

# Waterproof 4G Wireless Router AP510

**Manual**

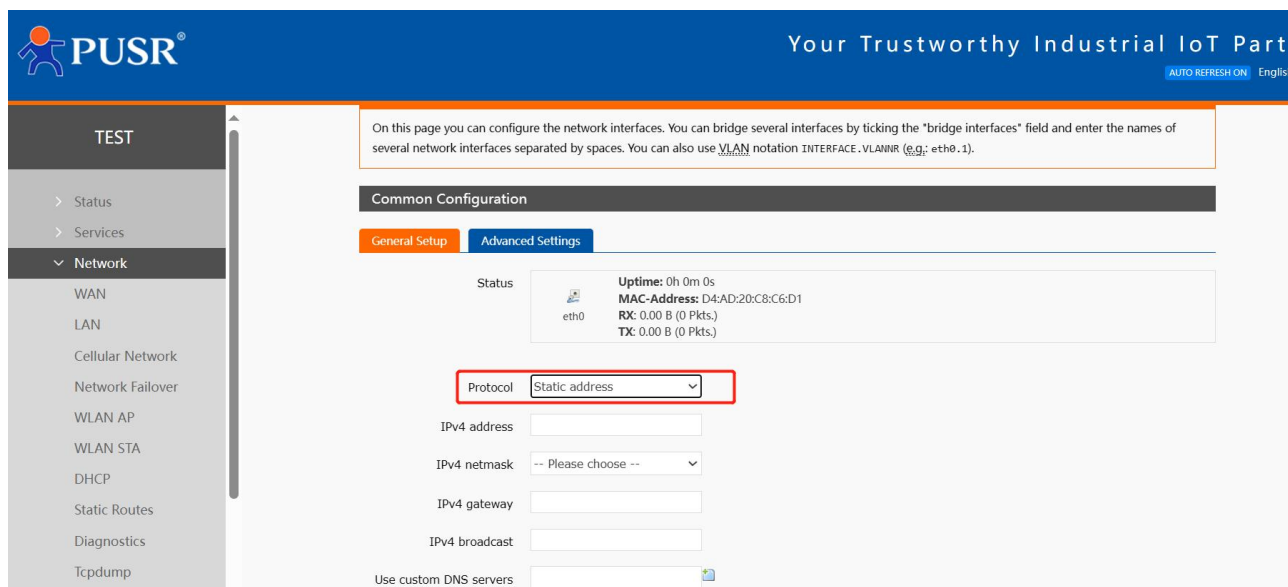
Industrial IoT Gateways Ranked First in China by Online Sales for Seven Consecutive Years

\*\*Data from China's Industrial IoT Gateways Market Research in 2023 by Frost & Sullivan

**Your Trustworthy Smart Industrial IoT Partner**

## Content

1. Product introduction .....	5
1.1. Product features .....	5
1.2. Consumption .....	7
1.3. Indicators .....	7
1.4. Dimensions .....	8
2. Operation Instruction .....	8
2.1. Test .....	8
3. Network interface function .....	10
3.1. WAN networks .....	10
3.1.1. Cellular network configuration .....	10
3.1.2. SIM .....	12
3.1.3. SIM card information .....	13
3.2. LAN .....	13
3.2.1. DHCP Server of LAN .....	15
3.2.2. VLAN .....	15
3.2.3. WAN/LAN Select .....	16
3.2.4. DHCP .....	17
3.3. WAN_wired interface .....	17
3.3.1. DHCP mode .....	17
3.3.2. Static IP mode .....	18
3.3.3. PPPoE .....	19
3.4. Network switching .....	19
3.5. Wireless configuration .....	20
3.5.1. Wireless AP mode .....	20



3.6. Wireless client .....	21
3.7. Static routing .....	23
3.8. Network diagnostic function .....	25
3.9. TCPDUMP traffic monitoring .....	25
4. VPN function .....	26
4.1. PPTP Client .....	26
4.2. L2TP Client .....	29
4.3. IPSec .....	31
4.4. OpenVPN .....	33
4.4.1. OpenVPN TAP bridge example .....	41
4.4.2. An example of subnet interworking in OpenVPN TUN mode .....	45
4.5. GRE .....	50
5. Firewall .....	51
5.1. Basic Settings .....	51
5.2. Traffic rules .....	52
5.2.1. IP address blacklist .....	53
5.2.2. IP address whitelist .....	55
5.3. NAT function .....	57
5.3.1. IP address spoofing .....	57
5.3.2. SNAT .....	57
5.3.3. DNAT .....	错误！未定义书签。
5.3.4. Port forwarding .....	60
5.3.5. NAT DMZ .....	62
5.4. Access restrictions .....	63
5.4.1. Domain blacklists .....	63
5.4.2. Domain name whitelist .....	63
6. Service function .....	64
6.1. Dynamic domain name resolution (DDNS) .....	64
6.1.1. Supported services .....	64
6.1.2. DDNS come into force .....	65
6.1.3. functional characteristics .....	66
6.2. SSH Port .....	66
6.3. SMS .....	67
6.4. SNMPD .....	68
7. system function .....	70
7.1. host name .....	70
7.2. Time Settings .....	70
7.3. Login password Settings .....	71
7.4. HTTP port .....	71
7.5. Parameter backup and upload .....	72
7.6. factory data reset .....	72
7.7. firmware upgrade .....	73

---

7.8. restart .....	73
7.9. Restart at regular intervals .....	74
7.10. Daily record .....	74
8. AT order set .....	75
8.1. AT code repertory .....	75
8.1.1. AT order set .....	76
9. Disclaimer .....	85
10. Update log .....	85



## 1. Product introduction

The AP510 is a high-speed waterproof 4G wireless router featuring global cellular band. It supports dual Ethernet ports (including standard 48V PoE IN), Qualcomm WiFi (AP/STA/Bridge modes), and a built-in eSIM (eliminating the need for a physical SIM card for customers), providing customers with high-speed and reliable connectivity.

Housed in an IP65 waterproof enclosure, it withstands high temperatures up to 75°C and low temperatures down to -40°C, making it particularly suitable for providing wired and wireless networks in outdoor areas where running cables is inconvenient. Applicable scenarios include: scenic area monitoring, construction site monitoring, orchard monitoring, farm monitoring, reservoir monitoring, community monitoring, rural household monitoring, mountainous area monitoring, and other challenging monitoring environments where network deployment is difficult.

### 1.1. Product features

#### ✧ Stable and reliable

- Qualcomm chip to ensure the performance and stability.
- IP65 rated, wide operating temperature range (-40°C to 75°C), suitable for outdoor scenarios.
- Optional installations: poll and wall mounting
- Dual power supply redundancy: standard 48V PoE IN / DC 9-36V with reverse polarity protection
- Built-in hardware watchdog which can provide self-diagnostics and self-recovery to ensure system stability.

#### ✧ Uninterrupted Network Access

- Supports 2G/3G/4G network all over the world ,supports APN/VPDN sim card.
- Failover between 4G, WAN and WiFi, ensures automatic switch to alternative backup connection,effectively ensuring
- Equipped with strong Wi-Fi capability,802.11 a/b/g/n,2.4G Wi-Fi,2\*2 MIMO, up to 300Mbps,Support AP/STA/repeater mode
- VPN tunnel detection: maintains stable connection of the VPN tunnel, ensuring continuous transmission.
- Multi-layer link detection mechanism, automatic redial and recovery.

#### ✧ Powerful Functionality

- Supports remote monitoring, upgrade and parameter configuration, remote access to the built-in web pages.
- Supports IPsec VPN, PPTP,L2TP, OPENVPN,GRE etc., ensuring secure data transmission.
- Supports firewall, NAT,DMZ,black and white list of access control.
- Supports DDNS,PPPOE,DHCP,Static IP.
- Supports firewall functions including NAT, access control, DDoS defense, IP-MAC binding, etc., protecting the network against external attacks.
- Support SNMP,VLAN

**Tab 1 AP510 Specification**

Project	describe
---------	----------

## AP510 manual

Cellular	Band(China, India)	LTE FDD: B1/3/5/8 LTE TDD: B34/38/39/40/41 WCDMA: B1/5/8 GSM: 900/1800MHz
	Band(global)	TDD-LTE:Band 34/38/39/40/41 FDD-LTE: Band 1/2/3/4/5/7/8/12/13/18/19/20/25/26/28/66 WCDMA:B1/2/4/5/6/8/19 GSM/GPRS/EDGE: B2/3/5/8
	Antenna	Built-in full bidirectional antenna
	SIM slot	1 x Nano-SIM
Ethernet	WAN	1 x WAN port (can be configured to LAN) 10/100 Mbps, compliance with IEEE 802.3, supports auto MDI/MDIX
	LAN	1 x LAN port, 10/100 Mbps, compliance with IEEE 802.3, IEEE 802.3u standards, supports auto MDI/MDIX,
Wi-Fi	Standards & Frequency	IEEE 802.11b/g/n, 2.4GHz
	Mode	AP/STA/Repeater
	Data speed	300Mbps
	Antenna	Built-in full bidirectional antenna
	Transmission distance	50 meters by line of sight.Actual transmission distance depends on environment of the site.
	MIMO	2 x 2
	WiFi users	8
Power supply	Adaptor	DC 12V/1A
	Connector	DC Power Jack Barrel Type Female 5.5*2.1mm Round socket or 2 PIN industrial terminal block, reverse polarity protection
	Input voltage	DC 9-36V
	Power consumption	12V@300mA
physical characteristics	Casing material	IP65 rated, ABS material
	Dimensions	172.06*89.94*57.06mm
	Installation	Poll mounting and 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	-40°C to +75°C
	Storage Temperature	-40°C to +85°C (non-condensing)
	Operating Humidity	5%-95% (non-condensing)

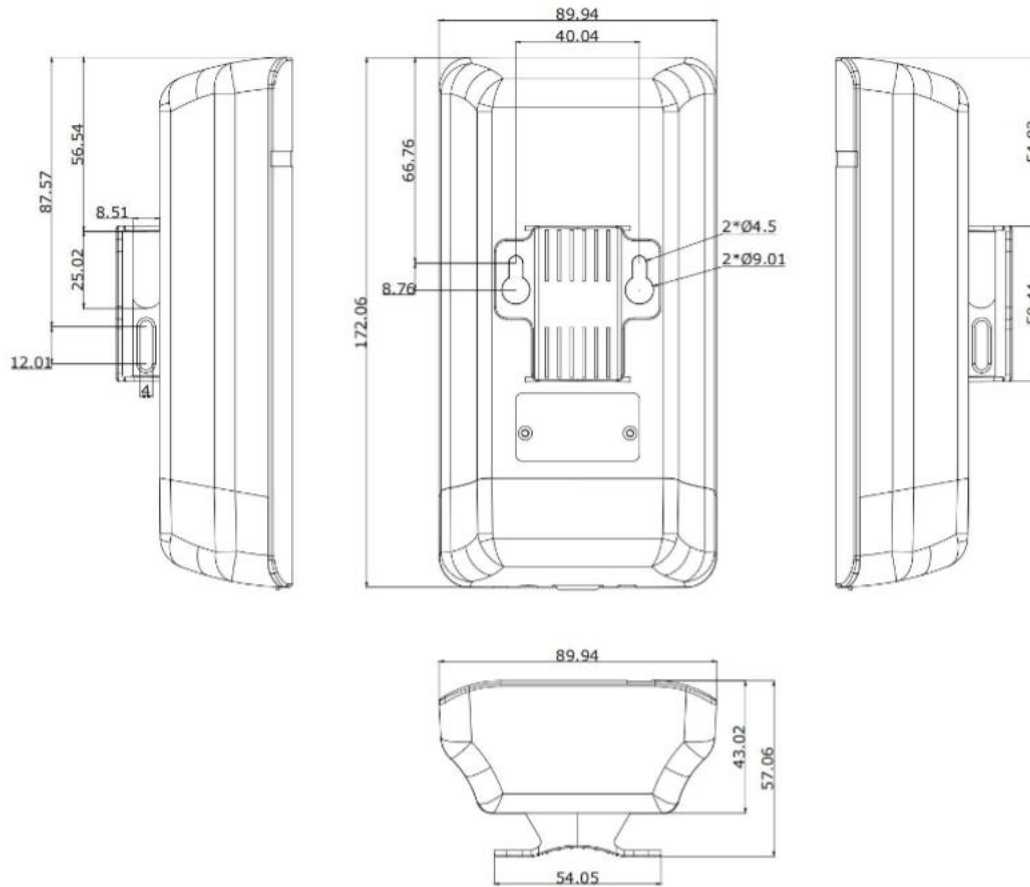
other	Indicators	POWER、WIFI、NET、SIG、WAN/LAN1、LAN2
	Reload button	Long press 5-15s to reset to factory settings

## 1.2. Consumption

## 1.3. Indicators

Indicators	Status
Power	ON: Power supply is normal.
WiFi	ON: the WiFi is open. OFF: the WiFi is closed.
NET	ON: connected to 4G network. Fast flashing: connected to 3G network. Slow flashing: connected to 2G network. OFF: not connect to cellular network.
SIG	Blue: the signal is strong. Dual-color: the signal is medium. Red: the signal is week.
WAN/LAN1	Flashing: there are data transmitting. ON: the network cable is connected. OFF: the network cable is not connected.
LAN2	Flashing: there are data transmitting. ON: the network cable is connected. OFF: the network cable is not connected.

## 1.4. Dimensions



**Pic 1 AP510 Dimensions**

## 2. Operation Instruction

### 2.1. Test

When the AP510 is used for the first time, you can connect the LAN port of the AP510 to the PC or connect to the WLAN wireless, and then configure it using the web management page.

**Tab 2 Default parameter table for WEB pages**

parameter	default setting
SSID	AP510-XXXX
LAN IP	192.168.1.1
User name	admin
password	admin
Wireless password	88888888

AP510 English | 中文

**PUSR®** Your Trustworthy Industrial IoT Partner

**Authorization Required**  
Please enter your username and password.

Username:

Password:

Pic 2 Login page

**PUSR®** Your Trustworthy Industrial IoT Partner [AUTO REFRESH ON](#) English | 中文

**TEST**

▼ Status

- Overview
- Routes
- > Services
- > Network
- > VPN
- > Firewall
- > System
- > Logout

**Status**

**System**

Hostname	TEST
Firmware Version	V1.0.05
SN	0150112506060002052
IMEI	869312068015691
Local Time	Sat Oct 11 06:16:55 2025
Uptime	1h 19m 43s
Load Average	0.55, 0.62, 0.64

**Memory**

Total Available	88412 kB / 125028 kB (70%)
Free	58292 kB / 125028 kB (46%)
Cached	22660 kB / 125028 kB (18%)
Buffered	7460 kB / 125028 kB (5%)

Pic 3 Status overview

You can query routing information and ARP tables from here.

**PUSR®** Your Trustworthy Industrial IoT Partner English | 中文

**TEST**

▼ Status

- Overview
- Routes**
- > Services
- > Network
- > VPN
- > Firewall
- > System
- > Logout

**Routes**

The following rules are currently active on this system.

**ARP**

IPv4 Address	MAC Address	Interface
192.168.1.115	c8:5a:c2:f6:68:4b	br-lan
10.29.29.61	32:ef:86:d9:94:e5	eth2

**Active IPv4-Routes**

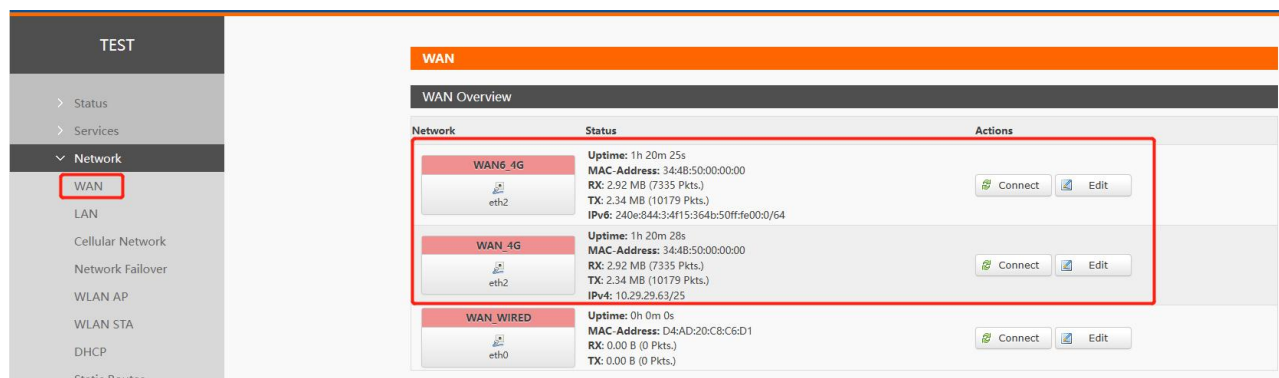
Network	Target	IPv4-Gateway	Metric	Table
wan6_4g	0.0.0.0/0	10.29.29.61	0	main
wan6_4g	0.0.0.0/0	10.29.29.61	10	main
wan6_4g	10.29.29.0/25		10	main
wan6_4g	10.29.29.61		10	main
lan	192.168.1.0/24		0	main

Pic 4 ARP

### 3. Network interface function

#### 3.1. WAN networks

The router supports WAN ports for access to external networks.

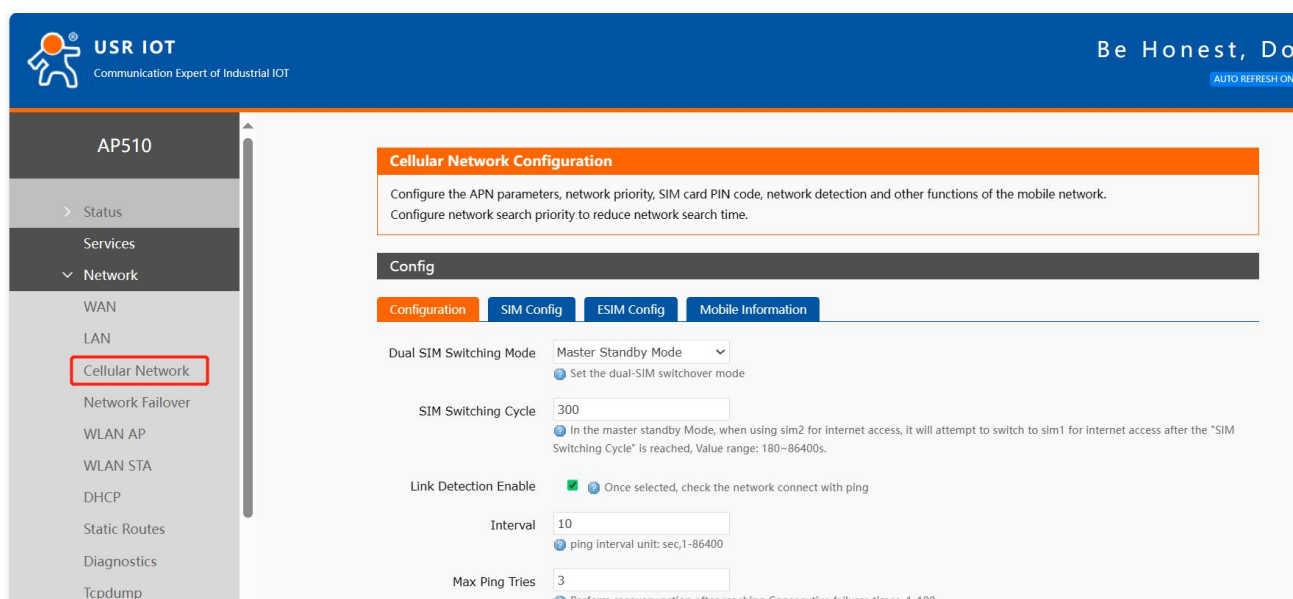


**Pic 5 4G Set up the interface**

**Tab 3 state table**

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

#### 3.1.1. Cellular network configuration



**Pic 6 Cellular network configuration page**

Note: The regular shipment of CPE does not have an ESIM card attached. There is a reserved space on the hardware circuit. If the customer requires an ESIM, it can be achieved through customization.

**Tab 4 Cell network configuration parameter table**

Item	function	default
Dual card switching mode	<p><b>Master-Backup Mode:</b> External SIM is the primary. When external SIM malfunctions, it automatically switches to ESIM for internet access. Once external SIM recovers, it will switch back to external SIM automatically.</p> <p><b>Mutual Backup Mode :</b> If the current SIM card can access the internet, no card switching will occur.</p> <p><b>Manual Mode:</b> Lock onto external SIM or ESIM, disabling automatic card switching. This function need the ESIM is attached.</p>	Master Standby Mode
Check the cycle	At present, when the card is connected to the network, the threshold time set here will detect whether external SIM returns to normal (the cellular network will be disconnected each time). If external SIM is restored, it will automatically switch to external SIM access. Unit: seconds	300
Fixed SIM card	When the mode is switched to manual mode, select the SIM card to be locked	external SIM
Link probing enabled	Open: Enable the SIM card Ping detection function Close: Disable the SIM card Ping detection function	Close
Detection time interval	Ping detection interval, unit: seconds	10
Number of re-tries for detection	Number of ping probe failures	3
Probe address 1	A total of 3 Ping addresses are detected. If one of them is pingable, the link is considered normal	8.8.8.8
Probe address 2	A total of 3 Ping addresses are detected. If one of them is pingable, the link is considered normal	119.29.29.29
Probe address 3	A total of 3 Ping addresses are detected. If one of them is pingable, the link is considered normal	255.5.5.5
Resume the exercise	Optional: None / Re-dial / Restart module / Restart module / Restart device	Restart the module
Signal strength detection enabled	Checked: detect the interval time once, and switch the SIM card when the sub-signal is less than the set trigger threshold for multiple times	Unchecked
Detection time interval	Signal detection interval time, unit: second	10
Number of re-tries	If the signal value is less than the threshold for several times, the	3

for detection	card will be cut	
Trigger threshold	Signal threshold, unit: dbm	-80
Ping delay detection is enabled	Checked : The interval time is detected once, and the delay of multiple probes is greater than the set trigger threshold to switch the SIM card	Unchecked
Detection time interval	Detection interval time, unit: seconds	10
Number of re-tries for detection	If the detection delay exceeds the threshold, the card will be cut	3
Trigger threshold	Delay threshold, unit: ms	80

### 3.1.2. SIM

Set the external SIM/ESIM card related parameters.

**Cellular Network Configuration**

Configure the APN parameters, network priority, SIM card PIN code, network detection and other functions of the mobile network.  
Configure network search priority to reduce network search time.

