USR-G806s User Manual

1. Introduction

1.1. Overview

USR-G806s is a high-performance industrial 4G wireless router with serial port and powerful DTU function. Using public wireless network, it provides users with an integrated solution of industrial 4G router and DTU. This product adopts high-performance embedded CPU and the operating frequency is up to 580MHz. Based on a variety of hardware interfaces and powerful software functions, users can quickly set up their own application network. It has been widely used in the M2M industry of the Internet of Things, providing reliable data transmission network for smart grid, personal medical care, smart home, self-service terminal, industrial automation, environmental protection agriculture, municipal services and other fields.

1.2. Features

Stable and Reliable

- Industrial design, metal housing, protection class IP30.
- Wide voltage input, with anti-reverse protection.
- Din-rail or panel mounting, suitable for various scenarios.
- ESD, surge and EFT protection.
- Hardware watchdog, link detection mechanism make it self-recovery from unexpected failure and guarantee system stability.

Flexible Networking

- Provide 4G network, compatible with 3G/2G network.
- Supports automatic network inspection, 4G/3G/2G network switching, APN/VPDN card.
- Supports wired /4G multi-network online at the same time, multi-network backup function.
- Supports 2.4GHz WIFI, flexibly choose wired or WiFi network.
- Supports VPN (PPTP, L2TP, IPSEC, OpenVPN, GRE) and VPN encryption.

Powerful Functions

- Supports connecting to USR Cloud to achieve remote monitoring, remote upgrading, Email alert and remote access the internal webpage.
- Supports serial to Ethernet communication, compatible with basic router functions and DTU functions, meeting various application scenarios.
- Supports 1 10/100Mbps LAN port and 1 WAN/LAN port.
- Supports WLAN wireless network, supports multiple LED indicator lights.
- Supports wired/wireless multi-network online at the same time, multi-network backup function.
- Supports automatic APN network check, system switching, SIM information display, supports APN/VPDN network card.
- Supports DDNS, PPPoE, DHCP and statis IP.
- Supports firewall, NAT, white/black list, SNAT and DNAT.
- Supports traffic services, set the network speed limit rules via interface, IP addresses, and MAC addresses as required.
- Supports SSH, Telnet and Web configuration.

- Support connecting to our remote monitoring platform to achieve remote monitoring, remote upgrading and remote configuration.
- Supports hardware reset, supports hardware watchdog, ensuring system stability.

1.3. Specification

USR-G806s Ordering Guide			
Product	USR-G806s		
Region	China/Southeast Asia		
Cellular Network	Frequency bands	FDD-LTE	B1/3/5/8
		TDD-LTE	B38/39/40/41
		WCDMA	B1/8
		CDMA2000	CDMA1X/ 1xEV-DO rel.0/ 1xEV-DO rev. A：800 MHz
		TD-SCDMA	B34/39
		GSM/GPRS/EDGE	900/1800MHz
	Theoretical bandwidth	FDD-LTE	Max. 150Mbps（DL）/50Mbps(UL)
		TDD-LTE	Max.135Mbps（DL）/35Mbps(UL)
		WCDMA	Max. 42Mbps（DL）/5.76Mbps(UL)
		CDMA2000	Max. 3.1Mbps（DL）/1.8Mbps(UL)
		TD-SCDMA	Max. 4.2Mbps（DL）/2.2Mbps(UL)
		GSM/GPRS/EDGE	Max. 384kbps（DL）/128kbps(UL)
Region	EMEA/Thailand		
Cellular Network	Frequency bands	FDD-LTE	B1/3/7/8/20/28A
		TDD-LTE	B38/40/41
		WCDMA	B1/8
		GSM/EDGE	B3/8
	Theoretical bandwidth	FDD-LTE	Max. 150Mbps（DL）/50Mbps(UL)
		TDD-LTE	Max. 130Mbps（DL）/35Mbps(UL)
		DC-HSPA+	Max. 42Mbps（DL）/5.76Mbps(UL)
		WCDMA	Max. 384Kbps（DL）/384Kbps(UL)
		EDGE	Max. 296Kbps（DL）/236.8Kbps(UL)
		GPRS	Max. 107Kbps（DL）/85.6Kbps(UL)

USR-G806s Basic Parameters

Product	4G wireless router	USR-G806s
Ethernet Port	Wired WAN	1*WAN/LAN
	Wired LAN	1*LAN
WIFI	WIFI wireless network	IEEE802.11b/g/n, 2.4GHz AP mode
	Antenna	1*3dbi antenna
	Distance	100m in open area
SIM/ Antenna	SIM/USIM	Standard 6-pin SIM slot, 3V/1.8V SIM card
	Antenna	2.5dbi full frequency stick antenna
DTU	DTU mode	NET, HTTPD, MODBUS
	Heartbeat/Identity packet	Support
	Baud rate	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
	Data bit	8
	Stop bit	1, 2
	Parity	NONE,ODD,EVEN
	Serial Type	RS485
	SOCKET	4 sockets support TCPS(only socket A supports)/TCPC/UDPS/UDPC
Button	Reload	Hardware reset button
Indicator	Indicator light	Power, WIFI, 2/3/4G, signal strength, WAN, LAN
Temperature	Operating temperature	-20℃～ +70℃
	Storage temperature	-40℃～+125℃
Humidity	Operating humidity	5%～95%RH(non-condensing)
	Storage humidity	1%～95%RH(non-condensing)
Power Supply	Power Voltage	DC 9～36V
	Power consumption	Under DC 12V power supply, the average current is 270mA and the maximum current is 400mA.

Power consumption:

USR-G806s works at full speed, with 1 WIFI station access, 1 LAN port access, and 4G access to the external network, data transmission speed is 10KByte/s.

Operating mode	Power supply	Average current (mA)	Maximum current (mA)
LAN+WAN, full speed (4G +WLAN)	DC12V	151	385
LAN, full speed (4G+WLAN)	DC12V	270	400
LAN+WAN, full speed (WLAN)	DC12V	130	236
WAN, full speed (WLAN)	DC12V	128	295

When G806s is powered by 12V and working at full speed:
The average power consumption is 3.24W and the maximum is 4.8W. The average current is 270mA and the maximum is 400mA.

1.4. Interface

No.	Item	Description
1	DC interface	DC:9~36V, standard 5.5*2.1mm round socket
2	DC terminal	DC:9~36V, green terminal block, 5.08mm-2
3	WAN/LAN	1*10/100M, MDI/MDIX, 1.5KV electromagnetic isolation protection
4	LAN	1*10/100M, MDI/MDIX, 1.5KV electromagnetic isolation protection
5	TBD	1
6	RS485	1*standard 3.81mm*3 pin (A,B,G) interface
7	Indicator	Power, WIFI, 2/3/4G, signal strength, WAN, LAN
8	SIM slot	3V/1.8V SIM card
9	Reload	Press and hold for more than 5s to reset the device
10	WIFI antenna	2.4G stick antenna
11	4G antenna	Full frequency stick antenna
12	Ground screw	Recommend to connect the ground screw on the side to the ground cable.

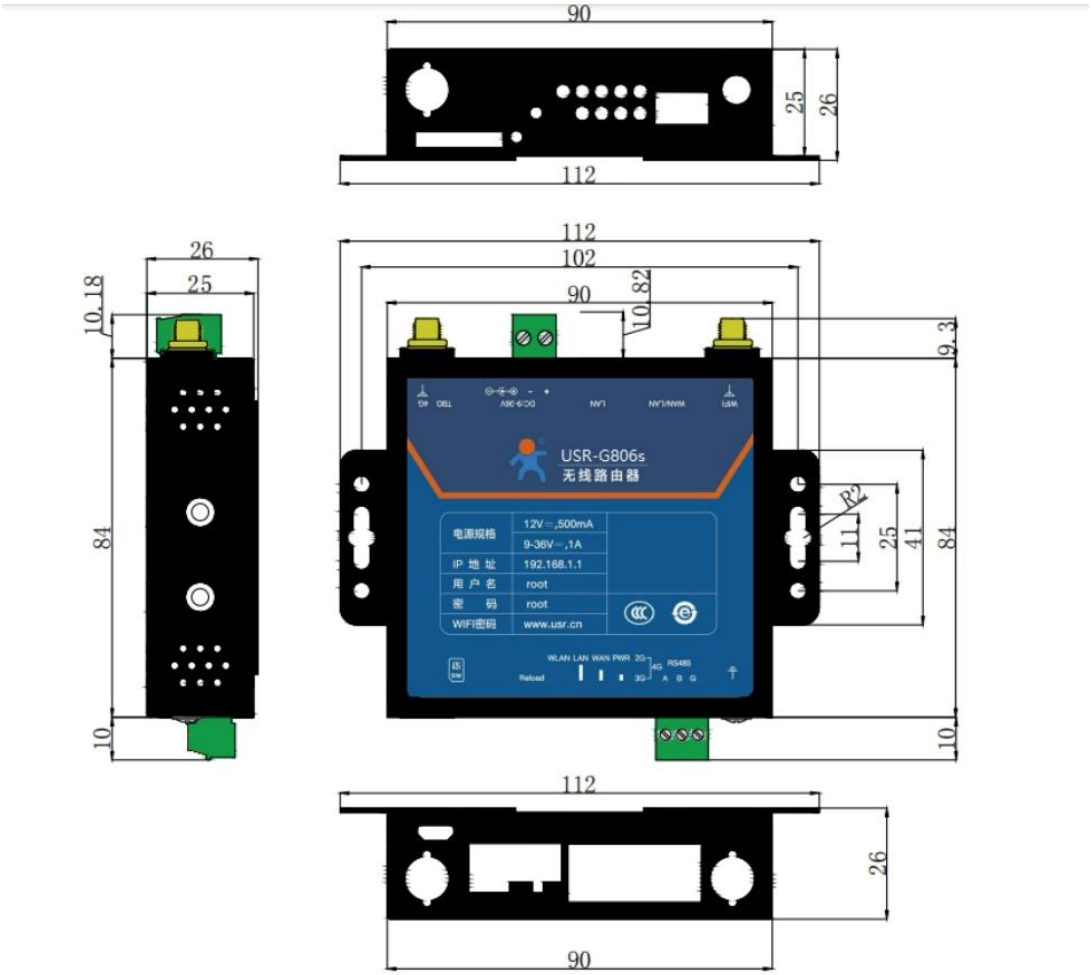
Grounding screw installation:

- Unscrew the ground screw --→ insert the ground ring of the ground cable into the ground screw --→ tighten the ground screw --→ connect the ground cable.
- In order to improve the anti-interference ability of the router, the ground cable should be connected to the ground screw of the router according to the specific environment during installation.

1.5. Indicator

Item	Description
PWR	Power indicator, always on after powered on
WAN	WAN indicator will be on after connecting Ethernet cable, blink during data transmission
LAN	LAN indicator will be on after connecting Ethernet cable, blink during data transmission
WLAN	WLAN indicator will be on during normal operation
2G Indicator	2G indicator will be on when connects to 2G network
3G Indicator	3G indicator will be on when connects to 3G network
Signal strength (1-3)	The more signal strength indicators are on, the stronger the signal is.

1.6. Dimensions



- Metal housing, supports panel and DIN-rail mounting.
- Dimensions: 112*84.0*26.0mm (Power terminals, RS485 terminals, antennas, and antenna mounts are excluded)

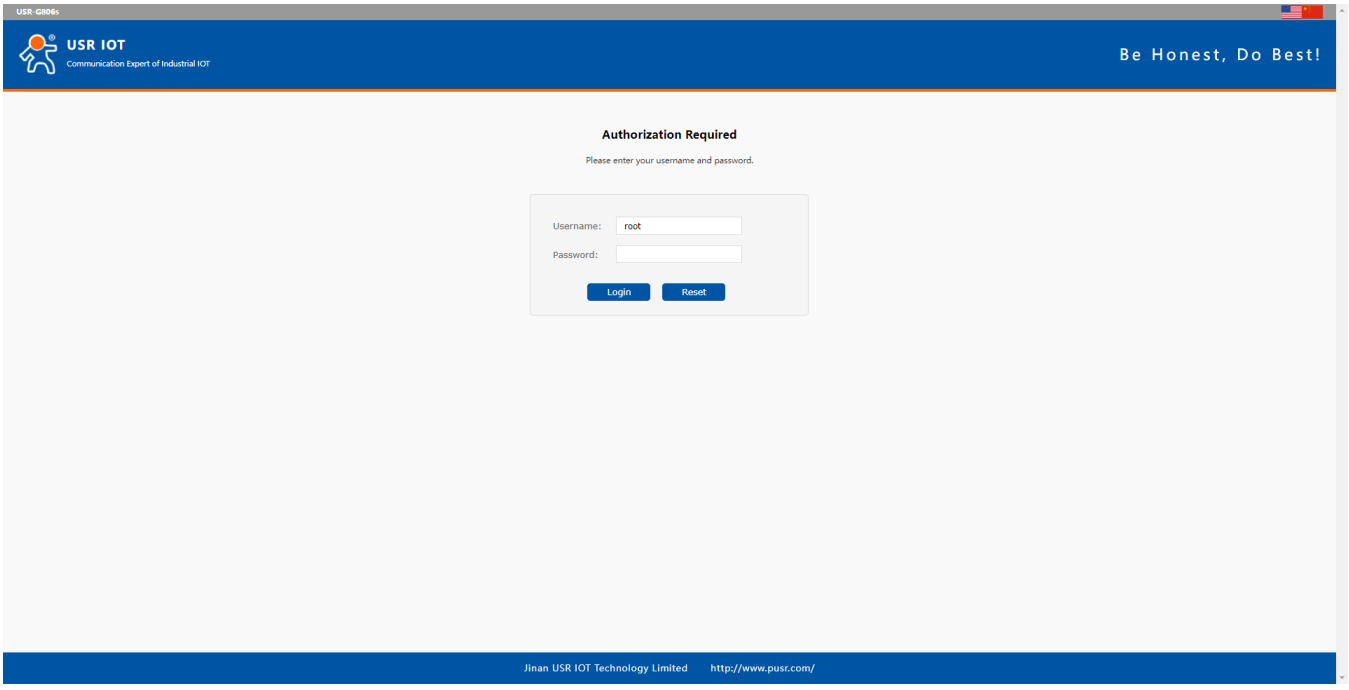
2. General Function

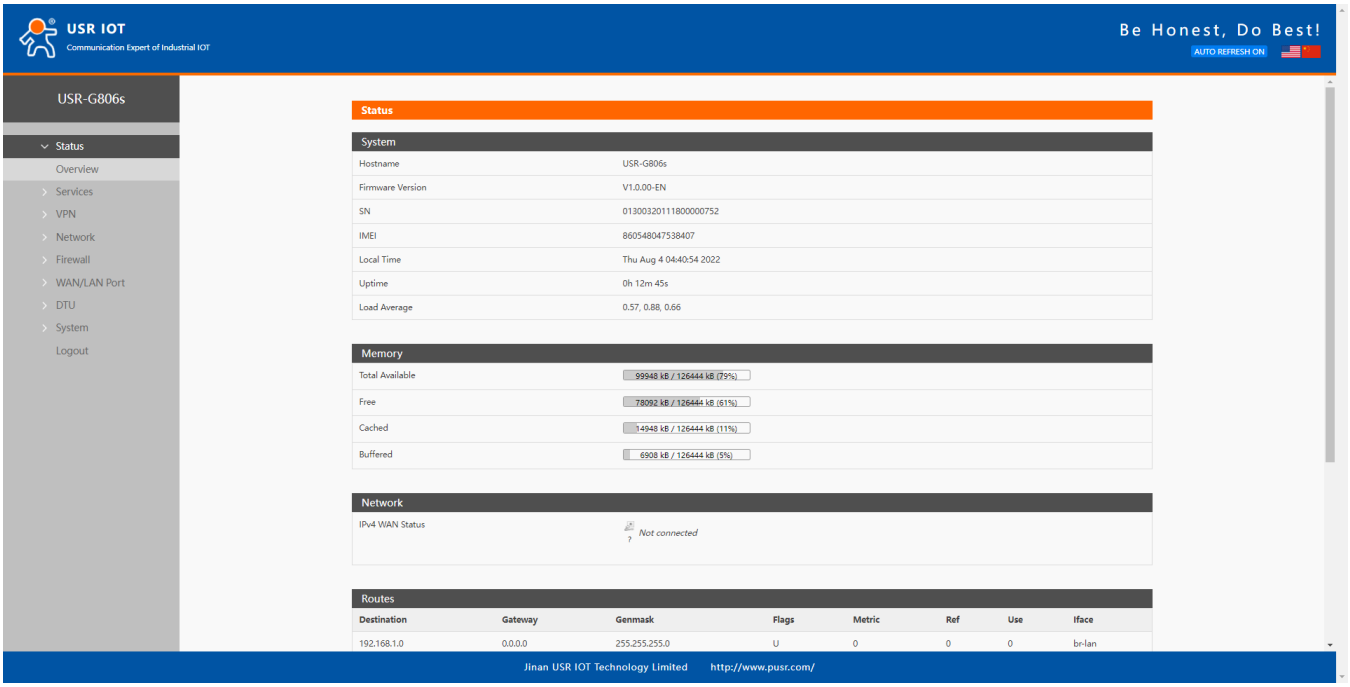
2.1. Web Interface

Connect PC to the LAN port of USR-G806s via a Ethernet cable, or directly connect the PC to the WiFi of the G806s, then log into the webpage. Default parameters are as below:

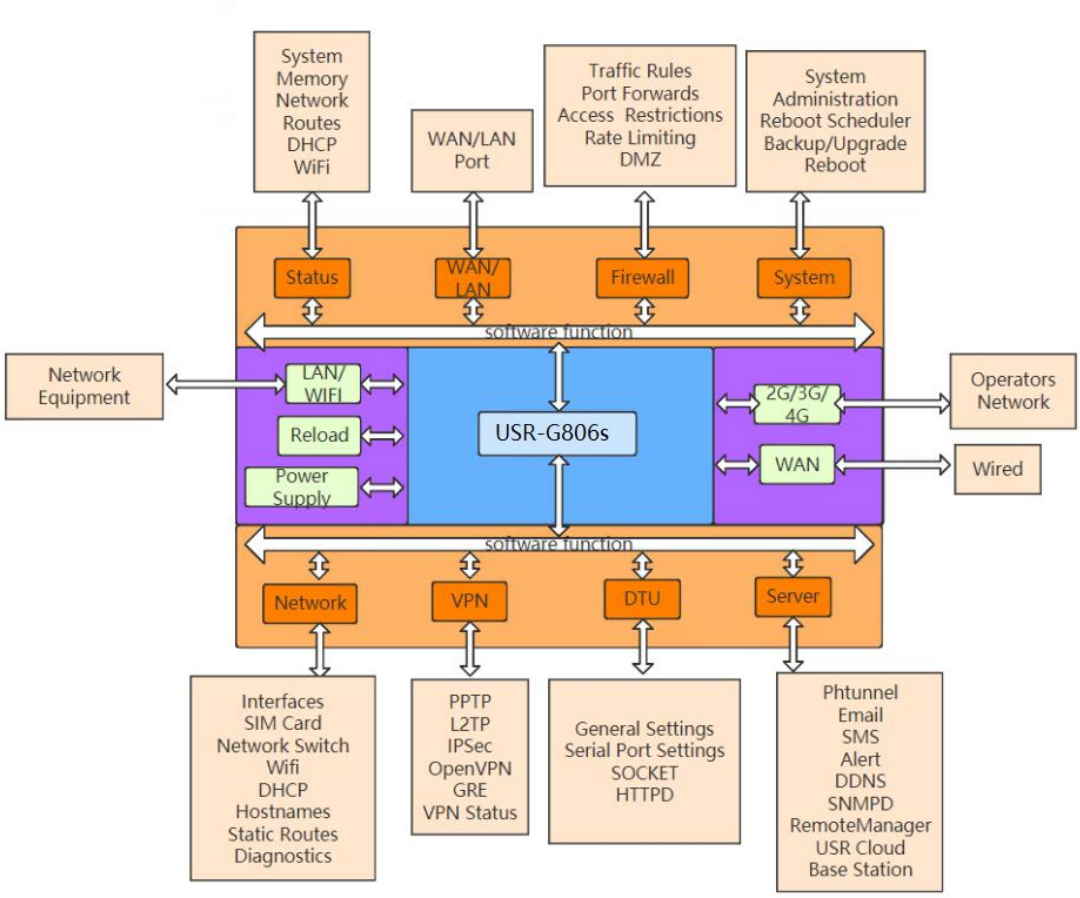
Parameters	Default
SSID	USR-G806s-XXXX
LAN IP address	192.168.1.1
Username	root
Password	root
WiFi password	www.pusr.com

Enter 192.168.1.1 in the browser to log into the webpage of USR-G806s, username and password are both “root”, then click “Login”.



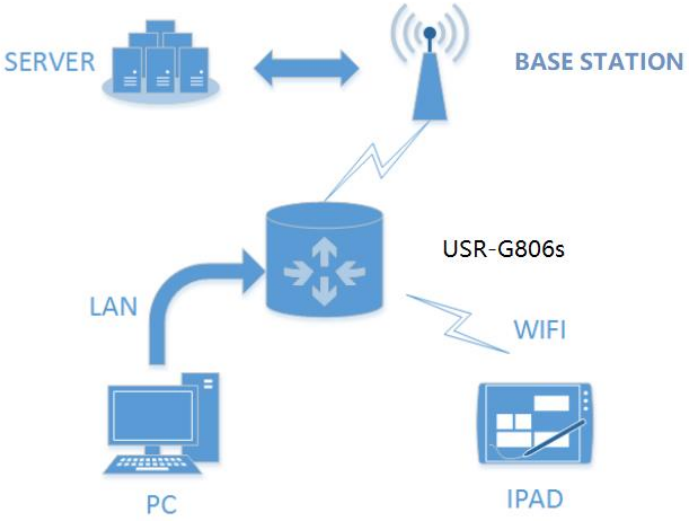

USR IOT
Communication Expert of Industrial IOT
Be Honest, Do Best!
AUTO REFRESH ON
USR-G806s
Status
Overview
Services
VPN
Network
Firewall
WAN/LAN Port
DTU
System
Logout
Status
System
Hostname USR-G806s
Firmware Version V1.0.00-EN
SN 01300320111800000752
IMEI 860548047538407
Local Time Thu Aug 4 04:40:54 2022
Uptime 0h 12m 45s
Load Average 0.57, 0.88, 0.66
Memory
Total Available 99948 kB / 126444 kB (79%)
Free 78092 kB / 126444 kB (61%)
Cached 14948 kB / 126444 kB (11%)
Buffered 6908 kB / 126444 kB (5%)
Network
IPv4 WAN Status Not connected
Routes
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 br-lan
Jinan USR IOT Technology Limited http://www.pusr.com/

2.2. Functional Diagram



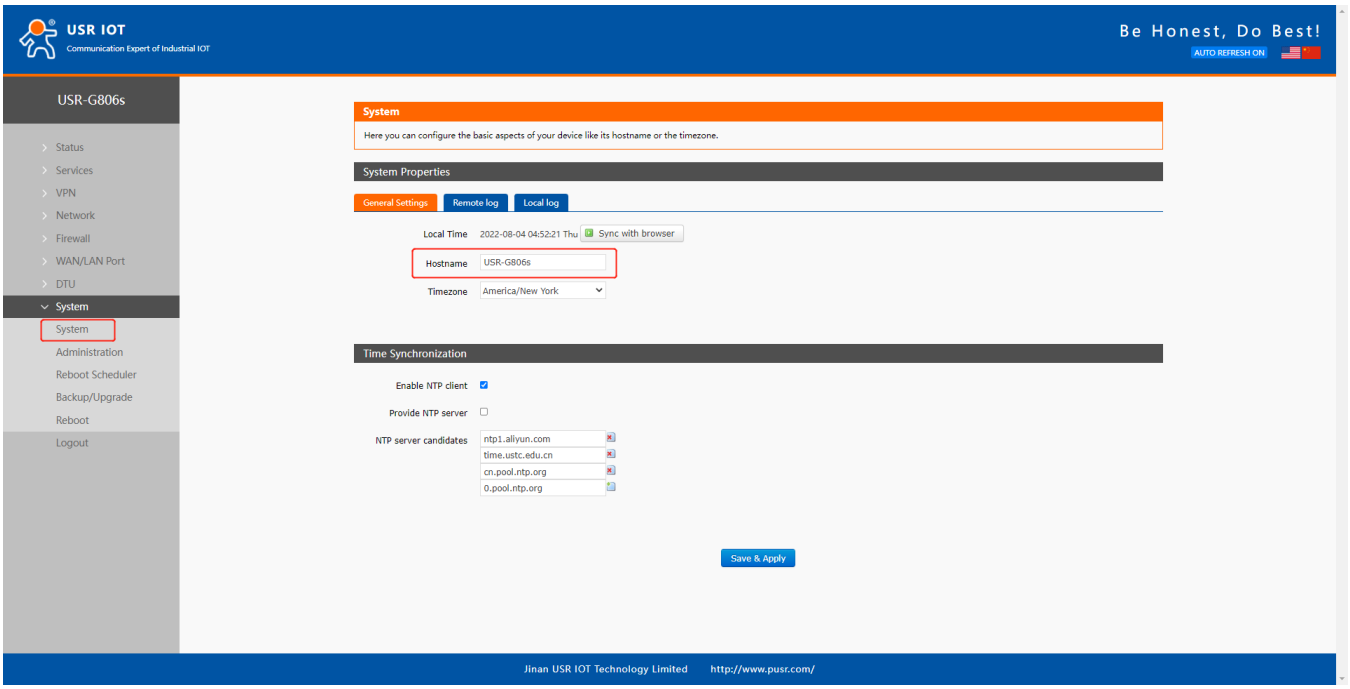
Network card	No.	Interface
LAN	br-lan	LAN
WIFI AP	ra0	LAN
Wired WAN	eth0.2	WAN_WIRED
4G	eth1	WAN_4G

Following is the application diagram:



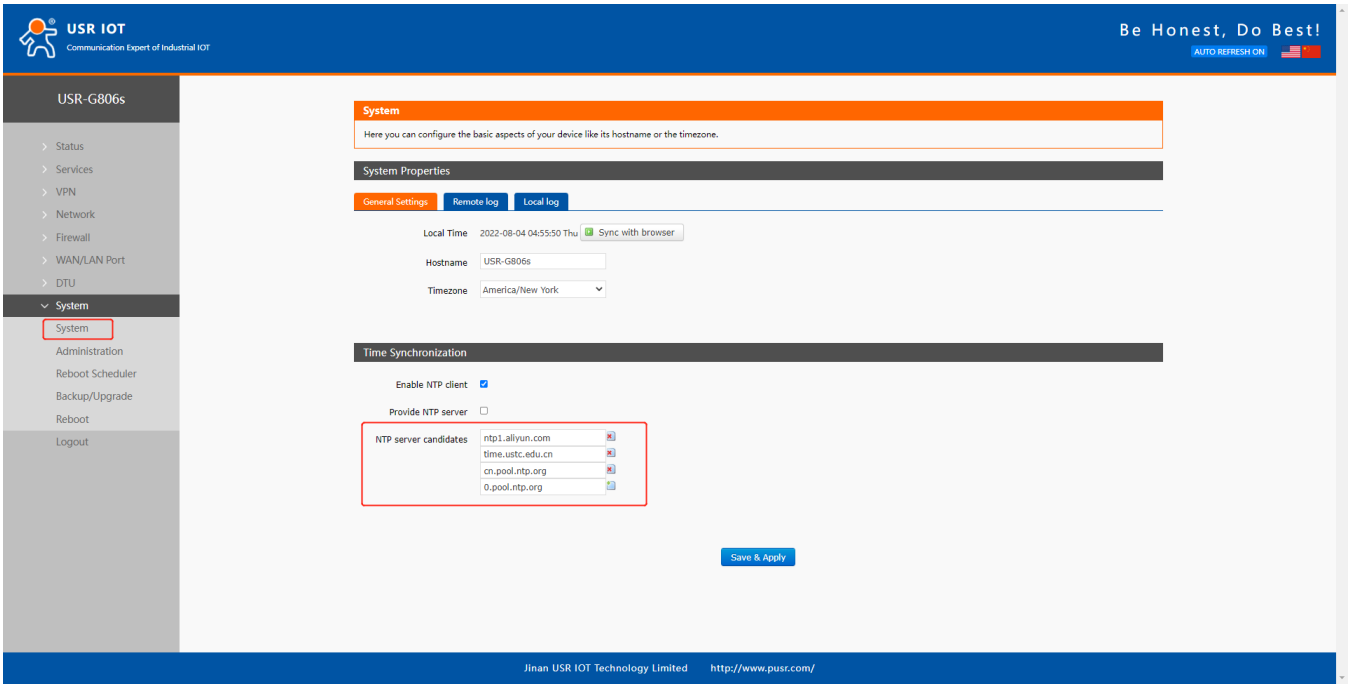
2.3. Hostname

The hostname defaults to USR-G806s.



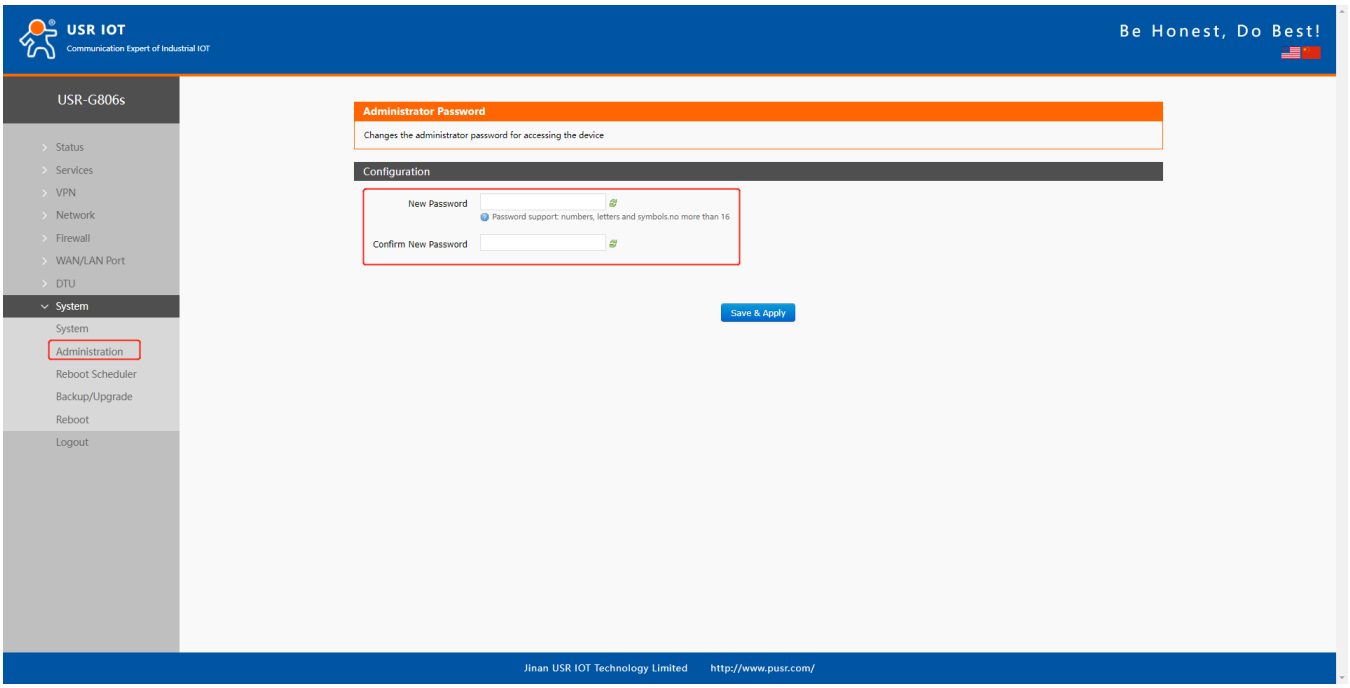
2.4. NTP Settings

NTP client function is default to be enabled, you can set different NTP server address.



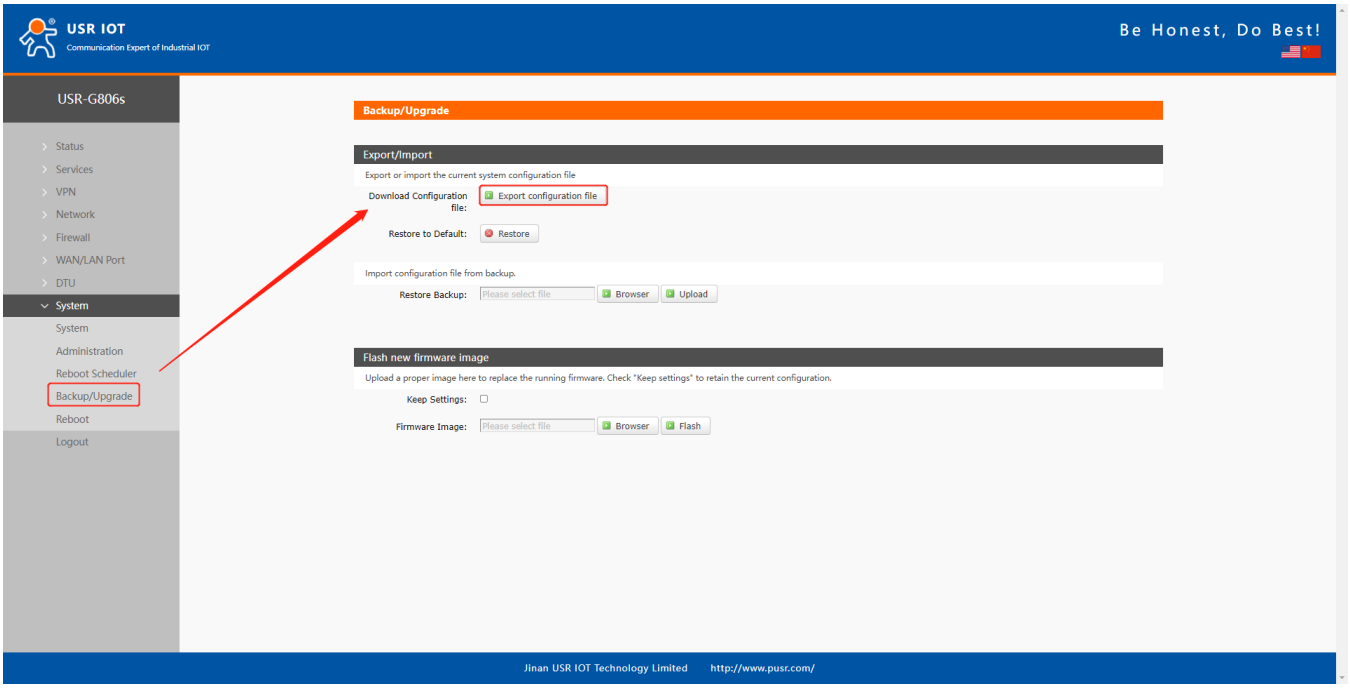
2.5. Username/Password Settings

Username and password are default to “root” which used to log into the webpage of the device. Password can be changed but the username cannot be changed.

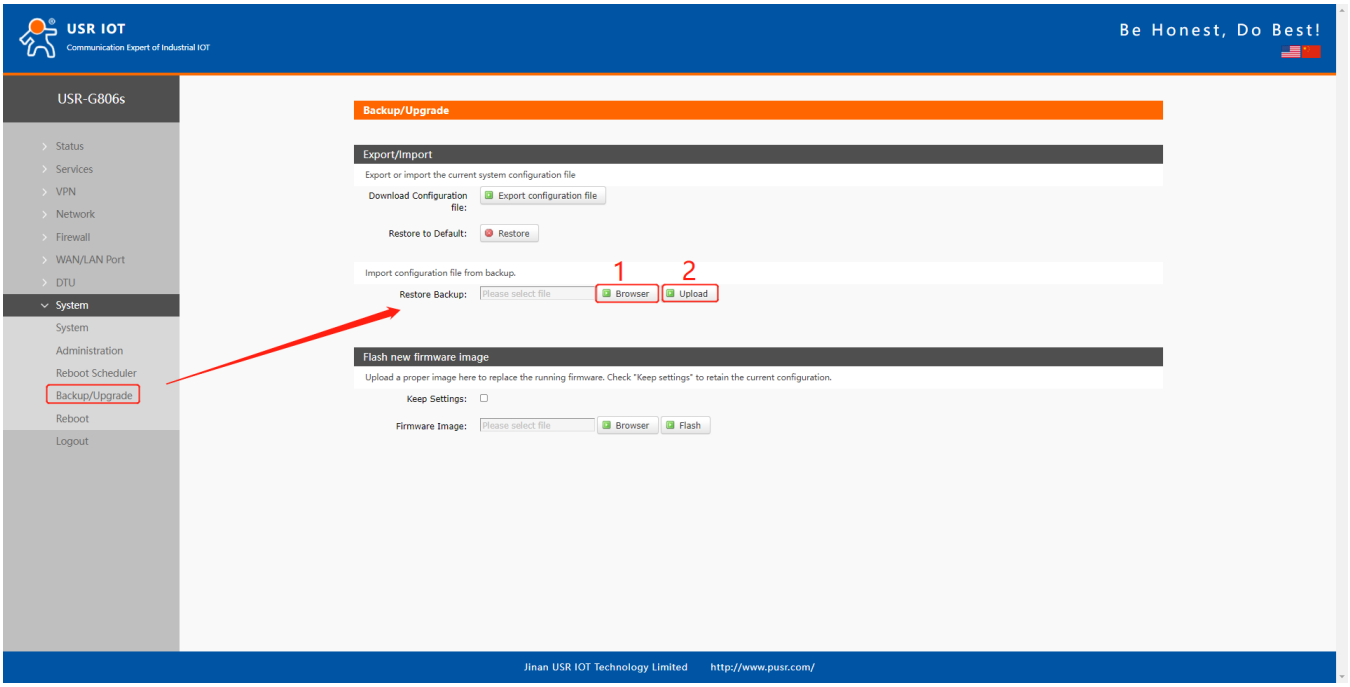


2.6. Backup Parameters

Download configuration file: Click **Export configuration file**, we can download the current parameters to a zip file, like **backup-USR-G806s-2022-08-04.tar.gz**, then save it in the computer.



Upload configuration file: Upload the configuration file to the router, then the parameters will be saved and take effect.



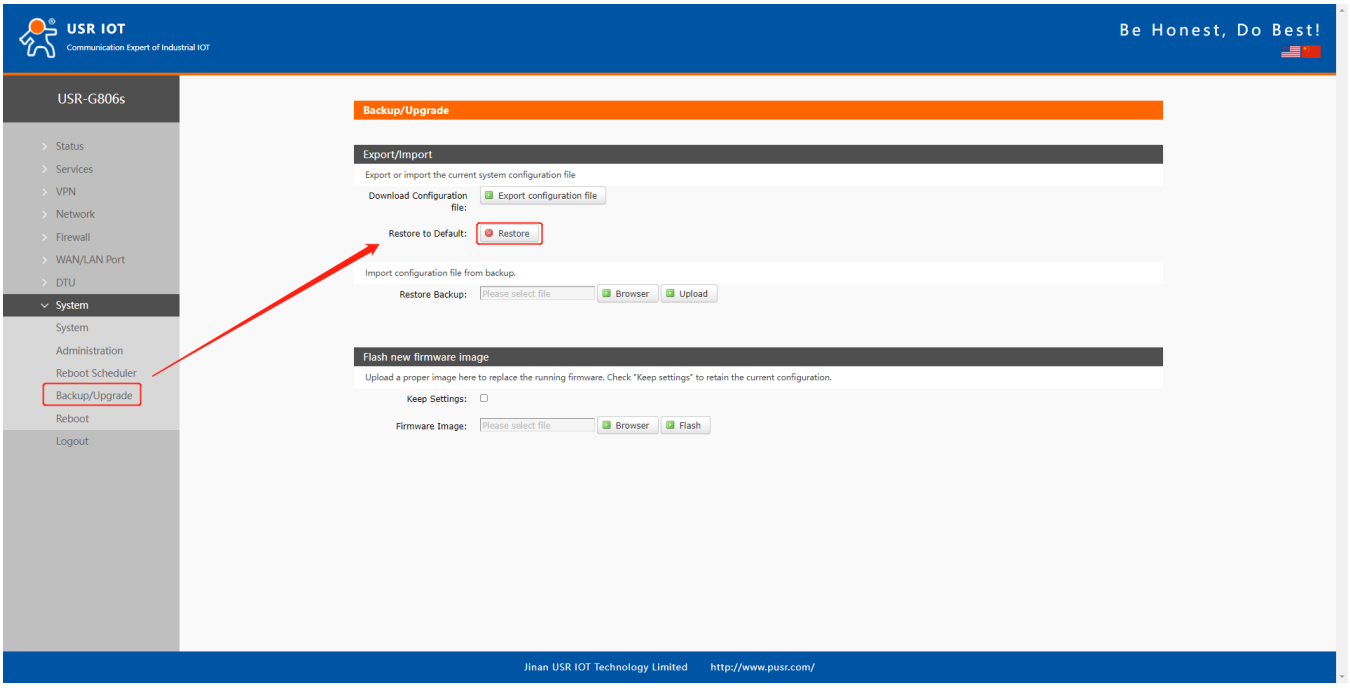
2.7. Reset

2.7.1. Hardware Reset

There is a **Reload** button in the device. After power on G806s device, press and hold the **Reload** button for more than 5s then release it, the device will restore to factory and restart automatically. When the device restarts, all the indicators will flash once and then turn off (the power indicator is still on).

