PUSR®
www.pusr.com

Communication
Expert of Industrial
IOT

Gigabit Edge Router

USR-G809 Flagship

Manual



Be Honest & Do Best

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Your Trustworthy Smart Industrial IoT Partner

Contents

1. Product introduction 6
1.1. Product feature 6
1.2. Specification parameters 7
1.3. OLED & indicator display 8
1.4. Hardware Interface Diagram 9
2. Size description 11
3. Internet operation instructions 12
3.1. Cellular network 14
3.1.1. Enabled 15
3.1.2. Configuration 15
3.1.3. SIM configuration 17
3.1.4. SIM card information display 18
3.1.5. AT command test 19
3.2. LAN interface 19
3.2.1. DHCP function 21
3.2.2. DHCP IPv6 21
3.2.3. VLAN configuration 22
3.2.4. WAN/ LAN selection 23
3.2.5. DHCP 23
3.3. WAN port 24
3.3.1. DHCP mode 25
3.3.2. Static IP mode 25
3.3.3. PPPoE mode 26
3.4. Network Failover 27
3.5. Wireless configuration 27
3.5.1. 2.4G AP1 Configuration 28
3.5.2. 5.8G AP1 Configuration 29
3.5.3. 2.4G AP2 Configuration 30
3.5.4. 5.8G AP2 Configuration 30
3.5.5. MAC-Filter 31
3.5.6. Client information 32
3.6. WWAN 32
3.6.1. 2.4G Settings 32
3.6.2. 5.8G Settings 33
3.6.3. AP information 34
3.7. Static routing 35
4. Service function 36
4. 1. Dynamic domain name resolution (DDNS) 36
4.1.1. Supported services 37
4.1.2. DDNS takes effect 37
4.1.3. functional characteristics 38
4.2. GNSS 38
4.2.1. Report Private Cloud 38
4.3. OLED 41
4.3.1. Generalized usage 41

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

4.3.2. Secondary development OLED 42
4.4. Data monitoring services 44
4.4.1. Basic configuration 44
4.4.2. Set Link Information 44
4.4.3. TCPC Data Monitoring Examples 46
4.5. Event alarm service 48
4.6. SMS service 48
4.6.1. Basic configuration 49
4.6.2. SMS Service 50
4.6.3. Transmission list 50
4.7. SNMPD 51
5. VPN function 53
5.1. PPTP Client 53
5.2. L2TP Client 56
5.3. IPSec 58
5.4. VXLAN 60
5.5. OpenVPN 60
5.5.1. Openvpn TAP Bridge Instance 67
5.5.2. An Example of Implementing Subnet Interworking in Openvpn TUN 71
5.6. GRE 75
5.7. Wireguard 76
6. Developers 81
6.1. Application management 81
6.1.1. Custom program upload 81
6.1.2. Back-end implementation logic 82
6.2. web console 86
7. Firewall 86
7.1. Basic setup 86
7.2. Communication rules 87
7.2.1. IP address blacklist 88
7.2.2. IP address whitelist 90
7.3. Nat function 92
7.3.1. IP address masquerading 92
7.3.2. SNAT 93
7.3.3. Port forwarding 96
7.3.4. DNAT 97
7.3.5. NAT DMZ 99
7.4. Access restriction 100
7.4.1. Domain name blacklist 100
7.4.2. domain name white list 101
7.5. custom rules 102
8. Edge computing 102
8.1. data point 103
8.1.1. Add Slave 105
8.1.2. Add Point Table 106
8.1.3. Edge computing 107

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

8.2. IO Management 108
8.2.1. IO hardware connection 109
8.2.2. IO function 109
8.2.3. IO status 111
8.3. Protocol conversion 112
8.3.1. Modbus RTU 112
8.3.2. Modbus TCP 113
8.3.3. JSON 113
8.4. Edge Gateway 116
8.4.1.1. Serial port management 116
8.4.1.2. Communications link 117
8.4.1.3. Network disconnection cache 118
8.4.1.4. Data reporting 119
8.4.1.5. Json Reporting Template 120
8.4.1.6. Linkage control 121
8.5. Edge computing management 124
8.5.1. configuration management 124
9.1. Serial port settings 125
9.1.1. Time triggered mode 125
9.1.2. Length Trigger Mode 126
9.2. Communication configuration 126
9.2.1. TCPC mode (TCP Client mode) 126
9.2.2. TCPS mode (TCP Server mode) 128
9.2.3. UDPC mode (UDP Client mode) 128
9.2.4. UDPS mode (UDP Server mode) 130
9.2.5. MQTT mode 130
9.2.6. Connect to Amazon 133
9.2.7. Connect to Alibaba Cloud Platform 134
9.2.8. HTTPD mode (HTTP Clientmode) 135
9.2.9. Registration Package/Heartbeat Package Features 136
9.3. Advanced settings 137
10. System function 138
10.1. host name 138
10.2. Time setting 139
10.3. Username Password Settings 139
10.4. Safety management 140
10.5. Memory management 140
10.6. configuration snapshot 141
10.7. Parameter backup and upload 142
10.8. Factory data reset 142
10. 9. Firmware upgrade 143
10.10. Set built-in web pages to neutral 143
10.11. Restart 146
10.12. Timed restart 146
10.13. Instrument 147
10.13.1. Network diagnostic function 147
10.13.2. TCPUDMP Traffic Monitoring 147

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

10.14. Log 147
11. AT Command set 148
11.1. AT Instruction list 150
11.1.1. AT Command Set 152

1. Product introduction

G809 series is a new generation flagship router launched by some companies for industrial fields. It adopts high-end Qualcomm solution master control in the industry. It has Gigabit （2*SFP+8*RJ45）, supports 4G cellular network board capability, has 8GB large storage capacity and Python two-switch, has Qualcomm dual-frequency WIFI6 function and rich hardware interfaces, and has 1*RS232+1*RS485 , 1*DIDO, dual SIM redundancy, GNSS positioning, OLED display screen, USB interface and SD interface. It provides uninterrupted Internet access at any time and anywhere. With its comprehensive hardware interface and strict industrial-grade design, it provides stable and reliable networking solutions for digital upgrades in various industries.

This product adopts industrial standard, wide temperature-40℃~75℃,wide voltage DC 9-60V power supply, strong hardware protection, and after a number of harsh environment tests, built-in software and hardware dual watchdog, fault recovery and other mechanisms, can adapt to different industry scenarios, in harsh environments still stable and reliable operation.

Save money: Gigabit 10 network port +DC 60V, save the cost of buying Gigabit fiber switches and power supplies separately.such as factory renovation, energy cabinet,

Labor saving: Qualcomm WiFi6, faster and more convenient data transmission and operation and maintenance.For example, chain stores, coal mine networking

Worry-free: 8G large storage, user data and programs can be stored at ease. For example,humanoid robot localization edge calculation

1.1. Product feature

Stable and reliable

- Aluminum alloy shell, IP40 protection: reduce the impact of dust;
- Industrial wide temperature：-40℃~+75℃ design;
- The voltage input is DC 9-60V, and the power supply reverse protection is available;
- EMC National standard 3B hardware high protection level, specially designed for harsh industrial environment;
- Built-in hardware and software watchdog, self-detection and self-repair of faults to ensure system stability;
- Standard rail installation method Standard rail installation method;

Flexible networking

- Support Gigabit 2*SFP +Gigabit 8*RJ45;
- Support 4G Global Band;
- Support TF and USB peripheral access;
- Link redundancy design, dual SIM card slots;
- 1*RS232/RS485+1*RS485;
- 1*DI+1*DO;
- Supports Qualcomm dual-band Wi-Fi6 (AP/STA/Relay/Bridge);

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Powerful

- 1GB memory +8GB eMMC, Python;
- Support PPTP/L2TP/IPSec/OpenVPN/GRE/VXLAN/DMVPN/Wireguard;
- Support cellular network to lock frequency band and frequency point、PCI;
- Supports TCP/UDP/Modbus/MQTT/HTTP protocol serial port transmission;
- Support edge collection computing and report through MQTT+JSON format;
- Support cloud services such as PUSR Cloud Monitoring/Alibaba Cloud;
- Support SNMP/ SMS/alarm/monitor/DDNS and other network services;
- Support key service information of OLED display, and support two open custom OLED display content;
- Supports failover, dual SIM/dual WAN/wireless WIFI mutual backup capability, and always keeps the network offline;
- Supports GPS positioning, and supports displaying location information on the cloud and reporting to private servers;
- Supports static routing, policy routing, and dynamic routing protocols;
- Supports IPV6;
- Support ICMP keep-alive detection, heartbeat packet detection and other functions to ensure stable operation of the equipment;
- Supports security firewall, DNAT, SNAT, DMZ, port forwarding, access restriction, etc;
- Supports remote networking and boundaryless remote access terminal capability;
- Supports opening the built-in web page of the router through the PUSR Cloud, so that you can easily access the router without a dedicated network or public IP;
- Support network IO management and remote control of switches;
- Supports APP installation;
- Support RTC clock;
- Supports data acquisition breakpoint continuation and GNSS breakpoint continuation.

1.2. Specification parameters

Hardware Specifications		
Cellular	4G Global frequency bands	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 interface	2* Standard SMA-K interface (outer screw and inner hole)
	SIM card slot	2 *None-SIM
Ethernet Interface	Number of network ports	Version with 10 LAN ports：2*WAN/LAN+6*LAN+2*SFP；SFP: 1*WAN/LAN+1*LAN
	Network port specifications	RJ45：10/100 /1000Mbps，IEEE 802.3 SFP：Gigabit optical port It has 1.5KV network isolation transformer protection
Connecting Terminal	V+，V-	Built-in power reverse protection
	GND	Ground terminal;
	Tx	RS232
	Rx	RS232
	A	RS485
	B	RS485
	DI1	Digital input port
	DO1	Digital output port
	Com	Common teminal

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Wi-Fi6	Antenna interface	2 * Standard RP-SMA-K interface (External screw and internal pins)
	MIMO	2×2
	Standard and frequency band	Support IEEE802.11b/g/n/ac/ax，2.4GHz&5.8G
	Wireless functionality	AP / STA/ Relay / Bridge
	The rate of the theory	2976Mbps(5GHz:2402Mbps,2.4GHz:574Mbps)
	Secure encryption	No encryption/mixed-psk/psk/psk2/psk2+ccmp
	Transmission distance	Open outside / no obstruction, coverage radius up to 200 meters; Indoor office environment/barrier, coverage radius up to 40 meters Note: The measured rate is affected by the field environment, please take the measured rate as the standard
	Theoretical device capacity	2.4G+5.8G:256
Positioning Function	Antenna interface	1 * Standard SMA-K interface (external screw and internal hole)
	Positioning criteria	GPS
Power Supply Specifications	Adapter	DC 12V/2.5A
	Power supply interface	Power supply for industrial terminals with anti-polarity protection
	Scope of power supply	DC 9-60V
Serial Port	RS485/RS232	Industrial terminal
	Baud rate（bps）	1200,2400,4800,9600,19200,38400,57600,115200,230400
	Data bit	7,8
	Stop bit	1,2
	Check bit	NONE,ODD,EVEN
Physical Characteristics	Hull	Aluminum alloy shell, dustproof grade IP40
	Size;	118.0*96.0*48.7mm（L*W*H，Parts and antenna seats are not included）
	Way to install	Guide rail installation, horizontal desktop placement
	EMC	National standard 3B grade
	working temperature	-40℃ ~ +75℃
	Storage temperature	-40℃~+85℃（No condensation）
	Working humidity	5%~95%（No condensation）
Other	Reset/Switch Screens	Long press for 5-15 seconds to restore factory settings, and short press for 1-3 seconds to switch screens.
	USB	Supports USB flash drives to expand storage space
	SD card slot	Support SD card to expand storage space
	RTC	RTC
	Ground protection	Grounding screws
	Built-in watchdog	Supports self-detection of equipment and self-recovery of faults
	OLED	Display the basic information of the router

Product power consumption table

operate mode	supply voltage	maximum current	power consumption
No-load power consumption	DC12V	0.71A	8.52W
Full load power consumption	DC12V	1.785A	21.42W

1.3. OLED & indicator display

Name	Icon	Description
PWR	⏻	The power is on and always on

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

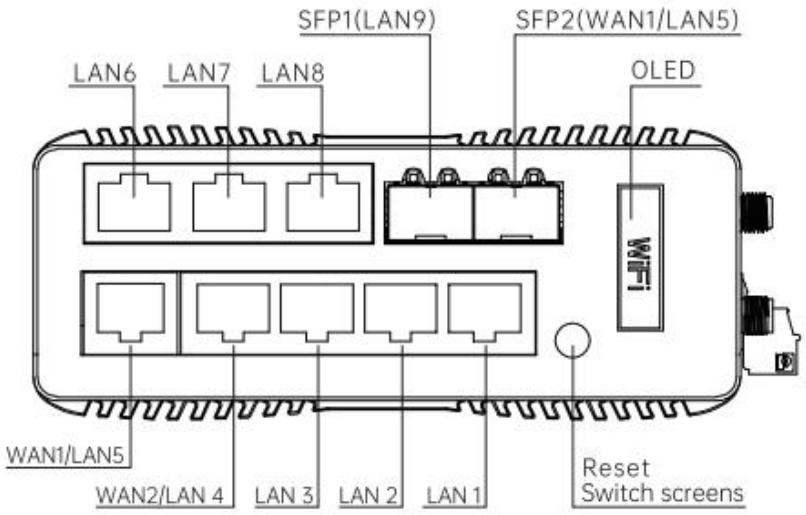
WIFI		Turn on WiFi
		Turn off WiFi
NET		2G Cellular registered
		3G Cellular registered
		4G Cellular registered
		5G Cellular registered
		No Signal
	NOT READY	No SIM card detected
	READY	SIM card detected，but not registered on the network
RSRP	S3 S2 S1	dbm[-51 ~ -63] S3： Strong signal dbm[-63 ~ -83] S2： Medium signal dbm[<-83] S1： Weak signal
GPS		Turn on GPS
		Turn off GPS
DI		DI input is in low level state (DI is off)
		DI input is in high level state (DI is on)
DO		DO make-and-break
		DO disconnect state
DATE	2025-01-01 12:00:00（+0800）	System date/Time zone
SIM	SIM1:0.00MB SIM2:0.00MB	Displays the current month's usage (SIM1 and SIM2)
Reset	Release button Reset is ready	Restore the release prompt at factory
Starting up	System booting Please wait...	Device startup prompt
Firmware upgrade	Upgrading Please Wait	Firmware upgrade in progress
	Upgrade Successful	The firmware upgrade was successful

1.4. Hardware Interface Diagram

Interface Specification

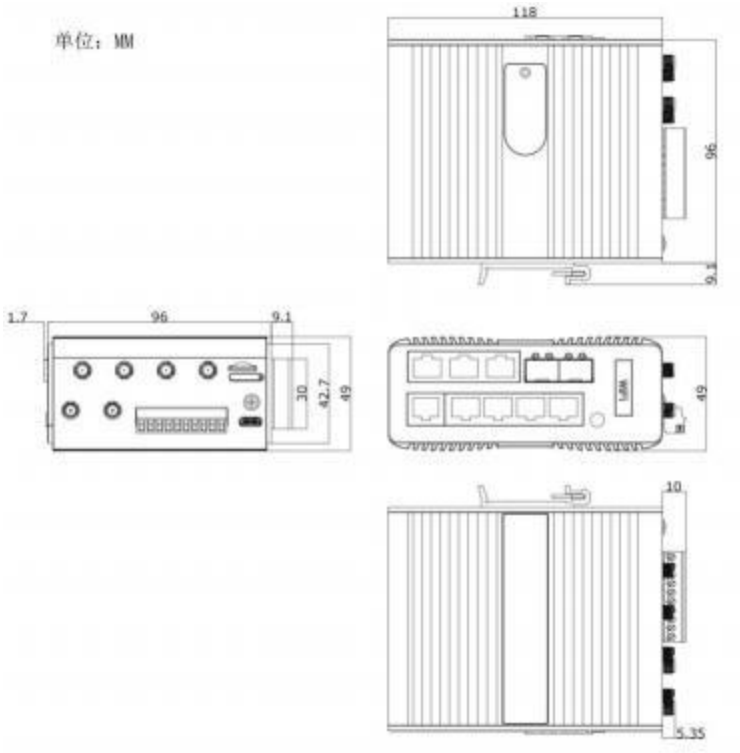
Binding post	Description
V+, V-	DC 9-60 V wide voltage supply, 2 core terminals, built-in power reverse protection
RX/TX	RS232 pin
A2/B2	RS485 pin
GND	Earth terminal
DI	Digital input interface (Dry contact); The input voltage is 0-30V,0-3V is low, 10-30V is high, and the maximum input voltage is 30V
DO	Digital output interface (wet node); Maximum withstand voltage current 30VDC@300mA
COM	common port
Interface/Button	**Description**
SIM card slot	2 * None-SIM
Reset	Long press for 5s~15s and release to restore the device to factory default Settings; Short press 1~3S and release, the LED screen switches pages
SD	Supports SD card to expand storage space (plug-in standard micro SD card)
Type-C	You can insert a U disk to expand the storage space (Use Type-C to USB-A adapter)
Ethernet Interface	**Description**
Number	2*WAN/LAN+6*LAN+2*SFP; Among them, SFP: 1WAN/LAN (electro-optical or LAN) +1LAN; ports marked with numbers 1,2,3,4 support VLAN division
Specification	RJ45 interface: 10/100 /1000Mbps adaptive, conforming to IEEE 802.3 SFP optical port: Gigabit optical port It has 1.5KV network isolation transformer protection
Network port indicator light	No network cable inserted: off Plug in the network cable: On Data communications: Flashes
Antenna Interface	**Description**
WIFI	2 * WIFI antenna interface, SMA-K interface (External screw and internal hole)
4G	4 * 4G antenna interface, SMA-K interface (External screw and internal hole)

Web portal description



Web Port Name	explain	default type
WAN1/LAN5	Electrical port: WAN/LAN conversion can be set through the router built-in webpage VLAN function	WAN
WAN 2/LAN4	Electrical port: WAN/LAN conversion can be set through the router built-in webpage VLAN function	LAN
LAN1 ~ LAN4	Electrical port: support VLAN partition function	LAN
LAN6 ~ LAN8	Electrical port: does not support VLAN division, bridging to br-lan NIC	LAN
SFP1(LAN9)	Optical port: does not support VLAN segmentation, bridging to br -lan NIC	LAN
SFP2（WAN1/LAN5）	Optical port: and electrical port WAN1/LAN5 physical interface can not be used at the same time, you need to choose one of the two to use,through the router built-in web WAN function settings WAN_WIRED network card to select the interface type GE Interface: Select WAN1/LAN5 Physical Interface Use SFP interface: Select SFP2 (WAN1/LAN5) physical interface use	GE interface

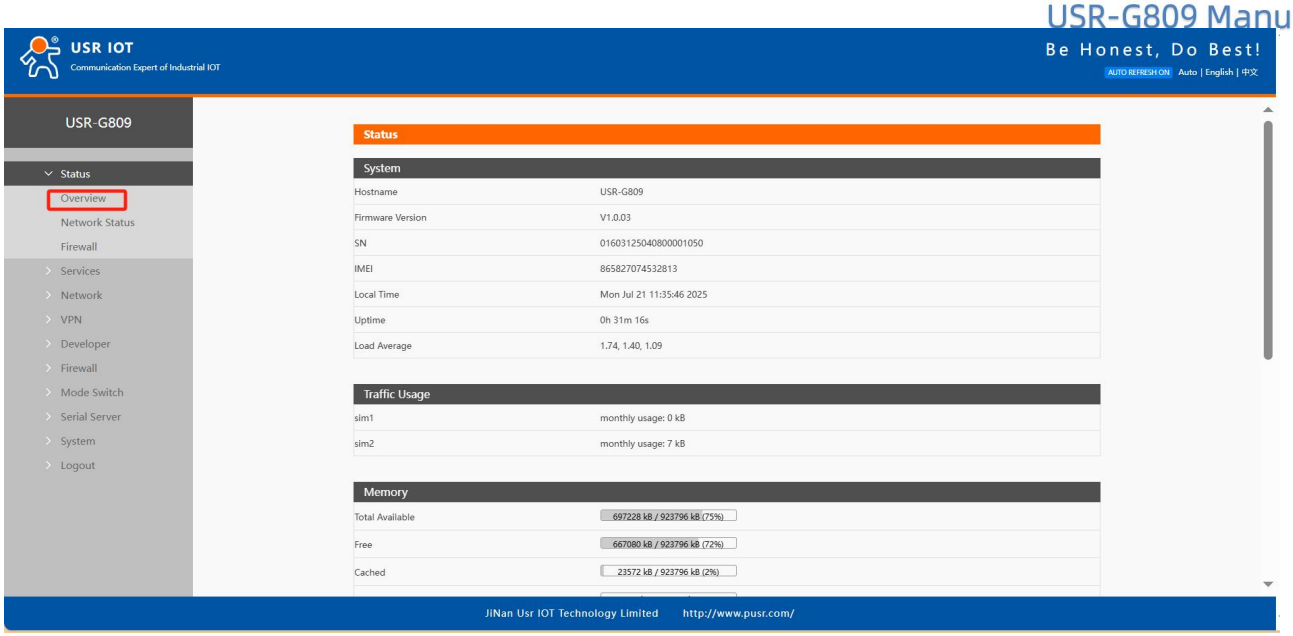
2. Size description



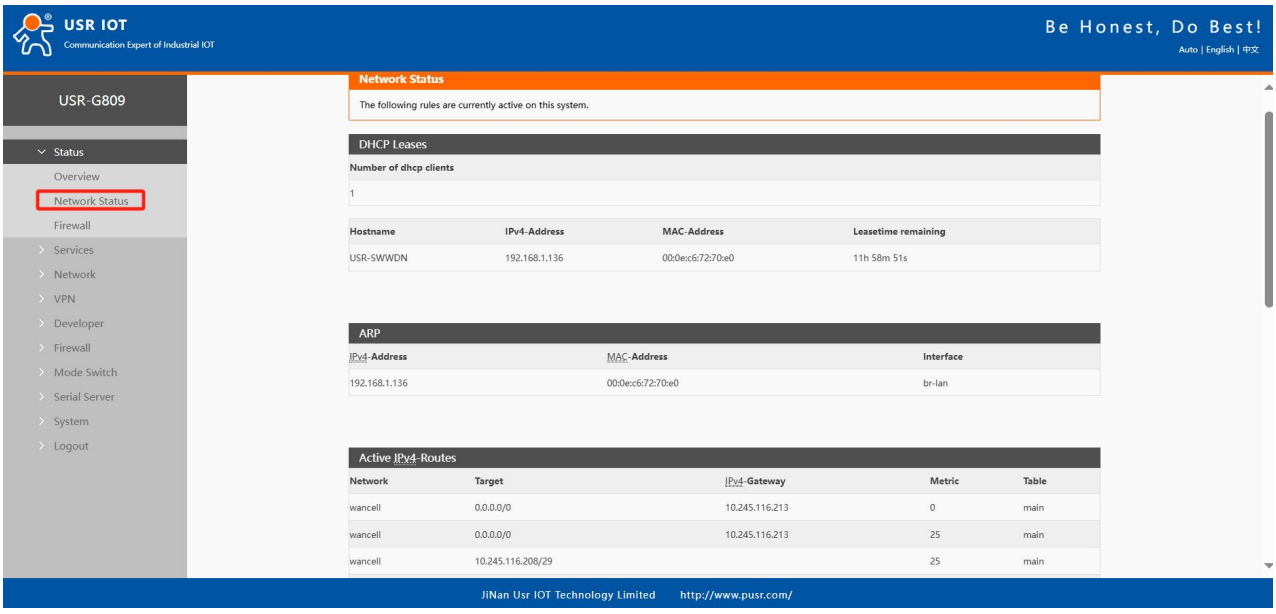
3. Internet operation instructions

When using the USR-G809 for the first time, you can connect to the LAN port of the USR-G809 through a PC, or connect to Wi-Fi, and then configure it using the web management page.

Parameter	Default setting
SSID	USR-G809-XXXX
LAN port IP address	192.168.1.1
user name	admin
password	admin
wireless password	88888888

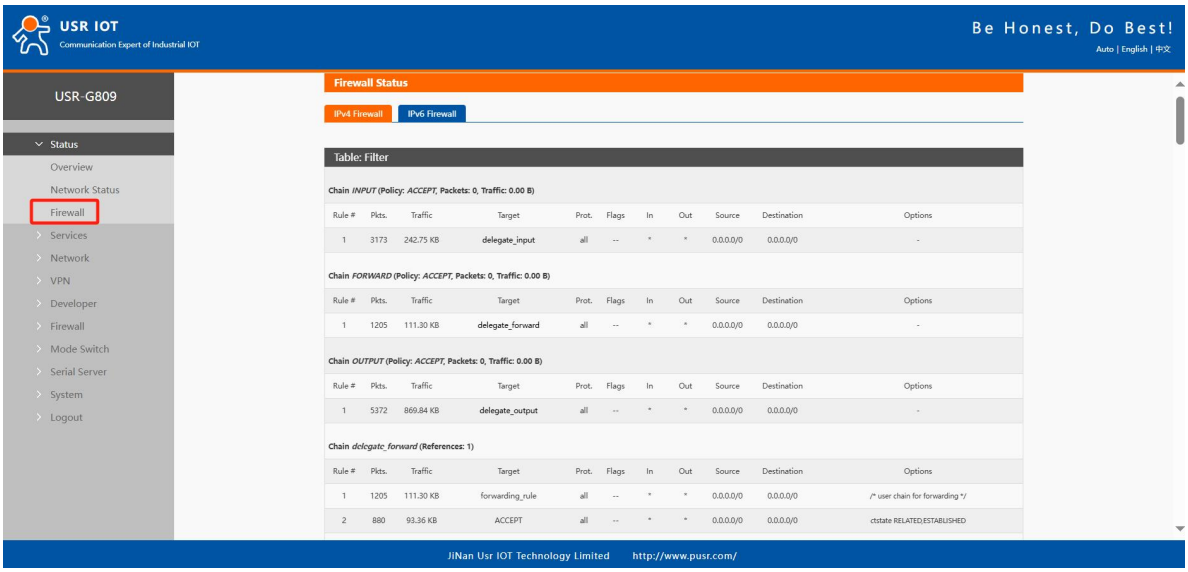


Query routing information and ARP tables here.



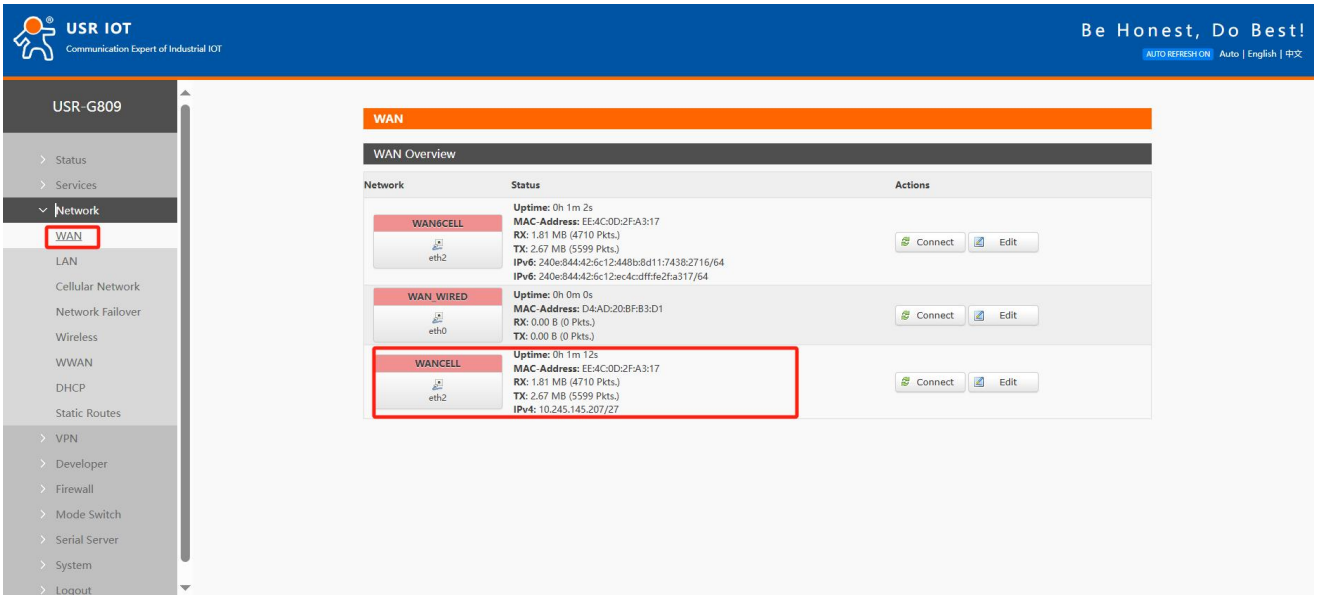
View firewall list information here.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



3.1. Cellular network

This router supports a 4G communication module interfacefor accessing externalnetworks.



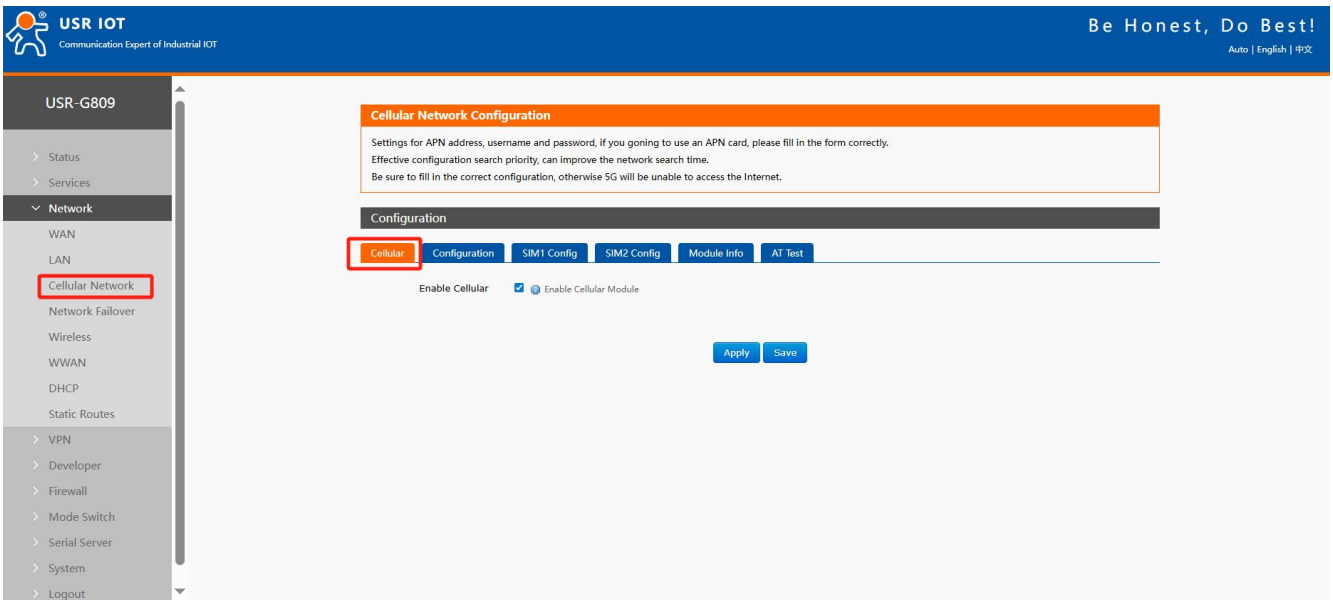
state table

serial number	name	implication
1	performance period	Running time of 4G network card startup of this interface
2	Mac address	MAC address of this NIC interface
3	receive/transmit	Statistics of the accumulated receiving and sending data of this NIC

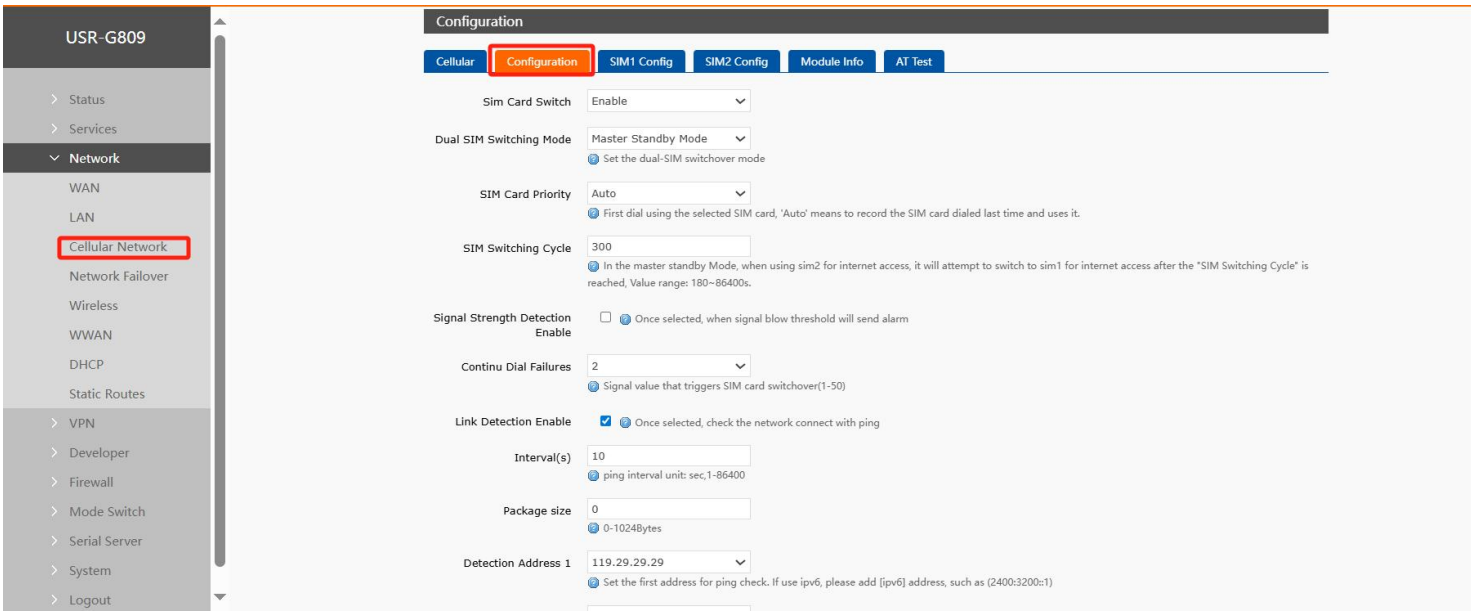
Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

3.1.1. Enabled

Turning off this feature will stop cellular service and the router will not be able to access the network through cellular.



