

GW-R4513-E/AU Software Manual

File Version: V1.0.1



Contents

GW-R4513 Software Manual.....	1
1. Product Overview	6
1.1. Product Function	6
2. Basic Function of Router	6
2.1. 4G Interface	8
2.2. LAN Interface	10
2.2.1. DHCP Function	11
2.3. WAN Interface	13
2.4. Wi-Fi Wireless Interface.....	13
2.5. Network Diagnostic Function.....	16
2.6. Host Name and Time Zone	17
2.7. NTP Setting	18
2.8. Password Setting.....	18
2.9. Backup Function	19
2.10. Reset to Default	20
2.11. Indicator Light.....	21
2.12. Firmware Upgrade	22
2.13. Reboot	23
3. Advanced Function	24
3.1. DDNS	24
3.1.1. Supported Services	24
3.1.2. Custom Service	25
3.1.3. Functional Characteristics.....	26
3.2. WiFiDog	26
3.3. APN Setting.....	29
3.3.1. Modify APN.....	29
3.3.2. SIM Card Settings.....	30
3.3.3. SIM Card Information.....	31
3.4. VPN Client(PPTP/L2TP/GRE/OPENVPN)	32
3.4.1. Concept	32
3.4.2. PPTP Client.....	32
3.4.2.1. PC Connect to VPN (Based on PPTP Protocol).....	32
3.4.2.2. Router Connect to VPN(Based on PPTP Protocol)	33
3.4.3. L2TP Client	35
3.4.4. IPSEC.....	37
3.4.5. OPENVPN	38
3.4.6. GRE	42
3.4.7. SSTP Client	44
3.5. VPN+ Port Forward	45
3.6. Host Names	46
3.7. Static Router	46
3.8. Setup Limit Speed	47

3.9.	Firewall	48
3.9.1.	General Setting	48
3.9.2.	Traffic Rules	48
3.9.2.1.	IP-Reject	49
3.9.2.2.	IP-Allow	51
3.9.3.	NAT Function	52
3.9.3.1.	MASQ.....	52
3.9.3.2.	SNAT.....	52
3.9.3.3.	DNAT	54
3.9.4.	Custom Rules	57
3.9.5.	Access Restrictions.....	57
3.9.5.1.	Domain Blacklist.....	57
3.9.5.2.	Whitelist.....	58
3.9.6.	Rate Limiting.....	58
3.10.	Task Scheduler	59
3.11.	Webpage Sitting.....	60
3.12.	Web Function	61
4.	DTU Function.....	63
4.1.	Work Mode.....	63
4.1.1.	Net Transparent Transmission Mode	64
4.1.1.1.	Mode Declaration	64
4.1.2.	HTTPD Mode.....	66
4.1.2.1.	Mode Declaration	66
4.1.3.	UDC Mode	68
4.1.3.1.	Mode Declaration	68
4.2.	Serial Port	70
4.2.1.	Basic Parameters.....	70
4.2.2.	Frame Forming Mechanism	70
4.2.2.1.	Time Triggered Mode.....	70
4.2.2.2.	Length Triggered Mode.....	71
4.3.	Characteristic Functions	72
4.3.1.	Registration Package	72
4.3.2.	Heartbeat Package.....	74
4.3.3.	USR-Cloud.....	75
5.	AT Commands.....	77
5.1.	AT+VER.....	79
5.2.	AT+MAC	79
5.3.	AT+ICCID	79
5.4.	AT+IMEI.....	79
5.5.	AT+SYSINFO	80
5.6.	AT+APN	80
5.7.	AT+CSQ.....	80
5.8.	AT+NETMODE	80
5.9.	AT+TRAFFIC	81

5.10.	AT+UPTIME.....	81
5.11.	AT+WANN	81
5.12.	AT+LANN.....	81
5.13.	AT+WEBU	82
5.14.	AT+PLANG.....	82
5.15.	AT+CLEAR	82
5.16.	AT+Z.....	82
5.17.	AT+DHCPEN	82
5.18.	AT+UPDATE	83
5.19.	AT+MONITOR	83
5.20.	AT+HEARTPKT	83
5.21.	AT+ LINUXCMP	84
5.22.	AT+UART	84
5.23.	AT+UARTFT	84
5.24.	AT+UARTFL.....	85
5.25.	AT+SOCKA	85
5.26.	AT+SOCKB	85
5.27.	AT+SOCKC	85
5.28.	AT+SOCKD	86
5.29.	AT+SOCKAEN.....	86
5.30.	AT+SOCKBEN.....	86
5.31.	AT+SOCKCEN	86
5.32.	AT+SOCKDEN	87
5.33.	AT+SOCKALK	87
5.34.	AT+SOCKBLK.....	87
5.35.	AT+SOCKCLK.....	87
5.36.	AT+SOCKDLK	87
5.37.	AT+SOCKIND	87
5.38.	AT+REGEN	88
5.39.	AT+REGTP	88
5.40.	AT+REGDT	88
5.41.	AT+REGSND.....	88
5.42.	AT+CLOUD.....	89
5.43.	AT+HEARTEN.....	89
5.44.	AT+HEARTDT	89
5.45.	AT+HEARTSND	89
5.46.	AT+HEARTTM	90
5.47.	AT+HTPTP	90
5.48.	AT+HTPURL.....	90
5.49.	AT+HTPSV	90
5.50.	AT+HTPHD.....	91
5.51.	AT+HTPTO	91
5.52.	AT+HTPFLT	91
6.	Contact Us	92

7. Disclaimer	92
8. Update History.....	92

1. Product Overview

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

1.1. Product Function

- 1 wired LAN ports, 1 wired WAN ports (WAN ports can be switched to LAN ports).
- 2.4G WIFI wireless LAN
- Multiple LED communication indicators
- Supports SSH, TELNET, Web multi platform management configuration mode.
- One button to restore factory settings.
- The Ethernet support 10/100Mbps rate.
- VPN Client (PPTP/L2TP/IPSEC/GRE/OPENVPN/SSTP) and supports VPN encryption and static IP functions.
- Supports APN automatic checking network, 2/3/4G system switching, SIM information display, support APN/VPDN special network card.
- Supports for wired wireless multi network simultaneous online and multi network intelligent switching backup function
- Supports remote upgrade and remote monitoring.
- Dynamic Domain Name System (DDNS), Static Routing, PPPOE, DHCP, Static IP Function
- Mandatory portal (WIFIDOG), this function needs to be customized according to customer needs.
- Supports the firewall, NAT, DMZ host, access control black-and-white list, IP speed limit, NTP, MAC speed limit.
- SMS AT command
- 4 network work mode: 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.
- Supports for sending registration package / heartbeat data.
- Supports network transmission mode, HTTPD mode, UDC mode and USR-Cloud.
- AT command
- Supports external hardware watchdog design to ensure system stability.

2. Basic Function of Router

This chapter introduces the functions of GW-R4513, and the following is the overall block diagram of module functions.

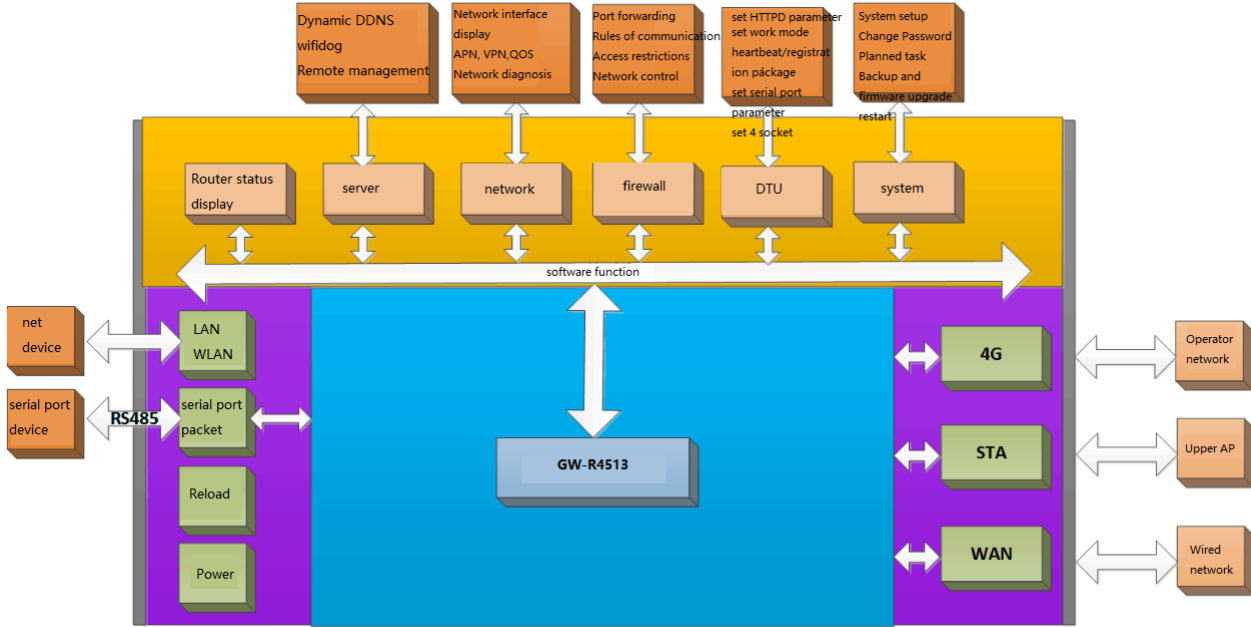


Figure 1 product function

Interface comparison table:

Table 1 interface comparison table

Network card name	Network card code	Corresponding network interface
Wired LAN port	br-lan	LAN
Default AP port of WIFI	ra0	LAN
Wired WAN port	eth0.2	WAN_WIRED
4G port	eth1	WAN_4G

Application scenario:

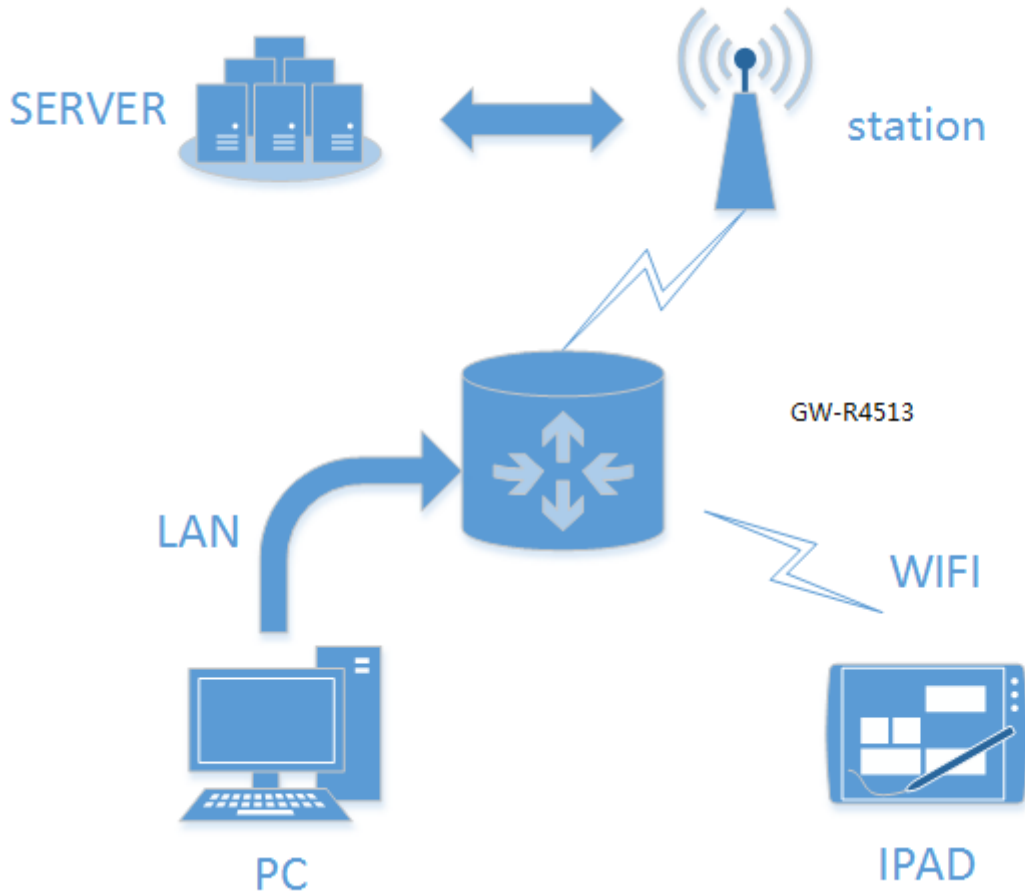


Figure 2 application scenario

- User equipment or computer can access the external network through the wired LAN port or WIFI interface of GW-R4513.
- If you use an ordinary mobile phone card, you can switch to the external network without any need.

2.1. 4G Interface

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

4G interface function:

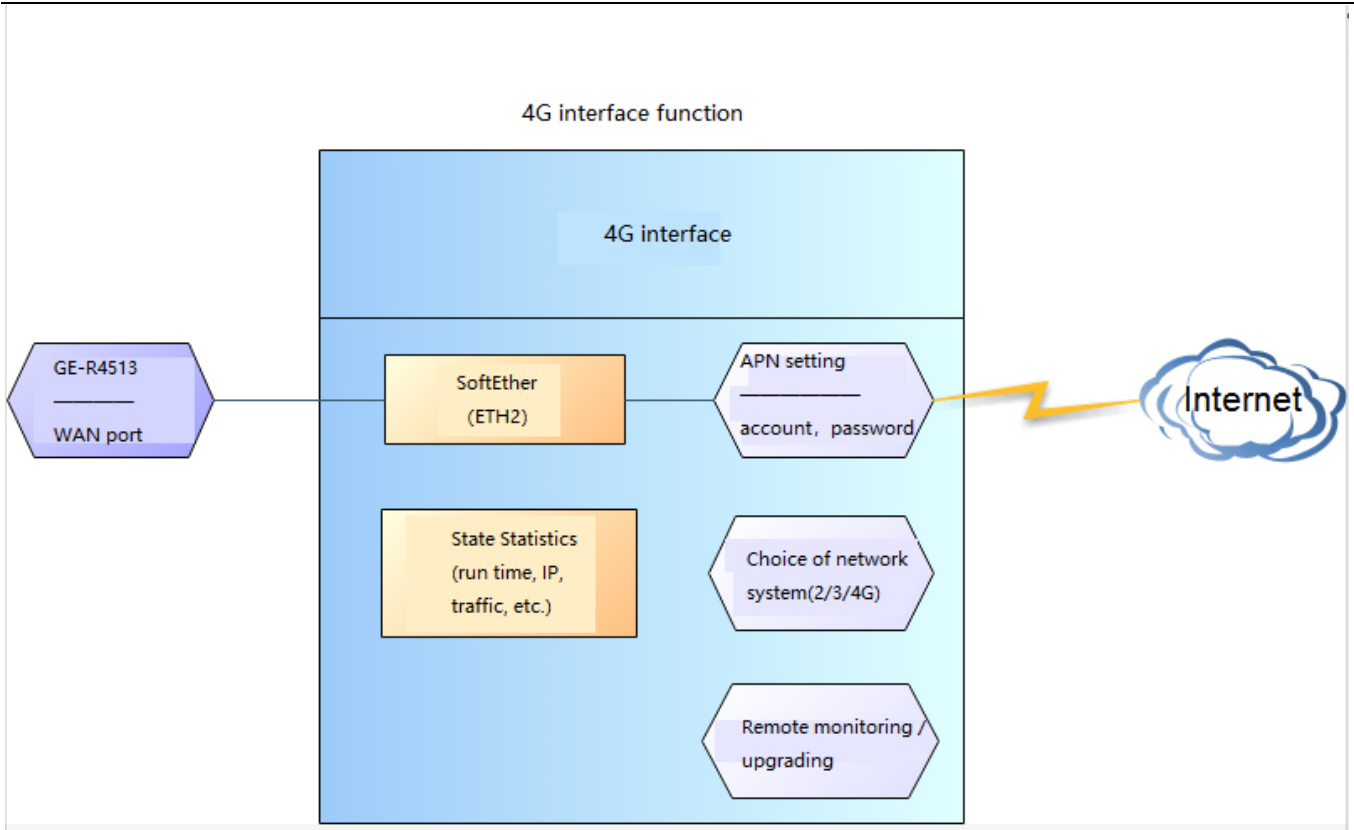


Figure 3 4G interface function

Webpage:

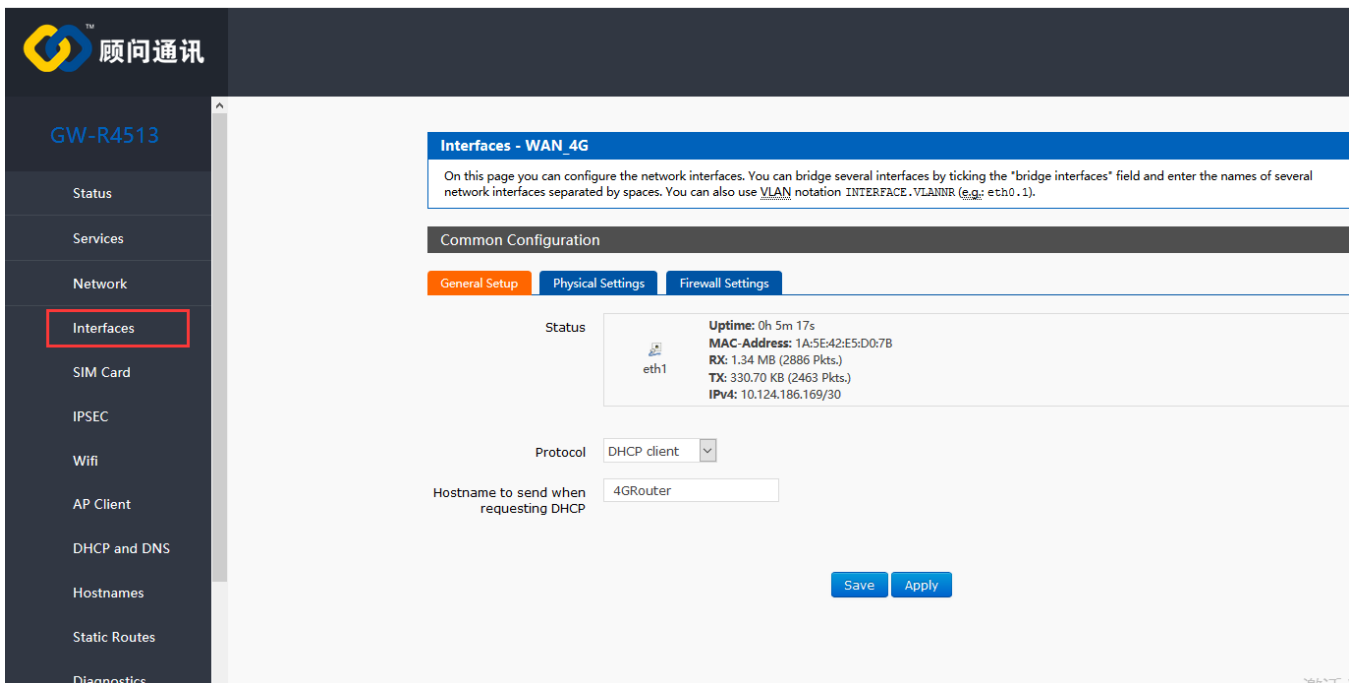


Figure 4 webpage

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

Table2 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.

2.2. 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).

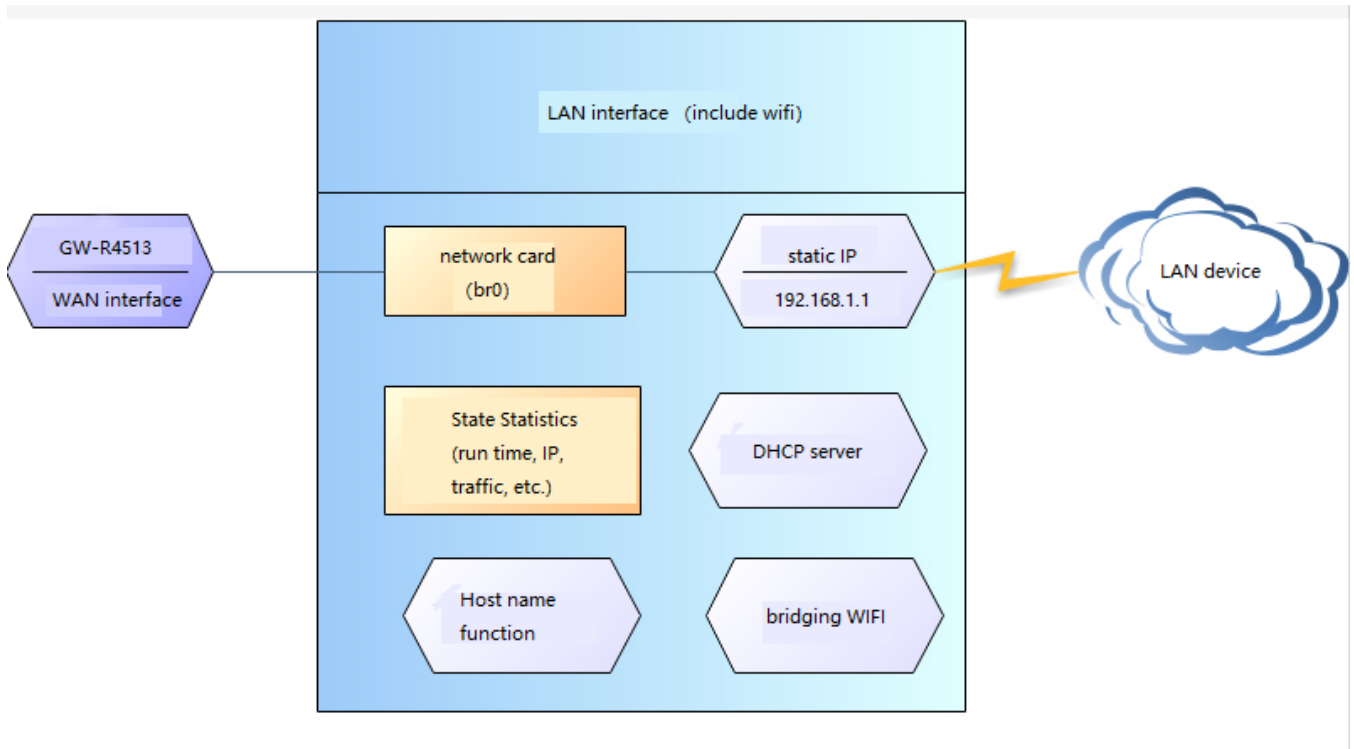


Figure 5 LAN interface function

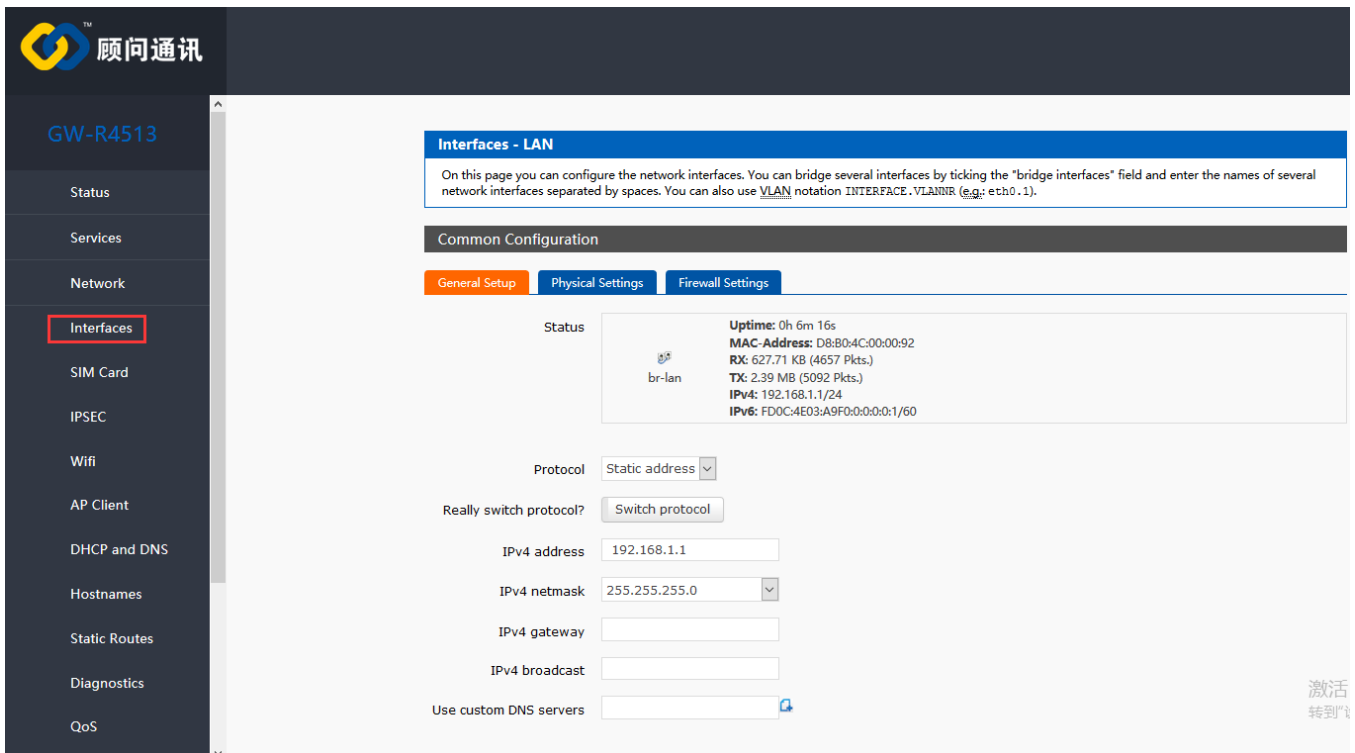


Figure 6 webpage of LAN interface setting

< 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.

2.2.1. 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.

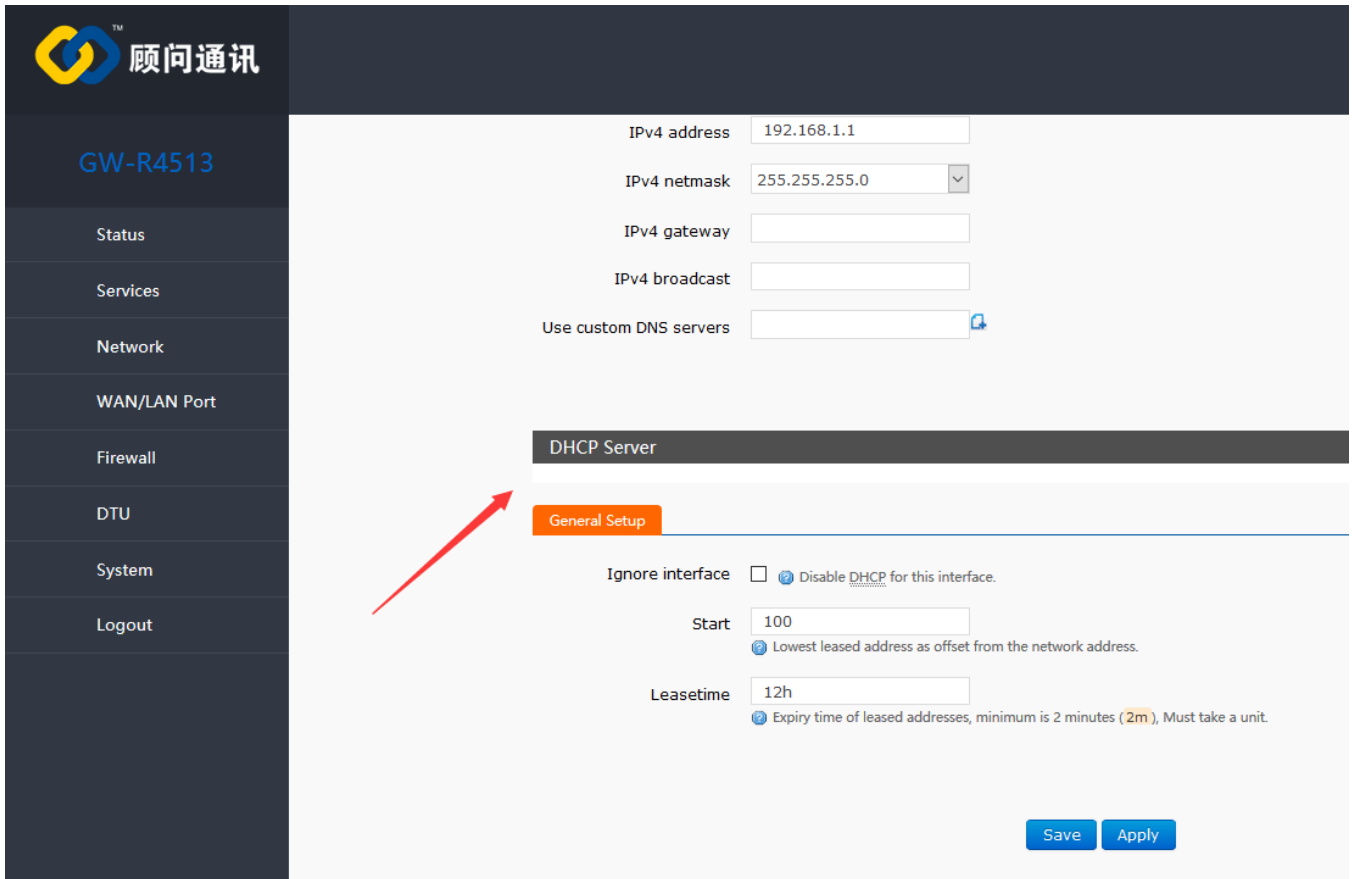
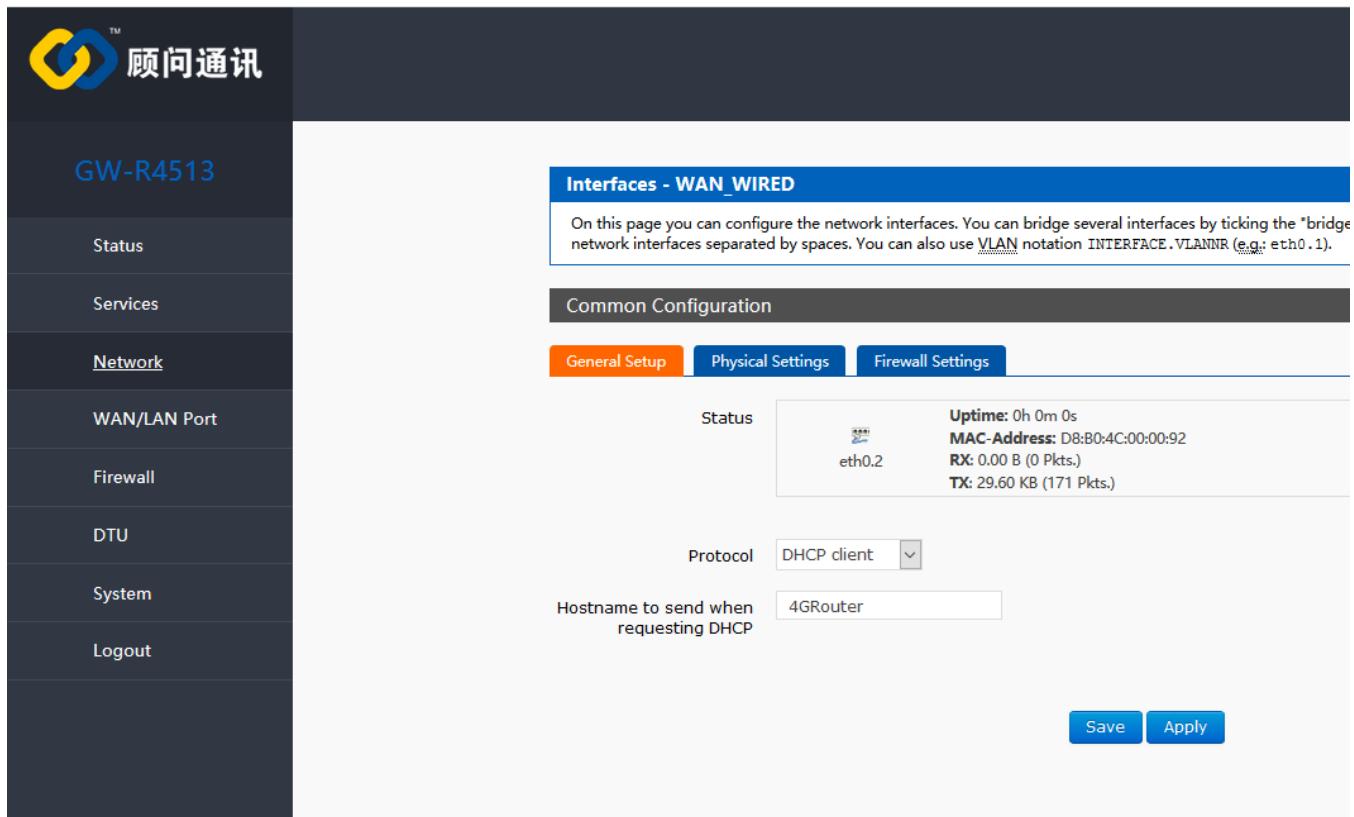


Figure7 webpage of DHCP setting

< 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.

2.3. WAN Interface



Interfaces - WAN_WIRED

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge" network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: eth0.1).

Common Configuration

General Setup | Physical Settings | Firewall Settings

Status

eth0.2

Uptime: 0h 0m 0s
 MAC-Address: D8:B0:4C:00:00:92
 RX: 0.00 B (0 Pkts.)
 TX: 29.60 KB (171 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP: 4GRouter

Save Apply

Figure8 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.

2.4. Wi-Fi Wireless Interface

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

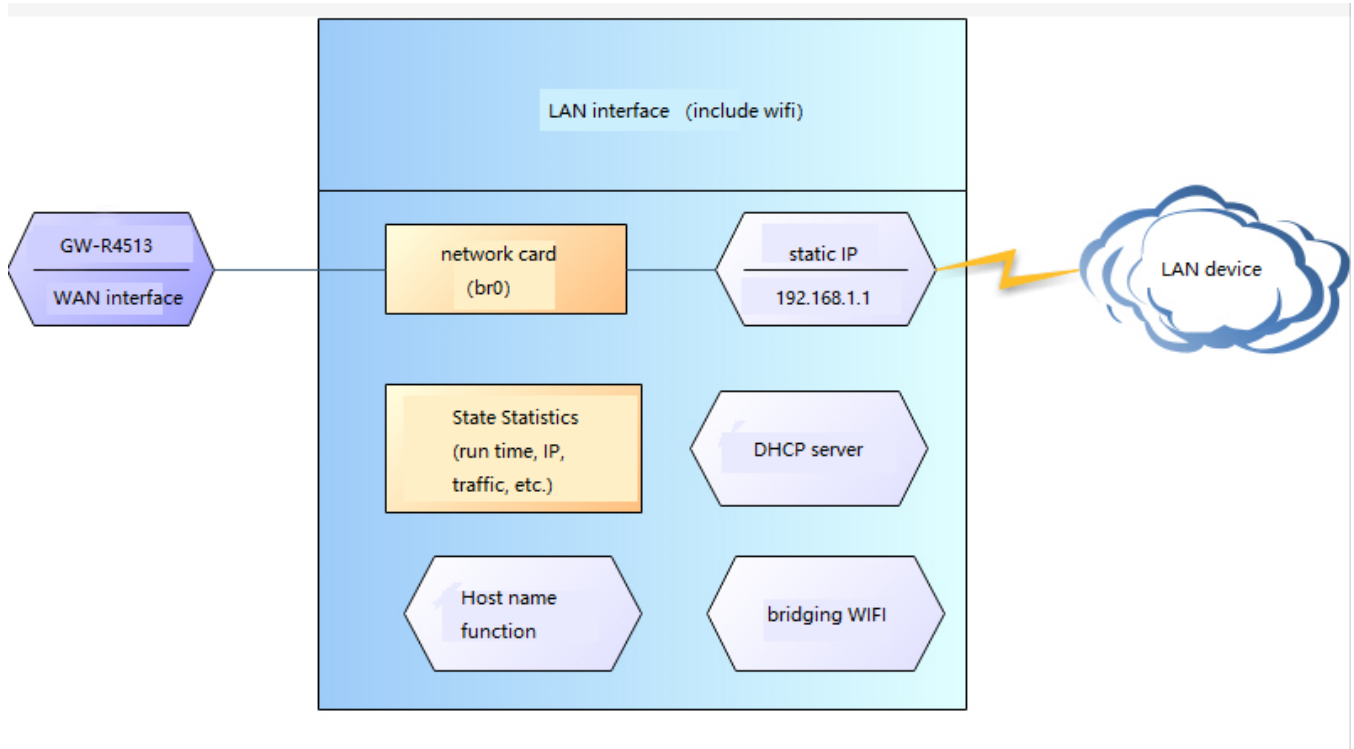


Figure9 WI-FI function

< 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.