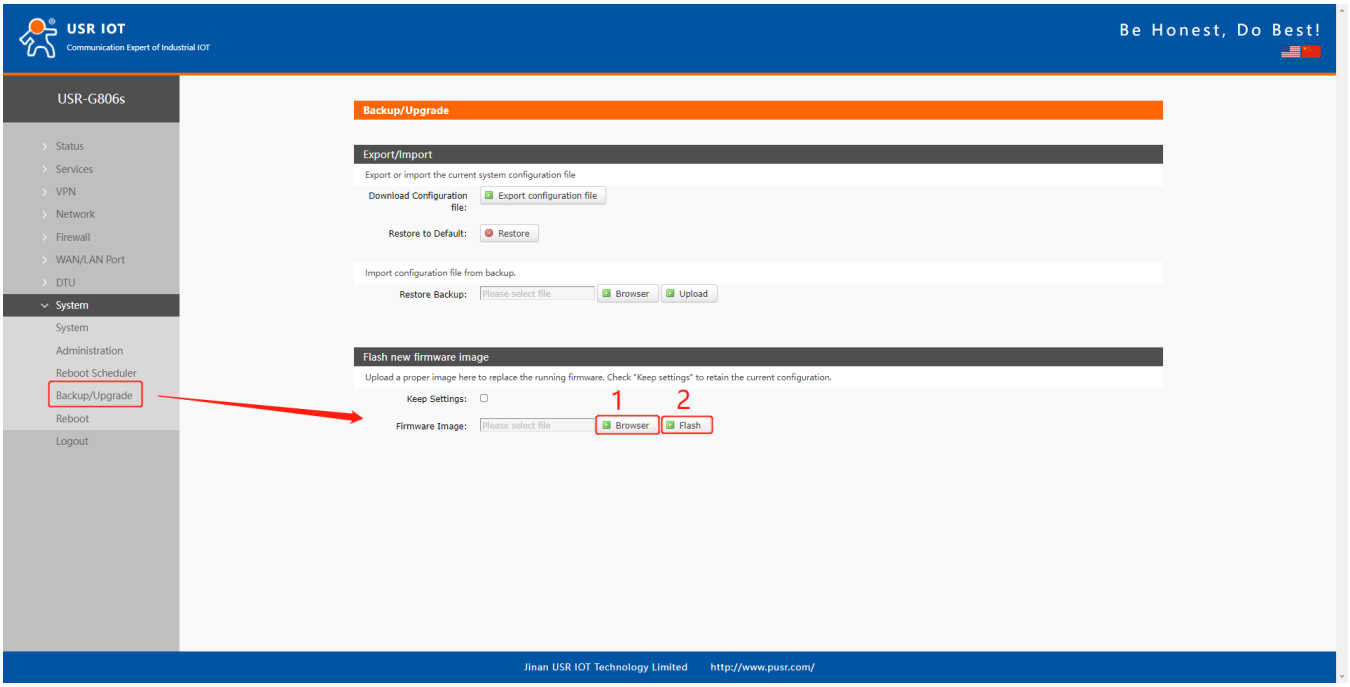
2.7.2. Software Reset

We can also reset the device via its webpage.



2.8. Firmware Upgrade

USR-G806s supports upgrading via webpage.

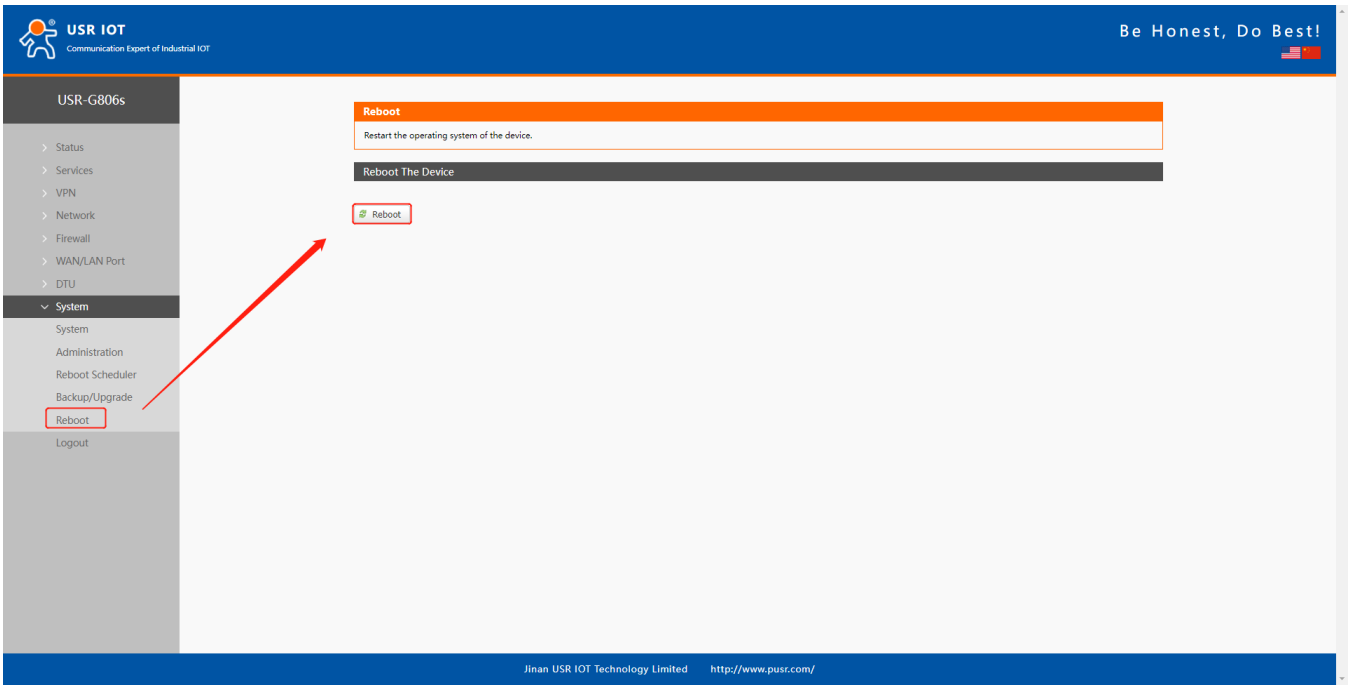


Note:

- The firmware upgrading will last 3-4 minutes , please log into the page again after 4 minutes.
- You can choose whether to enable **Keep Settings**.
- During the upgrading, please do not power off the device or disconnect the Ethernet cable.

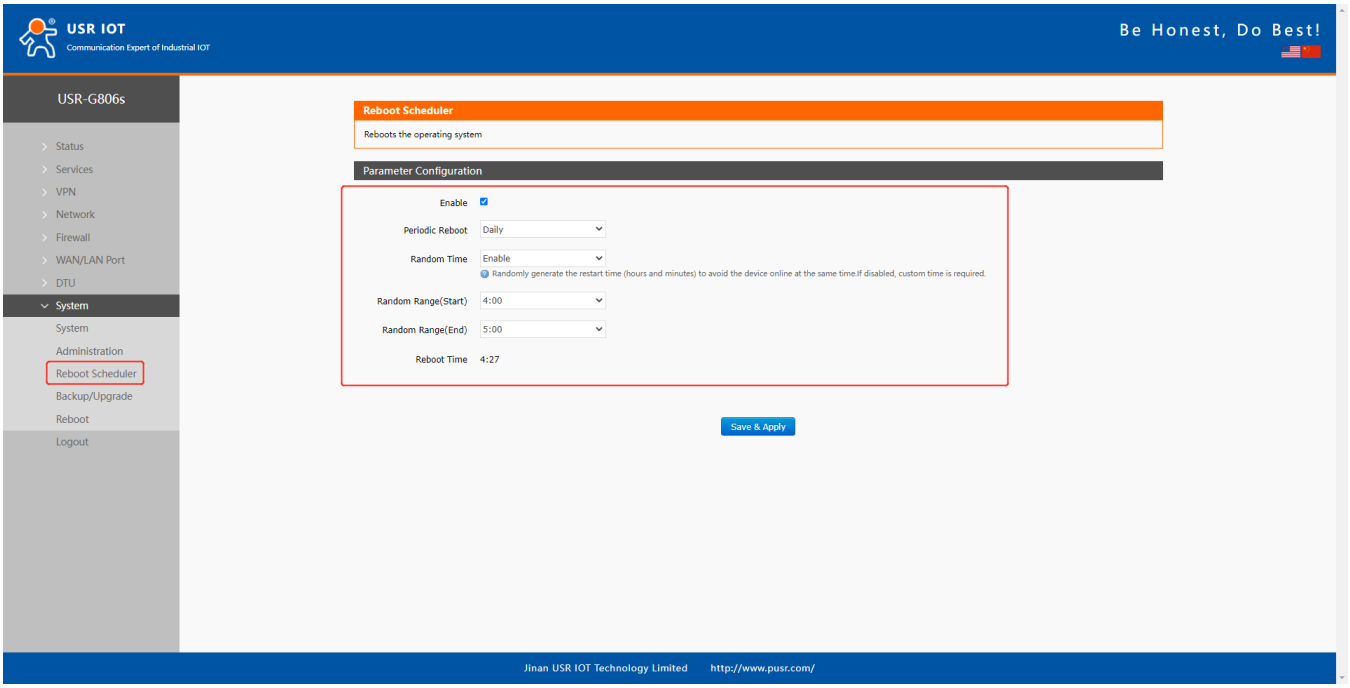
2.9. Reboot

Click **Reboot** to restart the device, it will last about 1 minute.



2.10. Reboot Sheduler

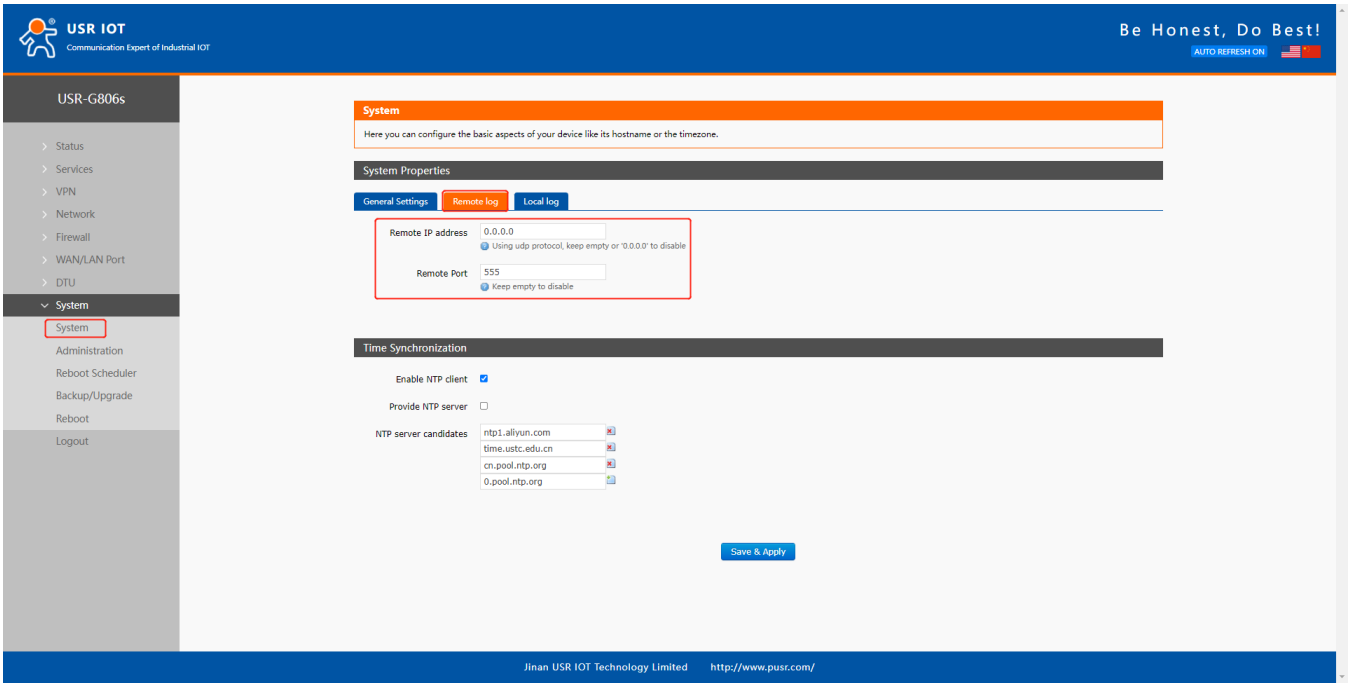
Users can restart the router at any time every day, every week and every month, and clear the running cache regularly to improve the running stability.



2.11. Log

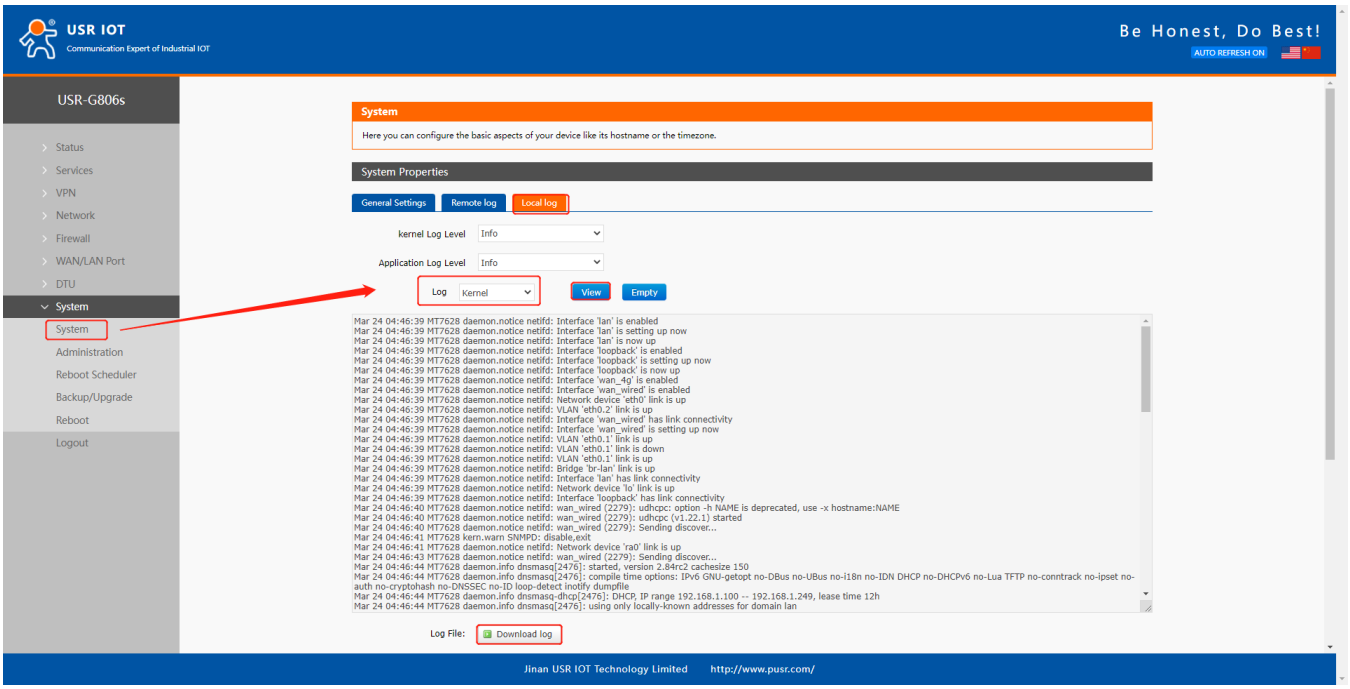
2.11.1. Remote Log

- Remote IP address: Remote UDP server IP/domain name, this function is disabled when the IP is 0.0.0.0.
- Remote port: Remote UDP server port.



2.11.2. Local Log

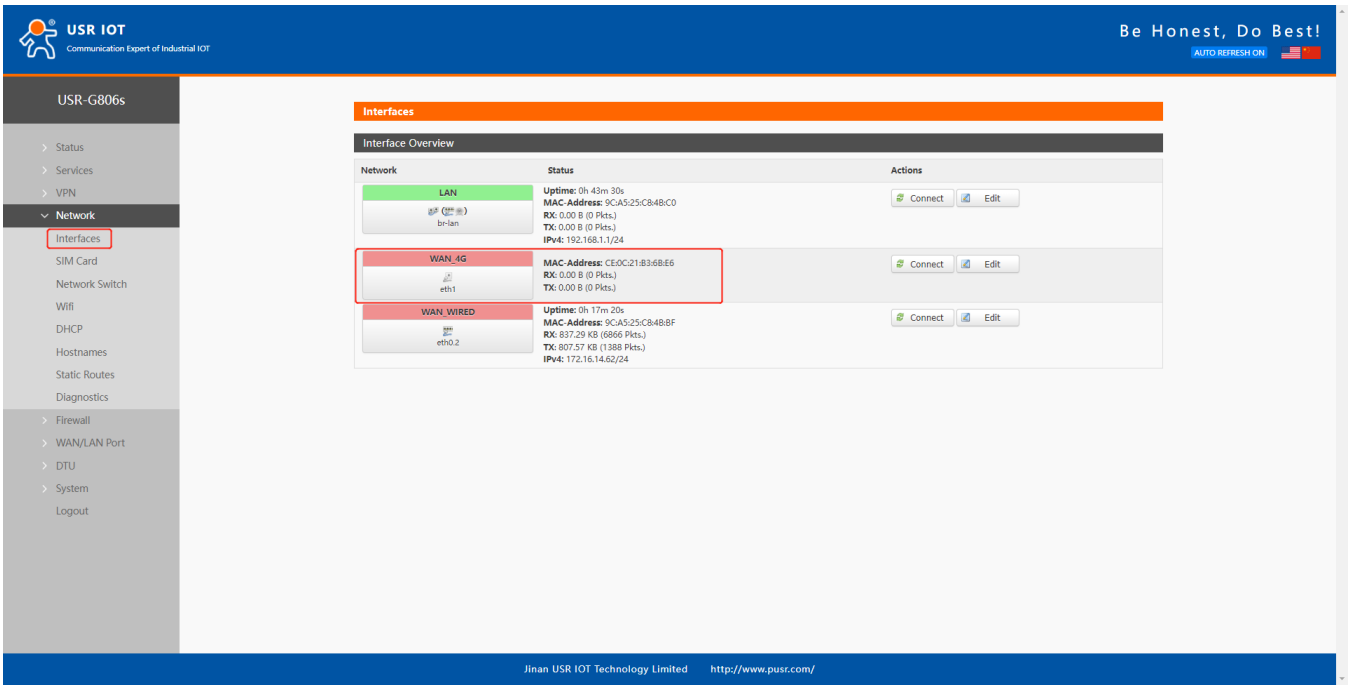
We can view and download the router logs from below interface.



3. Interface

3.1. 4G Interface

USR-G806s supports one 4G/3G/2G interface to access the external network.



For the interface status, if the uptime is 0, means the network card is not running normally.

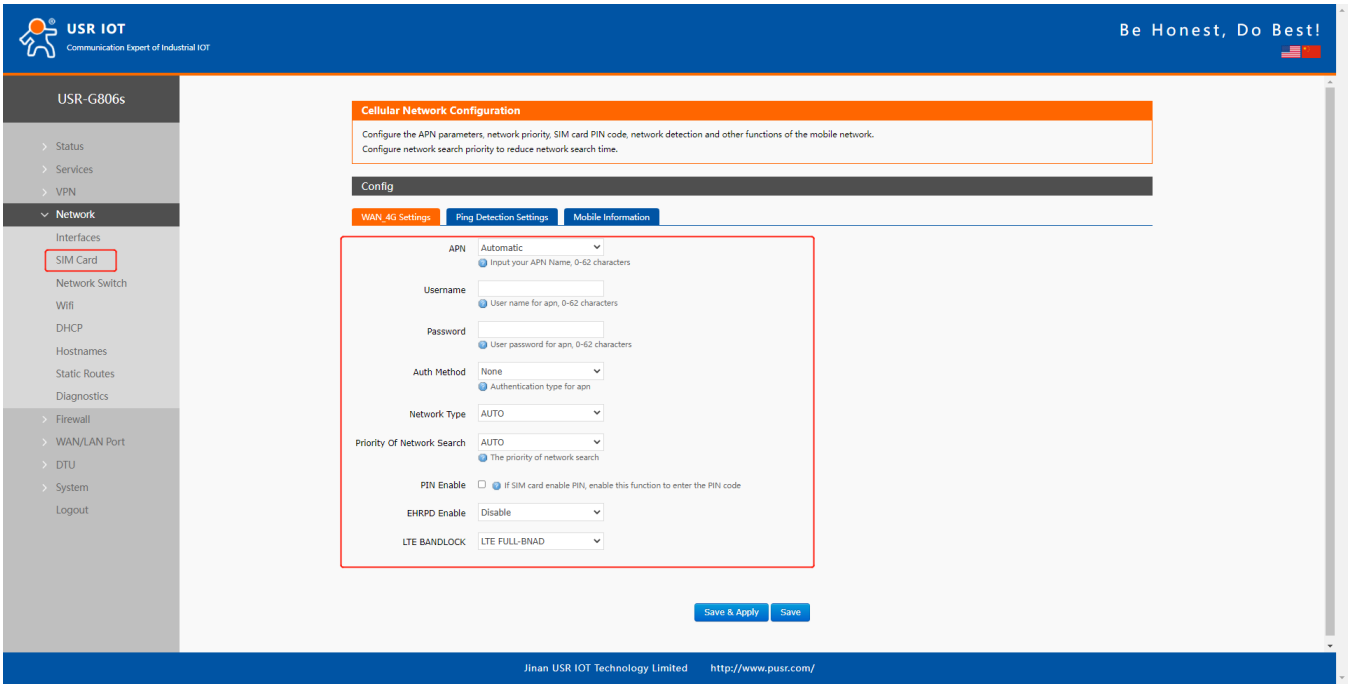
No.	Item	Description
1	Uptime	Time of this interface connected to the network.
2	MAC	MAC address of this interface.
3	RX/TX	Data received and sent of the this interface after connecting to the network.
4	IPv4	Indicates this interface use the IPV4 protocol.

Note: Network priority: Wired WAN>4G.

3.2. SIM Card

3.2.1. APN Settings

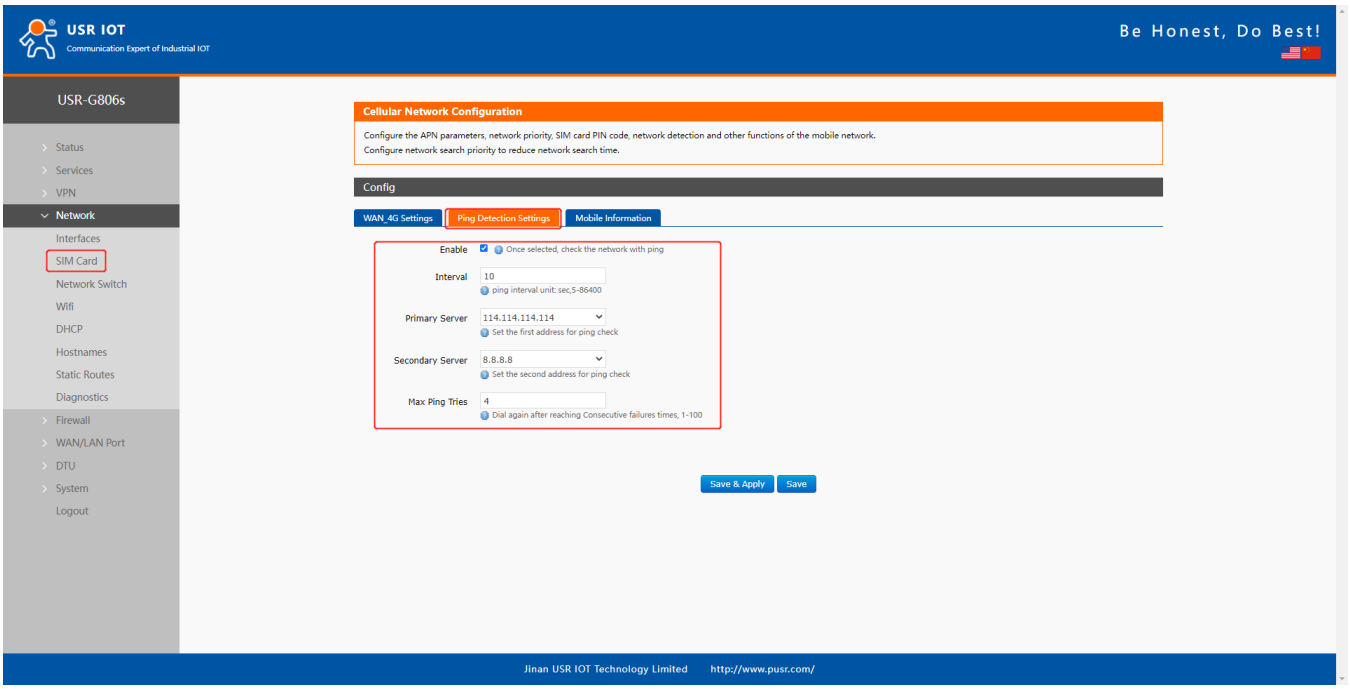
Please set the APN parameters here if the device cannot connect to the network automatically. After setting all parameters, restart the device to take effect.



Item	Description	Default
APN	Please set the correct APN address.	Autocheck
Username	APN username	None
Password	APN password	None
Auth Method	APN authentication type: None/PAP/CHAP	None
Network Type	AUTO/2G/3G/4G	AUTO
Priority of network search	Can set the priority of the network, AUTO/2G/3G/4G	AUTO
PIN Enable	Enable: Fill in the pin code of the SIM card.	Disable
EHRPD Enable	Enable/Disable, enable when there is 3.5G network	Disable
LTE BANDLOCK	LTE FULL-BAND or LTE-TDD	LTE FULL-BAND

3.2.2. Ping Detection Settings

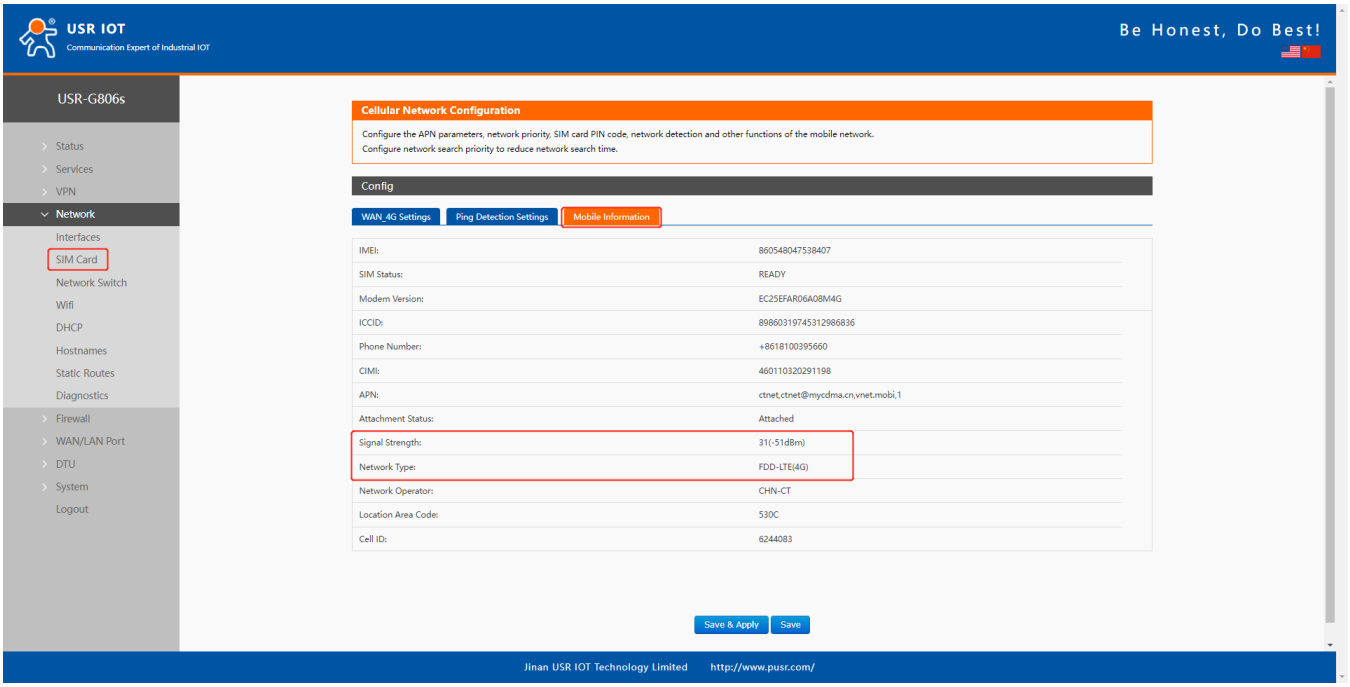
Ping detection is used to check the network status of the device, defaults to be disabled. After enable this function, the device will try to ping the set address, dial again after reaching consecutive failures times.



Item	Description	Default
Enable	/	/
Interval	Ping time interval, 5-86400s	10
Primary Server	Ping detection address: IP/domain name	114.114.114.114
Secondary Server	Ping detection address: IP/domain name	8.8.8.8
Max Ping Tries	Dial again after reaching consecutive failures times, 1-100	4

3.2.3. Mobile Information

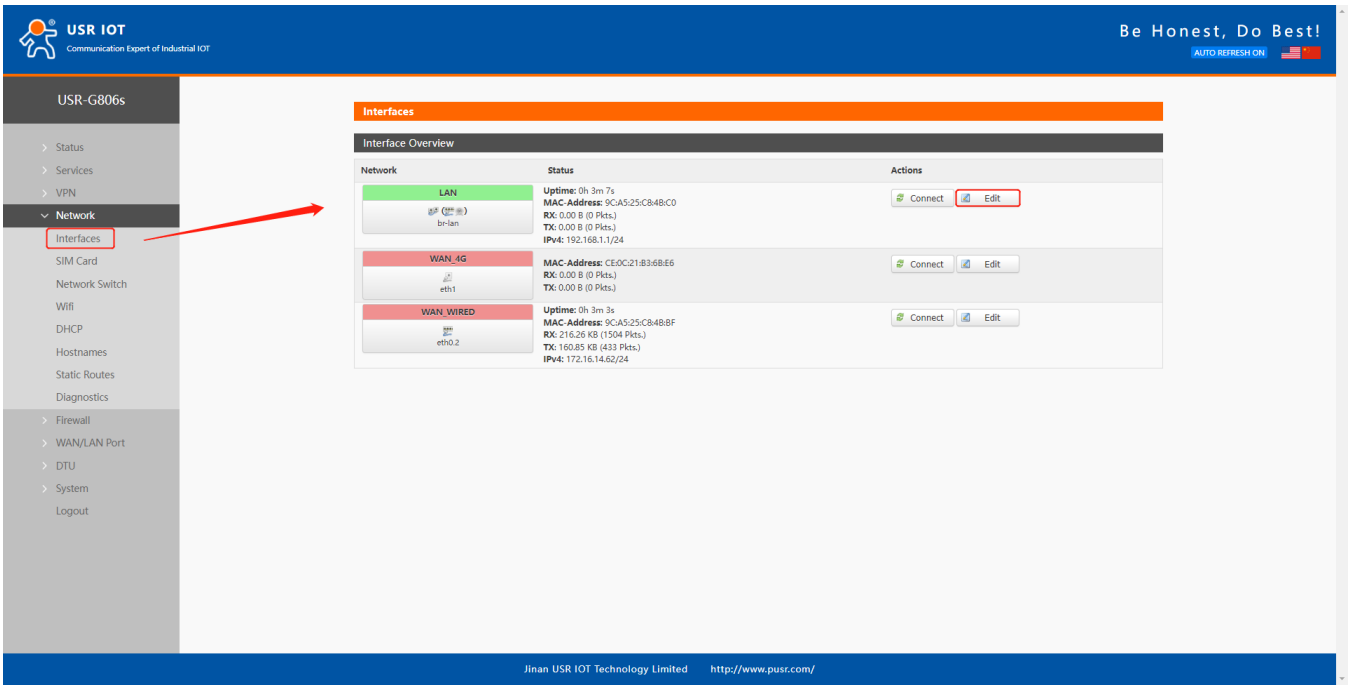
Users can check the detailed configuration information of the SIM card.

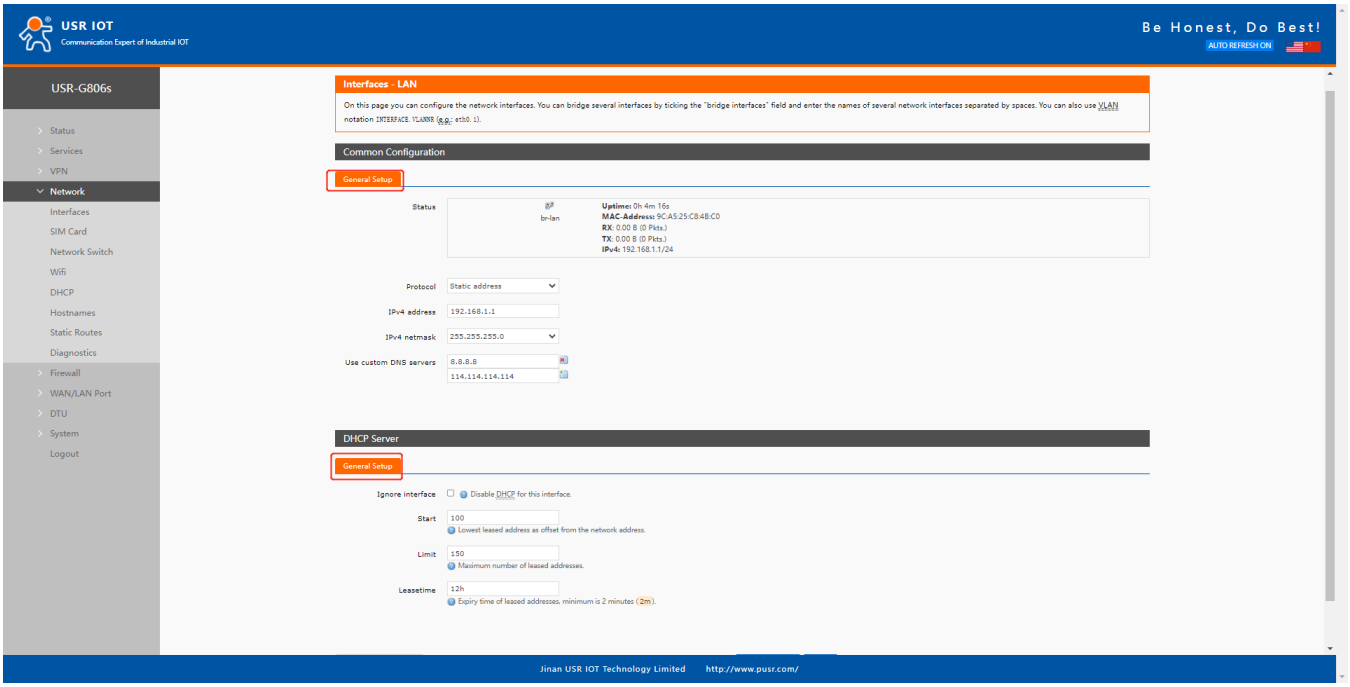


Description:

- Unit of the signal strength is dBm and asu. dBm=-113+2*asu.
- USR-G806s supports display via asu, asu ranges from 1 to 31, and the higher the value, the better the signal strength.
- In general, dBm≥-90dBm, ASU ≥12, the signal is normal.

3.3. LAN Interface



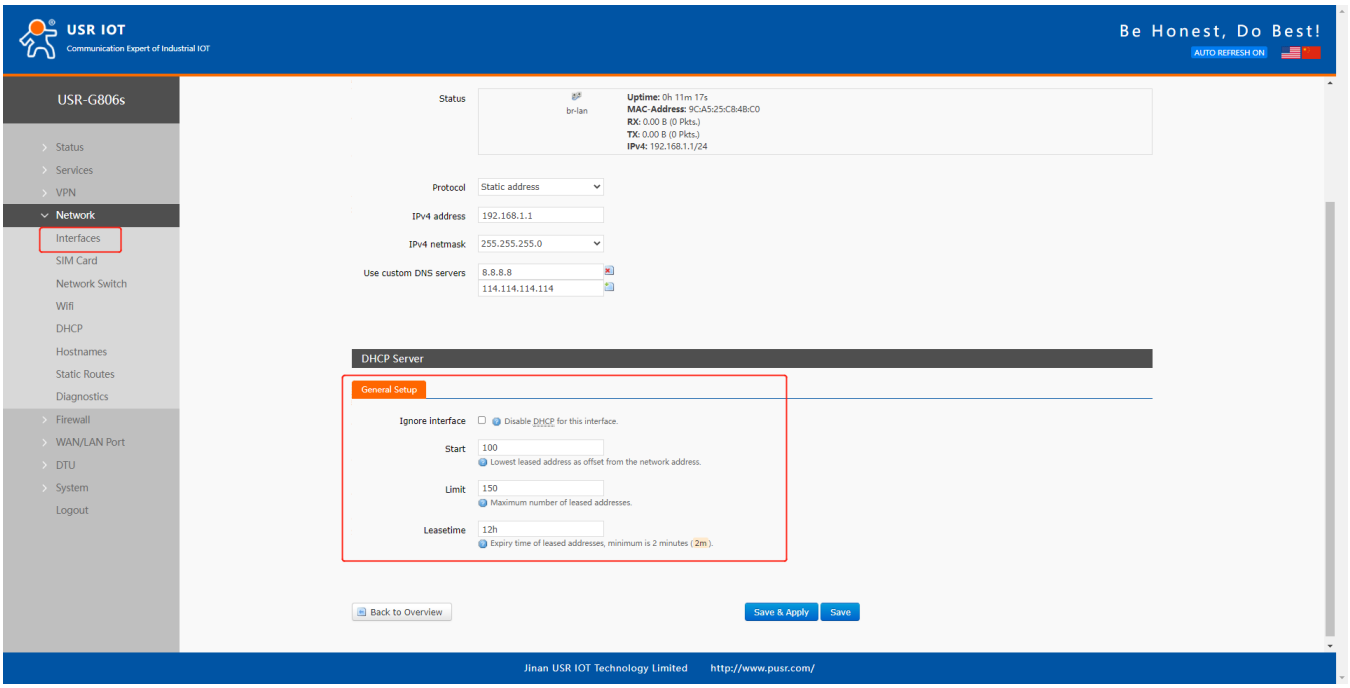


Descriptions:

- LAN interface defaults to the static IP address 192.168.1.1 and netmask 255.255.255.0. These parameters can be modified.
- WiFi interface (WLAN) and wired LAN are in the same lan network.

3.3.1. DHCP

DHCP server function is default to be enabled, all the devices connect to the LAN port will get IP address automatically.

