GW-R4513 User Manual

File Version: V1.0.1

Contents

GW-R4513 User Manual 1
1. Get Start 4
1.1. Hardware Test 4
1.2. Net Connection 4
1.3. Router Initial Value 4
2. Product Overview 5
2.1. Product Introduction 5
2.2. Function 5
2.3. Basic Function 6
2.4. Product Dimensions 8
3. Produce Function 10
3.1. Configuration Process 11
3.2. Interconnection of GW-R4513 12
3.2.1. WAN+4G 12
3.2.2. Double LAN+4G 13
3.3. Basic Function 14
3.3.1. Network Diagnostic Function 14
3.3.2. Host Name and Time Zone 15
3.3.3. Password Setting 16
3.3.4. Reset to Default 16
3.3.5. Indicator Light 17
3.3.6. Firmware Upgrade 18
3.3.7. Reboot 19
3.4. Advanced Function 19
3.4.1. Supported Services 19
3.4.2. WiFiDog 20
3.4.3. LAN Interface 23
3.4.4. DHCP Function 25
3.4.5. WAN Interface 26
3.4.6. Wi-Fi Wireless Interface 26
3.4.7. 4G Interface 29
3.4.8. APN Setting 31
3.4.9. VPN Client(PPTP/LTTP/GRE/OPENVPN) 32
3.4.9.1. PPTP Client 32
3.4.9.2. L2TP Client 34
3.4.9.3. IPSEC 36
3.4.9.4. OPENVPN 37
3.4.9.5. GRE 41
3.4.9.6. SSTP Client 43
3.4.10. Static Router 44
3.4.11. NAT Function 44
3.4.11.1. MASQ 44

3.4.11.2. SNAT 44
3.4.11.3. DNAT 46
3.4.12. Access Restrictions 49
3.4.12.1. Domain Blacklist 49
3.4.12.2. Whitelist 49
3.4.13. Rate Limiting 50
4. DTU Function 51
4.1. Work Mode 52
4.1.1. Net Transparent Transmission Mode 53
4.1.1.1. Mode Declaration 53
4.1.2. HTTPD Mode 55
4.1.2.1. Mode Declaration 55
4.1.3. UDC Mode 57
4.1.3.1. Mode Declaration 57
4.2. Serial Port 59
4.2.1. Basic Parameters 59
4.2.2. Frame Forming Mechanism 59
4.2.2.1. Time Triggered Mode 59
4.2.2.2. Length Triggered Mode 60
4.3. Characteristic Functions 61
4.3.1. Registration Package 61
4.3.2. Heartbeat Package 63
4.3.3. USR-Cloud 64
5. Webpage Sitting 66
5.1. Web Function 67
6. AT Commands 69
7. Contact Us 72
8. Disclaimer 72
9. Update History 72

1. Get Start

GW-R4513 is a 4G wireless router with powerful DTU function, which provides users with an integrated solution of 4G router and DTU.

1.1. Hardware Test

Figure 1 hardware connection

1.2. Net Connection

- Insert SIM card
- Install WIFI antenna, M2M antenna
- Connect PC to the LAN port of GW-R4513
- Set PC to get dynamic IP
- Power on GW-R4513
- Wait for about a minute, and the 2/3G indicator lights up, indicating that the router's 4G network is successful and can be connected to the Internet.

1.3. Router Initial Value

Table 1 router initial value

Parameter	Initial value
Account	root
Password	root
IP address	192.168.1.1

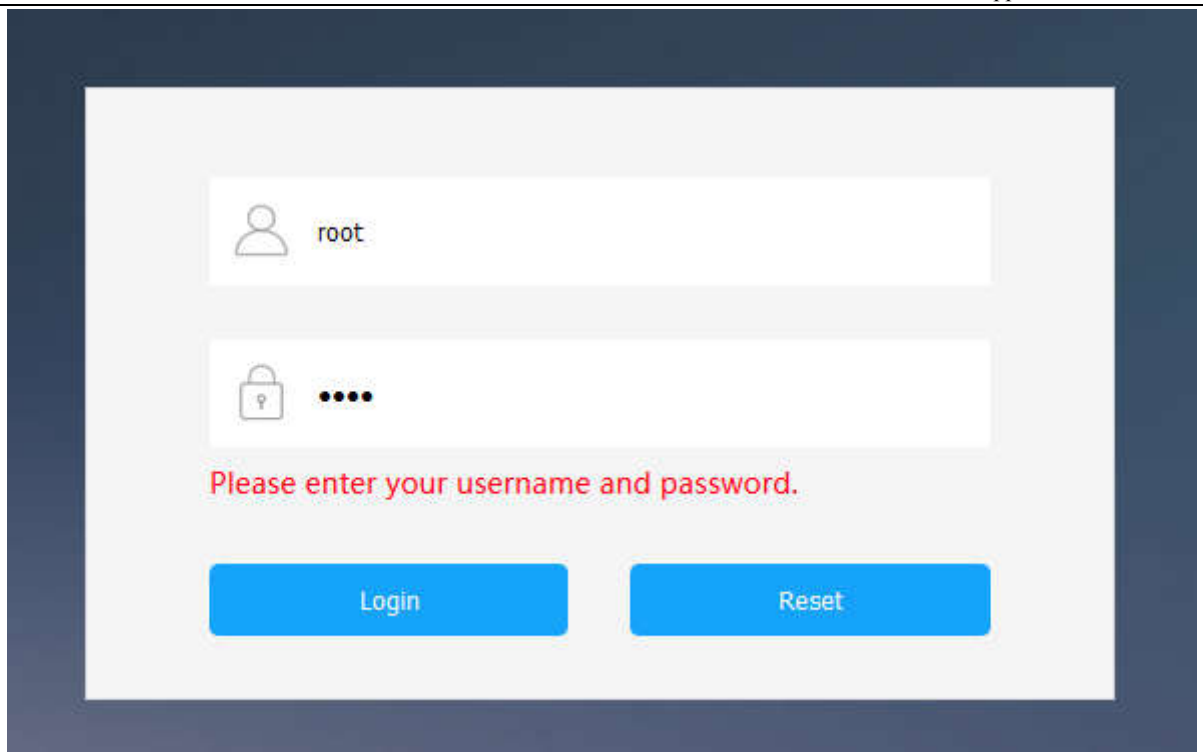


Figure 2 webpage

2. Product Overview

2.1. Product Introduction

GW-R4513 is a 4G wireless router with powerful DTU functions, providing users with an industrial 4G router and DTU integration solution.

It adopts the high-performance embedded structure of the industry, and provides reliable data transmission network for the data transmission fields of smart home, smart grid, personal medical, industrial control and so on.

Support wired WAN ports, LAN ports, wireless WLAN network, 4G network interface, rich and diverse networking functions, easy for users to lay their own network.

2.2. Function

- Support 1 wired LAN ports, 1 wired WAN ports (WAN ports can be switched to LAN ports).
- Support 1 WIFI wireless LAN
- Support multiple LED communication indicators
- Support SSH, TELNET, Web multi platform management configuration mode.
- Support one button to restore factory settings.
- 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 automatic checking network, 2/3/4G system switching, SIM information display, support

APN/VPDN 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), Static Routing, PPPOE, DHCP, Static IP Function
- Support mandatory portal (WIFIDOG), this function needs to be customized accodeing to customer needs.
- Support the firewall, NAT, DMZ host, access control black-and-white list, IP speed limit, NTP, MAC speed limit.
- Support SMS AT command
- Support 4 network connections online, support TCP Server, TCP Client, UDP Server and UDP Client
- Every connection supports 20KB serial data cache. When connection is abnormal, cached data can ‘t be lost.
- Support for sending registration package / heartbeat data.
- Support network transmission mode, HTTPD mode, UDC mode and USR-Cloud.
- Support basic instruction set
- Support external hardware watchdog design to ensure system stability.

2.3. Basic Function

Table 2 parameter

Wireless parameters（-AU module）		
Standard	TD-LTE	
	FDD-LTE	
	WCDMA	
	TD-SCDMA	
	GSM/GPRS/EDGE	
Frequency band standard	TD-LTE	Band 40
	FDD-LTE	Band 1/2/3/4/5/7/8/28
	WCDMA	Band 1/2/5/8
	GPRS	Band 2/3/5/8
Emissive power	TD-LTE	+23dBm(Power class 3)
	FDD-LTE	+23dBm(Power class 3)
	WCDMA	+23dBm(Power class 3)
	TD-SCDMA	+24dBm(Power class 2)
	GSM Band8	+33dBm(Power class 4)
	GSM Band3	+30dBm(Power class 1)
Technical specifications	TD-LTE	3GPP R9 CAT4 down 150 Mbps Up 50 Mbps
	FDD-LTE	3GPP R9 CAT4down150 Mbps Up 50 Mbps
	WCDMA	HSPA+ down 21 Mbps Up 5.76 Mbps
	TD-SCDMA	3GPP R9 down 2.8 Mbps

		Up 2.2 Mbps
	GSM/GPRS/EDGE	MAX: down 384 kbps up 128 kbps
Wireless parameters（-E module）		
Standard	TD-LTE	
	FDD-LTE	
	WCDMA	
	TD-SCDMA	
	EVDO/CDMA1X	
	GSM/EDGE	
Frequency band standard	TD-LTE	Band 38/40/41
	FDD-LTE	Band 1/3/5/7/8/20
	WCDMA	Band 1/5/8
	GPRS	Band 3/8
Emissive power	TD-LTE	+23dBm(Power class 3)
	FDD-LTE	+23dBm(Power class 3)
	WCDMA	+23dBm(Power class 3)
	TD-SCDMA	+24dBm(Power class 2)
	CDMA2000	+23dBm(Power class 3)
	GSM Band8	+33dBm(Power class 4)
	GSM Band3	+30dBm(Power class 1)
Technical specifications	TD-LTE	3GPP R9 CAT4 down 150 Mbp up 50 Mbps
	FDD-LTE	3GPP R9 CAT4 down 150 Mbp up 50 Mbps
	WCDMA	HSPA+ down 21 Mbps up 5.76 Mbps
	TD-SCDMA	3GPP R9 down 2.8 Mbps up 2.2 Mbps
	CDMA2000	down 3.1 Mbps up 1.8 Mbps
	GSM/EDGE	MAX: down 384 kbps up 128 kbps
Function		
DDNS	Support	
APN	Support	
VPN	Support	
Port mapping	Support	
Firewall	Support	
Intelligent backup	Support	
DTU	Support	
Net /WIFI		
LAN	1	

WAN	1
Net rate	10/100M
RS485	Support
Electromagnetic isolation protection	1.5KV
Automatic switching between crossover and direct connection	1.5KV
TBD	1
Power	
VCC	DC 9~36v
Working current	Average 270mA/max 400mA/12V
Power interface	DC
Power protection	Anti reverse connection
Interface	
Antenna	WIFI /4G antenna
Status lamp	signal intensity/4G/WIFI/LAN/WAN/power
Software	
V-COM	Windows(32/64 bit)
Setting method	Webpage, support SSH, telnet ,GW-R4513 setting software
Work environment	
Work temperature	-20~70 ℃
Storage temperature	-40~+125℃
Storage humidity	1%~95%RH（non condensation）
Size	
Size	112.0 * 84.0* 28.0 mm(L*W*H)

2.4. Product Dimensions

Unit: mm

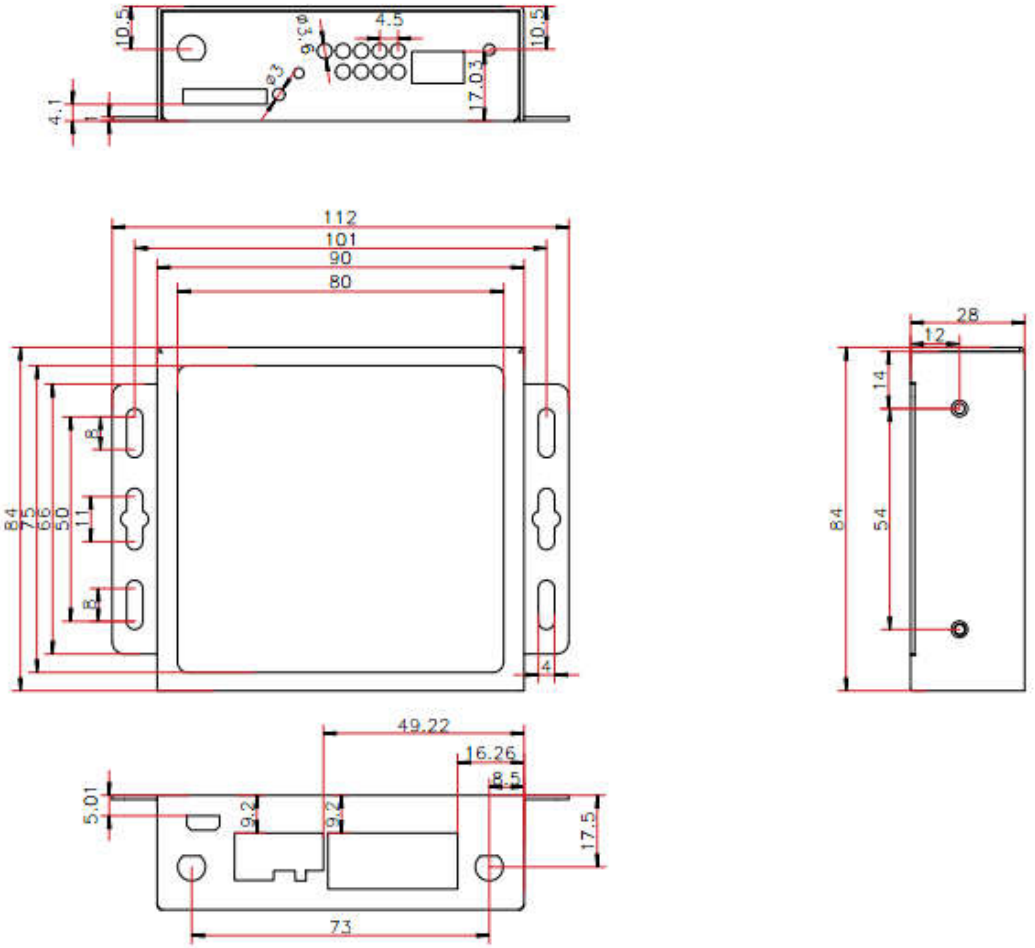


Figure 3 size

3. Produce Function

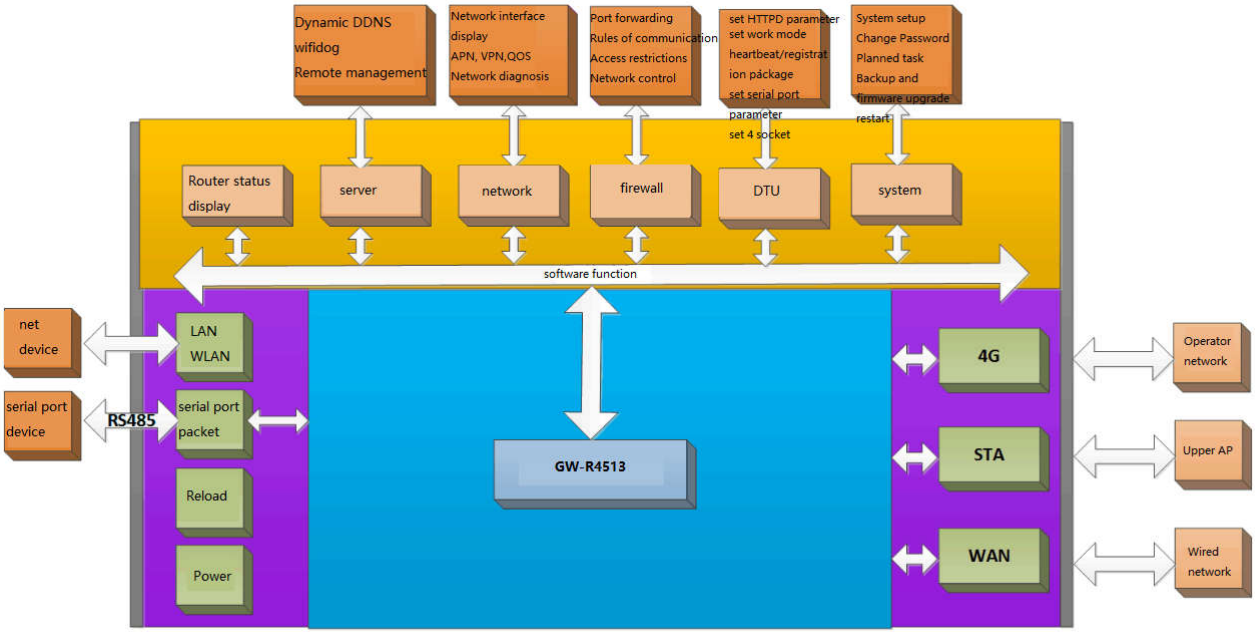


Figure 4 product function

3.1. Configuration Process

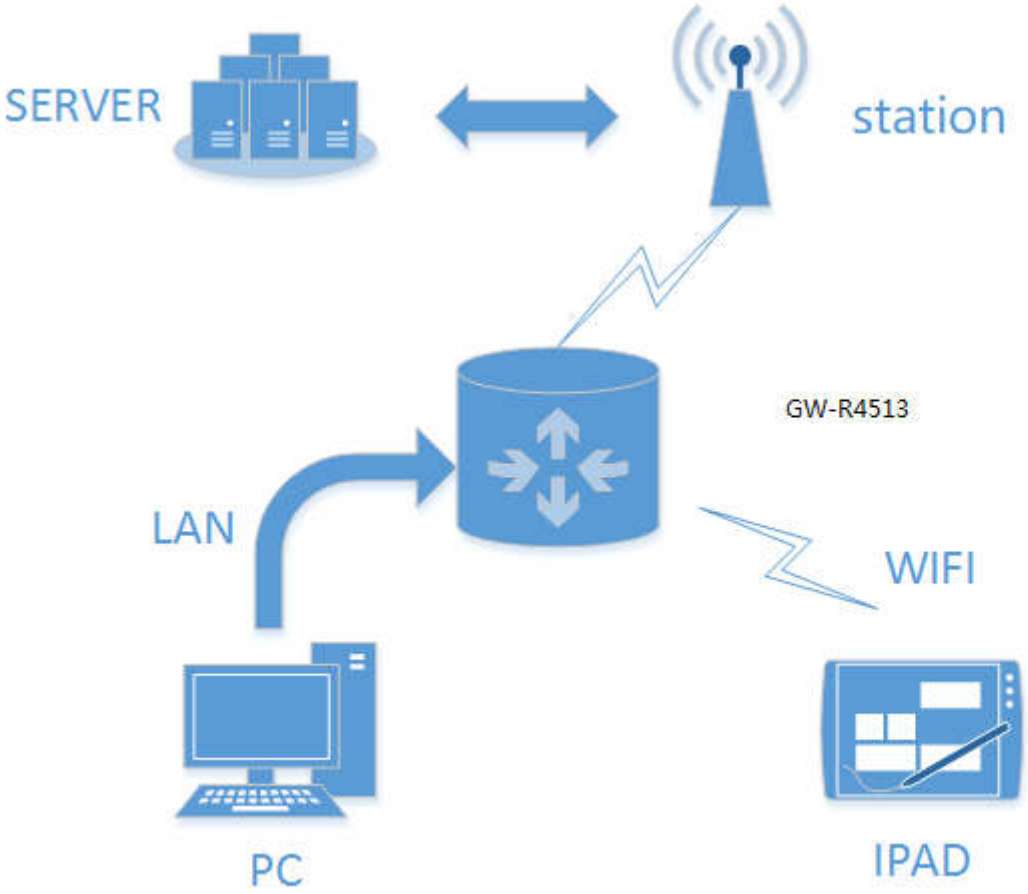


Figure 5 Schematic diagram of interconnection

3.2. Interconnection of GW-R4513

3.2.1.WAN+4G

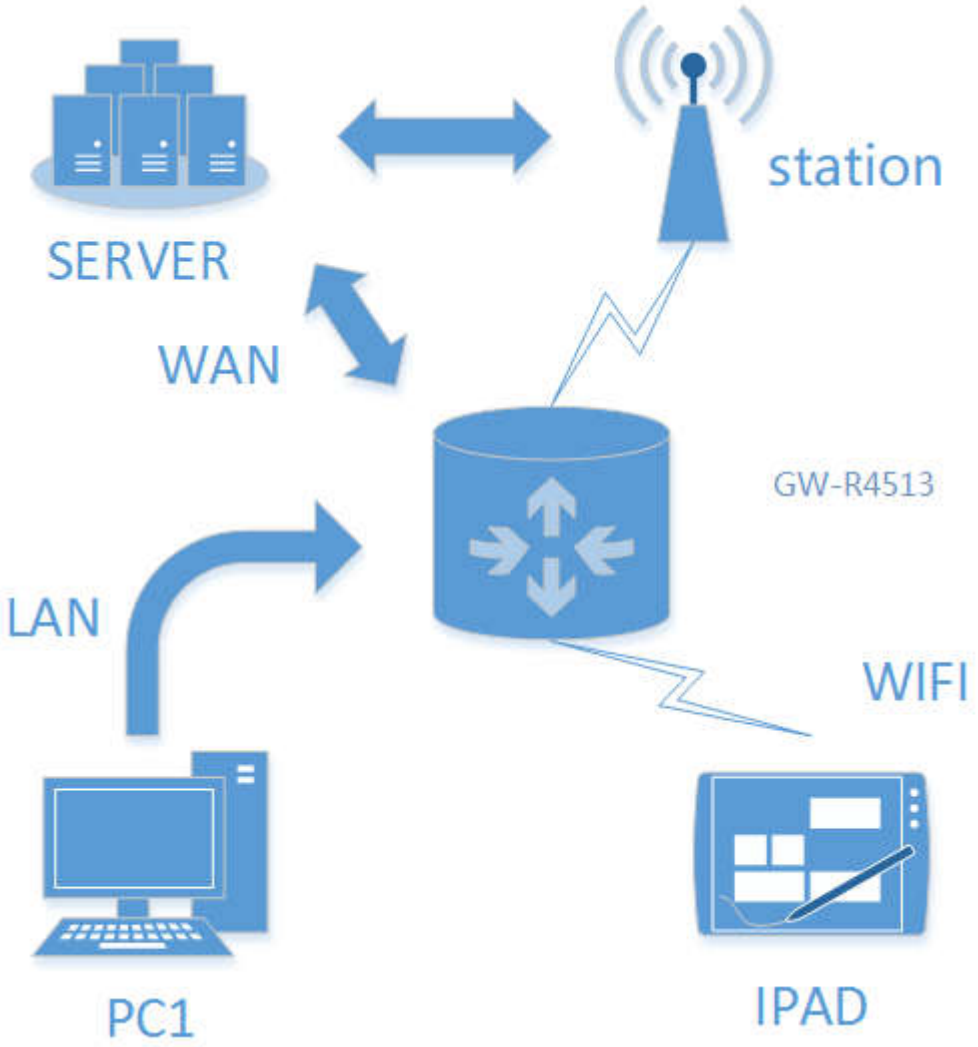


Figure 6 WAN+4G

This networking mode has two WAN ports (WAN ports of Ethernet port and 4G ports of M2M network) that can be connected to WAN simultaneously. The two channels form complementary and backup. At the same time, WAN ports of Ethernet port are preferred to ensure data fluency and save the traffic of 4G. When WAN ports are abnormal, they can't be connected to WAN. The router can also connect to the server through the 4G network port.

In this way, the router doesn't need any settings to connect to the network line, plug in 4G SIM card, and supply power to the router. The process of setting up customers is reduced to the greatest extent. Under this networking mode, the WIFI function of router can also work at the same time to maximize the number of LAN access.

This method is mainly used in the stably network, Such as factory buildings, intelligent buildings, smart cities and other related industries.

3.2.2. Double LAN+4G

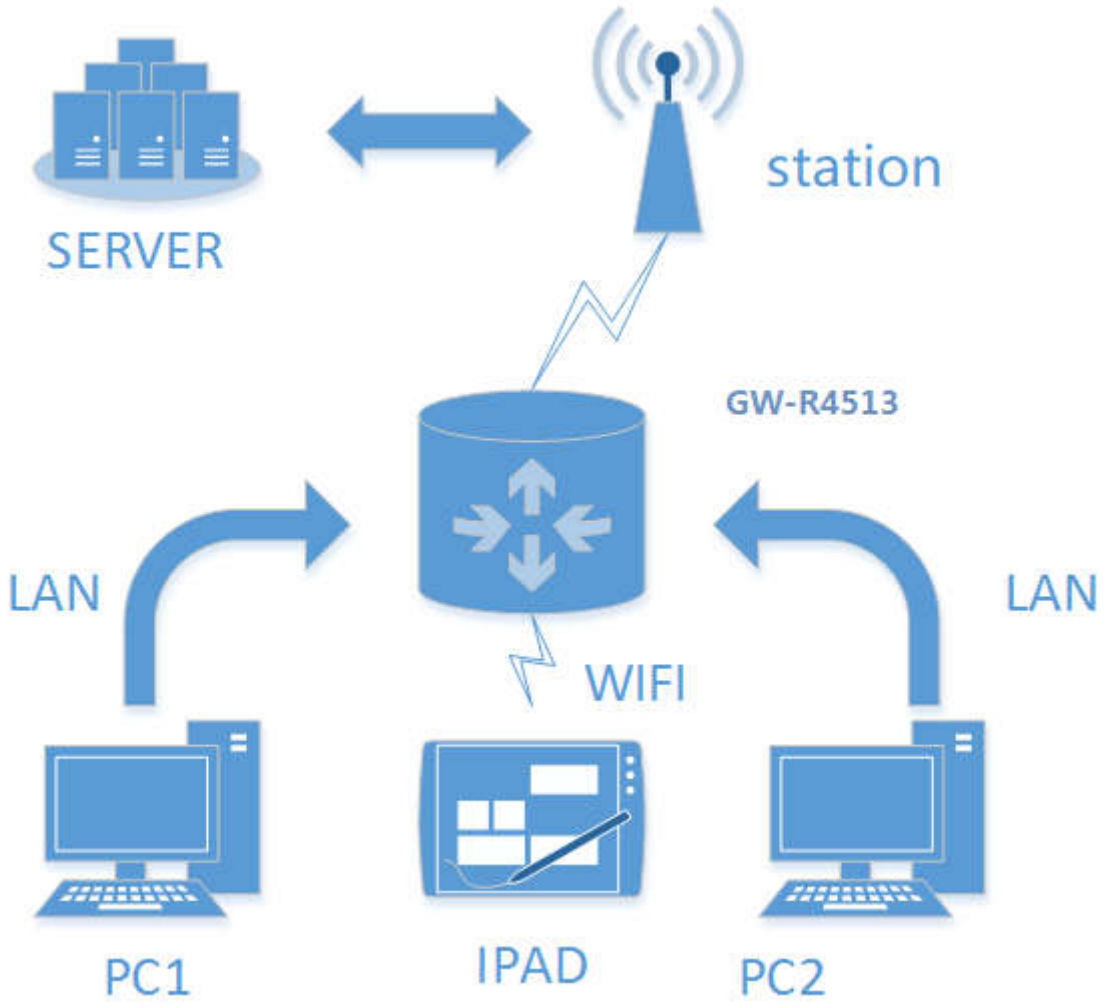


Figure 7 double LAN+4G

Set the two Ethernet port work as LAN port, the webpage is as follow,

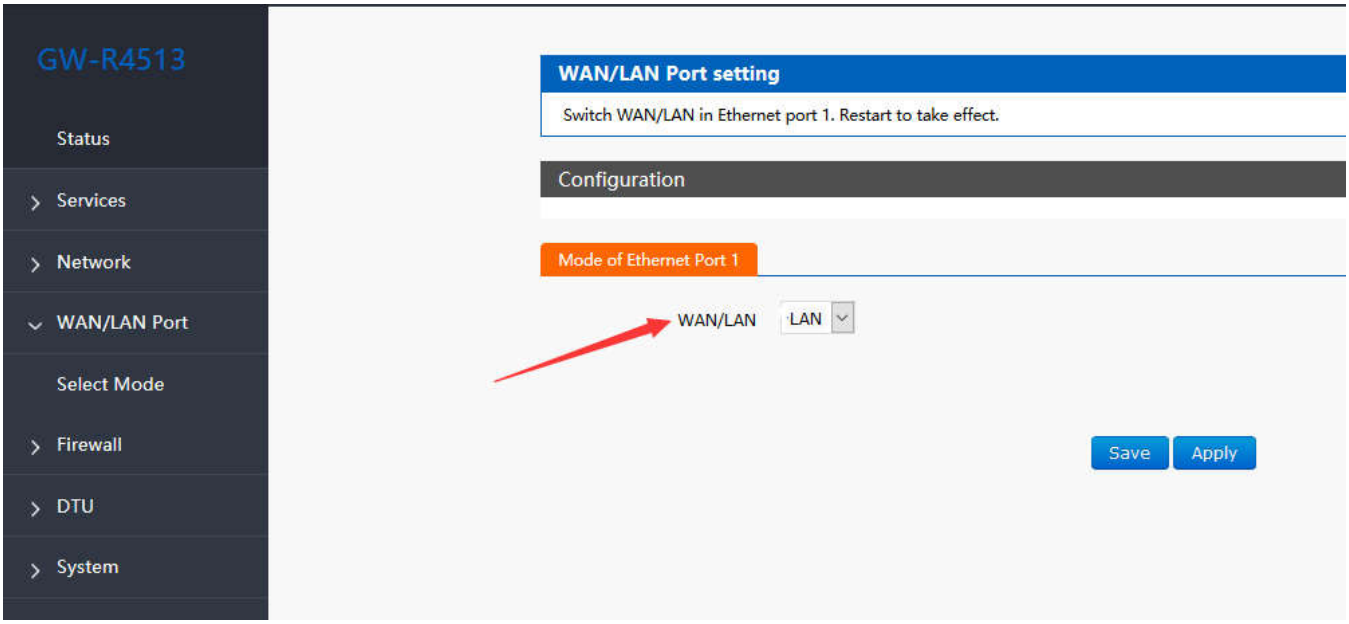


Figure 8 webpage setting

3.3. Basic Function

3.3.1. Network Diagnostic Function

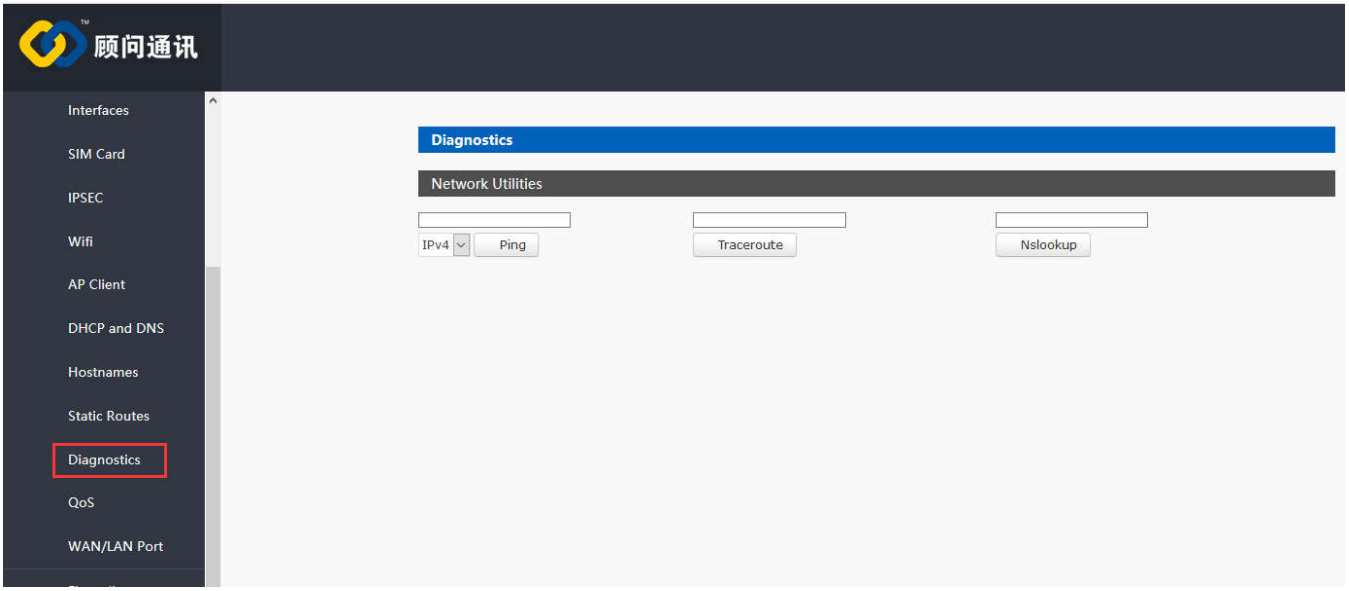


Figure9 the webpage of diagnostic

- Online diagnostic functions include Ping tools, routing parsing tools, and DNS View tools.
- 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.