Table3 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

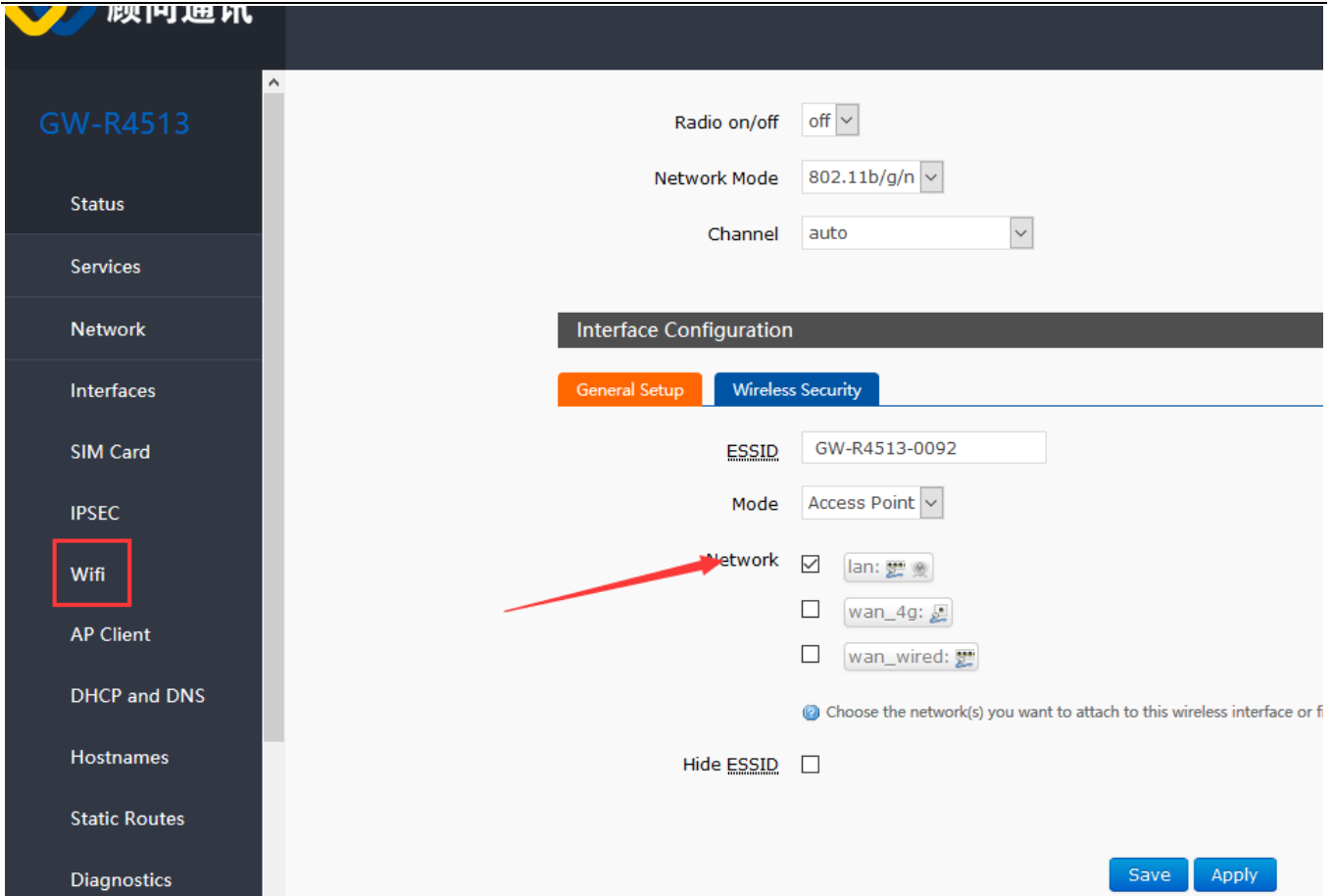


Figure10 the setting page of SSID

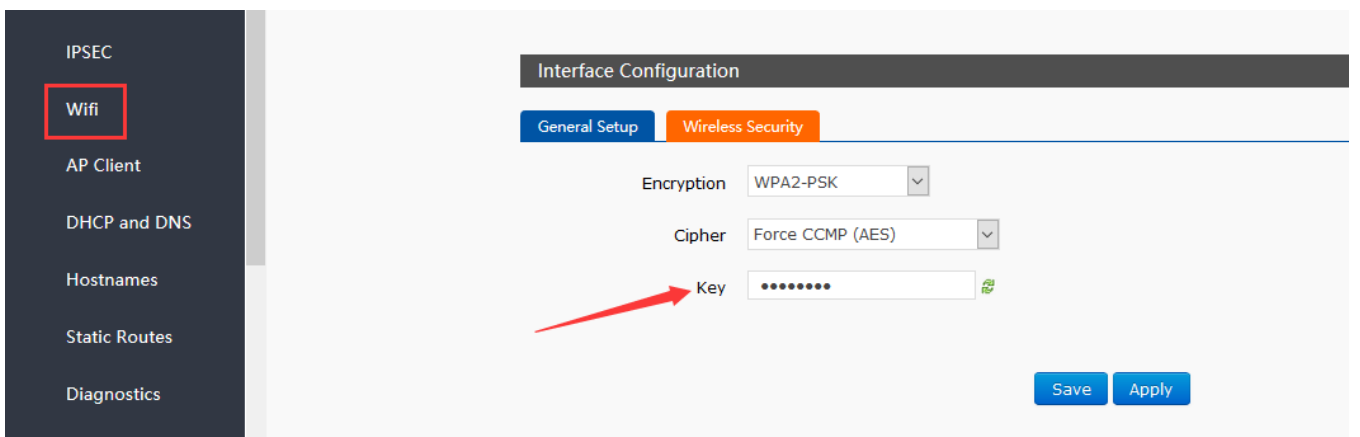


Figure11 the setting page of WI-FI

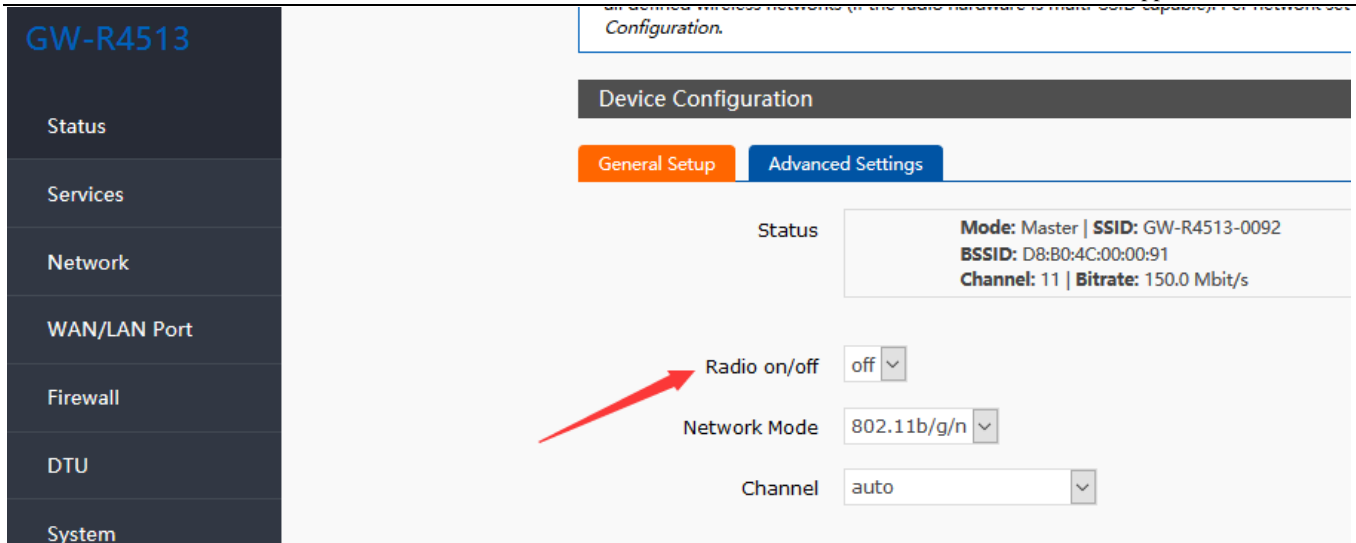


Figure12 the setting page of radio on/off

2.5. Network Diagnostic Function

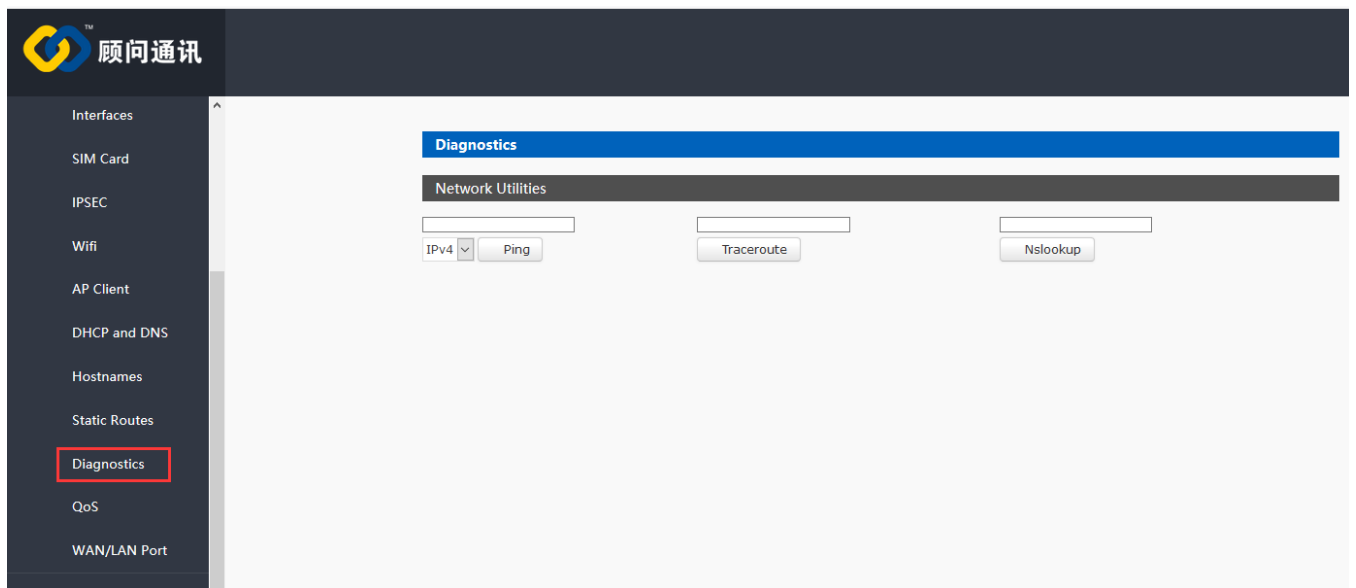
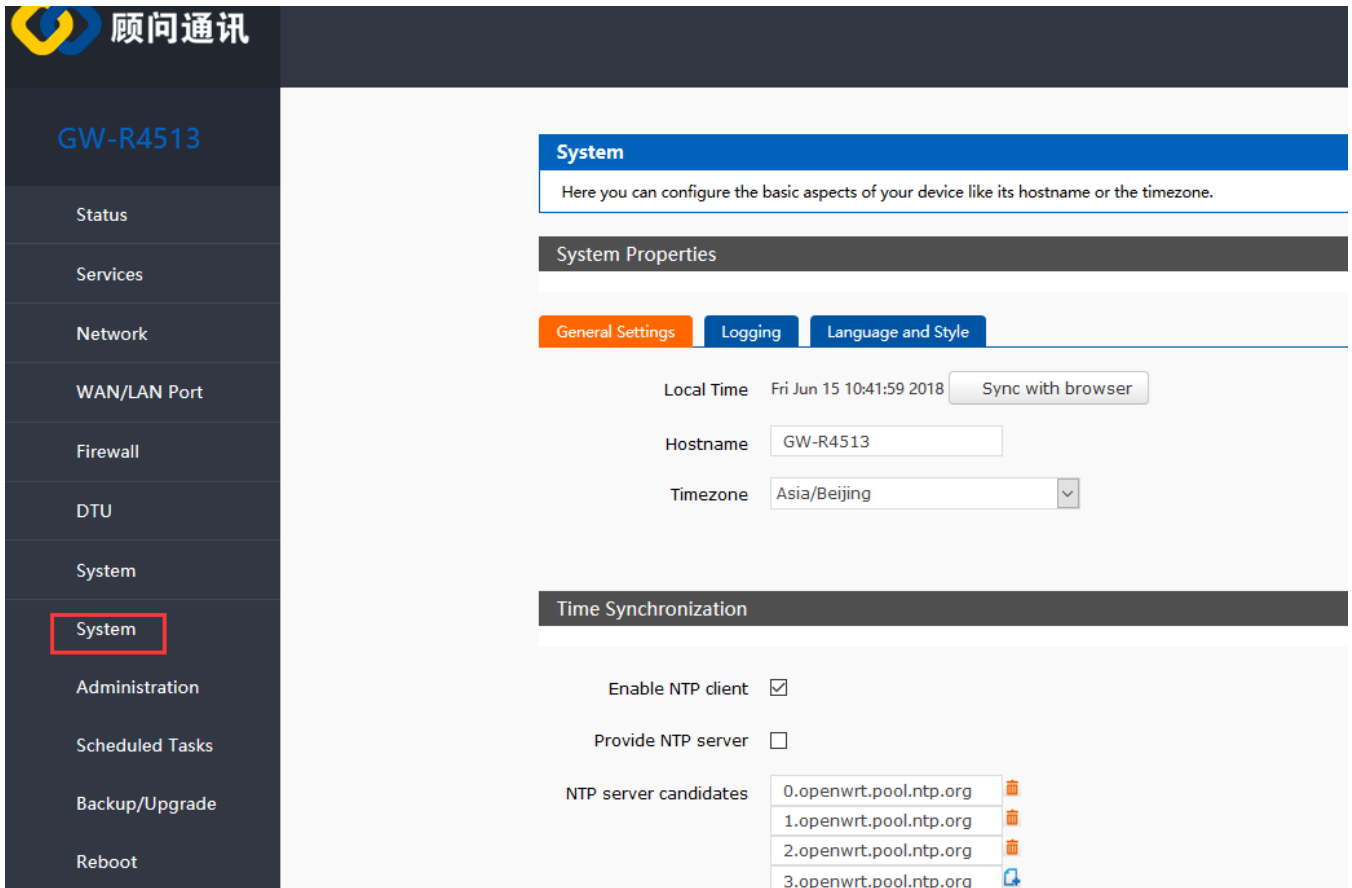


Figure13 the webpage of diagnostic

- 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.

2.6. Host Name and Time Zone



The screenshot displays the web management interface for a USR IOT device. On the left is a dark sidebar with a navigation menu. The main content area is titled 'System' and contains configuration options for 'System Properties'. The 'General Settings' tab is active, showing fields for 'Local Time', 'Hostname', and 'Timezone'. Below these is a 'Time Synchronization' section with checkboxes for 'Enable NTP client' and 'Provide NTP server', and a list of 'NTP server candidates'.

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings | Logging | Language and Style

Local Time: Fri Jun 15 10:41:59 2018

Hostname:

Timezone:

Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates:

- 0.openwrt.pool.ntp.org
- 1.openwrt.pool.ntp.org
- 2.openwrt.pool.ntp.org
- 3.openwrt.pool.ntp.org

Figure14 hostname and time zone

2.7. NTP Setting

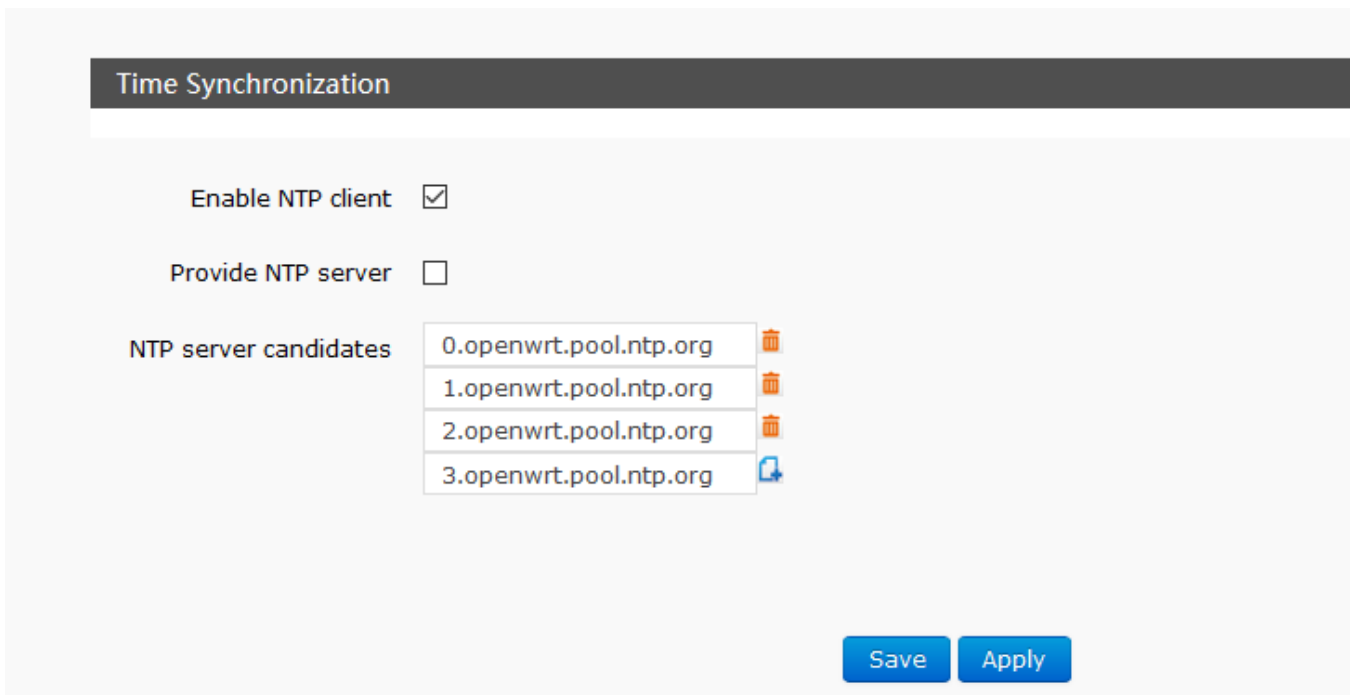


Figure15 the webpage of NTP

The router can start the NTP client function by default.

2.8. Password Setting

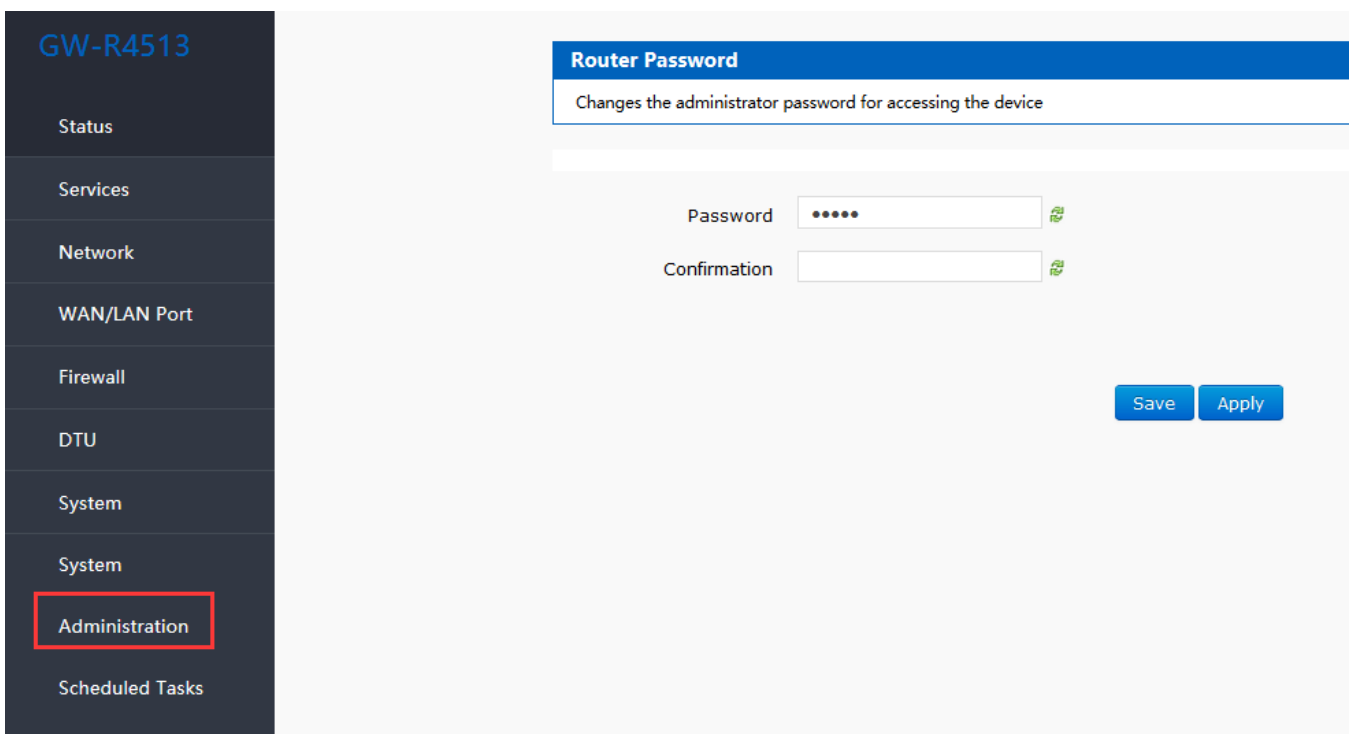


Figure16 the webpage of setting password

The default password can be set, the default password is root, and the user name can't be set. This password is the management password (web page login password).

User name can't be modified.

2.9. Backup Function

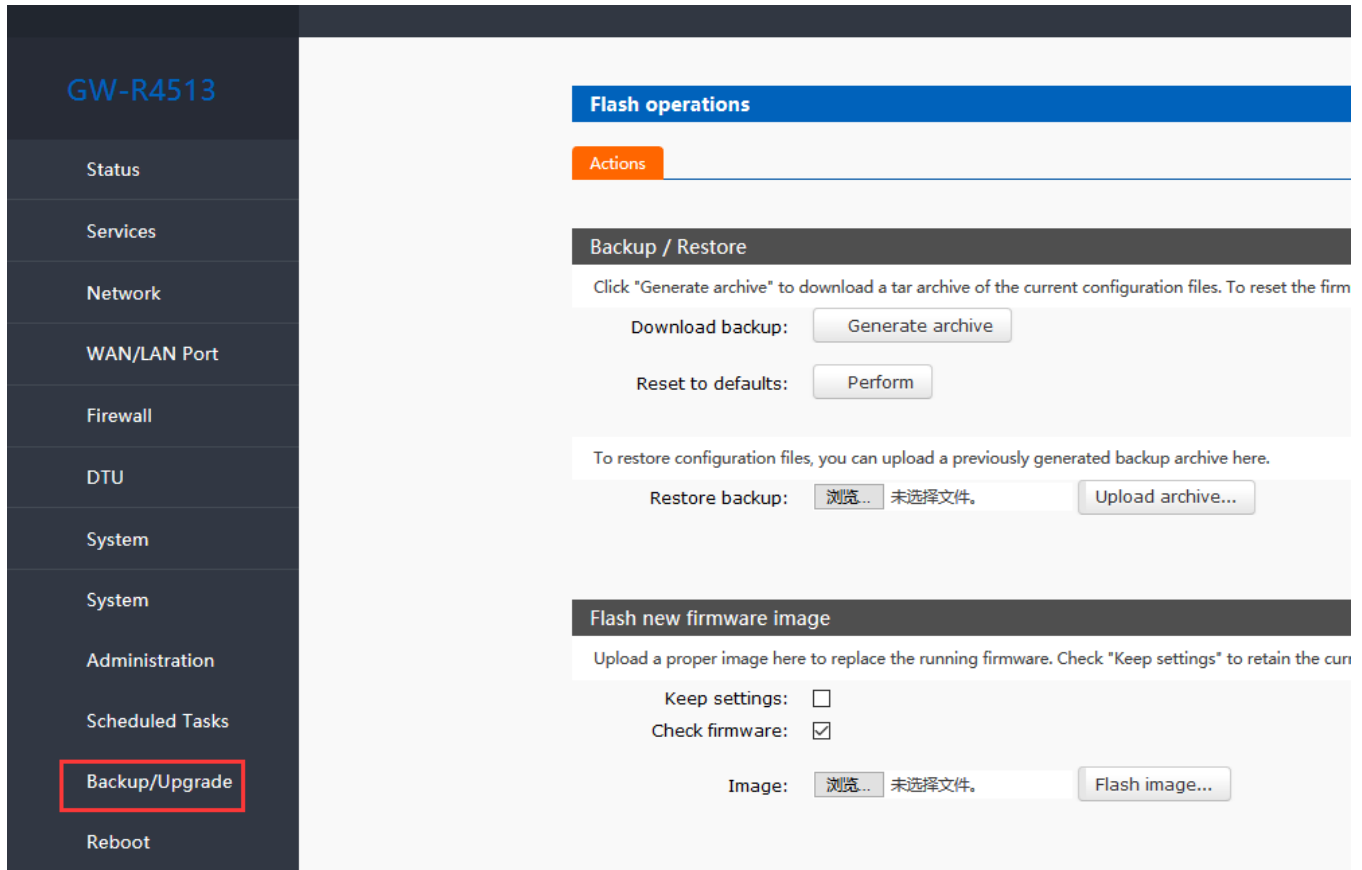


Figure17 the webpage of backup

Upload parameter file

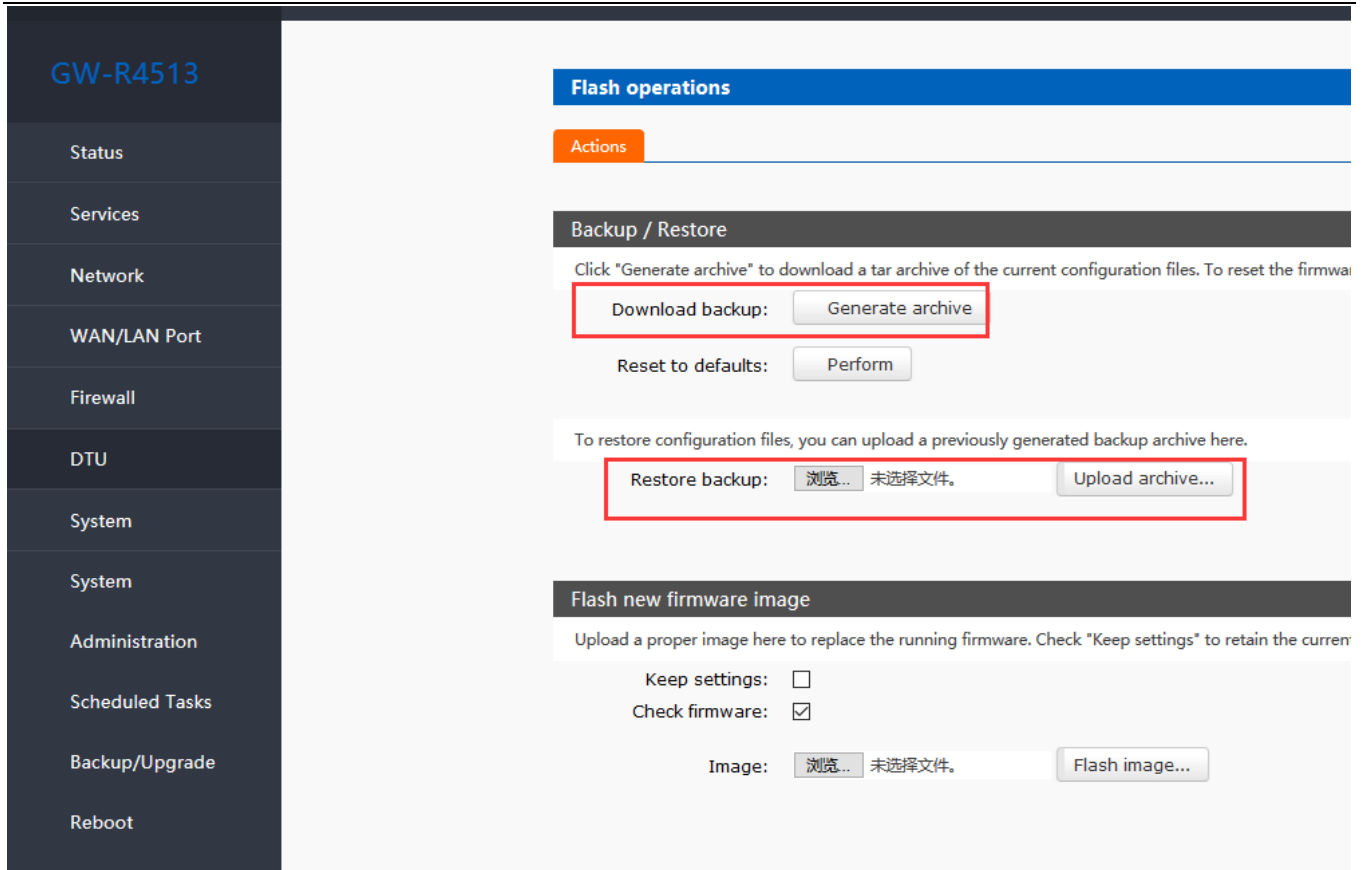


Figure18 the webpage of backup or recover

Backup parameters

2.10. Reset to Default

You can restore factory parameter settings through web pages.

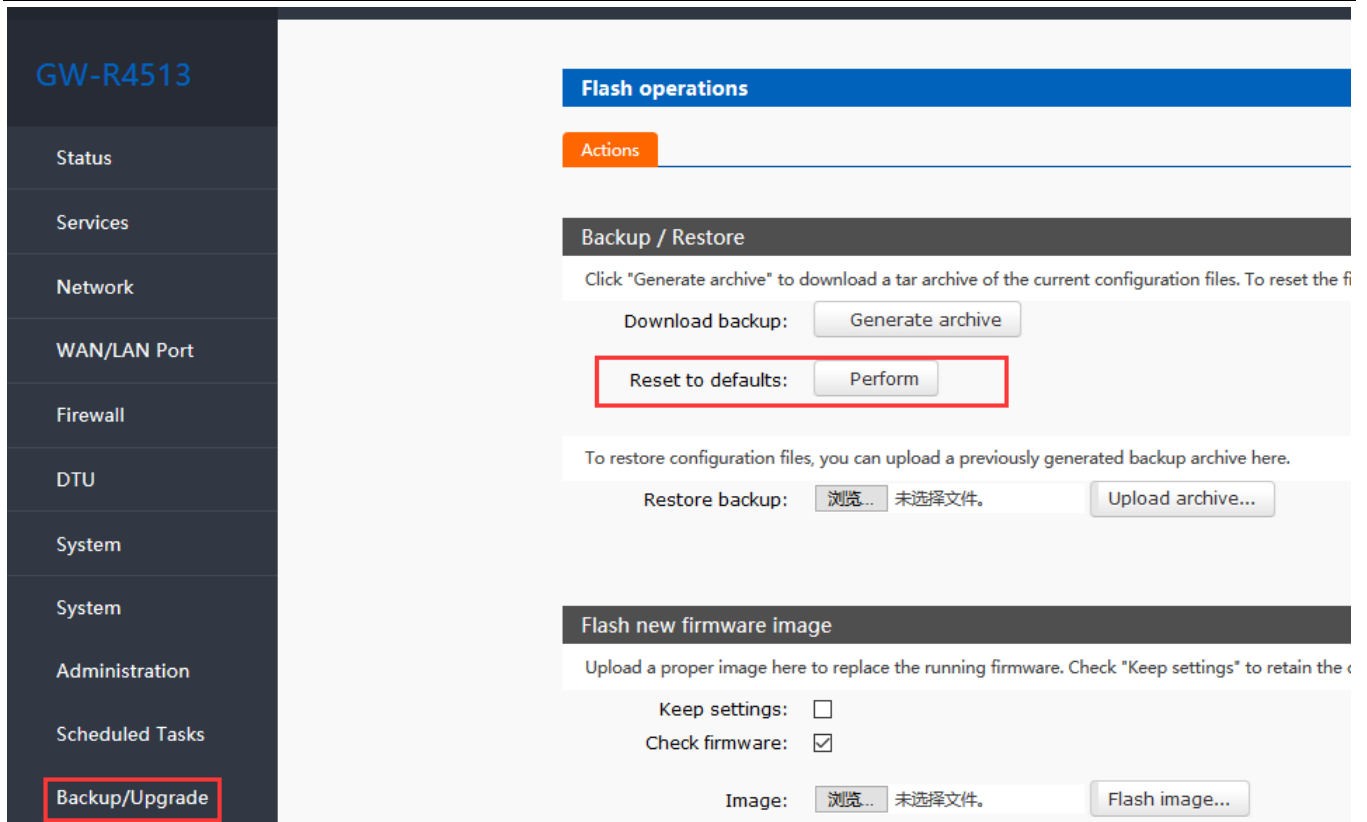


Figure19 the webpage of reset to default

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.

2.11. 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.

2.12. Firmware Upgrade

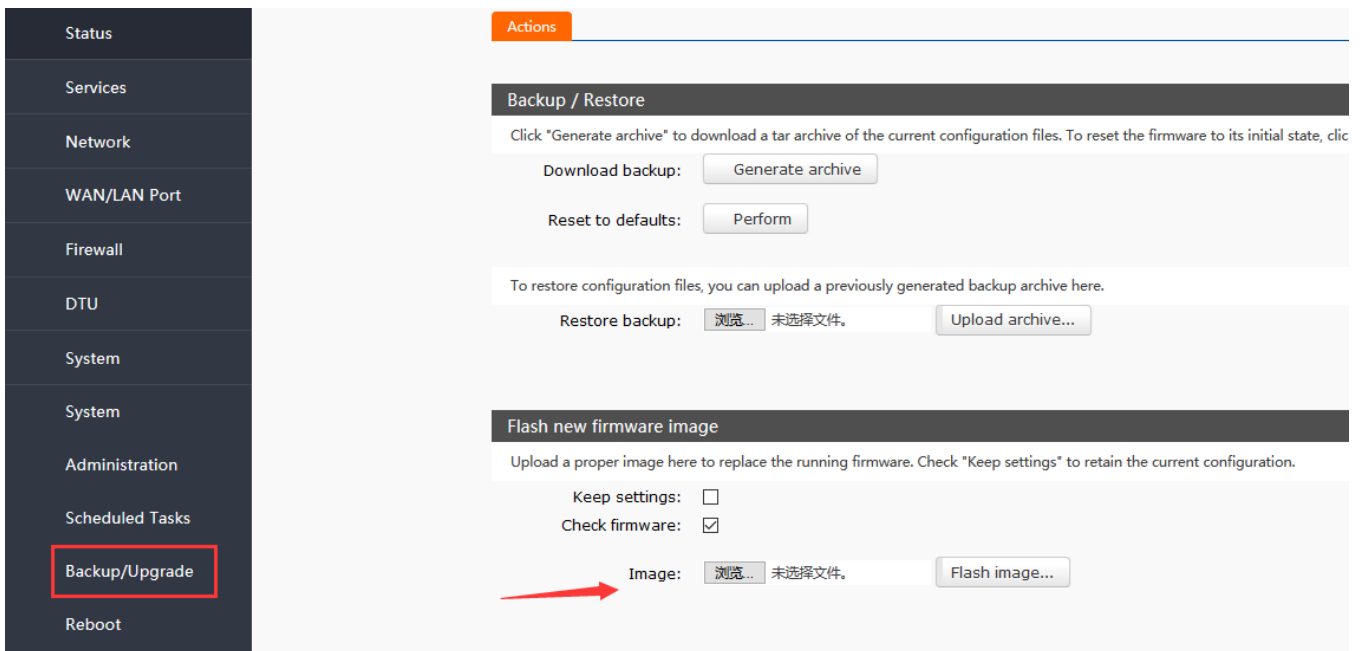


Figure20 the webpage of upgrade

< 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.

2.13. Reboot

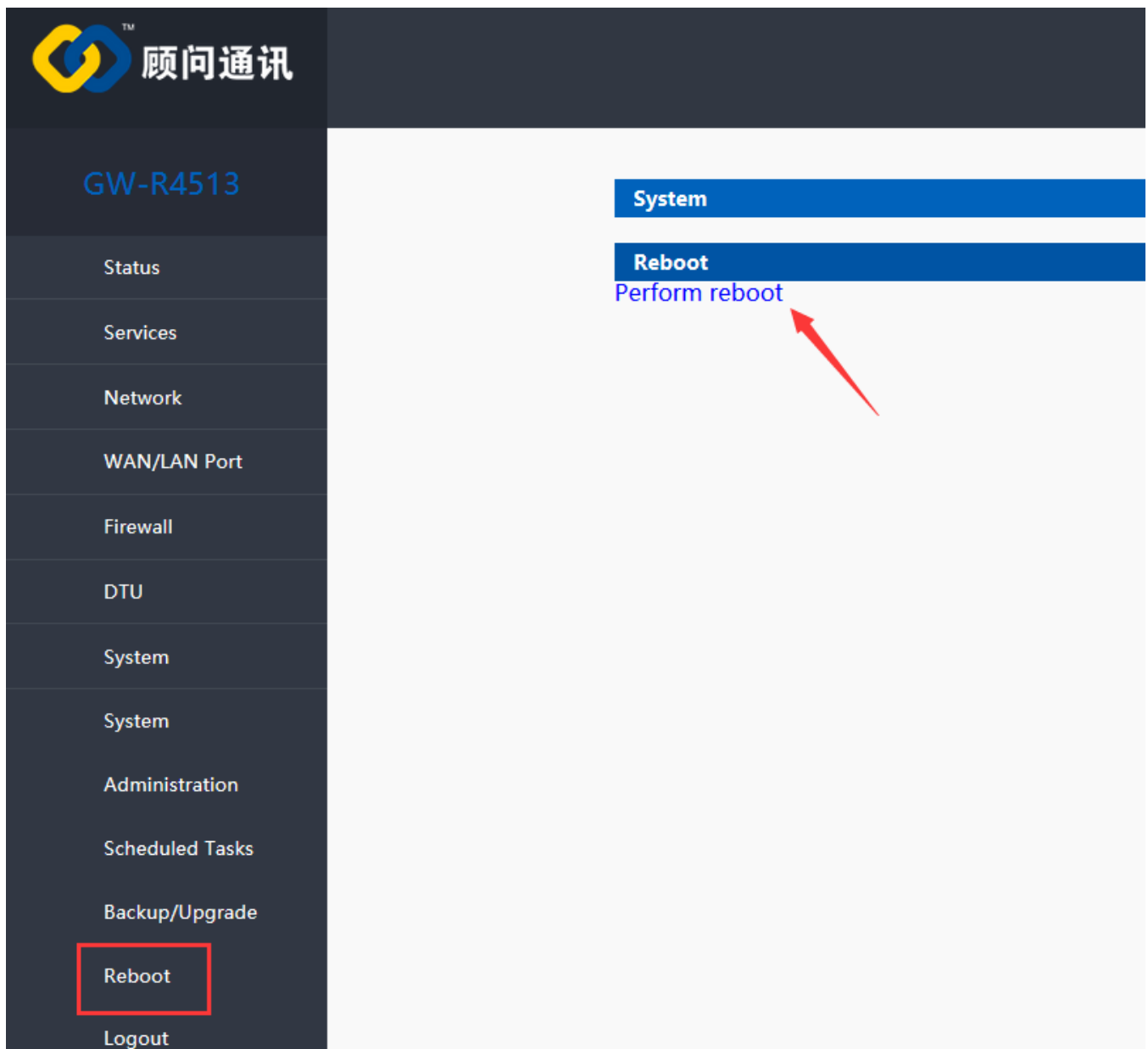


Figure21 the webpage of reboot

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. Advanced Function

3.1. DDNS

3.1.1. Supported Services

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

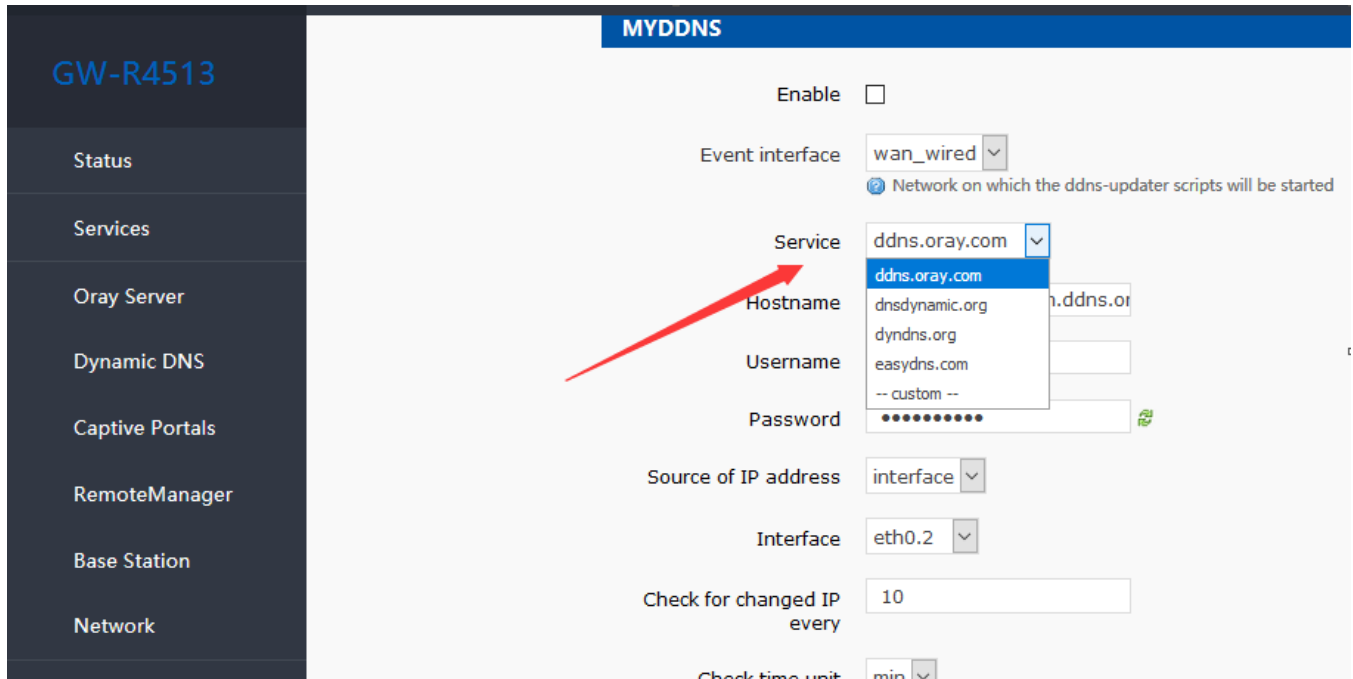


Figure22 the webpage of setting DDNS

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	e.g. 1 min

	smaller the value, the more frequent the detection.	
Force update time /force-time unit	Mandatory update interval	e.g. 72 h

3.1.2. Custom Service

The first is that the router itself supports this service (see the "Services" drop-down box and select the corresponding DDNS service provider). The settings are as follows:

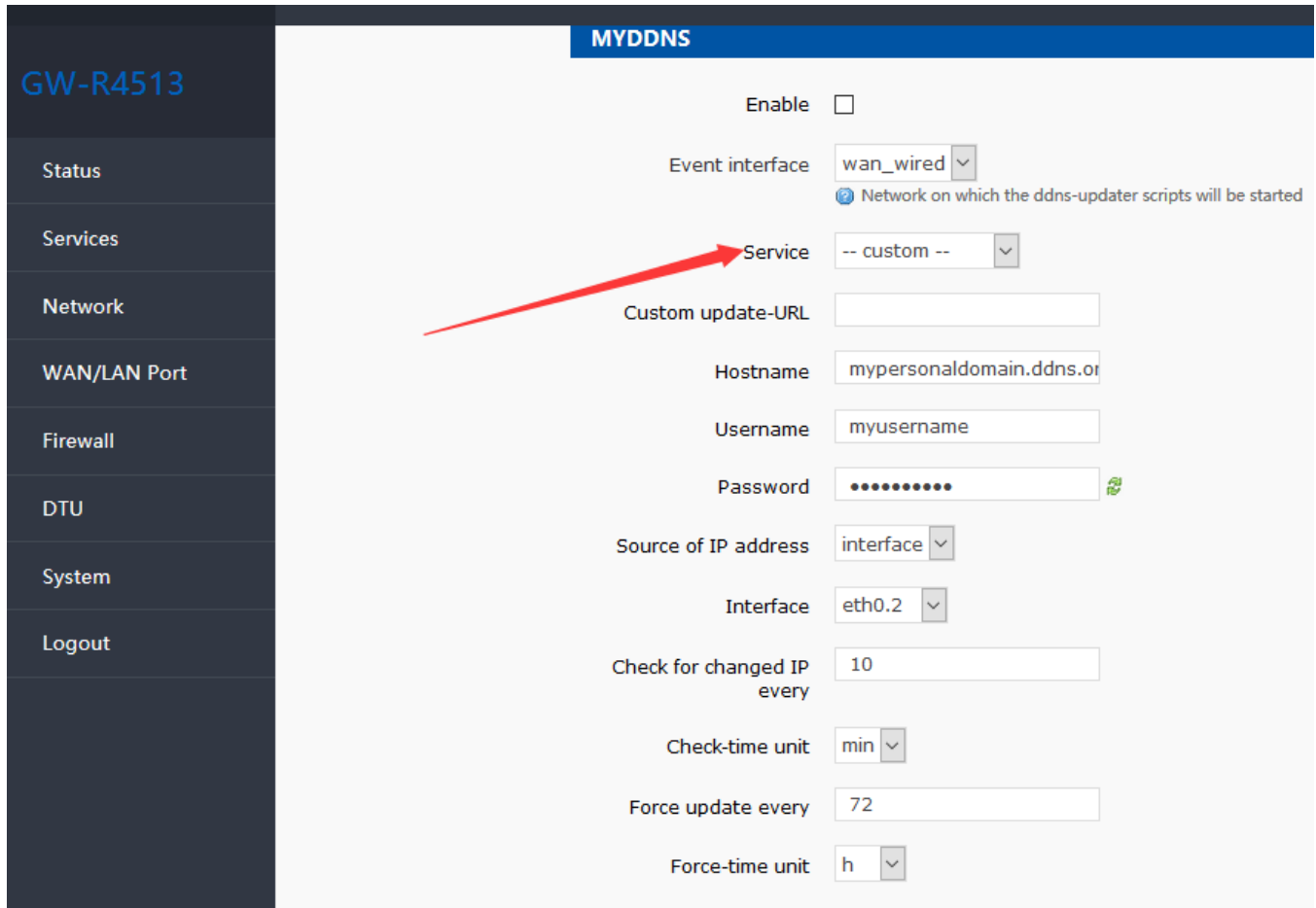


Figure23 the webpage of DDNS

DDNS function, provides a dynamic domain name resolution function for the router in the external network, and requests a domain name for itself to point to own WAN port IP address.

