



4G Wireless Router

User Manual

USR-G805s-42, USR-G805s-G



V2.0

Be Honest & Do Best

Your Trustworthy Smart Industrial IoT Partner

Content

1. Introduction	- 6 -
1.1. Features	- 6 -
1.2. Parameters table	- 6 -
1.3. Indicator introduction	- 8 -
1.4. Dimension	- 8 -
2. Get Started	- 9 -
2.1. Login router	- 9 -
2.2. Brief introduction of the webpage	- 10 -
3. Status & System	- 11 -
3.1. Status	- 11 -
3.2. System (Hostname)	- 11 -
3.3. Administration password	- 12 -
3.4. Reboot timer (Timed restart function)	- 13 -
3.5. NTP service	- 13 -
3.6. HTTP port	- 14 -
3.7. System log	- 14 -
3.8. Backup/Upgrade	- 16 -
3.9. Reboot	- 16 -
4. Network introduction	- 17 -
4.1. WAN interface	- 17 -
4.1.1. WAN_4G interface	- 17 -
4.1.2. WAN_WIRED interface	- 17 -
4.2. LAN interface	- 19 -
4.2.1. Basic configuration	- 19 -
4.2.2. VLAN enable	- 20 -
4.2.3. WAN/LAN switching	- 21 -
4.2.4. IPv6 configuration	- 21 -
4.3. Cellular network	- 23 -
4.3.1. Configuration	- 23 -
4.3.2. SIM1 configuration	- 24 -
4.3.3. SIM1/SIM2 configuration	- 25 -

4.3.4. Mobile information	- 26 -
4.4. Network failover	- 27 -
4.5. WLAN AP	- 28 -
4.5.1. Basic settings	- 28 -
4.5.2. Client information	- 29 -
4.6. WLAN STA	- 29 -
4.6.1. Basic settings	- 29 -
4.6.2. AP information	- 31 -
4.7. DHCP introduction	- 31 -
4.8. Static routes	- 31 -
4.8.1. Static routing adding	- 31 -
4.8.2. Routing table	- 32 -
4.9. Network diagnostics	- 33 -
4.10. TCP dump	- 34 -
5. VPN	- 34 -
5.1. PPTP Client	- 34 -
5.2. L2TP Client	- 36 -
5.3. IPSec VPN	- 37 -
5.4. OpenVPN	- 39 -
5.4.1. OpenVPN client	- 40 -
5.4.2. OpenVPN server	- 42 -
5.5. GRE	- 42 -
6. Firewall	- 43 -
6.1. General Settings	- 43 -
6.2. Port forward	- 44 -
6.2.1. Port forward	- 44 -
6.2.2. DMZ function	- 45 -
6.3. Traffic rules	- 46 -
6.3.1. Open ports on router	- 47 -
6.3.2. Add new forward rule	- 48 -
6.3.3. Source NAT	- 49 -
6.4. Access restrictions	- 51 -

6.4.1. Blacklist settings	- 52 -
6.4.2. Whitelist settings	- 52 -
7. Additional services	- 53 -
7.1. PUSR Cloud	- 53 -
7.1.1. Add USR-G805s on PUSR Cloud	- 53 -
7.1.2. Gateway Information	- 55 -
7.1.3. Remote access	- 56 -
7.1.4. Firmware upgrade	- 57 -
7.1.5. Alarm settings	- 58 -
7.2. DDNS	- 60 -
7.3. SSH function	- 60 -
7.4. SNMPD	- 60 -
7.5. SMS	- 61 -
8. AT Command	- 63 -
8.1. AT command set	- 63 -
8.2. Description of AT command	- 64 -
8.2.1. AT	- 64 -
8.2.2. AT+R	- 64 -
8.2.3. AT+CLEAR	- 64 -
8.2.4. AT+VER	- 64 -
8.2.5. AT+MAC	- 65 -
8.2.6. AT+APN	- 65 -
8.2.7. AT+SN	- 65 -
8.2.8. AT+CSQ	- 66 -
8.2.9. AT+CPIN	- 66 -
8.2.10. AT+IMEI	- 66 -
8.2.11. AT+ICCID	- 66 -
8.2.12. AT+MCCMNC	- 66 -
8.2.13. AT+SYSINFO	- 67 -
8.2.14. AT+CELLULAR	- 67 -
8.2.15. AT+NETMODE	- 67 -
8.2.16. AT+WEBU	- 67 -

8.2.17. AT+PLANG	- 67 -
8.2.18. AT+UPTIME	- 68 -
8.2.19. AT+WANINFO	- 68 -
8.2.20. AT+DIALINFO	- 69 -
8.2.21. AT+LANINFO	- 69 -
8.2.22. AT+WANN	- 70 -
8.2.23. AT+LANN	- 70 -
8.2.24. AT+LAN	- 70 -
8.2.25. AT+PING	- 70 -
8.2.26. AT+NETSTATUS	- 71 -
8.2.27. AT+ALYSIMSWITCH	- 71 -
8.2.28. AT+DUALSIMMODE	- 71 -
9. Contact Us	- 72 -
10. Disclaimer	- 72 -

1. Introduction

1.1. Features

Stable and reliable

- ◆ Industrial grade design for harsh environments, IP30 metal housing.
- ◆ Qualcomm processor, to ensure powerful performance.
- ◆ Support wall mounting and flat surface placement.
- ◆ Wide input voltage range 9~36VDC, reverse polarity protection.
- ◆ Multiple EMC protection level 2: 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 global mainstream 4G band, can work in global area.
- ◆ Equipped with 5 Ethernet ports: 1*WAN, 1*WAN/LAN (Switchable), 3*LAN.
- ◆ Supports 2.4G Wi-Fi, AP/STA/bridge mode, flexible networking.

Powerful function

- ◆ Supports 4G APN/VPDN sim cards.
- ◆ 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, Ipsec, GRE and enhanced OpenVPN.

1.2. Parameters table

Table 1. Parameters of USR-G805

USR-G805 specifications		
Cellular Interface	Frequency	4G LTE LTE-FDD: B1/2/3/4/5/7/8/12/13/18/19/20/25/26/28/66; LTE-TDD: B34/38/39/40/41; WCDMA: B1/2/4/5/6/8/19; GSM/EDGE: B2/3/5/8;

	Maximum Transmission	LTE-FDD (Mbps) :150 (DL)/50 (UL)
	Data Rate	LTE-TDD (Mbps):130 (DL)/30 (UL)
	Antennas	1 x SMA-K Connectors (Center PIN: SMA Female)
	SIM Slot	2 x (3 V/1.8 V) Nano-SIM(4FF) Push-push type slot
Ethernet Interface	WAN	2 x WAN ports, RJ45, 10/100 Mbps, the WAN2 port can be configure as LAN port, supports auto MDI/MDIX crossover, Ethernet Isolation 1.5 KV
	LAN	3 x RJ45 port, 10/100 Mbps, supports auto MDI/MDIX crossover, Ethernet Isolation 1.5 KV
Indicators	PWR	red, always on after powered on
	WLAN	green, always solid on when WiFi is enabled and working properly
	NET	ON: Signal strength 25-31 (signal strong) Blinking: Signal strength 15-24 (signal strength is basically normal, and equipment maybe disconnect with the base station) OFF: Signal strength 1-14 (Signal strength is weak, please check antenna and the signal strength of current location)
	Antennas	1 x SMA-K Connectors (Center PIN: SMA Male)
Wi-Fi Interface	Standards	IEEE 802.11b/g/n (2.4GHz)
	Modes	AP/AP+STA/AP+WDS repeater
	Data speed	Up to 150 Mbps
	Security	Wi-Fi security with mixec-psk, psk+ccmp, psk2, psk2+tkip
	Transmission distance	150 meters by line of sight. Actual transmission distance depends on environment of the site.
	Adapter	DC 12V/1A
Power Supply	Connector	DC Power Jack Barrel Type Female 5.5*2.1mm Round socket
	Input voltage range	DC9-36V
	Power consumption	Max 700mA@12C Average 376mA@12V
Physical Characteristics	Casing material	Metal shell, ingress protection IP30
	Dimensions	127.0*84.0*27.0mm (L*W*H, antenna pedestal, terminal block and DIN Rail are not included)
	Installation	Desktop, wall mounting
	EMC	Static IEC61000-4-2, level 2 Pulsed Electric Field IEC61000-4-4, level 2 Surge IEC61000-4-5, level 2
	Operating Temperature	-20°C ~ +70°C
	Storage Temperature	-40°C ~ +125°C (Non-condensing)
	Relative Humidity 0	5%~95% (Non-condensing)
Others	Reload button	1 x 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, OpenVPN, Ipsec, GRE

	Security	Access Control, DMZ, Port Forwarding, SYN-Flood Protection, Filtering (IP& MAC & Domain)
	Management	Web UI, PUSR cloud
	Reliability	WAN Failover, Dual SIM Backup
Certificate	In progress	CE, *FCC, *WEEE, RoHS, *RCM, *WPC

1.3. Indicator introduction

USR-G805s provides 3 indicators in total, the specific description is as follows.

Table 2. LED indicator

Name	Description
PWR(Red)	On: power supply is normal. Off: No power supply or abnormal power supply.
WLAN(Green)	green, always solid on when WiFi is enabled and working properly
Cellular(Green)	ON: Signal strength 25-31 (signal strong) Blinking: Signal strength 15-24 (signal strength is basically normal, and equipment maybe disconnect with the base station) OFF: Signal strength 1-14 (Signal strength is weak, please check antenna and the signal strength of current location)

1.4. Dimension

- Sheet metal housing, wall mounting supported.
- 127.0*84.0*27.0mm (L*W*H, accessories not included)

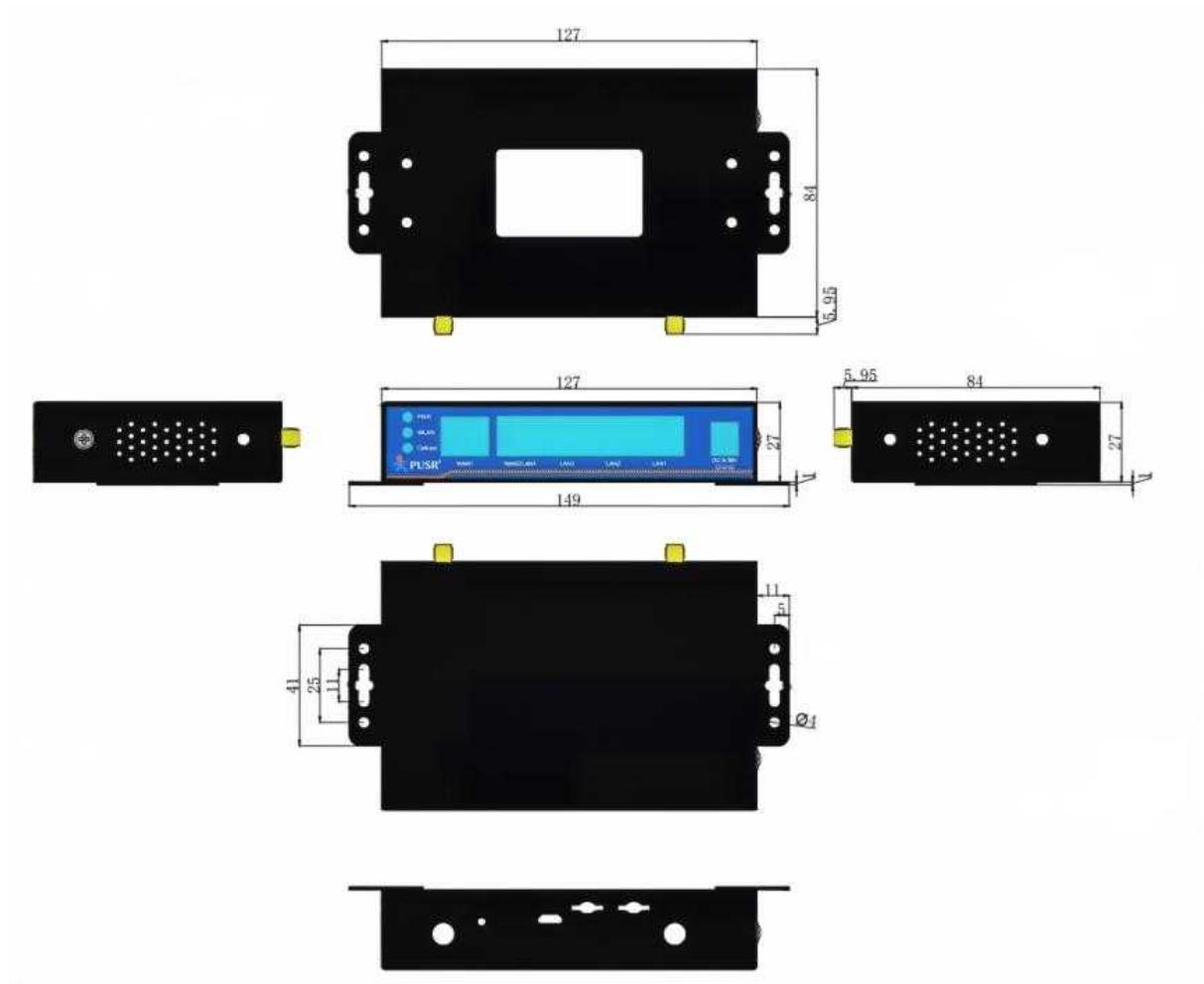


Figure 1. Dimension of USR-G805s

2. Get Started

2.1. Login router

Power on the G805s router, connect PC to USR-G805s 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-G805s-xxxx
LAN IP	192.168.1.1
Username	admin
Password	admin
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-G805s.

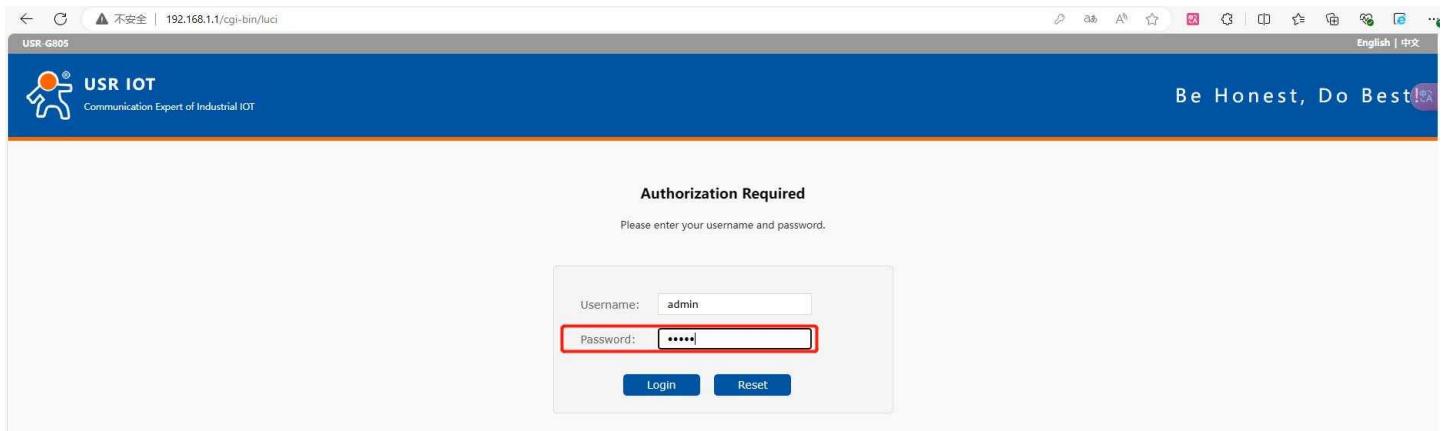


Figure 2. Login webpage

2.2. Brief introduction of the webpage

There are several tabs on the left side of the webpage, users can set parameters of USR-G805s 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.

Status	
Hostname	USR-G805
Firmware Version	V1.00-EN
SN	01601223020300068651
IMEI	869312066104521
Local Time	Thu Jun 6 07:15:49 2024
Uptime	2h 22m 55s
Load Average	0.35, 0.50, 0.50

Memory	
Total Available	85540 kB / 125068 kB (68%)
Free	52836 kB / 125068 kB (42%)
Cached	24940 kB / 125068 kB (19%)
Buffered	7764 kB / 125068 kB (6%)

Network	
IPv4 WAN Status	Not connected
IPv6 WAN Status	...

Figure 3. Status webpage

3. Status & System

3.1. Status

Users can get the basic information of USR-G805s, 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-G805s. 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.

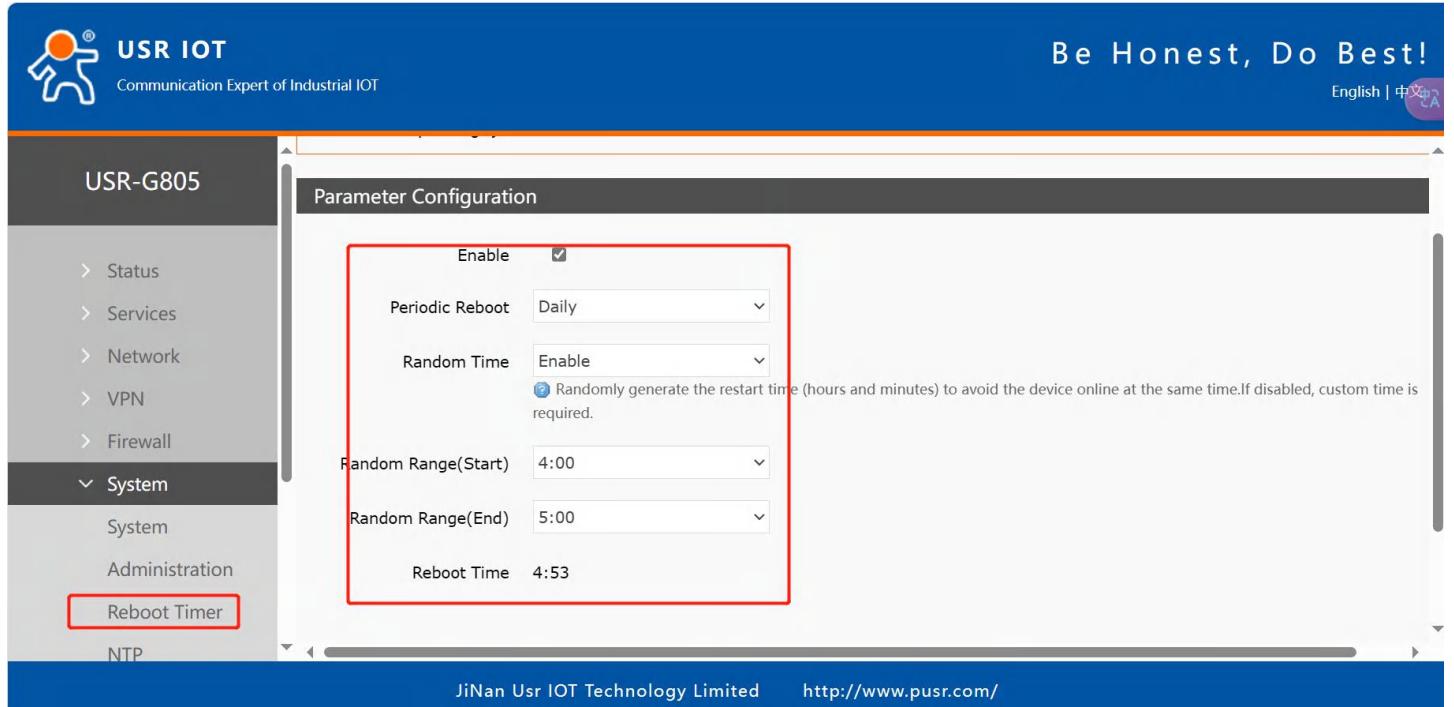


Figure 6. Timed restart function

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-G805s 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.