3.3.2. Host Name and Time Zone

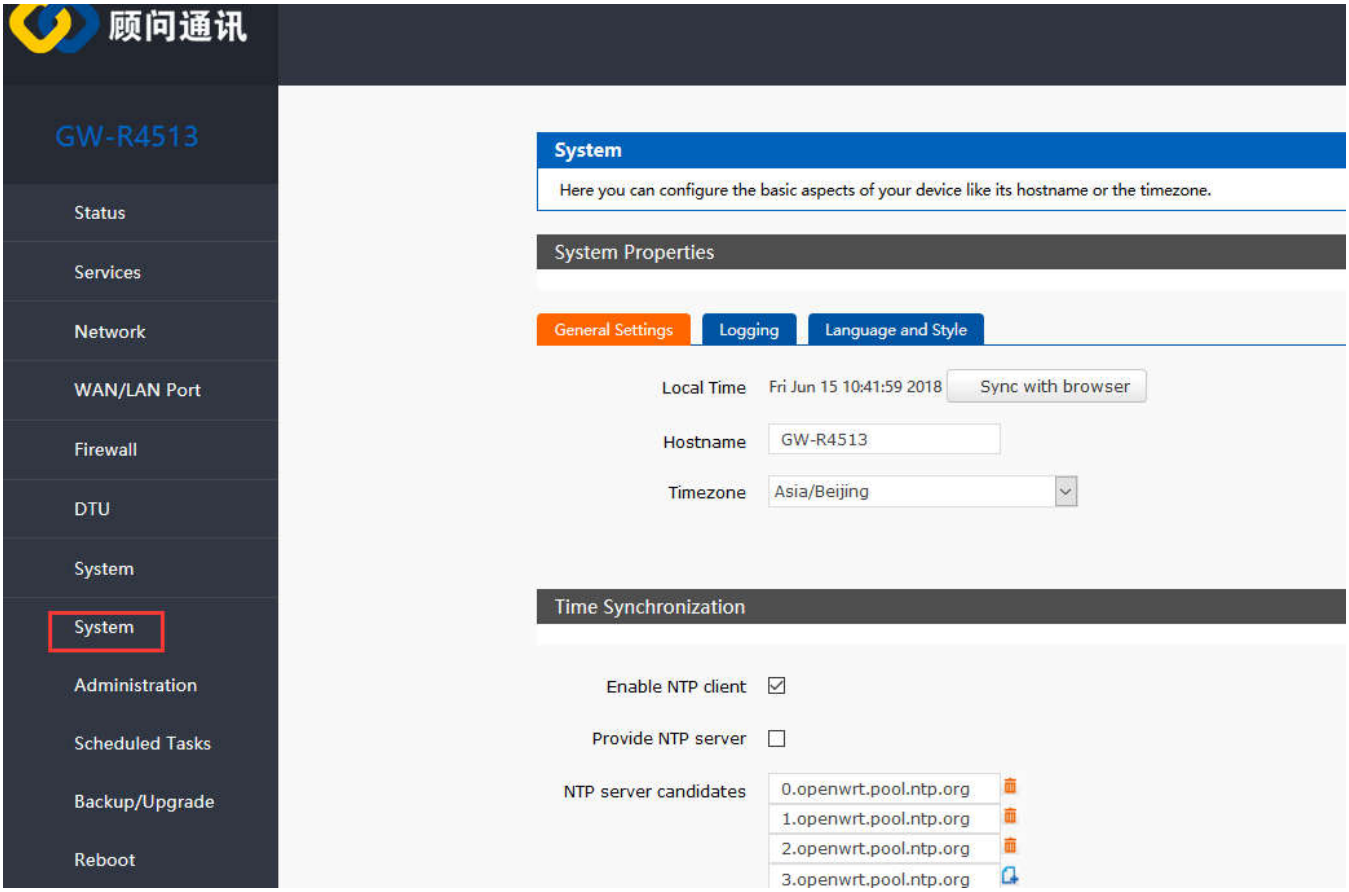


Figure10 hostname and time zone

3.3.3. Password Setting

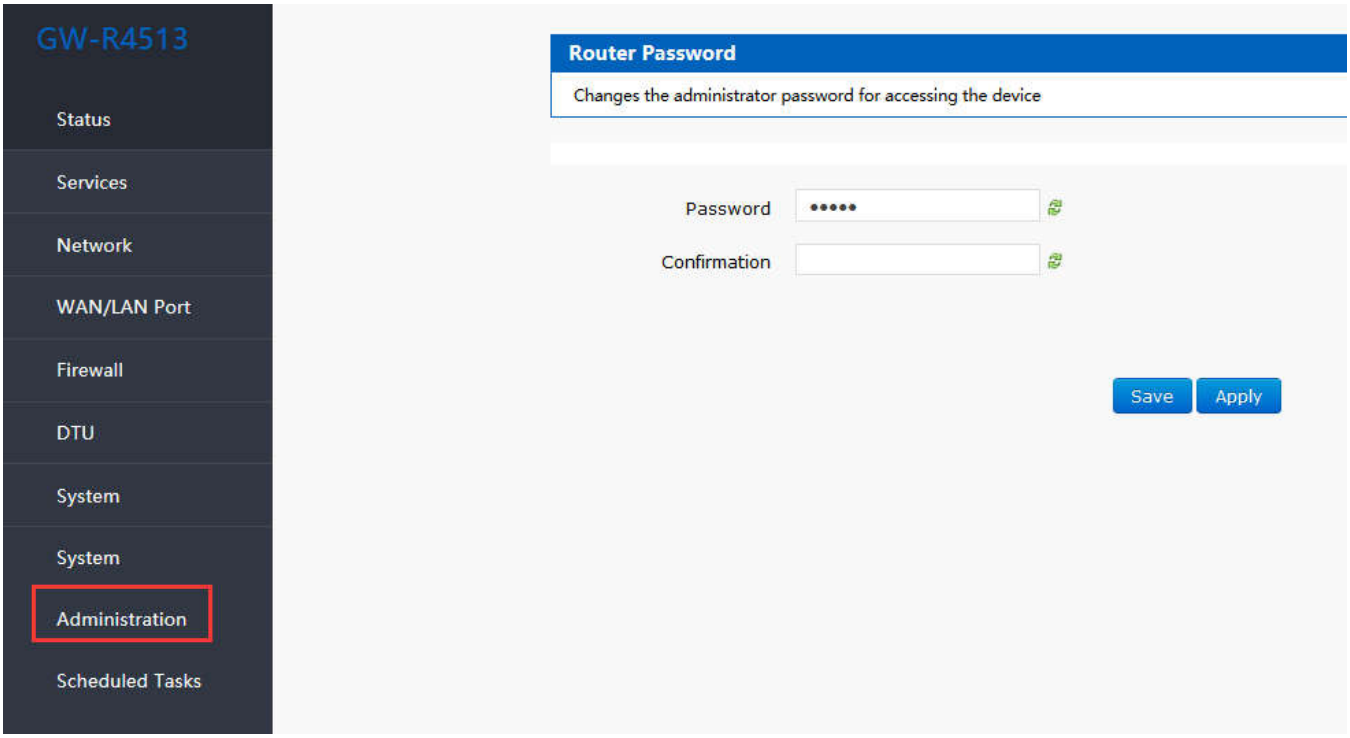


Figure11 the webpage of setting password

3.3.4. Reset to Default

You can restore factory parameter settings through web pages.

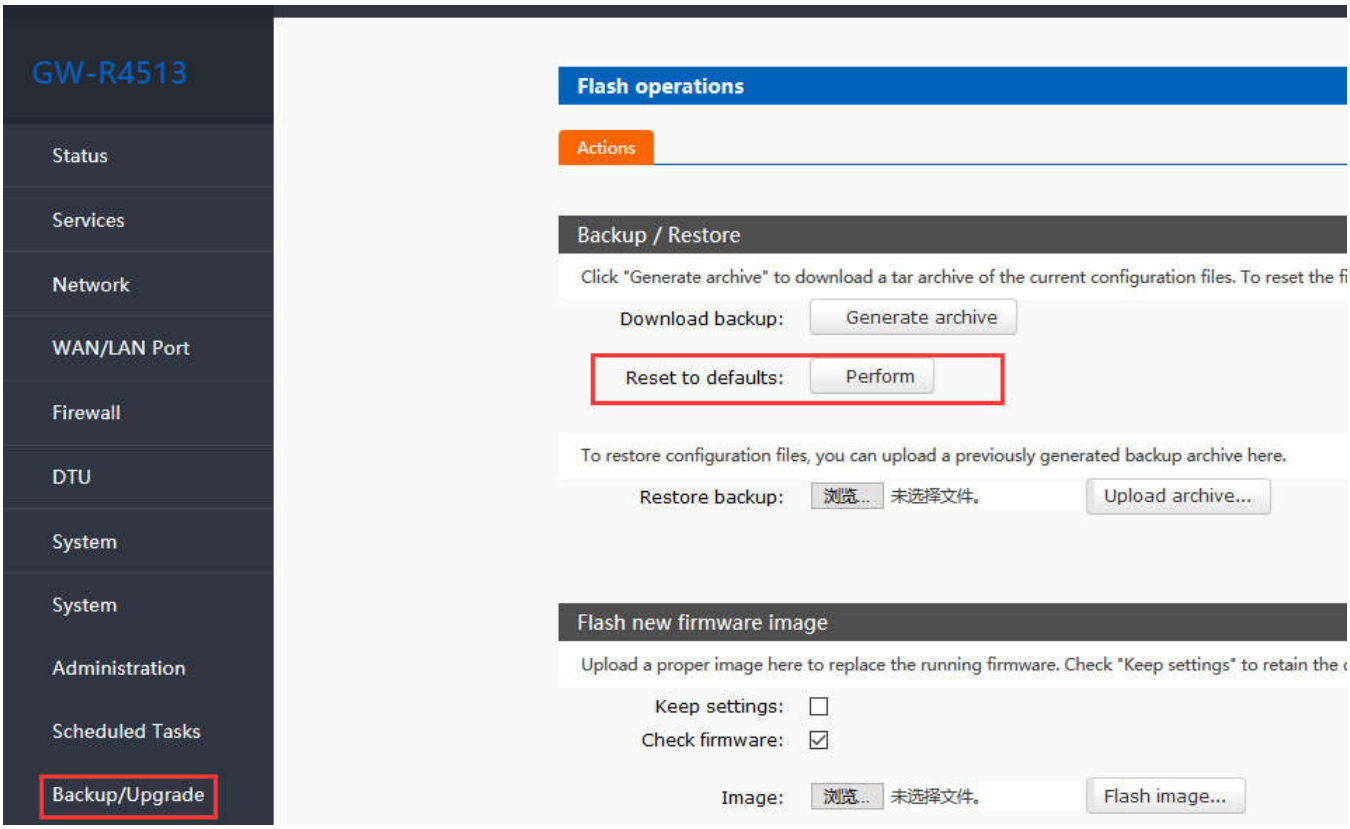


Figure12 the webpage of reset to default

Click the button to restore the factory settings. This function is consistent with the Reload button function of the hardware.

The use of Reload keys

- Long press 5S above and then release, the router will restore the factory parameter settings automatically and restart automatically.
- When the reboot takes effect, all the lights will be flashing 1 times and then destroyed.

3.3.5. Indicator Light

Table3 WIFI default parameter

Name	Intro
PWR	On when power on
WAN	On when use the WAN port, flicker when data transmission
LAN	On when use the LAN port, flicker when data transmission
WLAN	On when use WI-FI
2G indicator light	On when work on 2G
3G indicator light	On when work on 3G
Signal intensity（1-3）	The more, the stronger the signal is.

< Description >

- The 2/3/4G indicator lights up whether the GW-R4513 network is successful or not (the most important indicator).
- After WIFI starts successfully, the WLAN (or WIFI) indicator light on.
- The working conditions of WAN and LAN are indicated by WAN and LAN indicators.

- The corresponding WAN/LAN indicator flashes when the network line is connected and the network device working.
- The power lamp will always be bright.
- When the LTE module works at 4G, the 2G indicator and the 3G indicator light are all on.

3.3.6. Firmware Upgrade

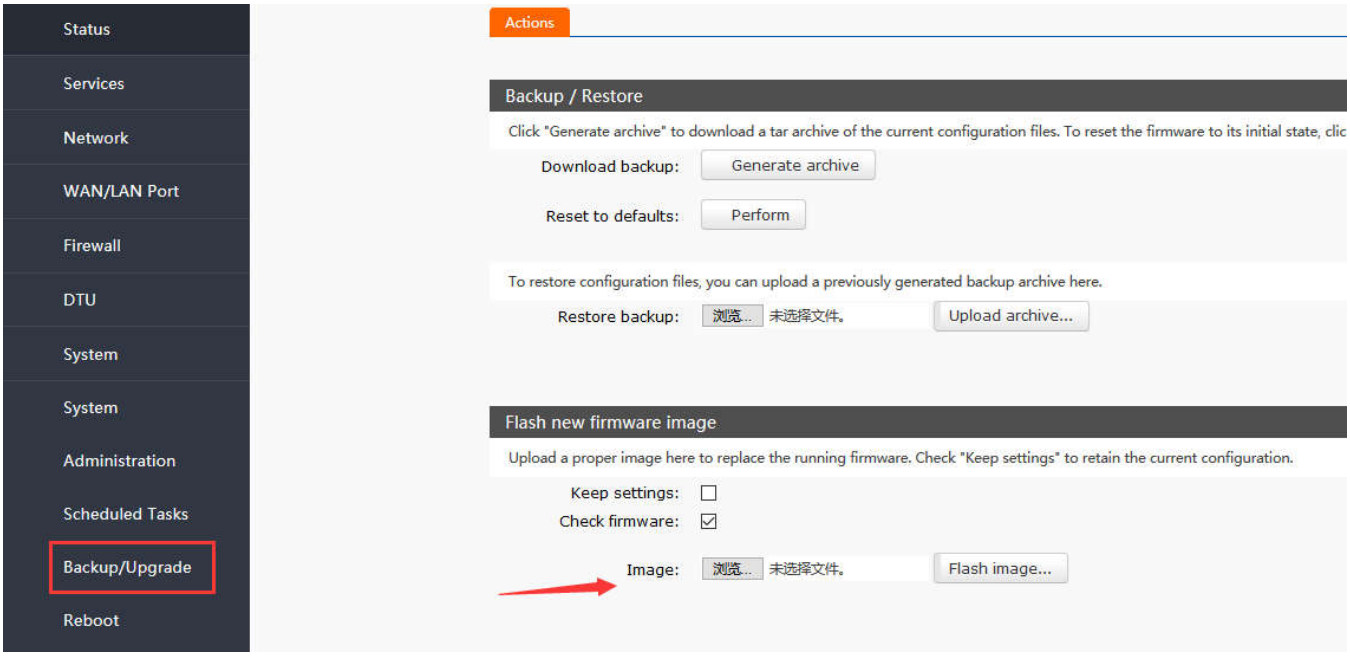


Figure13 the webpage of upgrade

< Description >

- The firmware upgrade process will last about 3-4 minutes. Please login again after 4 minutes.
- You can choose whether to save configuration.

During the process of firmware burning, please do not power down or unplug the wire.

3.3.7. Reboot

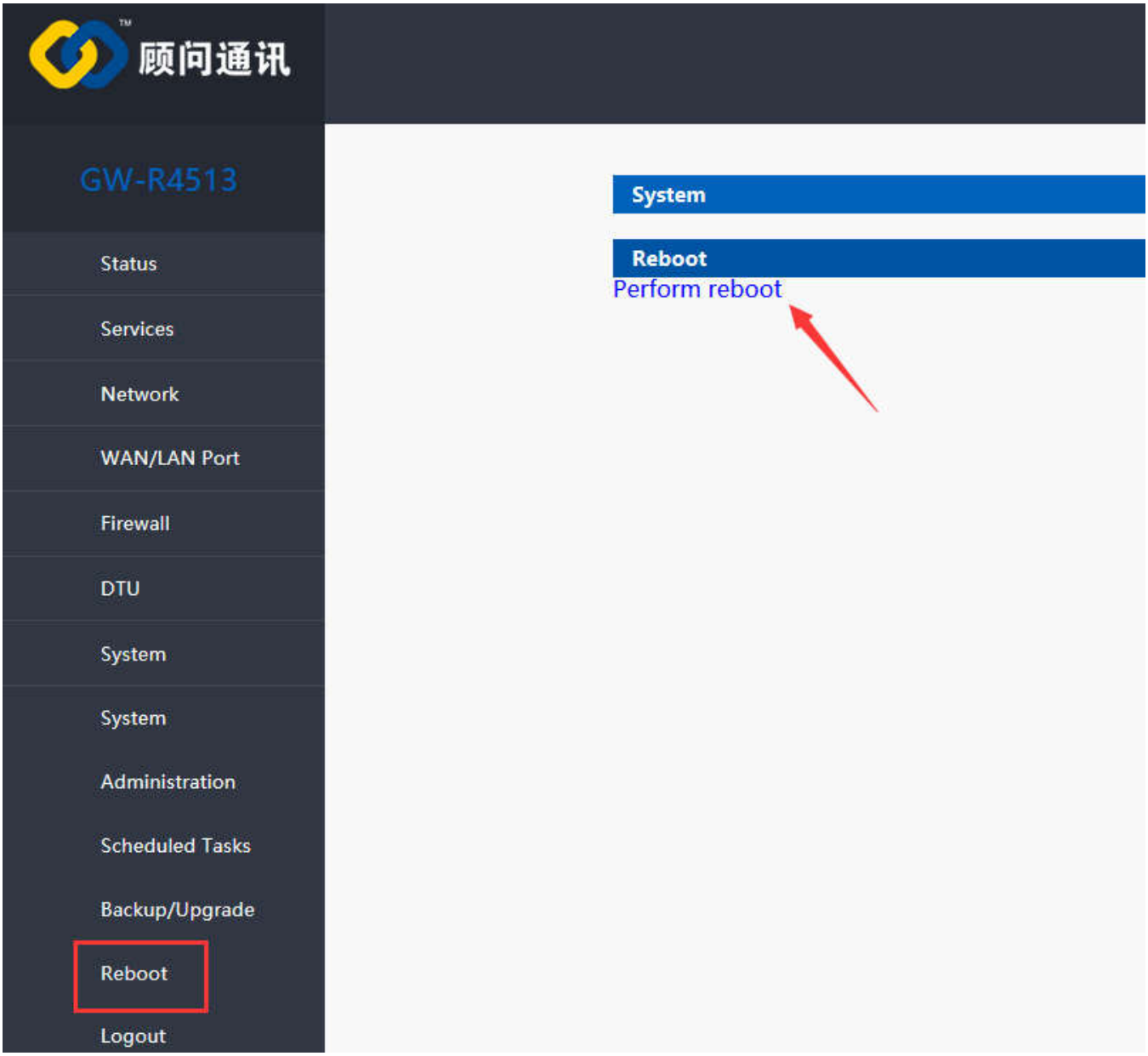


Figure14 the webpage of reboot

Click the button to restart the router.

The restart time is consistent with the router's power on startup time, which is about 40~60 seconds.

3.4. Advanced Function

3.4.1. Supported Services

The use of dynamic domain names can be divided into two situations. The first is that routers support DDNS.

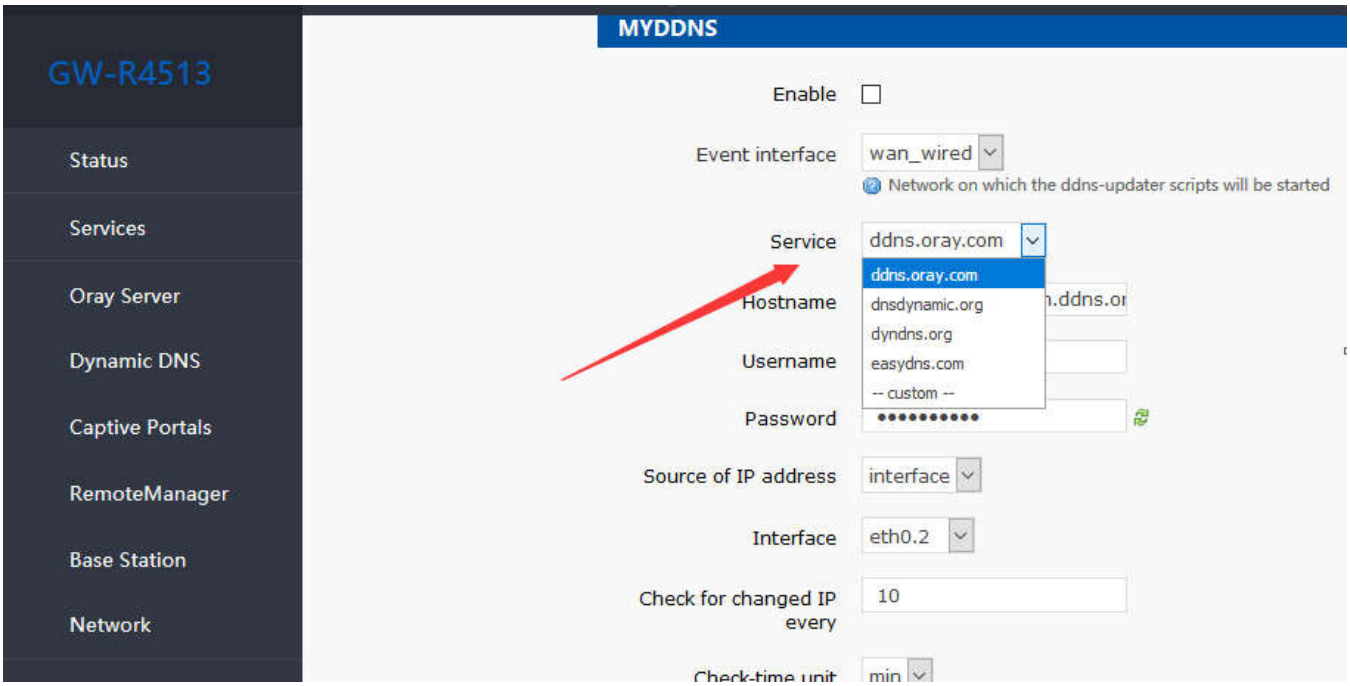


Figure15 the webpage of setting DDNS

Table4 DDNS custom server parameter

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

3.4.2. WiFiDog

Forced Portal (WiFiDog) allows devices accessing the router network to login to an authentication page for the first

time when browsing an extranet web page. Only when the authentication is successful can they access the extranet.

The significance of mandatory portal function lies in the security of LAN network, recodeing illegal acts such as network attacks using public networks, in addition, it can also be used for advertising purposes, it collects customer information with the tacit consent of current broadband users, so as to facilitate manufacturers to promote marketing.

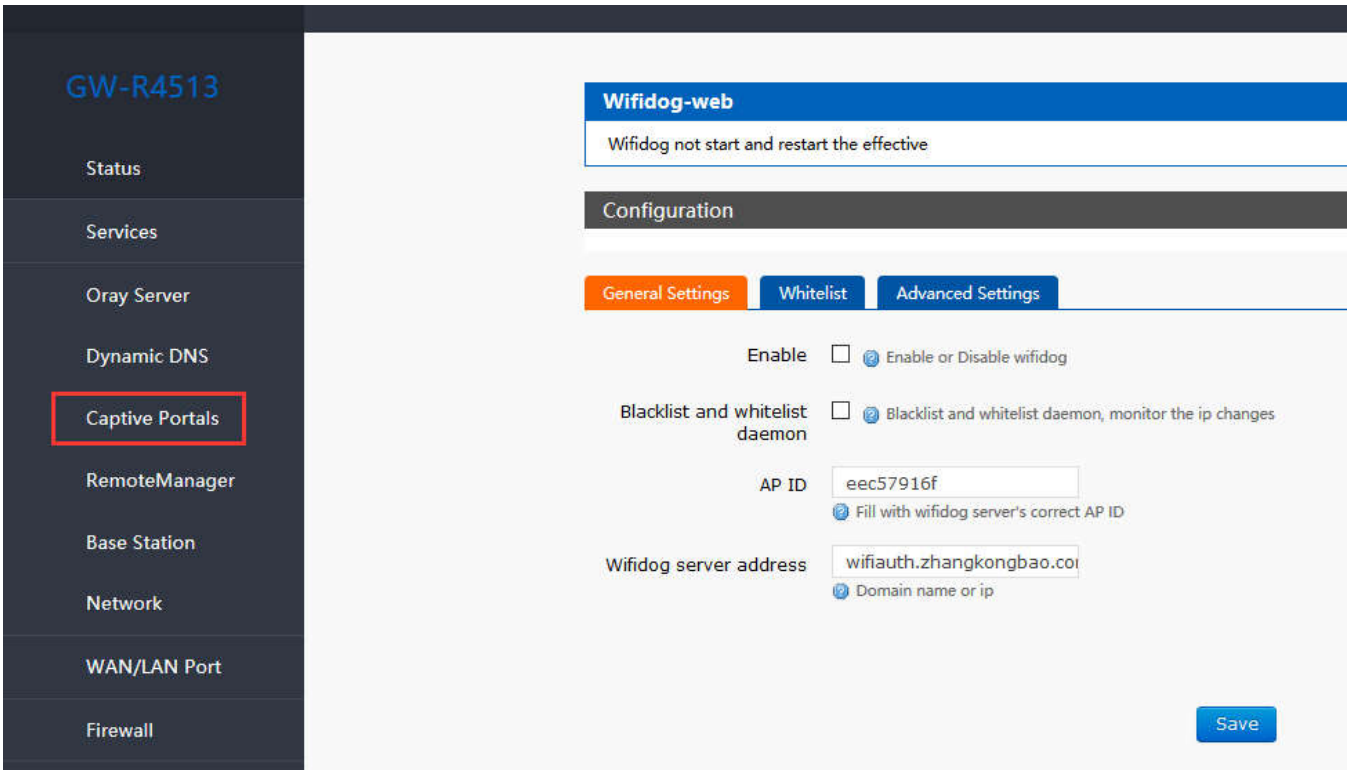
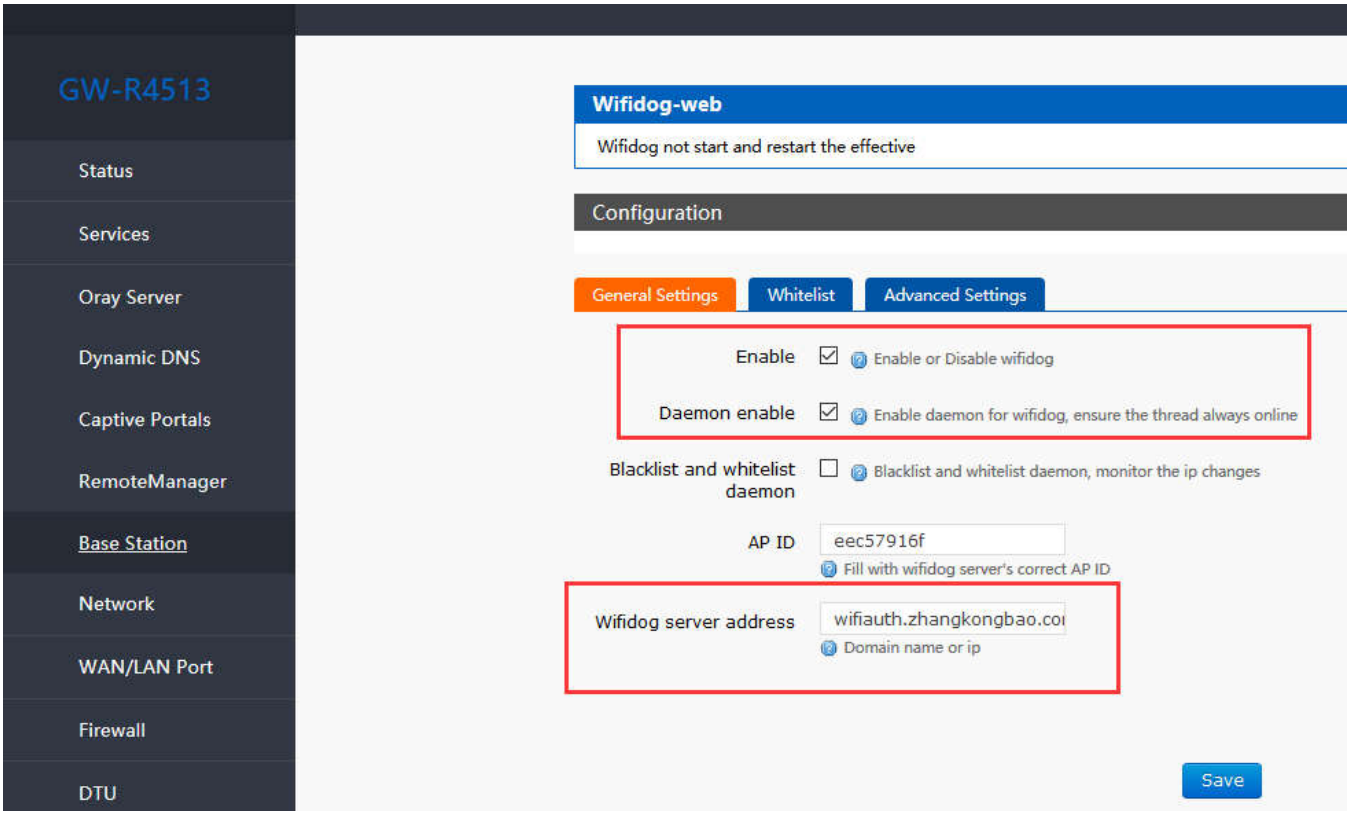


Figure16 the webpage1 of wifidog

Enable WI-FI dog


GW-R4513
Status
Services
Oray Server
Dynamic DNS
Captive Portals
RemoteManager
Base Station
Network
WAN/LAN Port
Firewall
DTU
Wifidog-web
Wifidog not start and restart the effective
Configuration
General Settings
Whitelist
Advanced Settings
Enable
Enable or Disable wifidog
Daemon enable
Enable daemon for wifidog, ensure the thread always online
Blacklist and whitelist daemon
Blacklist and whitelist daemon, monitor the ip changes
AP ID
eec57916f
Fill with wifidog server's correct AP ID
Wifidog server address
wifiauth.zhangkongbao.co
Domain name or ip
Save

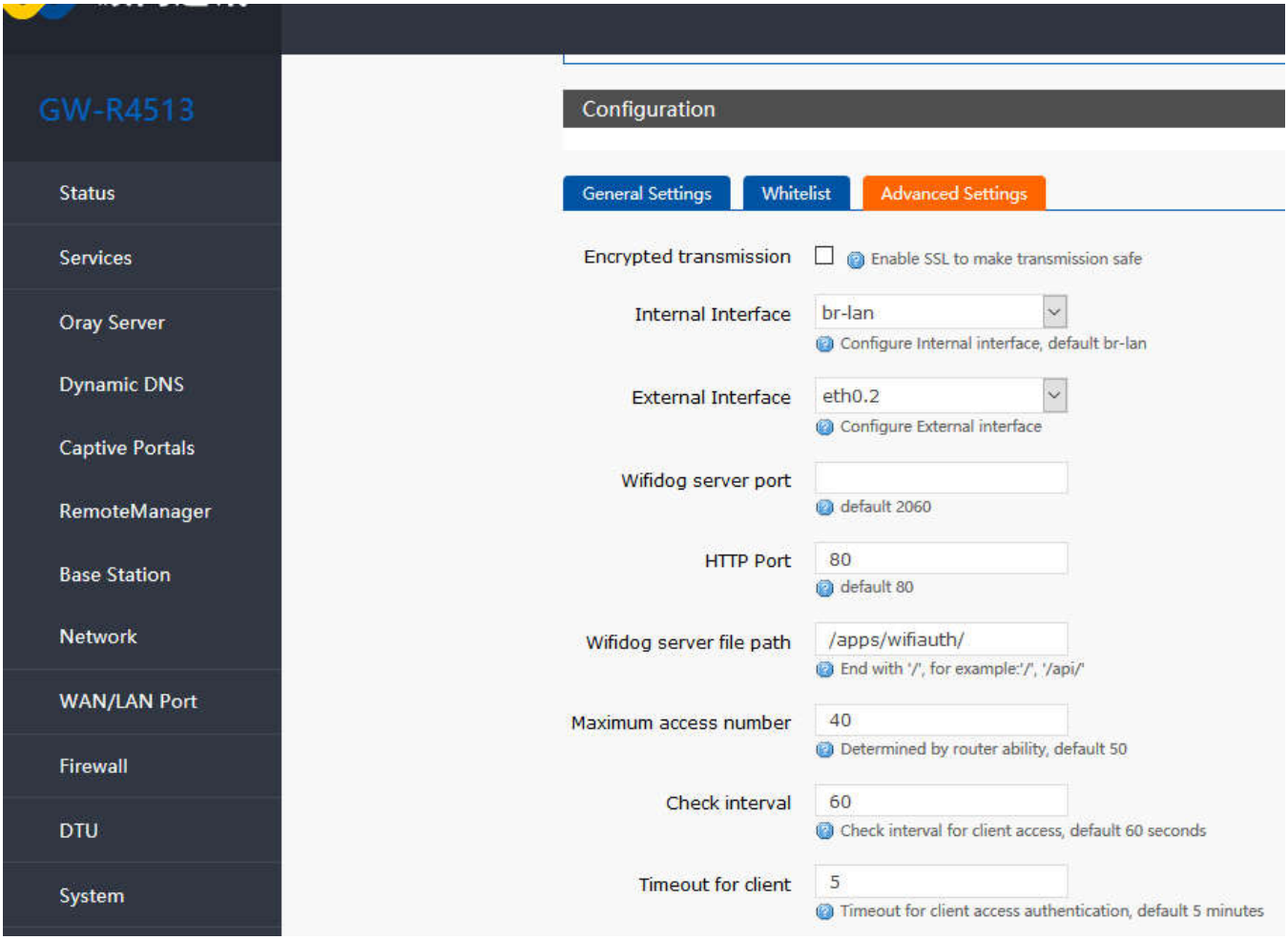


Figure17 the webpage2 of wifidog

Table5 WI-FI dog parameter

Function	Intro	Note
Enable WI-FI dog	Enable	If use
Daemon enable	Enable	If use
AP ID	nfuoId700	
Wifi dog server address	www.XXX.cn	
Internal interface	Br-lan	
External interface	Eth0.2	If use 4G, please fill in eth1
Wifi dog server file path	/apps/WIFIguanjia/	

3.4.3. LAN Interface

The LAN port is a local area network, there is 1 wired LAN port (WAN port can also be set to LAN port).