This function allows remote access to the router directly through the domain name.

The parameters need to be filled in as follows. The dynamic domain name I applied for is 1a516r1619.iask.in, the user name is ouclihuibin123, and the password is ouclihuibin1231.

Table5 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:ouclihui

		bin1231@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

Next, confirm whether the DDNS settings are effective (the router must restart to make the settings effective). First, let's take a look at the IP address of the public network of our network.

Then on the PC, the Ping domain name 1a516r1619.iask.in can be Ping, indicating that DDNS has come into effect.

3.1.3. Functional Characteristics

- After modifying the settings, please restart the router to ensure that it is effective.
- Please fill in the parameters, service/URL, domain name, username password, interface and other parameters strictly according to the form instructions to ensure that they are correct.
- Even if it is a router under the subnet, this function should also enable the dynamic domain name to take effect.
- DDNS + port mapping can remote access to the router's intranet.
- If the router's network is not allocated to an independent public network IP, this function can't be used.
- You can add multiple DDNS domains to this router.

3.2. 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, recording 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.

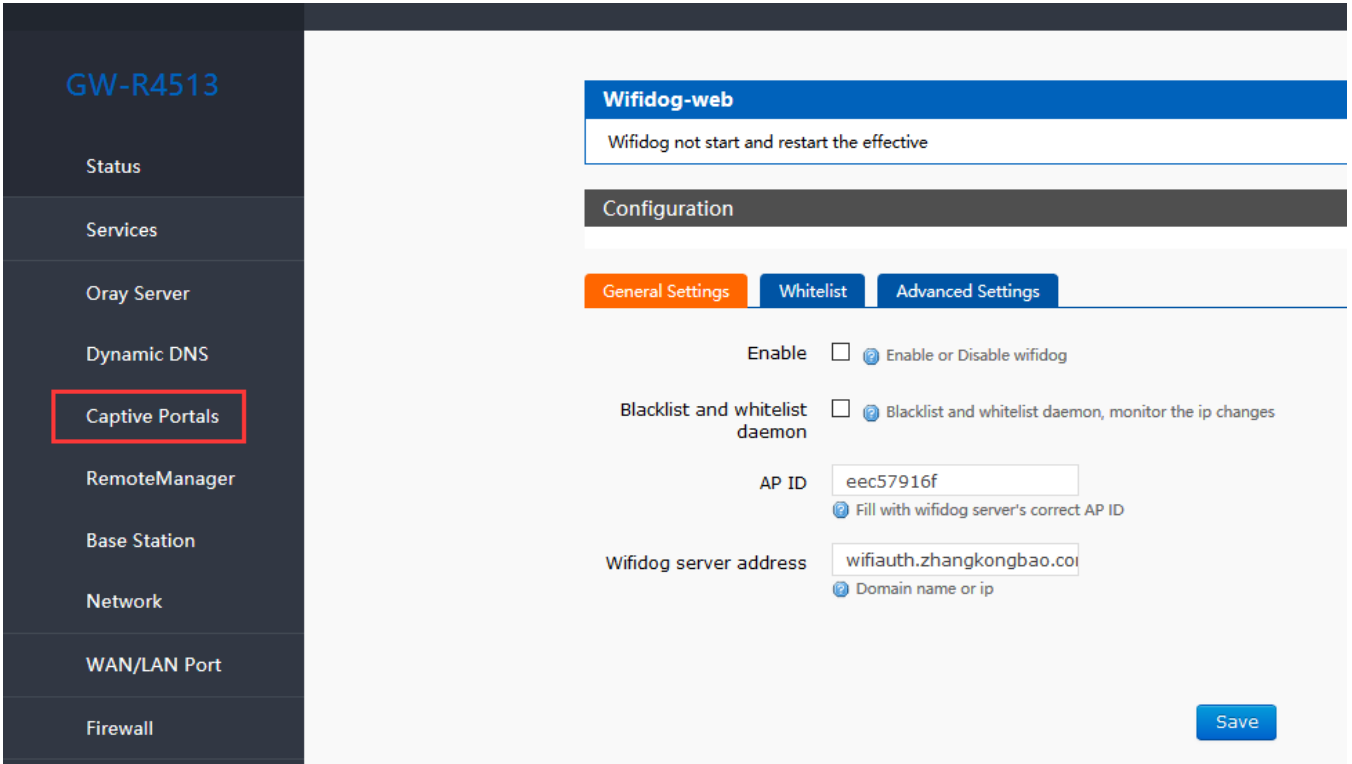
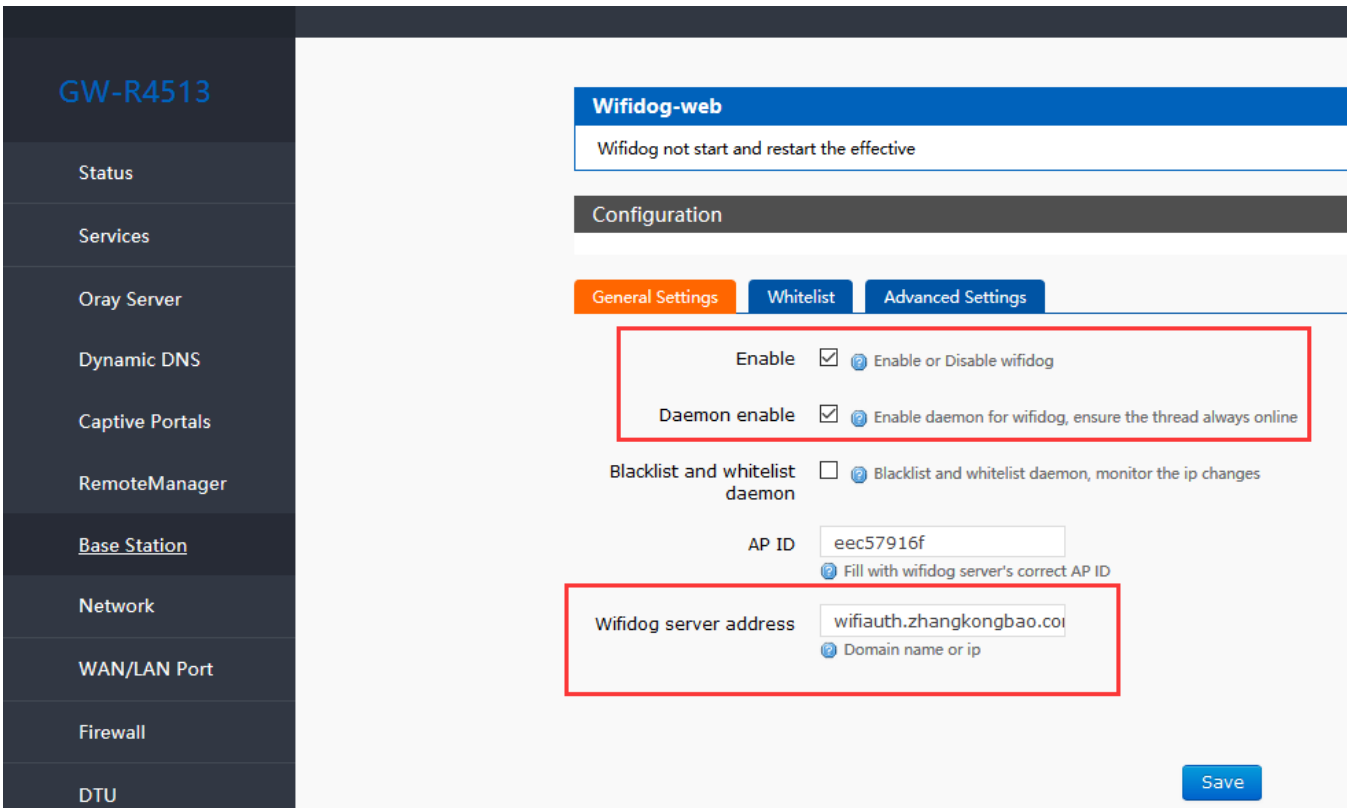


Figure24 the webpage1 of wifidog

Enable WI-FI dog



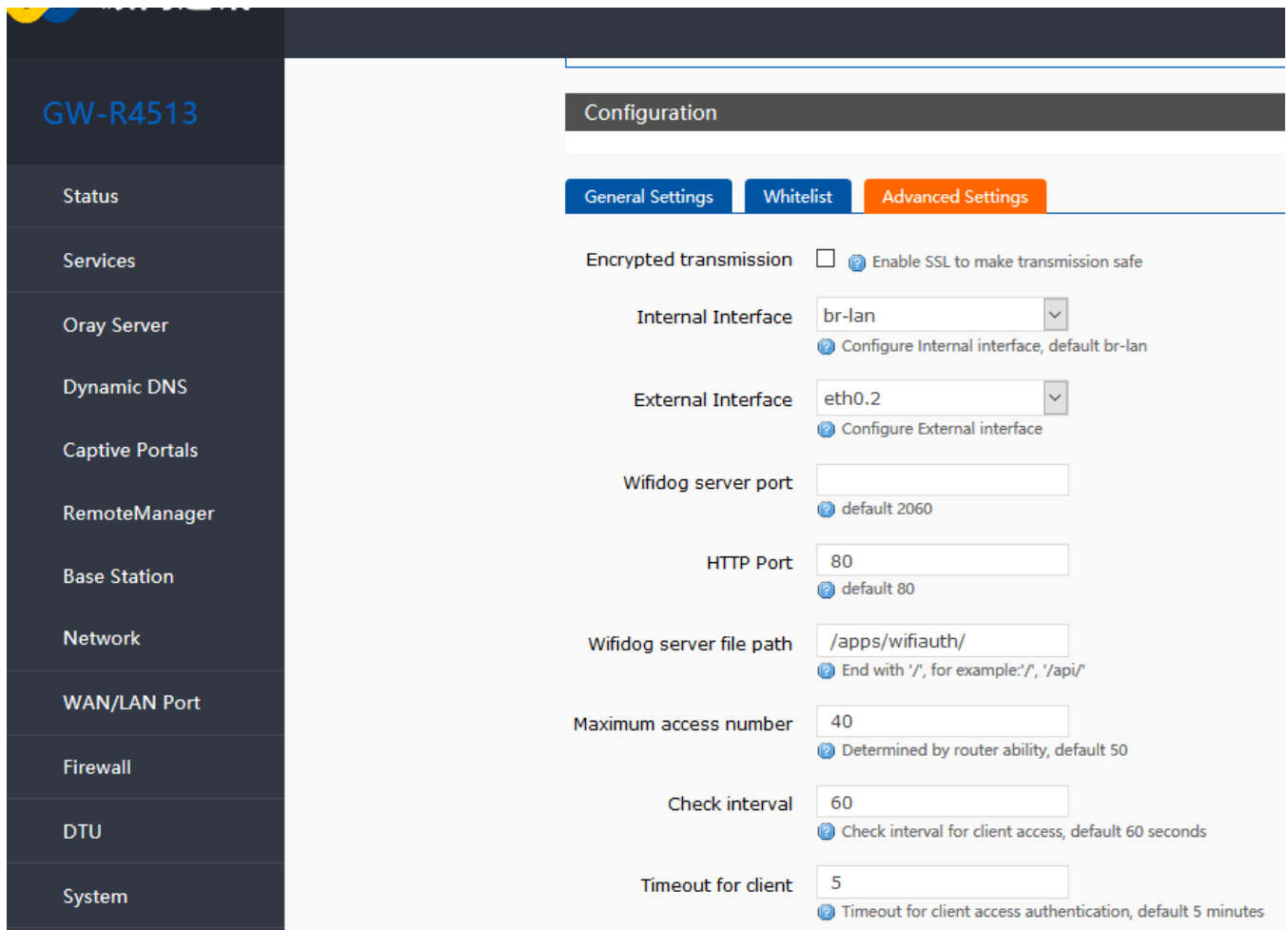


Figure25 the webpage2 of wifidog

Table6 WI-FI dog parameter

Function	Intro	Note
Enable WI-FI dog	Enable	If use
Daemon enable	Enable	If use
AP ID	nfuold700	
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/	

Note

- The mandatory portal functionality of this router is a demonstration, and if you want to use it formally, you need to customize it with the server
- If you do not intend to use this feature, uncheck it, or it will result in inaccessible access to the external network under the router (authenticated only)

3.3. APN Setting

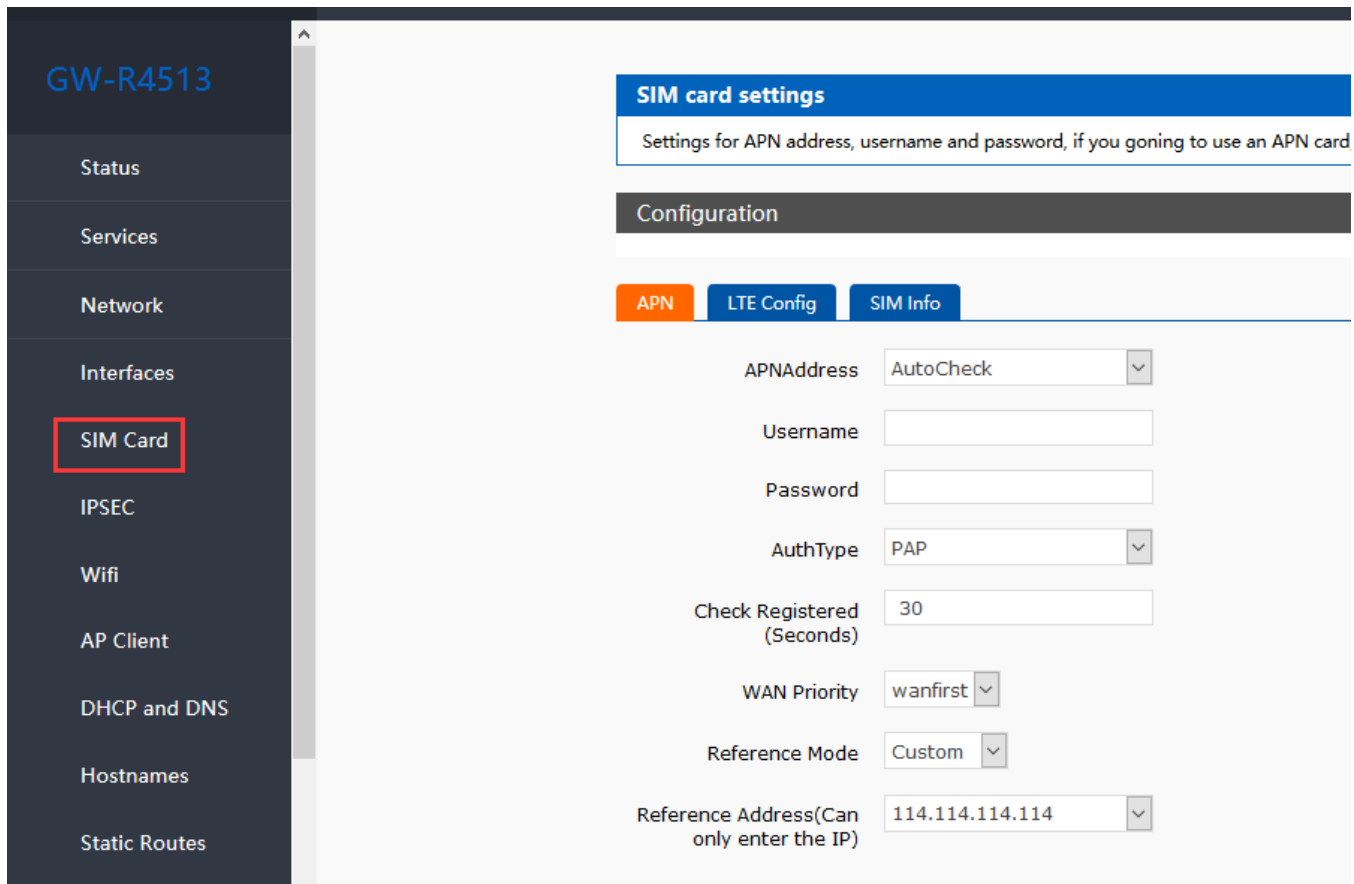


Figure26 the webpage2 of APN setting

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

Table7 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.

3.3.1. Modify APN

First, select the "Customize" option, and then fill in the exact APN address as required. After successful setup, restart

the router.

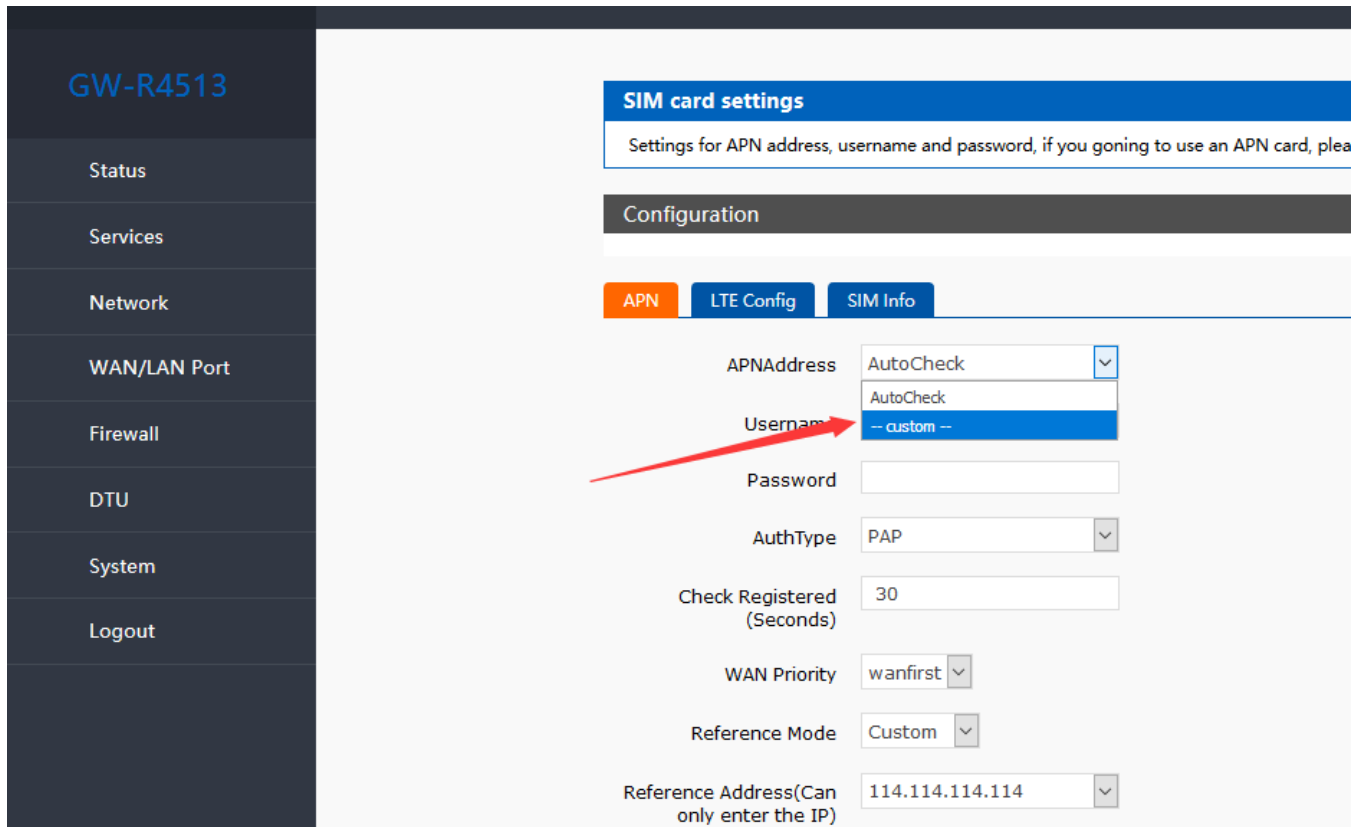


Figure27 the webpage of modify APN

3.3.2. SIM Card Settings

The networking format of 4G-router is set automatically by default, that is, the priority of 4G - > 3G - > 2G, and automatically selects the networking.

If it's not a 4G SIM card, or if the network needs to be specified (for example, you specify that you want to use 2G or 3G networks), then you need to choose the network format (otherwise it will affect the network rate, etc.)

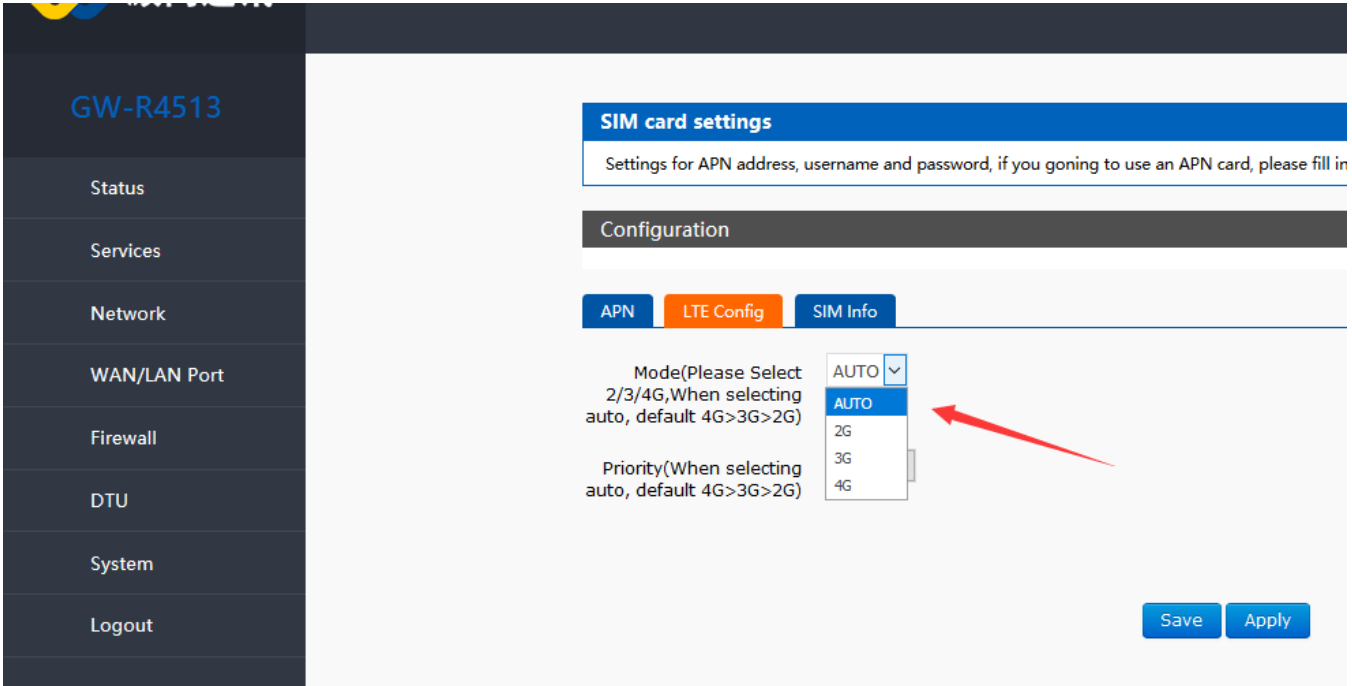


Figure28 the webpage of SIM card setting

3.3.3. SIM Card Information

The SIM card information displays the configuration information of the SIM card in detail, and you can see the cause of the problem here if the network fails.

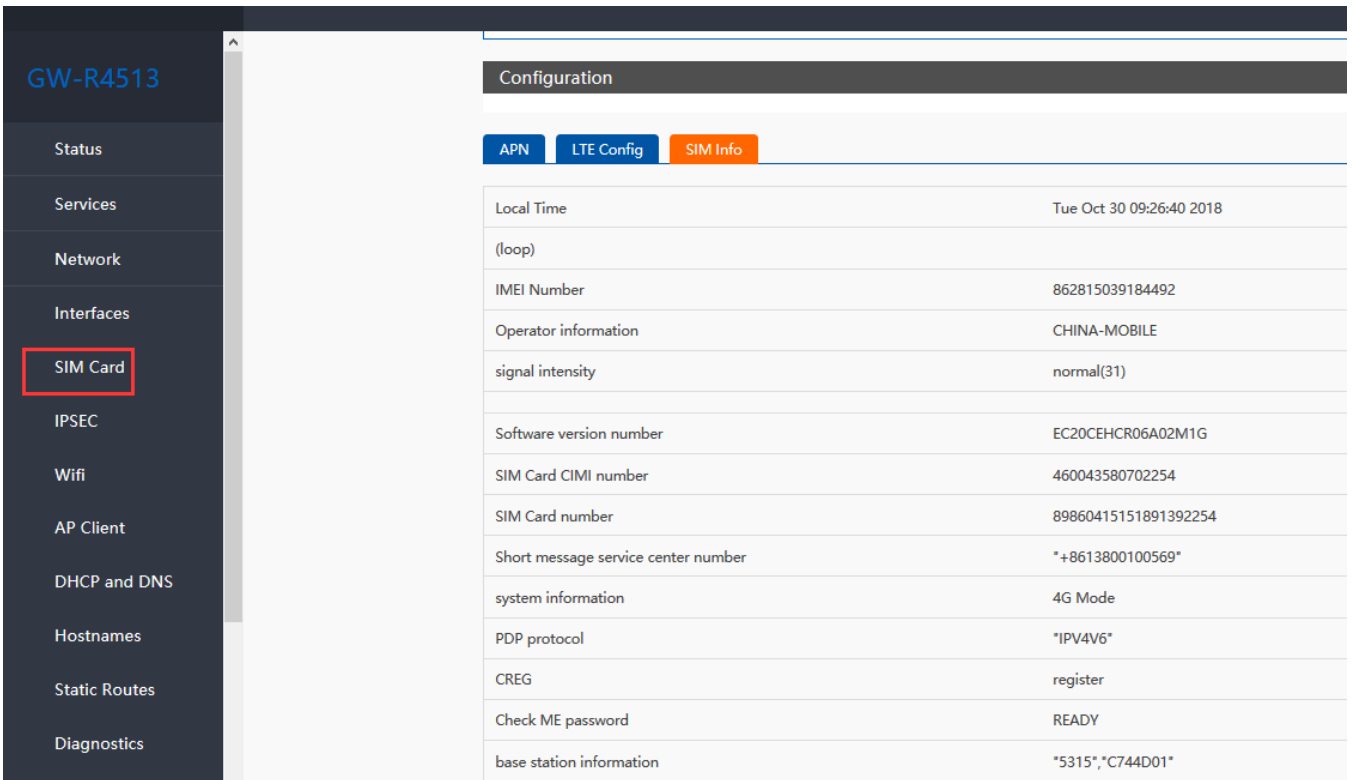


Figure29 the webpage of SIM card info

3.4. VPN Client(PPTP/L2TP/GRE/OPENVPN)

3.4.1. Concept

VPN, virtual private network, include client and server, divided into PPTP,L2TP,ipsec,openvpn,gre,sstp.etc on protocol.

PPTP:

A point-to-point tunneling protocol that uses a TCP (port 1723) connection to maintain tunnels, encapsulates data into PPP data frames via tunnels using general routing encapsulation (GRE) technology, and encrypts or compresses load data in encapsulated PPP frames. MPPE encrypts PPP frames with encryption keys generated by MS-CHAP, MS-CHAP V2, or EAP-TLS authentication procedures.

L2TP:

The second tier tunneling protocol is similar to PPTP. Currently GW-R4513 supports many authentication methods, such as tunnel password authentication, CHAP, etc. Encryption methods support MPPE encryption and L2TP OVER IPSEC pre-shared key encryption.

IPSEC:

IPSEC protocol is not a separate protocol. It provides a complete set of network data security architecture between application and IP layer, including network authentication protocol AH, ESP, IKE and some algorithms for network authentication and encryption. Among them, AH protocol and ESP protocol are used to provide security services, and IKE protocol is used for key exchange.

OPENVPN:

The application layer VPN based on Openssl library. Support certificate-based two-way authentication, that is, the client needs to authenticate the server, the server also needs to authenticate the client

GRE:

GRE(Generic Routing Encapsulation) protocol encapsulates packets of some network layer protocols, such as IP and IPX, so that these encapsulated packets can be transmitted in another network layer protocol, such as IP. GRE uses tunnel technology, which is VPN's third layer tunneling protocol.

SSTP:

SSTP, also known as Secure Socket Tunneling Protocol, is an Internet protocol that creates a VPN tunnel for transmission over HTTPS.

SSTP is only suitable for remote access, and can 't support VPN tunnels between sites and sites.

3.4.2. PPTP Client

3.4.2.1. PC Connect to VPN (Based on PPTP Protocol)

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.

3.4.2.2. Router Connect to VPN(Based on PPTP Protocol)

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.

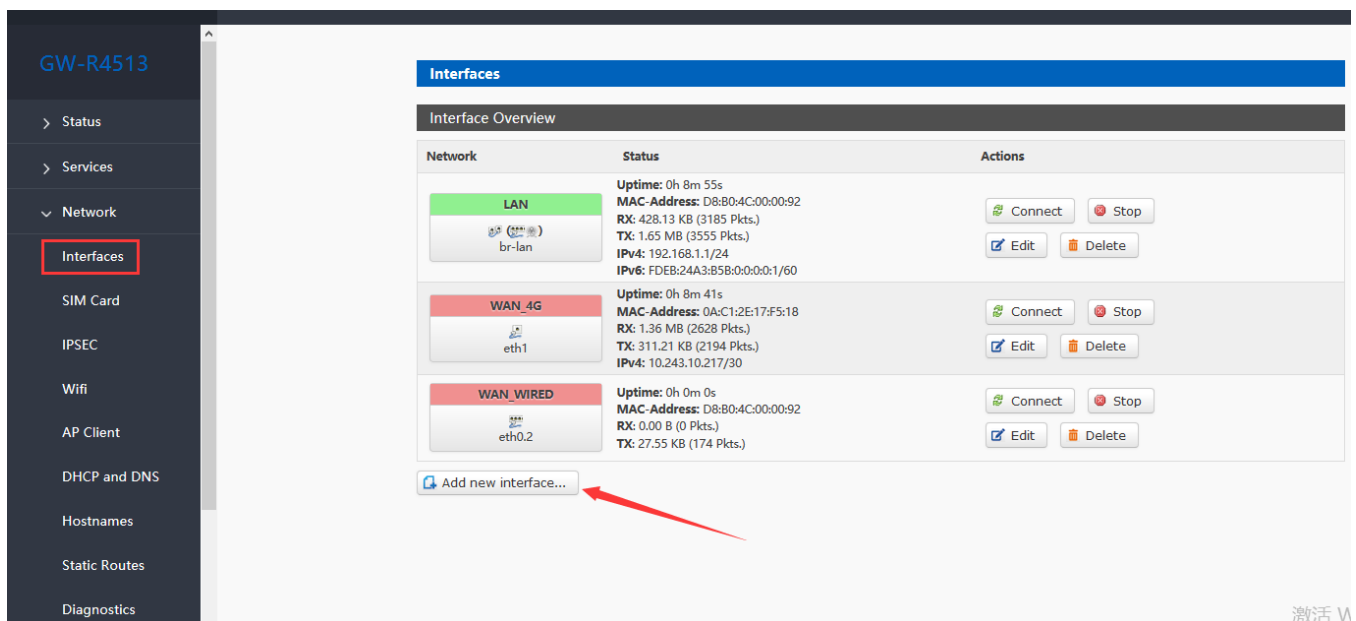


Figure30 the webpage1 of VPN

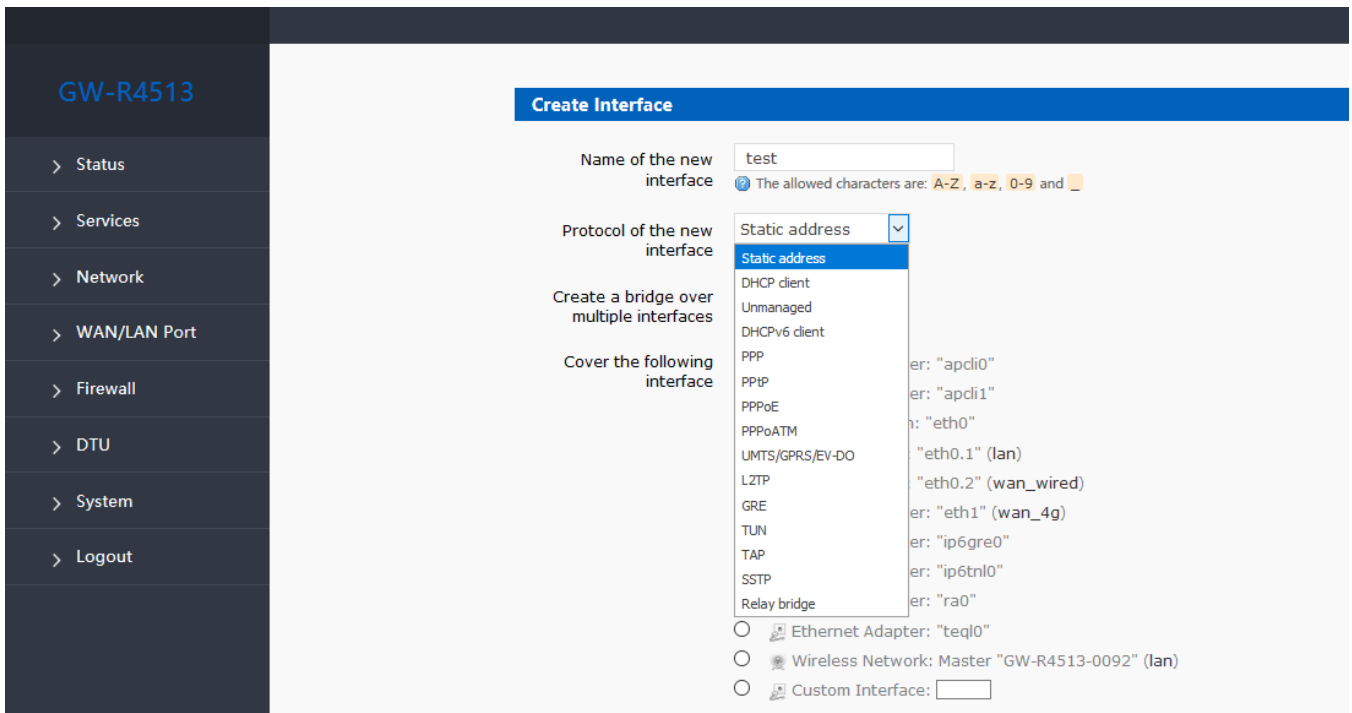


Figure31 the webpage2 of VPN

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

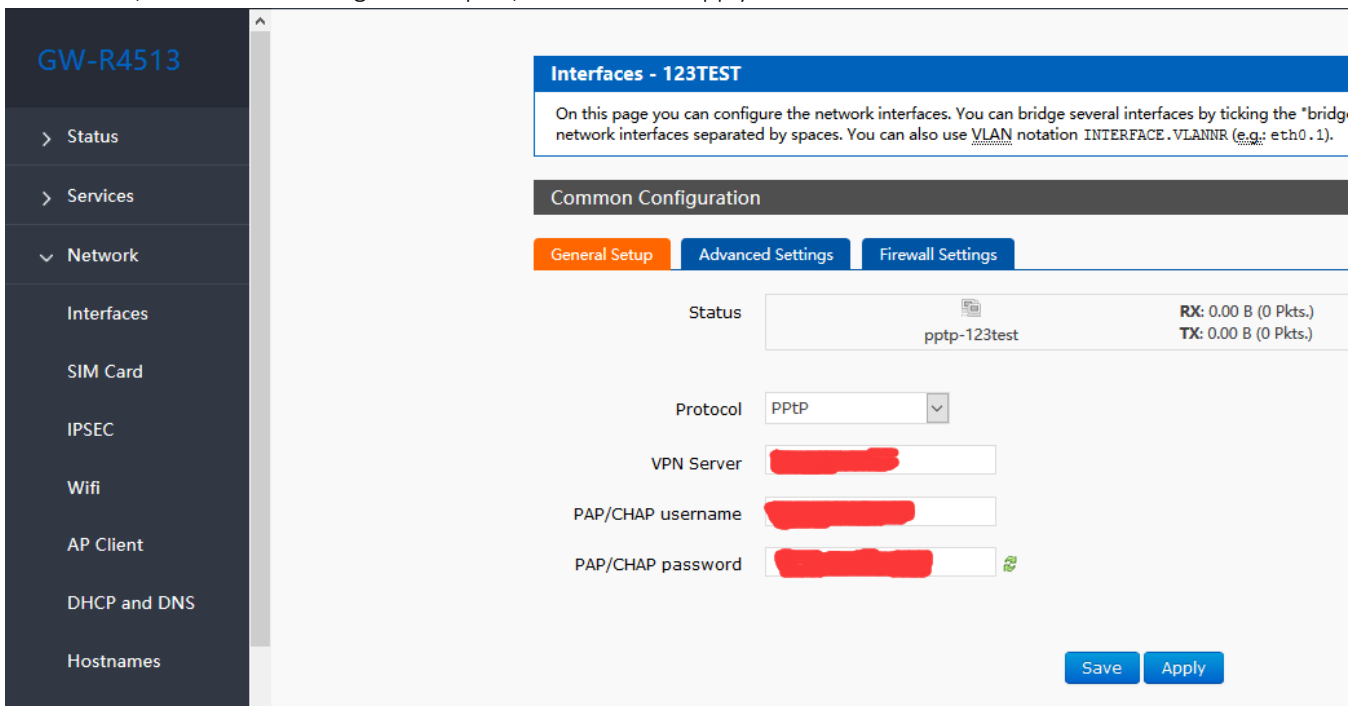


Figure32 the webpage3 of VPN

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.

