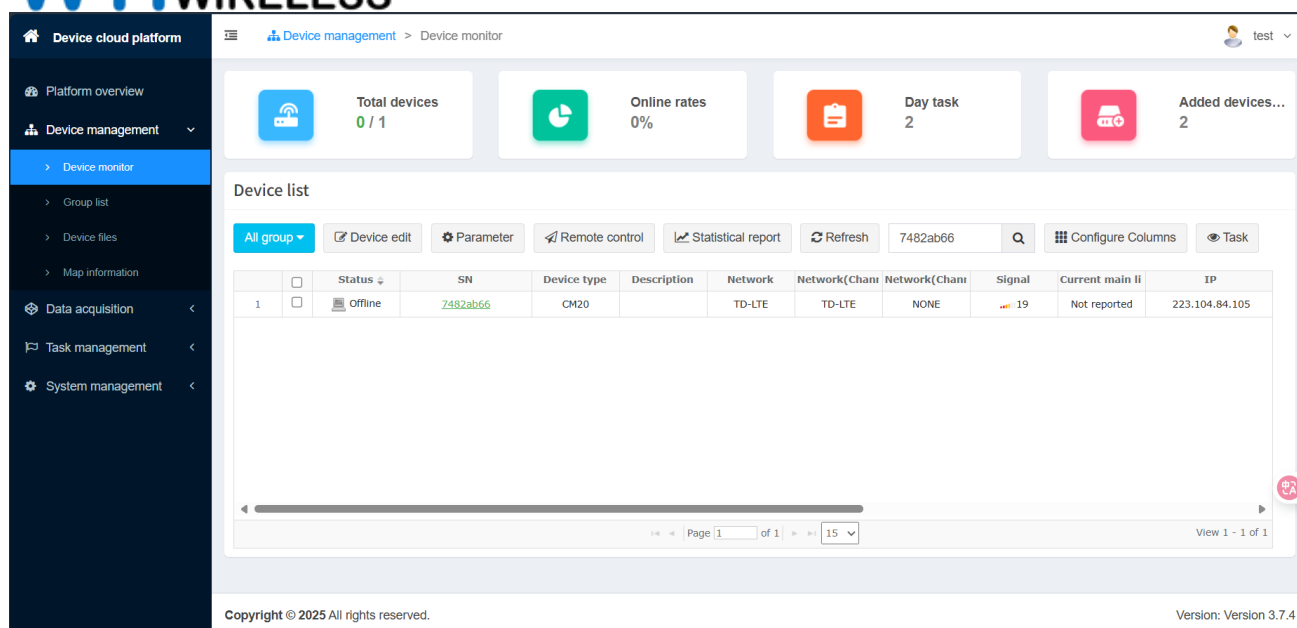


Figure 7-49

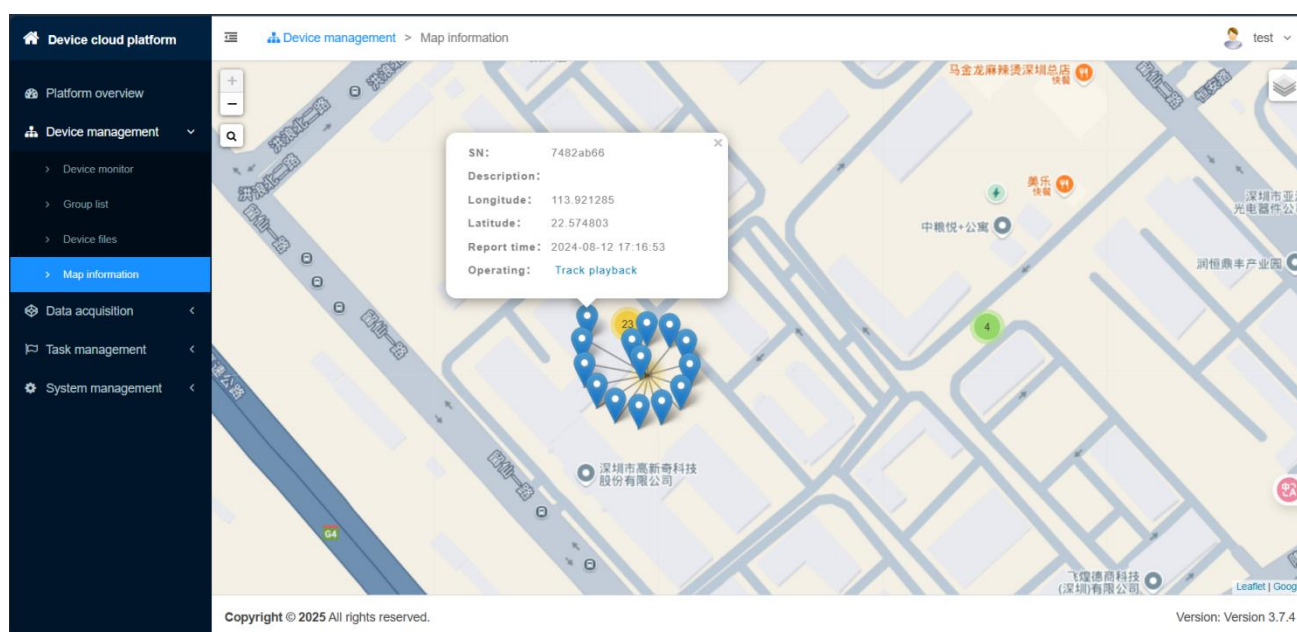


Figure 7-50 Platform device trajectory display

7.11. 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.

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

AT Over IP	
Mode	Enable
Type	UDP
Local IP	192.168.1.1
Local Port	5400
Idle Timeout	15 (seconds)