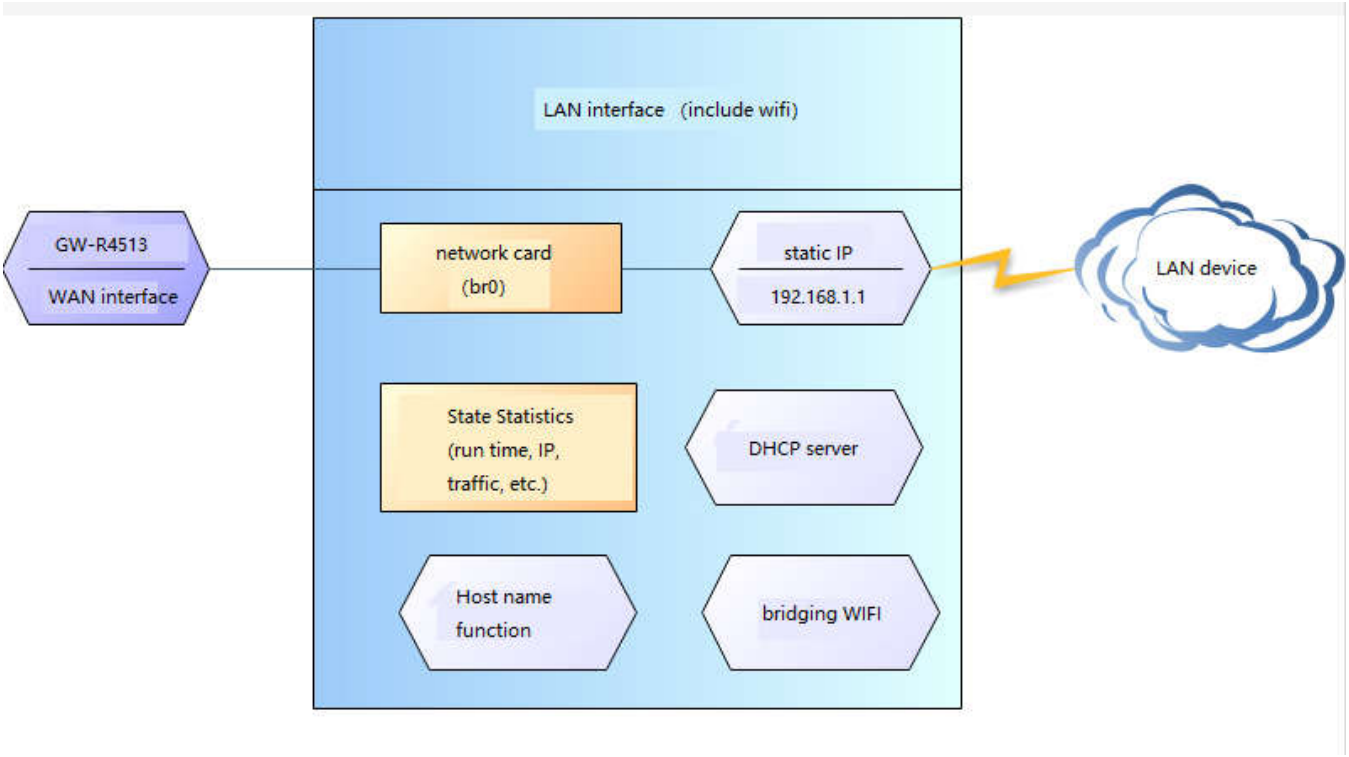


Figure18 LAN interface function

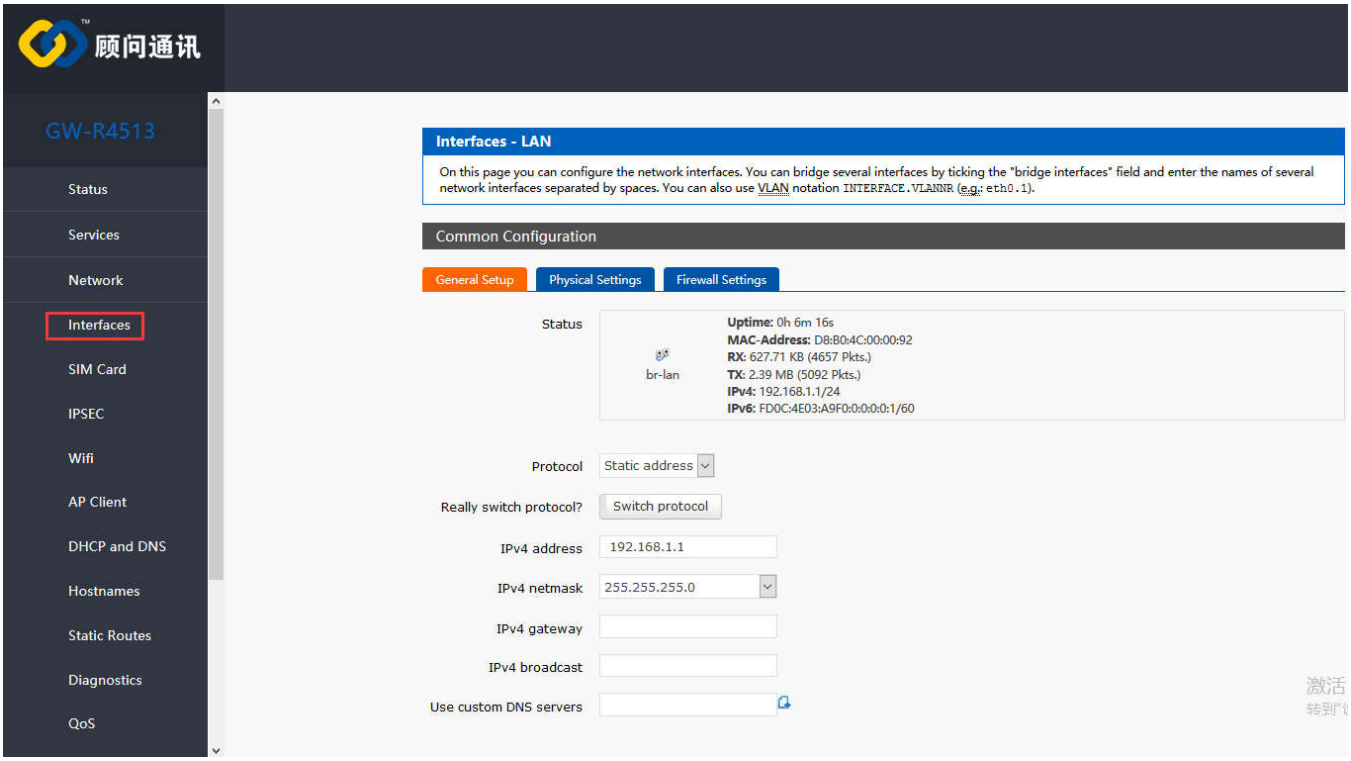


Figure 19 webpage of LAN interface setting

< Description >

- 1 LAN ports
- The default static IP address 192.168.1.1 and the subnet mask 255.255.255.0. This parameter can be modified,

such as static IP modification to 192.168.2.1.

- The WIFI interface (WLAN port) is bridged to the LAN port.
- By default, open the DHCP server function. All devices connected to the router's LAN port can automatically get the IP address.
- Simple state statistics function.

3.4.4. DHCP Function

The DHCP Server function of the LAN port is enabled by default (optionally turned off), and all network devices connected to the LAN port can automatically obtain IP addresses.

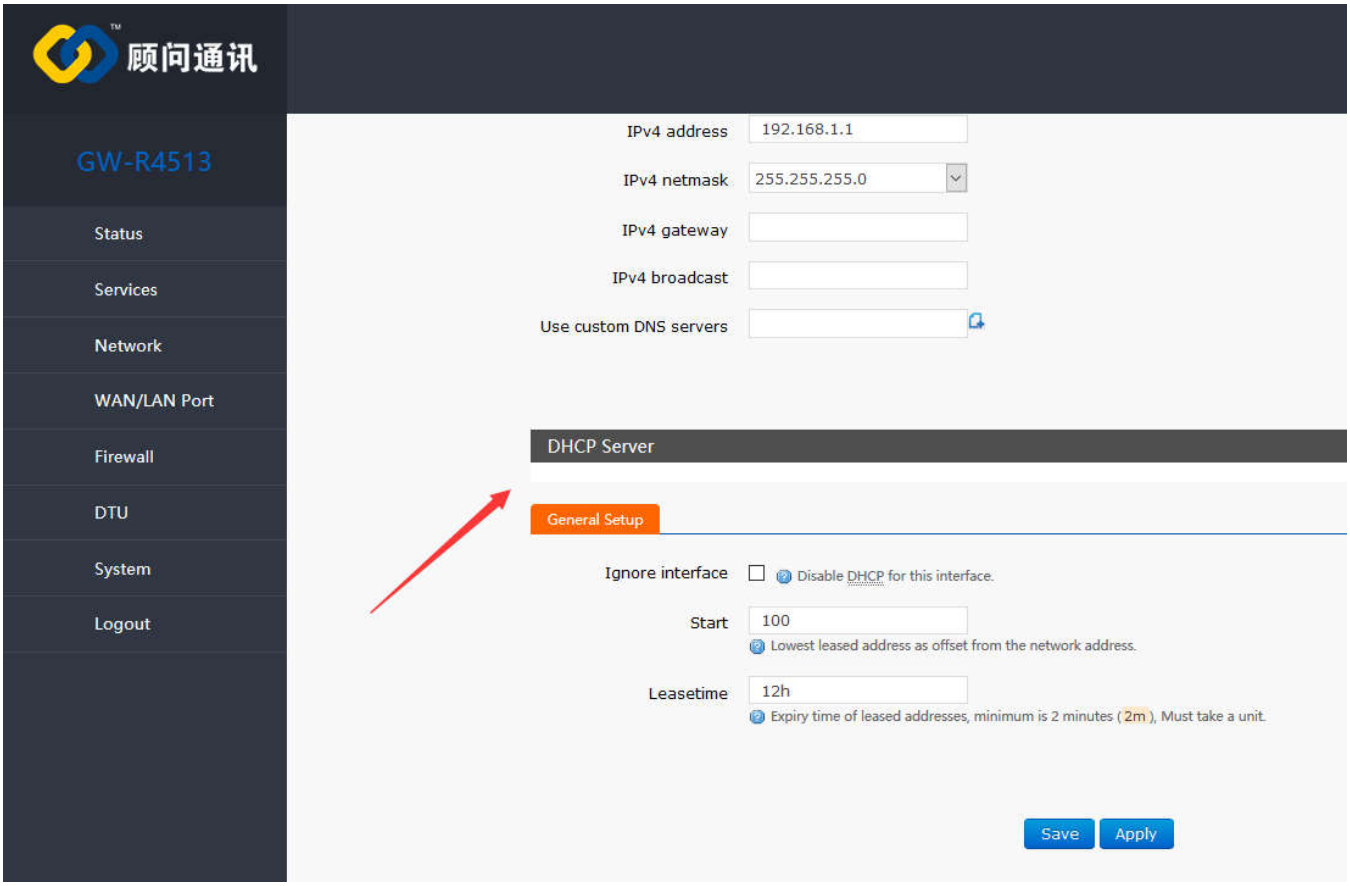


Figure20 webpage of DHCP setting

< Description >

- You can adjust the initial address of DHCP pool and address renting time.
- The default allocation range of DHCP starts from 192.168.1.100.
- Default rental time is 12 hours.

3.4.5. WAN Interface

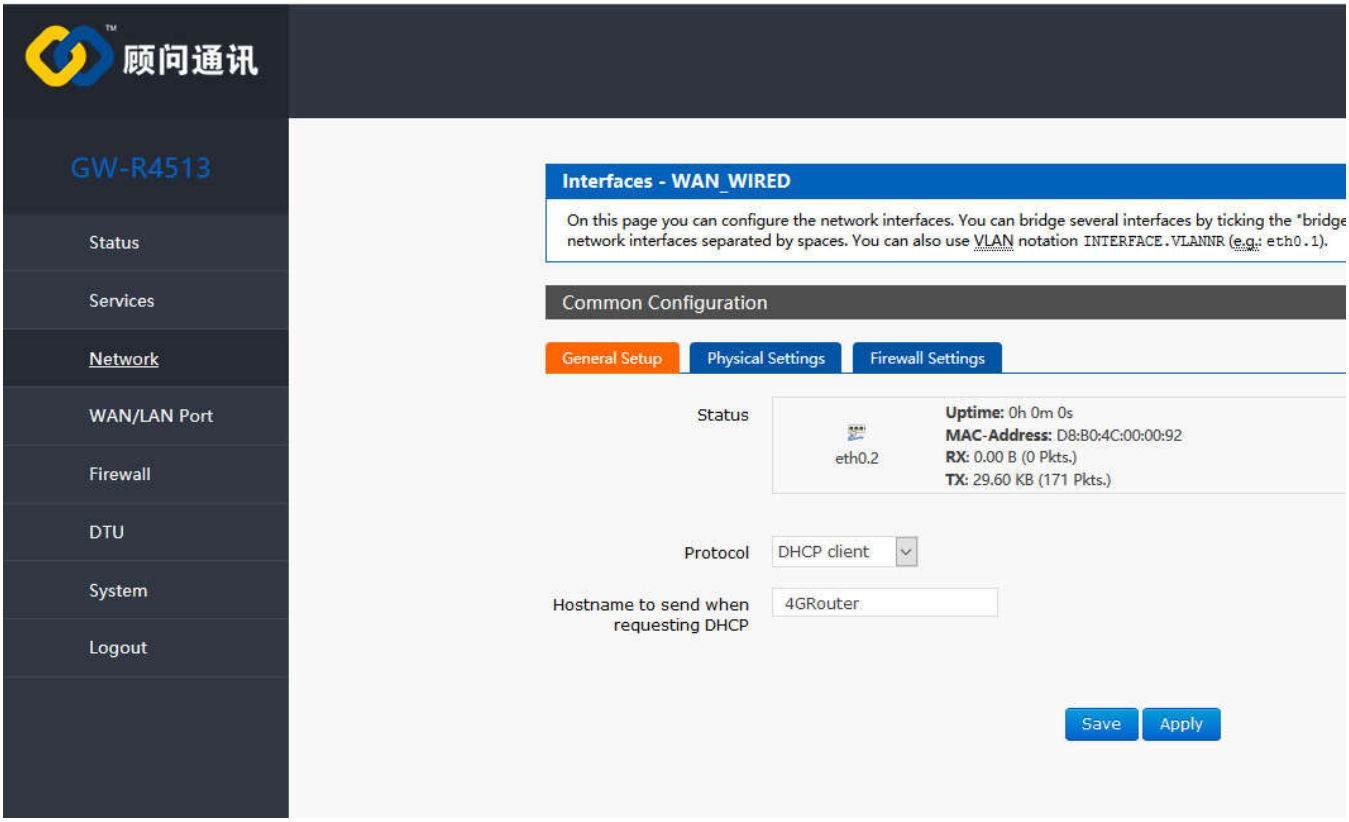


Figure21 webpage of WAN interface setting

WAN port is WAN interface.

< Description >

- 1 wired WAN ports
- Support DHCP client, static IP, PPPOE mode.
- Default DHCP client
- Note: The WAN interface can be set to LAN for the convenience of customers to communicate with multiple devices in the LAN. For specific settings, please refer to the Network Port Mode page.

3.4.6. Wi-Fi Wireless Interface

The functional diagram of WLAN is shown in the following figure:

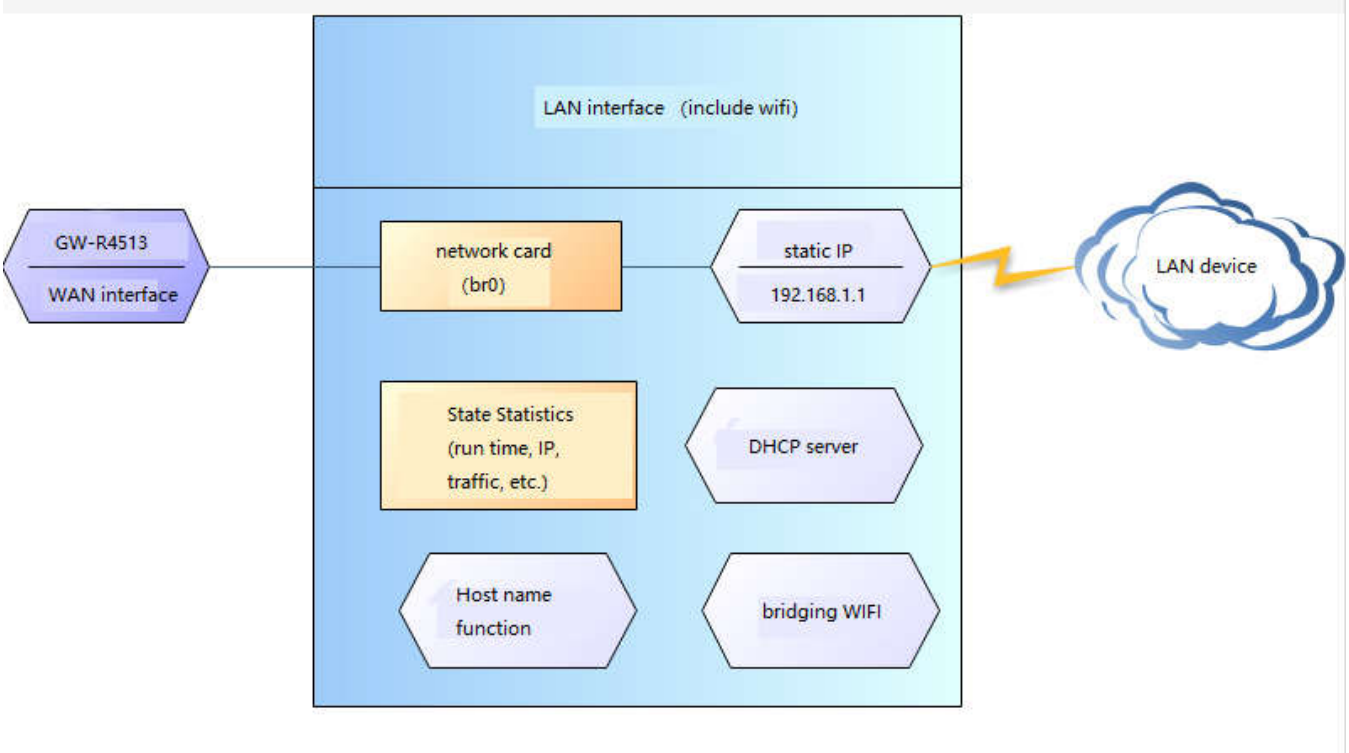


Figure22 WI-FI function

< Description >

- The GW-R4513 router is an AP, and other wireless terminals can access its WLAN network.
- Supports up to 24 wireless STA connections.
- WLAN, LAN and wired LAN port exchange each other.
- The maximum coverage of WIFI is 150m in the open area.

Table6 WIFI default parameter

Name	Parameter
SSID name	GW-R4513-XXXX（XXXX is the last 4 bit of MAC address）
Wi-Fi password	12345678
Channel	Auto
Bandwidth	40MHz
Encryption	WPA2-PSK

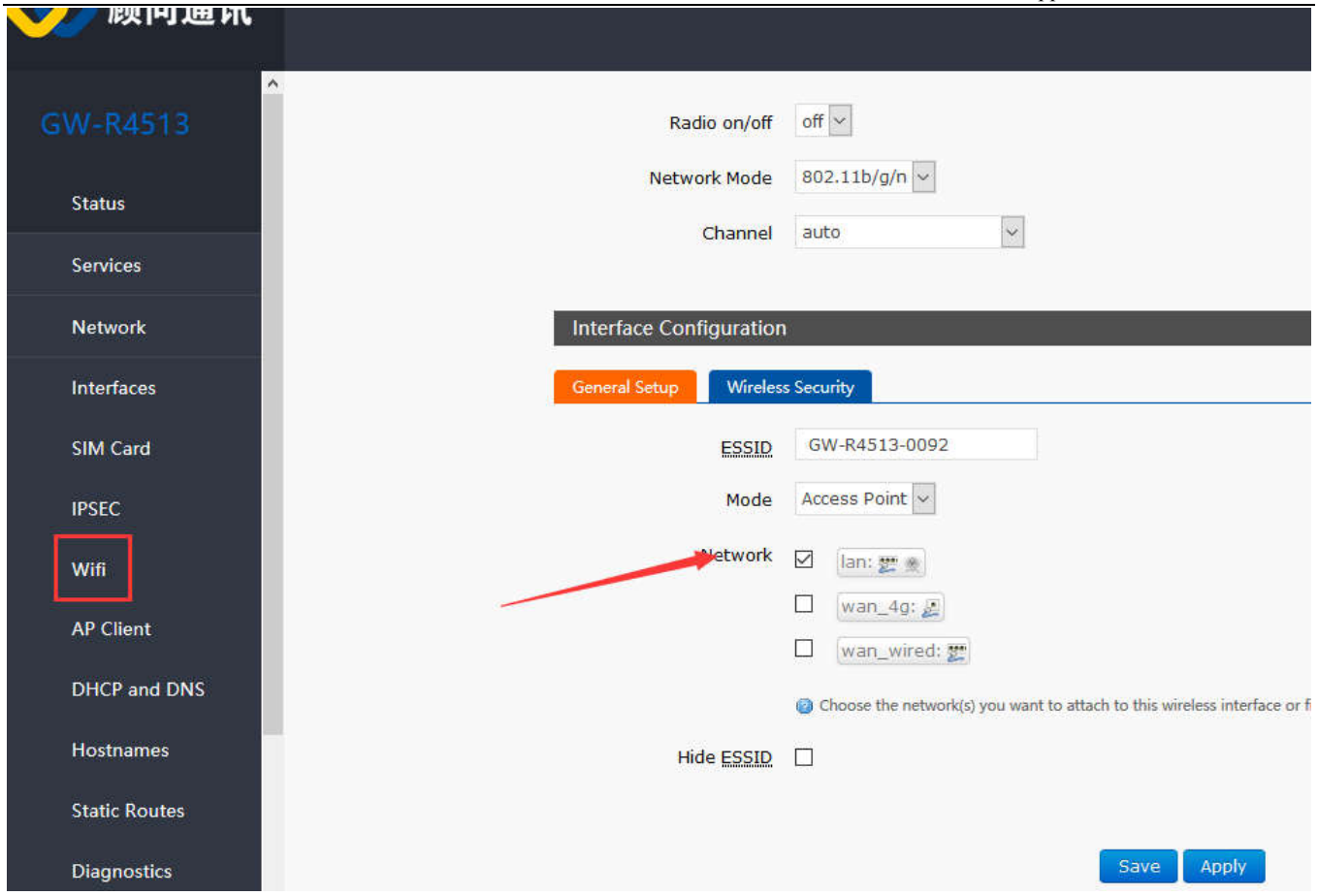


Figure23 the setting page of SSID

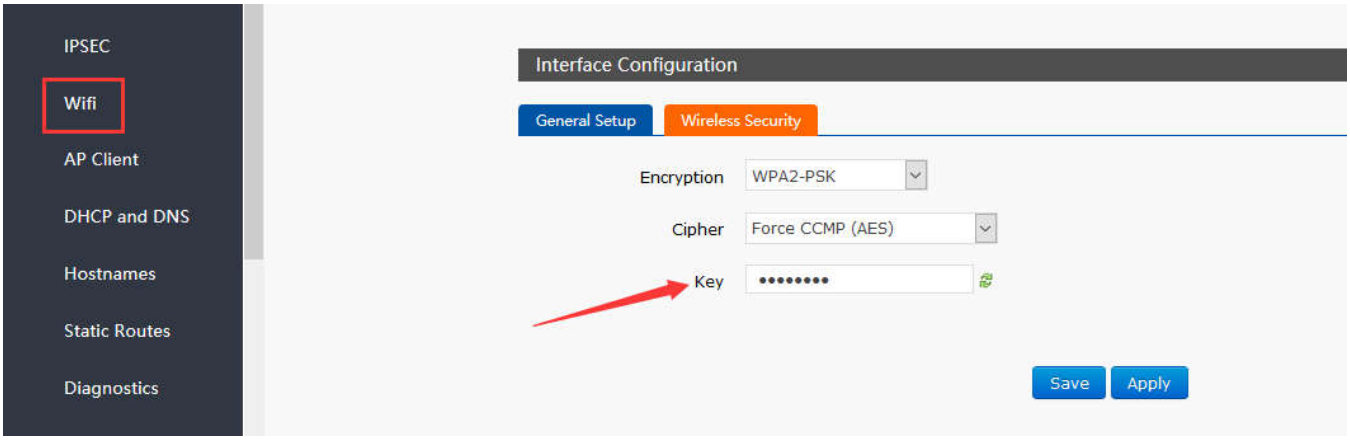


Figure24 the setting page of WI-FI

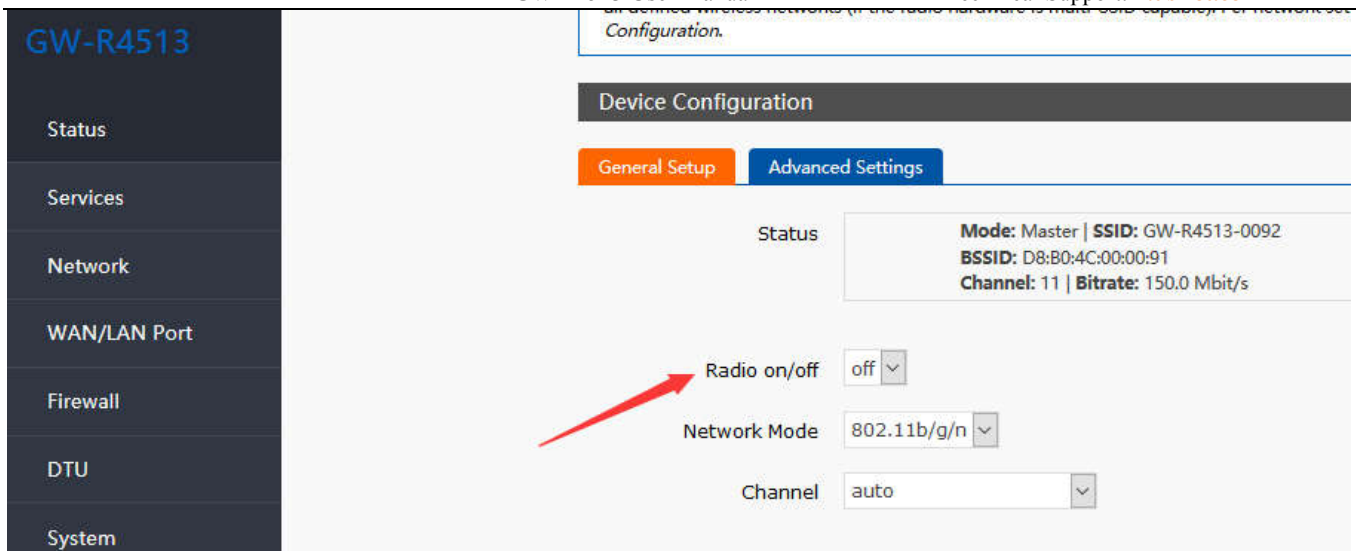


Figure25 the setting page of radio on/off

3.4.7.4G Interface

This router supports the interface of one 4G/3G/2G communication module to access external network.
4G interface function:

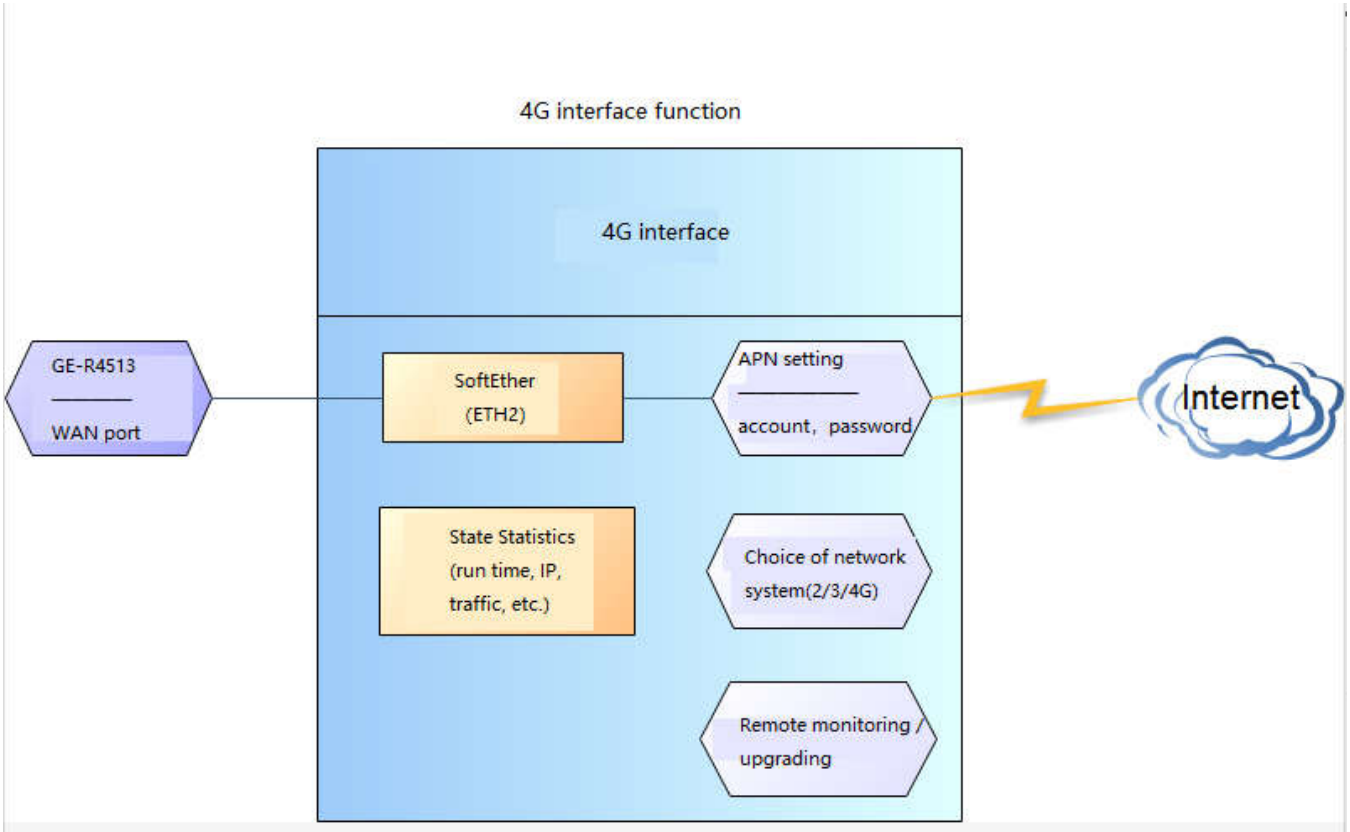


Figure 26 4G interface function

Webpage:

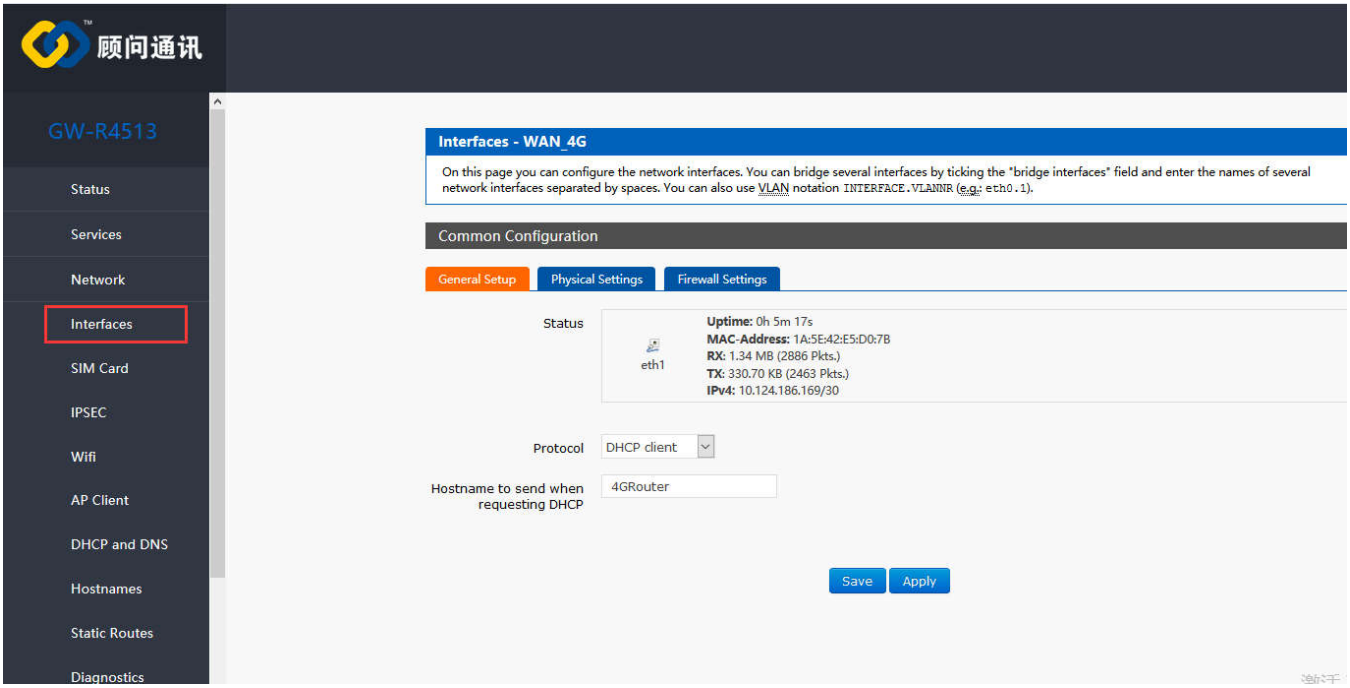


Figure 27 webpage

If the run time is 0, the network card can't run successfully.

Table7 status table

No	Name	Intro
1	Run time	The running time after power on
2	MAC address	The MAC address of interface
3	Receive/send	Statistics of receiving and sending data of this network card
4	IPv4	The IPv4 protocol of this network card

< Description >

- GW-R4513-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)
- GW-R4513-E(operating band): FDD-LTE(1/3/5/7/8/20),TDD-LTE(38/40/41),WCDMA(1/5/8),GPRS(3/8)
- The protocol of 4G interface: do not modify, keep the default.
- The router will give priority to the use of wired WAN ports, followed by the use of 4G networks.
- If you use APN private network, please refer to the introduction of APN chapter.

3.4.8. APN Setting

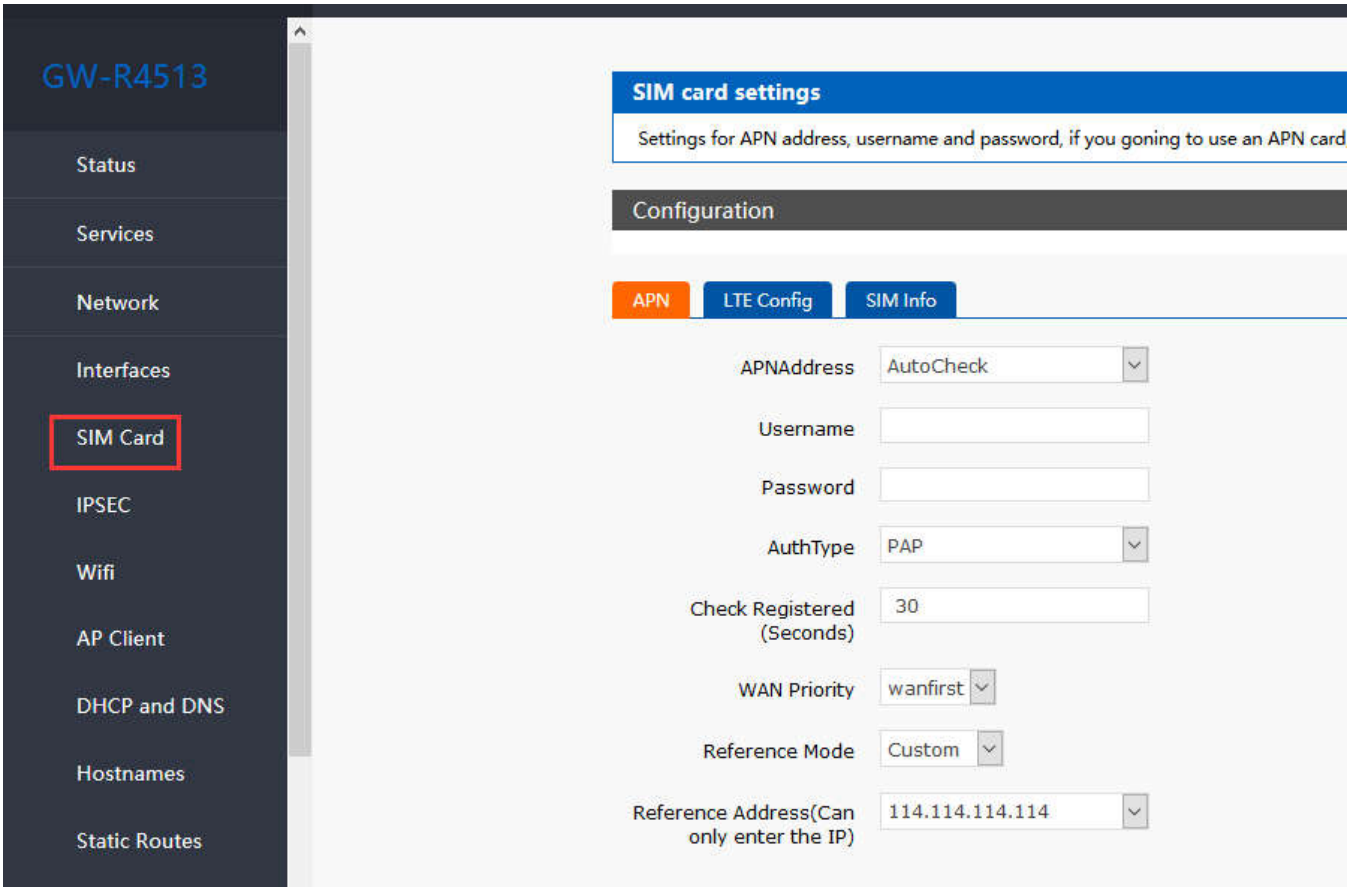


Figure28 the webpage2 of APN setting

If you use an APN card and have a special APN address, you need to set the APN address, username, and password.

