

4G Industrial Router Pioneer

USR-G806p

Manual



Be Honest & Do Best

Your Trustworthy Smart Industrial IoT Partner

Content

| | |
|--|----|
| 1. Product introduction | 5 |
| 1.1. Product features | 5 |
| 1.2. Hardware interface diagram | 7 |
| 1.3. Size description | 8 |
| 2. Operation Instruction | 9 |
| 2.1. Test | 9 |
| 3. Network interface function | 10 |
| 3.1. Cellular networks | 11 |
| 3.1.1. Cellular network configuration | 11 |
| 3.1.2. SIM | 13 |
| 3.1.3. SIM card information | 14 |
| 3.2. LAN | 15 |
| 3.2.1. DHCP | 16 |
| 3.2.2. VLAN | 16 |
| 3.2.3. WAN/LAN Select | 17 |
| 3.2.4. DHCP | 18 |
| 3.3. WAN | 18 |
| 3.3.1. DHCP | 19 |
| 3.3.2. Static IP mode | 20 |
| 3.3.3. PPPoE | 20 |
| 3.4. Network switching | 21 |
| 3.5. Wireless configuration | 22 |
| 3.6. Wireless client | 23 |
| 3.7. Static routing | 25 |
| 3.8. Network diagnostic function | 27 |
| 3.9. TCPDUMP traffic monitoring | 27 |
| 4. VPN function | 28 |
| 4.1. PPTP Client | 28 |
| 4.2. L2TP Client | 31 |
| 4.3. IPSec | 33 |
| 4.4. OpenVPN | 35 |
| 4.4.1. OpenVPN TAP bridge example | 43 |
| 4.4.2. An example of subnet interworking in OpenVPN TUN mode | 47 |
| 4.5. GRE | 52 |
| 5. Firewall | 53 |
| 5.1. Basic Settings | 53 |
| 5.2. Communication rules | 54 |
| 5.2.1. IP address blacklist | 55 |
| 5.2.2. IP address whitelist | 57 |

| | |
|--|----|
| 5.3. NAT function | 59 |
| 5.3.1. IP address spoofing | 59 |
| 5.3.2. SNAT | 60 |
| 5.3.3. DNAT | 63 |
| 5.3.4. Port forwarding | 64 |
| 5.3.5. NAT DMZ | 65 |
| 5.4. Access restrictions | 66 |
| 5.4.1. Domain blacklists | 67 |
| 5.4.2. Domain name whitelist | 67 |
| 6. Service function | 68 |
| 6.1. Dynamic domain name resolution (DDNS) | 68 |
| 6.1.1. Supported services | 68 |
| 6.1.2. DDNS come into force | 69 |
| 6.1.3. functional characteristics | 70 |
| 6.2. SSH Port | 70 |
| 6.3. SMS | 71 |
| 6.4. SNMPD | 72 |
| 6.5. GNSS | 73 |
| 7. Serial port server function | 74 |
| 7.1. Serial port Settings | 74 |
| 7.1.1. Time-triggered mode | 75 |
| 7.1.2. Length-triggered mode | 75 |
| 7.2. Communication configuration | 75 |
| 7.2.1. MQTT pattern | 76 |
| 7.2.2. Connect to the Amazon platform | 79 |
| 7.2.3. Connect to Ali Cloud platform | 81 |
| 7.2.4. HTTPD mode (HTTP Client mode) | 82 |
| 7.2.5. Registration packet/handshake packet function | 84 |
| 7.3. advanced setup | 84 |
| 8. system function | 86 |
| 8.1. host name | 86 |
| 8.2. Time Settings | 87 |
| 8.3. Username and password Settings | 87 |
| 8.4. HTTP port | 88 |
| 8.5. Parameter backup and upload | 88 |
| 8.6. factory data reset | 89 |
| 8.7. firmware upgrade | 89 |
| 8.8. restart | 90 |
| 8.9. Restart at regular intervals | 91 |
| 8.10. Daily record | 91 |
| 9. AT order set | 92 |
| 9.1. AT code repertory | 92 |

| | |
|---------------------------|-----|
| 9.1.1. AT order set | 95 |
| 10. Disclaimer | 130 |
| 11. Update log | 130 |

1. Product introduction

The USR-G806p is a flagship industrial router with 5 network ports, built on the industry-leading Qualcomm CPU solution. It features multiple hardware interfaces, including 5 network ports (1WAN + 1 LAN + 3 LAN), dual serial ports (1 RS232 + 1 RS485), Qualcomm enhanced WIFI, and GNSS positioning. Additionally, it supports dual external expansion cards, providing advanced internet connectivity and high-speed data access for terminals. Users can quickly set up their own application networks with this device, which also offers robust software support.

Designed for harsh industrial environments, this device meets industrial-grade standards and is designed for a wide temperature range of -40°C to 75°C. It operates on a wide voltage DC range of 9 to 48V, with hardware EMC protection up to Class 3B. The device has undergone rigorous professional environmental testing and features built-in dual watchdogs for software and hardware, as well as mechanisms for automatic fault recovery. These features ensure robust and reliable operation in various industrial settings, even in harsh and demanding environments.

The product is widely used in meteorological monitoring system, store cashier monitoring system, energy storage power station system, agricultural environment monitoring system, smart water system and other scenarios.

1.1. Product features

✧ **Stable and reliable**

- Industrial grade design: wide temperature -40°C~75°C, sheet metal shell, IP30 protection;
- Support horizontal desktop placement, wall hanging, rail installation;
- Wide voltage DC 9-48V input, with power reverse protection;
- Static electricity, surge, electric fast pulse group and other multiple hardware protection;
- Built-in hardware and software watchdogs, self-detection and self-repair of faults to ensure system stability.

✧ **Flexible networking**

- Provide 4G network system;
- Theoretical rate of cellular network: download: 150Mbps/uplink: 50Mbps
(interference exists in the real environment, so the actual measurement is taken as the standard);
- Support automatic network inspection, 4G/3G/2G mode switching, support APN/VPDN private network card
- Supports dual SIM cards;
- Support 3LAN+1WAN/LAN+1WAN, 10/100Mbps rate;
- Support network cable /4G/WIFI online at the same time, intelligent switching and backup function;
- Supports 2.4GHz WiFi band and supports AP/STA/routing modes;
- Support 1*RS232+1*RS485;

✧ Powerful

- Supports TCP/UDP/Modbus TCP to Modbus RTU/MQTT data acquisition capability;
- Support GPS positioning service;
- Support PUSR Cloud services to facilitate centralized management of device systems;
- Supports VPN (PPTP, L2TP, IPSec, OpenVPN, GRE) and supports VPN encryption function;
- Support dynamic domain name (DDNS), PPPoE, DHCP, static IP function;
- Supports firewall, NAT, black and white list access restrictions, and supports SNAT and DNAT functions;
- Support SSH, TELNET and Web multi-platform management and configuration;
- Support SNMP, VLAN division, SMS service and other diversified functions;
- Supports one-click restore factory Settings and hardware watchdog;

Tab 1 USR-G806p Specification parameters

| Project | | describe |
|----------|--|---|
| Cellular | Band (-GL) | TDD-LTE:Band 34/38/39/40/41 FDD-LTE: Band 1/2/3/4/5/7/8/12/13/18/19/20/25/26/28/66 WCDMA:B1/2/4/5/6/8/19 GSM/GPRS/EDGE: B2/3/5/8 |
| | Theoretical rate | The download speed of 150Mbps and the uplink speed of 50Mbps are affected by environmental interference, and the on-site measurement is taken as the standard |
| | Antenna interface | 1* Standard SMA-K antenna interface (outer screw and inner hole) |
| | SIM | 2*Nano-SIM |
| Ethernet | Number of network ports | 1* WAN, 1* WAN/LAN , 3* LAN |
| | Network port specifications | RJ45 interface: IEEE 802.3 compliant |
| | Network port rate | 10/100 Mbps adaptive, Auto MDI/MDIX |
| Wi-Fi | Wireless standards | IEEE 802.11b/g/n,2.4GHz, AP /STA/AP+STA/repeater |
| | Theoretical rate | 300Mbps; Note: The wireless rate is affected by the environment. Please measure it as the standard. |
| | MIMO | 2×2 |
| | Antenna interface | 2* Standard SMA-K interface |
| | Transmission distance | 500 meters; Note: The actual transmission distance depends on the field environment. Please measure according to the actual measurement. |
| DTU | SOCKET | TCP/UDP/Modbus TCP to RTU/MQTT/HTTPD/AWS/ALI Pass-Through/Modbus RTU |
| | Heartbeat packet / registration packet | Support |
| | Serial port baud rate | 1200/2400/4800/9600/19200/38400/57600/115200/230400 |

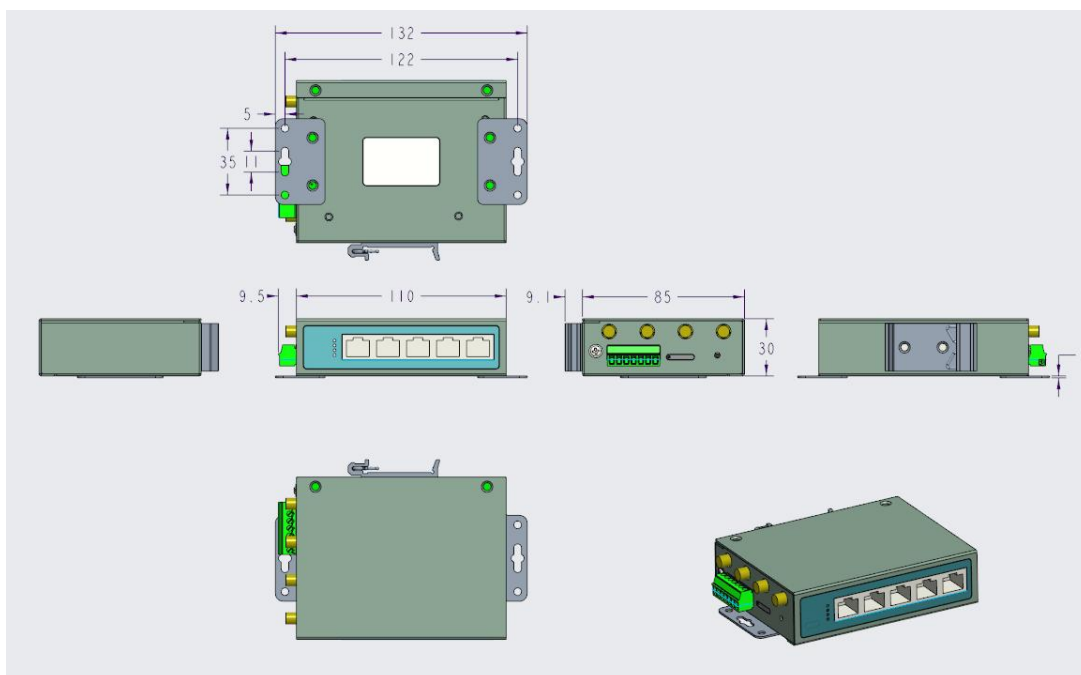
| | | |
|-----------------------------|---------------------|---|
| | data bit; | 7, 8 |
| | stop bit | 1, 2 |
| | check bit | NONE, ODD, EVEN |
| | Serial port type | 1*RS232、1*RS485 |
| pilot light; | PWR | The power indicator light is on after power on |
| | WIFI | WiFi light, which lights up when WiFi is turned on and working properly |
| | NET | Green-4G Orange-3G Red-2G |
| | SIG | Signal 25-31-Green Signal 15-25-Orange Signal 0-15-Red |
| Power supply specifications | adapter | DC 12V/1A |
| | Power | V+、V- 2p terminal, Anti-polarity protection is available |
| | Power supply range | DC 9-48V |
| | average current | < 500mA@12V |
| physical characteristics | hull | Sheet metal enclosure, IP30 |
| | Size | 110.0*85.0*30.0mm (L*W*H,) |
| | way to install | Hang ear installation, horizontal desk placement |
| | EMC | National standard 3B |
| | working temperature | -40°C~75°C |
| | Storage temperature | -40°C ~ 85°C |
| | Working humidity | 5%~95% (No condensation) |
| other | Reload | Support restore factory |
| | ground protection | Grounding screws |

1.2. Hardware interface diagram



Pic 1 USR-G806p Product interface diagram

1.3. Size description



Pic 2 USR-G806p View size diagram

2. Operation Instruction

2.1. Test

When the USR-G806p is used for the first time, you can connect the LAN port of the USR-G806p to the PC or connect to the WLAN wireless, and then configure it using the web management page.

Tab 2 Default parameter table for WEB pages

| parameter | default setting |
|-------------------|-----------------|
| SSID | USR-G806p-XXXX |
| LAN IP | 192.168.1.1 |
| User name | admin |
| password | admin |
| Wireless password | www.usr.cn |

USR-G806p English | 中文

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

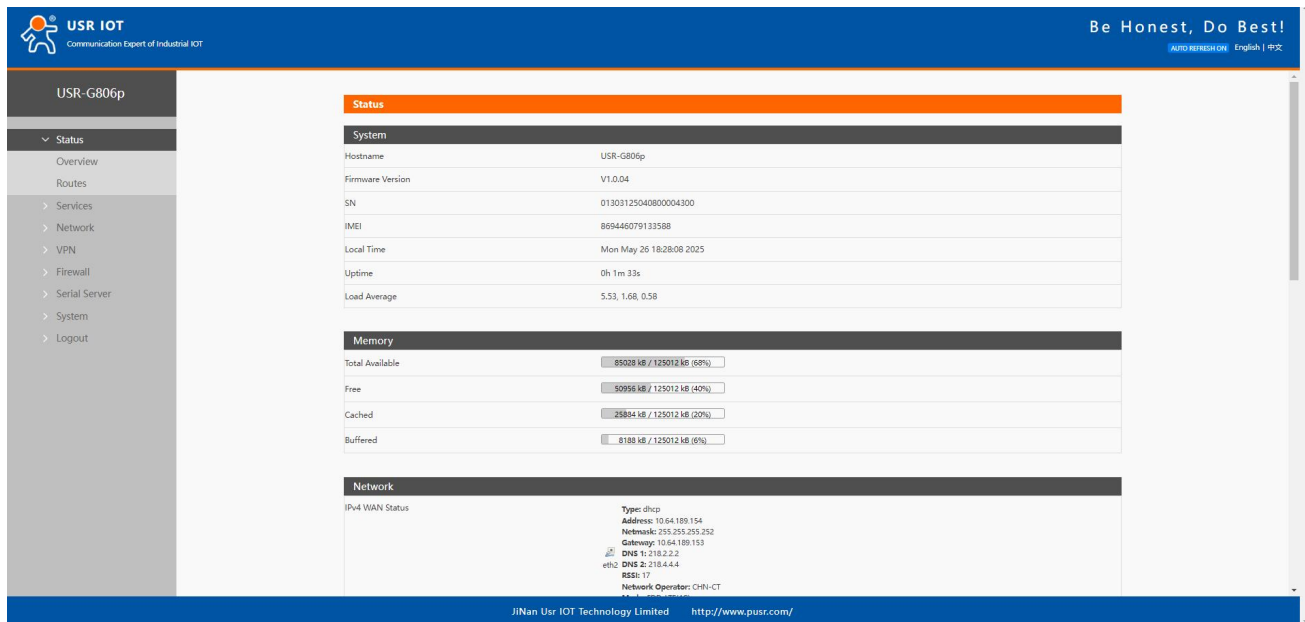
Authorization Required
Please enter your username and password.

Username:

Password:

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 3 Login page



USR-G806p

Status

System

| | |
|------------------|--------------------------|
| Hostname | USR-G806p |
| Firmware Version | V1.0.04 |
| SN | 0130312504080004300 |
| IMEI | 869446079133588 |
| Local Time | Mon May 26 18:28:08 2025 |
| Uptime | 0h 1m 33s |
| Load Average | 5.53, 1.68, 0.58 |

Memory

| | |
|-----------------|----------------------------|
| Total Available | 85028 KB / 125012 KB (68%) |
| Free | 50956 KB / 125012 KB (40%) |
| Cached | 25884 KB / 125012 KB (20%) |
| Buffered | 8188 KB / 125012 KB (6%) |

Network

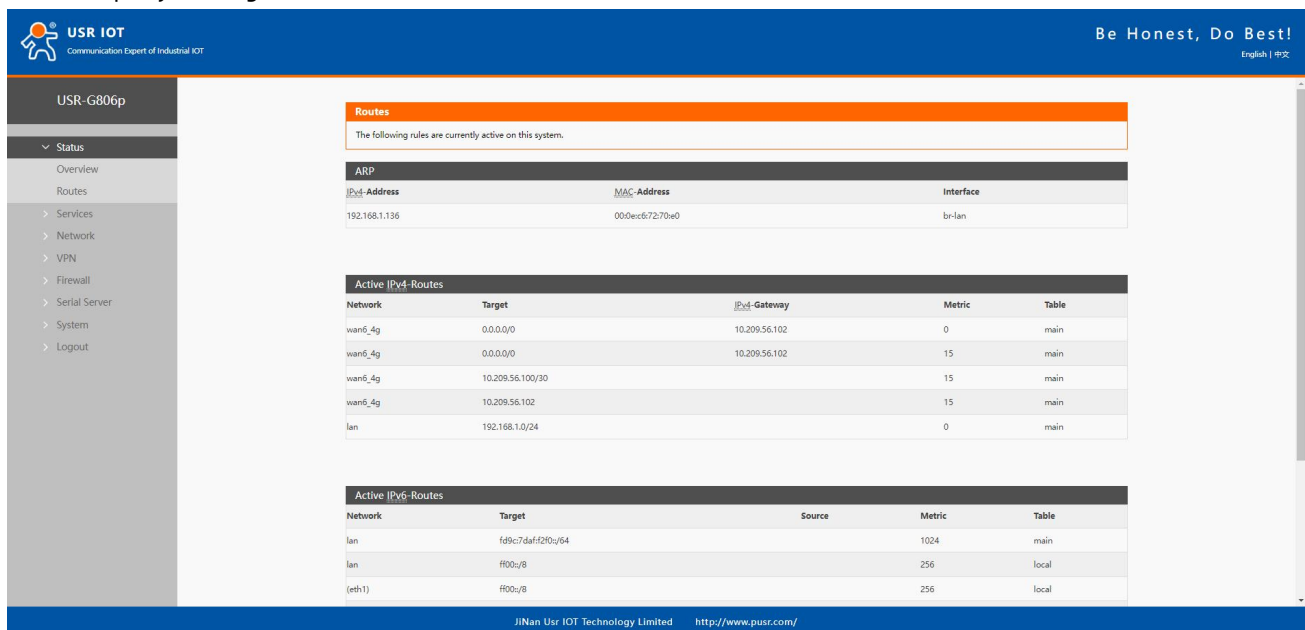
IPv4 WAN Status

| |
|---------------------------|
| Type: dhcp |
| Address: 10.64.189.154 |
| Netmask: 255.255.255.252 |
| Gateway: 10.64.189.153 |
| DNS 1: 218.2.2.2 |
| DNS 2: 218.4.4.4 |
| BSSID: 17 |
| Network Operation: CHN-CT |

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 4 Status overview

You can query routing information and ARP tables from here.



USR-G806p

Status

Routes

The following rules are currently active on this system.

ARP

| IPv4-Address | MAC-Address | Interface |
|---------------|---------------|-----------|
| 192.168.1.136 | 000ec67270be0 | br-lan |

Active IPv4-Routes

| Network | Target | IPv4-Gateway | Metric | Table |
|---------|------------------|---------------|--------|-------|
| wan6_4g | 0.0.0.0/0 | 10.209.56.102 | 0 | main |
| wan6_4g | 0.0.0.0/0 | 10.209.56.102 | 15 | main |
| wan6_4g | 10.209.56.100/30 | | 15 | main |
| wan6_4g | 10.209.56.102 | | 15 | main |
| lan | 192.168.1.0/24 | | 0 | main |

Active IPv6-Routes

| Network | Target | Source | Metric | Table |
|---------|------------------|--------|--------|-------|
| lan | fd9c7daf:f20c:64 | | 1024 | main |
| lan | R00::8 | | 256 | local |
| (eth1) | R00::8 | | 256 | local |

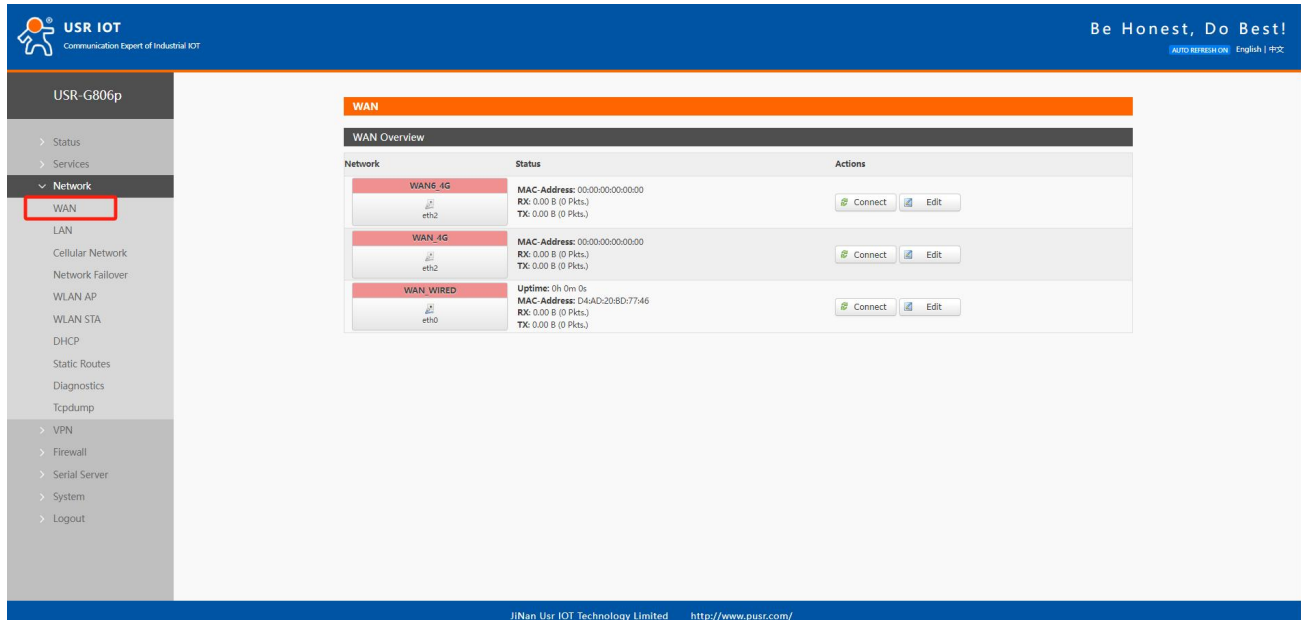
JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 5 ARP

3. Network interface function

3.1. Cellular networks

The router supports WAN ports for access to external networks.

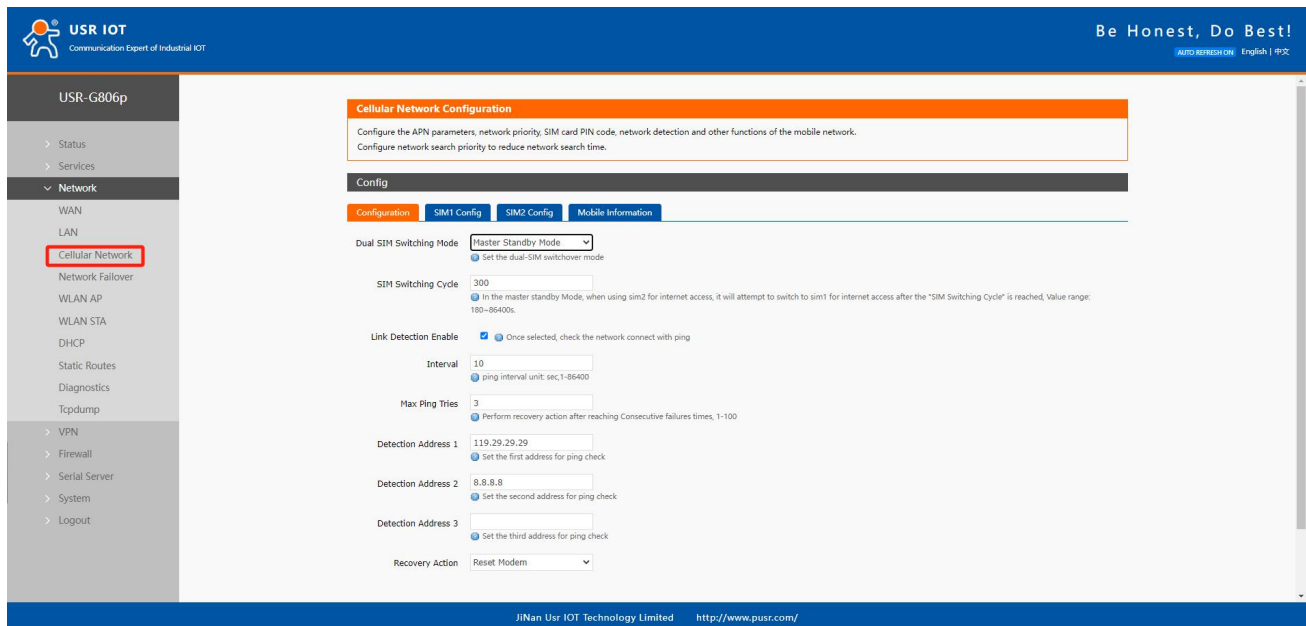


Pic 6 4G Set up the interface

Tab 3 state table

| Num | Name | meaning |
|-----|--------------|--|
| 1 | Running Time | The running time of the 4G network card started by this interface |
| 2 | MAC | The MAC address of the network card interface |
| 3 | Receive/send | Statistics on the total amount of data received and sent by this website |

3.1.1. Cellular network configuration



Pic 7 Cellular network configuration page

Tab 4 Cell network configuration parameter table

| Item | function | default |
|----------------------------------|---|--------------------|
| Dual card switching mode | <p>Master-Backup Mode : SIM1 is the primary. When SIM1 malfunctions, it automatically switches to SIM2 for internet access. Once SIM1 recovers, it will switch back to SIM1 automatically.</p> <p>Mutual Backup Mode : If the current SIM card can access the internet, no card switching will occur.</p> <p>Manual Mode : Lock onto SIM1 or SIM2, disabling automatic card switching.</p> | Master-Backup Mode |
| Check the cycle | At present, when the card is connected to the network, the threshold time set here will detect whether SIM1 returns to normal (the cellular network will be disconnected each time). If SIM1 is restored, it will automatically switch to SIM1 access. Unit: seconds | 300 |
| Fixed SIM card | When the mode is switched to manual mode, select the SIM card to be locked | SIM1 |
| Link probing enabled | <p>Open: Enable the SIM card Ping detection function</p> <p>Close: Disable the SIM card Ping detection function</p> | Close |
| Detection time interval | Ping detection interval, unit: seconds | 10 |
| Number of re-tries for detection | Number of ping probe failures | 3 |
| Probe address 1 | A total of 3 Ping addresses are detected. If one of them is | 8.8.8.8 |

| | | |
|-----------------------------------|---|--------------------|
| | pingable, the link is considered normal | |
| Probe address 2 | A total of 3 Ping addresses are detected. If one of them is pingable, the link is considered normal | 119.29.29.29 |
| Probe address 3 | A total of 3 Ping addresses are detected. If one of them is pingable, the link is considered normal | 255.5.5.5 |
| Resume the exercise | Optional: None / Re-dial / Restart module / Restart module / Restart device | Restart the module |
| Signal strength detection enabled | Checked: detect the interval time once, and switch the SIM card when the sub-signal is less than the set trigger threshold for multiple times | Unchecked |
| Detection time interval | Signal detection interval time, unit: second | 10 |
| Number of re-tries for detection | If the signal value is less than the threshold for several times, the card will be cut | 3 |
| Trigger threshold | Signal threshold, unit: dbm | -80 |
| Ping delay detection is enabled | Checked : The interval time is detected once, and the delay of multiple probes is greater than the set trigger threshold to switch the SIM card | Unchecked |
| Detection time interval | Detection interval time, unit: seconds | 10 |
| Number of re-tries for detection | If the detection delay exceeds the threshold, the card will be cut | 3 |
| Trigger threshold | Delay threshold, unit: ms | 80 |

3.1.2. SIM

Set the SIM1/2 card related parameters.

The screenshot displays the USR-IOT web management interface. On the left, a sidebar menu shows the navigation structure, with 'Cellular Network' selected under the 'Network' category. The main content area is titled 'Cellular Network Configuration' and contains a 'Config' tab with sub-tabs for 'Configuration', 'SIM1 Config', 'SIM2 Config', and 'Mobile Information'. The 'SIM1 Config' sub-tab is active, showing various parameters for the first SIM card. These parameters include APN (set to Automatic), Username, Password, Auth Method (set to PAP AND CHAP), Network Type (set to AUTO), LTE band selection (set to auto), PDP Type (set to IPV4/V6), MTU (set to 1500), Priority Of Network Search (set to AUTO), and a checkbox for PIN Enable. The interface also includes a footer with the USR-IOT logo, slogan 'Be Honest, Do Best!', and contact information.

Pic 8 SIM

Tab 5 SIM

| Item | Description | Default |
|-------------------------|---|-------------|
| APN | Please set the correct APN address | Auto |
| Username | APN username | empty |
| Password | APN Password | empty |
| Auth Method | APN authentication type: None/PAP/CHAP | empty |
| Network Type | Force 4G, 3G or 2G network | Auto |
| LTE band selection | Lock the frequency band | Auto |
| PDP Type | IPv4/IPv6/IPv4&v6 are optional | IPv4&v6 |
| MTU | Set the cellular network card MTU | 1500 |
| Network search priority | Auto/2G/3G/4G | Auto |
| PIN enable | SIM PIN | Not enabled |
| PIN | Four to eight digits Note: The PIN code is invalid if the PIN enablement item is not enabled | 1234 |
| EHRPD | This option is generally not required when 5G network is started | Not enabled |

3.1.3. SIM card information

The SIM card information display shows the configuration information of the SIM card in detail. If there is a problem with the network connection, you can check the cause of the problem.

The screenshot displays the USR-G806p web interface. On the left, a sidebar menu shows 'Cellular Network' selected. The main content area is titled 'Cellular Network Configuration' and includes a 'Config' tab with sub-tabs for 'Configuration', 'SIM1 Config', 'SIM2 Config', and 'Mobile Information' (which is highlighted). The 'Mobile Information' tab displays the following details:

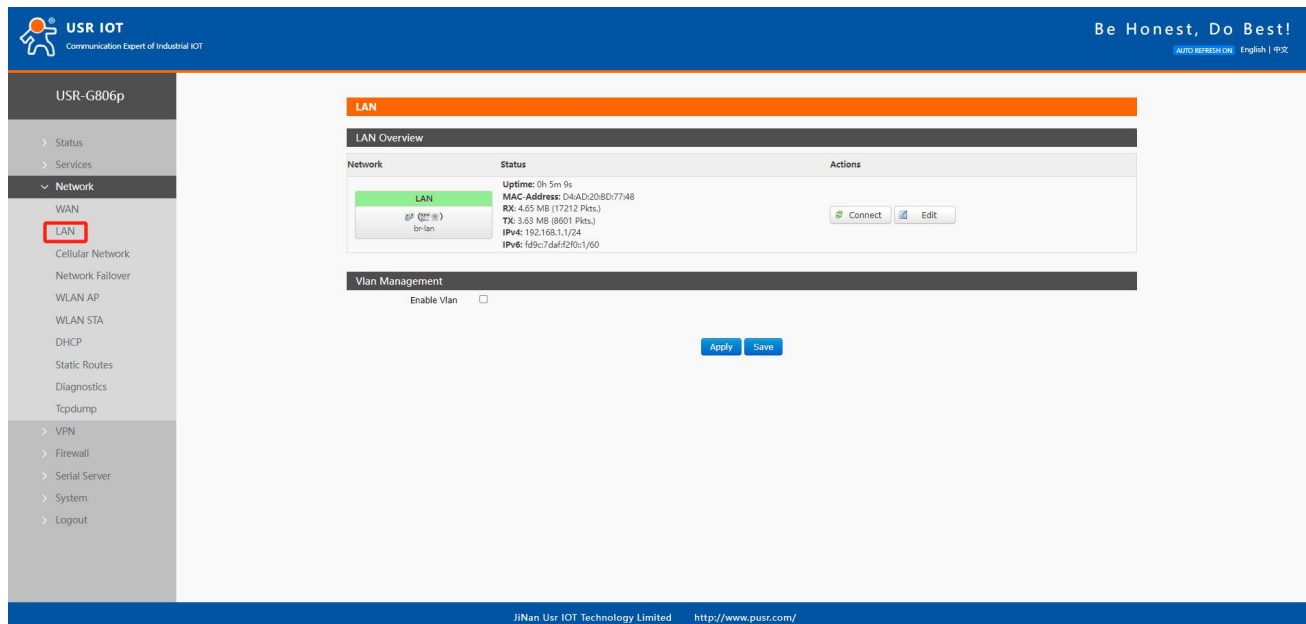
| | |
|---------------------|-----------------------------------|
| Modem Version: | EC20CEHDLGR06A09M1G |
| IMEI: | 860446079133588 |
| Dial SIM: | sim2 |
| SIM Status: | READY |
| SMS Service Center: | +8613334786200 |
| ICCID: | 89861124204041429026 |
| CIMi: | 460113453150069 |
| APN: | ctnet.ctnet@mycdma.cn.vnet.mobi.1 |
| Attachment Status: | Attached |
| Signal Strength: | 20(-73dBm) |
| Network Type: | FDD-LTE(4G) |
| BAND: | LTEBAND3 |
| Network Operator: | CHN-CT |
| IP Address: | 10.25.130.194 |
| Location Area Code: | 5277 |
| Cell ID: | 8085F34 |

At the bottom of the interface, it shows 'J/Nan Usr IOT Technology Limited' and the URL 'http://www.pusr.com/'.

Pic 9 SIM Information

3.2. LAN

LAN port is a LAN with 4 wired LAN ports (LAN4 can be set to WAN2 for use).



Pic 10 LAN

Tab 6 LAN

| Item | meaning | Windows default |
|--------------------------|---|-----------------|
| IPv4 | The IP address of the LAN card | 192.168.1.1 |
| subnet mask | The subnet mask of the network card | 255.255.255.0 |
| IPv4 Gateway | The gateway address of the LAN card is usually empty | empty |
| IPv4 broadcast | The broadcast address of the LAN card is usually empty | empty |
| Use a custom DNS server | The alternative DNS server is used to resolve the DNS server when the DNS server issued by the superior route cannot be resolved normally | empty |
| IPv6 allocation length | Assign a fixed portion of the specified length to each public IPv6 prefix, usually the default value | 60 |
| IPv6 allocation reminder | Use the hexadecimal subprefix ID of this interface to assign the prefix portion, which is usually the default value | empty |

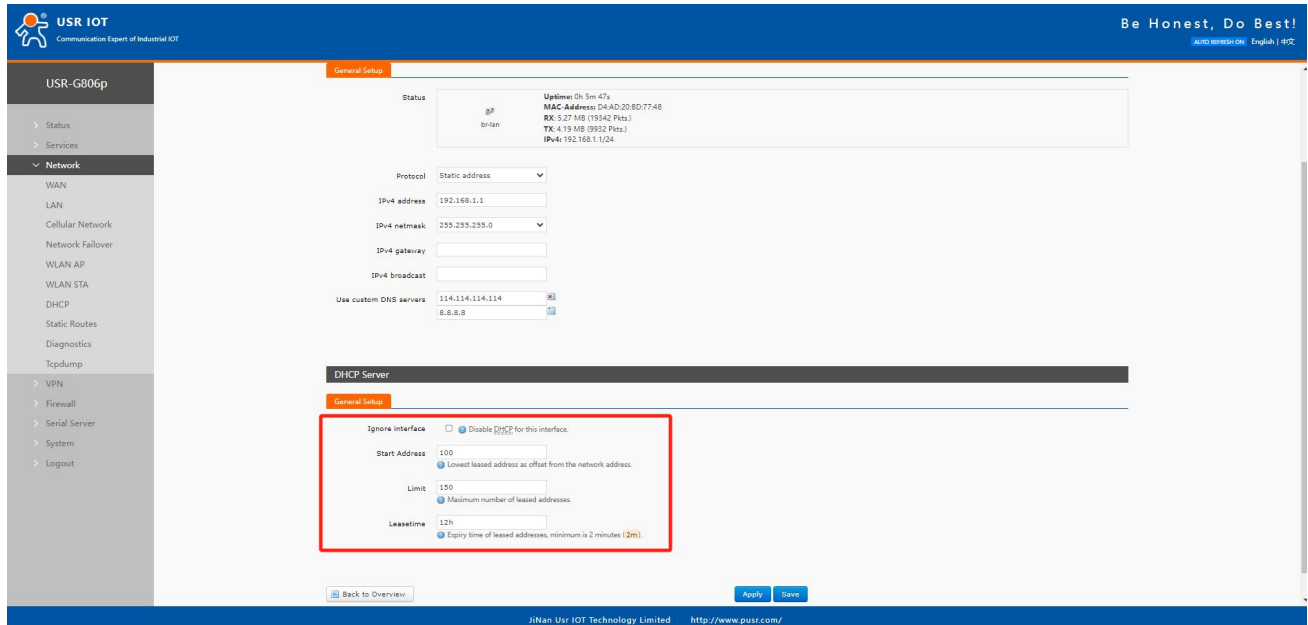
< Instruction >

- The default static IP address is 192.168.1.1 and the subnet mask is 255.255.255.0. This parameter can be modified, for example, to change the static IP address to 192.168.2.1;
- The DHCP server function is enabled by default, and the devices connected to the LAN port of the router can automatically obtain IP addresses;

- If VLAN division is used, the WIFI interface is bridged to the br-lan port, and the WIFI obtains IP and the same network segment as the br-lan network card.

3.2.1. DHCP

The LAN port DHCP Server function is enabled by default (you can choose to disable it).



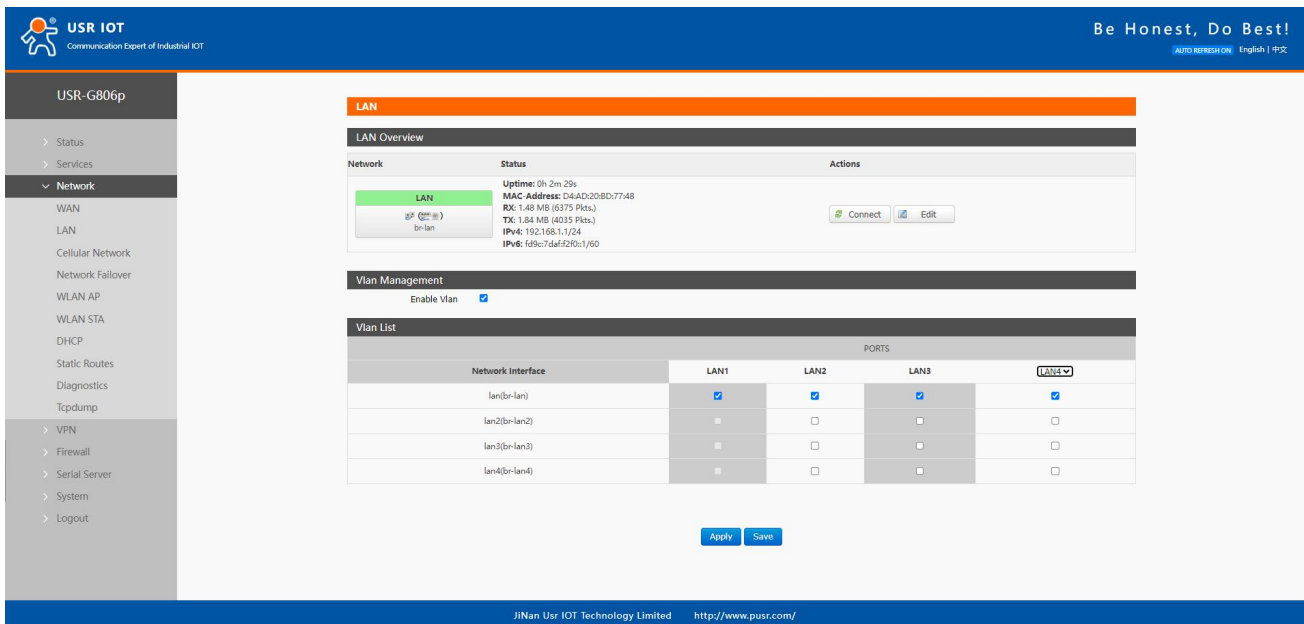
Pic 11 DHCP

< instruction >

- The starting address of the DHCP pool and the address lease time can be adjusted;
- DHCP The default allocation range starts from 192.168.1.100;
- The default lease period is 12 hours, which can be set as "h" -hour or "m" -minute;
- If you disable DHCP, the subnet device needs to set the correct static IP and gateway to connect to 806w.

3.2.2. VLAN

This router supports VLAN division of network ports, which can divide multiple network ports into different network segments.



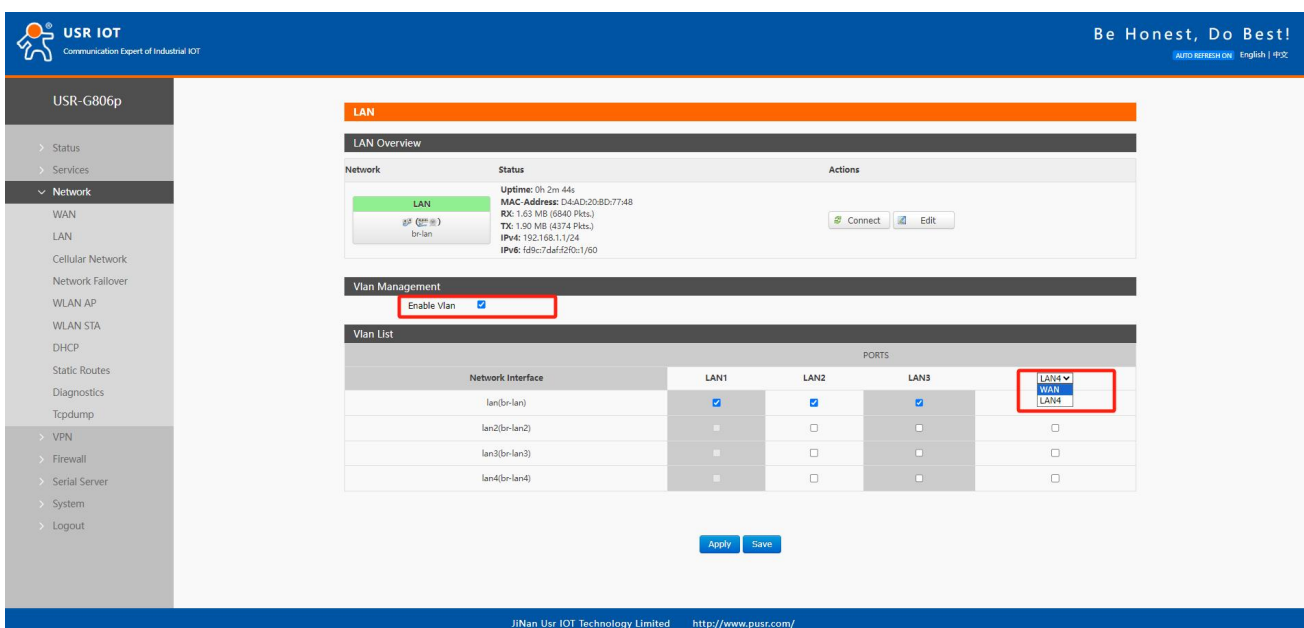
Pic 12 LAN

< explain >

- Disable VLAN division by default. If enabled, LAN port IP will be automatically changed to 192.168.1.1, LAN2 to 192.168.2.1 and so on;
- WIFI is bridged to LAN. When a device connects to the router's WIFI, the device obtains the IP network segment and LAN network interface in the same network segment;
- LAN2 and LAN3 can be bridged to lan~lan4 network interface at will.

