



SLK-R680 Series

**Industrial 4G 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 4G Modem	8
2.3 WAN Setting	10
2.3.1 DHCP address	10
2.3.2 PPPoE	10
2.3.3 Static address	11
2.3.4 As lan (convert WAN port to LAN port)	11
2.4 DHCP Setting	12
2.5 WIFI Access Point	13
2.6 WIFI Client(Bridge)	14
2.7 WIFI repeater	16
2.7.1 Change the local IP address	16
2.7.2 Connect to the main wireless AP	17
2.7.3 Disable DHCP	18
2.8 Time Reboot	18
2.9 Watchcat	18
2.10 Diagnosis	20
Chapter 3 Firewall and Application	21
3.1 Firewall on and off	21
3.2 DMZ	21
3.3 Prot Forwards	22
3.4 Black/White List	24
3.4.1 White List	24
3.4.2 Black List	26
3.5 Frp Client	27
3.5.1 Connect to Frps	27
3.5.2 Add TCP proxy protocol	30
3.5.3 Add STCP Proxy Rules	32
3.5.4 Add UDP Proxy Rules	37
3.5.5 Add HTTP Proxy Rules	38
Chapter 4 VPN Service	40
4.1 PPTP VPN	40
4.2 L2TP VPN	40
4.3 GRE VPN	41
4.4 OpenVPN	42
Chapter 5 System	44
5.1 Date Time	44

5.2 Language Setting	44
5.3 Modify Password	45
5.4 Update Firmware	45
5.5 Factory Reset	46
5.6 Reboot	46
5.7 page log out	47

SERIALLINK CONFIDENTIAL

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.

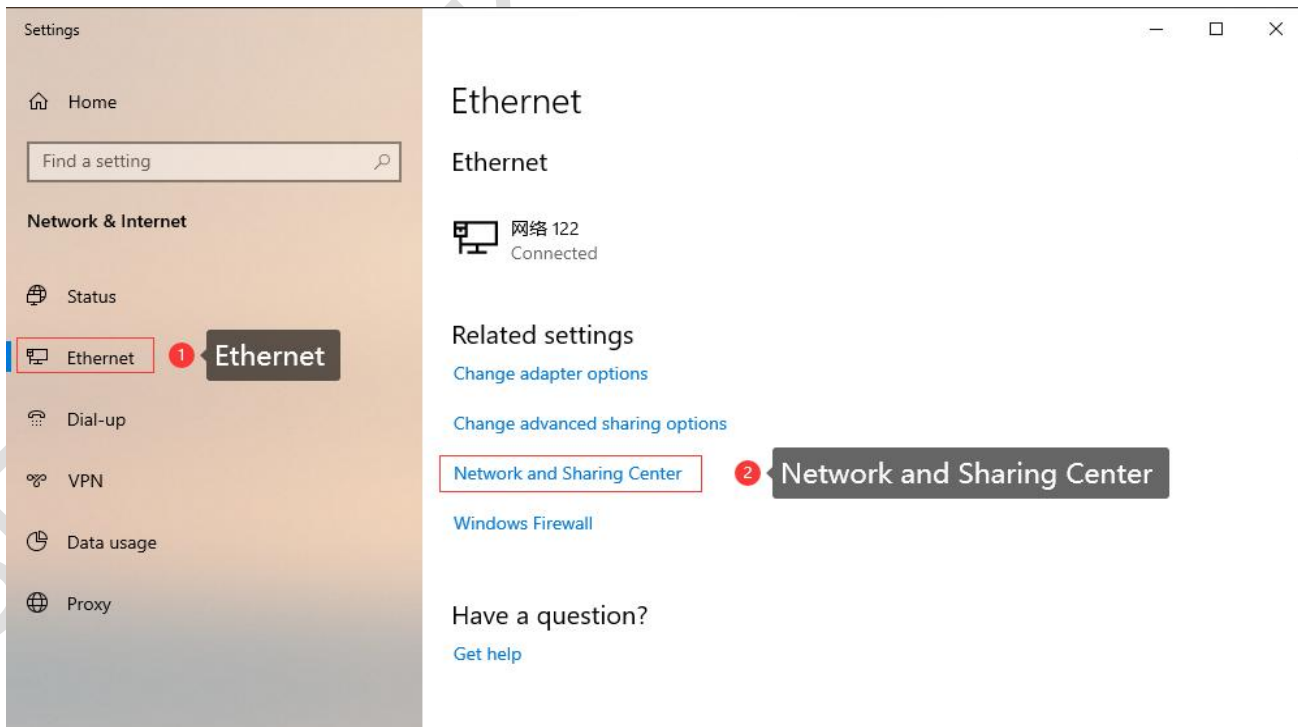
Set the IP address of the management PC (for example: 192.168.2.59) and the IP address of the device's LAN port in the same network segment(The initial IP address of the LAN port of the device is: 192.168.2.1, and the subnet mask is 255.255.255.0) The method is as follows.

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

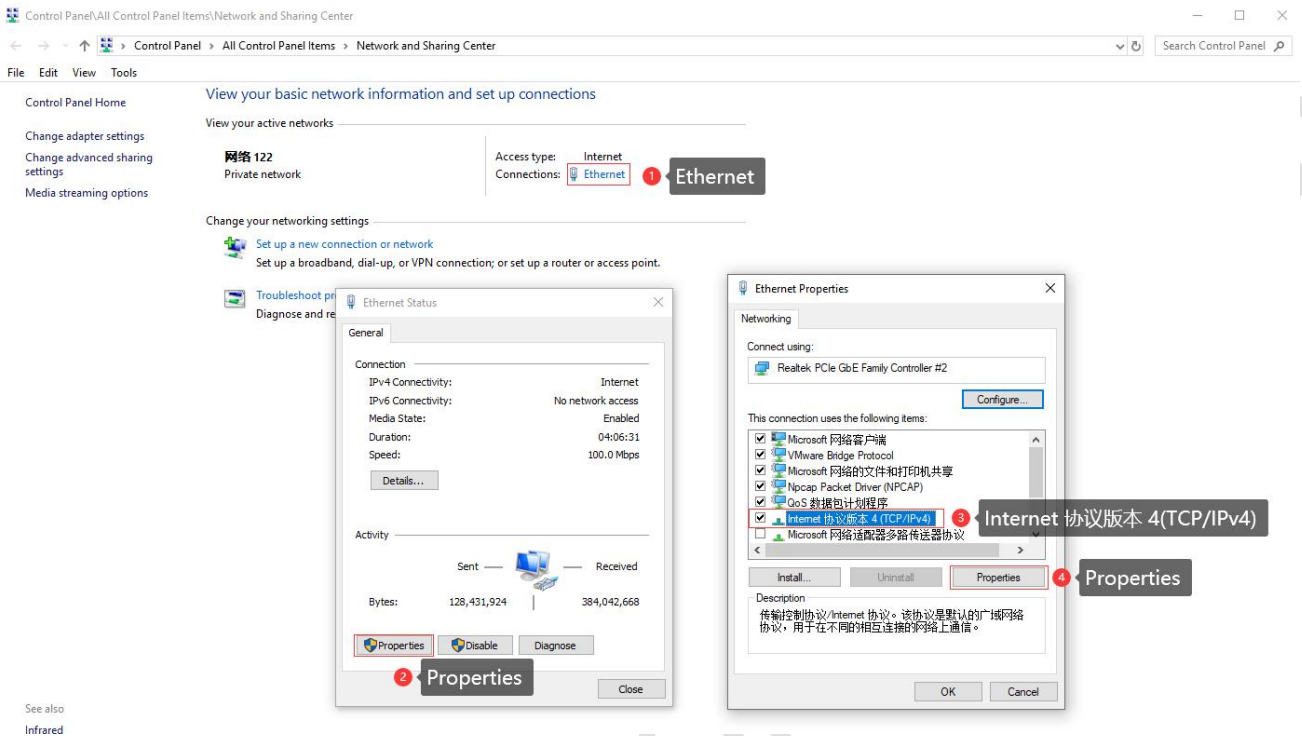
Step 1: Right-click the network logo in the lower right corner of the desktop (as shown in the figure), and choose to Open Network & Internet settings.



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

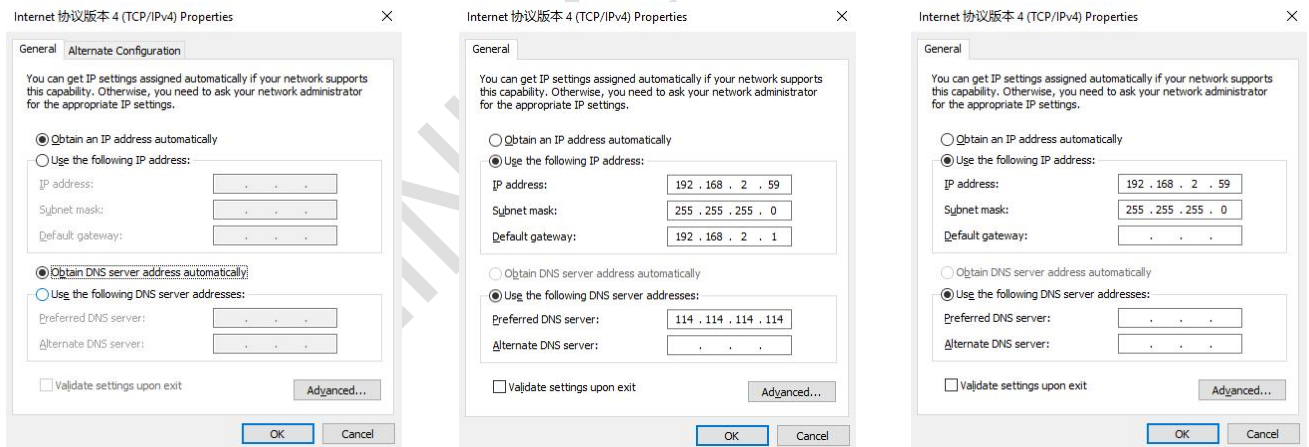


Step 4: There are three setting methods

method 1

method 2

method 3

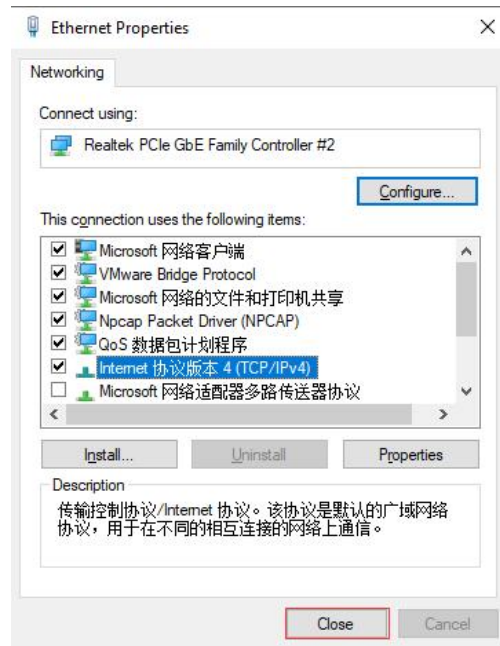
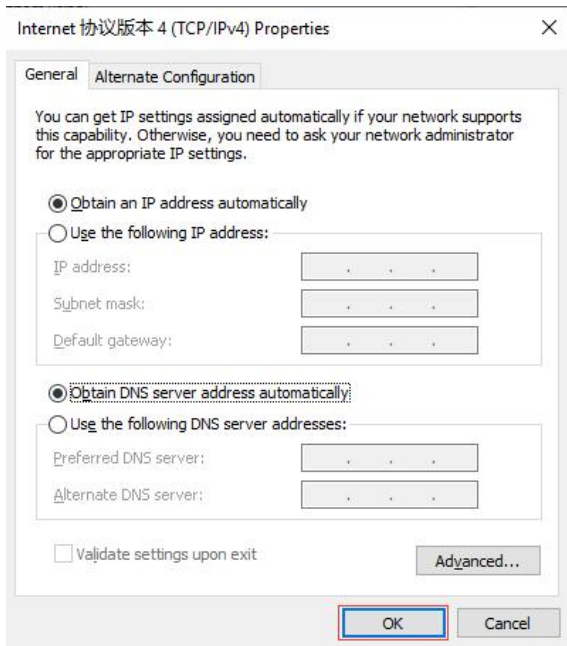


method 1: It can be used to configure the device and access the external network. It is recommended to use it (Note: If there are multiple routes with different network segments in the current environment, the IP obtained by the computer may not be able to connect to the device. In this case, method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

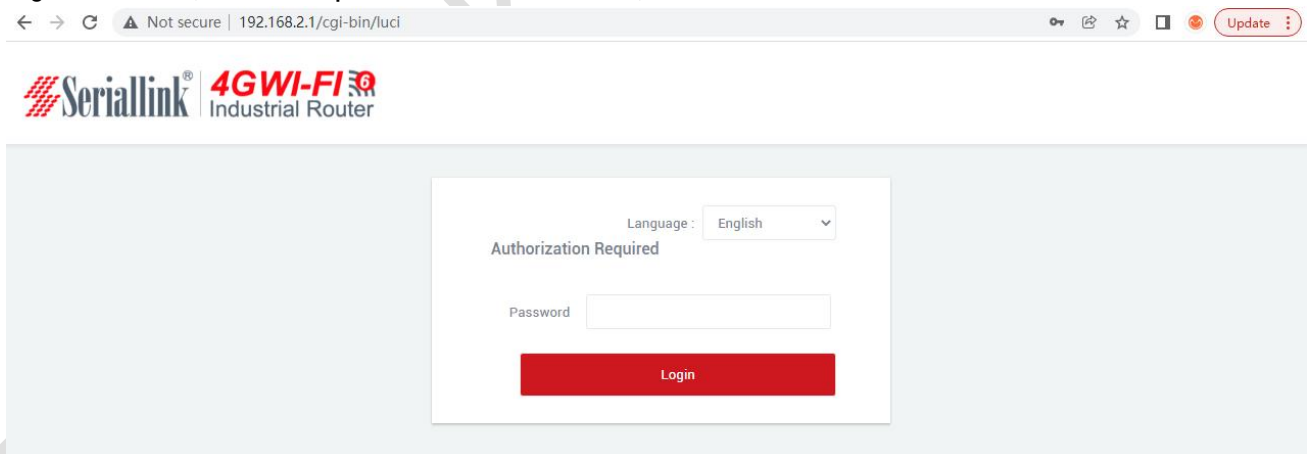
method 3: Only connect the device for configuration use, the computer cannot access the external network through the device network, and the IP address is set as in method 2;

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

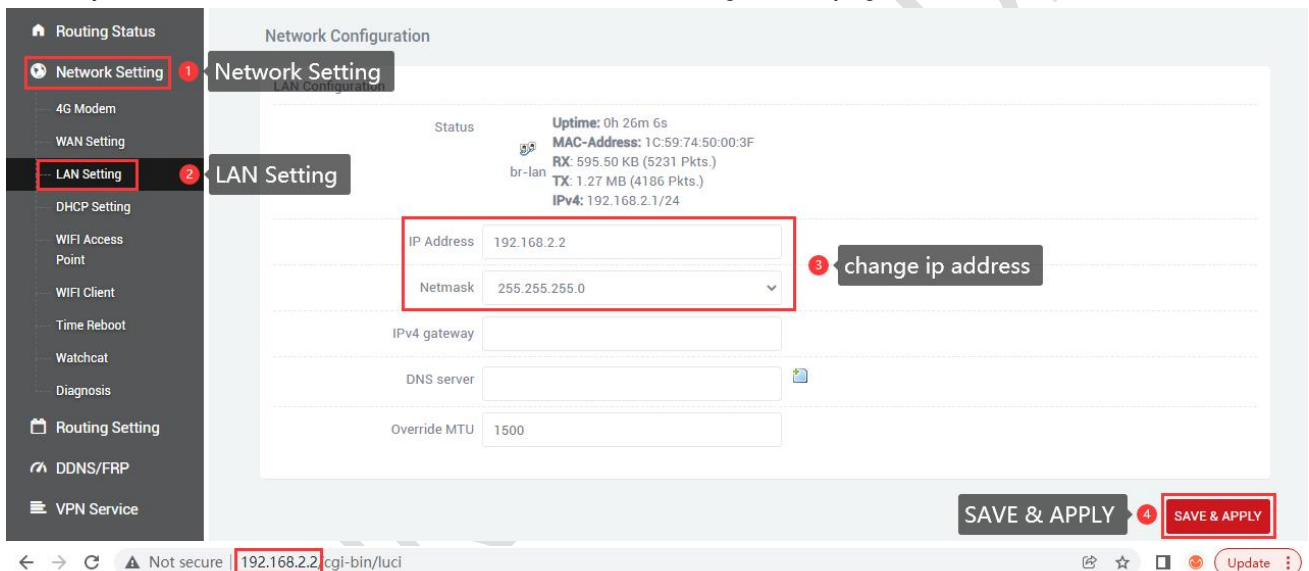
The default address of the router is 192.168.2.1. You can modify the static IP address in the navigation bar "Network Setting" - "LAN Setting". After modification, the new IP address will be used to log in to the page.

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

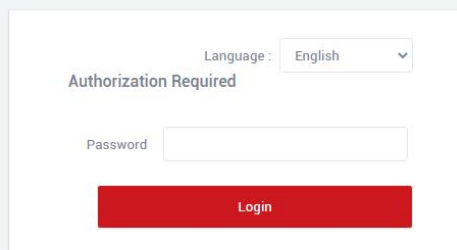
B.Netmask: It is generally 255.255.255.0, which can be modified as needed.

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.



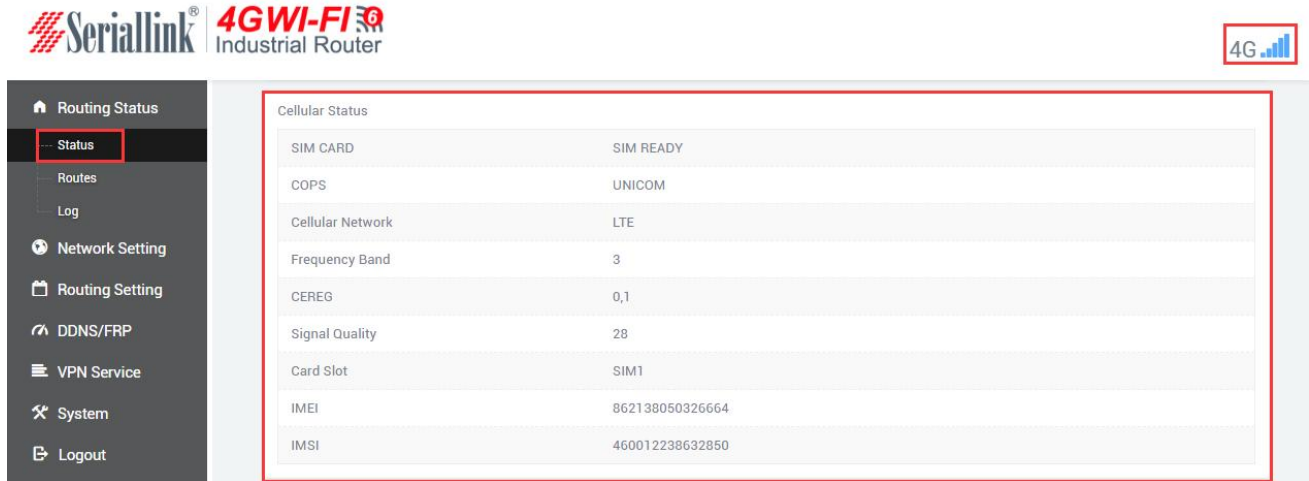
The screenshot displays the 'Network Configuration' page for the Seriallink router. The left sidebar shows navigation options, with 'Network Setting' and 'LAN Setting' highlighted. The main content area shows the 'LAN Setting' configuration. The IP Address is set to 192.168.2.2, and the Netmask is 255.255.255.0. A red box highlights the IP Address field, and a callout bubble says 'change ip address'. The browser address bar shows '192.168.2.2/cgi-bin/luci'. The page includes a 'SAVE & APPLY' button.




The screenshot shows the login page for the Seriallink router. It features a language dropdown menu set to 'English', a 'Password' input field, and a red 'Login' button. The text 'Authorization Required' is displayed above the password field.

2.2 4G Modem

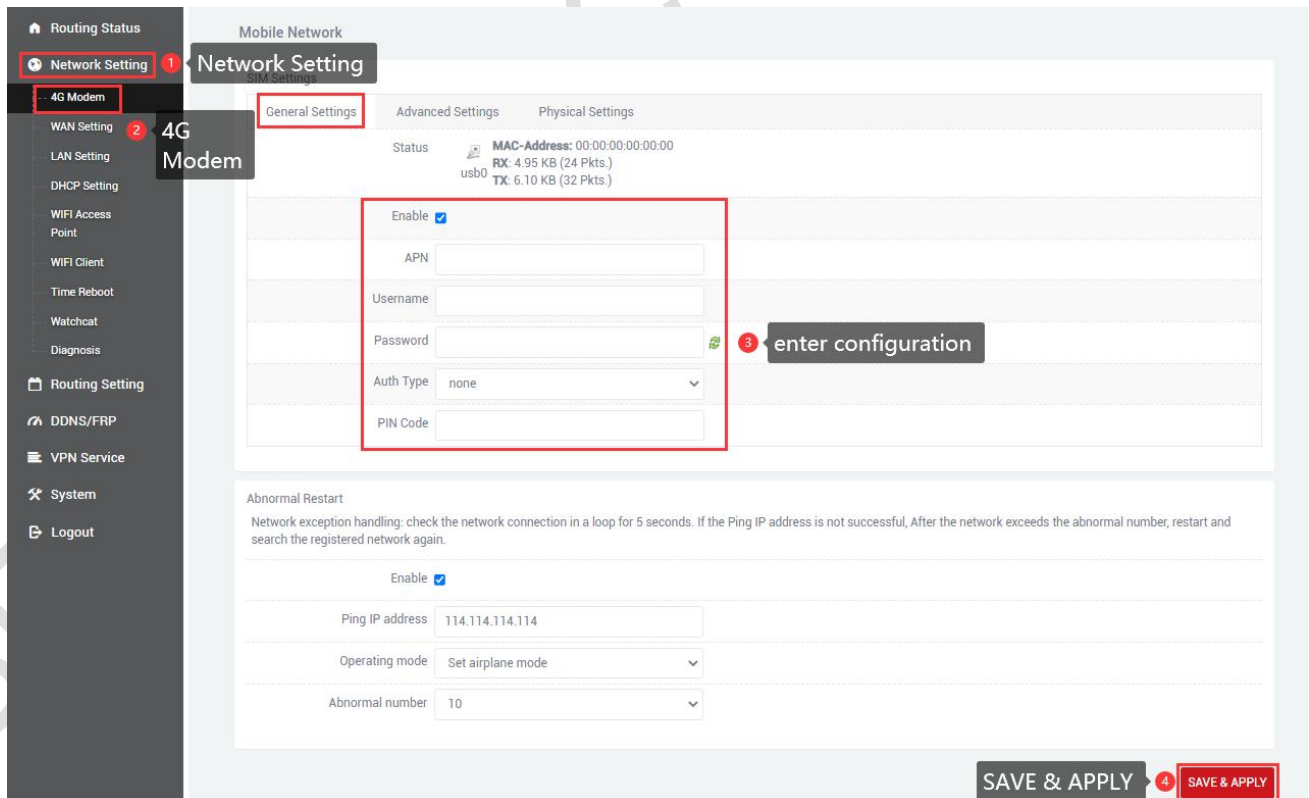
By default, the router uses the SIM card 2/3/4G to access the Internet. You can see the information of the SIM card in the "Routing Status" - "Status" in the navigation bar. You can check the network is 2/3/4G and the signal of the mobile phone card - in the upper right corner.