3.1.2. Configuration

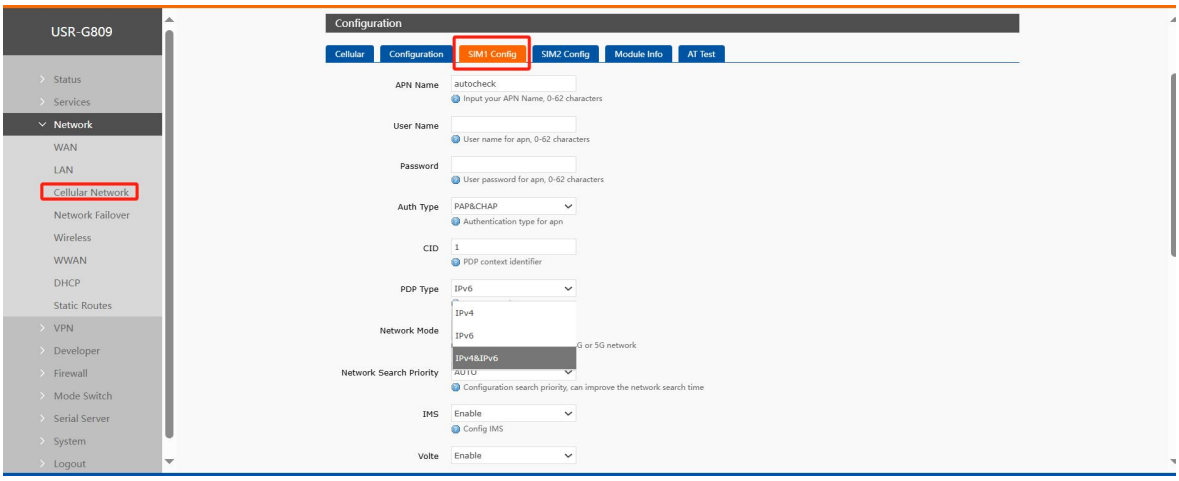


Configuration Parameter Table

name of parameter	function	default
SIM card switching	Enable: Enable dual card automatic switching function Close: Lock one of the SIM cards	enabled
Dual card switching mode	Main/standby card mode: if SIM1is the main card,SIM2 will be automatically switched to network when SIM1 is abnormal, and SIM1 will be automatically switched to network when SIM1 returns to normal.	Master/Backup Card Mode
SIM card priority	Automatic: means to record the SIM card used for the last dial and use it SIM1: SIM1 is the master card SIM2: SIM2 is the main card	voluntarily
Cheka cycle	Main/standby card mode parameter. When the standby card is currently connected to the network, it will detect whether the main card is restored to normal after reaching the threshold time set here (the network will be disconnected every time the cellular network is detected).If the main card is restored, it will automatically switch to the main card for network access. Unit: second	300
Fixed SIM card	Lock SIM1 or SIM2 into the network	SIM1
signal strength monitor switch	Check: alarm according to set signal threshold value	not checked
sounding interval	Intervals for querying signal strength are in units: s	10
trigger threshold	An alarm will be given when ever CSQ(converted to dBm) is queried for the first time below this value. If CSQ (converted to dBm) is queried continuously below this value, an alarm will be given only once. Unit: dBm	-100
Number of consecutive dialing failures	Number of consecutive dialing failures that trigger SIM card switching	2
Link Probe Enable	Check: Enable SIM card Ping detection function Unchecked: Disable SIM Ping detection	check
data break	Ping detection interval time in seconds	10
Ping packet size	Set the ping probe packet size. The smaller the packet size, the less traffic it consumes.	0
detection times	Number of ping failures	10
Probe Address 1	There are 3 Ping detection addresses in total, one of which can ping the general rule that the link is normal.IP/domain name	8.8.8.8
Probe Address 2	There are 3 Ping detection addresses in total, one of which can ping the general rule that the link is normal	2001:4860:4860::8888
Probe Address 3	There are 3 Ping detection addresses in total, one of which can ping the general rule that the link is normal	empty
recovery action	Optional: None/Redial/Restart Module/Restart Device	not have

3.1.3. SIM configuration

Set SIM1/2 card related parameters.



SIM Card Parameters Table

name of parameter	describe	default
APN name	If SIM card needs to fill in APN address, please fill in correctly	Auto check
user name	If SIM card needs to fill in user name, please fill in correctly	empty
password	If SIM card needs to fill in password, please fill in correctly	empty
authentication mode	If SIM card needs to fill in authentication method, please fill in correctly	PAP&CHAP
CID	Set SIM card CID parameter, generally set to default value	1
PDP type	PDP network stack type: optionalIPv4/IPv6/IPv4 IPv6	IPv4&IPv6
network mode	This setting locks the net 2/3/4G Settings:Auto/2G/3G/4G	voluntarily
frequency band	Network Mode Select 4G Active Auto: Unlocked Frequency Input specified frequency band: for example, input 1 lock BAND1 band	Auto
network search priority	Configure search priority, you can search the specified network first to save search time	voluntarily
IMS	IMS is configured according to SIM card, generally set to default value.	enabled
Volte	Depending on whether the SIM card is configured to enable Volte service, it is generally set to the default value	enabled
MTU	Setting the MTU of a	empty
PIN enable	If SIM has PIN enabled, this feature needs to be enabled	not enabled
PIN code	4-8 digits Note: PIN enable item is not open, this PINcode setting is	1234

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	invalid	
EHRPD activated	3.5G network starts, generally set to the default value	close
Manual operator selection switch	Check to manually select operator	not checked
search	Start searching for operators in the current area. This process takes a long time. Please keep the page open.	not have

operator information	From the list of operators searched out, select the "operator name"of the target operat or and manually set it here.	empty
Enable operator blacklist	Add carrier names to the list that need to be disabled	not checked
Set operator blacklist	Set operator numeric name, e.g. 46601, operators added to this list are not available	empty
Manual selection of subnetmask ON/OFF	Set SIM card subnet mask manually, check Enable	not checked
configure the subnet mask	Select subnet mask	empty
Using a custom DNS server	Set up custom IPv4 DNS	empty
Use a customDNSserver(IPv6)	Set up custom IPv6 DNS	empty
Data Flow Limit (KB)	Set the monthly traffic limit threshold. Setting it to 0 means unlimited	0
Flow settlement date	After the settlement date, the used traffic is cleared and recalculated.	7
Used traffic (KByte)	Traffic used this month	0
SMS restrictions	Set the maximum number of SMS messages per month. Set it to 0 to indicate no limit.	0
SMS settlement date	After the settlement date arrives, the number of used SMS is cleared and statistics are recalculated.	8
Number of SMS used	Number of currently used SMS messages	0

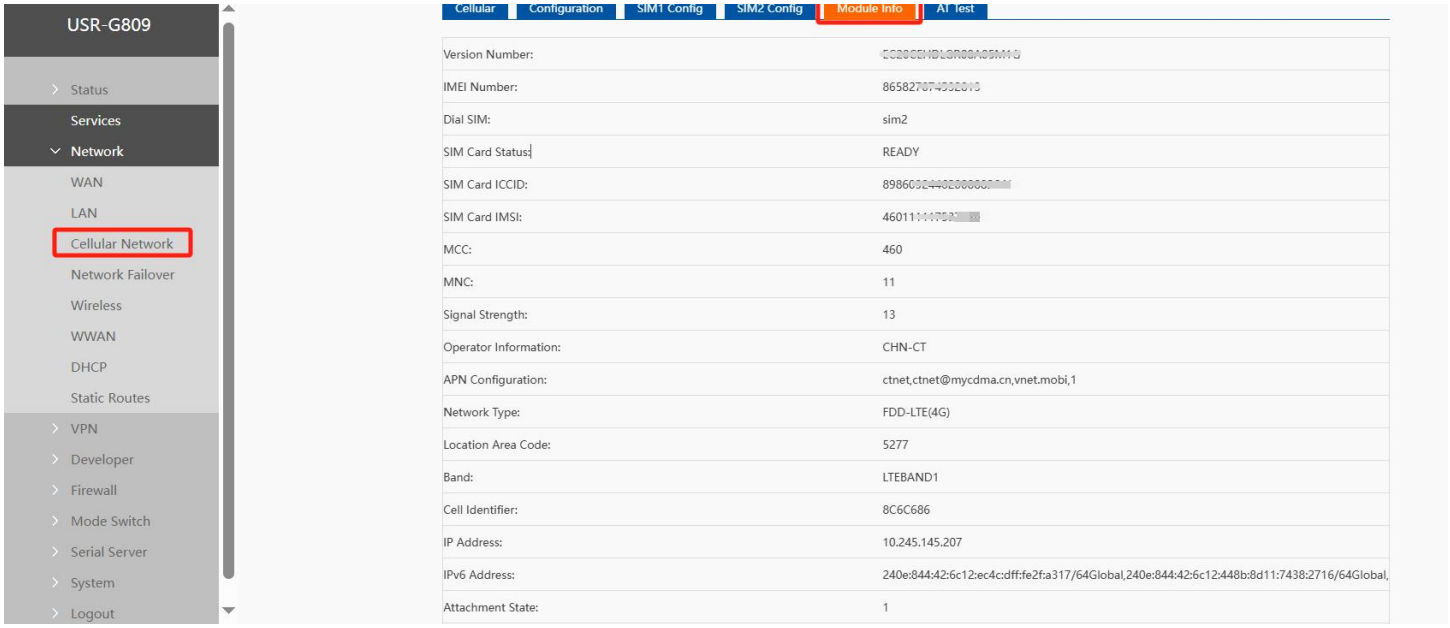
〈Attention〉

- Ordinary 4G mobile phone card Internet access, do not care about APN settings, card ready to use;
- If you use an APN network card, be sure to fill in the APN address, username and password, and authentication (consult the operator for details).

3.1.4. SIM card information display

SIM card information display will show the SIM card configuration information in detail. If there is a problem with networking, you can check the cause of the problem

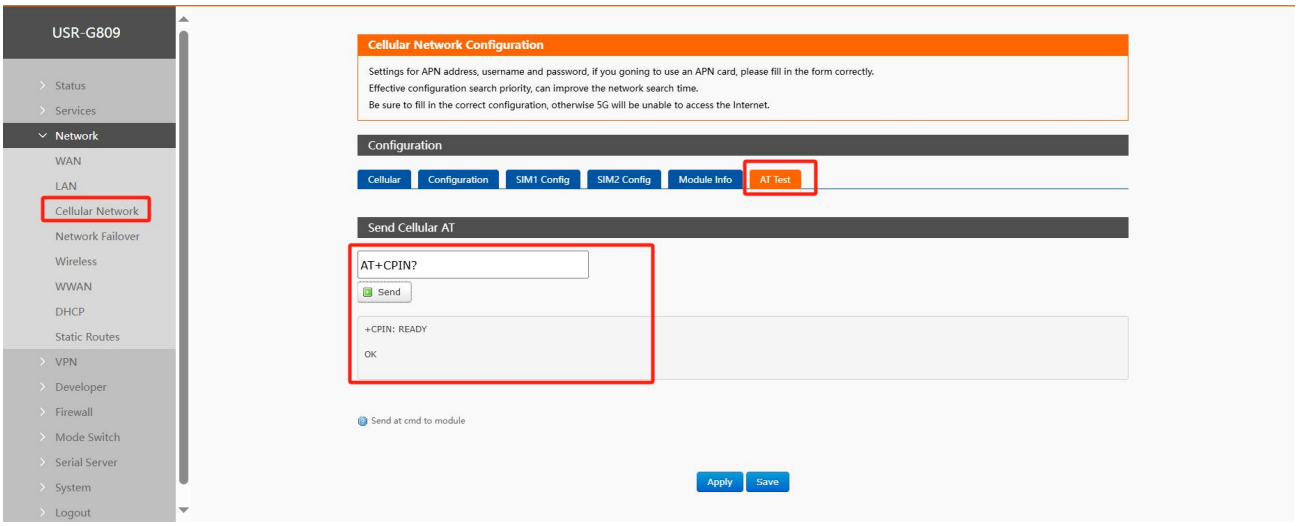
LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



3.1.5. AT command test

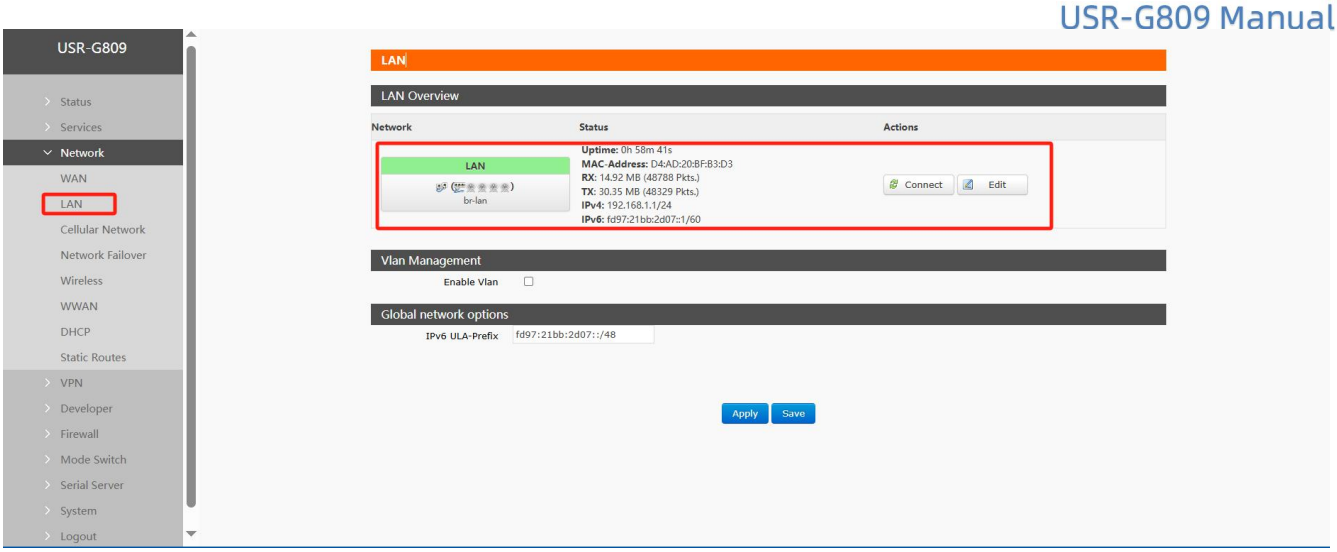
Module AT can be sent here.

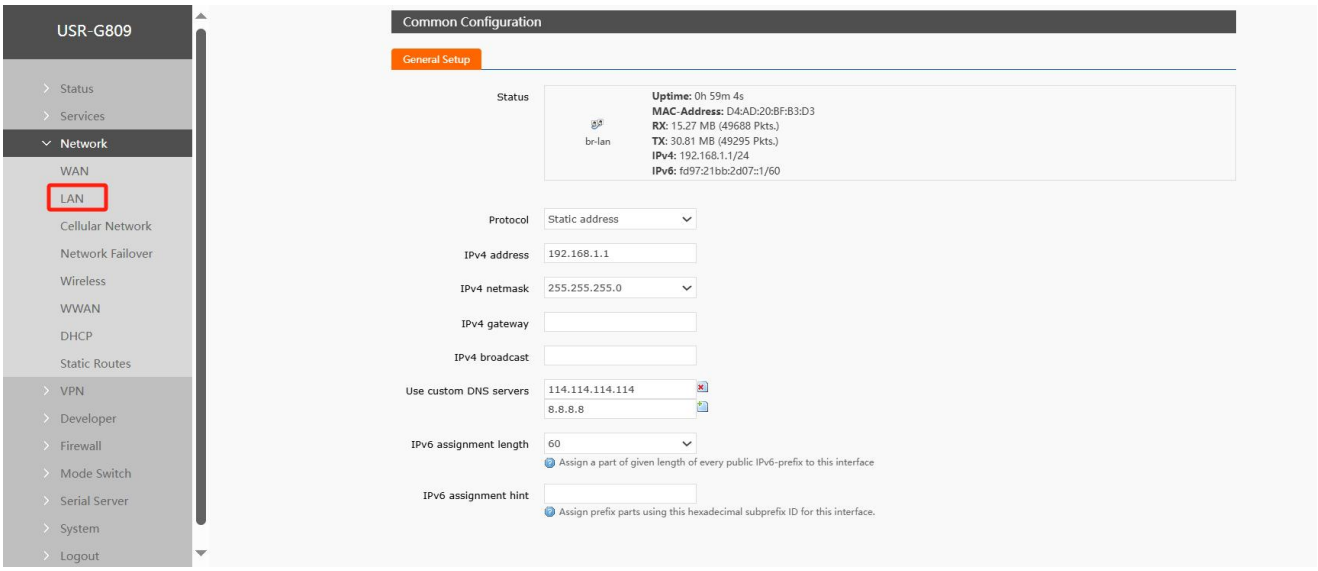
Note: If you need to send the module AT,please send it under the guidance of a technical support engineerto avoid sending wrong instructions that may cause equipment abnormalities.



3.2. LAN interface

LAN port is a local area network.





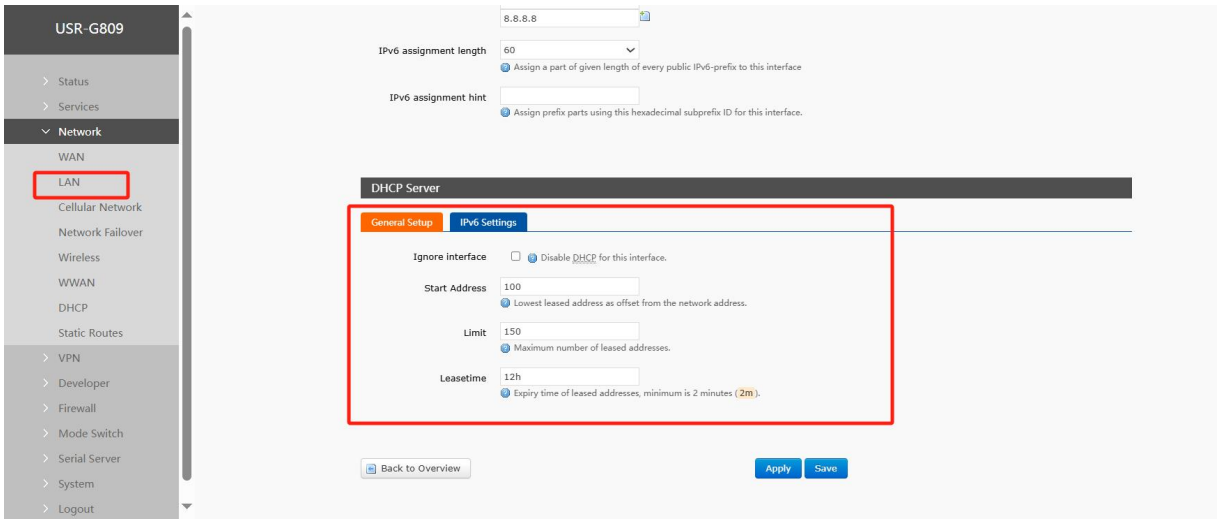
name	implication	default
IPv4 address	IP address of LAN card	192.168.1.1
subnet mask	subnet mask of the NIC	255.255.255.0
IPv4 gateway	Gateway address of LAN card, usually empty	empty
IPv4 broadcast	Broadcast address of LAN card, usually empty	empty
Using a custom DNS server	Alternative DNS server. When the DNS server sent by the superior route cannot be resolved normally,this custom DNS will be used for resolution.	empty
IPv6 allocation length	Assign a fixed-length portion to each commonIPv6 prefix, usually the default value.	60
IPv6 Allocation Reminder	Use the hex adecimal prefixID of this interface to assign the prefix part, which is generally the default value.	empty

<Description>

- Default static IP address192.168.1.1, subnet mask255.255.255.0www.example.com. This parameter can be modified,for example, static IP is modified to192.168.2.1;
- DHCP server functionis enabled by default, and devices connected to the router LAN port can automatically obtain IP addresses;
- If VLAN division is used, WIFI interface bridges to br-lan port, and WIFI obtains IP and br-lan network card on the same network segment.

3.2.1. DHCP function

DHCP Server function of LAN port is enabled by default (optionally disabled).



<Description>

- You can adjustthe DHCP pool start address, as well as address lease time;
- DHCP default assignments range from192.168.1. 100 starts;
- The default lease period is12 hours, and the unit can be set as "h"-hour or "m"-minute;
- If DHCP is turned off, subnet devices need to have the correct static IP and gateway settings to connect to the network via the router.

3.2.2. DHCP IPv6

DHCP V6 Server function settings for LAN

name	implication	default
Router Advertisement	Disable: Disables routing advertisements Server mode:RAbroadcast messages are Relay mode: relay RA data delivered by DHCP v6 Mixed mode: Use both stateless and state ful configurations, i.e. mixed mode. There are two types of simultaneous state and state	relay mode

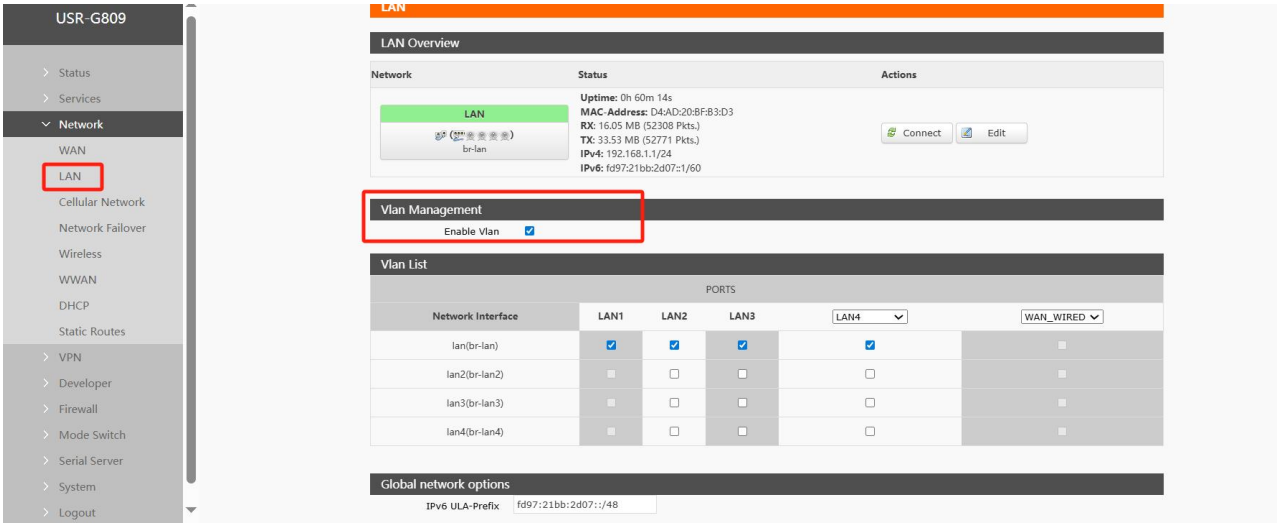
DHCPv6 Services	Disable: Disable DHCPv6 services Server mode: through the router itself as DHCPv6 server Relay mode: relay DHCPv6 server to cellular interface Mixed mode: Use both the state less and the state ful configuration at the same time, i.e. mixed mode. There are two types of simultaneous state and state	relay mode
NDP-Agent	Disable: Disable NDP proxy services Relay mode: Relay NDP(Neighbor Discovery Packet) to cellular interface Mixed mode: Allows devices to use both NDP proxy and standard NDP	relay mode
DHCPv6 mode	Stateless: Configure IPv6addresses automatically Status: DHCP Server assigned address fully enabled Stateless + stateful: devices canobtainIPv6 addresses and other network configuration information through DHCPv6 servers, andIPv6 addresses can also be automatically configured through SLAA C.	stateless + stateful
Broadcast DNS Server	Configuration will broadcast the configured IPv6 DNS server	empty
DNS domain name broadcast	Set DNS suffix search list sent to terminal, generally default value	empty

<Description>

- DHCP v6relay mode supports relay to cellular cards only.

3.2.3. VLAN configuration

This router supports VLAN segmentation and can divide multiple network ports into different network segments.

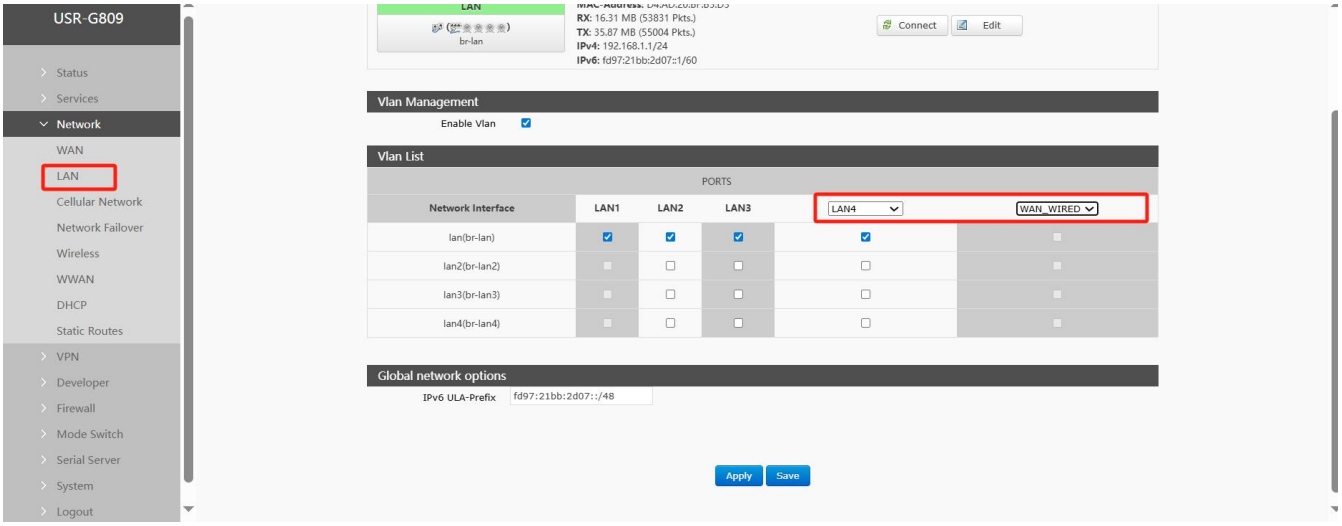


<Description>

- VLAN division is disabled by default. If enabled, LAN port IP will automatically be changed to192.168.1.1, LAN2to192.168.2.1, and so on.
- The physical interfaces are silk-screened to representWAN1/ LAN5 or WAN2/ LAN4 for WAN/LAN switching;
- The tag LANx (x=1~4) indicates that VLAN division can be performed;
- SFP1 optical port is LANport;
- SFP2 (WAN1/LAN5) optical port and WAN1/LAN5electrical port cannot be used at the same time, only one of them can be used (SFP interface/GE interface can be selected through WAN_WIRED setting);
- If VLAN division is enabled, LAN5~LAN9 physical interfaces (ifLAN5 is set to WAN,LAN5 is ignored)and WiFi are divided into br-lan networks.

3.2.4. WAN/ LAN selection

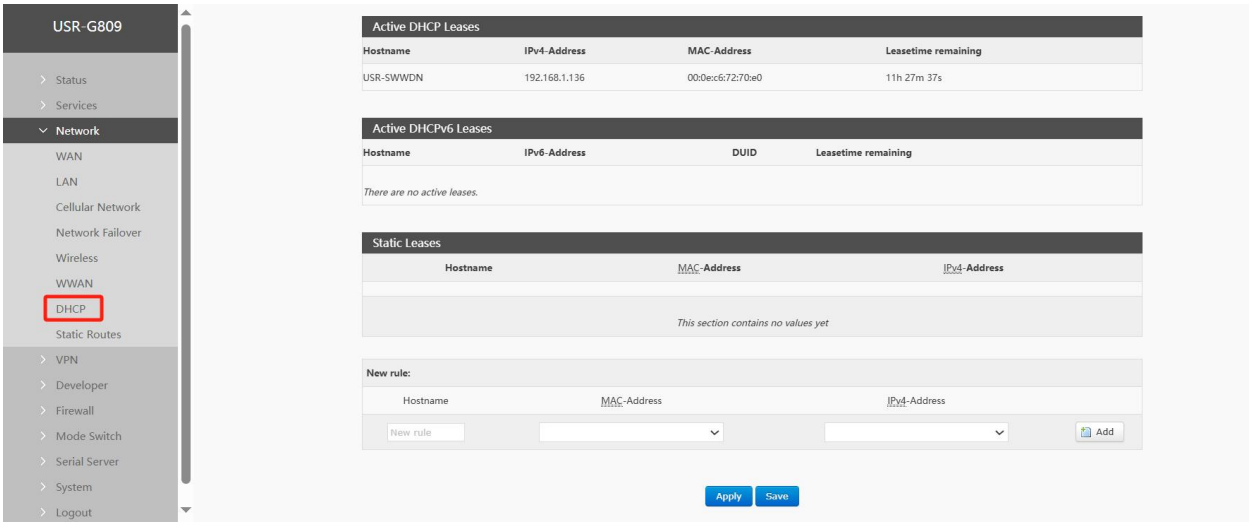
After the VLAN switch isturnedon,LAN 4can be set to WAN 2_WIR (shell screen WAN 2/LAN 4),WAN_WIRED can beset to LAN (shell screenWAN1/LAN5).