3.2.3. WAN/LAN Select

After the VLAN switch is turned on, LAN4 can be set to WAN.

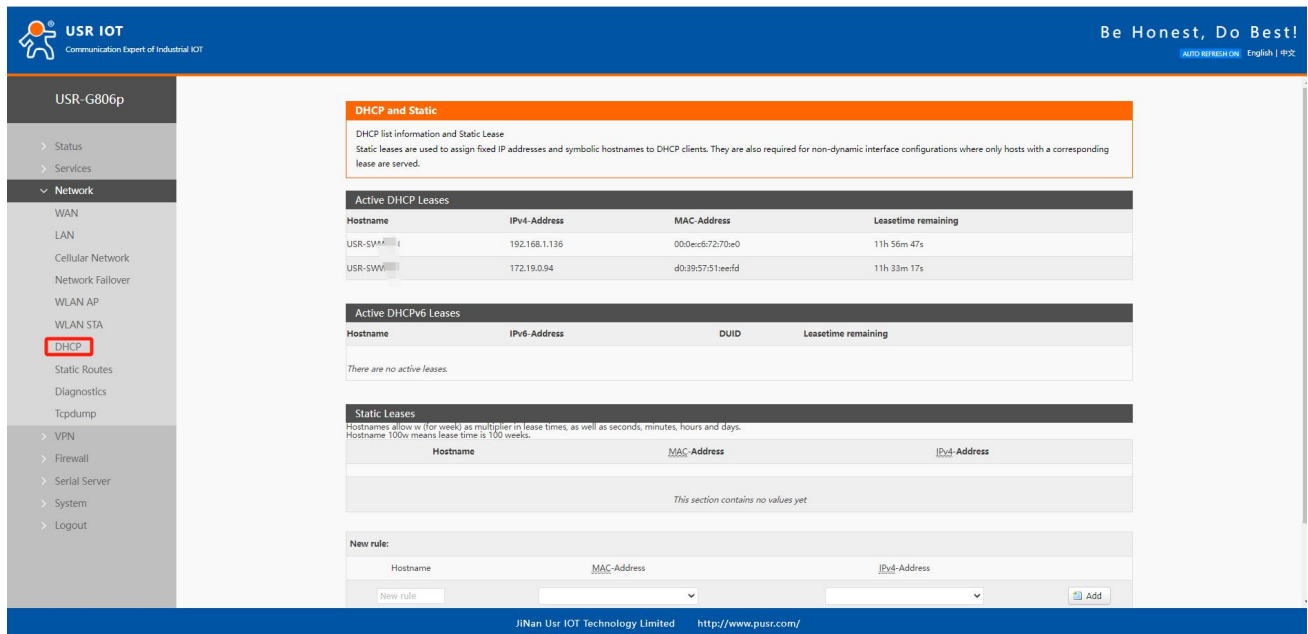


Pic 13 VLAN

3.2.4. DHCP

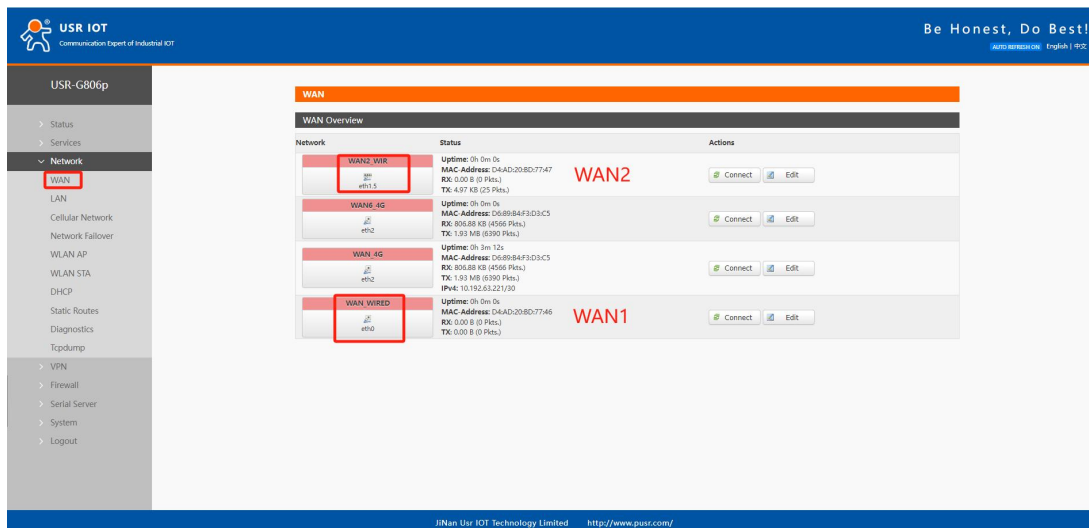
Static address allocation: Set at the interface-DHCP. This function extends the LAN interface DHCP Settings to assign a fixed IP address and host ID to the DHCP client. Only the specified host can be connected, and the interface must be configured dynamically.

Use add to add new lease entries. Use the MAC address to identify the host, the IPv4 address to assign the address, and the hostname to assign the identifier.



Pic 14 DHCP

3.3. WAN

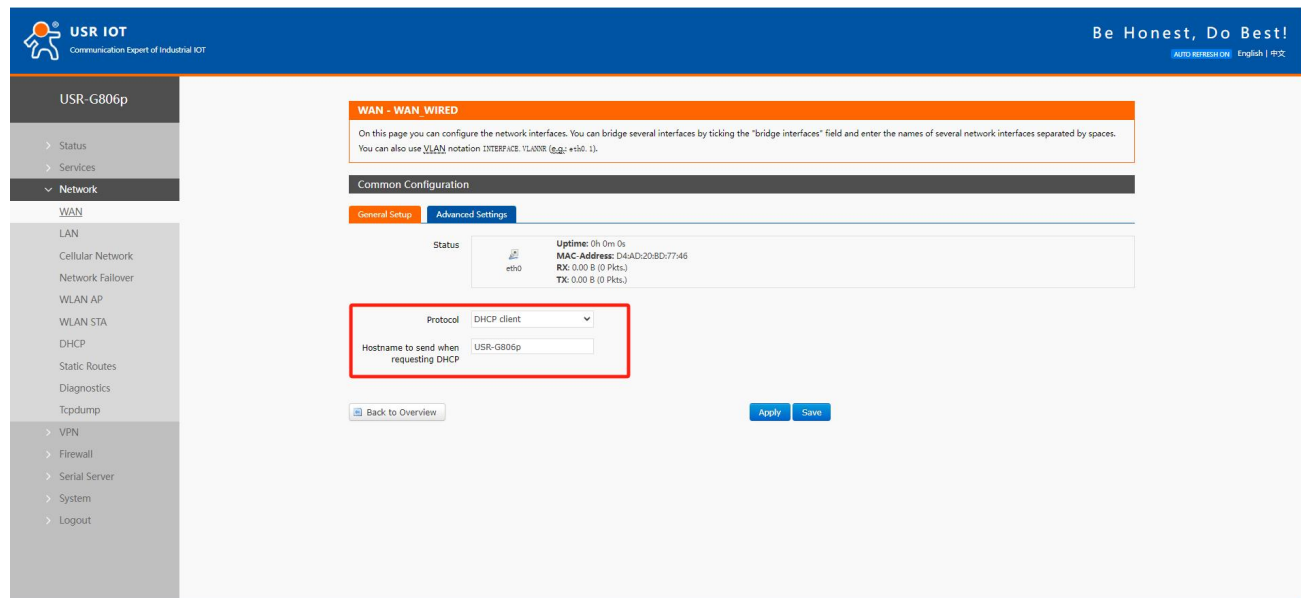


Pic 15 Interface configuration interface

< explain >

- By default, the 1WAN port is enabled, and the LAN port VLAN division is enabled for WAN2;
- WAN supports DHCP client, static IP and PPPoE mode;
- The default IP acquisition method is DHCP Client.

3.3.1. DHCP



Pic 16 WAN

< explain >

- The default IP acquisition method is DHCP Client;
- Supports the hostname for a change request DHCP.

3.3.2. Static IP mode

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

AUTO REFRESH ON English | 中文

USR-G806p

- > Status
- > Services
- > Network
 - WAN
 - LAN
 - Cellular Network
 - Network Failover
 - WLAN AP
 - WLAN STA
 - DHCP
 - Static Routes
 - Diagnostics
 - Tcpdump
- > VPN
- > Firewall
- > Serial Server
- > System
- > Logout

WAN - WAN WIRED

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.VLANID (e.g.: eth0.1).

Common Configuration

General Setup Advanced Settings

Status

Uptime: 0h 0m 0s
MAC Address: D4:AD:20:8D:77:46
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol Static address

IPv4 address

IPv4 netmask -- Please choose --

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

Back to Overview

Apply Save

Pic 17 WAN

< explain >

- Static address mode requires manual input of IPv4 address, mask and IPv4 gateway address;
- The gateway address must be accessible, otherwise the network cannot be used normally;
- The general IP address should be in the same subnet as the gateway
- Note that the IP address should not be in the same subnet as the LAN port IP address, otherwise the network will be abnormal.

3.3.3. PPPoE

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

AUTO REFRESH ON English | 中文

USR-G806p

- > Status
- > Services
- > Network
 - WAN
 - LAN
 - Cellular Network
 - Network Failover
 - WLAN AP
 - WLAN STA
 - DHCP
 - Static Routes
 - Diagnostics
 - Tcpdump
- > VPN
- > Firewall
- > Serial Server
- > System
- > Logout

WAN - WAN WIRED

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.VLANID (e.g.: eth0.1).

Common Configuration

General Setup Advanced Settings

Status

Uptime: 0h 0m 0s
MAC Address: D4:AD:20:8D:77:46
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol PPPoE

PAP/CHAP username

PAP/CHAP password

Back to Overview

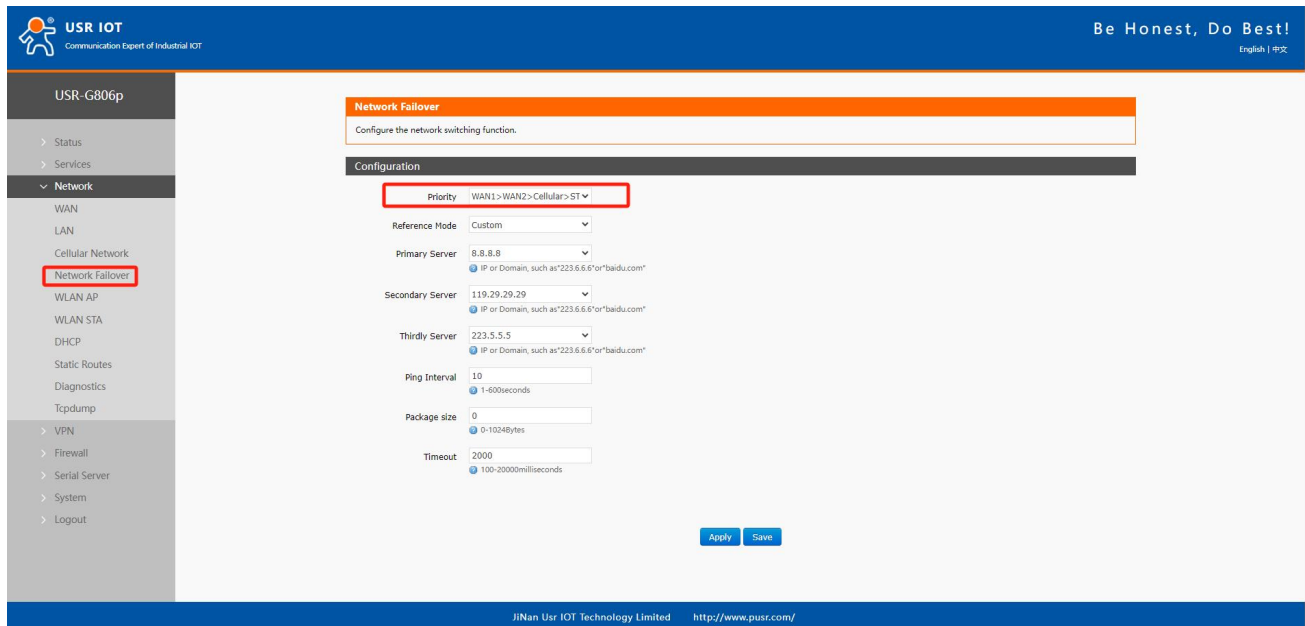
Apply Save

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 18 WAN

< explain >

- The user name and password need to be obtained from the operator and filled in the corresponding position;
- Using this function is equivalent to using the router as a modem for dialing;
- Click save, and then click Apply to complete the configuration.

3.4. Network switching**Pic 19 Network switching configuration****Tab 7 Network switching configuration**

| name | description | Default parameter |
|-------------------|---|-----------------------|
| priority | Set the NIC priority policy here For example, select: WAN1> WAN2> Cellular> STA. When the WAN1 network card can detect the target address is open, the WAN1 network card will be used to access the Internet. When the WAN1 network card fails to detect the target address, the WAN2, Cellular, and STA network cards will be used in sequence to detect the target address. Disable: Use the last network | WAN1 takes precedence |
| reference pattern | Customization: Determine the network status based on the custom reference address Gateway: Probe the gateway address of each network card to determine the network status | user-defined |
| Reference 1 | You can set IP/domain name | 8.8.8.8 |
| Reference 2 | You can set IP/domain name | 8.26.56.26 |
| Reference 3 | You can set IP/domain name | 208.67.222.222 |

| | | |
|--------------------------------|--|------|
| Detection interval (unit: s) | Set the link detection interval: 1-600s can be set | 10 |
| Ping packet size (unit: bytes) | Packet size for link detection: 32-1024 bytes can be set | 0 |
| Ping timeout (unit: ms) | Set the ping timeout time: can set 100-20000ms | 2000 |

3.5. Wireless configuration

2.4G wireless LAN (Wi-Fi) function.

The screenshot displays the USR IOT web interface for configuring the WLAN AP. The left sidebar shows the navigation menu with 'WLAN AP' highlighted. The main content area is titled 'WLAN AP Settings' and includes a 'Client Information' tab. The 'WLAN AP Settings' section has a '2.4G Settings' tab selected. The 'Status' section shows the device is a Master with SSID: USR-G806p-7746 and BSSID: 04A4D209BD7748. The 'Enable' checkbox is checked. The 'Hide SSID' checkbox is unchecked. The 'SSID' field is set to 'USR-G806p-7746'. The 'Encryption' dropdown is set to 'mixed-psk'. The 'Key' field is masked with asterisks. The 'HW Mode' dropdown is set to '11ng'. The 'Channel' dropdown is set to 'auto'. The 'HT Mode' dropdown is set to 'auto'. The 'Regions' dropdown is set to 'CN - China'. The bottom of the page shows the footer with 'JiNan Usr IOT Technology Limited' and the website 'http://www.pusr.com/'.

Pic 20 Wi-Fi configuration intent

< explain >

- Wi-Fi and LAN can simultaneously support up to 30 clients, with a maximum of 20 being Wi-Fi clients. When Wi-Fi and LAN are not simultaneously loading clients, if there are no LAN port clients, Wi-Fi can support up to 20 wireless clients; if there are no Wi-Fi clients, only LAN port clients can support up to 50 clients. When the LAN port is configured with VLAN division, the AP segment and the LAN network share the same subnet;
- The maximum coverage of Wi-Fi is 500m in open areas, and the environment affected by obstacles such as offices can be covered within 50m;
- The actual connection distance of Wi-Fi is greatly affected by the environment. Please test it as the actual test.

Tab 8 Wi-Fi configuration parameter

| name | description | Windows default |
|-------------|--|-----------------|
| start using | Turn on the WIFI LAN function | check |
| hide SSID | To enable this function: The device will not be able to search for 806w WIFI, and you need to manually enter the correct WIFI name and password to connect, ensuring the WIFI security | Not selected |
| WIFI name | The router's WIFI name can be customized The default value of XXXX is the last four bits of the router MAC | USR-G806w-XXXX |

| | | |
|------------------------|---|-------------|
| encryption | selectable : No encryption/mixed-psk/psk+ccmp/psk2/psk2-tkip | mixed-psk |
| password | WIFI password, customizable | www.usr.cn |
| Network model | Options: 11ng/11n/11g/11bgn/11bg/11b | 11ng |
| channel | Automatic, lockable channel | voluntarily |
| frequency bandwidth | Auto/40MHz/20MHz is optional | auto |
| Country or region | You can select a country or region | CN-China |

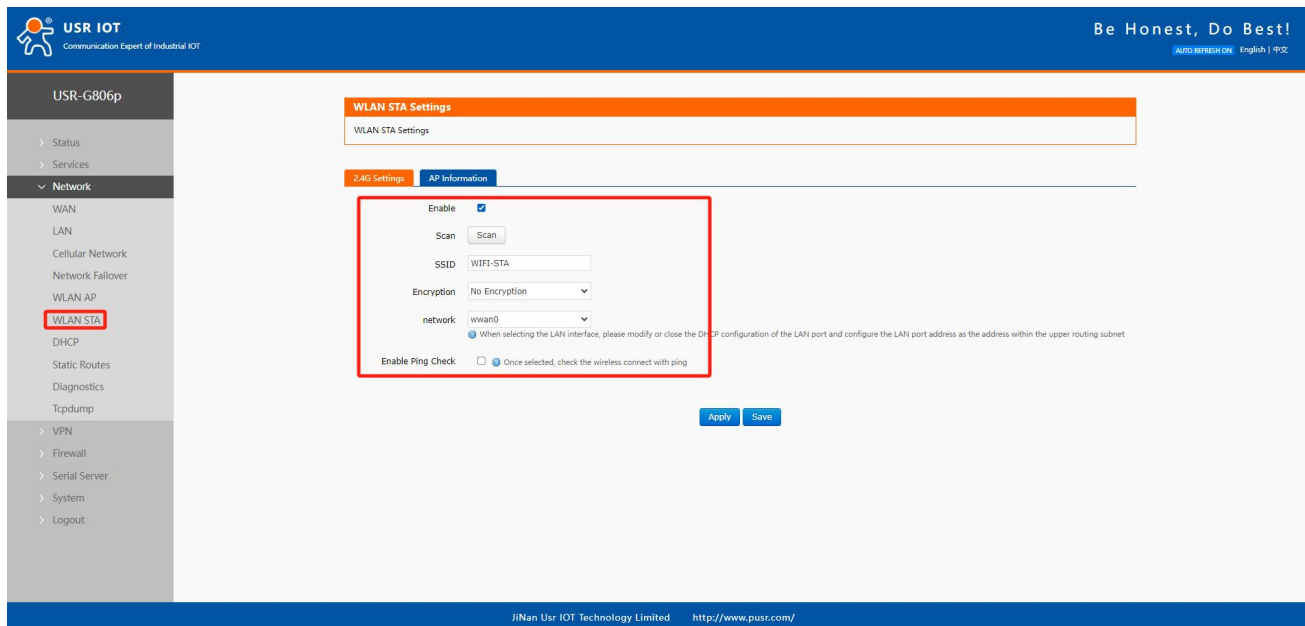
The list of wifi clients can be viewed in the client information interface.

The screenshot displays the USR IOT web management interface. On the left, a sidebar menu for 'USR-G806p' includes options like Status, Services, Network, and VPN. The 'Network' section is expanded, showing 'WLAN AP' as the selected item. The main panel shows the 'WLAN AP Settings' configuration page. Within this page, the 'Client Information' tab is active, revealing a table intended for listing connected WiFi clients. The table headers are SSID, MAC Address, IPv4 Address, Signal, Noise, RX Rate, and TX Rate. As of the screenshot, the table is empty, showing 'No information available'. 'Apply' and 'Save' buttons are located at the bottom right of the table area.

Pic 21 WiFi client list page

3.6. Wireless client

The router is turned off by default for WIFI (wireless) client, and the WIFI client can be enabled to connect to the hotspot coverage on site for Internet access.

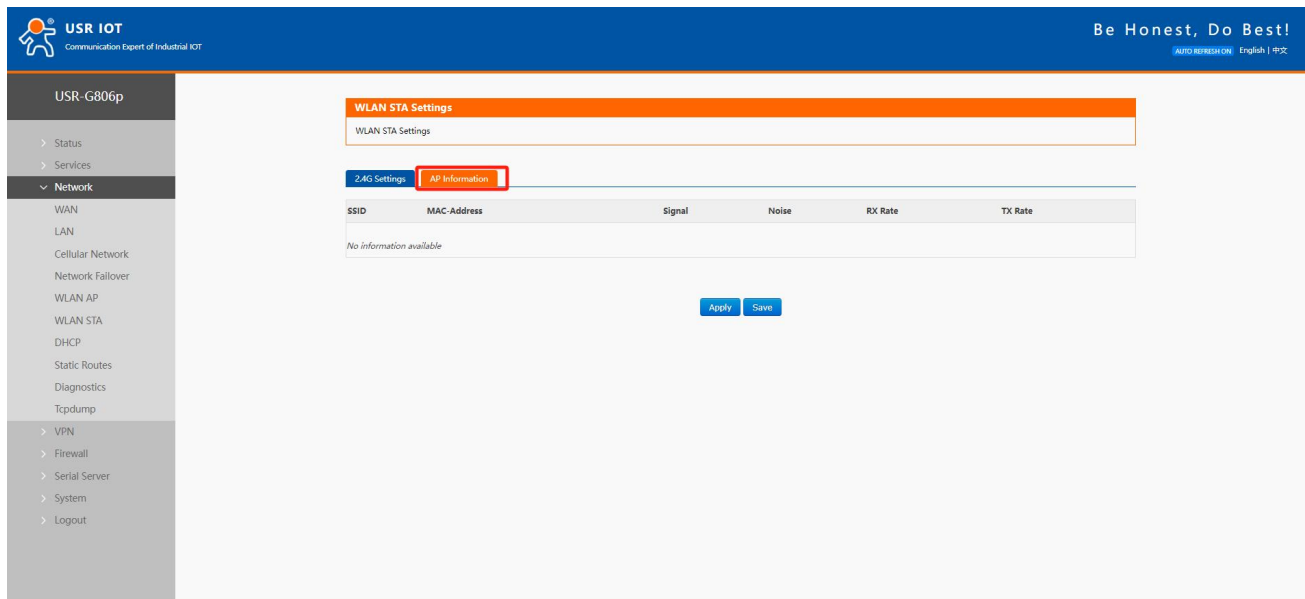


Pic 22 Wireless client configuration

Tab 9 WiFi configuration parameter

| name | description | Windows default |
|--|--|-----------------|
| start using | Turn on the WIFI client | Not selected |
| search | Click search to start searching for hot spots It takes about 30 seconds to 1 minute to search for hot spots, so be patient | not have |
| WIFI name | You can select hot spots by searching or manually | WIFI-STA |
| encryption | It can be set to: no encryption /mixed-psk | No encryption |
| network | Can be set to: wwan0/lan To use the STA function normally, select wwan0 If you need to use WIFI bridge mode, select lan | wwan0 |
| Forcing the update of LAN IP addresses | When the network selects LAN (bridge mode), select this function to restart LAN | check |
| Enable Ping detection | After checking, the live detection function is enabled. If the detection address is not available, the connection to the wireless will be re-established | Not selected |
| reference address | Option: Gateway / specified address | gateway |
| Ping address | The address of the STA probe, note that you need to set the address that the STA can ping | empty |

On the hot spot information interface, you can check whether the router is connected to the AP.



Pic 23 Connect to the AP information page

< explain >

- When the network selects lan, it is set to bridge mode;
- To set the bridge mode, please pay attention to the need to turn off the dhcp of the LAN port;
- When LAN is enabled with DHCP, bridge mode bridges to the LAN network.

3.7. Static routing

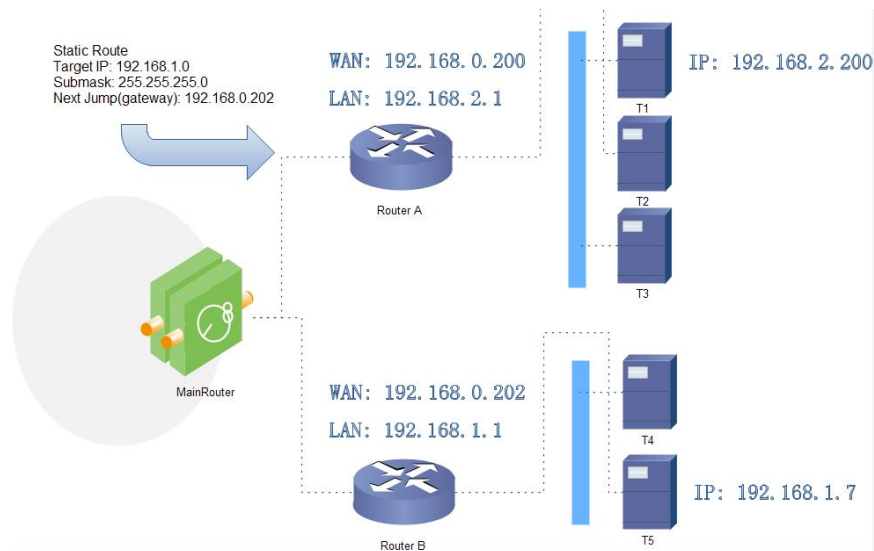
Static routes have the following parameters. The default static route can be added up to 20.

Tab 10 Static routing parameter table

| name | description | Default parameter |
|-------------------------|--|-------------------|
| joggle | LAN, wan_4G, wan_wired, and vpn interfaces | lan |
| Object (target address) | The address or address range of the object to be accessed | empty |
| subnet mask | The subnet mask of the network to which you want to access | empty |
| Gateway (next hop) | The address to which to forward | empty |
| Jump point (Metric) | Number of jumps in the package | empty |

Static routing describes the routing rules for packets on an Ethernet.

Test example: Test environment, two peer routers A and B, as shown in the figure below.



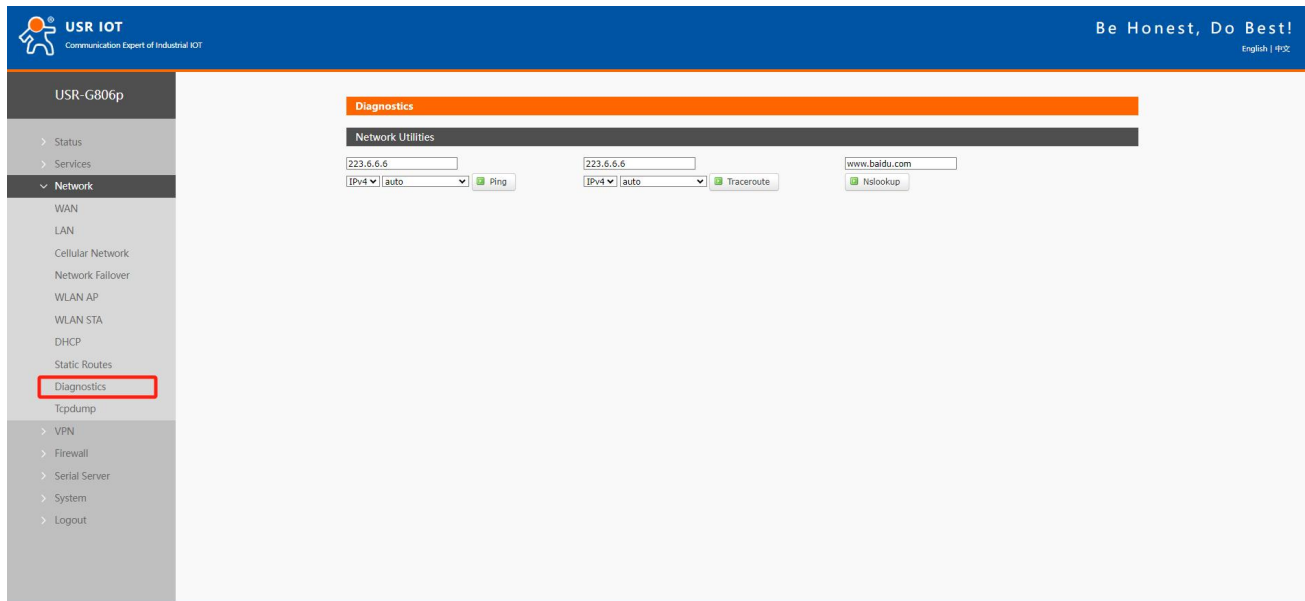
Pic 24 An example of a static routing table

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

Now, if we want to make a route on router A so that when we access the 192.168.1.x address, it automatically goes to router B.

Pic 25 Route table add page

3.8. Network diagnostic function



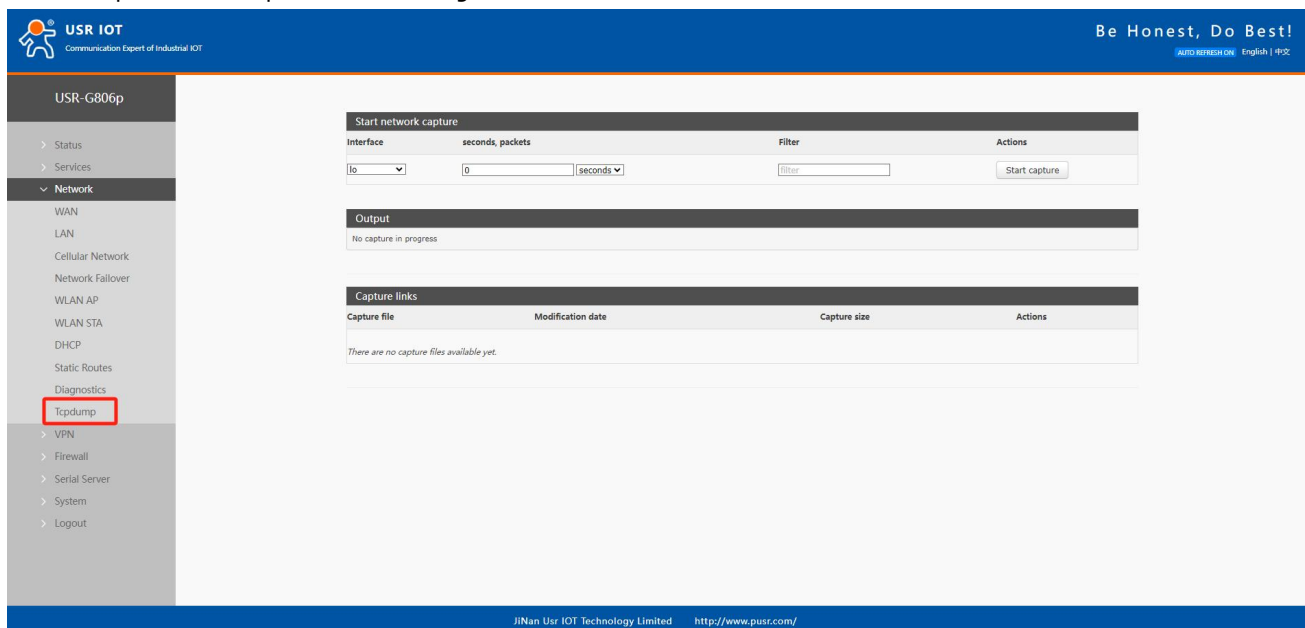
Pic 26 Network diagnostic interface

The router's online diagnostic functions include Ping tools, route resolution tools, and DNS viewing tools.

- Ping is a Ping tool that can directly ping a specific address on the router;
- Traceroute is a routing analysis tool that can obtain the route path when accessing an address;
- Nslookup is a DNS viewing tool that resolves domain names to IP addresses.

3.9. TCPDUMP traffic monitoring

Packet capture can be performed through the web interface.



Pic 27 TCPDUMP

Tab 11 WiFi configuration parameter

| name | description | Windows default |
|----------------------|--|-----------------|
| joggle | Select the capture interface Br-lan: LAN interface Wan_wired: WAN1 interface Wan2_wir: WAN2 interface Wan_4G: Cellular interface Ath1: WIFI STA interface | Lo |
| Capture restrictions | Capture duration or number of packets | 0 seconds |
| filter | Fill in the filter conditions for the Tcpdump command, such as port 80 | empty |

- The captured packets will be cleared after the router restarts.

4. VPN function

VPN (Virtual Private Network) is a virtual private network technology. In terms of protocol, this router supports: PPTP, L2TP, IPSec, OpenVPN, GRE, VXLAN.

4.1. PPTP Client

Before application, you need to build a VPN server first. Fill in the server address, account, password and encryption mode correctly to connect.

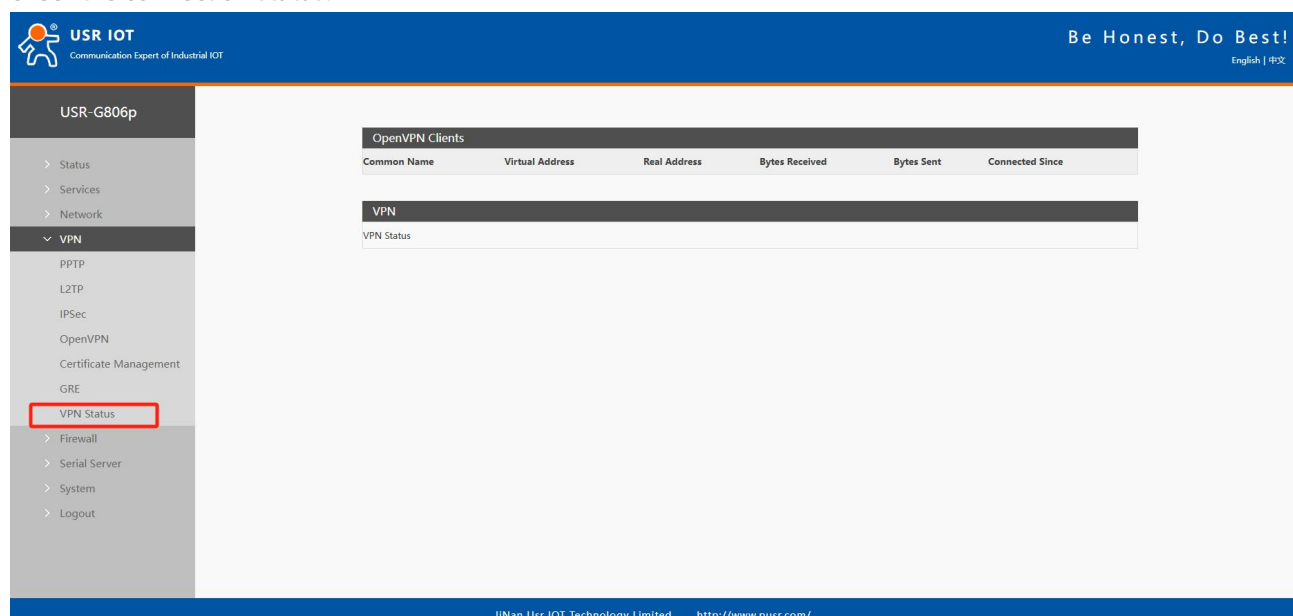
Pic 28 Router adds VPN operation diagram 1

Tab 12 PPTP configure

| name | description | Default parameter |
|-----------------------------------|--|-------------------|
| PPT Enable the PPTP client | Enable: Start PPTP client Disable: Close the PPTP client | forbidden |
| Server address | Enter the IP address or domain name of the VPN server to connect to | 192.168.0.2 |
| joggle | Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Connect to a VPN using cellular 5G Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN | voluntarily |
| user name | Fill in the correct user name | empty |
| password | Enter the correct password | empty |
| To the subnet | Use a static route through the VPN to enable subnet communication between the client and the server. Enter the server subnet segment here | 192.168.55.0 |
| For the subnet mask | Use a static route through the VPN to enable subnet communication between the client and the server. Enter the subnet mask of the server subnet here | 255.255.255.0 |
| NAT | Check: Data passing through the VPN will be sent after NAT No line: Data passing through a VPN does not go through NAT | check |
| MPPE encryption | After checking, it is: mppe required, stateless Not checked: Do not start mppe encryption If the server uses require-mppe-128 encryption, you can uncheck this option and try the following additional configuration: mppe required,no40,no56,stateless refuse-eap refuse-chap refuse-pap refuse-mschap | check |
| MTU | Set PPTP MTU value to the default value | 1450 |
| Additional configuration | Special parameters are usually configured for the server. If the client interface does not have these parameters, configure them here. Do not operate by non-professionals | empty |
| Enable static tunnel IP addresses | Customize PPTP client IP. Note that if the IP server is assigned to other clients or the IP is not within the IP range | Not enabled |

| | | |
|--------------------------|--|--------------|
| | defined by the server, the connection will not be made to the server | |
| Static tunnel IP address | Customize PPTP client IP. Note that if the IP server is assigned to other clients or the IP is not within the IP range defined by the server, the connection will not be made to the server | empty |
| default gateway | After checking: All data traffic will be transmitted through the VPN channel after the VPN is established Unchecked: Only the VPN channel is established. If you need subnet intercommunication, static routes should be established Note: If the WAN port is connected by PPPOE, this option is invalid | Not selected |
| enable ping | Check: Enable VPNping ping alive detection, and reconnect to the VPN if ping fails Unchecked: Do not enable ping to keep alive | Not selected |
| Ping address | PPT The address that the PPTP network card can ping is usually filled with the PTP address | empty |
| Ping period | Ping maintenance interval period, unit: seconds | 10 |
| Ping number of times | After the Ping failure upper threshold is exceeded, ping will not be sent to the set IP address, and the VPN will reconnect | 3 |

PPTP connection success: After filling in the relevant parameters, save and apply, and enter the VPN--VPN state to check the connection status.



Pic 29 Router VPN connection status

4.2. L2TP Client

The screenshot displays the 'L2TP Setting' page in the USR-G806p web management system. The left sidebar shows the navigation menu with 'L2TP' highlighted under the 'VPN' section. The main content area is titled 'L2TP Setting' and contains the following configuration fields:

- L2TP Client:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Server Address:** Text input field with the value '192.168.0.2'.
- Interface:** Dropdown menu set to 'auto'.
- User Name:** Text input field.
- Password:** Text input field with a green checkmark.
- Tunnel Name:** Text input field.
- Tunnel Password:** Text input field with a green checkmark.
- Enable IPsec:** Check box (unchecked).
- Remote Subnet:** Text input field with the value '192.168.0.0'.
- Remote Subnet Mask:** Text input field with the value '255.255.255.0'.
- NAT:** Check box (checked).
- MTU:** Text input field with the value '1450'.
- Extra option:** Text input field.
- Enable Static Tunnel IP Address:** Check box (unchecked).
- Default Gateway:** Check box (unchecked) with the text 'All traffic goes to VPN, except WAN protocol is PPPoE'.
- Enable Ping:** Check box (unchecked) with the text 'Reconnect When Fails to Ping'.

Pic 30 L2TP client Settings interface

Tab 13 L2TP configuration parameters

| name | description | Default parameter |
|---------------------|---|-------------------|
| L2TP client enabled | Enable: Start the L2TP client Disable: Close the L2TP client | forbidden |
| Server address | Enter the IP address or domain name of the VPN server to connect to | 192.168.0.2 |
| joggle | Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Use cellular 5G to connect to a VPN Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN | voluntarily |
| user name | Fill in the correct user name | empty |
| password | Enter the correct password | empty |
| Name of tunnel | If the server specifies the tunnel name of the Client, it must be correct | empty |
| The Tunnel Code | Fill in the correct tunnel password | empty |

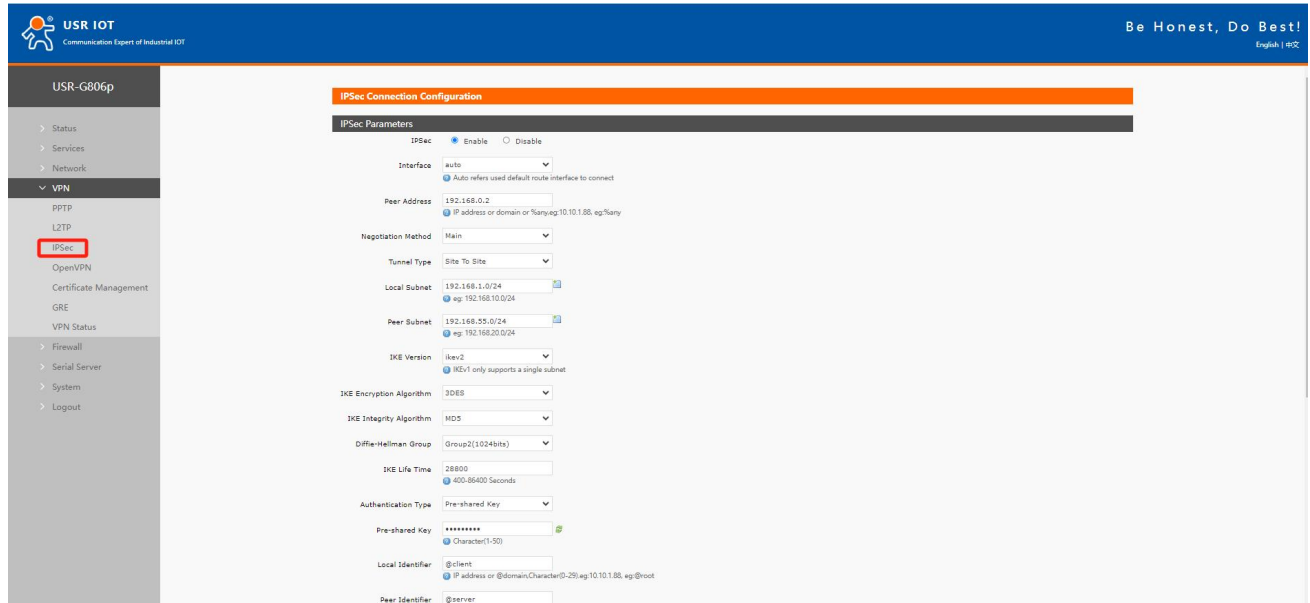
| | | |
|-----------------------------------|--|---------------|
| IPSec encryption | <p>Check: Enable L2TP over IPSec function</p> <p>Not checked: Single L2TP function</p> <p>After IPSEC encryption is enabled</p> <p>IKE encryption: 3des-md5-modp1024, 3des-sha1-modp1024</p> <p>ESP encryption: des-md5, des-sha1, 3des-md5, 3des-sha1</p> | Not selected |
| end on ID | The ID set on the server side | |
| To the subnet | Use a static route through the VPN to enable subnet communication between the client and the server. Enter the server subnet segment here | 192.168.55.0 |
| For the subnet mask | Use a static route through the VPN to enable subnet communication between the client and the server. Enter the subnet mask of the server subnet here | 255.255.255.0 |
| NAT | <p>Check: Data passing through the VPN will be sent after NAT</p> <p>No line: Data passing through a VPN does not go through NAT</p> | check |
| MTU | Set the PPTP MTU value to the default value | 1450 |
| Additional configuration | Special parameters are usually configured for the server. If the client interface does not have these parameters, configure them here. Do not operate by non-professionals | empty |
| Enable static tunnel IP addresses | Customize the L2TP client IP address. Note that if the IP server is assigned to other clients, or the IP is not within the IP range defined by the server, the connection will not be established to the server | Not enabled |
| Static tunnel IP address | Customize the L2TP client IP. Note that if the IP server is assigned to other clients, or the IP is not within the IP range defined by the server, the connection will not be established to the server | empty |
| default gateway | <p>After checking: All data traffic will be transmitted through the VPN channel after the VPN is established</p> <p>Unchecked: Only the VPN channel is established. If you need subnet intercommunication, you need to establish a static route</p> <p>Note: If the WAN port is connected by PPPOE mode, the check here is invalid</p> | Not selected |
| enable ping | <p>Check: Enable VPNping ping alive detection, and reconnect to the VPN if ping fails</p> <p>Unchecked: Do not enable ping to keep alive function</p> | Not selected |
| Ping address | The address that the L2TP network card can ping is usually filled in as the PTP address | empty |
| Ping period | Ping maintenance interval period, unit: seconds | 10 |
| Ping number of times | After the Ping failure upper threshold is exceeded, ping will | 3 |

| | | |
|--|--|--|
| | not be sent to the set IP address and the VPN will reconnect | |
|--|--|--|

< explain >

- The mppe mode is: mppe required, stateless.