Save ✓ Cancel ✕

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.
```

7.12. 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.

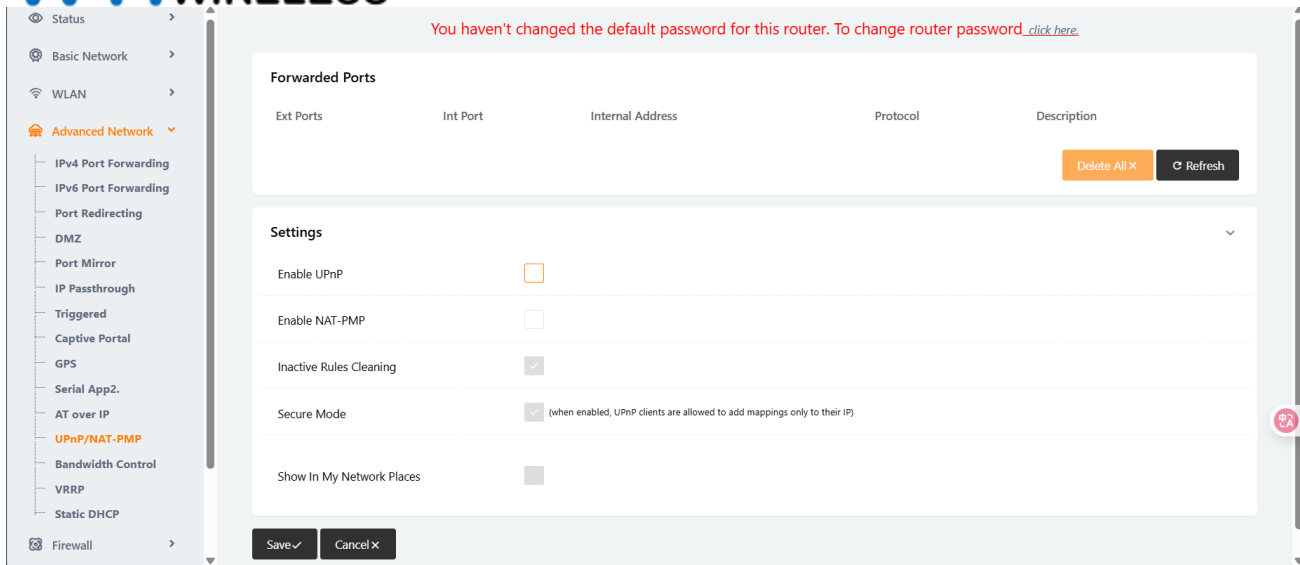


Figure 7-51

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.

7.13. 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.

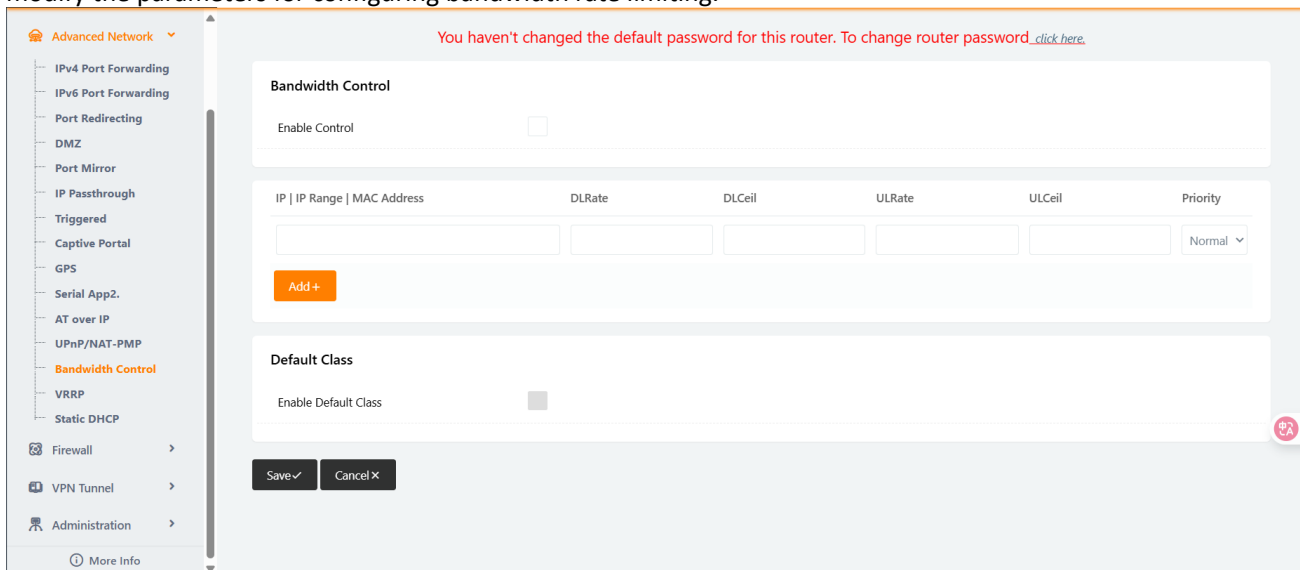


Figure 7-52

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.

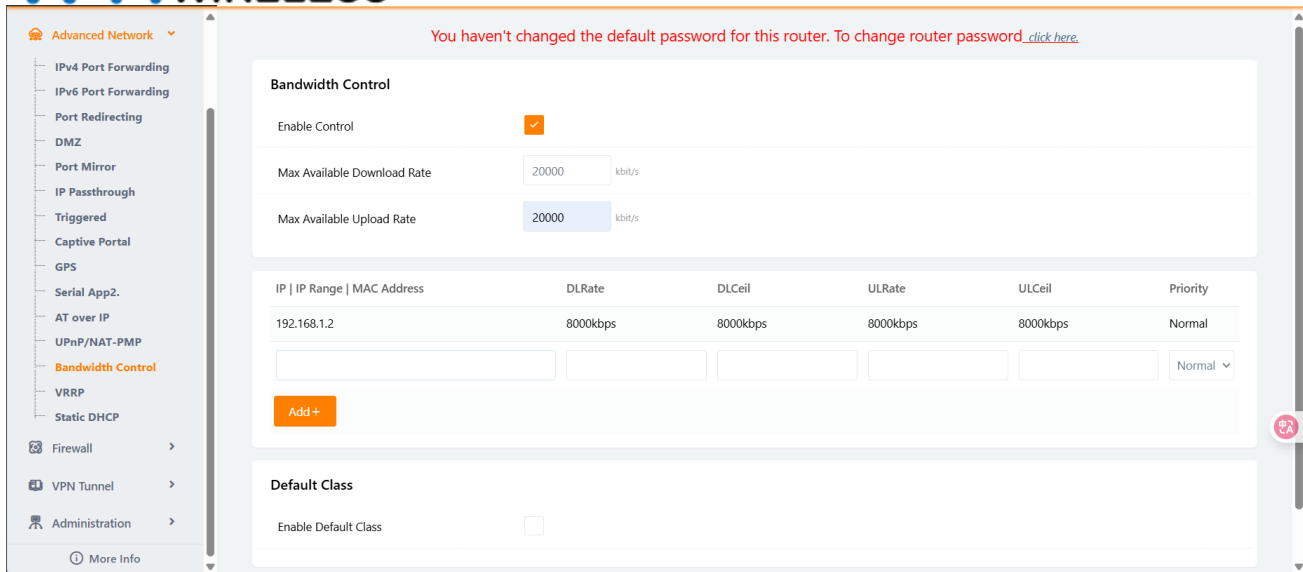


Figure 7-53 Bandwidth rate limiting configuration

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)

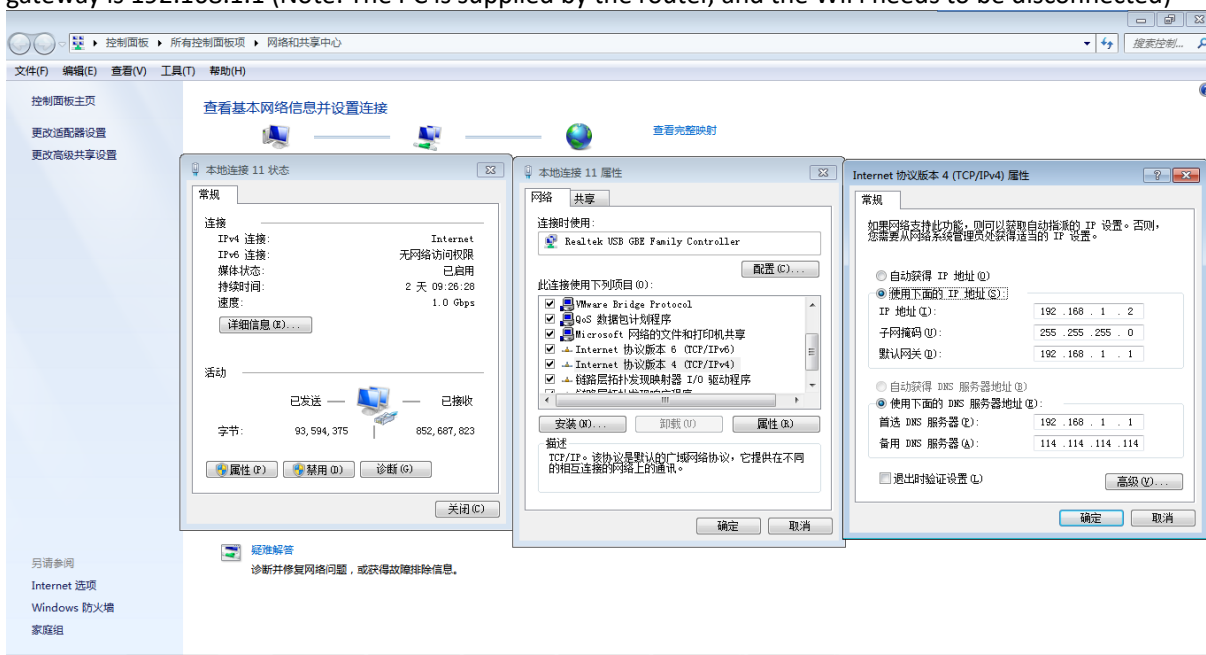


Figure 7-54 PC Local Connection Configuration

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