Seriallink 4GWI-FI Industrial Router 4G 

Cellular Status	
SIM CARD	SIM READY
COPS	UNICOM
Cellular Network	LTE
Frequency Band	3
CEREG	0,1
Signal Quality	28
Card Slot	SIM1
IMEI	862138050326664
IMSI	460012238632850

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" - "4G Modem" - "General Settings".




Seriallink 4GWI-FI Industrial Router

Mobile Network

Network Setting

4G Modem

General Settings

Status:  **MAC-Address:** 00:00:00:00:00:00
usb0 **RX:** 4.95 KB (24 Pkts.)
TX: 6.10 KB (32 Pkts.)

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"/>

enter configuration

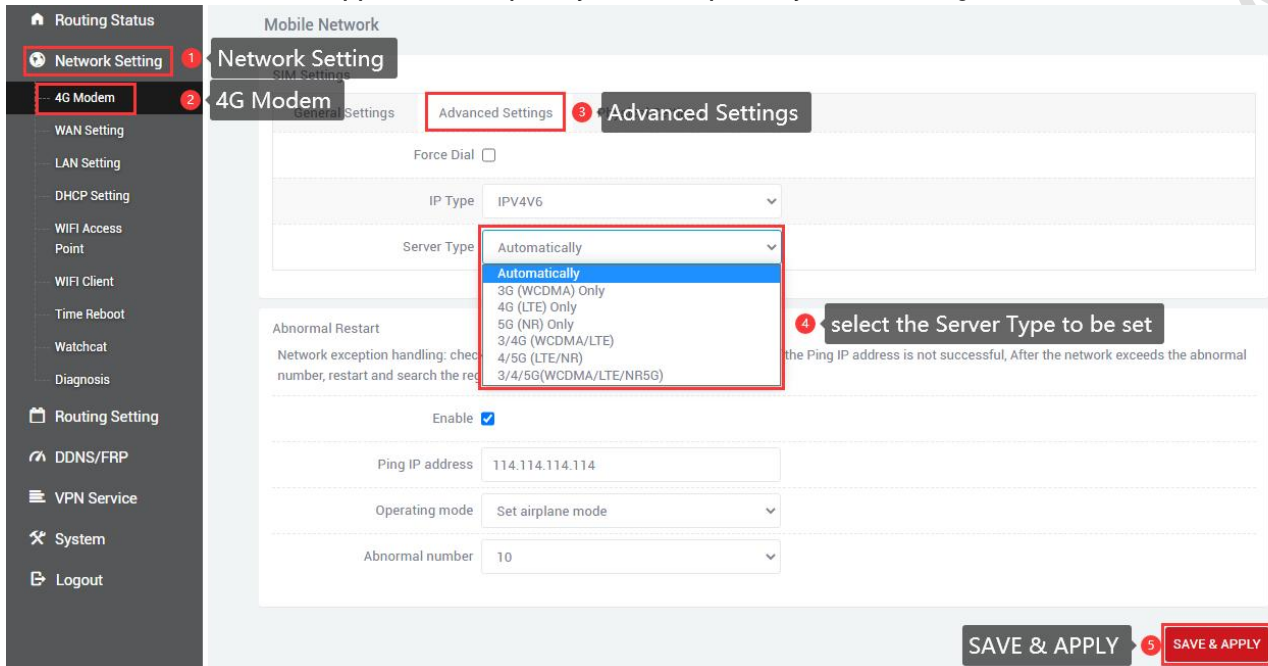
Abnormal Restart

Network exception handling: check the network connection in a loop for 5 seconds. If the Ping IP address is not successful, After the network exceeds the abnormal number, restart and search the registered network again.

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

SAVE & APPLY **SAVE & APPLY**

"Network Setting" - "4G Modem" - "Advanced Settings" can bind 2/3/4G. If 4G (LTE) Only is selected for the service type, it means that only the 4G network is used. If there is no 4G network nearby, there will be no network automatically. The default is 2/3/4G, the frequency band with good signal is given priority, and 4G 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".



Mobile Network

Network Setting

4G Modem

Advanced Settings

Force Dial

IP Type: IPv4v6

Server Type: Automatically

Abnormal Restart

Network exception handling: check the network connection in a loop for 5 seconds. If the Ping IP address is not successful, After the network exceeds the abnormal number, restart and search the registered network again.

Enable

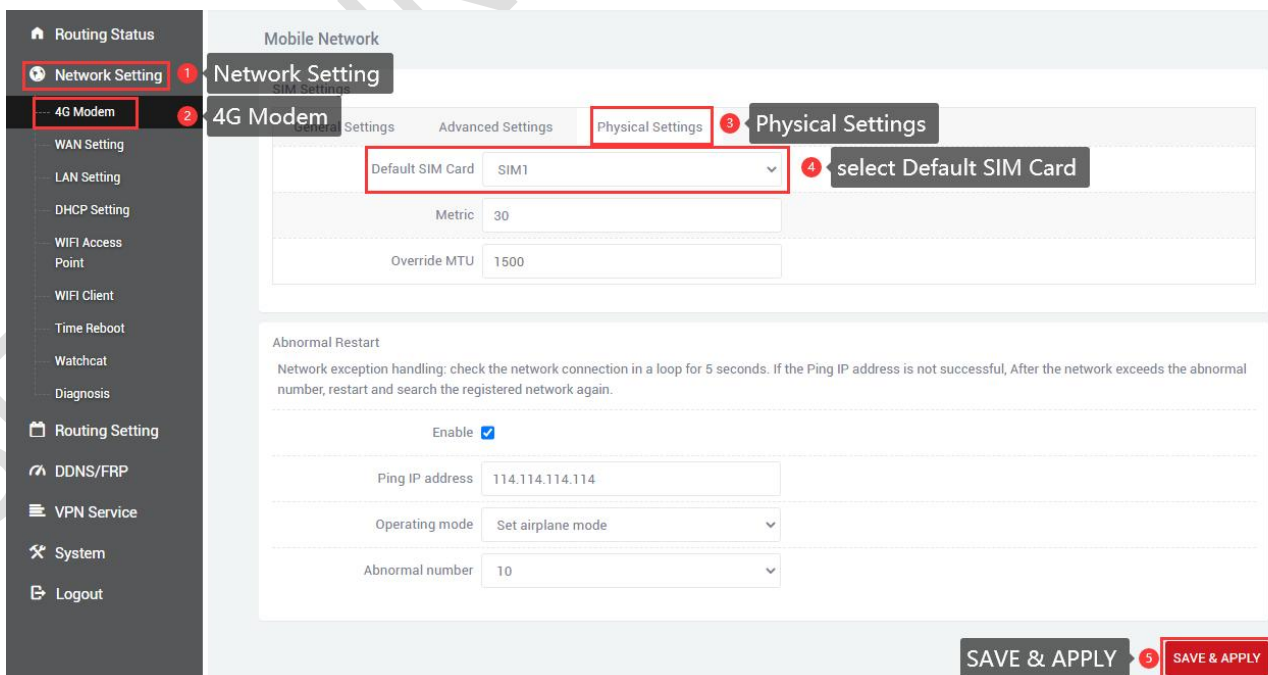
Ping IP address: 114.114.114.114

Operating mode: Set airplane mode

Abnormal number: 10

SAVE & APPLY

"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.



Mobile Network

Network Setting

4G Modem

Physical Settings

Default SIM Card: SIM1

Metric: 30

Override MTU: 1500

Abnormal Restart

Network exception handling: check the network connection in a loop for 5 seconds. If the Ping IP address is not successful, After the network exceeds the abnormal number, restart and search the registered network again.

Enable

Ping IP address: 114.114.114.114

Operating mode: Set airplane mode

Abnormal number: 10

SAVE & APPLY

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". You can also not enable network diagnostics, just leave it unchecked.

Abnormal Restart

Network exception handling: check the network connection in a loop for 5 seconds. If the Ping IP address is not successful, After the network exceeds the abnormal number, restart and search the registered network again.

Enable

Ping IP address

Operating mode

Abnormal number

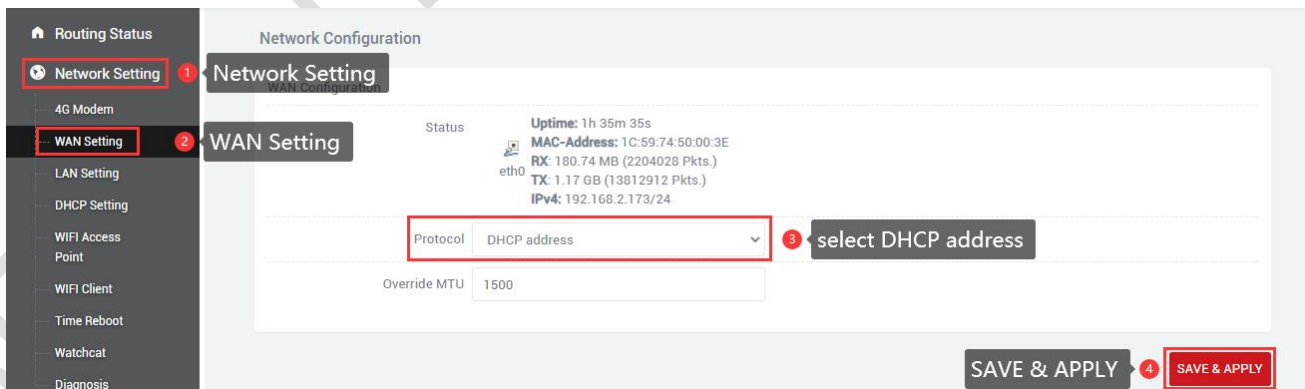
note:

- Ordinary 4G 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

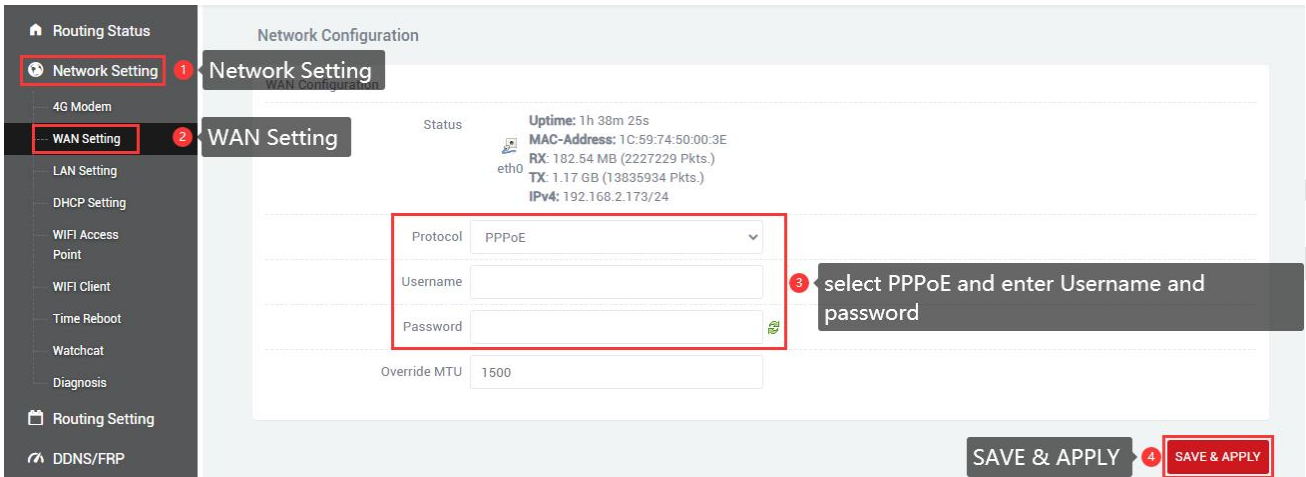
2.3.1 DHCP address

Navigation bar "Network Setting" - "WAN Setting", 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, the value of MTU does not need to be changed (default: 1500).



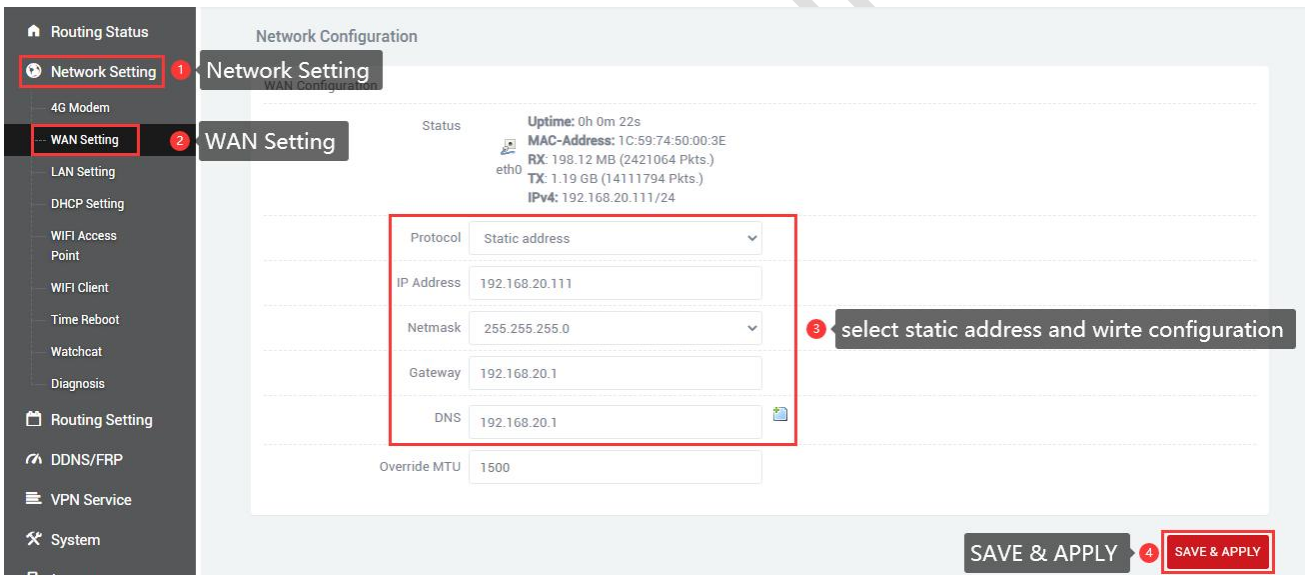
2.3.2 PPPoE

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, the value of MTU does not need to be changed (default value: 1500).



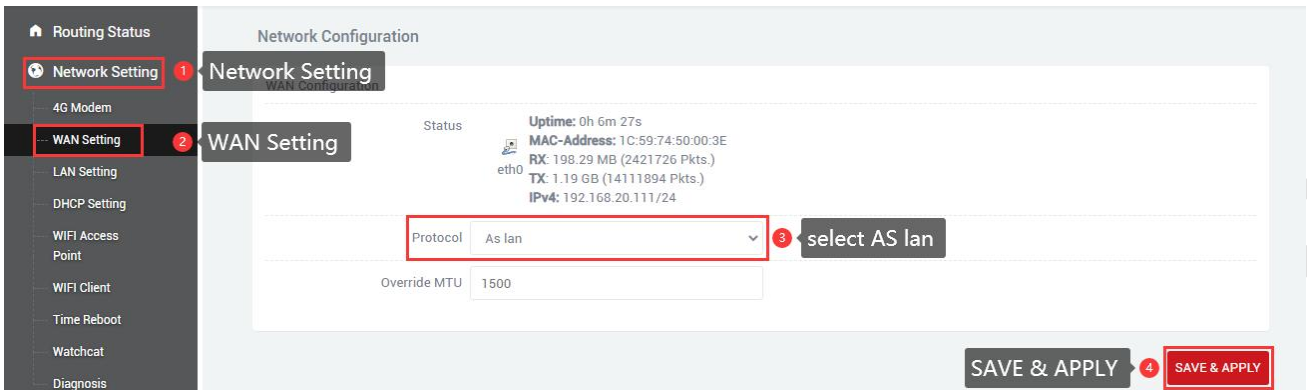
2.3.3 Static address

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, and the value of MTU does not need to be changed (default value: 1500).



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, the value of MTU does not need to be changed (default value: 1500).



The screenshot shows the 'Network Configuration' page. On the left sidebar, 'Network Setting' is selected (1), and 'WAN Setting' is highlighted (2). The main content area shows the 'WAN Setting' configuration for the 'eth0' interface. The 'Protocol' dropdown is set to 'As lan' (3), with a callout 'select AS lan'. The 'Override MTU' is set to 1500. At the bottom right, there are two 'SAVE & APPLY' buttons (4).

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.

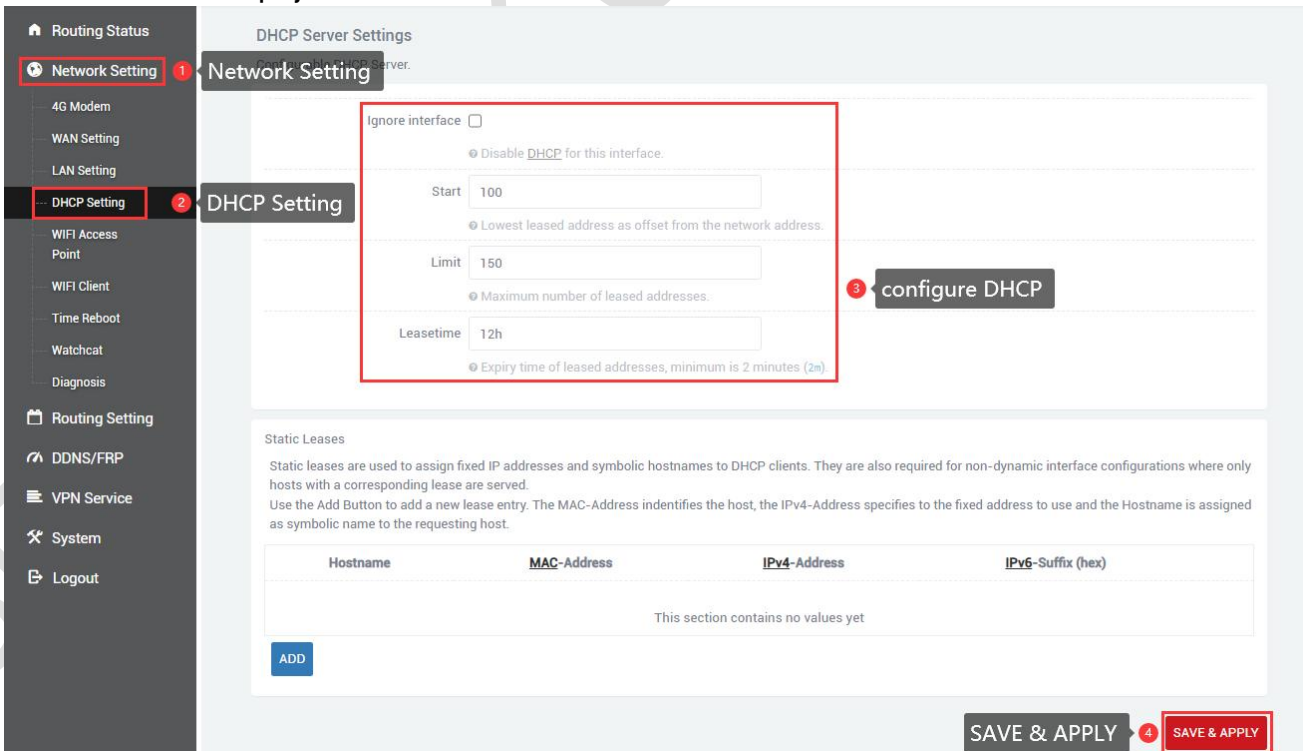
DHCP client configuration (enabled by default), select "Network Setting" - "DHCP Settings", "SAVE & APPLY".

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.

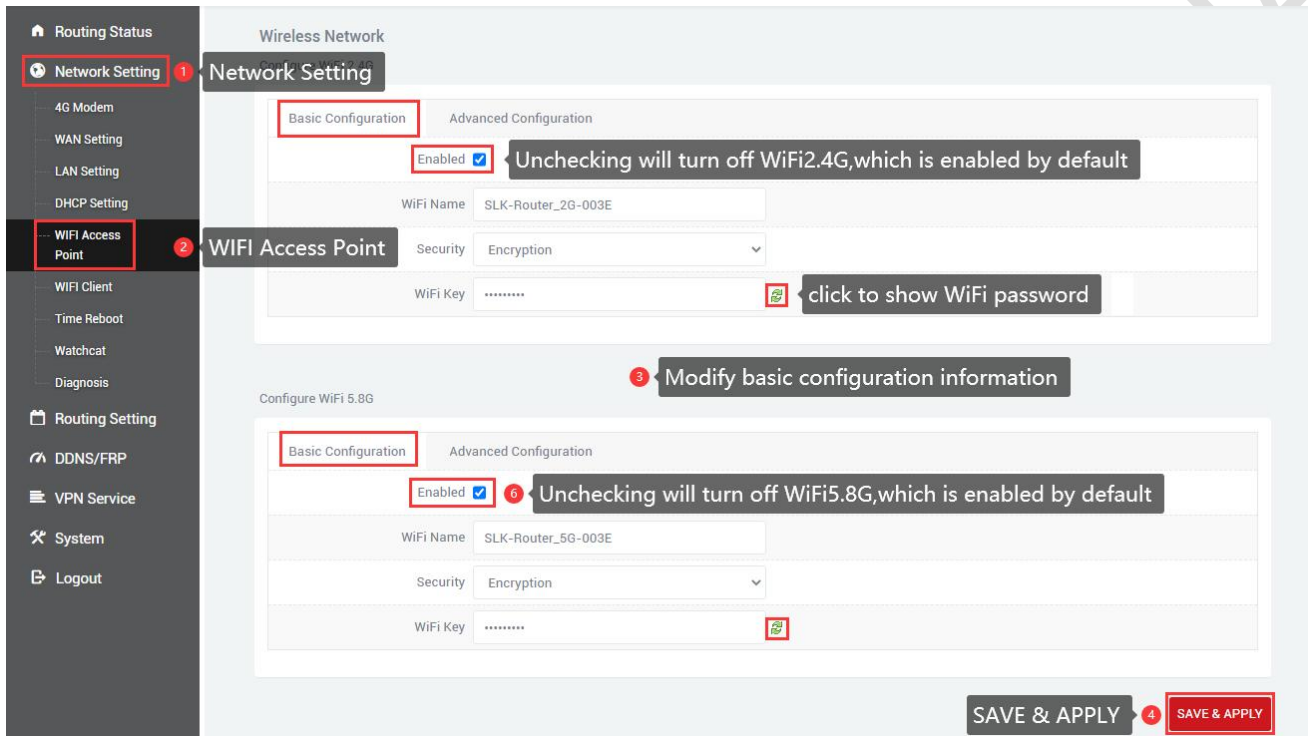
D.Leasetime: Expiry time of leased addresses.