4.3. IPSec



Pic 31 IPSec Settings interface

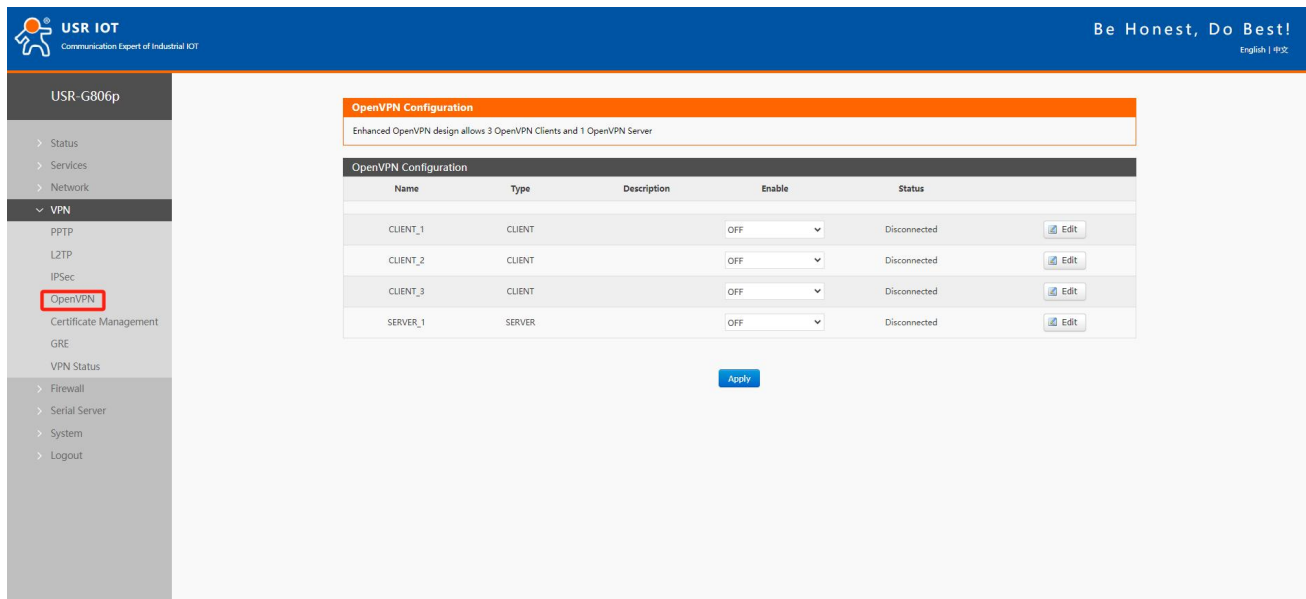
Tab 14 IPSec configuration parameters

| name | description | Default parameter |
|--------------|--|-------------------|
| IPSec enable | Enable: Enable IPSec Disable: Disable IPSec | forbidden |
| joggle | Automatic: Use the default route to connect to the VPN Wan_wired: Use the WAN interface to connect to the VPN Wan_4g: Use cellular 4g to connect to the VPN Automatic example: When the wired connection is the default route, if you attempt to connect to the VPN via the wired connection, even if there is a 4G network available, it will still try to use the wired network card to connect to the VPN. If the wired connection is disconnected, it will automatically switch to the 4G network and attempt to connect to the VPN using the 4G method. If the VPN connects via 4G and the wired connection becomes available, the default route will switch to the wired network. However, since the 4G connection remains active, the VPN will still be connected. Only when the 4G connection is disconnected and the IPsec connection is broken once, the default route network card will attempt to reconnect to the VPN again. | voluntarily |

| | | |
|----------------------------|---|------------------|
| | Wan_4G example: 4G has IP and tries to connect to VPN with 4G.4G has no IP and other network cards have IP but cannot connect to VPN. | |
| Destination address | Fill in the IP address or domain name of the other end Fill in:%any for passive server mode | 192.168.0.2 |
| machinery of consultation | Optional main mode / active mode (brutal mode) | holotype |
| This subnet | Fill in the subnet segment of this end, and keep it consistent with the subnet set at the other end You can fill in up to 10 segments | 192.168.1.0/24 |
| To the subnet | Fill in the destination subnet segment, and set the destination to be consistent with the destination subnet You can fill in up to 10 segments | 192.168.55.0/24 |
| IKE edition | ikev2/ikev1, and the configuration is consistent with that of the other end | ikev2 |
| IKE encryption algorithm | Select the IKE encryption algorithm and configure it to be consistent with the other end | 3DES |
| IKE verification algorithm | Select the IKE verification algorithm and configure it to be consistent with the other end | MD5 |
| Diffie-Hellman group | Select the DH group and configure it to be consistent with the other end | Group2(1024bits) |
| IKE survival time | IKE survival time setting, unit: seconds | 28800 |
| Type of certification | Pre-shared key type | Pre-share keys |
| Pre-share keys | Consistent with the configuration on the other end | 123456abc |
| Local identification | It can be FQDN or IP type, and must be consistent with the peer identifier set on the peer | @client |
| End identification | It can be FQDN or IP type, and should be consistent with the local identifier set on the other end | @server |
| ESP encryption algorithm | Select the ESP encryption algorithm and configure it to be consistent with the other end | AES-128 |
| ESP verification algorithm | Select the ESP verification algorithm and configure it to be consistent with the other end | SHA-1 |
| PFS | Select the PFS configuration and match it to the end configuration | DH2 |
| ESP life cycle | ESP life cycle Settings, unit: seconds | 3600 |
| DPD overtime | Set the DPD timeout time in seconds | 60 |
| DPD detection cycle | DPD detection cycle setting, unit: second | 60 |
| DPD activity | Optional: None/removal/maintenance/reboot | restart |

4.4. OpenVPN

This router supports 1 OpenVPN Server and 3 OpenVPN Clients. Several VPNs do not interfere with each other, so it is recommended to use only one OpenVPN.



Pic 32 Open the OpenVPN page

Tab 15 OpenVPN Client parameter table

| name | description | Default parameter |
|------------------------------------|---|-------------------|
| start using | Open: Open the openvpn client Close: Disable the openvpn client | close |
| description | You can customize the description of this OpenVPN path, but you don't have to fill it in | empty |
| Use the OpenVPN configuration file | Open: You can import the OpenVPN configuration parameters in the form of a file. If you are very familiar with the OpenVPN configuration file, you can use this method. It is recommended to use the router configuration box form Note: Use the router configuration box form | open |
| OpenVPN configuration file | The configuration file is passed to OpenVPN | not have |
| protocol | tcp/udp/tcp ipv4/udp ipv4 | udp |
| Remote host IP address | Set the openvpn server address: domain name or IP | 192.168.0.2 |
| port | Set the openVPN server port number | 1194 |
| Type of certification | None, SSL/TLS, user name and password, pre-shared key, SSL/TLS+ user name and password | SSL/TLS |
| TUN/TAP | tun/tap | tun |
| topology | Net30/p2p/subnet | subnet |
| bridge pattern | Tap bridges LAN and implements layer 2 interaction point | not have |

| | | |
|---|---|---------------|
| | to point | |
| user name | When the authentication type is selected with a user name and password, you must enter the correct user name | empty |
| password | When the authentication type is selected with a user name and password, you must enter the correct password | empty |
| Local tunnel IP | When the authentication type is no/pre-shared password, fill in the TUN tunnel IP of this end | empty |
| Remote tunnel IP | When the authentication type is no/pre-shared password, fill in the end-to-end tunnel IP of this end | empty |
| Enter the IP address of the Tap network card | When the authentication type is no/pre-shared password, fill in the IP address of the TAP network card on this end | empty |
| Tap the subnet mask of the network card | If the authentication type is no/pre-shared password, fill in the TAP network card mask of this end | empty |
| joggle | Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Use cellular 4G to connect to the VPN Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN | voluntarily |
| Redirect gateway | Use openvpn as the default gateway It takes effect after you select "None" in "Network Switching" The WAN port cannot use the redirect gateway function in PPPoE mode You cannot enable the redirect gateway function for multiple VPNs | close |
| Nat | Whether the data on the VPN network card is NAT | open |
| Enable Keepalive | Enable the live detection mechanism | open |
| Connection detection time interval (seconds) | VPN live heartbeat detection interval | 10 |
| Connection detection timeout interval (seconds) | If the heartbeat exceeds the set time without response, reconnect to the VPN | 120 |
| enable LZO | Data compression method | No preference |

| | | |
|-------------------------------|---|------------------|
| encryption algorithm | Data encryption algorithm | BF-CBC |
| Hash algorithm | The data's hash algorithm | SHA1 |
| TLS way | Select the TLS authentication method | OFF |
| LINK-MTU/TUN-MTU/TCP MSS | Set the data pack length | Air / air / 1450 |
| Maximum frame length | The maximum frame length of data is the default without special configuration | empty |
| Allows remote address changes | Whether to allow remote address change Settings | close |
| Log grade | Openvpn log level, the larger the number, the more detailed the log is. Generally, open a higher level to troubleshoot problems when the connection is abnormal | Warning (3) |
| Additional configuration | Non-professionals should not configure it. You need to input openvpn recognizable parameters | empty |
| Local route-destination | Set the static route target segment established by the openvpn network card on this end | empty |
| Local route-Network mask | Set the subnet mask of the static route target established by the openvpn network card on this end | empty |
| CA | Upload CA certificate | not have |
| CERT | Upload the client certificate | not have |
| KEY | Upload the client private key | not have |
| TLS | Upload the TLS certificate. If the TLS mode is selected OFF, you do not need to upload the certificate here | not have |
| Pre-shared key | Upload the pre-shared key. You can upload the certificate only when you select the authentication type as pre-shared key | not have |

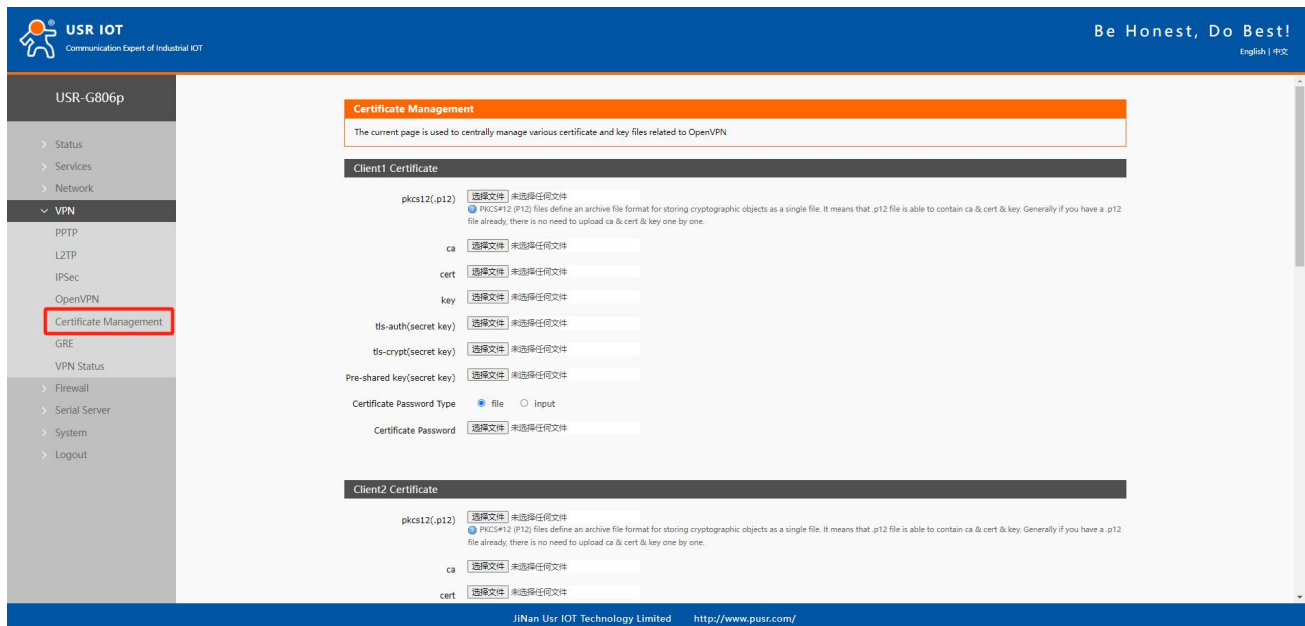
Tab 16 OpenVPN Server parameter table

| name | description | Default parameter |
|-----------------------|--|---------------------------|
| start using | Open: Start the openVPN server Close: Disable the openvpn client | close |
| description | You can customize the description of this OpenVPN path, but you don't have to fill it | empty |
| protocol | tcp/udp/tcp ipv4/udp ipv4 | udp |
| port | Set the openvpn server port number | 1194 |
| Type of certification | None, SSL/TLS, user name and password, pre-shared key, SSL/TLS+ user name and password | SSL/TLS |
| TUN/TAP | Select the network communication mode, tun/tap | tun |
| Bridge the network | The Tap mode can bridge LAN and realize two-layer interaction point to point | not have |
| Bridge network mode | TAP bridge network mode Settings | Use the device's own DHCP |

| | | |
|--|---|--------------|
| configuration | Use the device's own DHCP service: Use the router LAN port DHCP service Specify the gateway, mask, starting address and ending address: the device under the route must be connected to the same subnet as the gateway | service |
| topology | Net30/p2p/subnet, which is usually the default value | subnet |
| IPv4 tunnel network | Open the IP subnet assigned to the client for OpenVPN, such as 192.168.100.0 | empty |
| IPv4 tunnel subnet mask | Enter the subnet mask assigned to the client by OpenVPN, for example: 255.255.255.0 | empty |
| Local tunnel IP | When the authentication type is no/pre-shared password, fill in the local TUN tunnel IP | empty |
| Remote tunnel IP | When the authentication type is no/pre-shared password, fill in the end-to-end tunnel IP of this end | empty |
| begin IP | The TAP bridge mode specifies the starting IP address, such as 192.168.100.100 The LAN port of the router needs to be set to the same subnet as the network segment | empty |
| finish IP | The TAP bridge mode specifies the end IP address, such as 192.168.100.200 | empty |
| Enter the IP address of the Tap network card | If the authentication type is no/pre-shared password, fill in the IP address of the TAP network card on this end | empty |
| Tap the subnet mask of the network card | If the authentication type is no/pre-shared password, fill in the TAP network card mask of this end | empty |
| The client renegotiates the time interval | When the client reaches the set value, it will renegotiate and reconnect. This is a security mechanism of openvpn Setting both the client and this end to 0 means that only one negotiation is performed when openvpn is established If the renegotiation time is set, a very short data delay will occur after this value is reached. Unit: seconds If the router client is set to 0, additional configuration is required: reneg-sec 0 | 3600 |
| Maximum number of customers | Set the upper limit of the number of clients that can connect to the service | 16 |
| Allow client to client | Check to enable data exchange between OpenVPN clients Unchecked: Data is only exchanged between the client and the server, not between clients | check |
| Multiple clients use the same certificate | Check: Allow multiple clients to use the same client certificate to connect to the OpenVPN Server | Not selected |
| Redirect gateway | Use openvpn as the default gateway It takes effect after you select "None" in "Network Switching" | close |

| | | |
|---|---|------------------|
| | <p>The WAN port cannot use the redirect gateway function in PPPoE mode</p> <p>You cannot enable the redirect gateway function for multiple VPNs</p> | |
| Nat | Whether the data on the VPN network card is NAT | open |
| Enable Keepalive | Enable the live detection mechanism | open |
| Connection detection time interval (seconds) | VPN live heartbeat detection interval | 10 |
| Connection detection timeout interval (seconds) | If the heartbeat exceeds the set time without response, reconnect the VPN | 120 |
| Enable LZO | Data compression method | No preference |
| encryption algorithm | Data encryption algorithm | BF-CBC |
| Hash algorithm | The data's hash algorithm | SHA1 |
| TLS way | Select the TLS authentication method | OFF |
| LINK-MTU/TUN-MTU/TCP MSS | Set the data pack length | Air / air / 1450 |
| Maximum frame length | The maximum frame length of data is the default without special configuration | empty |
| Allows remote address changes | Whether to allow remote address change Settings | close |
| Log grade | Openvpn log level, the larger the number of log is more detailed, generally open a larger level to troubleshoot problems when the connection is abnormal | Warning (3) |
| Additional configuration | Non-professionals should not configure it. You need to input openvpn recognizable parameters | empty |
| user | Set the user name and password account for the client connection. Select the option with the user name and password to take effect. Set multiple accounts to set a user name and password for each client | |
| user name | Set the client connection user name, and you can set multiple user names and passwords | empty |
| password | Set the client connection password, and you can set multiple user name passwords | empty |
| The client is assigned a static IP address | Set the parameters for assigning fixed IP addresses to clients. You can set multiple fixed IP addresses for multiple clients, and each client's fixed IP address cannot be repeated | |
| user | Use the certificate form: This is set to the CN corresponding value of the client certificate, such as client1 If you use only the form of user name and password: Enter the user name value here | empty |
| Static IP address | Set the static IP address assigned to the client, such as | empty |

| | | |
|------------------------|--|----------|
| | 192.168.100.2 | |
| subnet mask | Set the subnet mask assigned to the client, for example: 255.255.255.0 | empty |
| Customer subnet | To enable subnet interworking, you need to fill in the subnet segment of each client, and openvpn will automatically push the routing function | |
| name | Use the certificate form: This is set to the CN corresponding value of the client certificate, such as client1 If you use only the form of user name and password: Enter the user name value here | empty |
| subnet | The subnet segment corresponding to the client, such as 192.168.1.0 | empty |
| subnet mask | The subnet mask corresponding to the client subnet segment, such as: 255.255.255.0 | empty |
| Local routing | Set up a static route created by the openvpn network card | |
| target | Set the static route target segment established by the openvpn network card on this end | empty |
| Network mask | Set the subnet mask of the static route target established by the openvpn network card on this end | empty |
| Certificate management | | |
| CA | Upload CA certificate | not have |
| CERT | Upload the client certificate | not have |
| KEY | Upload the client private key | not have |
| TLS | Upload the TLS certificate. If the TLS mode is selected OFF, you do not need to upload the certificate here | not have |
| Pre-shared key | Upload the pre-shared key. You can upload the certificate only when you select the authentication type as pre-shared key | not have |



Pic 33 OpenVPN certificate page

Tab 17 OpenVPN Server parameter table

| name | description | Default parameter |
|---------------------------------|---|-------------------|
| Client certificate | Openvpn Settings with SSL/TLS or user name and password require the corresponding certificate to be passed If openvpn opens client 1, please upload the certificate to the client 1 certificate list, otherwise the openvpn will fail to establish | |
| Pkcs12(.p12) | This certificate type is a file archiving format. If the generated client certificate suffix is.p12, you can enter it here. Generally, if you enter X.p12 certificate, you do not need to enter ca&.cert&.key certificate one by one | empty |
| Ca | If you choose to authenticate with a user name and password or SSL, the CA certificate must be sent | empty |
| Cert | Enter the client certificate and select the SSL authentication type. This certificate must be sent | empty |
| Key | Enter the client key and select the SSL authentication type. This certificate must be sent | empty |
| Tls-auth (key) | If the openvpn TLS mode is set to tls-auth, you need to enter the TLS key here | empty |
| Tls-crypt (key) | If the openvpn TLS mode is set totls-crypt, the TLS key must be passed here | empty |
| Pre-share the key | When the authentication type is selected to pre-share the key, enter the pre-shared key certificate here | empty |
| Certificate password input type | If a certificate password is generated, it must be set according to the file or manually entered type | document |
| Certificate password | The password of the PEM certificate can be entered or uploaded (the password is in the file). If the certificate is | empty |

| | | |
|---------------------------------|--|----------|
| | generated without a password, do not fill in this field | |
| Server certificate | Openvpn server Settings with SSL/TLS or user name and password require the corresponding certificate to be passed | |
| Pkcs12(.p12) | This certificate type is a file archiving format. If the generated client certificate suffix is.p12, you can enter it here. Generally, if you enter an X.p12 certificate, you do not need to enter one by one certificates with the suffix.ca&.cert&.key | empty |
| Ca | If you choose to authenticate with a user name and password or SSL, the CA certificate must be sent | empty |
| Cert | Pass the client certificate, if you select authentication type with user name and password or SSL, this certificate must be passed | empty |
| Key | Pass the client secret key, if you select the authentication type with user name and password or ssl, this certificate must be passed | empty |
| DH | To transfer the DH certificate, if you select an authentication type with a user name and password or SSL, this certificate must be passed | |
| Tls-auth (key) | If the openvpn TLS mode is set to tls-auth, you need to enter the TLS key here | empty |
| Tls-crypt (key) | If the openvpn TLS mode is set to tls-crypt, you need to enter the TLS key here | empty |
| Pre-share the key | When the authentication type is selected to pre-share the key, enter the pre-shared key certificate here | empty |
| Certificate revocation list | | |
| Certificate password input type | If a certificate password is generated, it must be set according to the file or manually entered type | document |
| Certificate password | The password of the PEM certificate can be entered or uploaded (the password is in the file). If the password is generated, do not fill in here | empty |

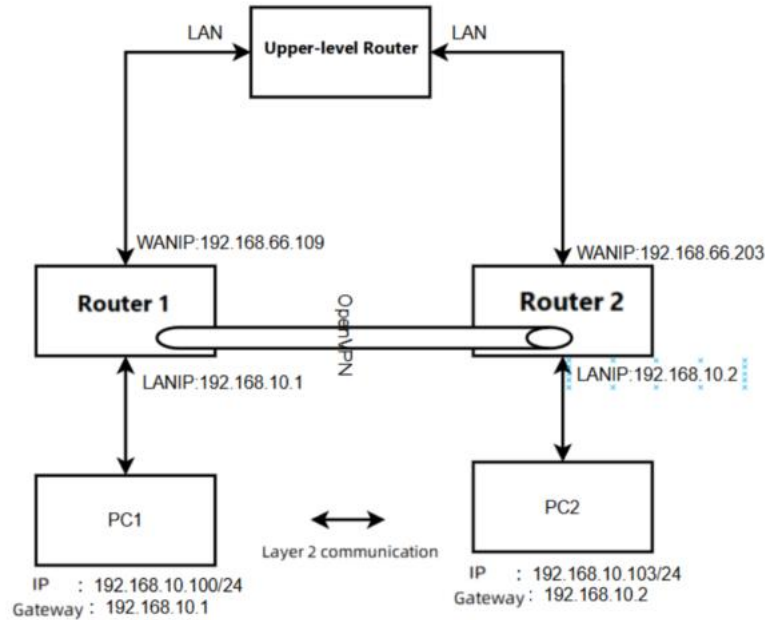
< explain >

- Tap bridge mode can realize the two-layer data interaction;
- When the router is used as a VPN server, it is recommended to access up to 2 VPN clients. If the transmission service is used, please use professional VPN server equipment to build a VPN Server;
- Some people do not provide the certificate required for OpenVPN, and customers need to generate it themselves.

4.4.1. OpenVPN TAP bridge example

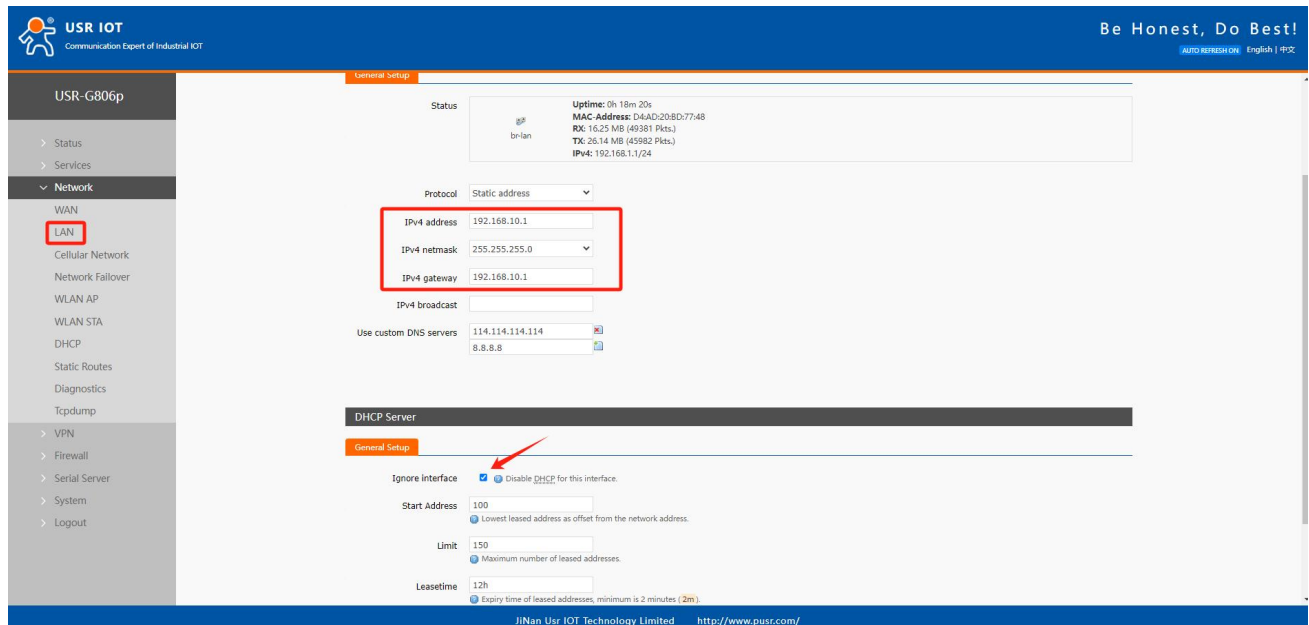
It is generally used for APN dedicated network card +OpenVPN to realize the function of LAN for multiple terminals.

Note: In this scheme, LAN port DHCP should be turned off for each router, and the router configuration should be in the same network segment and the IP address should not conflict.



Pic 34 Connect the topology

The router 1 is configured as an openVPN server. The specific configuration is as follows: The LAN port is set to the network segment and DHCP allocation is turned off. At this time, PC1 needs to be set to a static IP address to log in to the router web for configuration.



Pic 35 LAN port configuration

The following screenshot is configured, and the rest are default parameters.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!
English | 中文

USR-G806p

- > Status
- > Services
- > Network
- > **VPN**
 - PPTP
 - L2TP
 - IPSec
 - OpenVPN**
 - Certificate Management
 - GRE
 - VPN Status
- > Firewall
- > Serial Server
- > System
- > Logout

SERVER 1 - OpenVPN Configuration

Configuration

Enable: ON

Description: The maximum length is 50 Bytes.

Enable OpenVPN Config from file: Not Support

Protocol: UDP

Port: 1194

Authentication Type: Username/Password

TUN/TAP: TAP

Bridge Network: LAN

Tap bridging network configuration mode: Use your own dhcp service

Renegotiation Interval(s): 3600

max clients: 16 Allow a maximum of n simultaneously connected clients.

Client to client: ☒ Internally route client-to-client traffic.

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 36 OpenVPN configuration 1

Set a set of user names and passwords.

USR IOT
Communication Expert of Industrial IOT

Be Honest,

USR-G806p

- > Status
- > Services
- > Network
- > **VPN**
 - PPTP
 - L2TP
 - IPSec
 - OpenVPN**
 - Certificate Management
 - GRE
 - VPN Status
- > Firewall
- > Serial Server
- > System
- > Logout

Extra Option

The content here will be written directly to the configuration file. Please fill in carefully

| User | |
|----------|----------|
| Username | Password |
| test | test |

New User:

Username: Password:

Client Static Ip

| User | Static Ip | Netmask/P2P IP |
|-------------------------------------|-----------|----------------|
| This section contains no values yet | | |

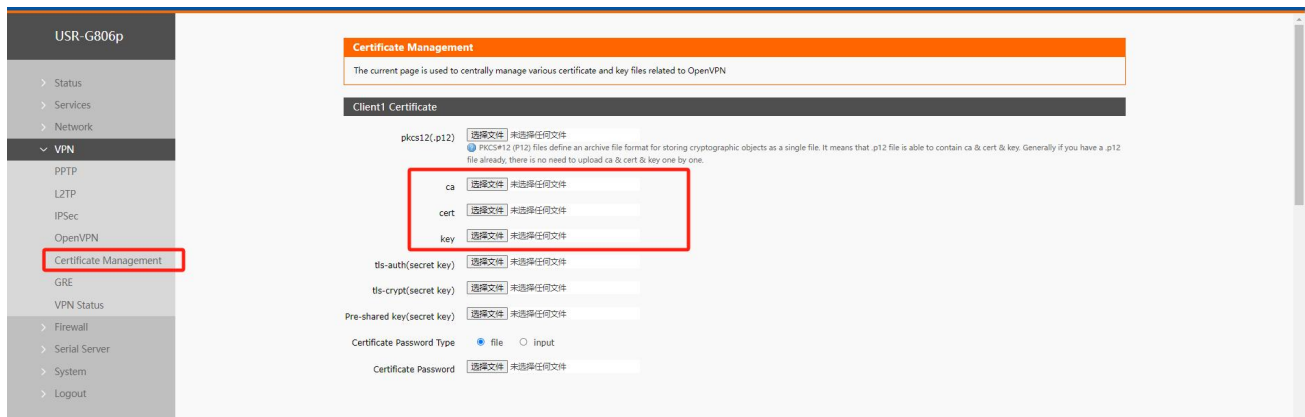
Tunnel static IP:

| User | Static IP | Netmask/P2P IP |
|------|-----------|----------------|
|------|-----------|----------------|

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

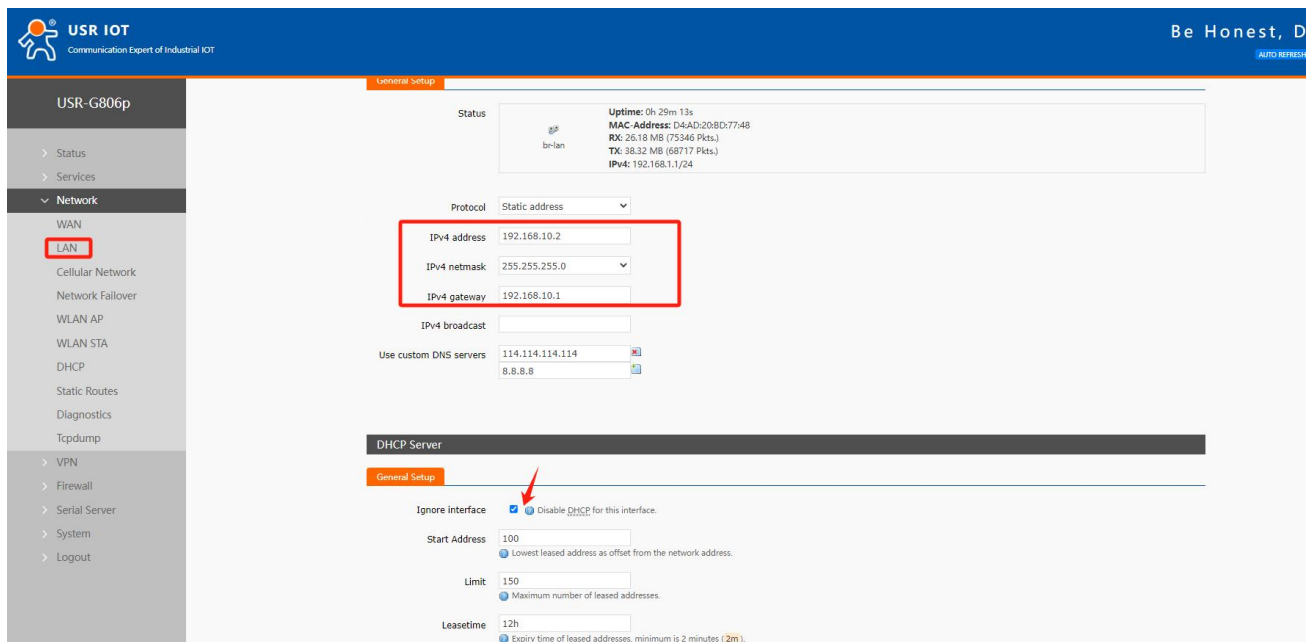
Pic 37 OpenVPN configuration 2

The server needs to pass the openvpn server certificate, including the CA certificate, server certificate, server key and DH certificate.



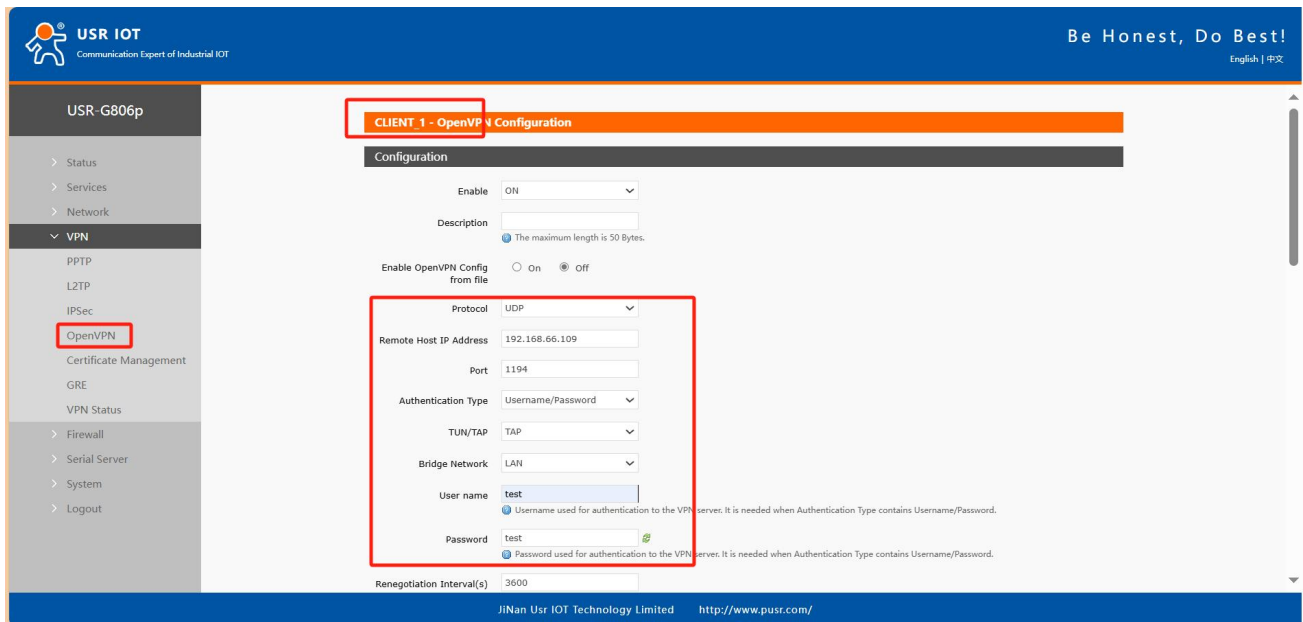
Pic 38 OpenVPN configuration 3

The router is configured as an openVPN client. The specific configuration is as follows: LAN port is set to the network segment and DHCP allocation is turned off. At this time, PC2 needs to be set to a static IP address to log in to the router web for configuration.

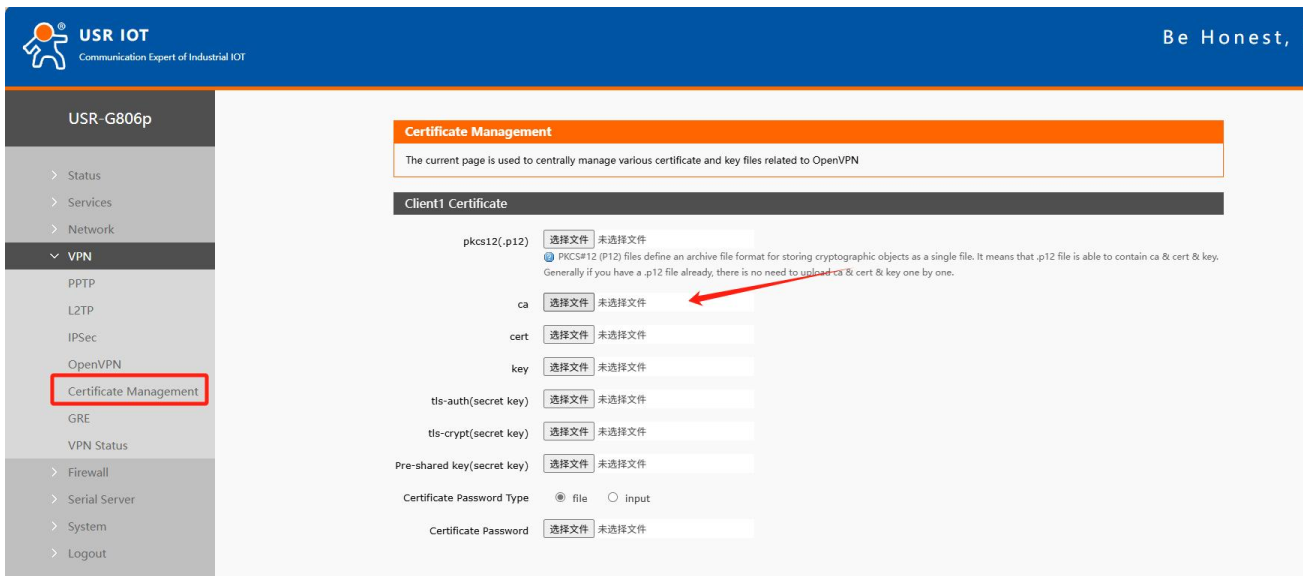


Pic 39 LAN port configuration

The following screenshot is configured. All other parameters are default parameters.



Pic 40 OpenVPN configuration 1



Pic 41 OpenVPN configuration 2

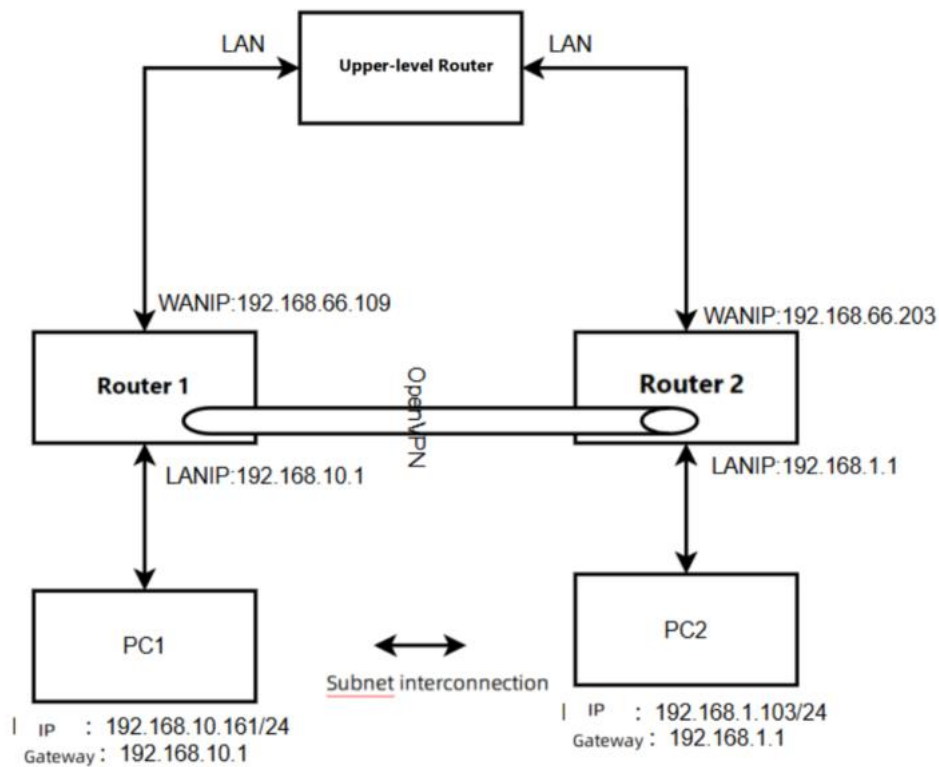
Test that PC1 and PC2 can communicate with each other:

```

    最长 = 1ms, 最长 = 1ms, 平均 = 1ms
Control-C
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.10.1
正在 Ping 192.168.10.1 具有 32 字节的数据:
来自 192.168.10.1 的回复: 字节=32 时间<1ms TTL=64
192.168.10.1 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最长 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
C:\Users\Administrator>ping 192.168.10.2
正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间<2ms TTL=64
192.168.10.2 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最长 = 2ms, 最长 = 2ms, 平均 = 2ms
Control-C
C:\Users\Administrator>ping 192.168.10.103
正在 Ping 192.168.10.103 具有 32 字节的数据:
来自 192.168.10.103 的回复: 字节=32 时间=76ms TTL=64
来自 192.168.10.103 的回复: 字节=32 时间=5ms TTL=64
192.168.10.103 的 Ping 统计信息:
    数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最长 = 5ms, 最长 = 76ms, 平均 = 40ms
Control-C
C:\Users\Administrator>

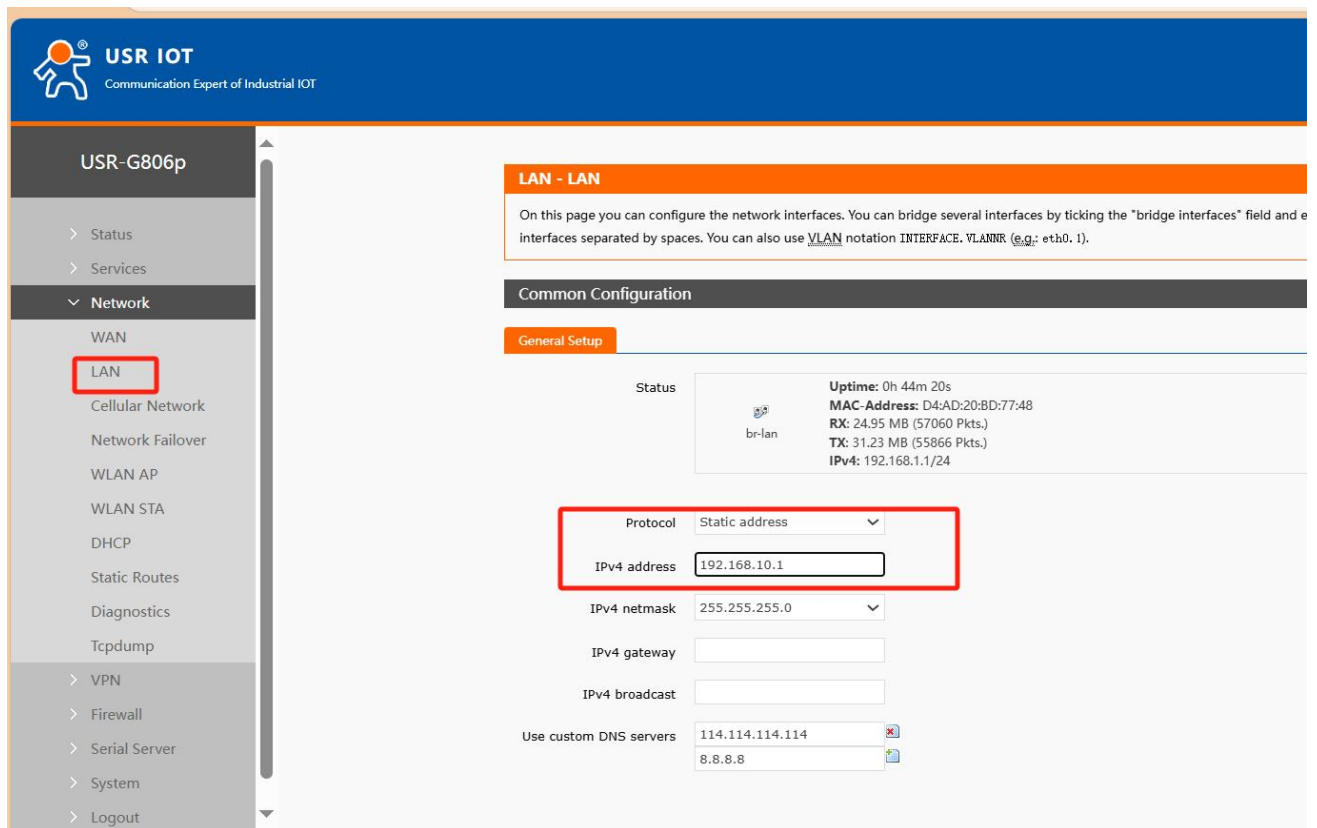
```

4.4.2. An example of subnet interworking in OpenVPN TUN mode



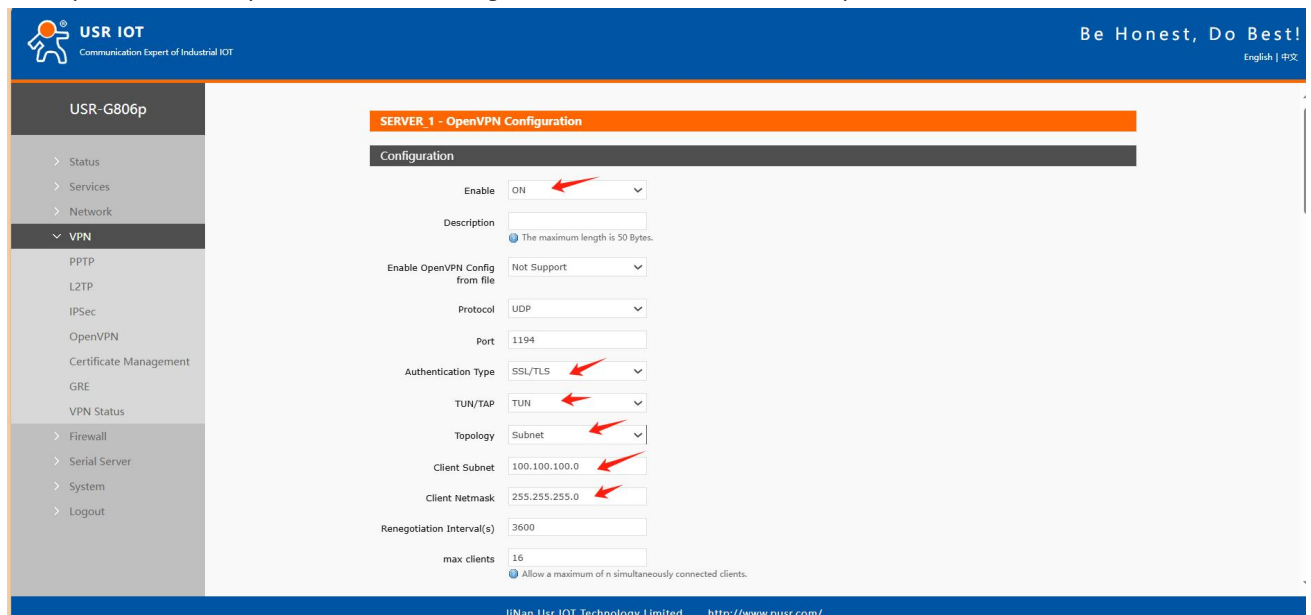
Pic 42 Connect the topology

Router 1 configuration, LAN port setting



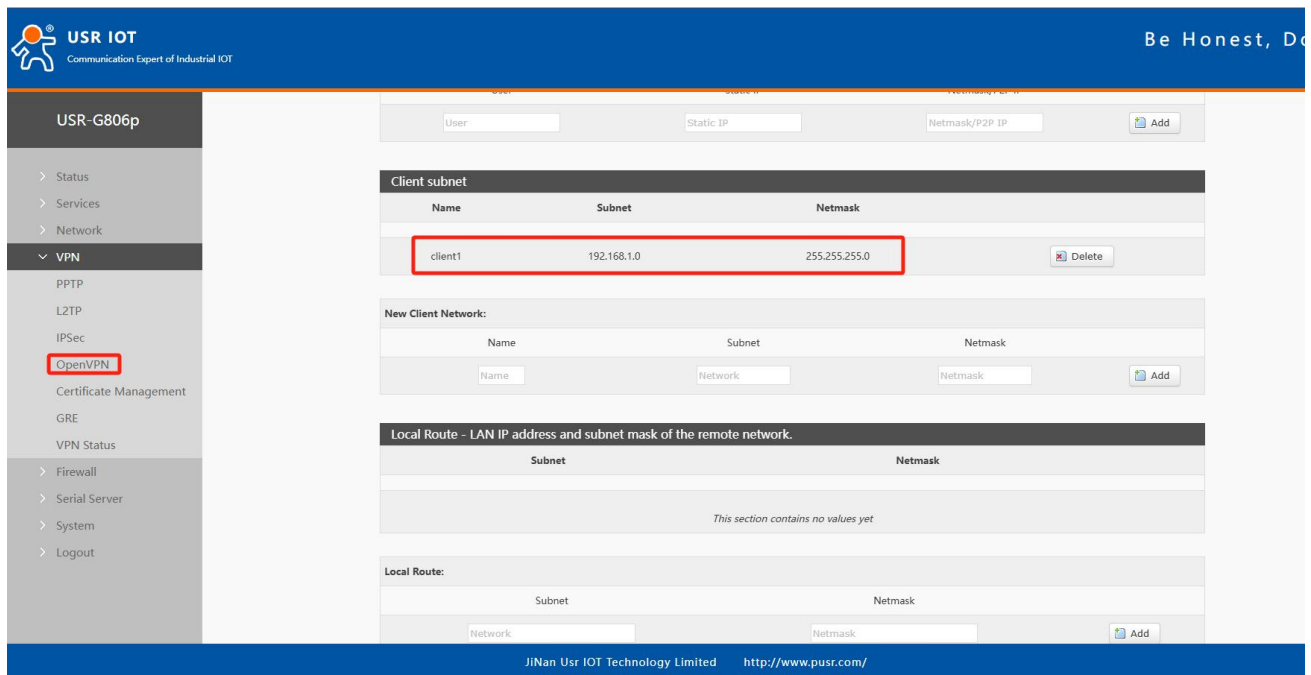
Pic 43 Router 1 is configured 1

The OpenVPN Server parameters are configured as follows, and all other parameters remain the default.



