SLK-R660 Series

Industrial Grade 4G Multifunctional Gateway
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 10
2.3.4 As lan (convert WAN port to LAN port) 11
2.4 DHCP server 11
2.4.1 enable DHCP 11
2.4.2 Disable DHCP 12
2.5 Hostnames 13
2.6 Network Backup 13
2.7 Time Reboot 14
2.8 Watchcat 15
2.9 Diagnosis 16
Chapter 3 Serial port configuration 18
3.1 Use Tools And Preparation 18
3.2 TCP Server 19
3.3 TCP Client 21
3.4 UDP Server 23
3.5 UDP Client 25
3.6 Modbus TCP 27
3.7 Transport Proto 31
3.8 Switch quantity control 33
3.8.1 Switch quantity DI 34
3.8.2 Switch quantity DO 35
Chapter 4 Firewall and Application 37
4.1 Firewall on and off 37
4.2 DMZ 37
4.3 Prot Forwards 38
4.4 Black/White List 40
4.4.1 White List 40
4.4.2 Black List 42
4.5 Frp Client 44
4.5.1 Connect to Frps 44
4.5.2 Add TCP proxy protocol 48
4.5.3 Add STCP Proxy Rules 50

4.5.4 Add UDP Proxy Rules....56
4.5.5 Add HTTP Proxy Rules....58
4.6 1:1 NAT....60
Chapter 5 VPN Service....62
5.1 L2TP VPN....62
5.2 GRE VPN....63
5.3 OpenVPN....65
Chapter 6 System....67
6.1 Date Time....67
6.2 Language Setting....67
6.3 Modify Password....68
6.4 Update Firmware....68
6.5 Factory Reset....69
6.6 Reboot....69
6.7 page log out....70

Chapter 1 login

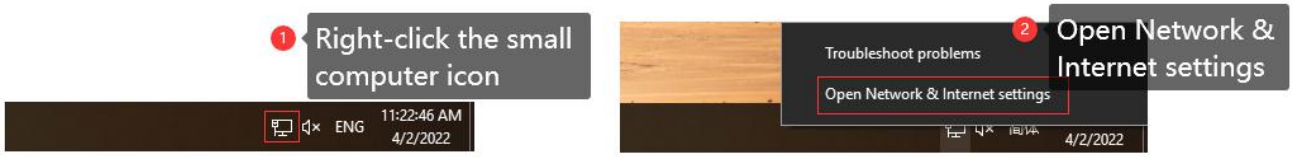
1.1 Prepare before logging in

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.

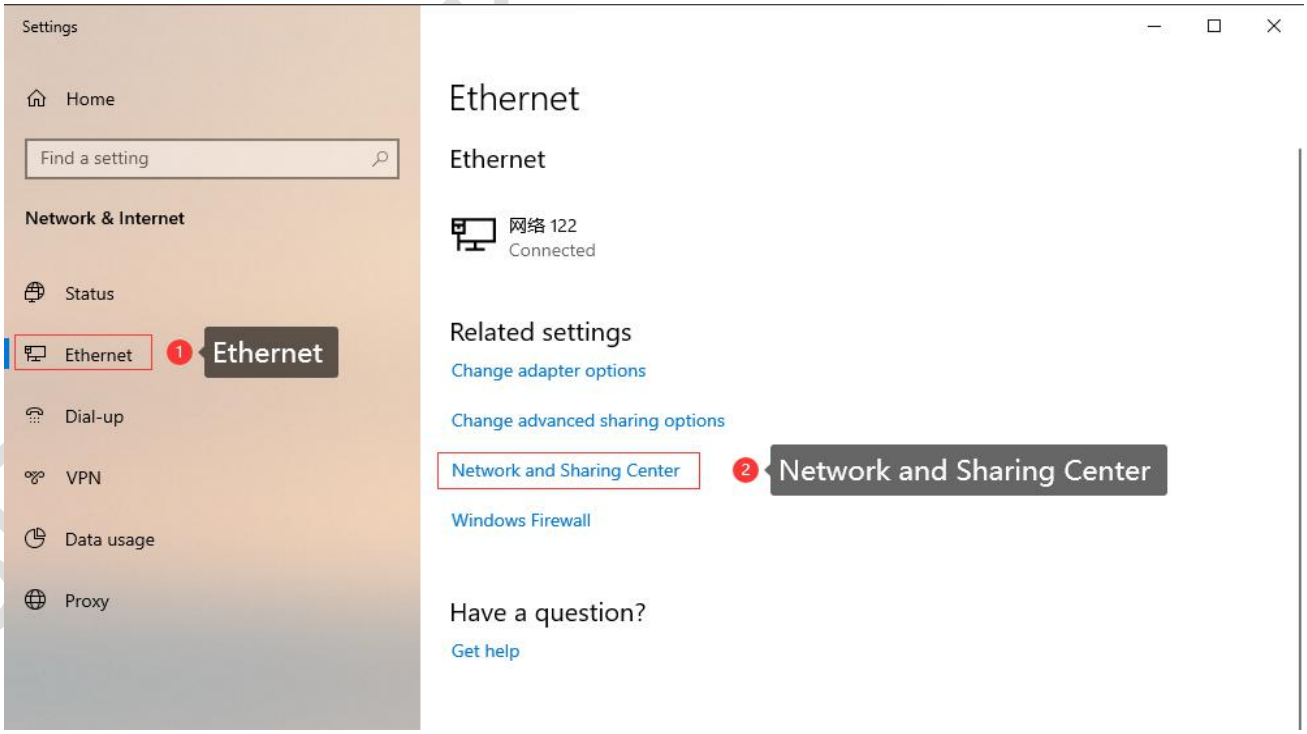
Set the IP address of the management PC (for example: 192.168.2.59) and the IP address of the device's LAN port in the same network segment(The initial IP address of the LAN port of the device is: 192.168.2.1, and the subnet mask is 255.255.255.0) The method is as follows.

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

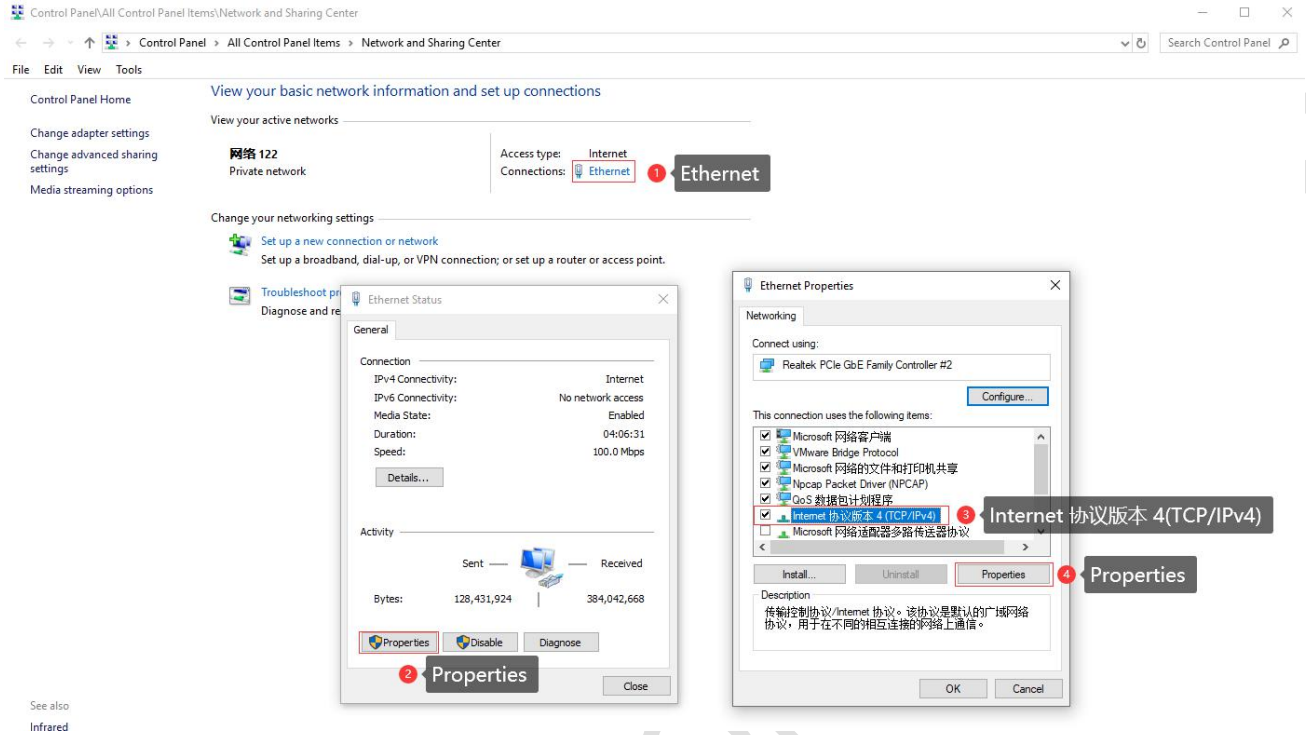
Step 1: Right-click the network logo in the lower right corner of the desktop (as shown in the figure), and choose to Open Network & Internet settings.



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

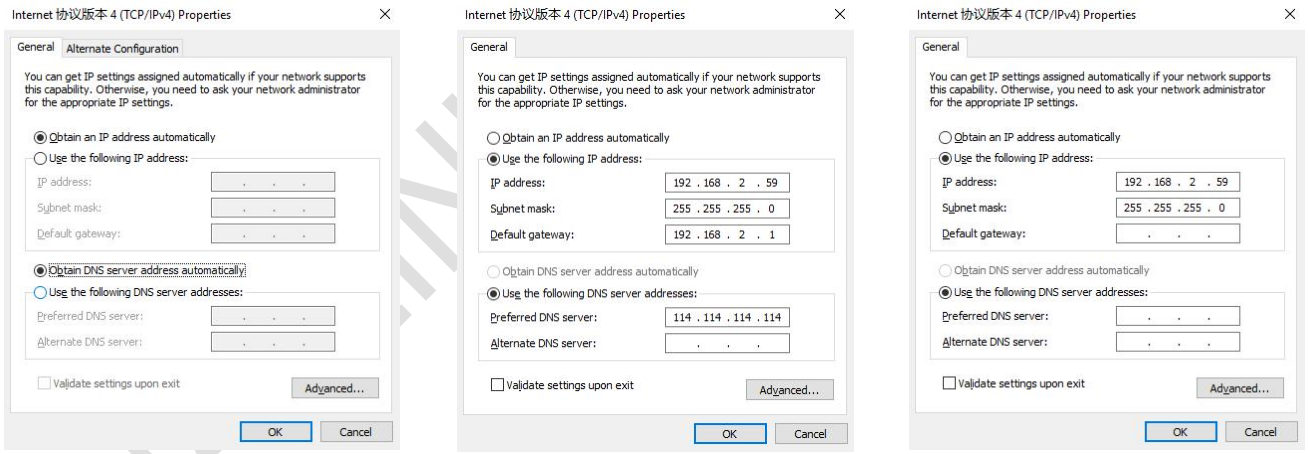


Step 3: Click Enternet with the mouse, click Properties in the pop-up box (Ethernet status), select Internet Protocol version 4 (TCP/IPv4) in the pop-up box (Ethernet properties), and click Properties



Step 4: There are three setting methods

method 1 method 2 method 3

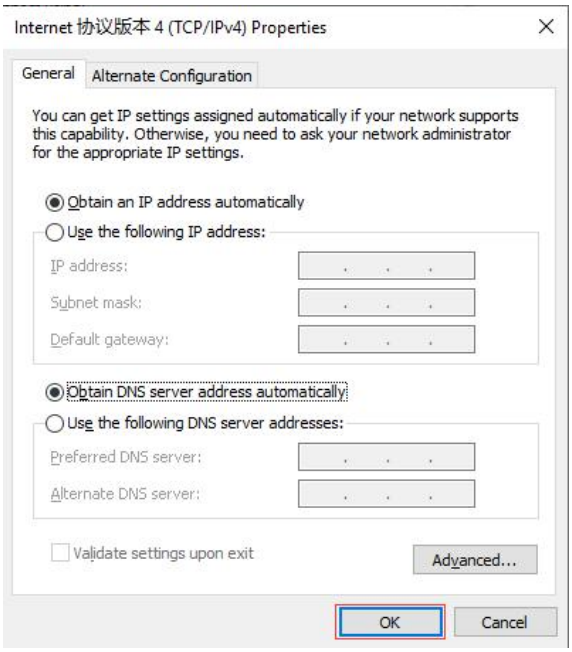


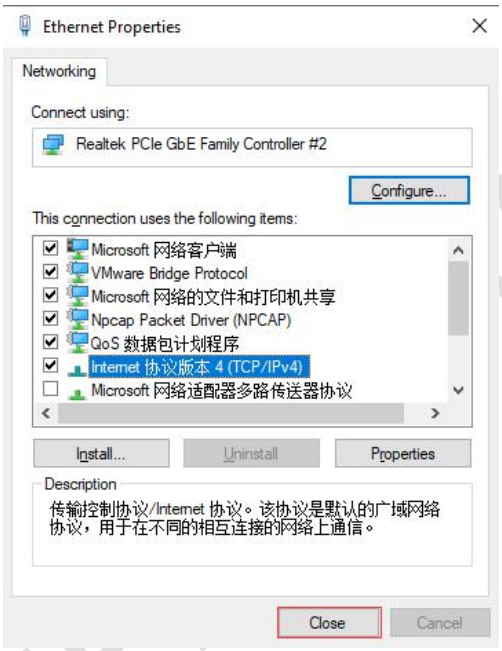
method 1: It can be used to configure the device and access the external network. It is recommended to use it (Note: If there are multiple routes with different network segments in the current environment, the IP obtained by the computer may not be able to connect to the device. In this case, method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

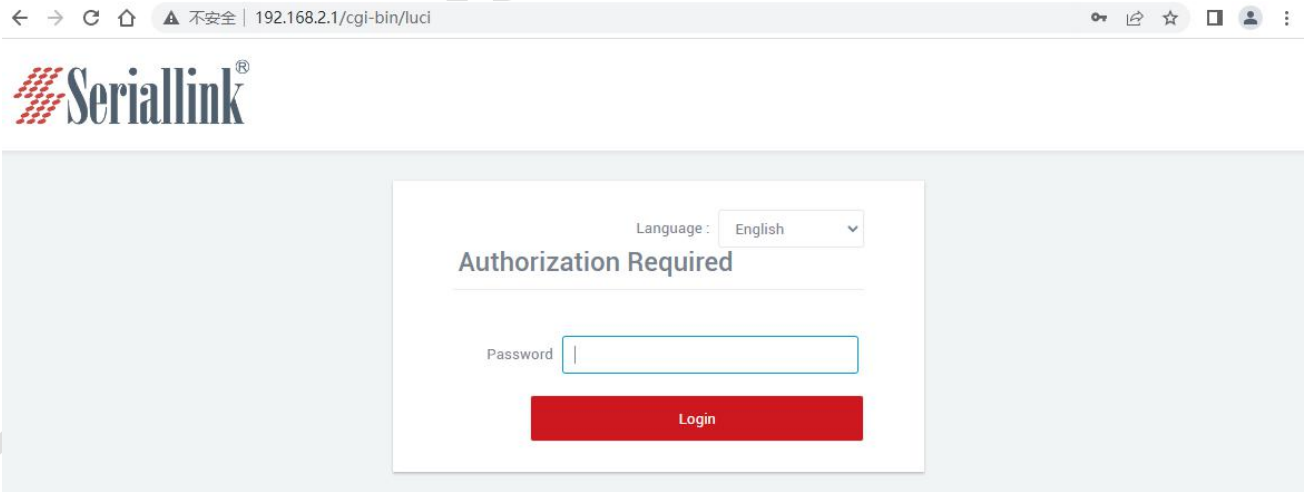
Step 5: Click OK with the mouse, and then click Close to save the changes in Steps 3 and 4;





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.

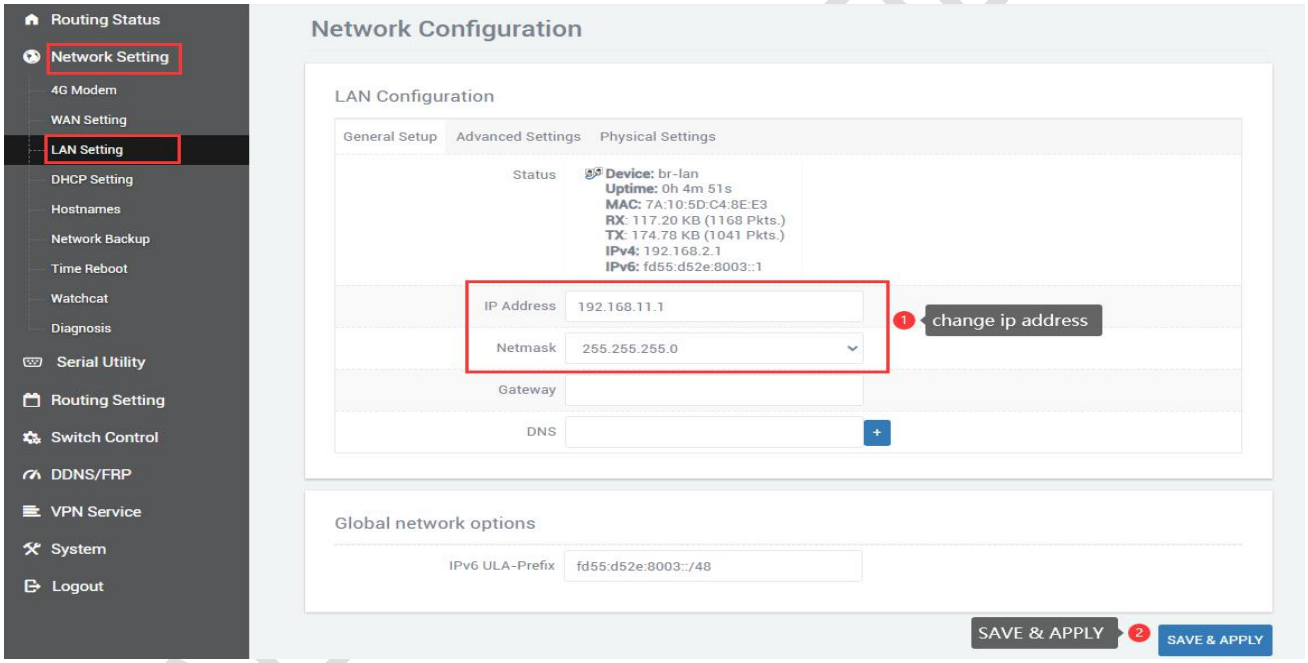
A.IP Address: Modify the ip address of the device (default is 192.168.2.1).

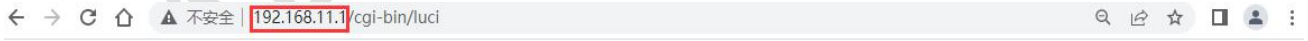
B.Netmask: It is generally 255.255.255.0, which can be modified as needed.

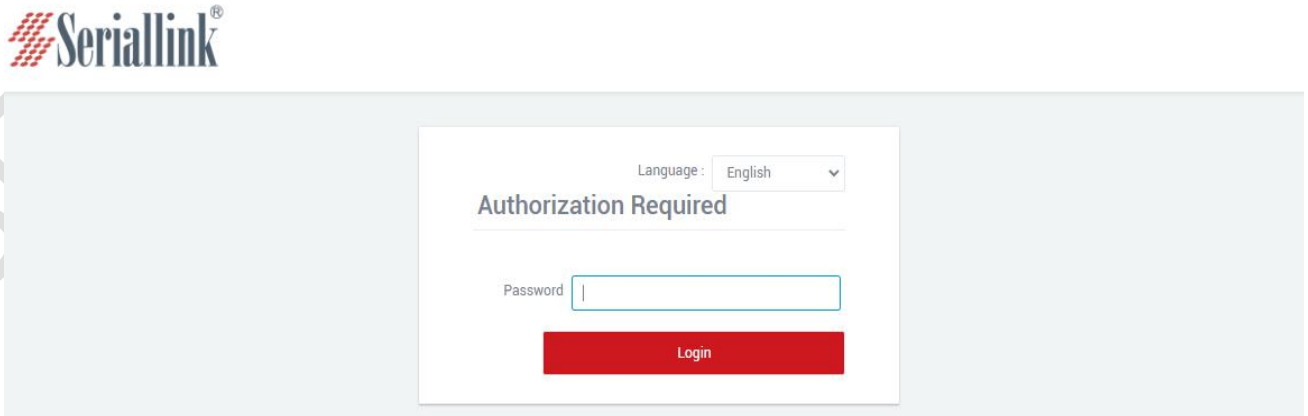
C.IPv4 gateway、DNS server、Override MTU: No special cases do not need to be set.

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.

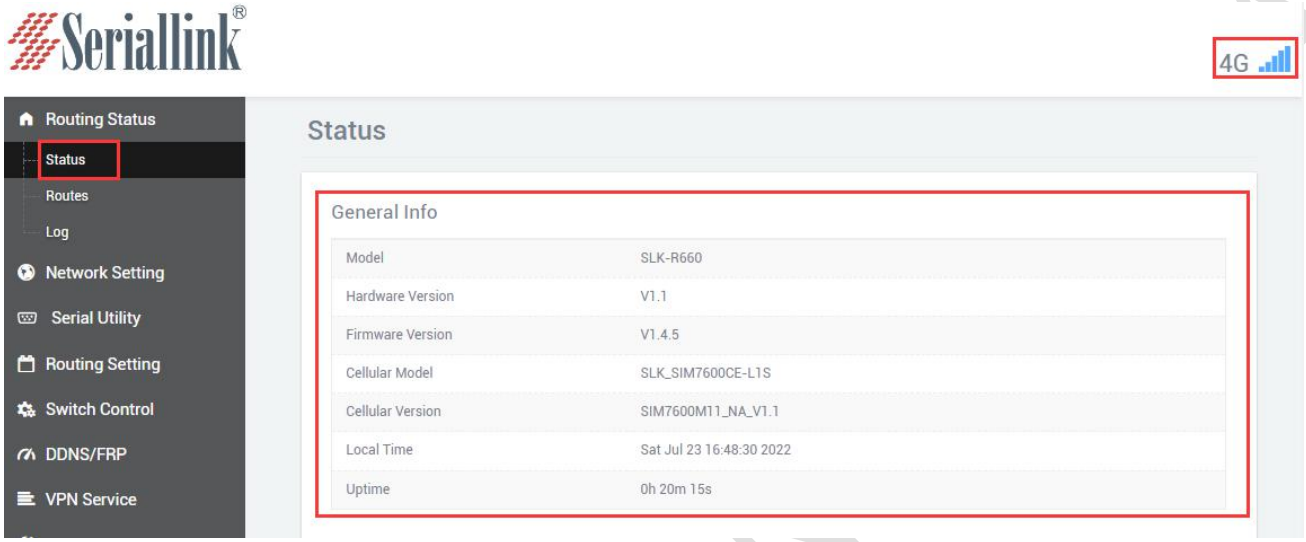




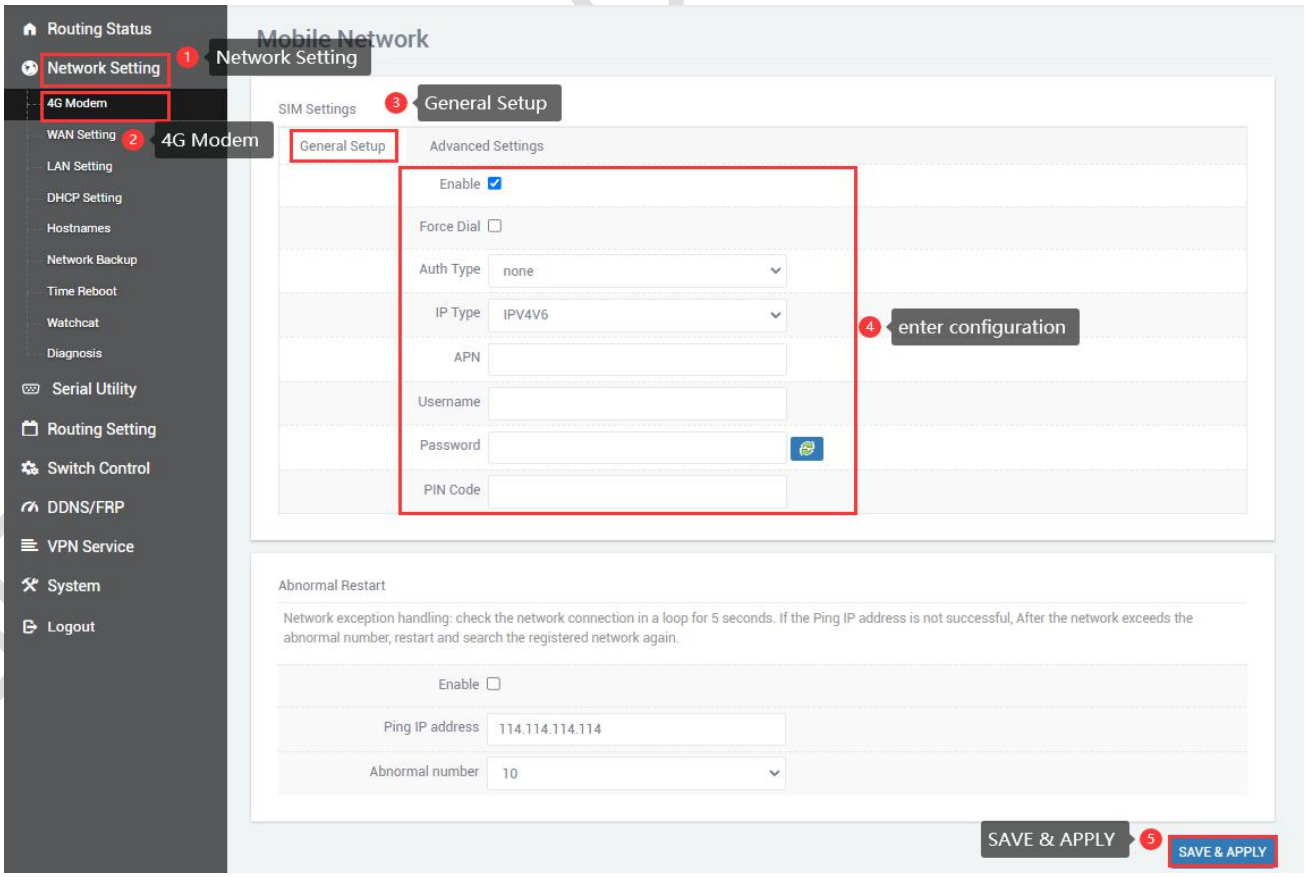


2.2 4G Modem

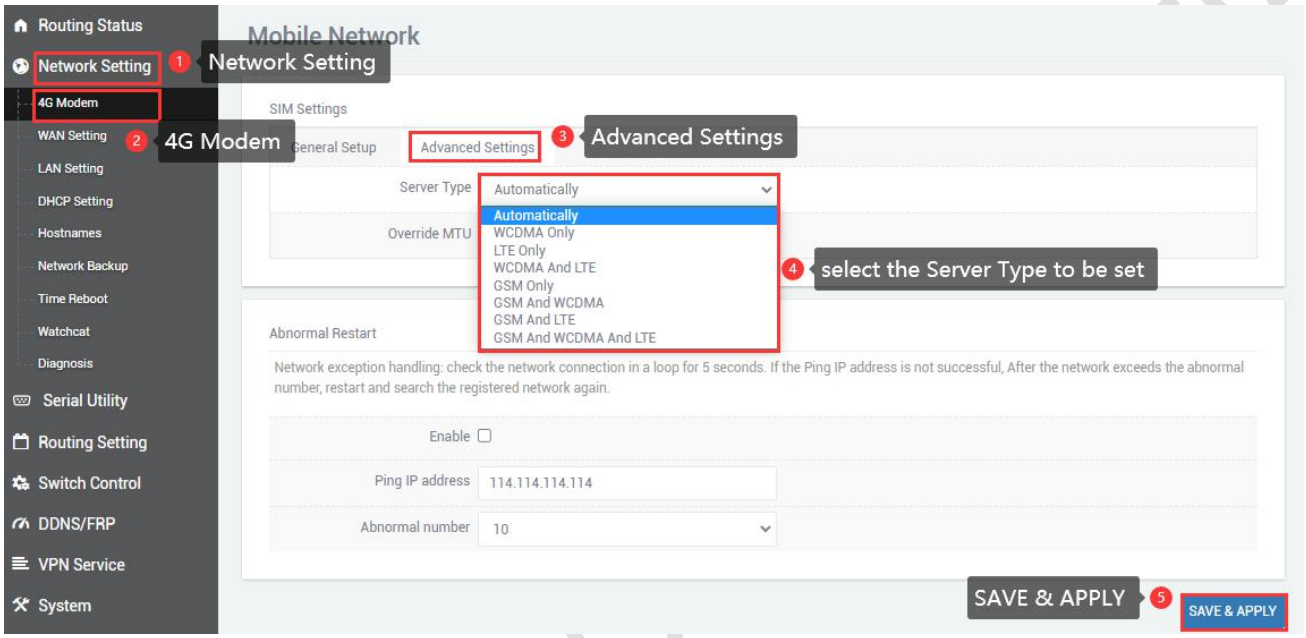
By default, the router uses the SIM card 2/3/4G to access the Internet. You can see the information of the SIM card in the "Routing Status" - "Status" in the navigation bar. You can check the network is 2/3/4G and the signal of the mobile phone card in the upper right corner.



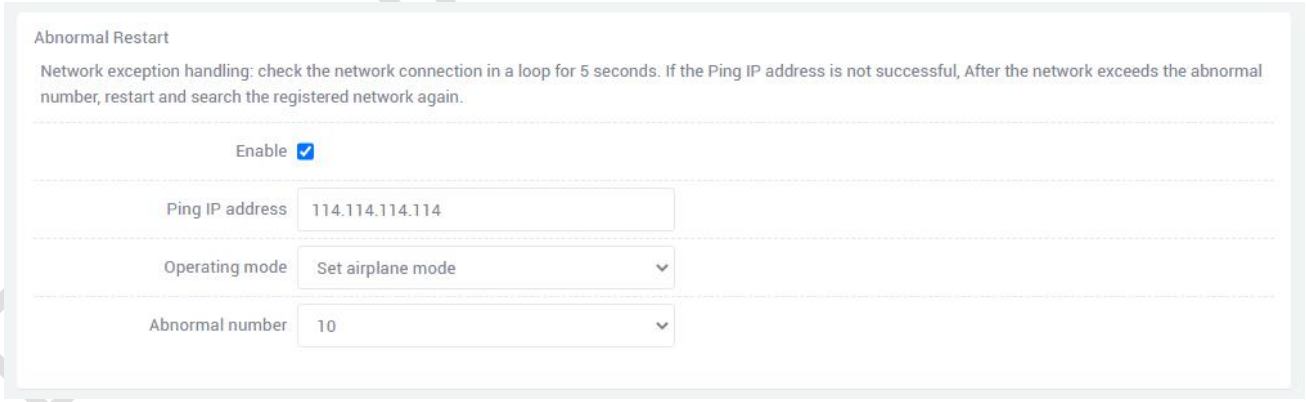
If you use an ordinary mobile phone data card, you don't need to care about the location of the APN setting, it can be empty by default. If you use an APN card, you need to set the APN in "Network Setting" - "4G Modem" - "General Settings".



"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".



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.



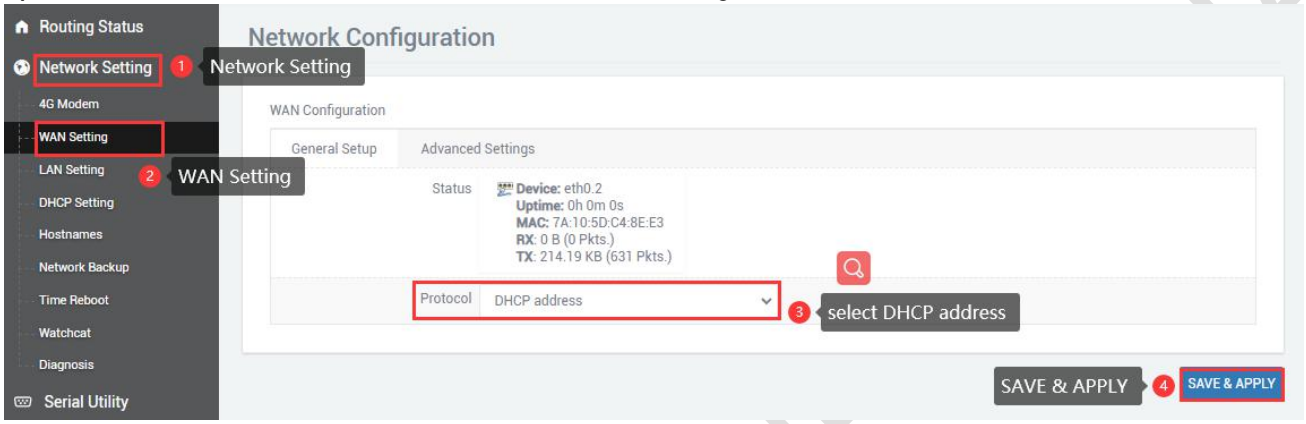
note:

- 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

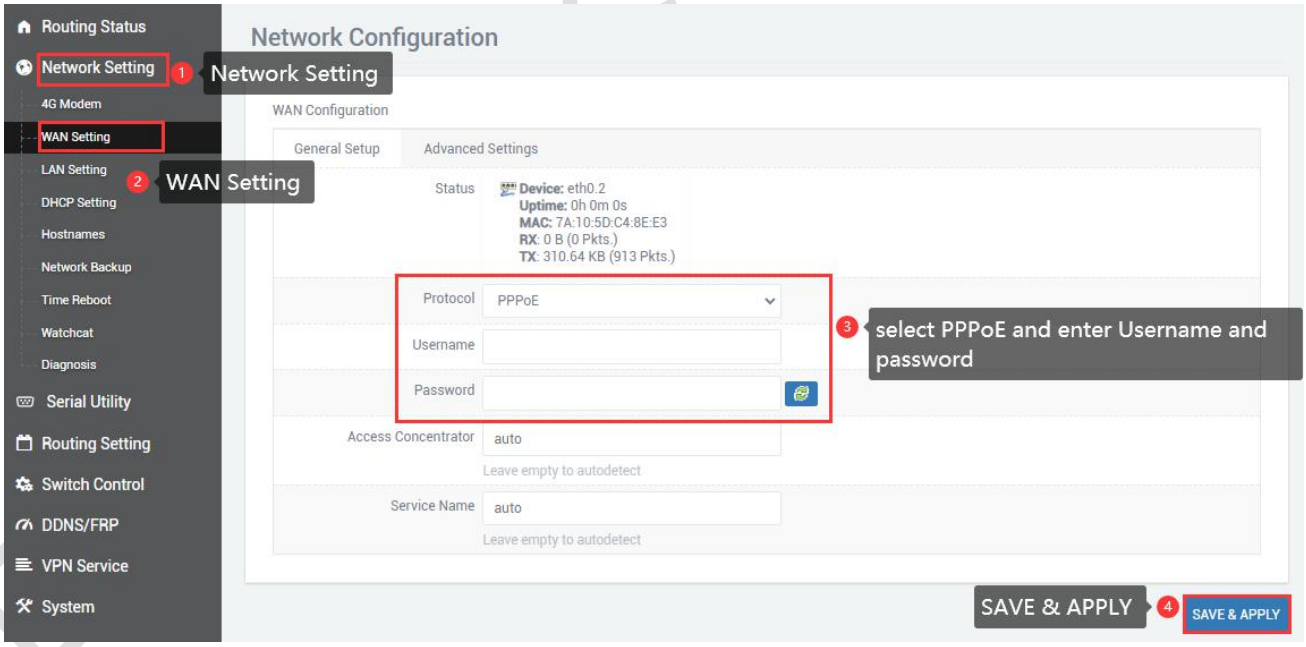
2.3.1 DHCP address

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).



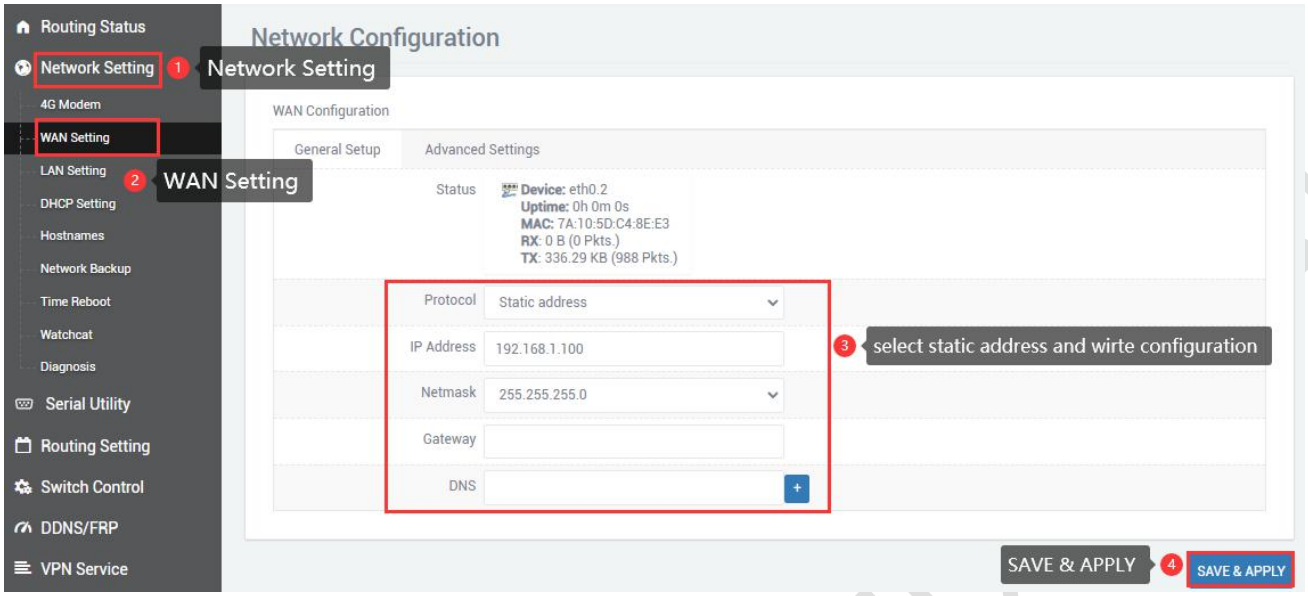
2.3.2 PPPoE

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).