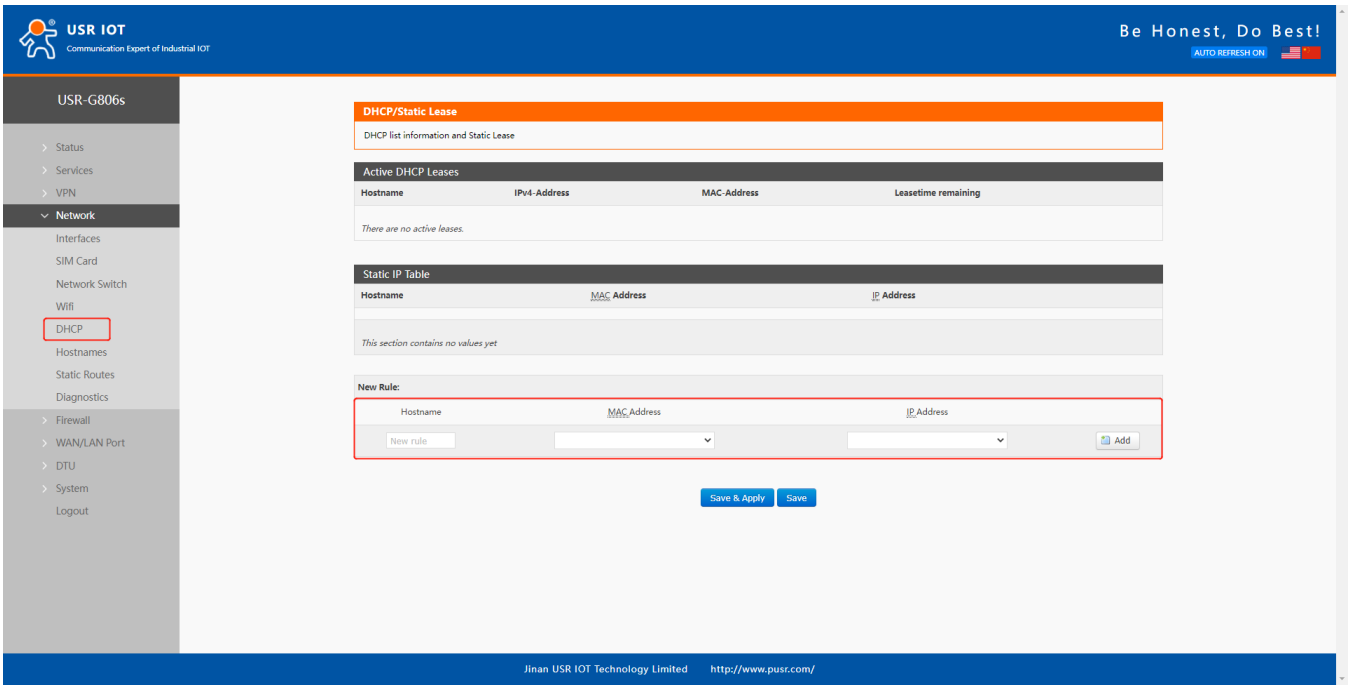


Descriptions:

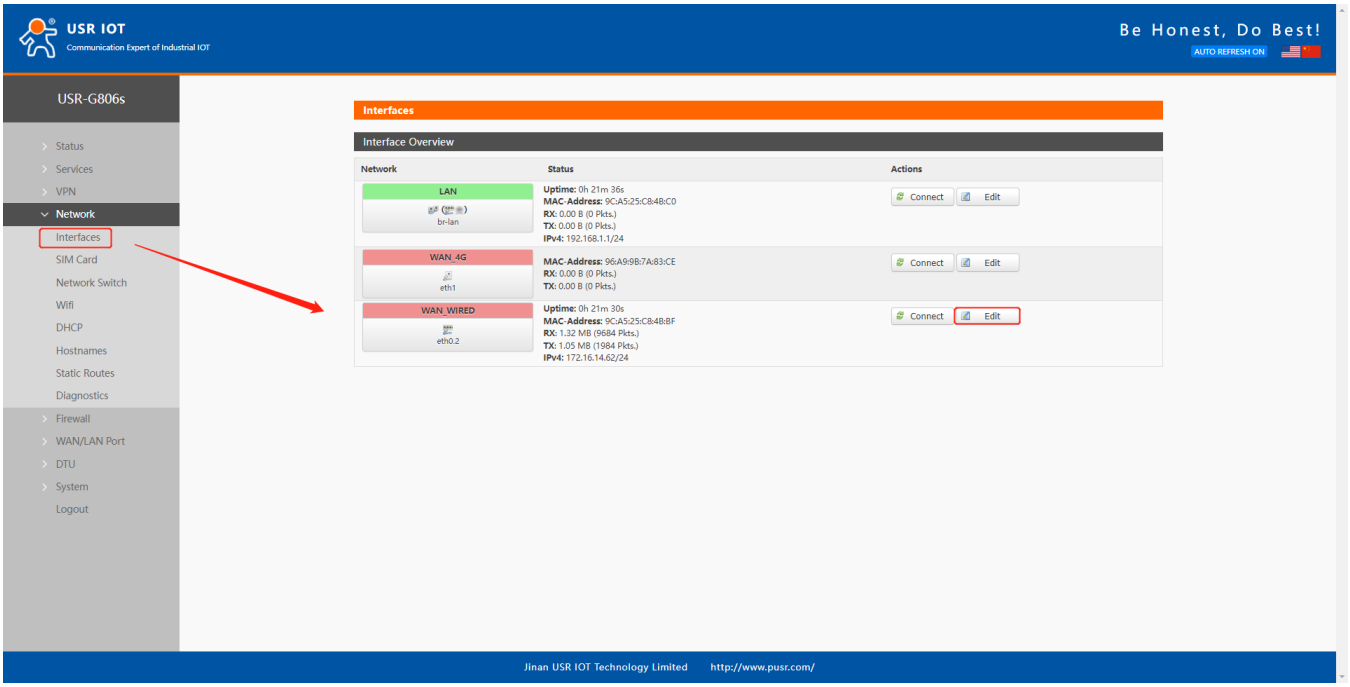
- We can change the start address and leased time of the DHCP Client.
- DHCP addresses are default to be assigned from 192.168.1.100.
- Default lease time is 12 hours.

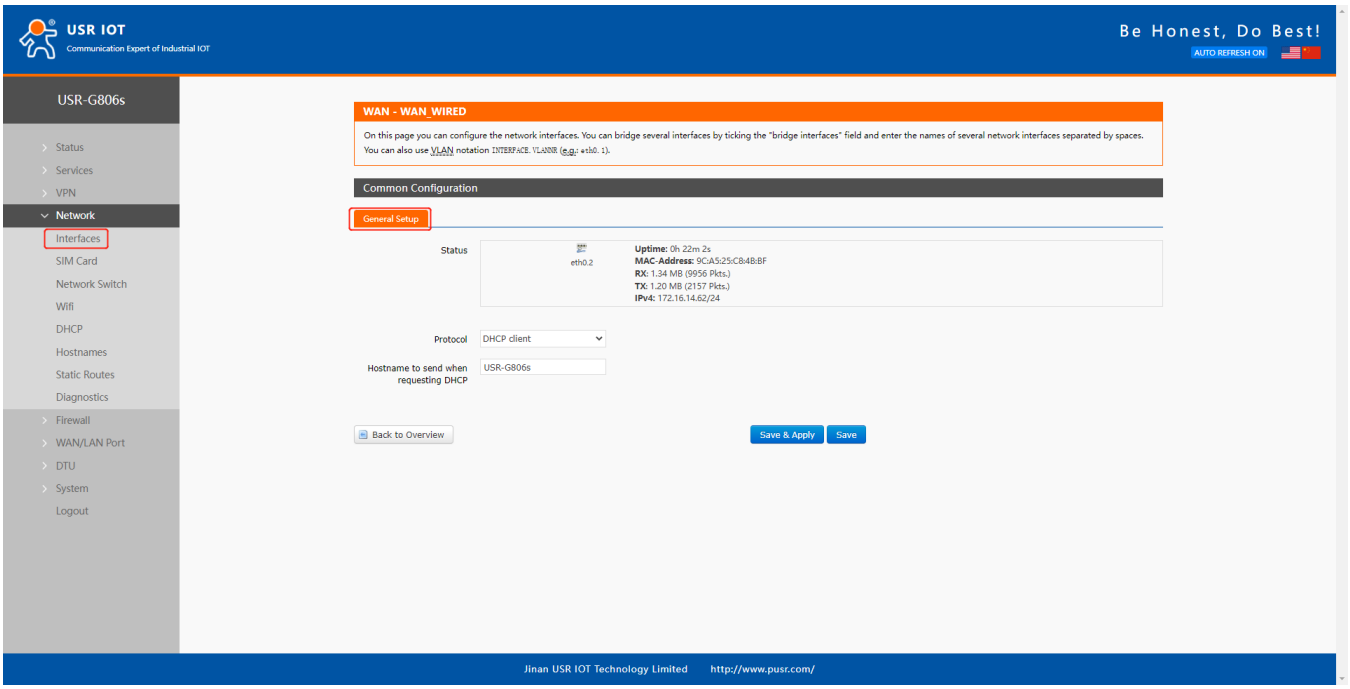
3.3.2. Static IP

In **Network--DHCP**, we can assign a fixed IP address and hostname to a DHCP Client device. Only the specific client can be connected and the LAN interface mode cannot be DHCP.



3.4. WAN Interface



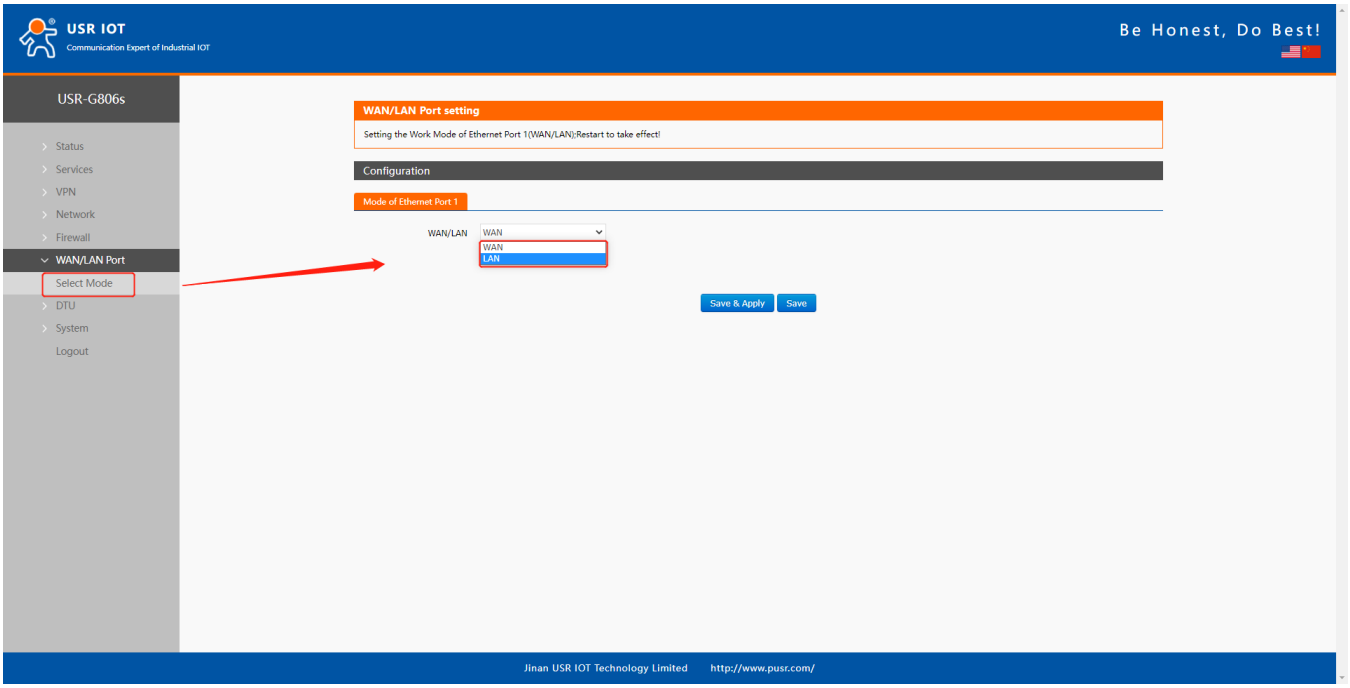


Descriptions:

- 1 wired WAN interface, WAN is a wide area network interface.
- Supports DHCP Client, static address and PPPoE, defaults to DHCP Client.
- This WAN interface can be configured to LAN.

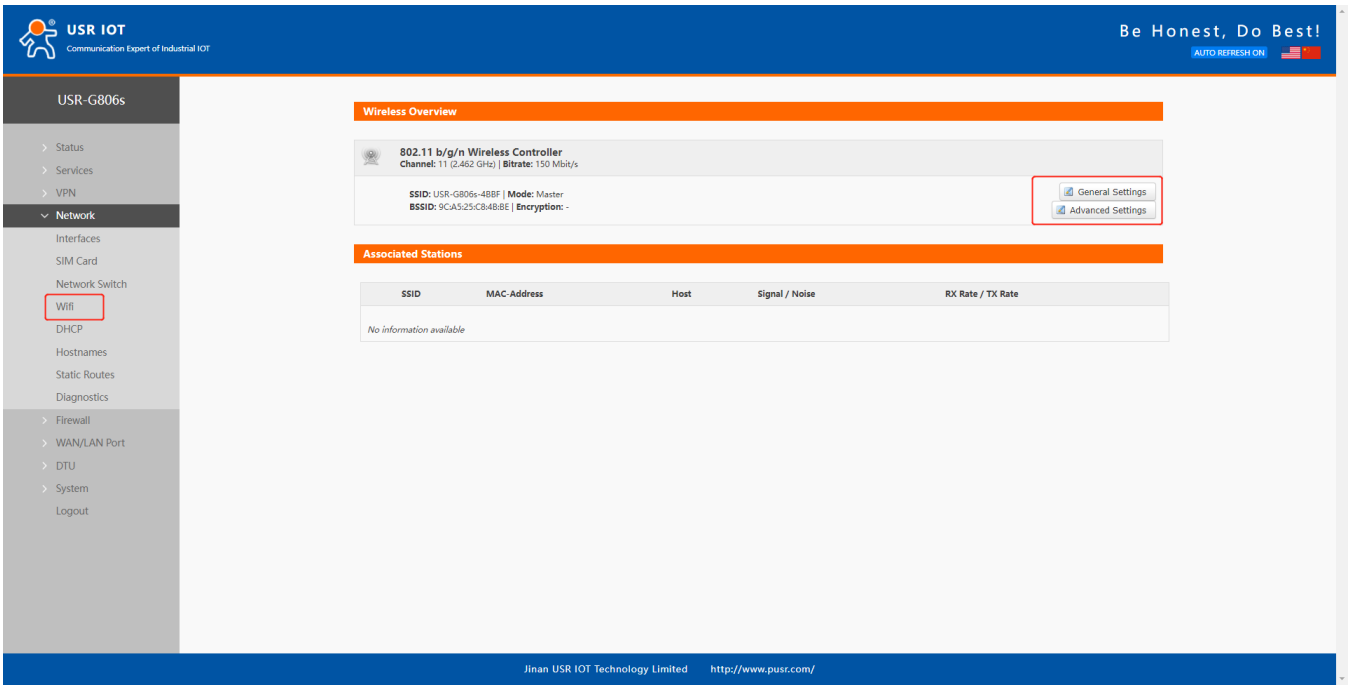
3.5. WAN/LAN Mode Selection

In **WAN/LAN Port--Select Mode**, you can change the WAN port to LAN. After changing it, click **Save&Apply**, then restart the device to take the parameters effect.



3.6. WiFi Interface

USR-G806s supports WiFi-AP function, 2.4GHz WiFi network. Users can modify the WiFi parameters in below interface.

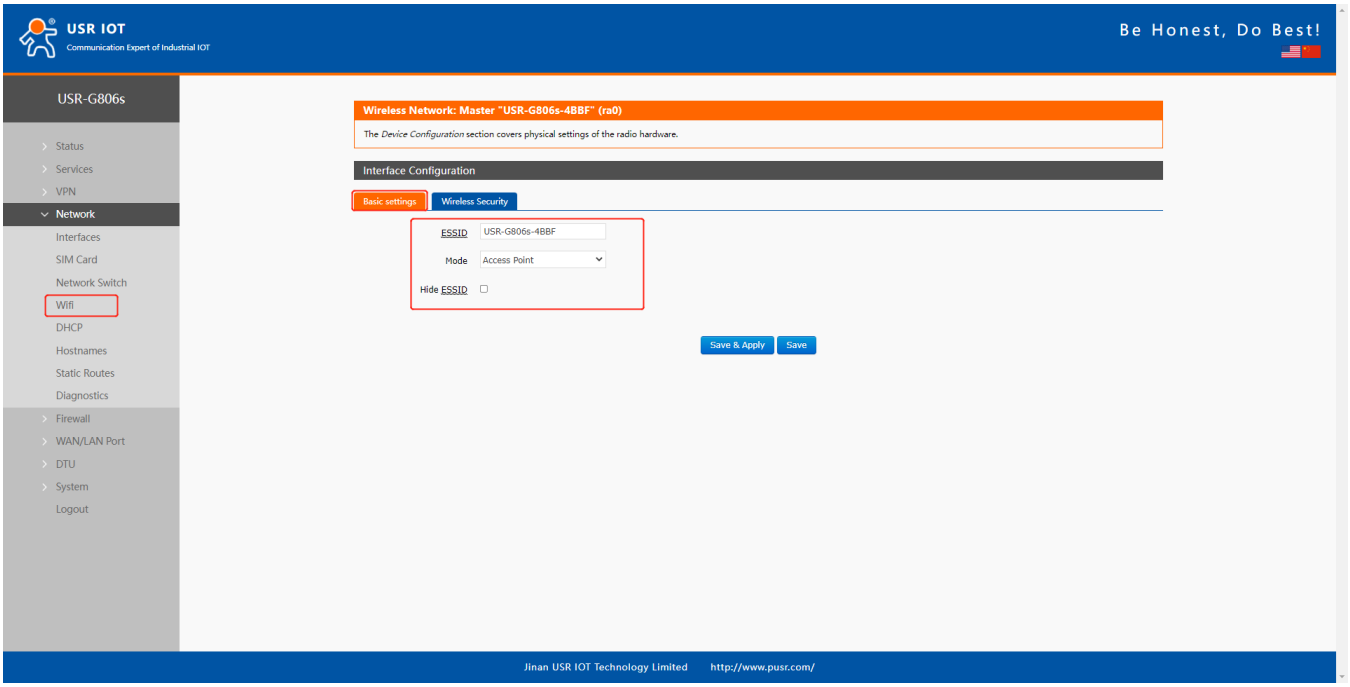


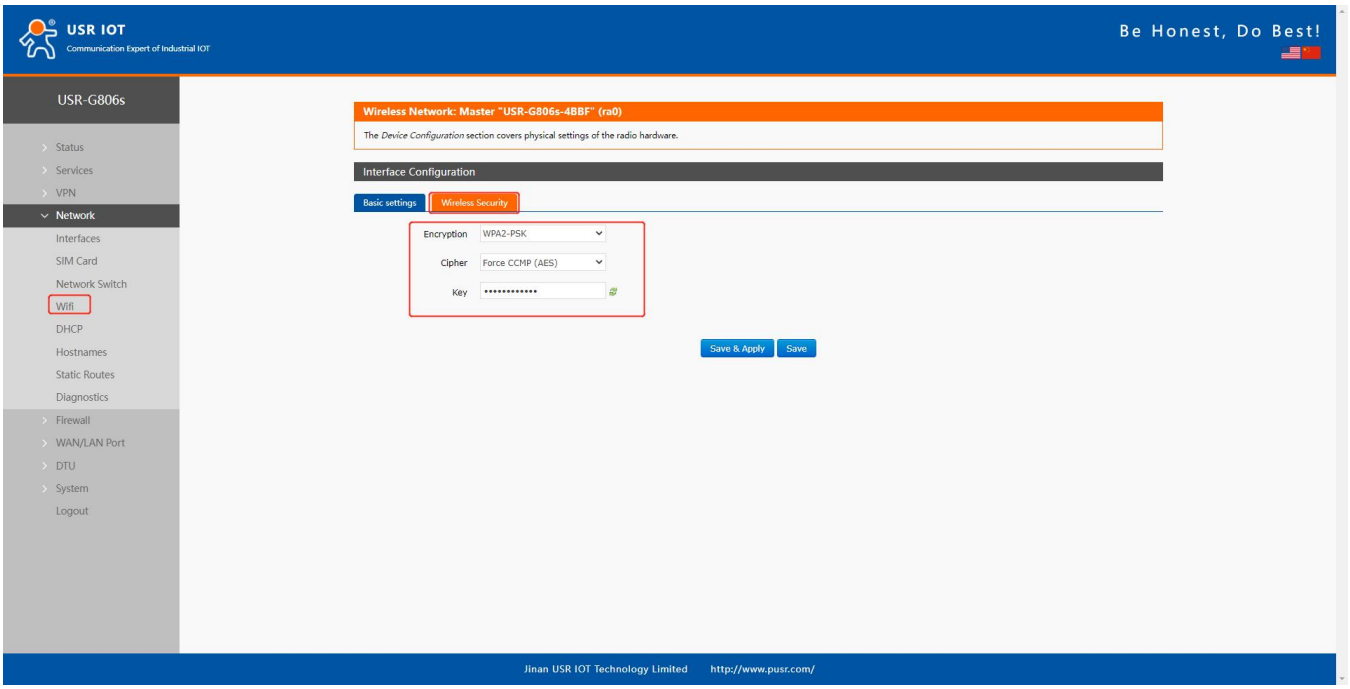
Descriptions:

- USR-G806s is an access point, other station devices can connect to its WiFi.
- It supports up to 24 WiFi stations.
- The maximum WiFi range is 100m in open area, and within 50m in the office with obstacles.

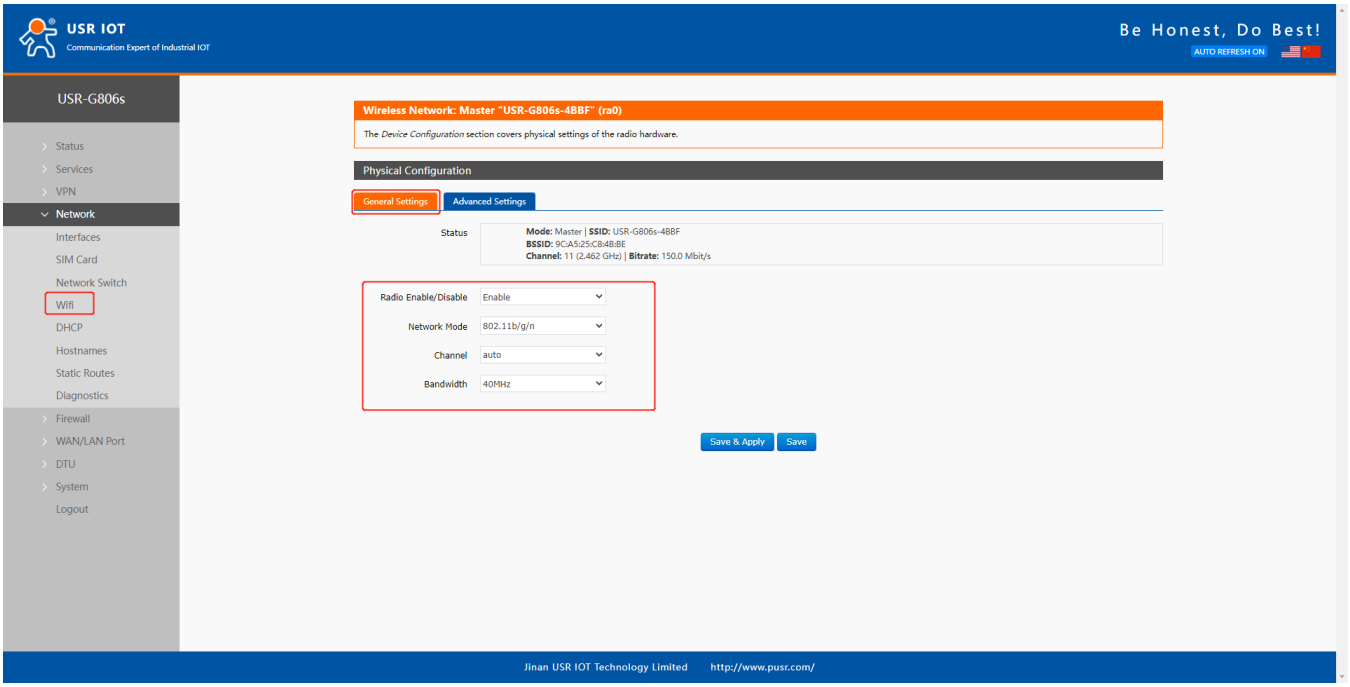
Item	Description	Default
ESSID	Network name of the WiFi, can be modified.	USR-G806s-8899 (8899=the last 4 bits of the MAC)
Mode	Access Point	AP
Hide ESSID	Enable: None of client could scan the SSID. If you want to connect to the router AP, must enter the ESSID at WiFi client side manually. Disable: Enable the SSID broadcasting. So that the client can scan the SSID.	Disable
Encryption	WPA2-PSK/WPA-PSK/No Encryption	WPA2-PSK
Cipher	CCMP/TKIP/CCMP&TKIP	CCMP
Key	WiFi password, can be modified.	www.pusr.com
Radio Enable/Disable	Enable: open WiFi radio, AP can be used. Disable: close WiFi radio, AP cannot be used, “WLAN” indicator light will be off.	Enable
Network Mode	802.11b/g/n	802.11b/g/n
Channel	Auto, can be selected.	Auto
Bandwidth	40MHz/20MHz	40MHz
Regions	Optional	none
Channel	Optional	CH1~11

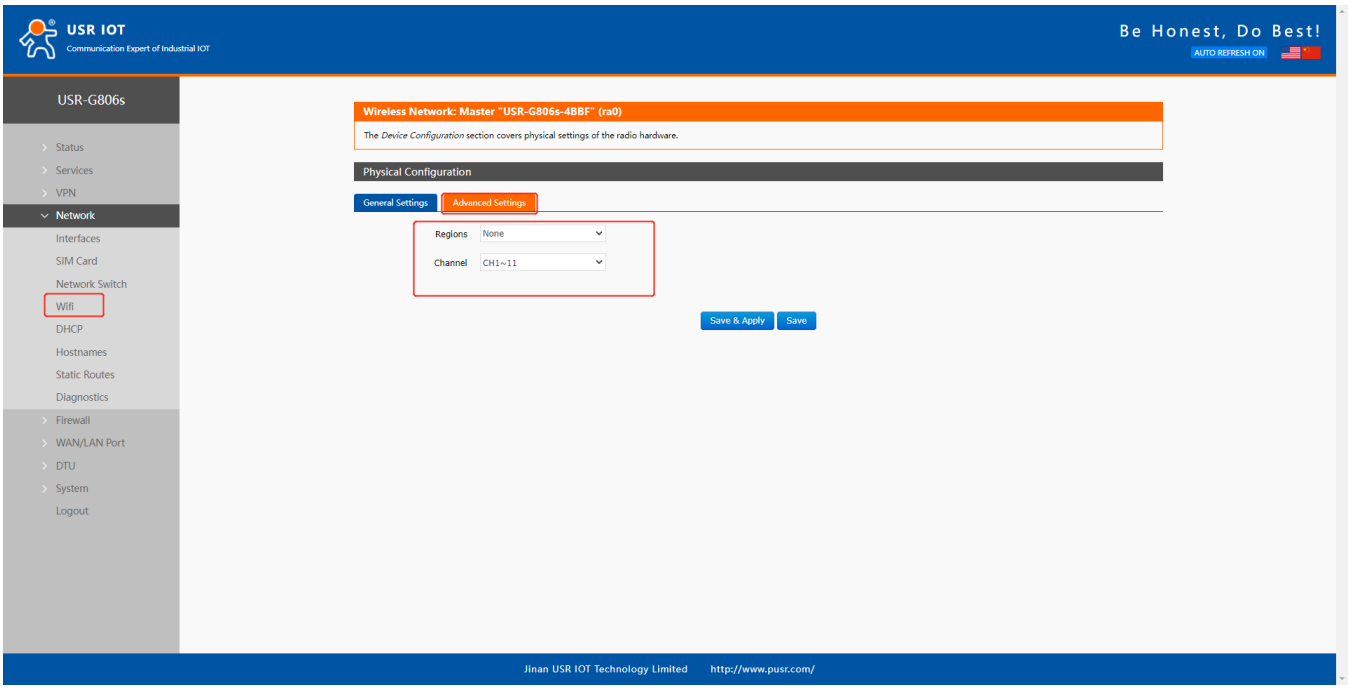
In **WiFi--General Settings**, we can change the WiFi SSID and password.



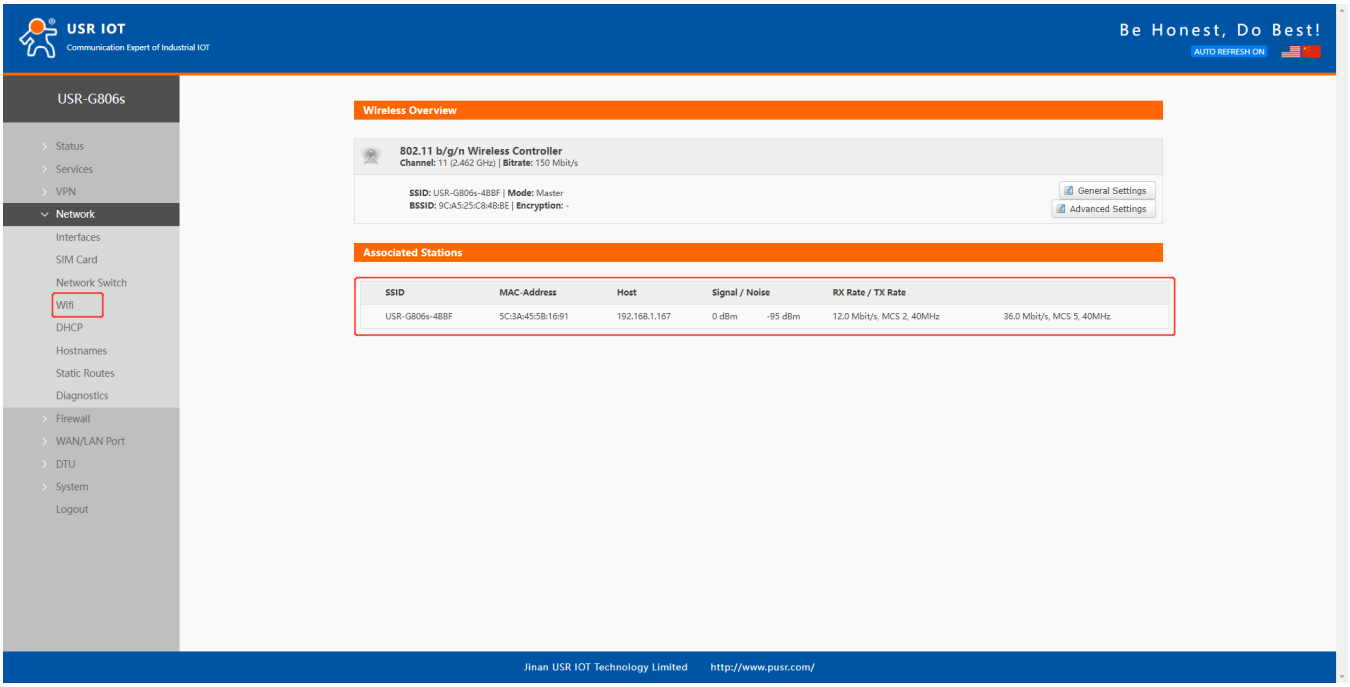


In **WiFi--Advanced Settings**, we can enable/disable WiFi radio.

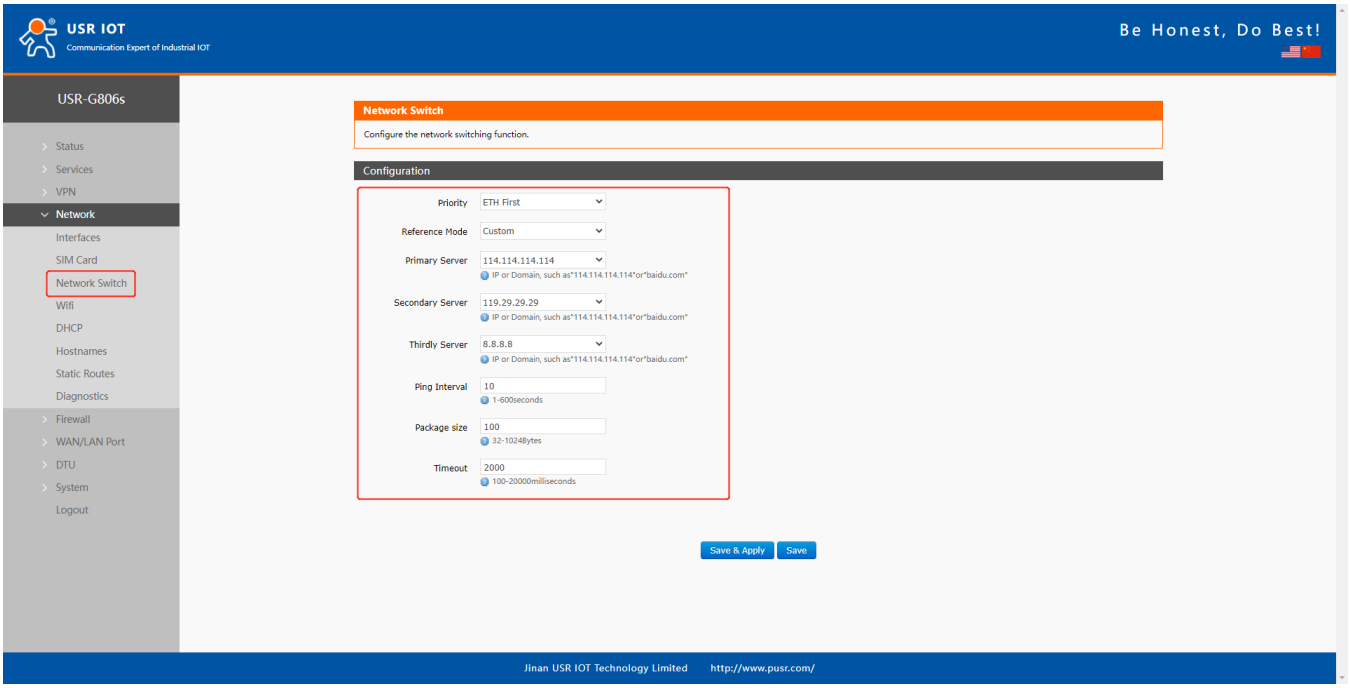




We can check the WiFi client information in below interface:



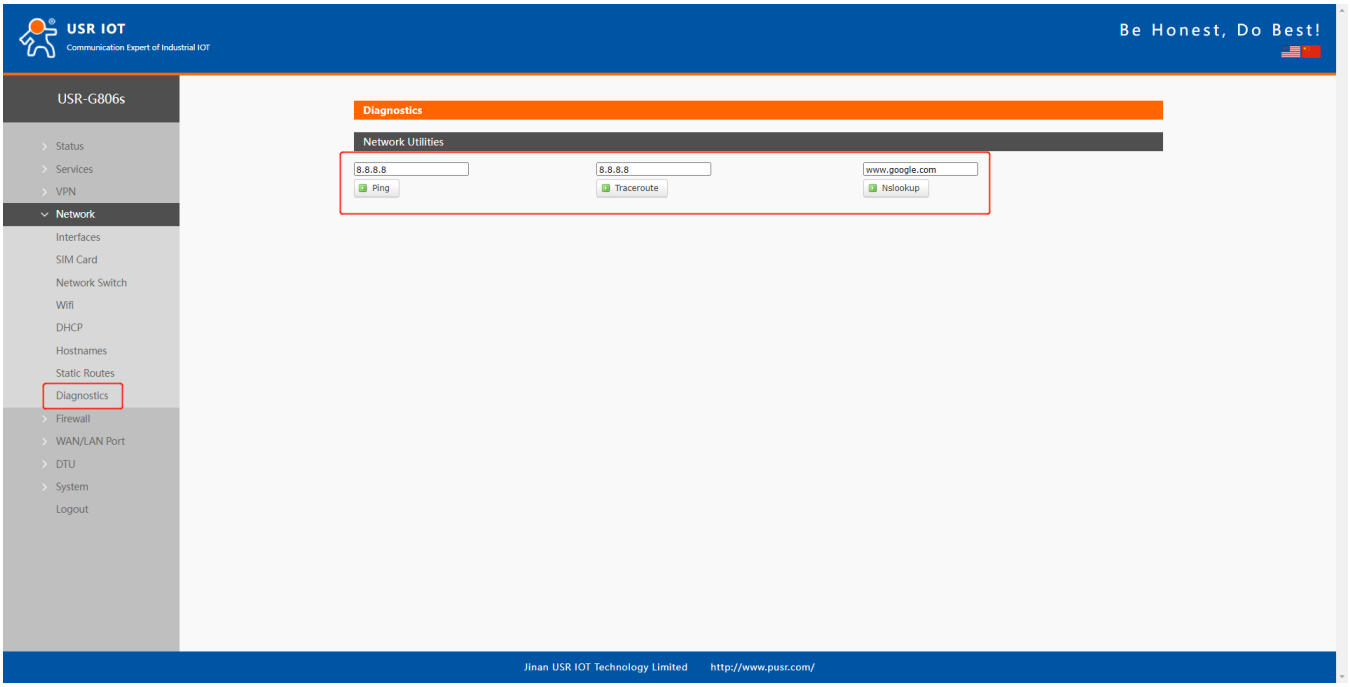
3.7. Network Switch



Item	Description	Default
Priority	ETH First: Select to make WAN Ethernet port as the primary link. 4G First: Select to make SIM card as the primary wireless link. Disable: disable network switch function, access the network with current link.	ETH First
Reference Mode	Custom: Router will ping the custom reference address/domain name to check that if the current connectivity is active. Gateway: Router will ping the gateway to check if the current connectivity is active.	Custom
Primary Server	IP address/domain name	114.114.114.114
Secondary Server	IP address/domain name	119.29.29.29
Thirdly Server	IP address/domain name	8.8.8.8
Ping interval (s)	Set the ping interval, 1-600s.	10
Package size(byte)	Set the ping package size, 32-1024 bytes.	100
Timeout (ms)	Ping timeout, 100-20000ms	2000

Descriptions: If all of these three IP addresses/domain name cannot be pinged, then the device will change the network connection and continue to perform the next circle of ping detection.

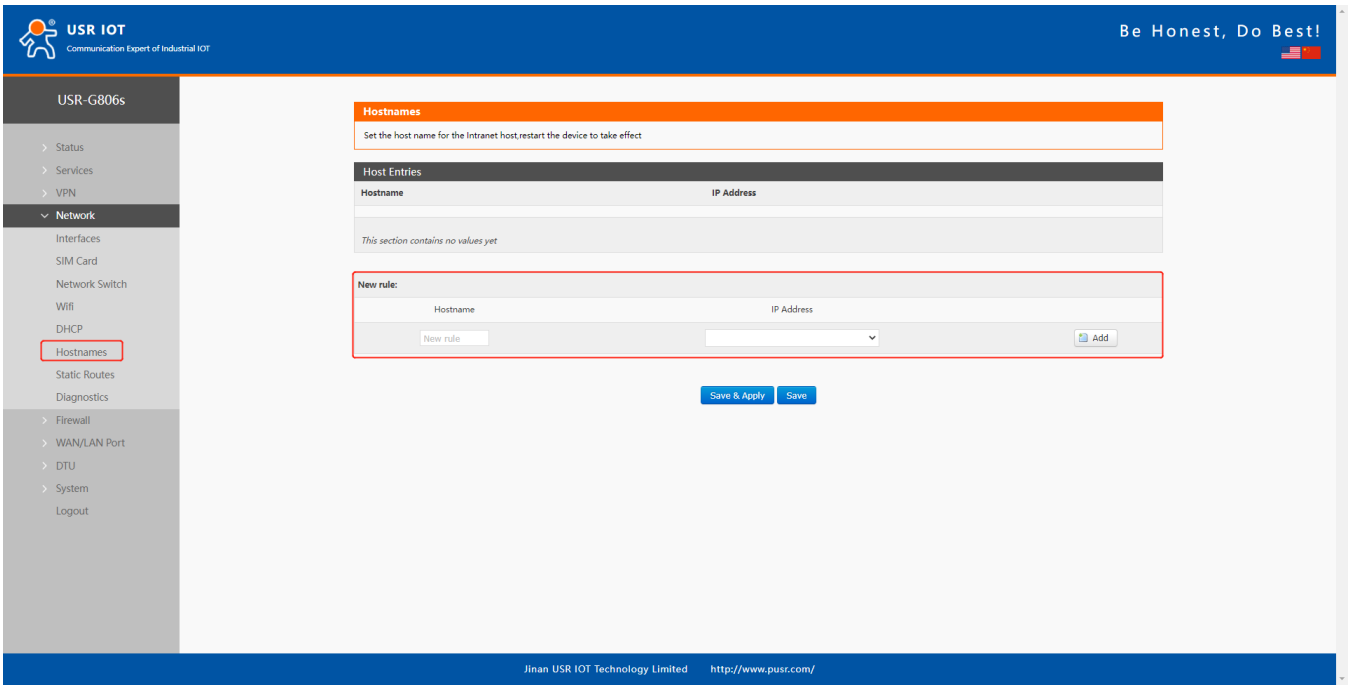
3.8. Diagnostics



This interface provides users three tools: Ping, Traceroute and Nslookup.

- Ping: Ping a destination address to check the network status.
- Traceroute: Send traceroute request to a destination address.
- Nslookup: Resolve the domain name to an IP address.

3.9. Hostname



USR-G806s supports custom domain name resolution. Set the hostname and IP address in below interface, to achieve the mapping between hostname and IP address.