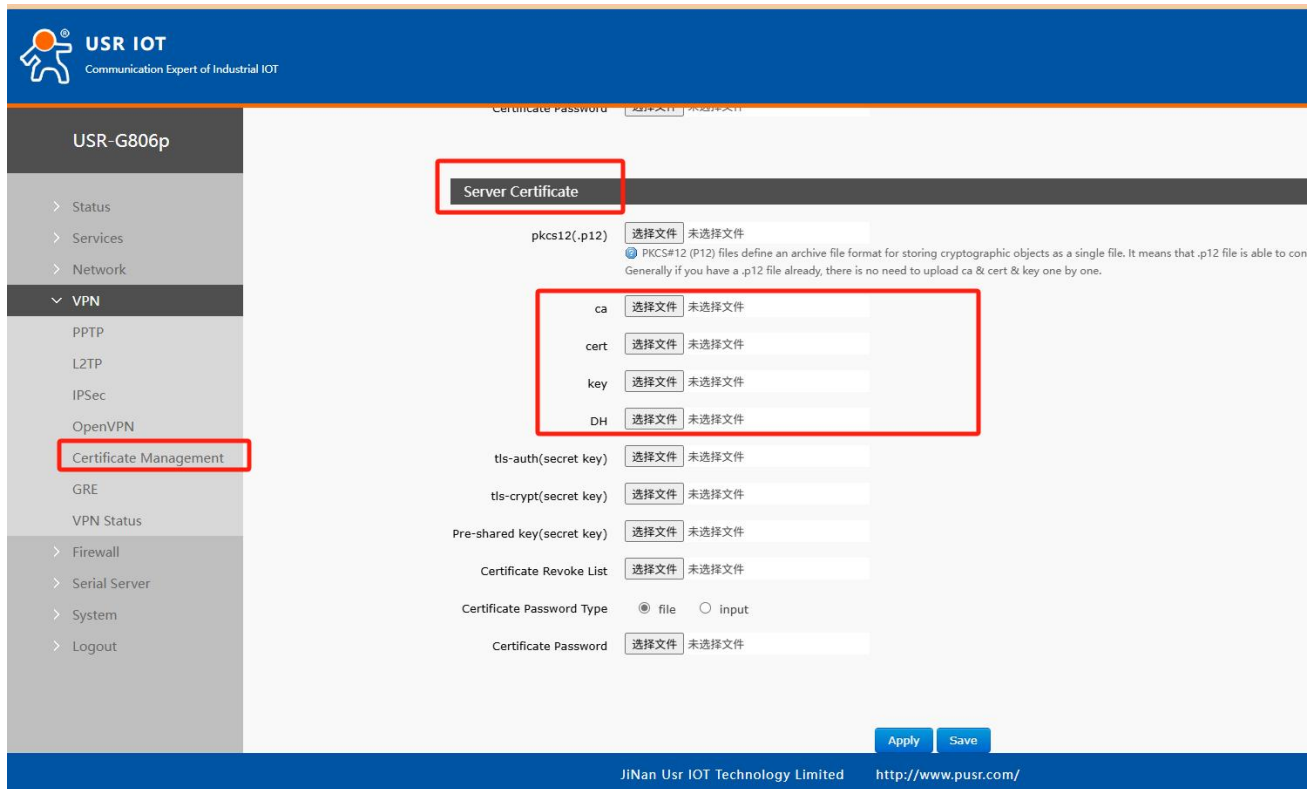
Pic 44 Router 1 is configured 2

Enter the client subnet information and click "Save"



Pic 45 Router 1 is configured 3

Enter the OpenVPN server certificate and click "Apply".



Pic 46 Router 1 is configured for 4

The router is configured as OpenVPN client. The configuration is as follows, and other parameters are kept as default (the parameters and the server are consistent).

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

- Status
- Services
- Network
- VPN**
 - PPTP
 - L2TP
 - IPSec
 - OpenVPN**
 - Certificate Management
 - GRE
 - VPN Status
- Firewall
- Serial Server
- System
- Logout

CLIENT 1 - OpenVPN Configuration

Configuration

Enable: ON

Description: The maximum length is 50 Bytes.

Enable OpenVPN Config from file: ☐ On ☒ Off

Protocol: UDP

Remote Host IP Address: 192.168.66.109

Port: 1194

Authentication Type: SSL/TLS

TUN/TAP: TUN

Topology: Subnet

Renegotiation Interval(s): 3600

Interface: Auto Auto refers used default route interface to connect

redirect-gateway: ☐

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

Pic 47 Router 2 is configured 1

Client adds information to the server subnet.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

- Status
- Services
- Network
- VPN**
 - PPTP
 - L2TP
 - IPSec
 - OpenVPN**
 - Certificate Management
 - GRE
 - VPN Status
- Firewall
- Serial Server
- System
- Logout

Fragment: ☐ Enable internal datagram fragmentation:128~1500.If you are not familiar with this option, please leave it empty.

Remote Addr Float: ☐ Allowing the remote end to change its IP address/port

Log Level: warning(3) Log Level:0-11

Extra Option: The content here will be written directly to the configuration file. Please fill in carefully

Local Route - LAN IP address and subnet mask of the remote network.

| Subnet | Netmask | |
|--------------|---------------|--------|
| 192.168.10.0 | 255.255.255.0 | Delete |

Local Route:

| Subnet | Netmask | |
|----------|----------|-----|
| Network: | Netmask: | Add |

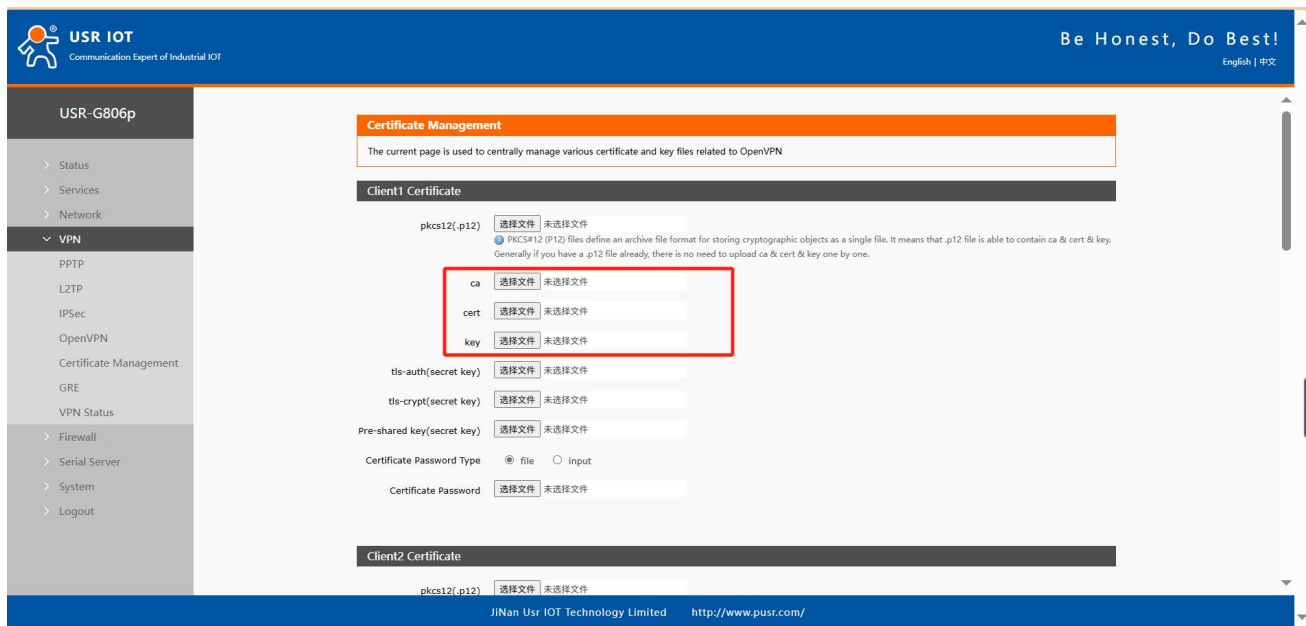
Back to Overview

Apply Save

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

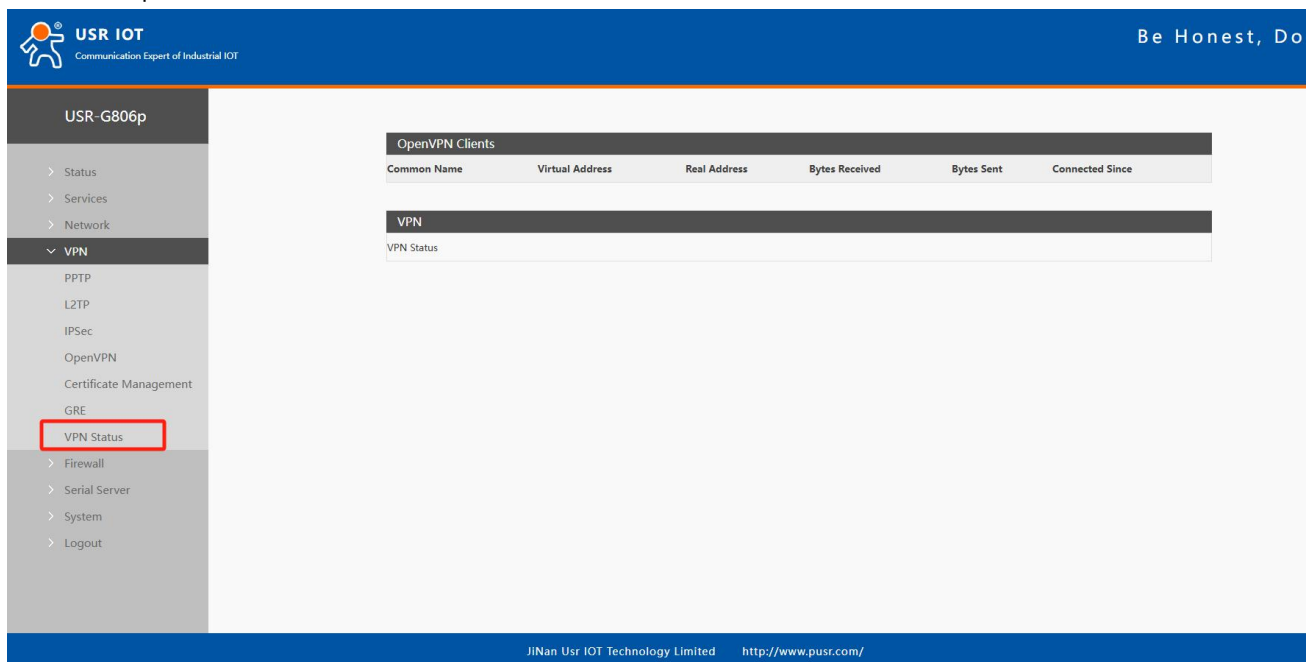
Pic 48 Router 2 is configured 2

Enter the OpenVPN client certificate and click "Apply".

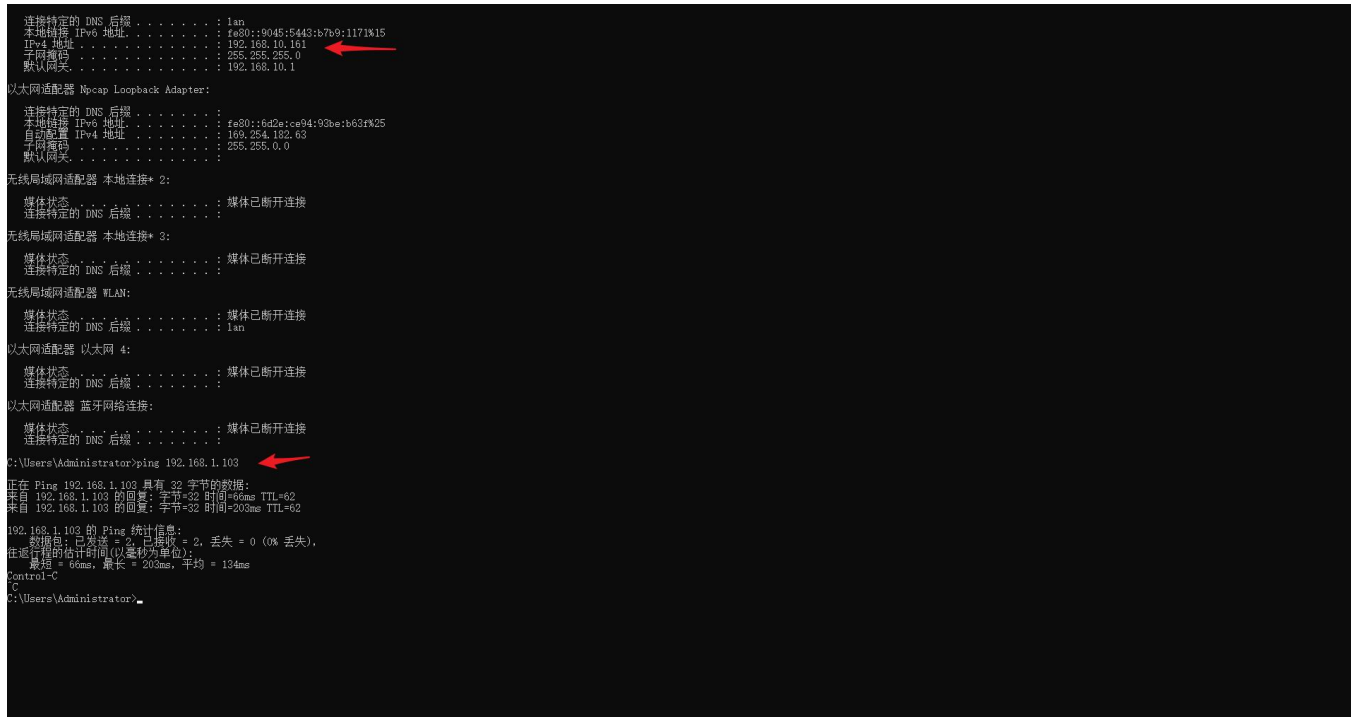


Pic 49 Router 2 is configured 3

Check the OpenVPN connection status. There is a client1 connected to the service.

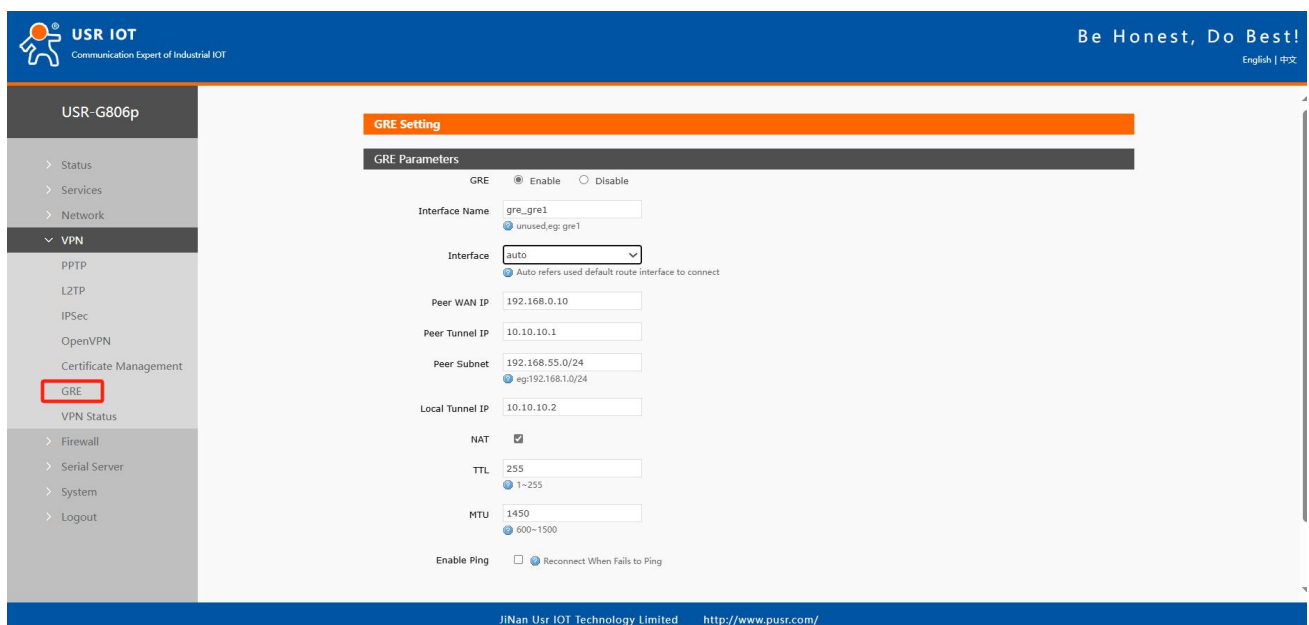


PC1 and PC2 are interconnected



Pic 50 PC1 and PC2 are interconnected

4.5. GRE



Pic 51 GRE basic configuration

< explain >

- Remote address: WAN port IP address of the remote GRE;
- Local address: The local wan_wired and wan_4g addresses are input according to different networking modes;
- Remote tunnel address: GRE tunnel IP of the other end;
- For the subnet: For setting the subnet mask, it can be expressed as follows: 255.255.255.0 can be written as

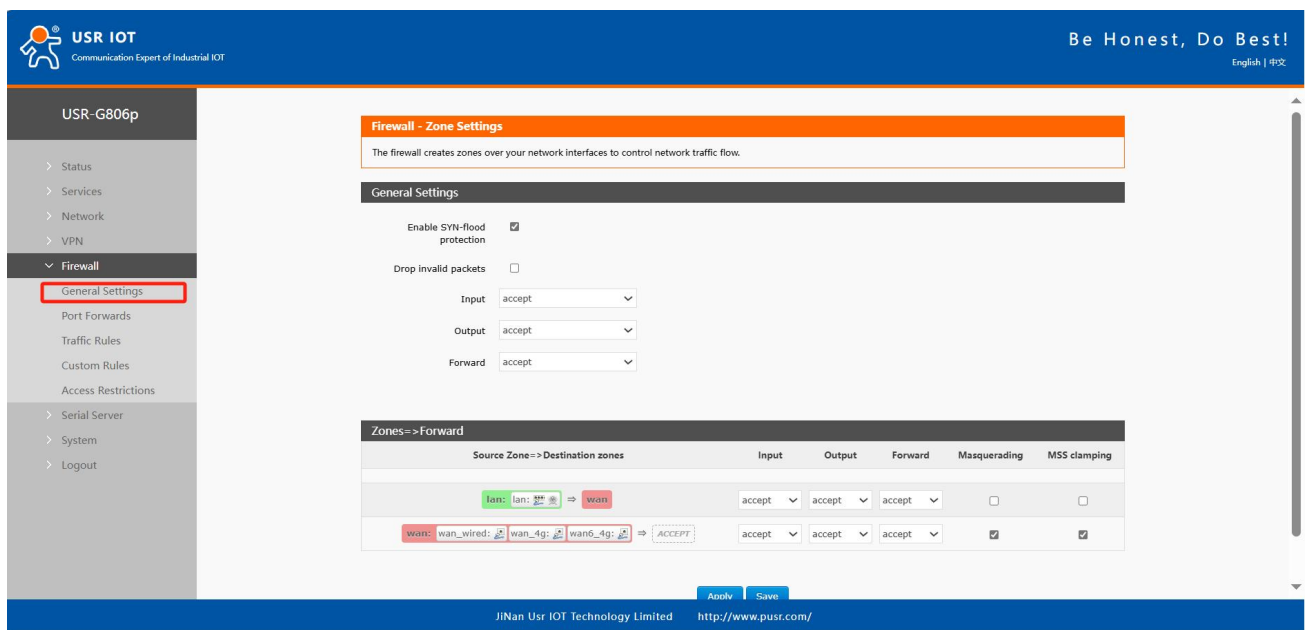
IP/24, and 255.255.255.255 can be written as IP/32. For example: 172.16.10.1/24 corresponds to IP 172.16.10.1, and the subnet mask is 255.255.255.0;

- Local tunnel IP: Local GRE tunnel IP address;
- NAT: Whether the data passing through the GRE interface needs NAT;
- TTL setting: Set the TTL of GRE channel, default 255;
- Set MTU: Set the MTU of the GRE channel. The default is 1450.

5. Firewall

5.1. Basic Settings

The default is to enable two firewall rules.



Pic 52 Firewall Settings page

[Term Introduction]

- Inbound: packets that access the router IP;
- Outgoing: The packet that the router IP is sending;
- Forwarding: Data forwarding between interfaces does not go through the routing itself;
- IP dynamic disguise: only meaningful for WAN port and 4G port, IP address disguise when accessing the Internet;
- MSS clamping: limit the MSS size of the message, usually 1460.

[Rule 1]

- Inbound LAN port to wired WAN port, and forwarding, are all received;
- If a packet comes from the LAN port and wants to access the WAN port, this rule allows the packet to be forwarded from the LAN port to the WAN port, which is forwarding;
- You can also open the router's web page under the LAN port, which is "inbound";
- The router itself connects to the Internet, such as synchronizing time, which is "outgoing".



[Rule 2]

- The wired WAN port and 4G port accept "incoming", "outgoing" and allow "forwarding";
- If there is an "incoming" packet, such as someone trying to log in to the router's web page from a WAN port, it will be allowed;
- If there is an "outgoing" packet, such as a router accessing the Internet through a WAN port or 4G port, this action is allowed;
- If there is a "forwarding" packet, such as a packet coming from the WAN port that wants to be forwarded to the LAN port, this action is allowed.

5.2. Communication rules

Communication rules can selectively filter specific Internet data types and block Internet access requests to enhance network security. Firewalls are widely used, and the following is a brief introduction to some common applications.

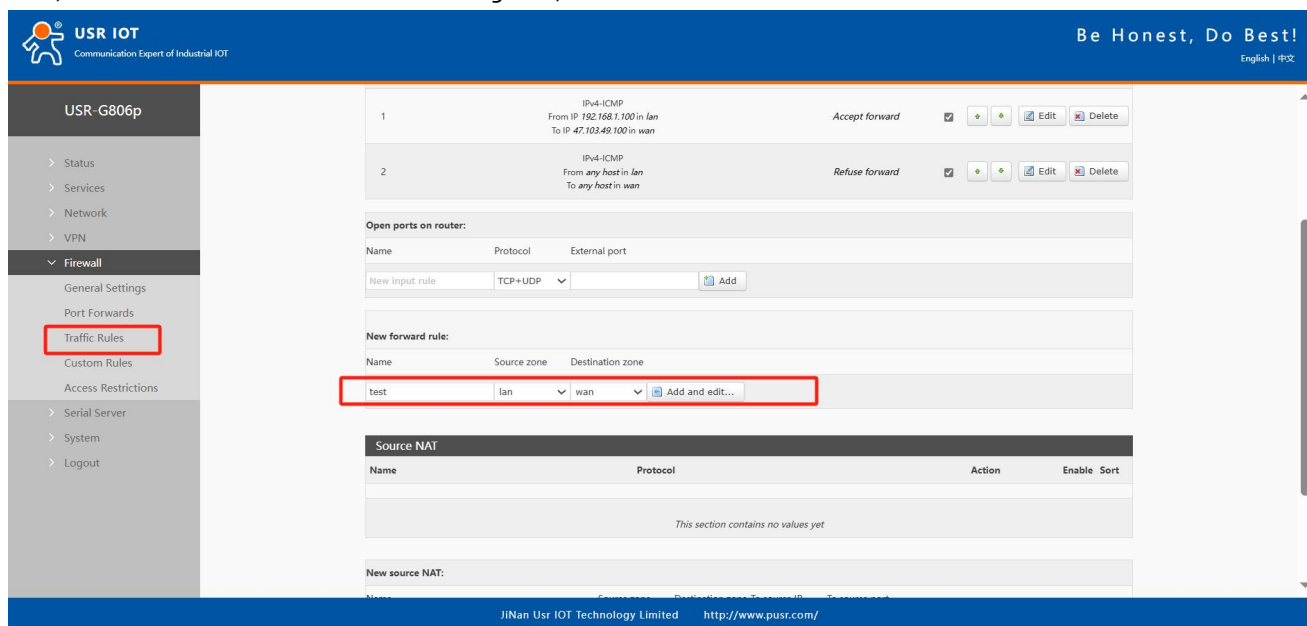
Tab 18 Communication rule parameter table

| name | description | Default parameter |
|--------------------|--|---------------------|
| start using | The display  indicates the enabled state The display  indicates the disabled state | start using |
| name | Name of this rule, character type | - |
| Limit addresses | Restrict IPv4 addresses | Only IPv4 addresses |
| protocol | The types of protocols that can be restricted by rules are selected from: TCP+UDP/TCP/UDP/ICMP | TCP+UDP |
| Match ICMP type | For the matching ICMP rule, select any | Any |
| Source area | Data stream source area, can be selected: any area, WAN, LAN LAN: Indicates the rules for subnet access to the Internet WAN: Indicates the rules for accessing the Intranet from the Internet | LAN |
| Source MAC address | The source MAC that needs to match the rule Empty: Represents a match for all MACs Note: When matching the source MAC address, set the source IP address to empty | empty |
| Source IP address | The source IP to match the rule with Empty: Matches all IP addresses Note: When matching the source IP address, set the source MAC address to null | empty |
| Source port | The source port that needs to match the rule Empty: Represents matching all ports | empty |
| target area | Data flow target area, can be selected: any area, WAN, LAN | WAN |

| | | |
|---------------------|--|--------|
| | LAN: Indicates the rules for subnet access to the Internet WAN: Indicates the rules for accessing the Intranet from the Internet | |
| destination address | The target IP address to visit Empty: Represents all addresses | empty |
| Target port | The target port number to visit Air: represents all | empty |
| movement | Receive such packets with options: discard, accept, reject, or no action Discard: This rule packet will be discarded upon receipt Accept: The packet will be accepted if it is received Reject: This rule packet will be rejected upon receipt No action: No action is taken when this rule packet is received | accept |

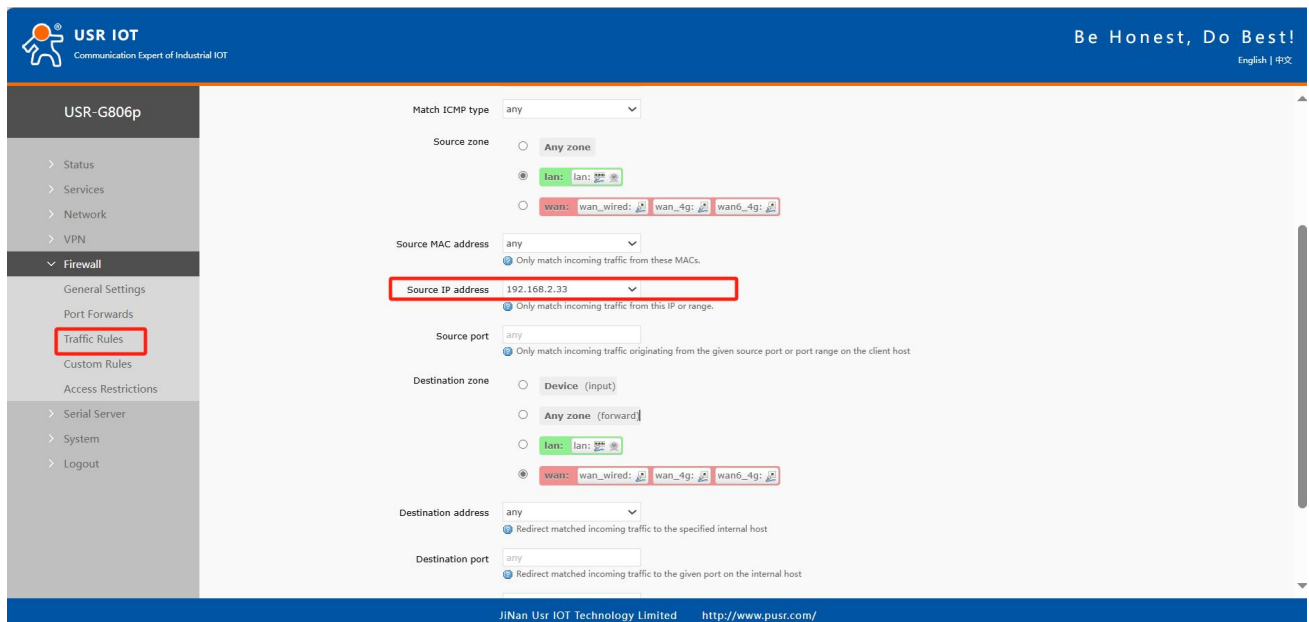
5.2.1. IP address blacklist

First, enter the name of the new forwarding rule, and then click the "Add and Edit" button



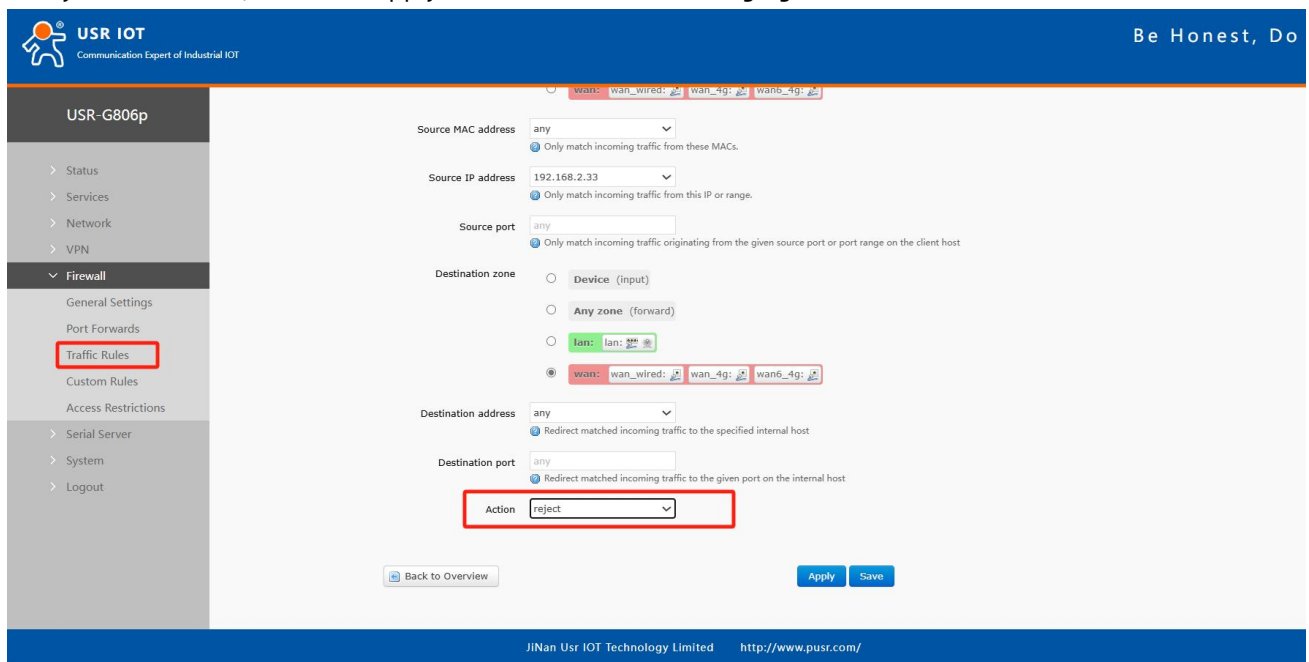
Pic 53 Figure 1 of the firewall blacklist

In the redirected page, select LAN for the source area, and select all for the source MAC address and source address (if you only restrict a specific IP address within the LAN to access a specific IP address outside the LAN, you need to fill in the IP address or MAC address), as shown in the following figure:

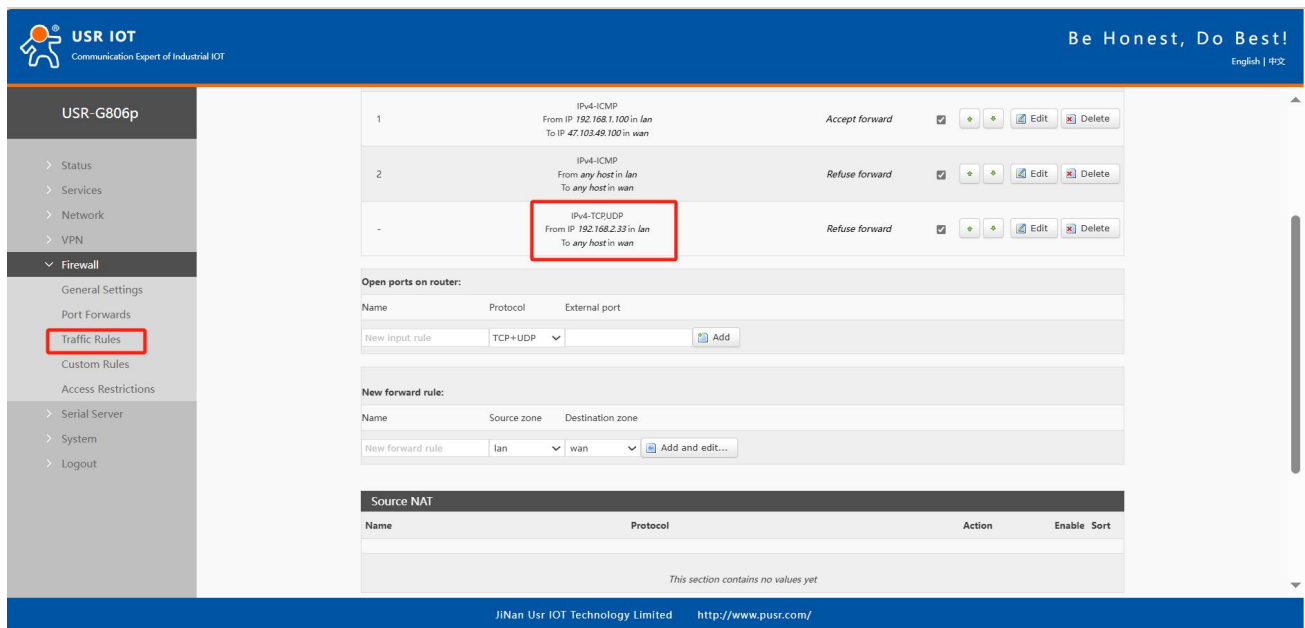


Pic 54 Figure 2 of the firewall blacklist

Select WAN in the target area, fill in the IP address that is prohibited from access in the target address, select "Deny" for the action, and click "Apply". As shown in the following figure.



Pic 55 Figure 3 of the firewall blacklist

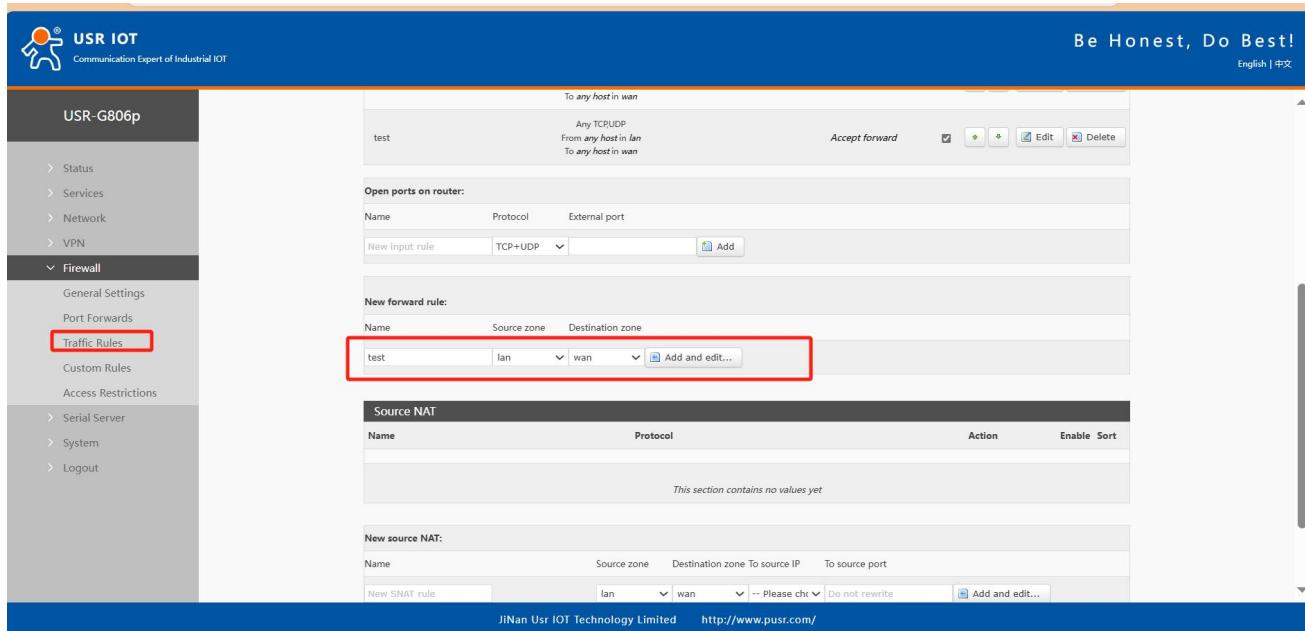


Pic 56 Figure 4 of the firewall blacklist

After this setting is completed, the blacklist function is implemented. That is, the IP address of the subnet device 192.168.2.133 is prohibited from accessing all external networks.