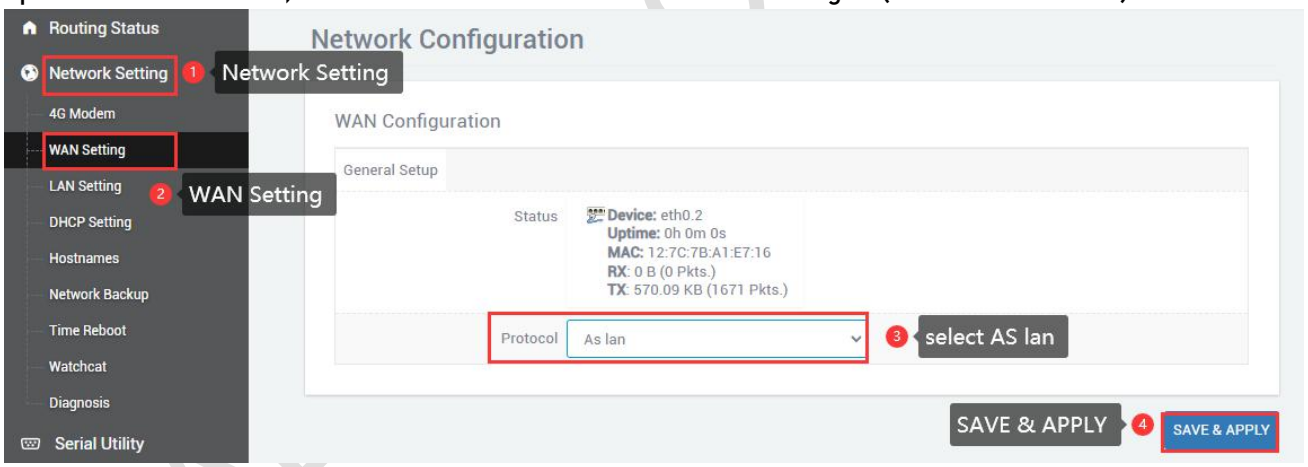
2.3.3 Static address

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).



2.4 DHCP server

2.4.1 enable DHCP

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.

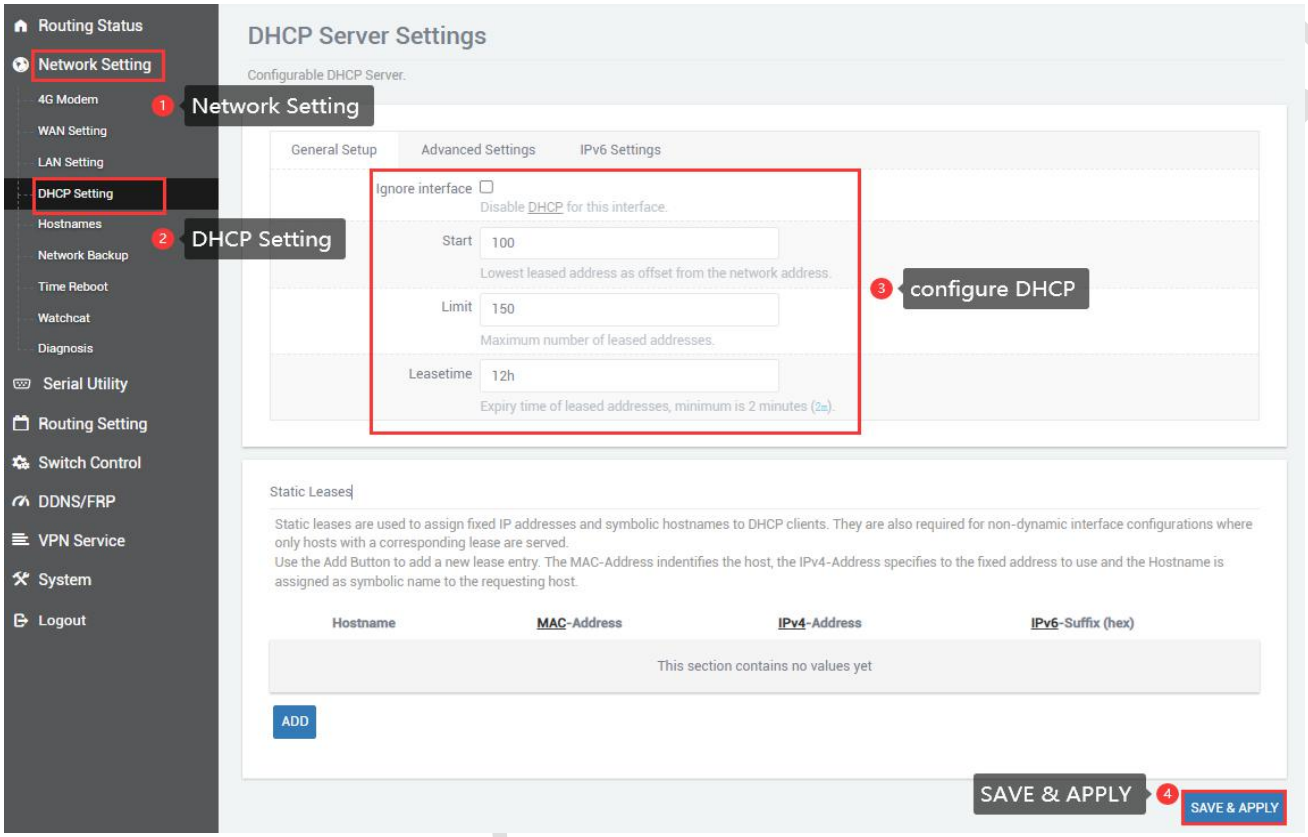
DHCP client configuration (enabled by default), select "Network Setting" - "DHCP Settings", "SAVE & APPLY".

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.

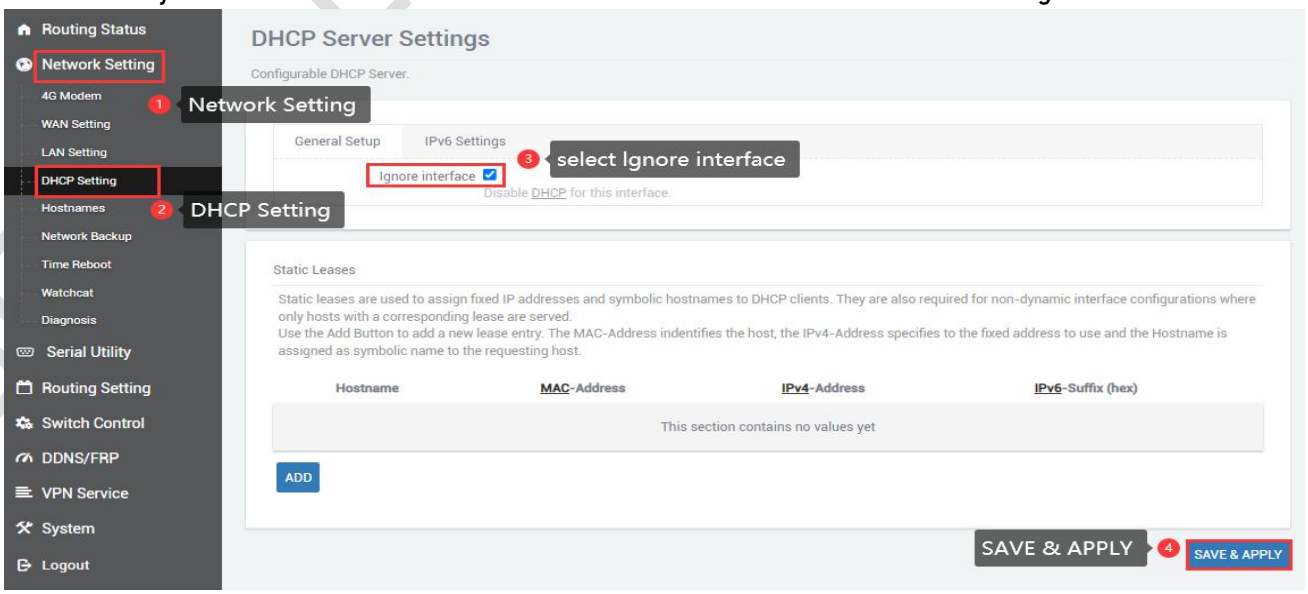
C. Limit: Maximum number of leased addresses.

D.Leasetime: Expiry time of leased addresses.



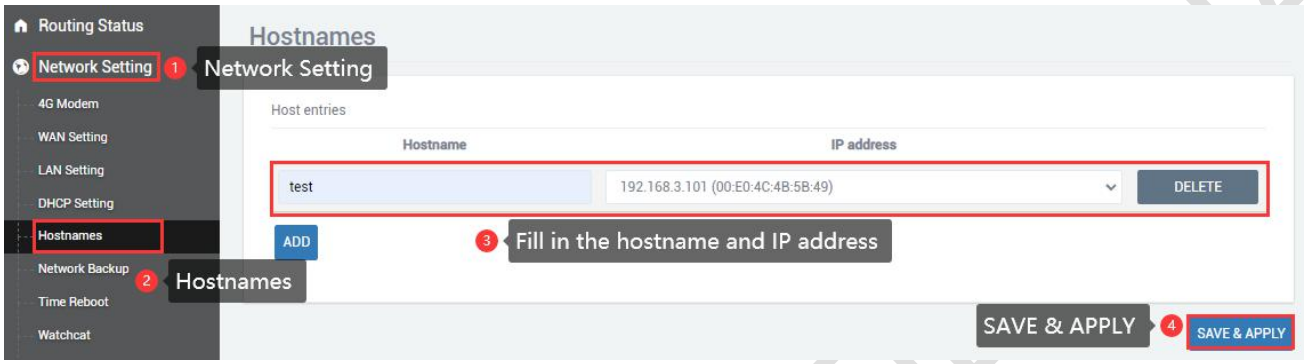
2.4.2 Disable DHCP

Disable the DHCP server function of the SLK-R660. In this way, the SLK-R660 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.



2.5 Hostnames

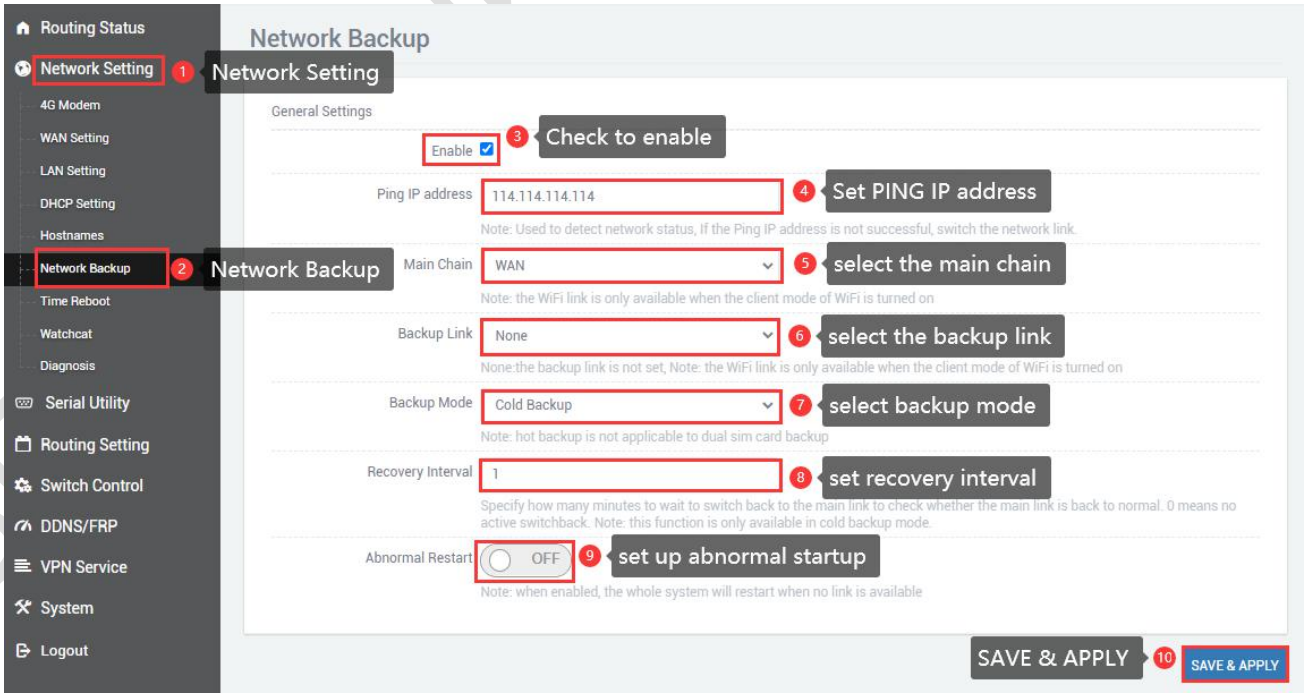
Navigation bar "Network Settings" - "Host Name", click Add, enter the host name and IP address, save and apply; in the network test, you can use the host name instead of the IP address (see 2.9 for the specific network test steps).



2.6 Network Backup

This part is a new function. It is mainly used to use wired (i.e. wan port) or wifi client first when accessing the Internet. The network of the main link is used first, and the network of the backup route is used when the main link has no network.

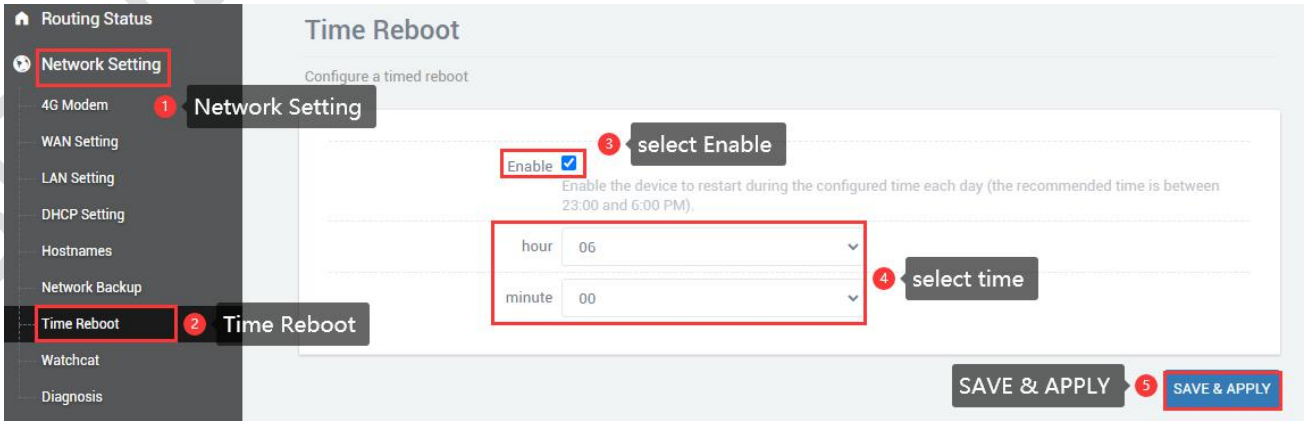
Network backup is disabled by default, check it to enable it when using it, and then configure it according to the actual situation.



General Settings@Link Management		
project	illustrate	default
PING address	Address for testing network connectivity performance	114.114.114.114
Main Chain	"WAN" or "WIFI" can be selected. WAN: use wan as the primary wired link WIFI: use the wifi client as the main wireless link Note: The wifi link is only available when the wifi client mode is turned on. For details, please refer to "2.5	WAN
Backup Link	"WAN", "WIFI" or "None" can be selected. WAN: Wired link using wan as backup WIFI: Use the wifi client as a backup wireless link None: means do not use this backup link Note: The wifi link is only available when the wifi client mode is turned on. For details, please refer to "2.5"	None
Backup Mode	"Cold Backup" or "Hot Backup" can be selected Hot backup: the backup link is always online Cold backup: supports automatic recovery of the main link	Cold Backup
Recovery Interval	When the backup link is used in cold backup mode, specify the number of minutes to wait to switch back to the primary link to detect whether the primary link is back to normal. 0 means no active switchback. NOTE: This feature is only displayed when cold backup mode is selected.	1
Abnormal Restart	Click the button to enable/disable the abnormal restart function When enabled, the device will reboot when no link is available.	OFF

2.7 Time Reboot

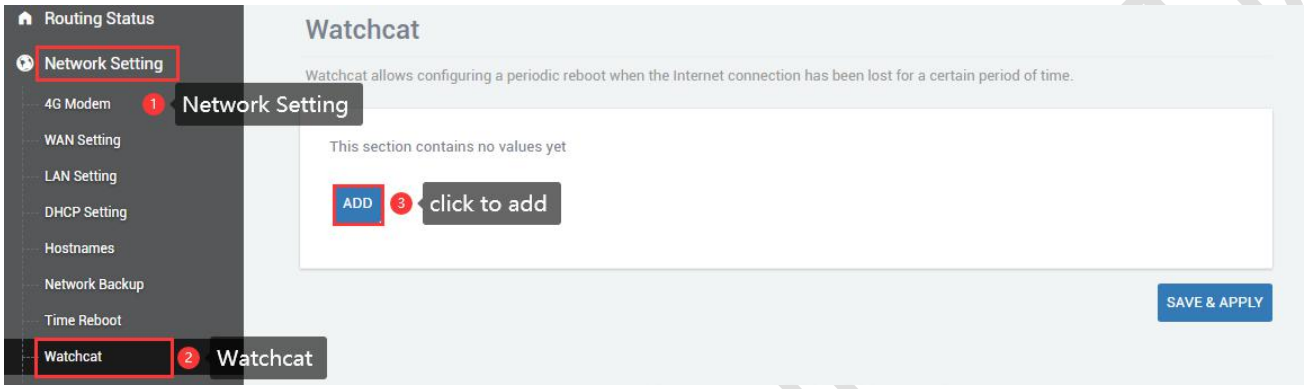
Navigation bar "Network Setting" - "Time Reboot", users can check to enable and set the time to restart every day, pay attention to check whether the device time is correct, modify the correct time: "System" - "Date Time", see chapter 5.1 for details .



2.8 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".

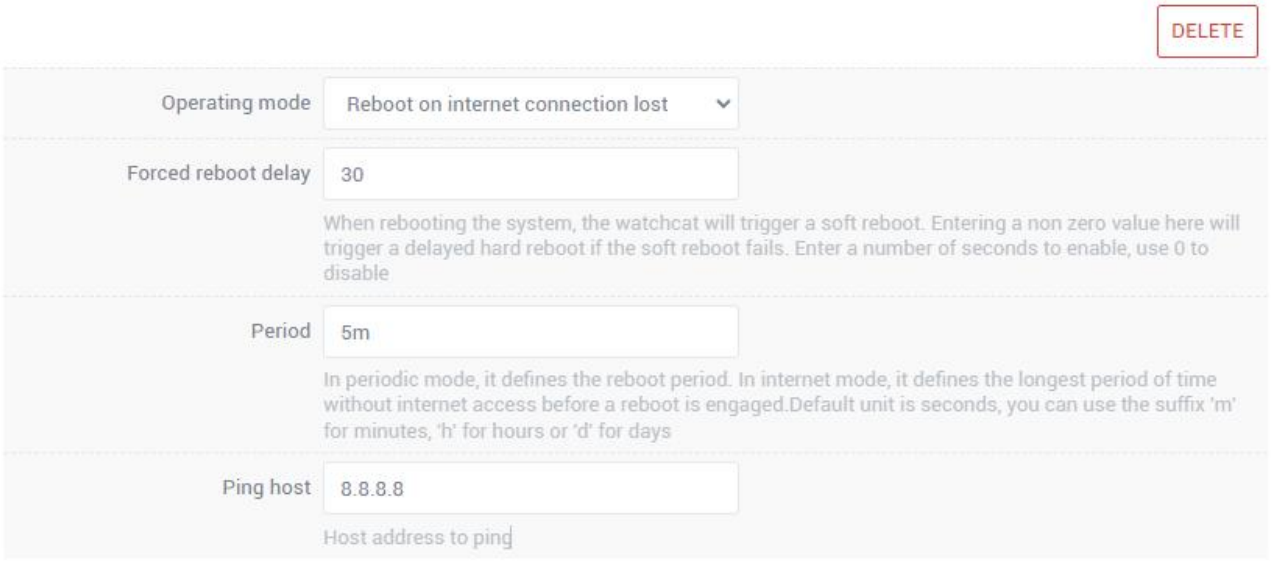


A.Forced reboot delay: When rebooting the system the watchcat will trigger a soft reboot, Entering a non zero value here, will trigger a delayed hard reboot if the soft reboot fails. Enter a number of seconds to enable, use 0 to disable

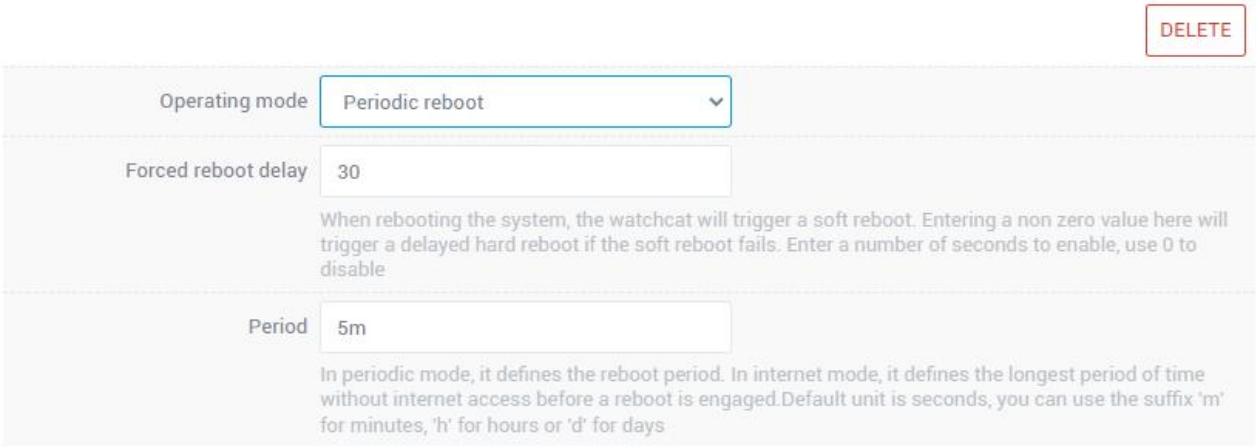
B.Period: In periodic mode, it defines the reboot period. In internet mode, it defines the longest period of time without internet access before a reboot is engaged.Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

C.Ping host: Host address to ping

1.Reboot on internet connection lost



2.Periodic reboot



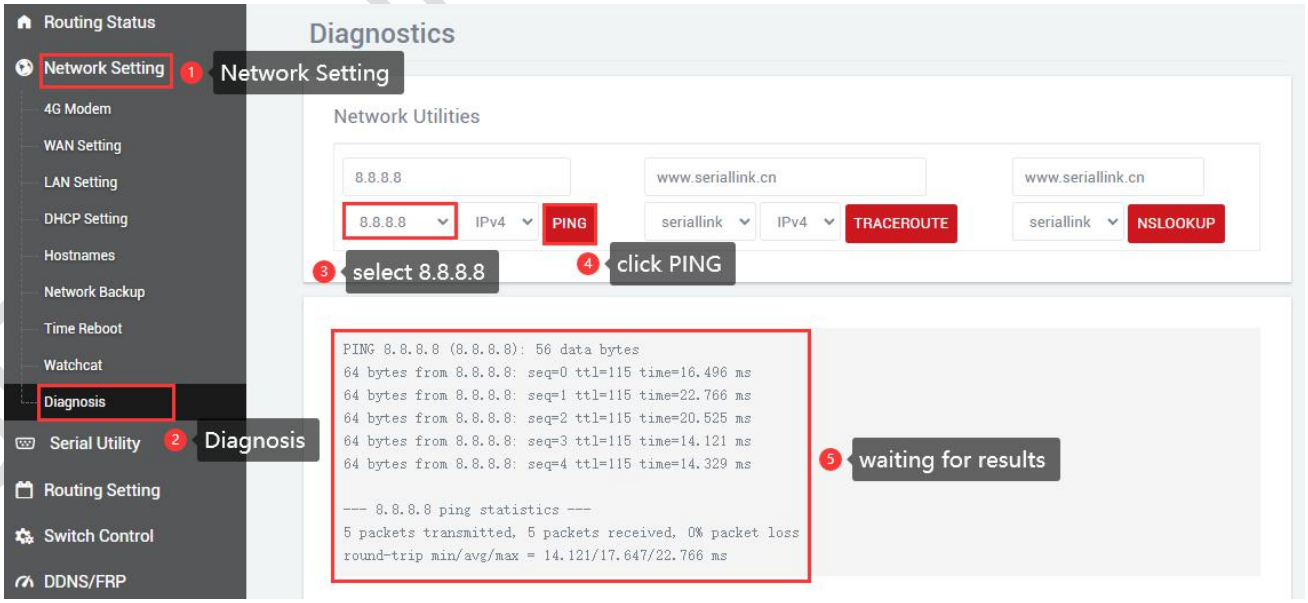
After adding and configuring, click "SAVE & APPLY" to take effect. To delete the configuration, just click the "DELETE" button in the upper right corner, and then "SAVE & APPLY".

2.9 Diagnosis

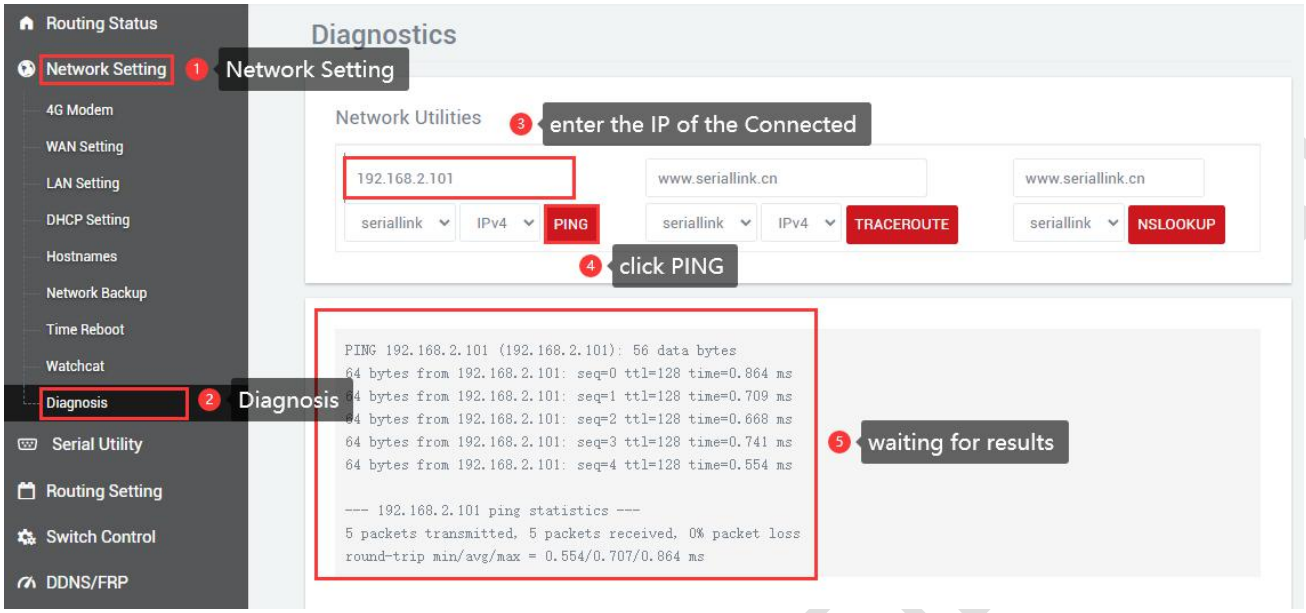
Through network diagnosis, you can determine whether the router and the connected device can communicate with each other, whether the device can access the Internet, and whether the device is successfully connected to the VPN. It can also be used to test other aspects, and you can test it according to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



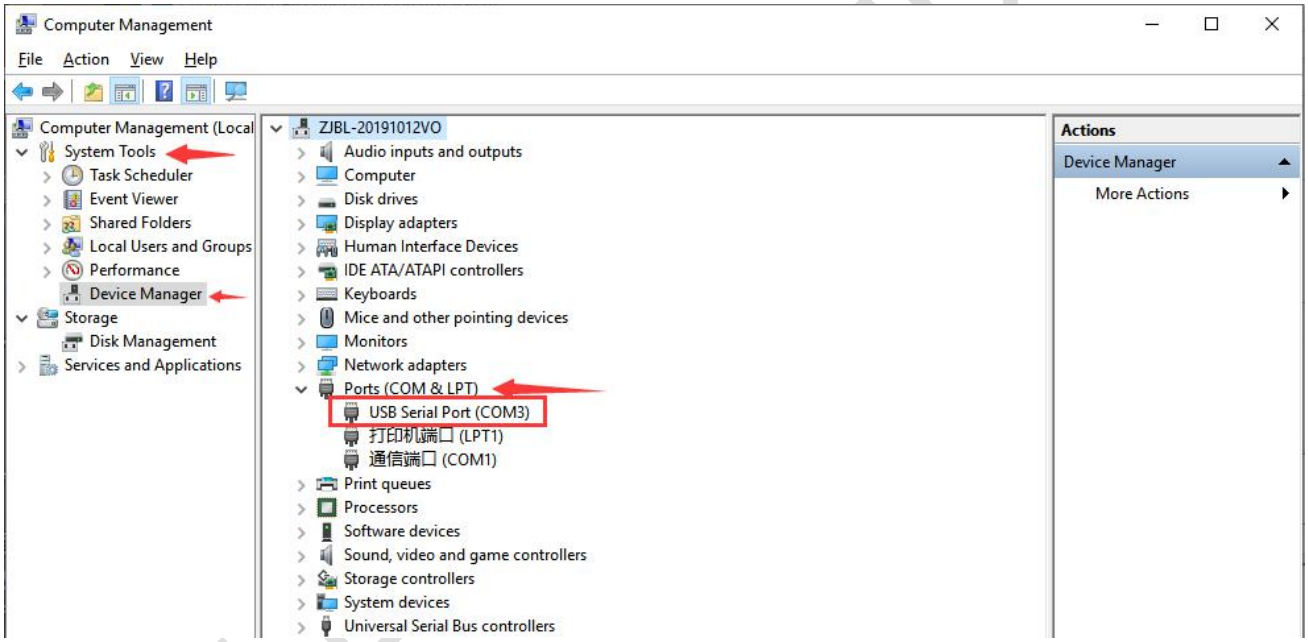
Custom input box: generally used to test whether the connected device can be pinged.



Chapter 3 Serial port configuration

3.1 Use Tools And Preparation

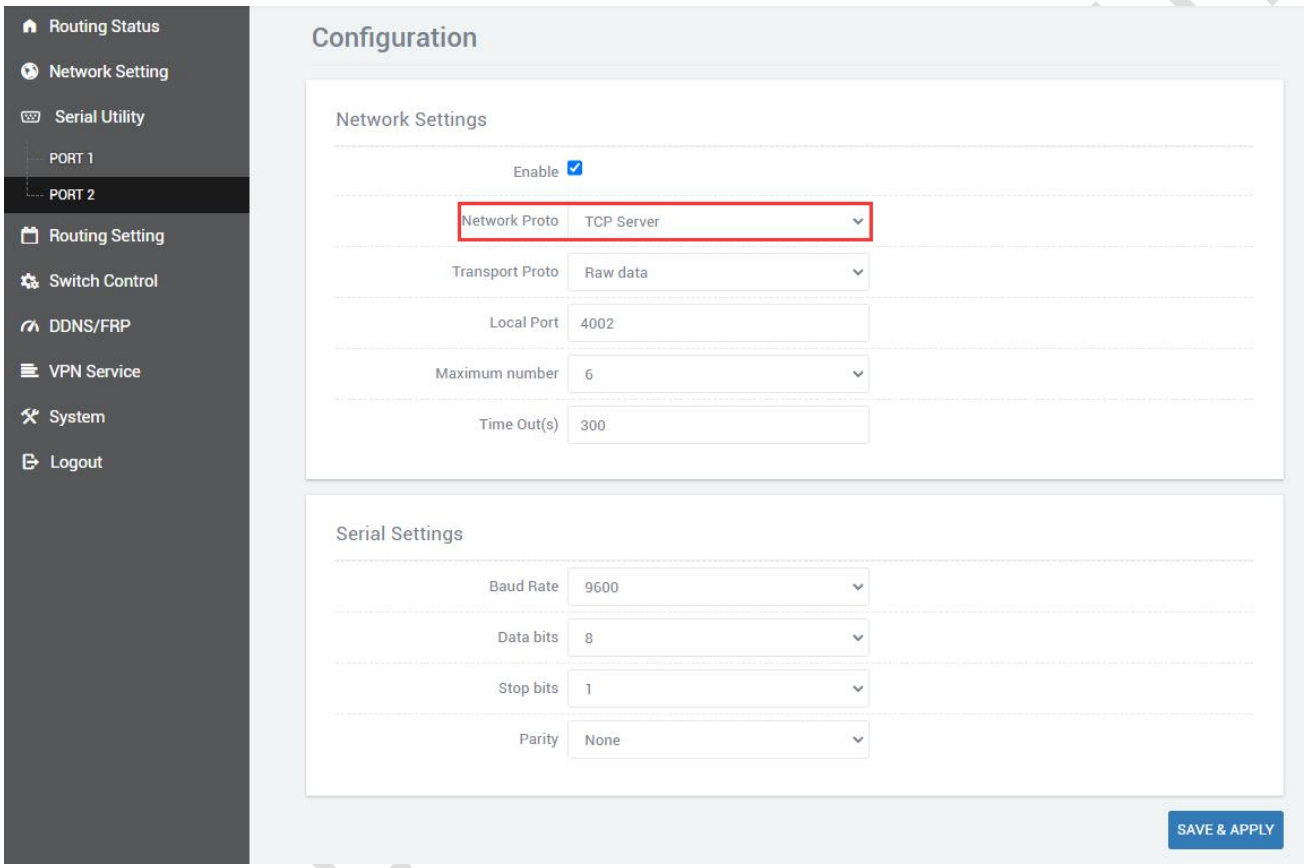
Select Serisl Utility>>>PROT 2 in turn to configure a port according to your needs. Here is an example of PORT 2. Connect the computer serial port, check the serial port as shown in the figure below, right click on the desktop This PC>>>Manage>>>System Tools>>>Device Manage>>>Ports(COM &LPT). Use tools 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

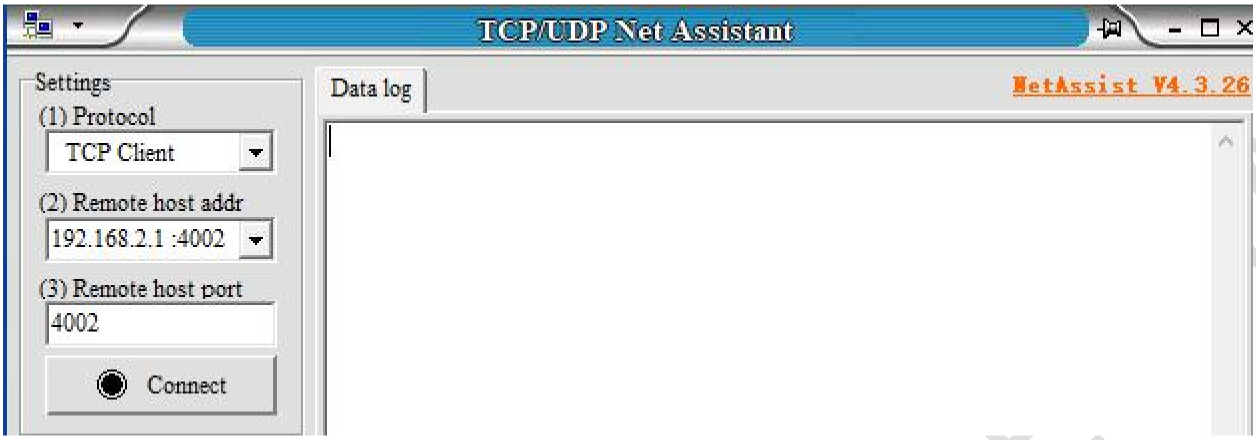
Select Serisl Utility>>>PORT2 in turn,select TCP Server as the network protocol, and choose the data type according to your needs. Generally, the choice is "Raw date". You need to remember the local port after setting. When establishing a TCP connection, you need to use the IP address and port number 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.



