USR-G806 Software Manual

File version: V1.0.5

Content

1. Product Overview....4
1.1. Product feature....4
1.2. Band....4
2. Product Functions....6
2.1. Configuration Process....6
2.2. Basic Function....7
2.2.1 Network Diagnostic Function....7
2.2.2 Host Name and Time Zone....7
2.2.3 Password....8
2.2.4 Restore to Factory Setting....8
2.2.5 Upgrade Firmware Version....8
2.2.6 Reset....9
3. Advanced Function....10
3.1. DDNS....10
3.2. WIFI-Dog....11
3.3. SMS AT Commands....11
3.4. LAN Interface....12
3.4.1 DHCP Function....13
3.4.2 WAN Interface....13
3.4.3 WLAN Function....13
3.4.4 4G Interface....15
3.4.5 APN....16
3.5. VPN Client....17
3.5.1 PPTP Client....17
3.5.2 L2TP Client....20
3.5.3 IPSEC....24
3.5.4 OPENVPN....26
3.5.5 GRE....30
3.5.6 SSTP Client....33
3.6. Static Router....34
3.7. NAT Function....34
3.7.1 MASQ....34
3.7.2 SNAT....35
3.7.3 DNAT....36
3.8. Access Restrictions....37
3.8.1 Domain Blacklist....38
3.8.2 Whitelist....38
3.9. Rate Limiting....38
4. AT Commands....39
4.1. AT+VER....40
4.2. AT+MAC....40

4.3. AT+ICCID 40
4.4. AT+IMEI 40
4.5. AT+SYSINFO 40
4.6. AT+APN 41
4.7. AT+CSQ 41
4.8. AT+TRAFFIC 41
4.9. AT+UPTIME 41
4.10. AT+WANN 42
4.11. AT+LANN 42
4.12. AT+WEBU 42
4.13. AT+PLANG 42
4.14. AT+RELD 43
4.15. AT+Z 43
4.16. AT+DHCPEN 43
4.17. AT+ LINUXCMP 43
5. Contact us 44
6. Disclaimer 44
7. Updated History 44

1. Product Overview

1.1. Product feature

- One RJ45 for WAN/LAN port. 1 RJ45 for LAN port only.
- Support 1 WLAN
- Support Web Server
- Support multiple LED communication indicators
- Support Reload button to restore default settings by hardware way
- The wired net ports support 10/100Mbps rate
- Support VPN Client (PPTP/L2TP/IPSEC/GRE/OPENVPN/SSTP) and supports VPN encryption and static IP functions.
- Support APN special network card.
- Support for wired wireless multi network simultaneous online and multi network intelligent switching backup function
- Support remote upgrade and remote monitoring
- Support Dynamic Domain Name System (DDNS)
- Support mandatory portal (WIFIDOG), this function needs to be customized according to customer needs.
- Support SMS AT command

1.2. Band

USR-G806 has different band model to support different area. To check whether the USR-G806 works in specific country, please check which 3G/4G technology and band is used in this country and operator. Then please contrast our form of different model.

G806-43	Asia
G806-E	Europe
G806-A	America AT&T
G806-AU	Australia

	G806-43 Operating Band
FDD-LTE	1
	3
	8
TDD-LTE	38
	39
	40
	41
WCDMA	1
	8
CDMA1X	800MHz
CDMA2000-EVDO	
GPRS	3
	8

	G806-E Operating Band
FDD-LTE	1
	3
	5
	7
	8
	20
TDD-LTE	38
	40
	41
WCDMA	1
	5
	8
GPRS	3
	8

	G806-A Operating Band
FDD-LTE	2
	4
	12
WCDMA	2
	4
	5

	G806-AU Operating Band
FDD-LTE	1
	2
	3
	4
	5
	7
	8
	28
TDD-LTE	40
WCDMA	1
	2
	5
	8
GPRS	2
	3
	5
	8

2. Product Functions

This chapter introduces the functions of USR-G806, as the following diagram shown, you can get an overall knowledge of it.

Figure 1 Product function

2.1. Configuration Process

（1） Connect the 4G antenna and Wi-Fi antenna to the router. (Longer one is 3G/4G antenna and Shorter one is Wi-Fi antenna.)

（2） Plug the SIM card in G806.

（3） Power on the module by power adaptor and check the LED status.

（4） Connect PC or mobile to the G806 router via LAN interface or Wi-Fi interface. Wi-Fi password is “www.usr.cn”.

（5） Log in Web Server of router. (Default IP address of router is 192.168.1.1, either the username and password is “root”.)

（6） Configure APN parameters according to SIM card. Some SIM card APN can be recognized automatically.(Network->APNSET)

（7） Configure other parameters according to user applications.

2.2. Basic Function

2.2.1 Network Diagnostic Function

User can use network diagnosis function by Web Server as follow:

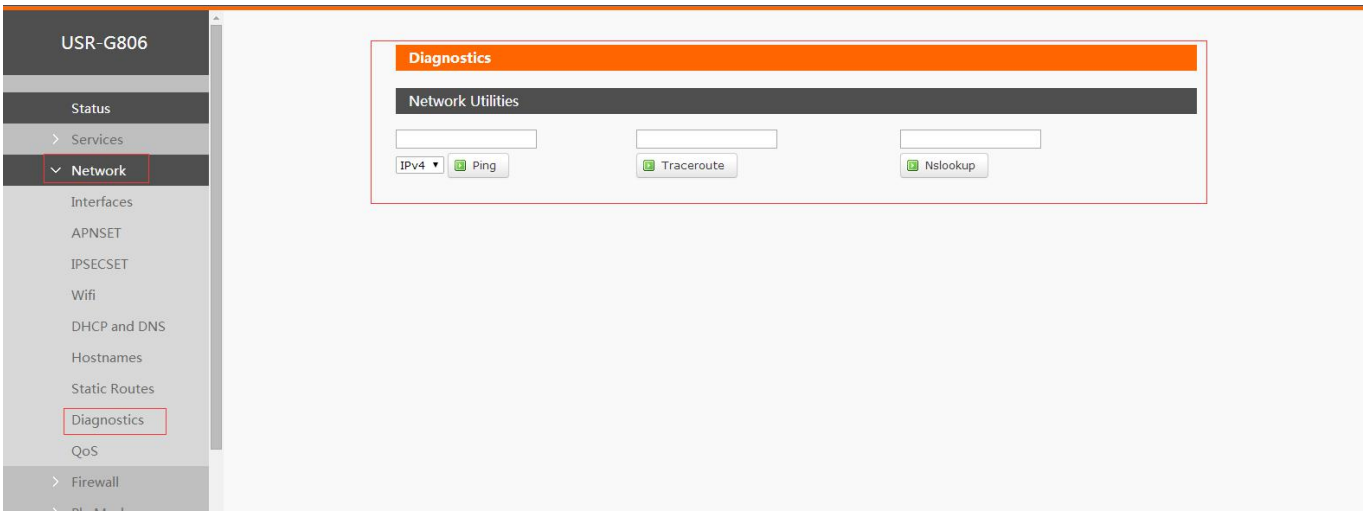

Figure 2 network diagnosis

- Ping is a Ping tool, which can directly test Ping at a specific address on the router side.
- Traceroute is the routing parsing tool, which can get the routing path when accessing an address.
- Nslookup is a DNS view tool, which can resolve domain names to IP addresses.

2.2.2 Host Name and Time Zone

G806 default module name is USR-G806 and default Time Zone is Beijing time zone.
User can configure module name and Time Zone by Web Server as follow:

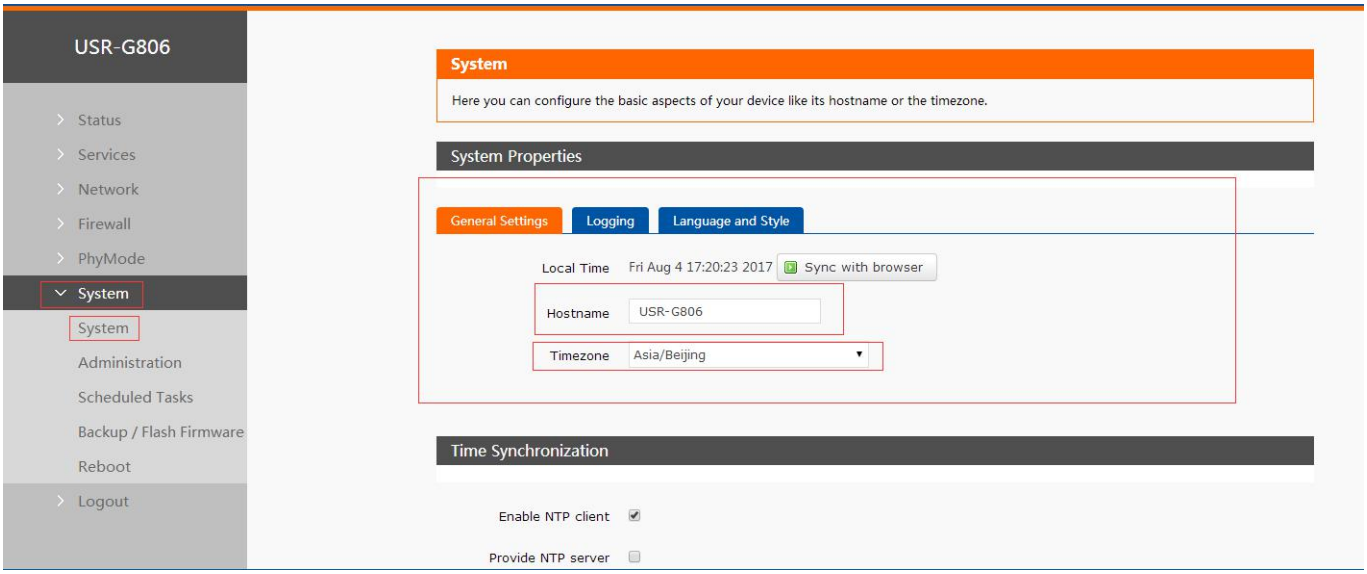

Figure 3 hostname and time zone

2.2.3 Password

Default password is root, this password is used to enter Web Server.
User can change password by Web Server as follow:

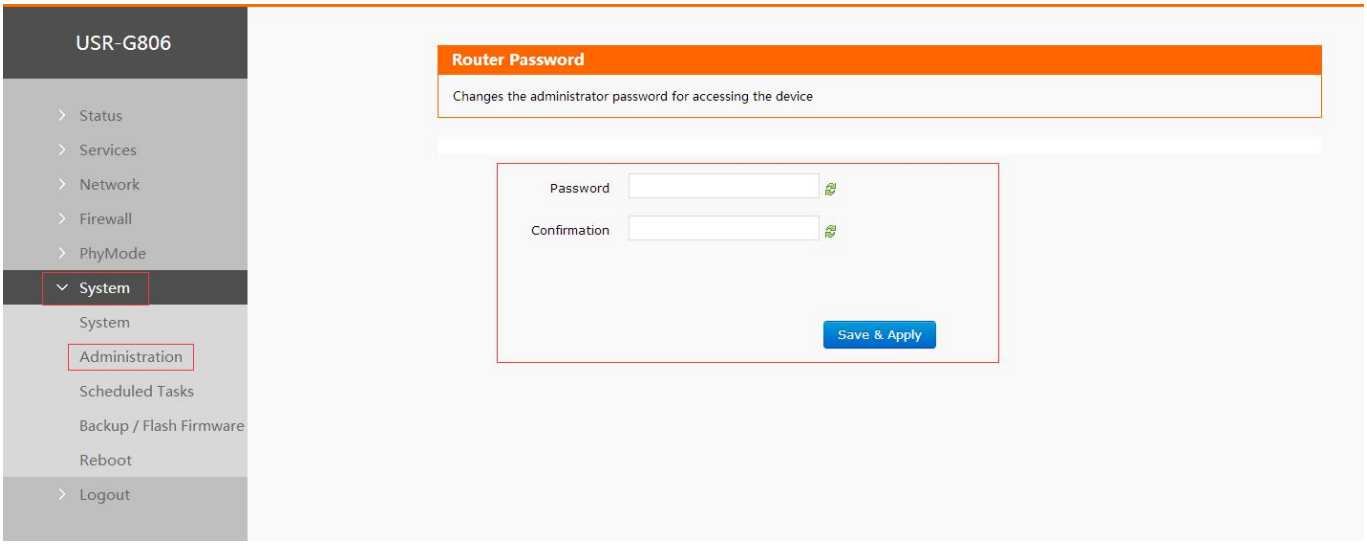

Figure 4 change web server password

2.2.4 Restore to Factory Setting

Hardware restore: Press Reload button over 5 seconds and release, G806 will restore default settings and reset.
User can restore default settings by Web Server as follow:

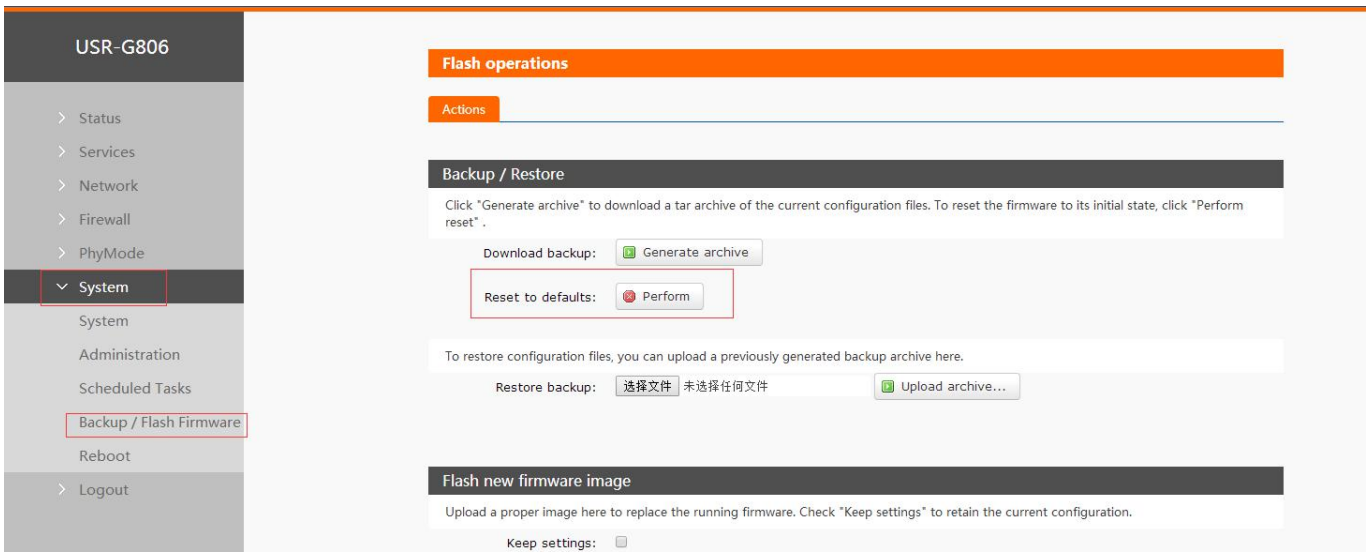

Figure 5 restore default settings

2.2.5 Upgrade Firmware Version

Upgrade by Web Server as follow:

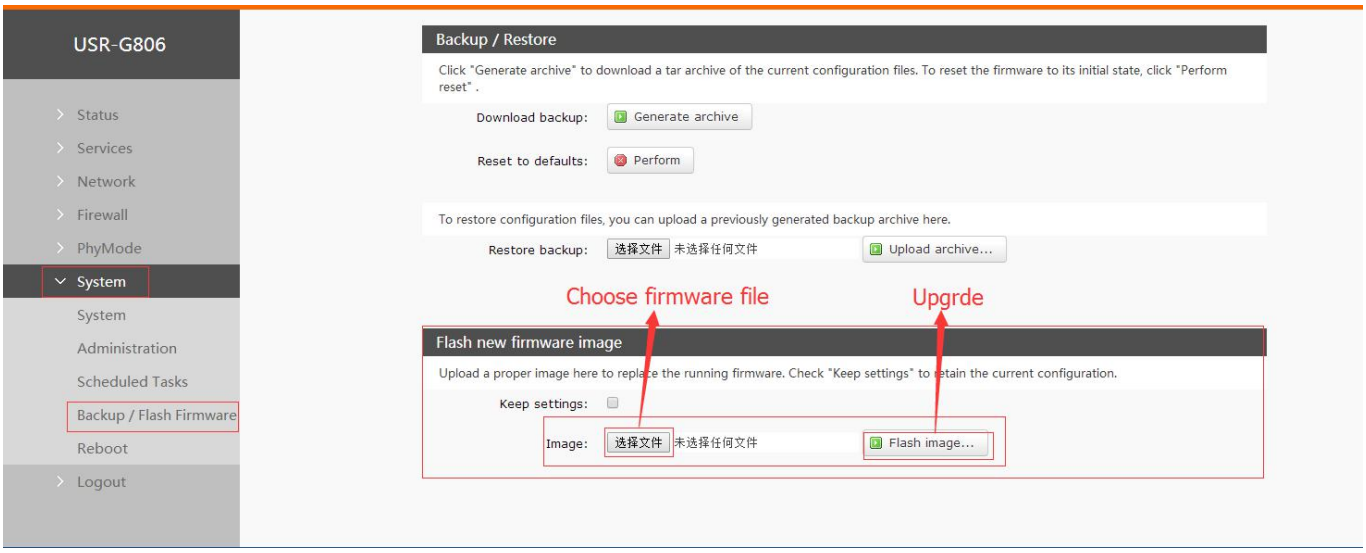

Figure 6 upgrade firmware

Note:

- The whole upgrade process will last about one minute , user can enter Web Server after about 1 minute.
- User can choose saving settings.
- User should keep powering up and LAN/WIFI connection during the whole upgrade process.

2.2.6 Reset

Reset time is about 40~60 seconds.