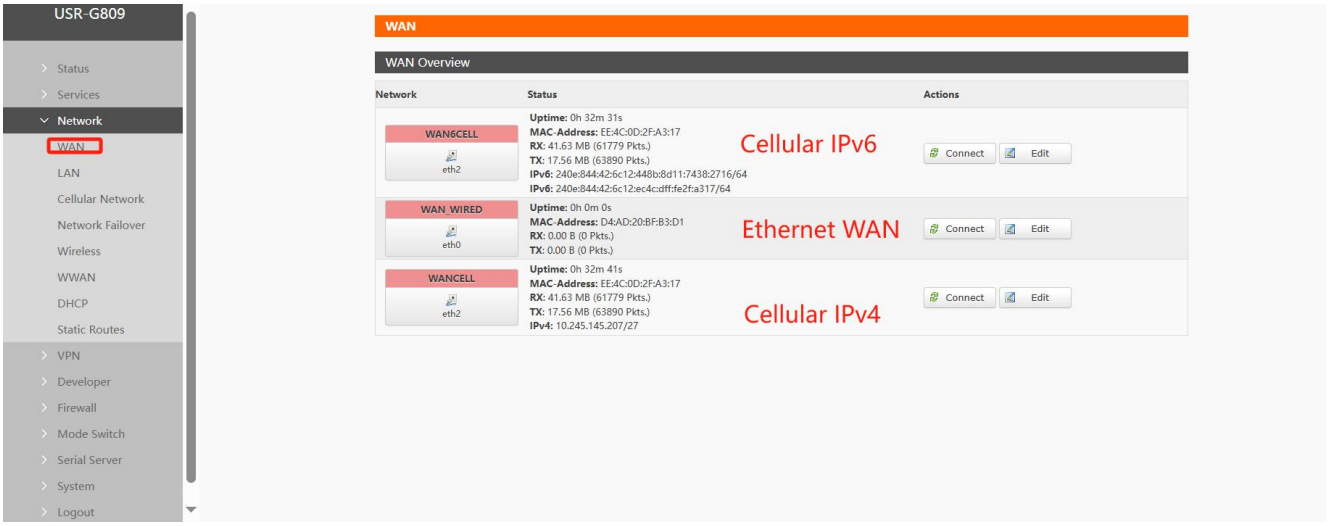
3.2.5. DHCP

Static Address Assignment: Set at Interface-DHCP. This feature is an extension of the LAN interface DHCP settings and is used to assign fixed IP addresses and host IDs to DHCP clients. Only specified hosts can connect and interfaces must be non-dynamically configured.

Use Add to add new lease entries.Host authentication using MAC-address, IPv4-address assignment address, host name assignment identifier.



3.3. WAN port

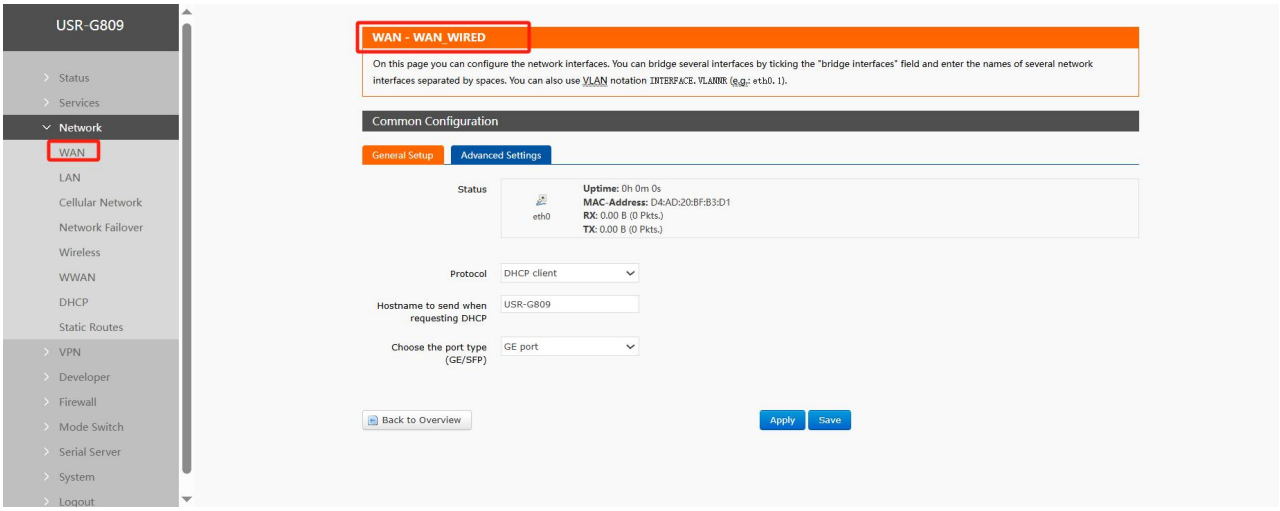


<Description>

- The default WAN1/LAN5port is WAN mode, and the WAN can beturned on at the LAN port and set to LAN for VL AN division;
- The default WAN2/LAN4port is LAN mode, and VLAN division can be set to WAN2atLAN
- WAN supports DHCP (default), static IP, PPPOE mode;
- SFP2 (WAN1/LAN5) optical port and WAN1/LAN5electrical port physical interface can not be used at the same time, only can choose one(select SFP through WAN_WIRED setting)

Optical port/GE electrical port).

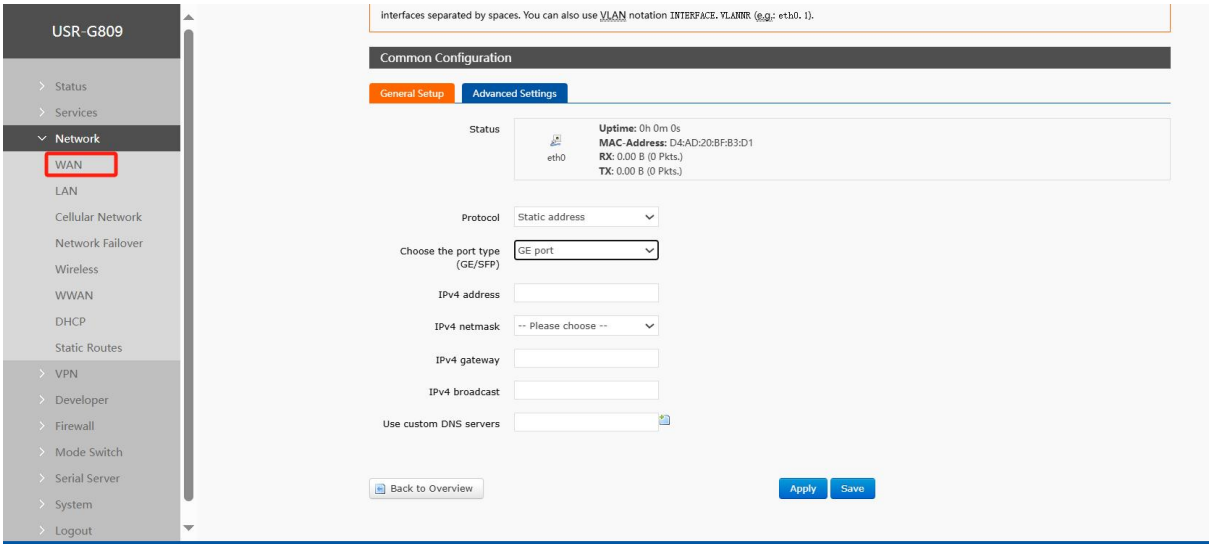
3.3.1. DHCP mode



<Description>

- The default IP acquisition method is DHCP Client;
- Support changing the host name when DHCP is;
- WAN_WIRED port type can be selected: GE port corresponds to shell silk screen WAN1/LAN5 physical port;SFP port corresponds to shell silk screen SFP2(WAN1/LAN5)physical port.

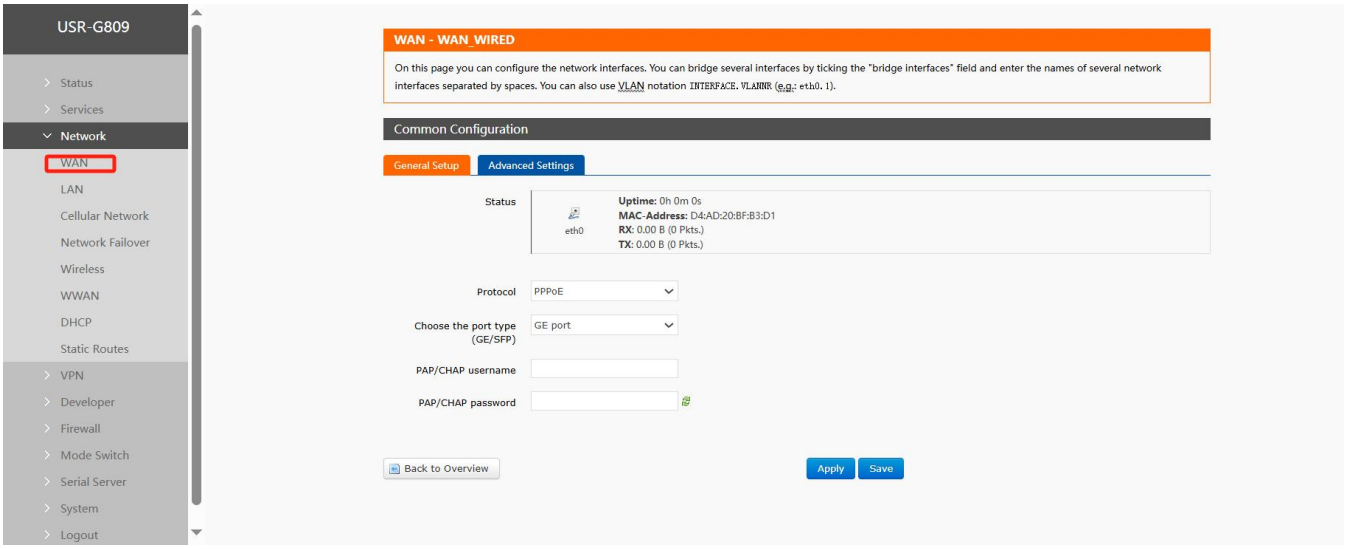
3.3.2. Static IP mode



<Description>

- Static address mode requires manual input ofIPv4 address, mask andIPv4gateway address;
- Gateway address must be reachable, otherwise the network cannot be used normally;
- General IP address and gateway in the same network segment, if there are special applications, please contact the network administrator or someone technical support;
- Note that the IP address and LAN port IP address are not in the same network segment, otherwise the network will be abnormal.

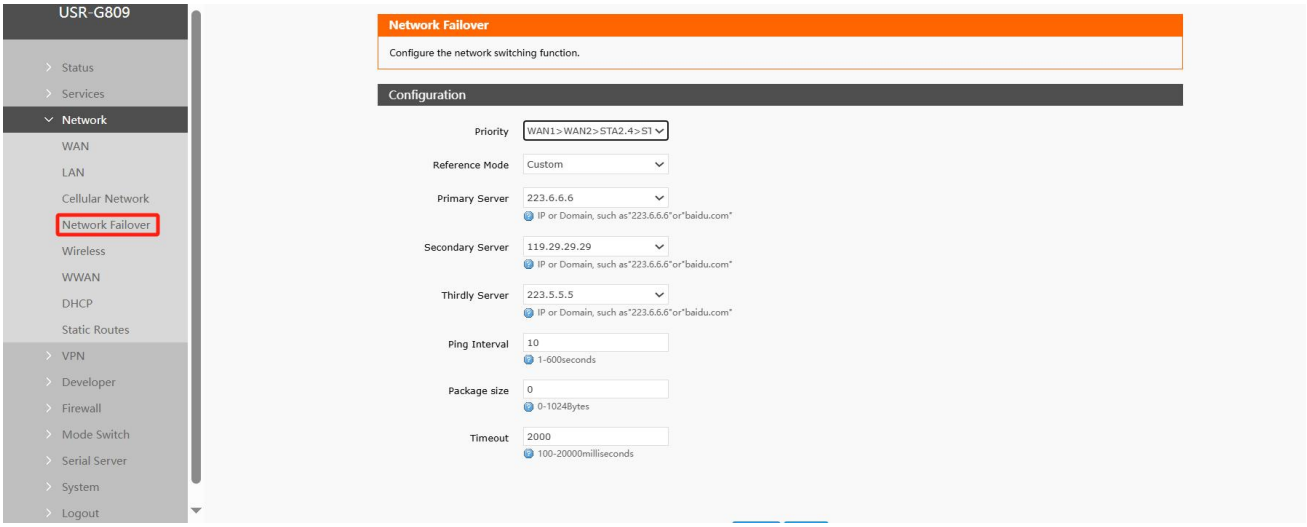
3.3.3. PPPoE mode



<Description>

- User name and password need to be obtained from the operator, fill in the corresponding position;
- Using this function is equivalent to dialing the router as a modem;
- Click Save, then click Apply to complete the configuration.

3.4. Network Failover



name	describe	default parameters
priority	Set NIC priority policy here WAN1: Corresponding to WAN/LAN port of shell silkscreen, corresponding to WAN_WIRED network card WAN2: corresponding to shell silk screen WAN/LAN4ports, corresponding to WAN2_WIRED network cardSTA2.4: corresponding to 2.4G wireless client network card STA5: Corresponding to5G wireless client NIC Cellular: CellularIPv4NIC Off: Use Last Network Priority	WAN1>WAN2>STA2.4>STA5>Cellular
reference mode	Custom: Determine network status according to custom reference address Gateway: Detect gateway address of respective NIC to determine network status	custom
Probe Address 1	IP/domain name settable	8.8.8.8
Probe Address 2	IP/domain name settable	8.26.56.26
Probe Address 3	IP/domain name settable	208.67.222.222
Detection interval (unit: s)	Set link detection interval: 1-600s	10
ping packet size (in bytes)	Packet size when detecting links: 32-1024 bytes	0
overtime	Set ping timeout time: 100-20000 unit: ms	2000

3.5. Wireless configuration

This router supports2.4G& 5.8G dual-band WiFi6 function, dual-band supports 2-way AP function.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

<Description>

- WiFi theoretical load 2.4G +5.8G: 256 units:
- Wi-Fi coverage is measured as 500m in open area bysomepeople, and indoor coverage is 50m. The signal coverage is affected by the site environment. Please measure it on site.

3.5.1. 2.4G AP1 Configuration

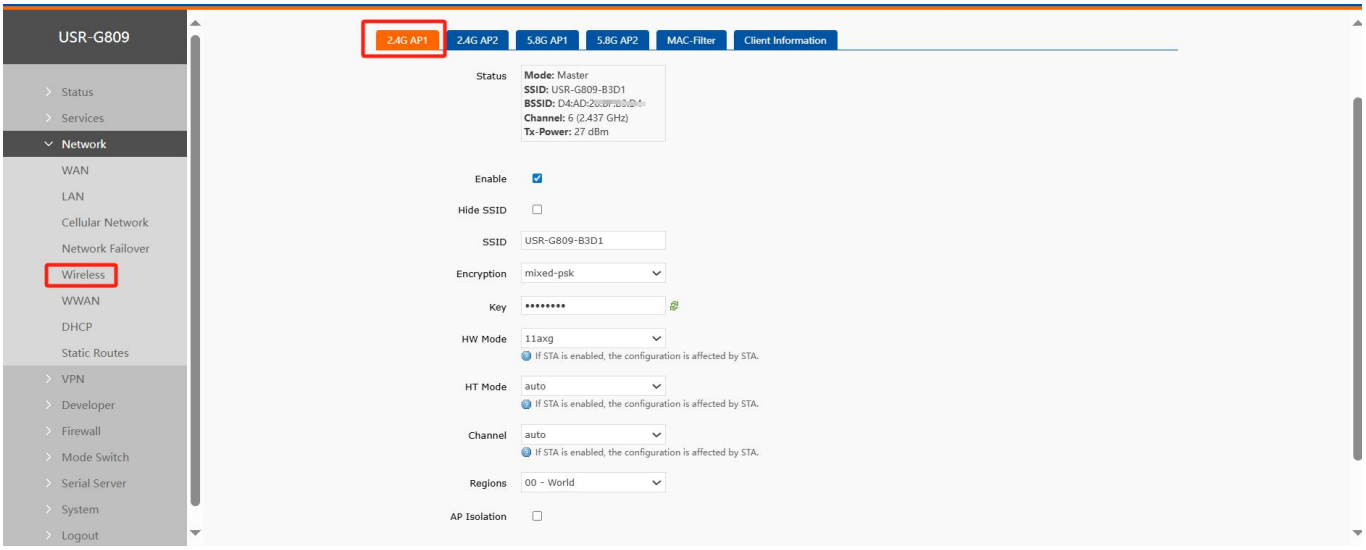


Fig. 26 Wi-Fi configuration

table 13 WiFi configuration parameters

name	describe	default
enabled	Enable 2.4G AP1 function	check
hidden SSID	Turn on this function: the terminal will not find the WiFi name, you need to manually input the correct WIFI name and password to connect, ensuring WIFI security	not checked
WiFi name	WIFI name of router, customizable XXXX of default value is the last four bits of router MAC	USR-G809-XXXX
encryption	Optional: no encryption/mixed-psk/psk/psk2/psk2+ccmp	mixed-psk
password	WIFI password, customizable	88888888
network mode	Optional:11axg/11ng/11g/11b	11axg
(information) channel	automatic, lockable channel	voluntarily
frequency bandwidth	Selectable: Auto/40MHz/20MHz	voluntarily
country or region	Select country or region	00-World
client isolation	Open client isolation connectionNo intercommunication between terminals of the same AP	not checked

3.5.2. 5.8G AP1 Configuration

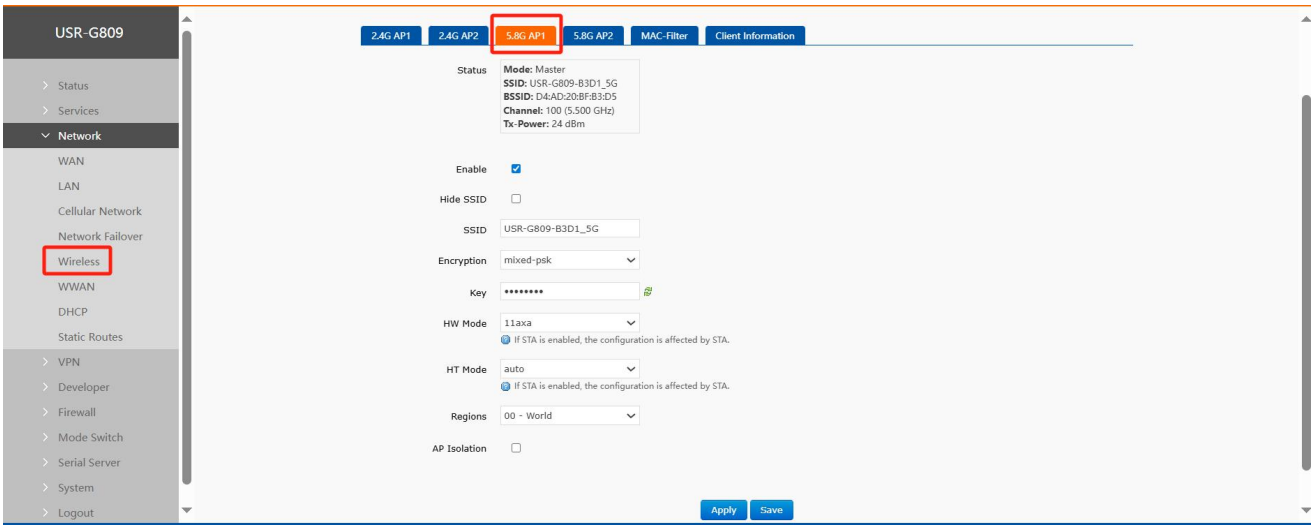


FIG. 27 Wi-Fi configuration

table 14 WiFi configuration parameters

name	describe	default
enabled	Enable 5.8G AP1 function	check
hidden SSID	Turn on this function: the terminal will not find the WiFi name, you need tomanually input the correct WIFI name and password to connect, ensuring WIFI security	not checked
WiFi name	WIFI name of router, customizable XXXX of default value is the last four bits of router MAC	USR-G809-XXXX
encryption	Optional: no encryption/mixed-psk/psk/psk2/psk2+ccmp	mixed-psk
password	WIFI password, customizable	88888888
network mode	Optional:11axa/11ac/11na/11a	11axa
(information) channel	automatic, lockable channel	voluntarily
frequency bandwidth	Selectable: Auto/40MHz/20MHz	voluntarily
country or region	Select country or region	00-World
client isolation	Open client isolation connectionNo intercommunication between terminals of the same AP	not checked

3.5.3. 2.4G AP2 Configuration

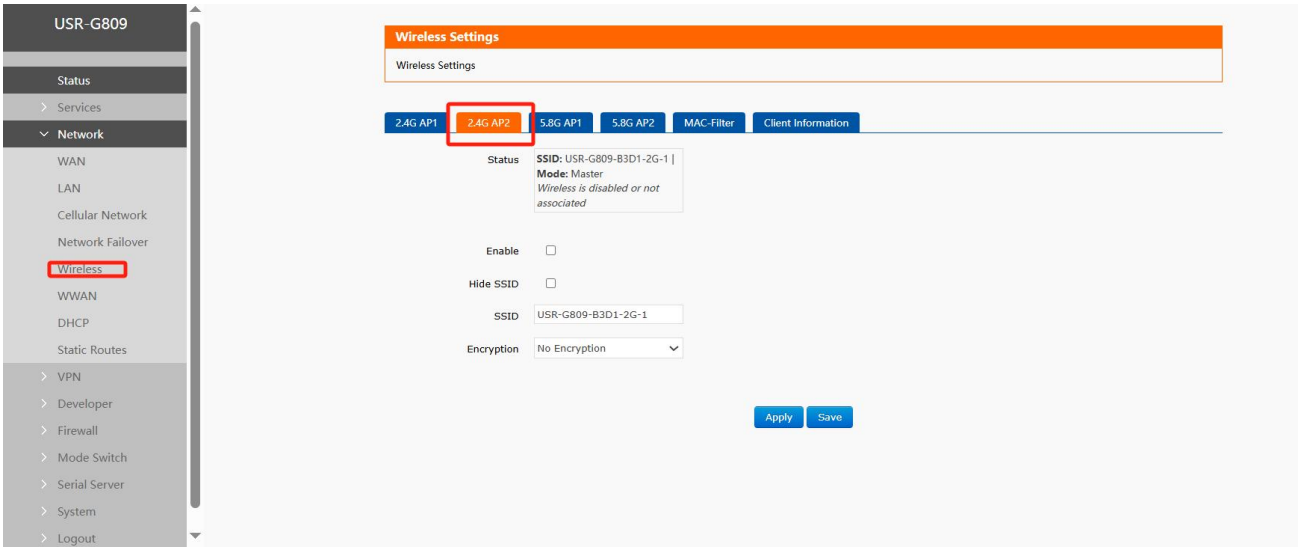


Fig. 28 Wi-Fi configuration

table 15 WiFi configuration parameters

name	describe	default
enabled	Enable 2.4G AP2 function	check
hidden SSID	Turn on this function: the terminal will not find the WiFi name, you need tomanually input the correct WIFI name and password to connect, ensuring WIFI security	not checked
WiFi name	WIFI name of router, customizable XXXX of default value is the last four bits of router MAC	USR-G809-XXXX-2G-1
encryption	Optional: No Encryption/mixed-psk/psk/psk2/psk2+ccmp	No Encryption

3.5.4. 5.8G AP2 Configuration

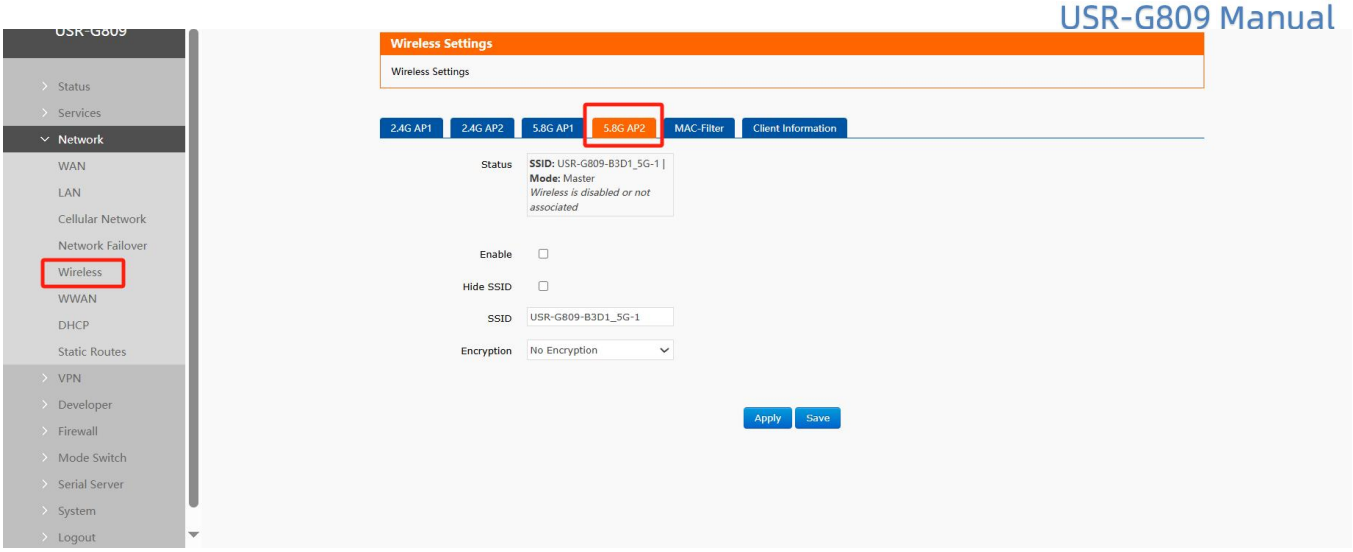


FIG. 29 Wi-Fi configuration

table 16 WiFi configuration parameters

name	describe	default
enabled	Enable 5.8G AP2 function	check
hidden SSID	Turn on this function: the terminal will not find the WiFi name, you need to manually input the correct WIFI name and password to connect, ensuring WIFI security	not checked
WiFi name	WIFI name of router, customizable XXXX of default value is the last four bits of router MAC	USR-G809-XXXX-5G-1
encryption	Optional: No Encryption/mixed-psk/psk/psk2/psk2+ccmp	No Encryption

3.5.5. MAC-Filter

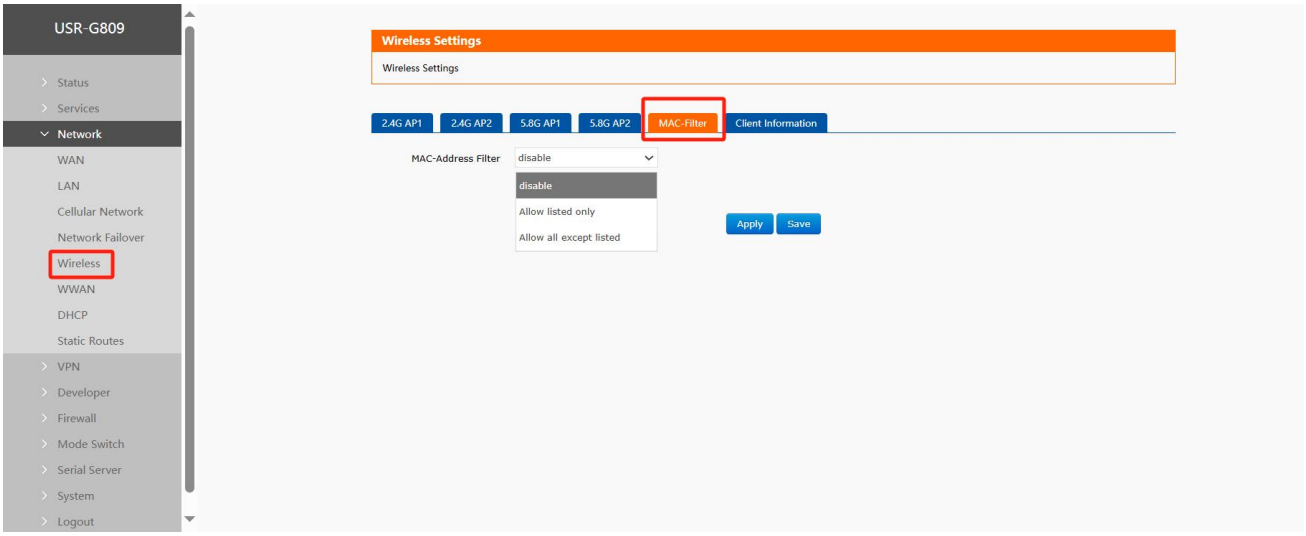


Fig. 30 Wi-Fi configuration

table 17 MAC-Filter Parameters

name	describe	default
MAC address filtering	Disabled: All terminals can connect to router WiFi Only allowed in the list: only terminals corresponding to MAC addresses in the list can connect to router WiFi Only allowed outside the list: terminals corresponding to MAC addresses in the list cannot connect to router WiFi	forbidden
MAC-List	Fill in MAC-list, maximum support 64 MAC list	empty

3.5.6. Client information

Displays a list of terminals.

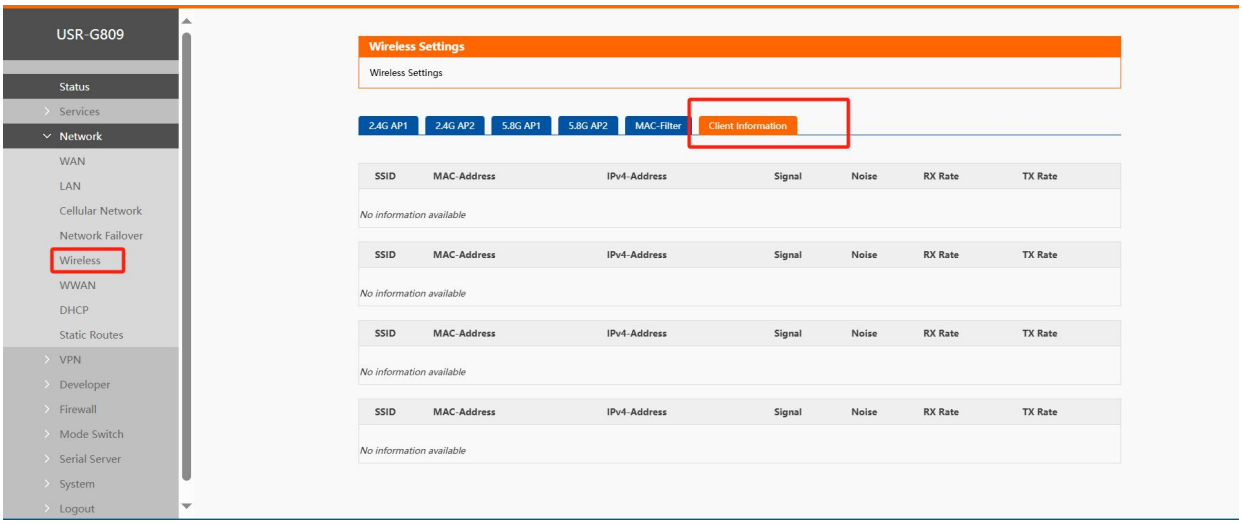


FIG. 31 terminal list

3.6. WWAN

By default, the router turns off the WIFI(wireless) client, and can turn on the WIFI client to connect to the AP on site.

