



# **SLK-R680 Series**

**Industrial 5G CPE With Wifi6  
User Manual**

## catalog

Chapter 1 login .....	4
1.1 Prepare before logging in .....	4
1.2 Login configuration page .....	6
Chapter 2 Network Setting .....	7
2.1 Change the login page address .....	7
2.2 5G Modem .....	8
2.3 WAN Setting .....	9
2.3.1 DHCP address .....	9
2.3.2 PPPoE .....	10
2.3.3 Static address .....	10
2.3.4 As lan (convert WAN port to LAN port) .....	11
2.3.5 Advanced Configuration .....	11
2.4 DHCP Setting .....	11
2.5 Hostnames .....	12
2.6 WIFI Access Point .....	12
2.7 WIFI Client(Bridge) .....	13
2.8 WIFI repeater .....	15
2.8.1 Change the local IP address .....	15
2.8.2 Connect to the main wireless AP .....	15
2.8.3 Disable DHCP .....	16
2.9 Time Reboot .....	16
2.10 Network Backup .....	17
2.11 Watchcat .....	17
2.12 Diagnosis .....	19
Chapter 3 Serial port configuration .....	20
3.1 Use Tools And Preparation .....	20
3.2 TCP Server .....	21
3.3 TCP Client .....	22
3.4 UDP Server .....	24
3.5 UDP Client .....	25
3.6 Modbus TCP .....	27
3.7 Transport Proto .....	30
Chapter 4 Firewall and Application .....	32
4.1 Firewall on and off .....	32
4.2 DMZ .....	32
4.3 Prot Forwards .....	33
4.4 Black/White List .....	35
4.4.1 White List .....	35
4.4.2 Black List .....	36
Chapter 5 Service Manage .....	38
5.1 Remote management - CWMP .....	38

5.2 Remote management - SNMP .....	39
5.3 Frp Client .....	39
5.3.1 Connect to Frps .....	40
5.3.2 Add TCP proxy protocol .....	42
5.3.3 Add STCP Proxy Rules .....	44
5.3.4 Add UDP Proxy Rules .....	48
5.3.5 Add HTTP Proxy Rules .....	50
Chapter 6 VPN Service .....	52
6.1 PPTP VPN .....	52
6.2 L2TP VPN .....	52
6.3 GRE VPN .....	53
6.4 OpenVPN .....	54
6.5 WireGuard VPN .....	55
6.6 Remote management - P2P VPN .....	56
Chapter 7 System .....	57
7.1 Date Time .....	57
7.2 Language Setting .....	57
7.3 Modify Password .....	58
7.4 Update Firmware .....	58
7.5 Backup/Restore .....	58
7.6 Factory Reset .....	59
7.7 Reboot .....	60
7.8 page log out .....	60

# Chapter 1 login

## 1.1 Prepare before logging in

After completing the hardware installation, you will need to ensure that the management computer has an Ethernet card installed before logging into the router's web setup page. Please set the management PC to "Obtain an IP address automatically" and "Obtain DNS server address automatically" (the default configuration of the computer system), and the device will automatically assign an IP address to the management PC.

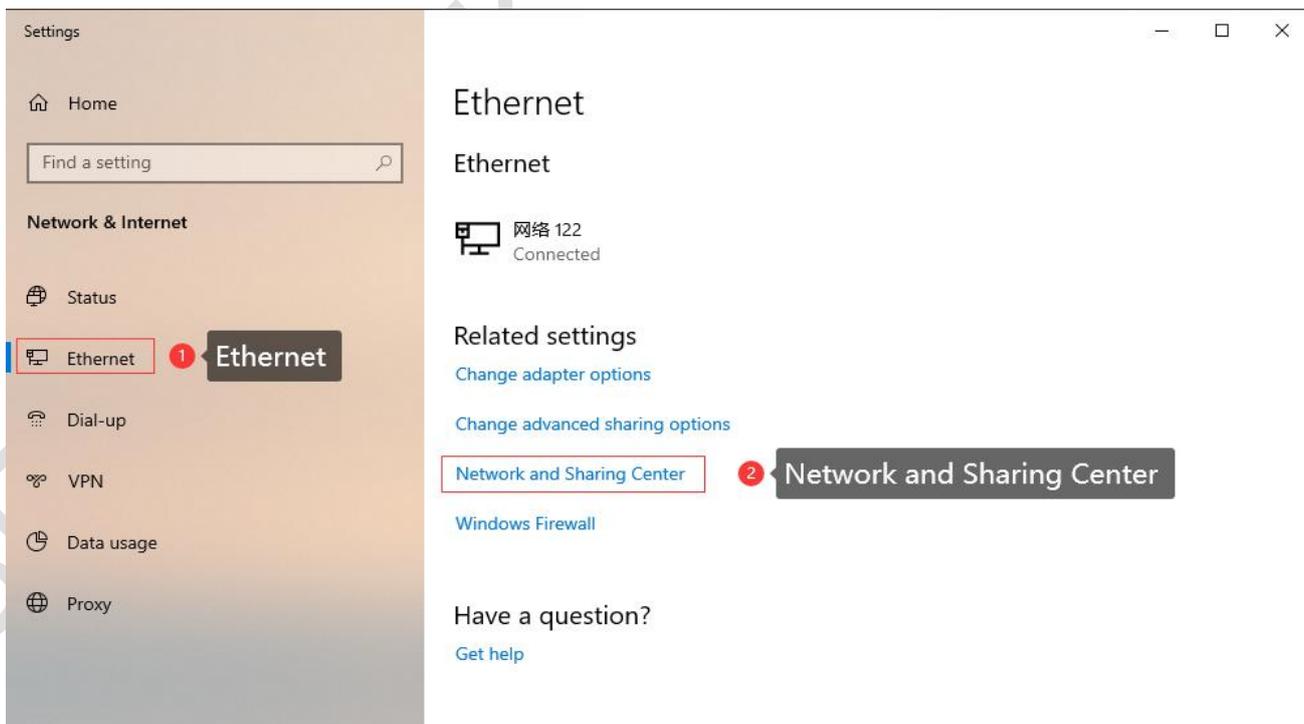
Set the IP address of the management PC (for example: 192.168.2.59) and the IP address of the device's LAN port in the same network segment(The initial IP address of the LAN port of the device is: 192.168.2.1, and the subnet mask is 255.255.255.0) The method is as follows.

Take win10 as an example, the operation is as follows:

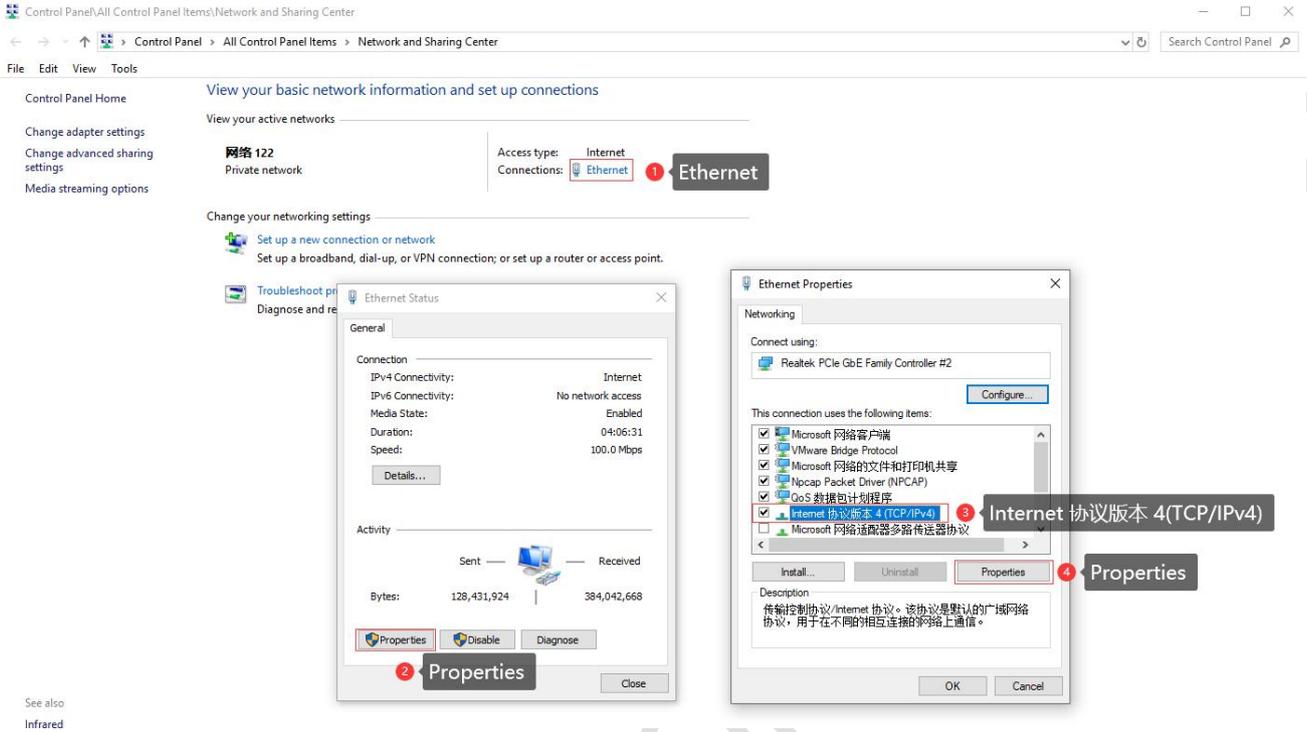
Step 1: Right-click the network logo in the lower right corner of the desktop (as shown in the figure), and choose to Open Network & Internet settings.



Step 2: First click on "Ethernet", then click on "Network and Sharing Center".



**Step 3: Click Ethernet with the mouse, click Properties in the pop-up box (Ethernet status), select Internet Protocol version 4 (TCP/IPv4) in the pop-up box (Ethernet properties), and click Properties**

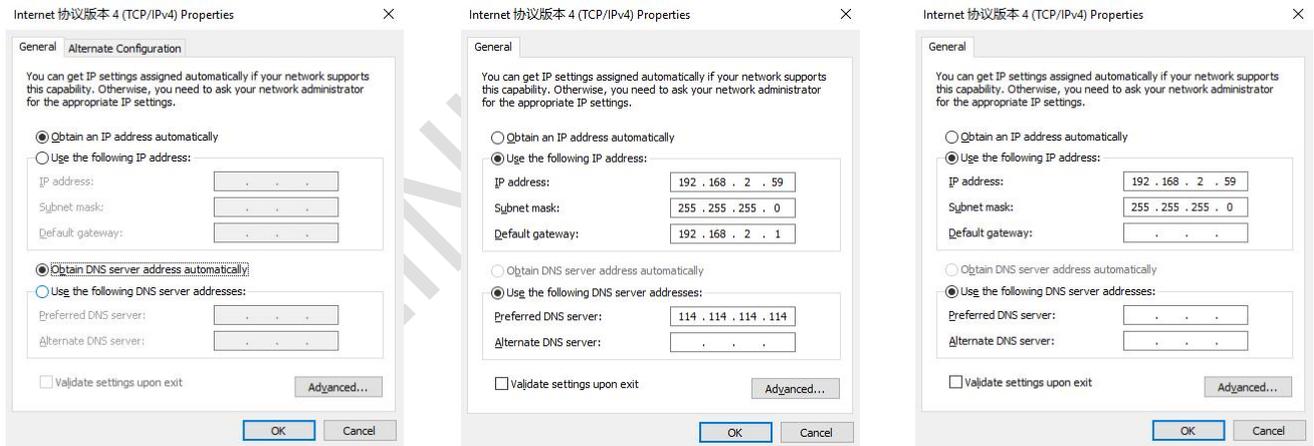


**Step 4: There are three setting methods**

**method 1**

**method 2**

**method 3**

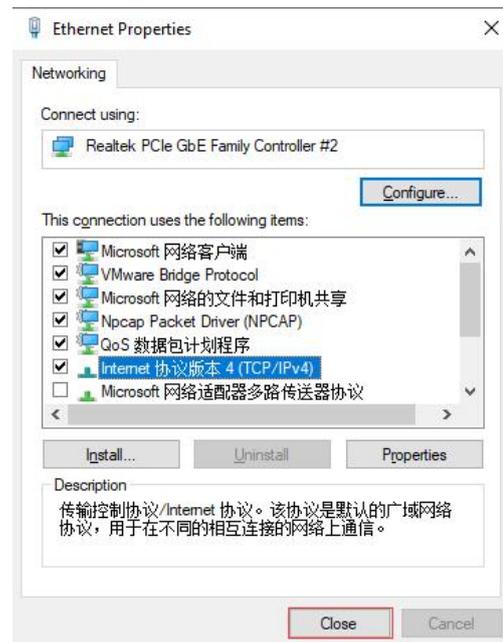
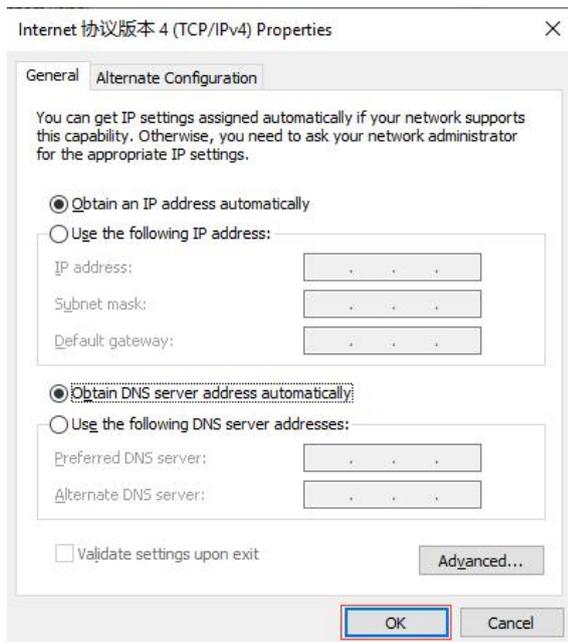


**method 1:** It can be used to configure the device and access the external network. It is recommended to use it (Note: If there are multiple routes with different network segments in the current environment, the IP obtained by the computer may not be able to connect to the device. In this case, method 2 can be used);

**method 2:** It can be used to configure the device and access the external network. The IP address is set to the device IP (the device defaults to 192.168.2.1) and the same network segment IP: 192.168.2.X (X is any number between 2 and 254, such as 192.168.2.2) , the default gateway is set to device IP: 192.168.2.1, DNS can be set to 8.8.8.8 and other general DNS;

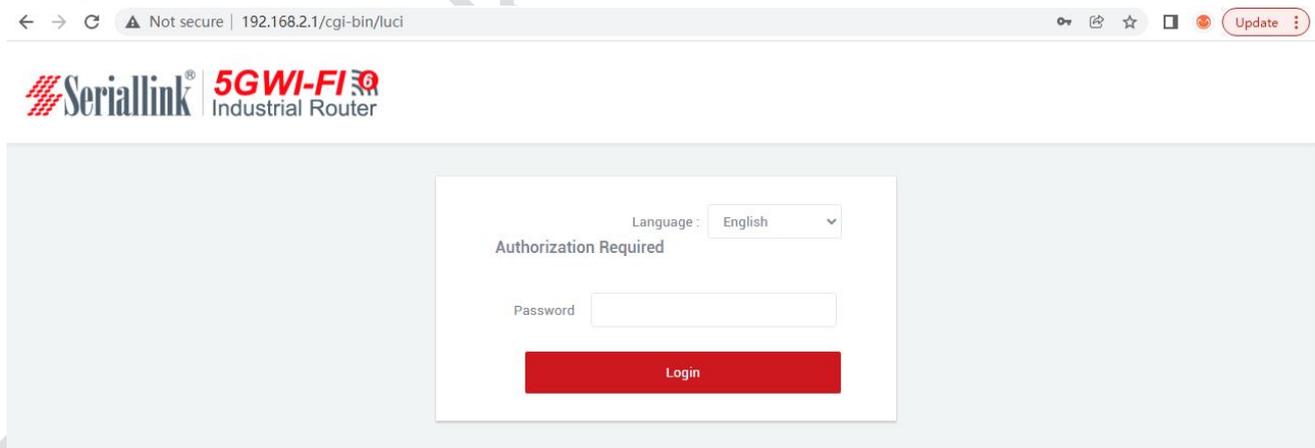
**method 3:** Only connect the device for configuration use, the computer cannot access the external network through the device network, and the IP address is set as in method 2;

Step 5: Click OK with the mouse, and then click Close to save the changes in Steps 3 and 4;



## 1.2 Login configuration page

Open IE or other browsers, enter 192.168.2.1 in the address bar, after the connection is established, in the pop-up login interface, log in as the system administrator (admin), that is, enter the password in the login interface (the default password is set to admin).



The default login password is admin. If the user needs to protect the configuration interface to avoid being modified by others, he can modify the login password, click "System" - "Modify Password" in turn, then fill in the password to be modified, and then "SAVE & APPLY", please refer to Chapter 5.3 for details.

## Chapter 2 Network Setting

### 2.1 Change the login page address

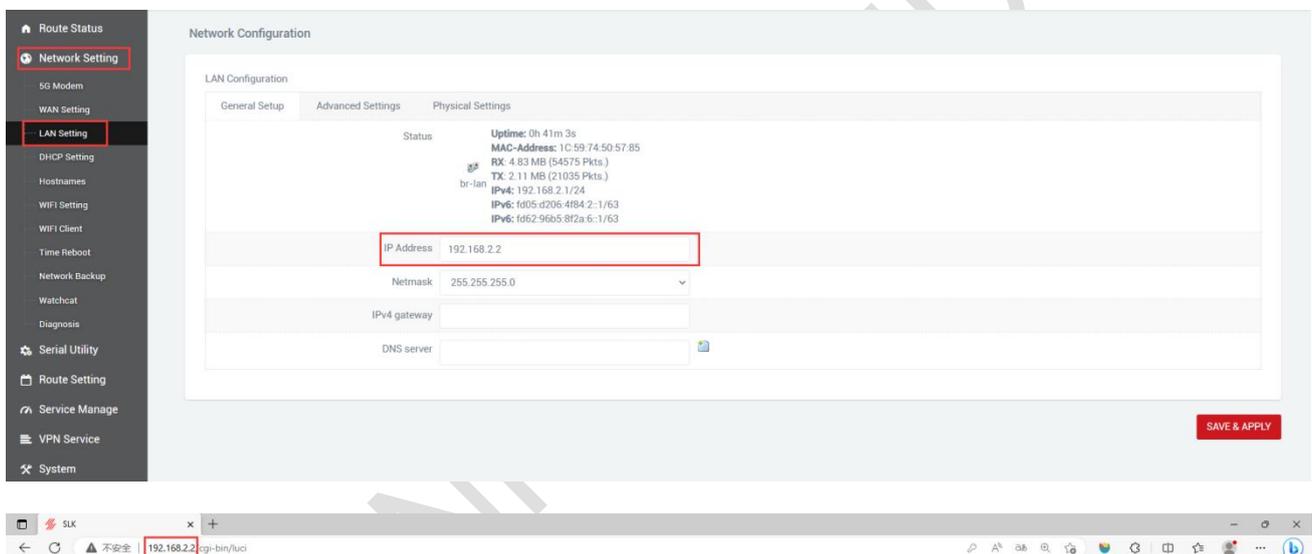
The default address of the router is 192.168.2.1. You can modify the static IP address in the navigation bar "Network Setting" - "LAN Setting" - "General Setting". After modification, the new IP address will be used to log in to the page.

A.IP Address: Modify the ip address of the device (default is 192.168.2.1).

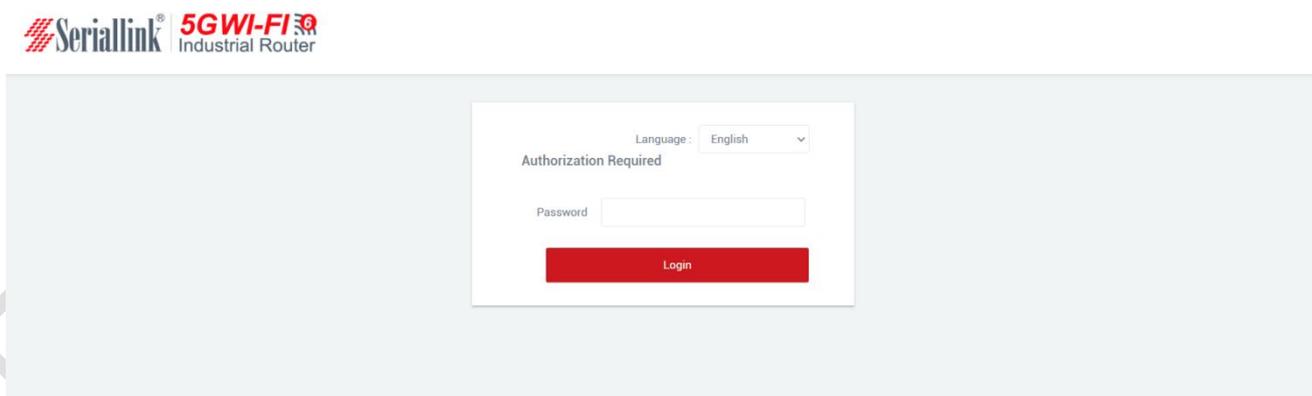
B.Netmask: It is generally 255.255.255.0, which can be modified as needed.

C.IPv4 gateway、DNS server、Override MTU: No special cases do not need to be set.

D.After the configuration is complete, click "SAVE & APPLY" to make it take effect. After it takes effect,you need to use a new IP address to access the configuration page of the device.



The screenshot shows the 'Network Configuration' page in the Seriallink web interface. The left sidebar contains navigation options, with 'Network Setting' and 'LAN Setting' highlighted. The main content area shows the 'LAN Configuration' section, which is divided into 'General Setup', 'Advanced Settings', and 'Physical Settings'. The 'General Setup' tab is active, displaying fields for 'IP Address' (192.168.2.2), 'Netmask' (255.255.255.0), 'IPv4 gateway', and 'DNS server'. A 'SAVE & APPLY' button is located at the bottom right of the configuration area. Below the configuration page, a browser window is shown with the address bar containing '192.168.2.2/cgi-bin/luc'.



The screenshot shows the Seriallink login page. The page header includes the Seriallink logo and '5GWI-FI Industrial Router'. The main content area features a login form with a 'Language' dropdown menu set to 'English', a 'Password' input field, and a red 'Login' button. The background is a light blue color.

## 2.2 5G Modem

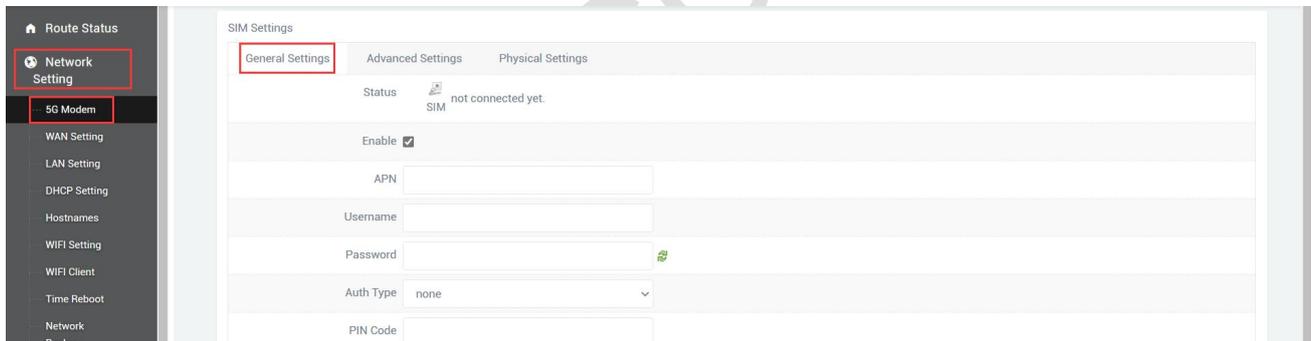
By default, the router uses the SIM card 3/4/5G to access the Internet. You can see the information of the SIM card in the "Routing Status" - "Status" in the navigation bar. You can check the network is 3/4/5G and the signal of the mobile phone card in the upper right corner.



The screenshot shows the 'Cellular Status' page in the router's web interface. The left sidebar has 'Status' highlighted. The main content area displays the following information:

Cellular Status	
SIM CARD	SIM READY
COPS	UNICOM
Cellular Network	NR5G
Frequency Band	5078
ARFCN	627264
PCI	365
CEREG	GPRS: 0,1 / EPS: 0,1 / 5GS: 0,1
Signal Quality	RSRQ: -11.0 dB / RSRP: -77 dBm
Card Slot	SIM1
IMEI	861702060003869
IMSI	460012238632850
ICCID	89860120801345580028

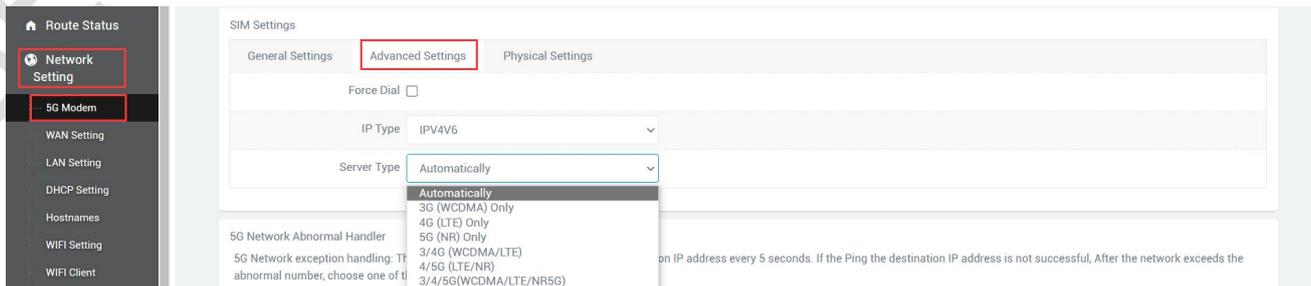
If you use an ordinary mobile phone data card, you don't need to care about the location of the APN setting, it can be empty by default. If you use an APN card, you need to set the APN in "Network Setting" - "5GModem" - "General Settings".



The screenshot shows the 'SIM Settings' page in the router's web interface. The left sidebar has 'Network Setting' and '5G Modem' highlighted. The main content area displays the following information:

SIM Settings	
General Settings	
Status	 not connected yet.
Enable	<input checked="" type="checkbox"/>
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Auth Type	none
PIN Code	<input type="text"/>

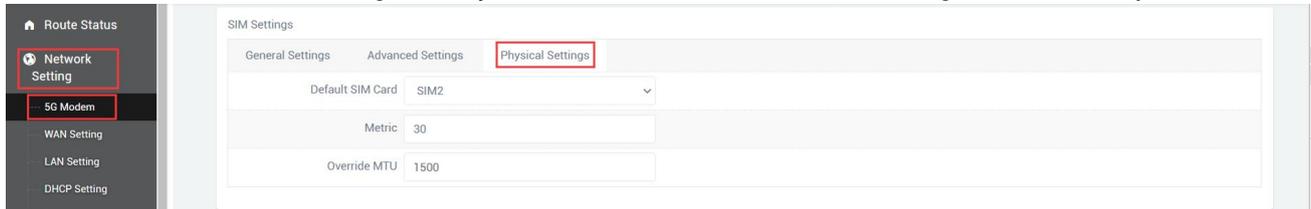
"Network Setting" - "5G Modem" - "Advanced Settings" can bind 3/4/5G. If 5G (NR) Only is selected for the service type, it means that only the 5G network is used. If there is no 5G network nearby, there will be no network automatically. The default is 3/4/5G, the frequency band with good signal is given priority, and 5G is given priority under the same signal. Locking the frequency band is automatic, and you can also lock the frequency band according to your own needs. If the locked frequency band is unsuccessful, it means that the module does not support this frequency band temporarily. After setting, click "SAVE & APPLY".



The screenshot shows the 'SIM Settings' page in the router's web interface. The left sidebar has 'Network Setting' and '5G Modem' highlighted. The main content area displays the following information:

SIM Settings	
Advanced Settings	
Force Dial	<input type="checkbox"/>
IP Type	IPv4V6
Server Type	Automatically
5G Network Abnormal Handler	3G (WCDMA) Only 4G (LTE) Only 5G (NR) Only 3/4G (WCDMA/LTE) 4/5G (LTE/NR) 3/4/5G(WCDMA/LTE/NR5G)
5G Network exception handling: T1 abnormal number, choose one of t	on IP address every 5 seconds. If the Ping the destination IP address is not successful, After the network exceeds the

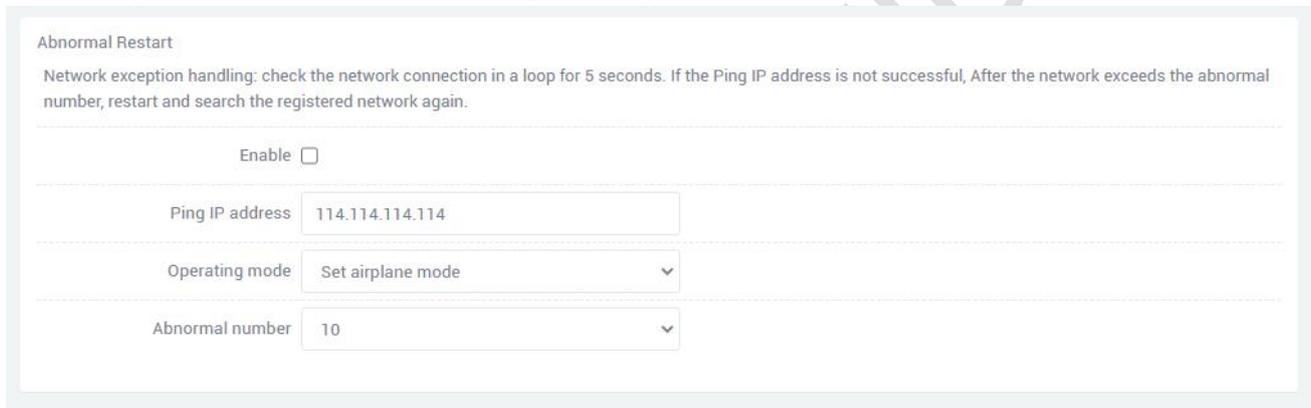
"Network Setting" - "5G Modem" - "Physical Settings" can modify the default SIM card. If only one card is inserted, it will be used by default, and there is no need to modify the configuration here. Metric (default: 30) generally does not need to be modified. The smaller the value, the higher the priority of using the network (networks include: wifi client, WAN port, 4G network, etc.). MTU (default: 1400), the maximum transmission unit, generally do not need to be modified, affecting the network speed.



The screenshot shows the 'SIM Settings' page with the 'Physical Settings' tab selected. The settings are as follows:

Setting	Value
Default SIM Card	SIM2
Metric	30
Override MTU	1500

**Abnormal Restart:** It is to deal with network exceptions, ping the set ip address (114.114.114.114) every 5s, and still can't ping after the abnormal number of pings, it will be set according to the selection (Reboot on internet connection lost, Set airplane mode) (default), Switch SIM card). Network diagnostics can be set in "General Settings", "Advanced Settings", and "Physical Settings". It is not enabled by default. If you need to enable network diagnostics, you can enable it.



