

USR-G808 User Manual

File Version: V1.0.6



Contents

USR-G808 User Manual.....	1
1. Get Start.....	4
1.1. Hardware Testing Environment.....	4
1.2. Net Connecting.....	5
1.3. Web Log and Netting Testing.....	6
2. Product Overview.....	7
2.1. Brief Introduce.....	7
2.2. Features.....	8
2.3. Basic Parameters.....	8
2.4. Hardware and Dimension.....	10
3. Function.....	12
3.1. User Configuring.....	12
3.2. Common Function.....	13
3.2.1. DDNS.....	13
3.2.2. WIFIdog.....	16
3.2.3. Remote Manager.....	19
3.2.4. LAN Interface.....	21
3.2.5. DHCP.....	23
3.2.6. WAN Interface.....	23
3.2.7. WLAN.....	25
3.2.8. Dual 4G Interface.....	28
3.2.9. APN Setting.....	29
3.2.10. Network Backup.....	32
3.2.11. Load balancing.....	32
3.2.12. VPN Client (PPTP、L2TP、IPSEC、OPENVPN、GRE、SSTP).....	34
3.2.12.1. PPTP Client.....	34
3.2.12.2. L2TP Client.....	36
3.2.12.3. IPSEC.....	37
3.2.12.4. OPENVPN Client.....	39
3.2.12.5. GRE.....	41
3.2.12.6. SSTP Client.....	43
3.2.13. Static Routes.....	45
3.2.14. Firewall.....	47
3.2.14.1. Basic Setting.....	47
3.2.14.2. Port Forwards.....	48
3.2.14.3. Traffic rules.....	50
3.2.14.4. Custom Rules.....	56
3.2.14.5. Restricting access.....	56
3.2.14.6. Rate-limiting.....	57
3.3. Basic Function.....	57
3.3.1. Network Diagnosis.....	57
3.3.2. Host Name and Time Zone.....	58

3.3.3. Web Server Password.....	59
3.3.4. Scheduled Tasks.....	59
3.3.5. Restore to Default Factory Settings.....	60
3.3.6. Introduce LED.....	60
3.3.7. Upgrade Firmware Version.....	61
3.3.8. Reset.....	61
3.3.9. NTP.....	62
4. Configuring.....	63
4.1. Webpage Setting.....	63
4.2. Web Function.....	63
5. Contact Us.....	65
6. Disclaimer.....	66
7. Update History.....	66

1. Get Start

USR-G808 is a dual SIM 4G LTE WiFi wireless outer, with SIM card slot. Dual SIM cards provide a auto fail-over for higher stability and convenience. Simple setting and the router can work, user no need to care about the details. Configuring the parameters via the webpage, save all the time.

In this character, we introduce the basic thing about the G808, users are suggested operating according to this instruction, then will have a systematic realization for it. Also you can read the character that you are interesting.

Product link: <https://www.usriot.com/products/dual-sim-4g-lte-wifi-router.html>

Dual SIM 4G LTE WiFi Router

Model: USR-G808

USR-G808 is a Dual SIM 4G LTE WiFi Wireless Router, with SIM Card Slot. Dual SIM cards provide a auto fail-over for higher stability and convenience.

- Working voltage: DC 9-36V
- Supports Dual SIM
- DIN-Rail Installing
- Europe / Australia/ North America Version

Share to:



General Details	Specifications	Downloads	How to Buy	Models
User Manual				
[User Manual]USR-G808-User-Manual-V1.0.4.1 download				
[Datasheet] USR-G808-Datasheet_V1.0.0 download				

Diagram 1-1 Product Webpage

Any question please submit it into the USR Custom Supports: <http://h.usriot.com/>

1.1. Hardware Testing Environment

- USR-G808*1

- PC*1
- Cable*1
- Power adapter(DC12V / 1A)
- 4G SIM cards *2



Diagram1.1-1 Testing Connection

1.2. Net Connecting

Taking USR-G808 as an example

- Insert SIM cards, notice the direction
- Connect the WIFI and 4G antennas to the correspond interface
- Connect the net port of the PC to the LAN of the router via cable
- Configure the PC card, obtain an IP address automatically

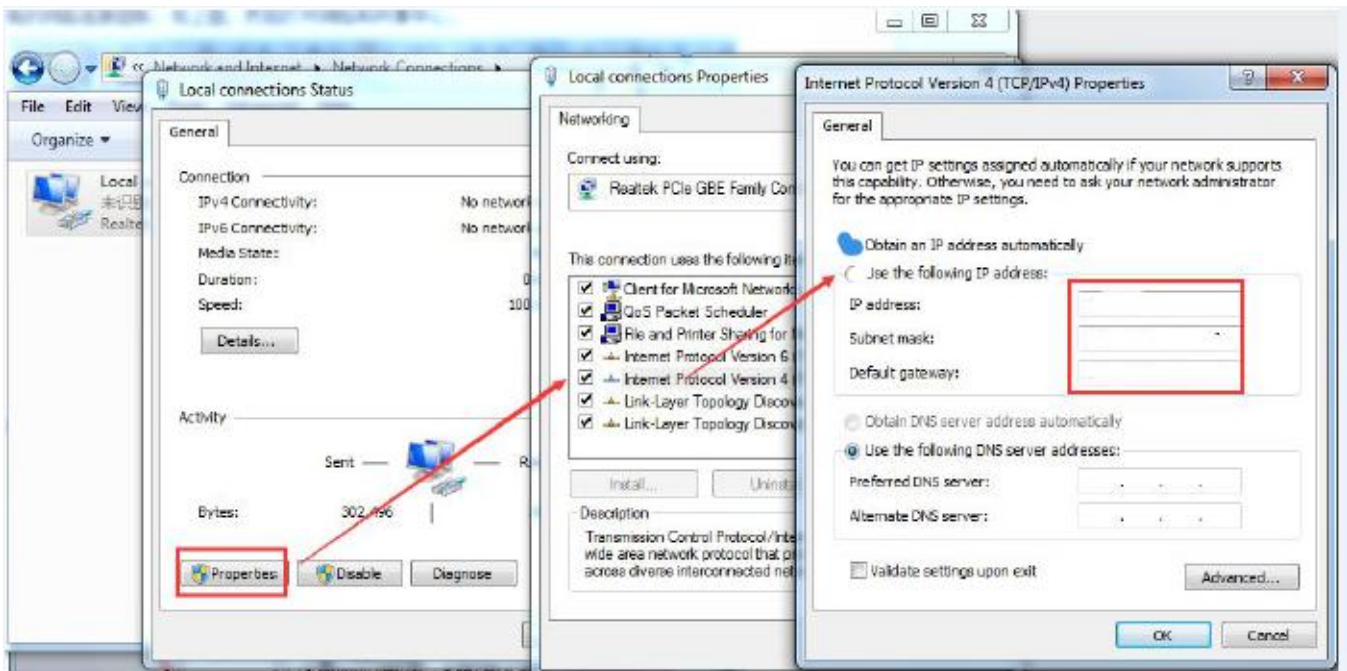


Diagram 1.2-1 Local Connection of the PC

- Power on the router using the adapter
- 2min waiting and the signal lights will on which means the 4G router connecting to the net.

1.3. Web Log and Netting Testing

Initial parameters:

Parameters	Initial value
Username	root
Password	root
IP	192.168.1.1

Form 1.3-1 Webpage Default Parameters

Fill:192.168.1.1 into the browser, both the username and password are root, then enter. The webpage are as following:

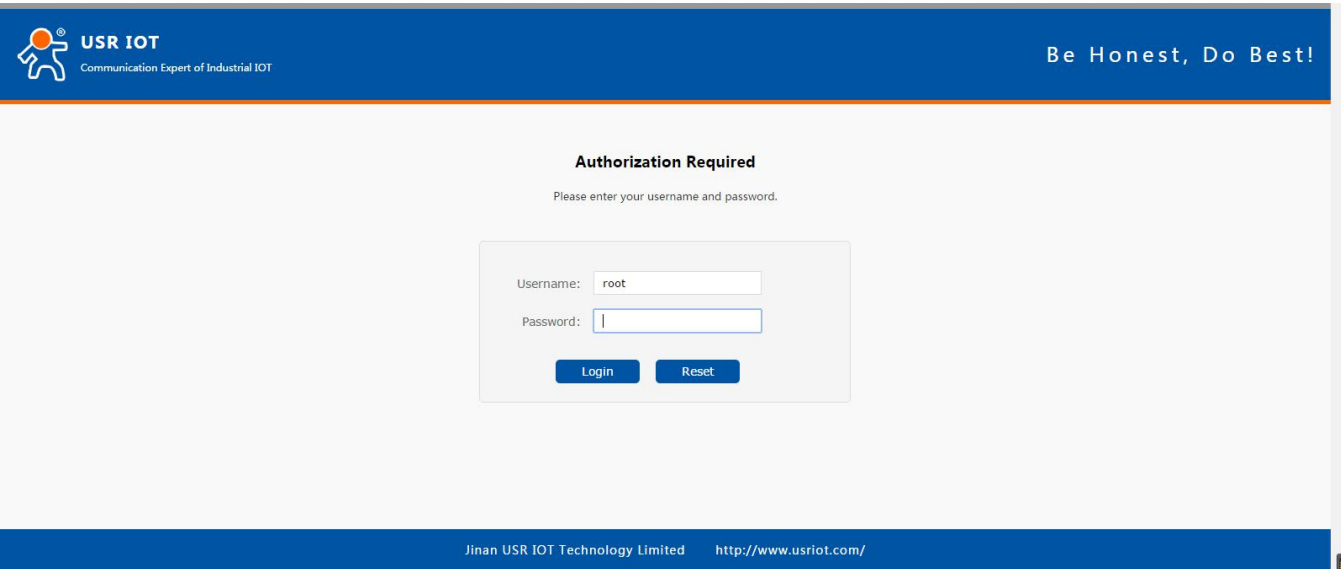


Diagram1.3-1 Login Webpage

Note:

- Change language on the top right.
- Default username and pass word :root

Testing results in the testing tool(4G cards are used in this testing. There might be difference between the regions.

In theory the max value would be 50Mbps upstream and 150Mbps downstream, as below:



Diagram 1.3-2 Net Testing

2. Product Overview

2.1. Brief Introduce

Dual 4G wireless router, G808 provides a solution for user accessing to net via WIFI or net port of the 4G. Adopting industrial CPU, work speeds reaching 580MHz, G808 provides reliable data transmission networking for the intelligent

power grids, personal medical, smart house and so on. Rich functions:dual 4G, net backups, APN, VPN, watchdog, firewall, NAT, DMZ and so on.

Wired WAN port, LAN port and wireless WLAN, dual 4G interface, several way to access the net.

2.2. Features

- Supports 4 LAN interface, 1 WAN interface, and a command serial port
- Supports 1 WLAN(802.11b/g/n)
- Supports LED indicators to show status(power, system, dual 4G type and signal power)
- Supports serial port, ssh, telnet and Web Server to manage and configure
- Supports Reload button to restore default settings by hardware way
- All Ethernet interface supports 10/100Mbps
- Supports VPN Client(PPTP, L2TP, IPSEC, OPENVPN, GRE, SSTP) and VPN encryption function
- Supports APN check the net, switching the net automatically, SIM information display and the APN special card
- Supports domain module, backup module, wired WAN online, several net to backup(can be select)
- Supports load balancing,
- Supports firewall, NAT, DMZ host, black and white list, IP speed, MAC speed limited
- Supports QOS, flow service and limiting speed according to interface
- Supports DDNS and port forwarding
- Supports WIFIDOG, this function need user custom according to own needs
- Supports static routes, PPPOE, DHCP/static IP
- Supports remote upgrade and remote monitoring
- Supports NTP, internal RTC
- Supports watchdog to guarantee the system stability

2.3. Basic Parameters

Model	Carrier/Region	Bands
—E	Europe/International (EMEA,Korea,Thailand,India) (HongKong,China) Southeast Asia	FDD:B1/2/3/5/7/8/20 TDD:B38/40/41 HSPA/UMTS: B1/2/5/8 GSM/EDGE: B2/3/5/8
—AU	Australia (Taiwan,China) New Zeland Latin America	FDD:B1/2/3/5/7/8/28 TDD:B38/40/41 HSPA/UMTS: B1/2/5/8 GSM/EDGE: B2/3/5/8
—A	AT&T,T-Mobile/North America	FDD:B2/4/12 WCDM:B2/4/5

Form 2.3-1 Model and Bands

Project		Instr
Name	USR-G808	4G wireless

Wired port	Wired WAN port	WAN * 1
	Wired LAN port	LAN * 4
	Net speed	10/100Mbps, Auto MDI/MDIX
WIFI	WIFI wireless LAN	Support 802.11b/g/n
	Antenna	WIFI antenna * 2
	Cover range	Open filed radius is 150m
SIM card and antenna	SIM/USIM card	Standard pin SIM card interface, 3V/1.8V SIM card *2
	Antenna	3/4G full frequency antenna*2 (4G-M/4G-A)
Button	Reload	One button to restore to the fault setting
LED	States instr light	Power, WIFI, Work, 2/3/4G(divide into SIM1 and SIM2),the indicators for the strength of the signal (for SIM1and SIM2), WAN*1, LAN*4,
Serial port	Console port	Manage the command serial port by webpage register.
Temperature	Work temperature	-20°C~ +70°C
	Storage temperature	-40°C~ +125°C
Humidity	Work humidity	5%~95%
	Storage humidity	1%~95%
Supply	Supply voltage	DC9~36V
	Current consumption	Under DC12V, average:391mA, maximum:578mA

Form 2.3-1 Basic Parameters
Consumption parameters:

The values are acquired under the full speed work, transmit with 1 WIFI access, 4 LAN ports access, WAN port access and dual 4G access and 10KByte/s.

Work mode	Running voltage	Average current	Max current
LAN+WAN speed communication(4G normal +WALN normal)	DC12V	391mA	578mA
Single LAN port full speed communication(4G normal +WALN normal)	DC12V	265mA	445mA
LAN+WAN full speed communication(no 4G+WALN normal)	DC12V	230mA	345mA
Single WAN □ full speed communication(no 4G+WALN normal)	DC12V	265mA	381mA

Form 2.3-2 Consumption Parameters

12V power supply and full speed work:

Average consumption:4.7W, max consumption 6.9W. Average current 391mA, max current 578mA

2.4. Hardware and Dimension



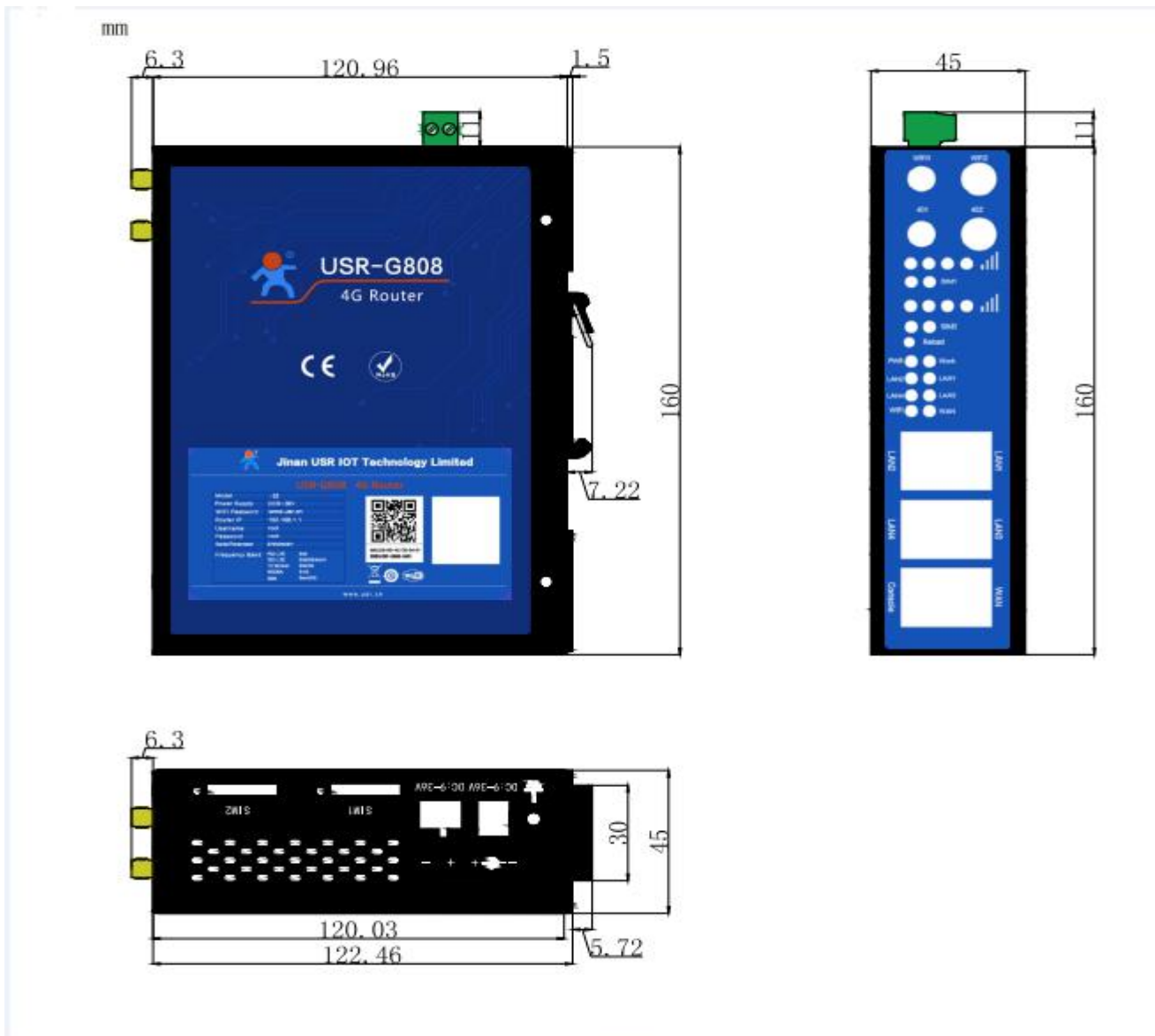
Diagram 2.4-1 Outlook

Num.	Name	Note
1	DC power	Supply DC:9-36V, standard5.5*2.1 supplier
2	DC terminal power	Supply range DC:9-36V, green terminal, size is 5.08mm-2P, note anti reverse
3	WAN port	WAN interface, 10/100Mbps, support Auto MDI/MDIX
4	LAN port	LAN interface, 10/100Mbps, support Auto MDI/MDIX

5	Console port	Manage the command serial port information via net to registration.
6	Instr light	20 road instr LED for status, the details are in the specific chapter.
7	SIM card seat	Drawer style SIM card seat, if need to installed SIM card, push the yellow button with a sharper, and exit the card.
8	Reload button	Reload: press for more than 5s and loosen,restore to default setting
9	WIFI antenna	2* 2.4G stick antenna
10	Full frequency antenna	2* full frequency sucker antenna.

Form 2.4-1 G808 Interface Parameters

Note: please distinguish the WIFI antenna and 4G antenna via the mark .


Diagram 2.4-2 Dimension

Note: 160*122.46*45mm(no power terminal, antenna and antenna seat)

3. Function

Introduce the functions of the G808 in this characters, including the user configuring , networking, common function and basic function introduce.

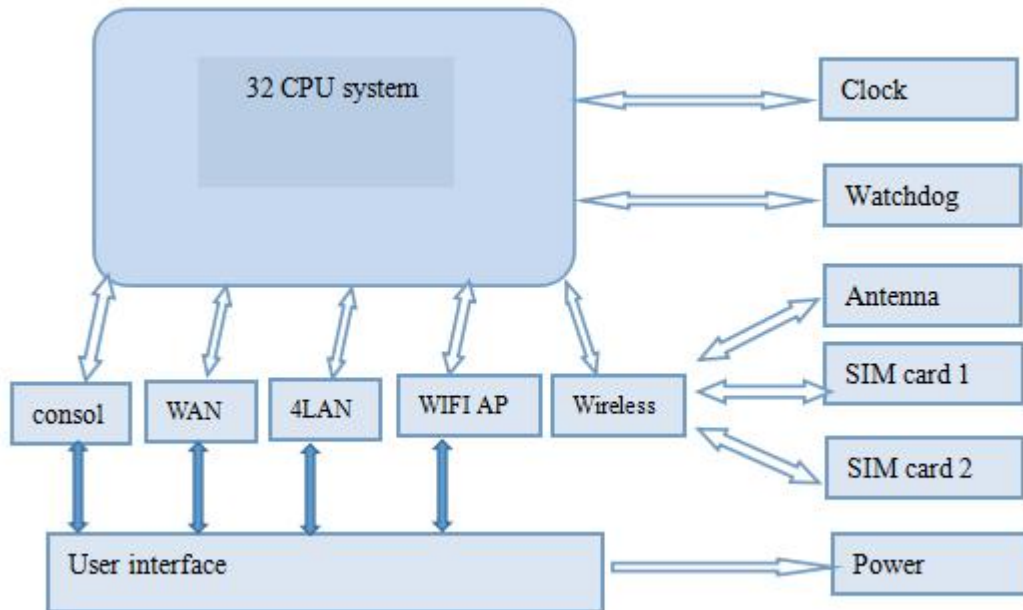


diagram 3-1 Product Function

Card name	Net card code name	Respond net interface name
LAN interface	br-lan	LAN
Default WIFI AP interface	ra0	LAN
WAN interface	eth0.2	WAN_WIRED
4G1 interface	eth1	WAN_4G1
4G2 interface	eth2	WAN_4G2

Form 3-1 Interface

3.1. User Configuring

After USR-G808 powered, it will access to 4G net and allow the devices under LAN access the external net.

Please ignore the configuring if you using the common SIM card, powering on is ok. if you using APN card, setting the accurate address, if you need to use the VPN, port mapping and so on, reference to the related function chapter.

- 1.Power off the G808 and insert SIM card.
- 2.Connect WIFI antenna and 4G antenna.(the longer one is 3G/4G antenna and shorter one is EIFI antenna)
- 3.Power on the G808 by 12V power supply.
- 4.Waiting about 2 min, 2/3G instr LED begin light, and success. Then you can be online.
5. connect PC or mobile to the G808 router via LAN interface or WIFI interface. The pass word of the WIFI is “www.usr.cn”
6. Then you can log in the webpage of the router(default address is:192.168.1.1. both the username and password are “root”)

Application diagram as follow, user can access internet through LAN interface or WLAN interface of G808:



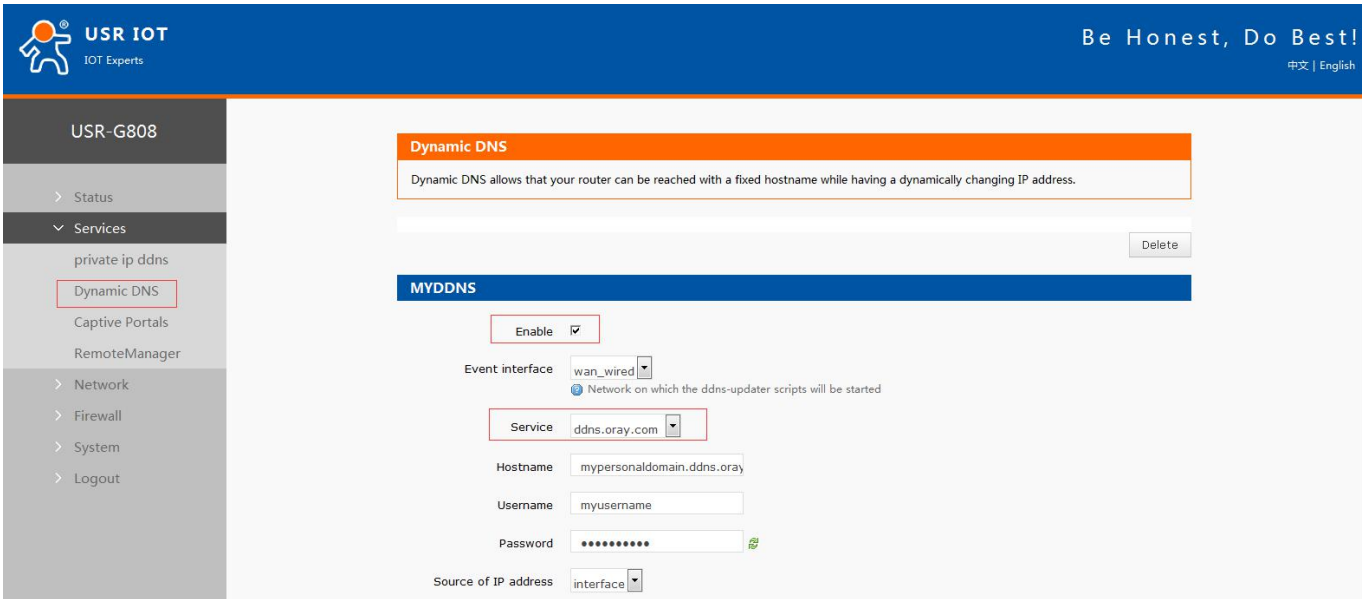
Diagram 3.1-1 Application diagram

3.2. Common Function

3.2.1. DDNS

There are two situations to adopt DDNS function:

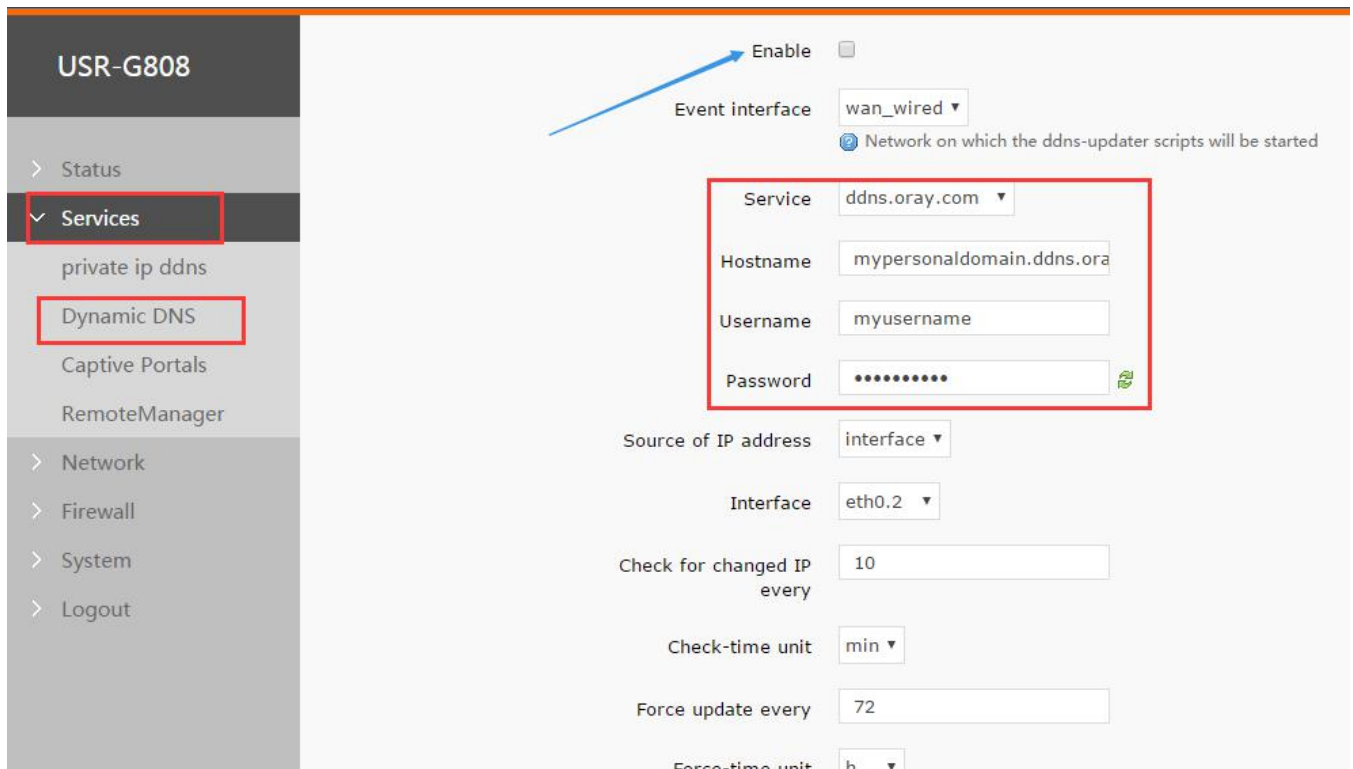
- G808 supports, user can choose one operator on ‘Service’(here we use the ddns.oray.com)


Diagram 3.2.1-1 DDNS Configuration

Note: If user wants to enable this function, the network that G808 belongs to must be distributed independent public network IP.