Reset by Web Server as follow:

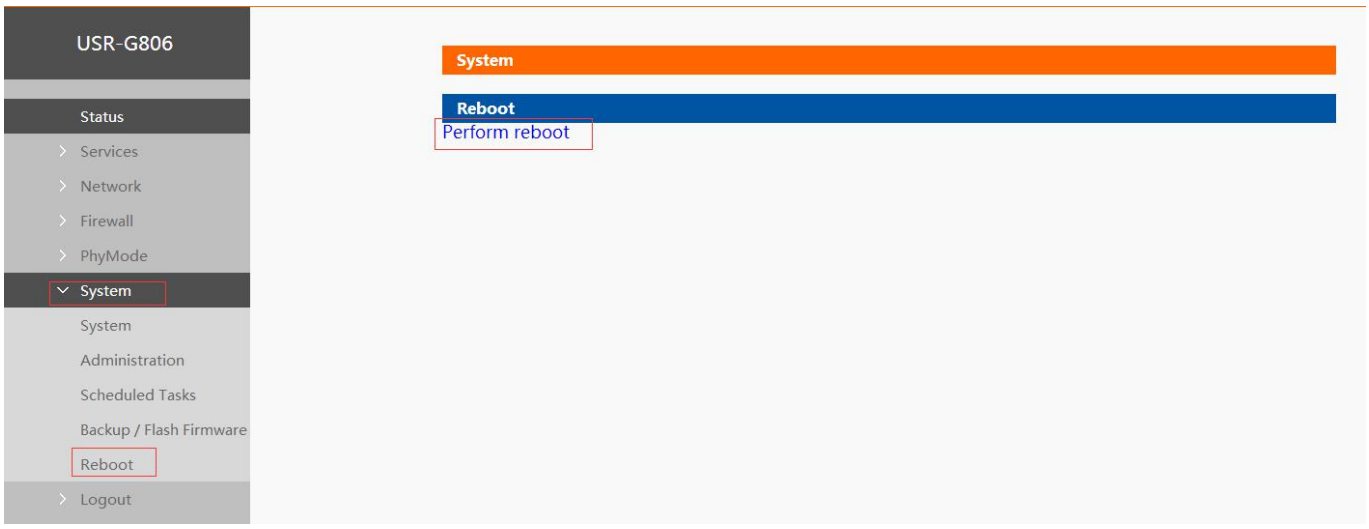

Figure 7 reset

3. Advanced Function

3.1. DDNS

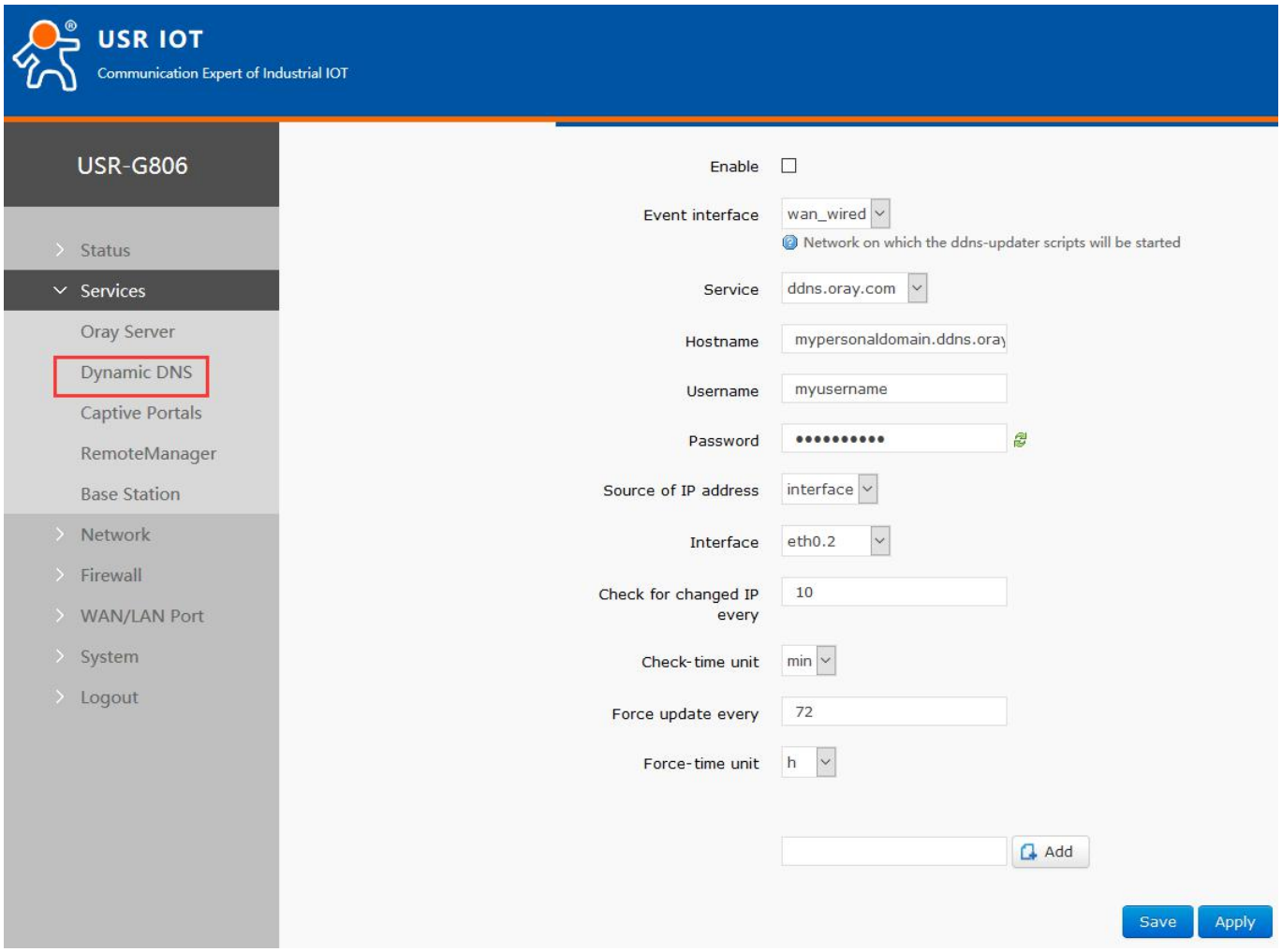

Figure 8 DDNS

Function	Intro	Note
Enable	Enable/disable DDNS function	Default disable
Event interface	Choose the WAN port	e.g. choose wan_wired
Service/URL	Fill in the service address of DDNS.	e.g. http://ouclihuibin123:ouclihuibin1231@ddns.oray.com/ph/update?hostname=1a516r1619.iask.in
Hostname	Fill in the domain name	e.g. 1a516r1619.iask.in
User name	Fill in account name	e.g. ouclihuibin123
Password	Fill in password	e.g. ouclihuibin1231
Source of IP address	Choose the interface	

Interface	Choose the interface name	e.g. choose eth0.2
Check for changed IP/check-time unit	The interval between detecting IP address changes, domain name pointing to the IP may change frequently, the smaller the value, the more frequent the detection.	e.g. 1 min
Force update time /force-time unit	Mandatory update interval	e.g. 72 h

3.2. WIFI-Dog

After clicking on open and save, the router needs to be restarted, and the authentication server needs to be customized.

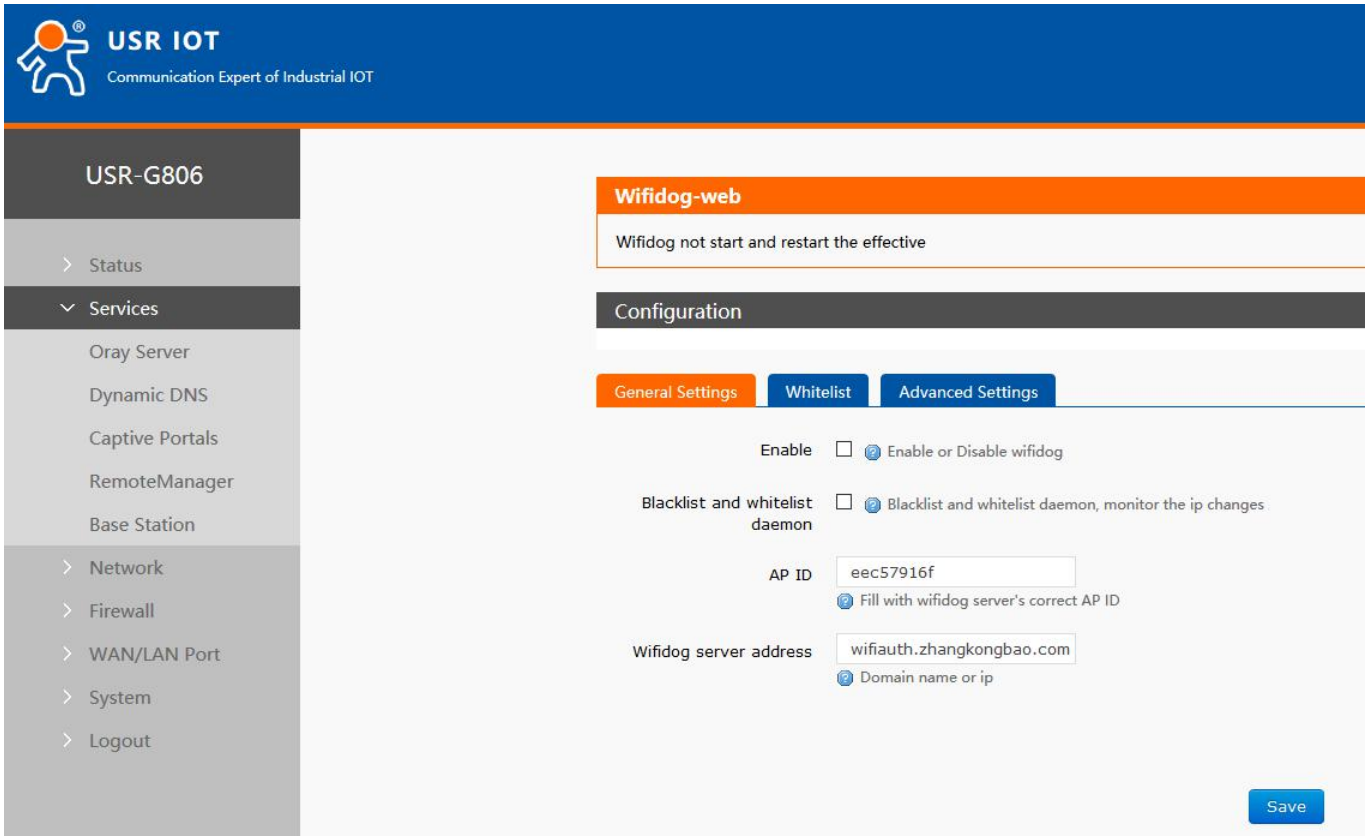

Figure 9 wifi-dog

3.3. SMS AT Commands

You should send SMS in this format: root#AT+COMMAND

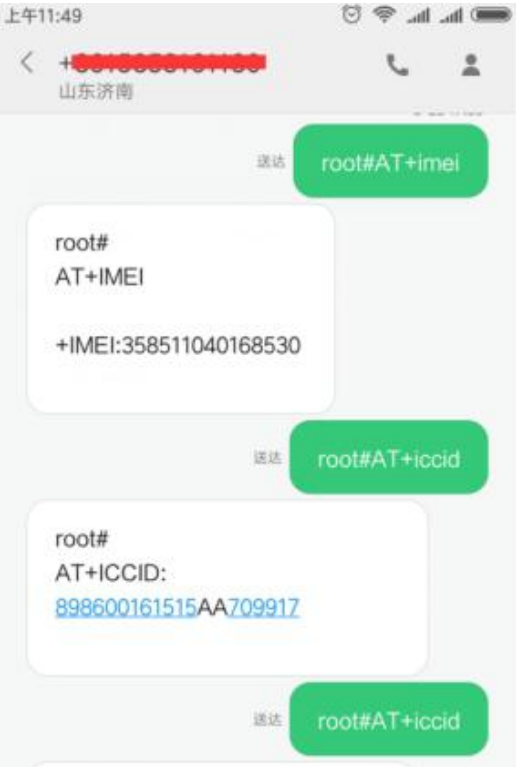

Figure 10 SMS AT commands

3.4. LAN Interface

G806 supports two LAN interface (one is WAN/LAN interface).
Default settings: One LAN interface (WAN/LAN used as WAN interface; IP address: 192.168.1.1; Subnet mask: 255.255.255.0; Open DHCP function).
User can configure LAN interface by webpage as follow:

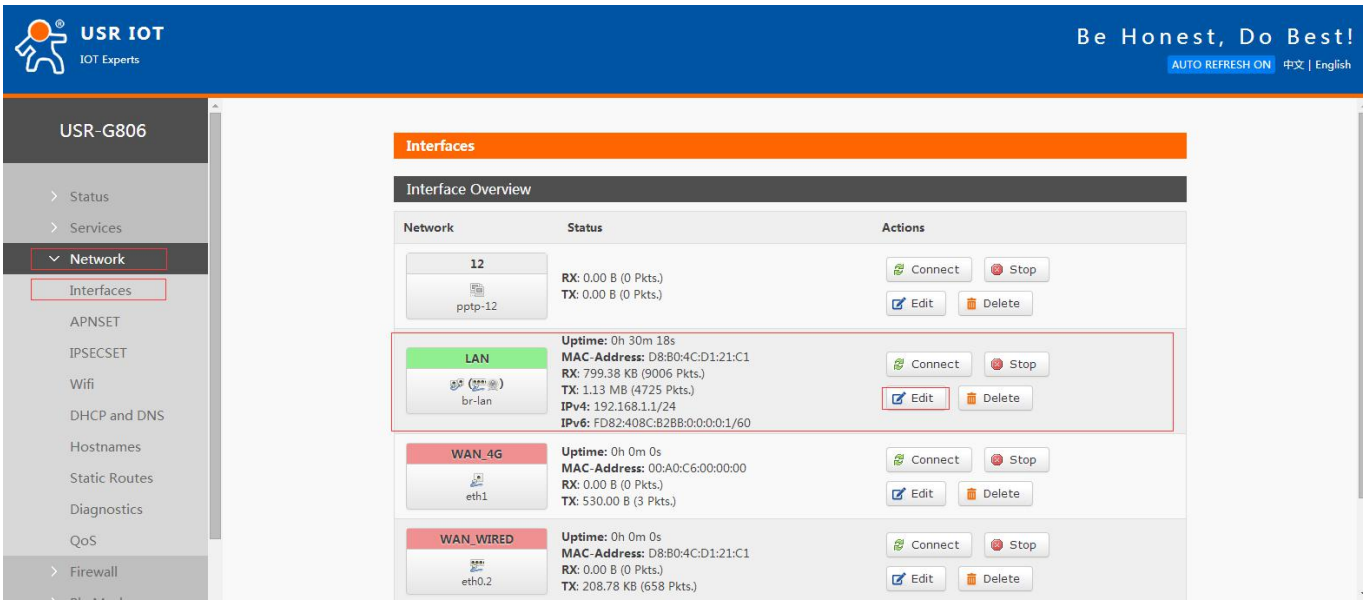

Figure 11 LAN interface

3.4.1 DHCP Function

DHCP default range of distribution is from 192.168.1.100 to 192.168.1.250 and default address lease time is 12 hours. Address range and lease time can be changed.

After you enter Web Server LAN interface, you can find 'DHCP Server' on Web Server as follow:

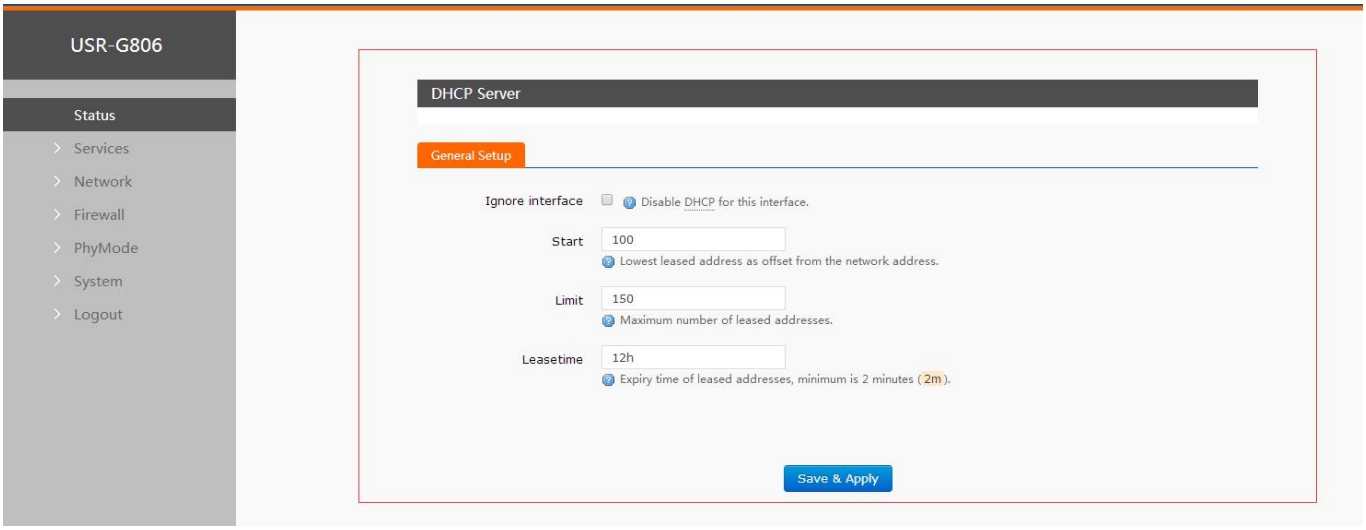

Figure 12 DHCP function

3.4.2 WAN Interface

G806 supports one WAN interface and WAN interface can switch between WAN/LAN interface. WAN interface supports DHCP and Static IP, and default setting is DHCP.

User can configure WAN interface by Web Server as follow:

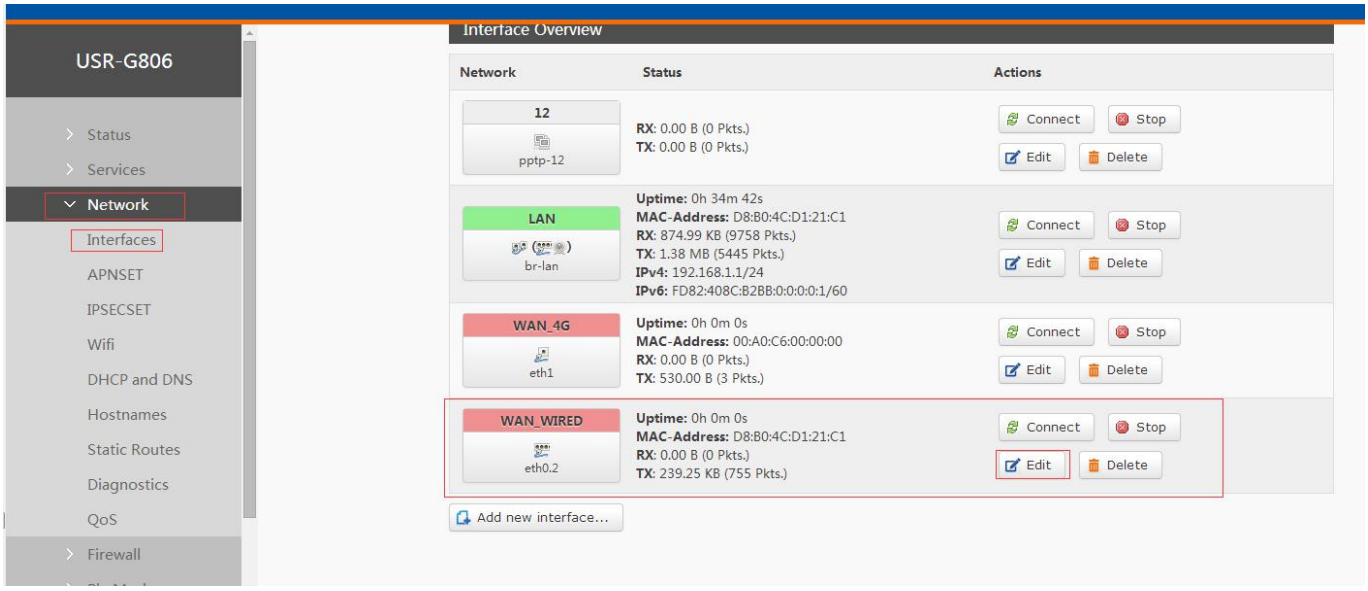

Figure 13 WAN interface

3.4.3 WLAN Function

G806 supports at most 24 STA devices connected. The maximum coverage of WIFI is 180m

Default parameters as follows:

SSID	USR-G806-XXXX(XXXX is MAC)

Password	www.usr.cn
Channel	Auto
Bandwidth	40MHz
Encryption Mode	WPA2-PSK

WLAN interface on Web Server as follow:

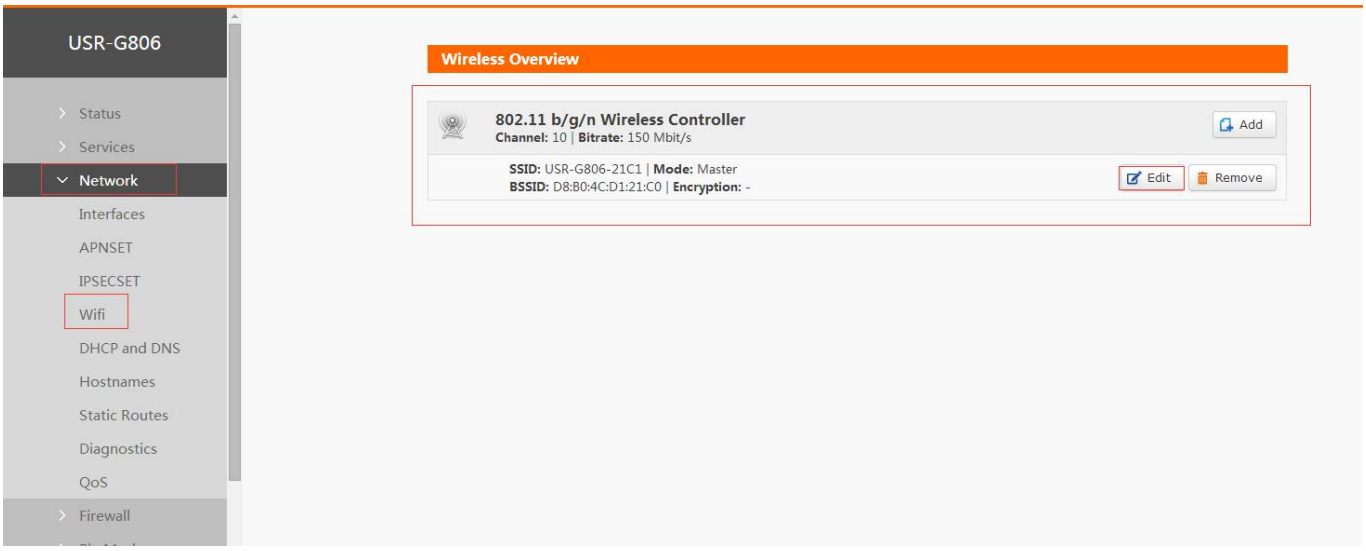

Figure 14 WLAN interface

After clicking “Edit” and entering WLAN interface configuration web, user can change follow parameters.

