PUSR®
www.pusr.com

Industrial 5G Router

USR-G816

User Manual

V2.0

Be Honest & Do Best

Your Trustworthy Smart Industrial IoT Partner

Content

1. Introduction ..... - 5 -
1.1. Features ..... - 5 -
1.2. Parameters table ..... - 6 -
1.3. Indicator introduction ..... - 7 -
1.4. Dimension ..... - 8 -
2. Get Started ..... - 8 -
2.1. Login router ..... - 8 -
2.2. Brief introduction of the webpage ..... - 9 -
3. Status & System ..... - 10 -
3.1. Status ..... - 10 -
3.2. System (Hostname) ..... - 10 -
3.3. Administration password ..... - 11 -
3.4. Reboot timer (Timed restart function) ..... - 12 -
3.5. NTP service ..... - 12 -
3.6. HTTP port ..... - 13 -
3.7. System log ..... - 14 -
3.8. Backup/Upgrade ..... - 15 -
3.9. Reboot ..... - 16 -
4. Network introduction ..... - 17 -
4.1. WAN interface ..... - 17 -
4.1.1. WAN_5G interface ..... - 17 -
4.1.2. WAN_WIRED interface ..... - 17 -
4.2. LAN interface ..... - 20 -
4.3. Cellular network ..... - 21 -
4.3.1. Configuration ..... - 21 -
4.3.2. SIM1/SIM2 configuration ..... - 22 -
4.3.3. Module information ..... - 24 -
4.4. Network switch ..... - 24 -
4.5. Wireless (Wi-Fi) ..... - 25 -
4.5.1. Wi-Fi settings of 2.4 & 5.8G ..... - 25 -
4.5.2. Client information ..... - 26 -

4.6. WWAN(STA) - 27 -
4.6.1. Basic settings - 27 -
4.6.2. 2.4G / 5.8G settings - 27 -
4.6.3. AP information - 29 -
4.7. DHCP introduction - 30 -
4.8. Static routes - 30 -
4.8.1. Static routing adding - 30 -
4.8.2. Router table - 31 -
4.9. WAN/LAN port switching - 32 -
4.10. Network diagnostics - 33 -
5. VPN - 33 -
5.1. PPTP Client - 33 -
5.2. L2TP Client - 35 -
5.3. OpenVPN - 36 -
5.3.1. OpenVPN client - 37 -
5.3.2. OpenVPN server - 39 -
6. Firewall - 39 -
6.1. General Settings - 39 -
6.2. Port forward - 40 -
6.2.1. Port forward - 40 -
6.2.2. DMZ function - 41 -
6.3. Traffic rules - 42 -
6.3.1. Open ports on router - 43 -
6.3.2. Add new forward rule - 44 -
6.3.3. Source NAT - 45 -
6.4. Access restrictions - 47 -
7. DTU Function - 50 -
7.1. General settings - 51 -
7.1.1. Protocol selection - 51 -
7.1.2. Heartbeat packet - 52 -
7.1.3. Registration packet - 52 -
7.1.4. Advanced settings(AT command password) - 54 -
7.2. Serial port settings - 54 -

7.2.1. Parameter description ..... - 54 -
7.2.2. Packeting mechanism ..... - 55 -
7.3. SOCKET ..... - 56 -
7.4. HTTP Client ..... - 58 -
7.5. Modbus gateway setting and test ..... - 59 -
7.6. Transparent data communication ..... - 61 -
8. Additional services ..... - 63 -
8.1. PUSR Cloud ..... - 63 -
8.1.1. Add USR-G816 on PUSR Cloud ..... - 63 -
8.1.2. Gateway Information ..... - 65 -
8.1.3. Remote access ..... - 66 -
8.1.4. Firmware upgrade ..... - 67 -
8.1.5. Alarm settings ..... - 68 -
8.2. DDNS ..... - 70 -
9. Contact Us ..... - 73 -
10. Disclaimer ..... - 73 -

1. Introduction

1.1. Features

Stable and reliable

- Industrial grade design for harsh environments, IP30 mental housing.
- Support DIN rail mounting, wall mounting and flat surface placement.
- Wide input voltage range 9~36VDC, reverse polarity protection.
- Multiple EMC protection: Surge, EFT and ESD protection
- Built-in hardware watchdog, fault self-detection and self-repair, to ensure system stability.

Flexible networking

- Dual sim cards, single standby.
- Supports 5G SA/NSA network, compatible with 4G/3G network.
- Equipped with gigabit Ethernet ports: 1*WAN/LAN (Switchable), 3*LAN.
- Equipped with 1*RS232/RS485 serial port which can be directly connected to sensors and other serial acquisition devices for data transmission.
- Optional GNSS function, realize precise positioning of assets.
- Supports dual band Wi-Fi, adopting Qualcomm chip.

Powerful function

- Supports 5G APN/VPDN sim cards.
- Supports worldwide main frequency band with 4G network backup.
- Support Modbus TCP/RTU protocol conversion， transparent TCP/UDP/HTTP data communication.
- Built-in ICMP keep-alive detection, heartbeat packet detection and other functions to ensure the stable operation of the device.
- Supports firewall, NAT, DMZ, port forwarding, access restriction, etc. to ensure data security.
- Cooperating with PUSR service, it can realize centralized management of remote equipment and improve operation and maintenance efficiency.
- Supports mainstream VPN: PPTP, L2TP and enhanced OpenVPN.

1.2. Parameters table

Table 1. Parameters of USR-G816

USR-G816 specifications		
Cellular Interface	Frequency	5G NR sub-6 GHz (3GPP Rel-16) Band(NA/NSA): n1/2/3/5/7/8/12/13/14/18/20/25/26/28/29/30/38/40/41/48/66/70/71/75/76/77/78/ 79; 4G LTE (CAT 19 DL / CAT 18 UL) LTE-FDD: B1/2/3/4/5/7/8/12/13/14/17/18/19/20/25/26/28/29/30/32/66/71; LTE-TDD: B34/38/39/40/41/42/43/48; LAA: B46; 3G WCDMA: B1/2/4/5/8/19
	Maximum Transmission Data Rate	5G SA Sub-6: Max. 2.4Gbps (DL)/Max. 900Mbps (UL); 5G NSA Sub-6: Max. 3.4Gbps (DL)/Max. 550Mbps (UL) LTE-FDD: Max. 1.6Gbps (DL)/Max. 200Mbps (UL) WCDMA: Max. 42 (DL)/Max. 5.76 (UL)
	Antennas	4 × SMA-K Connectors (Center PIN: SMA Female)
	SIM Slot	2 x (3 V/1.8 V) mini-SIM(2FF) Push-push type slot (SIM Card 2 can be configured with built-in eSIM)
Ethernet Interface	WAN	1 x WAN port (can be configured as LAN) 10/100/1000 Mbps, compliance with IEEE 802.3, IEEE 802.3u, supports auto MDI/MDIX crossover, Ethernet Isolation 1.5 KV RMS
	LAN	3 x RJ45 port, 10/100/1000 Mbps, supports auto MDI/MDIX crossover, Ethernet Isolation 1.5 KV RMS
Indicators	PWR	red, always on after powered on
	WORK	green, blinking every 1second when the router is ready and working properly
	NET	Mobile network type LEDs NET lights on after device is connected to the network. Green stands for 5G, green and red for 4G, and red for 3G
	SIG	Mobile signal strength indication LED Green represents excellent signal, two-color light represents good signal, red represents poor signal
	WLAN	always solid on when WiFi is enabled and working properly
	WAN	LED blinking When Connection established and data is being transferred over this port.
	LAN	LED blinking When Connection established and data is being transferred over this port.
Wi-Fi Interface	Antennas	2 × SMA-K Connectors (Center PIN: SMA Female)
	MIMO	2×2
	Standards	Concurrent dual-band 802.11a/n/ac (5.8GHz) and 802.11b/g/n (2.4GHz)
	Modes	AP/AP+STA/AP+WDS repeater
	Data speed	Up to 1733Mbps wireless operation rate at 5.8GHz
	Security	Wi-Fi security with WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA2-PSK+CCMP
	Transmission distance	200 meters by line of sight. Actual transmission distance depends on environment of the site.
GNSS(Optional)	Antenna	1 × SMA-K Connector (Center PIN: SMA Female)
	Technology	GPS, GLONASS, BeiDou, Galileo
	Protocol	NMEA 0183
Power Supply	Adapter	DC 12V/2A
	Connector	DC Power Jack Barrel Type Female 5.5*2.1mm Round socket or industrial terminal block(V+,V-),reverse polarity protection

	Input voltage range	DC9-36V
	Power consumption	Average current 630mA@12V and the maximum current 1.6A@12V
Serial Interface	Numbers	1 × RS485/RS232
	Connector	Terminal block
	Baud Rate(bps)	1200,2400,4800,9600,19200,38400,57600,115200,230400,460800(only 485)
	Signal definition	RS232: TXD, RXD, GND RS485: A, B, GND
	Data bits	7,8
	Stop bits	1,2
	Parity	NONE, ODD, EVEN
Physical Characteristics	Casing material	Metal shell, ingress protection IP30
	Dimensions	125.0*103.0*45.0mm (L*W*H, antenna pedestal, terminal block and DIN Rail are not included)
	Installation	Desktop, wall mounting and DIN-rail mounting
	EMC	Static IEC61000-4-2, level 3 Pulsed Electric Field IEC61000-4-4, level 3 Surge IEC61000-4-5, level 3
	Operating Temperature	-35℃ ~ +75℃
	Storage Temperature	-40℃ ~ +125℃ (Non-condensing)
	Relative Humidity 0	5%~95% (Non-condensing)
Others	Reload button	1 × Reload
	TBD	Debug interface (TTL Level)
	Ground protection	Screw
	Built-in	Watchdog
Software	Network Protocols	PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, HTTP, DNS, ARP, NTP, Telnet, SSH, DDNS, etc.
	VPN	LT2P, PPTP
	Security	Access Control, DMZ, Port Forwarding, SYN-Flood Protection, Filtering (IP& MAC & Domain)
	Management	Web UI, PUSR cloud
	Reliability	WAN Failover, Dual SIM Backup
	Serial port	Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to Modbus TCP)
Certificate	In progress	CE, *FCC, *WEEE, RoHS, *RCM, *WPC

1.3. Indicator introduction

USR-G816 provides 6 indicators in total, the specific description is as follows.

Table 2. LED indicator

Name	Description
PWR	Steady on: power supply is normal. Off: No power supply or abnormal power supply.
WORK	Blinking: The system works normally.
SIG	Green: Signal strength 25-31 (signal strong) Orange: Signal strength 15-24 (signal strength is basically normal, and equipment can be used under normal conditions) Red: Signal strength 1-14 (Signal strength is weak, please check antenna and the signal strength of current location)

WLAN	On: Enable WLAN Off: Enable WLAN
GNSS	Used for GNSS version
NET	Green: 5G network Orange: 4G network Red: 3G network

1.4. Dimension

- Sheet metal housing, DIN-Rail mounting and wall mounting supported.
- 125.0*103.0*45.0mm (L*W*H, accessories not included)

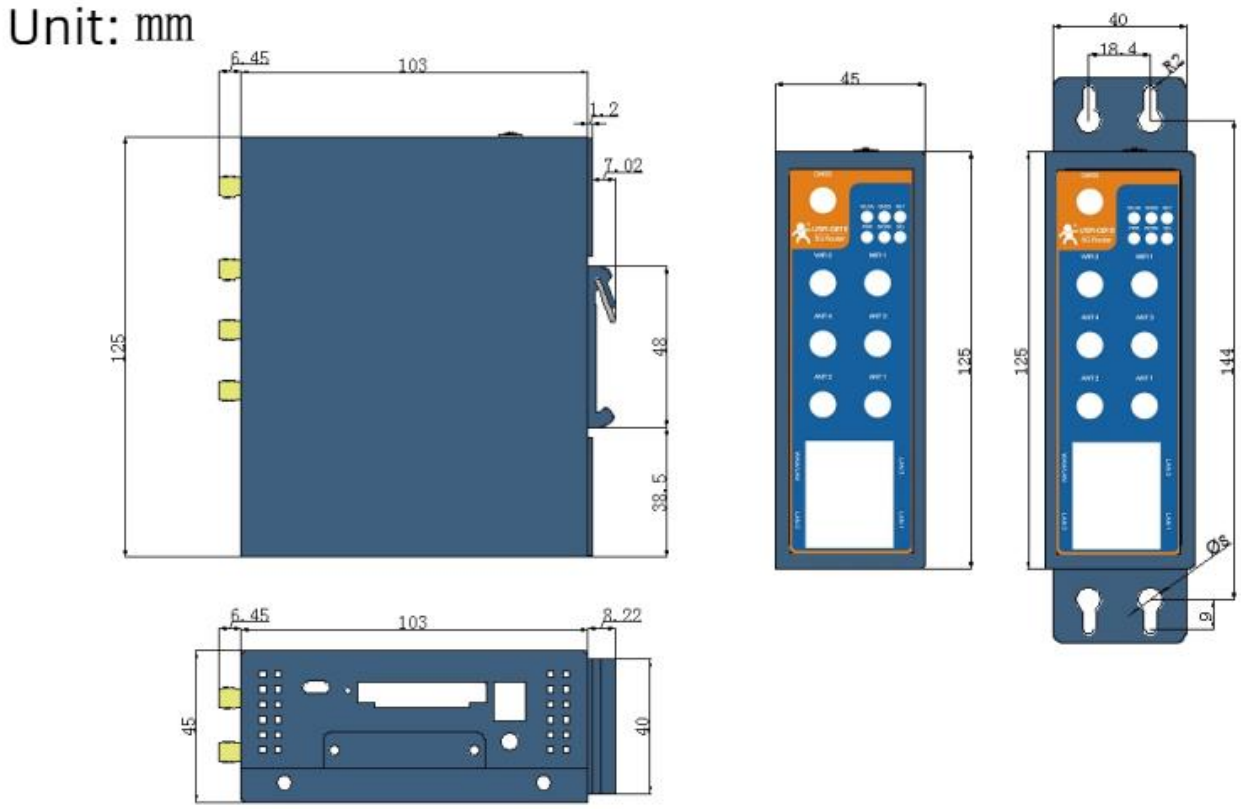

Figure 1. Dimension of USR-G816

2. Get Started

2.1. Login router

Power on the G816 router, connect PC to USR-G816 via LAN port or via Wi-Fi, users can login router via Chrome or the other browser. The default network parameters are shown in the following table:

Table 3. Default network parameters

Parameter	Default value

SSID	USR-G816-xxxx
LAN IP	192.168.1.1
Username	root
Password	root
Wi-Fi password	www.pusr.com

Open the browser, enter 192.168.1.1 in the URL blank, and press Enter, it will navigate to the following webpage. After entering the login password, clicking login, the web page will show configuration page of USR-G816.

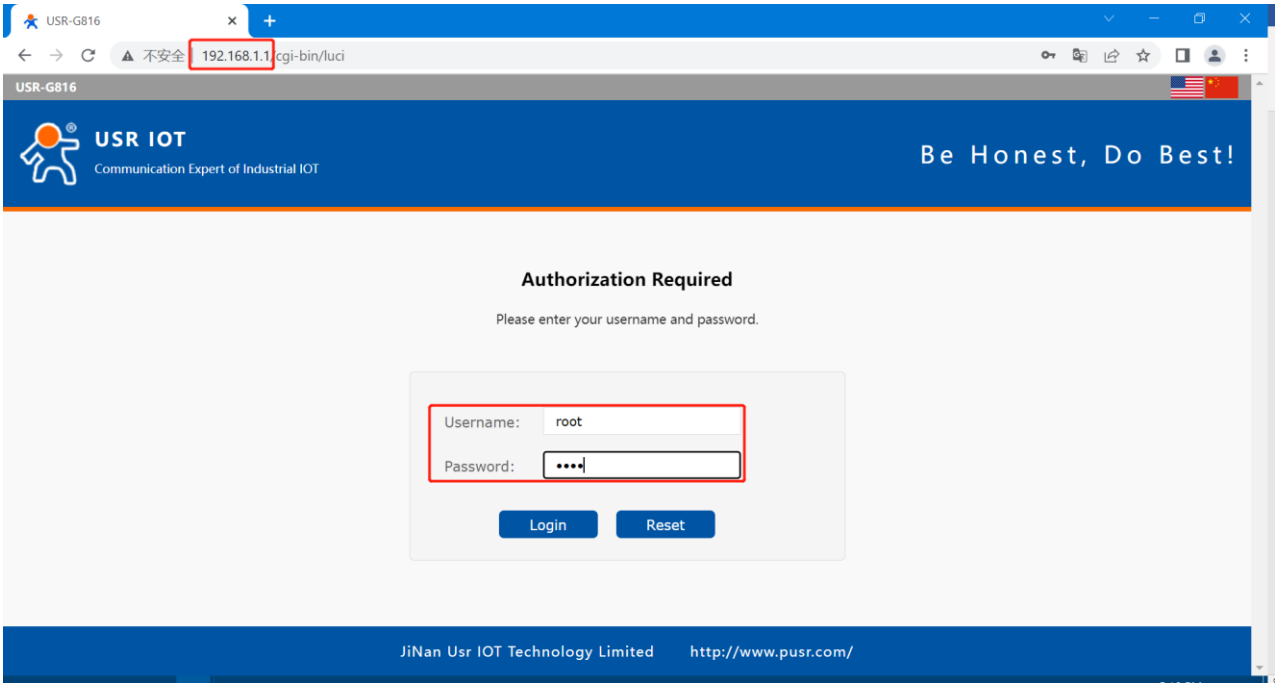

Figure 2. Login webpage

2.2. Brief introduction of the webpage

There are several tabs on the left side of the webpage, users can set parameters of USR-G816 on the tab pages.

- Status: Mainly display device name, firmware version, running status, and routes etc.
- Service: Mainly some additional functions, including dynamic DNS, GPS (GPS version), PUSR cloud.
- VPN: Configuration of VPN, such as PPTP, L2TP and OpenVPN.
- Network: In this interface, there are many categories related to network connection. Users can set parameters such as WAN port, LAN port and cellular network.
- Firewall: User can set firewall rule on this page such as inbound and outbound rules, port forwarding, blacklist, whitelist, and other information.
- DTU: Configure parameters related to DTU such as serial port and SOCKET.
- System: Mainly some basic functions, including restart, restore factory settings, firmware upgrade,

log checking, etc.

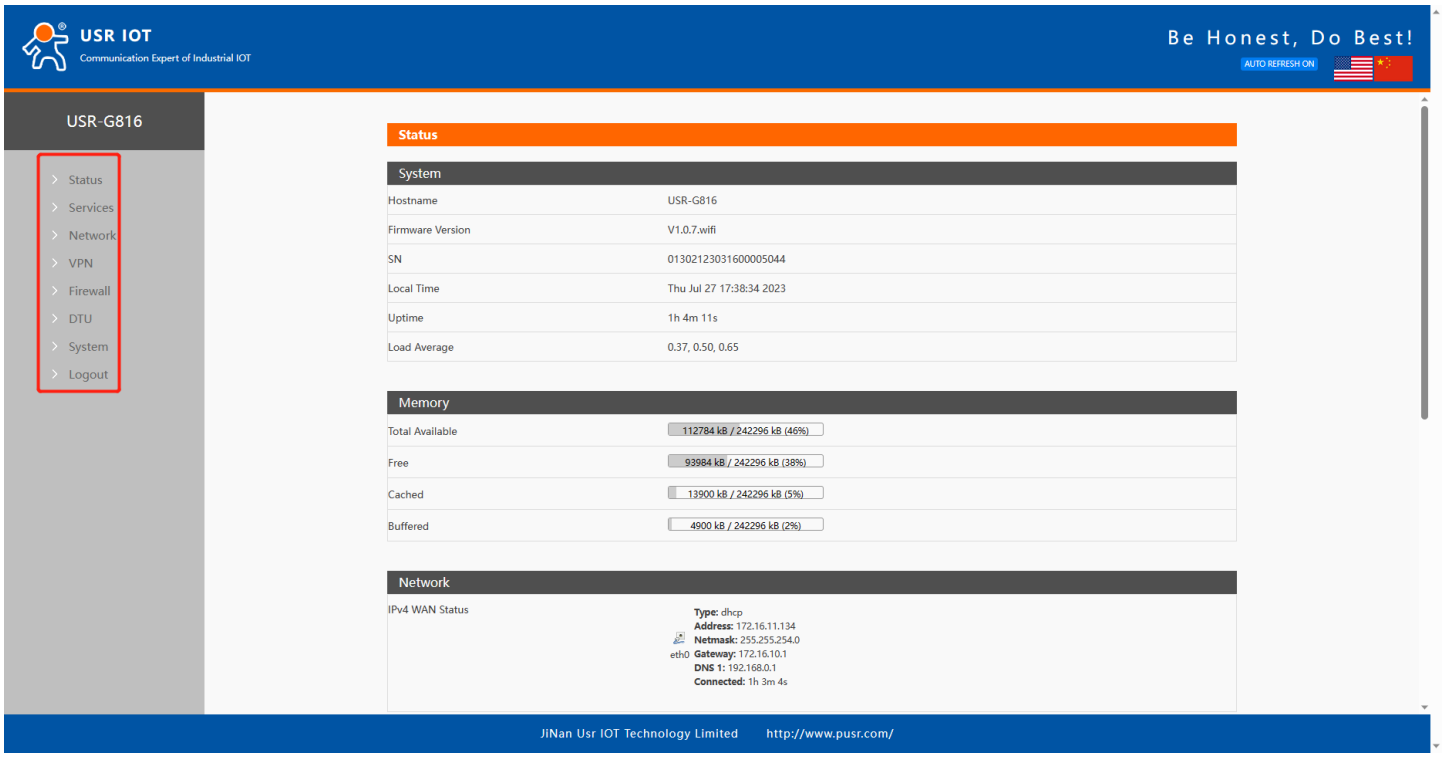

Figure 3. Status webpage

3. Status & System

3.1. Status

Users can get the basic information of USR-G816, such as firmware version, running time, IPv4 WAN status, routes list, and information about DHCP client.

3.2. System (Hostname)

In this page, users can modify the hostname, the default is USR-G816. After changing, click “Apply”, the changed value will take effect.

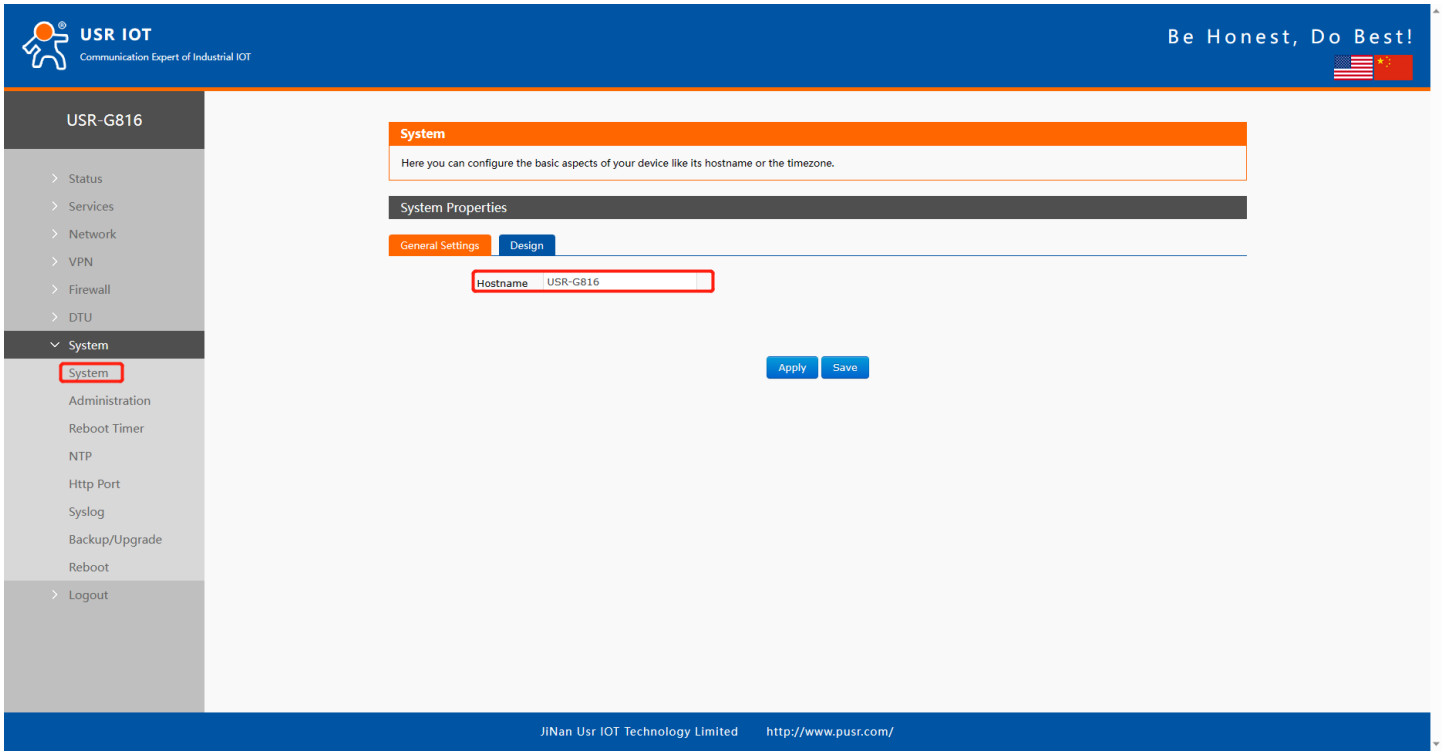

Figure 4. Hostname page

3.3. Administration password

This password is used when users login the built-in webpage.

The default login password is root. Users can modify it in this page for secure login.

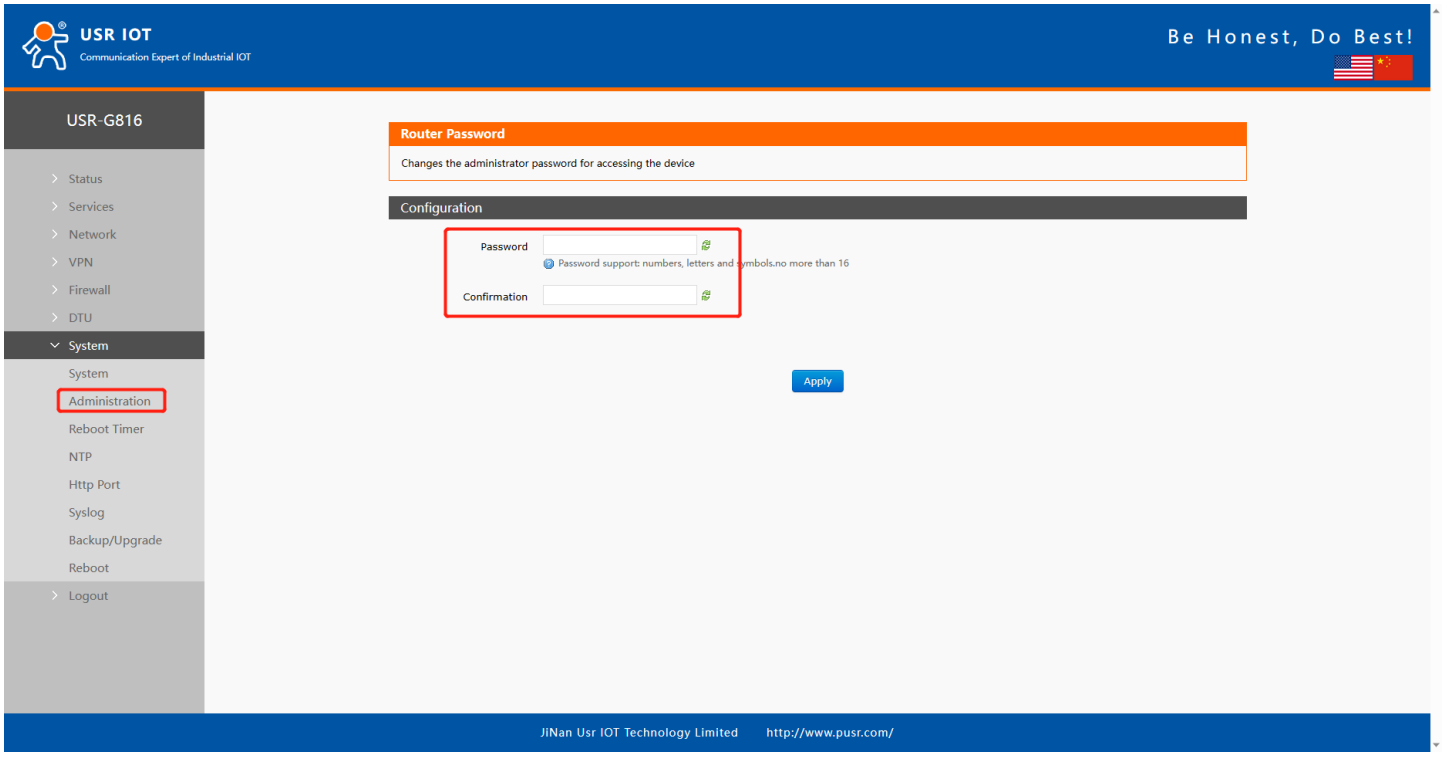

Figure 5. Administration password

3.4. Reboot timer (Timed restart function)

Users can realize the periodic restart of the router through parameter setting. It can be restarted on a daily, weekly, or monthly basis. Timed restart can regularly clear the operation cache to improve the stability of the router operation.

By default, this function is enabled and the router restarts every Sunday between 4 and 5 AM.

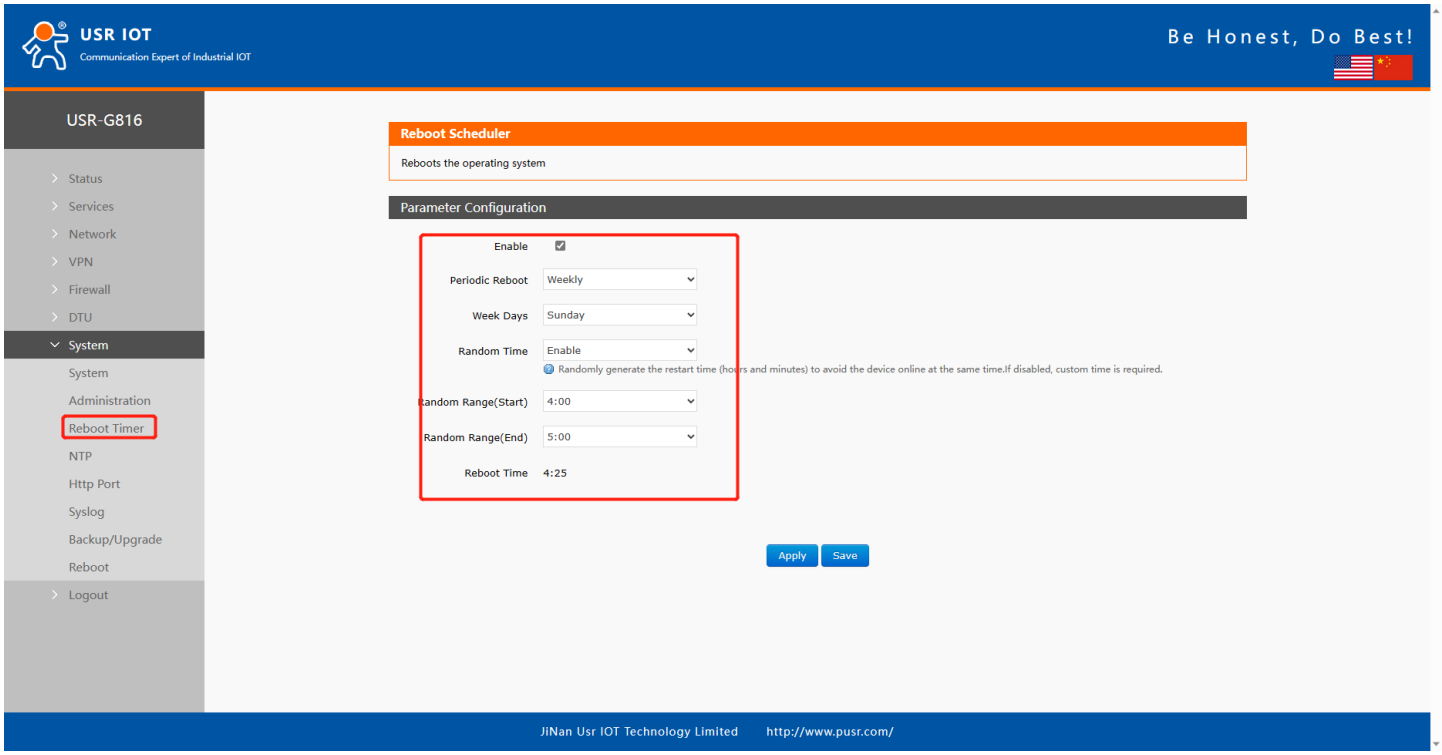

Figure 6. Timed restart function

3.5. NTP service

In the time parameter item, it can achieve the function of synchronizing the browser time and the time zone can be set as needed.

In Time Synchronization item, the router can be set to work at NTP client or NTP server. USR-G816 provides 4 configurable NTP server options on webpage.

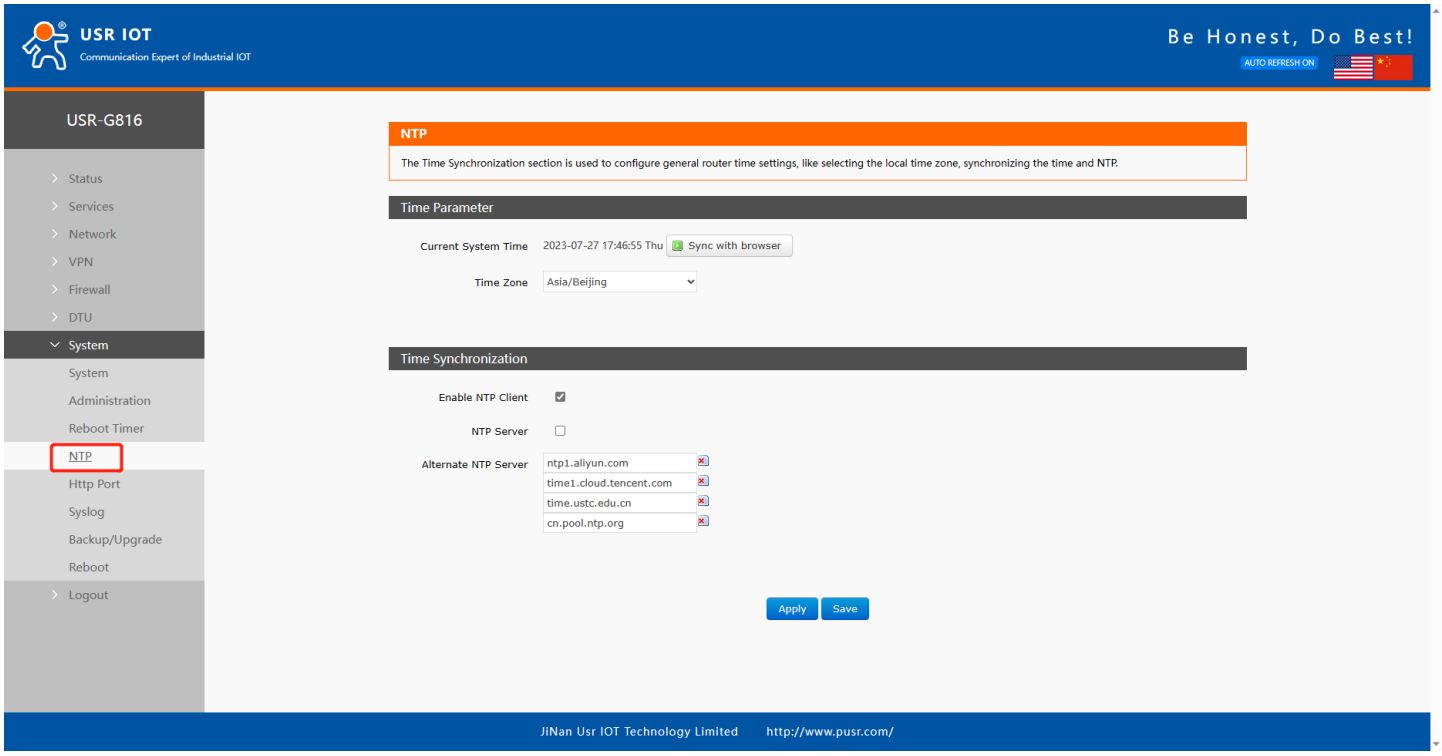

Figure 7. NTP Settings

3.6. HTTP port

The port of logging in the webpage, default is 80, users can modify it in this page.

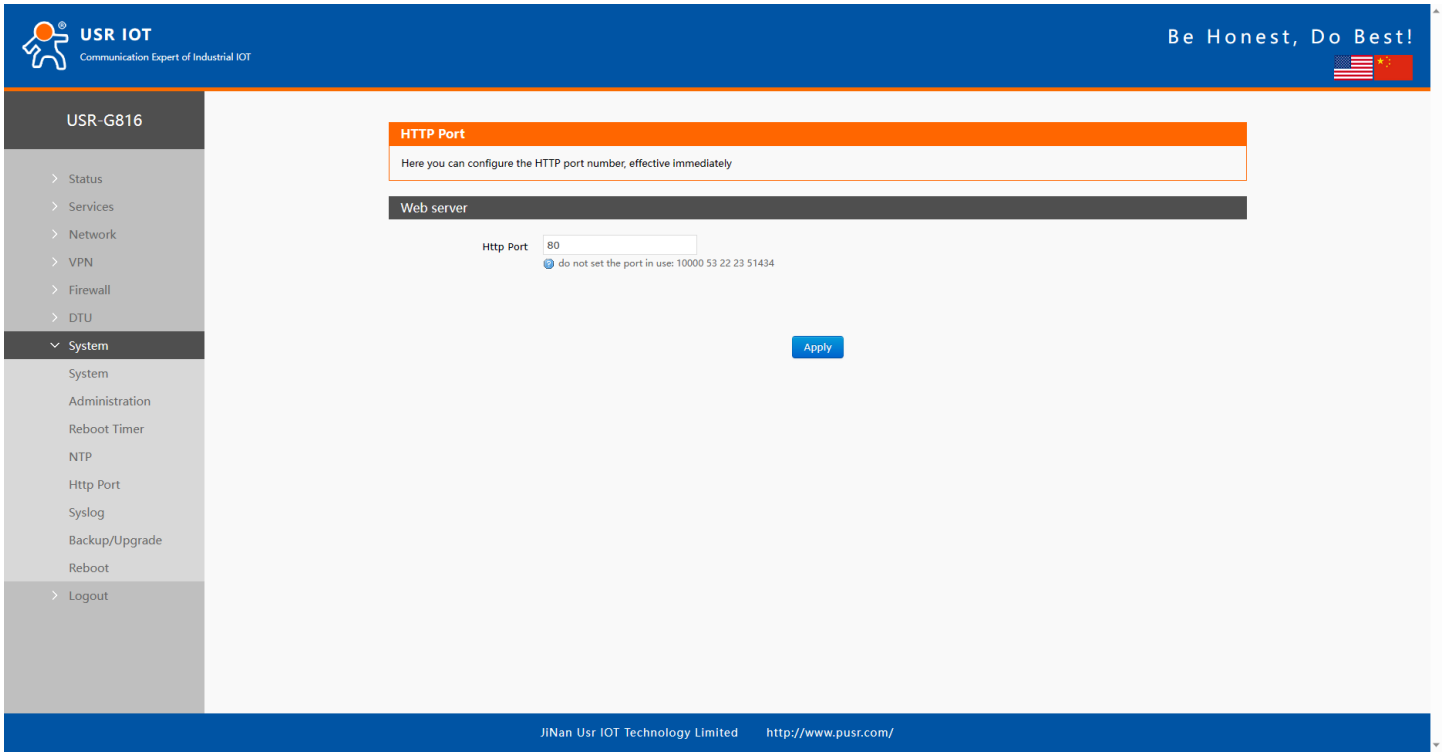

Figure 8. HTTP port

3.7. System log

- Local log

  Users can view the log information and download the log information in this page.