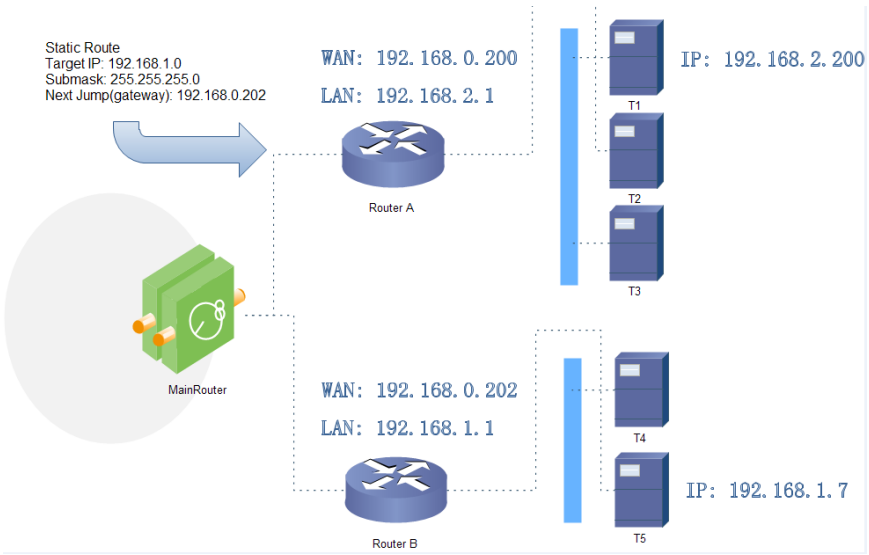
The outside IP address can also be mapped(must be a unique public IP address). The hostname of DHCP and static IP cannot be a number. After setting all parameters, restart the device to take the parameters effect.

3.10. Static Routes

USR-G806s supports up to 20 static route rules.

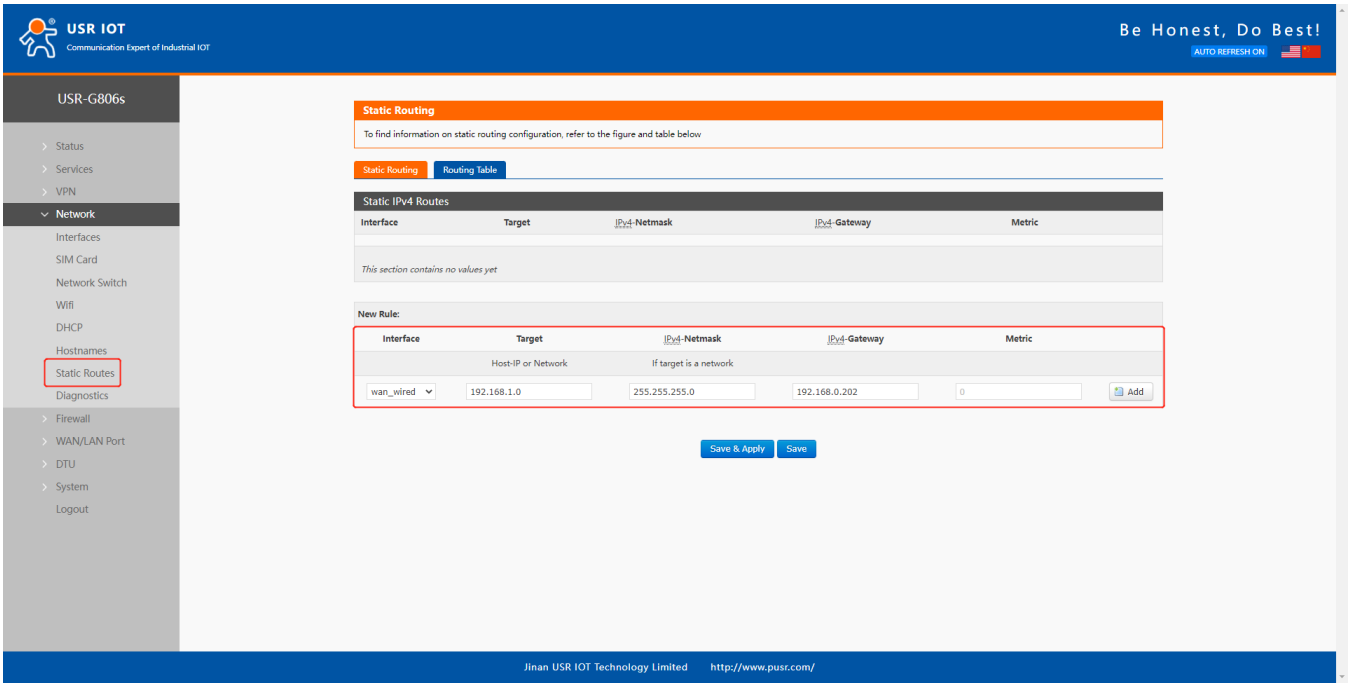
Item	Description	Default
Interface	Lan, wan_4G, wan_wired, vpn	lan
Target	Destination IP address or IP range	Null
Netmask	Netmask of the destination network	Null
Gateway	The IP address to forward to	Null
Metric	Used to make routing decisions	Null

Test example:

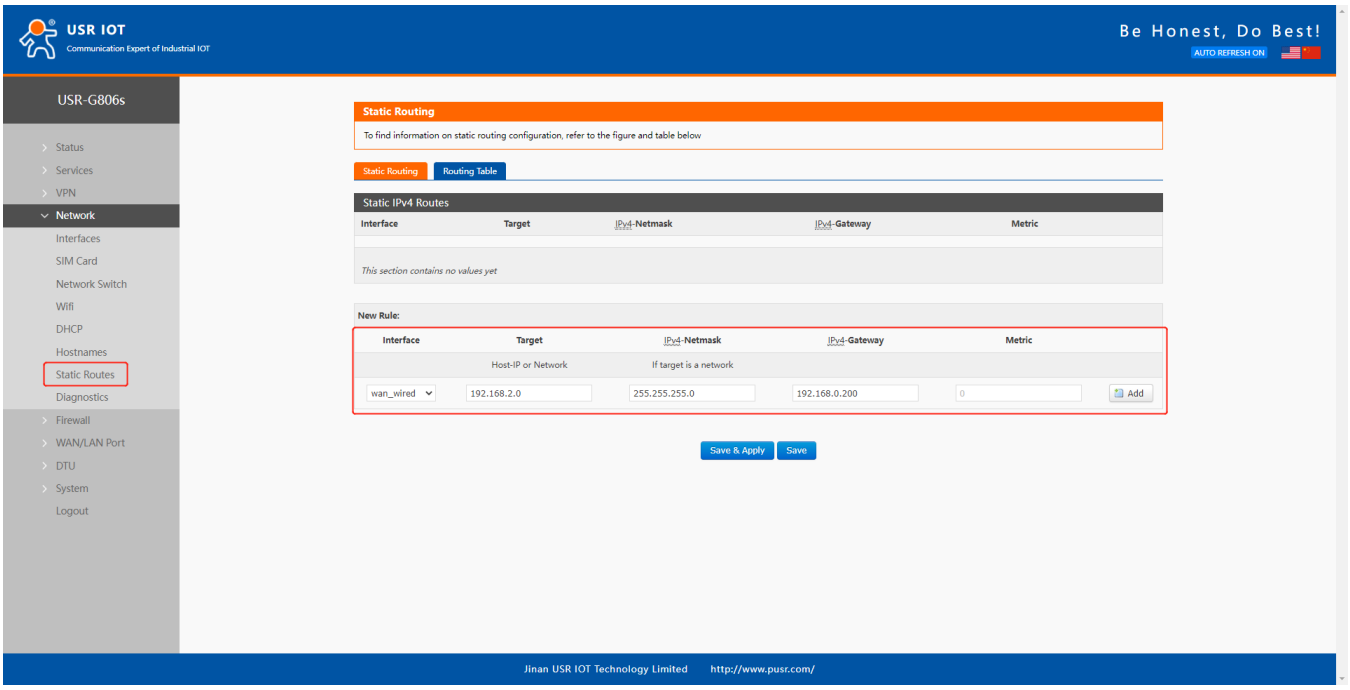


The WAN port of router A and router B are connected to the network 192.168.0.0, LAN network of router A is 192.168.2.0, LAN network of router B is 192.168.1.0.

Now we can do a static route in router A, when we access the 192.168.1.X, will automatically forward to router B.

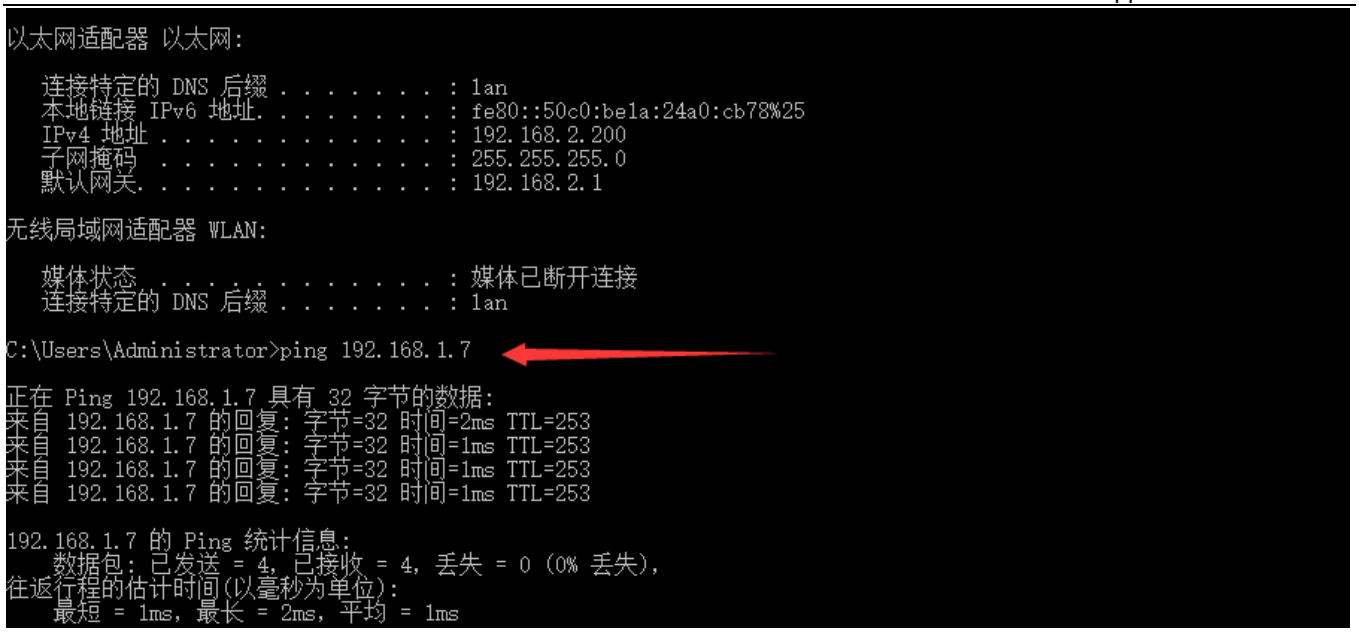


In router B:



After setting all parameters, restart the device.

Ping from T1 to T5:



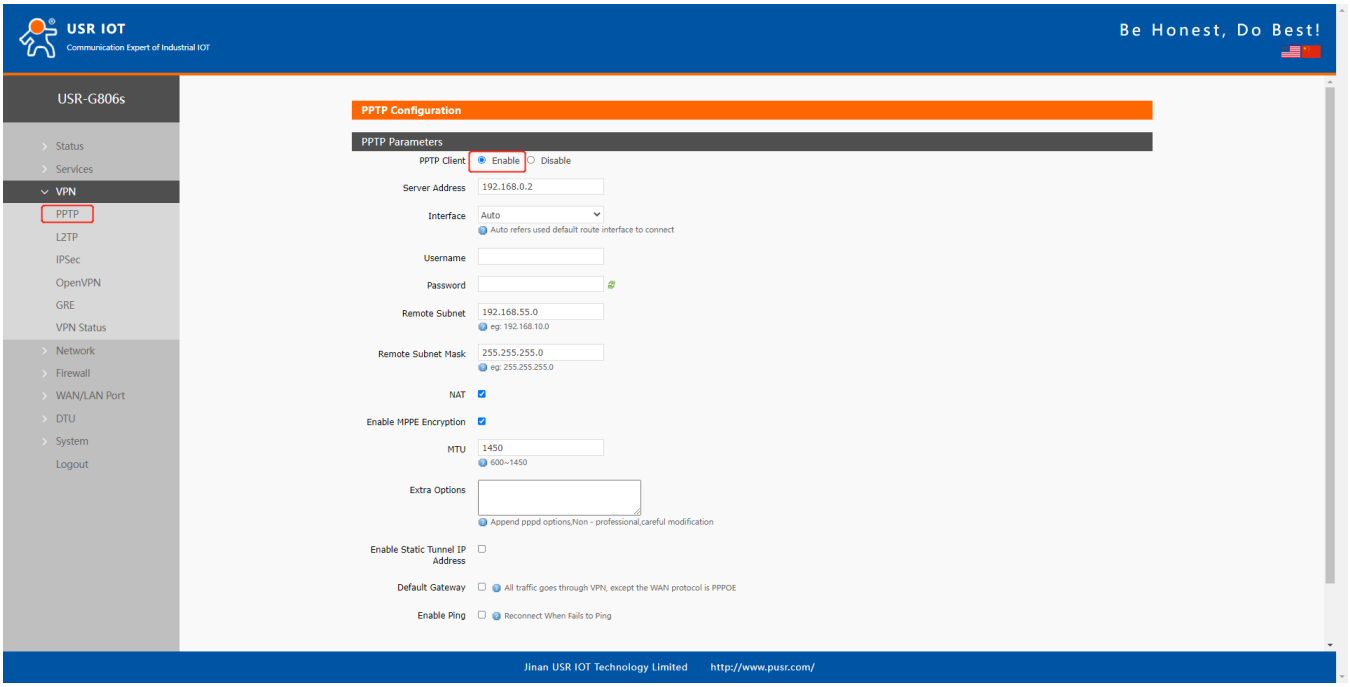
4. VPN

USR-G806s supports PPTP, L2TP, IPSEC, openVPN and GRE.

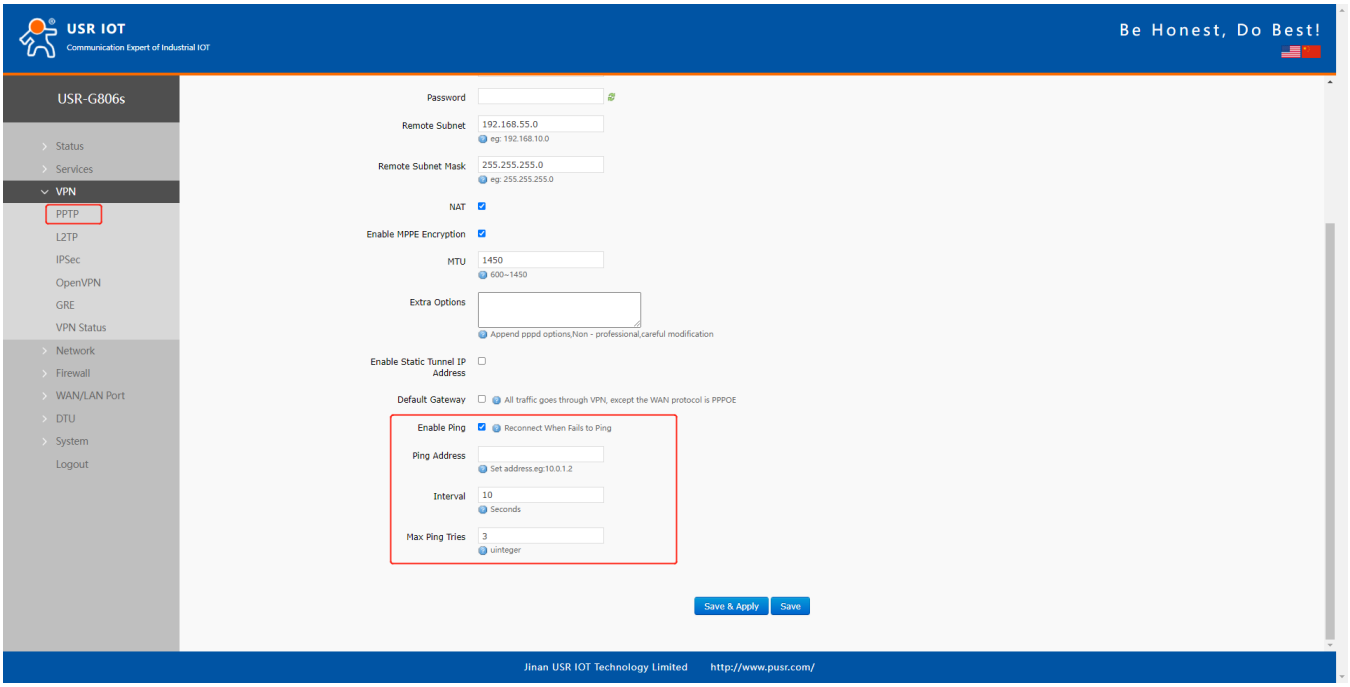
No.	Protocol	Version
1	PPTP	V1.10.0
2	L2TP	V1.3.15
3	IPSec	V5.3.3
4	OpenVPN	V2.3.18

4.1. PPTP Client

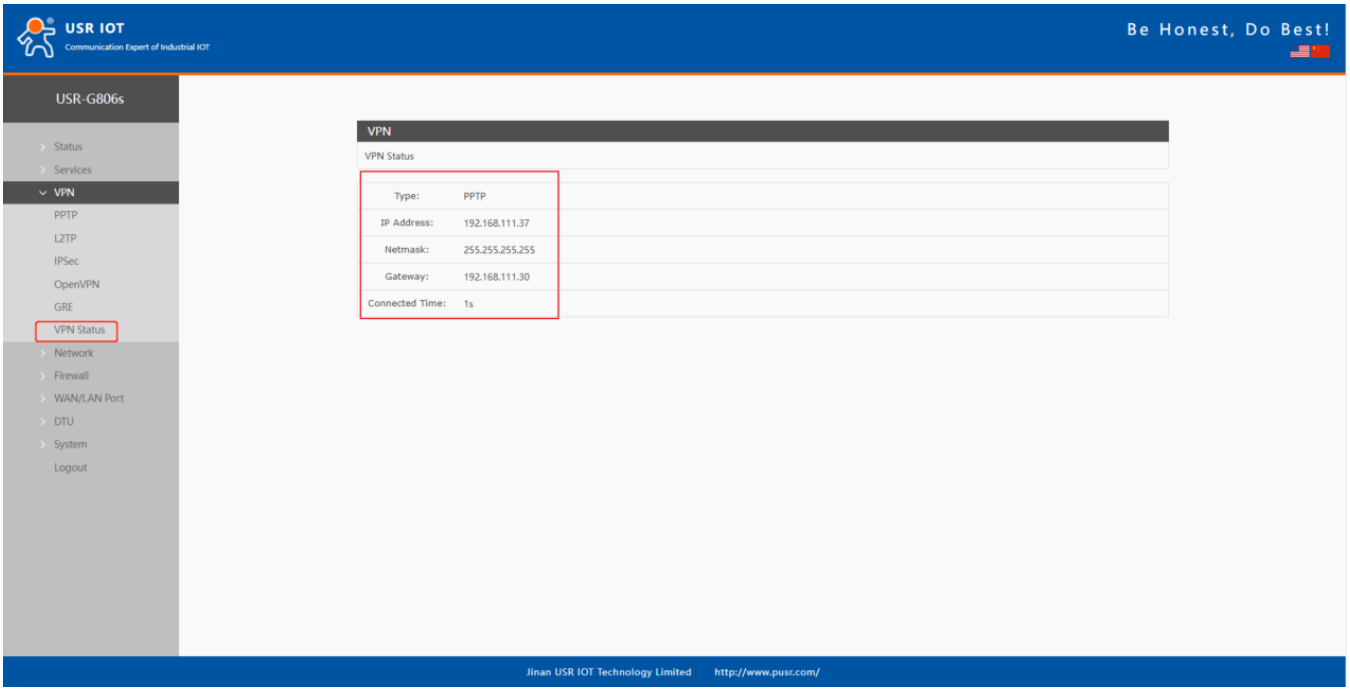
This interface allows users to set the PPTP server parameters.



Item	Description	Default
Server address	VPN server address or domain name	192.168.0.2
Interface	wan_4G, wan_wired or auto	auto
Username/Password	Get from the VPN server	Null
Encryption	MPPE or no encryption	MPPE
MTU	Consistent with the VPN server	1450
NAT	The source IP address of host behind G806s will be disguised before accessing the remote address.	Enable
Remote Subnet/Mask	When NAT is enabled, can achieve the subnet communication under VPN.	192.168.55.0/255.255.255.0
Enable Static Tunnel IP Address	When it is disabled, VPN server will assign an IP address dynamically.	Disable
Extra Options	Append pppd parameters, magic number.	Null
Enable ping	Real-time VPN online detection and reconnection mechanism.	Disable



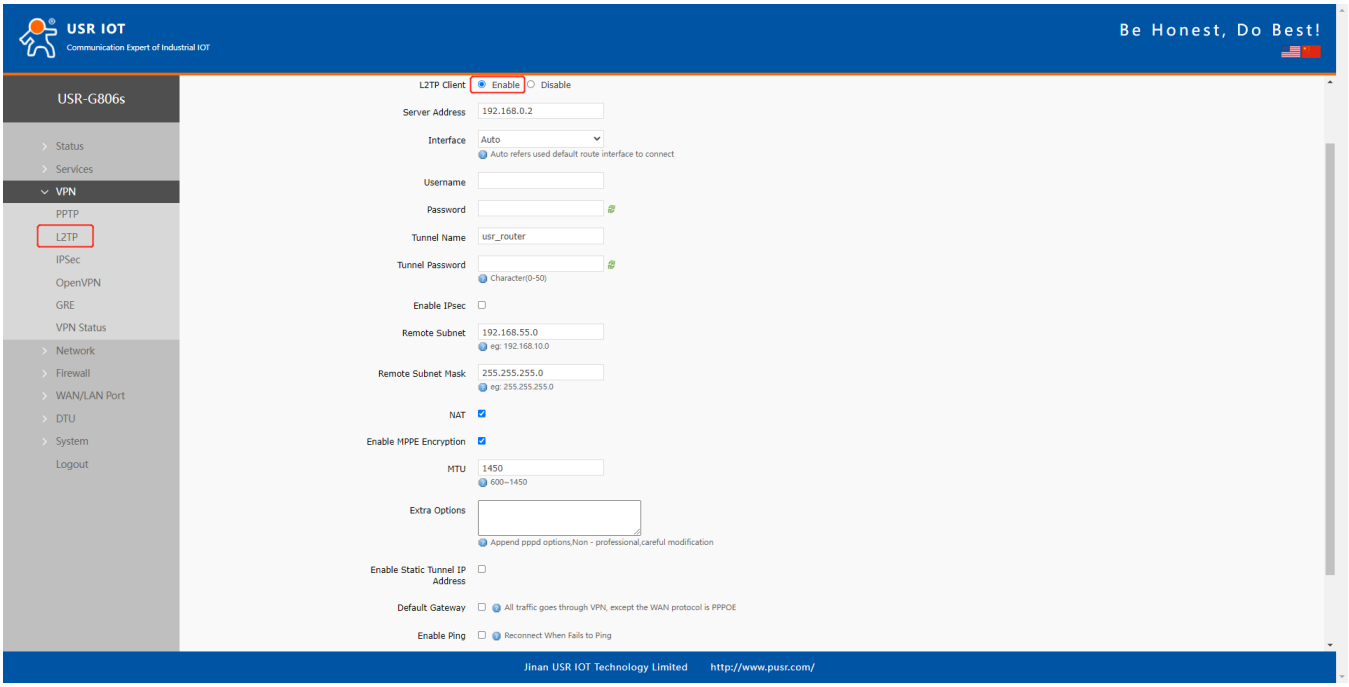
After connecting to PPTP server, we can check the connection status in “VPN Status”.



4.2. L2TP

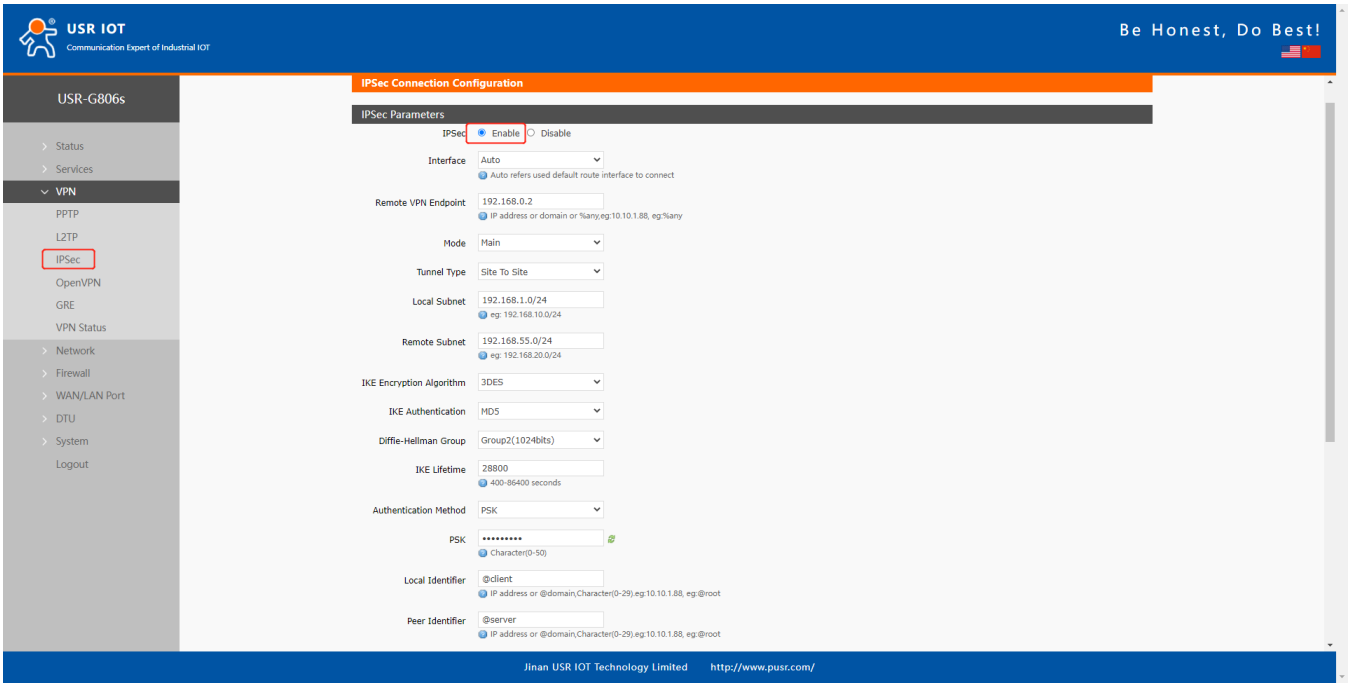
L2TP is the layer 2 tunneling protocol which similar to PPTP. G806s supports tunnel password authentication, supports MPPE and L2TP over IPSEC encryption.

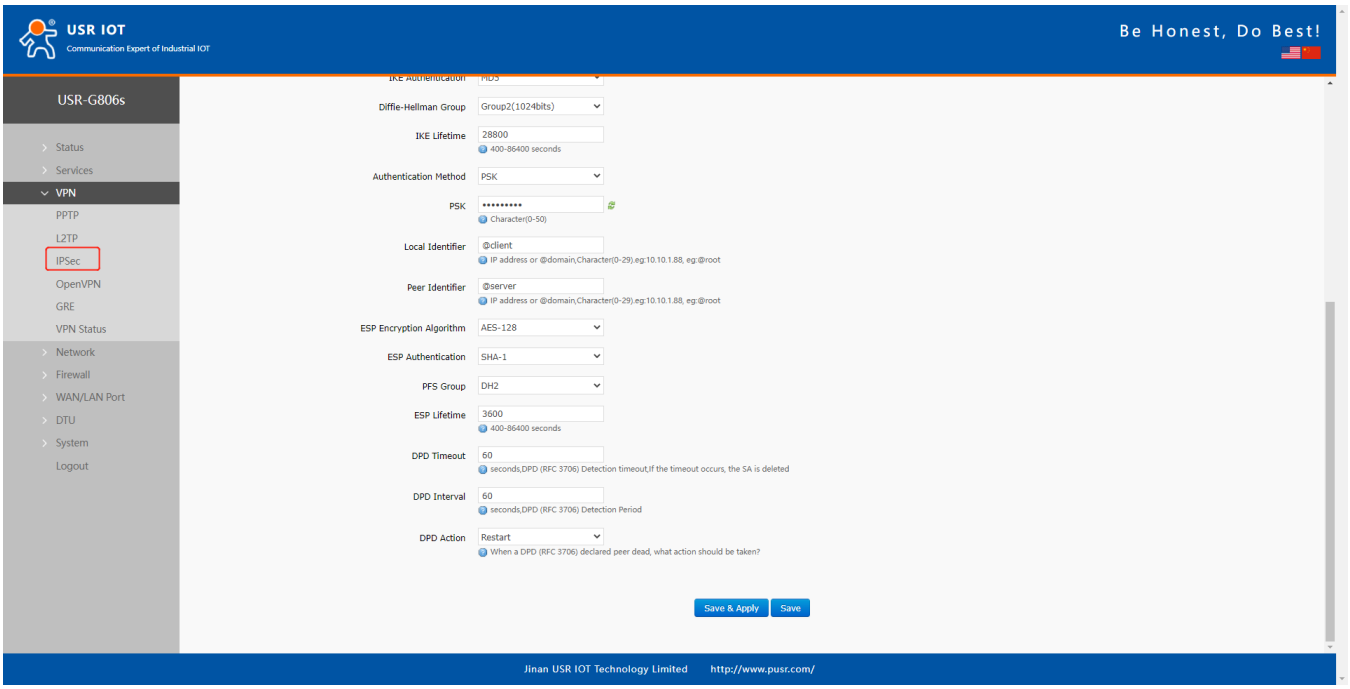
In **VPN---L2TP**, enable L2TP Client, set the related parameters.



Item	Description	Default
Server address	VPN server address or domain name	192.168.0.2
Interface	wan_4G, wan_wired or auto	auto
Username/Password	Get from the VPN server	Null
Encryption/Authentication	Tunnel password, MPPE, IPSEC, consistent with the VPN server.	MPPE
Enable Static Tunnel IP Address	When it is disabled, VPN server will assign an IP address dynamically.	Disable
Extra Options	Append pppd parameters, magic number.	Null
NAT	The source IP address of host behind G806s will be disguised before accessing the remote address.	Enable
Remote Subnet/Mask	When NAT is enabled, can achieve the subnet communication under VPN.	192.168.55.0/255.255.255.0
Enable ping	Real-time VPN online detection and reconnection mechanism.	Disable

4.3. IPSec

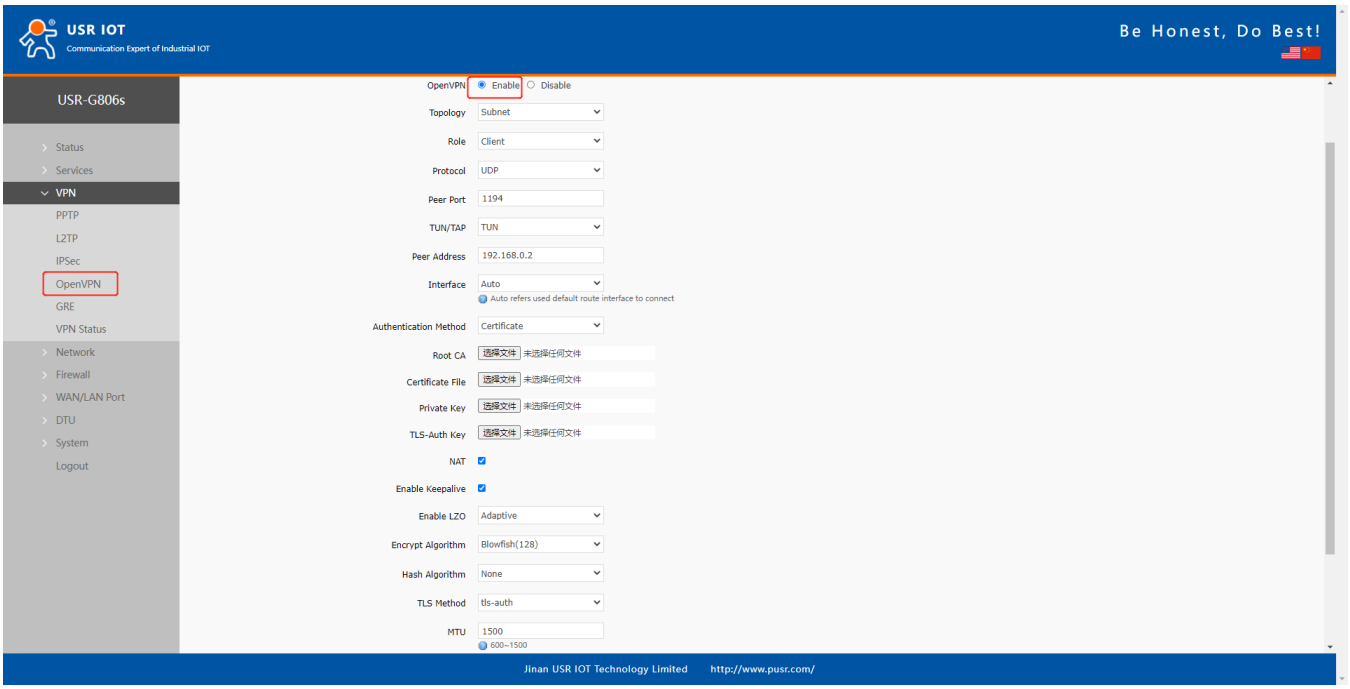




Item	Description	Default
Interface	wan_4G, wan_wired or auto	auto

Remote VPN Endpoint	VPN Client/Server, remote endpoint IP/domain	192.168.0.2
Mode	Main, aggressive	main
Tunnel type	Site to site, site to host, host to host, host to site	Site to site
Local subnet	IPSec local subnet and mask	192.168.1.0/24
Remote subnet	IPSec remote subnet and mask	192.168.55.0/24
Local Identifier	IP address or FQDN preceded by @, e.g. @domain	@client
Peer Identifier	IP address or FQDN preceded by @, e.g. @domain	@server
IKE Encryption	Phase 1 IKE encryption algorithm, authentication and DH group settings.	3DES/MD5/Group2
IKE Lifetime	Set the lifetime in IKE negotiation, 400~86400s	28800
Authentication Method	Pre-shared key	PSK
ESP Encryption	3DES/AES-128/AES-192/AES-256	AES-128
ESP Authentication	SHA-1/SHA2-256/MD5	SHA-1
ESP Lifetime	Set the ESP lifetime/s	3600
PFS Group	None/DH1/DH2/DH5	DH2
DPD Interval	Set the interval after which DPD is triggered if no IPsec protected packets is received from the peer/s	60
DPD Timeout	Set the timeout of DPD packets/s	60
DPD Action	Sets the action for connection detection, None/Clear/Hold/Restart	Restart

4.4. OpenVPN



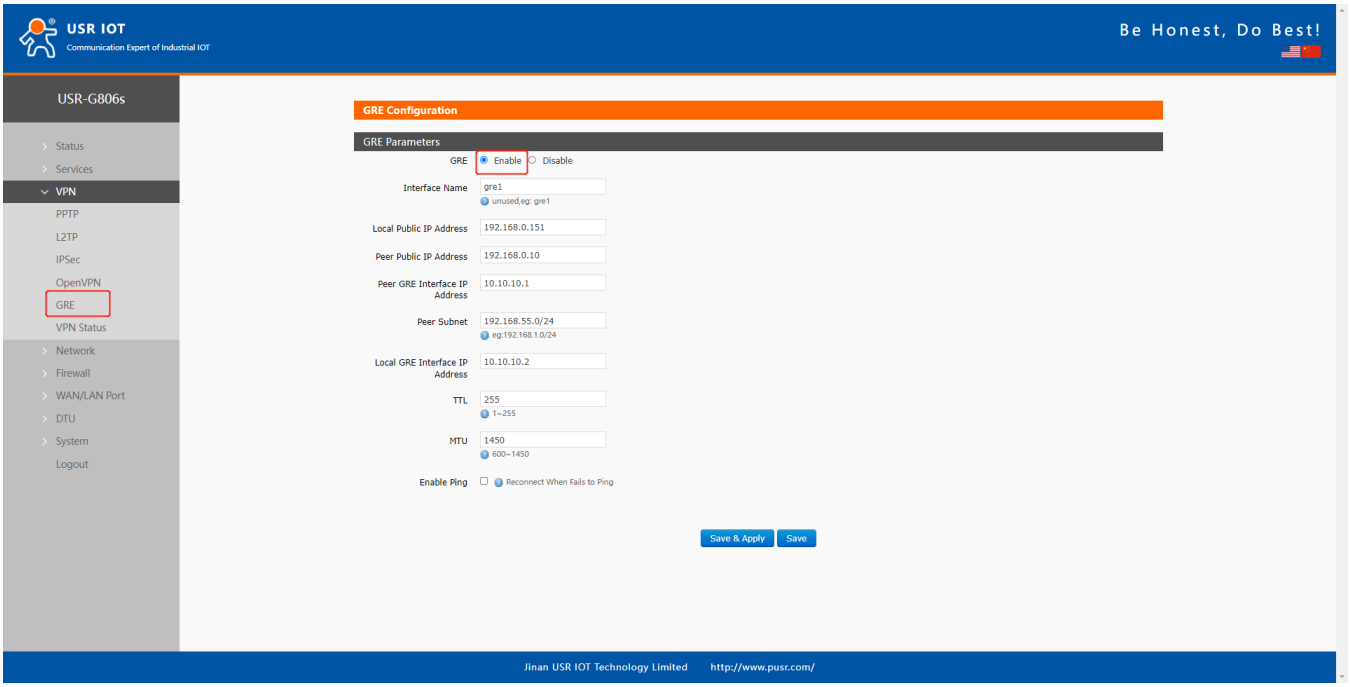
Item	Description	Default
TUN/TAP	TUN/TAP	TUN
Protocol	TCP/UDP	UDP
Peer Port	Listening port of the OpenVPN server	1194
Peer Address	IP/domain name of the OpenVPN server	192.168.0.2
Interface	Auto/wan_wired/wan_4g	Auto
Root CA	Import the ca root file to the router	Null
Certificate File	Import the client certificate file to the router	Null
Private Key	Import the client private key to the router	Null
TLS-Auth Key	Import the TLS authentication key to the router	Null
Encrypt Algorithm	None/Blowfish-128/DES-128/3DES-192/AES-128/AES-192/AES-256	Blowfish-128
Hash Algorithm	None/SHA1/SHA256/SHA512/MD5	None
Enable LZO	Yes/No/Adaptive	Adaptive
Enable Keepalive	Defaults to 10,120, consistent with VPN server	On
MTU	Consistent with VPN server	1500
Enable Ping	Reconnect when fails to ping	Off

After connected successfully, we can check the connection status in “VPN - VPN Status”.