USR-IOT Communication Expert of Industrial IOT

Be Honest, Do Best!

English | 中文

USR-G805

System Log

Here you can view system logs, including application, kernel, and VPN logs. Remote logs based on UDP protocol can also be configured.

Configuration

Local log Remote log

kernel log level: Info

Application log level: Info

Log Kernel View Empty

Time	Level	Message
Jun 6 07:26:09	(none)	daemon.notice netifd: wwan0 (20852): udhcpc: sending discover
Jun 6 07:26:12	(none)	daemon.notice netifd: wwan0 (20852): udhcpc: sending discover
Jun 6 07:26:36	(none)	daemon.warn dnsmasq-dhcp[3067]: DHCP packet received on ath1 which has no address
Jun 6 07:27:08	(none)	kern.info kernel: [9253.42741] usb 1-1: USB disconnect, device number 80
Jun 6 07:27:08	(none)	kern.info kernel: [9253.42742] cdc_ether 1-1.1.0:0 eth2: register 'cdc_ether' usb-1b000000.usb-1, CDC Ethernet Device
Jun 6 07:27:08	(none)	kern.info kernel: [9253.42742] cdc_ether 1-1.1.0 eth2: register 'cdc_ether' usb-1b000000.usb-1, CDC Ethernet Device
Jun 6 07:27:08	(none)	kern.info kernel: [9253.42742] option 1-1:1.2: device disconnected
Jun 6 07:27:08	(none)	kern.info kernel: [9253.460295] option1 ttyUSB1: GSM modem (1-port) converter now disconnected from ttyUSB1
Jun 6 07:27:08	(none)	kern.info kernel: [9253.468645] option 1-1:1.3: device disconnected
Jun 6 07:27:08	(none)	kern.info kernel: [9253.473722] option1 ttyUSB2: GSM modem (1-port) converter now disconnected from ttyUSB2
Jun 6 07:27:08	(none)	kern.info kernel: [9253.482124] option 1-1:1.4: device disconnected
Jun 6 07:27:08	(none)	kern.info kernel: [9253.482148] option1 ttyUSB3: GSM modem (1-port) converter now disconnected from ttyUSB3
Jun 6 07:27:08	(none)	kern.info kernel: [9253.482148] option1 ttyUSB4: GSM modem (1-port) converter now disconnected from ttyUSB4
Jun 6 07:27:08	(none)	kern.info kernel: [9253.508950] option1 ttyUSB4: GSM modem (1-port) converter now disconnected from ttyUSB4
Jun 6 07:27:08	(none)	kern.info kernel: [9253.508950] option1 1-1:1.6: device disconnected
Jun 6 07:27:08	(none)	kern.info kernel: [9254.930007] usb 1-1: new high-speed USB device number 81 using ehci-ath79
Jun 6 07:27:13	(none)	kern.info kernel: [9258.524113] usb 1-1: USB disconnect, device number 81
Jun 6 07:27:26	(none)	kern.info kernel: [9271.969909] usb 1-1: new high-speed USB device number 82 using ehci-ath79
Jun 6 07:27:26	(none)	kern.info kernel: [9272.126383] cdc_ether 1-1:1.0 eth2: register 'cdc_ether' at usb-1b000000.usb-1, CDC Ethernet Device, 34:4b:50:00:00:00
Jun 6 07:27:26	(none)	kern.info kernel: [9272.160571] option 1-1:1.2: GSM modem (1-port) converter detected
Jun 6 07:27:26	(none)	kern.info kernel: [9272.167427] usb 1-1: GSM modem (1-port) converter now attached to ttyUSB0
Jun 6 07:27:26	(none)	kern.info kernel: [9272.175147] option 1-1:1.3: GSM modem (1-port) converter detected
Jun 6 07:27:26	(none)	kern.info kernel: [9272.181942] usb 1-1: GSM modem (1-port) converter now attached to ttyUSB1

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.

USR-IOT Communication Expert of Industrial IOT

Be Honest, Do Best!

USR-G818

System Log

Here you can view system logs, including application, kernel, and VPN logs. Remote logs based on UDP protocol can also be configured.

Configuration

Local log Remote log

Remote Service IP: 192.168.1.115
Using udp protocol, keep empty for '0.0.0.0'

Remote Service Port: 555
Keep empty to disable

Network Assistant

Protocol: UDP

Local Host Add: 192.168.1.115

Local Host Port: 555

Recv Options: ASCII HEX
Log Display Mode
Auto Linefeed
Hide Received Data
Save Recv to File...
Auto Append Bytes
Send from File...
Cycle [1000 ms]
Auto Scroll Clear

Data log | Network Assistant V5.0.2

```
[2023-07-27 19:08:22.948]# RECV ASCII FROM 192.168.1.1.41525<br>[15:Jul 27 10:08:22 USR_DIALNET[3973] [usr_dialnet.c][100] -----: [select timeout_s = 1; select timeout_u = 359800]
```

```
[2023-07-27 19:08:22.948]# RECV ASCII FROM 192.168.1.1.41525<br>[15:Jul 27 10:08:22 USR_DIALNET[3973] [usr_dialnet.c][100] -----: [select timeout_s = 0; select timeout_u = 89940]
```

```
[2023-07-27 19:08:22.948]# RECV ASCII FROM 192.168.1.1.41525<br>[15:Jul 27 10:08:22 USR_DIALNET[3973] [usr_dialnet.c][100] -----: [select timeout_s = 0; select timeout_u = 10000]
```

```
[2023-07-27 19:08:22.948]# RECV ASCII FROM 192.168.1.1.41525<br>[15:Jul 27 10:08:22 USR_DIALNET[3973] [usr_dialnet.c][100] -----: [Enough hosts reachable (required 1, reachable: 3)]
```

```
[2023-07-27 19:08:22.948]# RECV ASCII FROM 192.168.1.1.41525<br>[15:Jul 27 10:08:22 USR_DIALNET[3973] [usr_dialnet.c][100] -----: [Enough hosts reachable (required 1, reachable: 3)]
```

Data Send | Remote: 192.168.1.1.41525 Clean Clear Reset

Ethernet, WiFi, RS232/RS485, 2 x digital Inputs/Outputs

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-G805s will restore to factory default settings.

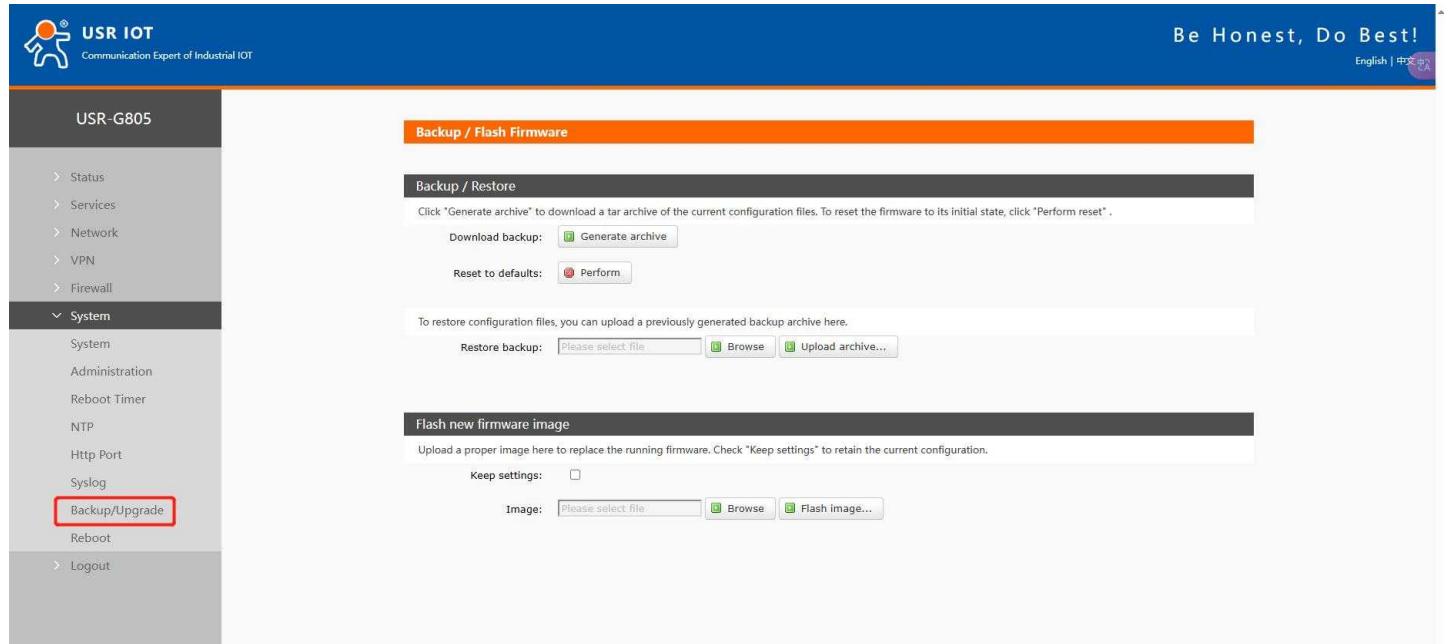


Figure 11. Backup and firmware upgrade

3.9. Reboot

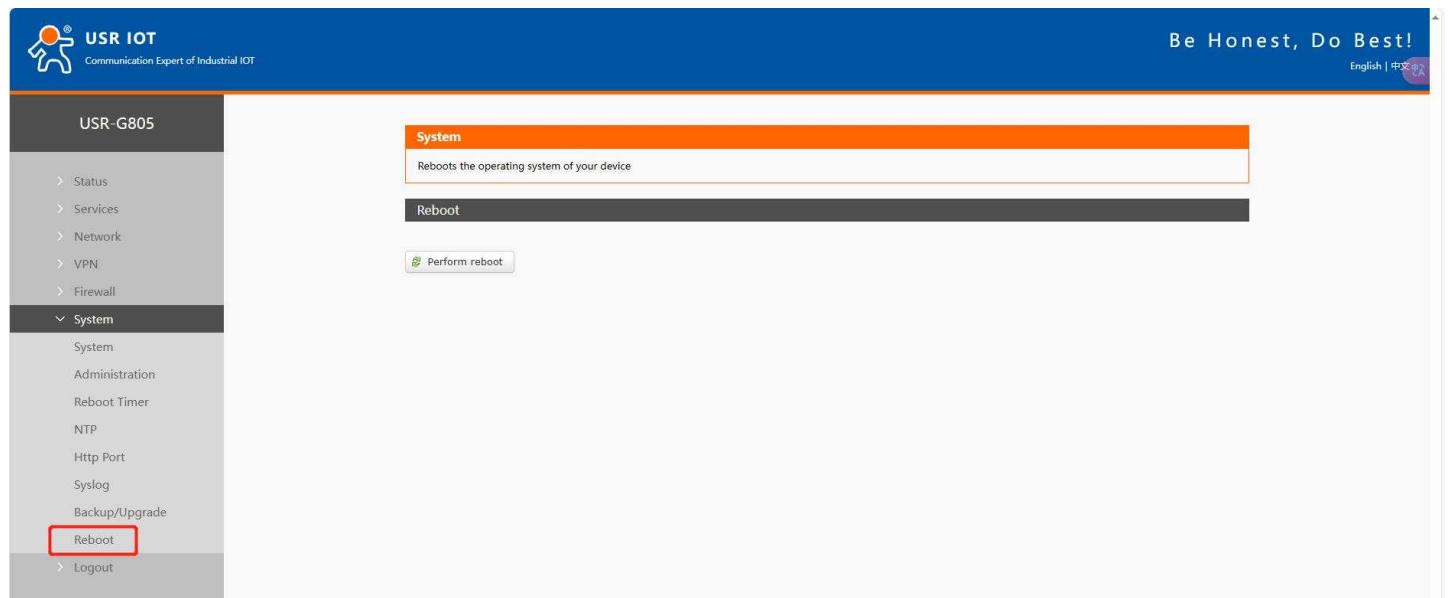


Figure 12. Reboot Function

4. Network introduction

4.1. WAN interface

For USR-G805s device, it supports multiple WAN interface: 4G connectivity, STA connectivity and wired WAN connectivity.

4G connectivity: this router support connect to base station both in IPv6 and IPv4, in the following picture, it's WAN6_4G(IPv6) and WAN_4G(IPv4).

Wired WAN connectivity: USR-G805s comes with two WAN ports, of which WAN2 is configurable, the factory default is LAN4, and can be configured as WAN2. WAN_WIRED is for WAN1 port, and WAN2_WIR is for WAN2 port.

STA connectivity: This router connects to the upper router to get network connectivity, it's WWAN0 interface.

In factory default, USR-G805s enables 3 WAN interface: WAN_WIRED, WAN_4G, WAN6_4G.

Network	Status	Actions
WAN2_WIR	Uptime: 0h 0m 0s MAC-Address: F4:70:0C:6FA3:6D RX: 0.00 B (0 Pkts.) TX: 5.43 KB (32 Pkts.)	Connect Edit
WAN6_4G	Uptime: 0h 54m 1s MAC-Address: 34:4B:50:00:00:00 RX: 36.15 MB (63539 Pkts.) TX: 12.65 MB (58699 Pkts.) IPv6: 2408:8418:0:62c2:3abaa:040:3ea8/64 IPv6: 2408:8418:0:62c2:364b:50ff:fe00:0/64	Connect Edit
WAN_4G	Uptime: 0h 54m 5s MAC-Address: 34:4B:50:00:00:00 RX: 36.15 MB (63539 Pkts.) TX: 12.65 MB (58699 Pkts.) IPv4: 10.6.16.187/29	Connect Edit
WAN_WIRED	Uptime: 0h 0m 0s MAC-Address: F4:70:0C:6FA3:6B RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Edit
WWAN0	Uptime: 0h 0m 0s MAC-Address: FA:70:0C:6FA3:6E Client: "USR-G805"	Connect Edit

Figure 13. WAN interface

4.1.1. WAN_4G 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-G805s is assigned by the upper-level router, and the upper-level router must enable the DHCP service. G805s is connected to the WAN port of the upper-level router through the LAN port.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

AUTO REFRESH ON English | 中文

USR-G805

Status

> Services

< Network

- WAN
- LAN
- Cellular Network
- Network Failover
- WLAN AP
- WLAN STA
- DHCP
- Static Routes
- Diagnostics
- Tcpdump
- > VPN
- > Firewall

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

Common Configuration

General Setup Advanced Settings

Status

Uptime: 0h 0m 0s
MAC-Address: F4:70:0C:6F:A3:6B
RX: 0.00 B (0 Pkts.)
TX: 0.00 B (0 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP: USR-G805

Back to Overview Apply Save

Figure 14. DHCP Client of WAN interface

➤ Static address Mode

In this mode, users can set the IP address of USR-G805s.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

AUTO REFRESH ON English | 中文

USR-G805

> Status

> Services

< Network

- WAN
- LAN
- Cellular Network
- Network Failover
- WLAN AP
- WLAN STA
- DHCP
- Static Routes
- Diagnostics
- Tcpdump
- > VPN
- > Firewall
- > 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_VLANNN (e.g.: eth0.1).

Common Configuration

General Setup Advanced Settings

Status

Uptime: 0h 0m 0s
MAC-Address: F4:70:0C:6F:A3:6B
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

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.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Be
AUTO REFRESH ON English

USR-G805

- > Status
- > Services
- < Network
 - WAN
 - LAN
 - Cellular Network
 - Network Failover
 - WLAN AP
 - WLAN STA
 - DHCP
 - Static Routes
 - Diagnostics
 - Tcpdump
- > VPN
- > Firewall
- > 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,VLANNN` (e.g.: `eth0,1`).

Common Configuration

General Setup **Advanced Settings**

Status

Uptime: 0h 0m 0s
MAC Address: F4:70:0C:6F:A3:6B
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**

Figure 16. PPPoE Mode

4.2. LAN interface

4.2.1. Basic configuration

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-G805s will automatically assign an IP address to the device connected to the LAN port.

Figure 17. LAN interface

Figure 18. Settings of LAN interface

4.2.2. VLAN enable

USR-G805s supports VLAN function, multiple network ports can be divided into different network segments. If needed, users can enable it manually.

Network Interface	LAN1	LAN2	LAN3	WAN
lan(br-lan)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lan2(br-lan2)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lan3(br-lan3)	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
lan4(br-lan4)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note:

- VLAN division is disabled by default. If this function is enabled, the IP address of the LAN1 port is automatically changed to 192.168.1.1, the IP address of LAN2 is changed to 192.168.2.1, and so on.
- WIFI bridges to the LAN1. When a device connects to the wifi of 805s, the device obtains the same IP network segment as the LAN1 network interface.
- LAN2 and lan3 can be arbitrarily bridged to LAN1-LAN3 networks.

4.2.3. WAN/LAN switching

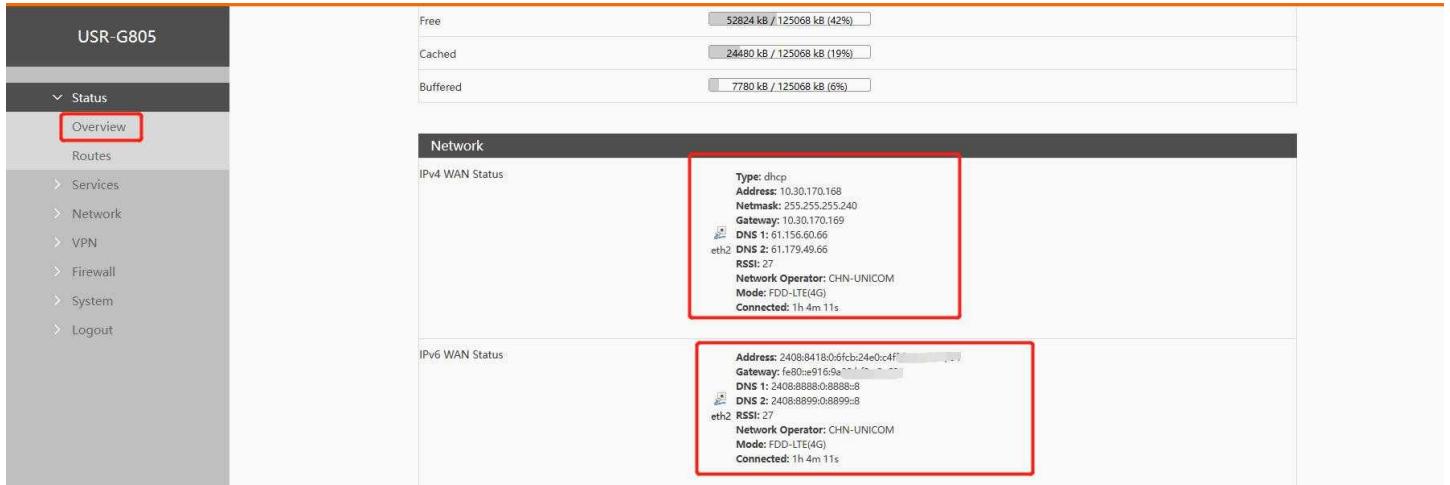
After enabling the VLAN function, WAN port can be configured as LAN4 port. If you need three LAN ports without VLAN division, you can select the LAN2 and LAN3 network ports at the same time.