The screenshot shows the 'Abnormal Restart' settings page. The settings are as follows:

Setting	Value
Enable	<input type="checkbox"/>
Ping IP address	114.114.114.114
Operating mode	Set airplane mode
Abnormal number	10

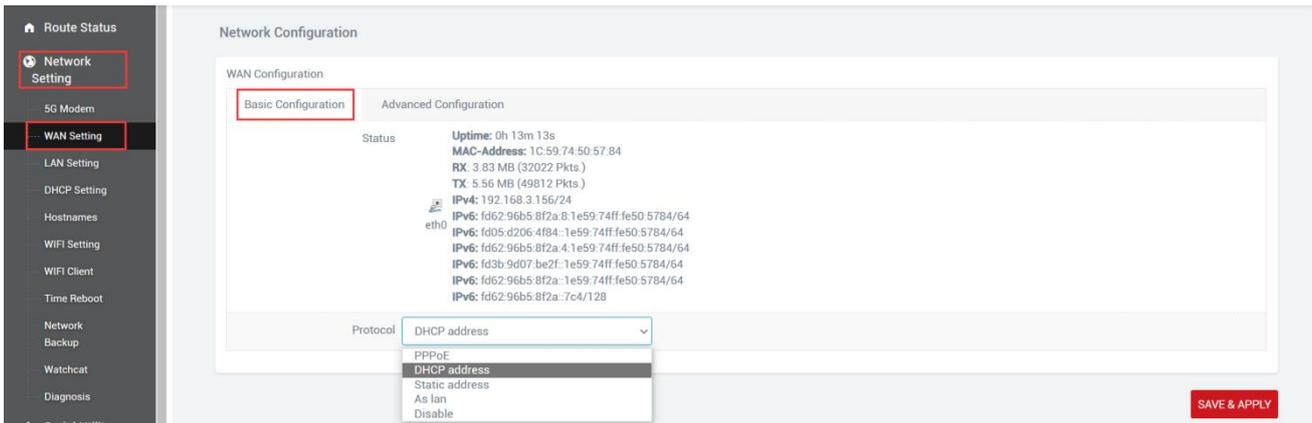
**note:**

- Ordinary 5G mobile phone card can access the Internet without worrying about APN settings.
- If an APN dedicated network card is used, be sure to fill in the APN address, username and password.
- Different operators have different specifications of APN dedicated network cards. Please consult the local operator for the APN address, user name and password.

## 2.3 WAN Setting

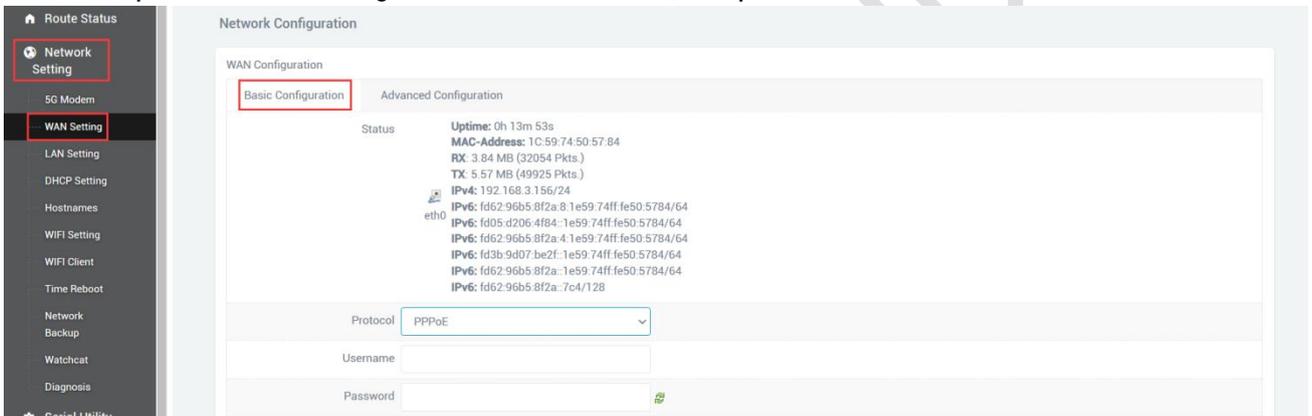
### 2.3.1 DHCP address

Navigation bar "Network Setting" - "WAN Setting" - "Basic Configuration", the default protocol of WAN port is dynamic address (ie DHCP client), the upper-level device needs to be able to assign ip to the wan port, Without special cases.



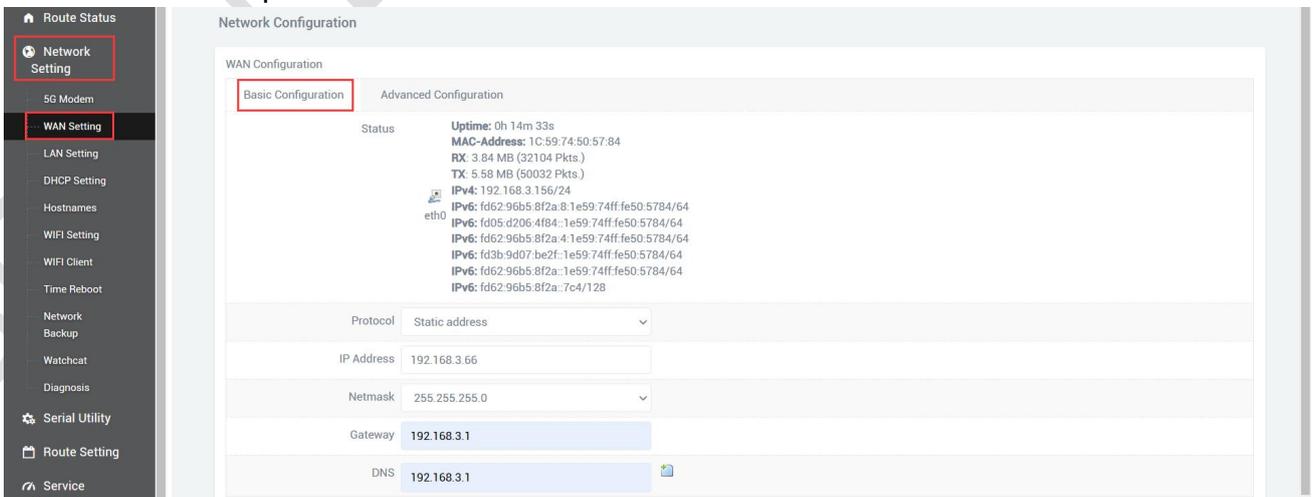
### 2.3.2 PPPoE

If the wan port needs to dial up to access the Internet, you need to select PPPoE, fill in the user name and password according to the actual situation, no special circumstances.



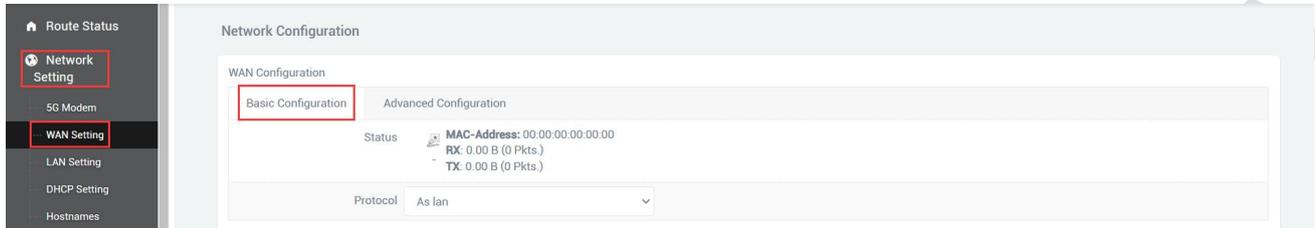
### 2.3.3 Static address

You can also choose to manually set the IP address for the wan port. You need to set the same IP address as the upper-level network segment, subnet mask, and gateway to fill in the IP address of the upper-level device. DNS can be the same as the gateway. Generally, there are common DNS such as 8.8.8.8. There is no special case.



### 2.3.4 As lan (convert WAN port to LAN port)

If you want to convert the WAN port into a LAN port, change the protocol of "WAN Setting" to "As lan", click "SAVE & APPLY", you can convert the wan port to a lan port(In the case of associated LAN, please be careful not to connect the WAN port and LAN port to the switch or the same computer), no special circumstances.



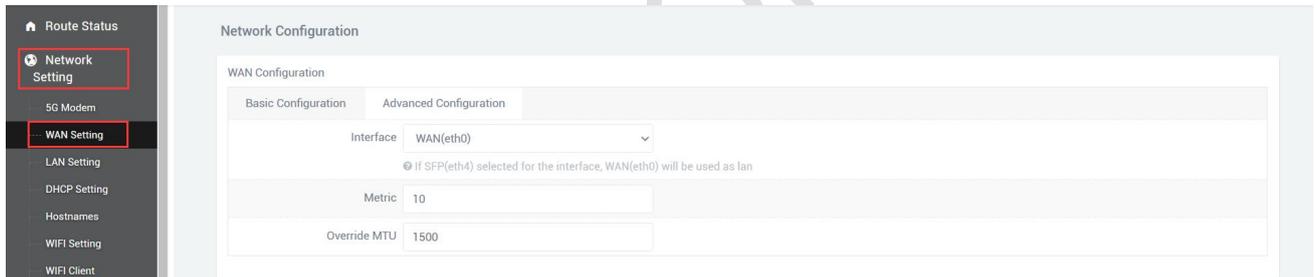
### 2.3.5 Advanced Configuration

Navigation bar "Network Setting" - "WAN Setting" - "Advanced Configuration".

Interface: This refers to the physical interface, which can be switched between the network port (WAN) and the optical fiber port (optical port SFP).

Metric(default:30): Generally, it does not need to be modified, the smaller the value, the higher the priority of using the network (networks include: wifi clients, WAN ports, 4G networks, etc.).

Override MTU (default: 1400): The maximum transmission unit, generally without modification, affecting network speed.



## 2.4 DHCP Setting

DHCP adopts the client/server communication mode, the client submits a configuration application to the server, and the server returns the corresponding configuration information such as the IP address assigned to the client, so as to realize the dynamic configuration of the IP address and other information.

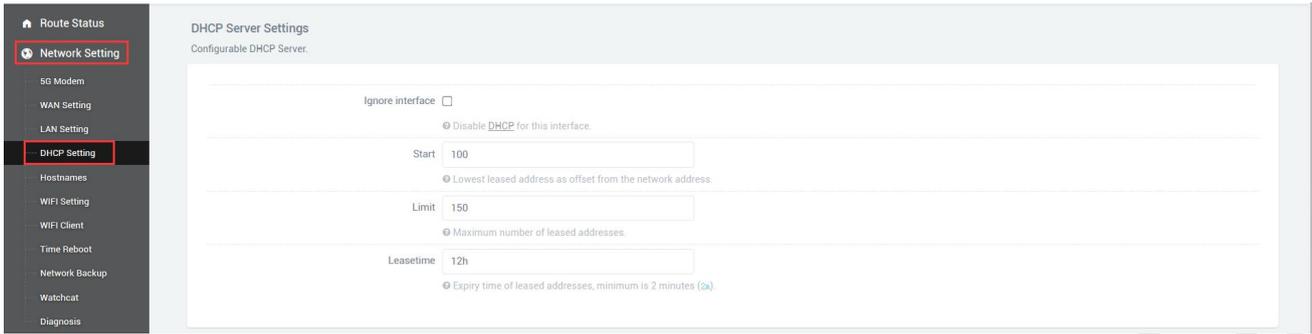
DHCP client configuration (enabled by default), select "Network Setting" - "DHCP Settings", "SAVE & APPLY".

A.Ignore interface: Checking this will turn off the DHCP server.

B.Start: The starting address of the allocated dhcp server, such as 100, means that the allocation starts from 192.168.2.100.

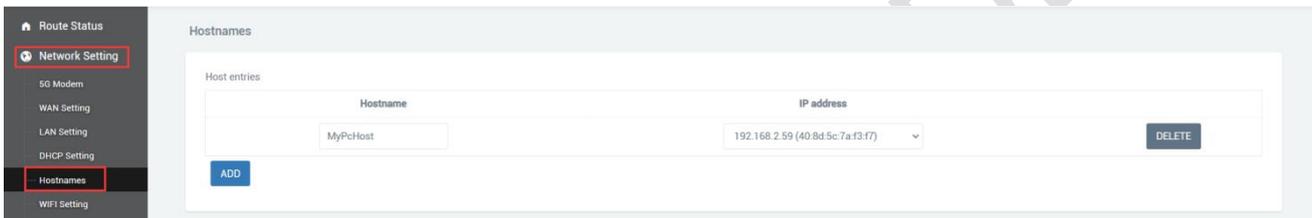
C. Limit: Maximum number of leased addresses.

D.Leasetime: Expiry time of leased addresses.

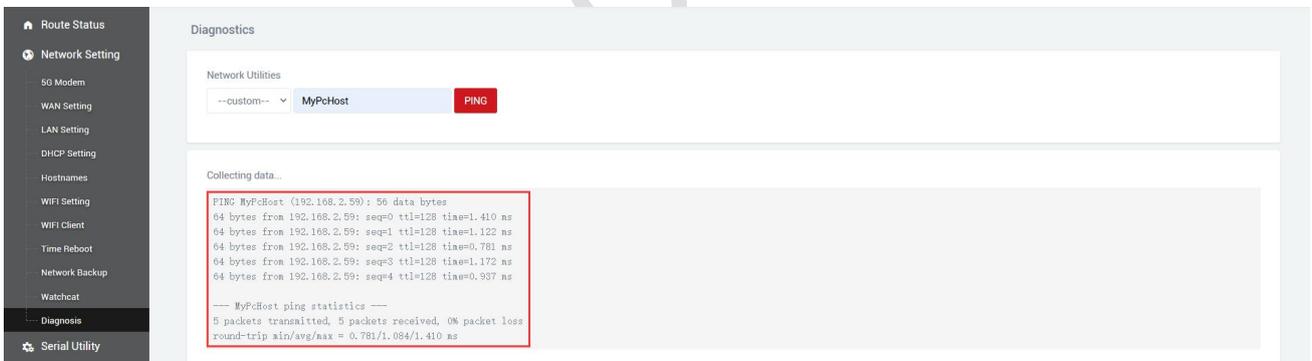


## 2.5 Hostnames

Navigation bar "Network Setting" - "Hostnames", You can name the target known IP address for easy memorization, as shown in the figure.

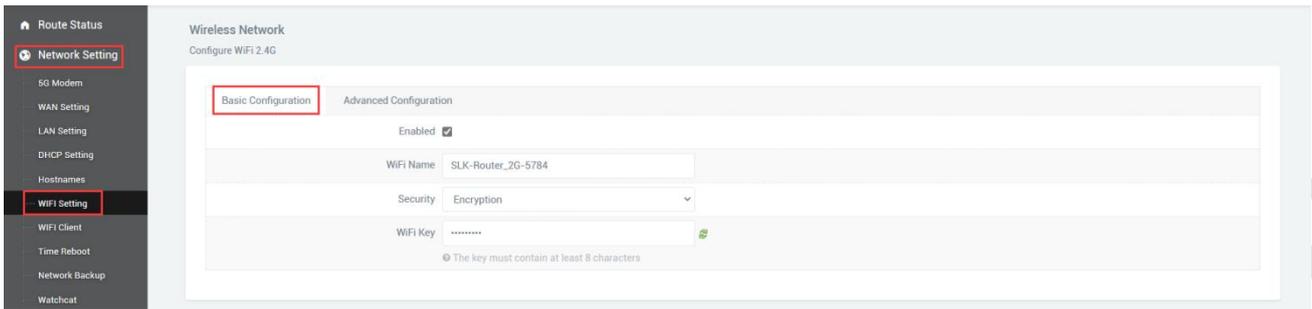


It should be noted that the alias must be unique, otherwise there will be a conflict, resulting in access to the wrong address, such as baidu, google and other existing domain names, the alias only takes effect on the current device network.



## 2.6 WIFI Access Point

WIFI AP supports WIFI dual-band 2.4G+5.8G, WIFI is enabled by default, wifi name: SLK-Router\_2G-XXXX, SLK-Router\_5G-XXXX (to avoid the same name of wifi between different devices, the "XXXX" part will be different), password : slk100200(Password needs to be 8 characters or more). Navigation bar "Network Setting" - "WIFI Setting"- "Basic Configuration", you can change the basic configuration of WIFI.



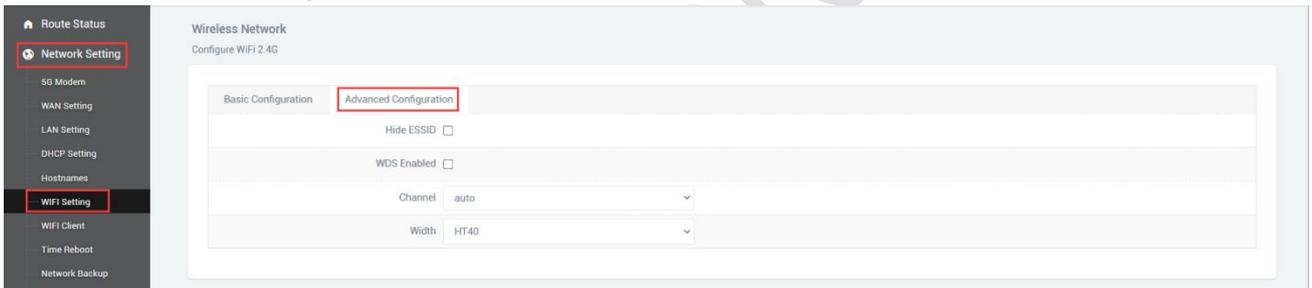
Navigation bar "Network Setting" - "WIFI Setting" - "Advanced Configuration", under normal circumstances do not need to modify.

Hide ESSID: If checked, this WiFi will not be searched on mobile phones, computers and other devices.

WDS Enabled: When you need to use trunking and bridging mode, if the other one turns on WDS, then it also needs to be turned on here.

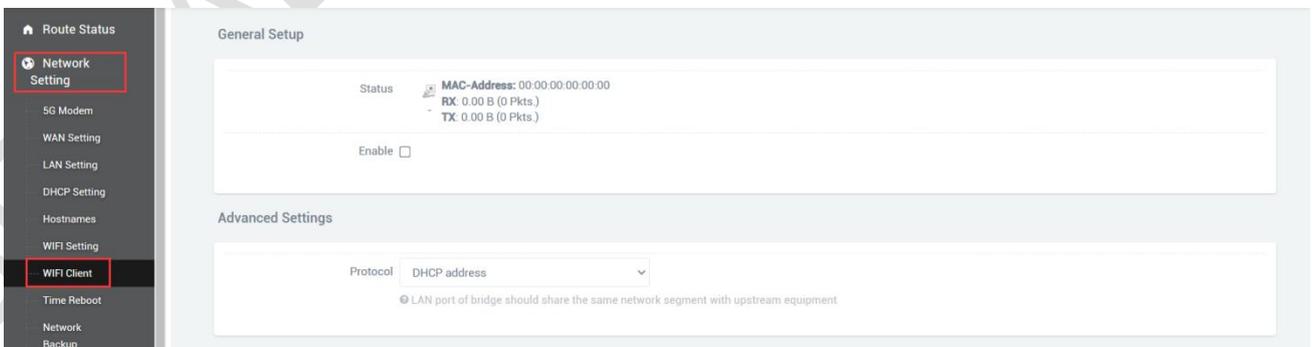
Channel: If you know the channel of other wifi nearby, you can set this device to a different channel to improve wifi speed and signal.

Width: WiFi speed HT80 (5.8G exclusive) > HT40 > HT20, WiFi stability HT20 > HT40 > HT80 (5.8G exclusive), affected by distance and partitions (such as walls), use large bandwidth at close range, use a small bandwidth for long distances.



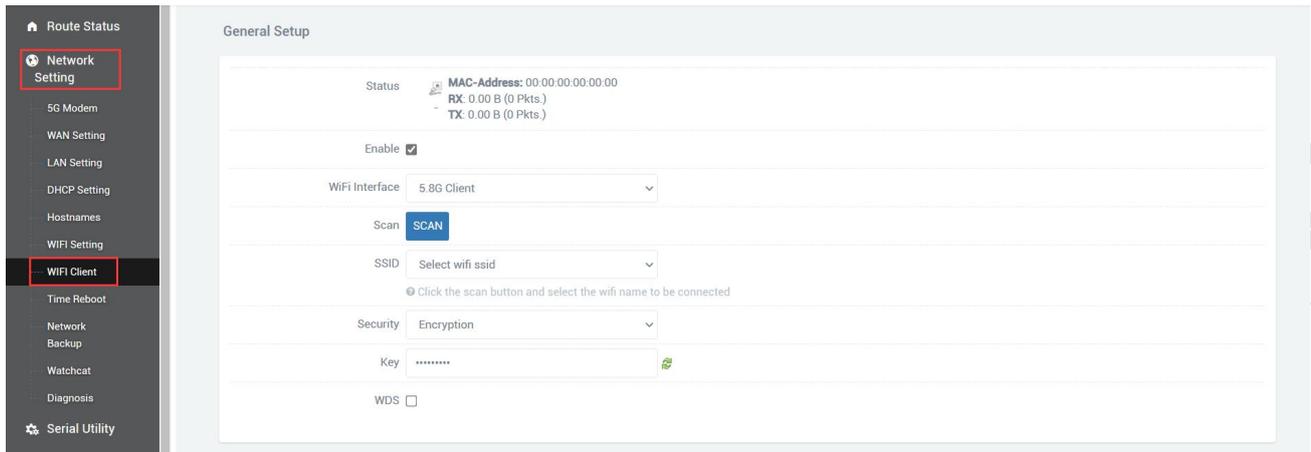
## 2.7 WIFI Client(Bridge)

The WIFI Client is not enabled by default, you need to check to enable it in the navigation bar "Network Setting" - "WIFI Client".



Then select the client wifi interface: 2.4G Client, 5.8G Client, search the corresponding WIFI list, select WIFI in the SSID list, change the security option according to whether there is a password, None (no password), Encryption (Encryption mixed mode Mixed WPA/WPA2-PSK), WDS is not checked by

default.



After successfully connecting to WIFI, the WIFI status will be displayed.

### Status



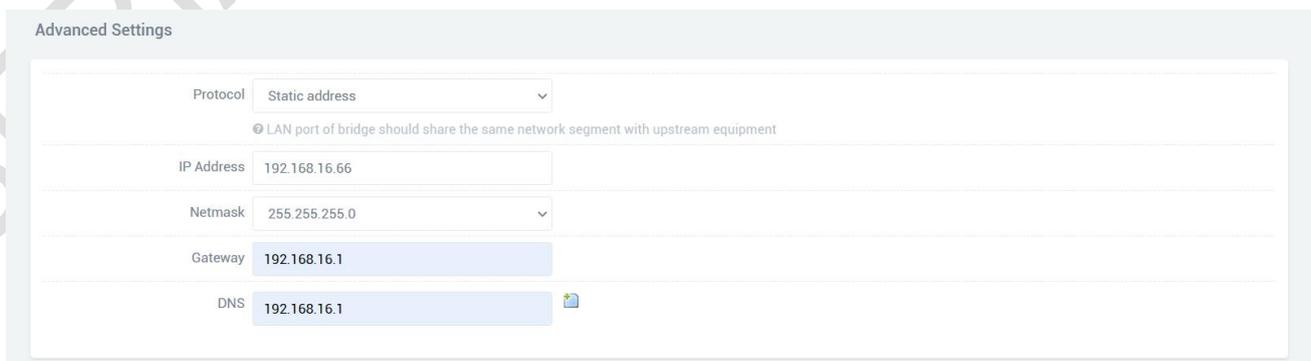
Client "赛诺联克"

Uptime: 0h 0m 8s  
 MAC-Address: 22:59:74:50:57:86  
 RX: 7.73 KB (67 Pkts.)  
 TX: 1.20 KB (6 Pkts.)  
 IPv4: 192.168.16.201/24

**Note:** The wireless interface 2.4G client search requires WIFI wireless AP WiFi-2.4G is in the activated state, the wireless interface 5.8G client search requires WIFI wireless AP WiFi-5.8G is in the activated state, otherwise, the search result will not be displayed (after saving the page configuration of WIFI wireless AP and WIFI wireless client, WiFi-5.8G starts slowly, please wait for a while).

### WiFi wireless client advanced settings protocol selection:

- A. DHCP address (default): The WiFi client automatically obtains the IP address assigned by the superior route.
- B. Static address: The WiFi client uses the user-configured IP address, subnet mask, gateway, and DNS.
- C. Bridge Lan: Use the LAN port configuration IP address, subnet mask, gateway, DNS, Lan port configuration reference WiFi wireless client advanced settings static address (relay mode select this item).



Status

Client "赛诺联克"

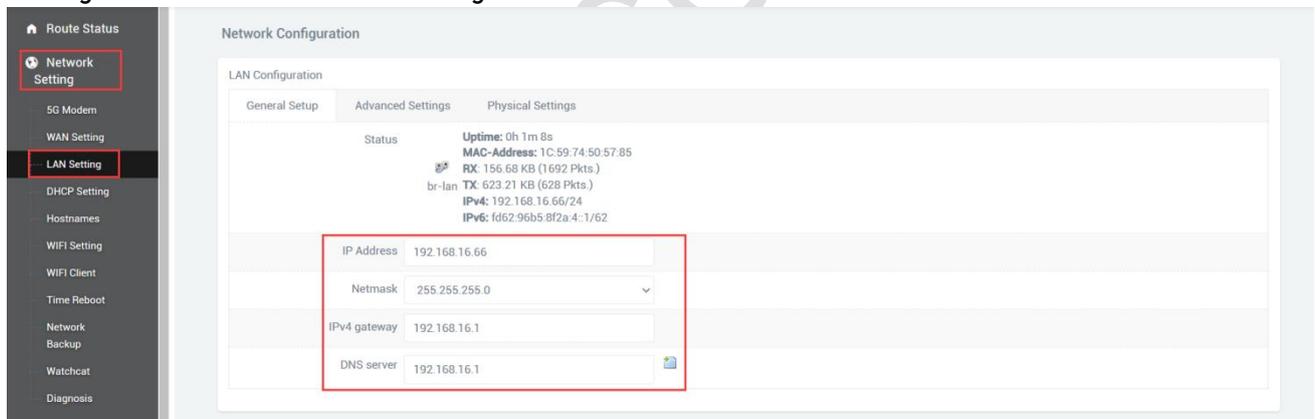
**Uptime:** 0h 0m 5s  
**MAC-Address:** 22:59:74:50:57:86  
**RX:** 0.00 B (0 Pkts.)  
**TX:** 0.00 B (0 Pkts.)  
**IPv4:** 192.168.16.66/24

## 2.8 WIFI repeater

This section describes how to extend the wireless signal length by means of relays. In this configuration mode, the computer terminal connected to the SLK-R680 is in the same IP address segment as the main wireless network.

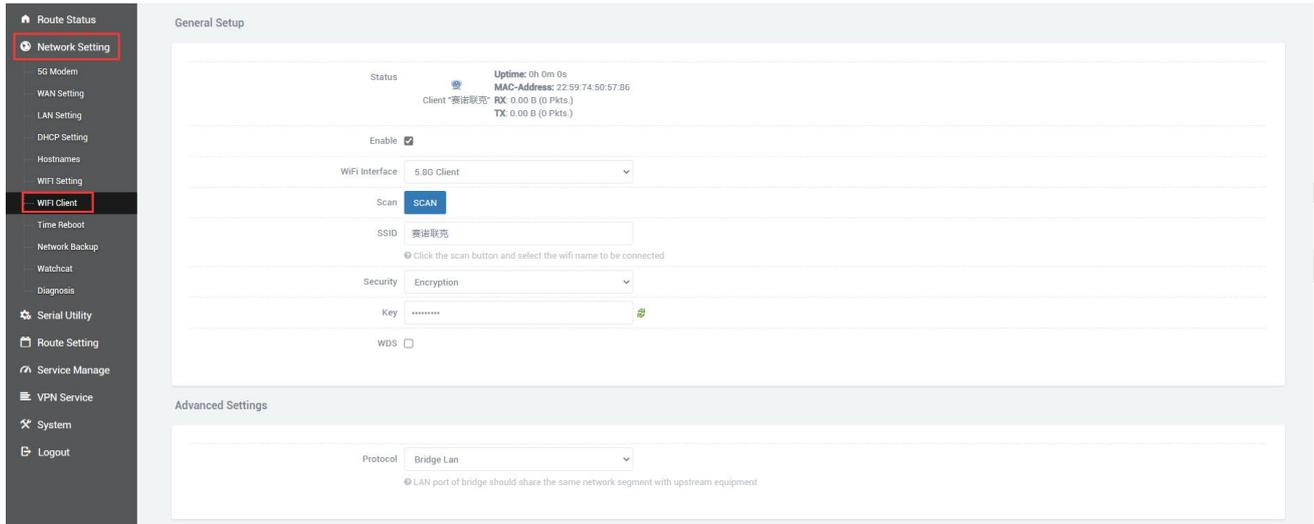
### 2.8.1 Change the local IP address

It is necessary to modify the local IP address of SLK-R680 to be in the same network segment as the main wireless AP. For example, the IP address of the main wireless AP to be connected is 192.168.100.1, then modify the IP address of SLK-R680 to 192.168.100.100. It should be noted that the LAN port gateway is empty by default. After using the relay mode setting, if you need to connect to the Internet through the WAN port in the future, you need to delete the gateway information in the LAN settings to avoid the situation of being unable to access the Internet.



### 2.8.2 Connect to the main wireless AP

In the navigation bar "Network Setting" - "WIFI Client", check to enable the WIFI wireless client, and configure the connection to the main wireless AP. For example, the SSID of the main wireless AP to be connected here is WIFI6-2G, and the password is slk100200, Search and select the SSID as shown in the figure below, fill in the password, select "Bridge Lan" from "Protocol", and click "SAVE & APPLY".

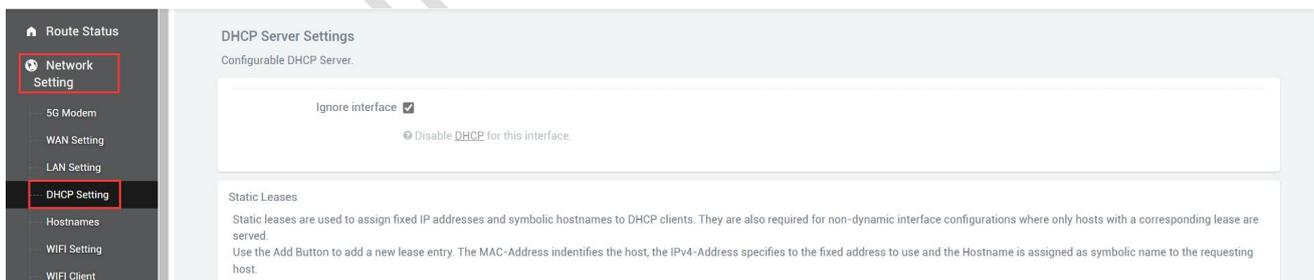


It should be noted that in this mode, the main wireless AP no longer assigns an IP address to this SLK-R680. Therefore, the obtained IP address will not be updated in "Status", and you can confirm whether the connection is successful through the icon color and MAC address. The picture below is successful.