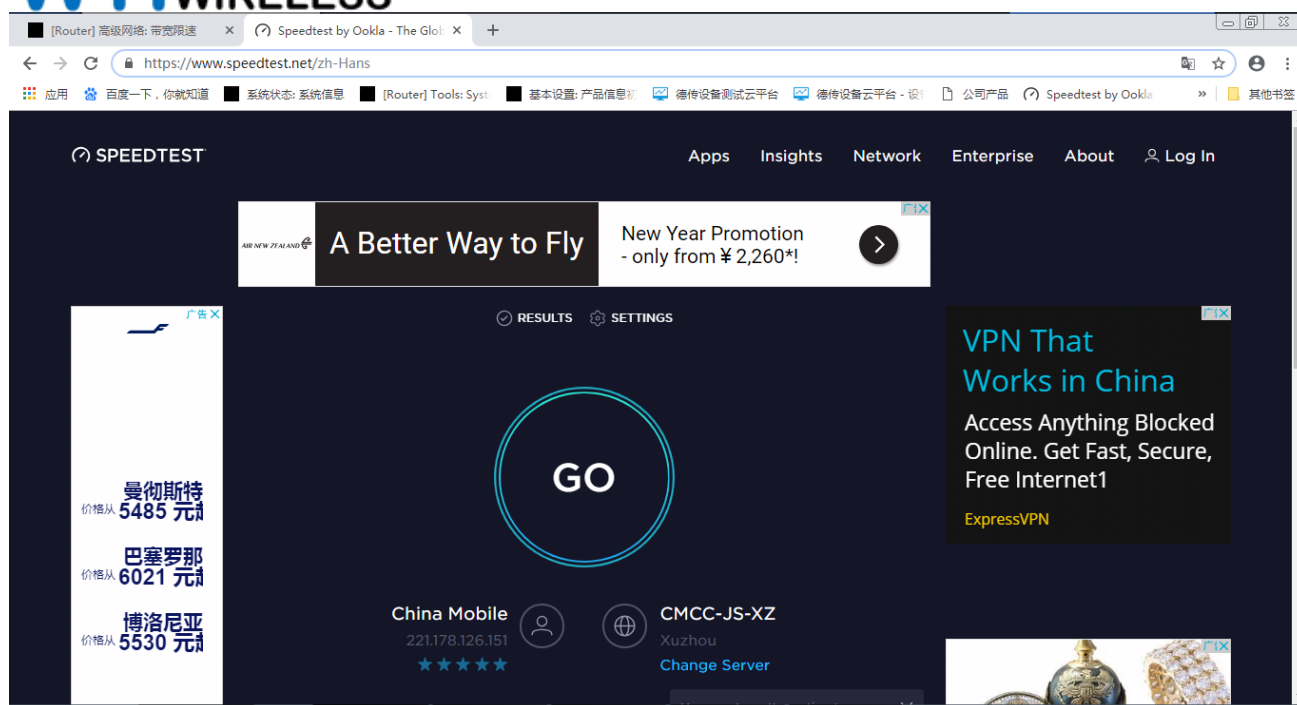


Figure 7-55

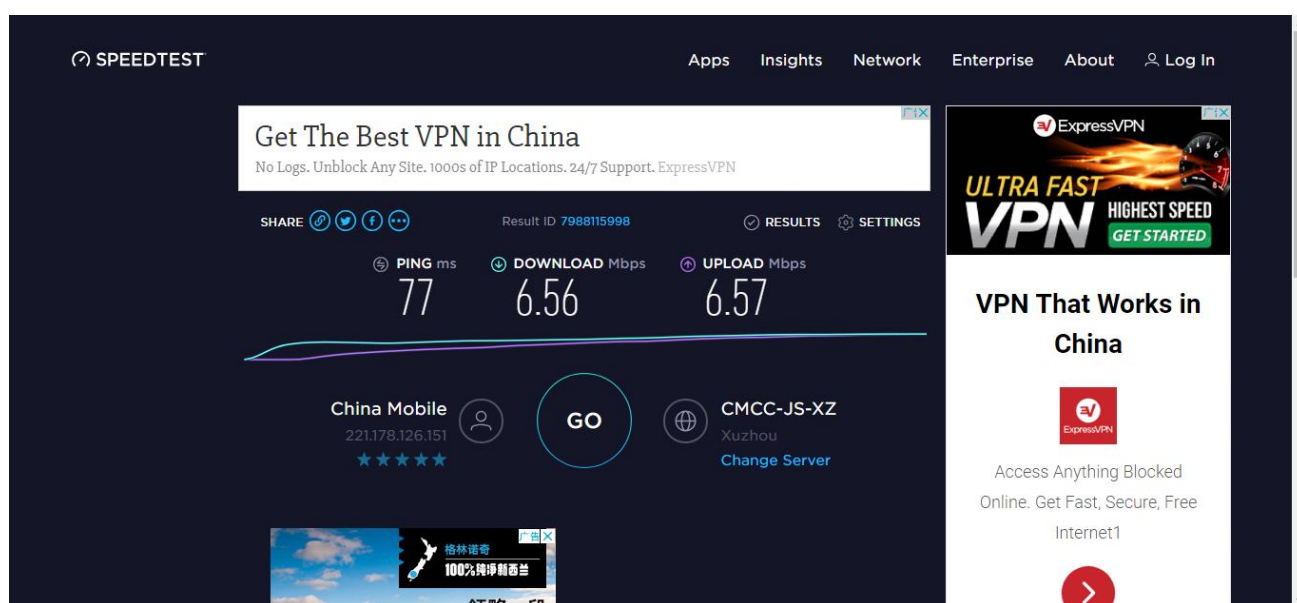


Figure 7-56 Speed test on the web interface

7.14. 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.

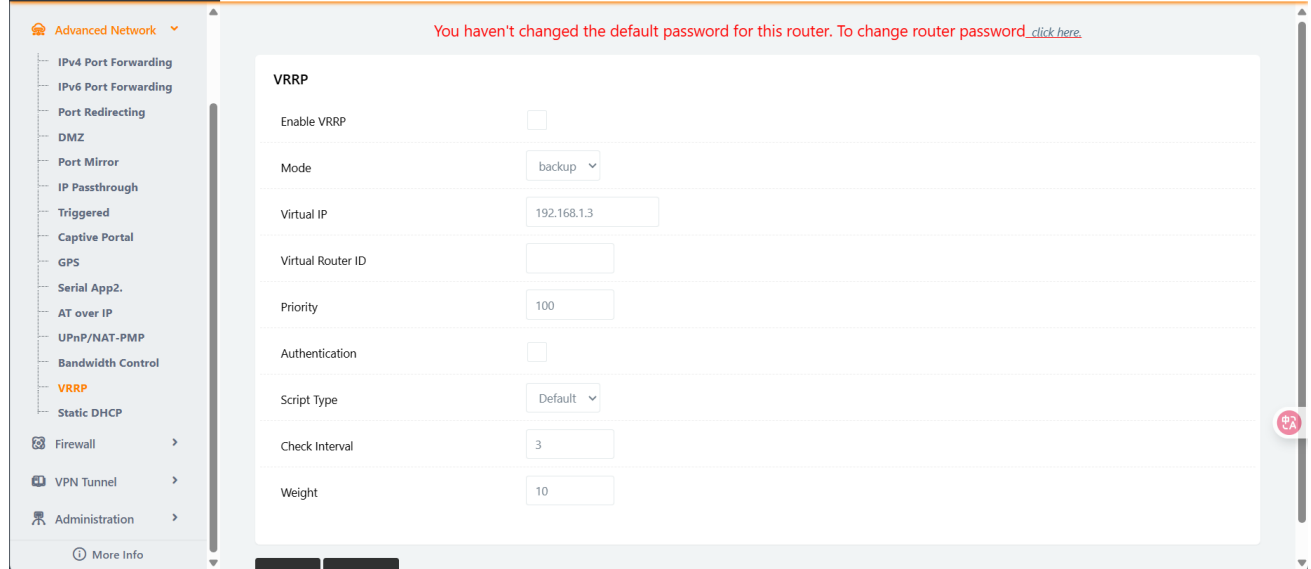


Figure 7-57

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

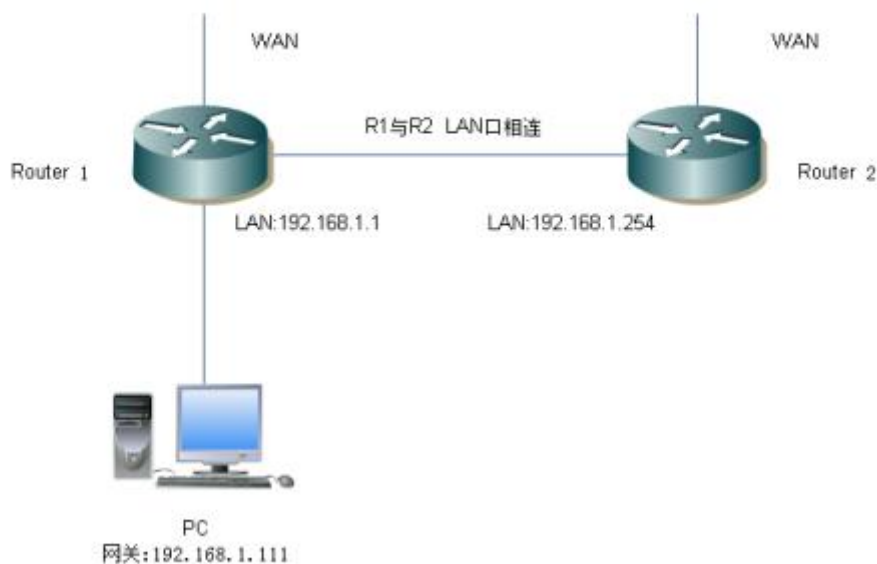


Figure 7-58 VRRP networking diagram

Primary Route Configuration (Router1).

Step 1:

LAN Configuration (Primary Routing Gateway is still 192.168.1.1)

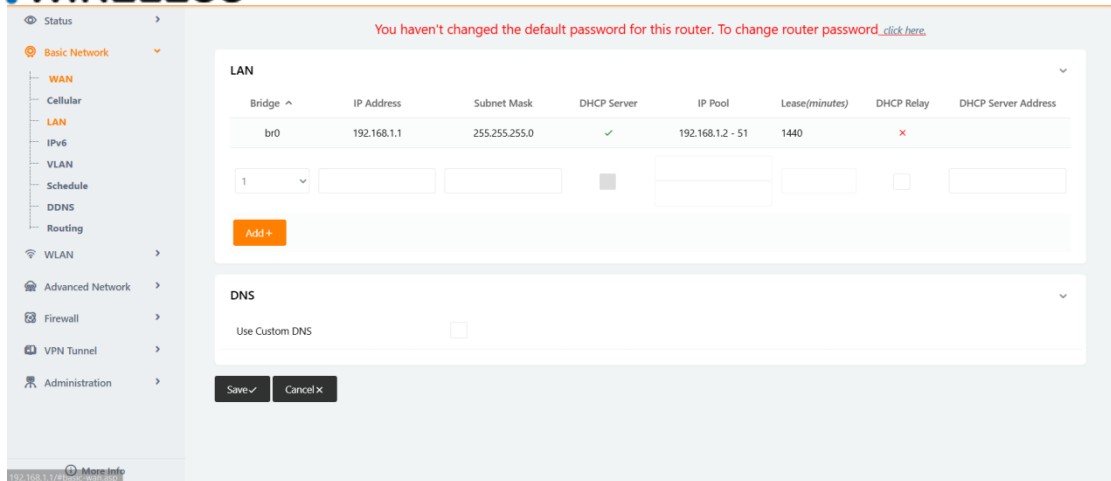


Figure 7-59 Local Area Network

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):

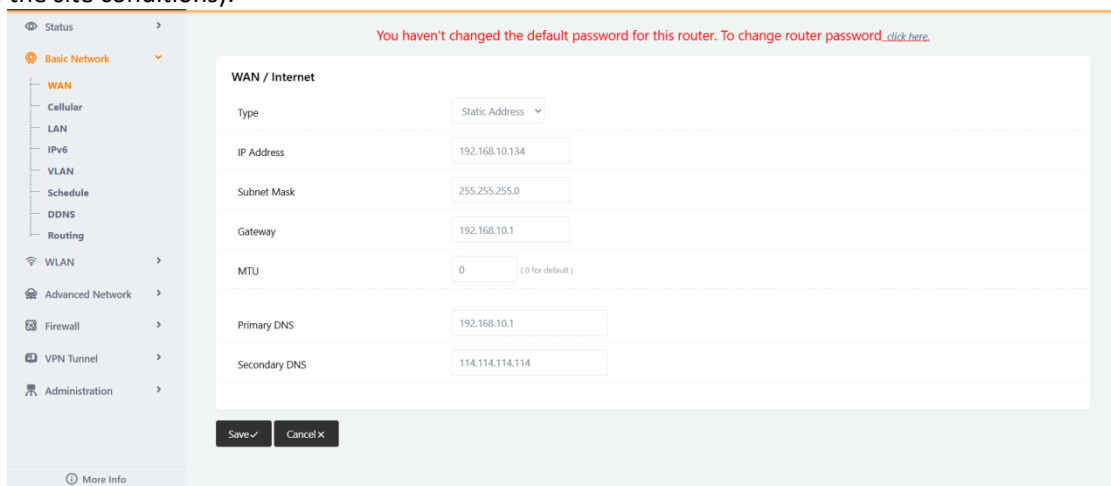


Figure 7-60 Static address settings

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