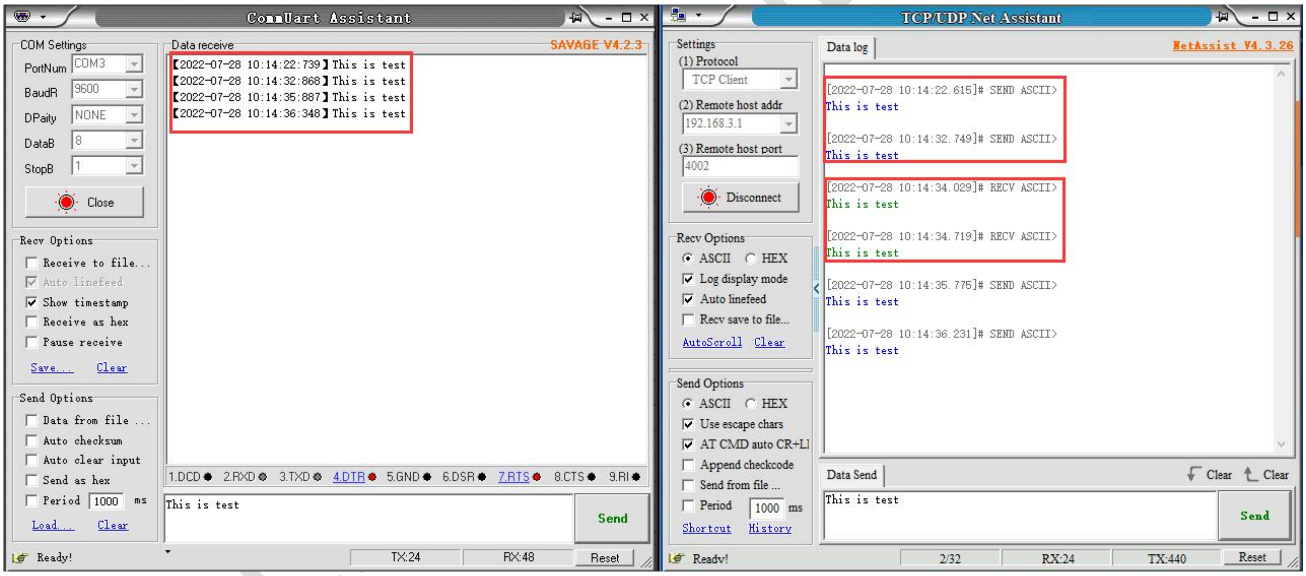
Maximum number: The default is 6, which means that up to 6 TCP Clients are supported to connect to the same serial port.

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.

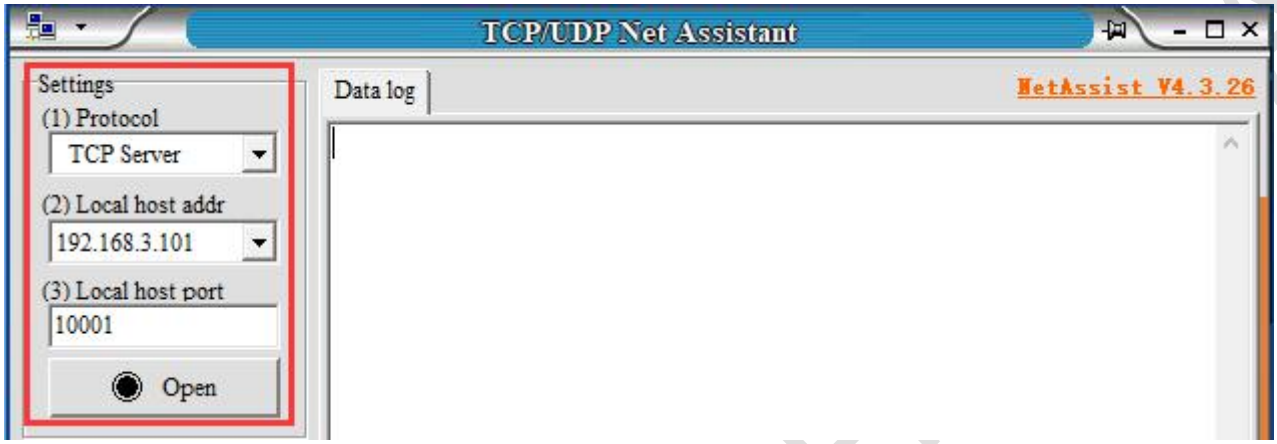


TCP Server and TCP Client send and receive data diagram.

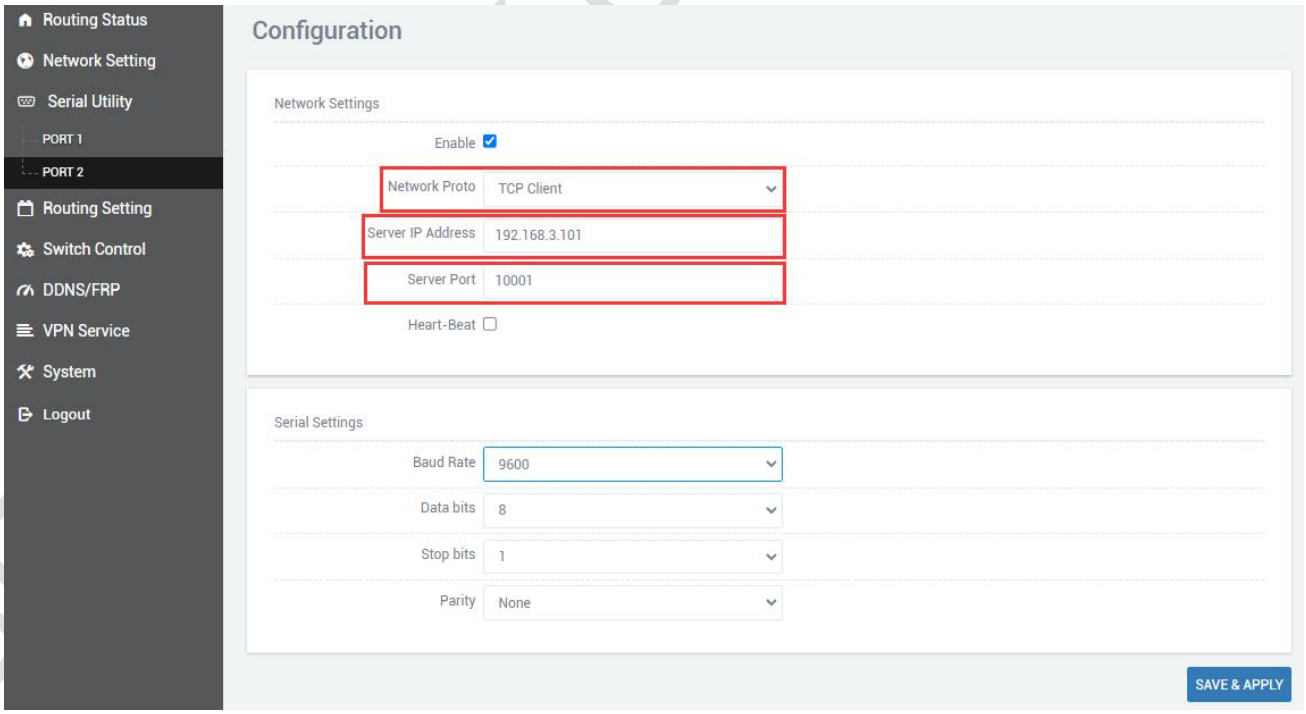


3.3 TCP Client

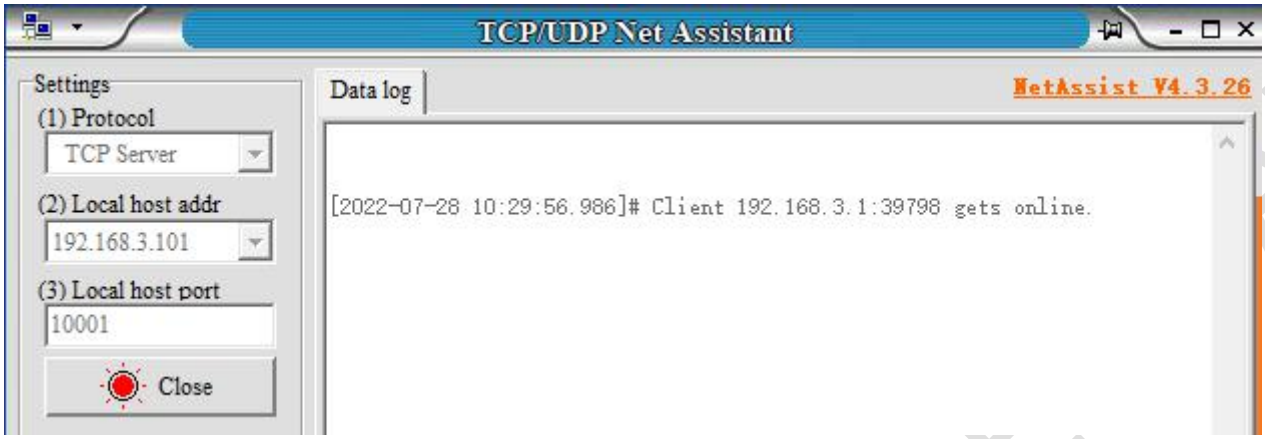
Protocol select TCP Server, Local host addr select the IP address set by the computer, which is in the same network segment as the device's LAN port IP. The Local host port is the default, and the client settings need to use Local host addr and Local host port,click Open.



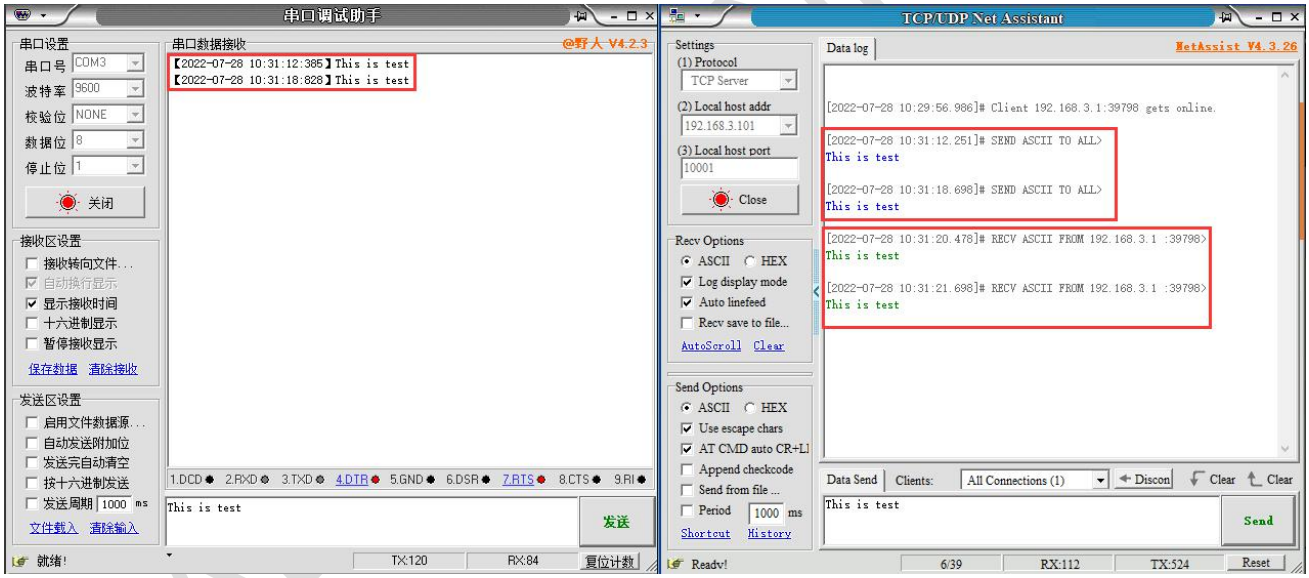
Select Serisl Utility>>>PORT2 in turn,select TCP Client as the network protocol, and the server IP and port number should be consistent with the software settings. Configure the baud rate, data bit, stop bit and parity bit of the serial port according to your needs through the serial port configuration 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.

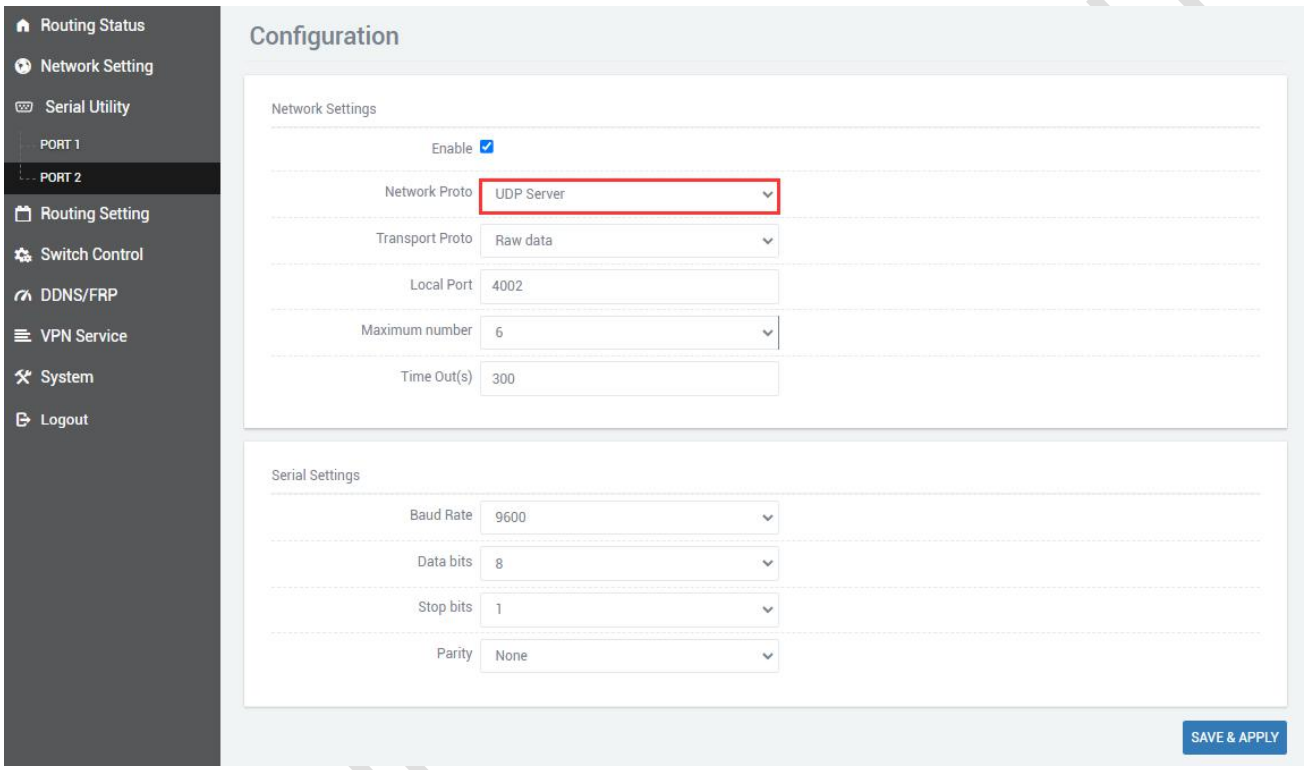


TCP Client and TCP Server send and receive data diagram.



3.4 UDP Server

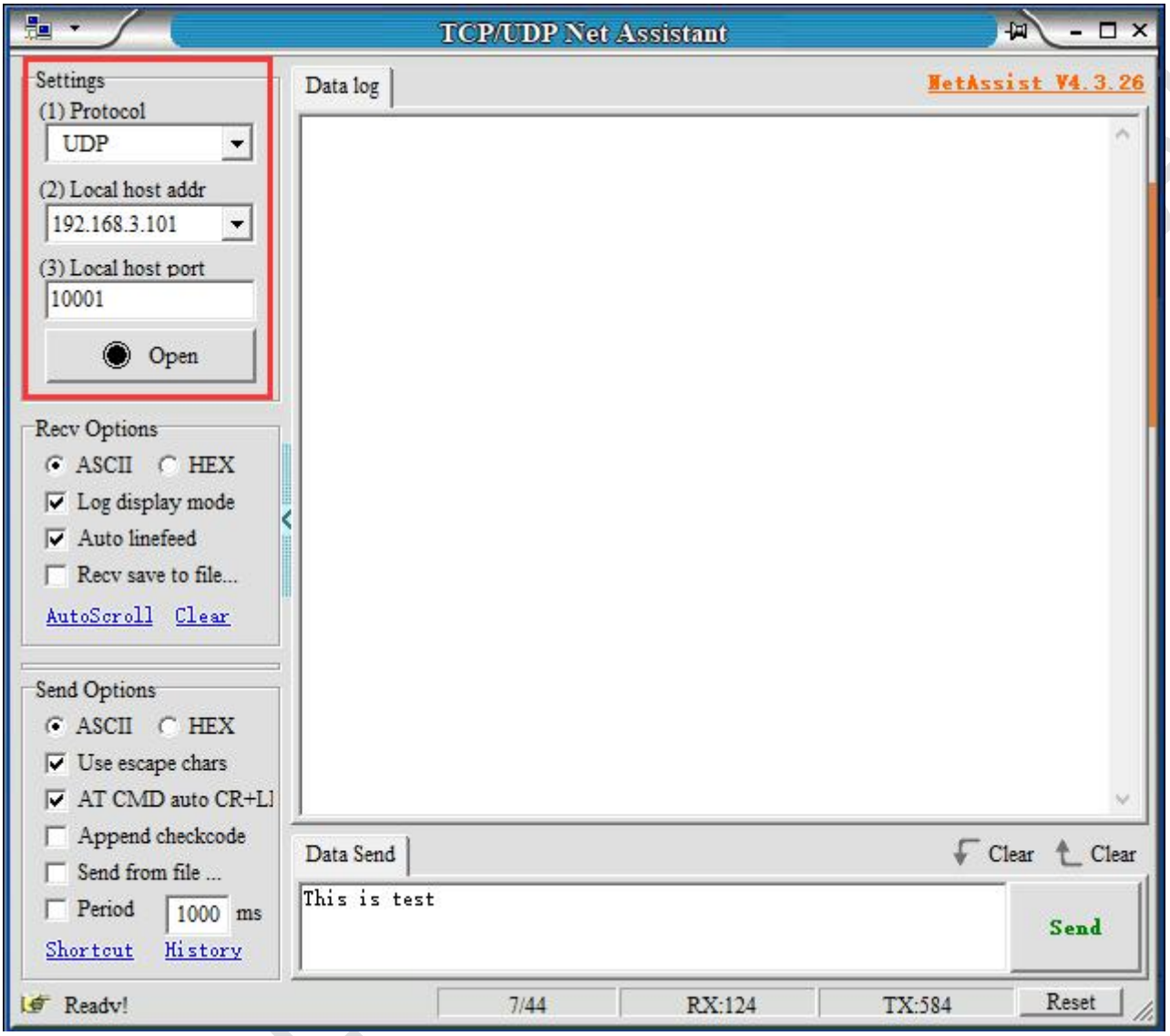
Select Serisl Utility>>>PORT2 in turn,select UDP Server as the network protocol, choose the data type according to your needs. Generally, the choice is Raw date. You need to remember the local port after setting. When establishing a UDP connection, you need to use the IP address and port number of the 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.



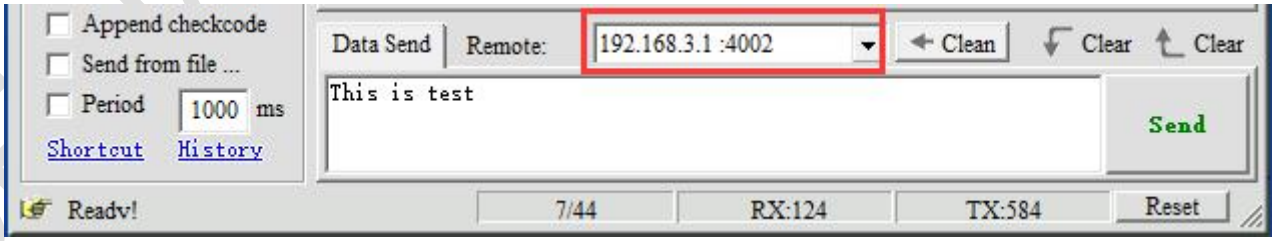
Maximum number: The default is 6, which means that up to 6 UDP Clients are supported to connect to the same serial port.

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.

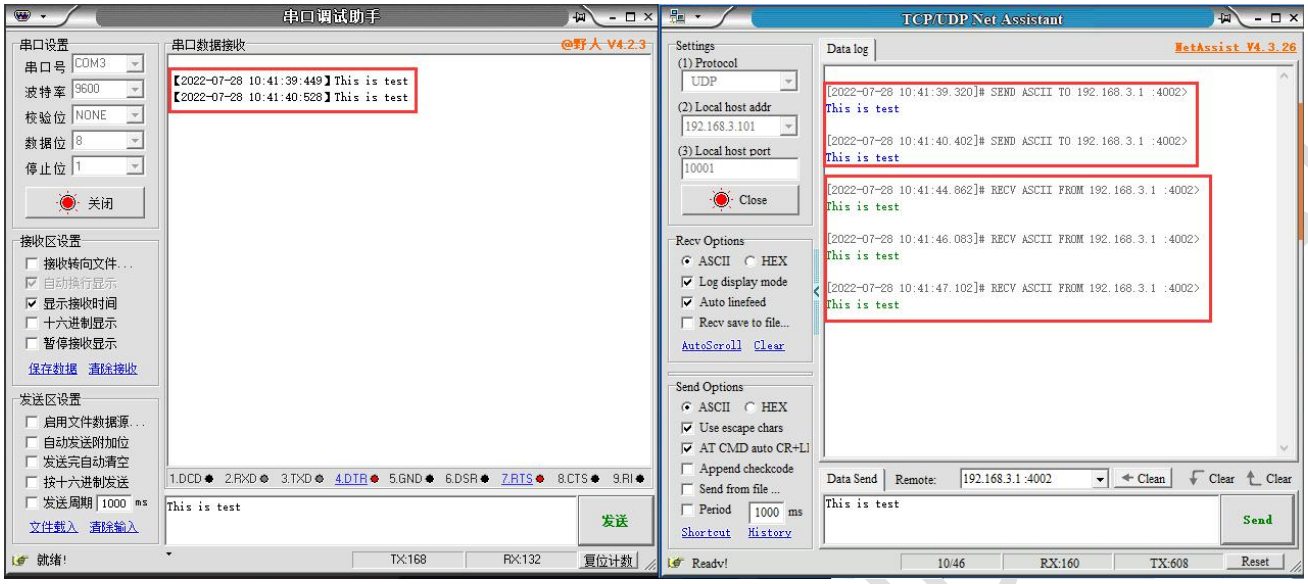
The software settings are as follows, Protocol selects UDP, Local host addr selects the same network segment IP set by the computer and the device, and the Local host port defaults to it. Click Open after setting.



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

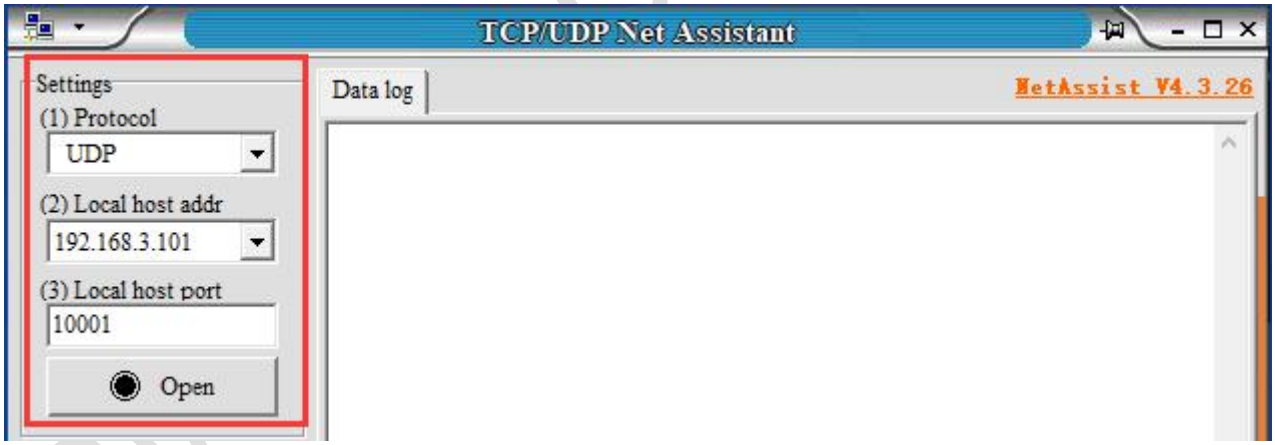


UDP Server and UDP Client send and receive data diagram.

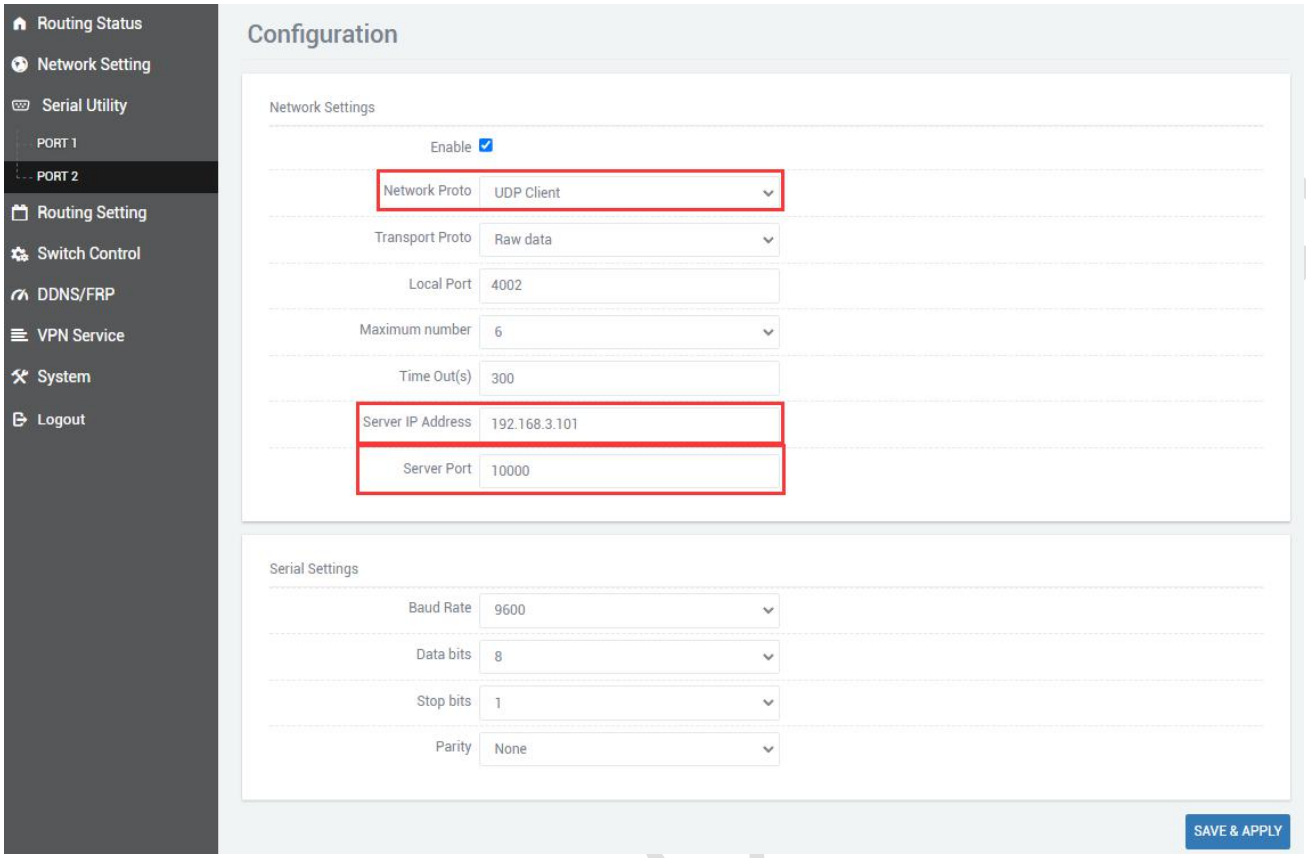


3.5 UDP Client

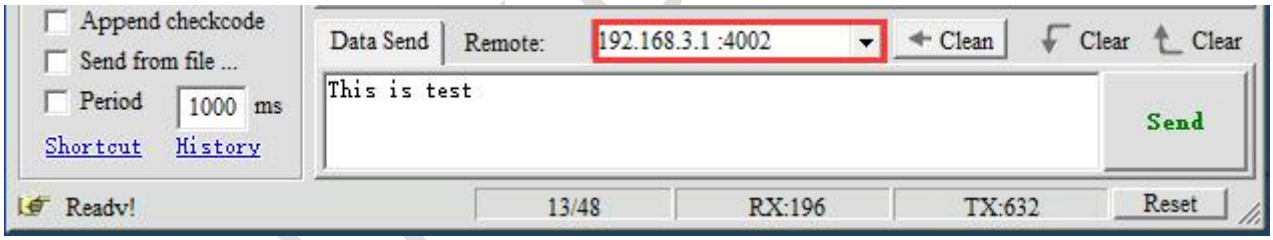
Protocol select UDP, Local host addr select the IP address set by the computer, which is in the same network segment as the device's LAN port IP. The Local host port is the default, and the client settings need to use Local host addr and Local host port,click Open.



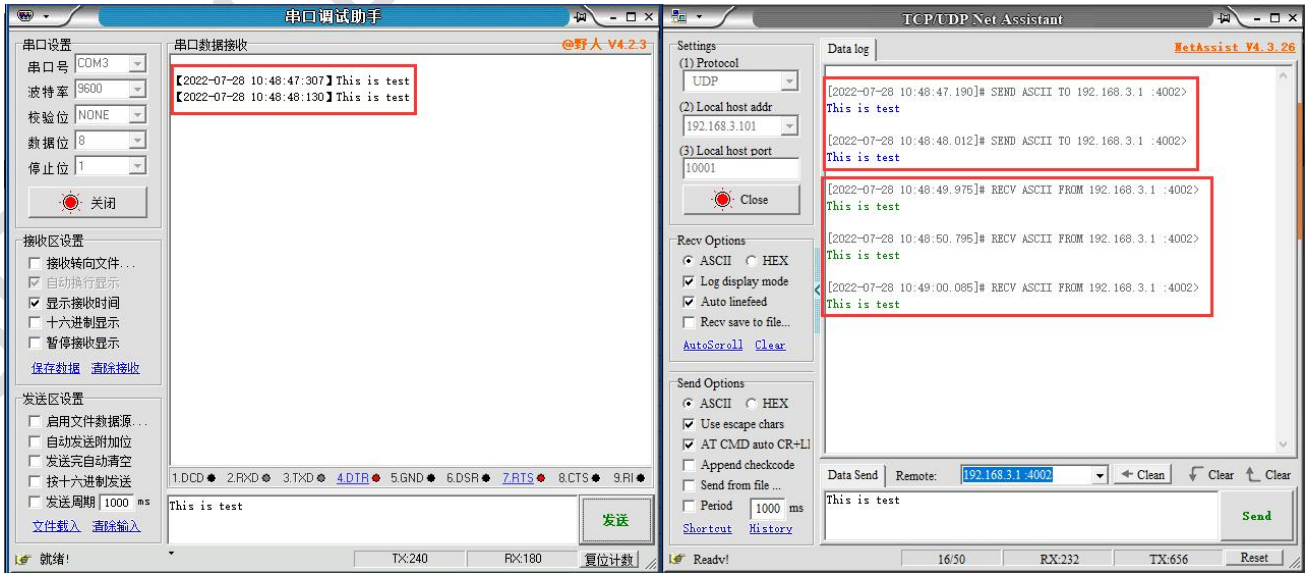
Select Serisl Utility>>>PORT2 in turn,choose UDP Client as the network protocol, and choose the data type according to your needs. Generally, the choice is Raw date. You need to remember the local port after setting. The IP address and port number of the serial port server are used when establishing 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.



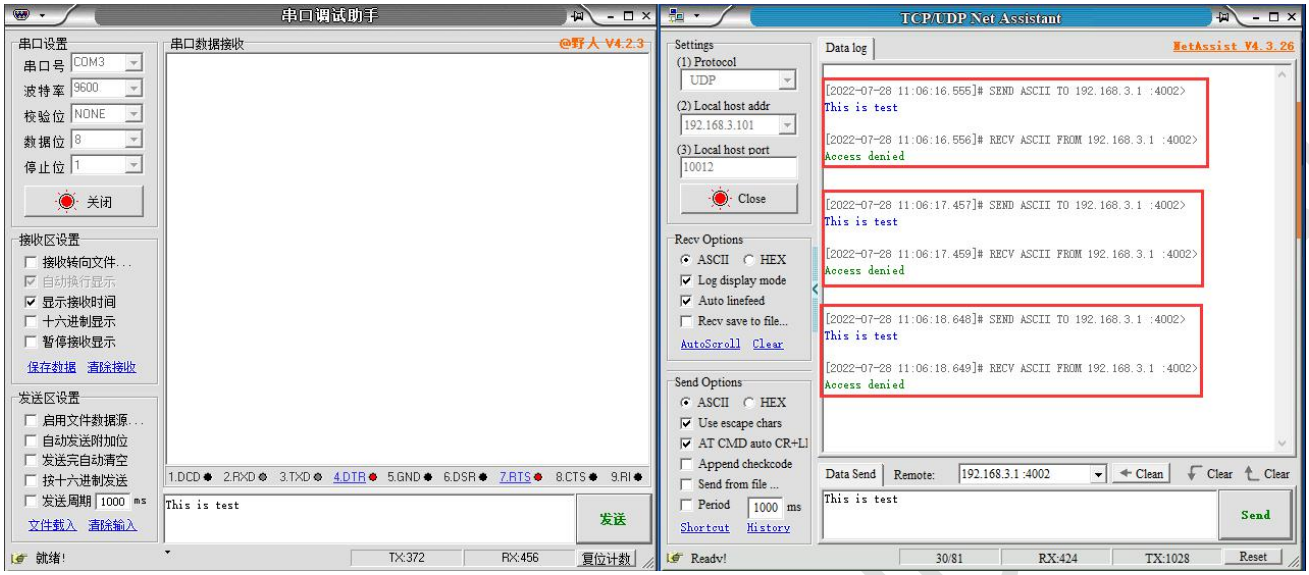
In the next step, the following information needs to be filled in the software.



UDP Client and UDP Server send and receive data diagram,

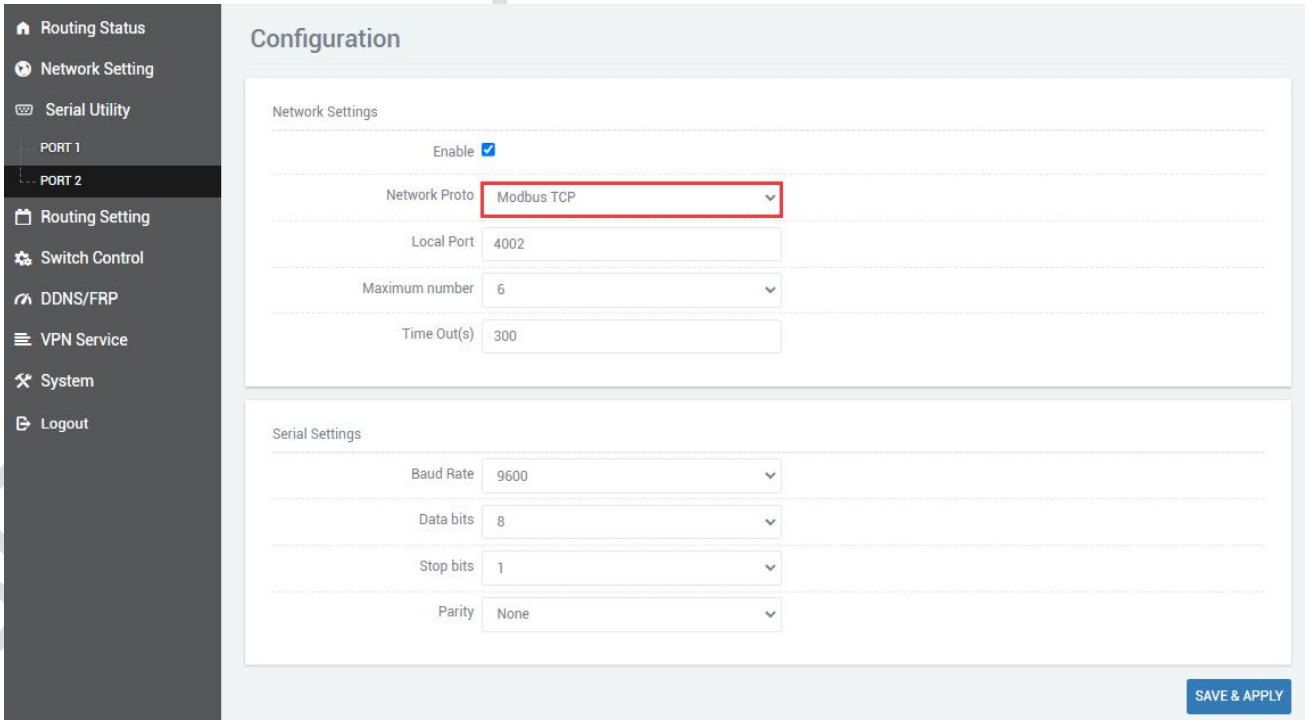


If the data is not sent from the server IP and port, it will be rejected.