Table8 APN parameter

Parameter name	Function
APN address	Fill in the APN address
Use name	The default is empty. If you use APN card, please fill in correctly.
Password	The default is empty. If you use APN card, please fill in correctly.
Type of PDP	Default
Auth type	Default
Others	Please keep default

Note

- Normal 4G mobile phone card, without setting up, you can access the Internet.
- If you use APN special network card, you must fill in the APN address, user name and password.

3.4.9. VPN Client(PPTP/LTTP/GRE/OPENVPN)

3.4.9.1. 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.

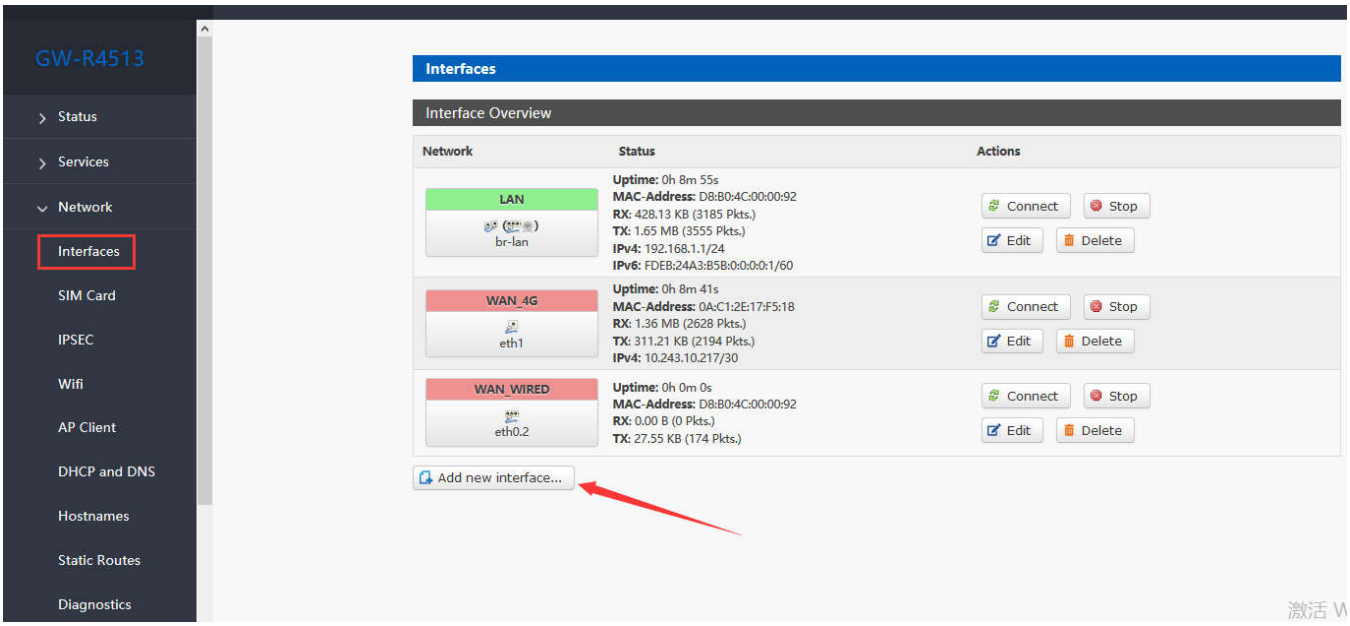


Figure29 the webpage1 of VPN

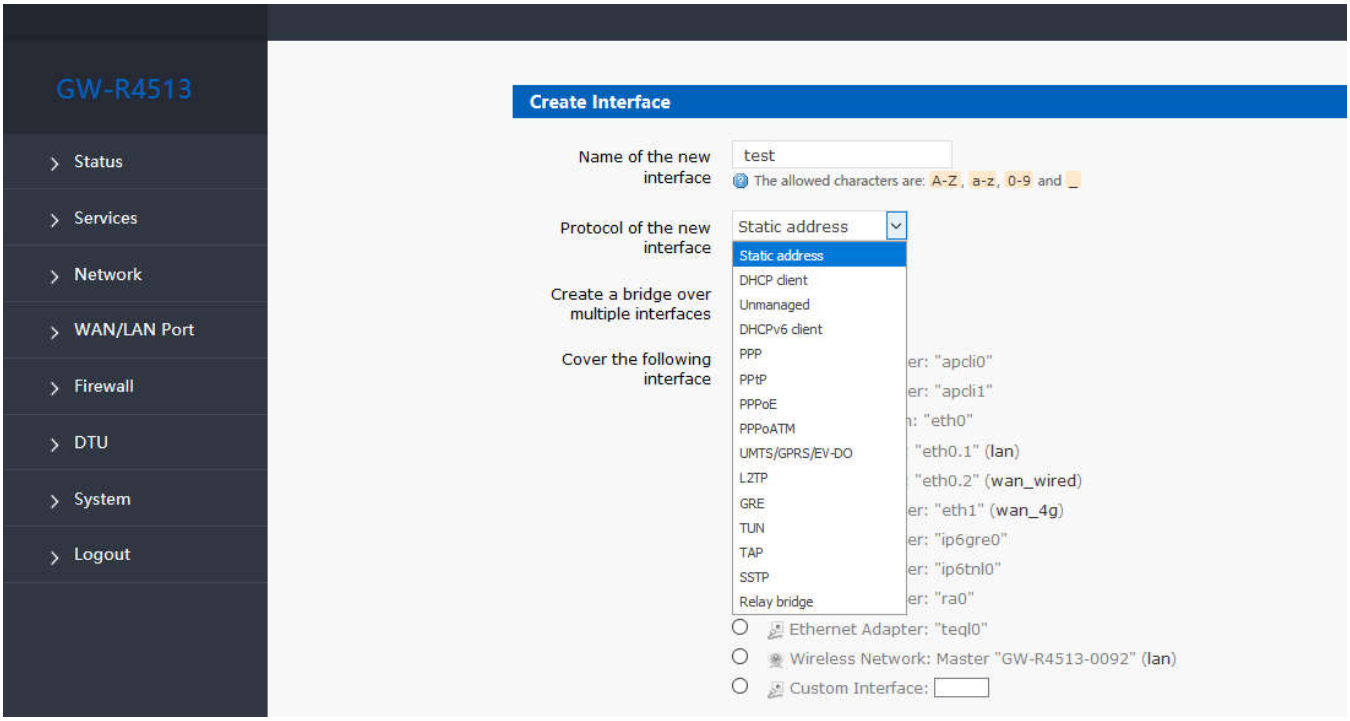


Figure30 the webpage2 of VPN

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

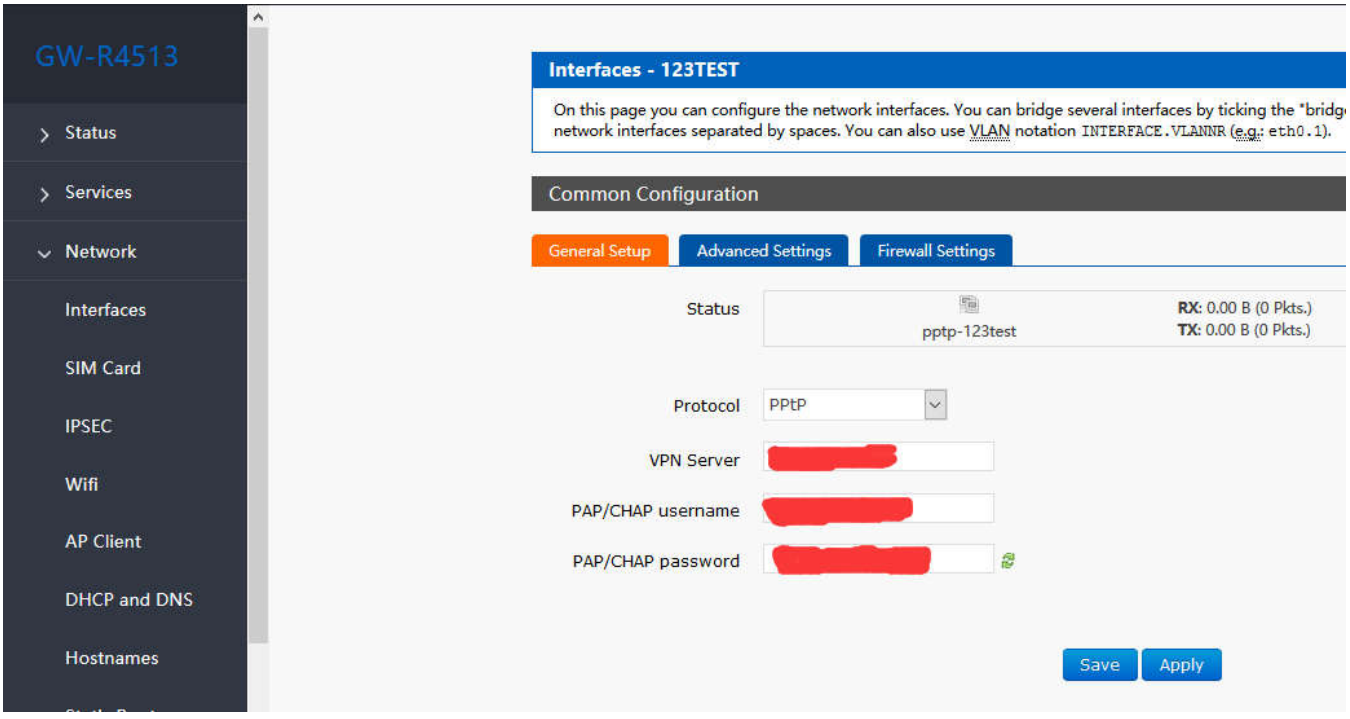


Figure31 the webpage3 of VPN

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.

3.4.9.2. L2TP Client

1. L2TP supports multiple authentication (MSCHAPV2, CHAP, EAP, PAP), MPPE encryption, L2TP OVER IPSEC encryption.
2. increased the way of tunnel password authentication.

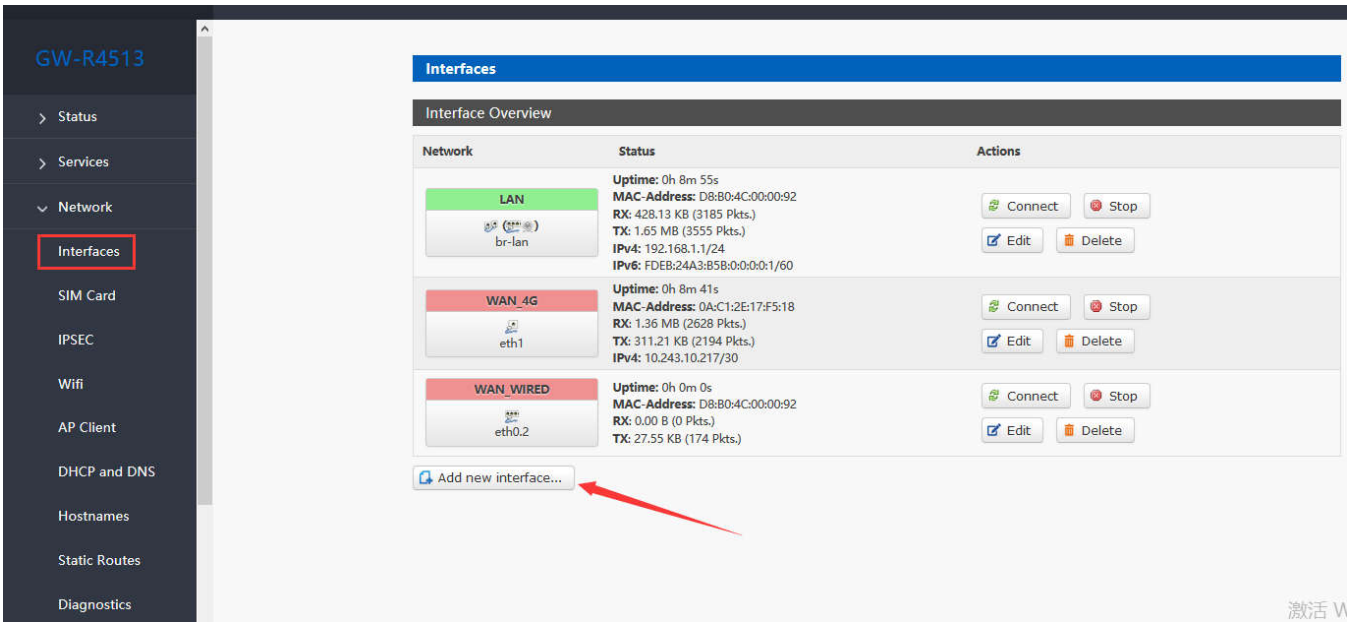


Figure32 create interface

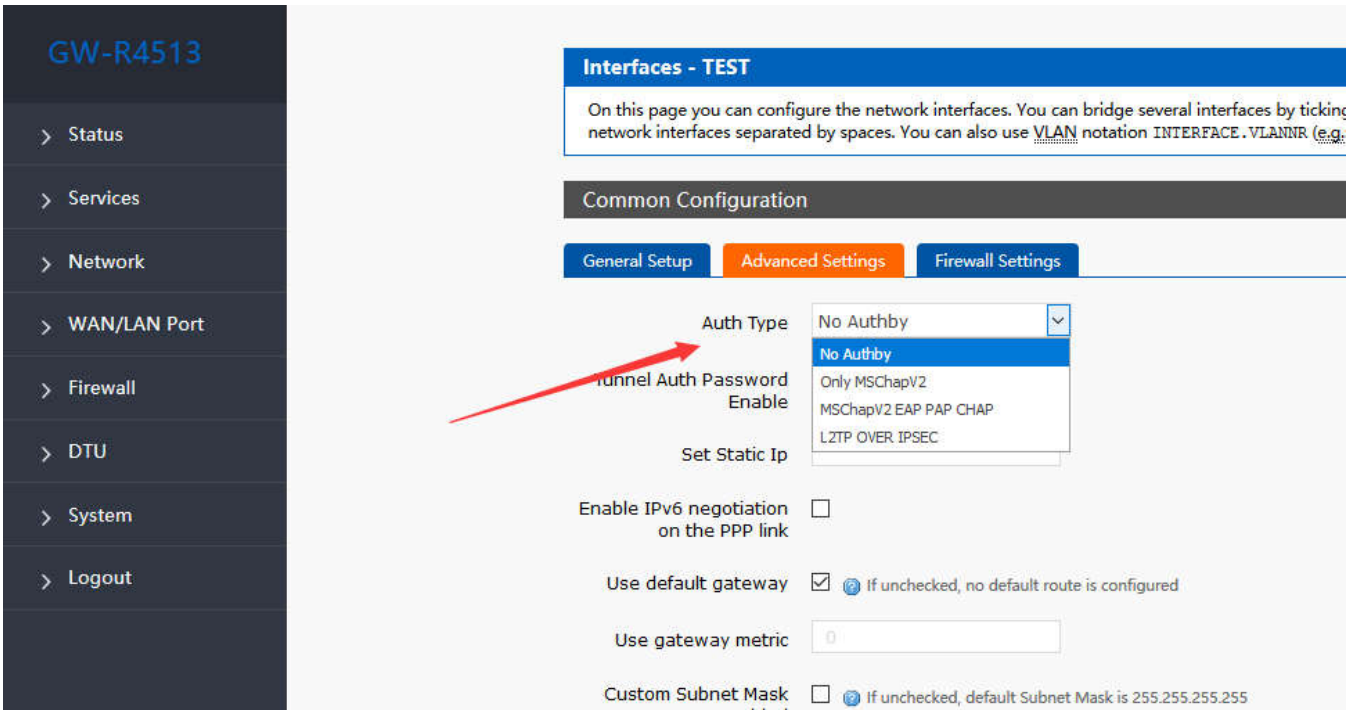


Figure33 auth type

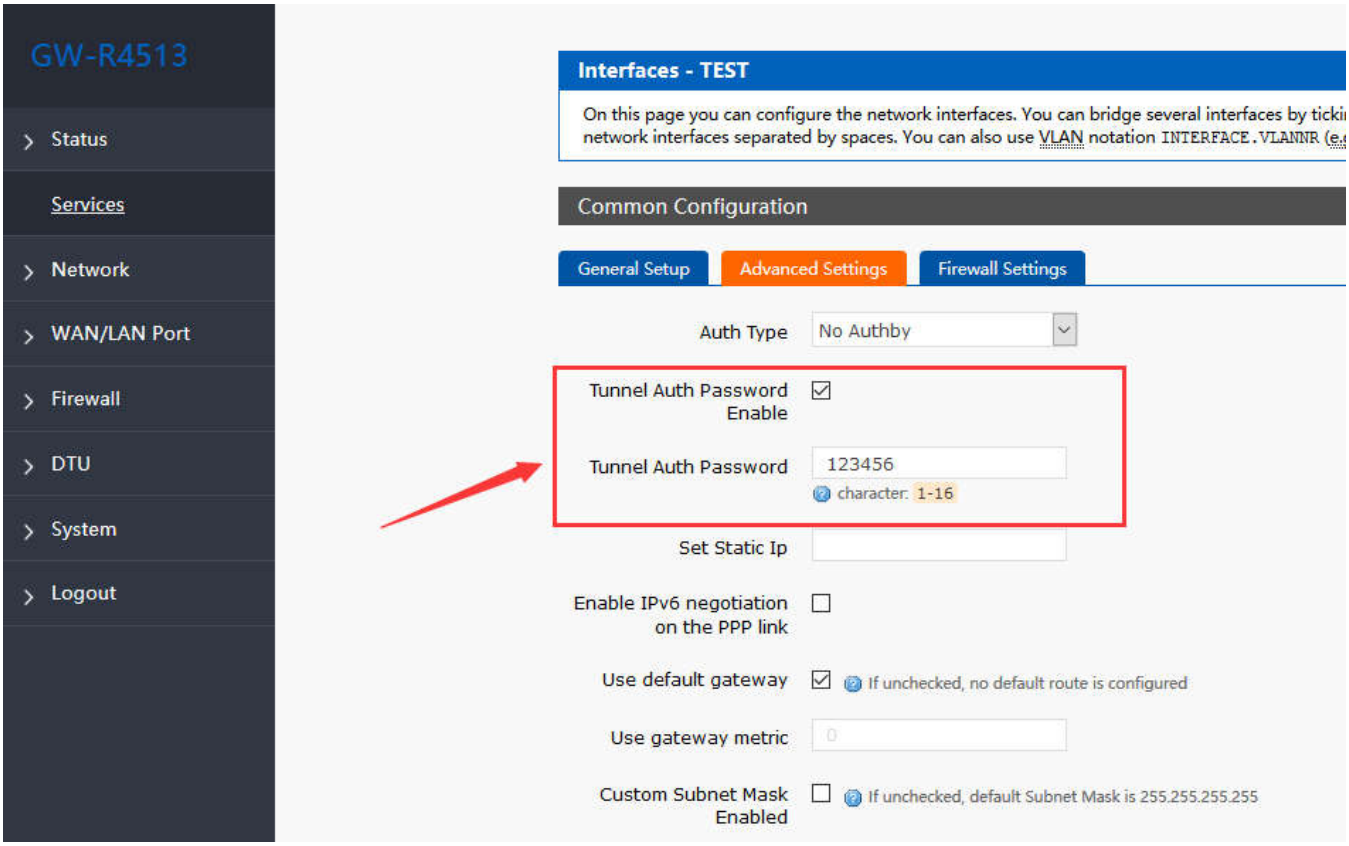


Figure34 tunnel auth password

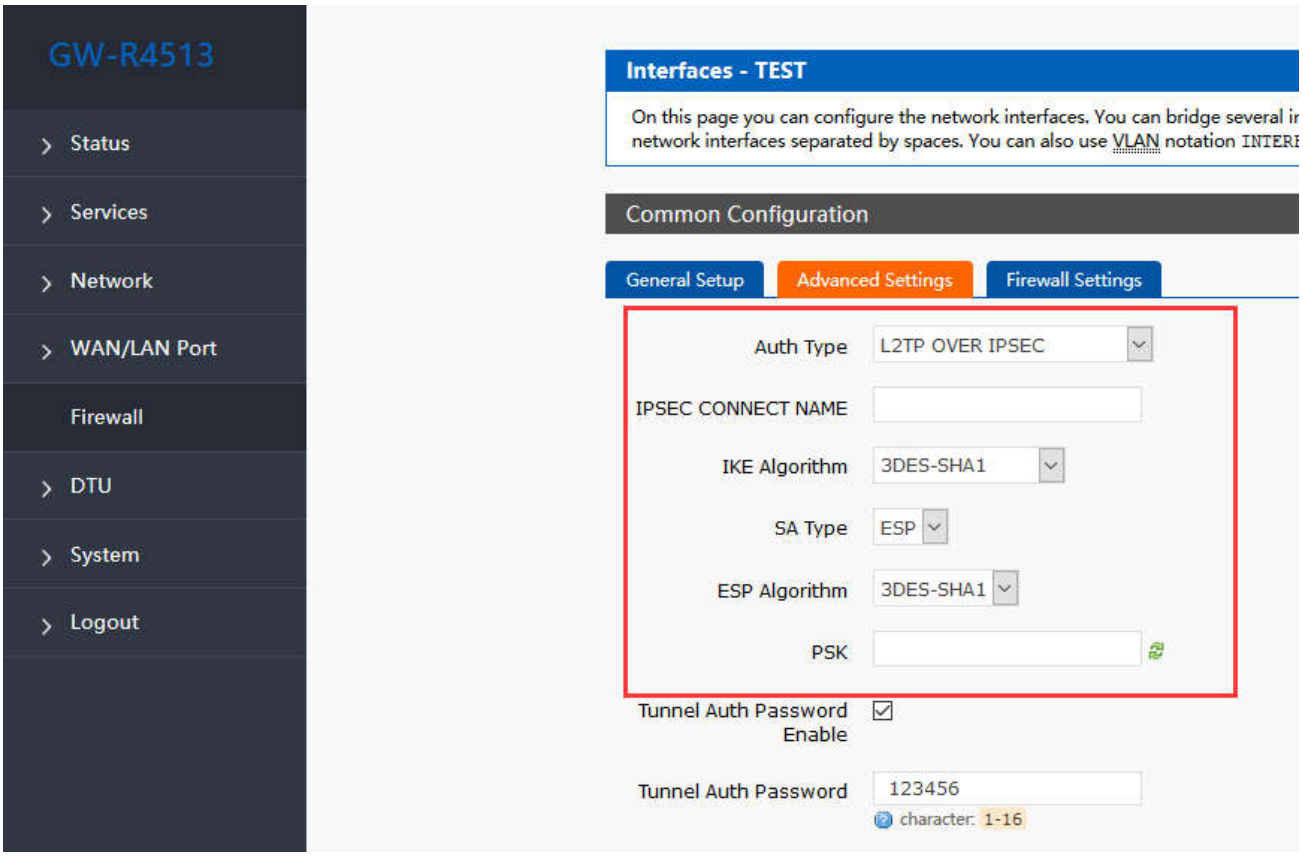


Figure35 L2TP OVER IPSEC auth type

3.4.9.3. IPSEC

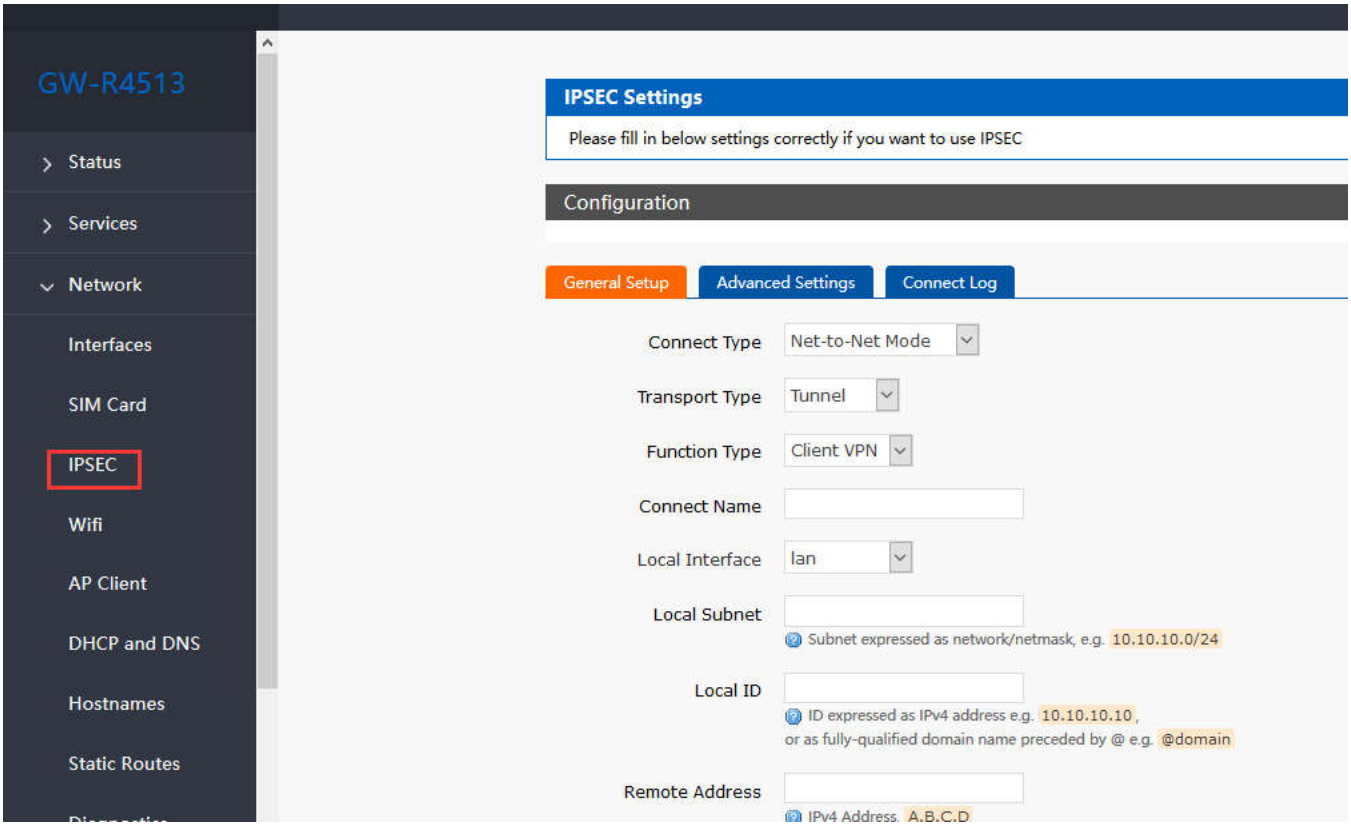


Figure36 IPSEC setting

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 @

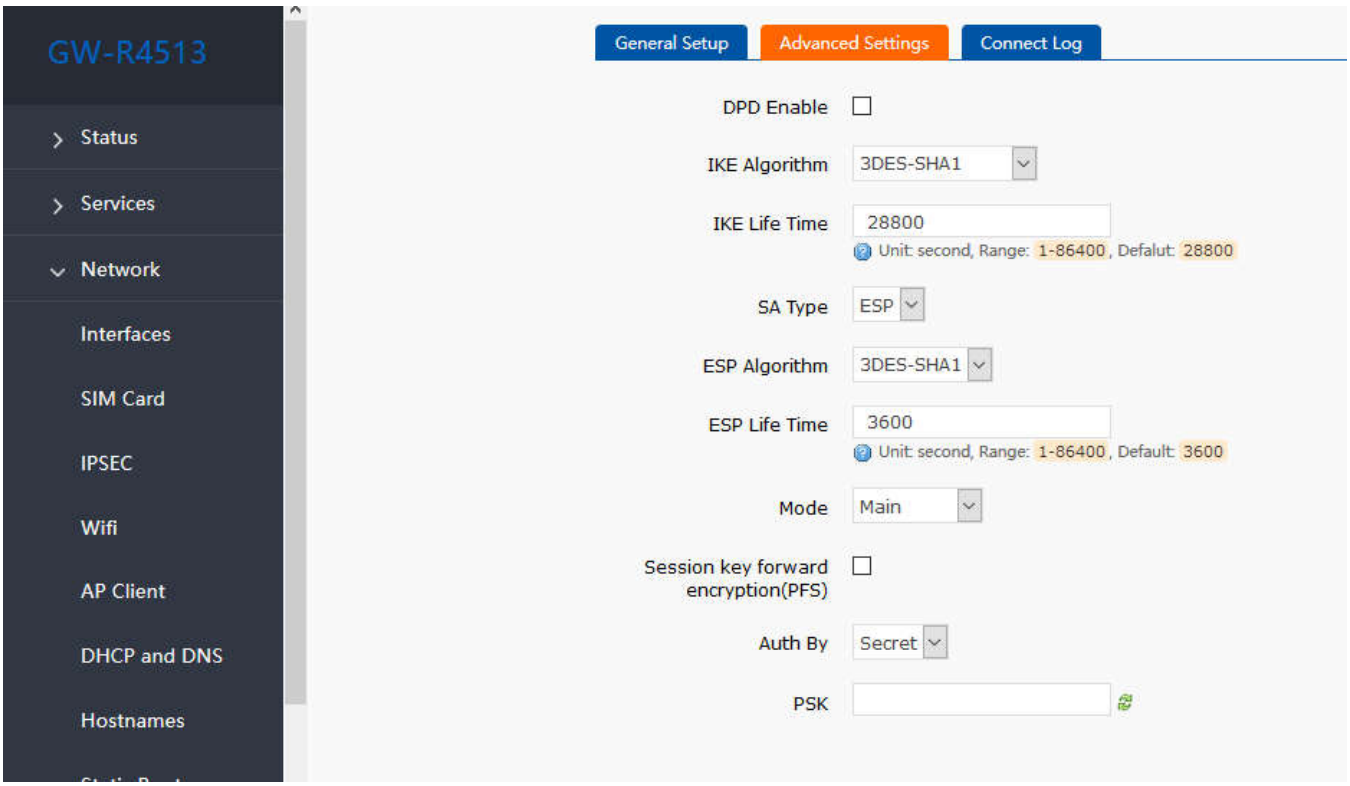


Figure37 IPSEC advance setting

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.

