



SLK-R602 Series

Industrial 4G/3G Router

Usermanual

Directory

1 Parameter configuration	4
1.1 Preparation before router configuration	4
1.1.1 Obtain ip address automatically (recommended)	4
1.1.2 Set static ip address	4
1.2 Login configuration page	5
2 Network Setting	6
2.1 Modify static login page address	6
2.1 SIM card 2/3/4G Internet access	7
2.3 DHCP server	9
2.4 WAN port settings	10
2.4.1 DHCP client	10
2.4.2 PPOE dial	10
2.4.3 Static Address	11
2.4.4 As Lan (convert WAN port to LAN port)	12
2.5 Wireless AP	12
2.5.1 WIFI Access Point	12
2.5.1 WIFI Client	13
2.5.3 WIFI repeater	15
①Change the local IP address	15
②Connect to the main wireless AP	15
③Disable DHCP	16
2.6 Time Reboot	17
2.7 Network backup	17
2.8 Watchcat	19
2.9 Diagnosis	20
3 Firewall	22
3.1 Firewall on and off	22
3.2 DMZ setting	22
3.3 Port Forwarding	24
3.4 Intranet penetration (frp)	26
3.4.1 Add TCP proxy protocol	31
3.4.2 Add STCP proxy protocol	33
3.4.3 Add UDP proxy protocol	40
3.4.4 Add HTTP proxy protocol	42
4 VPN (Virtual Private Network)	43
4.1 PPTP VPN	44
4.2 L2TP VPN	44
4.3 OPENVPN	45
5 Basic Management (Device Management)	48
5.1 Date Time	48
5.2 Language Setting	49
5.3 Backup File	49

5.4 Upgrade firmware	50
5.5 Factory Reset	51
5.6 Device restart	51
5.7 Page Exit	52

SERIALLINK CONFIDENTIAL

1 Parameter configuration

1.1 Preparation before router configuration

After completing the hardware installation, you need to ensure that the management computer has an Ethernet card installed before logging in to the router's Web setting page.

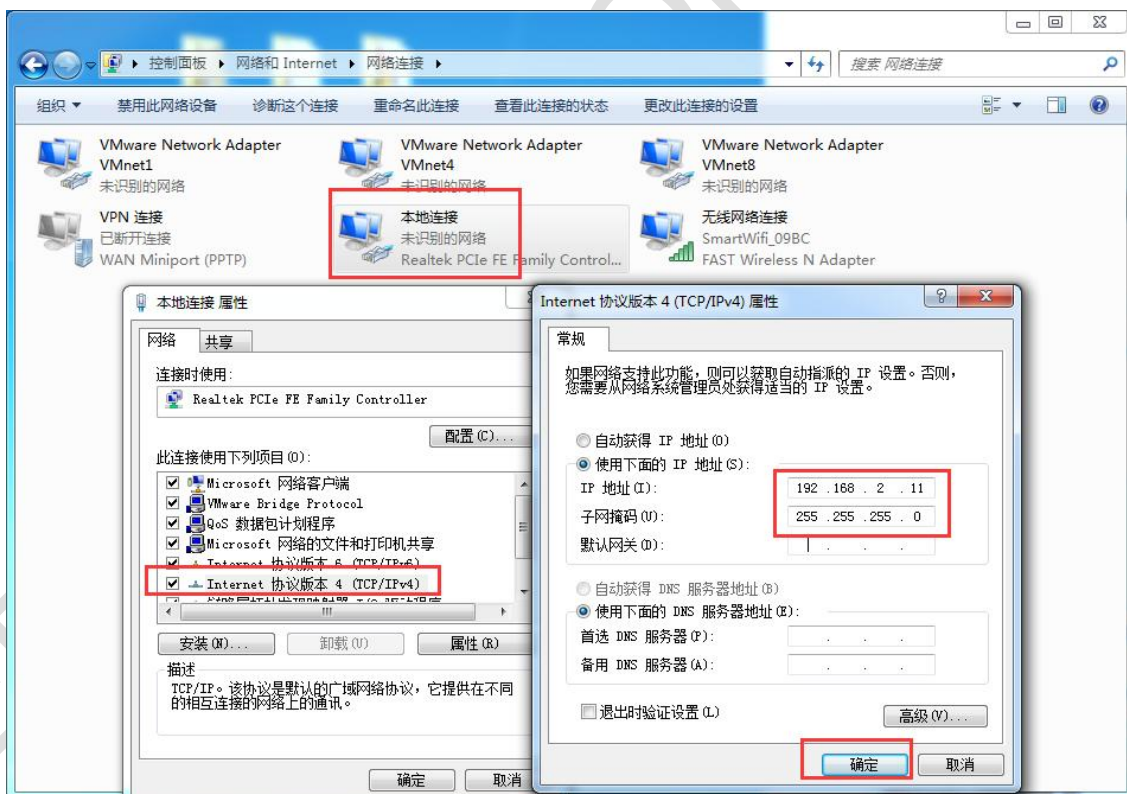
1.1.1 Obtain ip address automatically (recommended)

Please set the management PC to "Obtain IP address automatically" and "Obtain DNS server address automatically" (computer system Default configuration), the device automatically assigns an IP address to the management PC.

1.1.2 Set static ip address

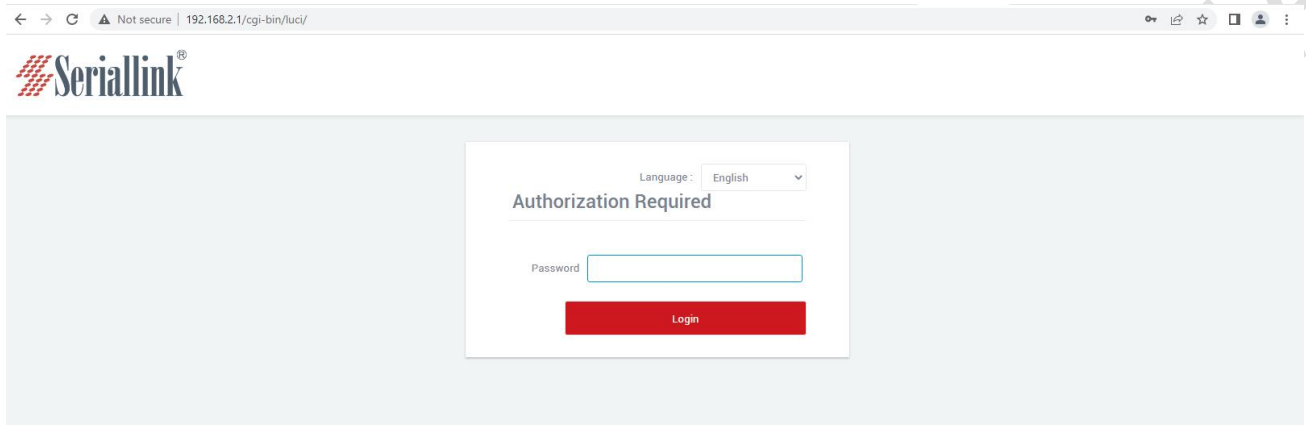
Please set the IP address of the management PC (for example: 192.168.2.11) and the IP address of the LAN port of the device in the same network segment (the initial IP address of the device's LAN port is 192.168.2.1, and the subnet mask is 255.255.255.0).

Open "Control Panel"->"Network and Internet"->"Network Connections"->"Local Area Connection" and modify as follows:

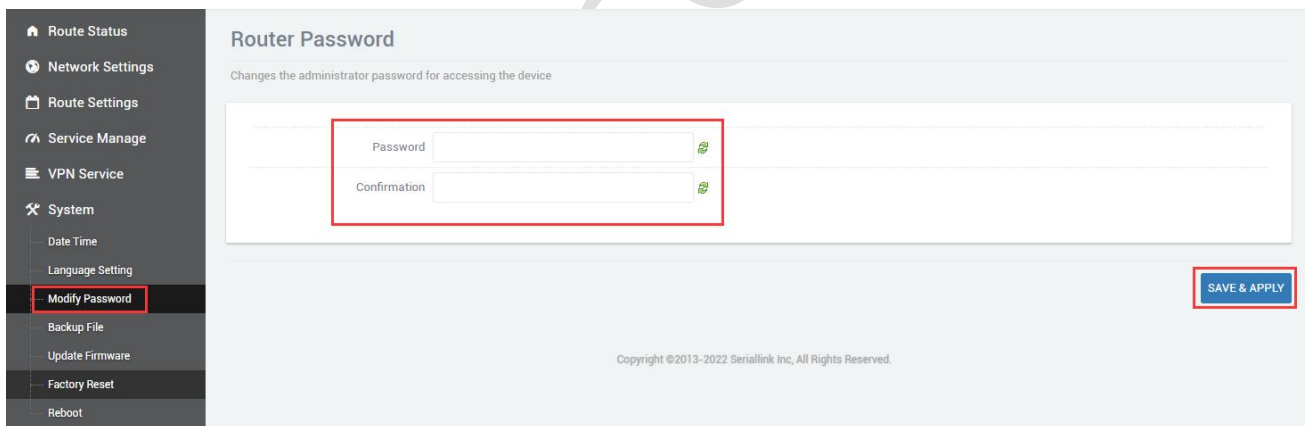


1.2 Login configuration page

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



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



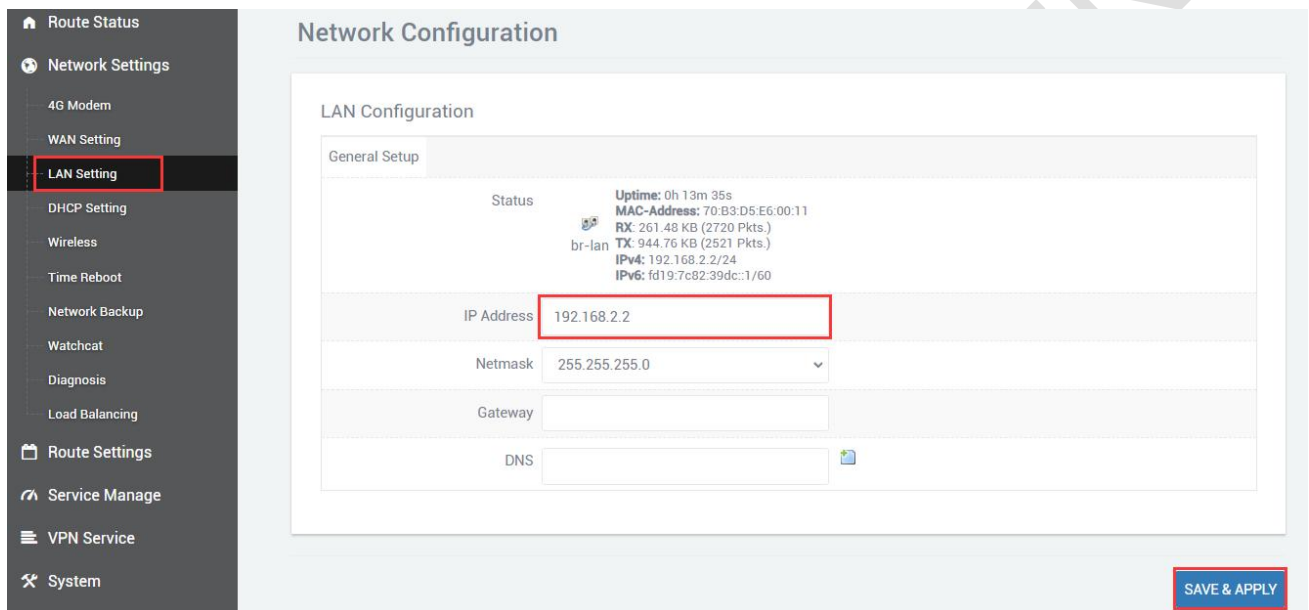
2 Network Setting

2.1 Modify static login page address

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

IP Address: Fill in the ip address to be modified.

Netmask: Fill in netmask.



Network Configuration

LAN Configuration

General Setup

Status	Uptime: 0h 13m 35s MAC-Address: 70:B3:D5:E6:00:11 RX: 261.48 KB (2720 Pkts.) TX: 944.76 KB (2521 Pkts.) br-lan IPv4: 192.168.2.2/24 IPv6: fd19:7c82:39dc::1/60
IP Address	192.168.2.2
Netmask	255.255.255.0
Gateway	
DNS	

SAVE & APPLY

← → ↻ 🏠 ⚠️ 不安全 192.168.2.2/cgi-bin/luci 🔍 📄 ☆ 🗄️ 🌐 更新



语言: 中文 (Chinese) ▼

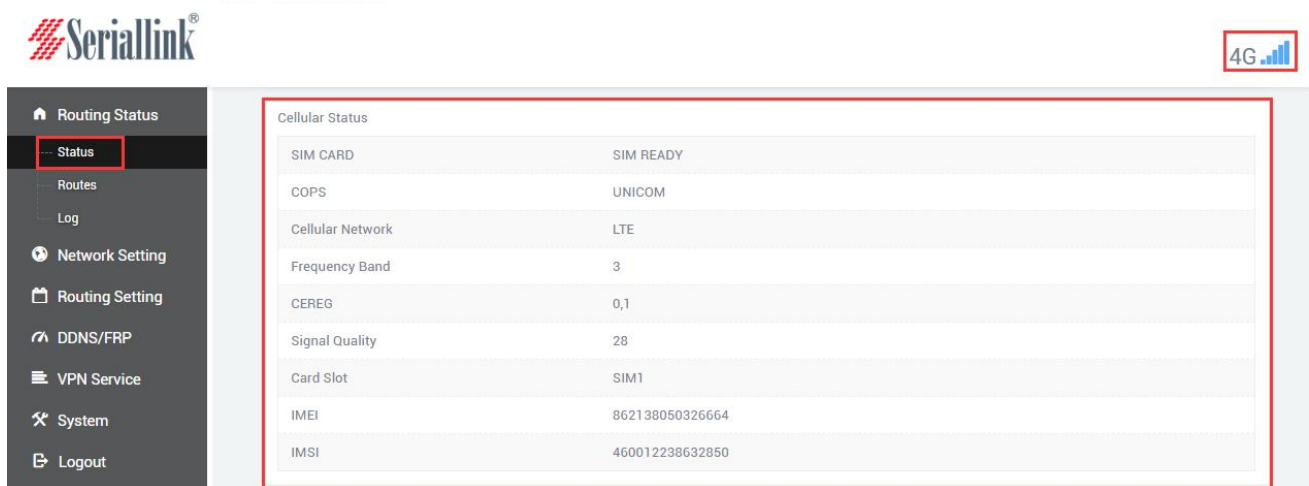
需要授权

密码

登录

2.1 SIM card 2/3/4G Internet access

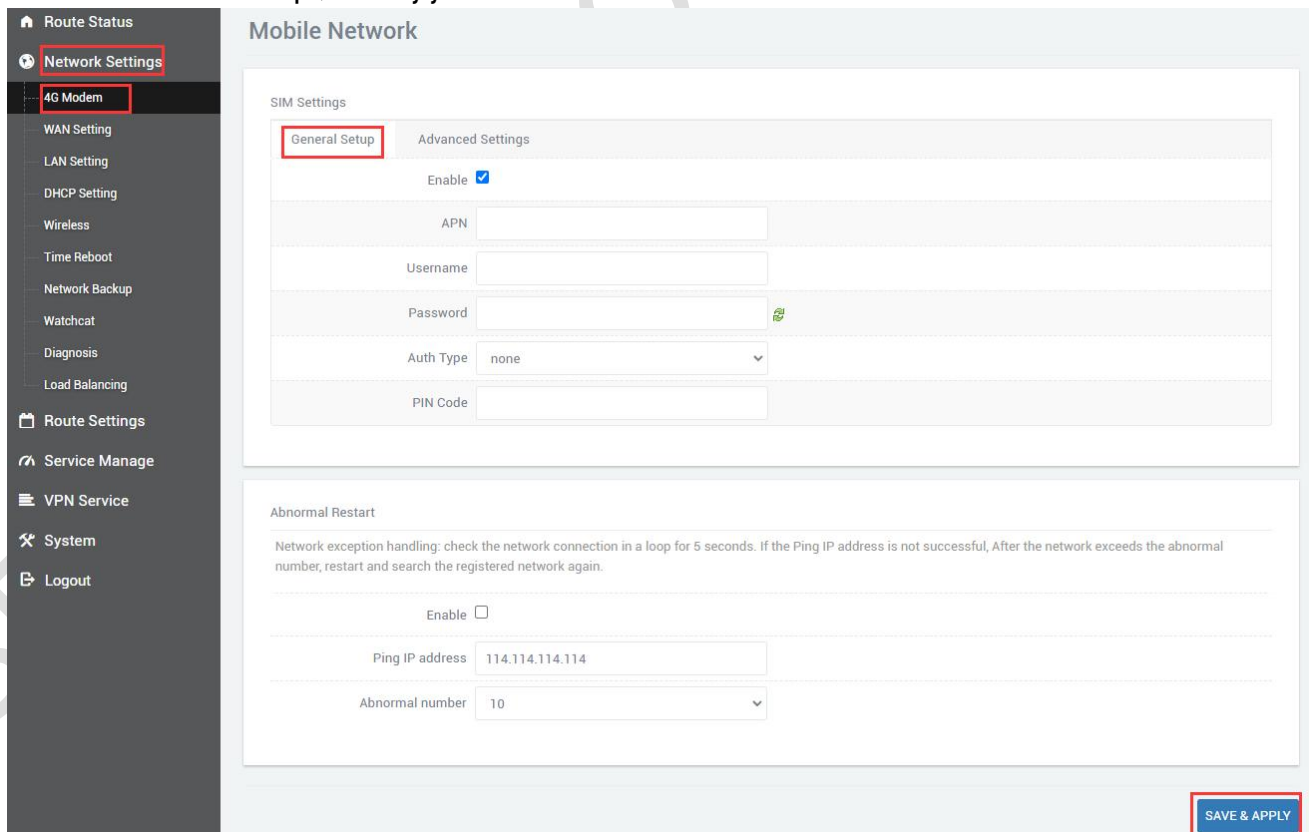
The router uses SIM card 2/3/4G to surf the Internet by default. You can see the information of the SIM card in the navigation bar "Routing Status"->"Status", and you can check the network is 2/3/4G and the signal of the mobile phone card in the upper right corner.



The screenshot shows the Seriallink web interface. In the top right corner, there is a '4G' signal indicator. The left sidebar contains a navigation menu with 'Status' highlighted. The main content area displays the 'Cellular Status' table, which is enclosed in a red box:

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, and the default is empty. If you use an APN card, you need to set the APN in "Network Settings"->"4G Modem"->"General Setup", fill in by yourself.



The screenshot shows the Seriallink web interface. In the left sidebar, 'Network Settings' and '4G Modem' are highlighted. The main content area displays the 'Mobile Network' settings page. The 'SIM Settings' section has the 'General Setup' tab selected and highlighted with a red box. The settings are as follows:

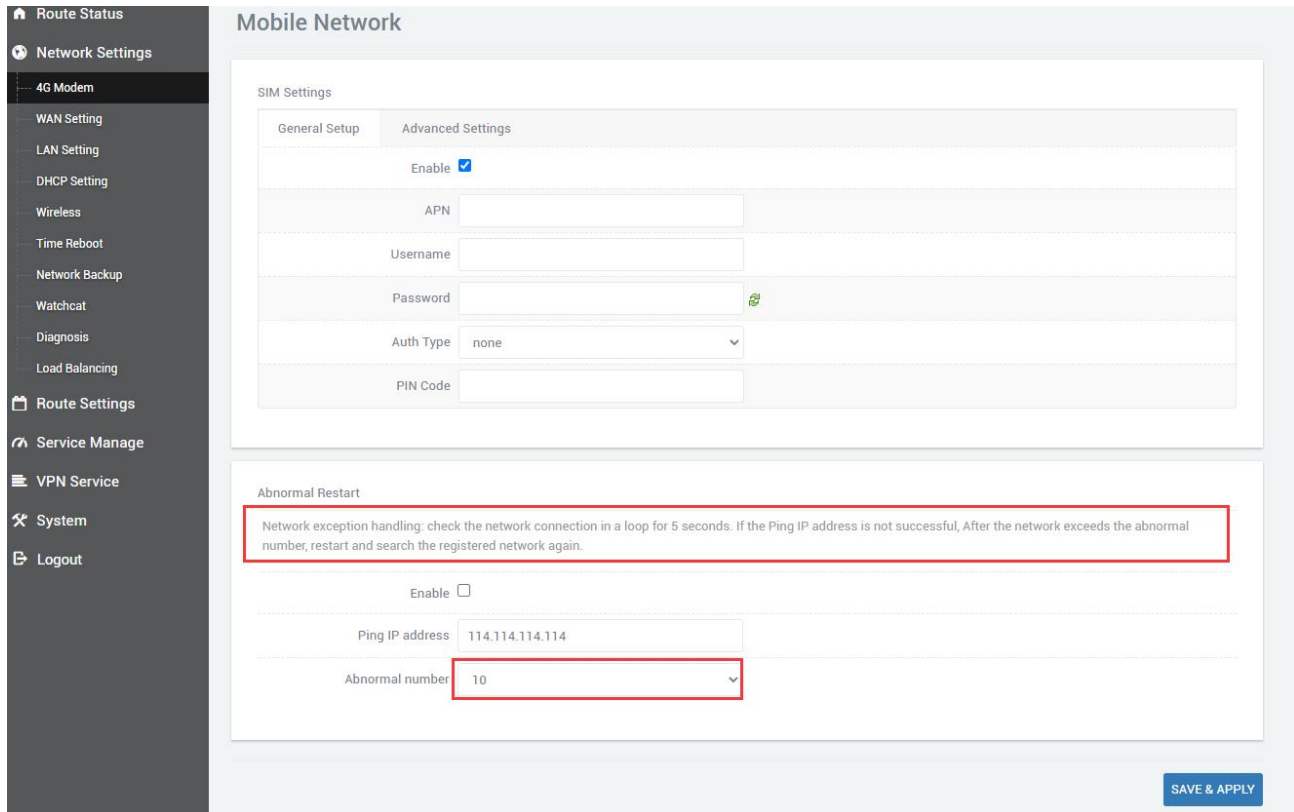
SIM Settings	
General Setup	Advanced Settings
Enable	<input checked="" type="checkbox"/>
APN	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
Auth Type	none
PIN Code	<input type="text"/>

Below the SIM Settings, there is an 'Abnormal Restart' section with the following settings:

Abnormal Restart	
Enable	<input type="checkbox"/>
Ping IP address	114.114.114.114
Abnormal number	10

A 'SAVE & APPLY' button is located at the bottom right of the page, highlighted with a red box.

Network diagnosis: It is to deal with network abnormalities. Ping the set ip address every 5s. After the abnormal number of pings, the network still cannot be pinged, and the network will be re-registered. You can set network diagnostics in both "Basic Settings" and "Advanced Settings", or you don't need to enable network diagnostics, just leave it unchecked.



The screenshot displays the 'Mobile Network' configuration page. The left sidebar contains navigation options: Route Status, Network Settings (selected), 4G Modem, WAN Setting, LAN Setting, DHCP Setting, Wireless, Time Reboot, Network Backup, Watchcat, Diagnosis, Load Balancing, Route Settings, Service Manage, VPN Service, System, and Logout. The main content area is titled 'Mobile Network' and is divided into 'SIM Settings' and 'Abnormal Restart' sections.

SIM Settings

General Setup	Advanced Settings
	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"/>

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.

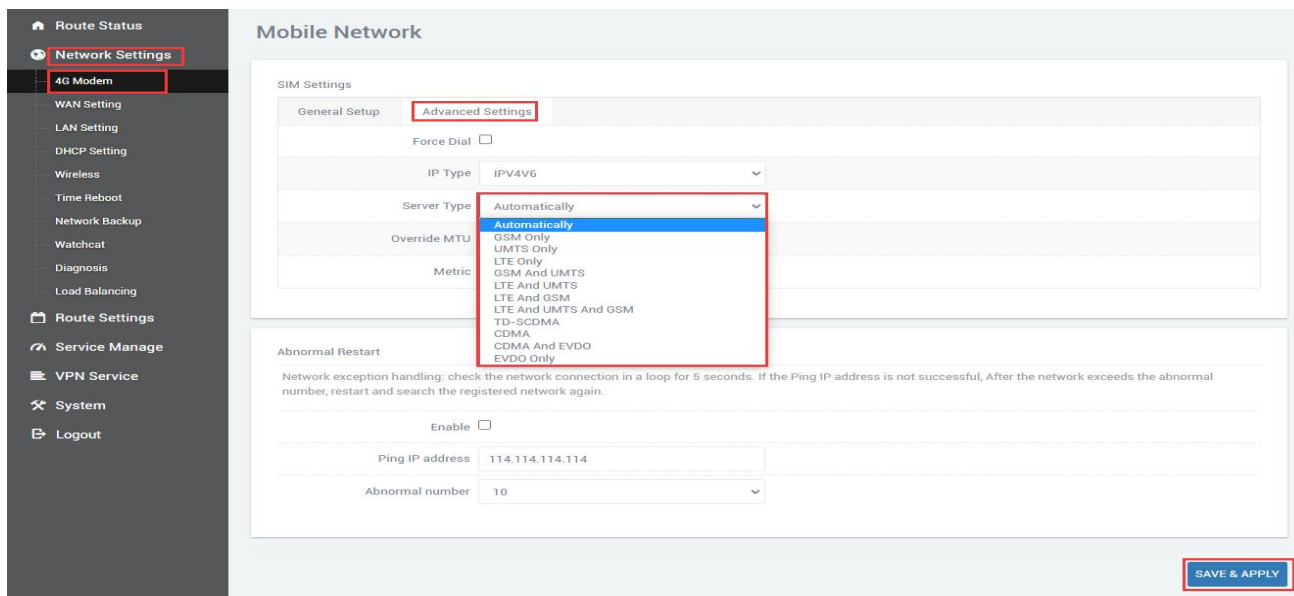
Enable

Ping IP address: 114.114.114.114

Abnormal number: 10

SAVE & APPLY

"Network Settings" - "4G Network" - "Advanced Settings" can bind 2/3/4G. If the service type is selected as LTE Only, it means that only 4G network is used. If it is not 4G, there will be no network automatically. The default is 2/3/4G. Which one will be used first if the network signal is stronger, and 4G will be used first. Locking the frequency band is forbidden. The frequency band with good signal is preferred. You can also lock the frequency band according to your needs. If the locked frequency band is unsuccessful, the module does not support this frequency band temporarily. Click "SAVE & APPLY".