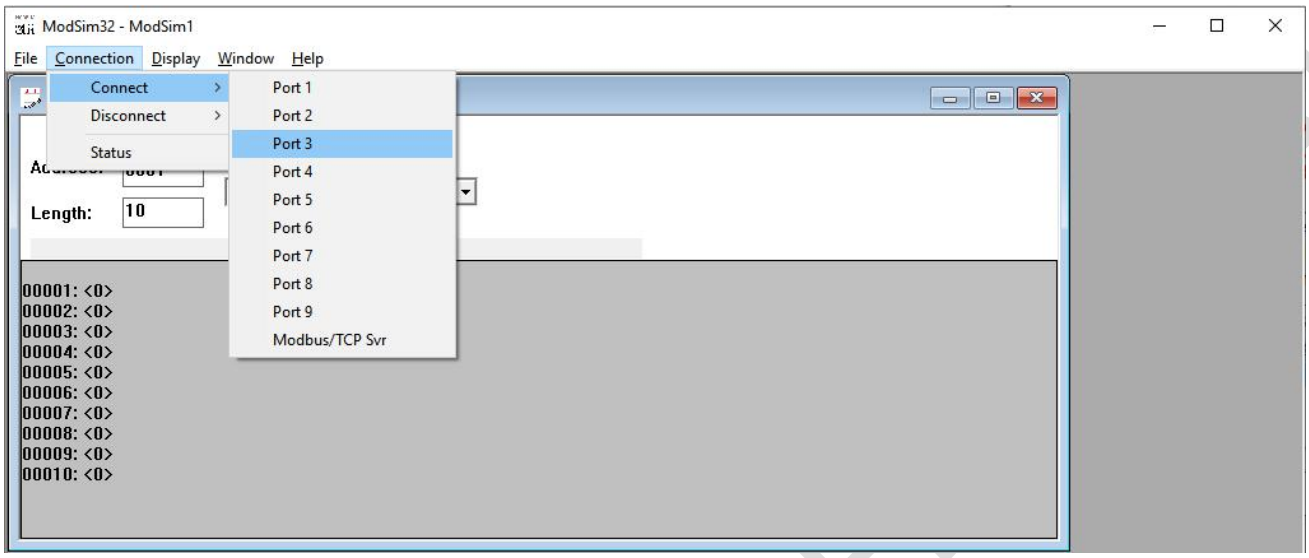


3.6 Modbus TCP

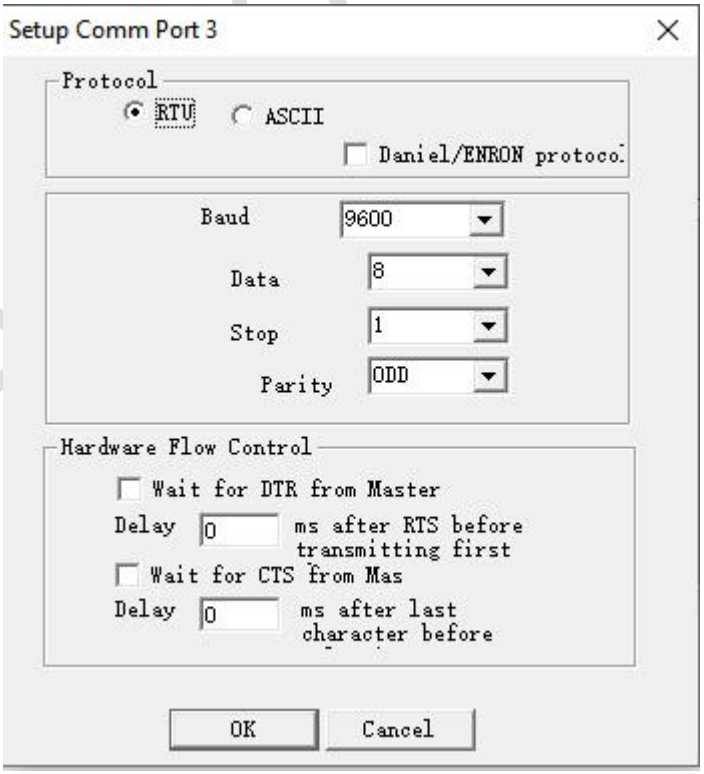
Select Serisl Utility>>>PORT2 in turn,Select Modbus TCP as the network protocol. After setting the local port, remember to configure the baud rate, data bit, stop bit and parity bit of the serial port through the serial port configuration bar according to your needs. After the configuration is complete, click SAVA & APPLY.



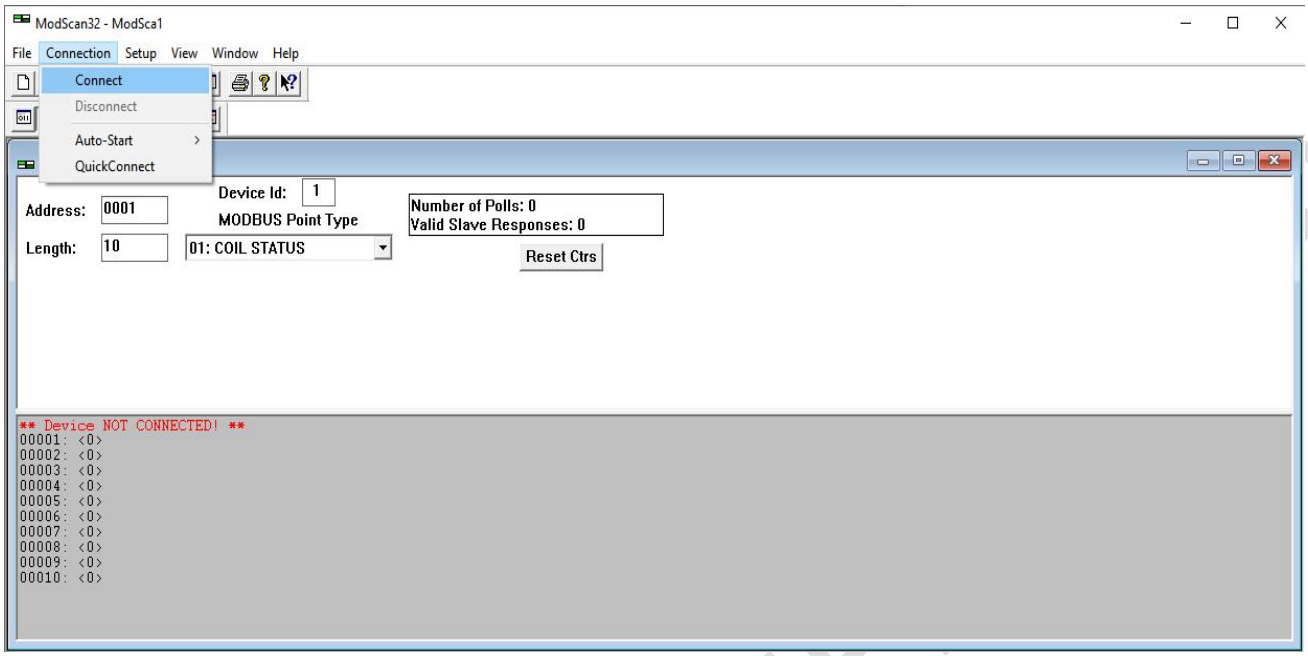
Here you need to use ModSim32.exe and ModScan32.exe to simulate the use, first open the software ModSim32, File>>>New to create a new file, Connection>>>Connect>>>Port 3 (the choice here is the connection between your computer and the device port).



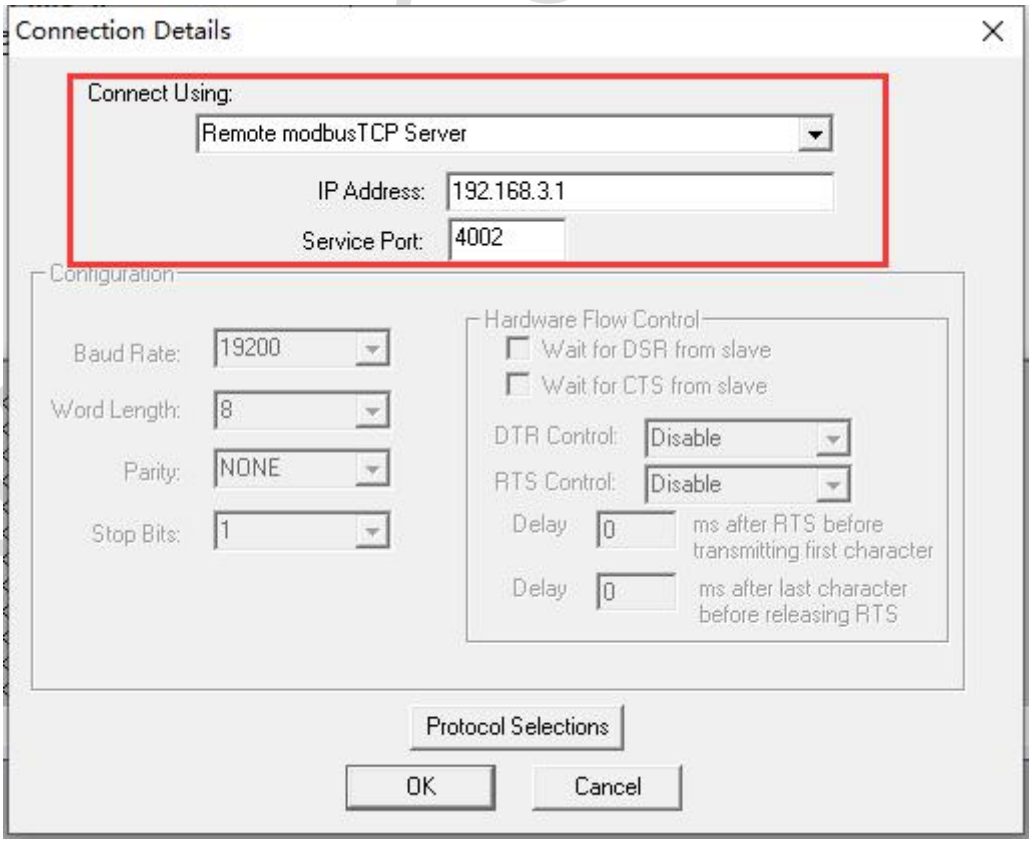
The pop-up dialog box is as follows, the baud rate, data bit, stop bit and parity bit are changed according to the values set on the web page.



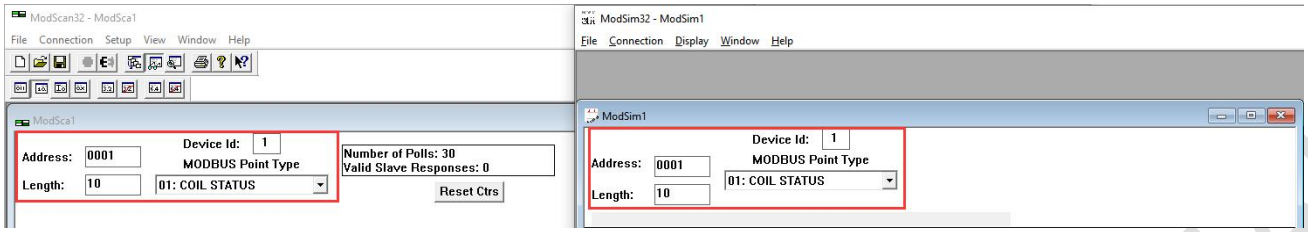
Open the software ModScan32, Connection>>>Connect.



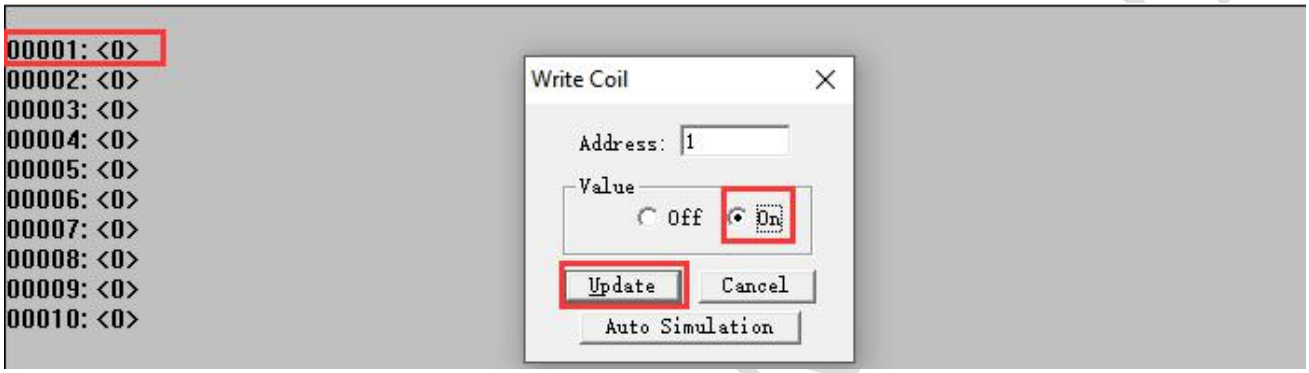
The pop-up dialog box is as follows, select Remote modbusTCP Server, fill in the IP Address and Service Port, and then click OK.



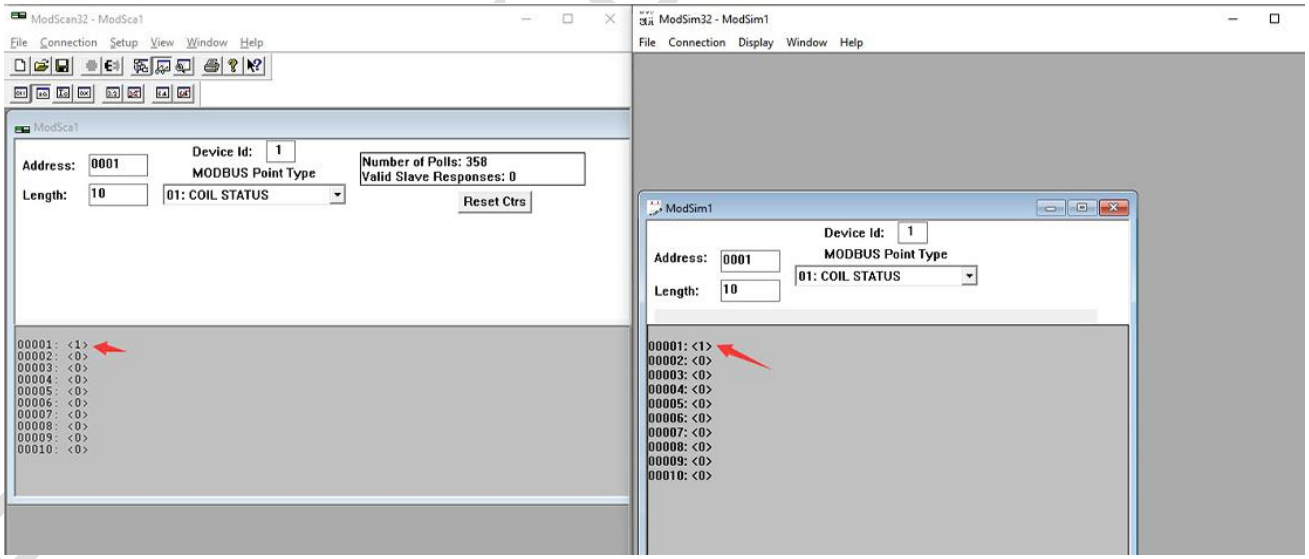
The selected settings in ModSim32 and ModScan32 software need to be consistent.



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

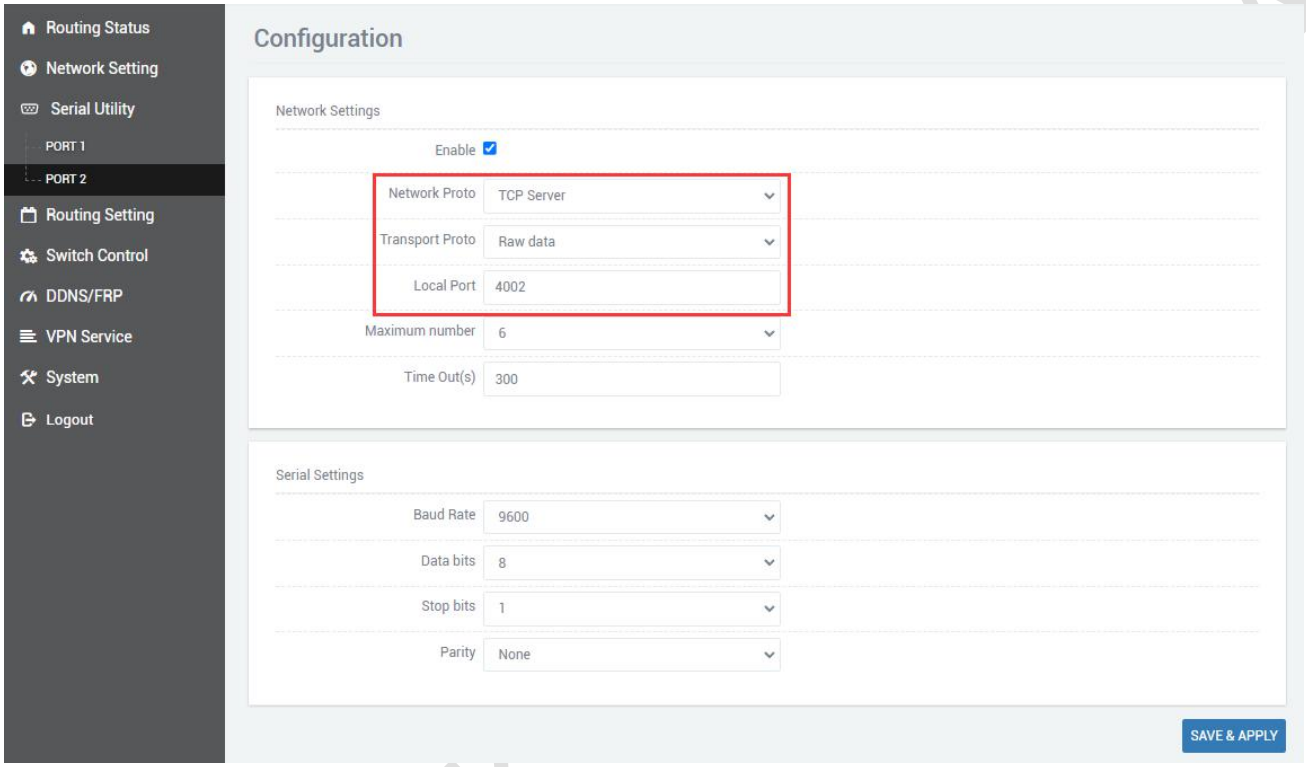


The effect is as follows

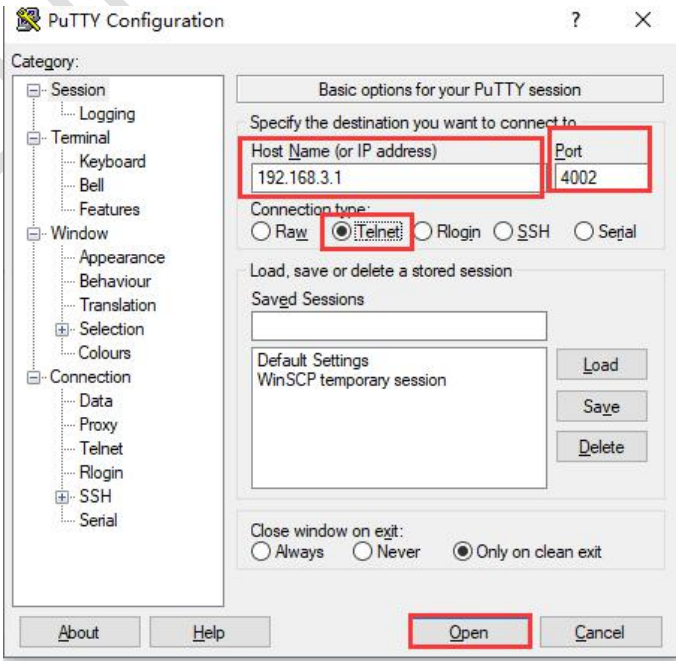


3.7 Transport Proto

When selecting TCP Server, the data type also has the option of Telnet (RFC2217), and a software putty.exe is used here.Select Serisl Utility>>>PORT2 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.

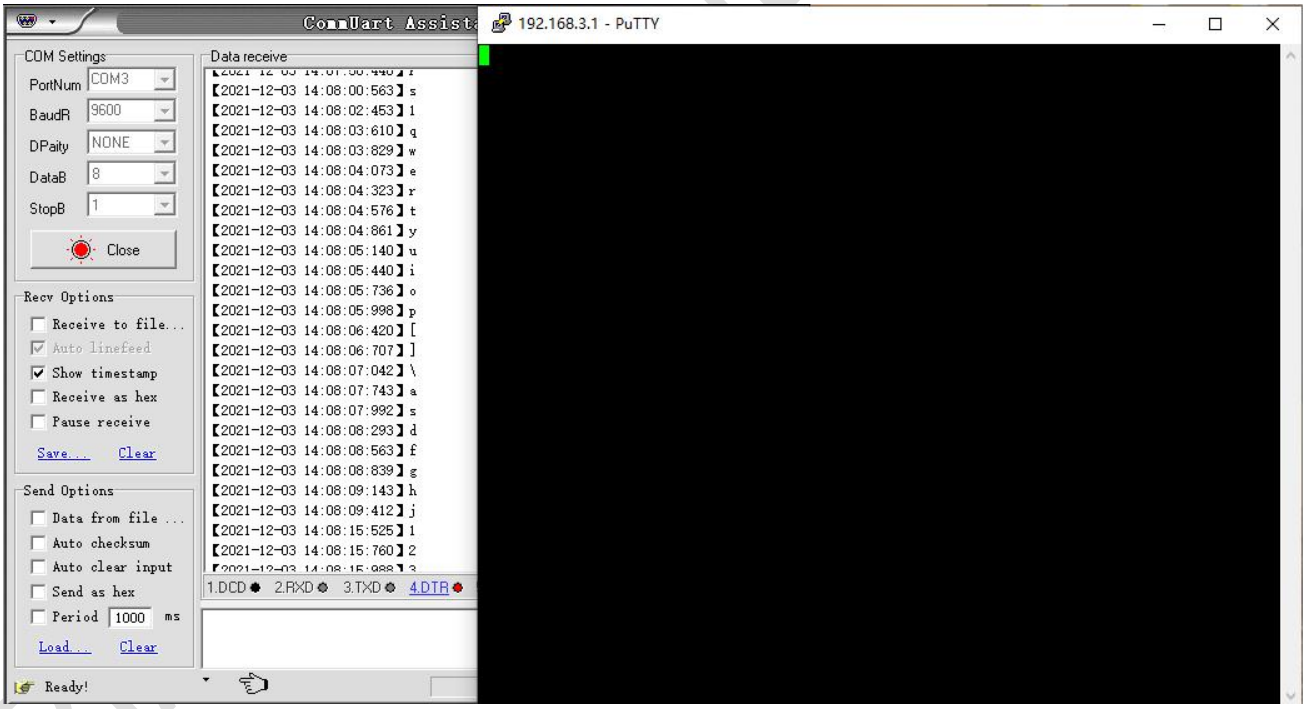


Open the putty.exe software, fill in the server IP address and port number, select Telent for Connection type, set as follows, click Open after the configuration is complete.



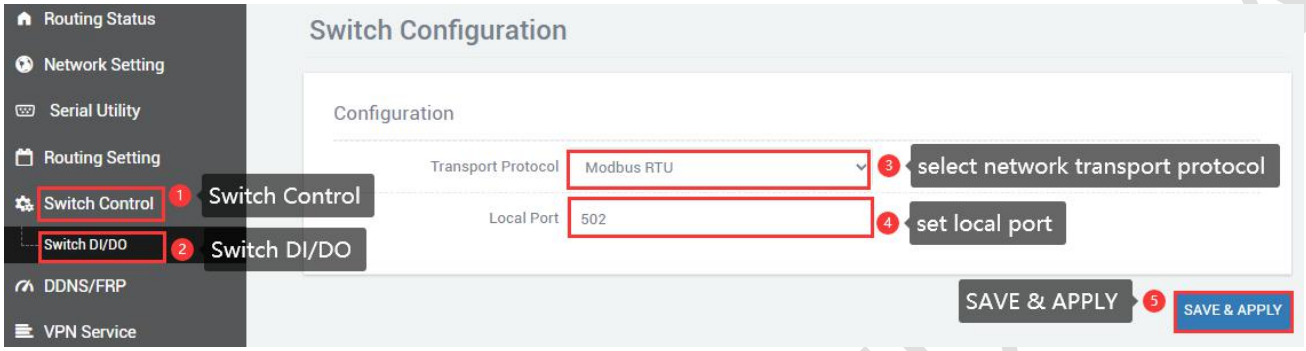
If no error is prompted after opening, a pure black dialog box will be displayed, as shown below.

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

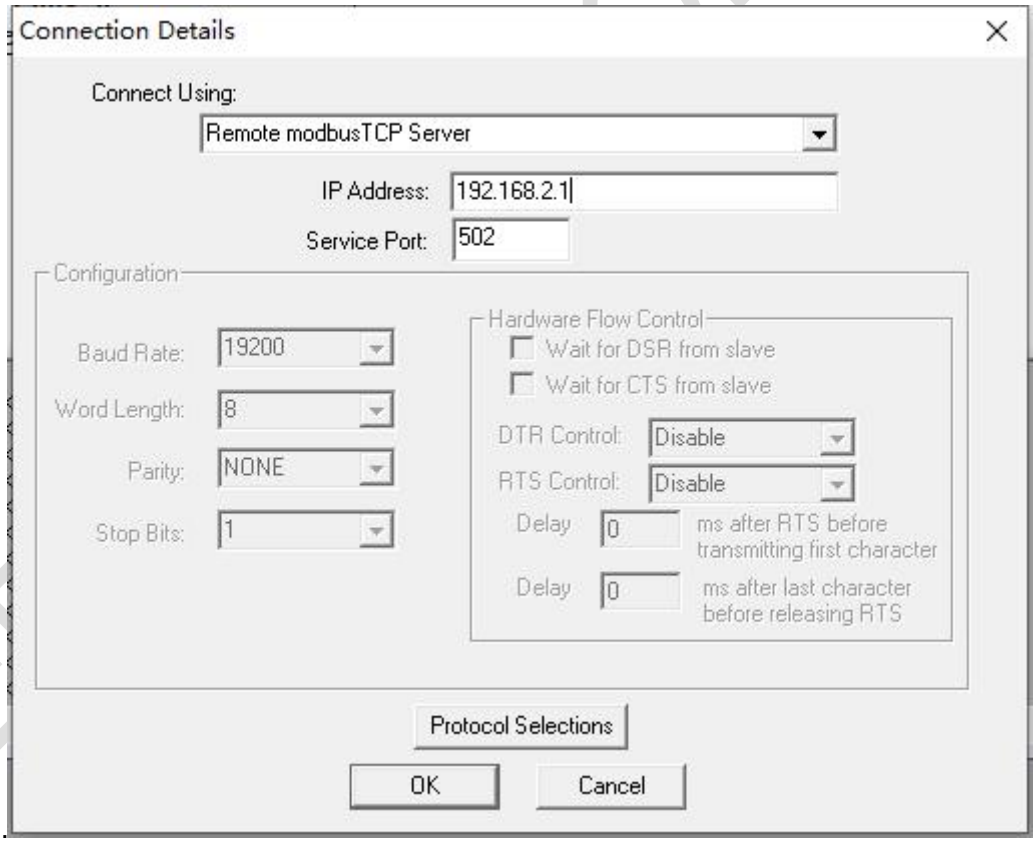


3.8 Switch quantity control

Click on the switch controller >>> switch DI/DO, select the network transmission protocol as required, set the local port number and click save and apply.

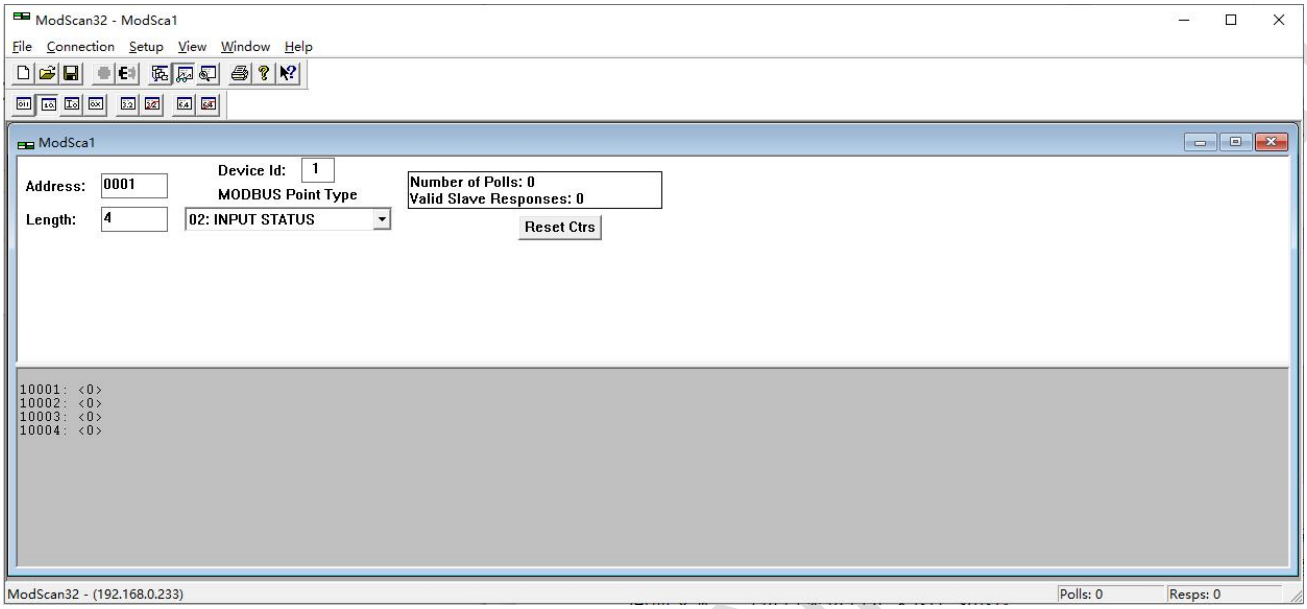


Open the ModScan32.exe software, click Connection Settings >>> Connection in the menu bar, fill in the IP Address in the pop-up window as the IP address of the LAN port, the service port is the local port in the switch setting, and then click OK, the settings are as follows:

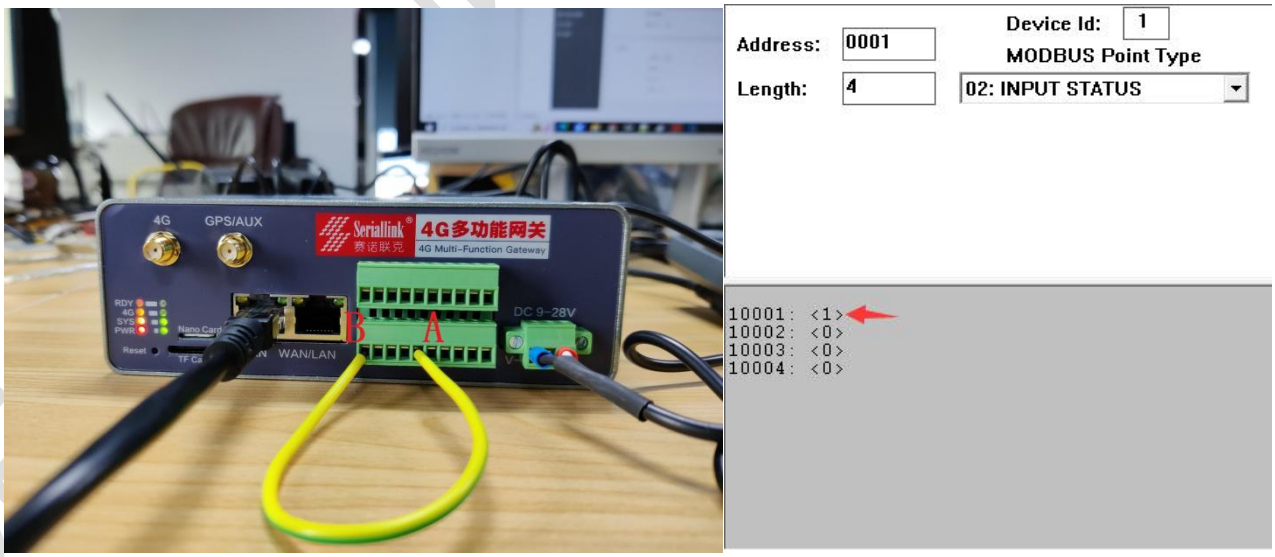


3.8.1 Switch quantity DI

As shown in the figure below, the set value of Address in the red box is 0001, the set value of Length: 4, and the MODBUS Point Type is 02: INPUT STATUS.



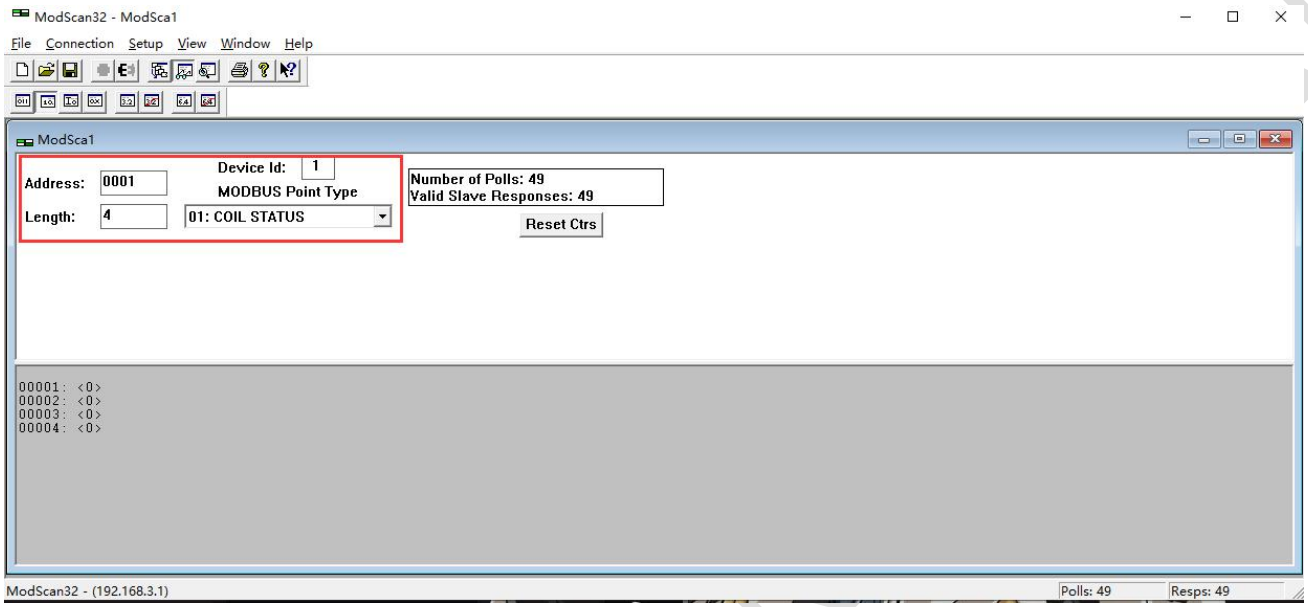
This is mainly for demonstration, using shorting method, A is connected to DCOM, B is connected to DIN1, the interface is corresponding to the value in the software, DIN1 corresponds to 10001, DIN2 corresponds to 10002, DIN3 corresponds to 10003, and DIN4 corresponds to 10004. The value in the angle brackets will change according to the wiring method, (see the interface definition diagram for the interface) as shown in the figure.



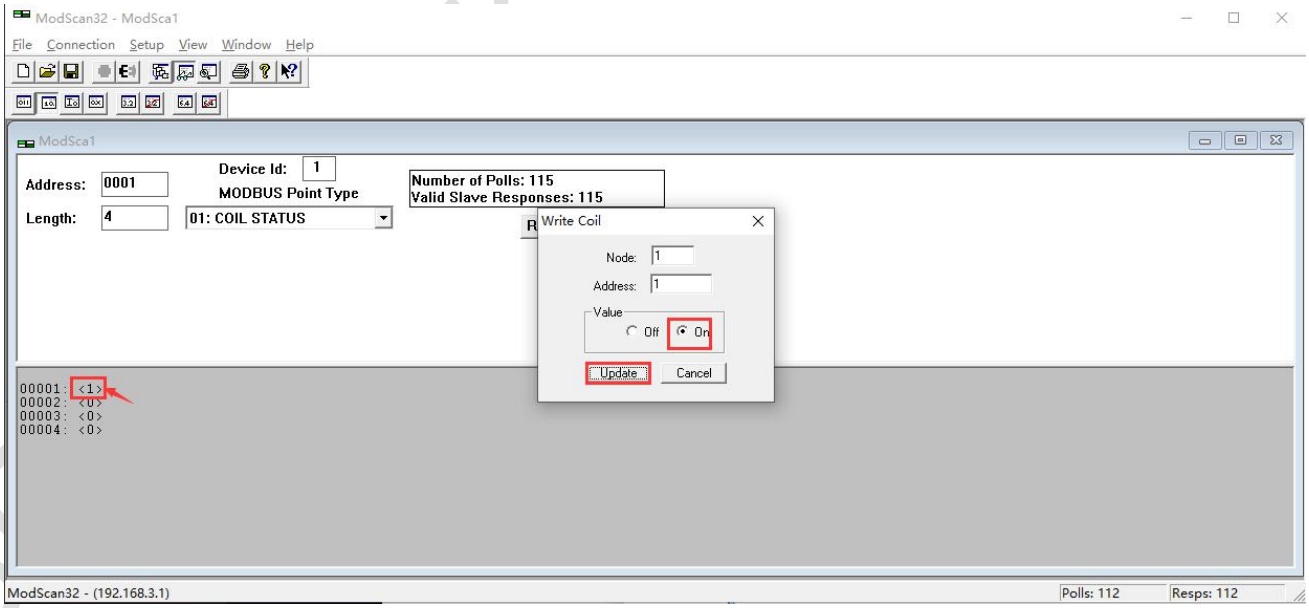
If B is connected to DIN2, the value of 10002 becomes 1.

3.8.2 Switch quantity DO

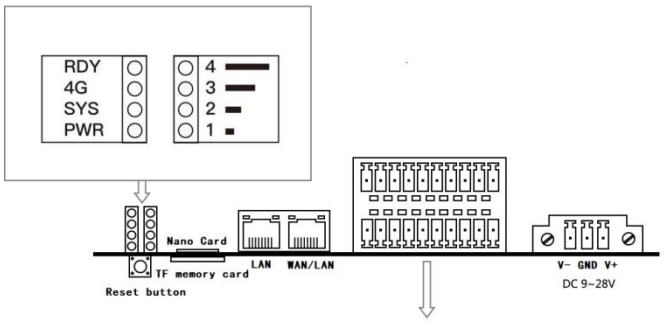
As shown in the figure below, the set value of Address in the red box is 0001, the set value of Length: 4, and the MODBUS Point Type is 01:COIL STATUS.