The screenshot shows the 'DHCP Server Settings' page. On the left sidebar, 'Network Setting' is selected (1), and 'DHCP Setting' is highlighted (2). The main content area shows the 'DHCP Server Settings' configuration. The 'Ignore interface' checkbox is unchecked. The 'Start' field is set to 100, 'Limit' is set to 150, and 'Leasetime' is set to 12h. A callout 'configure DHCP' (3) points to the configuration fields. At the bottom right, there are two 'SAVE & APPLY' buttons (4).

2.5 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 Access Point", you can change the basic configuration of WiFi.



The screenshot displays the 'Network Setting' page with the 'WiFi Access Point' sub-section selected. It shows configuration options for both 2.4G and 5.8G WiFi bands. Key elements include:

- Navigation Bar:** 'Network Setting' (1) and 'WiFi Access Point' (2).
- Basic Configuration:** Includes an 'Enabled' checkbox (3) with a tooltip: 'Unchecking will turn off WiFi2.4G, which is enabled by default'. Below this are fields for 'WiFi Name' (SLK-Router_2G-003E), 'Security' (Encryption), and 'WiFi Key' (masked with dots).
- Advanced Configuration:** A button labeled 'click to show WiFi password' is visible.
- Configure WiFi 5.8G:** Similar to the 2.4G section, it has an 'Enabled' checkbox (6) with a tooltip: 'Unchecking will turn off WiFi5.8G, which is enabled by default'. It also includes fields for 'WiFi Name' (SLK-Router_5G-003E), 'Security' (Encryption), and 'WiFi Key'.
- Buttons:** Two 'SAVE & APPLY' buttons (4) are located at the bottom right.

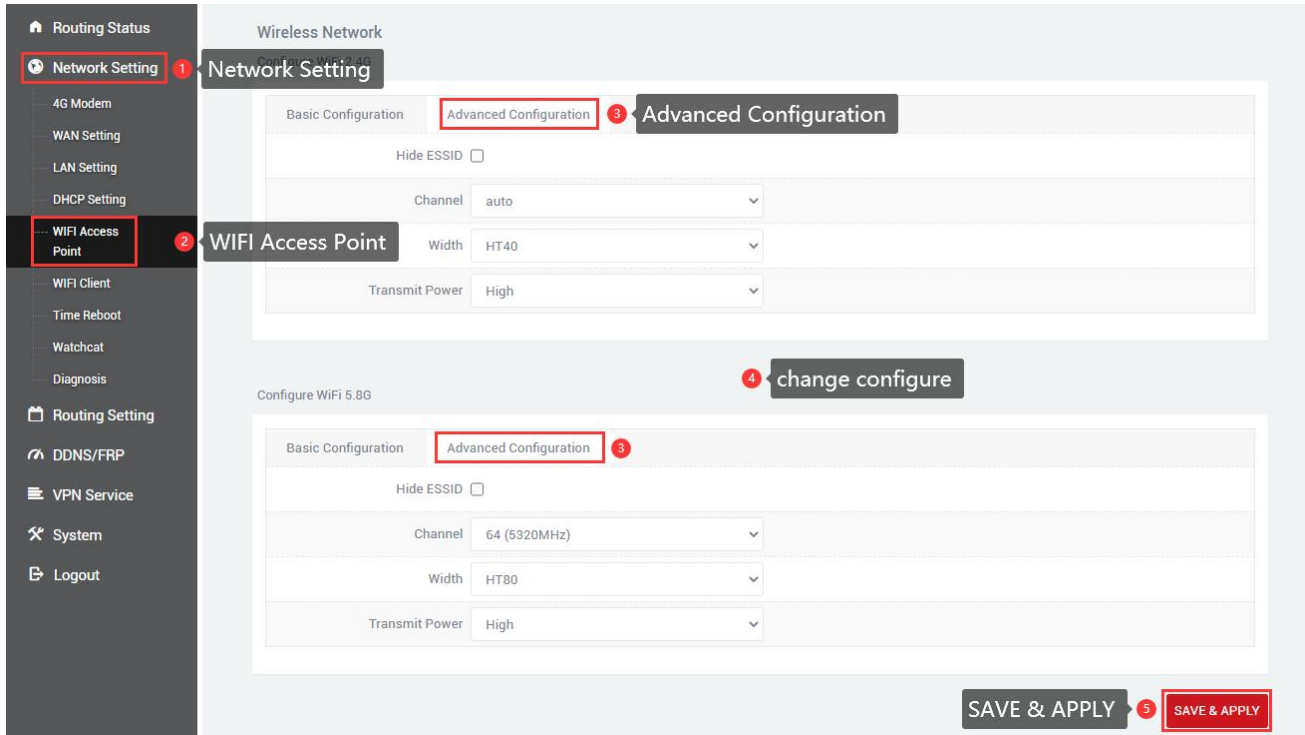
Navigation bar "Network Setting" - "WiFi Access Point" - "Advanced Configuration", under normal circumstances do not need to modify.

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

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.

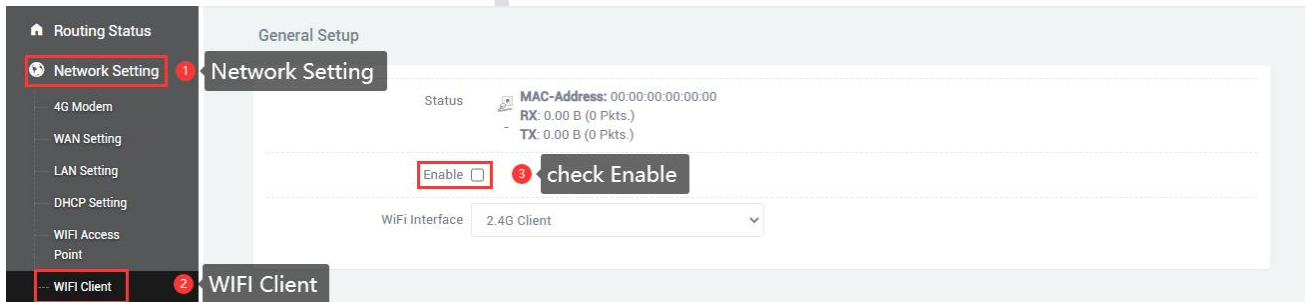
Width: WiFi speed HT80 (5.8G exclusive) > HT40 > HT20, WiFi stability HT20 > HT40 > HT80 (5.8G exclusive), affected by distance and partitions (such as walls), use large bandwidth at close range, use a small bandwidth for long distances.

Transmit Power: The higher the power, the better the wifi performance.




2.6 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.

General Setup

Status  **MAC-Address:** 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Enable

WiFi Interface 2.4G Client 4 select client interface


Scan SCAN 5 click scan

SSID __TEST_AP

Security WIFI6-2G 6 choose wifi

WDS

General Setup

Status  **MAC-Address:** 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Enable

WiFi Interface 2.4G Client

Scan SCAN

SSID WIFI6-2G

Security Encryption 7 security choose None or Encryption

Key ***** 8 if you choose Encryption,you need to enter a password

WDS


Advanced Settings

Protocol DHCP address

LAN port of bridge should share the same network segment with upstream equipment

SAVE & APPLY 9 SAVE & APPLY

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

Status 

Client "WIFI6-2G"

Uptime: 0h 0m 31s
MAC-Address: 06:03:7F:12:F2:1F
RX: 7.65 KB (63 Pkts.)
TX: 1.72 KB (9 Pkts.)
IPv4: 192.168.100.153/24

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).

Advanced Settings

Protocol	Static address	1	Select Static address
LAN port of bridge should share the same network segment with upstream equipment			
IP Address	192.168.100.117	2	Set the IP on the same network segment as the upper-level router
Netmask	255.255.255.0		
Gateway	192.168.100.1	3	Set as the upper-level routing IP
DNS	192.168.100.1	4	Generic DNS or upper-level routing IP, can be multiple

SAVE & APPLY
5 SAVE & APPLY

Status


 Client "WIFI6-2G"

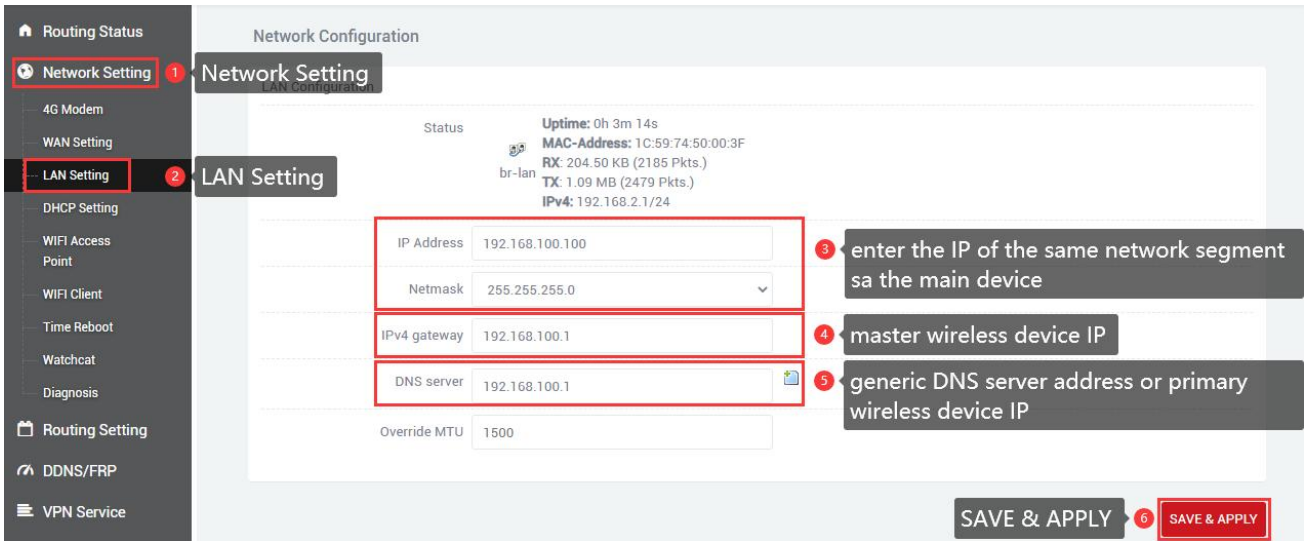
Uptime: 0h 0m 11s
 MAC-Address: 06:03:7F:12:F2:1F
 RX: 330.00 B (2 Pkts.)
 TX: 296.00 B (2 Pkts.)
IPv4: 192.168.100.117/24

2.7 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.

2.7.1 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.



Network Configuration

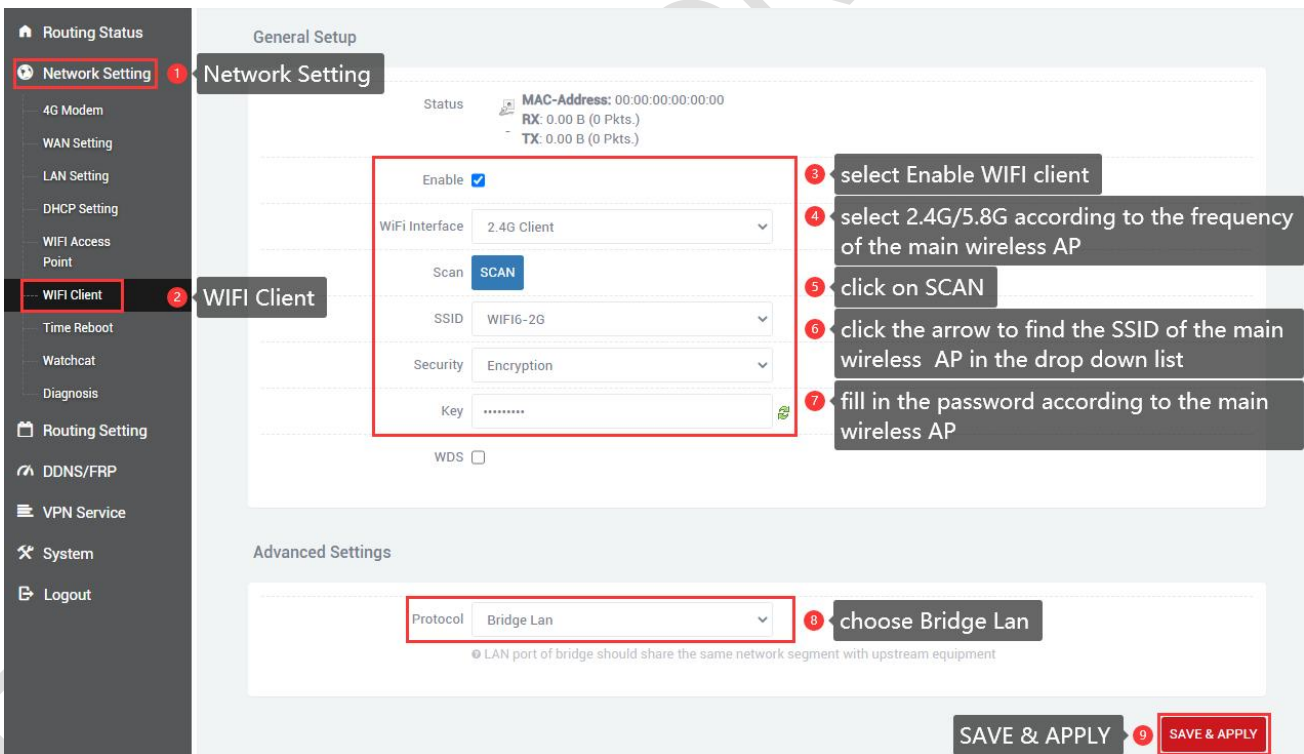
Status: Uptime: 0h 3m 14s
 MAC-Address: 1C:59:74:50:00:3F
 RX: 204.50 KB (2185 Pkts.)
 TX: 1.09 MB (2479 Pkts.)
 IPv4: 192.168.2.1/24

IP Address	192.168.100.100	3 enter the IP of the same network segment as the main device
Netmask	255.255.255.0	
IPv4 gateway	192.168.100.1	4 master wireless device IP
DNS server	192.168.100.1	5 generic DNS server address or primary wireless device IP
Override MTU	1500	

SAVE & APPLY 6 SAVE & APPLY

2.7.2 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".



General Setup

Status: MAC-Address: 00:00:00:00:00:00
 RX: 0.00 B (0 Pkts.)
 TX: 0.00 B (0 Pkts.)

Enable	<input checked="" type="checkbox"/>	3 select Enable WIFI client
WiFi Interface	2.4G Client	4 select 2.4G/5.8G according to the frequency of the main wireless AP
Scan	SCAN	5 click on SCAN
SSID	WIFI6-2G	6 click the arrow to find the SSID of the main wireless AP in the drop down list
Security	Encryption	
Key	7 fill in the password according to the main wireless AP

WDS

Advanced Settings

Protocol	Bridge Lan	8 choose Bridge Lan
----------	------------	---------------------

© LAN port of bridge should share the same network segment with upstream equipment

SAVE & APPLY 9 SAVE & APPLY

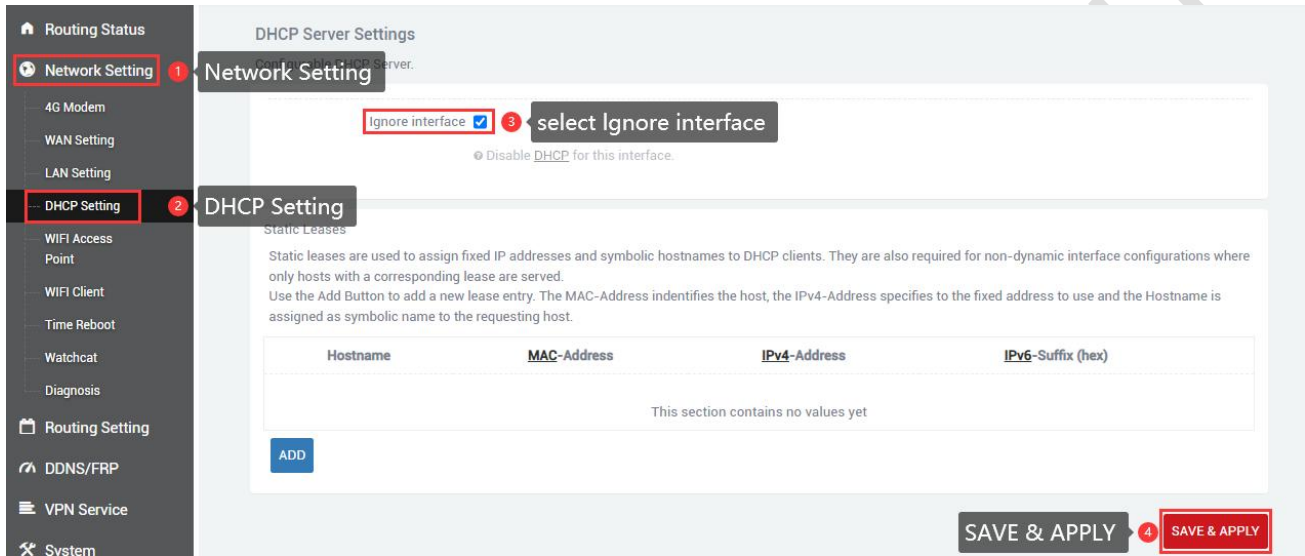
It should be noted that in this mode, the main wireless AP no longer assigns an IP address to this SLK-R680. Therefore, the obtained IP address will not be updated in "Status", and you can confirm whether the connection is successful through the icon color and MAC address. The picture below is successful.

Status

Uptime: 0h 0m 0s
MAC-Address: 06:03:7F:12:F2:1F
Client "WIFI6-2G" RX: 3.69 KB (25 Pkts.)
TX: 3.57 KB (34 Pkts.)

2.7.3 Disable DHCP

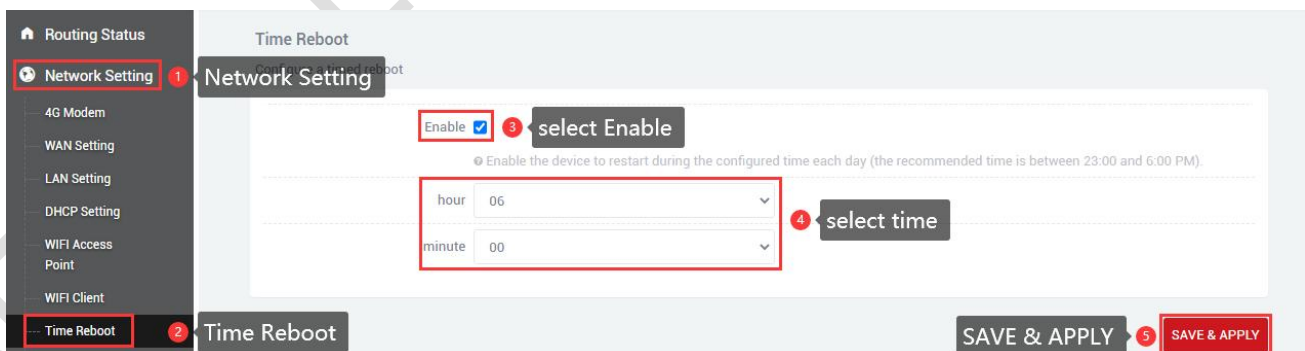
Disable the DHCP server function of the SLK-R680. In this way, the SLK-R680 no longer assigns IP addresses to the connected devices, and all devices connected to the local area network are assigned IP addresses by the main wireless to realize communication on the same network segment.



The screenshot shows the DHCP Server Settings page. The left navigation menu has "Network Setting" selected (1) and "DHCP Setting" selected (2). The main content area is titled "DHCP Server Settings" and includes a "Network Setting" section with an "Ignore interface" checkbox checked (3) and a "select Ignore interface" button. Below this is a "Static Leases" section with a table for adding leases. The table has columns for Hostname, MAC-Address, IPv4-Address, and IPv6-Suffix (hex). The table is currently empty, with the text "This section contains no values yet" and an "ADD" button. At the bottom right, there are "SAVE & APPLY" buttons (4).

2.8 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 5.1 for details.



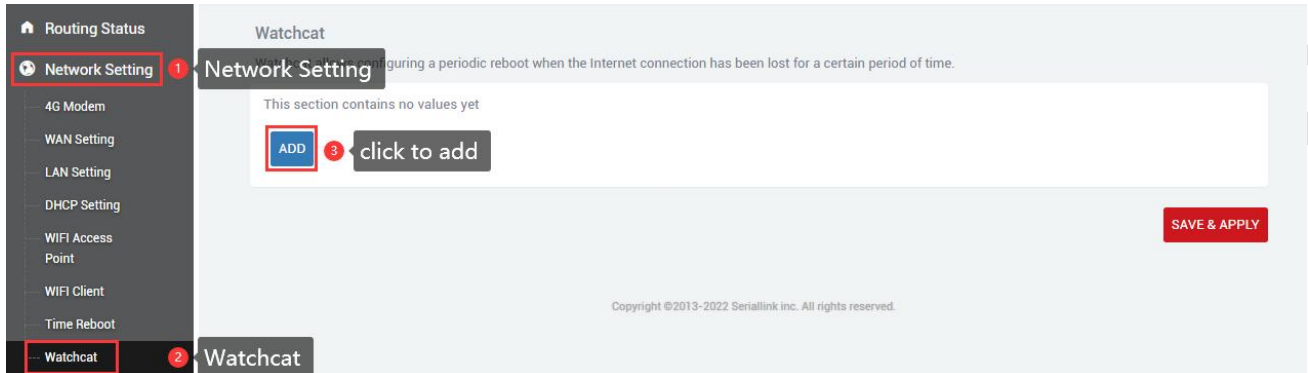
The screenshot shows the Time Reboot page. The left navigation menu has "Network Setting" selected (1) and "Time Reboot" selected (2). The main content area is titled "Time Reboot" and includes an "Enable" checkbox checked (3) and a "select Enable" button. Below this is a "select time" section with two dropdown menus for "hour" (06) and "minute" (00) (4). At the bottom right, there are "SAVE & APPLY" buttons (5).