User can configure SSID on Web Server as follow:

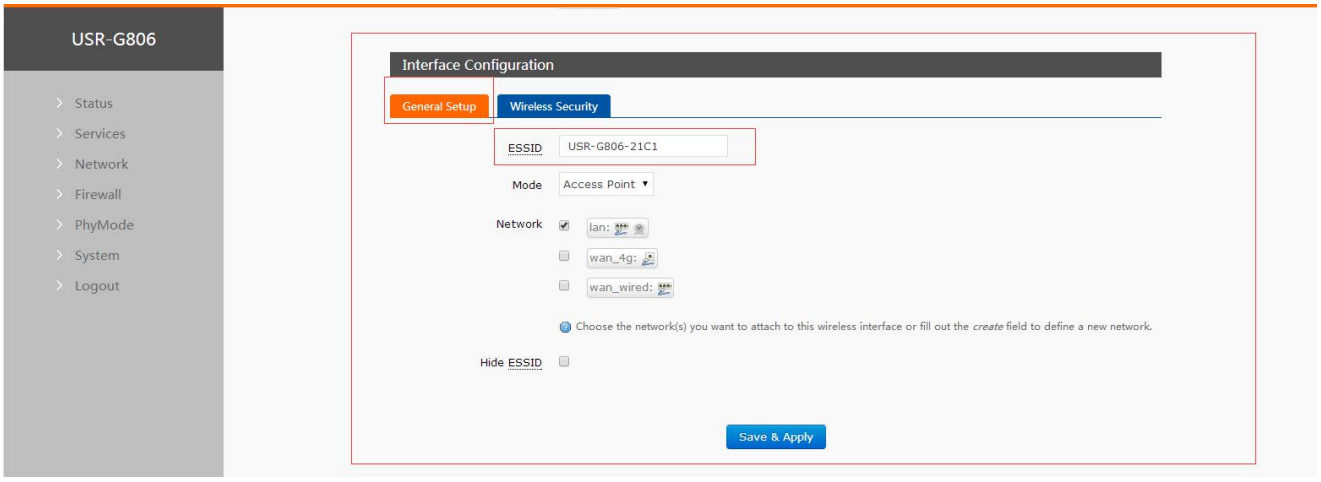

Figure 15 Configure SSID

User can configure password on Web Server as follow:

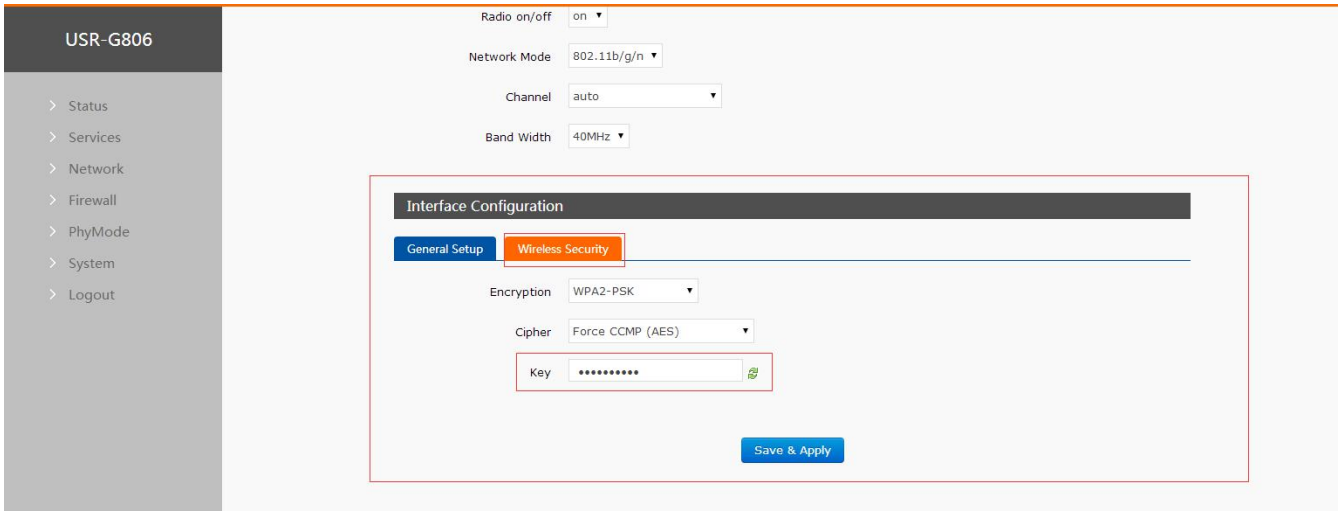

Figure 16 Configure password

Other settings on Web Server as follow:

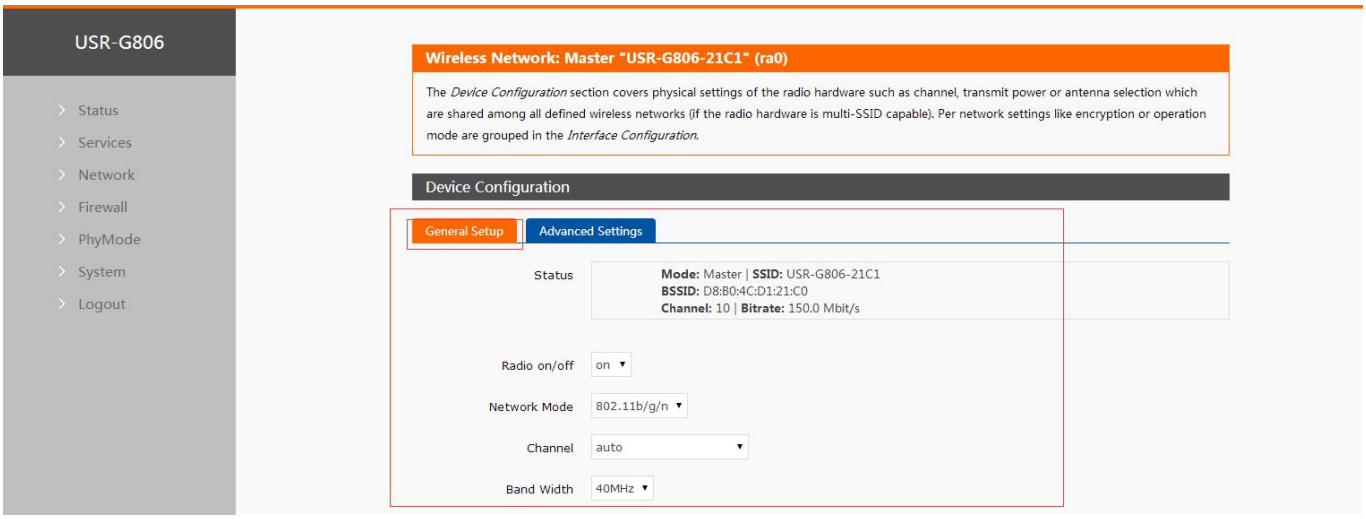

Figure 17 Other settings

User can close WLAN interface by changing ‘Radio on/off’ to off.

3.4.4 4G Interface

G806 supports one 4G interface to access internet. Functional diagram as follow:

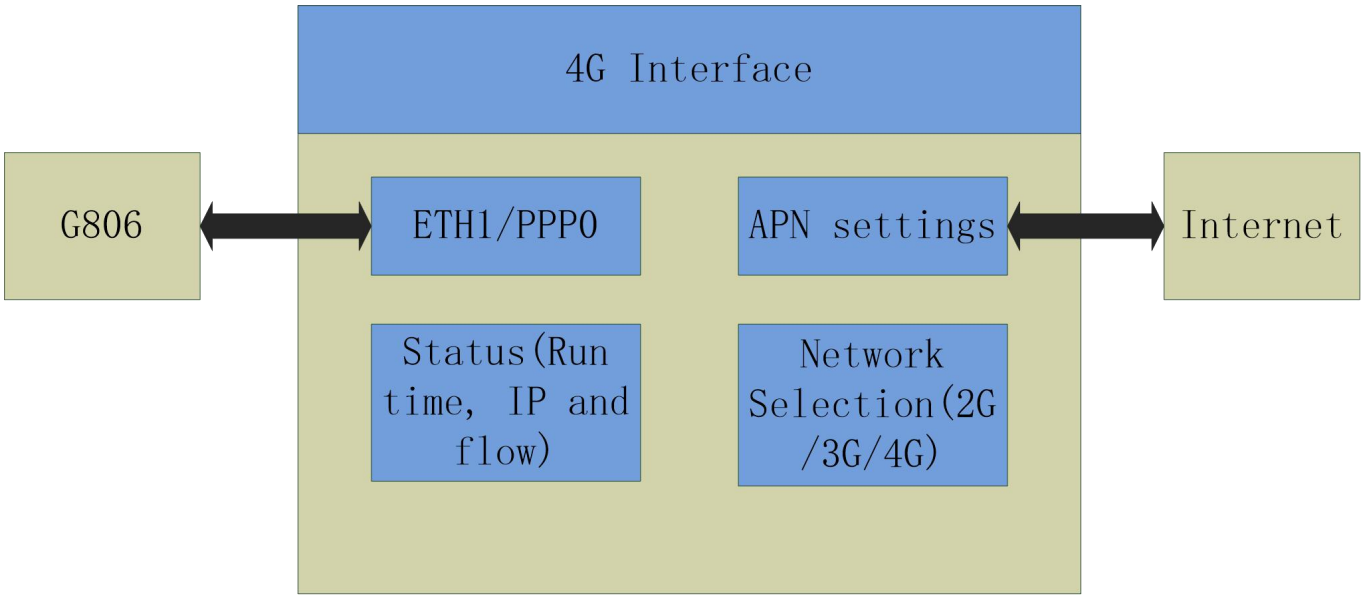

Figure 18 4G interface

User can configure 4G interface by Web Server as follow:

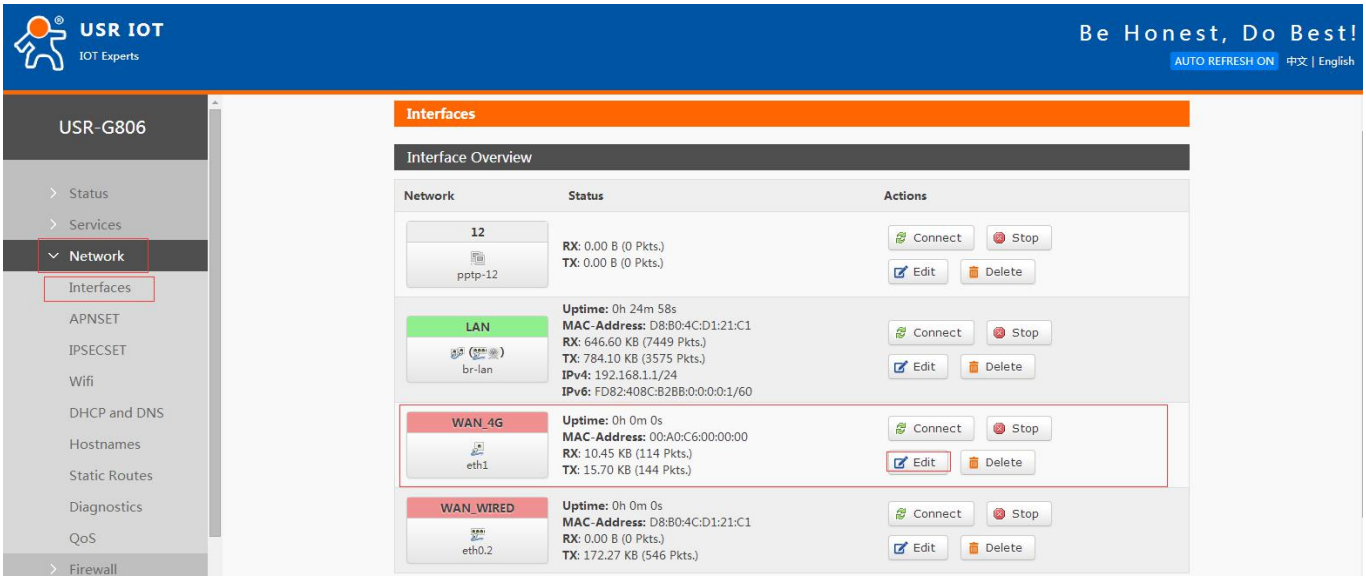

Figure 19 4G interface

3.4.5 APN

APN configuration by Web Server as follow:

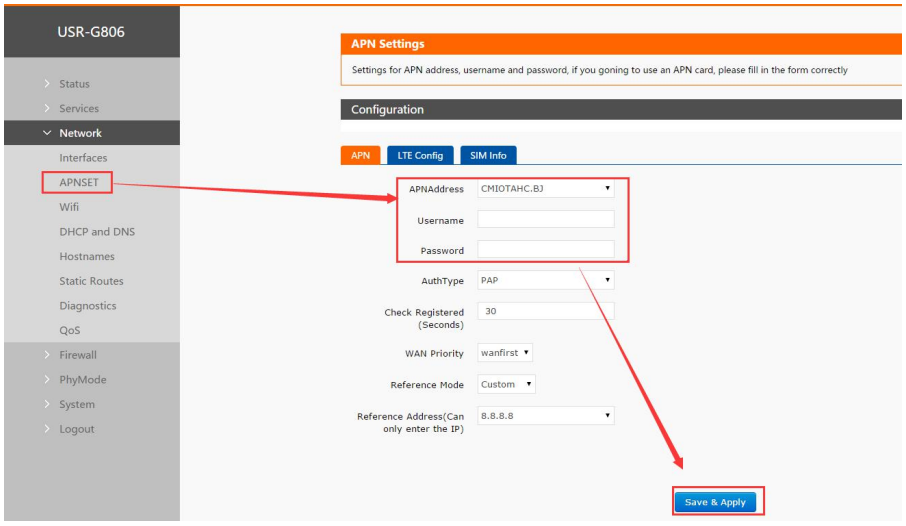

Figure 20 APN configuration

To choose the network type, please configure the LTE.

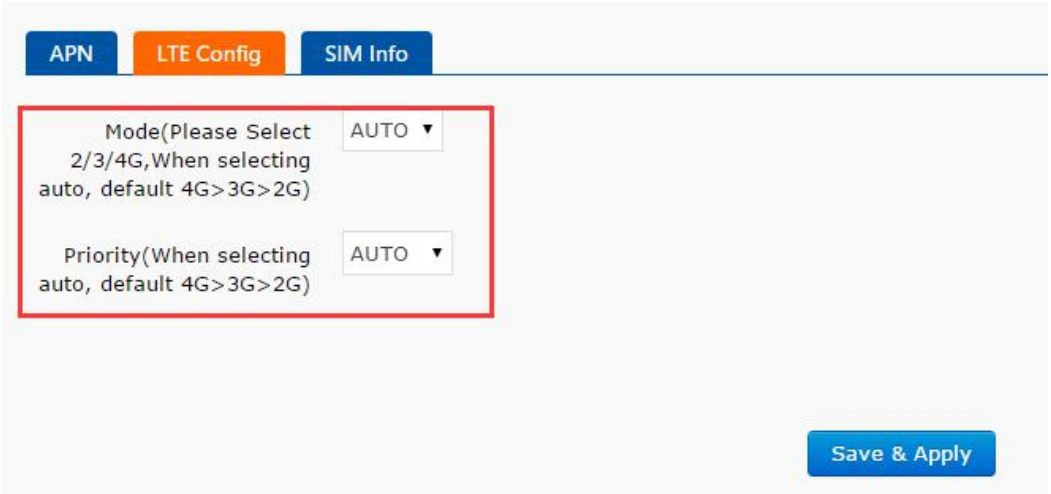

Figure 21 LTE configuration

3.5. VPN Client

3.5.1 PPTP Client

We first create VPN Server on the server.

Open the network connection page on the server (remote server) and click File - > New incoming connection.

Then, select Add account, please enter user name, password and other information..

Click Next and check through Internet to connect to this computer.

Then, select "Internet Protocol Version 4" to set the properties of the incoming IP, IP address assignment select "Specify IP Address", then select "OK" and "Allow Access".

Now we create a VPN server.

Let's talk about the use of VPN Client. We are looking for a computer in the LAN to ensure that it can access the server above. Then create a new VPN connection.

In the connection box, click "Properties", the tab can set the target address (the address of the VPN server),

security options to select "PPTP protocol", after the point is determined, enter the username, password.
Click the "Connect" button, after the connection is successful, you can see the VPN network card connection, from grey to bright color, representing the VPN connection has been successfully established.
Next we use the PPTP Client on the router to replace the way of computer dialing.
Assuming that the user has obtained the VPN server address, account and password, we create an interface, select the PPTP protocol, and write the other parameters in turn.