Default disable, please enable it if you want to use.

Setting step are as bellow:


Diagram 3.2.1-2 DDNS Setting Webpage

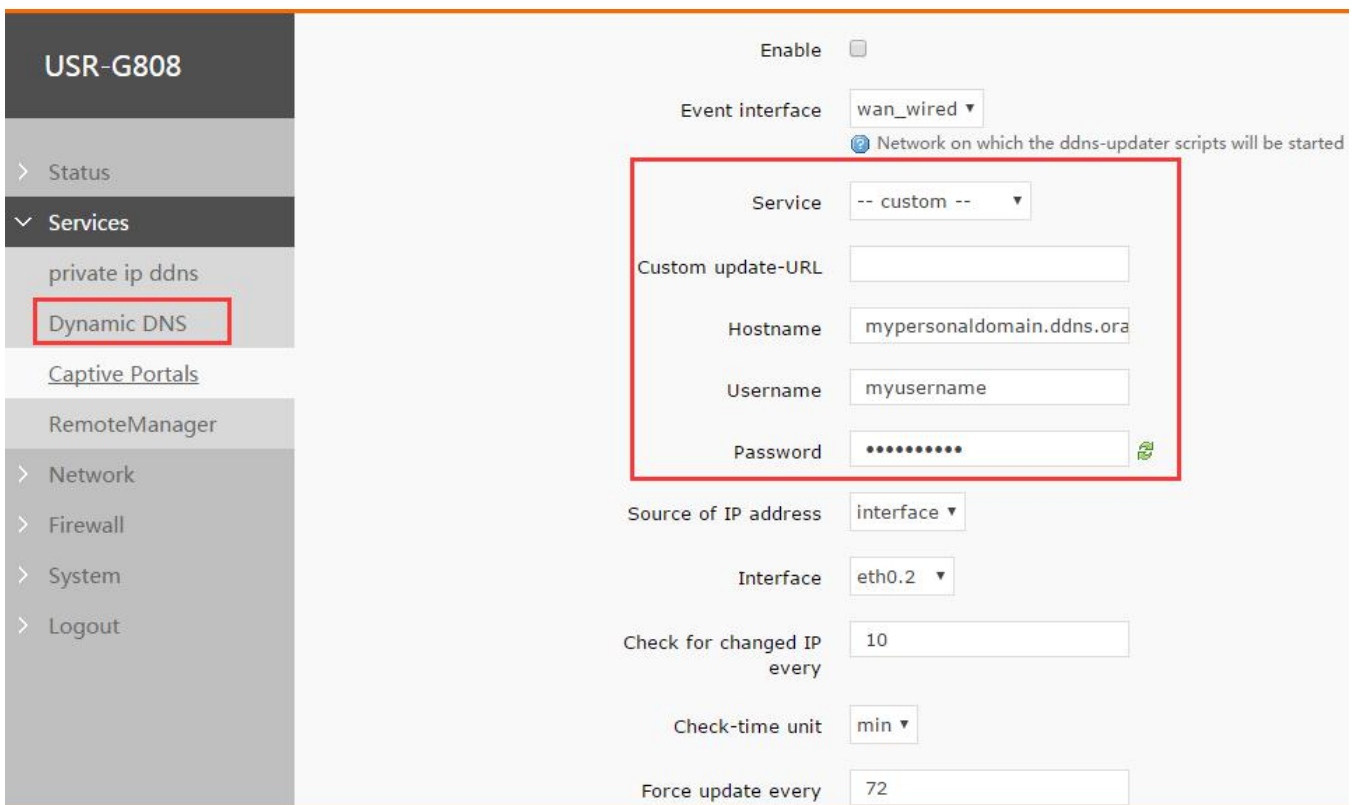
Please fill the parameters as the form below:

Function	Content	Note
Enable	Choose the DDNS function	Default disable, users can

		choose to enable
Event interface	Choose the WAN port according your requirement	E.g.choose wan_wired
Service /URL	Fill the DDNS server address	E.g. ddns.oray.com
Domain name	Fill the domain name you apply	E.g. 1a516r1619.iask.in
Username	Username	E.g. ouclihuibin123
Password	Password	E.g. ouclihuibin1231
IP original	Choose the interface here	Select interface
Interface	Name of the interface	E.g. choose eth0.2 here, (wired WAN port)
Check the interval of the IP changing time	Check the interval for IP changing for IP might changing commonly. The value is smaller and the check will be more frequency	E.g. 1 min
Forced update interval	Forced upgrade interval	E.g. 72min

Form 3.2.1-1 Parameters for DDNS

- G808 doesn't support, user need choose '--custom--' on 'Service' and write correct service provider.


Diagram 3.2.1-3 DDNS Setting Webpage

This function supports accessing to the router via domain name remotely

Parameters filled as below: apply a hostname to point you IP of the WAN

username

Password

Function	Content	Note
----------	---------	------

Enable	Choose the DDNS function	Default disable, users can choose to enable
Event interface	Choose the WAN port according your requirement	E.g.choose wan_wired
Service /URL	Fill the DDNS server address Format: http://username:password@ddns.oray.com/ph/update?hostname=domainname	E.g. http://ouclihuibin123:ouclihuibin1231@ddns.oray.com/ph/update?hostname=1a516r1619.iask.in
Domain name	Fill the domain name you apply	E.g. 1a516r1619.iask.in
Username	Username	E.g. ouclihuibin123
Password	Password	E.g. ouclihuibin1231
IP original	Choose the interface here	Select interface
Interface	Name of the interface	E.g. choose eth0.2 here, (wired WAN port)
Check the interval of the IP changing time	Check the interval for IP changing for IP might changing commonly. The value is smaller and the check will be more frequency	E.g. 1 min
Forced update interval	Forced upgrade interval	E.g. 72min

Form 3.2.1-2 Parameters for DDNS

- Check the DDNS work or not(restart the router to make it work)
- Check your public IP
- Then ping the domain name:1a516r1619.iask.in on the PC, if it is ok, the DDNS can be work

● Function feature

- User should choose 'Enable' on above figure to enable DDNS function at first
- Reset G808 to make new parameters take effect.
- Fill in the parameters strictly, make sure the accuracy of them like: service/URL, domain name, user name, password and the interface.
- Even though the router under the subnet,this function can enable dynamic domain name
- DDNS+port mapping can enable that remote access the subnet under the local router.
- Add more than one DDNS domain name.

3.2.2. WIFIdog

Have the device enter the external net. Then the first time for the device to enter the external net, login a certification webpage and do the certification.

The sense for WIFIdog:①to keep the safety of the LAN, record the illegal behaviors such as net attack when using the public net. ②using in the advertisement. Collecting the information of he users under the router if they allow which is convenient for factories to promote.

Note: default disable, please enable it at first

USR-G808

Configuration

General Settings | **whitelist** | Advanced Settings

Enable Enable or Disable wifidog

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:
Domain name or ip

Save

Diagram 3.2.2-1 WIFIdog Configuration 1

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.com
Domain name or ip

Save

Diagram 3.2.2-2 WIFIdog Configuration 2

The screenshot shows the 'Advanced Settings' tab for the 'WIFI dog' configuration. The 'Internal Interface' is set to 'br-lan' and the 'External Interface' is set to 'eth0.2'. The 'wifidog server file path' is set to '/apps/wifiauth/'. Other settings include 'wifidog server port' (2060), 'HTTP Port' (80), 'Maximum access number' (40), and 'Check interval' (60).

Diagram 3.2.2-3 WIFI dog Configuration 3

User need choose 'Enable' and 'daemon enable' to use WIFI dog function. After configuring and clicking 'Save', user need reset G808 to make changing take effect.

Function	Parameters setting(if you want to use)	Note
Enable certification	choose	Choose if you need, default keep disable
Daemon enable	choose	Choose if you need, default keep disable
AP ID	nfuold700	AP code
WIFI dog server address	E.g. www.xxx.cn	Assist certification server address
Internal interface	br-lan	The name of the LAN
External interface	eth0.2	Wired WAN port name (if you access the net via 4G ,

		fill the eth1)
Certification server road	/apps/WIFIguanjia/	Certification server road

Form3.2.2-1 WIFIdog Default Parameters List

Fill the parameters in the form and then open a browser enter a IP randomly, you can see the certification webpage, fill the phone number and enter.

Cooperating server to realize the SMS certificating login, wechat in and QQ in, of course you need custom the server software.

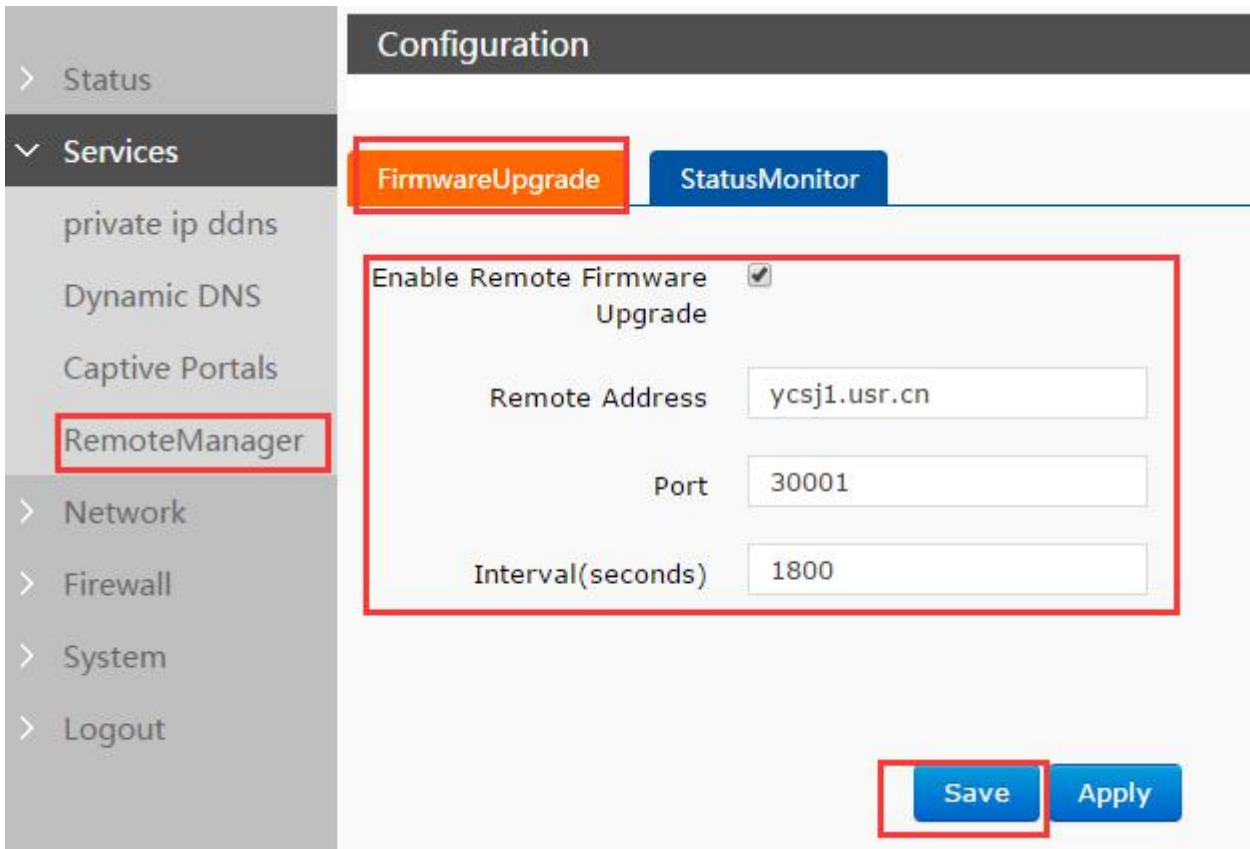
Note:

- The WIFIdog function in this router is demo. Please contact us and have a custom if you need:
<http://www.usr.cn/Custom/index.html>
- If you do not need it, please do not enable it, otherwise the router can not access the external net(certificate and you can access)
- Please do not enable this function with MultiWAN!!! They can not be used at same time.

3.2.3. Remote Manager

- Remote Firmware Upgrade

User can configure this function by Web Server as follow:


Diagram 3.2.3-1 Remote Firmware Upgrade

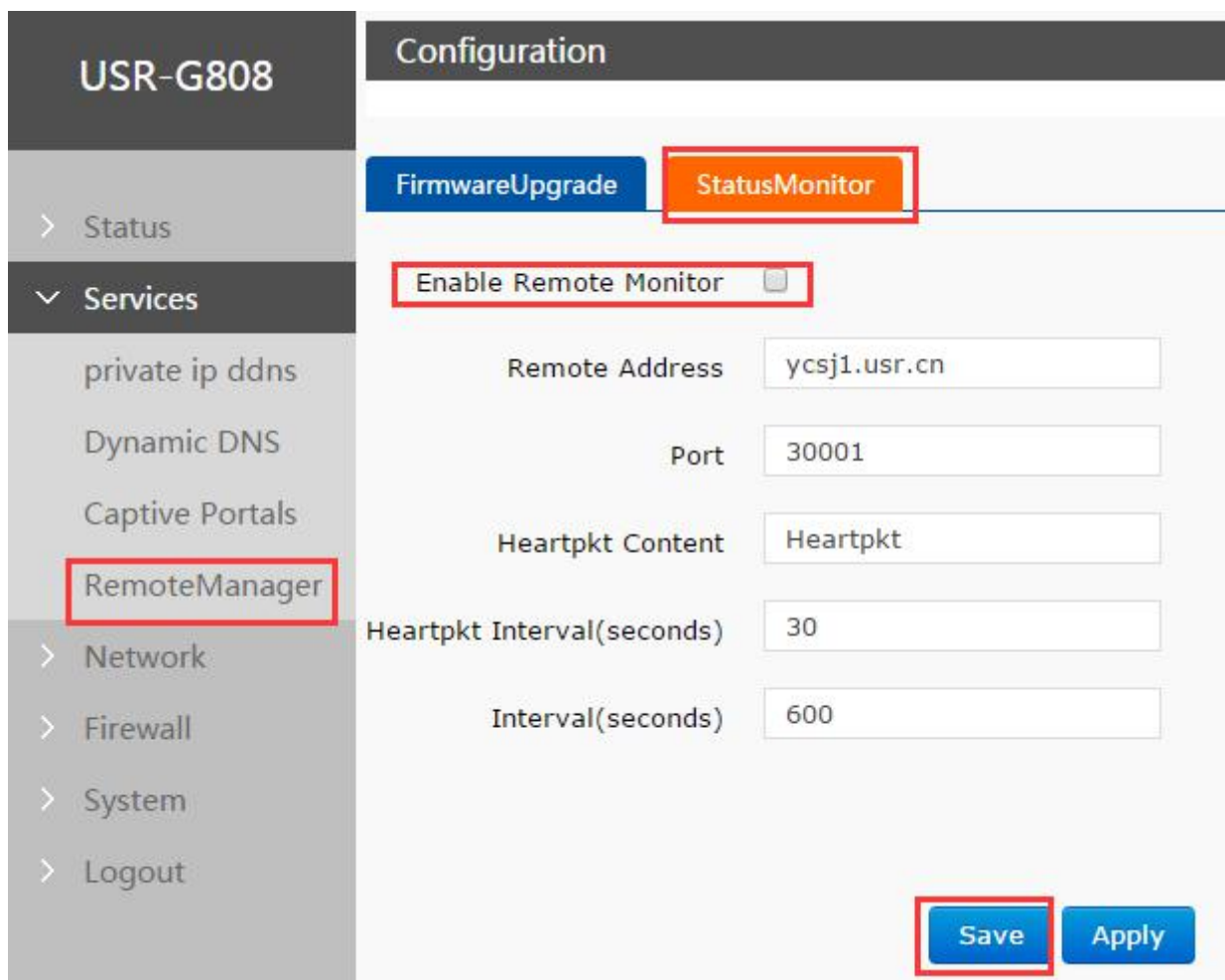
Function	Parameters setting (if will be need)	Note
----------	--------------------------------------	------

Enable remote firmware function	Choose	Default enable
Remote address	Remote firmware upgrade server address	Default ycsj1.usr.cn
Port	Remote upgrade firmware server port	Default 30001
Interval	The interval device sending information to server	Default 1800s

Form 3.2.3-1 Remote Upgrade Default Parameters

- **Remote Monitor**

This function can realize reporting G808 information(Such as flow, firmware version, RSSI, IMEI) to Remote Monitor server and Remoter Monitor server can also send commands to control G808. User can configure this function by Web Server as follow:



The screenshot shows the USR-G808 web interface. On the left is a navigation menu with 'RemoteManager' highlighted. The main area is titled 'Configuration' and has two tabs: 'FirmwareUpgrade' and 'StatusMonitor'. The 'StatusMonitor' tab is active. Below the tabs, there is a checkbox labeled 'Enable Remote Monitor' which is checked. Below this are several input fields: 'Remote Address' (value: ycsj1.usr.cn), 'Port' (value: 30001), 'Heartpkt Content' (value: Heartpkt), 'Heartpkt Interval(seconds)' (value: 30), and 'Interval(seconds)' (value: 600). At the bottom right, there are 'Save' and 'Apply' buttons.

Diagram 3.2.3-2 Remote Monitor

Function	Parameters setting (if will be used)	Note
Enable remote monitor	choose	Default is disable
Remote address	Remote firmware upgrade server address	Default ycsj1.usr.cn
Port	Remote monitor server port	Default 30001
Heartpkt content	The heartbeat package content	Default heartpkt

	that device send to serve.	
Heartpkt interval	The interval that device send heartbeat package.	Default 30s
Interval	the interval that device submit the operating information.	Default 600s

Form 3.2.3-2 Remote Monitor Default Parameters

Note: the detailed using of remote monitor and remote upgrade, please login yxsj1.usr.cn

3.2.4. LAN Interface

- G808 supports four wired LAN interfaces(LAN1~LAN4).
- WIFI interface also belongs to LAN interface(wireless LAN interface).
- Default settings: Static IP (IP address: 192.168.1.1);
- Subnet mask: 255.255.255.0;
- Enable DHCP Server function.
- LAN interface functional diagram as follow:
- Supports simple status statistics function

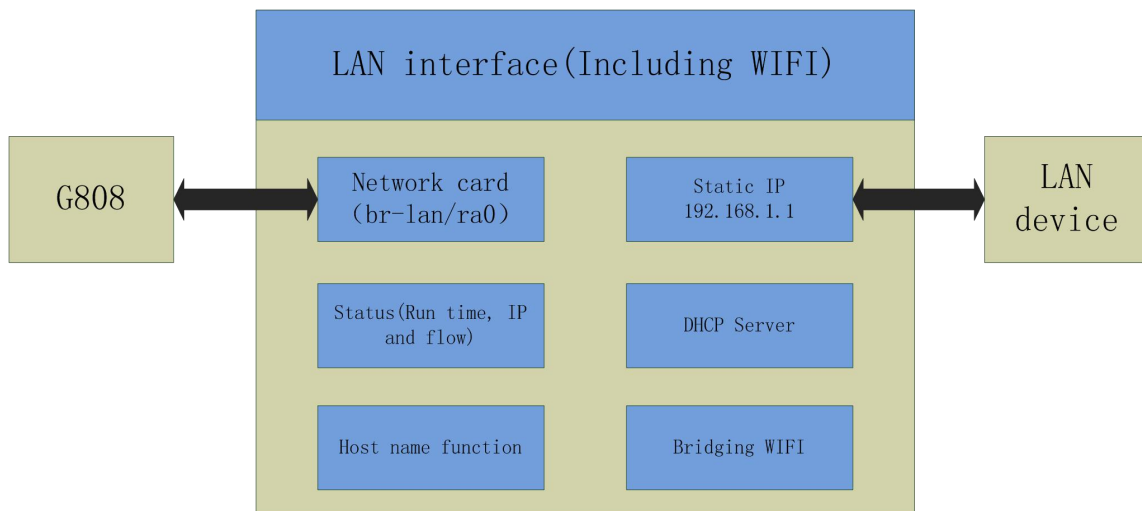


Diagram 3.2.4-1 LAN Interface Functional Diagram

User can configure LAN interface as follows:

Network	Status	Actions
LAN br-lan	Uptime: 0h 57m 50s MAC-Address: D8:B0:4C:D9:4F:30 RX: 1.54 MB (18252 Pkts.) TX: 1.35 MB (9755 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDD1:B494:14C5:0:0:0:1/60	Connect Stop Edit Delete
WAN_4G1 eth2	Uptime: 0h 0m 0s MAC-Address: E2:7C:98:39:B0:38 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN_4G2 eth1	Uptime: 0h 0m 0s MAC-Address: 00:A0:C6:00:00:00 RX: 0.00 B (0 Pkts.) TX: 10.14 KB (38 Pkts.)	Connect Stop Edit Delete
WAN_WIRED eth0.2	Uptime: 0h 0m 0s MAC-Address: D8:B0:4C:D9:4F:30 RX: 0.00 B (0 Pkts.) TX: 395.76 KB (1160 Pkts.)	Connect Stop Edit Delete

[Add new interface...](#)

Diagram 3.2.4-2 LAN Interface configuration 1

USR-G808

General Setup Physical Settings Firewall Settings

Status

br-lan

Uptime: 0h 59m 10s
MAC-Address: D8:B0:4C:D9:4F:30
RX: 1.60 MB (18857 Pkts.)
TX: 1.46 MB (10219 Pkts.)
IPv4: 192.168.1.1/24
IPv6: FDD1:B494:14C5:0:0:0:1/60

Protocol: Static address

Really switch protocol? Switch protocol

IPv4 address: 192.168.1.1

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers: 8.8.8.8, 8.8.4.4

Diagram 3.2.4-3 LAN Interface configuration 2

3.2.5. DHCP

Default DHCP sever function of the LAN enable(choose to disable) all the device access to the LAN interface can obtain IP address automatically.

DHCP Server default range of distribution is from 192.168.1.100 to 192.168.1.250

Default address lease time is 12 hours. Address range and lease time can be changed.

After entering Web Server LAN interface configuration web page, user can find 'DHCP Server' on Web Server as follow:

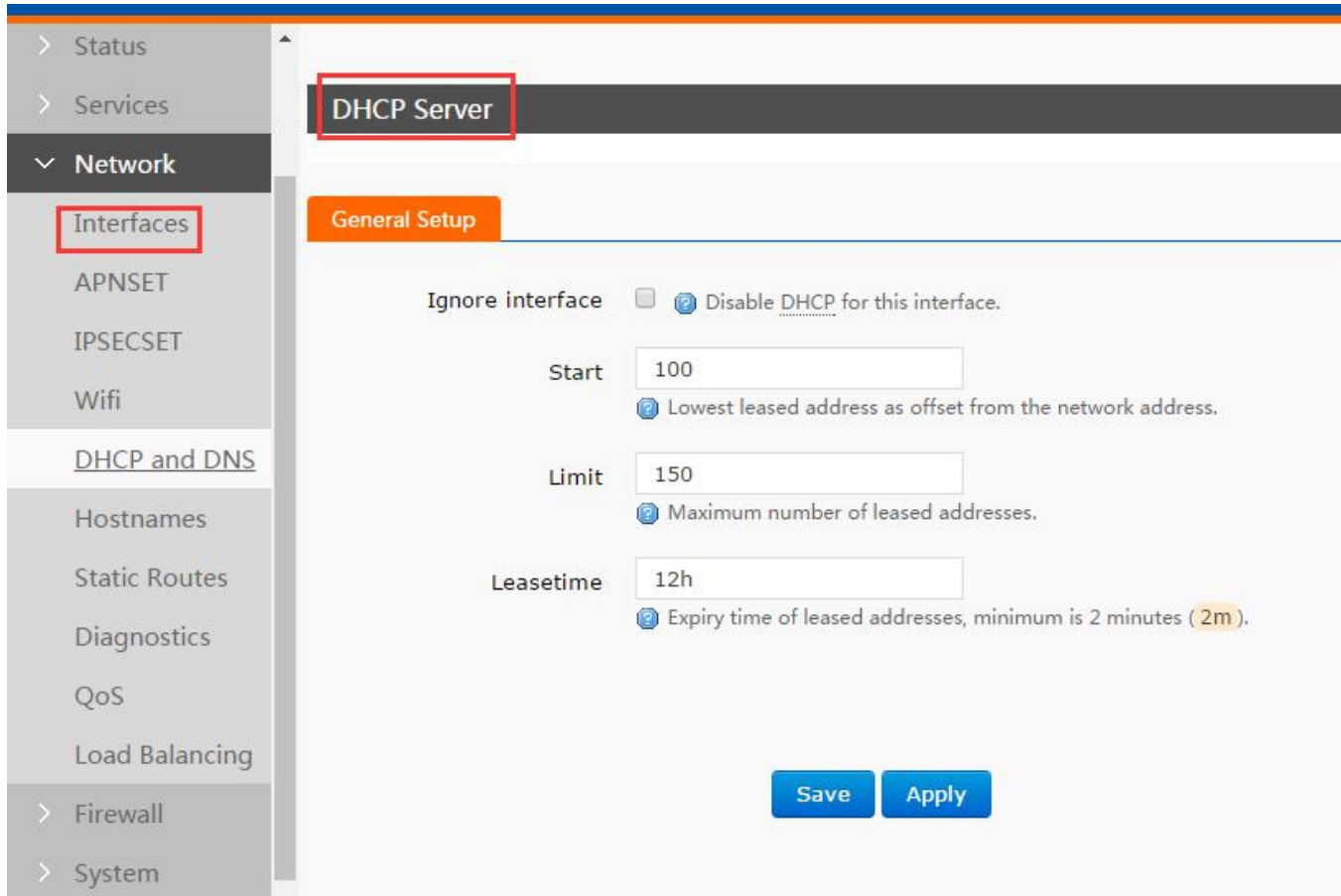


Diagram 3.2.5-1 DHCP Server Configuration

3.2.6. WAN Interface

- G808 supports one wired WAN interface.
- WAN interface supports DHCP Client, static IP and PPPOE mode.
- Default setting is DHCP Client mode.