Double-click the value in the angle brackets, select On or Off, click Update, and the device emits a sound, the switch DO value is changed successfully, DO1 corresponds to 10001, DO2 corresponds to 10002, as shown in the figure



see the interface definition diagram for the interface

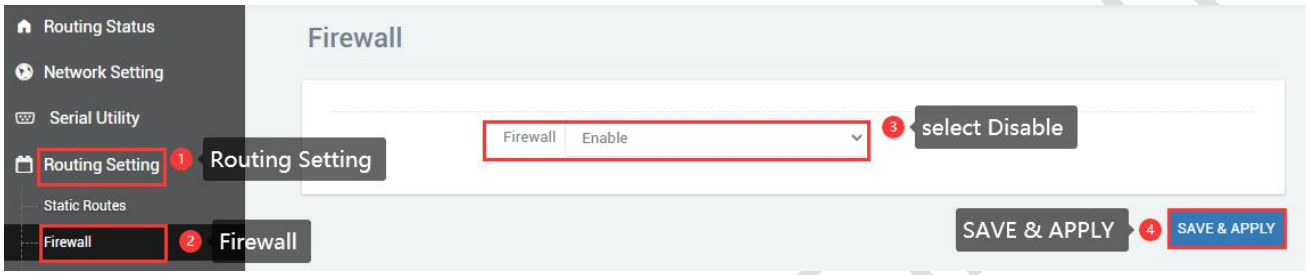


	1	2	3	4	5	6	7	8	9	10
ROW 1	TXD1	RXD1	GND	485-A1	485-B1	TXD2	RXD2	GND	485-A2	485-B2
ROW 2	DIN1	DIN2	DIN3	DIN4	DCOM		DO1	COM1	DO2	COM2

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.

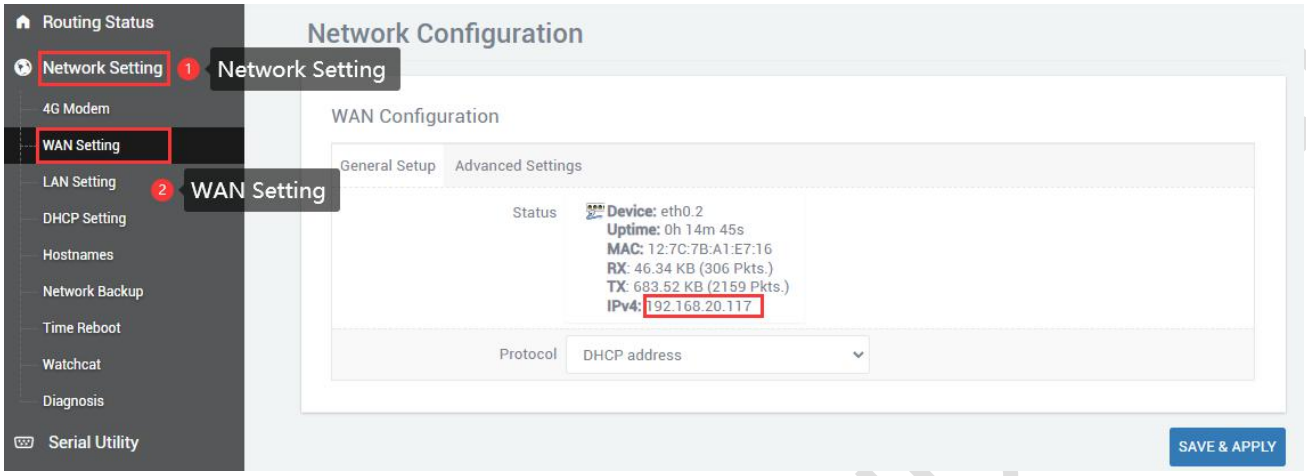
First, you need to disable the firewall, click "Routing Setting" - "DMZ" in the navigation bar, click Enable, set the IP address assigned by the lan port to the connected device, and forward all the ports of the connected device,It can be accessed directly through the IP address of the wan port.

Enable: Tick Enable.

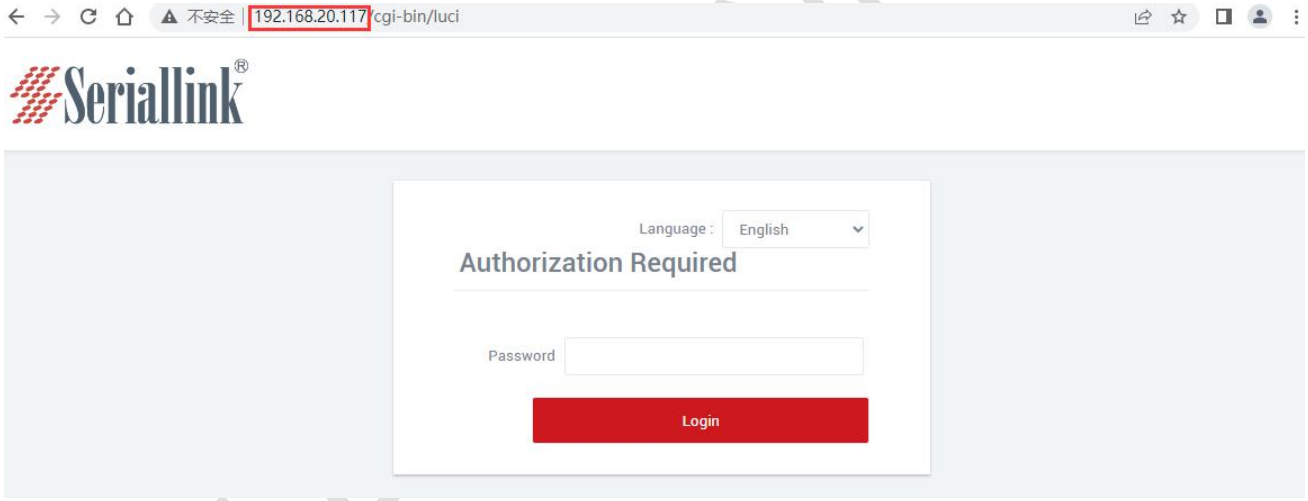
Internal IP address: The ip address of the local device or the ip assigned to the connected device through dhcp.

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.

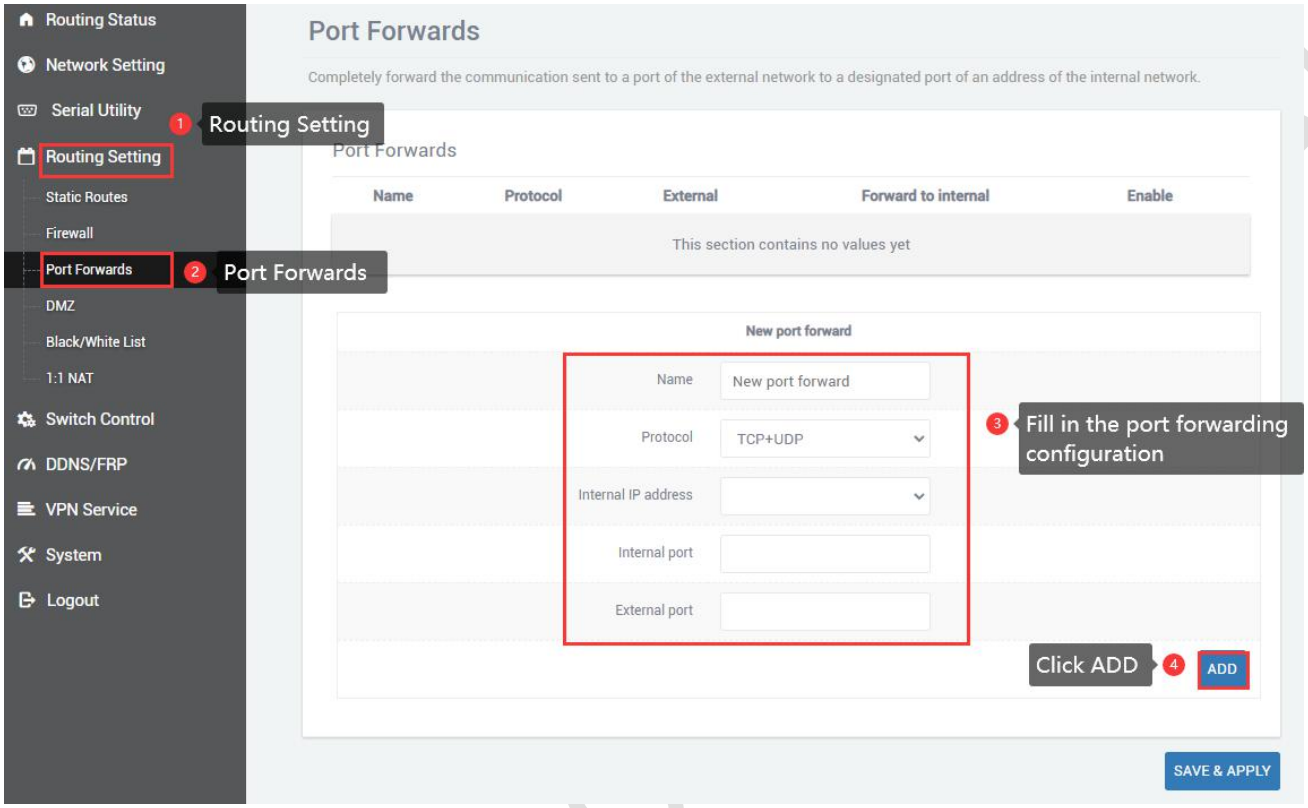
B.Protocol: Specifies the protocol to be forwarded, which can be TCP, UDP, or TCP/UDP.

C.Internal IP address: Select the IP address that needs to be forwarded to the external network.

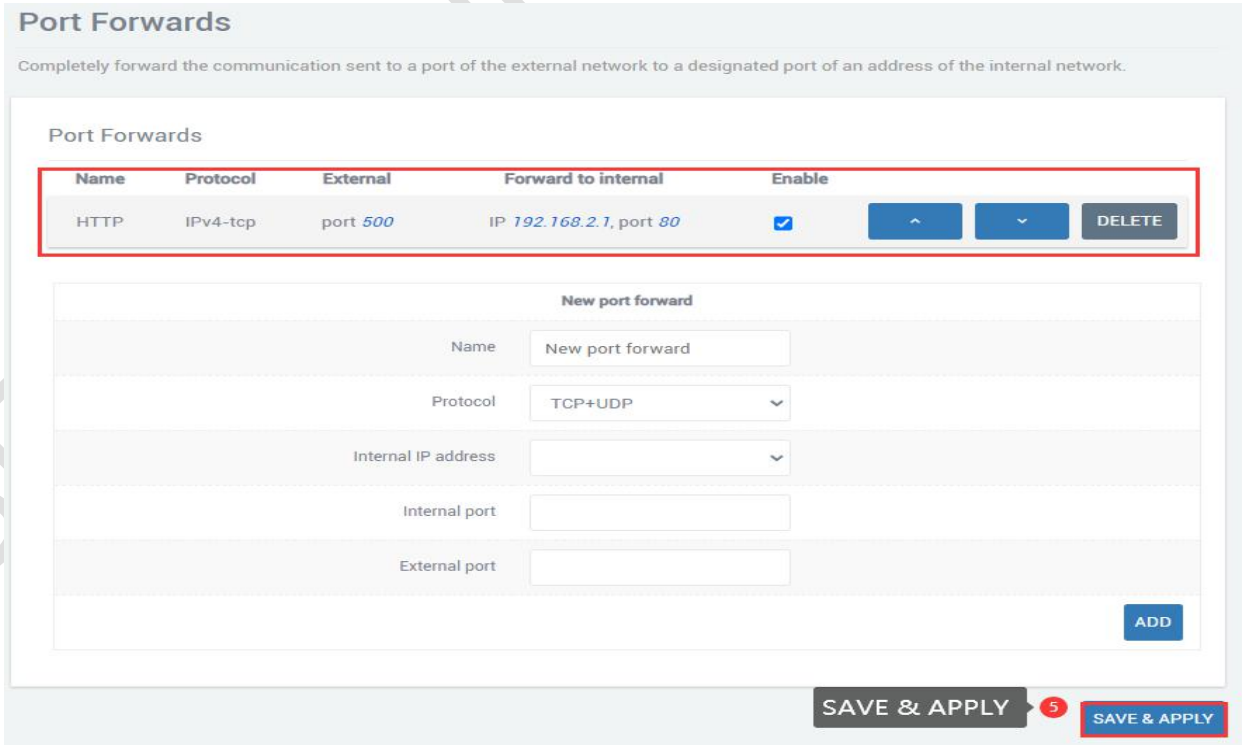
D.Internall port: The port to be forwarded by the connected device or the machine.

E.External port: Add this external port through the wan port ip to access the connected device.

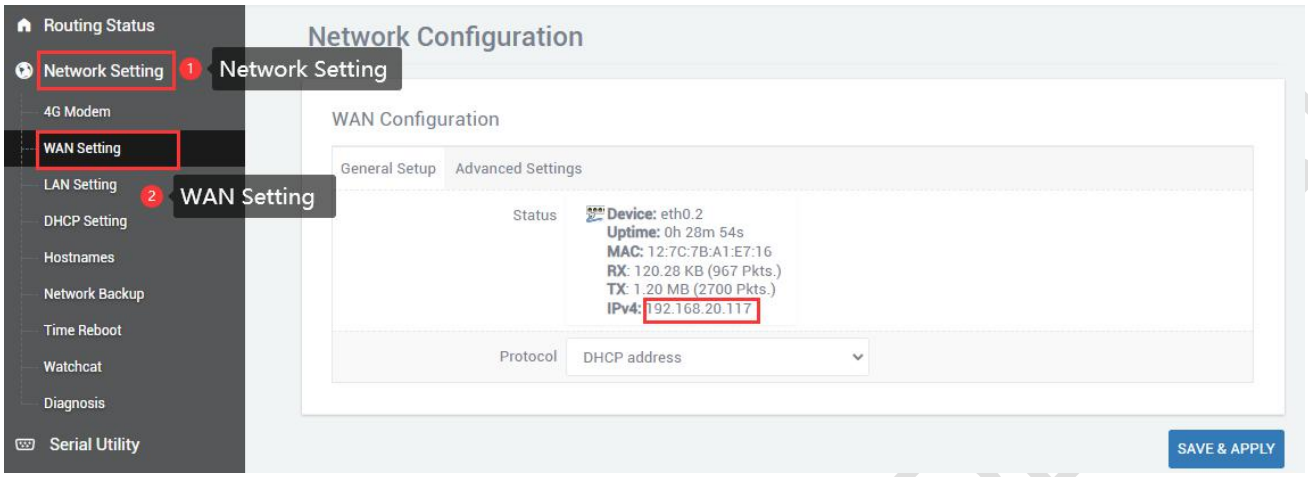
D.After configuration, click the "ADD" button to add a forwarding rule. Click the "SAVE & APPLY" button to make the rule take effect.



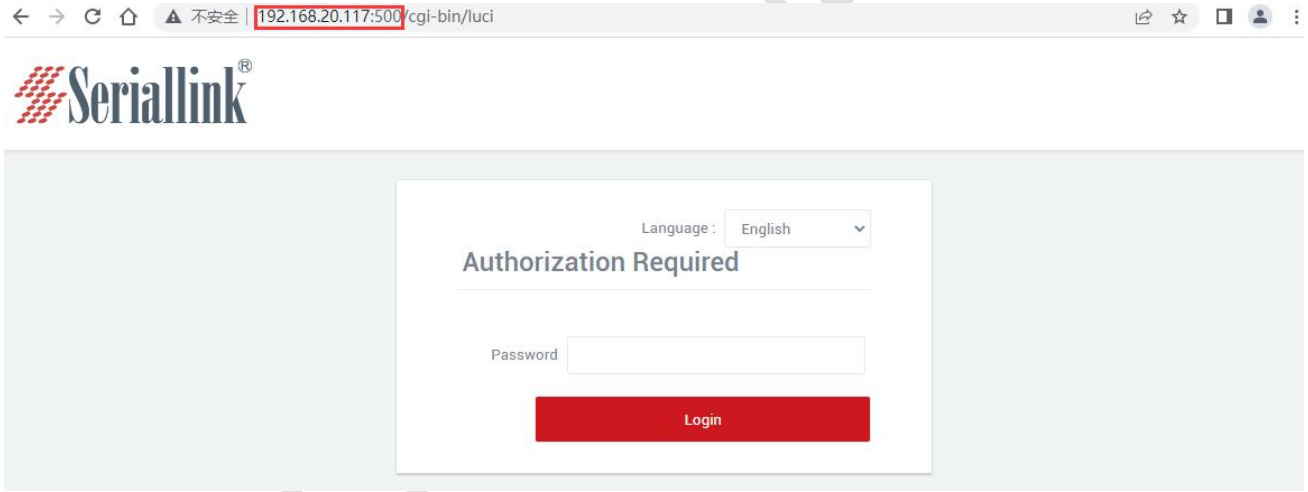
After the addition is successful, a port forwarding rule will be added. Click "SAVE & APPLY" to make the rule take effect. Multiple rules can be added.



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



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.

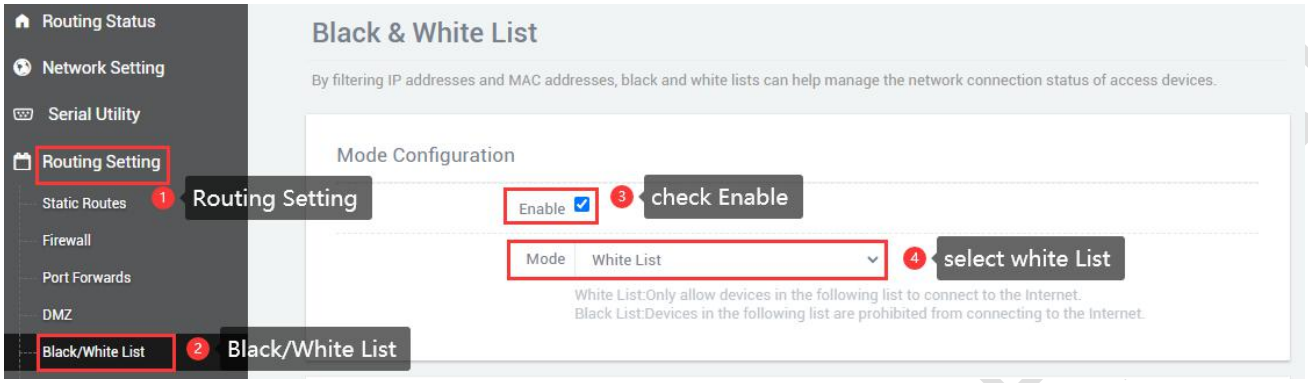
C.Match ICMP type: All types are selected by default, choose according to your needs.

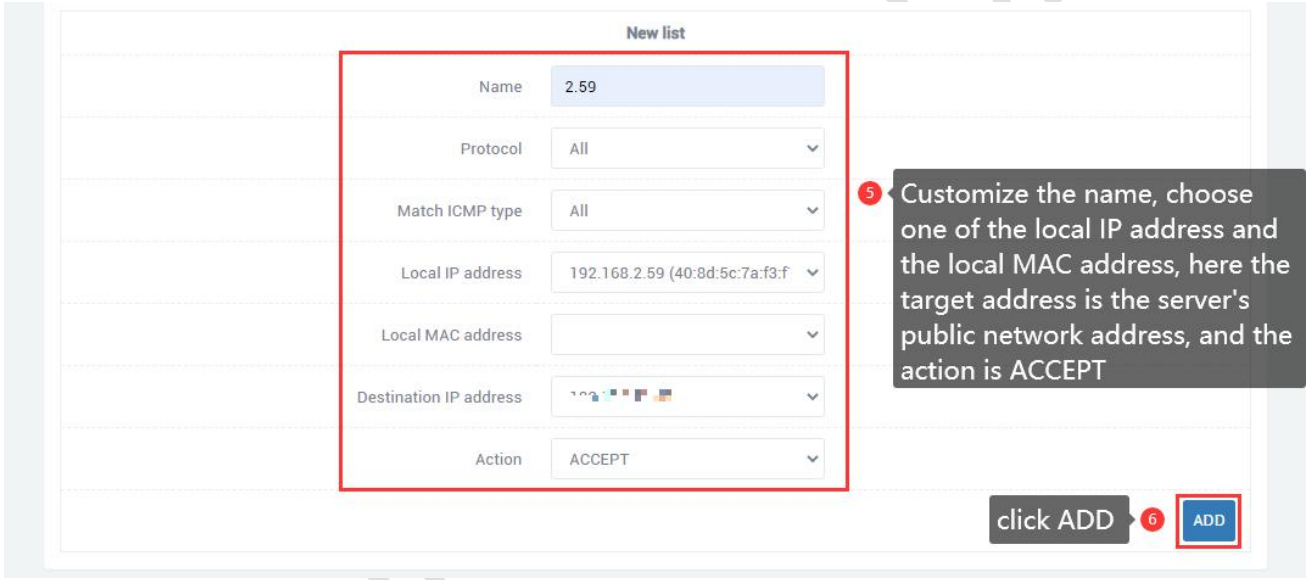
D.Local IP address: The IP address of the device added to the whitelist, the IP address change caused by man-made or other reasons, will change the device that can access the Internet.

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.

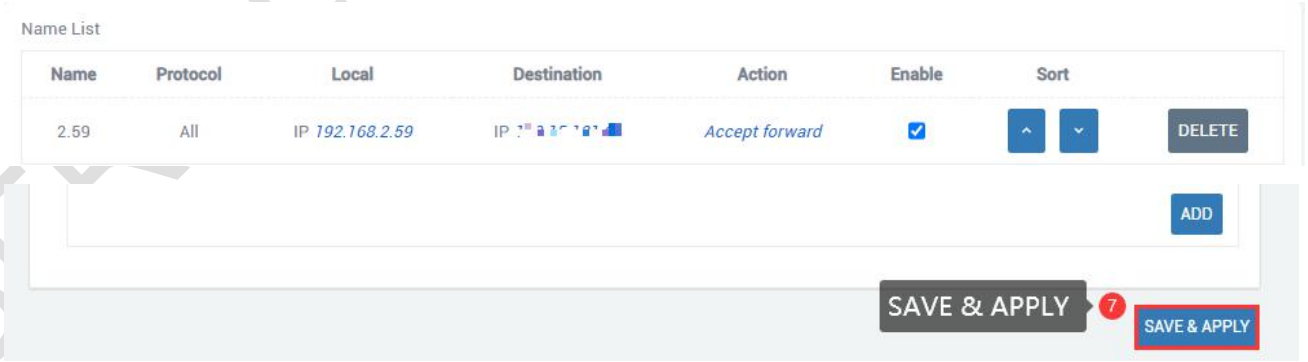
F.Destination IP address: If not selected, it means all networks. You can also enter an IP address, such as the public network server IP.

G.Action: Whitelist mode select ACCEPT.

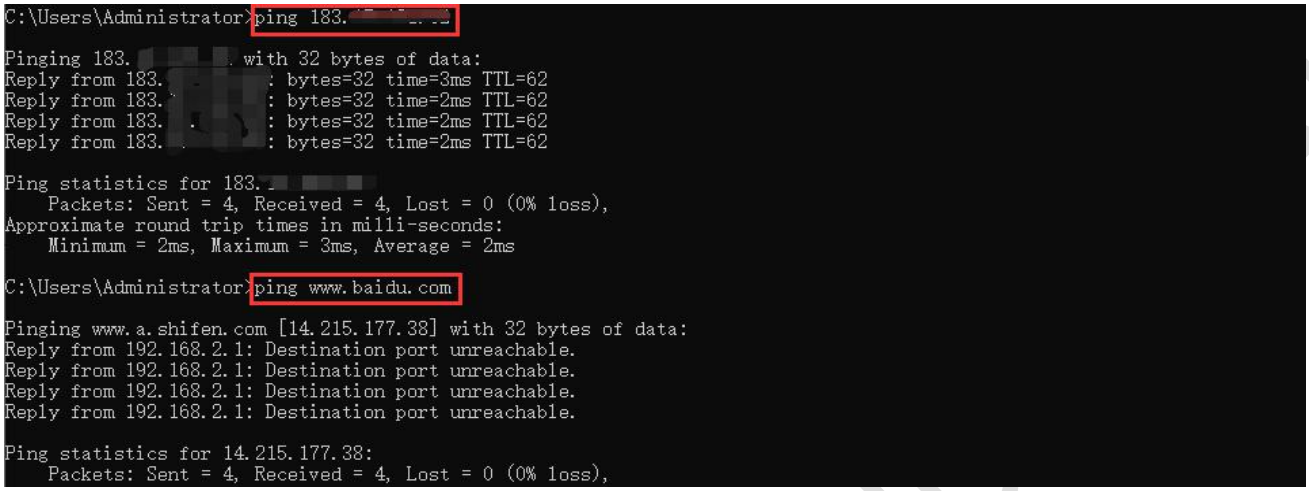




After clicking Add, a rule will be automatically refreshed in the page list, click "SAVE & APPLY".



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.



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.

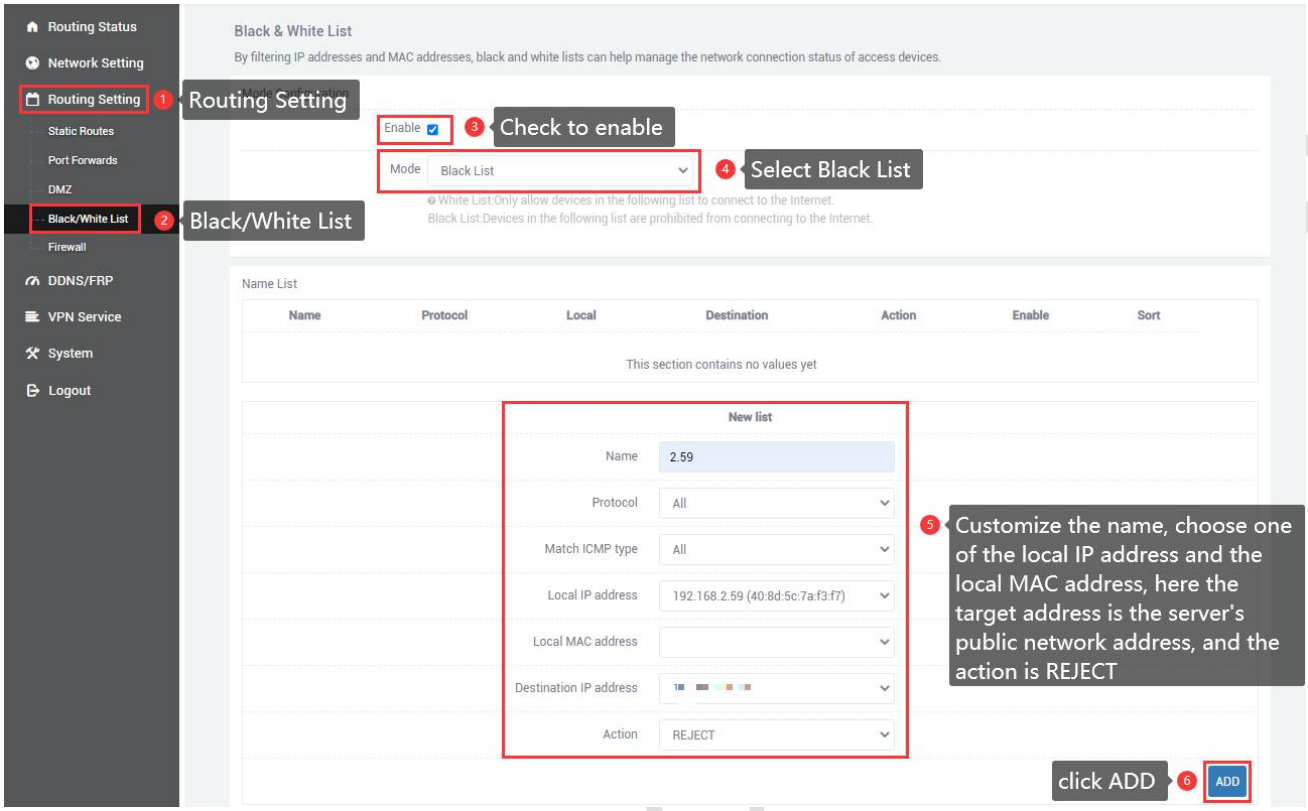
C.Match ICMP type: All types are selected by default, choose according to your needs.

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.

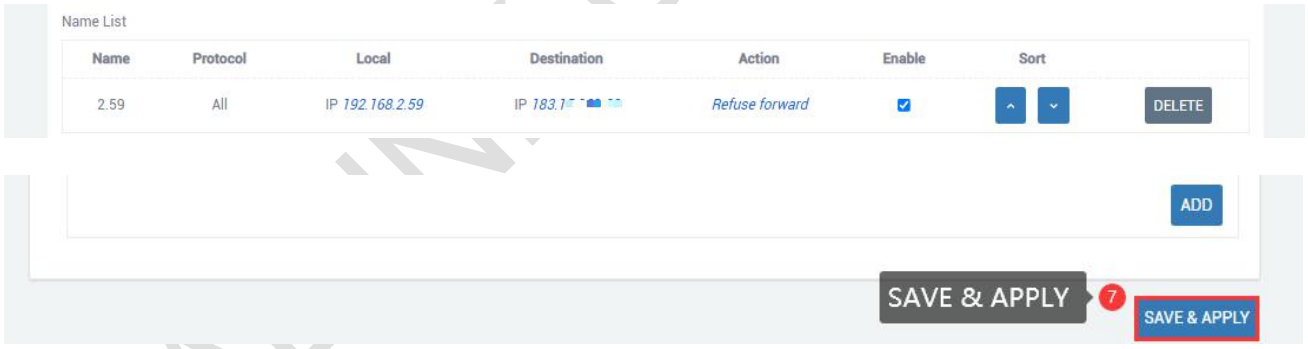
E.Local MAC address:The MAC address of the device added to the blacklist will not be invalid even if the device IP address is changed.

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.

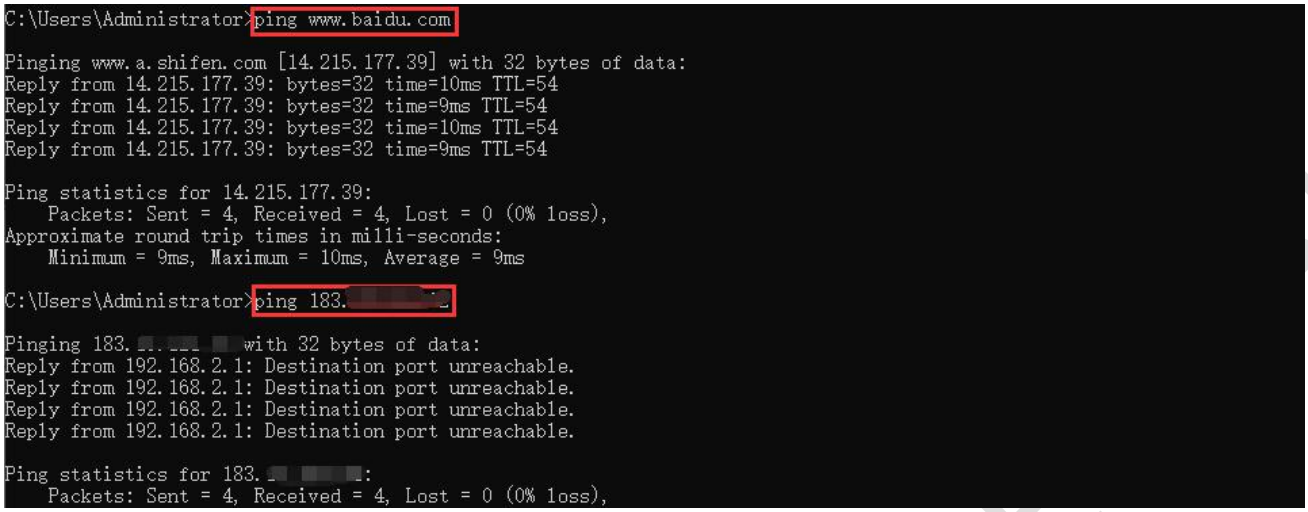
G.Action: Blacklist mode select REJECT.



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.



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".

4.5 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".

4.5.1 Connect to Frps

Preparation before configuration:

(1)One public network server.

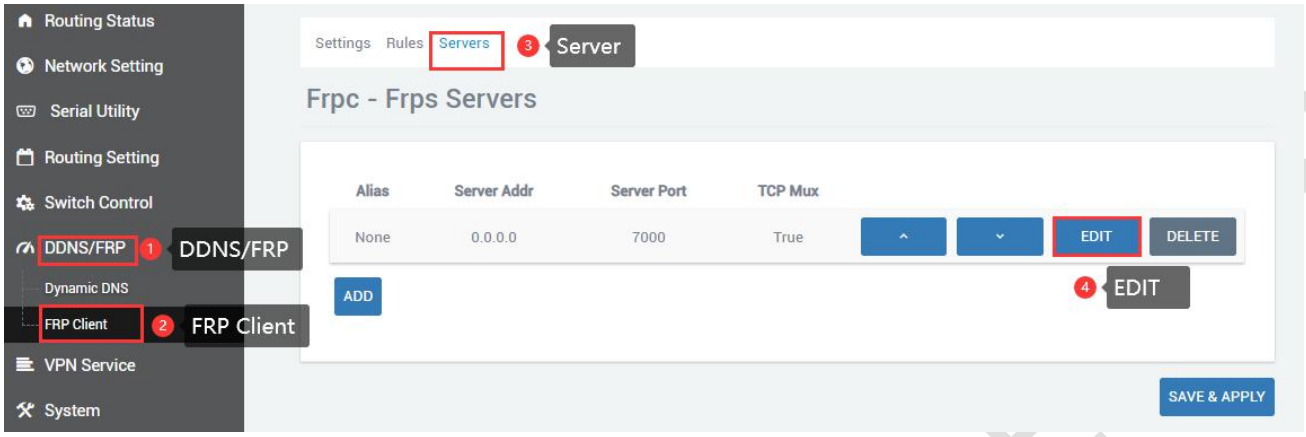
(2)One router (a router that supports frp, that is, 1 intranet server).

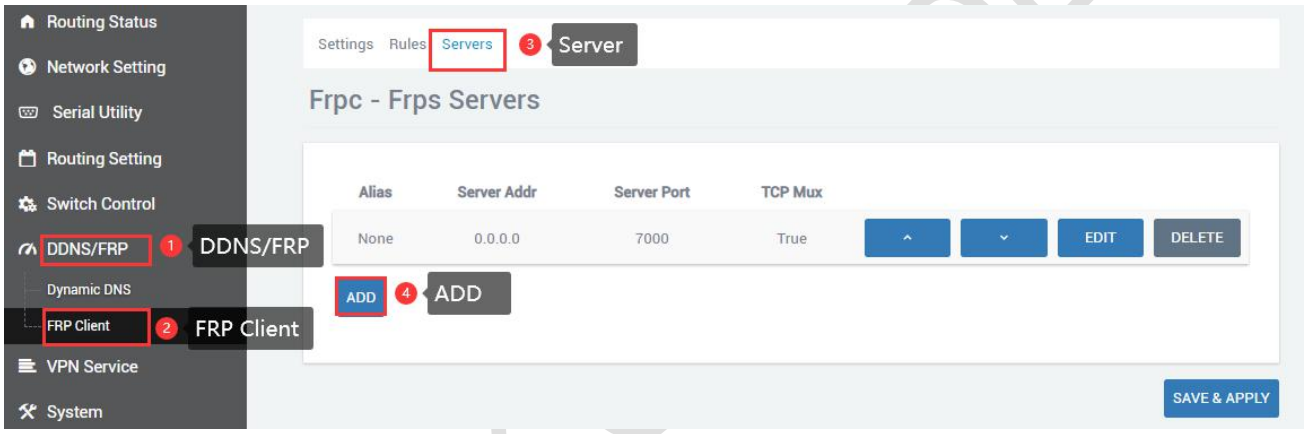
(3)One domain name is bound to the public network server.

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.

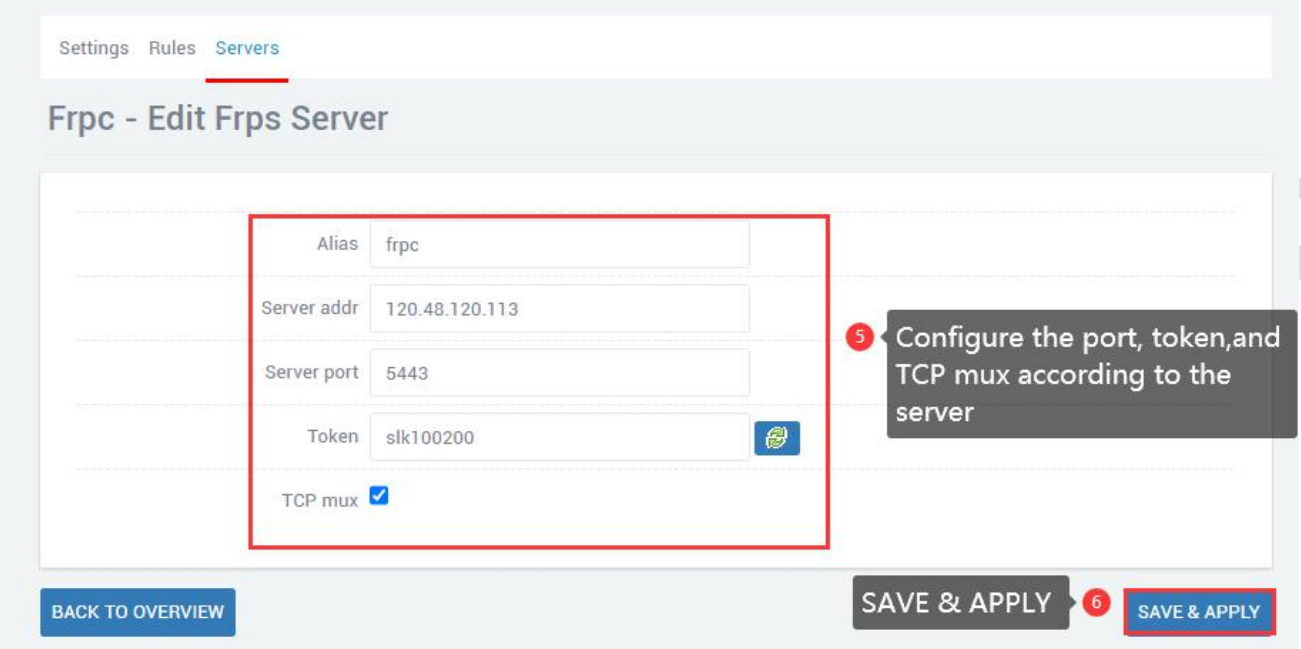
B.Server addr: The address of the server (usually the public IP address).