3.6.1. 2.4G Settings

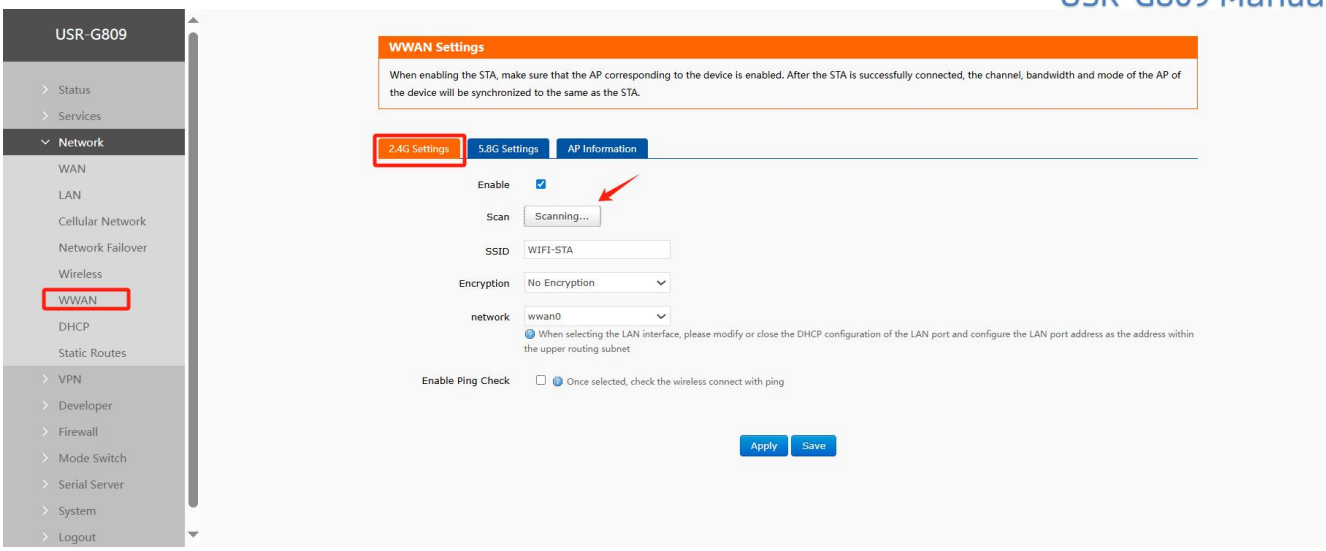


FIG. 32 Wireless Client Configuration

table 18 Wireless client parameters

Name	describe	default
enabled	Open 2.4G wireless client	not checked
search	Click Search to start searching out hot spots on the site It takes about 30 seconds to 1 minute to search for hot spots, so wait patiently.	not have
WiFi name	Hot spots can be selected by search or manually	WIFI-STA
encryption	Settable: no encryption/mixed-psk	no encryption
password	Enter the correct AP password	empty
network	Can be set: wwan0/lan Normal use STA function select wwan0ifyou need to use WIFI bridge mode please select lan	wwan0
Forcibly update LAN IP address	Check this functionto restart LAN when LAN (bridge mode) is	check
Enable Ping detection	If checked, enable the detection function to be kept active. If the detection address is notavailable, try to connectto wireless again.	not checked
reference address	Optional: Gateway/Designated Address	gateway
Ping Address	STA detection address, note that you need to set STA ping address	empty

3.6.2. 5.8G Settings

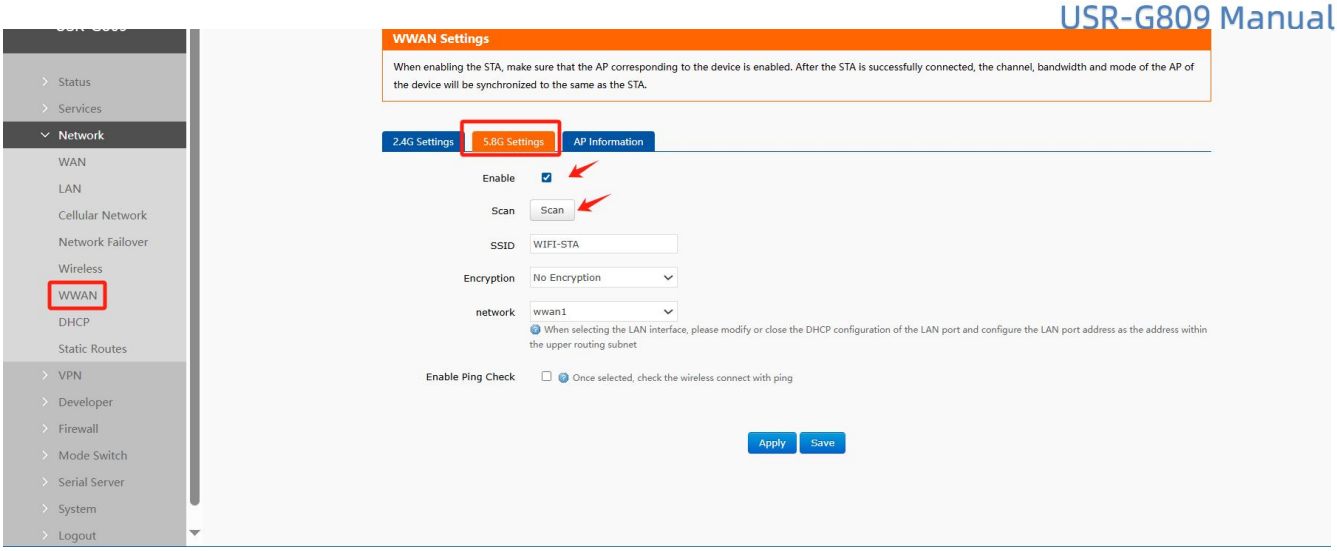


FIG. 33 Wireless Client Configuration

table 19 Wireless client parameters

name	describe	default
enabled	Open 5.8G wireless client	not checked
search	Click Search to start searching out hot spots on the site It takes about 30 seconds to 1 minute to search for hot spots, so wait patiently.	not have

WiFi name	Hot spots can be selected by search or manually	WIFI-STA
encryption	Settable: no encryption/mixed-psk	no encryption
password	Enter the correct AP password	empty
network	Can be set: wwan0/lan Normal use STA function select wwan0ifyou need to use WIFI bridge mode please select lan	wwan0
Forcibly update LAN IP address	Check this function to restart LAN when LAN (bridge mode) is	check
Enable Ping detection	If checked, enable the detection function to be kept active. If the detection address is not available, try to connect to wireless again.	not checked
reference address	Optional: Gateway/Designated Address	gateway
Ping Address	STA detection address, note that you need to set STA ping address	empty

<Description>

- 5.8G wireless client function needs to be enabled when 5.8G AP is enabled.

3.6.3. AP information

You can check whether the router is connected to the AP on the hot spot information interface.

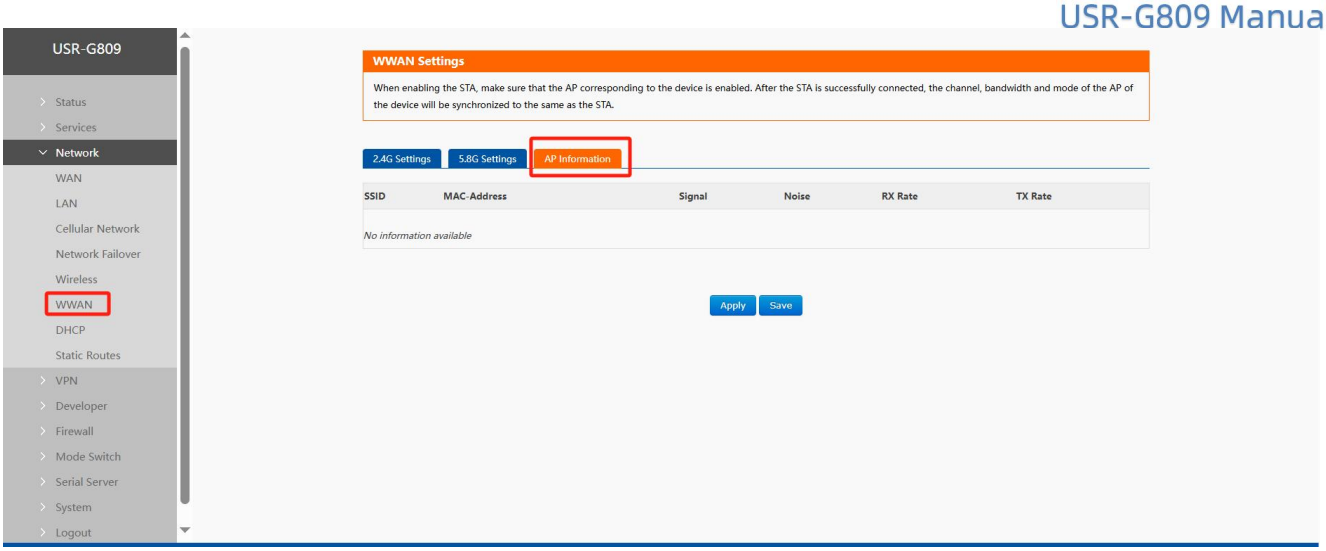


FIG. 34 Connect AP Info Page

<Description>

- When LAN is selected by the network, it is set to bridge mode, and the upper AP assigns IP to the terminal under the router.
- Set bridge mode, please note that DHCP needs to be turned off for LAN port.

3.7. Static routing

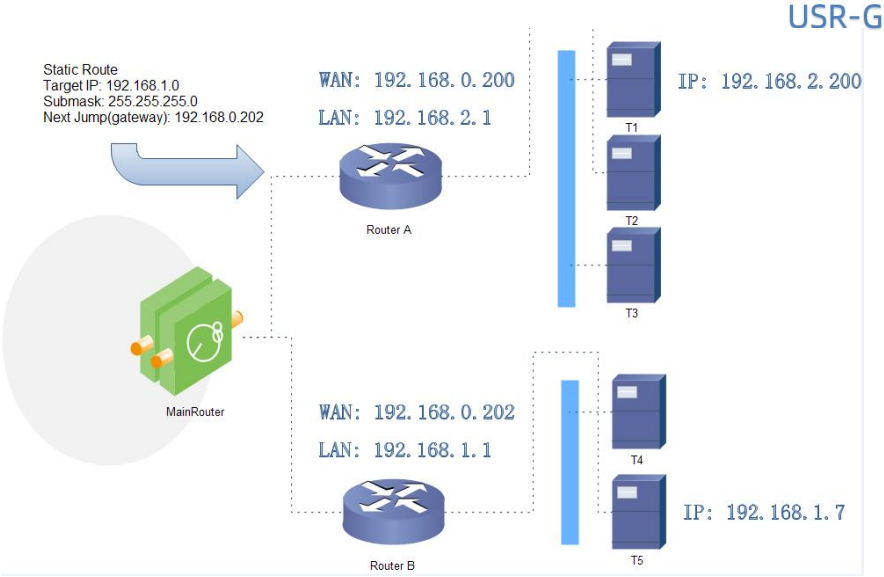
Static routes have the following parameters. The default static route can be added up to 20.

Tab 1 Static routing parameter table

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

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

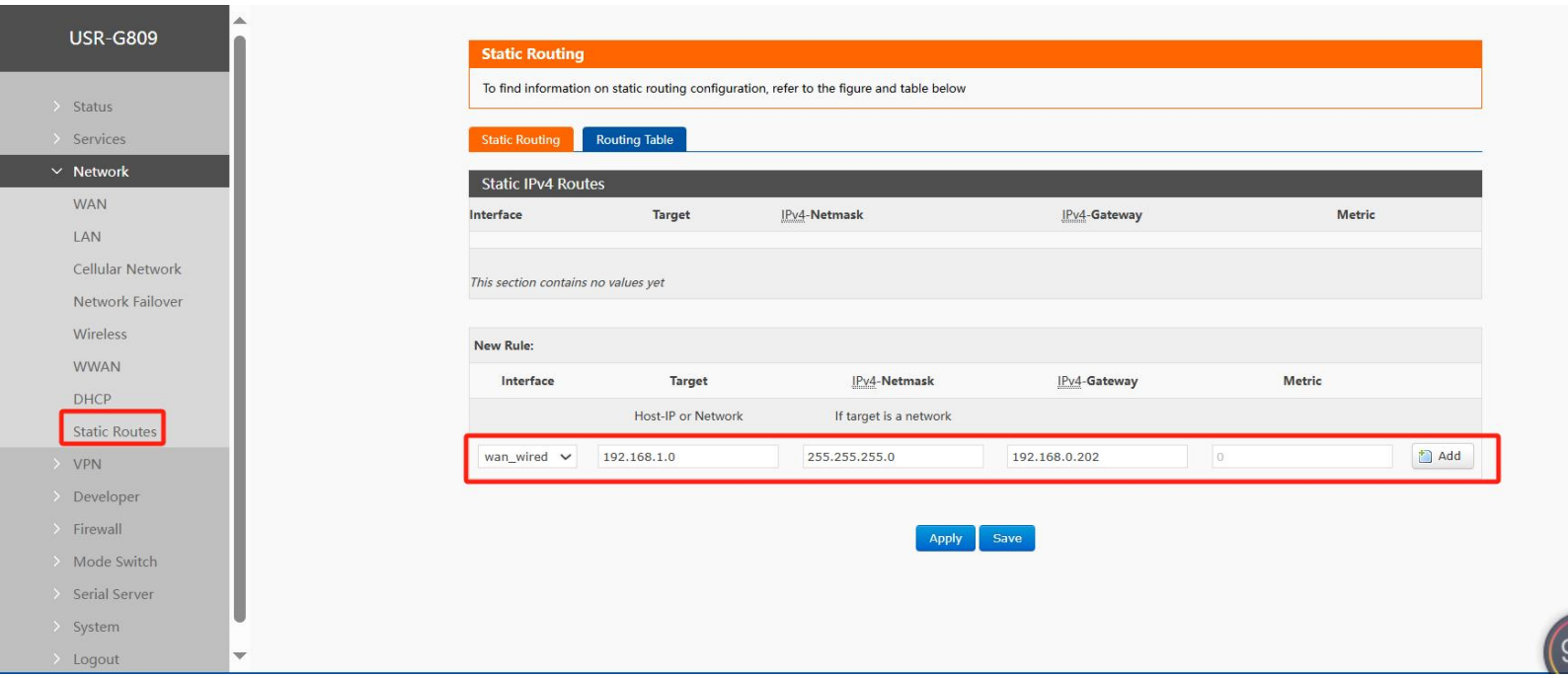
Test example: Test environment, two peer routers A and B, as shown in the figure below.



Pic 1 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 2 Route table add page

4. Service function

4.1. 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.

4.1.1. 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:

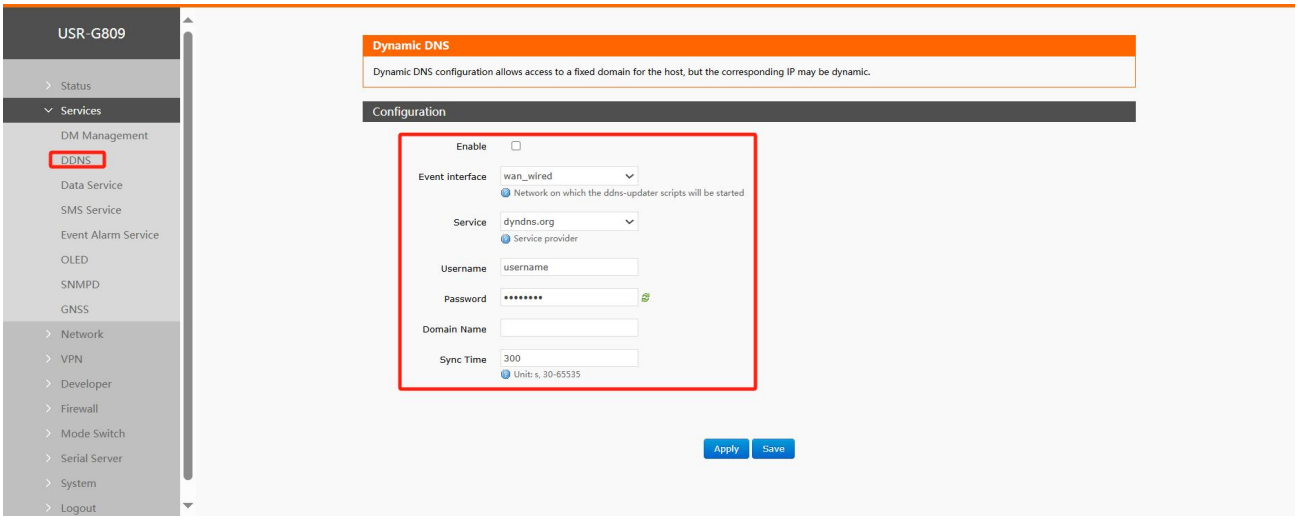


FIG. 39 DDNS Settings Page

table 22 List of DDNS

function	content	default
open	Check Enable DDNS function	not checked
effective interface	WAN port selection based on demand	wan_wired
ISP internet	Please fill in the DDNS service address	dyndns.org
user name	Peanut shell account name	username
password	peanut shell code	password
domain name	Domain name requested by DDNS	empty
Synchronization time (s)	Time interval to detect	300

4.1.2. DDNS takes effect

Verify that the DDNS settings are in effect below.First, let's look at the IP address of your network.

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



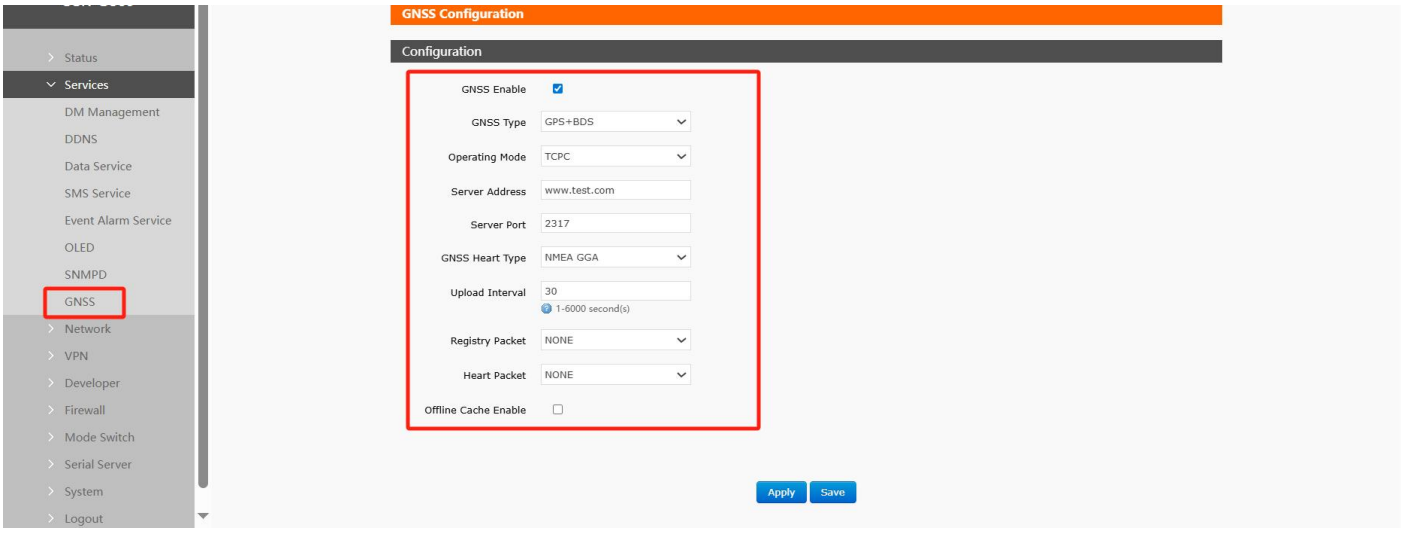
4.1.3. functional characteristics

- Please fill in the parameters strictly according to the form description, service/URL,domain name, username password, interface and other parameters to ensure accuracy;
- Even as a router under a subnet, this feature can also enable dynamic domain names to take effect;
- DDNS+ port mapping enables remote access to the router intranet;
- If the router is located in a network that is not assigned to an independent public IP, this feature cannot be used.

4.2. GNSS

4.2.1. Report Private Cloud

The router positioning data is regularly reported to the private cloud platform for analysis.



name	describe	default parameters
GNSS enabled	Check: Turn on GNSS Unchecked: GNSS OFF	checked by
fix type	GPS+BDS; GPS;	GPS+BDS

	BDS;	
work pattern	Optional: TCPC/TCPS/UDPC/UDPS	TCPC
server address	Target server address	www.test.com
server port	Destination Server Port	2317
Location packet type	Select bit raw data type: NMEA GGA/NMEARMC	NMEA GGA
reporting interval	Location data reporting interval unit: s	30
Registration packet	Optional: NONE/Custom/SN/ICCID/MAC/IMEI/IMSI	NONE
Custom Registration Package Type	HEX: Even digits in hexadecimal ASCLL: Character	HEX
Register package data	Register package content	7777772E7573722E636E
Register package sending method	Send a registration packet once when connecting to the server/add a registration packet to the front of every packet sent to the server	Send a registration packet when connecting to the server
heartbeat packet	Optional: NONE/Custom/SN/ICCID/MAC/IMEI/IMSI	NONE
Custom heartbeat packet types	HEX: Even digits in hexadecimal ASCLL: Character	HEX
heartbeat packet data	Register package content	7777772E7573722E636E
heartbeat interval	Send heartbeat packet interval unit: seconds	30
Offline cache enabled	Check: automatically cache location data during network disconnection, and automatically report after waiting for network Unchecked: positioning data will not be cached during network disconnection	Not checked
Maximum number of offline cache entries	Set the maximum number of cached items during network outage, after which the oldest items will be deleted	3600
Offline data upload frequency	Interval between each cache data transmission to the platform after waiting for normal network access Unit: seconds	1

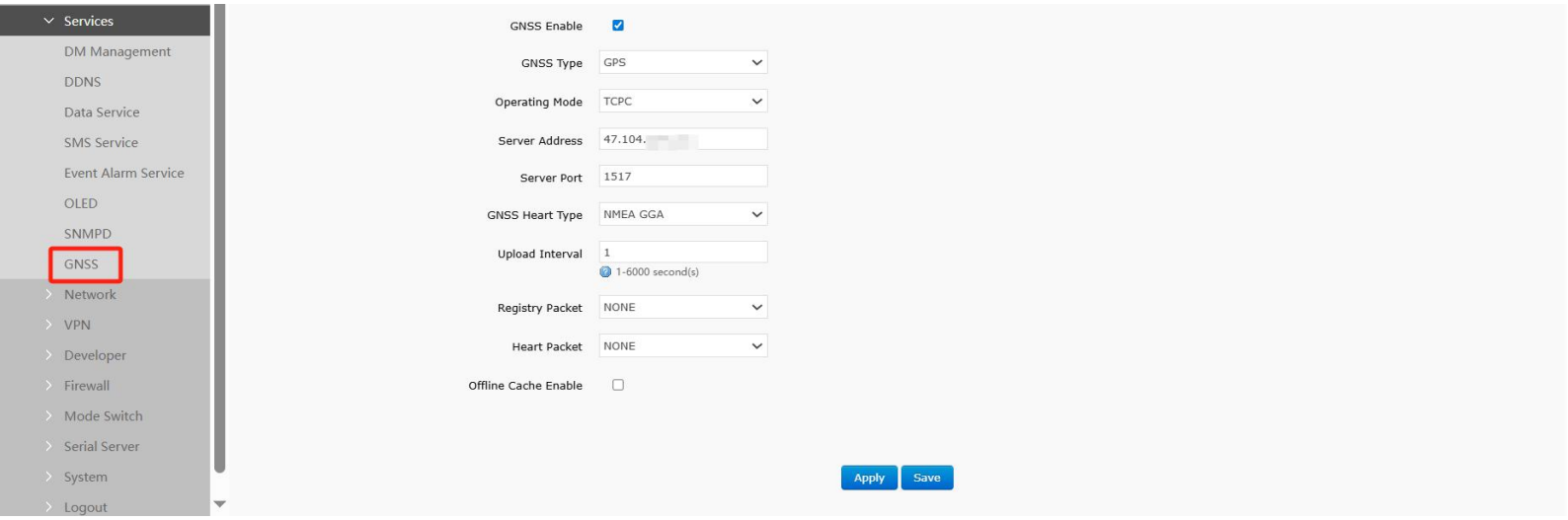


Fig. 43 GNSS settings

Report NMEA GGA data through TCPC.

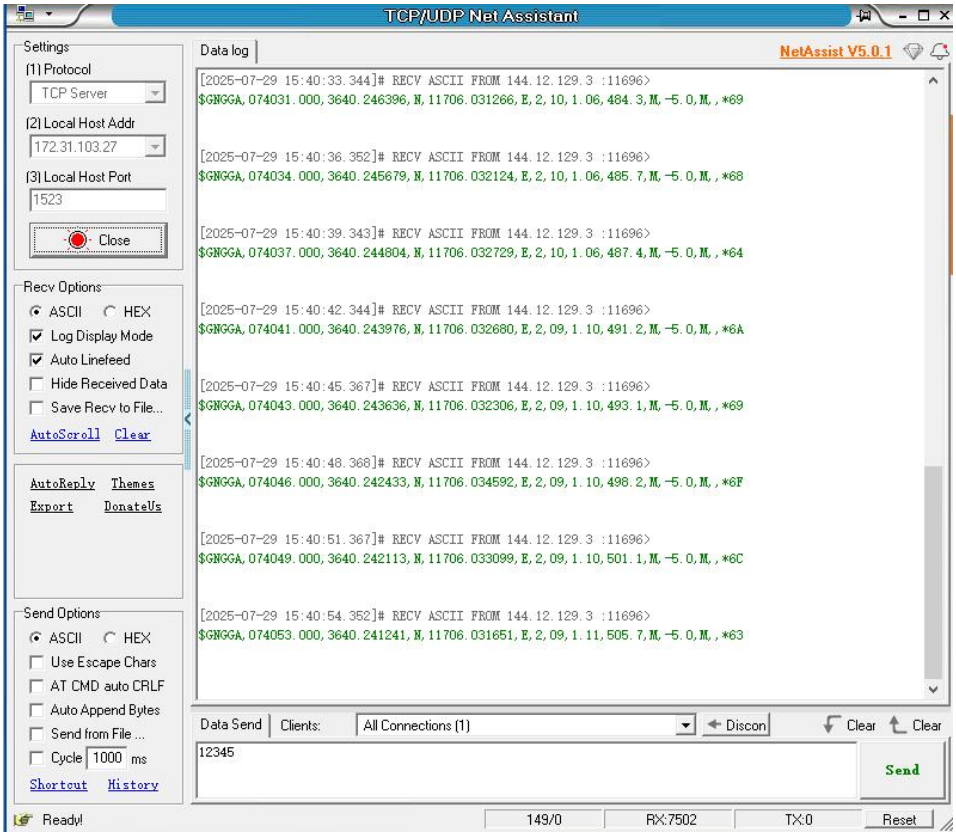


Fig. 44 GNSS data display

4.3. OLED

The router supports OLED screen, and has 4 pages of display content by default, which are system information, IO status, cellular network traffic consumption and system time. Configure LED display rules via WEB interface.

4.3.1. Generalized usage

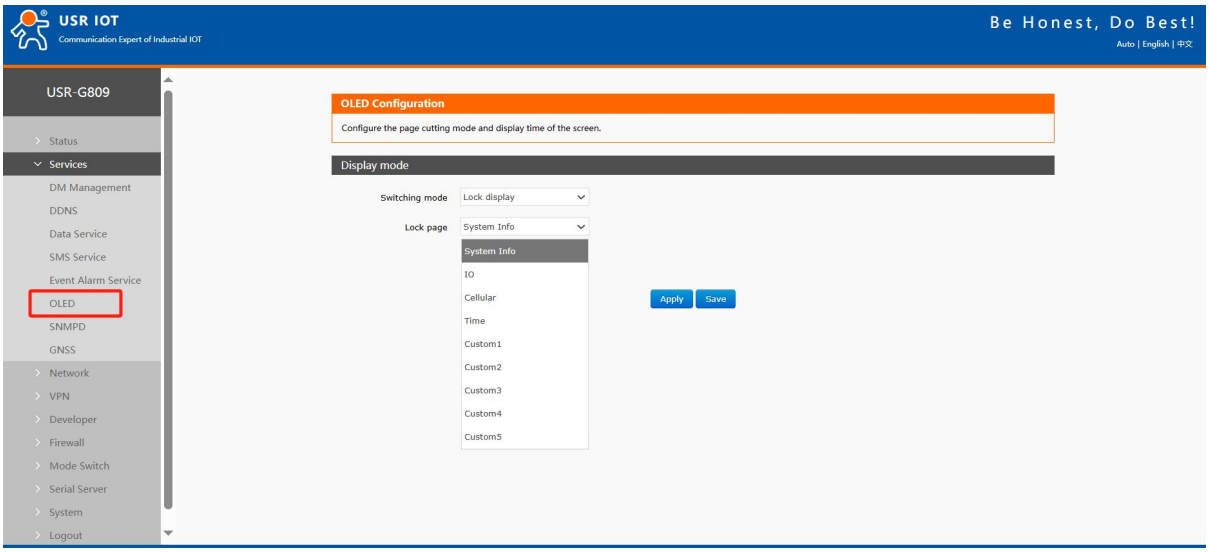


Fig. 45 OLED

table 24 configuration parameters

name	describe	default parameters
switching mode	Configure screen cut mode Scroll display: interval multi-screen content rotation displaylock display: lock a screen long display	scroll display
page turning time	Set the time interval between scrolling screen switching and page turning Unit: seconds	30
Lock page	Lock page selection: System information: Display whether WIFI is on, GNSS is on, cellular signal, etc.IO: DI, DO switch status Cellular network: Dual SIM card traffic consumption this monthTime: Display system time Custom page x: lock a certain screen information after two open	system information

<Description>

- No matter whether it is scrolling display or locking display, pressing Reset key for 1~3s will switch the screen.

4.3.2. Secondary development OLED

Currently supports shell commands and C functions to write content to specified pages and lines, displaying up to 16 characters per line, beyond which it will not be displayed. Shell script:

uci set -c /tmp custom_oled.custom1.line1='AABBC' uci set-c/tmpcustom_oled.custom1.line2='123654'uci set-c/tmpcustom_oled.custom3.line1='778899'uci set-c/tmpcustom_oled.custom3.line2='BBCCAA 'Description:

uci setcustom_oled.custom${page}.line${line}="${text}"-c/tmp${page} stands for custom page x,forexample1 stands for custom page1.

${line} represents rows, and each page can display upto 2rows.${test} represents display content.

C General function: /**

* Set custom OLED display content

*

* @param page_num Page number

* @param line_num line number

* @param content The incoming string willonly display the first16 characters

@return 0 for success, non-zerofor failure/

int set_custom_oled_ness2(int page_num, int line_num, char* content);

/**

* Delete custom OLED display content

*

* @param page_num Page number

* @param line_num line number

@return 0 for success, non-zerofor failure/

int delete_custom_oled_ness2(int page_num, int line_num);

2 Open shell script +C program example:

Step 1: Organize the package attribute file according to the package attribute file format. The controlfile is as follows:

```
Package: app                        #包名
Version: 1.1                        #包版本
Description: this is test app       #描述信息，32字符以内
PackageType: <pkg_type>             #lib | app
PackageBoot: 1|0                    #是否开机自启
NeedReboot: 1                       #有此字段，表示重启生效
RunCmd: app "param1"                #如果启动此程序不是直接运行包名，则需要指定启动命令
StopCmd: kill app                   #如果停止此程序不是直接kill包名，则需要指定停止命令
GetRunStateCmd:                     #如何获取程序是否运行的命令，如果不指定，则为ps | gre
p包名，此命令返回值有要求，如果运行中，返回"state=run"，否则返回"state=stop"
```

```
Package: usr_oledtest
Version: 1
Depends: libc, libssp, libuci, libpthread, usr_platcfg, libusr_basic
Source: package/usr_oled_test
Section: Usr Properties
Architecture: ipq
Installed-Size: 2313
DEV-Model: innerIPQ5018
Description:  usr_oledtest -- app manmagement test
```

Step 2: Create a data folder (note: the folder must be compressed to name: data.tar.gz)

The files under the data folder will be installed under the router's corresponding directory.The currentdata file includes the following files:

bin---usr_oledtest Executable binary program, compiled through the router cross-compiler tool chain after C language development is completed

etc/init.d---usr_oled_testStartup script content:

```
echo "usr_oledtest init script start ***********************************************\n" >> /dev/ttyMSM0
usr_oledtest "1" "2" "Hi OLED"
test_oled.sh
}

stop() {
ps | grep usr_oledtest | grep -v grep | awk '{print $1}' | xargs kill -s 9
ps | grep test_oled.sh | grep -v grep | awk '{print $1}' | xargs kill -s 9
}
```

sbin---test_oled.sh shell script

```
[ -z "$line" ] && line=1
[ -z "$text" ] && text="Hello World"

[ -z "$page" -o -z "$line" -o -z "$text" ] && {
    echo "param error,page=$1,line=$2,text=$3"
    exit 1
}

uci set custom_oled.custom${page}.line${line}="${text}" -c /tmp

#while true
#do
#    echo "test"
#    sleep 1
#done
```

Step 3: compress the data.tar.gz and control files into xxx.tar.gz (rename the compressed package usr_oledtest1ipq.ipk)

Step 4: Upload and install the application on the router developer.