User can configure WAN interface as follows:

The screenshot shows the 'Network' configuration page for the USR-G808 device. The left sidebar contains a navigation menu with 'Network' selected. The main content area displays a table of network interfaces with their status and available actions.

Network	Status	Actions
LAN br-lan	Uptime: 1h 5m 11s MAC-Address: D8:B0:4C:D9:4F:30 RX: 1.84 MB (21438 Pkts.) TX: 1.78 MB (12044 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDD1:B494:14C5:0:0:0:1/60	Connect, Stop, Edit, Delete
WAN_4G1 eth2	Uptime: 0h 0m 0s MAC-Address: E2:7C:98:39:B0:38 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect, Stop, Edit, Delete
WAN_4G2 eth1	Uptime: 0h 0m 0s MAC-Address: 00:A0:C6:00:00:00 RX: 0.00 B (0 Pkts.) TX: 33.15 KB (120 Pkts.)	Connect, Stop, Edit, Delete
WAN_WIRED eth0.2	Uptime: 0h 0m 0s MAC-Address: D8:B0:4C:D9:4F:30 RX: 0.00 B (0 Pkts.) TX: 446.03 KB (1307 Pkts.)	Connect, Stop, Edit, Delete

At the bottom of the interface list, there is a button labeled 'Add new interface...'. The 'Edit' button for the 'WAN_4G1' interface is highlighted with a red box.

Diagram 3.2.6-1 WAN Interface Configuration 1

The screenshot shows the 'Common Configuration' page for a WAN interface. The left sidebar has 'Network' selected. The main content area includes a description of the configuration options and a form for setting the interface protocol.

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several 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: eth1
MAC-Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP: 4GRouter

Save | Apply

Diagram 3.2.6-2 WAN Interface Configuration 2

3.2.7. WLAN

- G808 is a AP actually and supports other STA devices connecting to.
- G808 supports at most 24 STA devices to connect
- About 150 meters radius WIFI coverage area in open field.
- LAN and WLAN can be exchange
- Radio on/off default be on
- WIFI interface functional diagram as follow:

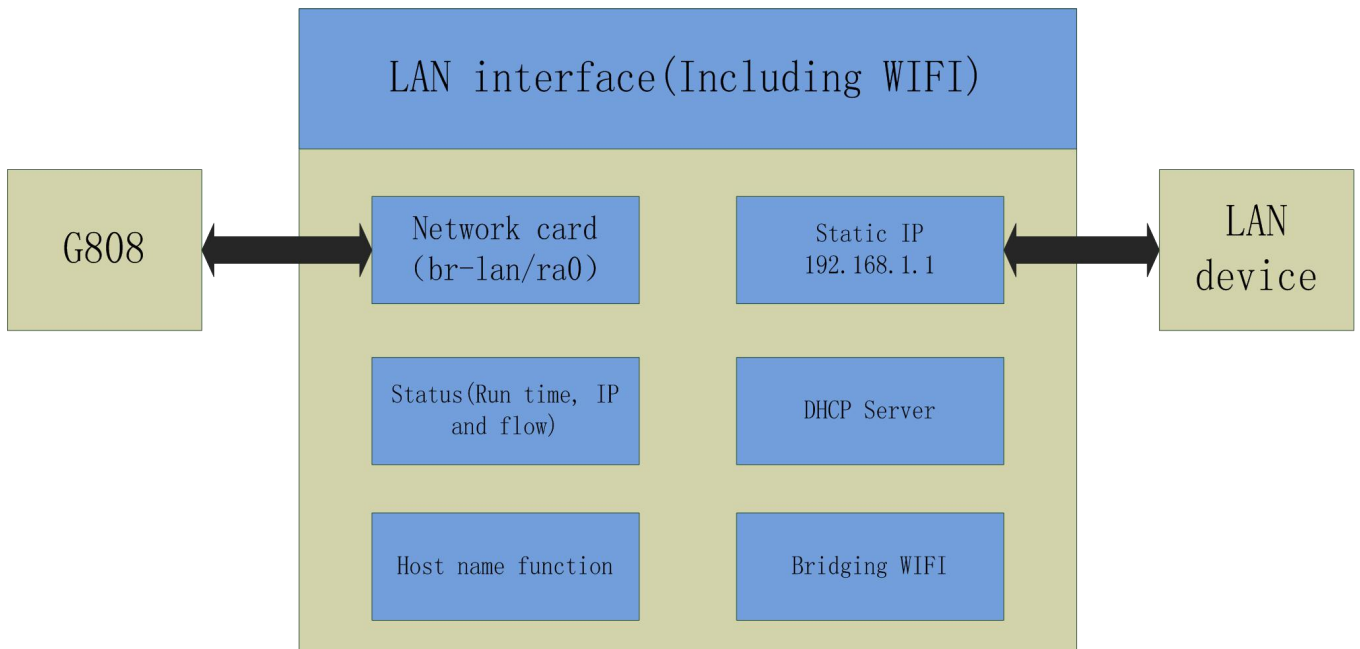


Diagram 3.2.7-1 WIFI Interface Functional Diagram

Default settings of WIFI interface as follows:

Parameters	Default setting
SSID	USR-G808-XXXX(XXXX is MAC address)
Password	www.usr.cn
Channel	Auto
Bandwidth	40MHz
Encryption method	WPA2-PSK

Form 3.2.7-1WIFI Interface Default Settings

User can configure WIFI interface as follow:

multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup | **Advanced Settings**

Status: **Mode:** Master | **SSID:** USR-G808-4F30
BSSID: D8:B0:4C:D9:4F:2F
Channel: 4 | **Bitrate:** 300.0 Mbit/s

Radio on/off: on

Network Mode: 802.11b/g/n

Channel: auto

Band Width: 40MHz

Interface Configuration

Diagram 3.2.7-2 WIFI Setting Webpage

Band Width: 40MHz

Interface Configuration

General Setup | **Wireless Security**

ESSID: USR-G808-4F30

Mode: Access Point

Network: lan: wan_4g1: wan_4g2: wan_wired:

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID:

Diagram 3.2.7-3 Modify the ESSID

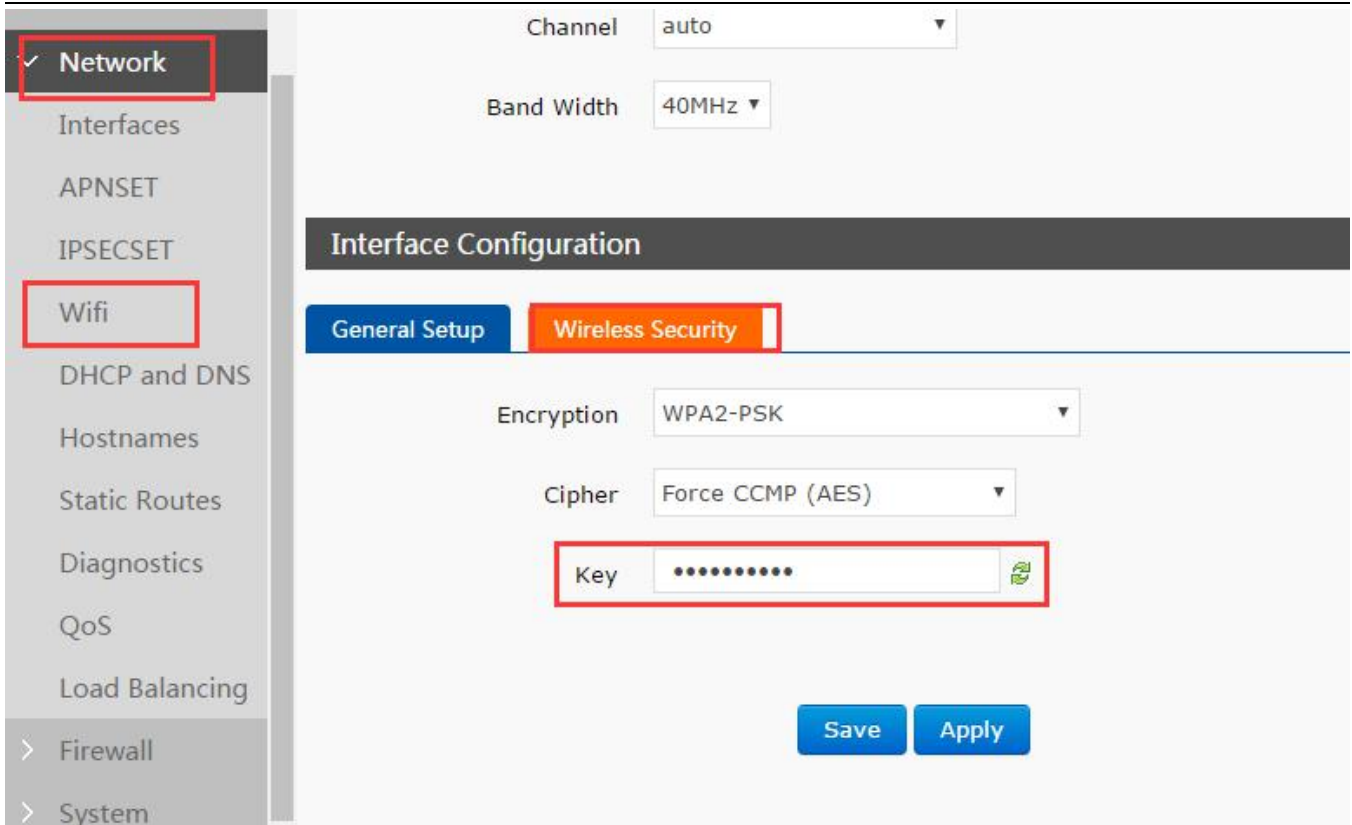


Diagram 3.2.7-4 Setting the WIFI Password

User can change Radio on/off to off to close WIFI interface(effect immediately), network mode, channel and band width

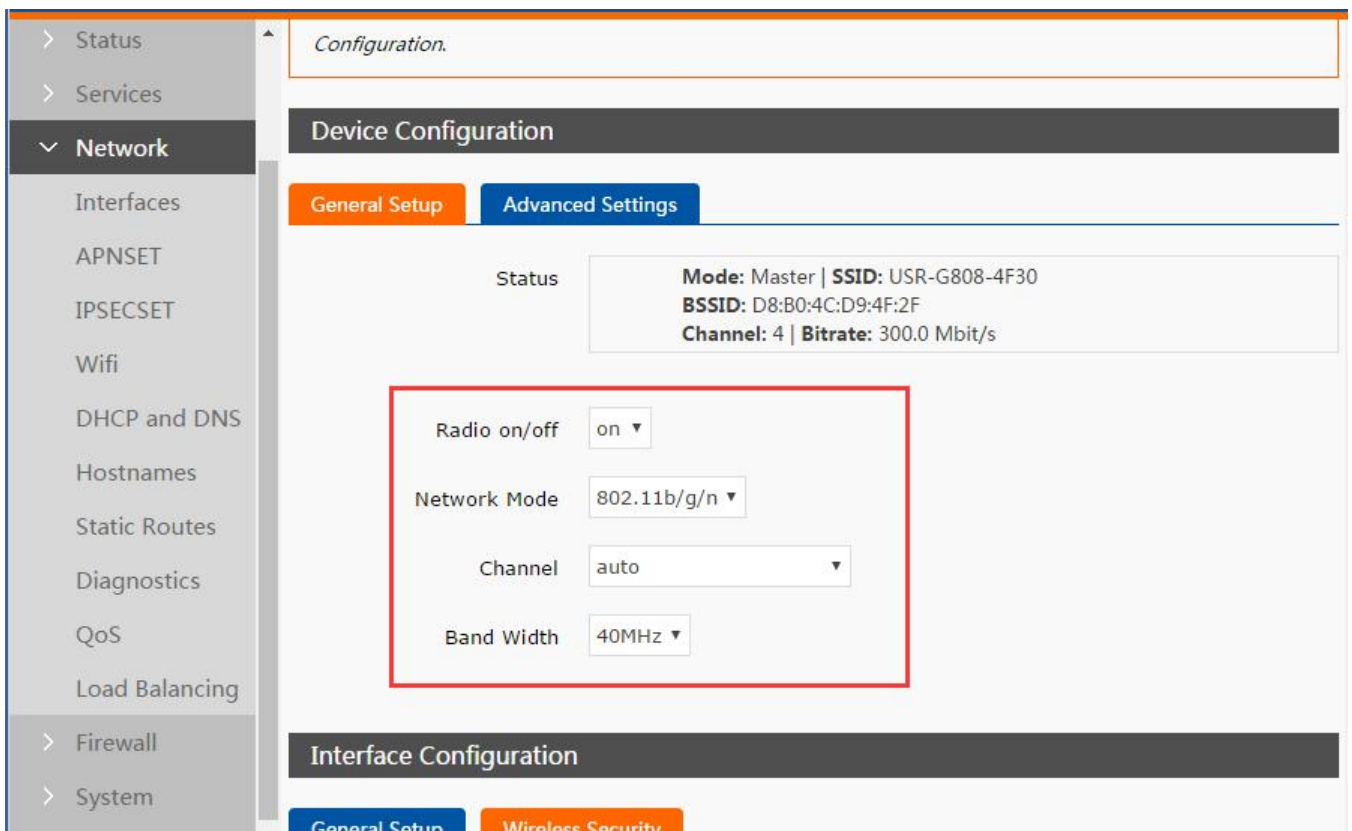


Diagram3.2.7-5 Other WIFI Setting

3.2.8. Dual 4G Interface

G808 supports dual 4G interfaces to access internet. 4G interface functional diagram as follow:

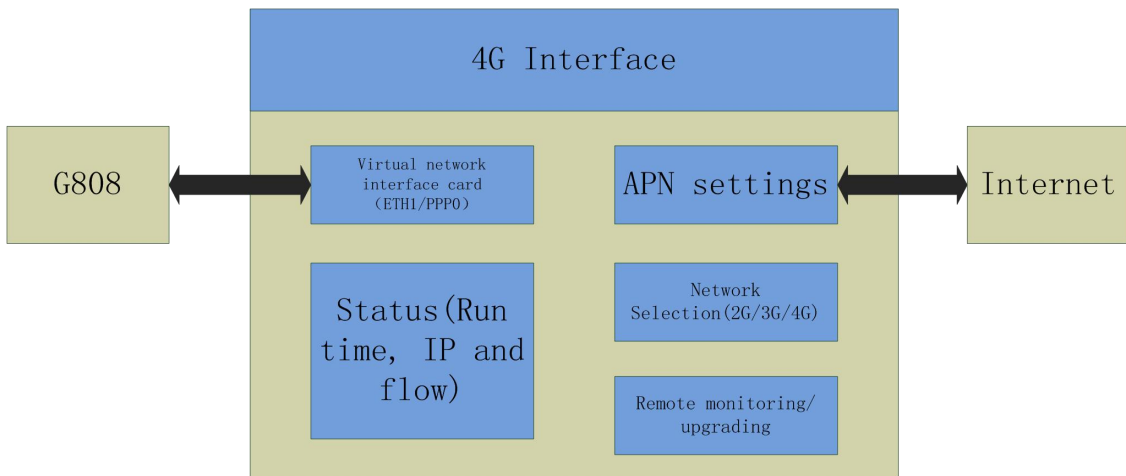


Diagram 3.2.8-1 4G Interface Functional

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

Network	Status	Actions
LAN br-lan	Uptime: 1h 18m 45s MAC-Address: D8:B0:4C:D9:4F:30 RX: 2.33 MB (26754 Pkts.) TX: 2.34 MB (15554 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDD1:B494:14C5:0:0:0:1/60	Connect Stop Edit Delete
WAN_4G1 eth2	Uptime: 0h 0m 0s MAC-Address: E2:7C:98:39:B0:38 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN_4G2 eth1	Uptime: 0h 0m 0s MAC-Address: 00:A0:C6:00:00:00 RX: 0.00 B (0 Pkts.) TX: 33.38 KB (120 Pkts.)	Connect Stop Edit Delete
WAN_WIRED eth0.2	Uptime: 0h 0m 0s MAC-Address: D8:B0:4C:D9:4F:30 RX: 0.00 B (0 Pkts.) TX: 538.72 KB (1578 Pkts.)	Connect Stop Edit Delete

Add new interface...

Diagram 3.2.8-2 4G Interface Configuration

- The protocol of the 4G interface: please keep default and do not modify
- The router using wired WAN port at first, then are the 4G nets. choose one interface in one application
- If you using APN private card, refer to the APN setting chapter.

3.2.9. APN Setting

APN parameters setting are as follows, including SIM 1 setting and SIM2 setting:

When user want to configure and use G808, the first and most important step is to configure APN settings. Different operator have different APN(access point name). If user uses the SIM card from the operator, must know the APN. User can ask SIM card operator for APN information. There are three main parameters about APN: APN address, username and password. Sometimes only configuring APN address is enough.

APN configuration by Web Server as follow:

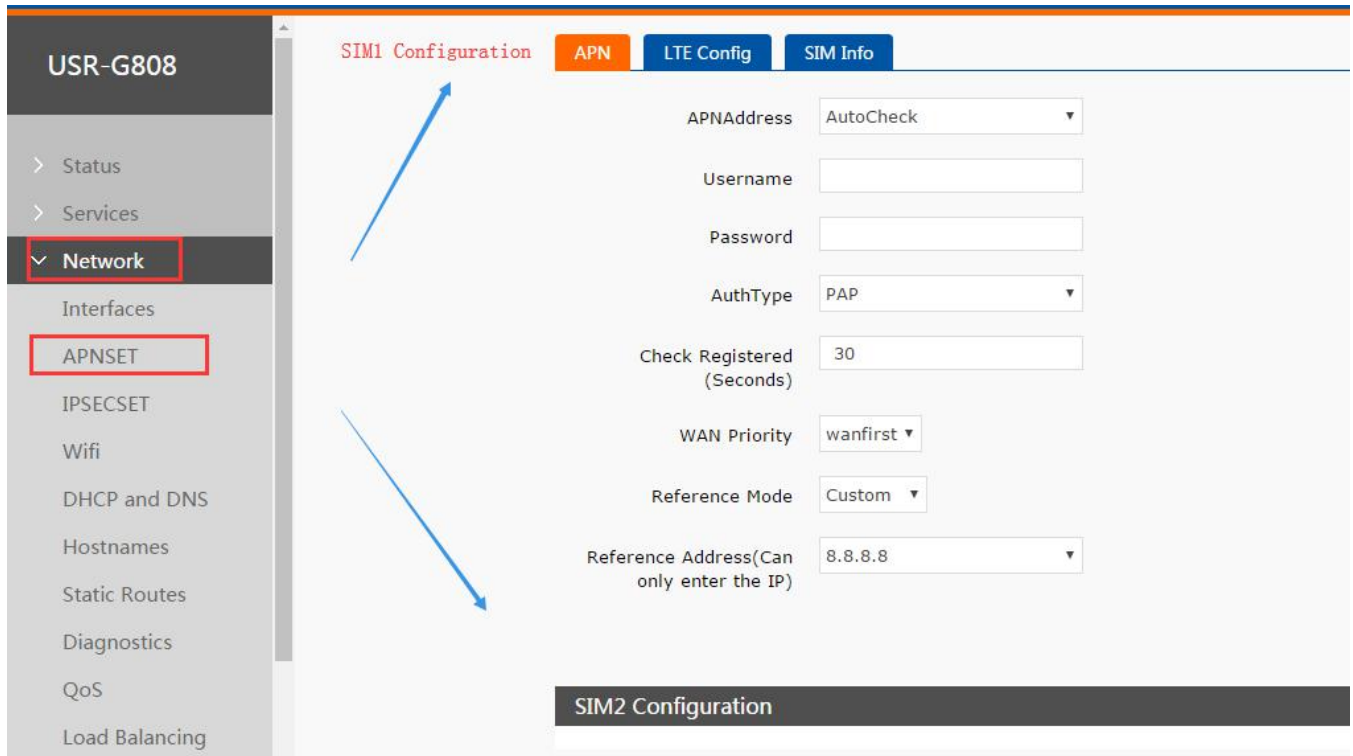


Diagram 3.2.9-1 APN configuration

APN Address: Default is AutoCheck, user can choose ‘--custom--’ and write correct SIM card APN address. And user can keep AuthType and Check Registered (Seconds) as default settings.

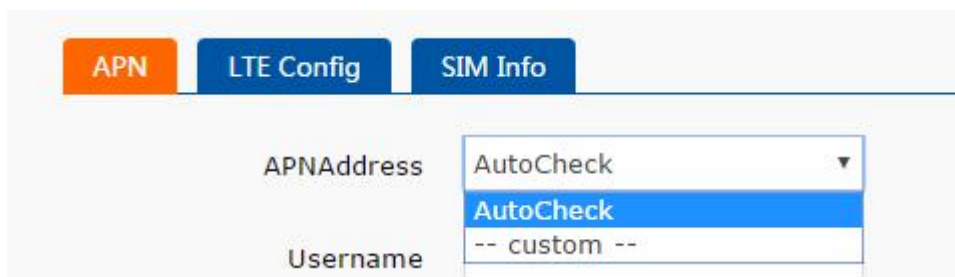


Diagram 3.2.9-2 APN Address Select

Parameters name	Function
APN address	Please fill the right APN address,default is check automatically.
Username	Default none, please fill if you use the APN

password	Default none, please fill if you use the APN
PDP type	Default
Auth Type	Default
Others	Please keep default

Form 3.2.9-1 APN Parameters

- Common phone card, please ignore it.
- If using the APN card, please fill the APN address , username and the password.
- The configuring way for SIM 1 and SIM2 are same.
- After user configuring successfully, user can click ‘SIM Info’ above to check SIM card 1 and SIM card 2 information.

● **Modify APN**

Firstly, select the “custom” in the APN, and fill the right APN address in it. After setting ,please restart the router.

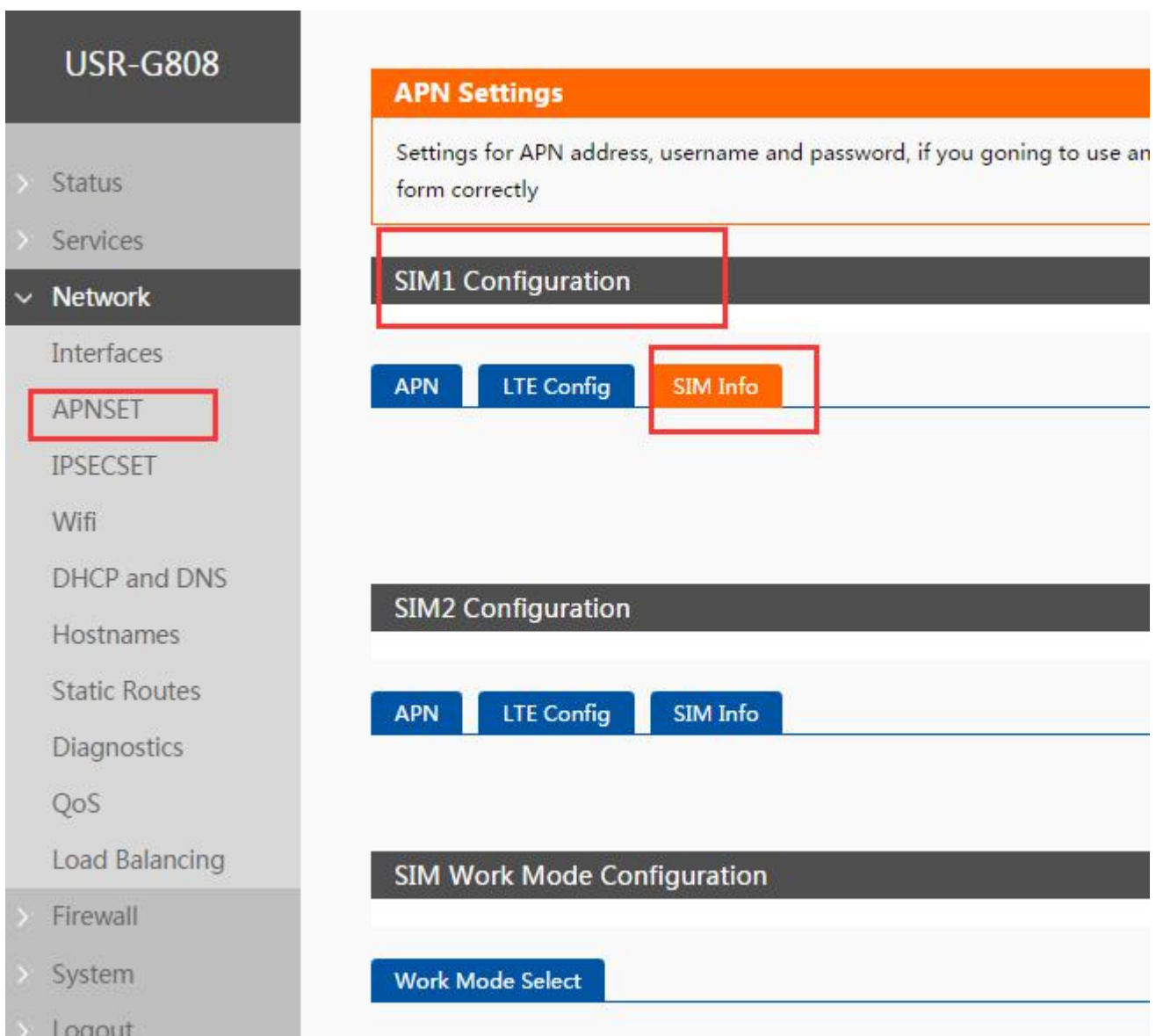


Diagram 3.2.9-3 SIM card 1 Information

● **Network format selection**

The network format, default is automatically: 4G →3G →2G, and access to the net automatically. If what you need

is not the 4G SIM card, or the net need to appoint(such as using the 2G or 3G), please select the network format, otherwise it will be affect for the netting rate.