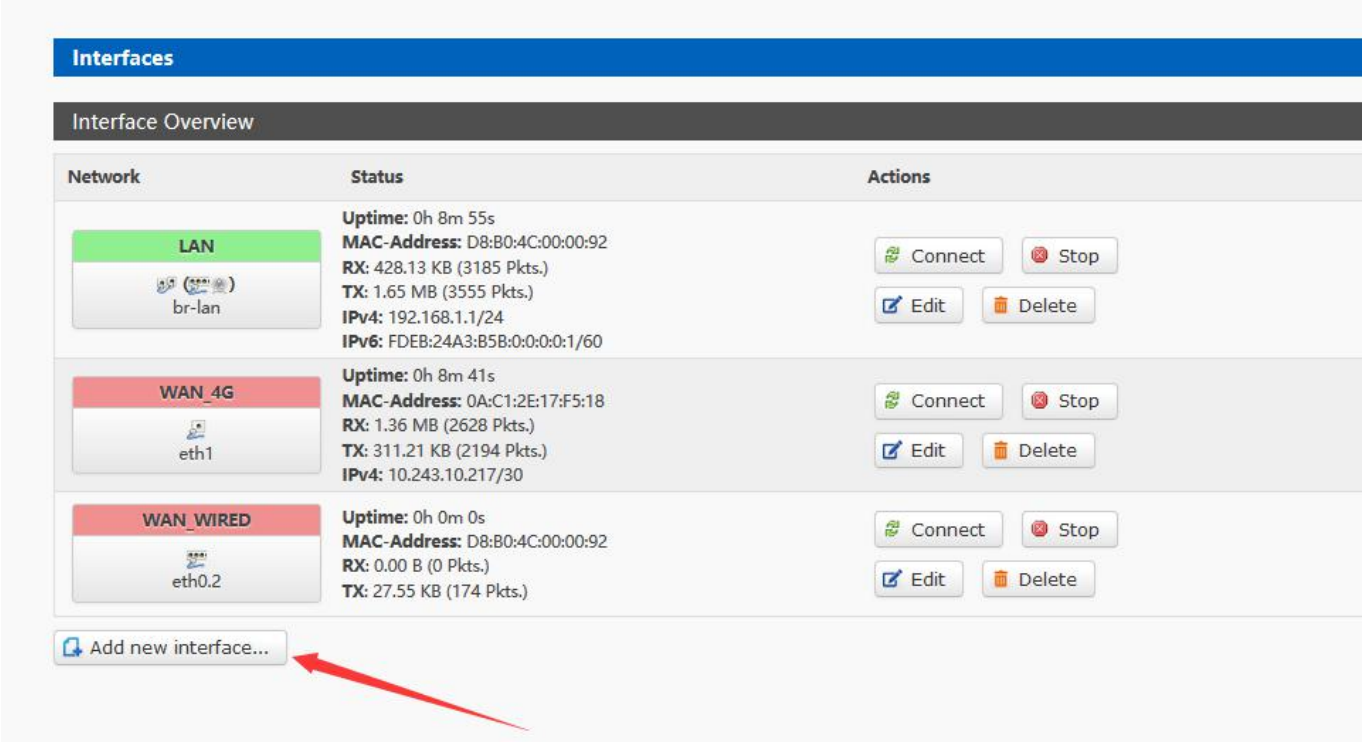

Figure22 the webpage1 of VPN

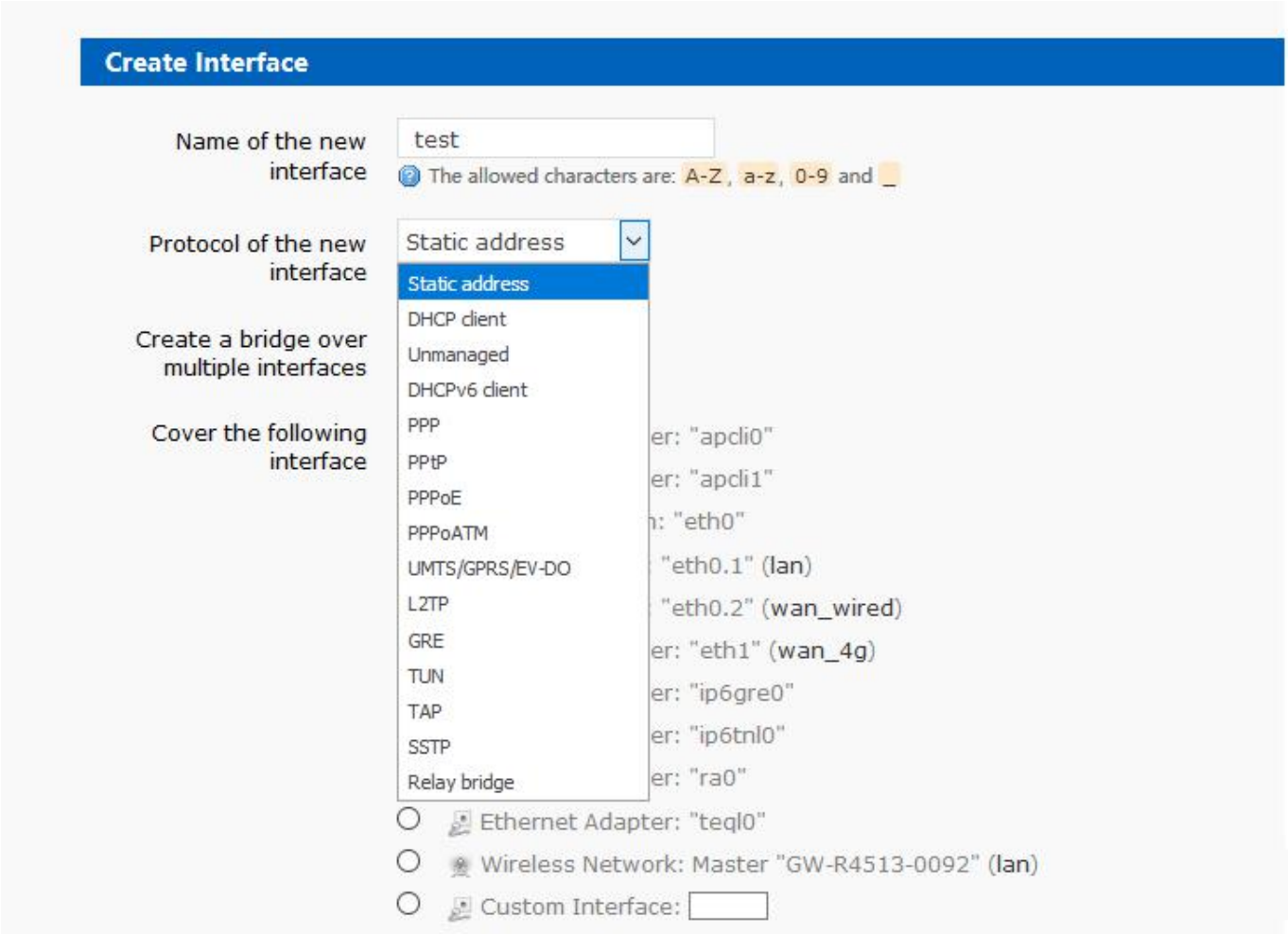

Figure23 the webpage2 of VPN

Select WAN, because it is dialing at WAN port, then save and apply.

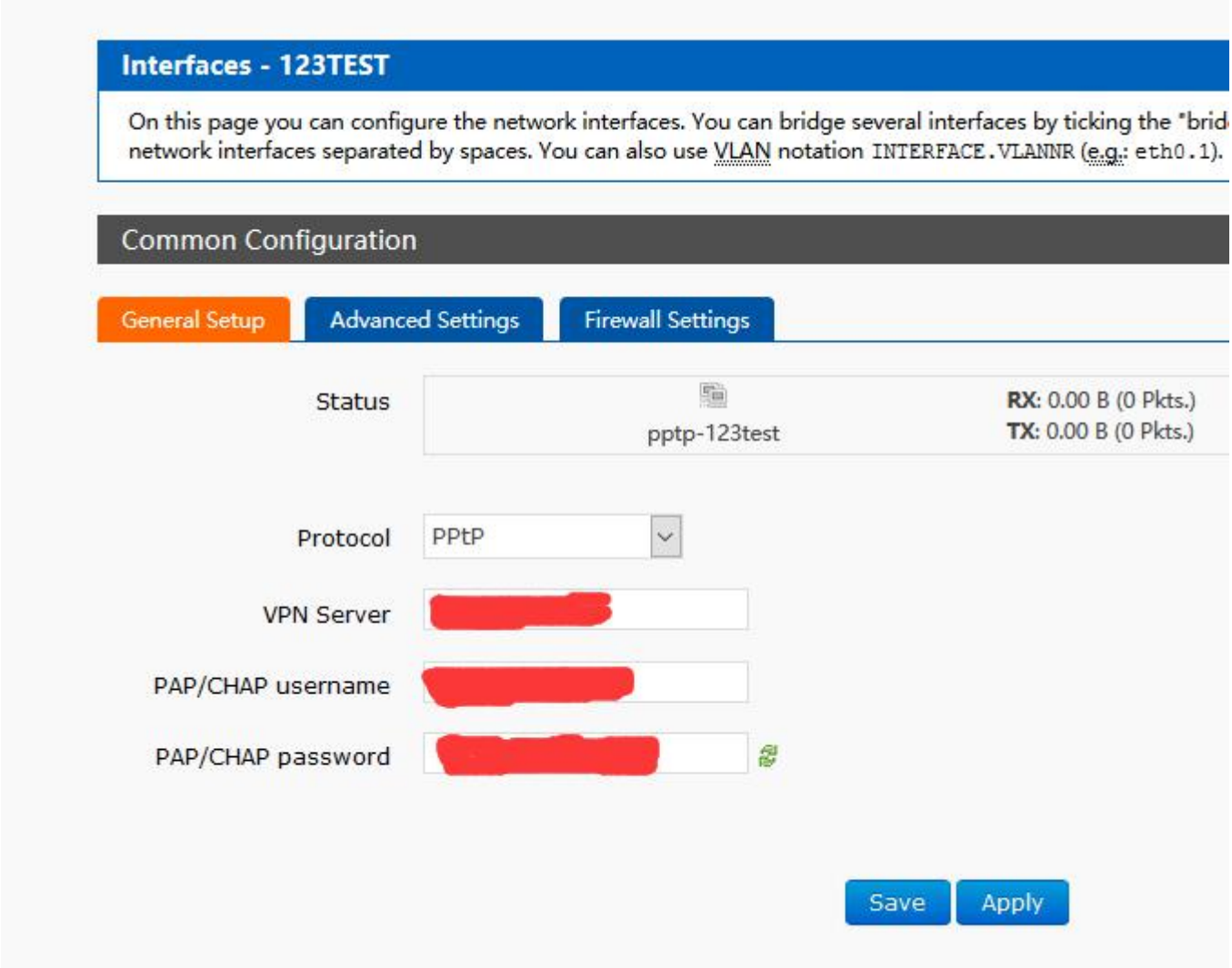

Figure24 the webpage3 of VPN

Wait a minute or restart the router, when you see the "VPN" interface in the router page, there is a run time (not 0), indicating that the current VPN has been successfully started.

Note:

- Currently PPTP supports MPPE encryption and a variety of authentication methods. Specific settings can be viewed in advanced settings for authentication.
- Only MSChapV2 indicates that MPPE encryption is only supported.
- MSChapV2 EAP PAP CHAP supports MPPE encryption and multiple authentications.
- Other means do not handle, default status, only CHAP authentication by default.

3.5.2 L2TP Client

L2TP is a layer 2 tunneling protocol, similar to PPTP. At present, G806 supports various authentication methods such as tunnel password authentication, CHAP, etc., supporting encryption methods of MPPE and pre-shared key encryption methods of L2TP OVER IPSEC.