Attached is the OpenVPN server configuration under Linux system:

```
port 1194
proto udp
dev tun
user nobody
group nogroup
persist-key
persist-tun
keepalive 10 120
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1 bypass-dhcp"
crl-verify crl.pem
ca ca.crt
cert server_Jz4Oqi4AWJnZuN8X.crt
key server_Jz4Oqi4AWJnZuN8X.key
tls-auth tls-auth.key 0
dh dh.pem
auth SHA256
cipher AES-256-CBC
#tls-server
#tls-version-min 1.2
#tls-cipher TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
status openvpn.log
verb 3
```

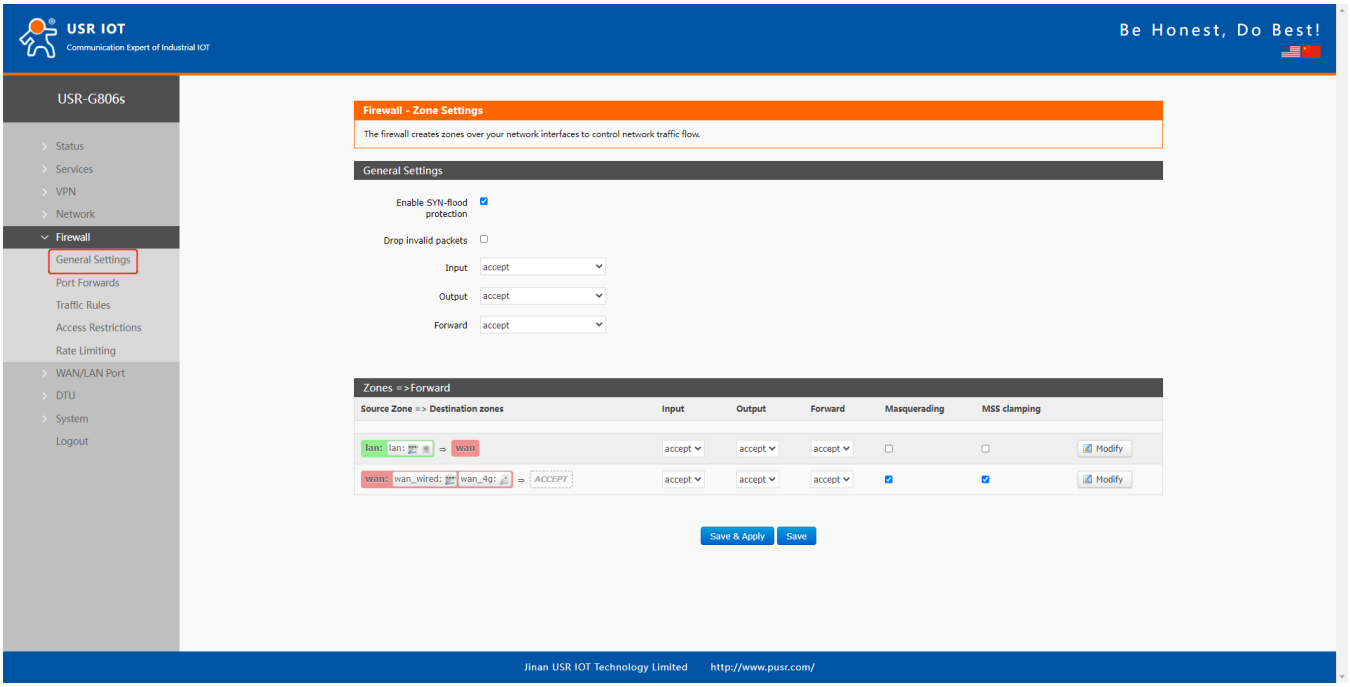
4.5. GRE



Item	Description	Default
Local public IP address	Local wan_wired or wan_4g address	192.168.0.151
Peer public IP address	Remote GRE WAN IP address	192.168.0.10
Peer GRE Interface IP Address	Remote GRE tunnel IP address	10.10.10.1
Peer Subnet	IP/Mask: 255.255.255.0: IP/24 255.255.255.255: IP/32	192.168.55.0/24
Local GRE Interface IP Address	Local GRE tunnel IP address	10.10.10.2
TTL	Set the TTL parameters(1~255)	255
MTU	Set the MTU(600~1450)	1450

5. Firewall

5.1. General Settings

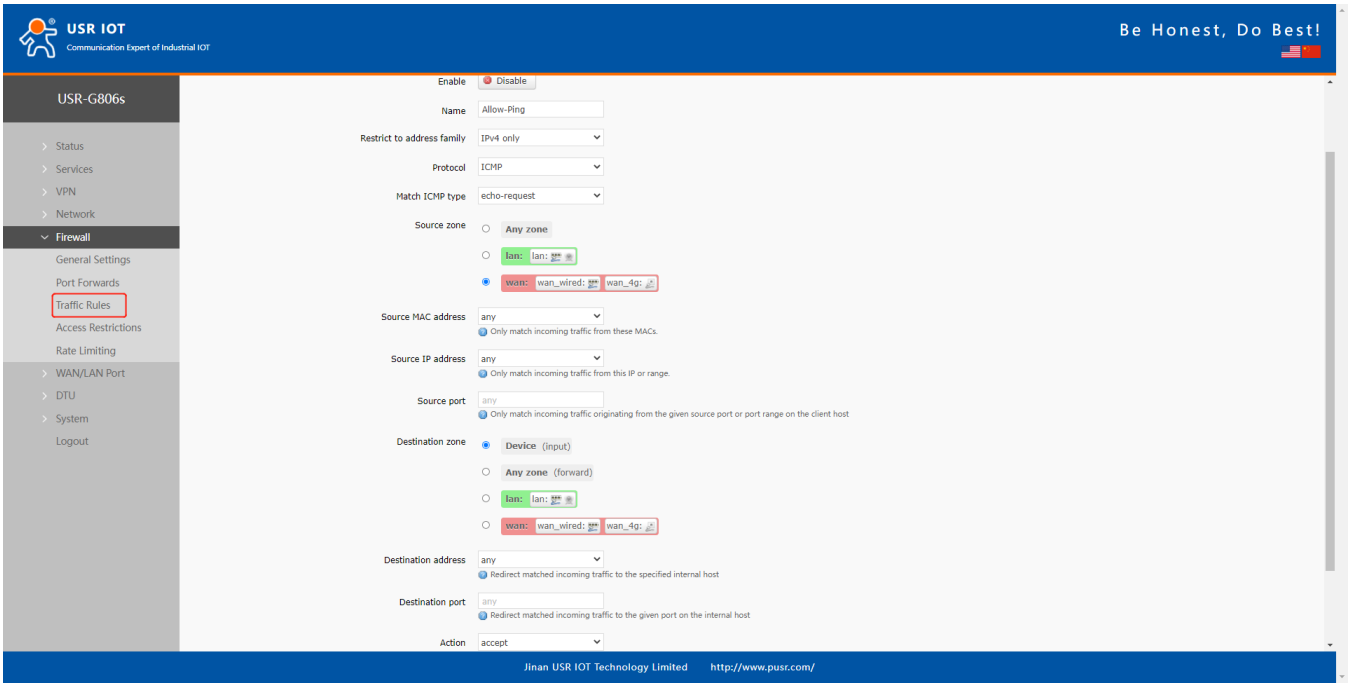


Descriptions:

1. Input: Data packets access to the router's IP.
2. Output: Data packets sent by the router's IP.
3. Forward: Data forwarding between the interfaces, not go through the router.
4. Masquerading: WAN and 4G interface. The source IP address will be disguised before accessing the external network.
5. MSS clamping: Limit the MSS packets, generally is 1460.

5.2. Traffic Rules

Traffic rules can filter specific internet data types and block internet access requests to enhance the security of the network.

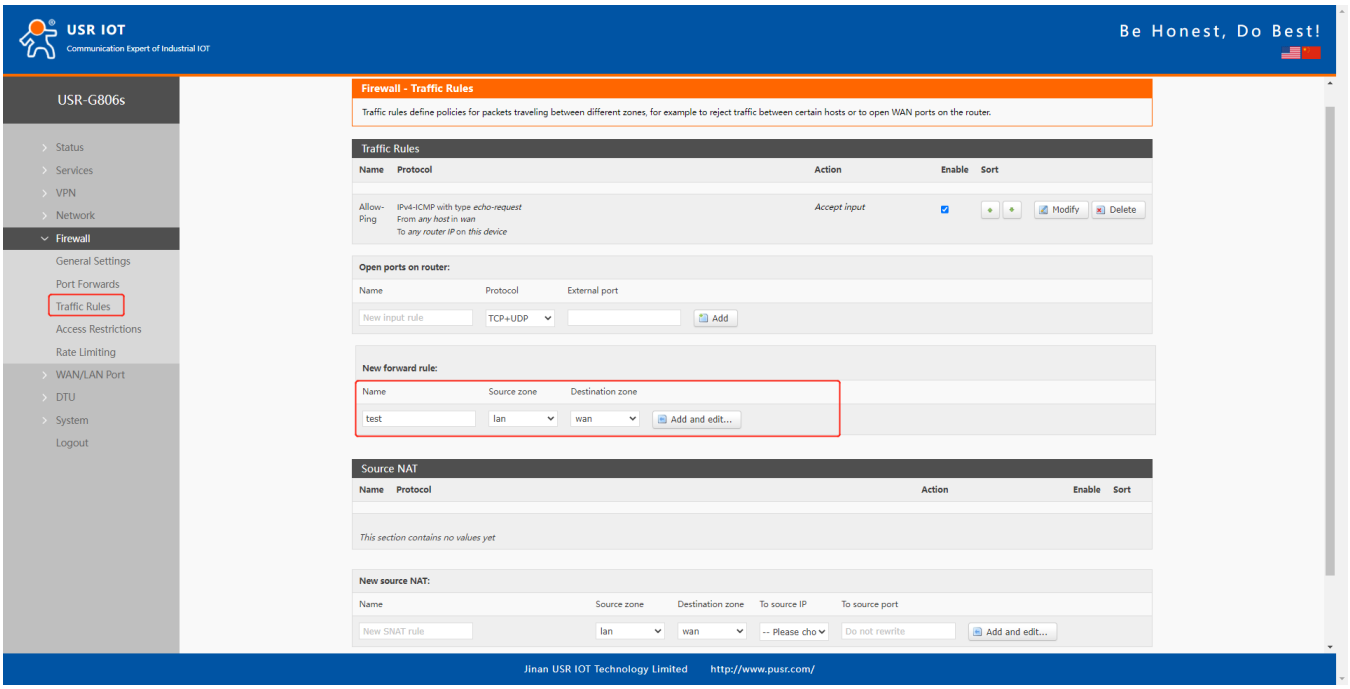


Item	Description	Default
Enable	/	Enable
Name	Name of this rule	-
Restrict to address family	IPv4 only	IPv4 only
Protocol	TCP+UDP/TCP/UDP/ICMP	TCP+UDP
Match ICMP type	Matched ICMP rule, choose **Any**	Any
Source zone	Any zone/LAN/WAN	LAN
Source MAC address	Source MAC address to match this rule, can be multiple MAC addresses. Each MAC address is separated by spaces. Any: match all the MAC addresses. Note: When matching the source MAC address, leave the source IP address blank.	Any
Source IP address	Source IP address to match this rule, can be a IP range, like 192.168.1.100-192.168.1.200. Any: match all the IP addresses. Note: When matching the source IP address, leave the source MAC address blank.	Any
Source port	Source IP port to match this rule, can be a port range, like 8000-9000. Null: match all the ports.	Null
Destination zone	Device/Any zone/LAN/WAN	WAN
Destination address	The destination IP address to be accessed.	Any

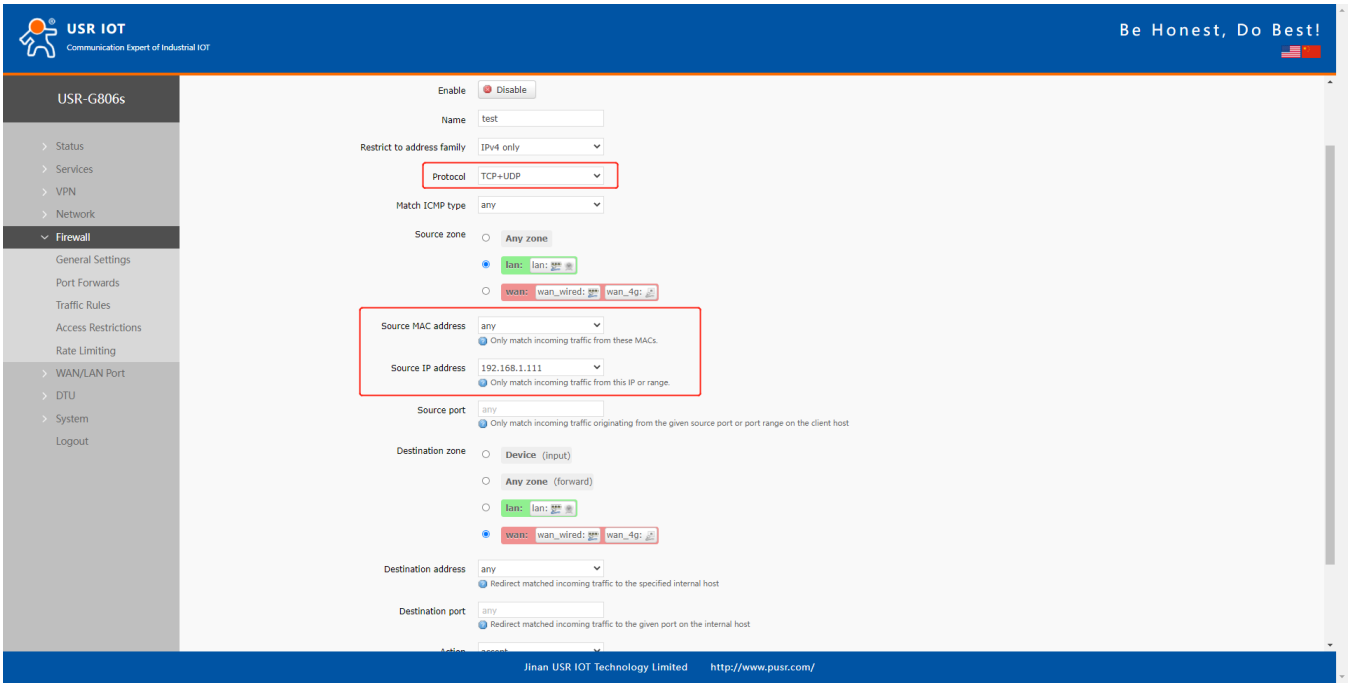
	Any: match all the addresses.	
Destination port	The destination port to be accessed. Null: match all the ports.	Null
Action	After receiving such data packets, you can select: drop, accept, reject, or don't track.	Accept

5.2.1. IP Address Blacklist

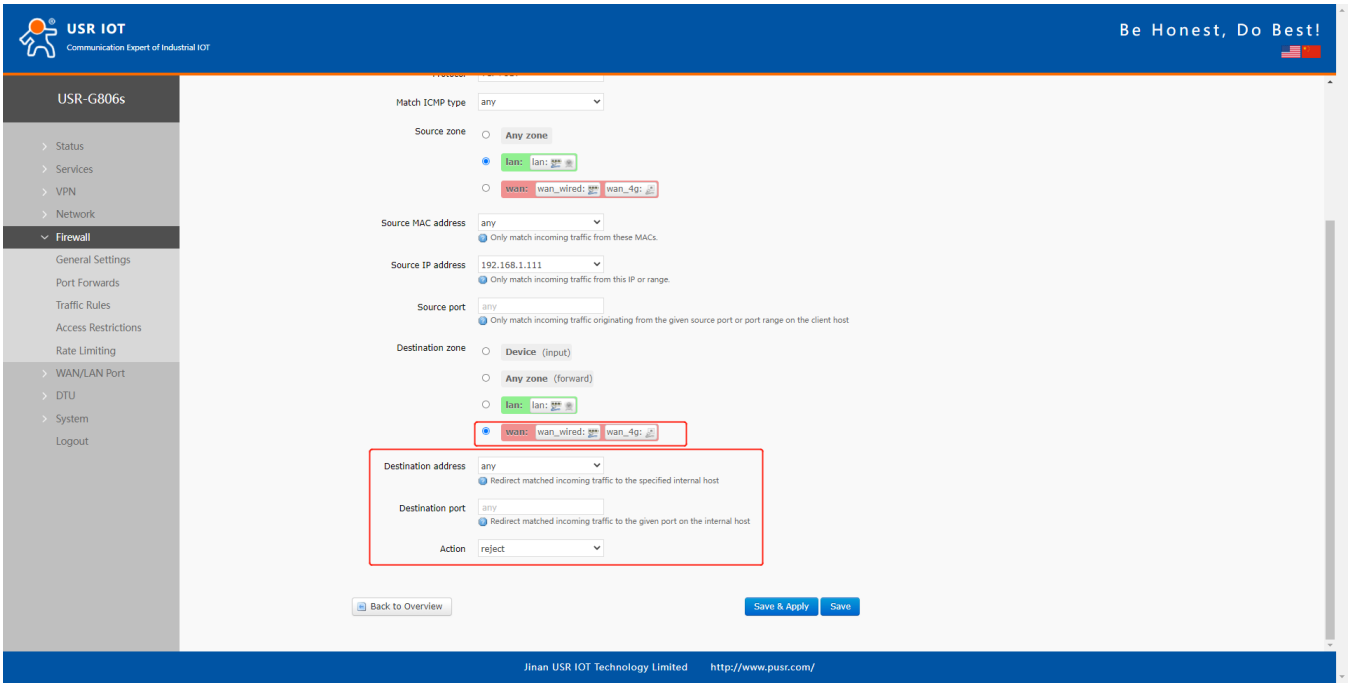
In **Traffic Rules--New forward rule**, enter the name and then click **Add and edit**.

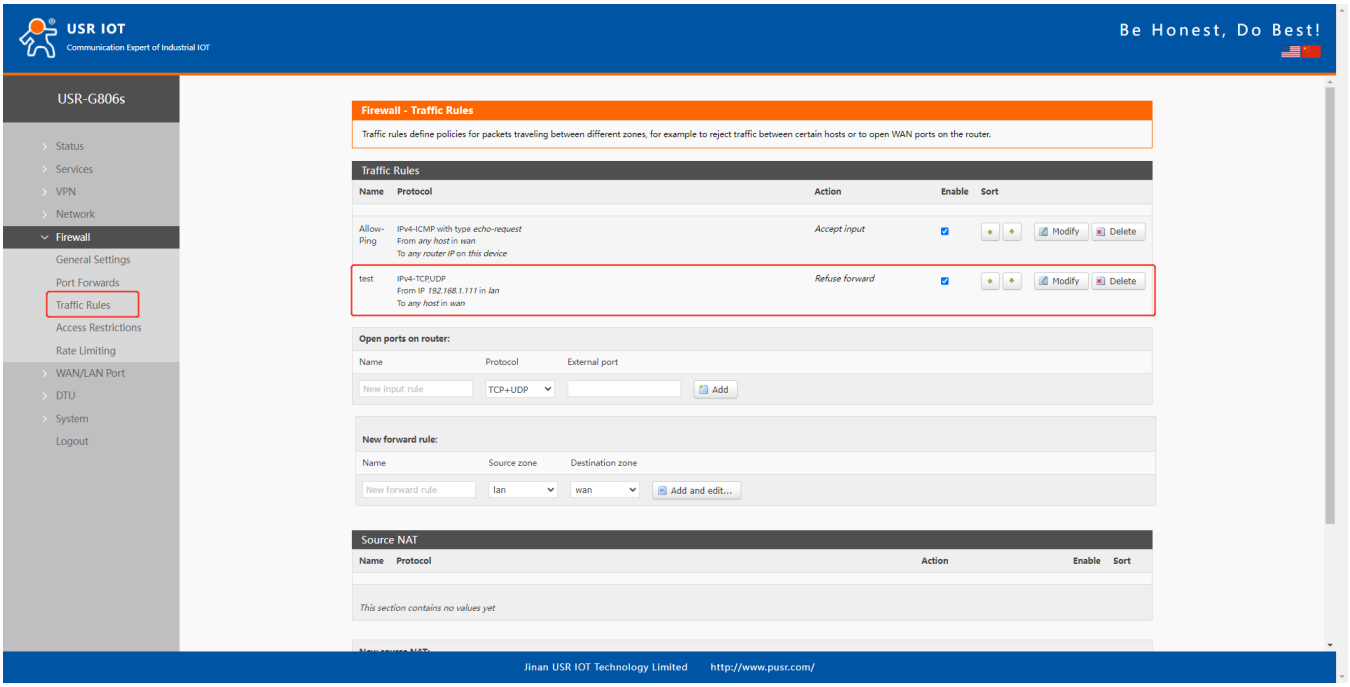


In below interface, set the **Source zone** to **lan**, set the source IP address to a specific IP address, like 192.168.1.111.



Configure the **Destination zone** to **wan**, change the destination address to **any**, change the **Action** to **reject**. Click **Save&Apply**.

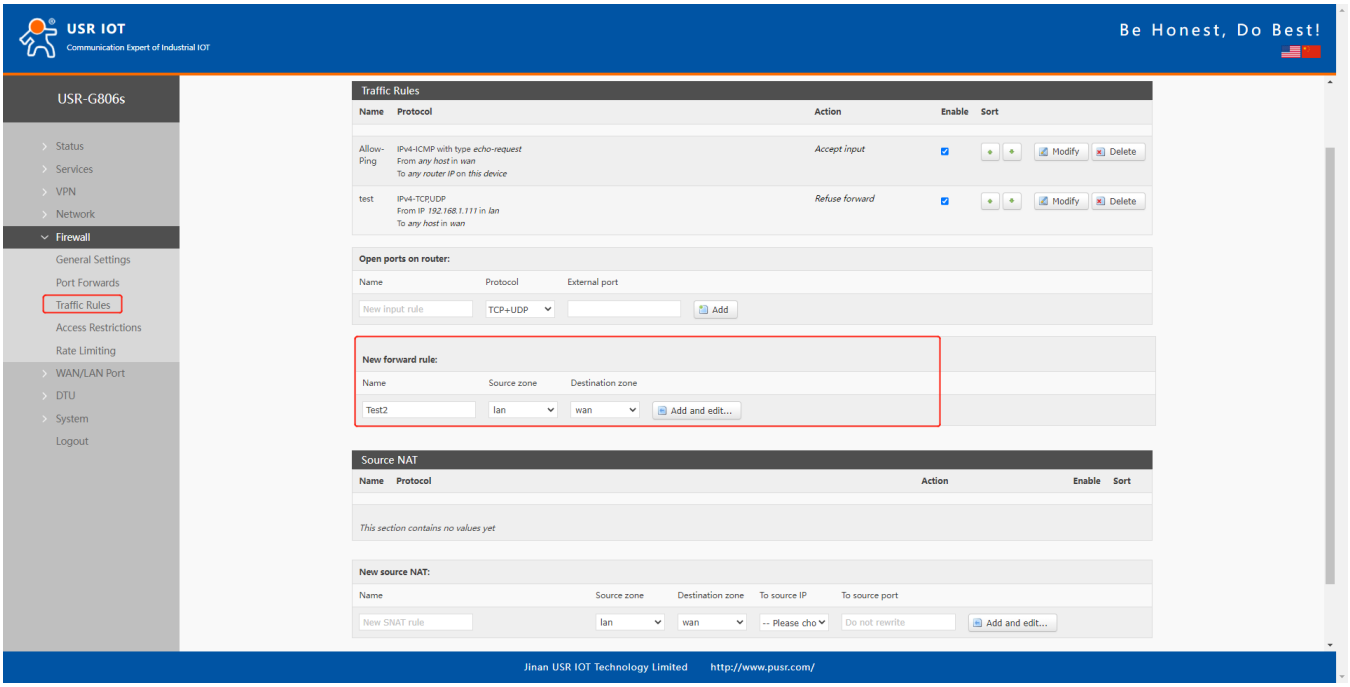




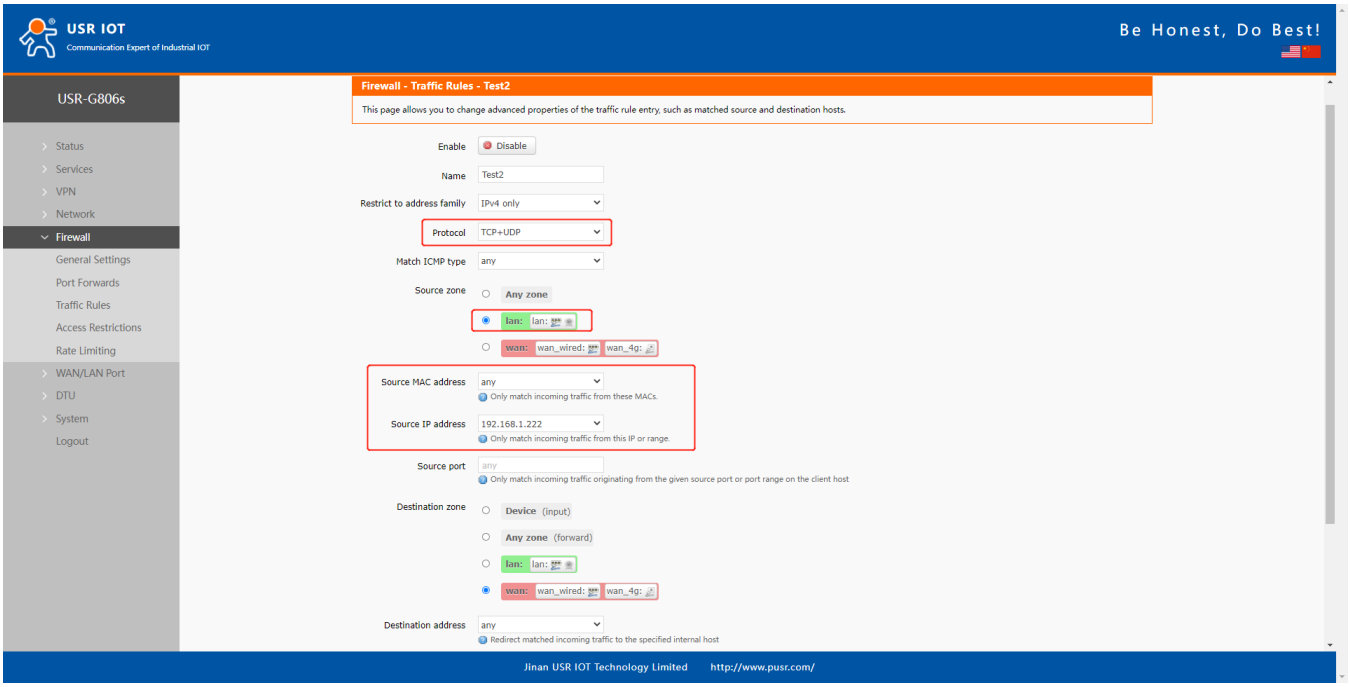
In this way, the device with IP 192.168.2.133 is forbidden to access all extranets.

5.2.2. IP Address Whitelist

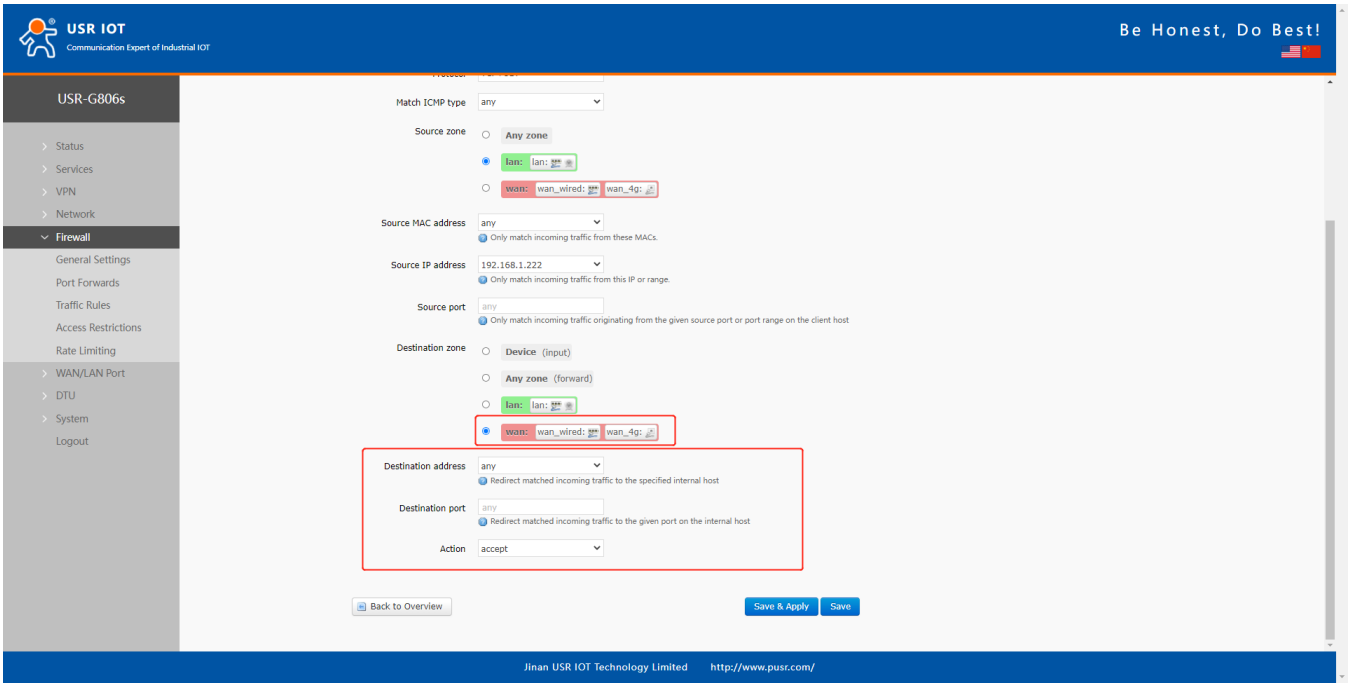
In **Traffic rules--New forward rule**, enter the rule's name, click **Add and edit** to create a whitelist rule.



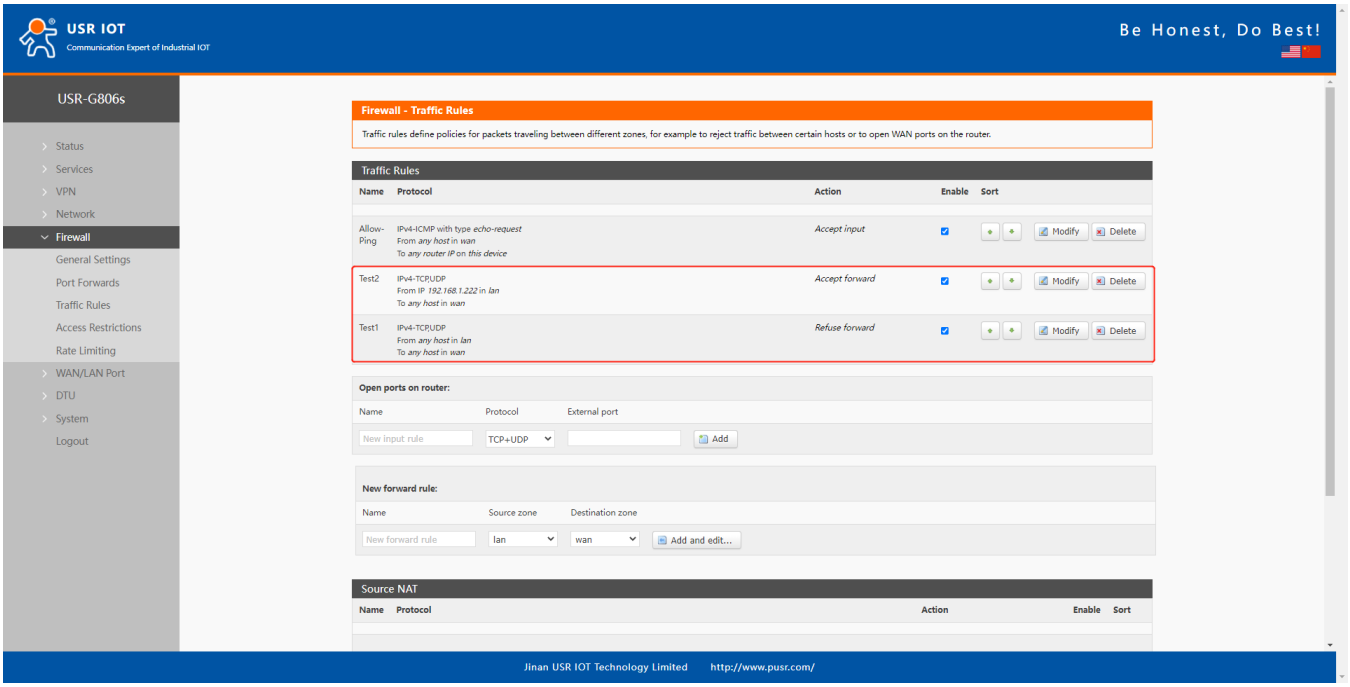
In below interface, set the **source zone** to **lan**, set the **source IP address** to a specific one, like 192.168.1.222.



Change the **destination zone** to **WAN**, the **destination address** to **any**, the **Action** is **accept**. Click **Save&apply**.



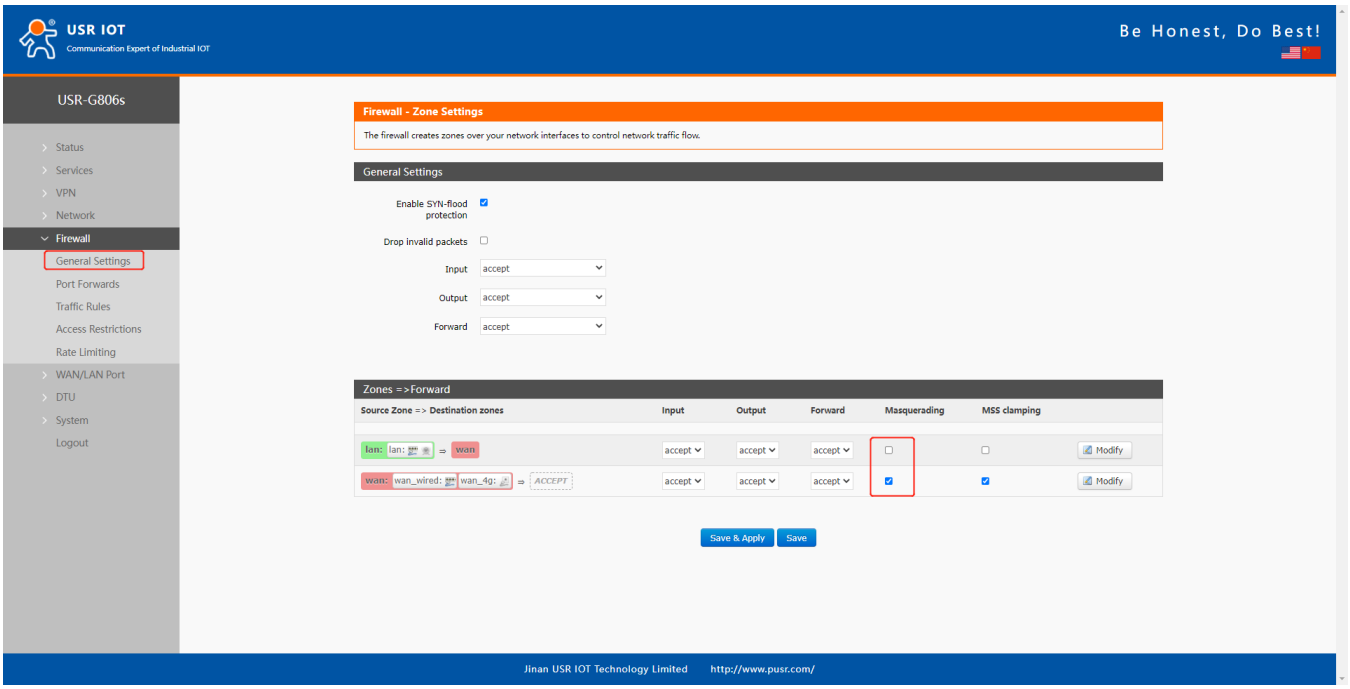
Then we need to set another rule to reject all the communication, the source IP address and destination IP address are “any”, set the action to “reject”. Please note the order of the two rules, the accepted rule must come before the rejected rule.



5.3. NAT

5.3.1. Masquerading

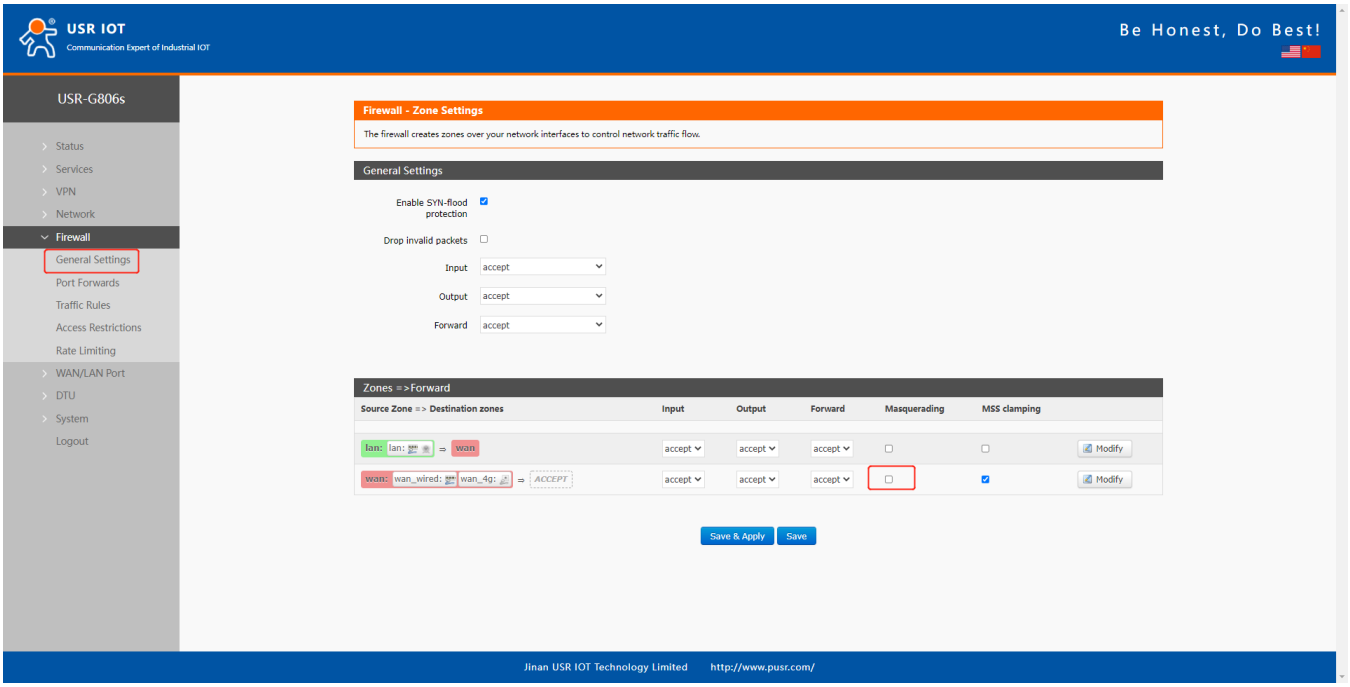
Masquerading will disguise the source IP address of the data packets to the WAN IP address of the router. The masquerading and MSS clamping of the WAN interface must be enabled, which must be disabled in the LAN interface.