Network Interface	LAN1	LAN2	LAN3	WAN
lan(br-lan)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
lan2(br-lan2)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lan3(br-lan3)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lan4(br-lan4)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

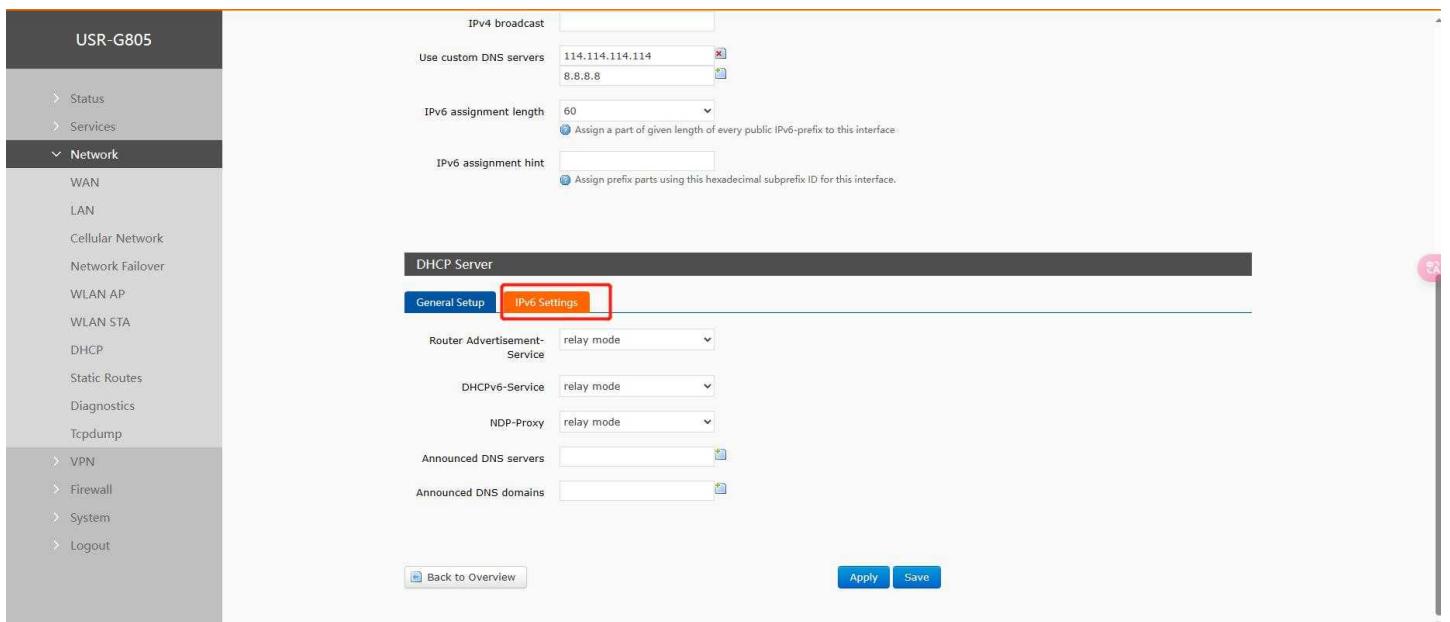
4.2.4. IPv6 configuration

For LAN ports and cellular networks, the USR-G805s supports IPv6.

If the using SIM card support IPv4 and IPv6, then it can get both IPv4 IP and IPv6 IP like the following figure.



For LAN port, the router can assign IPv6 IP to the LAN device, it also need the LAN device support IPv6 protocol.



The PC connect to LAN port of USR-G805s, and it can get IPv6 IP.

```
以太网适配器 以太网 3:
连接特定的 DNS 后缀 . . . . . : lan
IPv6 地址 . . . . . : 2408:8418:0:6fc:24e0:c4f
临时 IPv6 地址 . . . . . : 2408:8418:0:6fc:8158:b83e:8f67:2f2d
本地链接 IPv6 地址 . . . . . : fe80::16d0:1434:a917:f72f%2
IPv4 地址 . . . . . : 192.168.1.136
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : fe80::d6ad:20ff:fe42:8a93%2
192.168.1.1

无线局域网适配器 WLAN:
连接特定的 DNS 后缀 . . . . . : lan
本地链接 IPv6 地址. . . . . : fe80::c7d1:c124c:cf62%32
IPv4 地址 . . . . . : 192.168.66.182
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.66.1

C:\Users\Administrator>
```

4.3. Cellular network

4.3.1. Configuration

4.3.1.1. SIM switching

For USR-G805s, it supports dual sim single standby mode, and can get 4G connectivity according to user's settings. There are 3 mode for user to choose: master standby mode, mutual standby mode and manual mode.

Master standby mode: In this mode, SIM1 card is used for networking. If SIM1 fails to connect to the network, it will automatically switch to SIM2 to try to connect to the network. After SIM2 successfully connect to the network, SIM2 will be used for networking. When SIM1 is installed, it will switch back to SIM1 to try to connect to the network every set time(SIM Switching Cycle).

Mutual standby mode: in this mode, the router will give priority to the SIM card that can connect to the network normally, and the router will keep using this card to connect to the network, unless the SIM card can not connect to the network normally.

Manual mode: in this mode, the router will select the SIM card for networking according to the user's settings. Even if this SIM card can not connect to the Internet, it will not automatically switch to other SIM cards for networking. In this mode, users can remotely switch cards manually by SMS commands.

The screenshot shows the 'Cellular Network Configuration' page of the USR-G805 web interface. The left sidebar shows the navigation menu with 'Network' selected. The main content area has a sub-header 'Config' and tabs for 'Configuration', 'SIM1 Config', 'SIM2 Config', and 'Mobile Information'. The 'Configuration' tab is active. It contains the following settings:

- Dual SIM Switching Mode:** Master Standby Mode (radio button selected)
- SIM Switching Cycle:** 300 (input field)
- Link Detection Enable:** (checkbox checked)

At the bottom are 'Apply' and 'Save' buttons.

4.3.1.2. Link detection

After enabling the link detection function, users can set the ping interval and tries, if the success rate of ping is lower than the set value, the router will choose to restart the module or the router according to the parameter settings.

The screenshot shows the 'Config' tab selected in the top navigation bar. The left sidebar is titled 'USR-G805' and contains the following menu items: Status, Services, Network (with sub-items: WAN, LAN, Cellular Network, Network Failover, WLAN AP, WLAN STA, DHCP, Static Routes, Diagnostics, Tcpdump), VPN, Firewall, and System. The 'Cellular Network' item is highlighted with a red box. The main content area is titled 'Cellular Network' and contains the following configuration options:

- Dual SIM Switching Mode:** Master Standby Mode (dropdown menu with a note: Set the dual-SIM switchover mode)
- SIM Switching Cycle:** 600 (note: In the master standby Mode, when using sim2 for internet access, it will attempt to switch to sim1 for internet access after the "SIM Switching Cycle" is reached. Value range: 180-86400s.)
- Link Detection Enable:** Once selected, check the network connect with ping (checkbox is checked and highlighted with a red box)
- Interval:** 10 (note: ping interval units: sec, 1-86400)
- Max Ping Tries:** 3 (note: Perform recovery action after reaching Consecutive failures times, 1-100)
- Detection Address 1:** 8.8.8.8 (note: Set the first address for ping check)
- Detection Address 2:** (note: Set the second address for ping check)
- Detection Address 3:** (note: Set the third address for ping check)
- Recovery Action:** Reset Modem (dropdown menu)

Items	Description
Link Detection Enable	Whether to enable the link detection function. By default, it's not enabled.
Interval	The time interval between two consecutive pings. Range: 1-86400 s, It's 10 seconds by default.
Max Ping Tries	The maximum number of attempts to ping. Range: 1-100, it's 3 attempts by default.
Detection Address 1	The first destination IP address of ping command
Detection Address 2	The second destination IP address of ping command
Detection Address 3	The third destination IP address of ping command
Recovery Action	None: No action is performed Redial: Execute the redial procedure Reset modem: Restart 4G modem Reboot device: Restart the router

4.3.2. SIM1 configuration

For USR-G805s, it supports dual sim single standby mode,

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.	None

	SIM1: Prioritize using SIM1 to dial up and connect to the Internet. SIM2: Prioritize using SIM2 to dial up and connect to the Internet.	
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, G805s 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

4.3.3. 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.	PAP and CHAP
Network Type	AUTO: According to the on-site network environment, it can automatically select to stay on the network 4G/4G/3G. 2G: Lock the 2G network, if there is no 2G network on site, it can't connect to the network. 3G: Lock the 3G network, if there is no 3G network on site, it can't connect to the network. 4G: Lock the 4G network, if there is no 4G network on site, it can't connect to the network.	AUTO
LTE band selection	In custom mode, user can set specific band to connect to the network. And can select multiple bands, like 1:2:3	auto
PDP Type	PDP protocol context type.	IPv4&IPv6
Network Search Priority	Network priority selection.	auto
PIN Enable	If the SIM card has enabled the PIN function, the USR-G805s also needs to enable this function also.	None
EHRPD Enable	If 3.4G network is need, users can enable this function.	Disable

4.3.4. Mobile 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.

USR-G805		Configuration	SIM1 Config	SIM2 Config	Mobile Information
Status		Modem Version:	17016.1000.00.38.01.31		
		IMEI:	869312066104521		
		Dial SIM:	sim1		
		SIM Status:	READY		
		SMS Service Center:	+861000000000		
		ICCID:	898601234567890123456789		
		Phone Number:	+861000000000		
		CIMI:	460018600406728		
		APN:	mobile..1		
		Attachment Status:	Attached		
		Network Operator:	CHINA-UNICOM		
		Network Type:	4G Mode		
		BAND:	1		
		IP Address:	10.18.19.97		
		IPv6 Address:	2408:8418:0:2cad:00e2:5094:46e9:dacc:64Global,2408:8418:0:2cad:364b:50ff:fe00:0/64Global		
		Signal Strength:	29(-55dBm)		
		Location Area Code:	D306		
		Cell ID:	08C3B485		

Figure 21. Information of cellular network

For USR-G805 device, it supports display the input/output rate of 30 seconds and 5 minutes.

4.4. Network failover

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

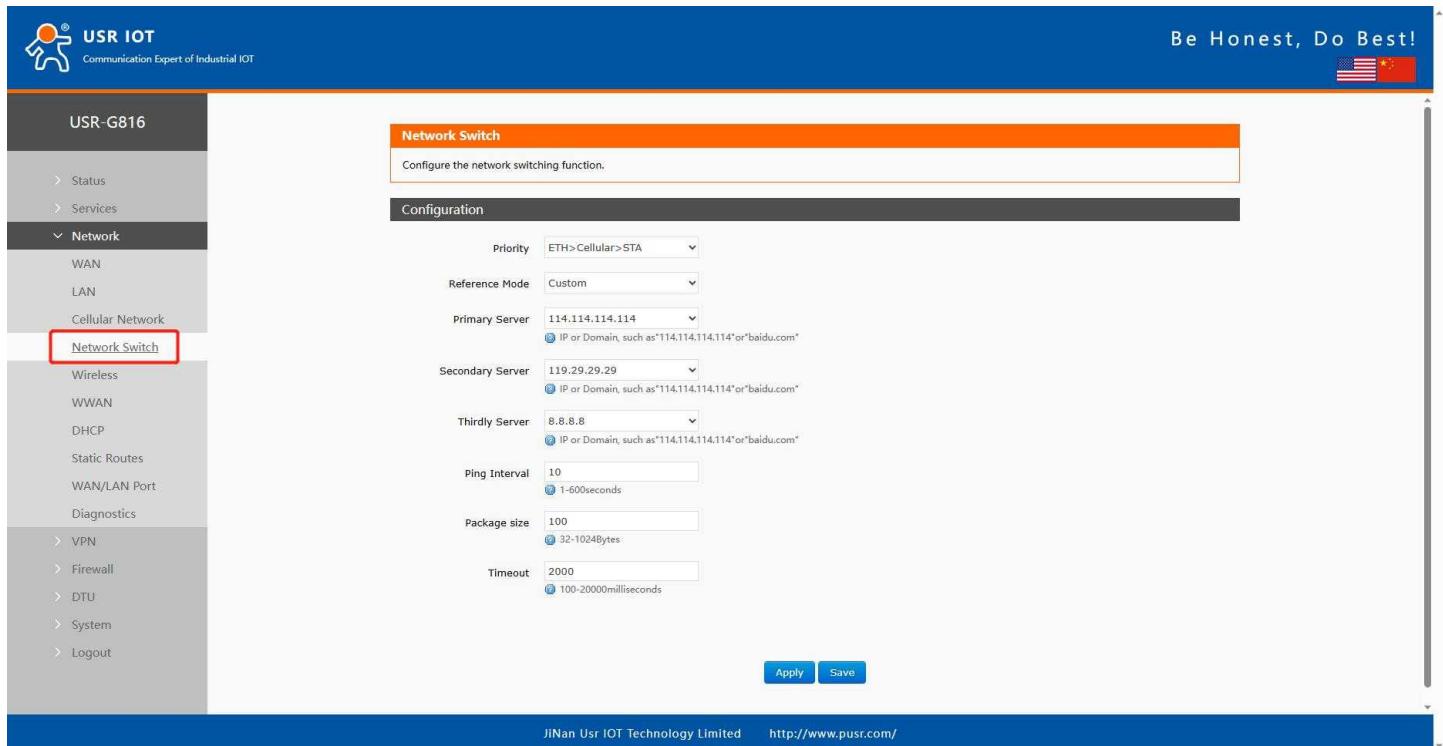


Figure 22. Network switch page

4.5. WLAN AP

4.5.1. Basic settings

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

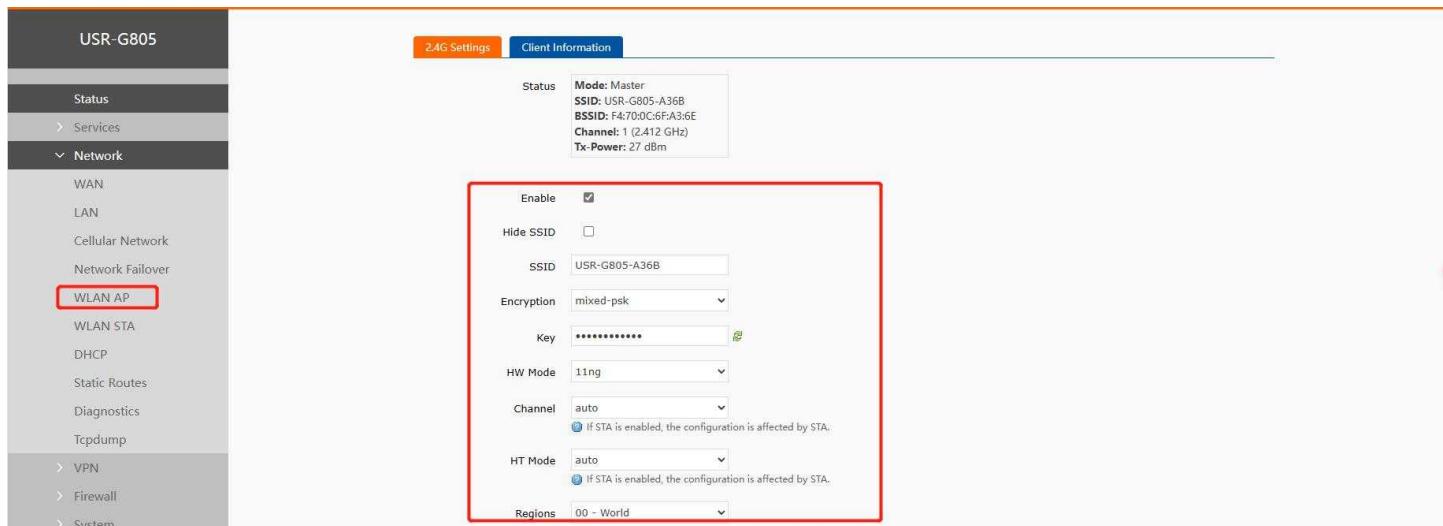


Figure 23. AP settings

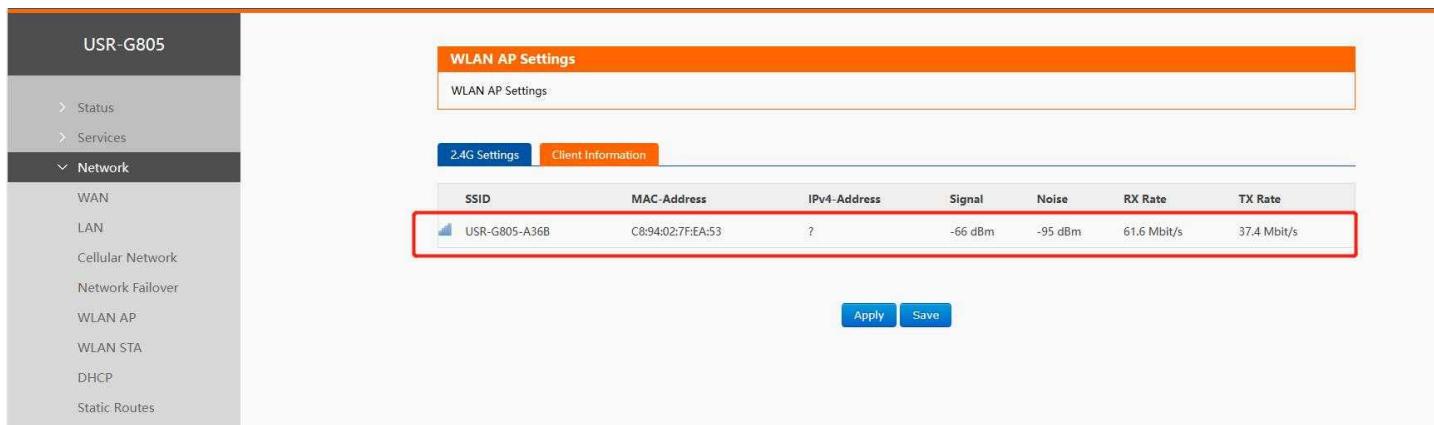
Table 7. Parameters description of Wi-Fi interface

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-G805s-xxxx
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.	auto
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-G805s through Wi-Fi.



The screenshot shows the 'WLAN AP Settings' page with the 'Client Information' tab selected. The table displays the following data for a connected device:

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
USR-G805-A36B	C8:94:02:7F:EA:53	?	-66 dBm	-95 dBm	61.6 Mbit/s	37.4 Mbit/s

Buttons for 'Apply' and 'Save' are visible at the bottom of the table.

Figure 24. Client information of Wi-Fi

4.6. WLAN STA

4.6.1. Basic settings

On this page, users can enable the STA function and set relevant parameter. The default setting is OFF.

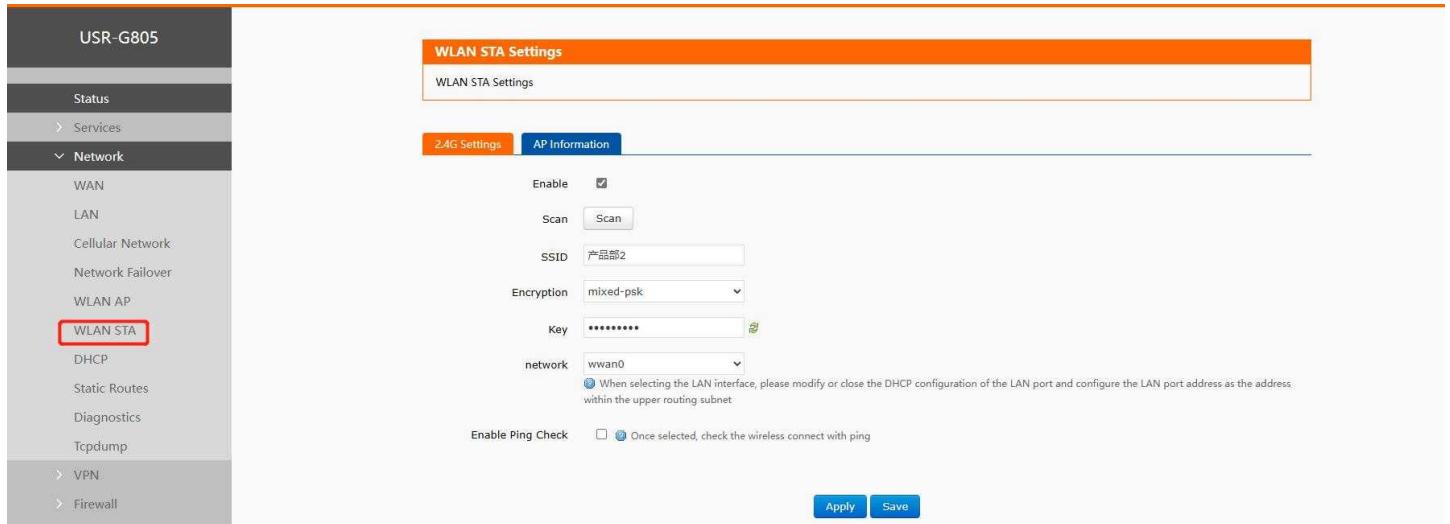


Figure 25. STA settings

The steps to connect to the upper-level routers:

- 1>Click "Scan" button,
- 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.