Note:

- Ordinary 4G mobile phone card can go online without worrying about APN settings
- If you use APN dedicated network card, you must fill in the APN address, user name and password
- Different operators have different specifications of APN dedicated network cards, APN address, user name and password (if any, please refer to the chapter of APN setting table) or consult the local operator.

2.3 DHCP server

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

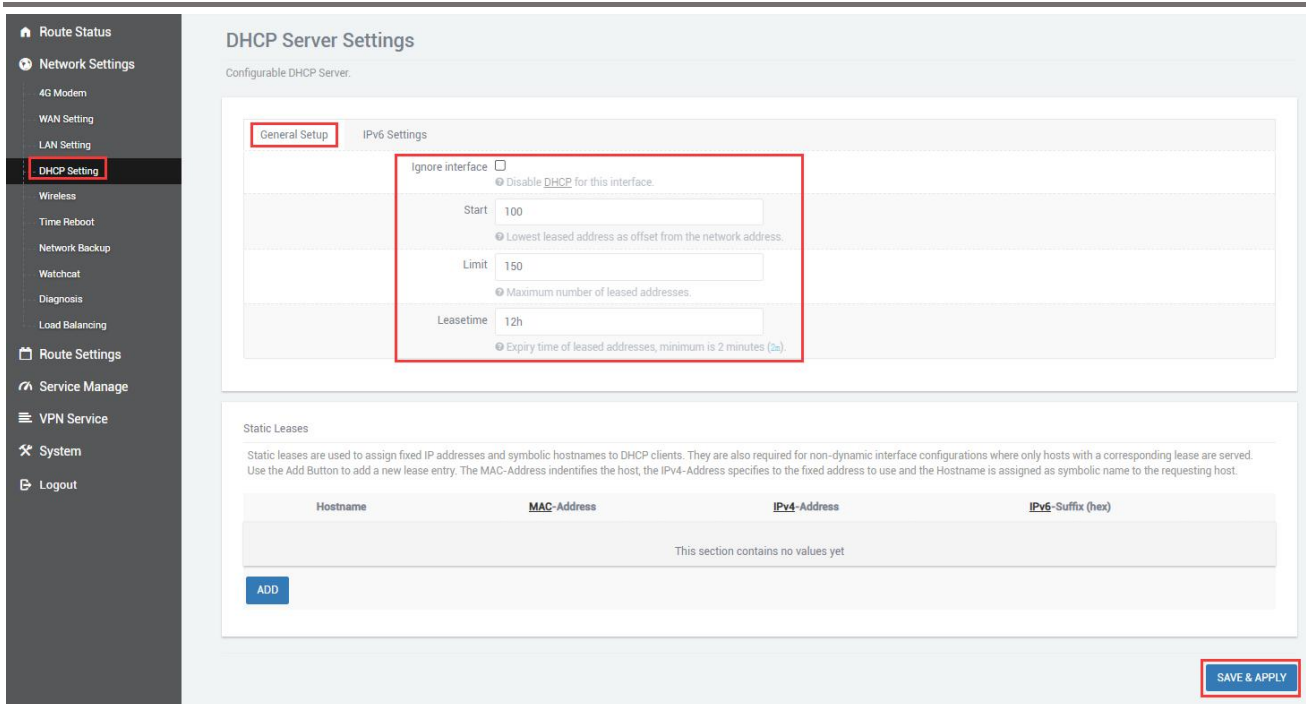
DHCP client configuration (usually the default): select "Network Settings"->"DHCP Settings" in turn, "SAVE & APPLY".

Turn off DHCP: Click to turn off the DHCP server

Start: the starting address of the assigned dhcp server, such as 100, which means the assignment starts from 192.168.2.100

Number of customers: the number of IP addresses that can be allocated, ensure that the starting number plus the number of customers cannot exceed 150

Lease time: the length of time of the assigned IP.

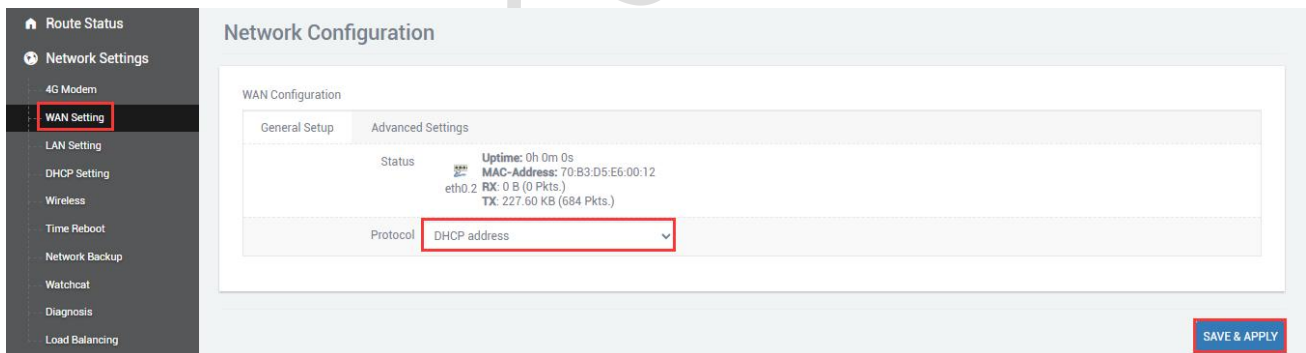


The screenshot shows the 'DHCP Server Settings' page. On the left sidebar, 'DHCP Setting' is highlighted. The main content area is titled 'DHCP Server Settings' and 'Configurable DHCP Server'. It has two tabs: 'General Setup' (selected) and 'IPv6 Settings'. Under 'General Setup', there is an 'Ignore interface' checkbox (unchecked) with a sub-option 'Disable DHCP for this interface'. Below this are three input fields: 'Start' (value: 100), 'Limit' (value: 150), and 'Leasetime' (value: 12h). Each input field has a tooltip explaining its function. At the bottom right of the main area is a 'SAVE & APPLY' button.

2.4 WAN port settings

2.4.1 DHCP client

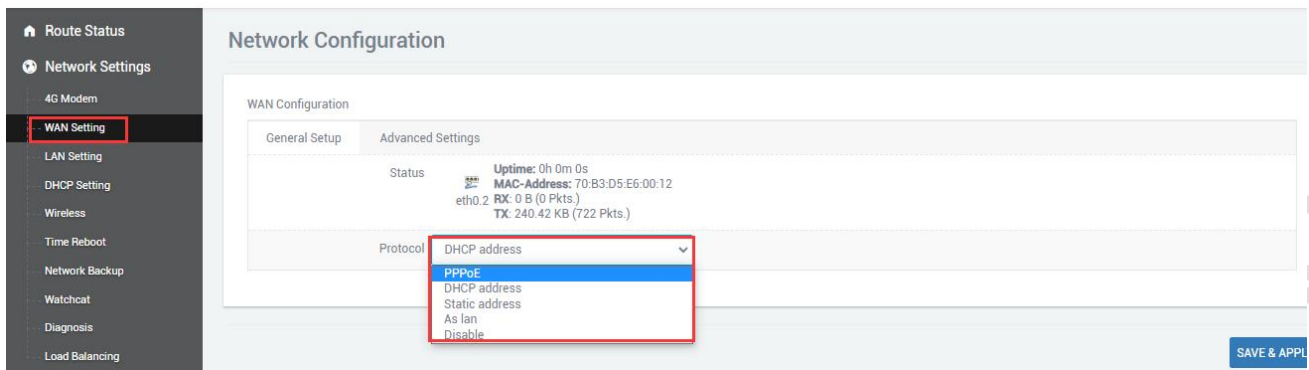
Navigation bar "Network Settings"->"wan Settings", Switch protocol of the WAN port to a DHCP address (DHCP client), and the upper-level device needs to be able to assign an IP to the wan port.



The screenshot shows the 'Network Configuration' page. On the left sidebar, 'WAN Setting' is highlighted. The main content area is titled 'Network Configuration' and 'WAN Configuration'. It has two tabs: 'General Setup' and 'Advanced Settings'. Under 'Advanced Settings', there is a 'Status' section showing 'Uptime: 0h 0m 0s', 'MAC-Address: 70:B3:D5:E6:00:12', and 'eth0.2 RX: 0 B (0 Pkts.) TX: 227.60 KB (684 Pkts.)'. Below this is a 'Protocol' dropdown menu with 'DHCP address' selected. At the bottom right of the main area is a 'SAVE & APPLY' button.

2.4.2 PPOE dial

If the wan port needs to dial-up to access the Internet, you need to select ppoe dial-up, and fill in the user name and password according to the actual situation.



Network Configuration

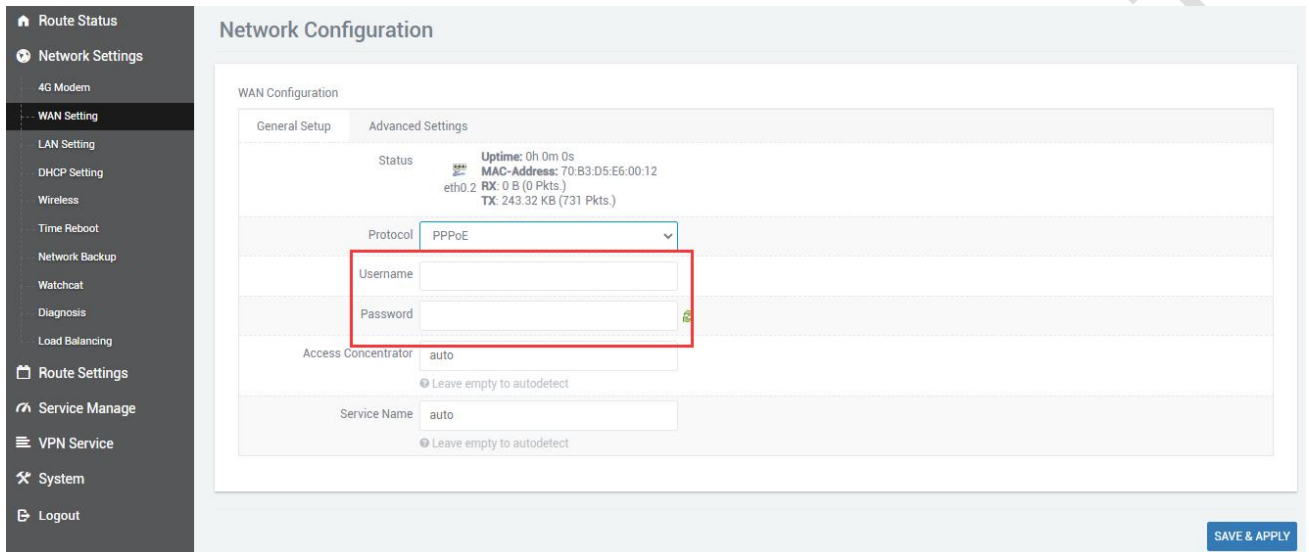
WAN Configuration

General Setup | Advanced Settings

Status **Uptime:** 0h 0m 0s
MAC-Address: 70:B3:D5:E6:00:12
 eth0.2 **RX:** 0 B (0 Pkts.)
TX: 240.42 KB (722 Pkts.)

Protocol: DHCP address (dropdown menu open showing options: DHCP address, PPPoE, Static address, As lan, Disable)

SAVE & APPLY



Network Configuration

WAN Configuration

General Setup | Advanced Settings

Status **Uptime:** 0h 0m 0s
MAC-Address: 70:B3:D5:E6:00:12
 eth0.2 **RX:** 0 B (0 Pkts.)
TX: 243.32 KB (731 Pkts.)

Protocol: PPPoE

Username:

Password:

Access Concentrator: auto
 Leave empty to autodetect

Service Name: auto
 Leave empty to autodetect

SAVE & APPLY

2.4.3 Static Address

The wan port can also choose to set the ip address manually.

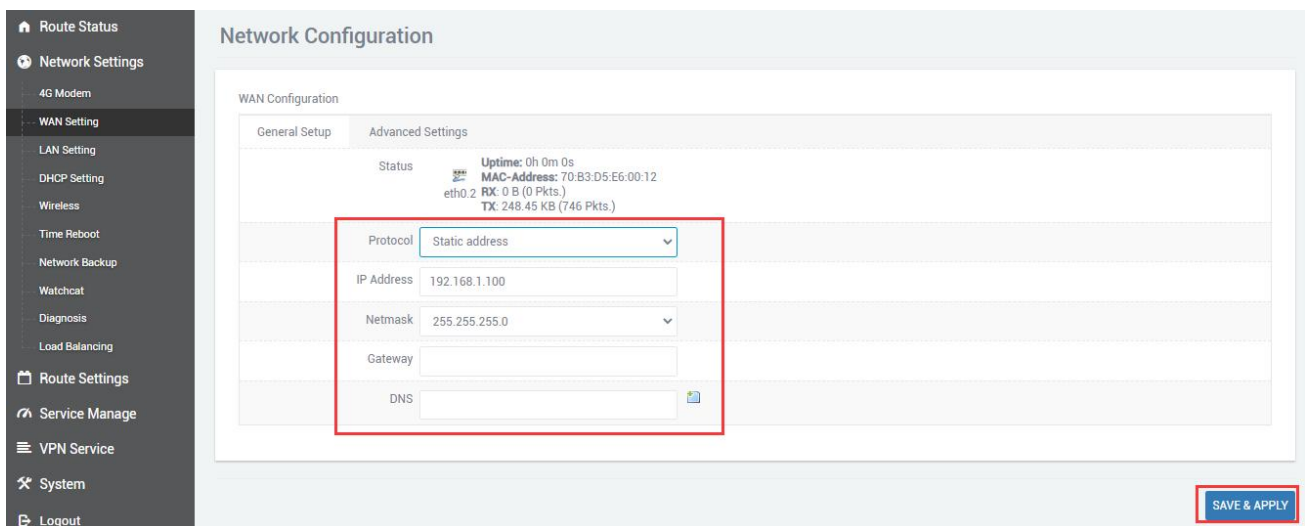
Protocol: Static address

IP Address: It can be in the same network segment as the upper-level route, but the upper-level route cannot be the same as the address of the LAN port of your own device, otherwise conflicts will occur. For example, the superior route is 192.168.1.1, so write 192.168.1.xxx here.

Netmask: generally 255.255.255.0.

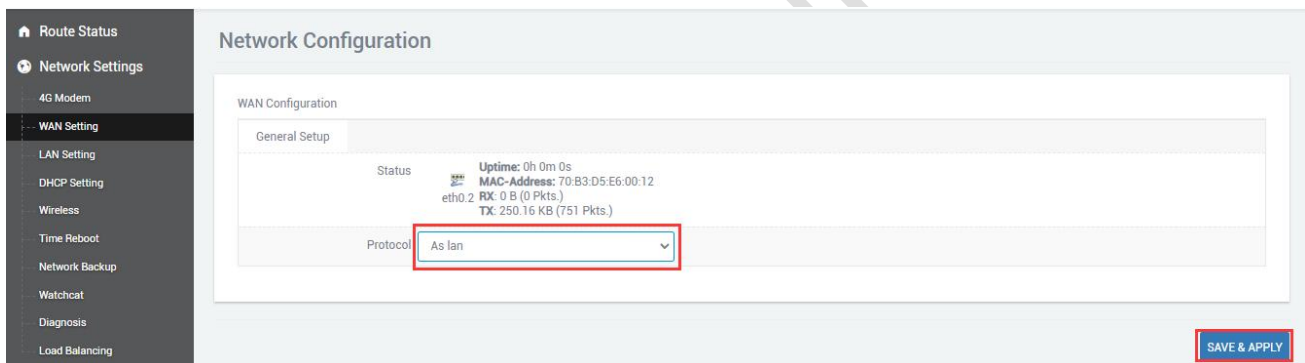
Gateway: such as 114.114.114.114, 8.8.8.8, etc.

DNS: such as 114.114.114.114, 8.8.8.8, etc.



2.4.4 As Lan (convert WAN port to LAN port)

If you need to convert the WAN port to a LAN port, change the wan setting protocol to "As lan", click "SAVE & APPLY", you can convert the wan port to a lan port.



2.5 Wireless AP

2.5.1 WIFI Access Point

The router supports both the wireless AP and the client to be turned on at the same time. It can open a wifi for other devices to connect and connect to other wifi. This function can realize wireless relay.

The router generally defaults wireless AP to be turned on, there is a wifi name of SLK-Routers_XXX, the default password is slk100200.

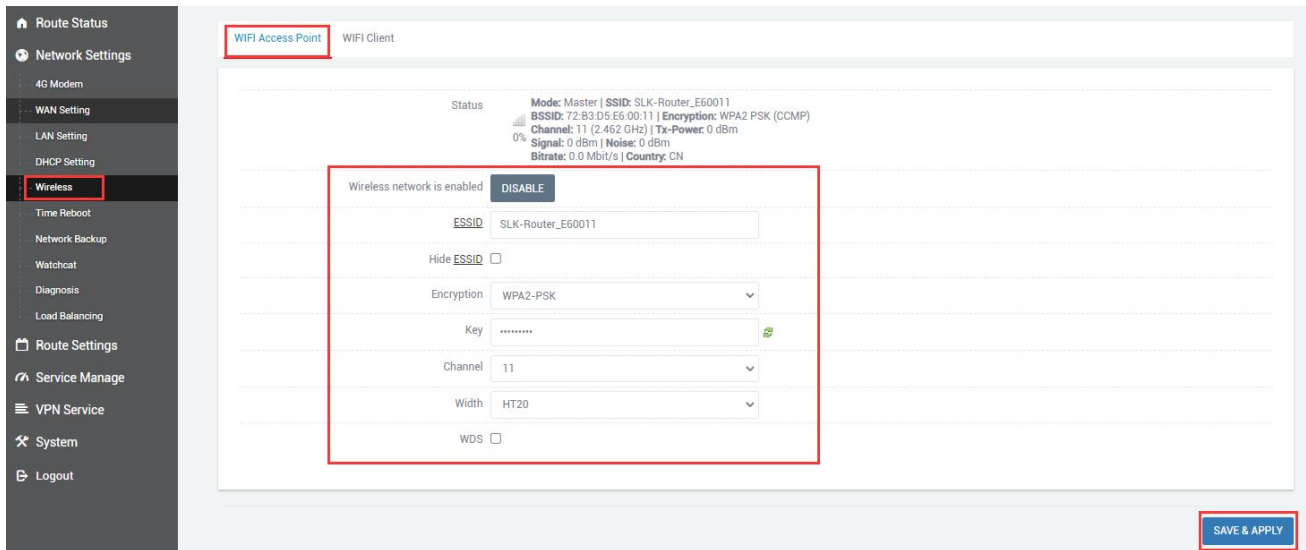
Click DISABLE to close router's AP for your needs.

Modify ESSID to rename the WiFi.

We suggest a Mixed Mode for the AP Encryption and also the Key should be modified too.

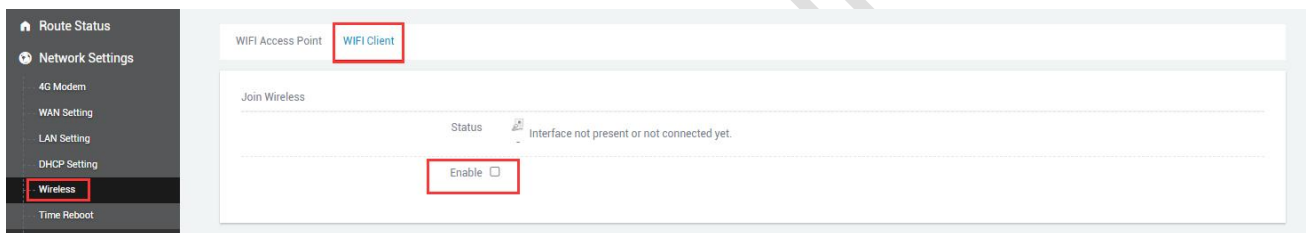
Channel and Width have an impact on wireless quality, change them according to the actual use environment.

After the configuration is complete, click "Save & Apply" to make it effective.

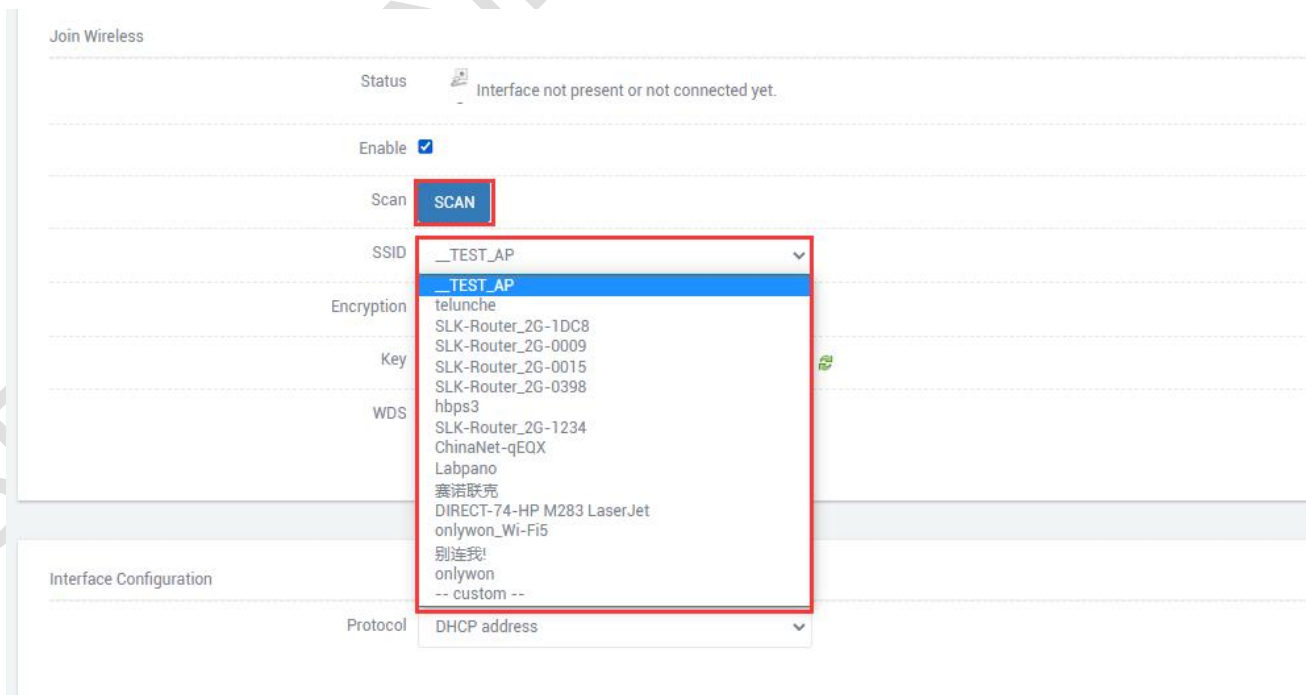


2.5.1 WIFI Client


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



Then select the client wifi interface: select WIFI in the SSID list, change the security option according to whether there is a password.No Encryption、WPA-PSK、WPA-2PSK、WPA-PSK/WPA2-PSK Mixed Mode, WDS is not checked by default.



Join Wireless

Status  Interface not present or not connected yet.

Enable

Scan

SSID 赛诺联克

Encryption WPA-2PSK

Key

WDS

Enable WDS if Bridge Lan is selected.

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

Status 

Client "赛诺联克"

Uptime: 0h 0m 22s
 MAC-Address: 70-B3:D5:E6:00:11
 RX: 705.74 KB (2703 Pkts.)
 TX: 26.65 KB (120 Pkts.)
 IPv4: 192.168.16.64/24

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).

Interface Configuration

Protocol Static address

IP Address 192.168.16.65

Netmask 255.255.255.0

Gateway 192.168.16.1

DNS 192.168.16.1

Status 

Client "赛诺联克"

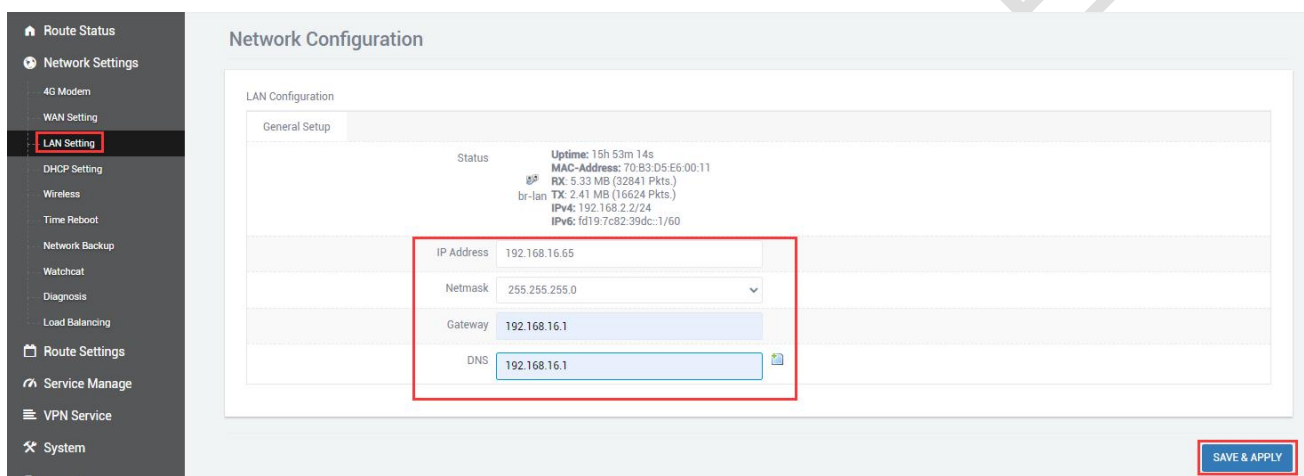
Uptime: 0h 0m 25s
 MAC-Address: 70-B3:D5:E6:00:11
 RX: 49.93 KB (167 Pkts.)
 TX: 2.38 KB (14 Pkts.)
 IPv4: 192.168.16.65/24

2.5.3 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-R602 is in the same IP address segment as the main wireless network.