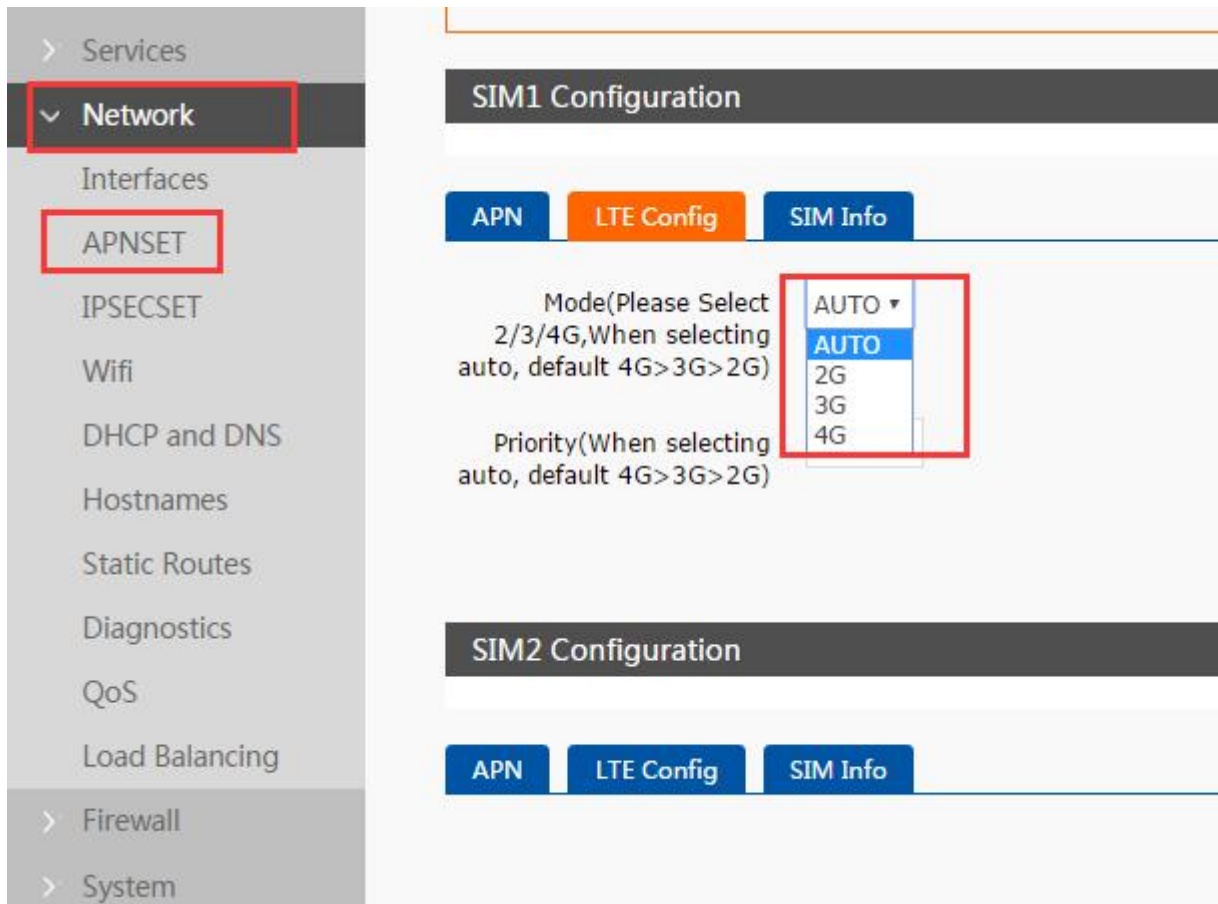


diagram 3.2.9-4 LTE Config

If you choose the 3G mode or 3G at first, when connecting the net, the router will connect the 3G net more accuracy.

Selection	Means	Order	Note
Automatic	Select automatically	4G>3G>2G	Default
2G	Using 2G	2G>3G>4G	When using the 2Gcard
3G	Using 3G	3G>2G>4G	When using the 3G card
4G	Using 4G	4G>3G>2G	When using the China Mobile/China Unicom/China Telecom 4G
Others			

Form 3.2.9-2 Network Format Selection

- **SIM card information display**

In this webpage, there is the information of the SIM1 and SIM2 where display the detailed parameters to configuring. If there is some issue for netting, check here and you might find the question.

3.2.10. Network Backup

Network backup determine whether the net is still work via ping one time according to the order of the priority, can be enable from the timing task. Mode option: wired priority, hot mode and cold mode(default is hot mode)

Wired priority: choose the wired priority in APN, testing ping or not, if it ok ,using wired,otherwise choose 4G.

Heat mode: choose hot mode in the SIM card of the APN, and the two 4G connect the module in time, but current only using SIM1, using SIM2 if the SIM1 can not work.

Cold mode: choose the cold mode ,only enable one SIM card, only using SIM1, using SIM2 if the SIM1 can not work.(default the SIM2 disable)

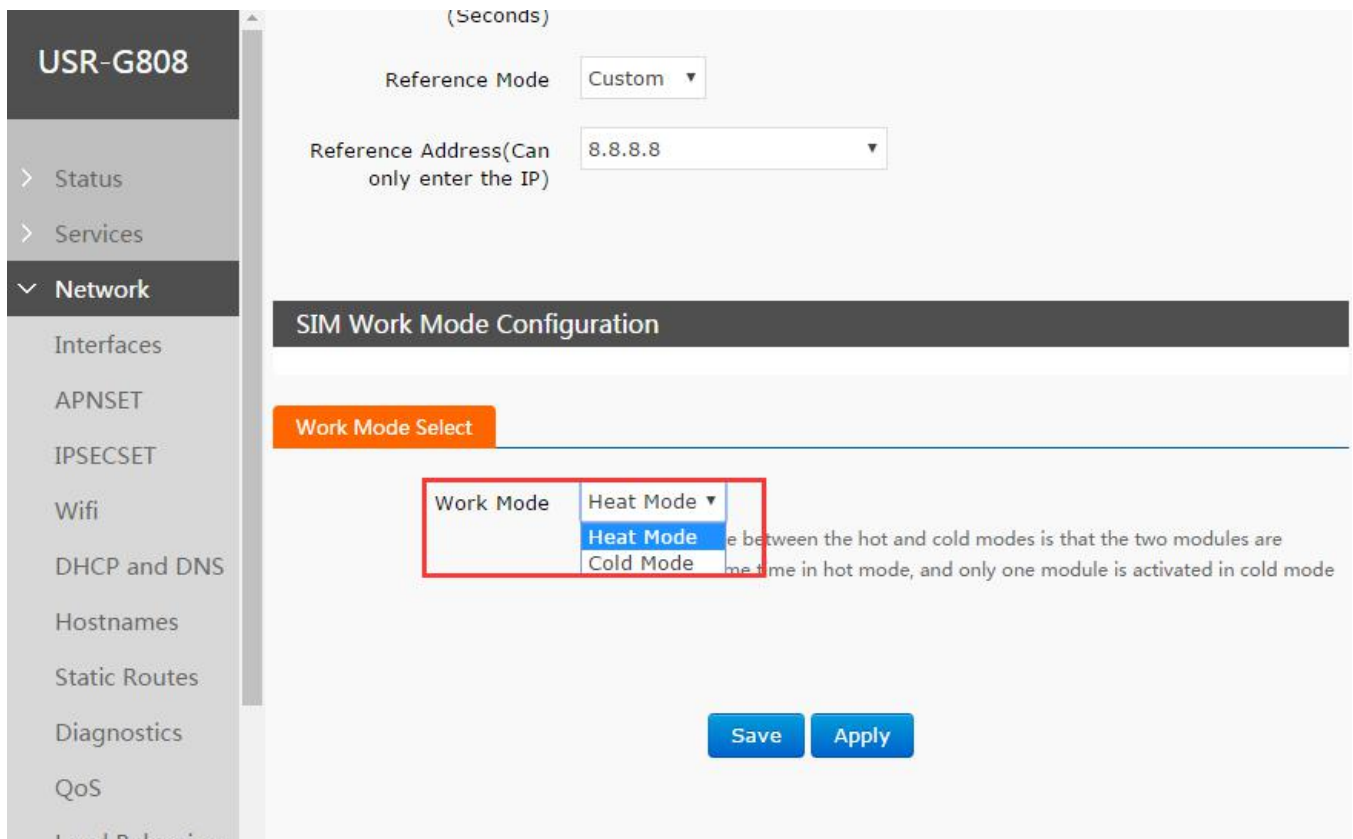


Diagram 3.2.10-1 Dual 4G Working

3.2.11. Load balancing

Load balancing function will configure dual 4G interfaces to realize dual 4G interfaces load balancing. User can configure this function by Web Server as follow:

- ✓ Setting the different gateway hops to the interface, then submit.
For example: set the gateway hop of the 4G1 as 40, 4G2 as 43 (**note:** no setting and no load balancing)
- ✓ Create two interfaces, here is wan_4g1 and wan_4g2, then add. Note:the name of the interface as same as the above.

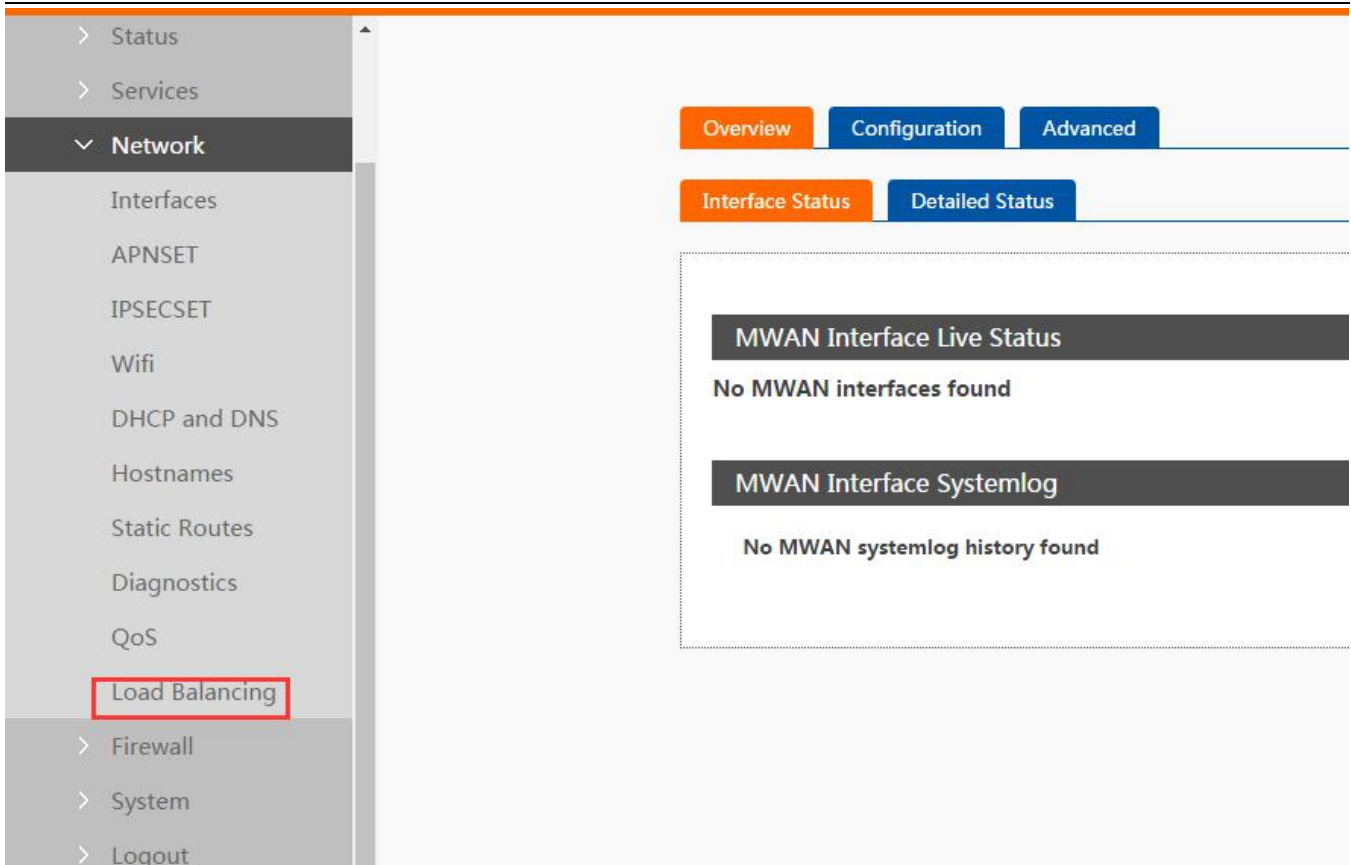


Diagram 3.2.11-2 Load Balancing Configuration

- ✓ Interface configuring
- ✓ Members configuring: setting the different weight for them:4G1:4G2=3:2=60%:40%
- ✓ Policies configuring: member used and standby member
- ✓ Rules configuring: set the remote IP , protocol and policies

Until now, save the 4G1 and 4G2 is ok. Please restart it.

From now, click the interface status in the overview, if the interface green, setting successful, otherwise is red. Also you can see the load weight.

Note:the below is my configuring file, copy it to advanced->MWAN configuring files, then restart G808.

```
config interface 'wan_4g1'
  option enabled '1'
  option count '1'
  option reliability '1'
  list track_ip '114.114.114.114'
  option timeout '3'
  option interval '5'
  option down '3'
  option up '3'
```

```
config interface 'wan_4g2'
  option enabled '1'
  option reliability '1'
  option count '1'
```

```
list track_ip '114.114.114.114'  
option timeout '3'  
option interval '5'  
option down '3'  
option up '3'  
  
config member 'wan_4g1_m_w'  
option interface 'wan_4g1'  
option weight '50'  
option metric '1'  
  
config member 'wan_4g2_m_w'  
option interface 'wan_4g2'  
option weight '40'  
option metric '1'  
  
config policy 'balanced'  
list use_member 'wan_4g1_m_w'  
list use_member 'wan_4g2_m_w'  
  
config rule 'default_rule'  
option dest_ip '0.0.0.0/0'  
option use_policy 'balanced'
```

3.2.12. VPN Client (PPTP、L2TP、IPSEC、OPENVPN、GRE、SSTP)

VPN(Virtual Private Network) has Client and Server two parts and protocols includes PPTP, L2TP, ipsec, openvpn, gre, sstp and so on.

Note: the below VPN default have not configured, choose the related VPN protocol to connect according to the related demand.

3.2.12.1. PPTP Client

PPTP is point-to-point tunnel protocol which uses one TCP connection(port 1723) to maintain tunnel. PPTP protocol will use GRE technology to encapsulate data into PPP data and transmit through tunnel, then encrypt or compress the PPP data.

- The setting way for the PPTP

E.g. a enterprise located in Jinan, and branches in Shenzhen, now it need to build a network to allow the employees in shenzhen to access the head office net. If the PPTP has built(according to the different setting way to the different server, you can refer to the server configuring instr)

Configuring PPTP client:

If PPTP Server has been established, user can configure PPTP Client by Web Server as follows:

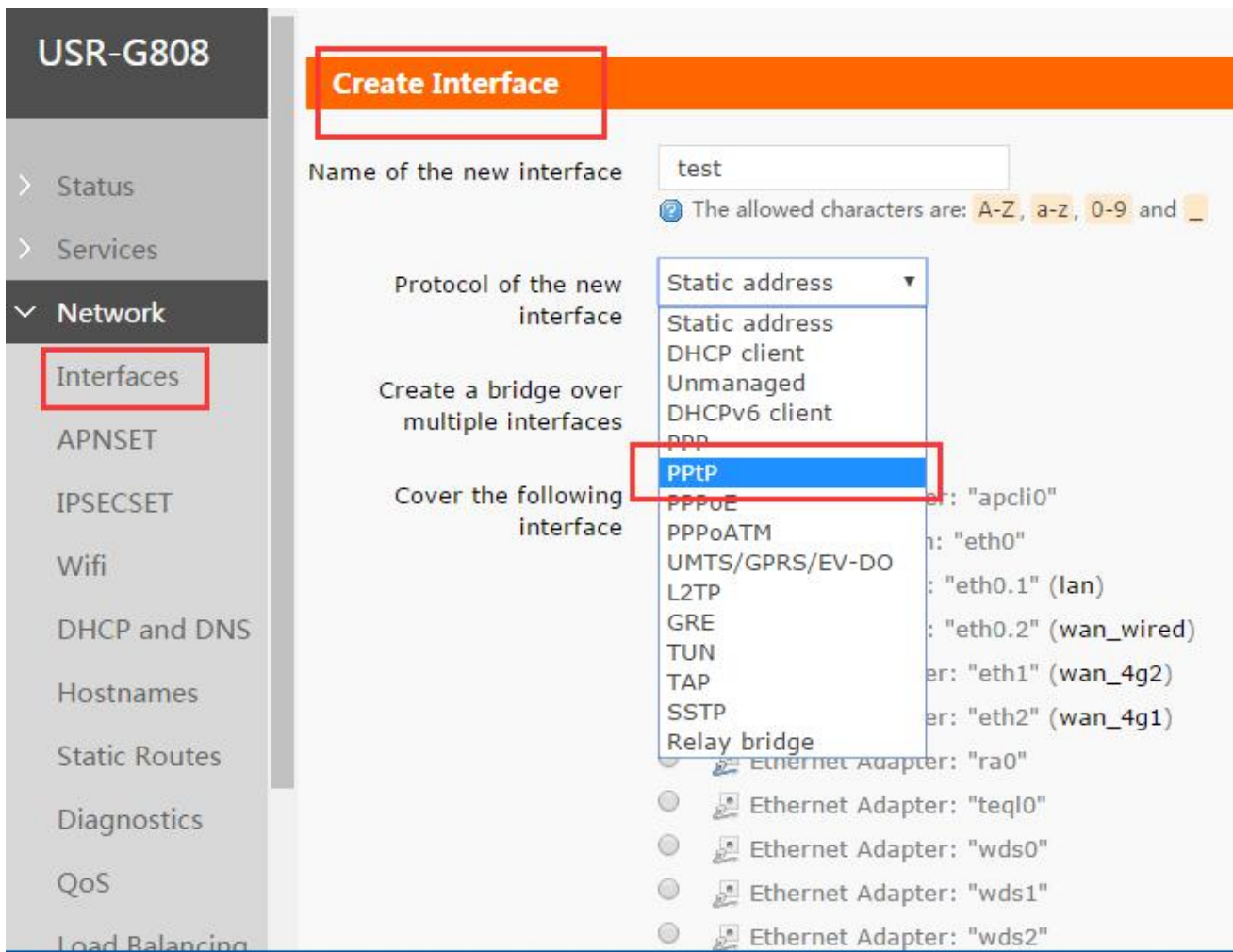


Diagram 3.2.12.1-1 PPTP Client Configuration 1

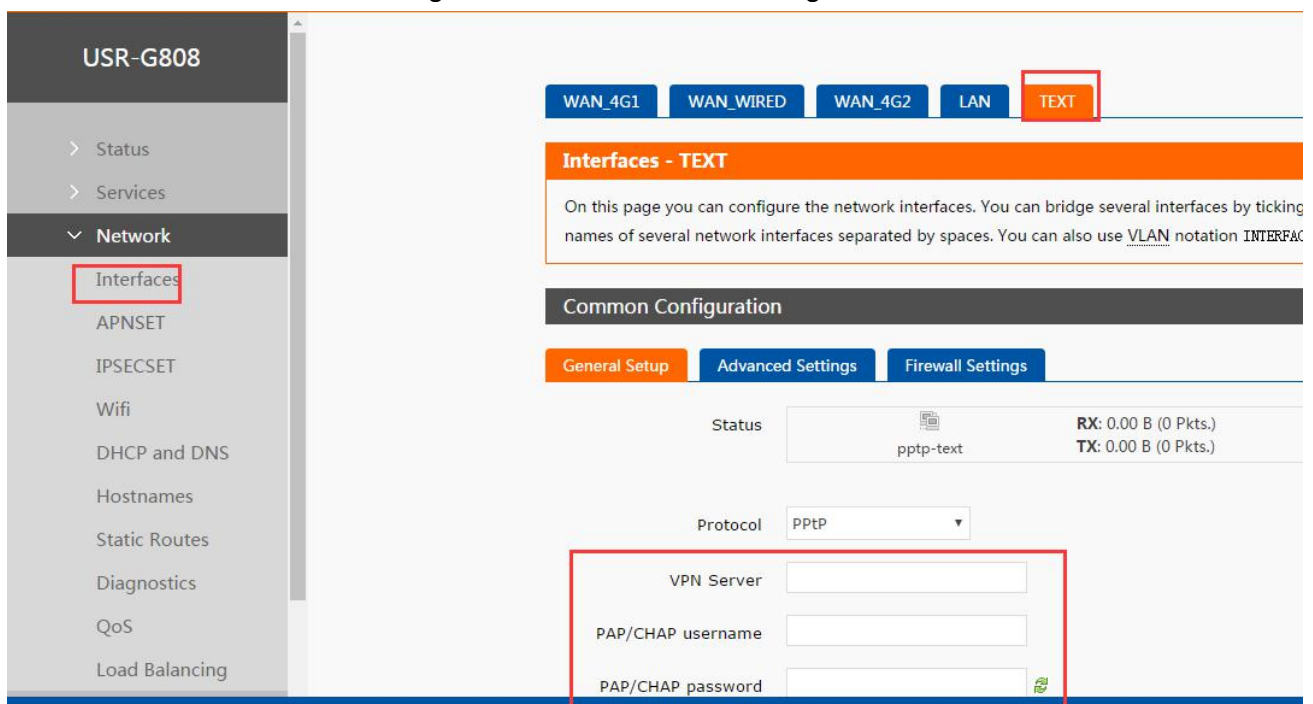
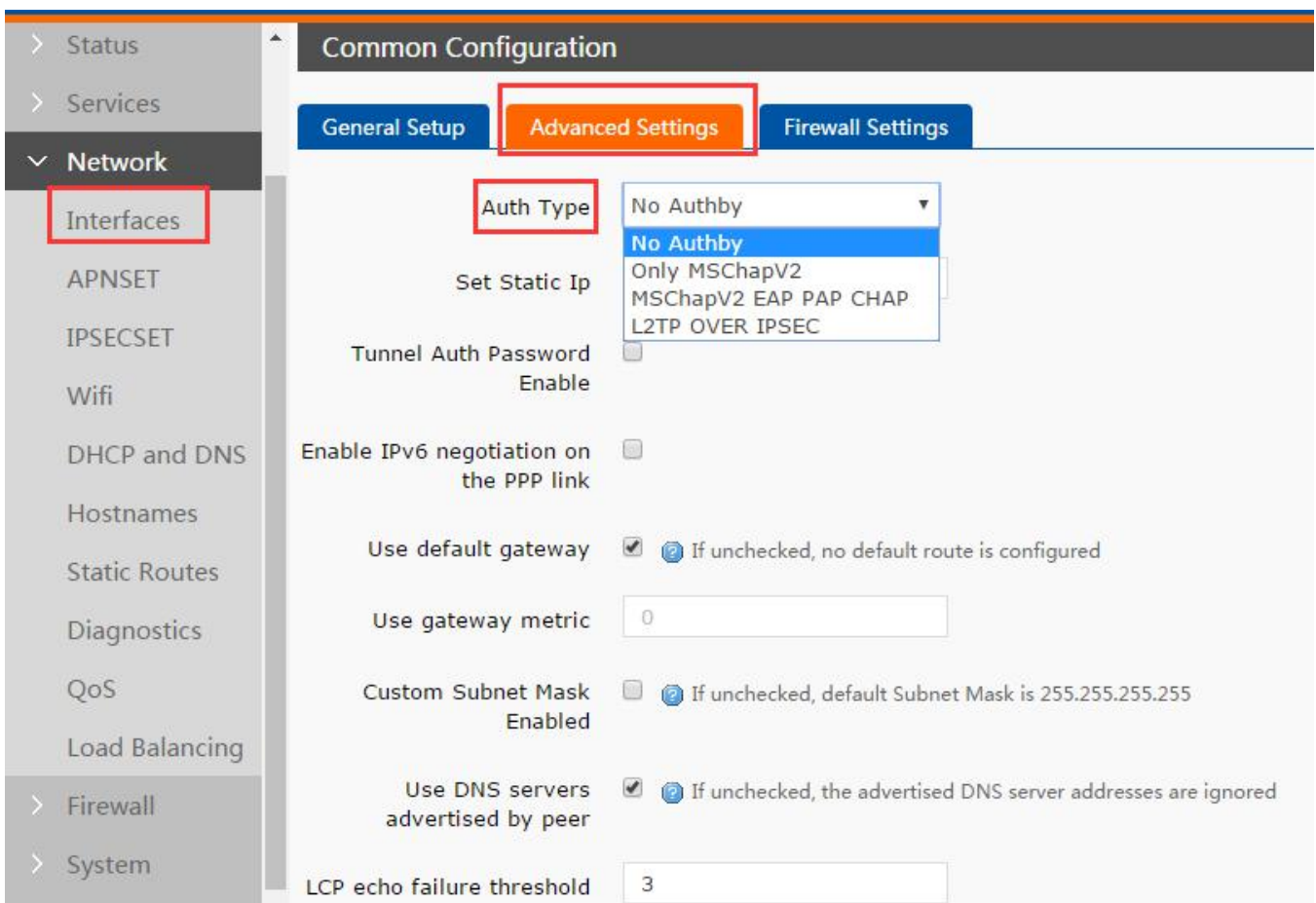


Diagram 3.2.12.1-3 PPTP Client Configuration 1

- ✓ User can choose only MSChapV2 encryption in 'Advanced Settings' according to whether PPTP Server only supports MPPE encryption.
- ✓ And in Firewall Settings, user can choose WAN or LAN according to dialing way.
- ✓ Then there is some running time in the webpage of the VPN interface, means the VPN has work, you can access the VPN network.