2.9 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".

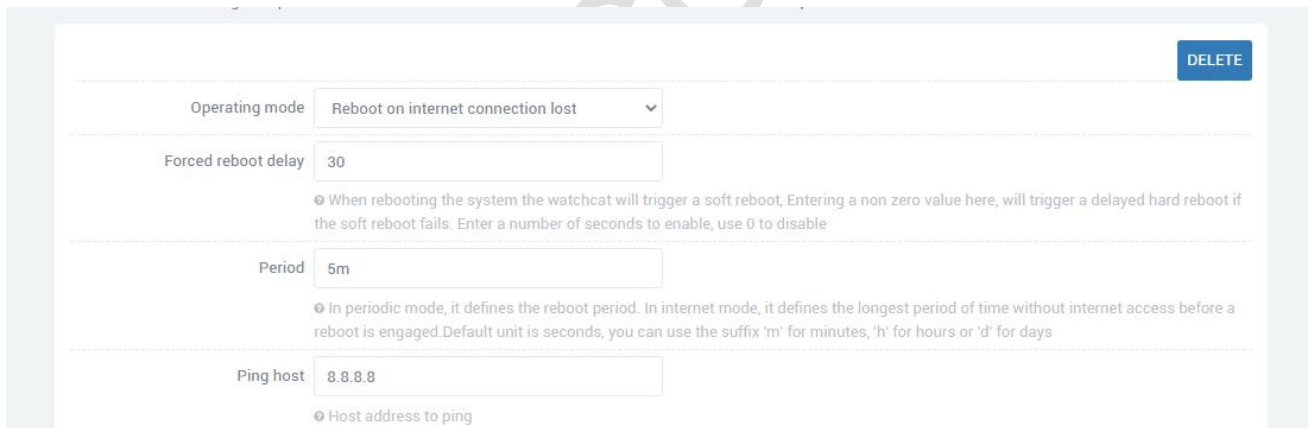


A. Forced reboot delay: When rebooting the system the watchcat will trigger a soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable

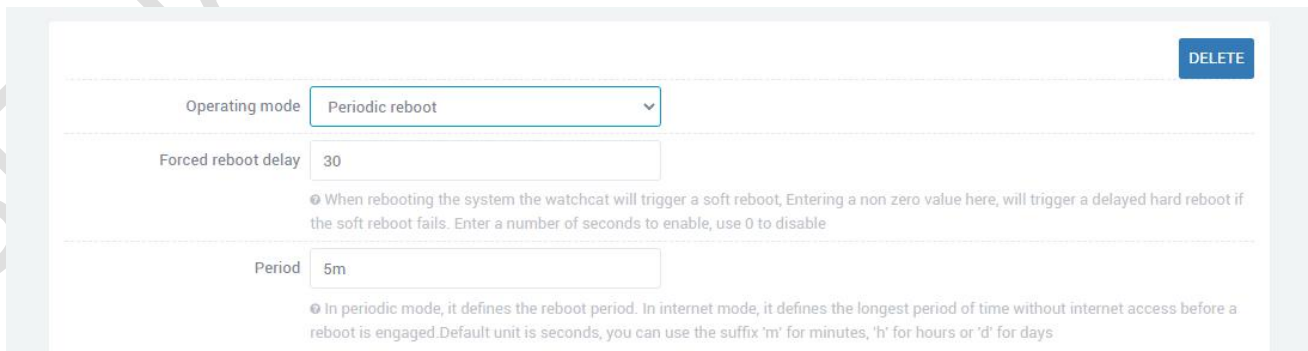
B. Period: In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

C. Ping host: Host address to ping

1. Reboot on internet connection lost



2. Periodic reboot



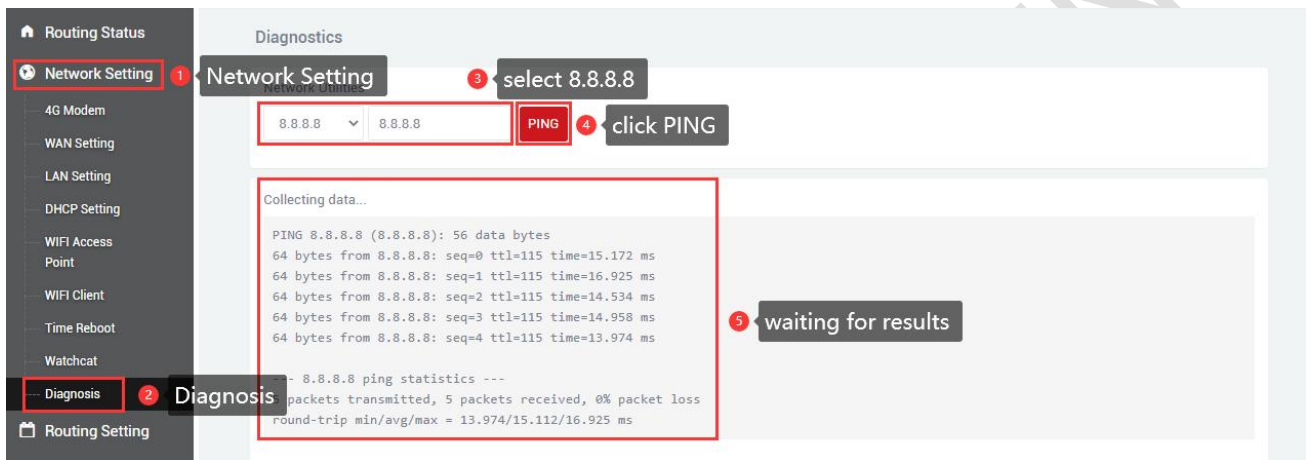
After adding and configuring, click "SAVE & APPLY" to take effect. To delete the configuration, just click the "DELETE" button in the upper right corner, and then "SAVE & APPLY".

2.10 Diagnosis

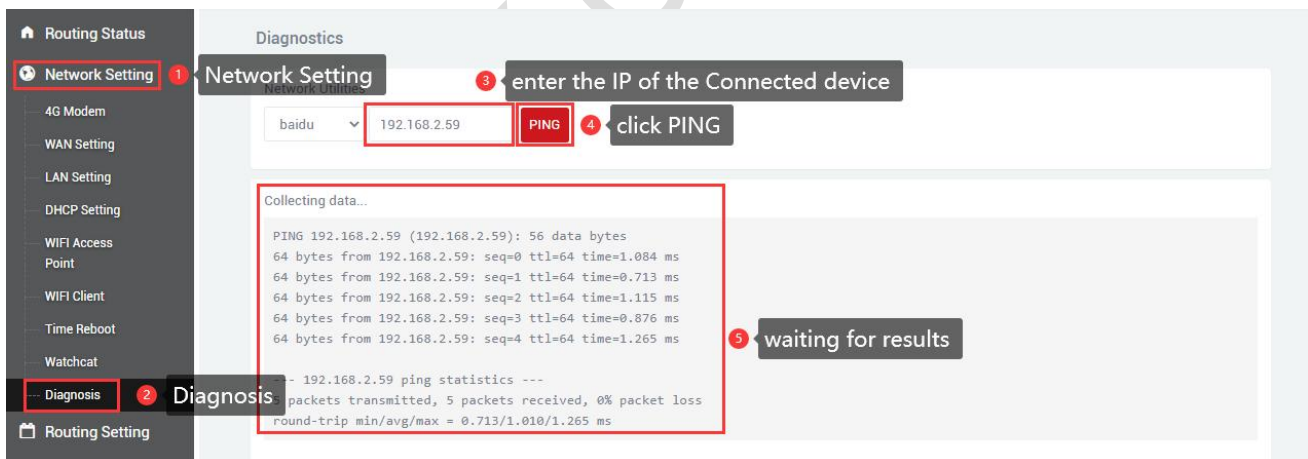
Through network diagnosis, you can determine whether the router and the connected device can communicate with each other, whether the device can access the Internet, and whether the device is successfully connected to the VPN. It can also be used to test other aspects, and you can test it according to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

3.1 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".



3.2 DMZ

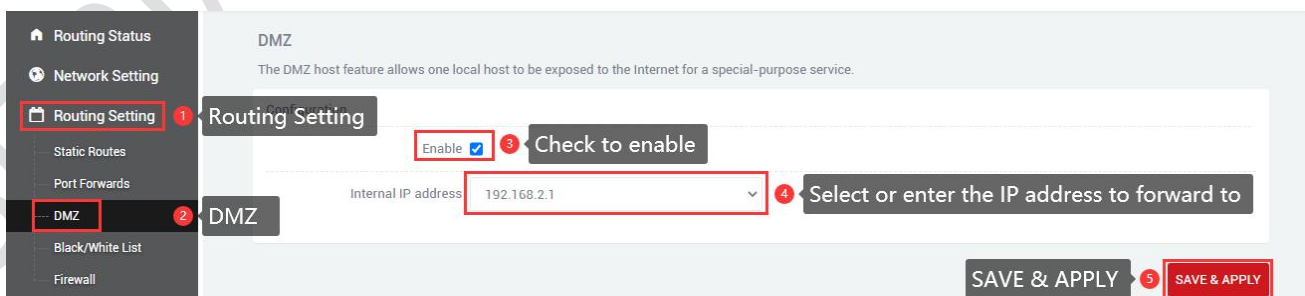
The DMZ function can map the WAN port address to a certain host on the LAN side; all packets to the WAN address will be forwarded to the specified LAN side host to achieve bidirectional communication. In fact, it is to completely expose a host in the intranet to the Internet and open all ports, which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

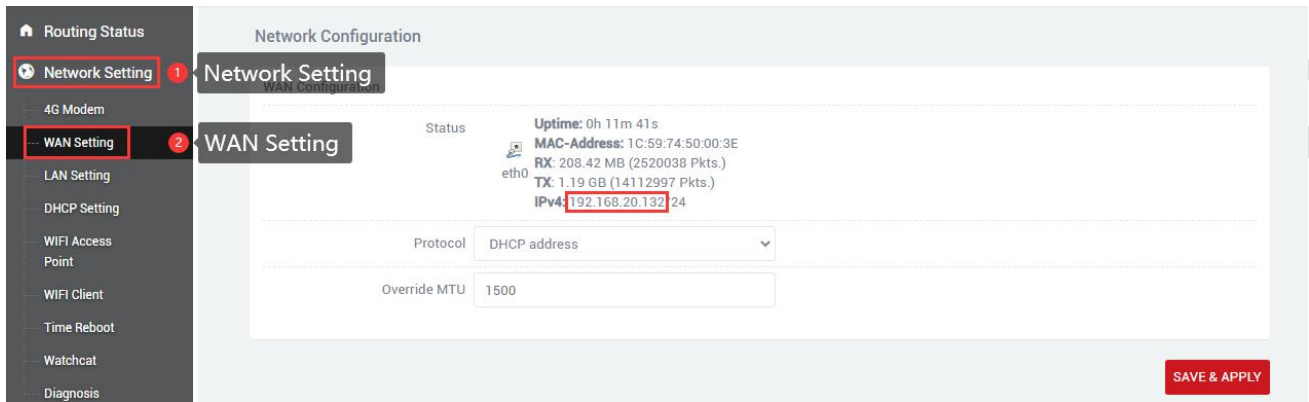
Enable: Tick Enable.

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

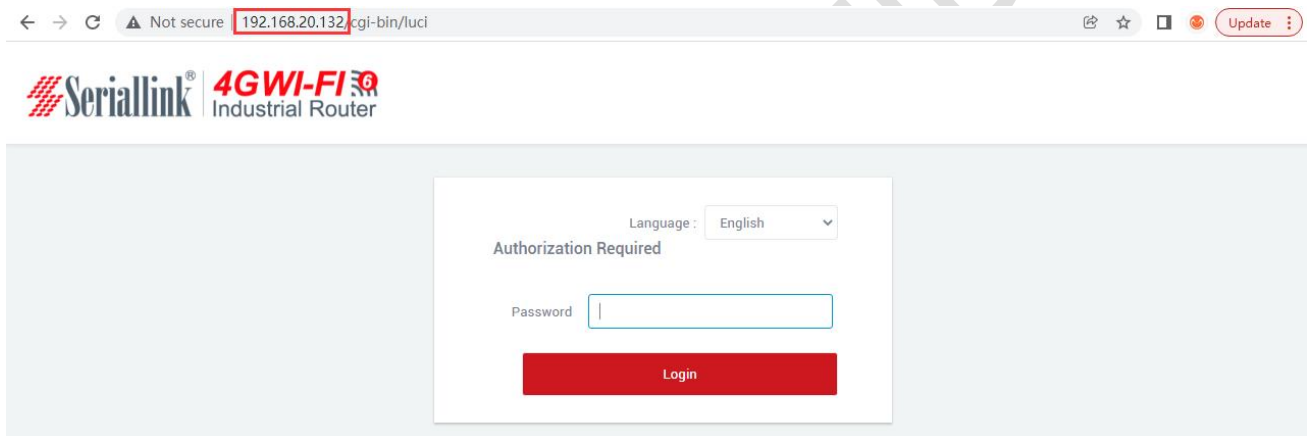
DMZ actually forwards all ports of the device. After the configuration is complete, click "SAVE & APPLY" to make it take effect.



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)



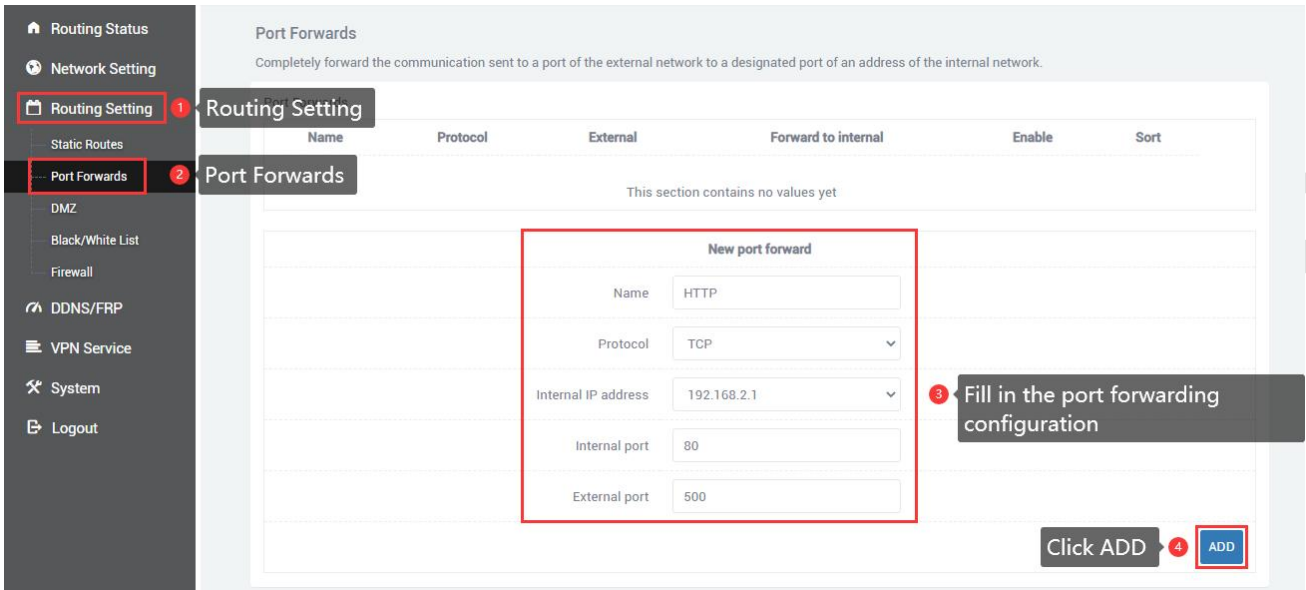
3.3 Prot Forwards

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.

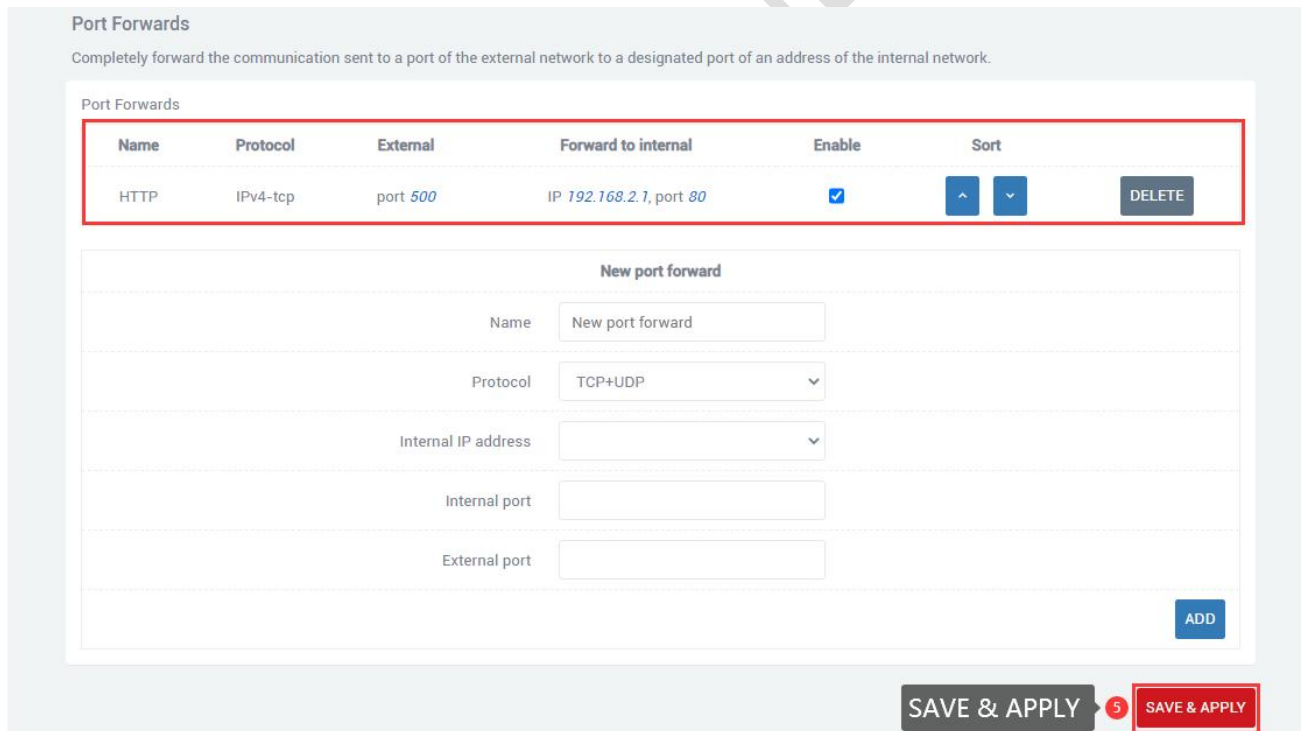
First you need to disable the firewall.

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

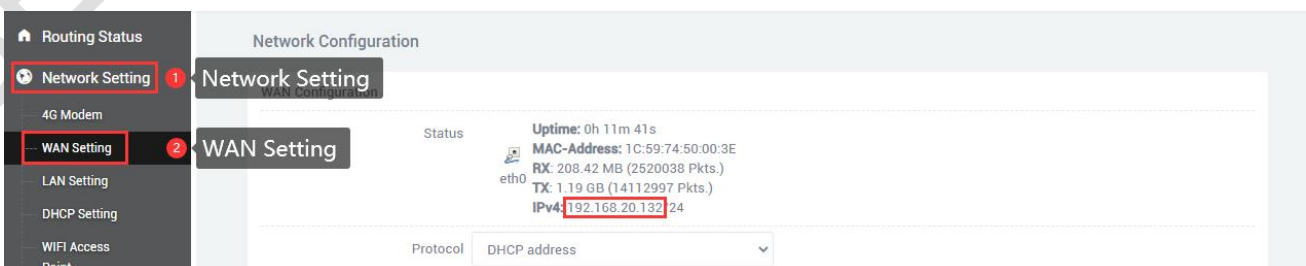
- A.Name: Specify the name of this rule, which can be a meaningful name.
- B.Protocol: Specifies the protocol to be forwarded, which can be TCP, UDP, or TCP/UDP.
- C.Internal IP address: Select the IP address that needs to be forwarded to the external network.
- D.Internall port: The port to be forwarded 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.



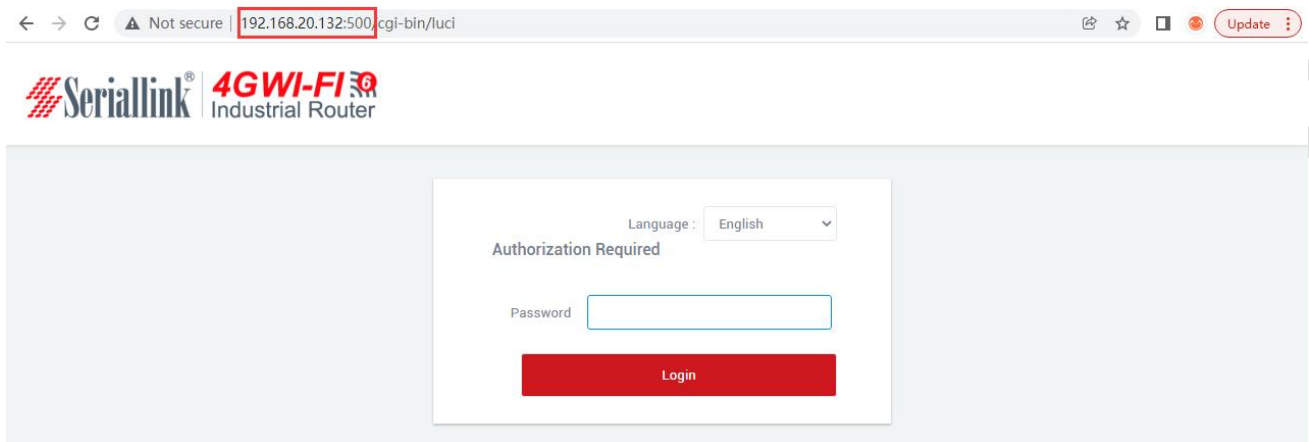
After the addition is successful, a port forwarding rule will be added. Click "SAVE & APPLY" to make the rule take effect. Multiple rules can be added.