① Change the local IP address

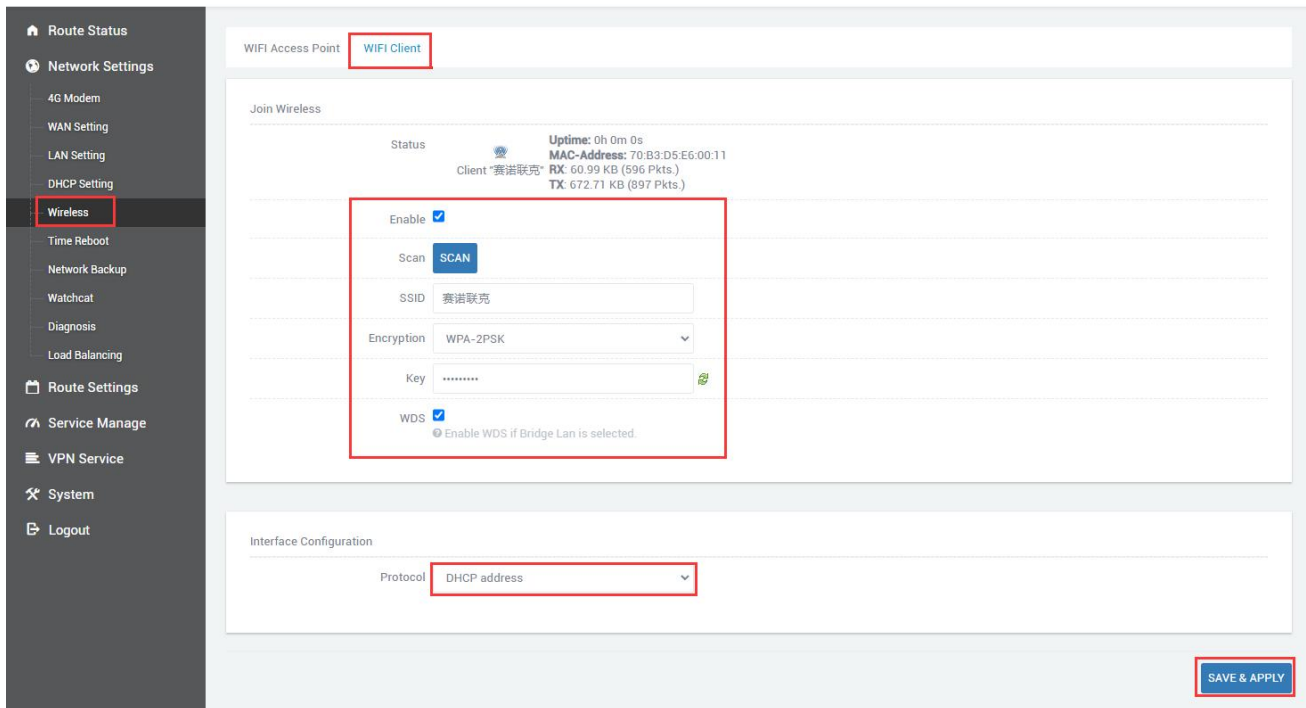
It is necessary to modify the local IP address of SLK-R602 to be in the same network segment as the main wireless AP. For example, the IP address of the main wireless AP to be connected is 192.168.16.1, then modify the IP address of SLK-R602 to 192.168.16.65. It should be noted that the LAN port gateway 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.



The screenshot shows the 'Network Configuration' page with the 'LAN Configuration' section expanded to 'General Setup'. A red box highlights the IP Address field, which is set to 192.168.16.65. Other fields include Netmask (255.255.255.0), Gateway (192.168.16.1), and DNS (192.168.16.1). A 'SAVE & APPLY' button is visible at the bottom right.

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 赛诺联克, and the password is slk100200, Search and select the SSID as shown in the figure below, fill in the password, select "Bridge Lan" from "Protocol", and click "SAVE & APPLY".

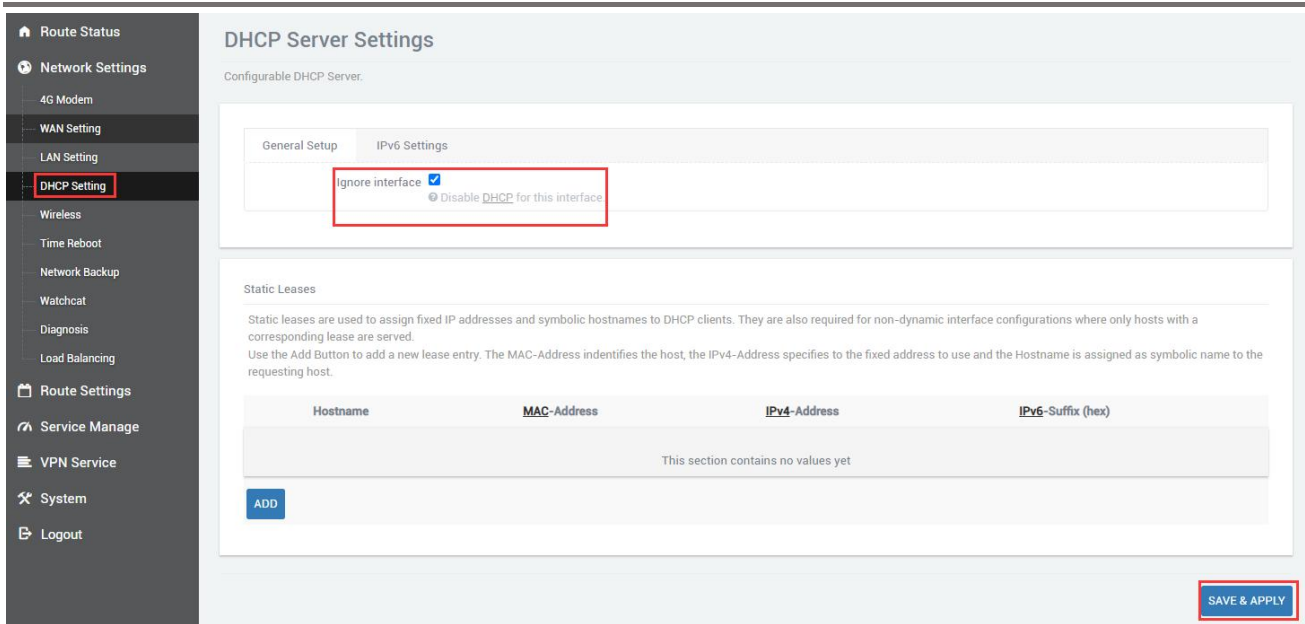


It should be noted that in this mode, the main wireless AP no longer assigns an IP address to this SLK-R602. Therefore, the obtained IP address will not be updated in "Status", and you can confirm whether the connection is successful through the icon color and MAC address. The picture below is successful.



③Disable DHCP

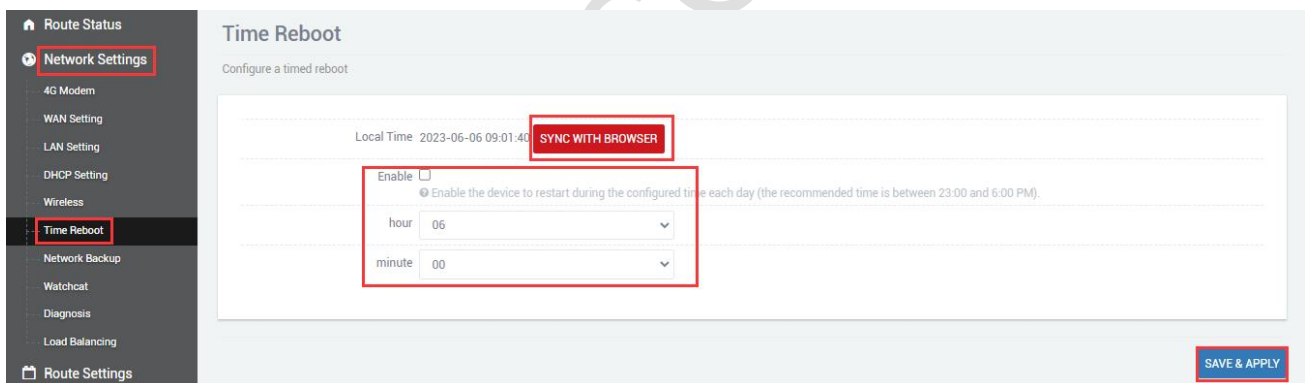
Disable the DHCP server function of the SLK-R602. In this way, the SLK-R602 no longer assigns IP addresses to the connected devices, and all devices connected to the local area network are assigned IP addresses by the main wireless to realize communication on the same network segment.



The screenshot shows the 'DHCP Server Settings' page. The left sidebar has 'DHCP Setting' highlighted. The main content area has two tabs: 'General Setup' and 'IPv6 Settings'. Under 'IPv6 Settings', the 'Ignore interface' checkbox is checked and highlighted with a red box. Below it, there is a 'Static Leases' section with a table that is currently empty. A 'SAVE & APPLY' button is located at the bottom right of the page.

2.6 Time Reboot

Navigation bar "Network settings" - "Restart time", the user can check the enabling and set the daily restart time, pay attention to check whether the device time is correct, click the button to modify the correct time.

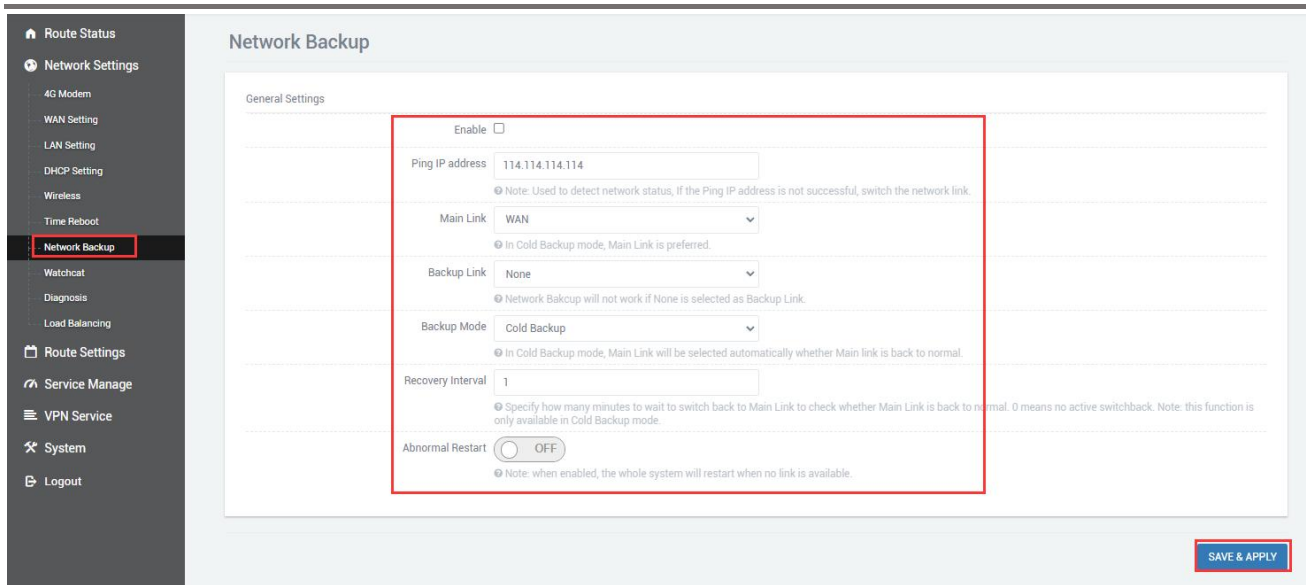


The screenshot shows the 'Time Reboot' page. The left sidebar has 'Time Reboot' highlighted. The main content area shows the 'Local Time' as 2023-06-06 09:01:40. There is a 'SYNC WITH BROWSER' button. Below that, the 'Enable' checkbox is checked and highlighted with a red box. Underneath, the 'hour' is set to 06 and the 'minute' is set to 00, both highlighted with a red box. A 'SAVE & APPLY' button is at the bottom right.

2.7 Network backup

It is mainly used to connect the Internet, whether the wired (i.e. WAN port) or 4G network or WiFi client is preferred, the network with the main link is preferred, and the network with the backup route is used when the main link has no network.

Network backup is off by default. You need to check enable and then configure it according to the actual situation.



Configure according to the table below.

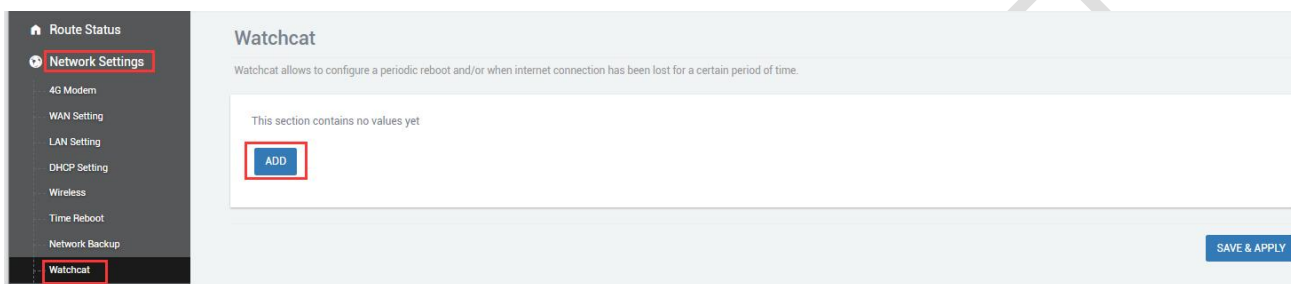
General settings @ link management		
Project	Explain	Default
Main Chain	<p>You can choose "WAN", "SIM1" or "WIFI".</p> <p>WAN: using Wan as the main wired link</p> <p>SIM1: use Sim1 as the main wireless link</p> <p>WIFI: use the WiFi client as the main wireless link</p> <p>Note: WiFi link is only available when WiFi client mode is turned on. Please refer to "5.2" for details.</p>	WAN
Backup Link	<p>You can choose "WAN", "SIM1", "WIFI" or "NONE".</p> <p>WAN: a wired link using Wan as backup</p> <p>SIM1: wireless link using Sim1 as backup</p> <p>WIFI: wireless link using WIFI client as backup</p> <p>Note: WIFI link is only available when WIFI client mode is turned on. Please refer to "5.2" for details.</p> <p>NONE: the backup link is not allowed</p>	NONE
Backup Mode	<p>Select "Cold Backup" or "Hot Backup"</p> <p>Cold backup: the backup link is dialed online only when it is switched</p> <p>Hot backup: the backup link is always online</p> <p>Note: hot backup is not applicable to dual sim card backup.</p>	Cold Backup
Recovery Interval	<p>When the backup link is used in cold backup mode, it specifies how many minutes to wait to switch back to the main link to detect whether the main link returns to normal. 0 means no active switchback.</p> <p>Note: this function is displayed only when cold backup mode is selected.</p>	1
Abnormal Restart	Click the button to turn on/off the abnormal restart function.	OFF

	When enabled, the device will restart when no link is available.	
--	--	--

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

D. Ping period: How often to check internet connection. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days

1. Reboot on internet connection lost

DELETE

Operating mode	<input type="text" value="Reboot on internet connection lost"/>	
Forced reboot delay	<input type="text" value="0"/>	<small>ⓘ 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.</small>
Period	<input type="text"/>	<small>ⓘ 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</small>
Ping host	<input type="text" value="8.8.8.8"/>	<small>ⓘ Host address to ping</small>
Ping period	<input type="text"/>	<small>ⓘ How often to check internet connection. Default unit is seconds, you can use the suffix 'm' for minutes, 'h' for hours or 'd' for days</small>

ADD

2. Periodic reboot

Operating mode:

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

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

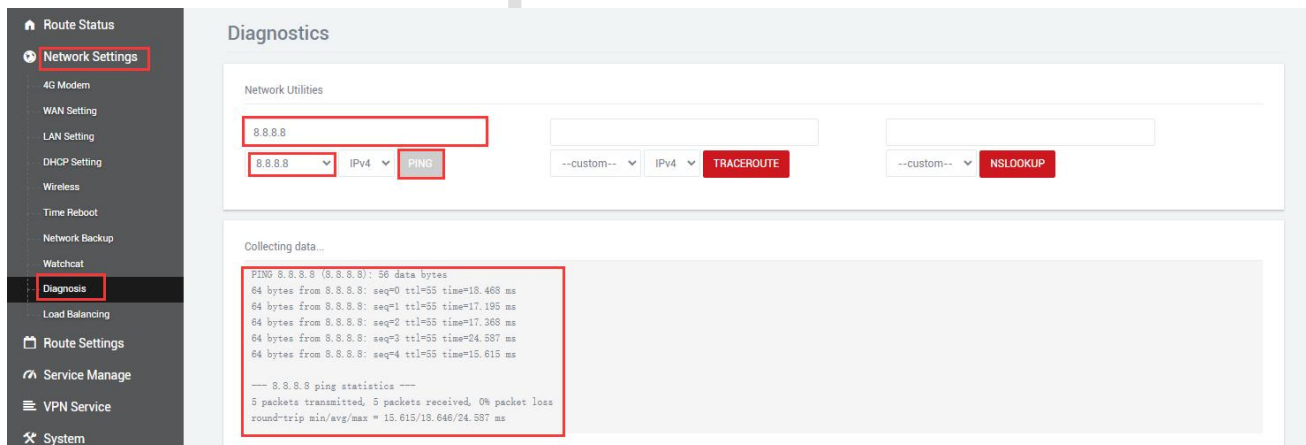
After adding and configuring, click "SAVE & APPLY" to take effect. To delete the configuration, just click the "DELETE" button in the upper right corner, and then "SAVE & APPLY".

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.



```
Collecting data...
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=55 time=18.469 ms
64 bytes from 8.8.8.8: seq=1 ttl=55 time=17.195 ms
64 bytes from 8.8.8.8: seq=2 ttl=55 time=17.269 ms
64 bytes from 8.8.8.8: seq=3 ttl=55 time=24.597 ms
64 bytes from 8.8.8.8: seq=4 ttl=55 time=15.615 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 15.615/18.646/24.597 ms
```

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

Route Status

Network Settings

4G Modem

WAN Setting

LAN Setting

DHCP Setting

Wireless

Time Reboot

Network Backup

Watchcat

Diagnosis

Load Balancing

Route Settings

Service Manage

VPN Service

System

Diagnostics

Network Utilities

192.168.8.1

8.8.8.8 IPv4 PING --custom-- IPv4 TRACEROUTE --custom-- NSLOOKUP

Collecting data...

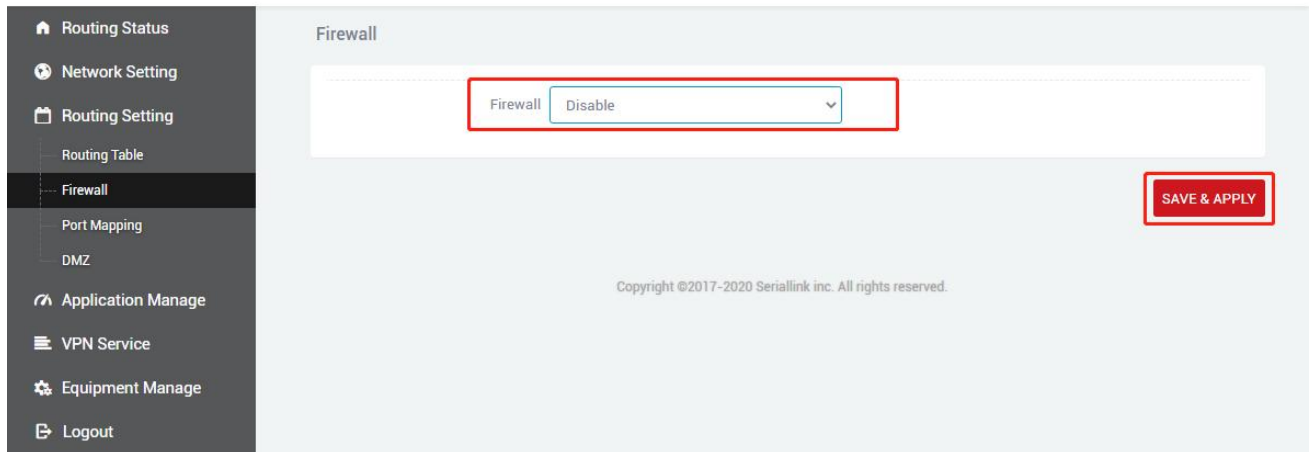
```
PING 192.168.8.1 (192.168.8.1): 56 data bytes
64 bytes from 192.168.8.1: seq=0 ttl=64 time=1.427 ms
64 bytes from 192.168.8.1: seq=1 ttl=64 time=1.382 ms
64 bytes from 192.168.8.1: seq=2 ttl=64 time=0.955 ms
64 bytes from 192.168.8.1: seq=3 ttl=64 time=1.216 ms
64 bytes from 192.168.8.1: seq=4 ttl=64 time=1.312 ms

--- 192.168.8.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.955/1.258/1.427 ms
```

3 Firewall

3.1 Firewall on and off

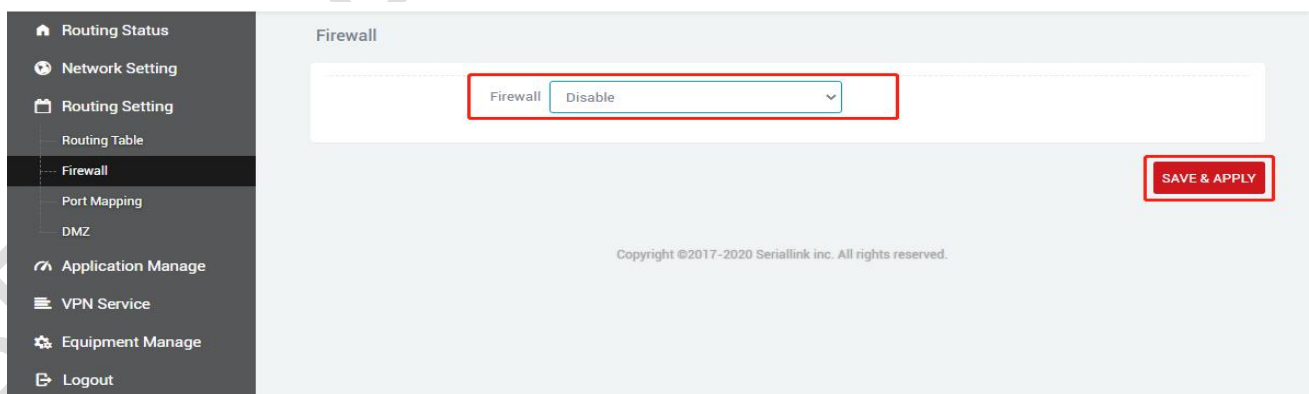
The firewall is enabled by default. When doing DMZ and port mapping, you need to disable the firewall. Steps to disable the firewall are in the navigation bar "Routing Setting"->"Firewall", select the firewall to disable, and click "SAVE & APPLY".



3.2 DMZ setting

The DMZ function can map the WAN port address to a host on the LAN side; all packets to the WAN address will be forwarded to the destination. Set the LAN side host to achieve two-way communication. In fact, a host in the intranet is completely exposed to the Internet and all ports are opened. It is equivalent to all port mapping. It is equivalent to using the public IP directly.

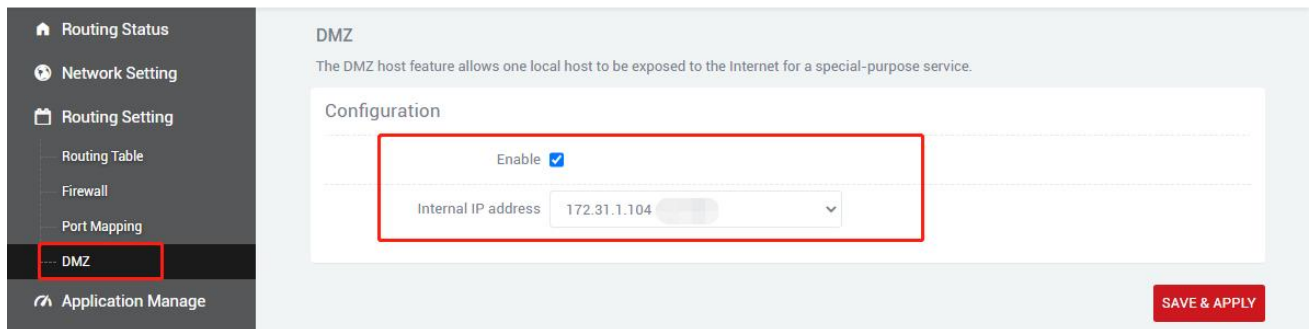
First, you need to disable the firewall.



In the navigation bar, "Route Setting"->"DMZ", click Enable, set the ip address assigned by the lan port to the connected device, and forward all the ports of the connected device, which can be directly accessed through the ip address of the wan port.

Check Enable.

Internal IP address: Fill in the ip assigned by the lan port to the downstream device or the ip of the machine.