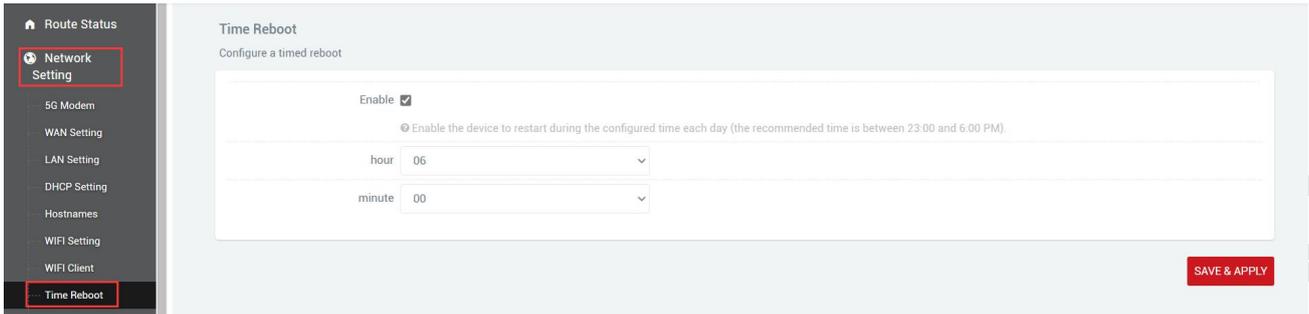
### 2.8.3 Disable DHCP

Disable the DHCP server function of the SLK-R680. In this way, the SLK-R680 no longer assigns IP addresses to the connected devices, and all devices connected to the local area network are assigned IP addresses by the main wireless to realize communication on the same network segment.



## 2.9 Time Reboot

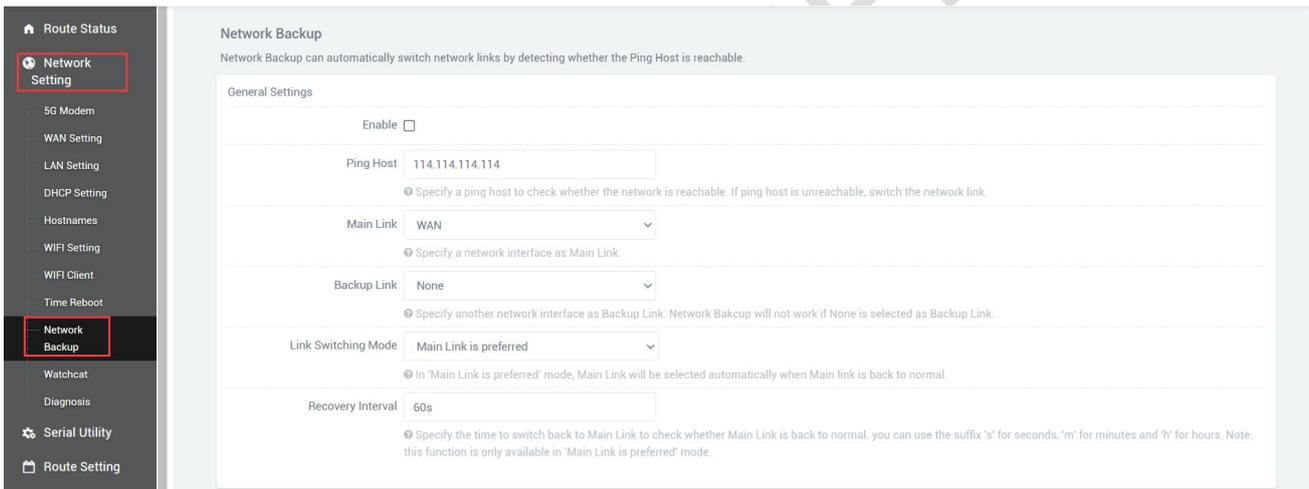
Navigation bar "Network Setting" - "Time Reboot", users can check to enable and set the time to restart every day, pay attention to check whether the device time is correct, modify the correct time: "System" - "Date Time", see chapter 7.1 for details .



## 2.10 Network Backup

This part is a new feature, mainly used to give priority to the use of wired (that is, WAN) or cellular network or WiFi client for the Internet, give priority to the network of the main link, and use the network of the backup route when the main link does not have a network.

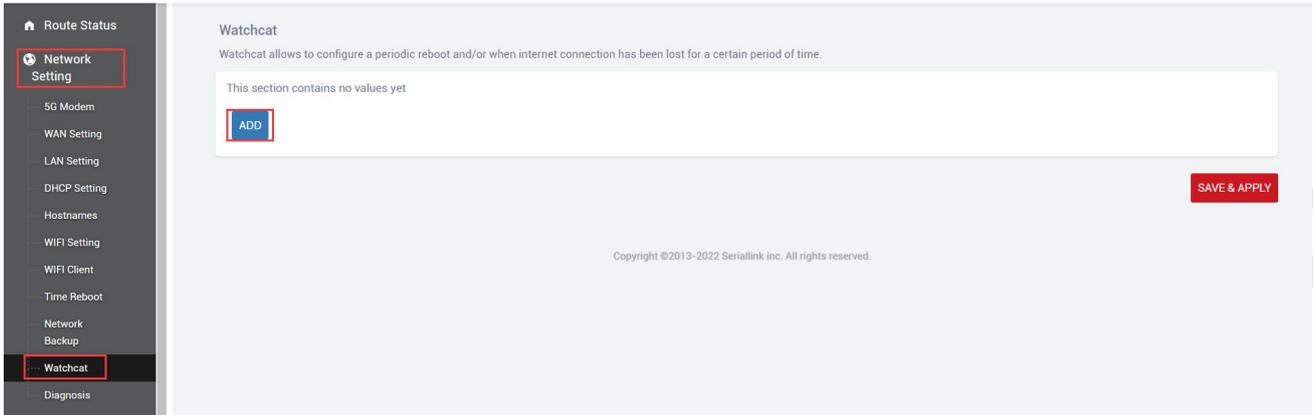
Network backup is disabled by default, you need to enable it, and then configure it according to the actual situation.



## 2.11 Watchcat

In the navigation bar "Network Setting" - "Watchcat", the network self-check function is disabled by default, and the network self-check allows setting periodic restarts or restarts when the network is abnormal.

If you need to activate this function, click Add, enter the configuration and click "SAVE & APPLY".

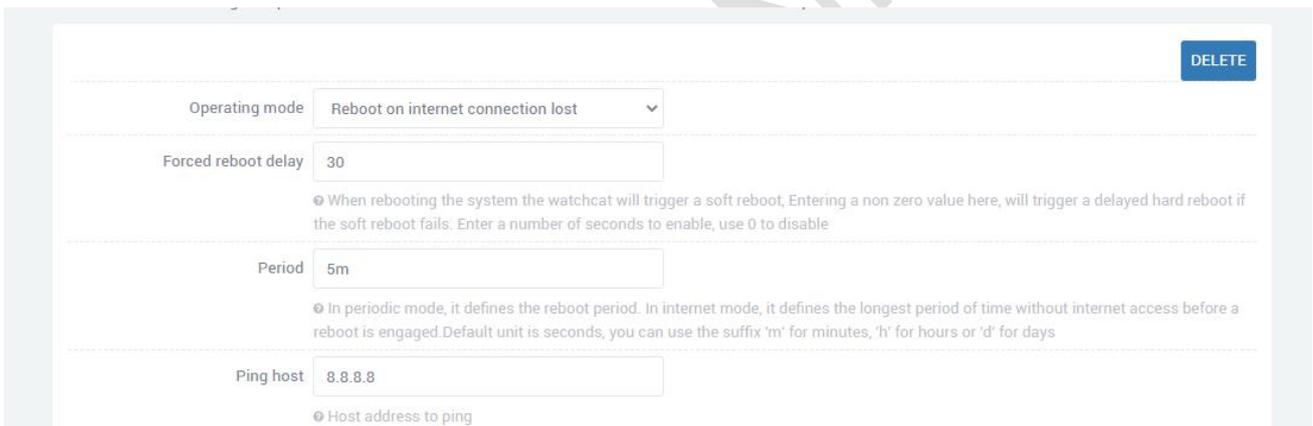


A. Forced reboot delay: When rebooting the system the watchcat will trigger a soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable

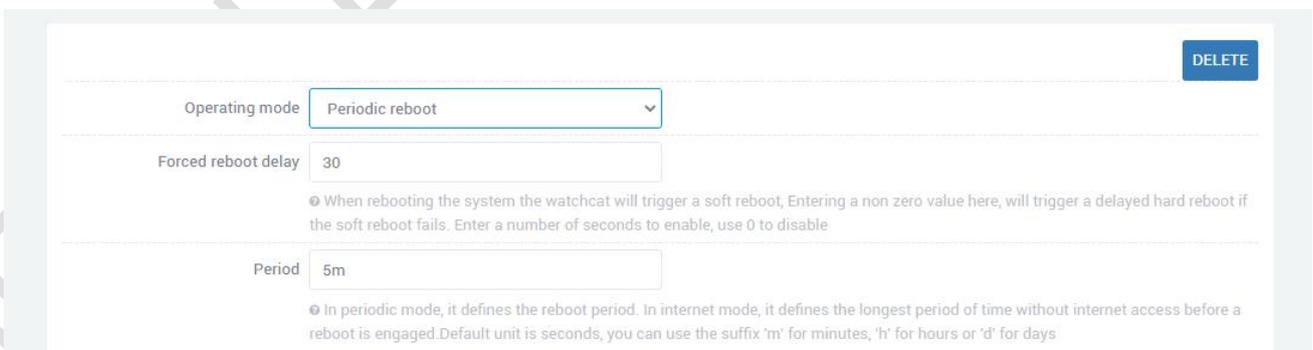
B. Period: In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

C. Ping host: Host address to ping

1. Reboot on internet connection lost



2. Periodic reboot



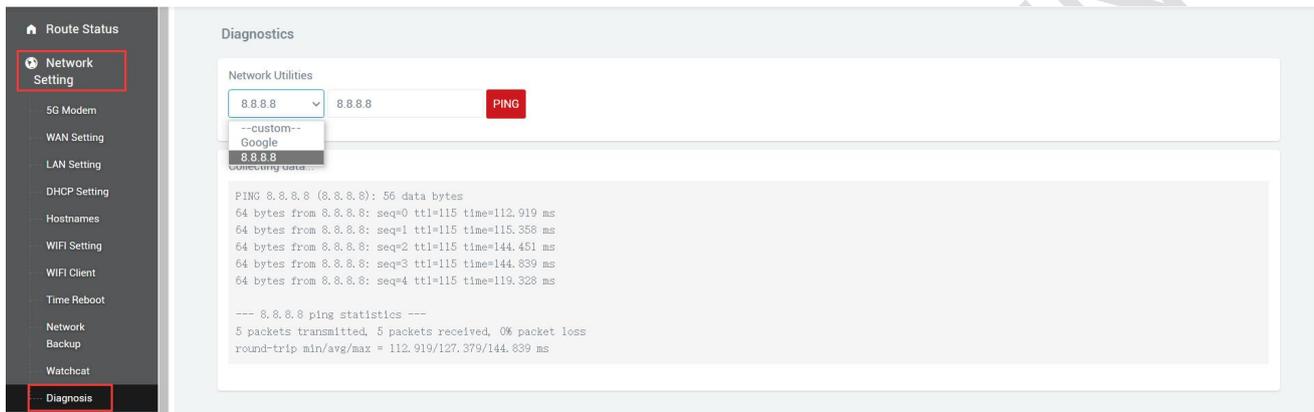
After adding and configuring, click "SAVE & APPLY" to take effect. To delete the configuration, just click the "DELETE" button in the upper right corner, and then "SAVE & APPLY".

## 2.12 Diagnosis

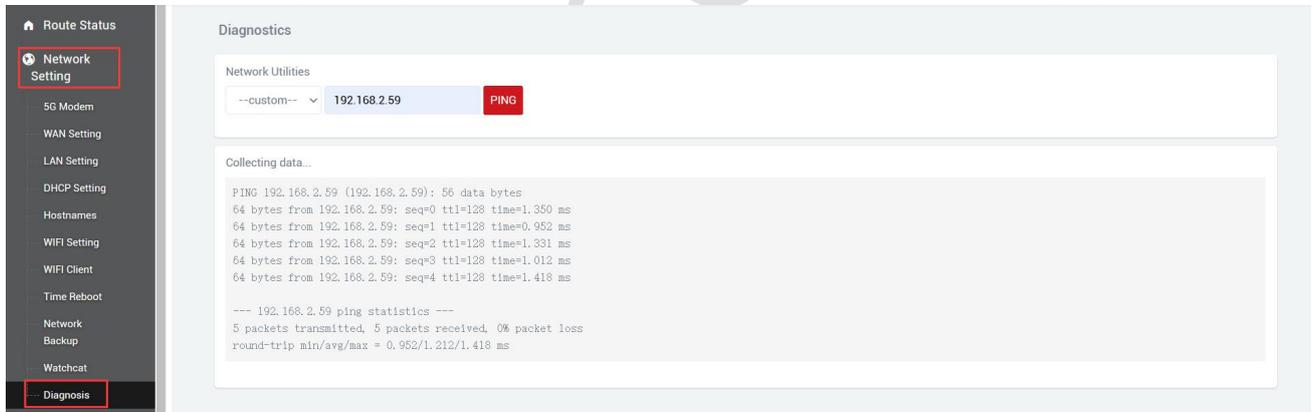
Through network diagnosis, you can determine whether the router and the connected device can communicate with each other, whether the device can access the Internet, and whether the device is successfully connected to the VPN. It can also be used to test other aspects, and you can test it according to your own needs.

Navigation bar "Network Setting" - "Diagnosis".

Baidu, seriallink, 8.8.8.8: It is generally used to test whether the device can access the Internet. If it can ping, it means the device can access the Internet. If it cannot ping, it means that the device cannot access the Internet.



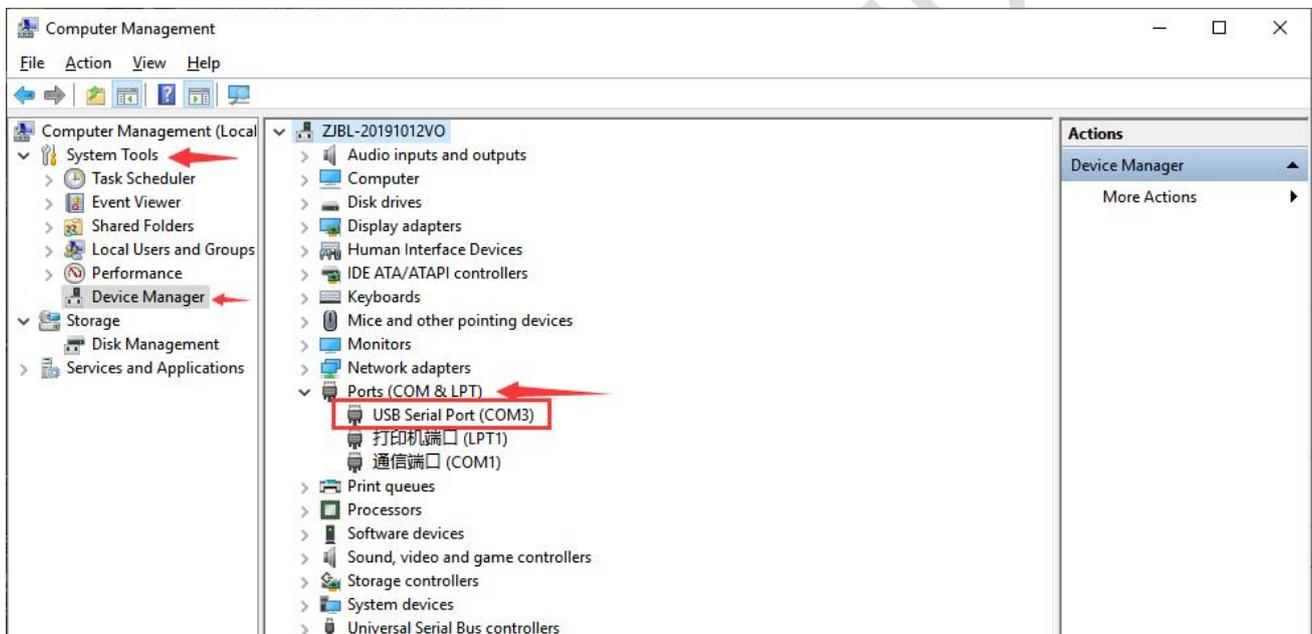
Custom input box: generally used to test whether the connected device can be pinged.



## Chapter 3 Serial port configuration

### 3.1 Use Tools And Preparation

Select "Serial Utility" - "RORT-RS232" in turn to configure a port according to your needs. Here is an example of RORT-RS232. Connect the computer serial port, check the serial port as shown in the figure below, right click on the desktop This PC>>>Manage>>>System Tools>>>Device Manager>>>Ports(COM &LPT). Use tools UartAssist.exe and NetAssist.exe for TCP Server, TCP Client, UDP Server, and UDP Client simulation, and ModSim32.exe and ModScan32.exe for Modbus TCP simulation. You can use your familiar serial port and network debugging software. The difference between UDP Client and UDP Server is whether it needs to communicate with only a specific IP address. UDP Client only communicates with a specific server IP address.

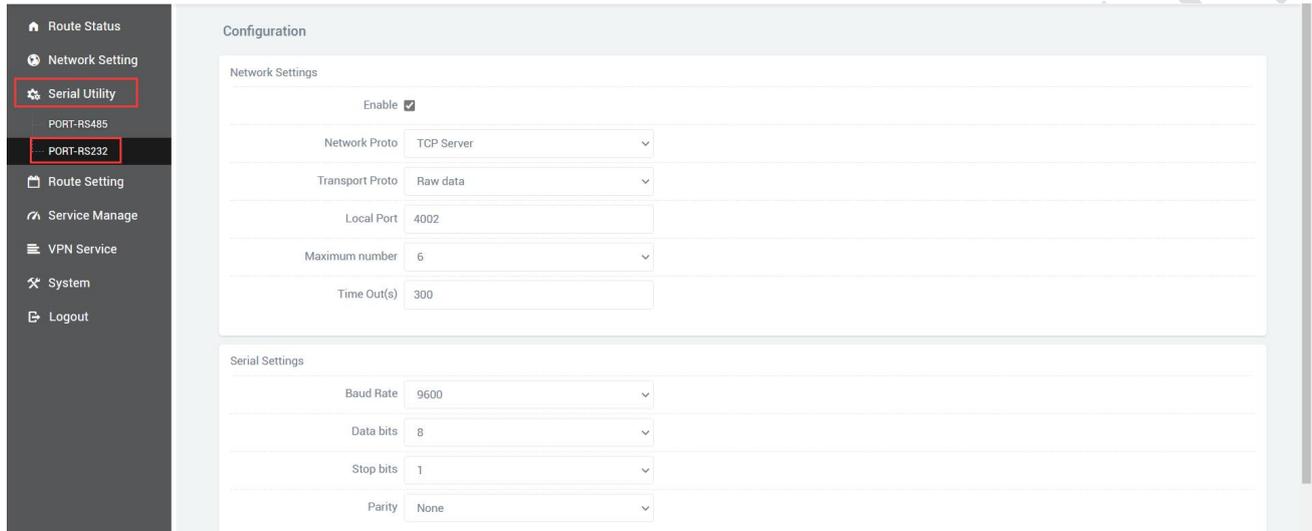


The settings of UartAssist.exe are as follows. The baud rate and stop bit can be changed as required. After the setting is completed, click Open.



## 3.2 TCP Server

Select "Serial Utility" - "RORT-RS232" in turn, select TCP Server as the network protocol, and choose the data type according to your needs. Generally, the choice is "Raw data". You need to remember the local port after setting. When establishing a TCP connection, you need to use the IP address and port number of the serial server. Configure the baud rate, data bit, stop bit and parity bit of the serial port through the serial port configuration bar according to your needs. After the configuration is complete, click SAVA & APPLY.



Network Settings	
Enable	<input checked="" type="checkbox"/>
Network Proto	TCP Server
Transport Proto	Raw data
Local Port	4002
Maximum number	6
Time Out(s)	300

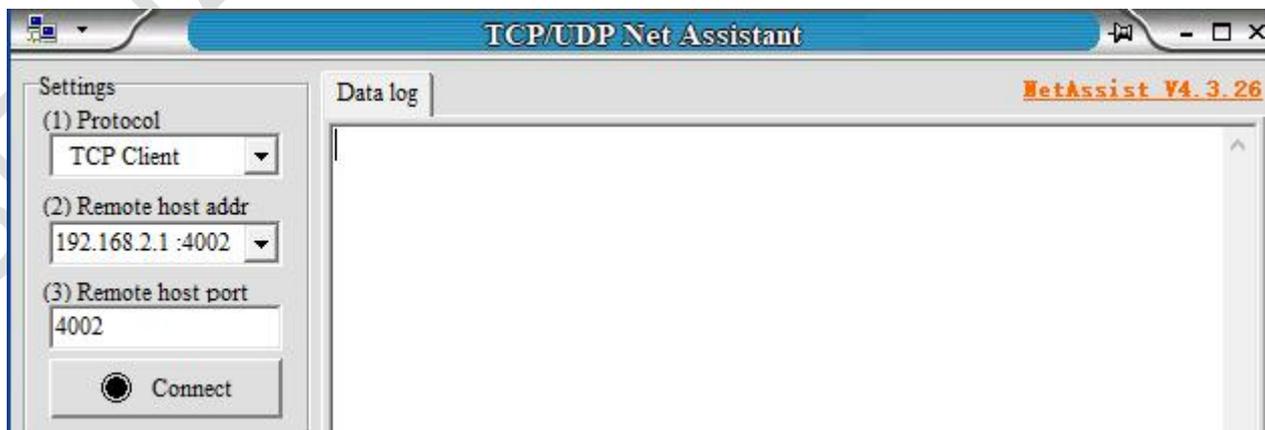
  

Serial Settings	
Baud Rate	9600
Data bits	8
Stop bits	1
Parity	None

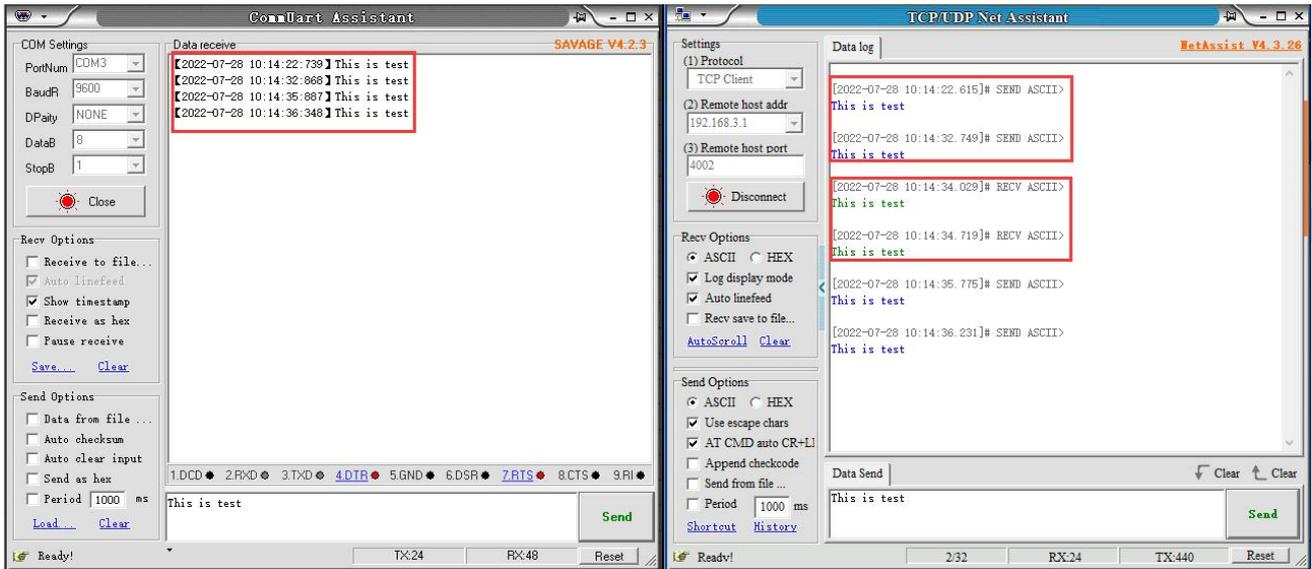
**Maximum number:** The default is 6, which means that up to 6 TCP Clients are supported to connect to the same serial port.

**Time Out (s):** The default is 300, which means that after the TCP Server establishes a connection, if there is no data, the connection will be disconnected after 300 seconds. If you need a permanent online connection, you can set the value to 0.

Open the software, select TCP Client, IP is the server address, the port is the same as the server port, and click Connect.

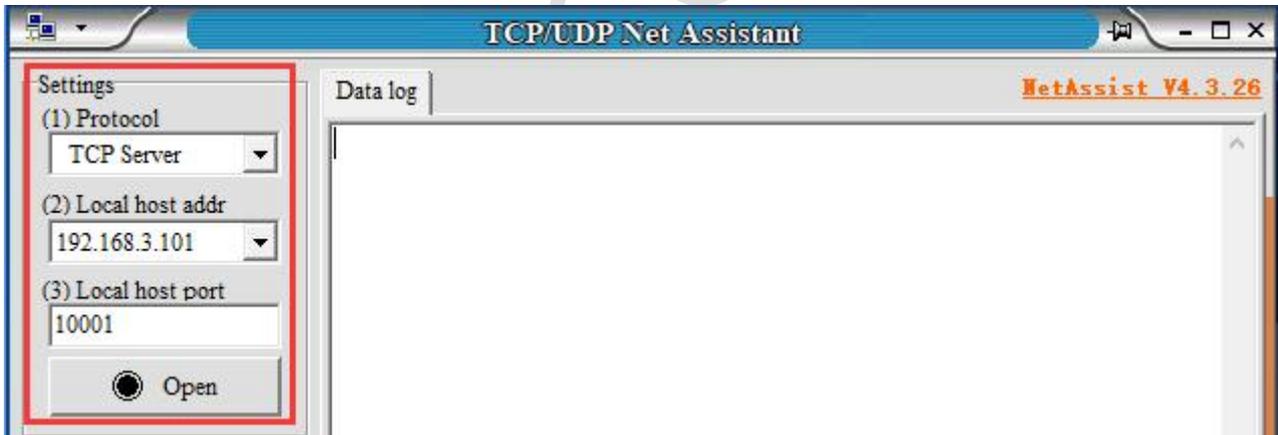


TCP Server and TCP Client send and receive data diagram.

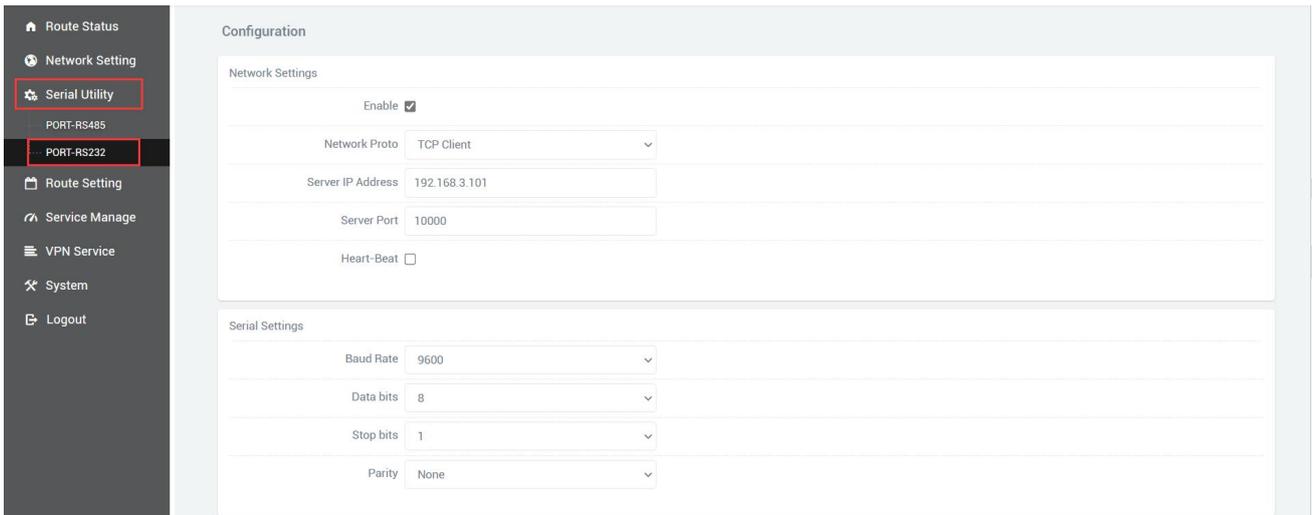


### 3.3 TCP Client

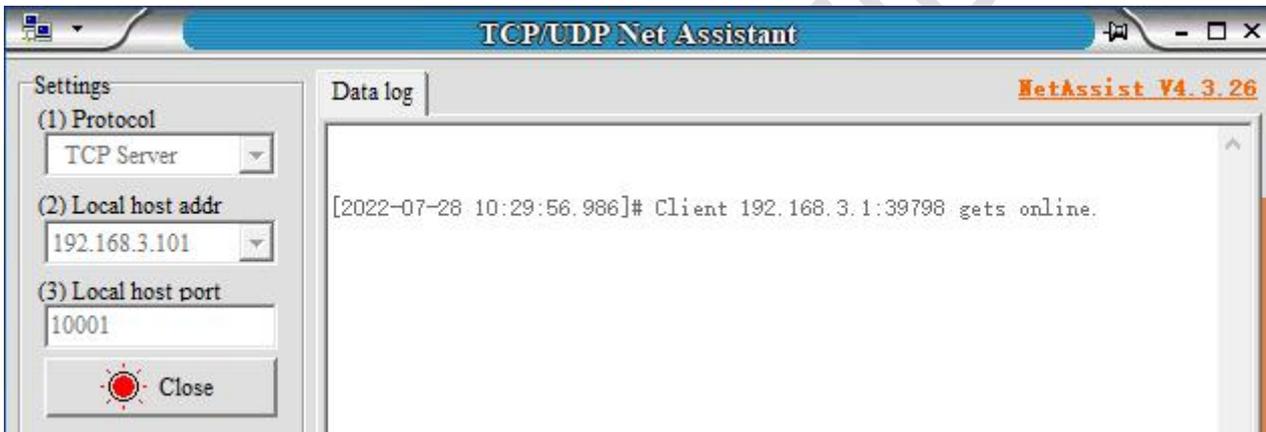
Protocol select TCP Server, Local host addr select the IP address set by the computer, which is in the same network segment as the device's LAN port IP. The Local host port is the default, and the client settings need to use Local host addr and Local host port,click Open.