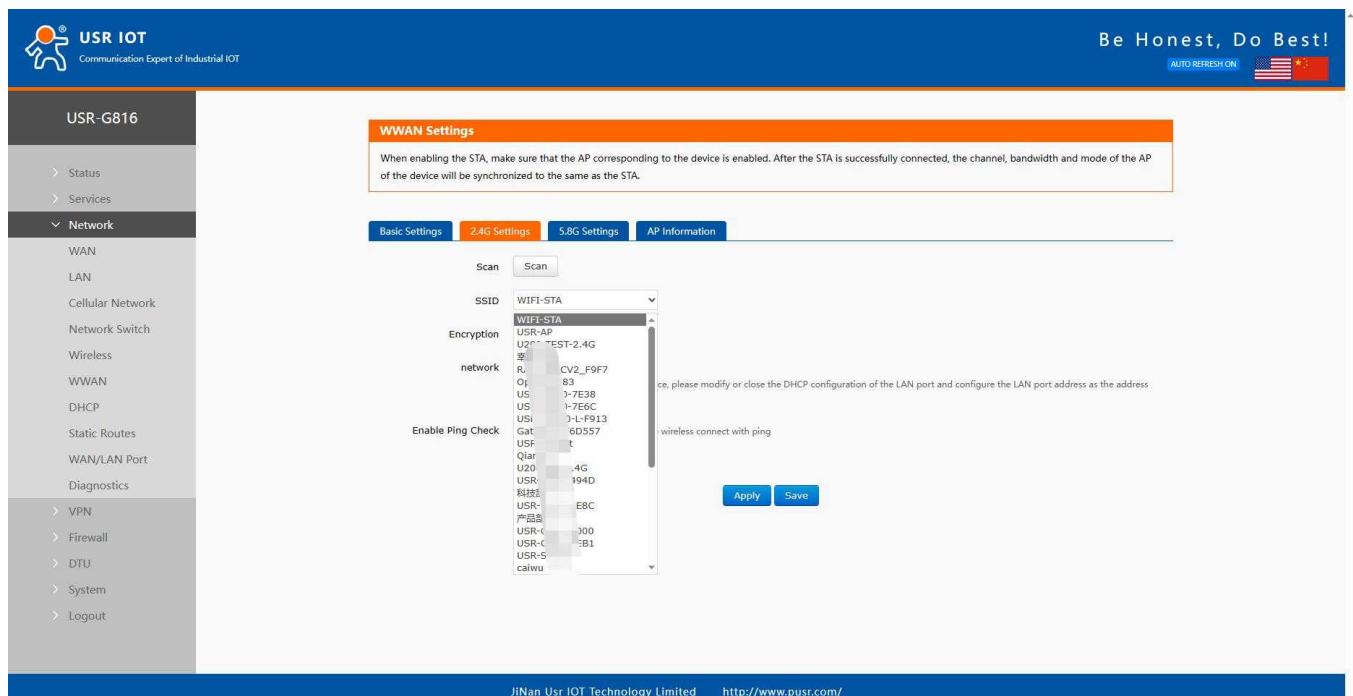


Figure 26. Searched AP list

4.6.2. AP information

If the USR-G805s connect to upper-level Wi-Fi successfully, the information will be displayed in this page.

Figure 27. The AP information

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 28. 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 29. 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 30. Routing table checking

4.9. Network diagnostics

USR-G805s provides online diagnostic functions, including Ping tools, routing analysis tools, and DNS viewing tools.

Figure 31. 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

4.10. TCP dump

The router supports tcpdump packet capture on web pages and can download the captured files for data analysis. Packets can be captured on multiple interfaces based on the number of packets or the interval.

USR-G805

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

Start network capture

Interface	seconds, packets	Filter	Actions
wan_4g	0	seconds	<input type="button" value="Stop capture"/>

Output

tcpdump: listening on eth2, link-type EN10MB (Ethernet), capture size 262144 bytes

Capture links

Capture file	Modification date	Capture size	Actions
capture_2024-07-10_06.10.42	10/7/2024 18:11:4	8.15 KiB	<input type="button" value="pcap file"/> <input type="button" value="Remove"/>
capture_2024-07-10_06.11.17	10/7/2024 18:11:17	0 B	<input type="button" value="pcap file"/> <input type="button" value="Remove"/>
capture_2024-07-10_06.11.26	10/7/2024 18:11:36	4 KiB	<input type="button" value="pcap file"/> <input type="button" value="Remove"/>
All files		12.15 KiB	<input type="button" value="Download"/> <input type="button" value="Remove"/>

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.

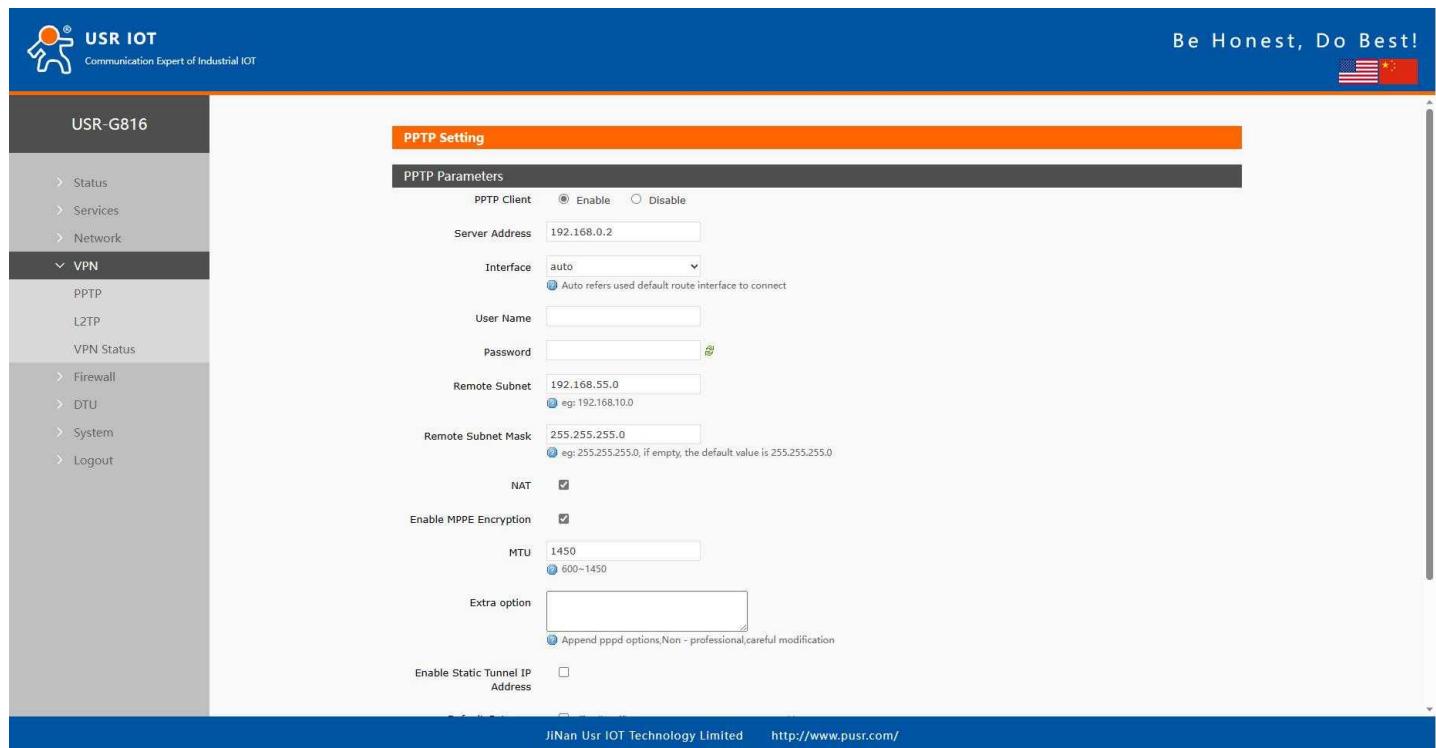


Figure 32. PPTP VPN settings

Table 10. Parameter details of PPTP VPN

Items	Description	Default
PPTP Client	Whether to enable PPTP client.	Disable
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-G805s 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.

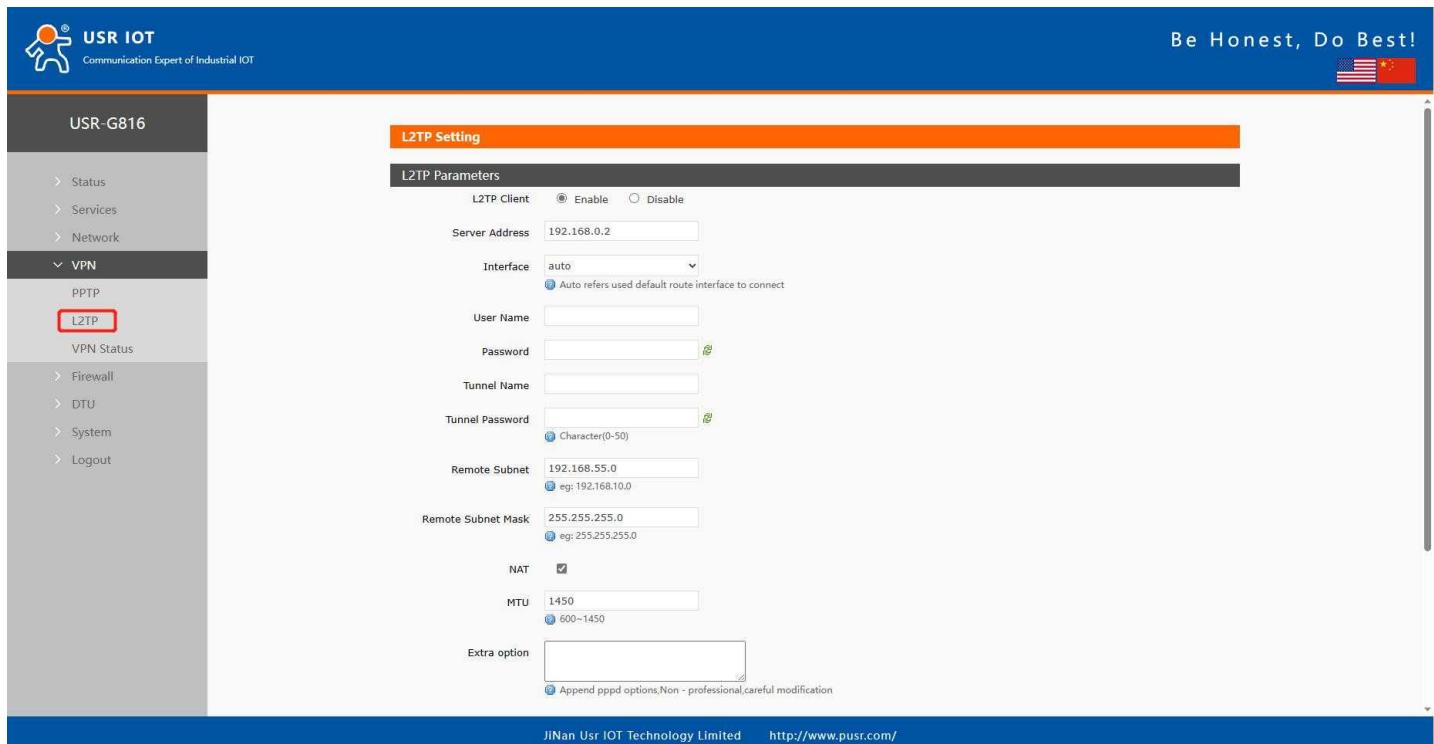


Figure 33. L2TP VPN settings

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-G805s 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. IPSec VPN

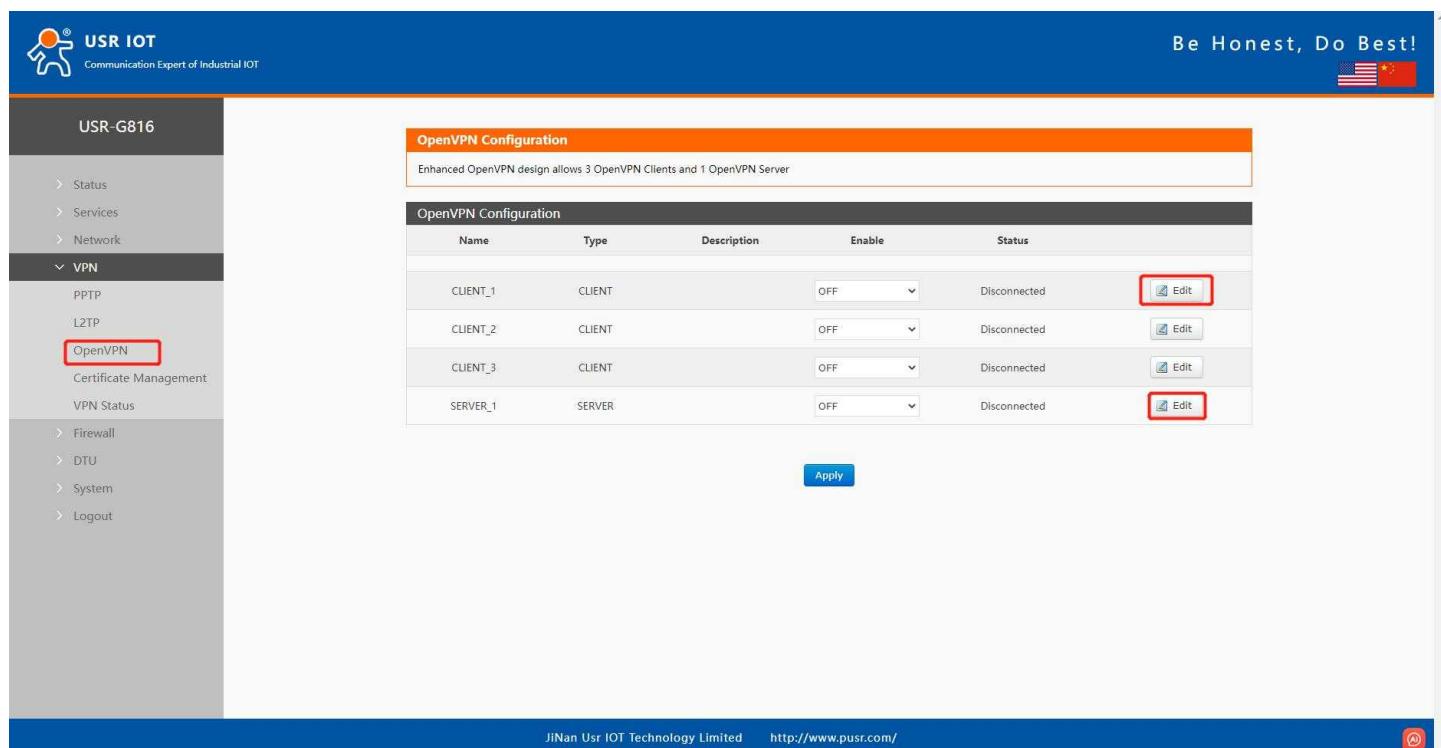
USR-G805s supports IPSec VPN, both v1 and v2 version.

Items	Description	Default
IPSec enable	Whether to enable IPSec VON	Disable
Interface	Select the interface according to different networking methods.	auto
Peer Address	Set L2TP server IP or domain name.	192.168.0.2
Negotiation Method	Main and aggressive are supported	main
Tunnel Type	4 types: Site to site, Site to host, Host to site, Host to host	Site to site
Local Subnet	Local IP and mask of IPSec VPN	192.168.1.0/24
Peer Subnet	Peer IP and mask of IPSec VPN	192.168.55.0/24
IKE Version	V1, V2 version are supported	Ikev2
IKE Encryption Algorithm	3DES, AES-128, AES-192, AES-256 are supported	3DES
IKE Integrity Algorithm	MD5, SHA1, SHA2-256, SHA2-512 are supported	MD5
Diffie-Hellman Group	Group1(768bits), Group2(1024bits), Group5(1536bits), Group14(2048bits).	Group2(1024bits)
IKE Life Time	Range: 400-86400 seconds	28800
Authentication Type	pre-shared key authentication is supported	Pre-shared Key
Pre-shared Key	Set the key of authentication type, 1-50characters can be set.	123456abc

Local Identifier	It can be IP address or @domain, 0-29 characters can be set.	@client
Peer Identifier	It can be IP address or @domain, 0-29 characters can be set.	@server
ESP Encryption Algorithm	3DES, AES-128, AES-192, AES-256 are supported	AES-128
ESP Integrity Algorithm	SHA1, SHA2-256, MD5 are supported	SHA-1
Perfect forward encryption(PFS)	None, DH1, DH2, DH5	DH2
ESP Life Time	Range: 400-86400 Seconds	3600
DPD Timeout	Sets the timeout duration for Dead Peer Detection	60
DPD Detection Period	Sets the detection period for Dead Peer Detection	60
DPD Action	Sets the action for DPD detection, including Restart, clear, Hold, None	Restart
Enable Ping Tracking	Whether to enable the PING detection	Disable

5.4. OpenVPN

In OpenVPN mode, the USR-G805s support 3 OpenVPN clients and 1 OpenVPN server. This means USR-G805s can connect to 3 OpenVPN servers simultaneously.