3.4.3. 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.

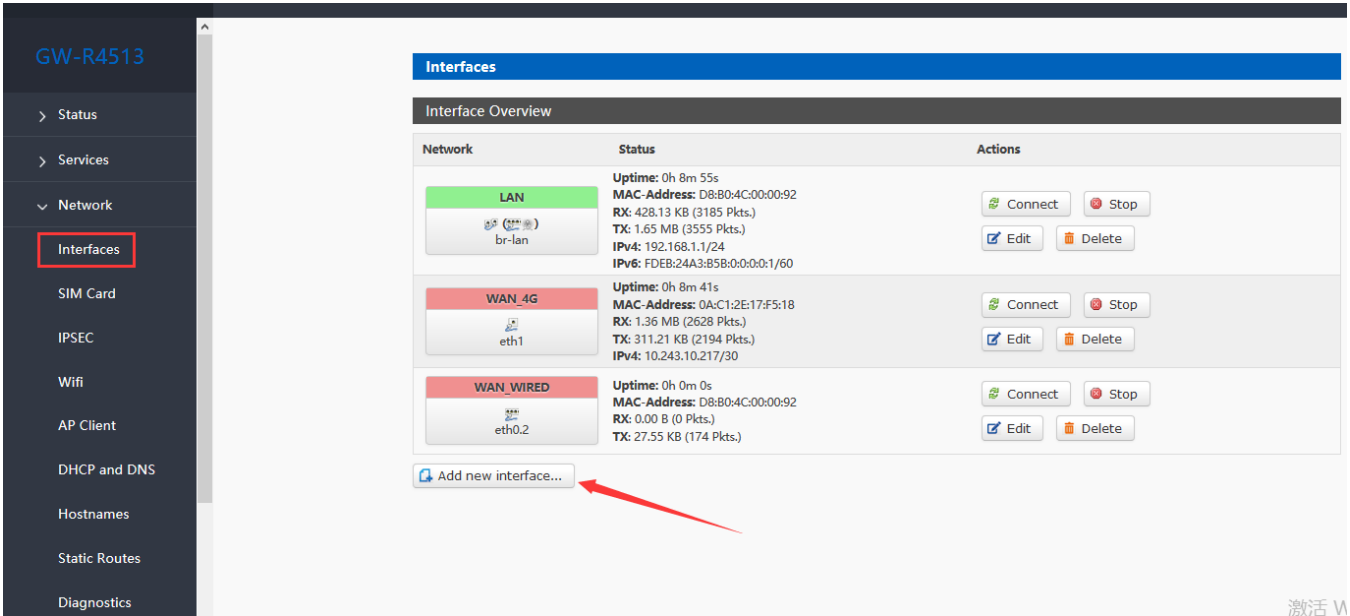


Figure33 create interface

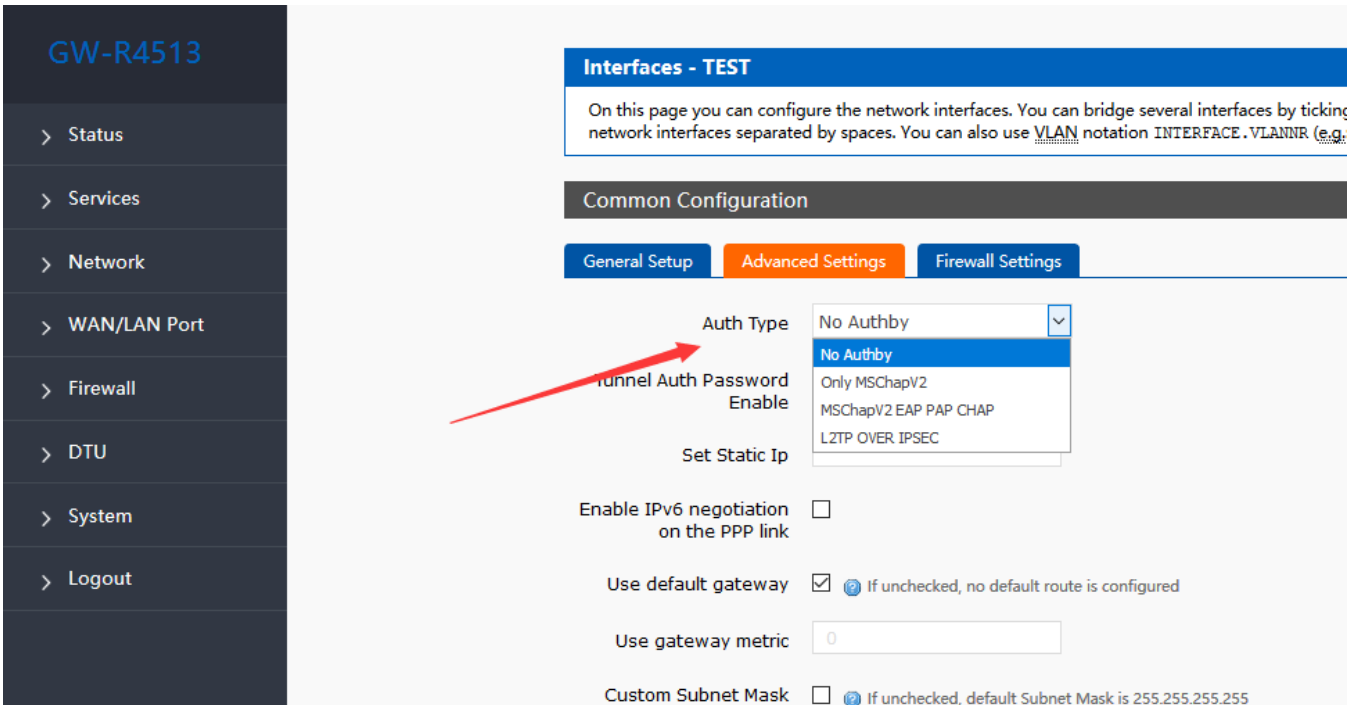


Figure34 auth type

GW-R4513

- > Status
- Services
- > Network
- > WAN/LAN Port
- > Firewall
- > DTU
- > System
- > Logout

Interfaces - TEST

On this page you can configure the network interfaces. You can bridge several interfaces by ticki network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.

Common Configuration

General Setup | **Advanced Settings** | Firewall Settings

Auth Type: No Authby

Tunnel Auth Password Enable:

Tunnel Auth Password: 123456
character: 1-16

Set Static Ip:

Enable IPv6 negotiation on the PPP link:

Use default gateway: If unchecked, no default route is configured

Use gateway metric: 0

Custom Subnet Mask Enabled: If unchecked, default Subnet Mask is 255.255.255.255

Figure34 tunnel auth password

GW-R4513

- > Status
- > Services
- > Network
- > WAN/LAN Port
- Firewall
- > DTU
- > System
- > Logout

Interfaces - TEST

On this page you can configure the network interfaces. You can bridge several ir network interfaces separated by spaces. You can also use VLAN notation INTERI

Common Configuration

General Setup | **Advanced Settings** | Firewall Settings

Auth Type: L2TP OVER IPSEC

IPSEC CONNECT NAME:

IKE Algorithm: 3DES-SHA1

SA Type: ESP

ESP Algorithm: 3DES-SHA1

PSK:

Tunnel Auth Password Enable:

Tunnel Auth Password: 123456
character: 1-16

Figure34 L2TP OVER IPSEC auth type

3.4.4. IPSEC

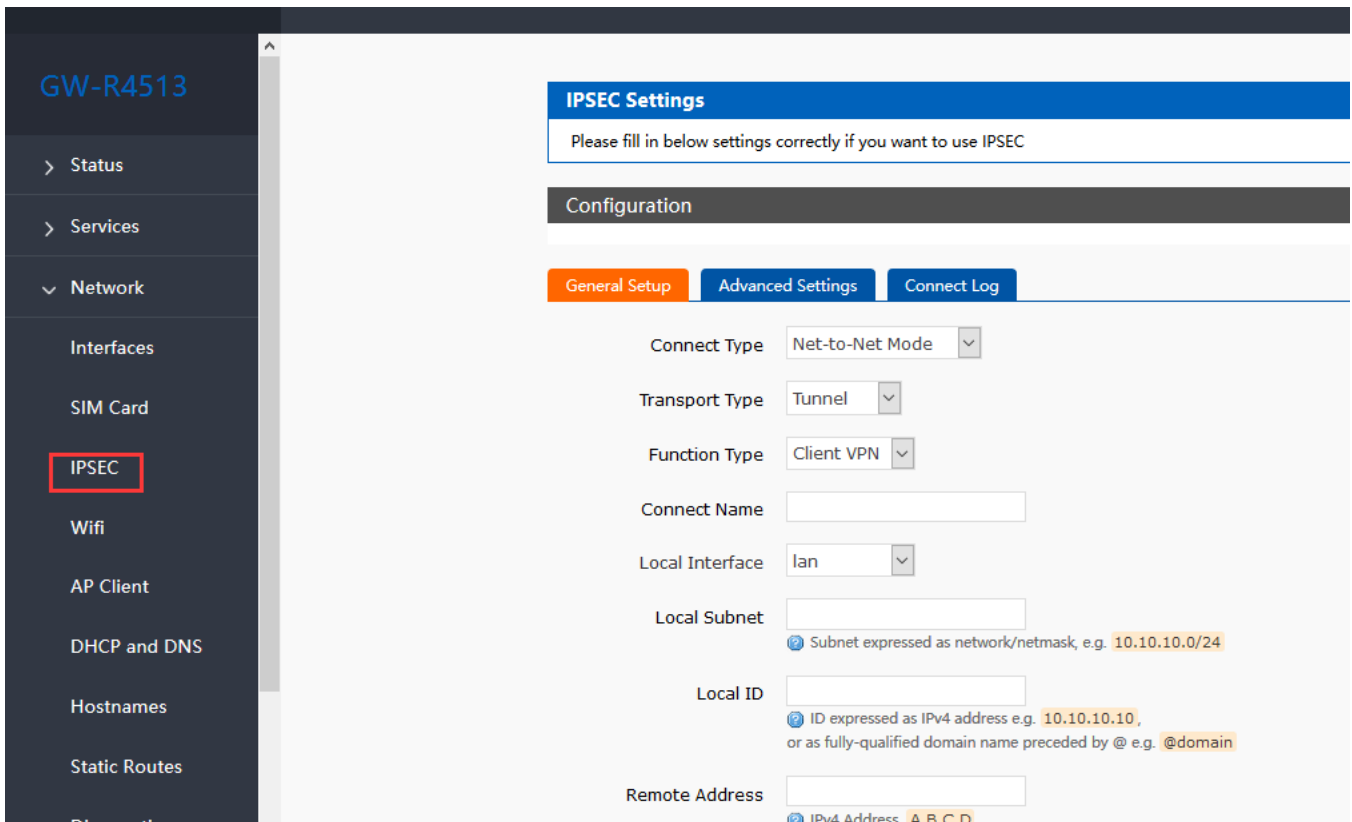


Figure34 IPSEC setting

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 @

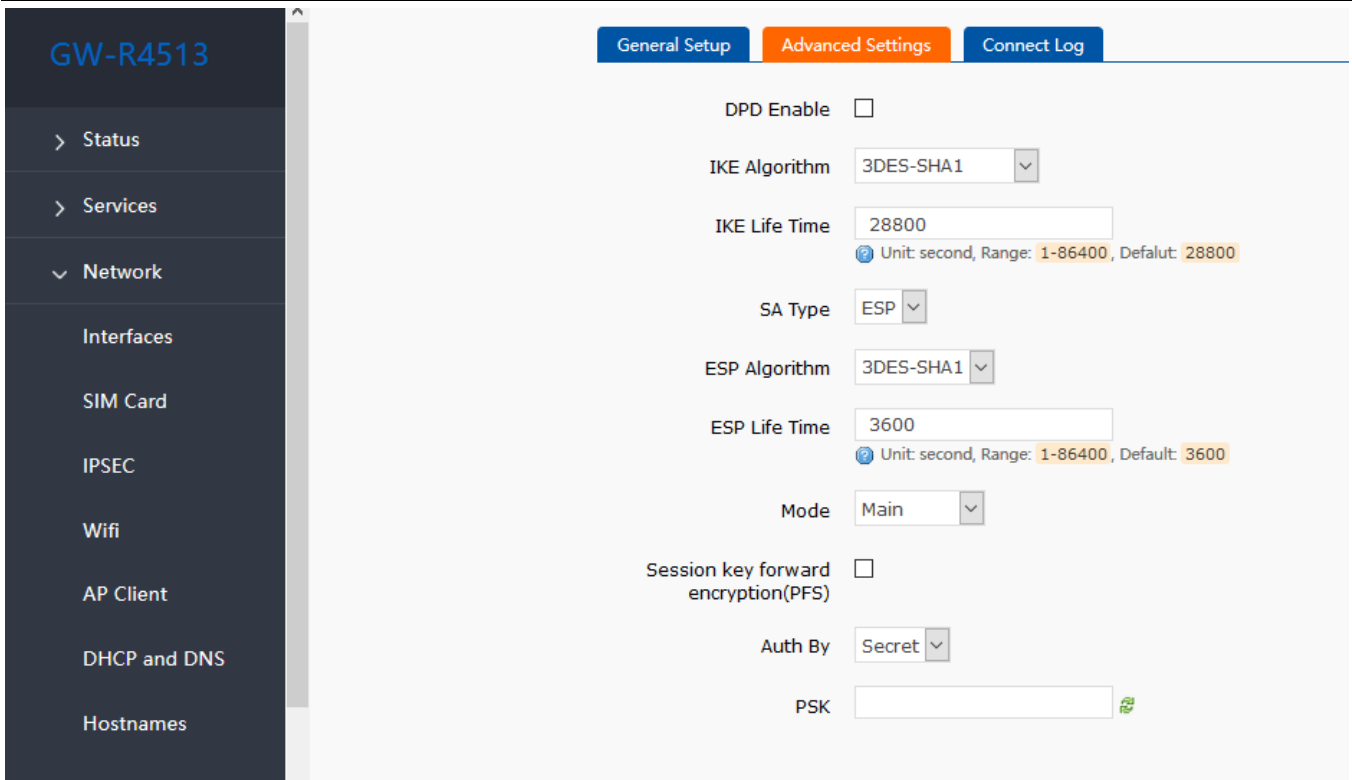


Figure35 IPSEC advance setting

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, agrmode 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.

3.4.5. OPENVPN

Add one interface, choose TUN or TAP mode:

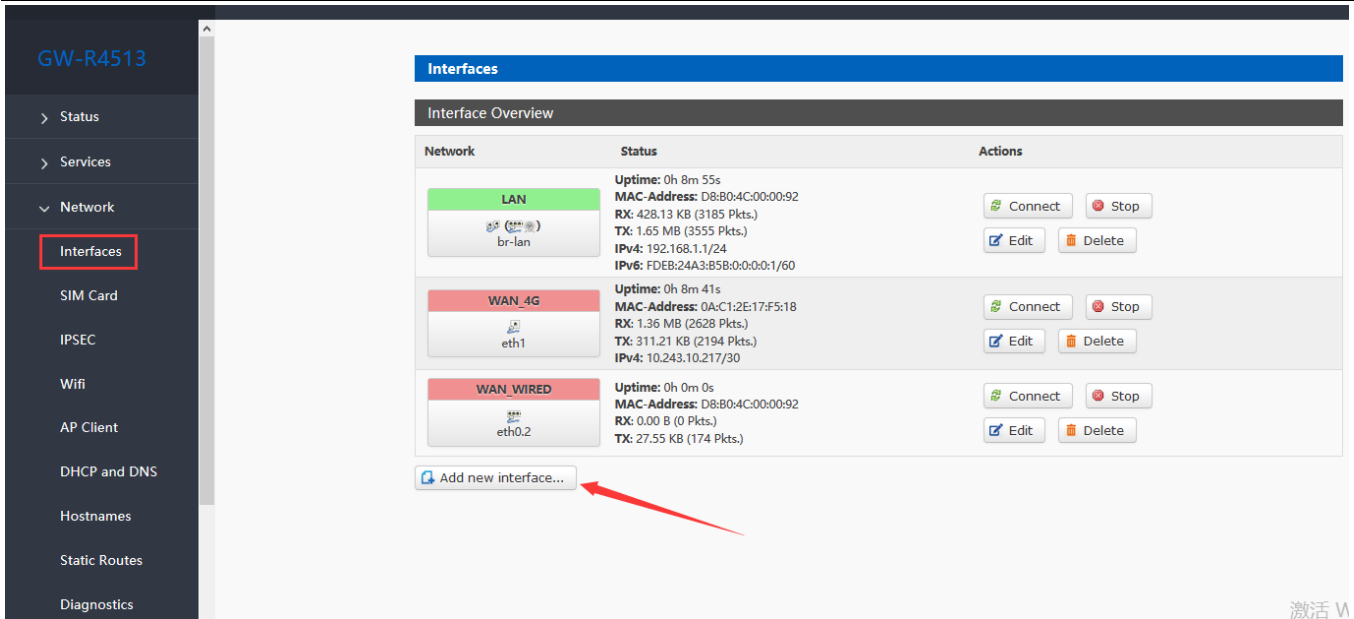


Figure36 add new interface

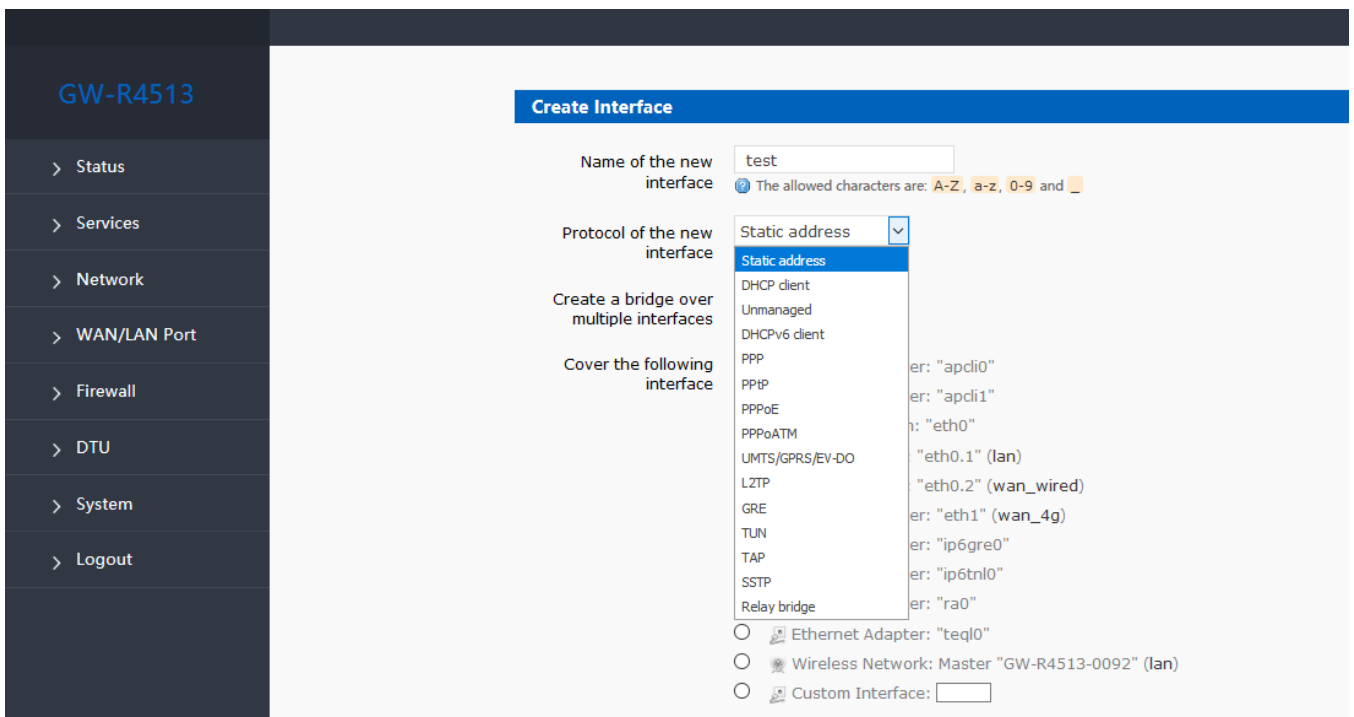
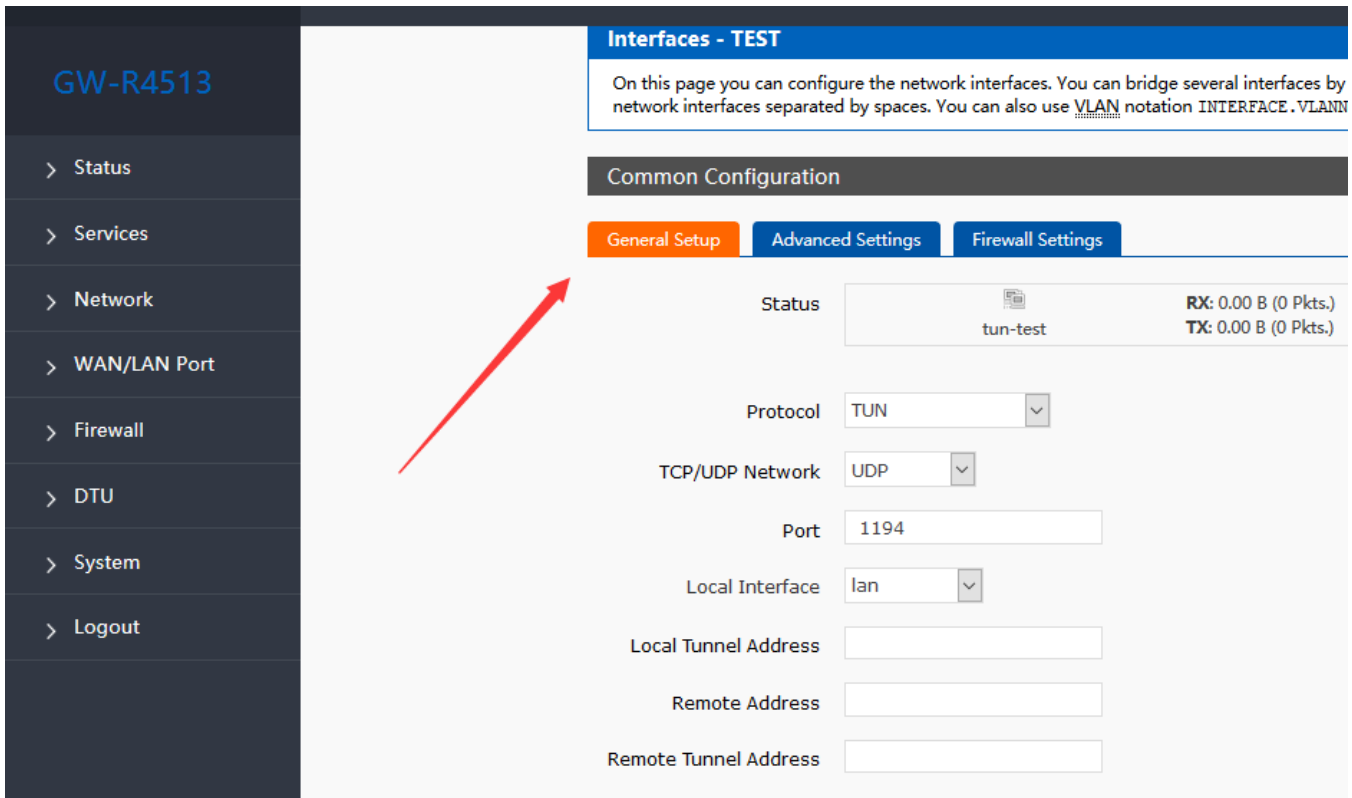


Figure37 add OPENVPN interface



GW-R4513

- > Status
- > Services
- > Network
- > WAN/LAN Port
- > Firewall
- > DTU
- > System
- > Logout

Interfaces - TEST

On this page you can configure the network interfaces. You can bridge several interfaces by network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANN

Common Configuration

General Setup | Advanced Settings | Firewall Settings

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

Protocol: TUN

TCP/UDP Network: UDP

Port: 1194

Local Interface: lan

Local Tunnel Address:

Remote Address:

Remote Tunnel Address:

Figure38 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.

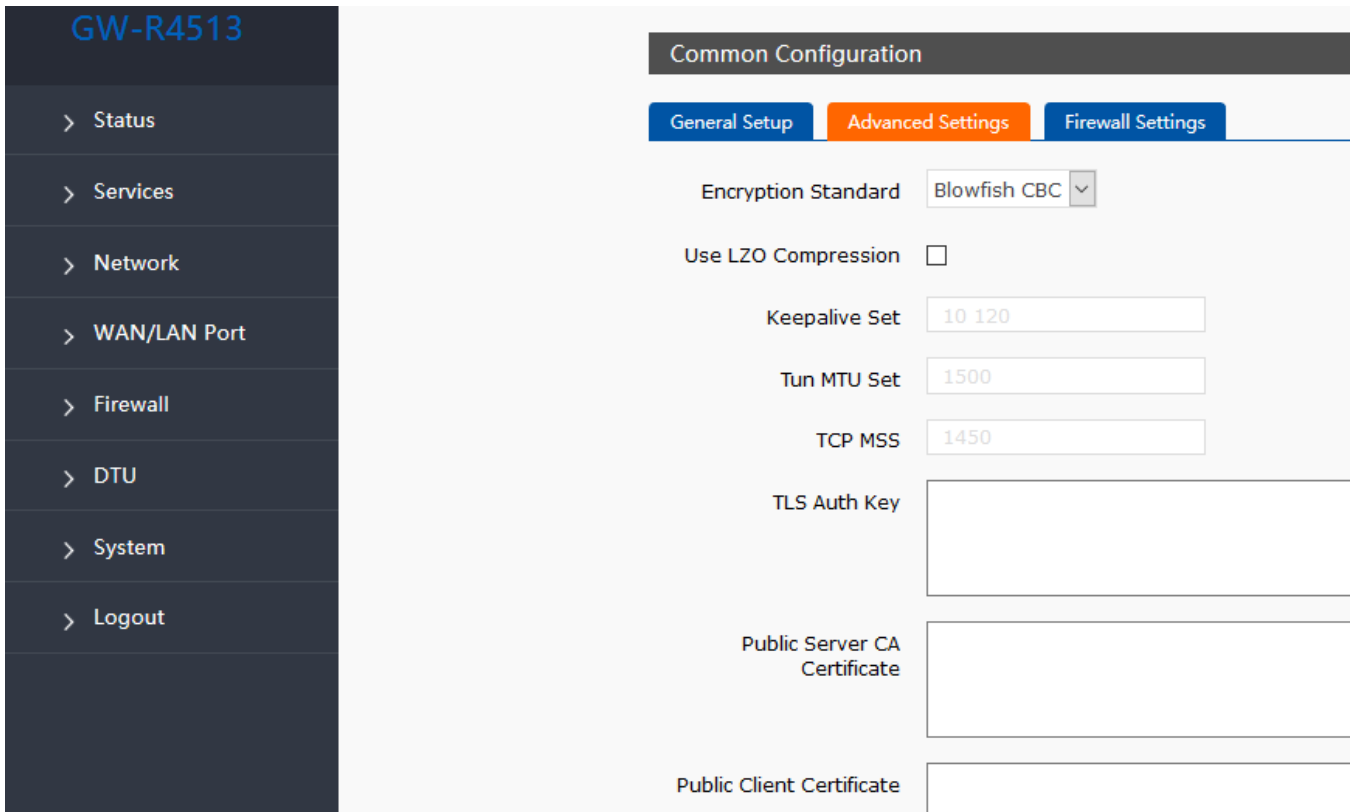


Figure39 advance setting

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.