3.2.12.2. L2TP Client

L2TP is Layer 2 Tunneling Protocol which is similar to PPTP protocol. G808 supports multiple authentication methods such as tunnel password authentication and CHAP, and supports MPPE and L2TP OVER IPSEC encryption way. User can add a new interface with L2TP protocol by **3.2.12.1 PPTP Client** way and configure by Web Server as follow:



The screenshot displays the 'Common Configuration' page for an L2TP Client. The 'Advanced Settings' tab is active. The 'Auth Type' dropdown menu is open, showing the following options: 'No Authby', 'Only MSChapV2', 'MSChapV2 EAP PAP CHAP', and 'L2TP OVER IPSEC'. Other configuration options include:

- Set Static Ip**: A checkbox that is currently unchecked.
- Tunnel Auth Password Enable**: A checkbox that is currently unchecked.
- Enable IPv6 negotiation on the PPP link**: A checkbox that is currently unchecked.
- Use default gateway**: A checked checkbox with a help icon and the text 'If unchecked, no default route is configured'.
- Use gateway metric**: A text input field containing the value '0'.
- Custom Subnet Mask Enabled**: A checkbox that is currently unchecked, with a help icon and the text 'If unchecked, default Subnet Mask is 255.255.255.255'.
- Use DNS servers advertised by peer**: A checked checkbox with a help icon and the text 'If unchecked, the advertised DNS server addresses are ignored'.
- LCP echo failure threshold**: A text input field containing the value '3'.

Diagram 3.2.12.2-1 L2TP Client configuration 1

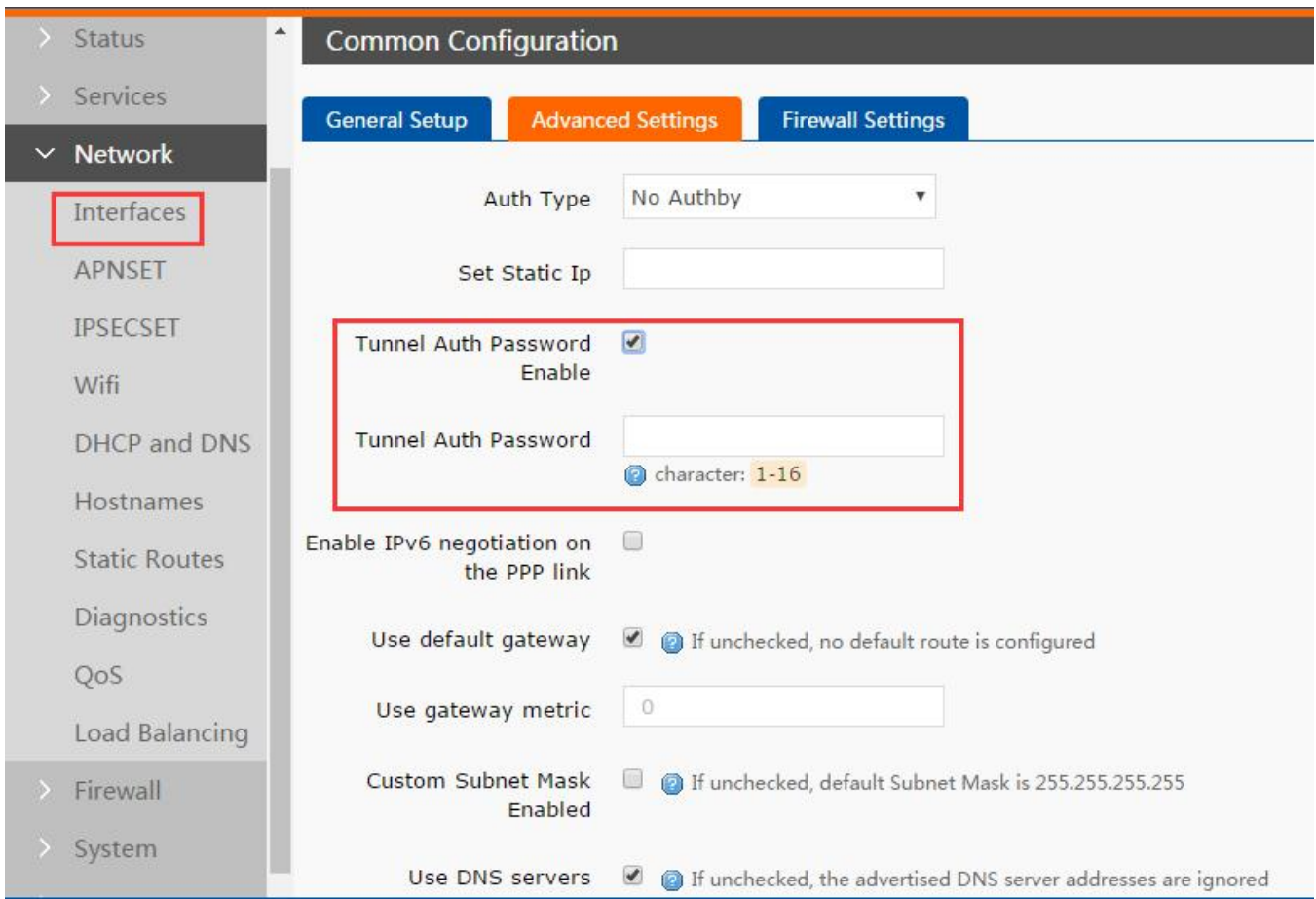


Diagram 3.2.12.2-2 L2TP Client configuration 2

Note:

Subnet and LCP setting way can setting according to the notice
When you choose the L2TP OVER IPSEC encryption, the IPSEC configuring can refer the IPSEC.

3.2.12.3. IPSEC

IPSEC protocol isn't a separate protocol. It gives a complete architecture of network data security on the IP layer and application layer which includes Network Authentication Protocol AH, ESP, IKE and some algorithms for network authentication/encryption. AH protocol and ESP protocol are used to provide security service, IKE protocol is used to key exchange.

User can configure IPSEC by Web Server as follow:

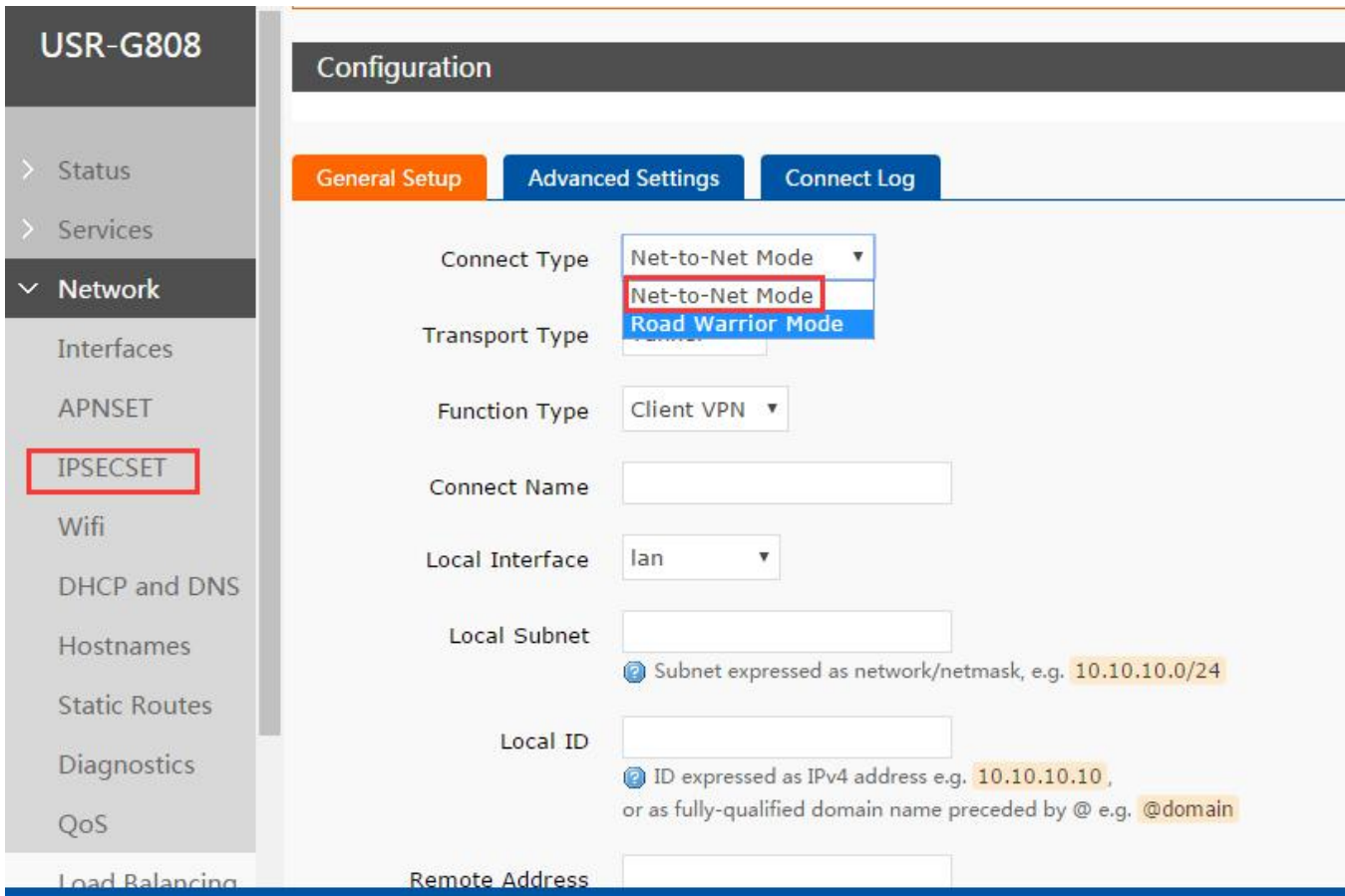
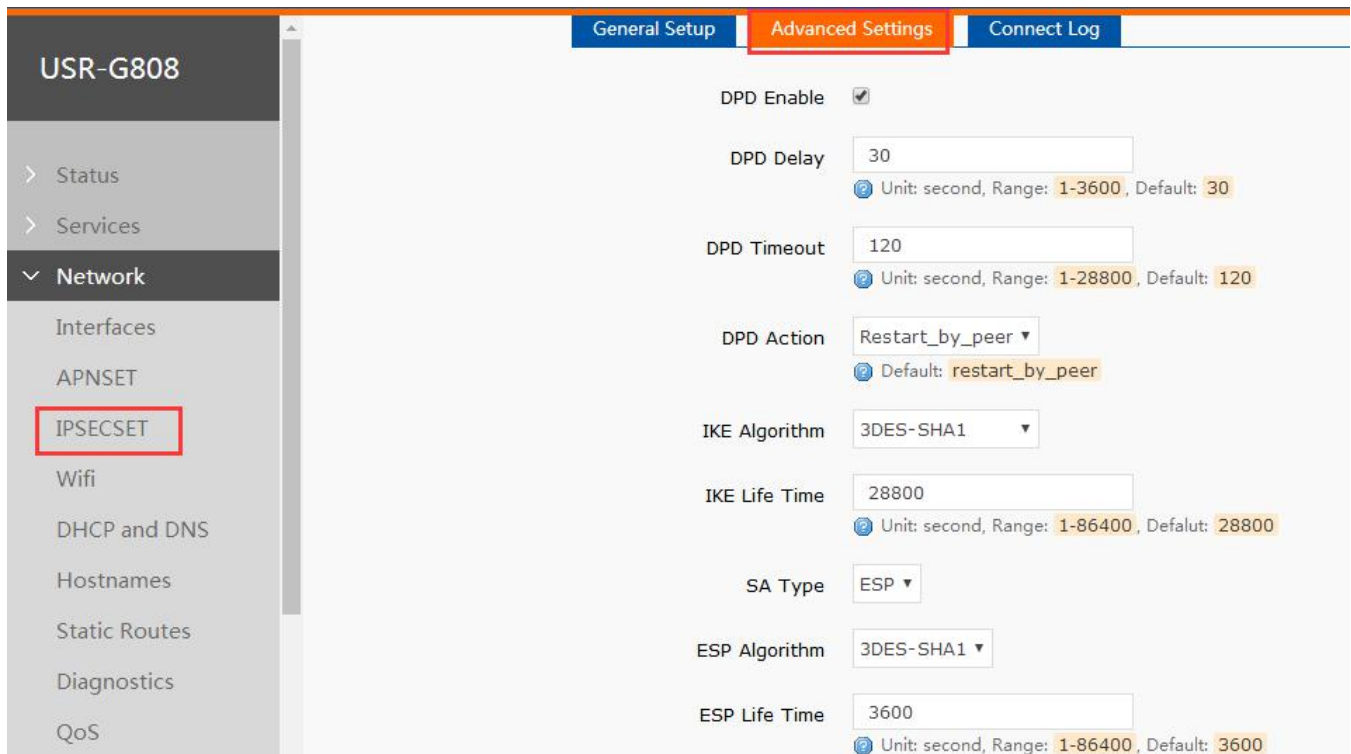


Diagram 3.2.12.3-1 IPSEC Configuration

1. Connect type: net to net mode(station to station or gateway to gateway), road warrior mode (terminal to station or PC to gateway)
2. Transport type: tunnel or transport,can be select
3. Function type: including VPN client and VPN server
4. Connect name: the name of this connection, the unique
5. Local interface: the local address passed, can choose the WAN,4G1,4G2
6. Local subnet: IPSEC local protection subnet and masks name, if choose the client of road warrior, no need to fill.
7. Local ID: tunnel local mark, can be IP or domain name,add @ when customize the domain name.
8. Remote address: the remote IP or address
9. Remote subnet:the terminal subnet and masks
10. Remote mark: tunnel remote mark, can be IP or domain name,add @ when customize the domain name



1. DPD enable: enable this function or not, ✓ means enable
2. DPD delay: setting connection testing interval
3. DPD timeout: setting connection testing timeout.
4. DPD action: setting connection testing operating
5. IKE algorithm: the first step including IKE encryption way, completely solution and DH exchange arithmetic
6. IKE life cycle: setting the IKE life cycle, the unit is second, default is 28800
7. SA type: in the second step can choose the ESP and AH.
8. ESP algorithm: choose the correspond way to encryption and complete solution
9. ESP life time: setting ESP life cycle, unit is S, default is: 3600
10. Mode: negotiation mode default is main mode, can choose the aggr mode
11. Session key forward encryption (PFS): enable PFS if ✓
12. Auth by: current support enjoy the key to certification.

Note:

Configuring successful, mark it in the ISAKMP SA established of the connection log; which is mean you have succeed to build.

3.2.12.4. OPENVPN Client

OPENVPN is based on Openssl library. It supports bidirectional authentication based on certificate, that's to say Client needs to certificate Server and Server needs to certificate Client.

User can add a OPENVPN interface and configure it by Web Server as follow. Protocol can choose TUN(route mode) or TAP(bridge mode).

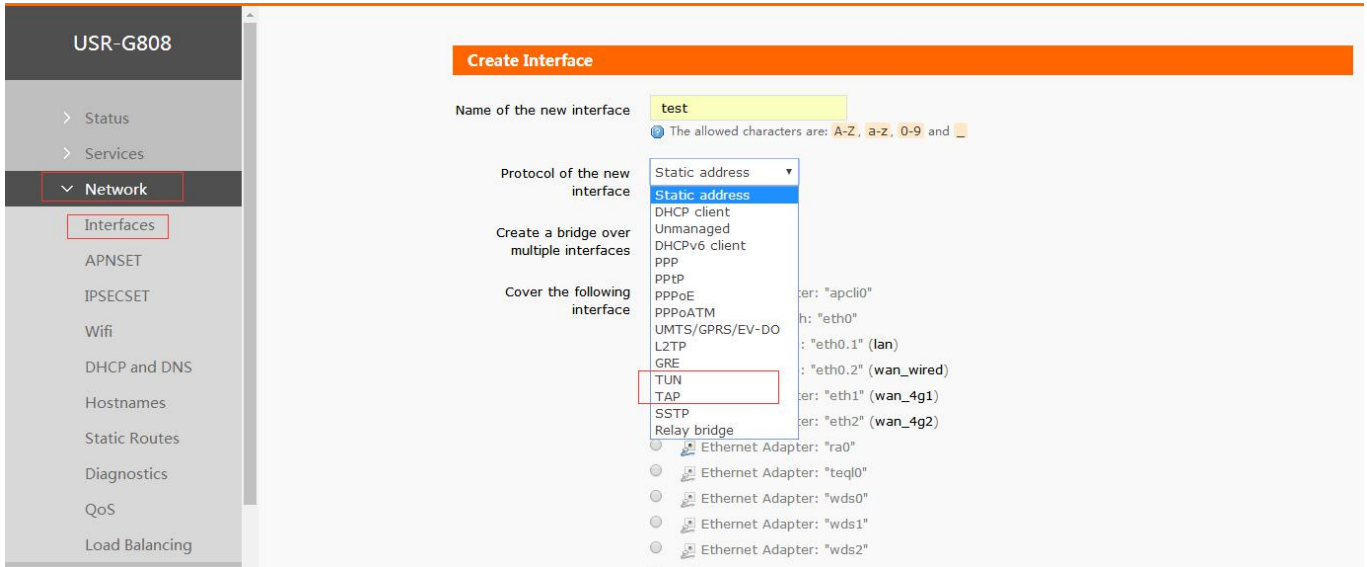


Diagram 3.2.12.4-1 OPENVPN Client configuration

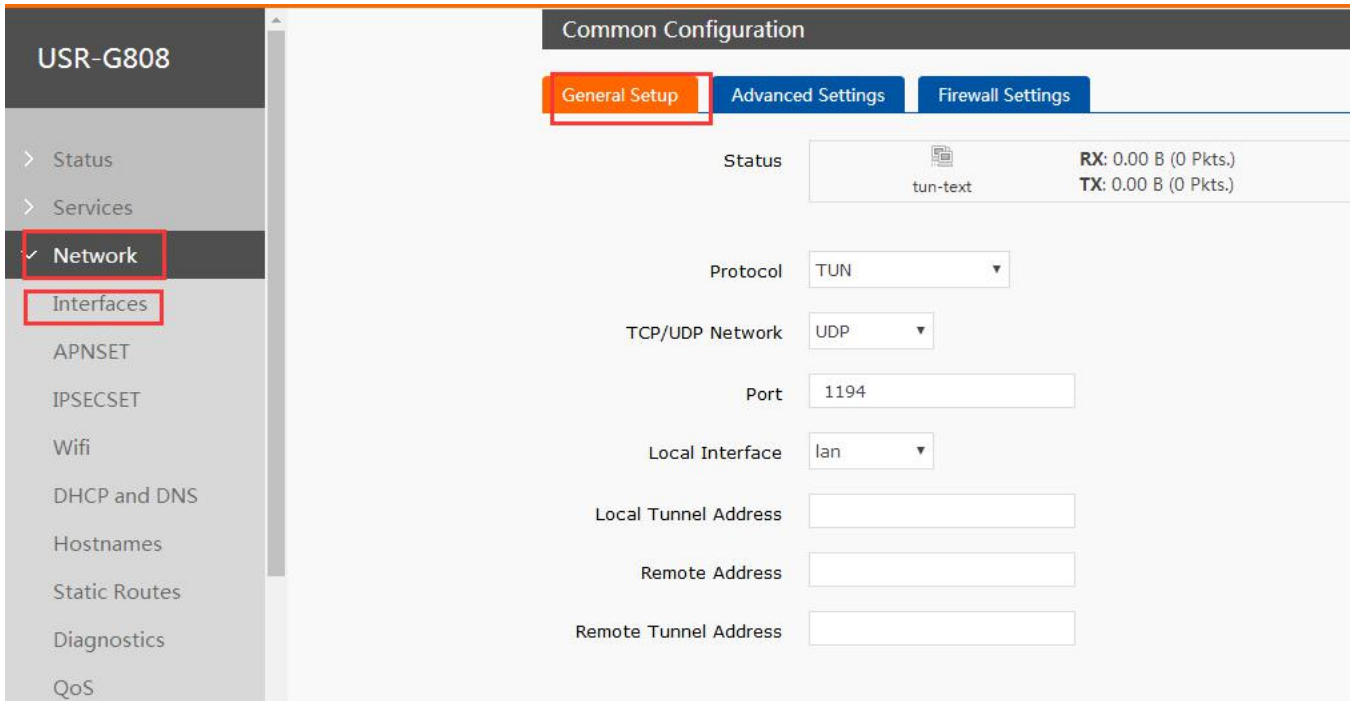


Diagram3.2.12.4-2 General Setup

Basic parameters introduce

1. Protocol: can operating the TUN or TAP
2. Tunnel protocol: UDP/TCP
3. Port: OPENVPN client port listening port
4. Remote interface: WAN ,4G1, 4G2
5. Remote address: server IP or domain name
6. Local tunnel address:can setting the tunnel address of this port, e.g.192.168.10.1,default server distribute if not fill
7. Remote tunnel address:can setting the tunnel address of this port, e.g.192.168.10.1,default server distribute if not fill

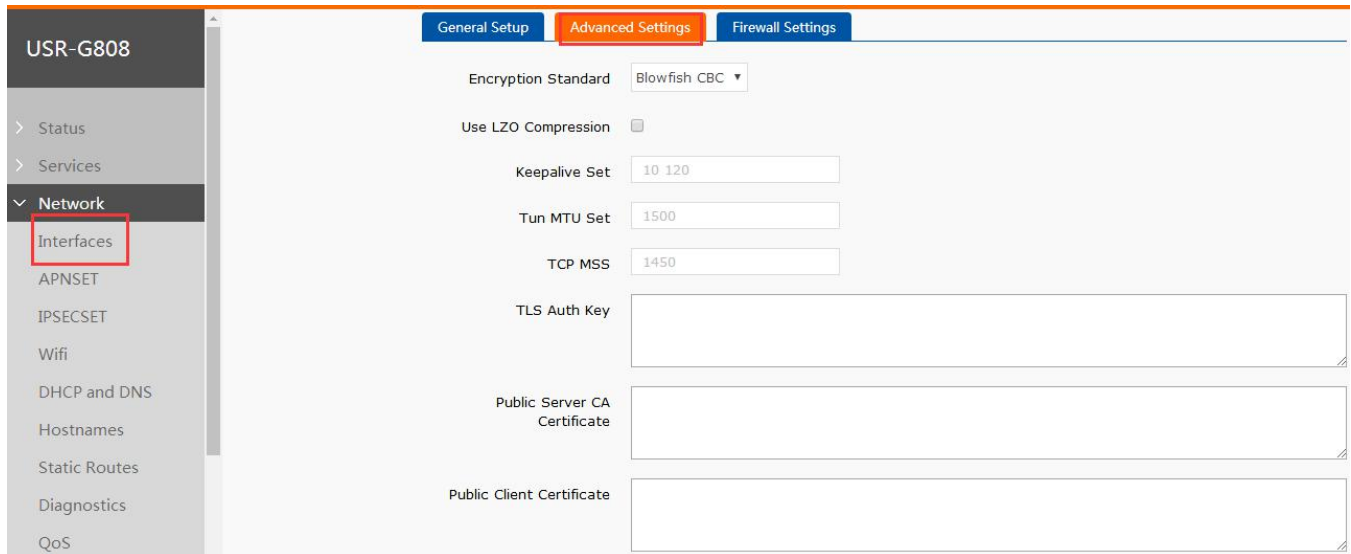


Diagram3.2.12.4-3 OPENVPN Advanced Settings

Advance parameters introduce

1. Encryption standard:tunnel encryption including 5 ways:Blowfish CBC， AES-128 CBC， AES-192 CBC， AES-256 CBC， AES-512 CBC
2. Using LZO compression: enable or disable data transport using LZO compression
3. Keepalive set: default is 10 120
4. TUN MTU set: setting the value of MTU
5. TCP MSS: the maximum of the section of the TCP data.
6. TLS auth key: authority key of the TLS, the certification of safety transmission
7. Public server CA certification: server and client public CA certification
8. Public client certification: client certification
9. Client private key: client private key.

Note:

Before the connection of the client and server, CA certification, client certification, client private, TLS certification key, the server should provide these.