Routing Status

Network Setting

Routing Setting

Routing Table

Firewall

Port Mapping

DMZ

Application Manage

DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service.

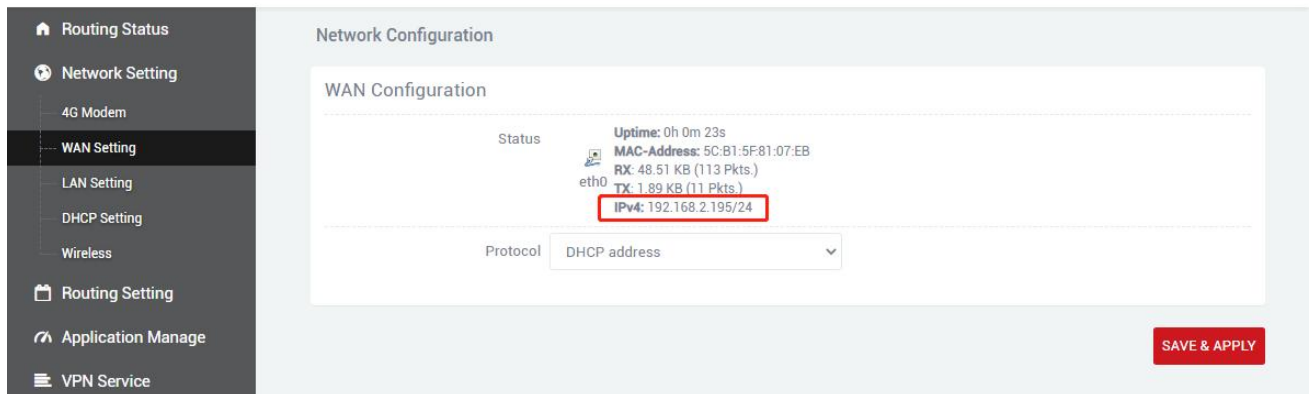
Configuration

Enable

Internal IP address 172.31.1.104

SAVE & APPLY

View wan port IP Address:



Routing Status

Network Setting

4G Modem

WAN Setting

LAN Setting

DHCP Setting

Wireless

Routing Setting

Application Manage

VPN Service

Network Configuration

WAN Configuration

Status

Uptime: 0h 0m 23s

MAC-Address: 5C:B1:5F:81:07:EB

RX: 48.51 KB (113 Pkts.)

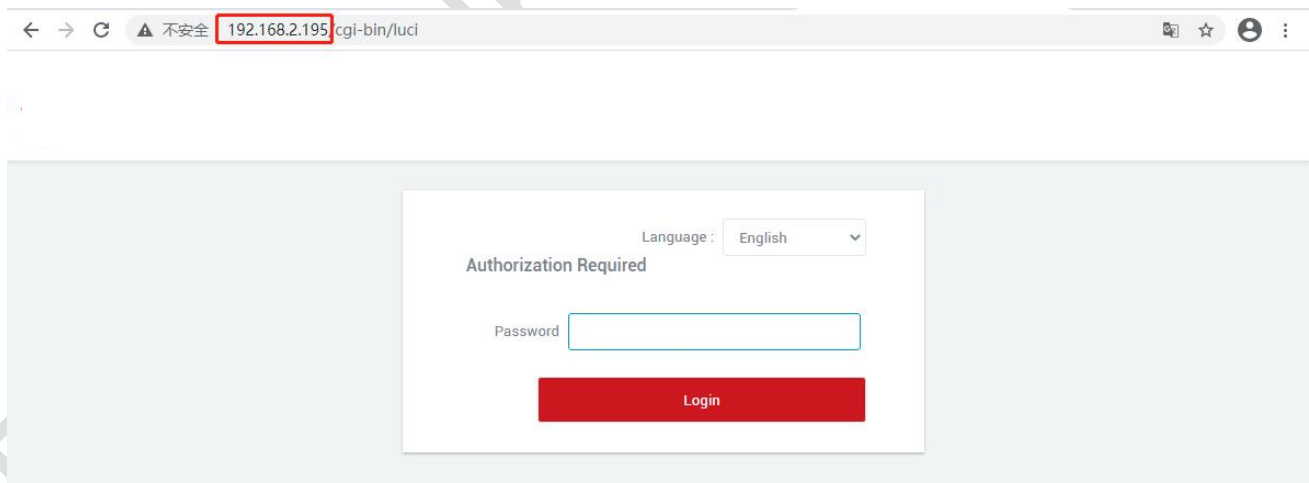
eth0 TX: 1.89 KB (11 Pkts.)

IPv4: 192.168.2.195/24

Protocol DHCP address

SAVE & APPLY

Through the device wan port ip, you can access all the ports of the device just filled in.



← → ↻ ⚠ 不安全 192.168.2.195/cgi-bin/luci

Language: English

Authorization Required

Password

Login

3.3 Port Forwarding

Compared with DMZ, port forwarding is more refined control. Data packets sent to a certain port can be forwarded to a certain host on the LAN side, and different ports can be transferred to different hosts.

First, you need to disable the firewall.



Navigate to the "Routing Settings" - "Port Mapping" setting menu in the navigation bar, and enter the "Port Forwarding" interface to configure.

Name: Specify the name of this rule, you can give a meaningful name.

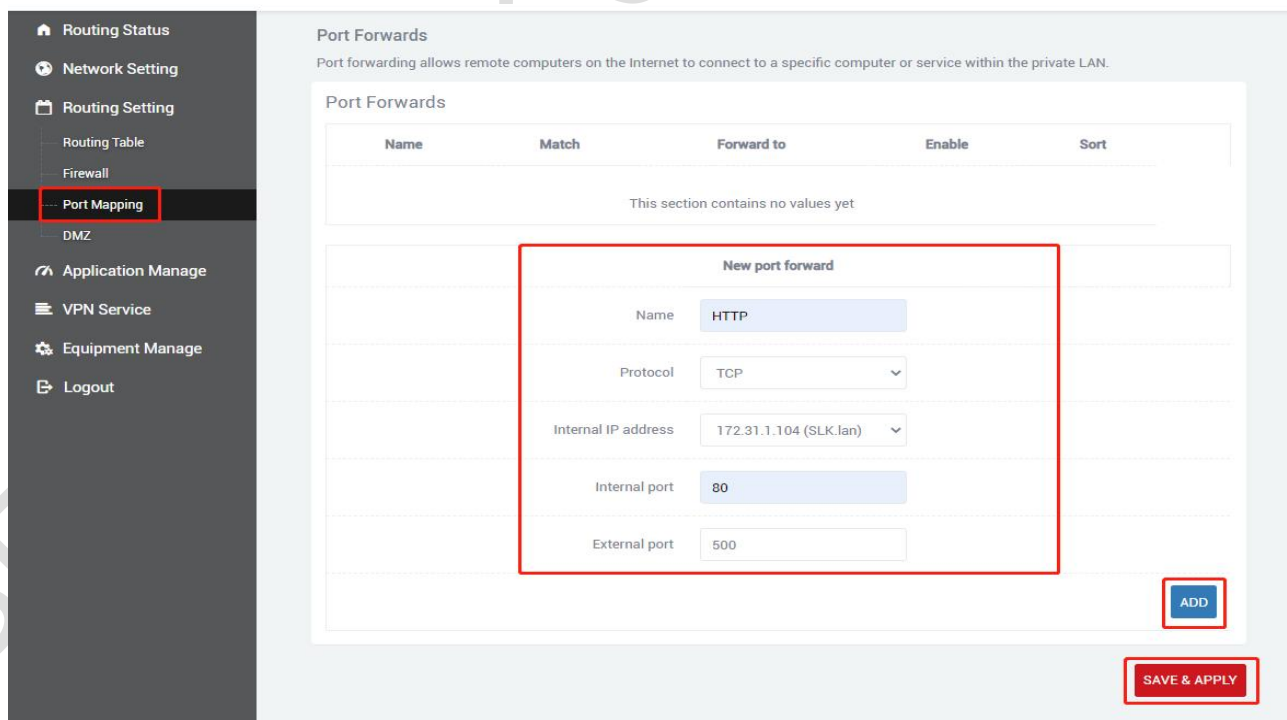
Protocol: Specify the protocol to be forwarded, which can be TCP, UDP, or TCP/UDP.

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

Internal port: the port to be forwarded by the downstream device.

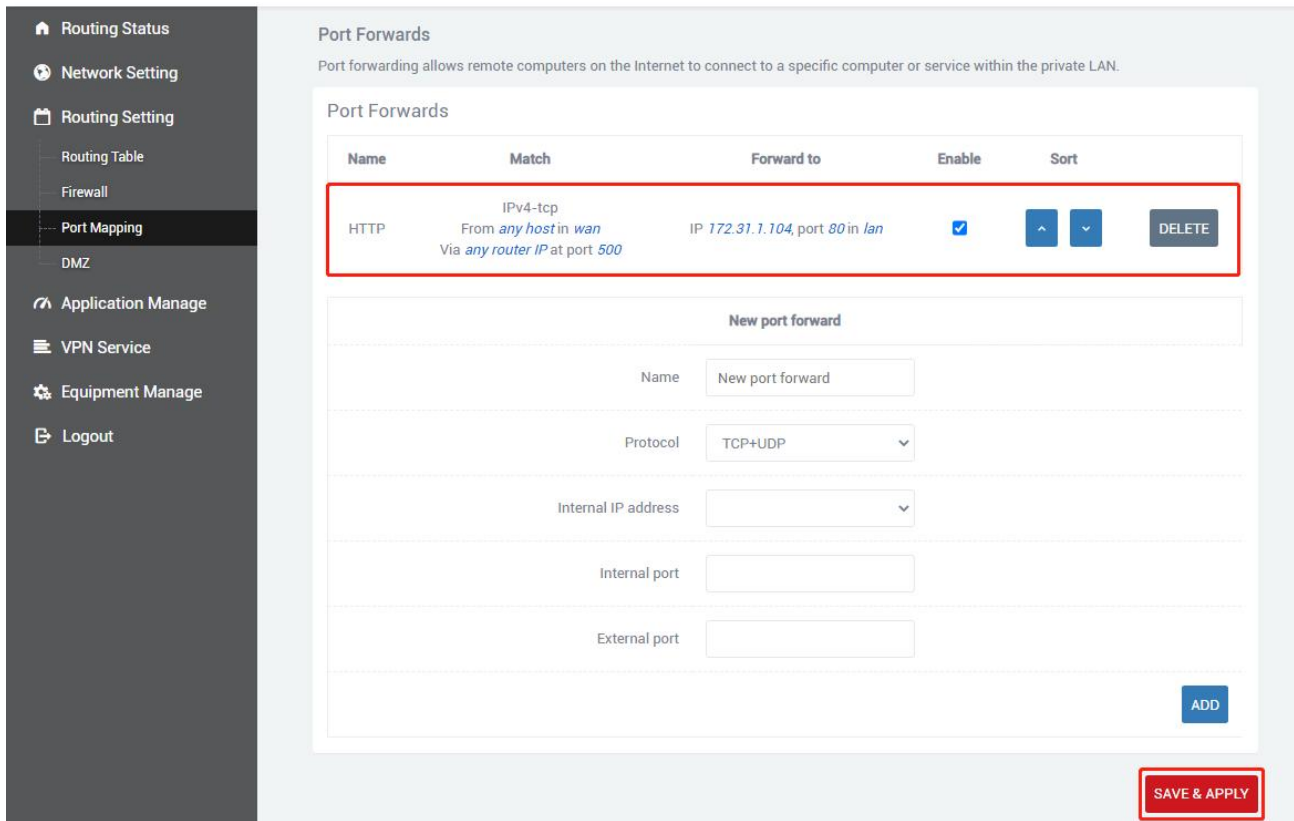
External port: add this external port through the wan port ip to access the downstream device

After configuration, click the "Add" button to add a forwarding rule. Click the "SAVE & APPLY" button to make the rule effective.



After the addition is successful, there will be an additional port forwarding rule, click "Save & Apply" to

make the rule effective.



Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Name	Match	Forward to	Enable	Sort	
HTTP	IPv4-tcp From <i>any host</i> in wan Via <i>any router IP</i> at port 500	IP 172.31.1.104, port 80 in lan	<input checked="" type="checkbox"/>	▲ ▼	DELETE

New port forward

Name:

Protocol:

Internal IP address:

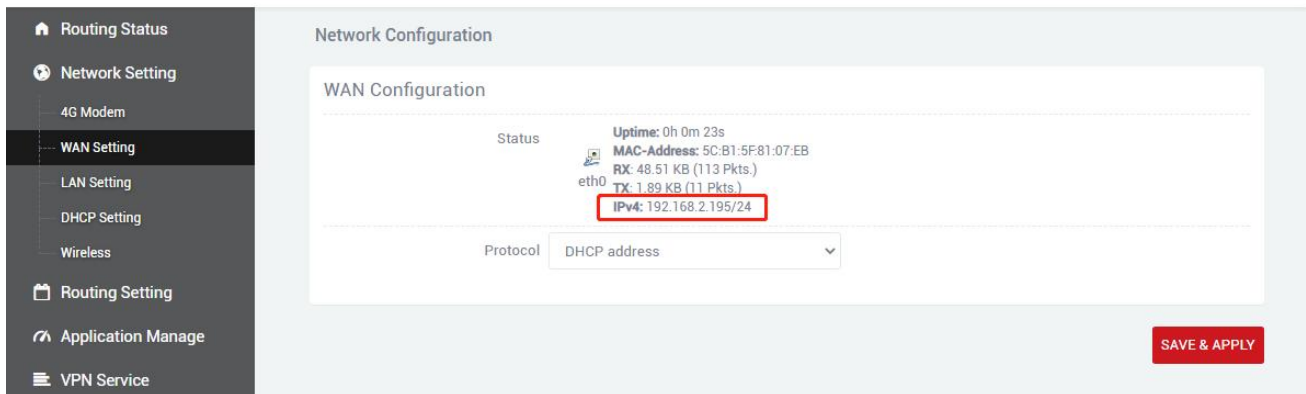
Internal port:

External port:

ADD

SAVE & APPLY

View wan port IP Address:



Network Configuration

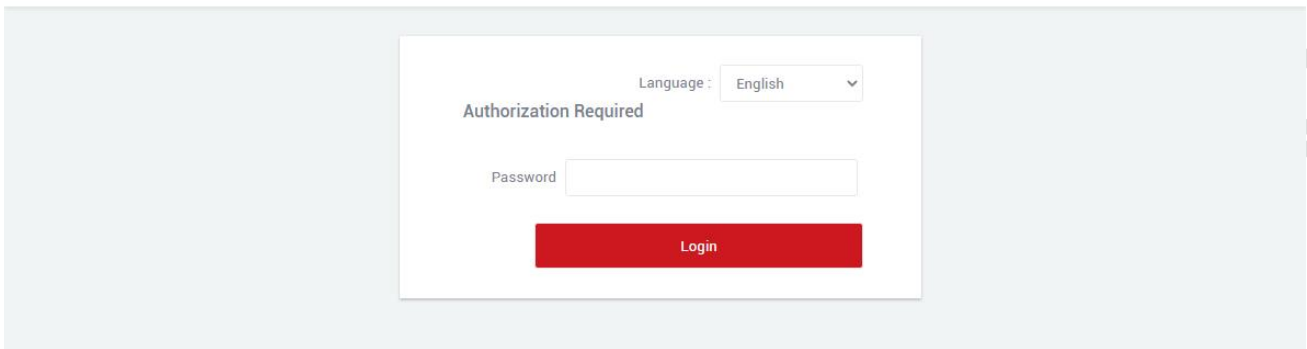
WAN Configuration

Status: Uptime: 0h 0m 23s
MAC-Address: 5C:B1:5F:81:07:EB
eth0 RX: 48.51 KB (113 Pkts.)
TX: 1.89 KB (11 Pkts.)
IPv4: 192.168.2.195/24

Protocol:

SAVE & APPLY

Through the wan port ip: remote port number, you can access the port number opened by the port forwarding device just configured.(access 192.168.2.195:500 through 172.31.1.104:80)



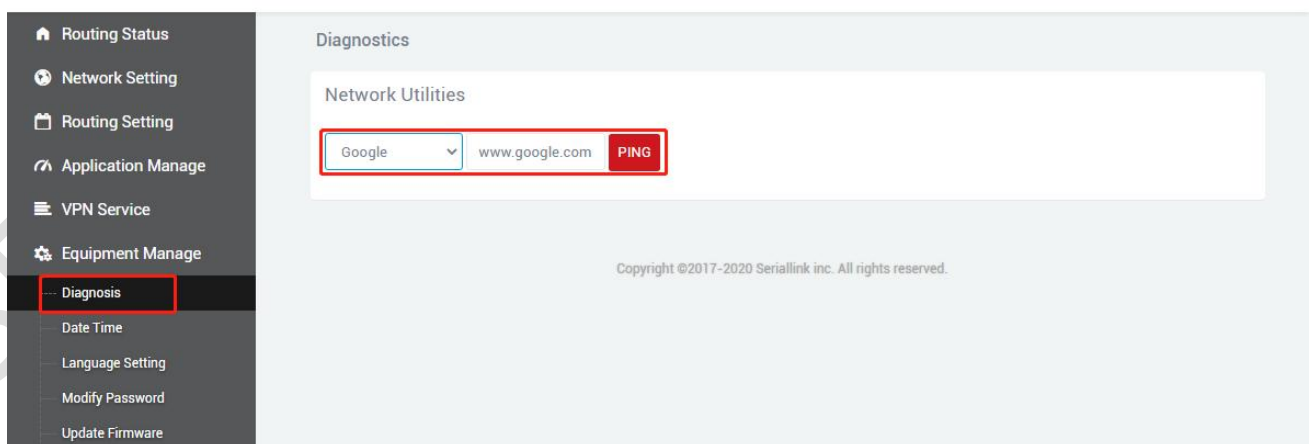
3.4 Intranet penetration (frp)

Frp uses machines behind the internal network or firewall to provide http or https services in multiple external network environments. For http and https services, it supports domain-based virtual hosts and supports custom domain name binding, so that multiple domain names share a port 80; Use machines behind the internal network or firewall to provide tcp and udp services in the external network environment, such as accessing the host in the company's internal network environment through ssh at home.

Frp mainly realizes the functions: the external network accesses the internal network machine through ssh; the external network accesses the internal network machine through the public network address plus the port number and the port forwarded by frp; the custom binding domain name accesses the internal network web service.

The prerequisite for configintranet penetration is to ensure that the router can access the Internet. If the router cannot access the Internet, the intranet penetration cannot be done. Navigation bar "Equipment Manage"->"diagnosis"; and disable the firewall, navigation bar "routing settings"->"firewall".

Ping Google on the diagnostic page. If it can ping, it means that the device can go online.



Disable firewall:

Routing Status
Network Setting
Routing Setting
Routing Table
Firewall
Port Mapping
DMZ
Application Manage

Firewall

Firewall Disable

SAVE & APPLY

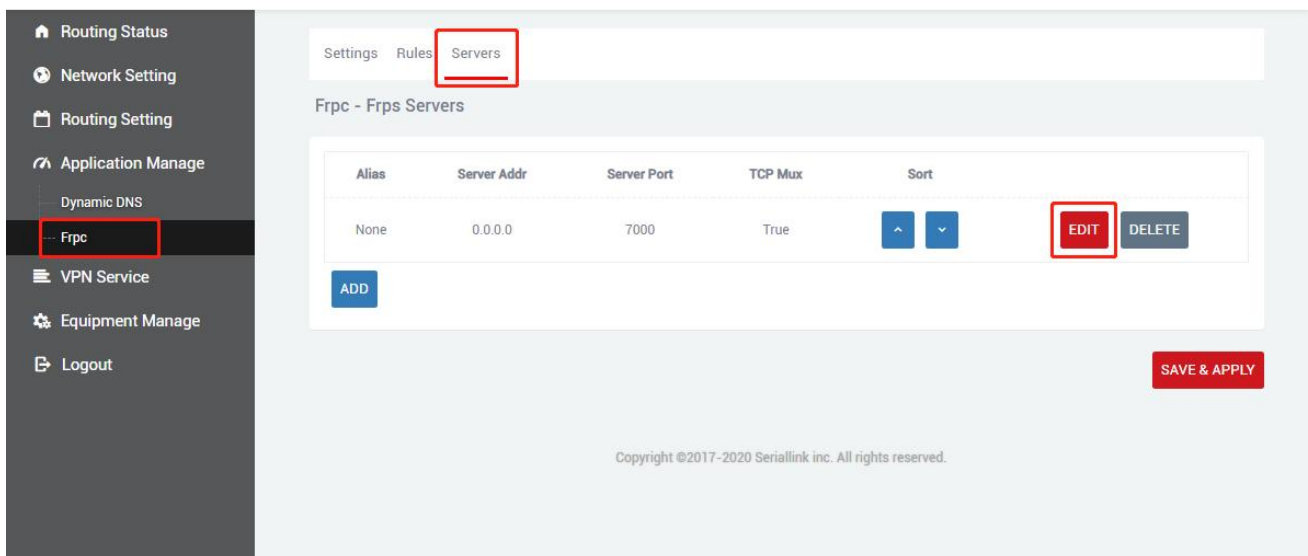
Copyright ©2017-2020 Seriallink inc. All rights reserved.

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.

Frp client configuration is as follows:

(1) The client needs to add the server configuration first to connect to the server, the navigation bar "Application Manage"->"Frpc", select the Servers, there is an empty server by default, you can click to modify it directly, or You can directly delete and add one yourself.



Settings Rules Servers

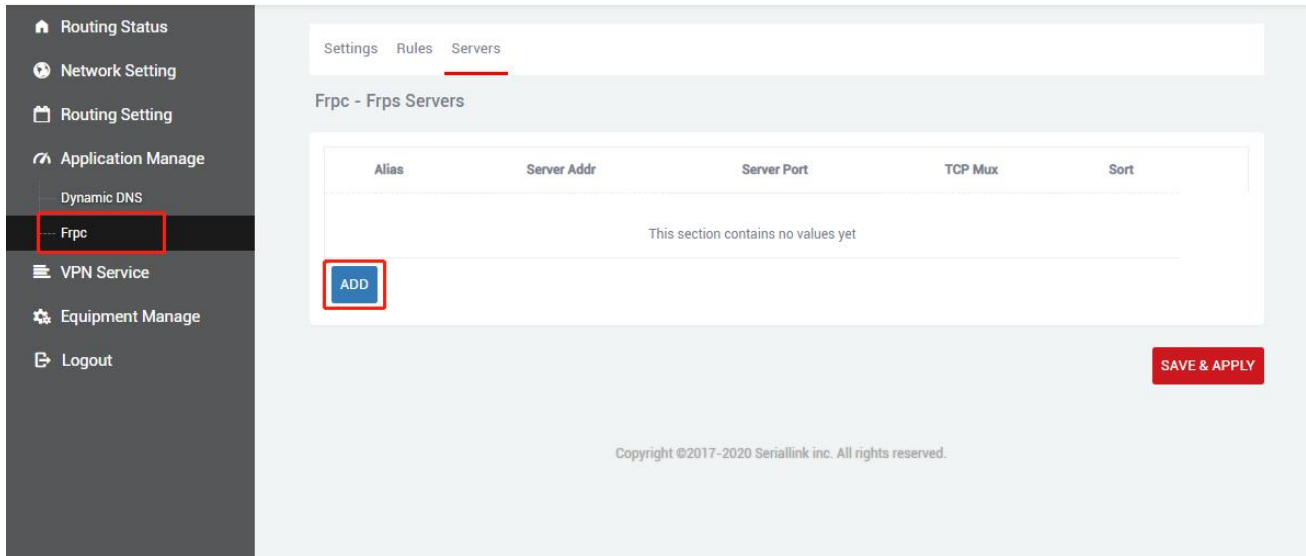
Frpc - Frps Servers

Alias	Server Addr	Server Port	TCP Mux	Sort
None	0.0.0.0	7000	True	↑ ↓

ADD EDIT DELETE

SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.



Routing Status

Network Setting

Routing Setting

Application Manage

Dynamic DNS

Frpc

VPN Service

Equipment Manage

Logout

Settings Rules Servers

Frpc - Frpc Servers

Alias	Server Addr	Server Port	TCP Mux	Sort
This section contains no values yet				

ADD

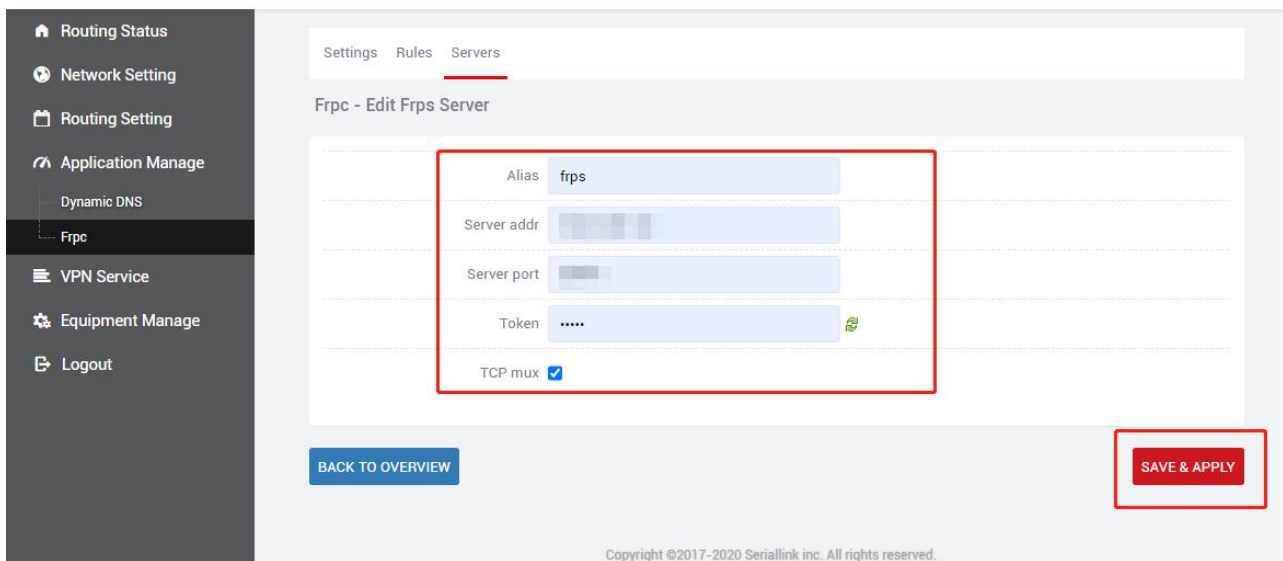
SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.