**Config**

Configuration | **SIM Config** | ESIM Config | Mobile Information

APN: Automatic  
☐ Input your APN Name, 0-62 characters

Username:   
☐ User name for apn, 0-62 characters

Password:   
☐ User password for apn, 0-62 characters

Auth Method: PAP AND CHAP  
☐ Authentication type for apn

Network Type: AUTO

LTE band selection: auto  
☐ Enter 'auto' or '1' or '123.....'  
 Supported LTE frequency bands: 13583438394041

PDP Type: IPV4&V6

MTU: 1500  
☐ 1280-1500

**Pic 7 SIM**

**Tab 5 SIM**

Item	Description	Default
APN	Please set the correct APN address	Auto
Username	APN username	empty
Password	APN Password	empty
Auth Method	APN authentication type: None/PAP/CHAP	empty
Network Type	Force 4G, 3G or 2G network	Auto
LTE band selection	Lock the frequency band	Auto
PDP Type	IPv4/IPv6/IPv4&v6 are optional	IPv4&v6
MTU	Set the cellular network card MTU	1500
Network search priority	Auto/2G/3G/4G	Auto
PIN enable	SIM PIN	Not enabled



PIN	Four to eight digits Note: The PIN code is invalid if the PIN enablement item is not enabled	1234
EHRPD	This option is generally not required when 5G network is started	Not enabled

### 3.1.3. SIM card information

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

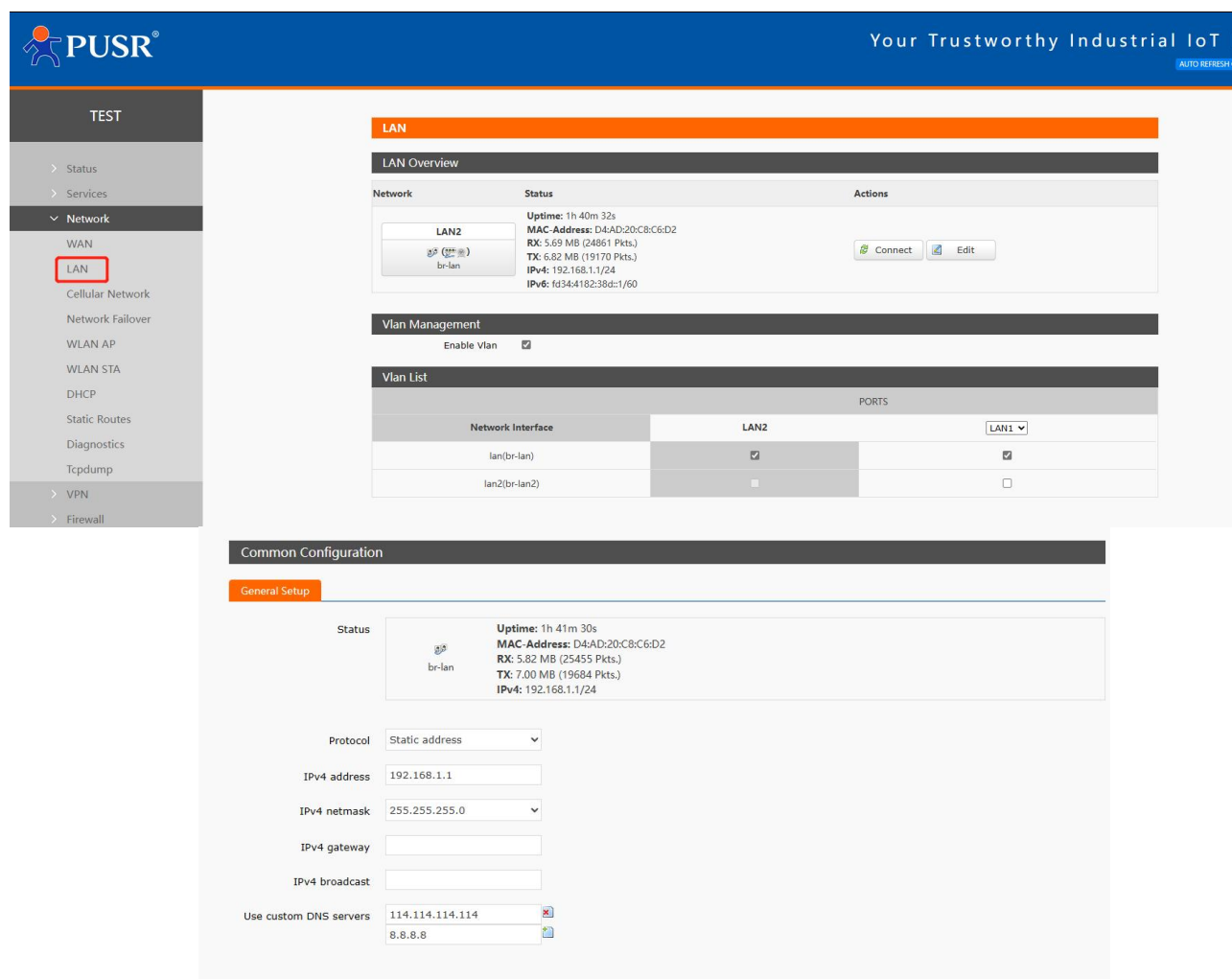
The screenshot displays the PUSR web interface. The top header includes the PUSR logo and the tagline "Your Trustworthy Industrial IoT Partner". A navigation menu on the left lists various settings, with "Cellular Network" highlighted. The main content area shows the "Cellular Network Configuration" section, which includes a description and a "Config" tab. Under the "Config" tab, the "Mobile Information" sub-tab is selected, displaying a table of cellular network parameters.

Mobile Information	
Modem Version:	17016.1000.00.38.01.31
IMEI:	869312068015691
Dial SIM:	sim2
SIM Status:	READY
ICCID:	89861125205036721193
CIMI:	460113311031408
APN:	ctnet.ctnet@mycdma.cn_vnet.mobi,1
Attachment Status:	Attached
Network Operator:	CHN-CT
Network Type:	4G Mode
MCC:	460
MNC:	11
BAND:	3
IP Address:	10.29.29.63

**Pic 8 SIM Information**

## 3.2. LAN

LAN port is a LAN with 2 wired LAN ports (LAN1 can be set to WAN for use, the default is WAN port).



Pic 9 LAN

Tab 6 LAN

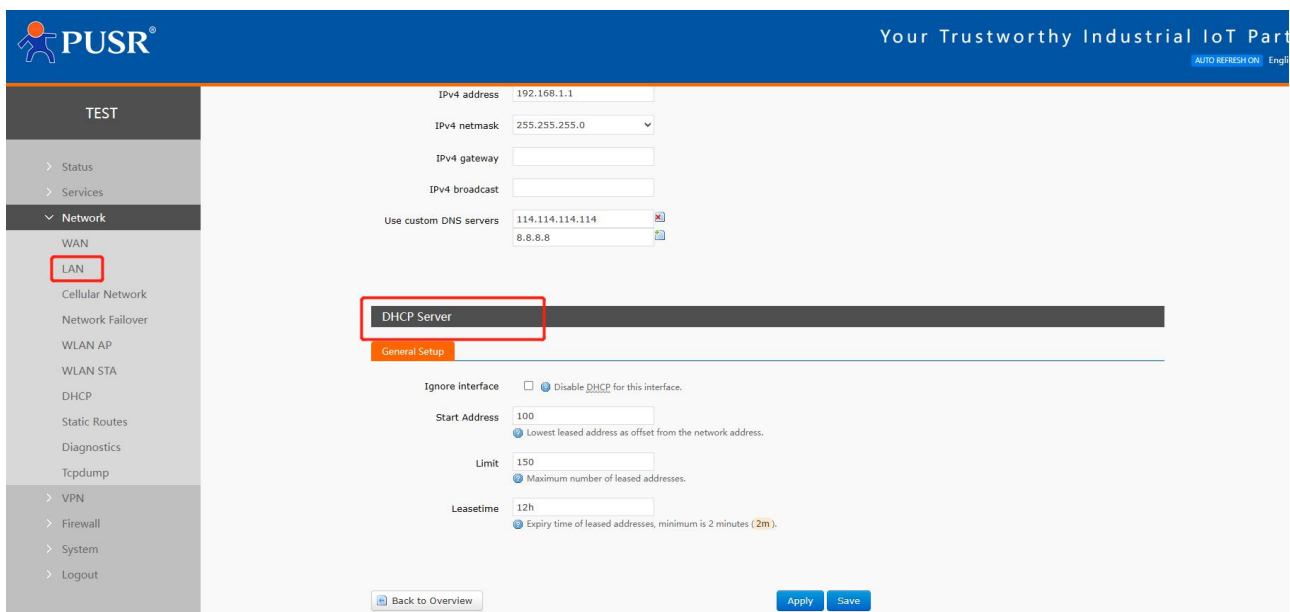
Item	meaning	Windows default
IPv4	The IP address of the LAN card	192.168.1.1
subnet mask	The subnet mask of the network card	255.255.255.0
IPv4 Gateway	The gateway address of the LAN card is usually empty	empty
IPv4 broadcast	The broadcast address of the LAN card is usually empty	empty
Use a custom DNS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

## < Instruction >

- The default static IP address is 192.168.1.1 and the subnet mask is 255.255.255.0. This parameter can be modified, for example, to change the static IP address to 192.168.2.1;
- The DHCP server function is enabled by default, and the devices connected to the LAN port of the router can automatically obtain IP addresses;
- If VLAN division is used, the WIFI interface is bridged to the br-lan port, and the WIFI obtains IP and the same network segment as the br-lan network card.

### 3.2.1. DHCP Server of LAN

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



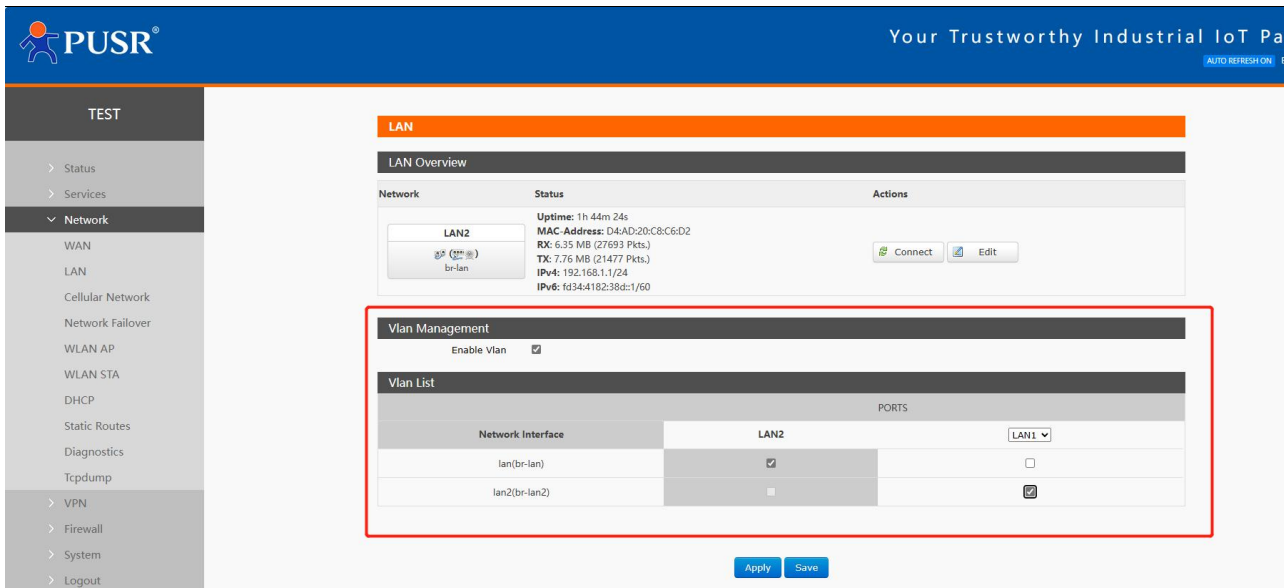
Pic 10 DHCP

## < instruction >

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

### 3.2.2. VLAN

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



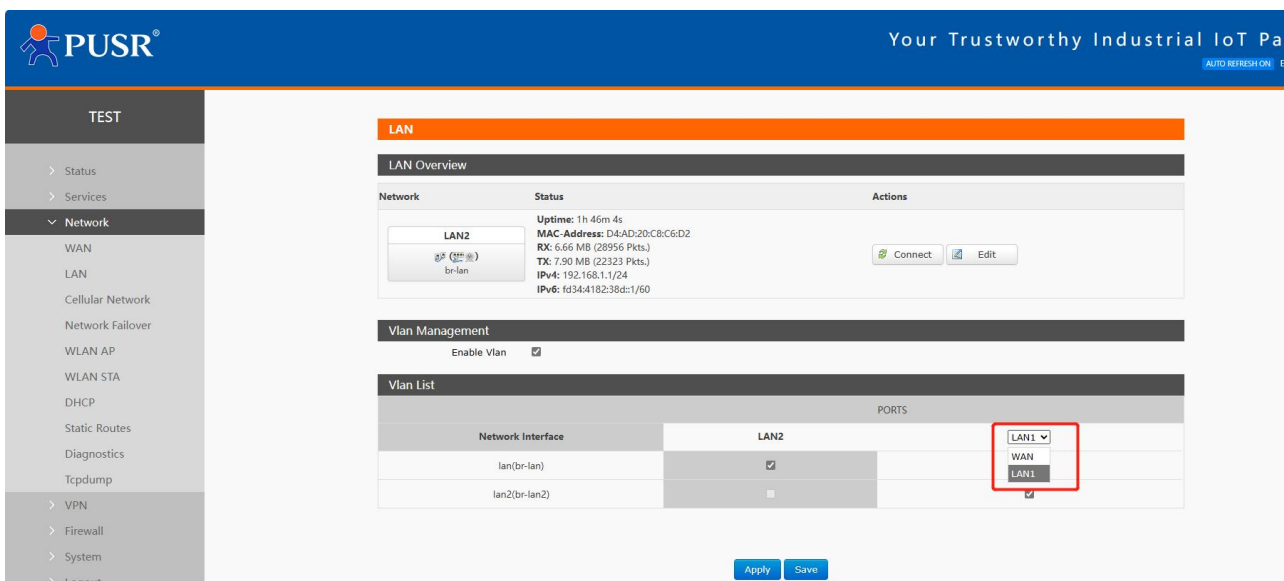
Pic 11 LAN

### < explain>

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

### 3.2.3. WAN/LAN Select

After the VLAN switch is turned on, LAN1 can be set to WAN.

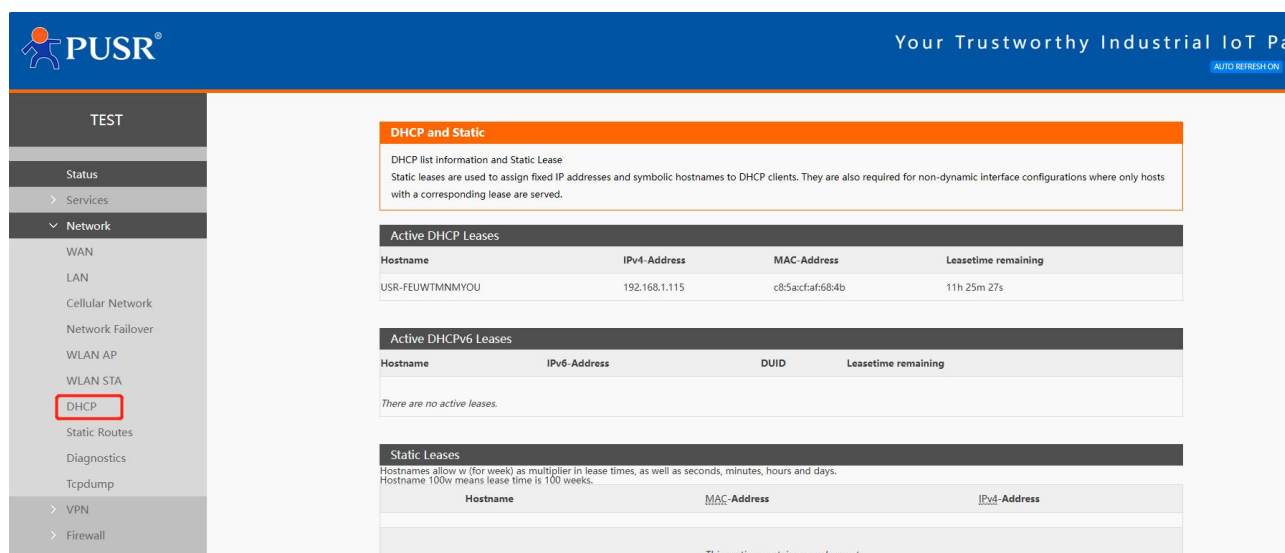


Pic 12 VLAN

### 3.2.4. DHCP

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

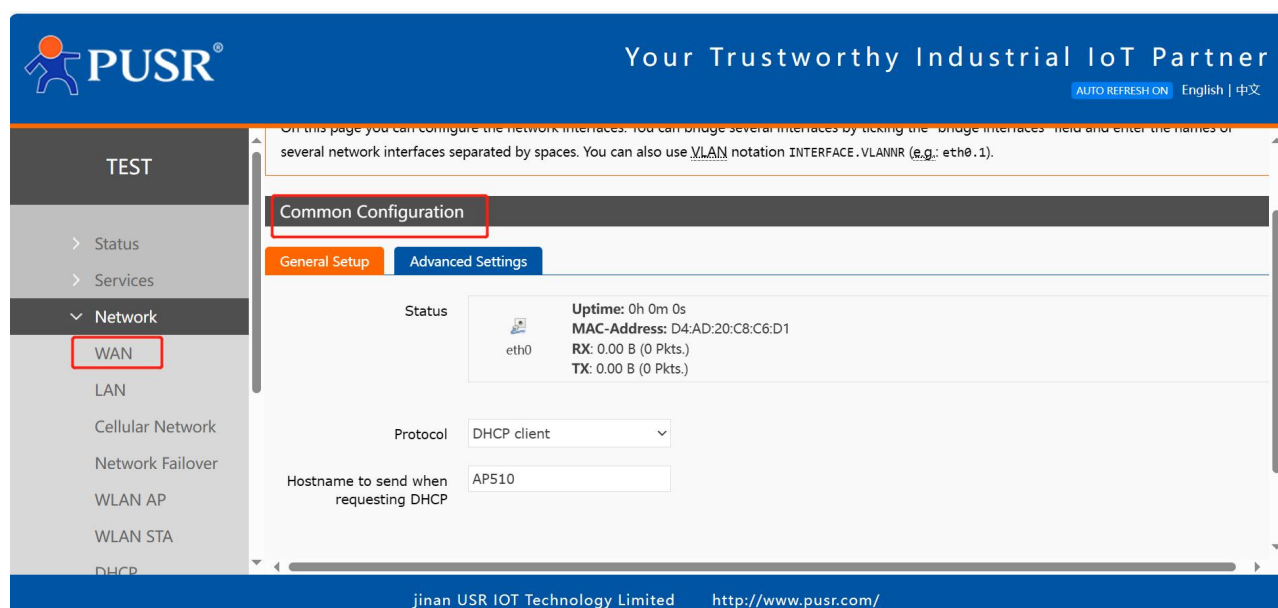
Use add to add new lease entries. Use the MAC address to identify the host, the IPv4 address to assign the address, and the hostname to assign the identifier.



Pic 13 DHCP

## 3.3. WAN\_wired interface

### 3.3.1. DHCP mode

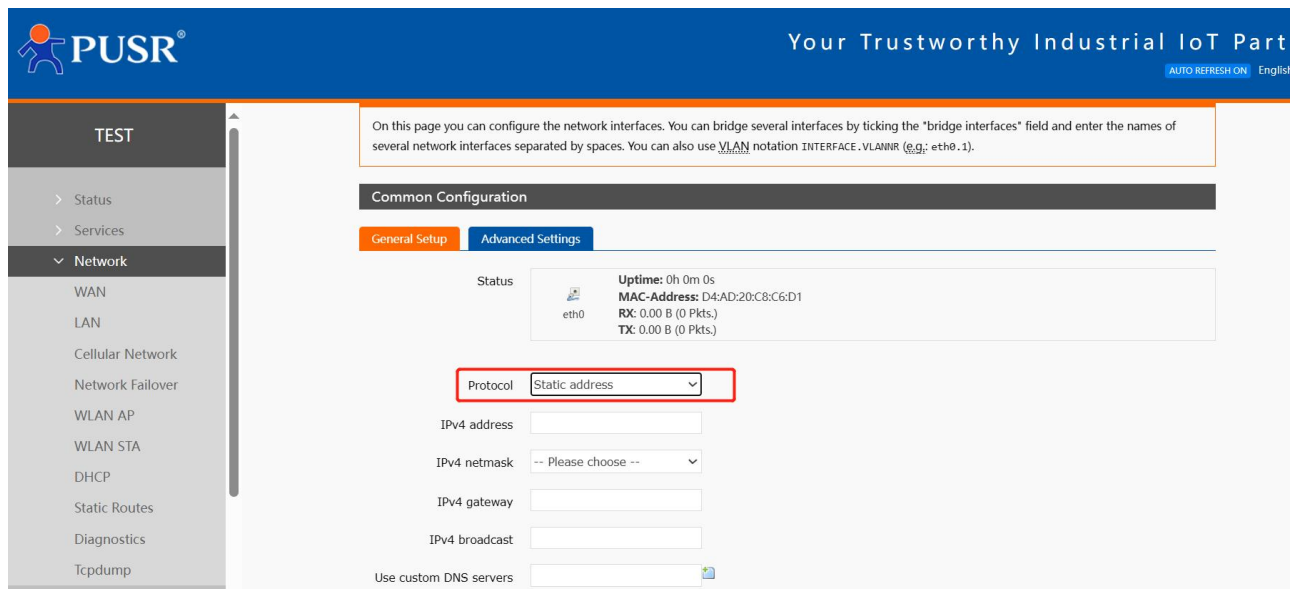


Pic 14 WAN

**< explain>**

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

## 3.3.2. Static IP mode



Pic 15 WAN

**< explain>**

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

## 3.3.3. PPPoE

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANID (e.g.: eth0.1).

**Common Configuration**

**General Setup** **Advanced Settings**

Status Uptime: 0h 0m 0s  
MAC-Address: D4:AD:20:C8:C6:D1  
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](#)

Pic 16 WAN

## &lt; explain &gt;

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

## 3.4. Network switching

**Network Failover**

Configure the network switching function.

**Configuration**

Priority **WAN>Cellular>STA**

Reference Mode **Custom**

Primary Server **8.8.8.8**  
IP or Domain, such as "223.6.6.6" or "baidu.com"

Secondary Server **119.29.29.29**  
IP or Domain, such as "223.6.6.6" or "baidu.com"

Thirdly Server **223.5.5.5**  
IP or Domain, such as "223.6.6.6" or "baidu.com"

Ping Interval **10**  
1-600seconds

Package size **0**

Pic 17 Network switching configuration

Tab 7 Network switching configuration

name	description	Default parameter
------	-------------	-------------------

## AP510 manual

priority	Set the NIC priority policy here For example, select: WAN> Cellular> STA. When the WAN network card can detect the target address is open, the WAN network card will be used to access the Internet. When the WAN network card fails to detect the target address, the Cellular, and STA network cards will be used in sequence to detect the target address. Disable: Use the last network	WAN takes precedence
reference pattern	Customization: Determine the network status based on the custom reference address Gateway: Probe the gateway address of each network card to determine the network status	custom
Reference 1	You can set IP/domain name	8.8.8.8
Reference 2	You can set IP/domain name	119.29.29.29
Reference 3	You can set IP/domain name	223.5.5.5
Detection interval (unit: s)	Set the link detection interval: 1-600s can be set	10
Ping packet size (unit: bytes)	Packet size for link detection: 32-1024 bytes can be set	0
Ping timeout (unit: ms)	Set the ping timeout time: can set 100-20000ms	2000

## 3.5. Wireless configuration

### 3.5.1. Wireless AP mode

The screenshot shows the PUSR AP510 web interface. The top header includes the PUSR logo and the tagline 'Your Trustworthy Industrial IoT'. The left sidebar contains a 'TEST' menu with options like Status, Services, Network, WAN, LAN, Cellular Network, Network Failover, WLAN AP (highlighted), WLAN STA, DHCP, Static Routes, Diagnostics, Tcpdump, VPN, Firewall, and System. The main content area is titled 'Z4G Settings' and 'Client Information'. The 'Z4G Settings' tab is active, showing configuration options for the WLAN AP. The 'Client Information' section displays: Status: Mode: Master, SSID: AP510-C6D1, BSSID: D4:AD:20:C8:C6:D3, Channel: 6 (2.437 GHz), Tx-Power: 26 dBm. Below this, the 'Enable' checkbox is checked. The 'Hide SSID' checkbox is unchecked. The 'SSID' field contains 'AP510-C6D1'. The 'Encryption' dropdown is set to 'mixed-psk'. The 'Key' field is masked with asterisks. The 'HW Mode' dropdown is set to '11ng'. The 'Channel' dropdown is set to 'auto'. The 'HT Mode' dropdown is set to 'auto'. The 'Regions' dropdown is set to '00 - World'. There are informational icons next to the 'Channel' and 'HT Mode' dropdowns indicating that the configuration is affected by the STA.

**Pic 18 Wi-Fi configuration intent**

### < explain >

- Wi-Fi load capacity: 8 devices.
- The maximum Wi-Fi coverage range in open areas is 50 meters.