3.2.12.5. GRE

GRE(Generic Routing Encapsulation) protocol is the third layer tunnel protocol of VPN which adopts Tunnel technology. It can encapsulate some network layer protocols data(such as IP, IPX) to transmit on another network layer protocol. User can add a GRE interface and configure by Web Server as follow:

Create interface:

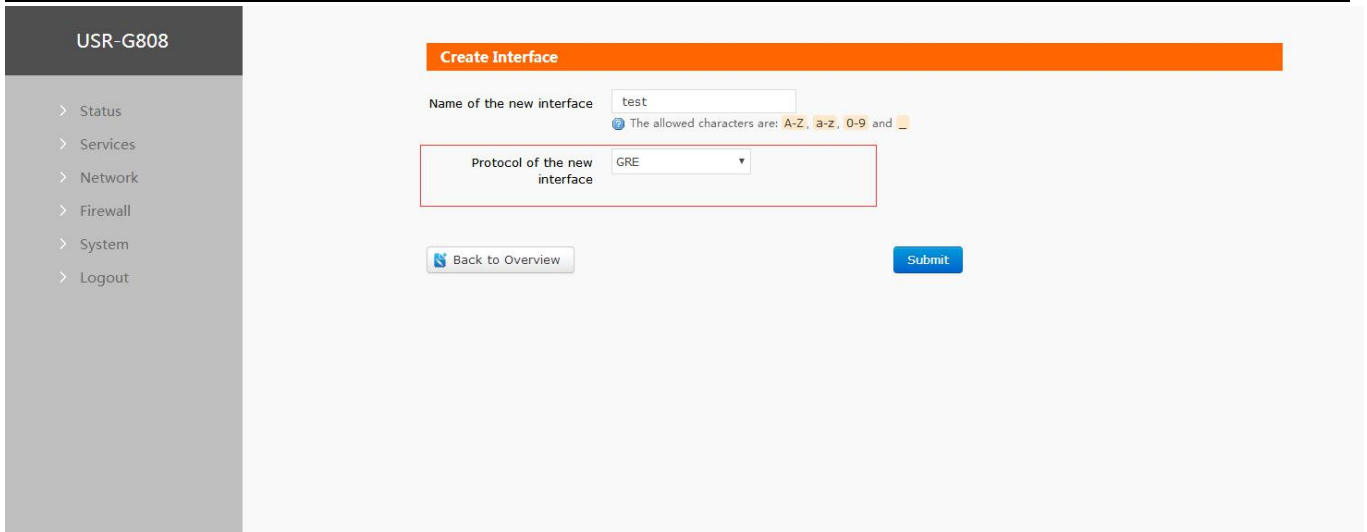


Diagram 3.2.12.5-1 GRE configuration

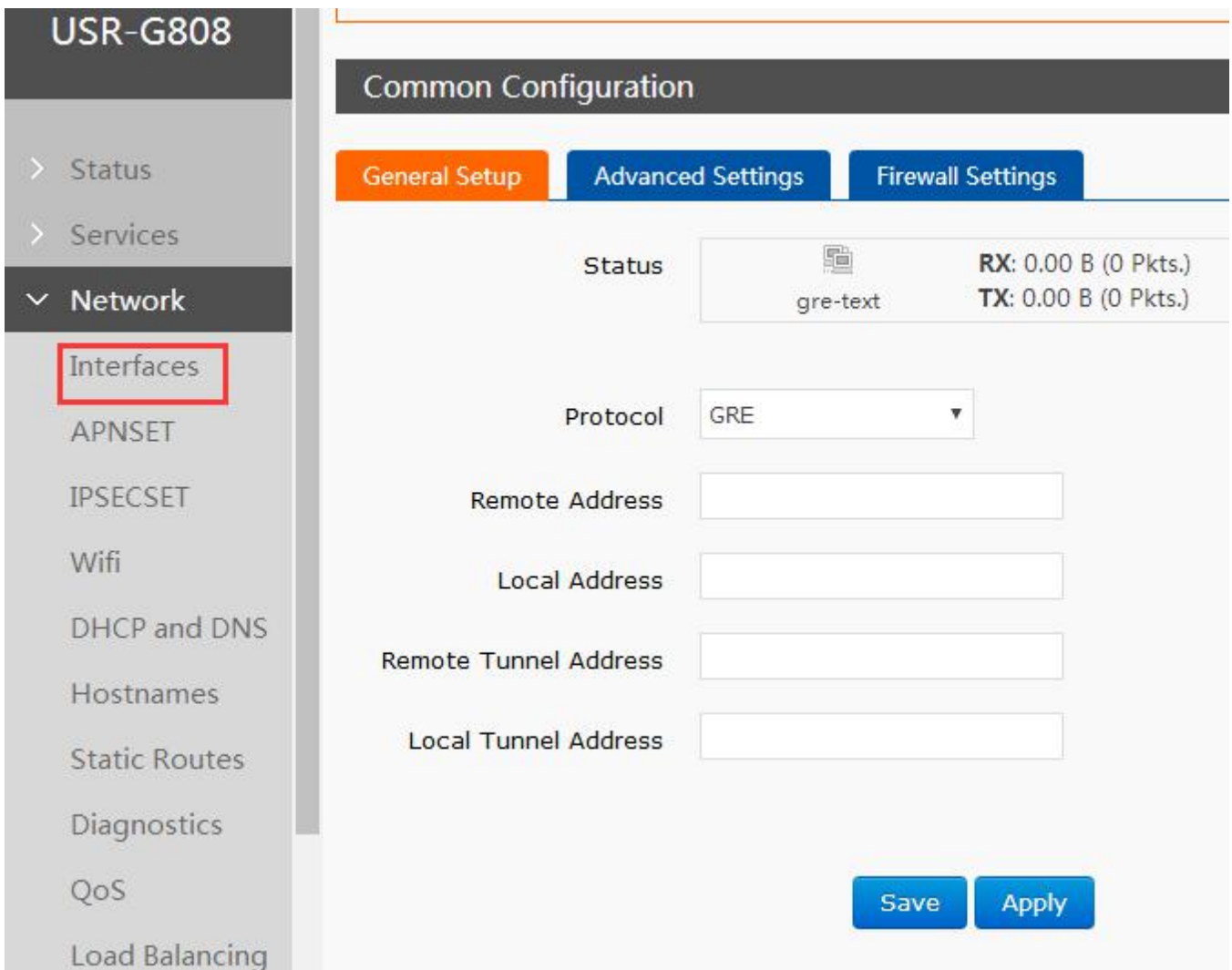


Diagram 3.2.12.5-2 General Setup

Basic parameters introduce

1. Remote address: the WAN port, IP address of the remote GRE
2. Local address: local WAN, 4G1, 4G2, these need to fill in

3. Remote tunnel address: remote GRE tunnel IP
4. Local tunnel IP: local GRE tunnel IP address

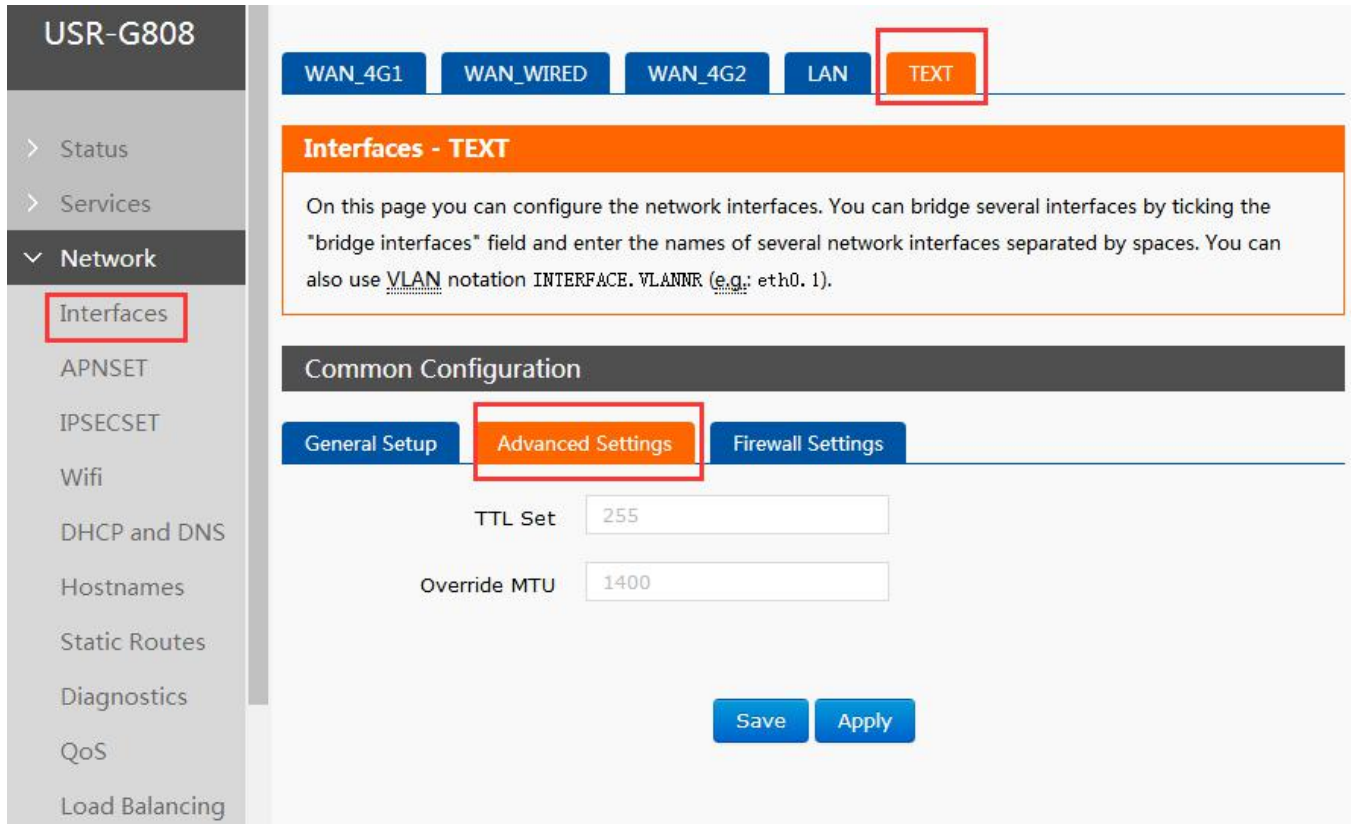


Diagram3.2.12.5-3 GRE Advanced Settings

Advance parameters introduce

1. TTL setting: setting the GRE tunnel TTL, default is 255
2. Setting MTU; setting GRE tunnel MTU, default is 1400

3.2.12.6. SSTP Client

SSTP (secure socket tunnel protocol) is a protocol which is applied for internet. It can create a VPN tunnel which can transmit on HTTPS. SSTP can only be used for remote access and doesn't support site-to-site VPN tunnel.

User can add a SSTP interface and configure by Web Server as follows:

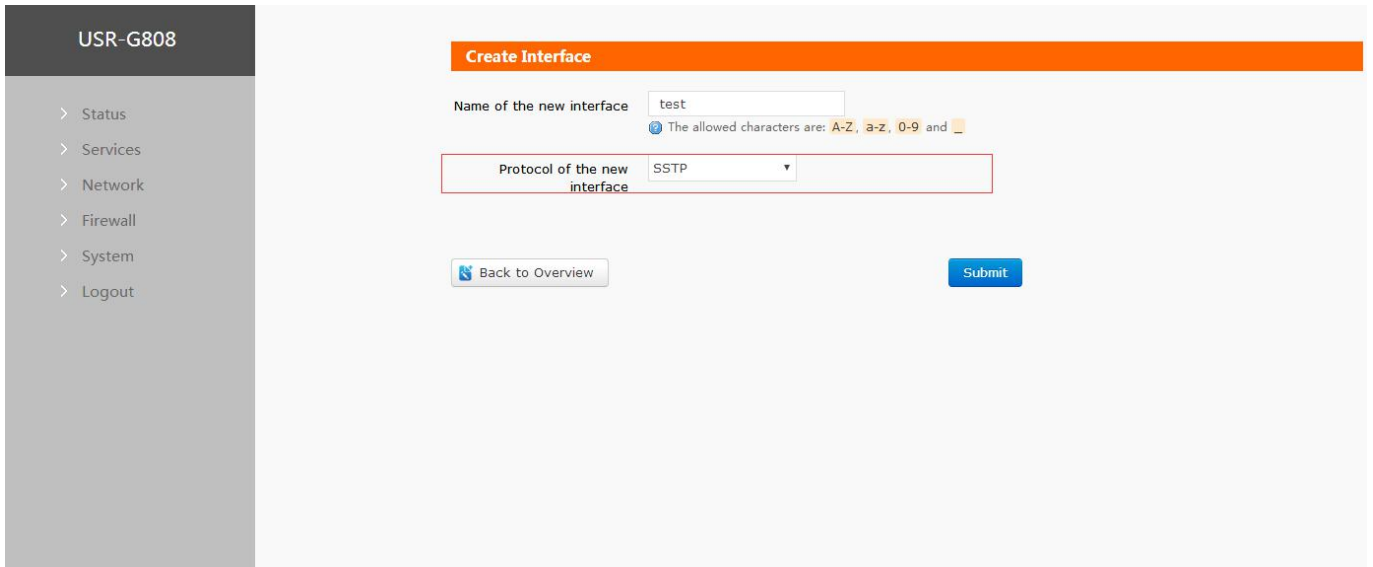


Diagram 3.2.12.6-1 SSTP Client configuration

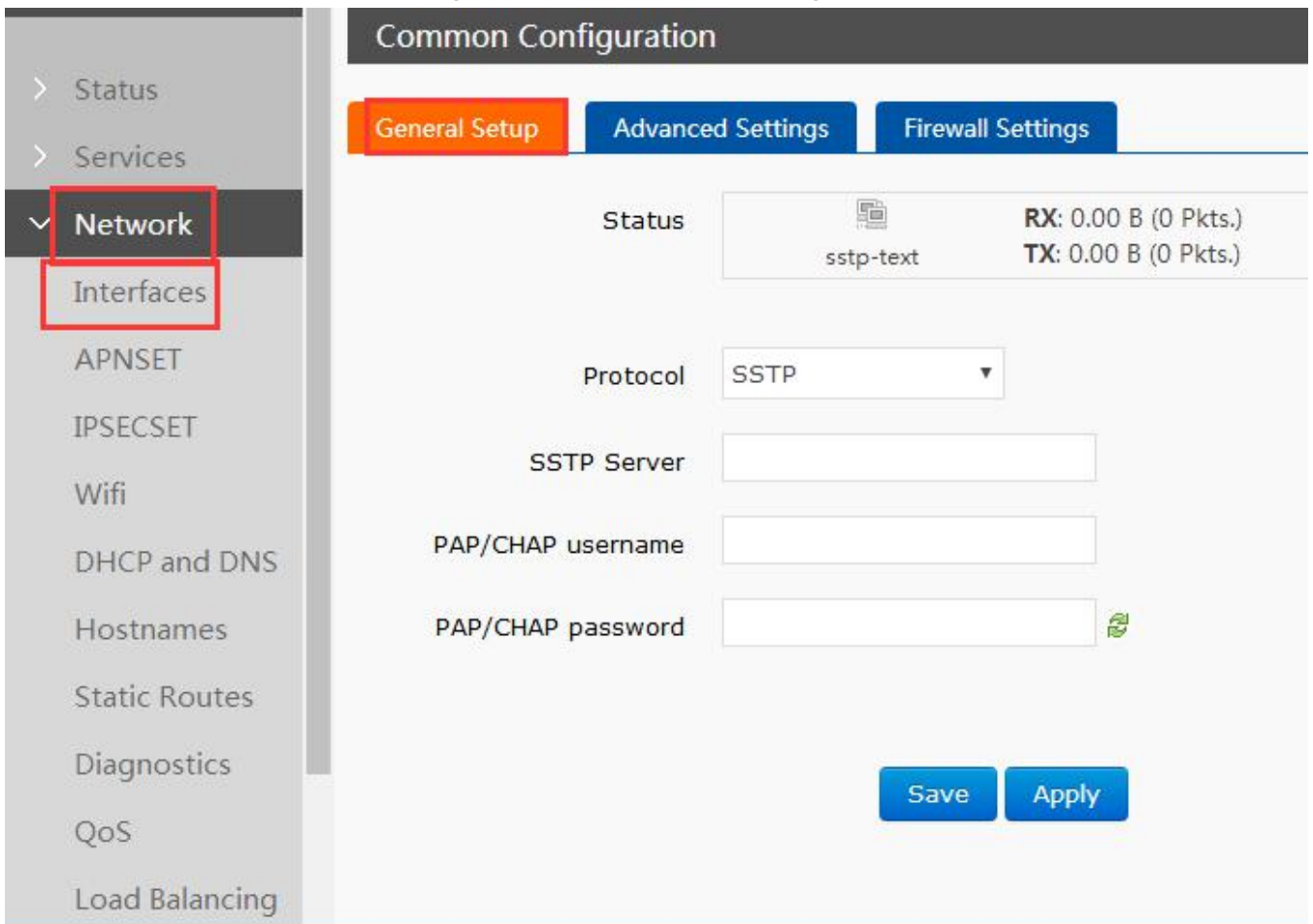


Diagram 3.2.16-2 General Setup

Basic parameters introduce

1. SSTP server: SSTP server IP or domain name
2. PAP/CHAP username: SSTP username
3. PAP/CHAP pass word:SSTP password

Note

Advanced settings please refer to PPTP

3.2.13. Static Routes

Here are some parameters for the static router.

Name	Means	备注
Interface	The port for router rule perform	eth0.2(wired WAN port)
Remote address	The address of the destination you want to access	192.168.1.0
Subnet masks	The subnet masks of the destination to access	255.255.255.0
Gateway	The address to transport	192.168.0.202
Metric	Number of packet jumps	Fill 0
MTU	The max transmission	1500

Form 3.2.13-1 Static Router Parameters

Static router describe the data package router rule on the Ethernet.

■ Static router using the application

Testing environment, two router A and B, like the diagram:

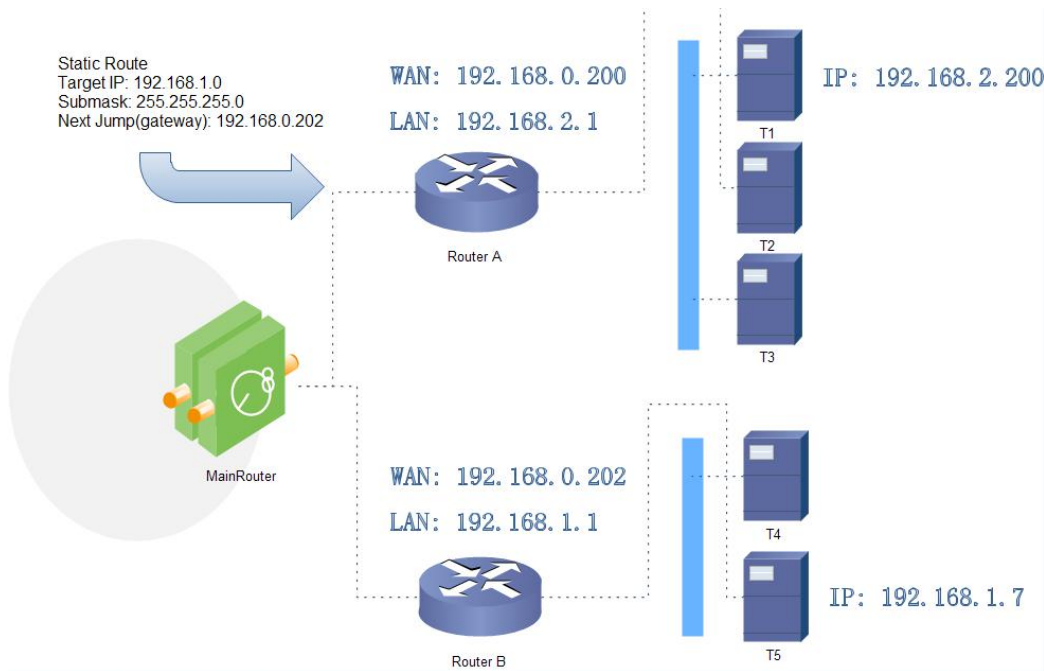


Diagram 3.2.13-1 Static Router List.

Both the WAN of the A and Bin the net of the 192.168.0.0, the LAN port of the router A is subnet:192.168.2.0, and router B is 192.068.1.0.

The create a route on the router A, so when we access the 192.168.1.X, then transfer to router B.

Set the static route on the A

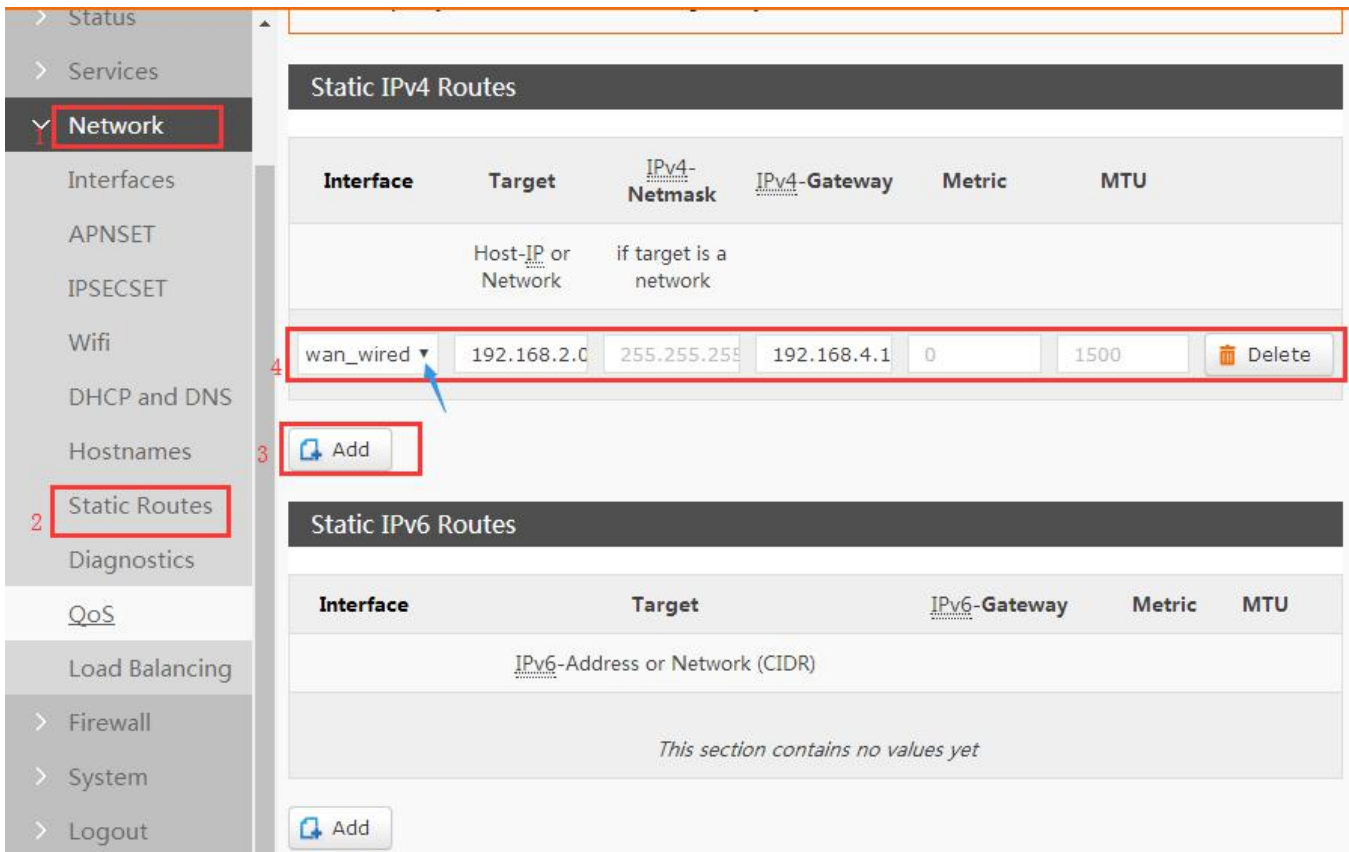


Diagram 3.2.13-1 Static Routes Configuration

On the PC, we ping the 192.168.1.1(the IP of the router B)

```
C:\Users\Administrator>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=4ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=15ms TTL=63
```

Diagram 3.2.13-2 Router Function Testing

Then the static route is work, otherwise we can nit access the LAN of the B from the PC. Then if we also want to access the PC5 under the router B, we should do as below:

Set the firewall of the router B and open the transfer from WAN to LAN. In this way, the data package from the WAN port can also be transfer into the LAN of the router B.

After the firewall setting, you can access to the PC5. The below picture shows it.

```
C:\Users\Administrator>ping 192.168.1.7

正在 Ping 192.168.1.7 具有 32 字节的数据:
来自 192.168.1.7 的回复: 字节=32 时间=6ms TTL=255
来自 192.168.1.7 的回复: 字节=32 时间<1ms TTL=255
```

Diagram 3.2.13-3 Router Function Testing 2

Note: default no static router, before using the function, please according to the detailed requirement.

3.2.14. Firewall

3.2.14.1. Basic Setting

Default two firewall rule.

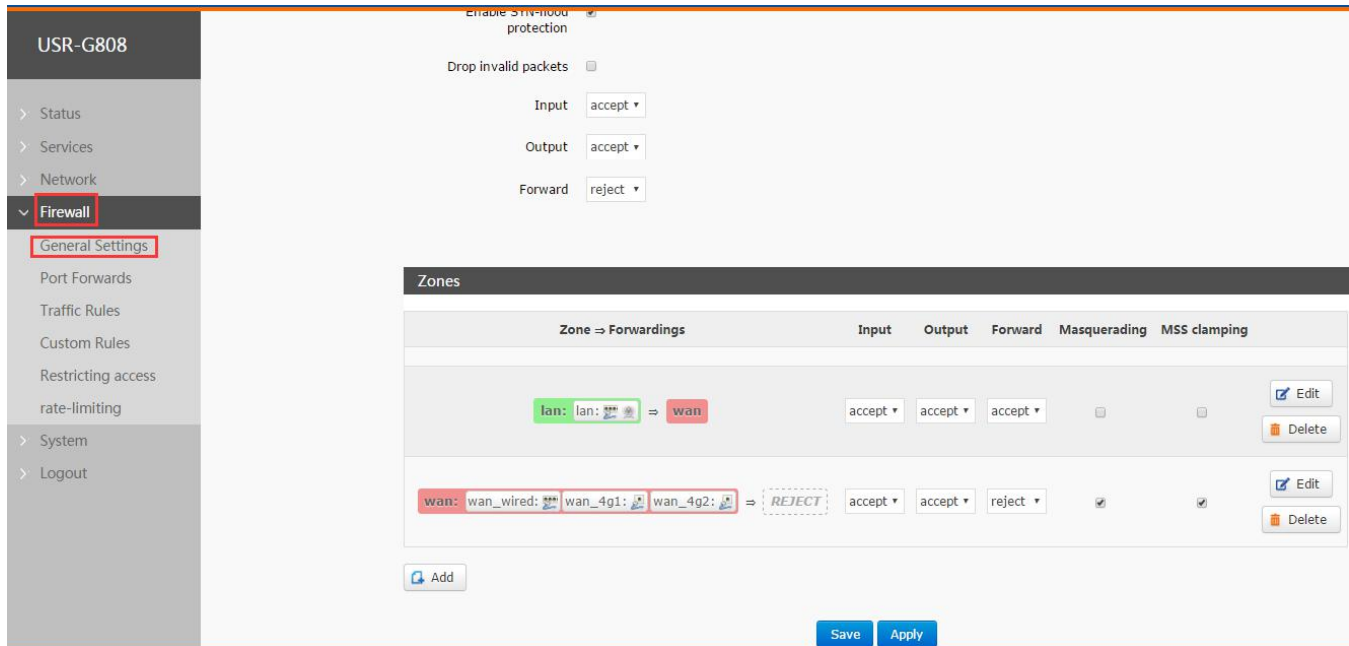


Diagram 3.2.14.1-1 Firewall Setting Webpage

Noun introduce:

- Input: the data package of the router's IP
- Output: the package router will send
- Masquerading: IP masquerading automatically, which is meaningful for the WAN port and 4G port, the masquerading for IP when access the external net.
- MSS clamping: limit the large of the MSS, generally it is 1460.

1. Rule1

The input and forward from LAN to WAN, default is accept.

If the data package will access the WAN from the LAN, so the rule allow data package from the LAN to WAN: this is forward.

Open the webpage of the router when you under the LAN: this is input

The router access the external net, like NTP: this is output

2. Rule2

WAN, 4G1 and 4G2 interface, default receive the input and output, reject the forward

If there is input data package and it will be allowed. Such as someone will login the webpage of the router from the WAN.

Same as the input, the output will be allow if access the external net from he WAN or 4G of the router.

As to the forward data package, forward the data package from the WAN to 4G is not allowed.

For example:

If add a new net interface, just like create a VPN interface, then you should add a rule to access the external.

3.2.14.2. Port Forwards

1. Function

This function can allow PC from internet access PC or service in private LAN. User can configure this function by Web Server as follow:

Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort
<i>This section contains no values yet</i>				

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
test	TCP+UDP	wan	100	lan	192.168.1.1	100	Add

Save **Apply**

Diagram 3.2.14.2-1 Port Forwards Configuration 1

After setting the rule, then click the add on the right, then it will displayed in the rule.

Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort
test	IPv4-TCP, UDP From any host in wan Via any router IP at port 100	IP 192.168.1.172, port 100 in lan	<input checked="" type="checkbox"/>	

New port forward:

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

Save **Apply**

Diagram 3.2.14.2-2 Port Forwards Configuration 2

Then save and apply to make it work.

192.168.1.172 is the PC under the LAN port of the router. After it works, the 100 port of the address that is under

the same segment of the WAN port can build connection with the 200 port under 192.168.1.172 of the WAN port.

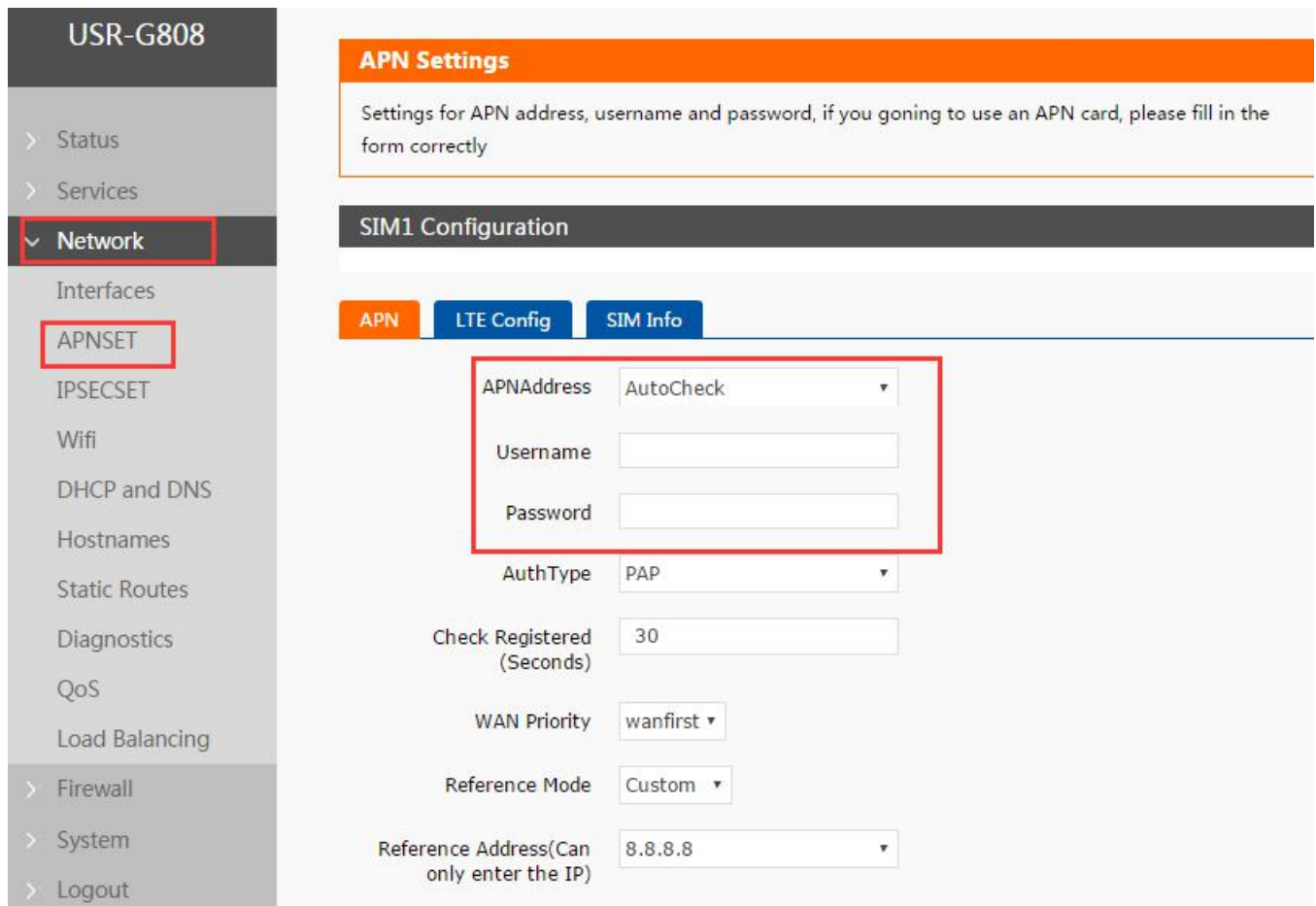
Note: default no port forward.

2. Forward on the 4G interface

Environment	Content	Instr
Router	G808* 1	External net access the device under the 4G router
	SIM card *1	APN (fixed IP: 10.201.20.47)
PC	IP of the PC in LAN	192.168.1.247
	Listening port	12129

Form 3.2.14.2-1 Related Parameters

Firstly, fill the APN address on the router:



The screenshot shows the USR-G808 web interface. On the left is a navigation menu with 'Network' selected and 'APNSET' highlighted. The main content area is titled 'APN Settings' and contains the following configuration fields:

- APN Settings:** Settings for APN address, username and password, if you going to use an APN card, please fill in the form correctly.
- SIM1 Configuration:**
 - APN:**
 - APNAddress: AutoCheck
 - Username: [text input]
 - Password: [text input]
 - AuthType: PAP
 - Check Registered (Seconds): 30
 - WAN Priority: wanfirst
 - Reference Mode: Custom
 - Reference Address(Can only enter the IP): 8.8.8.8

Diagram 3.2.14.2-3 4G net Port Forward

Then, add the related port forward

Diagram 3.2.14.2-4 4G net Port Forward

At last, restart the router .
Then, check the router.

3.2.14.3. Traffic rules

Traffic rules can filter the special internet data format selectively and prevent the internet from access. Strengthen the safety via this rules. The firewall is wide application range. Here introduced some common application.

1. IP address black list

Enter the name in the new forward rule then add and edit

Diagram 3.2.14.3-1 Firewall Black List 1

In the webpage turn out, source zone:LAN, source MAC address and source address:any(if you only limited the pointed IP access the point IP, please fill the IP address and MAC address.

The screenshot shows the configuration page for a firewall rule on a USR-G808 device. The left sidebar contains a navigation menu with 'Traffic Rules' highlighted. The main configuration area shows the following settings:

- Rule is enabled: Disable
- Name: ip-reject
- Restrict to address family: IPv4 and IPv6
- Protocol: TCP+UDP
- Match ICMP type: any
- Source zone: lan (selected), Any zone, wan: wan_wired, wan_4g1, wan_4g2
- Source MAC address: any
- Source address: any
- Source port: any
- Destination zone: Device (input), Any zone (forward), lan (selected)

Diagram 3.2.14.3-2 Firewall Black List 2

Select the WAN in the zone, remote address fill the IP forbidden to access. Select the reject, save and application, then save and apply

USR-G808

- > Status
- > Services
- > Network
- Firewall**
- General Settings
- Port Forwards
- Traffic Rules**
- Custom Rules
- Restricting access
- rate-limiting
- > System
- > Logout

Source MAC address: any

Source address: any

Source port: any

Destination zone:

- Device (input)
- Any zone (forward)
- lan: lan: [icon]
- wan: wan_wired: [icon] wan_4g1: [icon] wan_4g2: [icon]**

Destination address: 192.168.1.172 (00:25:AB)

Destination port: any

Action: reject

Extra arguments: []
Passes additional arguments to iptables. Use with care!

Back to Overview Save Apply

Diagram 3.2.14.3-3 Firewall Black List 3

IPv6-ICMP with types *echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type* Accept forward and limit to 1000 pkts. per second

Allow-ICMPv6-Forward From any host in wan To any host in any zone

ip-reject Any traffic From any host in lan To IP 192.168.1.172 in wan Refuse forward

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	[]

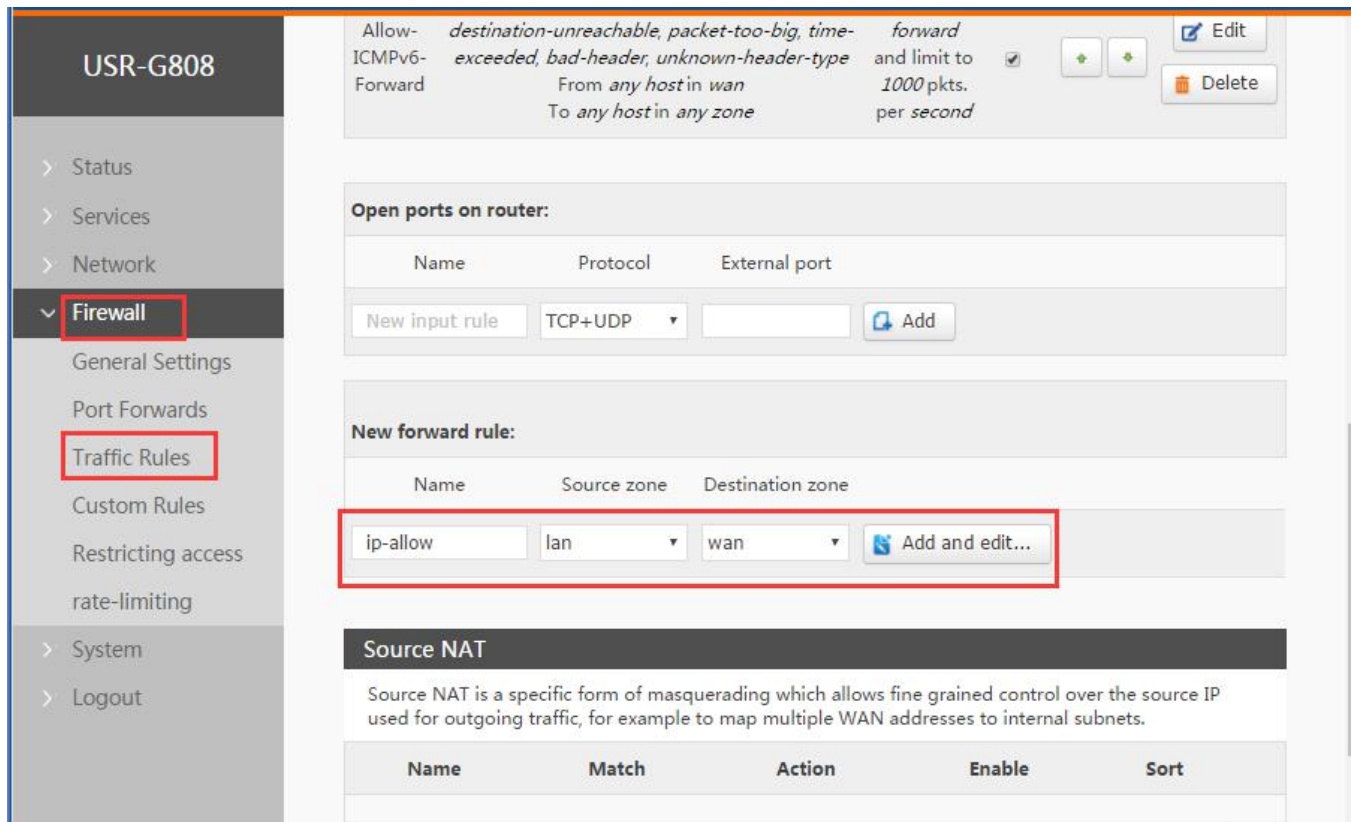
Add

New forward rule:

Diagram 3.2.14.3-4 Firewall Black List 4

2. IP address white list

Firstly, add the IP or the MAC address traffic rule of the white list, enter the name of the rule, then click add and edit.



The screenshot shows the USR-G808 Firewall configuration page. The left sidebar has 'Firewall' and 'Traffic Rules' highlighted. The main content area shows a list of rules at the top, followed by 'Open ports on router' and 'New forward rule' sections. In the 'New forward rule' section, a rule named 'ip-allow' is being added with 'lan' as the source zone and 'wan' as the destination zone. The 'Add and edit...' button is highlighted with a red box.

Diagram 3.2.14.3-4 Firewall White List 1

Select "lan" in the source zone and source address and source MAC address select "any" (if you want to allow point IP access the pointed external net, please fill the IP or the MAC address) as below:

USR-G808

- > Status
- > Services
- > Network
- > **Firewall**
 - General Settings
 - Port Forwards
 - Traffic Rules
 - Custom Rules
 - Restricting access
 - rate-limiting
- > System
- > Logout

Firewall - Traffic Rules - ip-allow

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled Disable

Name

Restrict to address family

Protocol

Match ICMP type

Source zone

Any zone

lan: lan:

wan: wan_wired: wan_4g1: wan_4g2:

Source MAC address

Source address

Source port

Diagram 3.2.14.3-5 Firewall White List 2

Destination zone please choose “wan” and fill the IP which is allowed to access, action access accept, then save and apply.

USR-G808

- > Status
- > Services
- > Network
- > **Firewall**
- General Settings
- Port Forwards
- Traffic Rules**
- Custom Rules
- Restricting access
- rate-limiting
- > System
- > Logout

Source MAC address

Source address

Source port

Destination zone

Device (input)

Any zone (forward)

lan:

wan:

Destination address

Destination port

Action

Extra arguments

Passes additional arguments to iptables. Use with care!

Diagram 3.2.14.3-6 Firewall White List 3

USR-G808

- > Status
- > Services
- > Network
- > **Firewall**
- General Settings
- Port Forwards
- Traffic Rules**
- Custom Rules
- Restricting access
- rate-limiting
- > System
- > Logout

Allow-ICMPv6-Forward	destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type	From any host in wan To any host in any zone	forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
ip-allow	Any traffic	From any host in lan To IP 192.168.1.172 in wan	Accept forward	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Open ports on router:

Name	Protocol	External port	
<input type="text" value="New input rule"/>	<input type="text" value="TCP+UDP"/>	<input type="text"/>	<input type="button" value="Add"/>

New forward rule:

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="button" value="Add and edit..."/>

Diagram 3.2.14.3-7 Firewall White List 4

3.2.14.4. Custom Rules

Custom rules can realize the above function. Enter the command to operating. Currently supports Iptables command. If you need, please refer to linux Iptable related command.

Currently, there is no defined rule

3.2.14.5. Restricting access

This function can set specified domain name into black list or white list.

When the black list was select, the devices connected to the router can not access the domain name in the black list, but they can access others.

When the white list was select, the device connected to the router can only access to the domain name in the white list.

Both black list and white list can set more than one.

Note: the default is disable,configuring according to the detailed requirement.

1. Domain name black list

At first, choose the black list in the ways to restrain, add the name and correct domain name then click to save, the rule will work immediately and the devices under the router will not access it. If you add black list but fill no name in it, it is meaning the device can access all the domain name

2. Domain name white list

At first, choose the white list in the ways to restrain, add the name and correct domain name then click to save, the rule will work immediately, and the device can only access the domain name in the list. If adding black list but fill no name in it, it is meaning the device can not access any.

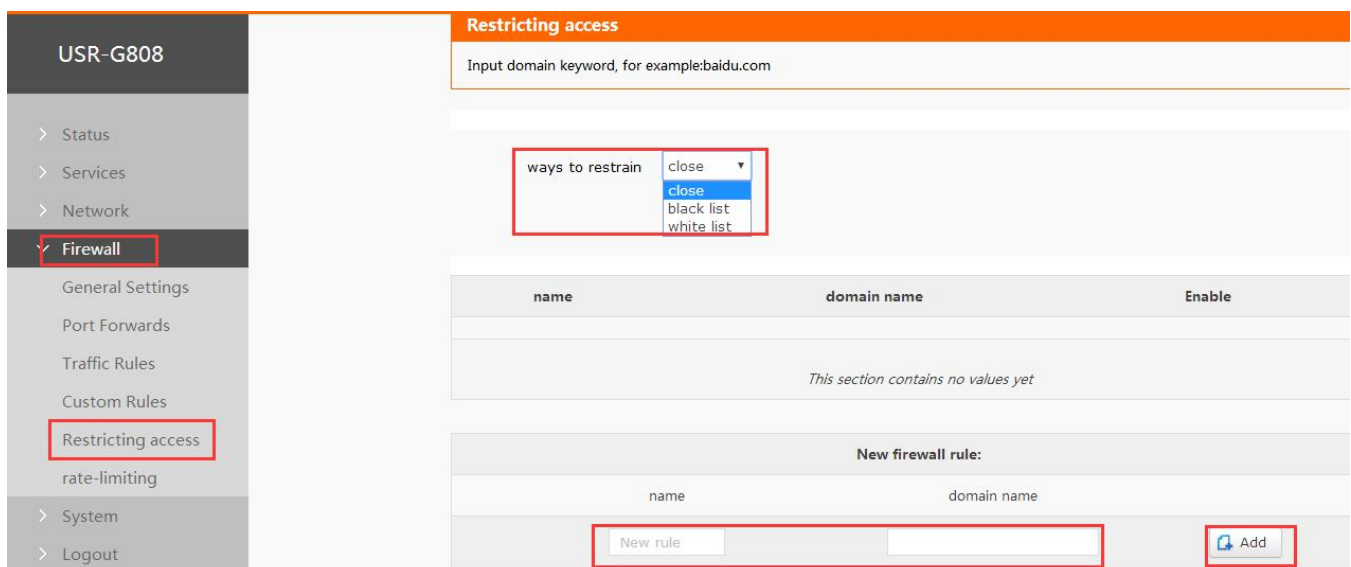


Diagram 3.2.14.5-1 Restricting access configuration

3.2.14.6. Rate-limiting

This function can do network speed control for specified IP and MAC. User can configure this function by Web Server as follow:

Note: default no control

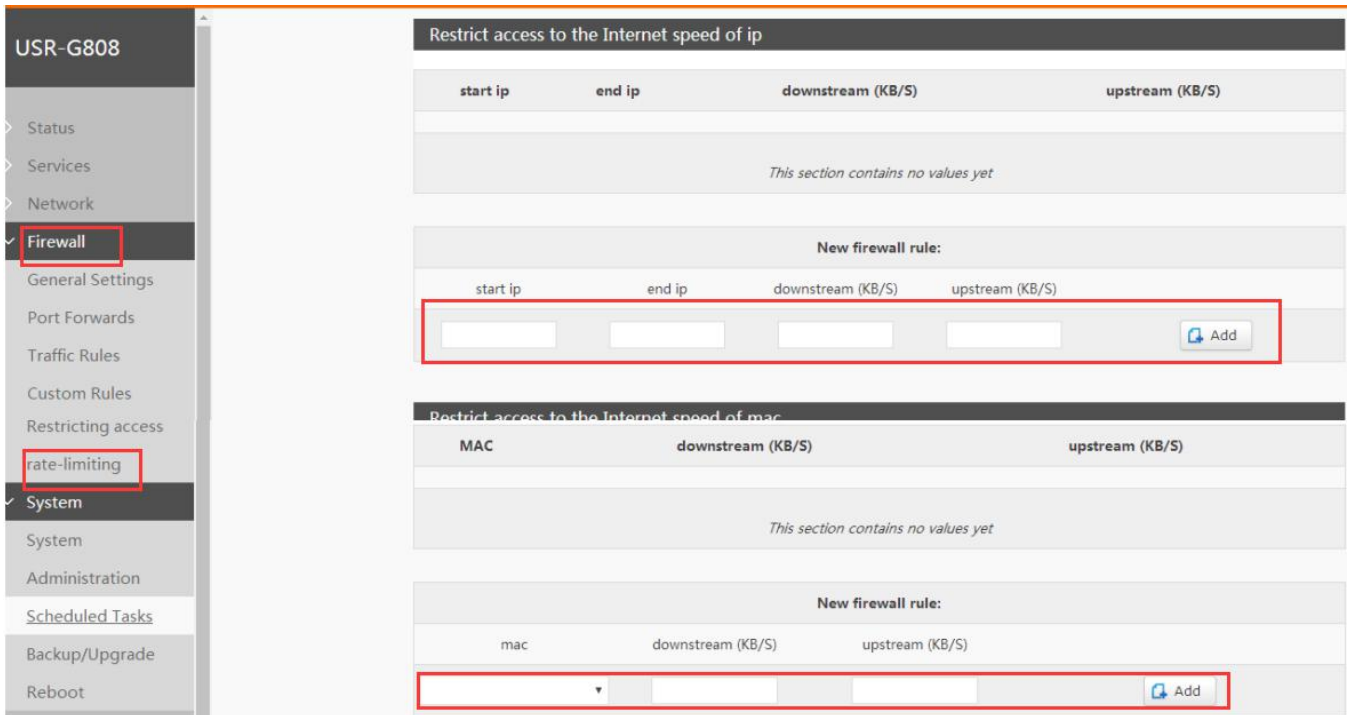


Diagram 3.2.14.6-1 Rate-limiting configuration

Function	Parameters setting (if used)	Note
Start IP	Segment limited start IP	IPV4
Stop IP	Segment limited stop IP	IPV4
Up speed rate	Limited the max up speed rate	Unit: byte/s
Down speed rate	Limited the max down speed rate	Unit:byte/s
MAC	MAC limited	Mac address of the device

Form 3.2.14.6-1 Net Control Parameters

3.3. Basic Function

3.3.1. Network Diagnosis

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

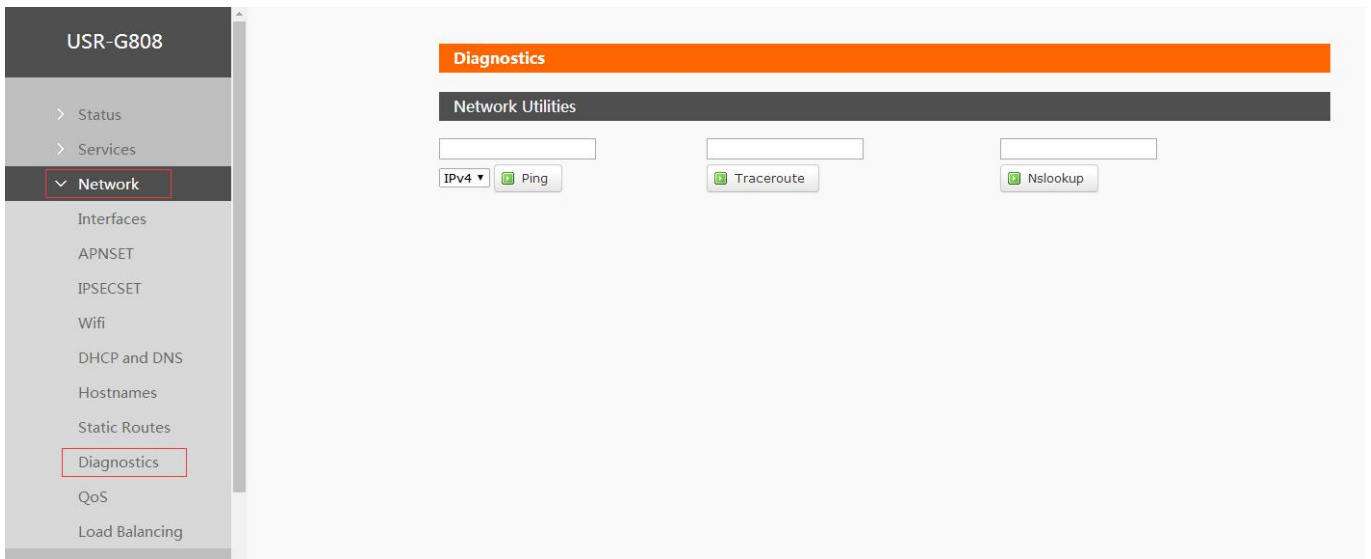


Diagram 3.3.1-1 Network diagnosis configuration

- ✓ Ping: User can do PING test to a specific address in G808.
- ✓ Traceroute: Can acquire routing path to visit a specific address.
- ✓ Nslookup: Can analyse DNS into IP address

3.3.2. Host Name and Time Zone

G808 default host name is USR-G808 and default Time Zone is Beijing time zone.

User can configure host name and Time Zone by Web Server as follow:

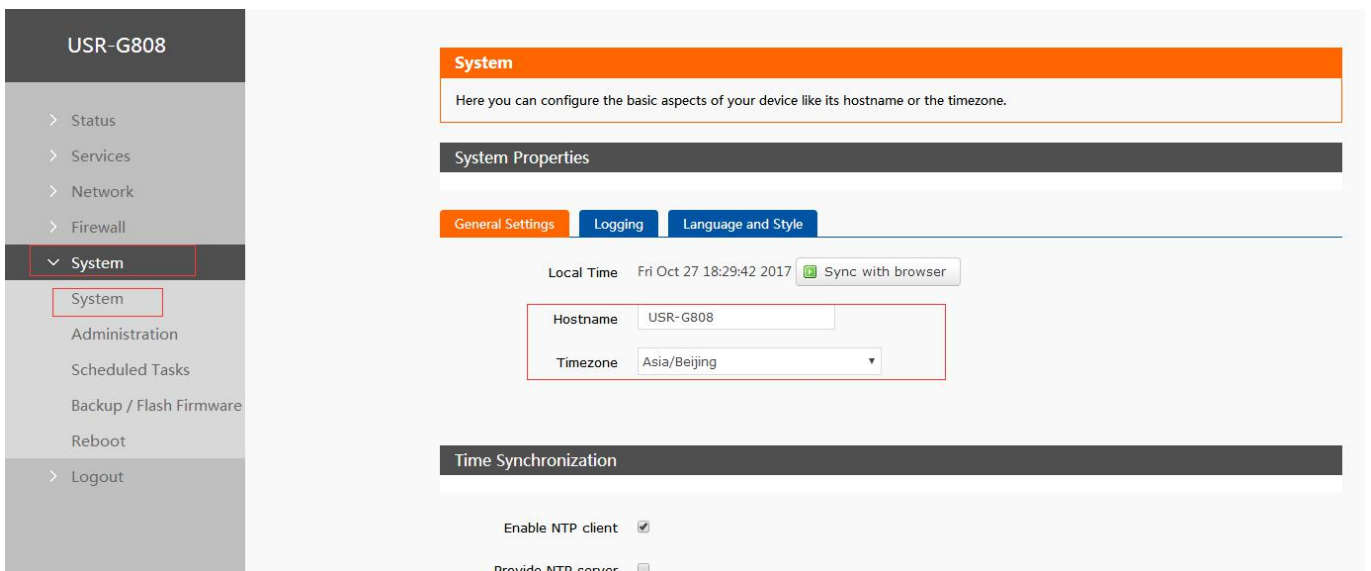


Diagram 3.3.2-1 Host Name and Time Zone Configuration

Note:

1. Host name :default USR-G808
2. Time Zone:default is east eight area

3.3.3. Web Server Password

Default password is root, this password is used to enter Web Server.