  Kernel log level: Debug, Info, Notice, Warning, Error, Critical, Alert and Emergency.

  Application log level: Debug, Info, Notice, Warning, Error, Critical, Alert and Emergency.

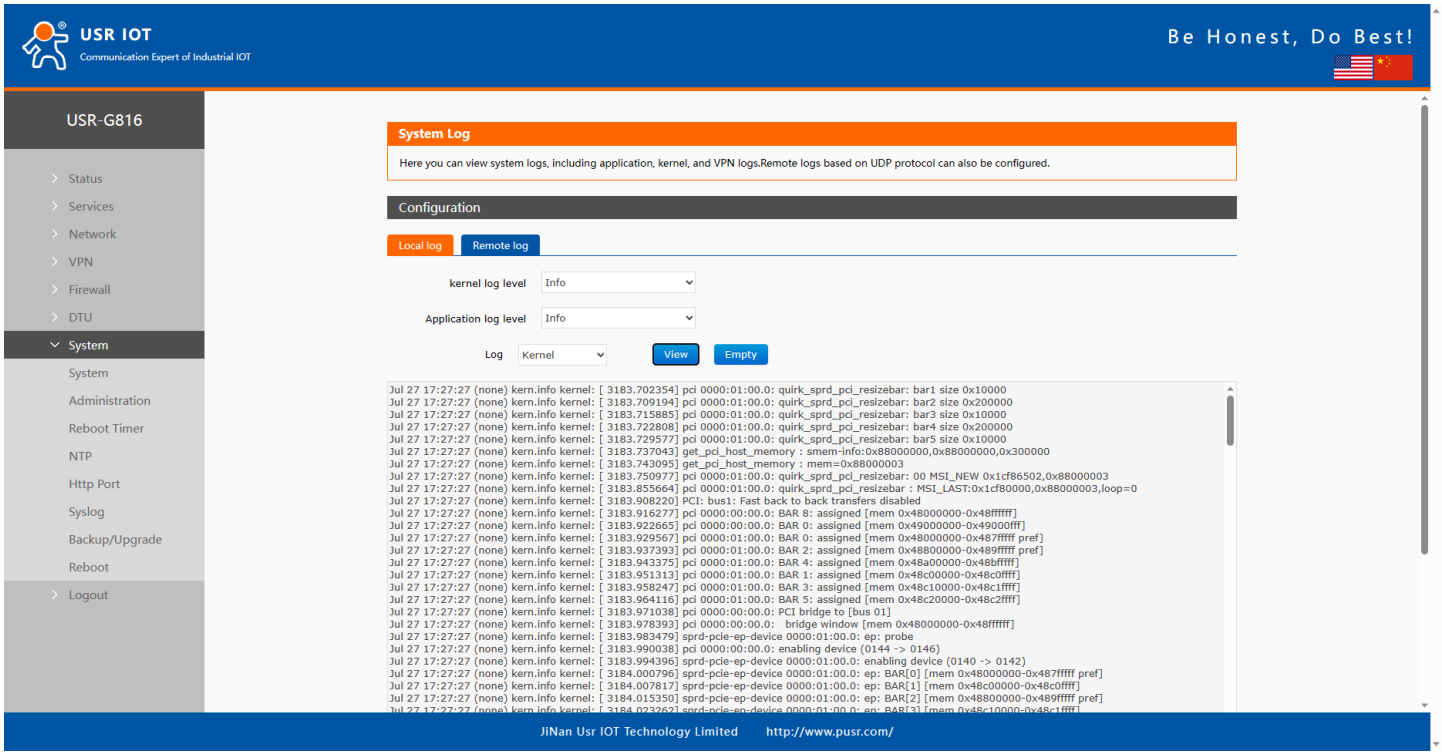

Figure 9. Local system log

- Remote log

  The remote service IP is 0.0.0.0, it means the remote log function is disabled. Users can change the remote service IP and port.

  Remote log is based on UDP protocol. The following picture shows how to receive the remote log.

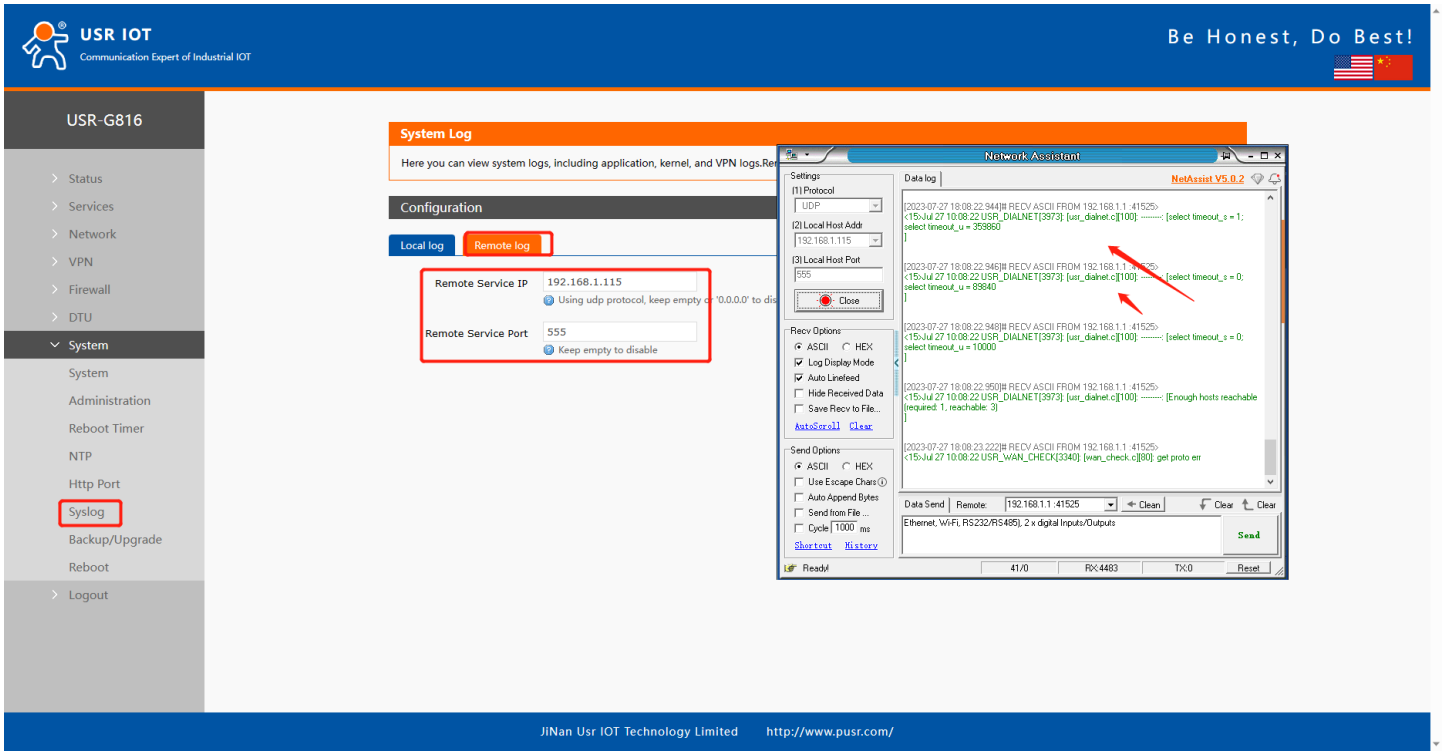

Figure 10. Remote system log

3.8. Backup/Upgrade

Download backup: Click "Generate archive" to download a tar archive of the current configuration files.

Restore backup: Click “Browse” to select the backup archive file (Downloaded backup file), and then upload the backup file.

Reset to defaults: Click this button, the USR-G816 will restore to factory default settings.

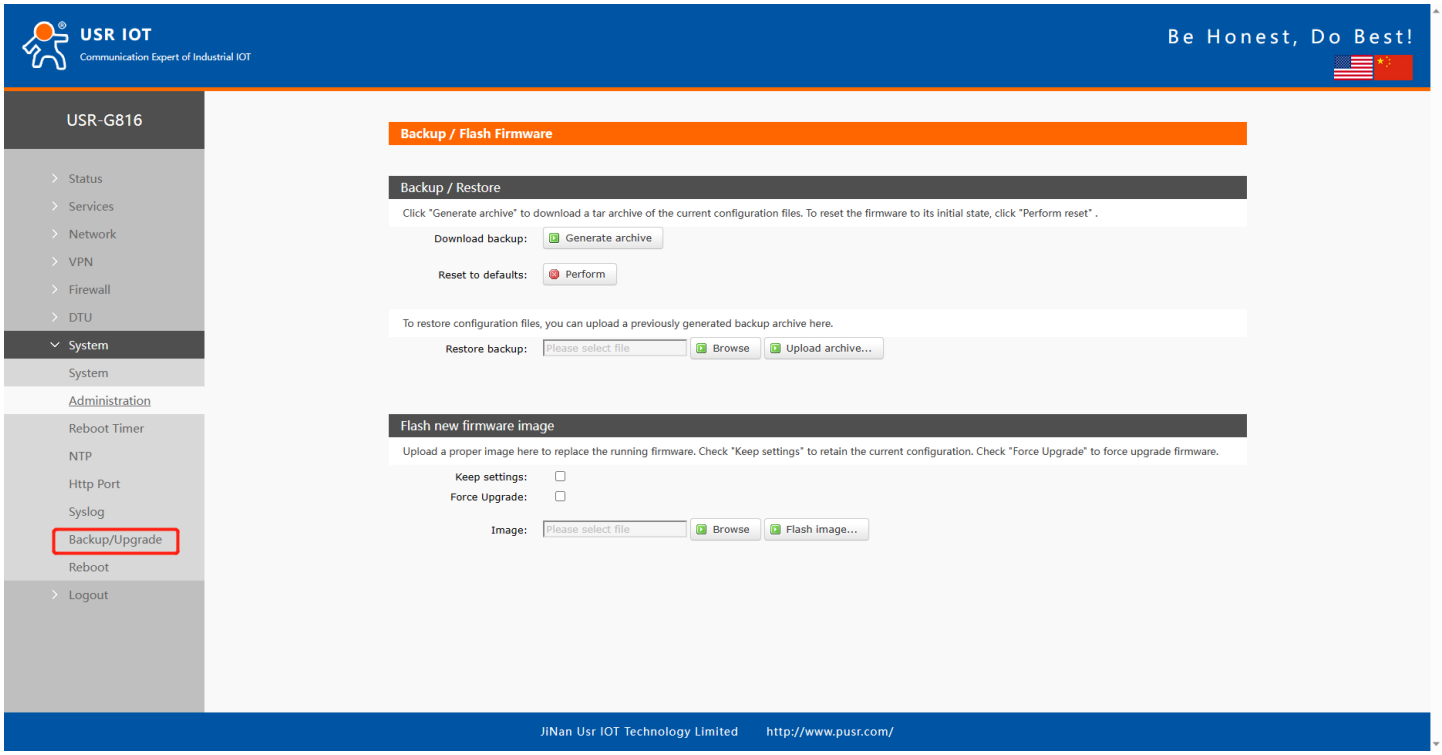

Figure 11. Backup and firmware upgrade

3.9. Reboot

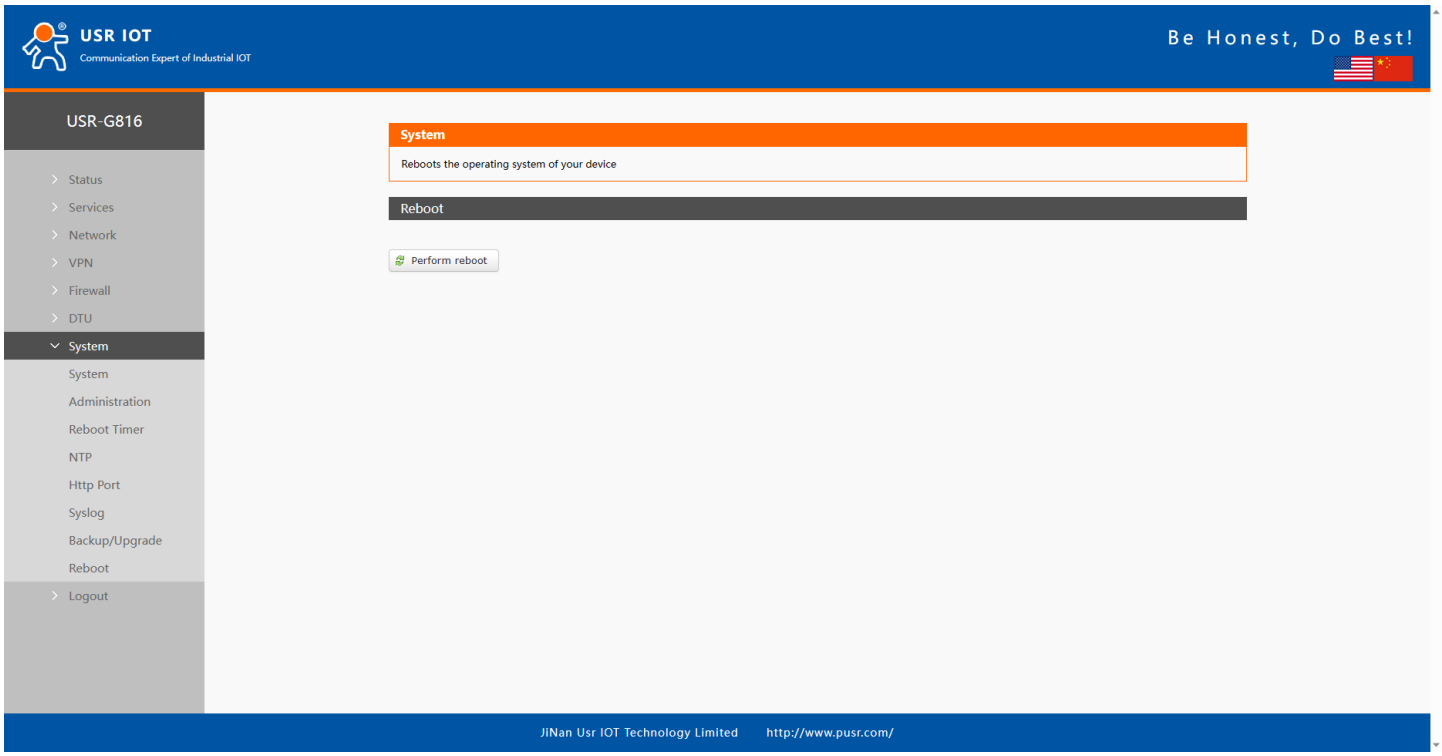

Figure 12. Reboot Function

4. Network introduction

4.1. WAN interface

On WAN interface page, there are 2 options: WAN_5G and WAN_WIRED. The detail of these 2 options will be introduced in later chapter.

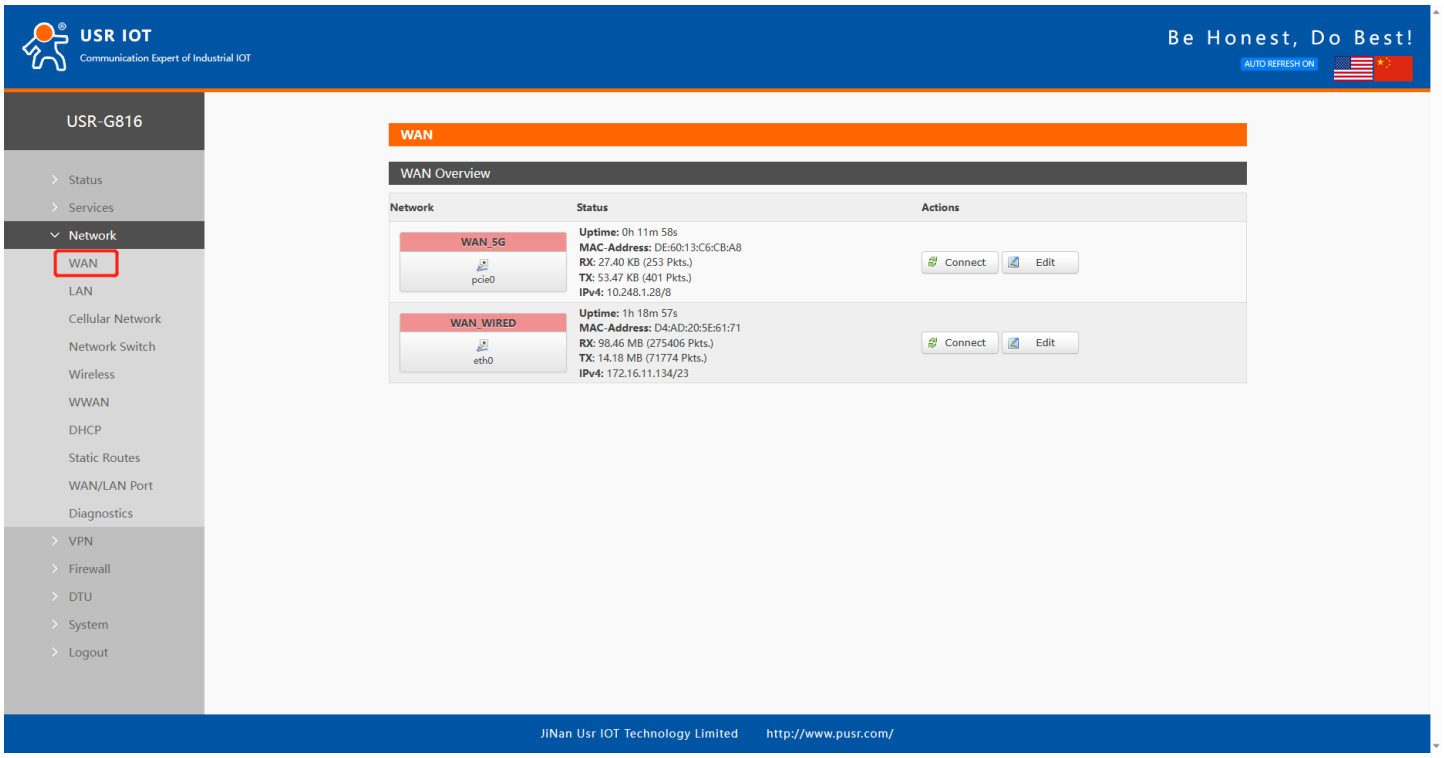

Figure 13. WAN interface

4.1.1. WAN_5G interface

This is the same with cellular network. Please check chapter 4.3.

4.1.2. WAN_WIRED interface

- DHCP Client Mode (Default)

  The IP address of USR-G816 is assigned by the upper-level router, and the upper-level router must enable the DHCP service. G816 is connected to the WAN port of the upper-level router through the LAN port.

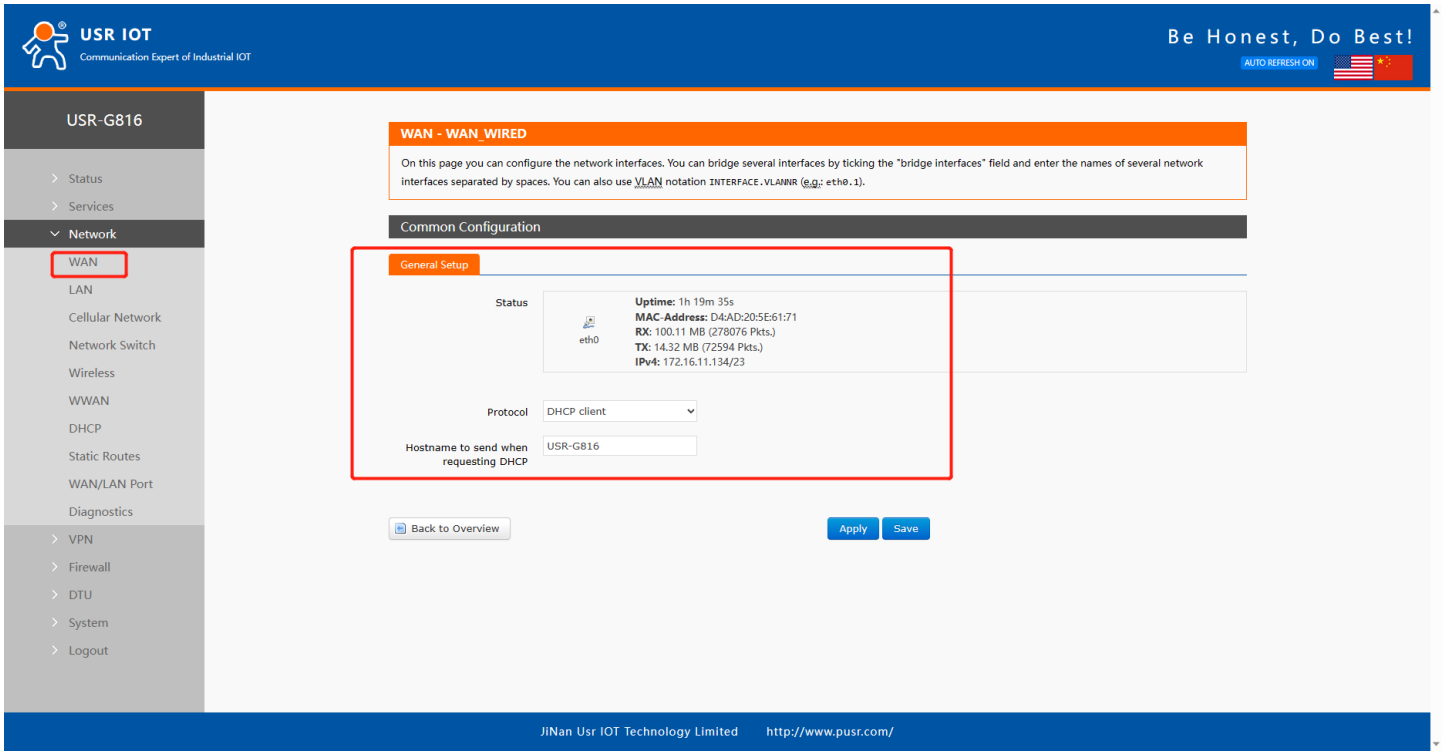

Figure 14. DHCP Client of WAN interface

- Static address Mode

  In this mode, uses can set the IP address of USR-G816.

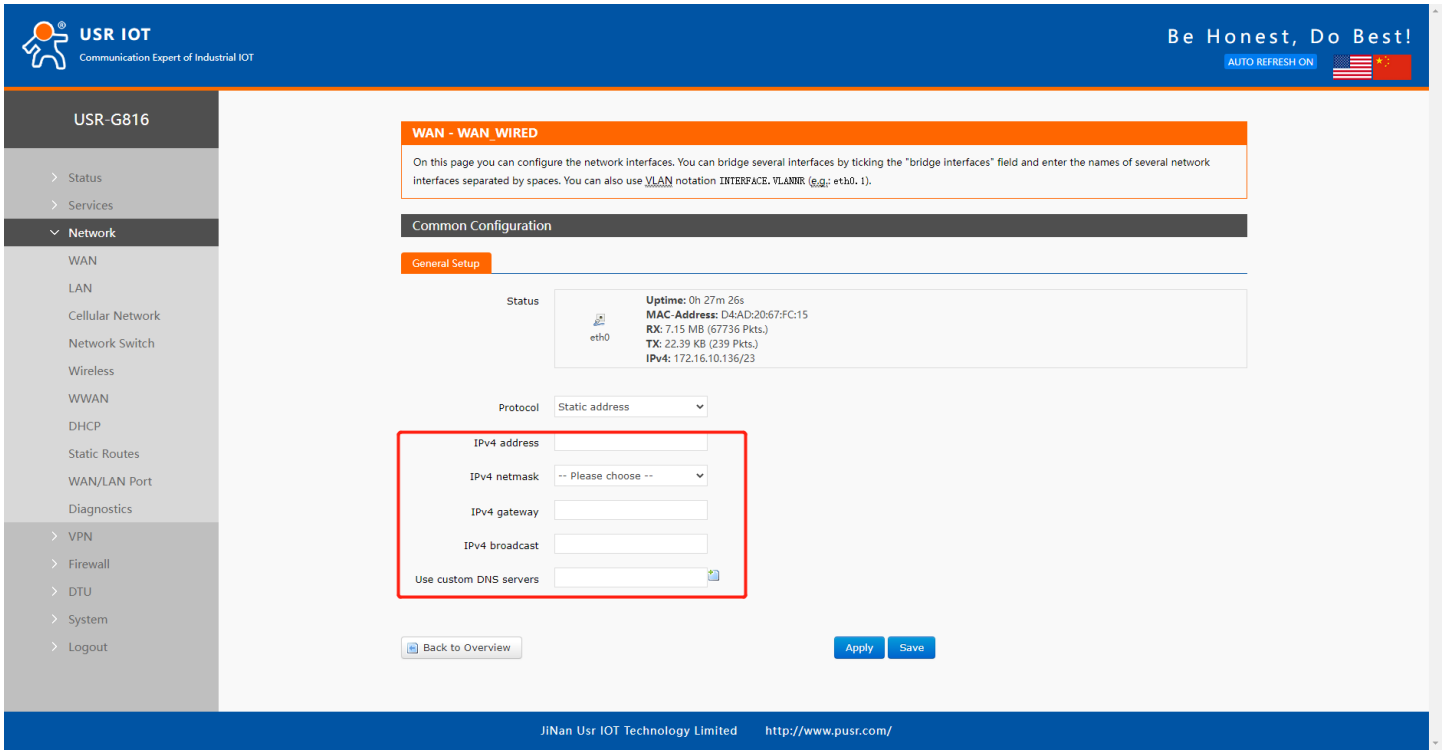

Figure 15. Static IP of WAN interface

Table 4. Detail parameters of WAN interface

Items	Description
IPv4 address	Should be on the same network segment as the LAN IP of the upper-level router.
IPv4 netmask	Users can choose the options provided by the web page or manually enter the subnet mask by themselves.
IPv4 gateway	Fill in the gateway address according to the actual network situation.
IPv4 broadcast	The broadcast address is calculated from the IP address and subnet mask.
Use custom DNS servers	User-defined.

- PPPoE Mode

  Fill in the correct username and password given by the operator.

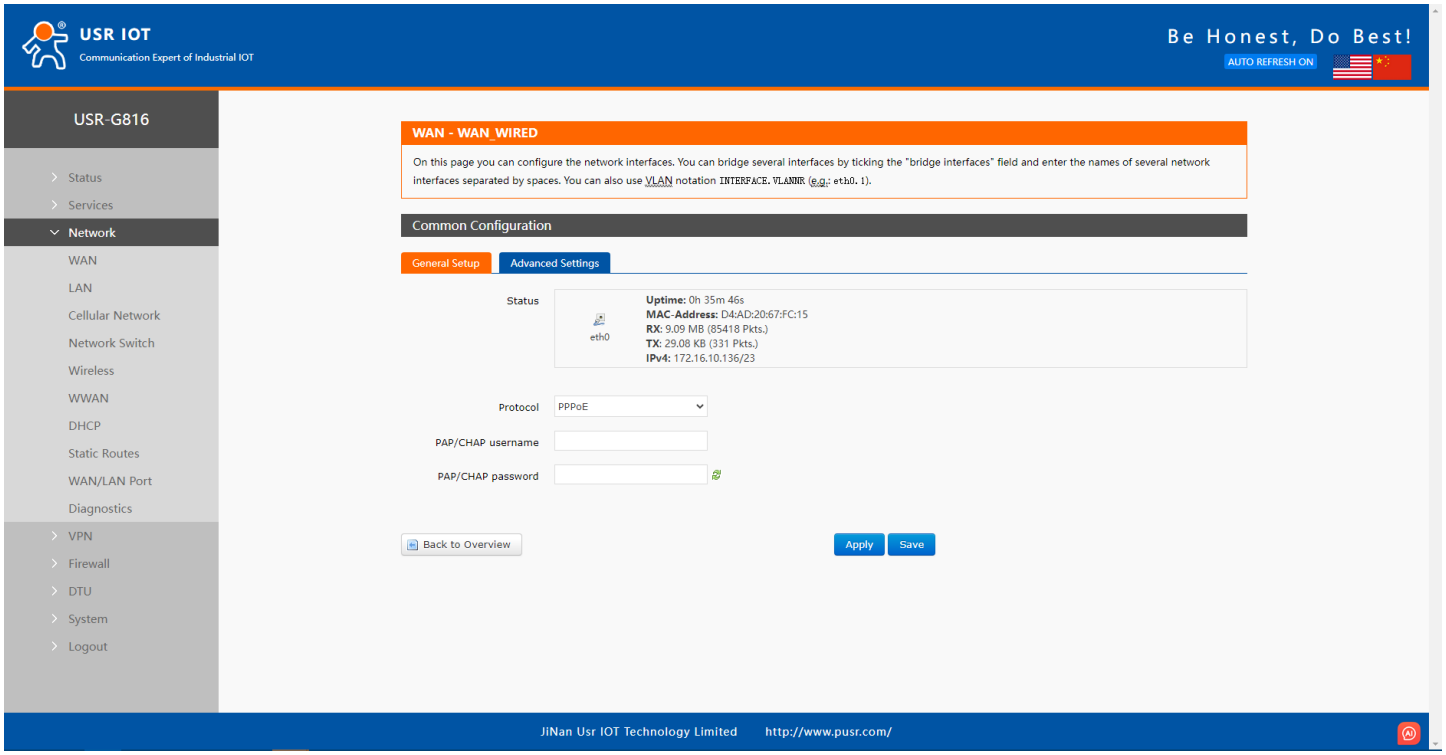

Figure 16. PPPoE Mode

4.2. LAN interface

Click the "Edit" button, the settings of the LAN port will be displayed. Users can set general settings like the IP address, gateway etc. The DHCP service of the LAN port is enabled by default, and USR-G816 will automatically assign an IP address to the device connected to the LAN port.

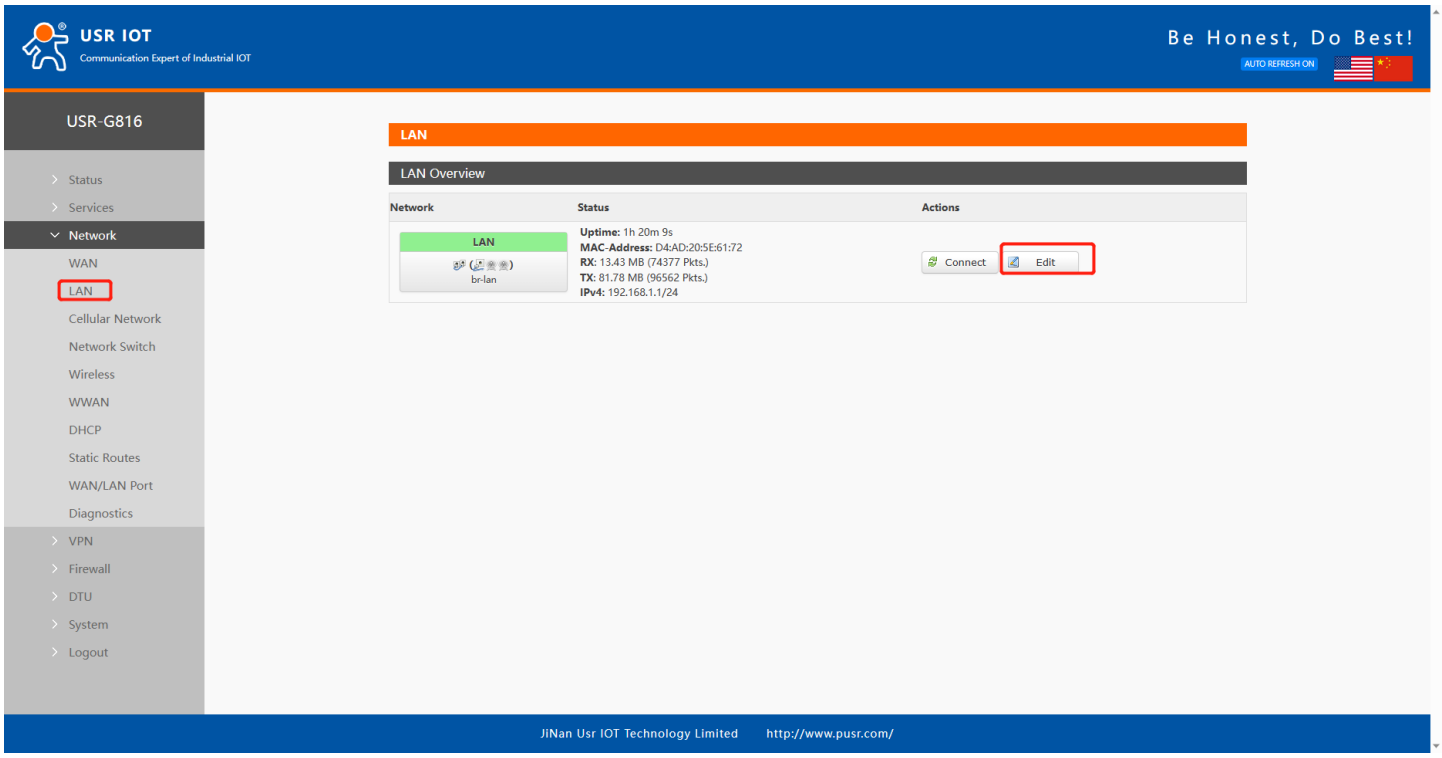

Figure 17. LAN interface

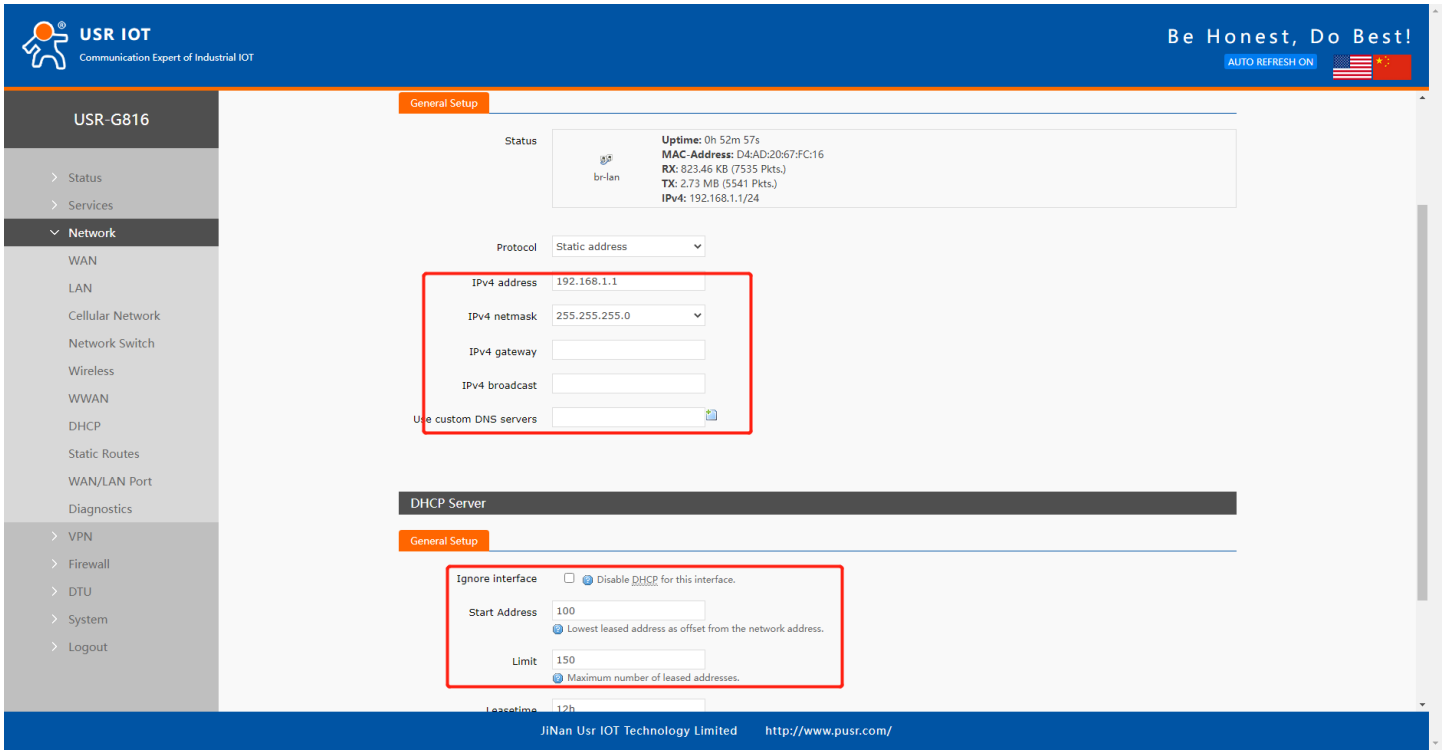

Figure 18. Settings of LAN interface

4.3. Cellular network

4.3.1. Configuration

On this page, users can set the basic parameters of the cellular network.