3.4.9.4. OPENVPN

Add one interface, choose TUN or TAP mode:

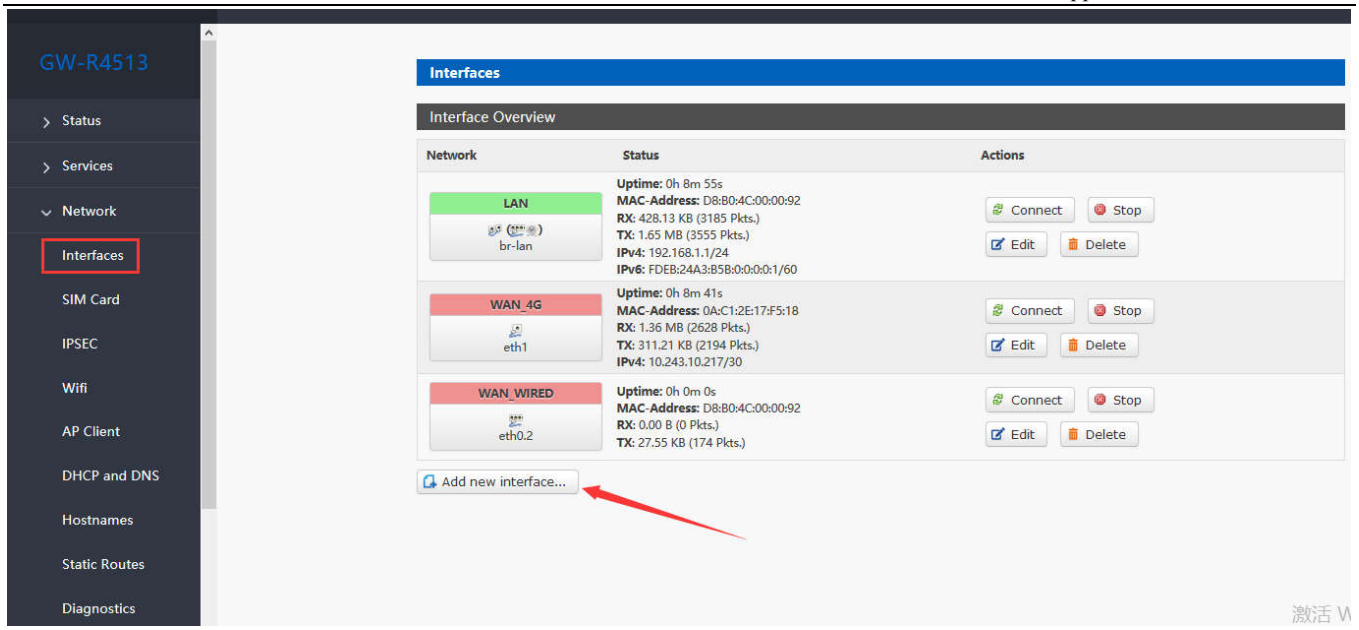


Figure38 add new interface

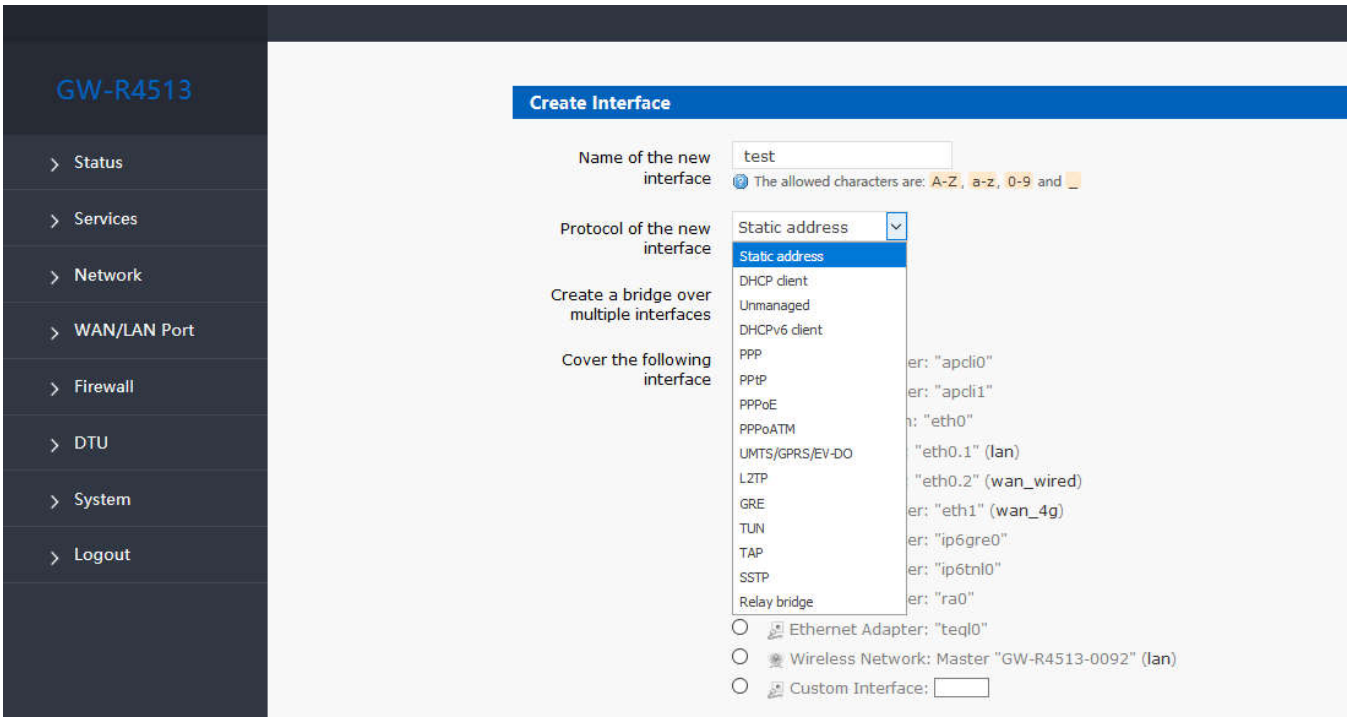


Figure39 add OPENVPN interface

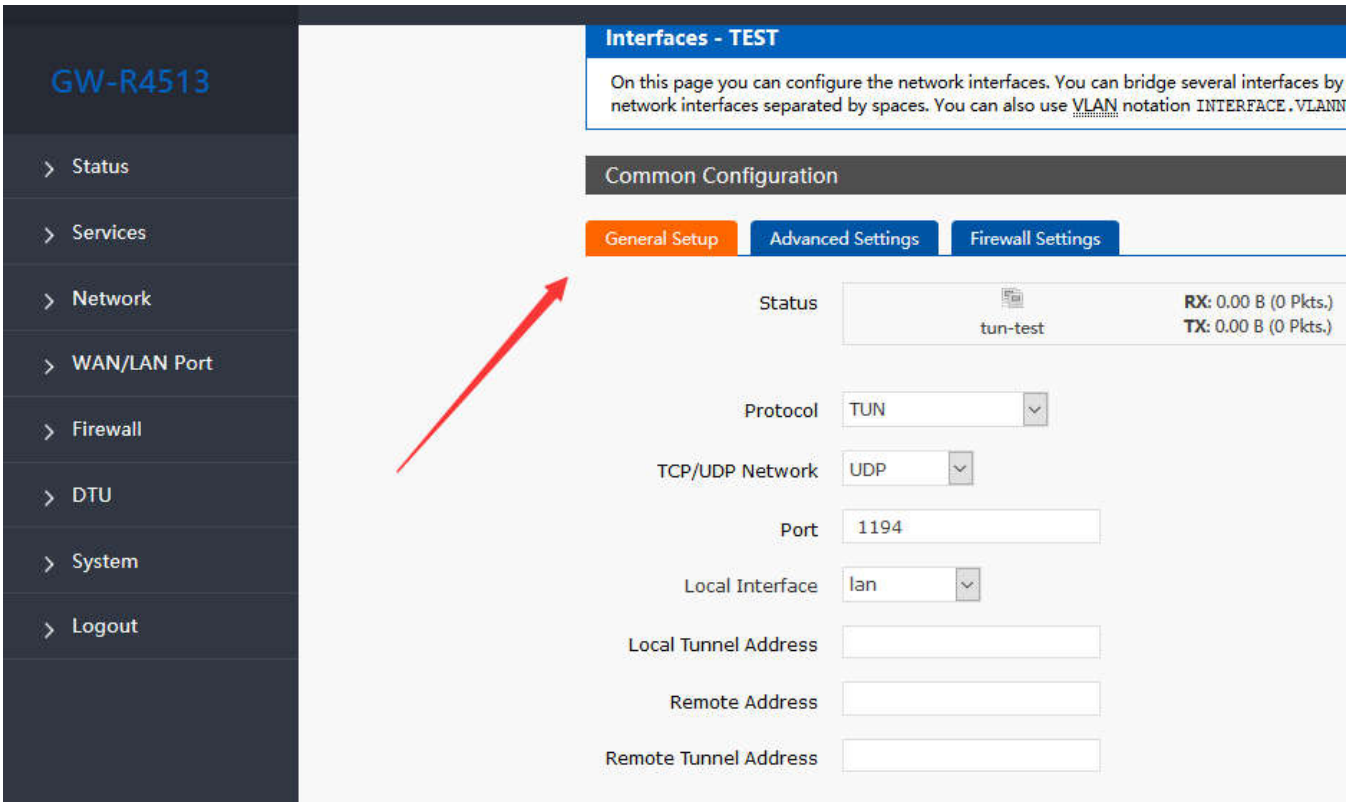


Figure40 general setting

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.

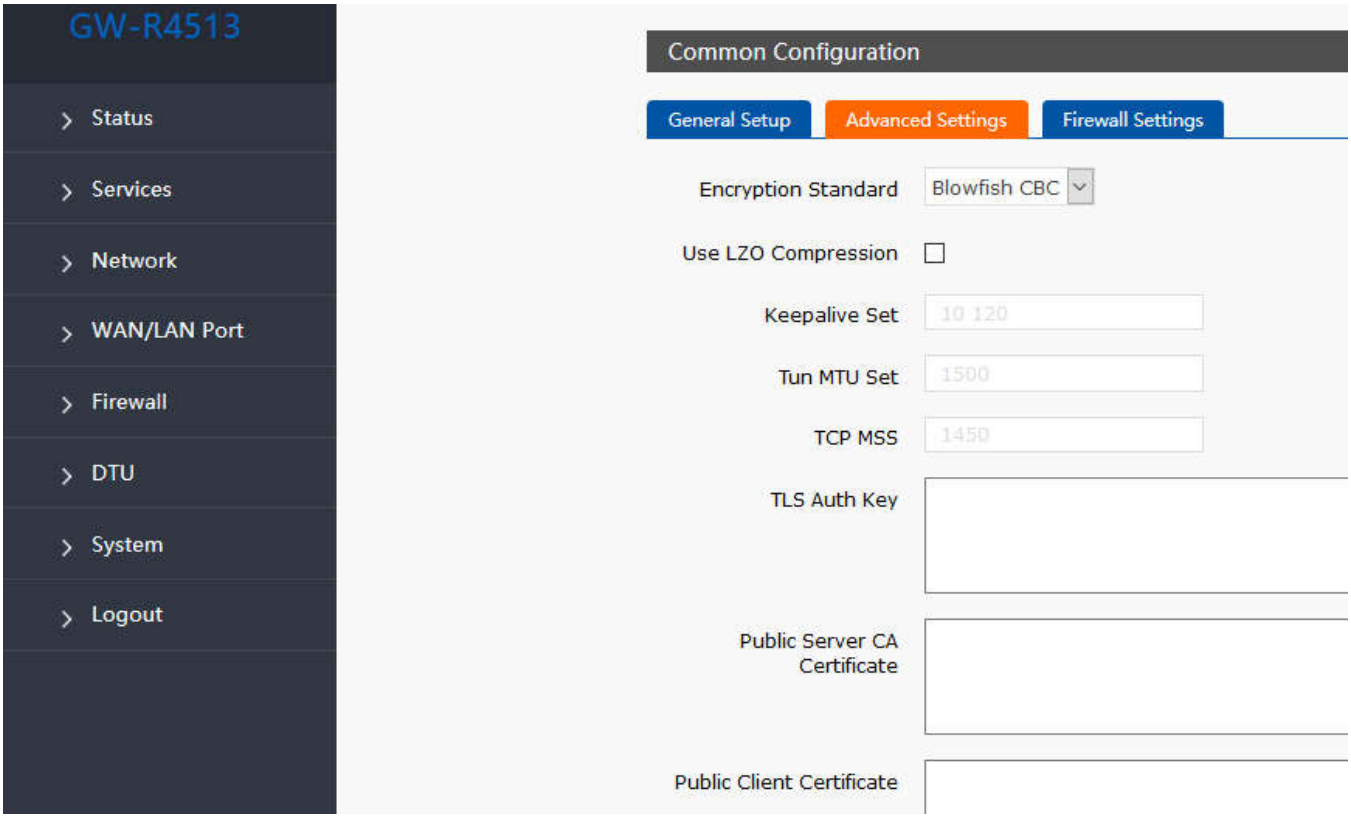


Figure41 advance setting

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.

3.4.9.5. GRE

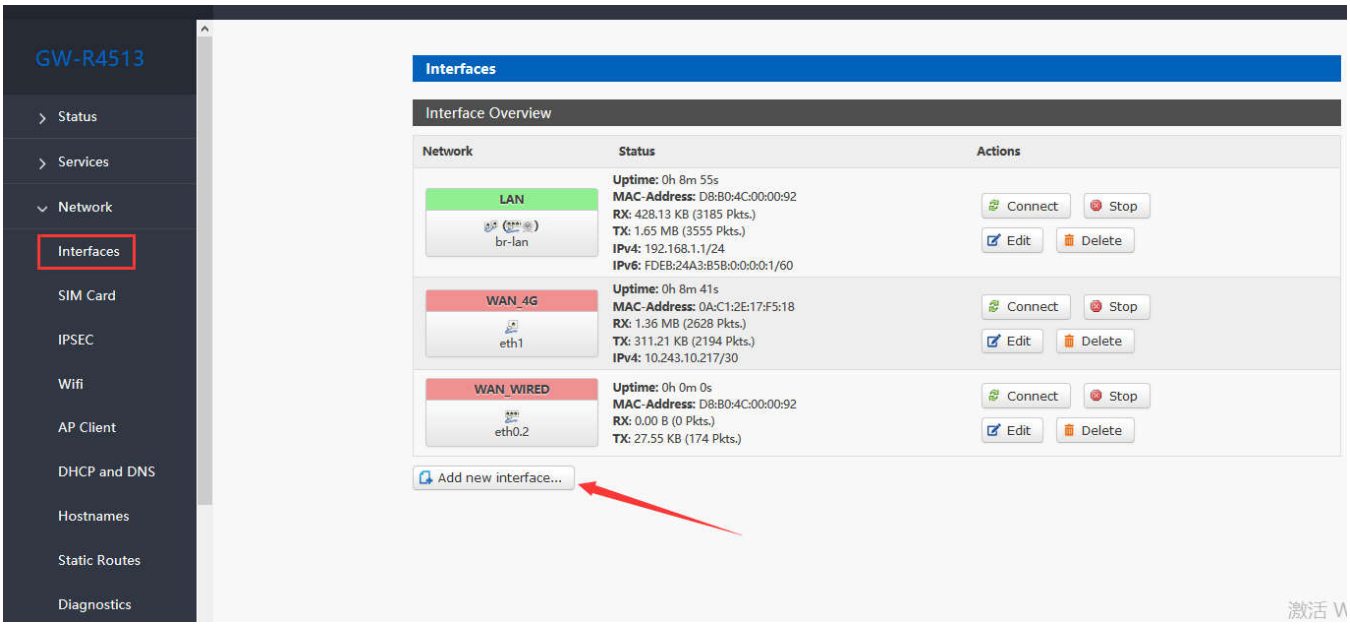


Figure42 add new interface

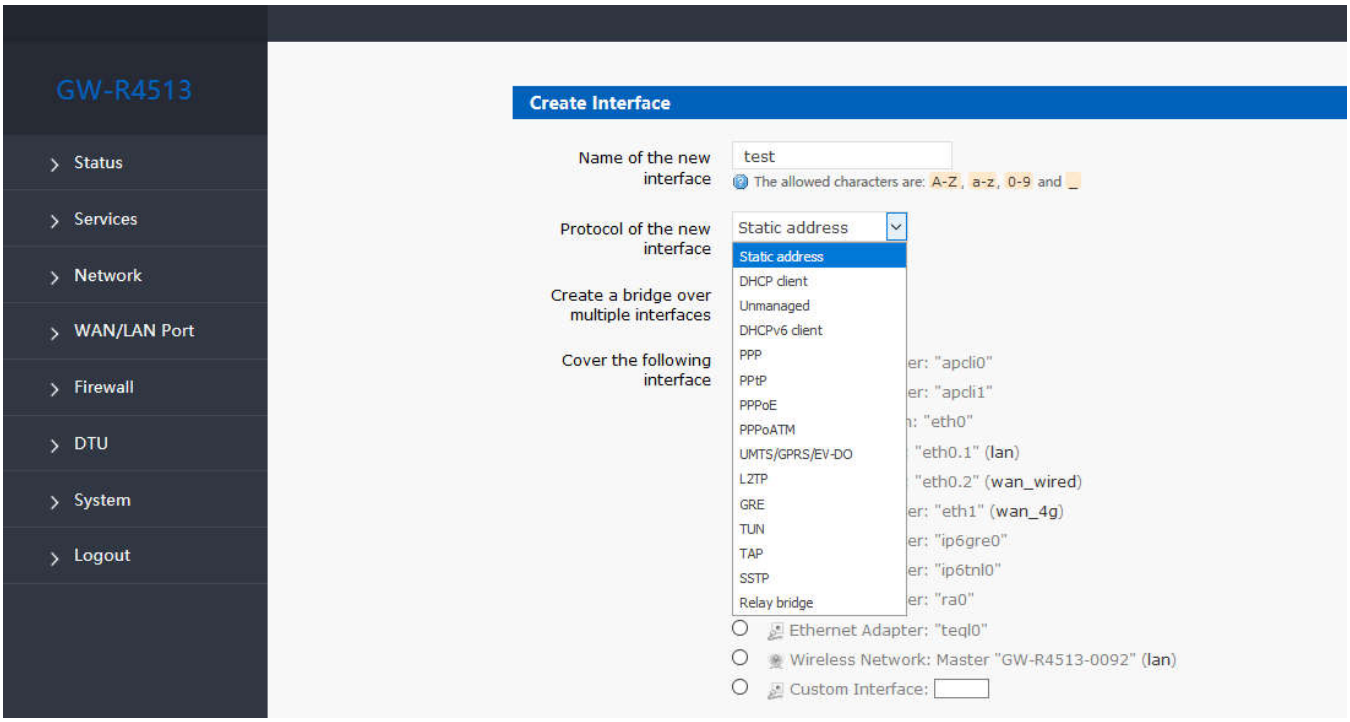


Figure43 add GRE interface

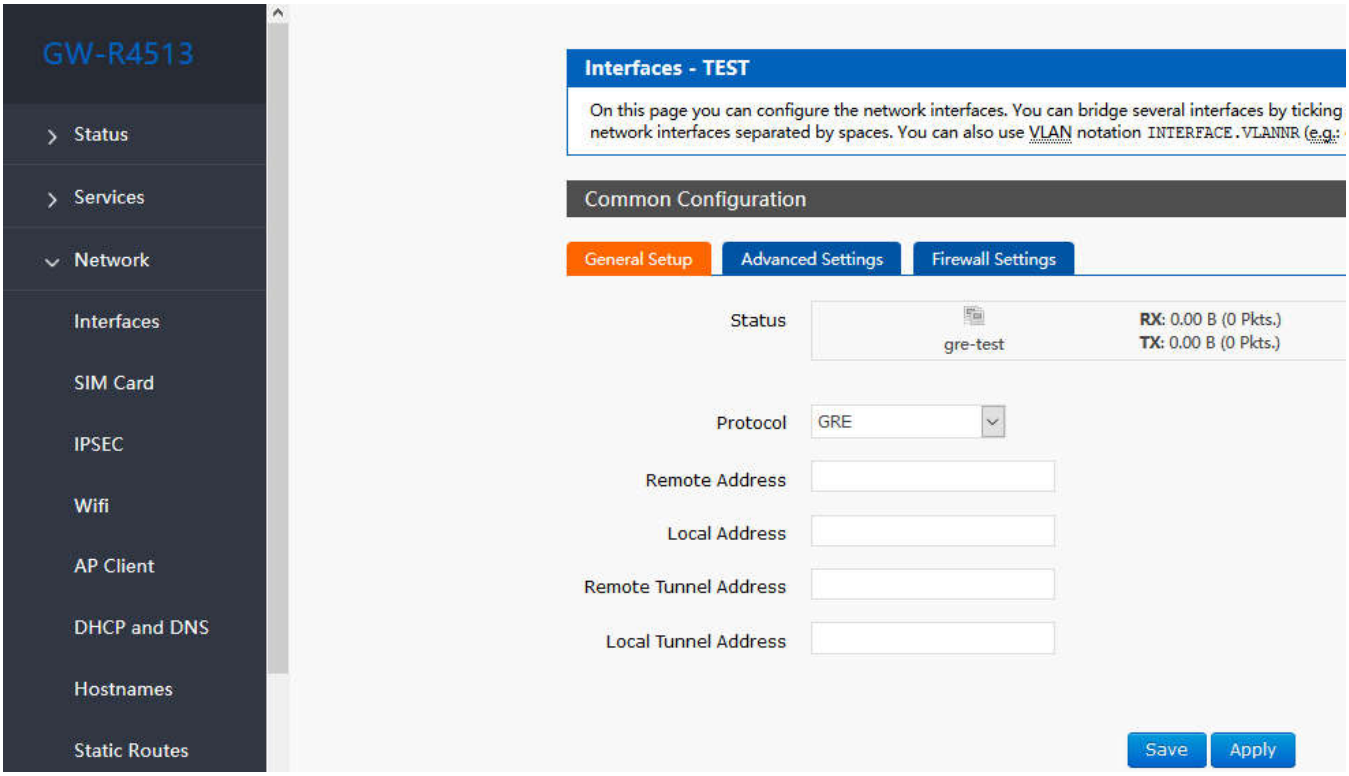


Figure44 GRE general setting

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 accodeing to need.

Remote Tunnel Address: the opposite GRE tunnel IP address , and the setting of subnet masks can be expressed as follows:

255.0.0.0 can be written as IP/8, 255.255.0.0 can be written as IP/16, 255.255.255.0 can be written as IP/24, 255.255.255.255 can be written as IP/32

For example, 172.16.10.1/24

Local tunnel IP: local GRE tunnel IP address

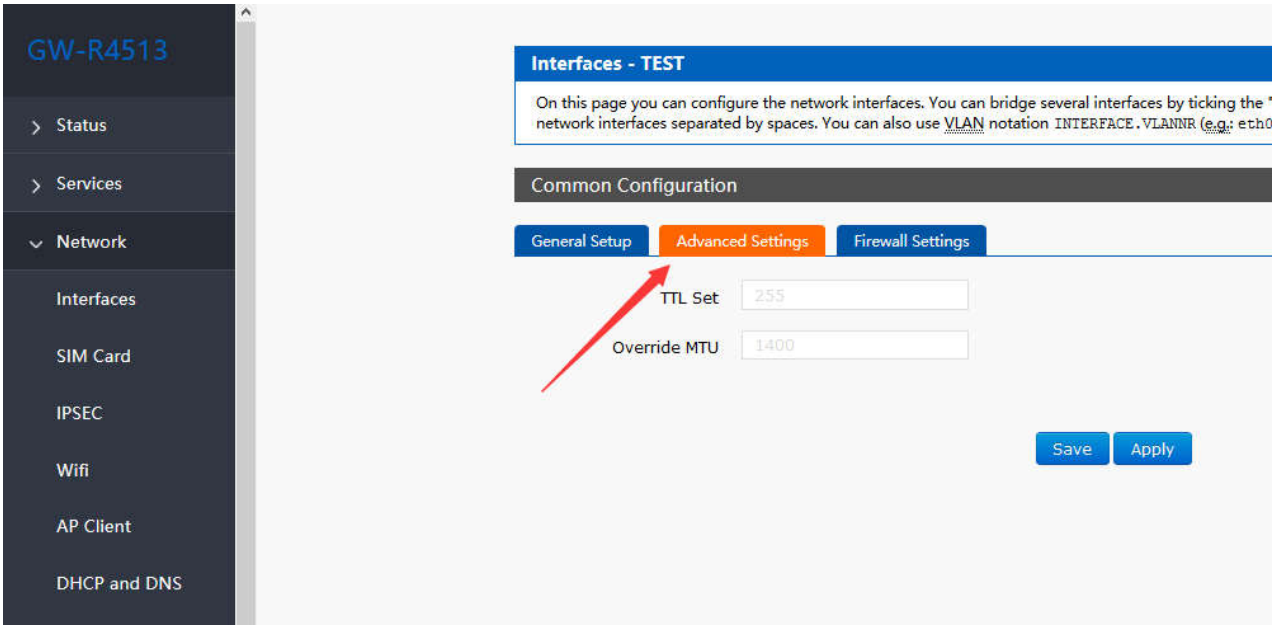


Figure45 GRE advance setting

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

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

3.4.9.6. SSTP Client

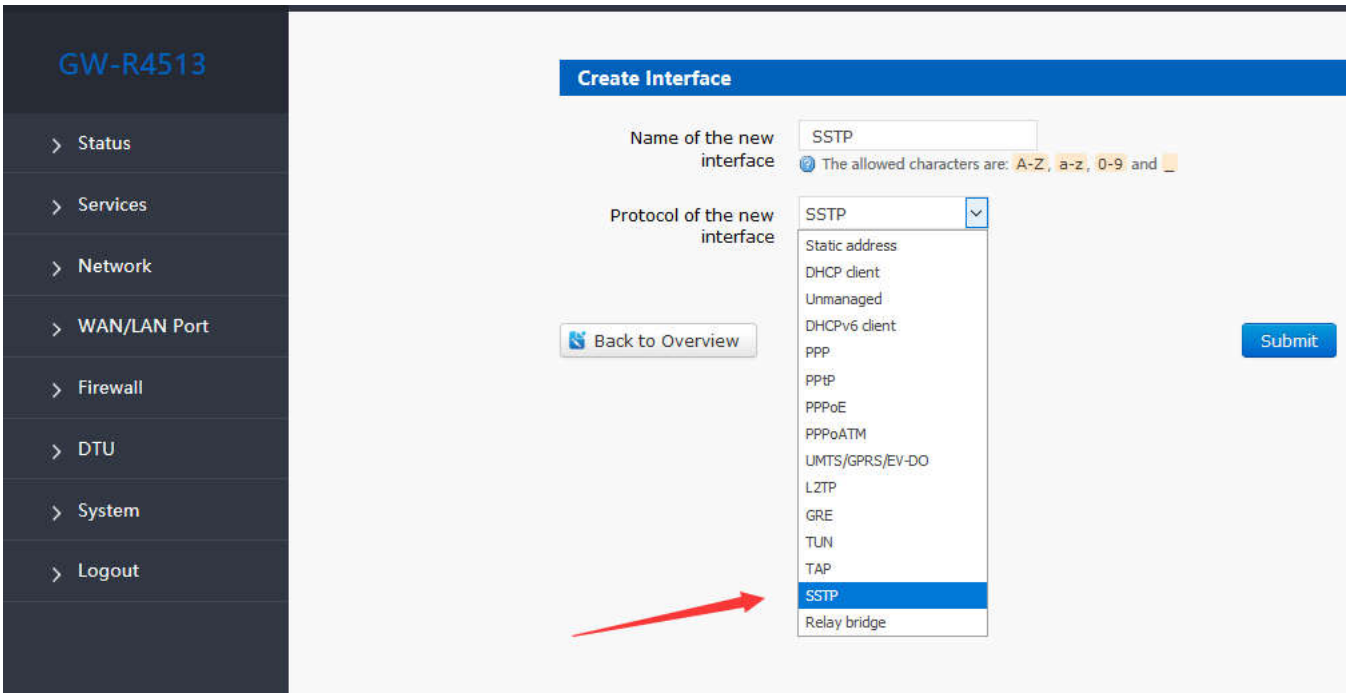


Figure46 add new interface

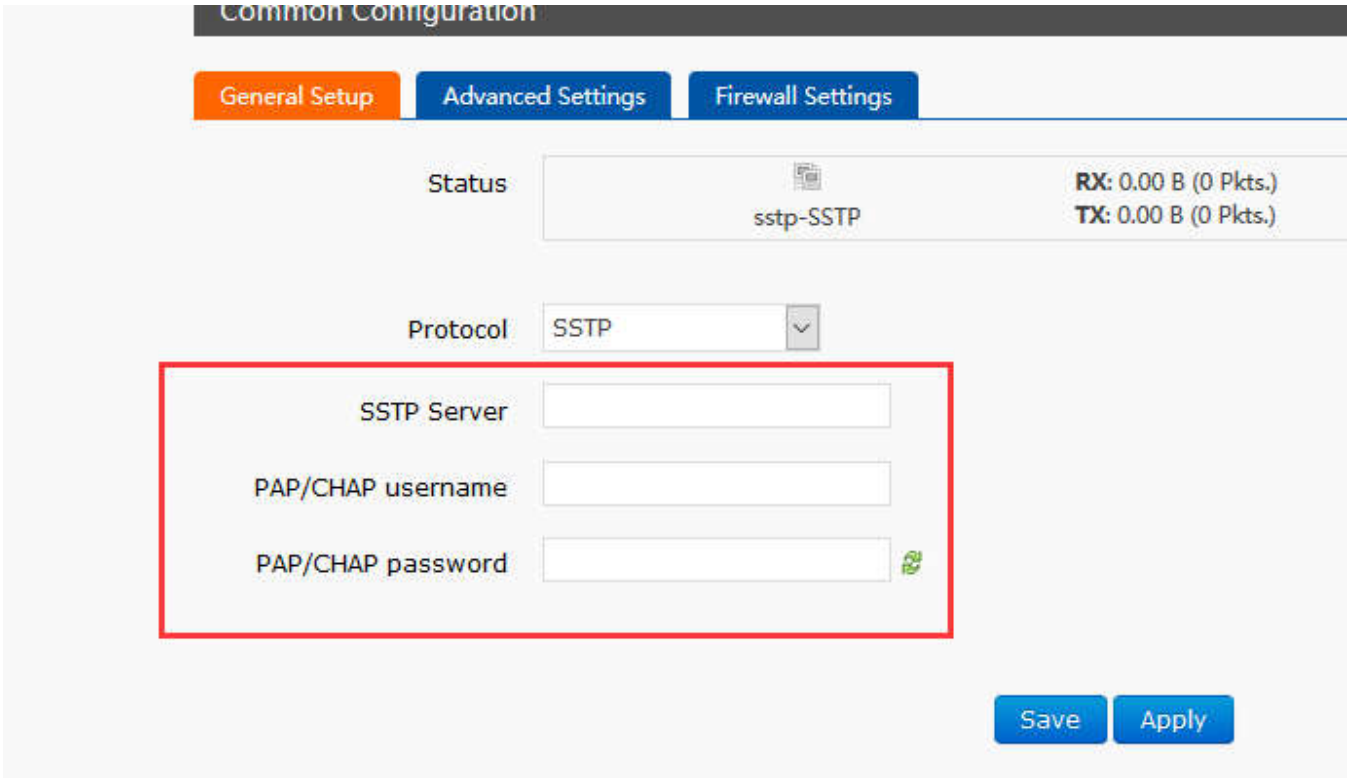


Figure47 SSTP general setting

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.

3.4.10. Static Router

Table9 static router parameter

Name	Info	Note
Interface	Port for executing rules	eth0.2
Remote IP	Remote IP or address	192.168.1.0
Subnet	The remote subnet	255.255.255.0
Gateway	Address to be forwarded to	192.168.0.202
Metric		0
MTU	Maximum transmission unit	1500

Static routing describes the routing rules of Ethernet packets.

3.4.11. NAT Function

3.4.11.1. 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.

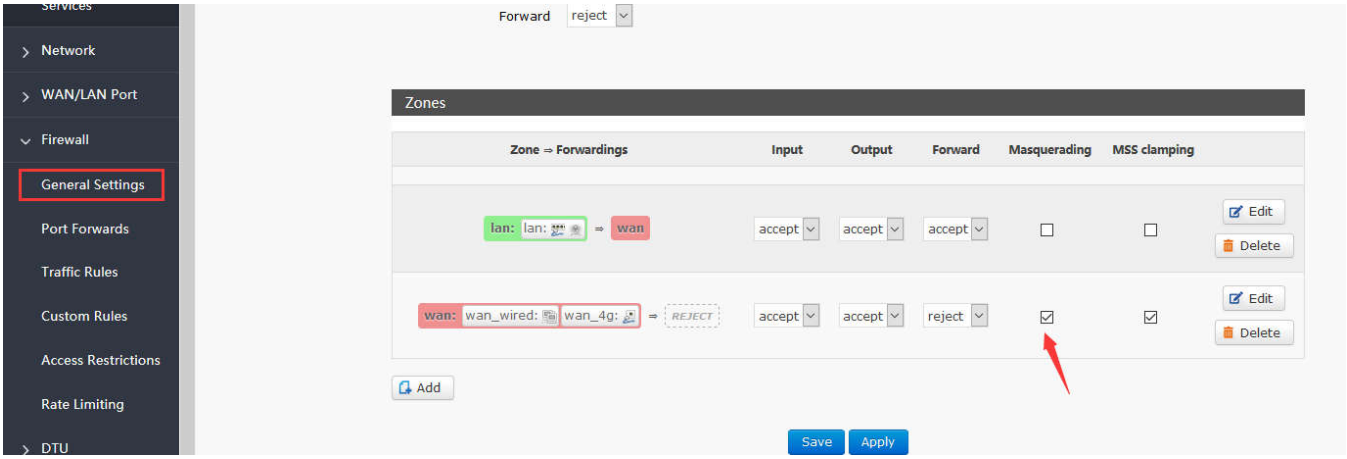


Figure48 MASQ setting

3.4.11.2. 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.

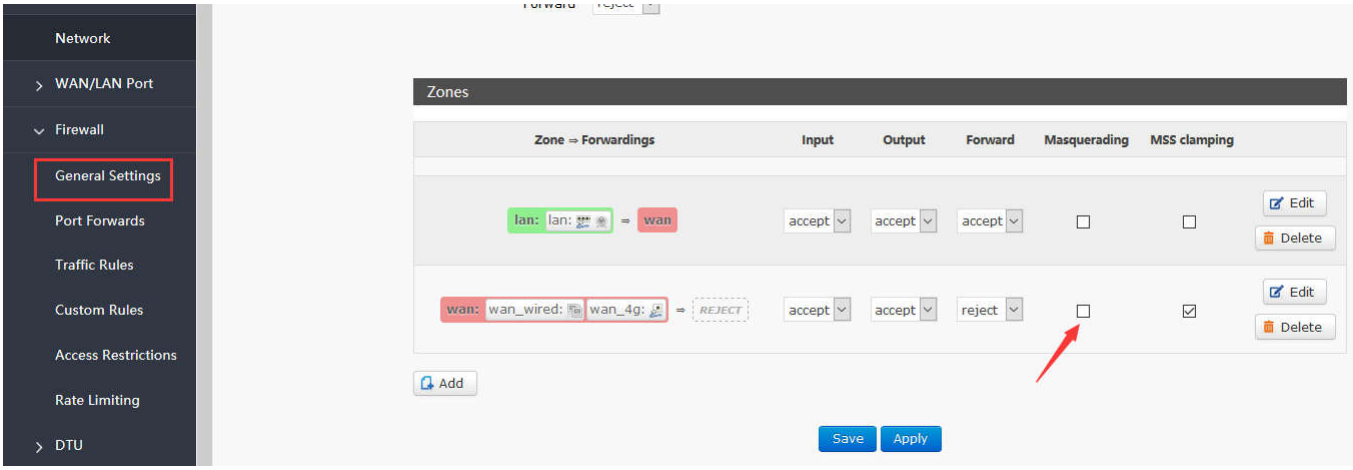


Figure49 close MASQ

Then setup SourceNAT.