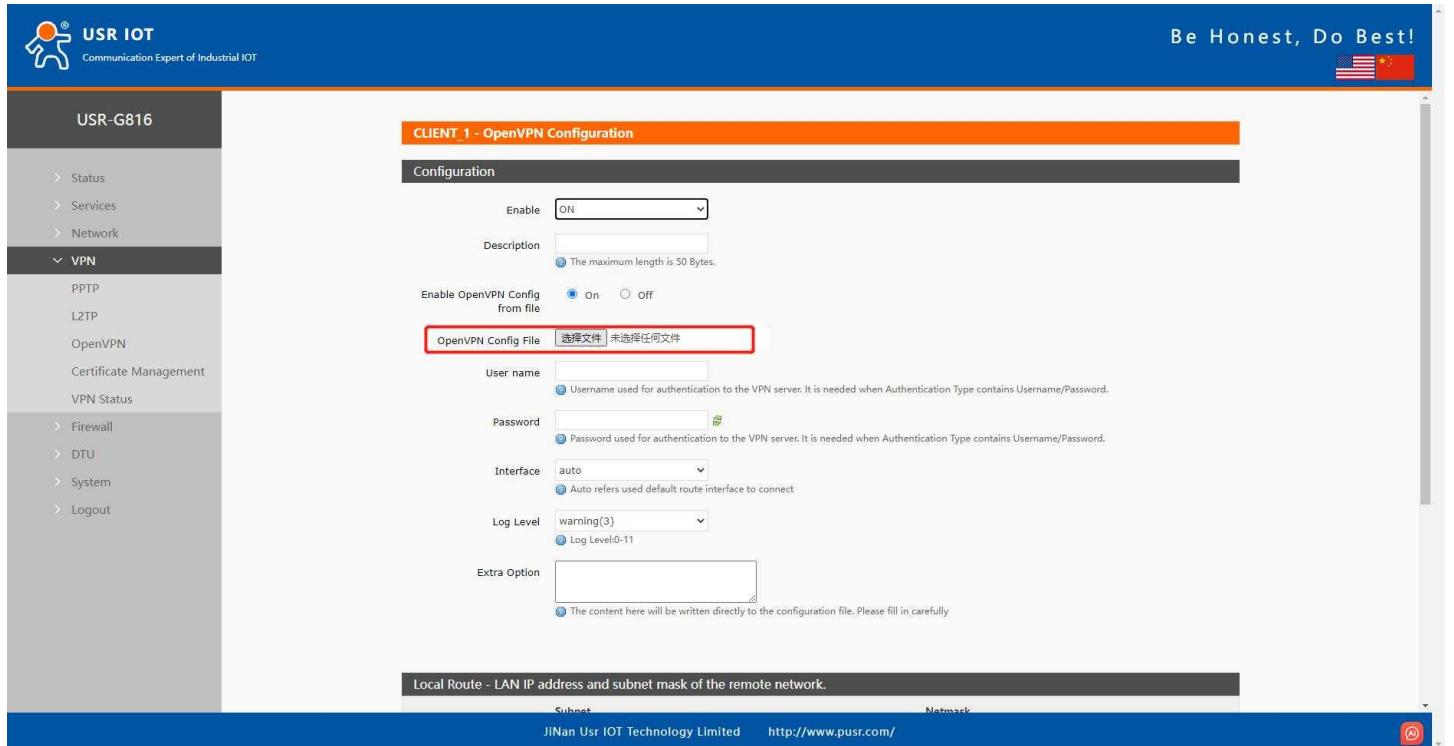
The screenshot shows the USR-G805 web interface with the following details:

- Header:** USR IOT, Communication Expert of Industrial IOT, Be Honest, Do Best! (with USA and China flags).
- Left Sidebar (USR-G806):**
 - Status
 - Services
 - Network
 - VPN** (selected)
 - PPTP
 - L2TP
 - OpenVPN** (highlighted with a red box)
 - Certificate Management
 - VPN Status
 - Firewall
 - DTU
 - System
 - Logout
- OpenVPN Configuration Section:**
 - OpenVPN Configuration:** Enhanced OpenVPN design allows 3 OpenVPN Clients and 1 OpenVPN Server.
 - Table:**| Name | Type | Description | Enable | Status |
| --- | --- | --- | --- | --- |
| CLIENT_1 | CLIENT | | OFF | Disconnected |
| CLIENT_2 | CLIENT | | OFF | Disconnected |
| CLIENT_3 | CLIENT | | OFF | Disconnected |
| SERVER_1 | SERVER | | OFF | Disconnected |
 - Buttons:** Apply (blue button at the bottom right of the table area).
 - Page Bottom:** JiNan Usr IOT Technology Limited, http://www.pusr.com/

Figure 34. Edit OpenVPN settings

5.4.1. OpenVPN client

USR-G805s 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 35. 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.

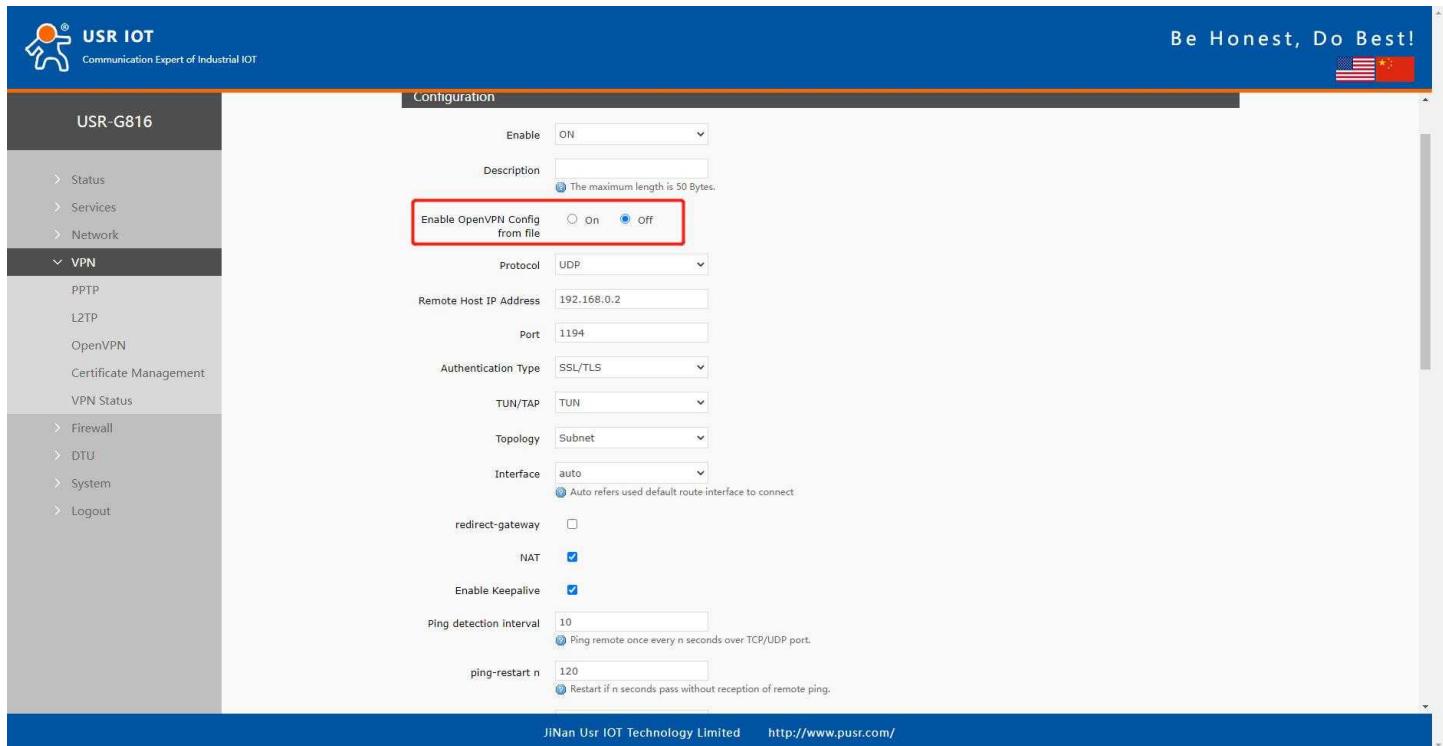


Figure 36. Enable traditional OpenVPN settings

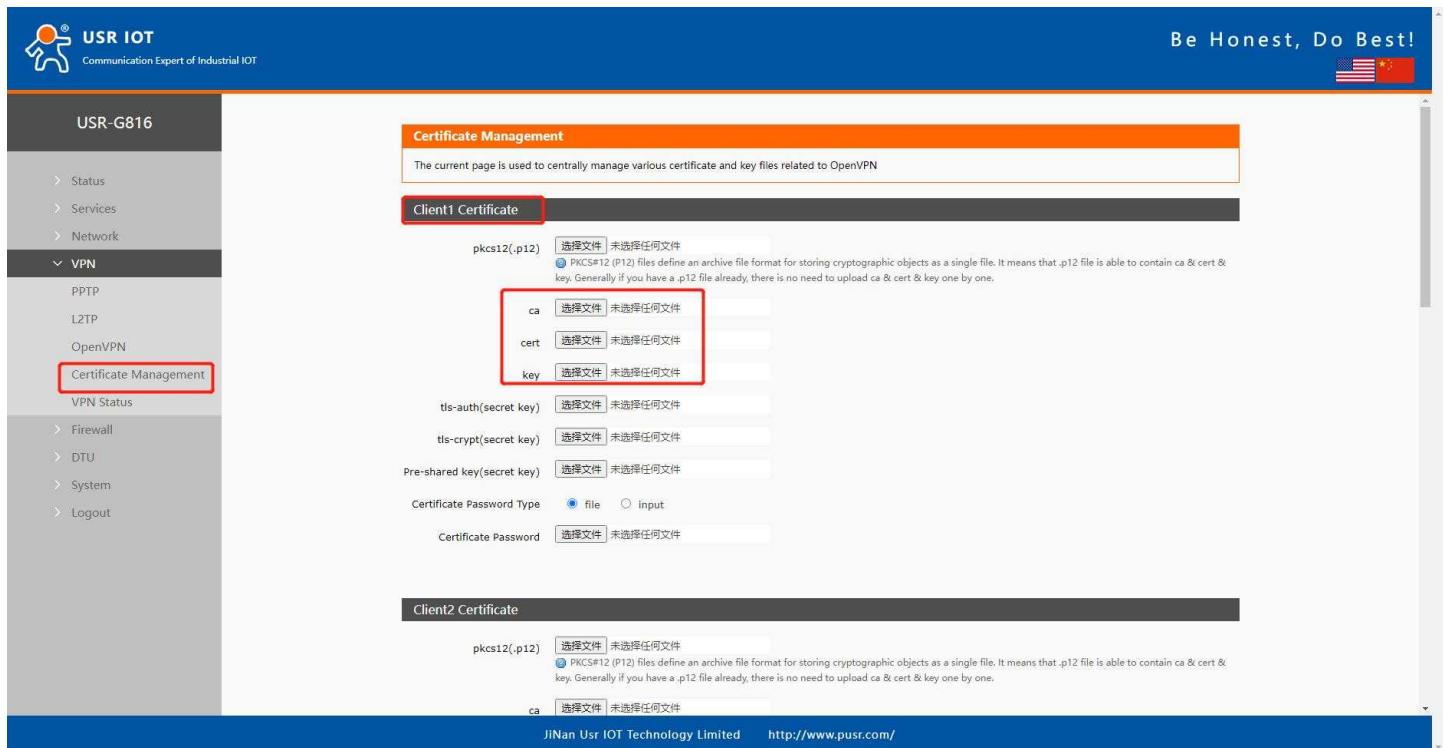


Figure 37. Upload certificate file

5.4.2. OpenVPN server

Figure 38. OpenVPN server settings

5.5. GRE

Items	Description	Default
GRE	Whether to enable GRE VPN.	Disable
Interface Name	The name of GRE VPN tunnel	gre_gre1
Interface		auto
Peer WAN IP	Remote GRE WAN IP address	192.168.0.10

Peer Tunnel IP	Remote GRE tunnel IP address	10.10.10.1
Peer Subnet	Remote IP/Mask	192.168.55.0/24
Local Tunnel IP	Local GRE tunnel IP address	10.10.10.2
NAT	Whether NAT is required for data passing through GRE interfaces	Enabled
TTL	Set the TTL parameters(1~255)	255
MTU	Set the MTU(600~1500)	1450
Enable Ping	The USR-G805s will reconnect to GRE VPN 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

6. Firewall

6.1. General Settings

There are 2 basic firewall rules by default in USR-G805s.

Figure 39. 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 4G 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 4G 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	IP address of device connected to LAN port.		None

address		
Internal port	<p>Users can set a single port or a range of ports, like 8000-9000.</p> <p>Note: It's DMZ function when external port and internal port are empty.</p>	None

USR-IOT Communication Expert of Industrial IOT

Be Honest, Do Best!

USR-G816

Status Services Network VPN Firewall General Settings Port Forwards Traffic Rules Access Restrictions DTU System Logout

Firewall - Port Forwards

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

Port Forwards

Name	Match Rules	Forwarding To	Enable	Sort
This section contains no values yet.				

New Port Forwarding Rules:

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

Apply Save

JINNan USR IOT Technology Limited <http://www.pusr.com/>

Figure 40. 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.

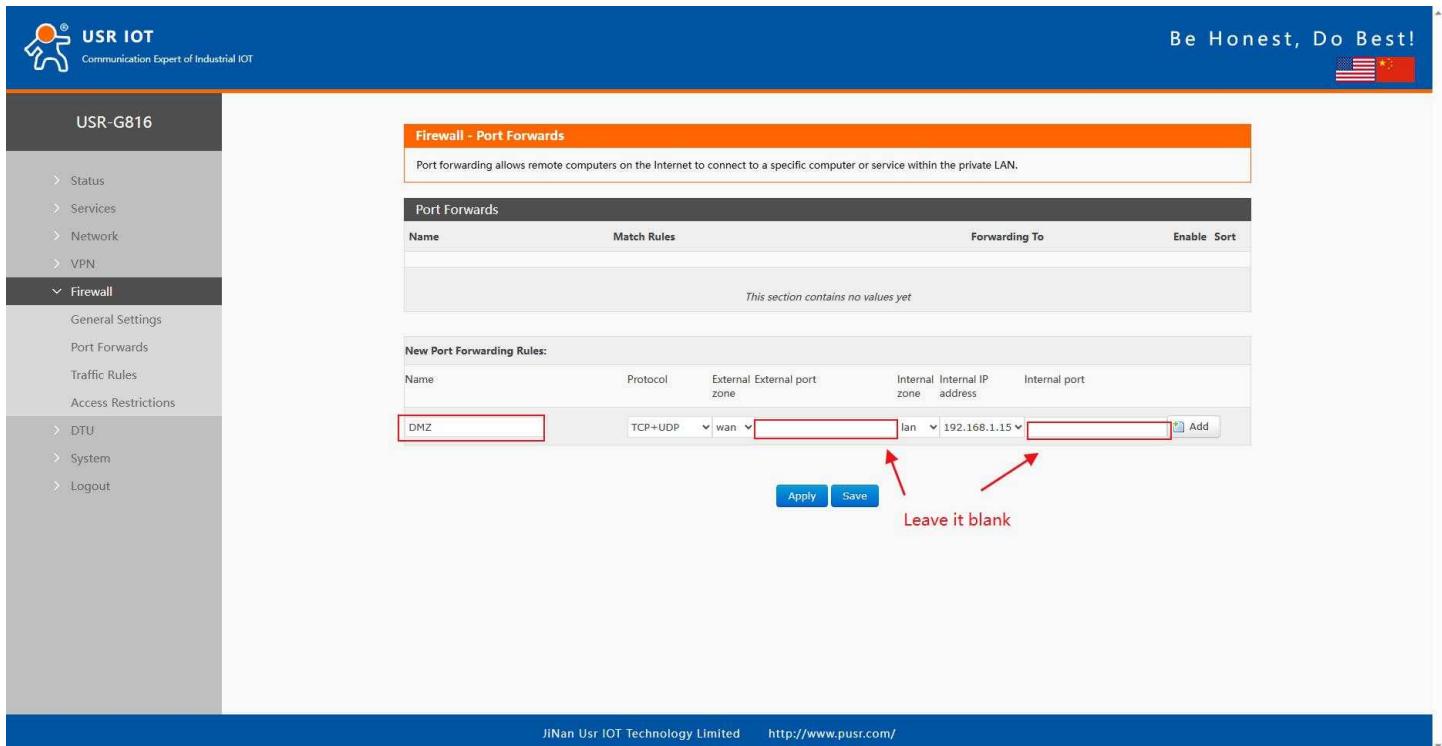


Figure 41. DMZ settings

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 the 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	Target IP address or network segment of the incoming connection.	any
Destination port	Target port or range of ports of the incoming connection.	None
Action	<p>Action that is to be taken when a packet matches the conditions of the rule.</p> <p>Drop: packet is stopped and deleted.</p> <p>Accept: packet gets to continue to the next chain.</p> <p>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.</p> <p>Don't track: packet is no longer tracked as it moves forward.</p>	Accept

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

USR-G805

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Protocol	Action	Enable	Sort
Allow-Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	

New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	

Source NAT

Name	Protocol	Action	Enable	Sort
This section contains no values yet				

JINan USR IOT Technology Limited <http://www.pusr.com/>

Figure 42. 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

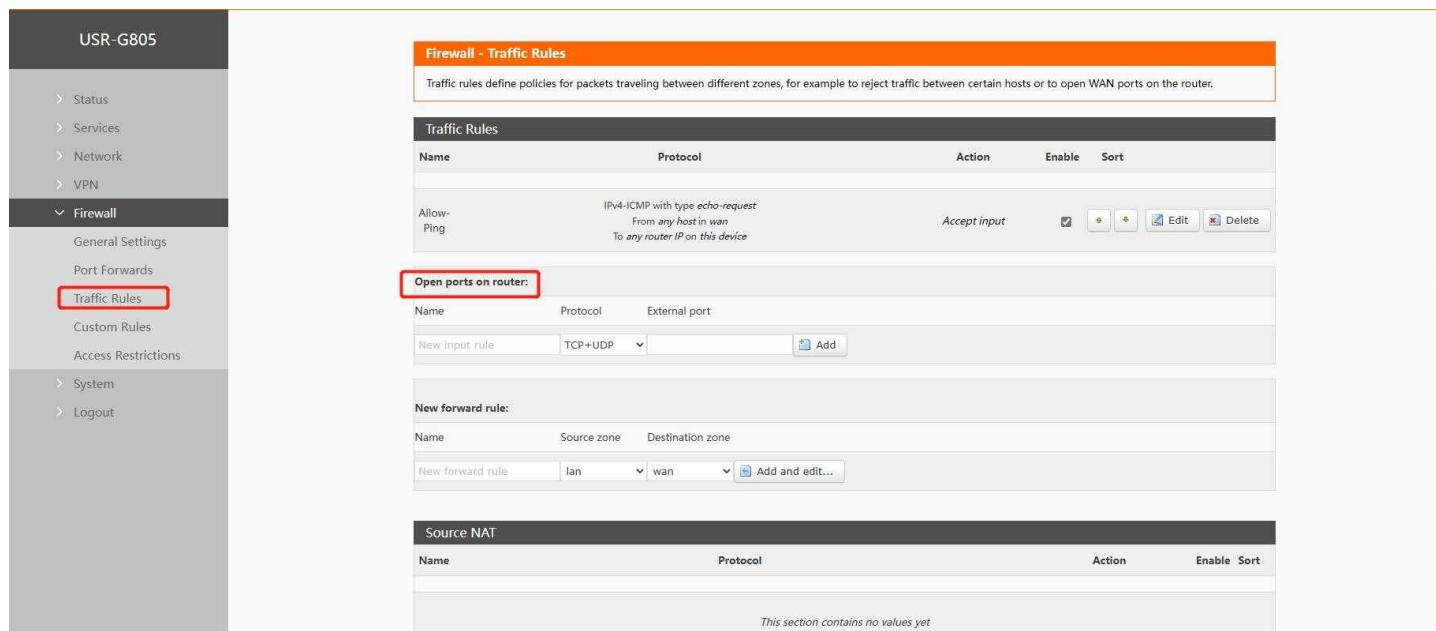


Figure 43.