3.4.6. GRE

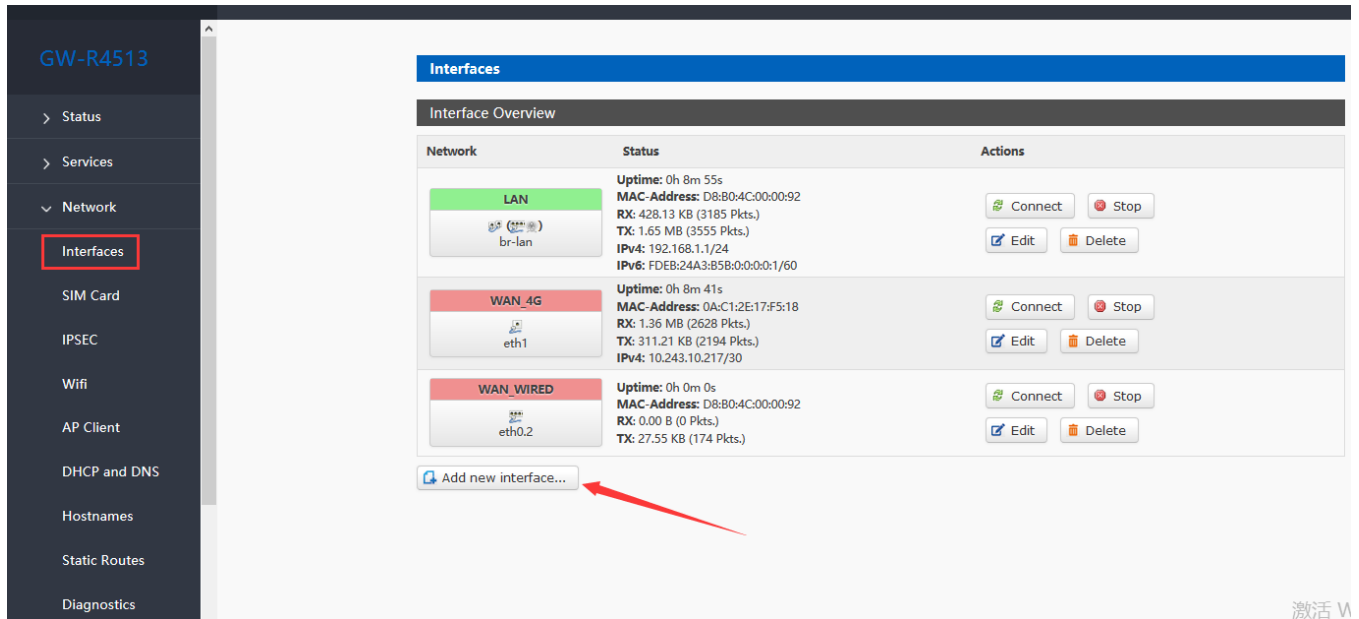


Figure40 add new interface

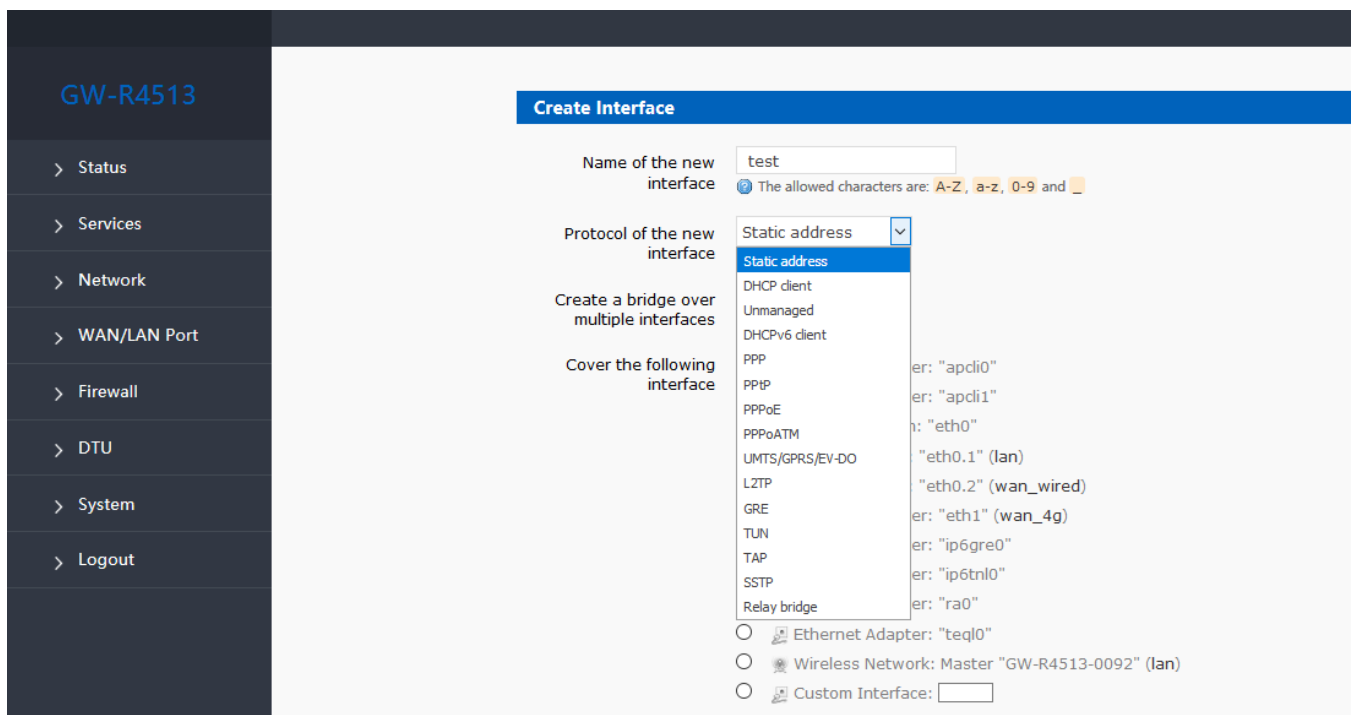


Figure41 add GRE interface

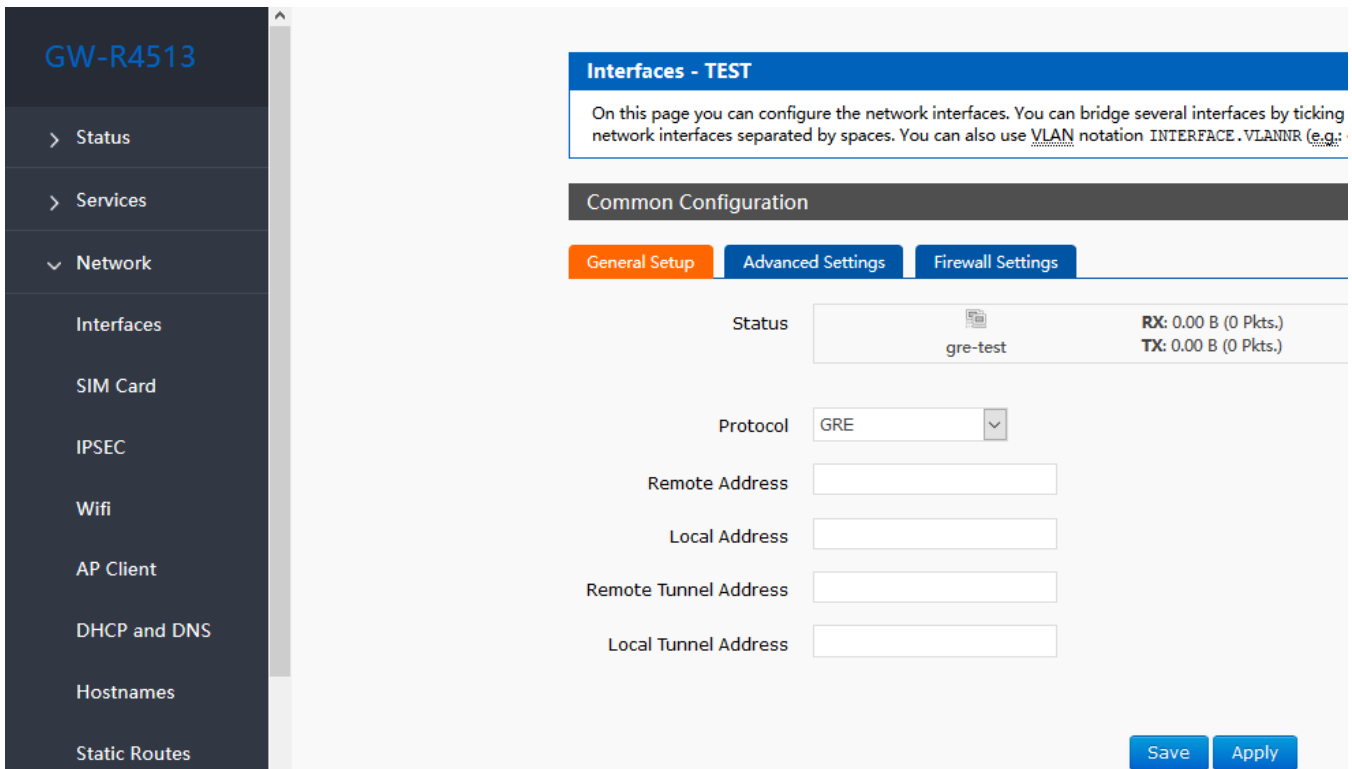


Figure42 GRE general setting

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

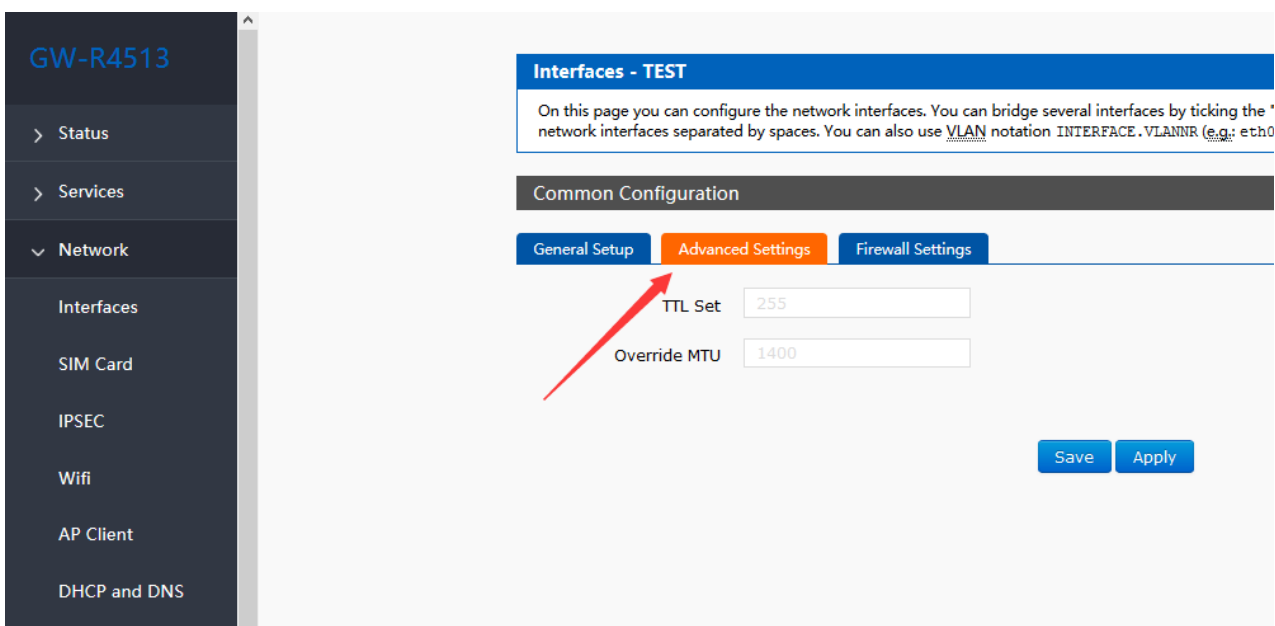


Figure43 GRE advance setting

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

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

3.4.7. SSTP Client

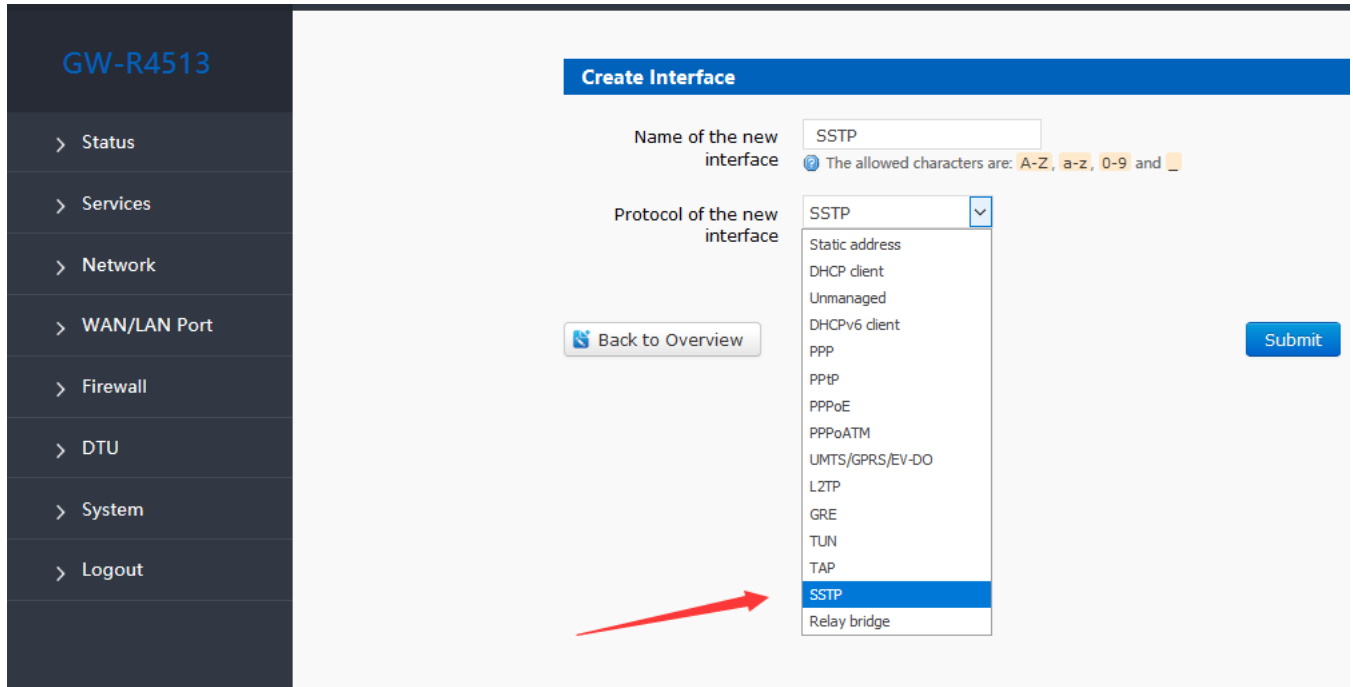


Figure44 add new interface

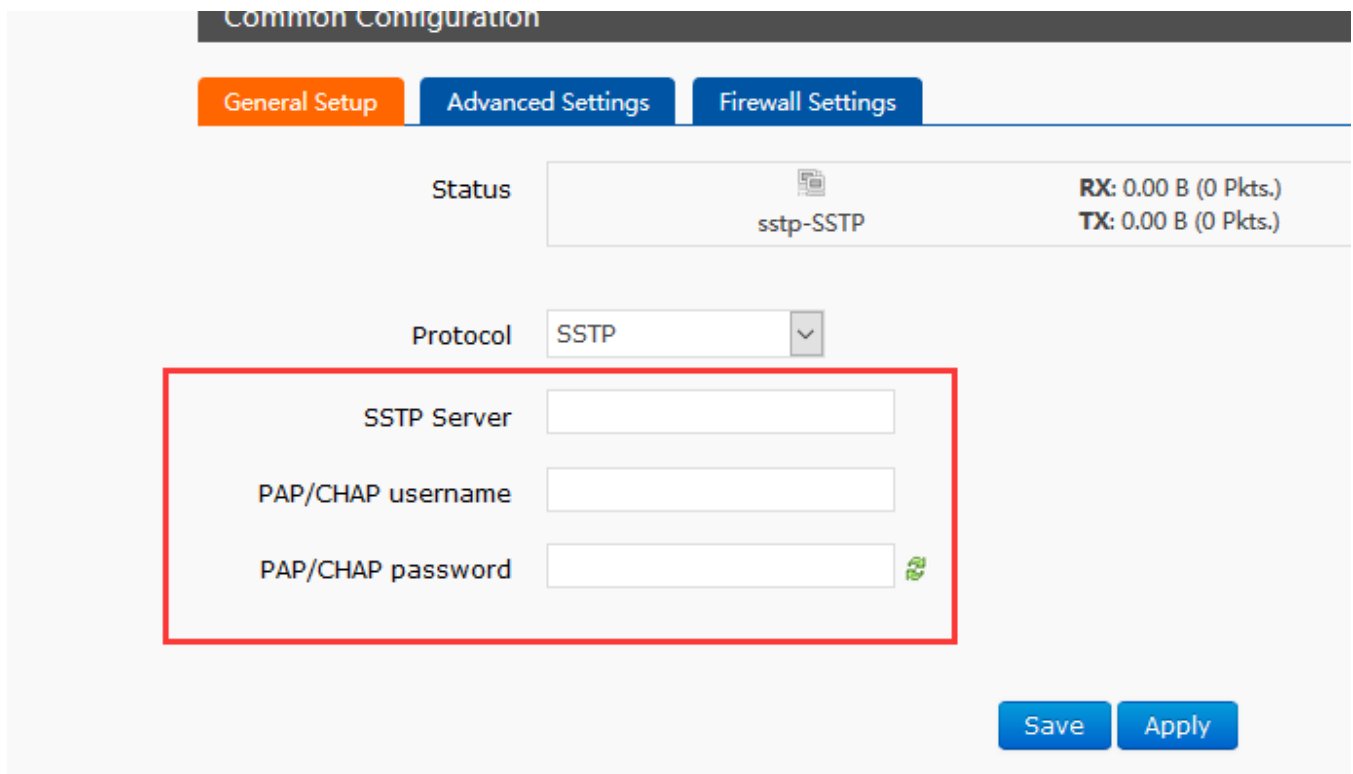


Figure45 SSTP general setting

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

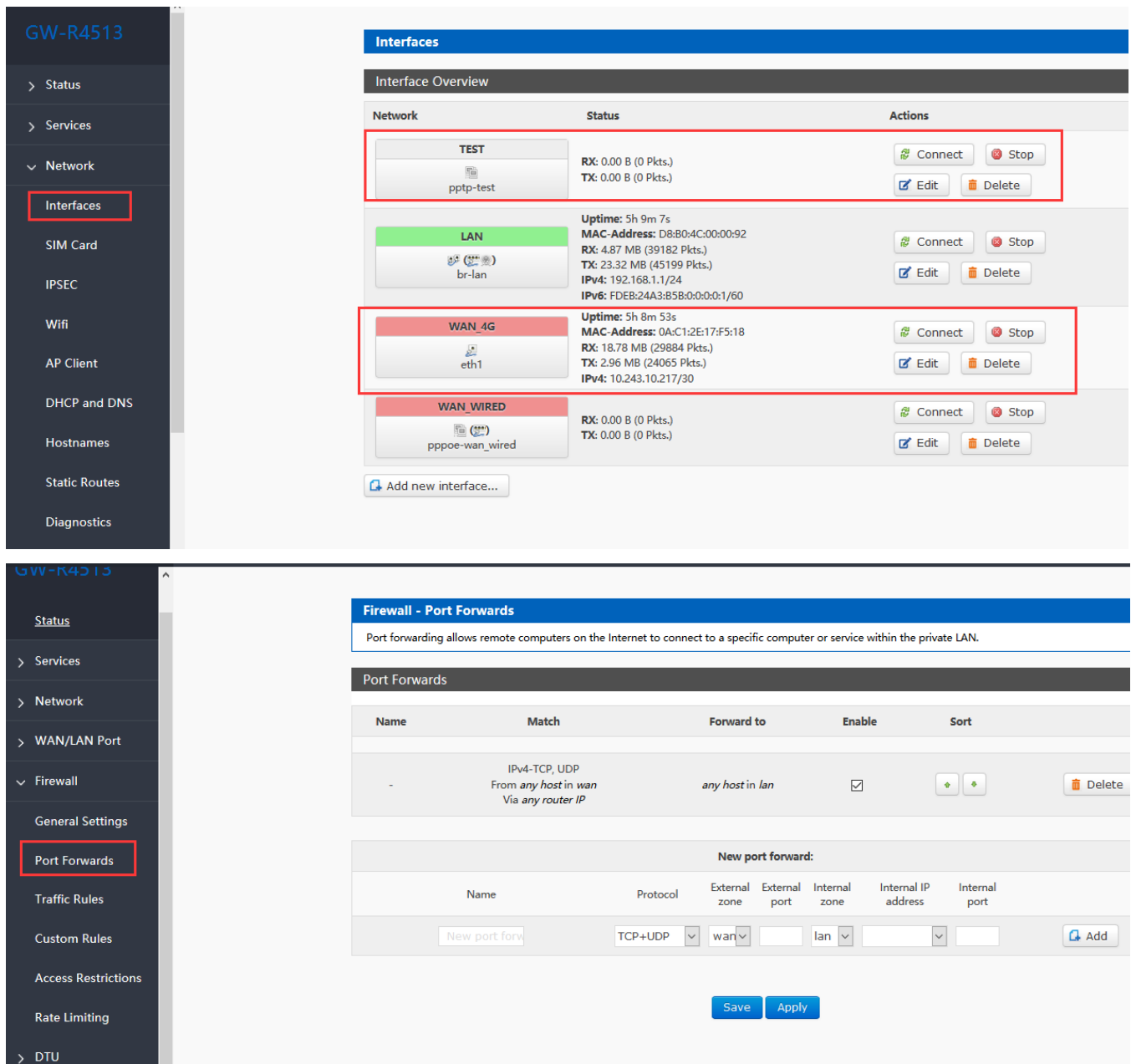
Note

Advanced settings can refer to advanced settings of PPTP.

3.5. VPN+ Port Forward

VPN+ port forward, can realize remote access between 4G routers.

Devices under routers can directly communicate with socket by port forwards.



The image shows two screenshots of the GW-R4513 web interface. The top screenshot displays the 'Interfaces' section, where the 'WAN_4G' interface (eth1) is highlighted with a red box. The bottom screenshot displays the 'Firewall - Port Forwards' section, where a port forward rule is shown with a red box around the 'Port Forwards' menu item in the sidebar.

Interfaces Section:

Network	Status	Actions
TEST pptp-test	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
LAN br-lan	Uptime: 5h 9m 7s MAC-Address: D8:80:4C:00:00:92 RX: 4.87 MB (39182 Pkts.) TX: 23.32 MB (45199 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDEB:24A3:B5B:0:0:0:0:1/60	Connect Stop Edit Delete
WAN_4G eth1	Uptime: 5h 8m 53s MAC-Address: 0A:C1:2E:17:F5:18 RX: 18.78 MB (29884 Pkts.) TX: 2.96 MB (24065 Pkts.) IPv4: 10.243.10.217/30	Connect Stop Edit Delete
WAN_WIRED pppoe-wan_wired	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete

Firewall - Port Forwards Section:

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

Name	Match	Forward to	Enable	Sort
-	IPv4-TCP, UDP From any host in wan Via any router IP	any host in lan	<input checked="" type="checkbox"/>	+ - Delete

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forw	TCP+UDP	wan		lan		

Buttons: Save, Apply, Add

Figure46 port forwards

The WAN port is not inserted, only using 4G interface, and create a VPN Client interface.

1\two PC, 4G router one (using 4G interface)

2\The IP address obtained by the WAN_4G interface is 192.168.109.7

3\Set port forwarding, external port 4444, intranet IP address 192.168.1.247 (PC1), intranet port 4444 on 192.168.1.247, create TCP Server, listen for port 4444

4\Create a TCP Client on a PC 2 (note that PC2 is on another network, not under this router) with the target IP address 192.168.109.7 and the target port 4444, which should be able to connect to the TCP Server under the 4G router and communicate.

3.6. Host Names

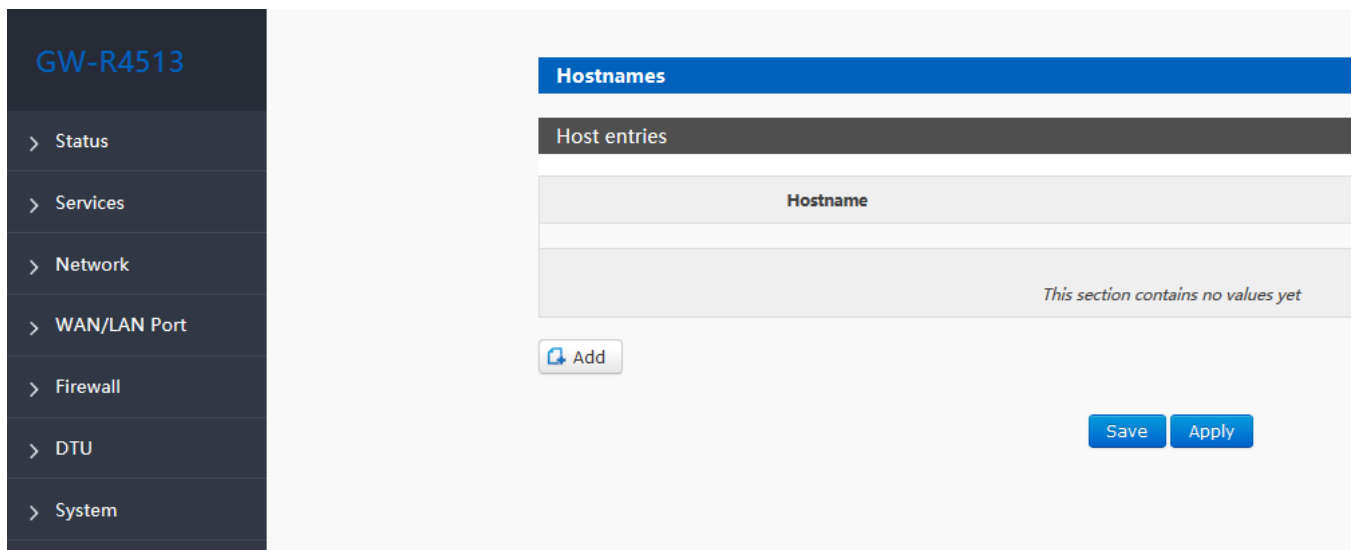


Figure47 host names

Routers can implement custom domain name resolution. Set the hostname (domain name) you want, such as "pc-linux" to the hostname, with the corresponding IP address 192.168.0.9. In this way, the mapping relationship between host name and IP address can be realized.

Note that this function will effect after the router restart.

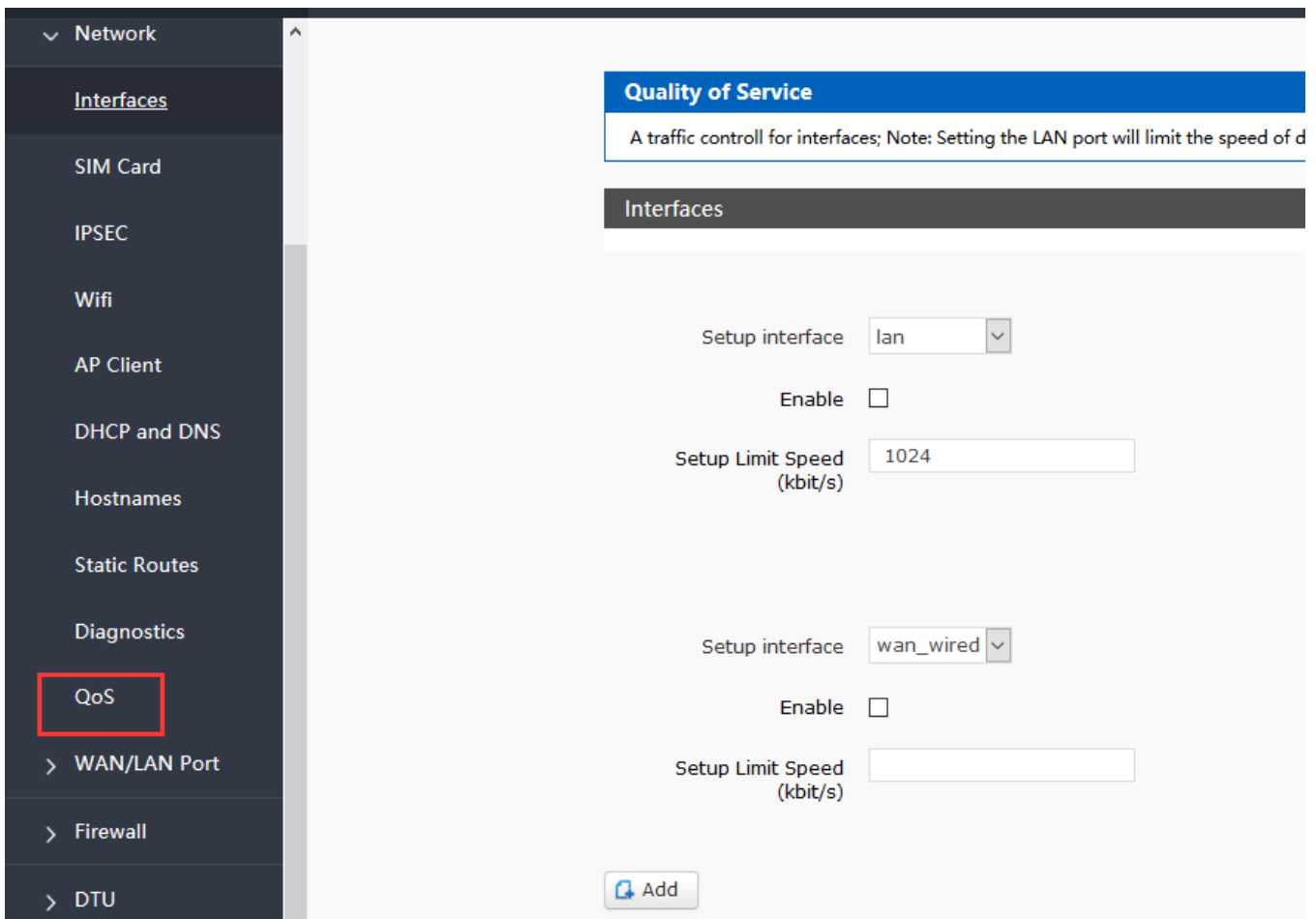
3.7. Static Router

Table8 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.

3.8. Setup Limit Speed



Setup interface	Enable	Setup Limit Speed (kbit/s)
lan	<input type="checkbox"/>	1024
wan_wired	<input type="checkbox"/>	

Figure48 setup limit speed

3.9. Firewall

3.9.1. General Setting

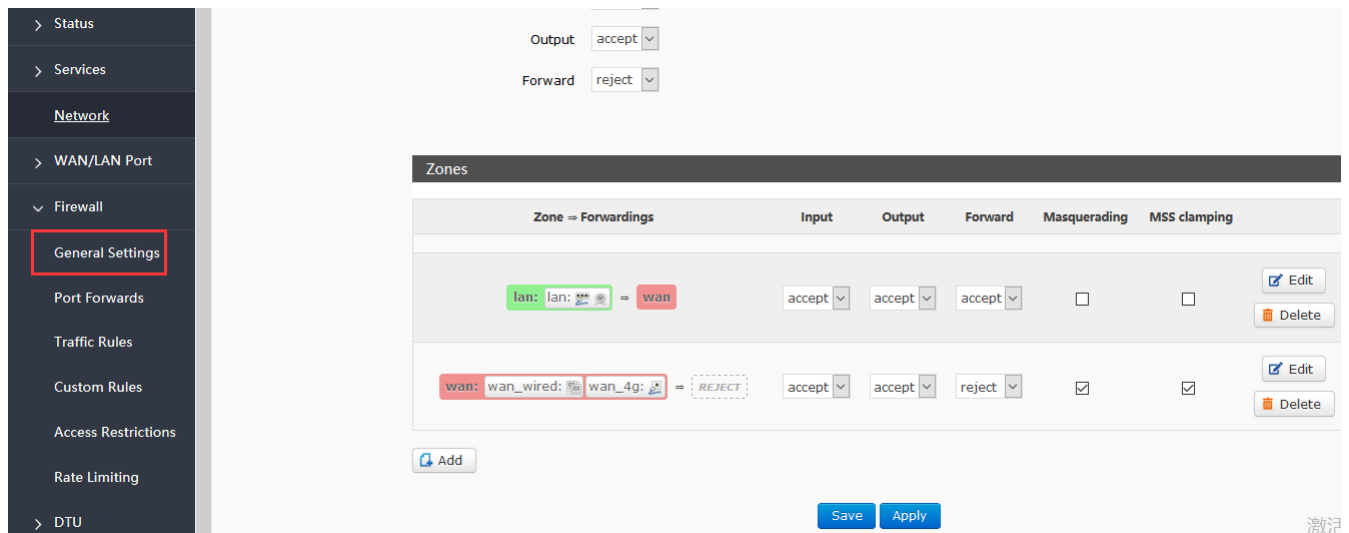


Figure49 general setting of firewall

Rule 1

LAN port to the cable WAN port inbound and forwarding, are accepted.

If a packet comes from a LAN port and wants to access the WAN port, this rule allows packets to be forwarded from the LAN port to the WAN port, which is forwarding.

You can also open the router's web page at LAN port, which is called "inbound".

The router connects to the external network, such as synchronization time, which belongs to "outbound".

Rule 2

Wired WAN port and 4G port, accept "inbound", accept "outbound", refuse to "forward".

If there are "inbound" packets, such as someone trying to log in to a router page from a WAN port, then they will be allowed

If there are "outbound" packets, such as routers accessing the extranet through a WAN or 4G port, this action is allowed

If there is a "forward" packet, such as a packet from a WAN port that wants to forward to a 4G port, this action is rejected.

3.9.2. Traffic Rules

Communication rules can selectively filter specific Internet data types and block Internet access requests, thereby enhancing network security.

3.9.2.1. IP-Reject

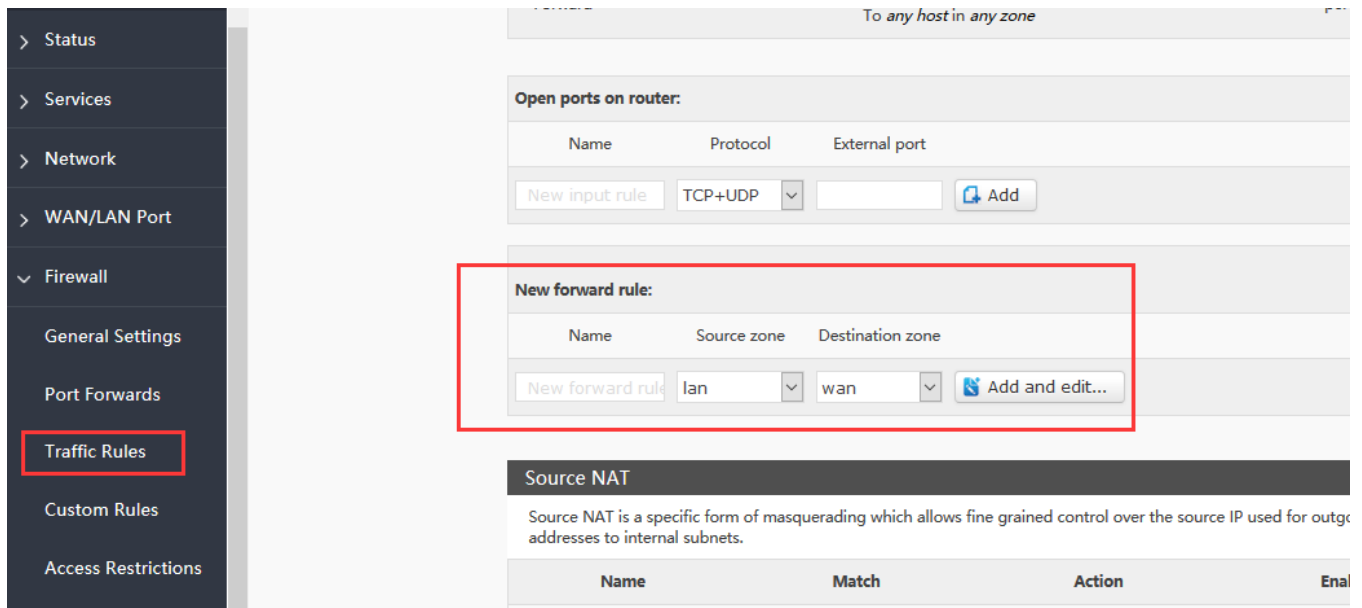


Figure50 IP-reject 1

Source area selection LAN, source MAC address and source address are all selected (if only a specific IP within the LAN is restricted to access a particular IP outside the network, then fill in the IP address or MAC address here)

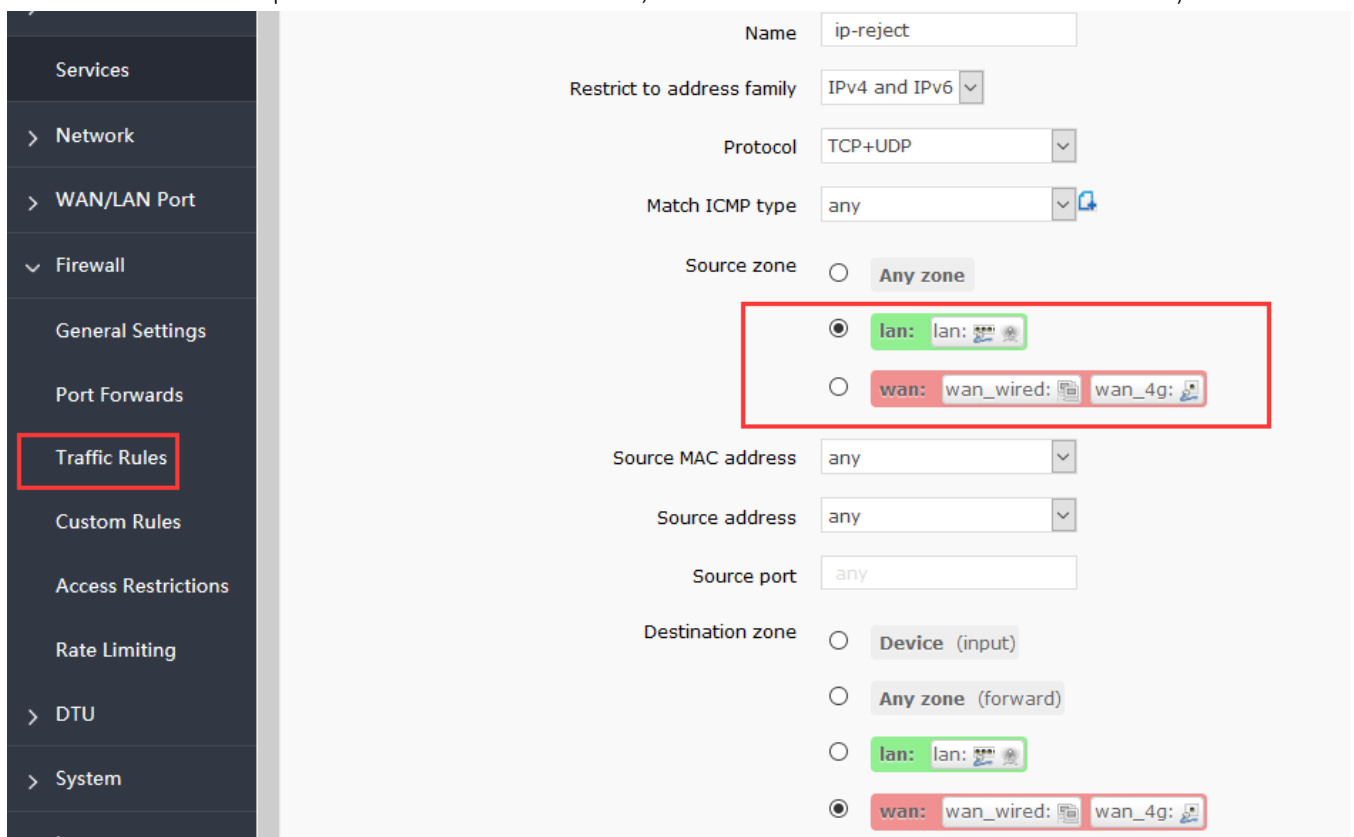


Figure51 IP-reject 2

Reject IP, and fill in the IP address, then apply and save.

The screenshot displays the 'Traffic Rules' configuration page in the USR IOT web interface. The left sidebar shows a navigation menu with 'Traffic Rules' highlighted. The main content area contains the following fields and options:

- Source MAC address: any
- Source address: any
- Source port: any
- Destination zone:
 - Device (input)
 - Any zone (forward)
 - lan: lan: [device icons]
 - wan: wan_wired: [device icons] wan_4g: [device icons]
- Destination address: any
- Destination port: any (highlighted with a red arrow)
- Action: reject
- Extra arguments: [empty field]
- Passes additional arguments to iptables. Use with care!

At the bottom, there are buttons for 'Back to Overview', 'Save', and 'Apply'.

Figure52 IP-reject 3

The screenshot shows a table of Firewall Traffic Rules. The rule 'ip-reject' is selected, and its details are displayed:

- Rule Name: ip-reject
- Direction: To any host in any zone
- Source: Any traffic From any host in lan
- Destination: To any host in wan
- Action: Refuse forward
- Buttons: Edit, Delete

Figure53 IP-reject 4

3.9.2.2. IP-Allow

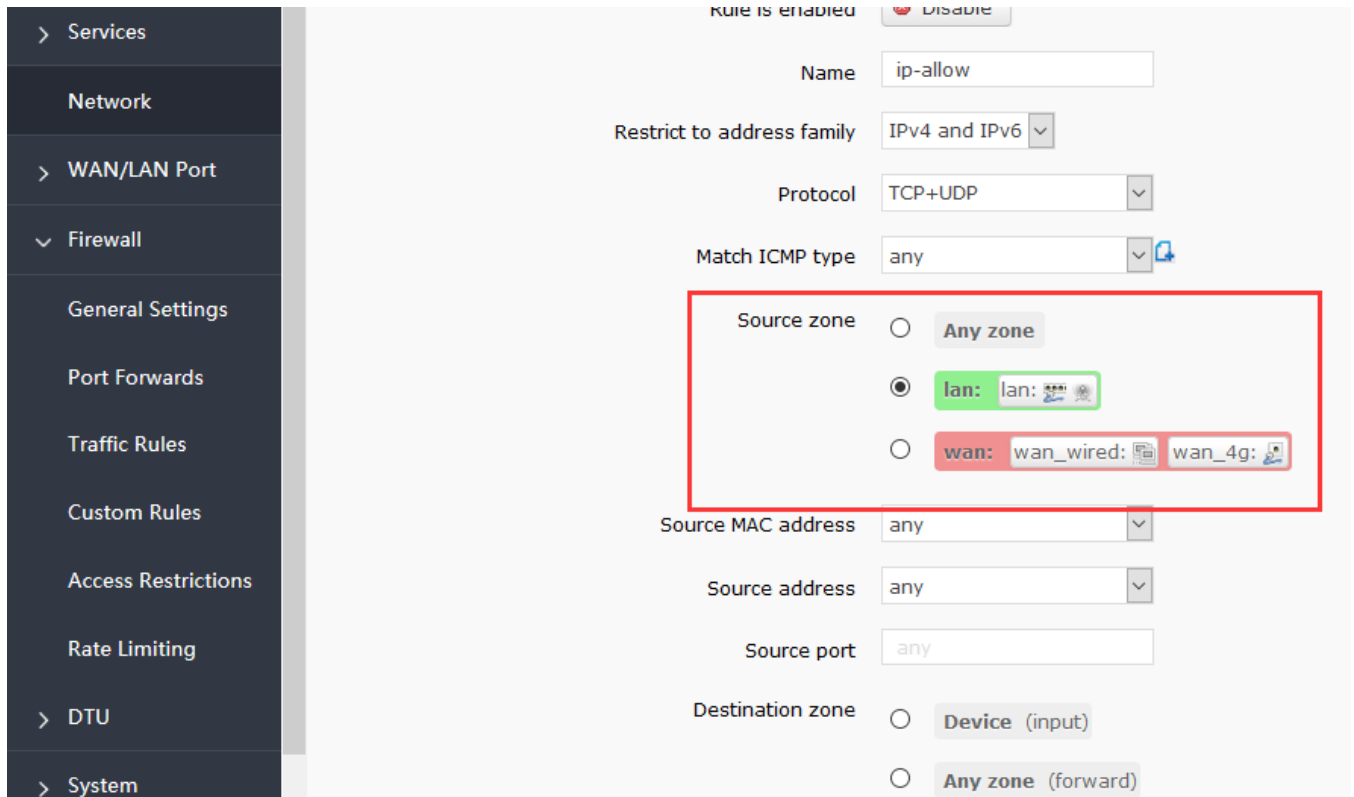


Figure54 IP-allow 1

Action: accept, then apply and save.

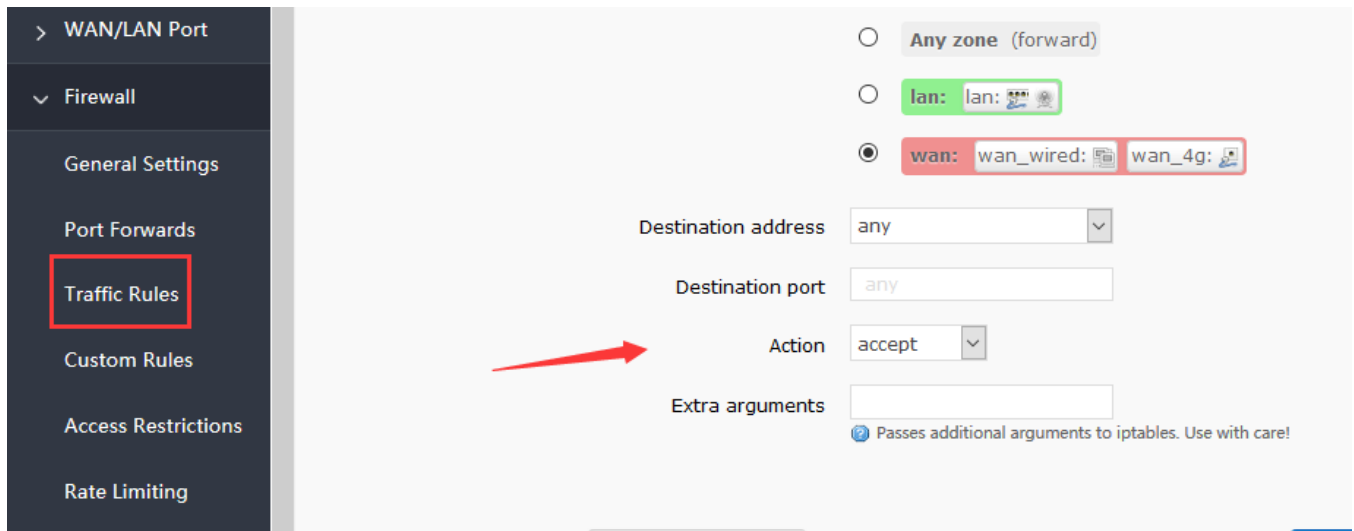


Figure55 IP-allow 2



Figure56 IP-allow 3

Next, set a rule that all communications are rejected. The source address is set to All , the target address is set to All, and the action selection is rejected. Note that the order of the two rules must be the rule of allow before, and the rule of rejection is later.