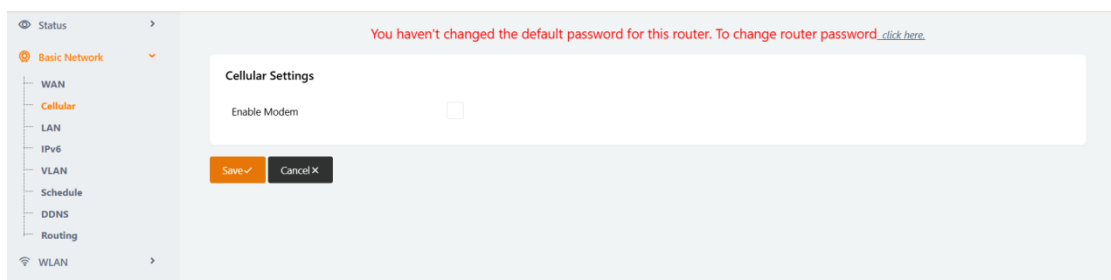


Figure 7-61 Mobile Network Settings

Step 4:

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:

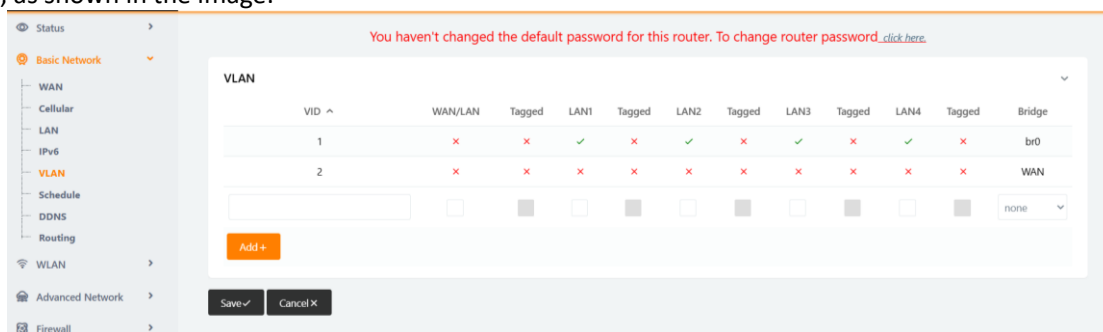


Figure 7-62 VLAN Setting

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

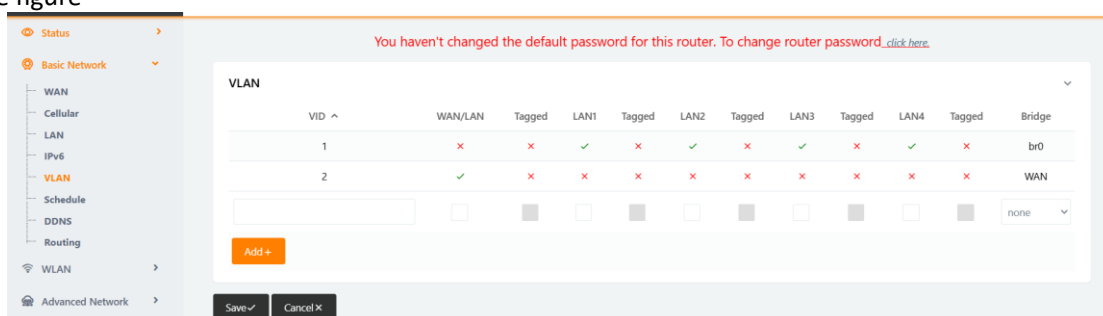


Figure 7-63 VLAN Settings

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

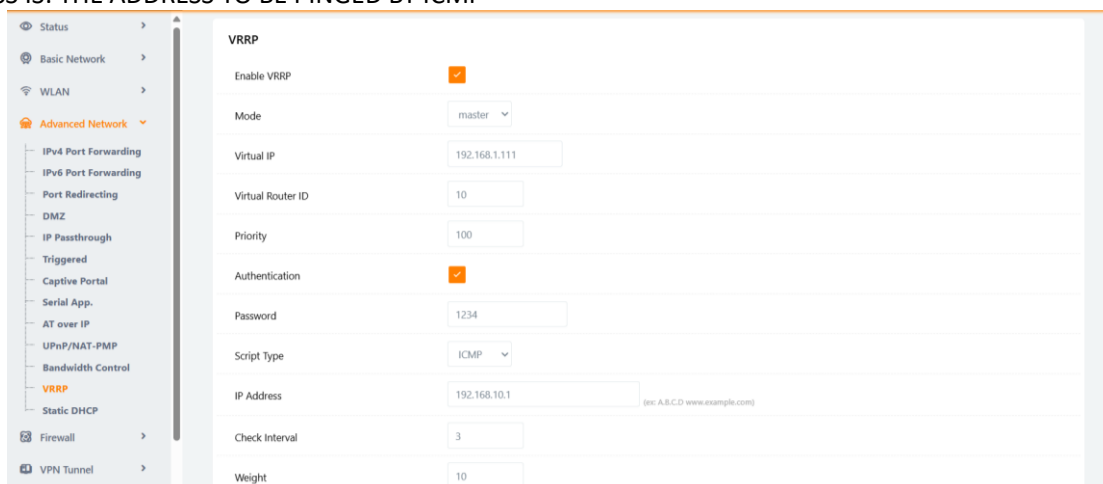


Figure 7-64 VRRP settings for the primary route

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

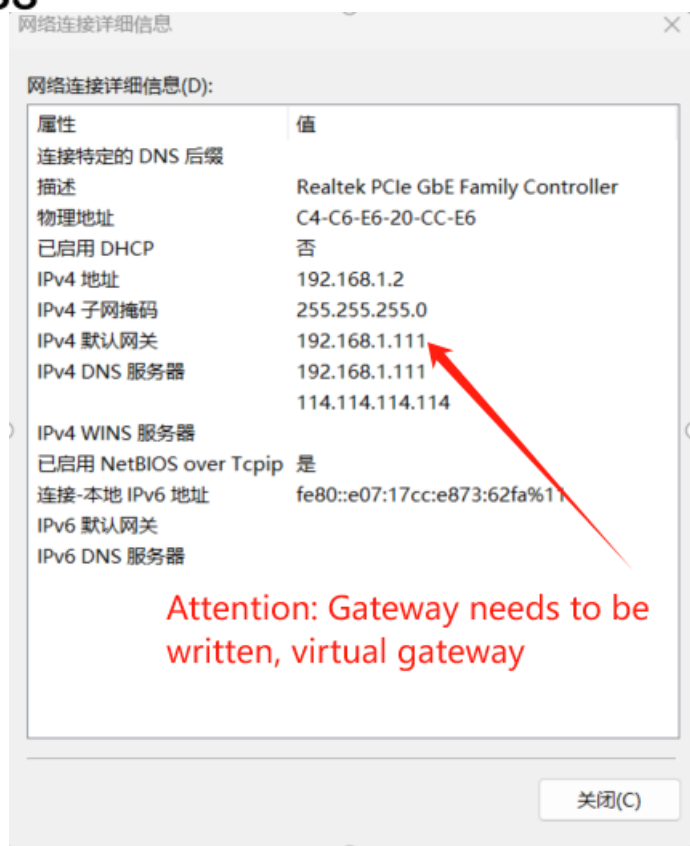


Figure 7-65 PC Local Connection Settings

Standby route configuration (Router2).

Step 1:

LAN Configuration (Changed to 192.168.1.254 for Standby Route Gateway)