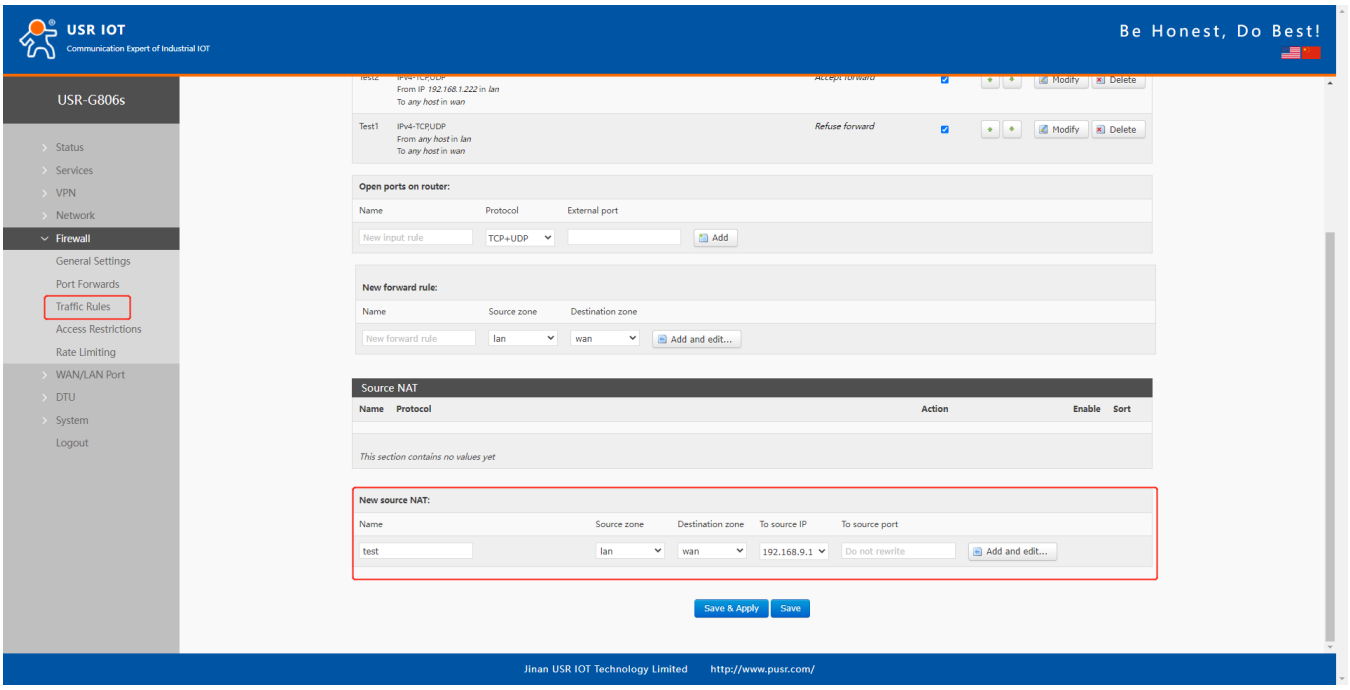
5.3.2. SNAT

Item	Description	Default
Enable	/	Enable
Name	Name of this rule	/
Protocol	TCP+UDP/TCP/UDP/ICMP	TCP+UDP
Source IP address	Source IP address or IP range to match this rule, like: 192.168.1.100 or 192.168.1.100-192.168.1.200 Any means match all the source IP addresses.	Any
Source port	Source port or port range to match this rule, like 9999 or 8888-9999. Null means match all the source ports.	Null
Destination IP address	Destination IP address or IP range to match this rule, like 192.168.2.100 or 192.168.2.100-192.168.2.200 Null means match all the destination addresses.	Null
Destination port	Destination port to or port range to match this rule, like 9999 or 8888-9999. Null means match all the destination ports.	Null
SNAT IP address	Change the source IP of the matched traffic to this address	Custom
SNAT port	Change the source port of the matched traffic to this port, null means use the original source port	Null

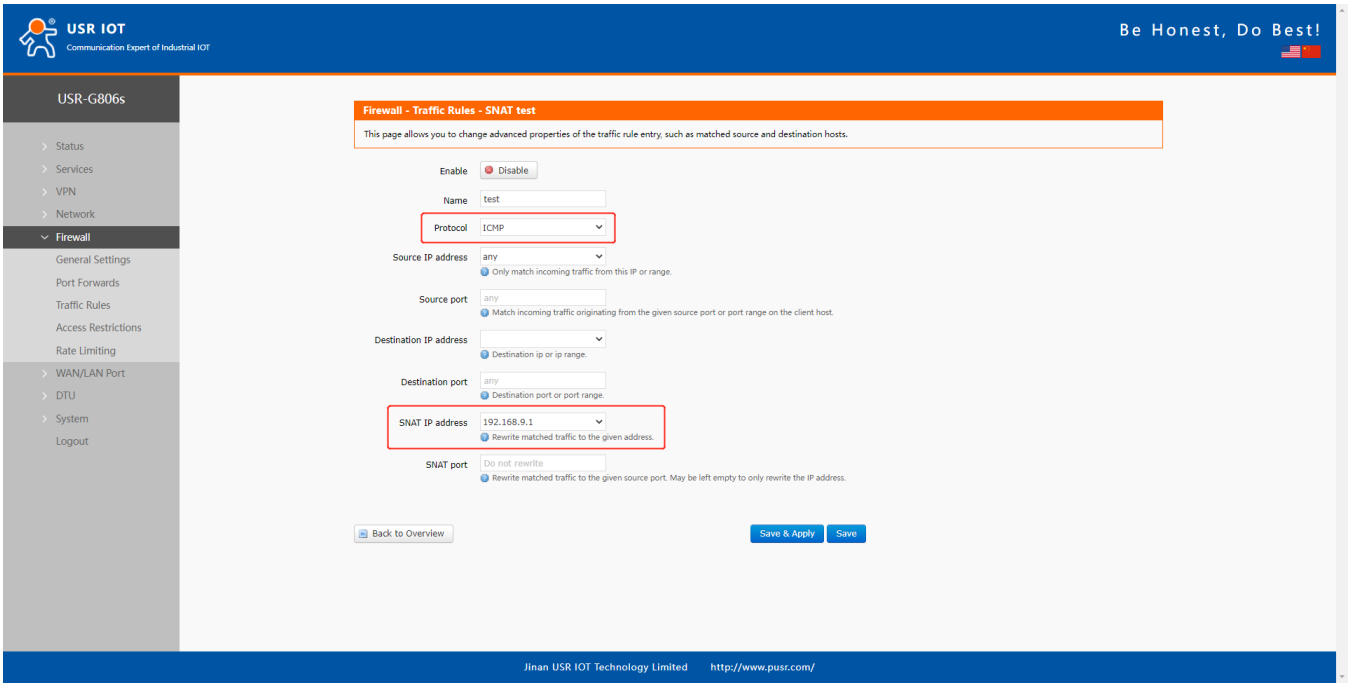
Source NAT is a special form of packet masking that changes the source address of a packet leaving the router. When using it, we need to disable the masquerading of the WAN port.



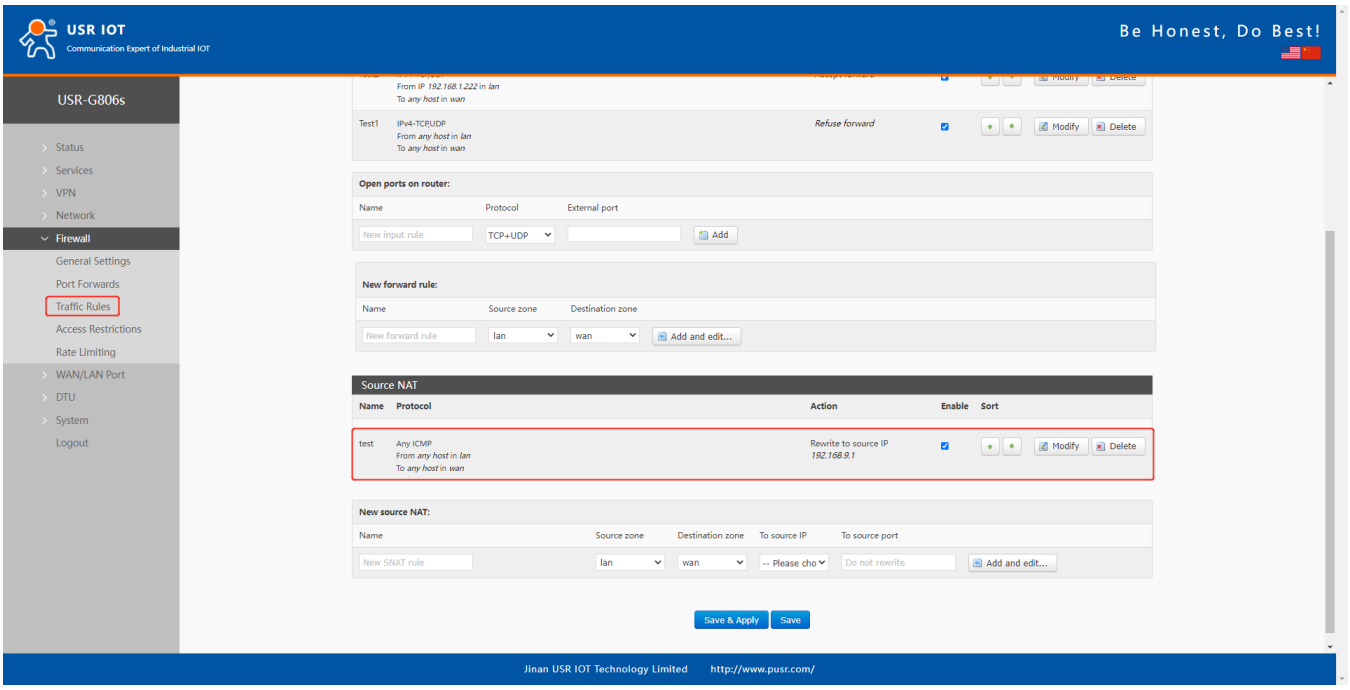
Then create a source NAT rule.



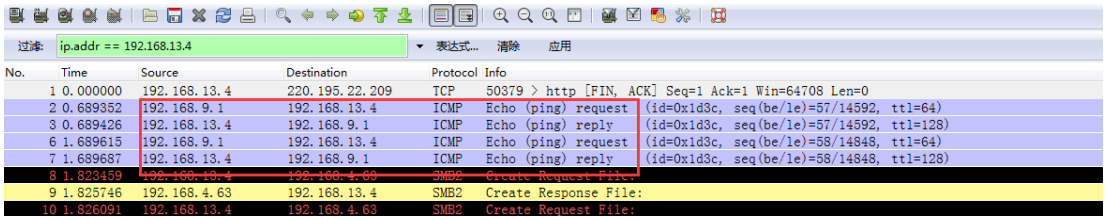
Click **Add and edit**.



Default to enable all the source IP address and destination IP address. Click **Save&Apply**.

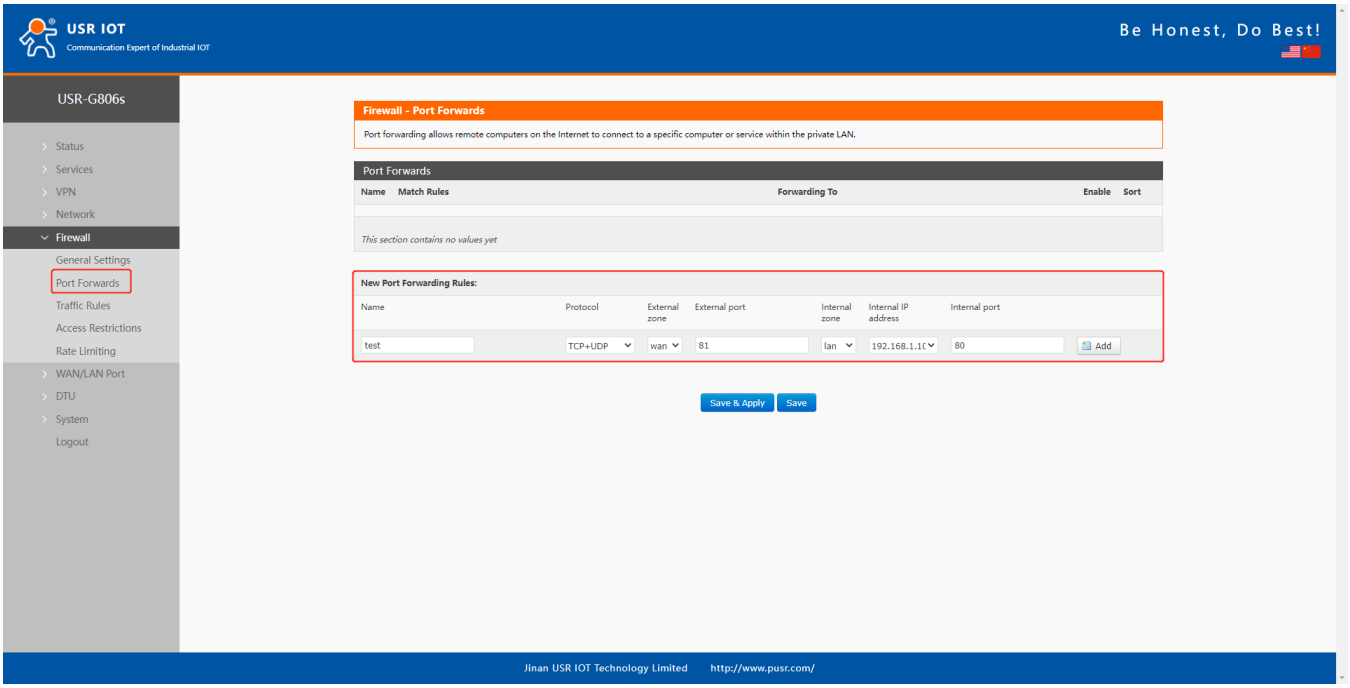


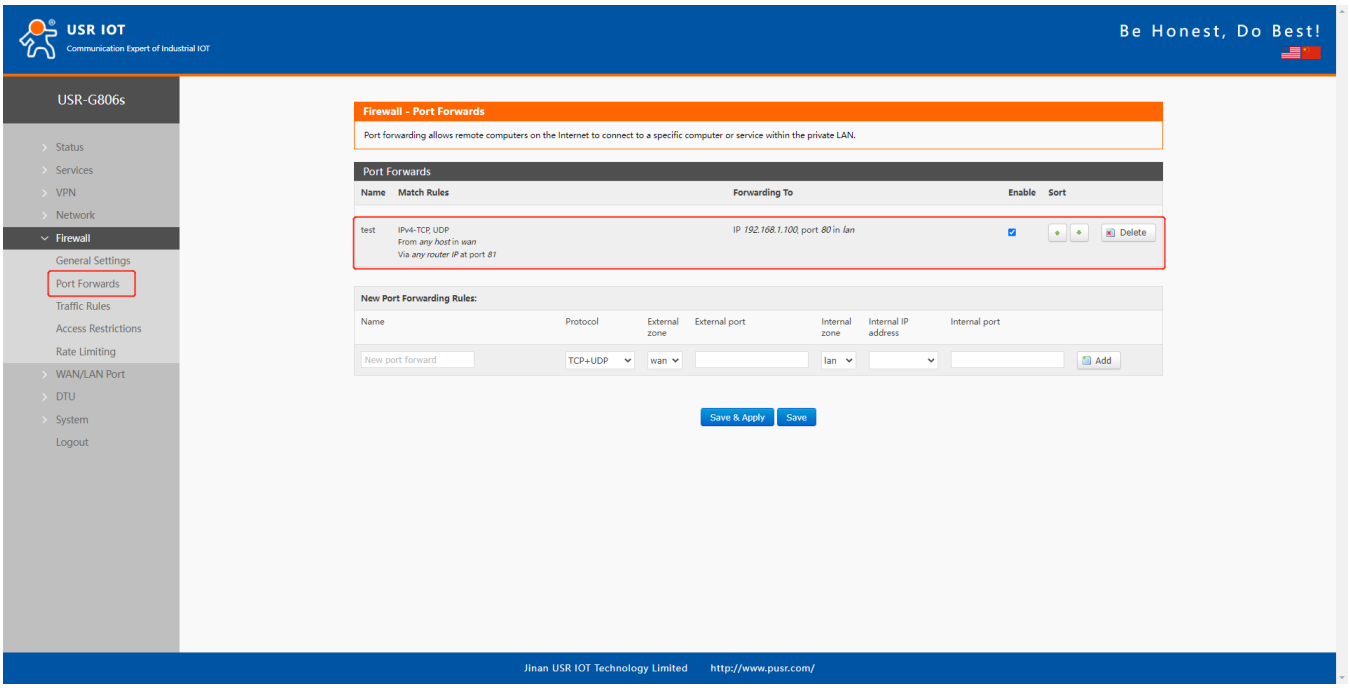
We have changed the source IP address that left the router to 192.168.9.1. When we use the device connected to the router (IP:192.168.1.114) to ping the PC connected to the same switch as the router (IP:192.168.13.4), the source IP address of the ICMP packet to 192.168.13.4 is 192.168.9.1, not 192.168.1.114.



5.3.3. Port Forwards

Port forwarding rules can map a specific port of the WAN interface to a intranet host.



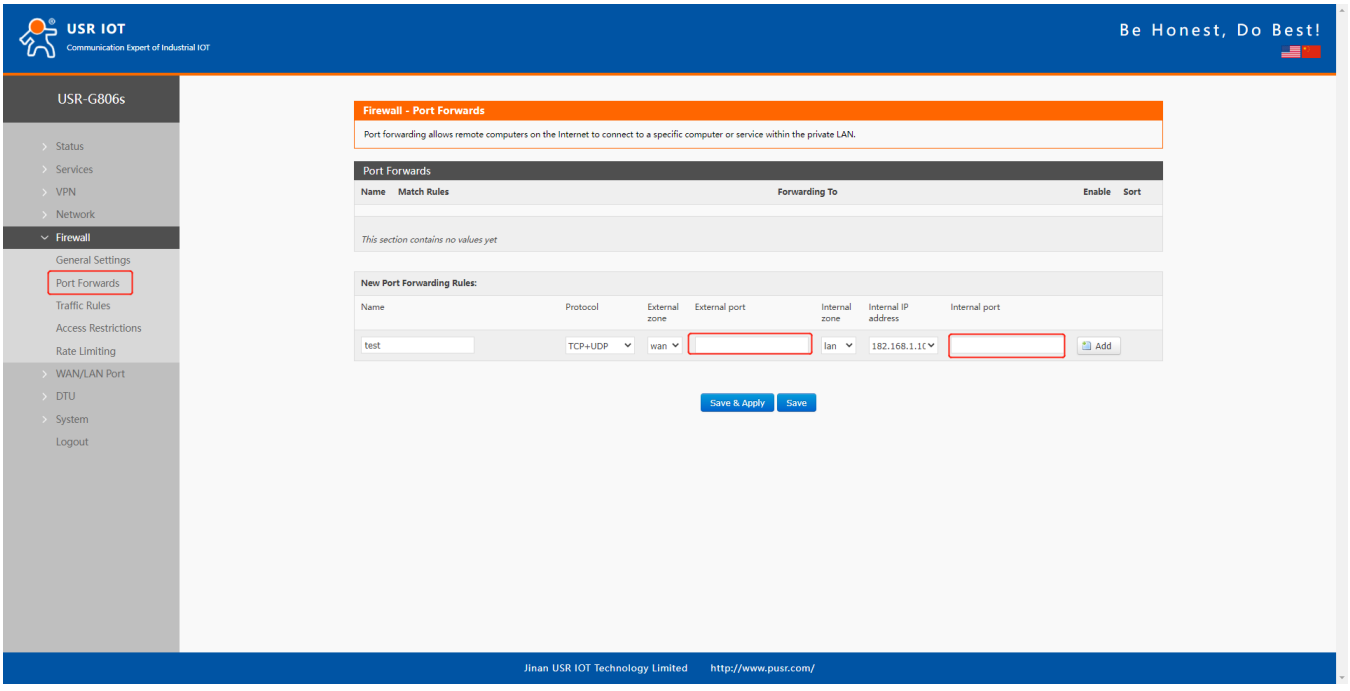


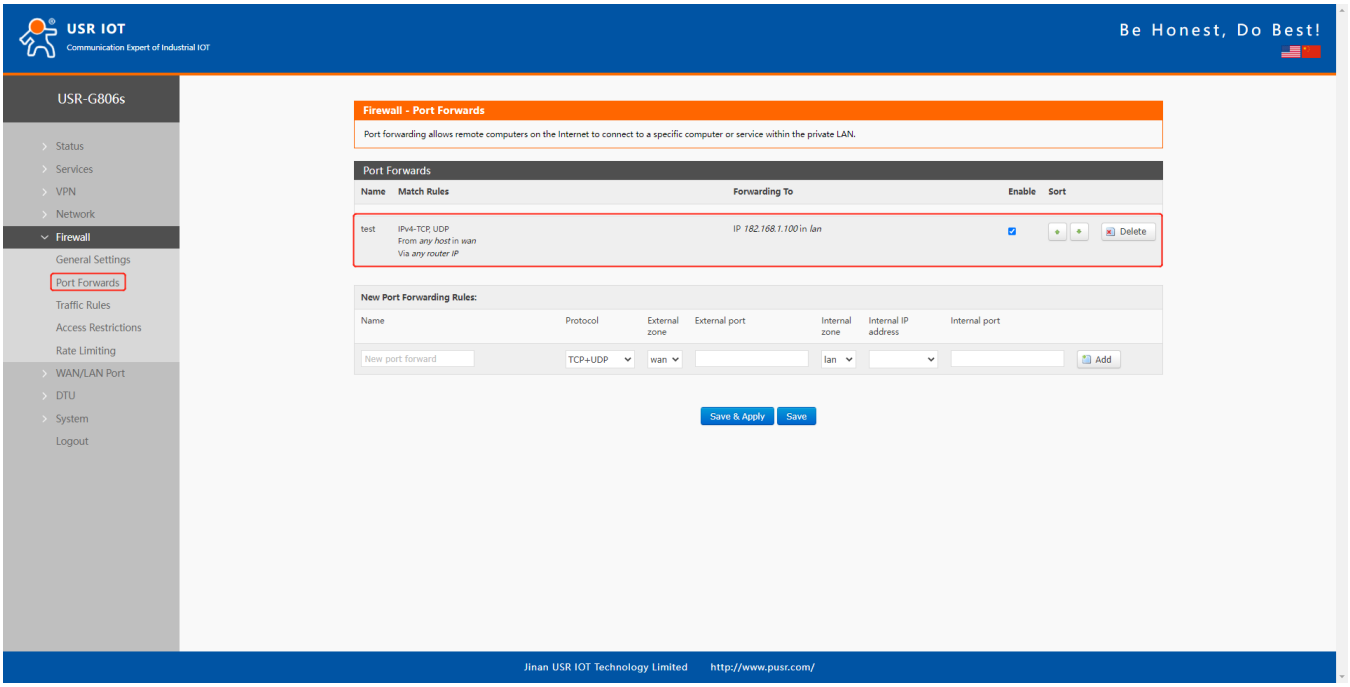
Item	Description	Default
Name	Name of this rule	Null
Protocol	TCP+UDP/TCP/UDP	TCP+UDP
External zone	Including wired wan、4G、VPN	wan
External port	Can be a port or port range, like: 8000-9000 When the external port and internal port are empty, it is DMZ function.	Null
Internal zone	LAN network	lan
Internal IP address	LAN IP address of the router	Null
Internal port	Can be a port or port range, like: 8000-9000 When the external port and internal port are empty, it is DMZ function.	Null

5.3.4. NAT DMZ

Port forwarding rules map a specified WAN port to a intranet host, DMZ rules will map all ports of the WAN interface to a intranet host.

DMZ rules are set in the port forwarding interface, in DMZ mode, do not need to set the external port and internal port.





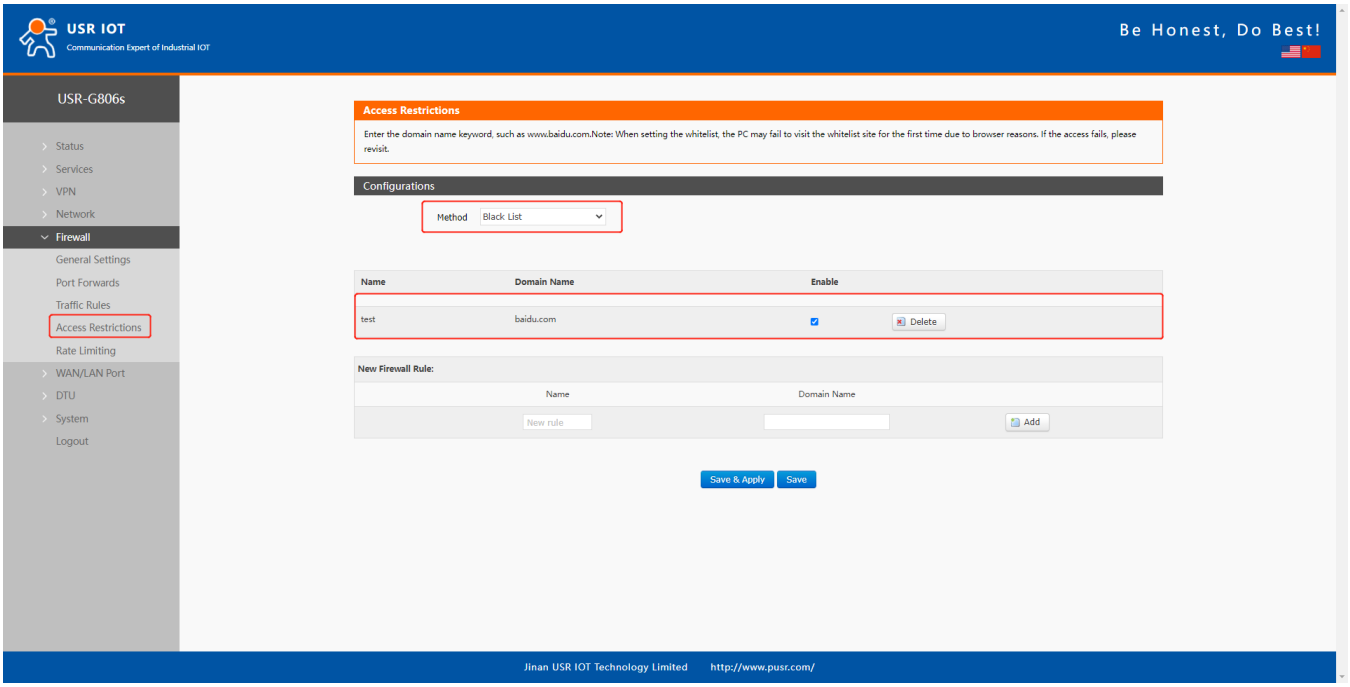
All the ports of the WAN address will be forwarded to the intranet host 192.168.1.100.

➢ Note: Port forwarding and DMZ cannot be used at the same time.

5.4. Access Restriction

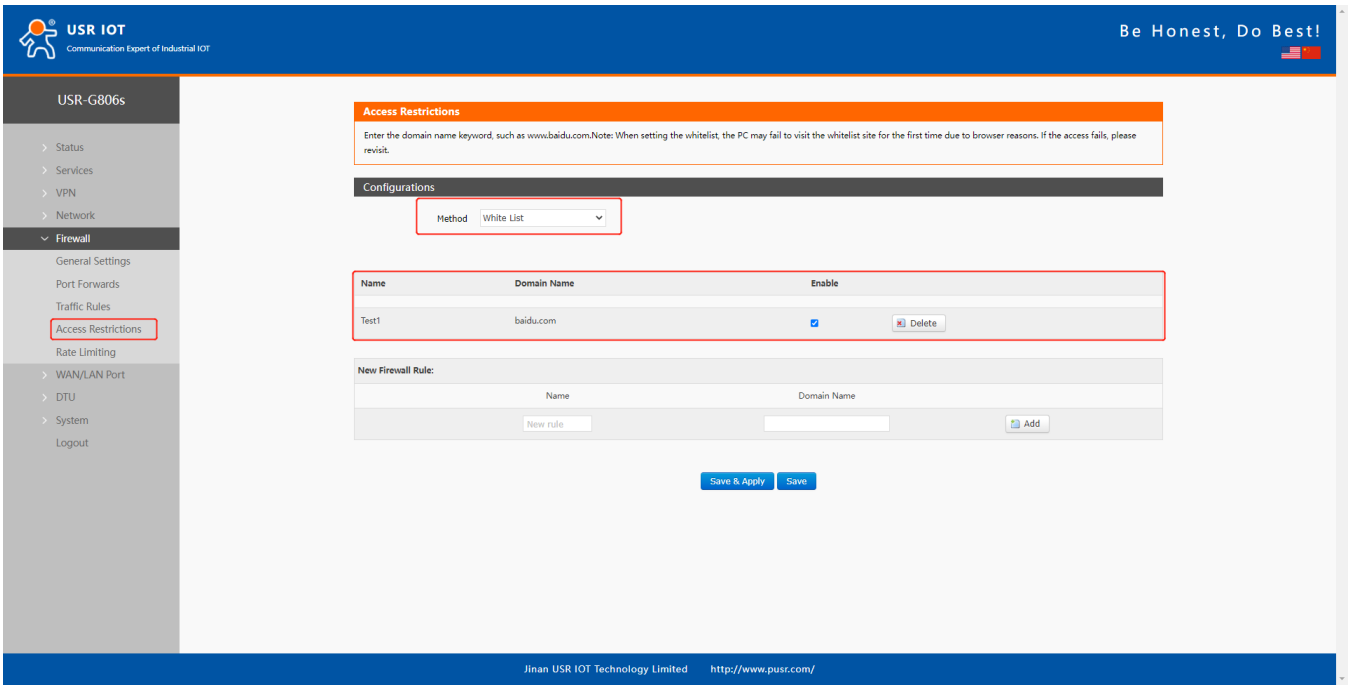
5.4.1. Black List

When we choose “Black list”, the devices connected to the router cannot access the domain name in blacklist, but can access all other domain names. Here, the device can access the domain name except **baidu.com**.



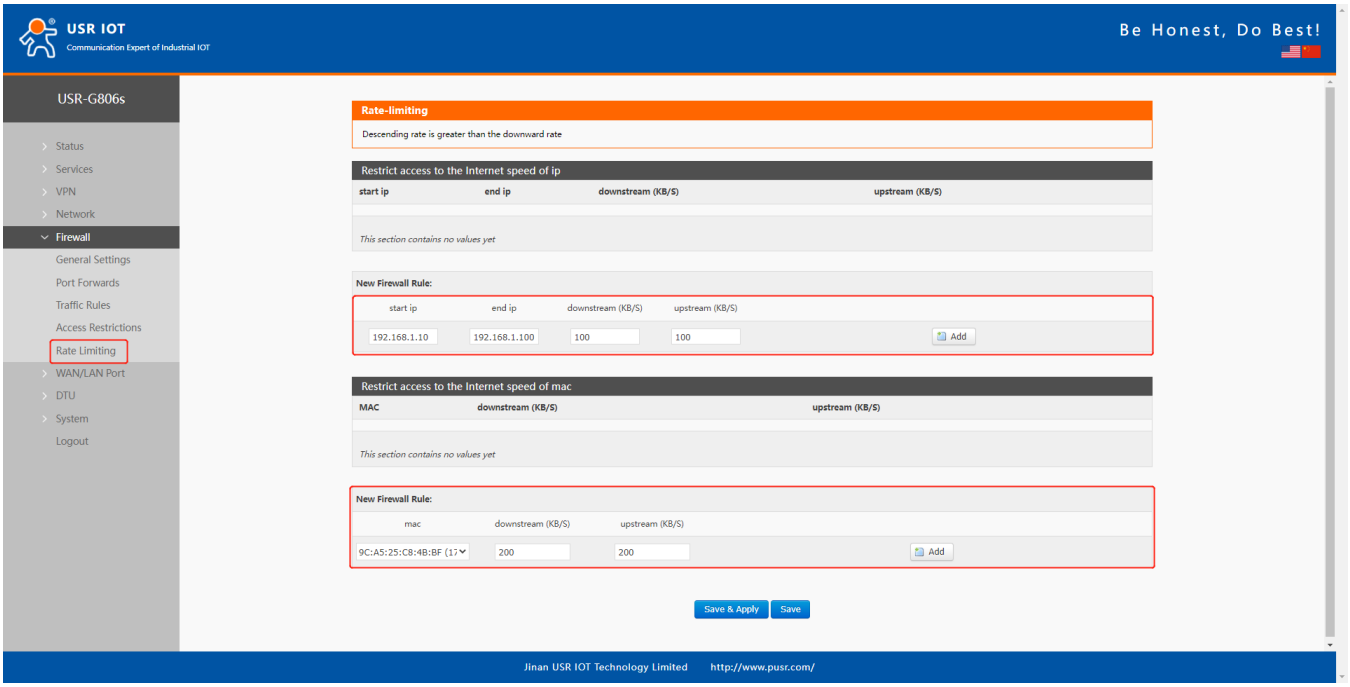
5.4.2. White List

After enable “White List”, the devices connected to the router can only access the domain name within whitelist. If just enable white list but do not add the rules, the device cannot access any domain name. Here, the device can only access **baidu.com**.



5.5. Rate Limiting

This function can limit the upload and download rate the the devices that connected to routers. You can add the rules related to the IP address and MAC address. Multiple rules can be created at the same time.
The minimum upstream and downstream rate is 10KB/S. The downstream rate is usually greater than the upstream rate.



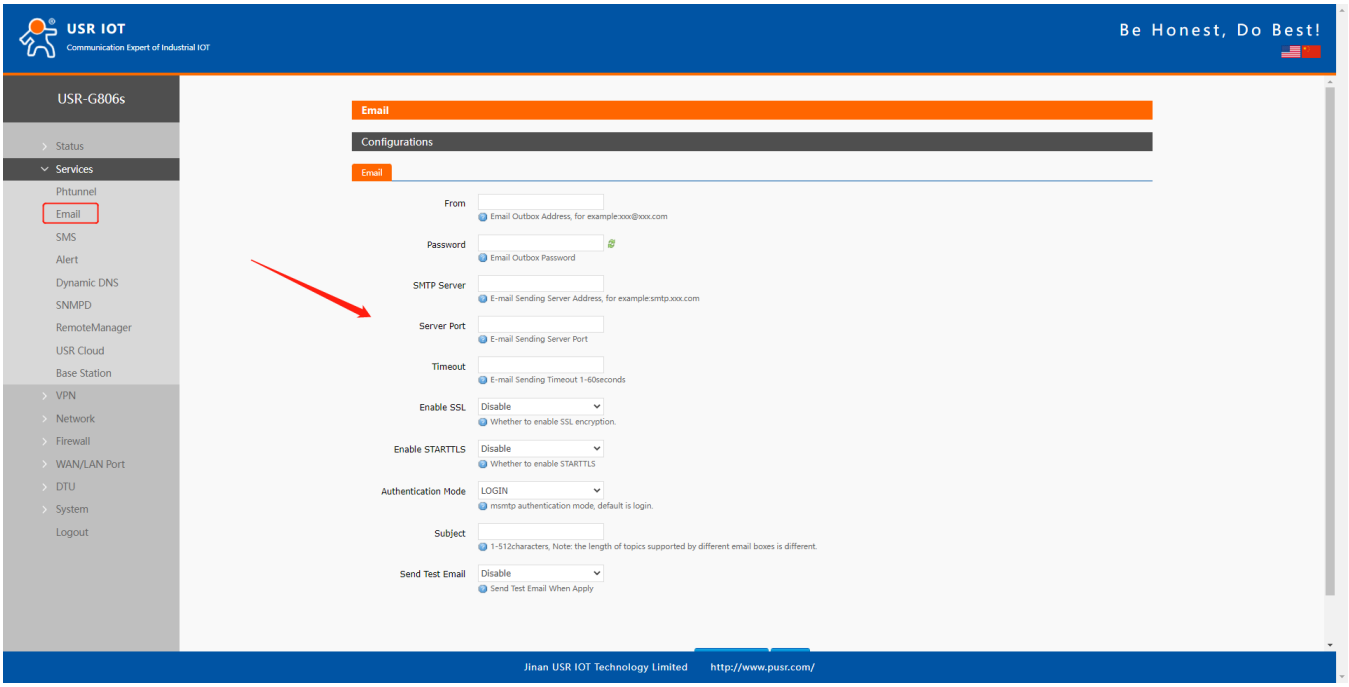
6. PUSR Cloud

For the details of connecting USR-G806s to our PUSR Cloud, please refer to our another manual: Remote Management of USR Router

7. Advances Services

7.1. Email

After connecting to the network, this mailbox will be used as the sender to send a specific alarm email to the set email address.



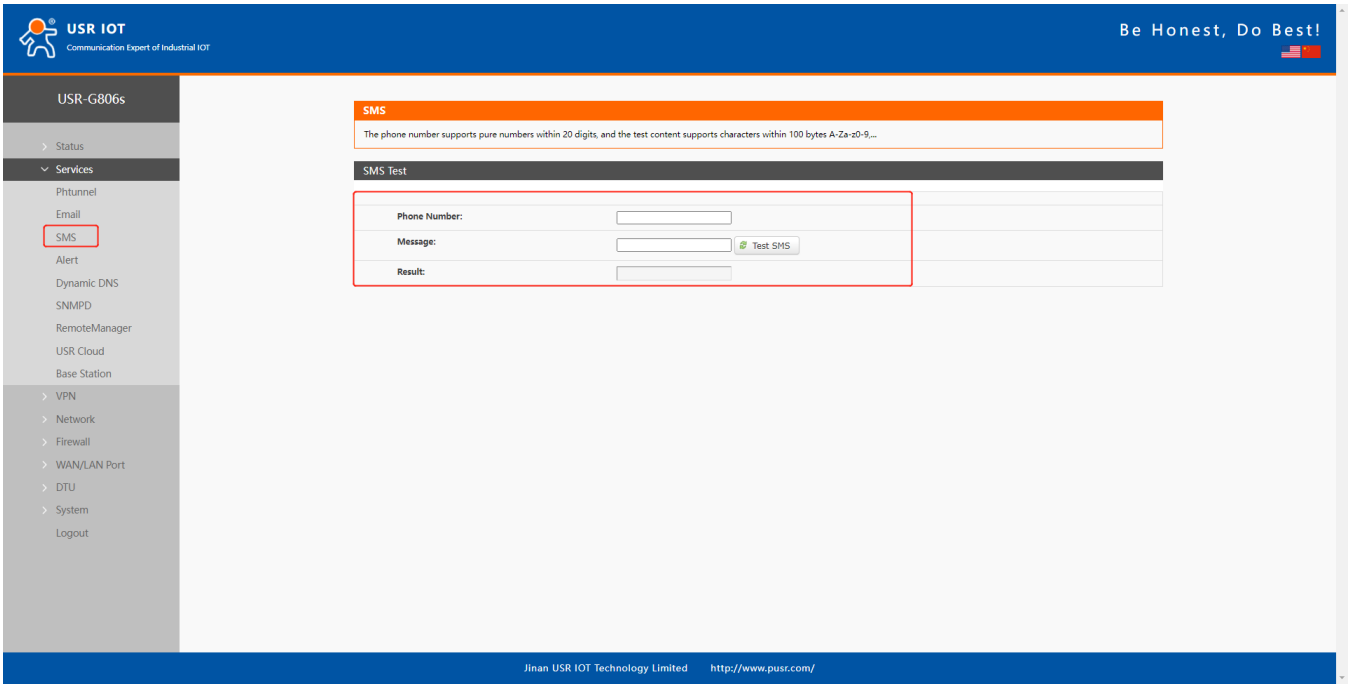
Item	Description	Default
From	Sender mail of the alarm	Null
Password	Sender mail password or the set third party mailbox authorization code	Null
SMTP server	Outgoing mail server. Can check in “Set--Client Settings” of the mail.	Null
Server port	Outgoing mail server port. Can check in “Set--Client Settings” of the mail.	Null
Timeout(Units: s)	Email sending timeout: 1~60s	Null
Enable SSL	Whether to enable SSL encryption. Can check in “Set--Client Settings” of the mail.	Disable
Enable STARTTLS	Whether to enable STARTTLS.	Disable
Authentication Mode	LOGIN/PLAIN/Custom	LOGIN
Subject	Subject when sending the email.	Null
Send test email	Whether to enable sending test email	Disable

Note:

1. If fails to send the email with the correct configuration, please check if the authorization code is needed. The authorization code is a special password used by the third party to log in the mail client.
2. Outlook and Tencent Exmail have been validated for this function.

7.2. SMS

This function is just for SMS test. Please waiting 2~15s after clicking **Test SMS**.



Item	Description	Default
Phone number	Send SMS to this phone number	Null
Message	SMS content	Null
Result	Success or Fail	-

7.3. Alert

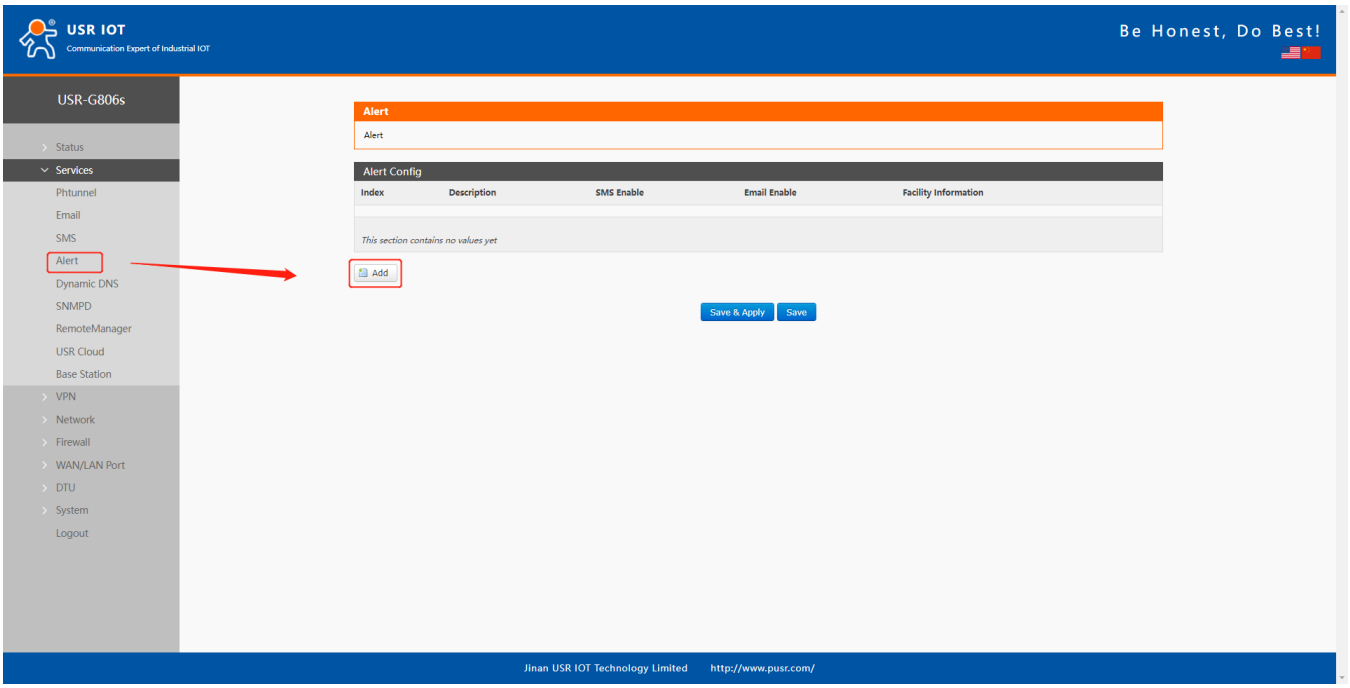
G806s supports alerting via SMS, Email and triggering DO, supports carrying device information.
It supports up to 20 alert messages with many different device status.