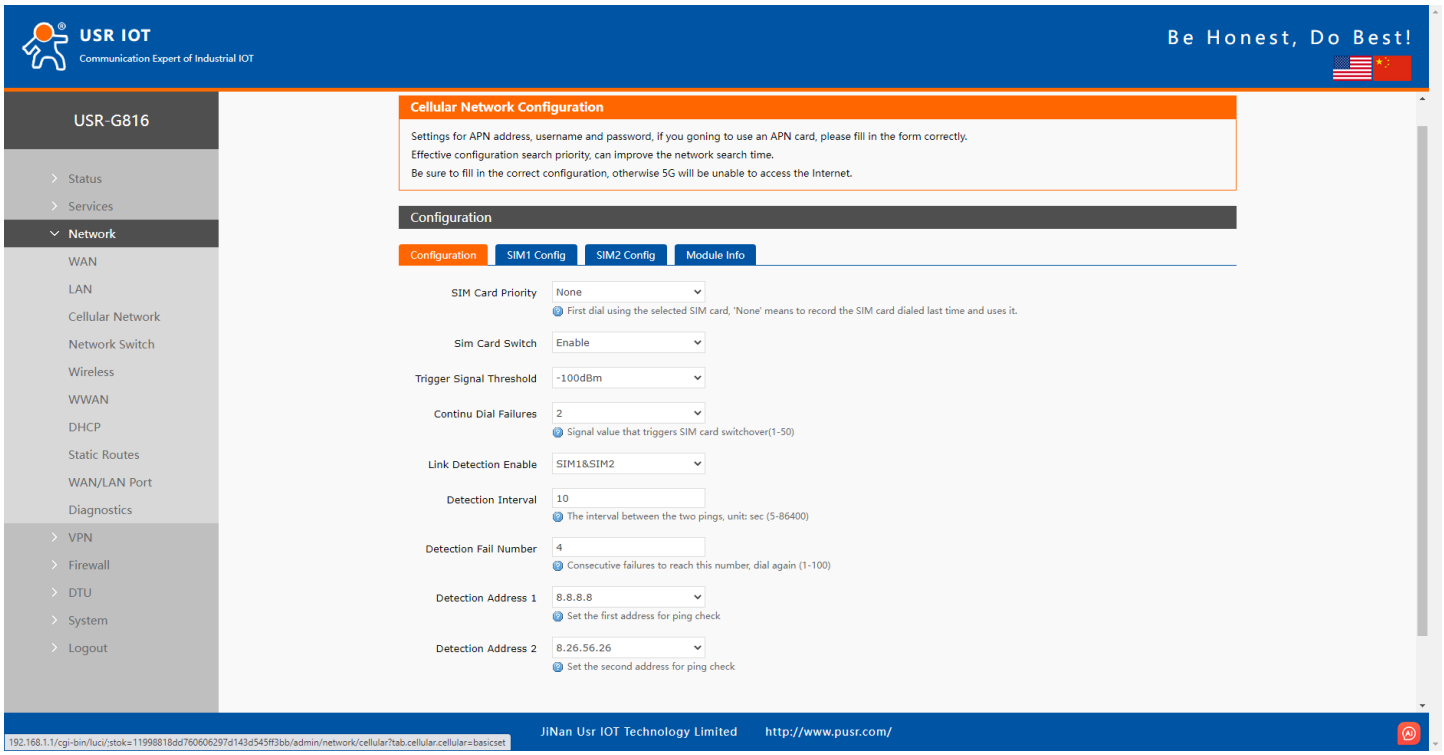

Figure 19. Basic configuration of cellular network

Table 5. Detail parameters of cellular network

Items	Description	Default
SIM Card Priority	None: Prioritize the use of the sim card used for the last dial-up. SIM1: Prioritize using SIM1 to dial up and connect to the Internet. SIM2: Prioritize using SIM2 to dial up and connect to the Internet.	None
Sim Card Switch	Enable: Enable automatic SIM switching. Disable: Disable automatic SIM switching.	Enable
Trigger Signal Threshold	If the signal value of the currently used SIM card is lower than the set value, G816 will automatically switch to another SIM card.	-100dBm
Continue Dial Failures	When the number of dialing failures reaches this value, switch to another SIM card and dial again.	2
Link Detection Enable (Ping detection)	OFF: Disable the Ping detection. SIM1: When using SIM1, enable the PING detection. SIM2: When using SIM2, enable the PING detection. SIM1&SIM2: Enable the PING detection Whether using SIM1 or SIM2.	SIM1&SIM2
Detection Interval	Interval of PING detection. Unit: s	10
Detection Fail Number	If the number of PING attempts exceeds this value, it will redial.	4
Detection Address 1	The main destination host of PING detection.	8.8.8.8
Detection Address 2	The alternate destination host of PING detection.	8.26.56.26

4.3.2. SIM1/SIM2 configuration

The settings of SIM1 can be configured on this page. And the SIM2 configuration is the same with SIM1.

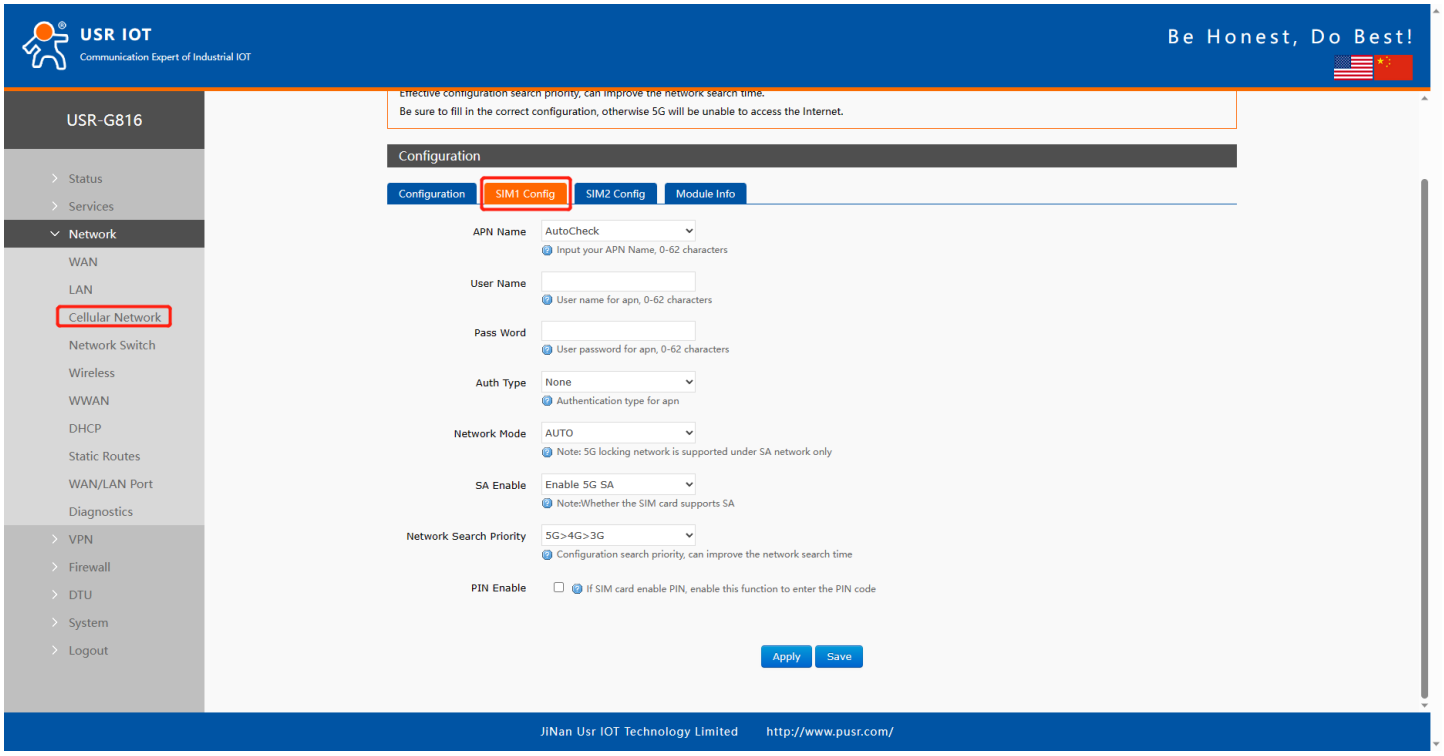

Figure 20. SIM card configuration

Table 6. Parameters description of SIM card

Items	Description	Default
APN Name	The SIM card operator provides this parameter.	Auto check
Username	The SIM card operator provides this parameter.	None
Password	The SIM card operator provides this parameter.	None
Auth Type	The SIM card operator provides this parameter.	None
PDP Type	PDP protocol context type.	IPv4
Network Mode	AUTO: According to the on-site network environment, it can automatically select to stay on the network 5G/4G/3G. 3G: Lock the 3G network, if there is no 3G network on site, it will not stay on the network. 4G: Lock the 3G network, if there is no 4G network on site, it will not stay on the network. 5G(Only SA): If the SIM card supports SA network, locking 5G network is valid.	AUTO
SA Enable	If the sim card supports SA network, enable 5G SA. Otherwise, disable the 5G SA.	Enable 5G SA
Network	Network priority selection.	5G>4G>3G

Search Priority		
PIN Enable	If the SIM card has enabled the PIN function, the USR-G816 also needs to enable this function also.	None

4.3.3. Module information

On this page, user can check some information about the SIM card, like the signal strength, the ICCID, network type etc. The detailed information is shown like the following picture.

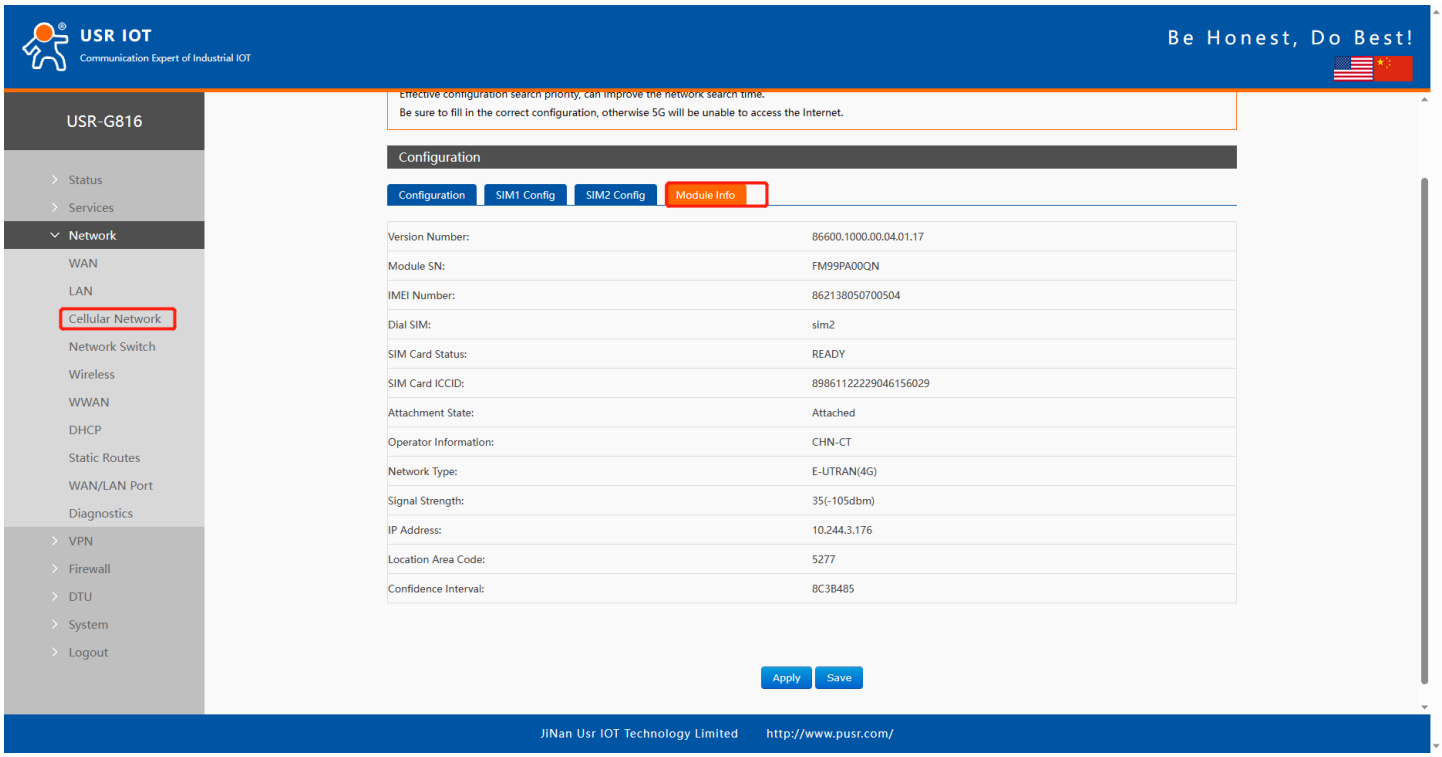

Figure 21. Information of cellular network

4.4. Network switch

In this interface, users can choose network priority. The default is to use the WAN port network first.

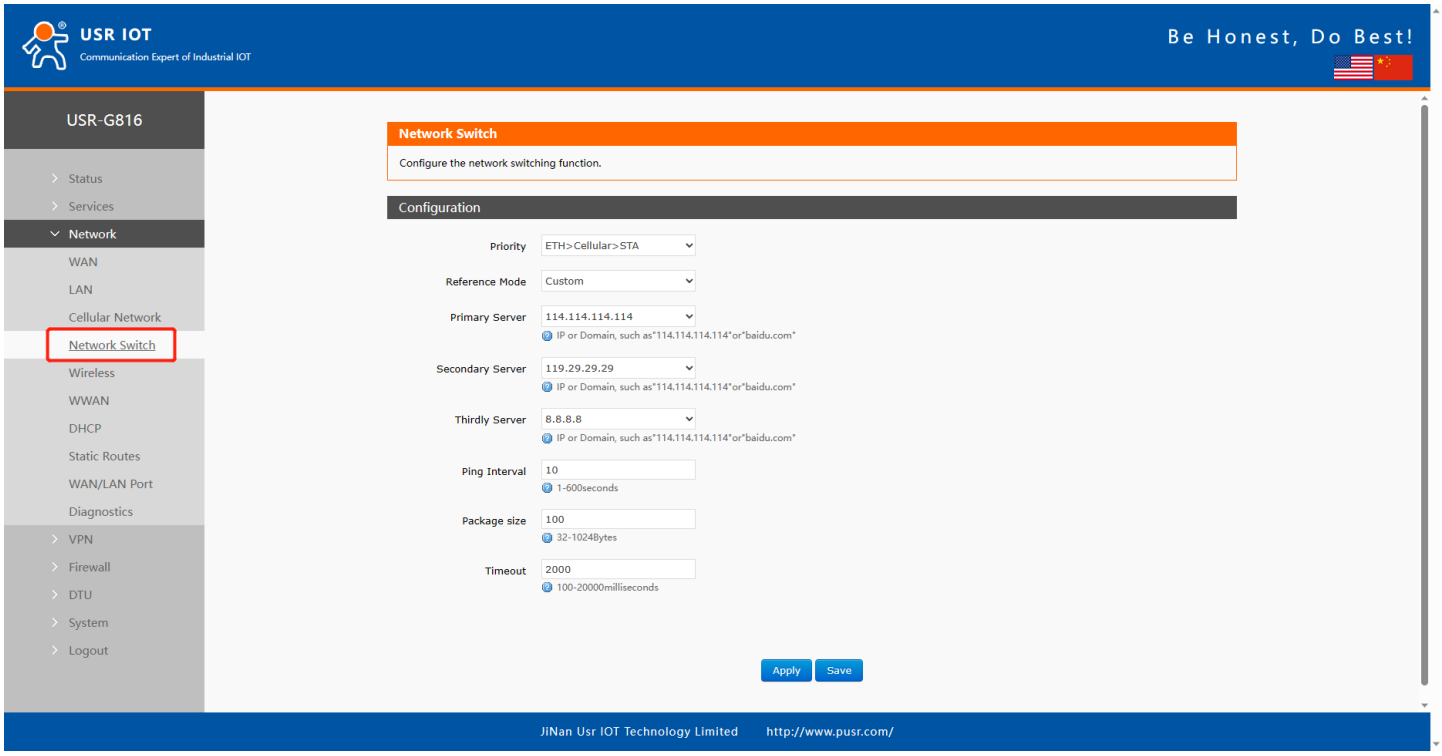

Figure 22. Network switch page

4.5. Wireless (Wi-Fi)

4.5.1. Wi-Fi settings of 2.4 & 5.8G

Users can set Wi-Fi related information on this page.

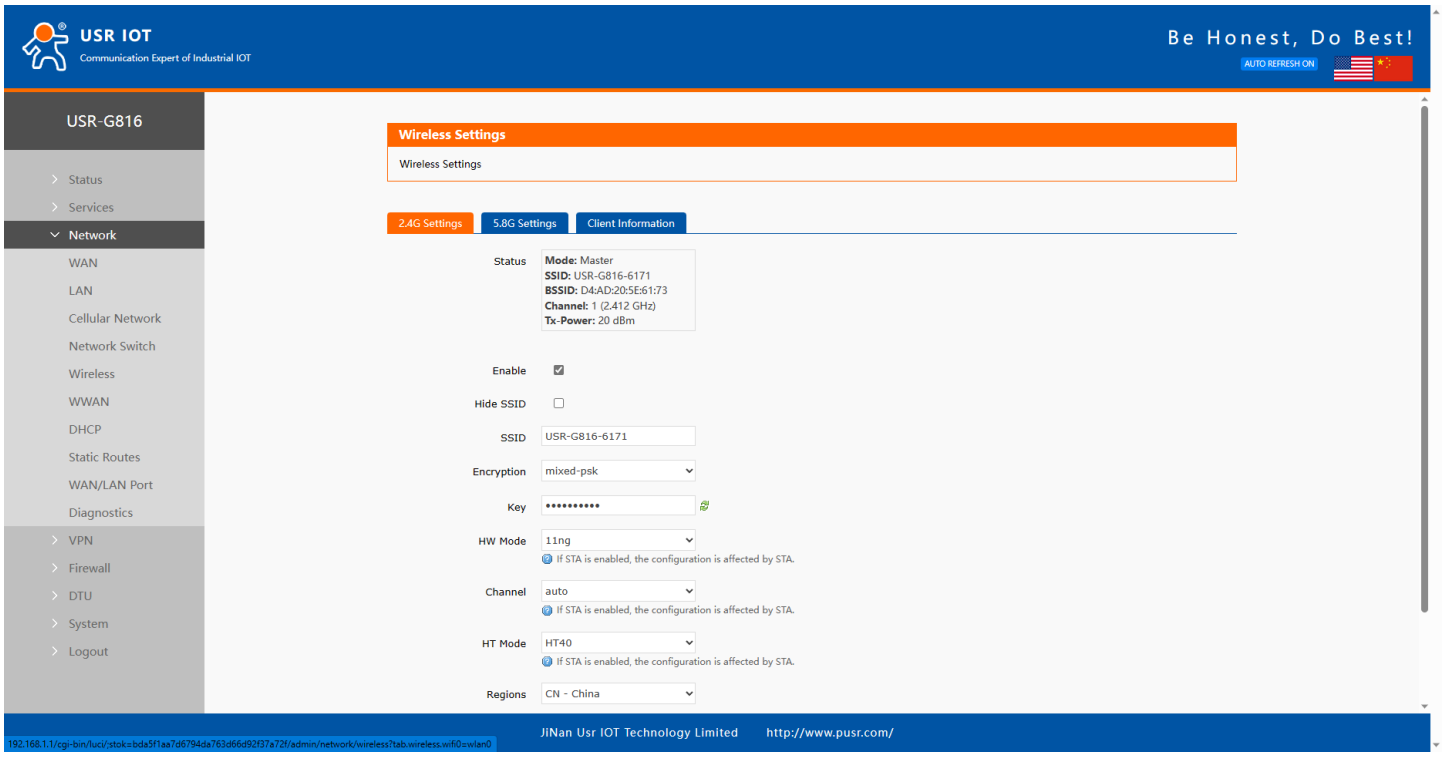

Figure 23. 2.4G & 5.8G Wi-Fi settings

Table 7. Parameters description of Wi-Fi interface

Items	Description	Default
Enable	To choose whether to enable the Wi-Fi function.	Enable
Hide SSID	To choose whether to hide the SSID. If the SSID is hidden, the user cannot search for the Wi-Fi name on the mobile phone or PC. Users can connect to Wi-Fi by manually entering the SSID.	Disable
SSID	Wi-Fi name, users can modify as needed.	USR-G816-xxxx/_5.8G
Encryption	To choose Wi-Fi encryption method.	Mixed-psk
Key	The password of Wi-Fi.	www.pusr.com
HW Mode	To choose Wi-Fi standard.	11ng
Channel	To choose Wi-Fi channel.	auto
HT Mode	To choose high throughput.	HT40
Regions	This option is for 5.8G Wi-Fi.	00-World

4.5.2. Client information

On this page, the users can view the device information connected to the USR-G816 through Wi-Fi.

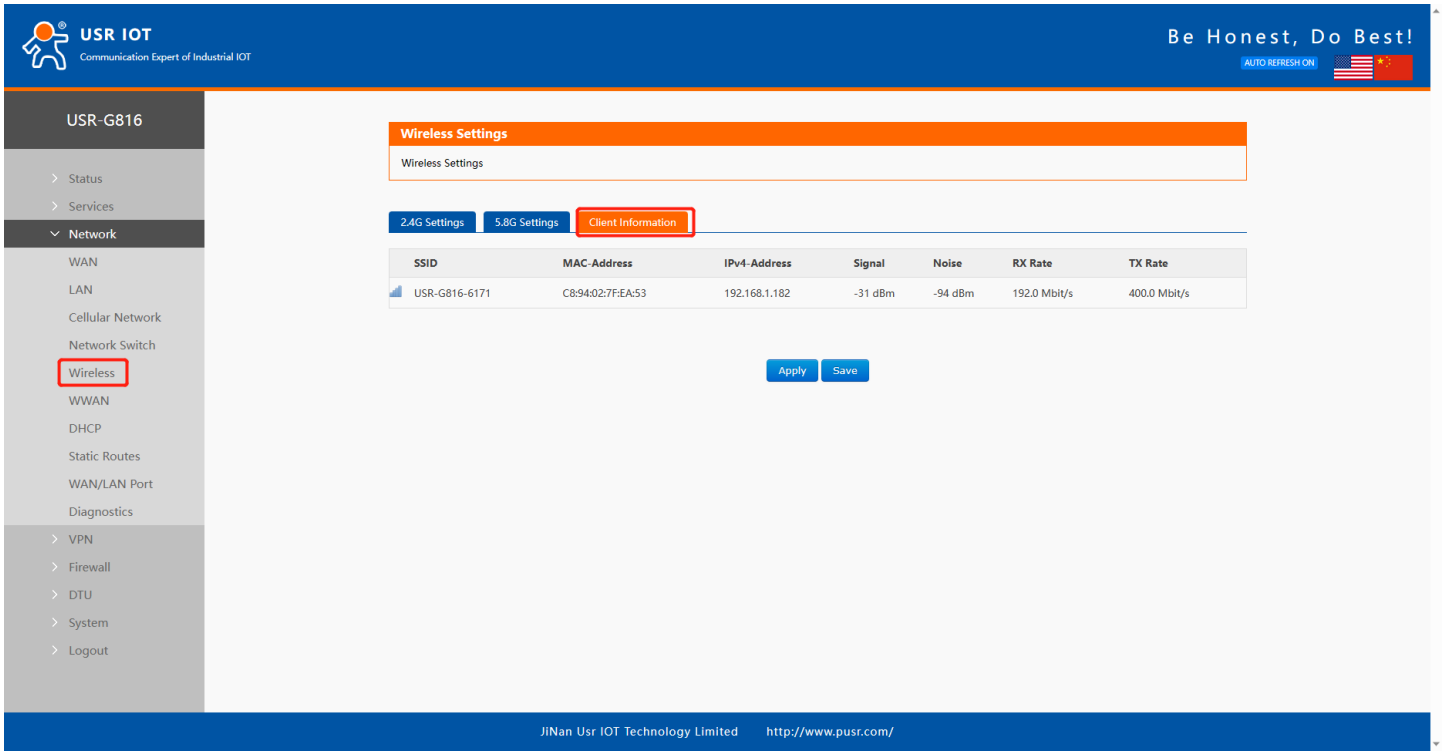

Figure 24. Client information of Wi-Fi

4.6. WWAN(STA)

4.6.1. Basic settings

On this page, users can enable the STA function. Users can choose 2.4G Wi-Fi or 5.8G Wi-Fi. The default setting is OFF.

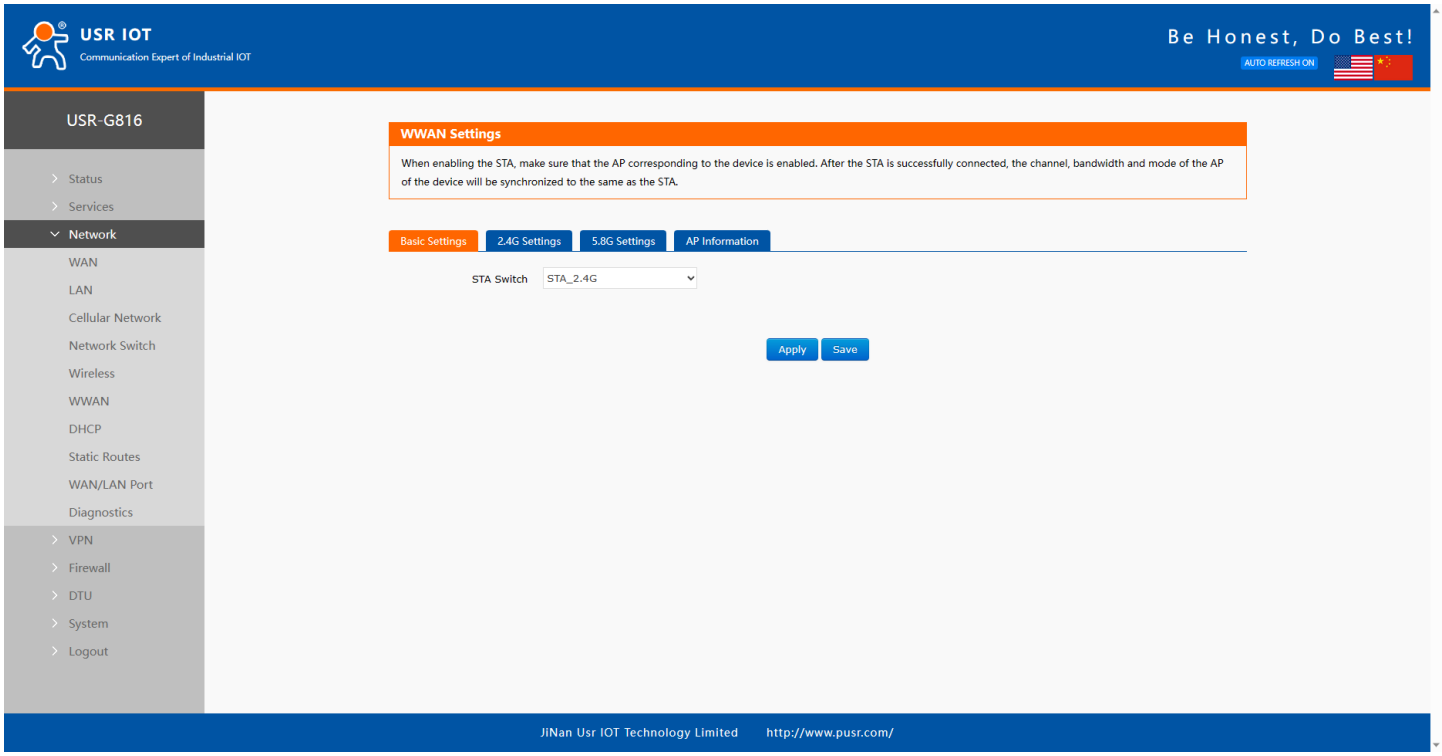

Figure 25. Choose 2.4G or 5.8G Wi-Fi

4.6.2. 2.4G / 5.8G settings

The steps to connect to the upper-level routers:

1>Click “Scan” button,

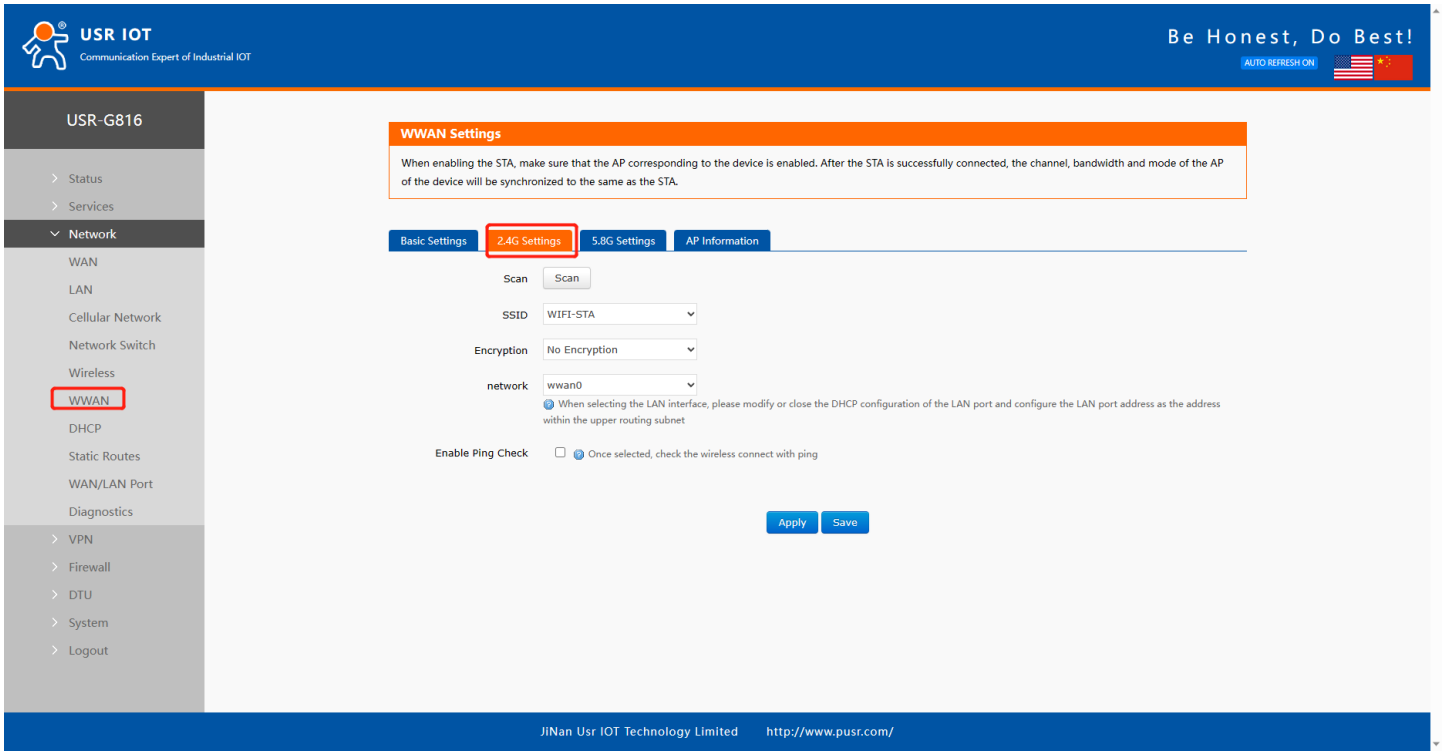

Figure 26. Scan AP information

2> Click the drop-down button of SSID, the available Wi-Fi network is displayed. Users can select the Wi-Fi network or enter the Wi-Fi name to connect to.

3>Enter the password of the Wi-Fi network if needed.

4>Choose network type:

Wwan0: Relay mode.

LAN: Bridge mode, the DHCP service should be closed, and the LAN IP should be in the same segment of upper-level router.

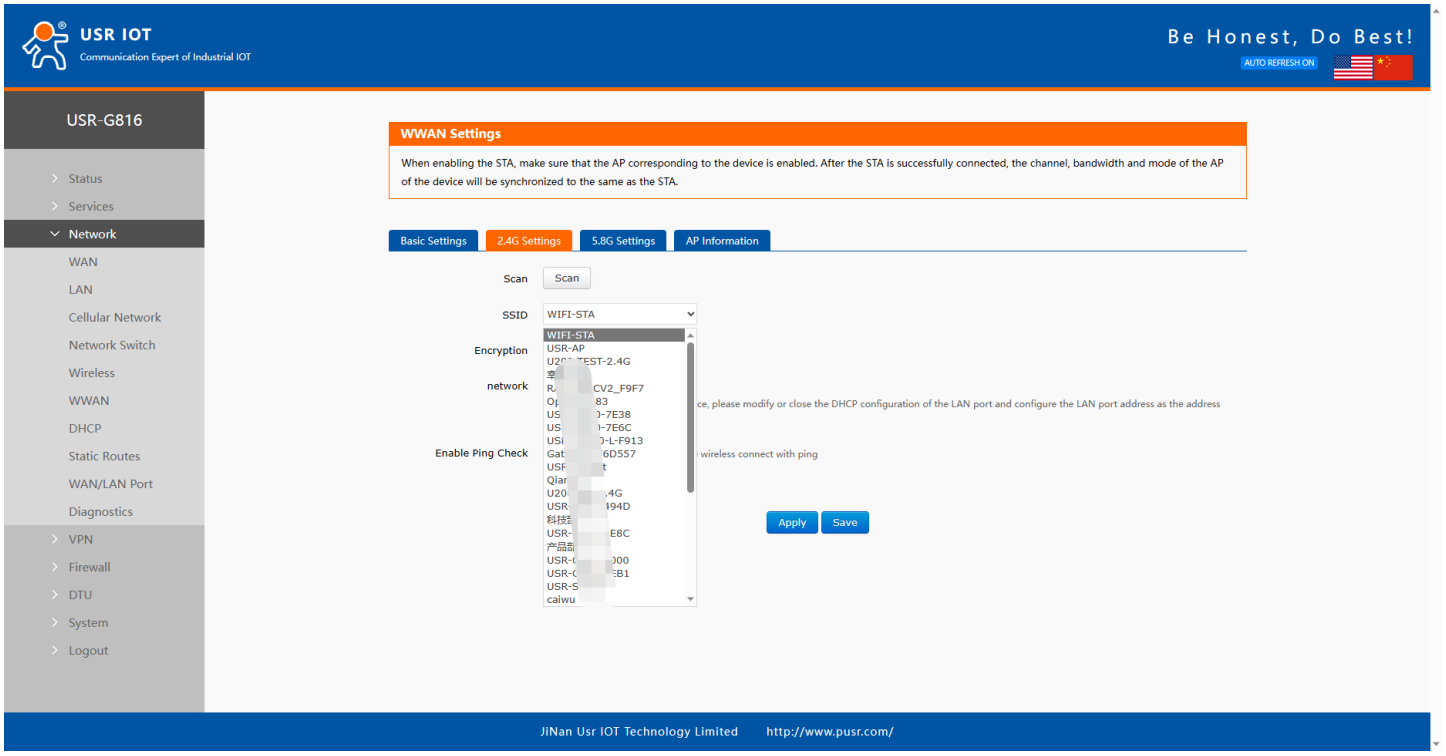

Figure 27. Searched AP list

4.6.3. AP information

If the USR-G816 connect to upper-level Wi-Fi successfully, the information will be displayed in this page.

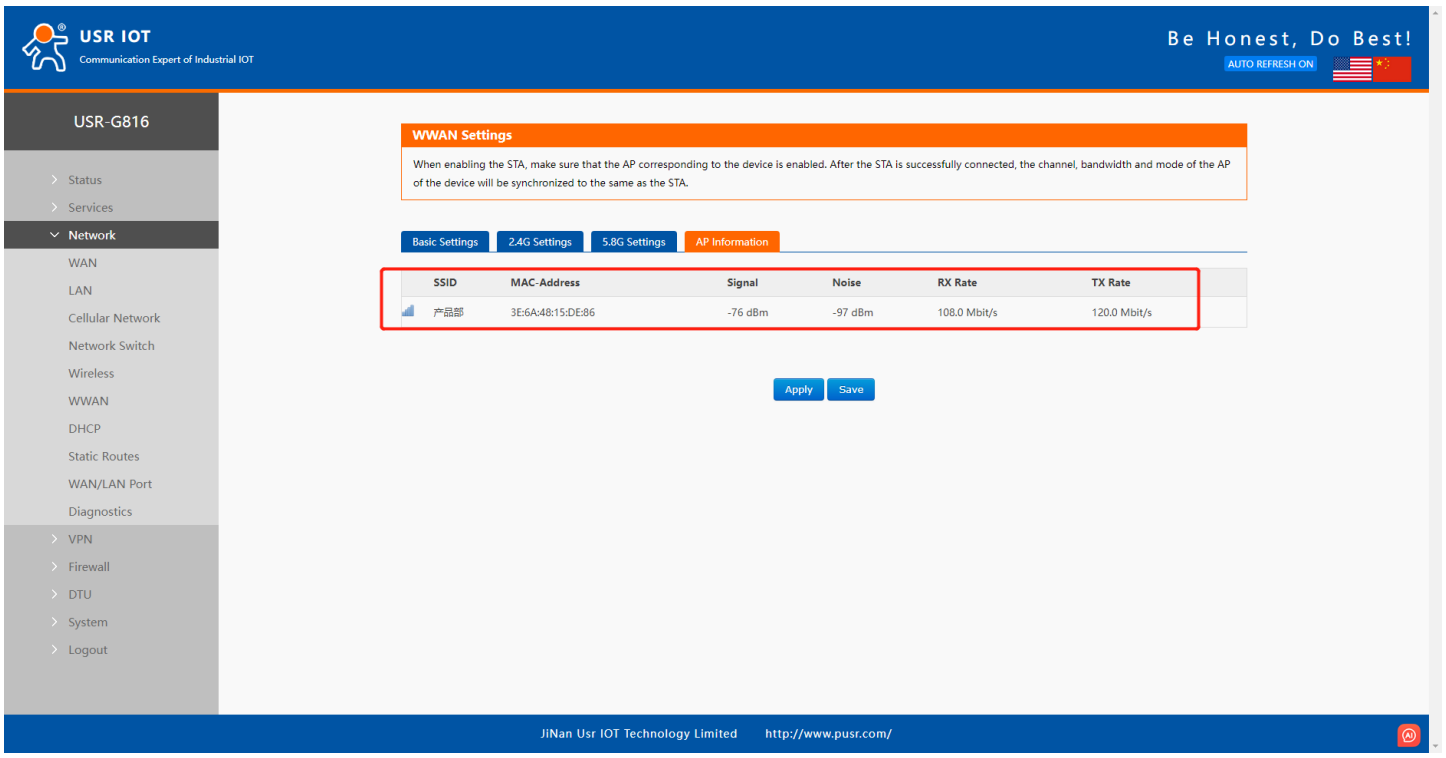

Figure 28.

4.7. DHCP introduction

On this page, users can assign static IP addresses to specific network devices and define device hostnames.

Note: Up to 10 rules can be added.

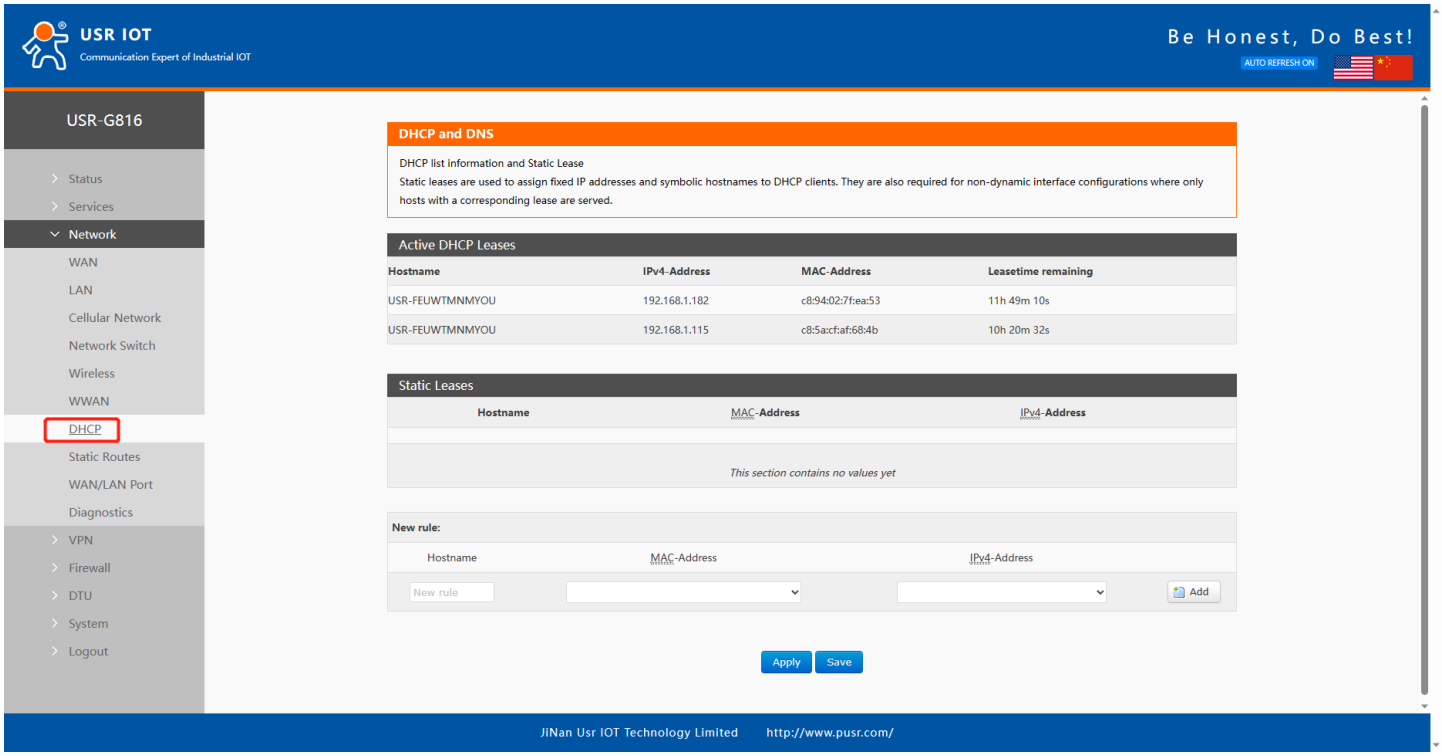

Figure 29. DHCP rules

4.8. Static routes

4.8.1. Static routing adding

Static routing describes the routing rules for packets on Ethernet.