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

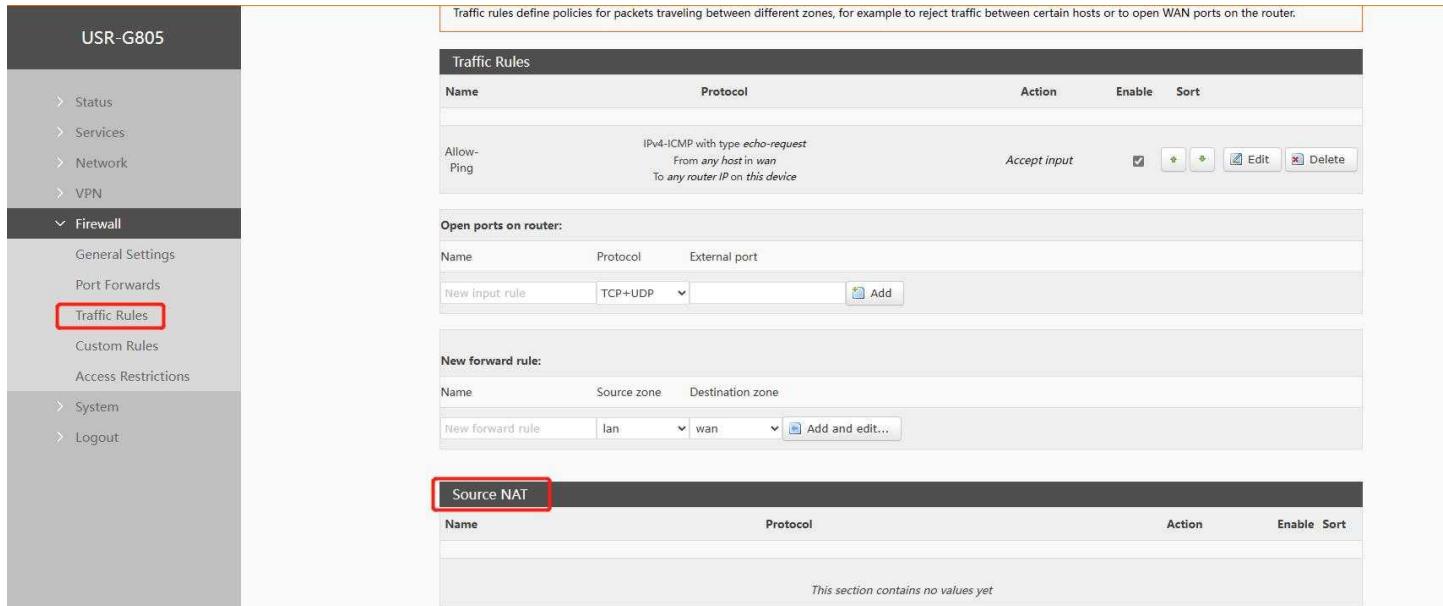


Figure 44. Add new forward rules

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

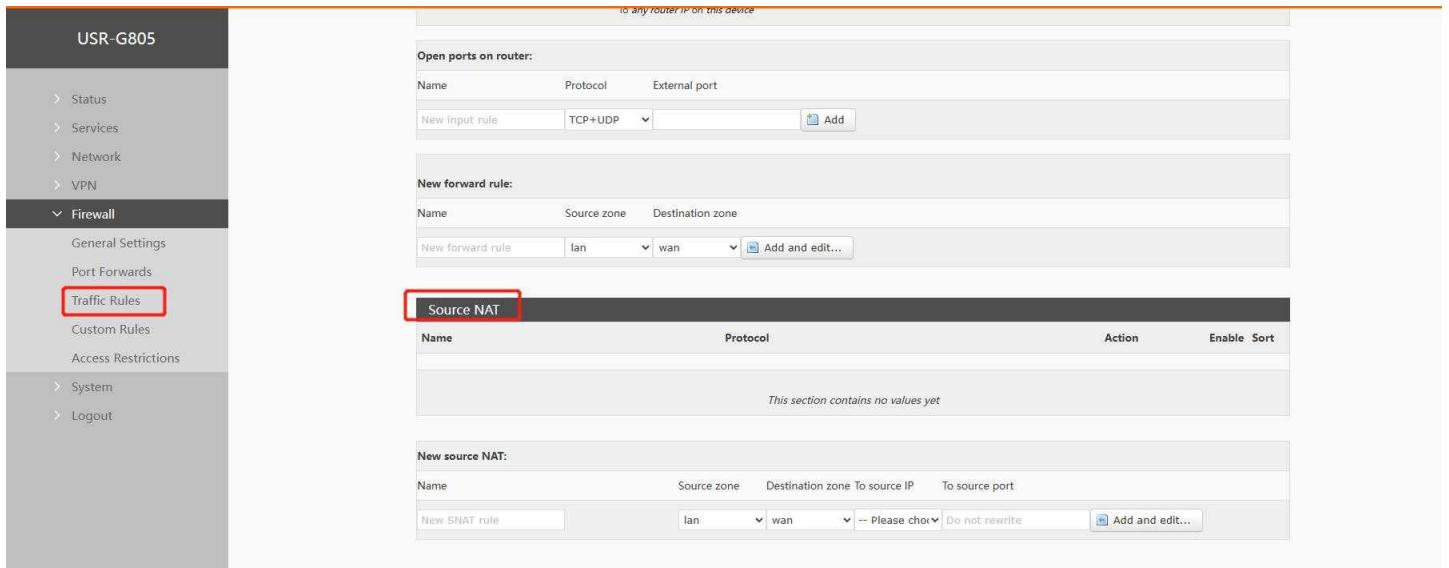


Figure 45. Settings of SourceNAT

Users need to fill in the basic information before clicking the “Add and edit” button, it will redirect you to the rule's configuration page.

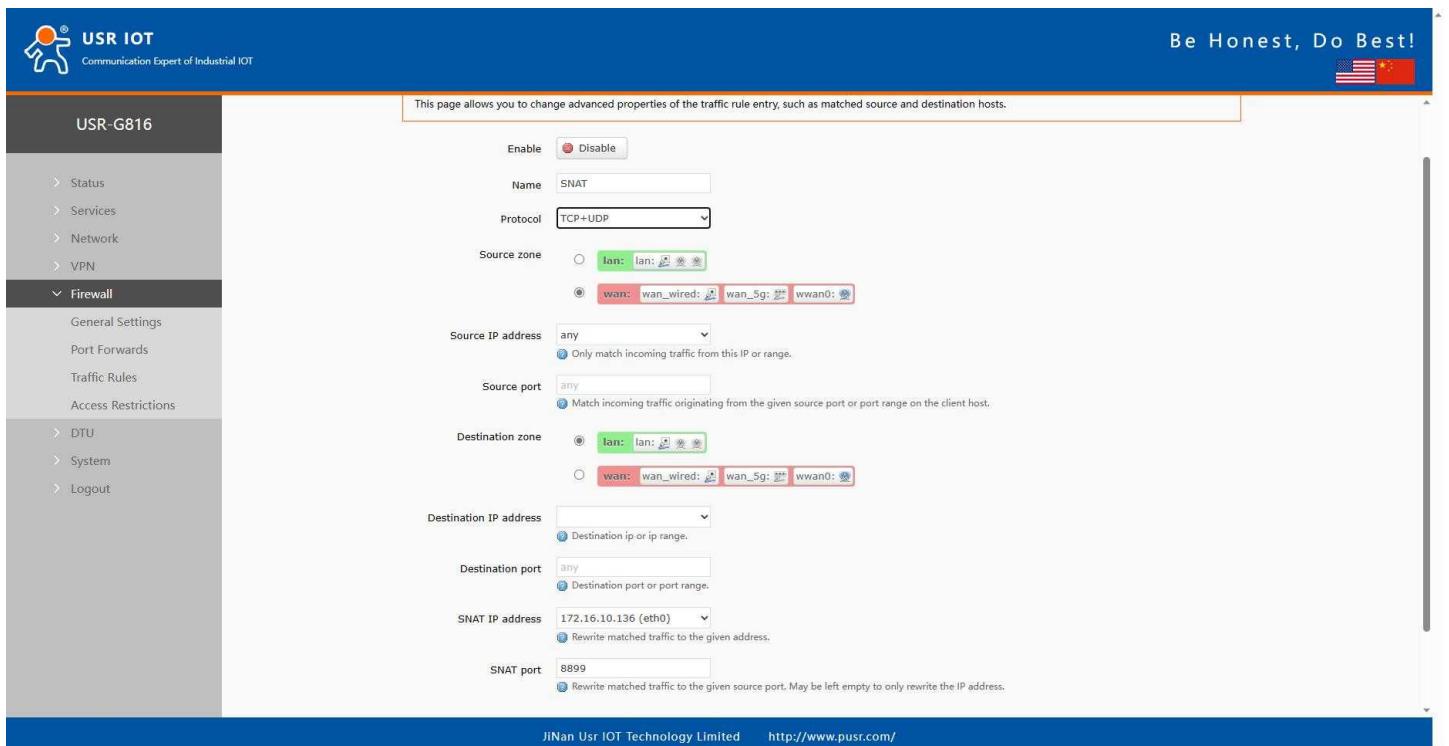


Figure 46. Detail settings of SourceNAT

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.

The screenshot shows the USR-G805 web interface. The left sidebar has a 'Firewall' section with 'Access Restrictions' highlighted. The main content area has a header 'Access Restrictions' with a note about entering domain names. Below is a 'Configurations' section with a table for 'Access Restrictions' and a section for 'New Firewall Rule' with 'Add' and 'Apply' buttons.

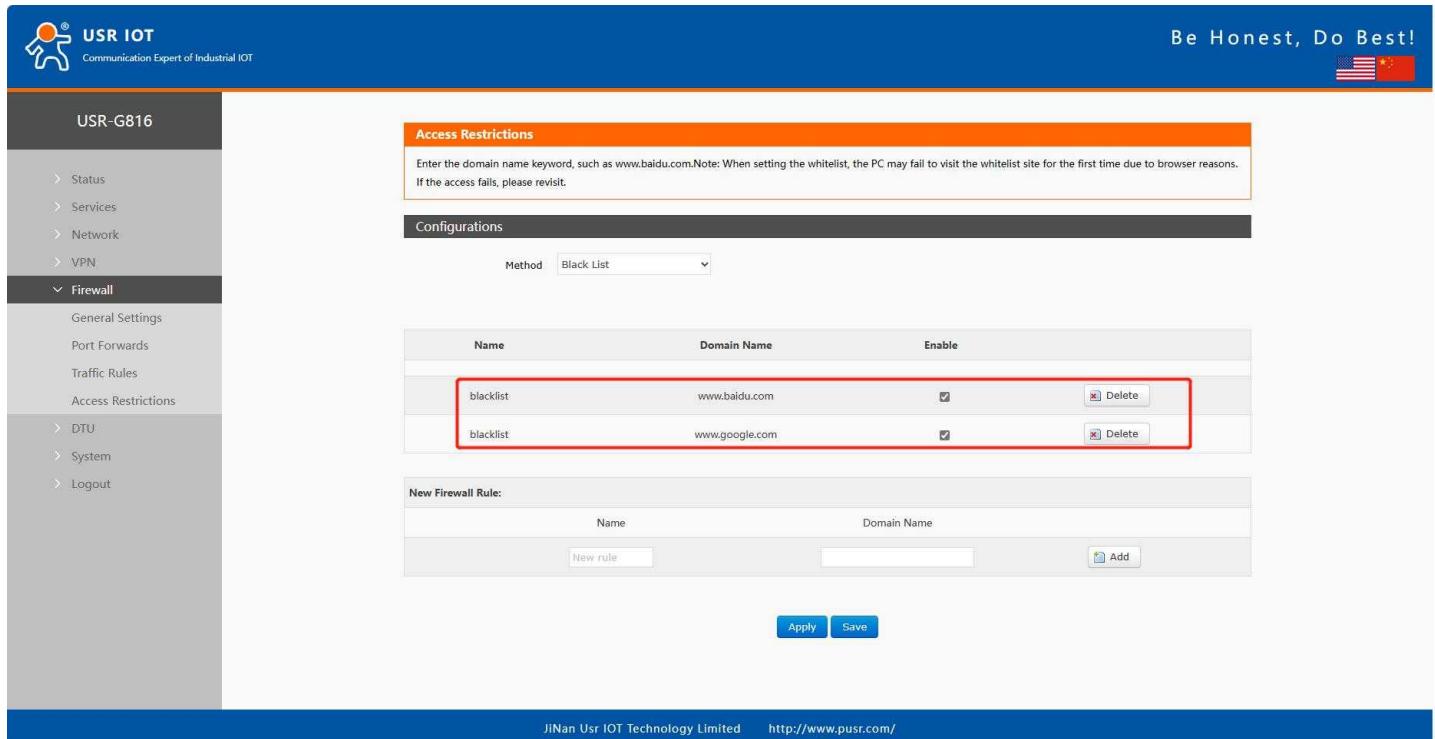
Name	Domain Name	Enable
This section contains no values yet		

Name	Domain Name	
<input type="button" value="New rule"/>	<input type="text"/>	<input type="button" value="Add"/>

Figure 47. 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.



The screenshot shows the 'Access Restrictions' configuration page for a 'Black List'. The 'Method' dropdown is set to 'Black List'. The table lists two rules:

Name	Domain Name	Enable	Action
blacklist	www.baidu.com	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
blacklist	www.google.com	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>

Below the table is a 'New Firewall Rule' section with a 'Name' field and a 'Domain Name' field, both currently empty. There are 'Add' and 'Delete' buttons for this section. At the bottom are 'Apply' and 'Save' buttons.

Figure 48. 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.

USR IOT
Communication Expert of Industrial IOT

Be Honest, Do Best!

USR-G816

Status
Services
Network
VPN
Firewall
General Settings
Port Forwards
Traffic Rules
Access Restrictions
DTU
System
Logout

Access Restrictions

Enter the domain name keyword, such as www.baidu.com. Note: When setting the whitelist, the PC may fail to visit the whitelist site for the first time due to browser reasons. If the access fails, please revisit.

Configurations

Method: White List

Name	Domain Name	Enable
blacklist	www.baidu.com	<input checked="" type="checkbox"/> Delete

New Firewall Rule:

Name	Domain Name
New rule	Add

Apply Save

JINNan USR IOT Technology Limited <http://www.pusr.com/>

Figure 49. Add whitelist rules

7. Additional services

7.1. PUSR Cloud

7.1.1. Add USR-G805s on PUSR Cloud

PUSR platform login address: <https://mp.usriot.com/>.

On USR-G805s side, users need enable the PUSR cloud first.

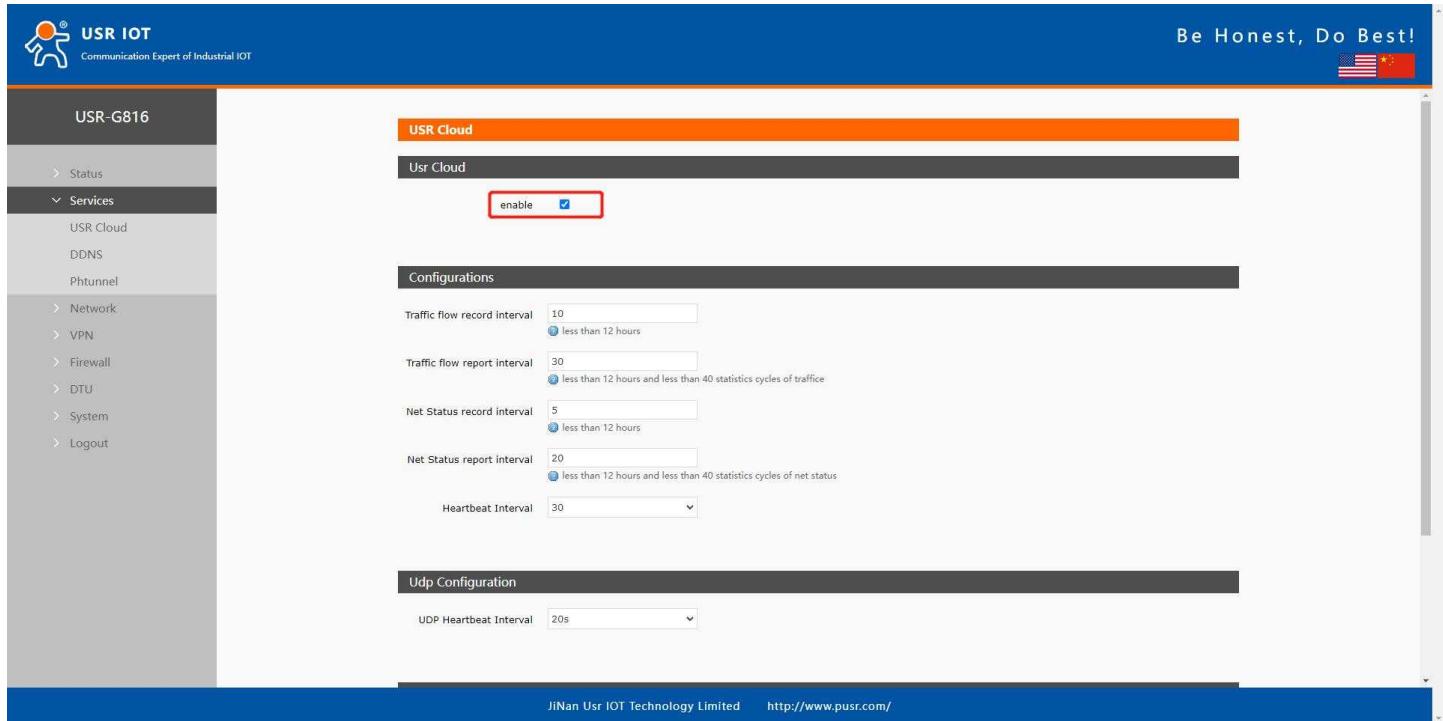


Figure 50. Enable the PUSR function of G805s

On PUSR cloud side, users can add USR-G805s on PUSR platform and monitor the status of USR-G805s.