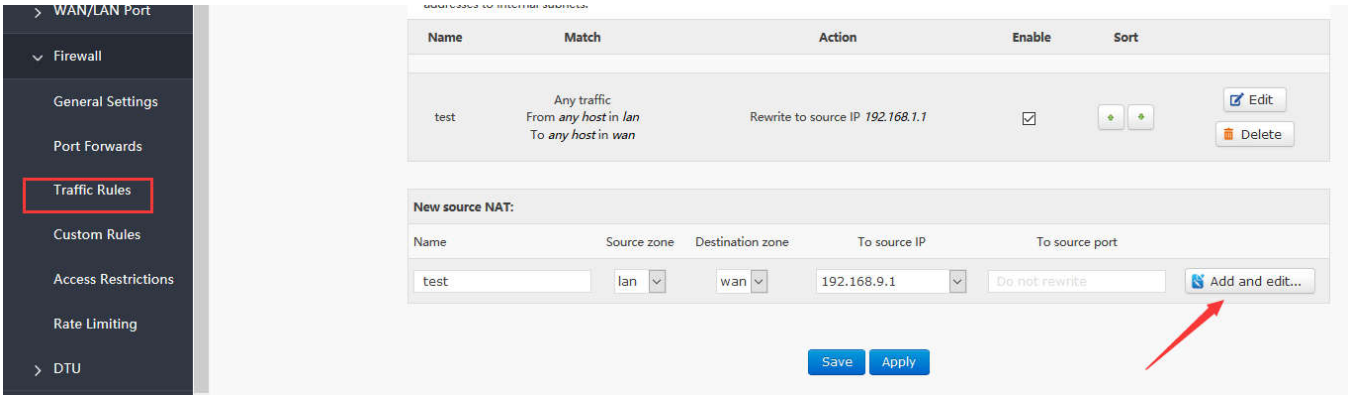


Figure50 NAT setting1

Figure51NAT setting2

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

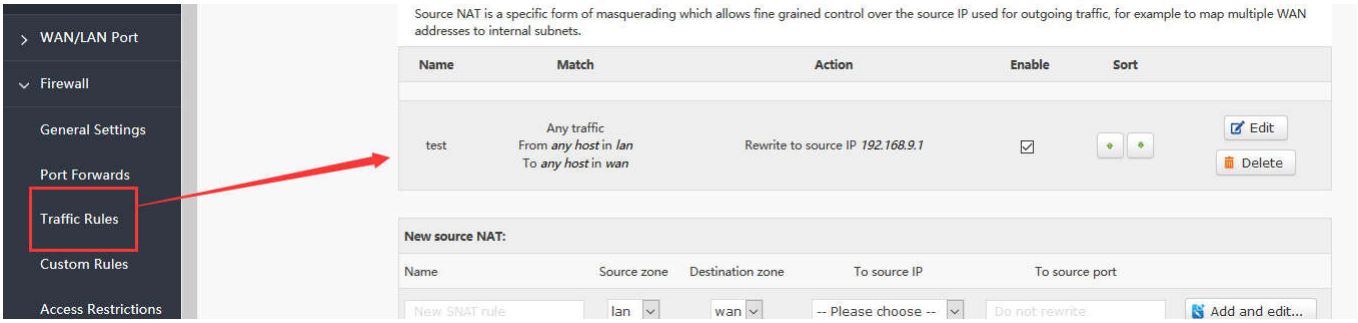


Figure52 NAT setting3

3.4.11.3. DNAT

DNA T 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

3.4.11.3.1. Port Forward

3.4.11.3.1.1. Introduce

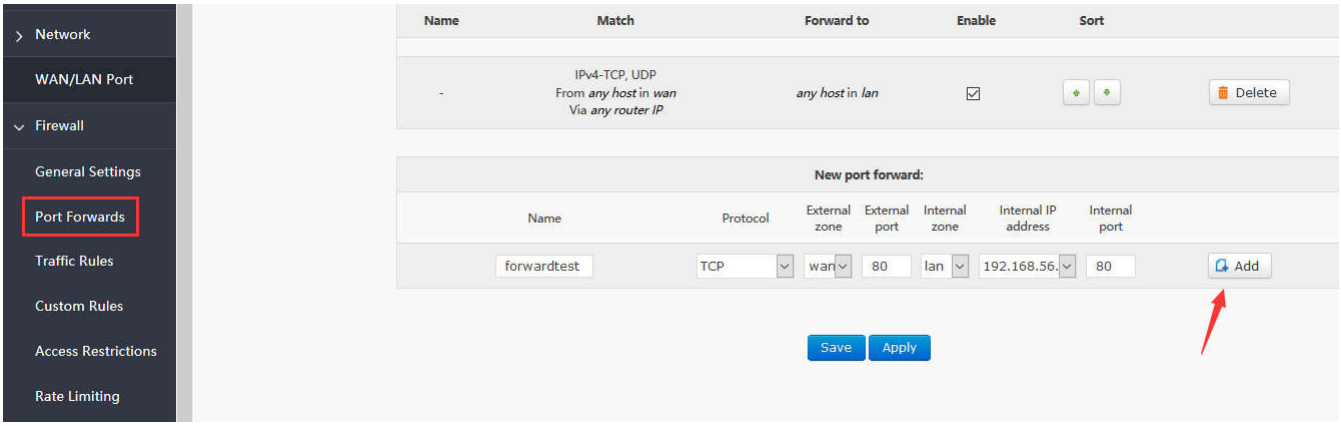


Figure53 port forward setting1

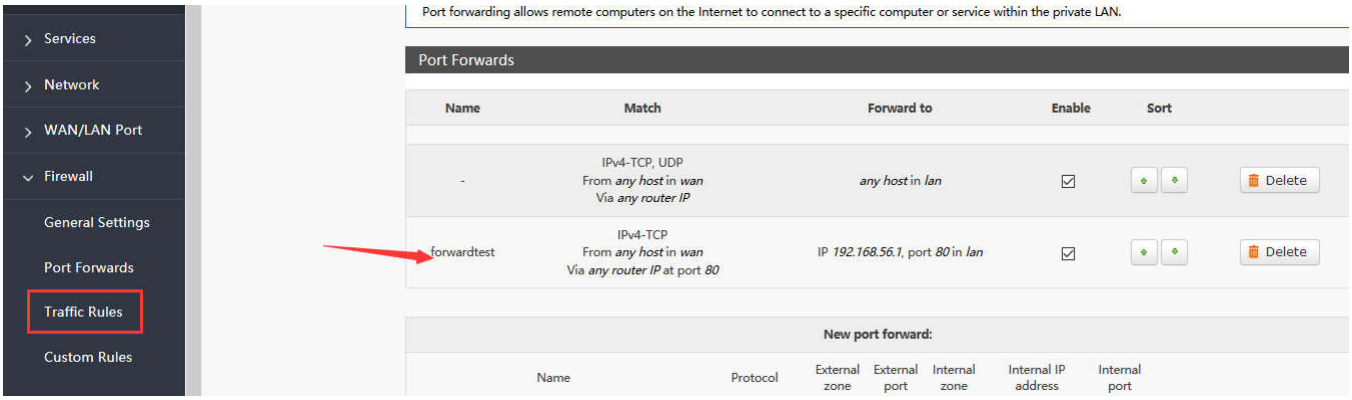


Figure54 port forward setting2

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.

3.4.11.3.1.2. Port Forward on 4G Interface

Table9 port forward parameter

Use environment	Content	Info
Router	4G router	
	SIM card	APN card (IP: 10.201.20.47)
PC	IP of PC in LAN	192.168.1.247
	Listing port of PC	12129

First, fill in the APN address on router.

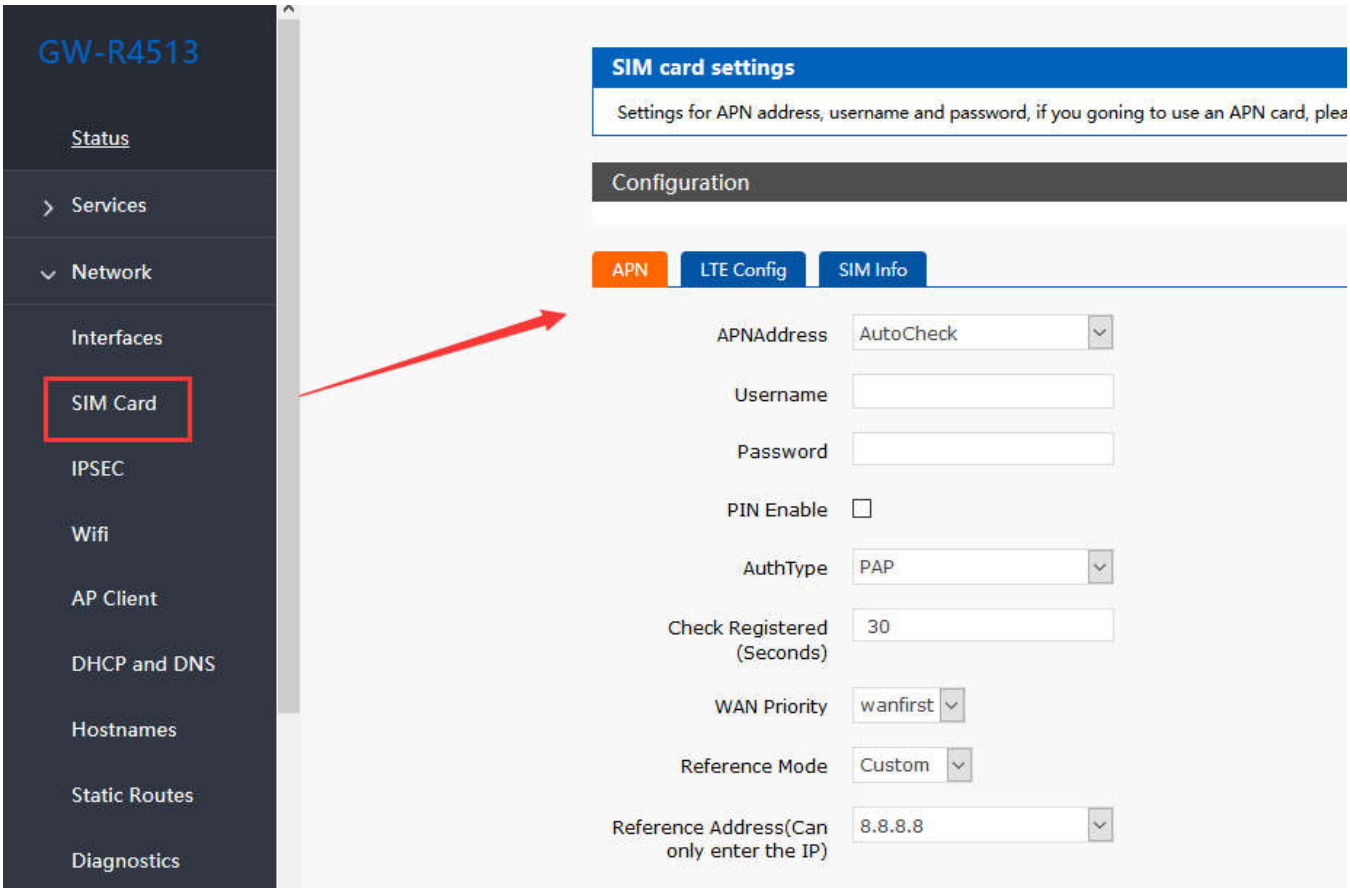


Figure55 4G port forward setting1

Then, add the port forward.

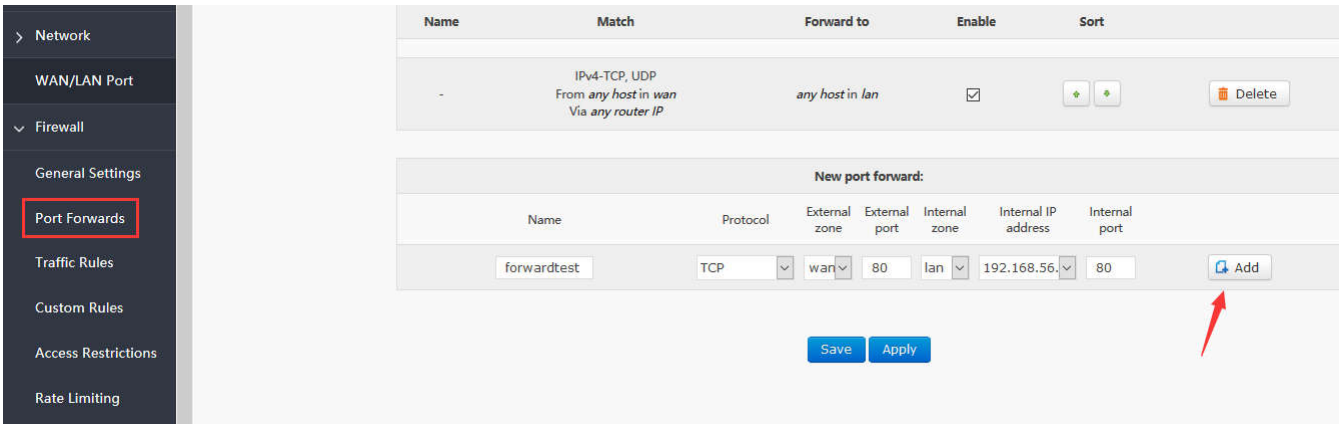


Figure56 4G port forward setting2

After setup all parameters, restart the router.

3.4.11.3.2. 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.

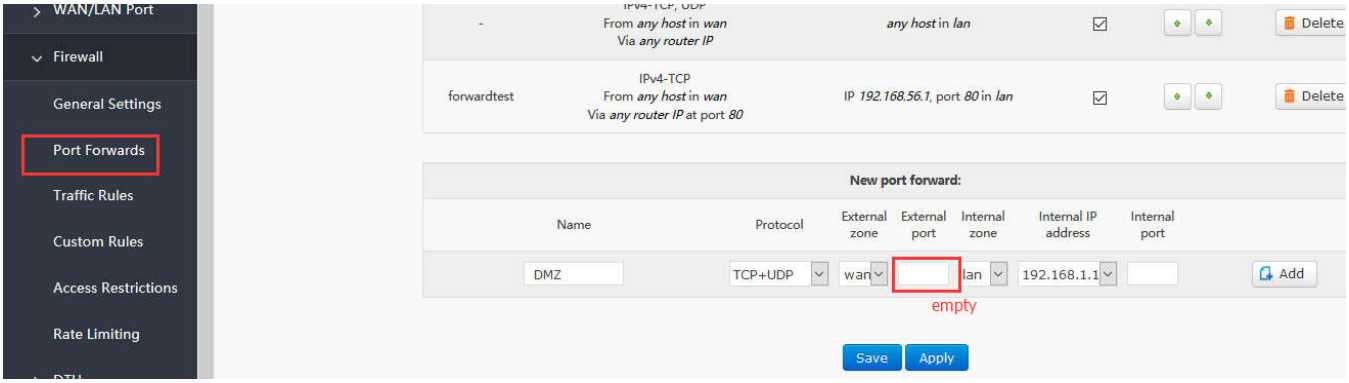


Figure57 DMZ setting1

Then add and save.

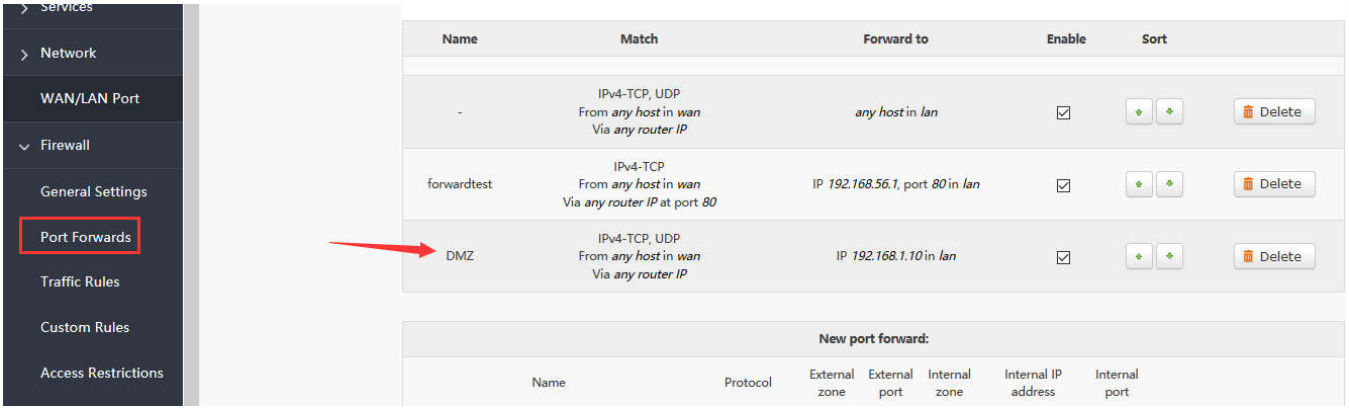


Figure58 DMZ setting2

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.

3.4.12. 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. This function is turned off by default

3.4.12.1. Domain Blacklist

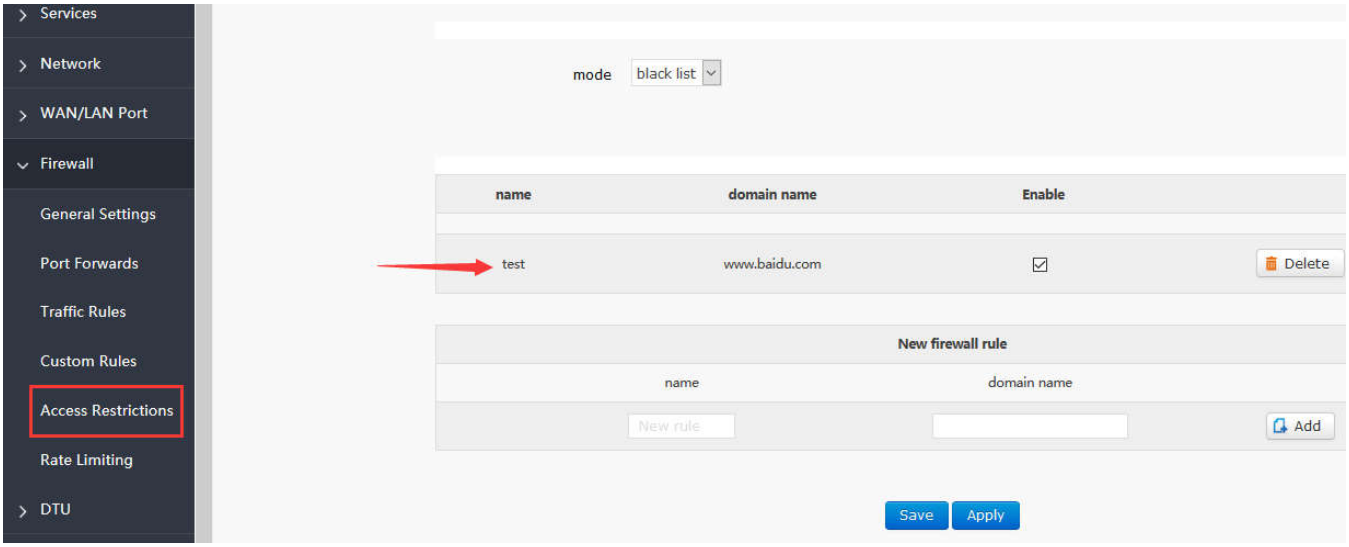


Figure59 blacklist

3.4.12.2. Whitelist

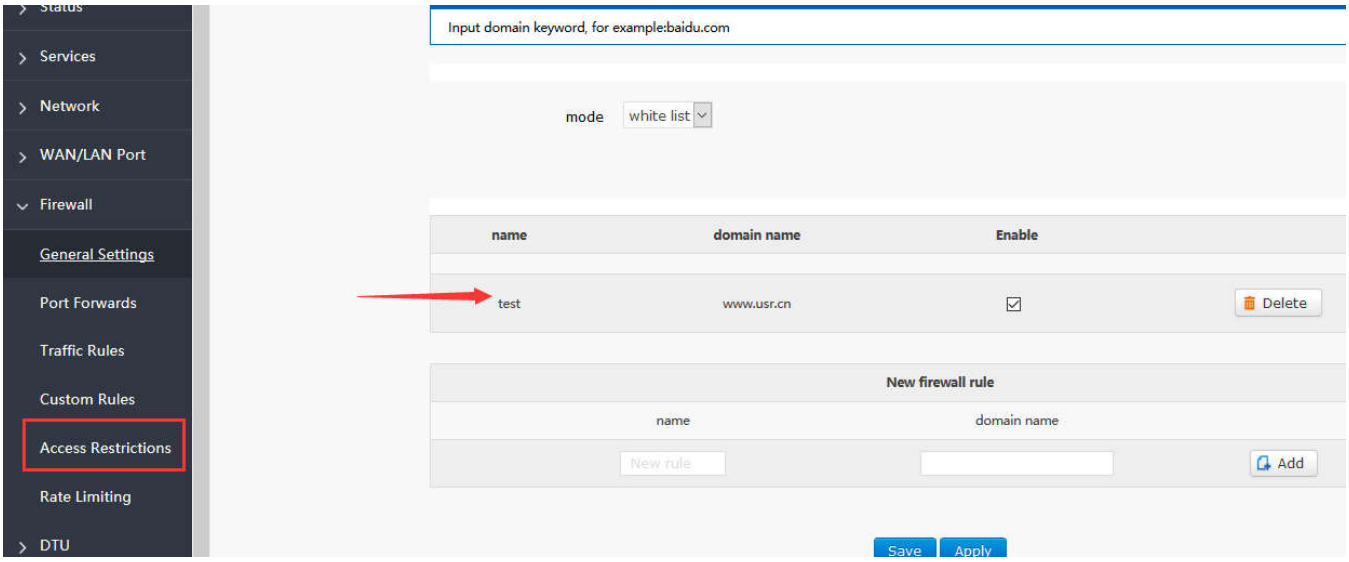


Figure60 whitelist

3.4.13. 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.

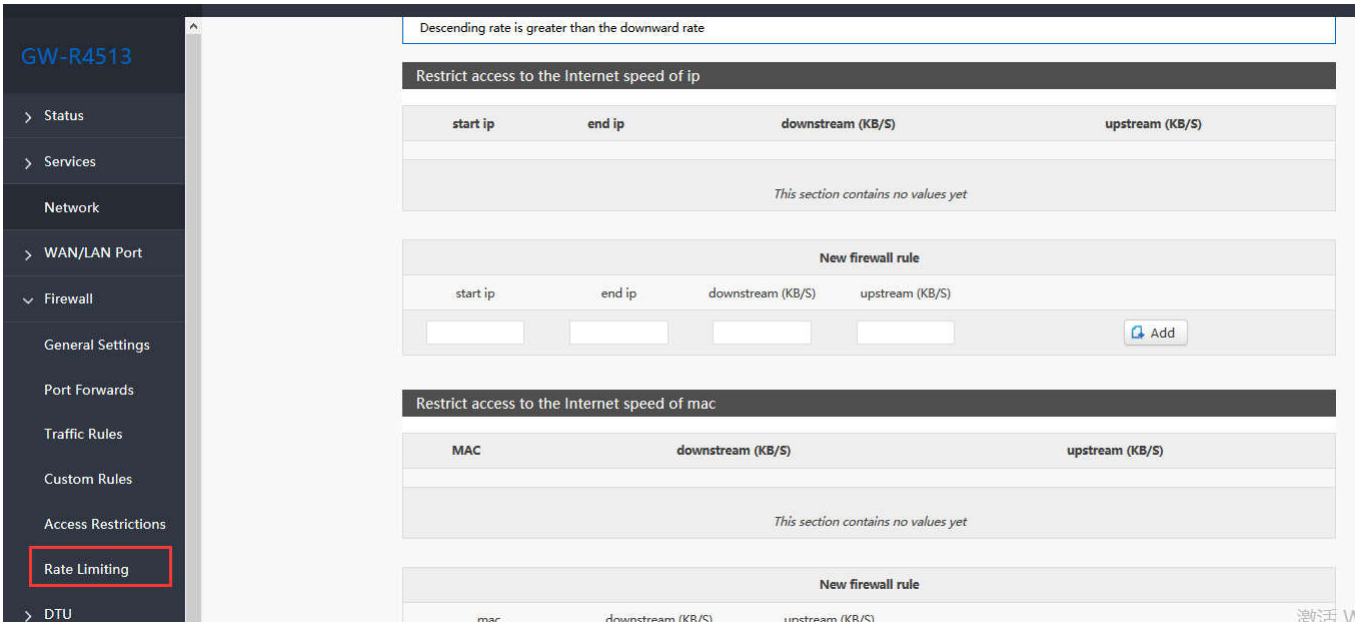


Figure61 rate limiting

4. DTU Function

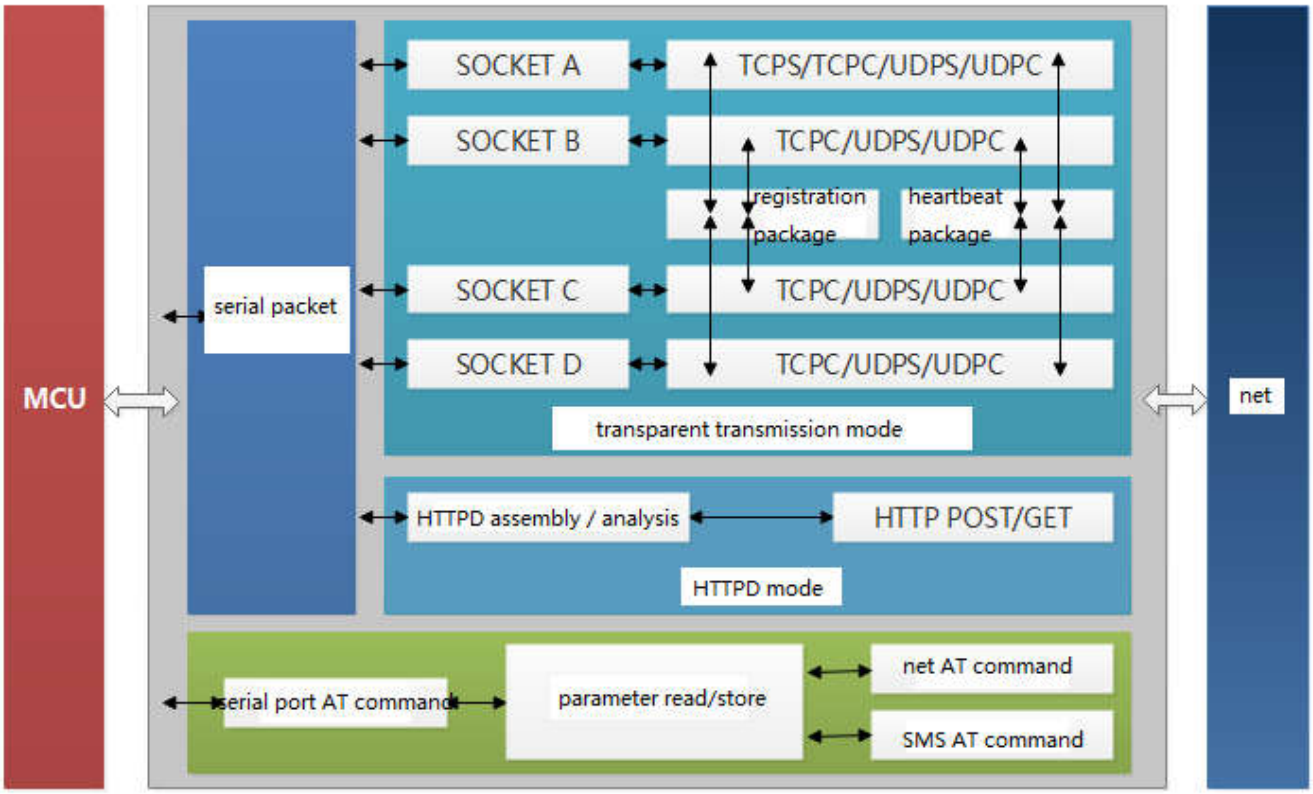


Figure62 DTU function

4.1. Work Mode

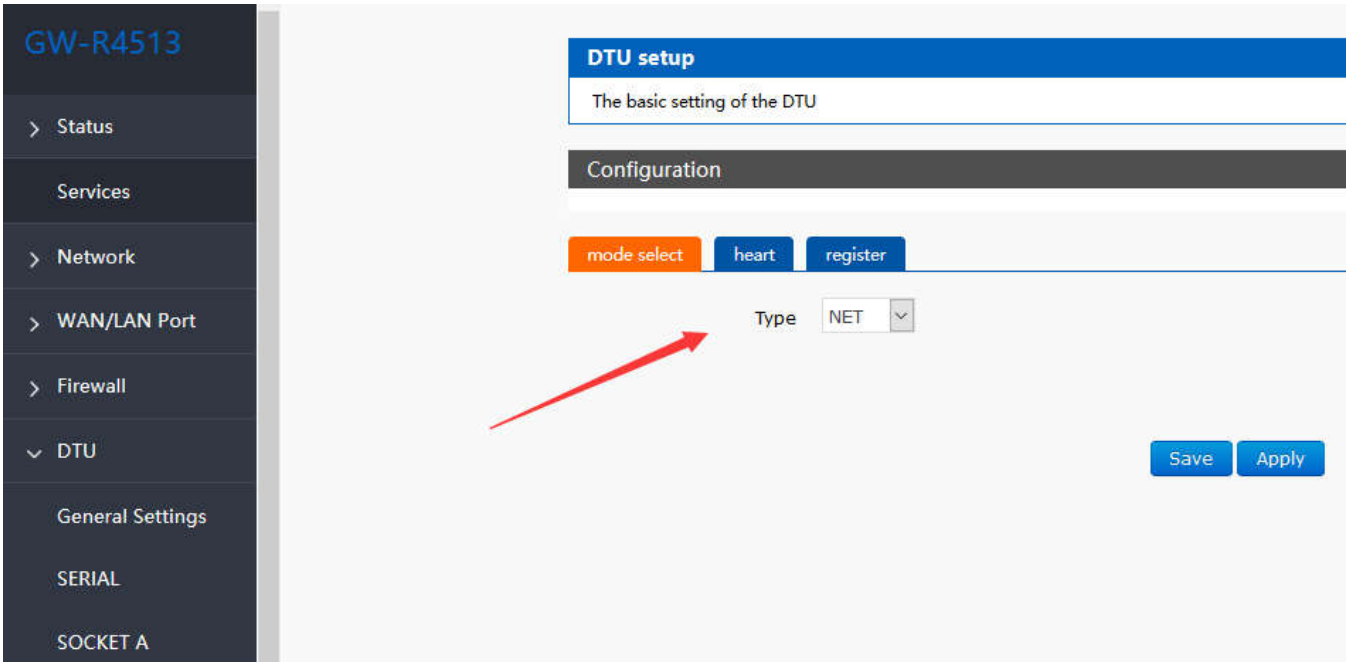


Figure63 mode select

4.1.1.Net Transparent Transmission Mode

4.1.1.1. Mode Declaration

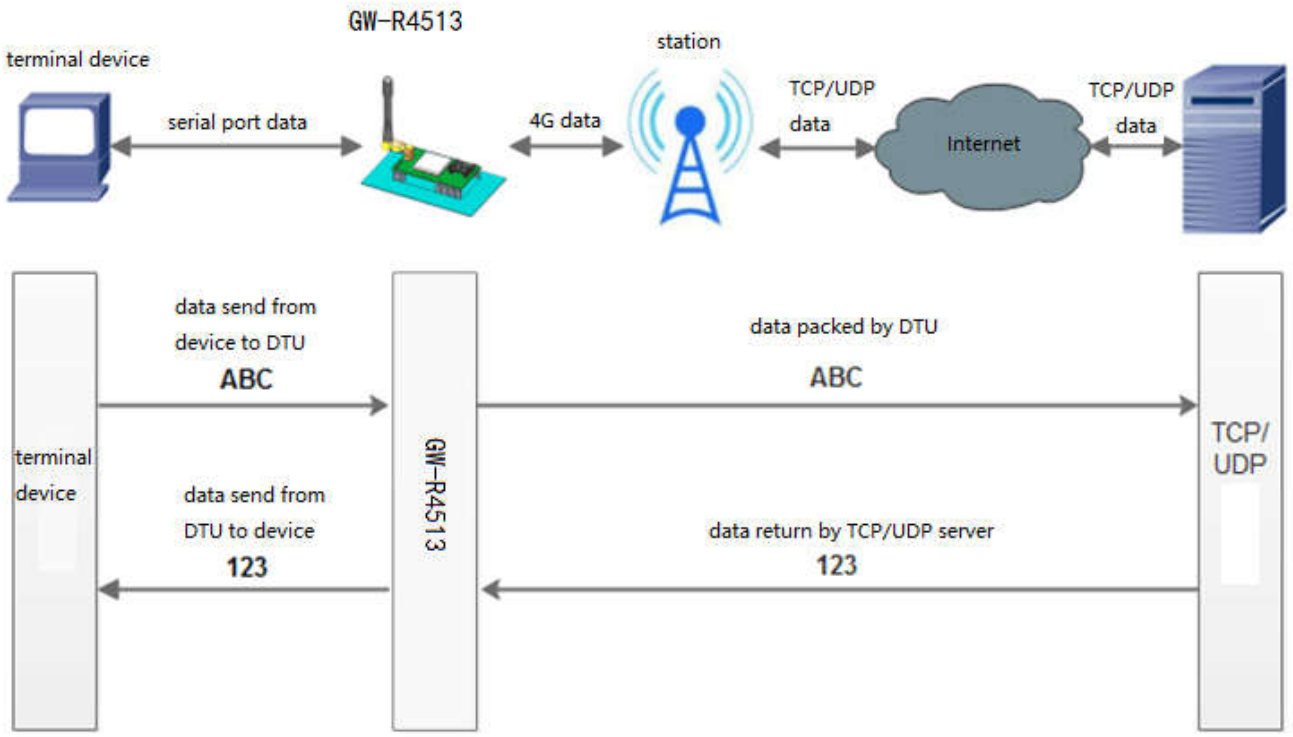


Figure64 net transparent transmission mode

GW-R4513 support 4 socket connection: socket A, socket B, socket C, socket D, they are independent of each other.