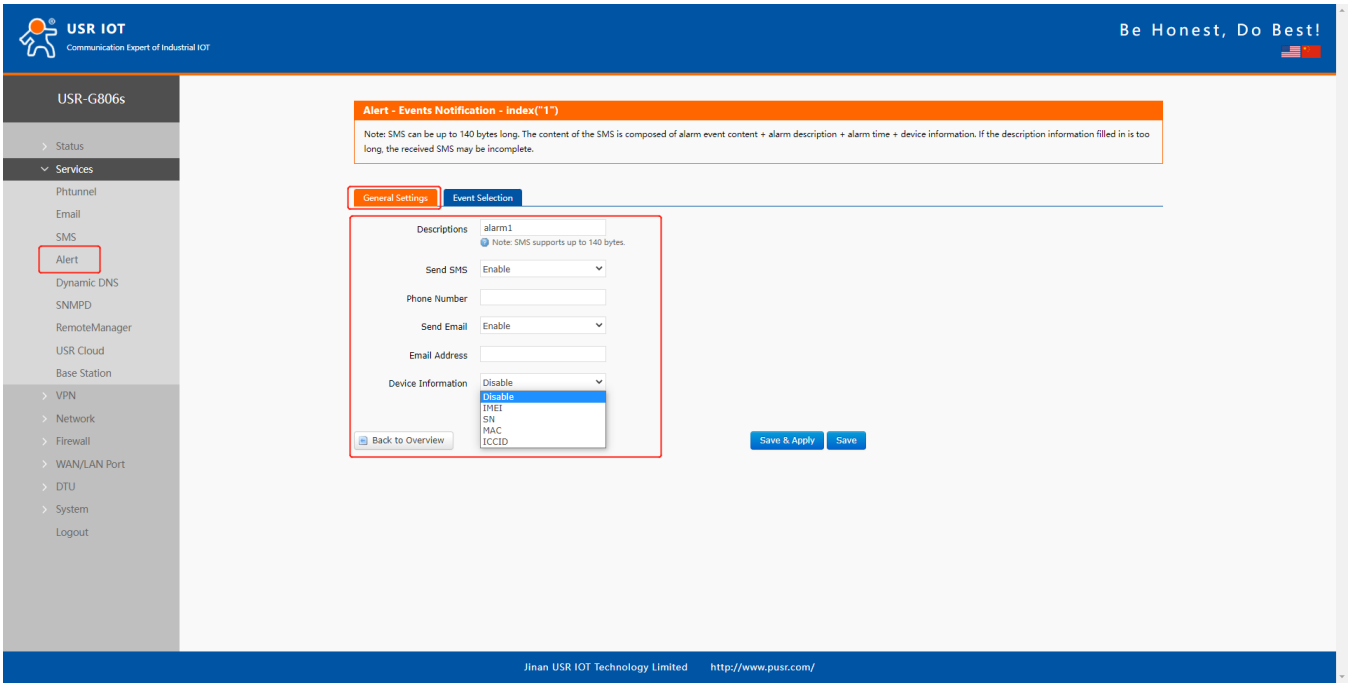
Item	Description	Default
Description	Alarm content	alarmx
Send SMS	Disable/Enable	Disable
Phone number	Phone number to receive the alarm message	Null
Send email	Disable/Enable	Disable
Email address	Email address to receive the alarm message, please set the correct email information in **Email** interface before using it.	Null
Device information	Disable/IMEI/SN/MAC/ICCID	Disable
Event	6 event status	Uncheck

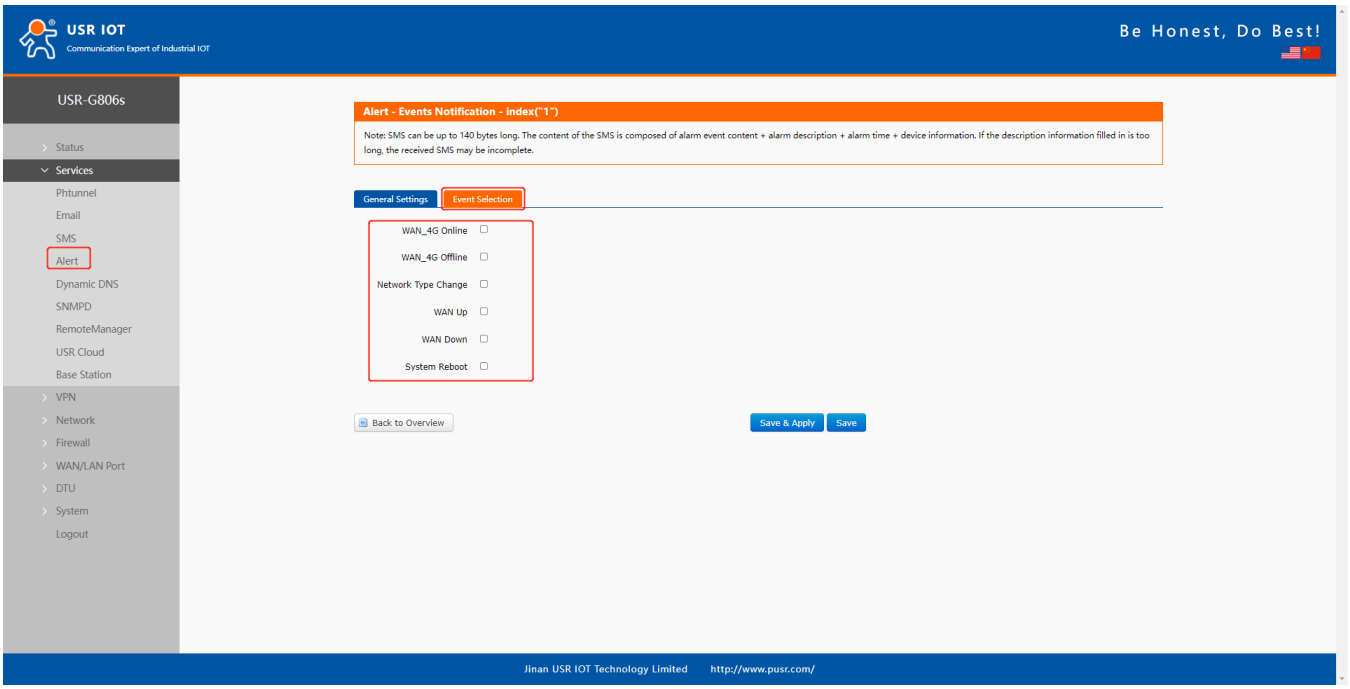
Description:

- SMS supports up to 140 bytes, including the description, event, time and the message. Do not make the description too long to avoid receiving incomplete messages.
- Please ensure the device has connected to the 4G network and the SIM card supports SMS function before sending SMS.
- Please ensure the device has connected to the network before sending email.
- WAN-4G online: Alarm after successful 4G networking.
- WAN-4G offline: Alarm after connecting to the 4G network again.
- Network type change: Alarm when changing the network type.
- WAN up: Alarm when connecting to wired network.
- WAN down: Alarm when the wired network disconnect.
- System reboot: Alarm if the device restart without power off.

Add an alert rule.

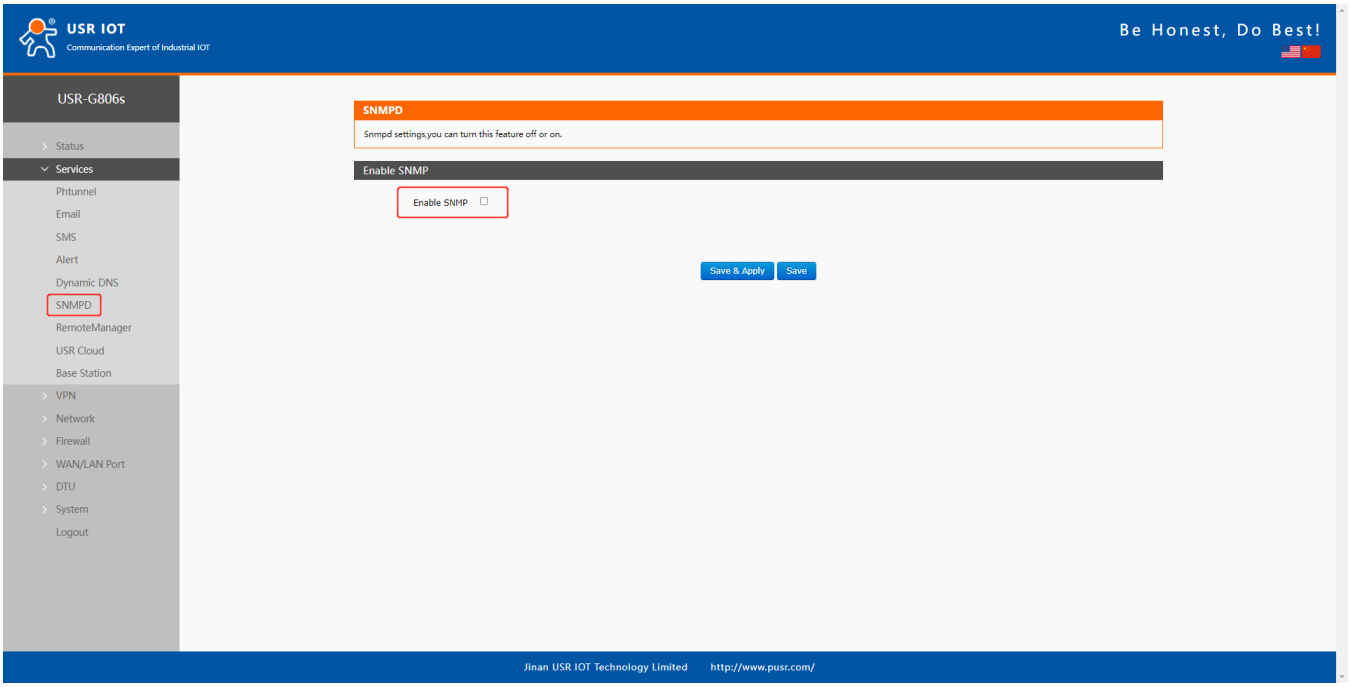






7.4. SNMPD

USR-G806s supports simple SNMP protocol. This function is default to be disabled.

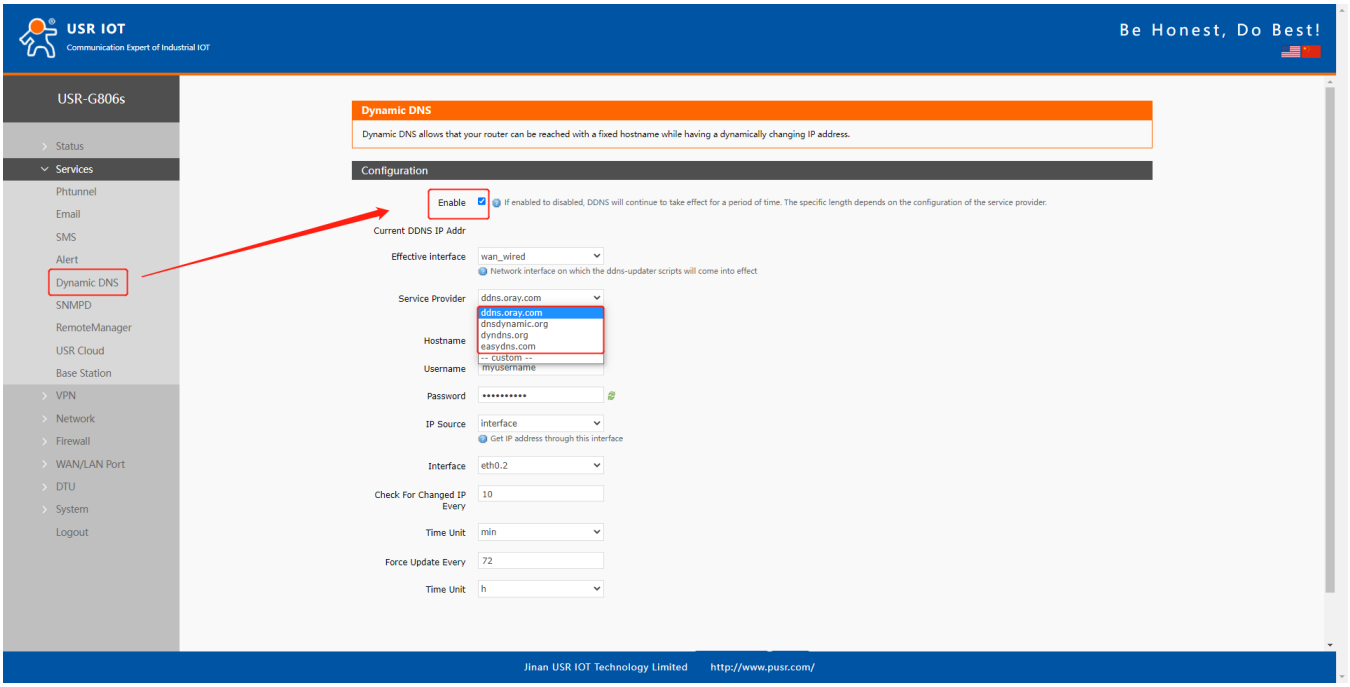


7.5. DDNS

DDNS function allows remote access to the router directly through the domain Item instead of your dynamic IP address, which changes from time to time.

7.5.1. Supported Services

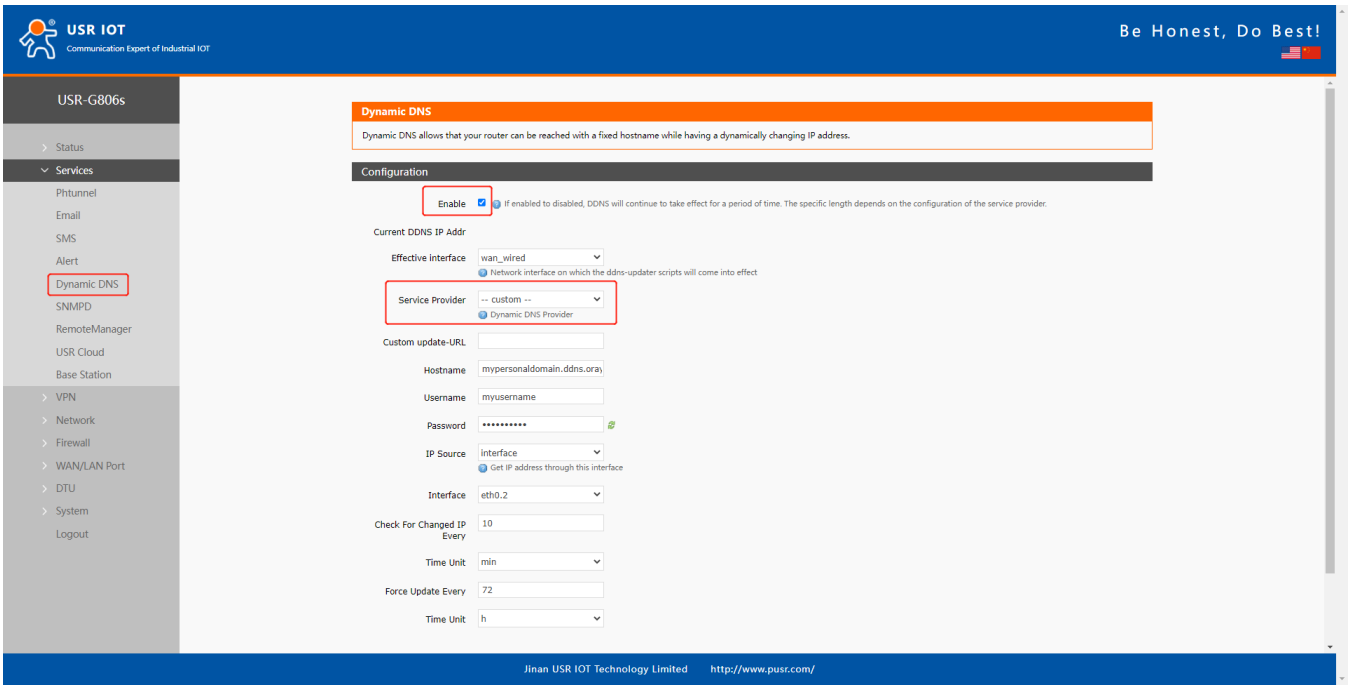
If you are using the DNS service provider can be found in **Services Provider** drop-down box, please configure like below:



Item	Description	Default
Enable	On/Off	Off
Effective interface	lan/wan_wired/wan_4g	wan_wired
Service Provider	DDNS server address	ddns.oray.com
Hostname	Enter the hostname provided by the DDNS server.	mypersonaldomain.dyndns.org
Username	Enter the username provided by the DDNS server	myusername
Password	Enter the password provided by the DDNS server	mypassword
IP Source	Network/Interface/URL	Interface
Interface	eth0.2/eth1	Eth0.2
Check for changed IP every/unit	The interval at which IP address changes are detected. The IP binding of the domain name may change frequently, and the lower the value, the more frequent the detection.	10 min
Force update every/unit	The time interval for forced updates.	72 h

7.5.2. Custom Services

If you are using the DNS service provider can not be found in **Service Provider** drop-down box, please select “Custom”, then configure like below:



Here we use “ddns.oray.com” as an example, the hostname is “1a516r1619.iask.in”, username is “ouclihuibin123”, password “ouclihuibin123”.

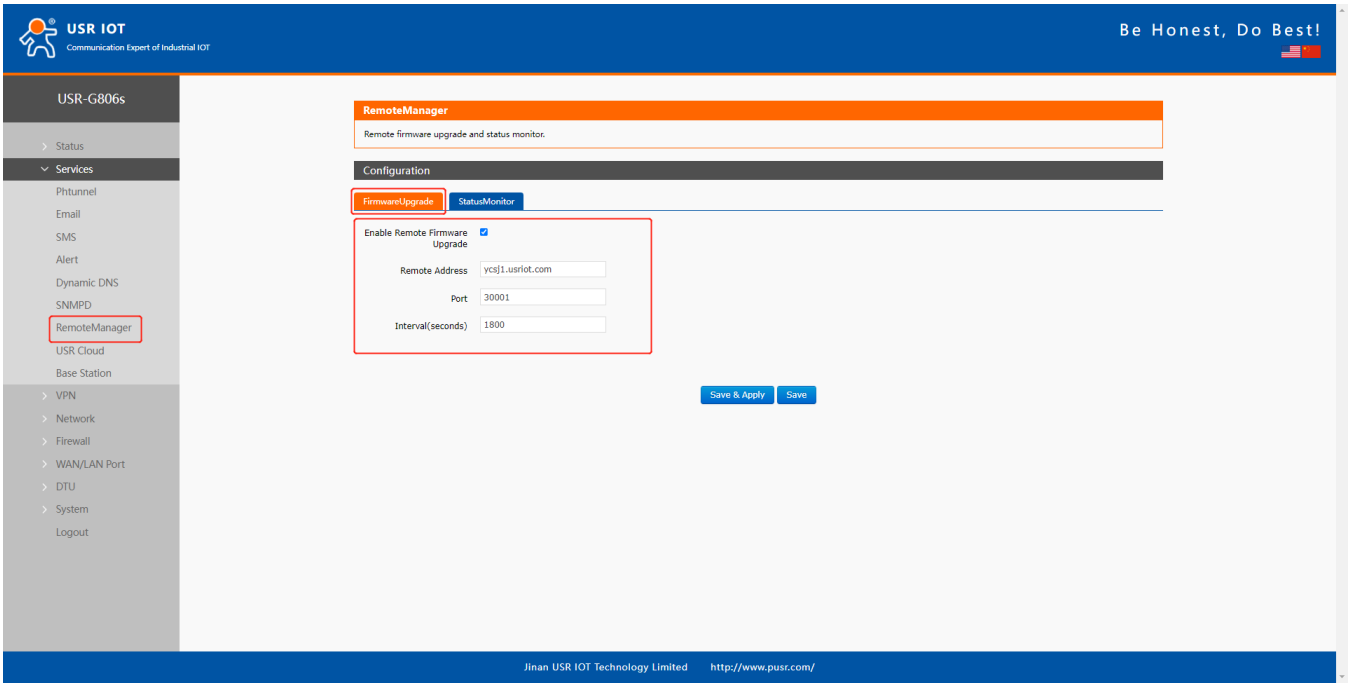
Item	Description	Default
Enable	On/Off	Off
Effective interface	lan/wan_wired/wan_4g	wan_wired
Service Provider	Custom	---
Custom update-URL	DDNS server address, here we take “ddns.oray.com” as an example. Please enter with the format of “http://username:password@ddns.oray.com/ph/update?hostname=hostname provided by the DDNS server”	Example: http://ouclihuibin123:ouclihuibin1231@ddns.oray.com/ph/update?hostname=1a516r1619.iask.in
Hostname	Enter the hostname provided by the DDNS server	Example: 1a516r1619.iask.in
Username	Enter the username provided by the DDNS server	Example: ouclihuibin123
Password	Enter the password provided by the DDNS server	Example: ouclihuibin123
IP Source	Network/Interface/URL	Interface
Interface	eth0.2/eth1	eth0.2
Check for changed IP every/unit	The interval at which IP address changes are detected. The IP binding of the domain name may change frequently, and the lower the value, the more frequent the detection.	10 min
Force update every/unit	The time interval for forced updates.	72 h

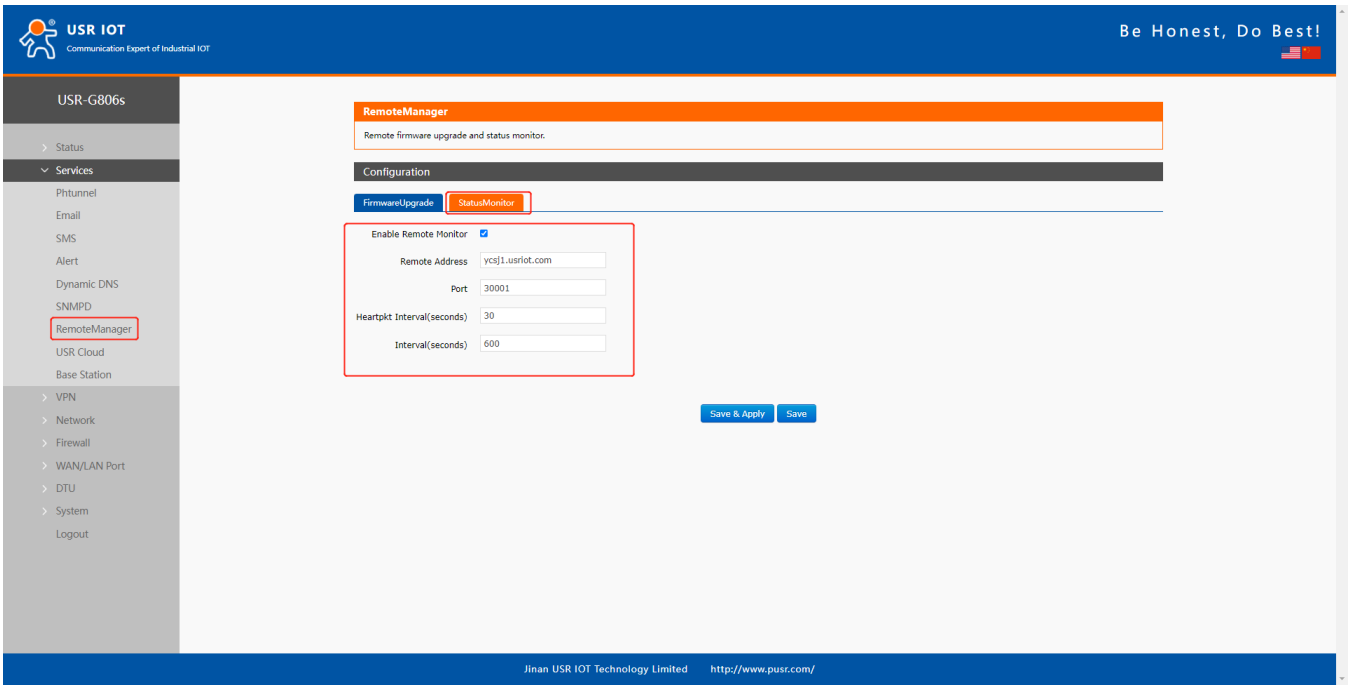
Note:

- After setting all parameters, please restart the device to take the parameters effect.
- Dynamic domain names work even if the router is in subnet.
- DDNS + port forwarding can realize remote access to the router subnet.
- This function requires to assign a separate public IP to the router's network.
- Multiple DDNS domain names can be added to this router.

7.6. Remote Manager

After enable **Remote Firmware Upgrade** and **Remote Monitor** function in G806s device, you can add it in our remote management platform **http://ycsj1.usriot.com/Public/login**. Please register and submit your account to technical engineers for authorization before using it.





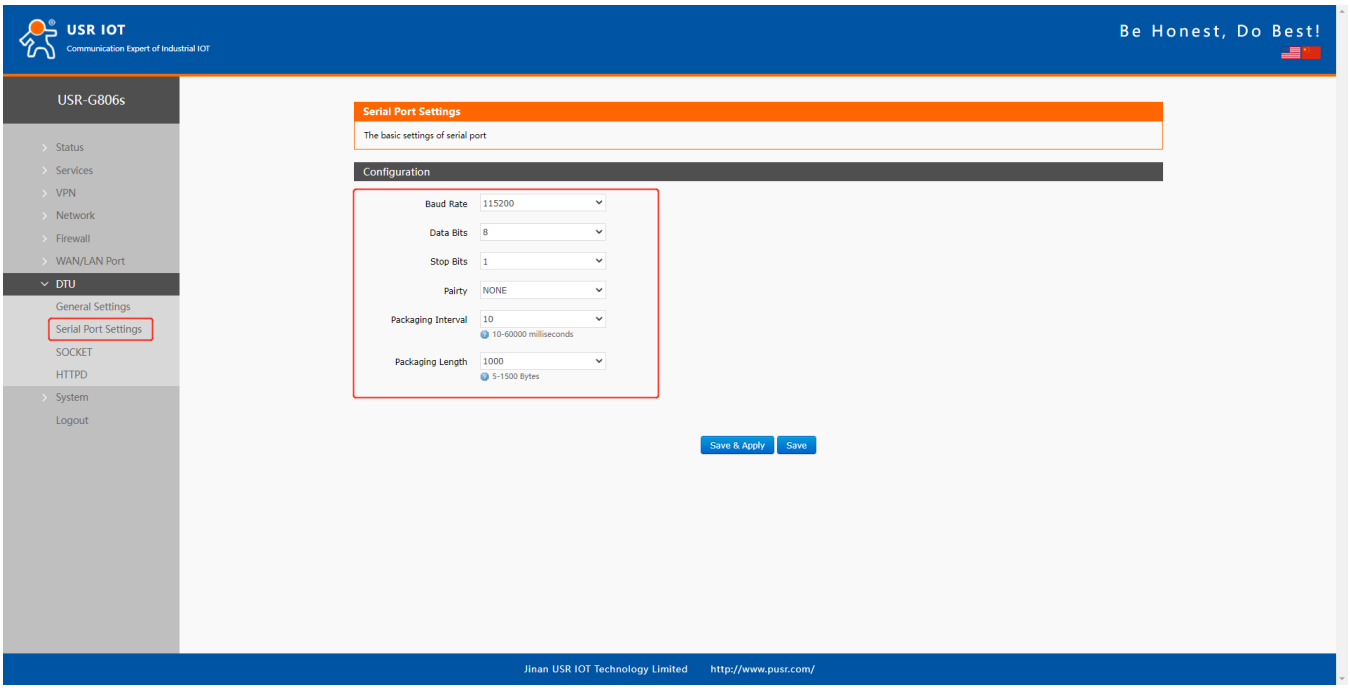
8. Serial Port

USR-G806s supports DTU function, which can achieve RS485 serial data transmission.

8.1. Serial Port Settings

8.1.1. Basic Settings

Serial parameters of USR-G806s must be consistent with the RS485 serial device. Otherwise, they cannot communicate with each other.

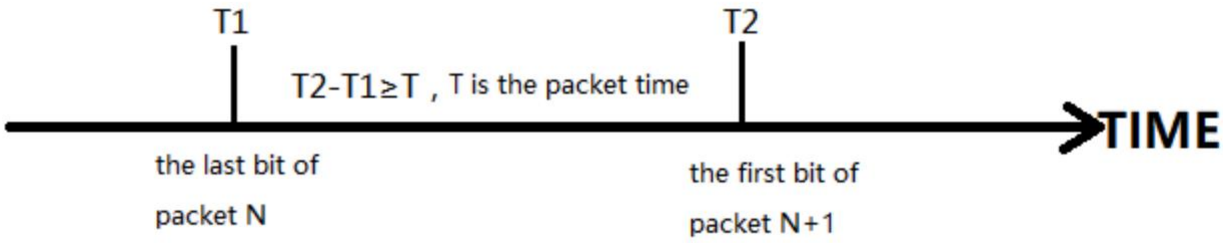


Item	Description	Default
Baud rate	Supports 1200/2400/4800/9600/19200/38400/57600/115200/230400	115200
Data bits	8	8
Stop bits	1 /2	1
Parity	NONE/ODD/EVEN	NONE
Packaging interval (ms)	10-60000	10
Packaging length(byte)	5-1500	1000

8.1.2. Framing Mechanism

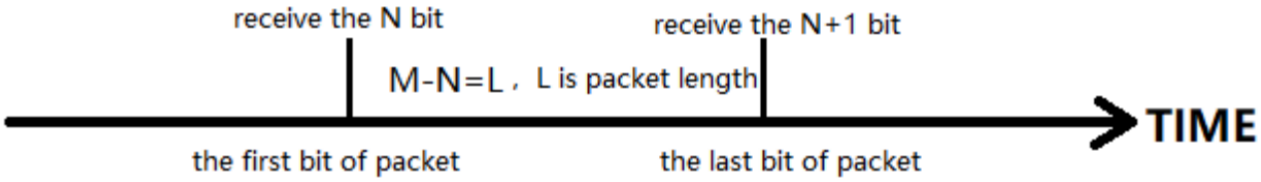
8.1.2.1. Time Trigger

When G806s receives data from the UART, it continuously checks the interval of two adjacent bytes. If the interval time is greater or equal to a certain "time threshold", then a frame is considered finished, otherwise the data is received until greater or equal to the packet length byte set (Defaults to 1000 bytes). This frame is sent to the network as a TCP or UDP packet. The "time threshold" here is the time between packages. The range of settable is 10ms~60000ms.Factory default: 10ms.
This parameter can be set by AT command, AT+UARTFT=<time>.



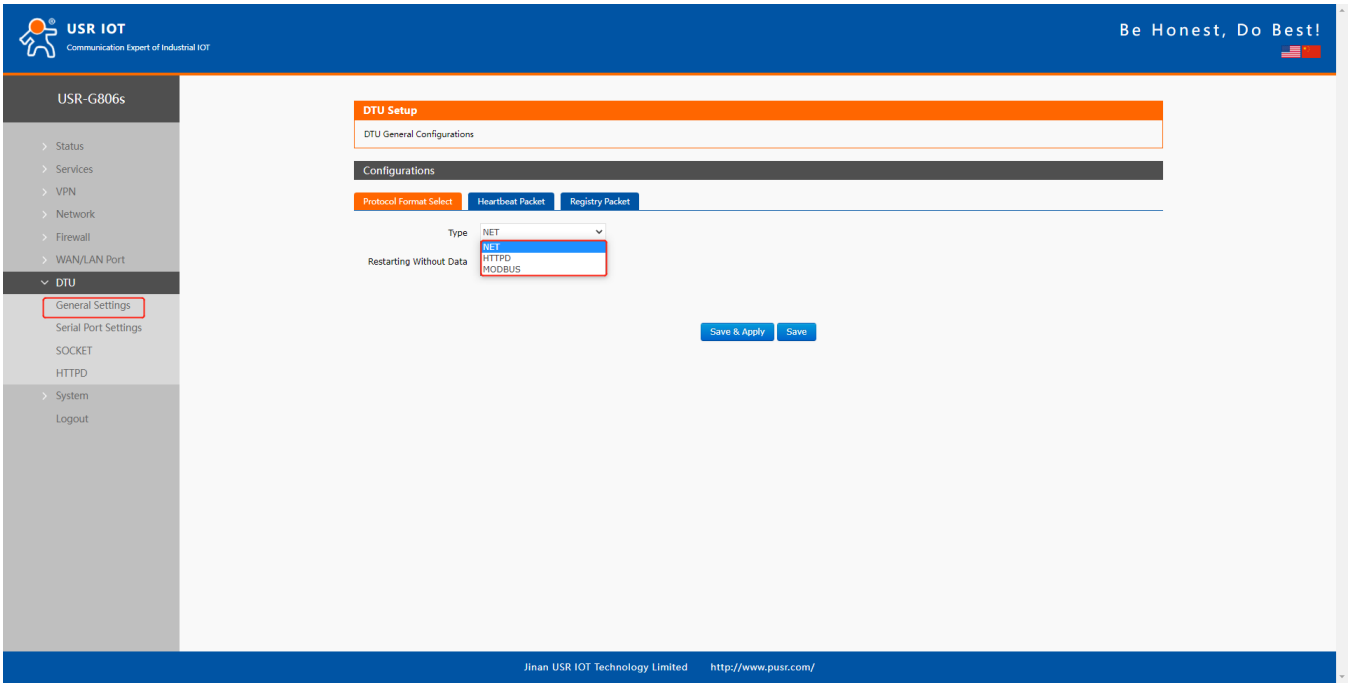
8.1.2.2. Length Trigger

When G806s receives data from the UART, it constantly checks the number of bytes received. If the number of bytes received is equal to a certain "length threshold", a frame is considered to have ended, then this frame is sent to the network as a TCP or UDP packet. The "length threshold" here is the package length. The settable range is 5~1500 bytes. Factory default 1000.
This parameter can be set by AT command, AT+UARTFL=<length>.



8.2. Operating Mode

USR-G806s supports three operating modes: NET(Transparent transmission), MODBUS(MODBUS RTU to MODBUS TCP), HTTPD(HTTP Client mode).



8.2.1. NET Mode

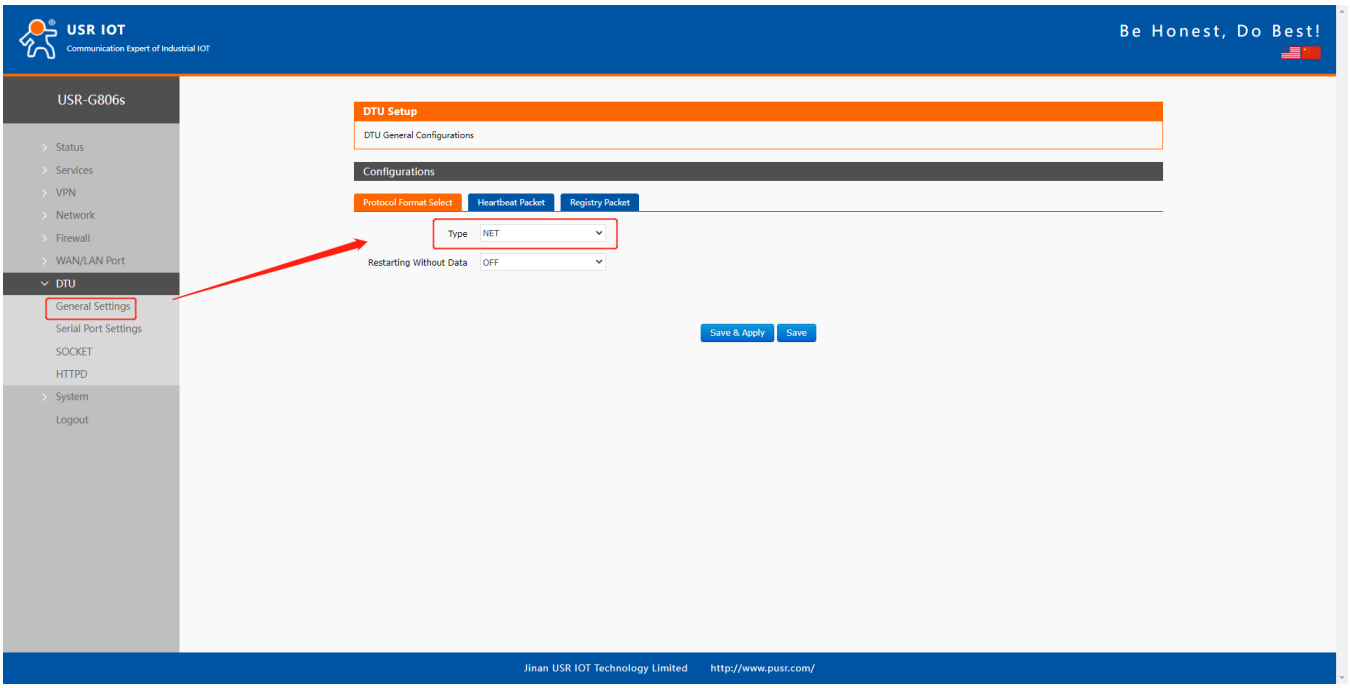
In this mode, user can achieve transparent data transmission between the serial device and the network server with simple parameter settings.

USR-G806s supports 4 socket connections, socket A~socket D, which are independent with each other.

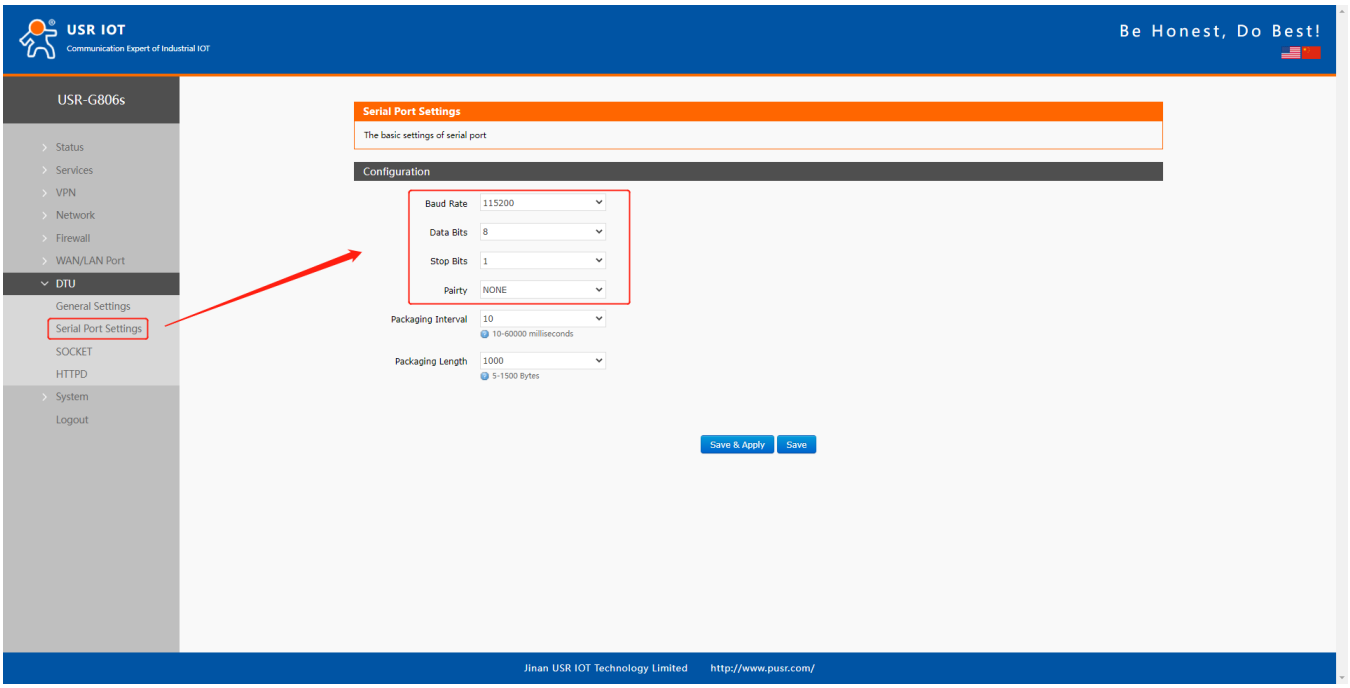
Socket A supports TCP client/TCP server, UDP client/server, socket B/C/D supports TCP client, UDP client/server.