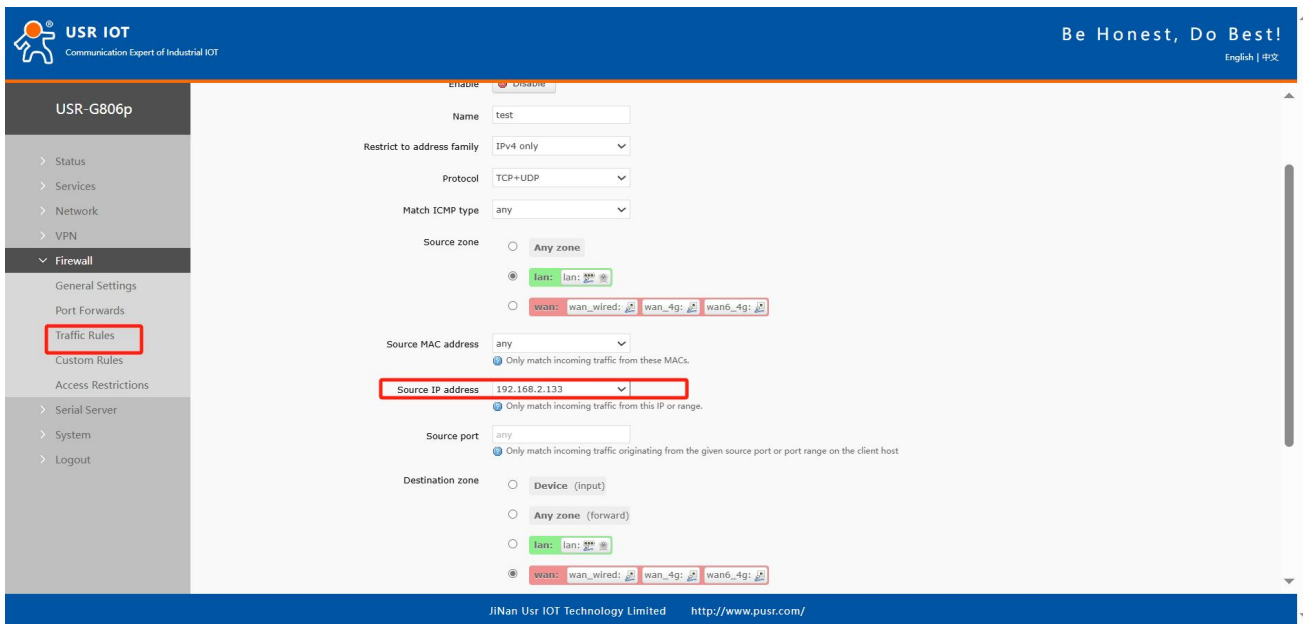
5.2.2. IP address whitelist

First, add the communication rules for the IP or MAC address to be added to the whitelist. Enter the name of the rule in the new forwarding rule, and then click the "Add and Edit" button.



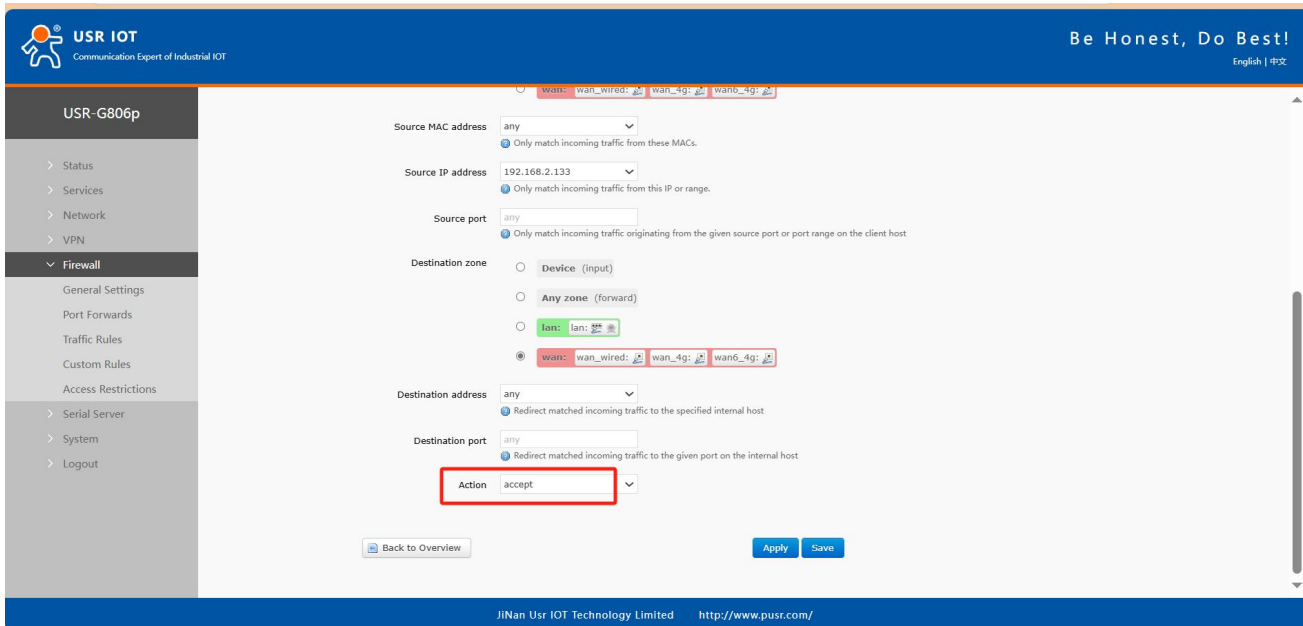
Pic 57 Firewall whitelist Figure 1

In the redirected page, select LAN for the source area, and select All for the source MAC address and source address (if you want to allow a specific IP address within the LAN to access a specific IP address outside the LAN, enter the IP address or MAC address here, as shown in the figure below



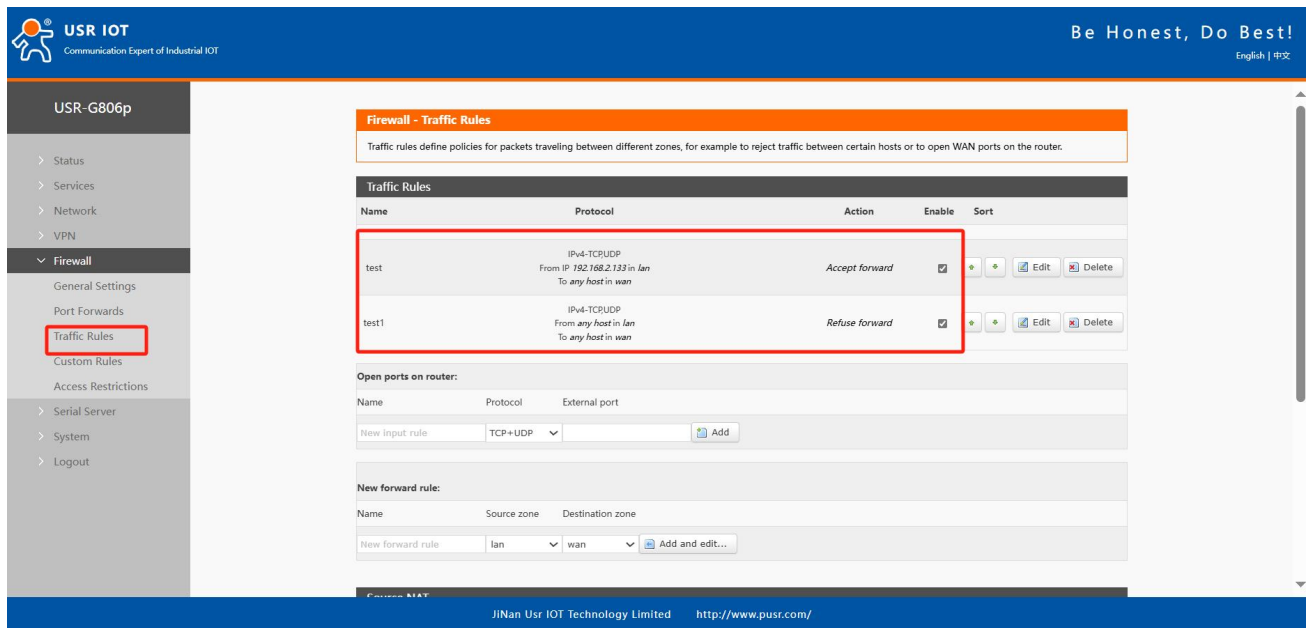
Pic 58 Figure 2 of the firewall whitelist

Select WAN in the target area, fill in the IP address that is allowed to access the target address, select "Accept" for the action, and click "Save and apply" after the setting is completed. As shown in the figure below.



Pic 59 Figure 3: Firewall whitelist

Next, set a rule that all communications are rejected. Set the source address to "all", the target address to "all", and the action to "reject". Note that the order of the two rules must be allowed first and rejected later. The overall setting is as follows



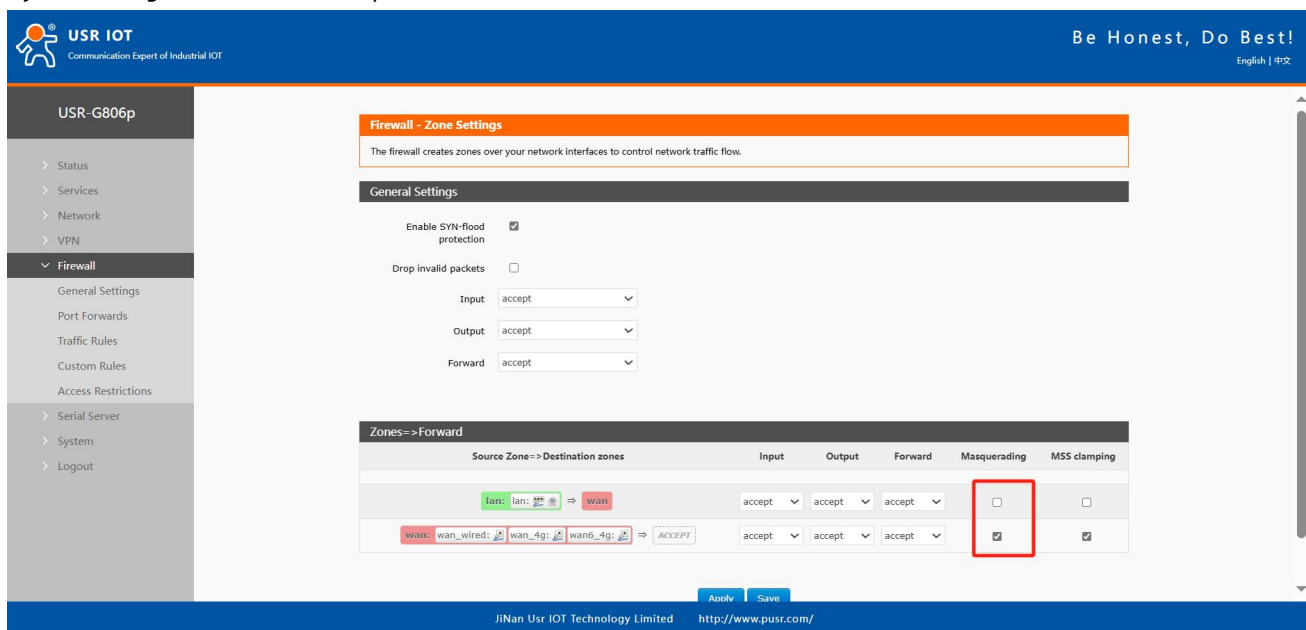
Pic 60 Figure 3 of the firewall whitelist

5.3. NAT function

5.3.1. IP address spoofing

IP address disguise converts the source IP of a departing packet to the IP address of a router interface. If you select IP dynamic disguise in the figure, the system changes the source IP address of a packet flowing out of the router to the WAN port IP address.

Note: WAN interface must enable IP dynamic disguise and MSS clamp, LAN interface is prohibited to enable IP dynamic disguise and MSS clamp.





Pic 61 IP address disguise Settings

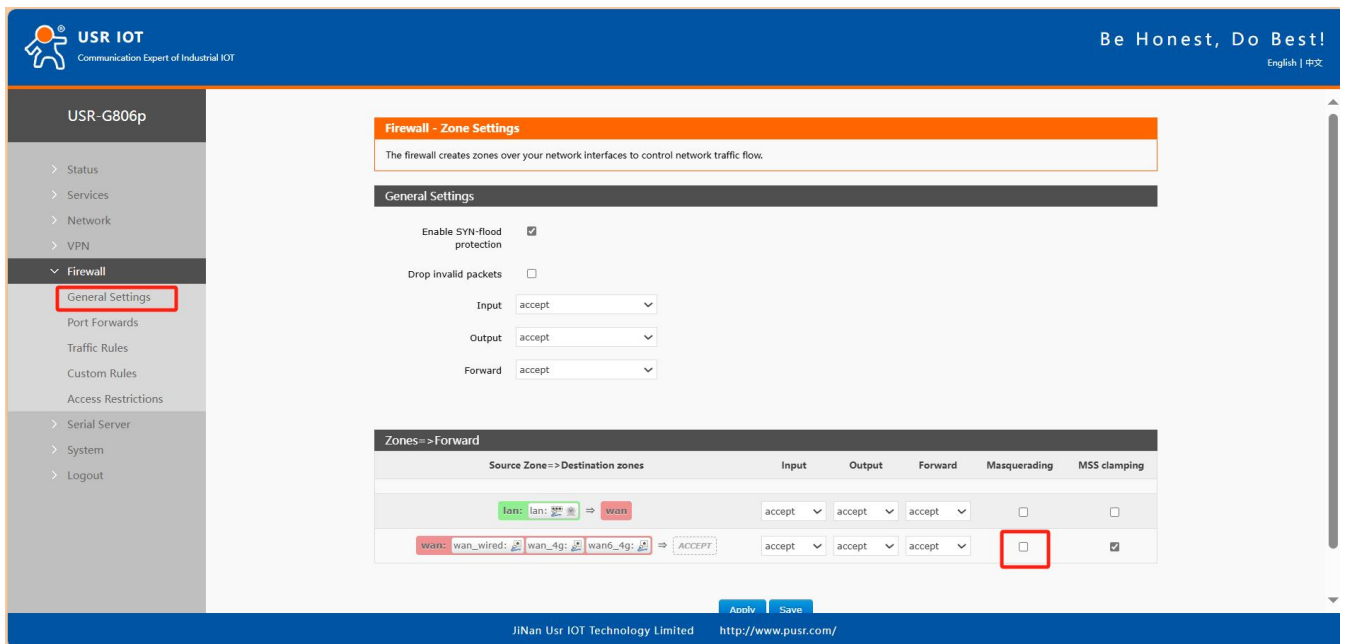
5.3.2. SNAT

Source IP conversion function.

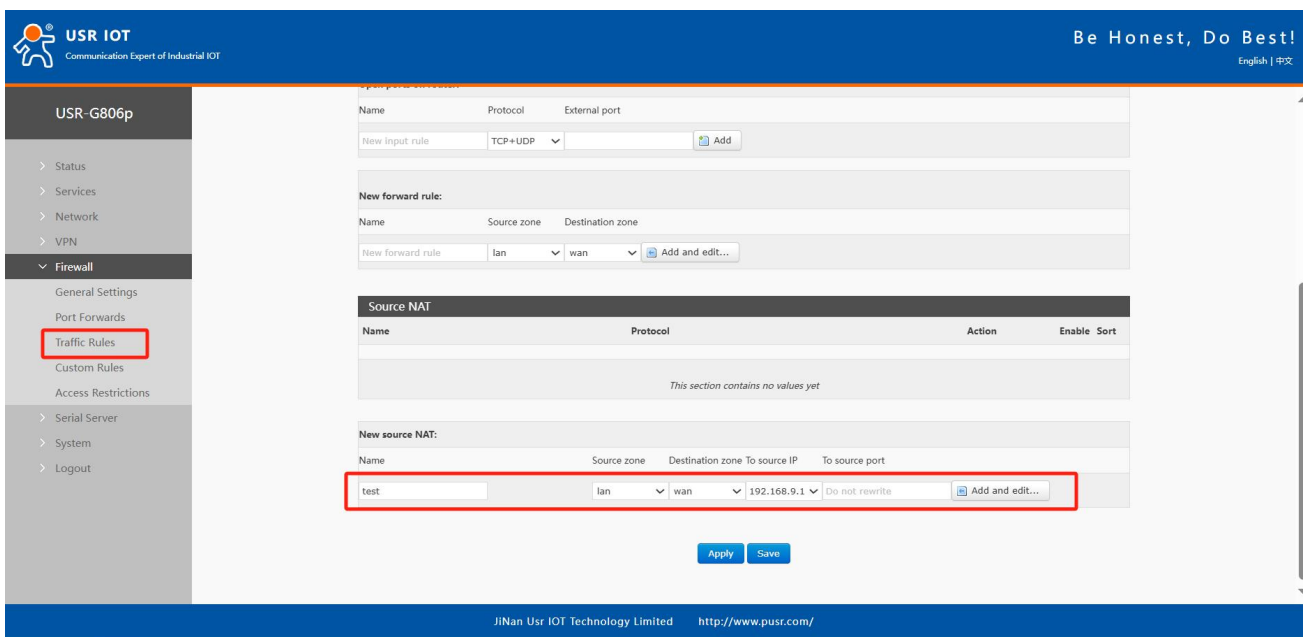
Tab 19 SNAT parameter list

| name | description | Default parameter |
|-------------------|---|-------------------------|
| Enable the button | The display  indicates the enabled state The display  indicates the disabled state | start using |
| name | The name of this firewall rule | - |
| protocol | Settings can be set: TCP+UDP/TCP/UDP/ICMP | TCP+UDP |
| Source IP address | The source IP that matches the incoming traffic needs to be matched Empty means that all source IP addresses are matched | empty |
| Source port | The source port that matches the incoming traffic needs to be matched Empty means that all source ports are matched | empty |
| objective IP | The target IP to match incoming traffic to Empty means that all target IP addresses are matched | empty |
| Target port | The target port or must be matched to inbound traffic Empty indicates that the target port is matched | empty |
| SNAT IP address | Change the source address of the matching traffic to this address | Add a custom IP address |
| SNAT port | Change the source port that matches the traffic to this port Empty indicates that the source port is used | empty |

Source NAT is a special form of packet disguise that changes the source address of packets leaving the router. When using it, the IP dynamic disguise on the wan port is first turned off

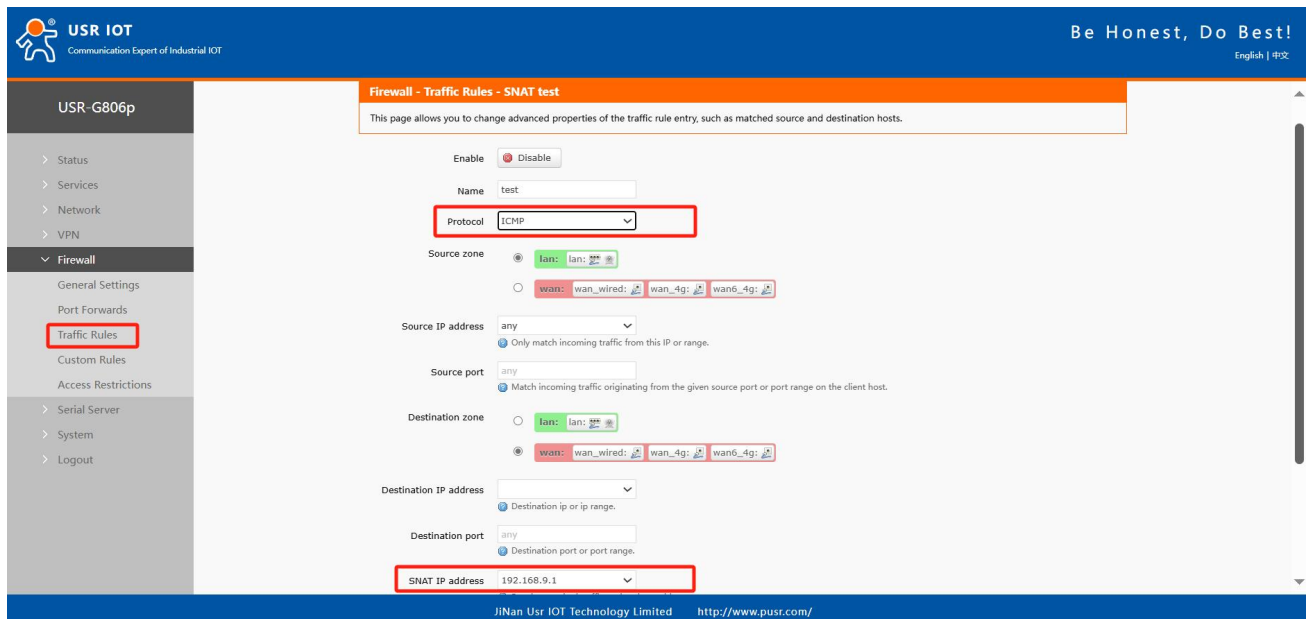


Then set up the Source NAT



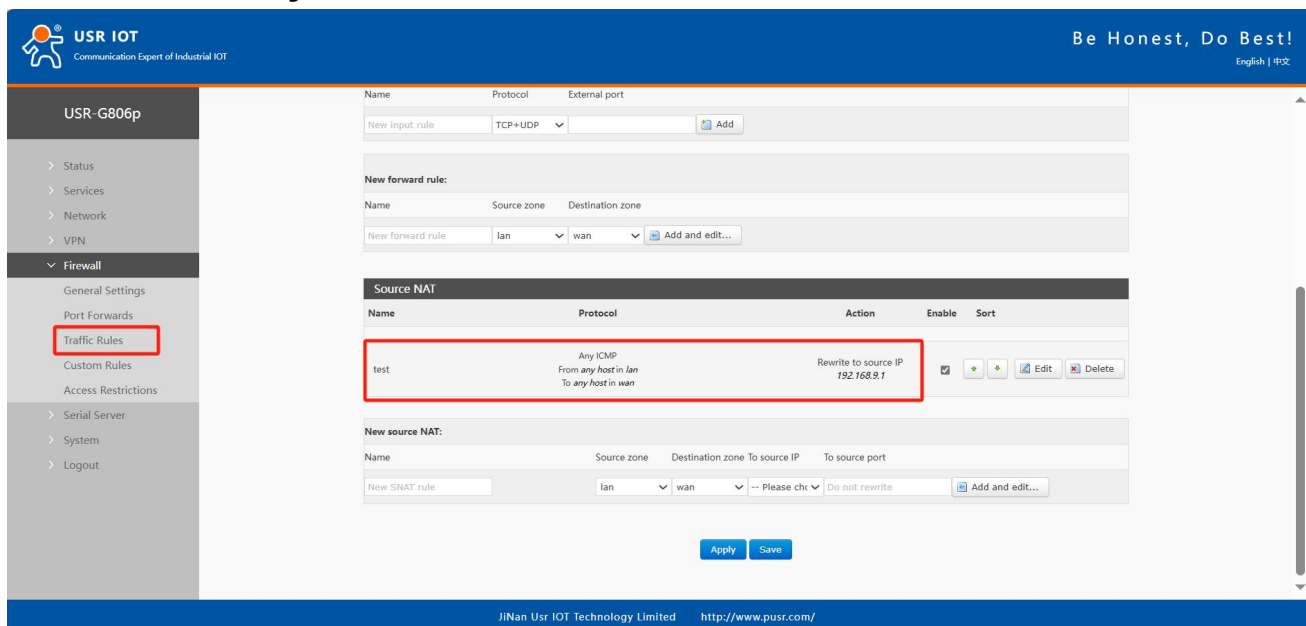
Pic 62 NAT Settings 1

Click Add and Edit



Pic 63 NAT Settings 2

If the source IP, source port and destination IP, destination port are not filled in, all ip and ports are assumed by default. Save after setting.



Pic 64 NAT Settings 3

As shown in the figure, the source IP address of the packet leaving the router is changed to 192.168.9.1. As can be seen in the figure, the source address of the ICMP packet to 192.168.13.4 is 192.168.9.1, instead of 192.168.1.114. Verify that the device under the router (IP: 192.168.1.114) pings the PC (IP: 192.168.13.4) under the same switch as the router, and the data of packet capture on the PC is as follows:

| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|--------------|----------------|----------|--|
| 1 | 0.000000 | 192.168.13.4 | 220.195.22.209 | TCP | 50379 > http [FIN, ACK] Seq=1 Ack=1 Win=64708 Len=0 |
| 2 | 0.689352 | 192.168.9.1 | 192.168.13.4 | ICMP | Echo (ping) request (id=0x1d3c, seq(be/le)=57/14592, ttl=64) |
| 3 | 0.689426 | 192.168.13.4 | 192.168.9.1 | ICMP | Echo (ping) reply (id=0x1d3c, seq(be/le)=57/14592, ttl=128) |
| 6 | 1.689615 | 192.168.9.1 | 192.168.13.4 | ICMP | Echo (ping) request (id=0x1d3c, seq(be/le)=58/14848, ttl=64) |
| 7 | 1.689687 | 192.168.13.4 | 192.168.9.1 | ICMP | Echo (ping) reply (id=0x1d3c, seq(be/le)=58/14848, ttl=128) |
| 8 | 1.823459 | 192.168.13.4 | 192.168.4.63 | SMB2 | Create Request File: |
| 9 | 1.825746 | 192.168.4.63 | 192.168.13.4 | SMB2 | Create Response File: |
| 10 | 1.826091 | 192.168.13.4 | 192.168.4.63 | SMB2 | Create Request File: |

Pic 65 NAT test and verify

5.3.3. DNAT

Exit target address translation.

USR-G806p

Be Honest, Do Best!

English | 中文

Firewall - Port Forwards

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

| Name | Match Rules | Forwarding To | Enable | Sort |
|--------|---|----------------------------------|-------------------------------------|---|
| 123456 | IPv4-TCP, UDP From any host in wan Via any router IP at port 81 | IP 192.168.2.1, port 8000 in lan | <input checked="" type="checkbox"/> | Edit Delete |

New Port Forwarding Rules:

| Name | Protocol | External zone | External port | Internal zone | Internal IP address | Internal port |
|------------------|----------|---------------|---------------|---------------|---------------------|---------------|
| New port forward | TCP+UDP | vpn | | lan | | |

[Apply](#) [Save](#)

JiNan Usr IOT Technology Limited <http://www.pusr.com/>

USR-G806p

Be Honest, Do Best!

English | 中文

Enable ☒ Disable ☐

Name 123456

Protocol TCP+UDP

Source zone

☐ lan: lan

☐ vpn: (empty)

☒ wan: wan_wired: wan_4g: wan_5g:

Source MAC address

☐ Only match incoming traffic from these MACs.

Source IP address

☐ any

☐ Only match incoming traffic from this IP or range.

Source port

☐ any

☐ Only match incoming traffic originating from the given source port or port range on the client host

External IP address

☐ any

☐ Only match incoming traffic directed at the given IP address.

External port

☐ 81

☐ Match incoming traffic directed at the given destination port or port range on this host

Internal zone



☒ lan: lan

☐ vpn: (empty)

☐ wan: wan_wired: wan_4g: wan_5g:

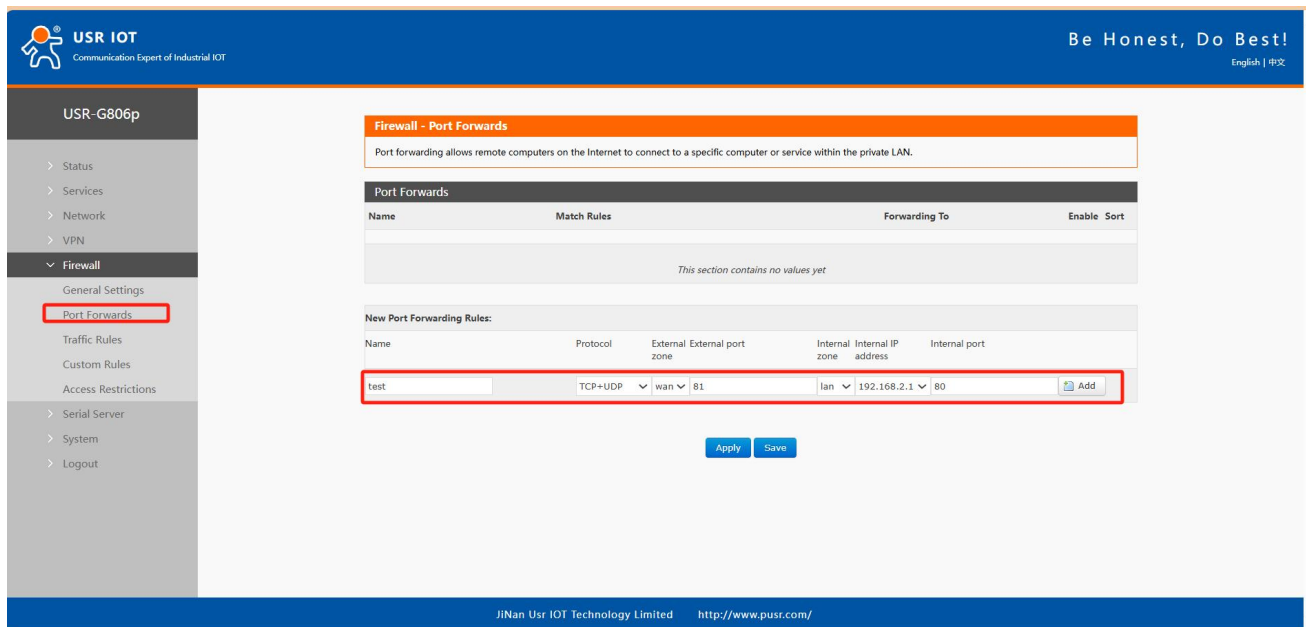
JiNan Usr IOT Technology Limited <http://www.pusr.com/>

DNAT parameter list

| Name | describe | Default Parameters |
|------------------------|--|--------------------|
| Enable | Enable  Disable:  | Enable Disable |
| Name | Customize the name of this rule | Empty |
| Source area | Data entry area selection | WAN |
| Source MAC address | Source MAC address filtering at entry | All |
| Source IP address | Source IP address screening at entry | All |
| Source port | Source port filtering at entry | All |
| External IP address | Target IP address at the time of entry | All |
| External port | Target port at entry | Empty |
| Interior zone | Redirection to the outbound area | LAN |
| An internal IP address | Target address when redirecting out of the station | Empty |
| Internal ports | Redirect the outgoing port to the target port | Empty |
| Enable NAT loopback | Check to enable NAT loopback | Check |

5.3.4. Port forwarding

Port forwarding allows a computer from the Internet to access a computer or service within a private LAN by mapping a specified port on a WAN port address to a host on the Intranet.

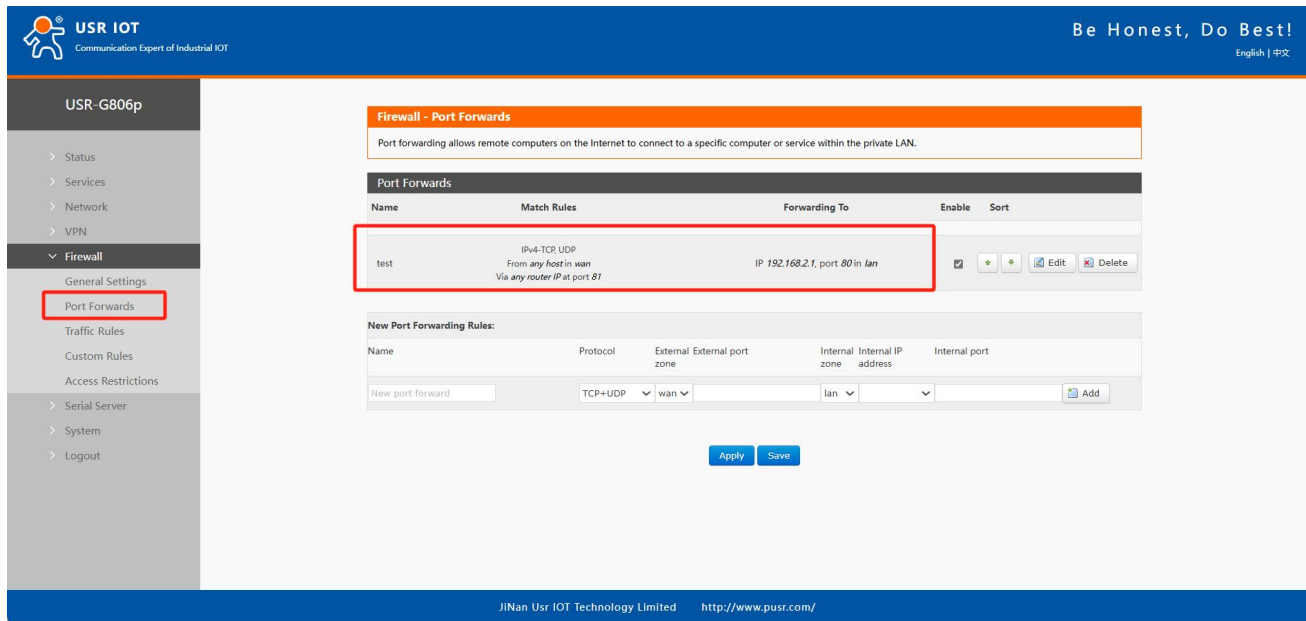


Pic 66 Port Settings page 1

- After setting the forwarding rule, you need to click the add button on the right, and then this rule will be displayed in the rule column;
- Then click the "Apply" button in the lower right corner to make the Settings effective;
- The following Settings: 192.168.2.1:80 is the router's own web server. If we want to access a device in the LAN from the Internet, we need to set up the mapping from the Internet to the LAN, such as setting the

Internet port to 81, the internal IP address to 192.168.2.1, and the internal port to 80;

- When we access port 81 from the WAN port, the access request will be redirected to 192.168.2.1:80.



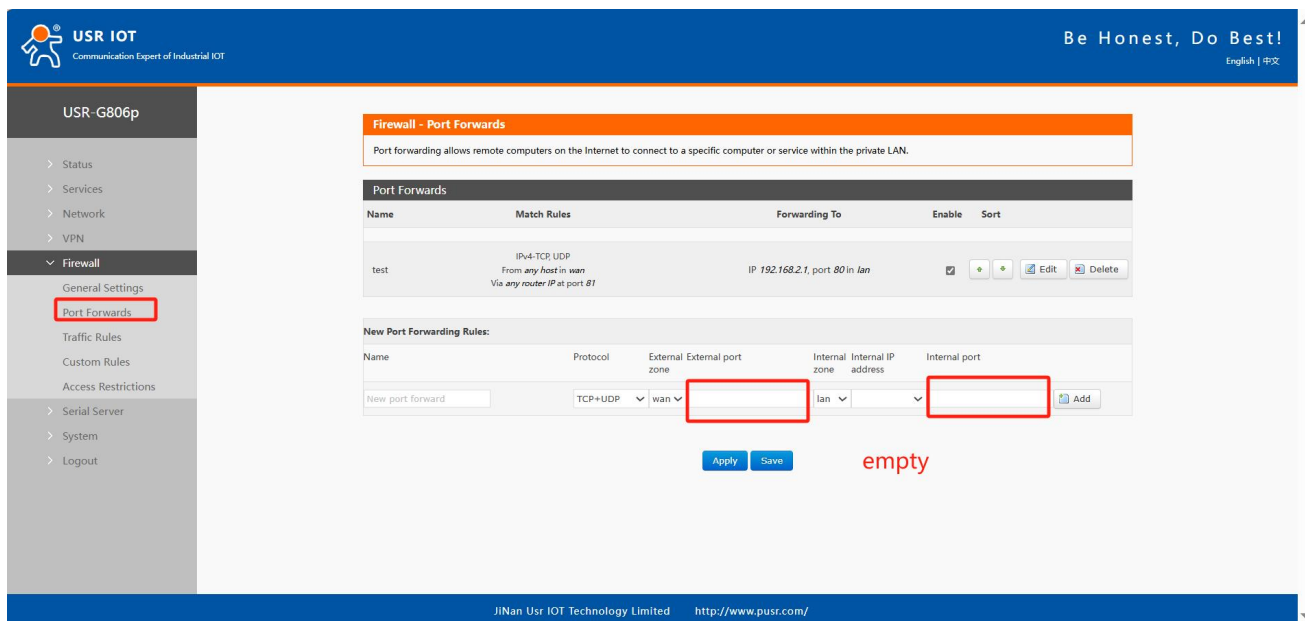
Pic 67 Port Settings page 2

Tab 20 Port forwarding parameter table

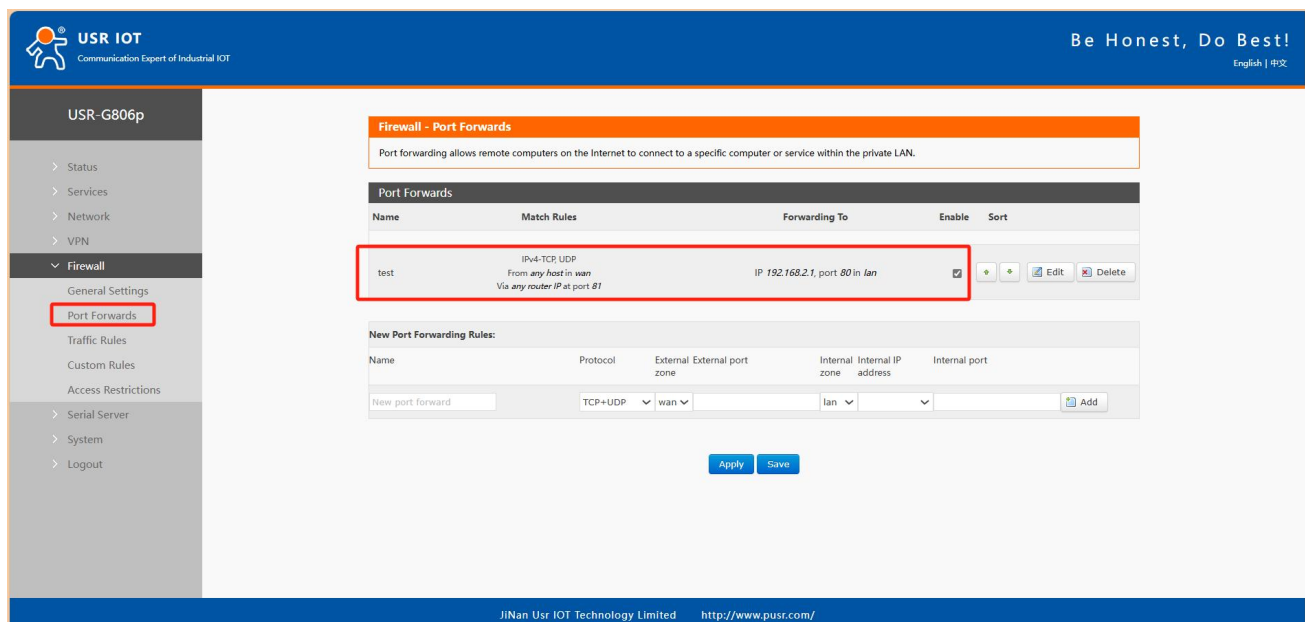
| name | description | Default parameter |
|---------------|--|-------------------|
| name | The name of this port forwarding rule, character type | empty |
| protocol | Protocol type can be set: TCP+UDP/TCP/UDP | TCP+UDP |
| exterior zone | Including wired wan, 4G, VPN | wan |
| External port | You can set a single port or a range of ports, such as 8000-9000 Note: When the external port and internal port are empty, it is a DMZ function | empty |
| interior zone | Router subnet area | lan |
| interior IP | The LAN area IP address of the router | empty |
| Internal port | You can set a single port or a range of ports, such as 8000-9000 Note: When the external port and internal port are empty, it is a DMZ function | empty |

5.3.5. NAT DMZ

Port mapping is to map a specified port of WAN port address to a host in the Intranet. DMZ function is to map all ports of WAN port address to a host. Setting interface and port forwarding are in the same interface. When setting, do not fill in the external port, and click "Add".



Pic 68 DMZ Settings 1



Pic 69 DMZ Settings 2

As shown in the figure, all ports of the WAN port address are mapped to the host 192.168.2.133 on the Intranet.

< pay attention to >

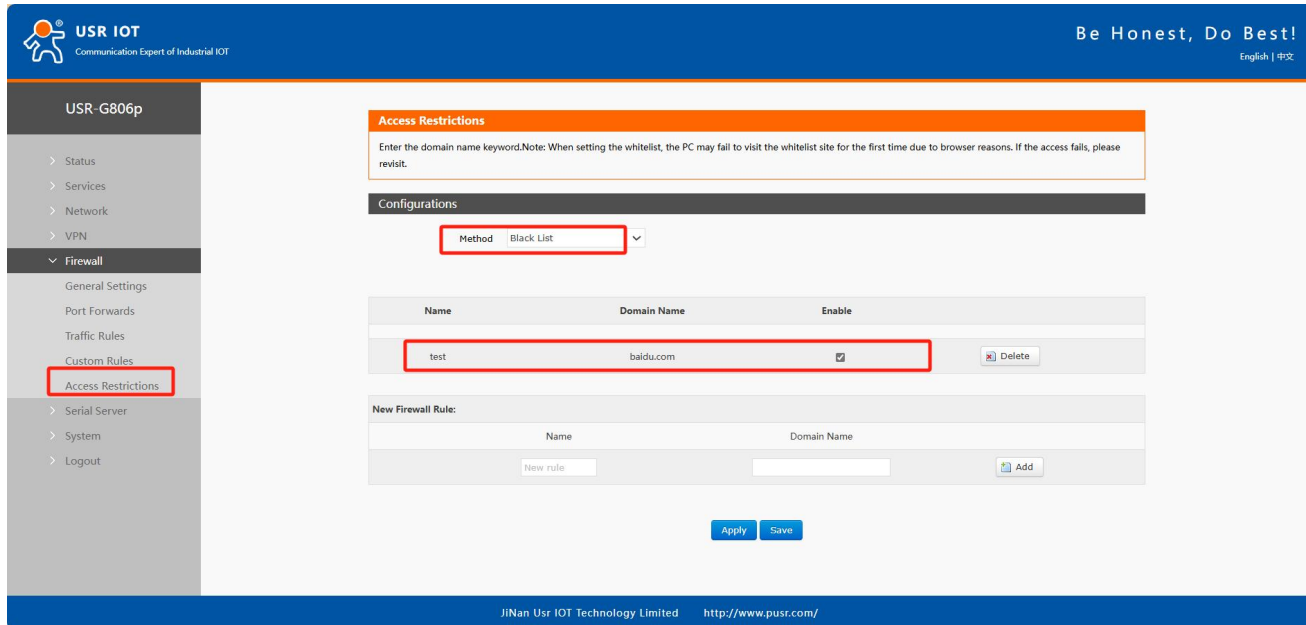
- Port mapping and DMZ functions cannot be used simultaneously.

5.4. Access restrictions

Access restrictions enable the control of access to specific domain names. It supports setting blacklists and whitelists for domain addresses. When a blacklist is selected, devices connected to the router cannot access the domains on the blacklist, while other domain addresses remain accessible. When a whitelist is selected, devices can only access the domain addresses listed in the whitelist, and all other domain addresses are inaccessible. Both blacklists and whitelists can be configured with multiple entries, and this feature is disabled by default.

5.4.1. Domain blacklists

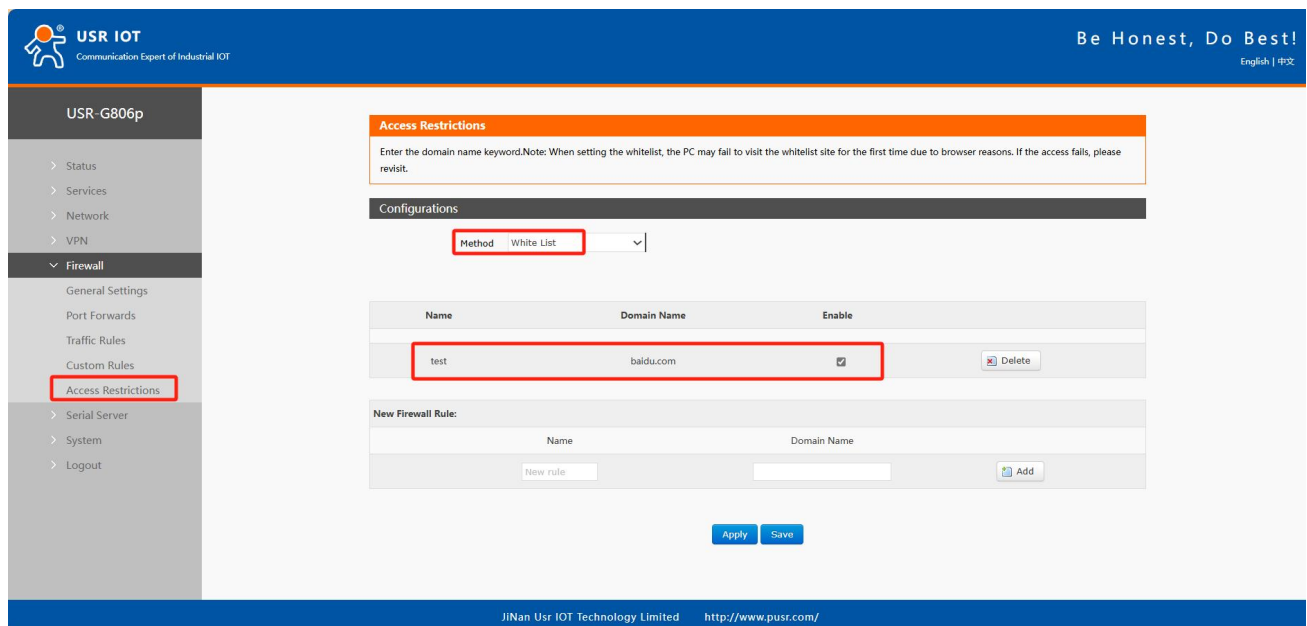
First, in the method options, select the blacklist. Click add to enter the name of the rule and the correct domain name, then click save. The rule will take effect immediately, preventing devices connected to the router from accessing the specified domain. If you choose the blacklist but do not add any rules, the default blacklist is empty, allowing all domains to be accessed. As shown in the figure, except for Baidu, all other domains can be accessed normally.