Figure 51. Add device on PUSR cloud

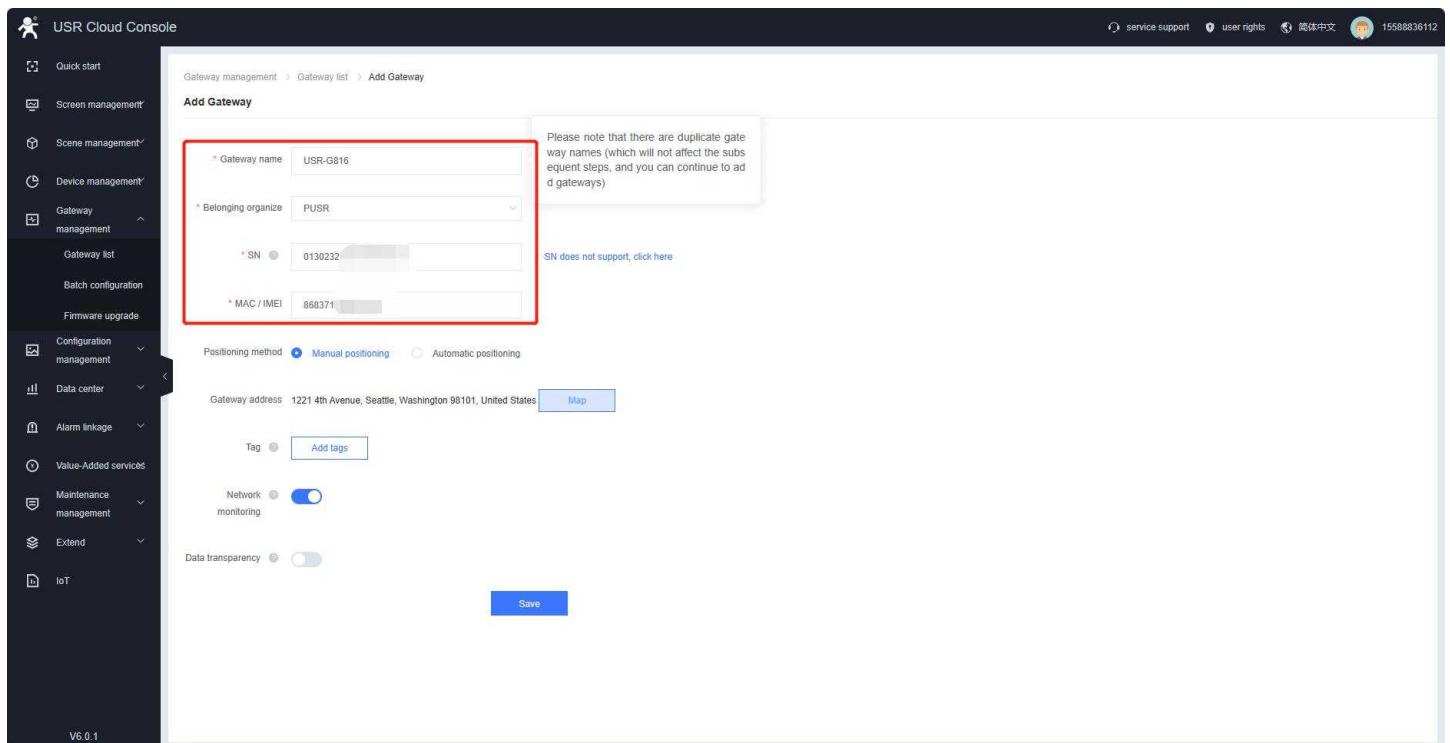


Figure 52. Enter the information of USR-G805s

Gateway list									
Gateway management		Gateway list							
Gateway list		Total Gateways: 5 ● Online gateway 1 ● Offline gateway 4							
Gateway status	Gateway name	SN	Gateway model	parameter loc k	Number of as sociated devi ces	Firmware Version	Belonging organize	Gateway address	Operation
Online	USR-G816	01302323060800000979	USR-G816w-G	--	0	V1.0.10.wifi-EN	PUSR	美莲广场, Jinan Shi, Shandong 2501...	View Edit Delete More
Waiting for the init	Unnamed_Gateway na...	00005450000000000003	未知型号	--	0	--	PUSR	山东省济南市历下区奥帆路	View Edit Delete More
Waiting for the init	Unnamed_Gateway na...	00005450000000000001	未知型号	--	0	--	PUSR	山东省济南市历下区奥帆路	View Edit Delete More
Offline	未命名_网关名称_84	01301822120100009921	USR-G806s-EAU	--	0	V1.0.06-EN	根组织	山东省济南市历下区奥帆路	View Edit Delete More
Offline	USR-M100	02700123031600055984	USR-M100	--	1	V2.0.03.000000.0000	根组织	Swatch Jinan Mixc, East Jingshi Ro...	View Edit Delete More

Figure 53. Online status

7.1.2. Gateway Information

Click "Gateway Name", it will guide you to a new page showing the detail of the USR-G805s.

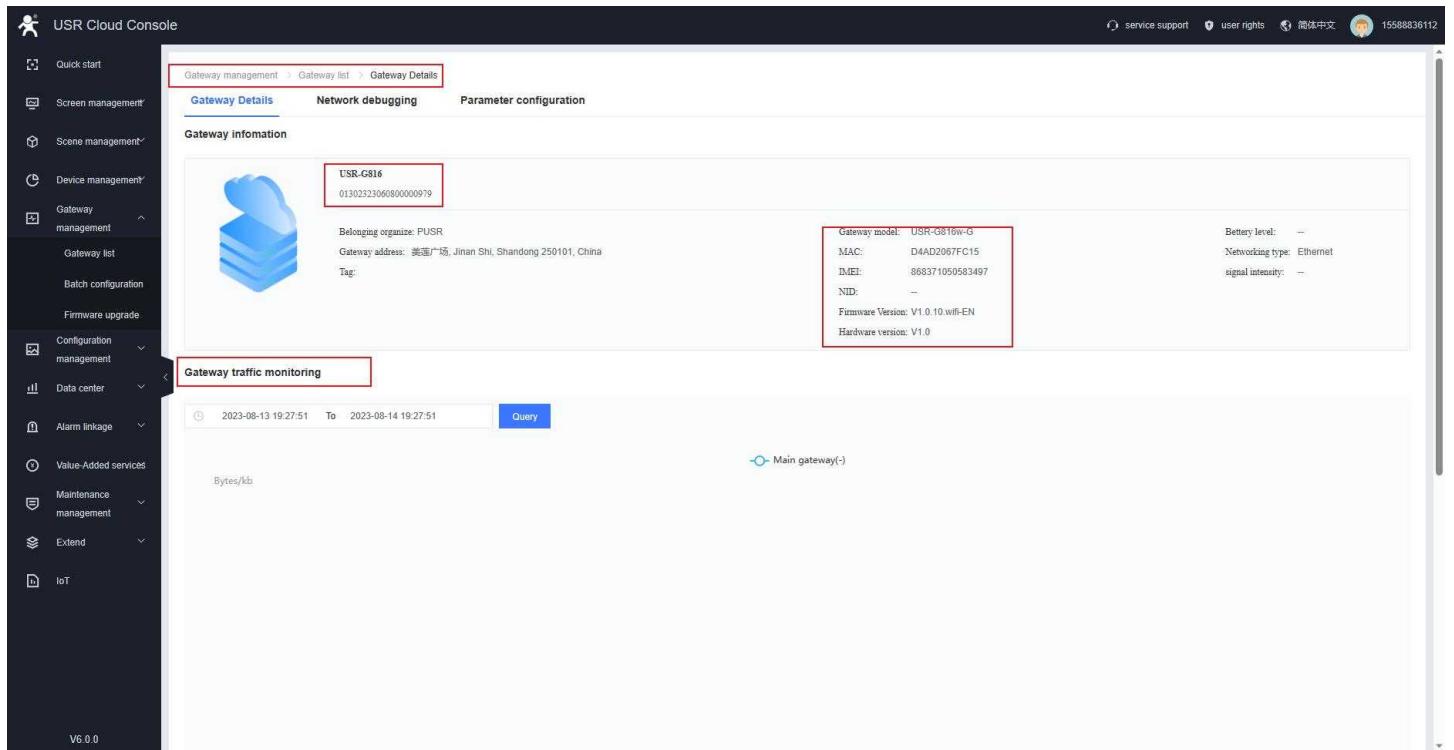


Figure 54. Check gateway information

Users can also send AT command to query parameters of USR-G805s

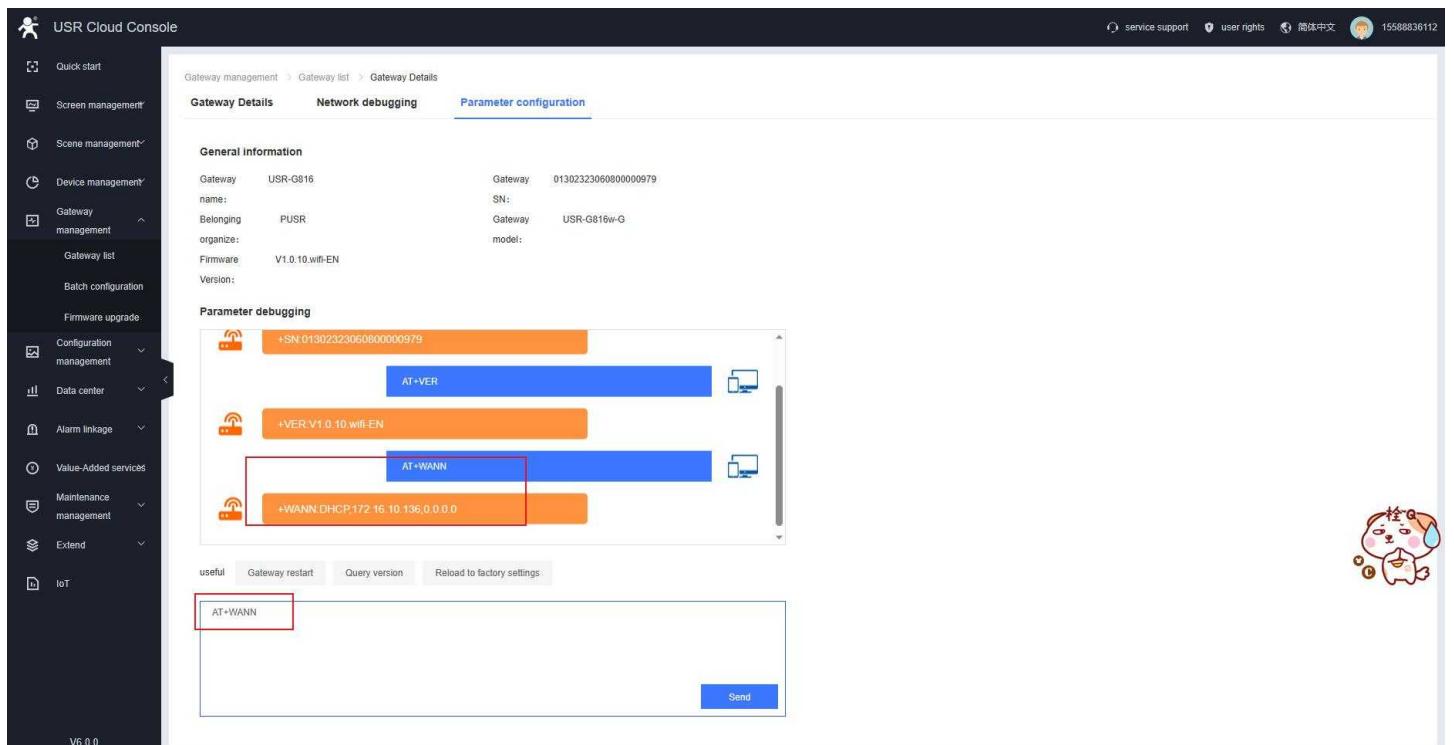


Figure 55. Parameters query and config

7.1.3. Remote access

After the USR-G805s 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 56. Login configuration page

Figure 57. Login page

7.1.4. Firmware upgrade

Users can also upgrade firmware via PUSR platform.

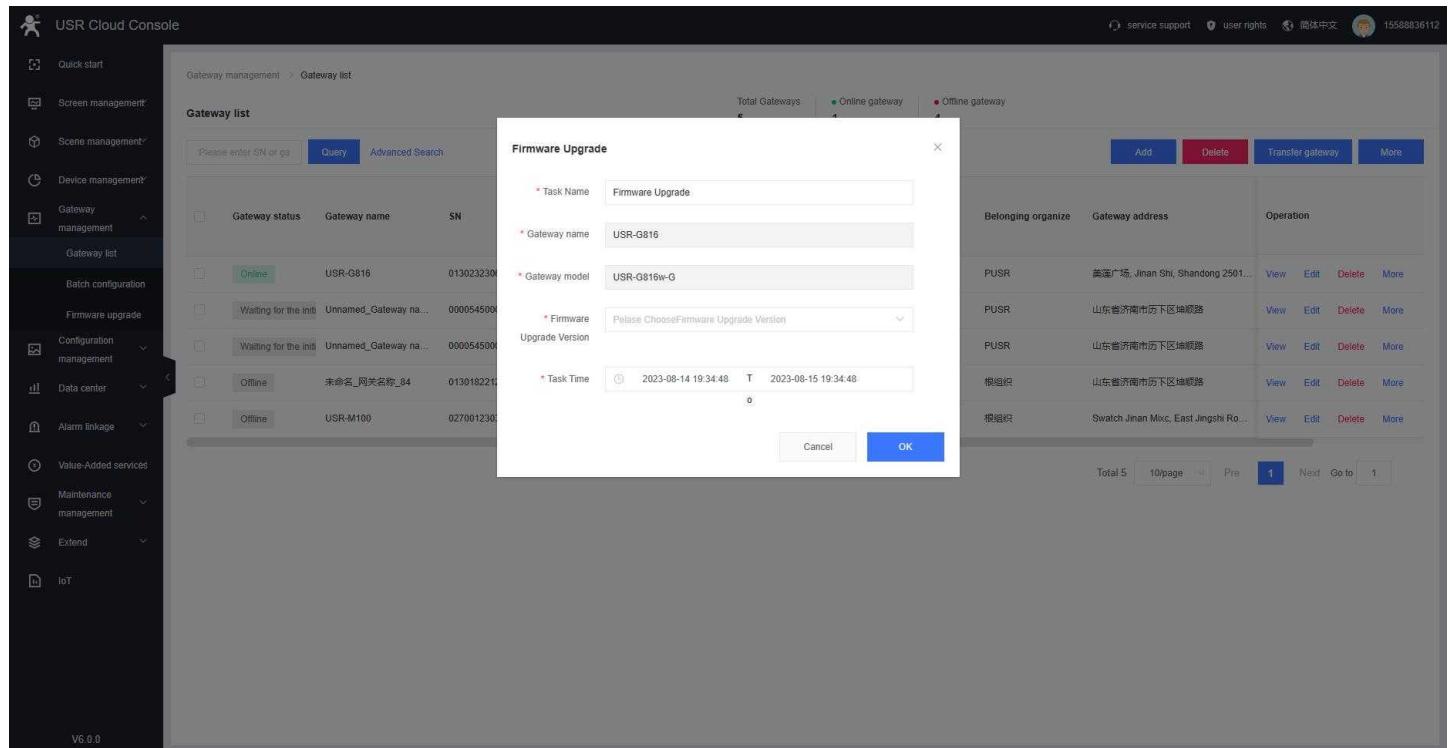


Figure 58. Firmware upgrade function

7.1.5. Alarm settings

➤ Add alarm trigger type, for USR-G805s, we add “Gateway monitoring trigger” .

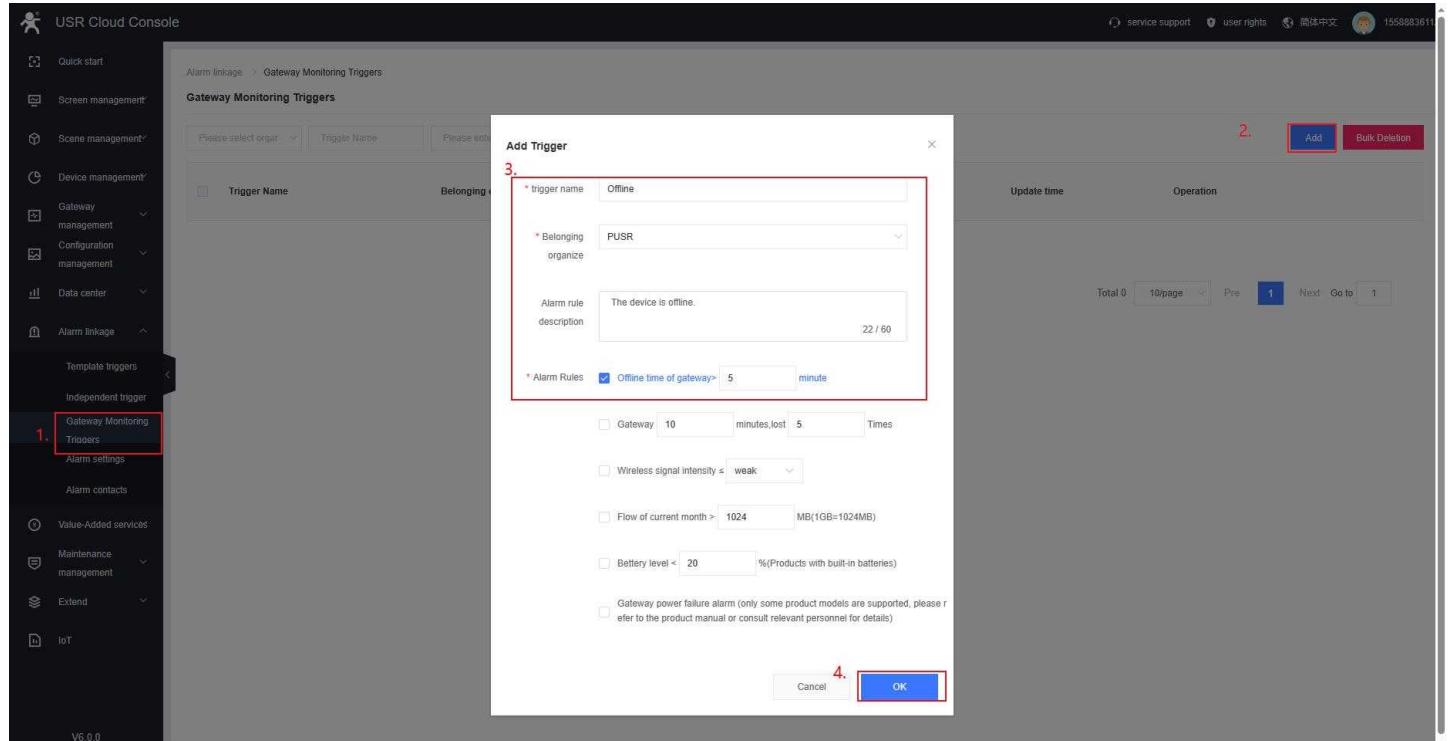


Figure 59. Add alarm trigger type

➤ Add alarm contacts and verify email.