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 192.168.20.132:500. (Note: The computer needs to be in the same local area network as the IP of the wan port before it can be accessed)

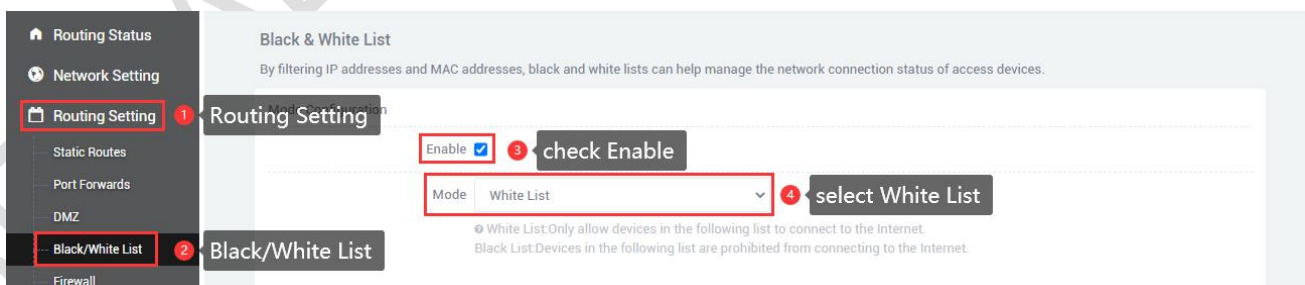


3.4 Black/White List

3.4.1 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.



New list

Name	2.59
Protocol	All
Match ICMP type	All
Local IP address	192.168.2.59 (40:8d:5c:7a:f3:f)
Local MAC address	
Destination IP address	192.168.2.1
Action	ACCEPT

5 Customize the name, choose one of the local IP address and the local MAC address, here the target address is the server's public network address, and the action is ACCEPT

click ADD 6 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 192.168.2.1	Accept forward	<input checked="" type="checkbox"/>	<div style="display: flex; align-items: center;"> ^ v </div>	DELETE

SAVE & APPLY 7 SAVE & APPLY

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 183.129.236.223
Pinging 183.129.236.223 with 32 bytes of data:
Reply from 183.129.236.223: bytes=32 time=3ms TTL=62
Reply from 183.129.236.223: bytes=32 time=2ms TTL=62
Reply from 183.129.236.223: bytes=32 time=2ms TTL=62
Reply from 183.129.236.223: bytes=32 time=2ms TTL=62

Ping statistics for 183.129.236.223:
    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.
Reply from 192.168.2.1: Destination port unreachable.
Reply from 192.168.2.1: Destination port unreachable.
Reply from 192.168.2.1: Destination port unreachable.

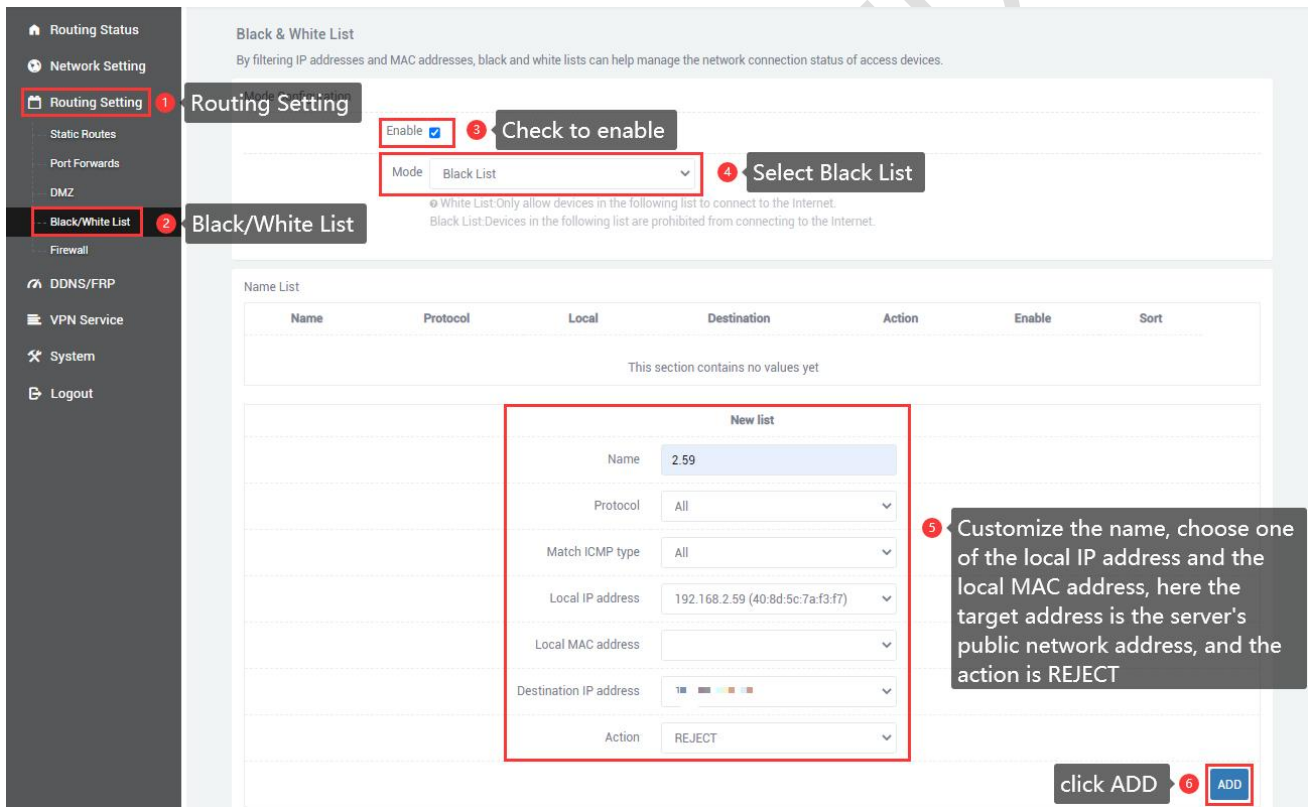
Ping statistics for 14.215.177.38:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    
```

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.

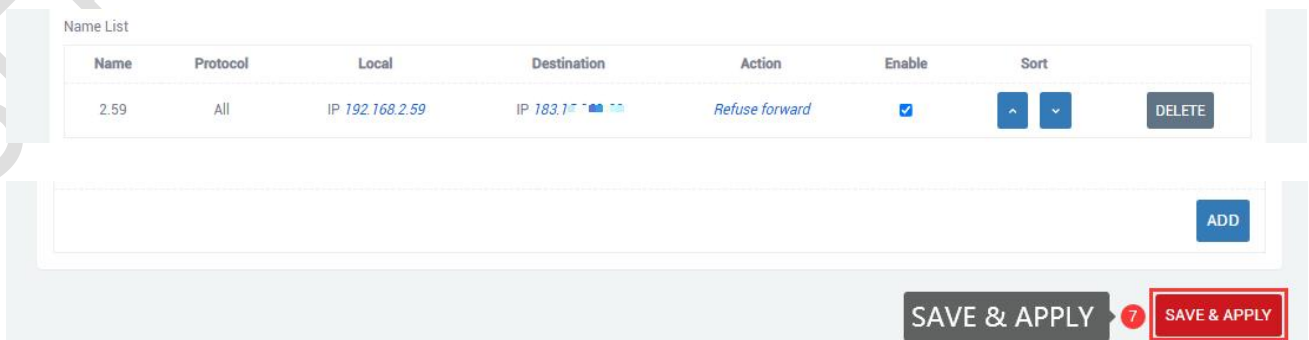
3.4.2 Black List

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.



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



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.
Reply from 192.168.2.1: Destination port unreachable.
Reply from 192.168.2.1: Destination port unreachable.
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".

3.5 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".

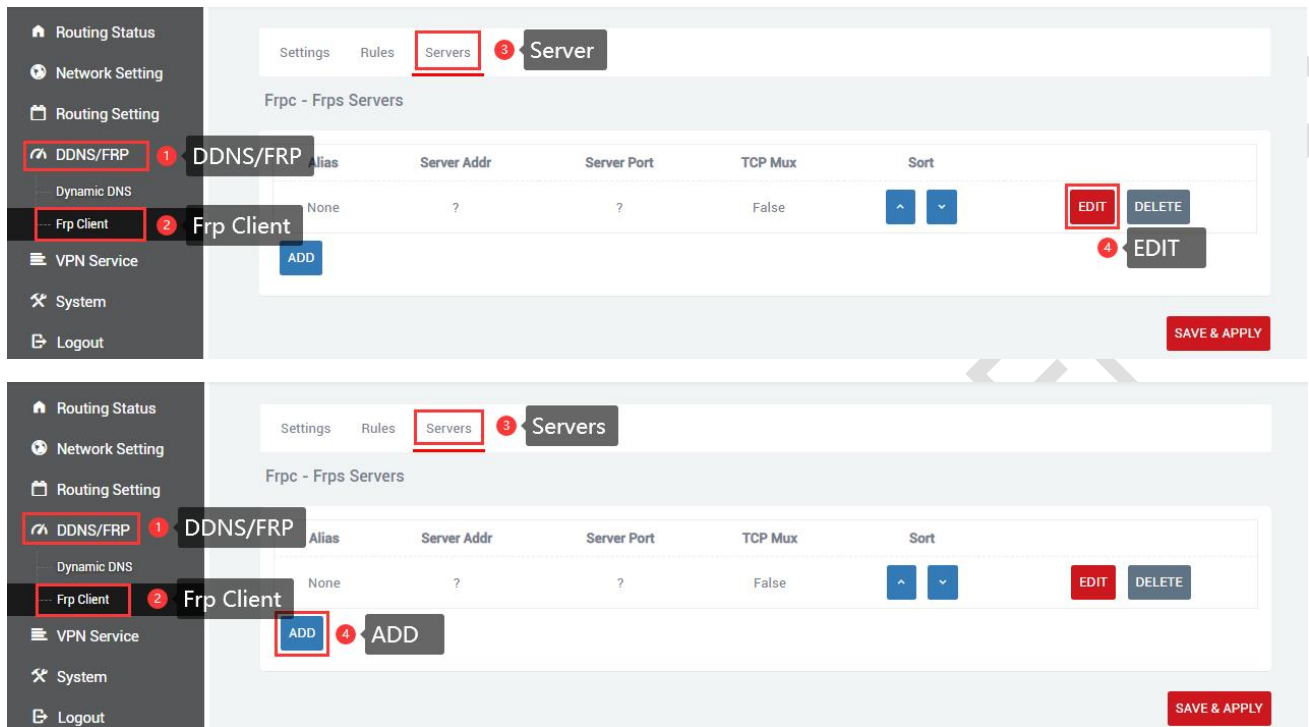
3.5.1 Connect to Frps

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.

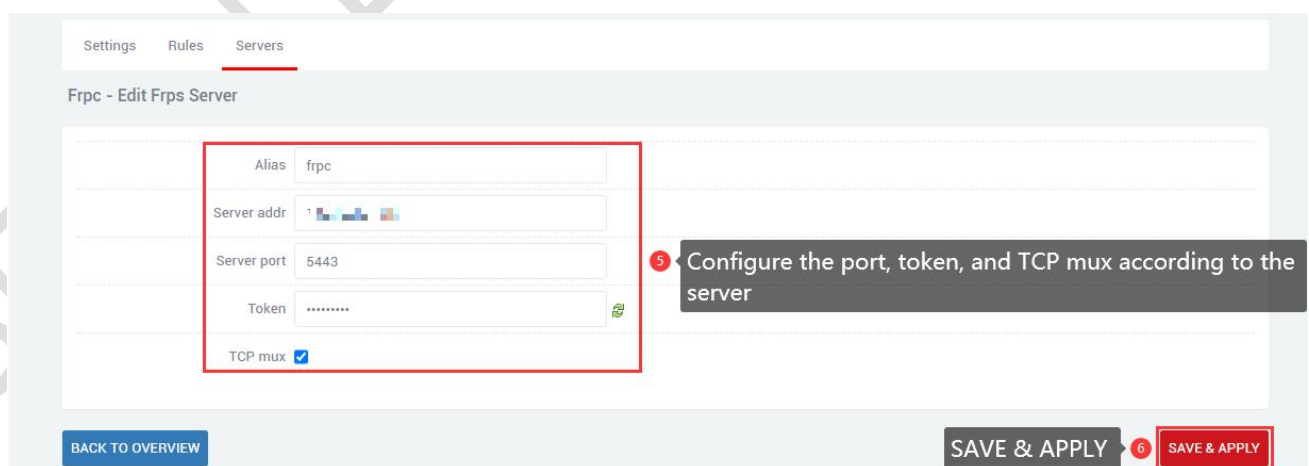
The frp client configuration is as follows:

(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.

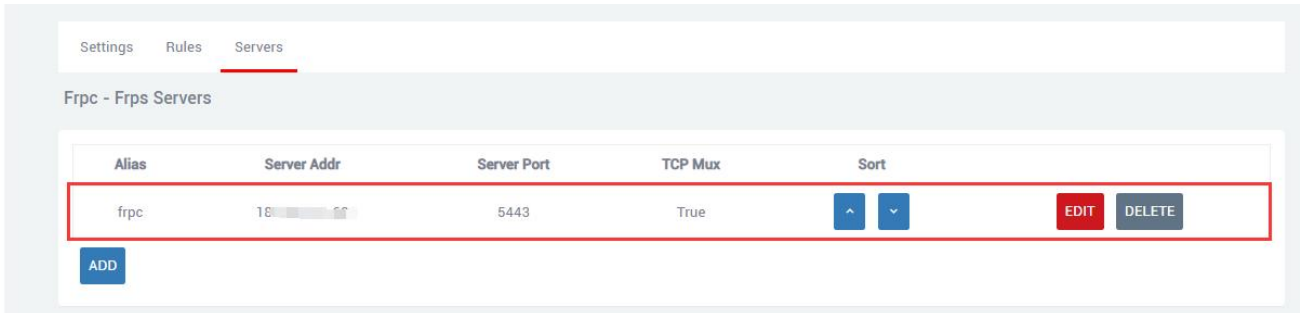


(2)After clicking "ADD" or "EDIT", a page for editing the frps server will pop up, configure it according to the settings of the server, and click "SAVE & APPLY" after the configuration is complete.

- 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.



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



(4)Next, go to the "Settings" page of "Frpc 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 frpc client has been started.

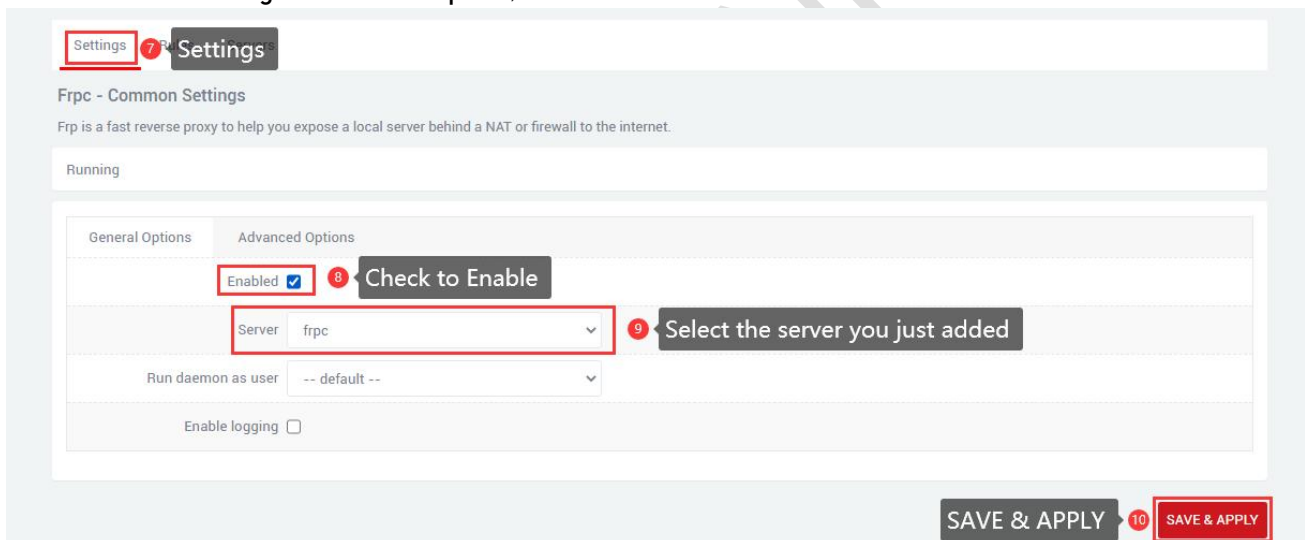
A.Enable: Tick Enabled.

B.Server: The server alias you just customized.

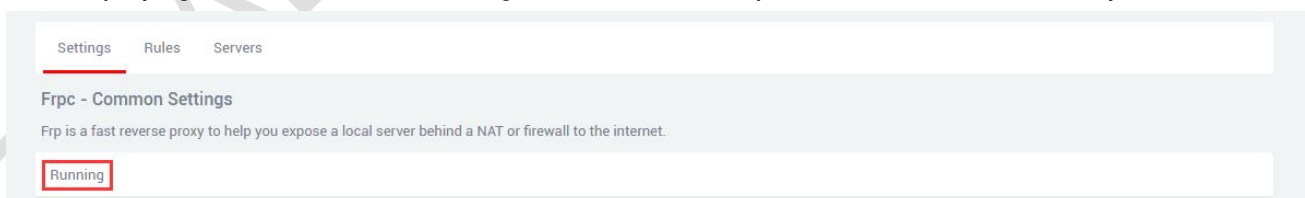
C.Run daemon as user: Generally choose the default, you can modify it according to your needs.

D.Enable logging: Tick as required.

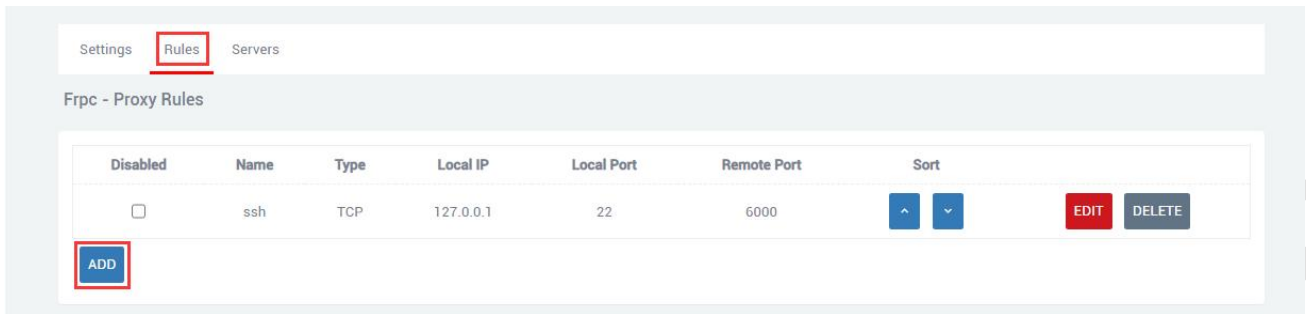
E:After the configuration is complete, click "SAVE & APPLY".



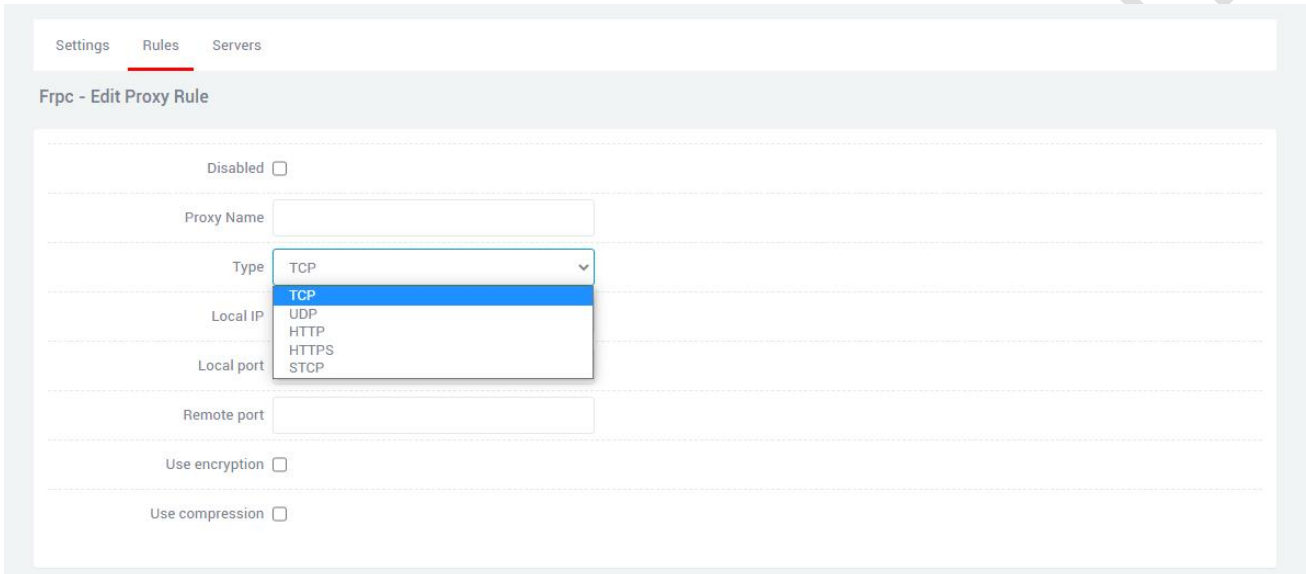
Displaying that the service is running indicates that the frpc client has been successfully started.



(5)Next, go to the "Rules" page of "Frpc 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.



3.5.2 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.

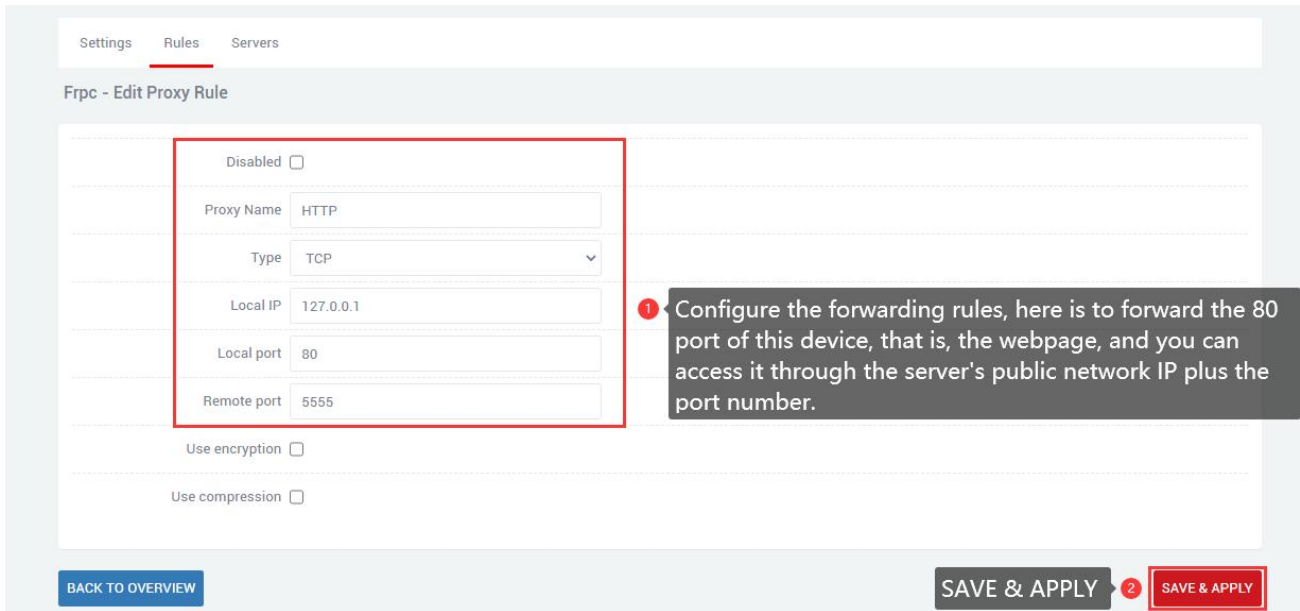
F.Remote port: Add this remote port to the public network address to access the local port opened by

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.

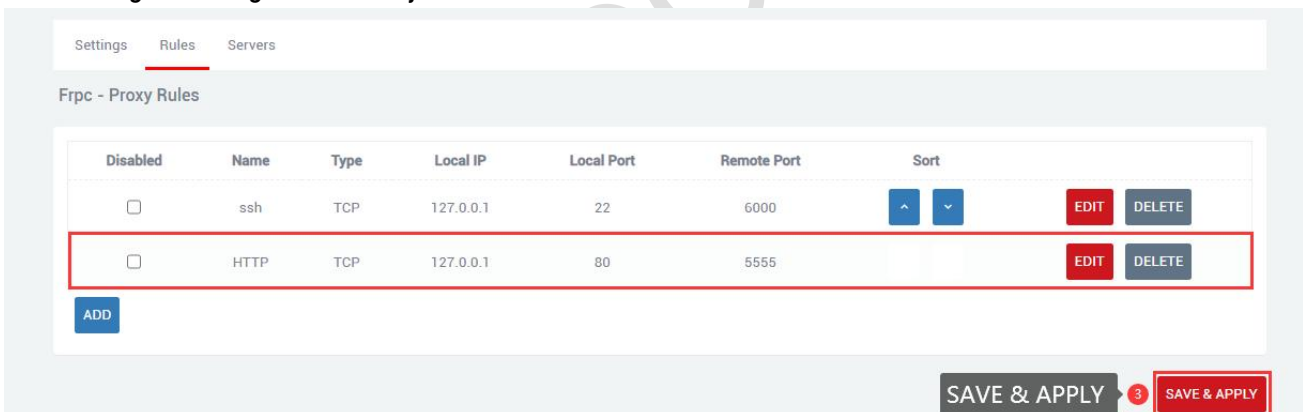
G. Use encryption, Use compression: Check these two as needed.

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

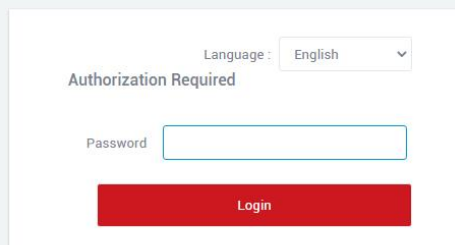
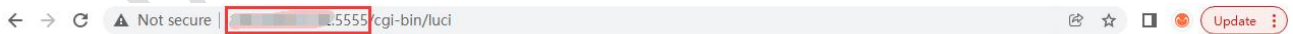
After the configuration is complete, click "SAVE & APPLY".



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



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.

3.5.3 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.

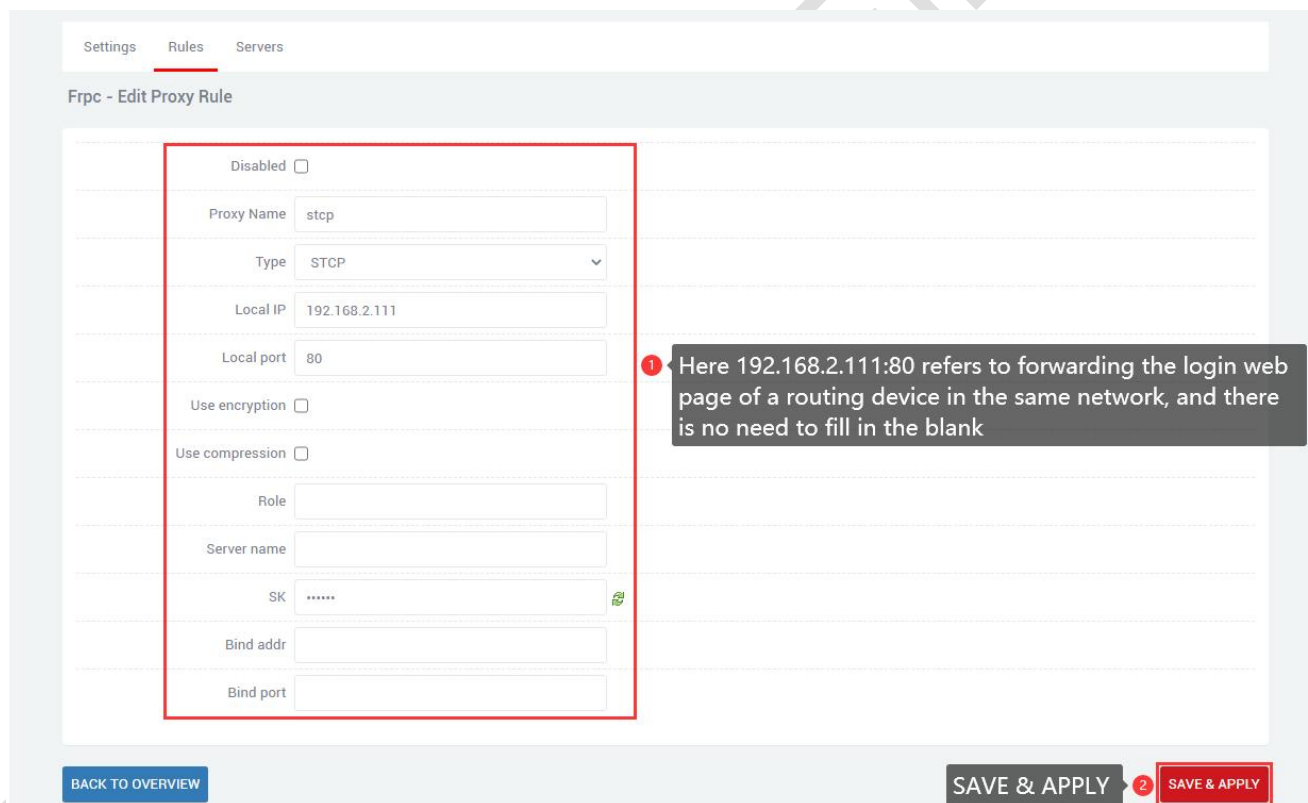
D.Local IP: The IP address assigned by the local device or the lan port to the connected device.

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

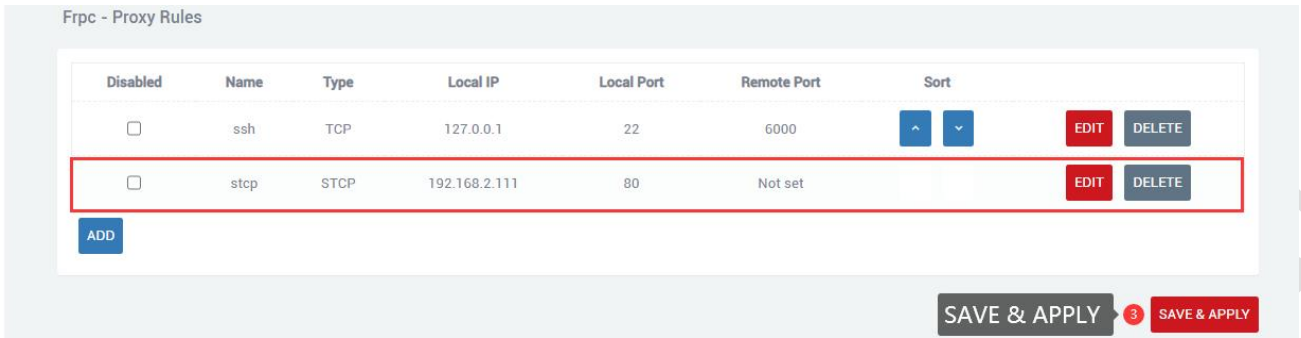
Bind addr

Bind port

1 Here 192.168.2.111:80 refers to forwarding the login web page of a routing device in the same network, and there is no need to fill in the blank

BACK TO OVERVIEW SAVE & APPLY SAVE & APPLY

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



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 frpc 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

frpc.ini - Notepad