(2) After clicking "Add" or "Modify", a page for Edit-Frpc Server will pop up. Configure it according to the settings of the server. After the configuration is complete, click "SAVE & APPLY".

Alias: Customize a frp server alias, which will be used when using the server.

Server addr, Server port, Token, Tcps mux Must be consistent with the server.



Routing Status

Network Setting

Routing Setting

Application Manage

Dynamic DNS

Frpc

VPN Service

Equipment Manage

Logout

Settings Rules Servers

Frpc - Edit Frpc Server

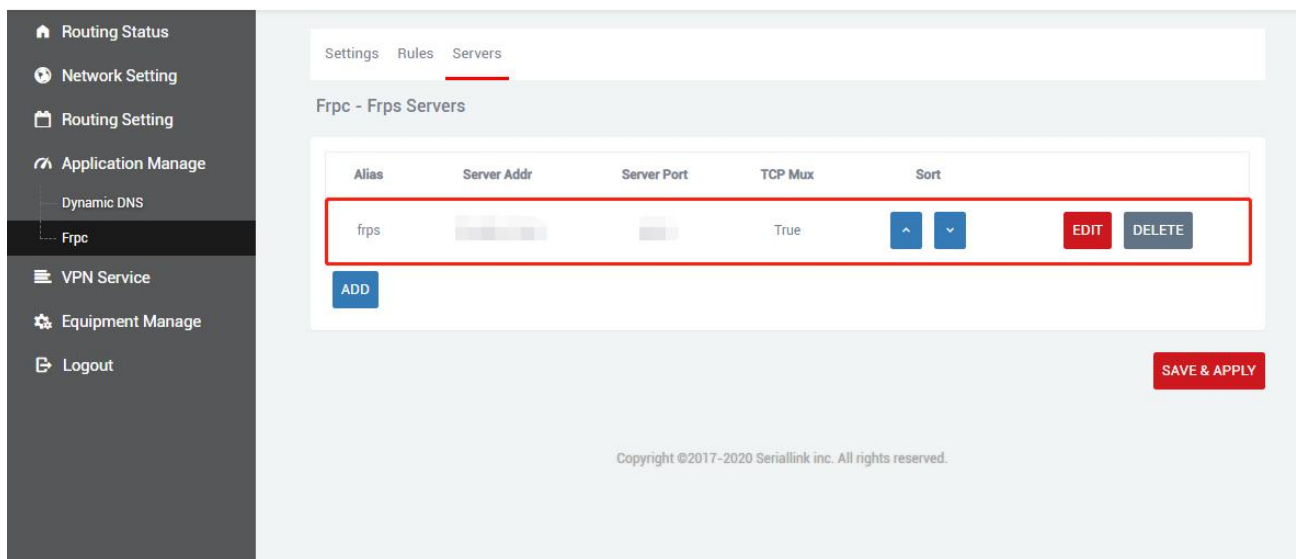
Alias	frps
Server addr	
Server port	
Token
TCP mux	<input checked="" type="checkbox"/>

BACK TO OVERVIEW

SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.

(3) After successful configuration, there will be a server, click "SAVE & APPLY" to let the server run.



(4) Next, enter the "Settings" page of "Intranet Penetration", start the frpc client, and configure according to the following figure. After the configuration is completed, click "Save & Apply", and the "Settings" page will appear after the configuration is completed The service is running", which proves that the frpc client has been started.

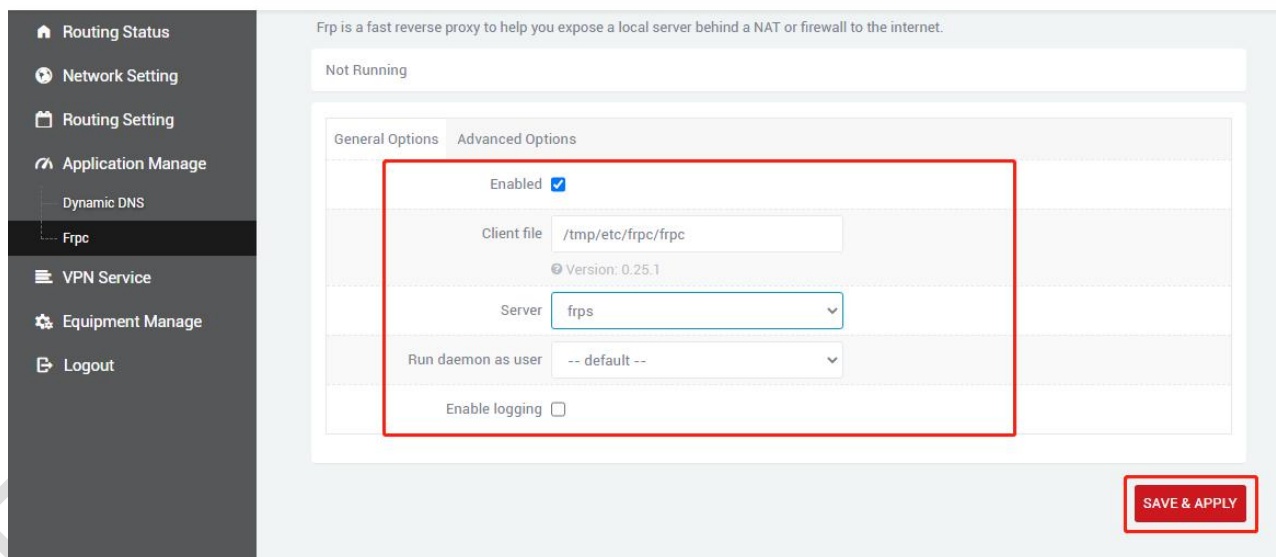
Enabled: Enable frpc service.

Server: Fill in the server alias you just customized.

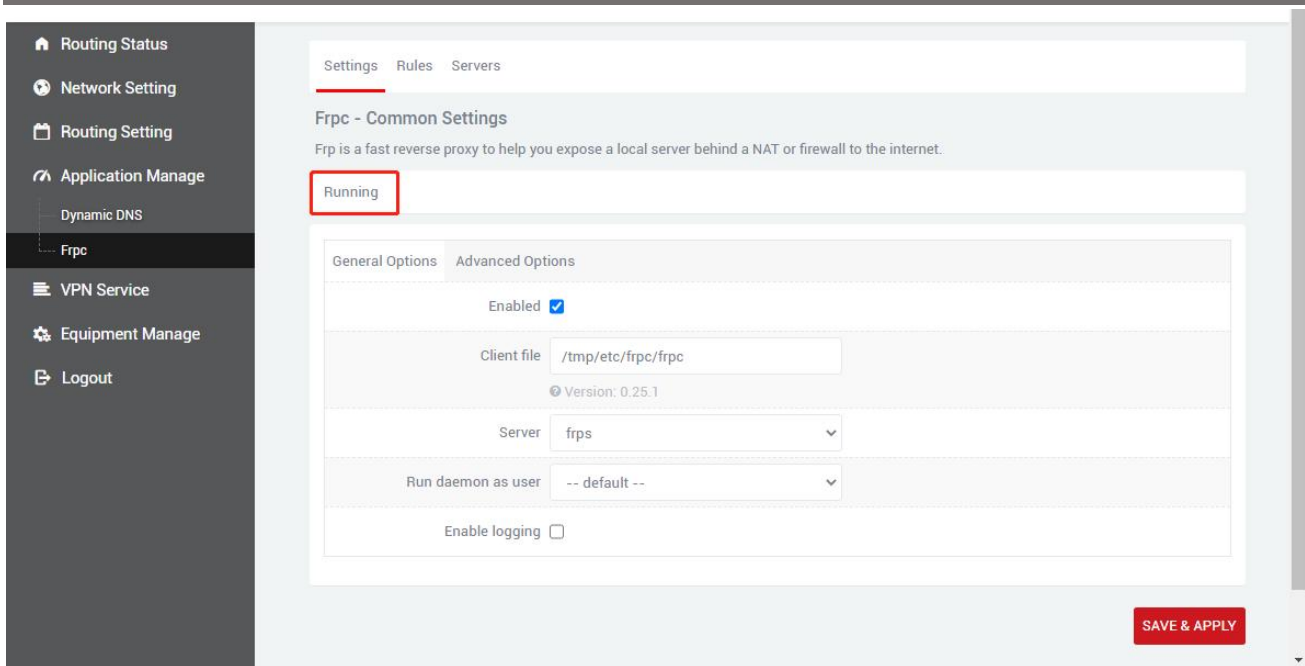
Run daemon as user: One group is the default choice, you can choose according to your needs.

Enable logging: Check according to your needs.

Click "SAVE & APPLY" after configuration.



The "Setting" page shows that it is running, indicating that frpc is started.



Settings Rules Servers

Frpc - Common Settings

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

Running

General Options Advanced Options

Enabled

Client file

Version: 0.25.1

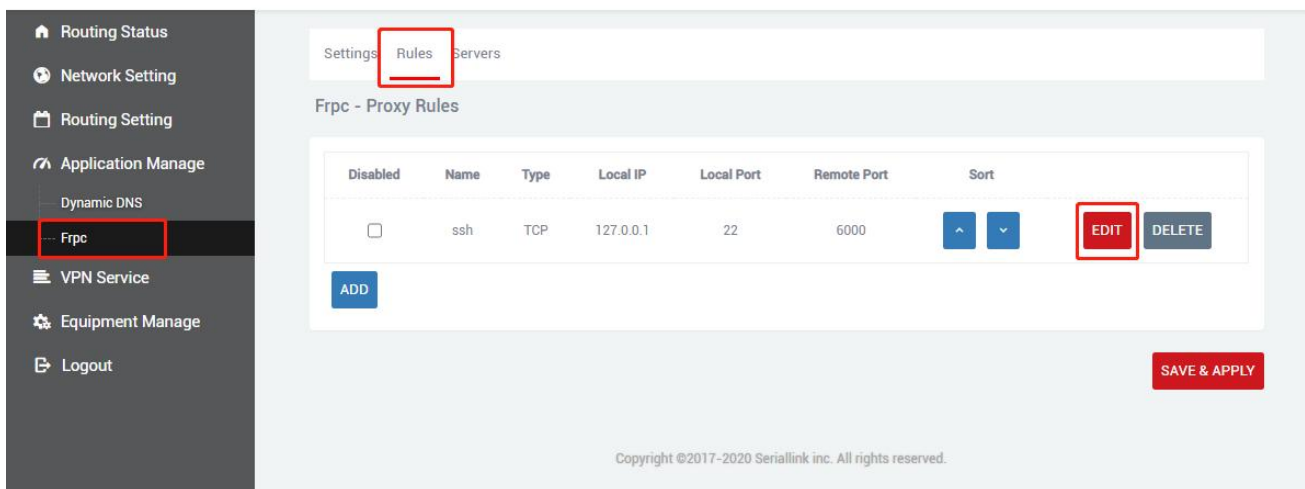
Server

Run daemon as user

Enable logging

SAVE & APPLY

(5) Next, enter the "Rules" page of "Intranet Penetration". The page itself has a rule. You can modify this rule or delete this rule and add a new rule. The final effect of the two methods is the same. Choose to modify the original rules or add new rules.



Settings Rules Servers

Frpc - Proxy Rules

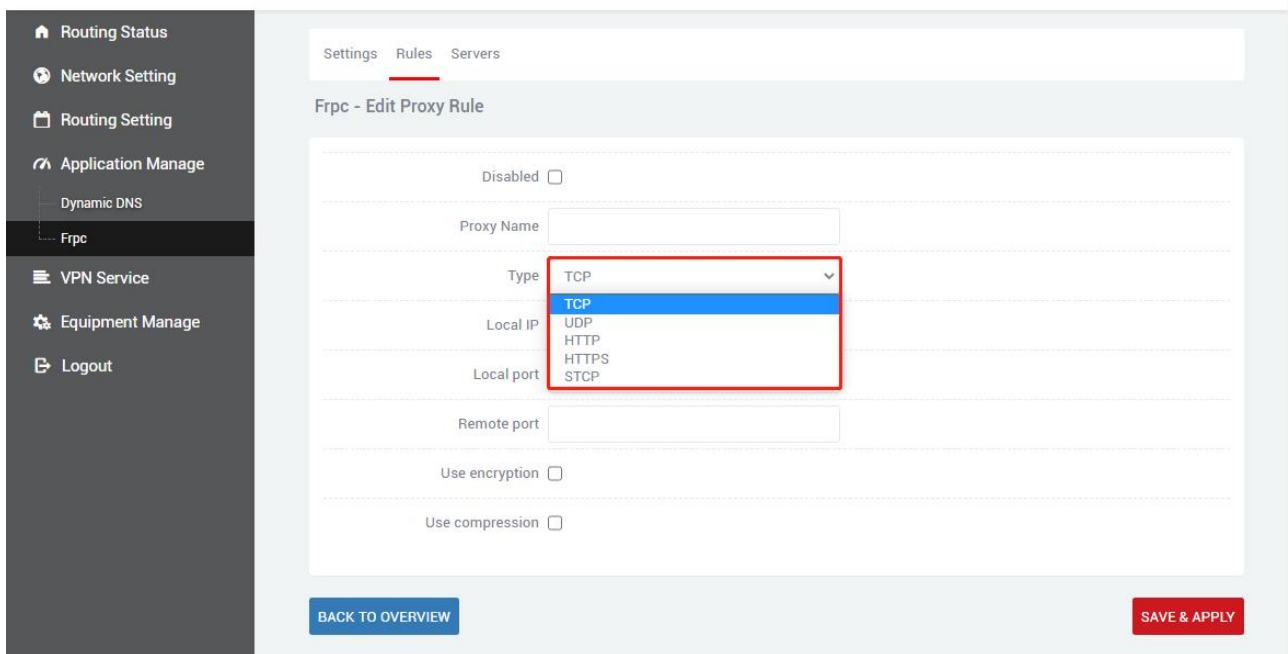
Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	ssh	TCP	127.0.0.1	22	6000	<input type="button" value="^"/> <input type="button" value="v"/>	<input checked="" type="button" value="EDIT"/> <input type="button" value="DELETE"/>

ADD

SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.

(6) After adding, a "Edit Proxy Rules" page will pop up, and there will be different protocol types, and different protocol types implement different functions.



3.4.1 Add TCP proxy protocol

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

On the "Edit Proxy Rules" page, configure as shown below according to your needs. After the configuration is complete, click "Save & Apply" and you will return to the "Proxy Rules" page. There will be an extra rule on the page. Click "Save &" again. Apply" to make the rule effective, and finally through the public network ip: port number (format: 111.111.111.111:6001 where 111.111.111.111 is the public network address) to access the local port opened by the local device. You can add multiple tcp rules, just ensure that the remote port is not the same. If the remote port is the same as the previous setting, the latest one will overwrite the previous one, and the previous rule will not take effect.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose TCP protocol.

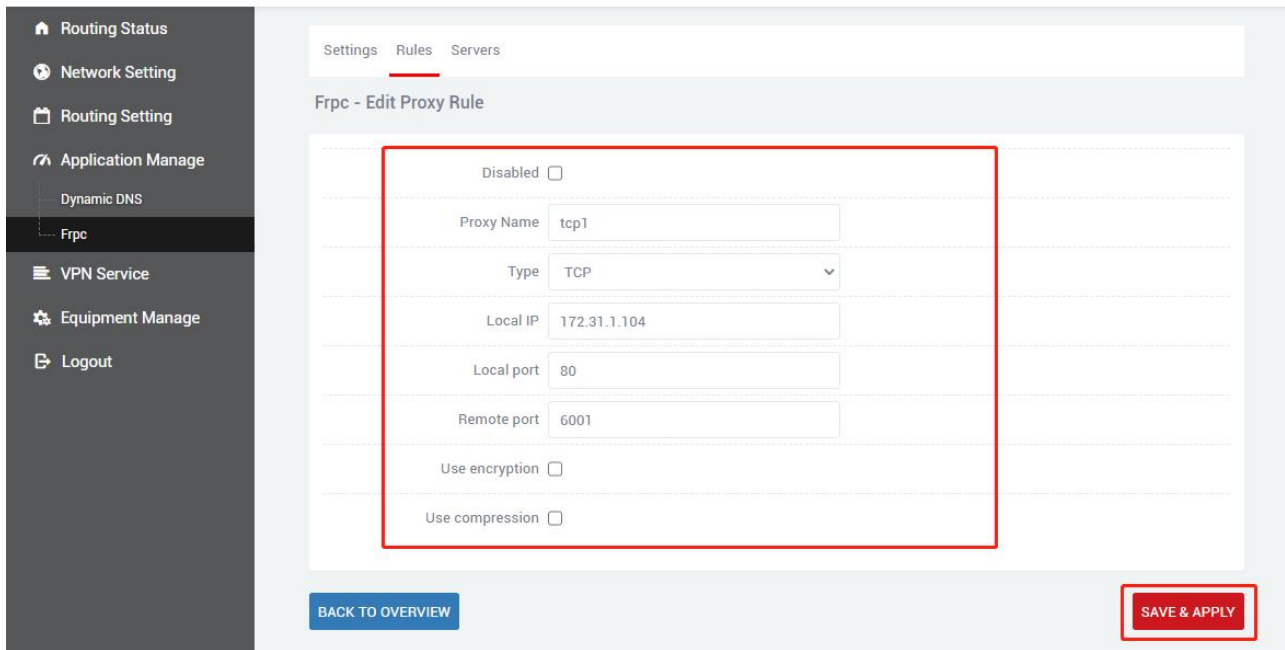
Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

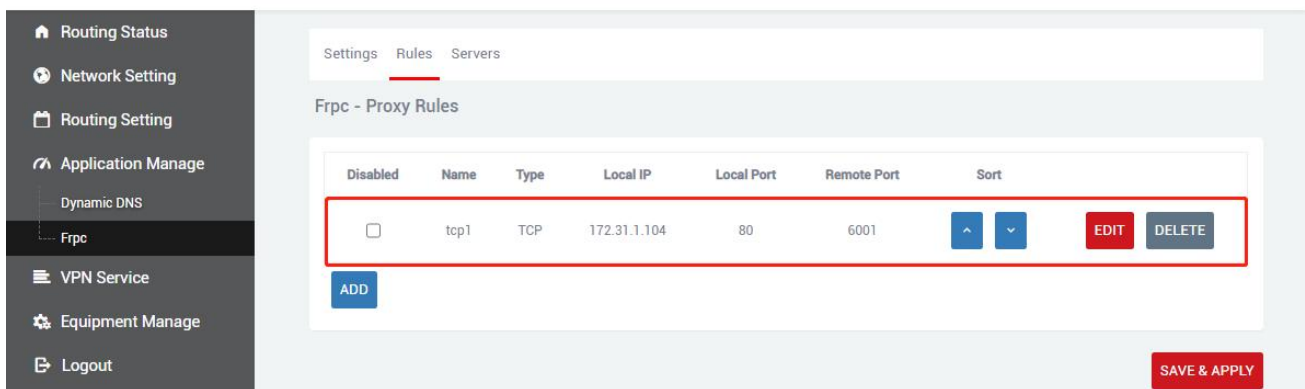
Remote port: Fill in a port number that is not used by the server, and you can access the Local port opened by the internal device through the public network ip and this remote port number.

Use encryption, Use compression: These two are checked according to your needs.

Click "SAVE & APPLY" after configuration.

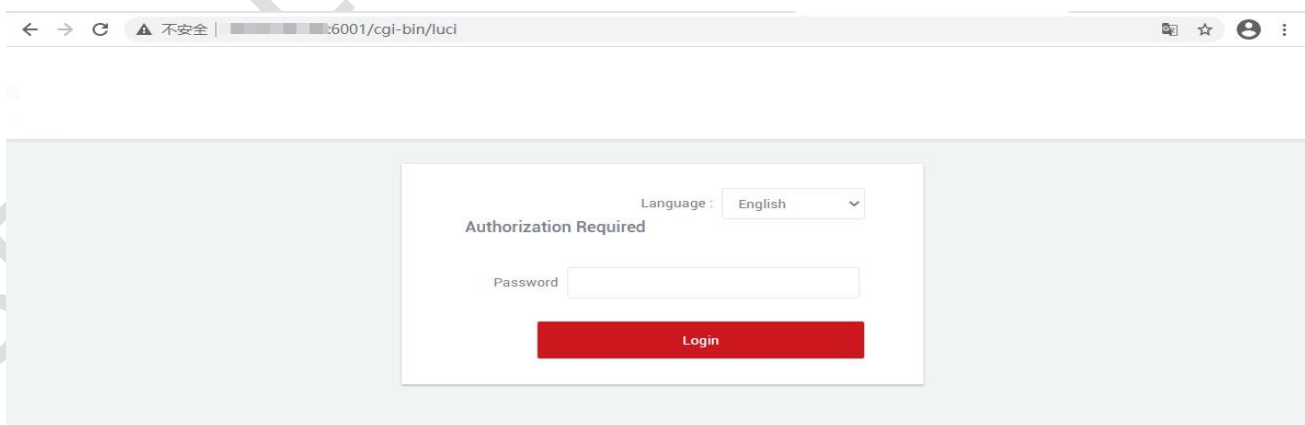


After successfully adding a new rule, click "SAVE & APPLY" to make the rule effective.



Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort	
<input type="checkbox"/>	tcp1	TCP	172.31.1.104	80	6001	<input type="button" value="↑"/> <input type="button" value="↓"/>	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

Through the public network ip: remote port, you can access the corresponding device's open port on the public network (that is, 111.111.111.111:6001 to access 172.31.1.104:80)



You can add multiple tcp rules, and you need to ensure that the remote port number is not repeated with the previous setting. If it is repeated, the previous rules will be overwritten and the previous rules will

not take effect. You can connect to the device through ssh, the same is the public network ip: remote port number (111.111.111.111:6000).

3.4.2 Add STCP proxy protocol

(1) STCP needs to configure the client and access terminal. Among them, 192.168.2.99 (the device connected to the lan port) is used as the client, and the PC is the access terminal. The access terminal can access the client by binding the local IP and port.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

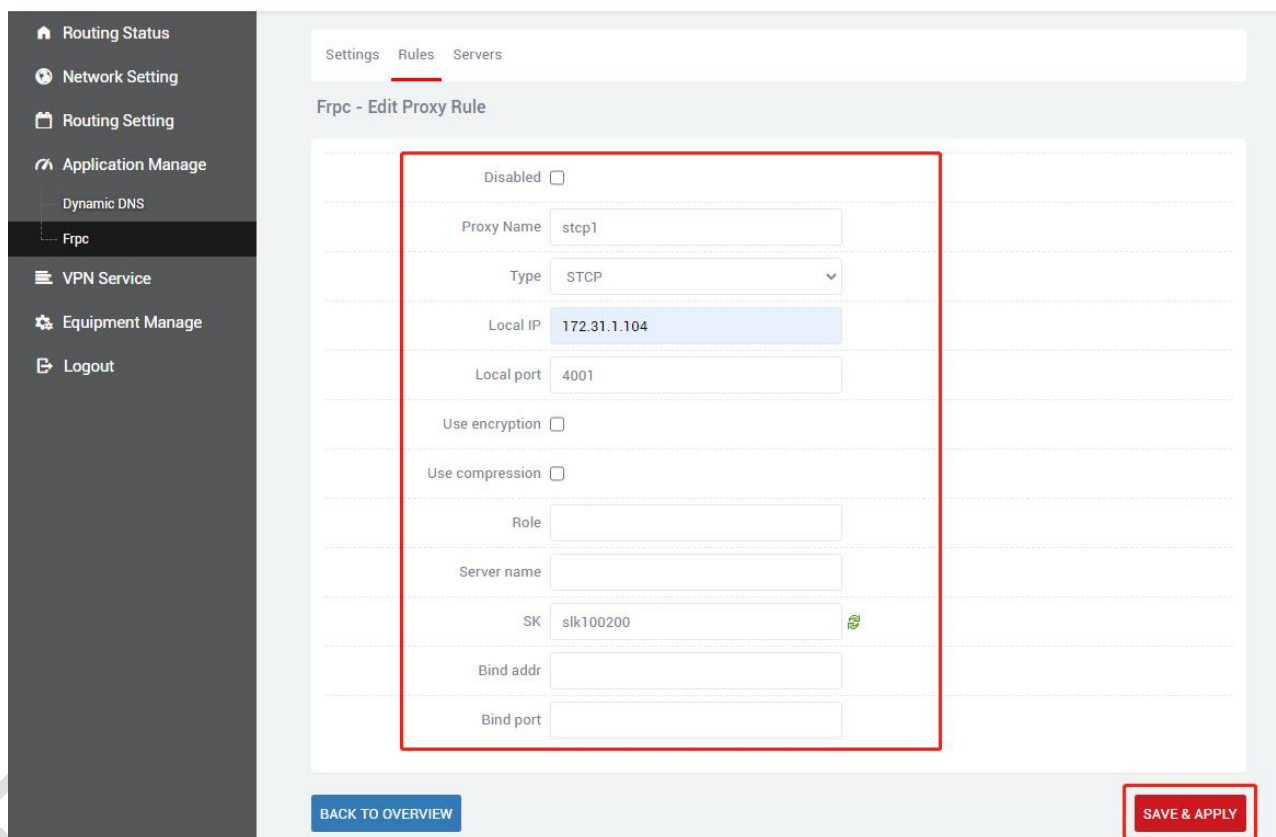
Local port: Fill in which port to remotely access the device.