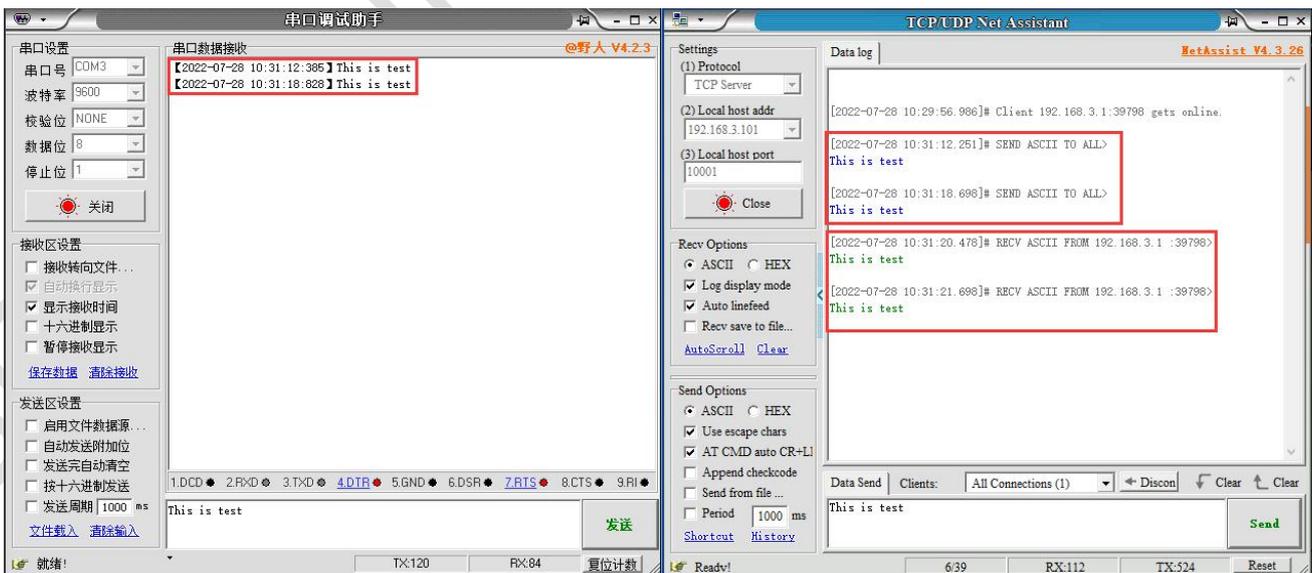
Select "Serial Utility" - "RORT-RS232" in turn,select TCP Client as the network protocol, and the server IP and port number should be consistent with the software settings. Configure the baud rate, data bit, stop bit and parity bit of the serial port according to your needs through the serial port configuration bar. After the configuration is complete, click SAVA & APPLY.



After saving and applying, the software will print "[2021-12-02 17:36:44.743]# Client 192.168.0.233:44380 gets online.", indicating that the connection is successful.

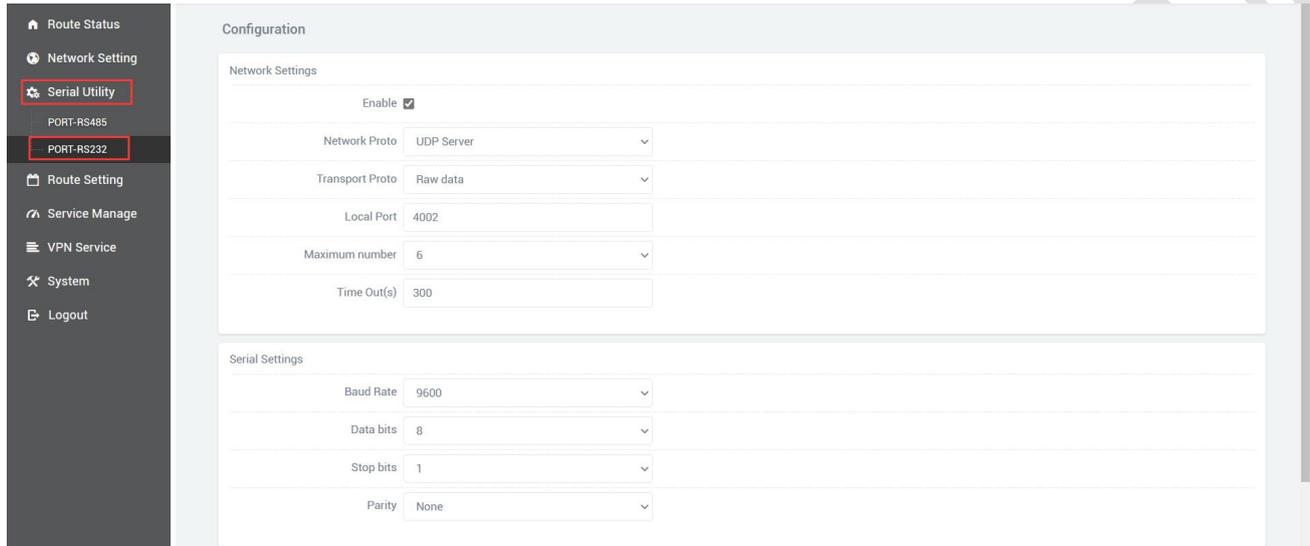


TCP Client and TCP Server send and receive data diagram.



### 3.4 UDP Server

Select "Serial Utility" - "RORT-RS232" in turn, select UDP Server as the network protocol, choose the data type according to your needs. Generally, the choice is Raw data. You need to remember the local port after setting. When establishing a UDP connection, you need to use the IP address and port number of the serial server. The baud rate, data bit, stop bit and parity bit of the serial port are configured according to your needs. After the configuration is complete, click SAVA & APPLY.



Network Settings	
Enable	<input checked="" type="checkbox"/>
Network Proto	UDP Server
Transport Proto	Raw data
Local Port	4002
Maximum number	6
Time Out(s)	300

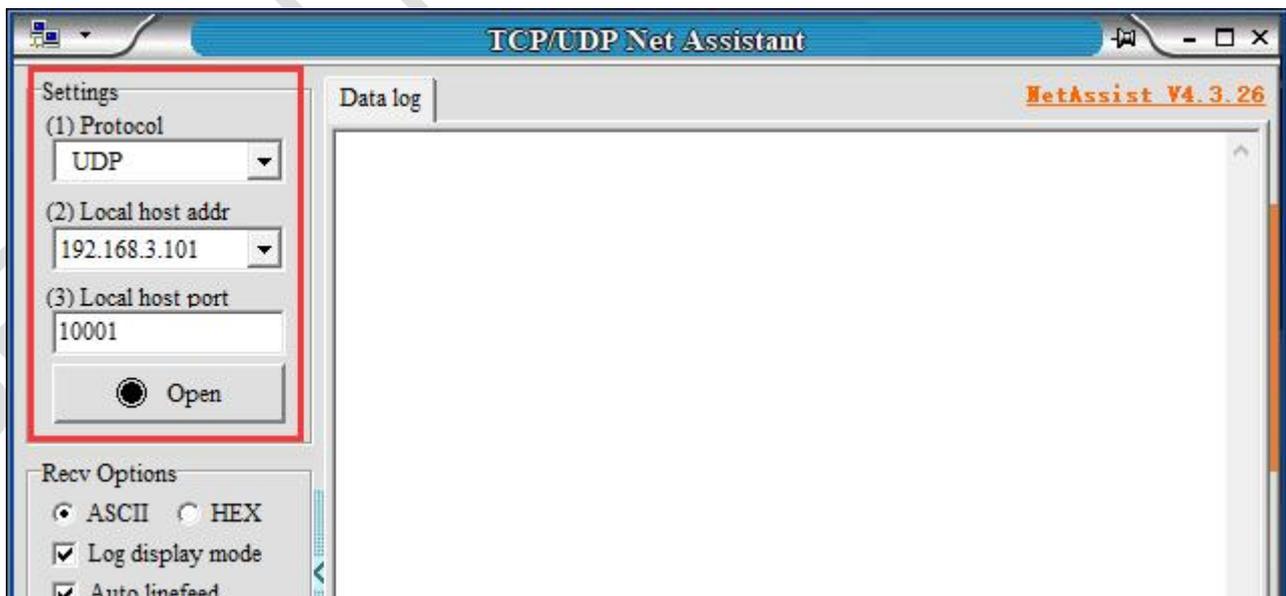
  

Serial Settings	
Baud Rate	9600
Data bits	8
Stop bits	1
Parity	None

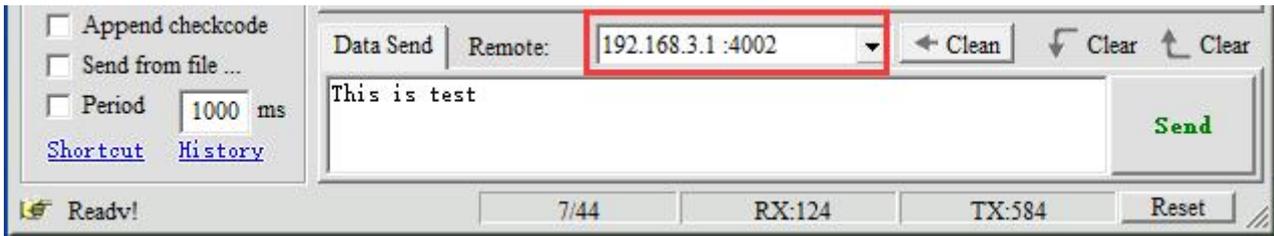
**Maximum number:** The default is 6, which means that up to 6 UDP Clients are supported to connect to the same serial port.

**Time Out (s):** The default is 300, which means that after the UDP Server establishes a connection, if there is no data, the connection will be disconnected after 300 seconds. If you need a permanent online connection, you can set the value to 0.

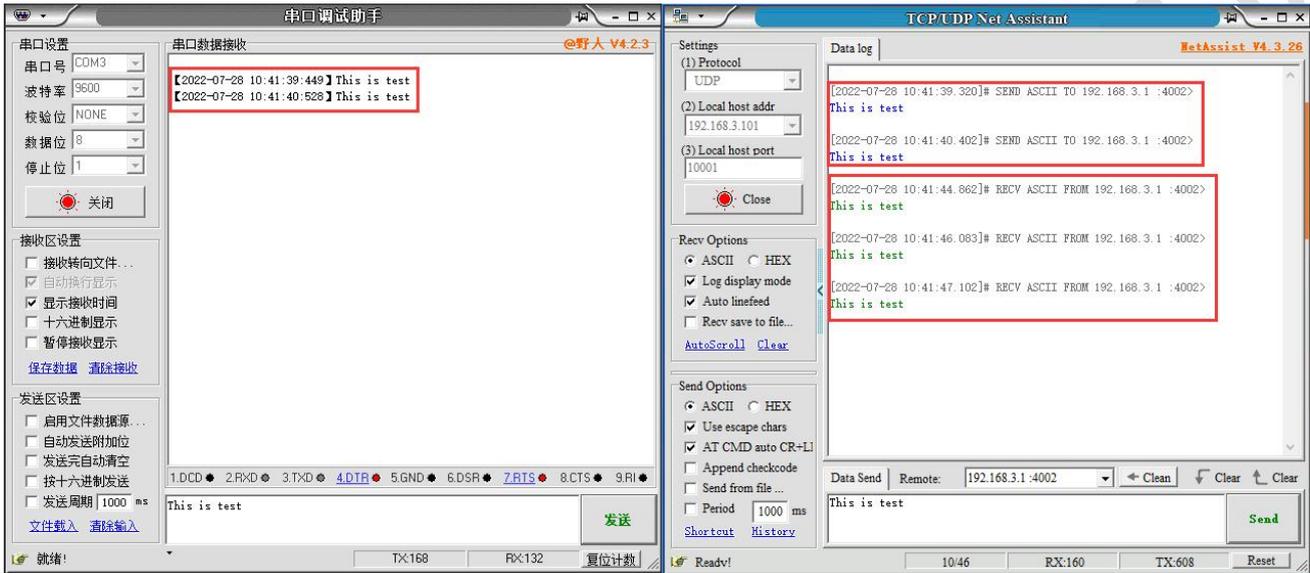
The software settings are as follows, Protocol selects UDP, Local host addr selects the same network segment IP set by the computer and the device, and the Local host port defaults to it. Click Open after setting.



After opening, fill in "192.168.0.233:4002", the server's IP address and port number, separated by ':'.

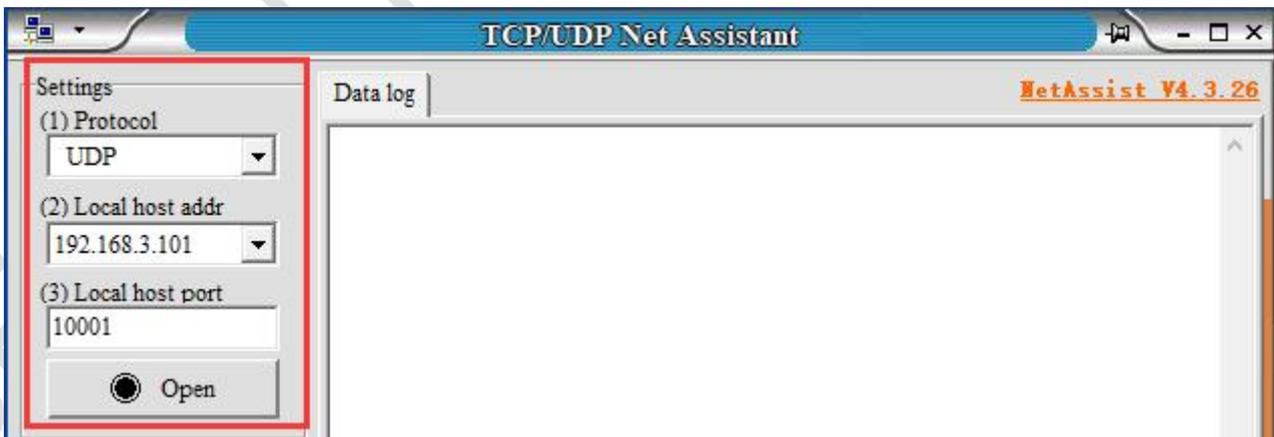


UDP Server and UDP Client send and receive data diagram.



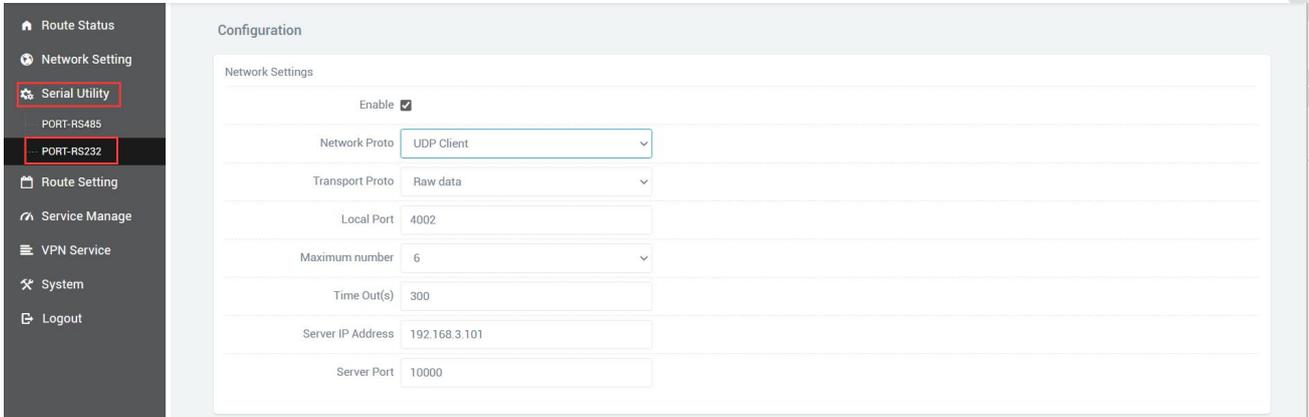
### 3.5 UDP Client

Protocol select UDP, Local host addr select the IP address set by the computer, which is in the same network segment as the device's LAN port IP. The Local host port is the default, and the client settings need to use Local host addr and Local host port,click Open.

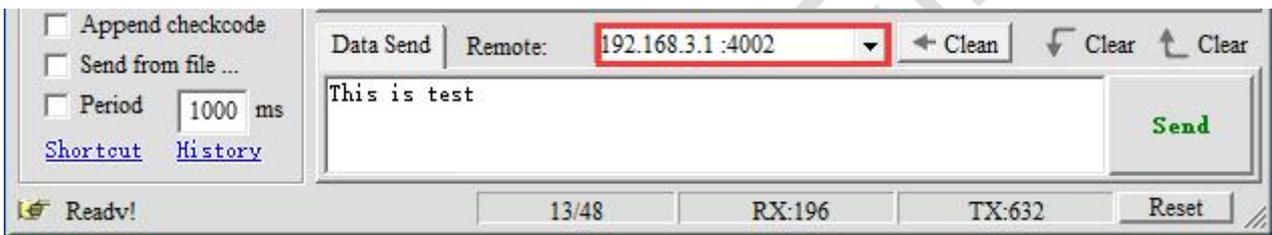


Select "Serial Utility" - "RORT-RS232" in turn,choose UDP Client as the network protocol, and choose the data type according to your needs. Generally, the choice is Raw date. You need to remember the local port after setting. The IP address and port number of the serial port server are used when establishing a UDP connection. Compared with UDP Server, UDP Client has an additional server IP address and server port

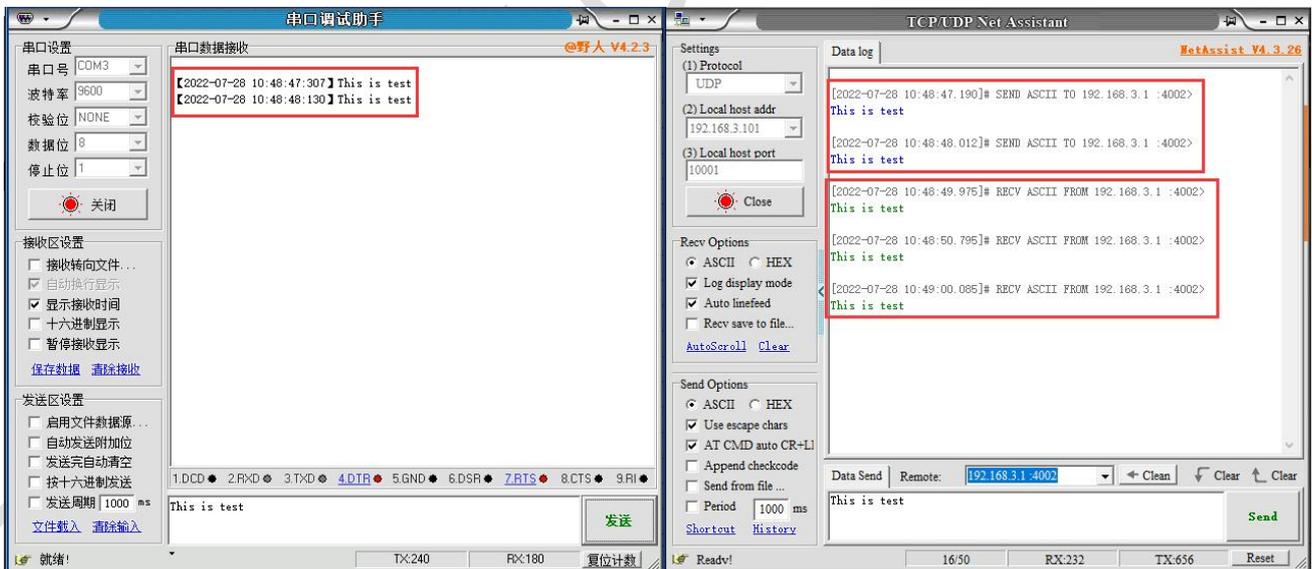
number. The purpose of this addition is to ensure the security of UDP data transmission. Network data only receives data from the server IP and server port number. The rest of the data are denied access. Configure the baud rate, data bit, stop bit and parity bit of the serial port through the serial port configuration bar according to your needs. After the configuration is complete, click SAVA & APPLY.



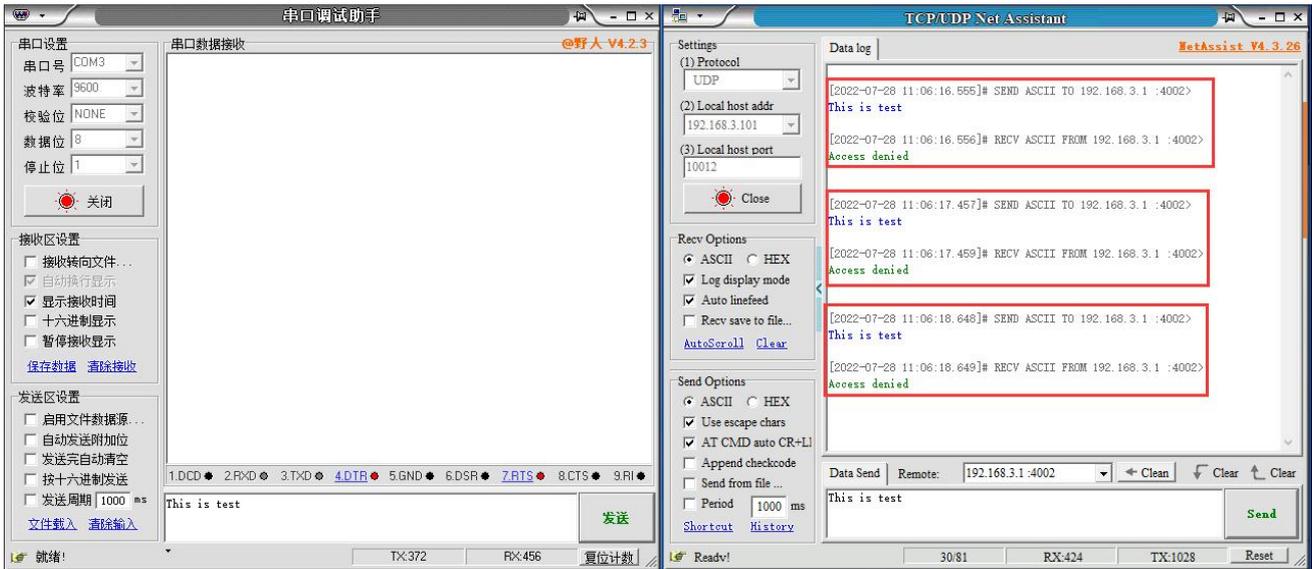
In the next step, the following information needs to be filled in the software.



UDP Client and UDP Server send and receive data diagram,

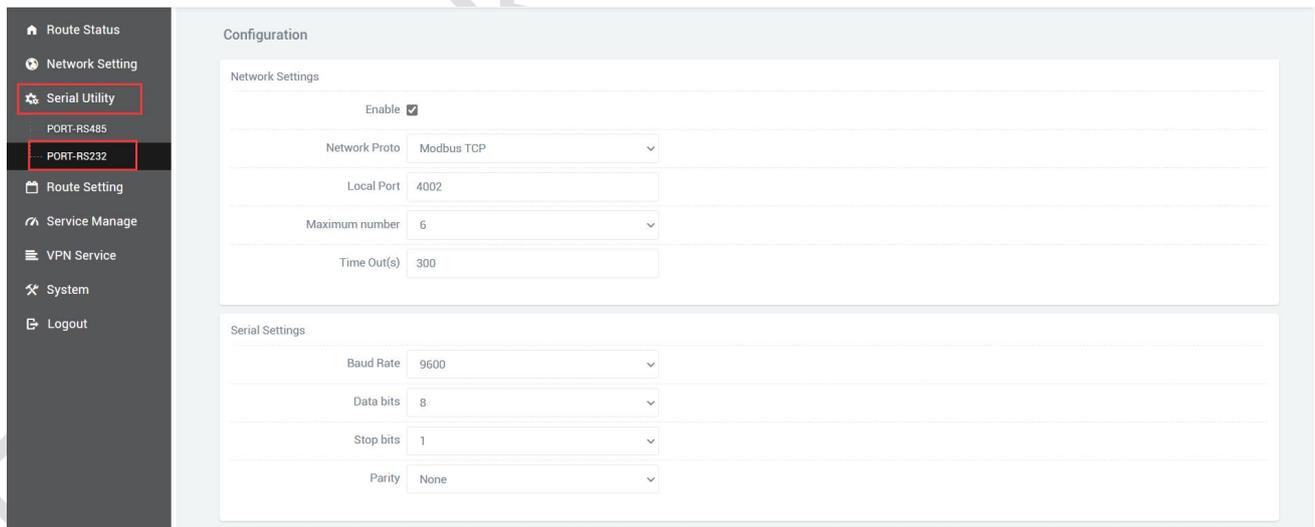


If the data is not sent from the server IP and port, it will be rejected.

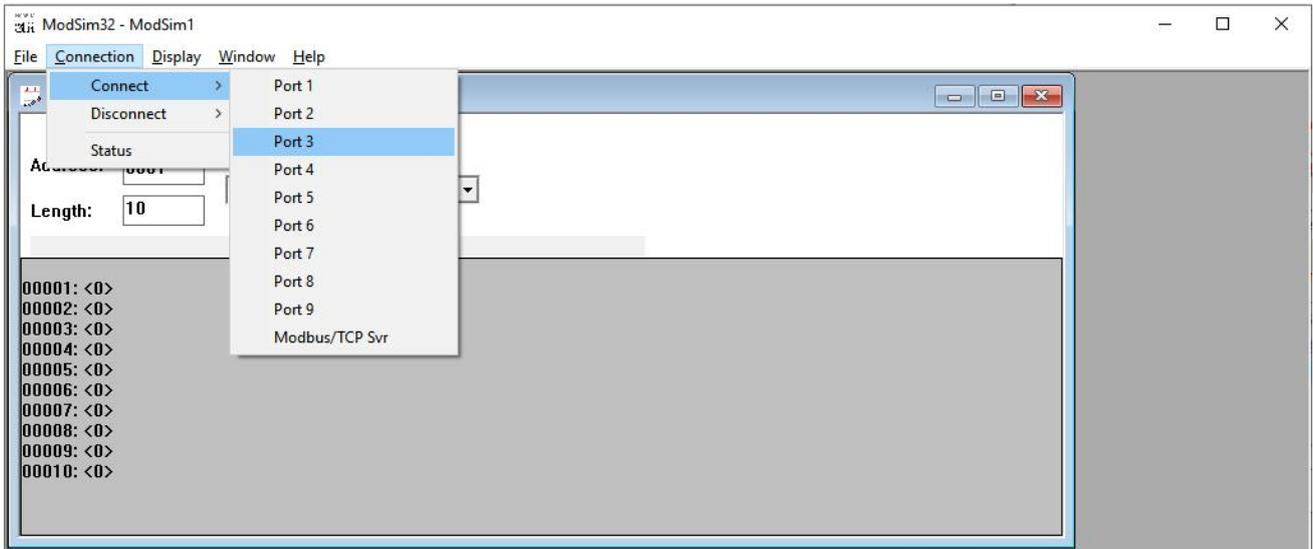


## 3.6 Modbus TCP

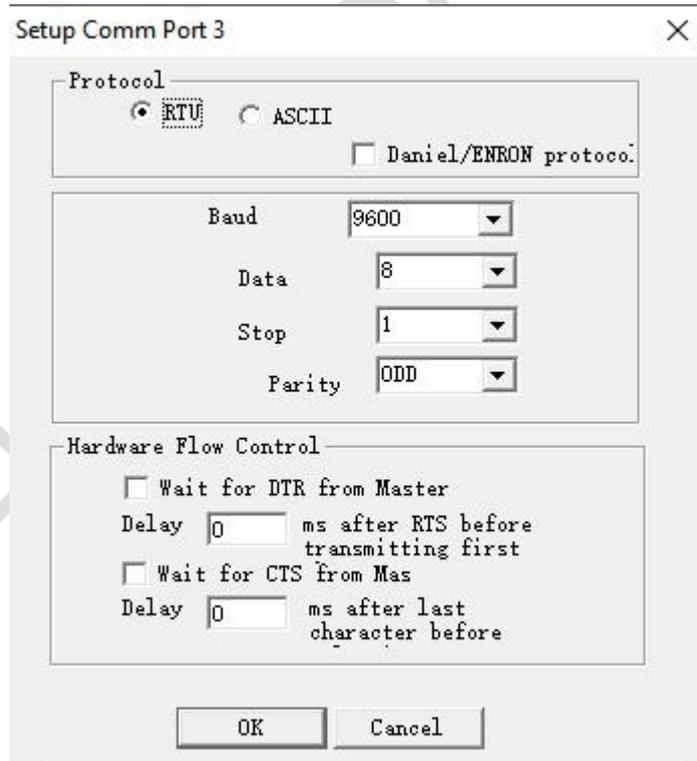
Select "Serial Utility" - "RORT-RS232" in turn, Select Modbus TCP as the network protocol. After setting the local port, remember to configure the baud rate, data bit, stop bit and parity bit of the serial port through the serial port configuration bar according to your needs. After the configuration is complete, click SAVA & APPLY.



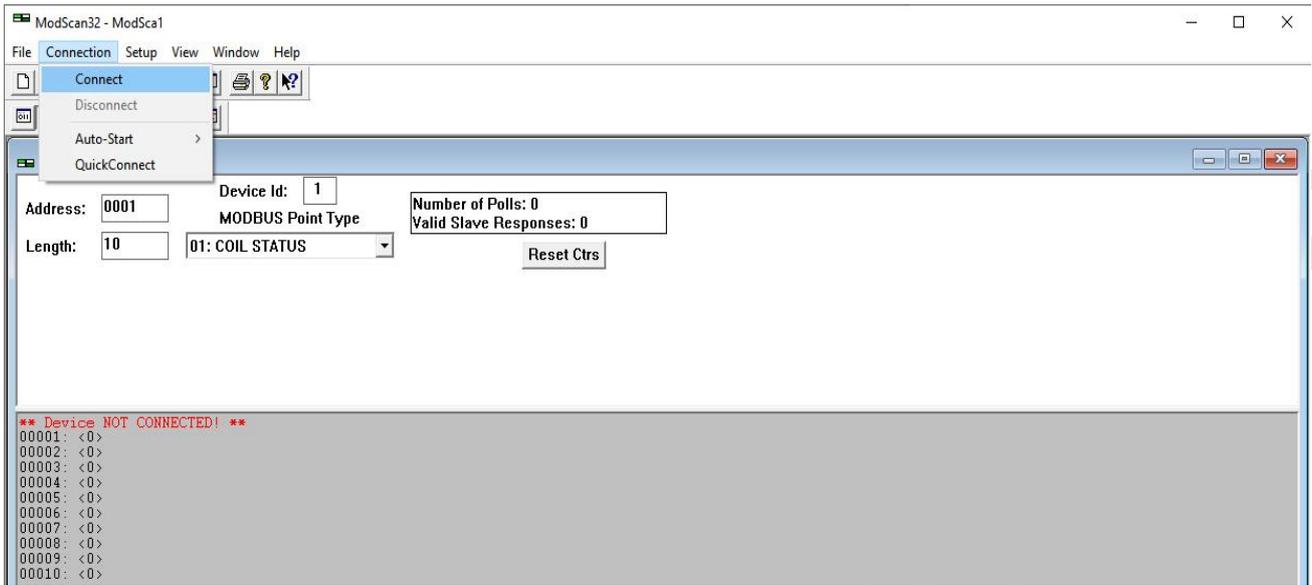
Here you need to use ModSim32.exe and ModScan32.exe to simulate the use, first open the software ModSim32, File>>>New to create a new file, Connection>>>Connect>>>Port 3 (the choice here is the connection between your computer and the device port).