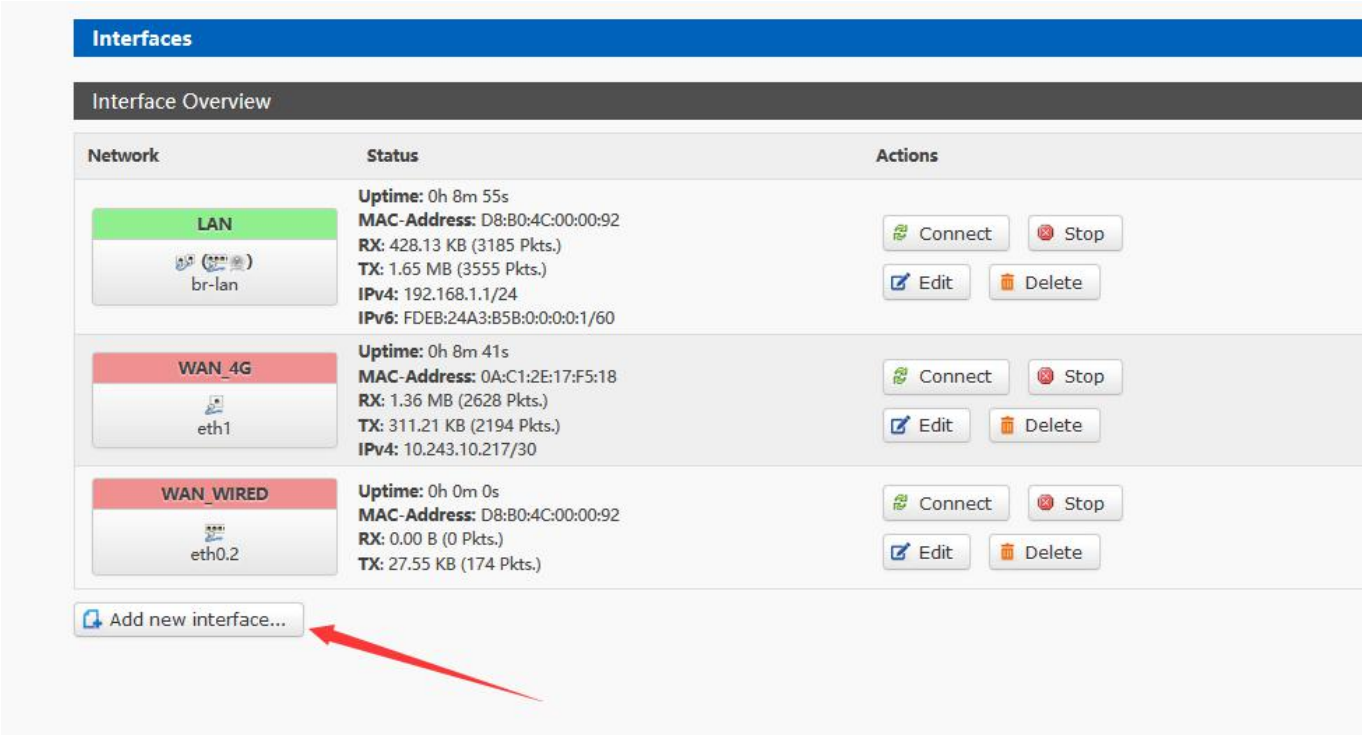

Figure25 create interface

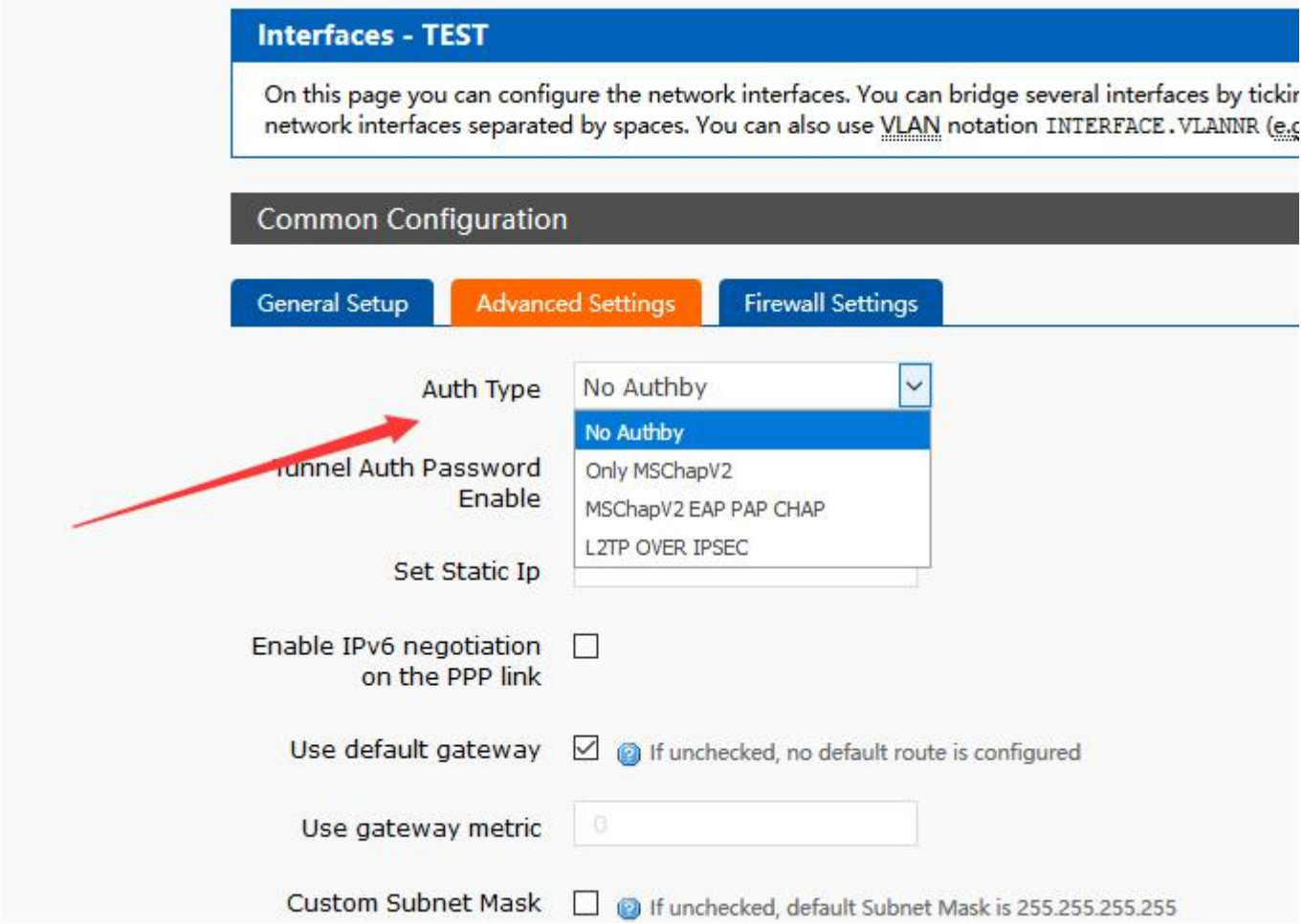

Figure26 auth type

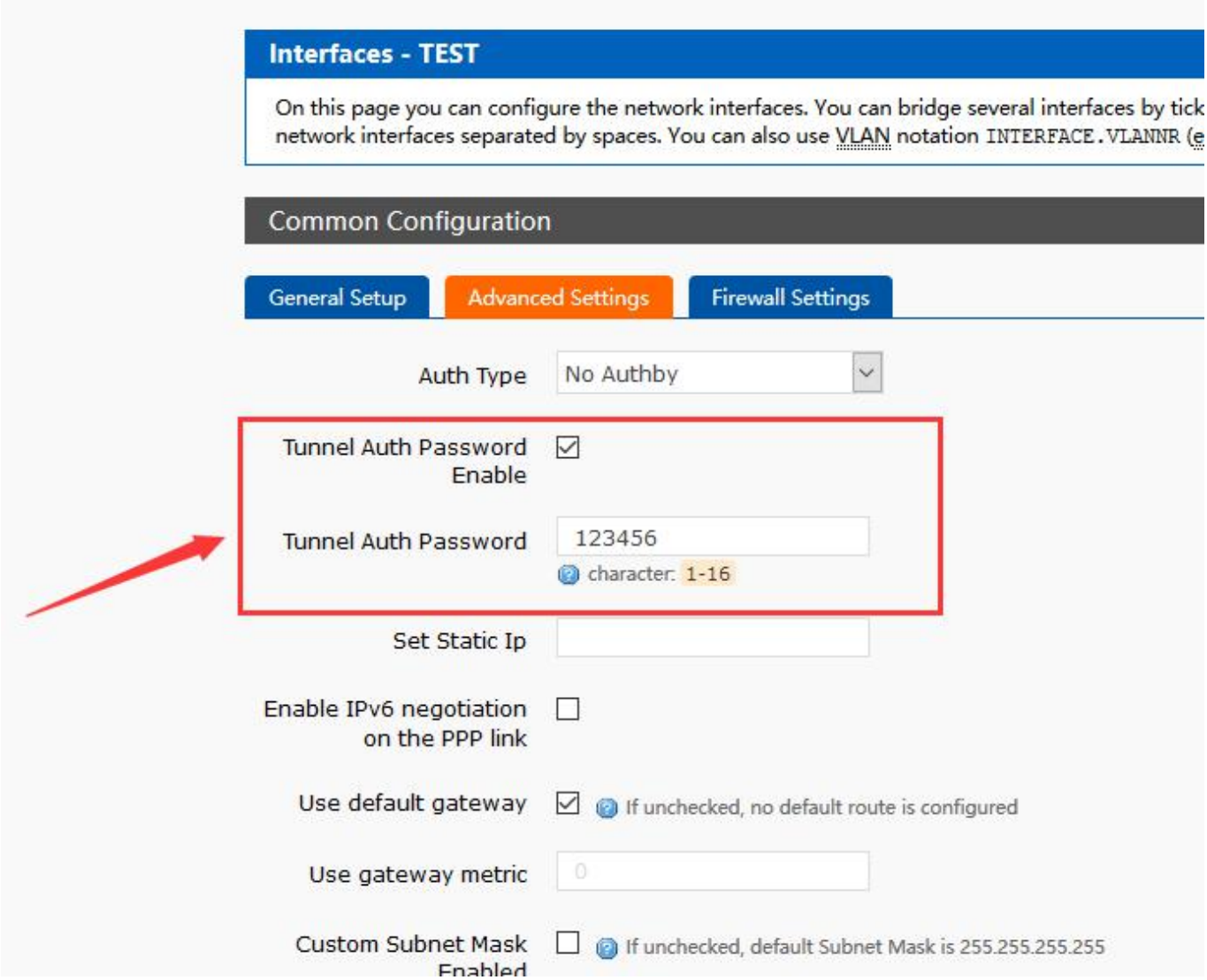

Figure27 tunnel auth password

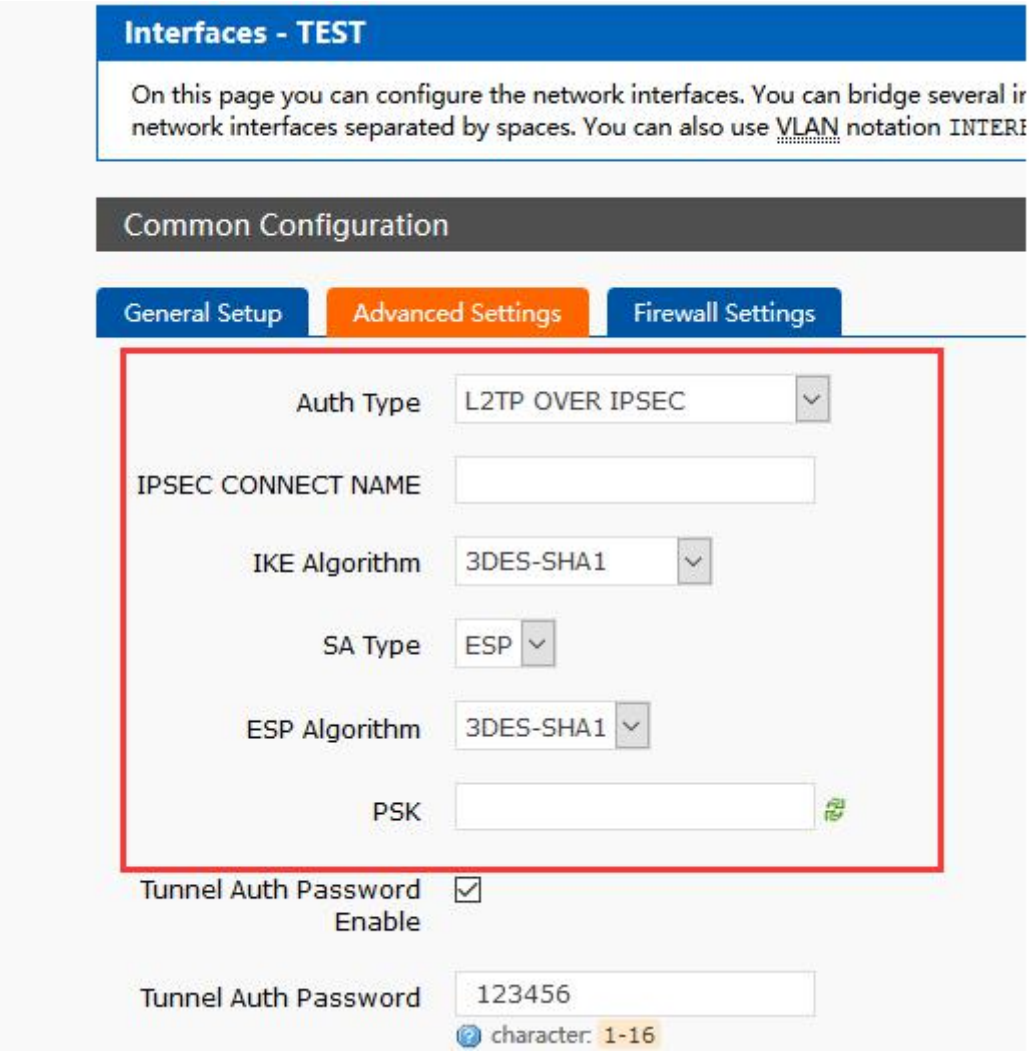

Figure28 L2TP OVER IPSEC auth type

3.5.3 IPSEC

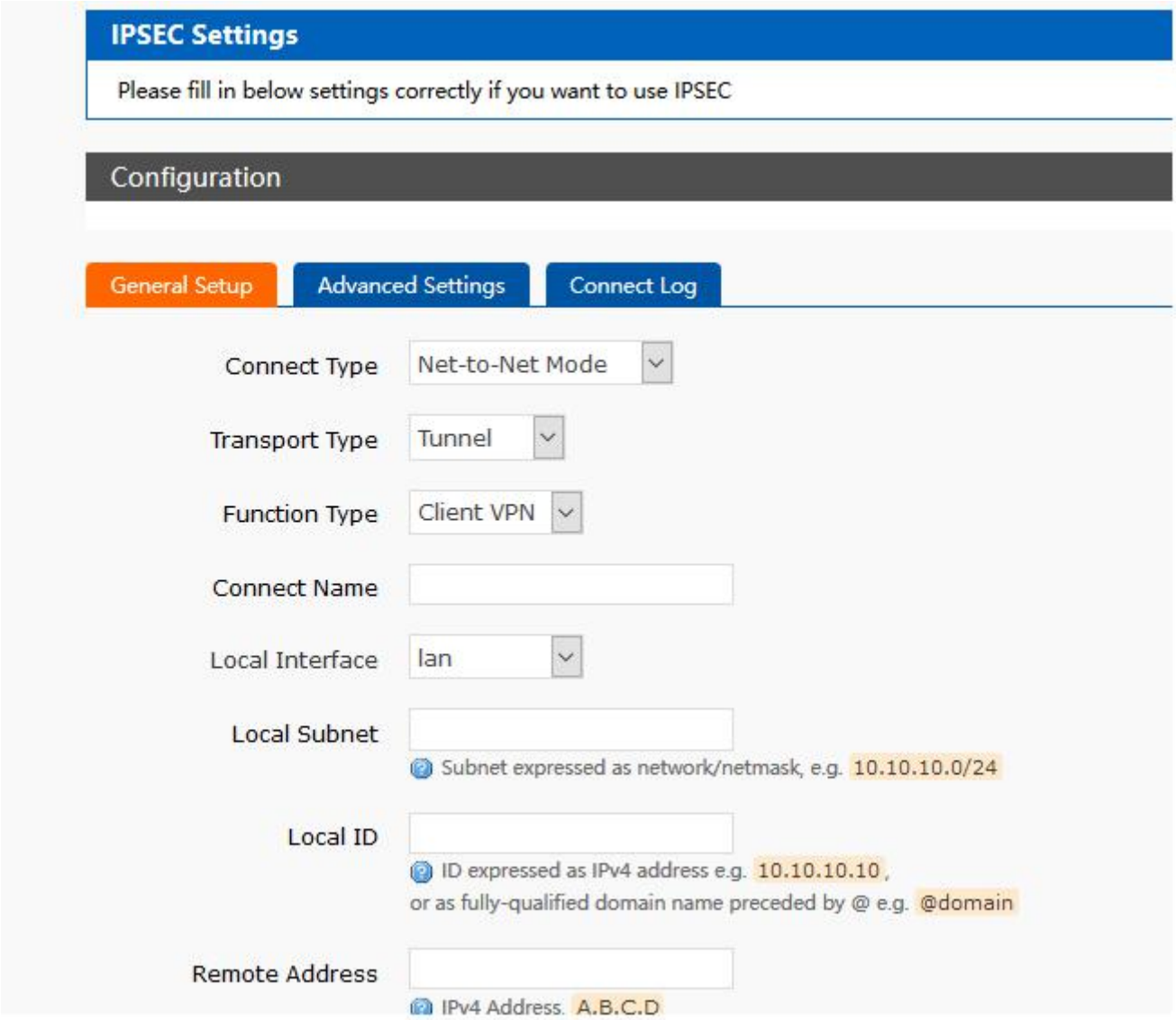

Figure29 IPSEC setting

Selection of application modes: Net-to-Net mode (site-to-site or gateway-to-gateway), Road Warrior mode (end-to-site or PC-to-gateway)

- Transmission mode selection: tunnel mode and transmission mode. It can be selected in the transport type.
- Functional types: VPN client and VPN server.
- Connection name: indicate the name of the connection, must be unique.
- Local interface: wan_wried, wan_4g.
- Remote address: IP/ domain name.
- Local Subnet: IPSEC Local Protected Subnet and Subnet Mask. If you choose the Road Warrior client, you do not need to fill in.
- For terminal network: IPSEC end protection subnet and subnet mask.
- Local terminal identifier: the channel local identifier can be IP or domain name. Note that when the domain name is customized, add @

- End terminal identifier:the channel end identifier, it can be IP or domain name. Note that when domain name is customized, add @

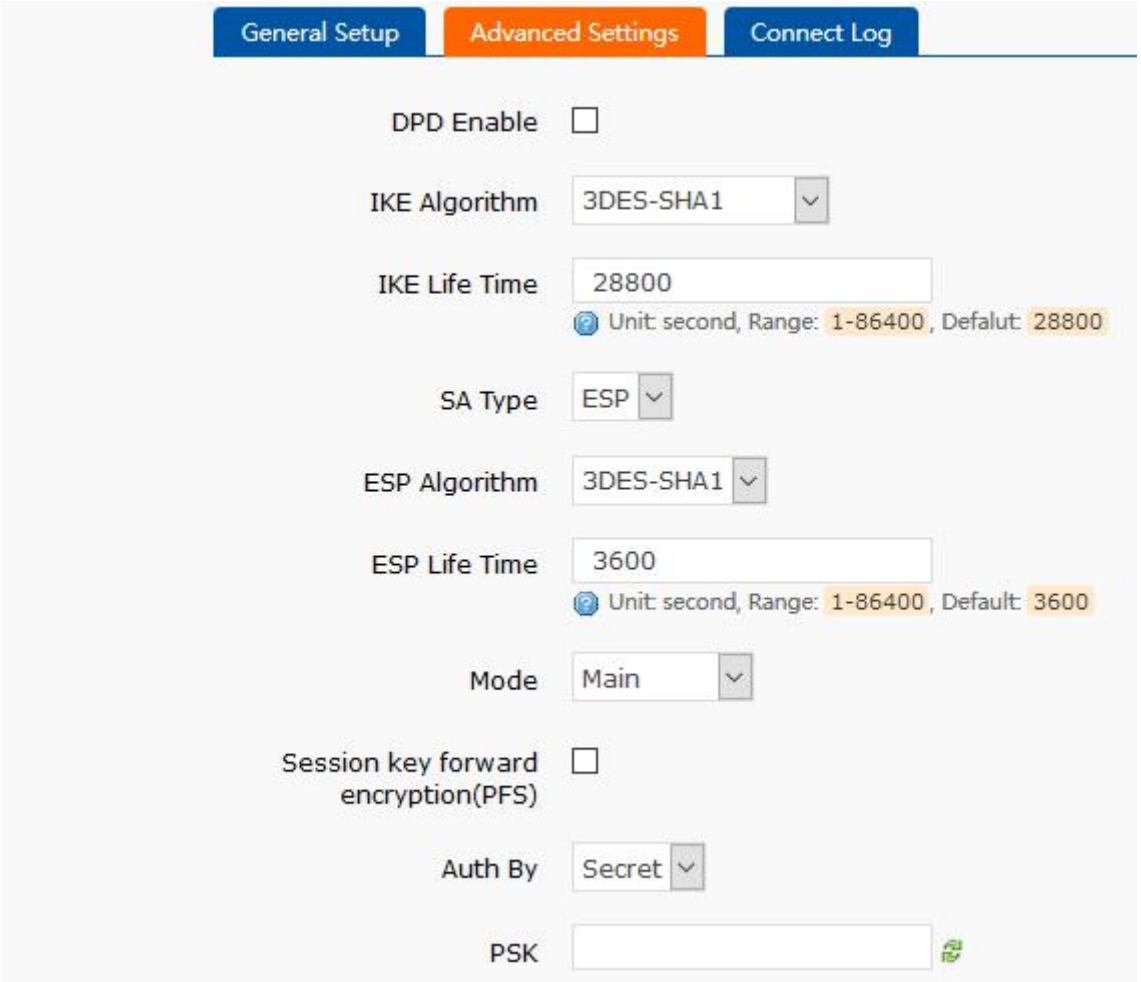

Figure30 IPSEC advance setting

Start DPD detection: whether to enable this function, hook is indicated to enable.
DPD interval: set the time interval of connection detection (DPD).
DPD timeout time: set up the timeout time of connection detection (DPD).
DPD operation: sets the operation of connection detection.
IKE encryption: the first phase includes encryption, integrity and DH switching in the IKE stage.
IKE life cycle: set the life cycle of IKE, in seconds, default: 28800.
SA type: ESP and AH can be selected in the second stage.
ESP encryption: select the corresponding encryption mode and integrity scheme.
ESP life cycle: set ESP life cycle, unit: s, default: 3600
Mode: negotiation mode default main mode, aggrmode can be selected.
Session secret key forward encryption (PFS): if hook is activated, PFS will enable.
Authentication method: currently supports the pre shared key authentication method.

Note

After the configuration, the ISAKMP SA established flag in the connection log indicates that the IPSEC VPN was created successfully.

3.5.4 OPENVPN

Add one interface, choose TUN or TAP mode:

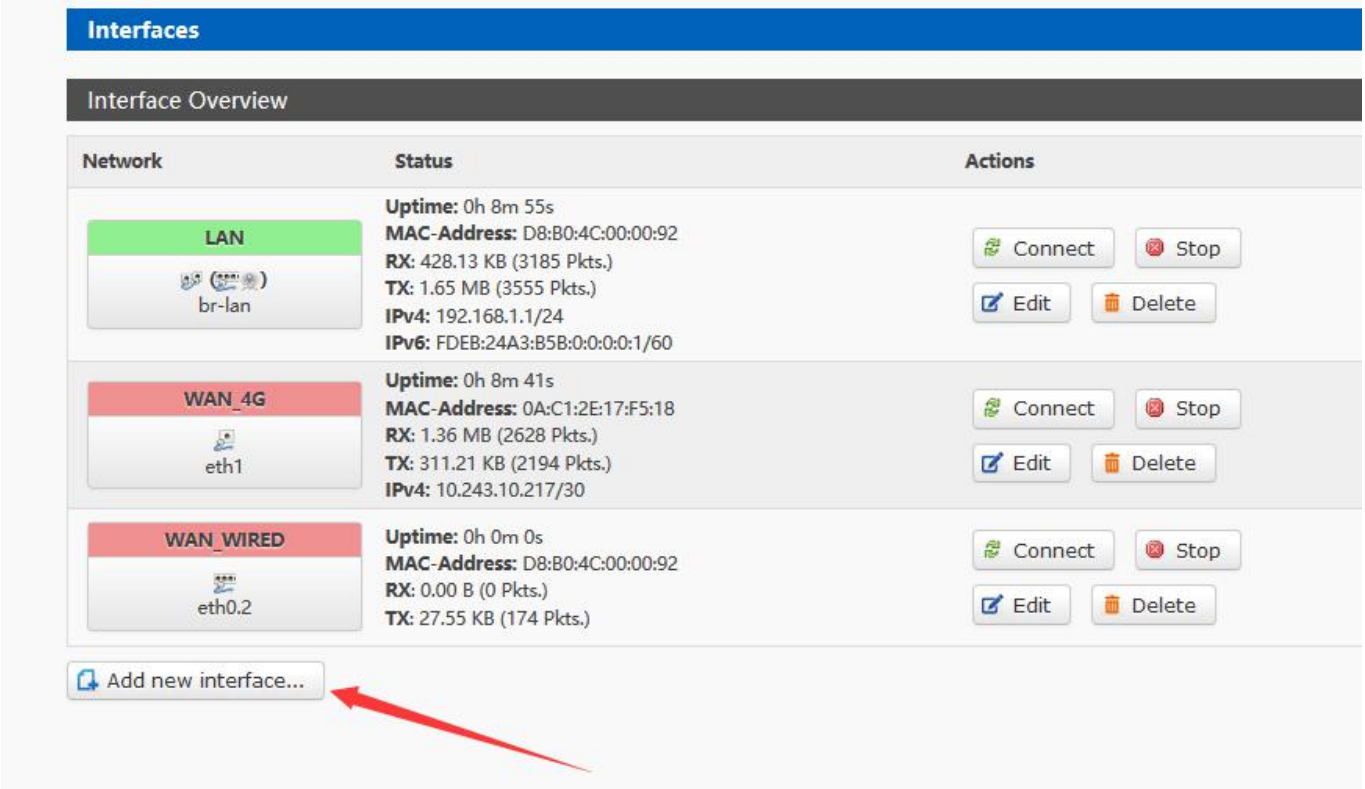

Figure31 add new interface

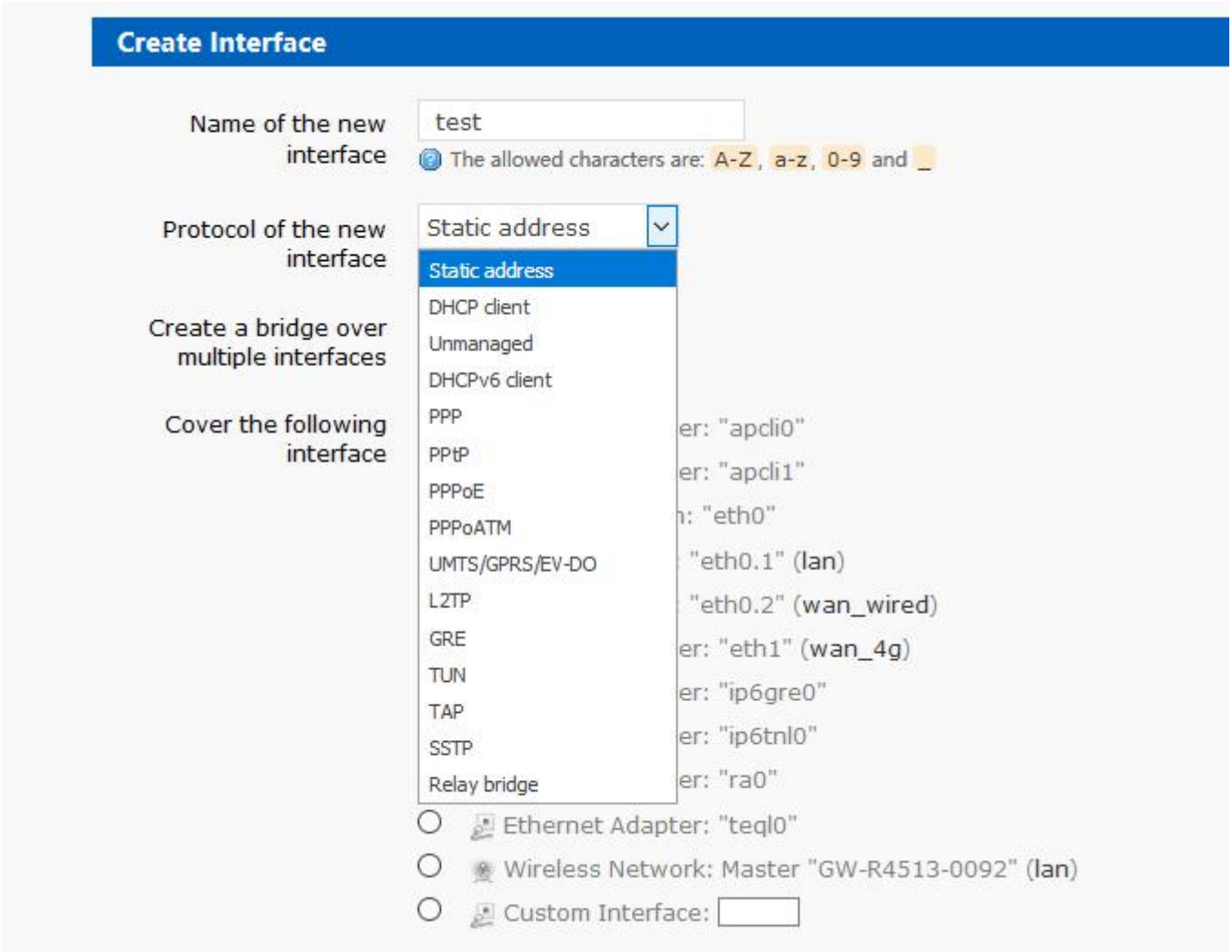

Figure32 add OPENVPN interface

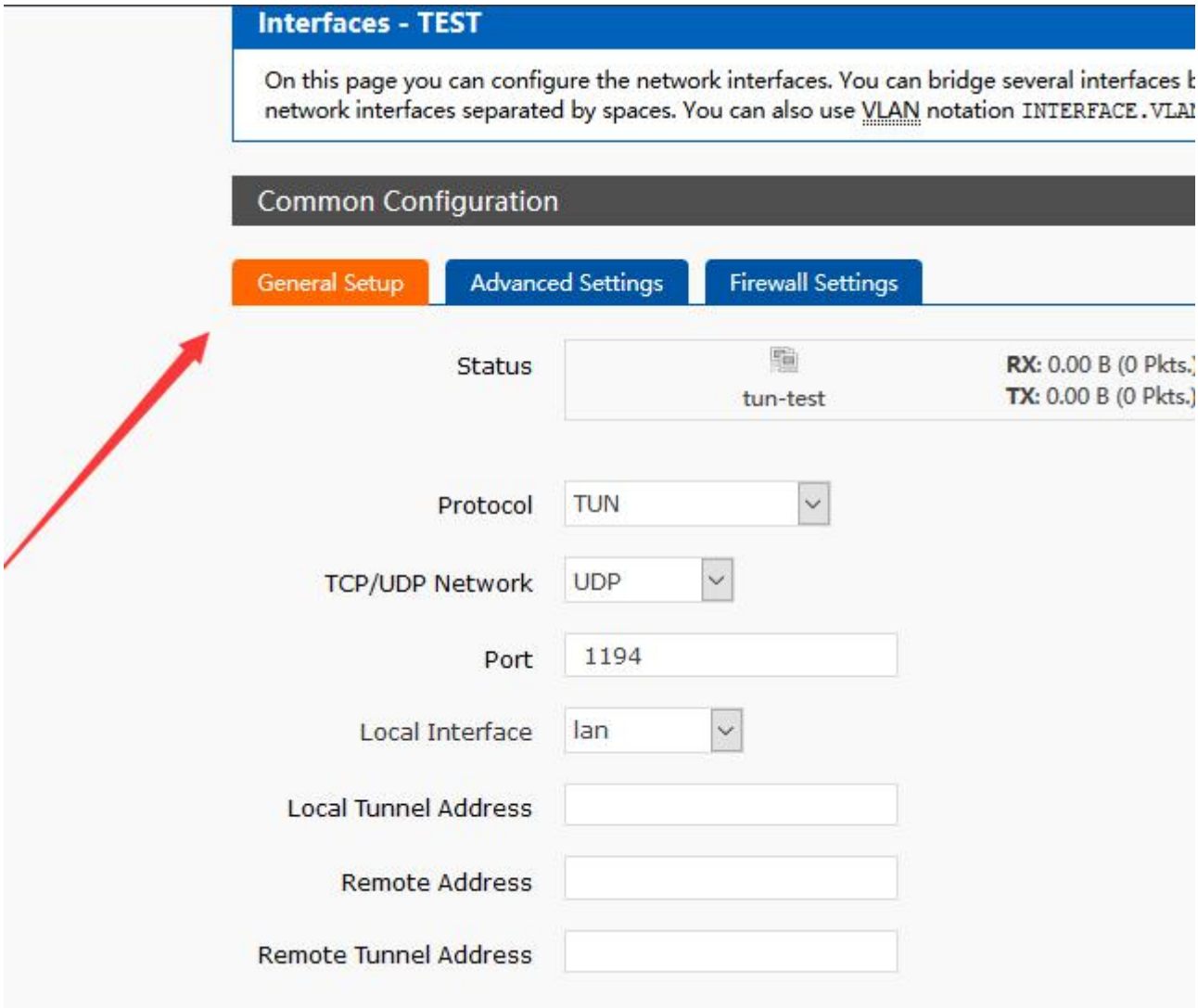

Figure33 general setting

Protocol: TUN (routing mode) or TAP (bridge mode).

Channel protocol: UDP or TCP

Port: the listening port of the OPENVPN client.

Interface of this terminal: it can be wan_wired and wan_4g.

Remote address: the IP/ domain name of the server.

Local tunnel address: set the local tunnel address, such as 192.168.10.1, otherwise the default server automatically allocates.

Remote Tunnel Address: set the tunnel address on the opposite side, such as 192.168.10.1, otherwise the default server automatically allocates.

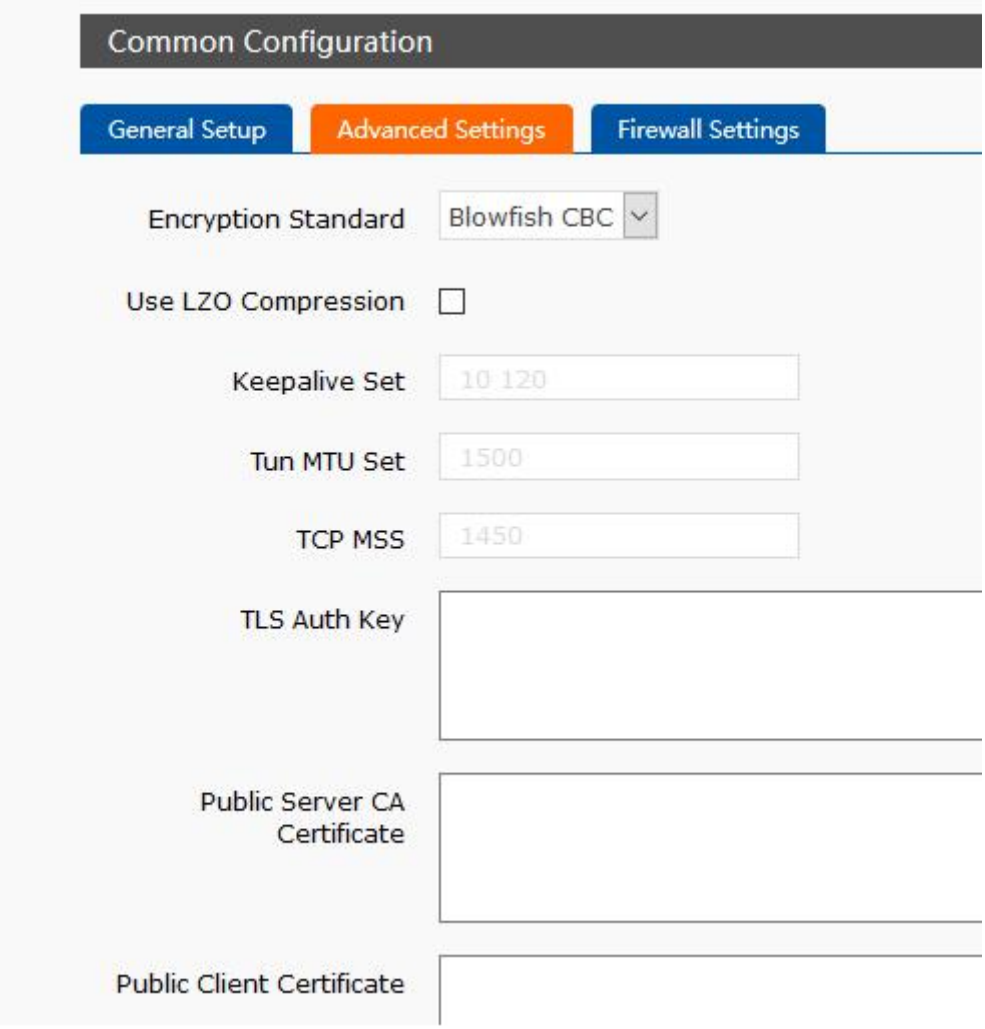

Figure34 advance setting

Encryption Standard: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

LZO compression: enable or disable transmission data using LZO compression.

Keep-alive settings: default is 10120.

TUN MTU settings: set the MTU value of the channel.

TCP MSS : maximum segment size of TCP data

TLS authentication key: authentication key of secure transport layer

Public service CA certificate: CA certificate of server and client public

Public client certificate: client certificate

Client private key: client key

Note

1. Before the client connects to the server, the Ca certificate, the client certificate, the client key, the TLS authentication key, these need to be provided by the server.

2. After obtaining the certificate file, copy the different certificate contents into the edit box corresponding to the configuration interface.

3.5.5 GRE

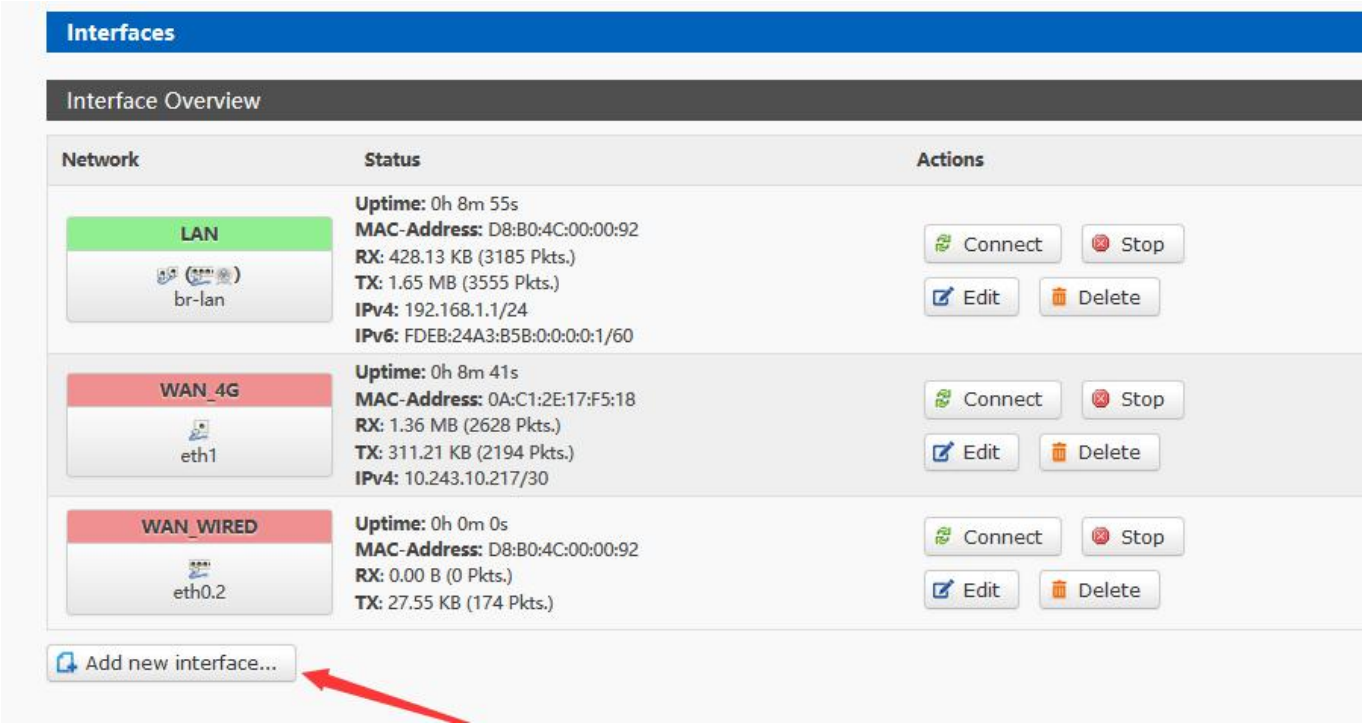

Figure35 add new interface

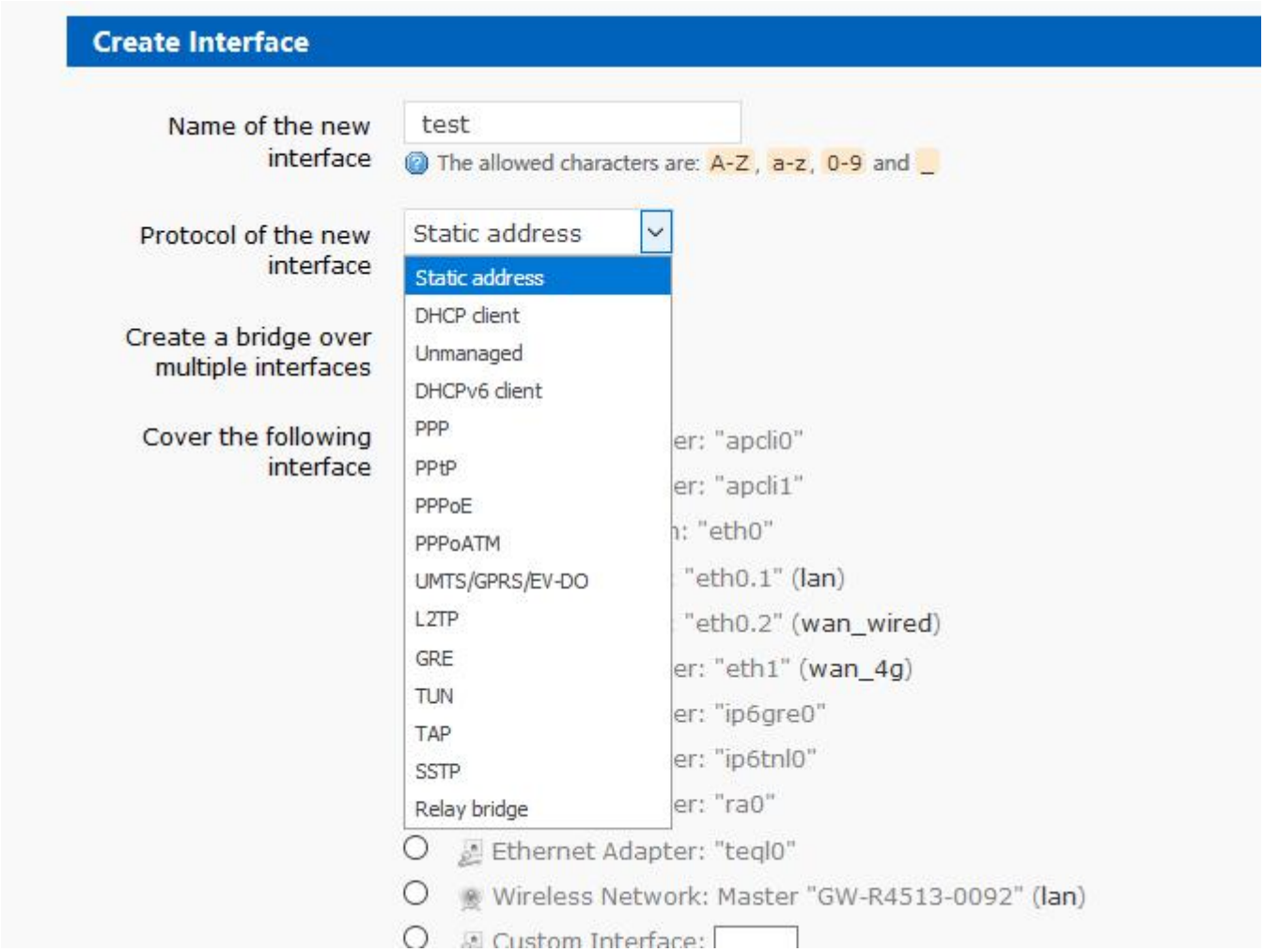

Figure36 add GRE interface

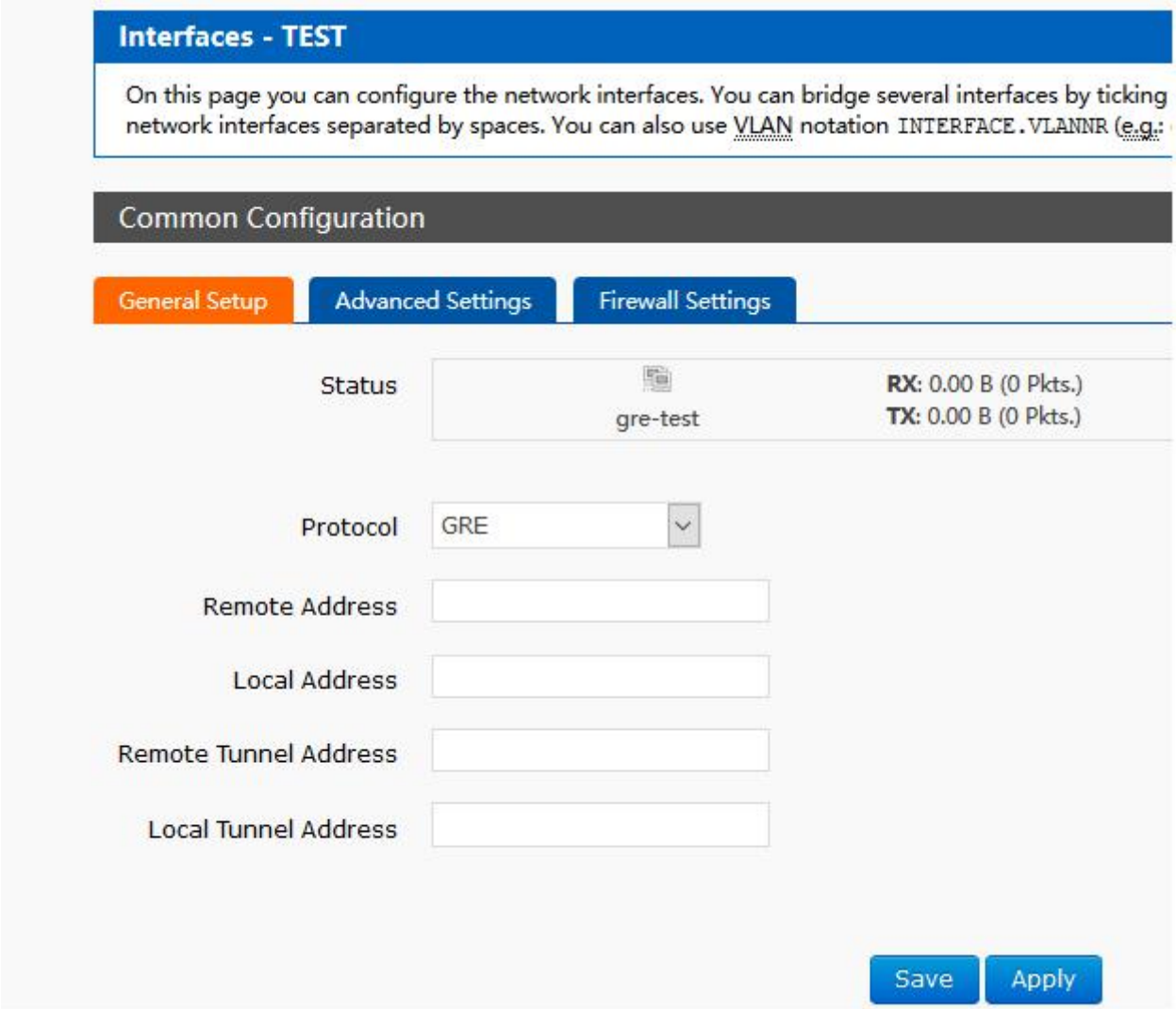

Figure37 GRE general setting

Remote address: IP address for WAN port of terminal GRE

Local address: the local address of wan_wried and wan_4g, users need fill in one of them according to need.