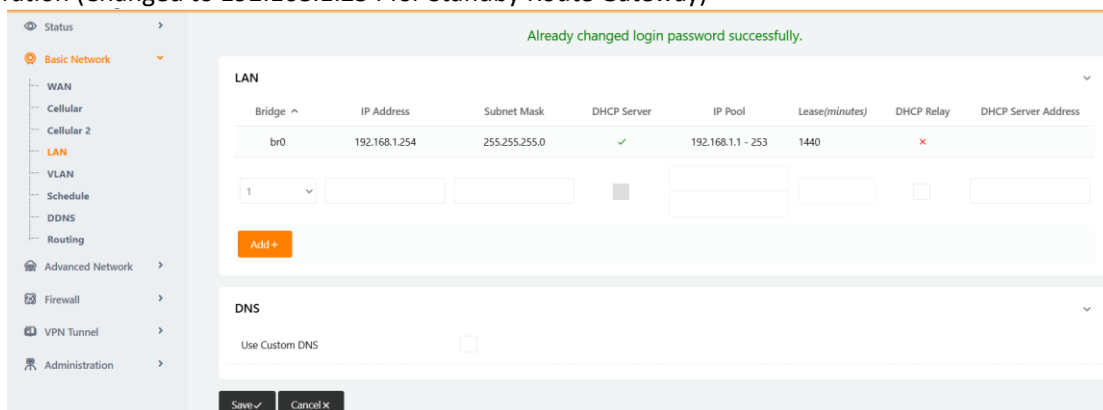


Figure 7-66 Standby LAN

Step 2:

In the navigation bar, select Basic 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):

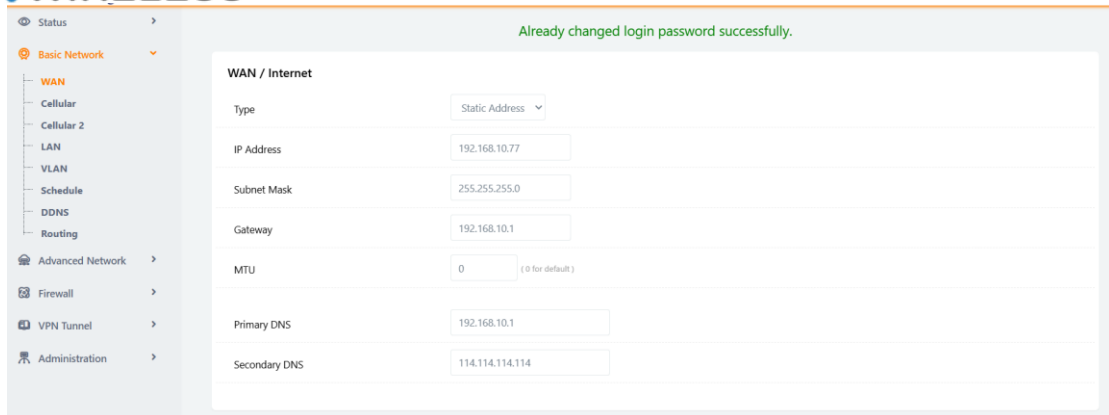


Figure 7-67 Static address settings

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

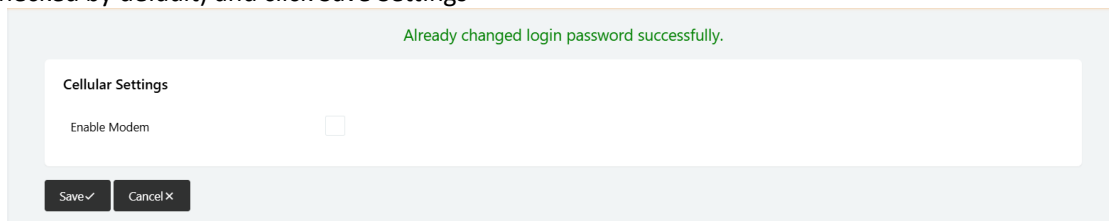
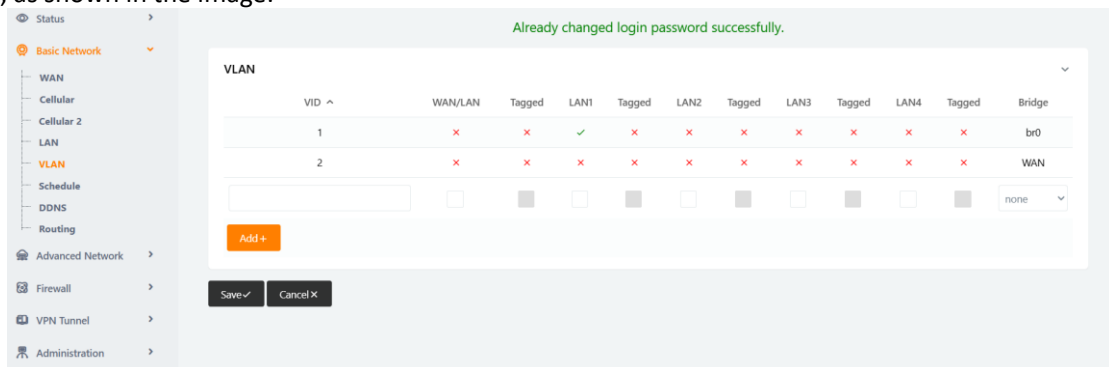


Figure 7-68 Mobile Network Setup

Step 4:

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:



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

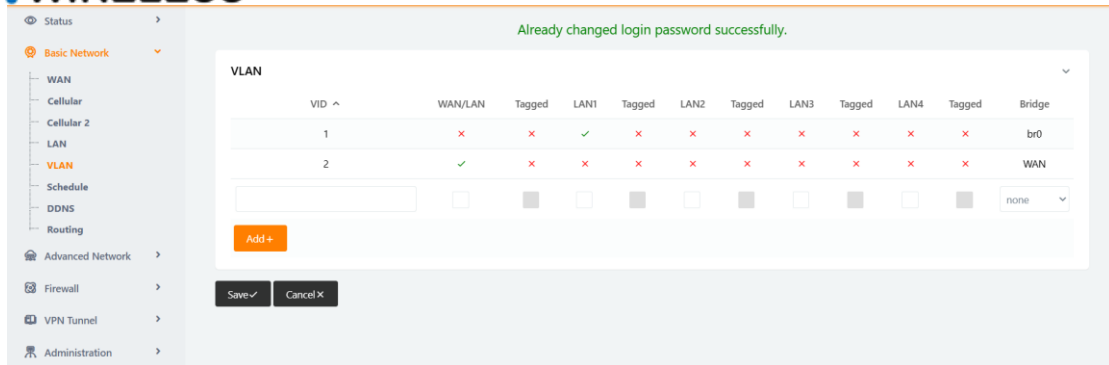


Figure 7-70 VLAN Setup

Step 5:

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

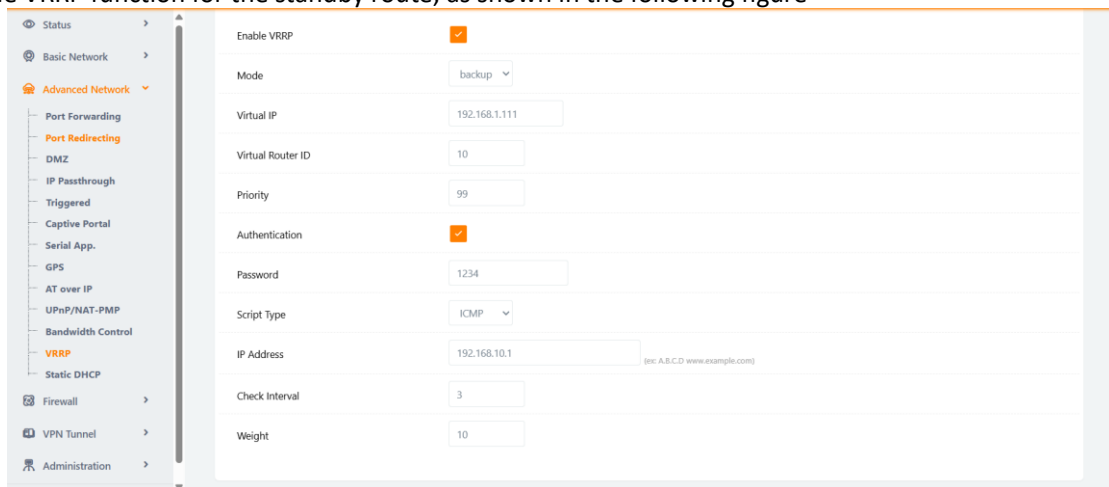