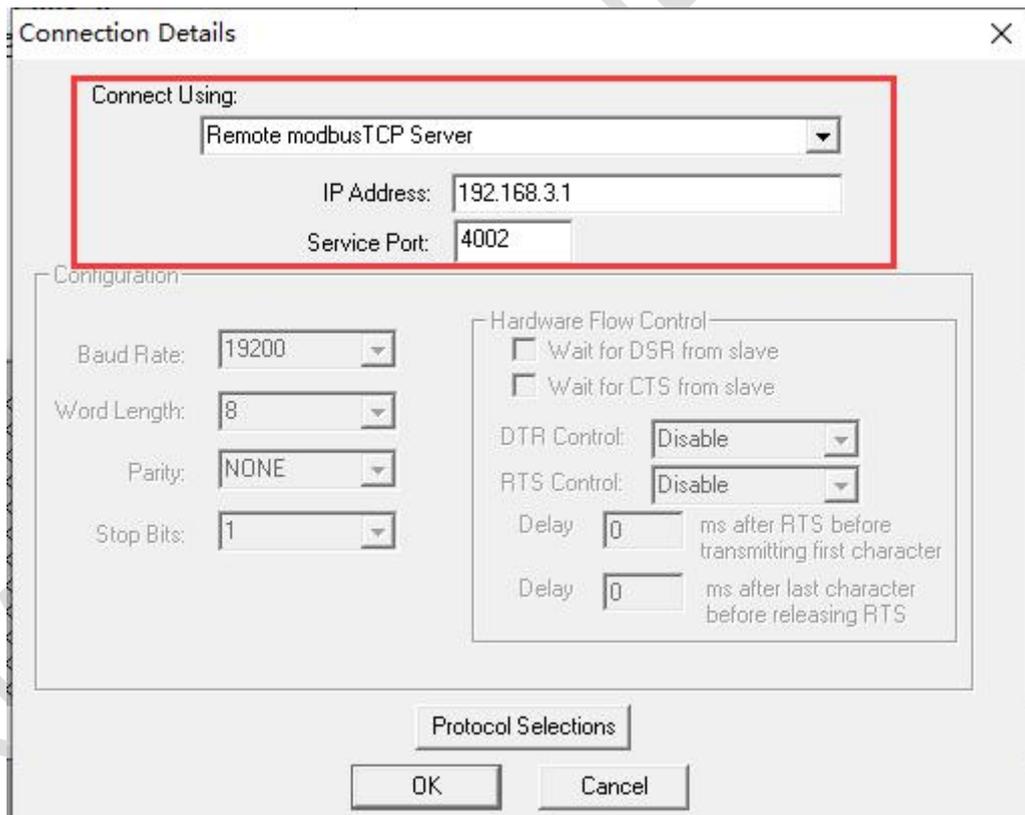
The pop-up dialog box is as follows, the baud rate, data bit, stop bit and parity bit are changed according to the values set on the web page.



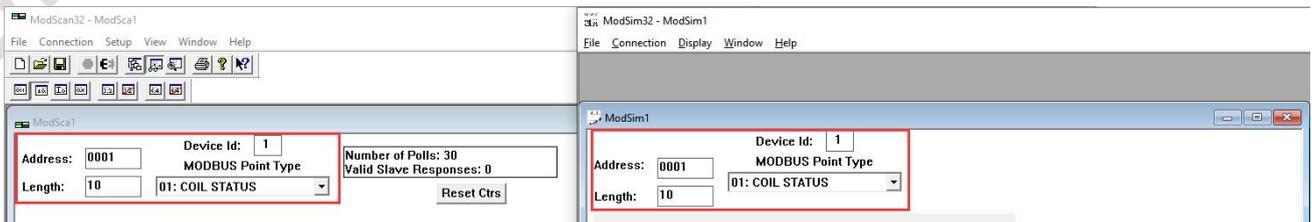
Open the software ModScan32, Connection>>>Connect.



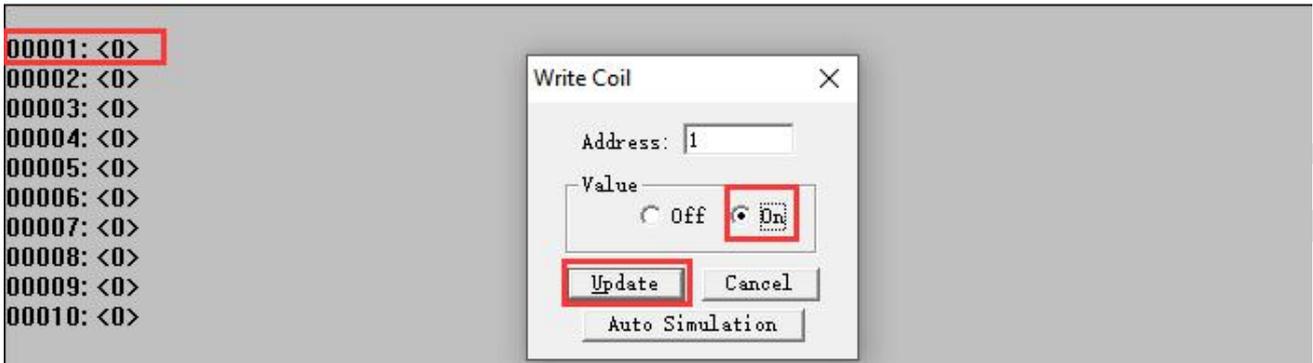
The pop-up dialog box is as follows, select Remote modbusTCP Server, fill in the IP Address and Service Port, and then click OK.



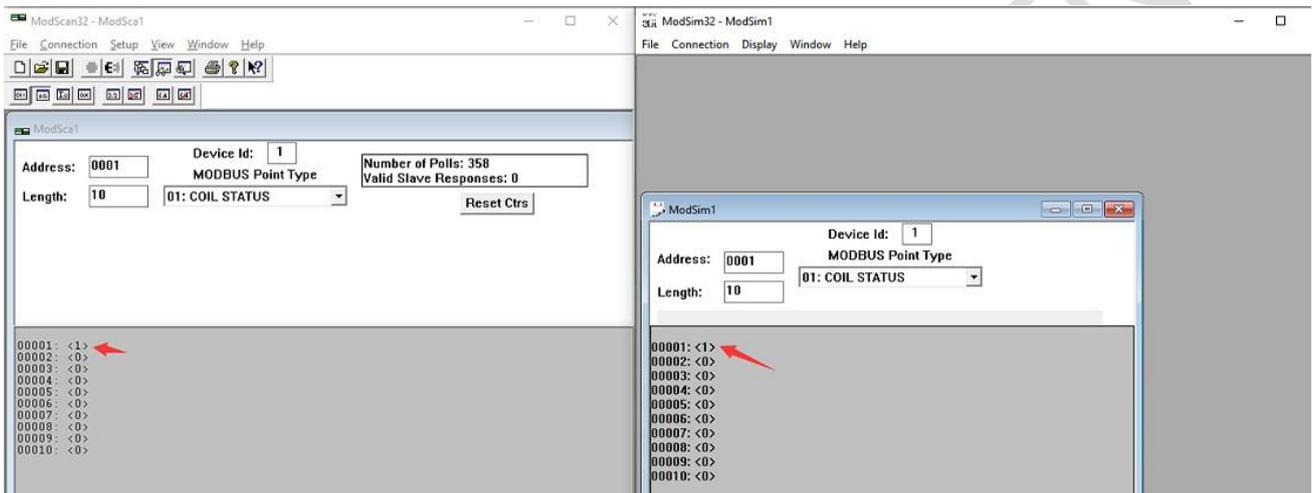
The selected settings in ModSim32 and ModScan32 software need to be consistent.



Double-click 00001: <0> area, a dialog box pops up, select On, and then click Update.

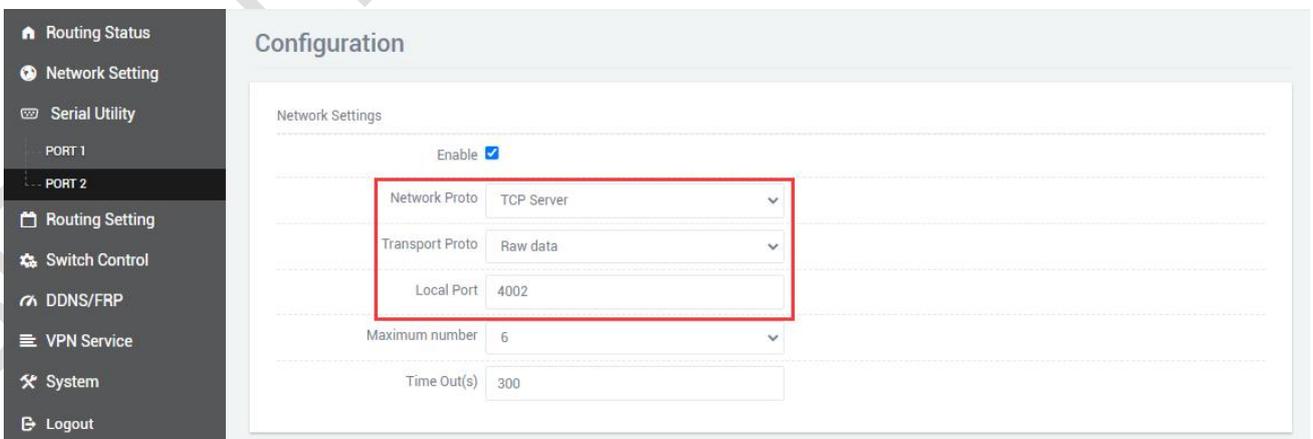


The effect is as follows

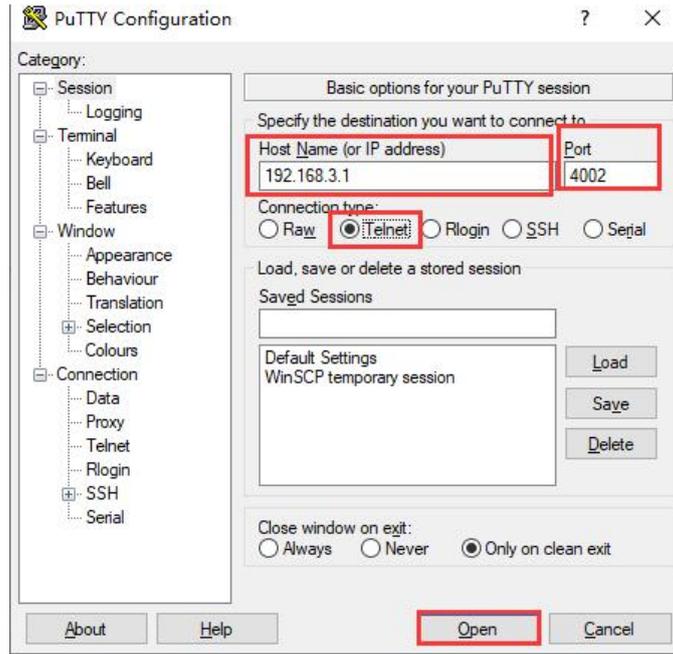


### 3.7 Transport Proto

When selecting TCP Server, the data type also has the option of Telnet (RFC2217), and a software putty.exe is used here. Select "Serial Utility" - "RORT-RS232" in turn, Select TCP Server or UDP Server as the Network Proto, and Telnet (RFC2217) as the Transport Proto. After the configuration is complete, click SAVE & APPLY.



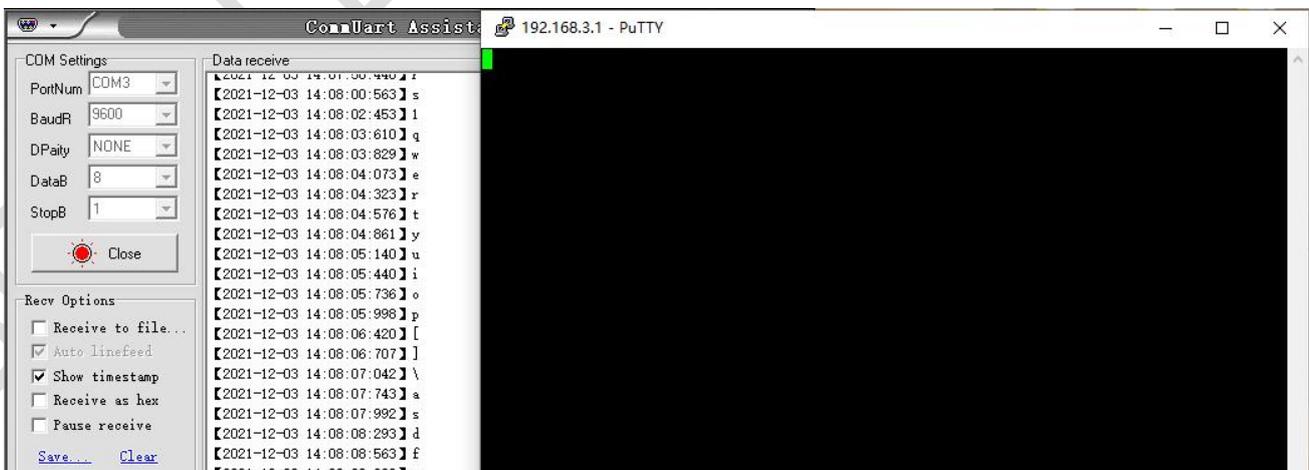
Open the putty.exe software, fill in the server IP address and port number, select Telnet for Connection type, set as follows, click Open after the configuration is complete.



If no error is prompted after opening, a pure black dialog box will be displayed, as shown below.



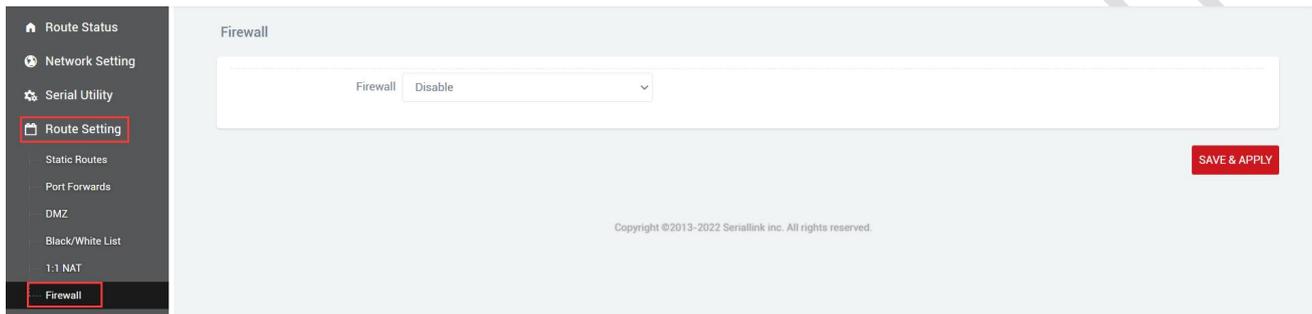
Click the putty dialog box, enter any character, and the result is as follows.



## Chapter 4 Firewall and Application

### 4.1 Firewall on and off

The firewall is enabled by default. When doing DMZ and Port Forwards, you need to disable the firewall. Steps to disable the firewall, go to the navigation bar "Routing Setting" - "Firewall", select disable the firewall, and then click "SAVE & APPLY".



### 4.2 DMZ

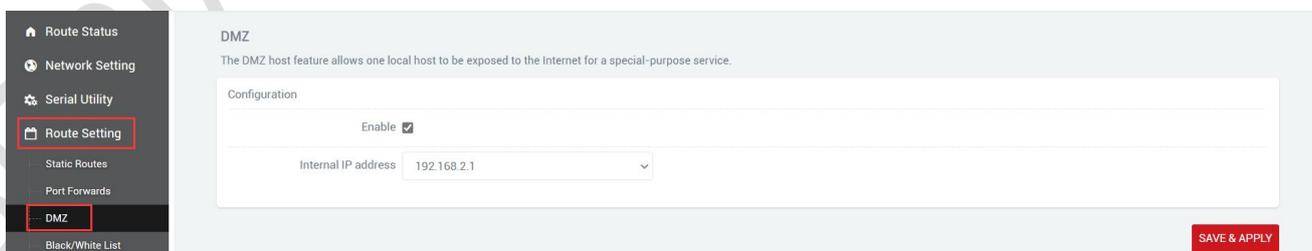
The DMZ function can map the WAN port address to a certain host on the LAN side; all packets to the WAN address will be forwarded to the specified LAN side host to achieve bidirectional communication. In fact, it is to completely expose a host in the intranet to the Internet and open all ports, which is equivalent to all port mapping. It is equivalent to using the public IP directly.

First, you need to disable the firewall, click "Routing Setting" - "DMZ" in the navigation bar, click Enable, set the IP address assigned by the lan port to the connected device, and forward all the ports of the connected device, it can be accessed directly through the IP address of the wan port.

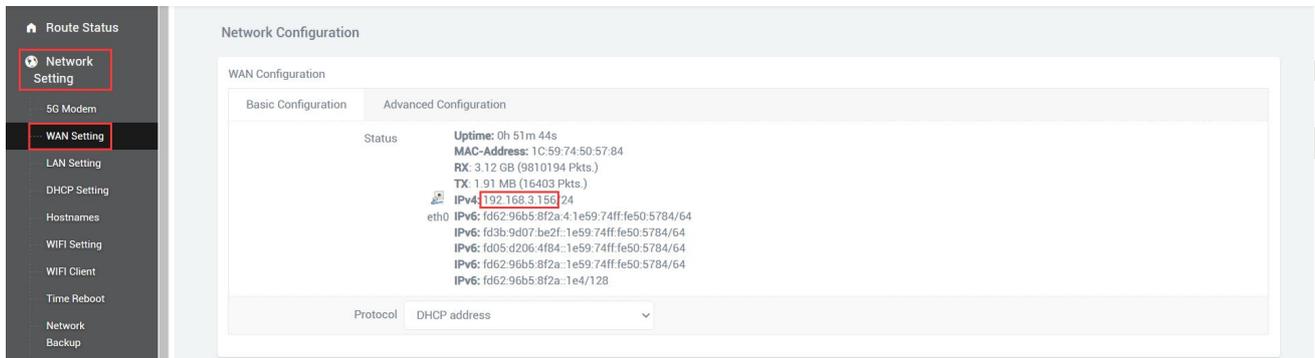
Enable: Tick Enable.

Internal IP address: The ip address of the local device or the ip assigned to the connected device through dhcp.

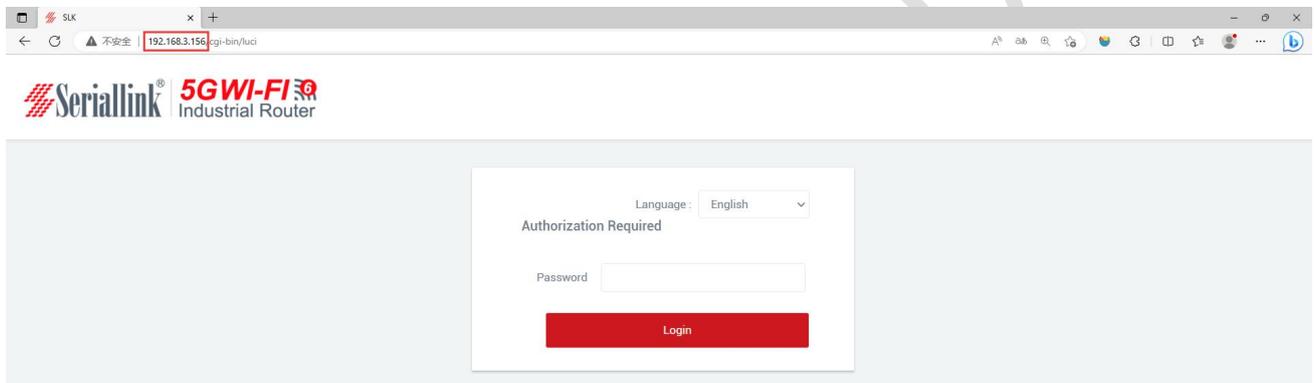
DMZ actually forwards all ports of the device. After the configuration is complete, click "SAVE & APPLY" to make it take effect.



Check the IP of the wan port, you can directly access the connected device through the IP of the wan port. If you can't access it, the possible reason is that the firewall of the connected device is opened, and you need to turn off the firewall of the connected device.



You can access the connected device directly through the IP of the wan port. (Note: The computer needs to be in the same local area network as the IP of the wan port before it can be accessed)



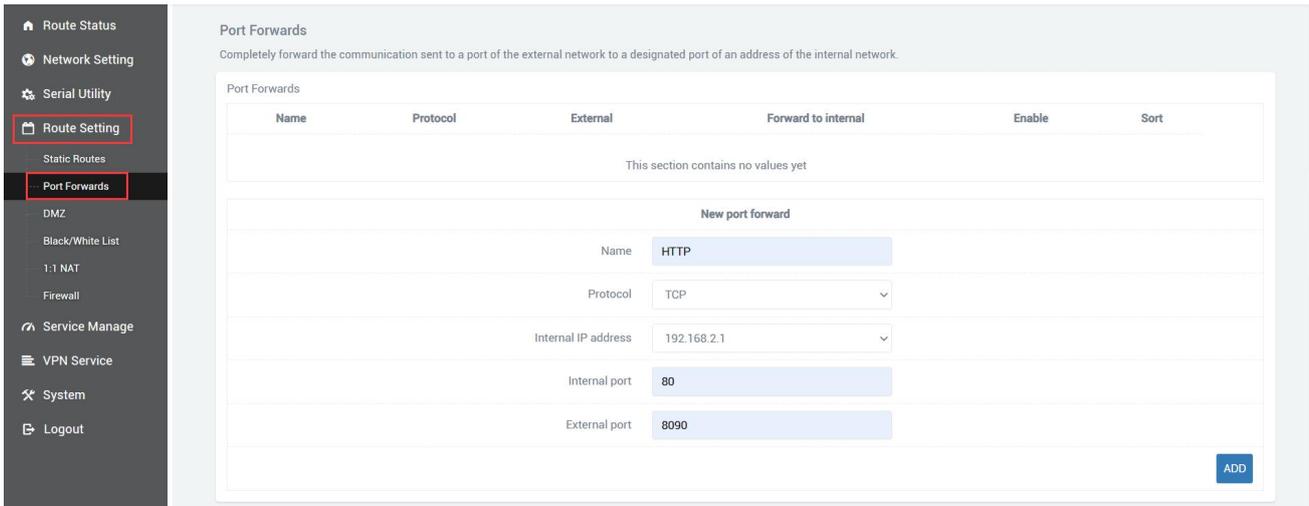
## 4.3 Prot Forwards

Compared with the DMZ, port forwarding is a more refined control, which can forward the data packets sent to a certain port to a certain host on the LAN side, and can realize the transfer of different ports to different hosts.

First you need to disable the firewall.

Navigation bar "Routing Setting" - "Port Forwards" setting menu, enter the "Port Forwards" interface to configure.

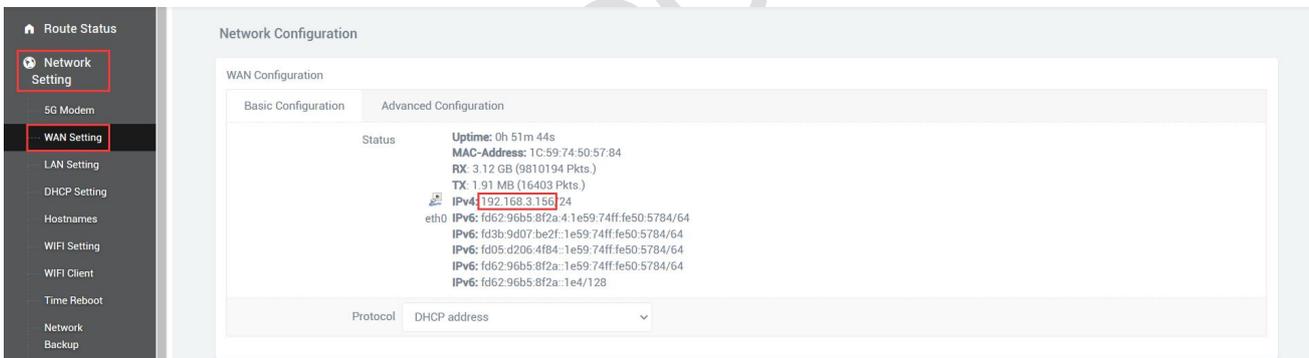
- A.Name: Specify the name of this rule, which can be a meaningful name.
- B.Protocol: Specifies the protocol to be forwarded, which can be TCP, UDP, or TCP/UDP.
- C.Internal IP address: Select the IP address that needs to be forwarded to the external network.
- D.Internall port: The port to be forwarded by the connected device or the machine.
- E.External port: Add this external port through the wan port ip to access the connected device.
- D.After configuration, click the "ADD" button to add a forwarding rule. Click the "SAVE & APPLY" button to make the rule take effect.



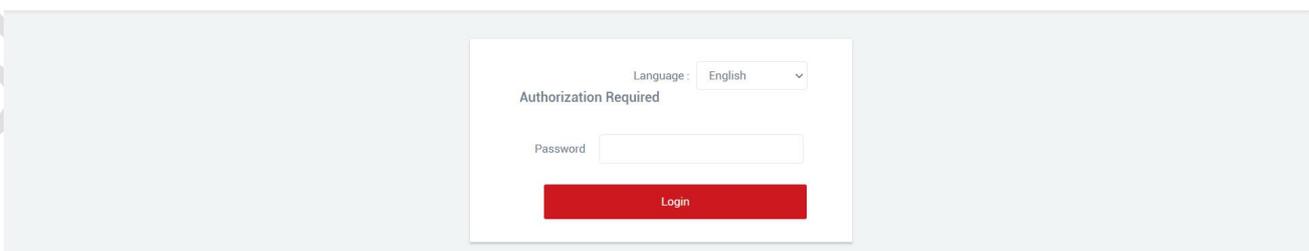
After the addition is successful, a port forwarding rule will be added. Click "SAVE & APPLY" to make the rule take effect. Multiple rules can be added.



View the wan port ip, and access the internal port of the connected device or the local device through the wan port ip and external port number.



Access the internal port of the connected device through 192.168.3.156:8090. (Note: The computer needs to be in the same local area network as the IP of the wan port before it can be accessed)



## 4.4 Black/White List

### 4.4.1 White List

Restrict all non-whitelisted hosts from accessing the external network through the local device. For example, all devices cannot access the Internet, and only a certain computer can be allowed, then this computer can be added to the whitelist.

A.Name: Customize the name.

B.Protocol: All protocols are selected by default, choose according to your needs.

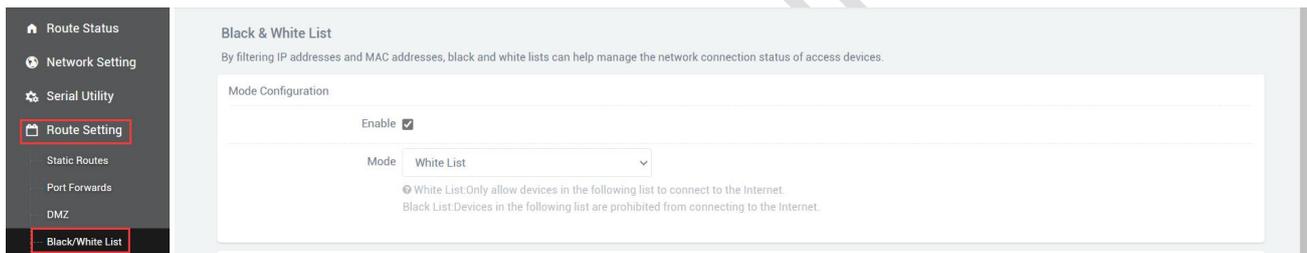
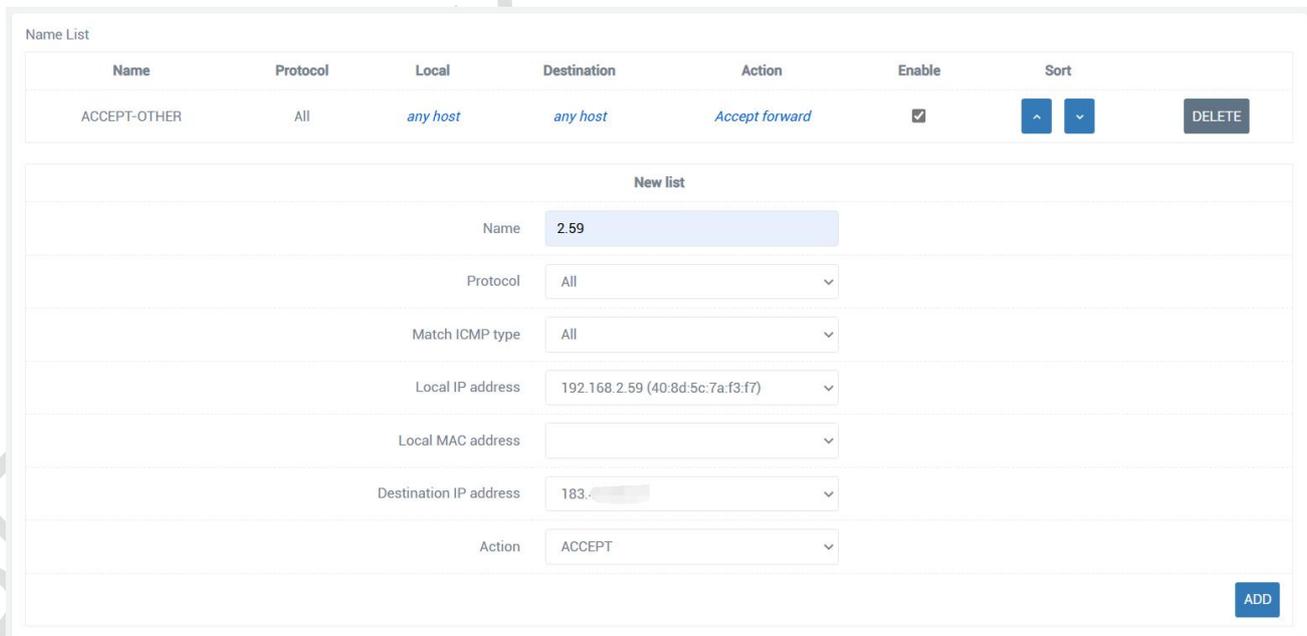
C.Match ICMP type: All types are selected by default, choose according to your needs.

D.Local IP address: The IP address of the device added to the whitelist, the IP address change caused by man-made or other reasons, will change the device that can access the Internet.