SK: Set a password, which is needed when the client accesses it.

Use encryption, Use compression: These two are checked according to your needs.

Role, Server name, Bind addr, Bind port: These four parameters do not need to be filled in as the client.

Click "SAVE & APPLY" after configuration.



A new rule is successfully generated, click "Save & Apply" to make the rule effective.

Settings Rules Servers

Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort				
<input type="checkbox"/>	tcp1	TCP	172.31.1.104	80	6001		↑	↓	EDIT	DELETE
<input type="checkbox"/>	stcp1	STCP	172.31.1.104	4001	Not set				EDIT	DELETE

ADD

SAVE & APPLY

If the PC wants to be the access terminal to access the router's downstream equipment, it needs to be a frp client, and it is also the stcp protocol, but it must set the visitor role and bind the local address and port. Windows frp files can be downloaded from the company's official website. After downloading, open the frpc_602.ini configuration file for configuration.

frp_0.25.1_windows_amd64

名称	修改日期	类型	大小
frpc.exe	2020-09-03 9:56	应用程序	9,962 KB
frpc.ini	2020-09-07 12:52	配置设置	2 KB
frpc_602.ini	2020-12-08 17:07	配置设置	1 KB
frpc_full.ini	2019-03-15 17:10	配置设置	7 KB
frps.exe	2019-03-15 17:08	应用程序	10,694 KB
frps.ini	2019-03-15 17:10	配置设置	1 KB
frps_full.ini	2019-03-15 17:10	配置设置	3 KB
LICENSE	2019-03-15 17:10	文件	12 KB

frpc_602.ini - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
#Connect to the server
[common]
#Server public IP address
server_addr=
#Server port
server_port=5443
#The server provides a token for verification
token=slk100200
#Connect to the server through the tcp protocol
protocol=tcp
#Consistent with server configuration
tcp_mux=true
#Prevent exit after a connection failure
login_fail_exit=false
```

Consistent with public network server

#Connect client 1-192.168.2.99

[stcp1_visitor]

#Select STCP protocol

type =stcp fill in stcp

#As a visitor

role=visitor the role of the visitor should be configured as a visitor

#Agent name of client 1

server_name=stcp1 fill in the Proxy Name just set

#Same as the SK of client 1

sk=slk100200 fill in the SK set in the client section just now

#Bind the local address and port to access client 1

bind_addr=127.0.0.1

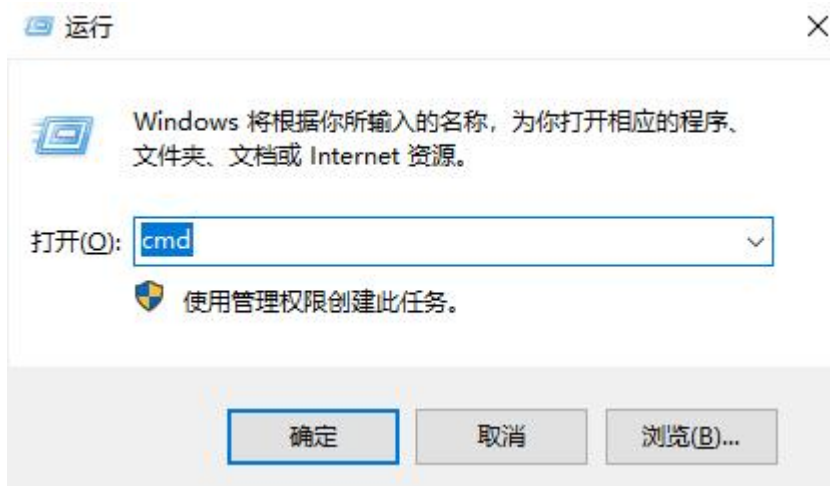
bind_port=6006 access the client by binding local ip and port

C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64

名称	修改日期	类型	大小
frpc.exe	2020-09-03 9:56	应用程序	9,962 KB
frpc.ini	2020-09-07 12:52	配置设置	2 KB
frpc_602.ini	2020-12-16 10:44	配置设置	1 KB
frpc_full.ini	2019-03-15 17:10	配置设置	7 KB
frps.exe	2019-03-15 17:08	应用程序	10,694 KB
frps.ini	2019-03-15 17:10	配置设置	1 KB
frps_full.ini	2019-03-15 17:10	配置设置	3 KB
LICENSE	2019-03-15 17:10	文件	12 KB

cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64

Use the shortcut key "win+R" and enter "cmd" to quickly open the cmd command line.



Enter in the command line: "cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64", then enter "frpc.exe -c frpc_602.ini".

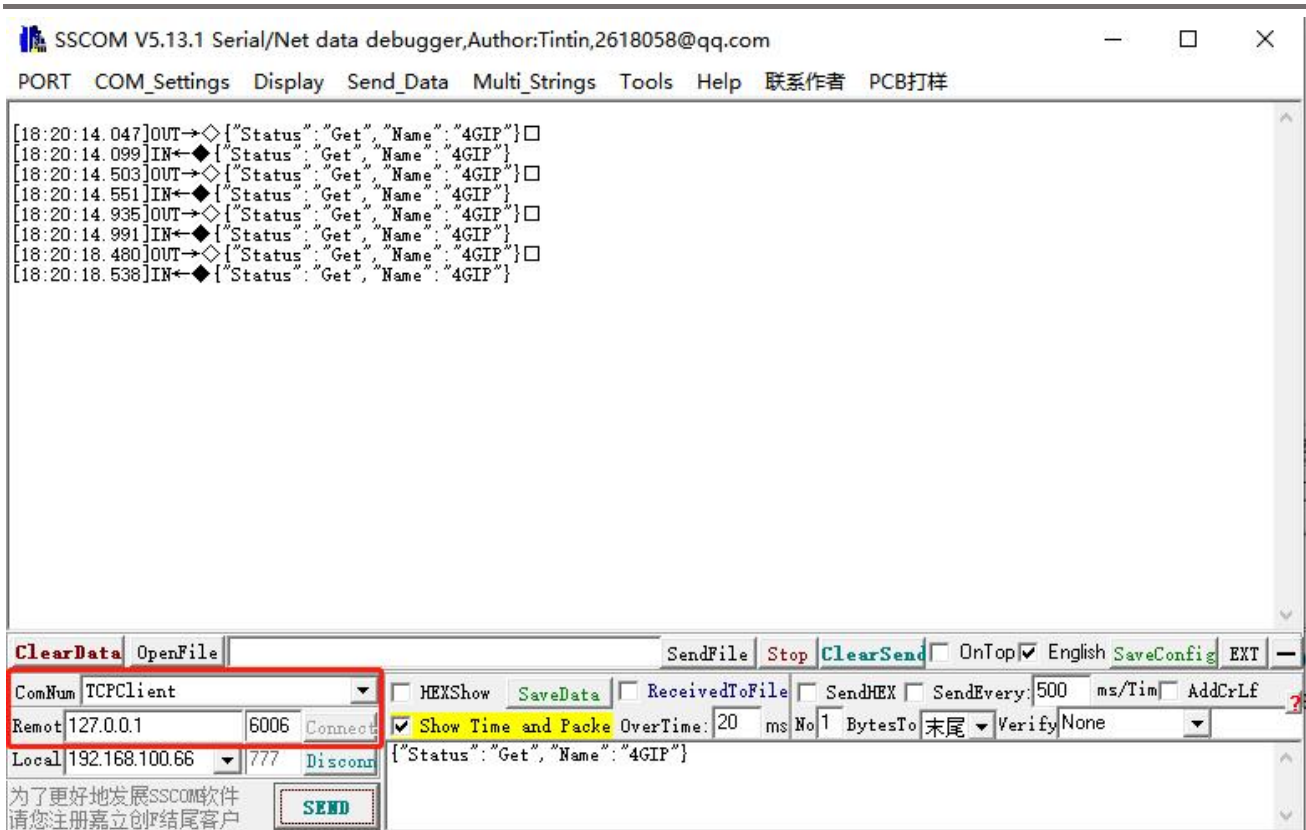
```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.19041.264]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64>
```