Figure 7-71 VRRP configuration of the standby route (R2).

❖ 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.

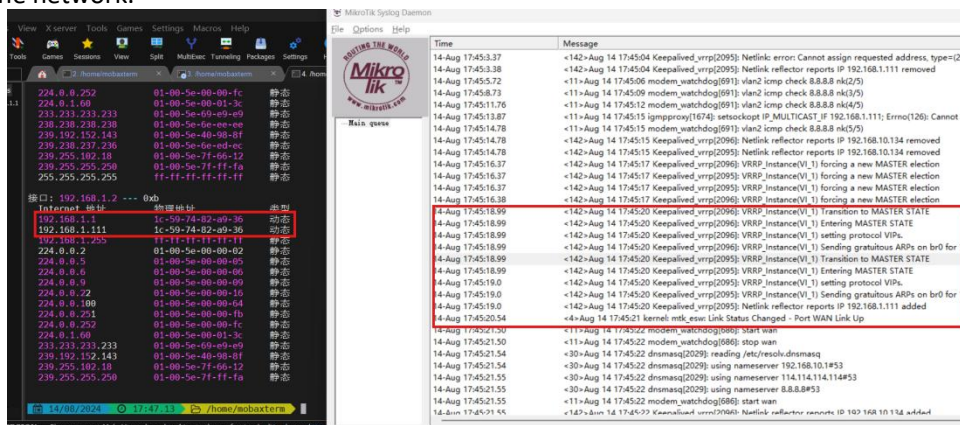


Figure 7-72: Both the primary and standby WAN ports are present

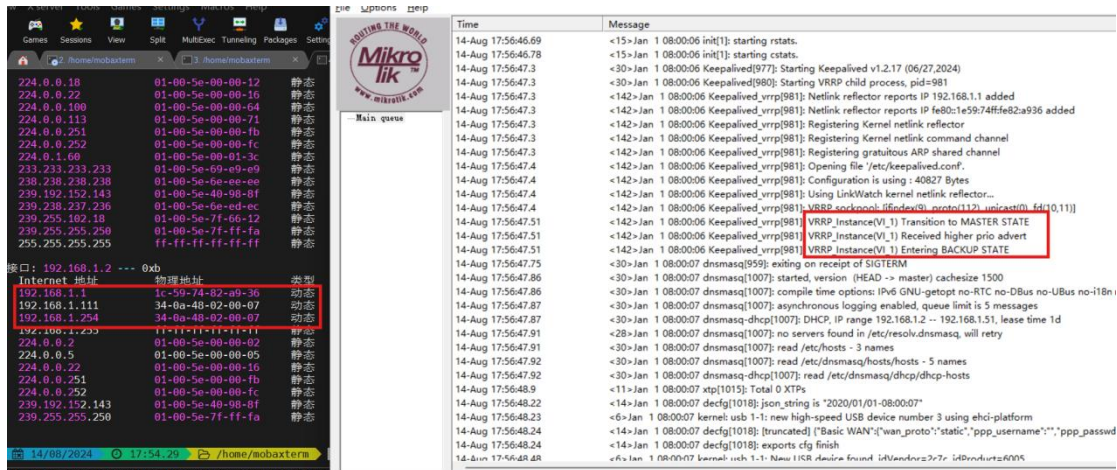


Figure 7-73: Unplug the WAN port of the primary device

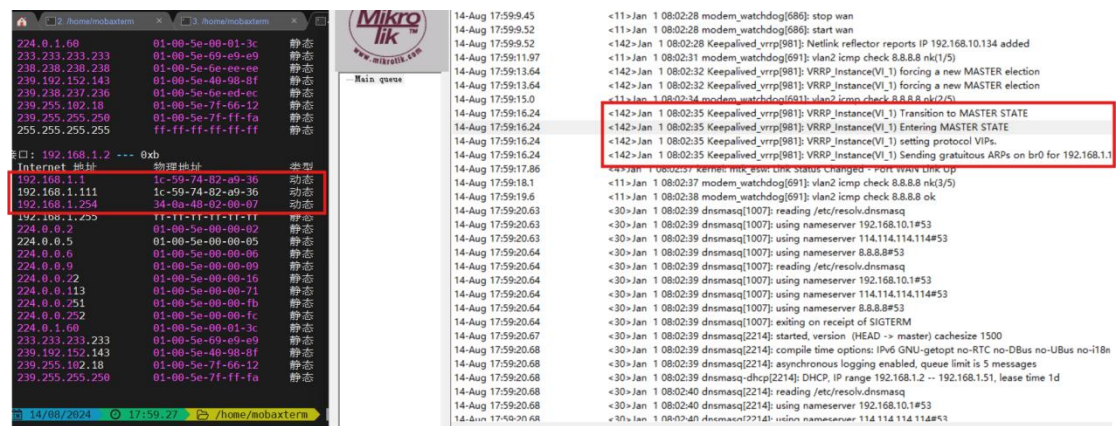


Figure 7-74 Replug the WAN port back into the main device

7.15. 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.

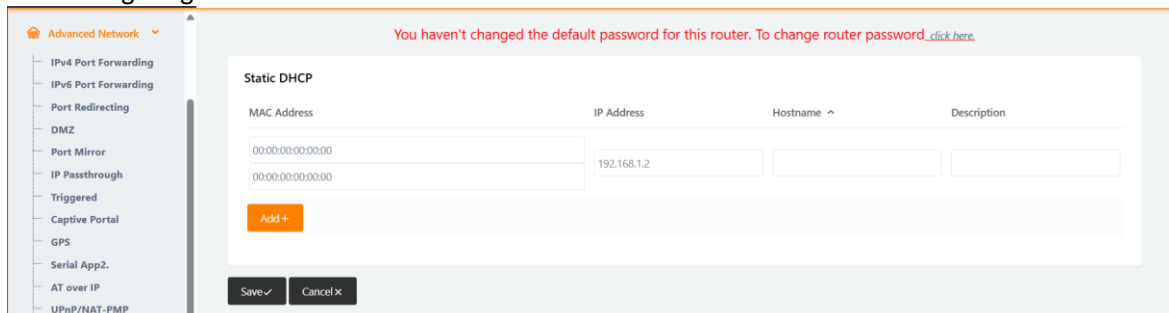


Figure 7-75

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

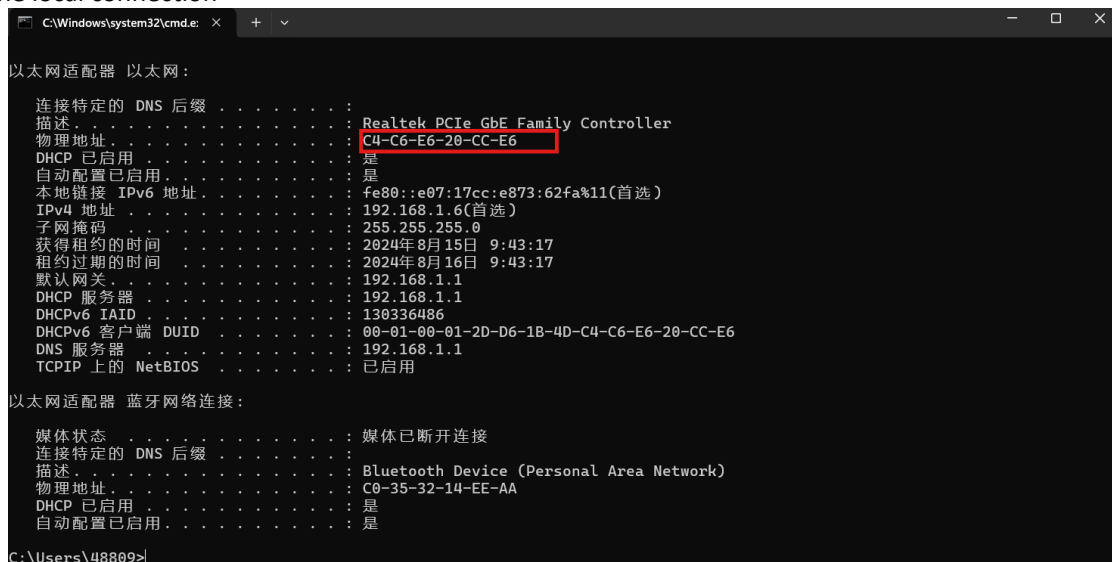
Table 7-6 DHCP Server Settings

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