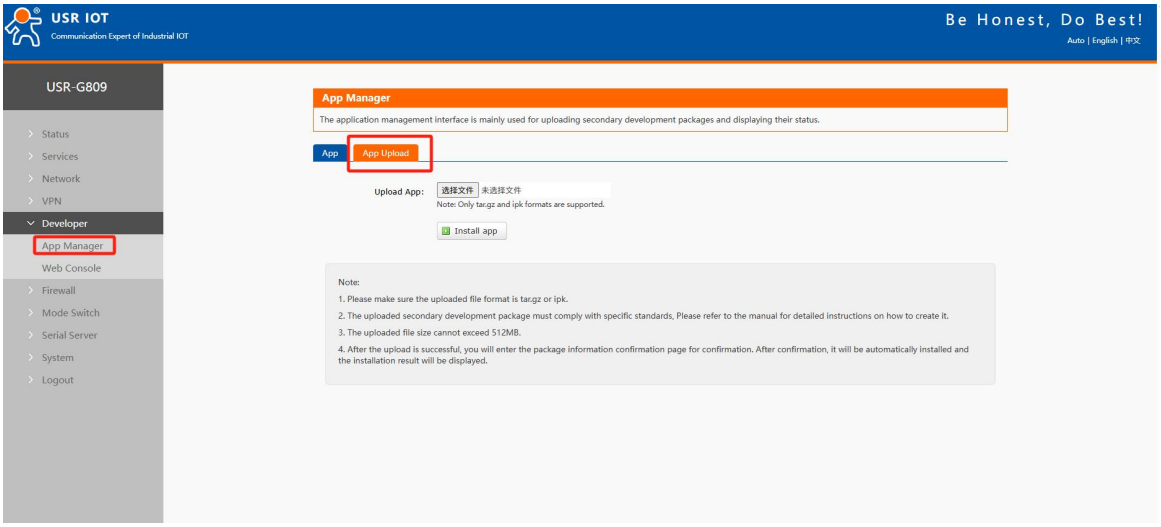


Fig. 46 install the application

After clicking Run, observe that OLED screen displays custom content on customization page 1.

The current case is displayed in the first line of the custom page 1: Hello World, and the second line shows Hi OLED.

4.4. Data monitoring services

Through data monitoring service, router system information, network information, wireless information, etc. can be transmitted to the client server for remote monitoring of router operation status.

4.4.1. Basic configuration

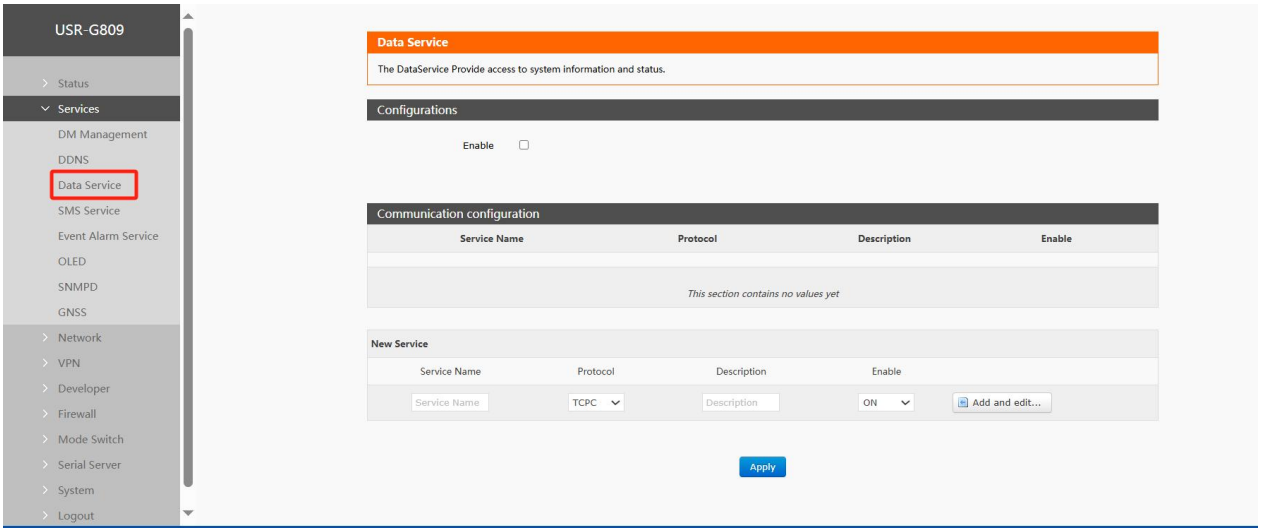


Fig. 48 Data monitoring services

table 25 configuration parameters

name	describe	default parameters
enabled	Enable: Enable data monitoring services Disable: Disable data monitoring services	forbidden
new service	Fill in the link service name	empty
agreement	TCPC/TCPS/UDPC/UDPS/HTTPD/HTTPS	TCPC
describe	Describe the link	empty
enabled	Open this link	ON

<Description>

- Up to 6 links can be established to transmit router device data to 6 server monitors simultaneously.

4.4.2. Set Link Information

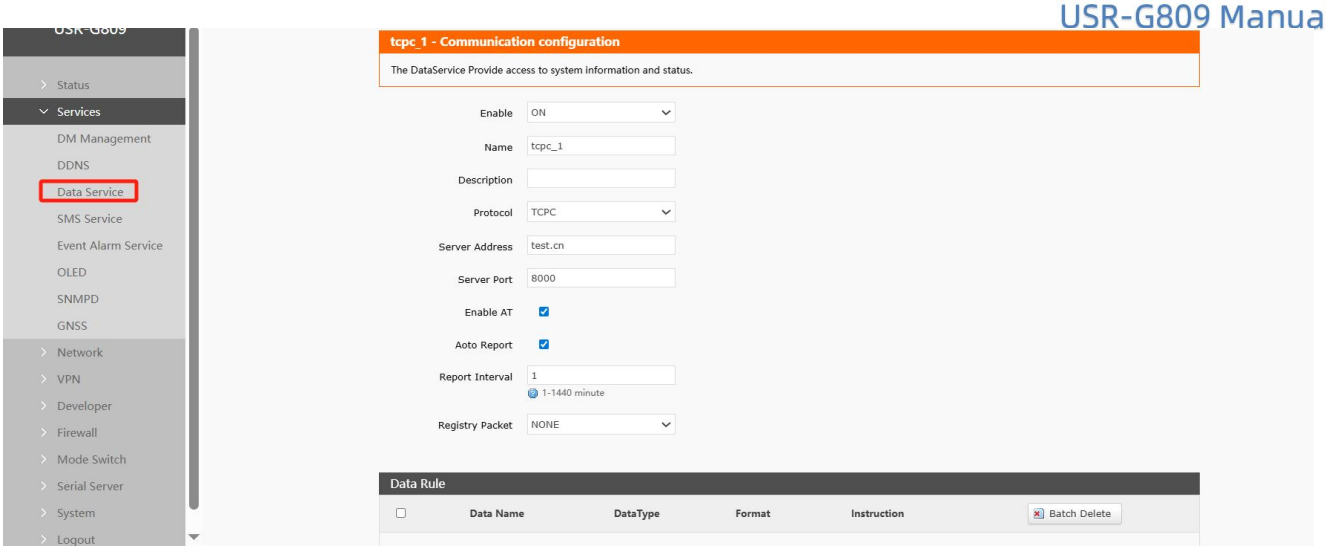


Fig. 49 link information

table 26 configuration parameters

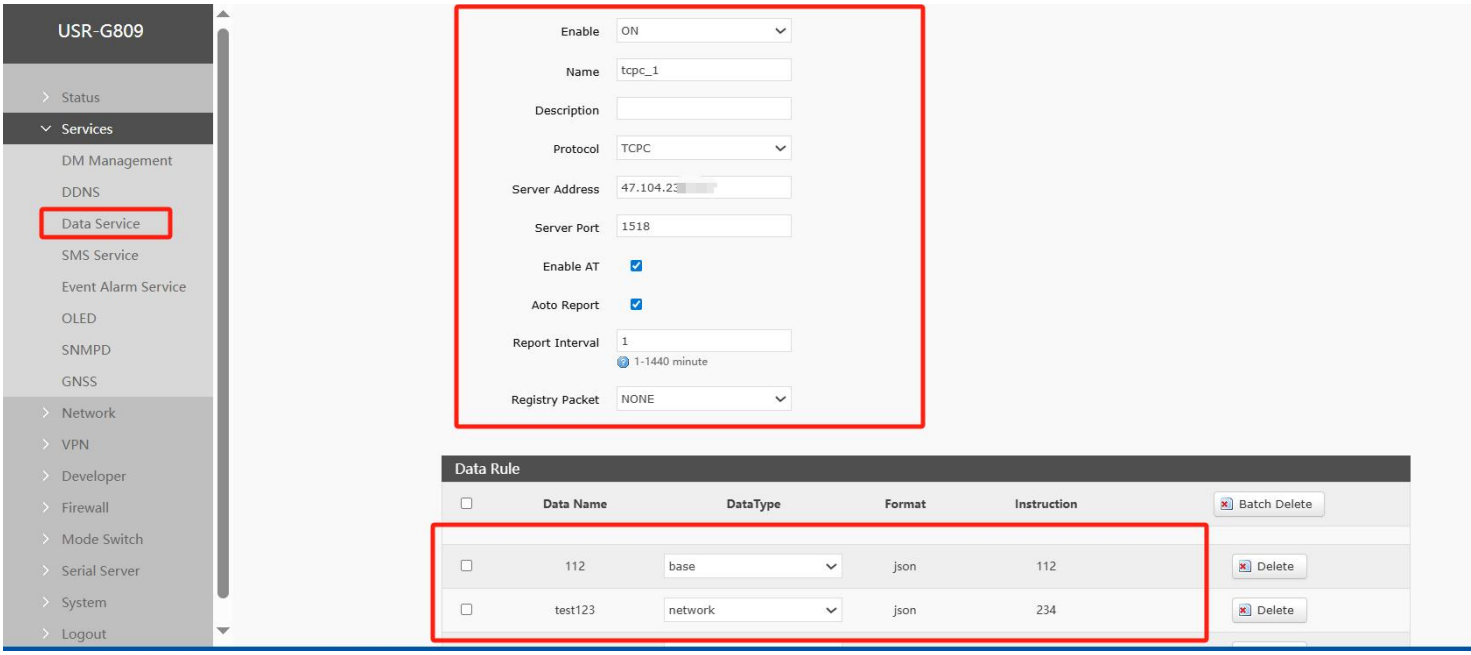
name	describe	default parameters
enabled	Enable: Open this link Disable: Disable this link	open
name	the service name of that link	Custom when creating this link
describe	Describe the link	Custom when creating this link
agreement	Select the protocol type for this link	Select when creating this link
server address	Address of target server, IP or domain name	Test.cn
server port	Destination Server Port	8000
Enable AT	You can query/set router parameters through AT commands. See AT command collection for details of AT support.	check
automatic reporting	The selected data will be reported according to the reporting frequency interval after opening	check
reporting frequency	Set interval Reporting frequency Unit: minutes	1
Registration packet	Optional: NONE/Custom/ICCID/IMEI/SN/MAC	NONE

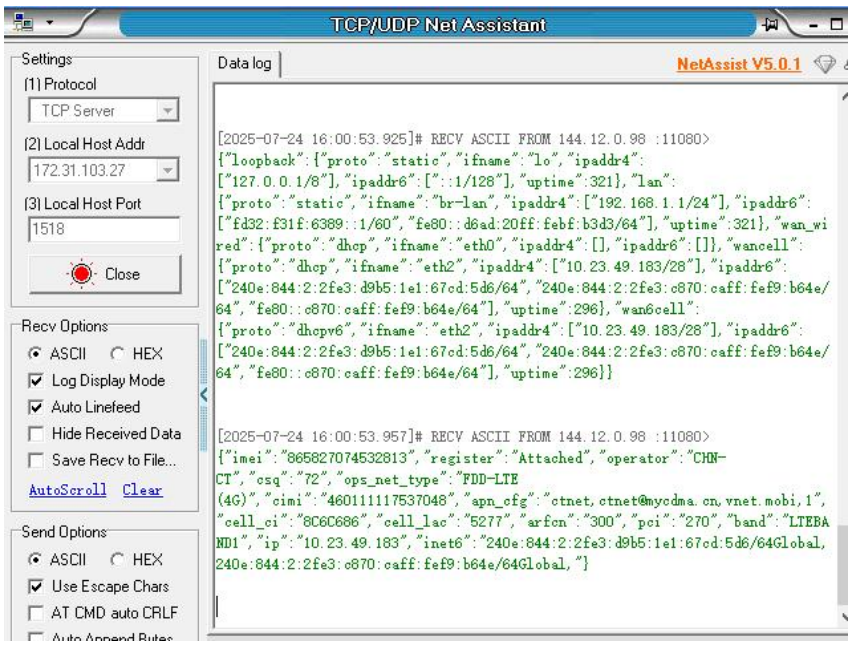
Register Package Type	Custom packet types: HEX: hexadecimal even digit ASCLL: character	HEX
Register package data	Custom registration package content	empty
Registration package sending method	Send a registration packet once when connecting to the server/add a registration packet to the front of every packet	Send a registration packet when connecting to the server
name	User-defined data rule name. If the query instruction of the data rule is blank, the name can be used as an instructionto obtain the content of the data rule in response from the server.	empty
data type	System base: including host name	
Reporting format	Jsonformat reporting	Json
query instructions	Set the query instruction of the data rule, and obtain the contentof the data rule by	empty

<Description>

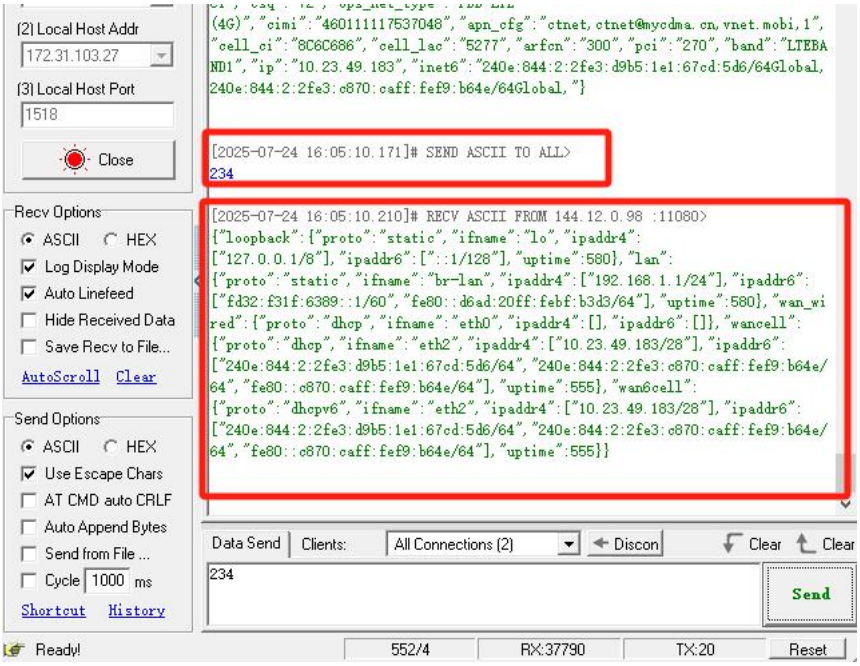
- A maximum of 6 data rules can be established per link.

4.4.3. TCPC Data Monitoring Examples





According to the query instruction set by the data rule, actively query the data in the data type, for example:234



4.5. Event alarm service

Query router exception alarm list.

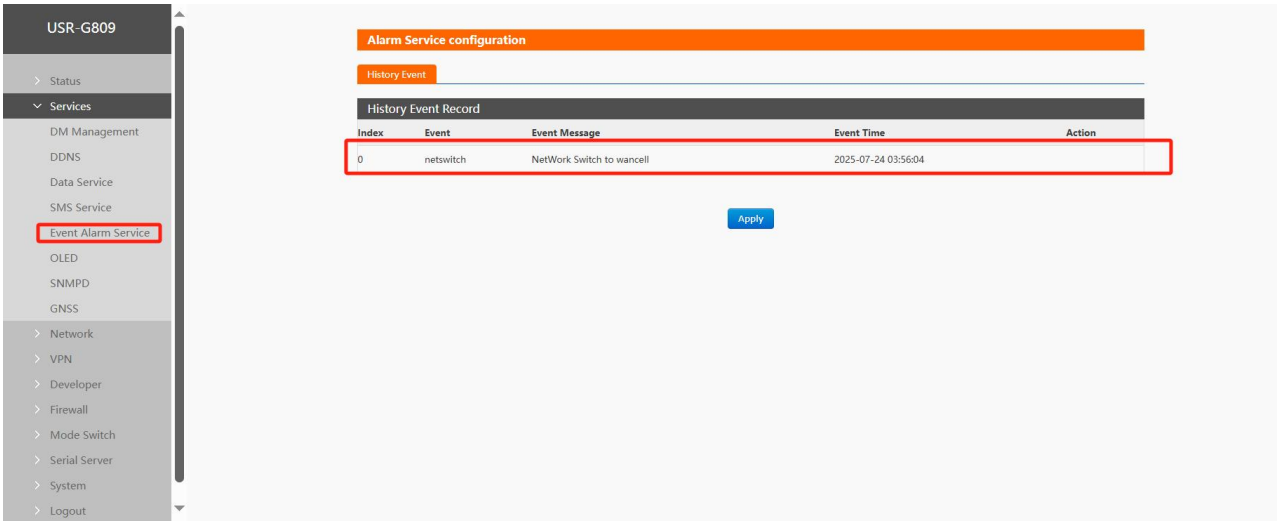


Fig. 58 alarm list

4.6. SMS service

Enable SMS function, you can query/configure the router by sending SMS AT and command, and the router needs to use SIM card that can send SMS.

4.6.1. Basic configuration

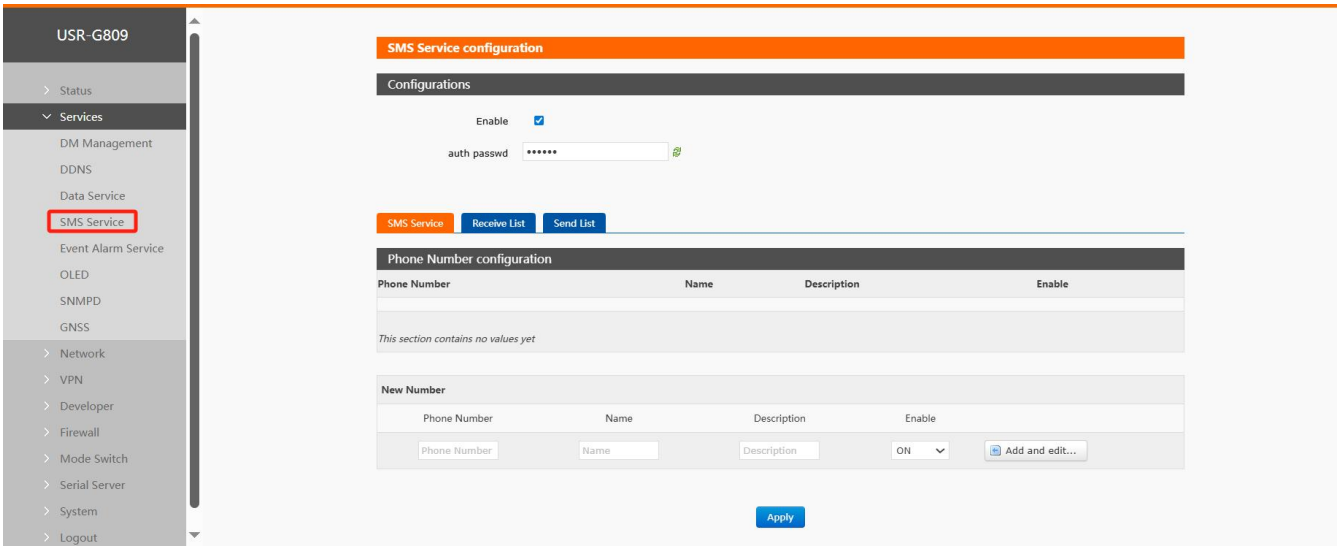


Fig. 59 Authorized mobile phone number settings

table 27 configuration parameters

Name	Describe	default parameters
note	Enable: Enable SMS service Disable: Turn off SMS	enabled
authentication password	Send command prefix password	123456
phone number	Set phone numbers for authorized access	empty
name	Give the phone a name.	empty
describe	Give the phone a description	empty
enabled	ON: Authorize the mobile phone number to send query/set router information OFF: do not accept the mobile phone number information	ON

<Description>

- Up to 6 mobile phone numbers can be authorized.

4.6.2. SMS Service

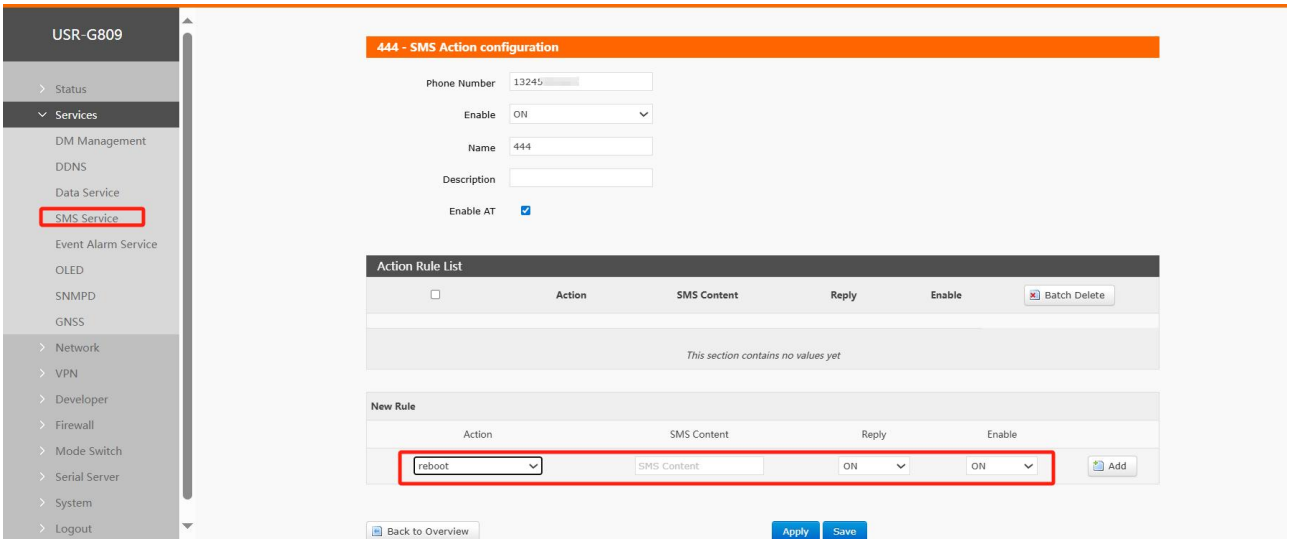


Fig. 60 SMS Action Rules

table 28 configuration parameters

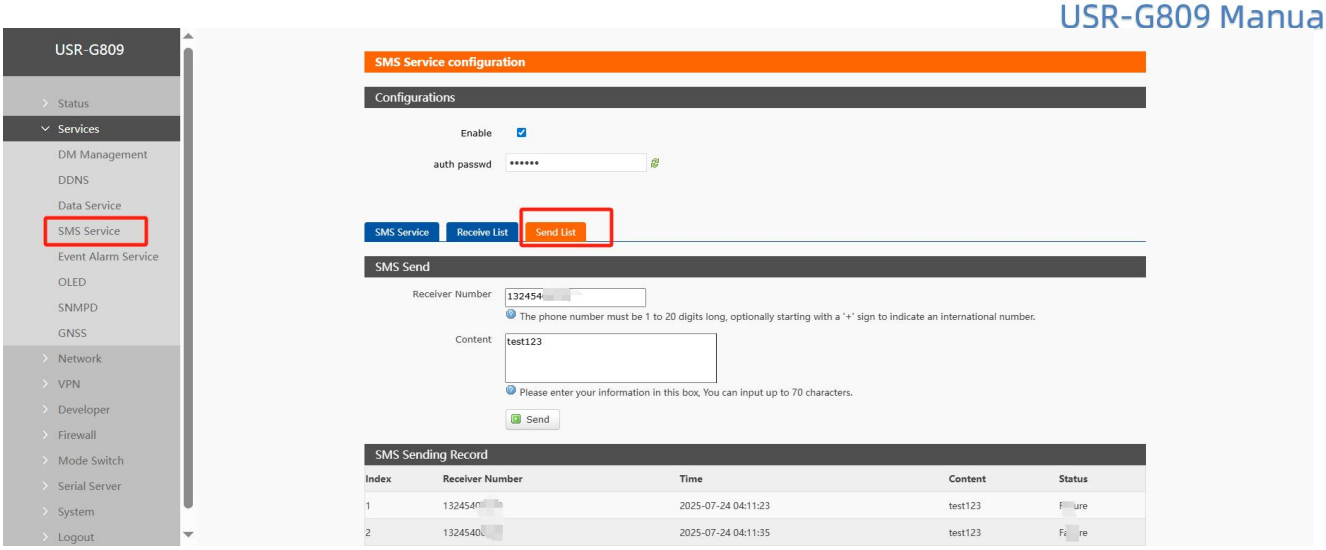
Name	Describe	Default parameters
phone number	Set Authorized Phone Number	not have
enabled	ON: Accept the phone number information OFF: do not accept the mobile phone number information	ON
name	Give the phone a name.	empty
describe	Give the phone a description	empty
Enable AT	Enable SMS AT function	check
movement	Selection action	restart
SMS content	Authorize the mobile phone number to send authentication password + short message content, and the router executes the action.	empty
reply	After receiving the short message, the router replies to enable the mobile phone number	ON
enabled	the action enable switch	ON

<Description>

- A maximum of 40 action rules can be created for each mobile phone number.

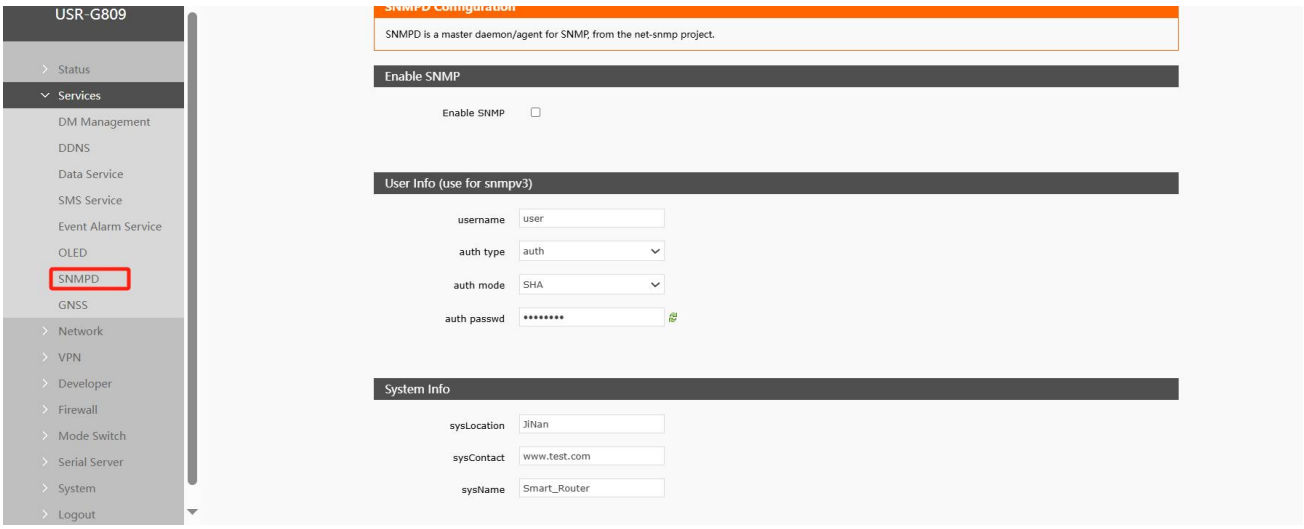
4.6.3. Transmission list

The router's cell phone number can be determined by sending a list of test text messages to authorized cell phone numbers



4.7. SNMPD

SNMP (Simple Network Management Protocol) service, you can remotelyview device information, modify device parameters, monitor device status and other functions of your device through SNMP protocol, without having to go to the site to monitor and configure the device one by one. The version of SNM supported by this device is V2C and V3.



function	content	default
Snmp switch configuration	Check Enable SNMP Service	not checked
user name	Names assigned to	user
authentication type	Authentication or authentication and encryption	authentication
authentication mode	Authentication protocols used by users and hosts to receive traps.MD5 or Sha	SHA
authentication password	User authorization password	authpass
alliance	Location of this equipment	JiNan
system contact	Contacts for this device	www.test.com
system name	System name of this device	Smart_Router

Basic router information can be obtained through SNMP. OID is as follows.

table 30 SNMP OID List

OID	describe	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	Get device IMEI	GET
.1.3.6.1.4.1.2021.8.2.101.3	Get firmware version number	GET
.1.3.6.1.4.1.2021.8.2.101.4	Acquire registration status of cellular network	GET
.1.3.6.1.4.1.2021.8.2.101.5	Get SIM card ICCID	GET
.1.3.6.1.4.1.2021.8.2.101.6	Get Registered Network Types	GET
.1.3.6.1.4.1.2021.8.2.101.7	Get 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	Get cellular IP address (IPv4)	GET
.1.3.6.1.4.1.2021.8.2.101.10	obtaining signal strength	GET
.1.3.6.1.4.1.2021.8.2.101.11	Get tac	GET
.1.3.6.1.4.1.2021.8.2.101.12	Get cid	GET

Open router SNMP service, LAN port PC SNMP tool can test to view the basic information of the router.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

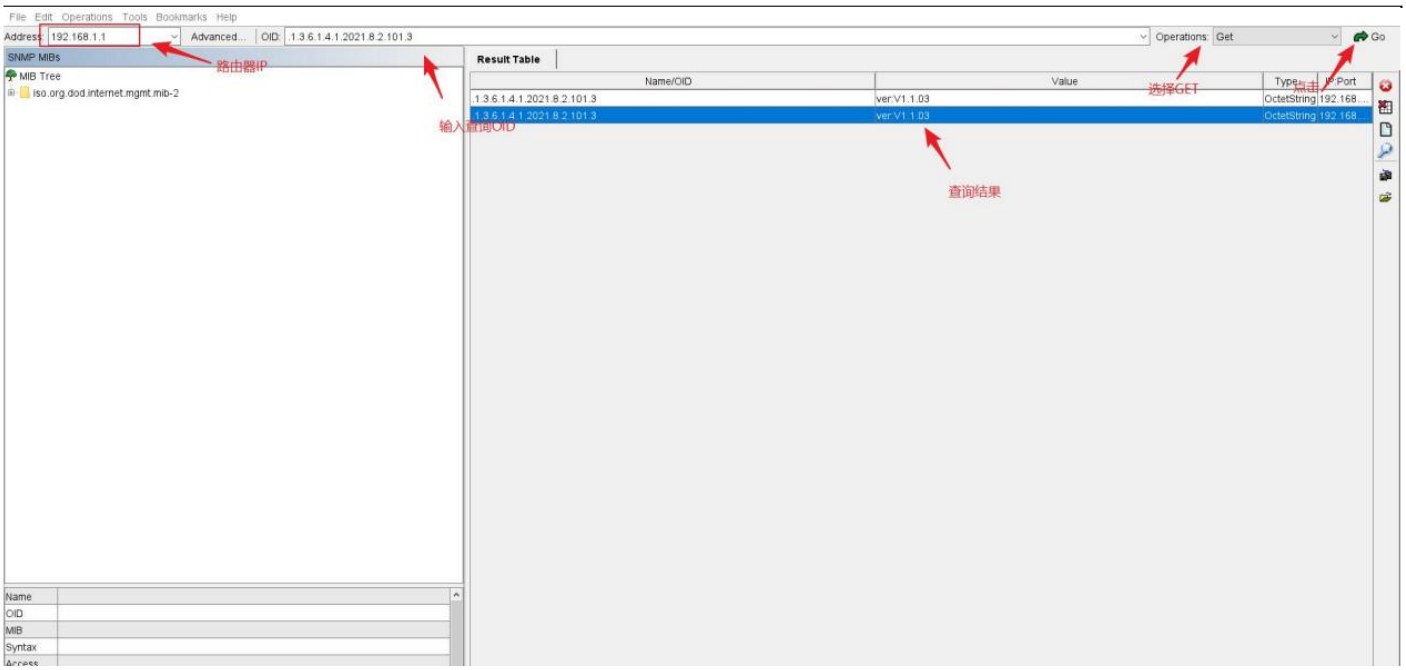


Fig. 64 SNMP Application Interface

5. VPN function

VPN (Virtual Private Network) is a kind of virtual private network technology. In terms of protocols, this router supports PPTP, L2TP, IPSec,OpenVPN, GRE,VXLAN and Wireguard respectively.