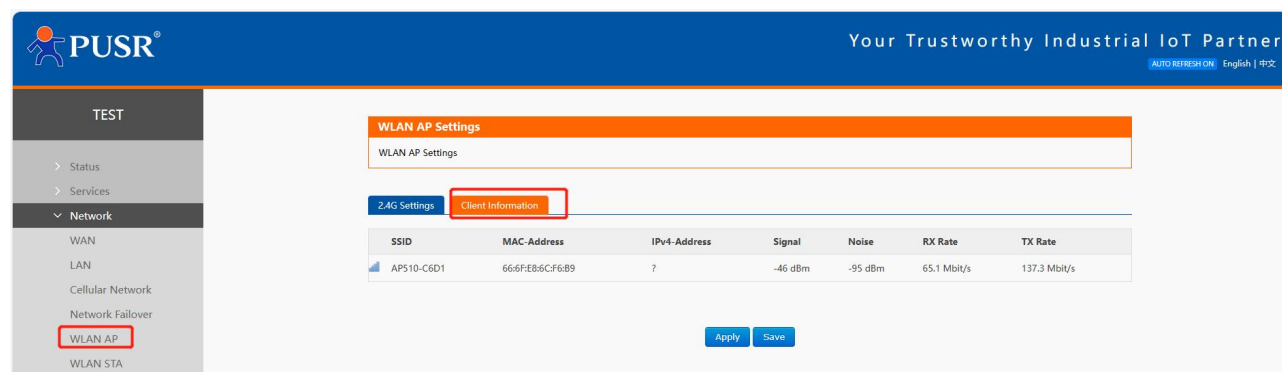


- The actual Wi-Fi connection distance is greatly affected by the environment. Please refer to the actual test results.

**Tab 8 WiFi configuration parameter**

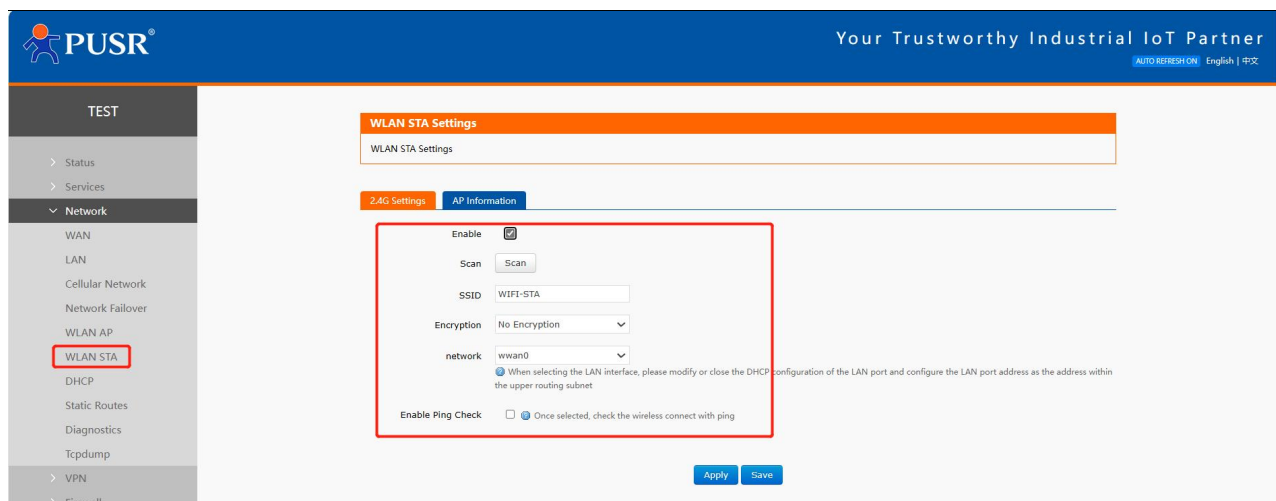
name	description	default
enable	Turn on the WIFI LAN function	checked
hide SSID	To enable this function: The device will not be able to search for 806w WIFI, and you need to manually enter the correct WIFI name and password to connect, ensuring the WIFI security	Not selected
WIFI name	The router's WIFI name can be customized The default value of XXXX is the last four bits of the router MAC	AP510-XXXX
encryption	selectable : No encryption/mixed-psk/psk+ccmp/psk2/psk2-tkip	mixed-psk
password	WIFI password, customizable	88888888
Network model	Options: 11ng/11n/11g/11bgn/11bg/11b	11ng
channel	Automatic, lockable channel	auto
frequency bandwidth	Auto/40MHz/20MHz is optional	auto
Country or region	You can select a country or region	00-world

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

**Pic 19 WiFi client list page**

### 3.6. Wireless client

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

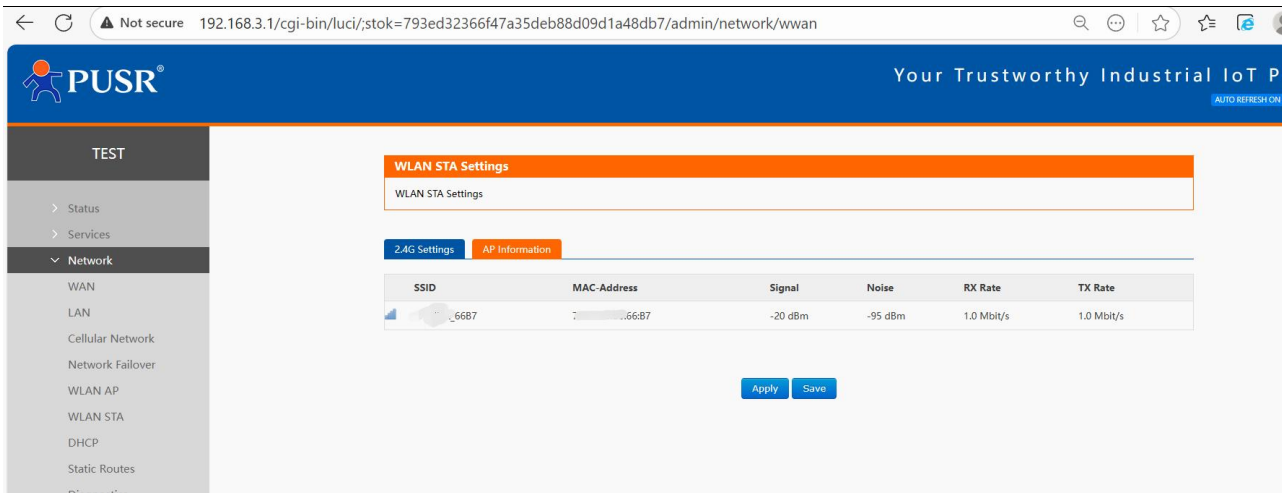


Pic 20 Wireless client configuration

Tab 9 WiFi configuration parameter

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

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



**Pic 21 Connect to the AP information page**

### < explain >

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

## 3.7. Static routing

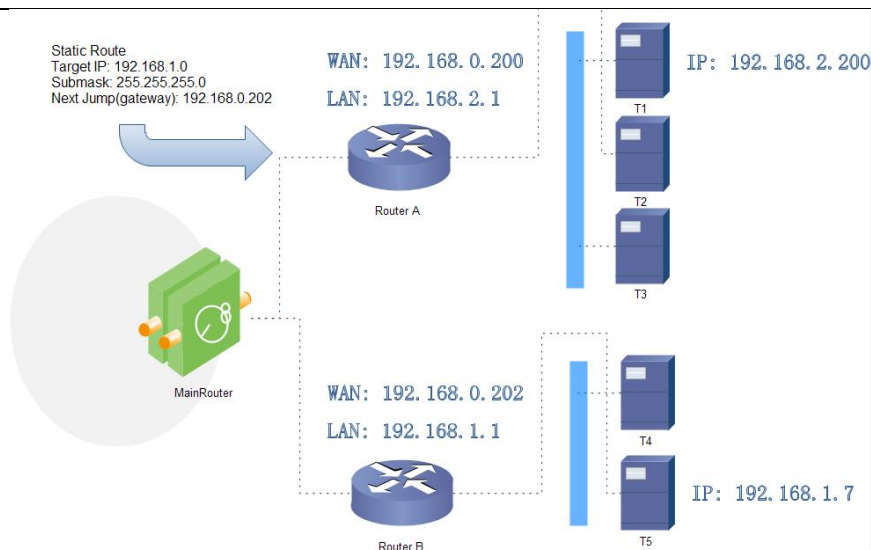
Static routes have the following parameters. The default static route can be added up to 20.

**Tab 10 Static routing parameter table**

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

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

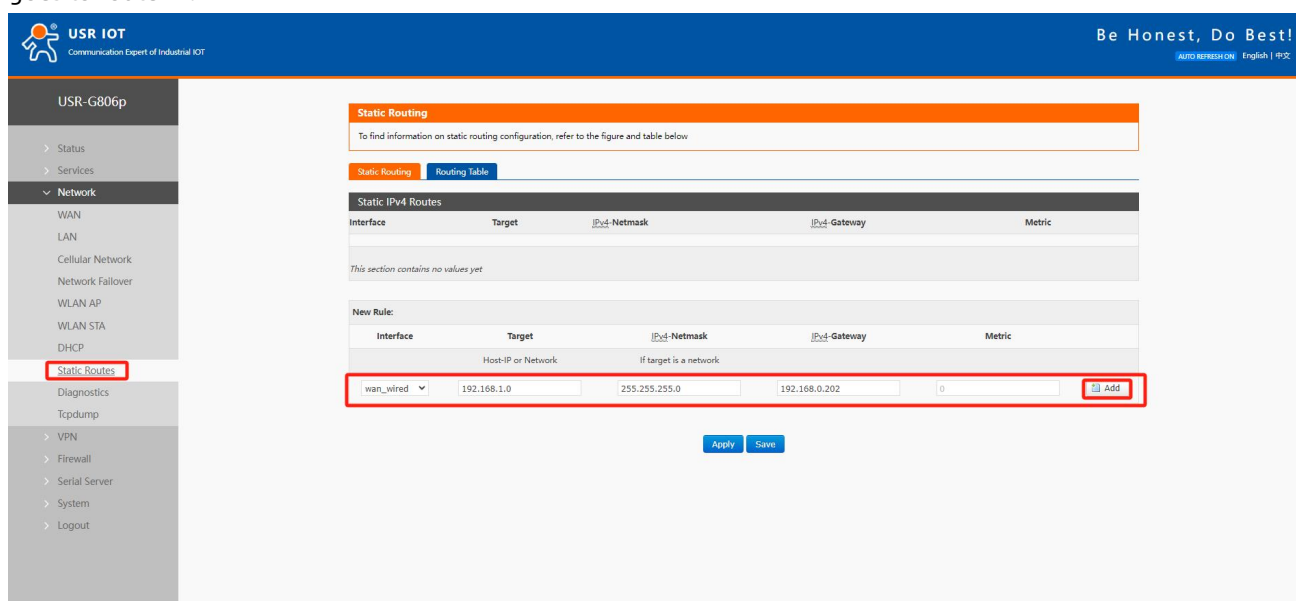
Test example: Test environment, two peer routers A and B, as shown in the figure below.



Pic 22 An example of a static routing table

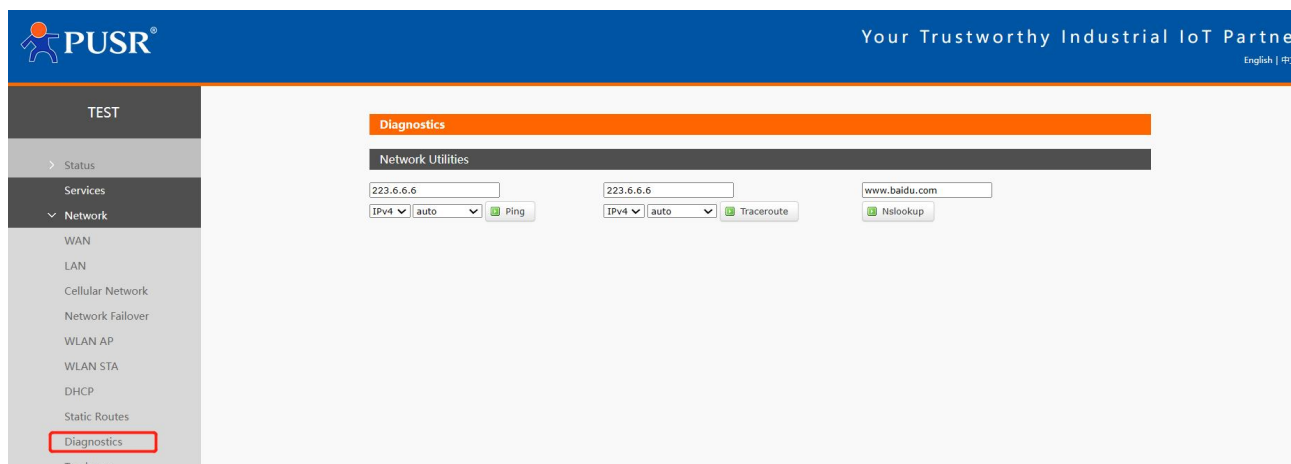
The WAN ports of routers A and B are connected to the network 192.168.0.0, the LAN port of router A is the subnet 192.168.2.0, and the LAN port of router B is the subnet 192.168.1.0.

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



Pic 23 Route table add page

### 3.8. Network diagnostic function



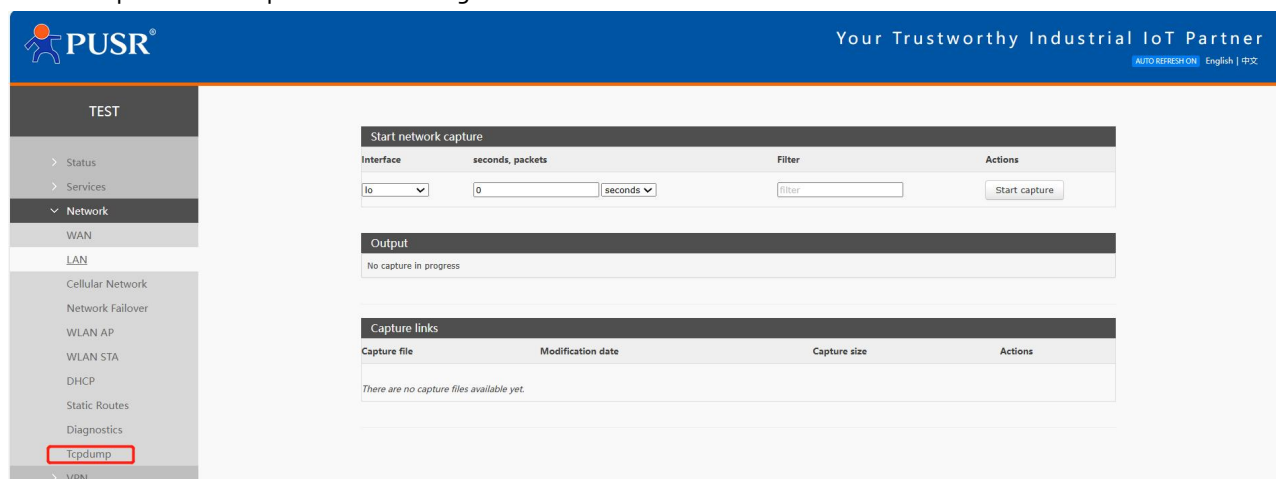
**Pic 24 Network diagnostic interface**

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

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

### 3.9. TCPDUMP traffic monitoring

Packet capture can be performed through the web interface.



**Pic 25 TCPDUMP**

**Tab 11 WiFi configuration parameter**

name	description	Windows default
Interface	Select the capture interface Br-lan: LAN interface Wan_wired: WAN interface Wan2_wir: WAN2 interface Wan_4G: Cellular interface	Lo

	Ath1: WIFI STA interface	
Capture restrictions	Capture duration or number of packets	0 seconds
filter	Fill in the filter conditions for the Tcpdump command, such as port 80	empty

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

## 4. VPN function

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

### 4.1. PPTP Client

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

**Pic 26 Router adds VPN operation diagram 1**

**Tab 12 PPTP configure**

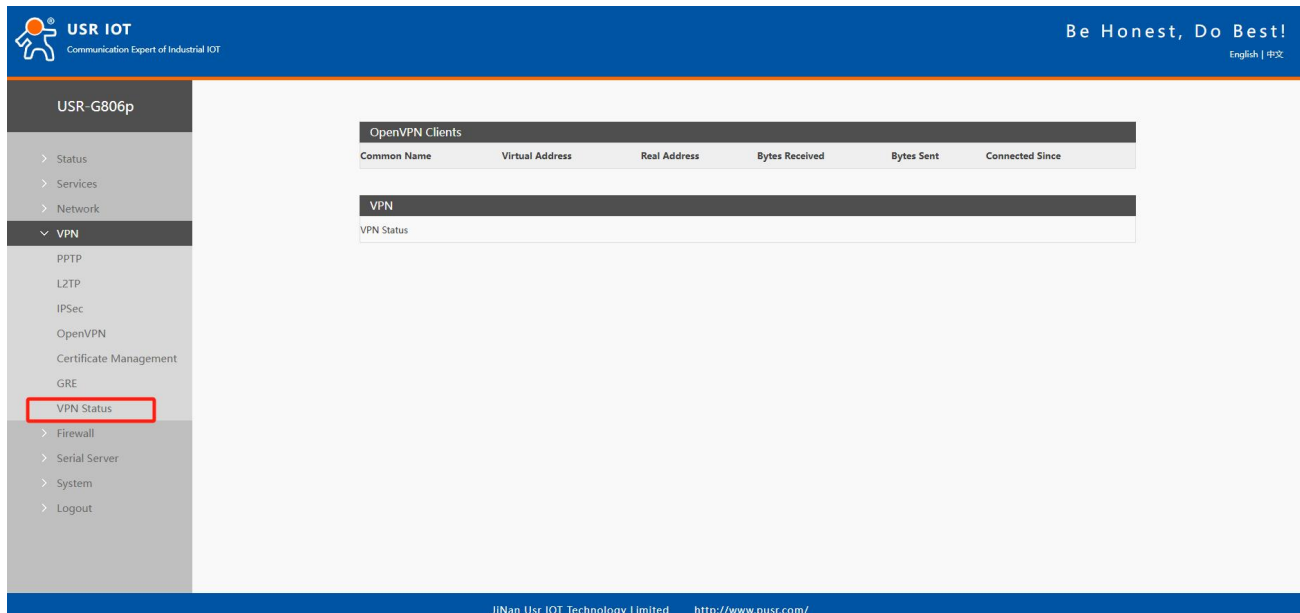
name	description	Default parameter
PPT Enable the PPTP client	Enable: Start PPTP client Disable: Close the PPTP client	forbidden
Server address	Enter the IP address or domain name of the VPN server to connect to	192.168.0.2
joggle	Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Connect to a VPN using cellular network	voluntarily

	<p>Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN</p> <p>Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN</p>	
user name	Fill in the correct user name	empty
password	Enter the correct password	empty
To the subnet	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the server subnet segment here	192.168.55.0
For the subnet mask	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the subnet mask of the server subnet here	255.255.255.0
NAT	<p>Check: Data passing through the VPN will be sent after NAT</p> <p>No line: Data passing through a VPN does not go through NAT</p>	check
MPPE encryption	<p>After checking, it is: mppe required, stateless</p> <p>Not checked: Do not start mppe encryption</p> <p>If the server uses require-mppe-128 encryption, you can uncheck this option and try the following additional configuration:</p> <p>mppe required,no40,no56,stateless</p> <p>refuse-eap refuse-chap refuse-pap refuse-mschap</p>	check
MTU	Set PPTP MTU value to the default value	1450
Additional configuration	Special parameters are usually configured for the server. If the client interface does not have these parameters, configure them here. Do not operate by non-professionals	empty
Enable static tunnel IP addresses	Customize PPTP client IP. Note that if the IP server is assigned to other clients or the IP is not within the IP range defined by the server, the connection will not be made to the server	Not enabled
Static tunnel IP address	Customize PPTP client IP. Note that if the IP server is assigned to other clients or the IP is not within the IP range defined by the server, the connection will not be made to the server	empty
default gateway	<p>After checking: All data traffic will be transmitted through the VPN channel after the VPN is established</p> <p>Unchecked: Only the VPN channel is established. If you need subnet intercommunication, static routes should be established</p>	Not selected

## AP510 manual

	Note: If the WAN port is connected by PPPOE, this option is invalid	
enable ping	Check: Enable VPNping ping alive detection, and reconnect to the VPN if ping fails Unchecked: Do not enable ping to keep alive	Not selected
Ping address	PPTP The address that the PPTP network card can ping is usually filled with the PTP address	empty
Ping period	Ping maintenance interval period, unit: seconds	10
Ping number of times	After the Ping failure upper threshold is exceeded, ping will not be sent to the set IP address, and the VPN will reconnect	3

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



The screenshot shows the USR IOT web interface for a USR-G806p device. The left sidebar contains a navigation menu with the following items: Status, Services, Network, VPN (expanded), PPTP, L2TP, IPSec, OpenVPN, Certificate Management, GRE, VPN Status (highlighted with a red box), Firewall, Serial Server, System, and Logout. The main content area displays the 'OpenVPN Clients' table and the 'VPN Status' section. The 'OpenVPN Clients' table has columns: Common Name, Virtual Address, Real Address, Bytes Received, Bytes Sent, and Connected Since. The 'VPN Status' section shows the current status of the VPN connection.

**Pic 27 Router VPN connection status**



## 4.2. L2TP Client

The screenshot displays the 'L2TP Setting' page in the PUSR web interface. The left sidebar shows the navigation menu with 'L2TP' highlighted under the 'VPN' section. The main content area is titled 'L2TP Setting' and contains the following configuration options:

- L2TP Parameters**
  - L2TP Client:** ☒ Enable ☐ Disable
  - Server Address:** 192.168.0.2
  - Interface:** auto (Note: Auto refers used default route interface to connect)
  - User Name:** [Empty field]
  - Password:** [Empty field] (Green lock icon)
  - Tunnel Name:** [Empty field]
  - Tunnel Password:** [Empty field] (Green lock icon) (Note: Character(0-50))
  - Enable IPsec:** ☐
  - Remote Subnet:** 192.168.55.0 (Note: e.g: 192.168.10.0)
  - Remote Subnet Mask:** 255.255.255.0 (Note: e.g: 255.255.255.0)
  - NAT:** ☒
  - MTU:** 1450 (Note: 600~1450)

Pic 28 L2TP client Settings interface

Tab 13 L2TP configuration parameters

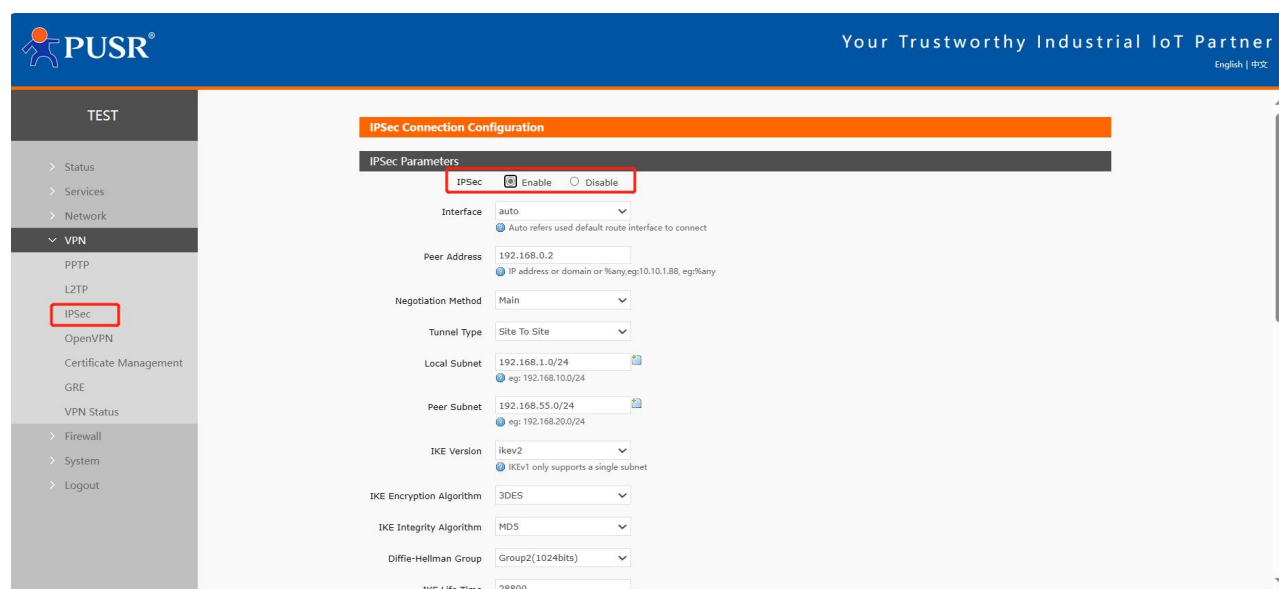
name	description	Default parameter
L2TP client enabled	Enable: Start the L2TP client Disable: Close the L2TP client	forbidden
Server address	Enter the IP address or domain name of the VPN server to connect to	192.168.0.2
joggle	Automatic: Connect to the VPN using the default routing interface Wan_wired: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

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

<explain >

- The mppe mode is: mppe required, stateless.