```
选择管理员: C:\Windows\system32\cmd.exe - frpc.exe -c frpc_602.ini
Microsoft Windows [版本 10.0.19041.264]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64>frpc.exe -c frpc_602.ini
2020/12/17 15:02:04 [I] [service.go:221] login to server success, get run id [c7b44136f74c7fa0], server udp port [0]
2020/12/17 15:02:04 [I] [visitor_manager.go:69] [stcp1_visitor] start visitor success
2020/12/17 15:02:04 [I] [visitor_manager.go:112] visitor added: [stcp1_visitor]
```

Access the client according to the local address and port bound by frpc_602.ini



(2) If there are two routers, one router wants to remotely access the other router or the downstream equipment of the other router, then one will be the stcp access terminal and the other will be the stcp client. The configuration is as follows

① Configure the client

Add new rule

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

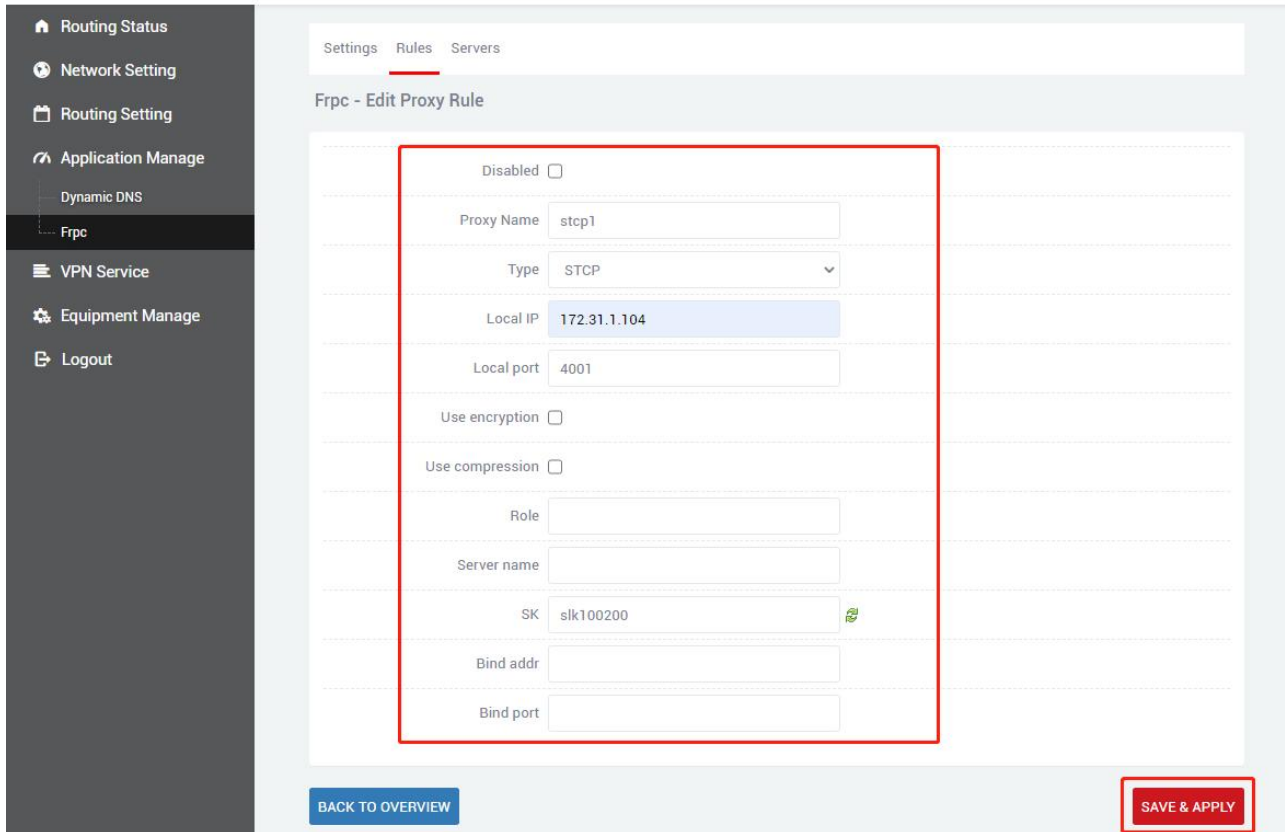
Local port: Fill in which port to remotely access the device.

SK: Set a password, which is needed when the client accesses it.

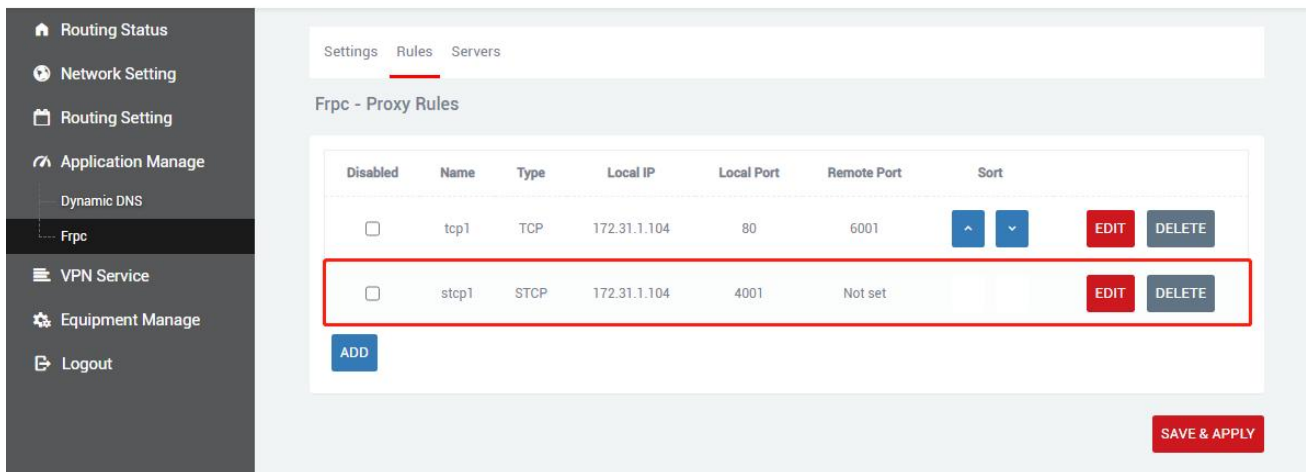
Use encryption, Use compression: These two are checked according to your needs.

Role, Server name, Bind addr, Bind port: These four parameters do not need to be filled in as the client.

Click "SAVE & APPLY" after configuration.



A new rule is successfully generated, click "Save & Apply" to make the rule effective.



Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort				
<input type="checkbox"/>	tcp1	TCP	172.31.1.104	80	6001		^	v	EDIT	DELETE
<input type="checkbox"/>	stp1	STCP	172.31.1.104	4001	Not set				EDIT	DELETE

② Configure access point

The binding address can be the ip address of your own machine, or the ip assigned by the lan port to the connected device.

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose STCP protocol.

Local IP, Local port: These two do not need to be filled in as the access point.

Role: The role of the visitor should be filled in "visitor".

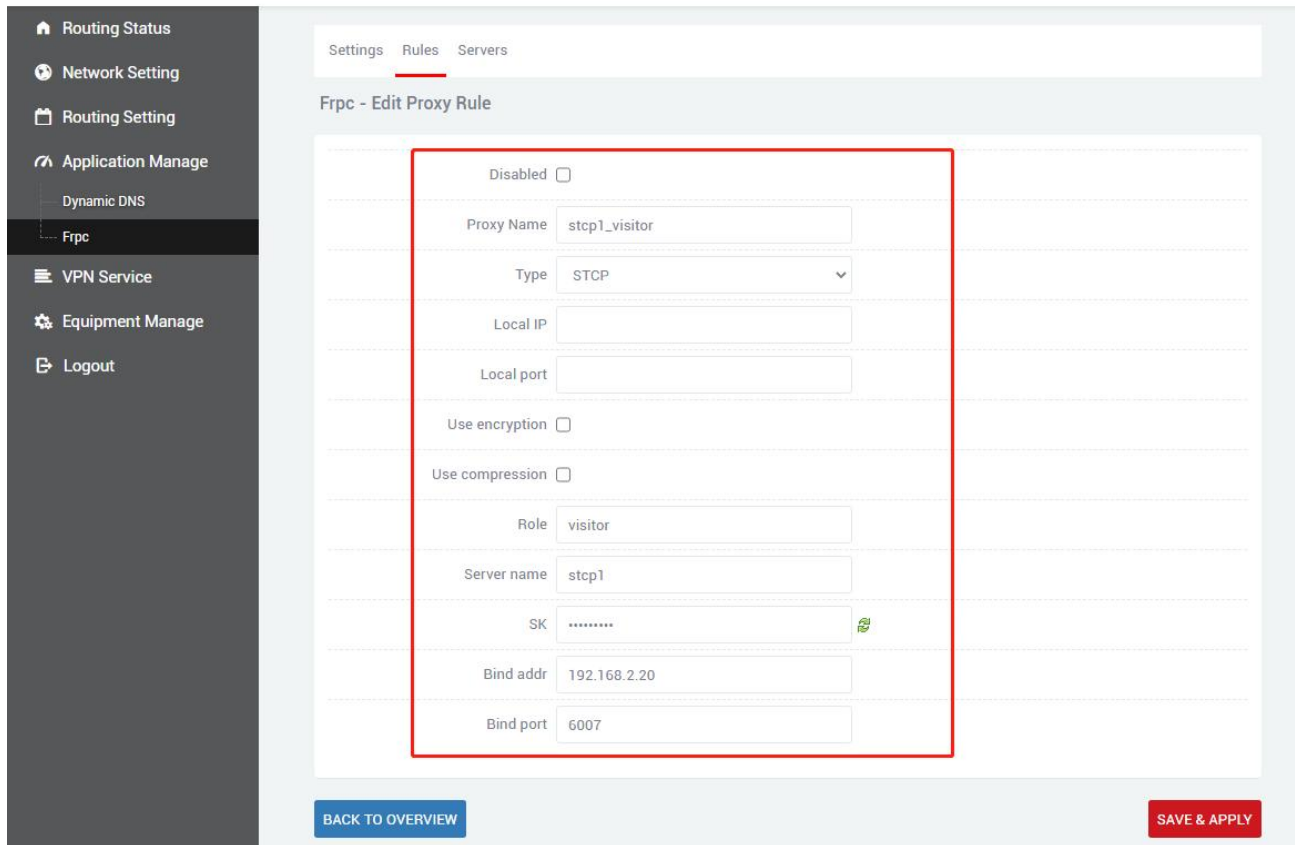
Server name: "Proxy Name" set by the client.

SK: Fill in the "SK" set by the client to be consistent

Bind addr, Bind port: Bind the ip and port of the machine, the client can be accessed through this ip and port.

Use encryption, Use compression: These two are checked according to your needs.

Click "SAVE & APPLY" after configuration.



Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name stcp1_visitor

Type STCP

Local IP

Local port

Use encryption

Use compression

Role visitor

Server name stcp1

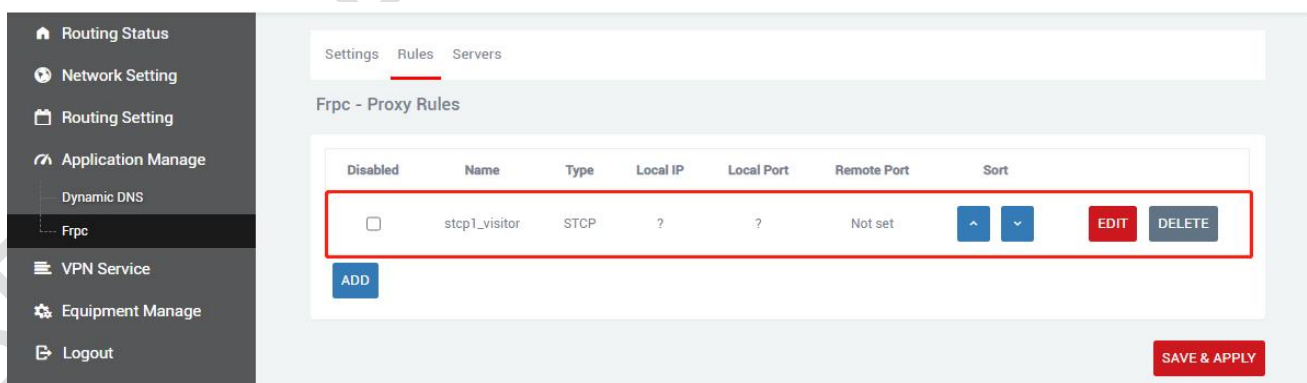
SK

Bind addr 192.168.2.20

Bind port 6007

BACK TO OVERVIEW SAVE & APPLY

A new rule is successfully generated, click "Save & Apply" to make the rule effective.



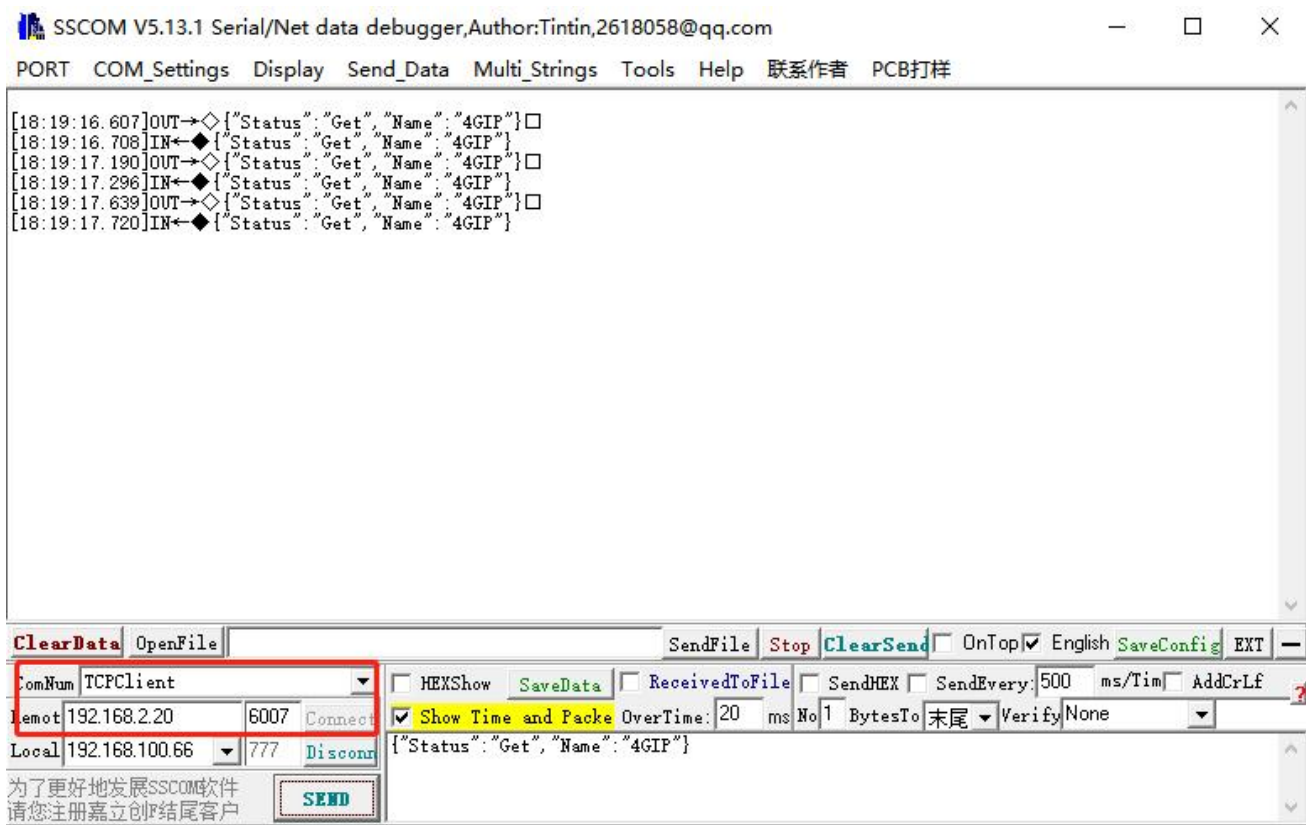
Settings Rules Servers

Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort
<input type="checkbox"/>	stcp1_visitor	STCP	?	?	Not set	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

ADD SAVE & APPLY

Access the client through the bound ip address and bound port of the access terminal.



3.4.3 Add UDP proxy protocol

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

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

Type: Choose UDP protocol.

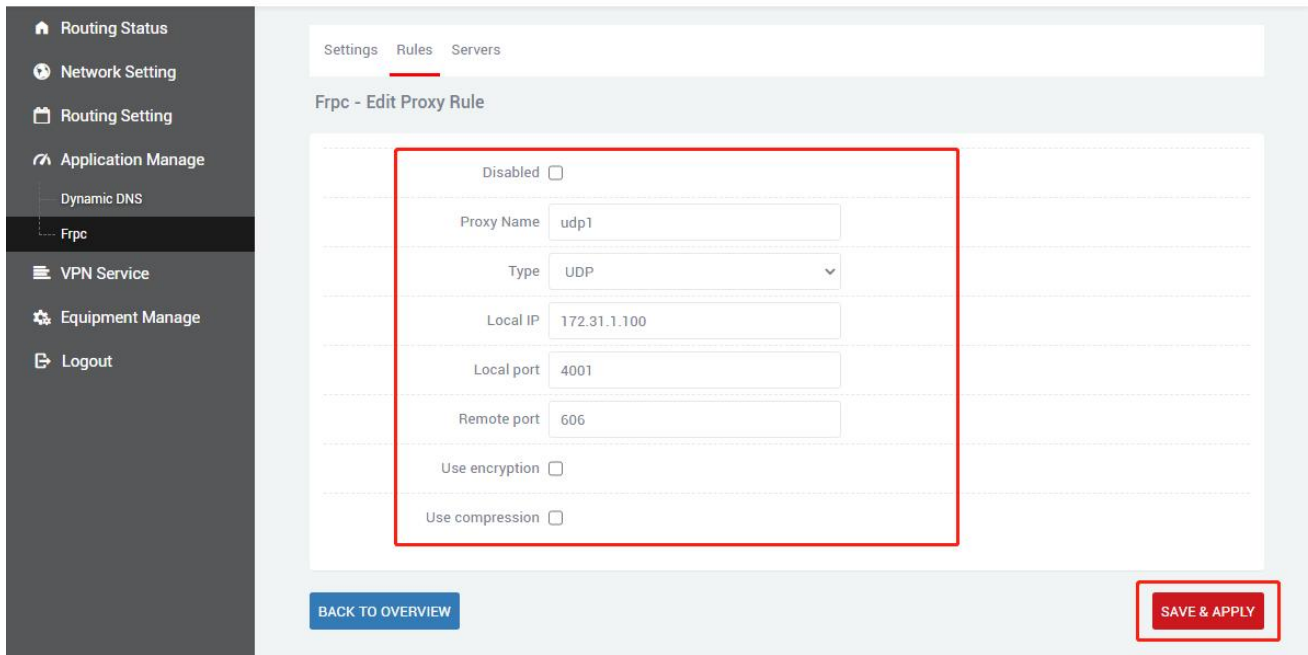
Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

Local port: Fill in which port to remotely access the device.

Remote port: Fill in a port number that is not used by the server, and you can access the Local port opened by the internal device through the public network ip and this remote port number.

Use encryption, Use compression: These two are checked according to your needs.

Click "SAVE & APPLY" after configuration.



Routing Status

Network Setting

Routing Setting

Application Manage

Dynamic DNS

Frpc

VPN Service

Equipment Manage

Logout

Settings Rules Servers

Frpc - Edit Proxy Rule

Disabled

Proxy Name

Type

Local IP

Local port

Remote port

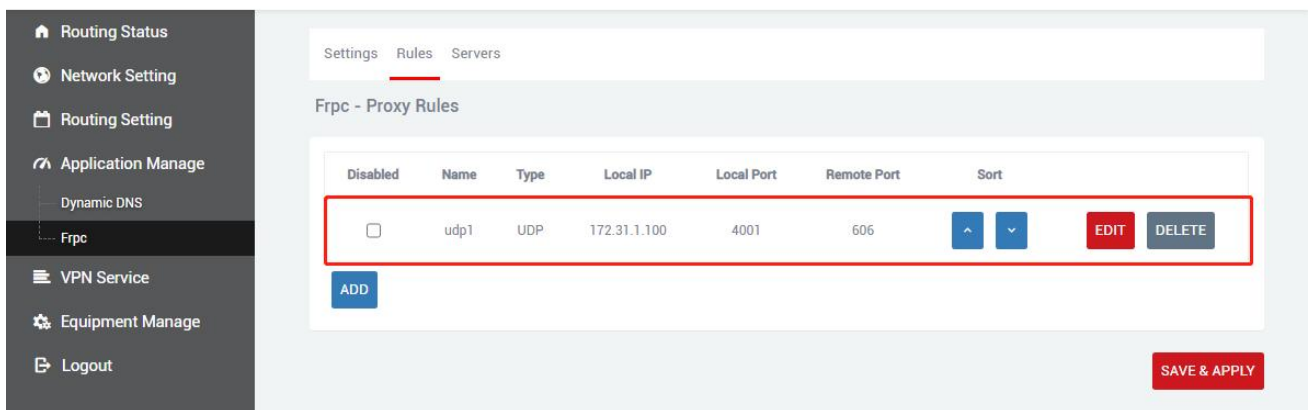
Use encryption

Use compression

BACK TO OVERVIEW

SAVE & APPLY

A new rule is successfully generated, click "Save & Apply" to make the rule effective.



Routing Status

Network Setting

Routing Setting

Application Manage

Dynamic DNS

Frpc

VPN Service

Equipment Manage

Logout

Settings Rules Servers

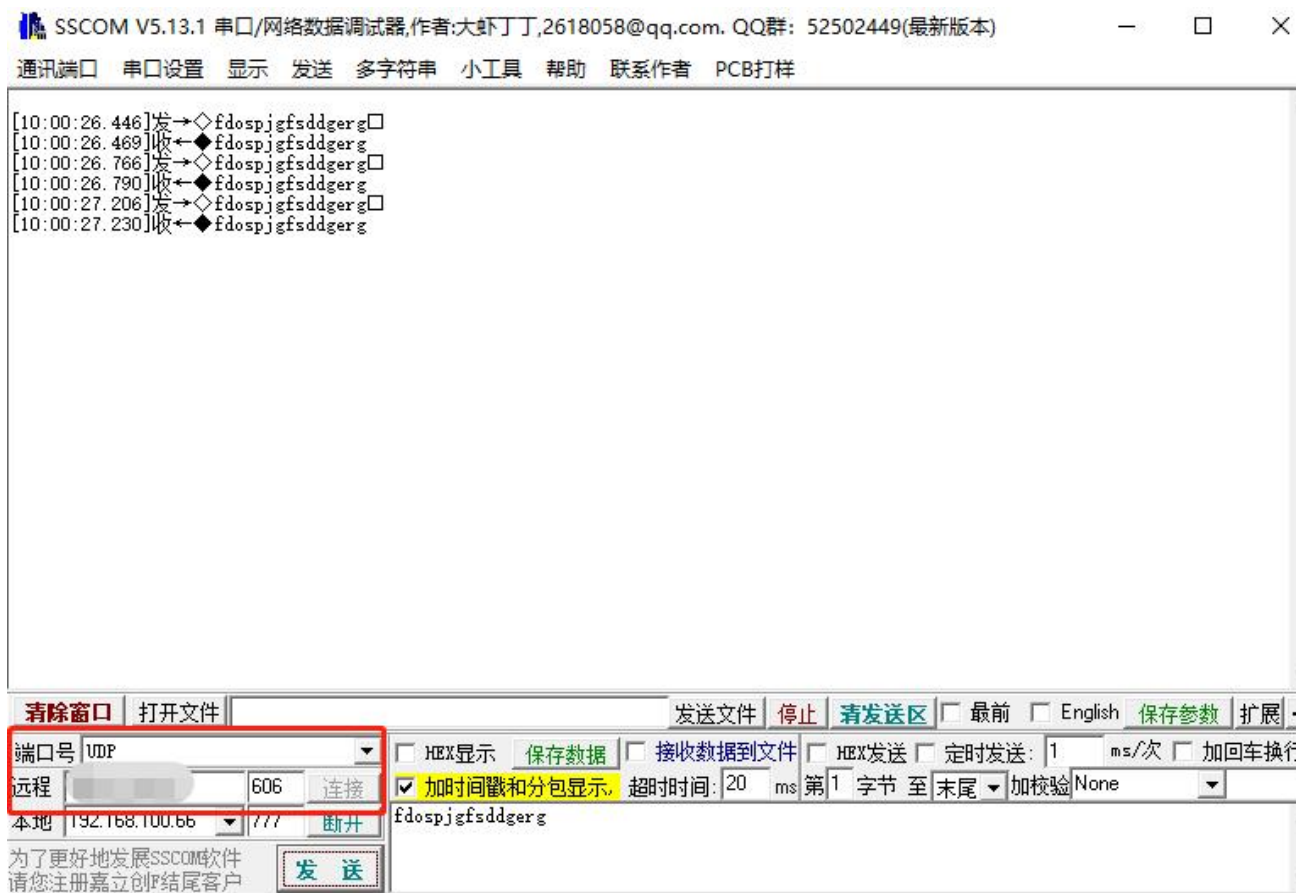
Frpc - Proxy Rules

Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort				
<input type="checkbox"/>	udp1	UDP	172.31.1.100	4001	606		↑	↓	EDIT	DELETE

ADD

SAVE & APPLY

Select the udp protocol, use the public network ip and remote port to access the router's downstream equipment.



3.4.4 Add HTTP proxy protocol

For http and https services, it supports domain-based virtual hosts, and supports custom domain name binding, so that multiple domain names share a port 80, and access intranet web pages through custom domain names. Multiple http rules can be configured, and 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 provided by the server (vhost_http_port).

Disable: Check it to disable this rule.

Proxy Name: Customize a Proxy Name.

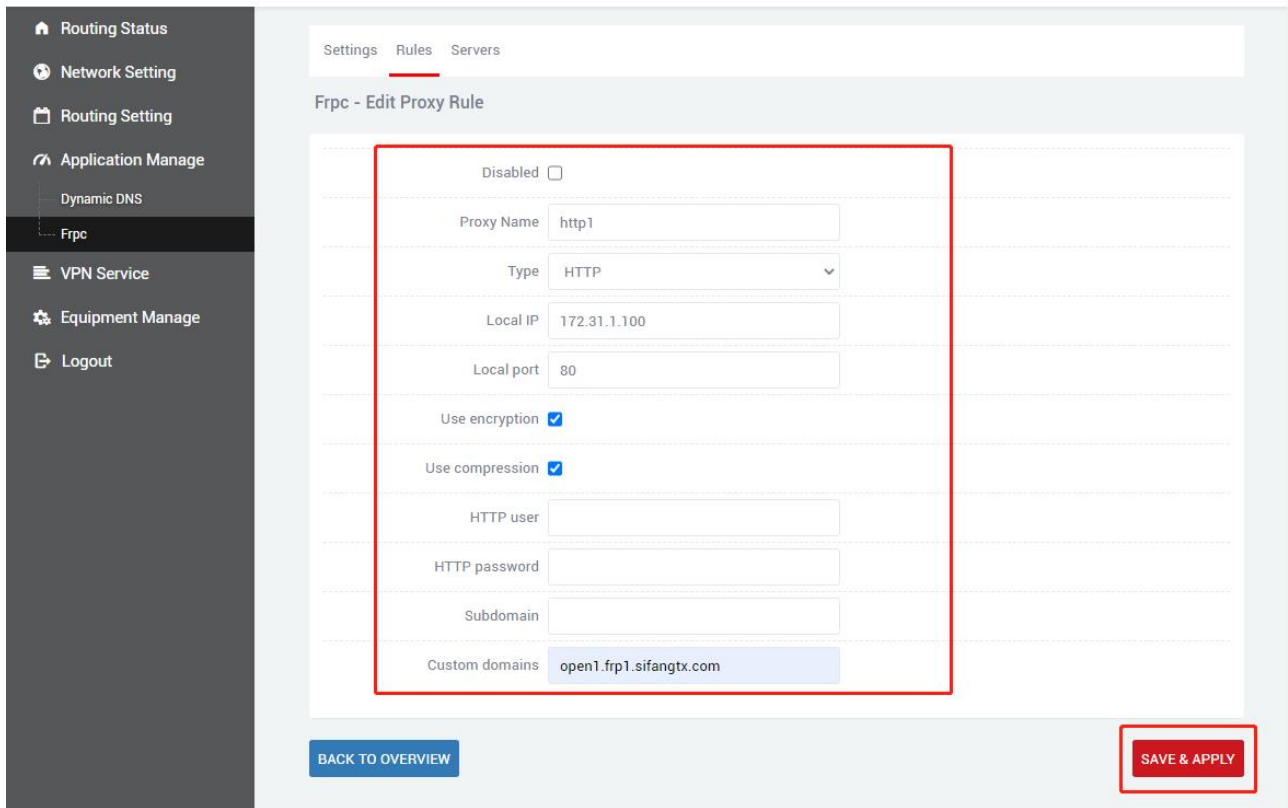
Type: Choose HTTP protocol.

Local IP: Fill in the IP of the device to be accessed remotely. The ip is mainly the ip address of the local device or the ip address assigned by the lan port for the device connected to it.

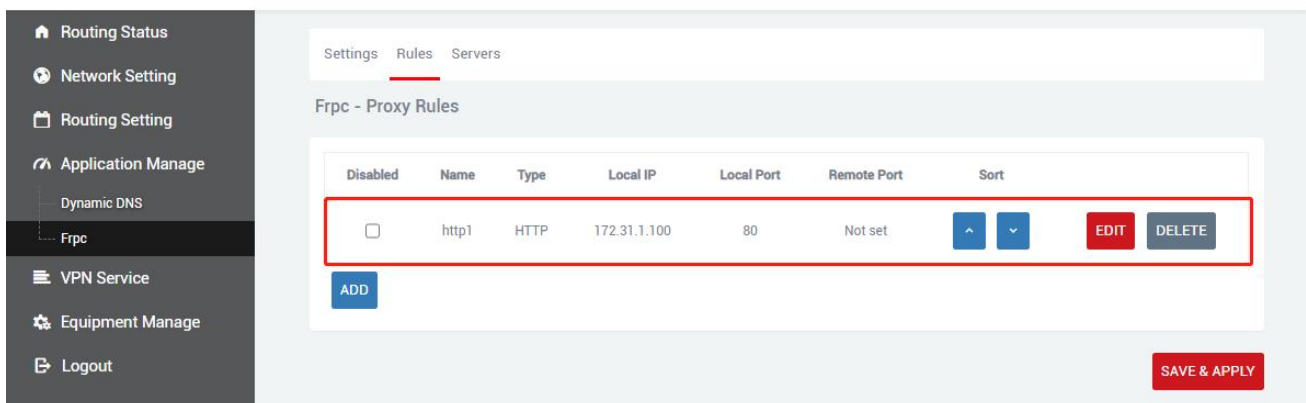
Local port: Fill in the web port number of the device

Use encryption, Use compression, HTTP user, HTTP password: These four are checked according to your needs.

Click "SAVE & APPLY" after configuration.



A new rule is successfully generated, click "Save & Apply" to make the rule effective.



Disabled	Name	Type	Local IP	Local Port	Remote Port	Sort
<input type="checkbox"/>	http1	HTTP	172.31.1.100	80	Not set	<input type="button" value="EDIT"/> <input type="button" value="DELETE"/>

Browser login openwrt1.frp1.sifangtx.com:8080 to enter the client routing management page, where 8080 port is the intranet penetration port provided by the server (ie vhost_http_port), and openwrt1.frp1.hytera.com is a custom domain name. Multiple http rules can be configured in this way, and the custom domain names need not be the same.

4 VPN (Virtual Private Network)

When configuring VPN, you need to disable the firewall first. No matter which VPN you use, you need to disable the firewall first.



Routing Status
Network Setting
Routing Setting
Routing Table
Firewall
Port Mapping
DMZ
Application Manage

Firewall

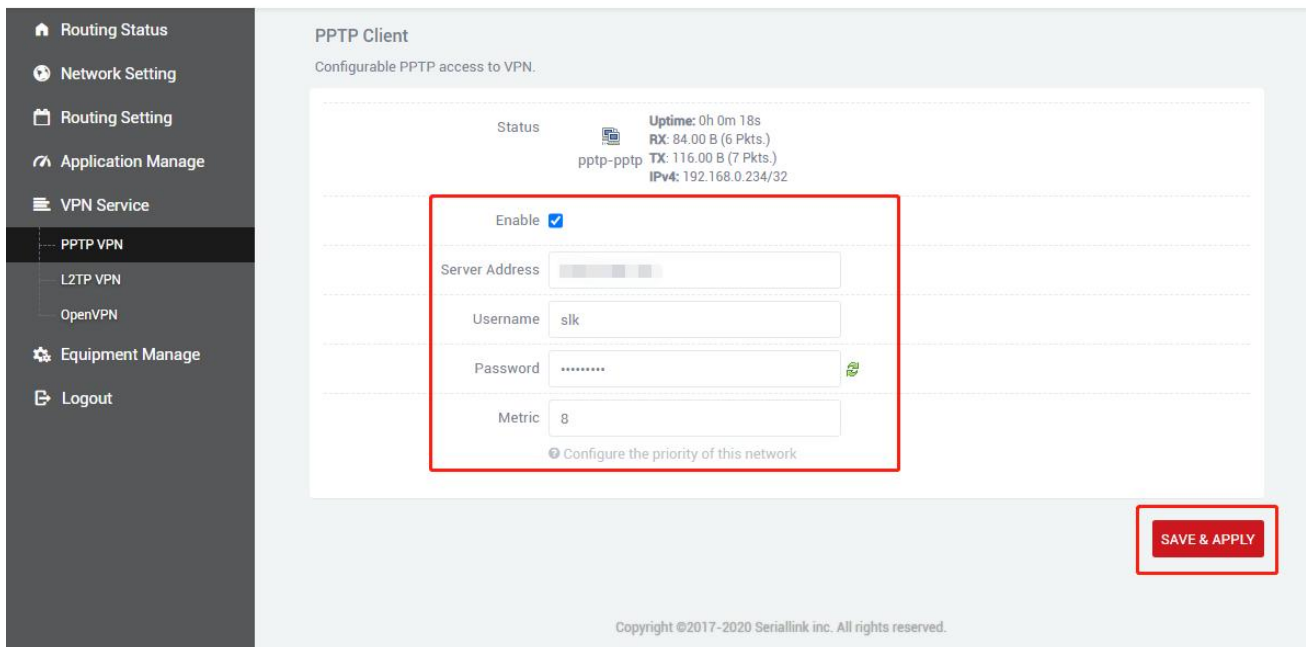
Firewall: Disable

SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.