User can change password by Web Server as follow:

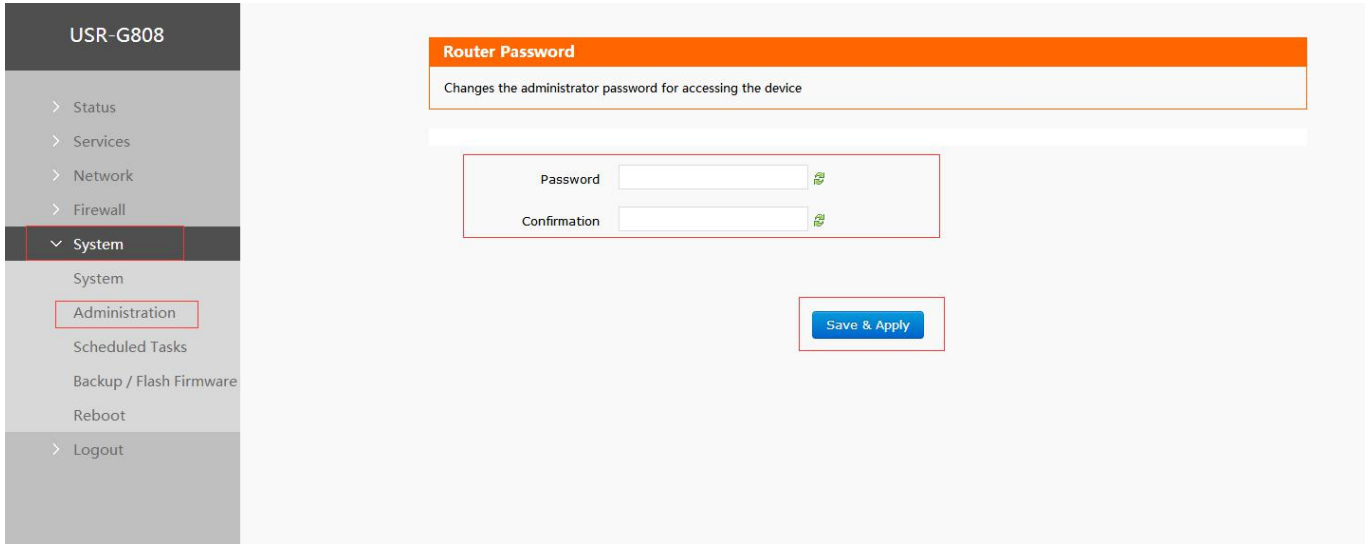


Diagram 3.3.3-1 Web Server password configuration

3.3.4. Scheduled Tasks

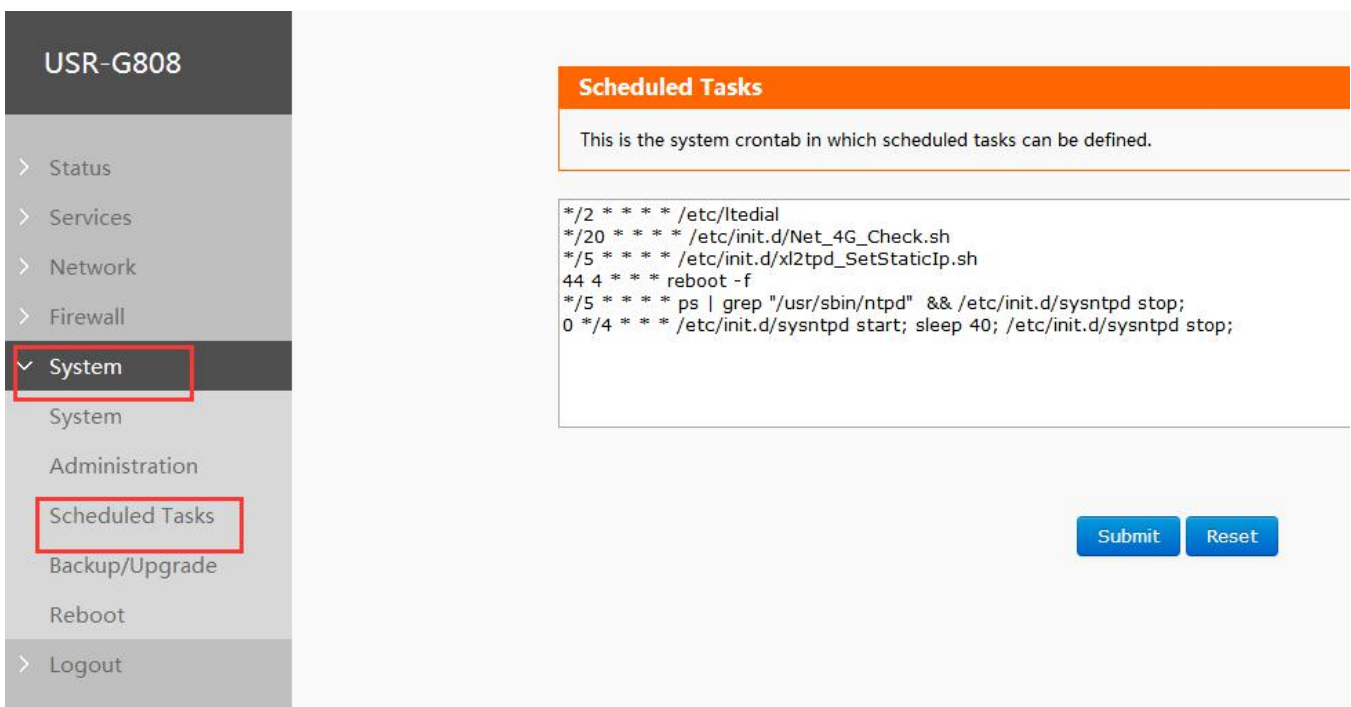


Diagram 3.3.4-1 Scheduled Tasks

Shell command to study

Parameters divide into min, hour, day, week, year, as below

```
* /1 * * * * echo crontest:`date` > /tmp/cron.log
```

Every two minutes, fill the current date in the cron.log under the /tmp

Reboot to restart this function; or send data to some serial port, such as: echo 123 > /dev/ttyS1

Note:

In this function, please do not delete the original tasks for the router normal running.

3.3.5. Restore to Default Factory Settings

Hardware restore:

- ✓ Press Reload button over 5 seconds and release, G808 will restore default settings and reset.
- ✓ Work after restart, SIM 2 LED and mandatory LED, 4LAN, WAN port light for 1s, then off.

User can also restore default settings by Web Server as follow:

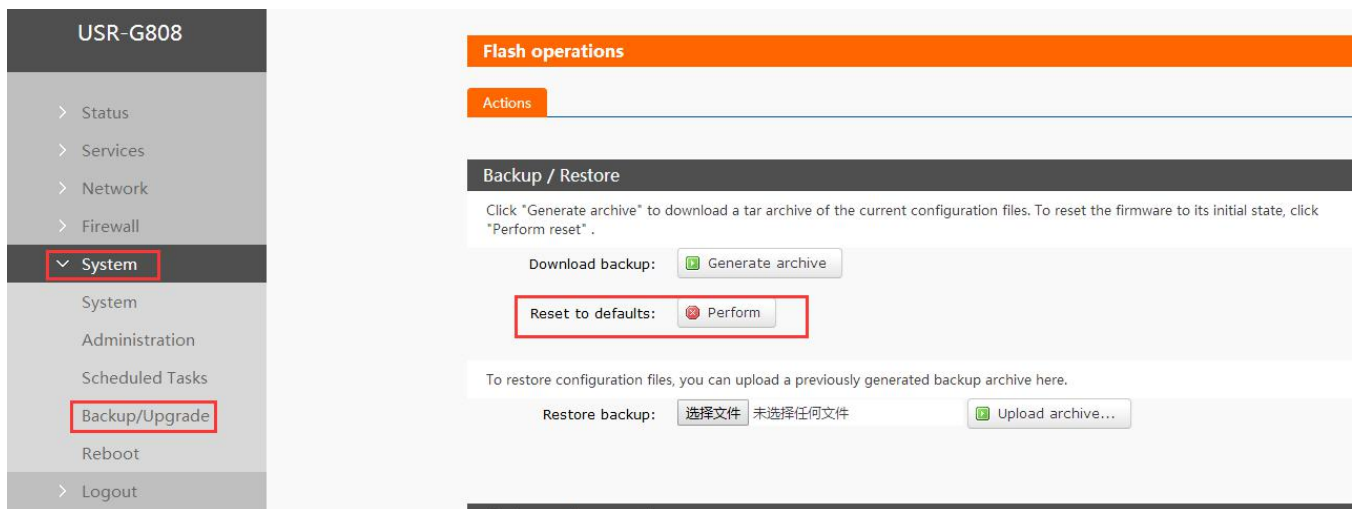


Diagram 3.3.5-1 Restore default settings

Click the bottom to restore

Note:

- ✓ This function is same as the hardware reload
- ✓ Download backup: download current parameters files of the router to backup
- ✓ Upload backup: put the files backed up into the router and work.

3.3.6. Introduce LED

20 indicators like below:

Name	Instr
Power	Supply the power and light for long time
Work	After the router work ,blink every 2s
WAN	WAN port wired and the led light, blink when communication
LAN1-4	LAN port wired and the led light, blink when communication
WLAN	When WIFI network work and keep light, blink if station access or the data transport.
2G instr (SIM1)	LTE modem 1 work in 2G
3G instr (SIM1)	LTE modem 1 work in 3G
Signal	The more SIM card 1signal instr light, the more strength the signal is.

strength 1-4(SIM1)	
2G instr (SIM2)	LTE modem 2 work in 2G
3G instr (SIM2)	LTE modem 2work in 3G
Signal strength 1-4(SIM2)	The more SIM card 1signal instr light, the more strength the signal is.

Form 3.3.6-1 Indicator Default Parameters

Instr:

- ✓ WAN and LAN indicator show the WAN and LAN running status
- ✓ Insert the net cable and the remote net device also work, the WAN/LAN indicator will blink.
- ✓ Power light on all the time
- ✓ When working in the 4G, 2Gand 3G will also light.

3.3.7. Upgrade Firmware Version

Upgrade by Web Server as follow:



Diagram 3.3.7-1 Upgrade Firmware Version

Note:

- The whole upgrading process will last about 2 minutes, user can enter Web Server after about 2 minutes.
- User can choose saving settings.
- User should keep powering up and LAN/WIFI connection during the whole upgrading process.

3.3.8. Reset

Reset time is about 40~60 seconds.

Reset by Web Server as follow:

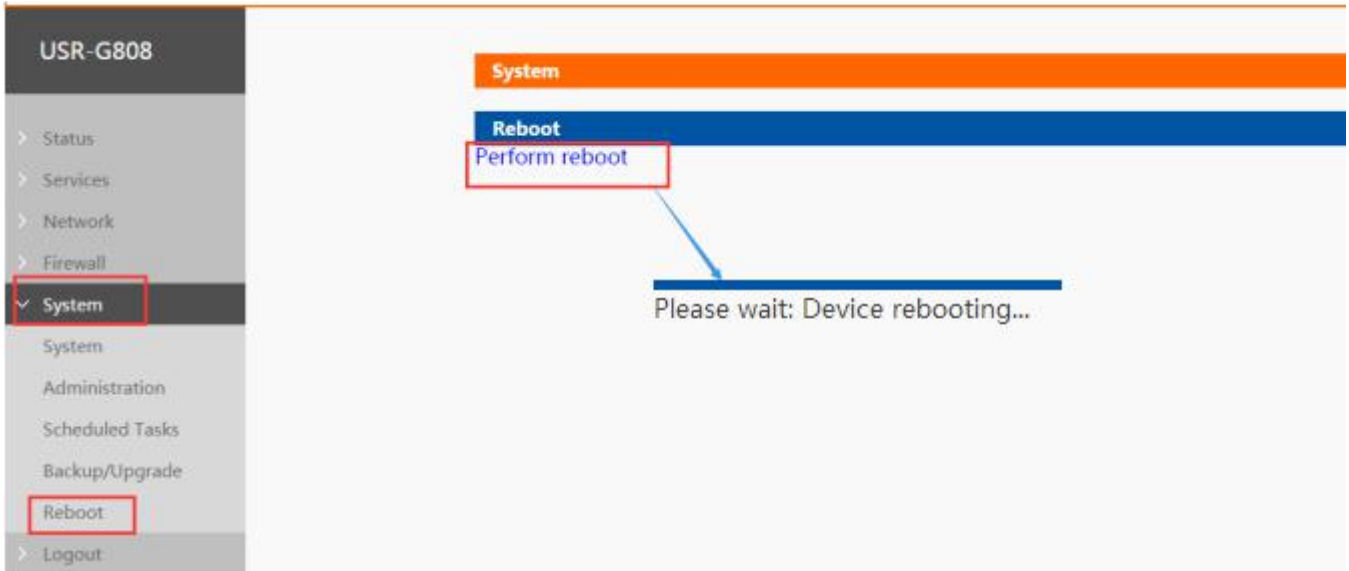


Diagram 3.3.8-1 Reset Function

3.3.9. NTP

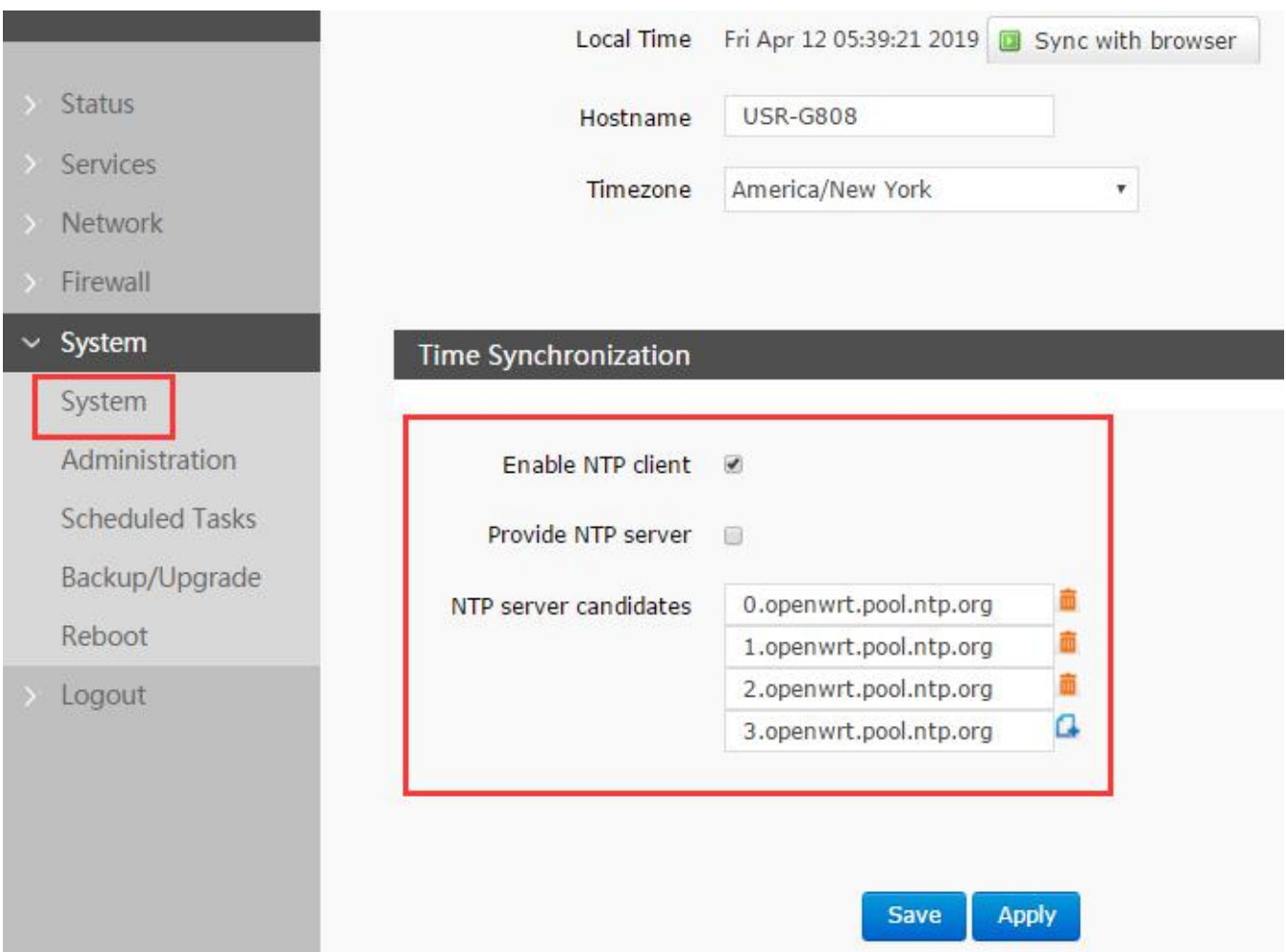


Diagram 3.3.9-1 NTP Enable

The router supports NTP(default enable it), and you can set the NTP server address.

4. Configuring

4.1. Webpage Setting

For the first time using the G808, please configuring it. Connect the LAN of the G808 via PC or connect the WLAN ,then open Web Server and configure in the management webpage

Parameters	Defaults settings
SSID	USR-G808-XXXX
LAN interface IP Address	192.168.1.1
User name	root
Password	root
WLAN Password	www.usr.cn

Diagram 4.1-1 G808 Default Parameters

Take default parameters as example:

User can connect PC to SSID USR-G808-XXXX.

Then open browser and enter 192.168.1.1, log in with User name and Password(both are root), user can enter Web Server.

Please change language in the up right for the default language is Chinese.

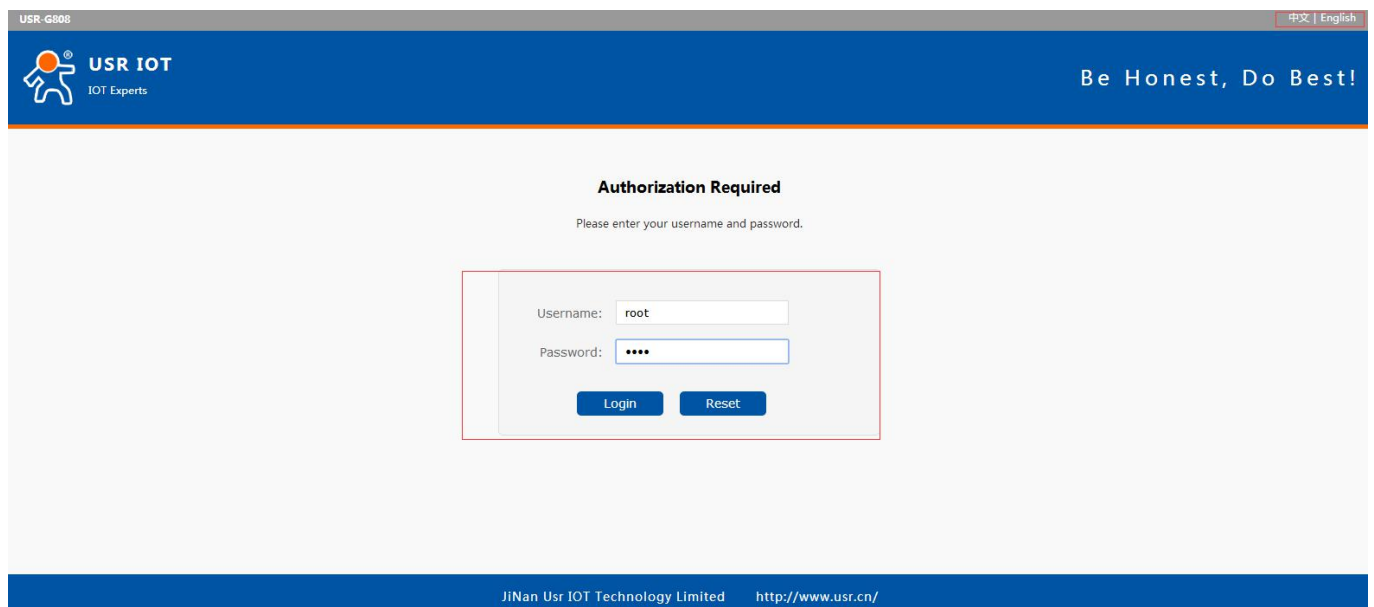


Diagram 4.1-2 Web Server Login Webpage

4.2. Web Function

The left is a label, can set some parameters

➤ Status

USR-G808

- Status
- Overview
- Services
- Network
- Firewall
- System
- Logout

Status

System

Hostname	USR-G808
Firmware Version	V1.0.13(EN)
Local Time	Fri Apr 12 02:42:50 2019
Uptime	0h 4m 18s
Load Average	1.50, 1.19, 0.54

Memory

Total Available	99840 kB / 126000 kB (79%)
Free	78380 kB / 126000 kB (62%)
Cached	14844 kB / 126000 kB (11%)
Buffered	6616 kB / 126000 kB (5%)

Network

IPv4 WAN Status	Not connected
IPv6 WAN Status	Not connected

Diagram 4.2-1 Status

In this page shows the name of the device, version of firmware, current running status.

➤ Network interface page:

WAN_4G2 | WAN_4G1 | WAN_WIRED | LAN

Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	Uptime: 0h 4m 26s MAC-Address: D8:B0:4C:D9:4F:30 RX: 228.91 KB (2529 Pkts.) TX: 258.10 KB (1492 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDD1:B494:14C5:0:0:0:0:1/60	Connect Stop Edit Delete
WAN_4G1 eth1	MAC-Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN_4G2 eth2	Uptime: 0h 0m 0s MAC-Address: 00:A0:C6:00:00:00 RX: 0.00 B (0 Pkts.) TX: 32.25 KB (107 Pkts.)	Connect Stop Edit Delete
WAN_WIRED eth0.2	Uptime: 0h 0m 0s MAC-Address: D8:B0:4C:D9:4F:30 RX: 0.00 B (0 Pkts.) TX: 30.50 KB (92 Pkts.)	Connect Stop Edit Delete

Add new interface...

Diagram 4.2-2 Interface

Webpage, main is interface device including(LAN port and WAN port setting,WIFI wireless parameters DHCP/DNS and so on. Mainly is the device operating parameters setting.

➤ System page

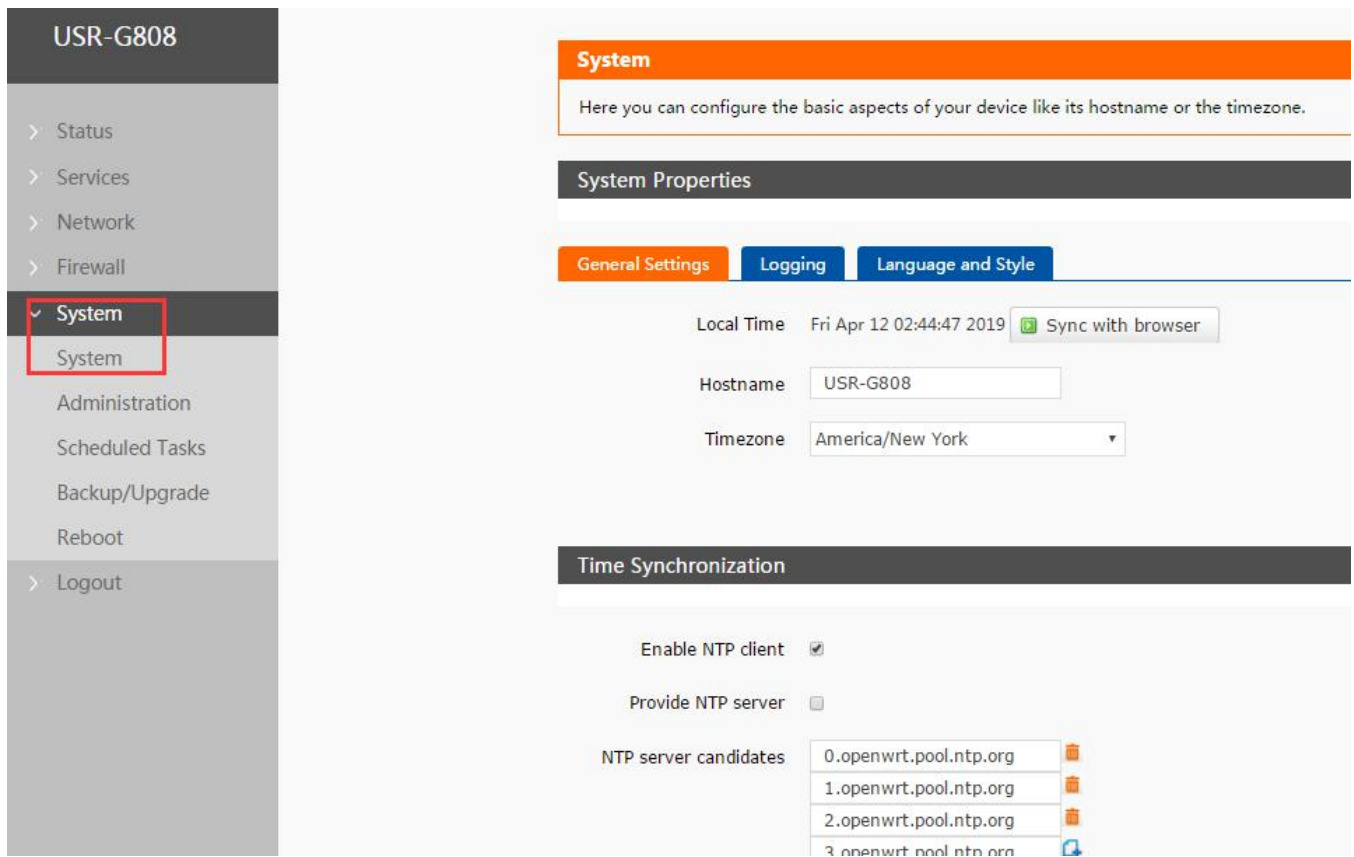


Diagram 4.2-3 System

System page, including login password,time setting, firmware upgrade, reset and so on.

5. Contact Us

Company: Jinan USR IOT Technology Limited

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

Web: www.usriot.com

Support: h.usriot.com

Email: sales@usr.cn

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

6. Disclaimer

This document provides the information of USR-G808 products, it hasn't been granted any intellectual property license by forbidding speak or other ways either explicitly or implicitly. Except the duty declared in sales terms and conditions, we don't take any other responsibilities. We don't warrant the products sales and use explicitly or implicitly, including particular purpose merchant ability and marketability, the tort liability of any other patent right, copyright, intellectual property right. We may modify specification and description at any time without prior notice.

7. Update History

Time	Version	Content modified
2017-7-3	V1.0.1	Built
2017-7-25	V1.0.2	Default parameters instr
2017-7-31	V1.0.3	Add the outlook diagram
2017-9-19	V1.0.4	Modify the error
2017-11-07	V1.0.5	Modify the humidity range