### 4.3. IPSec



**Pic 29 IPSec Settings interface**

**Tab 14 IPSec configuration parameters**

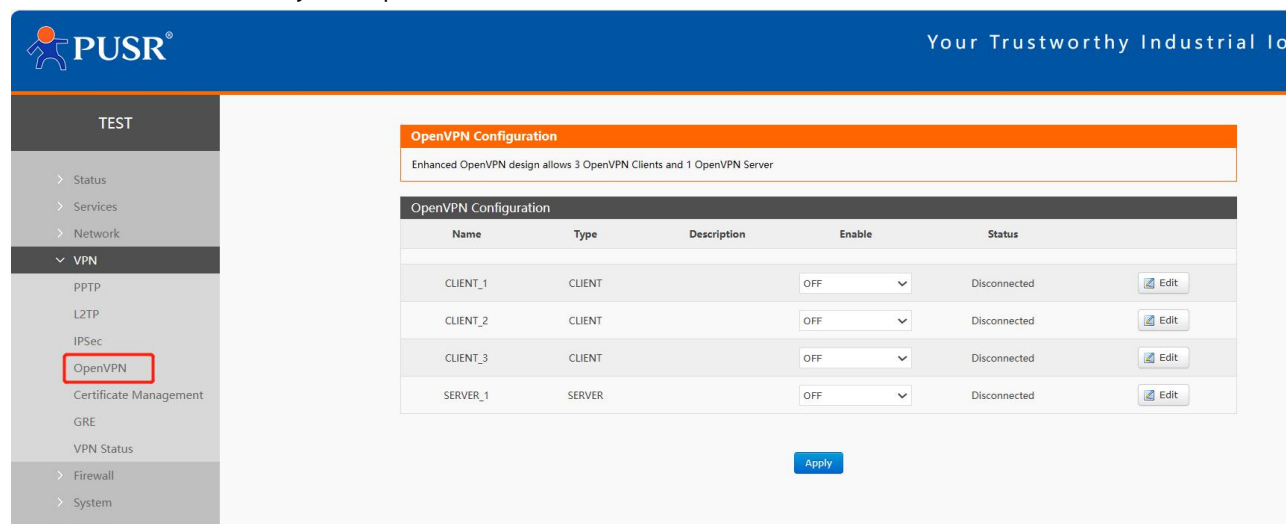
name	description	Default parameter
IPSec enable	Enable: Enable IPSec Disable: Disable IPSec	forbidden
joggle	Automatic: Use the default route to connect to the VPN Wan_wired: Use the WAN interface to connect to the VPN Wan_4g: Use cellular 4g to connect to the VPN Automatic example: When the wired connection is the default route, if you attempt to connect to the VPN via the wired connection, even if there is a 4G network available, it will still try to use the wired network card to connect to the VPN. If the wired connection is disconnected, it will automatically switch to the 4G network and attempt to connect to the VPN using the 4G method. If the VPN connects via 4G and the wired connection becomes available, the default route will switch to the wired network. However, since the 4G connection remains active, the VPN will still be connected. Only when the 4G connection is disconnected and the IPsec connection is broken once, the default route network card will attempt to reconnect to the VPN again. Wan_4G example: 4G has IP and tries to connect to VPN	voluntarily

## AP510 manual

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

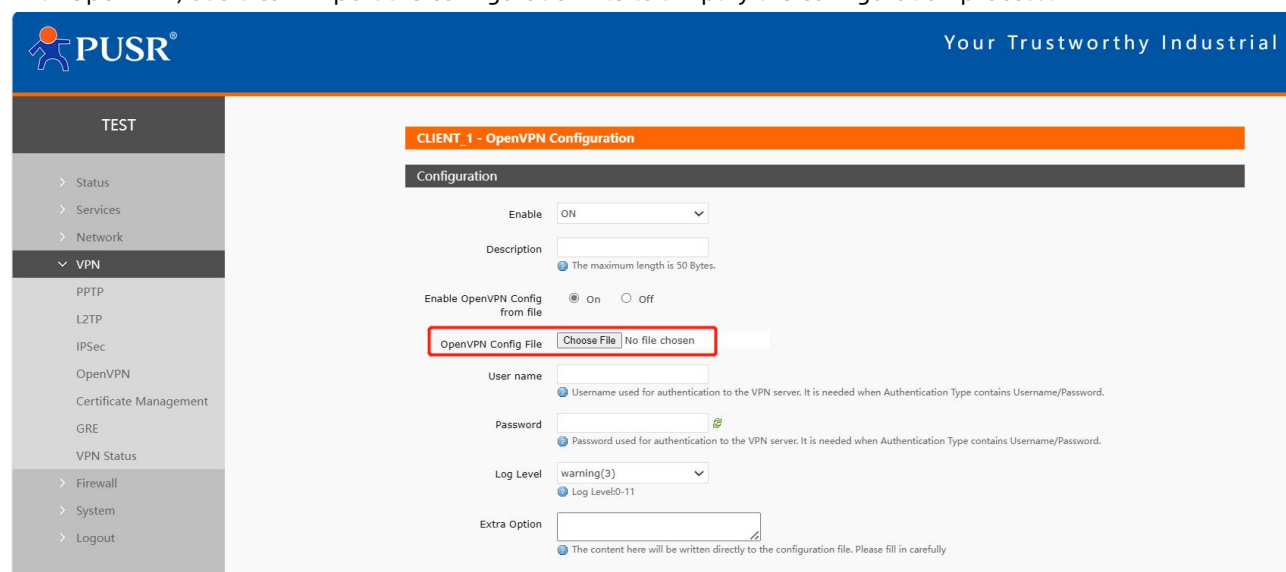
## 4.4. OpenVPN

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



**Pic 30 Open the OpenVPN page**

With OpenVPN, users can import the configuration file to simplify the configuration process.



**Tab 15 OpenVPN Client parameter table**

name	description	Default parameter
start using	Open: Open the openvpn client Close: Disable the openvpn client	close
description	You can customize the description of this OpenVPN path, but you don't have to fill it in	empty
Use the OpenVPN configuration file	Open: You can import the OpenVPN configuration parameters in the form of a file. If you are very familiar with the OpenVPN configuration file, you can use this method. It is recommended to use the router configuration box form	open

	Note: Use the router configuration box form	
OpenVPN configuration file	The configuration file is passed to OpenVPN	not have
protocol	tcp/udp/tcp ipv4/udp ipv4	udp
Remote host IP address	Set the openvpn server address: domain name or IP	192.168.0.2
port	Set the openVPN server port number	1194
Type of certification	None, SSL/TLS, user name and password, pre-shared key, SSL/TLS+ user name and password	SSL/TLS
TUN/TAP	tun/tap	tun
topology	Net30/p2p/subnet	subnet
bridge pattern	Tap bridges LAN and implements layer 2 interaction point to point	not have
user name	When the authentication type is selected with a user name and password, you must enter the correct user name	empty
password	When the authentication type is selected with a user name and password, you must enter the correct password	empty
Local tunnel IP	When the authentication type is no/pre-shared password, fill in the TUN tunnel IP of this end	empty
Remote tunnel IP	When the authentication type is no/pre-shared password, fill in the end-to-end tunnel IP of this end	empty
Enter the IP address of the Tap network card	When the authentication type is no/pre-shared password, fill in the IP address of the TAP network card on this end	empty
Tap the subnet mask of the network card	If the authentication type is no/pre-shared password, fill in the TAP network card mask of this end	empty
Interface	Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN WAN_STA: Connect to the VPN using the 2.4G STA interface WAN_4G: Use cellular 4G to connect to the VPN Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN	voluntarily
Redirect gateway	Use openvpn as the default gateway It takes effect after you select "None" in "Network Switching" The WAN port cannot use the redirect gateway function in	close

	PPPoE mode You cannot enable the redirect gateway function for multiple VPNs	
Nat	Whether the data on the VPN network card is NAT	open
Enable Keepalive	Enable the live detection mechanism	open
Connection detection time interval (seconds)	VPN live heartbeat detection interval	10
Connection detection timeout interval (seconds)	If the heartbeat exceeds the set time without response, reconnect to the VPN	120
enable LZO	Data compression method	No preference
encryption algorithm	Data encryption algorithm	BF-CBC
Hash algorithm	The data's hash algorithm	SHA1
TLS way	Select the TLS authentication method	OFF
LINK-MTU/TUN-MTU/TCP MSS	Set the data pack length	Air / air / 1450
Maximum frame length	The maximum frame length of data is the default without special configuration	empty
Allows remote address changes	Whether to allow remote address change Settings	close
Log grade	Openvpn log level, the larger the number, the more detailed the log is. Generally, open a higher level to troubleshoot problems when the connection is abnormal	Warning (3)
Additional configuration	Non-professionals should not configure it. You need to input openvpn recognizable parameters	empty
Local route-destination	Set the static route target segment established by the openvpn network card on this end	empty
Local route-Network mask	Set the subnet mask of the static route target established by the openvpn network card on this end	empty
CA	Upload CA certificate	not have
CERT	Upload the client certificate	not have
KEY	Upload the client private key	not have
TLS	Upload the TLS certificate. If the TLS mode is selected OFF, you do not need to upload the certificate here	not have
Pre-shared key	Upload the pre-shared key. You can upload the certificate only when you select the authentication type as pre-shared key	not have

Tab 16 OpenVPN Server parameter table

name	description	Default parameter
------	-------------	-------------------

start using	Open: Start the openVPN server Close: Disable the openvpn client	close
description	You can customize the description of this OpenVPN path, but you don't have to fill it	empty
protocol	tcp/udp/tcp ipv4/udp ipv4	udp
port	Set the openvpn server port number	1194
Type of certification	None, SSL/TLS, user name and password, pre-shared key, SSL/TLS+ user name and password	SSL/TLS
TUN/TAP	Select the network communication mode, tun/tap	tun
Bridge the network	The Tap mode can bridge LAN and realize two-layer interaction point to point	not have
Bridge network mode configuration	TAP bridge network mode Settings Use the device's own DHCP service: Use the router LAN port DHCP service Specify the gateway, mask, starting address and ending address: the device under the route must be connected to the same subnet as the gateway	Use the device's own DHCP service
topology	Net30/p2p/subnet, which is usually the default value	subnet
IPv4 tunnel network	Open the IP subnet assigned to the client for OpenVPN, such as 192.168.100.0	empty
IPv4 tunnel subnet mask	Enter the subnet mask assigned to the client by OpenVPN, for example: 255.255.255.0	empty
Local tunnel IP	When the authentication type is no/pre-shared password, fill in the local TUN tunnel IP	empty
Remote tunnel IP	When the authentication type is no/pre-shared password, fill in the end-to-end tunnel IP of this end	empty
begin IP	The TAP bridge mode specifies the starting IP address, such as 192.168.100.100 The LAN port of the router needs to be set to the same subnet as the network segment	empty
finish IP	The TAP bridge mode specifies the end IP address, such as 192.168.100.200	empty
Enter the IP address of the Tap network card	If the authentication type is no/pre-shared password, fill in the IP address of the TAP network card on this end	empty
Tap the subnet mask of the network card	If the authentication type is no/pre-shared password, fill in the TAP network card mask of this end	empty
The client renegotiates the time interval	When the client reaches the set value, it will renegotiate and reconnect. This is a security mechanism of openvpn Setting both the client and this end to 0 means that only one negotiation is performed when openvpn is established If the renegotiation time is set, a very short data delay will	3600



	occur after this value is reached. Unit: seconds If the router client is set to 0, additional configuration is required: reneg-sec 0	
Maximum number of customers	Set the upper limit of the number of clients that can connect to the service	16
Allow client to client	Check to enable data exchange between OpenVPN clients Unchecked: Data is only exchanged between the client and the server, not between clients	check
Multiple clients use the same certificate	Check: Allow multiple clients to use the same client certificate to connect to the OpenVPN Server	Not selected
Redirect gateway	Use openvpn as the default gateway It takes effect after you select "None" in "Network Switching" The WAN port cannot use the redirect gateway function in PPPoE mode You cannot enable the redirect gateway function for multiple VPNs	close
Nat	Whether the data on the VPN network card is NAT	open
Enable Keepalive	Enable the live detection mechanism	open
Connection detection time interval (seconds)	VPN live heartbeat detection interval	10
Connection detection timeout interval (seconds)	If the heartbeat exceeds the set time without response, reconnect the VPN	120
Enable LZO	Data compression method	No preference
encryption algorithm	Data encryption algorithm	BF-CBC
Hash algorithm	The data's hash algorithm	SHA1
TLS way	Select the TLS authentication method	OFF
LINK-MTU/TUN-MTU/TCP MSS	Set the data pack length	Air / air / 1450
Maximum frame length	The maximum frame length of data is the default without special configuration	empty
Allows remote address changes	Whether to allow remote address change Settings	close
Log grade	Openvpn log level, the larger the number of log is more detailed, generally open a larger level to troubleshoot problems when the connection is abnormal	Warning (3)
Additional configuration	Non-professionals should not configure it. You need to input openvpn recognizable parameters	empty

user	Set the user name and password account for the client connection. Select the option with the user name and password to take effect. Set multiple accounts to set a user name and password for each client	
user name	Set the client connection user name, and you can set multiple user names and passwords	empty
password	Set the client connection password, and you can set multiple user name passwords	empty
The client is assigned a static IP address	Set the parameters for assigning fixed IP addresses to clients. You can set multiple fixed IP addresses for multiple clients, and each client's fixed IP address cannot be repeated	
user	Use the certificate form: This is set to the CN corresponding value of the client certificate, such as client1 If you use only the form of user name and password: Enter the user name value here	empty
Static IP address	Set the static IP address assigned to the client, such as 192.168.100.2	empty
subnet mask	Set the subnet mask assigned to the client, for example: 255.255.255.0	empty
Customer subnet	To enable subnet interworking, you need to fill in the subnet segment of each client, and openvpn will automatically push the routing function	
name	Use the certificate form: This is set to the CN corresponding value of the client certificate, such as client1 If you use only the form of user name and password: Enter the user name value here	empty
subnet	The subnet segment corresponding to the client, such as 192.168.1.0	empty
subnet mask	The subnet mask corresponding to the client subnet segment, such as: 255.255.255.0	empty
Local routing	Set up a static route created by the openvpn network card	
target	Set the static route target segment established by the openvpn network card on this end	empty
Network mask	Set the subnet mask of the static route target established by the openvpn network card on this end	empty
Certificate management		
CA	Upload CA certificate	not have
CERT	Upload the client certificate	not have
KEY	Upload the client private key	not have
TLS	Upload the TLS certificate. If the TLS mode is selected OFF, you do not need to upload the certificate here	not have
Pre-shared key	Upload the pre-shared key. You can upload the certificate only when you select the authentication type as pre-shared	not have

key

Pic 31 OpenVPN certificate page

Tab 17 OpenVPN Server parameter table

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

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

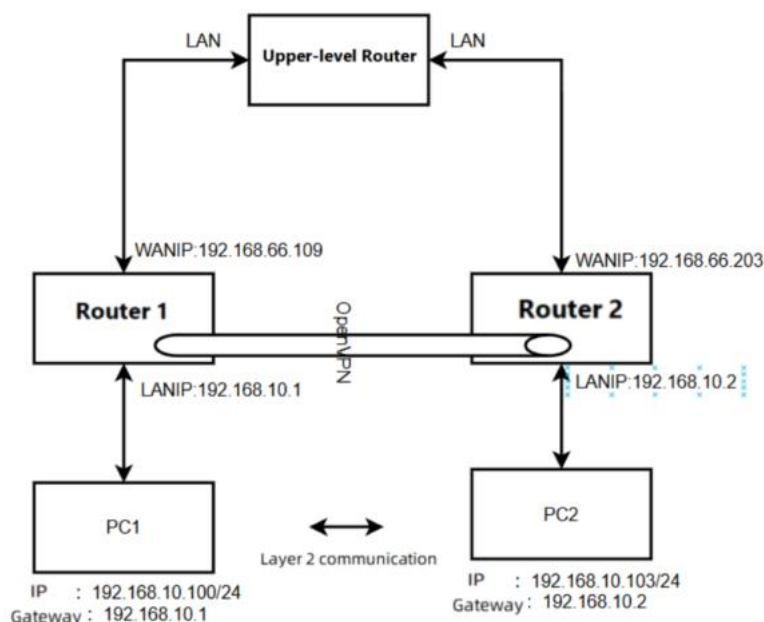
### **< explain >**

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

#### 4.4.1. OpenVPN TAP bridge example

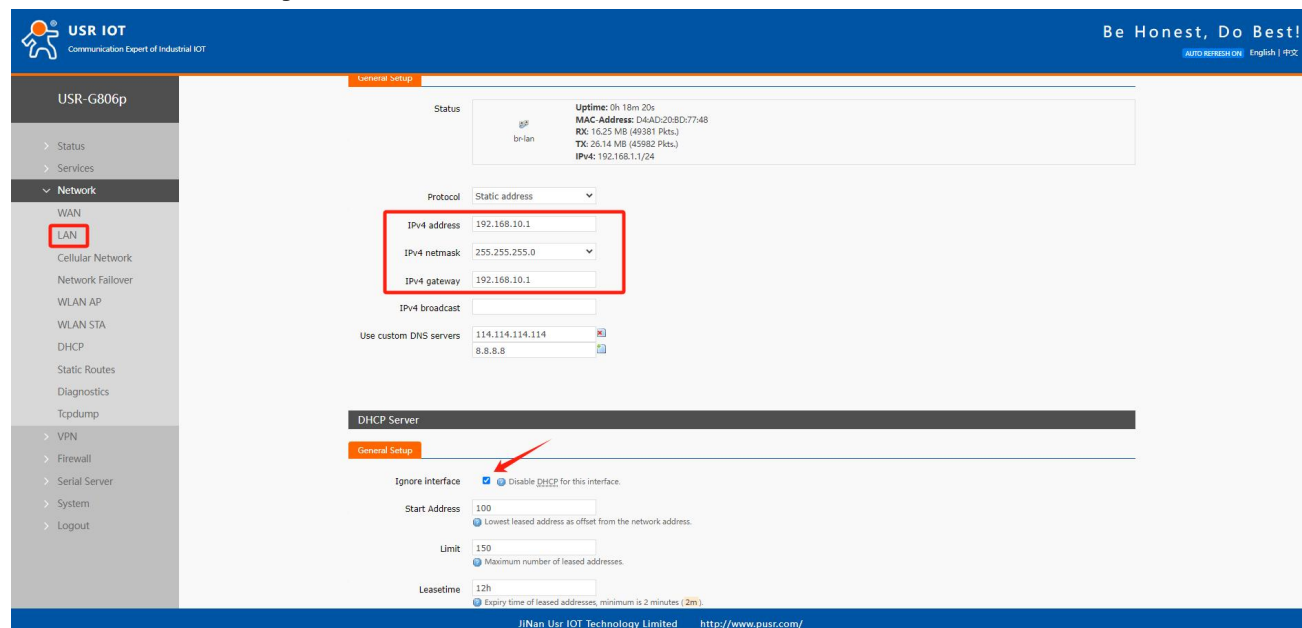
It is generally used for APN dedicated network card +OpenVPN to realize the function of LAN for multiple terminals.

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



**Pic 32 Connect the topology**

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



**Pic 33 LAN port configuration**

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

USR IOT  
Communication Expert of Industrial IOT

Be Honest, Do Best!  
English | 中文

USR-G806p

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

**SERVER 1 - OpenVPN Configuration**

Configuration

Enable: ON

Description: The maximum length is 50 Bytes.

Enable OpenVPN Config from file: Not Support

Protocol: UDP

Port: 1194

Authentication Type: Username/Password

TUN/TAP: TAP

Bridge Network: LAN

Tap bridging network configuration mode: Use your own dhcp service

Renegotiation Interval(s): 3600

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

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

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

Pic 34 OpenVPN configuration 1

Set a set of user names and passwords.

USR IOT  
Communication Expert of Industrial IOT

Be Honest,

USR-G806p

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

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

**User**

Username	Password	
test	test	<a href="#">Delete</a>

**New User:**

Username:  Password:

**Client Static Ip**

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

**Tunnel static IP:**

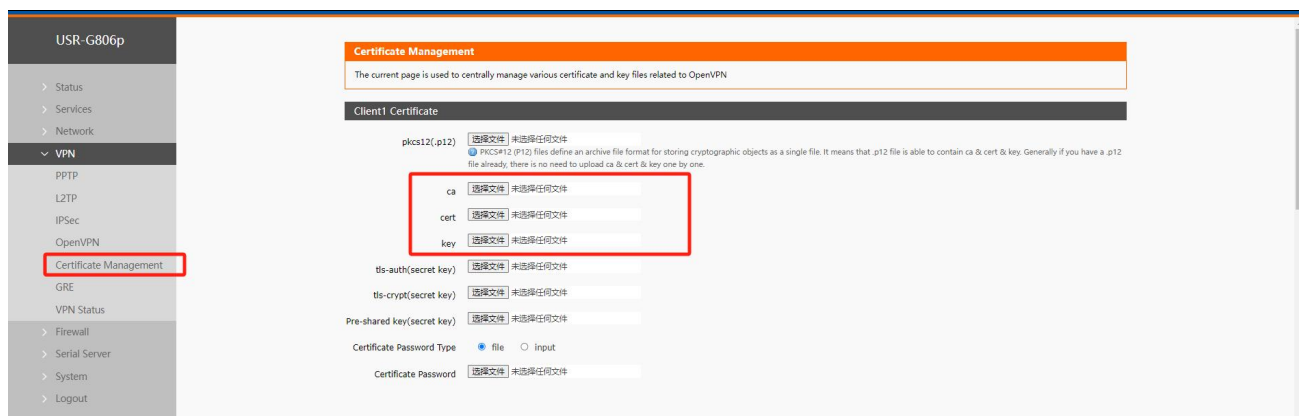
User	Static IP	Netmask/P2P IP
------	-----------	----------------

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

Pic 35 OpenVPN configuration 2

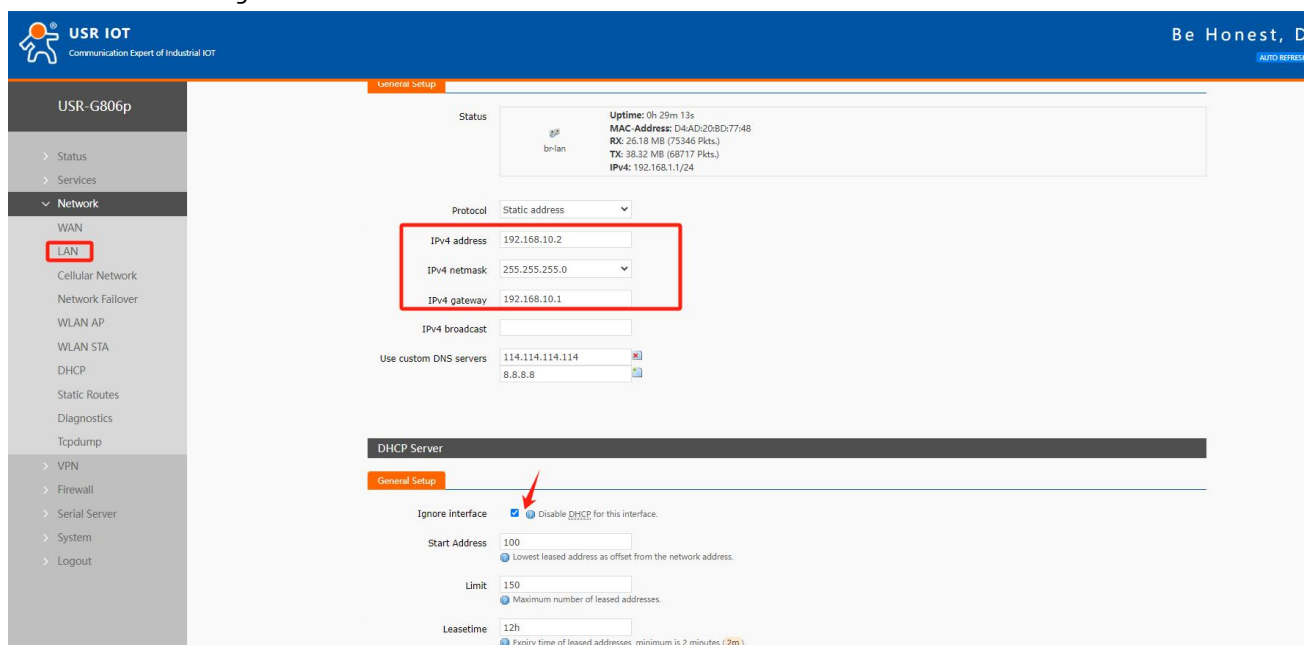
The server needs to pass the openvpn server certificate, including the CA certificate, server certificate, server key and DH certificate.