Note: Up to 100 static router rules can be added.

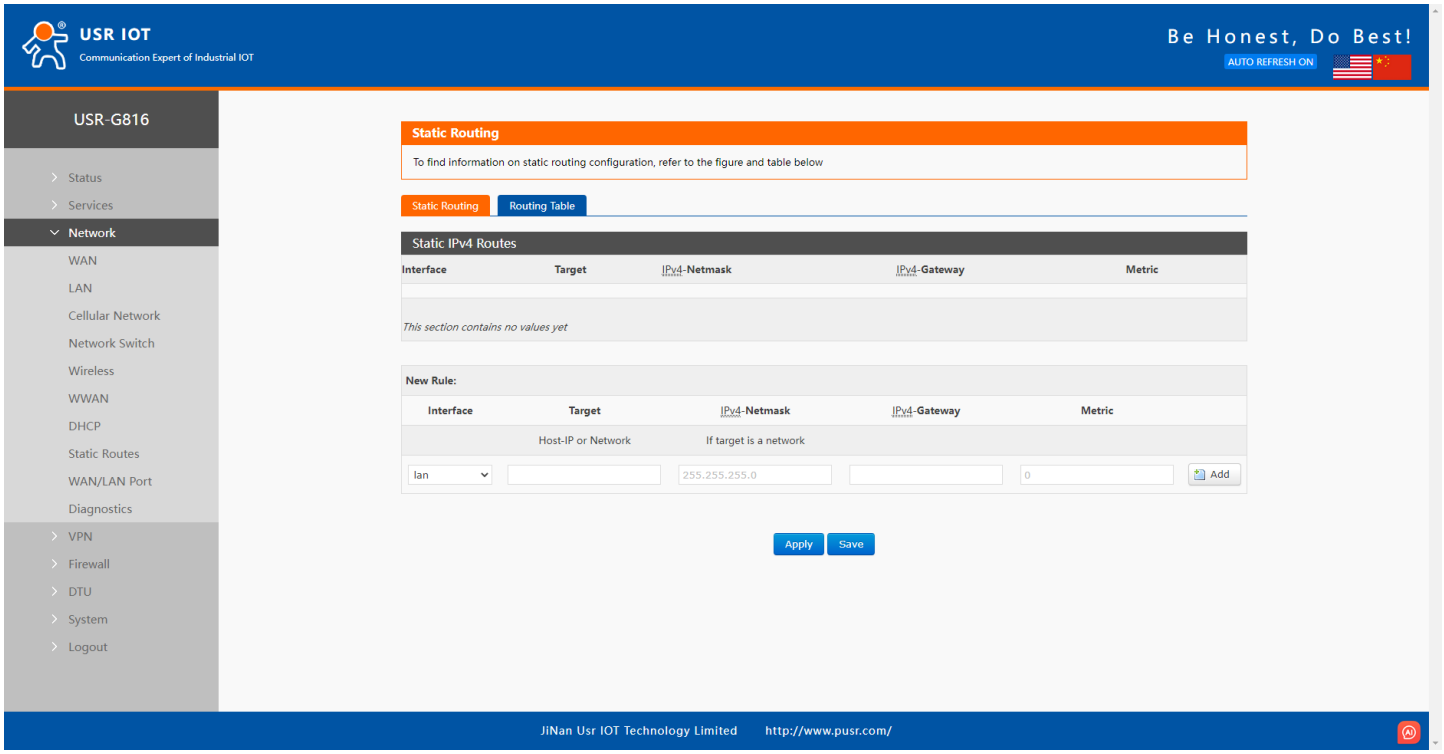

Figure 30. Static routing rule

Table 8. Parameters description of static routing

Items	Description	Default
Interface	Network interface of the target network.	
Target	Destination network address.	LAN
IPv4 Netmask	A netmask is used to divide an IP address into sub-networks (subnets). Combined, the 'Netmask' and 'Target' values define the exact destination network or IP address to which this route applies.	None
IPv4 Gateway	A gateway can be any machine in a network that is capable of serving as an access point to another network. Traffic that matches this route will be directed over the IP address specified in this field.	None
Metric	The metric value acts as a measurement of priority. If a packet about to be routed matches two or more rules, the one with the lower metric is applied.	None

4.8.2. Routing table

All routing rules are displayed on routing table page.

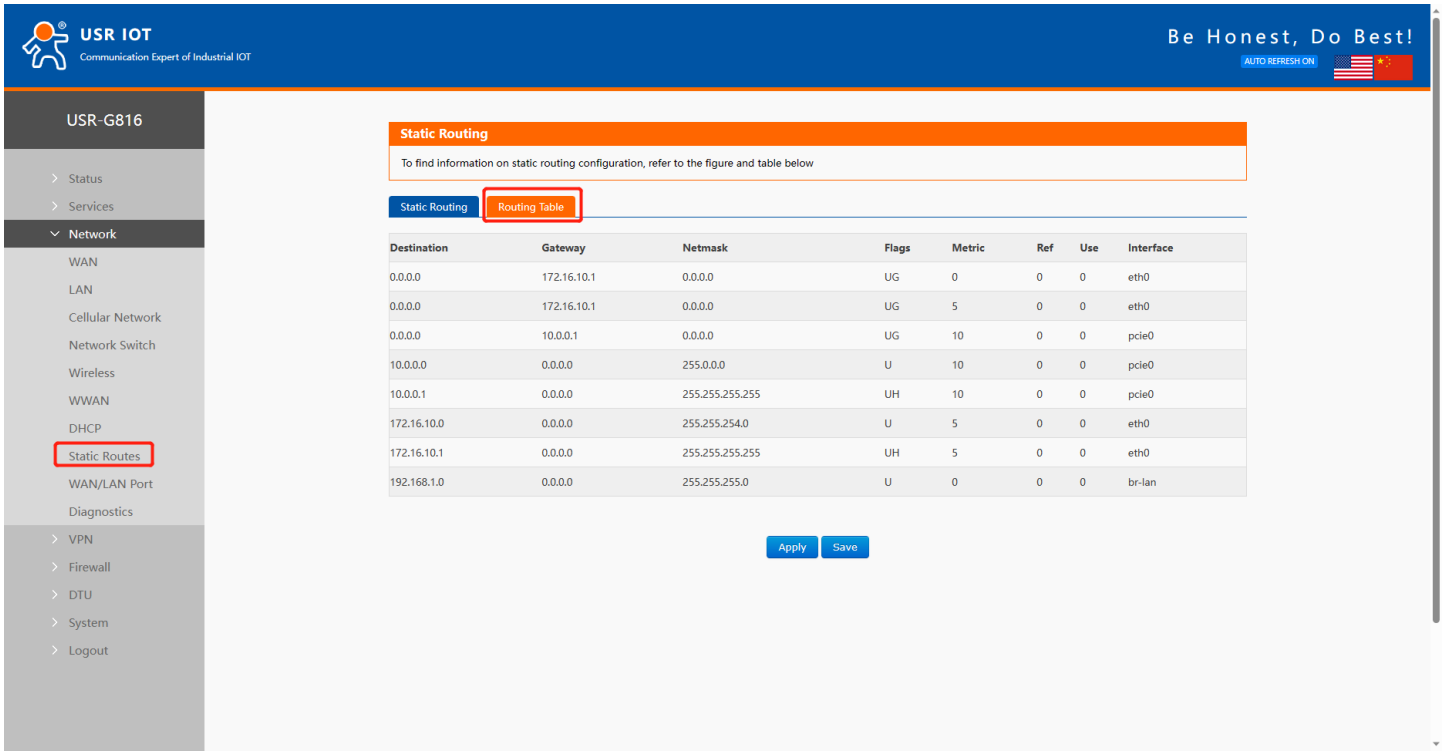

Figure 31. Routing table checking

4.9. WAN/LAN port switching

USR-G816 is equipped with 1* WAN/LAN port which is WAN port by default. And this port can be set to LAN port on this page.

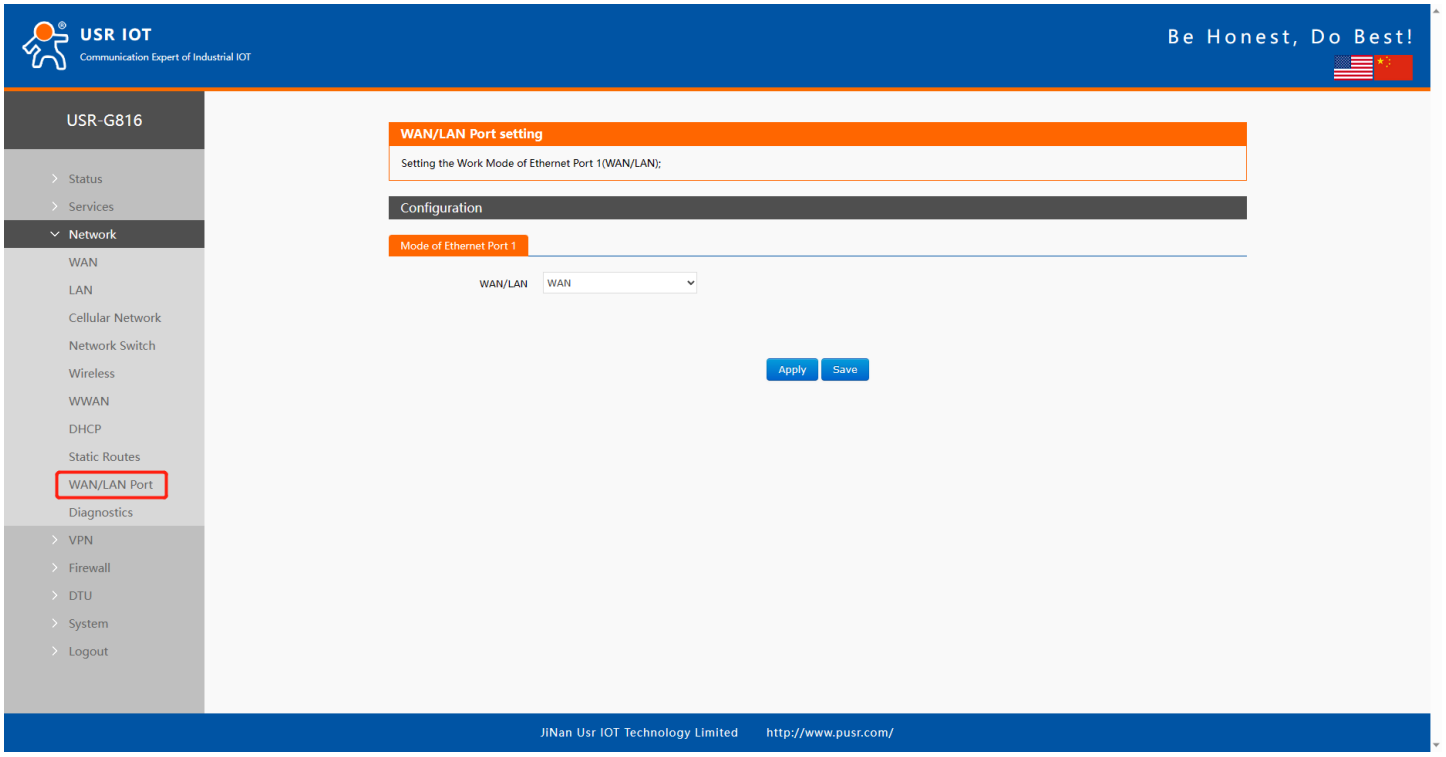

Figure 32. WAN/LAN switching setting

4.10. Network diagnostics

USR-G816 provides online diagnostic functions, including Ping tools, routing analysis tools, and DNS viewing tools.

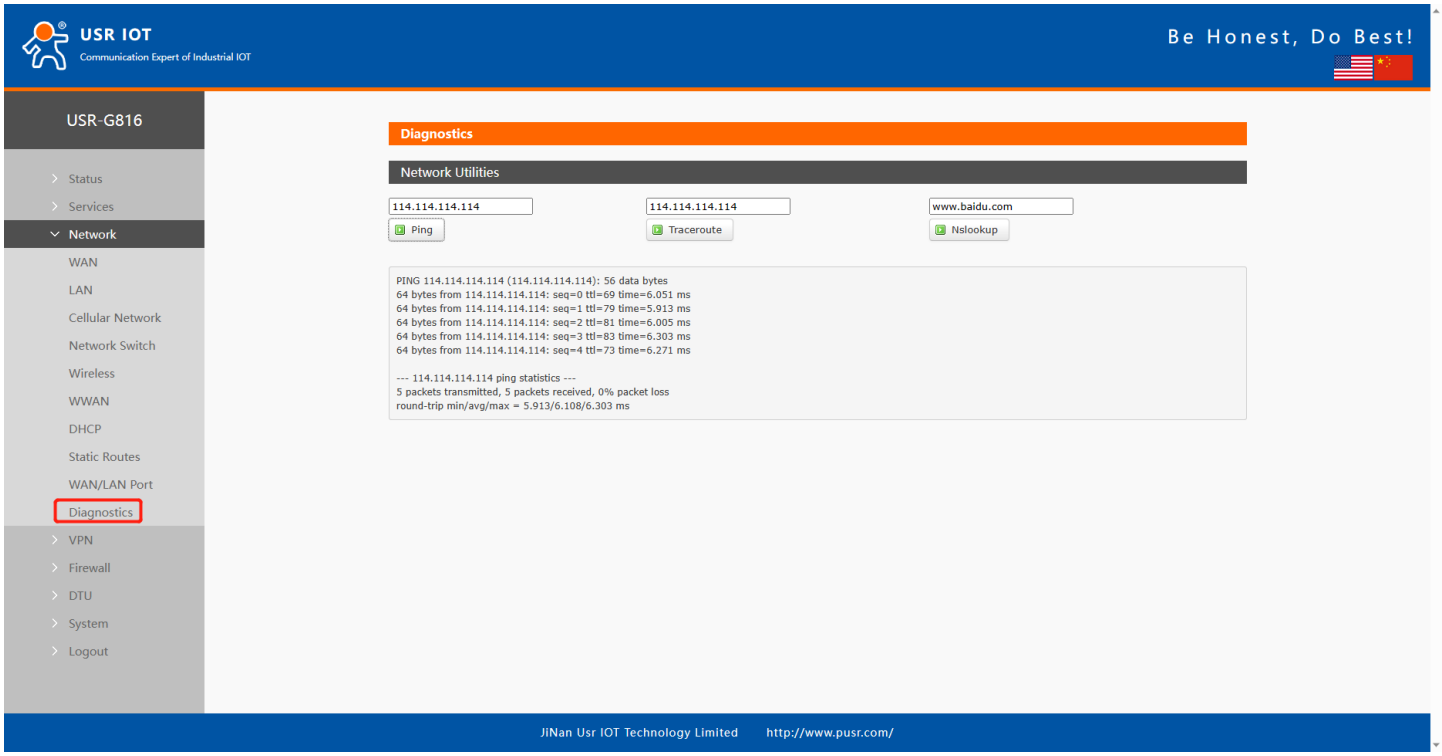

Figure 33. Network diagnostics

Table 9. Description of diagnostic types

Items	Description	Default value
Ping	Users can ping a specific IP address directly on the router side.	8.8.8.8
Traceroute	Routing analysis tool, which can obtain the routing path passed when accessing an address.	8.8.8.8
Nslookup	A DNS viewing tool that can resolve domain names to IP addresses.	www.google.com

5. VPN

5.1. PPTP Client

Point-to-Point Tunneling Protocol (PPTP) is a type of VPN protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.

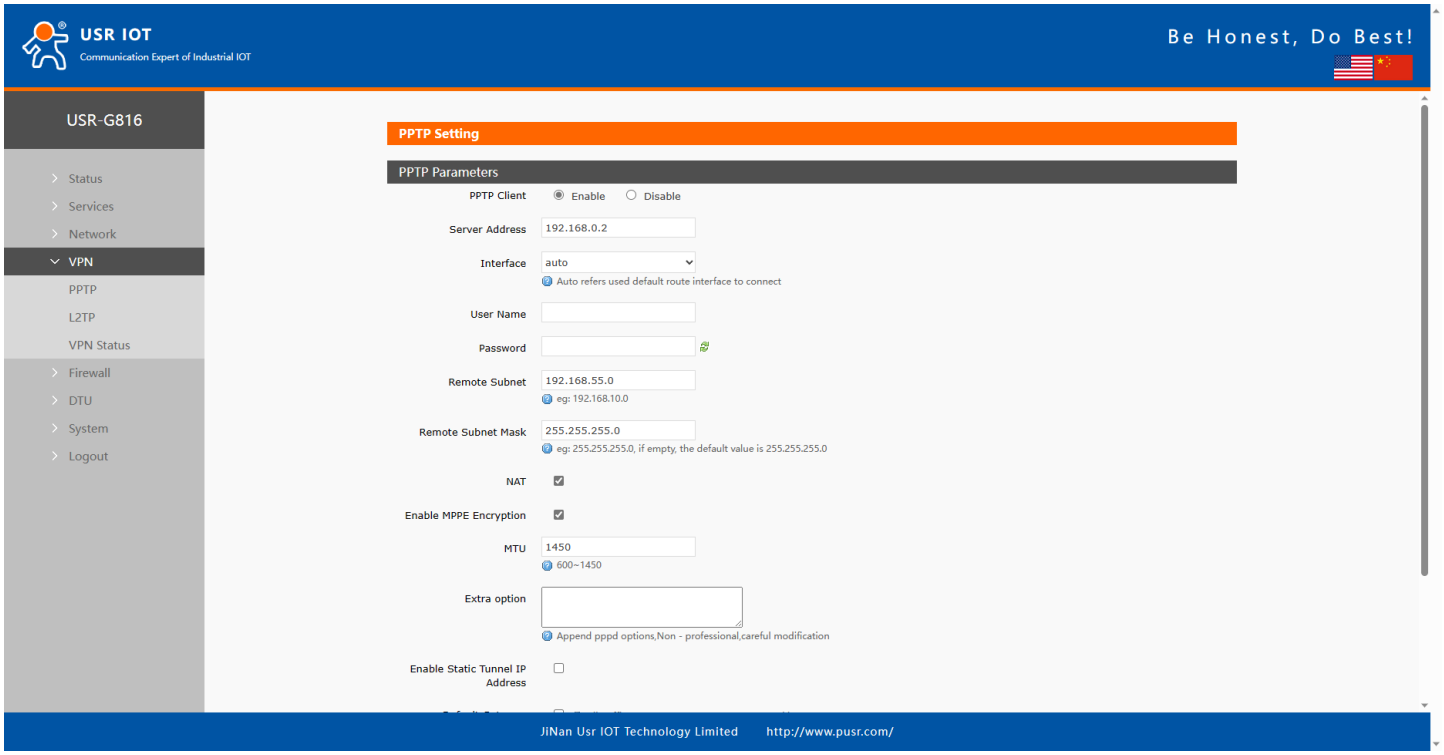

Figure 34. PPTP VPN settings

Table 10. Parameter details of PPTP VPN

Items	Description	Default
PPTP Client	Turns the PPTP client on or off.	Off
Server Address	Set PPTP server IP or domain name.	192.168.0.2
Interface	Select the interface according to different networking methods.	auto
Username /Password	Username used for authentication to the PPTP server. They are provided by the VPN server.	None
Remote Subnet	These are the IPv4 client-side networks that will be routed to this client specifically using route, so that a site-to-site VPN can be established.	192.168.55.0
Remote Subnet Mask	Subnet mask of remote client network.	255.255.255.0
NAT	Network address translation. It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet.	Enabled
Enable MPPE Encryption	This option must be consistent with the VPN server.	Enabled
MTU	The MTU value of the PPTP channel must be consistent with the	1450

	VPN server.	
Extra option	Append pppd parameters, non-professionals, prohibited operation.	None
Enable Static Tunnel IP Address	Users need to enter static IP manually if this option is enabled.	Disabled
Default Gateway	Force all client generated traffic through the tunnel, except WAN protocol is PPPOE.	Disabled
Enable Ping	The USR-G816 will reconnect to PPTP server if the PING command fails more than preset times.	Disabled
Ping Period	The time interval between two ping commands.	10
Ping times	Number of ping attempts.	3

5.2. L2TP Client

L2TP, also called Layer 2 Tunneling Protocol, is a tunneling protocol used to create VPN connections. Its main purpose is to securely transport data over public networks.

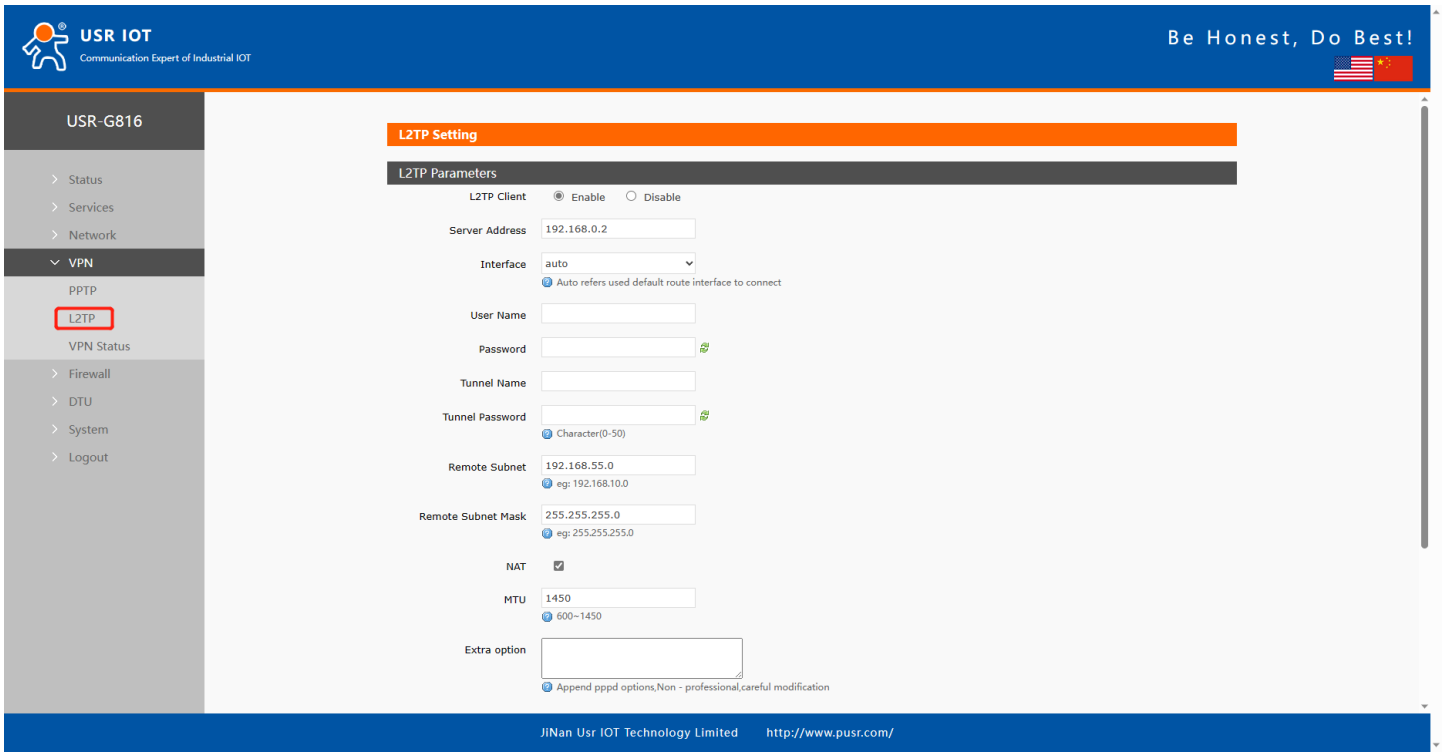

Figure 35. L2TP VPN settings

Table 11. Parameter details of L2TP VPN

Items	Description	Default

L2TP Client	Turns the L2TP client on or off.	Off
Server Address	Set L2TP server IP or domain name.	192.168.0.2
Interface	Select the interface according to different networking methods.	auto
Username/ Password	Username used for authentication to the PPTP server. They are provided by the VPN server.	192.168.55.0
Tunnel Name	The name of L2TP tunnel.	None
Tunnel Password	The password of L2TP tunnel.	None
Remote Subnet	These are the IPv4 client-side networks that will be routed to this client specifically using route, so that a site-to-site VPN can be established.	192.168.55.0
Remote Subnet Mask	Subnet mask of remote client network.	255.255.255.0
NAT	Network address translation. It's a way to map multiple private addresses inside a local network to a public IP address before transferring the information to the internet.	Enabled
MTU	The MTU value of the PPTP channel must be consistent with the VPN server.	1450
Extra Option	Append pppd parameters, non-professionals, prohibited operation.	None
Enable Static Tunnel IP Address	Users need to enter static IP manually if this option is enabled.	Disabled
Default Gateway	Force all client generated traffic through the tunnel, except WAN protocol is PPPOE.	Disabled
Enable Ping	The USR-G816 will reconnect to PPTP server if the PING command fails more than preset times.	Disabled
Ping Period	The time interval between two ping commands.	10
Ping times	Number of ping attempts.	3

5.3. OpenVPN

In OpenVPN mode, the USR-G816 support 3 OpenVPN clients and 1 OpenVPN server. This means USR-G816 can connect to 3 OpenVPN servers simultaneously.

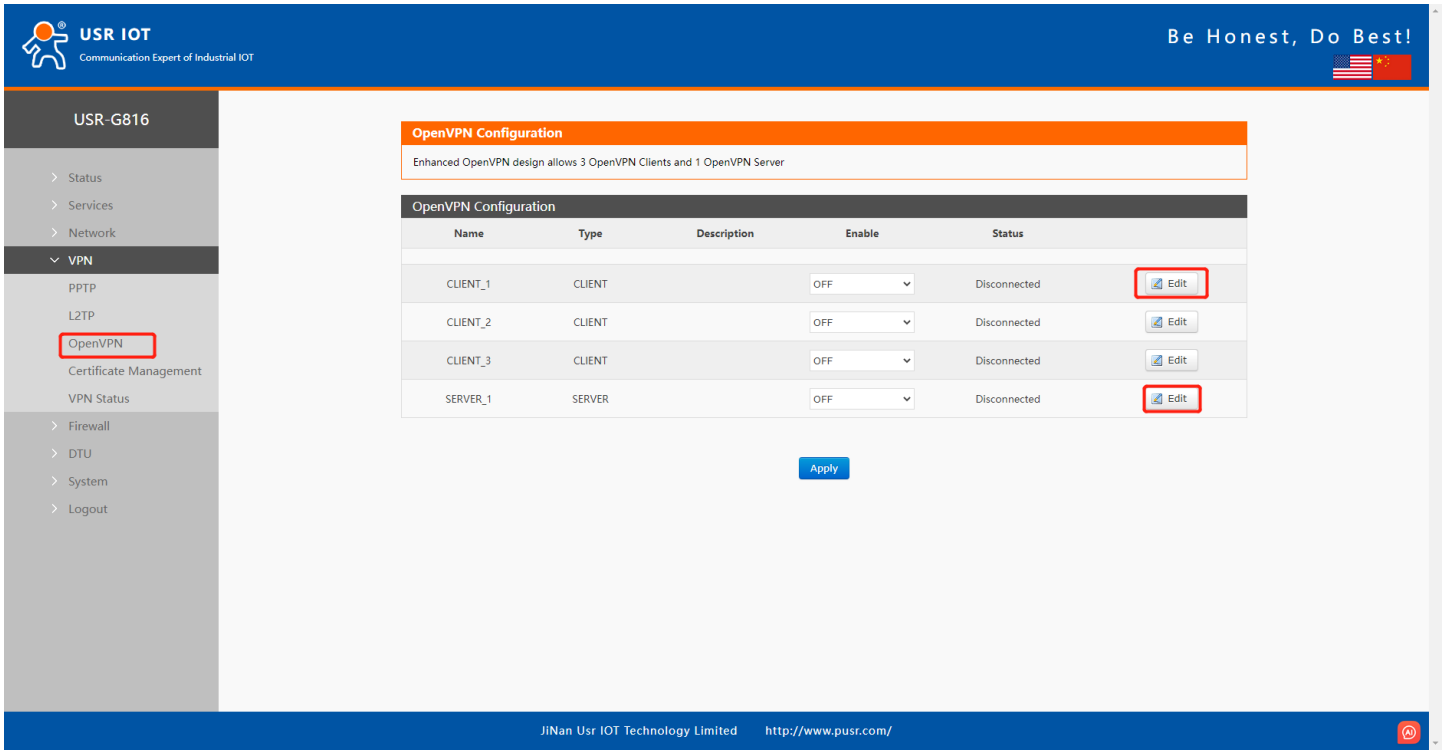

Figure 36. Edit OpenVPN settings

5.3.1. OpenVPN client

USR-G816 supports import .ovpn config file and PKCS#12 cert-file. Say goodbye to complex parameter settings. After importing the ovpn file, users just need to config the username and password.

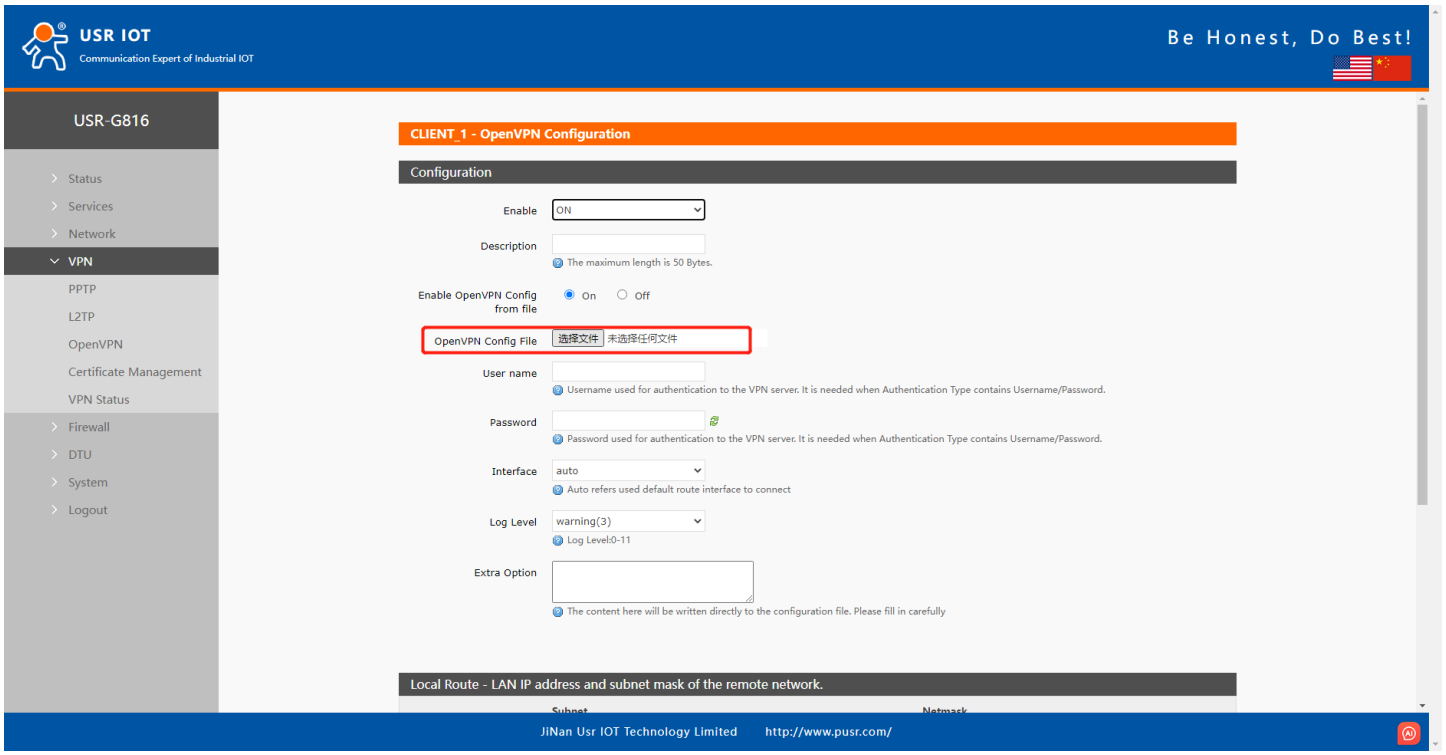

Figure 37. Upload OpenVPN Config file

If users need to set parameters using traditional way, just turn off the config file. The ca, cert, and key file can be loaded in “Certificate Management” page.

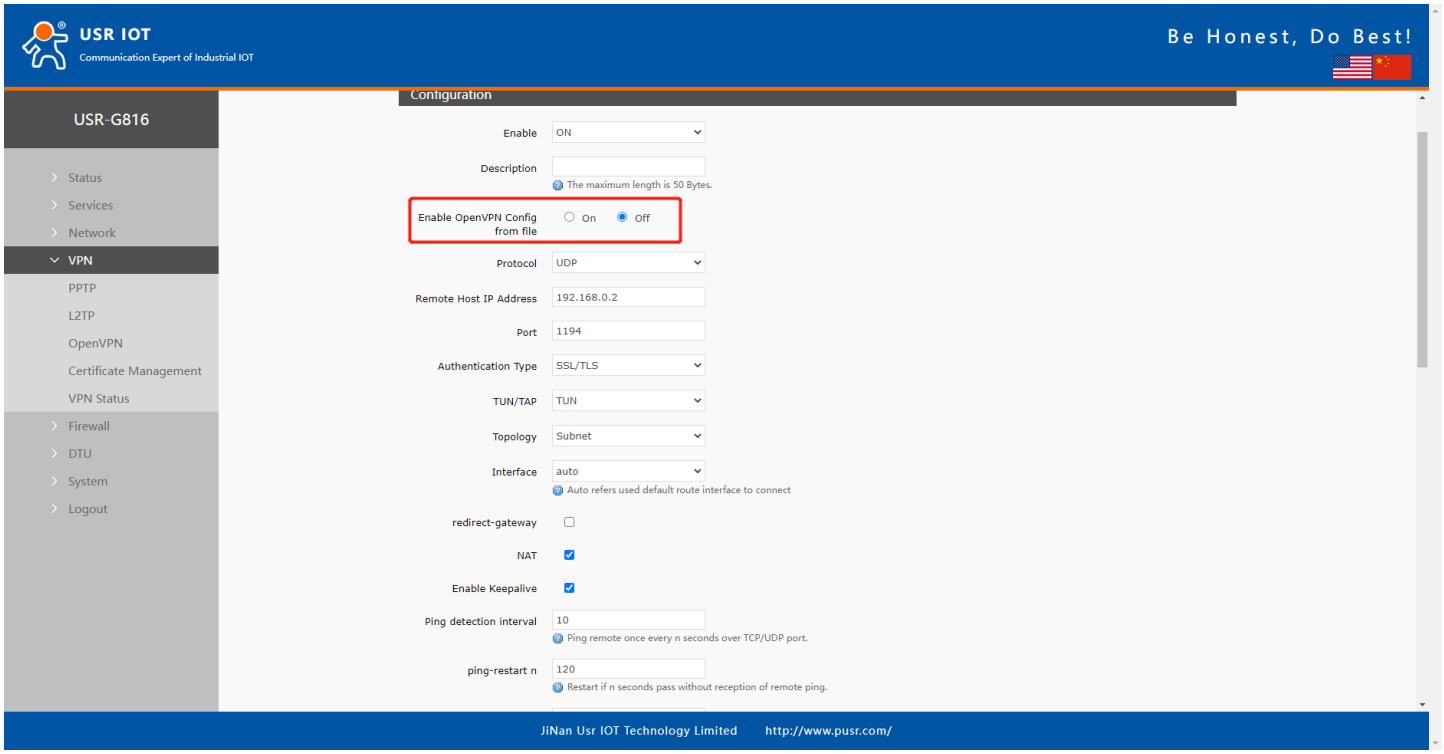

Figure 38. Enable traditional OpenVPN settings

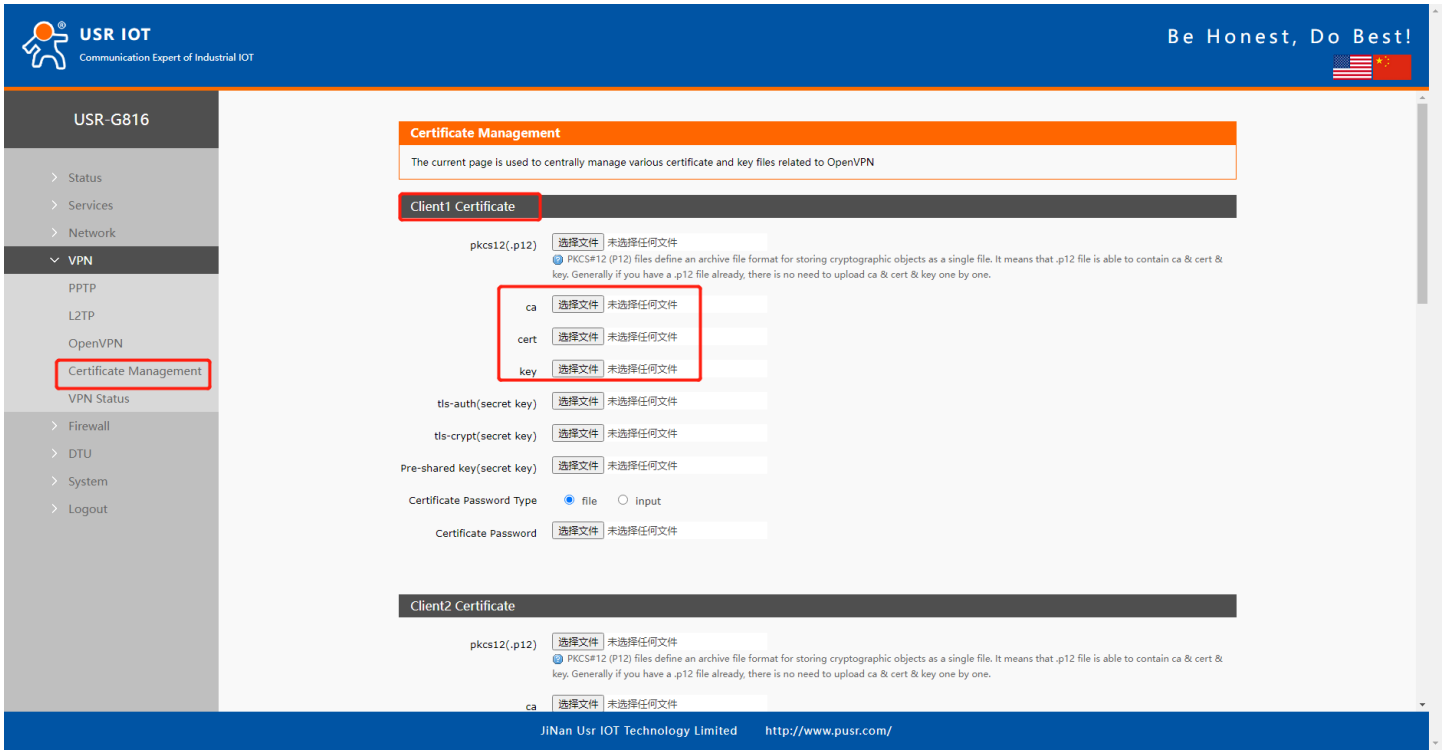

Figure 39. Upload certificate file

5.3.2. OpenVPN server

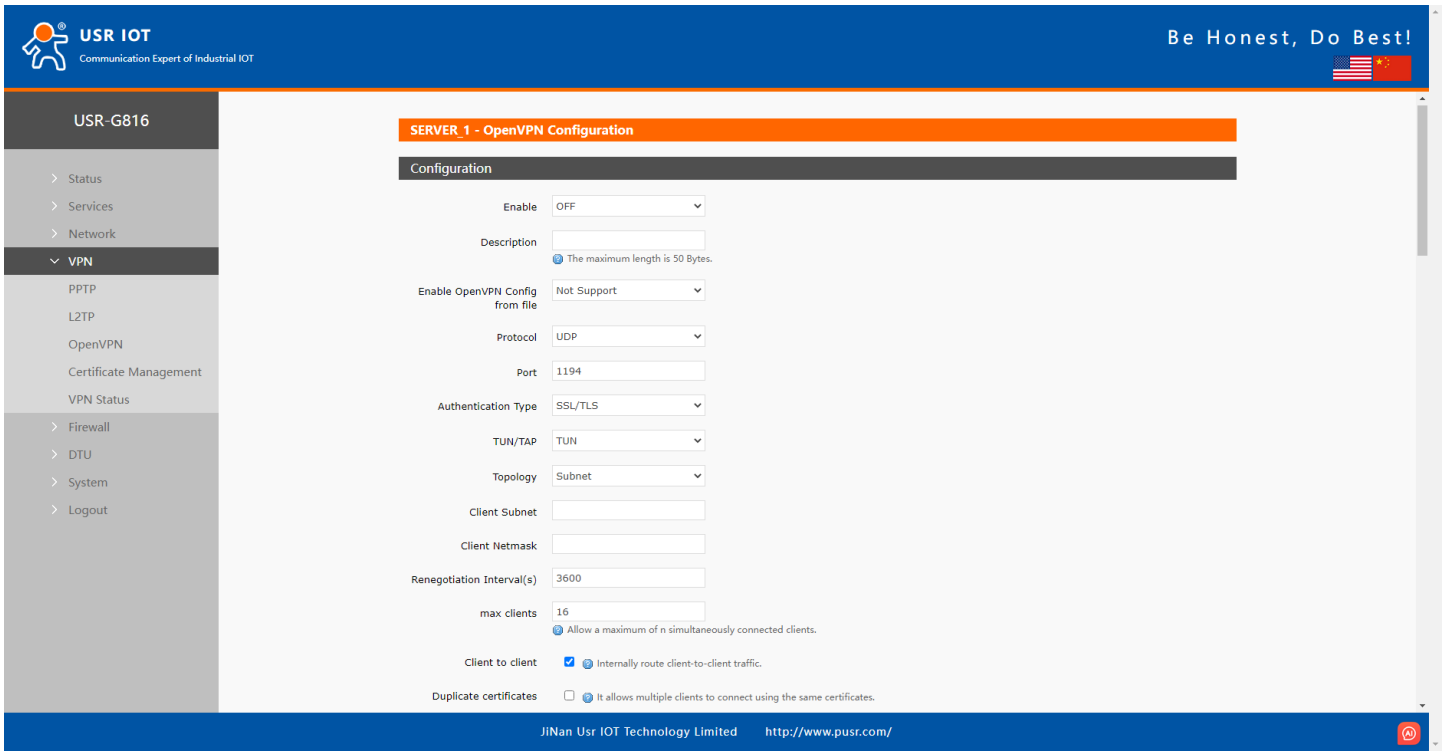

Figure 40. OpenVPN server settings

6. Firewall

6.1. General Settings

There are 2 firewalls by default in USR-G816.