Pic 70 Domain blacklists

5.4.2. Domain name whitelist

First, in the method options, select the whitelist. Click add to enter the name of the rule and the correct domain name, then click save. The rule takes effect immediately, allowing devices connected to the router to access only the domain name specified in the rule; all other domains are blocked. If you choose the whitelist but do not add any rules, the default whitelist is empty, meaning no domain can be accessed. As shown in the figure, the device can access Baidu.



Pic 71 Domain name whitelist

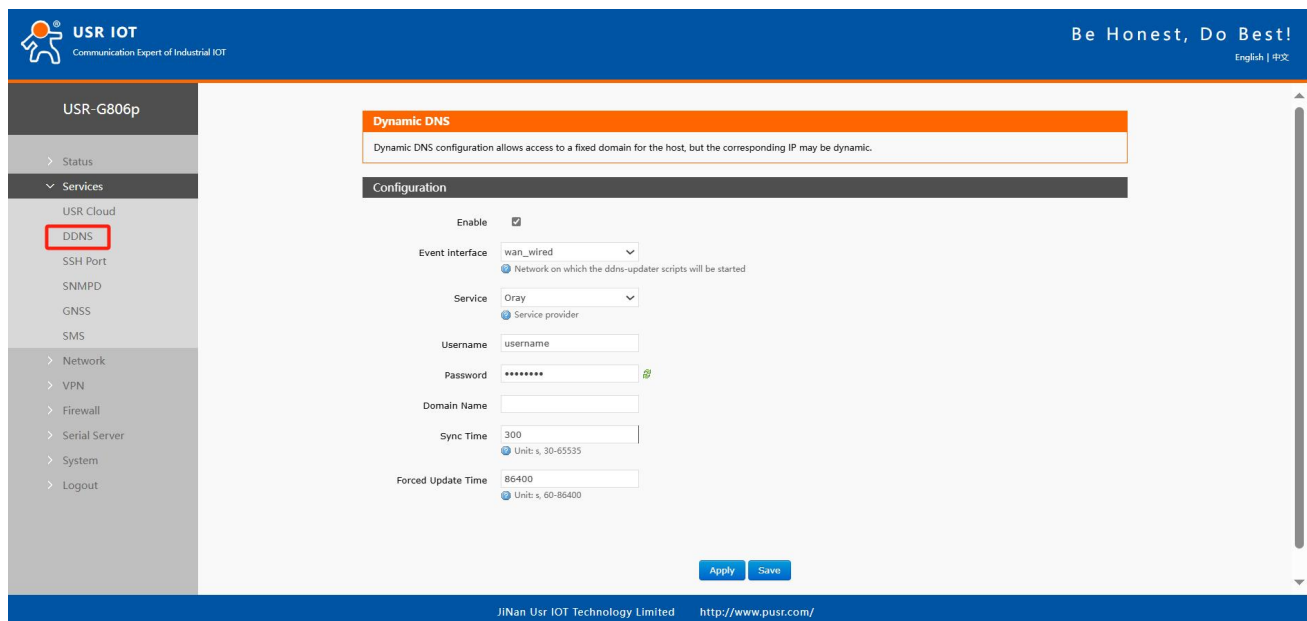
6. Service function

6.1. Dynamic domain name resolution (DDNS)

DDNS (Dynamic Domain Name Server) is a service that maps a user's dynamic IP address to a fixed domain name resolution server. Each time a user connects to the network, the client program sends the host's dynamic IP address to the server program on the service provider's host via information transmission. The server program provides DNS services and performs dynamic domain name resolution.

6.1.1. Supported services

The use of dynamic domain names is divided into two cases. The first case is that the router itself supports this service (view the "Service" drop-down box and select the corresponding DDNS service provider, here using Peanut Shell). The setting method is as follows:



Pic 72 DDNS Settings page

Parameter filling requirements are as follows:

Tab 21 DDNS parameter list

| function | content | Windows default |
|---------------------------|--|----------------------------|
| open | Check to enable DDNS function | Not selected |
| Valid interface | Select WAN port according to requirements | wan_wired |
| ISP internet | Please fill in the service address of DDNS | dyndns.org |
| DDNS facilitator | Please fill in the DDNS service address | dyndns.org |
| DDNS updates the URL path | Set the IP source URL address | http://checkip.dyndns.com/ |
| user name | Peanut shell account name | username |
| password | The peanut shell code | password |
| realm name | The domain name for which the DDNS application is made | empty |
| lock-in time (s) | The time interval for detecting IP address changes | 300 |
| Mandatory update time | Enforce a mandatory update interval | 86400 |

6.1.2. DDNS come into force

To confirm that the DDNS Settings are in effect, first look at your network's public IP address.

Then, we ping the domain name fe26203015.zicp.vip on the PC, which can be pinged, indicating that DDNS has taken effect.

```

C:\Users\Administrator>
C:\Users\Administrator>ping fe26203015.zicp.vip

正在 Ping fe26203015.zicp.vip [60.28.138] 具有 32 字节的数据:
来自 60.28.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138 的回复: 字节=32 时间<1ms TTL=127

60.28.138 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

```

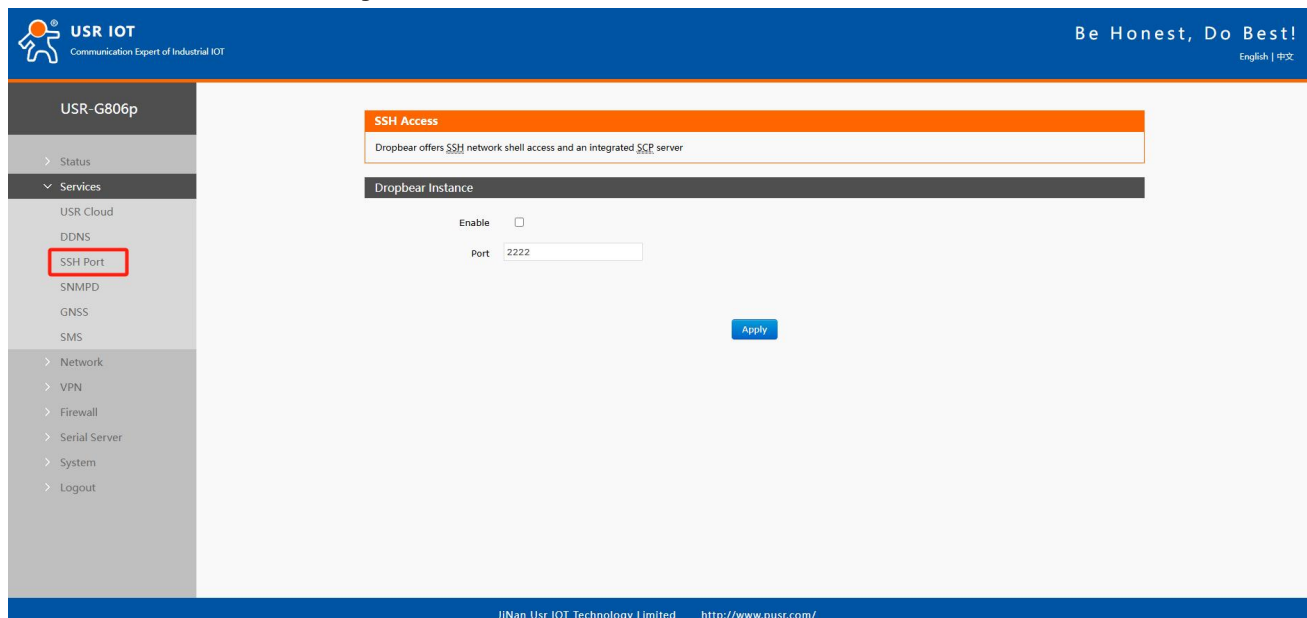
Pic 73 DDNS test Figure 3

6.1.3. functional characteristics

- Please fill in the parameters, service/URL, domain name, user name and password, interface and other parameters strictly according to the form description to ensure correctness;
- Even as a router under the subnet, this function can also make dynamic domain name effective;
- DDNS + port mapping can realize remote access to the internal network of this router;
- If the network where the router is located does not have an independent public IP address, this function cannot be used.

6.2. SSH Port

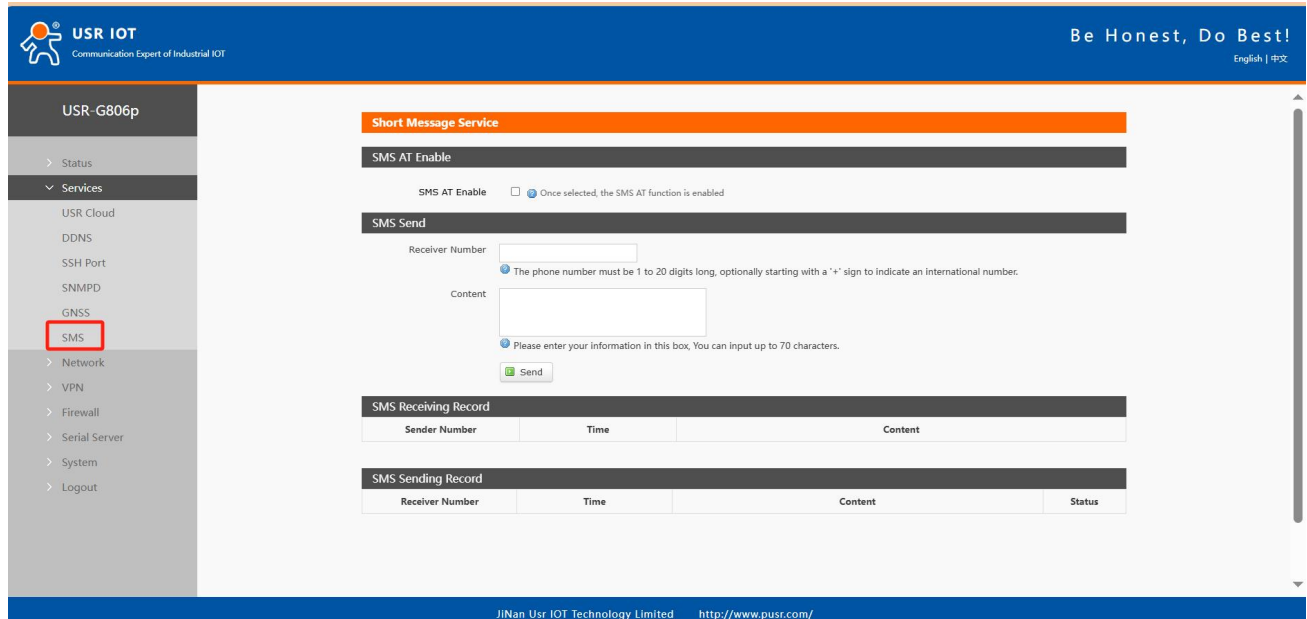
Enable or disable SSH to manage the router.



Pic 74 SSH

6.3. SMS

To enable the SMS function, you can view the router parameters by sending SMS AT. You need a SIM card that can send SMS to the router.



Pic 75 SMS

Tab 22 configuration parameter

| name | description | Default parameter |
|--------------------------|---|-------------------|
| SMS AT enabled | Enable: Enable SMS AT Disable: Turn off SMS AT | forbidden |
| SMS authorization method | All: Accept SMS AT from all mobile phone numbers and respond Specify: Accept the SMS AT of the specified mobile phone number and respond | whole |
| Authorized phone number | Set the SMS AT authorization phone number, up to 5 numbers | empty |
| Destination number | The router sends a text message to the specified number | empty |
| content | The content of a text message sent to a specified number | empty |

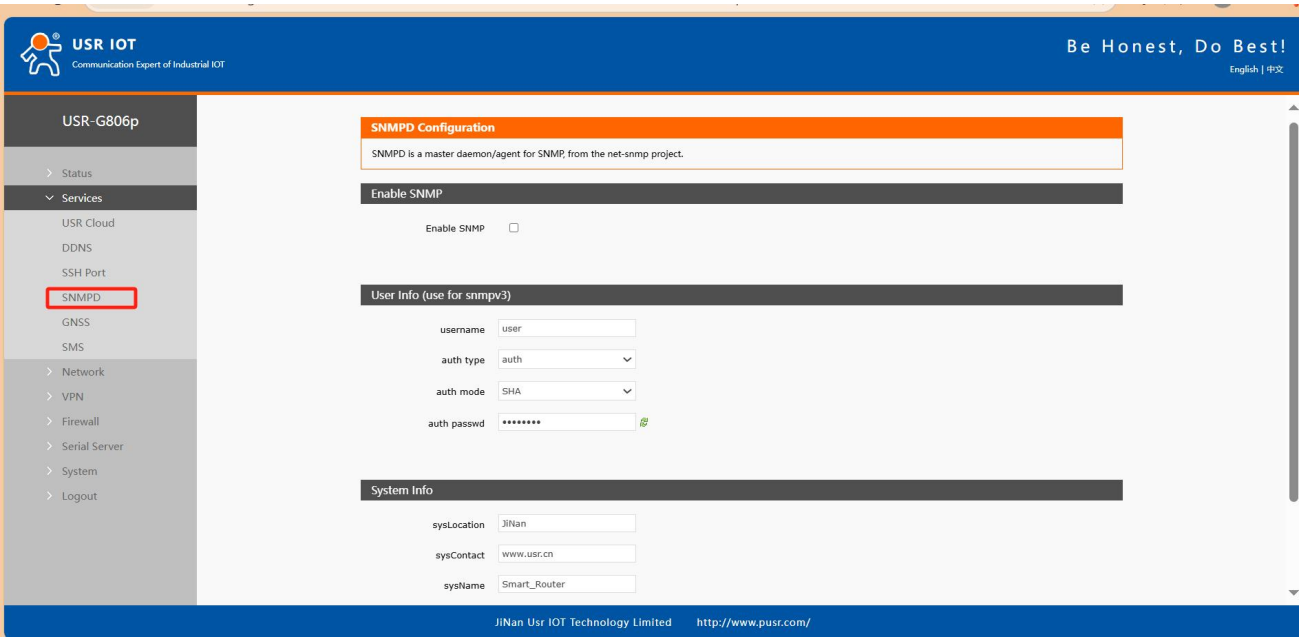
The following screenshot shows the AT sent to the end to obtain router information. For details of SMS AT supported by the router, see the AT instruction table.



Pic 76 SMS AT

6.4. SNMPD

The G806p has SNMP (Simple Network Management Protocol) service. You can remotely view device information, modify device parameters, monitor device status and other functions of your device through SNMP protocol without going to the site for monitoring and configuring the device one by one. The SNMP version supported by this device is V2C and V3.



Pic 77 SNMP service Settings interface

Tab 23 SNMP parameter list

| function | | content | Windows default |
|---------------|--------|---------------------------------|-----------------|
| SNMP | switch | Check to enable SNMP services | Not selected |
| configuration | | | |
| user name | | The name assigned to SNMP users | user |

| | | |
|-------------------------|---|--------------|
| Type of certification | Certification or certification and encryption | attestation |
| Authentication mode | The authentication protocol used by the user and host to receive the trap. MD5 or SHA | SHA |
| Authentication password | User authorization password | authpass |
| Encryption type | Encryption protocol type, DES or AES | DES |
| Encrypt the password | The encryption password used as the private key | privpass |
| alliance | Location of the equipment | JiNan |
| System contact | Contact person for this equipment | www.usr.cn |
| systematic name | The system name of this device | Smart_Router |

Supports obtaining basic router information through SNMP. OID is as follows.

Tab 24 SNMP OID list

| OID | description | Request method |
|------------------------------|---|----------------|
| .1.3.6.1.4.1.2021.8.2.101.1 | Get CPU information | GET |
| .1.3.6.1.4.1.2021.8.2.101.2 | Obtain the device IMEI | GET |
| .1.3.6.1.4.1.2021.8.2.101.3 | Get the firmware version number | GET |
| .1.3.6.1.4.1.2021.8.2.101.4 | Get the registration status of the cellular network | GET |
| .1.3.6.1.4.1.2021.8.2.101.5 | Obtain the SIM card ICCID | GET |
| .1.3.6.1.4.1.2021.8.2.101.6 | Get the registered network type | GET |
| .1.3.6.1.4.1.2021.8.2.101.7 | gain imsi | GET |
| .1.3.6.1.4.1.2021.8.2.101.8 | Get carrier information | GET |
| .1.3.6.1.4.1.2021.8.2.101.9 | Obtain cellular network IP address (IPv4) | GET |
| .1.3.6.1.4.1.2021.8.2.101.10 | Get the signal strength | GET |
| .1.3.6.1.4.1.2021.8.2.101.11 | gain tac | GET |
| .1.3.6.1.4.1.2021.8.2.101.12 | gain cid | GET |

6.5. GNSS

Supports GPS positioning data reporting to private platforms.

7. Serial port server function

G806p has RS232/RS485, supports TCP, UDP, MODBUS, MQTT, HTTPD and other network protocols, and supports heartbeat packets, registration packets and AT features.

| name | functional description | Windows default |
|----------------|--|-----------------|
| Baud rate | Set the baud rate of RS232 or RS485. You can set: 1200/2400/4800/9600/19200/38400/57600/115200/230400 Note: Only RS485 supports 230400 | 115200 |
| data bit | Set the data bit of RS232 or RS485. You can set it to 7/8 | 8 |
| stop bit | The stop bit of RS232 or RS485 can be set to 1/2 | 1 |
| check bit | The parity bit of RS232 or RS485 can be set to NONE/ODD/EVEN | NONE |
| Packaging time | Set the data packing time for RS232 or RS485 Unit: ms (range: 10-60000ms) | 50 |
| Pack length | Set the data packing length of RS232 or RS485 Unit: bytes (range: 5-1500 bytes) | 1000 |

7.1. Serial port Settings

In this interface, you can set the baud rate, data bits and other parameters of the serial port.

Serial Port Settings

Serial port basic Settings, the package time can be set in the range of 0-1000 ms (0 indicates automatic packaging), package length can be set in the range of 5-1460 bytes.

| Name | Baud Rate | Data Bits | Stop Bits | Parity | Packaging Interval | Packaging Length |
|----------|-----------|-----------|-----------|--------|--------------------|------------------|
| COM1-485 | 115200 | 8 | 1 | NONE | 0 | 1000 |
| COM2-232 | 115200 | 8 | 1 | NONE | 0 | 1000 |

485 collision prevention Configuration

485 collision prevention: OFF

Apply

Pic 78 Serial port setting interface

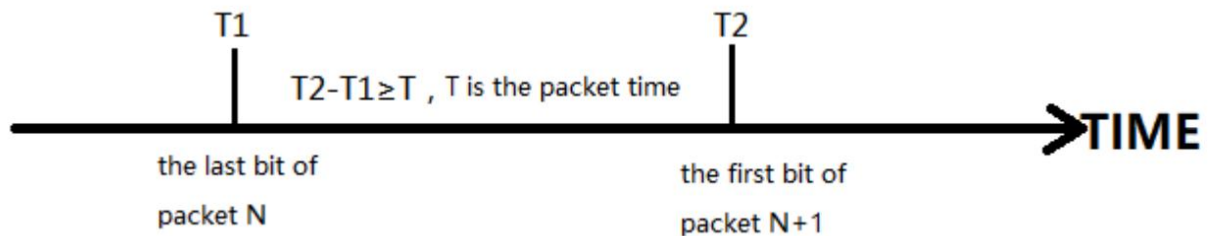
Tab 25 Serial port setting parameter table

| name | functional description | Windows default |
|-----------|--|-----------------|
| Baud rate | Set the baud rate of RS232 or RS485. You can set: 1200/2400/4800/9600/19200/38400/57600/115200/230400 | 115200 |
| data bit | Set the data bit of RS232 or RS485 to 7/8 | 8 |

| | | |
|----------------|--|------|
| stop bit | The stop bit of RS232 or RS485 can be set to 1/2 | 1 |
| check bit | The parity bit of RS232 or RS485 can be set to NONE/ODD/EVEN | NONE |
| Packaging time | Set the data packing time for RS232 or RS485 Unit: ms (range: 10-60000ms) | 50 |
| Pack length | Set the data packing length of RS232 or RS485 Unit: bytes (range: 5-1500 bytes) | 1000 |

7.1.1. Time-triggered mode

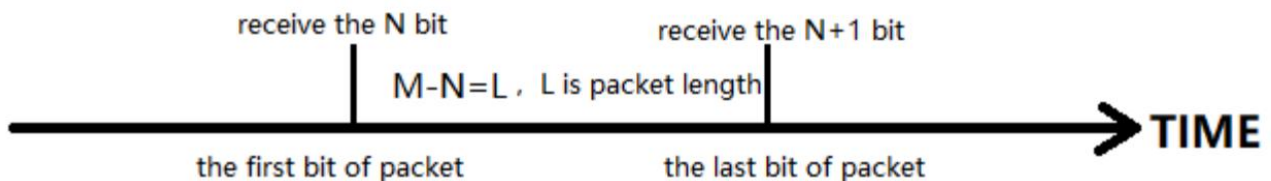
When the G806p receives data from the UART, it continuously checks the interval between adjacent bytes. If the interval is greater than or equal to a specific 'time threshold,' the frame is considered complete. Otherwise, it continues to receive data until the total length reaches or exceeds the packet size (default is 1000 bytes). The frame is then sent to the network as a single packet. The 'time threshold' is the interval between packets, which can be set from 10ms to 60000ms. The default setting is 50ms.



Pic 79 Time-triggered mode

7.1.2. Length-triggered mode

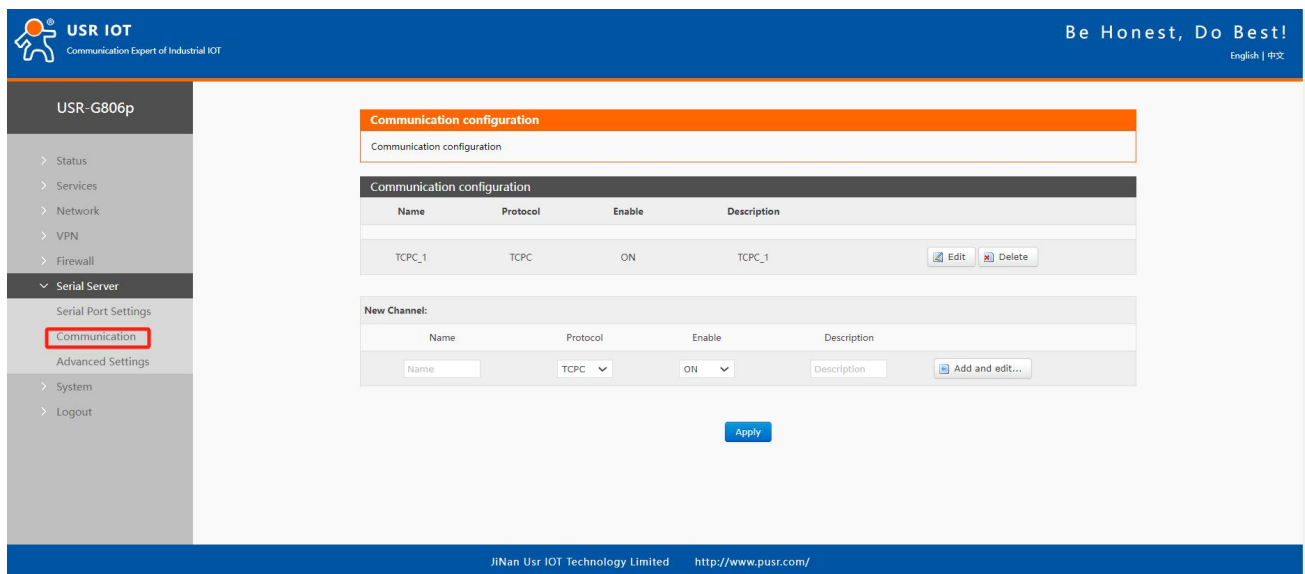
When the 806p receives data from the UART, it continuously checks the number of bytes received. If the number of received bytes reaches a certain 'length threshold,' the frame is considered to have ended. The frame data is then sent as a TCP or UDP packet to the network. The 'length threshold' refers to the packet size, which can be set between 5 and 1500 bytes. The default setting is 1000 bytes.



Pic 80 Length-triggered mode

7.2. Communication configuration

In this interface, you can set the network configuration of DTU function.



Pic 81 Communication configuration

Tab 26 Communication configuration parameter table

| name | functional description | Windows default |
|-------------|--|-----------------|
| name | Set the name of this link | empty |
| protocol | You can select the following network protocol: TCPC/TCPS/UDPC/UDPS/HTTPD/MQTT/AWS/ALI | TCPC |
| start using | Whether this link is enabled, ON (enabled)/OFF (disabled) | start using |
| description | Set the remarks for this link | empty |

explain :

- Follow up with different protocol choices, and the "add and edit" interface will vary accordingly;
- Up to six links can be set.

7.2.1. MQTT pattern

The device supports the MQTT Client function, allowing users to easily connect to their own private MQTT server through simple configuration. Both data publishing and subscription support multi-topic configurations, enabling users to send serial port data to a specific topic or direct the server's pushed data to a bound serial port, thus achieving seamless data transmission between the serial port and the server.

7.2.1.1. MQTT basic configuration

Pic 82 MQTT configuration interface

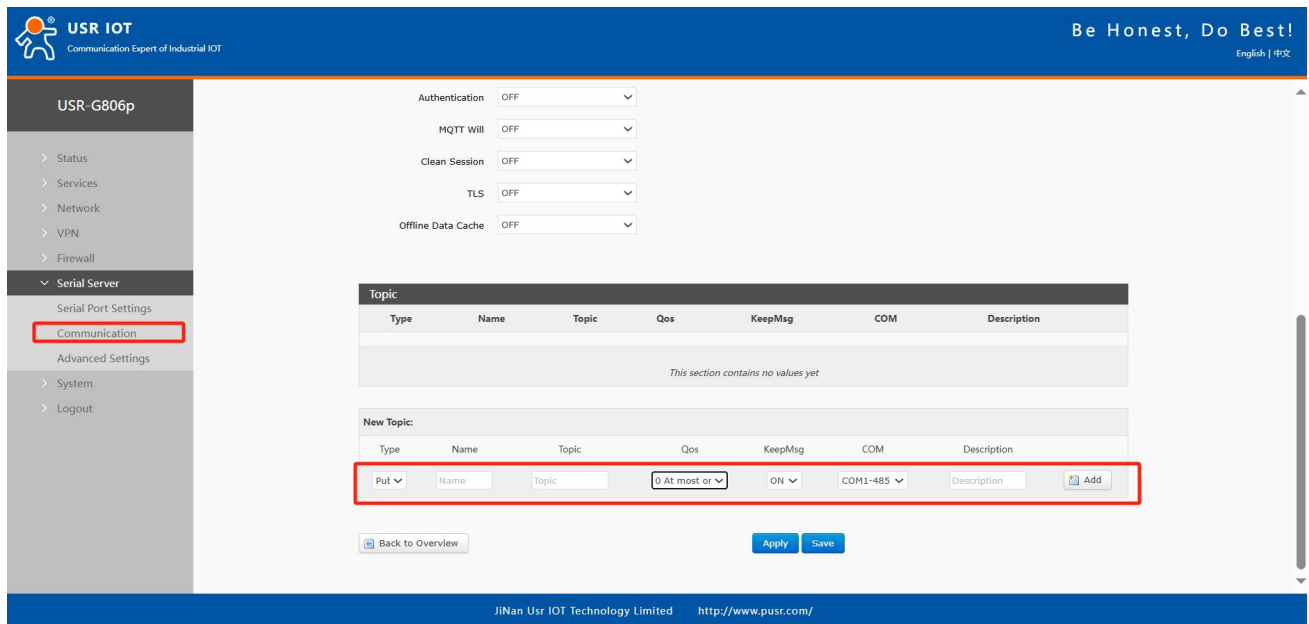
Tab 27 MQTT parameter list

| name | functional description | Windows default |
|-------------------------------|--|------------------|
| start using | Whether this link is enabled, ON (enabled) / OFF (disabled) | ON |
| name | The name of the link | MQTT_X |
| description | This link notes information | MQTT_X |
| MQTT edition | You can choose: MQTTV3.1.1/V3.1 version | V3.1.1 |
| Server address | MQTT server address: IP or domain name | cloudmqtt.usr.cn |
| Server port | MQTT server port | 1883 |
| client ID | MQTT client identifier | 123456 |
| The heartbeat packet time | MQTT protocol heartbeat time, unit: seconds | 30 |
| Redundancy detection interval | The interval between the next reconnection after MQTT disconnection. Unit: seconds | 5 |
| attestation | If the server needs user name and password authentication, it needs to be enabled ON: Enable MQTT user name and password authentication OFF: Disable MQTT user name and password authentication | OFF |
| words of the deceased | MQTT connection flag, when the network is abnormal and disconnected, the server will publish this will message to other clients who subscribe to this will topic. ON: Enable subscription to the will topic OFF: Turn off the subscription to the will topic | OFF |
| theme | Testament topic | empty |
| The contents of | Set the contents of your will | empty |

| | | |
|---------------------------|--|-------------------------------|
| the will | | |
| QOS | QOS Settings can be set for: 0 at most 1 At least once 2. Get it right the first time | 0 |
| Keep the message | Whether to enable the legacy message retention function ON: open OFF: close | OFF |
| Clean up the conversation | MQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is on | OFF |
| TLS | The version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directions | OFF |
| TLS authentication method | No certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity, which requires the pre-set server root certificate, client certificate and client private key | Do not verify the certificate |
| Offline data cache | Data overflow processing mode selection, cache mode, cache length setting, etc | OFF |

7.2.1.2. Theme subscription/publish

The topic addition feature is primarily used to add topics for publication or subscription. Configuration parameters include the topic name, TOPIC, QOS, and whether to retain messages. The serial port association function links a topic to a specific serial port. When publishing, the original data from the serial port serves as the Payload of the topic. When receiving subscription messages, the Payload of the subscribed topic is sent to the serial port as the original data.



Pic 83 MQTT topic configuration interface

Tab 28 MQTT topic parameter table

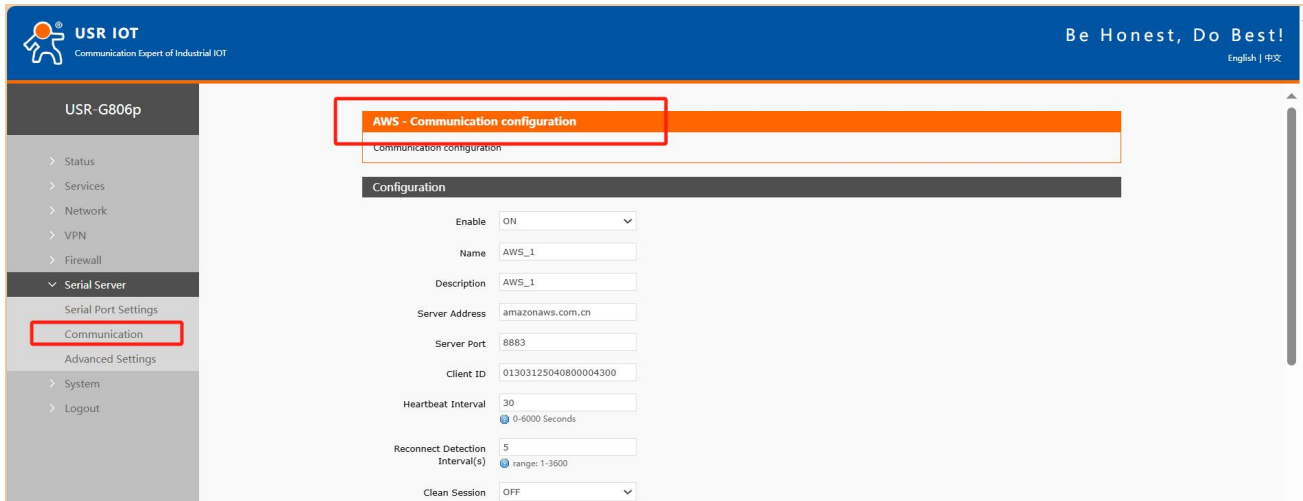
| name | functional description | Windows default |
|------------------|---|-----------------|
| type | Theme type: Publish/subscribe is optional | publish |
| name | The name of the topic | empty |
| theme | Theme: Theme content | empty |
| Qos | The quality of the topic message can be set: 0 At most once 1 At least once 2. Get it right the first time | 0 |
| Keep the message | Set whether to retain messages, ON (retain) / OFF (do not retain) | ON |
| channel | COM1-485: Use the 485 channel for data communication COM2-232: Use channel 232 for data communication COM1+COM2: Use RS232 or RS485 channels to transmit data | COM1-485 |
| description | Set the remarks information for this topic rule | empty |

explain :

- You can set up a maximum of 16 theme rules.

7.2.2. Connect to the Amazon platform

In this mode, the user terminal can send request data to the AWS platform via this device. Data publishing and subscription to the AWS platform can be configured for multiple topics. Users can configure the serial port data to be sent to a specific topic or direct the server-pushed data to the bound serial port, enabling seamless data transmission between the serial port and the server.



Pic 84 AWS configuration interface

Tab 29 AWS parameter list

| name | functional description | Windows default |
|-------------------------------|---|------------------|
| start using | Whether the link is enabled, ON (enabled) / OFF (disabled) | ON |
| name | The name of the AWS platform link | AWS_2 |
| description | AWS platform link remarks | AWS_2 |
| Server address | AWS platform MQTT service server connection address: IP or domain name | amazonaws.com.cn |
| Server port | AWS platform MQTT server port | 1883 |
| client ID | The AWS platform MQTT client identifier | 123456 |
| The heartbeat packet time | MQTT protocol heartbeat time, unit: seconds | 30 |
| Redundancy detection interval | The interval between the next reconnection after MQTT disconnection. Unit: seconds | 5 |
| Clean up the conversation | MQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is on | OFF |
| Server root certificate | Select the corresponding file | not have |
| Device signature certificate | Select the corresponding file | not have |
| Device private key | Select the corresponding file | not have |
| Offline data cache | Data overflow processing mode selection, cache mode, cache length setting, etc | OFF |

7.2.2.1. Theme subscription/publish

The topic add function is mainly used to add the topic for publishing or subscribing. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages. The serial port association is used to associate a topic with a serial port. Up to 16 topic rules can be set.

7.2.3. Connect to Ali Cloud platform

The Alibaba Cloud IoT Platform is a highly popular public cloud platform. It supports the MQTT protocol for device access, offering both industrial and enterprise instances. The platform supports SSL functions, enabling unencrypted, one-way, and two-way authentication connections to Alibaba Cloud. In this mode, data can be published and subscribed to terminal devices through the Alibaba Cloud platform, supporting multi-topic configuration. Users can configure serial port data to be sent to specific topics or direct server-pushed data to the bound serial ports, facilitating seamless data transmission between the serial port and the server.

Pic 85 ALI configuration interface

Tab 30 ALI parameter list

| name | functional description | Windows default |
|---------------|---|-----------------|
| start using | Whether the link is enabled, ON (enabled) / OFF (disabled) | ON |
| name | The name of the ALI platform link | ALI_2 |
| description | ALI platform link remarks | ALI_2 |
| Instance type | Supports Ali Cloud public instances and enterprise instances | Public instance |
| ProductKey | Device attributes, the triplet ProductKey is added to the device in Ali Cloud | not have |
| deviceName | Device name, the DeviceName in the triplet added to Aliyun devices | not have |
| deviceSecret | Device key, the triplet DeviceSecre added to the device in Ali Cloud | not have |

| | | |
|-------------------------------|---|-------------------------------|
| client ID | Supports custom customer ID for MQTT client concatenation | not have |
| region | The regional code of Ali Cloud, such as East China 2 (Shanghai), is filled in: cn-shanghai | East China 2-Shanghai |
| Server port | ALI platform MQTT server port | 1883 |
| The heartbeat packet time | MQTT protocol heartbeat time, unit: seconds | 300 |
| Redundancy detection interval | The interval between the next reconnection after MQTT is disconnected, unit: seconds | 5 |
| Clean up the conversation | MQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is on | OFF |
| TLS | The version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directions | OFF |
| TLS authentication method | No certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private key | Do not verify the certificate |
| Offline data cache | Data overflow processing mode selection, cache mode, cache length setting, etc | OFF |

7.2.3.1. Theme subscription/publish

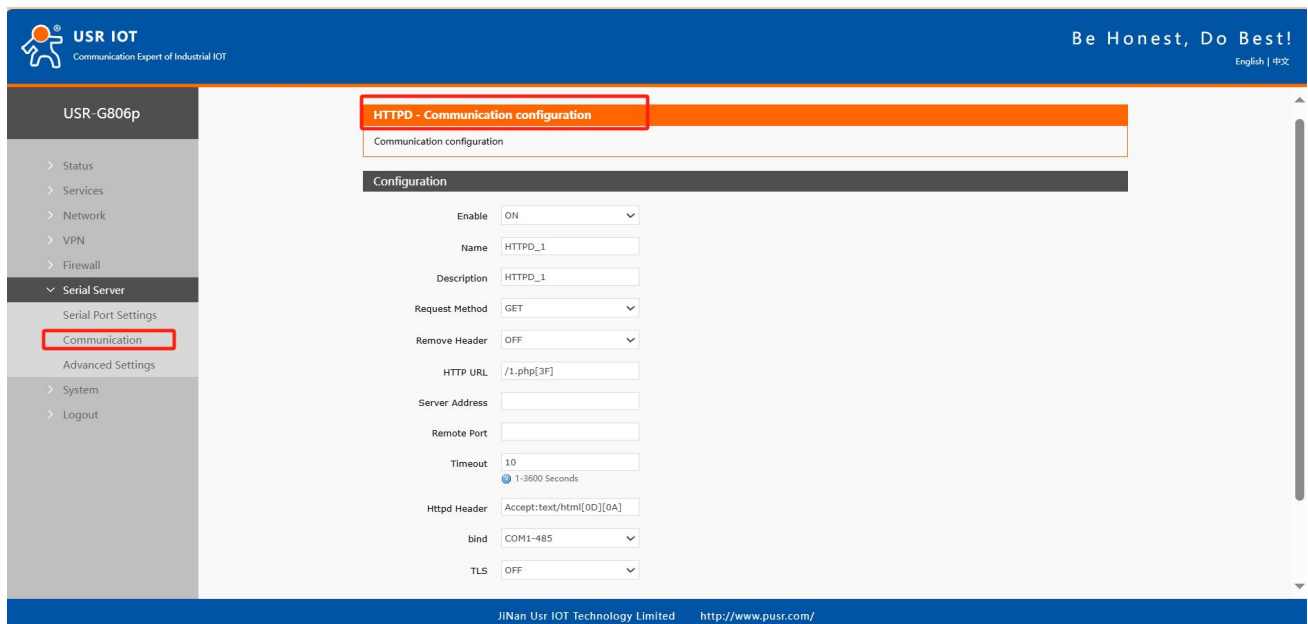
The topic add function is mainly used to add the topic for publishing or subscribing. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages. The serial port association is used to associate the topic with a certain serial port. A maximum of 16 topic rules can be set.

7.2.4. HTTPD mode (HTTP Client mode)

In this mode, the user's terminal device can send request data to the specified HTTP server through this device, and then the device receives the data from the HTTP server, parses the data and sends the result to the serial port device.

Users do not need to pay attention to the data conversion process between serial port data and network packets. They can realize the data request from serial port device to HTTP server through simple parameter setting.

The device filters the received data by default and only outputs the user data to the serial port. The customer can use the AT command to select whether to filter the HTTPD data.



Pic 86 HTTPD configuration interface

Tab 31 HTTPD parameter list

| name | functional description | Windows default |
|----------------------------|---|--------------------------|
| start using | Whether this link channel is enabled: ON (enabled) / OFF (disabled) | ON |
| name | The name of the link | HTTPD_X |
| description | Add remarks to this link | HTTPD_X |
| Request method | The way to request data from an HTTP server GET/POST | GET |
| Clean the filter head | Set whether to filter HTTP header ON (filter) / OFF (no filter) | ON |
| HTTP URL | Add the URL you want to access | /1.php[3F] |
| Server address | HTTP server address, which can be filled with IP or domain name | empty |
| Remote port | HTTP server port number | empty |
| overtime | If the server does not actively disconnect the connection within the timeout time, this end needs to wait for the disconnection time, unit: seconds | 10 |
| Request header information | HTTP header information | Accept:text/html[0D][0A] |
| Channel binding | COM1-485: Use the 485 channel for data communication COM2-232: Use channel 232 for data communication COM1+COM2: Use RS232 or RS485 channels to transmit data | COM1-485 |
| TLS encryption | Supports TLS1.0\TLS1.2\OFF | OFF |

7.2.5. Registration packet/handshake packet function

7.2.5.1. Registration package description

Registration packet: This is used to enable the server to identify the data source device or as a password for obtaining server function authorization. The registration packet can be sent when the device connects to the server, or it can be appended to the beginning of each data packet as part of the data packet. The data in the registration packet can be either a MAC address or custom registration data.

explain :

- If MAC is selected, the WAN port MAC is used as the content of the registration packet;
- This function is available only when the link is set to tcpc or udpc mode.

7.2.5.2. Network heartbeat packet description

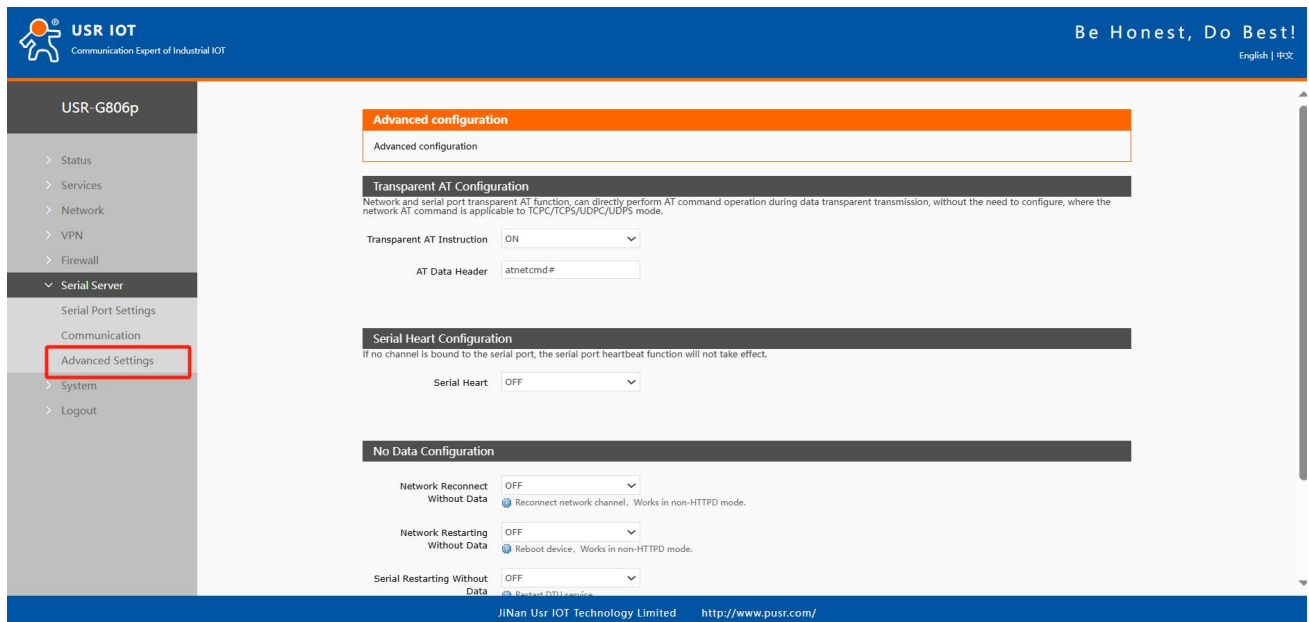
Network heartbeat packet: sent to the network end, the main purpose is to let the server know that the terminal W6305 is online, so as to maintain a long connection with the server.

explain :

- This function is available only when the link is set to tcpc or udpc mode.