## AP510 manual



**Pic 36 OpenVPN configuration 3**

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



**Pic 37 LAN port configuration**

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

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest, Do Best!  
English | 中文

USR-G806p

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

**CLIENT 1 - OpenVPN Configuration**

Configuration

Enable: ON

Description: The maximum length is 50 Bytes.

Enable OpenVPN Config from file: ☐ On ☒ Off

Protocol: UDP

Remote Host IP Address: 192.168.66.109

Port: 1194

Authentication Type: Username/Password

TUN/TAP: TAP

Bridge Network: LAN

User name: test

Password: test

Renegotiation Interval(s): 3600

JI'nan Ustr IOT Technology Limited. <http://www.pusr.com/>

Pic 38 OpenVPN configuration 1

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest,

USR-G806p

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

**Certificate Management**

The current page is used to centrally manage various certificate and key files related to OpenVPN

**Client1 Certificate**

pkcs12(.p12)  未选择文件

PKCS#12 (.P12) files define an archive file format for storing cryptographic objects as a single file. It means that .p12 file is able to contain ca & cert & key. Generally if you have a .p12 file already, there is no need to upload ca & cert & key one by one.

ca  未选择文件

cert  未选择文件

key  未选择文件

tls-auth(secret key)  未选择文件

tls-crypt(secret key)  未选择文件

Pre-shared key(secret key)  未选择文件

Certificate Password Type: ☒ file ☐ input

Certificate Password  未选择文件

Pic 39 OpenVPN configuration 2

Test that PC1 and PC2 can communicate with each other:

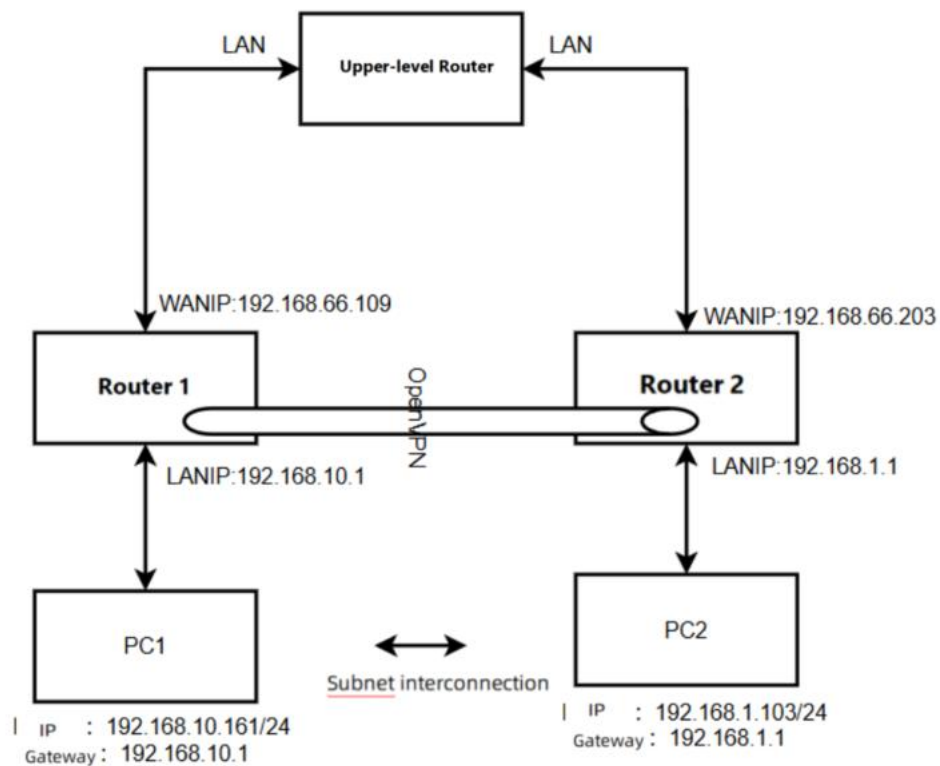


```

    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
Control-C
C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.10.1
正在 Ping 192.168.10.1 具有 32 字节的数据:
来自 192.168.10.1 的回复: 字节=32 时间<1ms TTL=64
192.168.10.1 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
C:\Users\Administrator>ping 192.168.10.2
正在 Ping 192.168.10.2 具有 32 字节的数据:
来自 192.168.10.2 的回复: 字节=32 时间=2ms TTL=64
192.168.10.2 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 2ms, 最长 = 2ms, 平均 = 2ms
Control-C
C:\Users\Administrator>ping 192.168.10.103
正在 Ping 192.168.10.103 具有 32 字节的数据:
来自 192.168.10.103 的回复: 字节=32 时间=76ms TTL=64
来自 192.168.10.103 的回复: 字节=32 时间=5ms TTL=64
192.168.10.103 的 Ping 统计信息:
    数据包: 已发送 = 3, 已接收 = 2, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 5ms, 最长 = 76ms, 平均 = 40ms
Control-C
C:\Users\Administrator>

```

#### 4.4.2. An example of subnet interworking in OpenVPN TUN mode



**Pic 40 Connect the topology**

Router 1 configuration, LAN port setting

**USR IOT**  
Communication Expert of Industrial IOT

**USR-G806p**

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

**LAN - LAN**

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and e interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0. 1).

**Common Configuration**

**General Setup**

Status

Uptime: 0h 44m 20s  
MAC-Address: D4:AD:20:BD:77:48  
RX: 24.95 MB (57060 Pkts.)  
TX: 31.23 MB (55866 Pkts.)  
IPv4: 192.168.1.1/24

Protocol: Static address

IPv4 address: 192.168.10.1

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers: 114.114.114.114, 8.8.8.8

Pic 41 Router 1 is configured 1

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

**USR IOT**  
Communication Expert of Industrial IOT

**USR-G806p**

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

**SERVER 1 - OpenVPN Configuration**

**Configuration**

Enable: ON

Description:

Enable OpenVPN Config from file: Not Support

Protocol: UDP

Port: 1194

Authentication Type: SSL/TLS

TUN/TAP: TUN

Topology: Subnet

Client Subnet: 100.100.100.0

Client Netmask: 255.255.255.0

Renegotiation Interval(s): 3600

max clients: 16

Allow a maximum of n simultaneously connected clients.

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

Pic 42 Router 1 is configured 2

Enter the client subnet information and click "Save"

USR IOT  
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

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

User Static IP Netmask/P2P IP Add

Name	Subnet	Netmask
client1	192.168.1.0	255.255.255.0

Delete

New Client Network:

Name Subnet Netmask Add

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

Subnet	Netmask
This section contains no values yet	

Local Route:

Subnet Netmask Add

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

Pic 43 Router 1 is configured 3

Enter the OpenVPN server certificate and click "Apply".

USR IOT  
Communication Expert of Industrial IOT

USR-G806p

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

Server Certificate

pkcs12(.p12) 选择文件 未选择文件

PKCS#12 (P12) files define an archive file format for storing cryptographic objects as a single file. It means that .p12 file is able to contain private key, certificate, and CA certificate. Generally if you have a .p12 file already, there is no need to upload ca & cert & key one by one.

ca 选择文件 未选择文件

cert 选择文件 未选择文件

key 选择文件 未选择文件

DH 选择文件 未选择文件

tls-auth(secret key) 选择文件 未选择文件

tls-crypt(secret key) 选择文件 未选择文件

Pre-shared key(secret key) 选择文件 未选择文件

Certificate Revoke List 选择文件 未选择文件

Certificate Password Type ☒ file ☐ input

Certificate Password 选择文件 未选择文件

Apply Save

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

Pic 44 Router 1 is configured for 4

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

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

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

**CLIENT 1 - OpenVPN Configuration**

**Configuration**

Enable: ON

Description:   
The maximum length is 50 Bytes.

Enable OpenVPN Config from file: ☐ On ☒ Off

Protocol: UDP

Remote Host IP Address: 192.168.66.109

Port: 1194

Authentication Type: SSL/TLS

TUN/TAP: TUN

Topology: Subnet

Renegotiation Interval(s): 3600

Interface: Auto  
Auto refers used default route interface to connect

redirect-gateway: ☐

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

Pic 45 Router 2 is configured 1

Client adds information to the server subnet.

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

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

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

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

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

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

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

Subnet	Netmask	
192.168.10.0	255.255.255.0	<input type="button" value="Delete"/>

**Local Route:**

Subnet	Netmask	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

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

Pic 46 Router 2 is configured 2

Enter the OpenVPN client certificate and click "Apply".

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest, Do Best!  
English | 中文

USR-G806p

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

**Certificate Management**

The current page is used to centrally manage various certificate and key files related to OpenVPN

**Client1 Certificate**

pkcs12(.p12)  未选择文件

PKCS#12 (.p12) files define an archive file format for storing cryptographic objects as a single file. It means that .p12 file is able to contain ca & cert & key. Generally if you have a .p12 file already, there is no need to upload ca & cert & key one by one.

ca  未选择文件

cert  未选择文件

key  未选择文件

tls-auth(secret key)  未选择文件

tls-crypt(secret key)  未选择文件

Pre-shared key(secret key)  未选择文件

Certificate Password Type ☒ file ☐ input

Certificate Password  未选择文件

**Client2 Certificate**

pkcs12(.p12)  未选择文件

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

Pic 47 Router 2 is configured 3

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

**USR IOT**  
Communication Expert of Industrial IOT

Be Honest, Do

USR-G806p

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

**OpenVPN Clients**

Common Name	Virtual Address	Real Address	Bytes Received	Bytes Sent	Connected Since

**VPN**

VPN Status

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

PC1 and PC2 are interconnected

## AP510 manual

```

连接特定的 DNS 后缀 . . . . . : lan
本地链接 IPv6 地址 . . . . . : fe80::9045:5443:b7b9:1171%15
IPv4 地址 . . . . . : 192.168.10.101
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 192.168.10.1

以太网适配器 Npcap Loopback Adapter:
连接特定的 DNS 后缀 . . . . . :
本地链接 IPv6 地址 . . . . . : fe80::6d2e:ce94:b63f%25
自动配置 IPv4 地址 . . . . . : 169.254.182.63
子网掩码 . . . . . : 255.255.0.0
默认网关 . . . . . :

无线局域网适配器 本地连接* 2:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 本地连接* 3:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

无线局域网适配器 WLAN:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . : lan

以太网适配器 以太网 4:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

以太网适配器 蓝牙网络连接:
媒体状态 . . . . . : 媒体已断开连接
连接特定的 DNS 后缀 . . . . . :

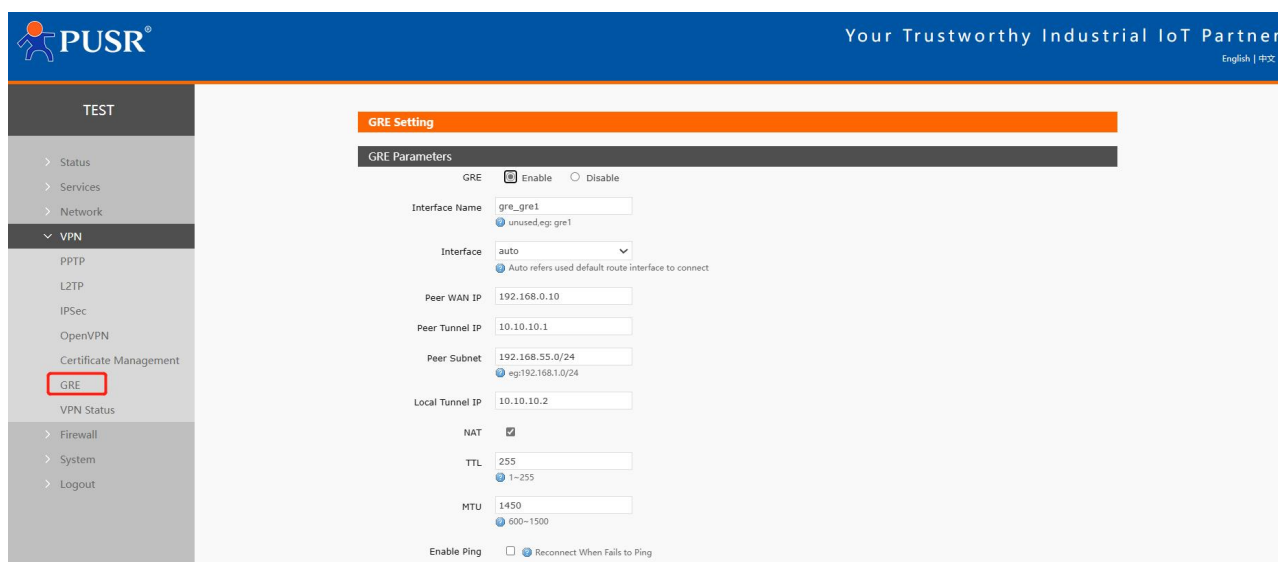
C:\Users\Administrator>ping 192.168.1.103
正在 Ping 192.168.1.103 具有 32 字节的数据:
来自 192.168.1.103 的回复: 字节=32 时间=60ms TTL=62
来自 192.168.1.103 的回复: 字节=32 时间=203ms TTL=62

192.168.1.103 的 Ping 统计信息:
数据包: 已发送 = 2, 已接收 = 2, 丢失 = 0 (0% 丢失),
往返时间估计时间(以毫秒为单位):
    最短 = 60ms, 最长 = 203ms, 平均 = 134ms
Control-C
^C
C:\Users\Administrator>

```

**Pic 48 PC1 and PC2 are interconnected**

## 4.5. GRE



**Pic 49 GRE basic configuration**

< explain >

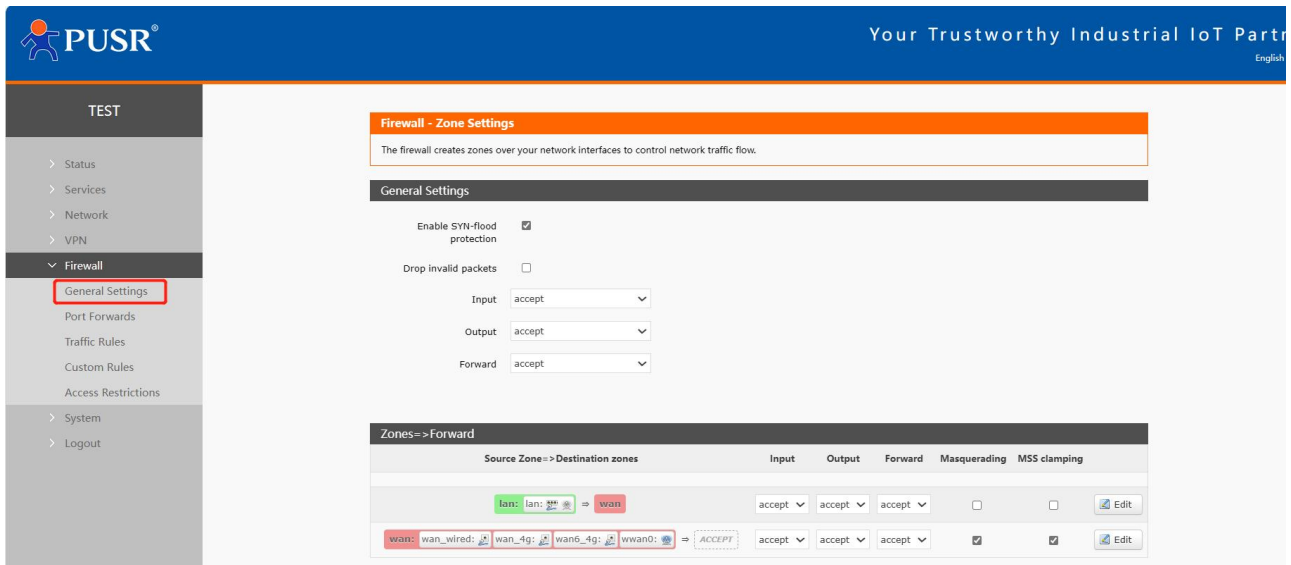
- Remote address: WAN port IP address of the remote GRE;
- Local address: The local wan\_wired and wan\_4g addresses are input according to different networking modes;
- Remote tunnel address: GRE tunnel IP of the other end;
- For the subnet: For setting the subnet mask, it can be expressed as follows: 255.255.255.0 can be written as IP/24, and 255.255.255.255 can be written as IP/32. For example: 172.16.10.1/24 corresponds to IP 172.16.10.1, and the subnet mask is 255.255.255.0;

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

## 5. Firewall

### 5.1. Basic Settings

The default is to enable two firewall rules.



Pic 50 Firewall Settings page

### [Term Introduction]

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

### [Rule 1]

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

### [Rule 2]

- The wired WAN port and 4G port accept "incoming", "outgoing" and allow "forwarding";
- If there is an "incoming" packet, such as someone trying to log in to the router's web page from a WAN port, it will be allowed;



- If there is an "outgoing" packet, such as a router accessing the Internet through a WAN port or 4G port, this action is allowed;
- If there is a "forwarding" packet, such as a packet coming from the WAN port that wants to be forwarded to the LAN port, this action is allowed.

## 5.2. Traffic rules

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

The screenshot displays the 'Firewall - Traffic Rules - (Unnamed Rule)' configuration page. The left sidebar shows the 'Firewall' section expanded, with 'Traffic Rules' highlighted. The main configuration area includes fields for enabling the rule, naming it, restricting to IPv4, selecting protocols (TCP+UDP), matching ICMP types, and defining source and destination zones (LAN, WAN, WAN6\_4g, WAN6\_4g, WAN0). Source MAC and IP addresses can also be specified, along with source ports.

**Tab 18 Traffic rule parameter table**

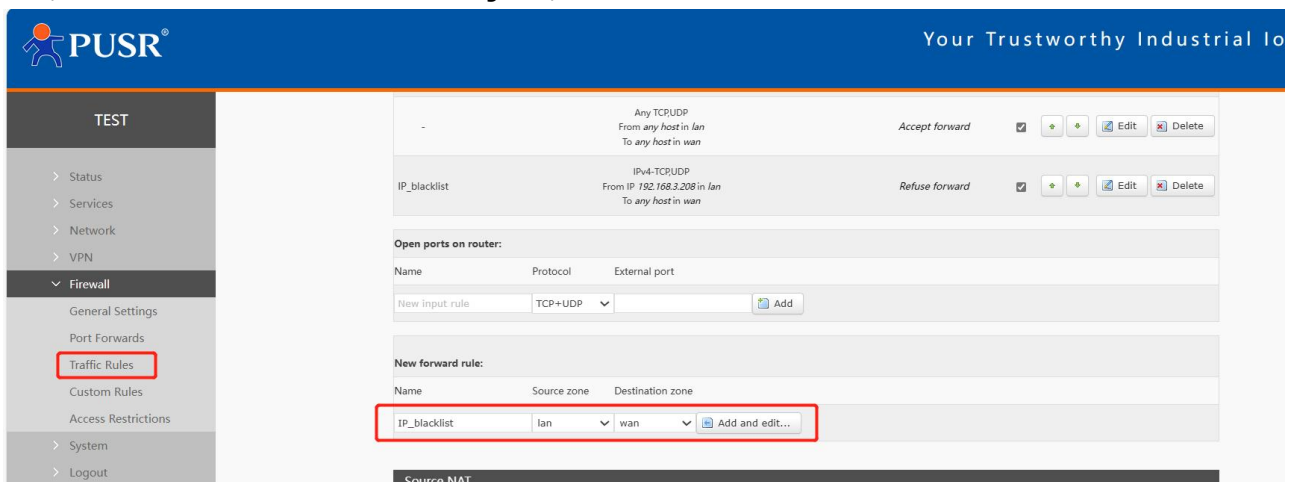
name	description	Default parameter
start using	The display  indicates the enabled state The display  indicates the disabled state	start using
name	Name of this rule, character type	-
Limit addresses	Restrict IPv4 addresses	Only IPv4 addresses
protocol	The types of protocols that can be restricted by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



	Note: When matching the source MAC address, set the source IP address to empty	
Source IP address	The source IP to match the rule with Empty: Matches all IP addresses Note: When matching the source IP address, set the source MAC address to null	empty
Source port	The source port that needs to match the rule Empty: Represents matching all ports	empty
target area	Data flow target area, can be selected: any area, WAN, LAN LAN: Indicates the rules for subnet access to the Internet WAN: Indicates the rules for accessing the Intranet from the Internet	WAN
destination address	The target IP address to visit Empty: Represents all addresses	empty
Target port	The target port number to visit Air: represents all	empty
Action	Receive such packets with options: discard, accept, reject, or no action Discard: This rule packet will be discarded upon receipt Accept: The packet will be accepted if it is received Reject: This rule packet will be rejected upon receipt No action: No action is taken when this rule packet is received	accept

### 5.2.1. IP address blacklist

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



**Pic 51 Figure 1 of the firewall blacklist**

In the redirected page, select LAN for the source area, and select all for the source MAC address and source address

(if you only restrict a specific IP address within the LAN to access a specific IP address outside the LAN, you need to fill in the IP address or MAC address), as shown in the following figure:

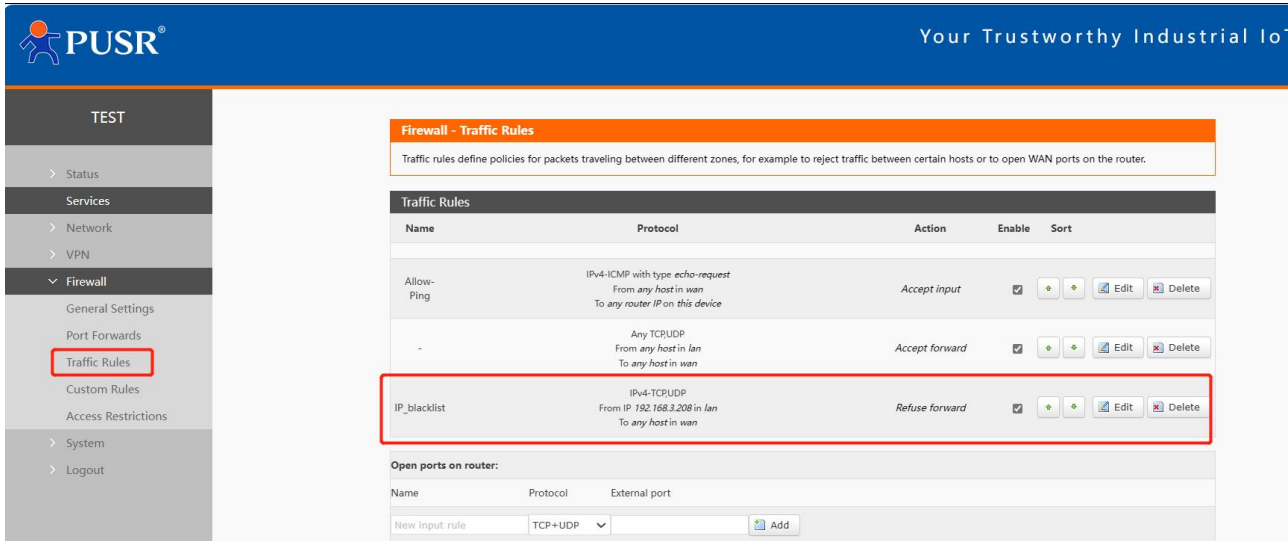
The screenshot shows the PUSR firewall configuration interface. The left sidebar has a 'TEST' tab and a 'Firewall' section with 'Traffic Rules' highlighted. The main area shows the configuration for a traffic rule. The 'Match ICMP type' is set to 'any'. The 'Source zone' is set to 'lan'. The 'Source MAC address' is set to 'any'. The 'Source IP address' is set to '192.168.3.208 (66:6F:E8:...)'. The 'Source port' is set to 'any'. The 'Destination zone' is set to 'wan'. The 'Destination address' is set to 'any'. The 'Destination port' is set to 'any'. The 'Action' is set to 'reject'.