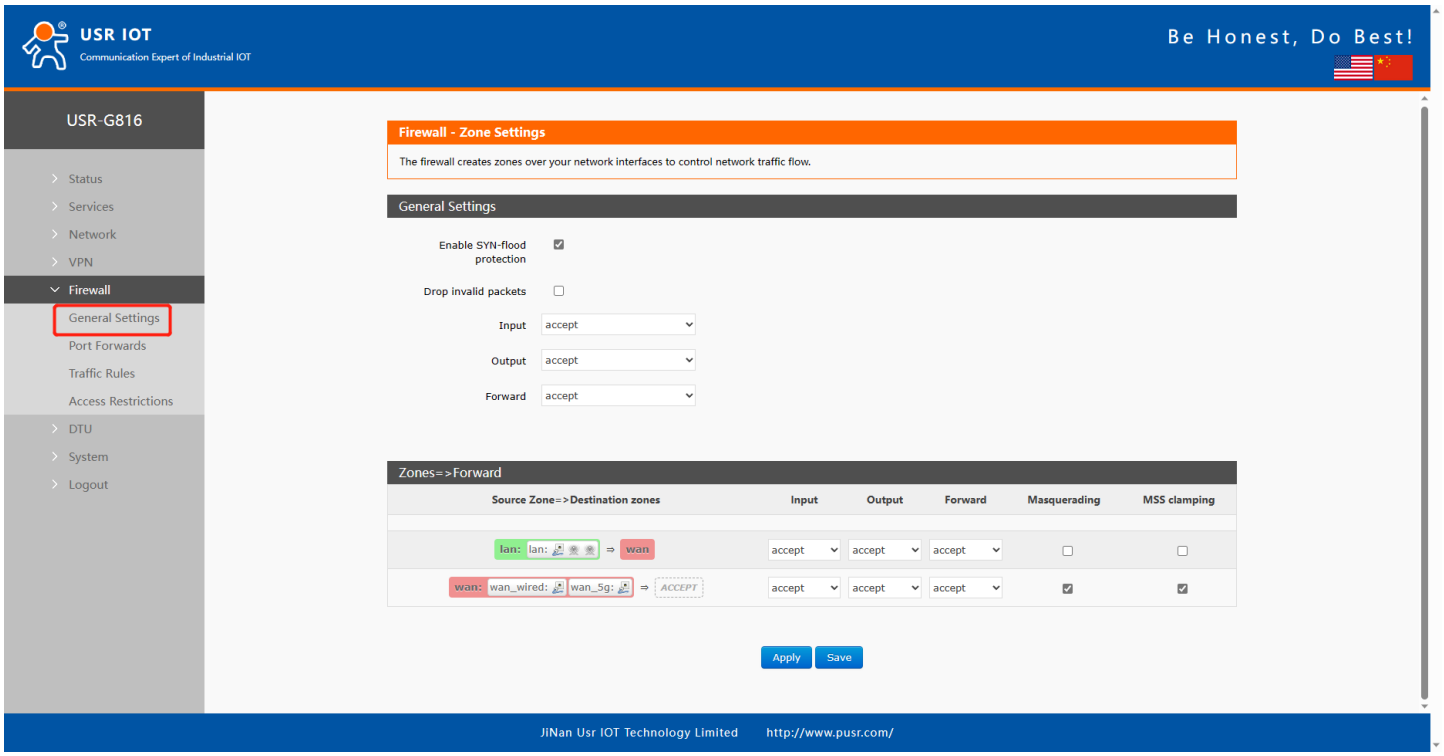

Figure 41. General settings of firewall

- Input: Packets that accessing router's IP.
- Output: Packets sent from the router.
- Forward: Data forwarding between interfaces, without routing itself.
- Masquerading: IP masquerading automatically, which is meaningful for the WAN port and 5G port, the masquerading for IP when access the external.
- MSS clamping: Limit the large of the MSS, generally it is 1460.

The first rule:

- The input, output, and forward packet from LAN to WAN is accept by default.
- Forward: If the data package will access the WAN from the LAN, so the rule allows data package from the LAN to WAN.
- Input: Open the webpage of the router when you under the LAN.
- Output: The router accesses the extern net, like NTP.

The second rule:

- WAN and 5G interface receive the input, output and forward packet by default.
- If there is input data package and it will be allowed. Such as someone will login the webpage of the router from the WAN.
- Same as the input, the output will be allowed if access the external net from the WAN or 4G of the router.
- The forward package is also allowed, data packets from the WAN port want to be forwarded to the LAN.

6.2. Port forward

6.2.1. Port forward

A port forward is a way of making a computer on your home or business network accessible to computers on the internet, even though they are behind a router or firewall.

Up to 100 port forwards can be added.

Table 12. Parameter details of port forward

Items	Description	Default
Name	The name of port forwarding rules, user-defined.	None
Protocol	Protocol type, options: TCP+UDP, TCP, UDP.	TCP+UDP
External Zone	WAN or VPN.	WAN

External port	Users can set a single port or a range of ports, like 8000-9000. Note: It's DMZ function when external port and internal port are empty.	None
Internal zone	LAN or VPN.	LAN
Internal IP address	IP address of device connected to LAN port.	None
Internal port	Users can set a single port or a range of ports, like 8000-9000. Note: It's DMZ function when external port and internal port are empty.	None

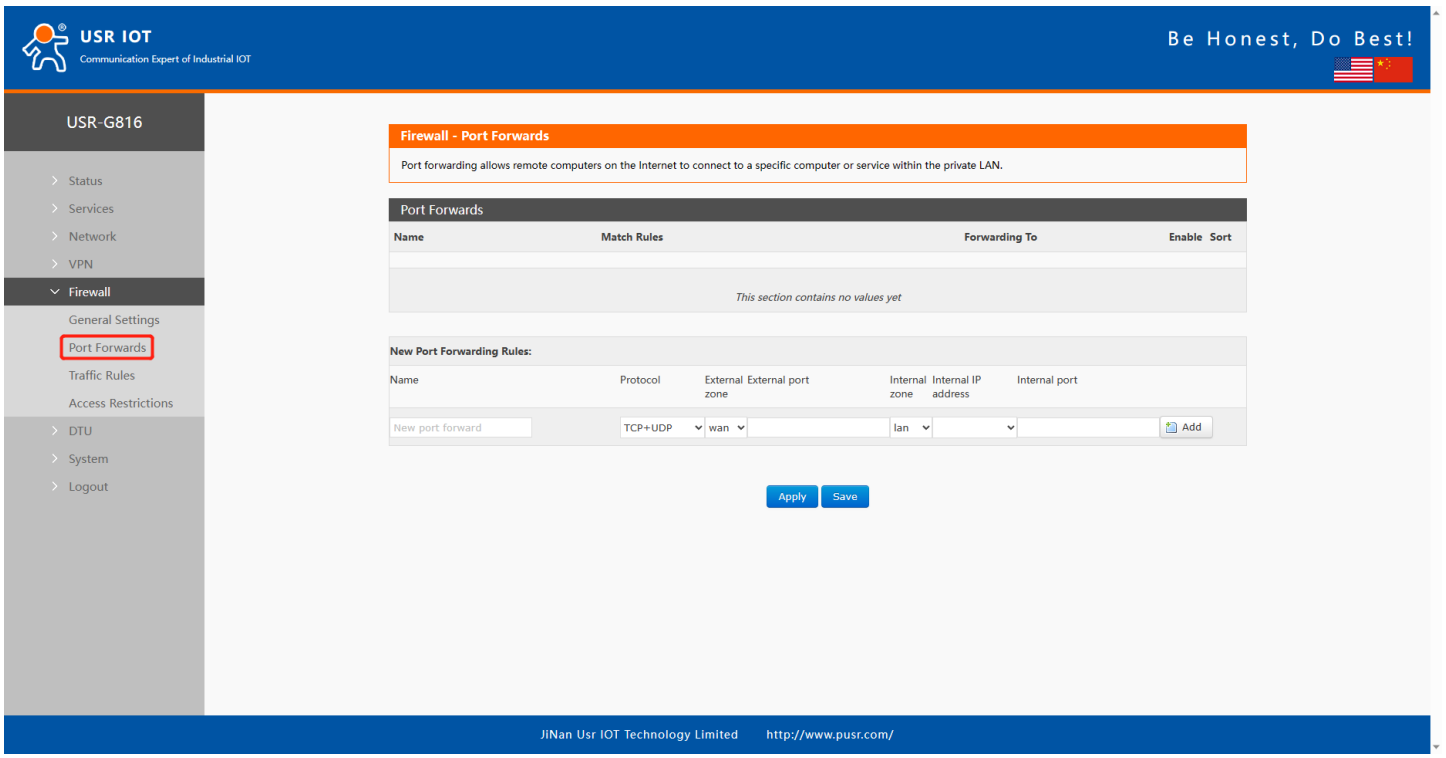

Figure 42. Port forwards settings

6.2.2. DMZ function

DMZ function is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks -- usually, the public internet.

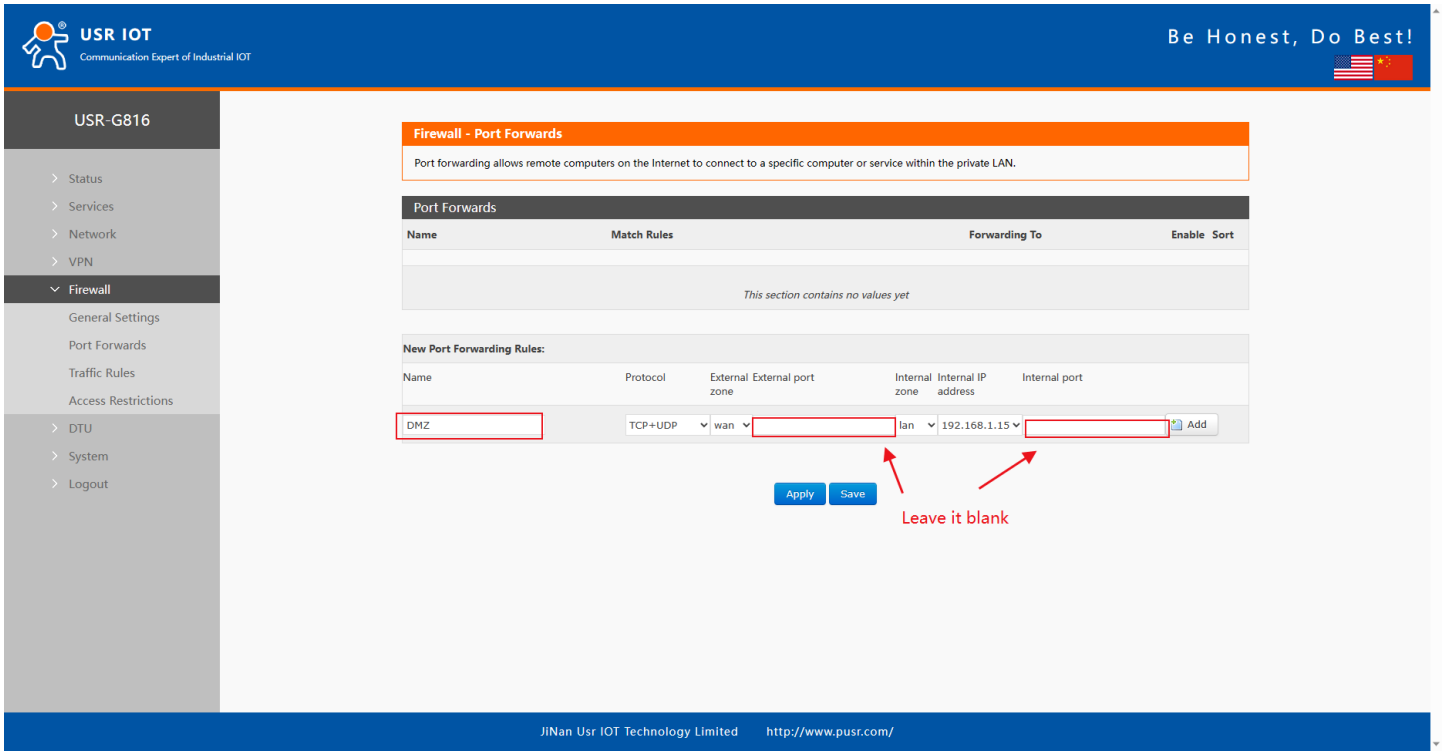

Figure 43. DMZ settings

6.3. Traffic rules

The Traffic Rules tab is a crucial feature of a firewall functionality that allows you to set rules to filter and control network traffic moving through the device. In essence, traffic rules determine which firewall rules will be applied to packets traveling through the network. These packets can be allowed, blocked, or rejected based on various criteria such as the source and destination IP addresses and port numbers specified in the packet headers.

Table 13. Parameter details of traffic rules

Items	Description	Default
Enable	Whether to enable the traffic rules.	Disable
Name	The name of traffic rules.	None
Restrict to address family	IP address family to which to rule will apply. It only supports IPv4 IP by now.	IPv4 only
Protocol	Choose the protocol of the traffic rules, including TCP+UDP, TCP, UDP, ICMP	TCP+UDP
Match ICMP type	Choose the ICMP type of the rules.	any
Source zone	The zone to which the third party will be connecting.	lan
Source MAC	MAC address(es) of connecting hosts.	any

	The rule will apply only to hosts that match MAC addresses specified in this field. Leave empty to make the rule skip MAC address matching.	
Source IP	IP address or network segment used by connecting hosts.	any
Source port	IP address or network segment used by connecting hosts.	None
Destination zone	Target zone of the incoming connection.	WAN
Destination IP	Tagert IP address or network segment of the incoming connection.	any
Destination port	Tagert port or range of ports of the incoming connection.	None
Action	Action that is to be taken when a packet matches the conditions of the rule. Drop: packet is stopped and deleted. Accept: packet gets to continue to the next chain. Reject: packet is stopped, deleted and, differently from Drop, an ICMP packet containing a message of rejection is sent to the source from which the dropped packet came. Don't track: packet is no longer tracked as it moves forward.	Accept

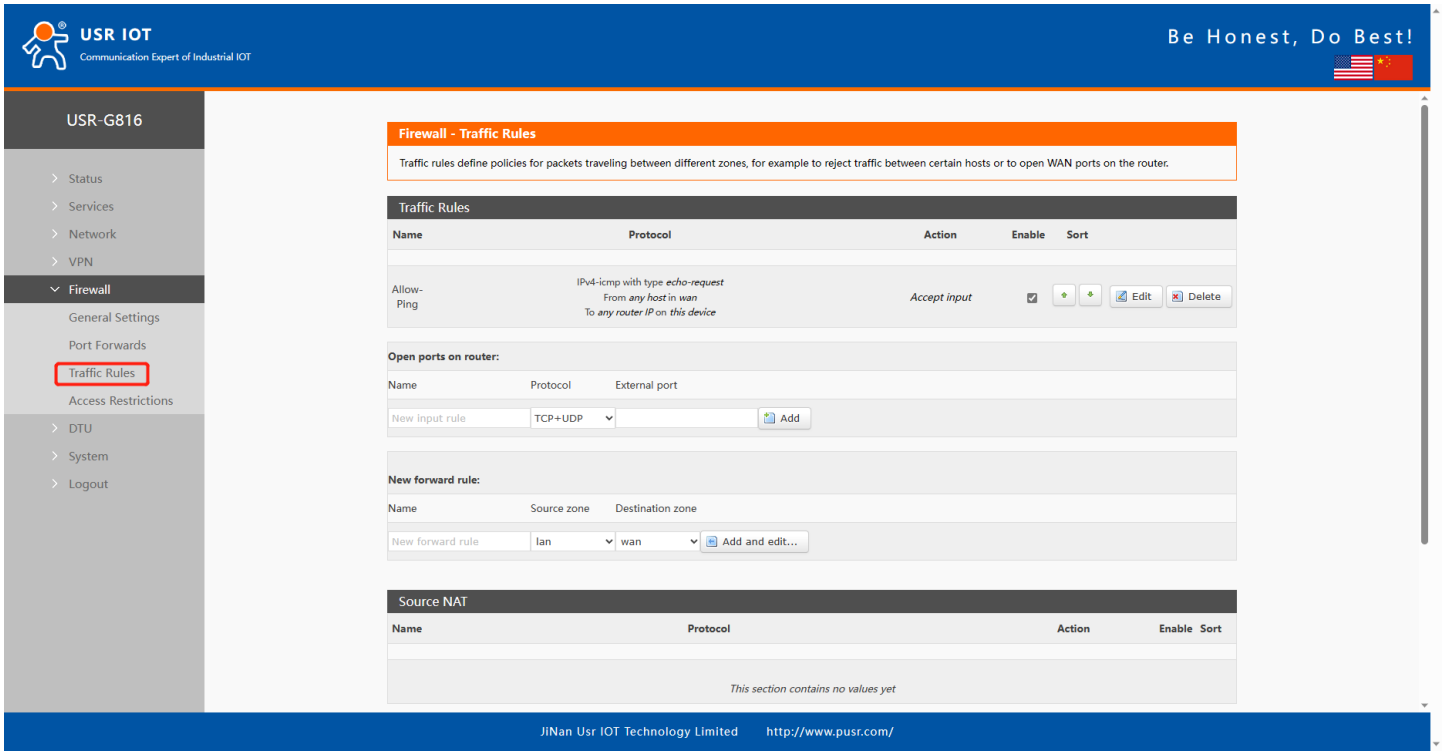

Figure 44. Traffic rules settings interface

6.3.1. Open ports on router

This provides a quick way to set simple rules that allow traffic on specified ports of the device. The figure

below is an example of the Open ports on device section and the table below provides information on the fields contained in that section.

Table 14. Parameter details

Items	Description	Default
Name	The name of the rule， user defined.	None
Protocol	Specifies to which protocols the rule should apply, including TCP+UDP, TCP, UDP.	TCP+UDP
External port	Specifies which port(s) should be opened.	None

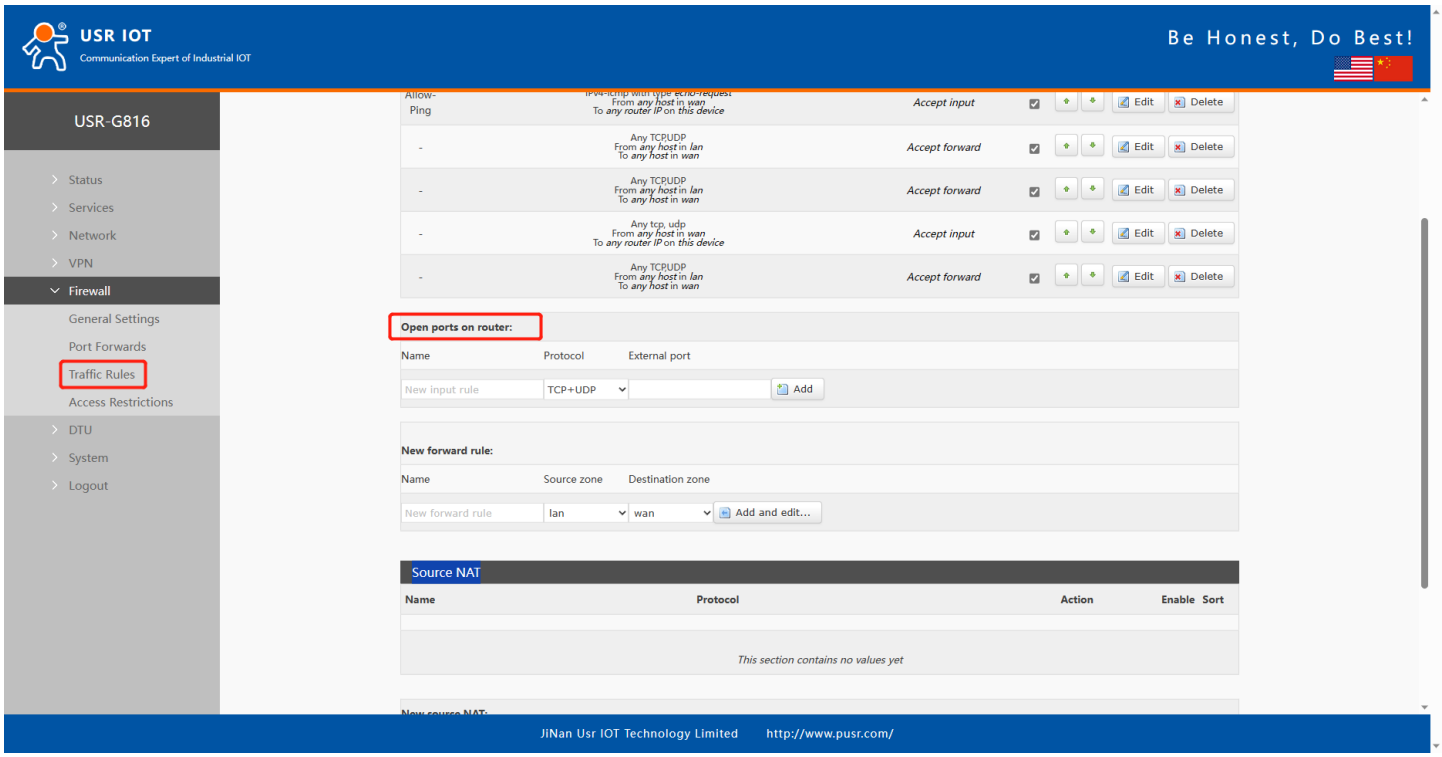

Figure 45.

6.3.2. Add new forward rule

This is used to create firewall rules that control traffic on the FORWARD chain. The figure below is an example of the Add New Forward Rule section and the table below provides information on the fields contained in that section.

Table 15. Parameter details

Items	Description	Default
Name	The name of the rule， user defined.	None

Source zone	The zone from which traffic has originated.	lan
Destination zone	The zone to which traffic will be forwarded to.	wan

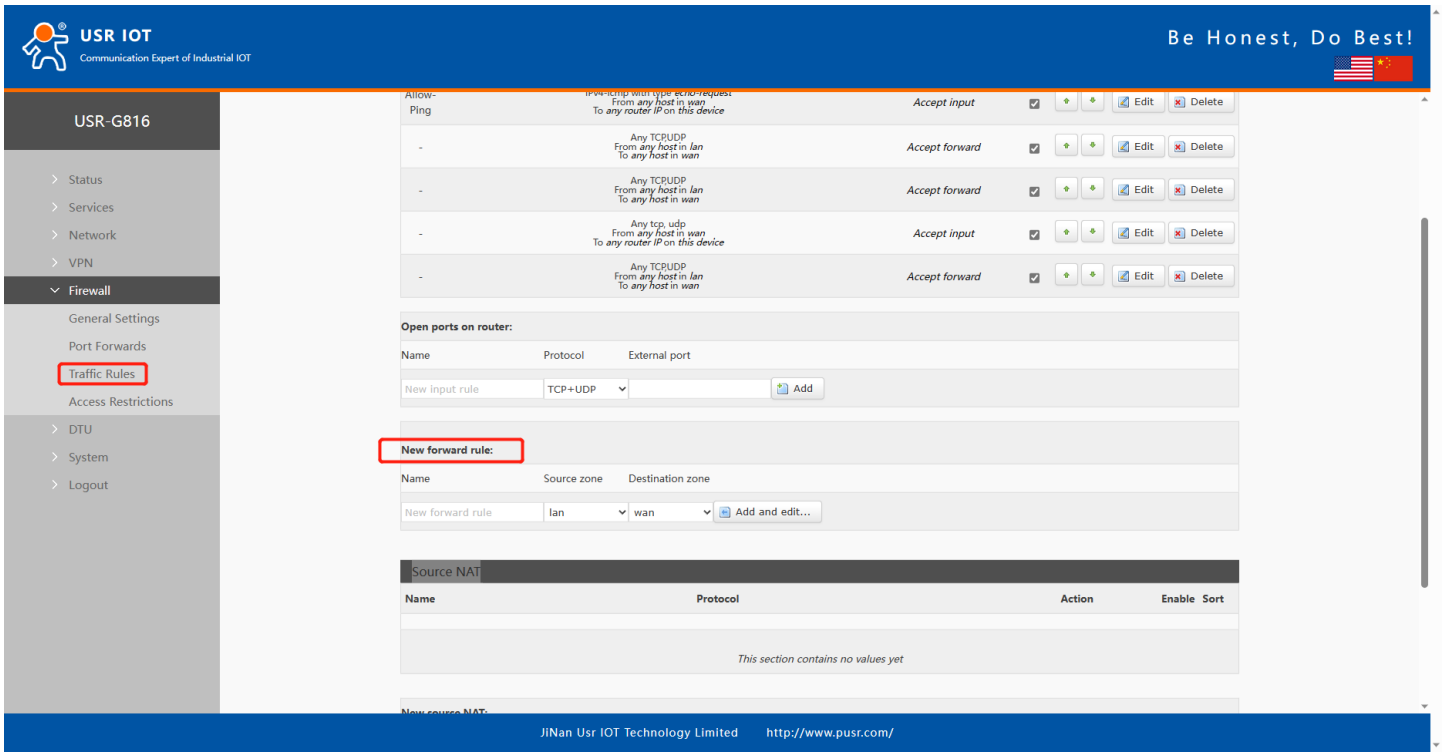

Figure 46. Add new forward rules

6.3.3. Source NAT

Source NAT (SNAT) is a form of masquerading used to change a packet's source address and/or port number to a static, user-defined value. SNAT is performed in the POSTROUTING chain, just before a packet leaves the device.

Up to 100 SNAT rules can be added.

Table 16. Brief parameters of Source NAT

Items	Description	Default
Name	The name of the rule， user defined.	None
Source zone	Matches traffic originated from the specified zone.	lan
Source zone	Matches traffic destined for the specified zone.	wan
To source IP	Matches traffic destined for the specified zone.	None
To source port	Matches traffic destined for the specified zone.	None

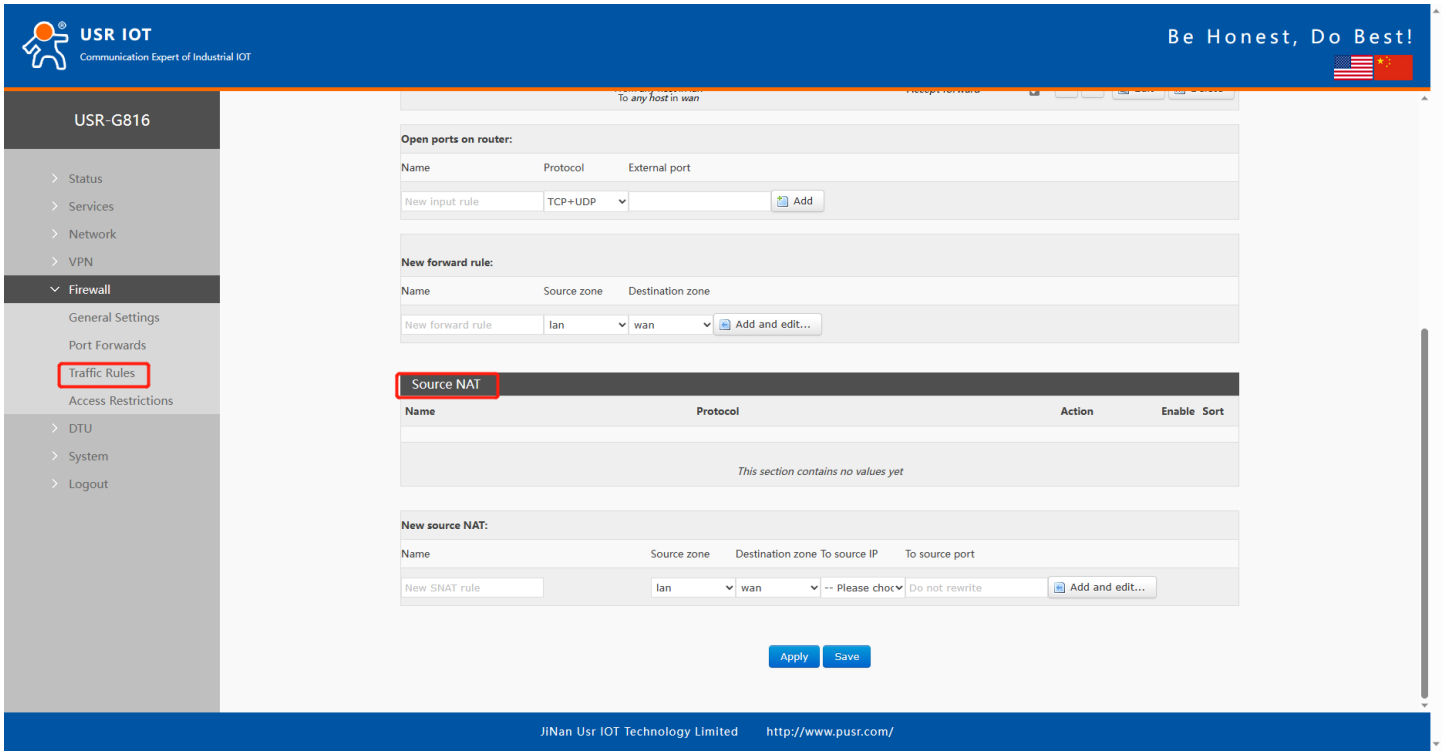

Figure 47. Settings of SourceNAT

After clicking the "Add and edit" button, it will redirect you to the rule's configuration page.

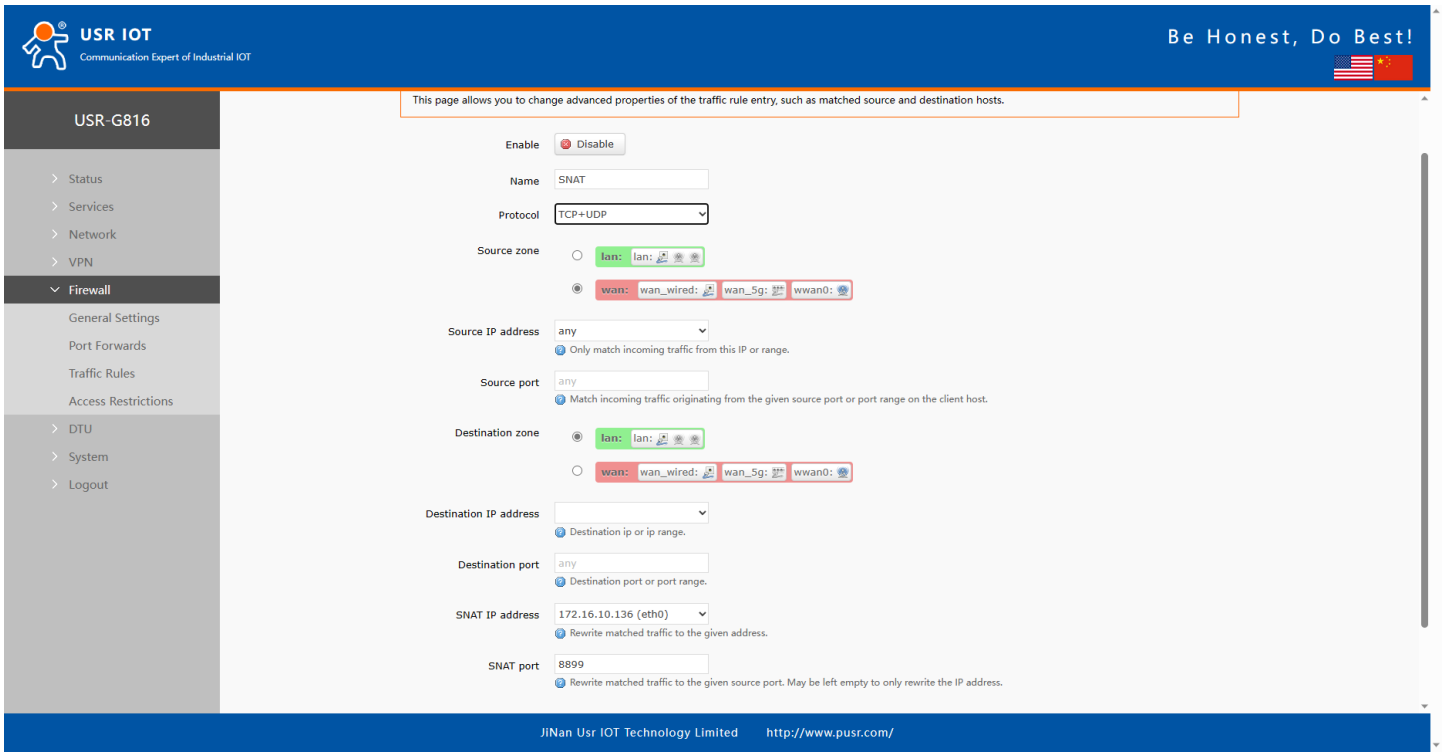

Figure 48. Detail settings of SourceNAT

Table 17. Parameter details of Source NAT

Items	Description	Default

Enable	Whether to turn on the rule.	Disable
Name	The name of the rule, user defined.	None
Protocol	Specifies to which protocols the rule should apply, including TCP+UDP, TCP, UDP, ICMP.	TCP+UDP
Source zone	Matches traffic originated from the specified zone.	LAN
Source IP	Mathes traffic originated from specified IP address or network segment.	any
Source port	Mathes traffic originated from specified port number.	None
Destination zone	Mathes traffic originated from specified port number.	wan
Destination IP	Matches traffic destined for the specified IP address or network segment.	None
Destination port	Matches traffic destined for the specified port number.	None
SNAT IP	Changes matched traffic packet source IP address to the value specified in this field.	None
SNAT port	Changes matched traffic packet source port number to the value specified in this field.	None

6.4. Access restrictions

Access restrictions implement access restrictions on specified domain names, and support blacklist and whitelist settings for domain name addresses. When blacklist is selected, devices connected to the router cannot access the blacklisted domain names, and other domain name addresses can be accessed normally. When the whitelist is selected, the devices connected to the router can only access the domain names in the white list, and other domain names cannot be accessed normally. Both the blacklist and the whitelist can be set with multiple entries, and this function is disabled by default.