3.9.3. NAT Function

3.9.3.1. MASQ

MASQ, MASQUERADE, 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.

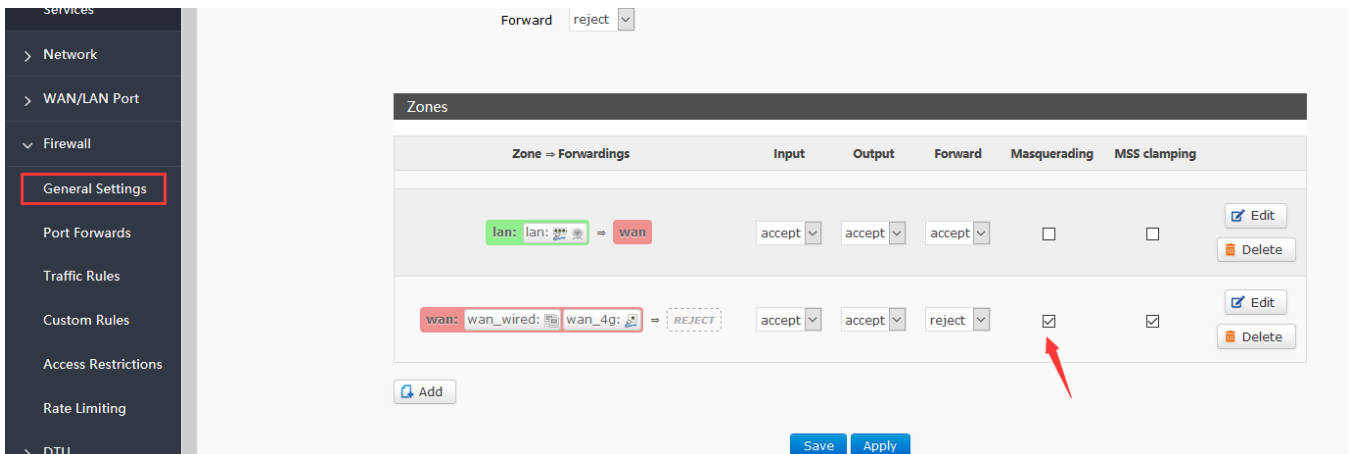


Figure57 MASQ setting

3.9.3.2. 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.

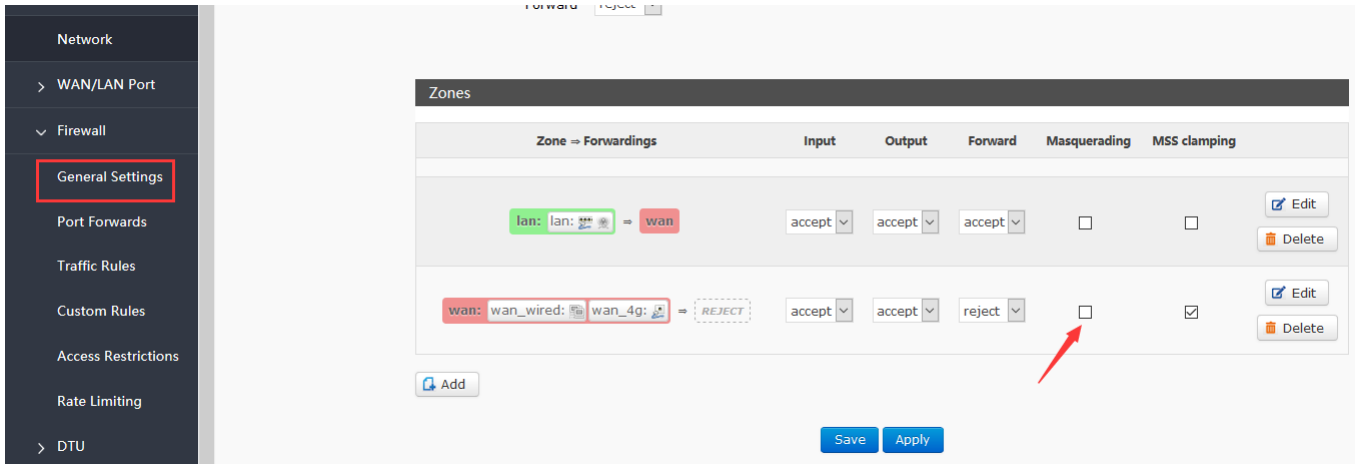


Figure58 close MASQ

Then setup SourceNAT.

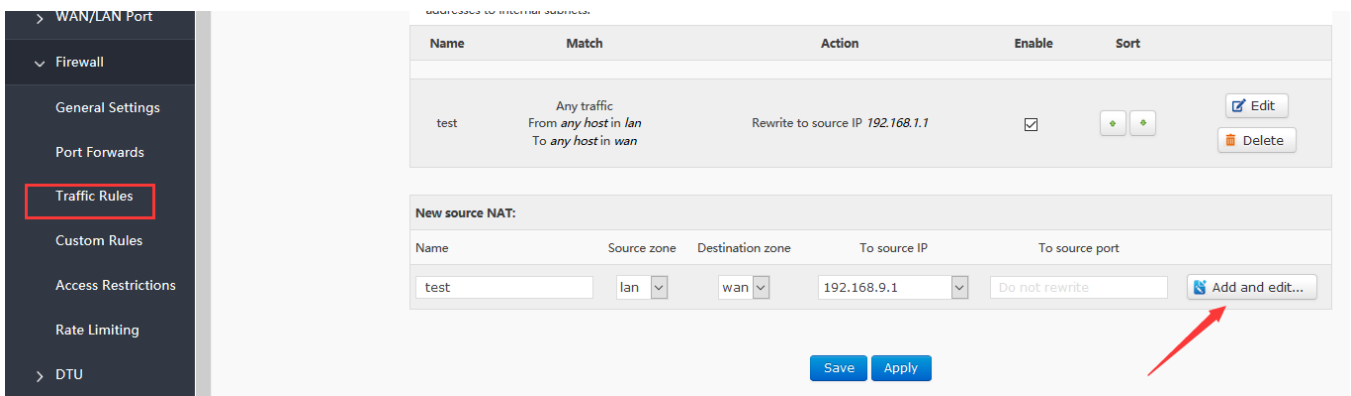


Figure59 NAT setting1



Figure60 NAT setting2

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

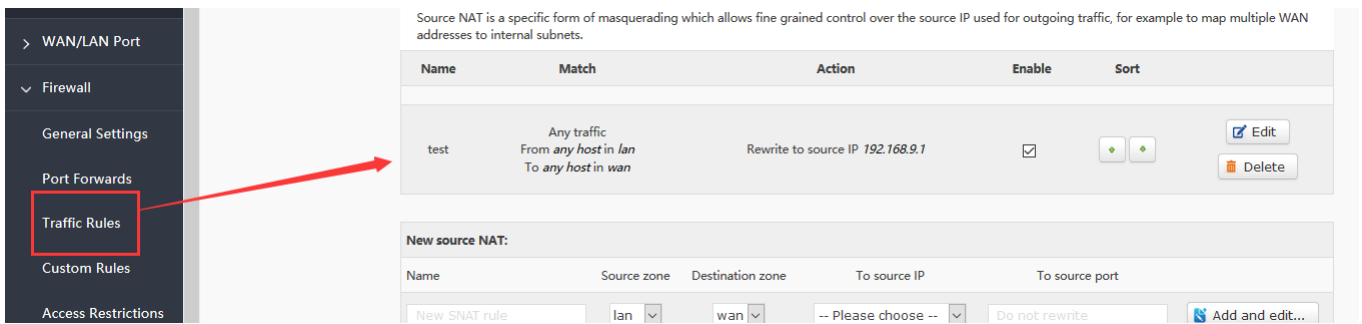


Figure61 NAT setting3

3.9.3.3. 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

3.9.3.3.1. Port Forward

3.9.3.3.1.1. Introduce

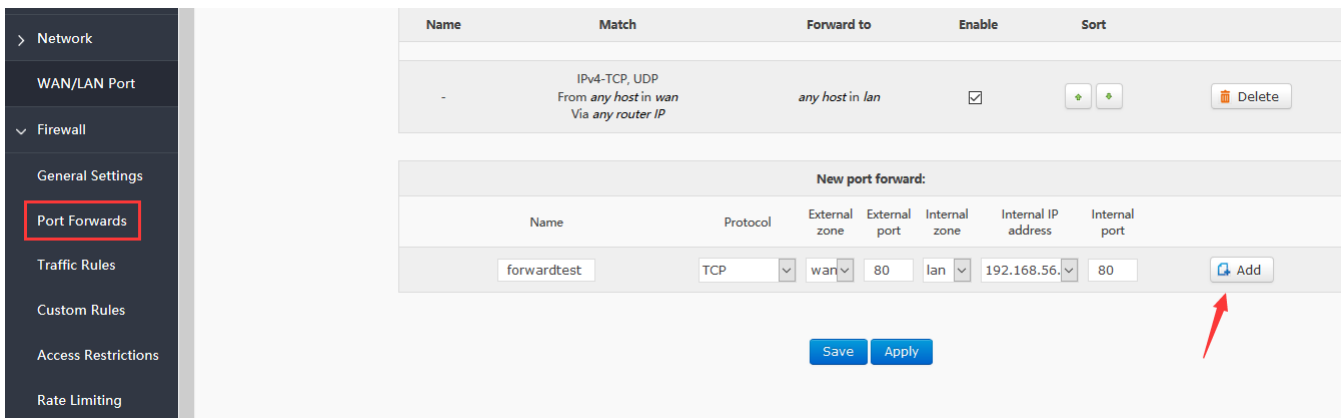


Figure62 port forward setting1

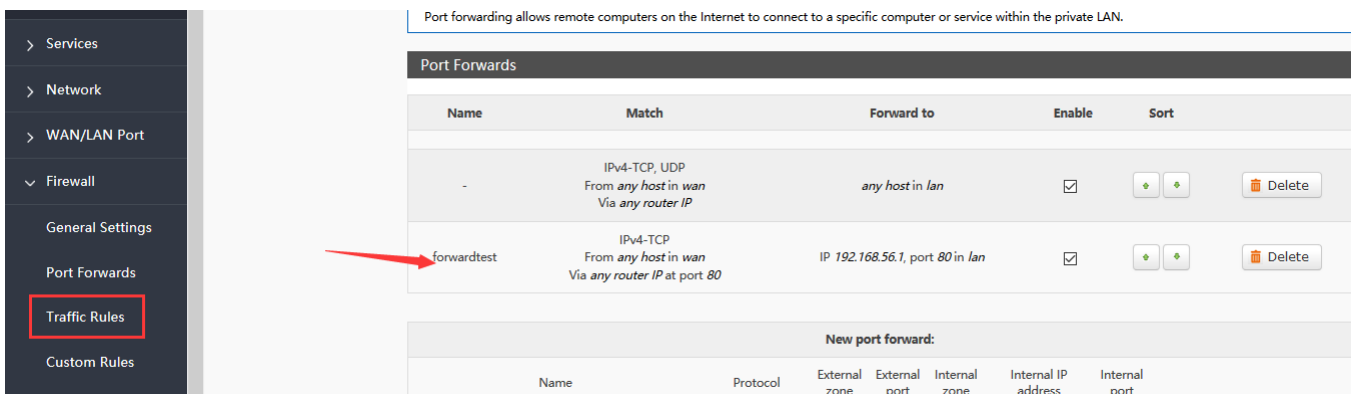


Figure63 port forward setting2

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.

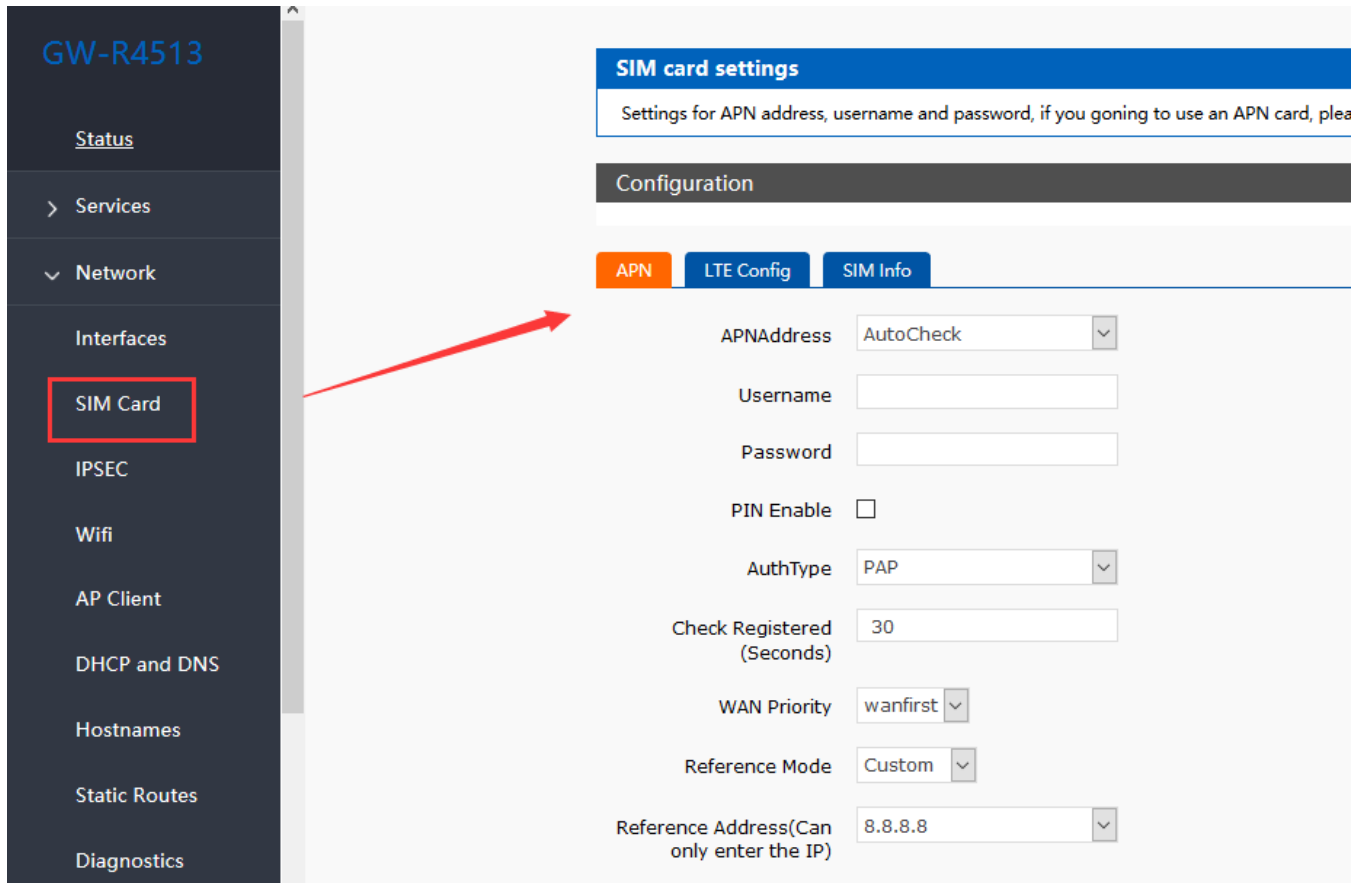
When we access the 81 port from the WAN port, the access request will be transferred to 192.168.1.1:80.

3.9.3.3.1.2. 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.



The screenshot shows the 'SIM card settings' configuration page. The left sidebar is titled 'GW-R4513' and includes a menu with 'SIM Card' highlighted. The main content area has tabs for 'APN', 'LTE Config', and 'SIM Info'. The 'APN' tab is active, showing the following settings:

- APNAddress: AutoCheck
- Username: [text input]
- Password: [text input]
- PIN Enable:
- AuthType: PAP
- Check Registered (Seconds): 30
- WAN Priority: wanfirst
- Reference Mode: Custom
- Reference Address(Can only enter the IP): 8.8.8.8

Figure64 4G port forward setting1

Then, add the port forward.

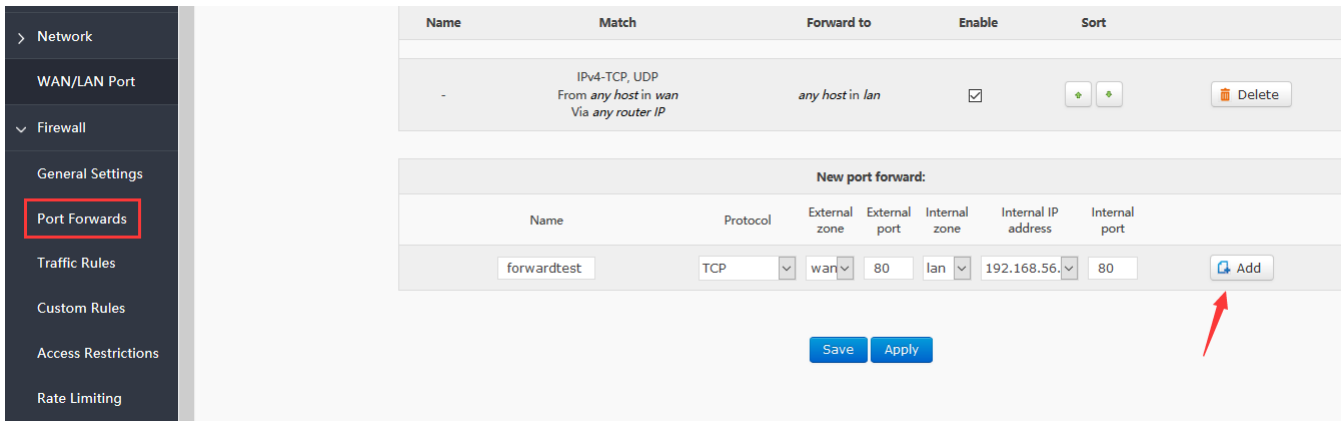


Figure65 4G port forward setting2

After setup all parameters, restart the router.

3.9.3.3.2. 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.

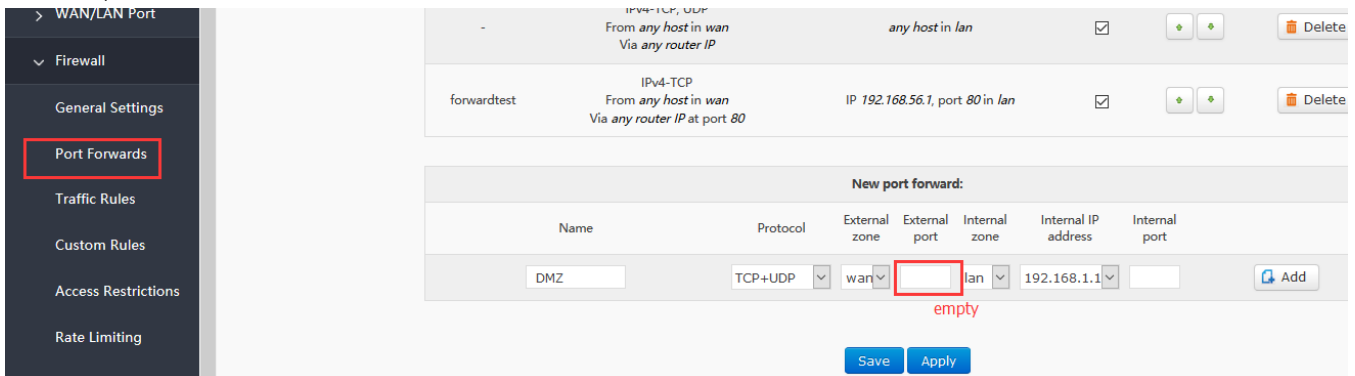


Figure66 DMZ setting1

Then add and save.

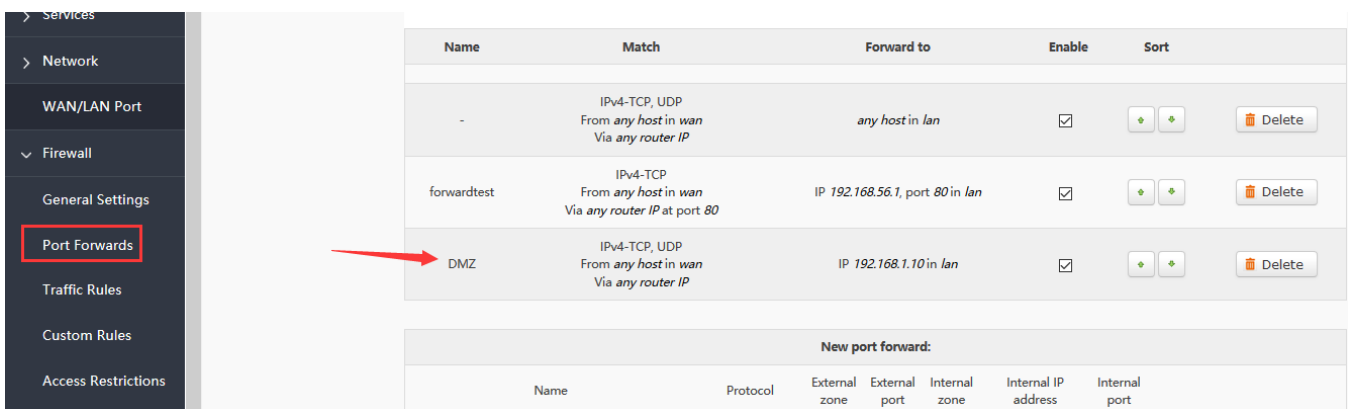


Figure67 DMZ setting2

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.

3.9.4. Custom Rules

Custom rules can implement the preceding functions and need to write commands to run. Support Iptables command.

3.9.5. 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

3.9.5.1. Domain Blacklist

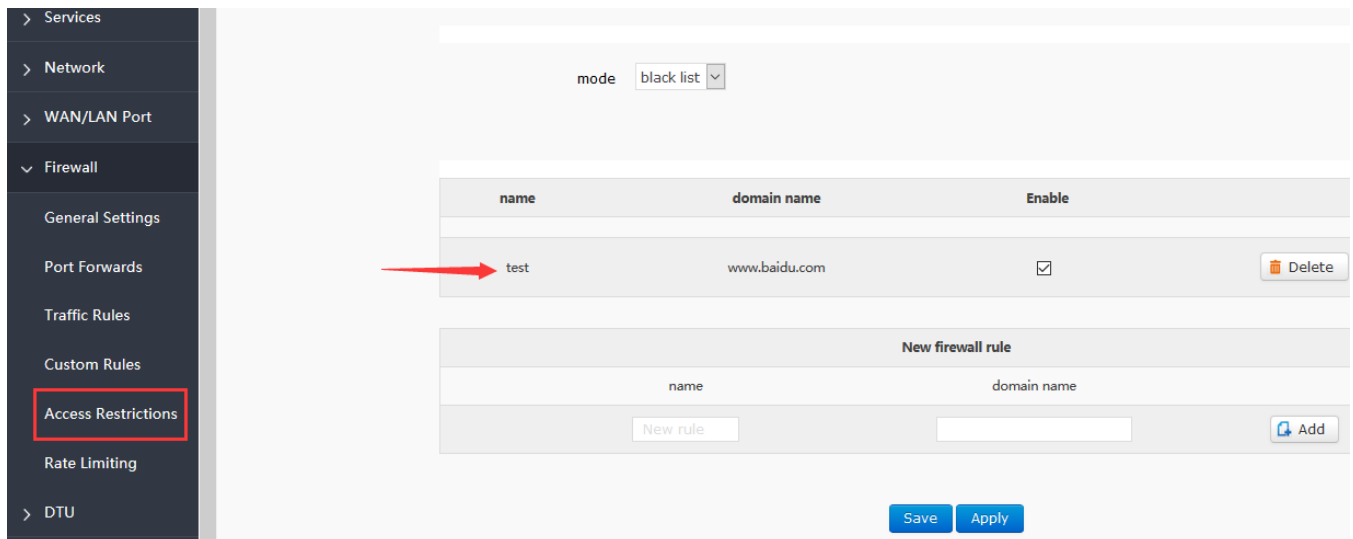


Figure68 blacklist

3.9.5.2. Whitelist

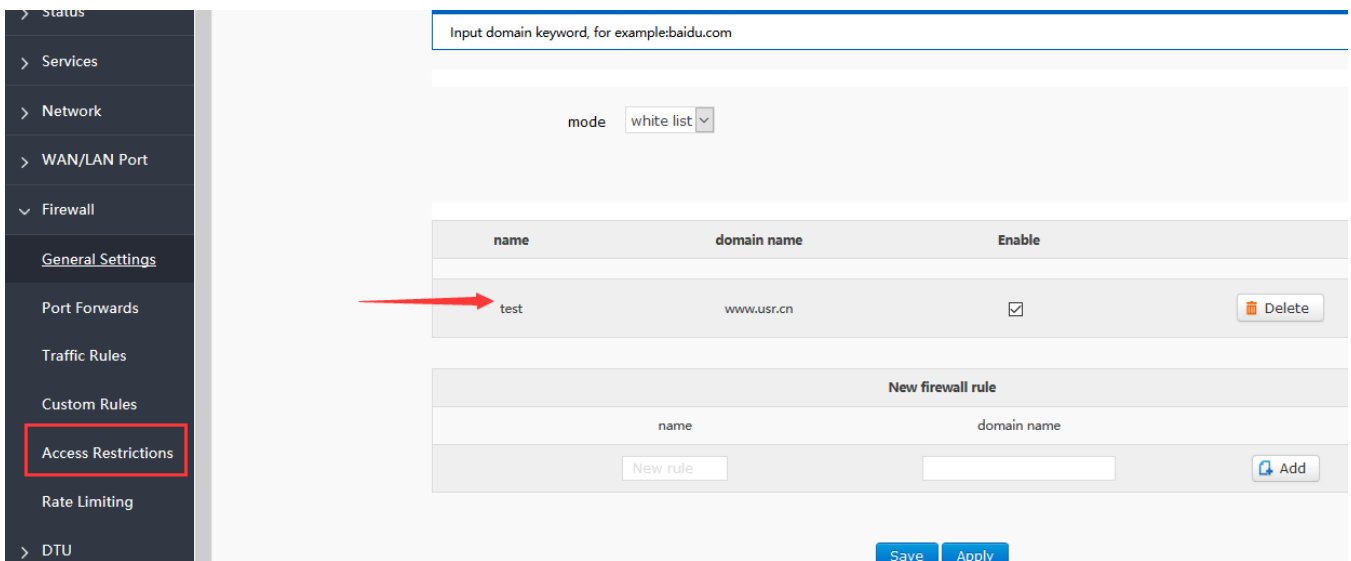


Figure69 whitelist

3.9.6. 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. IP segment speed limit, need to fill in the initial IP address, termination IP address, downlink rate, uplink rate, MAC address speed limit, need to select MAC, fill in the uplink rate, downlink rate, then save immediately take effect. The minimum uplink downlink rate is 10KB/S. If the set value is less than 10, it will be processed by 10. As shown in figure 192.168.1.10-192.168.1.100, the maximum upstream and downstream rate of the network is 100KB/S, and the maximum upstream and downstream rate of the network is 200KB/S for MAC address: 00:25:AB:84:66:6E. The downlink rate is usually greater than the uplink speed.

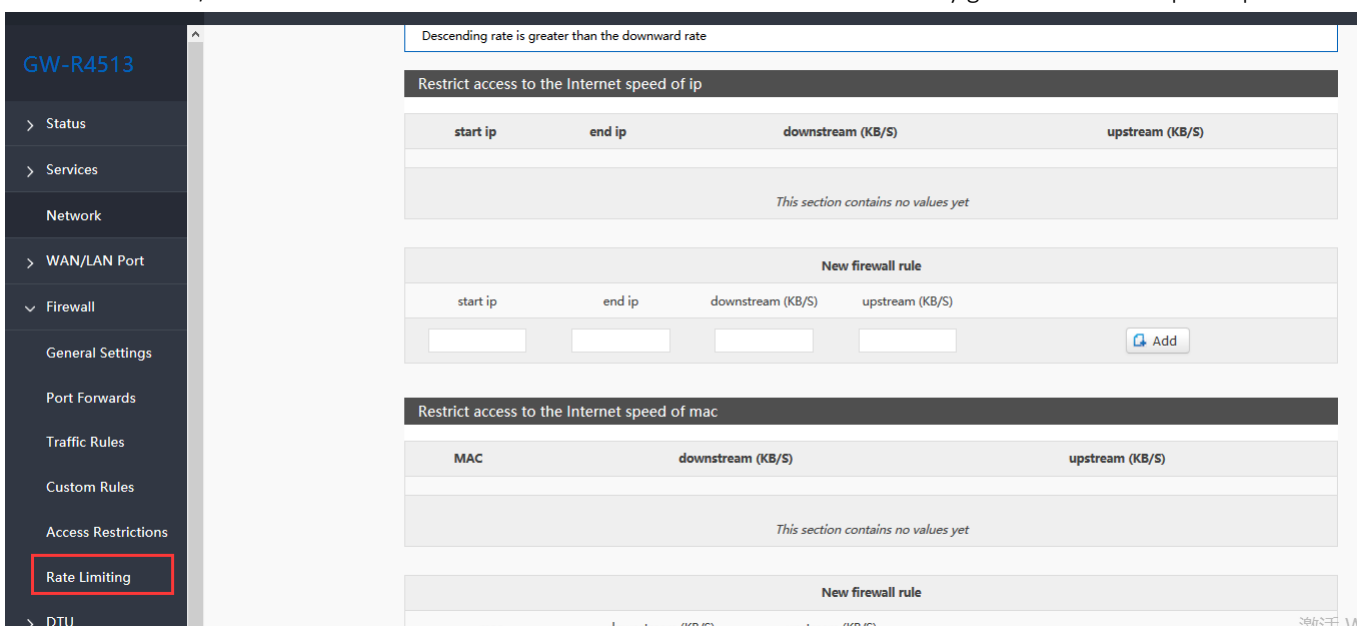


Figure70 rate limiting

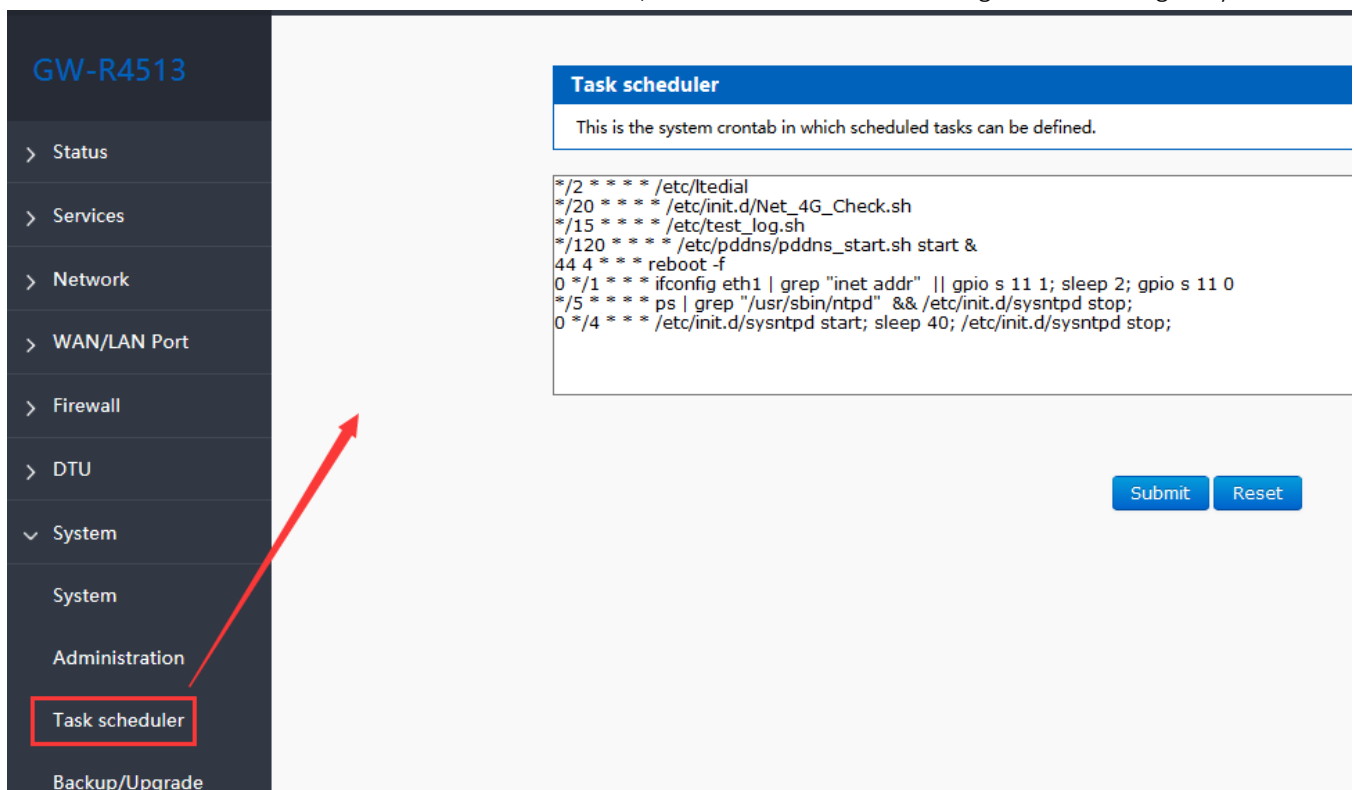
Table10 rate limiting parameter

Function	Parameter setting	Note
Start IP	The start IP of rate limiting	IPV4
End IP	The end IP of rate limiting	IPV4
Upstream	The max of upstream	Unit bit/s
Downstream	The min of downstream	Unit bit/s
MAC	The MAC of rate limiting	MAC address of device

3.10. Task Scheduler

Note: this function can't delete the original planned tasks, otherwise it may lead to abnormal operation of the router.

This router has reserved the interface of scheduled tasks, which enables users to manage the router regularly.



Task scheduler

This is the system crontab in which scheduled tasks can be defined.

```

*/2 * * * * /etc/ltedial
*/20 * * * * /etc/init.d/Net_4G_Check.sh
*/15 * * * * /etc/test_log.sh
*/120 * * * * /etc/pddns/pddns_start.sh start &
44 4 * * * reboot -f
0 */1 * * * ifconfig eth1 | grep "inet addr" || gpio s 11 1; sleep 2; gpio s 11 0
*/5 * * * * ps | grep "/usr/sbin/ntpd" && /etc/init.d/sysntpd stop;
0 */4 * * * /etc/init.d/sysntpd start; sleep 40; /etc/init.d/sysntpd stop;
    
```

Submit Reset

Figure71 task scheduler

If you need to add custom tasks, just start a new line in the input box and enter the relevant timed task instructions.

Format of scheduled task list:

[minute] [hour] [day of month] [month] [day of week] [program to be run]

The range of parameters is:

Minute (0-59), hour (0-23), day of month (1-31), month (1-12), day of week (0-7, 0 or 7)

The values of each parameter can be divided into 4 spacers.

“*” expressing arbitrary

“-” scope of representation

“, “represents multiple values enumerated

“/” every time

3.11. Webpage Sitting

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

Table11 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.

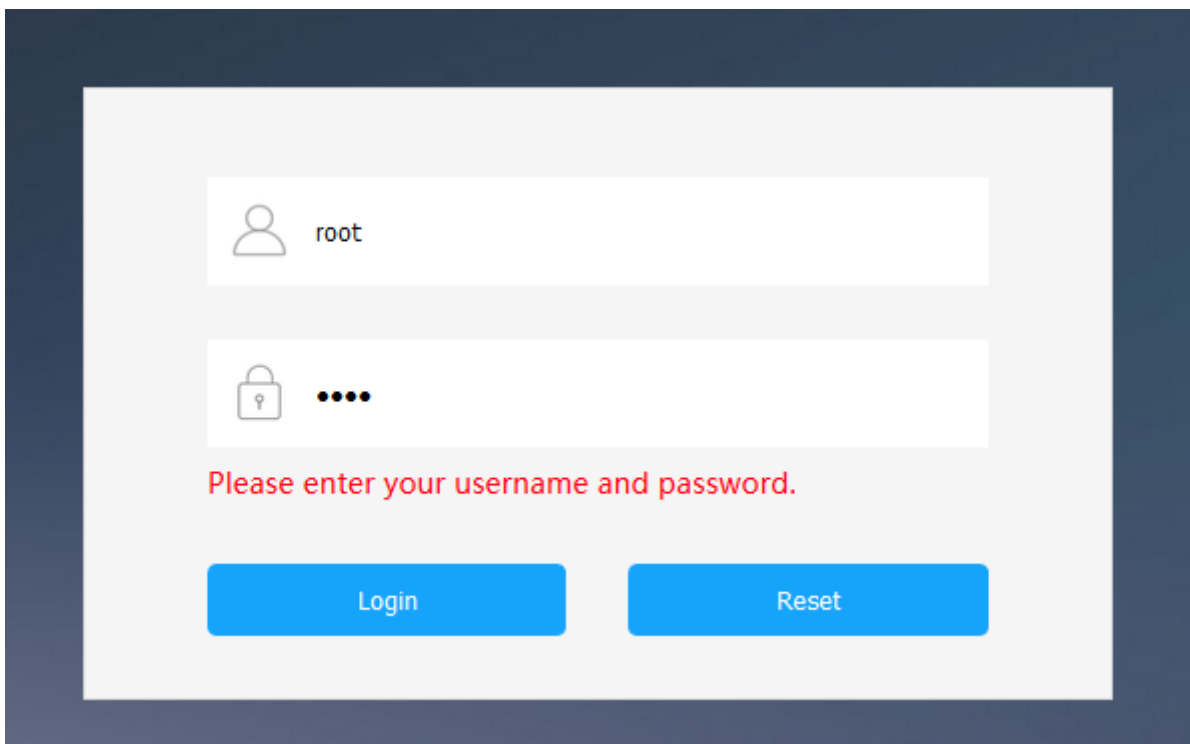


Figure72 login webpage

3.12. Web Function

Status	
System	
Hostname	GW-R4513
Firmware Version	V1.0.6(EN)
Local Time	Thu Nov 1 01:55:01 2018
Uptime	4h 51m 32s
Load Average	3.58, 3.74, 4.03

Figure73 status

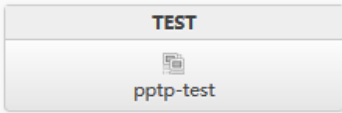




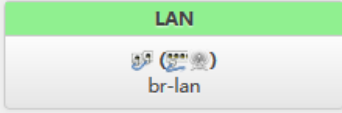
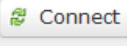



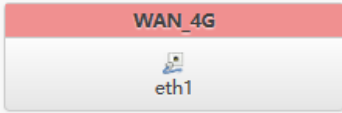




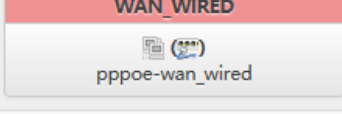
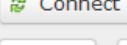



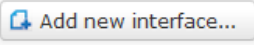
Interfaces		
Interface Overview		
Network	Status	Actions
TEST  pptp-test	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	 Connect  Stop  Edit  Delete
LAN  br-lan	Uptime: 4h 53m 1s MAC-Address: D8:B0:4C:00:00:92 RX: 3.23 MB (35219 Pkts.) TX: 6.24 MB (16053 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDEB:24A3:B5B:0:0:0:1/60	 Connect  Stop  Edit  Delete
WAN_4G  eth1	Uptime: 4h 52m 46s MAC-Address: 2E:6F:B5:39:F8:B3 RX: 4.64 MB (10022 Pkts.) TX: 2.48 MB (28322 Pkts.) IPv4: 10.59.58.25/30	 Connect  Stop  Edit  Delete
WAN_WIRED  pppoe-wan_wired	RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	 Connect  Stop  Edit  Delete
 Add new interface...		