```

[common]
#Server public address
server_addr = 192.168.2.111
#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
        
```

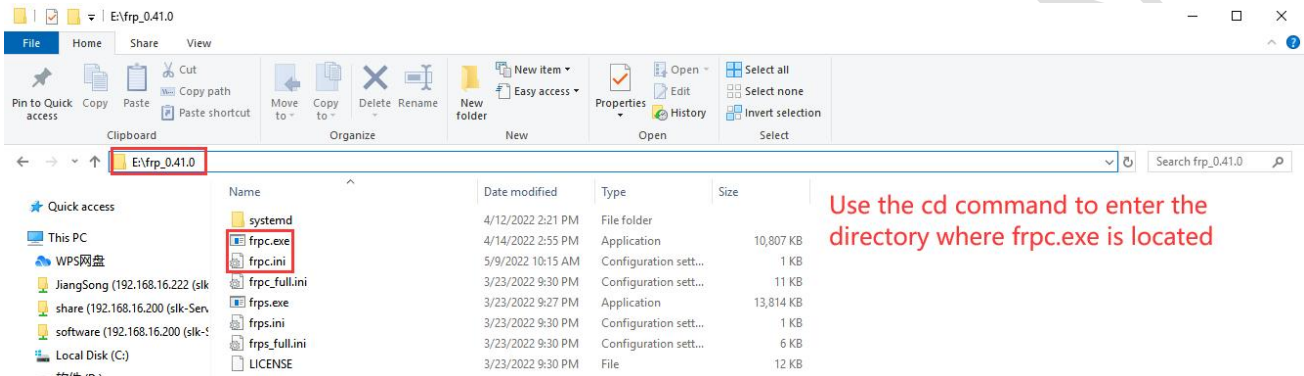
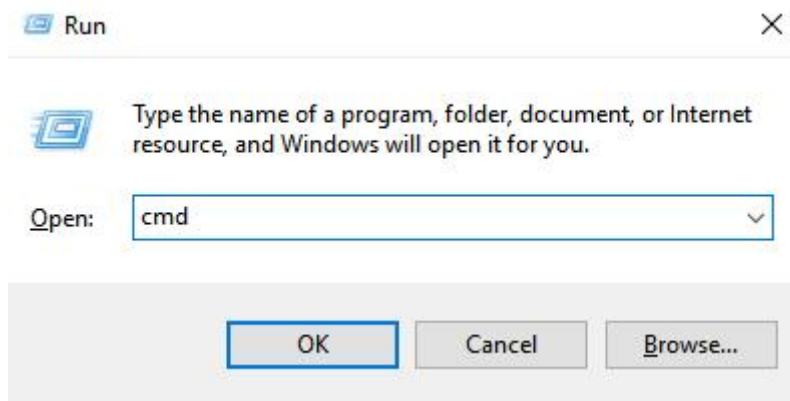
It can be consistent with the configuration of the public network server

Visitor role needs to be set as visitor

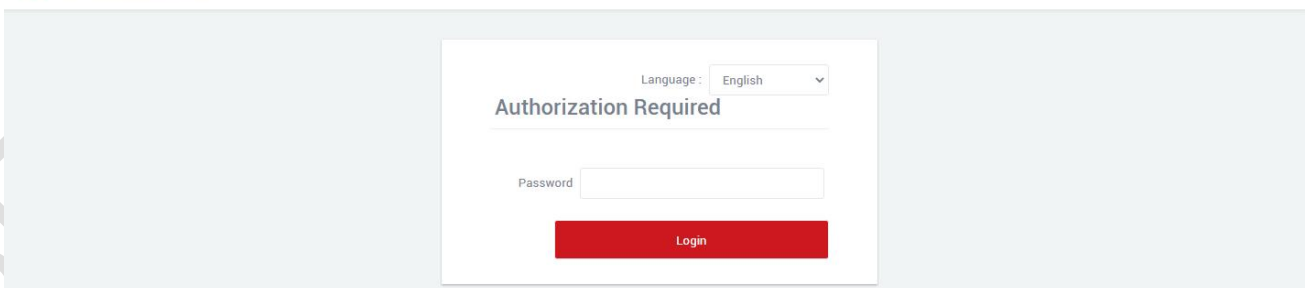
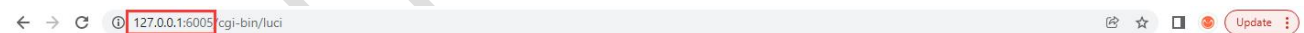
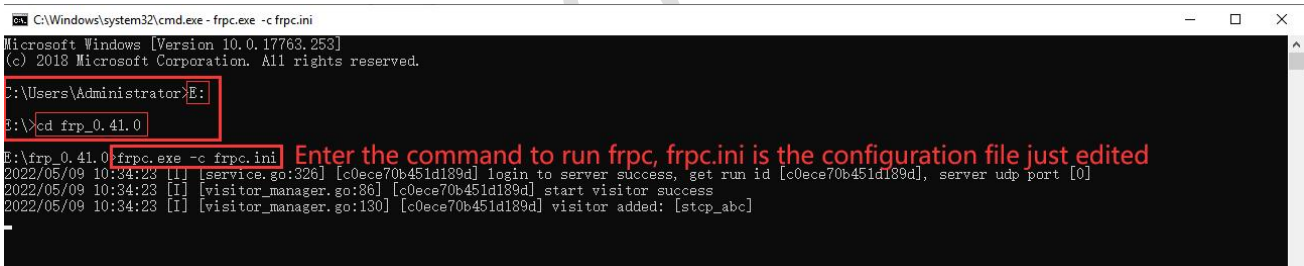
To be consistent with the proxy name of the client to be accessed

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.

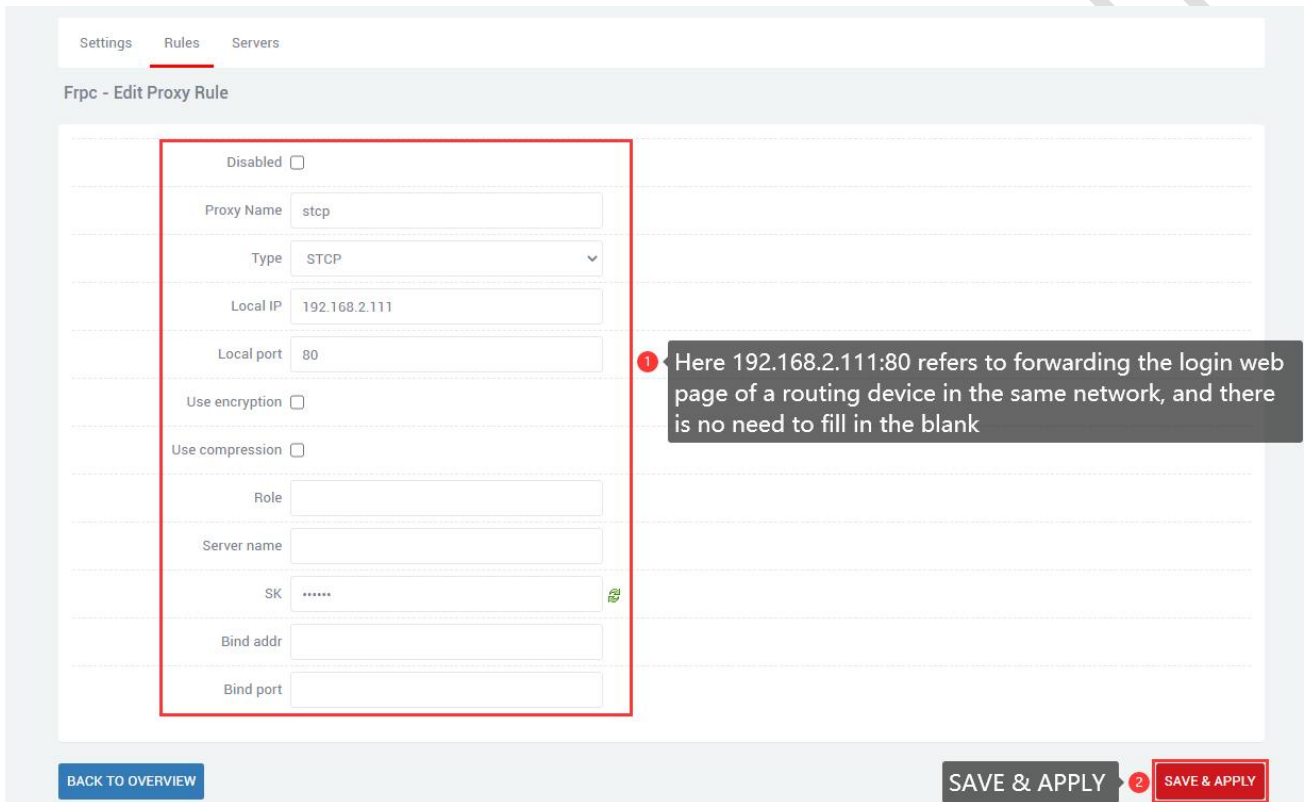


(2) If there are two routers, and one router needs to remotely access the other router or the connected device of the other router, one is the stcp access terminal, and the other is the stcp client.

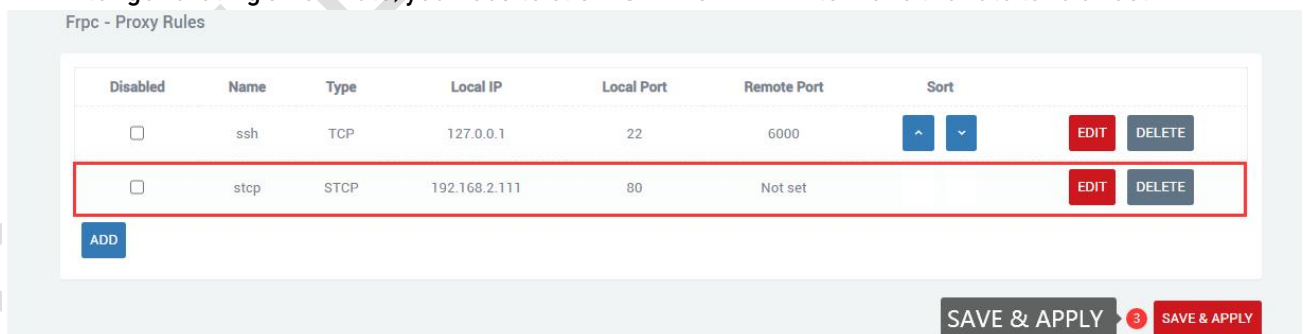
The configuration is as follows:

- 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.



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



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.

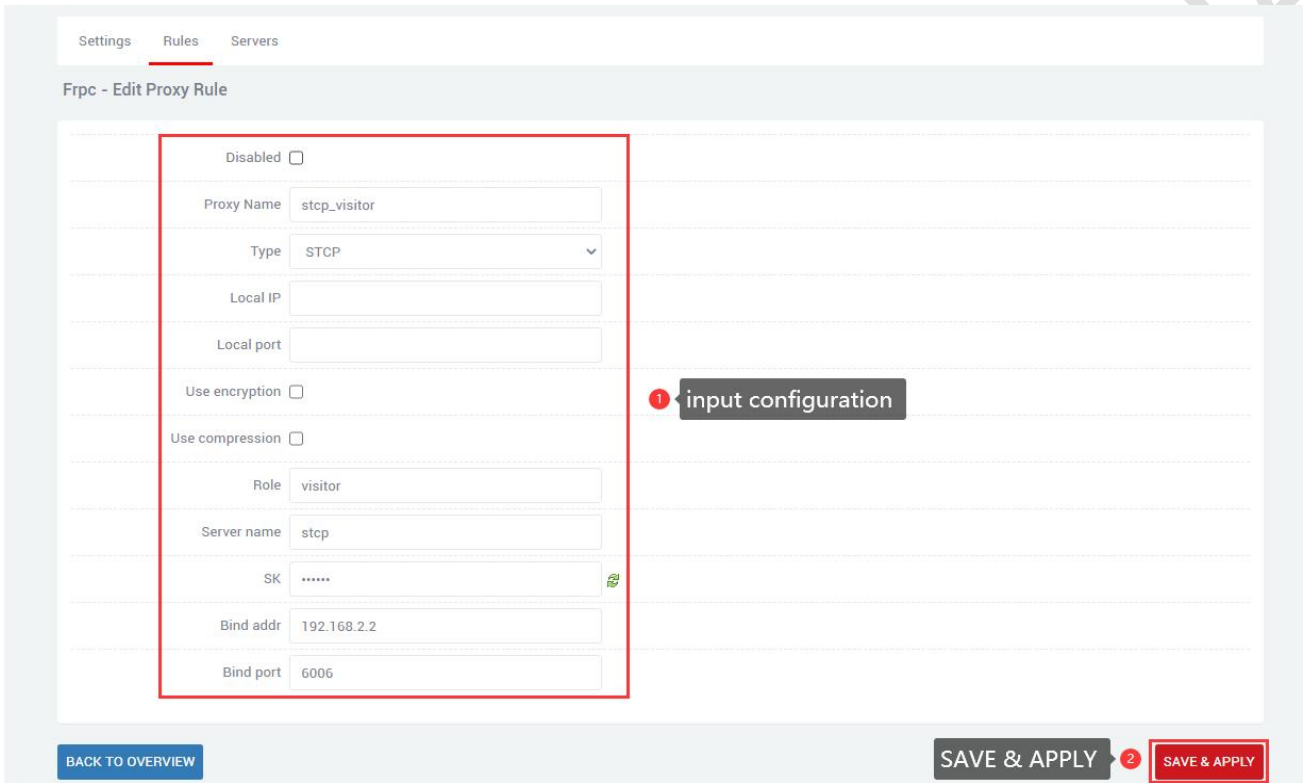
F. SK: Set a password, the access terminal needs to enter the SK set here when accessing the device.

Use encryption, Use compression: Configure as needed.

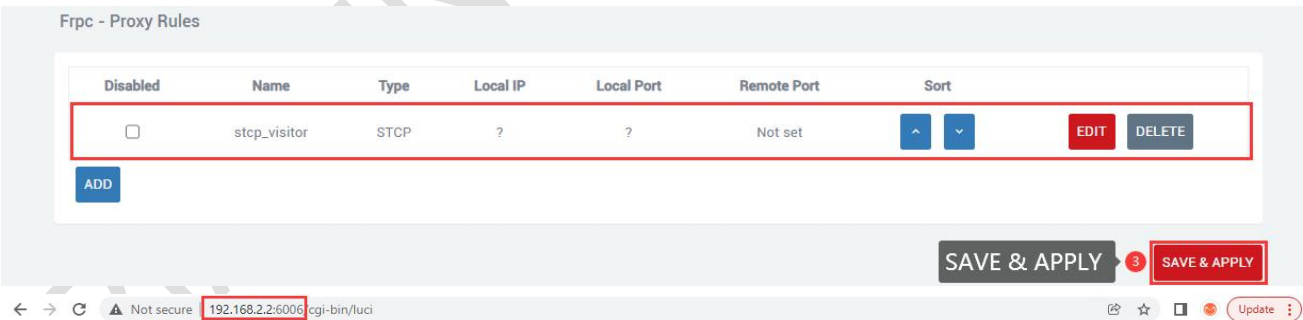
G. Role: The access terminal needs to fill in the visitor.

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

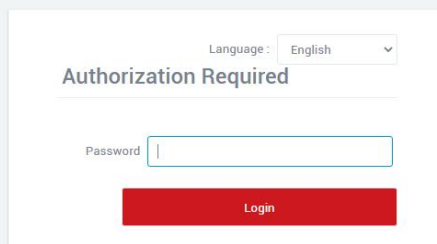
I. Bind addr, Bind port: The client can be accessed by binding the address and port. The address and port are the local machine or the connected device of the local machine.



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



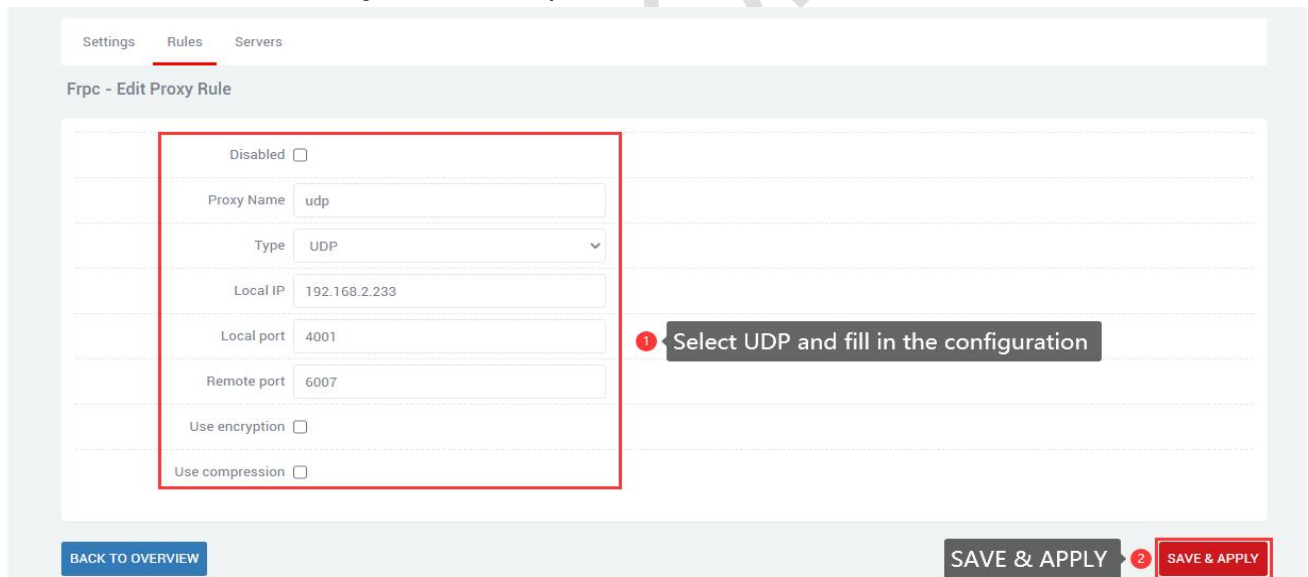
192.168.2.2:6006/cgi-bin/luci



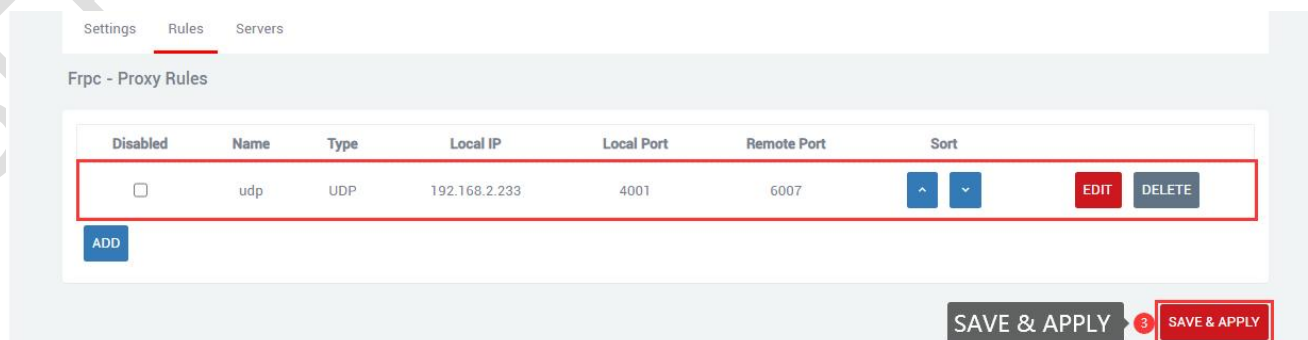
3.5.4 Add UDP Proxy Rules

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.

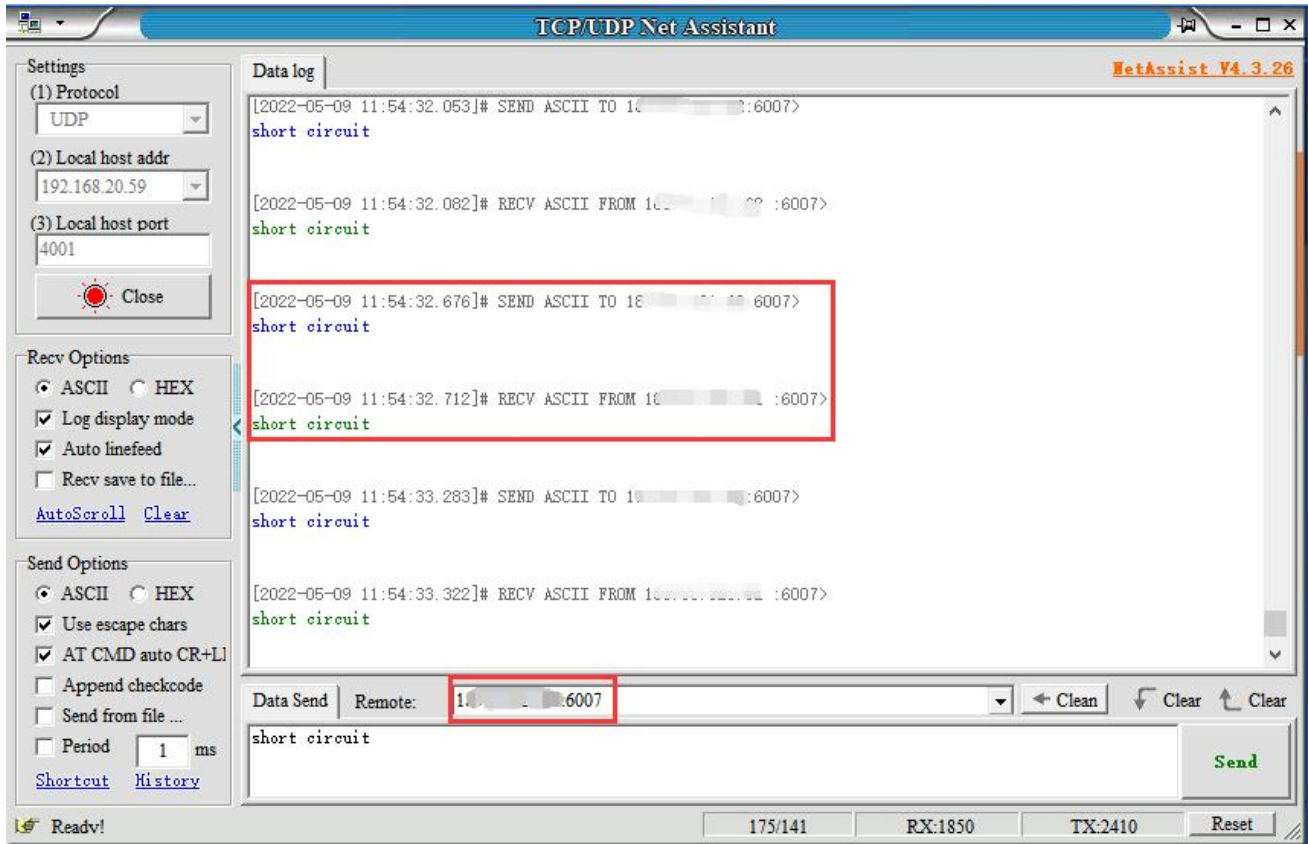
- A.Disabled: Checking here means to disable this rule.
- B.Proxy Name: Customize a proxy name. The proxy name cannot be repeated, otherwise the rule will not take effect due to conflict.
- C.Type: Select the UDP protocol.