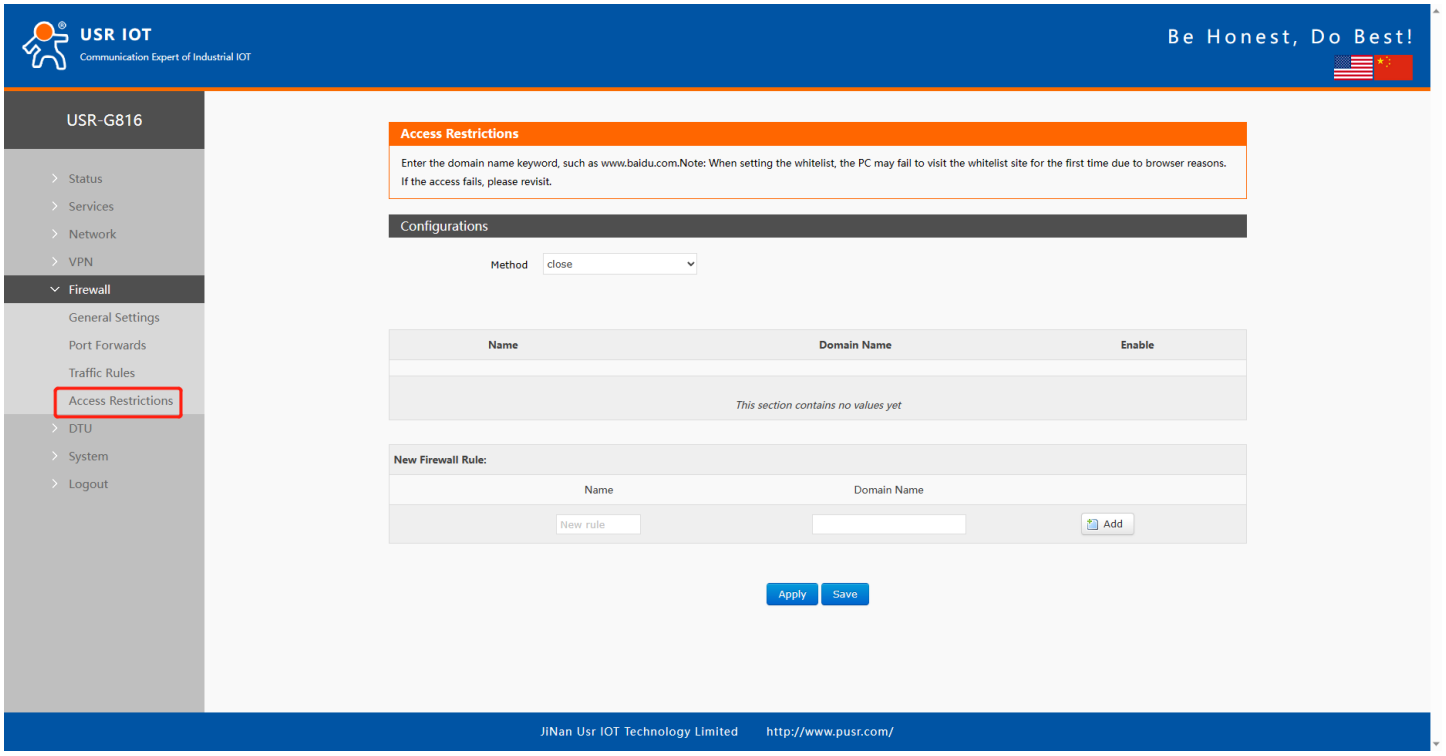

Figure 49. Access restrictions interface

6.4.1. Blacklist settings

First, select the blacklist, enter the name of the rule and the prohibited domain address, and then click Add, and the added rules will be displayed in the list. Click Apply and the rules take effect immediately. Devices connected to the router will not be able to access the domain address just added. If blacklist is selected but no rules are added, the default blacklist is empty, that is, all domain names can be accessed. As shown in the figure, except **www.baidu.com** and www.google.com, other domain names can be accessed normally.

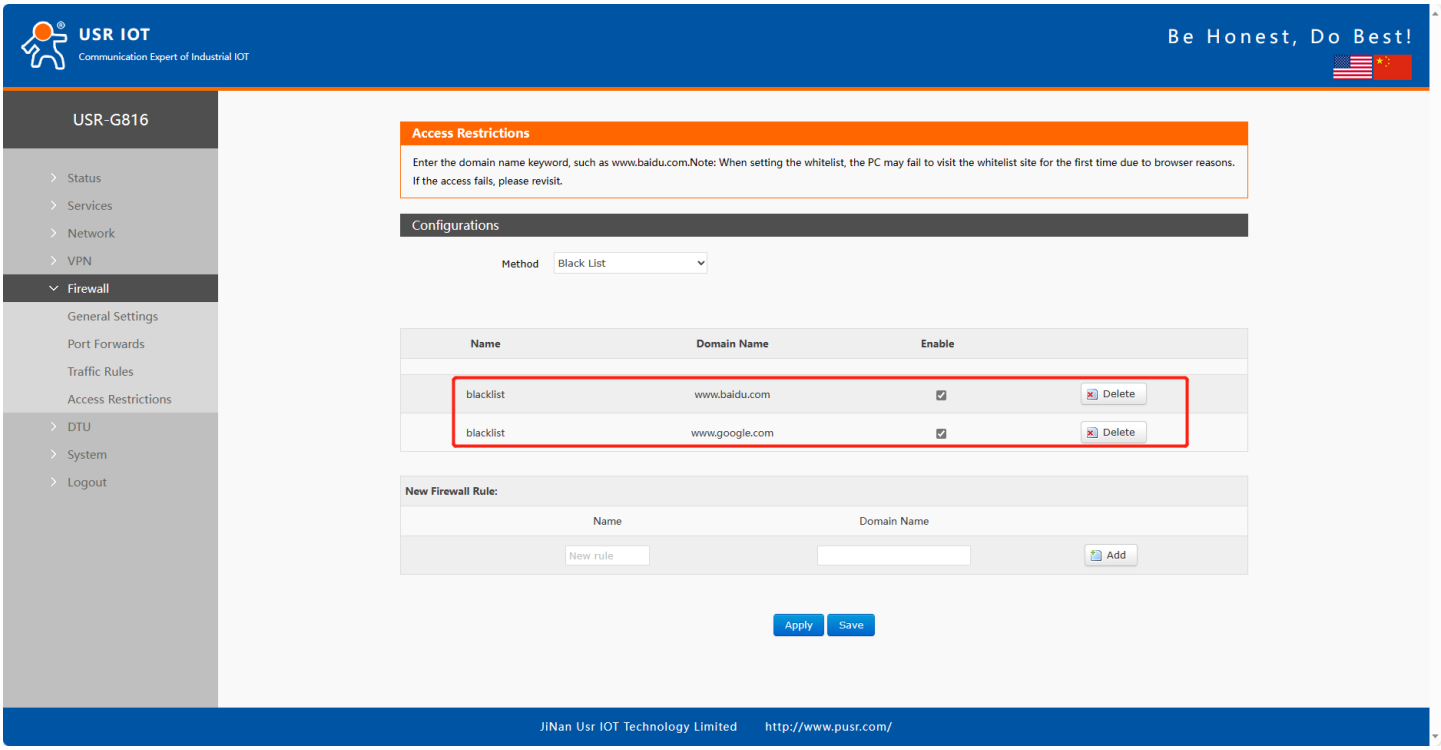

Figure 50. Add blacklist rules

6.4.2. Whitelist settings

Select the whitelist, enter the name of the rule and the domain address that is allowed to be accessed, and then click Add, and the added rules will be displayed in the list. Click Apply and the rules take effect immediately. Devices connected to the router will not be able to access the domain address except the ones in the rule. If you select the whitelist but do not add a rule, the default whitelist is empty, that is, all domain address cannot be accessed. As shown in the figure, the device can access Baidu.

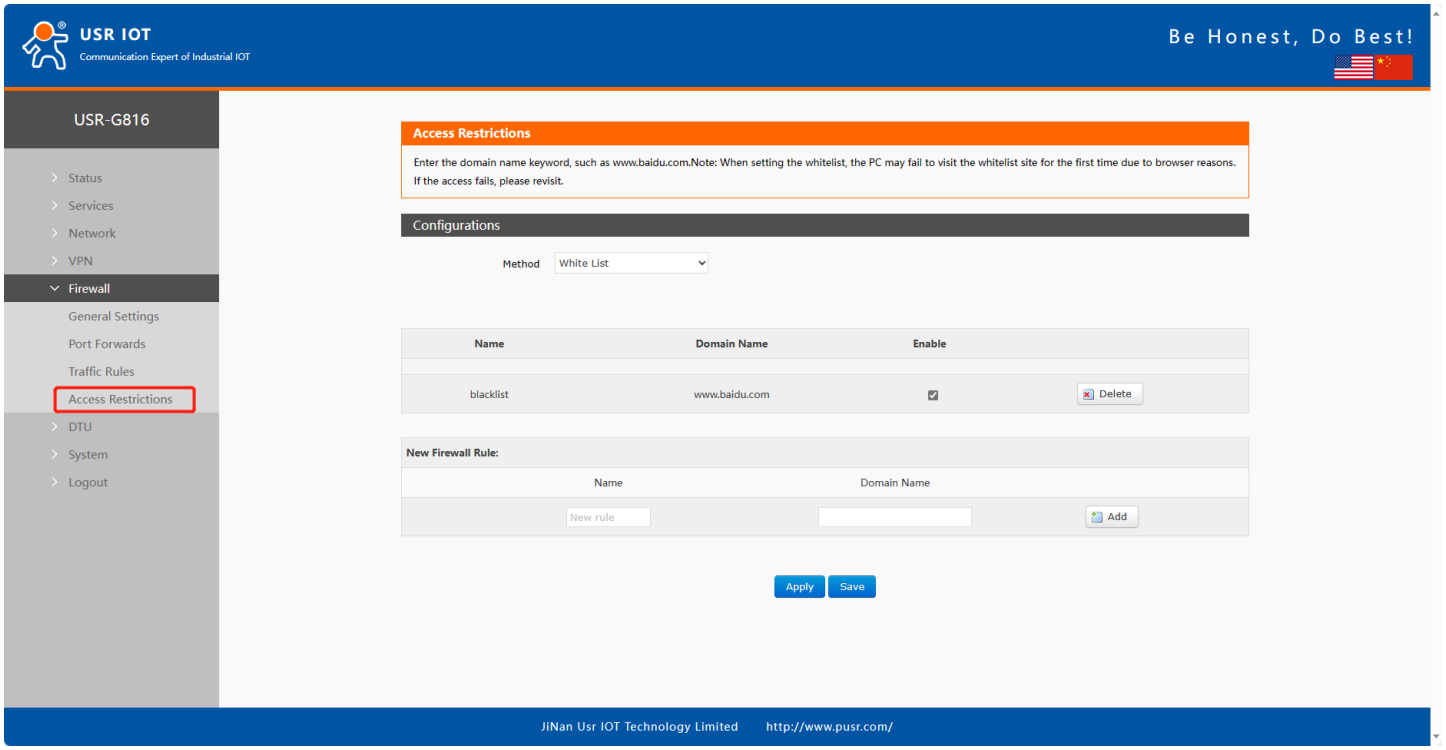

Figure 51. Add whitelist rules

7. DTU Function

USR-G816 comes with 1*RS232/485 serial port, through simple settings, the serial device can be connected to the network and achieve data communication with the remote server. There are 3 work mode for DTU function: NET, HTTPD, MODBUS.

- NET: In this mode, the user does not need to pay attention to the data conversion process between the serial port and the network and can realize the data transparent communication between the serial port device and the designated network server.
- HTTPD: In this mode, data communication between the serial device and the HTTP server can be realized. USR-G816 can pack the data from serial device into HTTP format and send it to HTTP server, or parse the data returned by server and send it to the serial device.
- MODBUS: In this mode, USR-G816 can realize Modbus RTU/TCP conversion between the serial port device and the designated network server.

Note: In NET and MODBUS mode, SOCKA, B, C, D can be used, but the HTTPD mode cannot be used at the same time.

7.1. General settings

7.1.1. Protocol selection

Users can choose the work mode as needed. The “Restarting without data” function is off by default.

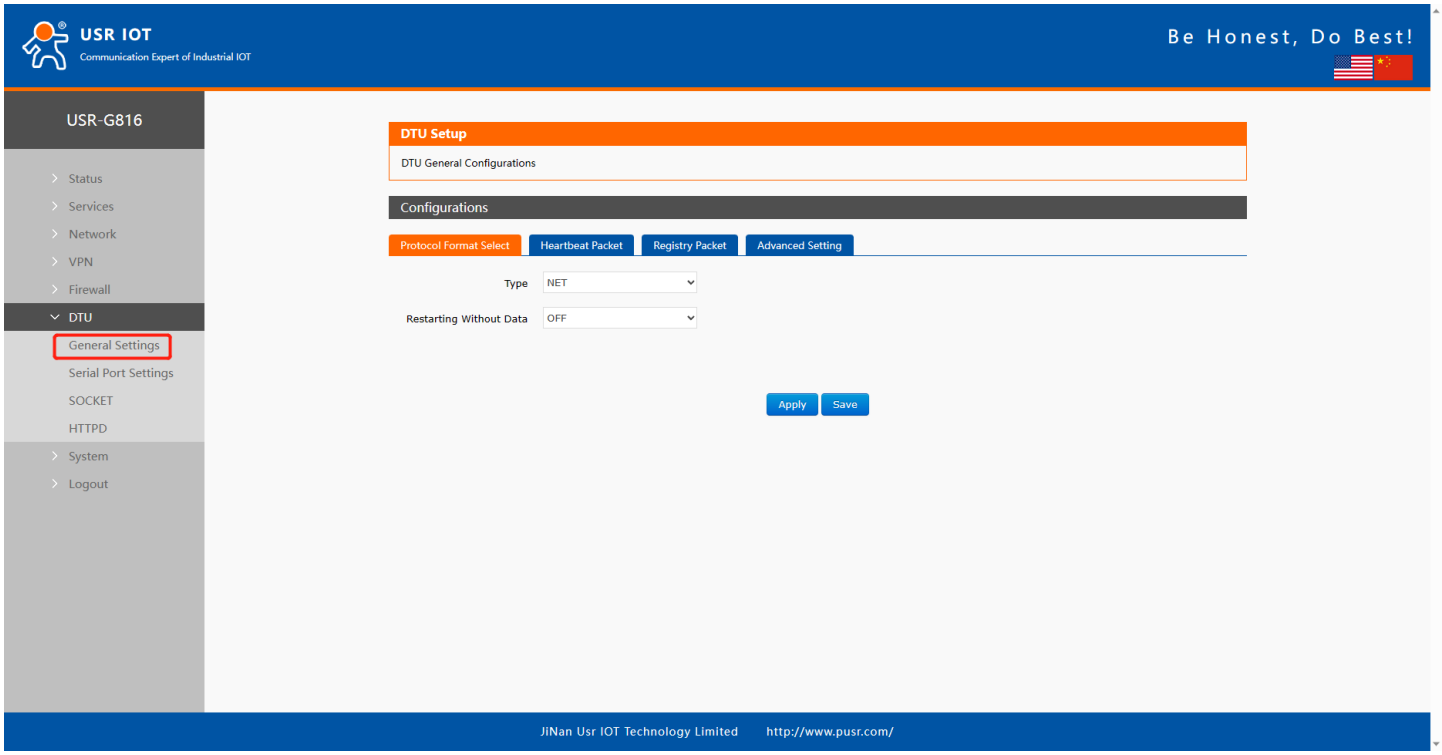

Figure 52. General settings of DTU function

If we turn on the “Restarting without data” function, there are two parameters:

Table 18. Parameters of restarting without data

Items	Description	Default
Reconnect Detection Interval(s)	If the USR-G816 does not receive the data sent by the server for more than pre-set seconds, it will actively reconnect to the server. Pre-set value range：1-3600s.	3600 seconds
Restart Detection Interval(s)	If the USR-G816 does not receive the data sent by the server for more than pre-set seconds, it will restart. Pre-set value range：60-36000s.	36000 seconds

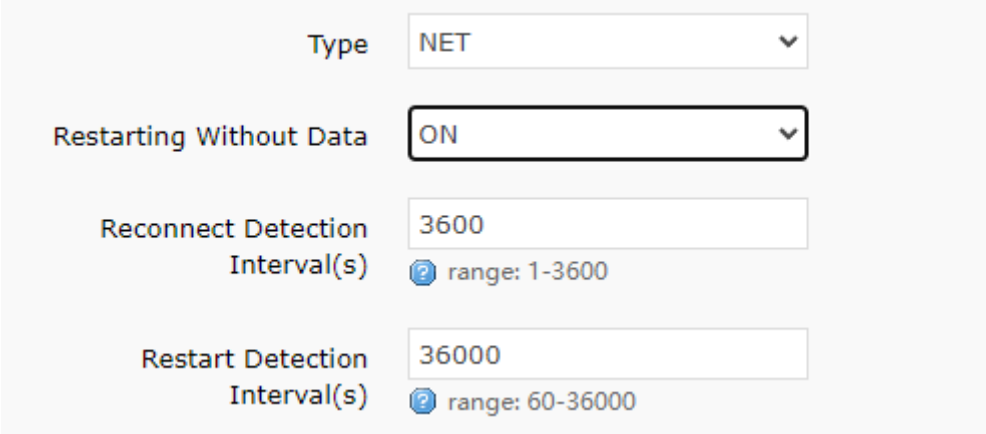

Figure 53. Settings about restarting without data

7.1.2. Heartbeat packet

When USR-G816 works in TCPC or UDPC mode, it can actively send heartbeat packet information to the remote server, which is convenient for the server to judge whether USR-G816 is still online.

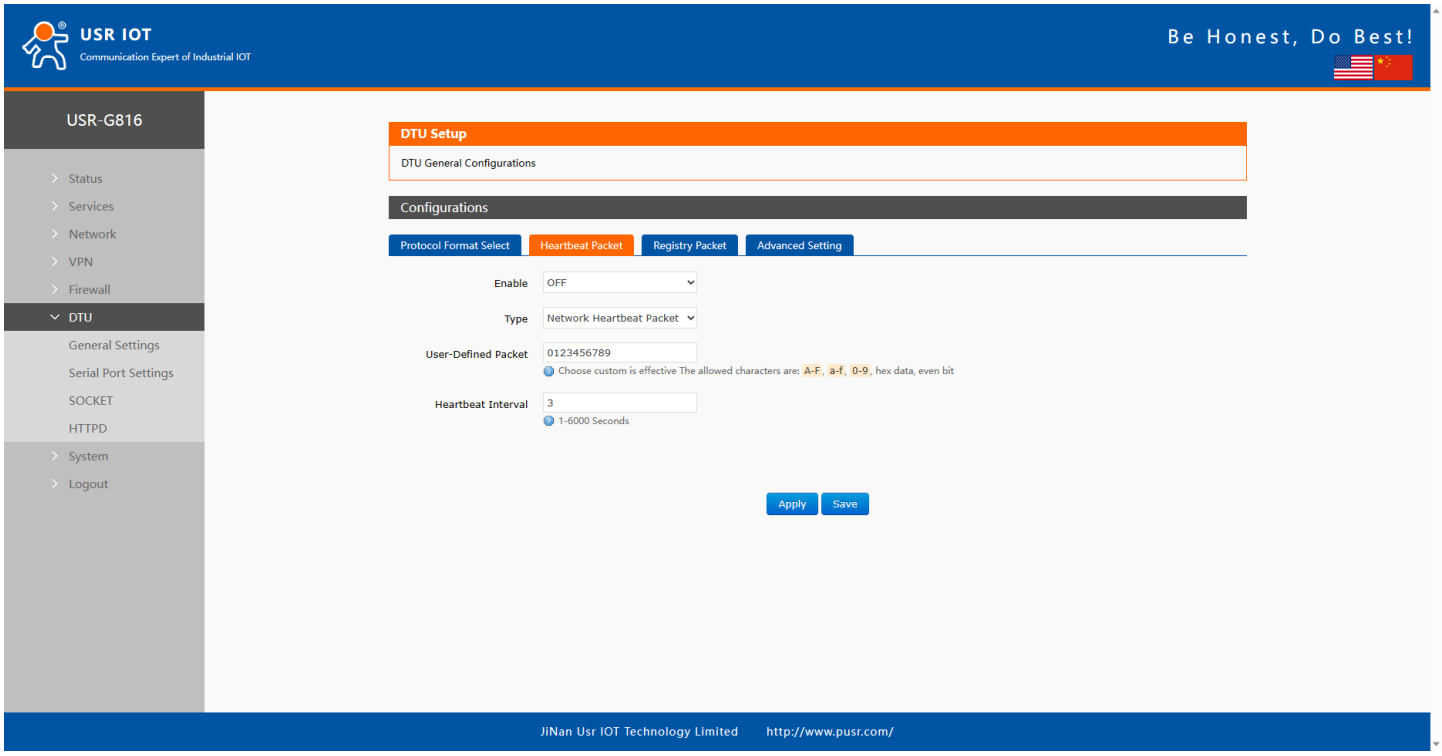

Figure 54. Settings of heartbeat packet

7.1.3. Registration packet

The remote server can distinguish different data sources by registering package information, to process the received data.

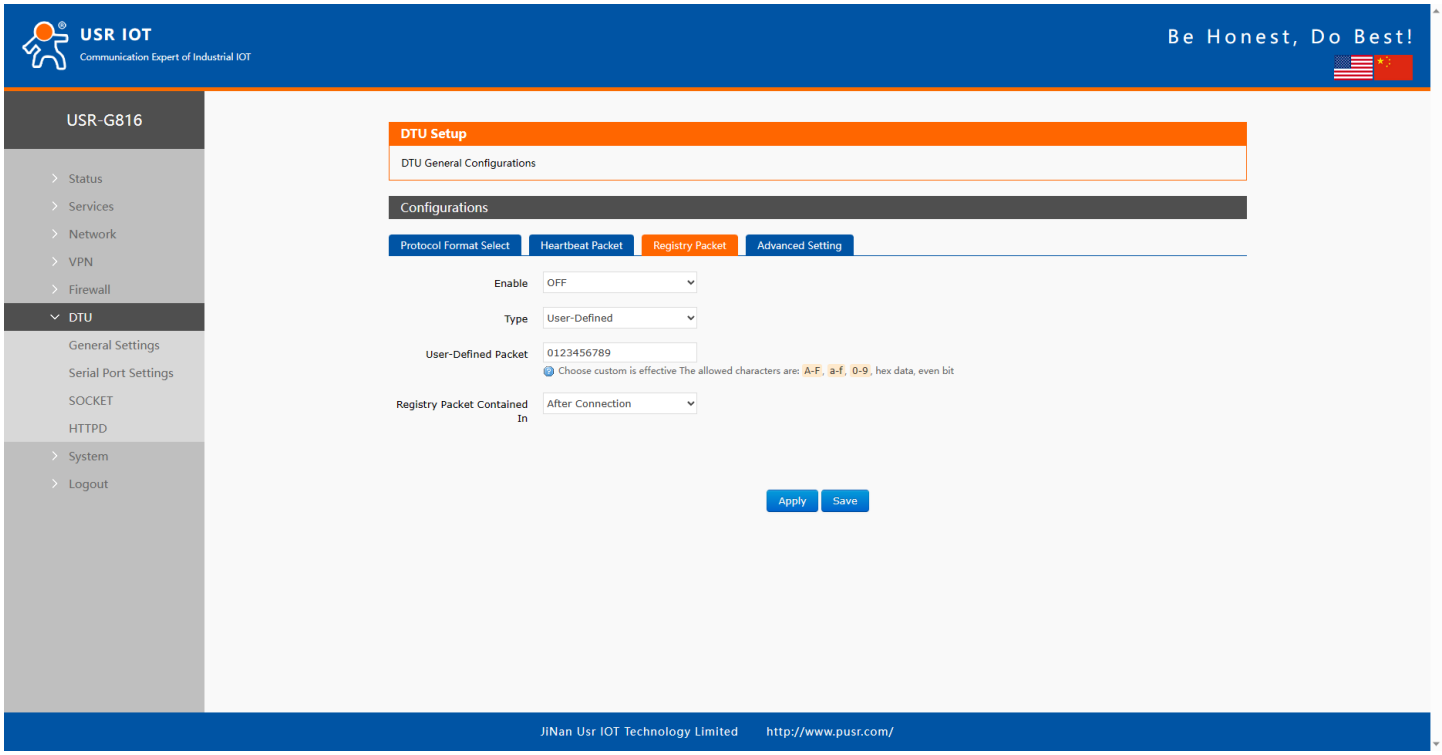

Figure 55. Settings of registration packet

Table 19. Parameter details of registration packet

Items	Description	Default
Enable	Master switch of registration packet function. ON: Enable registration packet function. OFF: Disable registration packet function.	OFF
Type	User-defined: Uses define the registration package content. ICCID: The registration package content is ICCID information. IMEI: The registration package content is IMEI information. USR-Cloud: The registration package content is device ID assigned by PUSR.	User-defined
User-Defined Packet	The content of registration packet. Only valid for user-defined registration packet type. Hex format.	0123456789
Registry Packet Contained In	After connection: Send the registration packet information only once after the socket connection is established. Prefix of data: Add registration packet information in front of each packet of data sent by the serial device.	After connection

7.1.4. Advanced settings (AT command password)

The password of network AT command. We will introduce it in later chapter.

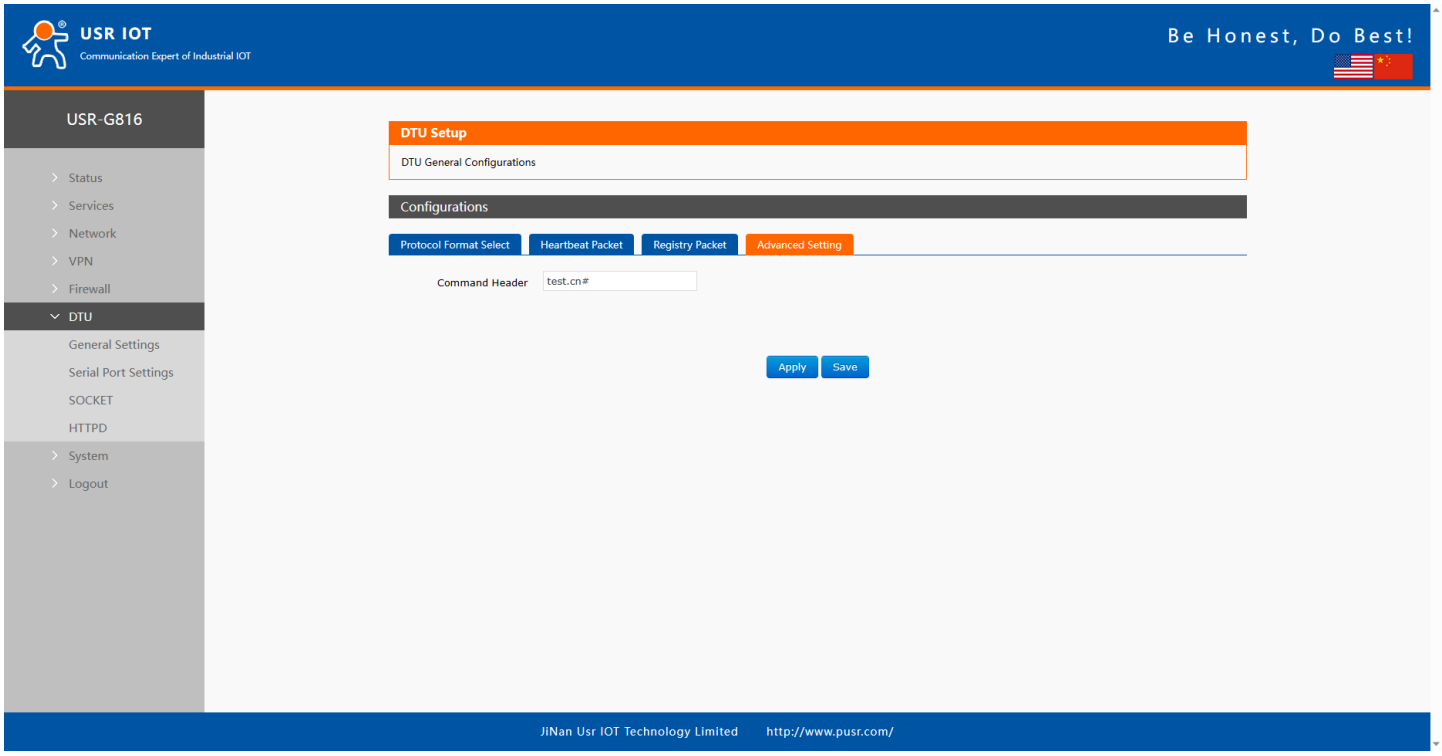

Figure 56. AT command password

7.2. Serial port settings

7.2.1. Parameter description

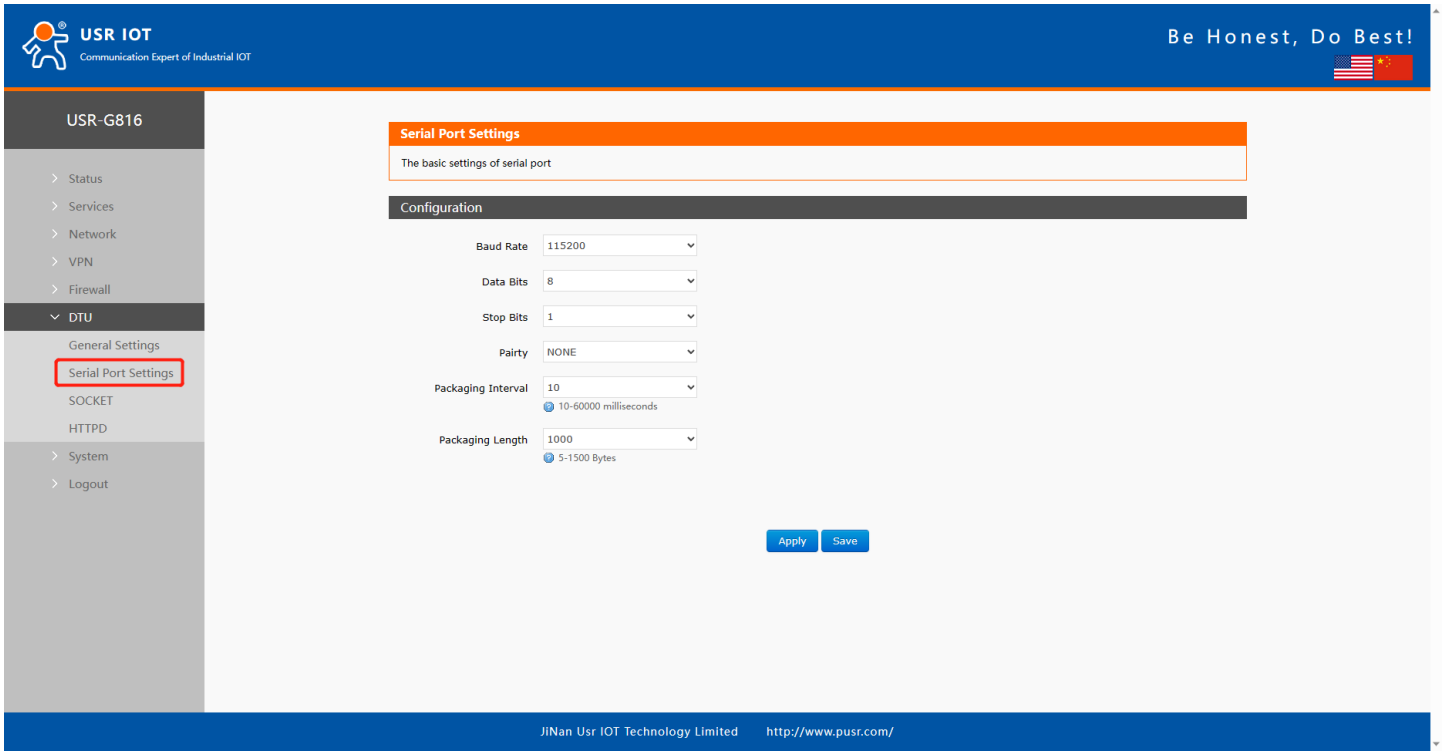

Figure 57. Serial port settings

Table 20. Parameter description of serial port

Items	Description	Default
Baud Rate	Baud rate of serial port. This parameter needs to be consistent with the serial device. Options: 1200, 2400,4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800.	115200
Data Bits	Data bits of serial port. This parameter needs to be consistent with the serial device. Options: 7, 8	8
Stop Bits	Stop bits of serial port. This parameter needs to be consistent with the serial device. Options: 1, 2	1
Parity	Parity of serial port. This parameter needs to be consistent with the serial device. Options: None, Odd, Even	None
Packeting Interval	If the time interval between two adjacent bytes exceeds the set value, it will be divided into two packets and sent. 10~60000ms	10ms
Packeting Length	When the length of the data packet reaches the set value, it will be sent out. 5-1500 Bytes	1000 Bytes

7.2.2. Packeting mechanism

- Packeting by time

When G816 receives data from UART, it will constantly check the interval time between two adjacent bytes. If the interval time is greater than or equal to a certain "time threshold", it is considered that a data frame is over, otherwise data is received until it is greater than or equal to the packet length (default is 1000 bytes). Send this frame of data as a TCP or UDP packet to the network side. The "time threshold" here is the packing interval. The range that can be set is 10ms~60000ms. The factory default is 10ms.

This parameter can be set according to AT command, AT+UARTFT=50.

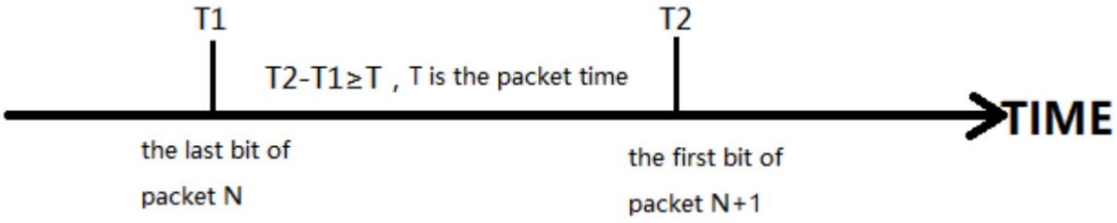

Figure 58. Packeting mechanism by time

- Packeting by length

When G816 receives data from UART, it will constantly check the number of bytes received. A frame is considered complete if the number of bytes received reaches a certain "length threshold". Send this frame of data as a TCP or UDP packet to the network side. The "length threshold" here is the packing length. The range that can be set is 5~1500 bytes. The factory default is 1000 bytes.

This parameter can be set according to AT command, AT+UARTFL=<length>.

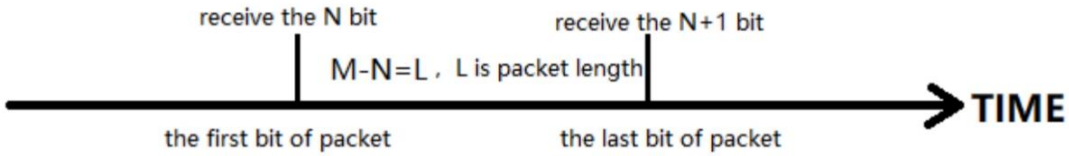

Figure 59. Packeting mechanism by length

7.3. SOCKET

When the USR-G816 work at NET or MODBUS mode, users need to set the parameters on this page.

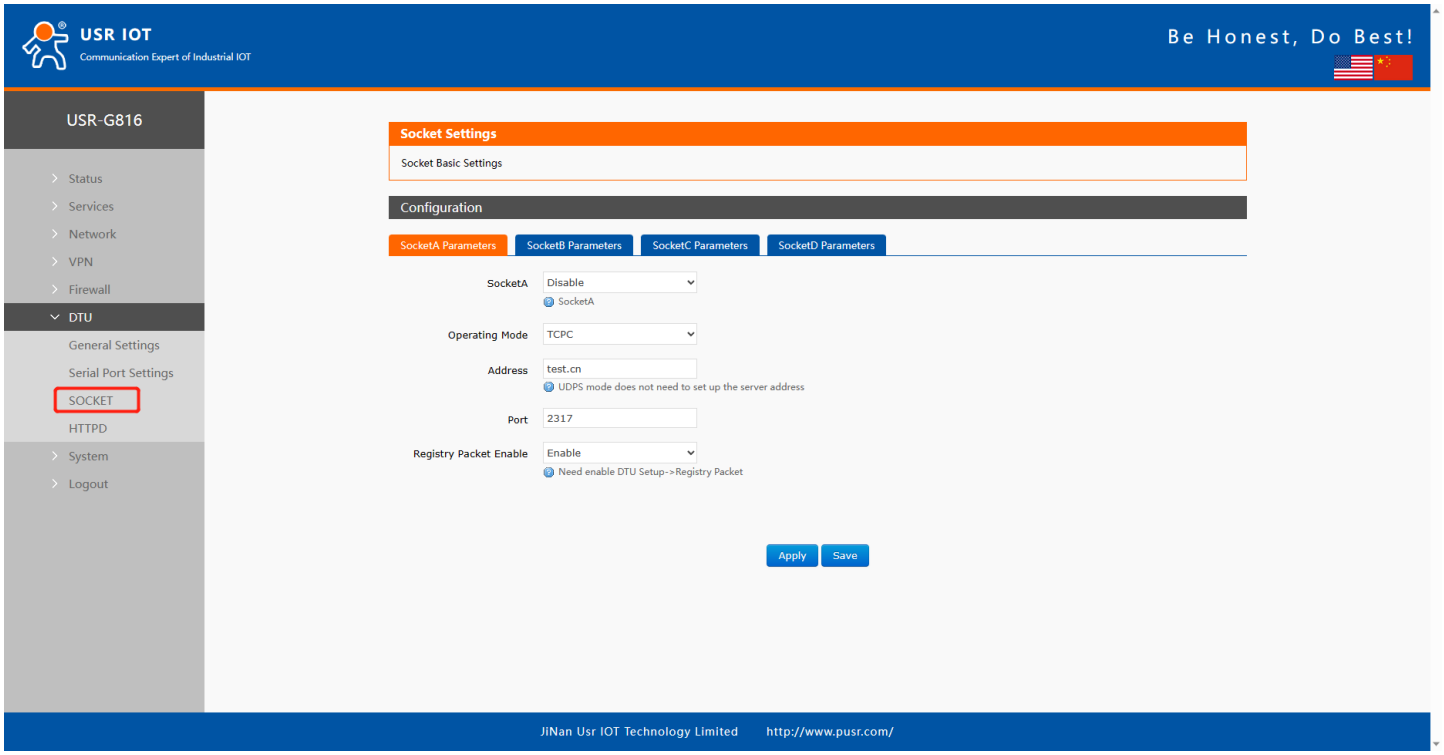

Figure 60. Settings of socket

Table 21. Parameters description of socket

Items	Description	Default
Socket A	Enable: Enable socket A communication. Disable: Disable socket A communication.	Disable
Operating Mode	TCPC: TCP client mode. TCPS: TCP server mode, Support simultaneous access to 8 clients (Only for SOCKA). UDPC: UDP client mode. UDPS: UDP server mode.	TCPC
Address	For TCPC and UDPC mode, it's the IP address of remote server. For TCPS and UDPS mode, it's no practical meaning.	test.cn
Port	For TCPC and UDPC mode, it's the listening port of remote server. For TCPS and UDPS mode, it's the listening port of USR-G816.	2317
Registry Packet Enable	This switch button is used together with the function in "General Settings". Enable: Enable the registration packet function corresponding to the socket.	Enable

	Disable: Disable the registration packet function corresponding to the socket.	

7.4. HTTP Client

When USR-G816 works at HTTPD mode, users need to set the parameters on this page.