Figure74 interface overview

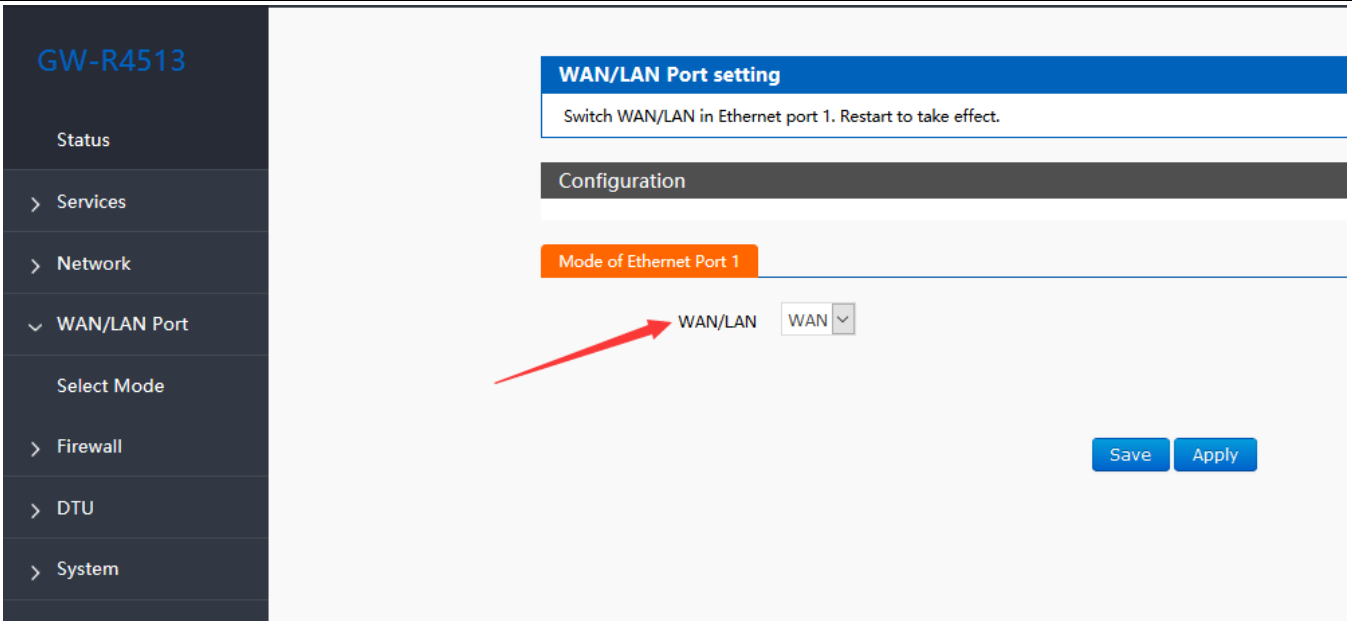


Figure75 mode of Ethernet port

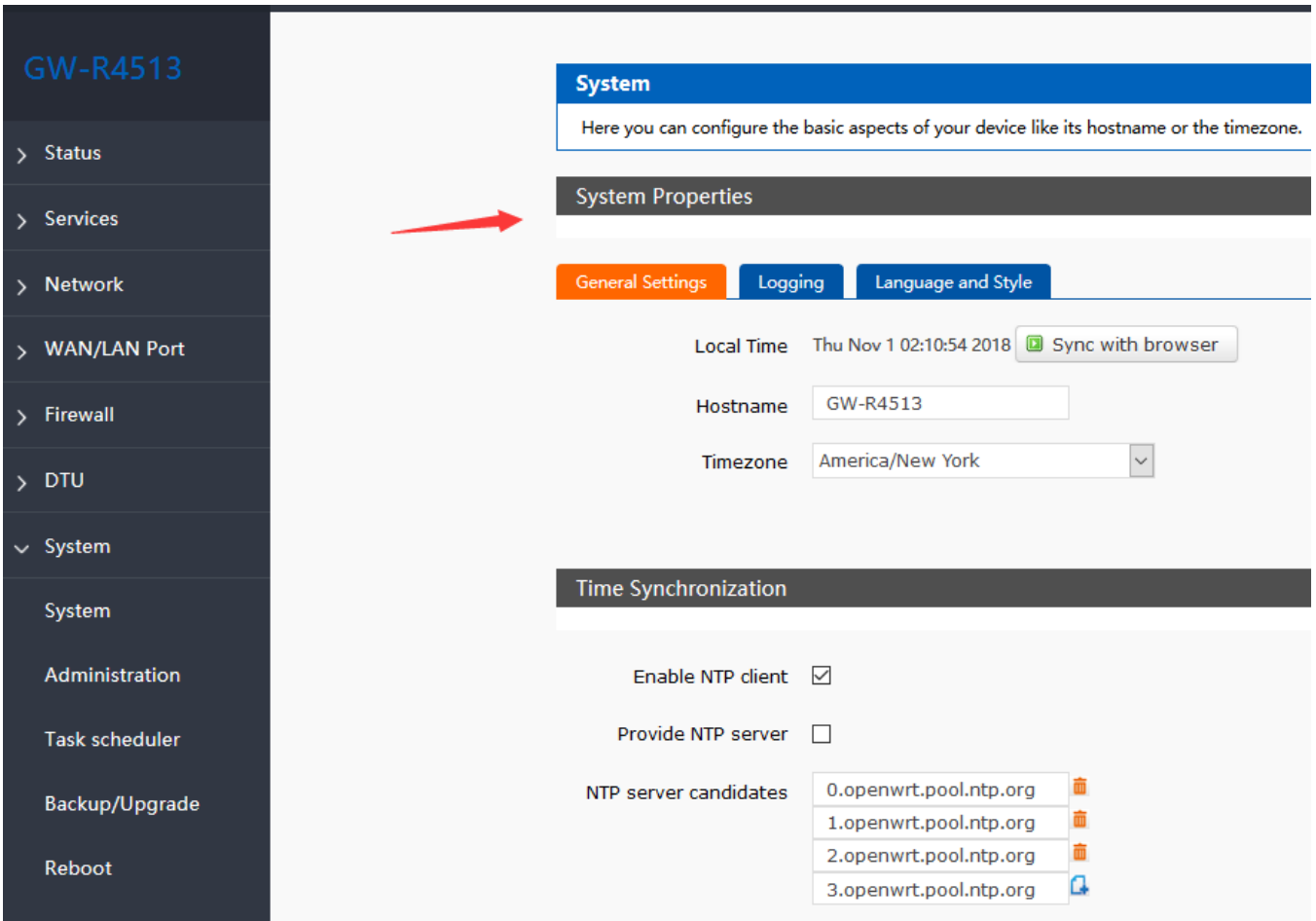


Figure76 system properties

4. DTU Function

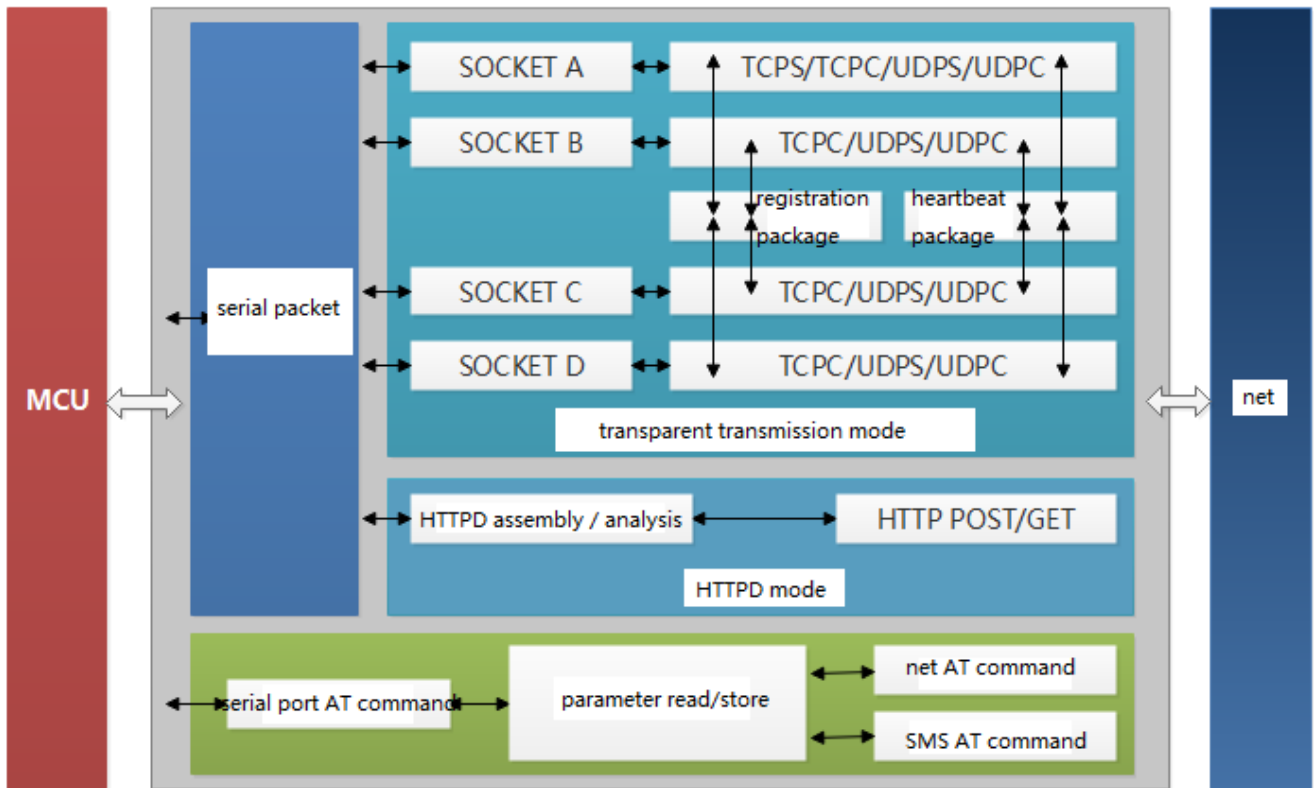


Figure77 DTU function

4.1. Work Mode

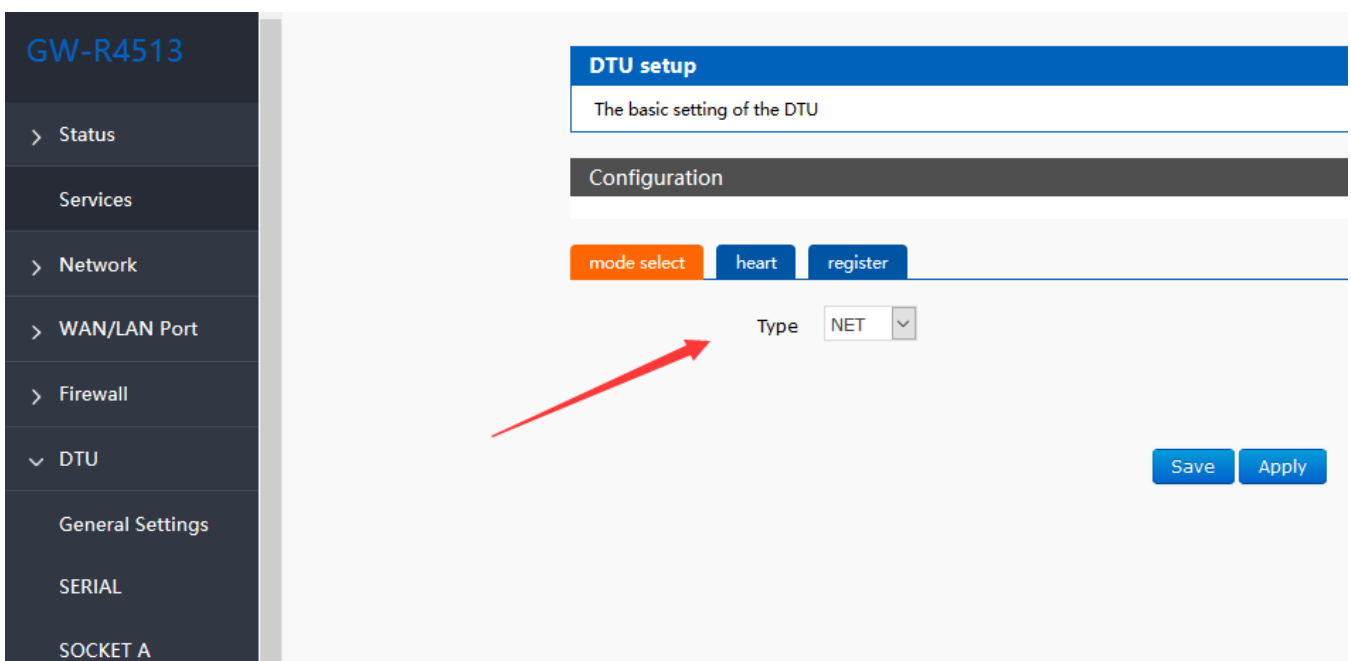


Figure78 mode select

4.1.1. Net Transparent Transmission Mode

4.1.1.1. Mode Declaration

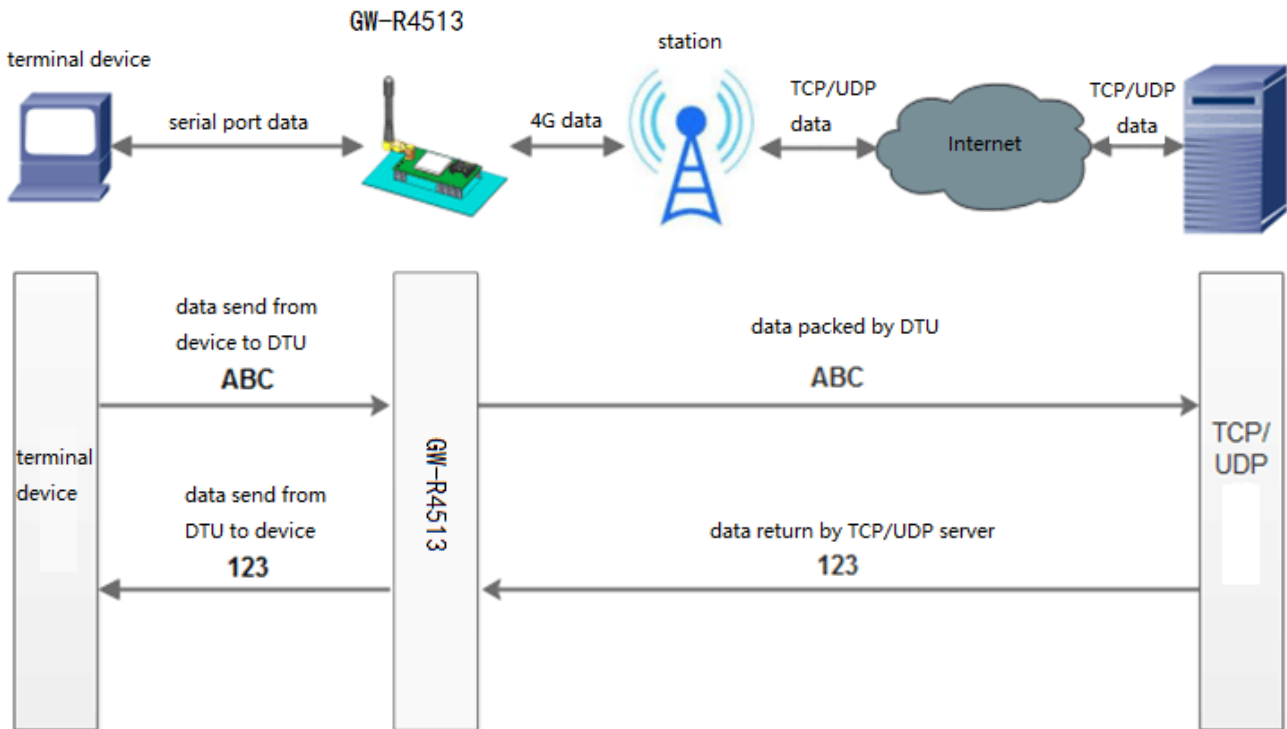


Figure79 net transparent transmission mode

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

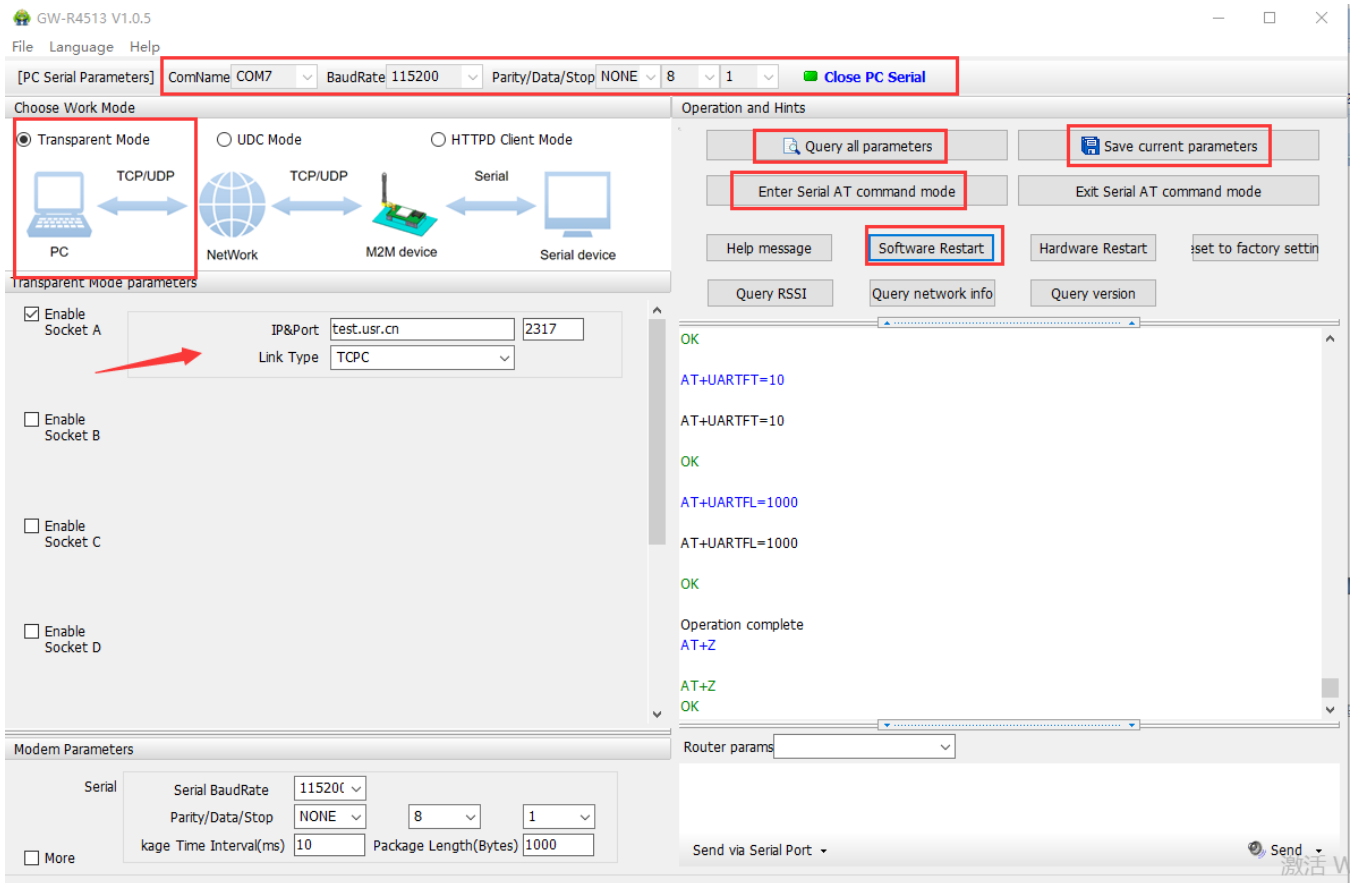


Figure80 setup software

4.1.2. HTTPD Mode

4.1.2.1. Mode Declaration

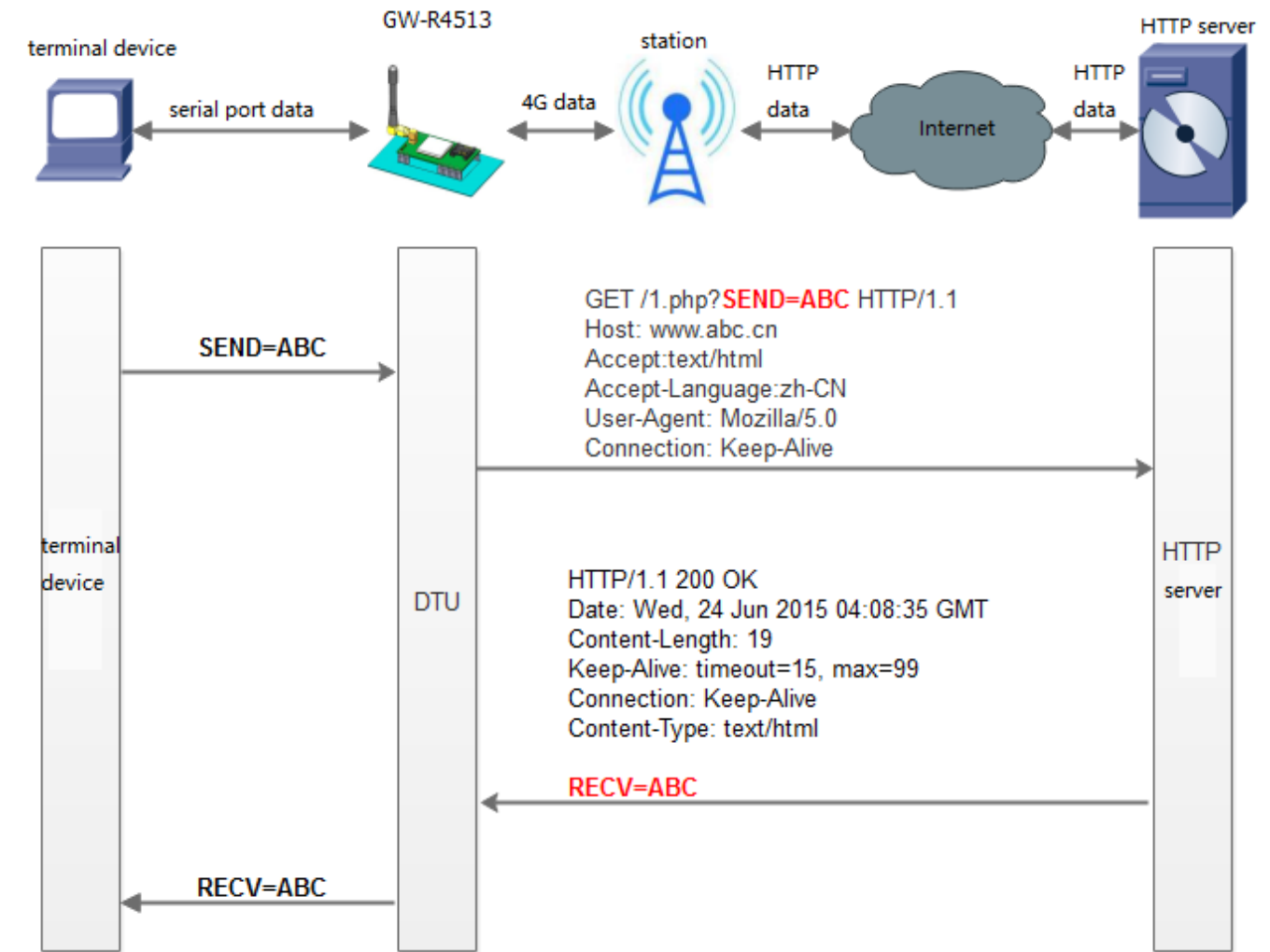


Figure81 HTTPD Mode

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

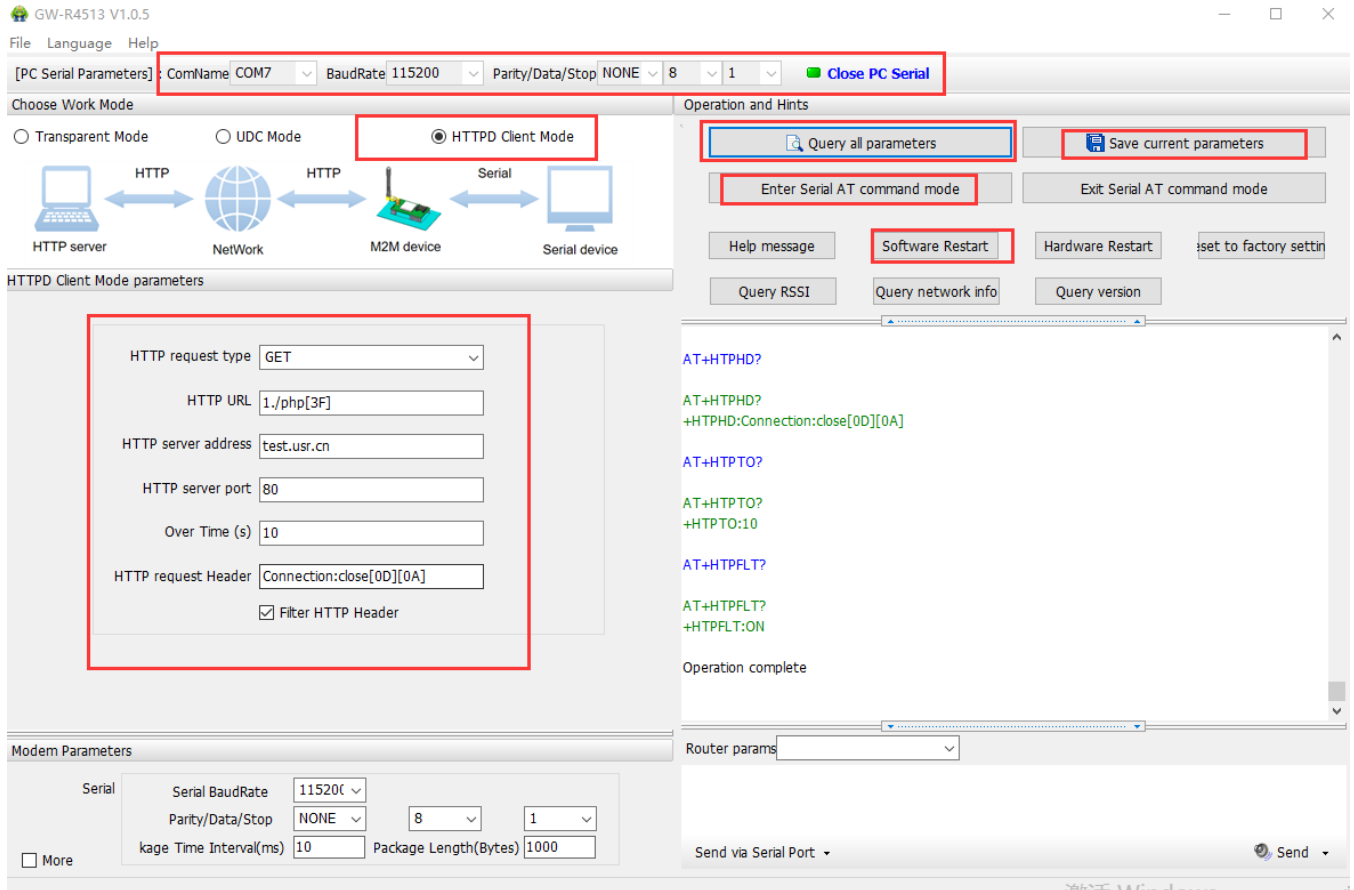


Figure82 setting software

4.1.3. UDC Mode

4.1.3.1. Mode Declaration

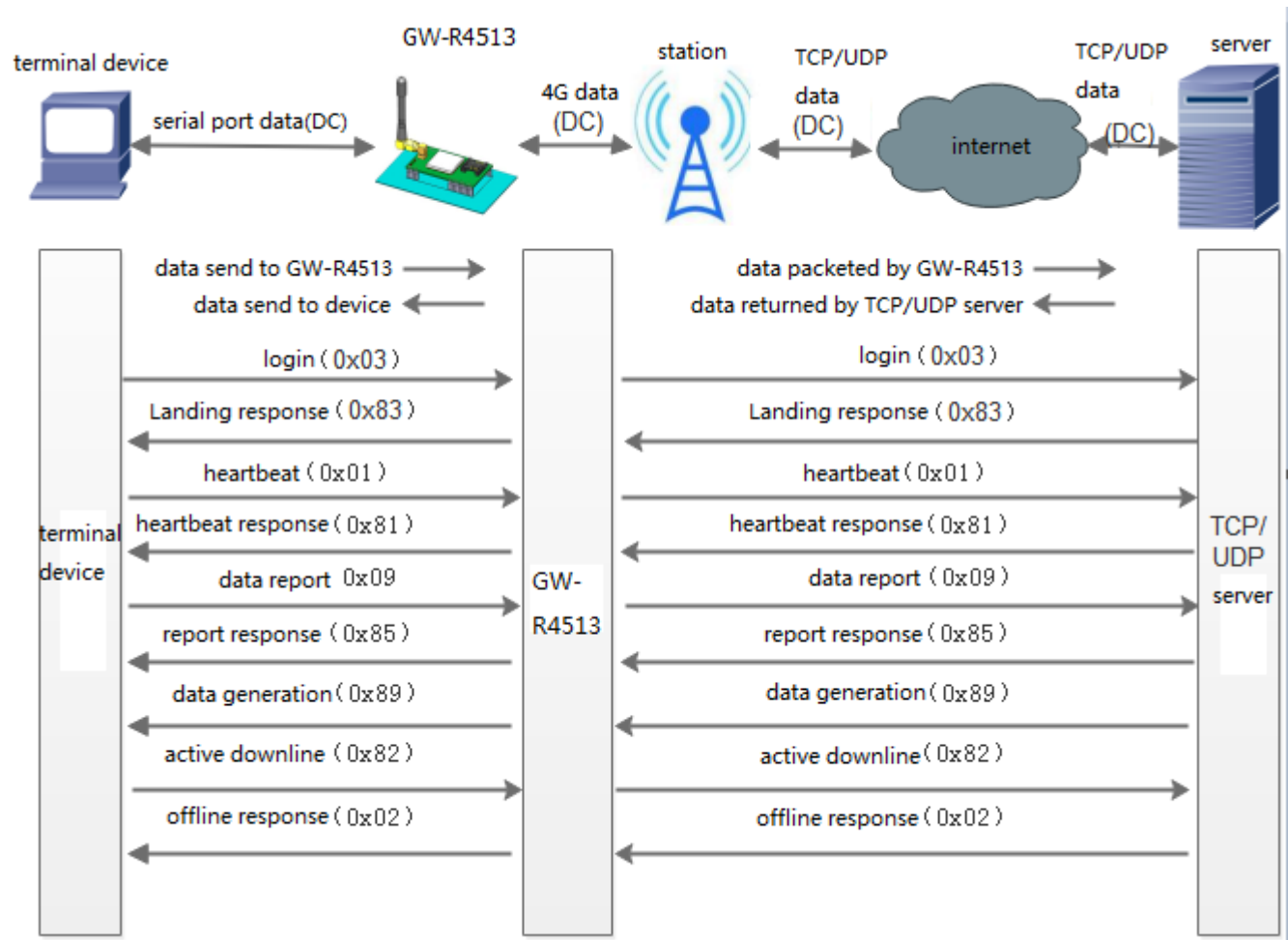


Figure83 UDC Mode

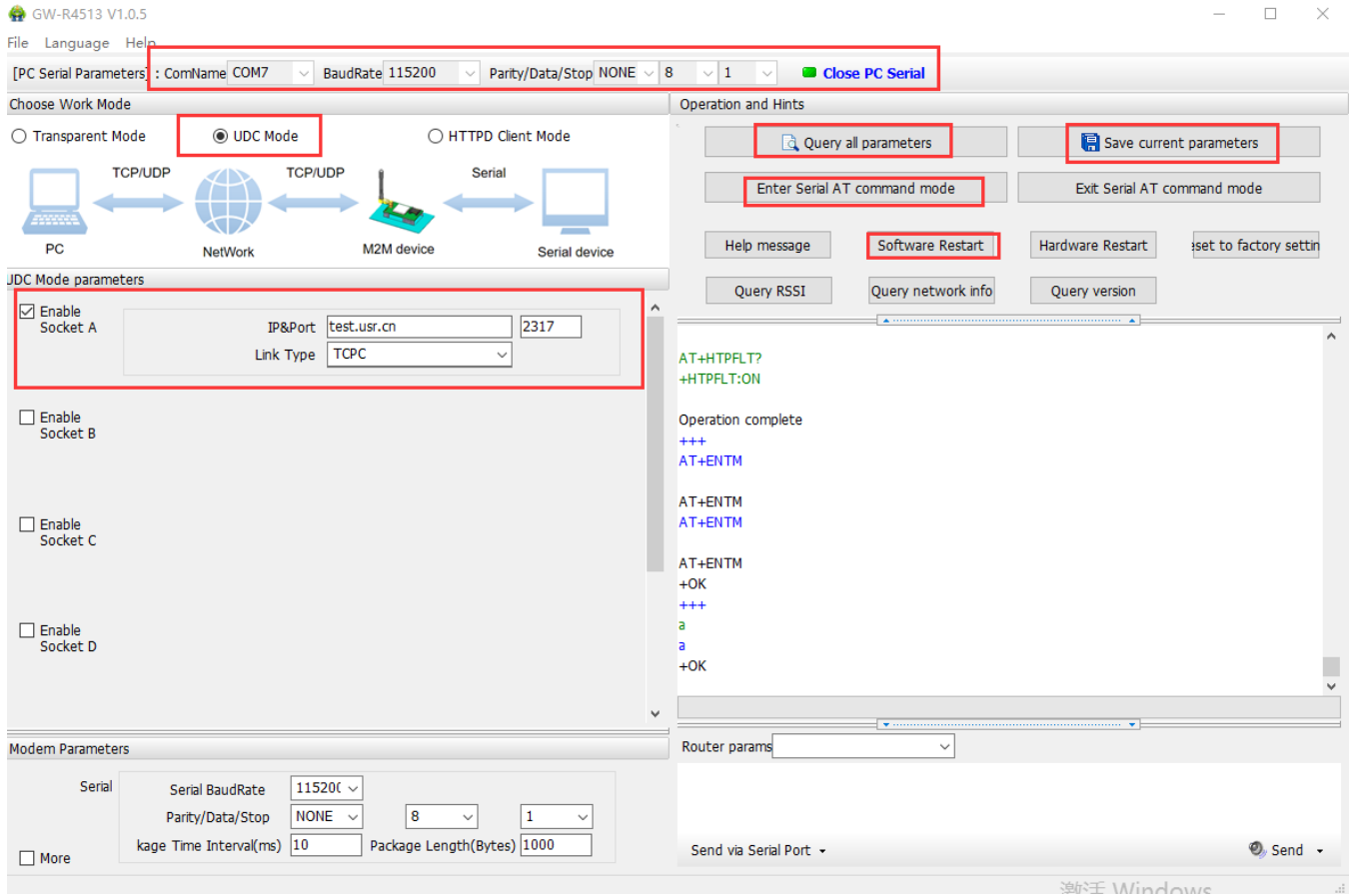


Figure84 setting software

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=30303030303030303031
The ID parameter here is hex form.
9. Send save command
AT+S

4.2. Serial Port

4.2.1. Basic Parameters

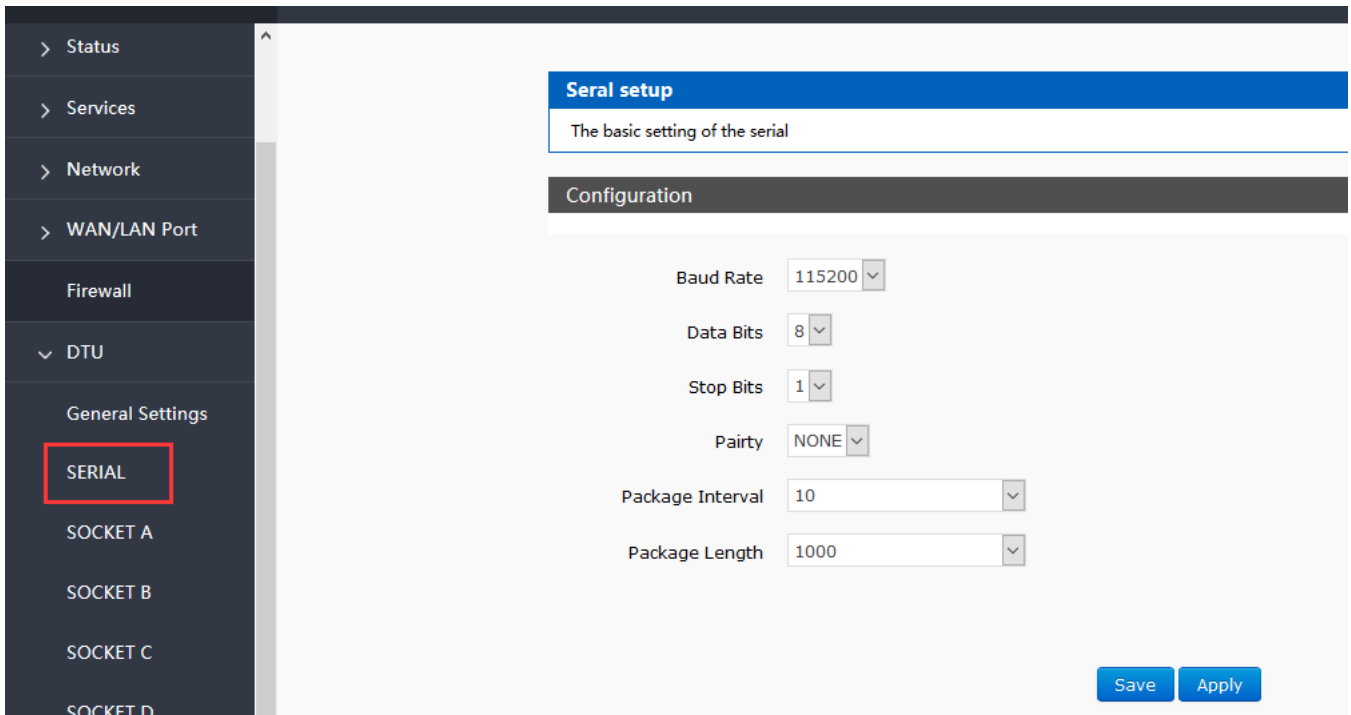


Figure85 serial port setting

Table12 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 according to the AT command, AT+UARTFT=10.