E.Local MAC address: The MAC address of the device added to the whitelist will not be invalid even if the device IP address is changed.

F.Destination IP address: If not selected, it means all networks. You can also enter an IP address, such as the public network server IP.

G.Action: Whitelist mode select ACCEPT.

Name	Protocol	Local	Destination	Action	Enable	Sort
ACCEPT-OTHER	All	any host	any host	Accept forward	<input checked="" type="checkbox"/>	▲ ▼

Name List	
Name	2.59
Protocol	All
Match ICMP type	All
Local IP address	192.168.2.59 (40:8d:5c:7a:f3:f7)
Local MAC address	
Destination IP address	183.
Action	ACCEPT

After clicking Add, a rule will be automatically refreshed in the page list, click "SAVE & APPLY".

Name	Protocol	Local	Destination	Action	Enable	Sort
2.59	All	IP 192.168.2.59	IP 183. [redacted]	Accept forward	<input checked="" type="checkbox"/>	<div style="display: flex; align-items: center;"> <span>▲</span> <span>▼</span> </div>

After adding the whitelist, you can only access the public network address of the server, but cannot access the Internet. At the same time, other computers can neither access the public network address nor the Internet.

```
C:\Users\Administrator>ping 183.[redacted]

Pinging 183.[redacted] with 32 bytes of data:
Reply from 183.[redacted]: bytes=32 time=3ms TTL=62
Reply from 183.[redacted]: bytes=32 time=2ms TTL=62
Reply from 183.[redacted]: bytes=32 time=2ms TTL=62
Reply from 183.[redacted]: bytes=32 time=2ms TTL=62

Ping statistics for 183.[redacted]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\Administrator>ping www.baidu.com

Pinging www.a.shifen.com [14.215.177.38] with 32 bytes of data:
Reply from 192.168.2.1: Destination port unreachable.

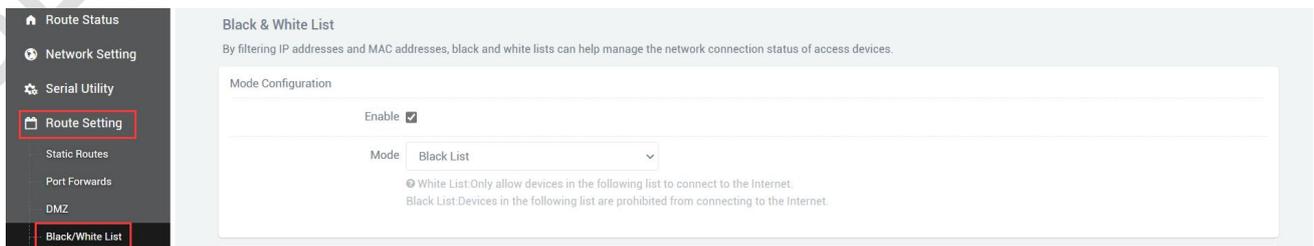
Ping statistics for 14.215.177.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

If the target address is empty, it means that the devices in the whitelist can access all networks, but other devices cannot. If you want to disable the blacklist and whitelist functions, you just need to uncheck the "SAVE & APPLY" option.

### 4.4.2 Black List

Restrict the host in the blacklist from accessing the external network through the local device. For example, if a computer is prohibited from accessing the Internet, the computer can be added to the blacklist.

- A.Name: Customize the name.
- B.Protocol: All protocols are selected by default, choose according to your needs.
- C.Match ICMP type: All types are selected by default, choose according to your needs.
- D.Local IP address: The IP address of the device added to the blacklist, the IP address change caused by man-made or other reasons, will change the device that refuses to access the Internet.
- E.Local MAC address: The MAC address of the device added to the blacklist will not be invalid even if the device IP address is changed.
- F.Destination IP address: If not selected, it means all networks. You can also enter an IP address, such as the public network server IP.
- G.Action: Blacklist mode select REJECT.



Name List

Name	Protocol	Local	Destination	Action	Enable	Sort
This section contains no values yet						

New list

Name: 2.59

Protocol: All

Match ICMP type: All

Local IP address: 192.168.2.59 (40:8d:5c:7a:f3:f7)

Local MAC address:

Destination IP address: 183.

Action: REJECT

ADD

After clicking Add, a rule will be automatically refreshed in the page list, click "SAVE & APPLY".

Name List

Name	Protocol	Local	Destination	Action	Enable	Sort
2.59	All	IP 192.168.2.59	IP 183.	Refuse forward	<input checked="" type="checkbox"/>	▲ ▼

DELETE

After adding the blacklist, you cannot access the public address of the server, only the Internet, and other devices are not restricted.

```
C:\Users\Administrator>ping www.baidu.com

Pinging www.a.shifen.com [14.215.177.39] with 32 bytes of data:
Reply from 14.215.177.39: bytes=32 time=10ms TTL=54
Reply from 14.215.177.39: bytes=32 time=9ms TTL=54
Reply from 14.215.177.39: bytes=32 time=10ms TTL=54
Reply from 14.215.177.39: bytes=32 time=9ms TTL=54

Ping statistics for 14.215.177.39:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 10ms, Average = 9ms

C:\Users\Administrator>ping 183.

Pinging 183. with 32 bytes of data:
Reply from 192.168.2.1: Destination port unreachable.

Ping statistics for 183.:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

If the destination address is empty, it means that the devices in the blacklist cannot access all external networks. If you want to disable the blacklist and whitelist function, just uncheck the enabled option, "SAVE & APPLY".

# Chapter 5 Service Manage

## 5.1 Remote management - CWMP

CWMP uses TR069 data transmission protocol, which can be used with Sinolink remote management platform, which can realize remote operations such as restart, upgrade, and configuration. The TR069 configuration parameters need to be consistent with the server.

- Route Status
- Network Setting
- Serial Utility
- Route Setting
- Service Manage
- CWMP
- SNMP
- Dynamic DNS
- Ftp Client
- VPN Service
- System
- Logout

### CWMP

General Settings
Physical Settings

Enable <input checked="" type="checkbox"/>	
Port	7547
Username	cpe
Password	...
Authentication	Digest
Provisioning code	
Serialnumber	
Logging level	Info

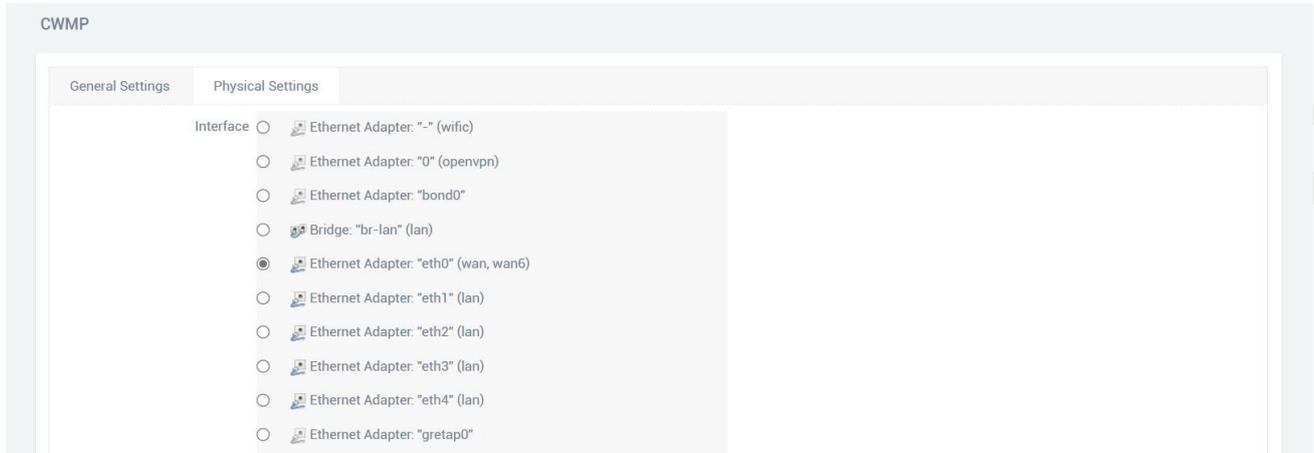
### STUN Settings

STUN Enable <input checked="" type="checkbox"/>	
STUN ServerAddress	192.168.16.248
STUN ServerPort	10011
STUN ServerUsername	stunuser
STUN ServerPassword	.....
STUN ServerMax Keepalive Period	30
STUN ServerMin Keepalive Period	5
STUN ServerKeepalive Period	5

### ACS Settings

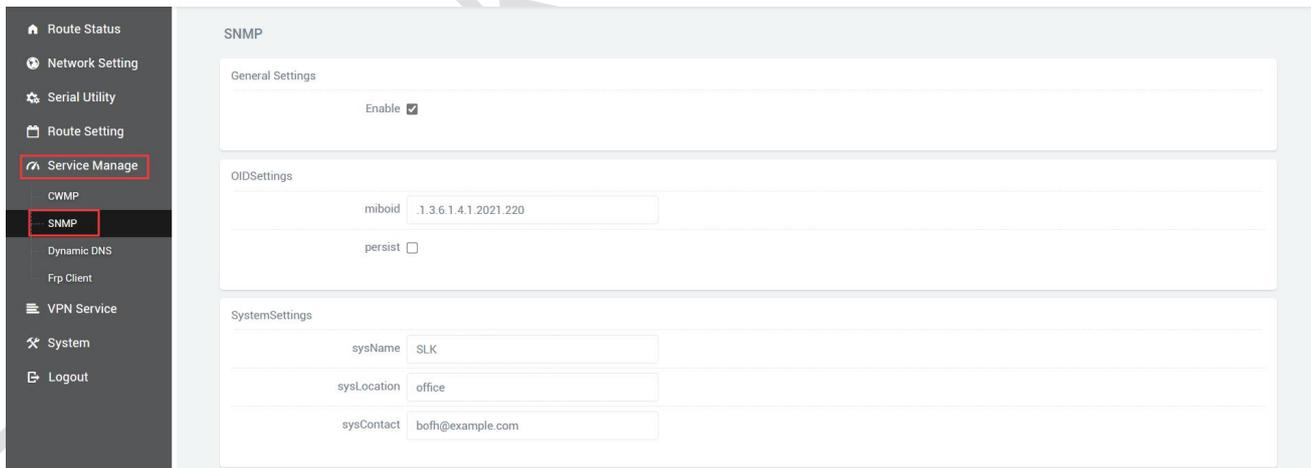
ACS URL	http://192.168.16.248:10090/acs
Username	easycwmp
Password	.....
Parameter key	unsetCommandKey
Periodic enable	<input checked="" type="checkbox"/>
Periodic interval	600

The interface in the physical settings is selected as the network interface connected to the server, such as eth0 for WAN port network and USB0 for 4/5G network.



## 5.2 Remote management - SNMP

SNMP is a data transmission protocol that can be used with Sinolink remote management platform to realize remote operations such as restart, upgrade, and configuration. Unlike TR069, the SNMP protocol requires that the device and the server are interoperable, both parties can initiate UDP connection, suitable for the internal network, although the network requirements are high, but the configuration is quite simple, as long as you check the enable can be used, of course, the server needs to enter the current device, it should be noted that the miboid can not be changed (the default is .1.3.6.1.4.1.2021.220), otherwise the Sinolink remote management platform will not get any information of the device.



## 5.3 Frp Client

Frp is to provide http or https services in multiple external network environments by using machines behind the intranet or firewall. For http, https services support domain name-based virtual hosts, and support custom domain name binding, so that multiple domain names share one port 80; Use

the machine behind the intranet or firewall to provide tcp and udp services to the external network environment, such as accessing the host in the company's intranet environment through ssh at home.

The main functions of frp: the external network accesses the internal network machine through ssh; the external network accesses the port forwarded by the internal network machine through frp through the public network address plus the port number; custom binding domain name accesses the internal network web service.

The premise of configuring intranet penetration is to ensure that the router can access the Internet. If the router cannot access the Internet, the intranet penetration cannot be performed. Navigation bar "Device Management" - "Diagnosis"; and disable the firewall, navigation bar "Routing Setting" - "Firewall".

If you can ping 8.8.8.8, it means that the device can access the Internet. For details, see Chapter 2.9. Disable the firewall. After choosing to disable the firewall, click "SAVE & APPLY".

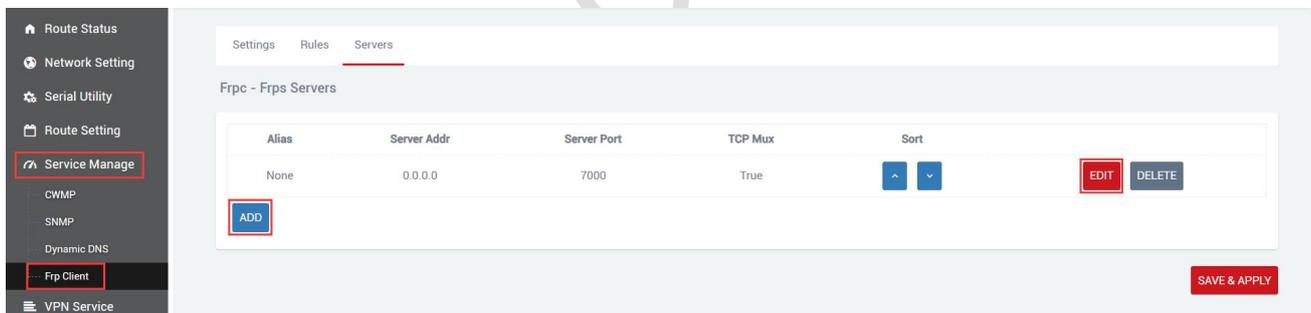
### 5.3.1 Connect to Frps

Preparation before configuration:

- (1) One public network server.
- (2) One router (a router that supports frp, that is, 1 intranet server).
- (3) One domain name is bound to the public network server.

The frp client configuration is as follows:

(1) The client needs to add the configuration of the server first to connect to the server, the navigation bar "DDNS/FRP" - "Frp Client", select "Servers", There is an empty server by default, you can directly click to modify it, or you can directly delete it and add one yourself.



Alias	Server Addr	Server Port	TCP Mux	Sort	
None	0.0.0.0	7000	True	~ v	EDIT DELETE

(2) After clicking "ADD" or "EDIT", a page for editing the frps server will pop up, configure it according to the settings of the server, and click "SAVE & APPLY" after the configuration is complete.

- A. Alias: To customize the name of a server, you can define a meaningful name.
- B. Server addr: The address of the server (usually the public IP address).
- C. Server port: The port set by the server.
- D. Token: The password set by the server.
- E. TCP mux: View and view are consistent with the server side. If the server side TCP mux is true, you need to choose here, if not, you don't need to choose.
- F. Click "SAVE & APPLY" after the setting is complete.

Settings Rules Servers

Frpc - Edit Frps Server

Alias	frpc
Server addr	120.0.0.0
Server port	5443
Token	*****
TCP mux	<input type="checkbox"/>

(3)After the addition is successful, there will be an additional frp server, click "SAVE & APPLY" to start the server.

Settings Rules Servers

Frpc - Frps Servers

Alias	Server Addr	Server Port	TCP Mux	Sort	
None	0.0.0.0	7000	True	^ v	EDIT DELETE
frpc	120.48.120.113	5443	True		EDIT DELETE

ADD

(4)Next, go to the "Settings" page of "Frp Client", start the frpc client, and configure as shown below. After the configuration is complete, click "SAVE & APPLY". After the configuration is complete, "Running" will appear on the "Common Settings" page,prove that the frp client has been started.

- A.Enable: Tick Enabled.
- B.Server: The server alias you just customized.
- C.Run daemon as user: Generally choose the default, you can modify it according to your needs.
- D:Enable logging: Tick as required.
- E:After the configuration is complete, click "SAVE & APPLY".

Settings Rules Servers

Frpc - Common Settings

Frp is a fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet.

Not Running

General Options	Advanced Options
Enabled <input checked="" type="checkbox"/>	
Server	frpc
Run daemon as user	-- default --
Enable logging	<input type="checkbox"/>

Displaying that the service is running indicates that the frp client has been successfully started.

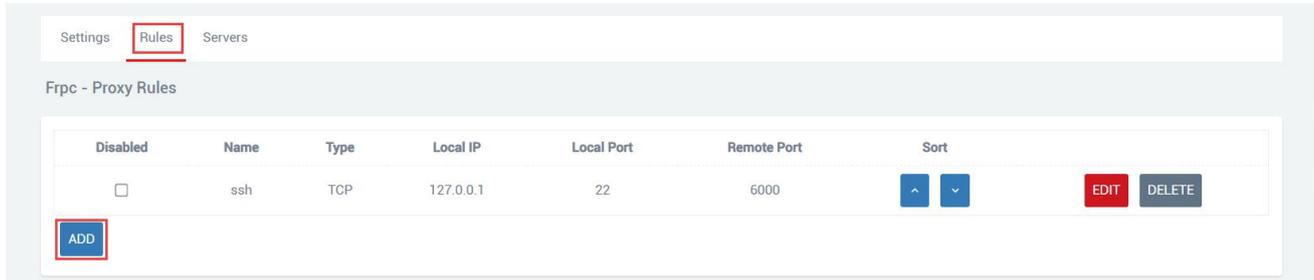
Settings Rules Servers

Frpc - Common Settings

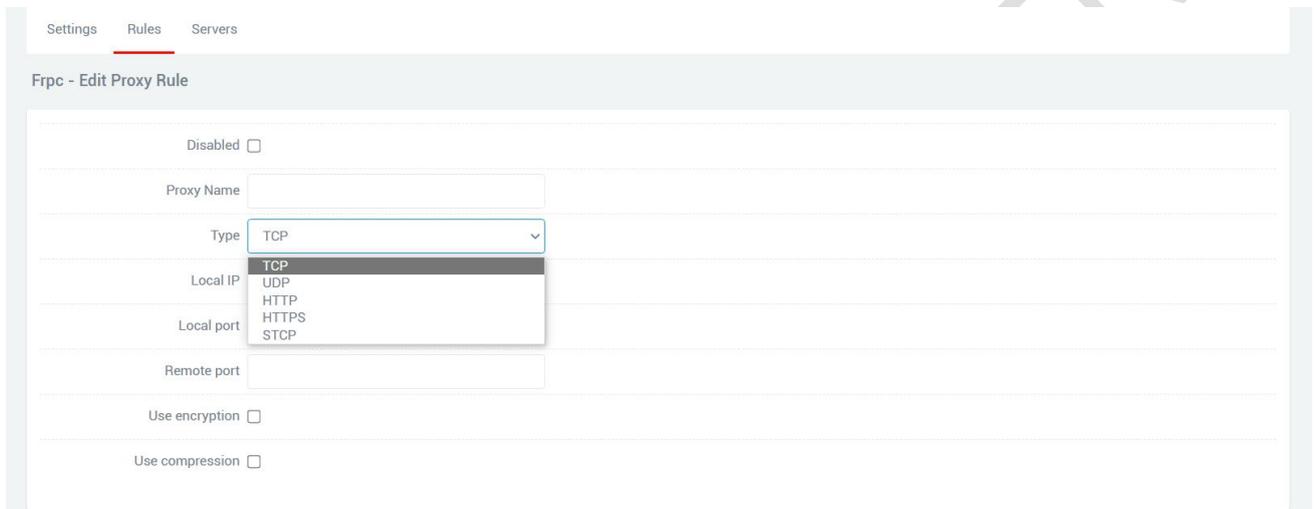
Frp is a fast reverse proxy to help you expose a local server behind a NAT or firewall to the internet.

Running

(5)Next, go to the "Rules" page of "Frp Client", click "ADD", there is a rule by default, if you don't need this rule, you can delete this rule, keep it if you need it, and add a new rule directly.



(6)After adding, an "Edit Proxy Rule" page will pop up, there will be different protocol types, and the functions implemented by different protocol types are different.



### 5.3.2 Add TCP proxy protocol

The TCP protocol supports ssh connection, and also supports forwarding the page port (usually port 80)Through the public network, the remote port can access the page of the local device.

On the "Edit Proxy Rule" page, configure according to the requirements as shown in the figure below. After the configuration is completed, click "SAVE & APPLY", and you will return to the "Proxy Rules" page, and there will be an additional rule on the page,click "SAVE & APPLY" again to make the rule take effect. Finally, you can access the local port opened by the local device through the public network ip: port number (format: 106.107.108.109:5555, where 106.107.108.109 is the public network address). You can add multiple tcp rules, just make sure that the remote ports are not the same. If the remote ports are the same as the previous ones, the latest ones will overwrite the previous ones, and the previous rules will not take effect.

A.Disabled: If checked, it means to disable this rule.

B.Proxy Name: Customize a proxy name. The proxy name cannot be repeated, otherwise it will not take effect due to name conflict.

C.Type: Select the TCP protocol.

D:Local IP: Fill in the ip of the local machine or the ip allocated by the lan port of the local machine for the connected device. (The ip address of the device that needs to be accessed through the public network).

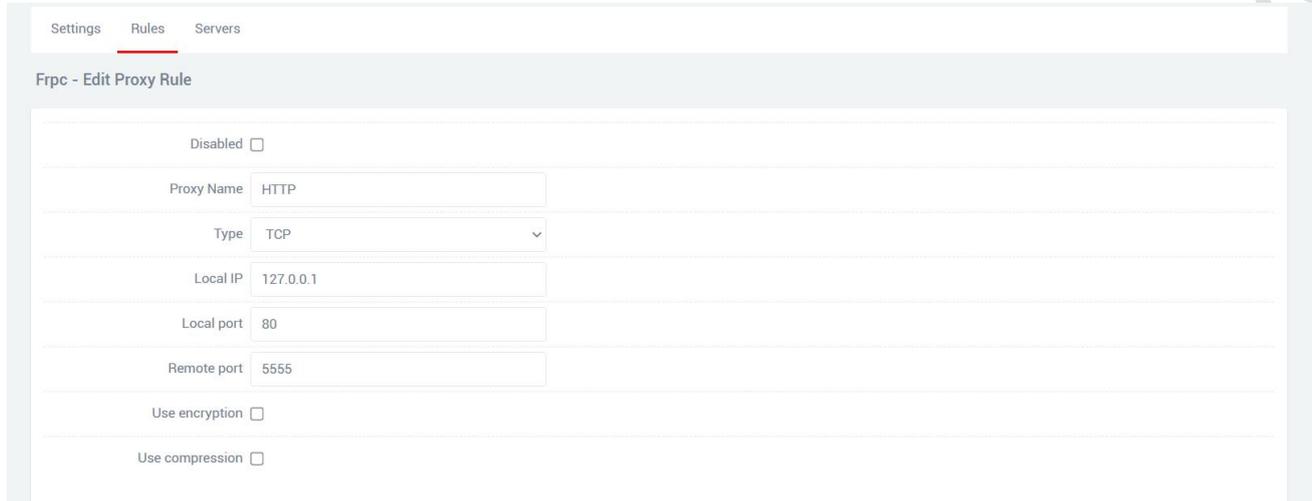
E.Local port: The selected device needs to be forwarded to the port of the public network.

F.Remote port: Add this remote port to the public network address to access the local port opened by the corresponding local device. This port number should not be the same as other rules, and do not use the occupied port, otherwise this rule will not take effect.

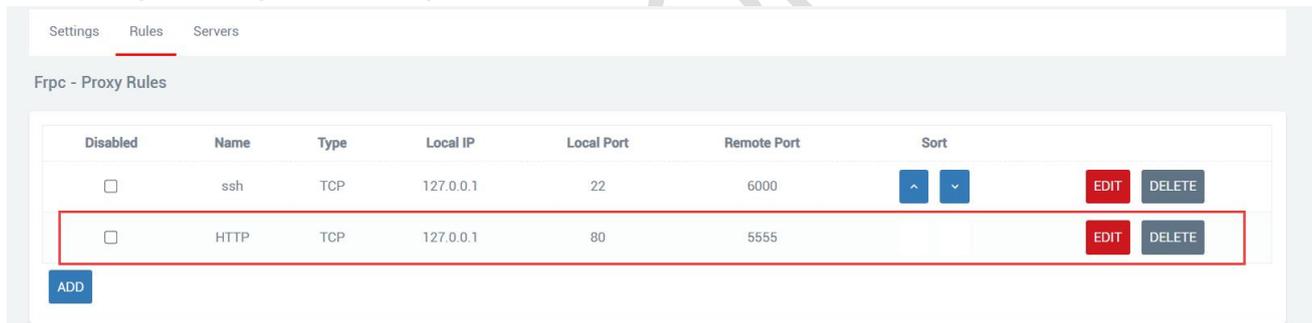
G.Use encryption, Use compression: Check these two as needed.

Multiple rules can be added, as long as the remote port numbers do not conflict.

After the configuration is complete, click "SAVE & APPLY".

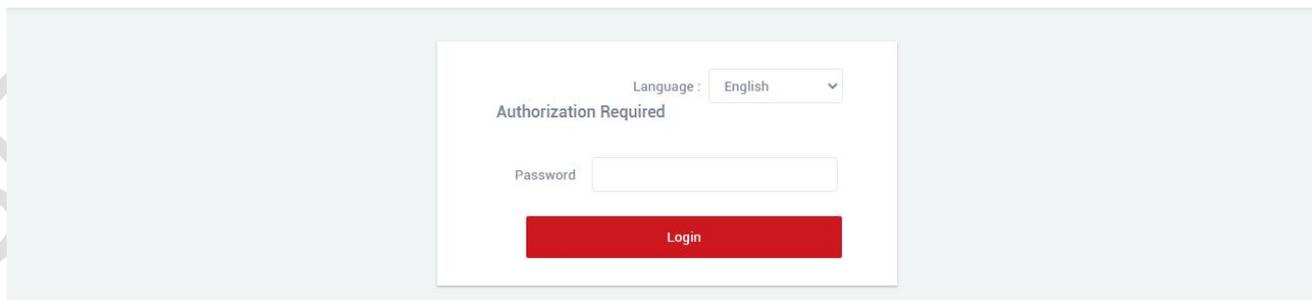
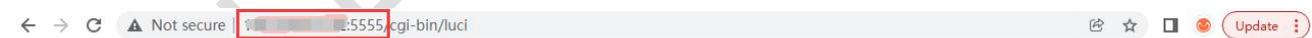


After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.



Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	^ v	EDIT DELETE
<input type="checkbox"/>	HTTP	TCP	127.0.0.1	80	5555		EDIT DELETE

Access the local port of the local device through the public network ip and port number, and 106.107.108.109:5555 to access 192.168.2.1 (default port 80).



Multiple tcp rules can be added. It is necessary to ensure that the remote port number and proxy alias are not repeated with those previously set. If they are repeated, the rule may not take effect even if it exists.

### 5.3.3 Add STCP Proxy Rules

(1)STCP needs to configure the client and the access terminal, of which 192.168.2.111 (the device connected to the lan port) is used as the client, and the PC is used as the access terminal. The access terminal can access the client by binding the local IP and port.

A.Disabled: Checking here will disable this rule.

B.Proxy Name: Customize a proxy name, which cannot be the same as other rules, otherwise it will not take effect due to conflict.

C.Type: Select the STCP protocol.

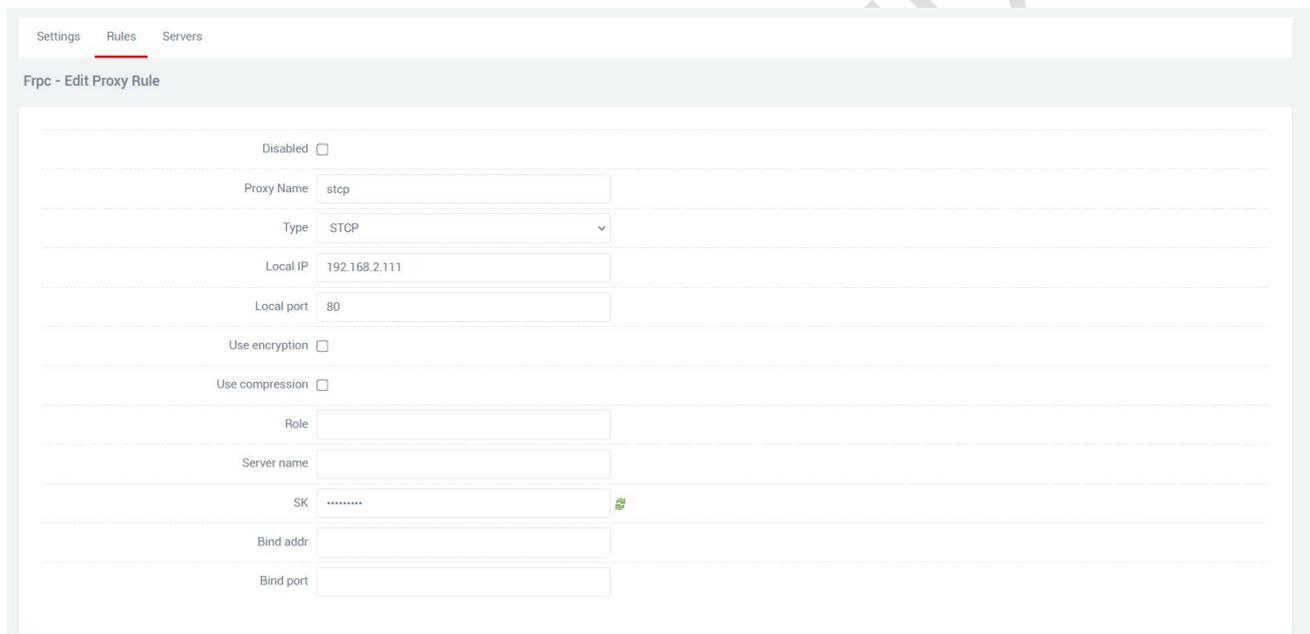
D.Local IP: The IP address assigned by the local device or the lan port to the connected device.

E.Local port: The device needs to open a port to the public network.

F.SK: Set a password, the access terminal needs to enter the SK set here when accessing the device.

G.Use encryption,Use compression: Configure as needed.

H.Role,Server name,Bind addr,Bind port:These four as clients do not need to be set.



Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

Local port

Use encryption

Use compression

Role

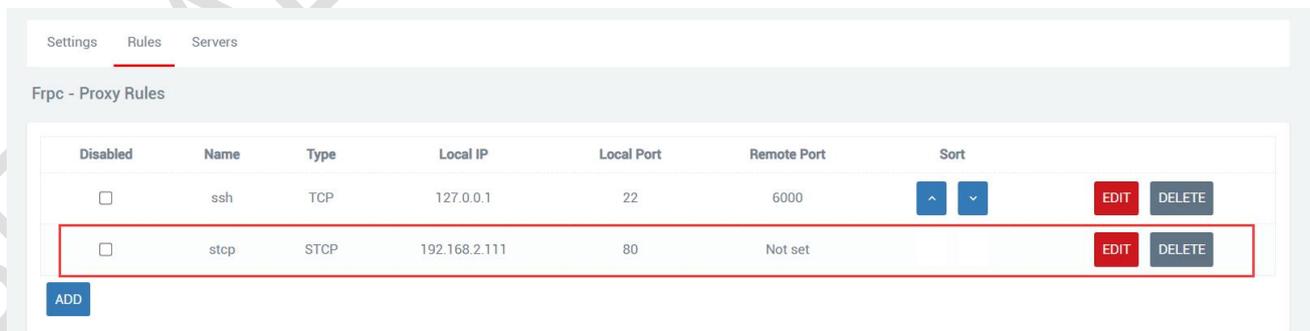
Server name

SK

Bind addr

Bind port

After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.