```

C:\Windows\system32\cmd.e: x  +  v
以太网适配器 以太网:

    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Realtek PCIe GbE Family Controller
    物理地址. . . . . : C4-C6-E6-20-CC-E6
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::e07:17cc:e873:62fa%11(首选)
    IPv4 地址 . . . . . : 192.168.1.6(首选)
    子网掩码 . . . . . : 255.255.255.0
    获得租约的时间 . . . . . : 2024年8月15日 9:43:17
    租约过期的时间 . . . . . : 2024年8月16日 9:43:17
    默认网关. . . . . : 192.168.1.1
    DHCP 服务器 . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 130336486
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2D-D6-1B-4D-C4-C6-E6-20-CC-E6
    DNS 服务器 . . . . . : 192.168.1.1
    TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 蓝牙网络连接:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Bluetooth Device (Personal Area Network)
    物理地址. . . . . : C0-35-32-14-EE-AA
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是

C:\Users\48809>
  
```

Figure 7-76 Administrator

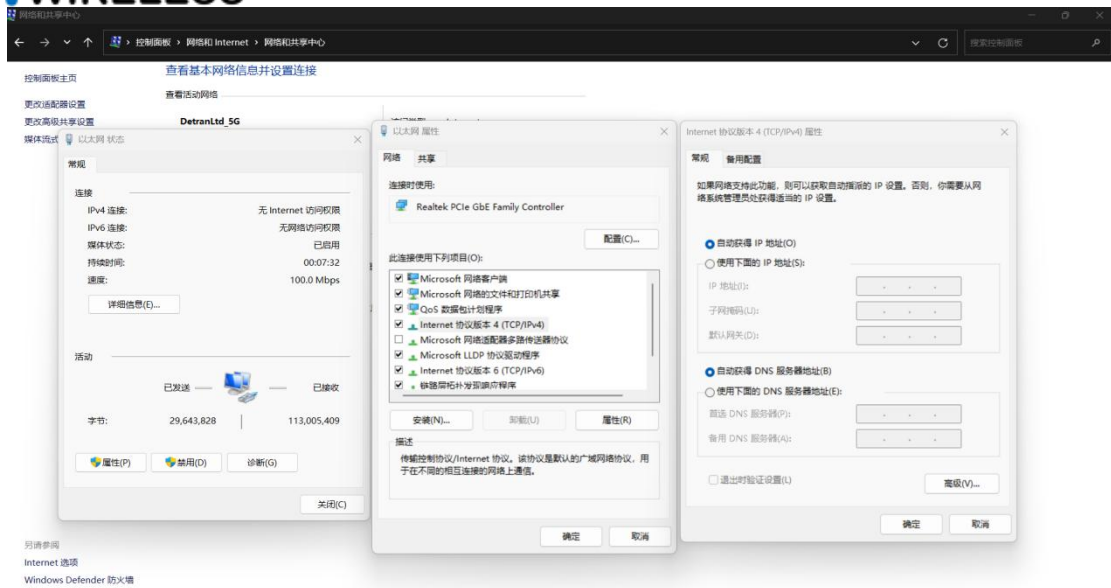


Figure 7-77 Automatic DHCP is enabled on the PC

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

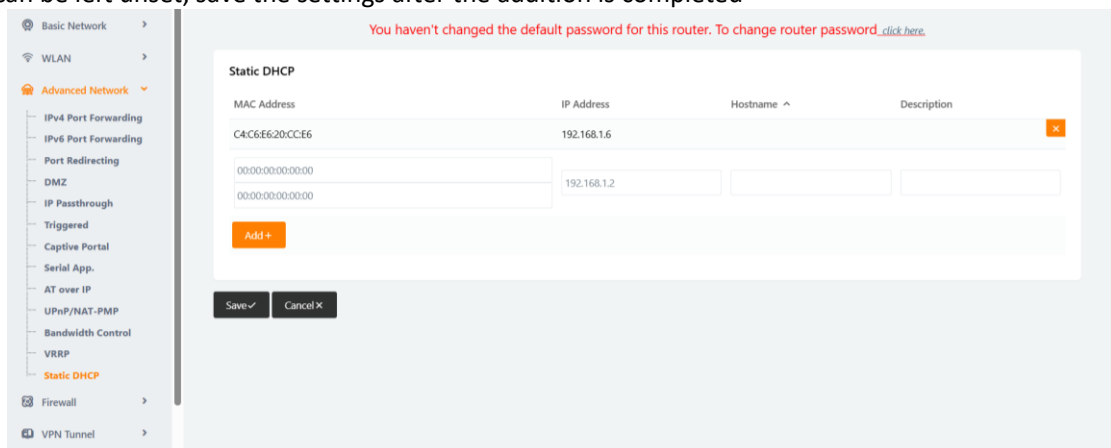


Figure 7-78 Static DHCP settings

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 unknown: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 unknown: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 unknown:0
  TX packets:133974 dropped:0 errors:148 txqueuelen:0
  
```

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.

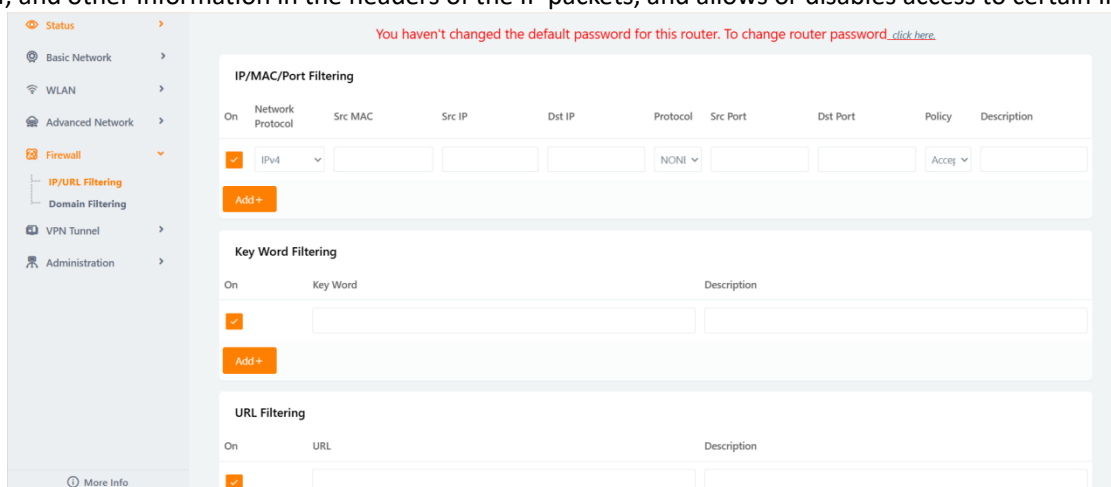
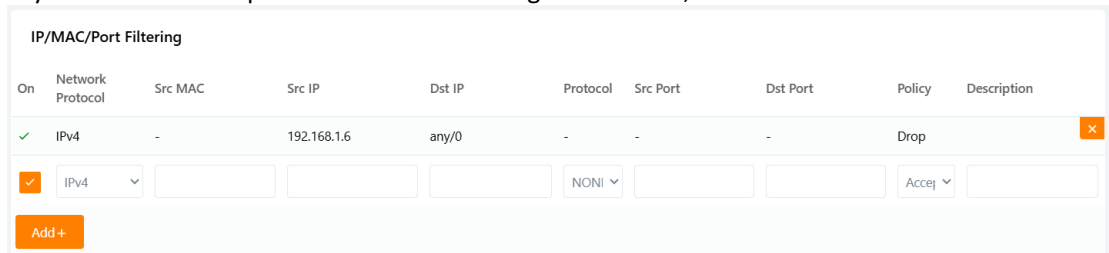


Figure 8-1

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

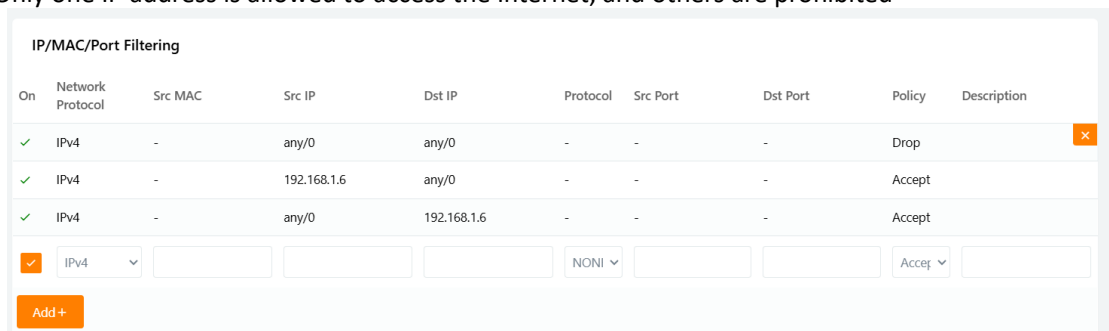


The screenshot shows the 'IP/MAC/Port Filtering' configuration window. It has a table with columns: On, Network Protocol, Src MAC, Src IP, Dst IP, Protocol, Src Port, Dst Port, Policy, and Description. A single rule is configured with 'On' checked, 'Network Protocol' set to 'IPv4', 'Src IP' set to '192.168.1.6', 'Dst IP' set to 'any/0', and 'Policy' set to 'Drop'. Below the table, there are input fields for adding a new rule, including a checked 'On' checkbox, 'IPv4' protocol, and empty fields for Src MAC, Src IP, Dst IP, Protocol (set to 'NONI'), Src Port, Dst Port, Policy (set to 'Accept'), and Description.

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



The screenshot shows the 'IP/MAC/Port Filtering' configuration window with three rules. The first rule has 'On' checked, 'Network Protocol' set to 'IPv4', 'Src IP' set to 'any/0', 'Dst IP' set to 'any/0', and 'Policy' set to 'Drop'. The second rule has 'On' checked, 'Network Protocol' set to 'IPv4', 'Src IP' set to '192.168.1.6', 'Dst IP' set to 'any/0', and 'Policy' set to 'Accept'. The third rule has 'On' checked, 'Network Protocol' set to 'IPv4', 'Src IP' set to 'any/0', 'Dst IP' set to '192.168.1.6', and 'Policy' set to 'Accept'. Below the table, there are input fields for adding a new rule, including a checked 'On' checkbox, 'IPv4' protocol, and empty fields for Src MAC, Src IP, Dst IP, Protocol (set to 'NONI'), Src Port, Dst Port, Policy (set to 'Accept'), and Description.