Table 22. Parameter description of HTTP

Items	Description	Default
Request Method	Support 2 methods: GET and POST	GET
Remove Header	ON: Parse the HTTP message returned by the server, and then output the payload to the serial port. OFF: Output the full http message returned by the server directly to the serial port.	ON
HTTP URL	The URL information of HTTP server	/1.php[3F]
Server Address	HTTP server address.	test.cn
Remote Port	The listening port of the HTTP server.	80
Timeout	If the set time is exceeded, the connection with the HTTP server will be disconnected. Range: 10~60s	10
Httpd Header	Header information of HTTP protocol.	Accept: text/html[0D][0A]

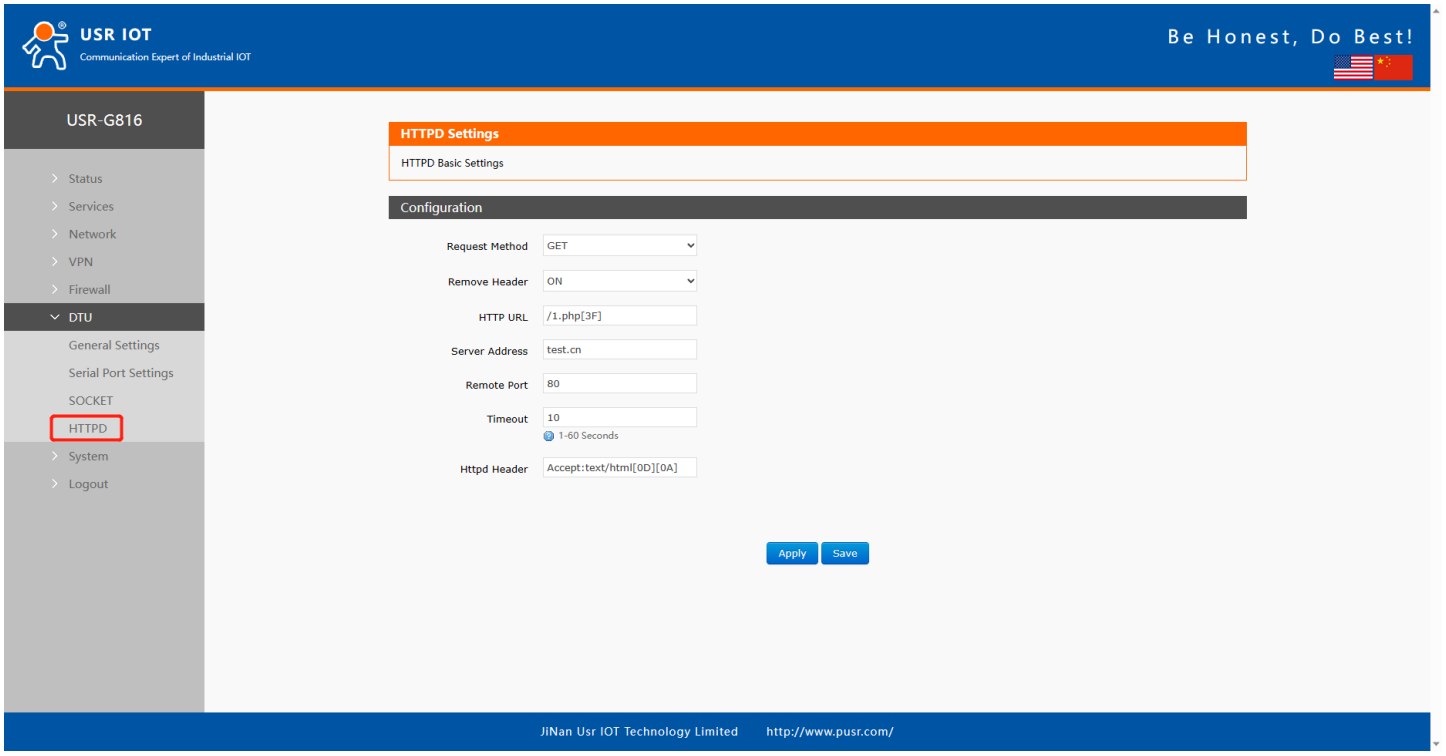

Figure 61. Settings of HTTPD

7.5. Modbus gateway setting and test

1> Enable MODBUS mode,

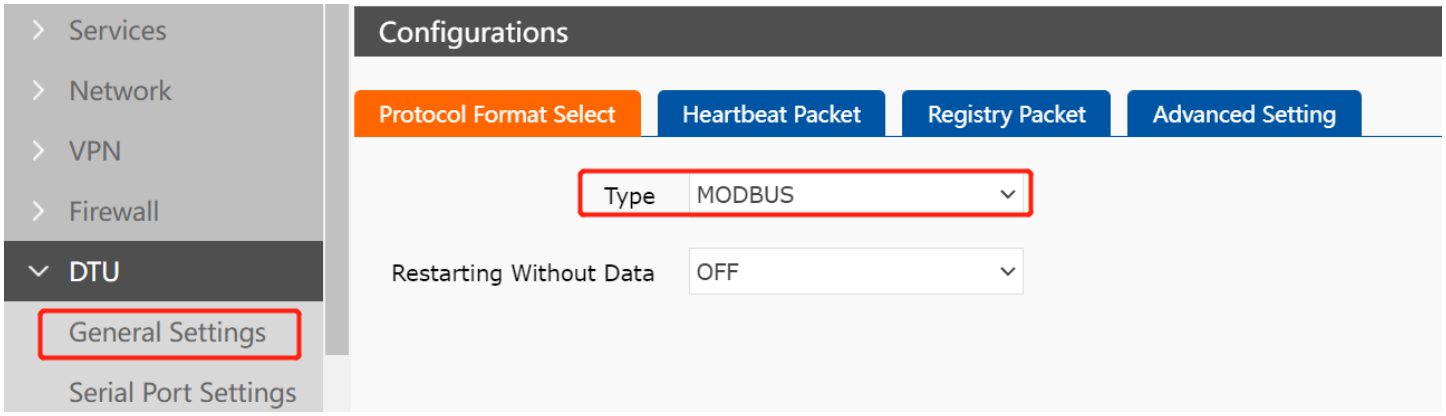

Figure 62. Enable MODBUS

2> Set Socket A settings,

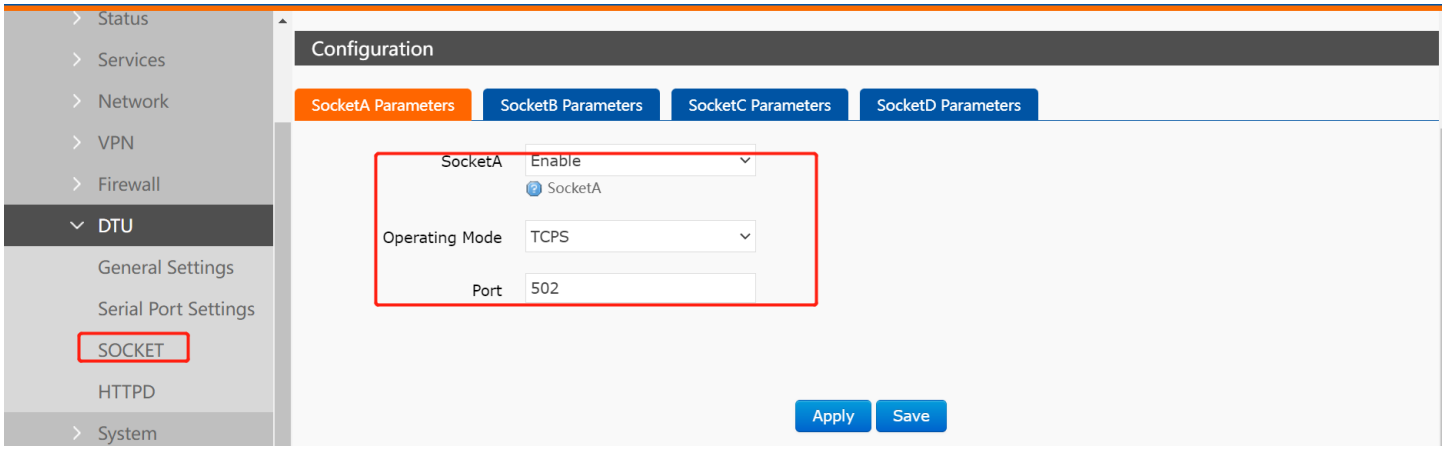

Figure 63. Modify settings of socket

3> Set Modbus poll software,

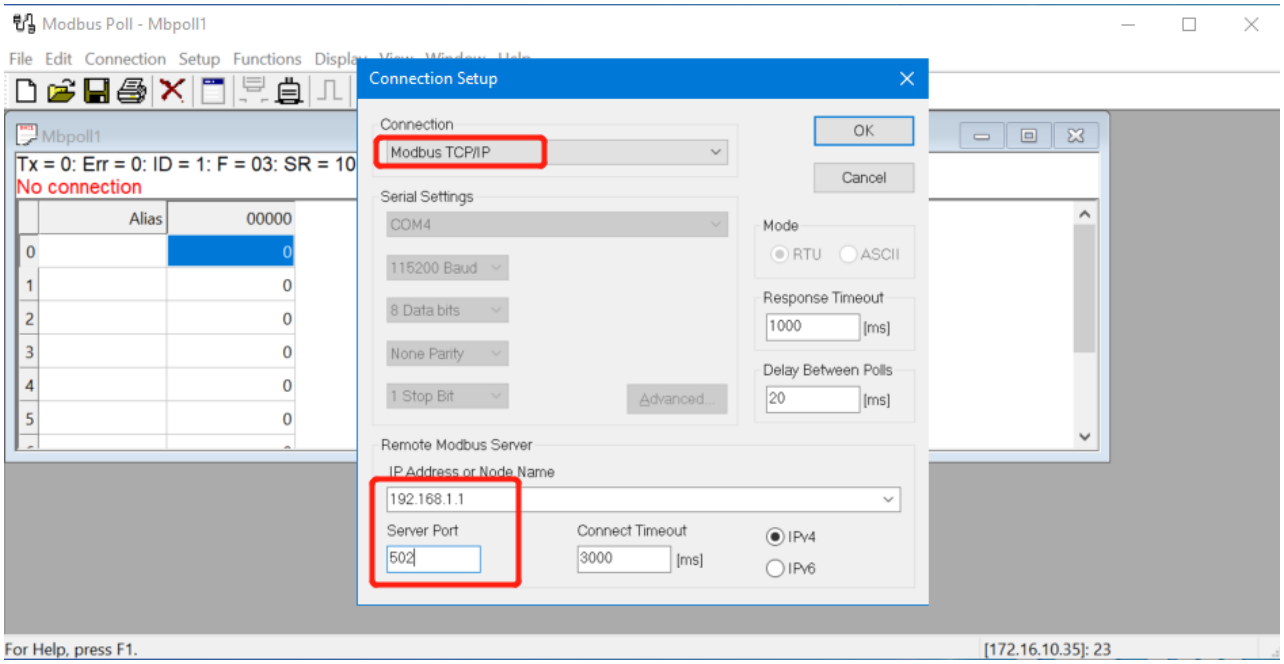

Figure 64. Modify settings of Poll

4> Set Modbus slave software,

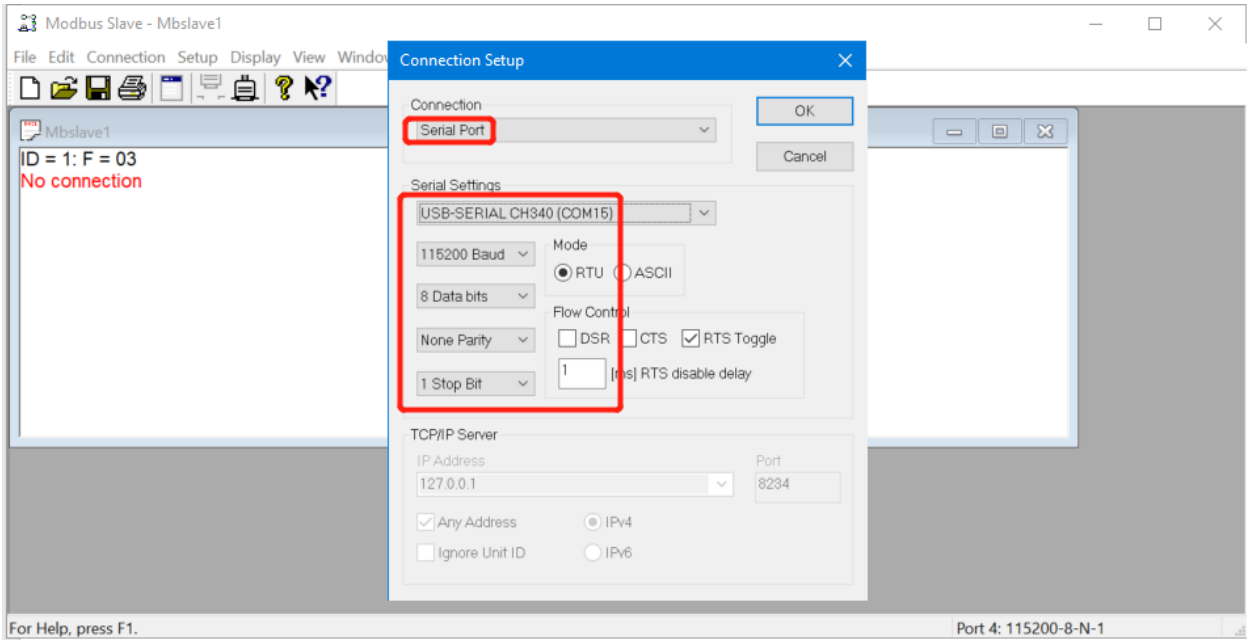

Figure 65. Modify settings of Poll

5> Test result.

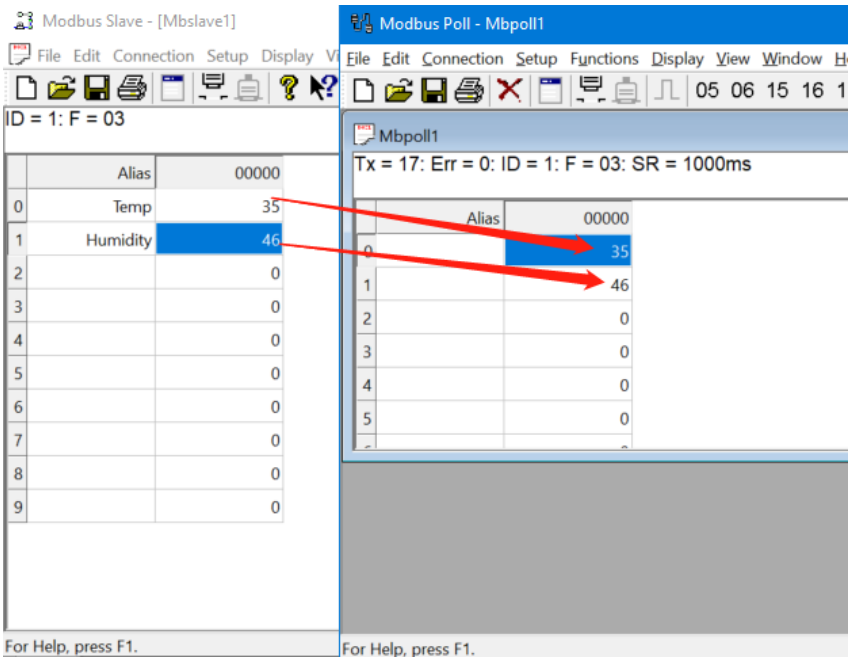

Figure 66. Modbus test result

7.6. Transparent data communication

1> Net mode setting,

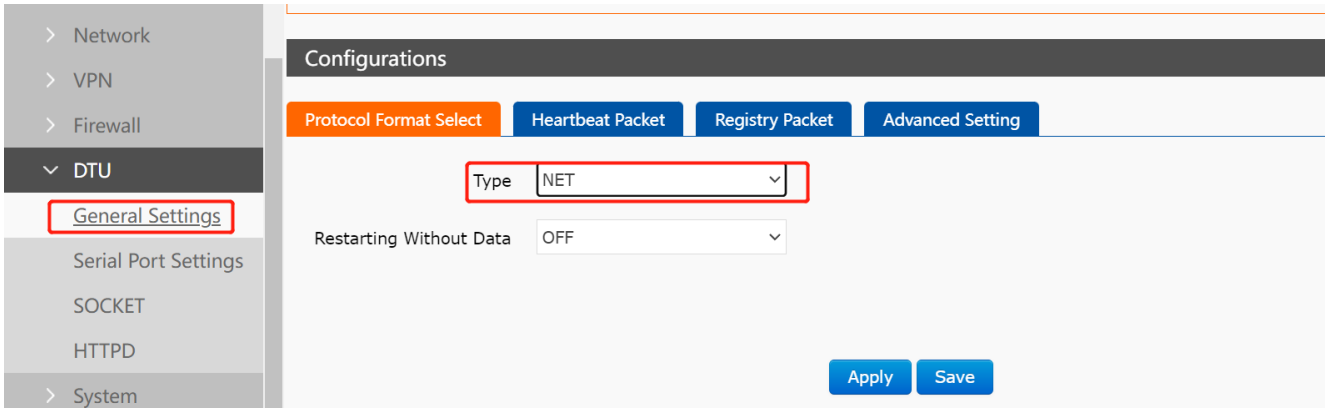

Figure 67. Enable NET mode

2> Socket settings,

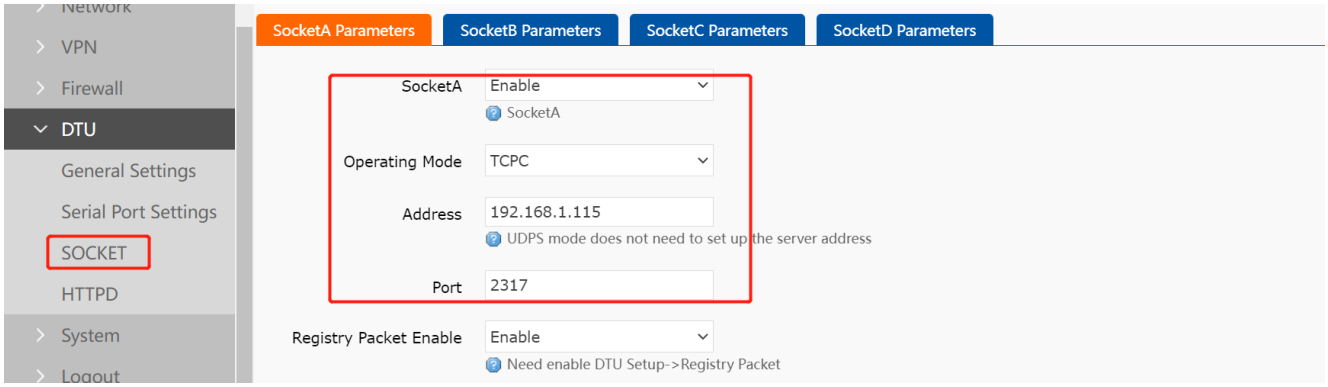

Figure 68. Modify settings of socket

3> Test result.

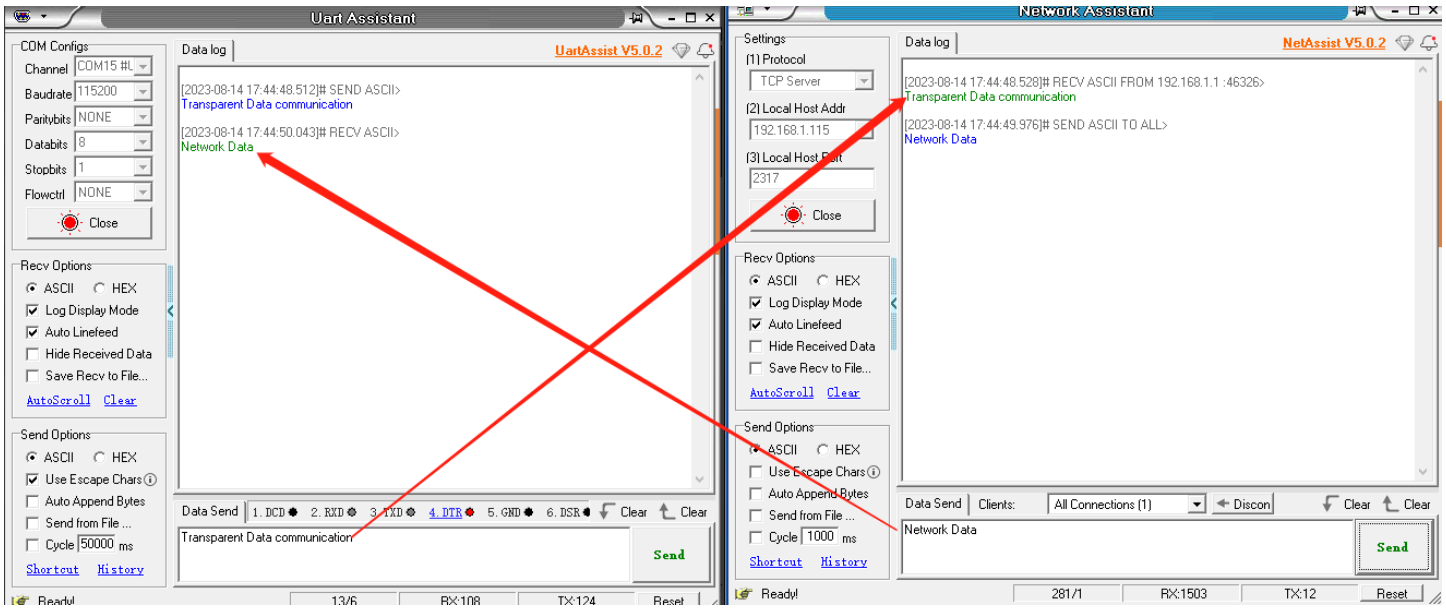

Figure 69. Data communication result

8. Additional services

8.1. PUSR Cloud

8.1.1. Add USR-G816 on PUSR Cloud

PUSR platform login address: **https://mp.usriot.com/**.

On USR-G816 side, users need enable the PUSR cloud first.

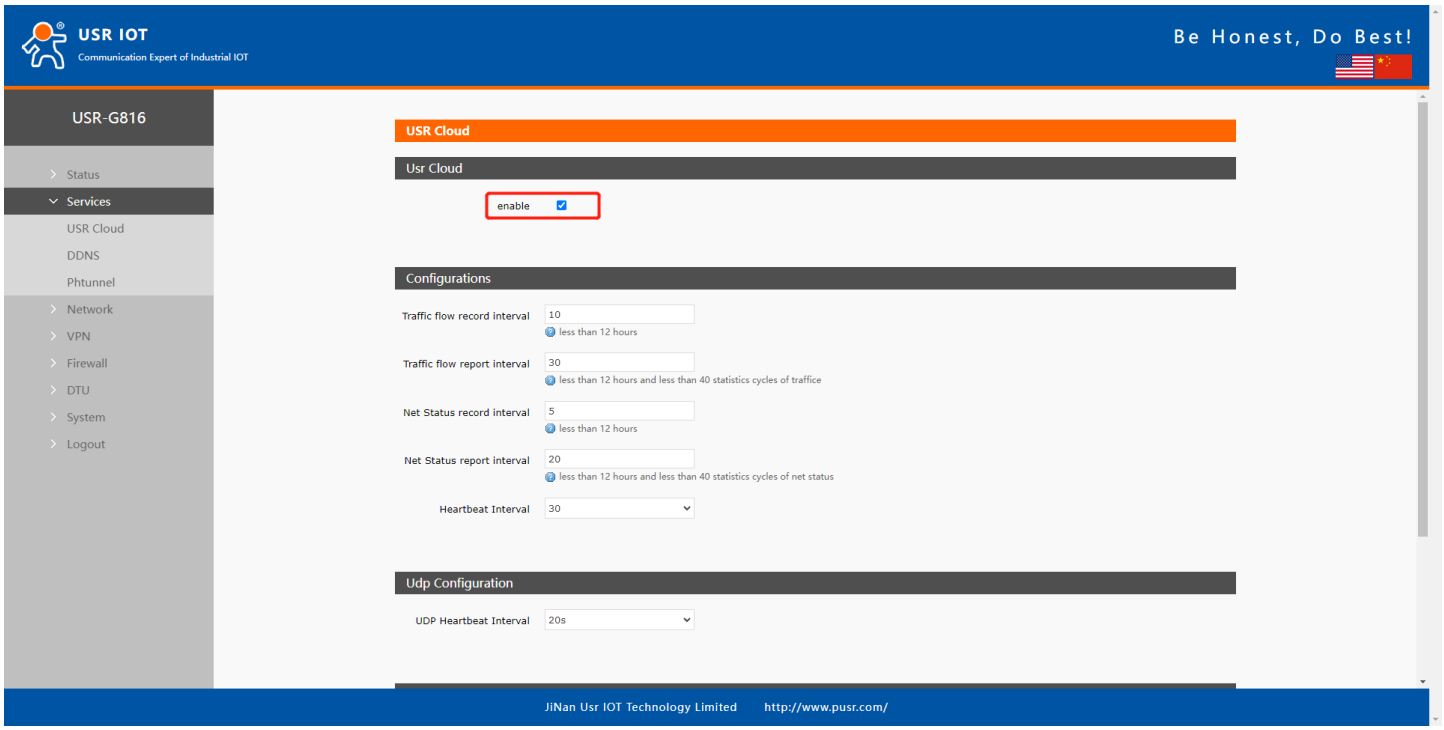

Figure 70. Enable the PUSR function of G816

On PUSR cloud side, users can add USR-G816 on PUSR platform and monitor the status of USR-G816.

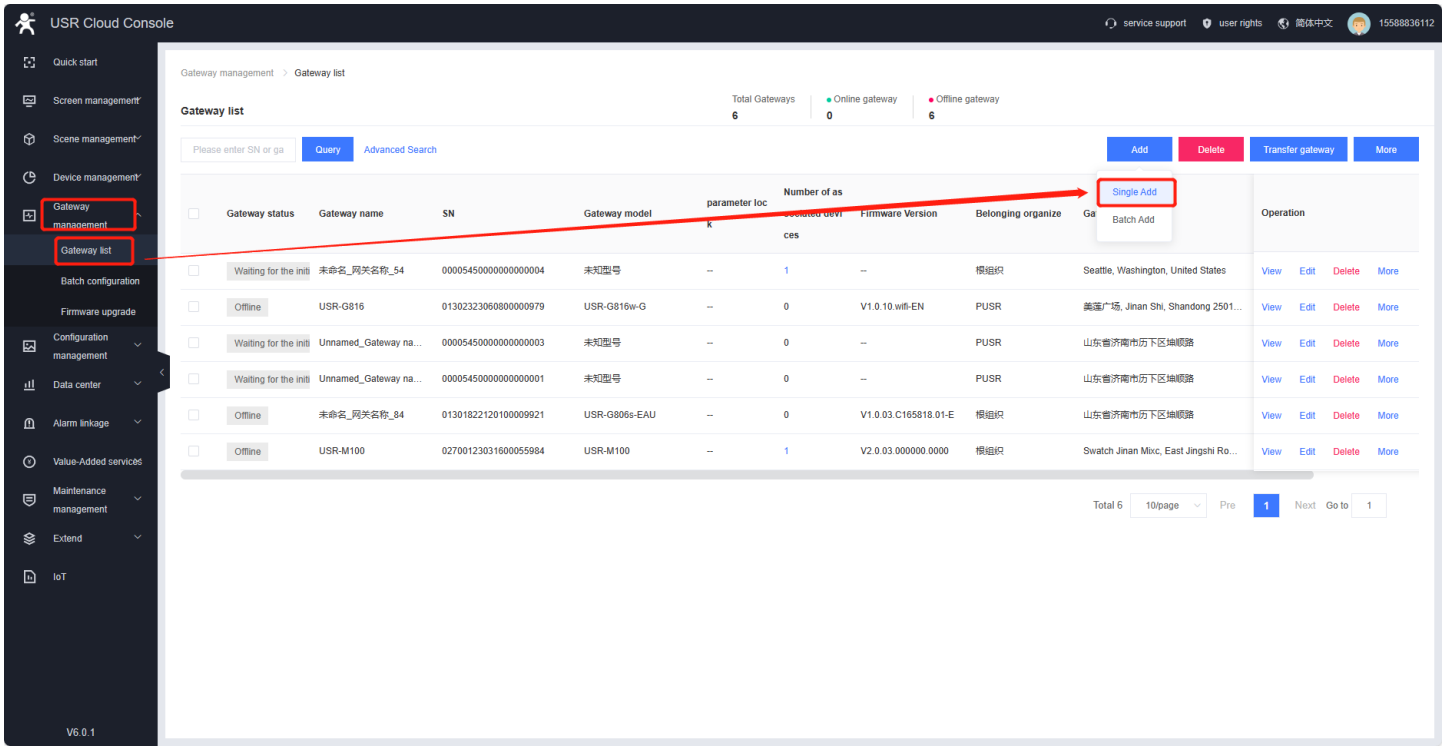

Figure 71. Add device on PUSR cloud

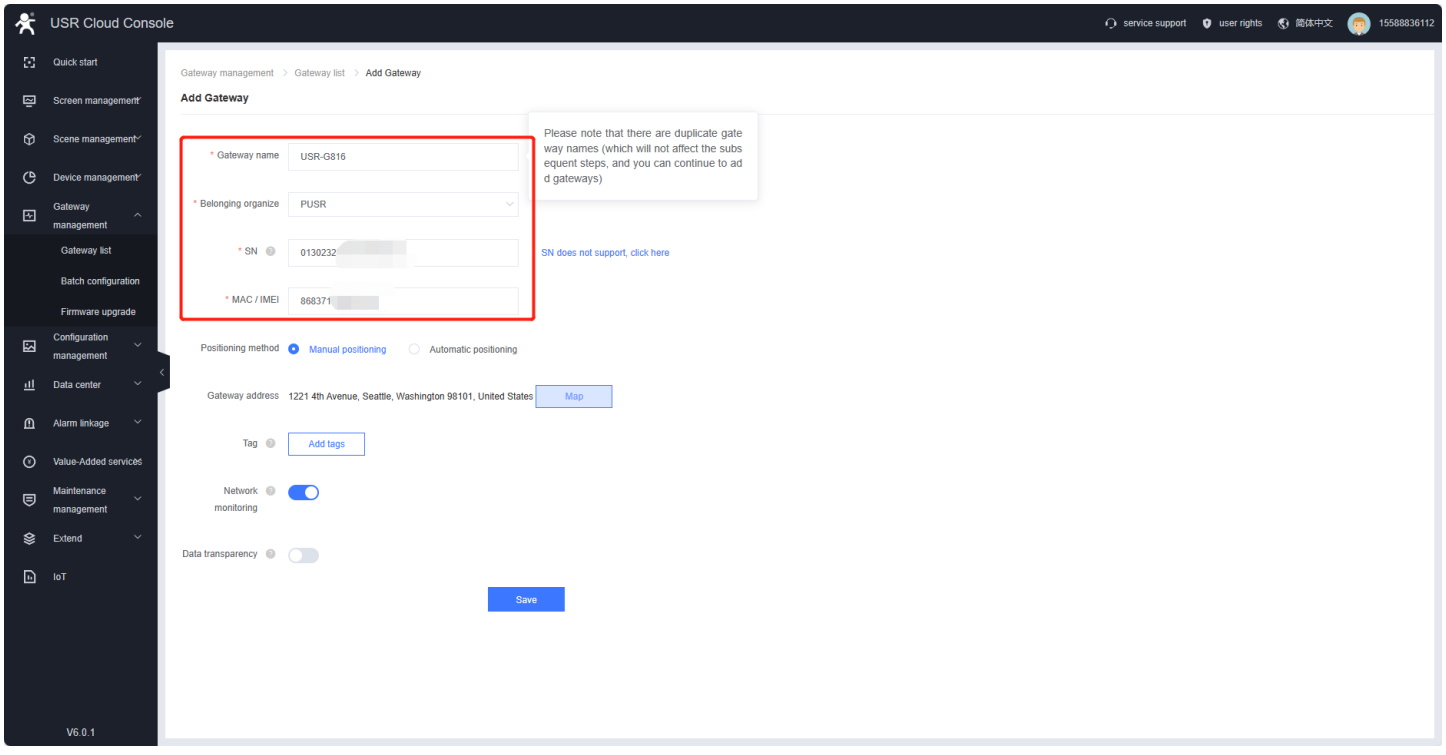

Figure 72. Enter the information of USR-G816

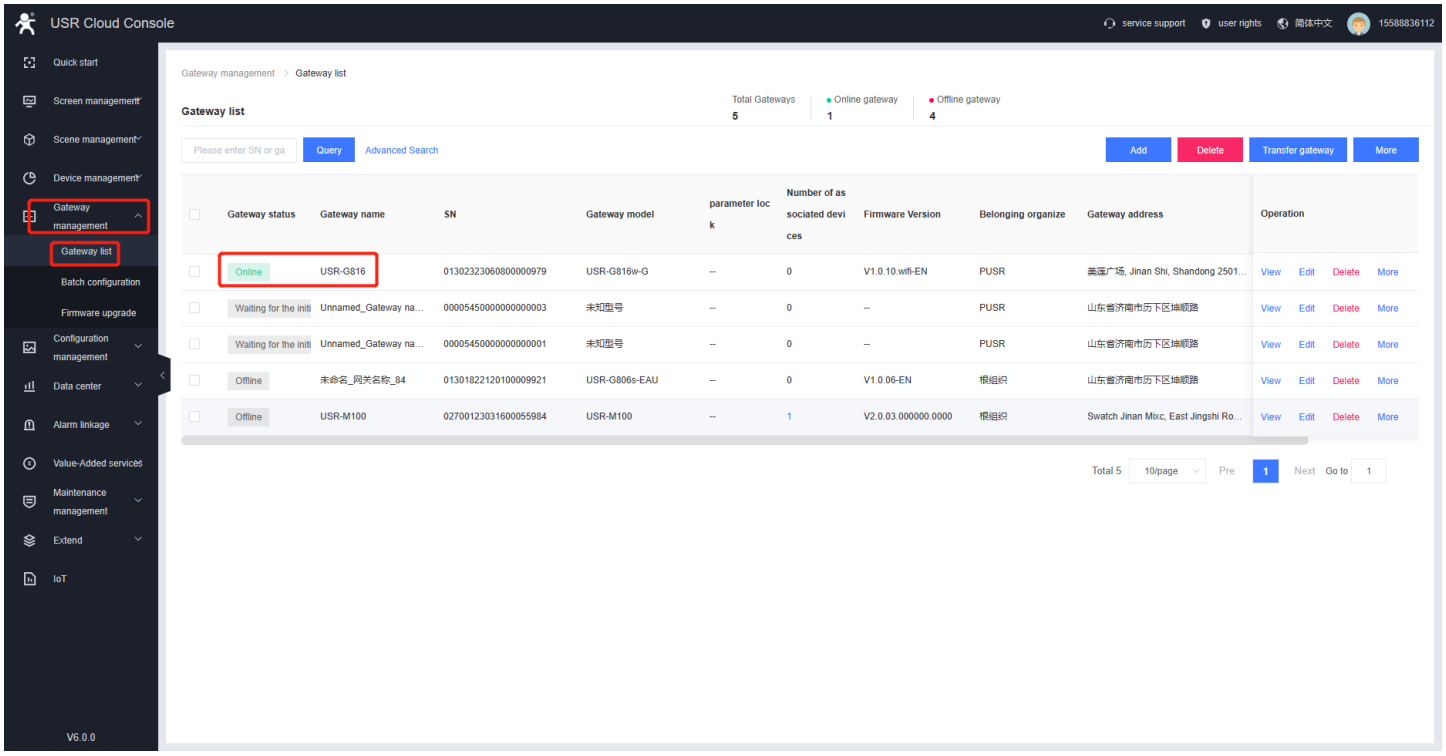

Figure 73. Online status

8.1.2. Gateway Information

Click “Gateway Name”, it will guide you to a new page showing the detail of the USR-G816.

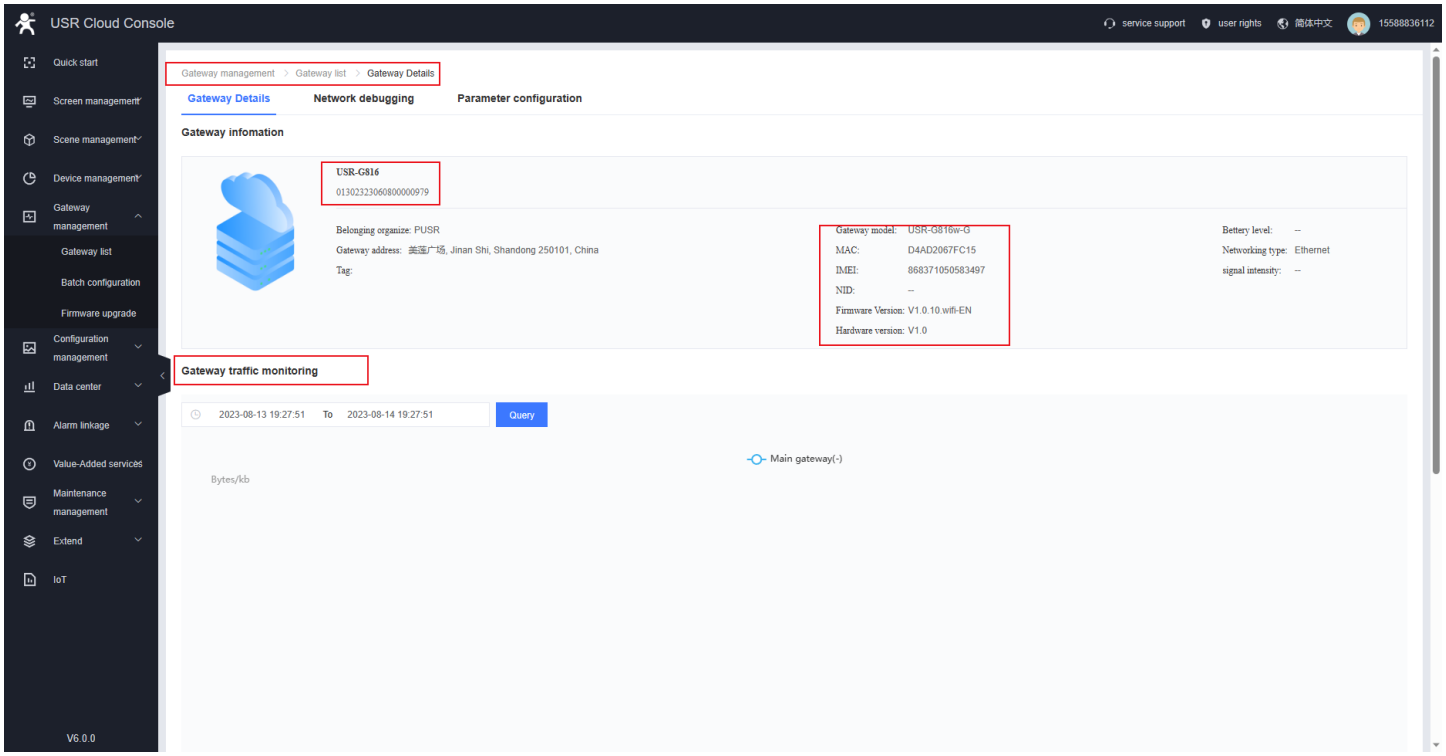

Figure 74. Check gateway information

Users can also send AT command to query parameters of USR-G816

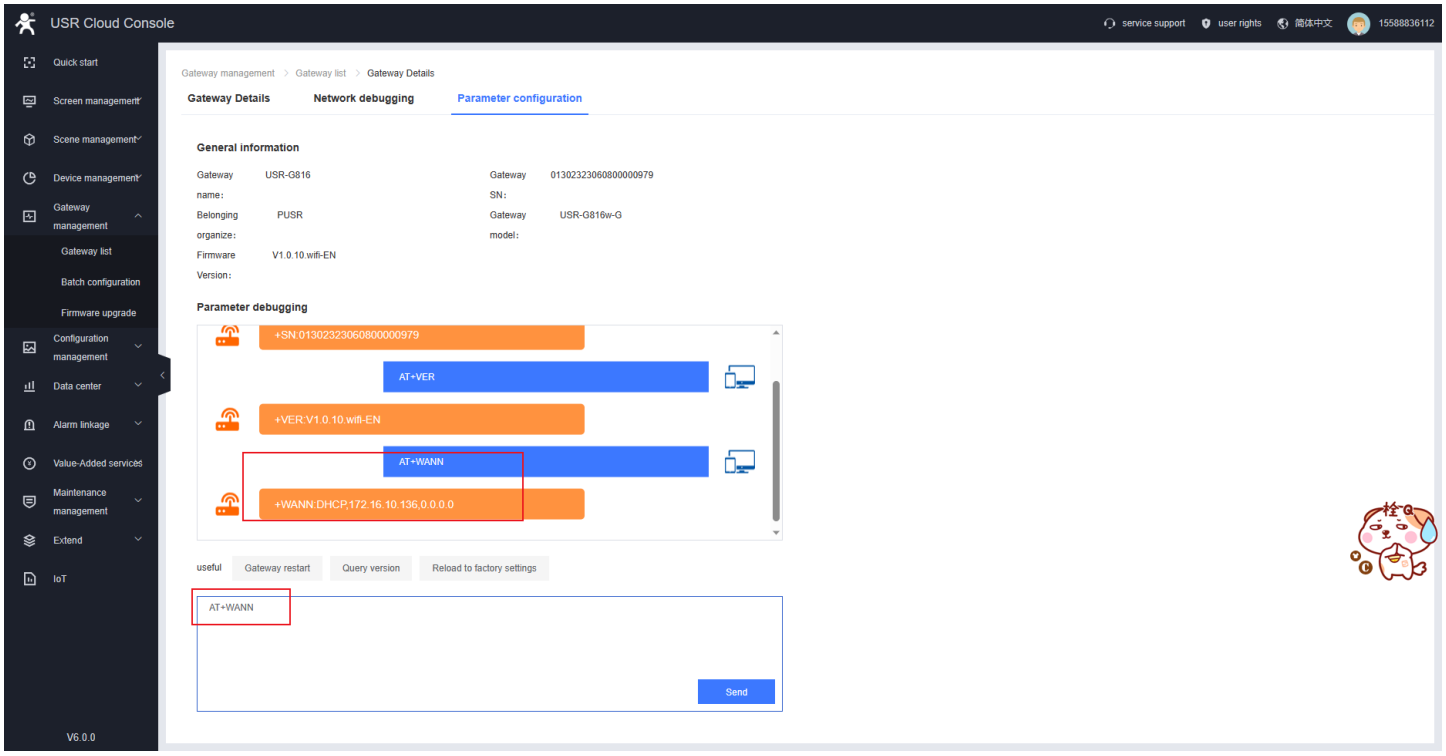

Figure 75. Parameters query and config

8.1.3. Remote access

After the USR-G816 is launched on the PUSR platform, you can remotely log in to the built-in webpage through the PUSR platform to view and modify parameters.