Remote Tunnel Address: the opposite GRE tunnel IP.

Local Tunnel Address: the local GRE tunnel IP.

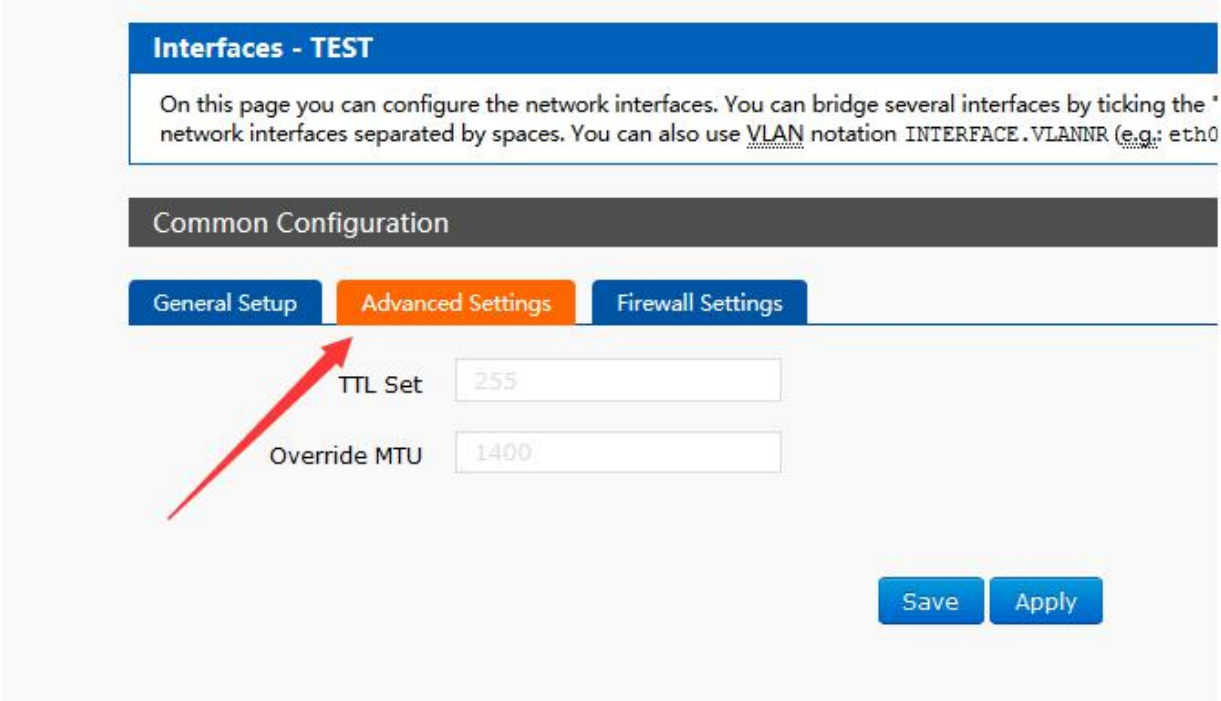

Figure38 GRE advance setting

TTL settings: set the TTL of the GRE channel, by default 255

Set MTU: set the MTU of the GRE channel, by default 1400

3.5.6 SSTP Client

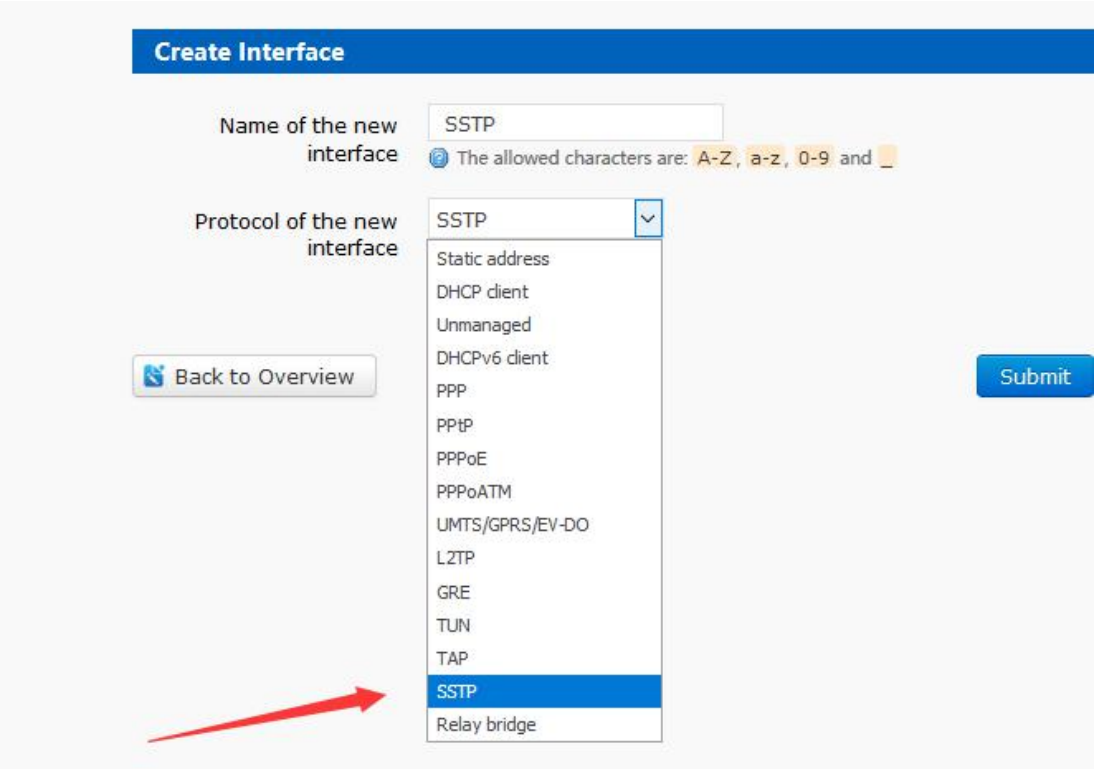

Figure39 add new interface

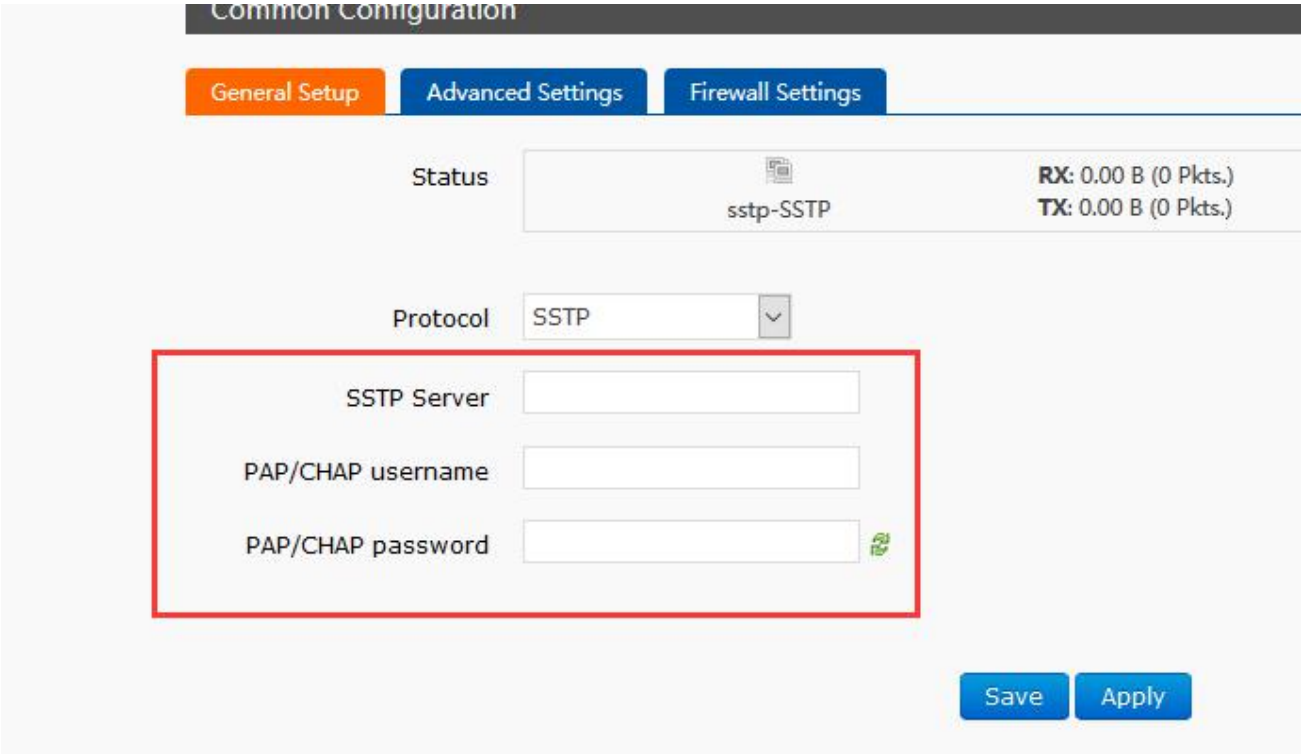

Figure40 SSTP general setting

SSTP server: the IP or domain name of the SSTP server.

PAP/CHAP Username: user name of SSTP

PAP/CHAP password: the password of SSTP

Note

Advanced settings can refer to advanced settings of PPTP.

3.6. Static Router

Static routing describes the routing rules of Ethernet packets.

3.7. NAT Function

3.7.1 MASQ

MASQ, MASQUREADE, address masking, will leave the packet source IP into a router interface IP address, such as check IP dynamic masking, the system will flow out of the router packet source IP address changed to WAN port IP address.

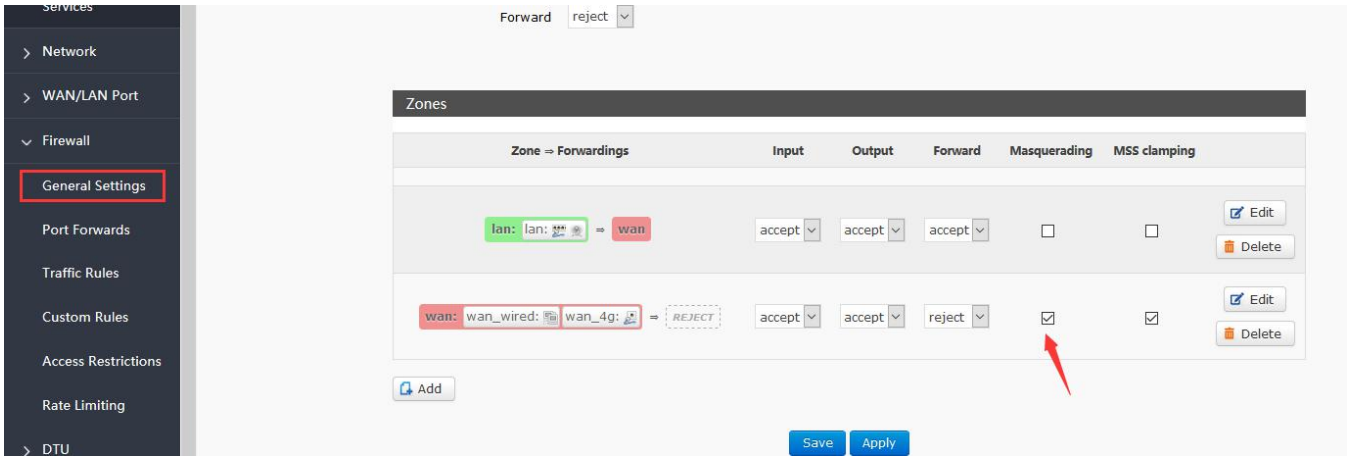

Figure41 MASQ setting

3.7.2 SNAT

Source NAT changes the source address of the packet leaving the router, closing the IP dynamic camouflage of the WAN port first when used.

Then setup SourceNAT.

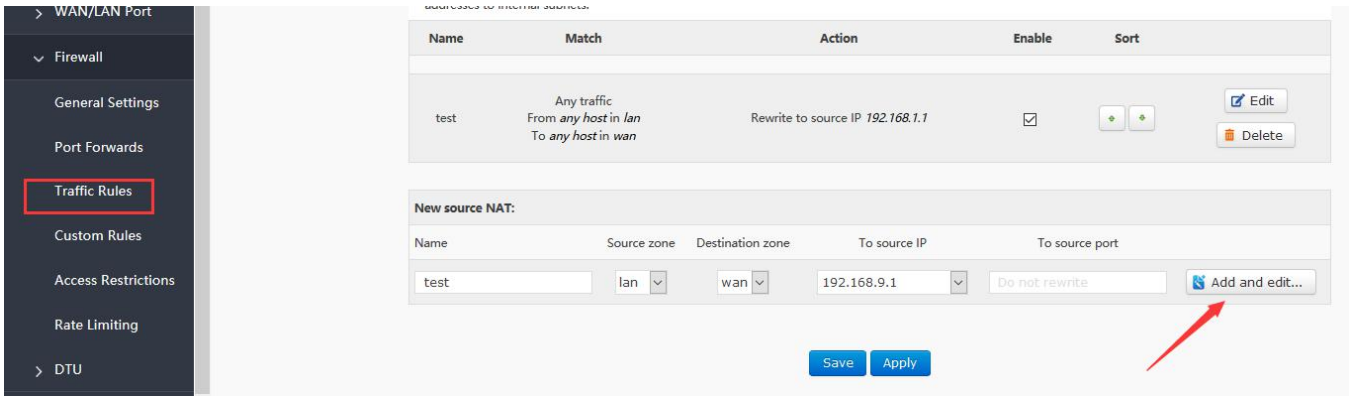

Figure42 NAT setting1

Figure43NAT setting2

Keep the source IP, port, the remote IP, port by default, then save.

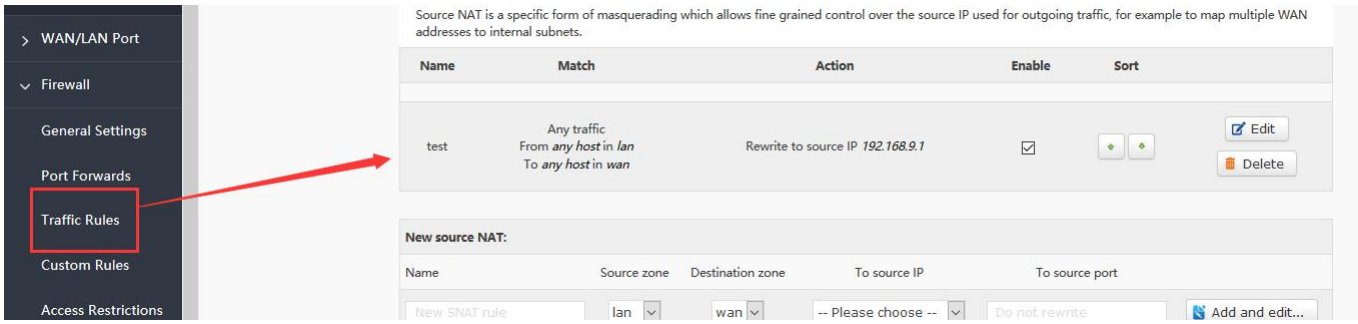

Figure44 NAT setting3

3.7.3 DNAT

DNAT is the replacement of destination addresses, replacing the destination IP address of packets that enter the router with the destination IP address of the WAN port IP with the user-set IP address

3.7.3.1 Port Forward

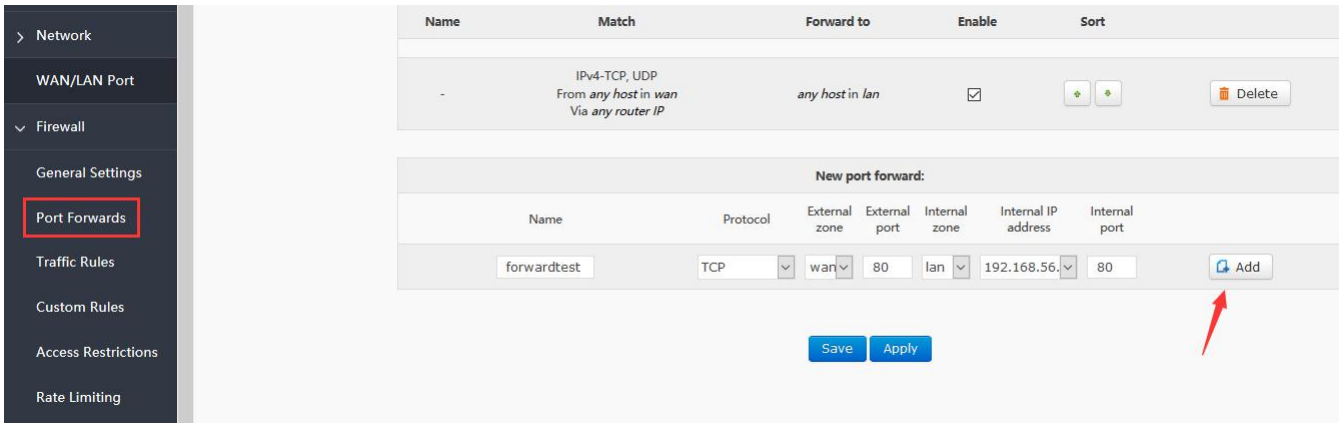

Figure45 port forward setting1

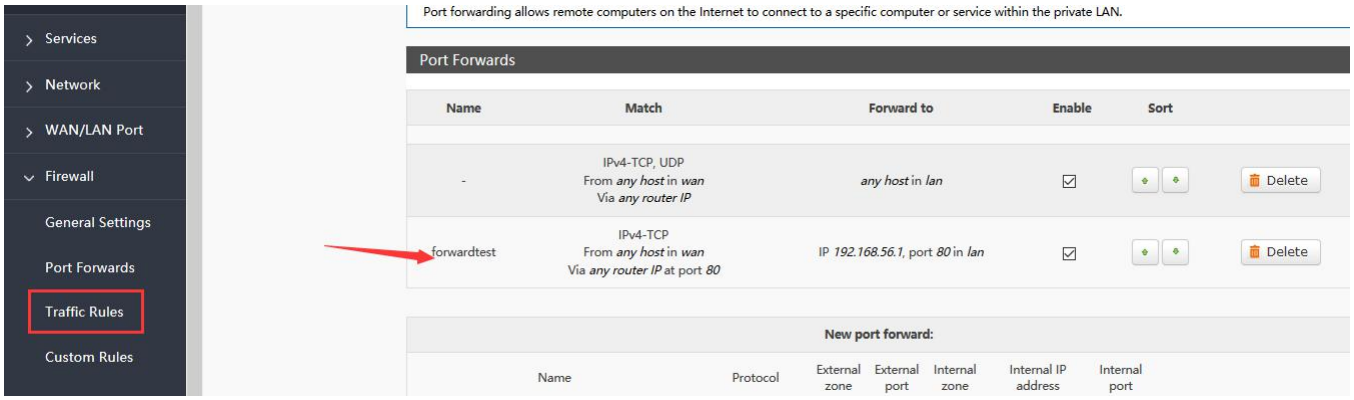

Figure46 port forward setting2

Then save the settings.