**Pic 52 Figure 2 of the firewall blacklist**

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

The screenshot shows the PUSR firewall configuration interface. The left sidebar has a 'TEST' tab and a 'Firewall' section with 'Traffic Rules' highlighted. The main area shows the configuration for a traffic rule. The 'Source MAC address' is set to 'any'. The 'Source IP address' is set to '192.168.3.208 (66:6F:E8:...)'. The 'Source port' is set to 'any'. The 'Destination zone' is set to 'wan'. The 'Destination address' is set to 'any'. The 'Destination port' is set to 'any'. The 'Action' is set to 'reject'. The 'Apply' button is highlighted.

**Pic 53 Figure 3 of the firewall blacklist**

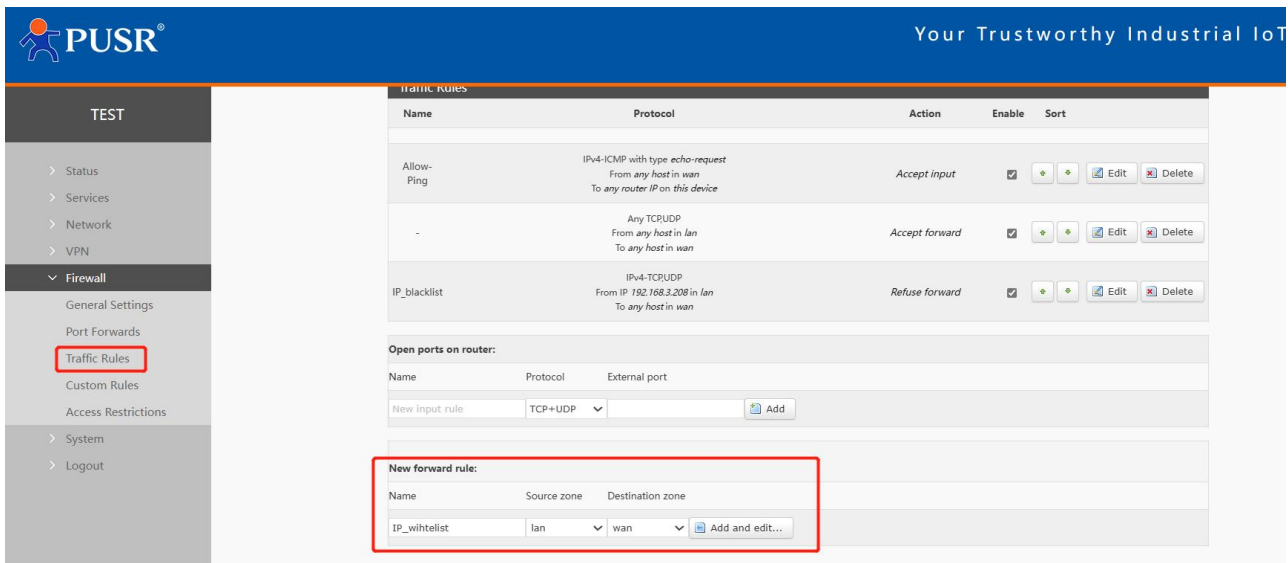


Pic 54 Figure 4 of the firewall blacklist

After this setting is completed, the blacklist function is implemented. That is, the IP address of the subnet device 192.168.3.208 is prohibited from accessing all external networks.

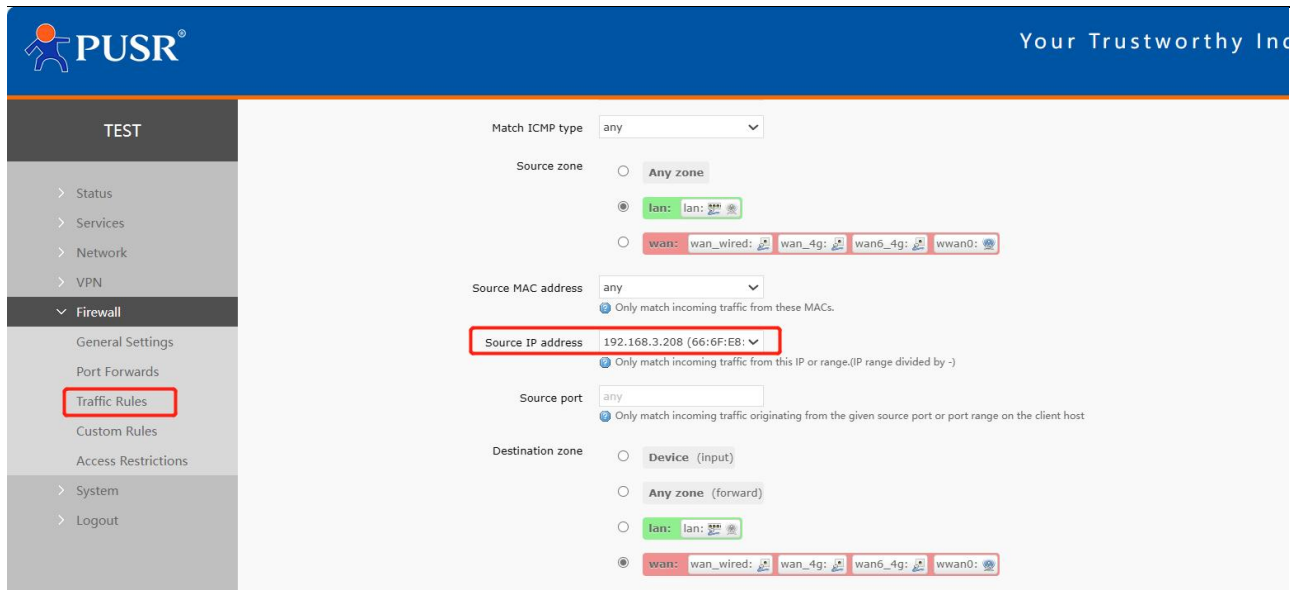
### 5.2.2. IP address whitelist

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



Pic 55 Firewall whitelist Figure 1

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



**PUSR®** Your Trustworthy Inc.

**TEST**

- > Status
- > Services
- > Network
- > VPN
- ▼ **Firewall**
  - General Settings
  - Port Forwards
  - Traffic Rules**
  - Custom Rules
  - Access Restrictions
- > System
- > Logout

Match ICMP type: any

Source zone:
 

- ☐ Any zone
- ☒ lan: lan: [MAC]
- ☐ wan: wan\_wired: [MAC] wan\_4g: [MAC] wan6\_4g: [MAC] wwan0: [MAC]

Source MAC address: any

Source IP address: 192.168.3.208 (66:6F:E8:)

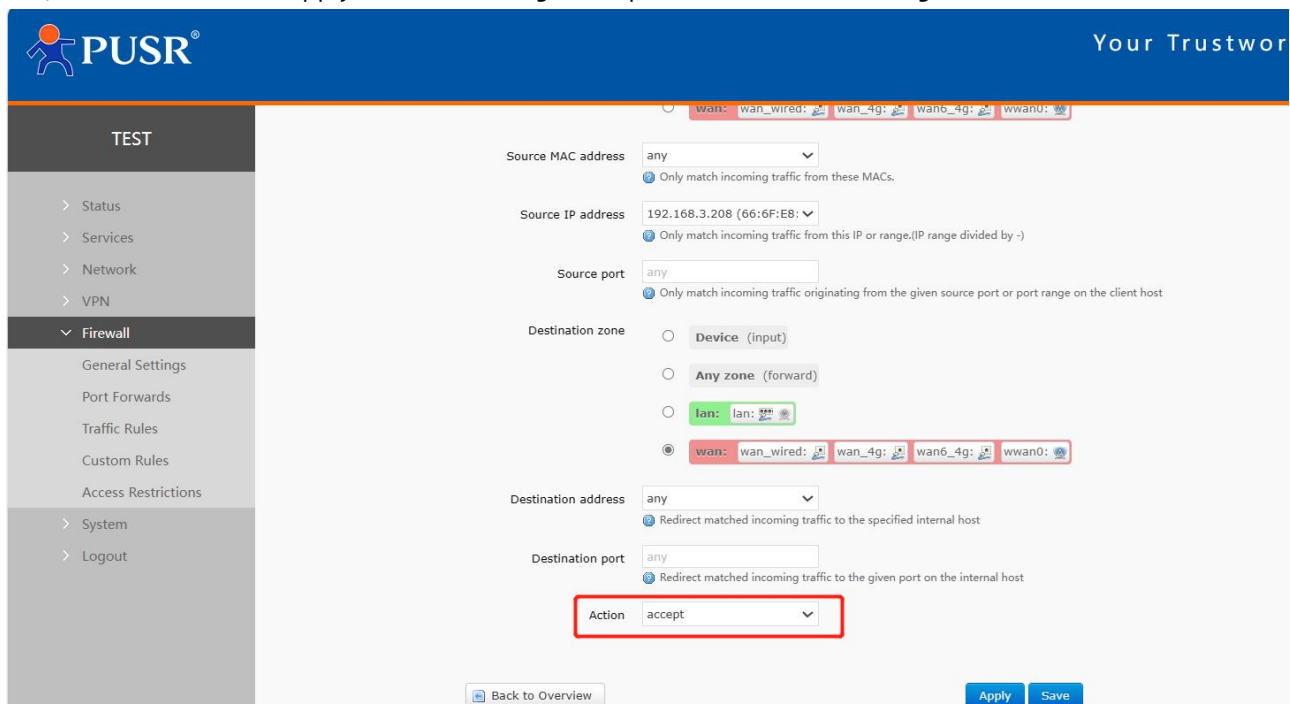
Source port: any

Destination zone:
 

- ☐ Device (input)
- ☐ Any zone (forward)
- ☐ lan: lan: [MAC]
- ☒ wan: wan\_wired: [MAC] wan\_4g: [MAC] wan6\_4g: [MAC] wwan0: [MAC]

Pic 56 Figure 2 of the firewall whitelist

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



**PUSR®** Your Trustworthy Inc.

**TEST**

- > Status
- > Services
- > Network
- > VPN
- ▼ **Firewall**
  - General Settings
  - Port Forwards
  - Traffic Rules
  - Custom Rules
  - Access Restrictions
- > System
- > Logout

Source MAC address: any

Source IP address: 192.168.3.208 (66:6F:E8:)

Source port: any

Destination zone:
 

- ☐ Device (input)
- ☐ Any zone (forward)
- ☐ lan: lan: [MAC]
- ☒ wan: wan\_wired: [MAC] wan\_4g: [MAC] wan6\_4g: [MAC] wwan0: [MAC]

Destination address: any

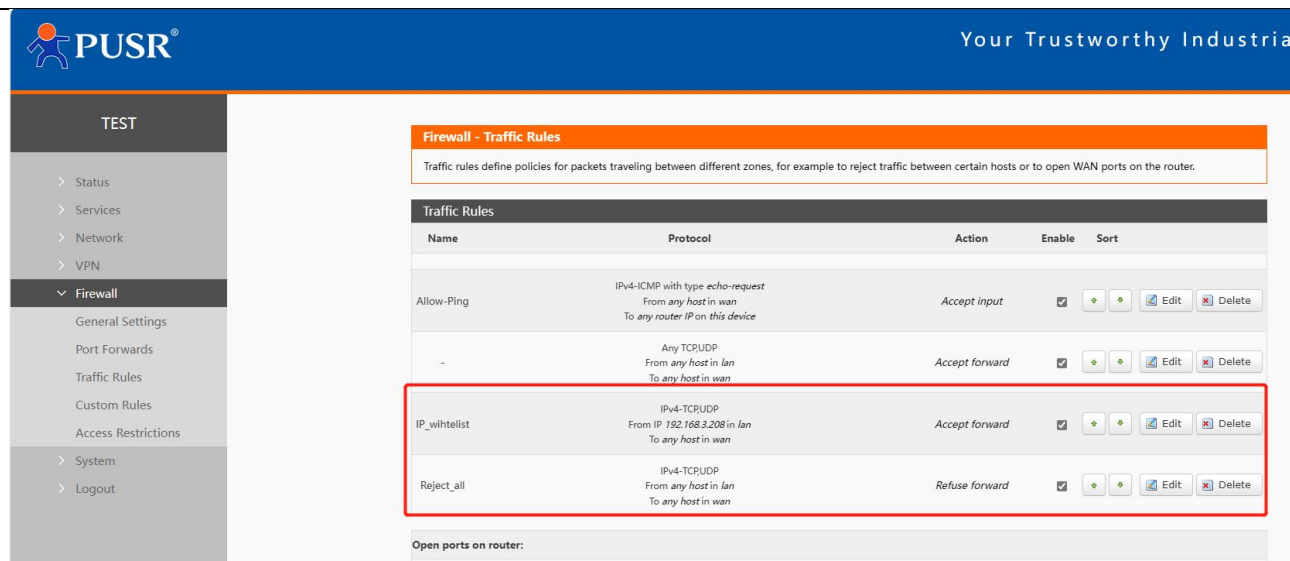
Destination port: any

Action: accept

Back to Overview Apply Save

Pic 57 Figure 3: Firewall whitelist

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



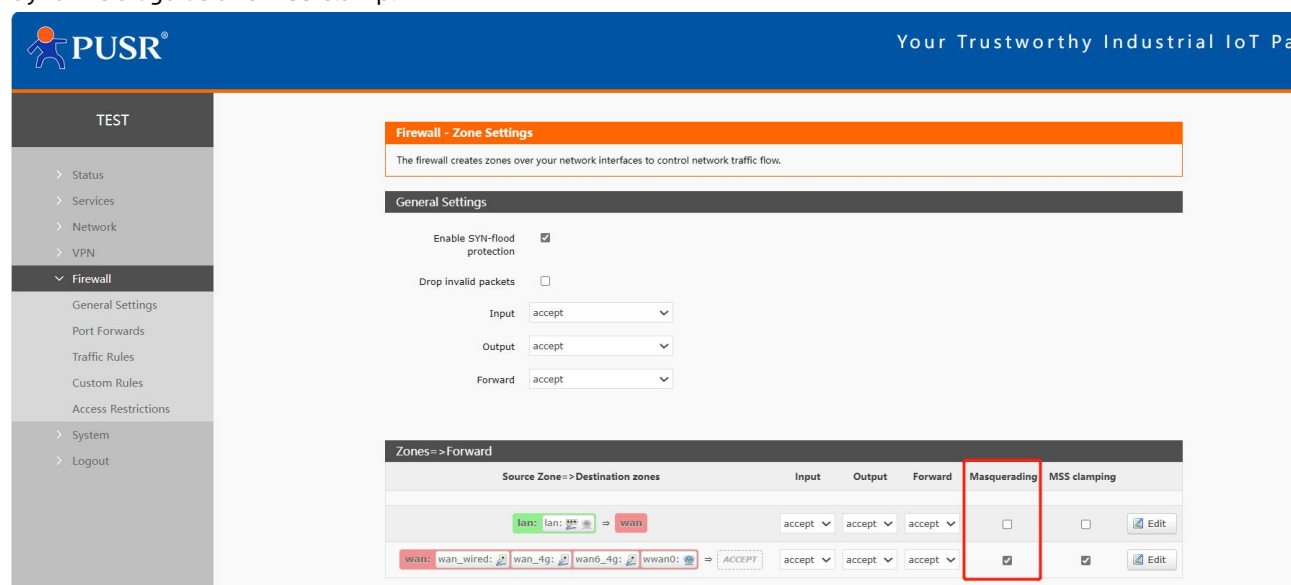
Pic 58 Figure 3 of the firewall whitelist

## 5.3. NAT function

### 5.3.1. IP address spoofing

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

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





Pic 59 IP address disguise Settings


### 5.3.2. SNAT

Source IP conversion function.

**Tab 19 SNAT parameter list**

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

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


Your Trustworthy Industrial IoT

TEST

> Status  
> Services  
> Network  
> VPN  
**> Firewall**  
General Settings  
Port Forwards  
Traffic Rules  
Custom Rules  
Access Restrictions  
> System  
> Logout



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☒  
Drop invalid packets ☐  
Input: accept  
Output: accept  
Forward: accept

Zones=>Forward

Source Zone=>Destination zones	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: => wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	 Edit
wan: wan_wired: wan_4g: wan5_4g: wwan0: => ACCEPT	accept	accept	accept	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	 Edit

Then set up the Source NAT

**PUSTR®** Your Trustworthy Industrial IoT Platform

**TEST**

- > Status
- > Services
- > Network
- > VPN
- ▼ **Firewall**
  - General Settings
  - Port Forwards
  - Traffic Rules**
  - Custom Rules
  - Access Restrictions
- > System
- > Logout

**New forward rule:**

Name	Protocol	External port
New input rule	TCP+UDP	

**Source NAT**

Name	Protocol	Action	Enable	Sort
This section contains no values yet				

**New source NAT:**

Name	Source zone	Destination zone	To source IP	To source port
SNAT	lan	wan	192.168.10.1	Do not rewrite

**Apply Save**

Pic 60 NAT Settings 1

Click Add and Edit

**PUSTR®** Your Trustworthy Industrial IoT Platform

**TEST**

- > Status
- > Services
- > Network
- > VPN
- ▼ **Firewall**
  - General Settings
  - Port Forwards
  - Traffic Rules**
  - Custom Rules
  - Access Restrictions
- > System
- > Logout

**SNAT**

**Protocol** ICMP

**Source zone** lan: lan: 192.168.10.1

**Source IP address** any

**Source port** any

**Destination zone** wan: wan\_wired: 192.168.10.1 wan\_4g: 192.168.10.1 wan6\_4g: 192.168.10.1 wwan0: 192.168.10.1

**Destination IP address** 192.168.10.1

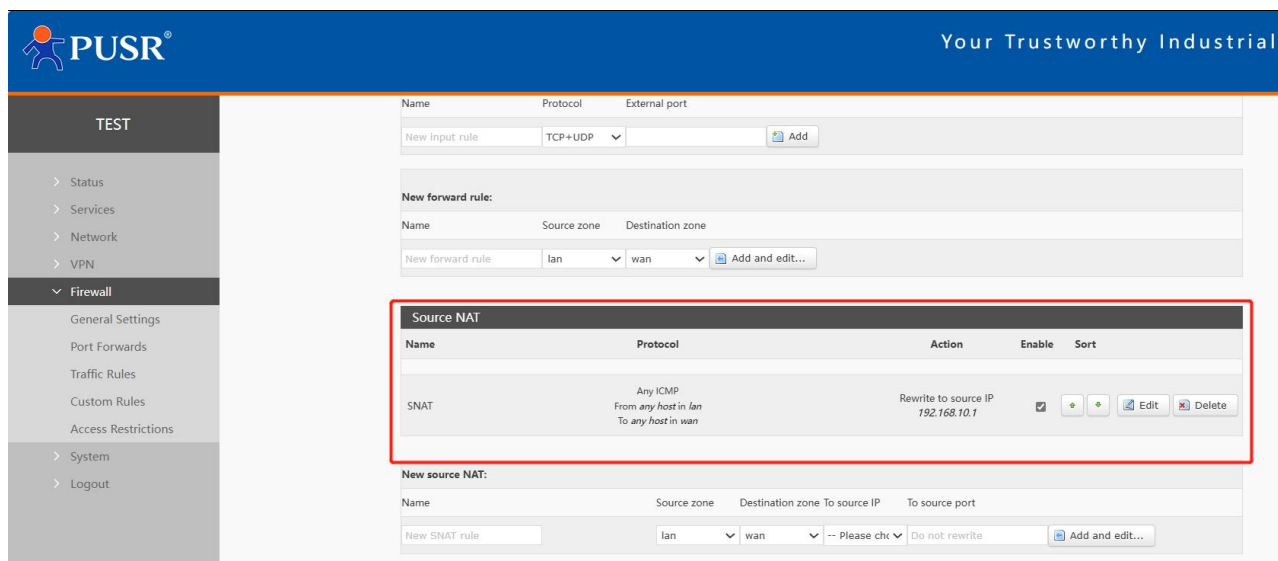
**Destination port** any

**SNAT IP address** 192.168.10.1

**SNAT port** Do not rewrite

Pic 61 NAT Settings 2

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



Pic 62 NAT Settings 3

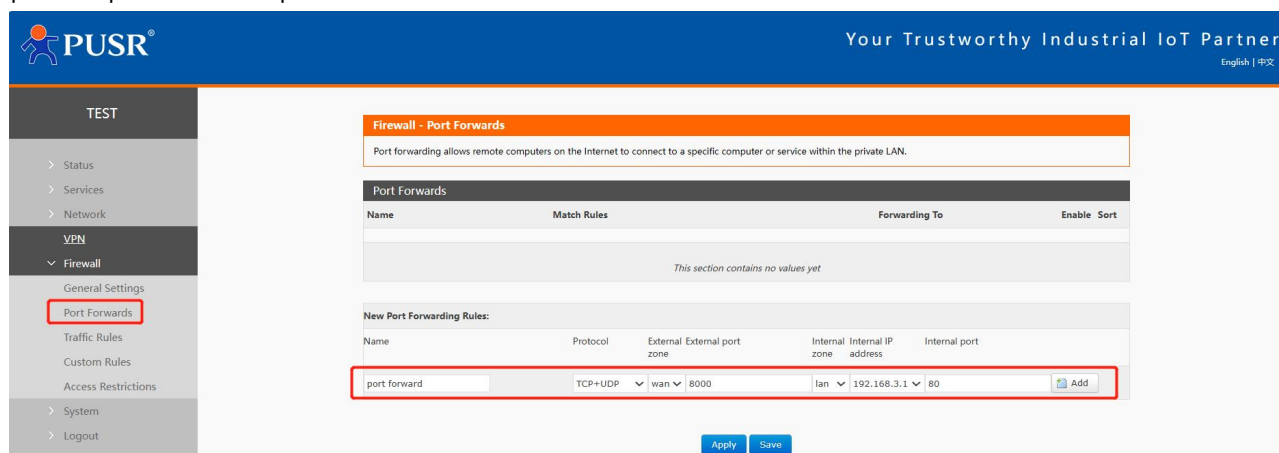
As shown in the figure, the source IP address of the packet leaving the router is changed to 192.168.9.1. As can be seen in the figure, the source address of the ICMP packet to 192.168.13.4 is 192.168.9.1, instead of 192.168.1.114. Verify that the device under the router (IP: 192.168.1.114) pings the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

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

Pic 63 NAT test and verify

### 5.3.3. Port forwarding

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



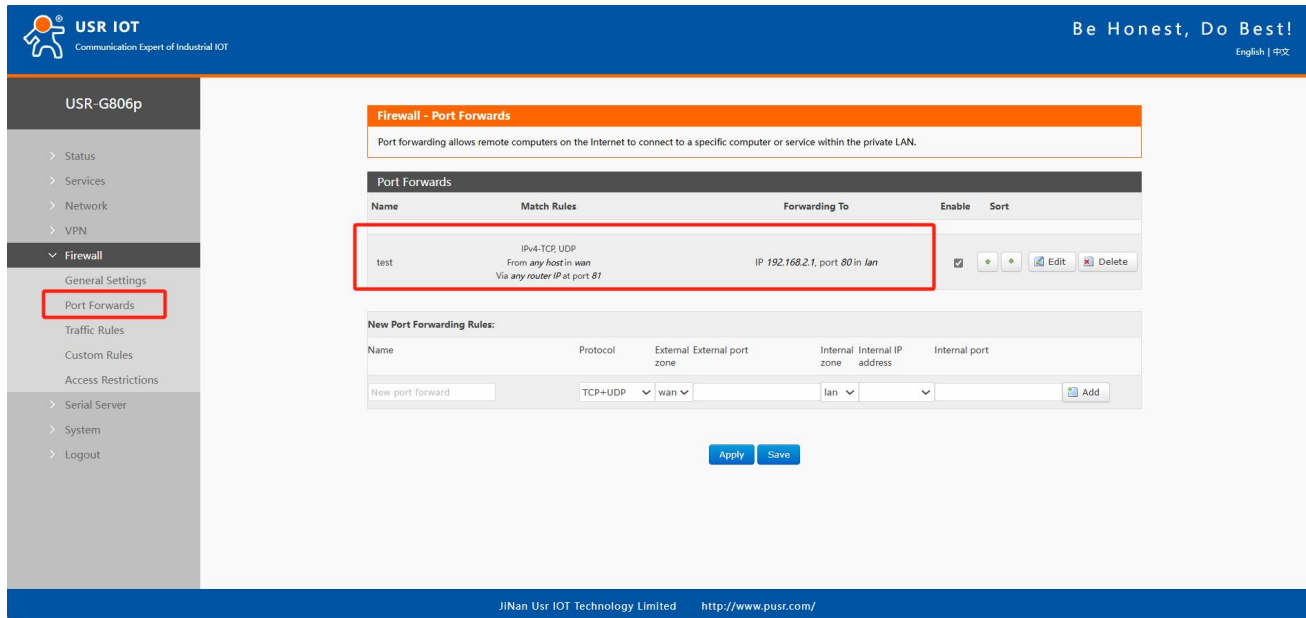
Pic 64 Port Settings page 1

- After setting the forwarding rule, you need to click the add button on the right, and then this rule will be



displayed in the rule column;

- Then click the "Apply" button in the lower right corner to make the Settings effective;
- The following Settings: 192.168.3.1:80 is the router's own web server. If we want to access a device in the LAN from the Internet, we need to set up the mapping from the Internet to the LAN, such as setting the Internet port to 81, the internal IP address to 192.168.3.1, and the internal port to 80;
- When we access port 8000 from the WAN port, the access request will be redirected to 192.168.3.1:80.