5.1. PPTP Client

Before application, you need to set up a VPN server, and fill in the server address, account, password and encryption method correctly to connect.

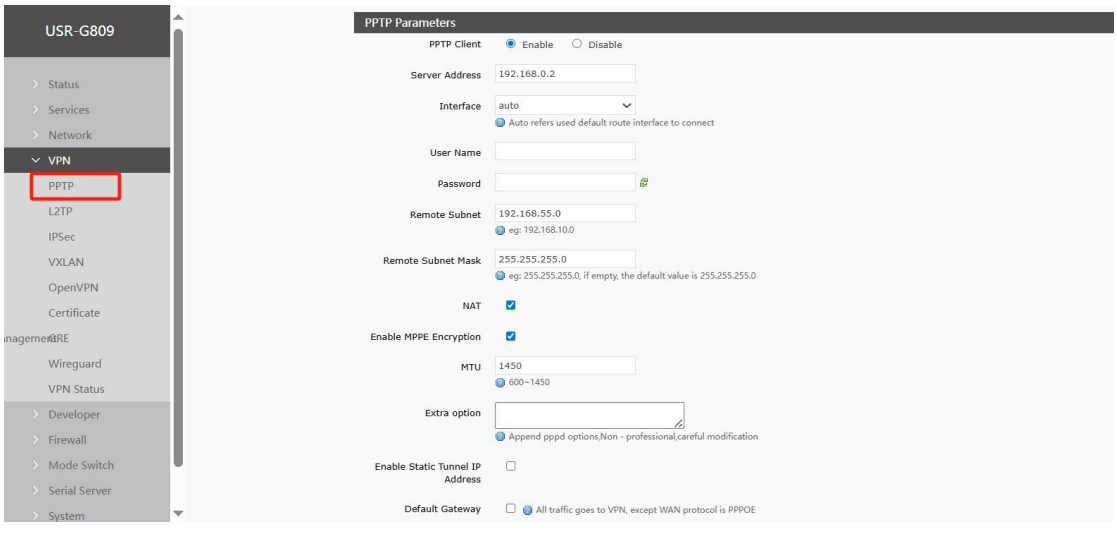


Fig. 65 Router Add VPN Operation Figure 1

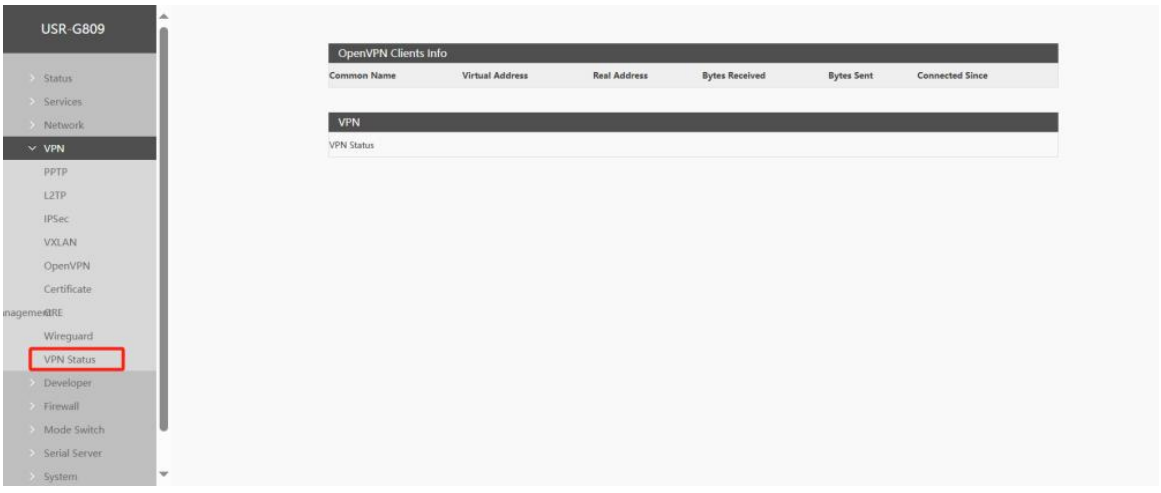
table 31 PPTP Configuration

Name	description	Default parameter
PPT Enable the PPTP client	Enable: Start PPTP client Disable: Close the PPTP client	forbidden
Server address	Enter the IP address or domain name of the VPN server to connect to	192.168.0.2
joggle	Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Connect to a VPN using cellular 5G Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN	voluntarily
user name	Fill in the correct user name	empty
password	Enter the correct password	empty
To the subnet	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the server subnet segment here	192.168.55.0
For the subnet mask	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the subnet mask of the server subnet here	255.255.255.0
NAT	Check: Data passing through the VPN will be sent after NAT No line: Data passing through a VPN does not go through NAT	check
MPPE encryption	After checking, it is: mppe required, stateless	check

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	Not checked: Do not start mppe encryption If the server uses require-mppe-128 encryption, you can uncheck this option and try the following additional configuration: mppe required,no40,no56,stateless refuse-eap refuse-chap refuse-pap refuse-mschap	
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	After checking: All data traffic will be transmitted through the VPN channel after the VPN is established Unchecked: Only the VPN channel is established. If you need subnet intercommunication, static routes should be established Note: If the WAN port is connected by PPPOE, this option is invalid	Not selected
enable ping	Check: Enable VPNping ping alive detection, and reconnect to the VPN if ping fails Unchecked: Do not enable ping to keep alive	Not selected
Ping address	PPT The address that the PPTP network card can ping is usually filled with the PTP address	empty
Ping period	Ping maintenance interval period, unit: seconds	10
Ping number of times	After the Ping failure upper threshold is exceeded, ping will not be sent to the set IP address, and the VPN will reconnect	3

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



5.2. L2TP Client

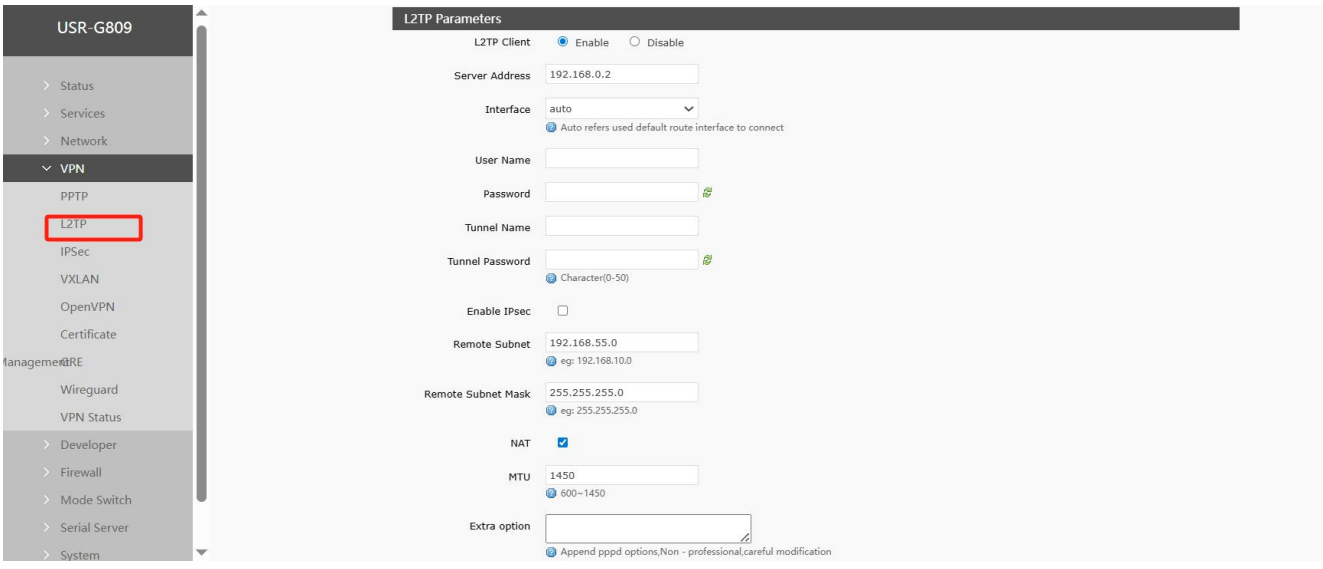


Fig. 67 L2TP Client Settings Interface

table 32 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 to connect to a VPN	voluntarily

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	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	
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 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	Not selected
end on ID	The ID set on the server side	
To the subnet	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the server subnet segment here	192.168.55.0
For the subnet mask	Use a static route through the VPN to enable subnet communication between the client and the server. Enter the subnet mask of the server subnet here	255.255.255.0
NAT	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	Not selected

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	check here 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 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.

5.3. IPSec

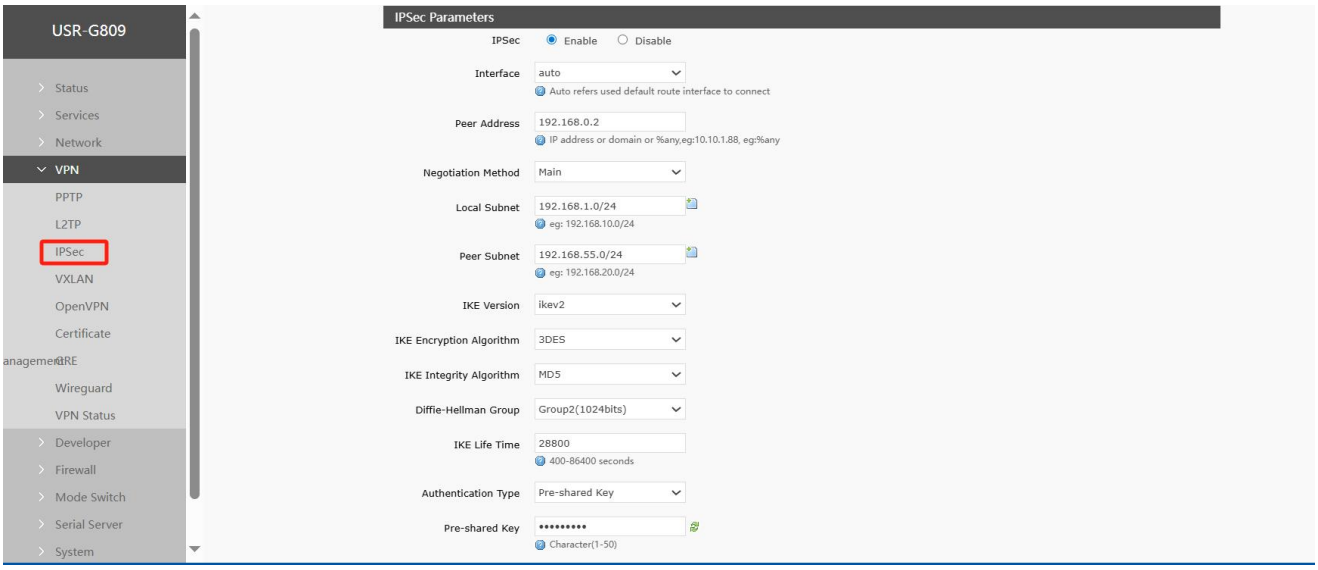


Fig. 69 IPSec Settings Interface

table 33 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	voluntarily

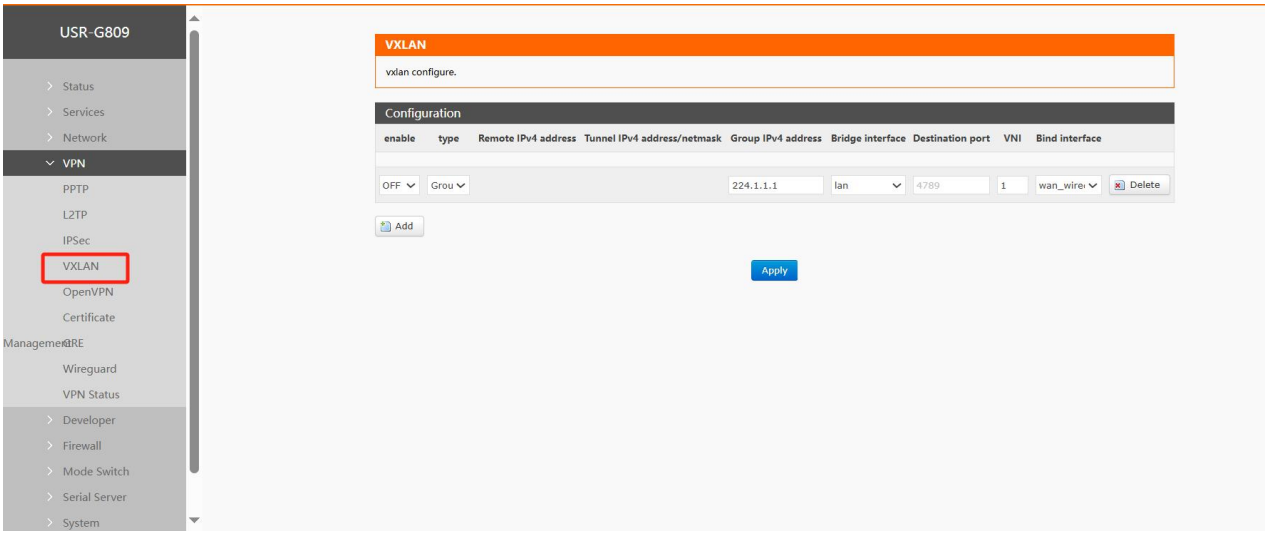
LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	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 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)	Holo type
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

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5.4. VXLAN

VXLAN is primarily used to create virtual local area network (VLAN) in large, multitenant data center environments. VXLAN builds a logical Layer 2 network on top of the physical network by using tunneling technology, so that hosts in different physical locations can communicate as if they were within the same physical LAN.



5.5. OpenVPN

This router supports1-way OpenVPN Server and3-way OpenVPN Client. Several VPNs do not interfere with each other. It is recommended to use only one way OpenVPN.

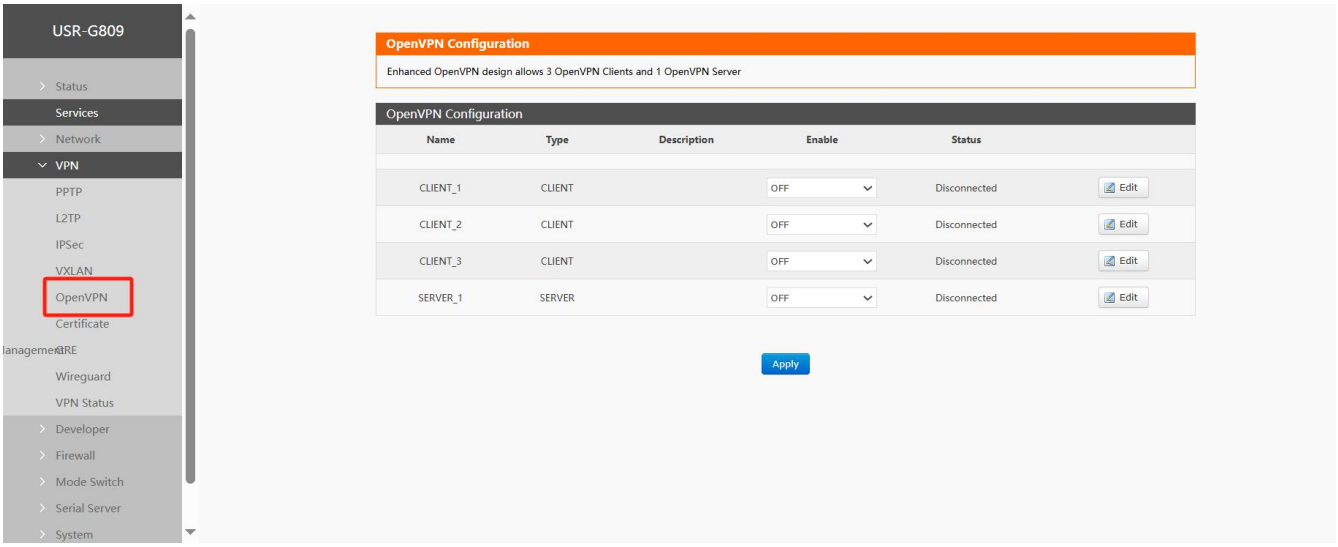


Fig. 84 OpenVPN page

table 35 OpenVPN Client Parameter Table

name	description	Default parameter
start using	Open: Open the openvpn client Close: Disable the openvpn client	close
description	You can customize the description of this OpenVPN path, but you don't have to fill it in	empty
Use the OpenVPN configuration file	Open: You can import the OpenVPN configuration parameters in the form of a file. If you are very familiar with the OpenVPN configuration file, you can use this method. It is recommended to use the router configuration box form Note: Use the router configuration box form	open
OpenVPN configuration file	The configuration file is passed to OpenVPN	not have
protocol	tcp/udp/tcp ipv4/udp ipv4	udp
Remote host IP address	Set the openvpn server address: domain name or IP	192.168.0.2
port	Set the openVPN server port number	1194
Type of certification	None, SSL/TLS, user name and password, pre-shared key, SSL/TLS+ user name and password	SSL/TLS
TUN/TAP	tun/tap	tun
topology	Net30/p2p/subnet	subnet
bridge pattern	Tap bridges LAN and implements layer 2 interaction point 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
joggle	Automatic: Connect to the VPN using the default routing interface Wan_wired: Use the WAN interface to connect to the VPN Sta_2g: Connect to the VPN using the 2.4G STA interface Cellular: Use cellular 4G to connect to the VPN Note: If you select a non-automatic interface, such as the selected interface and server address are not accessible, but other interfaces and server addresses are accessible, you cannot connect to the VPN Select the automatic interface. If one interface is	voluntarily

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	disconnected due to an exception, it can automatically switch to other interfaces to try to connect to the VPN	
Redirect gateway	Use openvpn as the default gateway It takes effect after you select "None" in "Network Switching" The WAN port cannot use the redirect gateway function in PPPoE mode You cannot enable the redirect gateway function for multiple VPNs	close
Nat	Whether the data on the VPN network card is NAT	open
Enable Keepalive	Enable the live detection mechanism	open
Connection detection time interval (seconds)	VPN live heartbeat detection interval	10
Connection detection timeout interval (seconds)	If the heartbeat exceeds the set time without response, reconnect to the VPN	120
enable LZO	Data compression method	No preference
encryption algorithm	Data encryption algorithm	BF-CBC
Hash algorithm	The data's hash algorithm	SHA1
TLS way	Select the TLS authentication method	OFF
LINK-MTU/TUN-MTU/TCP MSS	Set the data pack length	Air / air / 1450
Maximum frame length	The maximum frame length of data is the default without special configuration	empty
Allows remote address changes	Whether to allow remote address change Settings	close
Log grade	Openvpn log level, the larger the number, the more detailed the log is. Generally, open a higher level to troubleshoot problems when the connection is abnormal	Warning (3)
Additional configuration	Non-professionals should not configure it. You need to input openvpn recognizable parameters	empty
Local route-destination	Set the static route target segment established by the openvpn network card on this end	empty
Local route-Network mask	Set the subnet mask of the static route target established by the openvpn network card on this end	empty
CA	Upload CA certificate	not have
CERT	Upload the client certificate	not have
KEY	Upload the client private key	not have
TLS	Upload the TLS certificate. If the TLS mode is selected OFF, you do not need to upload the certificate here	not have
Pre-shared key	Upload the pre-shared key. You can upload the certificate only when you select the authentication type as pre-shared key	not have

Tab 2 OpenVPN Server parameter table

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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 occur after this value is reached. Unit: seconds If the router client is set to 0, additional configuration is required: reneg-sec 0	3600

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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	Set the parameters for assigning fixed IP addresses to clients. You can set multiple fixed	

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

a static IP address	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 key	not have

Tab 3 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	empty

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

	password or SSL, the CA certificate must be sent	
Cert	Enter the client certificate and select the SSL authentication type. This certificate must be sent	empty
Key	Enter the client key and select the SSL authentication type. This certificate must be sent	empty
Tls-auth (key)	If the openvpn TLS mode is set to tls-auth, you need to enter the TLS key here	empty
Tls-crypt (key)	If the openvpn TLS mode is set totls-crypt, the TLS key must be passed here	empty
Pre-share the key	When the authentication type is selected to pre-share the key, enter the pre-shared key certificate here	empty
Certificate password input type	If a certificate password is generated, it must be set according to the file or manually entered type	document
Certificate password	The password of the PEM certificate can be entered or uploaded (the password is in the file). If the certificate is generated without a password, do not fill in this field	empty
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	empty

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

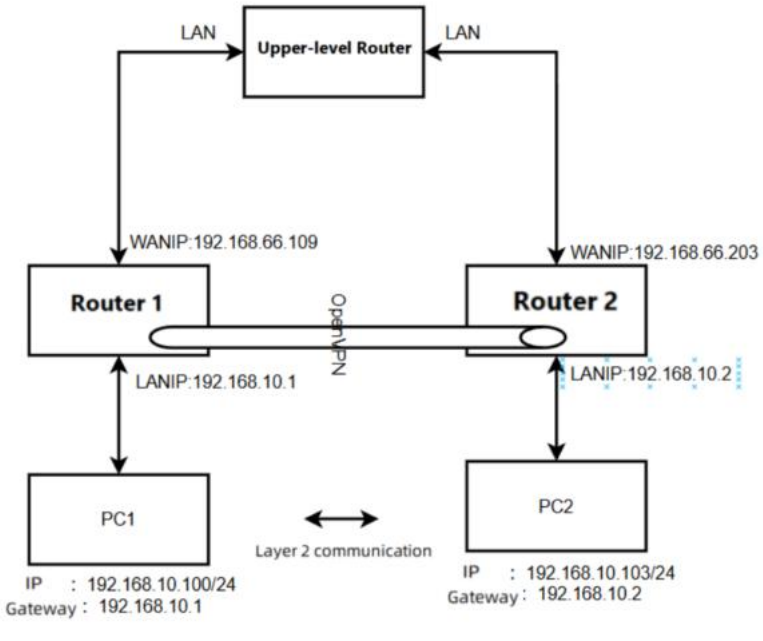
	generated, do not fill in here	

< 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.

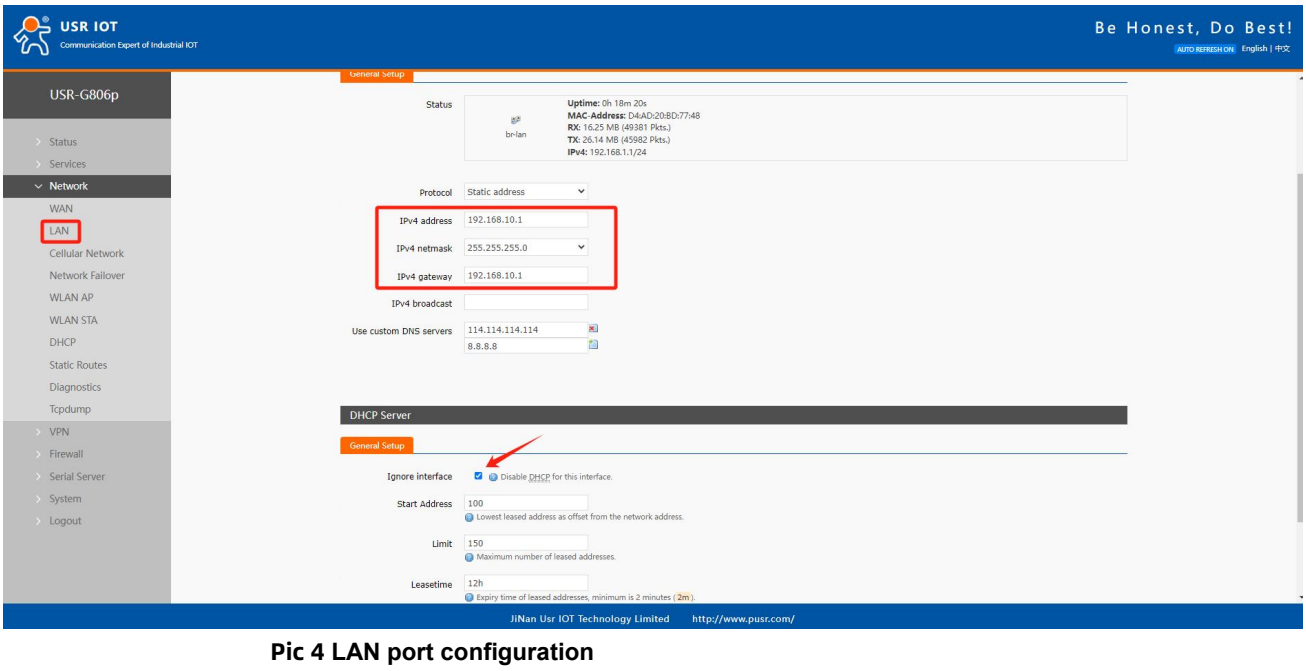
5.5.1. Openvpn TAP Bridge Instance

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.



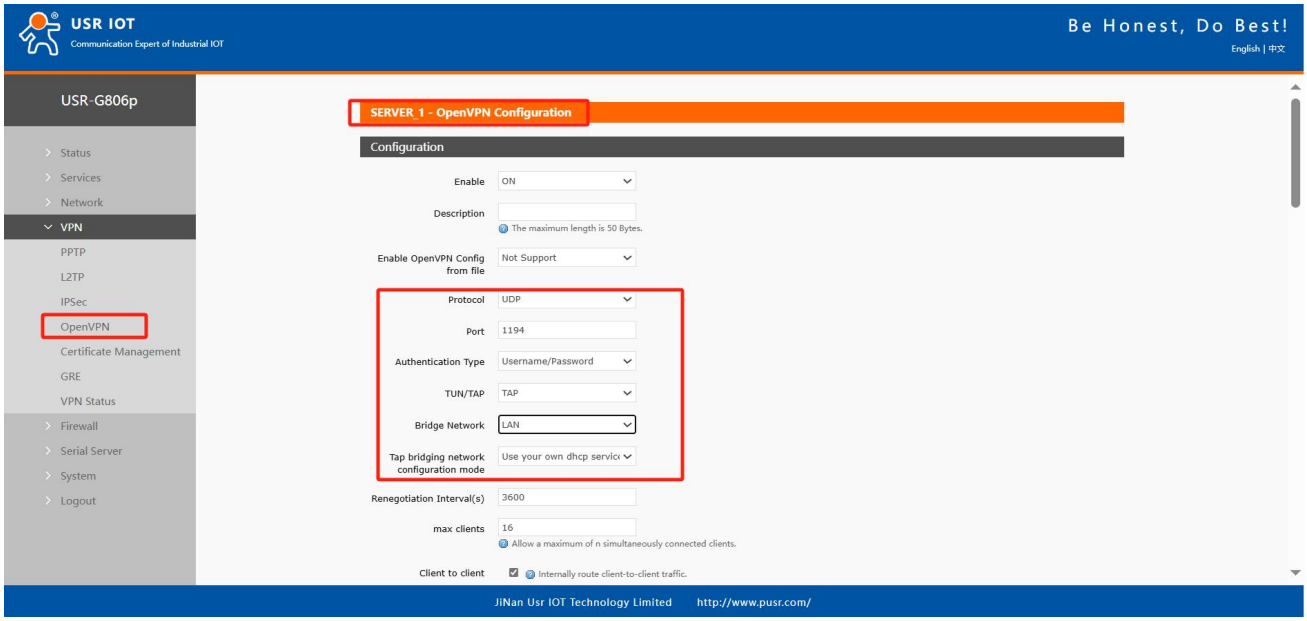
Pic 3 Connect the topology

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.



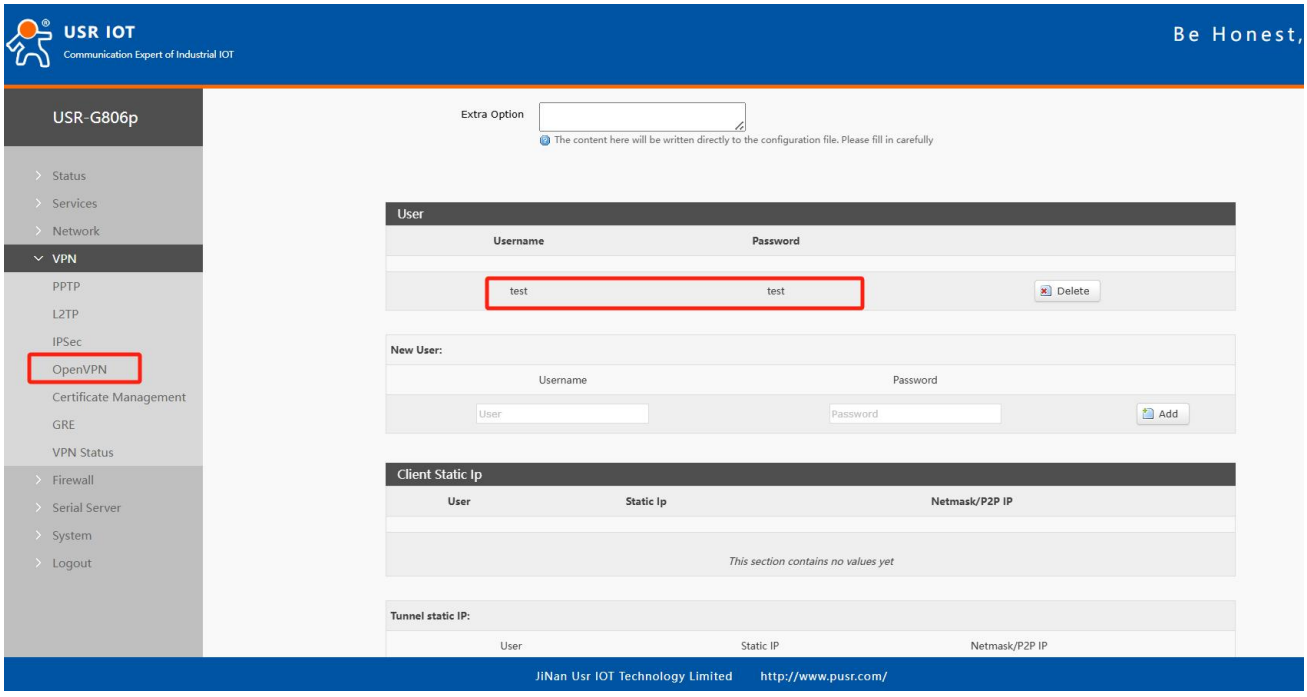
Pic 4 LAN port configuration

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



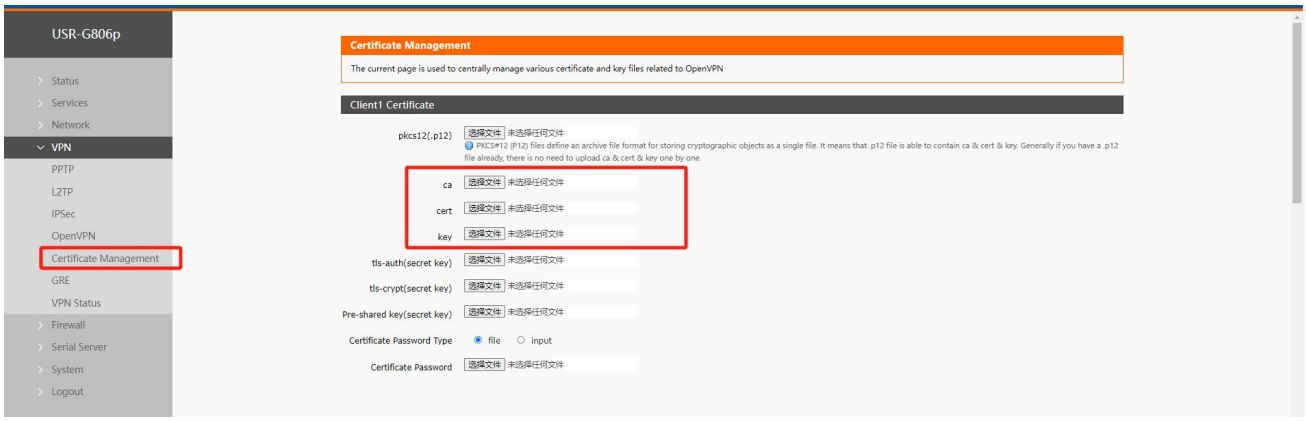
Pic 5 OpenVPN configuration 1

Set a set of user names and passwords.