Settings Rules Servers

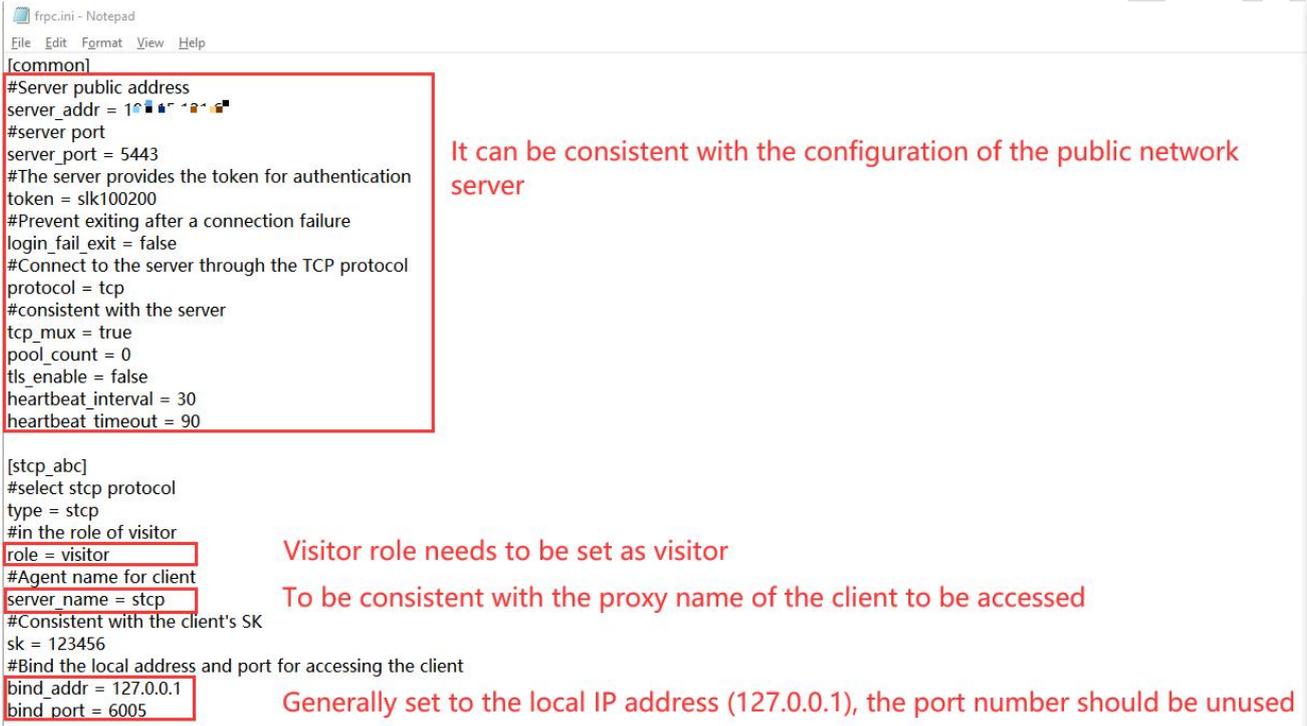
Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	<input type="button" value="^"/> <input type="button" value="v"/>	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/>	stcp	STCP	192.168.2.111	80	Not set		<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

If the PC wants to access the connected device of the router as the access end, it needs to be a client of frp, and it is also the stcp protocol, but it needs to set the visitor role and bind the local address and port. The frp file for Windows can be downloaded from the company's official website. After

downloading, open the frpc.ini configuration file for configuration.

Name	Date modified	Type	Size
systemd	4/12/2022 2:21 PM	File folder	
frpc.exe	4/14/2022 2:55 PM	Application	10,807 KB
frpc.ini	5/9/2022 9:25 AM	Configuration sett...	1 KB
frpc_full.ini	3/23/2022 9:30 PM	Configuration sett...	11 KB
frps.exe	3/23/2022 9:27 PM	Application	13,814 KB
frps.ini	3/23/2022 9:30 PM	Configuration sett...	1 KB
frps_full.ini	3/23/2022 9:30 PM	Configuration sett...	6 KB
LICENSE	3/23/2022 9:30 PM	File	12 KB



```
[common]
#Server public address
server_addr = 192.168.1.1
#server port
server_port = 5443
#The server provides the token for authentication
token = slk100200
#Prevent exiting after a connection failure
login_fail_exit = false
#Connect to the server through the TCP protocol
protocol = tcp
#consistent with the server
tcp_mux = true
pool_count = 0
tls_enable = false
heartbeat_interval = 30
heartbeat_timeout = 90

[stcp_abc]
#select stcp protocol
type = stcp
#in the role of visitor
role = visitor
#Agent name for client
server_name = stcp
#Consistent with the client's SK
sk = 123456
#Bind the local address and port for accessing the client
bind_addr = 127.0.0.1
bind_port = 6005
```

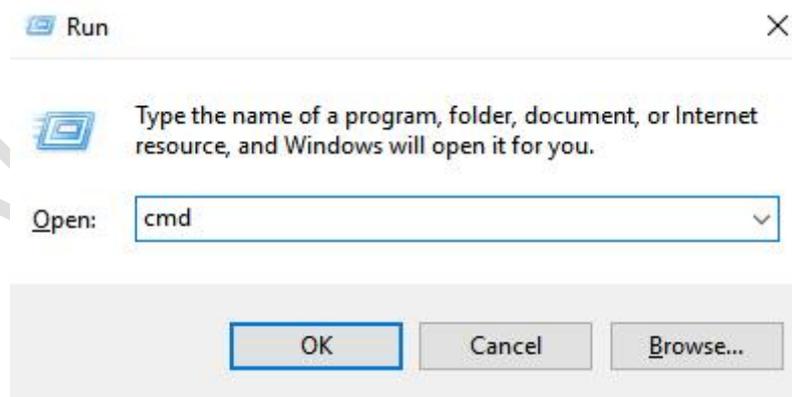
It can be consistent with the configuration of the public network server

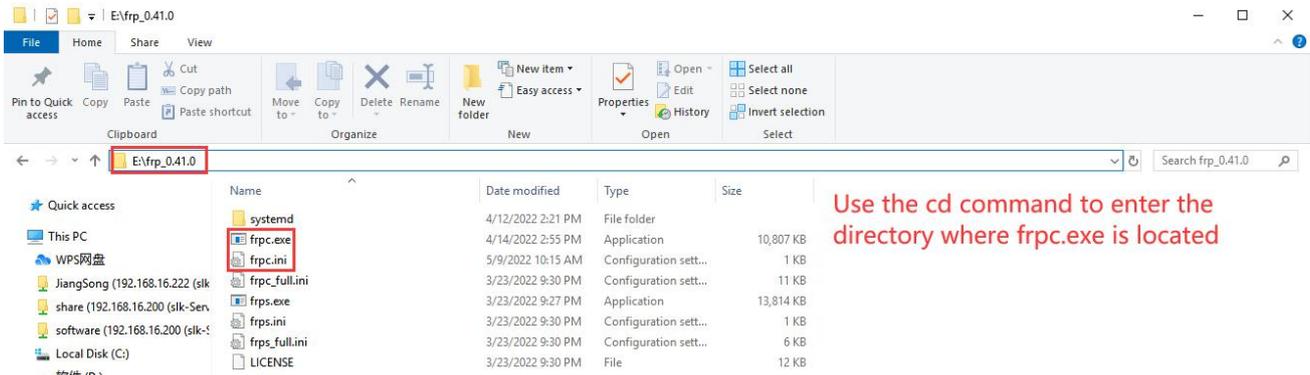
Visitor role needs to be set as visitor

To be consistent with the proxy name of the client to be accessed

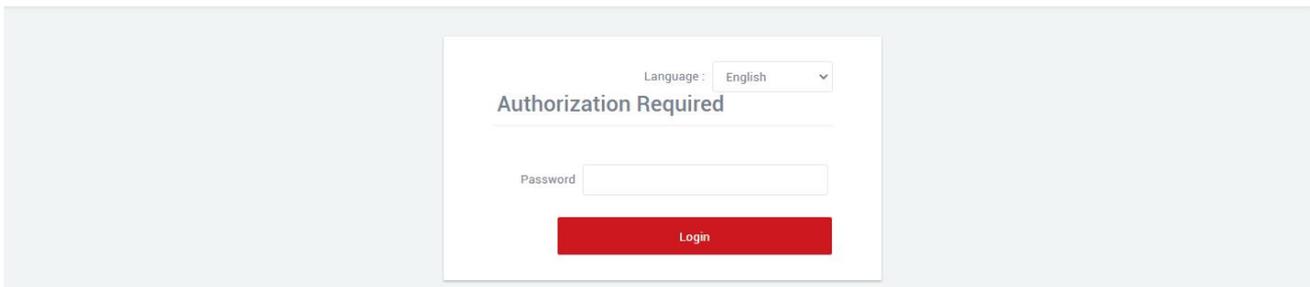
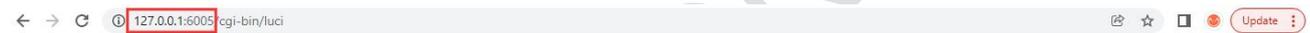
Generally set to the local IP address (127.0.0.1), the port number should be unused

Use the shortcut key "win+R" to quickly open the cmd command window.





First enter "E:" to enter the disk where frpc.exe is located, then use "cd+file path" to enter the folder where frpc.exe is located, and use the command "frpc.exe -c frpc.ini" to run the client.



(2) If there are two routers, and one router needs to remotely access the other router or the connected device of the other router, one is the stcp access terminal, and the other is the stcp client.

The configuration is as follows:

① Configure the client (first router, IP: 192.1682.1)

A. Disabled: Checking here will disable this rule.

B. Proxy Name: Customize a proxy name, which cannot be the same as other rules, otherwise it will not take effect due to conflict.

C. Type: Select the STCP protocol.

D. Local IP: The IP address assigned by the local device or the lan port to the connected device.

E. Local port: The device needs to open a port to the public network.

F. SK: Set a password, the access terminal needs to enter the SK set here when accessing the device.

G. Use encryption, Use compression: Configure as needed.

H. Role, Server name, Bind addr, Bind port: These four as clients do not need to be set.

Settings **Rules** Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

Local port

Use encryption

Use compression

Role

Server name

SK

Bind addr

Bind port

After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.

Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	^ v	EDIT DELETE
<input type="checkbox"/>	stcp	STCP	192.168.2.111	80	Not set		EDIT DELETE

ADD

SAVE & APPLY 3 SAVE & APPLY

## ② Configuring the Access Side (Second Router,IP:192.168.2.2)

A.You need to connect to the frp server first. For details, please refer to chapter 2.5.1

B.Disabled: If checked here, this rule will be disabled.

C.Proxy Name: Customize a proxy name, which cannot be the same as other rules, otherwise it will not take effect due to conflict.

D.Type: Select the STCP protocol.

E.Local IP,Local port: These two access terminals can be left blank.

F.SK:Set a password, the access terminal needs to enter the SK set here when accessing the device.

Use encryption,Use compression: Configure as needed.

G.Role: The access terminal needs to fill in the visitor.

H.Server name: The stcp proxy name set by the first router client.

I.Bind addr,Bind port: The client can be accessed by binding the address and port. The address and port are the local machine or the connected device of the local machine.

Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

Local port

Use encryption

Use compression

Role

Server name

SK

Bind addr

Bind port

After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.

Settings Rules Servers

Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	<input type="text" value="↑"/> <input type="text" value="↓"/>	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>
<input type="checkbox"/>	stcp_visitor	STCP	?	?	Not set		<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

← → ↻ Not secure 192.168.2.2:6606/cgi-bin/luci Update

Language:

**Authorization Required**

Password

### 5.3.4 Add UDP Proxy Rules

The UDP protocol is used to transmit a large amount of data. The port of the connected device needs to support the udp protocol. If the port that supports the udp protocol is opened to the public network, data transmission can be performed through the public network and the remote port number. Multiple udp protocol rules can be configured.

A.Disabled: Checking here means to disable this rule.

B.Proxy Name: Customize a proxy name. The proxy name cannot be repeated, otherwise the rule will not take effect due to conflict.

C. Type: Select the UDP protocol.

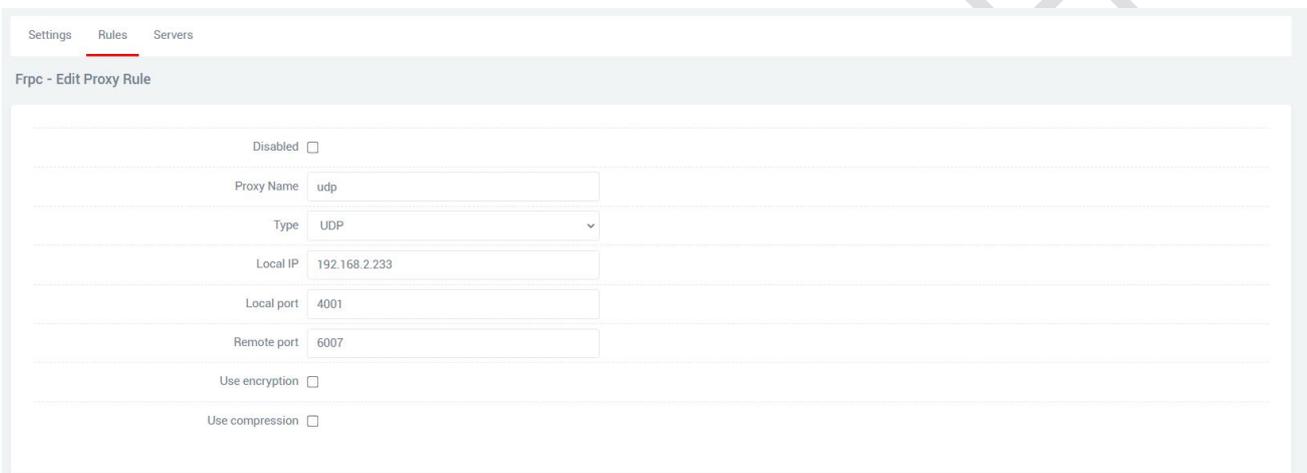
D. Local IP: Fill in the ip of the machine or the ip assigned by the lan port of the machine for the connected device (the ip address of the device that needs to be accessed through the public network).

E. Local port: The device needs to be forwarded to the port of the public network, which must be the port using the UDP protocol.

F. Remote port: Add this remote port to the public network address to access the local port opened by the corresponding local device. This port number should not be the same as other rules, and do not use the occupied port, otherwise this rule will not take effect.

G. Use encryption, Use compression: Check these two as needed.

H. Multiple rules can be added, the remote port and proxy name should not conflict, and click "SAVE & APPLY" after the configuration is complete.



Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

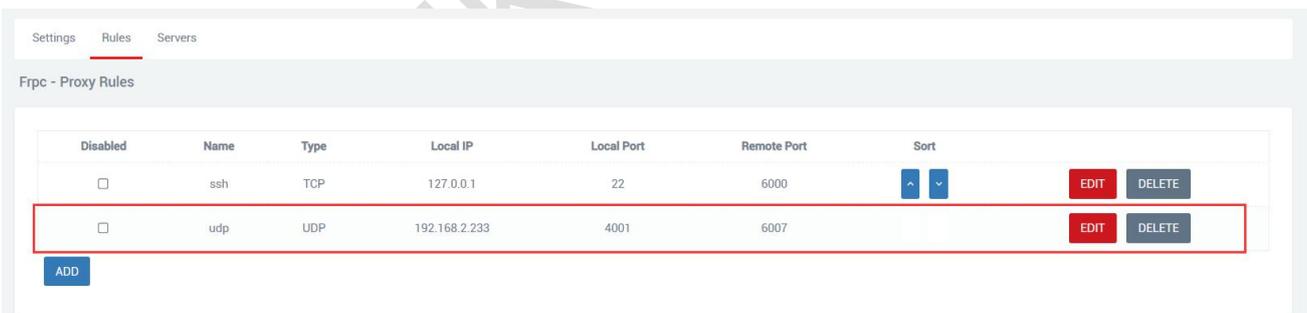
Local port

Remote port

Use encryption

Use compression

After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.

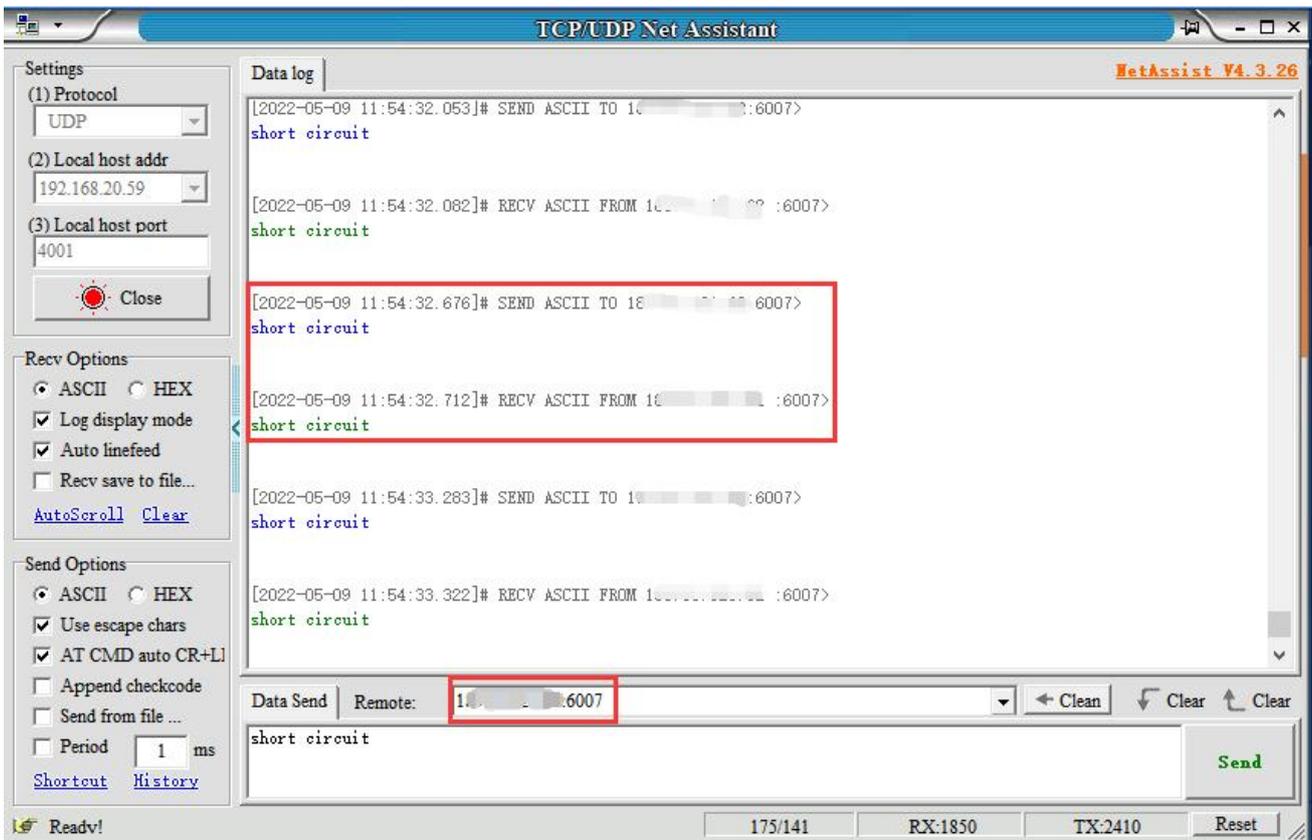


Settings Rules Servers

Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort		
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	<input type="button" value="^"/> <input type="button" value="v"/>	<input type="button" value="EDIT"/>	<input type="button" value="DELETE"/>
<input type="checkbox"/>	udp	UDP	192.168.2.233	4001	6007		<input type="button" value="EDIT"/>	<input type="button" value="DELETE"/>

Through the UDP protocol, use the public network address and remote port number to access the device forwarded to the public network (111.111.111.111:6007 accesses 192.168.2.233:4001).



### 5.3.5 Add HTTP Proxy Rules

For http and https services, domain name-based virtual hosts are supported, and custom domain name binding is supported, so that multiple domain names can share a port 80 and access intranet web pages through the custom domain name. Multiple http rules can be configured, which can be accessed directly through a custom domain name. After the configuration is complete, you can access the corresponding web page through the custom domain name plus the http penetration port (ie vhost\_http\_port) provided by the server.

- A.Disabled: Checking here means to disable this rule.
- B.Proxy Name: Customize an agent name. The agent name cannot be repeated, otherwise the rule will not take effect due to conflict.
- C.Type: Select the HTTP protocol.
- D.Local IP: Fill in the ip of the machine or the ip assigned by the lan port of the machine for the connected device (the ip address of the device that needs to be accessed through the public network).
- E.Local port: The device needs to be forwarded to the port of the public network, and this port must be the port number of the internal page.
- F.Use encryption,Use compression,HTTP user,HTTP password: These four are selected as needed.
- G.Subdomain: Write it if you have it, or leave it out if you don't have it.
- H.Custom domains: xxx. The domain name bound to the public network, xxx is defined by itself, but the latter must be the domain name bound to the public network.

Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

Local port

Use encryption

Use compression

HTTP user

HTTP password

Subdomain

Custom domains

After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.

Settings Rules Servers

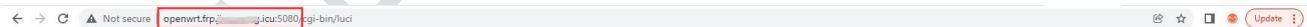
Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	^ v	EDIT DELETE
<input type="checkbox"/>	http	HTTP	192.168.2.111	80	Not set		EDIT DELETE

ADD

The browser can log in to `openwrt.frp.****.***:5080` to enter the client routing management page. Among them, `openwrt` is a custom part, and you need to add a record on the domain name application website to resolve the subdomain name; `frp.****.***` is the value of `subdomain_host` of the `frpc` server; port `5080` is the intranet penetration port provided by the server, and the value of `vhost_http_port`;

You can configure multiple `http` rules in this way, and the custom domain name does not need to be the same.



Language: English

Authorization Required

Password

Login

## Chapter 6 VPN Service

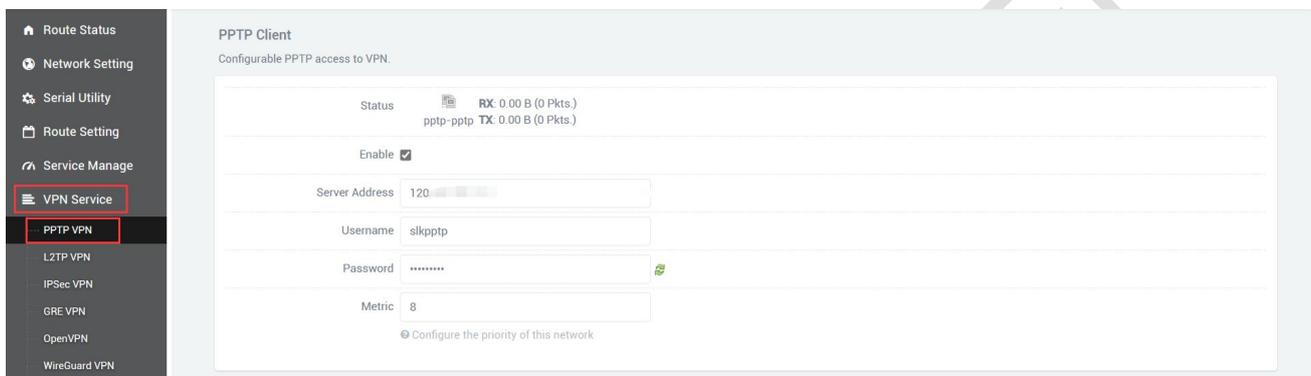
### 6.1 PPTP VPN

Navigation bar "VPN Service" - "PPTP VPN", select Enable, fill in the server address, fill in the user name and password according to the server settings, click "SAVE & APPLY".

A.Enable: To use PPTP VPN, you need to check it, and you can just uncheck it when you don't use it.

B.Server Address: The server IP address, usually the public IP.

C.Username,Password: Fill in the username and password set by the server.



After the connection is successful, the address assigned by the server will appear in the status bar. If pptp is not used, uncheck it and click "SAVE & APPLY".



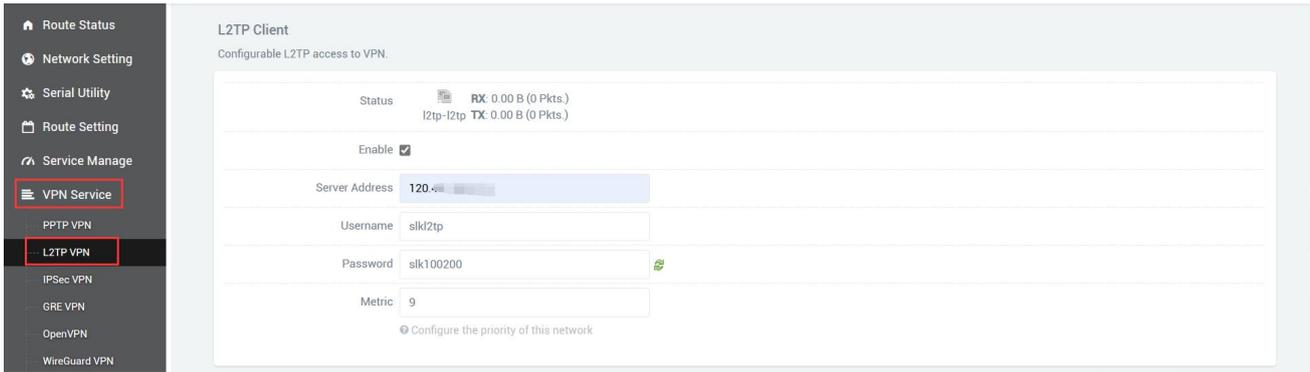
### 6.2 L2TP VPN

Navigation bar "VPN Service" - "L2TP VPN", select Enable, fill in the user name and password according to the server settings, click "SAVE & APPLY".

A.Enable: To use L2TP VPN, you need to check it, and you can just uncheck it when you don't use it.

B.Server Address: The server IP address, usually the public IP.

C.Username,Password: Enter the username and password set by the server.



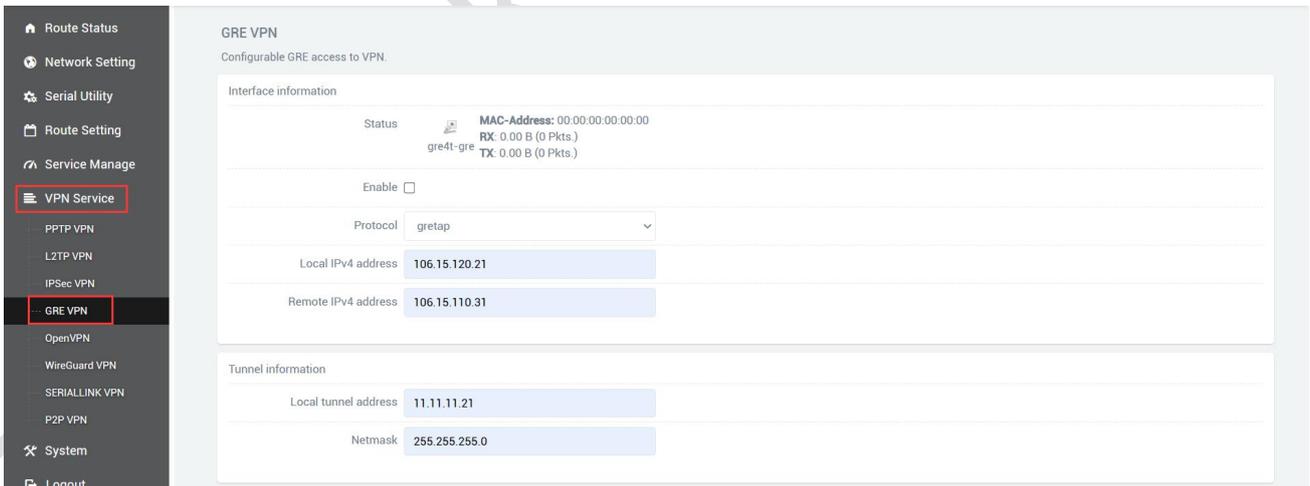
The screenshot shows the 'L2TP Client' configuration page. On the left, a navigation menu has 'VPN Service' selected, with 'L2TP VPN' highlighted. The main area is titled 'L2TP Client' and 'Configurable L2TP access to VPN'. It contains a status bar with RX and TX data, an 'Enable' checkbox which is checked, and several input fields: 'Server Address' (120.11.11.1), 'Username' (slkl2tp), 'Password' (slk100200), and 'Metric' (9). There is also a checkbox for 'Configure the priority of this network'.

After the connection is successful, the address assigned by the server will appear in the status bar. If l2tp is not used, uncheck it and click "SAVE & APPLY".

Status  **Uptime: 0h 0m 10s**  
**RX: 432.00 B (9 Pkts.)**  
l2tp-l2tp **TX: 324.00 B (10 Pkts.)**  
**IPv4: 192.168.18.2/32**

## 6.3 GRE VPN

Navigation bar "VPN Service" - "GRE VPN", select Enable, select gretap or gre according to the protocol of the opposite end (keep the protocol at both ends the same). The local IPv4 address and remote IPv4 address are filled in according to the local wan port (public network) address and the peer wan port (public network) address, and the local tunnel address and the peer tunnel address are in the same network segment.

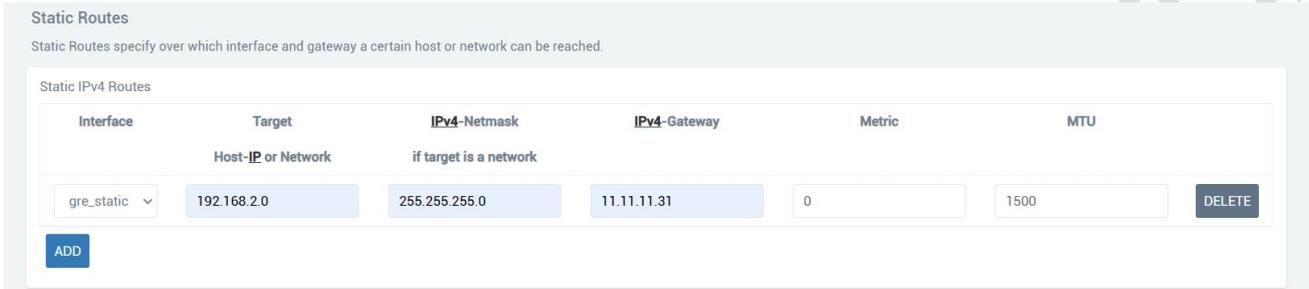
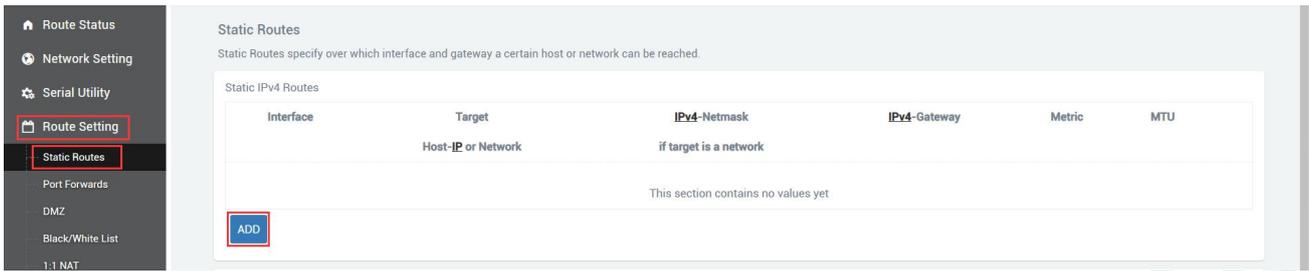


The screenshot shows the 'GRE VPN' configuration page. The navigation menu has 'GRE VPN' highlighted. The main area is titled 'GRE VPN' and 'Configurable GRE access to VPN'. It contains a status bar with MAC-Address, RX, and TX data, an 'Enable' checkbox which is unchecked, and several input fields: 'Protocol' (gretap), 'Local IPv4 address' (106.15.120.21), 'Remote IPv4 address' (106.15.110.31), 'Local tunnel address' (11.11.11.21), and 'Netmask' (255.255.255.0).