- D.Local IP: Fill in the ip of the machine or the ip assigned by the lan port 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.



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



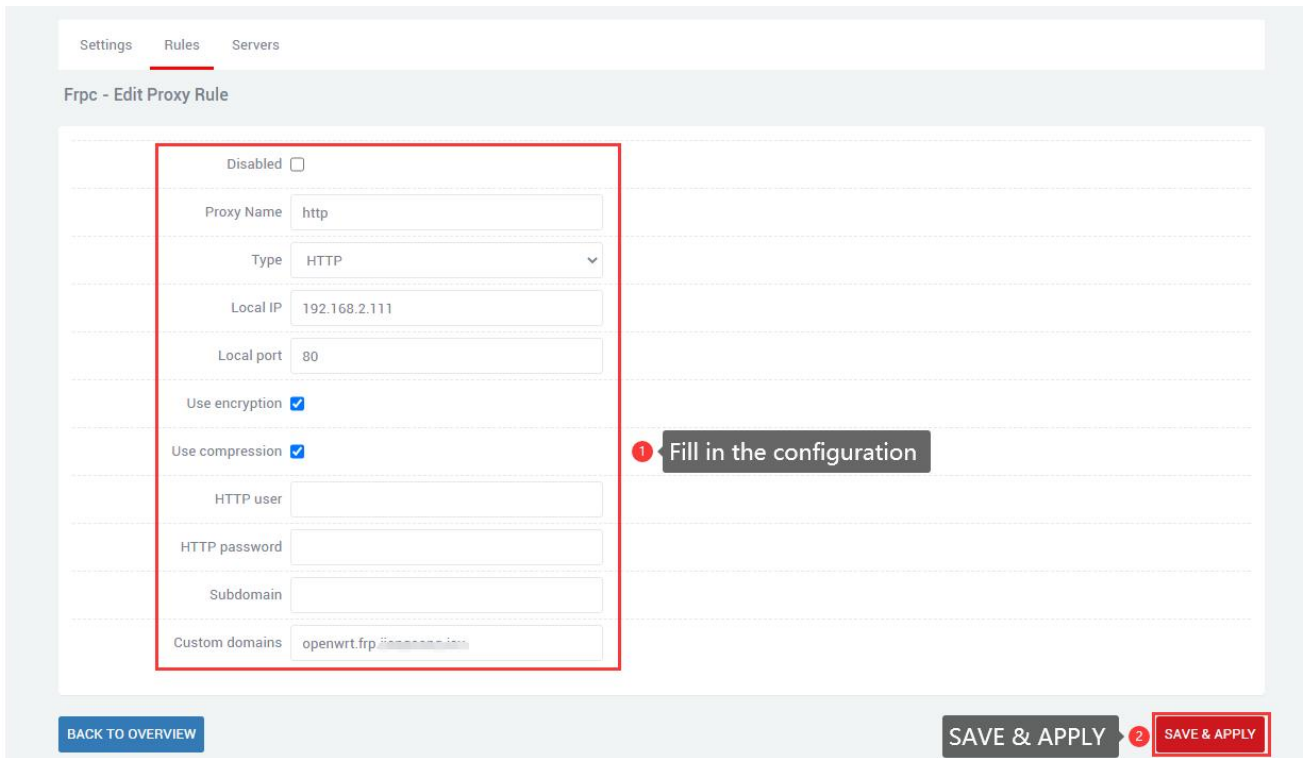
Through the UDP protocol, use the public network address and remote port number to access the device forwarded to the public network (111.111.111.111:6007 accesses 192.168.2.233:4001).



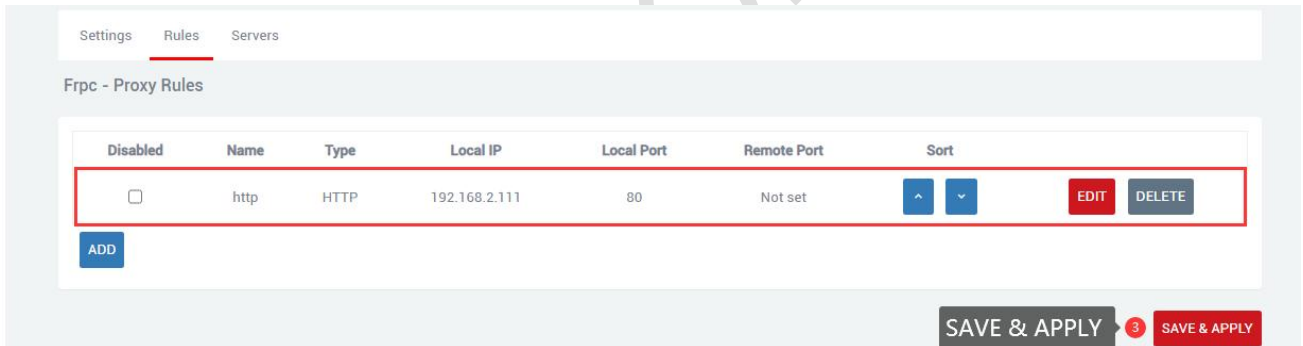
3.5.5 Add HTTP Proxy Rules

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.



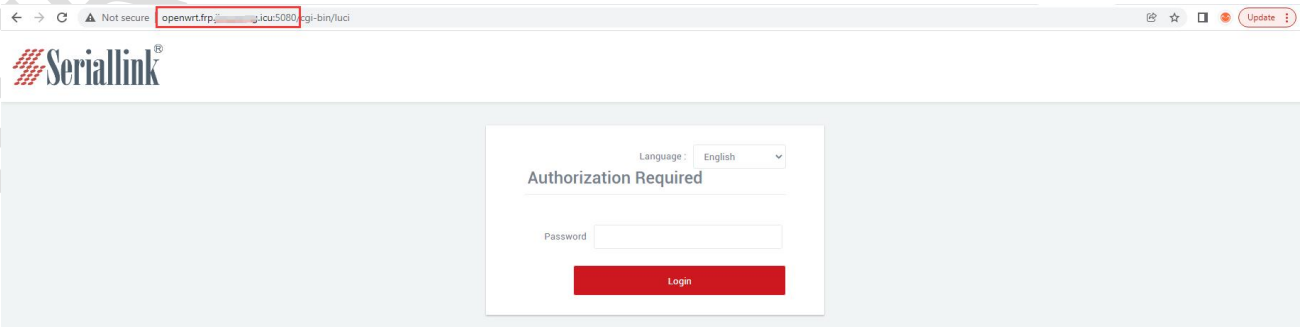
After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.



Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort
<input type="checkbox"/>	http	HTTP	192.168.2.111	80	Not set	^ v

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.



Chapter 4 VPN Service

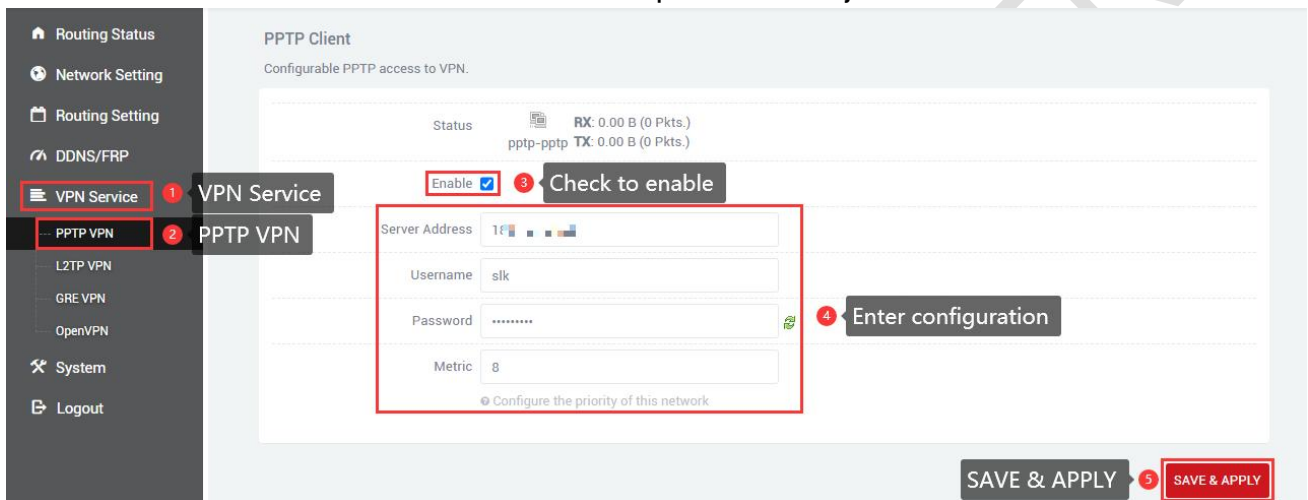
4.1 PPTP VPN

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".



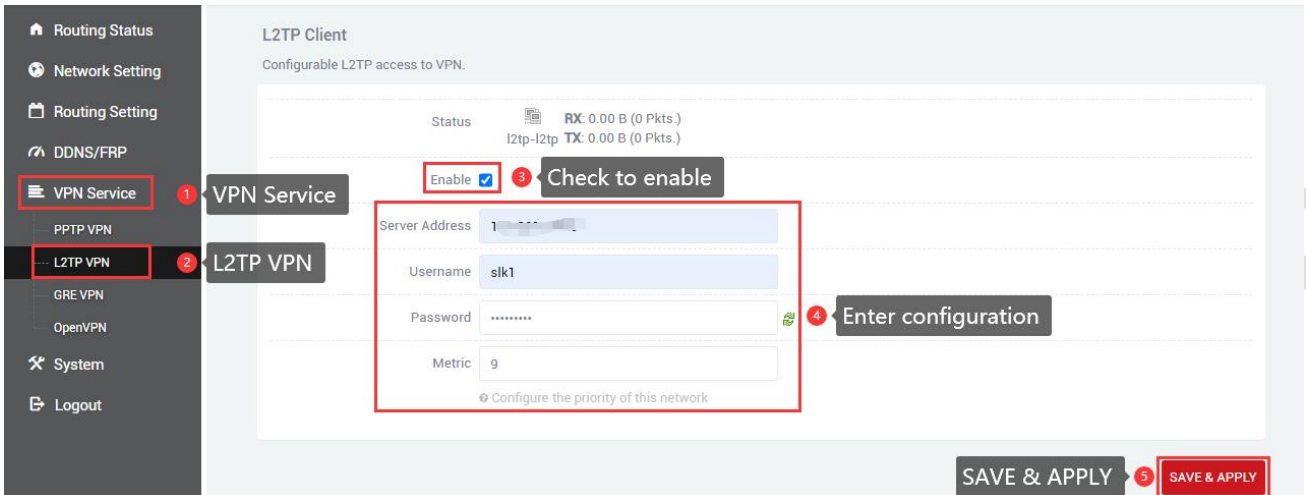
4.2 L2TP VPN

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

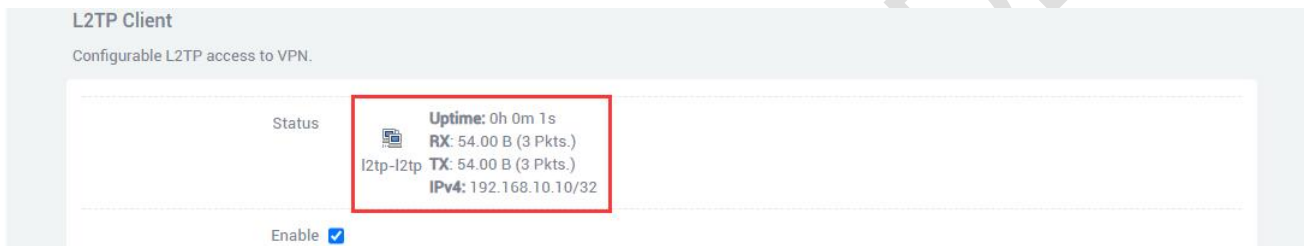
A.Enable: To use L2TP VPN, you need to check it, and you can just uncheck it when you don't use it.

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

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

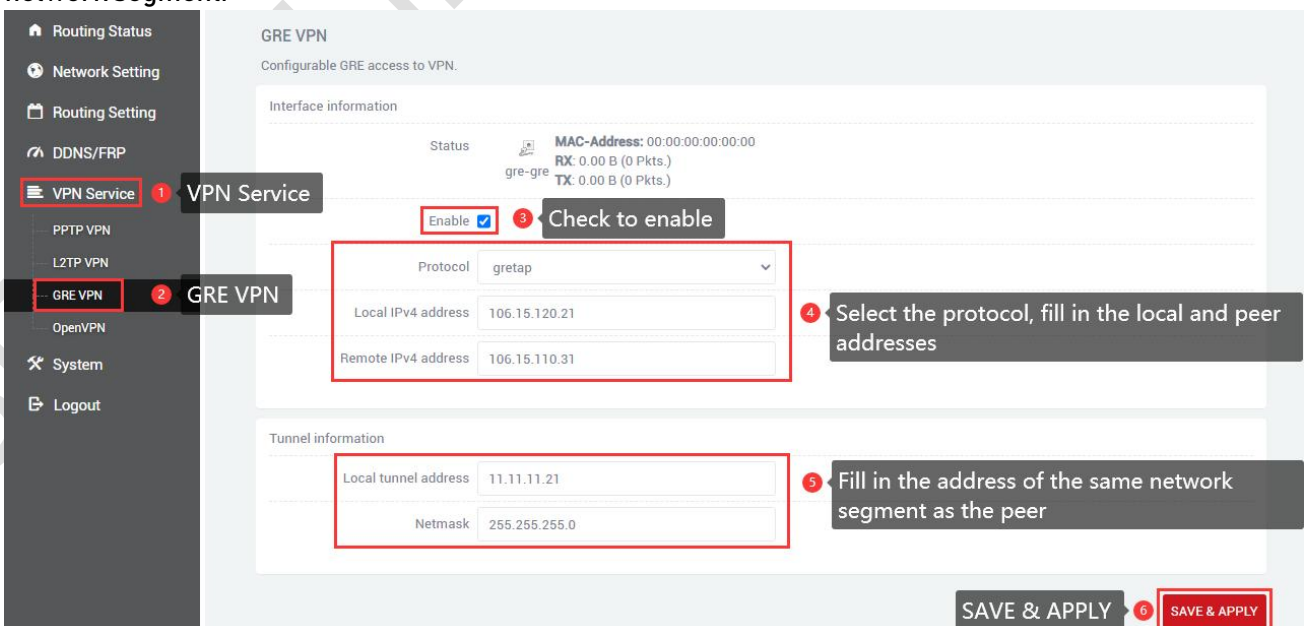


After the connection is successful, the address assigned by the server will appear in the status bar. If l2tp is not used, uncheck it and click "SAVE & APPLY".



4.3 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.



Refresh status information after "SAVE & APPLY".

GRE VPN
Configurable GRE access to VPN.

Interface information

Status **Uptime:** 0h 0m 4s
MAC-Address: BE:E3:F4:9B:7C:D5
gre-gre **RX:** 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)
IPv4: 11.11.11.21/24

Enable

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

Routing Status
Network Setting
Routing Setting 7
Static Routes 8
Port Forwards
DMZ
Black/White List
Firewall

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

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