Here we connect the RS485 port to the computer via a serial to USB adaptor to test:

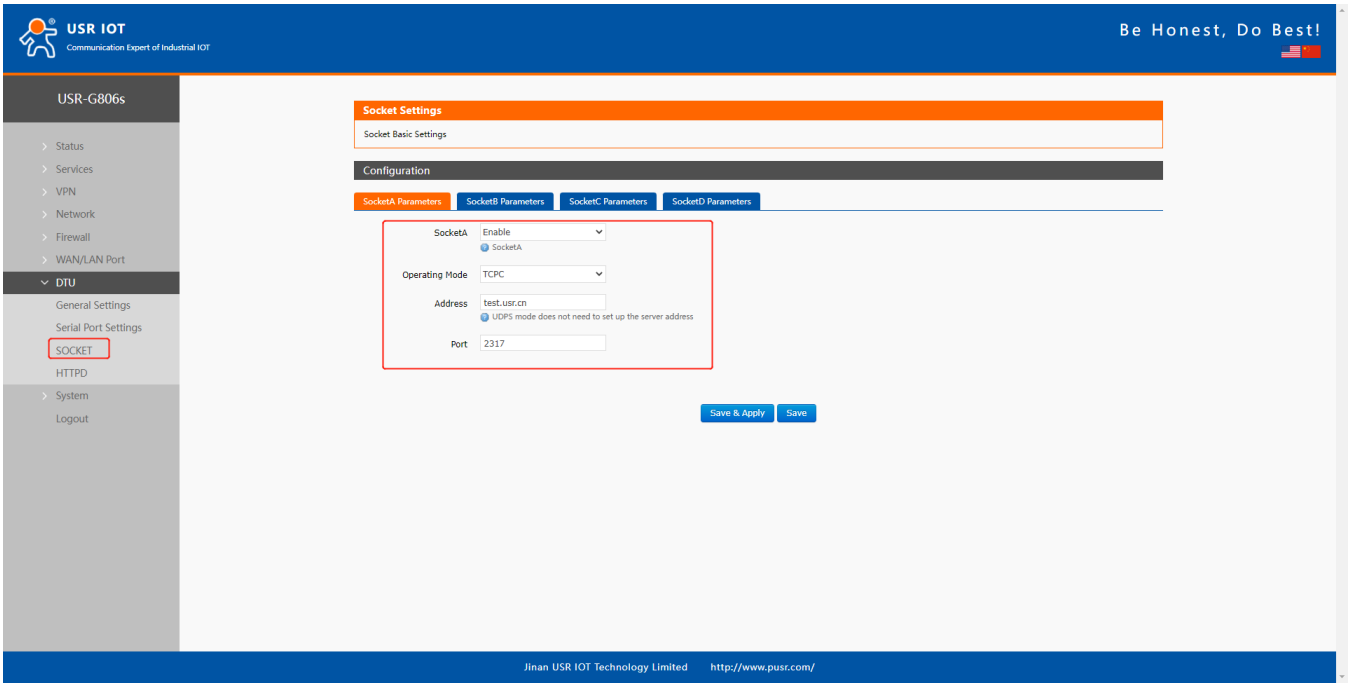
1. Set the operating mode to NET.



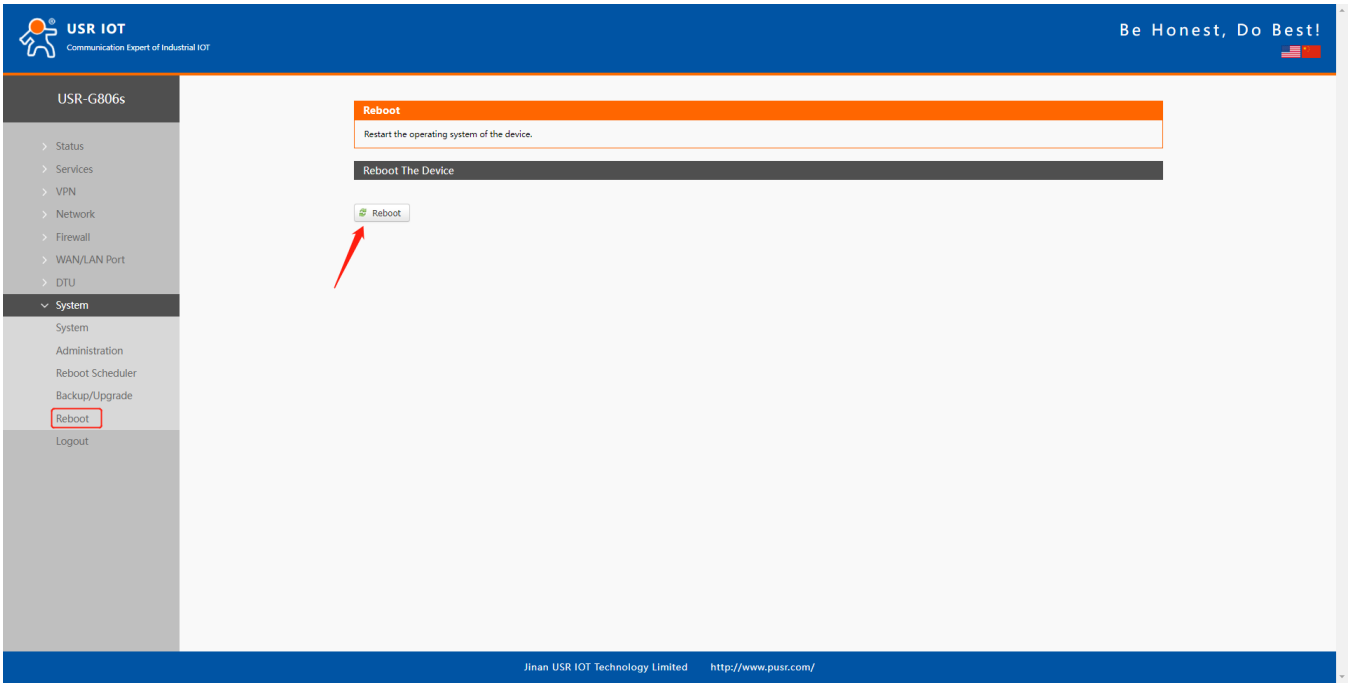
2. Set the serial port parameters.



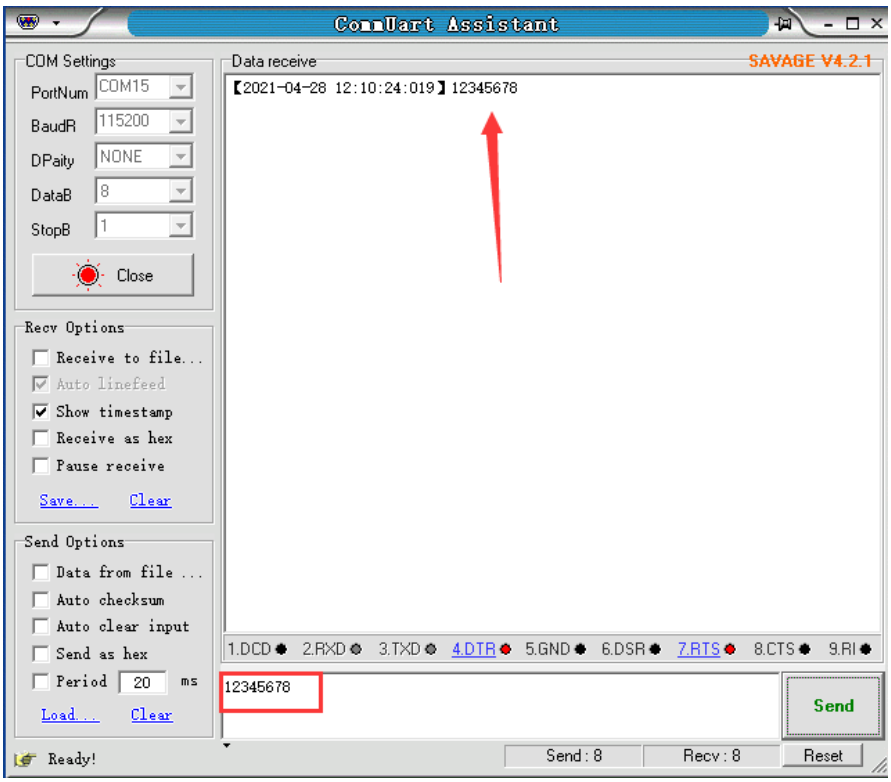
3. Set the device to TCP client, server address to test.usr.cn, port 2317.



4. After setting all parameters, restart the device to take the parameters effect.



5. After the device restarts, when we send data from the serial port, will receive the same data replied by the test server.

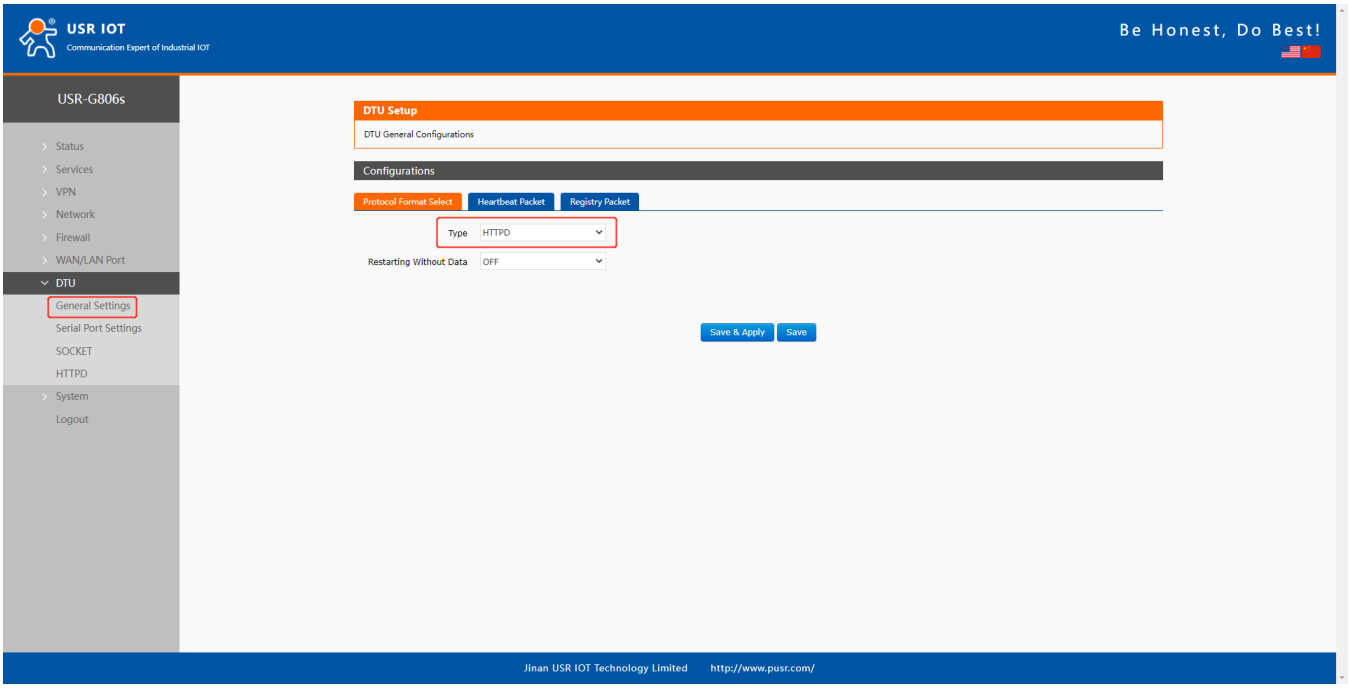


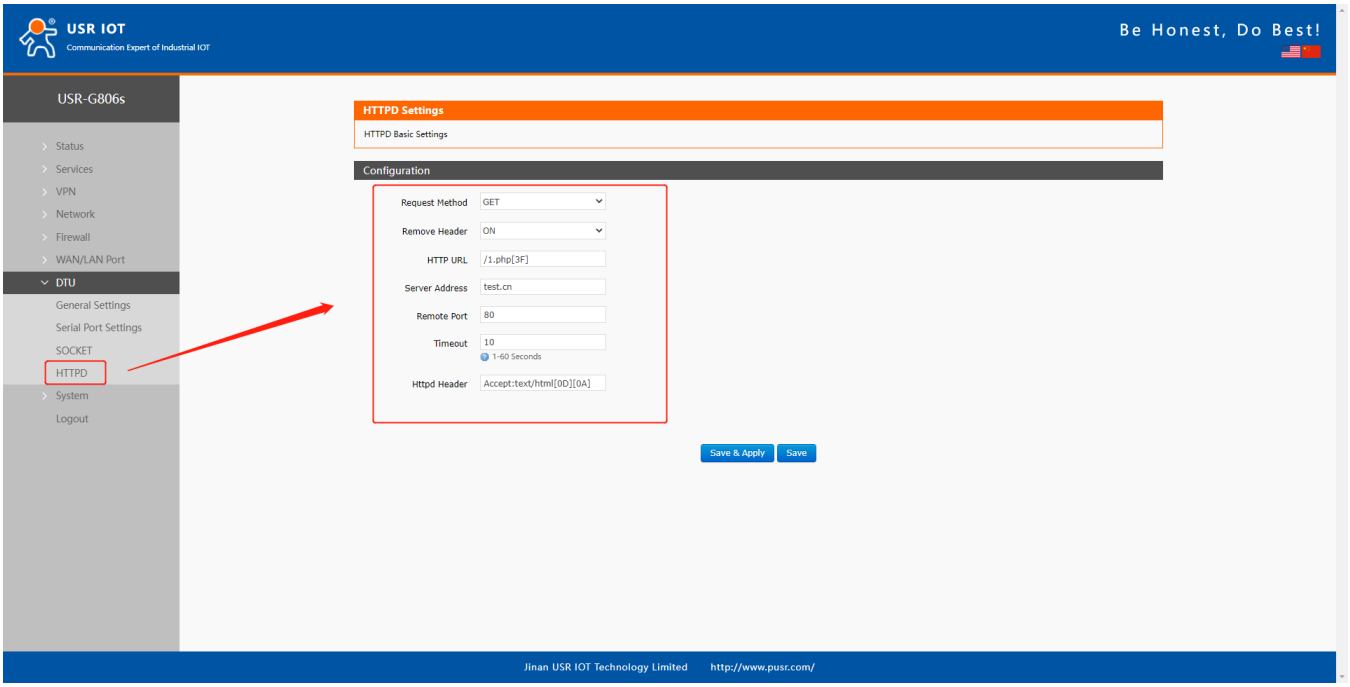
8.2.2. Modbus Mode

In this mode, USR-G806s can achieve bidirectional protocol conversion between serial MODBUS RTU data and network MODBUS TCP data.
MODBUS mode supports 4 socket connections, which are independent with each other.
Socket A supports TCP client/server, socket B/C/D only supports TCP client.

8.2.3. HTTPD Mode

In this mode, user's serial device can send request data to the HTTP server. USR-G806s will resolve the server data then send to serial device. It will remove the HTTP header of the server data by default, users can set whether to enable this function via AT commands.

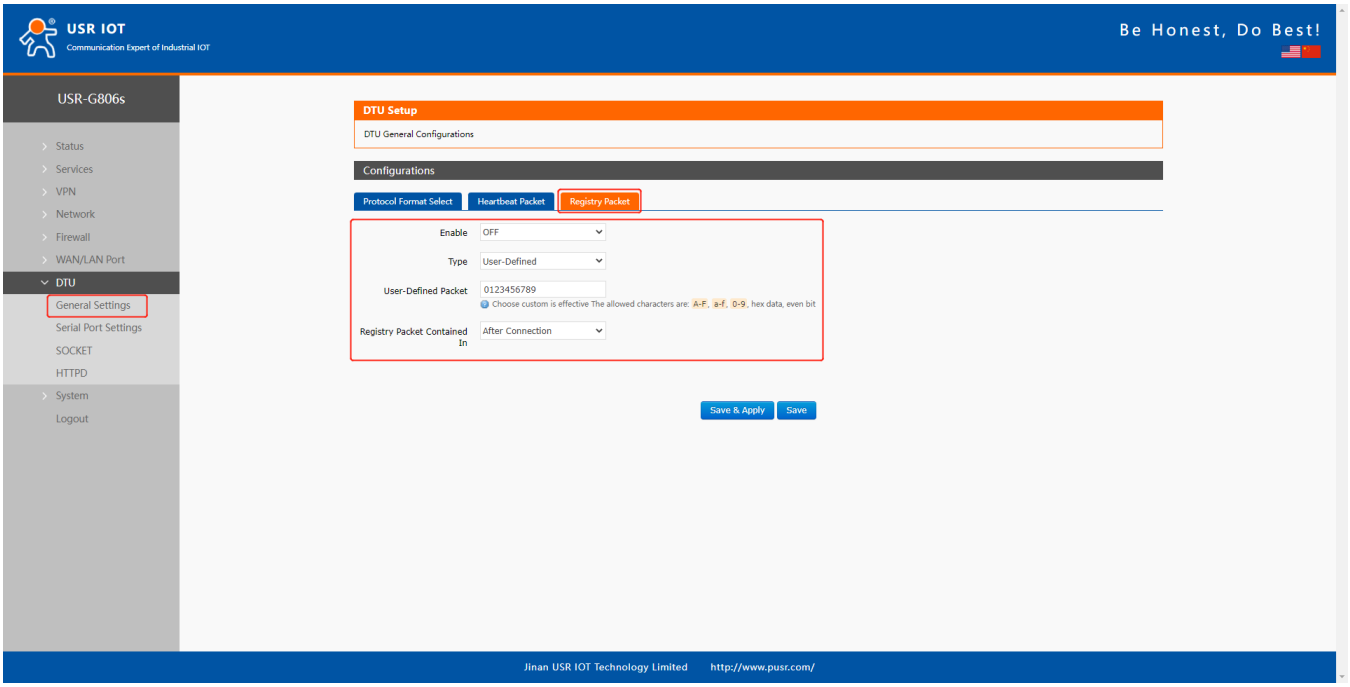




8.3. General Function

8.3.1. Registry Packet

Registry packet is intended to allow the server to identify the data from which device or to use it as a password to obtain authorization for the server's functions. Registry packet can be sent when the module establishes a connection with the server, or be added as the prefix of each data package. Registry packet data can be ICCID code, IMEI code, or User-defined data.

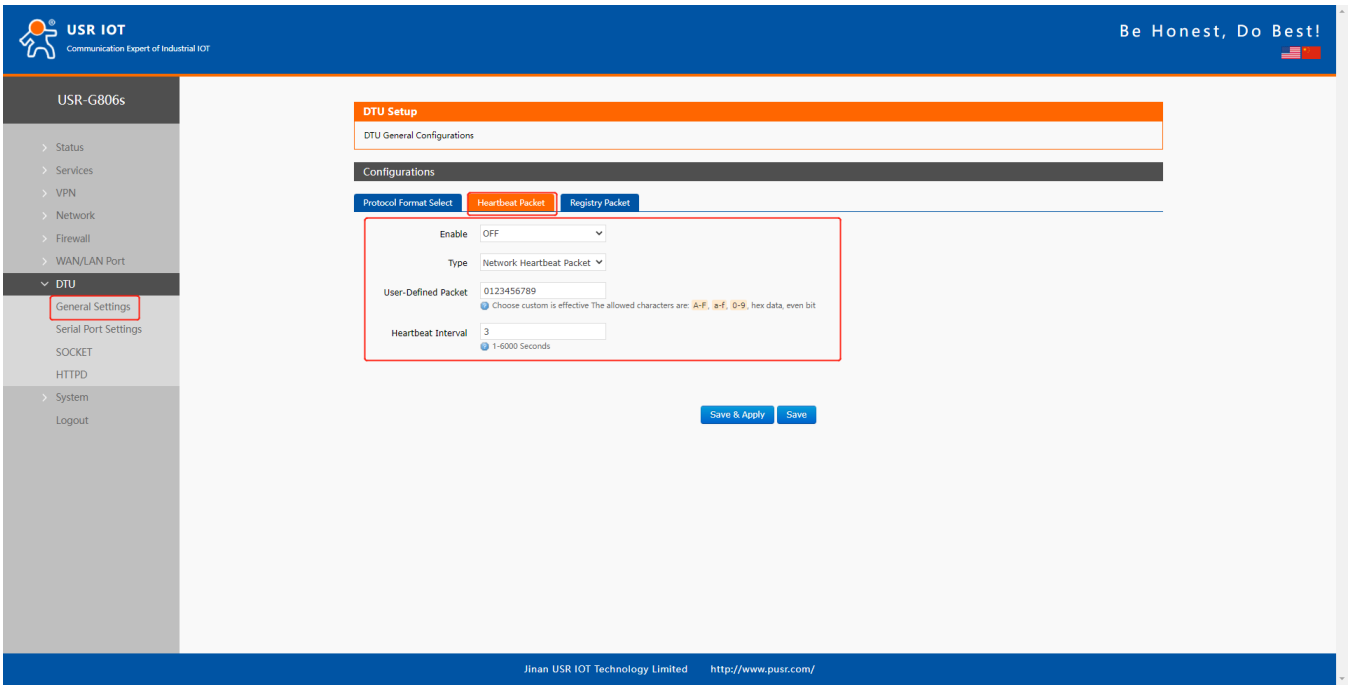


Item	Description	Default
Enable	ON/OFF	OFF
Type	IMEI, ICCID, USR Cloud, User-Defined	User-Defined
User-Defined packet	A-F, a-f, 0-9, hex data, even bit	0123456789
Cloud ID	Registry packet parameters of USR Cloud	SN code
Cloud psw	Registry packet parameters of USR Cloud	12345678
Registry packet contained in	After connection: Send once when establish a connection with the server. Prefix of data: Registry packet is added as the prefix of each data packet.	After connection

Note: Registry packet is only valid in TCPC, UDPC mode.

8.3.2. Heartbeat Packet

Heartbeat package can be sent to the network or serial port device. G806s defaults to send to the network to keep the connection stable and reliable.



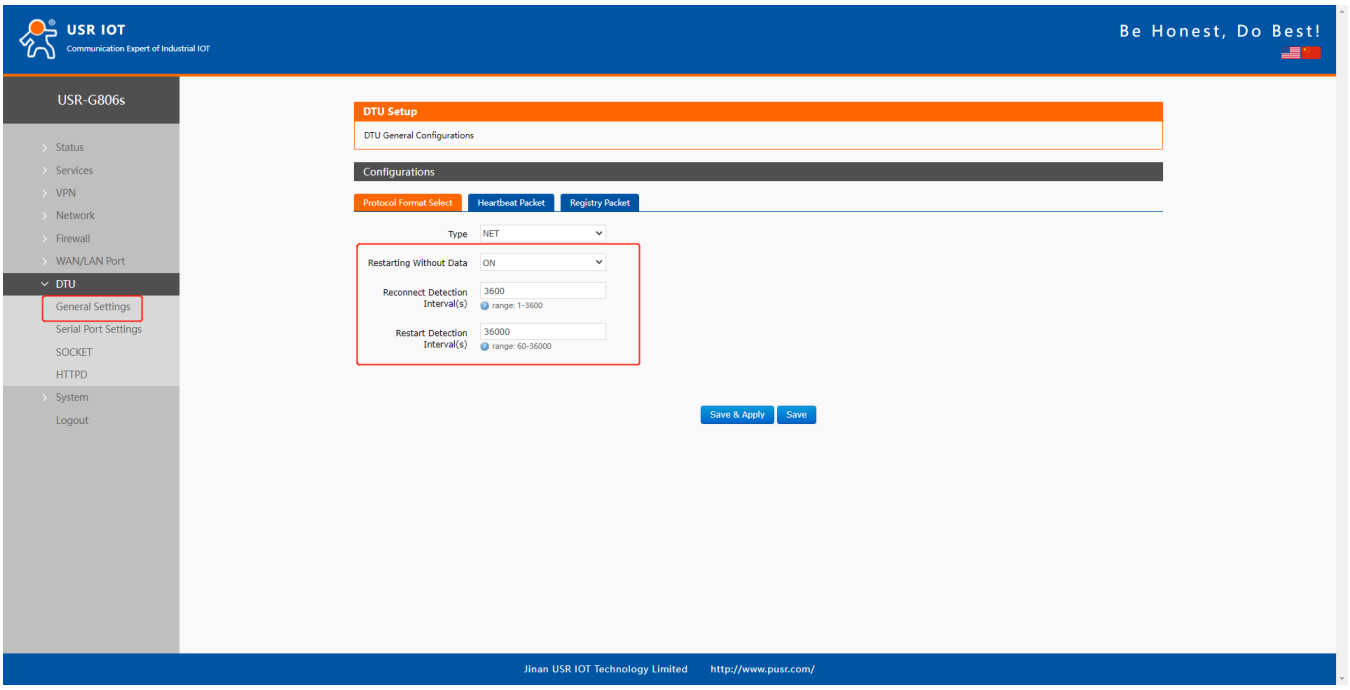
Item	Description	Default
Enable	ON/OFF	OFF
Type	Serial heartbeat packet/Network heartbeat packet	Network heartbeat packet
User-defined packet	A-F, a-f, 0-9, hex data, even bit	0123456789
Heartbeat interval (s)	1-6000s	3

Note: Heartbeat packet is only valid in TCPC, UDPC mode.

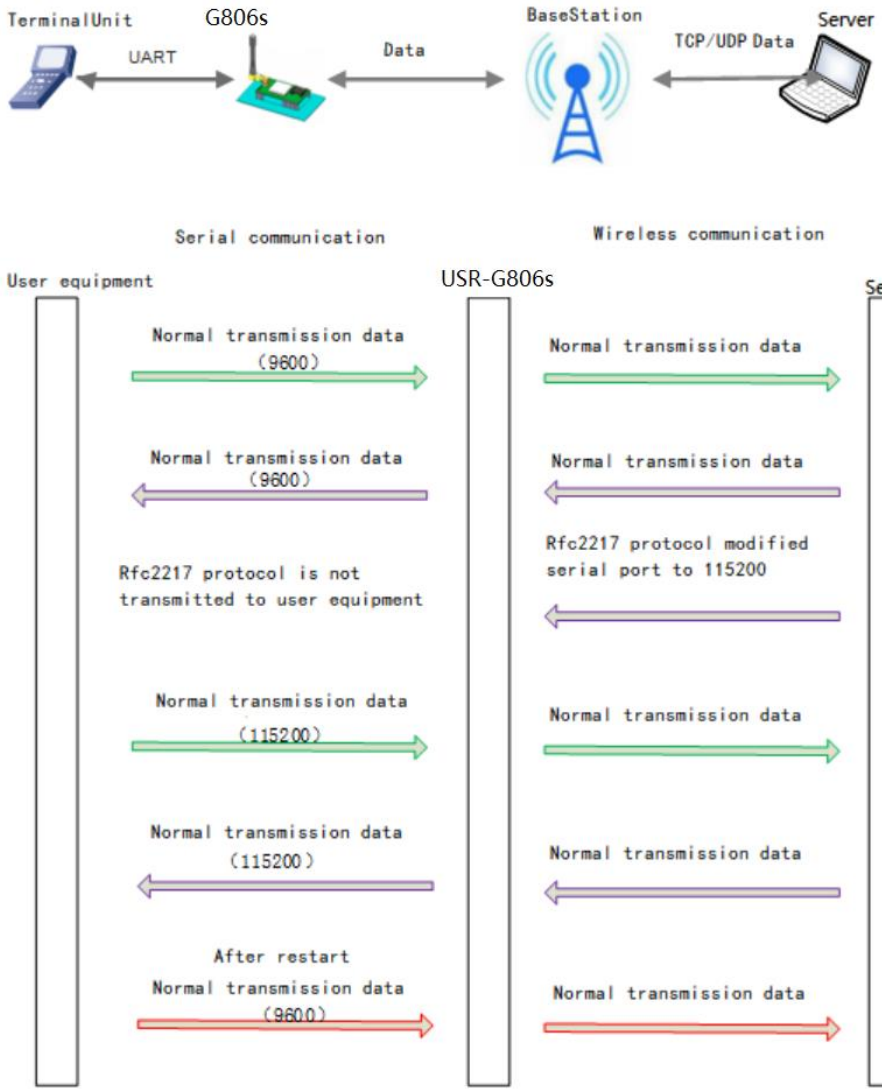
8.3.3. Restarting without Data

This function defaults to be disabled. When it is enabled, the device can actively disconnect the connection with the server and reconnect when there is no data from network side within the reconnect detection interval, which can prevent pseudo-connection due to an abnormal socket disconnection.

When the time reaches the restart detection interval, the device will restart automatically to recover the connection.



8.3.4. RFC2217



This function is similar to RFC2217, when we send the specific protocol data from the network side, can change the serial parameters in real time. Parameters take effect immediately, but it will be restored to the original after restarting.

Protocol description:

The protocol length is 8 bytes in HEX:

Item	Header	Baud rate	Bit	Parity
Bytes	3	3	1	1
Description	3 bytes reduce misjudgment	A baud rate value, high first	Please check below table	Parity of the first four digits, ignoring carry.

Example: (115200,N,8,1)	55 AA 55	01 C2 00	83	46
Example: (9600,N,8,1)	55 AA 55	00 25 80	83	28

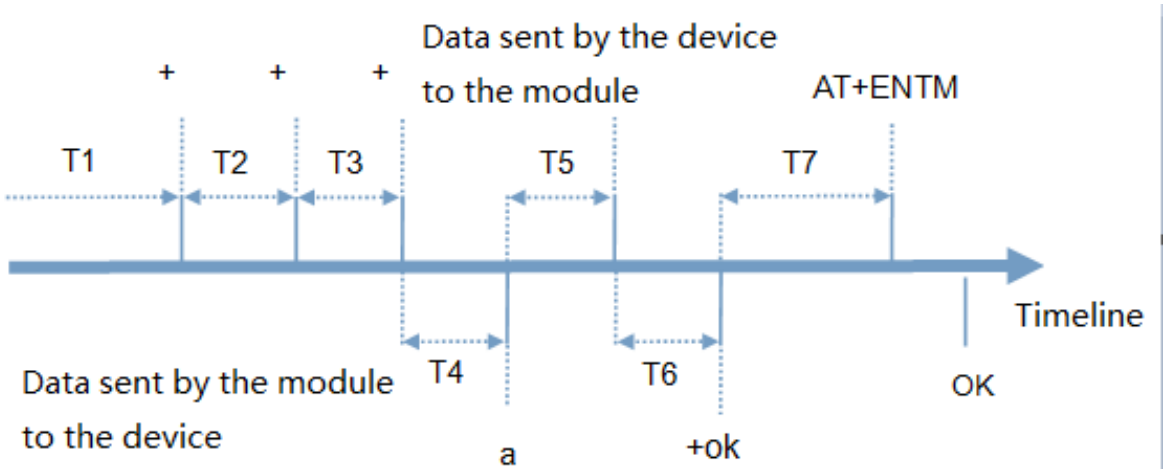
Bit	Description	Value	Description
1:0	Data bit	00	5
		01	6
		10	7
		11	8
2	Stop bit	0	1
		1	2
3	Parity	0	Disable
		1	Enable
5:4	Parity type	00	ODD
		01	EVEN
		10	Mark
7:6	NC	00	0

Note: This function needs to be enabled via AT command: AT+RFCEN.

9. AT Commands

9.1. AT Command Mode

When the device works in network transparent mode or HTTP mode, can switch to "AT command mode" by sending time-specific data by serial port. When the operation is completed in "AT command mode", send specific commands to return to the previous working mode.



Toggles the timing of command mode:

In the figure above, the horizontal axis is time, data above the time axis is sent by the serial device to G806s, data below the time axis is sent by G806s to the serial port.

Time requirement:

T1 > current serial port packaging interval

T2 < current serial port packaging interval time

T3 < current serial port packaging interval time

T4 = current serial port packaging interval time

T5 < 3 s

T6 = current serial port packaging interval time

The time sequence of switching from transparent mode/HTTP mode to “AT Command mode” :

1. Serial device continuously sends "+++" to the device. After receiving "+++", the device will send an "a" to the serial device. No data can be sent during a packaging cycle before sending "+++".
2. When the serial device receives “a”, a “a” must be sent to the device within 3 seconds.
3. After receiving 'a', the device returns "+ok" and enter “temporary command mode”.
4. After receiving "+ok", the device has enter "temporary command mode" and now can send AT command to it.

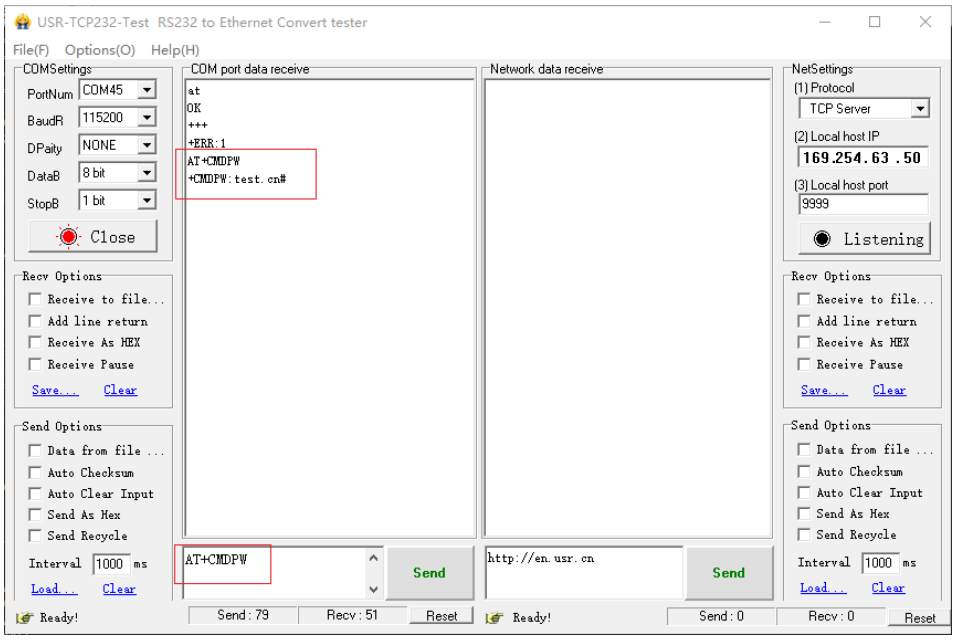
Time sequence of switching from AT command mode to transparent mode.HTTP mode:

1. Serial device sends "AT+ENTM" to G806s.
2. After receiving the command, sends "OK" to the serial device and returns to the previous working mode.
3. After the serial device receives "OK", it knows that the device has returned to its previous working mode.

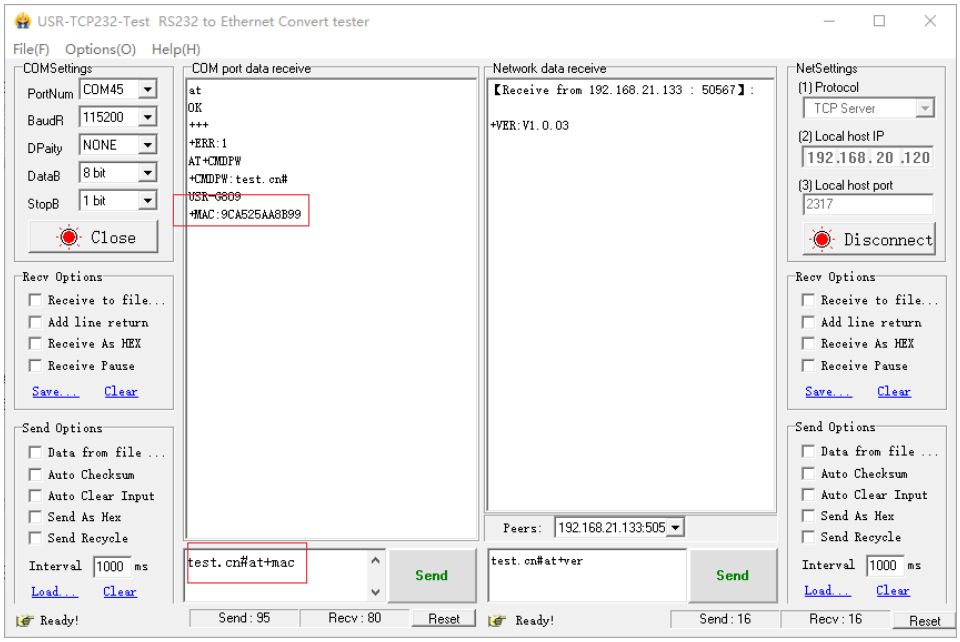
9.2. Serial AT Commands

In transparent mode, do not need to switch to the command mode, we can use “Command password + AT command” to query and set parameters. It does not need complicated “+++” timing sequence to enter AT command mode, so as to quickly query or set parameters.

Before sending, enter AT command mode, query the command password firstly. It defaults to “test.cn#”. Restart the device after setting.

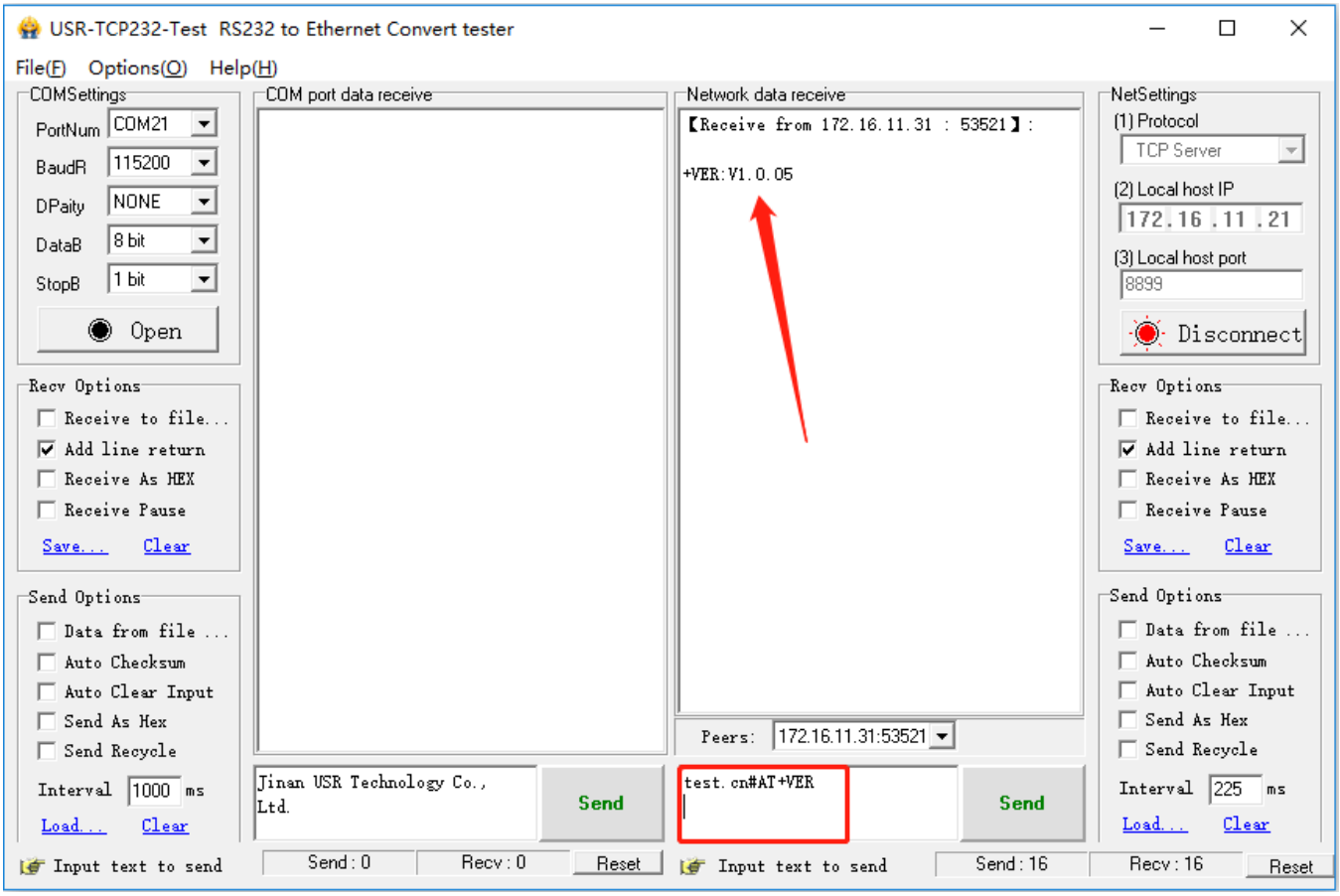


Send “test.cn#AT+MAC” from the serial port (there is an “Enter” after the command), then can receive the response from the device:



9.3. Network AT Commands

Network AT command refers to set and query parameters by sending “Command password + AT command” through the network when working in transparent mode. Here we query the firmware version of the device, there is an “Enter” after the command.



9.4. SMS AT Commands

In transparent mode, we can also send SMS to query and set the device parameters. Here we send “Command password+AT Commands” to query the socket connection status.

For detailed AT Commands, please refer to **AT Command set**.