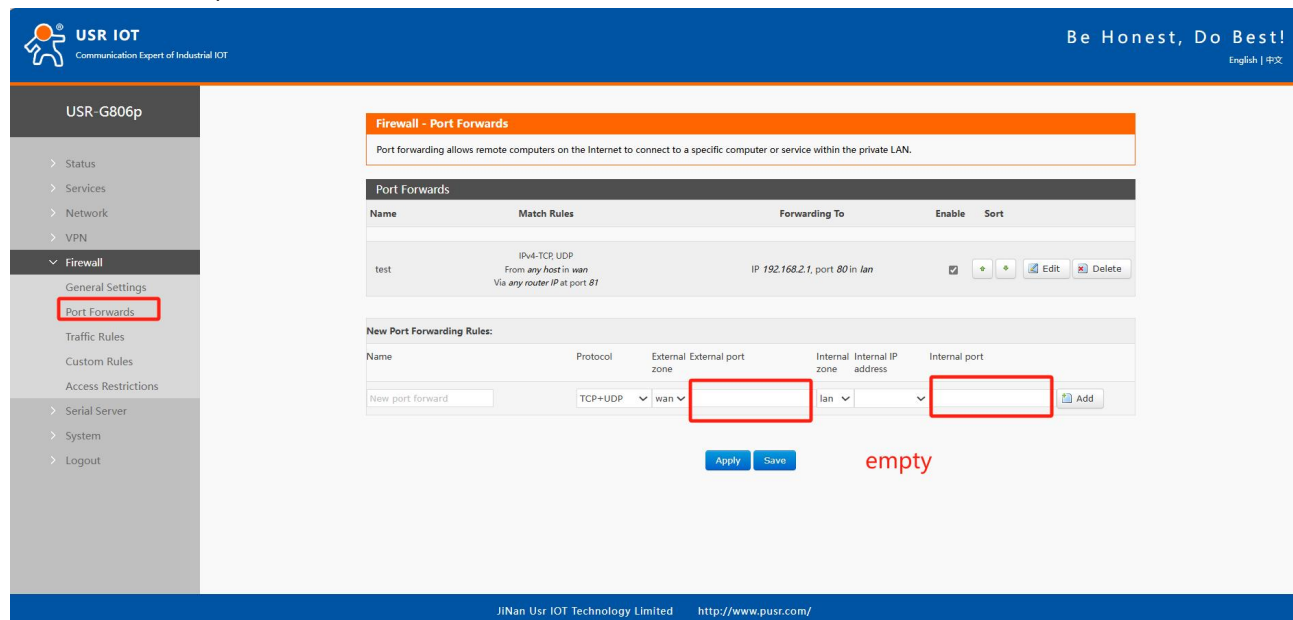
**Pic 65 Port Settings page 2**

**Tab 20 Port forwarding parameter table**

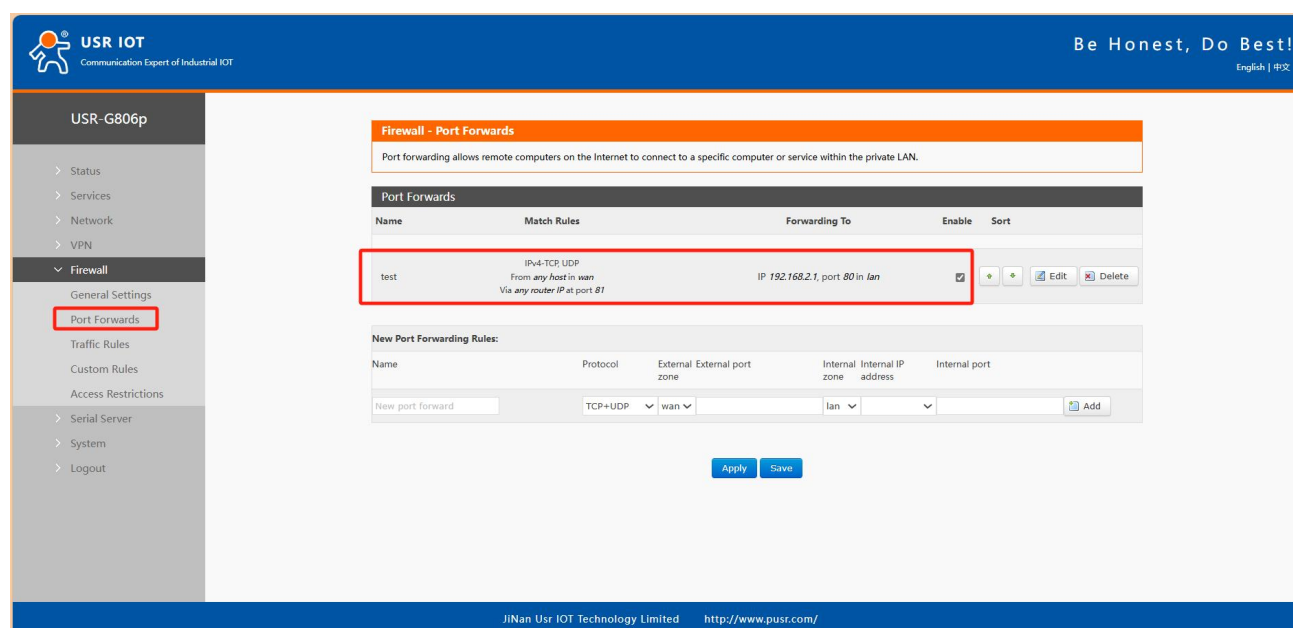
name	description	Default parameter
name	The name of this port forwarding rule, character type	empty
protocol	Protocol type can be set: TCP+UDP/TCP/UDP	TCP+UDP
exterior zone	Including wired wan, 4G, VPN	wan
External port	You can set a single port or a range of ports, such as 8000-9000 Note: When the external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

## 5.3.4. NAT DMZ

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



Pic 66 DMZ Settings 1



Pic 67 DMZ Settings 2

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

### < pay attention to >

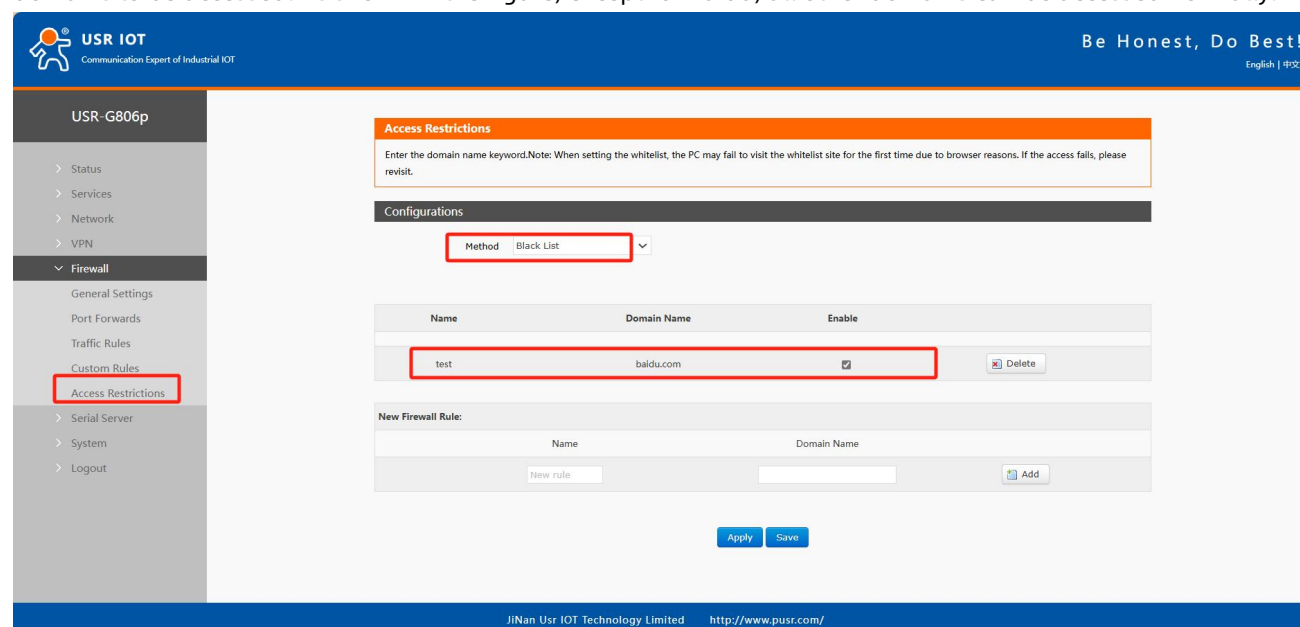
- Port mapping and DMZ functions cannot be used simultaneously.

## 5.4. Access restrictions

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

### 5.4.1. Domain blacklists

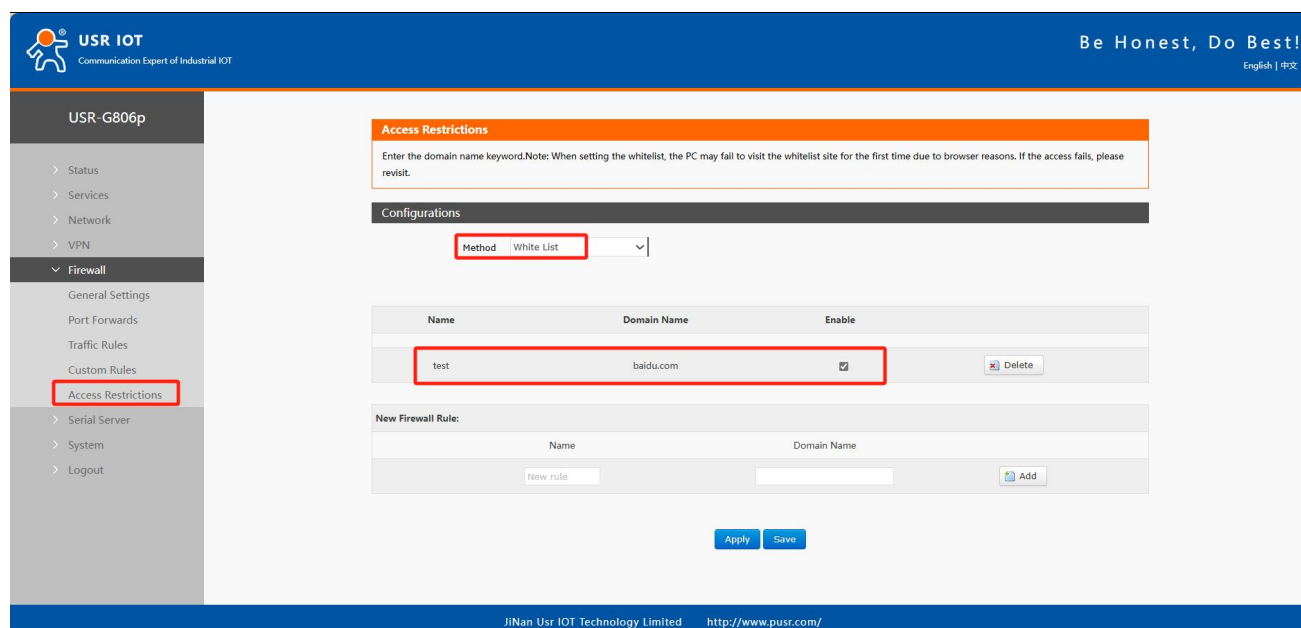
First, in the method options, select the blacklist. Click add to enter the name of the rule and the correct domain name, then click save. The rule will take effect immediately, preventing devices connected to the router from accessing the specified domain. If you choose the blacklist but do not add any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



**Pic 68 Domain blacklists**

### 5.4.2. Domain name whitelist

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



Pic 69 Domain name whitelist

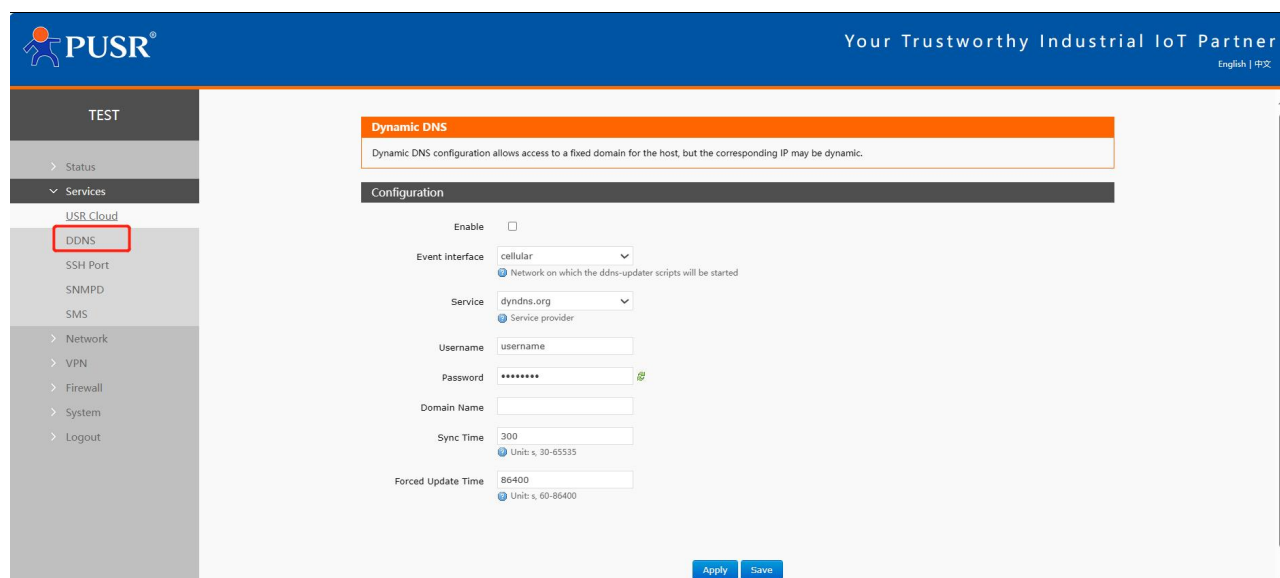
## 6. Service function

### 6.1. Dynamic domain name resolution (DDNS)

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

#### 6.1.1. Supported services

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



Pic 70 DDNS Settings page

Parameter filling requirements are as follows:

Tab 21 DDNS parameter list

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

### 6.1.2. DDNS come into force

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

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

```

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

正在 Ping fe26203015.zicp.vip [60.28.138.138] 具有 32 字节的数据:
来自 60.28.138.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138.138 的回复: 字节=32 时间<1ms TTL=127
来自 60.28.138.138 的回复: 字节=32 时间<1ms TTL=127

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

```

Pic 71 DDNS test Figure 3

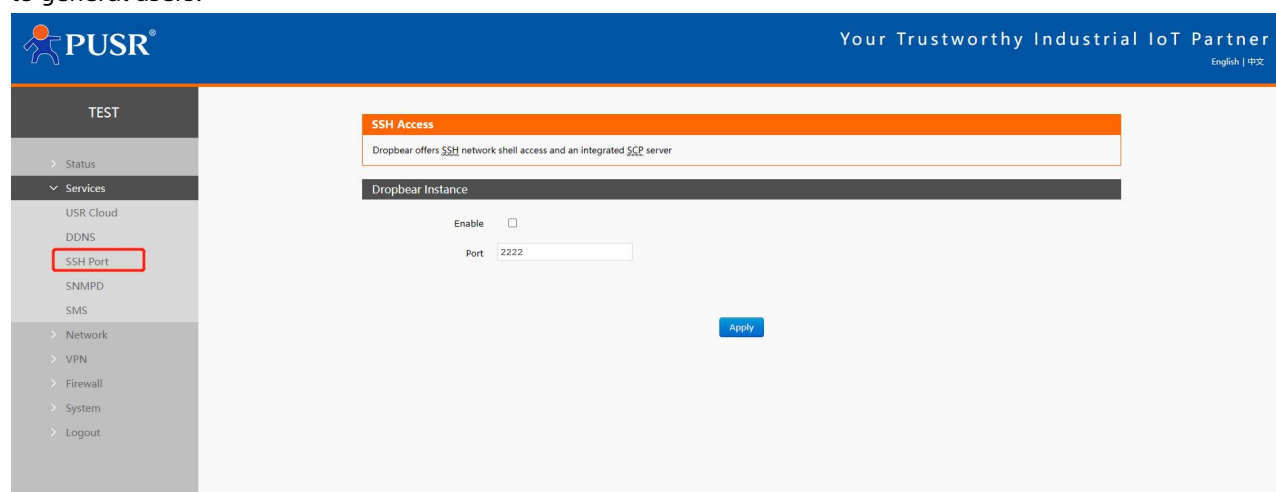
### 6.1.3. functional characteristics

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

## 6.2. SSH Port

Enable or disable SSH to manage the router.

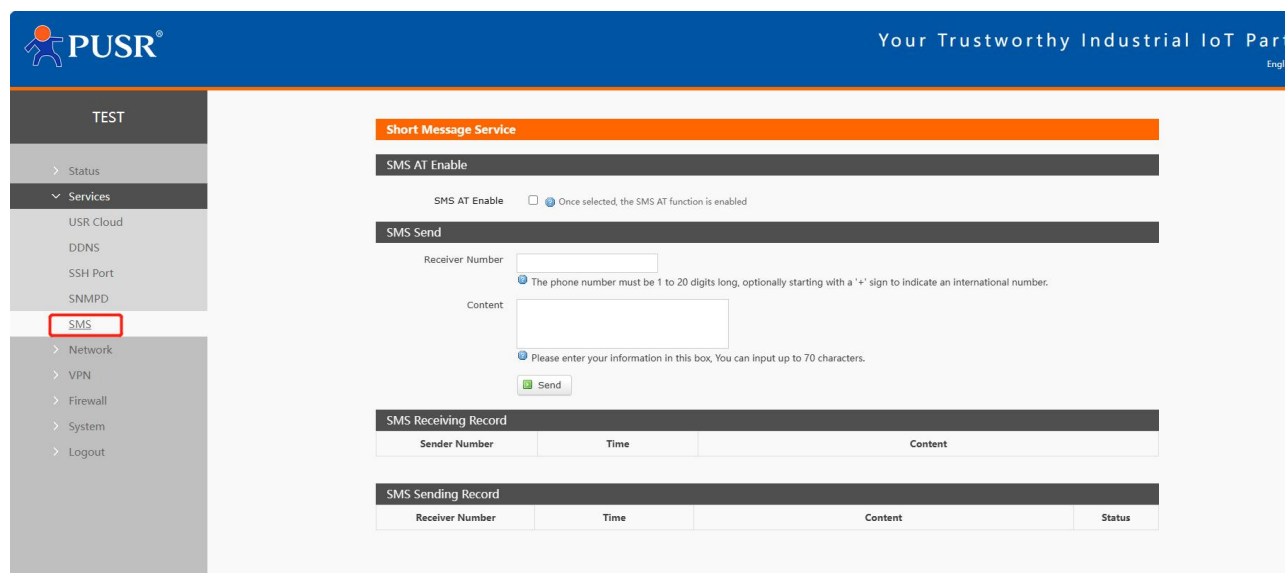
Note: This function is for PUSR technician to check technical problems. The user name and password is not available to general users.



Pic 72 SSH

### 6.3. SMS

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



**Pic 73 SMS**

**Tab 22 configuration parameter**

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

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



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



SNMP services

Exposed to SNMP users



**PUSR®**  
www.pusr.com



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

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

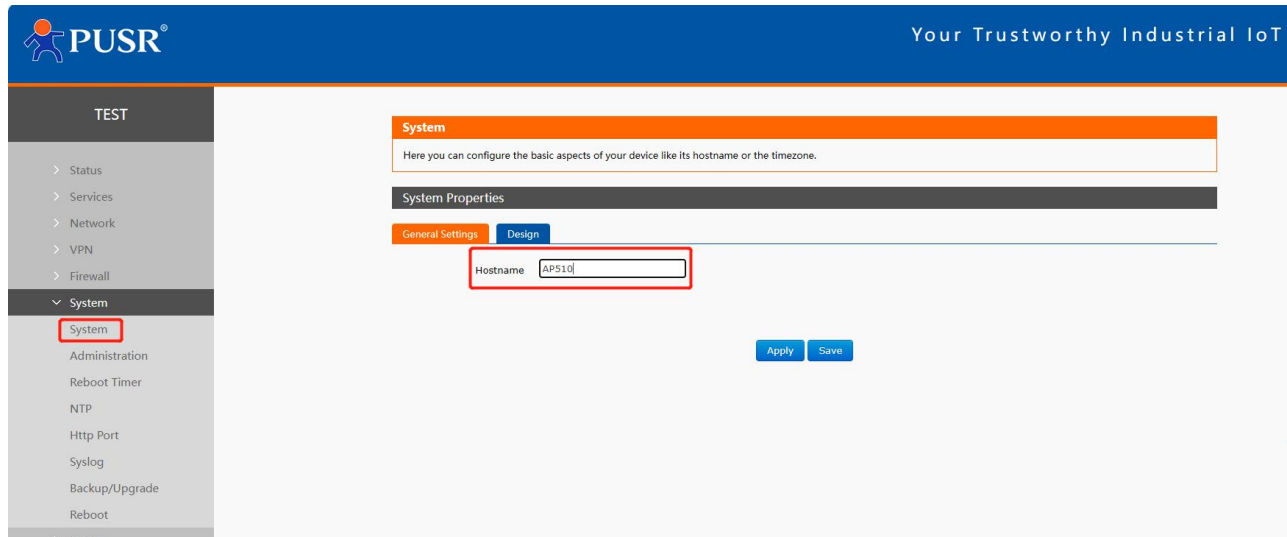
**Tab 24 SNMP OID list**

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

## 7. system function

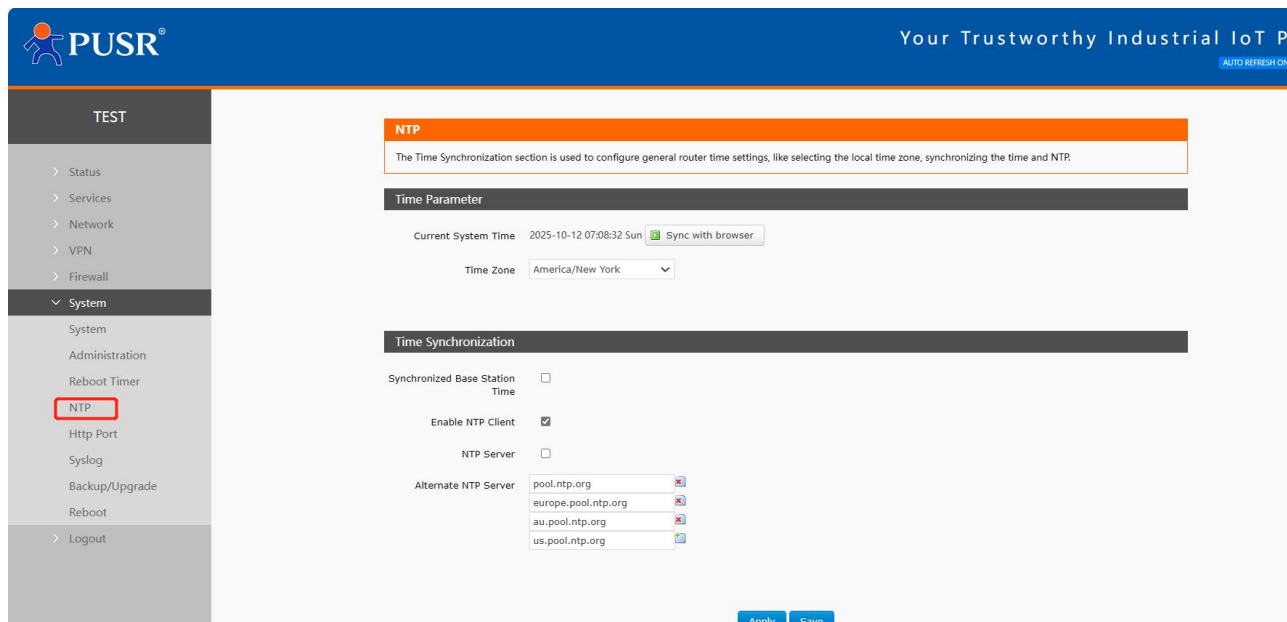
### 7.1. host name

The default hostname is AP510.