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

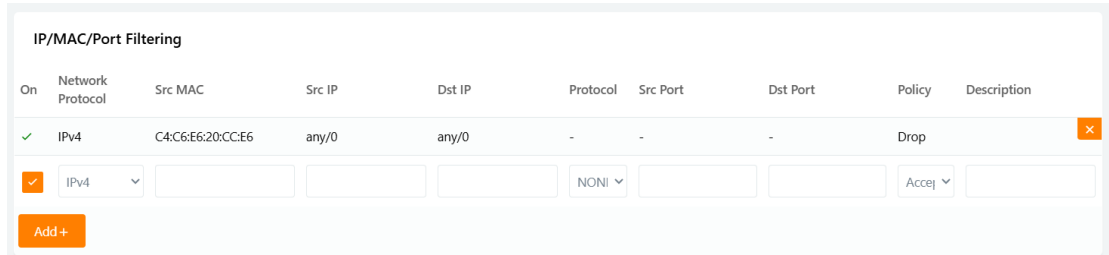
For example: 192.168.10.70

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



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

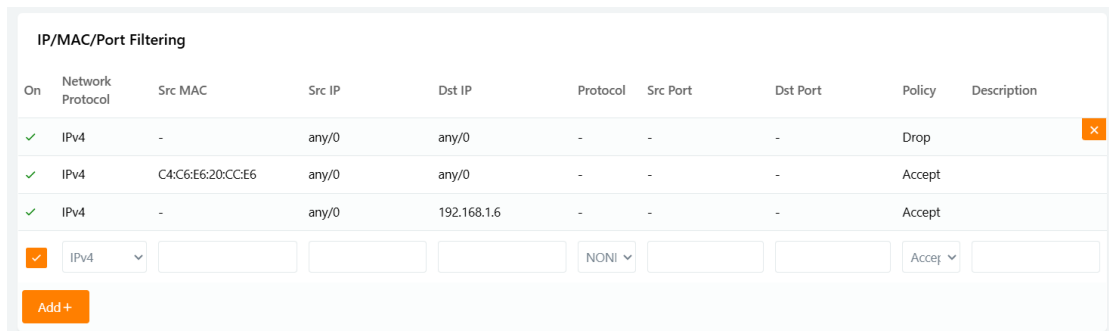
 Acce

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



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

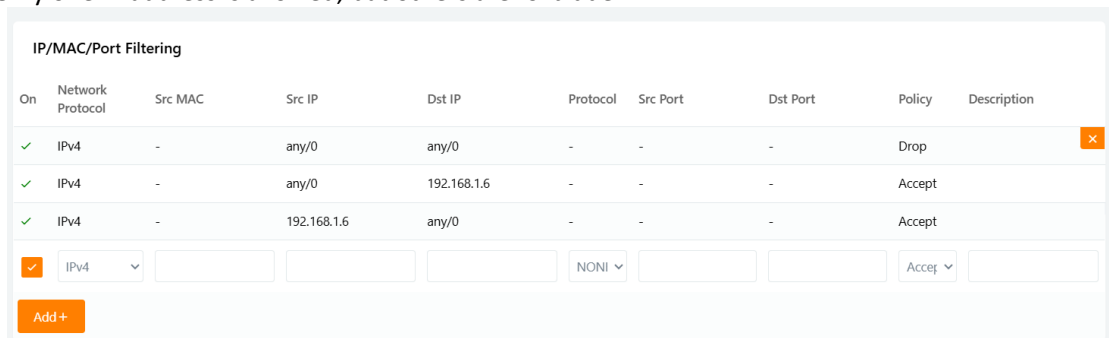
 Acce

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
✓	IPv4	-	any/0	any/0	-	-	-	Drop	
✓	IPv4	-	any/0	192.168.1.6	-	-	-	Accept	
✓	IPv4	-	192.168.1.6	any/0	-	-	-	Accept	

☒ IPv4

 NONI

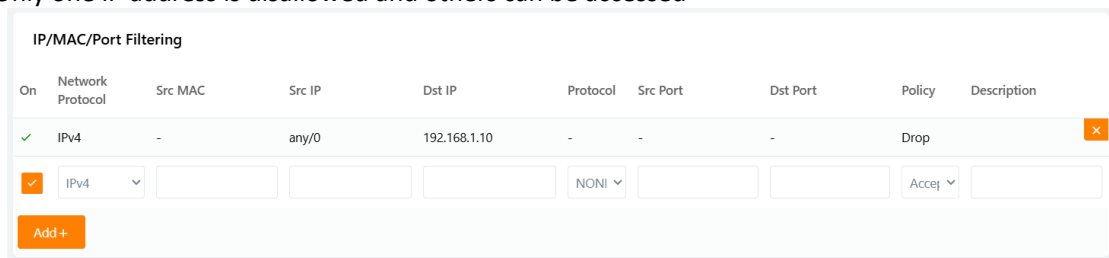
 Acce

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
☒	IPv4	-	any/0	192.168.1.10	-	-	-	Drop	
☒	IPv4				NONE			Accept	

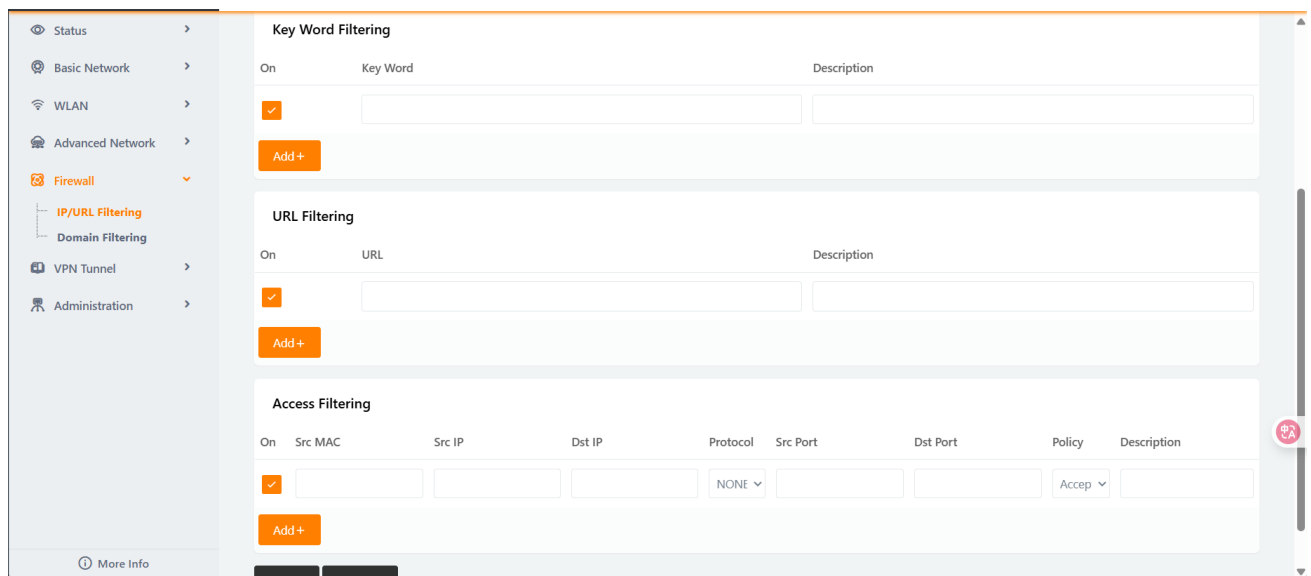
Add +

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.

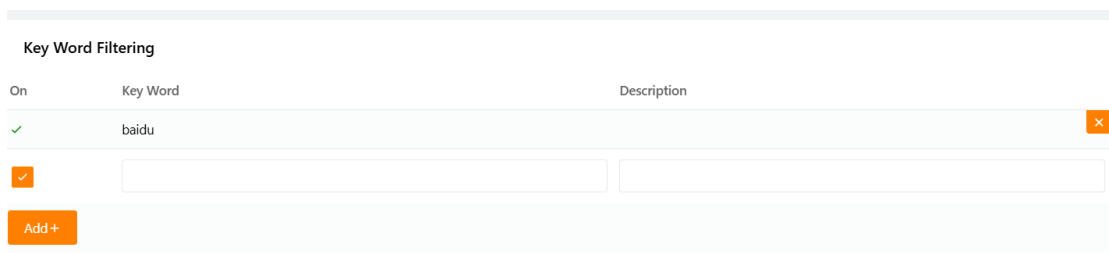


The screenshot shows the Firewall configuration page with a sidebar on the left containing links to Status, Basic Network, WLAN, Advanced Network, Firewall (selected), IP/URL Filtering, Domain Filtering, VPN Tunnel, and Administration. The main content area has three sections:

- Key Word Filtering:** A table with columns 'On', 'Key Word', and 'Description'. It contains one entry with 'On' checked and an 'Add +' button below.
- URL Filtering:** A table with columns 'On', 'URL', and 'Description'. It contains one entry with 'On' checked and an 'Add +' button below.
- Access Filtering:** A table with columns 'On', 'Src MAC', 'Src IP', 'Dst IP', 'Protocol', 'Src Port', 'Dst Port', 'Policy', and 'Description'. It contains one entry with 'On' checked, 'Protocol' set to 'NONE', and 'Policy' set to 'Accept'. There is an 'Add +' button below.

Figure 8-8

Example 1:



On	Key Word	Description
☒	baidu	
☒		

Add +

Figure 8-9

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

Figure 8–10

Example 3:

Only certain IPs are allowed to access the device;

Figure 8–11

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

<https://www.wtiwireless.com/>