7.3. advanced setup

You can configure network AT, serial port heartbeat packets, and no data action conditions.



Pic 87 Advanced configuration interface

Tab 32 Advanced configuration interface parameter table

| name | functional description | Windows default |
|---------------------|---------------------------------|-----------------|
| Network AT command | ON (enable)/OFF (disable) | ON |
| Network AT password | The password for the network AT | atnetcmd# |

| | | |
|---|---|-----------|
| word | | |
| Serial port heartbeat | ON: Enable the function of sending heartbeat packets to serial port OFF: Disable the function of sending heartbeat packets to serial port | OFF |
| Pacemaker types | HEX: 16-bit type ASCII: Character type The explanation of the heartbeat packet is shown in Chapter 8.2.7.2 | HEX |
| Pacemaker data | Heartbeat packet data content | empty |
| The heartbeat packet time | The time interval at which the heartbeat packet is sent, in seconds | 60 |
| Serial port binding | COM1-485: Use the 485 channel for data communication COM2-232: Use channel 232 for data communication COM1+COM2: Use RS232 or RS485 channels to transmit data | COM1+COM2 |
| The network channel does not enable data reconnection | If no data is received from the network end within the setting time, the channel triggers reconnection It is applicable to non-HTTP protocols. See the following description for details | OFF |
| Redundancy detection interval | Set the time interval, unit (seconds) | 3600 |
| The network channel is not enabled for data restart | If no data is received from the network end within the setting time, all channels will trigger the device to restart It is applicable to non-HTTP protocols. See the following description for details | OFF |
| Restart the detection interval | Set the time interval, unit (seconds) | 36000 |
| Serial port data restart enabled | The configuration serial port channel does not receive the serial port data, and triggers the DTU to restart If two serial ports are configured, the DTU will be restarted if no serial port data is received within the time of one channel | OFF |
| Enable serial port | COM1-485/COM2-232/COM1+COM2 | COM1-485 |

explain :

- Serial heartbeat packet: This function is only available if there is a link channel (at least one communication configuration);
- No data reconnection of the network channel: TCP/UDP/MQTT. If no time is received from the network end

within the set time, the link will be reconnected;

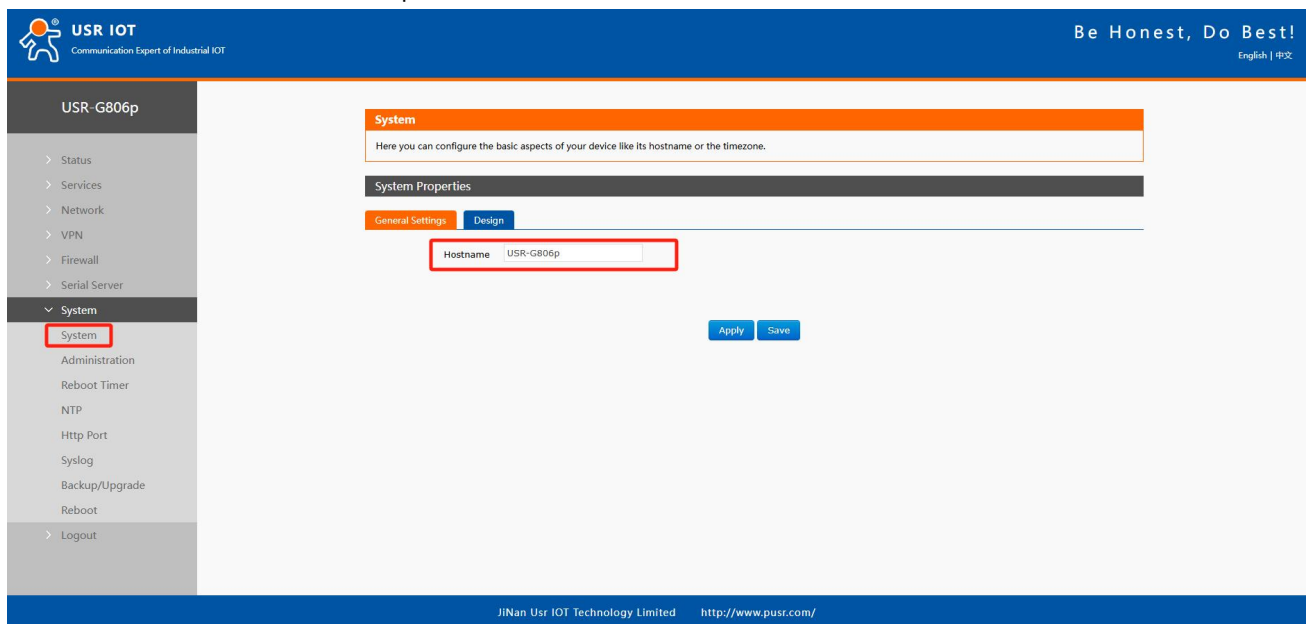
- No data reconnection of network channel: TCPs, if the client does not receive data within the set time, it will kick out the corresponding client;
- No data reconnection of the network channel: UDPS, if the client data is not received at the set time, the serial port data will not be sent to UDPC;
- Network channel no data restart: all link channels will restart when the set time is reached and no network data is received;
- Network channel restart without data: if the TCPC connection success data is received within the set time, the count is reset;
- Serial port channel restart without data: if the serial port data is not received at the set time, DTU restarts;

Restart of serial port channel without data: If COM1+COM2 dual channels are set, the DTU will restart when one of the channels does not receive serial port data after the set time.

8. system function

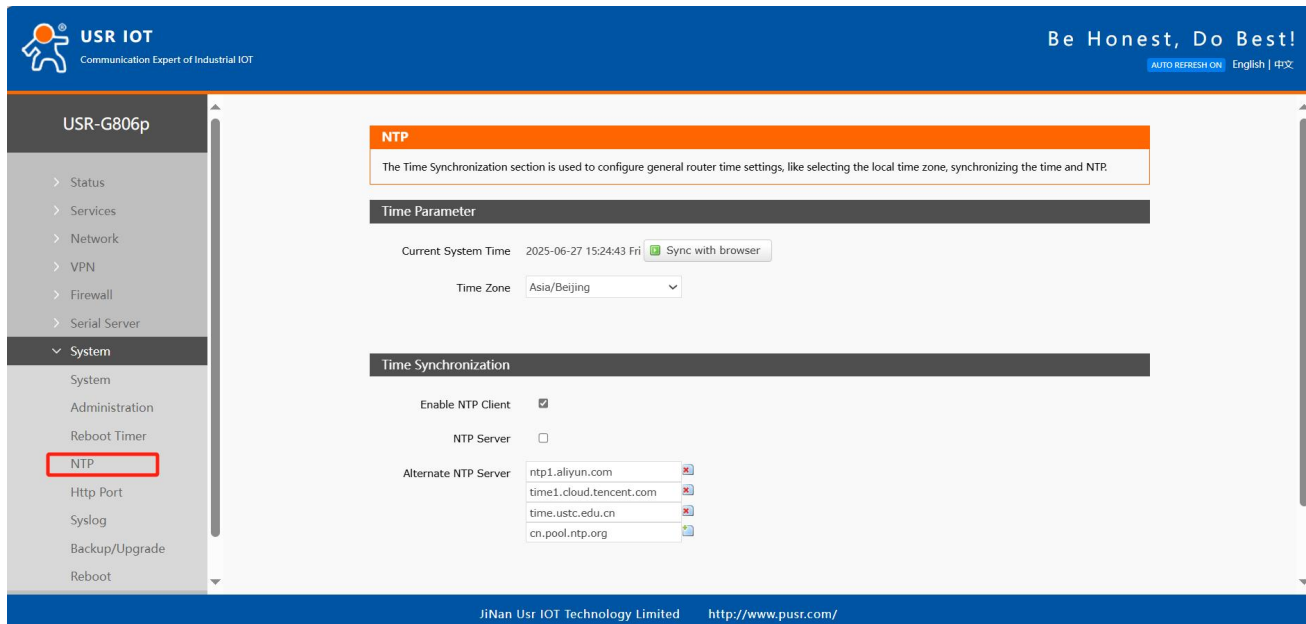
8.1. host name

The default hostname is USR-G806p.



Pic 88 host name

8.2. Time Settings

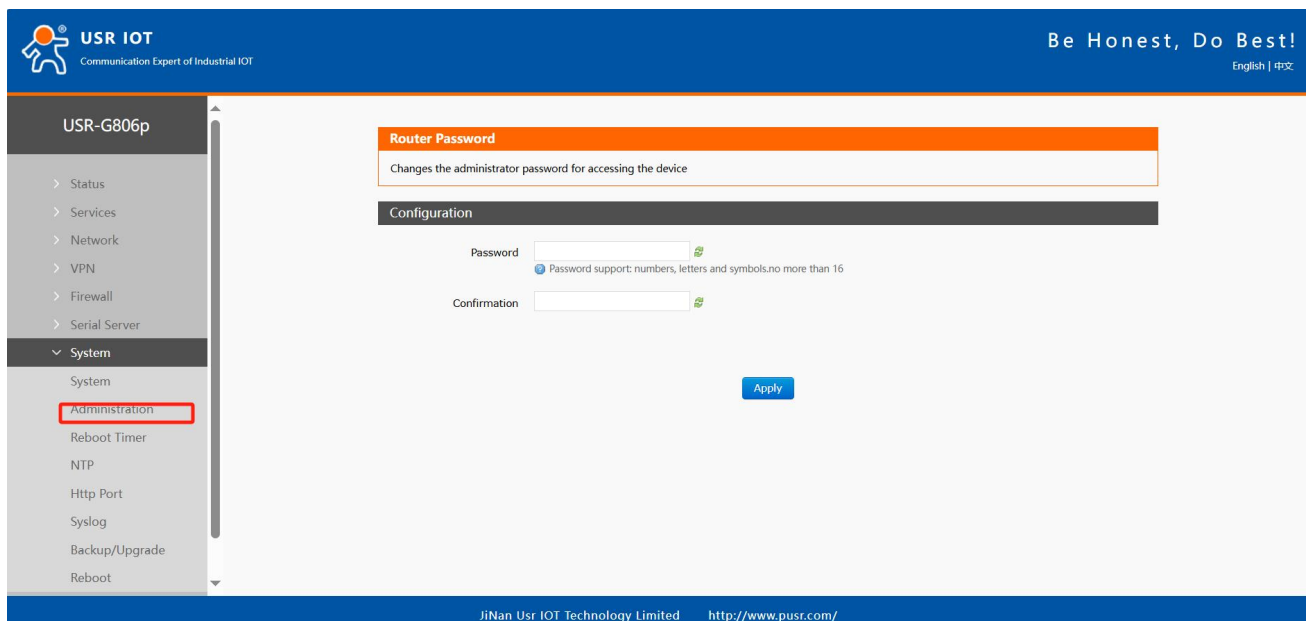


Pic 89 NTP page

< pay attention to >

- The router can perform network time synchronization and starts the NTP client function by default. The NTP server address is set.

8.3. Username and password Settings



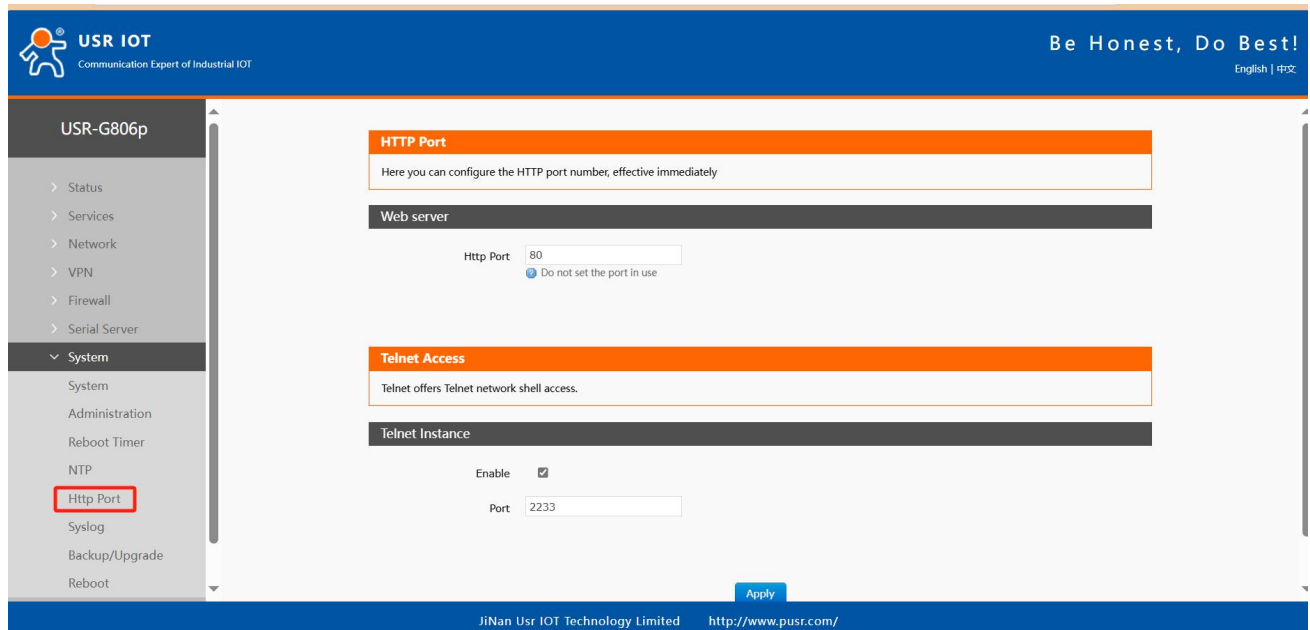
Pic 90 Username and password setup page

< pay attention to >

- The default password can be set. The default password is admin, and the user name cannot be set. This password is the management password (web login password).

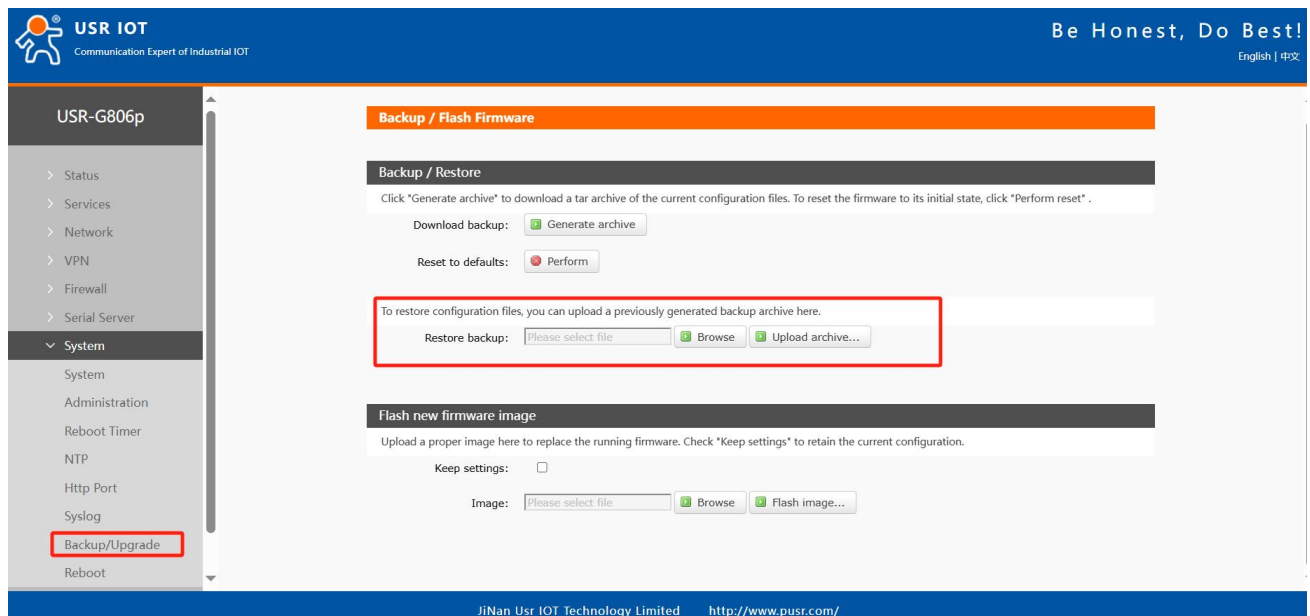
8.4. HTTP port

Set the port number of the web login page, and enable or disable the TELNET function.



Pic 91 HTTP port

8.5. Parameter backup and upload



Pic 92 Parameter backup upload page

Parameter upload: Upload the parameter file (xxx.tar.gz) to the router, then the parameter file will be saved and effective.

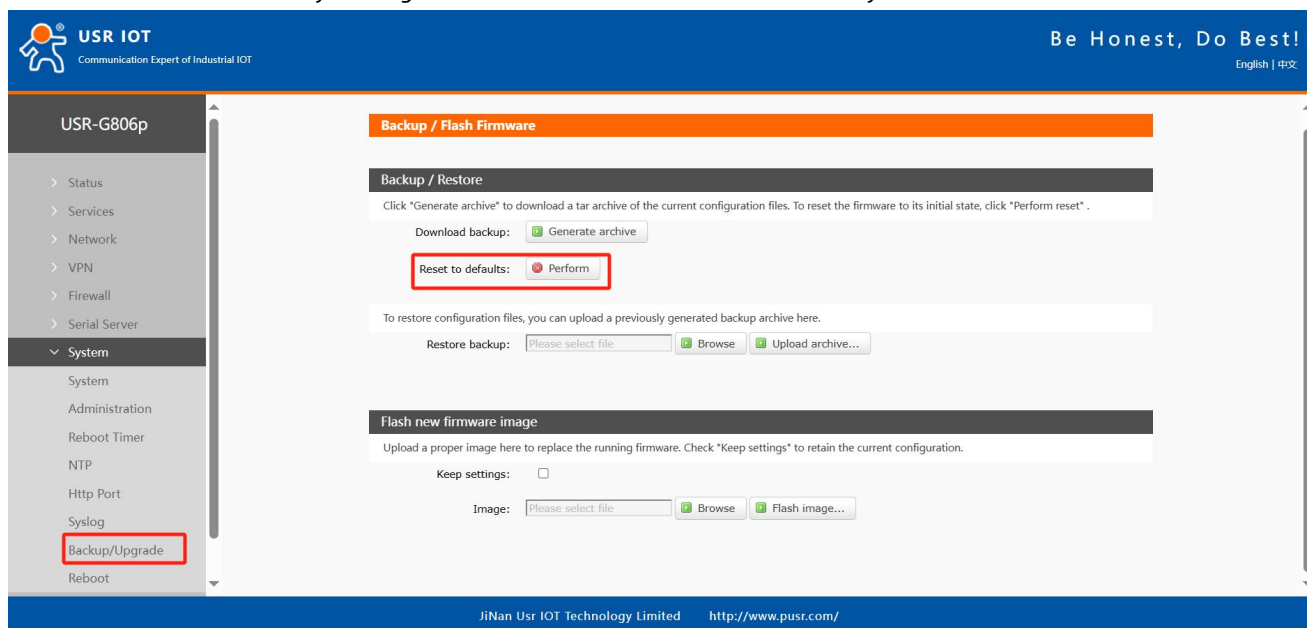
Note: Firmware recovery configuration is limited to the same version of firmware. Problems may occur due to different parameters in different versions. Users are advised to perform recovery configuration in the same version.

Parameter backup: Click the "Download Backup" button to backup the current parameter file as a compressed package file, such as backup-USR-G806ps-2019-09-16.tar.gz, and save it to the local.

8.6. factory data reset

You can restore factory parameters through the web page.

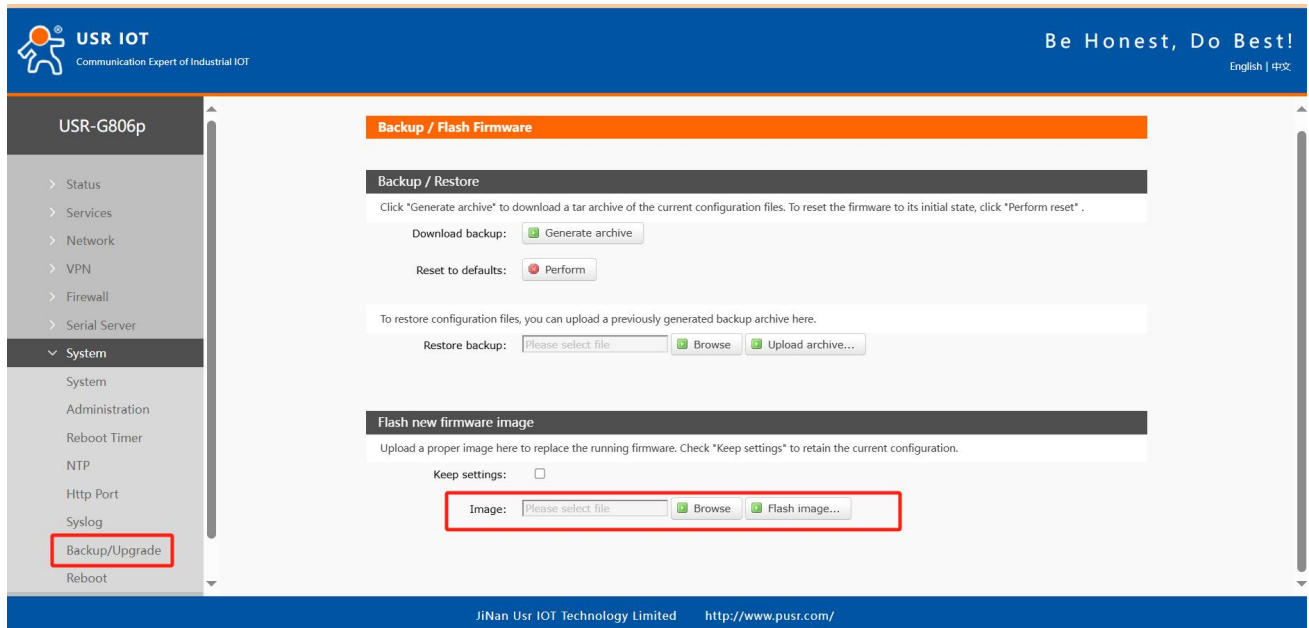
- By long pressing and releasing the Reload button (factory reset button) for 5~15 seconds, the USR-G806p router can be restored to the factory parameters;
- Do not disconnect power to the device during recovery. The factory recovery process lasts about 3 minutes;
- You can restore factory Settings via the web with the same functionality as follows.



Pic 93 Restore the factory page

8.7. firmware upgrade

The USR-G806p module supports online firmware upgrade in web mode.

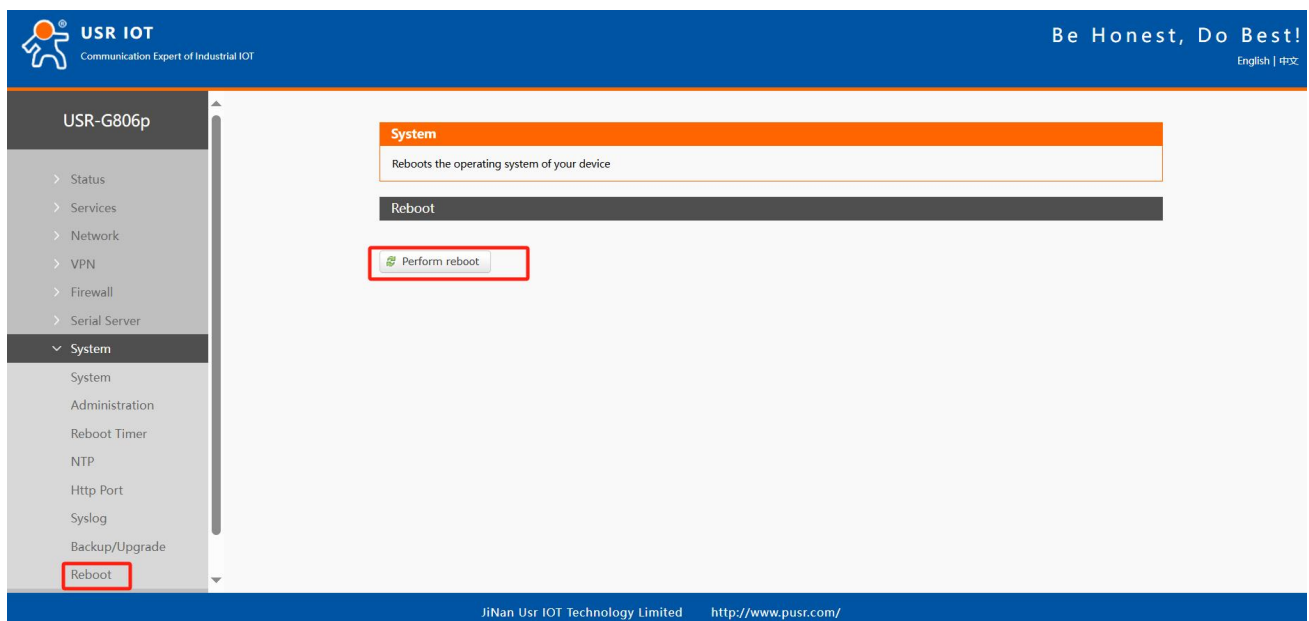


Pic 94 Restore the factory page

< explain >

- The firmware upgrade process will take 3 minutes, please try to log in the web page again after 3 minutes;
- You can choose whether to retain the configuration. By default, parameter upgrade is not retained (it is recommended not to retain parameter upgrade when upgrading to different versions);
- Do not disconnect power or unplug the network cable during firmware upgrade, otherwise the device may crash.

8.8. restart



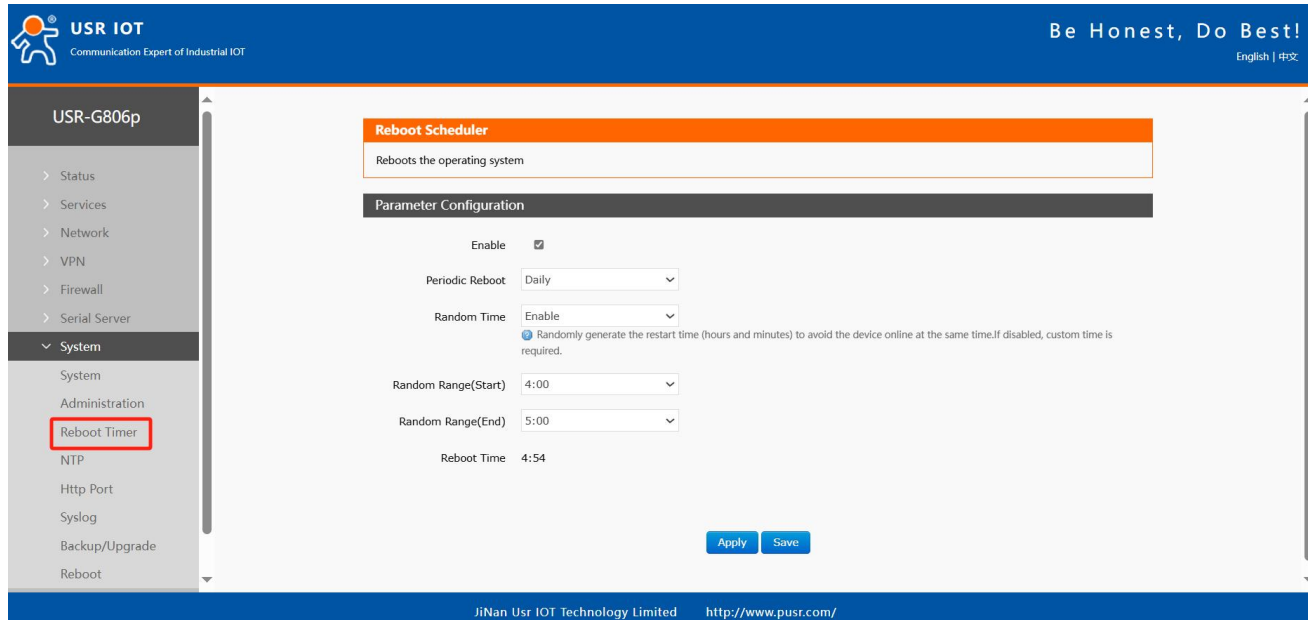
Pic 95 Restart the page

Click the button to restart the router. The restart time is the same as the power-on start time of the router, which

takes about 50 seconds to complete successfully.

8.9. Restart at regular intervals

To ensure the stability of router operation, it is recommended to enable the timed restart function. This function can facilitate users to manage the router in a timely manner.



Pic 96 Restart the Settings page

< explain >

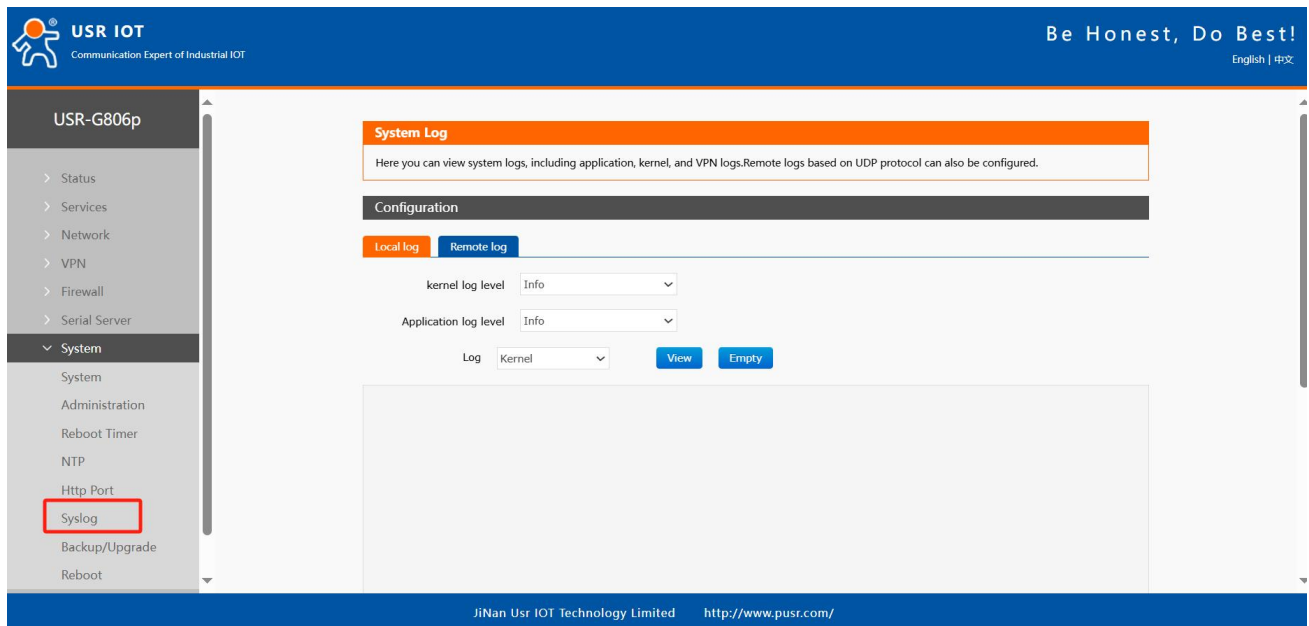
- The timer restart function is enabled by default. The restart plan will be completed at a random time between 4:00 and 5:00 every day. If you do not need this function, you can cancel it;
- According to the actual application, the scheduled restart plan that meets the conditions can be set, such as the fixed restart date every month or the fixed restart day every week;
- For example, if you select Monday at "Week", the scheduled restart task is executed randomly at 4-5 o'clock every Monday by default.

8.10. Daily record

Log is divided into remote log and local log, which are located in the system-system function menu.

long-range Log

- Remote log server: IP of the remote UDP server. Remote logging is not enabled when the IP is 0.0.0.0;
- Remote log server port: Remote UDP server port.



Pic 97 log page

Local logs

- Core log level: support debugging, information, attention, warning, error, key, alarm, emergency, a total of 8 levels; in order debugging is the lowest, emergency is the highest;
- Application log level: same as above;
- Logs (kernel, application, VPN) support instant view, clear, and log file export.

9. AT order set

The router's AT instruction set is suitable for SMS;

9.1. AT code repertory

Tab 33 Summary of AT instructions

| order number | name | function |
|--------------|----------|---|
| 1 | AT | The Test AT command is available |
| 2 | AT+R | Restart the device |
| 3 | AT+H | Help document and list all instructions |
| 4 | AT+CLEAR | Restore factory |
| 5 | AT+VER | Query the firmware version |
| 6 | AT+CMDPW | Query/set SMS password |
| 7 | AT+MAC | query LANMAC |
| 8 | AT+APN | Query/set APN parameters |
| 9 | AT+SN | query SN |

| | | |
|----------------------|-----------------|--|
| 10 | AT+CSQ | Query the current signal strength |
| 11 | AT+CPIN | Query SIM card status |
| 12 | AT+IMEI | query IMEI |
| 13 | AT+ICCID | query ICCID |
| 14 | AT+MCCMNC | query CIMI |
| 15 | AT+CNUM | query CUNM |
| 16 | AT+SYSINFO | Query network operators and formats |
| 17 | AT+CELLULAR | Query network mode |
| 18 | AT+WEBU | Query the web user name and password |
| 19 | AT+PLANG | query language |
| 20 | AT+UPTIME | Query the device running time |
| 21 | AT+WANINFO | Query wan information |
| 22 | AT+4GINFO | Query 4G information |
| 23 | AT+LANINFO | Query LAN information |
| 24 | AT+WANN | Query wan configuration |
| 25 | AT+LAN | Query the LAN configuration |
| 26 | AT+PING | Ping check |
| 27 | AT+TRAFFIC | Cellular traffic statistics |
| 28 | AT+WIREDTRAFFIC | Wired traffic statistics |
| 29 | AT+NETSTATUS | Get the default routing interface |
| 30 | AT+ALYSIMSWITCH | Query/set the SIM card operator |
| 31 | AT+DUALSIMMODE | Set dual SIM card switching mode |
| Serial port Settings | | |
| 32 | AT+S | Restart the DTU program |
| 33 | AT+UART1 | Query/Configure serial port 1 parameters |
| 34 | AT+UART2 | Query/Configure port 2 parameters |
| 35 | AT+UART1FT | Query/Configure the serial port 1 packing time |
| 36 | AT+UART1FL | Query/Configure the serial port 1 packet length |
| 37 | AT+UART2FT | Query/Configure the serial port 2 packing time |
| 38 | AT+UART2FL | Query/Configure the serial port 2 packet length |
| DTU set up | | |
| 39 | AT+CHLIST | Query all communication configurations of DTU |
| 40 | AT+CHSET | Set the DTU channel configuration |
| 41 | AT+CHDEL | Verify that the DTU channel configuration exists |
| 42 | AT+CHCLR | Remove all channel configurations of the DTU |

| | | |
|-----------------------|--------------------|---|
| 43 | AT+CHCFG | Query the DTU specified channel configuration |
| 44 | AT+CHCACHE | Query the cache configuration of the specified channel |
| 45 | AT+CHREG | Query the registration packet attributes of the specified channel |
| 46 | AT+CHHEART | Query the heartbeat packet attributes of the specified channel |
| 47 | AT+CHTLS | Query/set the TLS configuration for a specified channel |
| 48 | AT+CHMODBUS | Query/set the MODBUS configuration of a specified channel |
| MQTT | | |
| 49 | AT+MQTTFAMILYVER | Query/set the MQTT version of the specified channel |
| 50 | AT+MQTTFAMILYAUTH | Query/set MQTT authentication information for a specified channel |
| 51 | AT+MQTTFAMILYWILL | Query/set the MQTT legacy information for a specified channel |
| 52 | AT+MQTTFAMILYCLEAN | Query/set the MQTT clean session for a specified channel |
| 53 | AT+MQTTFAMILYRCTM | Query/set the MQTT reconnection interval for a specified channel |
| 54 | AT+MQTTFAMILYHEART | Query/set the MQTT heartbeat time for a specified channel |
| Theme Settings | | |
| 55 | AT+TOPICPUBLIST | Query the list of published topics for the specified channel |
| 56 | AT+TOPICPUBADD | Add a publishing topic |
| 57 | AT+TOPICPUBDEL | Delete the topic of the release |
| 58 | AT+TOPICPUBCLR | Clear the release topic |
| 59 | AT+TOPICSUBLIST | Query the list of subscription topics |
| 60 | AT+TOPICSUBADD | Add subscription topics |
| 61 | AT+TOPICSUBDEL | Delete the subscription topic |
| 62 | AT+TOPICSUBCLR | Clear the subscription topic |
| 63 | AT+NETAT | Query/set network AT configuration |
| Serial port heartbeat | | |
| 64 | AT+HEARTEN | Query/set serial port heartbeat enable |
| 65 | AT+HEARTBIND | Query/set serial heartbeat binding |
| 66 | AT+HEARTTM | Query/set serial port heartbeat time |
| 67 | AT+HEARTDT | Query/set serial heartbeat data |
| 68 | AT+HEARTDTHX | Query/set serial heartbeat data |

| | | |
|------|----------------|---|
| 69 | AT+NETRSTIM | Query/set network timeout reconnection |
| 70 | AT+NETRCTIM | Query/set the network timeout restart time |
| 71 | AT+COMRSTIM | Query/set the serial port timeout restart time |
| GNSS | | |
| 72 | AT+GNSSFUNEN | Query/Configure GNSS enabled information |
| 73 | AT+GNSSMOD | Query/Configure location type |
| 74 | AT+SOCKGLK | Query GNSS status |
| 75 | AT+QHEARTTM | Query/Configure heartbeat packet time |
| 76 | AT+QHWVER | Query GNSS hardware version |
| 77 | AT+QLOGOUT | Send a logout session signal |
| 78 | AT+QONLINE | Send an online session signal |
| 79 | AT+SOCKG | Query/set the working mode |
| 80 | AT+GHEARTEN | Query/set heartbeat packet enablement |
| 81 | AT+GHEARTTM | Query/set the heartbeat packet interval |
| 82 | AT+GHEARTCON | Query/set heartbeat packet data |
| 83 | AT+GPOSTP | Query/set the location package type |
| 84 | AT+GREGEN | Query/set the registration package enablement |
| 85 | AT+GREGTP | Query/set the registration package type |
| 86 | AT+GREGDT | Query/set the registration package data |
| 87 | AT+GCLOUD | Query/set the cloud ID and password |
| 88 | AT+GMDBS | Query/set the modbus device ID |
| 89 | AT+GPOSUPTM | Query/set the modbus reporting interval |
| 90 | AT+GREGSND | Query/set the registration package sending method |
| 91 | AT+GPGGA | Query gps gngga data |
| 92 | AT+GPRMC | Query gps gnrmc data |
| 93 | AT+CELLOCATION | Query the lac and CID information of the base station |
| 94 | AT+GNSSINFO | Query the GPS status |

9.1.1. AT order set

9.1.1.1. AT

| | |
|----------|---------------------------|
| name | AT |
| function | Test the AT command |
| query | order : AT return : OK |

| | |
|-----------|--|
| set up | not have |
| parameter | return : OK |
| explain | The instruction takes effect immediately, and the return OK represents that the AT instruction is in use |

9.1.1.2. AT+R

| | |
|-----------------|---|
| name | AT+IMEI |
| function | Query the IMEI code of the device |
| query | AT+IMEI +IMEI:code |
| parameter | Code: IMEI code. |
| give an example | Send: AT+IMEI Return: +IMEI: 868323023238378 |

9.1.1.3. AT+H

| | |
|-----------|---|
| name | AT+H |
| function | AT instruction set of the query module |
| query | order : AT+H return : OK AT AT+H ... |
| set up | not have |
| parameter | Return: AT instruction set Both are in English string format, without Chinese. |
| explain | not have |

9.1.1.4. AT+CLEAR

| | |
|-----------|---|
| name | AT+CLEAR |
| function | factory data reset |
| query | not have |
| set up | Command: AT+CLEAR |
| parameter | not have |
| explain | The command is executed correctly, and the device is restored to factory without a reply. |

9.1.1.5. AT+VER

| name | AT+VER |
|-----------|---|
| function | Query the device software version number |
| query | Command: AT+VER Return: +VER: ver |
| set up | not have |
| parameter | Ver: Current software version number, such as V1.0.03 |
| explain | The command is executed correctly and returns the current software version number |

9.1.1.6. AT+CMDPW

| name | AT+CMDPW |
|-----------|---|
| function | Query/set SMS AT command password |
| query | AT+CMDPW +CMDPW:<cmdpw> |
| set up | AT+CMDPW=<cmdpw> OK |
| parameter | cmdpw: The password set, such as test.cn#, can be set to 1-20Byte |
| explain | The command returns OK if it is executed correctly, and the device is restarted with this setting in effect |

9.1.1.7. AT+MAC

| name | AT+MAC |
|-----------|--|
| function | Query WAN port MAC |
| query | Command: AT+MAC Return: +MAC: mac |
| set up | not have |
| parameter | Mac: WAN port MAC, for example: 9CA525AA8B99 |
| explain | not have |

9.1.1.8. AT+APN

| name | AT+APN |
|----------|------------------------------|
| function | Query or set APN information |
| query | Command: AT+APN |

| | |
|-----------------|---|
| | Return: +APN: apn_name, user, pw, type |
| set up | Command: AT+APN=apn_name, user, pw, type return : OK |
| parameter | Apn_name: APN address, which can be empty [0-62] bytes, supports the character range [a-zA-Z0-9-.#@] User: user name, which can be empty [0-62] bytes, [33-126] ASCII characters PW: Password, which can be empty [0-62] bytes, [33-126] ASCII characters Type: authentication mode, none/pap/chap |
| give an example | Command: AT+APN=autocheck,,,,none return : OK |
| explain | The command is executed correctly and the configuration takes effect after restarting the device |

9.1.1.9. AT+SN

| | |
|-----------|----------------------------------|
| name | AT+SN |
| function | Query device SN information |
| query | order : AT+SN Return: +SN: sn |
| set up | not have |
| parameter | Sn: 20-bit sn code |
| explain | not have |

9.1.1.10. AT+CSQ

| | |
|-----------------|---|
| name | AT+CSQ |
| function | Query the current signal strength information of the device |
| query | AT+CSQ +CSQ: rssi |
| parameter | Rssi: Received signal strength indicator |
| give an example | Send: AT+CSQ Return: +CSQ: 31 |

< explain >

- Signal strength is commonly expressed in two units: dBm and asu.
- The US-G806p version uses asu value to indicate; the larger the value, the better the signal strength;

| | | |
|-------------------------------|-----------------------|-----------------------------------|
| standard | aus short-cut process | Signal strength (dBm) |
| GSM/CDMA/WCDMA/EVDO/EHRPD/LTE | 0-31 | dBm= -113dBm + signal strength *2 |

| | | |
|---------|--|---|
| | Nine of the nine had no signal | |
| TDSCDMA | 100-191 Nine of the nine had no signal | dBm= -116dBm + (signal strength-100) |

- When registered to different network modes, the signal strength can not be directly compared whether it is expressed as dBm or asu.
- In general, dBm \geq -90dBm and asu \geq 12. The signal strength meets the coverage requirements, which can be used to measure whether the current signal meets the standards.