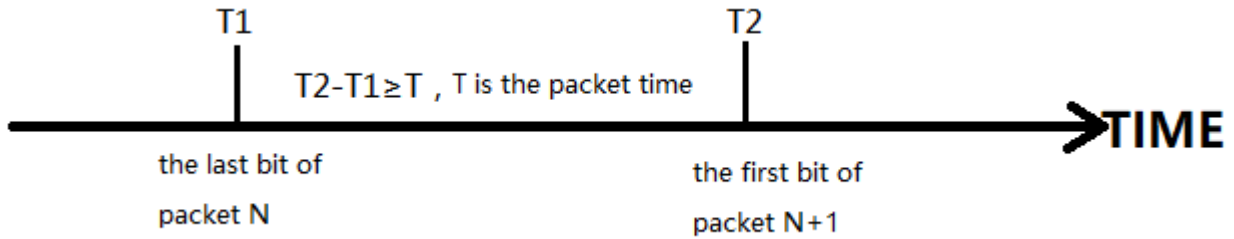


Figure86 time triggered mode

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 according to the AT command, AT+UARTFL=<length>

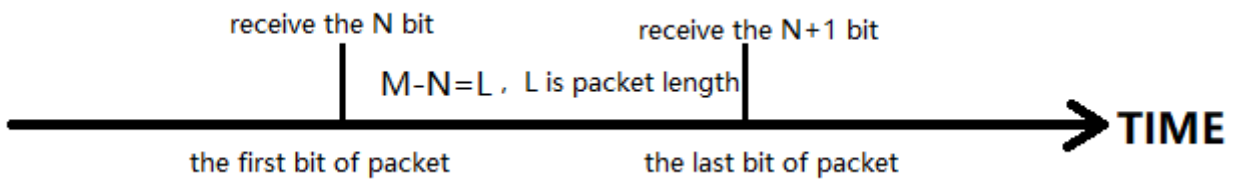


Figure87 length triggered mode

4.3. Characteristic Functions

4.3.1. Registration Package

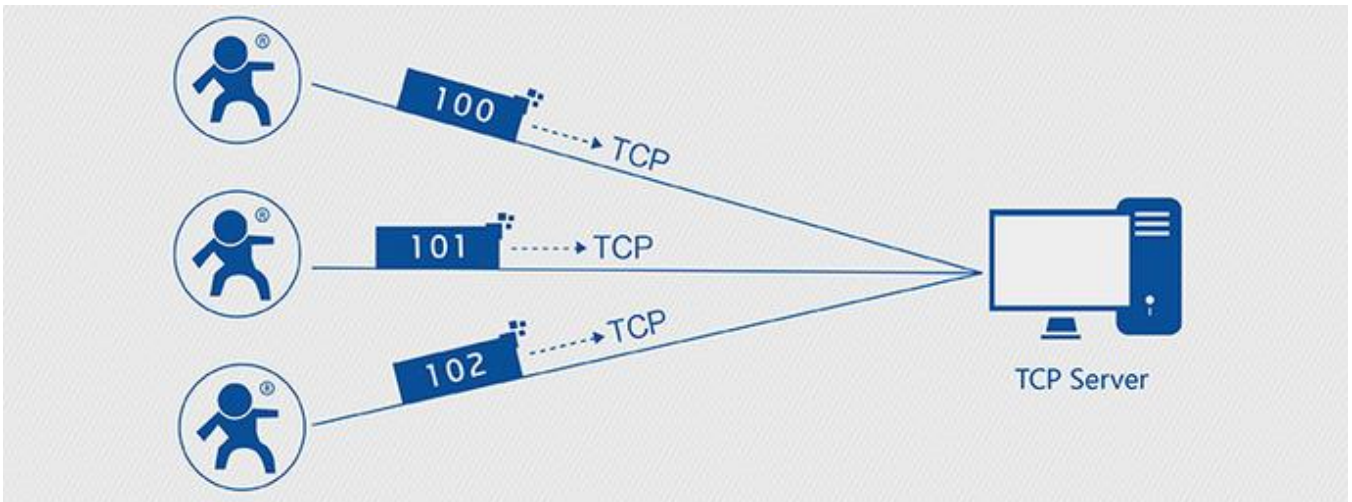


Figure88 registration package function

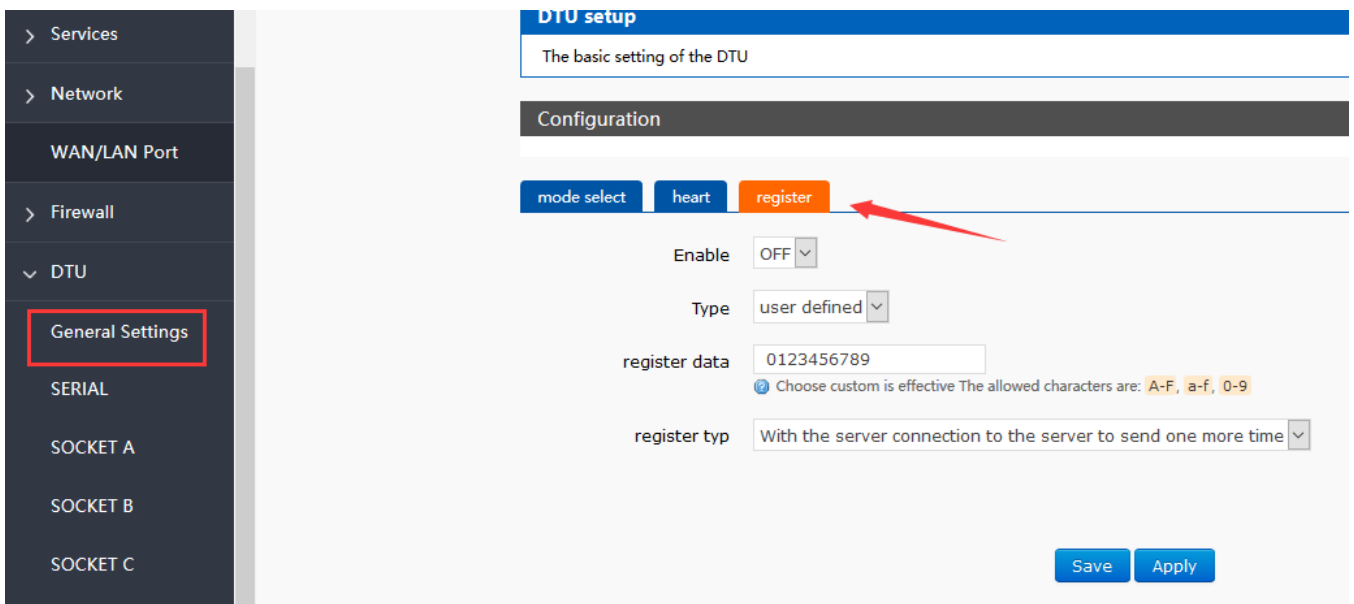


Figure89 registration package setting

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.

Table13 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

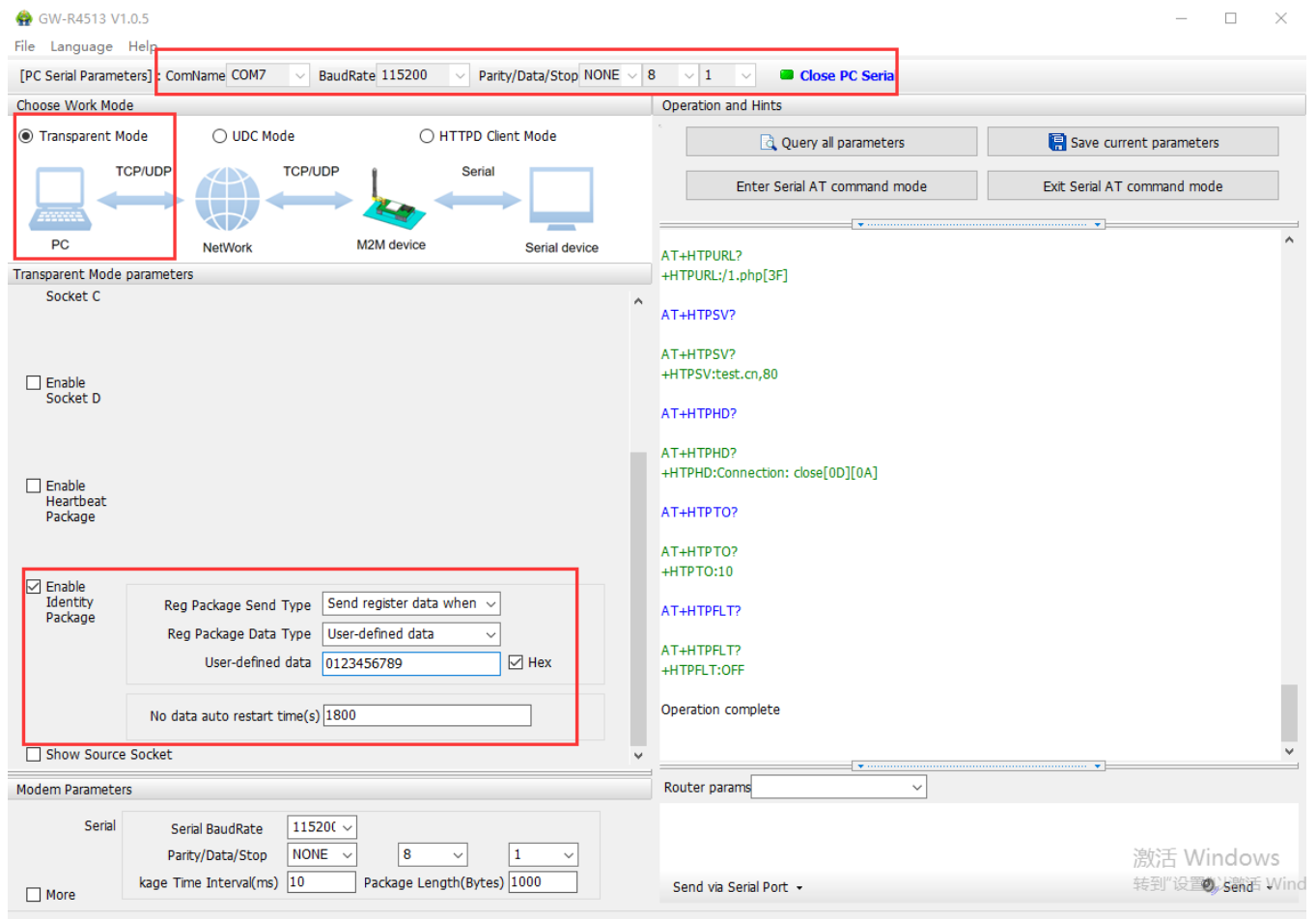


Figure90 setting software

4.3.2. Heartbeat Package

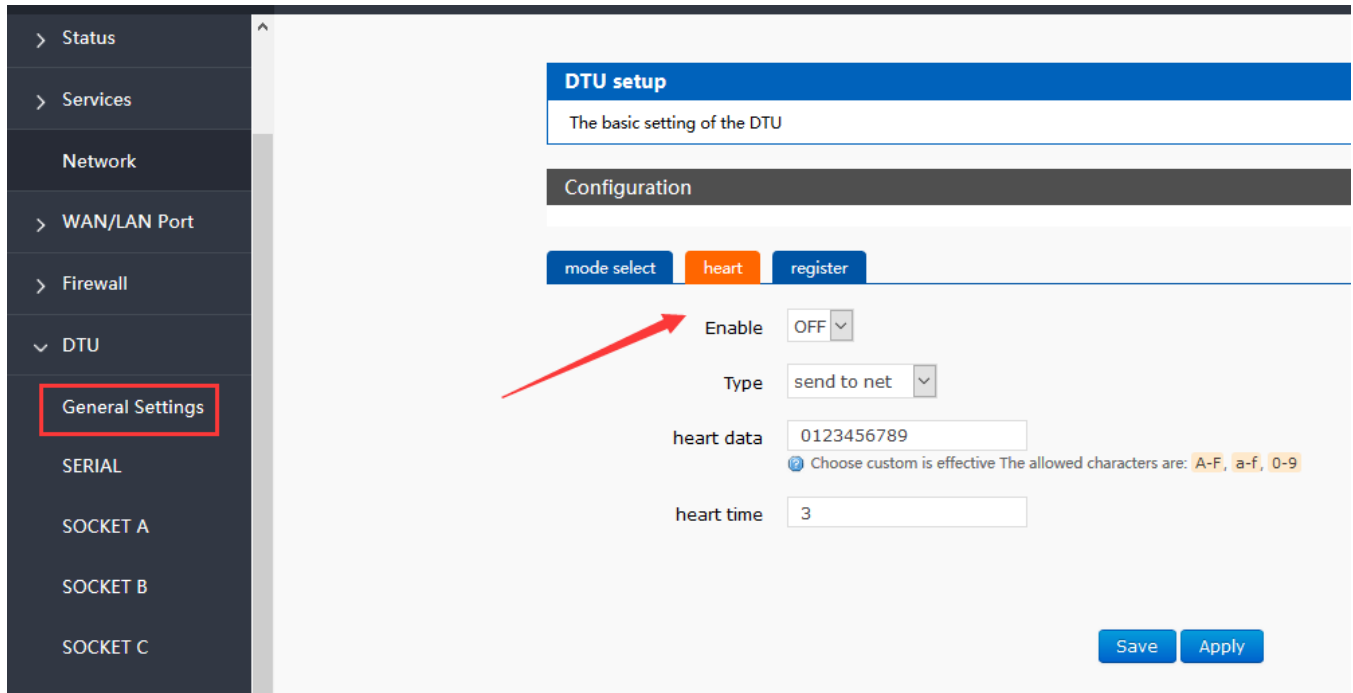


Figure91 heartbeat package setting

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.

Table14 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

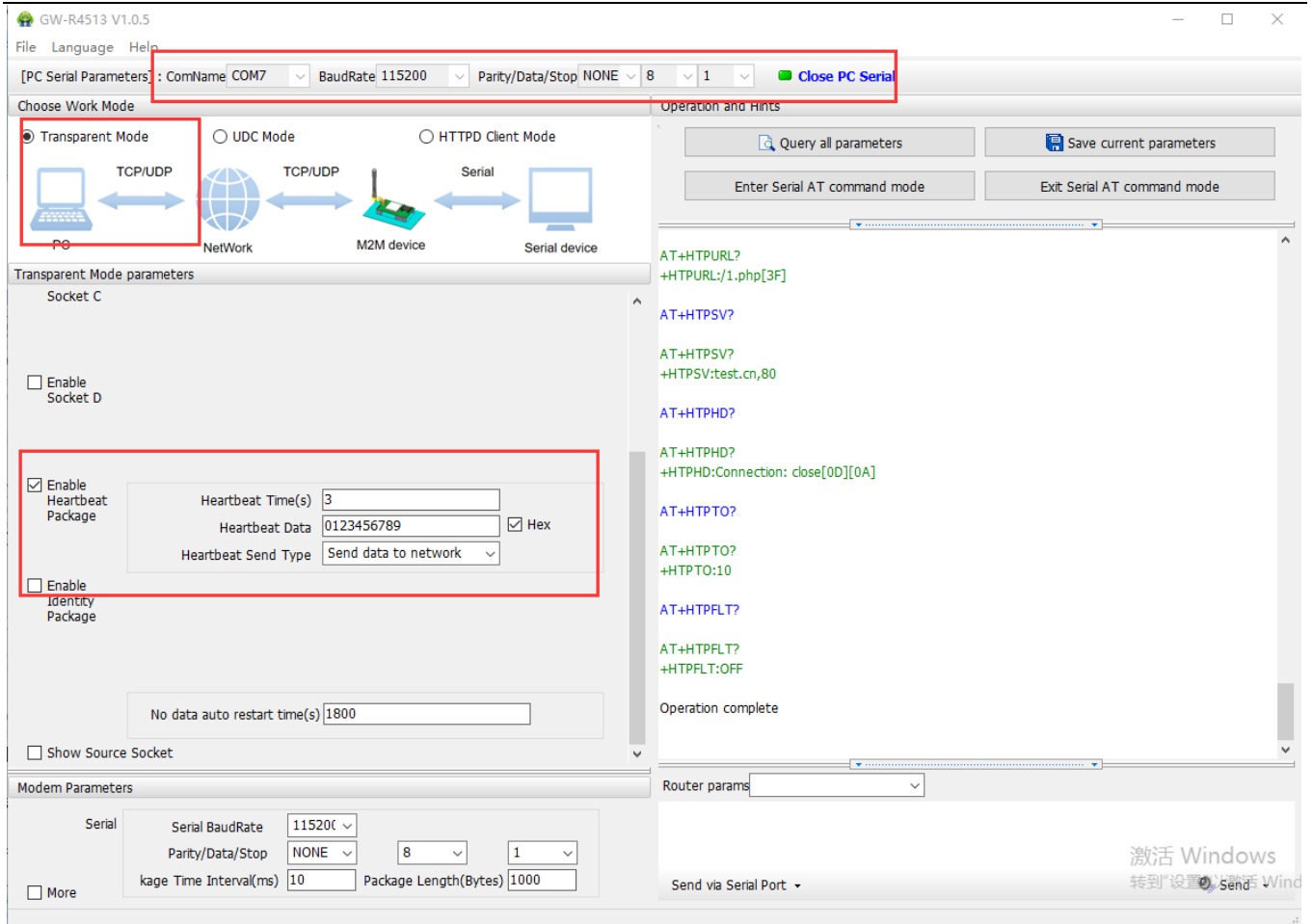


Figure92 setting software

4.3.3. USR-Cloud

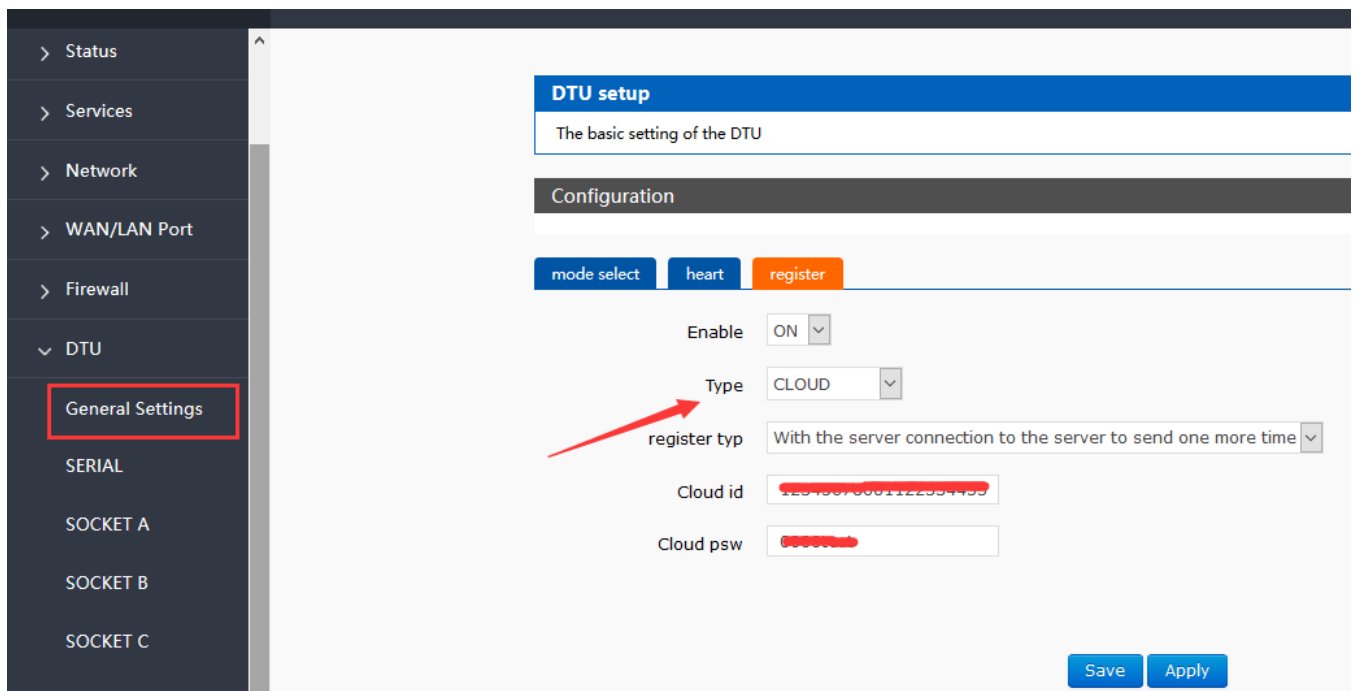


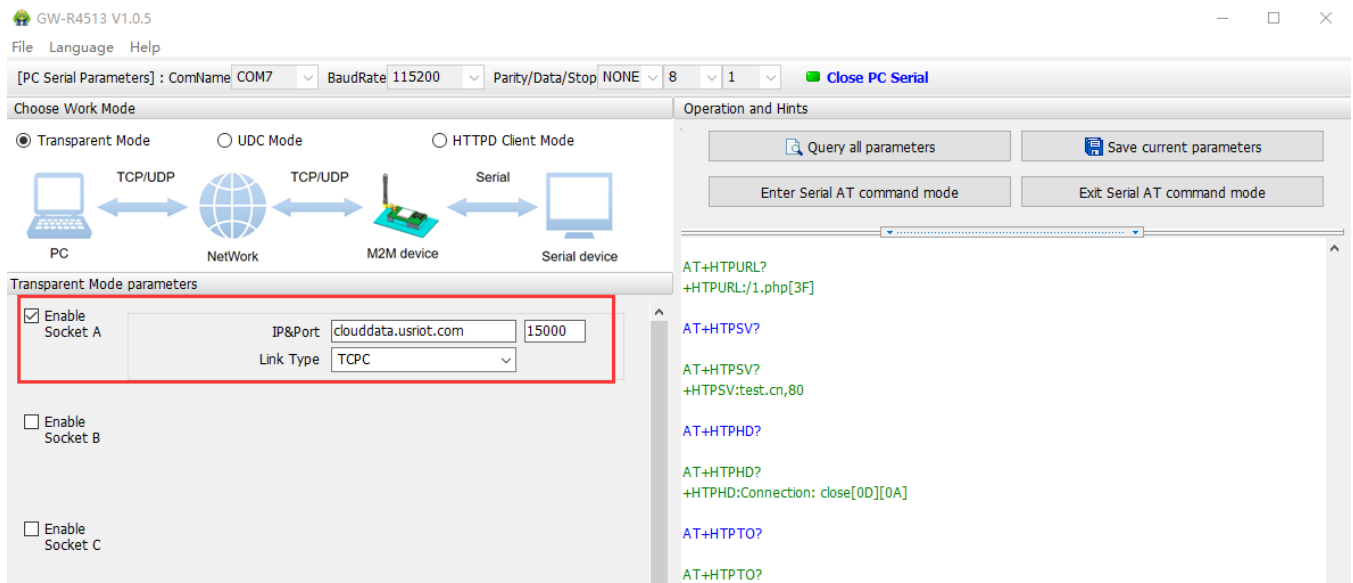
Figure93 USR-Cloud

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

Table15 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



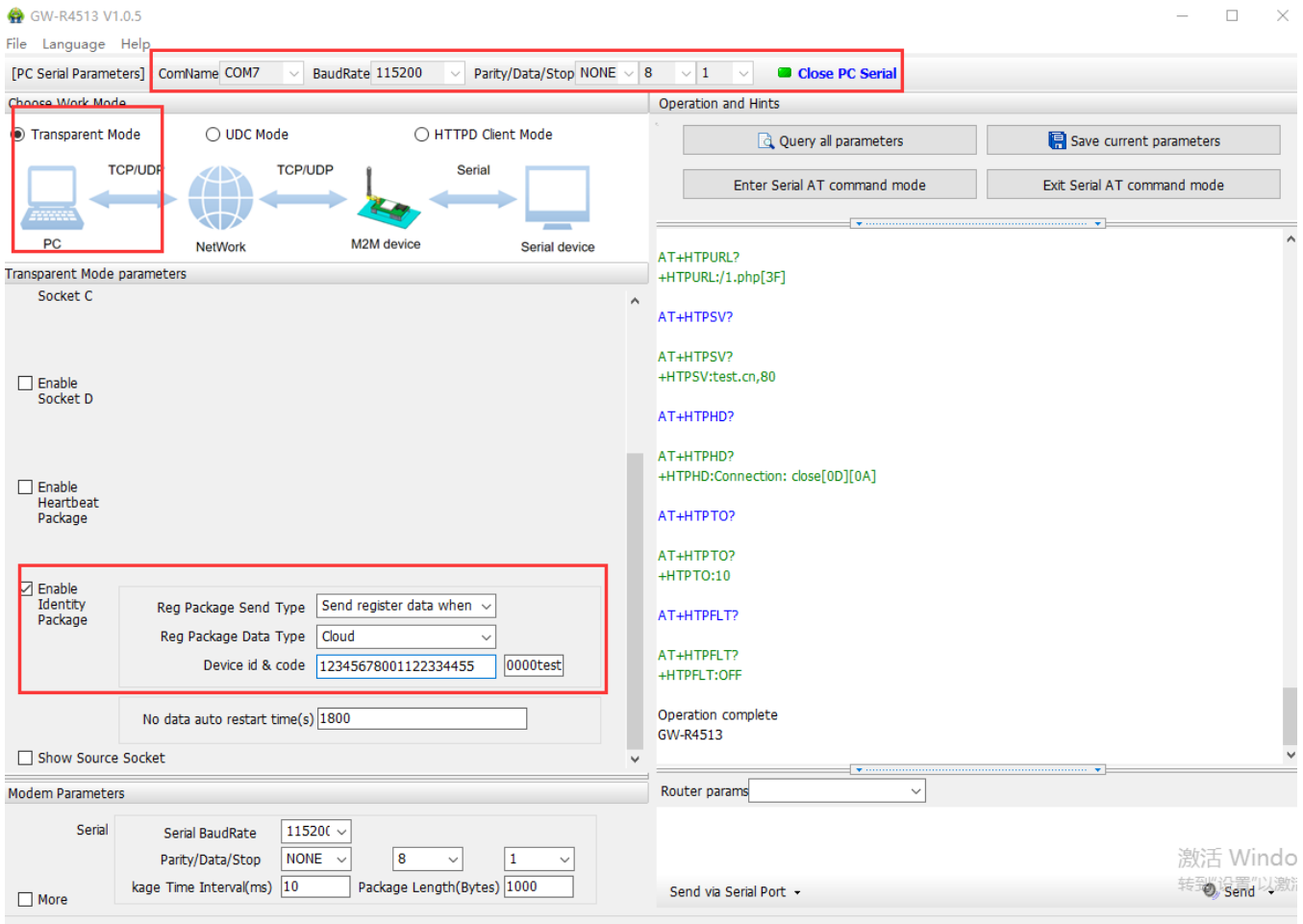


Figure94 setting software

5. AT Commands

Table 16 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

5.1. 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

5.2. AT+MAC

Function: query MAC

Query: AT+MAC<CR>

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

e.g.

send: AT+MAC

return:+MAC:D8B04CD01234

5.3. 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

5.4. 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

5.5. 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

5.6. 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

5.7. AT+CSQ

Function: query the signal intensity

```
AT+CSQ{CR}
```

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

e.g.:

send: AT+CSQ

return:+CSQ:31

5.8. AT+NETMODE

Function: query the net mode

Query:

```
AT+ NETMODE {CR}or AT+ NETMODE?{CR}
```

```
{CR}{LF}+ NETMODE:mode{CR}{LF}{CR}{LF}OK{CR}{LF}
```


5.9. 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
```

5.10. 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
```

5.11. 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
```

5.12. 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
```

5.13. 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>
```

5.14. 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

5.15. AT+CLEAR

Function: recover the default setting

```
AT+CLEAR<CR>
<CR><LF>+ CLEAR:ok<CR><LF>
```

e.g.:

send: AT+ CLEAR

return:+ CLEAR:OK

5.16. AT+Z

Function: restart

```
AT+Z<CR>
<CR><LF>+REBOOT:OK<CR><LF>
```

e.g.:

send: AT+Z=0

return:+ Z:OK

5.17. AT+DHCPEN

Function: enable/unable DHCP server

```
AT+DHCOPEN=SWITCH<CR>
<CR><LF>+ DHCOPEN:ok<CR><LF>
```

e.g.:

```
send: AT+ DHCOPEN=ON
return:+ DHCOPEN:ON
```

5.18. AT+UPDATE

Function: set/query remote upgrade parameter

Query:

```
AT+ UPDATE <CR>
<CR><LF>+ HTBT:status,ip,point,interval<CR><LF>
```

e.g.:

```
send:AT+ UPDATE
return:+ UPDATE: on, 192.168.1.110,3001,20
```

Set:

```
AT+ UPDATE = status,ip,point,interval <CR>
<CR><LF>+ UPDATE:OK<CR><LF>
```

e.g.:

```
send: AT+ UPDATE = on, 192.168.1.110,3001,20
return:+ UPDATE:OK
```

5.19. AT+MONITOR

Function: set/query remote monitor parameter

Query:

```
AT+ MONITOR<CR>
<CR><LF>+ HTBT:status,ip,ip,point,interval<CR><LF>
```

e.g.:

```
send:AT+ MONITOR
return:+ MONITOR: on, 192.168.1.110,3001,20
```

Set:

```
AT+ MONITOR =status,ip,ip,point,interval<CR>
<CR><LF>+ MONITOR:OK<CR><LF>
```

e.g.:

```
send:AT+ MONITOR = on, 192.168.1.110,3001,20
return:+ MONITOR:OK
```

5.20. AT+HEARTPKT

Function: set/query remote monitor heartbeat parameter

Query

```
AT+ HEARTPKT<CR>
```

```
<CR><LF> >+ HEARTPKT:interval,data<CR><LF>
```

e.g.:

```
send: AT+ HEARTPKT
```

```
return:+ HEARTPKT: 20, heartpkt
```

Set:

```
AT+ HEARTPKT =interval,data<CR>
```

```
<CR><LF> >+ HEARTPKT:OK<CR><LF>
```

e.g.:

```
send: AT+ HEARTPKT =20, heartpkt
```

```
return:+ HEARTPKT:OK
```

5.21. 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
```

5.22. AT+UART

Function: query/set serial port parameter

```
AT+UART{CR}or AT+UART?{CR}
```

```
{CR}{LF} >+UART:baud,data bit,stop bit,parity {CR}{LF}{CR}{LF}OK{CR}{LF}
```

Set:

```
AT+UART=baud,data bit,stop bit,parity {CR}
```

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

e.g.: AT+UART=115200,8,1,NONE

5.23. AT+UARTFT

Function: query/set the serial port package time

```
AT+UARTFT{CR}or AT+UARTFT?{CR}
```

```
{CR}{LF} >+UARTFT:time{CR}{LF}{CR}{LF}OK{CR}{LF}
```

Set:

```
AT+UARTFT=time{CR}
```

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

e.g.: AT+UARTFT=10

5.24. AT+UARTFL

Function: query/set the serial port package length

```
AT+UARTFL{CR}or AT+UARTFL?{CR}  
{CR}{LF}+UARTFL:length{CR}{LF}{CR}{LF}OK{CR}{LF}
```

Set:

```
AT+UARTFL=length{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ UARTFL =1000

5.25. AT+SOCKA

Function: query/set socket A parameter

◆ Query

```
AT+SOCKA{CR}or AT+SOCKA?{CR}  
{CR}{LF}+SOCKA:protocol,address,port{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set

```
AT+SOCKA=protocol,address,port{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+SOCKA=TCPC,test.usr.cn,2317

5.26. AT+SOCKB

Function: query/set socket B parameter

◆ Query parameter:

```
AT+SOCKB{CR}or AT+SOCKB?{CR}  
{CR}{LF}+SOCKB:protocol,address,port{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set:

```
AT+SOCKB=protocol,address,port{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+SOCKB=TCPC,test.usr.cn,2317

5.27. AT+SOCKC

Function: query/set socket C parameter

◆ Query :

```
AT+ SOCKC {CR}or AT+ SOCKC?{CR}  
{CR}{LF}+ SOCKC:protocol,address,port{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set:

```
AT+ SOCKC =protocol,address,port{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ SOCKC =TCPC,test.usr.cn,2317

5.28. AT+SOCKD

Function: query/set socket D parameter

- ◆ Query :
AT+ SOCKD {CR}or AT+ SOCKD?{CR}
{CR}{LF}+ SOCKD:protocol,address,port{CR}{LF}{CR}{LF}OK{CR}{LF}
- ◆ Set:
AT+ SOCKD =protocol,address,port{CR}
{CR}{LF}OK{CR}{LF}

e.g.: AT+ SOCKD =TCPC,test.usr.cn,2317

5.29. AT+SOCKAEN

Function: query/set enable socket A or not

- ◆ Query:
AT+SOCKAEN{CR}or AT+SOCKAEN?{CR}
{CR}{LF}+SOCKAEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
- ◆ Set:
AT+SOCKAEN=status{CR}
{CR}{LF}OK{CR}{LF}

5.30. AT+SOCKBEN

Function: query/set enable socket B or not

- ◆ Query :
AT+SOCKBEN{CR}or AT+SOCKBEN?{CR}
{CR}{LF}+SOCKBEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
- ◆ Set:
AT+SOCKBEN=status{CR}
{CR}{LF}OK{CR}{LF}

5.31. AT+SOCKCEN

Function: query/set enable socket C or not

- ◆ Query :
AT+ SOCKCEN {CR}or AT+ SOCKCEN?{CR}
{CR}{LF}+ SOCKCEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
- ◆ Set:
AT+ SOCKCEN =status{CR}
{CR}{LF}OK{CR}{LF}

5.32. AT+SOCKDEN

Function: query/set enable socket D or not

- ◆ Query :
AT+ SOCKDEN {CR}or AT+ SOCKDEN?{CR}
{CR}{LF}+ SOCKDEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
- ◆ Set :
AT+ SOCKDEN =status{CR}
{CR}{LF}OK{CR}{LF}

5.33. AT+SOCKALK

Function: query socket A establish or not

- ◆ Query :
AT+SOCKALK{CR}or AT+SOCKALK?{CR}
{CR}{LF}+SOCKALK:status{CR}{LF}{CR}{LF}OK{CR}{LF}

5.34. AT+SOCKBLK

Function: query socket B establish or not

- ◆ Query :
AT+SOCKBLK{CR}or AT+SOCKBLK?{CR}
{CR}{LF}+SOCKBLK:status{CR}{LF}{CR}{LF}OK{CR}{LF}

5.35. AT+SOCKCLK

Function: query socket C establish or not

- ◆ Query :
AT+ SOCKCLK {CR}or AT+ SOCKCLK?{CR}
{CR}{LF}+ SOCKCLK:status{CR}{LF}{CR}{LF}OK{CR}{LF}

5.36. AT+SOCKDLK

Function: query socket D establish or not

- ◆ Query :
AT+ SOCKDLK {CR}or AT+ SOCKDLK?{CR}
{CR}{LF}+ SOCKDLK:status{CR}{LF}{CR}{LF}OK{CR}{LF}

5.37. AT+SOCKIND

Function: query/set enable the data source of socket or not

- ◆ Query :

```
AT+SOCKIND{CR}or AT+SOCKIND?{CR}  
{CR}{LF}+SOCKIND:status{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+SOCKIND=status{CR}  
{CR}{LF}OK{CR}{LF}
```

5.38. AT+REGEN

Function: query/set enable the register package or not

◆ Query :

```
AT+REGEN{CR}or AT+REGEN?{CR}  
{CR}{LF}+REGEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+REGEN=status{CR}  
{CR}{LF}OK{CR}{LF}
```

5.39. AT+REGTP

Function: query/set the type of register

◆ Query :

```
AT+REGTP{CR}or AT+REGTP?{CR}  
{CR}{LF}+REGTP:type{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+REGTP=type{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ REGTP = ICCID

5.40. AT+REGDT

Function: query/set custom register data

◆ Query :

```
AT+REGDT{CR}or AT+REGDT?{CR}  
{CR}{LF}+REGDT:data{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+REGDT=data{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ REGDT = 123456789

5.41. AT+REGSND

Function: query/set the register sending type

◆ Query :

```
AT+REGSND{CR}or AT+REGSND?{CR}
```



```
{CR}{LF}+REGSND:type{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+REGSND=type{CR}
```

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

e.g.: AT+ REGSND = DATA

5.42. AT+CLOUD

Function: query/set the USR-Cloud register parameter

◆ Query :

```
AT+CLOUD{CR}or AT+CLOUD?{CR}
```

```
{CR}{LF}+CLOUD:id,password{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+CLOUD=id,password{CR}
```

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

e.g.: AT+ CLOUD = 12345678901234567890,12345678

5.43. AT+HEARTEN

Function: query/set enable heartbeat or not

◆ Query :

```
AT+HEARTEN{CR}or AT+HEARTEN?{CR}
```

```
{CR}{LF}+HEARTEN:status{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HEARTEN=status{CR}
```

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

5.44. AT+HEARTDT

Function: query/set heartbeat data

◆ Query :

```
AT+HEARTDT{CR}or AT+HEARTDT?{CR}
```

```
{CR}{LF}+HEARTDT:data{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HEARTDT=data{CR}
```

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

e.g.: AT+ HEARTDT = 123456789

5.45. AT+HEARTSND

Function: query/set the heartbeat sending type

◆ Query :

```
AT+HEARTSND{CR}or AT+HEARTSND?{CR}
```

```
{CR}{LF}+HEARTSND:type{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HEARTSND=type{CR}
```

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

e.g.: AT+ HEARTSND = COM

5.46. AT+HEARTTM

Function: query/set the heartbeat sending time

◆ Query :

```
AT+HEARTTM{CR}or AT+HEARTTM?{CR}
```

```
{CR}{LF}+HEARTTM:time{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HEARTTM=time{CR}
```

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

e.g.: AT+ HEARTTM = 30

5.47. AT+HTPTP

Function: query/set HTTP request type

◆ Query :

```
AT+HTPTP{CR}or AT+HTPTP?{CR}
```

```
{CR}{LF}+HTPTP:type{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPTP=type{CR}
```

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

e.g.: AT+ HTPTP = POST

5.48. AT+HTPURL

Function: query/set the URL of HTTP

◆ Query :

```
AT+HTPURL{CR}or AT+HTPURL?{CR}
```

```
{CR}{LF}+HTPURL:URL{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPURL=URL{CR}
```

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

e.g.: AT+ HTPURL = /1.php[3F]

5.49. AT+HTPSV

Function: query/set the request parameter of HTTP

◆ Query :

```
AT+HTPSV{CR}or AT+HTPSV?{CR}  
{CR}{LF}+HTPSV:address,port{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPSV=address,port{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ HTPSV = test.usr.cn,80

5.50. AT+HTPHD

Function: query/set the head info of HTTP

◆ Query :

```
AT+HTPHD{CR}or AT+HTPHD?{CR}  
{CR}{LF}+HTPHD:head{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPHD=head{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ HTPHD = Connection: close[OD][OA]

5.51. AT+HTPTO

Function: query/set the request time of HTTP

◆ Query :

```
AT+HTPTO{CR}or AT+HTPTO?{CR}  
{CR}{LF}+HTPTO:time{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPTO=time{CR}  
{CR}{LF}OK{CR}{LF}
```

e.g.: AT+ HTPTO = 10

5.52. AT+HTPFLT

Function: query/set filtering the header information of HTTP request or not

◆ Query :

```
AT+HTPFLT{CR}or AT+HTPFLT?{CR}  
{CR}{LF}+HTPFLT:status{CR}{LF}{CR}{LF}OK{CR}{LF}
```

◆ Set :

```
AT+HTPFLT=status{CR}  
{CR}{LF}OK{CR}{LF}
```

6. 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@usriot.com

Tel: 86-531-88826739/86-531-55507297

7. 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.

8. Update History

Edition	Describe
V1.0.1	2019-4 establish