4.1 PPTP VPN


In the navigation bar "Virtual Private Network"- "PPTP VPN", select Enable, fill in the server address, fill in the user name and password according to the server settings, and click "Save & Apply".



Routing Status
Network Setting
Routing Setting
Application Manage
VPN Service
PPTP VPN
L2TP VPN
OpenVPN
Equipment Manage
Logout

PPTP Client

Configurable PPTP access to VPN.

Status  Uptime: 0h 0m 18s
RX: 84.00 B (6 Pkts.)
TX: 116.00 B (7 Pkts.)
IPv4: 192.168.0.234/32

Enable

Server Address:

Username: slk

Password:

Metric: 8

Configure the priority of this network

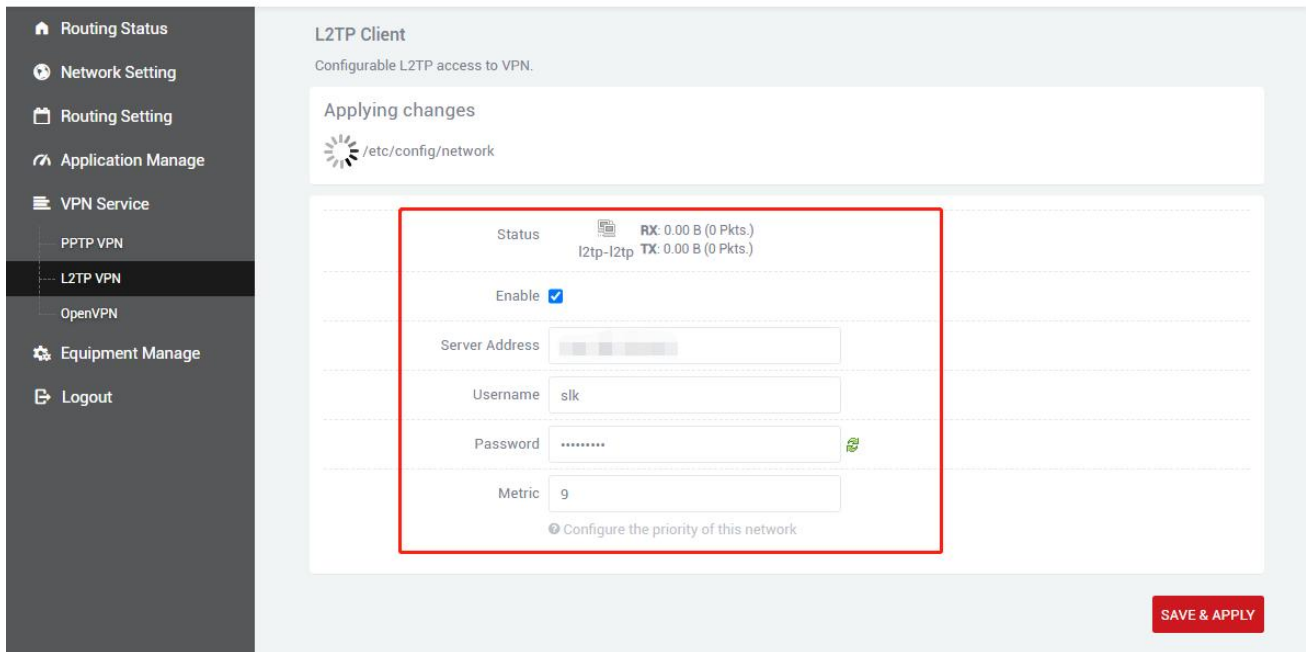
SAVE & APPLY

Copyright ©2017-2020 Seriallink inc. All rights reserved.

After the connection is successful, an address assigned by the server will appear in the status bar.


4.2 L2TP VPN

In the navigation bar "Virtual Private Network"- "L2TP VPN", select Enable, fill in the user name and password according to the server settings, and click "Save & Apply".



L2TP Client
Configurable L2TP access to VPN.


Applying changes
/etc/config/network

Status  RX: 0.00 B (0 Pkts.)
l2tp-l2tp TX: 0.00 B (0 Pkts.)

Enable

Server Address

Username

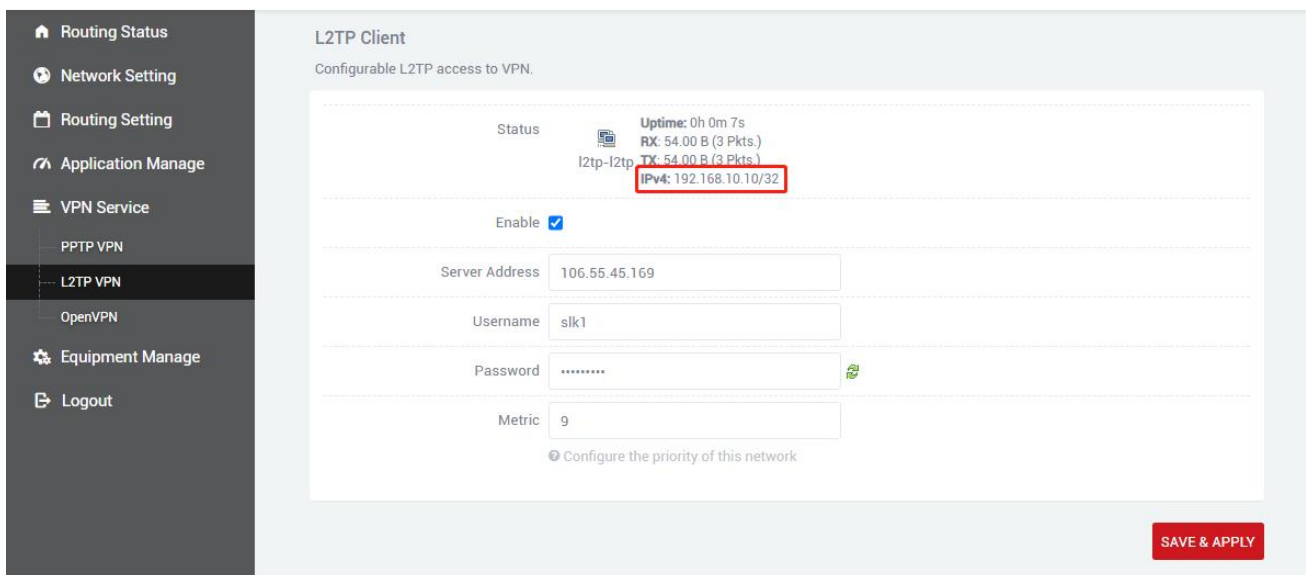
Password 

Metric


Configure the priority of this network

SAVE & APPLY

After the connection is successful, an address assigned by the server will appear in the status bar.




L2TP Client
Configurable L2TP access to VPN.

Status  Uptime: 0h 0m 7s
l2tp-l2tp RX: 54.00 B (3 Pkts.)
TX: 54.00 B (3 Pkts.)
IPv4: 192.168.10.10/32

Enable

Server Address

Username

Password 

Metric

Configure the priority of this network

SAVE & APPLY

4.3 OPENVPN

Navigation bar "Virtual Private Network" - "openvpn",

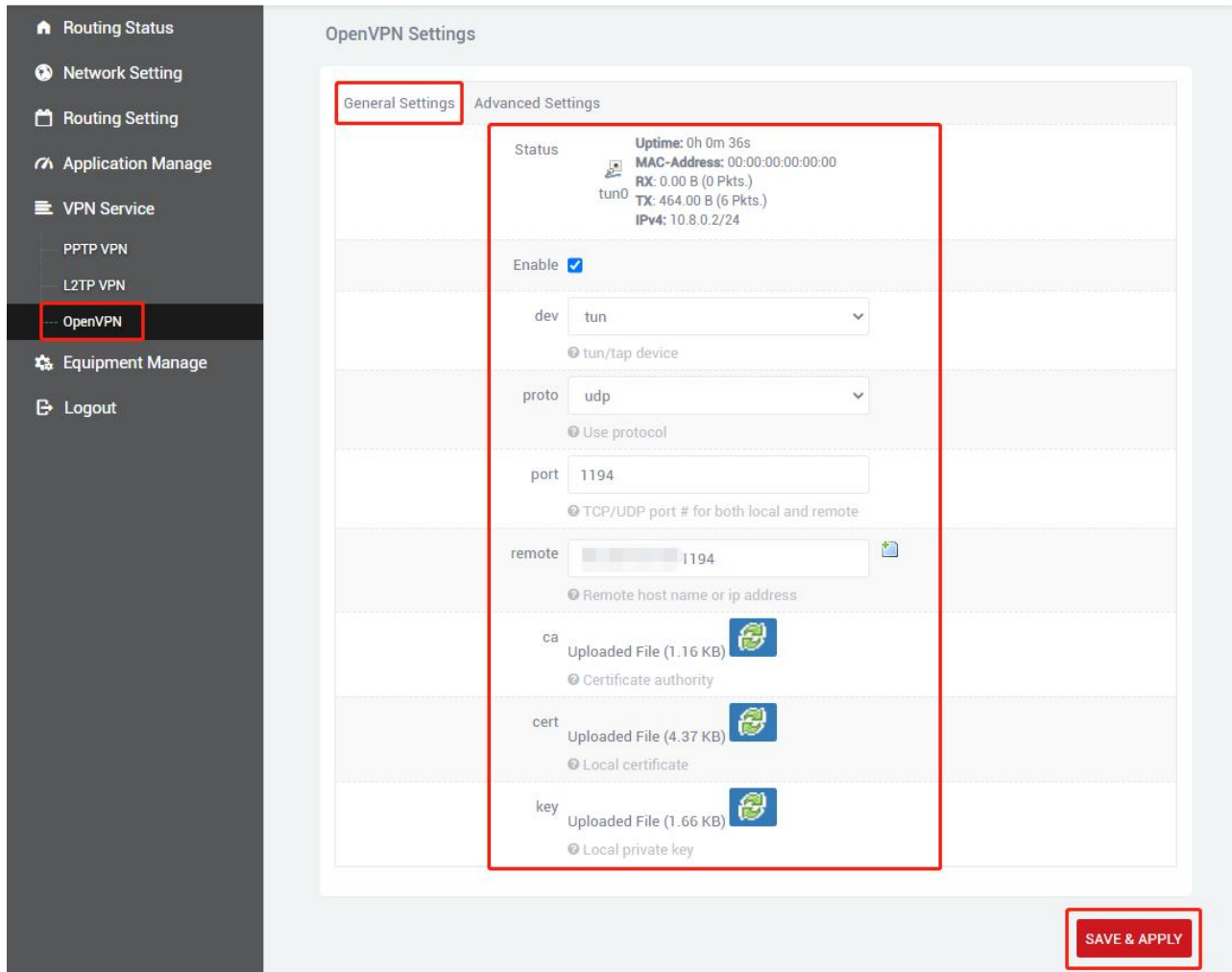
Choose tun or tap as you are using on the server.

Connecting to a TCP or UDP server depends on your server config.

If your server IP is 123.123.123.123 ,1194 as remote port ,then fill port with 1194 and complete remote with 123.123.123.123 1194

Separately upload the corresponding files including ca.crt ,client.crt and client.key

Click "SAVE & APPLY" after all configurations are consistent with the server



OpenVPN Settings

General Settings | Advanced Settings

Status
Uptime: 0h 0m 36s
MAC-Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 464.00 B (6 Pkts.)
IPv4: 10.8.0.2/24

Enable

dev tun

proto udp

port 1194

remote 1194

ca
Uploaded File (1.16 KB)
Certificate authority

cert
Uploaded File (4.37 KB)
Local certificate

key
Uploaded File (1.66 KB)
Local private key

SAVE & APPLY

Check relink to indicate that you can disconnect and reconnect the server after restoring the network.

Other configurations are supposed to consistent with the server configuration.

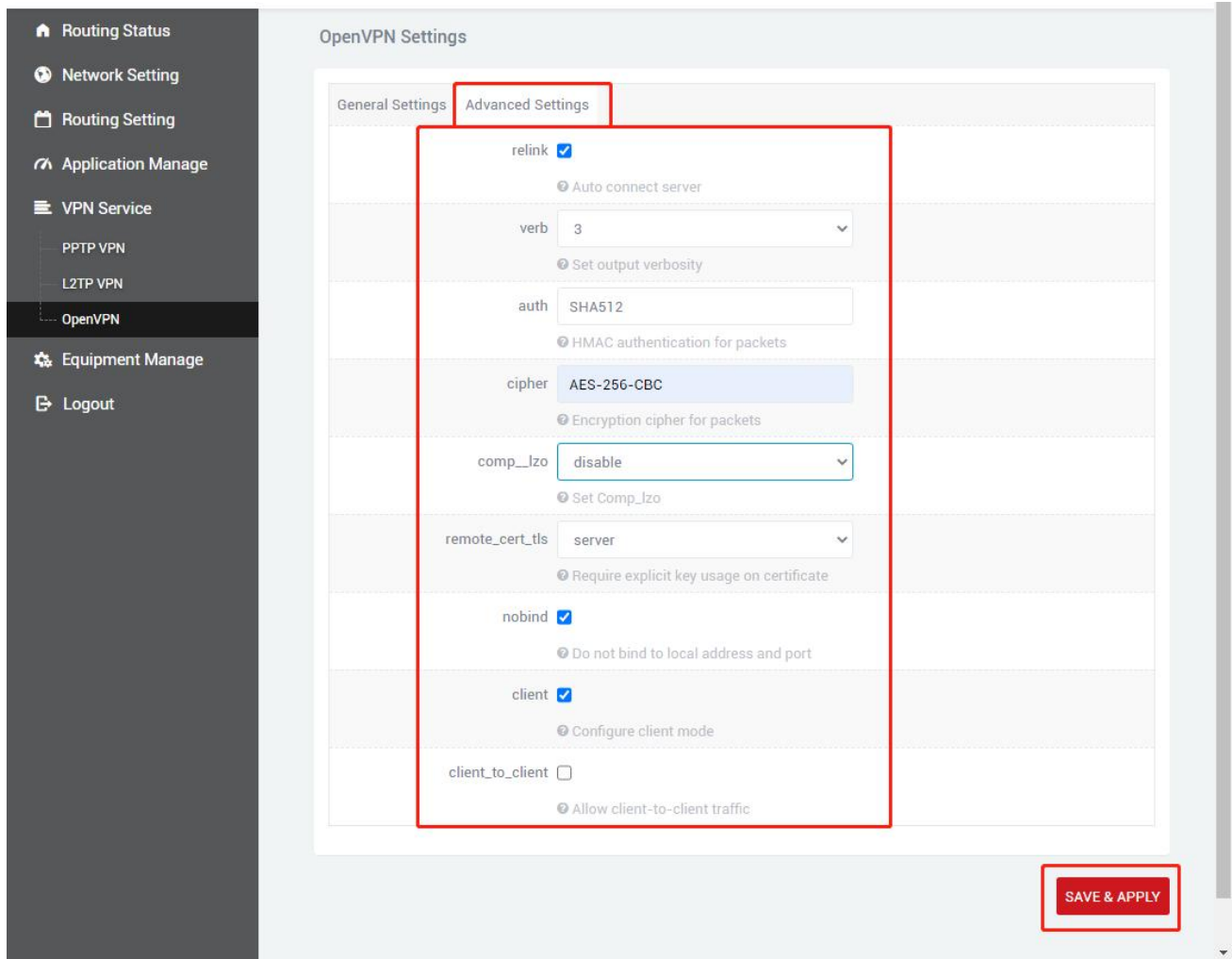
verb is the log output verbosity, the higher the verbosity, the more detailed the log content.

We disable comp_lzo by default,if you configure it as yes on your server,choose yes.

Selet server in option remote_cert_tls.

If you want to communicate between clients,click client_to_client.

SAVE & APPLY.

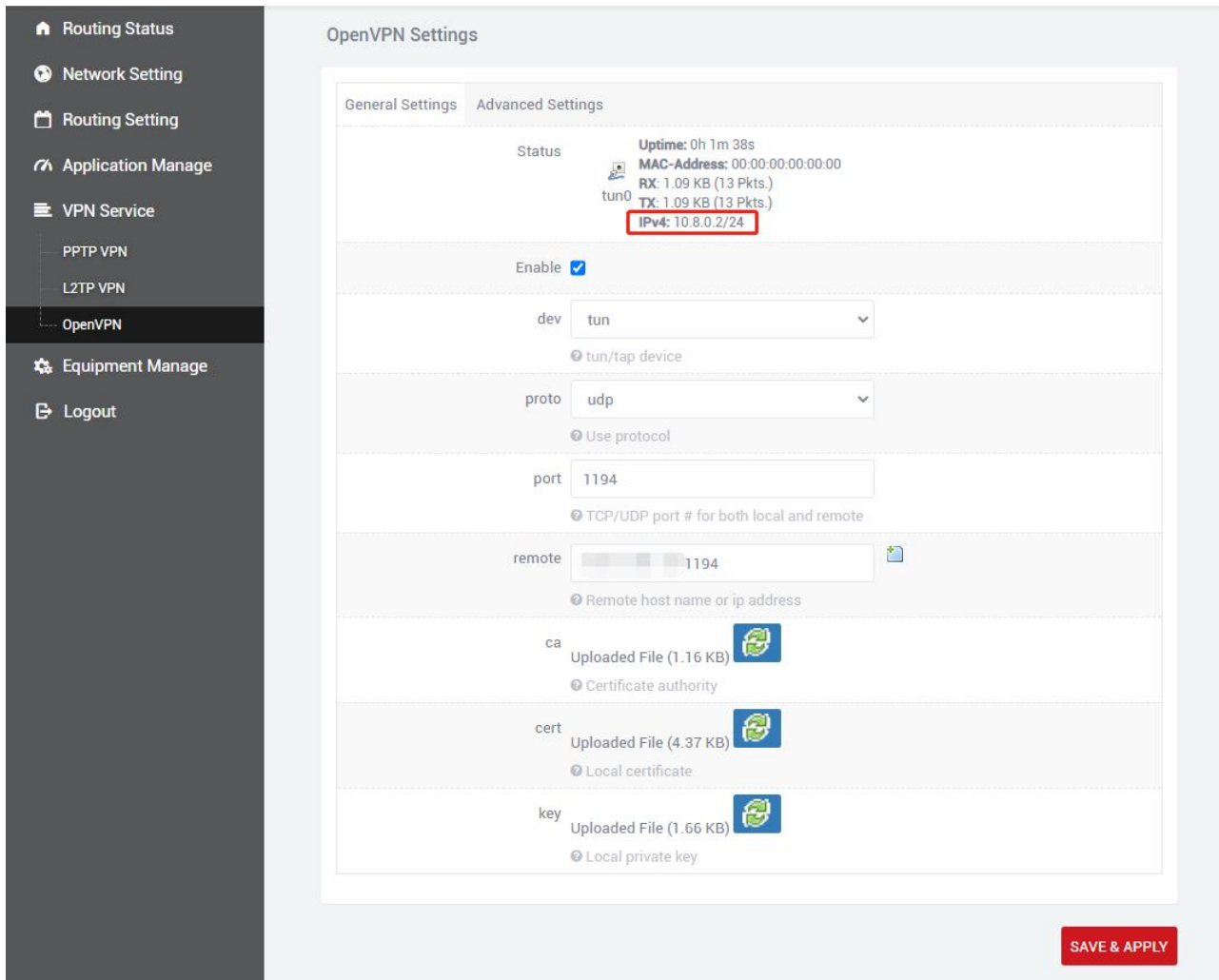


The screenshot shows the 'OpenVPN Settings' page with the 'Advanced Settings' tab active. A red box highlights the following settings:

- relink (Auto connect server)
- verb 3 (Set output verbosity)
- auth SHA512 (HMAC authentication for packets)
- cipher AES-256-CBC (Encryption cipher for packets)
- comp_lzo disable (Set Comp_lzo)
- remote_cert_tls server (Require explicit key usage on certificate)
- nobind (Do not bind to local address and port)
- client (Configure client mode)
- client_to_client (Allow client-to-client traffic)

A 'SAVE & APPLY' button is located at the bottom right of the settings area.

After the connection is successful, an address assigned by the server will appear in the status bar.

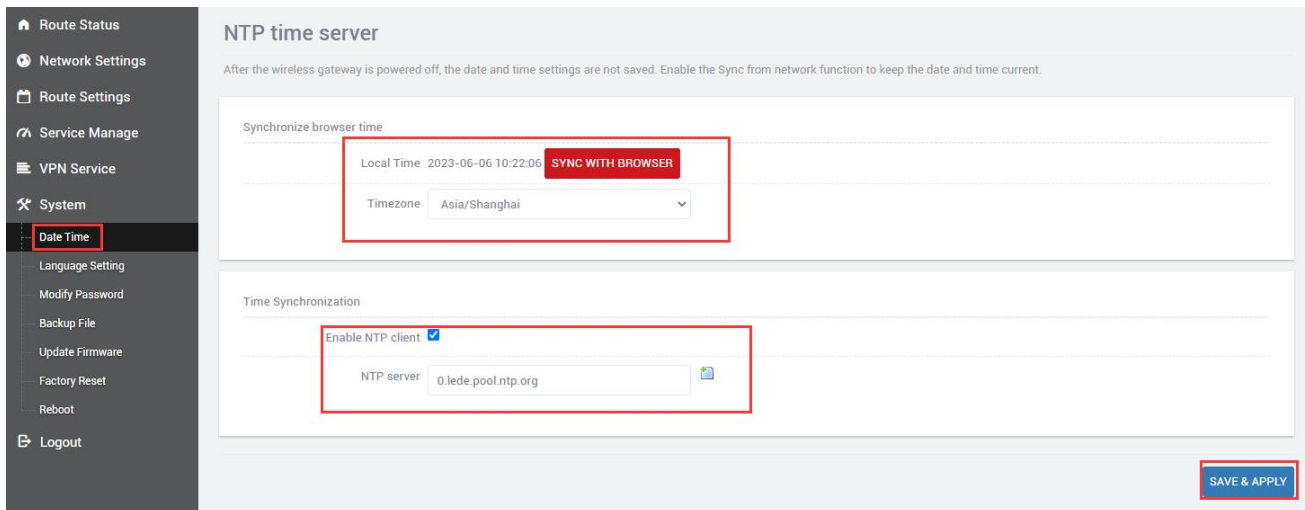


5 Basic Management (Device Management)

5.1 Date Time

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

Navigation bar "Equipment Manage" - "Date Time"



NTP time server

After the wireless gateway is powered off, the date and time settings are not saved. Enable the Sync from network function to keep the date and time current.

Synchronize browser time

Local Time 2023-06-06 10:22:06 **SYNC WITH BROWSER**

Timezone Asia/Shanghai

Time Synchronization

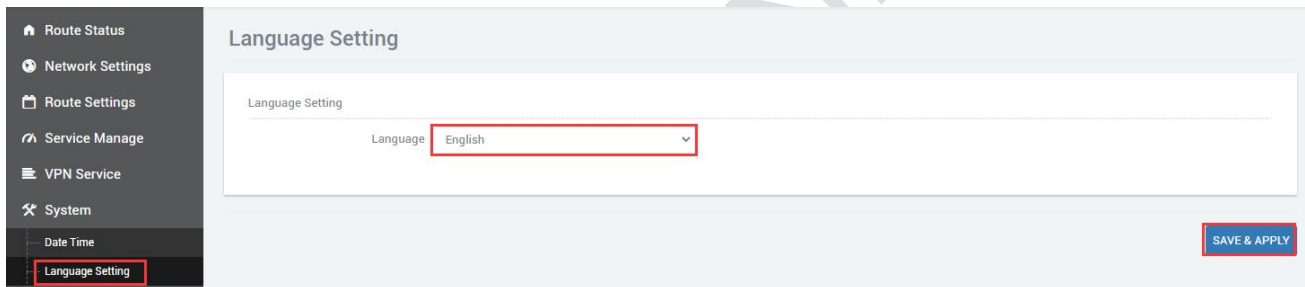
Enable NTP client

NTP server 0.lede.pool.ntp.org

SAVE & APPLY

5.2 Language Setting

Change the language displayed on the page according to your needs. You can choose English or Chinese and change it in the navigation bar "Device Management" - "Language Settings".



Language Setting

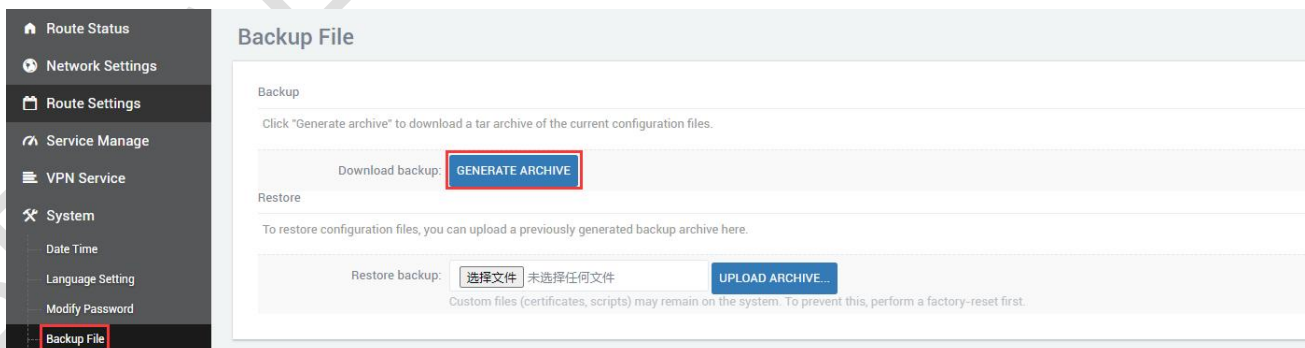
Language Setting

Language English

SAVE & APPLY

5.3 Backup File

The backup function can be used to generate device configuration files and download them locally.



Backup File

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup: **GENERATE ARCHIVE**

Restore

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: 选择文件 未选择任何文件 **UPLOAD ARCHIVE...**

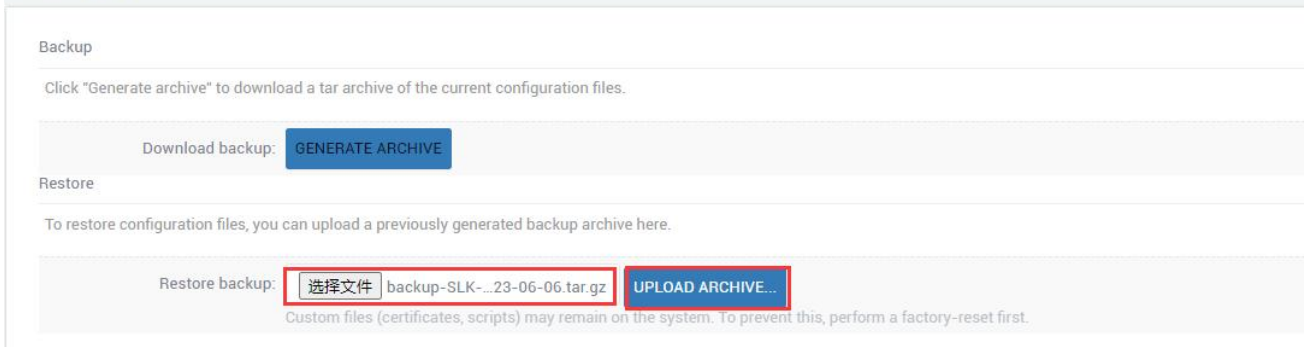
Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

The downloaded configuration file is as follows.



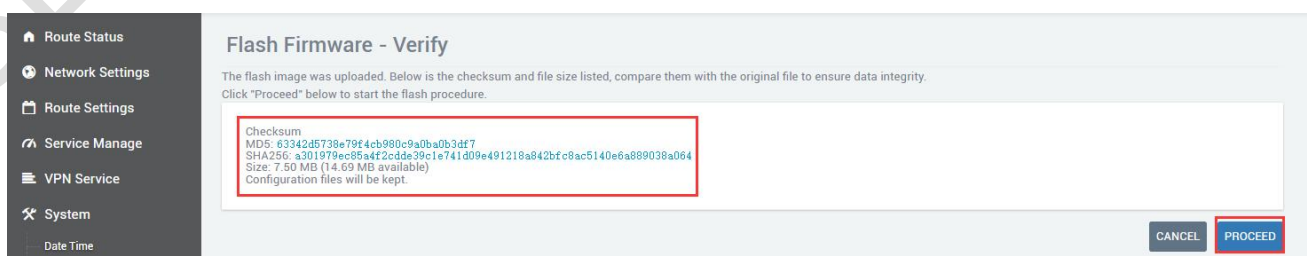
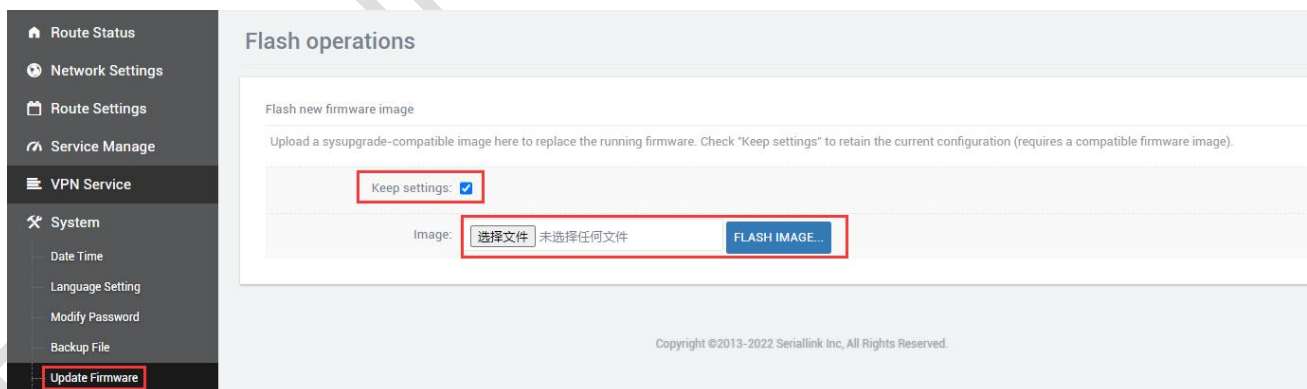
The recovery function restores device configuration through local configuration files, and during the recovery process, the device will restart.

Backup File



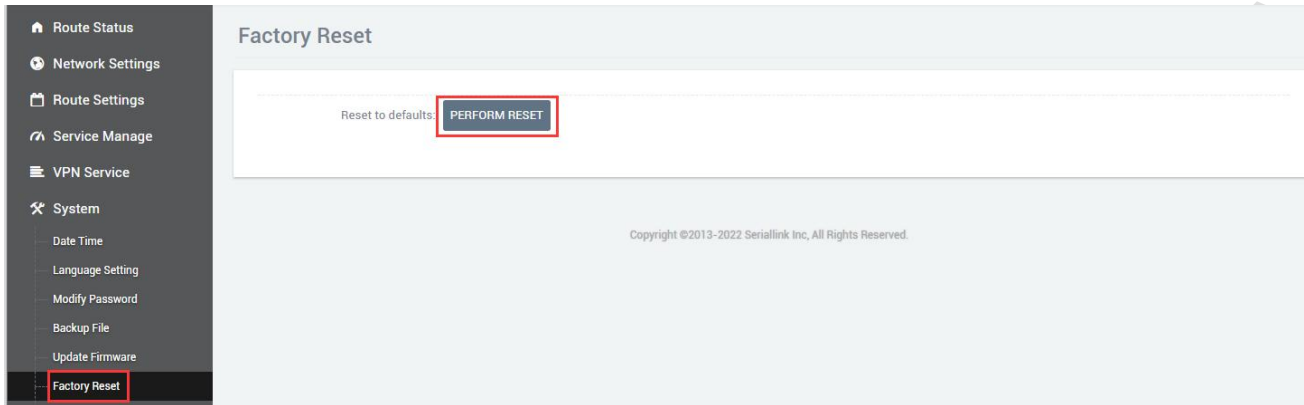
5.4 Upgrade firmware

Navigation bar "Equipment Manage" - "Upgrade Firmware", Uncheck "keep setting", select the file and click "UPDATE". After uploading, a page with MD5 verification code will appear. Click "Execute" to upgrade. The upgrade will take a certain amount of time, about 1~ 2 minutes, after the upgrade is complete, log in to the page again through "192.168.2.1".



5.5 Factory Reset

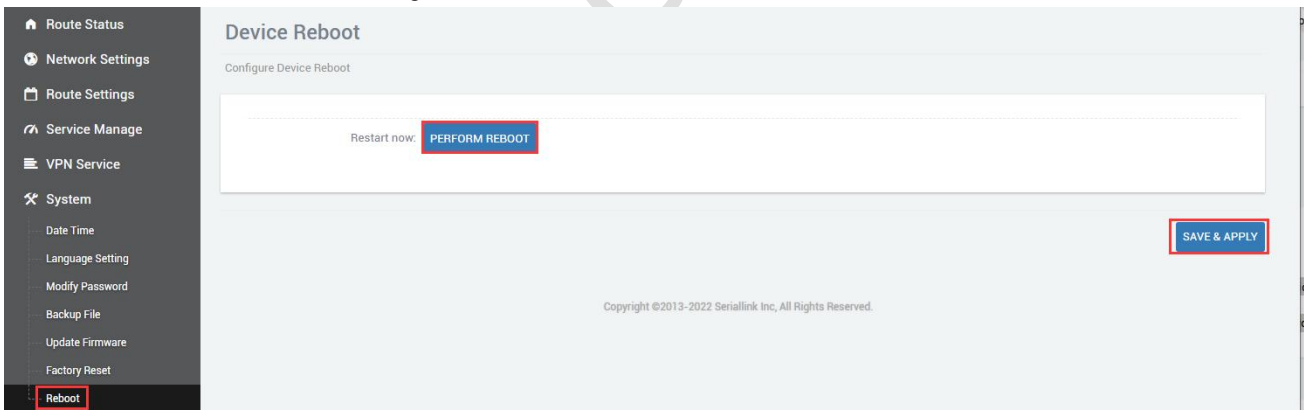
Factory reset is generally when the device fails to enter the device page, or there are many function settings, when you want to reset, you can restore the factory settings, the navigation bar "Equipment Manage"->"Factory Reset", Click "Execute Reset" to restore the device to factory defaults.



5.6 Device restart

The device can be restarted through the page, the navigation bar "device management"->"restart", click "execute restart" to restart the device.

You can also set the scheduled restart. To set the scheduled restart, you need to check "Enable", and click "SAVE & APPLY" after setting the time.



5.7 Page Exit

Click "Exit" to exit the page.