C.Server port: The port set by the server.

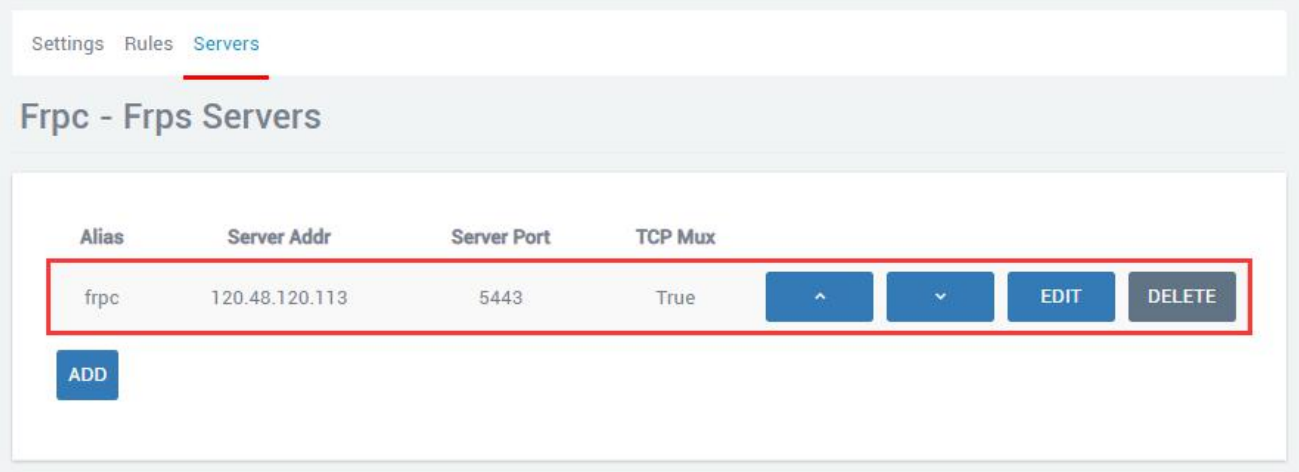
D.Token: The password set by the server.

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 frp server, click "SAVE & APPLY" to start the server.



(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.

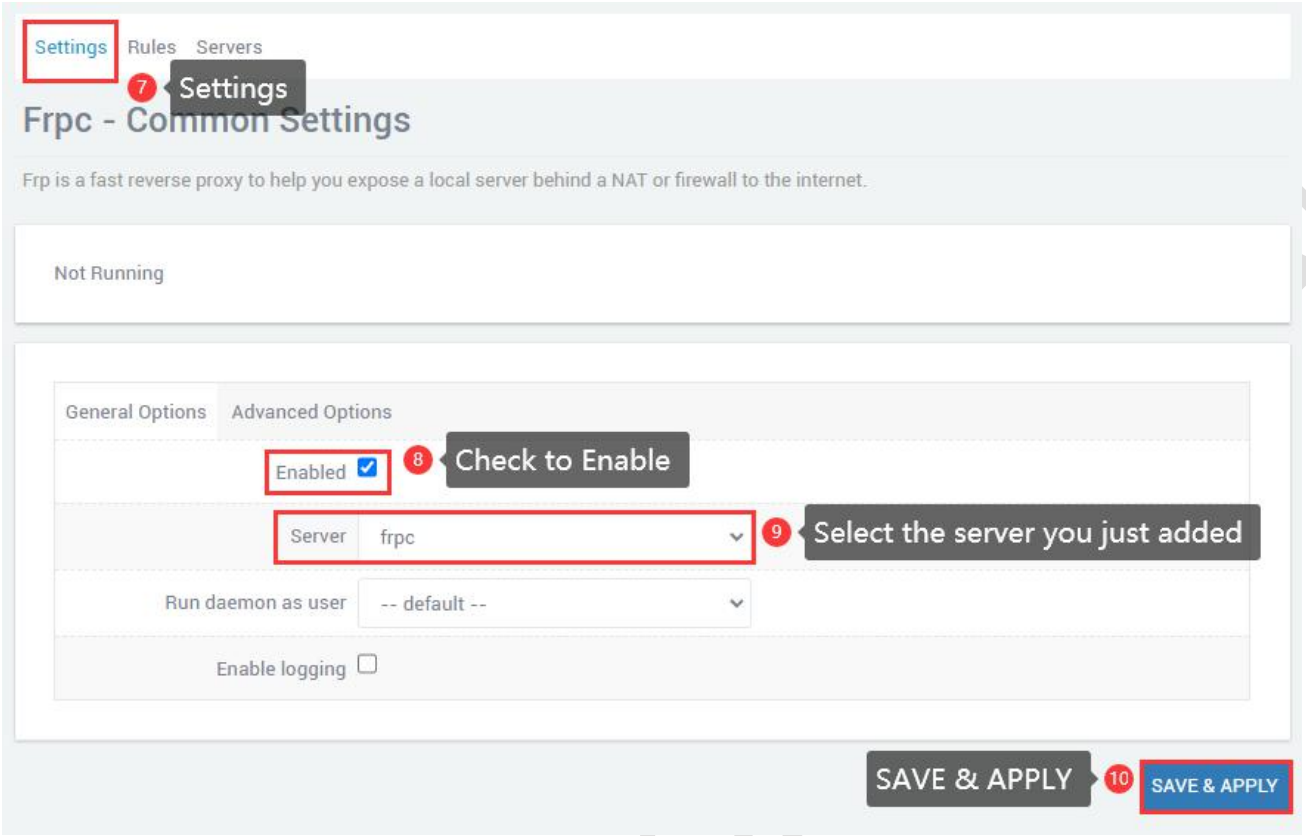
A.Enable: Tick Enabled.

B.Server: The server alias you just customized.

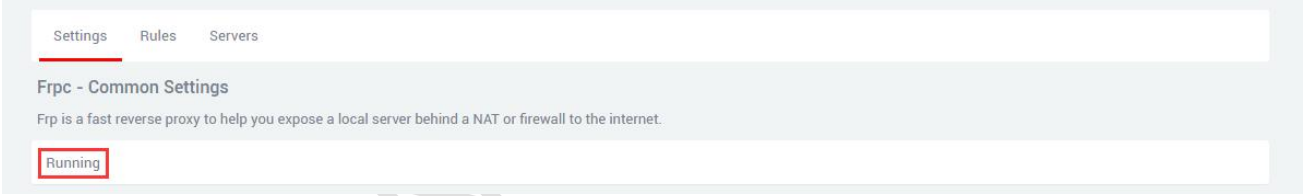
C.Run daemon as user: Generally choose the default, you can modify it according to your needs.

D:Enable logging: Tick as required.

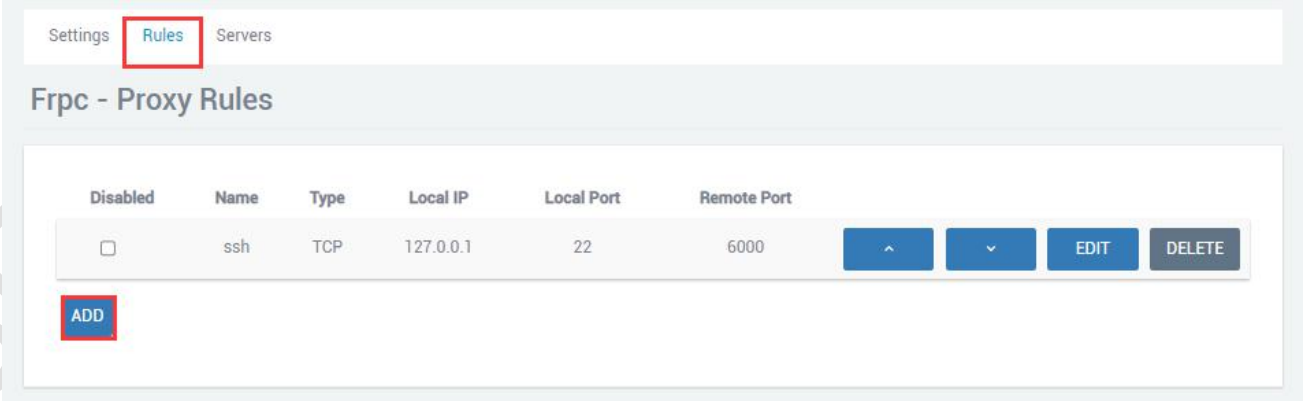
E:After the configuration is complete, click "SAVE & APPLY".



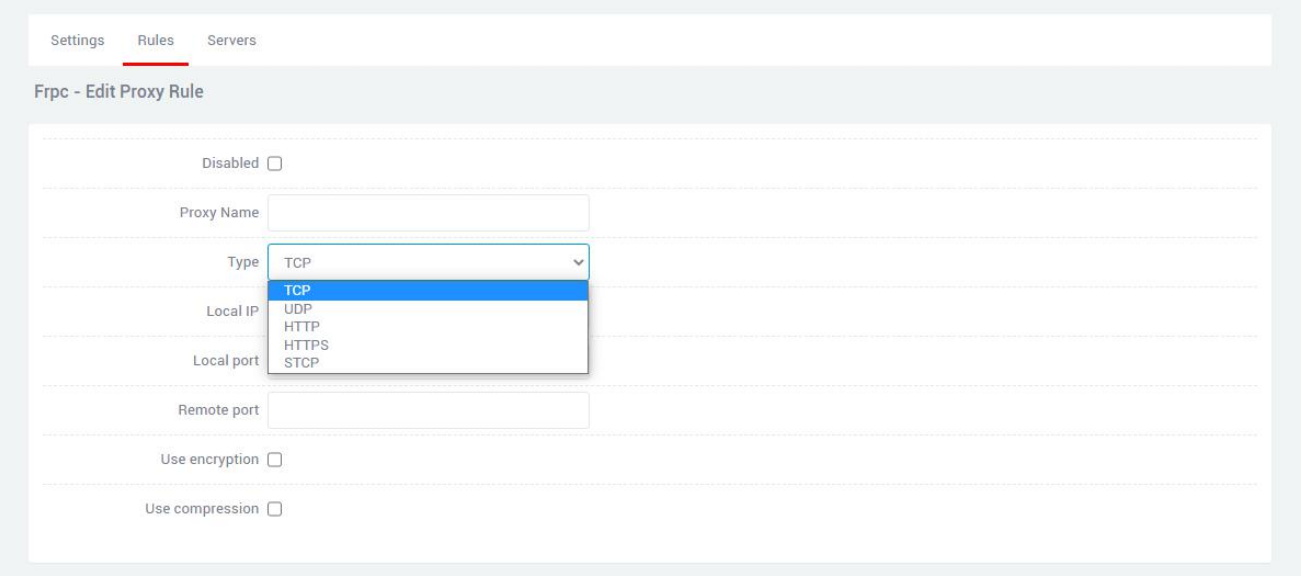
Displaying that the service is running indicates that the frp client has been successfully started.



(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.



4.5.2 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.

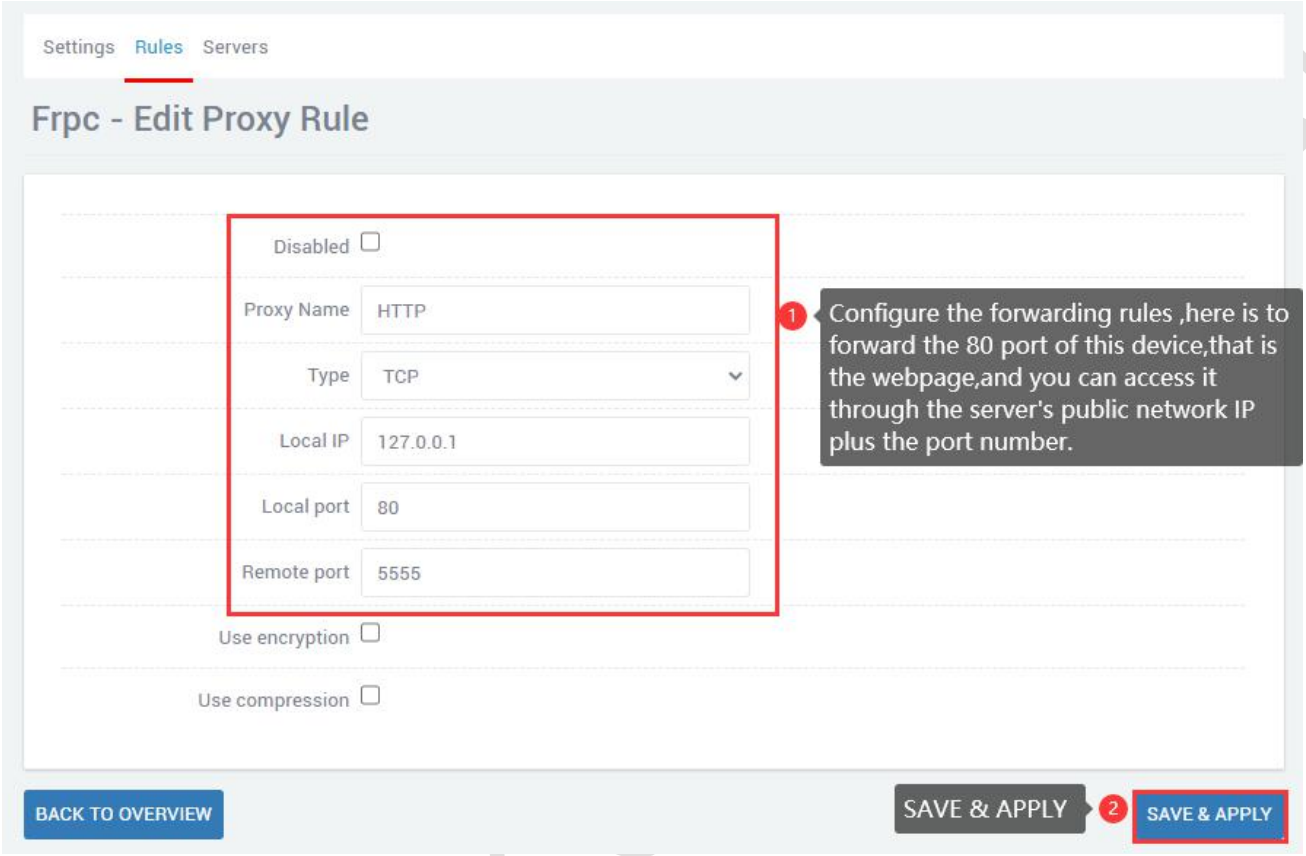
D:Local IP: Fill in the ip of the local machine or the ip allocated by the lan port of the local machine for the connected device. (The ip address of the device that needs to be accessed through the public network).

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

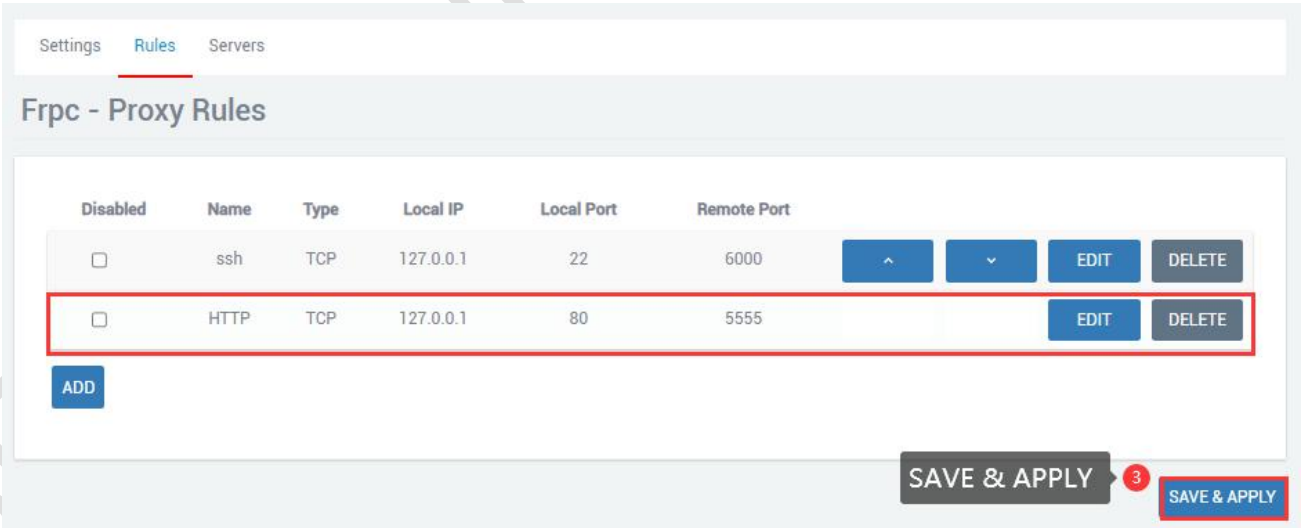
F.Remote port: Add this remote port to the public network address to access the local port opened by the corresponding local device. This port number should not be the same as other rules, and do not use the occupied port, otherwise this rule will not take effect.

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

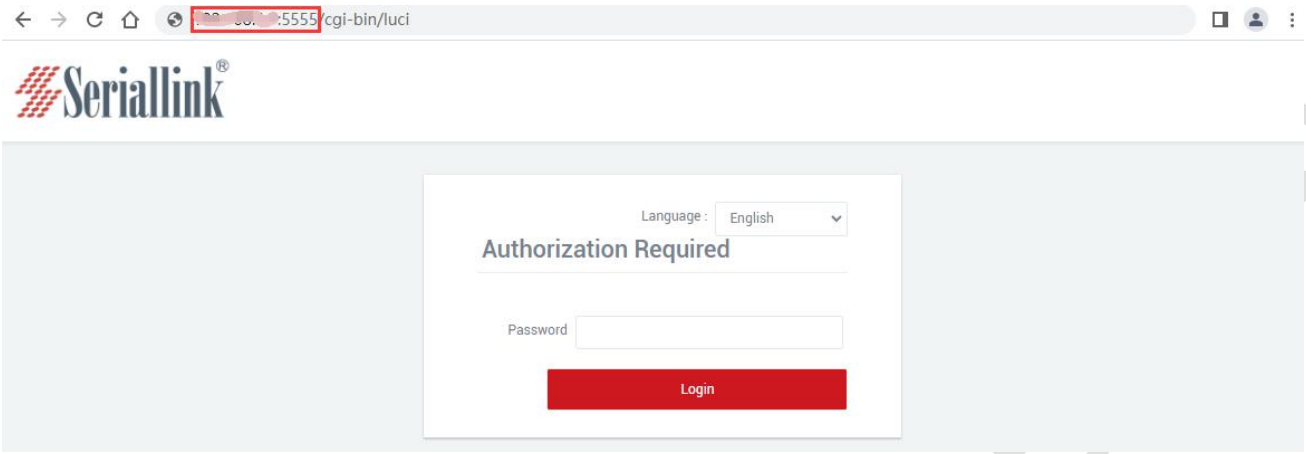
Multiple rules can be added, as long as the remote port numbers do not conflict.
After the configuration is complete, click "SAVE & APPLY".



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.

4.5.3 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.

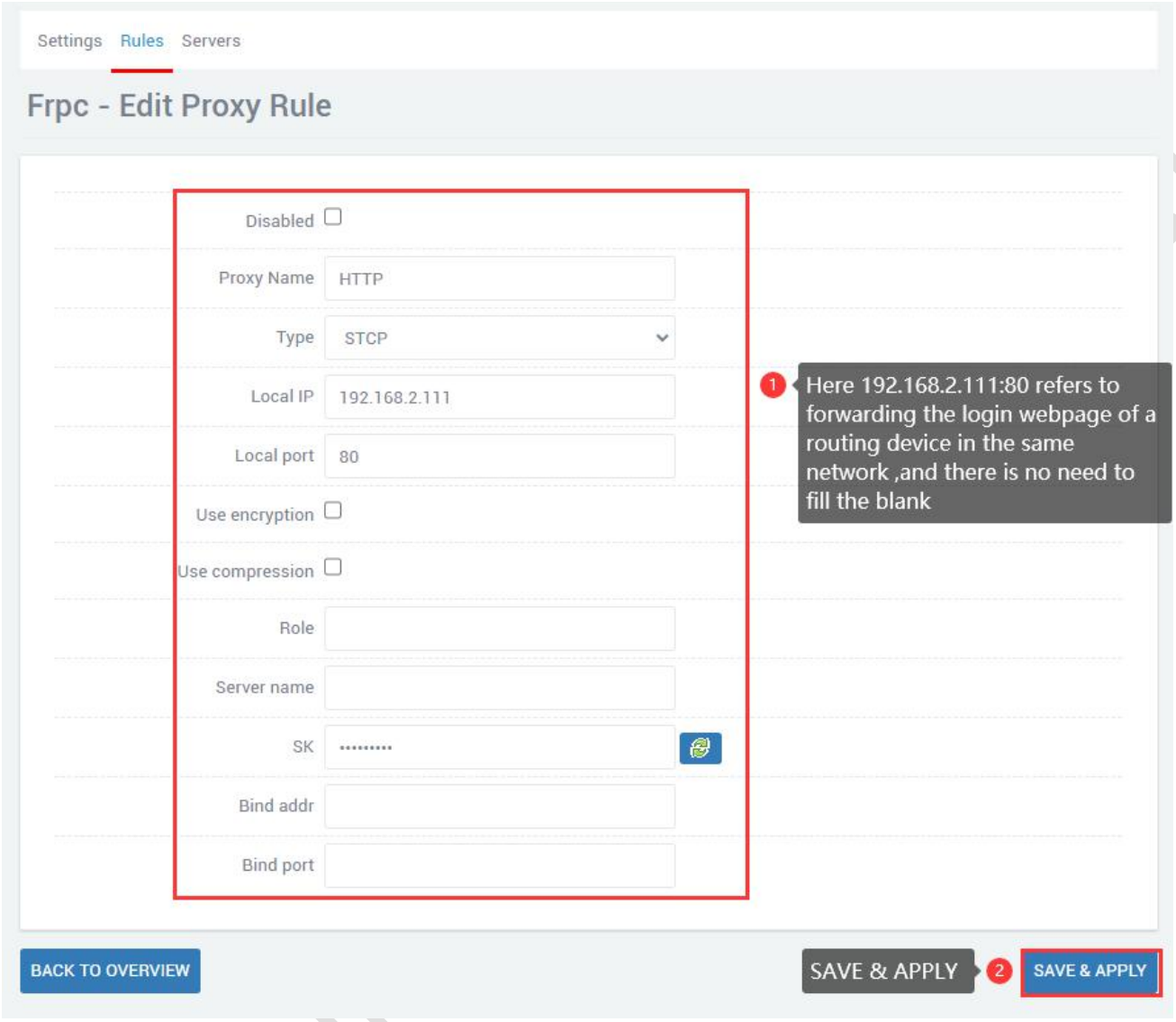
D.Local IP: The IP address assigned by the local device or the lan port to the connected device.

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

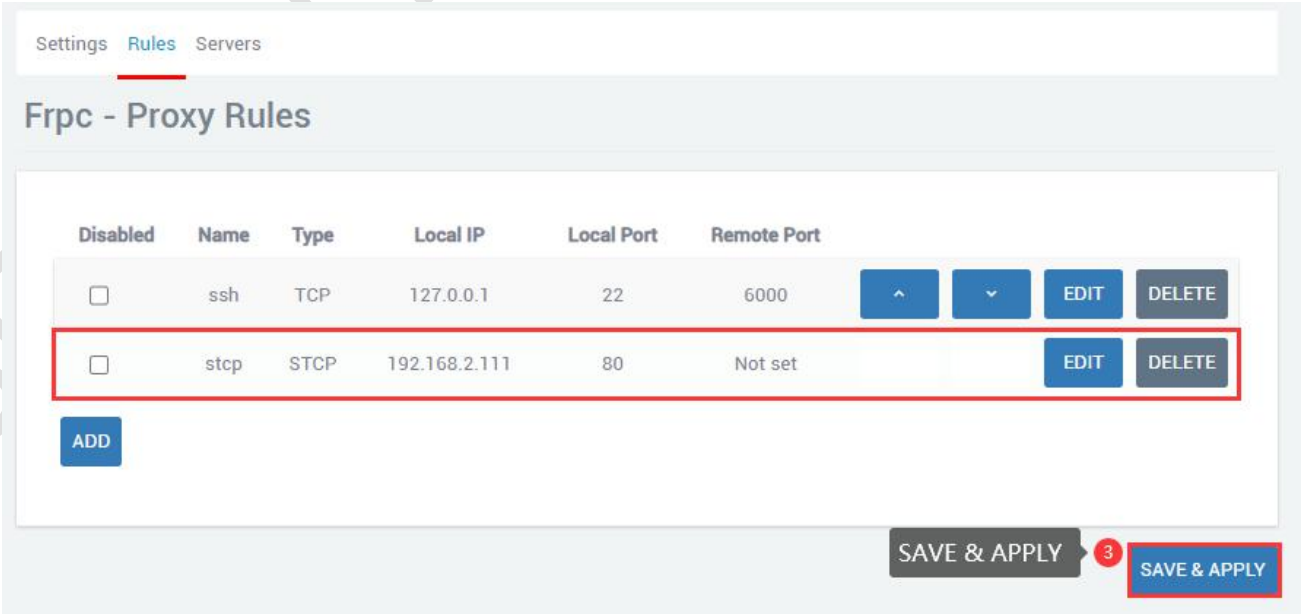
F.SK: Set a password, the access terminal needs to enter the SK set here when accessing the device.

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

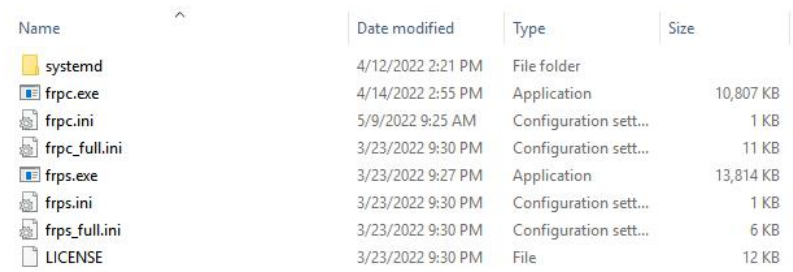
H.Role,Server name,Bind addr,Bind port:These four as clients do not need to be set.



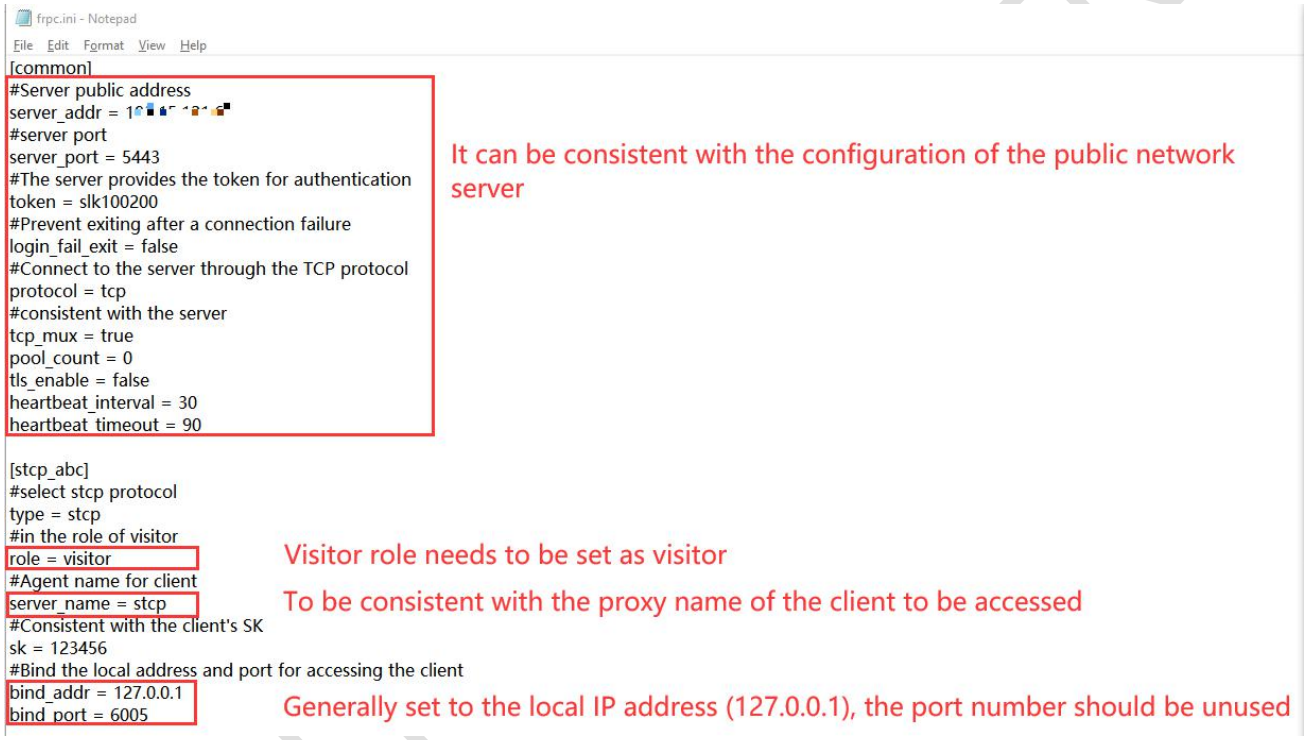
After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.



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 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



```
frpc.ini - Notepad
File  Edit  Format  View  Help
[common]
#Server public address
server_addr = 1[redacted]
#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
```

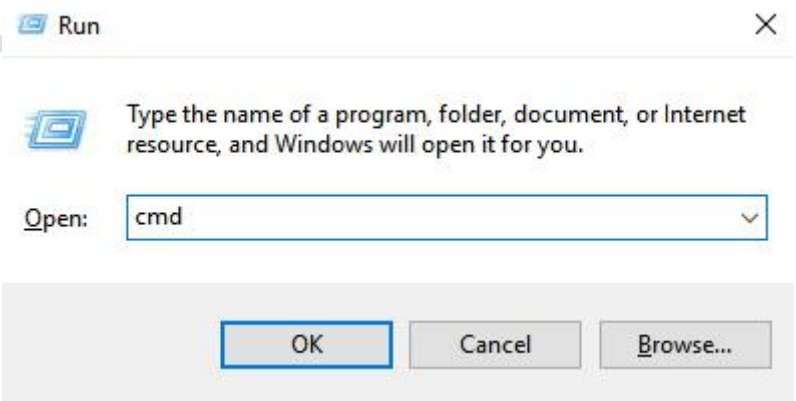
It can be consistent with the configuration of the public network server

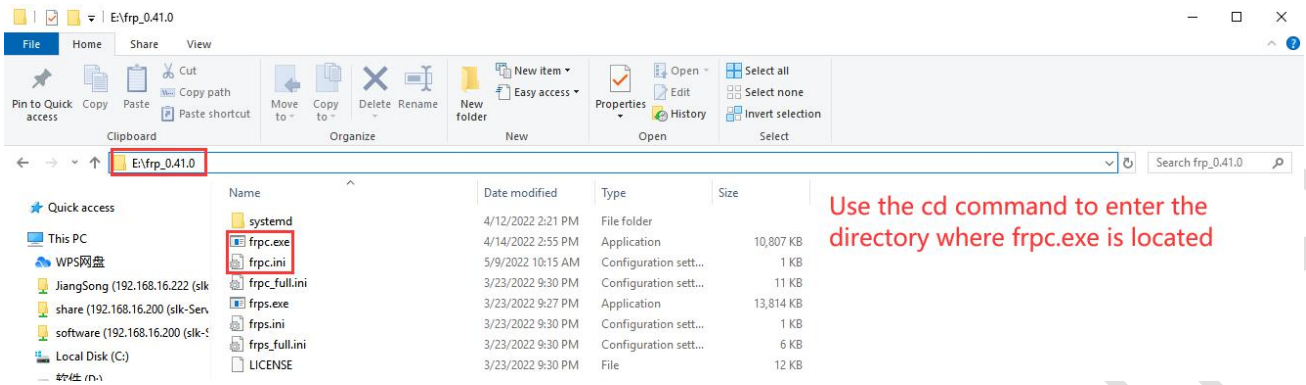
Visitor role needs to be set as visitor

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

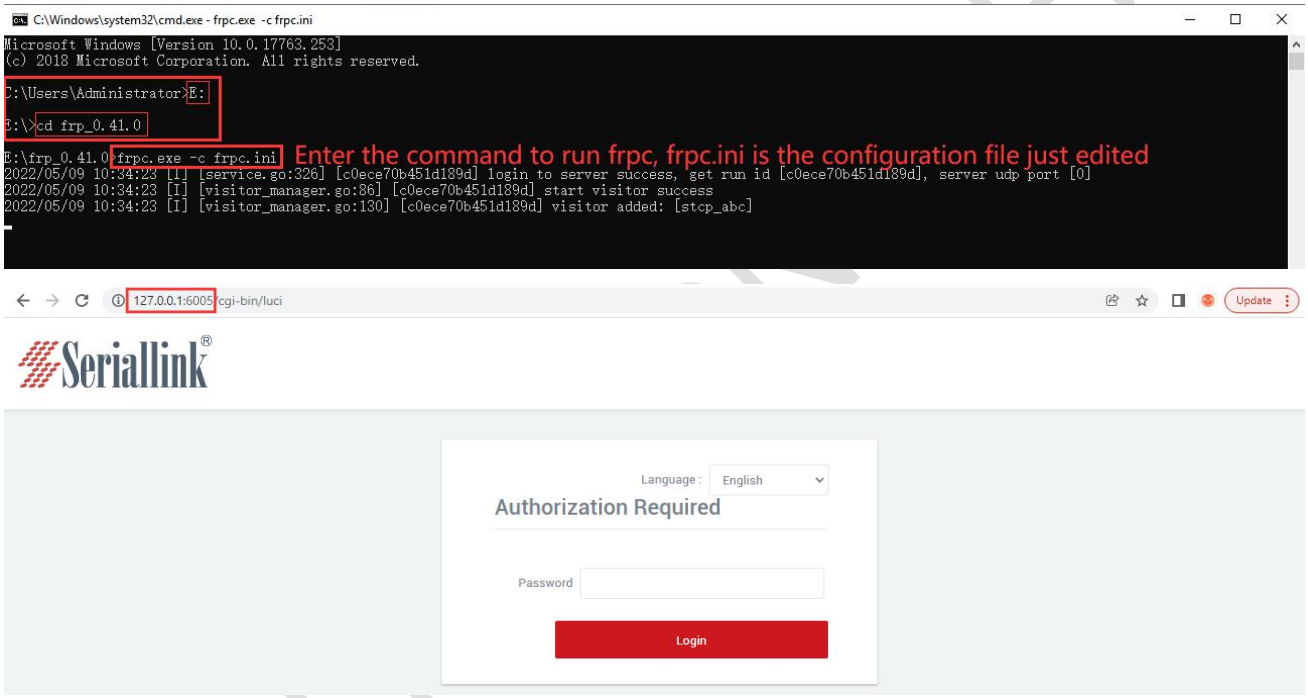
Generally set to the local IP address (127.0.0.1), the port number should be unused

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.