Refresh status information after "SAVE & APPLY".

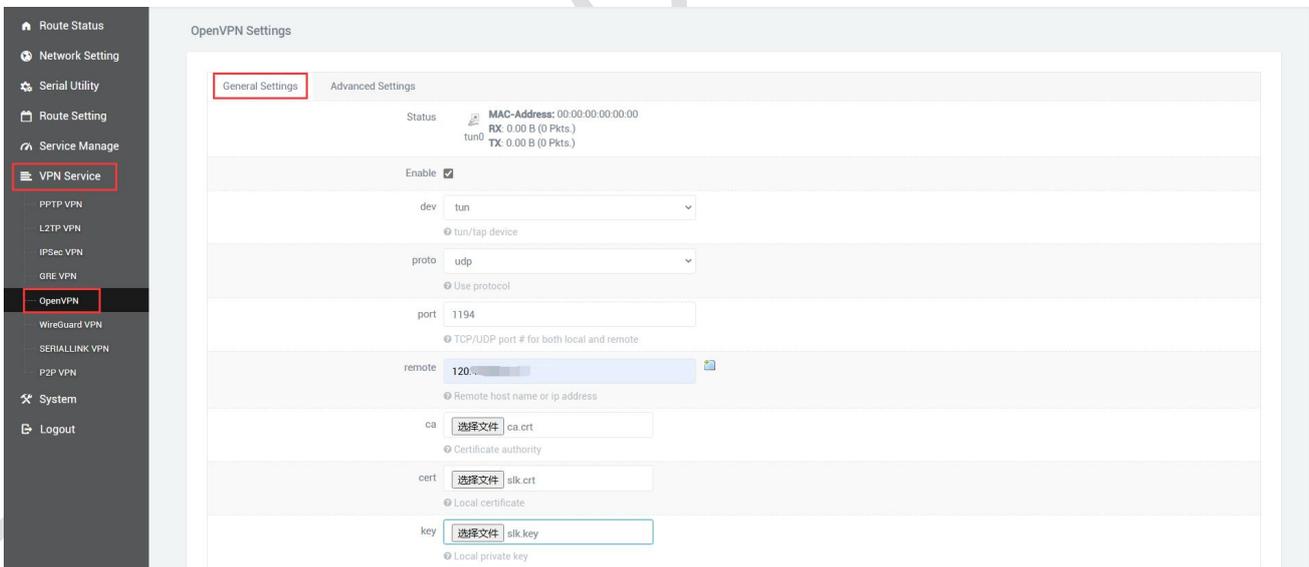
Status  **Uptime: 0h 0m 3s**  
**MAC-Address: C6:F5:E9:07:E7:05**  
gre-gre **RX: 0.00 B (0 Pkts.)**  
**TX: 0.00 B (0 Pkts.)**  
**IPv4: 11.11.11.21/24**

Then add routing table rules, you can successfully access the peer Lan port device.

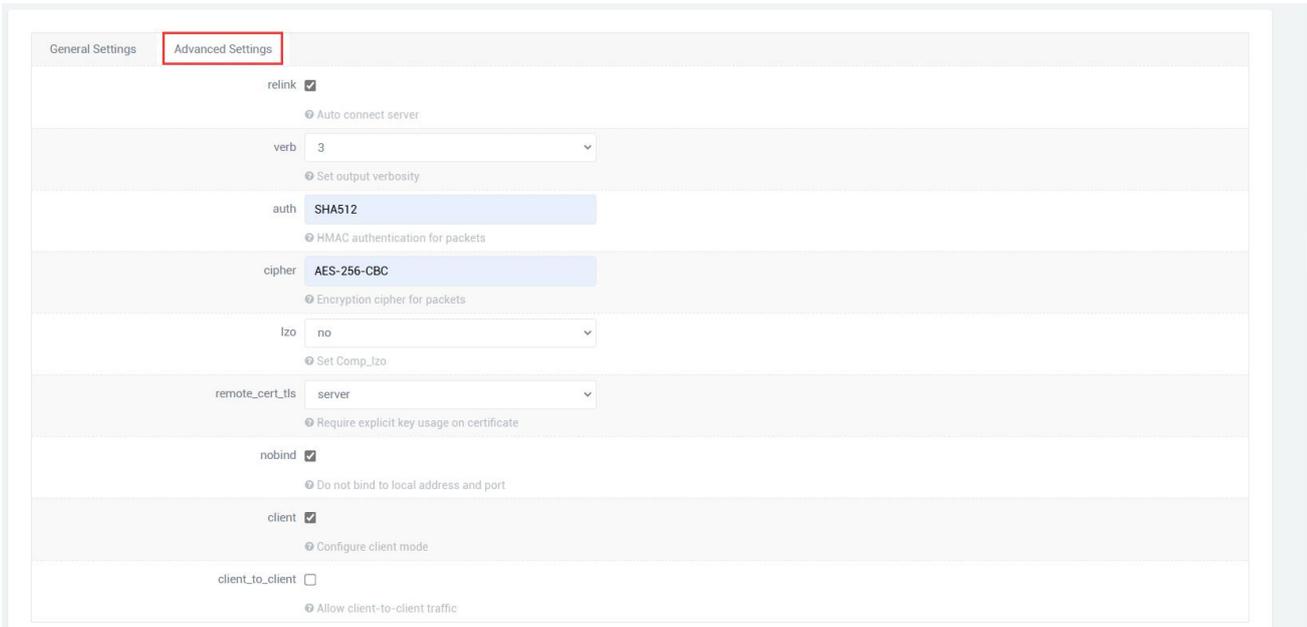


## 6.4 OpenVPN

Navigation bar "VPN Service" - "OpenVPN", click "SAVE & APPLY" after all configurations are consistent with the server, the three certificates are provided by the server.



The advanced settings page is modified according to the server. If relink is checked, it means that openvpn can automatically reconnect. If you need to automatically reconnect, you can check it. If you don't need it, leave it unchecked. After all configurations are completed, click "SAVE & APPLY".

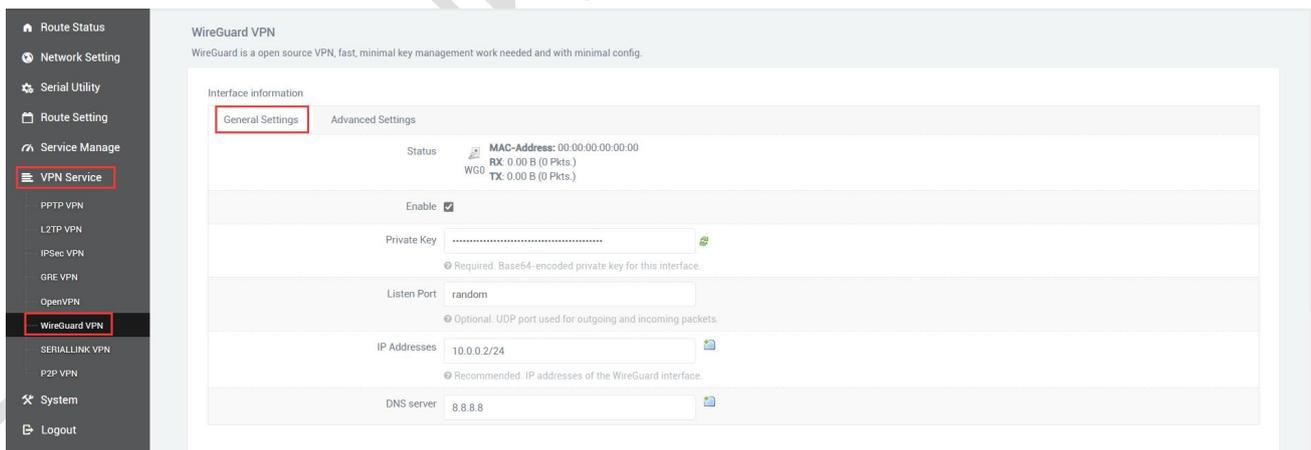


The screenshot shows the 'Advanced Settings' tab for OpenVPN. The 'relink' checkbox is checked, with a sub-option 'Auto connect server'. The 'verb' dropdown is set to '3', with a sub-option 'Set output verbosity'. The 'auth' dropdown is set to 'SHA512', with a sub-option 'HMAC authentication for packets'. The 'cipher' dropdown is set to 'AES-256-CBC', with a sub-option 'Encryption cipher for packets'. The 'lzo' dropdown is set to 'no', with a sub-option 'Set Comp\_lzo'. The 'remote\_cert\_tls' dropdown is set to 'server', with a sub-option 'Require explicit key usage on certificate'. The 'nobind' checkbox is checked, with a sub-option 'Do not bind to local address and port'. The 'client' checkbox is checked, with a sub-option 'Configure client mode'. The 'client\_to\_client' checkbox is unchecked, with a sub-option 'Allow client-to-client traffic'.

After the connection is successful, the status bar will refresh the address. If openvpn is not used, uncheck it and click "SAVE & APPLY".

## 6.5 WireGuard VPN

WireGuard is an easy-to-configure, fast and secure open source VPN, which uses the latest encryption technology and is checked and enabled on the basic configuration page, with interface information corresponding to the server [Interface] item and peer corresponding to the server [Peer] item.



The screenshot shows the 'WireGuard VPN' configuration page. The left sidebar has 'VPN Service' selected, with 'WireGuard VPN' highlighted. The main content area shows 'Interface information' with 'General Settings' selected. The status is 'Enabled'. The MAC-Address is '00:00:00:00:00:00'. The RX and TX statistics are '0.00 B (0 Pkts.)'. The 'Private Key' field is empty, with a note 'Required: Base64-encoded private key for this interface.'. The 'Listen Port' is set to 'random', with a note 'Optional: UDP port used for outgoing and incoming packets.'. The 'IP Addresses' are '10.0.0.2/24', with a note 'Recommended: IP addresses of the WireGuard interface.'. The 'DNS server' is '8.8.8.8'.

For peer configuration, click the Add button to add configuration information.



The screenshot shows the 'Peers' section. It contains the text 'Further information about WireGuard interfaces and peers. This section contains no values yet' and a blue 'ADD' button.

Peers  
Further information about WireGuard interfaces and peers.

[DELETE](#)

Public Key   
Required. Base64-encoded public key of peer.

Allowed IPs   
  
Required. IP addresses and prefixes that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the networks the peer routes through the tunnel.

Route Allowed IPs   
Optional. Create routes for Allowed IPs for this peer.

Endpoint Host   
Optional. Host of peer. Names are resolved prior to bringing up the interface.

Endpoint Port   
Optional. Port of peer.

Persistent Keep Alive

Enter the configuration information corresponding to the server, click "SAVE & APPLY", and the status of the connection is as follows.

Status

 WGO

**Uptime:** 0h 3m 27s  
**MAC-Address:** 00:00:00:00:00:00  
**RX:** 0.00 B (0 Pkts.)  
**TX:** 0.00 B (0 Pkts.)  
**IPv4:** 10.0.0.2/24

## 6.6 Remote management - P2P VPN

The remote management platform supports ad hoc networks and supports encrypted point-to-point connections, which means that only devices on your private network can communicate with each other, navigation bar "VPN Service" - "P2P VPN", after entering the configuration, click "SAVE & APPLY", the status bar will refresh and obtain the IP address indicating that the connection is successful.

P2P VPN  
P2P VPN enables encrypted point-to-point connections using the open source WireGuard protocol, which means only devices on your private network can communicate with each other.

General Settings    Advanced Settings

Status  Uptime: 0h 3m 13s  
 MAC-Address: 00:00:00:00:00:00  
 p2pvpn RX: 0.00 B (0 Pkts.)  
 TX: 0.00 B (0 Pkts.)

Enable

Server Address

Port

Preauthkey

Metric   
Configure the priority of this network

Status

 p2pvpn

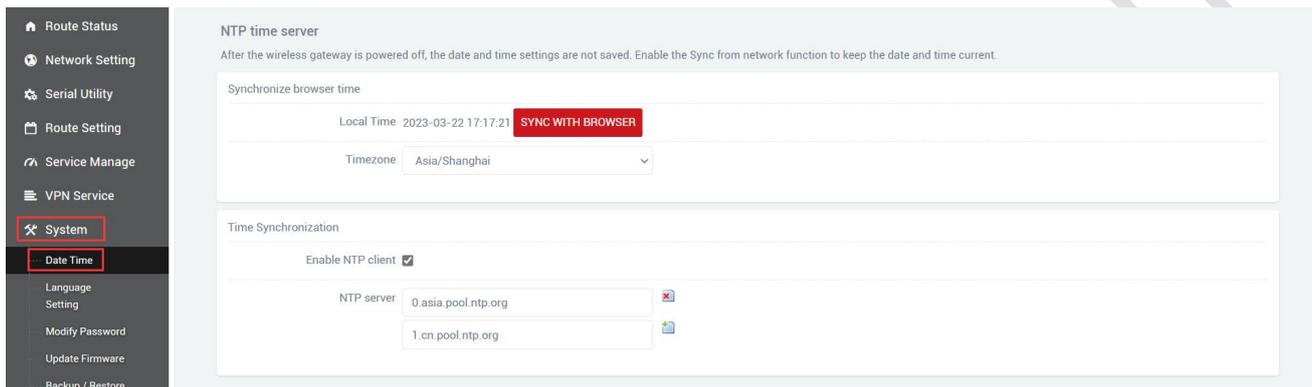
**Uptime:** 2h 24m 16s  
**MAC-Address:** 00:00:00:00:00:00  
**RX:** 0.00 B (0 Pkts.)  
**TX:** 232.00 B (2 Pkts.)  
**IPv4:** 100.64.0.6/32  
**IPv6:** fd7a:115c:a1e0::6/128

## Chapter 7 System

### 7.1 Date Time

Time synchronization is enabled by default. If necessary, you can change the NTP server to synchronize the time of the server.

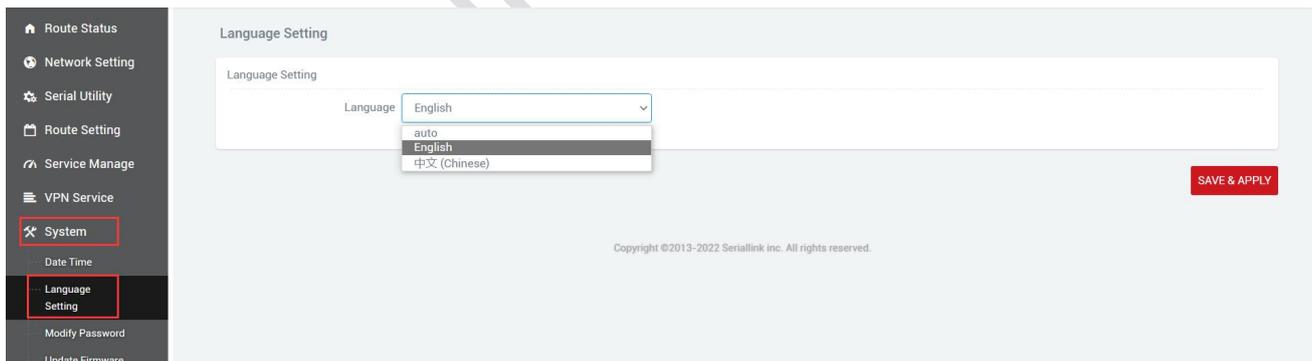
Navigation bar "System" - "Date Time", click "SAVE & APPLY" after setting.



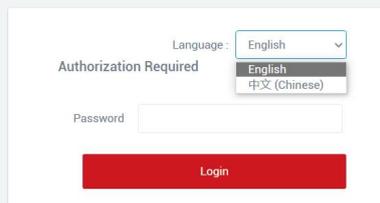
The screenshot shows the "NTP time server" configuration page. The left sidebar contains a navigation menu with "System" and "Date Time" highlighted. The main content area has a title "NTP time server" and a subtitle "After the wireless gateway is powered off, the date and time settings are not saved. Enable the Sync from network function to keep the date and time current." Below this, there is a "Synchronize browser time" section with a "Local Time" field showing "2023-03-22 17:17:21" and a "SYNC WITH BROWSER" button. A "Timezone" dropdown menu is set to "Asia/Shanghai". The "Time Synchronization" section has a checked "Enable NTP client" checkbox and two "NTP server" input fields: "0.asia.pool.ntp.org" and "1.cn.pool.ntp.org".

### 7.2 Language Setting

Change the language displayed on the page according to your own needs, you can choose English or Chinese, change it in the navigation bar "System" - "Language Setting", or change the language in the login interface.



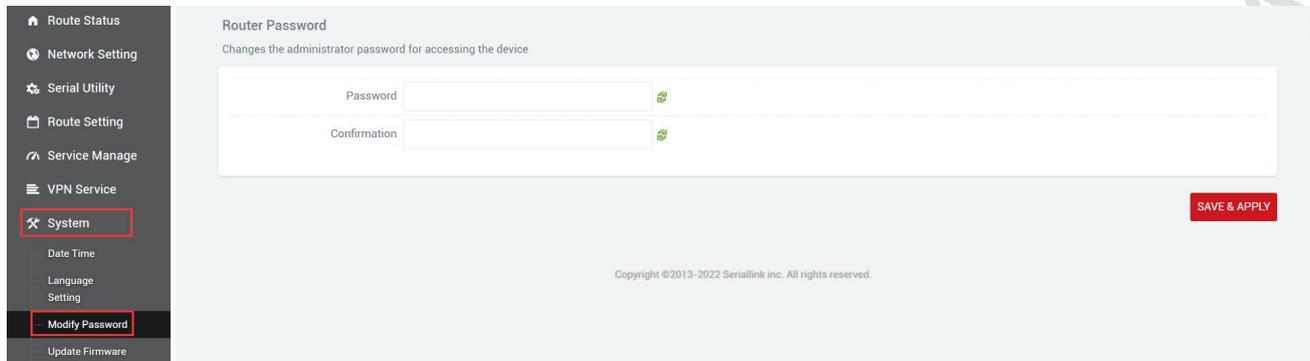
The screenshot shows the "Language Setting" page. The left sidebar has "System" and "Language Setting" highlighted. The main content area has a title "Language Setting" and a "Language" dropdown menu with options: "English", "auto", "English", and "中文 (Chinese)". A "SAVE & APPLY" button is visible in the bottom right corner. The footer of the page contains the text "Copyright ©2013-2022 Seriallink inc. All rights reserved."



The screenshot shows the login interface. It features a "Language" dropdown menu with options: "English", "English", and "中文 (Chinese)". Below the dropdown is a "Password" input field and a red "Login" button. The text "Authorization Required" is displayed above the password field.

## 7.3 Modify Password

The default password for login is admin. If the user needs to protect the configuration interface to avoid being modified by others, he can modify the login password, click "System" - "Modify Password" in turn, then fill in the password to be modified, and then SAVE & APPLY, as follows.



Router Password

Changes the administrator password for accessing the device

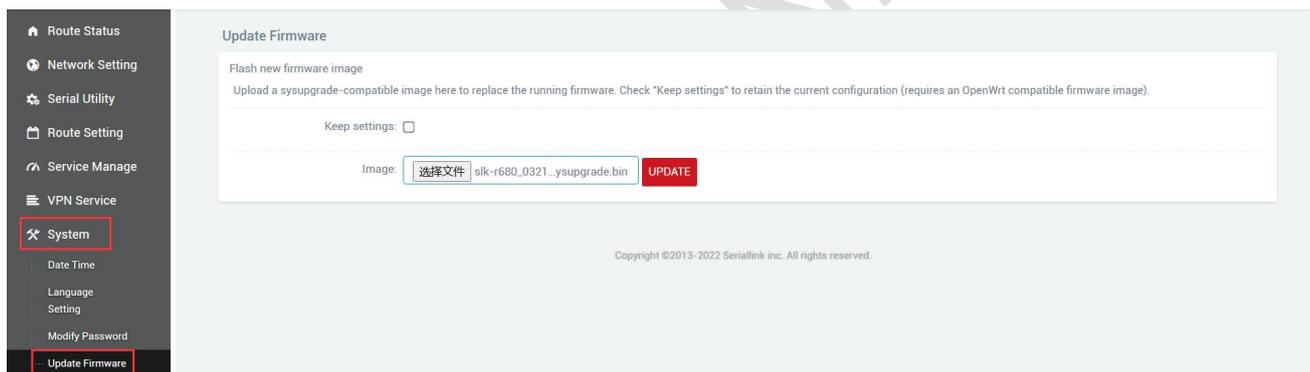
Password

Confirmation

SAVE & APPLY

Copyright ©2013-2022 Seriallink inc. All rights reserved.

## 7.4 Update Firmware



Update Firmware

Flash new firmware image

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

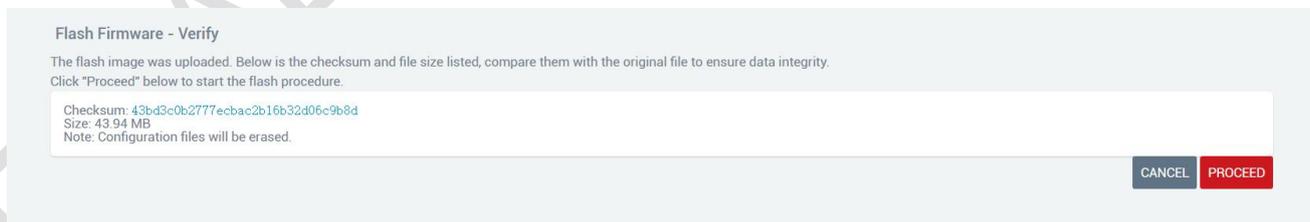
Keep settings:

Image:  slk-r680\_0321\_ysupgrade.bin

Copyright ©2013-2022 Seriallink inc. All rights reserved.

Navigation bar "System" - "Update Firmware", select the file and click "UPDATE", the MD5 check code page will appear after uploading, click "PROCEED" to upgrade, the upgrade will take a certain time, it takes about 1~2 minutes, after the upgrade is complete, log in again through "192.168.2.1".

When upgrading the firmware, you need to uncheck the "Keep settings" option.



Flash Firmware - Verify

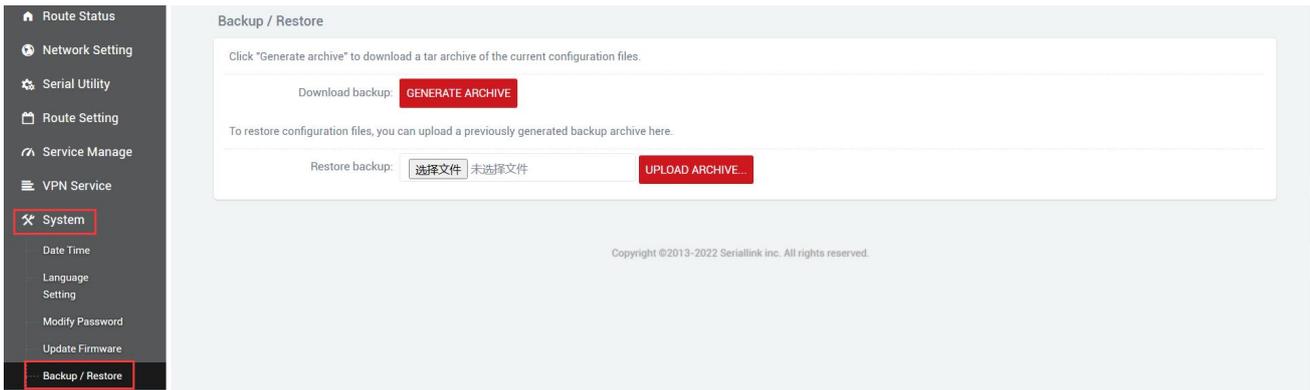
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

Checksum: 43bd3c0b2777ecbac2b16b32d06c9b8d  
Size: 43.94 MB  
Note: Configuration files will be erased.

CANCEL PROCEED

## 7.5 Backup/Restore

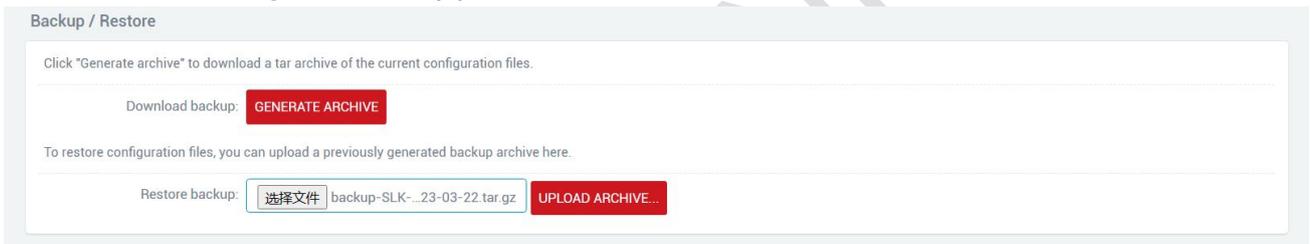
The backup function can be used to generate a configuration file for the device and download it locally.



The downloaded configuration file is as follows.

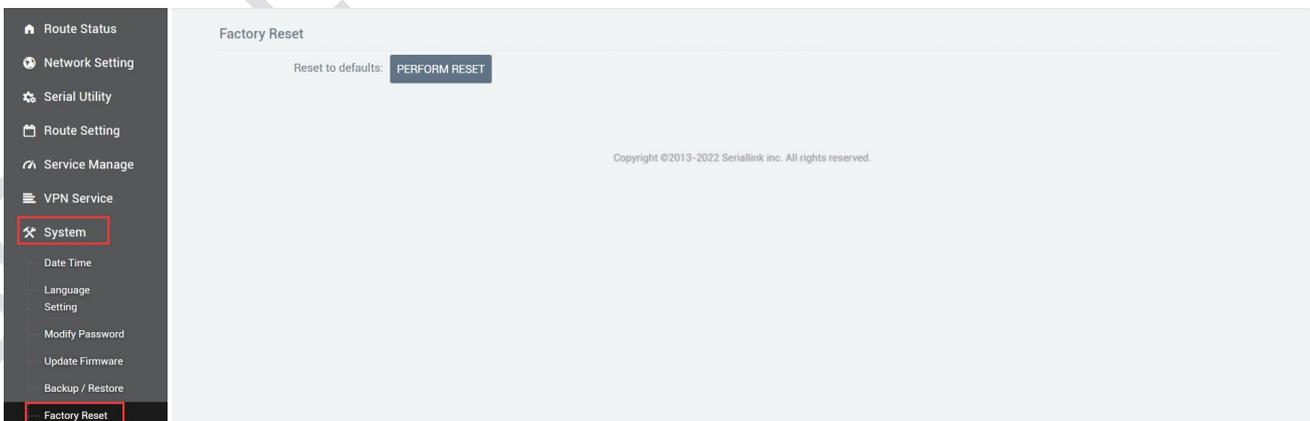


The recovery function restores the device configuration through the local configuration file, and the device restarts during the recovery process.



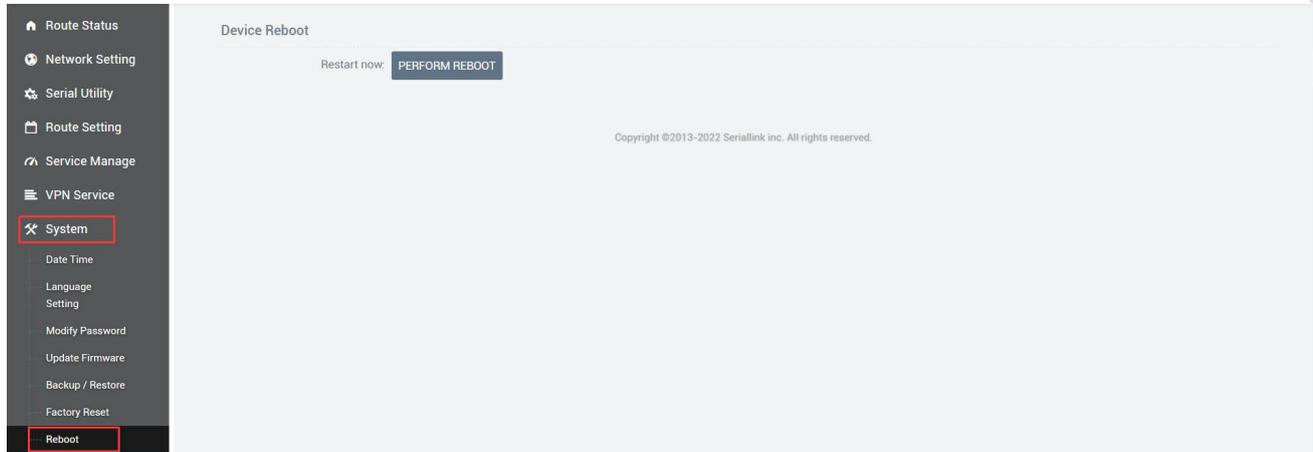
## 7.6 Factory Reset

Factory reset is generally when the device fails to enter the device page, or there are many function settings, and you want to reset it, you can restore the factory default settings, the navigation bar "System" - "Factory Reset", click "Execute reset", you can restore the device to the factory default.

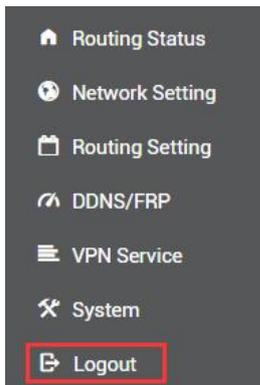


## 7.7 Reboot

Immediately restart, the device can be restarted through the page, the navigation bar "System" - "Reboot", click "Execute restart" to restart the device.



## 7.8 page log out



Click "Logout" to exit to the login interface.

Thank you for your support of SERIALLINK products.

If you have any questions, please email: [info@seriallink.net](mailto:info@seriallink.net) or [www.seriallink.net](http://www.seriallink.net)