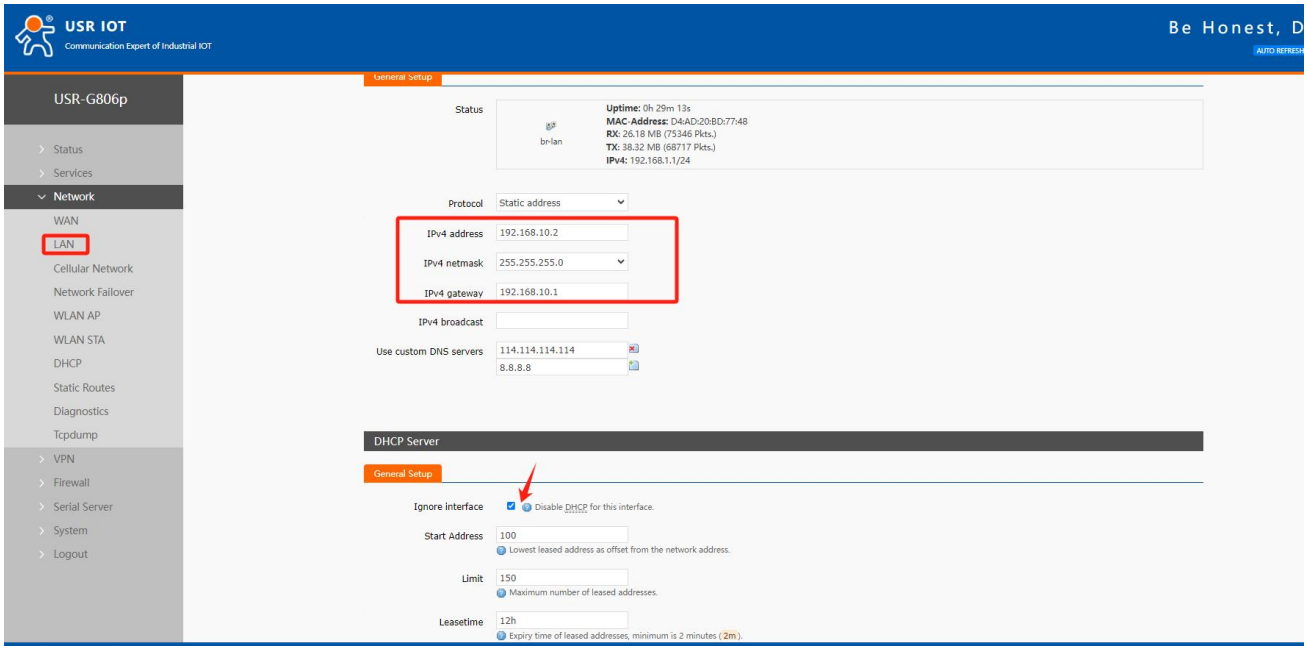
Pic 6 OpenVPN configuration 2

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



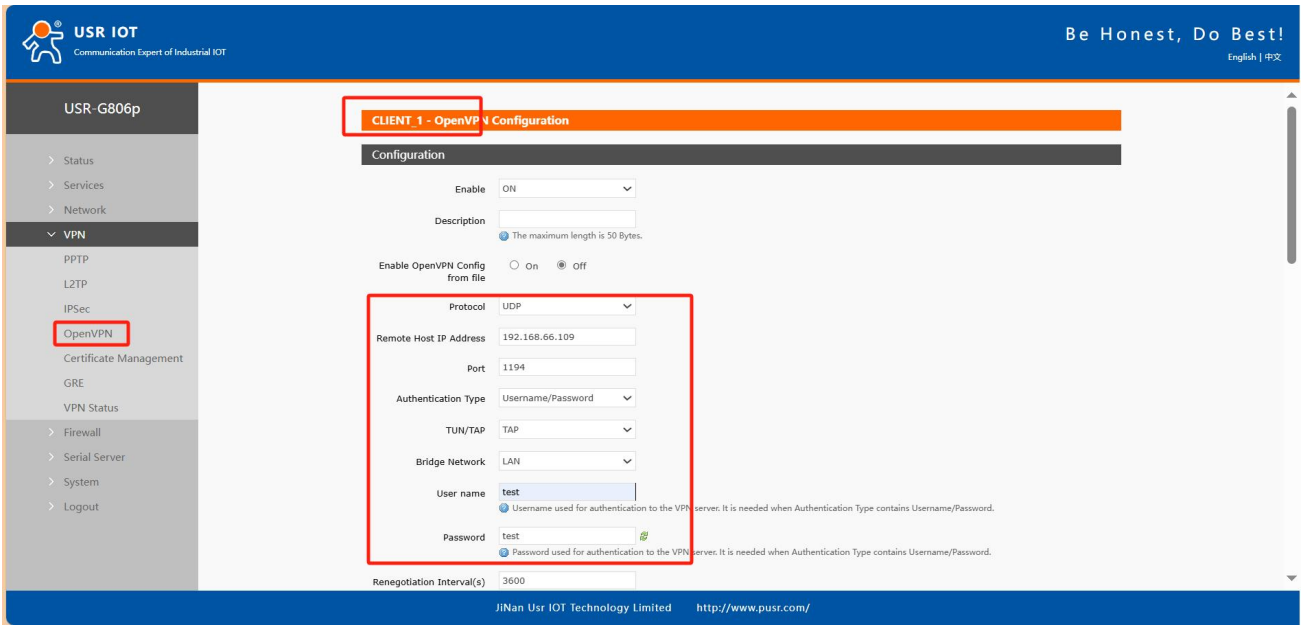
Pic 7 OpenVPN configuration 3

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.

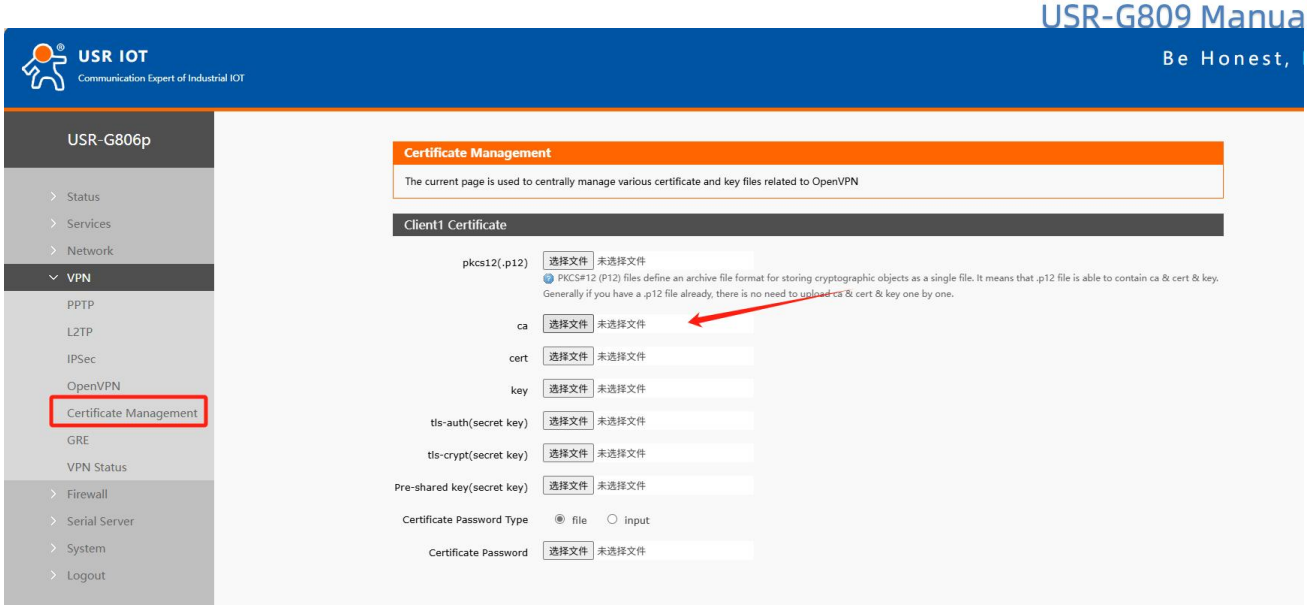


Pic 8 LAN port configuration

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



Pic 9 OpenVPN configuration 1



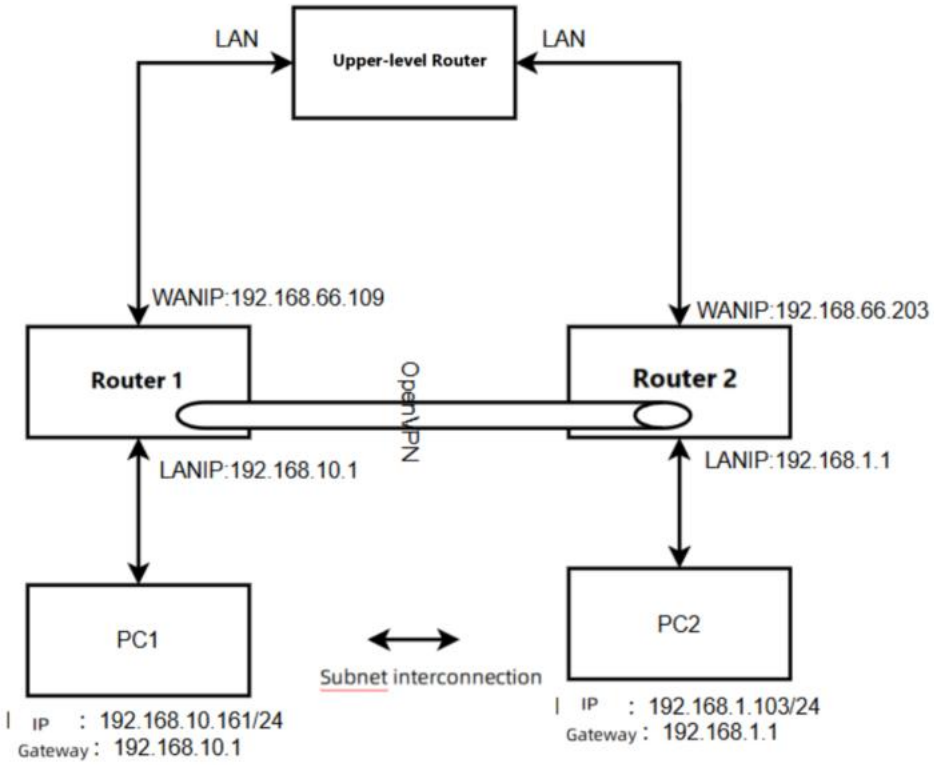
Pic 10 OpenVPN configuration 2

Test that PC1 and PC2 can communicate with each other:



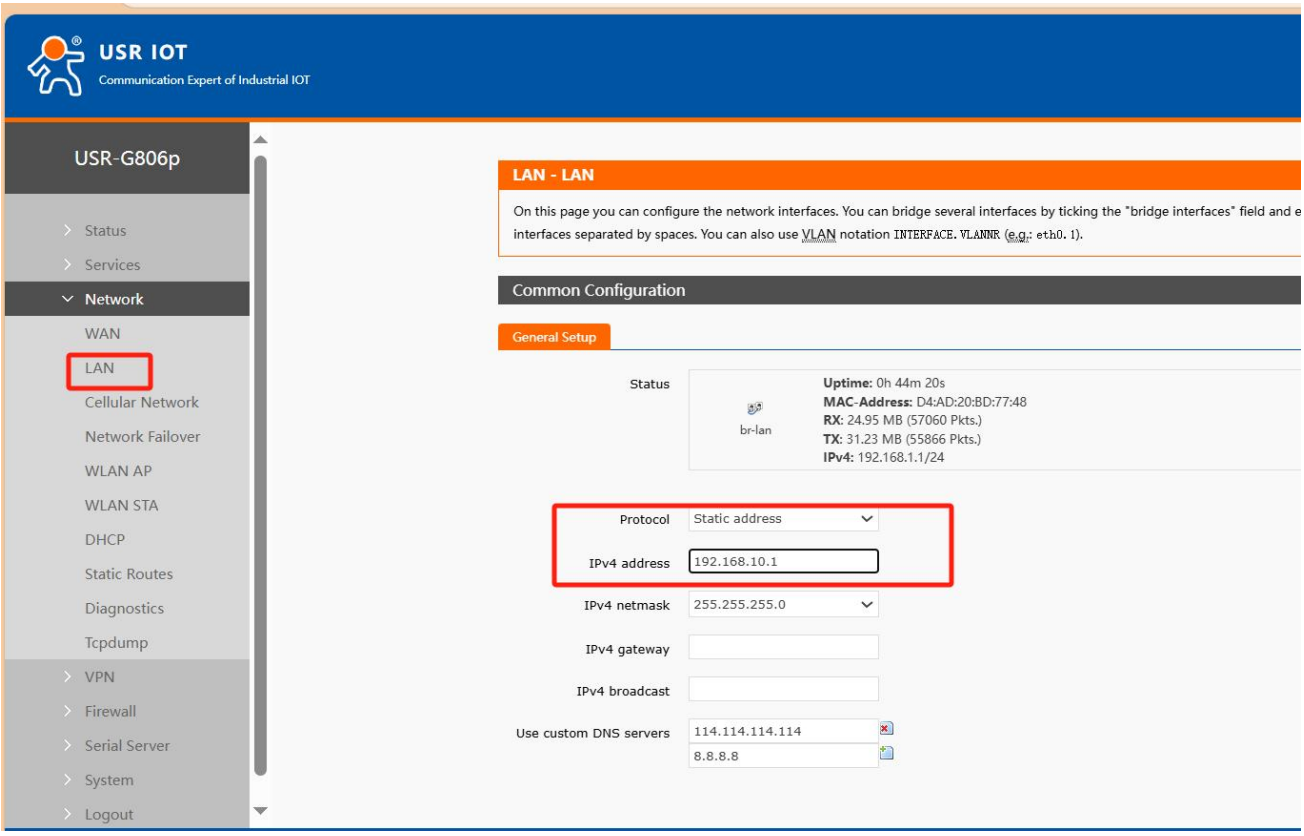
LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

5.5.2. An Example of Implementing Subnet Interworking in Openvpn TUN



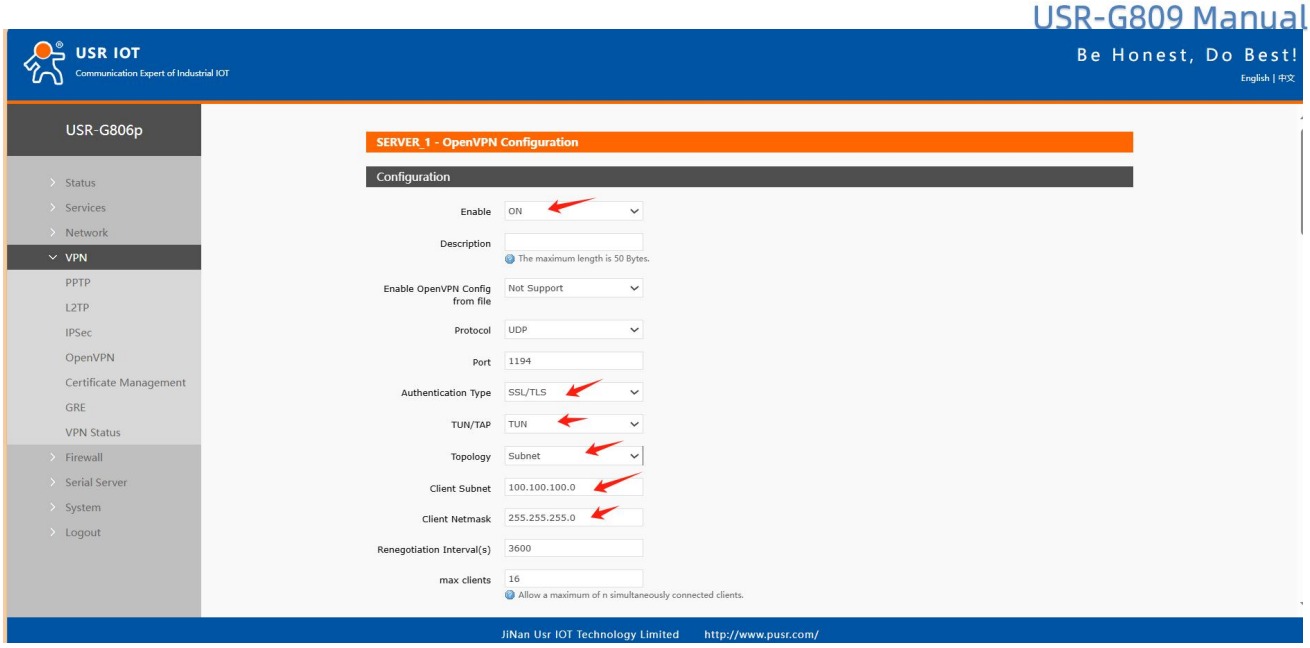
Pic 11 Connect the topology

Router 1 configuration, LAN port setting



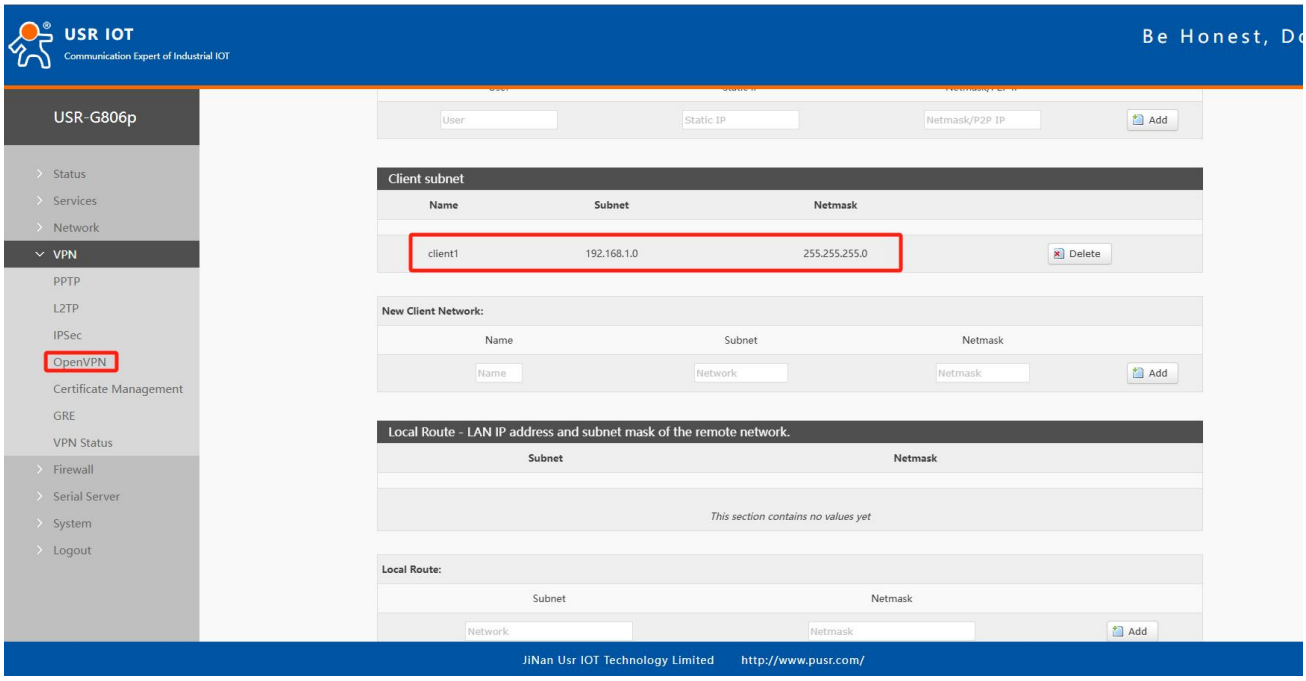
Pic 12 Router 1 is configured 1

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



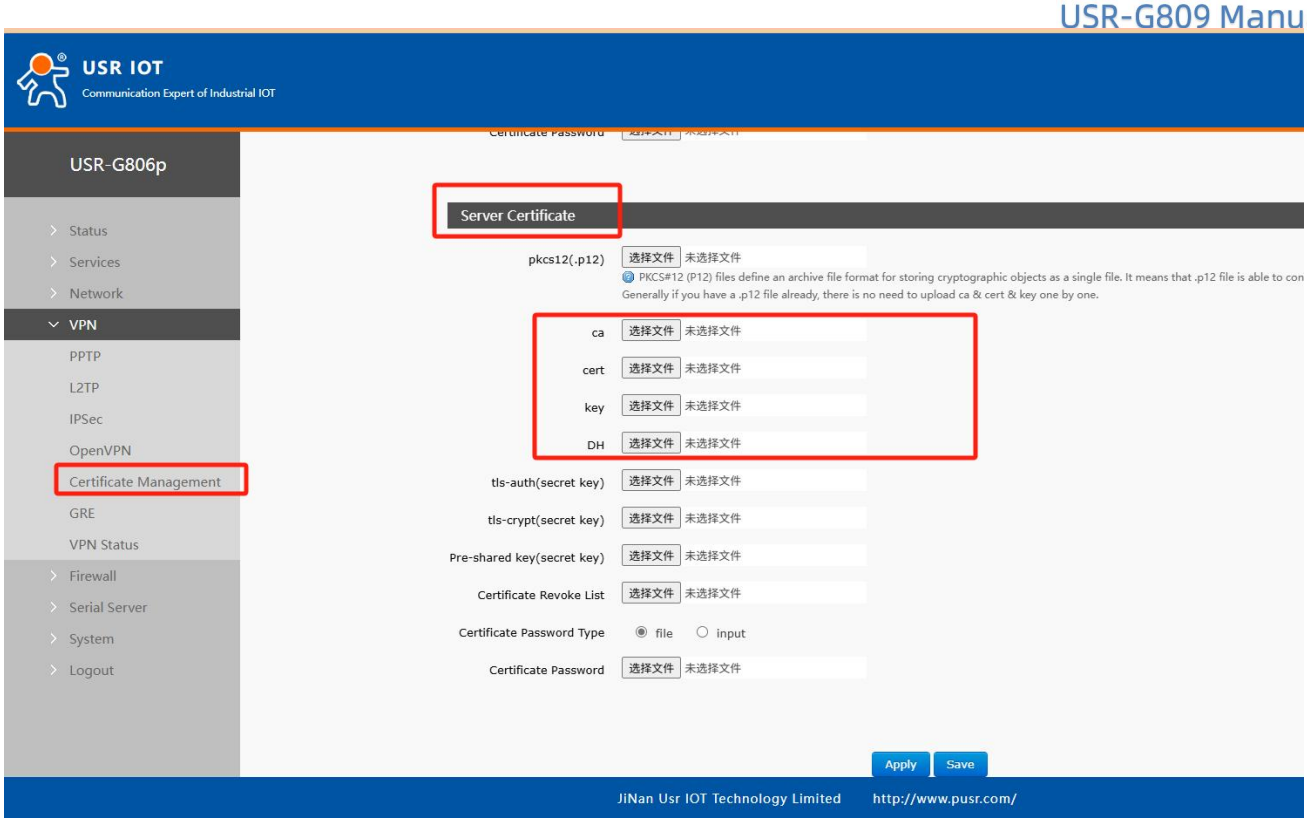
Pic 13 Router 1 is configured 2

Enter the client subnet information and click "Save"



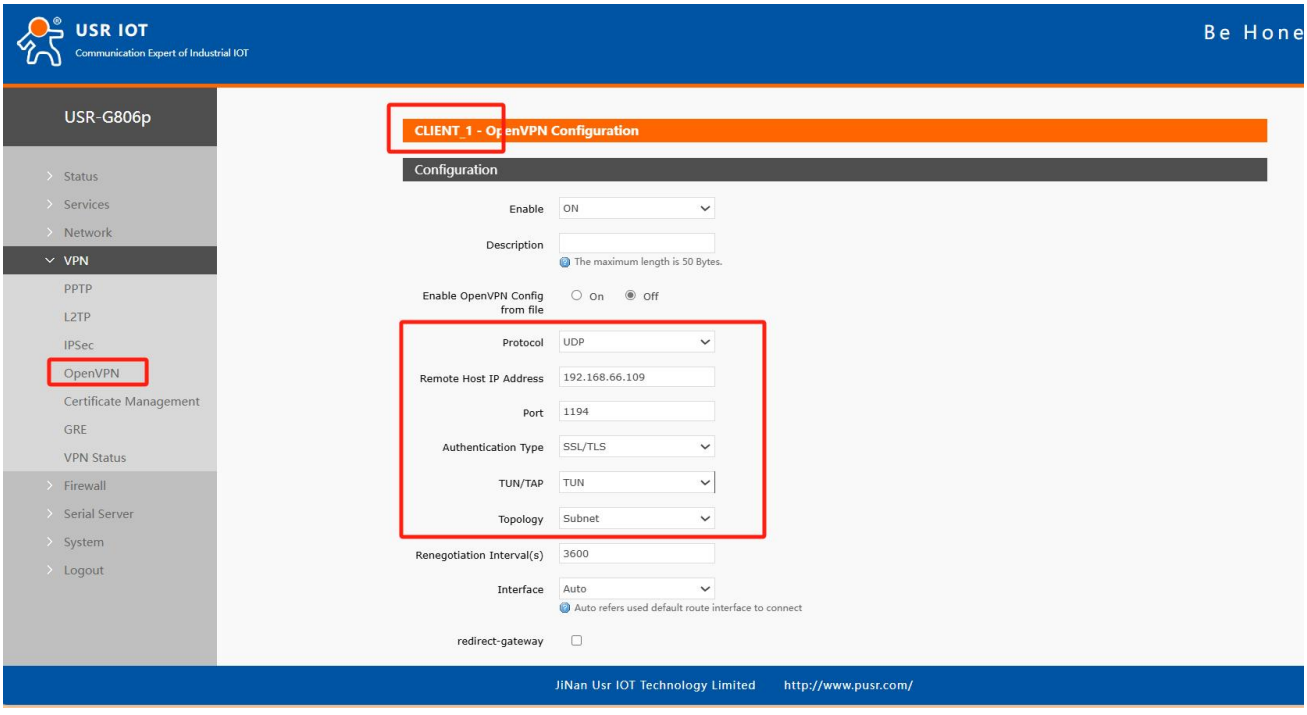
Pic 14 Router 1 is configured 3

Enter the OpenVPN server certificate and click "Apply".



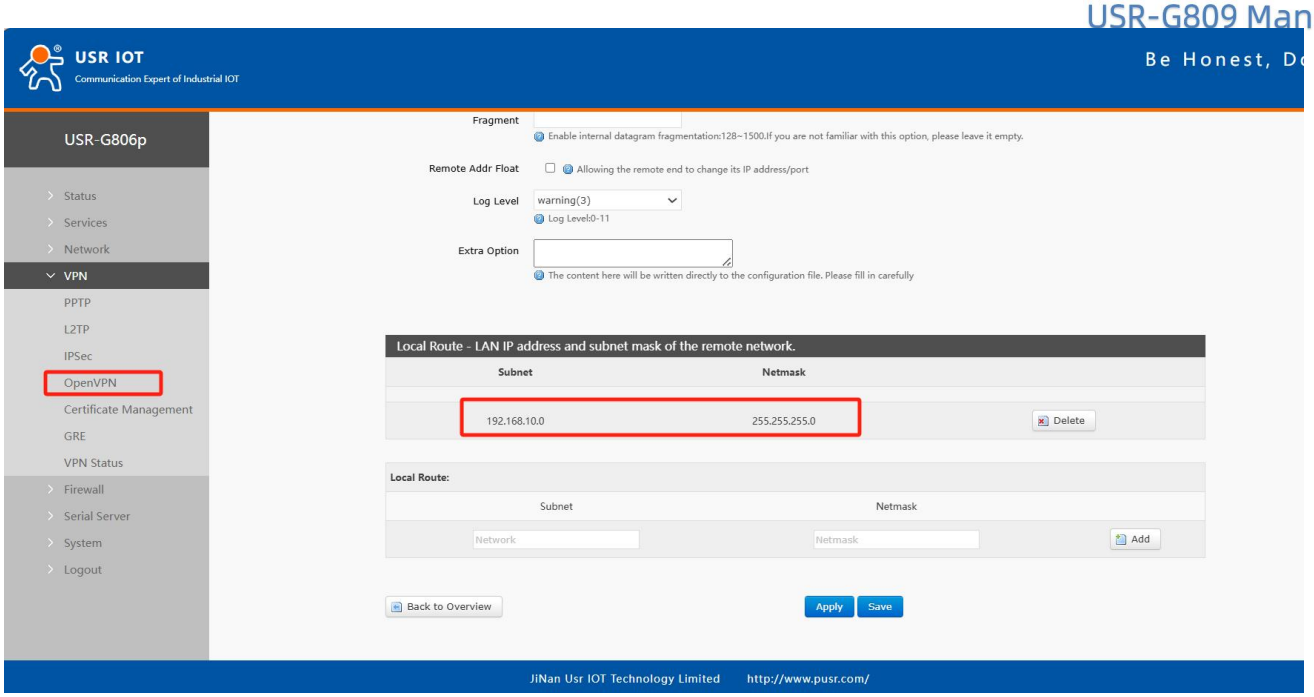
Pic 15 Router 1 is configured for 4

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).