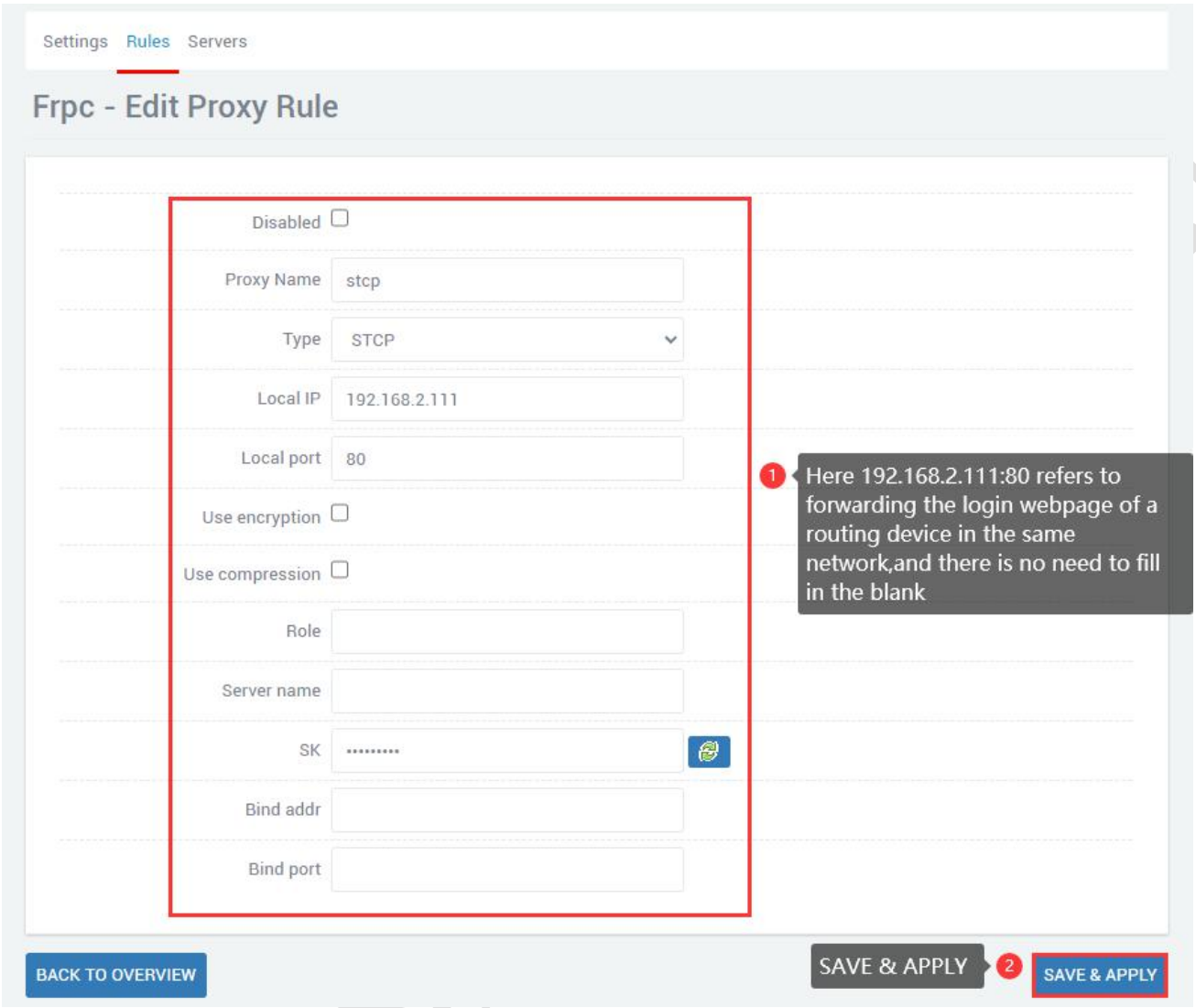
D.Local IP: The IP address assigned by the local device or the lan port to the connected device.

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

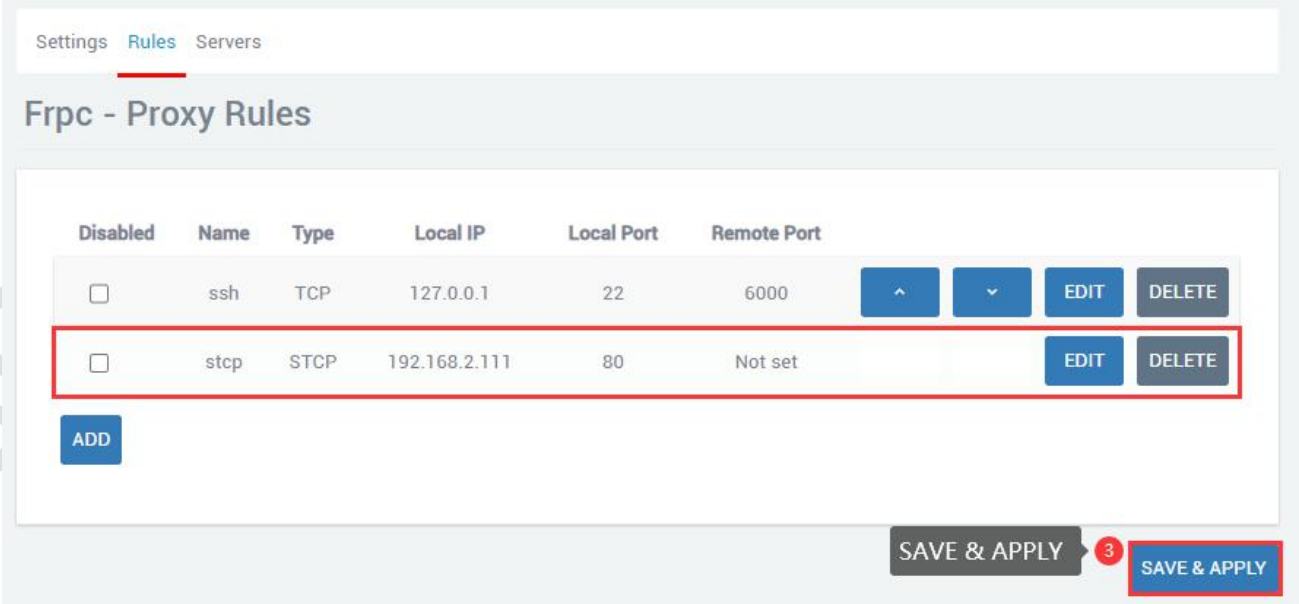
F.SK: Set a password, the access terminal needs to enter the SK set here when accessing the device.

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.

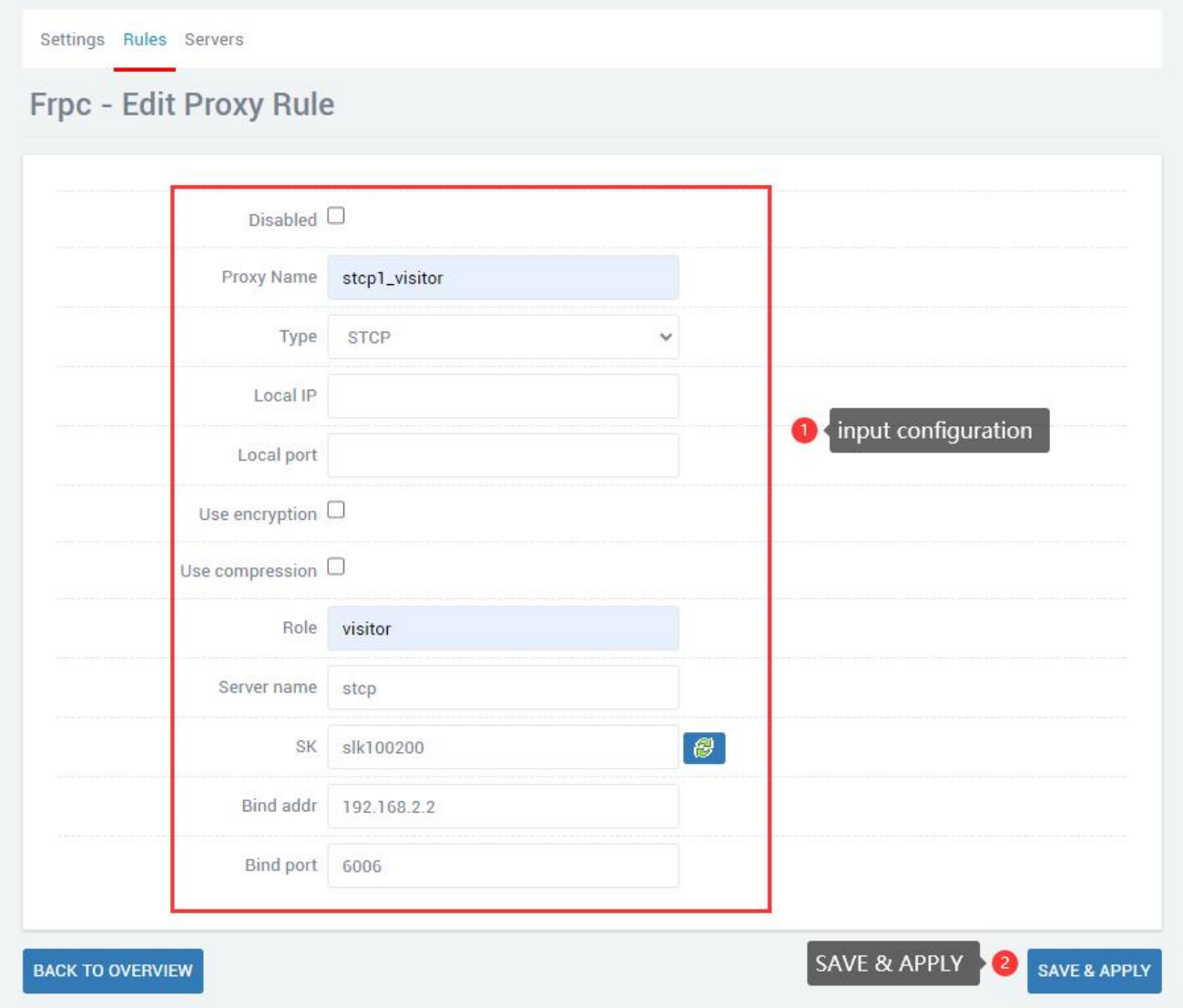
F.SK:Set a password, the access terminal needs to enter the SK set here when accessing the device.

Use encryption,Use compression: Configure as needed.

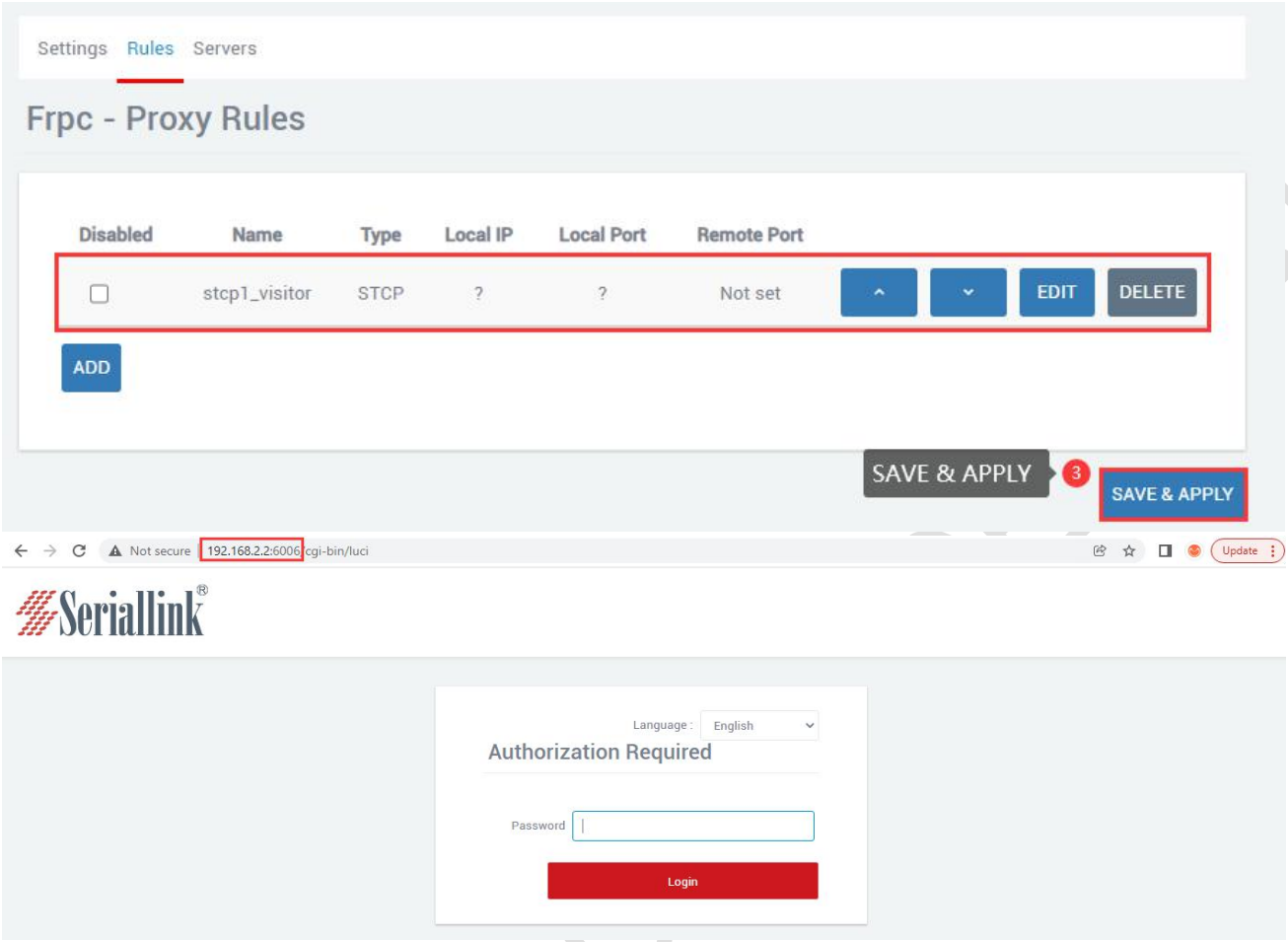
G.Role: The access terminal needs to fill in the visitor.

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.



4.5.4 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.

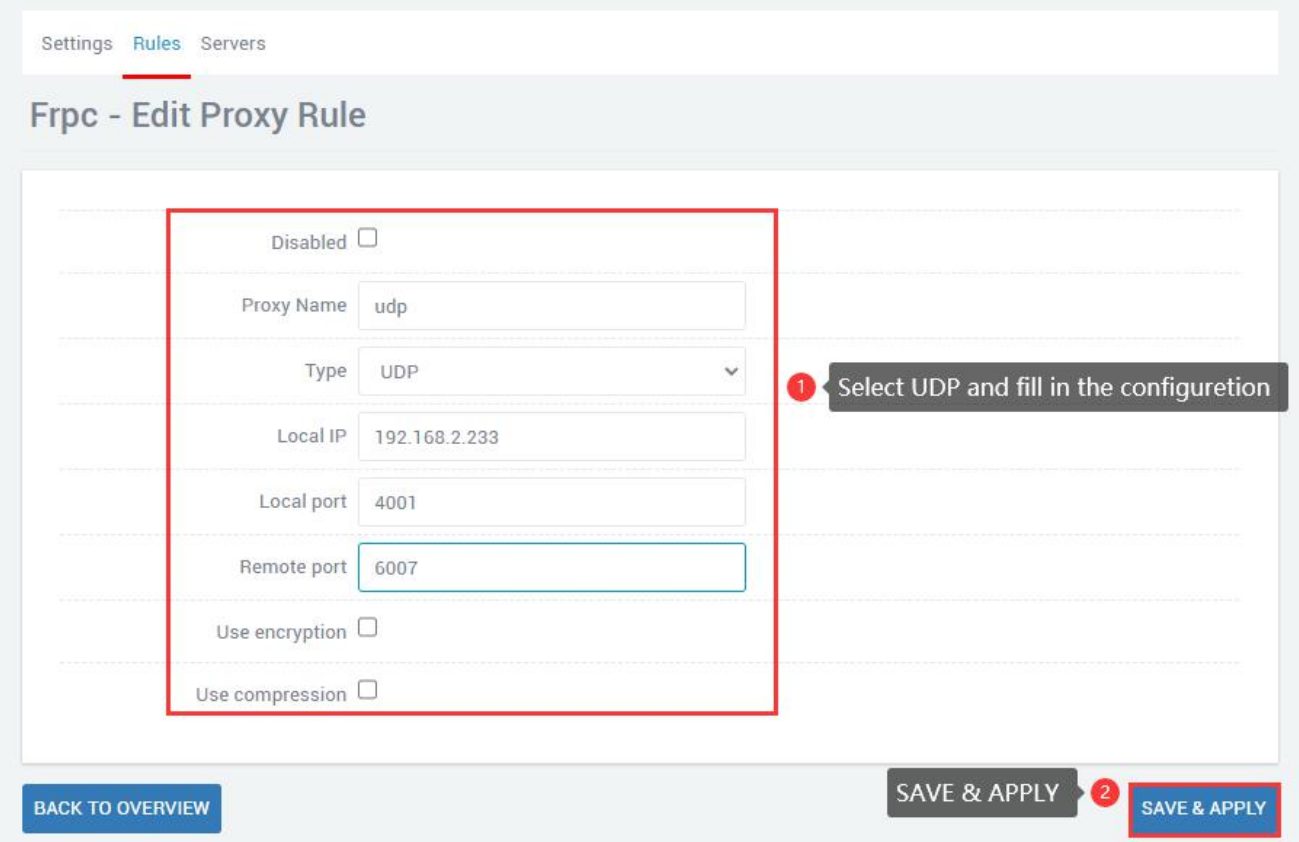
D.Local IP: Fill in the ip of the machine or the ip assigned by the lan port of the machine for the connected device (the ip address of the device that needs to be accessed through the public network).

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.

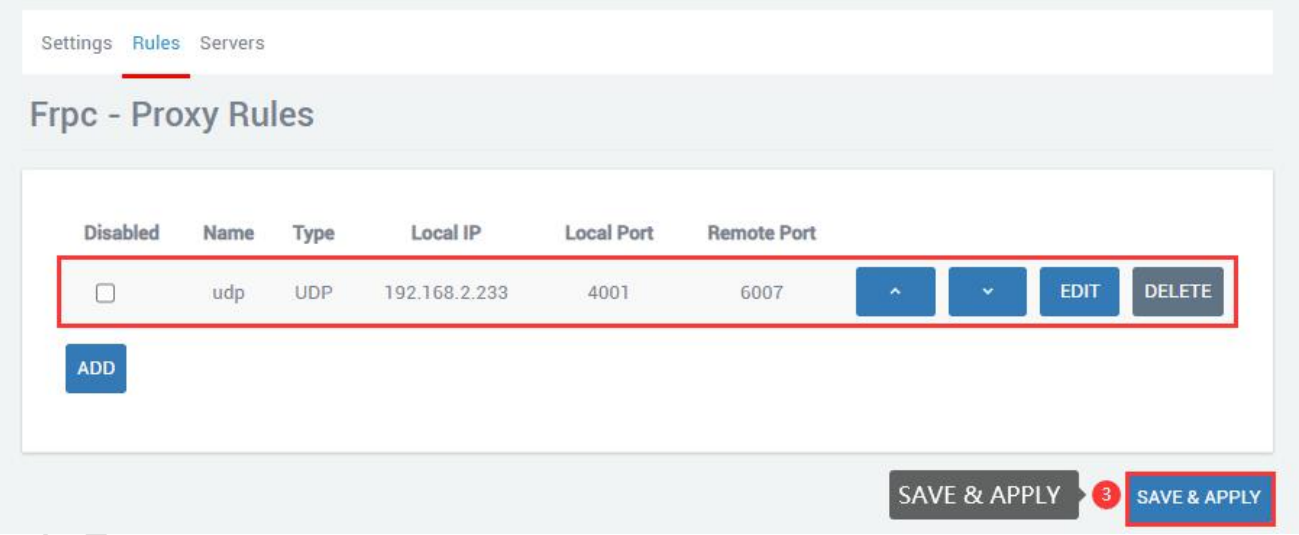
F.Remote port: Add this remote port to the public network address to access the local port opened by the corresponding local device. This port number should not be the same as other rules, and do not use the occupied port, otherwise this rule will not take effect.

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

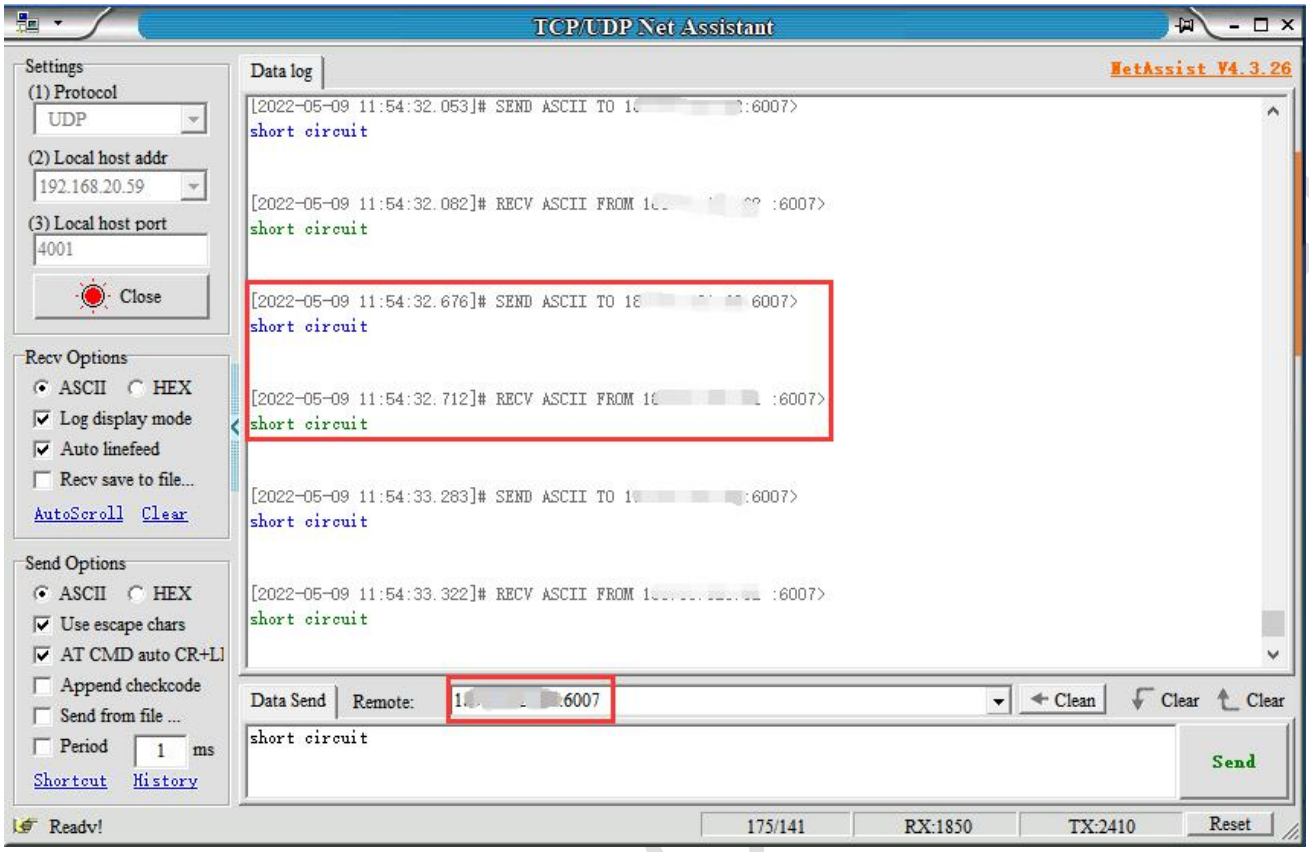
H.Multiple rules can be added, the remote port and proxy name should not conflict, and click "SAVE & APPLY" after the configuration is complete.



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).



4.5.5 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.

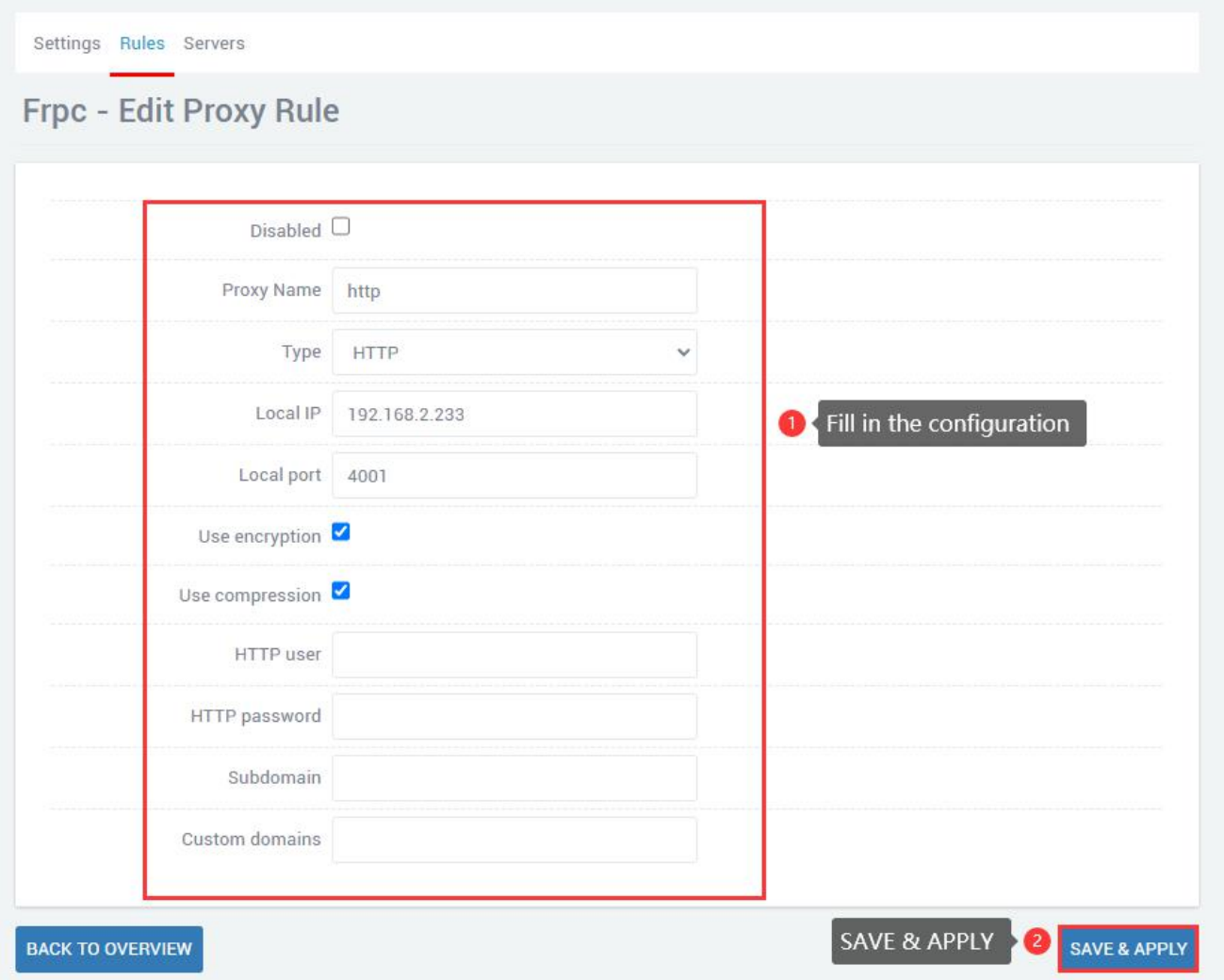
D.Local IP: Fill in the ip of the machine or the ip assigned by the lan port of the machine for the connected device (the ip address of the device that needs to be accessed through the public network).

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.

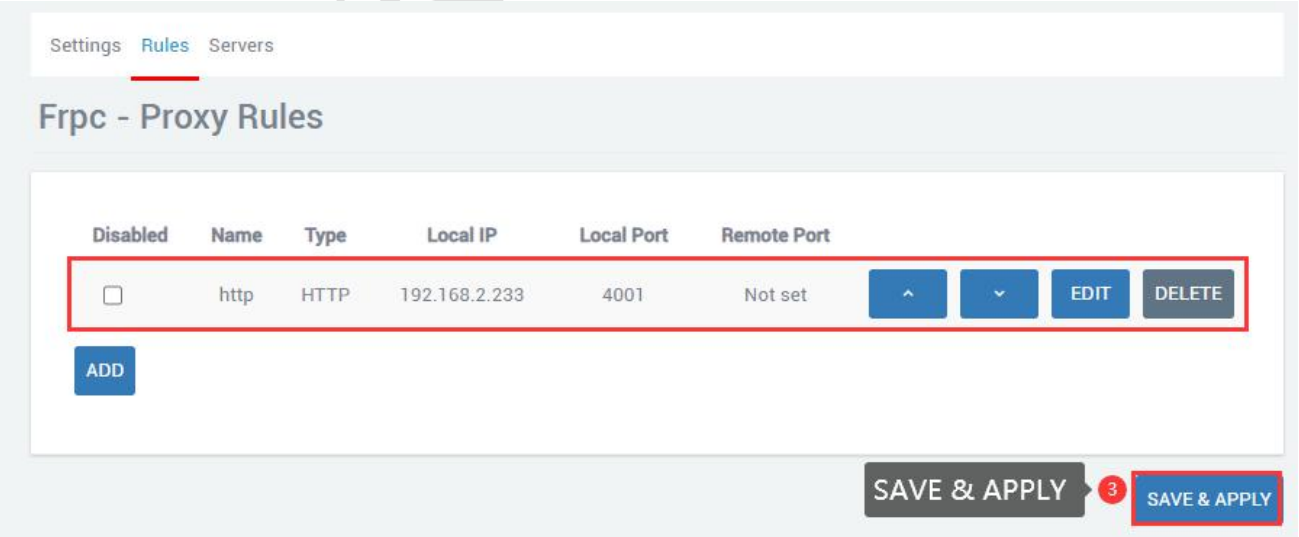
F.Use encryption,Use compression,HTTP user,HTTP password: These four are selected as needed.

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.

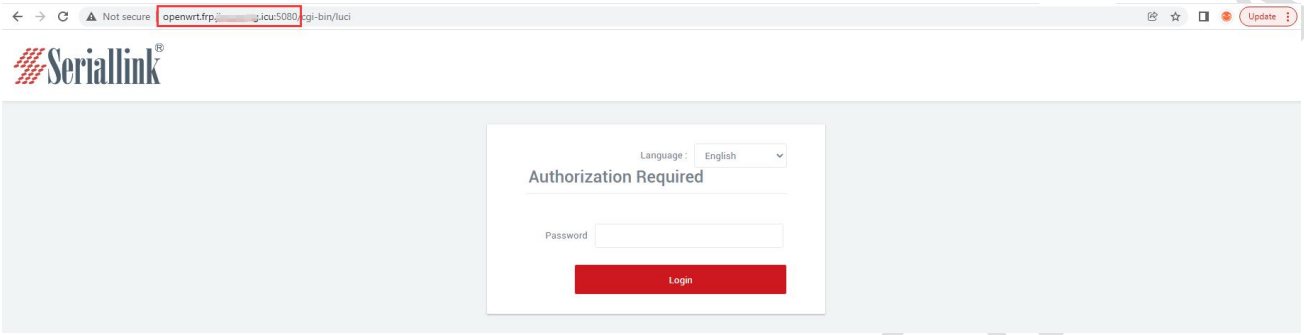


After generating a new rule, you need to click "SAVE & APPLY" to make the rule take effect.



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.



4.6 1:1 NAT

The specified address performs one-to-one mapping. In the navigation bar, "Route Settings" - "1:1 NAT" can establish a one-to-one correspondence between external addresses and internal addresses.

Enable: Check Enable to make it take effect.

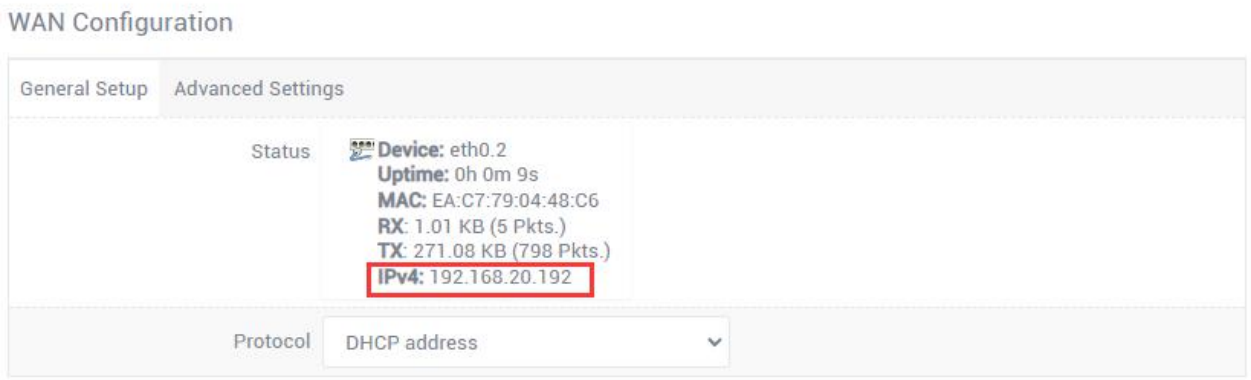
External interface: The external interface that needs to be mapped.

External IP Address: The external interface IP address that needs to be mapped.

Internal IP Address: The IP address of the internal network device.

After the configuration is complete, click "Save & Apply" to make it take effect. After it takes effect, you can directly access the internal network device with 1:1 NAT by accessing the external IP address.

external IP

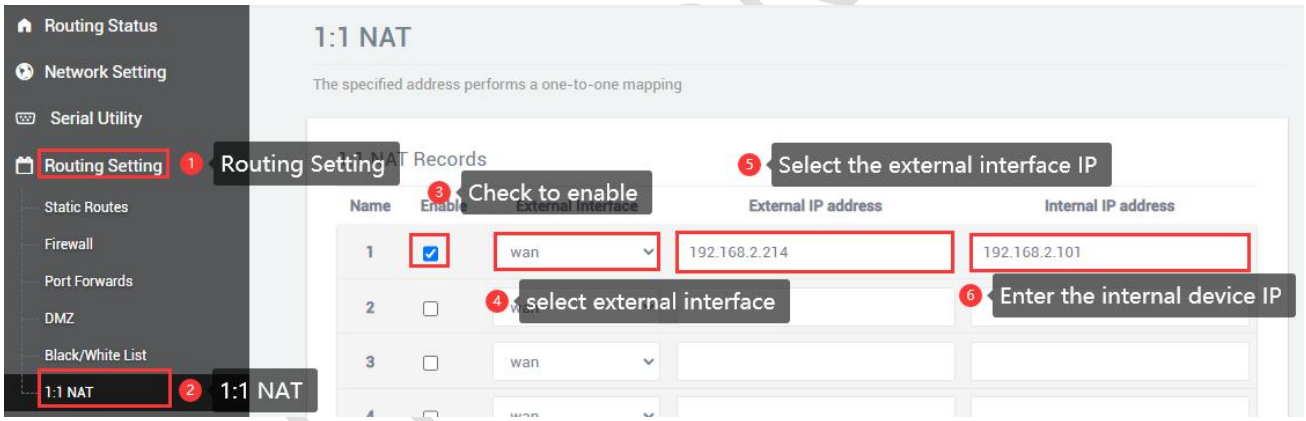


Ping internal network devices:


```
PING 192.168.2.101 (192.168.2.101): 56 data bytes
64 bytes from 192.168.2.101: seq=0 ttl=128 time=0.963 ms
64 bytes from 192.168.2.101: seq=1 ttl=128 time=0.795 ms
64 bytes from 192.168.2.101: seq=2 ttl=128 time=0.753 ms
64 bytes from 192.168.2.101: seq=3 ttl=128 time=0.896 ms
64 bytes from 192.168.2.101: seq=4 ttl=128 time=0.881 ms

--- 192.168.2.101 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.753/0.857/0.963 ms
```

Configure 1:1 NAT:



Click "Save & Apply" to make the configuration take effect. Here, the test can directly access the webpage of route 192.168.2.101 with the external IP address 192.168.20.192

Chapter 5 VPN Service

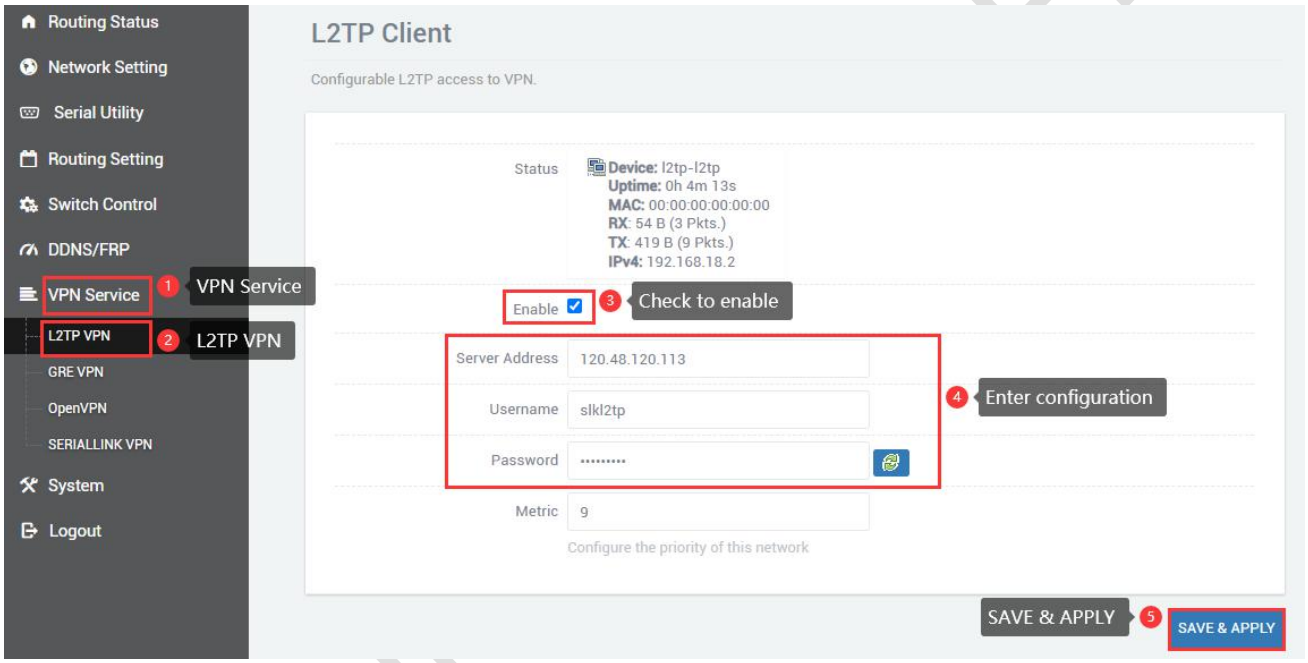
5.1 L2TP VPN

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

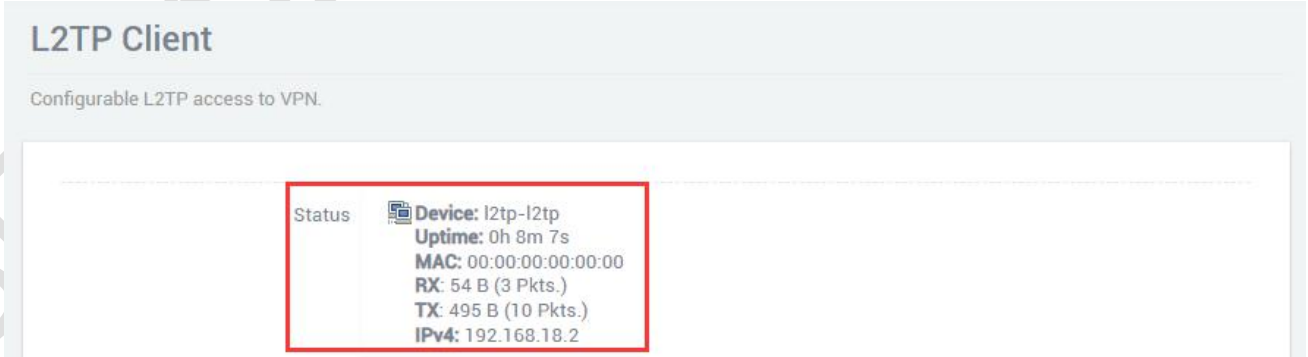
A.Enable: To us e L2TP VPN, you need to check it, and you can just uncheck it when you don't use it.