This section contains no values yet

ADD 9 click ADD

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

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
gre_static	192.168.2.0	255.255.255.0	11.11.11.31	0	1500

10 Interface selection gre static
11 Target is the remote LAN port
12 Peer lan port subnet mask
13 peer tunnel IP

Static IPv6 Routes

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

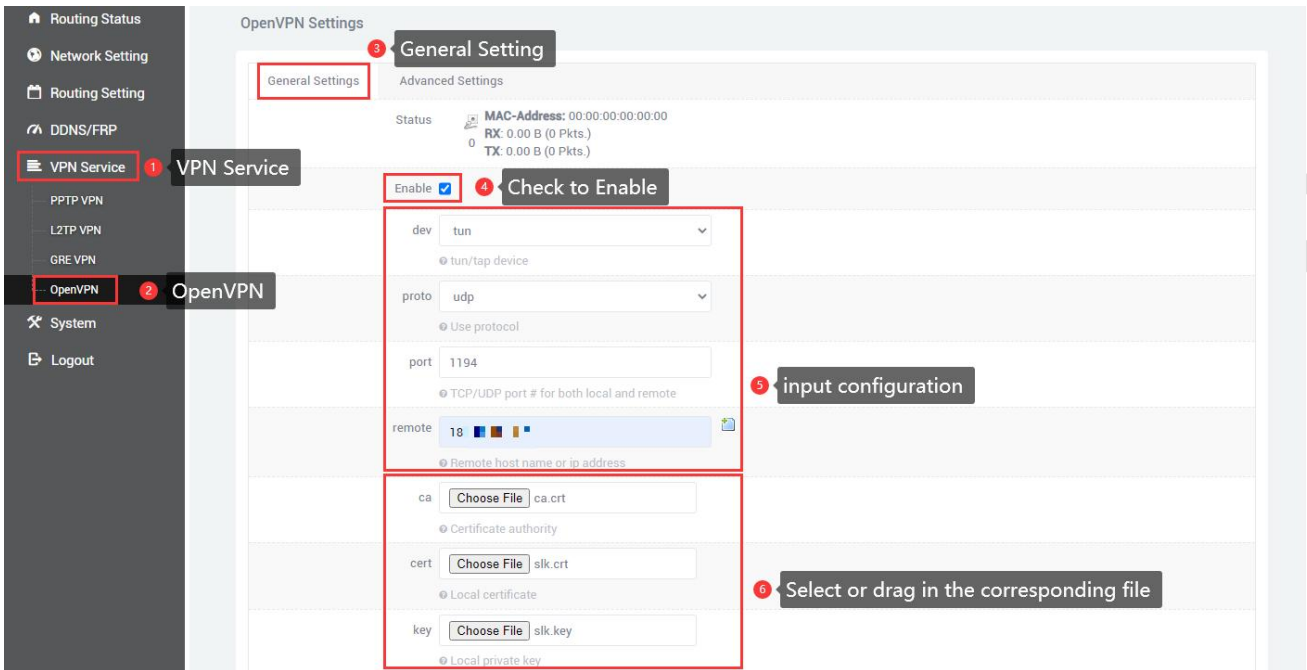
This section contains no values yet

ADD

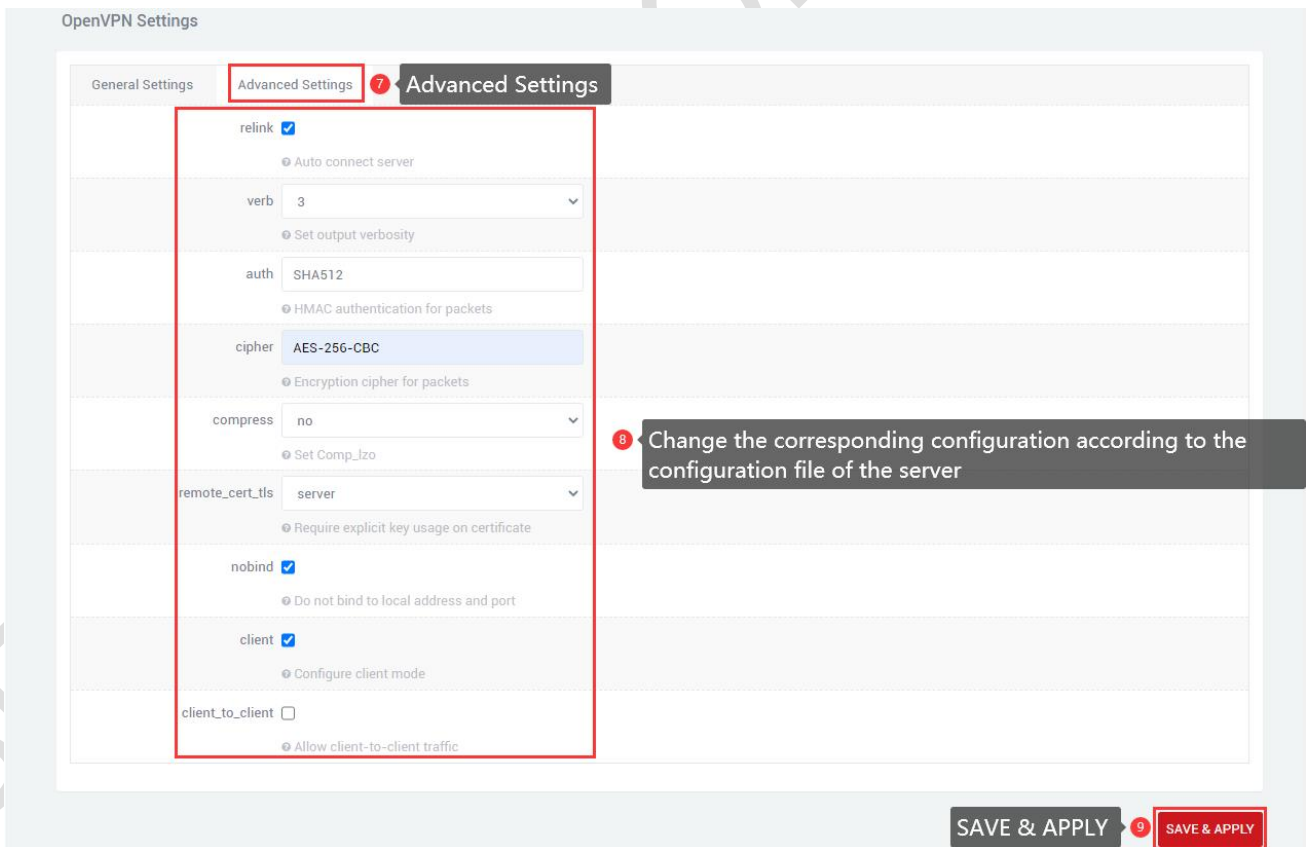
SAVE & APPLY 14 **SAVE & APPLY**

4.4 OpenVPN

Navigation bar "Virtual Private Network" - "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".



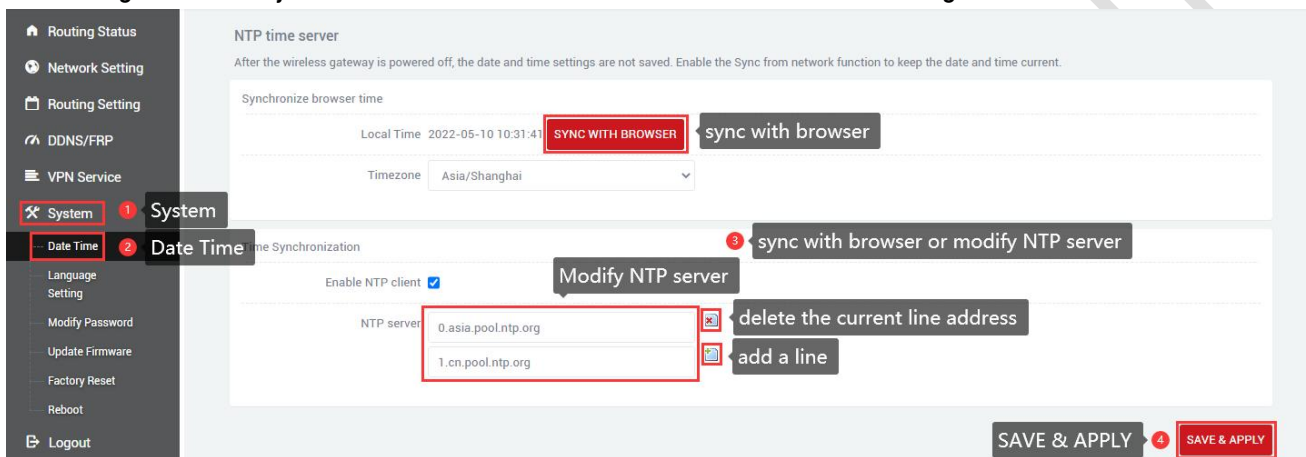
After the connection is successful, the status bar will refresh the address. If openvpn is not used, uncheck it and click "SAVE & APPLY".

Chapter 5 System

5.1 Date Time

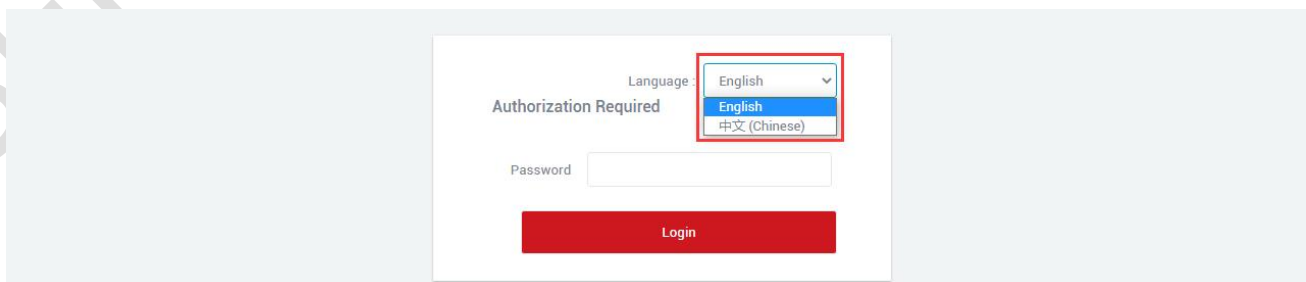
Time synchronization is enabled by default. If necessary, you can change the NTP server to synchronize the time of the server.

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



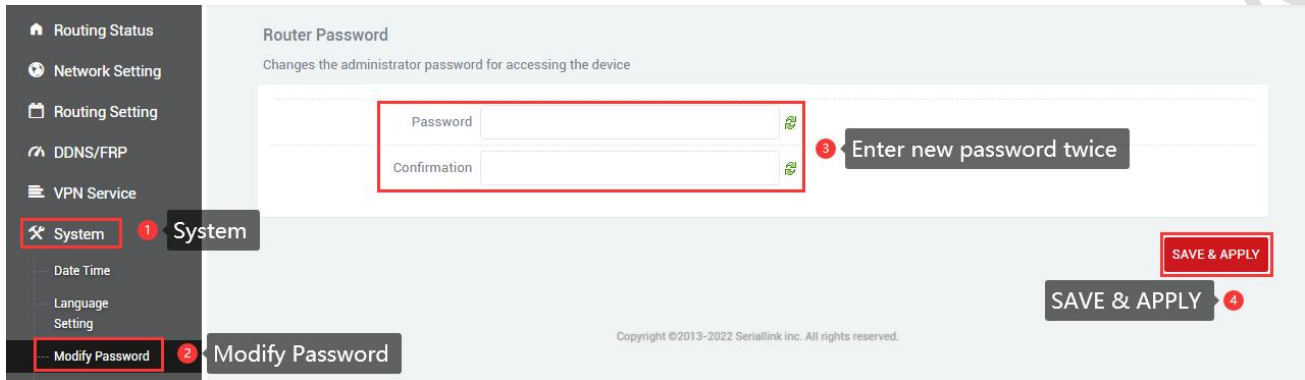
5.2 Language Setting

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.

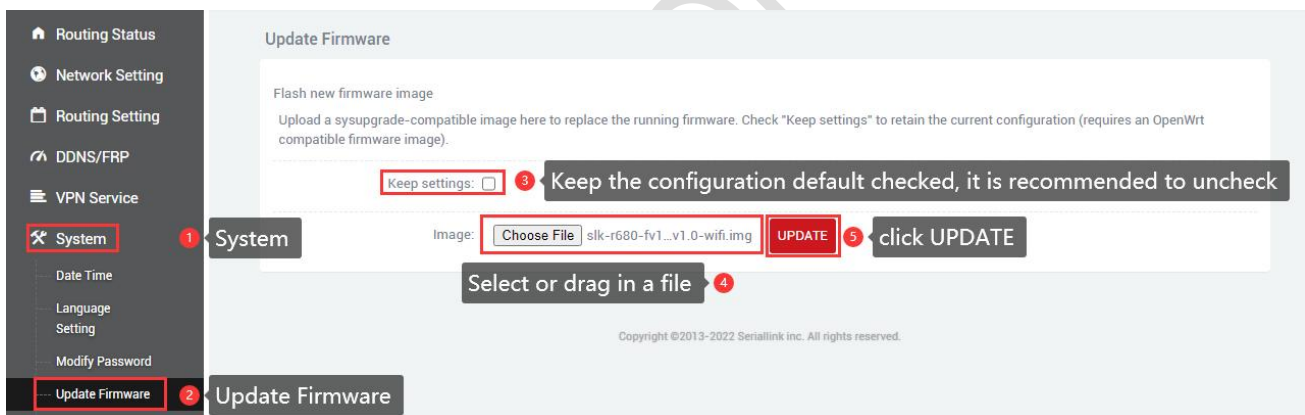


5.3 Modify Password

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.

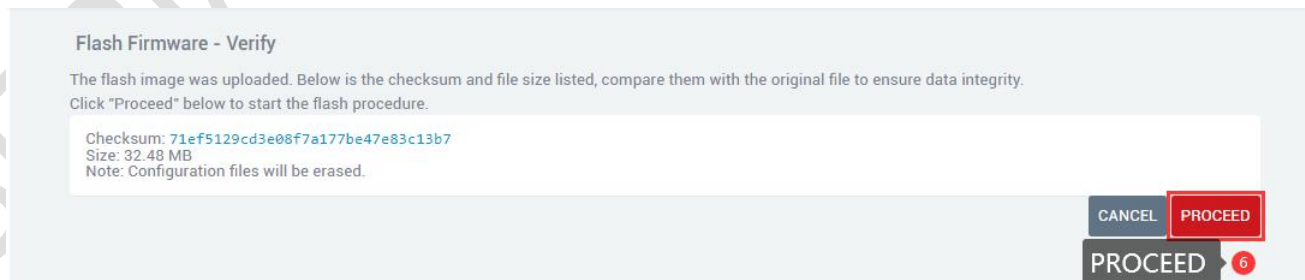


5.4 Update Firmware



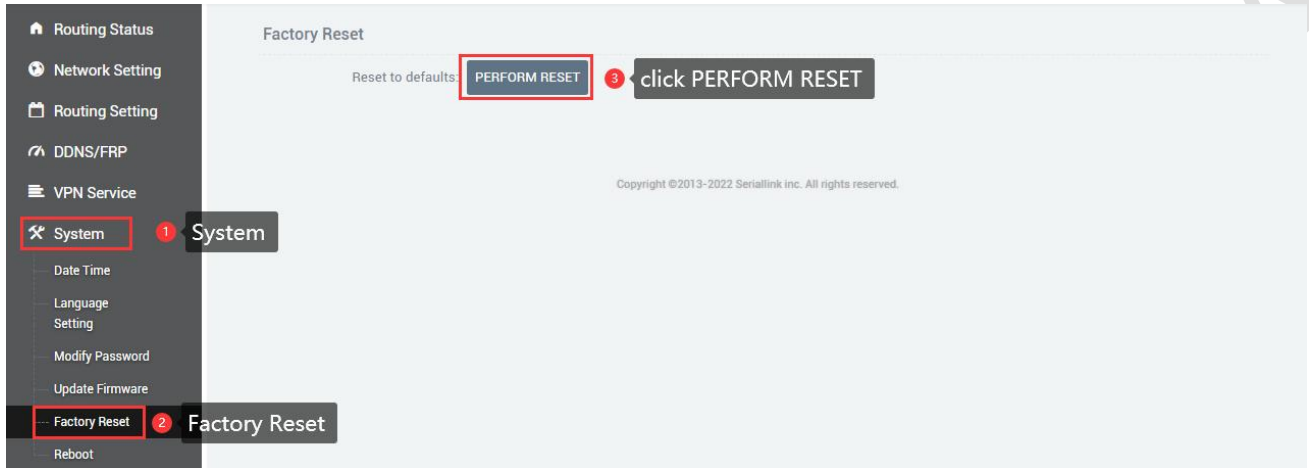
Navigation bar "System" - "Update Firmware", select the file and click "UPDATE", the MD5 check code page will appear after uploading, click "PROCEED" to upgrade, the upgrade will take a certain time, it takes about 1~2 minutes. After the upgrade is complete, log in again through "192.168.2.1".

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



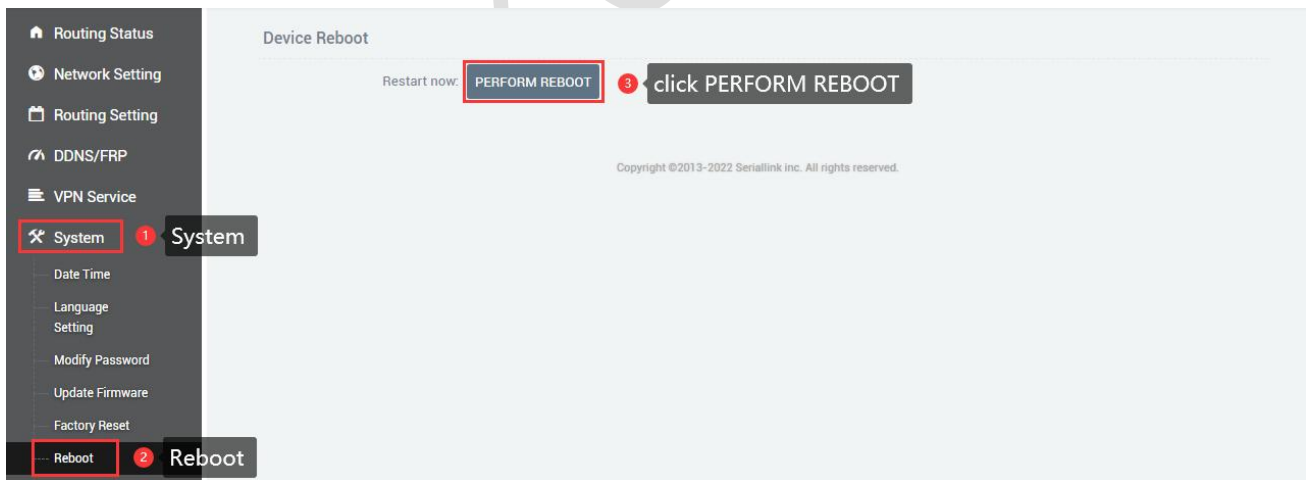
5.5 Factory Reset

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.

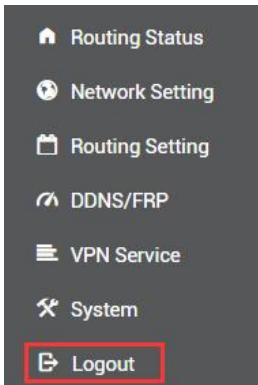


5.6 Reboot

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



5.7 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 or www.seriallink.net