192.168.1.1:80 is the web server of routers. If we want to access a device in the LAN from the outside network,

we need to set the mapping from the outside network to the inside network, such as setting the outside network port to 81, the inside network IP 192.168.1.1, and the inside network port to 80.
When we access the 81 port from the WAN port, the access request will be transferred to 192.168.1.1:80.

3.7.3.2 NAT DMZ

Port mapping is to map a specified port of WAN port address to a host in the intranet. DMZ function maps all ports of WAN port address to a host. Setting interface and port forwarding are in the same interface. When setting up, the external port is not filled in.

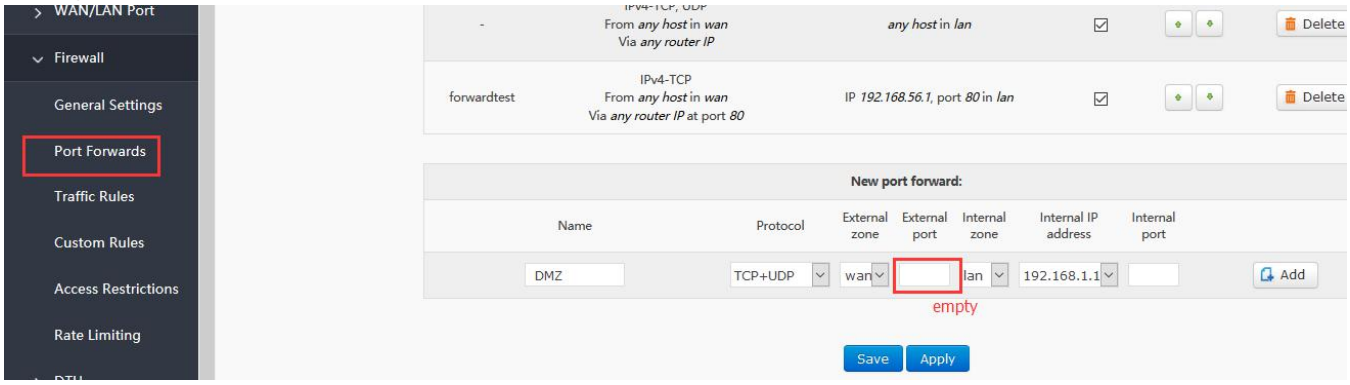

Figure47 DMZ setting1

Then add and save.

Figure48 DMZ setting2

As shown, all ports of the WAN address are mapped to the host 192.168.1.10 of the intranet.

Note

Port mapping and DMZ functions can't be used at the same time.

3.8. Access Restrictions

Access restriction implements the access restriction to the specified domain name, supports the blacklist and whitelist settings of domain name addresses. When a blacklist is selected, the device connecting the router can't access the domain name of the blacklist, and other domain name addresses can be accessed normally. When a whitelist is selected, the device connecting the router can access the domain name of the whitelist only.

3.8.1 Domain Blacklist

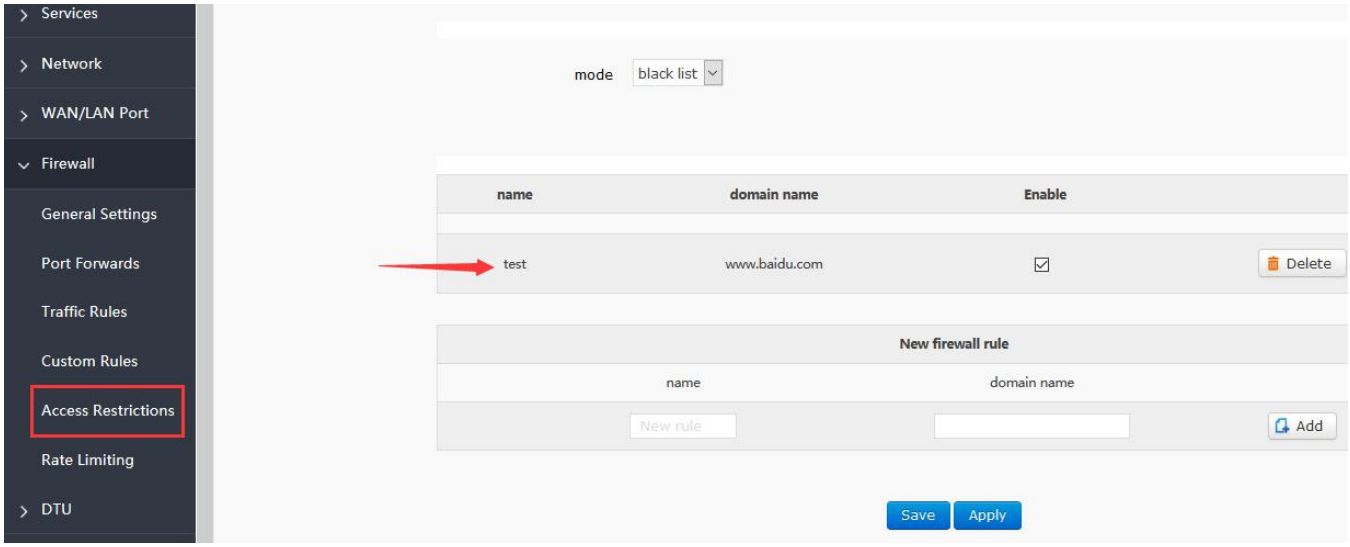

Figure49 blacklist

3.8.2 Whitelist

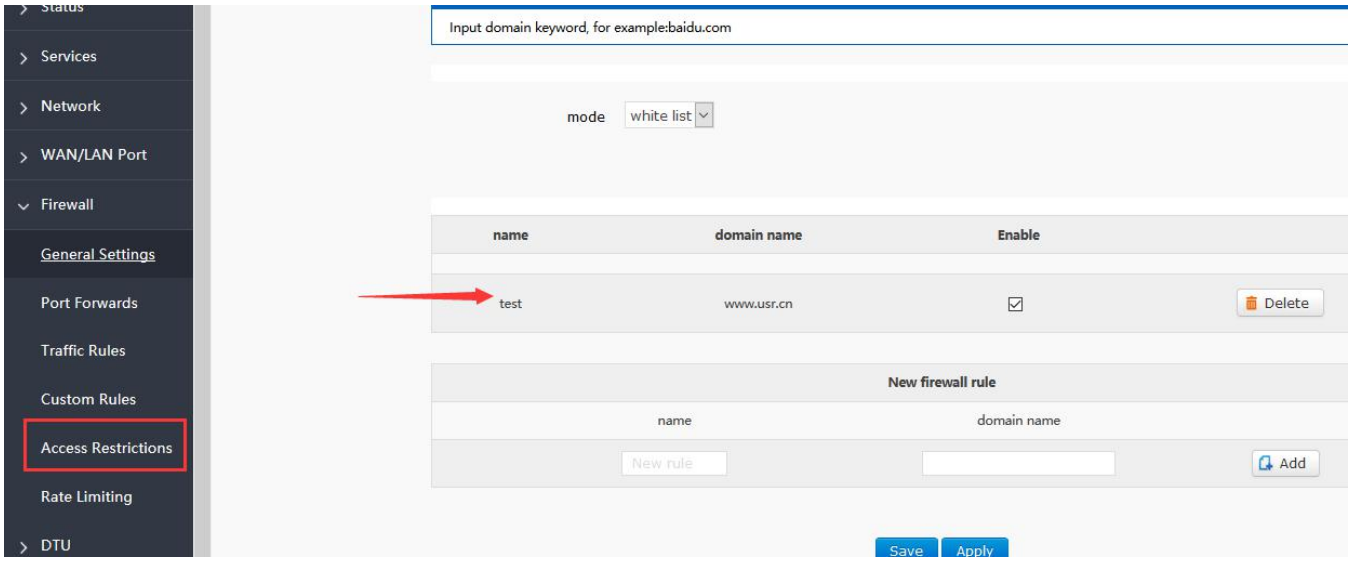

Figure50 whitelist

3.9. Rate Limiting

Network speed control can limit the speed of devices connecting to routers, support IP segment address speed limit and MAC address speed limit, and rules can be added at the same time.

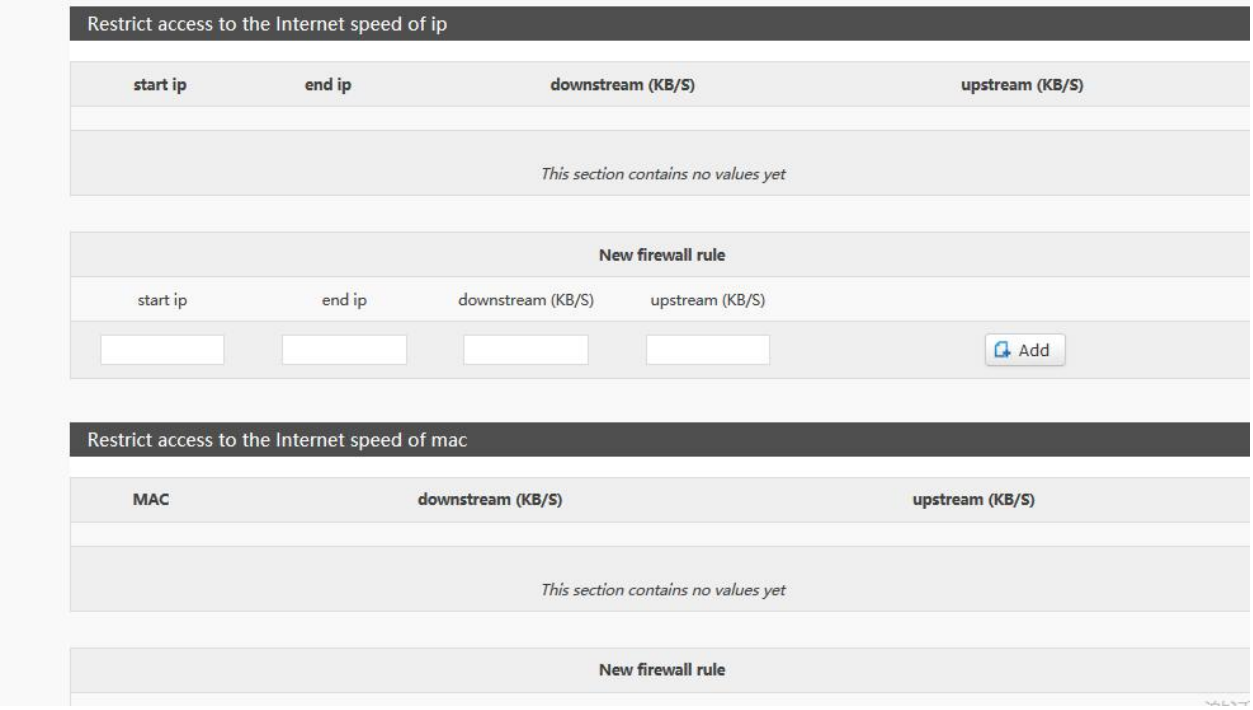

Figure51 rate limiting

4. AT Commands

No.	Command	Function
		Version
1	AT+VER	Query version information
2	AT+MAC	Query the MAC
3	AT+ICCID	Query ICCID code
4	AT+IMEI	Query IMEI code
		4G
5	AT+SYSINFO	Query the net info of device
6	AT+APN	APN address
7	AT+CSQ	Signal quality
8	AT+TRAFFIC	Query traffic information
		System
9	AT+UPTIME	Query running time
10	AT+WANN	Query the IP of device
11	AT+LANN	Query/set the LAN of IP
12	AT+WEBU	Query/set the webpage account and password
13	AT+PLANG	Query/set the default language
14	AT+RELD	Recover to factory setting
15	AT+Z	Restart
16	AT+DHCPEN	Open/close DHCP Server
		System shell command
20	AT+LINUXCMP	Execute system shell command

4.1. AT+VER

Function: query the firmware version

Query: AT+VER<CR>

<CR><LF>+VER:<ver><CR><LF>

e.g.

send: AT+VER

return:+VER:V1.0.9

4.2. AT+MAC

Function: query MAC

Query: AT+MAC<CR>

<CR><LF>+MAC=<mac><CR><LF>

e.g.

send: AT+MAC

return:+MAC:D8B04CD01234

4.3. AT+ICCID

Function: query the ICCID code

Query:

AT+ICCID{CR}

{CR}{LF}+ICCID:code{CR}{LF}{CR}{LF}

e.g.

send: AT+ICCID

return:+ICCID:898600161515AA709917

4.4. AT+IMEI

Function: query the IMEI code

Query :

AT+IMEI{CR} or AT+IMEI?{CR}

{CR}{LF}+IMEI:code{CR}{LF}{CR}{LF}OK{CR}{LF}

e.g.

send: AT+IMEI

return:+IMEI:868323023238378

4.5. AT+SYSINFO

Function: query the net info

Query

AT+SYSINFO{CR}

{CR}{LF}+ SYSINFO:operator,mode {CR}{LF}{CR}{LF}

e.g.,

send: AT+SYSINFO

return:+SYSINFO: CHINA-MOBILE,4G mode

4.6. AT+APN

Function: query/set APN code

Query

AT+APN{CR}

{CR}{LF}+APN:code,user_name,password{CR}{LF}{CR}{LF}OK{CR}{LF}

Set

AT+APN=code,user_name,password{CR}

{CR}{LF}OK{CR}{LF}

e.g.

send: AT+APN

return:+APN:3gnet

4.7. AT+CSQ

Function: query the signal intensity

AT+CSQ{CR}

{CR}{LF}+CSQ: rssi<CR><LF>

e.g.:

send: AT+CSQ

return:+CSQ:31

4.8. AT+TRAFFIC

Function: query traffic information

AT+TRAFFIC<CR>

<CR><LF>+TRAFFIC: < dev_down，dev_up，pro_time，at_time>，<CR><LF>

e.g.:

send: AT+TRAFFIC

return:+TRAFFIC: 111000000B, 2000000B,1486379553,1486380161

4.9. AT+UPTIME

Function: query the running time

AT+ UPTIME<CR>

<CR><LF>+UPTIME:<seconds,time><CR><LF>

e.g.:

send: AT+UPTIME

return:+UPTIME: 2096,34

4.10. AT+WANN

Function: query IP of the WAN（DHCP/STATIC）

AT+WANN<CR>

<CR><LF>+WANN=<mode,address,mask,gateway><CR><LF>

e.g.:

send: AT+WWAN

return:+WANN:DHCP,10.1.179.202,255.255.255.252,10.1.179.201

4.11. AT+LANN

Function: query/set up LAN gateway, mask.

AT+LANN<CR>

<CR><LF>+LANN:ip,netmask<CR><LF>

e.g.:

send: AT+LANN

return:+LANN:192.168.1.1,255.255.255.0

set:

AT+LANN=ip,netmask<CR>

<CR><LF>+LANN:OK<CR><LF>

e.g.:

send: AT+LANN=192.168.2.1,255.255.255.0

return:+LANN:OK

4.12. AT+WEBU

Function: query/set webpage username and password

Query:

AT+RELD<CR>

<CR><LF>+ WEBU:username,passwd<CR><LF>

e.g.: send: AT+ WEBU

return:+ WEBU:OK

Set:

AT+ WEBU =username,passwd<CR>

<CR><LF>+ WEBU:ok<CR><LF>

4.13. AT+PLANG

Function: set the default language

AT+ PLANG = LANGUAGE <CR>

<CR><LF>+ PLANG:ENGLISH<CR><LF>

e.g.:

send: AT+ PLANG =EN

return:+ PLANG: ok

4.14. AT+RELD

Function: recover the default setting

AT+RELD<CR>

<CR><LF>+ RELD: ok<CR><LF>

e.g.:

send: AT+ RELD

return:+ RELD:OK

4.15. AT+Z

Function: restart

AT+Z<CR>

<CR><LF>+REBOOT:OK<CR><LF>

e.g.:

send: AT+Z=0

return:+ Z:OK

4.16. AT+DHCPEN

Function: enable/unable DHCP server

AT+DHCPEN=SWITCH<CR>

<CR><LF>+ DHCPEN:ok<CR><LF>

e.g.:

send: AT+ DHCPEN=ON

return:+ DHCPEN:ON

4.17. AT+ LINUXCMP

CMP : linux command

Function: execute the Linux command and return the execution information.

AT+ LINUXCMP=cmp<CR>

<CR><LF>+ LINUXCMP: result<CR><LF>

e.g.:

send: AT+ LINUXCMP=pwd

return:+ LINUXCMP: /bin

5. Contact us

Company: Jinan USR IOT Technology Limited

Address: Floor 11, Building 1, No. 1166 Xinluo Street, Gaoxin District, Jinan, Shandong, 250101, China

Web: www.usriot.com

Support: h.usriot.com

Email: sales@usr.cn

Tel: 86-531-88826739

6. Disclaimer

This document provides the information of USR-G806 products, it hasn't been granted any intellectual property license by forbidding speak or other ways either explicitly or implicitly. Except the duty declared in sales terms and conditions, we don't take any other responsibilities. We don't warrant the products sales and use explicitly or implicitly, including particular purpose merchant-ability and marketability, the tort liability of any other patent right, copyright, intellectual property right. We may modify specification and description at any time without prior notice.

7. Updated History

2017-08-02 V1.0.4.1 established based on Chinese version V1.0.4.
2017-11-09 V1.0.4.2 updated. Modified some words to standards and corrected spelling/grammatical mistakes. Optimized whole manual arrangement. Changed related pictures to new G806 pictures.
2018-01-05 V1.0.4.3 updated. Changed related pictures to normal G806 version pictures. Optimized whole manual arrangement. Divided G806 user manual into normal version and G806-A version.
2019-2-17 V1.0.5 supplement the missing instructions.