Socket A support: TCP Server、TCP Client、UDP Server、UDP Client

Socket B/C/D support TCP Client、UDP Server、UDP Client

The AT commands of setting:

1. Set the work mode :net transparent
   AT+WKMOD=NET
2. Enable socket A
   AT+SOCKAEN=ON
3. Setting socket A work at TCP Client mode
   AT+SOCKA=TCPC, test.usr.cn,2317
4. Restart the module
   AT+Z

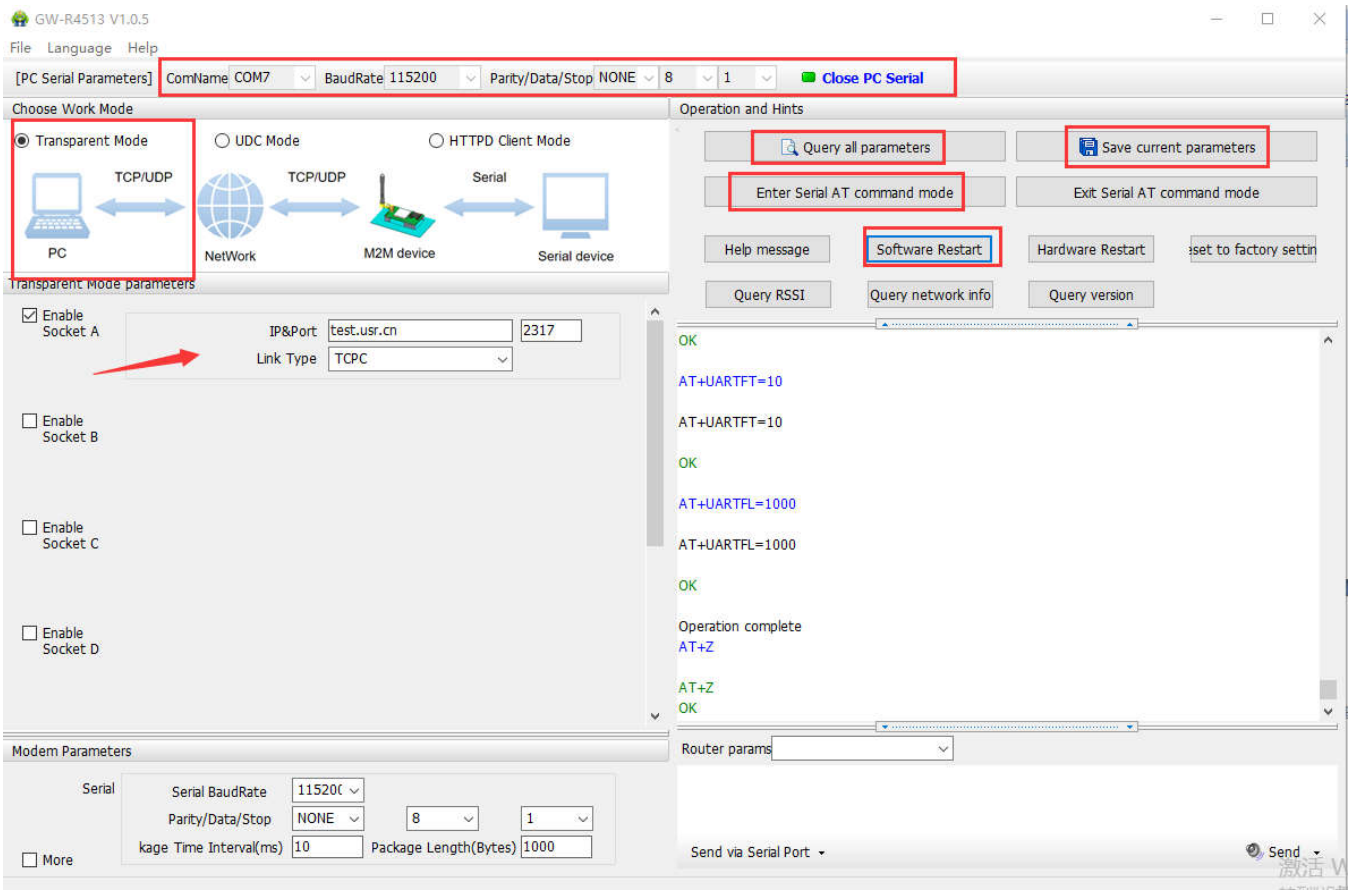


Figure65 setup software

4.1.2. HTTPD Mode

4.1.2.1. Mode Declaration

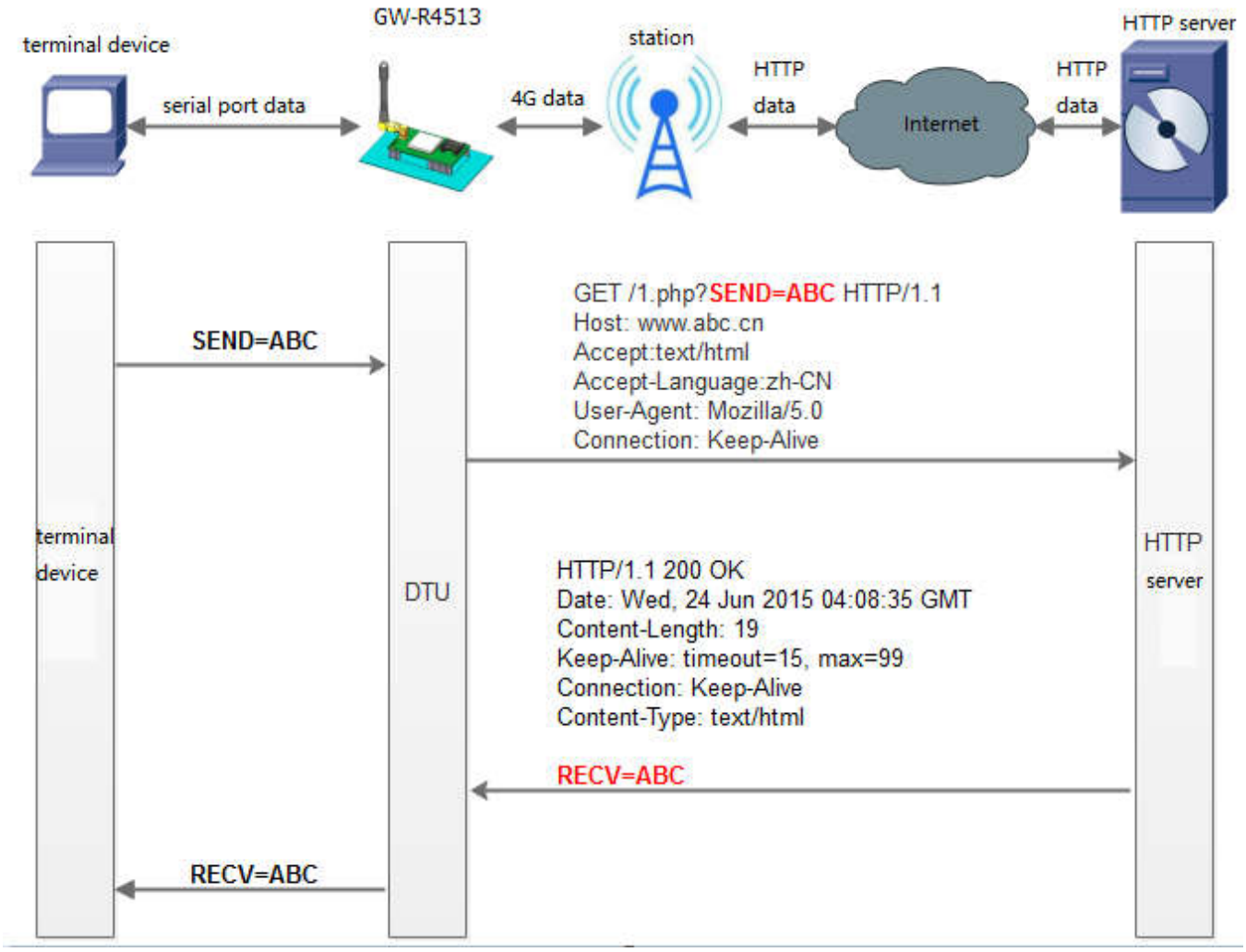


Figure66 HTTPD Mode

The AT commands of setting:

1. Set the work mode : HTTPD
   AT+WKMOD=HTTPD
2. Set the type of request:
   AT+HTPTP=GET
3. Set the URL
   AT+HTPURL=/1.php[3F]
4. Set the server
   AT+HTPSV=test.usr.cn,80
5. Set the head of HTTP
   AT+HTPHD=Connection: close[0D][0A]
6. Set the overtime of request

AT+HTPTO=10

7. Set whether to filter information back to head

   AT+HTPFLT=ON

8. Restart the module

   AT+Z

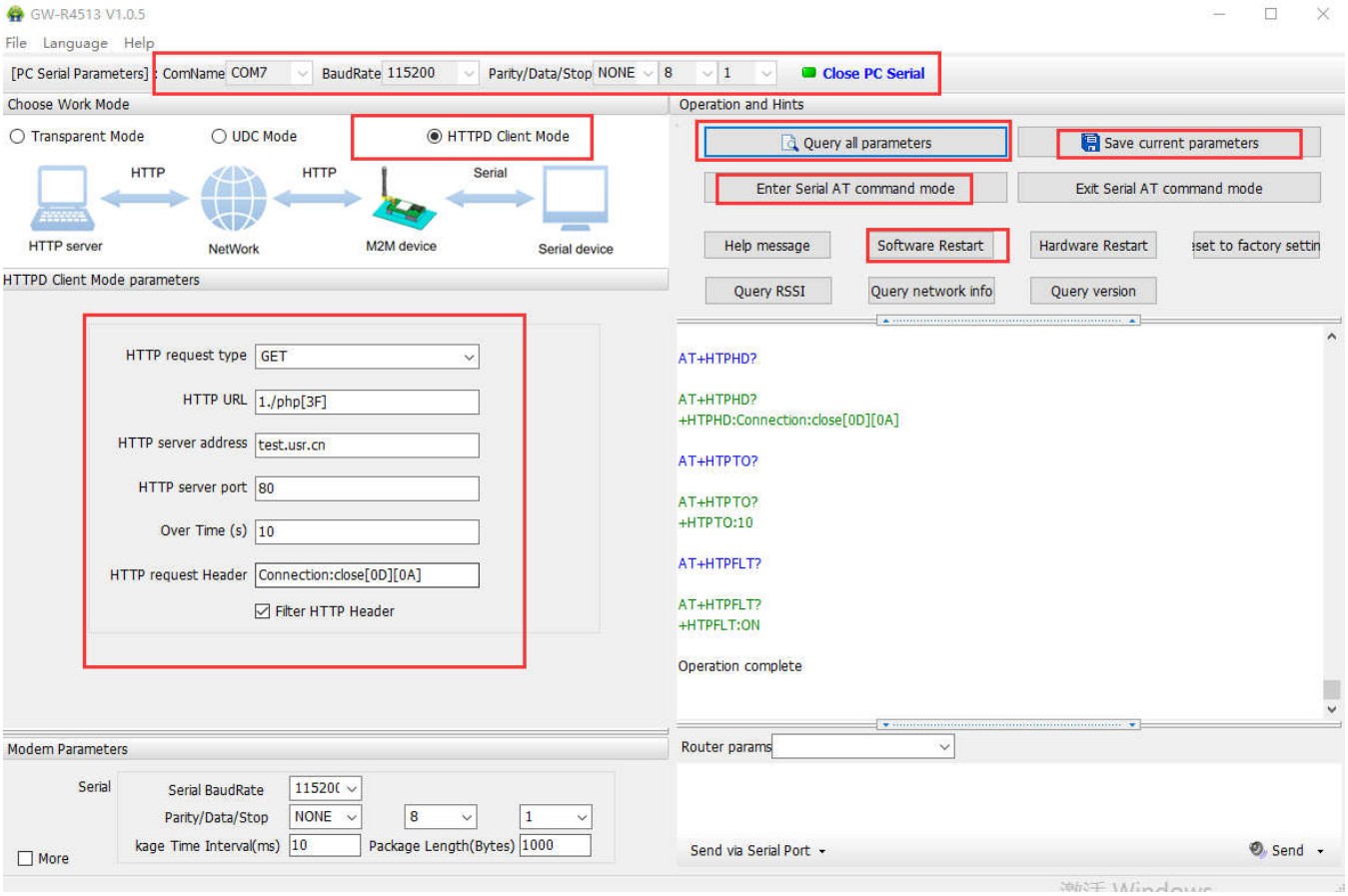


Figure67 setting software

4.1.3. UDC Mode

4.1.3.1. Mode Declaration

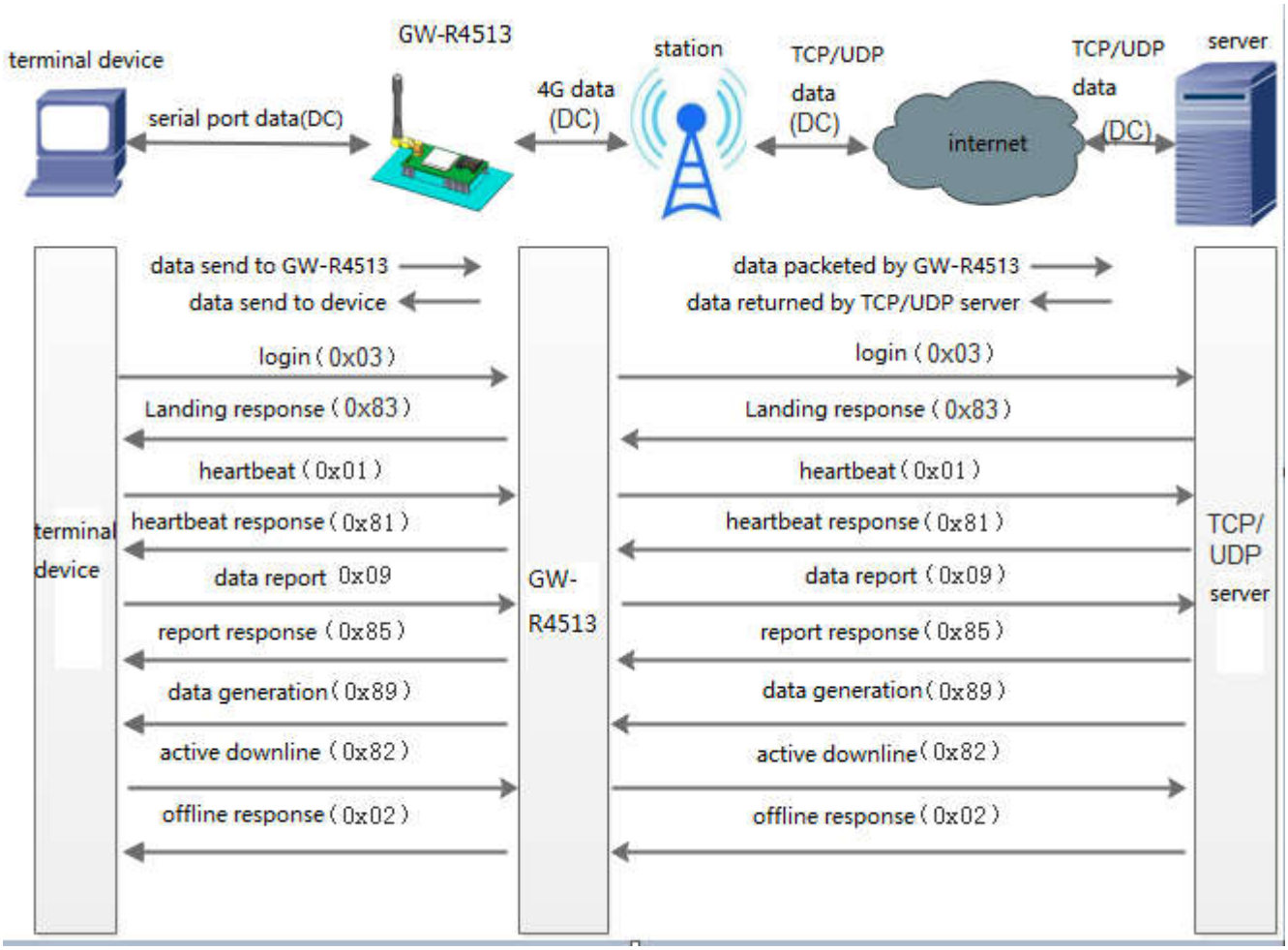


Figure68 UDC Mode

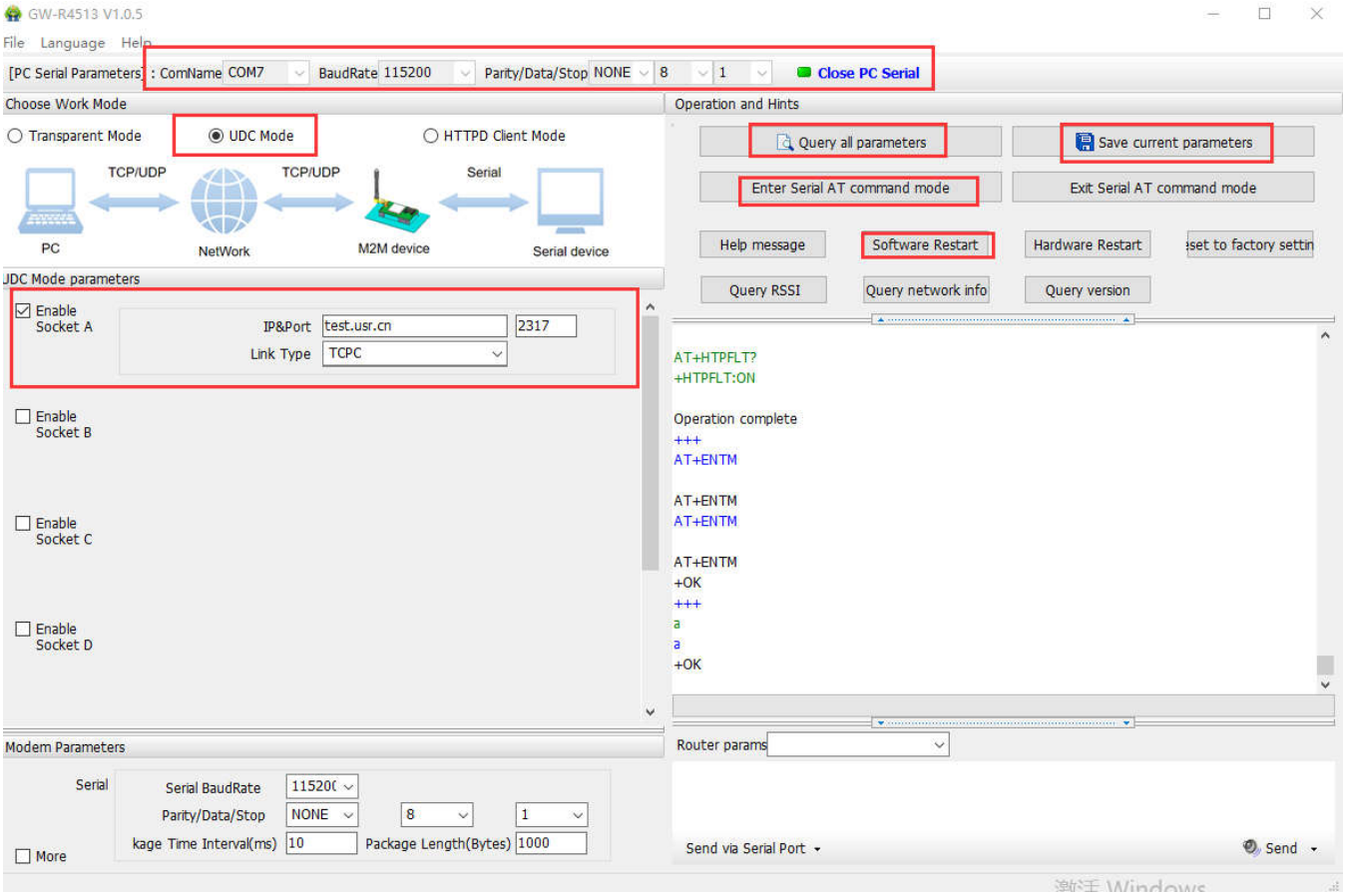


Figure69 setting software

The AT commands for setting GW-R4513:

1. Set the work mode: UDC
   AT+WKMOD=UDC
2. Enable socket A
   AT+SOCKAEN=ON
3. Set device work as TCP server, the server address is test.usr.cn, the port is 2317
   AT+SOCKA=TCPC,test.usr.cn,2317
4. Enable heartbeat package
   AT+HEARTEN=ON
5. Set the time interval
   AT+HEARTTM=30
6. Enable registration package
   AT+REGEN=ON
7. Set the registration mode: UDC
   AT+WKMOD=UDC
8. Set the ID of UDC device
   AT+UDCID=303030303030303030303031
   The ID parameter here is hex form.
9. Send save command
   AT+S

4.2. Serial Port

4.2.1. Basic Parameters

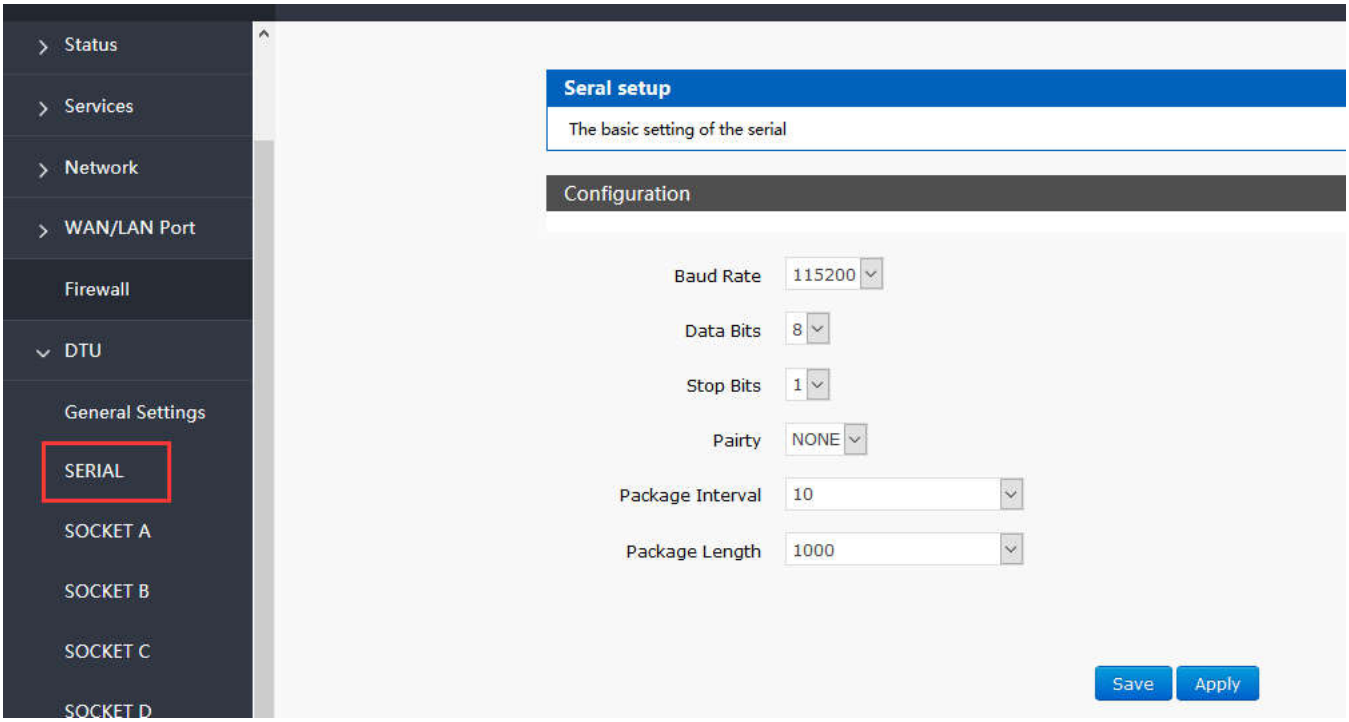


Figure70 serial port setting

Table10 serial port parameter

	Parameter
Baud rate	2400，4800，9600，19200，38400，57600，115200，230400
Data bit	8
Stop bit	1,2
Check bit	NONE
	EVEN
	ODD
	MARK
485	NFC
	485 communication

4.2.2. Frame Forming Mechanism

4.2.2.1. Time Triggered Mode

When receiving data from UART, GW-R4513 continuously checks the interval between 2 adjacent bytes. If the interval

time is greater than or equal to a certain "time threshold", a frame is considered to end, otherwise data is received until it is greater than or equal to the packing length (default is 1000 bytes).The range can be set to be 10ms~60000ms. The default time is 10ms.

This parameter can be set accodeing to the AT command, AT+UARTFT=10.

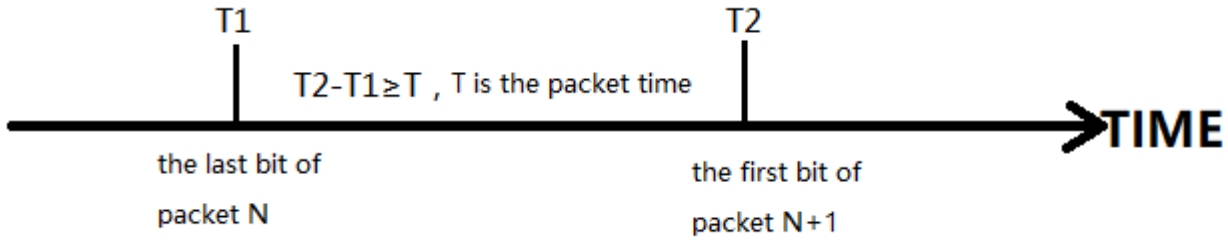


Figure71 time triggered mode

4.2.2.2. Length Triggered Mode

When receiving data from UART, GW-R4513 will check the number of bytes received continuously. If the number of bytes received reaches a certain "length threshold", it is considered that the end of a frame. The range of settings is 1~4096. Factory default 1000.

This parameter can be set accodeing to the AT command, AT+UARTFL=<length>

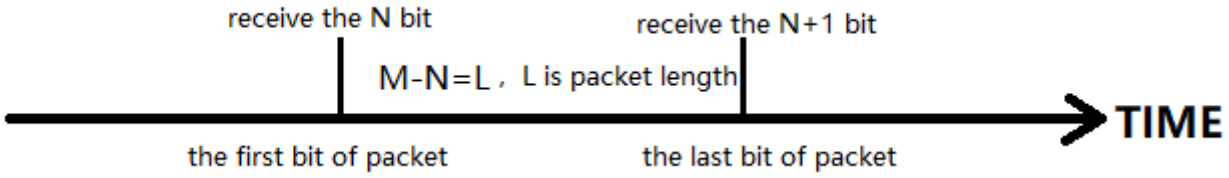


Figure72 length triggered mode

4.3. Characteristic Functions

4.3.1. Registration Package

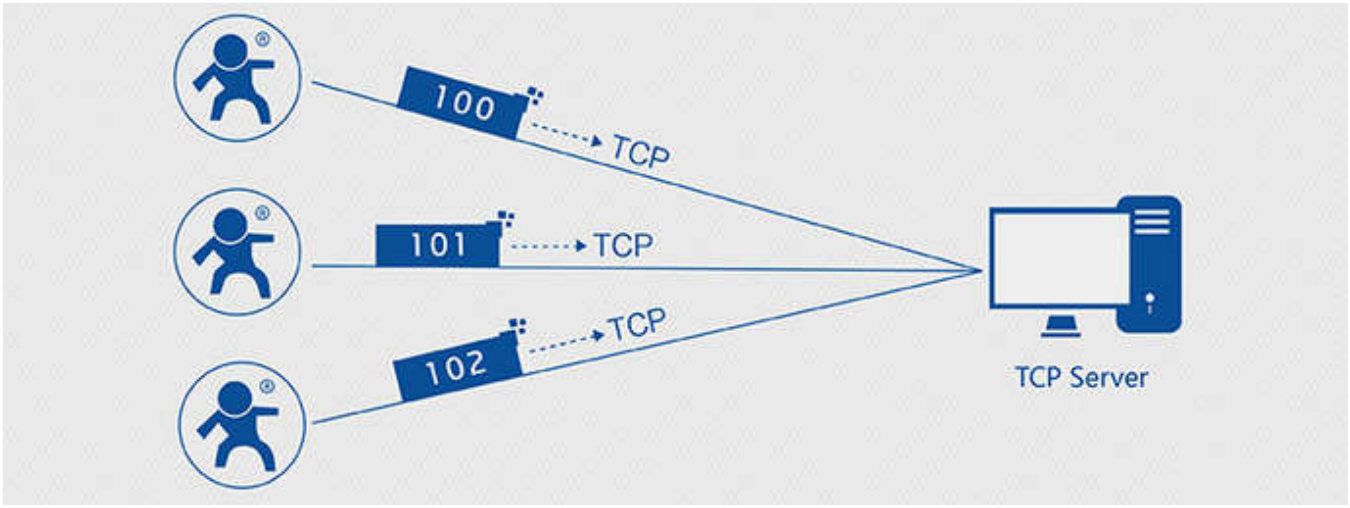


Figure73 registration package function

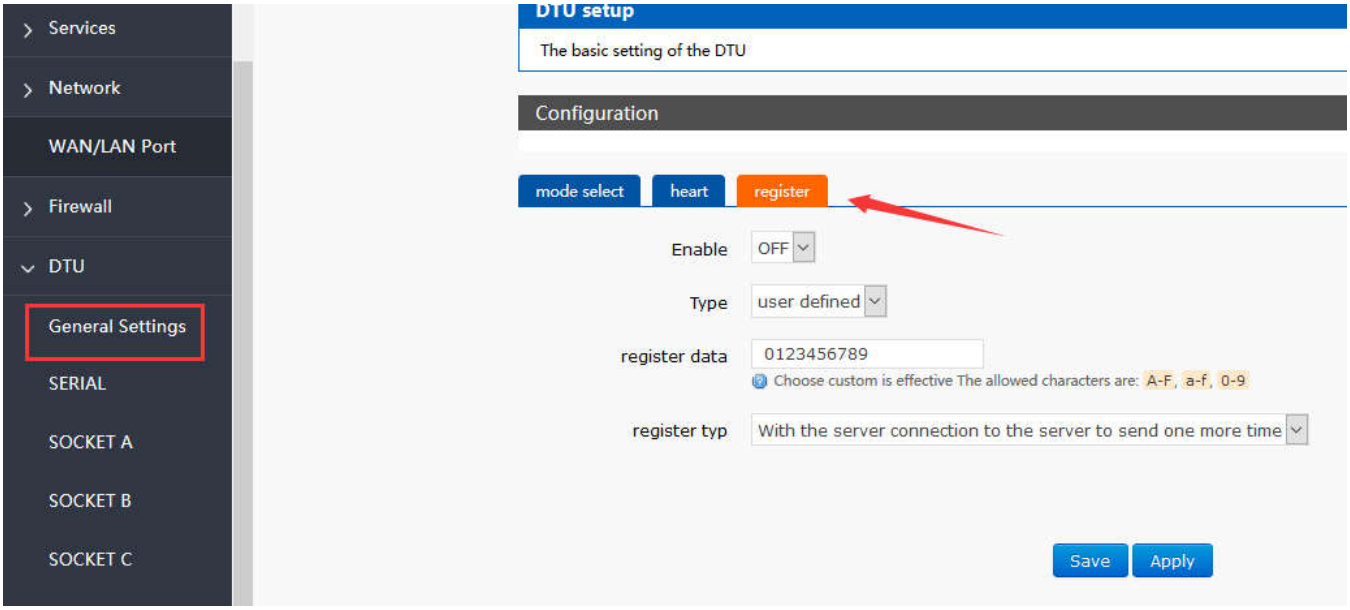


Figure74 registration package setting

When work at the net transparent transmission mode, the user can choose to send register package from device to server. The registration package is designed to enable the server to identify the data source device, or as a password to obtain authorization for the functions. Registered packets can be sent when a connection between the device and the server is established, or they can be spliced together at the front of each packet as a data package. The data of the registration package can be ICCID code, IMEI code, or custom registration data.

Table11 AT commands

Command	Function	Default parameter
AT+ REGEN	Query/set enable register function	OFF

AT+ REGTP	Query/set the type of register content	USER
AT+ REGDT	Query/set the info of custom register	0123456789
AT+ REGSND	Query/set register packet sending mode	DATA

AT commands

1. Enable register package
   AT+REGEN=ON
2. Set the register type is custom define
   AT+REGTP=USER
3. Set the data of register package
   AT+REGDT=123456789
4. Setting up the registration package is to send registered data as the head of each packet data
   AT+REGSND=DATA
5. Restart
   AT+Z

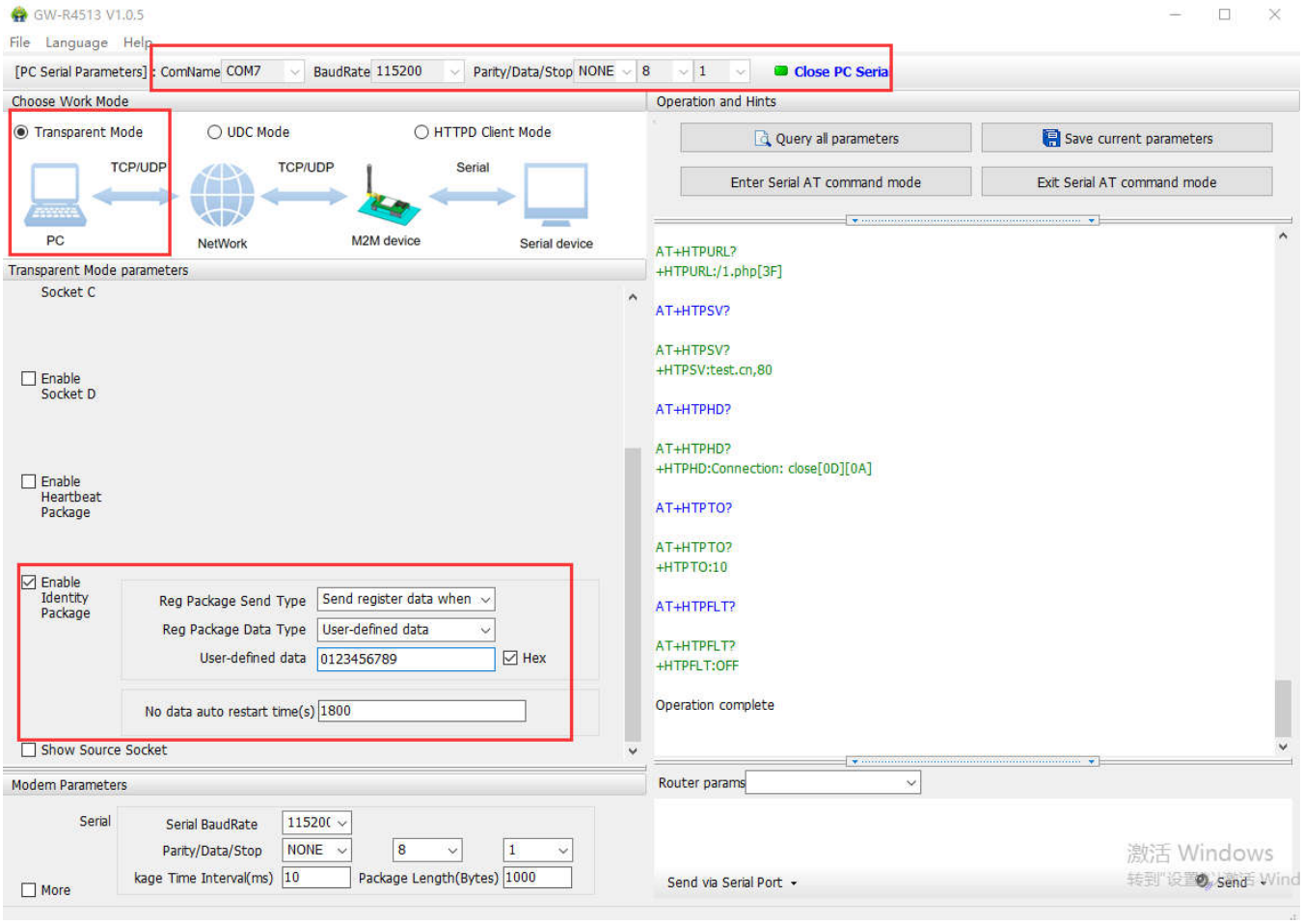


Figure75 setting software

4.3.2. Heartbeat Package

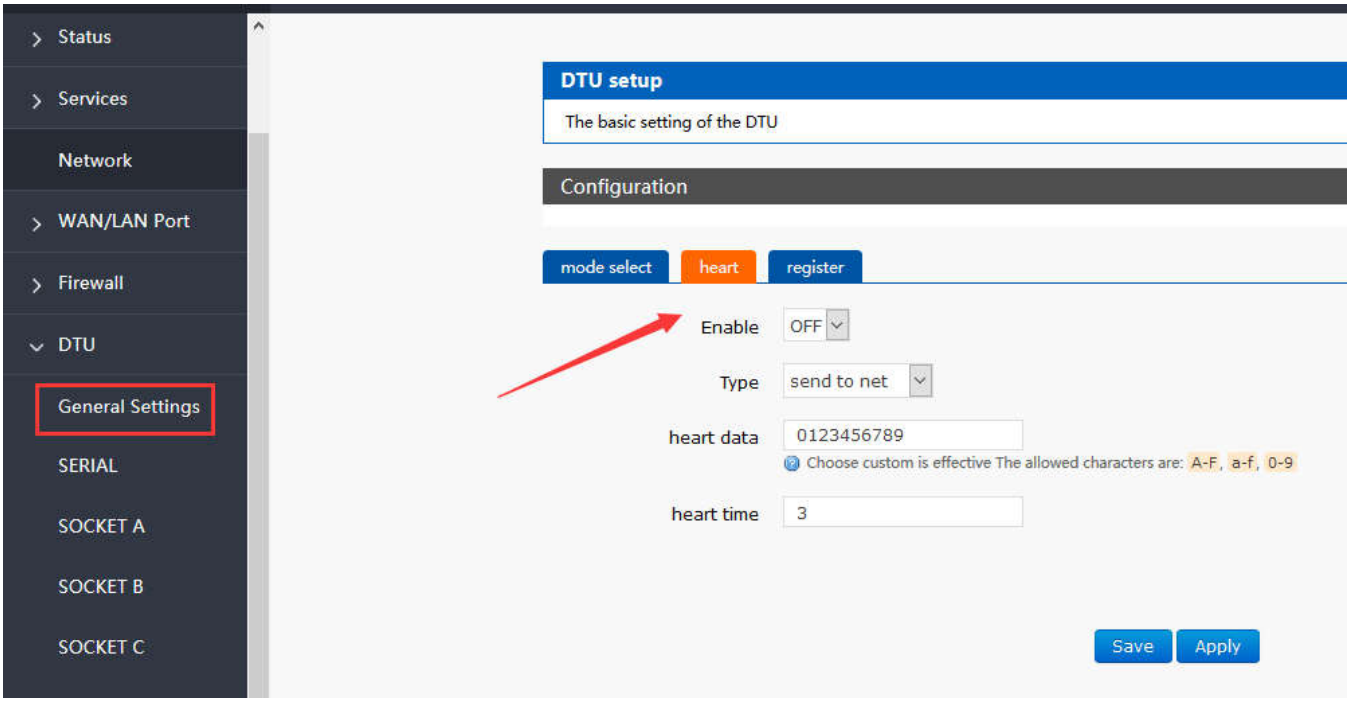


Figure76 heartbeat package setting

When work at net transparent transmission mode, the user can choose to send heartbeat packets to DTU. Heartbeat packets can be sent to the server side of the network, or to the device port of the serial port.