9.1.1.11.AT+CPIN

| name | AT+CPIN |
|-----------|--|
| function | Check the status of the device SIM card |
| query | Command: AT+CPIN Return: +CPIN: cpin |
| set up | not have |
| parameter | Cpin: SIM card status value NOTREADY: Card status is not recognized READY: Identify card status SIM PIN: Lock the PIN status SIM PUK: Lock the PUK state |
| explain | not have |

9.1.1.12.AT+IMEI

| name | AT+IMEI |
|-----------|---|
| function | query facility IMEI |
| query | Command: AT+IMEI Return: +IMEI: imei |
| set up | not have |
| parameter | IMEI: IMEI number of the device |
| explain | not have |

9.1.1.13.AT+ICCID

| name | AT+ICCID |
|----------|--|
| function | Query SIM card ICCID |
| query | Command: AT+ICCID Return: +ICCID: iccid |
| set up | not have |

| | |
|-----------|------------------------------|
| parameter | ICcid: SIM card ICCID number |
| explain | not have |

9.1.1.14.AT+MCCMNC

| | |
|-----------|---|
| name | AT+MCCMNC |
| function | Query SIM card CIMI |
| query | Command: AT+MCCMNC Return: +MCCMNC: cimi |
| set up | not have |
| parameter | Cimi: SIM card Cimi number |
| explain | not have |

9.1.1.15.AT+CNUM

| | |
|-----------|---------------------------------|
| name | AT+CNUM |
| function | Query the SIM card phone number |
| query | AT+CNUM +CNUM:<cnum> |
| set up | not have |
| parameter | CNUM: SIM card phone number |
| explain | |

9.1.1.16.AT+SYSINFO

| | |
|-----------------|--|
| name | AT+SYSINFO |
| function | Query SYSINFO information |
| query | Command: AT+SYSINFO Return: +SYSINFO: ops_operate, ops_net_type |
| set up | not have |
| parameter | ops Operate: Operator information ops_net_type: Network mode |
| give an example | Command: AT+SYSINFO Return: +SYSINFO: CHN-CT, LTE |
| explain | not have |

9.1.1.17.AT+CELLULAR

| | |
|------|-------------|
| name | AT+CELLULAR |
|------|-------------|

| | |
|-----------------|---|
| function | Query the network mode of the network |
| query | Command: AT+CELLULAR Return: +CELLULAR: ops_net_type |
| set up | not have |
| parameter | ops_net_type: Network mode |
| give an example | Command: AT+CELLULAR Return: +CELLULAR: LTE |
| explain | not have |

9.1.1.18.AT+WEBU

| | |
|-----------|---|
| name | AT+WEBU |
| function | Query the web login user name and password |
| query | AT+WEBU +WEBU:<user>,<pw> |
| set up | not have |
| parameter | User: Web login user name PW: Web login password |
| explain | |

9.1.1.19.AT+PLANG

| | |
|-----------|--|
| name | AT+PLANG |
| function | Query the web login language |
| query | AT+PLANG +PLANG:<plang> |
| set up | AT+PLANG=<plang> OK |
| parameter | plang:zh_cn/en zn_cn: the Chinese language en: English |
| explain | |

9.1.1.20.AT+UPTIME

| | |
|-----------|-----------------------------|
| name | AT+UPTIME |
| function | Query system running time |
| query | AT+UPTIME +UPTIME:<time> |
| set up | not have |
| parameter | time |
| explain | |

9.1.1.21.AT+WANINFO

| name | AT+WANINFO |
|-----------|--|
| function | Query WAN network card information |
| query | AT+WANINFO +WANINFO:<mac><ip><mask><rx_packets><tr_packets><rx_bytes><tx_bytes> |
| set up | not have |
| parameter | Mac: WAN card MAC IP: WAN card IP Mask: Subnet mask of the WAN card rx_packets: Number of received packets Tr_packets: Number of packets sent rx_bytes: Receive traffic tx_bytes: Send traffic |
| explain | |

9.1.1.22.AT+4GINFO

| name | AT+4GINFO |
|-----------|--|
| function | Query cellular network card information |
| query | AT+4GINFO +4GINFO:<mac><ip><mask><rx_packets><tr_packets><rx_bytes><tx_bytes> |
| set up | not have |
| parameter | Mac: 4G network card mac IP: IP of 4G network card Mask: Subnet mask of 4G network card rx_packets: Number of received packets Tr_packets: Number of packets sent rx_bytes: Receive traffic tx_bytes: Send traffic |
| explain | |

9.1.1.23.AT+LANINFO

| name | AT+LANINFO |
|----------|--|
| function | Query LAN network card information |
| query | AT+LANINFO +LANINFO:<mac><ip><mask><rx_packets><tr_packets><rx_bytes><tx_bytes> |
| set up | not have |

| | |
|-----------|---|
| parameter | Mac: LAN network card mac IP: LAN network card IP Mask: Subnet mask of LAN network card rx_packets: Number of received packets Tr_packets: Number of packets sent rx_bytes: Receive traffic tx_bytes: Send traffic pour : If VLAN is configured, this command returns the LAN information |
| explain | |

9.1.1.24.AT+WANN

| | |
|-----------|--|
| name | AT+WANN |
| function | Query WAN port configuration |
| query | AT+WANN +WANN:<type>,<ip>,<mask>,<gateway> |
| set up | not have |
| parameter | Type: WAN port protocol type ip:WAN IP Mask: WAN subnet mask Gateway: WAN gateway |
| explain | |

9.1.1.25.AT+LAN

| | |
|-----------|--|
| name | AT+LAN |
| function | Query/set LAN port configuration |
| query | AT+LAN +LAN:<ip>,<mask> |
| set up | AT+LAN=<ip>,<mask> |
| parameter | IP: LAN IP standard IP address format x.x.x. x x: [0-255] Mask: LAN subnet mask x.x.x. x x: [0-255] conforms to the standard format of subnet mask pour : If VLAN is configured, this command returns the LAN information |
| explain | |

9.1.1.26.AT+PING

| | |
|-----------|---|
| name | AT+PING |
| function | Run the ping command |
| query | not have |
| set up | AT+PING=<ip> PING IP(IP): 56 data bytes |
| parameter | IP: IP or domain name, which cannot be empty. Ping is carried, and the parameter is invalid For example, c1 is invalid limit [1-200] Note: Parameters can only be IP or domain names. Other parameters will be judged according to the address and return results |
| explain | |

9.1.1.27.AT+TRAFFIC

| | |
|-----------|--|
| name | AT+TRAFFIC |
| function | Query 4G traffic for the time period |
| query | AT+TRAFFIC +TRAFFIC:<rx>,<tx>,<pro_time>,<at_time> |
| set up | not have |
| parameter | rx: The number of bytes received in the time period between the last query and this query Tx: Number of bytes sent between the last query and this query Protime: The last time this instruction was used at_time: The time stamp of this instruction is used |
| explain | |

9.1.1.28.AT+WIREDDTRAFFIC

| | |
|-----------|---|
| name | AT+WIREDDTRAFFIC |
| function | Query the wan traffic period |
| query | AT+WIREDDTRAFFIC +WIREDDTRAFFIC:<rx>,<tx>,<pro_time>,<at_time> |
| set up | not have |
| parameter | rx: The number of bytes received in the time period between the last query and this query |

| | |
|---------|--|
| | Tx: Number of bytes sent between the last query and this query Pro_time: The last time this instruction was used at_time: The time stamp of this instruction is used |
| explain | |

9.1.1.29.AT+NETSTATUS

| name | AT+NETSTATUS |
|-----------|---|
| function | Query the default route usage of the network card |
| query | AT+NETSTATUS +NETSTATUS:<net> |
| set up | not have |
| parameter | Net: The status of the network card at this time |
| explain | |

9.1.1.30.AT+ALYSIMSWITCH

| name | AT+ALYSIMSWITCH |
|-----------|---|
| function | Query the SIM card operator |
| query | AT+ALYSIMSWITCH +NETSTATUS:<net> |
| set up | not have |
| parameter | net: CHN-CT Telecom CMCC shift CUCC log-in |
| explain | |

9.1.1.31.AT+DUALSIMMODE

| name | AT+DUALSIMMODE |
|-----------|---|
| function | Query/set dual SIM card switching mode |
| query | AT+DUALSIMMODE +DUALSIMMODE:<mode> |
| set up | AT+DUALSIMMODE=<mode> OK |
| parameter | mode: Master is the master Mutual backup Manual |
| explain | Restart the dtu service to make the configuration effective |

9.1.1.32.AT+S

| | |
|-----------|---|
| name | AT+S |
| function | Restart the dtu service to make the configuration effective |
| query | not have |
| set up | AT+SOK |
| parameter | not have |
| explain | Restart the dtu service to make the configuration effective |

9.1.1.33.AT+UART1

| | |
|-----------|--|
| name | AT+UART1 |
| function | Set/Query the parameters of the 485 interface |
| query | AT+UART1 +UART1:<baudrate>,<data_bit>,<stop_bit>,<parity> |
| set up | AT+UART1=<baudrate>,<data_bit>,<stop_bit>,<parity> OK |
| parameter | <Baudrate>: baud rate, 230400/115200 (default) /57600/38400/19200/9600/4800/2400/1200. <data_bit>: data bit, 7/8 <stop_bit>: Stop bit, 1/2 <parity>: Check bit, NONE/EVEN/ODD. |
| explain | |

9.1.1.34.AT+UART2

| | |
|-----------|---|
| name | AT+UART2 |
| function | Set/Query the 232 interface parameters |
| query | AT+UART2 +UART2:<baudrate>,<data_bit>,<stop_bit>,<parity> |
| set up | AT+UART2=<baudrate>,<data_bit>,<stop_bit>,<parity> OK |
| parameter | <Baudrate>: baud rate, 115200 (default) /57600/38400/19200/9600/4800/2400/1200. <data_bit>: data bit, 7/8 <stop_bit>: Stop bit, 1/2 <parity>: Check bit, NONE/EVEN/ODD. |
| explain | |

9.1.1.35.AT+UART1FT

| | |
|-----------|---|
| name | AT+UART1FT |
| function | Set/Query the 485 packaging time interval |
| query | AT+UART1FT? +UART1FT:<time> |
| set up | AT+UART1FT=<time> OK |
| parameter | <time>: Packing time Range [0,1000] 0 (default) |
| explain | |

9.1.1.36.AT+UART1FL

| | |
|-----------|--|
| name | AT+UART1FL |
| function | Set/Query the 485 package length |
| query | AT+UART1FL +UART1FL:<length> |
| set up | AT+UART1FL=<length> OK |
| parameter | <length>: Packing length Range [5,1460] 1000 (default) |
| explain | |

9.1.1.37.AT+UART2FT

| | |
|-----------|---|
| name | AT+UART2FT |
| function | Set/Query 232 Pack length |
| query | AT+UART2FT +UART2FT:<time> |
| set up | AT+UART2FT=<time> OK |
| parameter | <time>: Packing time Range [0,1000] 0 (default) |
| explain | |

9.1.1.38.AT+UART2FL

| | |
|----------|---------------------------|
| name | AT+UART2FL |
| function | Set/Query 232 Pack length |

| | |
|-----------|--|
| query | AT+UART2FL +UART2FL:<length> |
| set up | AT+UART2FL=<length> OK |
| parameter | <length>: Packing length Range [5,1460] 1000 (default) |
| explain | |

9.1.1.39.AT+CHLIST

| | |
|-----------|--|
| name | AT+CHLIST |
| function | Query the list of communication channels |
| query | AT+CHLIST +AT+CHLIST:<CH>,<Protocol>,<Enable>,<Description> |
| set up | not have |
| parameter | <CH>: Channel name <Protocol>: Channel protocol TCPC/TCPs/UDPC/UDPS/MQTT/HTTPD/AWS/ALI <Enable>: Channel enable ON (default)/ OFF <Description>: Channel description |
| explain | |

9.1.1.40.AT+CHSET

| | |
|-----------|--|
| name | AT+CHSET |
| function | Query the communication channel list |
| query | not have |
| set up | AT+CHSET=<CH>,<Protocol>,<Enable>,<Description> OK |
| parameter | <CH>: Channel name <Protocol>: Channel protocol TCPC/TCPs/UDPC/UDPS/MQTT/HTTPD/AWS/ALI <Enable>: Channel enable ON (default)/ OFF <Description>: Channel description, range [1,32] bytes |
| explain | |

9.1.1.41.AT+CHDEL

| | |
|-----------|---------------------------------------|
| name | AT+CHDEL |
| function | Delete the communication channel |
| query | not have |
| set up | AT+CHDEL=<CH> OK |
| parameter | <CH>: Channel name range [1,32] bytes |
| explain | |

9.1.1.42.AT+CHCLR

| | |
|-----------|---------------------------------|
| name | AT+CHCLR |
| function | Clear the communication channel |
| query | not have |
| set up | AT+CHCLR OK |
| parameter | not have |
| explain | Delete all added channels |

9.1.1.43.AT+CHCFG

| | |
|----------|---|
| name | AT+CHCFG |
| function | Modify or query channel parameters |
| query | AT+CHCFG=<CH>? +OK=<CH>, <Protocol>, <Variable parameters based on 'Protocol'> |
| set up | AT+CHCFG=<CH>, <Protocol>, <Variable parameters based on 'Protocol'...> |

| | |
|-----------|--|
| parameter | <p><CH>: Channel name</p> <p><Protocol>: Protocol</p> <p>TCPC/TCPS/UDPC/UDPS/HTTPD/MQTT/Ali/AWS <Variable parameter section></p> <p>TCPC: <Server>,<Re-Port>,<Lo-Port>,<Trans>,<BindCOM></p> <p><Server>: Remote server address range [0-63] bytes <Re-Port>: Server port range [1-65535]</p> <p><Lo-Port>: Local port range [0-65535].0 is random</p> <p><Trans>: Transmission mode</p> <p>TRANS-Transparent transmission (default) MODBUS-ModBUSRTU</p> <p><BindCOM> Channel binding (ALL is not supported in MODBUS)</p> <p>485-COM1-485 (default)</p> <p>COM1-485 (default)</p> <p>232 - COM2-232</p> <p>ALL - COM1&COM2</p> <p>UDPC: <Server>,<Re-Port>,<Lo-Port>,<checkPort>,<BindCOM></p> <p><Server>: Remote server address range [0-63] test.cn (default)</p> <p><Re-Port>: Server port range [1-65535] <Lo-Port>: Local port range [0-65535]</p> <p>0 (default) -0 indicates random</p> <p><checkPort>: Port check ON (default) / OFF</p> <p><BindCOM> Channel binding</p> <p>485-COM1-485 (default)</p> <p>232 - COM2-232</p> <p>ALL - COM1&COM2</p> <p>UDPS: <Lo-Port>,<BindCOM></p> <p><Lo-Port>: Local port range [0-65535]. <BindCOM>: Channel binding</p> <p>485-COM1-485 (default)</p> <p>232 - COM2-232</p> <p>ALL - COM1&COM2</p> <p>MQTT: <Server>,<Re-Port>,<ID></p> <p><Server>: Remote server address range [1-128] character cloudmqtt.usr.cn (default)</p> <p><Re-Port>: Server port range [1-65535] 1883 (default)</p> <p><ID>: Client ID range [1-128] characters 123456 (default)</p> <p>AWS: <Server>,<Re-Port>,<ID></p> <p><Server>: Remote server address Range [1-128] character amazonaws.com.cn (default)</p> <p><Re-Port>: Server port range [1-65535] 8883 (default)</p> <p><ID>: Client ID range [1-128] characters 123456 (default)</p> <p>ALI: <Re-Port>,<Type>,<Key>,<name>,<Secret>,<Cli_ID>,<ID>,<server></p> |
|-----------|--|

| | |
|---------|--|
| | <p><Re-Port>: Server port range [1-65535] 1883 (default)</p> <p><Type>: Instance type</p> <p>PUBLIC-Public instance (default) ENTERPRISE-Enterprise instance</p> <p><Key>: ProductKey Range [1-128] characters</p> <p><name>: devicename, range [1-128] character <Secret>: deviceSecret range [1-128] character <Cli_ID>: client ID range [1-128] character</p> <p>123456 (default)</p> <p><ID>: A geographical ID</p> <p>cn-hangzhou/cn-shanghai/cn-qingdao/cn-beijing/cn-zhangjiakou/cn-huhehaote/cn-shenzhen/cn-chengdu/cn-hongkong/ap-southeast-1/ap-southeast-3/ap-southeast-5/eu-central-1</p> <p>When the instance type is an enterprise instance</p> <p><server>: The server address range [1-128] characters</p> <p>HTTPD:</p> <p><Server>,<Port>,<TP>,<chD>,<URL>,<TO>,<HD>,<BindCOM></p> <p><Server>: Remote server address range [0-63] characters <Port>: Server port range [1-65535] characters</p> <p><TP>: Request method</p> <p>GET (default)/POST <chD>: Enable filtering packet header ON (default) / OFF</p> <p><URL>: HTTP URL range [1-128] bytes "/1.php[3F]" (default)</p> <p><TO>: Time-out range [1-3600 seconds] 10 (default)</p> <p><HD>: Request header information range [1-128] bytes</p> <p>"Accept: text/html[0D][0A]" (default)</p> <p><BindCOM> Channel binding</p> <p>485-COM1-485 (default)</p> <p>232 - COM2-232</p> <p>ALL - COM1&COM2</p> |
| explain | <p>The protocol is inconsistent with the existing channel protocol and an error is returned</p> <p>When polling MODBUS, the serial port binding parameter is not allowed to be ALL</p> |

9.1.1.44.AT+CHCACHE

| | |
|----------|--|
| name | AT+CHCACHE |
| function | Query/set channel data cache function |
| query | AT+CHCACHE +CHCACHE:<CH>,<Enable>,<Cure>,<Mode> |
| set up | AT+CHCACHE OK |

| | |
|-----------|---|
| parameter | <CH>: Channel name <Enable>: Enable authentication when connecting to the server ON / OFF (default) <Cure>: Measures to deal with data overflow DISOLD-Discard old data DISNEW-Discard new data <Mode>: Cache mode PCKLEN-Cache length limit PCKCNT-Cache packet limit |
| explain | You do not need to enter other parameters after closing Supported channel protocols: TCPC/TCPs/MQTT/AWS/ Ali Cloud |

9.1.1.45.AT+CHREG

| | |
|-----------|--|
| name | AT+CHREG |
| function | Query/set channel data cache function |
| query | AT+CHREG=<CH> +CHREG:<CH>,<Mode>,<Type>[,<DataType>][,<Data>] OK |
| set up | AT+CHREG=<CH>,<Mode>,<Type>[,<DataType>][,<Data>] OK |
| parameter | <CH>: Channel name (HTTPD and MQTT are not supported) <Mode>: Registration package mode NONE-Close USER-Custom SN MAC <Type>: Sending method First-Send a packet when connecting to the server EVERY-Add the registration packet to the front of each packet sent When the registration package mode is customized [<DataType>] Custom registration package data type (only when the custom mode is selected) HEX-Custom registration packet data type is hexadecimal string range [2-64] ACSII-Custom registration packet data type is ascii string range [1-32] ["<Data>"]: Custom registration packet data content |
| explain | Supported channel protocol: TCPC/UDPC You do not need to enter any other parameters when you close the registration package |

9.1.1.46.AT+CHHEART

| | |
|----------|---|
| name | AT+CHHEART |
| function | Query/set heartbeat packet function |
| query | AT+CHHEART=<CH> +CHHEART:<CH>,<Mode>,<Type>[,<DataType>][,<Data>] OK |
| set up | AT+CHHEART=<CH>,<Mode>,<Type>[,<DataType>][,<Data>] OK |

| | |
|-----------|--|
| parameter | <CH>: Channel name (HTTPD and MQTT are not supported) <Mode>: Registration package mode NONE-Close USER-Custom SN MAC <Type>: Sending method First-Send a packet when connecting to the server EVERY-Add the registration packet to the front of each packet sent when the registration packet mode is custom [DataType] Custom registration package data type (only when the custom mode is selected) HEX-Custom registration package data type is a hexadecimal string Range [2-64] ASCII-Custom registration package data type is an ascii string range [1-32] [<Data>]: Custom registration package data content |
| explain | Supported channel protocol: TCPC/UDPC You do not need to enter any other parameters when you close the registration package |

9.1.1.47.AT+CHTLS

| | |
|-----------|---|
| name | AT+CHTLS |
| function | Query/set heartbeat packet function |
| query | AT+CHTLS=<CH> +CHTLS:<CH>,<Enable>,<Method> OK |
| set up | AT+CHTLS=<CH>,<Enable>,<Method> OK |
| parameter | <CH>: Channel name <Enable>: Authentication enabled when connecting to the server is OFF-Off (default) TLS10 - TLS1.0 TLS12 - TLS1.2 <Method>: Certificate authentication mode NONE-Do not verify the certificate (default) SERVER-Verify the server certificate BOTH-Two-way authentication |
| explain | You do not need to enter other parameters after closing Supported channel protocols:MQTT,All,TCPC,HTTPD [Note: AWS supports TLS by default and does not support AT command query configuration] |

9.1.1.48.AT+CHMODBUS

| | |
|----------|-------------------------------------|
| name | AT+CHMODBUS |
| function | Query/set heartbeat packet function |

| | |
|-----------|---|
| query | AT+CHMODBUS=<CH>,<Enable>,<Ack>,<Time> +CHMODBUS:<CH>,<Enable>,<Ack>,<Time> OK |
| set up | AT+CHMODBUS=<CH>,<Enable>,<Ack>,<Time> OK |
| parameter | <CH>: Channel name <Enable>: Host polling enables the status OFF-off (default) ON- open Ack: Overdue response OFF-Off (default) ON- open <TIME>: Time out range [10-6000] milliseconds 200 (default) |
| explain | No other parameters need to be input when closing. Channel protocols supported: TCPC, TCPS If the protocol transmission mode is not MODBUS, an error is returned |

9.1.1.49.AT+MQTTFAMILYVER

| | |
|-----------|--|
| name | AT+MQTTFAMILYVER |
| function | Query/set MQTT, version information |
| query | AT+MQTTFAMILYVER=<CH> +MQTTFAMILYVER:<CH>,<Ver> OK |
| set up | AT+MQTTFAMILYVER=<CH>,<Ver> OK |
| parameter | <CH>: Channel name <Ver>: MQTT version V3.1-V3.1 V3.1.1-V3.1.1 (default) |
| explain | Supported channel protocol: MQTT |

9.1.1.50.AT+MQTTFAMILYAUTH

| | |
|-----------|---|
| name | AT+MQTTFAMILYAUTH |
| function | Query/set MQTT, version information |
| query | AT+MQTTFAMILYAUTH=<CH> +MQTTFAMILYAUTH:<CH>,<Enable>,<Username>,<Password> OK |
| set up | AT+MQTTFAMILYAUTH=<CH>,<Enable>,<Username>,<Password> OK |
| parameter | <CH>: Channel name <Enable>: Enable the authentication status ON (default) / OFF when connecting to the server <Username>: The user name required for authentication when connecting to the server [1-128 bytes] <Password>: The password required for authentication when connecting to the server [1-128 bytes] |
| explain | No other parameters need to be entered when closing. Channel protocol is supported:MQTT |

9.1.1.51.AT+MQTTFAMILYWILL

| | |
|-----------|---|
| name | AT+MQTTFAMILYWILL |
| function | Query/set MQTT, last message |
| query | AT+MQTTFAMILYWILL=<CH> +MQTTFAMILYWILL:<CH>,<Enable>,<Topic>,<Qos>,<Payload> OK |
| set up | AT+MQTTFAMILYWILL =<CH>,<Enable>,<Topic>,<Qos>,<Payload> OK |
| parameter | <CH>: Channel name <Enable>: Switch status ON / OFF (default) <Topic>: The name of the legacy topic. Scope [1-128 bytes] <Qos>: The quality of service guarantee level for the legacy 0-At most once 1-At least once 2-Get it right the first time <Payload>: Content of the will [1-128 bytes] |
| explain | No other parameters need to be entered when closing. Channel protocol is supported:MQTT |

9.1.1.52.AT+MQTTFAMILYCLEAN

| | |
|-----------|--|
| name | AT+MQTTFAMILYCLEAN |
| function | Query/set MQTT clean session function |
| query | AT+MQTTFAMILYCLEAN=<CH> +MQTTFAMILYCLEAN:<CH>,<Enable> OK |
| set up | AT+MQTTFAMILYCLEAN =<CH>,<Enable> OK |
| parameter | <CH>: Channel name <Enable>: Switch status ON / OFF (default) |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.53.AT+MQTTFAMILYRCTM

| | |
|-----------|---|
| name | AT+MQTTFAMILYRCTM |
| function | Query/set MQTT reconnection detection interval |
| query | AT+MQTTFAMILYRCTM=<CH> +MQTTFAMILYRCTM:<CH>,<CTim> OK |
| set up | AT+MQTTFAMILYRCTM =<CH>,<CTim> OK |
| parameter | <CH>: Channel name <RCTim>: Reconnection detection interval range [1-3600] 5 (default) |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.54.AT+MQTTFAMILYHEART

| | |
|-----------|--|
| name | AT+MQTTFAMILYHEART |
| function | Query/set MQTT, heartbeat time |
| query | AT+MQTTFAMILYHEART =<CH>,<CTim> +MQTTFAMILYHEART =<CH>,<CTim> OK |
| set up | AT+MQTTFAMILYHEART =<CH>,<CTim> OK |
| parameter | <CH>: Channel name <Heart>: Heartbeat packet time MQTT/AWS: 30 (default) (0-6000 seconds) ALI: 300 (default) (30-1200 seconds) |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.55.AT+TOPICPUBLIST

| | |
|-----------|--|
| name | AT+TOPICPUBLIST |
| function | Query the MQTT pre-release topic list |
| query | AT+ TOPICPUBLIST=<CH> +TOPICPUBLIST:<CH>,<name>,<Topic>,<Qos>,<Retained>,<BindCOM>,<description> OK |
| set up | not have |
| parameter | <CH>: Channel name <name>: Name <Topic>: Publish the topic name <Qos>: Service quality assurance level 0-up to one time 1-At least once 2-Get it right the first time <Retained>: Whether to retain the message ON (default) / OFF <BindCOM>: Bind channel 485 - COM1-485 232 - COM2-232 ALL-COM1&COM2 <description>: Description |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.56.AT+TOPICPUBADD

| | |
|-----------|---|
| name | AT+TOPICPUBADD |
| function | Add new topics to the preset release topic |
| query | not have |
| set up | AT+TOPICPUBADD =<CH>,<name>,<Topic>,<Qos>,<Retained>,<BindCOM>,<description> OK |
| parameter | <CH>: Channel name <name>: Name <Topic>: Publish the topic name <Qos>: Service quality assurance level 0-up to once 1-At least once 2-Get it right the first time <Retained>: Whether to retain the message ON (default) / OFF <BindCOM>: Bind channel 485 - COM1-485 232 - COM2-232 ALL-COM1&COM2 <description>: Description |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.57.AT+TOPICPUBDEL

| | |
|-----------|---|
| name | AT+TOPICPUBDEL |
| function | Delete the topic with this name from the preset release topics in the specified channel |
| query | not have |
| set up | AT+ TOPICPUBDEL =<CH>,<name> OK |
| parameter | <CH>: Channel name <name>: Publish the name of the topic [1-128 bytes] |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.58.AT+TOPICPUBCLR

| | |
|-----------|--|
| name | AT+TOPICPUBCLR |
| function | Clear the preset release topic for the specified channel |
| query | not have |
| set up | AT+TOPICPUBCLR=<CH> OK |
| parameter | <CH>: Channel name |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.59.AT+TOPICSUBLIST

| | |
|-----------|--|
| name | AT+TOPICSUBLIST |
| function | Query the MQTT pre-subscribed topic list |
| query | AT+TOPICSUBLIST=<CH> +TOPICSUBLIST:<CH>,<name>,<Topic>,<Qos>,<BindCOM>,<descripti on> OK |
| set up | not have |
| parameter | <CH>: Channel name <name>: Name <Topic>: Publish the topic name <Qos>: Service quality assurance level 0-up to once 1-At least once 2-Get it right the first time <Retained>: Whether to retain the message ON (default) / OFF <BindCOM>: Bind channel |

| | |
|---------|--|
| | 485 - COM1-485 232 - COM2-232 ALL-COM1&COM2 <description>: Description |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.60.AT+TOPICSUBADD

| | |
|-----------|--|
| name | AT+TOPICSUBADD |
| function | Add a new topic to the preset subscription topic |
| query | not have |
| set up | AT+TOPICSUBADD =<CH>,<name>,<Topic>,<Qos>,<BindCOM>,<description> OK |
| parameter | <CH>: Channel name <name>: Name <Topic>: Publish the topic name <Qos>: Service quality assurance level 0-up to once 1-At least once 2-Get it right the first time <Retained>: Whether to retain the message ON (default) / OFF <BindCOM>: Bind channel 485 - COM1-485 232 - COM2-232 ALL-COM1&COM2 <description>: Description |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.61.AT+TOPICSUBDEL

| | |
|-----------|--|
| name | AT+TOPICSUBDEL |
| function | Delete the topic in the preset subscription topic that specifies the channel |
| query | not have |
| set up | AT+TOPICSUBDEL=<CH>,<name> OK |
| parameter | <CH>: Channel name <name>: The name of the topic to be deleted |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.62.AT+TOPICSUBCLR

| | |
|----------|---|
| name | AT+TOPICSUBCLR |
| function | Clear the preset subscription topic for the specified channel |
| query | not have |

| | |
|-----------|---|
| set up | AT+TOPICSUBCLR=<CH> OK |
| parameter | <CH>: Channel name |
| explain | Supported channel protocols: MQTT/AlI/AWS |

9.1.1.63.AT+HEARTEN

| | |
|-----------|---|
| name | AT+HEARTEN |
| function | Enable or disable the heartbeat packet function |
| query | AT+HEARTEN +HEARTEN:<heart_enable> |
| set up | AT+HEARTEN=<heart_enable> OK |
| parameter | heart_enable: ON/OFF |
| explain | The command is executed correctly and the configuration takes effect after restarting the DTU |

9.1.1.64.AT+HEARTBIND

| | |
|-----------|--|
| name | AT+HEARTBIND |
| function | Query/set the serial heartbeat packet binding port |
| query | AT+HEARTBIND? +HEARTBIND:<BindCOM> OK |
| set up | AT+ HEARTBIND=<BindCOM> OK |
| parameter | <BindCOM>: Bind the serial port 485 - COM1-485 232 - COM2-232 ALL - COM1&COM2 |
| explain | |

9.1.1.65.AT+HEARTTM

| | |
|-----------|---|
| name | AT+HEARTTM |
| function | Set/Query heartbeat time |
| query | AT+HEARTTM? +HEARTTM:<heart_times> OK |
| set up | AT+HEARTTM=<heart_times> OK |
| parameter | <heart_times>: Heartbeat time, range [1,6000] seconds |
| explain | |

9.1.1.66.AT+HEARTDT

| | |
|-----------|---|
| name | AT+HEARTDT |
| function | Query or set heartbeat packet data |
| query | AT+HEARTDT +HEARTDT:<data> |
| set up | AT+HEARTDT=<data> OK |
| parameter | Data: [2-512] hexadecimal number: 0-9, a-f, A-F, even bits |
| explain | The command is executed correctly and the configuration takes effect after restarting the DTU |

9.1.1.67.AT+HEARTDTHX

| | |
|-----------|--|
| name | AT+HEARTDTHX |
| function | Query/set the serial heartbeat packet content |
| query | AT+HEARTDTHX? +HEARTDTHX:<heartbeat> OK |
| set up | AT+ HEARTDTHX =<heartbeat> OK |
| parameter | <heartbeat>: Custom heartbeat packet content (HEX) |
| explain | |

9.1.1.68.AT+NETRSTIM

| | |
|-----------|--|
| name | AT+NETRSTIM |
| function | Set/Query the restart time without data |
| query | AT+NETRSTIM? +NETRSTIM:<Enable>,<timeout_restart> OK |
| set up | AT+NETRSTIM=<Enable>[,<timeout_restart>] OK |
| parameter | <Enable>: Enable ON/OFF (default) <timeout_restart>: Restart time without data, range [60-36000] seconds 36000 (default) (60-36000 seconds) |
| explain | You do not need to enter any other parameters after closing this function |

9.1.1.69.AT+NETRCTIM

| | |
|----------|---|
| name | AT+NETRCTIM |
| function | Set/Query no data reconnection time |
| query | AT+NETRCTIM? +NETRCTIM:<Enable>,<timeout_restart> OK |
| set up | AT+NETRCTIM=<Enable>[,<timeout_restart>] OK |

| | |
|-----------|---|
| parameter | <Enable>: Enable ON/OFF (default) <timeout_restart>: No data restart time, range [60-3600] seconds 3600 (default) (60-3600 seconds) |
| explain | You do not need to enter any other parameters after closing this function |

9.1.1.70.AT+COMRSTIM

| | |
|-----------|---|
| name | AT+COMRSTIM |
| function | Set/reset the serial port restart time without data |
| query | AT+COMRSTIM? +COMRSTIM:<Enable>,<BindCOM>,<timeout_restart> OK |
| set up | AT+COMRSTIM=<Enable>[,<BindCOM>,<timeout_restart>] OK |
| parameter | <Enable>: Enable ON (default)/ OFF <BindCOM>: Bind the serial port 485 - COM1-485 232 - COM2-232 ALL - COM1&COM2 <timeout_restart>: No data restart time, range [60-3600] seconds 3600 (default) (60-3600 seconds) |
| explain | You do not need to enter any other parameters to close this function |

9.1.1.71.AT+GNSSFUNEN

| | |
|-----------|---|
| name | AT+GNSSFUNEN |
| function | Turn on/off GNSS function |
| query | Q: AT+GNSSFUNEN? Answer: +GNSSFUNEN: <enable> |
| set up | Q: AT+GNSSFUNEN=<enable> answer : OK |
| parameter | Enable: 1 means open, 0 means close, default is off |
| explain | |

9.1.1.72.AT+GNSSMOD

| | |
|----------|--|
| name | AT+GNSSMOD |
| function | Select GNSS working mode |
| query | Q: AT+GNSSMOD? Answer: +GNSSMOD: <mode> |
| set up | Q: AT+GNSSMOD=<mode> answer : OK |

| | |
|-----------|---|
| parameter | mode: NET: Private cloud mode CLOUD: Someone's cloud model Default working mode: NET |
| explain | |

9.1.1.73.AT+SOCKGLK

| | |
|-----------|--|
| name | AT+SOCKGLK |
| function | Query the status of the location server connection |
| query | Q: AT+SOCKGLK? Answer: +SOCKGLK: <state> |
| set up | |
| parameter | <state>: OFF: ununited ON: Connected |
| explain | |

9.1.1.74.AT+QHEARTTM

| | |
|-----------|--|
| name | AT+QHEARTTM |
| function | Query/set the heartbeat sending interval |
| query | Q: AT+QHEARTTM? A: +QHEARTTM <time> |
| set up | Q: AT+QHEARTTM=<time> answer : OK |
| parameter | <time>: Send interval, [1-6000]s The default is 30s |
| explain | |

9.1.1.75.AT+QHWVER

| | |
|-----------|--|
| name | AT+QHWVER |
| function | Query/set hardware version number |
| query | Q: AT+QHWVER? Answer: +QHWVER: <ver> |
| set up | Q: AT+QHWVER=<ver> answer : OK |
| parameter | <ver>: Hardware version number, string type, up to 20 bytes supported by default: GNSS-v1.0 |
| explain | |

9.1.1.76.AT+QLOGOUT

| | |
|-----------|---|
| name | AT+QLOGOUT |
| function | Log out of the terminal in Qianxun mode |
| query | Q: AT+QLOGOUT answer : OK |
| set up | |
| parameter | |
| explain | Qianxun platform does not support this instruction, and it is mainly adapted to JT808 standard protocol for reservation |

9.1.1.77.AT+QONLINE

| | |
|-----------|---|
| name | AT+QONLINE |
| function | The terminal is logged off and online in the Qianxun mode |
| query | Q: AT+QONLINE answer : OK |
| set up | |
| parameter | |
| explain | Qianxun platform does not support this instruction, and it is mainly adapted to JT808 standard protocol for reservation |

9.1.1.78.AT+SOCKG

| | |
|-----------|---|
| name | AT+SOCKG |
| function | Third-party cloud server related parameters |
| query | Q: AT+SOCKG? Answer: +SOCKG: <protocol>, <address>, <port> |
| set up | Q: AT+SOCKG=<protocol>, <address>, <port> answer : OK |
| parameter | <protocol>: Communication protocol, TCPC or TCPS <address>: Server address, domain name or IP. The default is test.usr.cn. In TCPS, this field can be empty <port>: Server port, range [1~65535], default: 2317 |
| explain | |

9.1.1.79.AT+GHEARTEN

| | |
|----------|--|
| name | AT+GHEARTEN |
| function | Heartbeat packet enablement control is enabled in the third-party cloud mode |

| | |
|-----------|---|
| query | Q: AT+GHEARTEN? A: +GHEARTEN: <enable> |
| set up | Q: AT+GHEARTEN=<enable> answer : OK |
| parameter | <enable>: Enable control, ON means on, OFF means off, default is off |
| explain | |

9.1.1.80.AT+GHEARTCON

| | |
|-----------|---|
| name | AT+GHEARTCON |
| function | Heartbeat packet content in the third-party cloud mode |
| query | Q: AT+GHEARTCON? A: +GHEARTCON: <content> |
| set up | Q: AT+GHEARTCON=<content> answer : OK |
| parameter | <content>: Heartbeat packet content, character type, length [1-512], default is 123456 |
| explain | |

9.1.1.81.AT+GHEARTTM

| | |
|-----------|--|
| name | AT+GHEARTTM |
| function | Query/set the heartbeat sending interval in third-party cloud mode |
| query | Q: AT+GHEARTTM? A: +GHEARTTM <time> |
| set up | Q: AT+GHEARTTM=<time> answer : OK |
| parameter | <time>: Sending interval, [1~6000]s, default is 30s |
| explain | |

9.1.1.82.AT+GPOSTP

| | |
|-----------|--|
| name | AT+GPOSTP |
| function | Query/set the heartbeat sending type in third-party cloud mode |
| query | Q: AT+GPOSTP? Answer: +GPOSTP <type> |
| set up | Q: AT+GPOSTP=<type> answer : OK |
| parameter | <type>: |
| | RMC: The original field of RMC in the GNSS information report |

| | |
|---------|---|
| | GGA: The original GGA field in the GNSS information reported MDBS: The MODBUS46 function code is reported. Default: MDBS |
| explain | |

9.1.1.83.AT+GREGEN

| | |
|-----------|--|
| name | AT+GREGEN |
| function | Query/set the heartbeat sending type in third-party cloud mode |
| query | Q: AT+GREGEN? A: +GREGEN: <enable> |
| set up | Q: AT+GREGEN=<enable> answer : OK |
| parameter | <enable>: Enable control, ON means open, OFF means close, default is off |
| explain | |

9.1.1.84.AT+GREGTP

| | |
|-----------|--|
| name | AT+GREGTP |
| function | Query/set the package type registered under third-party cloud mode |
| query | Q: AT+GREGTP? Answer: +GREGTP: <type> |
| set up | Q: AT+GREGTP=<type> answer : OK |
| parameter | <type>: [ICCID, IMEI, USER, IMSI, SN], default value: USER |
| explain | |

9.1.1.85.AT+GREGDT

| | |
|-----------|--|
| name | AT+GREGDT |
| function | Query/set the package type registered under third-party cloud mode |
| query | Q: AT+GREGDT? A: +GREGDT: <data> |
| set up | Q: AT+GREGDT=<data> answer : OK |
| parameter | <data>: User-defined registration packet data in hexadecimal string format with a maximum length of 256 bytes (after conversion), 2 to 512 even bytes, and a default of 7777772E7573722E636E |

| | |
|---------|--|
| explain | |
|---------|--|

9.1.1.86.AT+GCLOUD

| name | AT+GCLOUD |
|-----------|--|
| function | Query/set the content of human cloud parameters in third-party cloud mode |
| query | Q: AT+GCLOUD? Answer: +GCLOUD: <id>, <password> |
| set up | Q: AT+GCLOUD=<id>, <password> answer : OK |
| parameter | <id>: The registered ID of the cloud function is passed by someone. It is 20 bytes long and defaults to empty <password>: The communication password of the cloud function is passed by someone. The length is 8 bytes and the default is empty |
| explain | |

9.1.1.87.AT+GMDBS

| name | AT+GMDBS |
|-----------|--|
| function | Query/set MODBUS parameters in third-party cloud mode |
| query | Q: AT+GMDBS? Answer: +GMDBS: <id>, <address> |
| set up | Q: AT+GMDBS=<id>,<address> answer : OK |
| parameter | <id>: From the machine number, [0-255], default value: 1 <address>: Register address, [0-65535]. Default value: 0 |
| explain | |

9.1.1.88.AT+GPOSUPTM

| name | AT+GPOSUPTM |
|-----------|--|
| function | Query/set the interval of sending location information |
| query | Q: AT+GPOSUPTM? A: +GPOSUPTM: <time> |
| set up | Q: AT+GPOSUPTM=<time> answer : OK |
| parameter | <time>: Sending interval, [1~6000]s, default is 30s |
| explain | |

9.1.1.89.AT+GREGSND

| name | AT+GREGSND |
|-----------|---|
| function | Query/set the sending method of registration package under third-party cloud mode |
| query | Q: AT+GREGSND? Answer: +GREGSND <type> |
| set up | Q: AT+GREGSND=<type> answer : OK |
| parameter | <type>: <LINK/DATA>, default value: LINK |
| explain | |

9.1.1.90.AT+GPOSSND

| name | AT+GPOSSND |
|-----------|---|
| function | Query/set the heartbeat sending direction in private cloud mode |
| query | Q: AT+GREGSND? Answer: +GREGSND <type> |
| set up | Q: AT+GREGSND=<type> answer : OK |
| parameter | <type>: NET: Position the heartbeat packet to the network [default] COM: Position the heartbeat packet to the serial port DOUBLE: It is sent to both the network and the serial port |
| explain | |

9.1.1.91.AT+GPGGA

| name | AT+GPGGA |
|-----------|---|
| function | Query the original GPGGA information |
| query | Q: AT+GPGGA? Answer: +GPGGA: <gpgga> |
| set up | |
| parameter | Gpgga>: GPGGA raw information |
| explain | |

9.1.1.92.AT+GPRMC

| name | AT+GPRMC |
|----------|--------------------------------------|
| function | Query the original GPRMC information |
| query | Q: AT+GPRMC? |

| | |
|-----------|-----------------------------------|
| | Answer: +GPRMC: <gprmc> |
| set up | |
| parameter | GPRMC: Original GPRMC information |
| explain | |

9.1.1.93.AT+CELLOCATION

| | |
|-----------|--|
| name | AT+CELLOCATION |
| function | Query base station information |
| query | Q: AT+CELLOCATION? Answer: + CELLOCATION <lac>, <cid> |
| set up | |
| parameter | LAC: Location code <cid>: Cell ID |
| explain | |

9.1.1.94.AT+GNSSINFO

| | |
|-----------|---|
| name | AT+GNSSINFO |
| function | Query GNSS information |
| query | Q: AT+GNSSINFO? Answer: +GNSSINFO: <status>, <longitude_hem>, <longitude>, <latitude_hem>, <latitude> |
| set up | |
| parameter | <state>: Positioning status: A: valid positioning, V: invalid positioning <longitude_hem>: Longitude hemisphere: E and W <longitude>: Longitude (in degrees) <latitude_hem>: Latitude hemisphere: N and S <latitude>: Latitude (in degrees) |
| explain | |

10. Disclaimer

This document does not grant any intellectual property rights, either explicitly or implicitly, nor does it prohibit the granting of such rights. Apart from the liability stated in the terms and conditions for the sale of its products, our company assumes no other responsibilities. Furthermore, we do not make any explicit or implicit warranties regarding the sale and/or use of this product, including its suitability for specific purposes, marketability, or liability for any infringement of patents, copyrights, or other intellectual property rights. Our company reserves the right to modify the product specifications and descriptions at any time without prior notice.

11. Update log

| Version | Update content | Refresh time |
|---------|--|--------------|
| V1.0.0 | Create documents and complete relevant function descriptions | 2025-06-30 |



Your Trustworthy Smart IOT Partner



Official Website: www.pusr.com

Official Shop: shop.usriot.com

Technical Support: h.usriot.com

Inquiry Email: inquiry@usriot.com

Skype & WhatsApp: +86 13405313834

Click to view more: [Product Catalog](#) & [Facebook](#) & [Youtube](#)