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

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

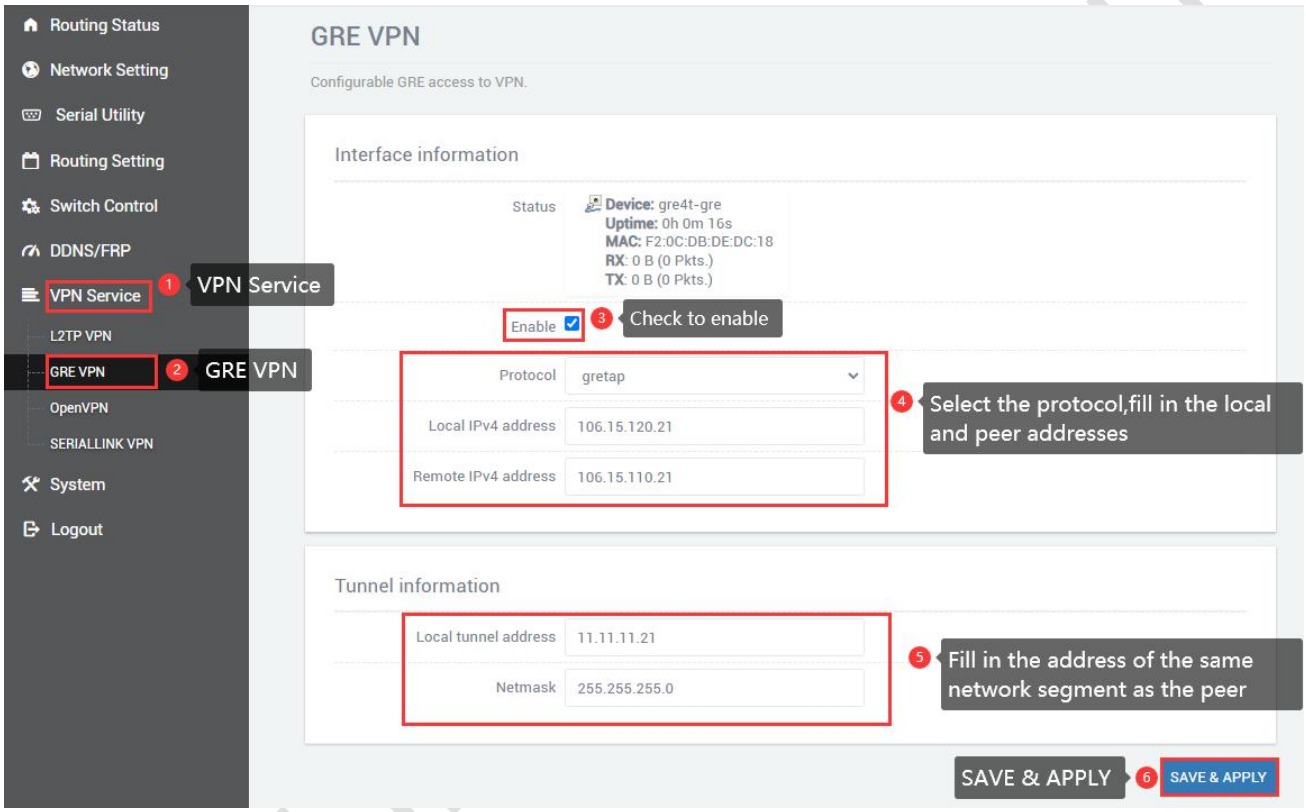


After the connection is successful, the address assigned by the server will appear in the status bar. If l2tp is not used, uncheck it and click "SAVE & APPLY".

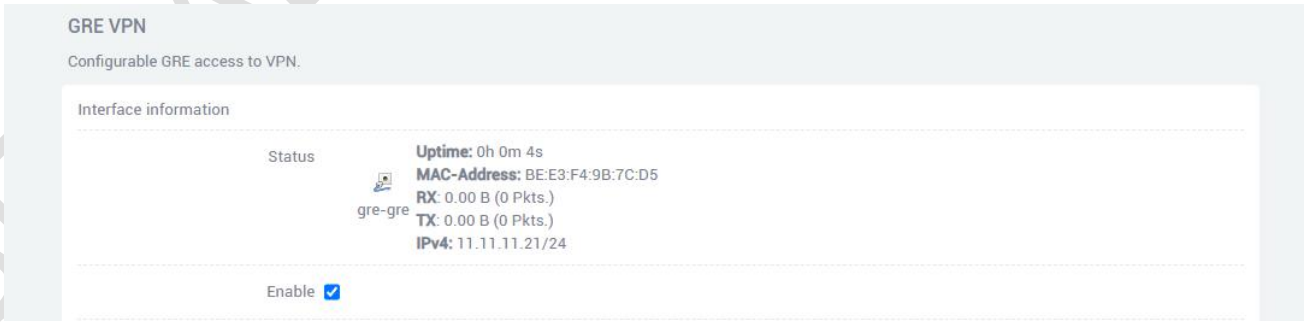


5.2 GRE VPN

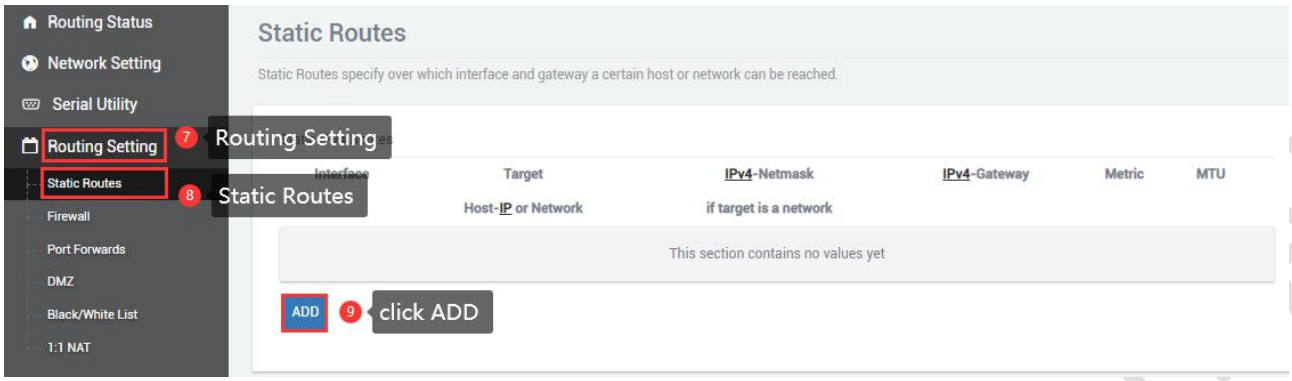
Navigation bar "VPN Service" - "GRE VPN", select Enable, select gretap or gre according to the protocol of the opposite end (keep the protocol at both ends the same). The local IPv4 address and remote IPv4 address are filled in according to the local wan port (public network) address and the peer wan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

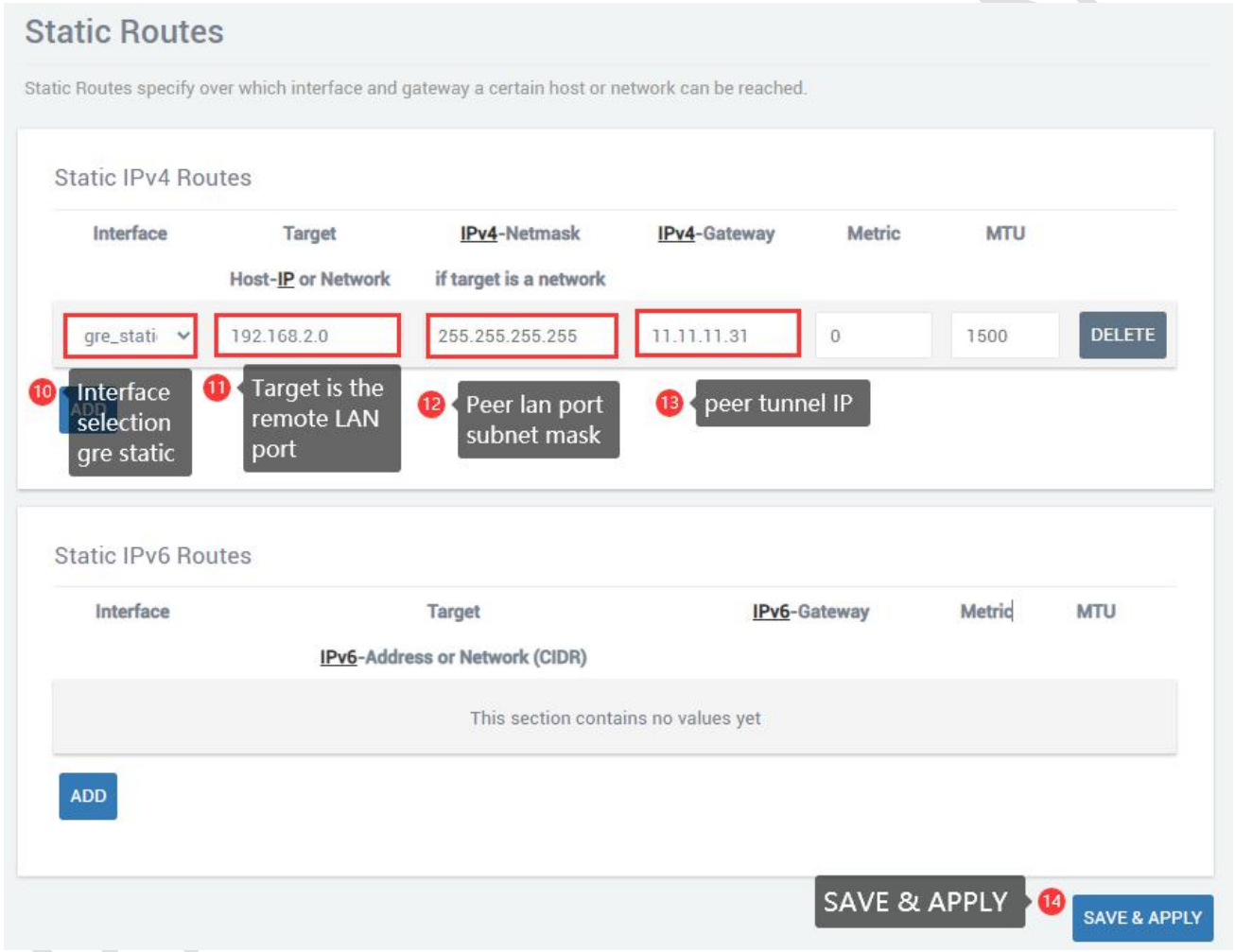


Refresh status information after "SAVE & APPLY".



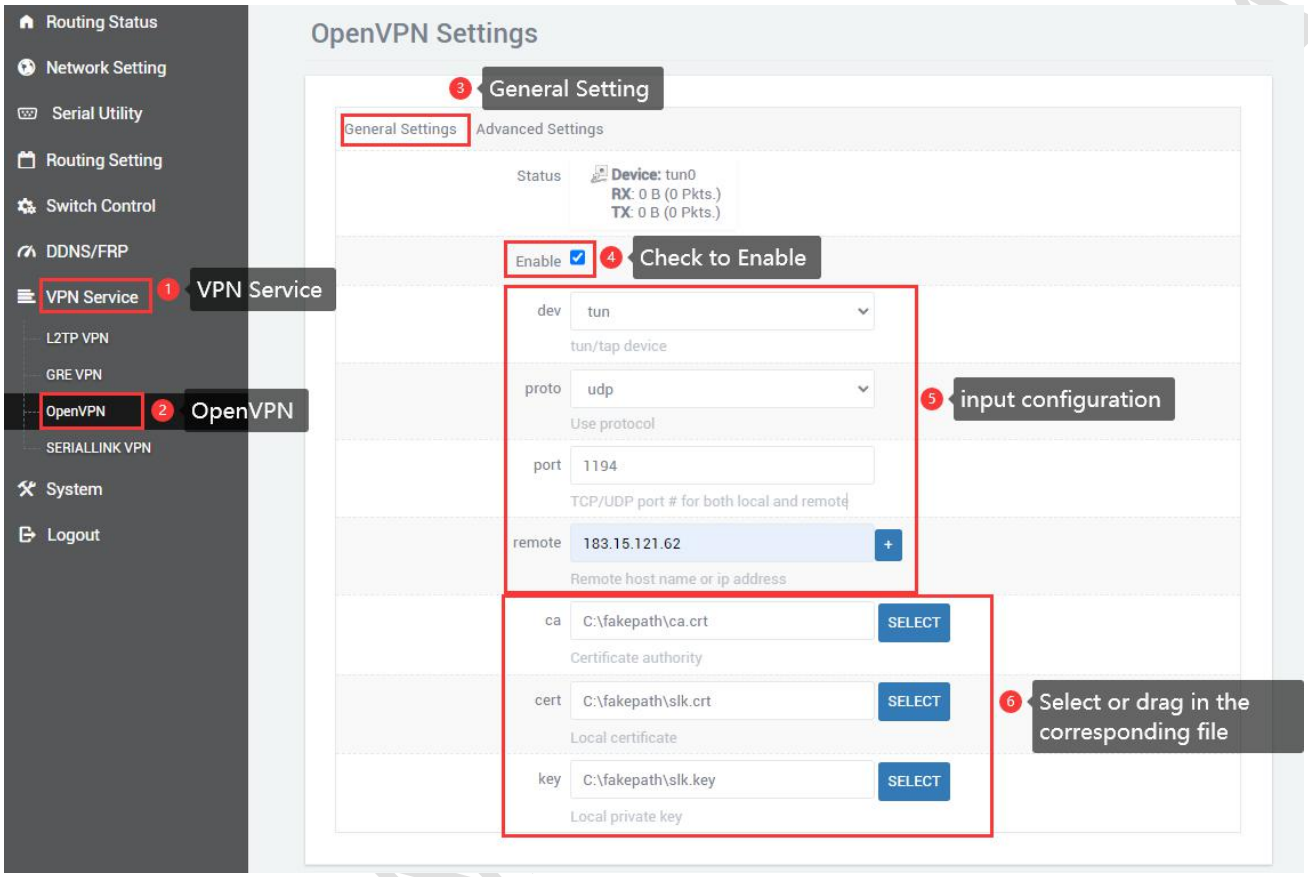
Then add routing table rules, you can successfully access the peer Lan port device.



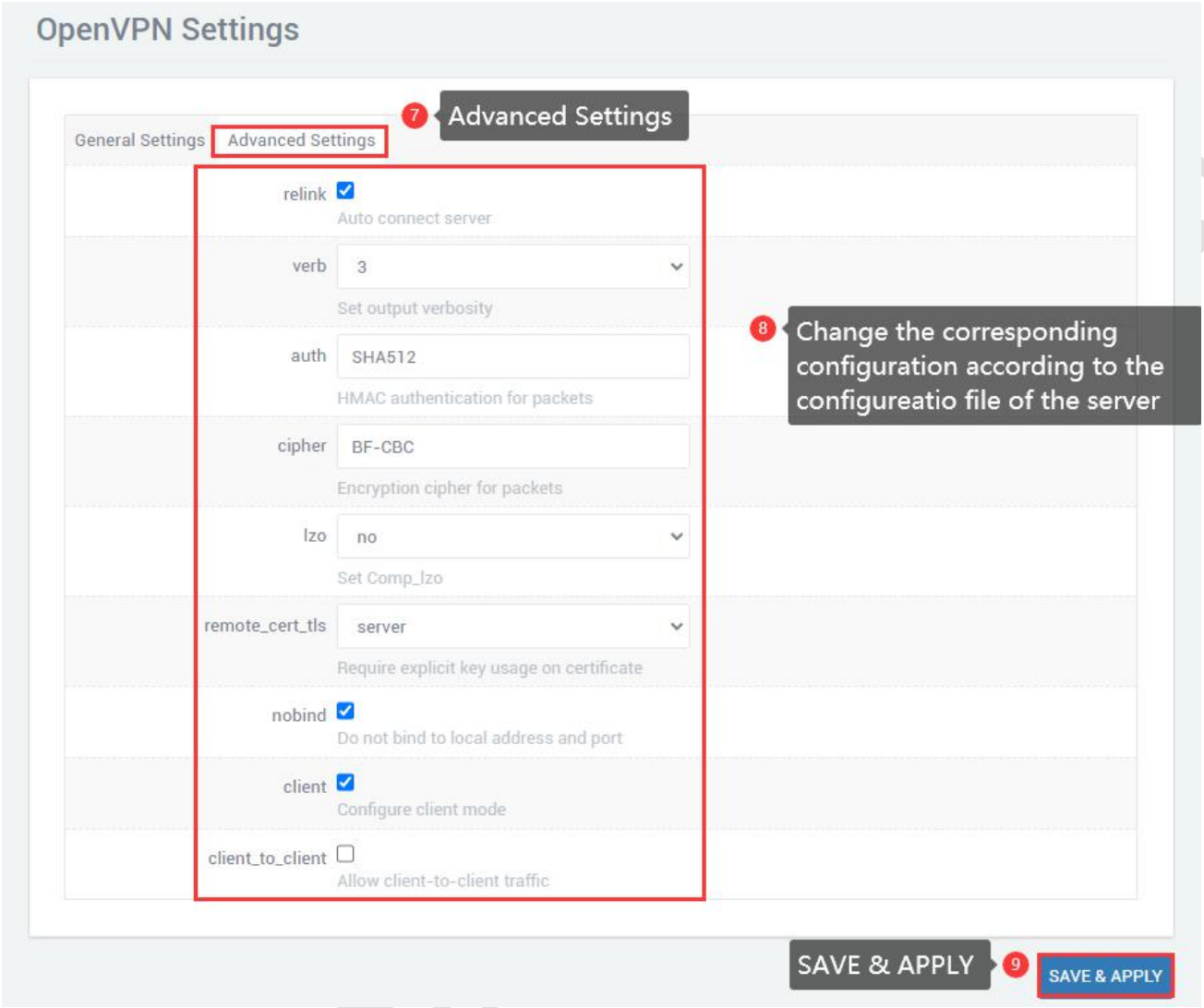


5.3 OpenVPN

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".



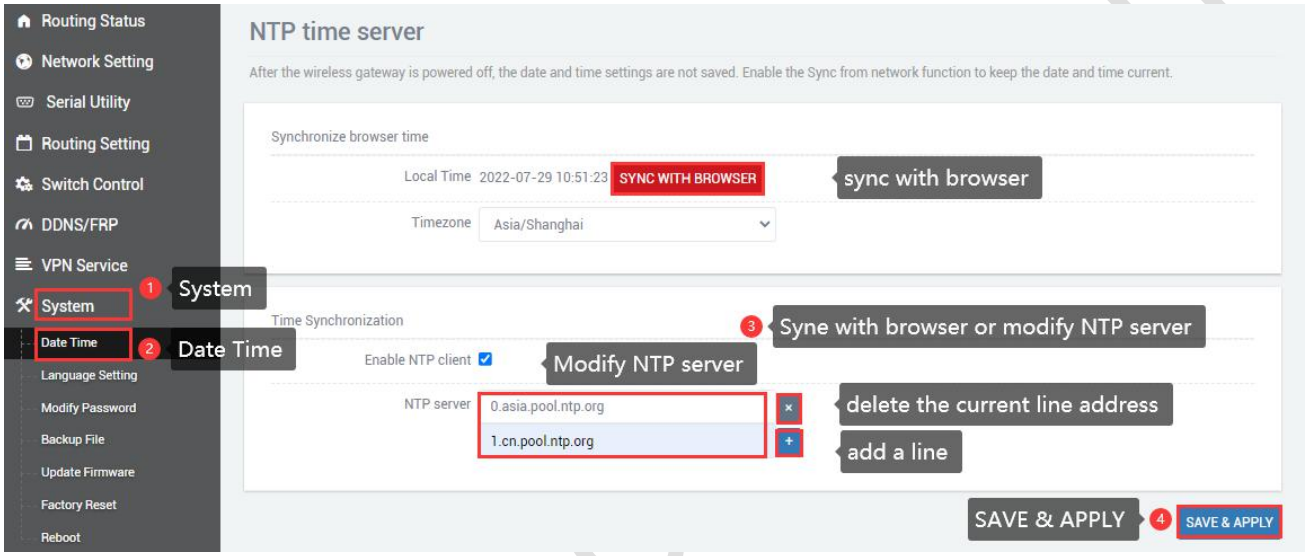
After the connection is successful, the status bar will refresh the address. If openvpn is not used, uncheck it and click "SAVE & APPLY".

Chapter 6 System

6.1 Date Time

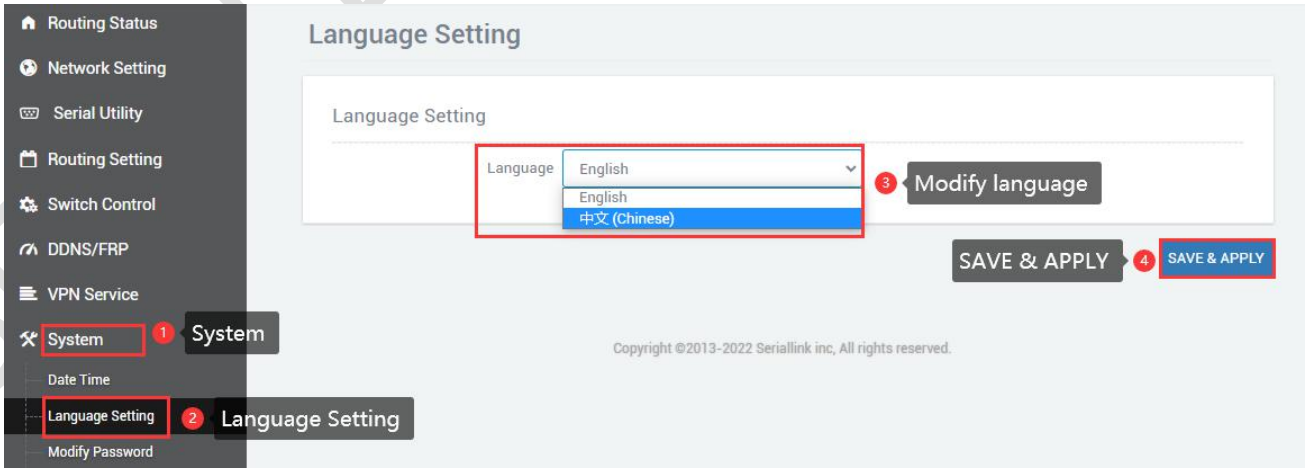
Time synchronization is enabled by default. If necessary, you can change the NTP server to synchronize the time of the server.

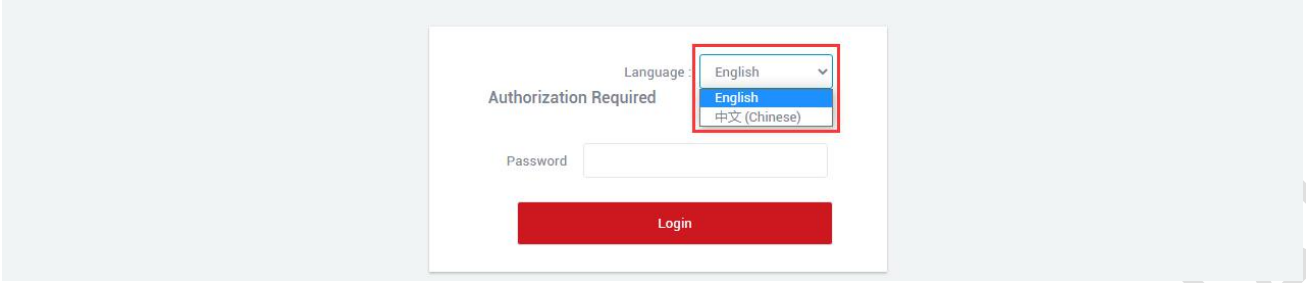
Navigation bar "System" - "Date Time", click "SAVE & APPLY" after setting.



6.2 Language Setting

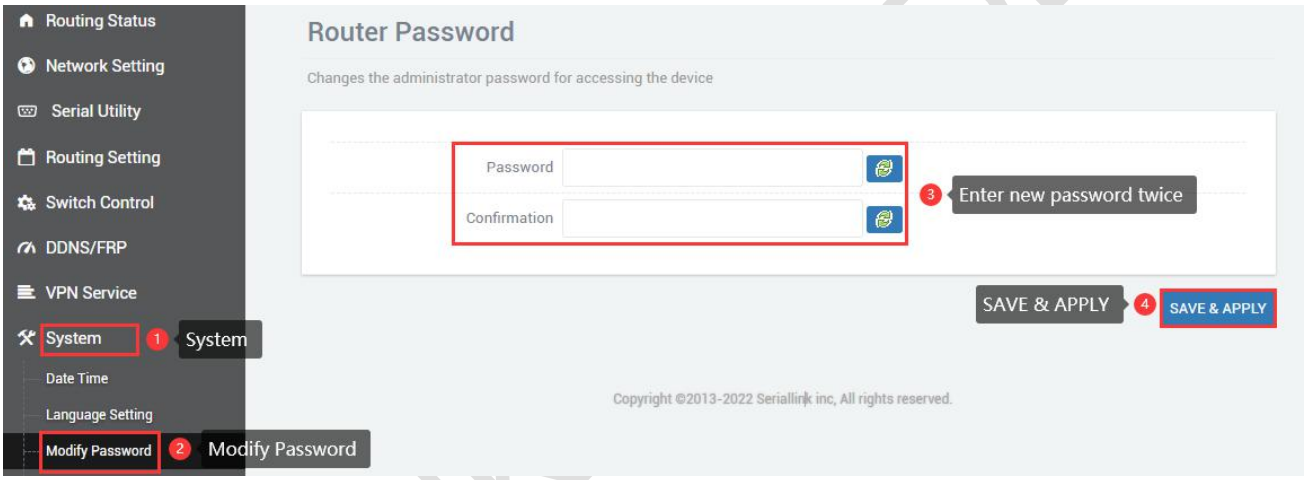
Change the language displayed on the page according to your own needs, you can choose English or Chinese, change it in the navigation bar "System" - "Language Setting", or change the language in the login interface.



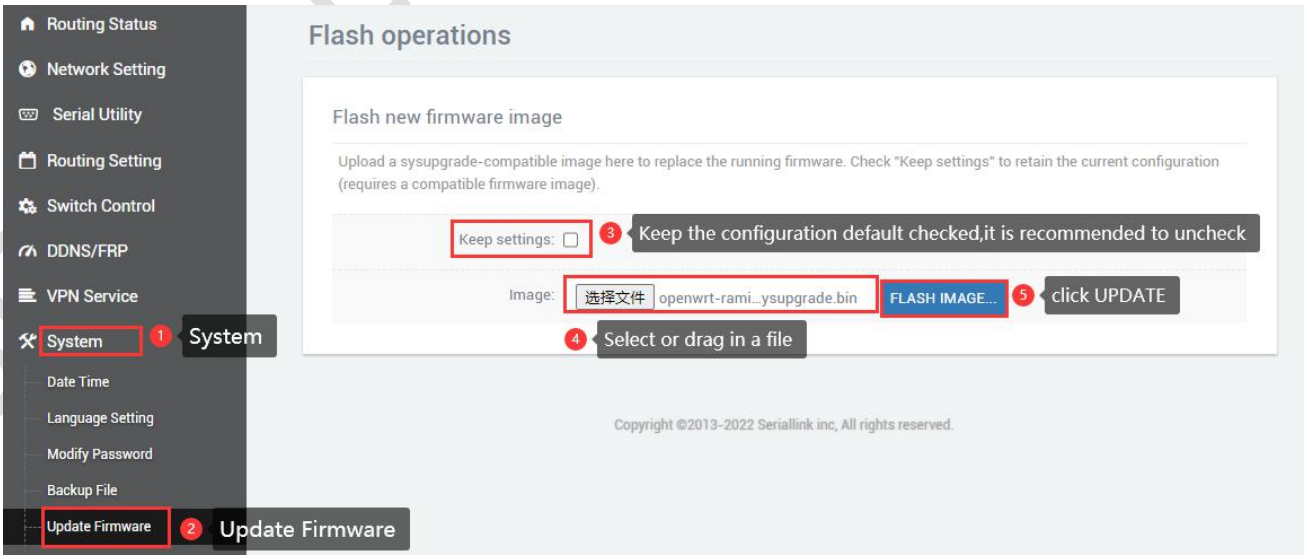


6.3 Modify Password

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.

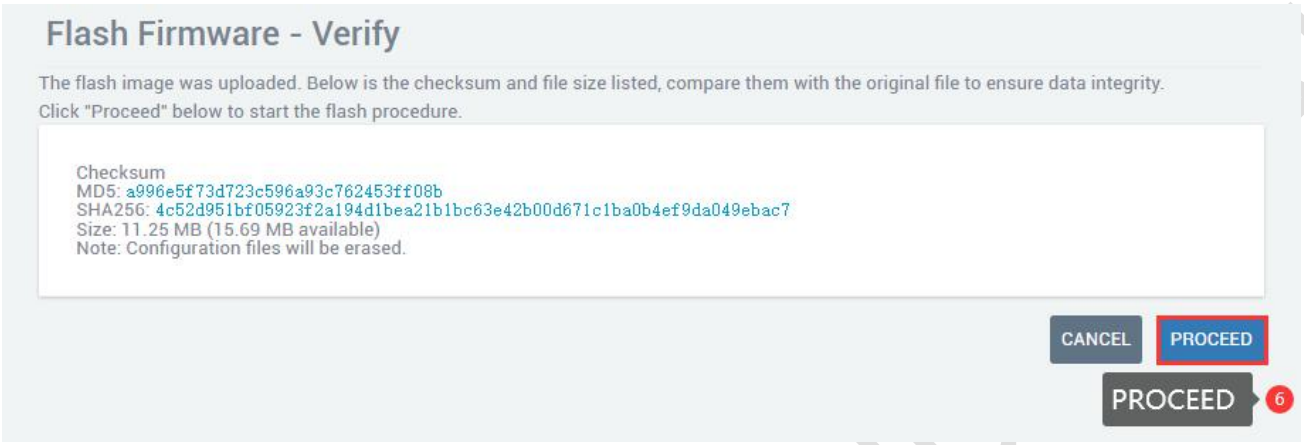


6.4 Update Firmware



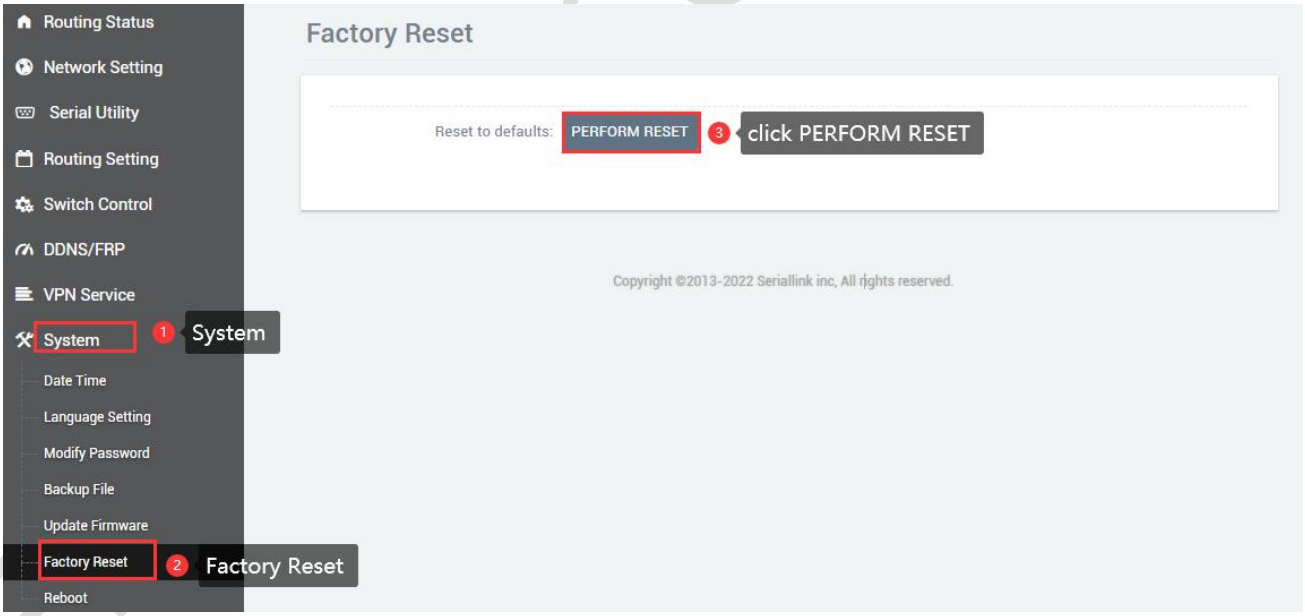
Navigation bar "System" - "Update Firmware", select the file and click "UPDATE", the MD5 check code page will appear after uploading, click "PROCEED" to upgrade, the upgrade will take a certain time,it takes about 1~2 minutes, after the upgrade is complete, log in again through "192.168.2.1".

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



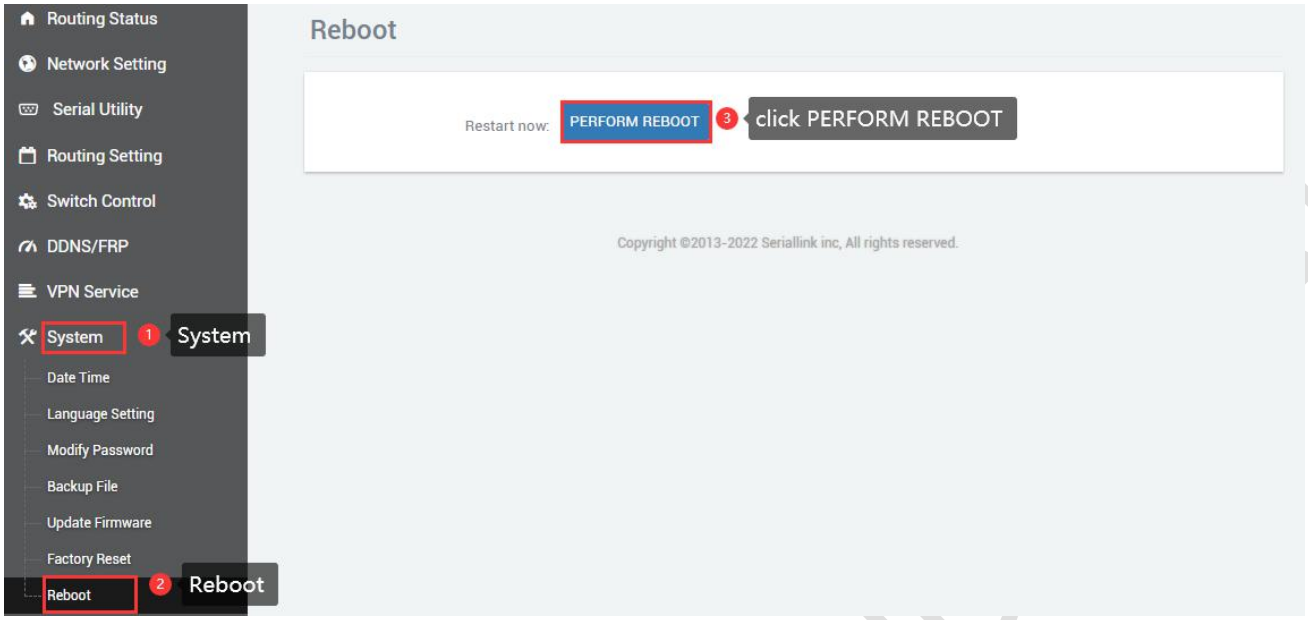
6.5 Factory Reset

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.

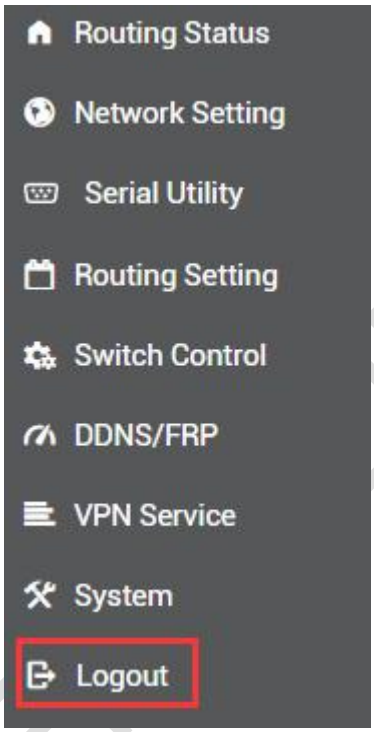


6.6 Reboot

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



6.7 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