**Pic 76 host name**

### 7.2. Time Settings



**Pic 77 NTP page**

< pay attention to >

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

### 7.3. Login password Settings

**Pic 78 Username and password setup page**

< pay attention to >

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

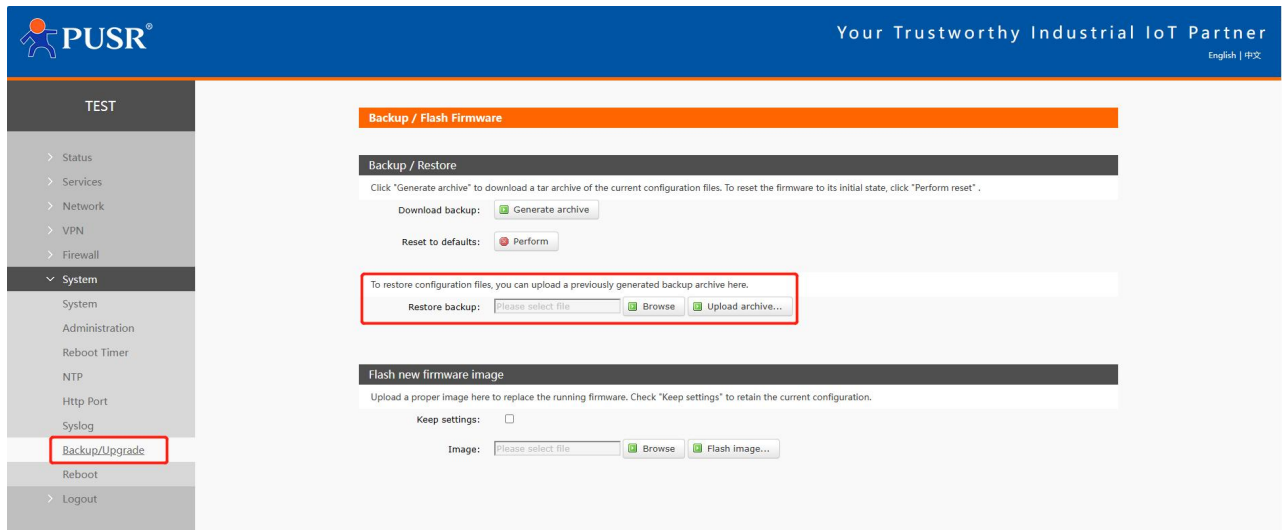
### 7.4. HTTP port

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

Note: The telnet function is for PUSR technician to check technical problems. The user name and password is not available to general users.

**Pic 79 HTTP port**

## 7.5. Parameter backup and upload



**Pic 80 Parameter backup upload page**

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

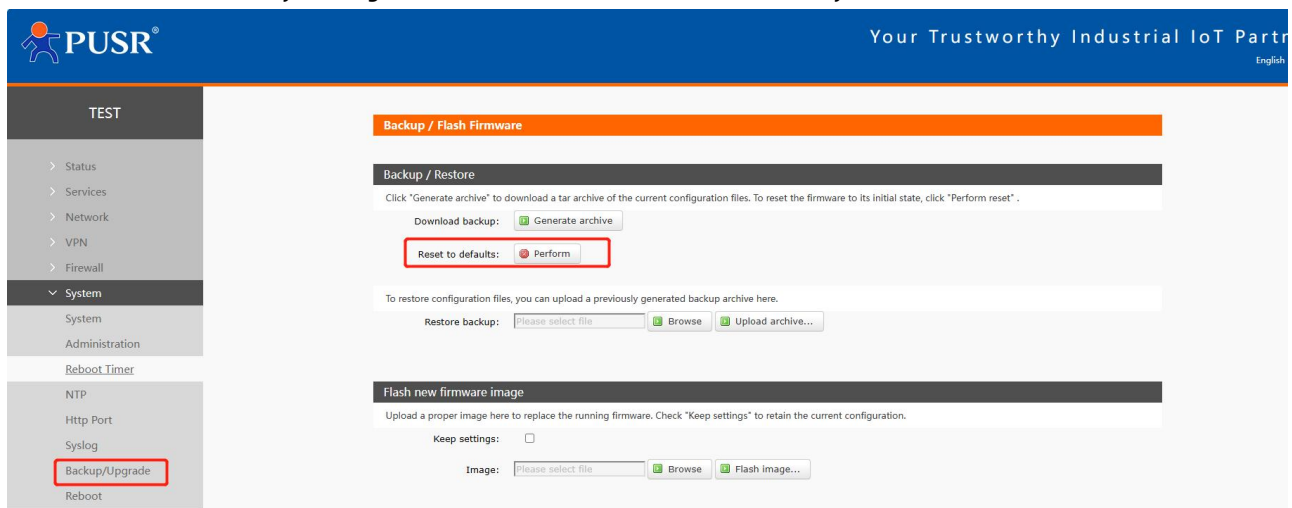
Note: Firmware recovery configuration is limited to the same version of firmware. Problems may occur due to different parameters in different versions. Users are advised to perform recovery configuration in the same version.

Parameter backup: Click the "Download Backup" button to backup the current parameter file as a compressed package file, such as backup-AP510s-2019-09-16.tar.gz, and save it to the local.

## 7.6. factory data reset

You can restore factory parameters through the web page.

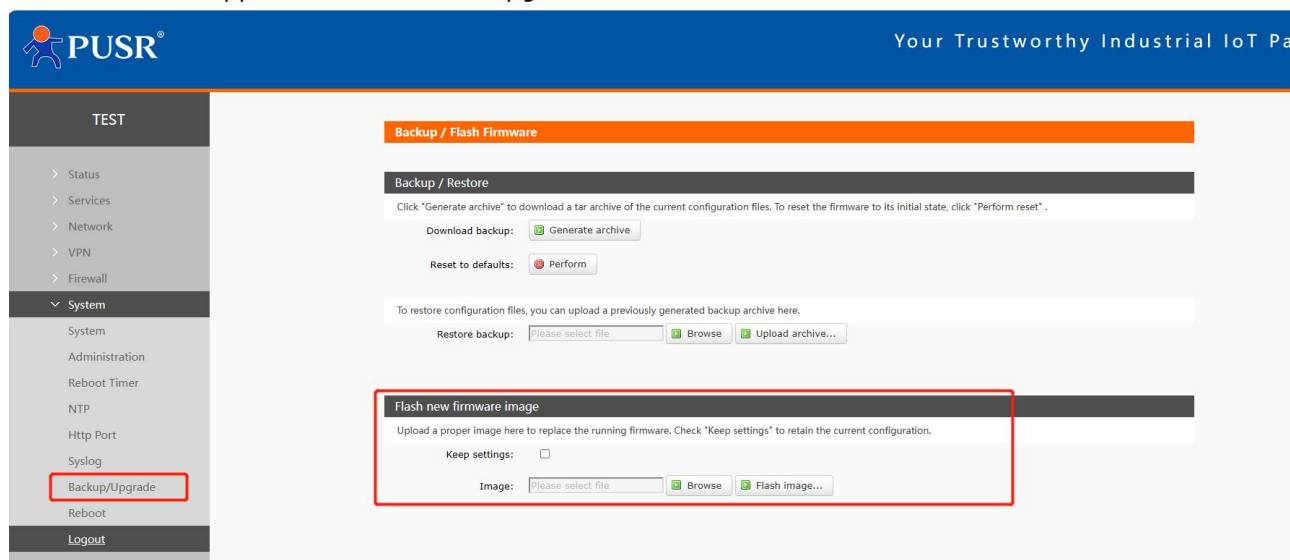
- By long pressing and releasing the Reload button (factory reset button) for 5~15 seconds, the AP510 router can be restored to the factory parameters;
- Do not disconnect power to the device during recovery. The factory recovery process lasts about 3 minutes;
- You can restore factory Settings via the web with the same functionality as follows.



## Pic 81 Restore the factory page

### 7.7. firmware upgrade

The AP510 module supports online firmware upgrade in web mode.

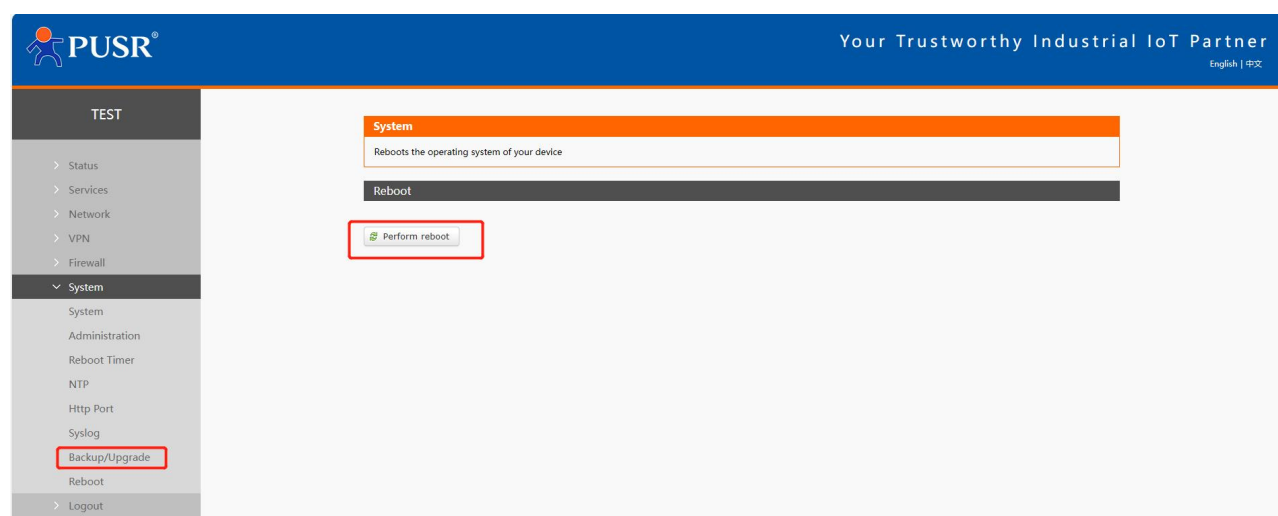


Pic 82 Restore the factory page

### < explain >

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

### 7.8. restart

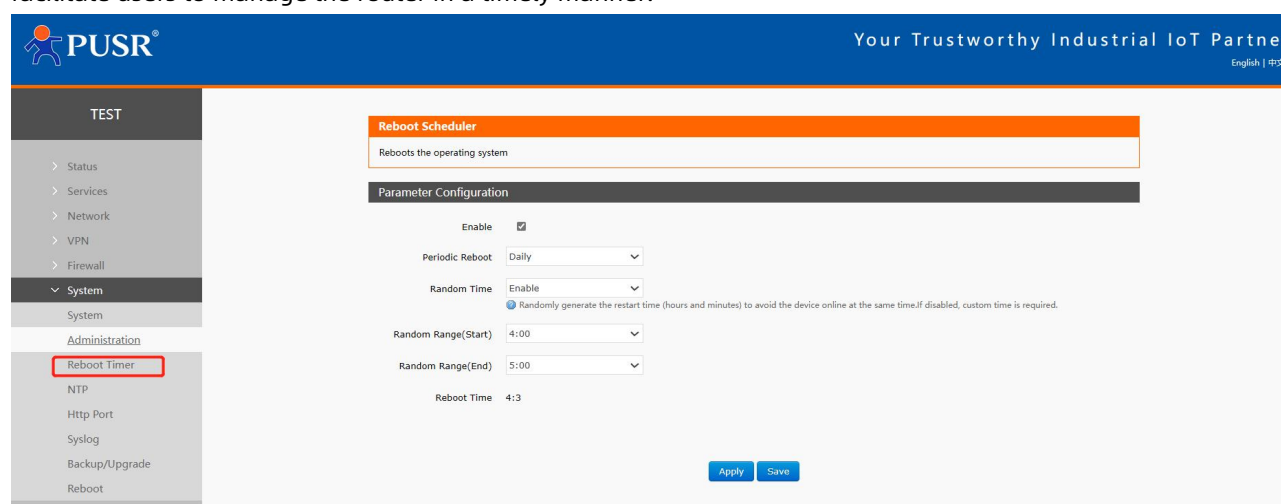


Pic 83 Restart the page

Click the button to restart the router. The restart time is the same as the power-on start time of the router, which takes about 50 seconds to complete successfully.

## 7.9. Restart at regular intervals

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



**Pic 84 Restart the Settings page**

### < explain >

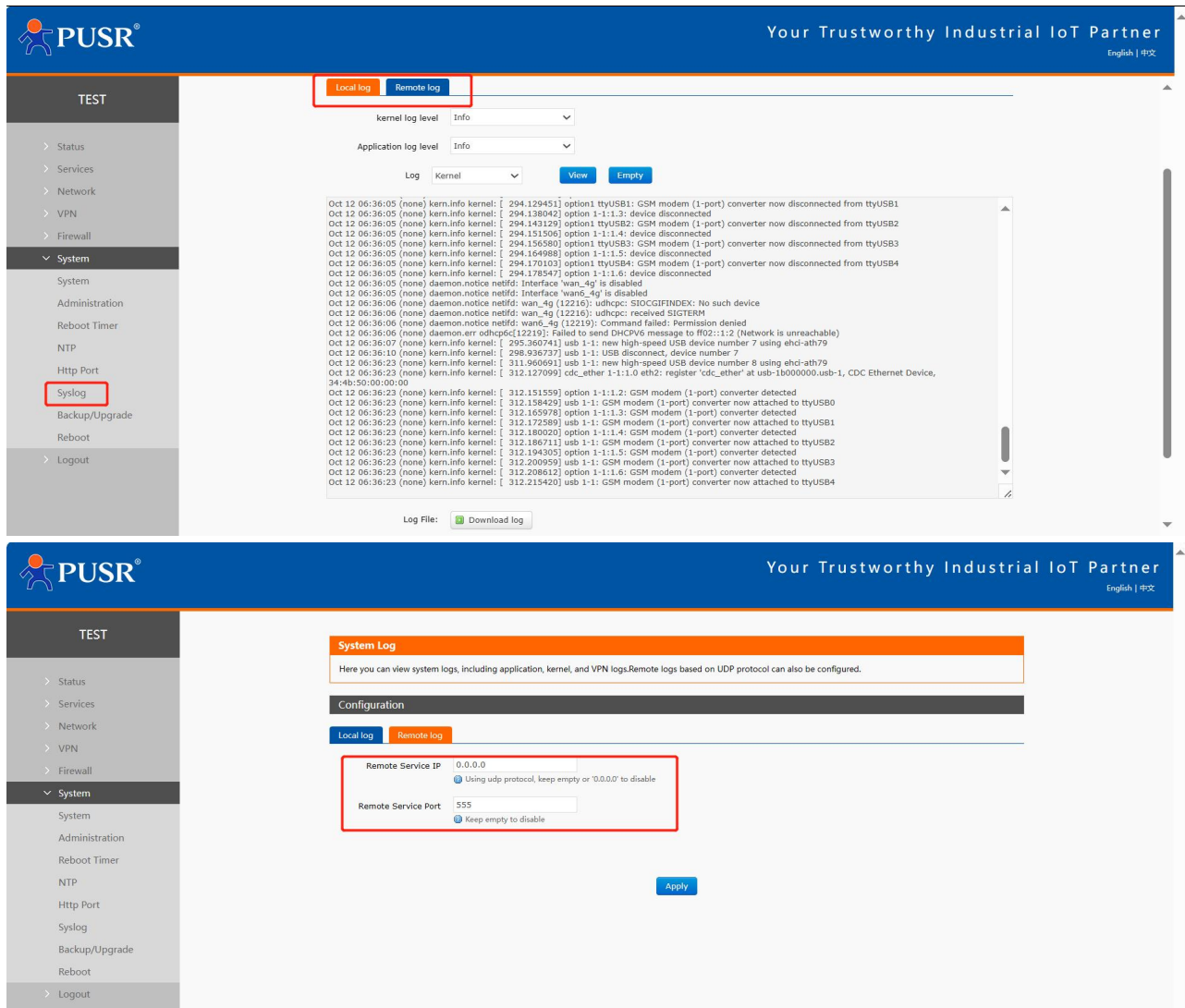
- The timer restart function is enabled by default. The restart plan will be completed at a random time between 4:00 and 5:00 every day. If you do not need this function, you can cancel it;
- According to the actual application, the scheduled restart plan that meets the conditions can be set, such as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

## 7.10. Daily record

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

### long-range Log

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



Pic 85 log page

### Local logs

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

## 8. AT order set

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

### 8.1. AT code repertory

Tab 25 Summary of AT instructions

order number	name	function
1.	AT	The Test AT command is available
2.	AT+R	Restart the device
3.	AT+H	Help document and list all instructions
4.	AT+CLEAR	Restore factory
5.	AT+VER	Query the firmware version
6.	AT+MAC	query LANMAC
7.	AT+APN	Query/set APN parameters
8.	AT+SN	query SN
9.	AT+CSQ	Query the current signal strength
10.	AT+CPIN	Query SIM card status
11.	AT+IMEI	query IMEI
12.	AT+ICCID	query ICCID
13.	AT+MCCMNC	query CIMI
14.	AT+SYSINFO	Query network operators and formats
15.	AT+CELLULAR	Query network mode
16.	AT+WEBU	Query the web user name and password
17.	AT+PLANG	query language
18.	AT+UPTIME	Query the device running time
19.	AT+WANINFO	Query wan information
20.	AT+4GINFO	Query 4G information
21.	AT+DIALINFO	Query cellular network information
22.	AT+LANINFO	Query LAN information
23.	AT+WANN	Query wan configuration
24.	AT+LANN	Query the LAN configuration
25.	AT+NETSTATUS	Query the default route

### 8.1.1. AT order set

#### 8.1.1.1. AT

name	AT
function	Test the AT command
query	order : AT return : OK
set up	not have
parameter	return : OK
explain	The instruction takes effect immediately, and the return OK represents that the AT instruction is in use



## 8.1.1.2. AT+R

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

## 8.1.1.3. AT+H

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

## 8.1.1.4. AT+CLEAR

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

## 8.1.1.5. AT+VER

name	AT+VER
------	--------

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

## 8.1.1.6. AT+MAC

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

## 8.1.1.7. AT+APN

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

## 8.1.1.8. AT+SN

name	AT+SN
------	-------

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

## 8.1.1.9. AT+CSQ

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

&lt; explain &gt;

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

standard	aus short-cut process	Signal strength (dBm)
GSM/CDMA/WCDMA/EVDO/EHRPD/LTE	0-31 Nine of the nine had no signal	$\text{dBm} = -113\text{dBm} + \text{signal strength} * 2$
TDSCDMA	100-191 Nine of the nine had no signal	$\text{dBm} = -116\text{dBm} + (\text{signal strength} - 100)$

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

## 8.1.1.10. AT+CPIN

name	AT+CPIN
function	Check the status of the device SIM card
query	Command: AT+CPIN Return: +CPIN: cpin
set up	not have
parameter	Cpin: SIM card status value

	NOTREADY: Card status is not recognized READY: Identify card status SIM PIN: Lock the PIN status SIM PUK: Lock the PUK state
explain	not have

## 8.1.1.11.AT+IMEI

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

## 8.1.1.12.AT+ICCID

name	AT+ICCID
function	Query SIM card ICCID
query	Command: AT+ICCID Return: +ICCID: iccid
set up	not have
parameter	ICcid: SIM card ICCID number
explain	not have

## 8.1.1.13.AT+MCCMNC

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

## 8.1.1.14.AT+SYSINFO

name	AT+SYSINFO
function	Query SYSINFO information

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

## 8.1.1.15.AT+CELLULAR

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

## 8.1.1.16.AT+WEBU

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

## 8.1.1.17.AT+PLANG

name	AT+PLANG
function	Query the web login language
query	AT+PLANG +PLANG:<plang>
set up	AT+PLANG=<plang> OK

parameter	plang:zh_cn/en zn_cn: the Chinese language en: English
explain	

## 8.1.1.18.AT+UPTIME

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

## 8.1.1.19.AT+WANINFO

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

## 8.1.1.20.AT+4GINFO

name	AT+4GINFO
function	Query cellular network card information
query	AT+4GINFO +4GINFO:<mac><ip><mask><rx_packets><tr_packets><rx_bytes><tx_bytes>
set up	not have
parameter	Mac: 4G network card mac

	IP: IP of 4G network card Mask: Subnet mask of 4G network card rx_packets: Number of received packets Tr_packets: Number of packets sent rx_bytes: Receive traffic tx_bytes: Send traffic
explain	

## 8.1.1.21.AT+DIALINFO

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

## 8.1.1.22.AT+LANINFO

name	AT+LANINFO
function	Query LAN network card information
query	AT+LANINFO +LANINFO:<mac><ip><mask><rx_packets><tr_packets><rx_b ytes><tx_bytes>
set up	not have
parameter	Mac: LAN network card mac IP: LAN network card IP Mask: Subnet mask of LAN network card rx_packets: Number of received packets Tr_packets: Number of packets sent rx_bytes: Receive traffic tx_bytes: Send traffic pour :

	If VLAN is configured, this command returns the LAN information
explain	

## 8.1.1.23.AT+WANN

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

## 8.1.1.24.AT+LAN

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

## 8.1.1.25.AT+PING

name	AT+PING
function	Run the ping command
query	not have
set up	AT+PING=<ip> PING IP(IP): 56 data bytes
parameter	IP: IP or domain name, which cannot be empty. Ping is carried, and the parameter is invalid For example, c1 is invalid limit [1-200]



9.		Note: Parameters can only be IP or domain names. Other parameters will be judged according to the address and return results
	explain	

## Disclaimer

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

## 10. Update log

Version	Update content	Refresh time
V1.0.1	Create documents and complete relevant function descriptions	2025-07-01



**Your Trustworthy Smart IOT Partner**

Official Website: [www.pusr.com](http://www.pusr.com)  
 **PUSR**<sup>®</sup>  
Official Shop: [shop.usriot.com](http://shop.usriot.com)  
[www.pusr.com](http://www.pusr.com)

Technical Support: [h.usriot.com](http://h.usriot.com)

Inquiry Email: [inquiry@usriot.com](mailto:inquiry@usriot.com)

Skype & WhatsApp: +86 13405313834

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