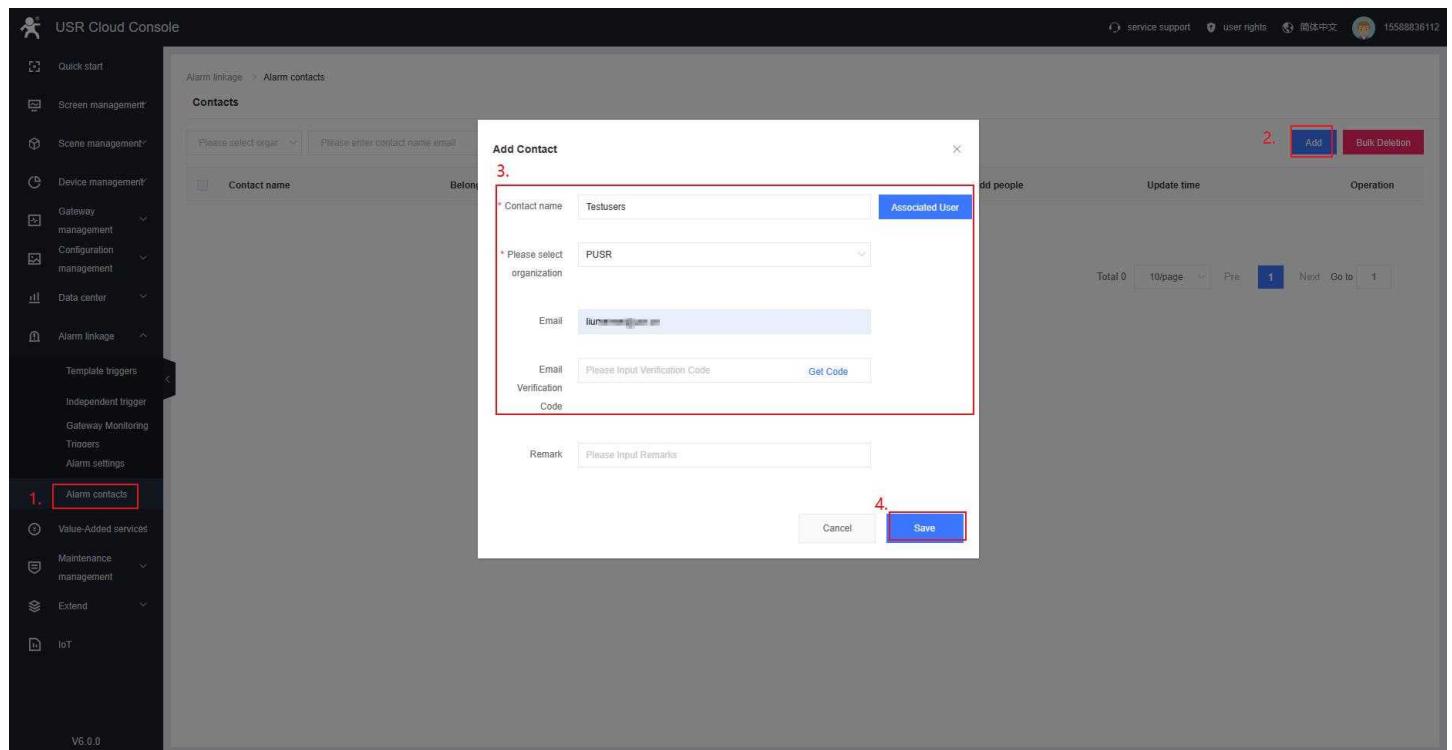


Figure 60. Add alarm contacts

➤Add alarm configuration

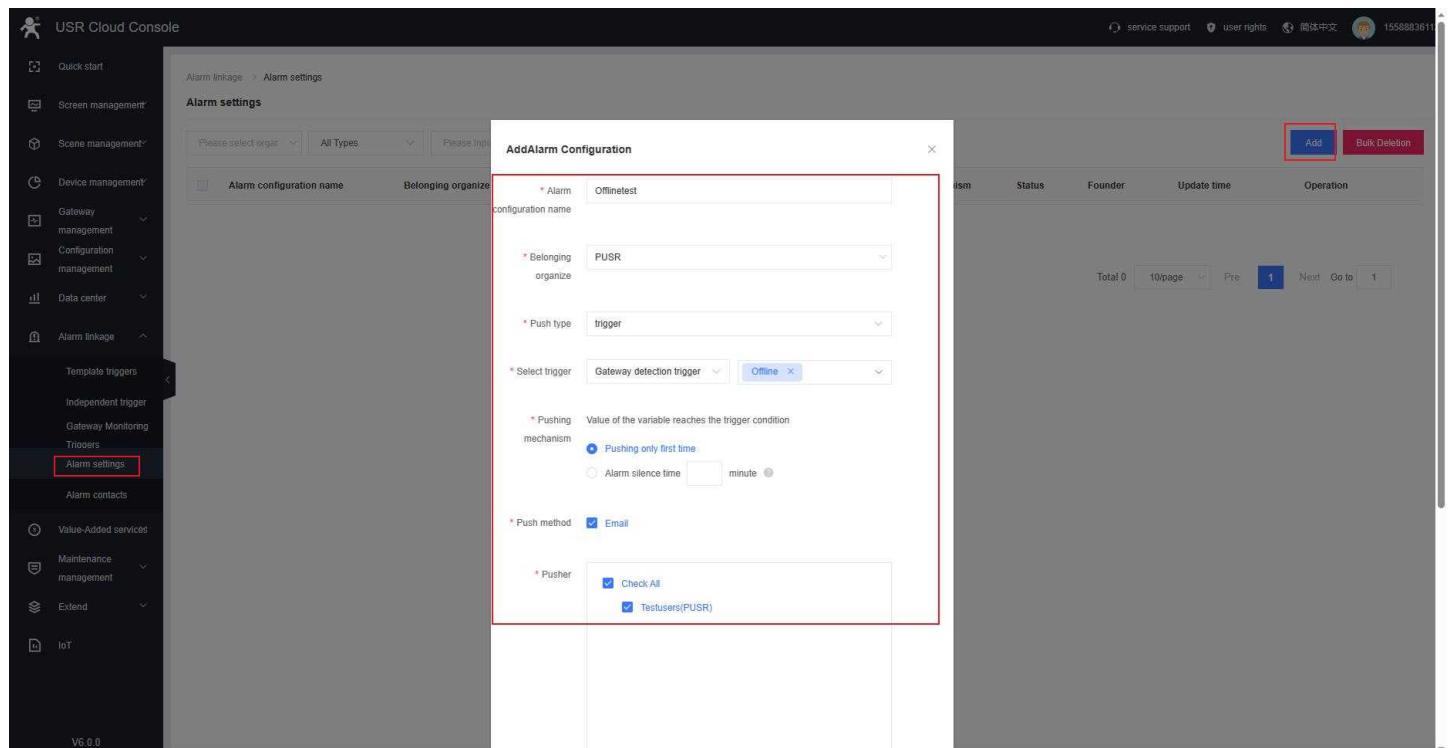


Figure 61. Add alarm configuration

➤Check the alarm email: Power off the USR-G805s

7.2. DDNS

It's disabled by default.

USR-G805

Dynamic DNS

Dynamic DNS configuration allows access to a fixed domain for the host, but the corresponding IP may be dynamic.

Configuration

Enable

Event interface: cellular

Service: dyndns.org

Username: username

Password:

Domain Name:

Sync Time: 300

Forced Update Time: 86400

Apply Save

Figure 62. DDNS function

7.3. SSH function

This function is in developing.

7.4. SNMPD

The G805s supports the Simple Network Management Protocol (SNMP) service. You can use SNMP to remotely view device information and monitor device status without going to the site one by one. The device supports SNMP version V2C and V3.

USR-G805

SNMPD Configuration

SNMPD is a master daemon/agent for SNMP, from the net-snmp project.

Enable SNMP

Enable SNMP

User Info (use for snmpv3)

username: user

auth type: auth

auth mode: SHA

auth passwd:

System Info

sysLocation: JiNan

sysContact: www.pusr.com

sysName: Smart_Router

Apply Save

Items	Description	Default
Enable SNMP	Whether to enable SNMP.	Disable
username	The name assigned to an SNMP user	user
auth type	Auth or auth-enc	auth
auth mode	SHA or MD5	SHA
auth passwd	The encryption password used as the encryption private key	authpass
sysLocation	The location of the device	JiNan
sysContact	The contact of USR-G805s	www.pusr.com
sysName	The system name of USR-G805s	Smart_Router

7.5. SMS

7.5.1. SMS AT function

This router support SMS function. After enabling the function, users can send AT command from SMS to check and to set parameters of USR-G805s.

SMS Authorization Mode is all, the router can receive the SMS command from any phone number and do the action. Users can also set specific phone number, and the router just receive SMS command from authorized phone numbers, it supports add up to 5 phone numbers.

Note: When the user changes the SIM card by SMS command, special attention should be paid to ensure that the SIM card can be normally connected to the network. If the user switches to the SIM card that cannot be connected to the network after executing the SIM switching command, the device will not be able to be connected to the network, and it will no longer be able to query and set parameters through SMS command, thus losing contact with the device.

USR-G805

Short Message Service

Users can control their devices by sending text messages.

Config

Configuration

SMS Enable: Once selected, the SMS function is enabled

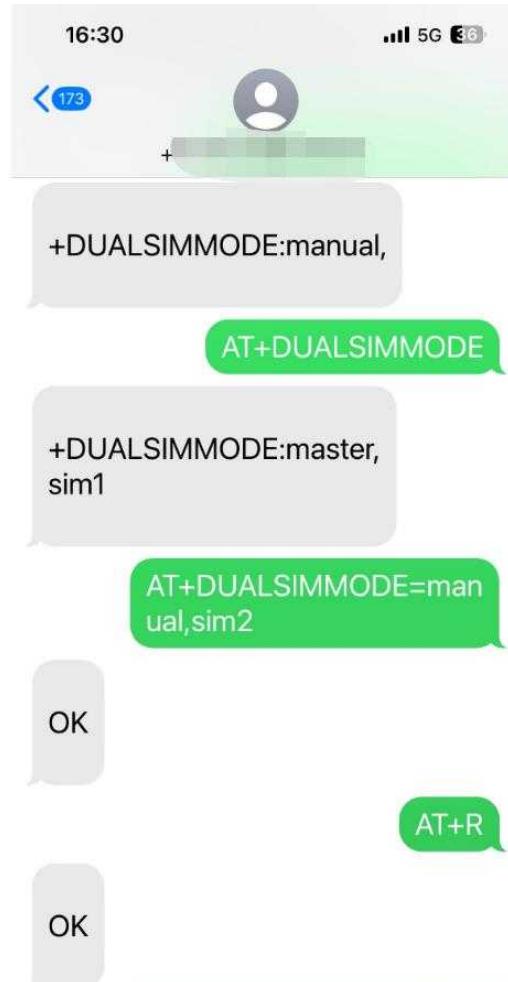
SMS Authorization Mode: all Only receive text messages from authorized phone numbers

Apply Save

Be Honest, Do Best

English | 中文

Query and set parameters of router.



7.5.2. SMS sending

This router support sending message to specified number, and can also record the sent message and received message content on the page, so users can check the

USR-G805

SMS Authorization Mode: All

Only accept SMS AT commands from authorized phone numbers

SMS Send

Receiver Number: 15

The phone number must be 1 to 20 digits long, optionally starting with a '+' sign to indicate an international number.

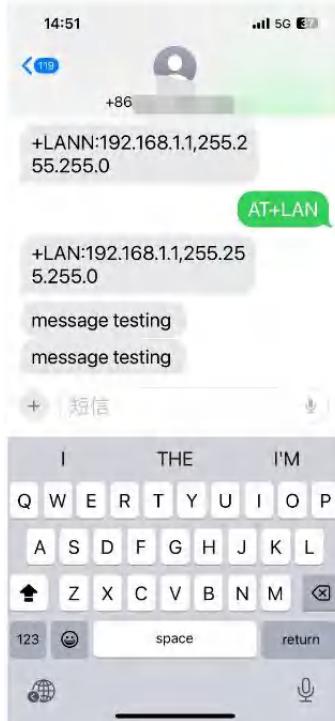
Content: message testing

Please enter your information in this box. You can input up to 70 characters.

Send

SMS Receiving Record

Sender	Time	Content
+8615	2024-09-09 02:41:00	AT+ver
+8615	2024-09-09 02:42:09	AT+VER
+8615	2024-09-09 02:42:29	AT+IMEI
+8615	2024-09-09 02:43:44	AT+DUALSIMMODE
+8615	2024-09-09 02:43:48	AT+IMEI
+8615	2024-09-09 02:43:59	AT+VER
+8615	2024-09-09 02:44:20	AT+CPIN
+861558	2024-09-09 02:44:45	AT+SYSINFO
+861558	2024-09-09 02:45:09	AT+LANN
+861558	2024-09-09 02:45:23	AT+LAN



8. AT Command

8.1. AT command set

Number	Name	Function
1	AT	Test AT command available
2	AT+R	Restart the device
3	AT+CLEAR	Factory data reset
4	AT+VER	Query firmware version
5	AT+MAC	Query current device wan port MAC
6	AT+APN	Query or set 4G APN information
7	AT+SN	Query Device SN
8	AT+CSQ	Query Device 4G Signal Strength
9	AT+CPIN	Inquiry SIM card status
10	AT+IMEI	Query Equipment IMEI
11	AT+ICCID	Inquiry SIM ICCID
12	AT+MCCMNC	Inquiry SIM card CIMI
13	AT+SYSINFO	Query operator and network model
14	AT+CELLULAR	Query the network mode of the device (dedicated to cloud)
15	AT+NETMODE	Query resident network mode
16	AT+WEBU	SearchWebLogin User Name Password
17	AT+PLANG	Query web landing language
18	AT+UPTIME	Query system runtime
19	AT+WANINFO	Query WAN network card information
20	AT+DIALINFO	Query 4G network card information
21	AT+LANINFO	Query LAN card information

22	AT+WANN	Query WAN Port Configuration
23	AT+LANN	Query LAN port configuration
24	AT+LAN	Query/Set LAN Port Configuration
25	AT+PING	Execute ping command
26	AT+NETSTATUS	Query default routing using NIC
27	AT+ALYSIMSWITCH	Query/Switch Operators
28	AT+DUALSIMMODE	Query/set the switch mode and active SIM card

8.2. Description of AT command

8.2.1. AT

name	AT
function	Test AT command
inquire	AT OK
set	not have
parameter	Return: OK
explain	The command takes effect immediately, and returning OK means that the AT command is OK.

8.2.2. AT+R

name	AT+R
function	restart the device
inquire	not have
set	AT+R OK
parameter	not have
explain	The command is executed correctly, OK is replied and the device restarts

8.2.3. AT+CLEAR

name	AT+CLEAR
function	factory data reset
inquire	not have
set	AT+CLEAR
parameter	not have
explain	This command is executed correctly and the device is factory restarted without recovery.

8.2.4. AT+VER

name	AT+VER
function	Query device software version number

inquire	AT+VER +VER:<ver>
set	not have
parameter	ver: Current software version number
explain	This command executes correctly and returns the current software version number.

8.2.5. AT+MAC

name	AT+MAC
function	Query WAN port MAC
inquire	AT+MAC +MAC:<mac>
set	not have
parameter	mac:WAN port MAC
explain	

8.2.6. AT+APN

name	AT+APN
function	Query or setAPNinformation
inquire	AT+APN +APN:<apn_name>,<user>,<pw>,<type>
set	AT+APN=<apn_name>,<user>,<pw>,<type> OK
parameter	apn_name: apn address, can be empty. [0-62] field, support character range [a-zA-Z0-9-.#@] user: username, can be empty [0-62] bytes, ASCII characters within [33-126] pw: password, can be empty [0-62] bytes, ASCII characters within [33-126] type: authentication mode, none/pap/chap
explain	This command is executed correctly, and the configuration takes effect after the device is restarted.

8.2.7. AT+SN

name	AT+SN
function	Query device SN information
inquire	AT+SN +SN:<sn>
set	not have
parameter	sn:20 bit sn code
explain	

8.2.8. AT+CSQ

name	AT+CSQ
function	Query Device 4G Signal Strength
inquire	AT+CSQ +CSQ:<csq>
set	not have
parameter	csq: cellular signal value
explain	not have

8.2.9. AT+CPIN

name	AT+CPIN
function	Query SIM card status
inquire	AT+CPIN +CPIN:<cpin>
set	not have
parameter	cpin:SIM card status value
explain	

8.2.10. AT+IMEI

name	AT+IMEI
function	Query Equipment IMEI
inquire	AT+IMEI +IMEI:<imei>
set	not have
parameter	imei: Equipment IMEI number
explain	

8.2.11. AT+ICCID

name	AT+ICCID
function	Inquiry SIM ICCID
inquire	AT+ICCID +ICCID:<iccid>
set	not have
parameter	ICCID:SIM card ICCID number
explain	

8.2.12. AT+MCCMNC

name	AT+MCCMNC
function	Inquiry SIM card CIMI
inquire	AT+MCCMNC +MCCMNC:<cimi>
set	not have
parameter	cimi:SIM card cimi number

explain	
---------	--

8.2.13. AT+SYSINFO

name	AT+SYSINFO
function	Query SYSINFO information
inquire	AT+SYSINFO +SYSINFO:<ops_operate>,<ops_net_type>
set	not have
parameter	ops_operate: operator information ops_net_type: network mode
explain	

8.2.14. AT+CELLULAR

name	AT+CELLULAR
function	Query resident network mode
inquire	AT+CELLULAR +CELLULAR:<ops_net_type>
set	not have
parameter	ops_net_type: network mode
explain	

8.2.15. AT+NETMODE

name	AT+NETMODE
function	Query resident network mode
inquire	AT+NETMODE +NETMODE:<type>
set	not have
parameter	type: cellular network standard
explain	

8.2.16. AT+WEBU

name	AT+WEBU
function	LoginUser name Password
inquire	AT+WEBU +WEBU:<user>,<pw>
set	not have
parameter	User:Web login User name pw:web login password
explain	

8.2.17. AT+PLANG

name	AT+PLANG
------	----------

function	Query web landing language
inquire	AT+PLANG +PLANG:<plang>
set	AT+PLANG=<plang> OK
parameter	plang:zh_cn/en zn_cn: Chinese en: English
explain	

8.2.18. AT+UPTIME

name	AT+UPTIME
function	Query system runtime
inquire	AT+UPTIME +UPTIME:<time>
set	not have
parameter	time
explain	

8.2.19. AT+WANINFO

name	AT+WANINFO
function	Query WAN network card information
inquire	AT+WANINFO +WANINFO:<mac> <ip> <mask> <rx_packets> <tr_packets> <rx_bytes> <tx_bytes>
set	not have
parameter	mac: wan mac ip:wan IP card mask:wansubnet maskrx_packets: number of packets received tr_packets: number of packets sent rx_bytes: received traffic tx_bytes: send traffic
explain	

8.2.20. AT+DIALINFO

name	AT+DIALINFO
function	Query 4G network card information
inquire	AT+DIALINFO +DIALINFO:<mac> <ip> <mask> <rx_packets> <tr_packets><rx_bytes> <tx_bytes>
set	not have
parameter	Mac:4G MAC ip:4G IP card mask:4GNIC subnet maskrx_packets: number of packets received tr_packets: number of packets sent rx_bytes: receive traffic tx_bytes: send traffic
explain	

8.2.21. AT+LANINFO

name	AT+LANINFO
function	Query LAN card information
inquire	AT+LANINFO +LANINFO:<mac> <ip> <mask> <rx_packets> <tr_packets><rx_bytes> <tx_bytes>
set	not have
parameter	mac:LAN card mac ip:LAN card IP mask:LAN card subnet mask rx_packets: Number of packets received tr_packets: Number of packets sent rx_bytes: receive traffic tx_bytes: send traffic Note: If VLAN is configured, this command returns LAN information
explain	

8.2.22. AT+WANN

name	AT+WANN
function	Query WAN Port Configuration
inquire	AT+WANN +WANN:<type>,<ip>,<mask>,<gateway>
set	not have
parameter	type:WANport protocol typeip:WANIP mask:WAN subnet mask gateway:WAN gateway
explain	

8.2.23. AT+LANN

name	AT+LANN
function	Query LAN port configuration
inquire	AT+LANN +LANN:<ip>,<mask>
set	not have
parameter	ip:LAN IP mask:LAN subnet mask Note: If VLAN is configured, this command returns LAN information
explain	

8.2.24. AT+LAN

name	AT+LAN
function	Query/Set LAN Port Configuration
inquire	AT+LAN +LAN:<ip>,<mask>
set	AT+LAN=<ip>,<mask>
parameter	ip:LAN IP Standard IP address format x.x x:[0-255] mask:LAN subnet mask x.x.x.x x:[0-255] conforms to subnet mask standard format Note: If VLAN is configured, this command returns LAN information
explain	

8.2.25. AT+PING

name	AT+PING
------	---------

function	Execute ping command
inquire	not have
set	AT+PING=<ip> PING IP(IP): 56 data bytes
parameter	ip:IP or domain name, cannot be null, invalidpingparameter,e.g. -c1 invalid Limitations [1-200) Note: Parameters can only be associated with IP or domain names
explain	

8.2.26. AT+NETSTATUS

name	AT+NETSTATUS
function	Query default routing using NIC
inquire	AT+NETSTATUS +NETSTATUS:<net>
set	not have
parameter	net: Internet card status at this time
explain	

8.2.27. AT+ALYSIMSWITCH

name	AT+ALYSIMSWITCH
function	Query/Switch Operators
inquire	Send:AT+ ALYSIMSWITCH[= Carrier Type]> Return to: stat>
set	not have
parameter	Carrier type: CMCC/ CUCC/ CTCC CMCC: Mobile CUCC: Unicom CTCC: Telecom state:OK/+NONE Return OK means successful setting and start switching (does not mean successful switching)
explain	If you do not use Cloud Eagle Card, please do not send this command.

8.2.28. AT+DUALSIMMODE

name	AT+DUALSIMMODE
function	Query/set the switch mode and active SIM card
inquire	Send:AT+ DUALSIMMODE Return to: +DUALSIMMODE:<dualsim_mode>[,<sim_fixed>]

set	AT+DUALSIMMODE=<dualsim_mode>[,<sim_fixed>] OK
parameter	dualsim_mode: Master:Master standby mode Mutual:Mutual standby mode Manual: Manual mode sim_fixed: sim1: sim1 is active sim2: sim2 is active
explain	

9. 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

10. 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.

FCC STATEMENT :

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.



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

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](#)