The main purpose of sending to the network side is to maintain the connection with the server.

In order to reduce communication flow, users can choose to send heartbeat packets (query instructions) to serial device instead of sending query instructions from server.

Table12 AT commands

Command	Function	Default parameter
AT+ HEARTEN	Query/set enable heartbeat package	OFF
AT+ HEARTDT	Query/set data of heartbeat package	0123456789
AT+ HEARSND	Query/set heartbeat sending type	NET
AT+ HEARTTM	Query/set transmission interval	30

AT commands

1. Enable heartbeat package:
   AT+HEARTEN=ON
2. Set the heartbeat data
   AT+HEARTDT=123456789
3. Set the heartbeat send to net port
   AT+HEARTTP=NET
4. Set the transmission interval
   AT+HEARTTM=30
5. Restart
   AT+Z

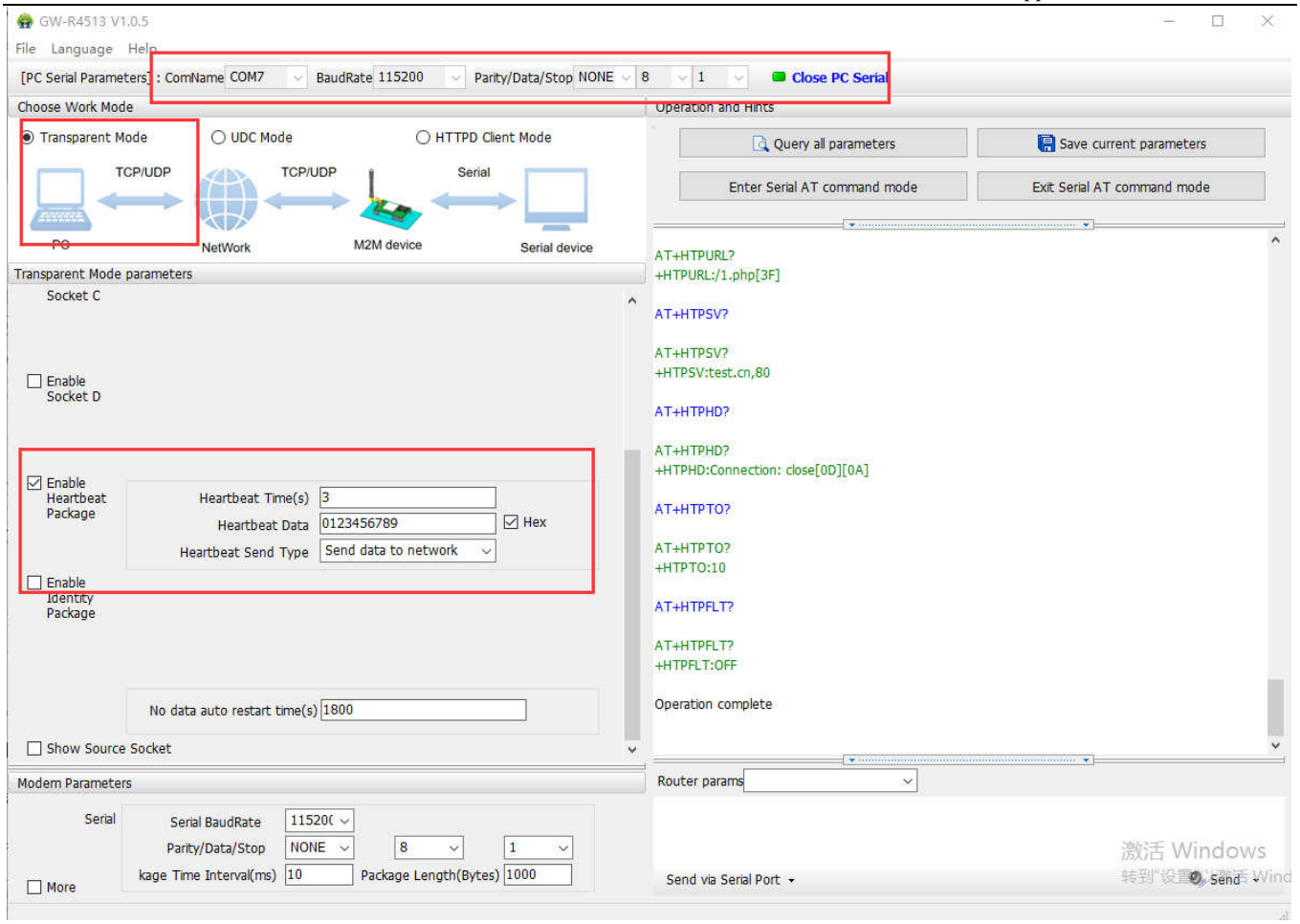


Figure77 setting software

4.3.3. USR-Cloud

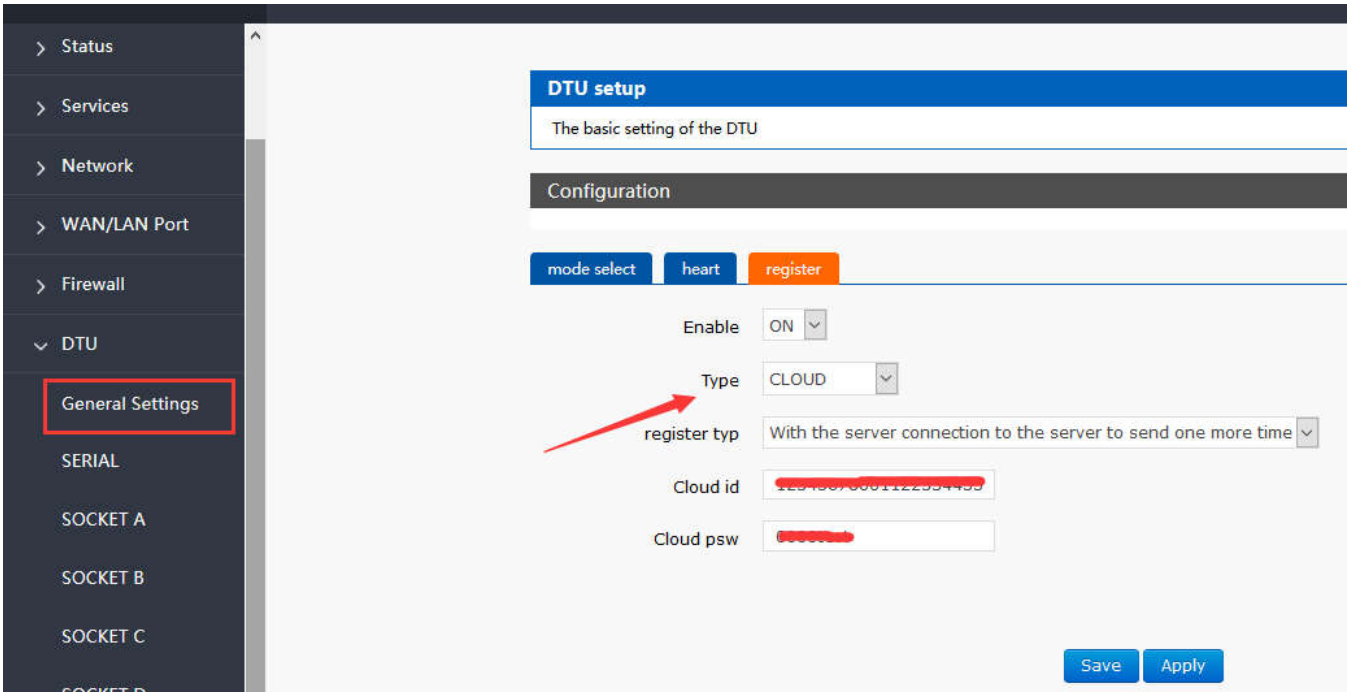


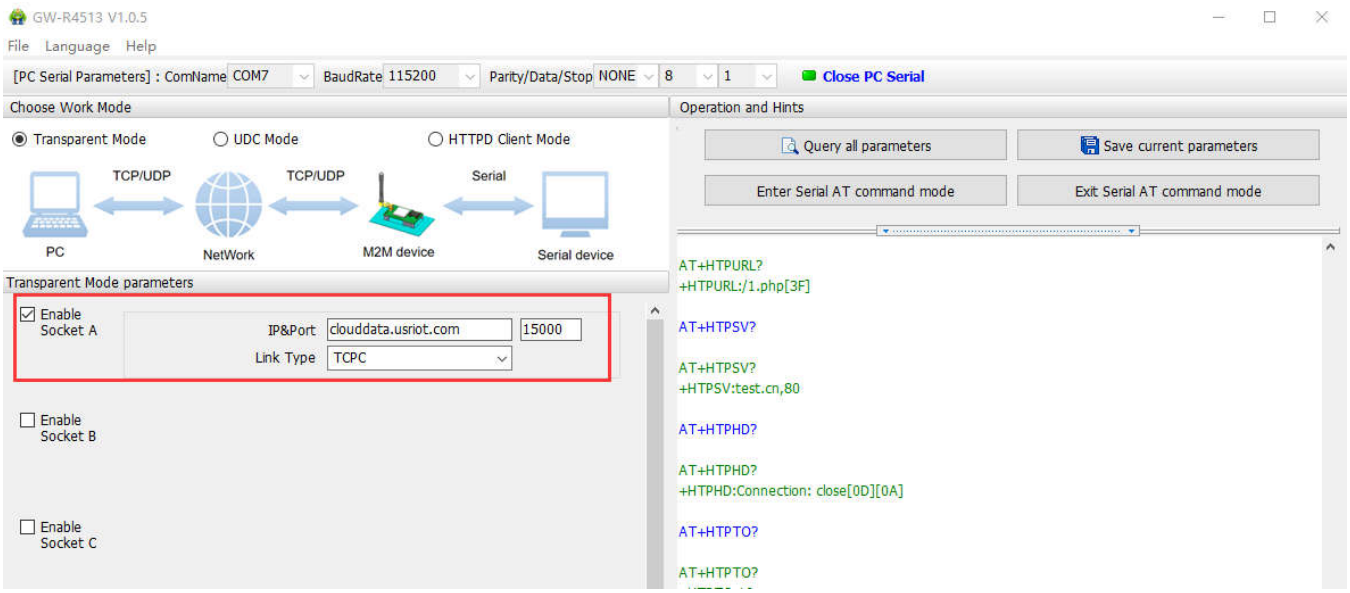
Figure78 USR-Cloud

Note: this function work only when socket A work at TCP Client mode.

Table13 AT commands

Command	Function	Default parameter
AT+ CLOUD	Set the cloud ID and password	
AT+ REGEN	Query/set enable register package	OFF
AT+ REGTP	Query/set data of register package	USER
AT+ REGSND	Query/set register sending type	DATA

1. Enable register function
   AT+REGEN=ON
2. Set the type is USR-Cloud
   AT+REGTP=CLOUD
3. Set the parameter of socket
   AT+SOCKA=TCPC,clouddata.usriot.com,15000
4. Set the sending type
   AT+REGSND=LINK
5. Set the cloud ID and password
   AT+CLOUD=xxxxxxxxxxxxx,xxxxxxx
6. Restart
   AT+Z



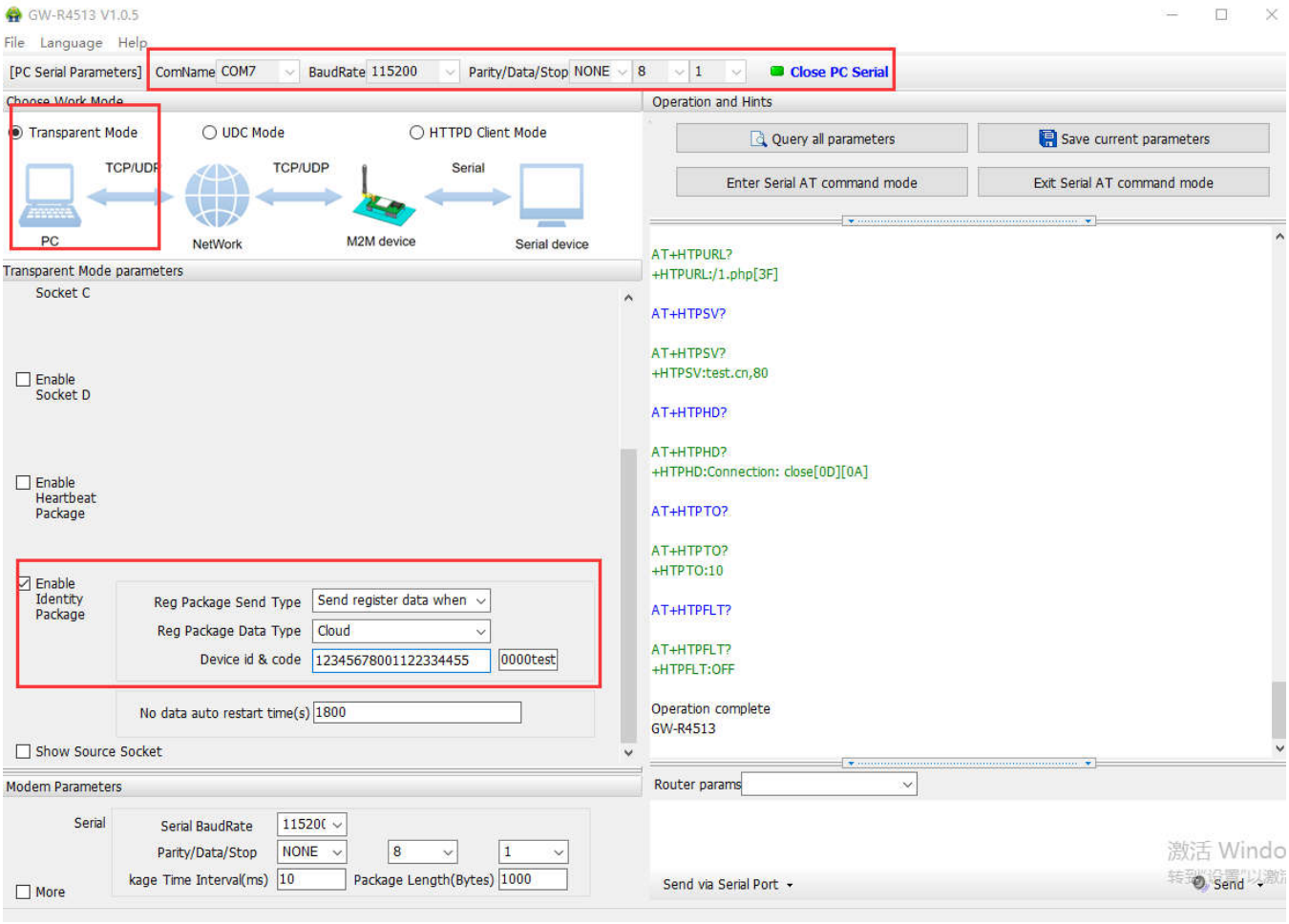


Figure79 setting software

5. Webpage Sitting

Connect PC and GW-R4513 with LAN port, or connect WLAN wireless, then login the webpage of setting.

Table14 GW-R4513 default parameter

Parameter	Default setting
SSID	GW-R4513-XXXX
IP of LAN port	192.168.1.1
User name	root
Password	root
WIFI key	12345678

Make PC join the WIFI GW-R4513-XXXX, enter 192.168.1.1 ,the user name and password both are root.

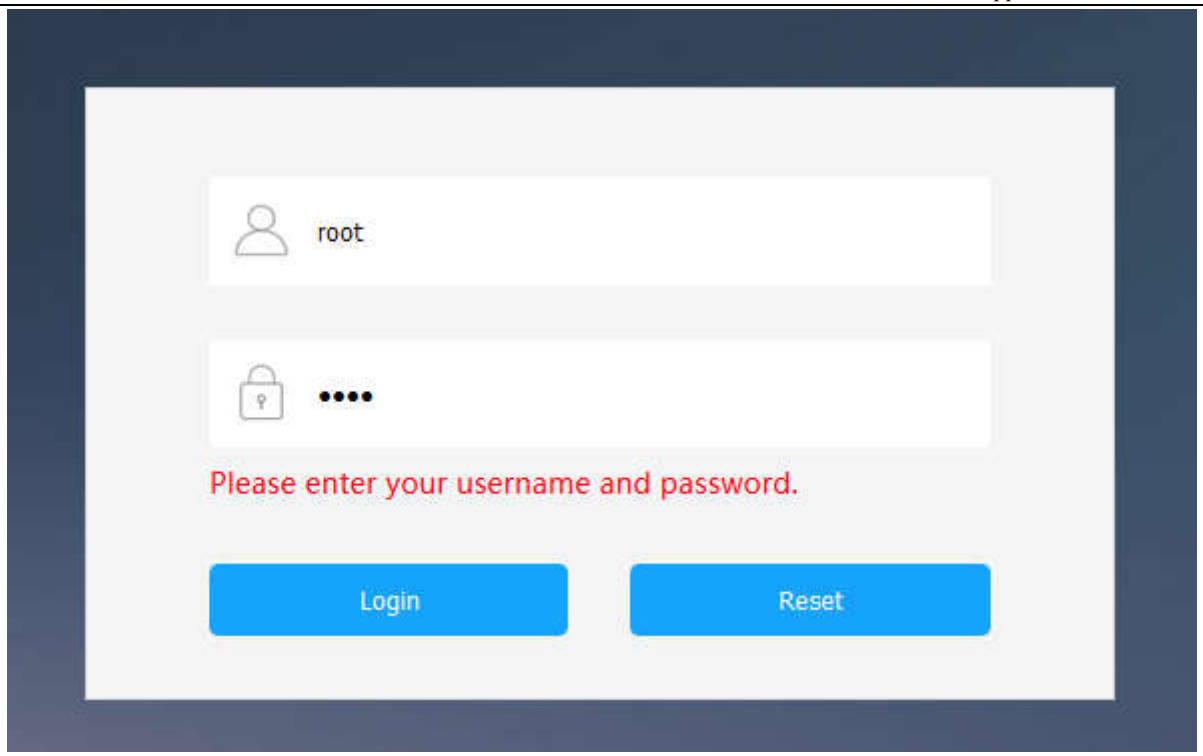


Figure80 login webpage

5.1. Web Function

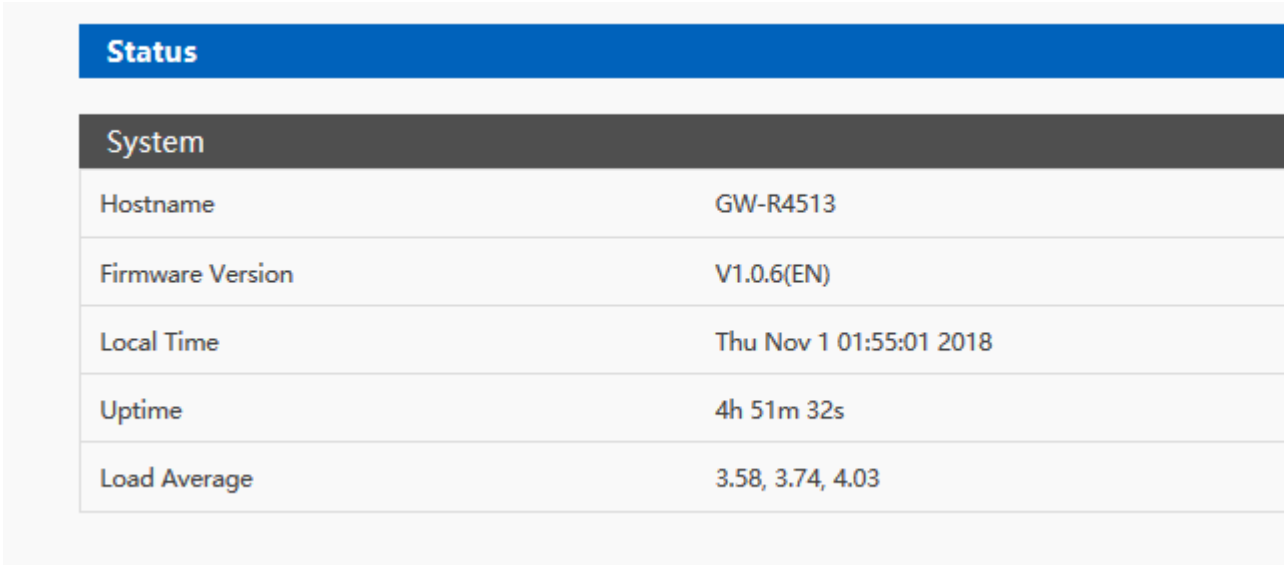


Figure81 status

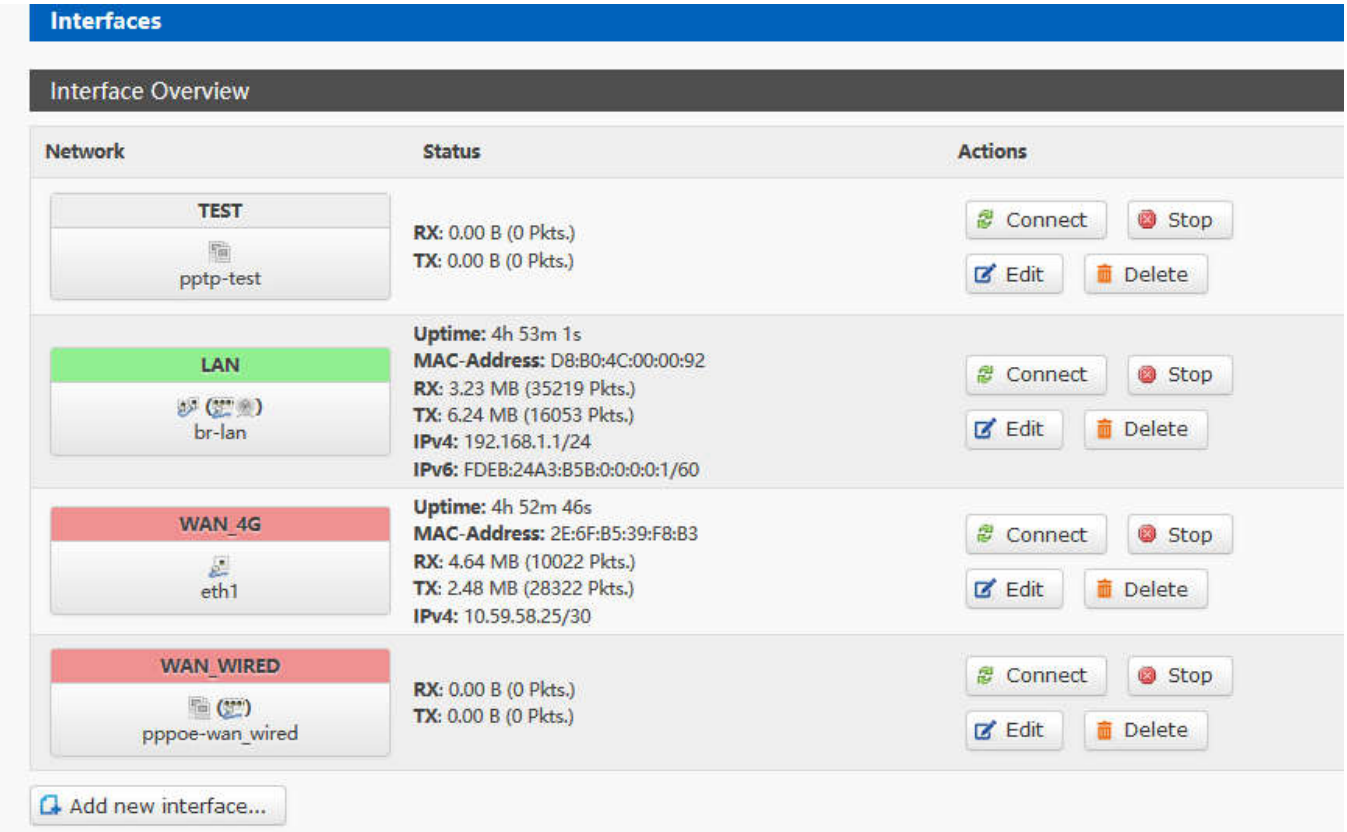


Figure82 interface overview

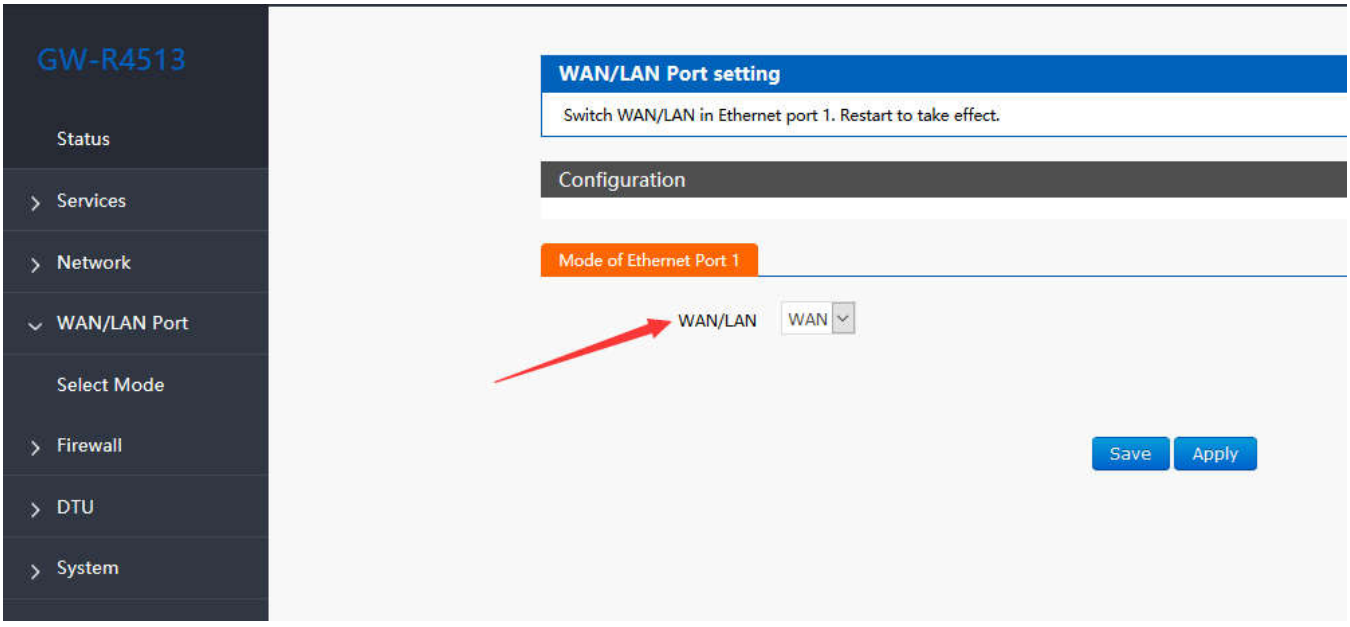


Figure83 mode of Ethernet port

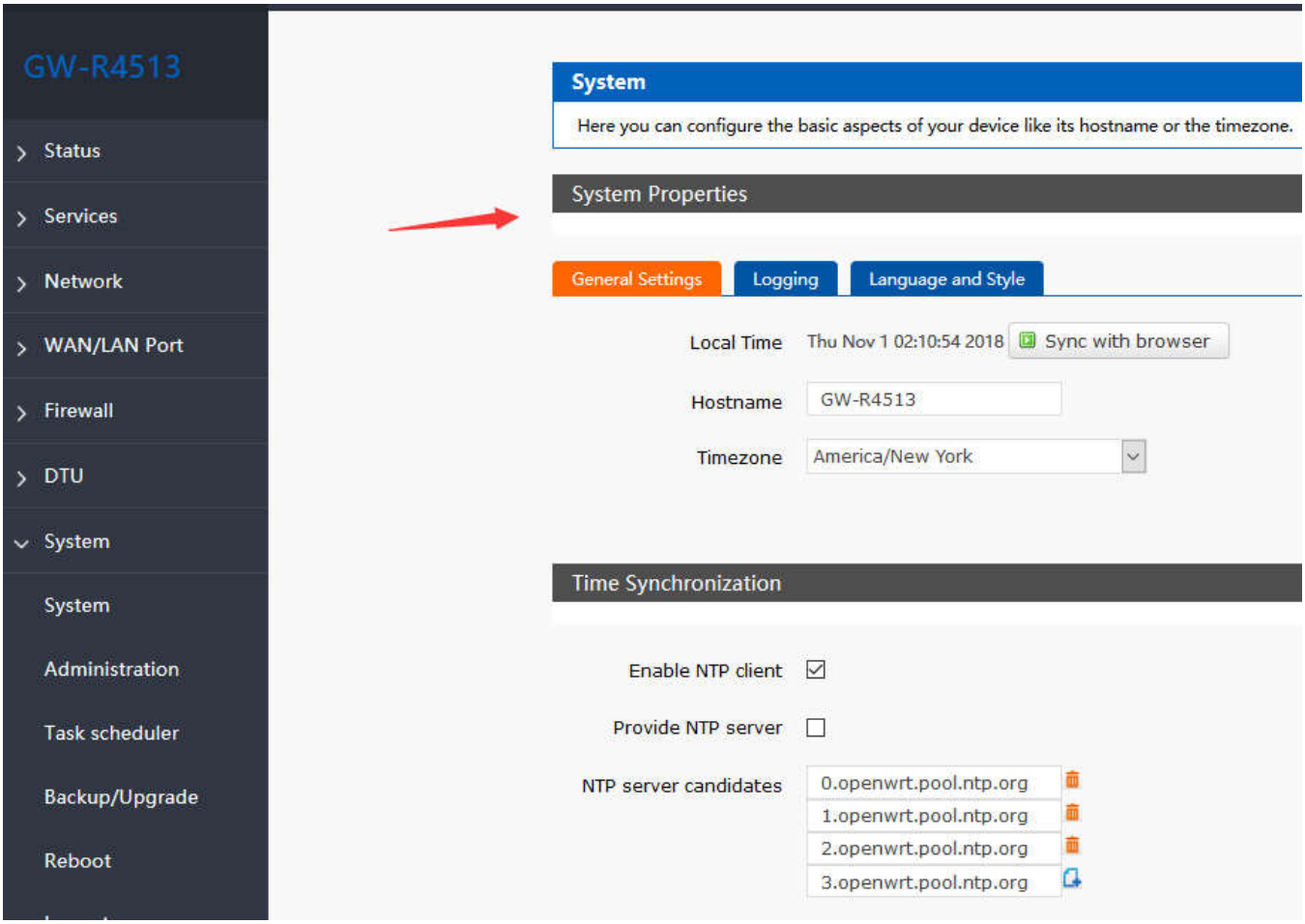


Figure84 system properties

6. AT Commands

Table 15 AT commands

NO.	Command	Function
Version		
1	VER	Query version information
2	MAC	Query the MAC
3	ICCID	Query ICCID code
4	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
9	AT+NETMODE	Query current network mode
System		
10	AT+UPTIME	Query running time

11	AT+WWAN	Query the IP of device
12	AT+LANN	Query/set the LAN of IP
13	AT+WEBU	Query/set the webpage account and password
14	AT+PLANG	Query/set the default language
15	AT+CLEAR	Recover to factory setting
16	AT+Z	Restart
17	AT+DHCPEN	Open/close DHCP Server
Remote monitor and upgrade		
18	AT+UPDATE	Query/set parameter of remote upgrade
19	AT+MONITOR	Query/set parameter of remote monitor
20	AT+HEARTPKT	Query/set parameter of remote heartbeat
System shell command		
21	AT+LINUXCMP	Execute system shell command
Serial command		
22	UART	Query/set parameter of serial port
23	UARTFT	Query/set serial port packing interval
24	UARTFL	Query/set the package length of serial port
Net command		
25	SOCKA	Query / setup socket A parameter
26	SOCKB	Query / setup socket B parameter
27	SOCKC	Query / setup socket C parameter
28	SOCKD	Query / setup socket D parameter
29	SOCKAEN	Query / setup whether to enable socket A
30	SOCKBEN	Query / setup whether to enable socket B
31	SOCKCEN	Query / setup whether to enable socket C
32	SOCKDEN	Query / setup whether to enable socket D
33	SOCKALK	Query socket A connection state
34	SOCKBLK	Query socket B connection state
35	SOCKCLK	Query socket C connection state
36	SOCKDLK	Query socket D connection state
37	SOCKIND	Query / setting enable or unable the source of data
Register command		
38	REGEN	Query / set enable registration package
39	REGTP	Query / set register package content type
40	REGDT	Query / set custom registration information
41	REGSND	Query / set register packet sending mode
42	CLOUD	Query/set the parameter of USR-Cloud
Heartbeat command		
43	HEARTEN	Query / settings enable heartbeat package
44	HEARTDT	Query / settings heartbeat data
45	HEARTTP	Query / settings heartbeat packet delivery mode
46	HEARTTM	Query / settings heartbeat packet interval

HTTPD command		
47	HTPTP	Query / setup HTTP operate mode
48	HTPURL	Query/setup URL
49	HTPSV	Query/setup remote IP and port
50	HTPHD	Query/setup head info of HTTP protocol
51	HTPTO	Query/setup the overtime time
52	HTPFLT	Query/setup enable or unable filter head

7. 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: 86-531-88826739/86-531-55507297

8. Disclaimer

This document provide the information of GW-R4513 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 merchantability 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.

9. Update History

Edition	Describe
V1.0.1	2018-04-10 establish