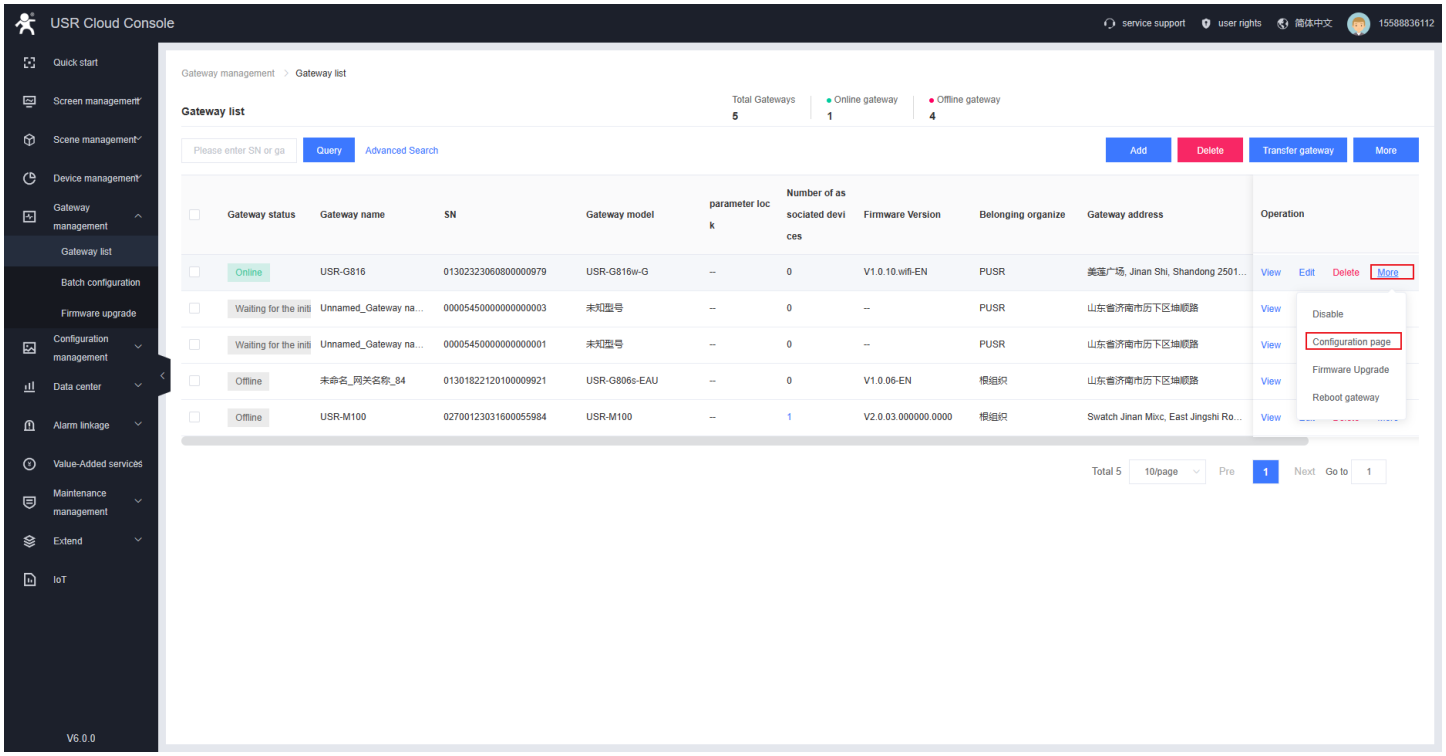

Figure 76. Login configuration page

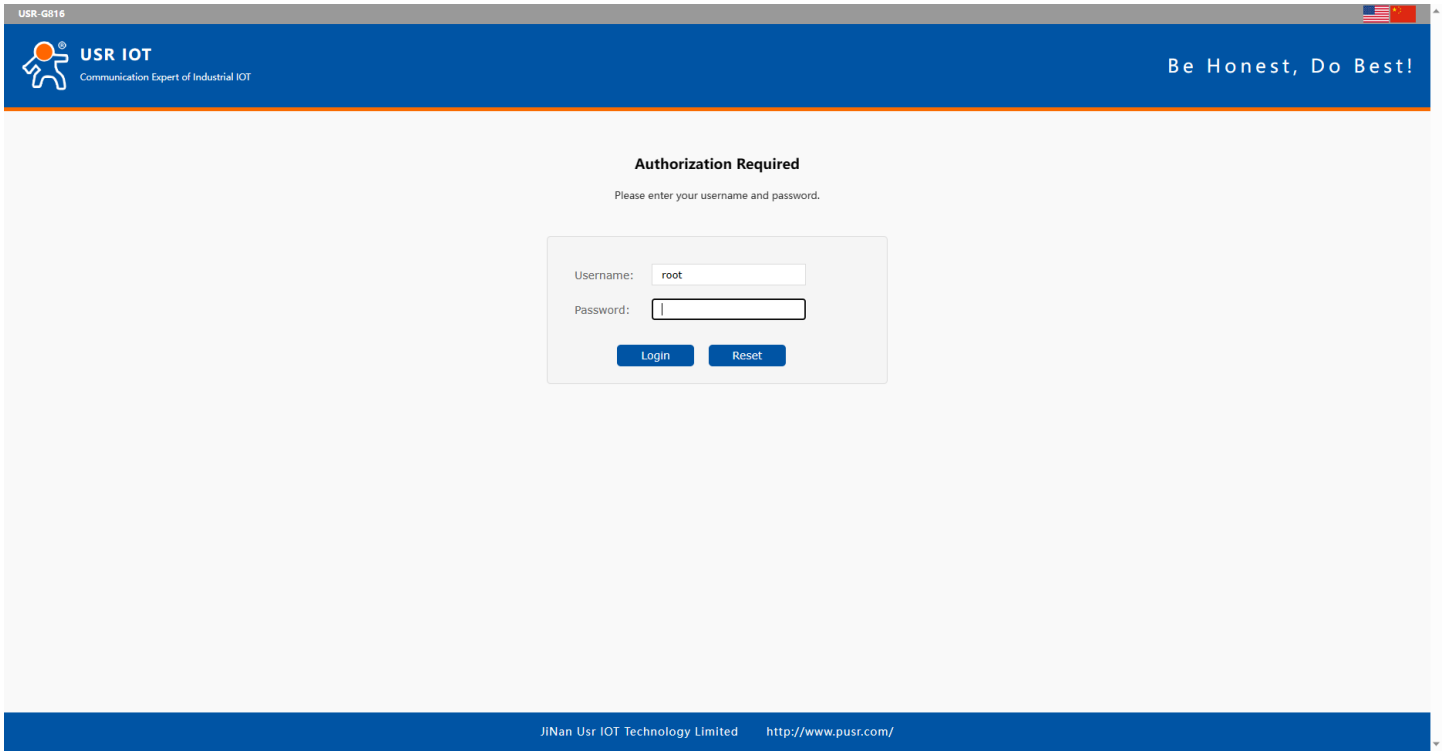

Figure 77. Login page

8.1.4. Firmware upgrade

Users can also upgrade firmware via PUSR platform.

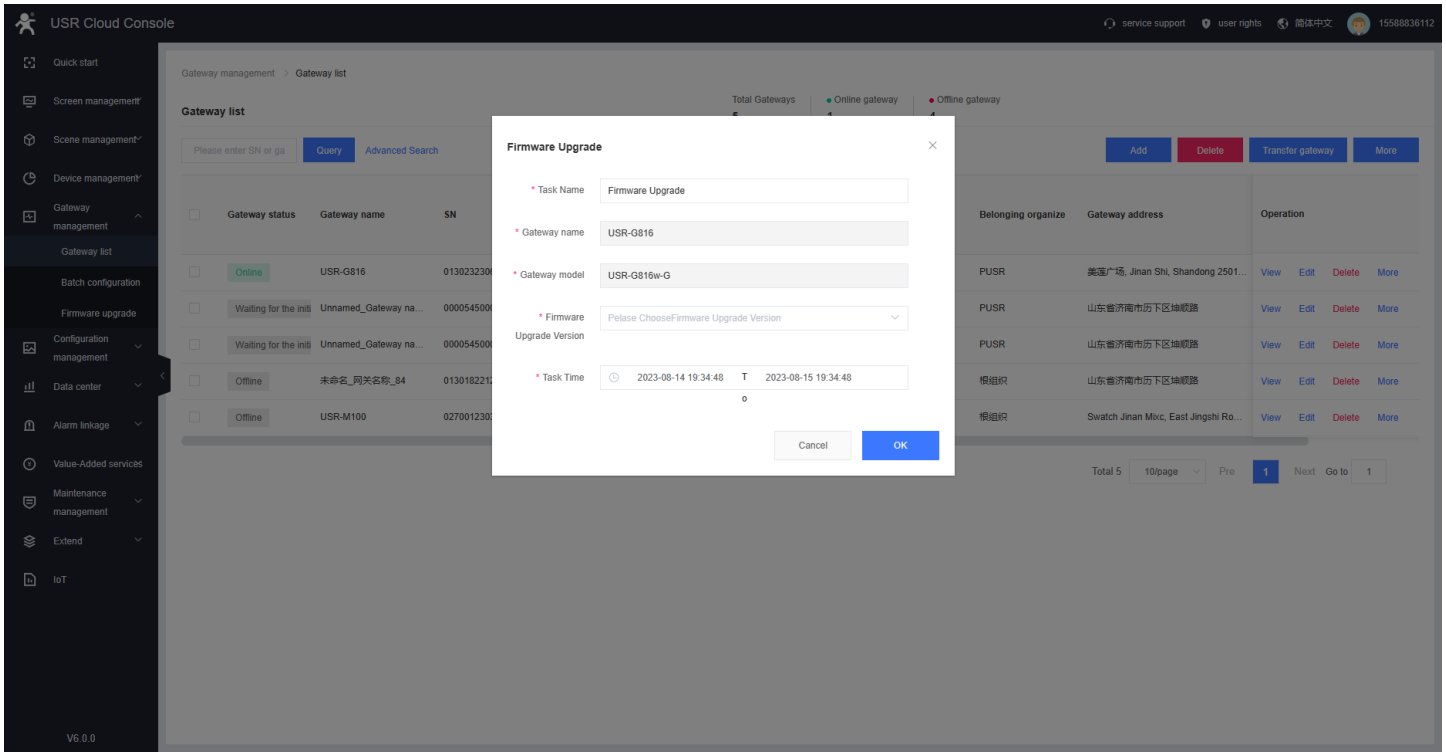

Figure 78. Firmware upgrade function

8.1.5. Alarm settings

➢ Add alarm trigger type, for USR-G816, we add “Gateway monitoring trigger”.

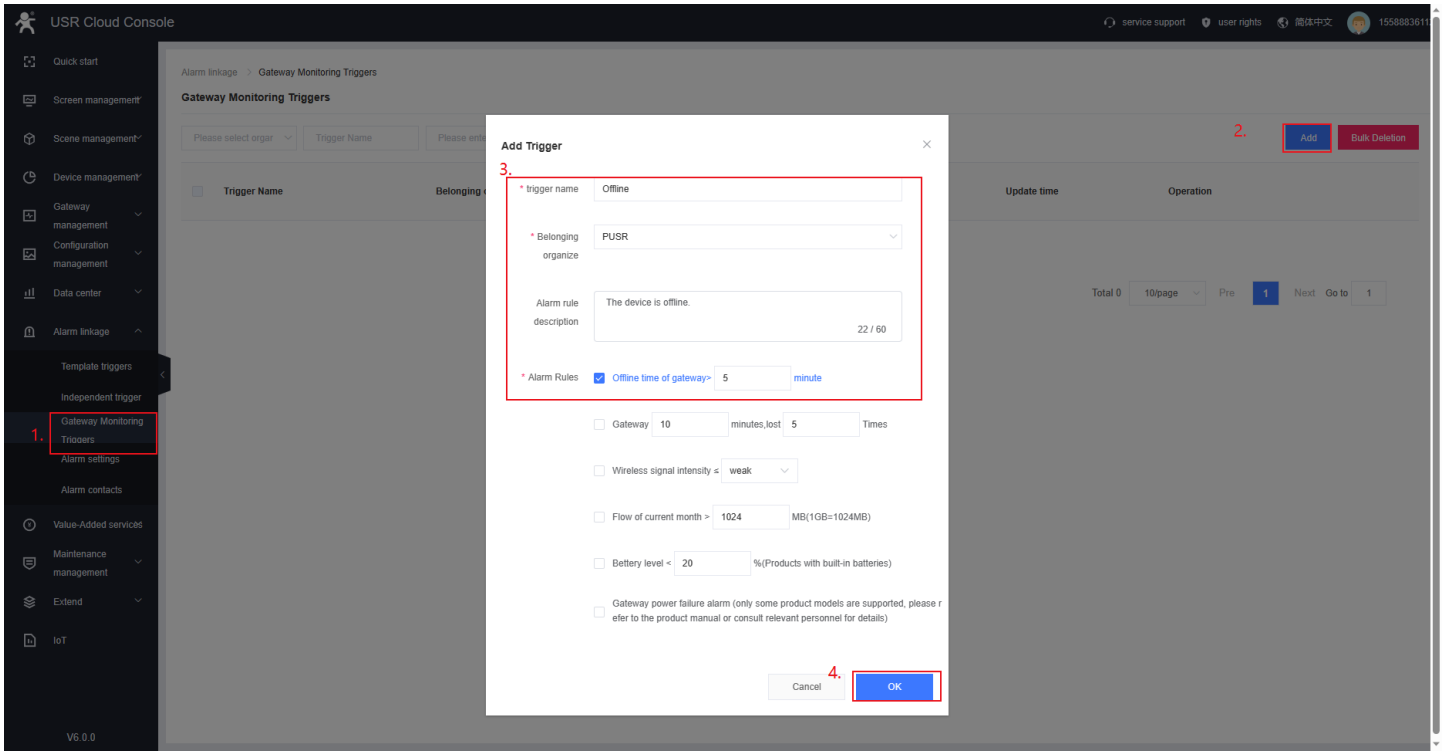

Figure 79. Add alarm trigger type

➢ Add alarm contacts and verify email.

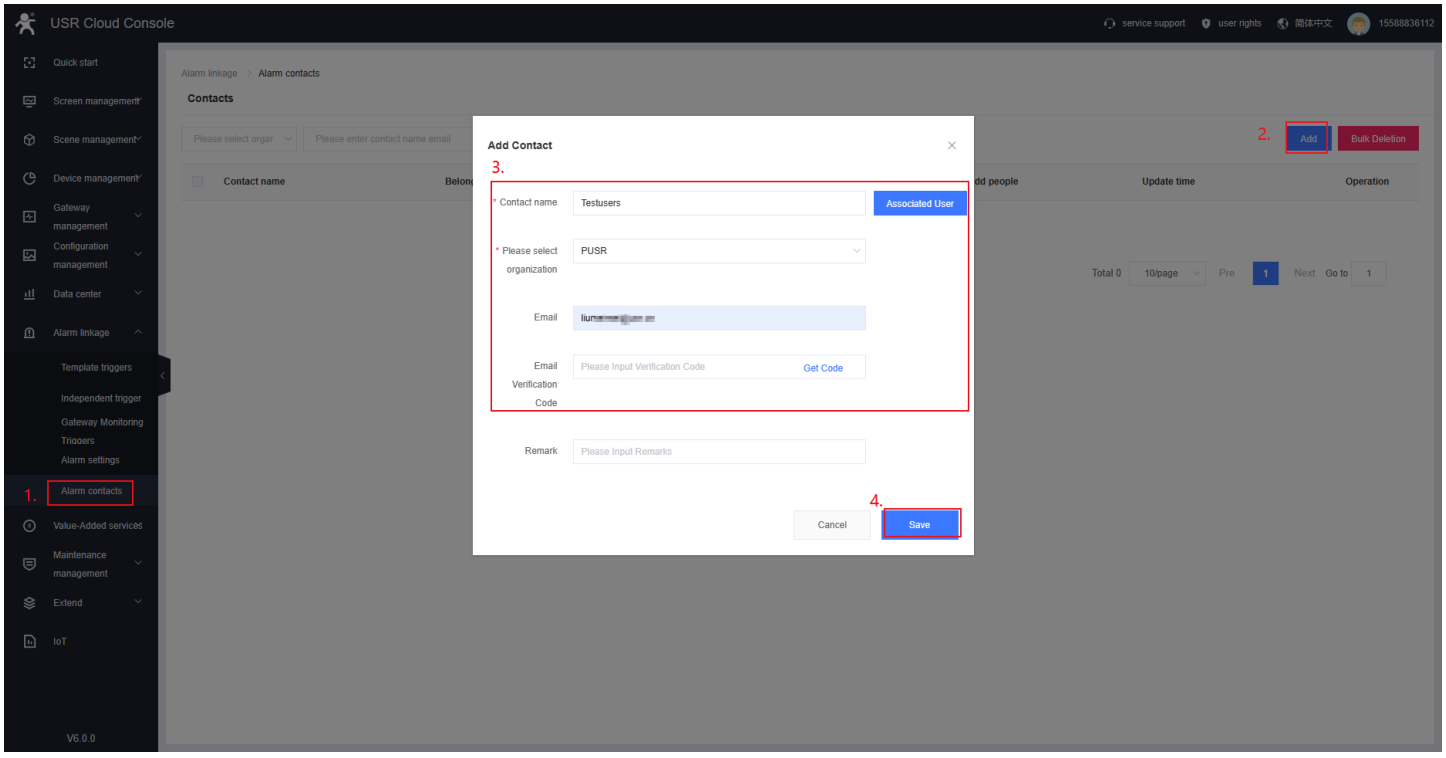

Figure 80. Add alarm contacts

➢ Add alarm configuration

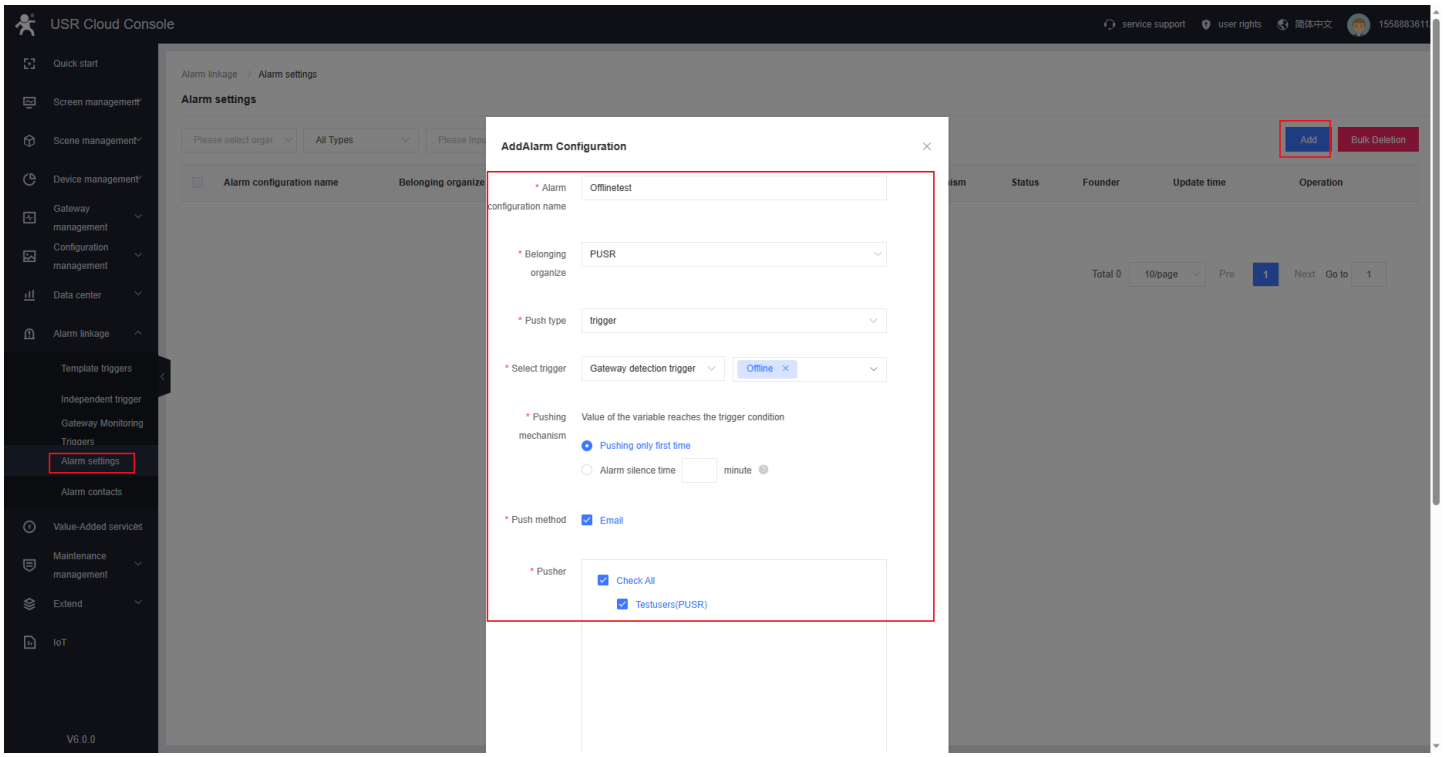

Figure 81. Add alarm configuration

➢ Check the alarm email: Power off the USR-G816

8.2. DDNS

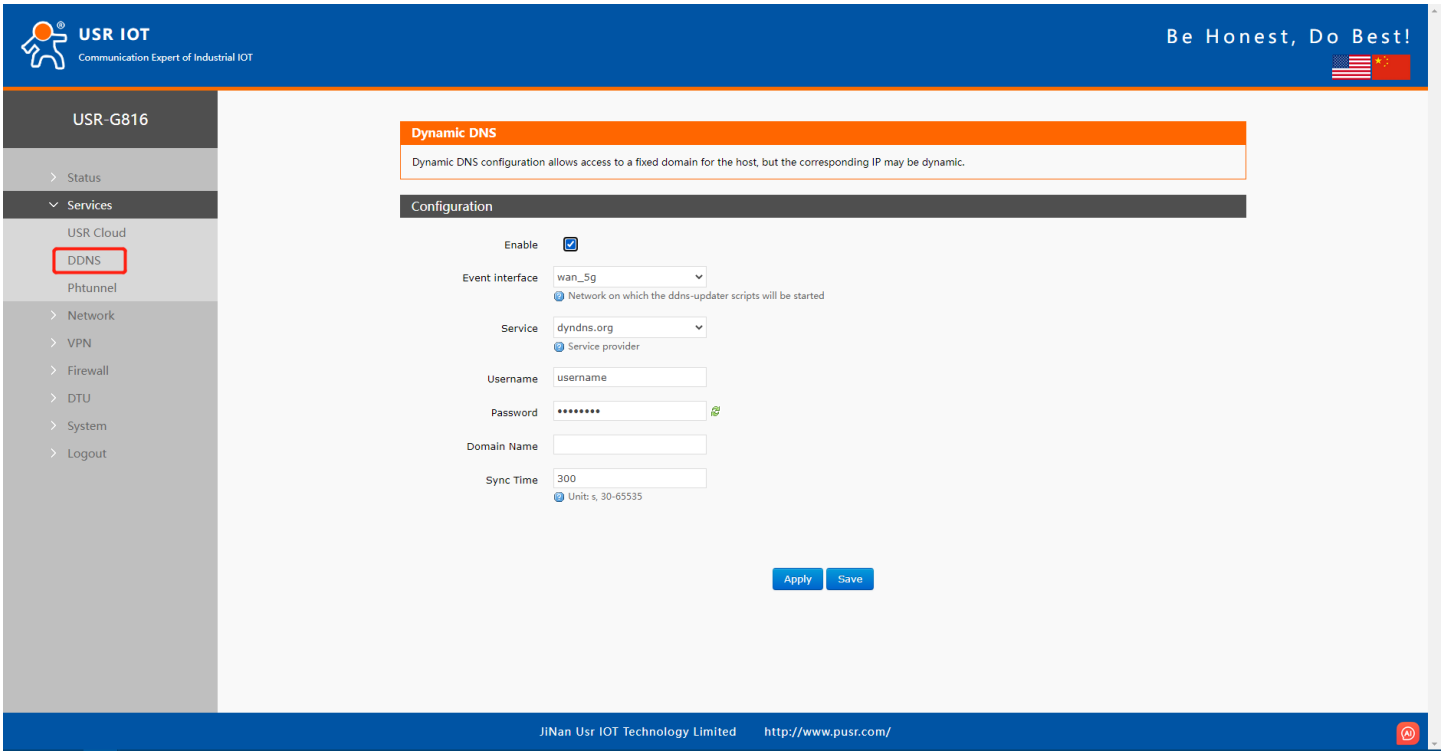

Figure 82. Enable DDNS

9. AT Command

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

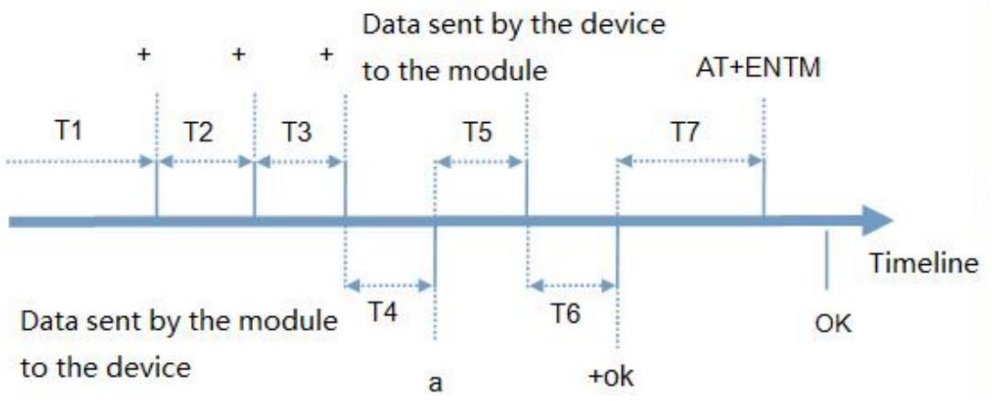

Figure 83. Sequence chart

Time sequence of switching from transparent mode to "AT Command mode":

1. Serial device continuously sends "+++" to the device. After receiving "+++", the device will send an "a" to the serial device.

2. No data can be sent during a packaging cycle before sending "+++".

3. When the serial device receives “a”, a “a” must be sent to the device within 3 seconds.

4. After receiving 'a', the device returns "+ok" and enter “temporary command mode”.

5. After receiving "+ok", the device has enter "temporary command mode" and now can send AT command to it.

6. Serial device sends command "AT+ENTM" to the PUSR device.

7. After receiving the command, the PUSR device sends "+OK" to the serial device and returns to the previous working mode.

8. When the serial device receives "+OK", it knows that the PUSR device has returned to the previous working mode.

9.1. Serial AT Commands

In transparent mode, we can directly send “Command Password+AT command” to query and configure the parameters without changing to command mode. The default password is test.cn#, the one in “7.1.4. Advanced settings (AT command password)”. Users can modify it in the following page.

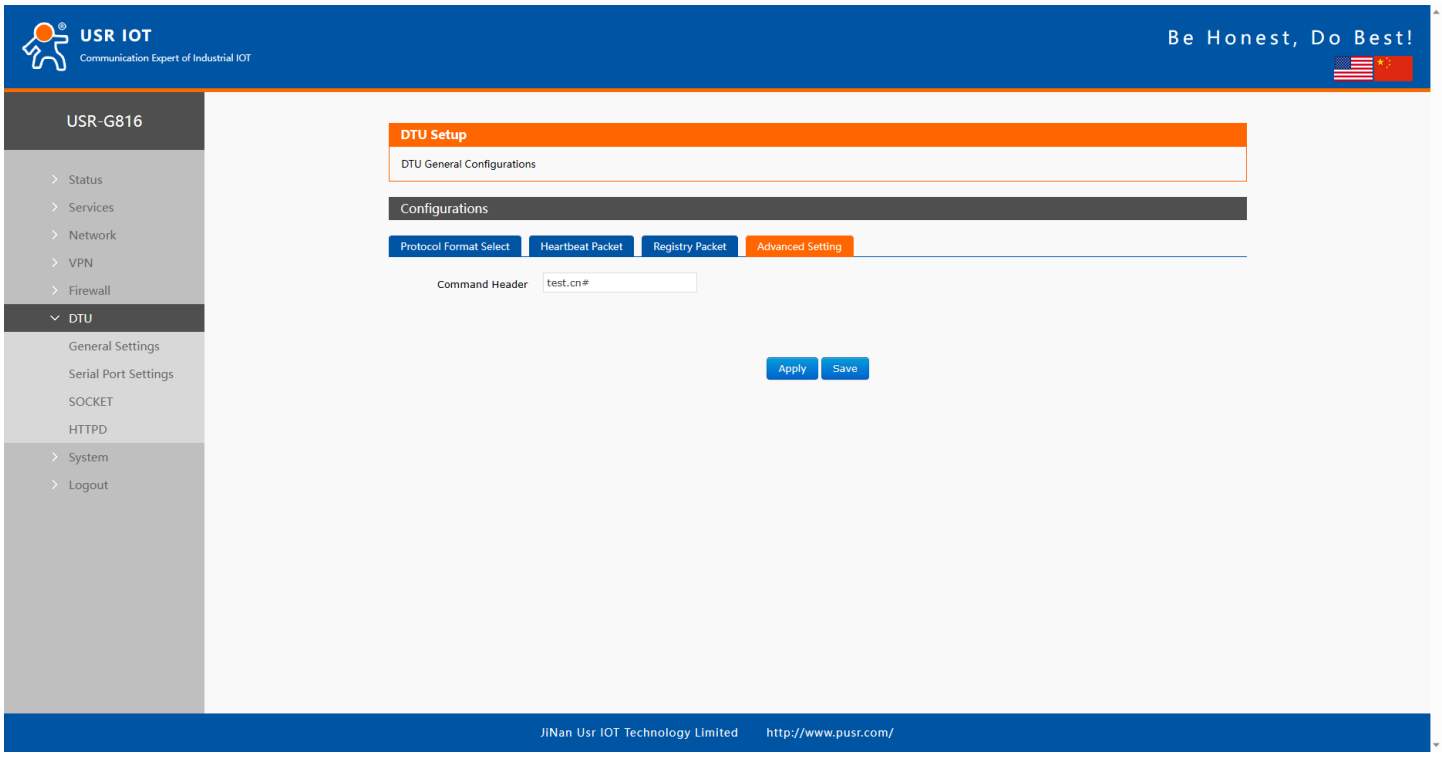

Figure 84. The default password

Send command to query parameters. Then send “test.cn#AT+WANN” from the serial port, we will receive the response from the module. (Please note there is a line feed after the command. User can also use “AT+CMDPW” to query or configure the command password.

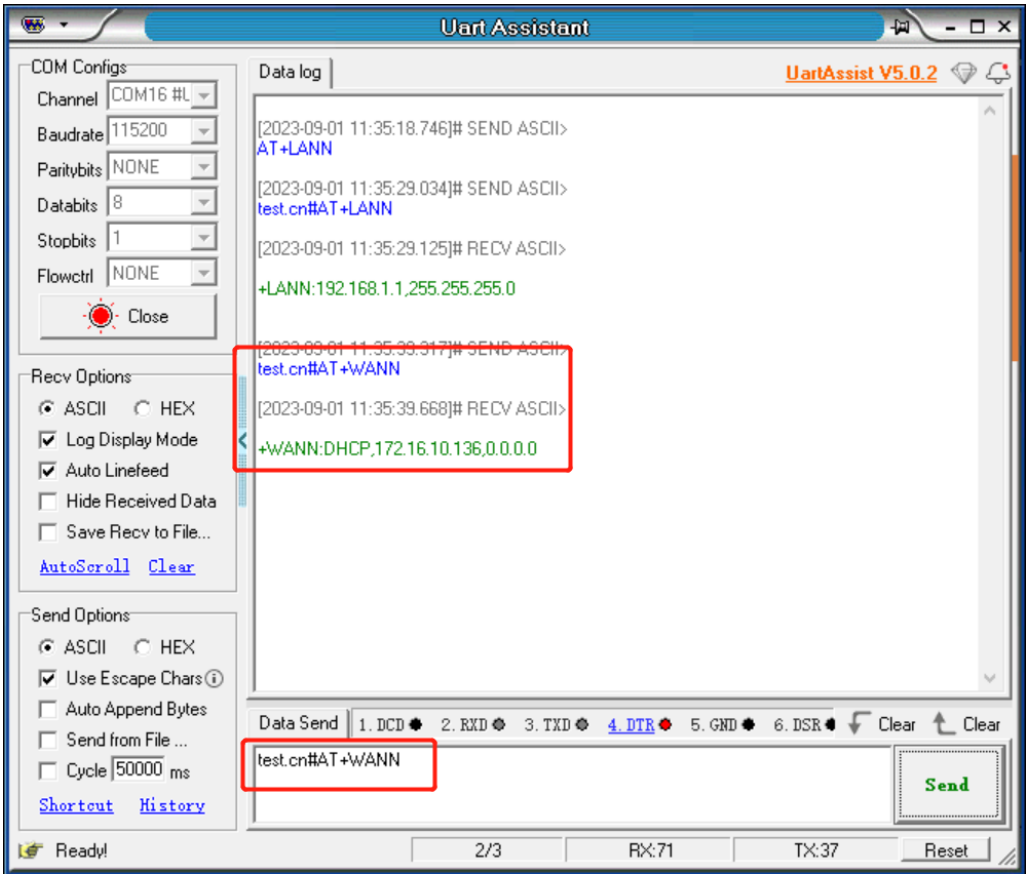

Figure 85. Serial AT command test

9.2. Network AT Command

In transparent mode, user can send "command password+AT command" to query and configure parameters. Network AT commands are used to query or configure the parameters from remote server, which is similar to serial AT commands. For example, we can send "www.usr.cn#AT+VER" to query the firmware version from server side (there is a line feed after the command).

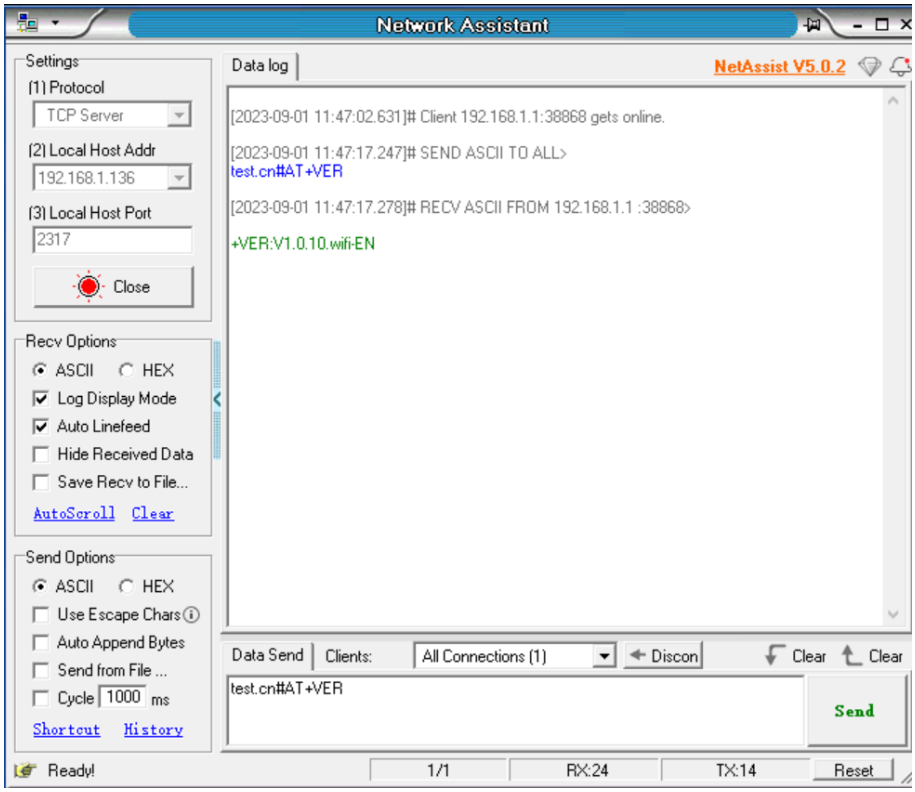

Figure 86. Network AT command test

10. Contact Us

Jinan USR IOT Technology Limited

Address : Floor 12 and 13, CEIBS Alumni Industrial Building, No. 3 Road of Maolingshan, Lixia District, Jinan, Shandong, China

Official website: https://www.pusr.com

Official shop: https://shop.usriot.com

Technical support: http://h.usriot.com/

Email : sales@usriot.com

Tel : +86-531-88826739

Fax : +86-531-88826739-808

11. Disclaimer

The information in this document provided in connection with Jinan USR IoT technology ltd. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of USR IoT products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, USR IoT AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING

TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL USR IoT AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF USR IoT AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. USR IoT and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. USR IoT and/or its affiliates do not make any commitment to update the information contained in this document.

Your Trustworthy Smart IOT Partner

PUSR®
www.pusr.com

Official Website: www.pusr.com

Official Shop: shop.usriot.com

Technical Support: h.usriot.com

Inquiry Email: inquiry@usriot.com

Skype & WhatsApp: +86 13405313834

关注有人微信公众号　登录商城快速下单

Click to view more: Product Catalog & Facebook & Youtube