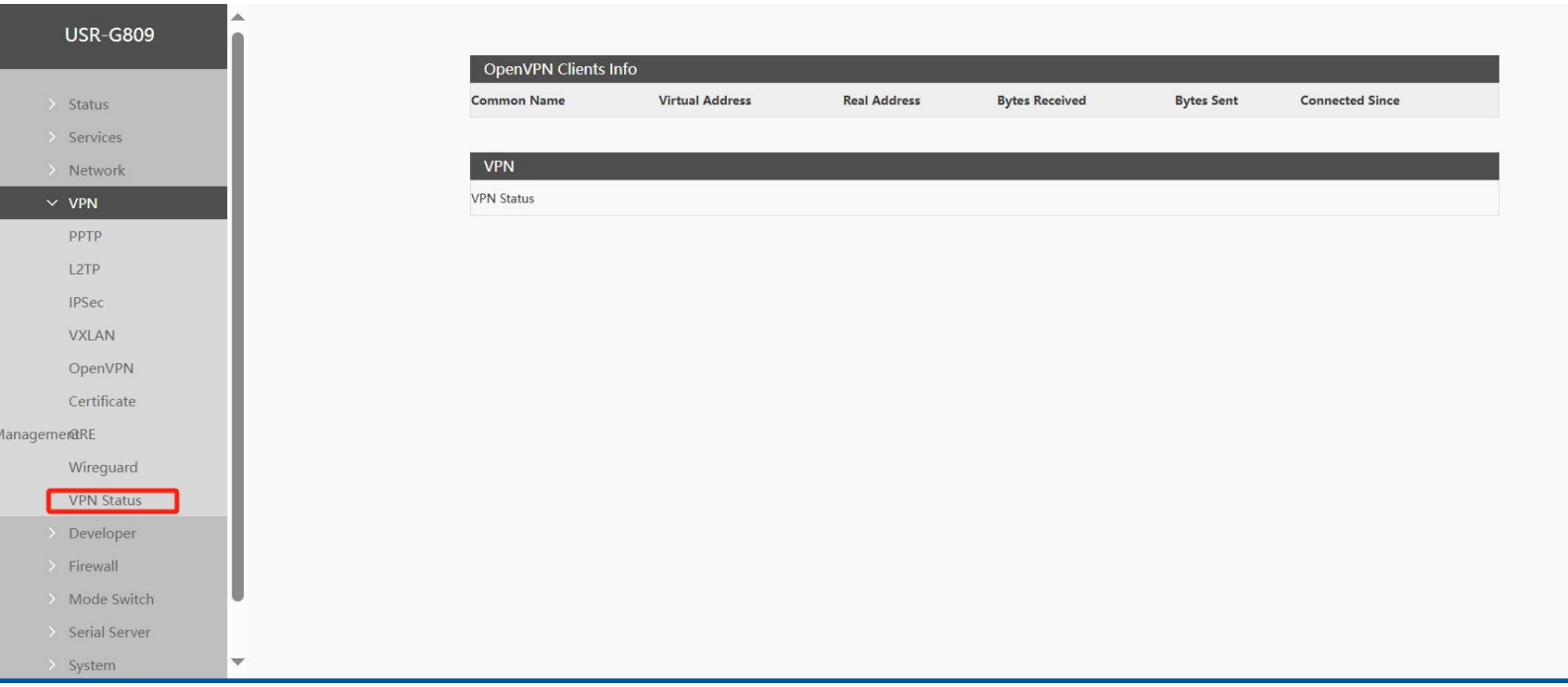
Pic 16 Router 2 is configured 1

Client adds information to the server subnet.

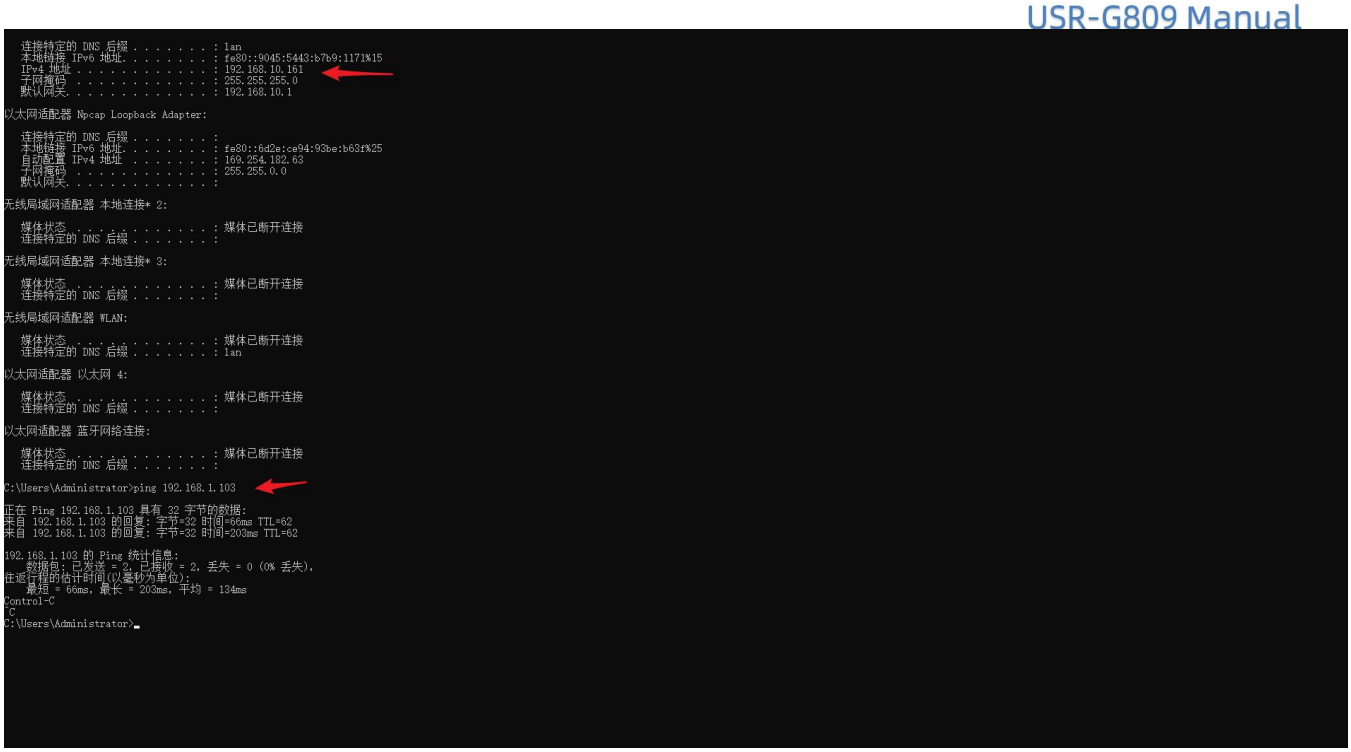


Pic 17 Router 2 is configured 2

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



PC1 and PC2 are interconnected



Pic 18 PC1 and PC2 are interconnected

5.6. GRE

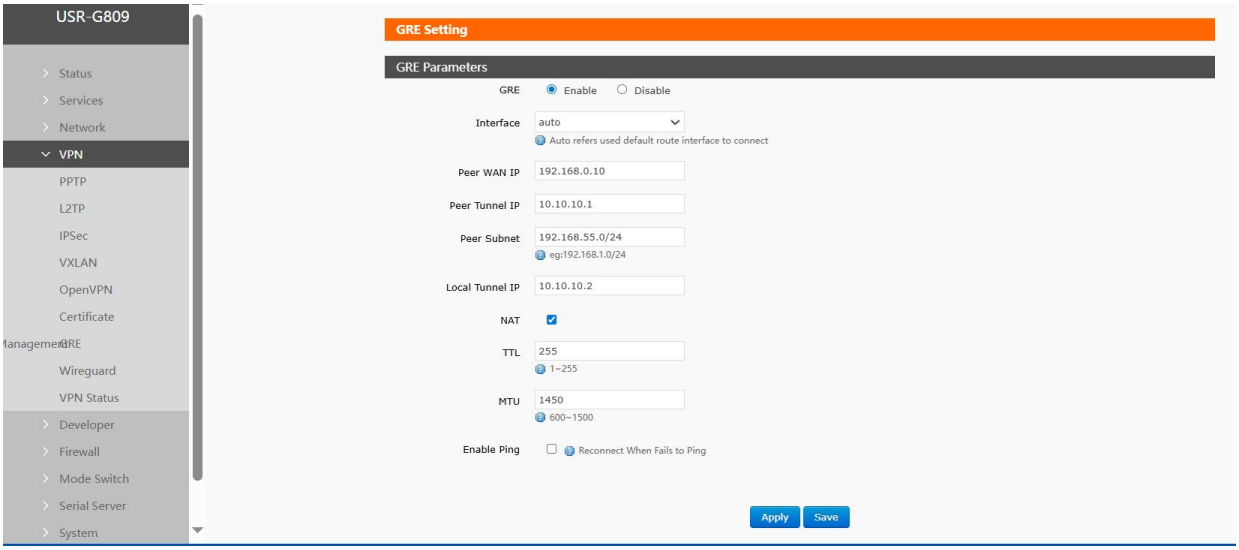


Fig. 106 GRE Basic Configuration

table 38 configuration parameters

name	describe	default parameters
GRE	Enable: Start GRE Close: Close GRE	forbidden
port	Automatic: Connect VPN using default routing interface Wan_wired: Connect to VPN using WAN1 interface Wan2_wired: Connect VPN using WAN2 interface Sta_2g: Connect VPN using 2.4G STA interface Sta_5g: ConnectVPNusing 5.8G STA interface Cellular Data: ConnectVPN using cellular Note: Select a non-automatic interface, such as selecting an interface that is not connected to the server address,while other interfaces and serveraddresses are connected to VPN. Select automatic interface. If one interface is abnormally disconnected, you can automatically switch toanother interface to try to connect to VPN.	voluntarily
Default NIC connection	Check: Use the specified NIC to connect toVPN when the specified NIC is the default route Unchecked: If the specified NIC hasIPand is not the default route, it will not connect to VPN.	not checked
Remote WAN IP	peer IP	192.168.0.10
Remote Tunnel IP	Opposite GRE Tunnel IP	10.10.10.1
pair terminal net	Used for subnet interworking to establish a static route to the terminal network	192.168.55.0/24
Local Tunnel IP	Local GRE Tunnel IP	10.10.10.2
NAT	Check: NAT data through GRE	check
TTL	TTL of GRE	255
MTU	MTU of GRE	1500
Enable ping	Check: Enable VPNping keepalive detection, ping failure will reconnect VPN Unchecked: ping keepalive function is	not checked
Ping Address	The address that can be pinged through the GRE tunnel. Generally, the IP address of the	empty
Ping period	Interval period of ping keepalive, unit: seconds	10
Number of pings	Ping failure threshold, after the number of times to throw ping set IP address, will reconnect VPN	3

5.7. Wireguard

WireGuard is a secure network tunnel.

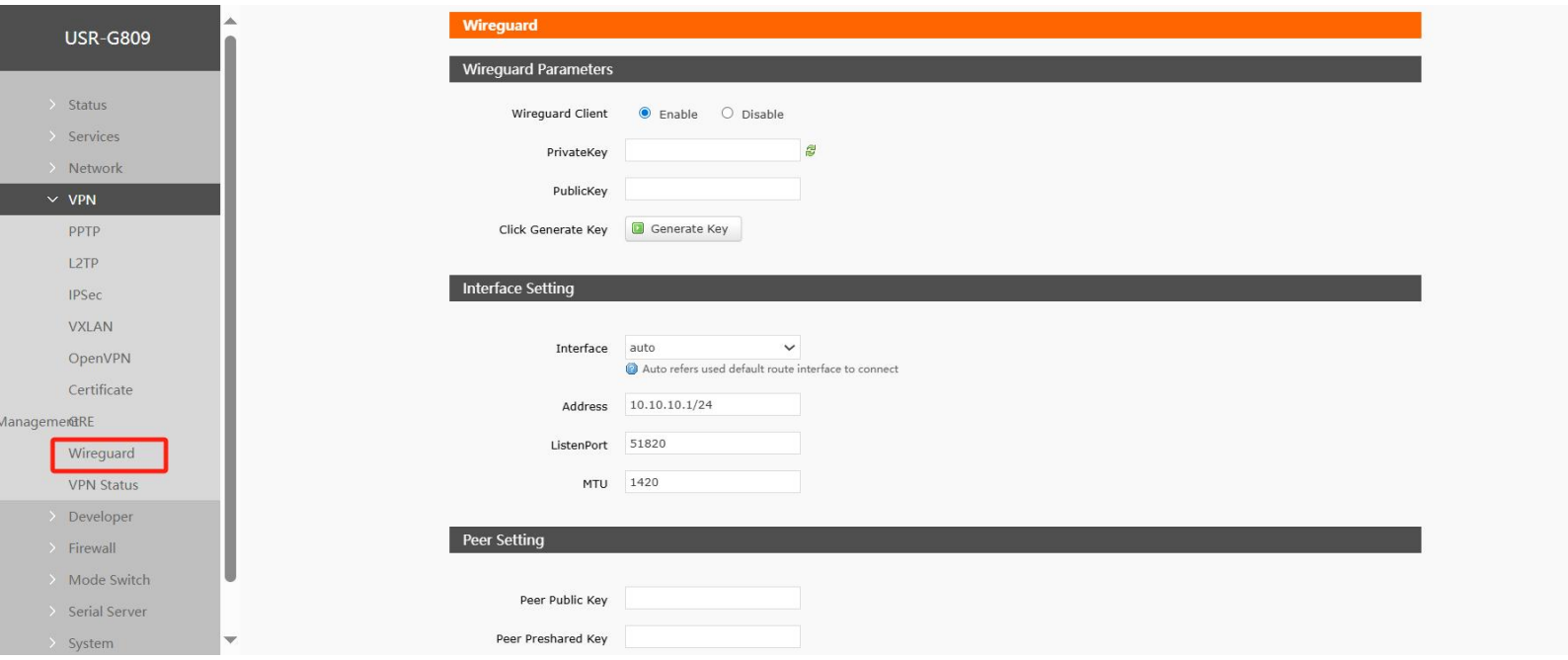


Fig. 107 Wireguard

table 39 configuration parameters

name	describe	default parameters
Wireguard Client	Enable: Start Wireguard Close: Close Wireguard	close
Local private key	Click Generate Key to fill in automatically	empty
local public key	Click Generate Key to fill in automatically	empty
Click Generate Key	Generate local private key and local public key and fill them in automatically	not have
port	Automatic: Connect VPN using default routing interface Wan_wired: Connect to VPN using WAN1 interface Wan2_wired: Connect VPN using WAN2 interface Sta_2g: Connect VPN using 2.4G STA interface Sta_5g: ConnectVPNusing 5.8G STA interface Cellular Data: ConnectVPN using cellular Note: Select a non-automatic interface, such as selecting an interface that is not connected to the server address,while other interfaces and serveraddresses are connected to VPN. Select automatic interface. If one interface is abnormally disconnected, you can automatically switch toanother interface to try to connect to VPN.	voluntarily
Default NIC connection	Check: Use the specified NIC to connect toVPN when the specified NIC is the default route Unchecked: If the specified NIC hasIPand is not the default route, it will not connect to VPN.	not checked
site	Local VPN Address	10.10.10.1/24
listening port	local listening port	51820
MTU	VPN NIC MTU value	1420
peer public key	Fill in the local public key generated by the peer	empty

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

pre-shared key	Can be blank, if necessary fill in this peer if fill in to keep consistent:Get pre-shared key method: You can use linux systems to send wg genpsk to generate pre-shared keys Technical support can be contacted for generation.Available values: 6o8K53bwKXzhZEby+wXyD9qcJk5G13LVzflaC9aM6Cc=	empty
opposite end port	peer listening port	51820
pair terminal net	For router subnet interworking, please fill in terminal network	192.168.55.0/24
allowed IP	IP or IP segment that allows Wireguard network cards to pass through, generally the default value	0.0.0.0/0
continuous keep-alive interval	Network card detection heartbeat time, unit: seconds	25
Enable ping	Check: Enable VPNping keepalive detection, ping failure will reconnect VPN Unchecked: ping keepalive function is	not checked
Ping Address	The address that can be pinged through Wireguard tunnel, generally you can fill in the IP address of the	empty
Ping period	Interval period of ping keepalive, unit: seconds	10
Number of pings	Ping failure threshold, after the number of times to throw ping set IP address, will reconnect VPN	3

5.7.1. Subnet Interworking Instance

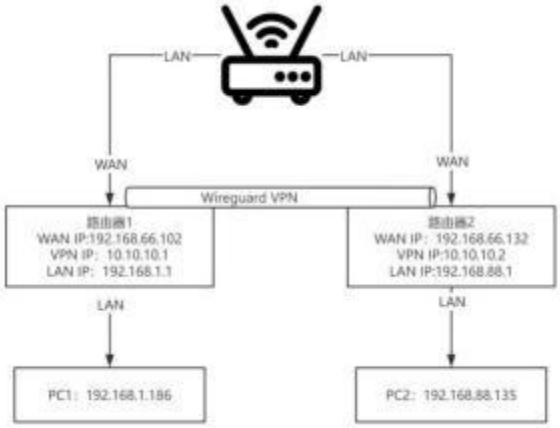


Fig. 108 connection topology

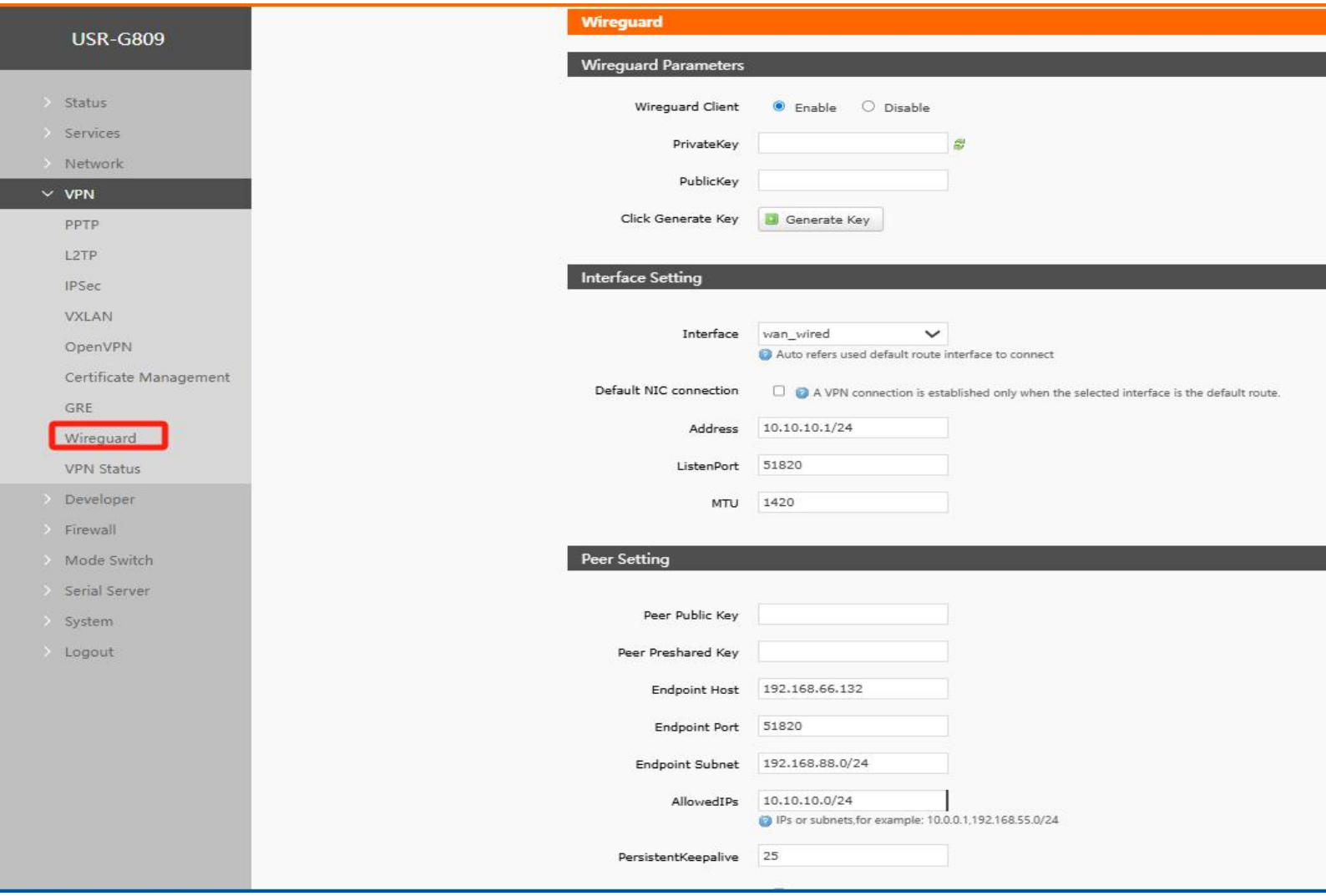


Fig. 109 Router 1 Settings Page

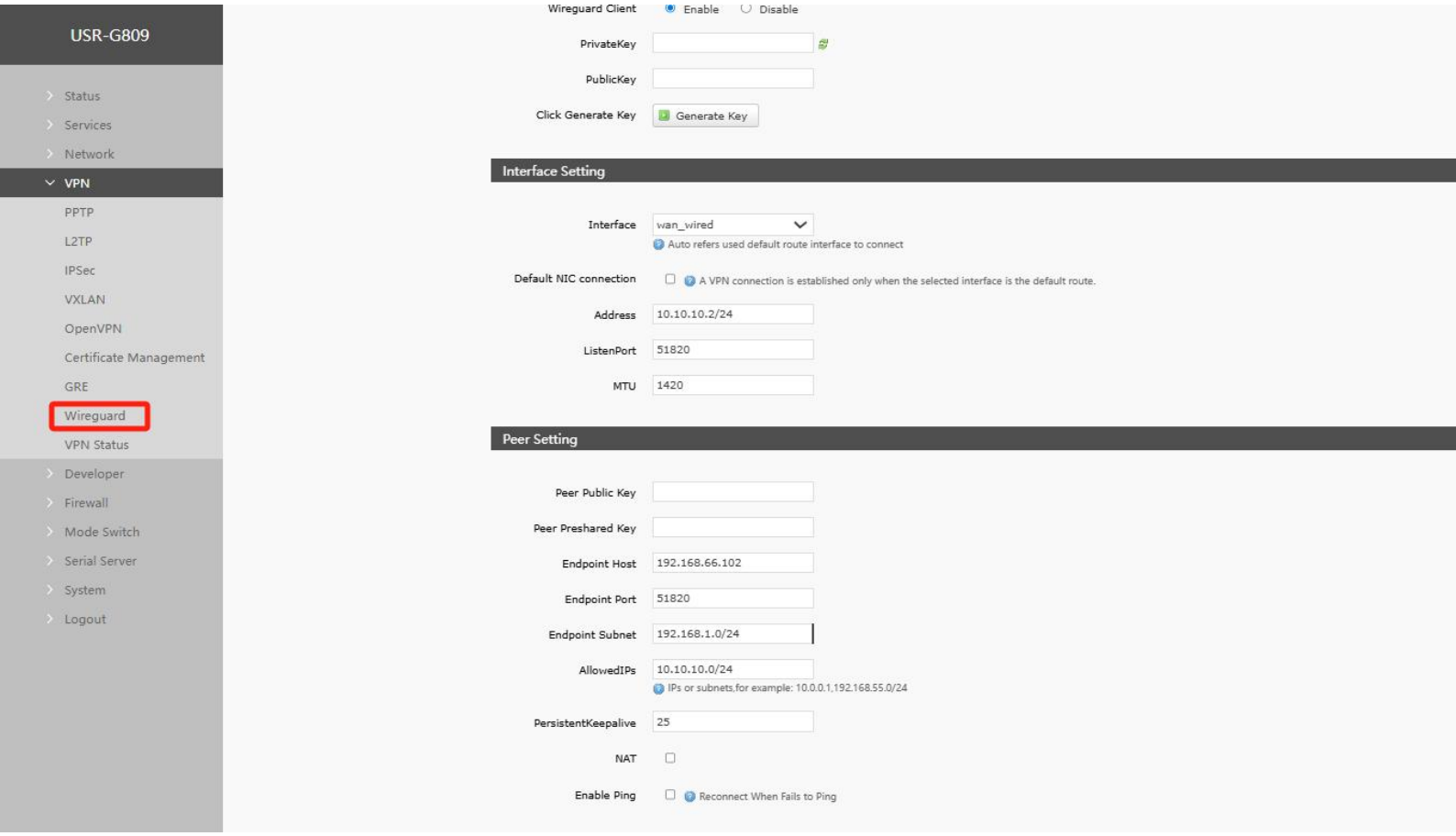


Fig. 110 Router 2 Settings Page

Verify subnet interworking

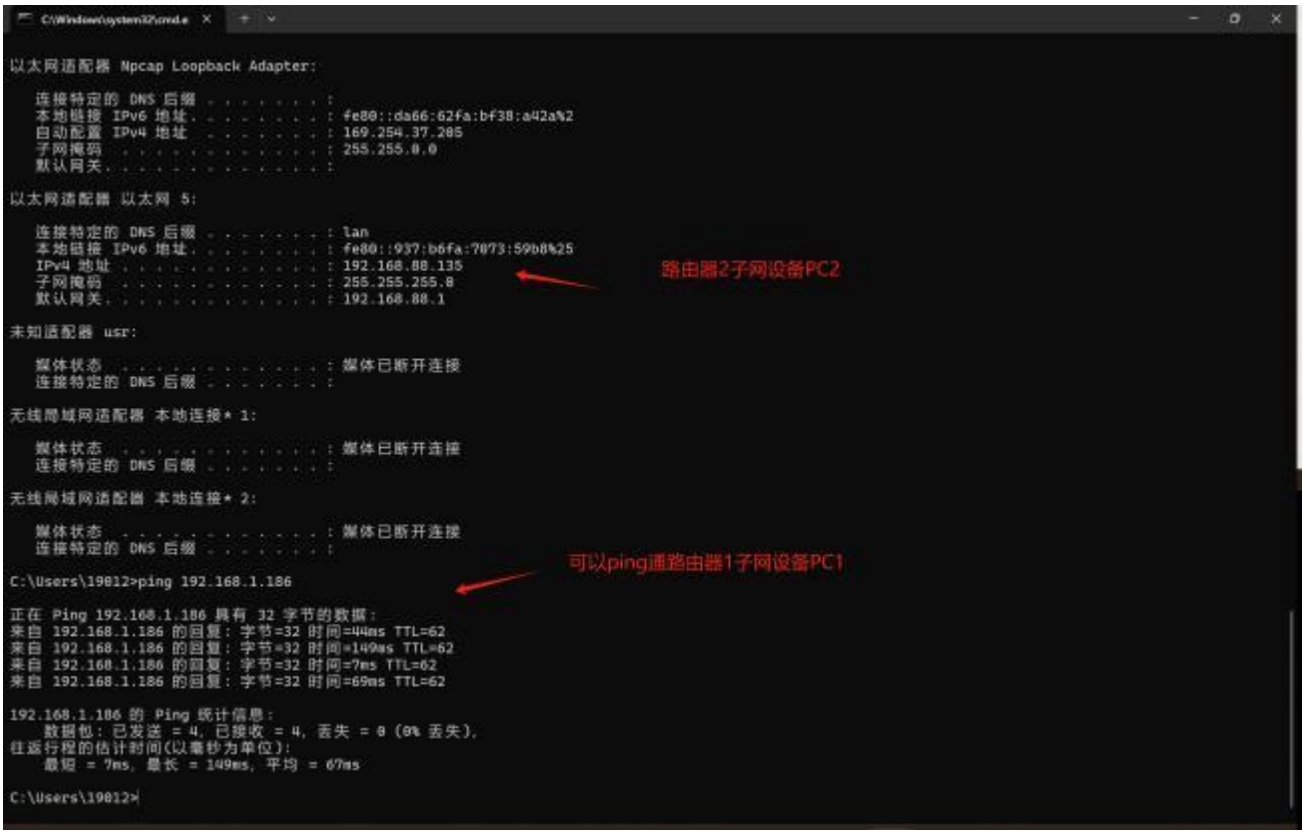


Fig. 111 terminal interworking

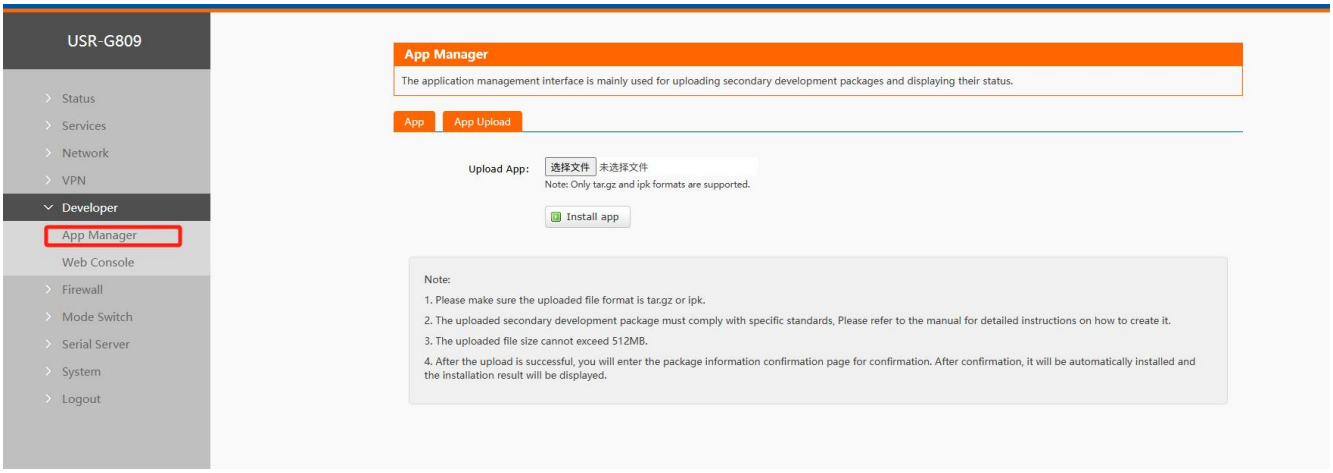
6. Developers

6.1. Application management

Customers can install C programs/Python programs/shell scriptsinto the router through application management to run.

6.1.1. Custom program upload

On the Upload page click Select File-click Install App.



6.1.2. Back-end implementation logic

6.1.2.1. Webpage logic

1. Click upload file, first check whether the file format selected is normal, abnormal pop-up prompt.

2. After the format check is completed, the attribute will be parsed and checked. If the attribute does not conform to the specification, the parsing fails and an error is prompted. The error code is as follows:

1. msg - 1 #Failed to parse the package
2. msg - 2 #Device model does not match
3. msg - 3 #Cannot find the package name when parsing the package
4. msg - 4 #Package already exists
5. msg - 5 #Failed to install the package
6. msg - 6 #Unable to get the uploaded file name
7. msg - 7 #Error in obtaining information from the page during installation
8. msg - 8 #Package installed successfully

Fig. 115 error code

3. After the application is checked, install it into the file system and give it permission to run.

4. After the application is installed, it will not run. After clickingRun on the page, it will call the backend program. The backend program will find the corresponding package according to the package name and then run it in an appropriate way. The running application status is listed as "Running (click Stop)"

5. When stopping the application, after clicking on the page, the backend program will be called. The backend program will find the corresponding package according to the package nameand then stop it in an appropriate way. The status of the stopped application is listed as "Not running (click to run)"

6. To remove an installed app, click the Delete button and the backend program is invoked. The backend program finds the corresponding package according to the package name and deletes all related files and information.

6.1.2.2. Two-pack design logic

1. Supports uploading data packages in ipk and tar.gz formats. ipk is the openwrt native support package format, and tar.gz is a custom package that needs to be created in the specified format.

2. ipk is an openwrt standard package, which is made using ope nWRT standard package method.

3. Tar.gz package for linux executable programs and libraries, which need to contain two files.

① The control file, which contains various information for the installation script to identify the attributes of this package.The information contained is as follows:

```
1. The content of the custom package parsing is as follows:
2. Package: app  #Package name
3. Version: 1.1  #Package version
4. Description: this is test app  #Description, within 32 characters
5. PackageType: <pkg_type>  #lib | app
6. PackageBoot: 1|0  #Whether to auto - start on boot
7. NeedReboot: 1  #If this field exists, it means taking effect after reboot
8. RunCmd: app "param1"  #If starting this program doesn't directly run the package name, need to specify the start command
9. StopCmd: kill app  #If stopping this program doesn't directly kill the package name, need to specify the stop command
10. GetRunStateCmd:  #Command for how to get whether the program is running. If not specified, it will be ps | gre
Package name. There are requirements for the return value of this command. If running, return "state=run"; otherwise, return "state=stop"
```

Fig. 116 control package property file format

②data.tar.gz is an app package in compressed format. The directory structure of this package should be prepared in advance, such as/usr/bin/app1/usr/lib/aaa.so 2, etc.

4. After the package is installed successfully, click Run.

① For IPK, there are three ways to start, the priority is as follows:

I. Check if there is an init.d script, if there is, execute this script restart

II. Check if there isRunCmd attribute, if there is, execute this attribute RunIII. Package name Run (package name must be the same asapp)

② For custom packages, there are two ways to start, with the following priorities:

I. Check if there isRunCmd attribute, if there is, execute this attribute RunII. Package name Run (package name must be the same asapp)

5. Package is running, click Stop when:

① For IPK, there are three ways to stop, the priority is as follows:

I. Check if there is an init.d script, if there is, execute this script stop

II. Check if there isStopCmd attribute, if there is, execute this attribute RunIII. package name stop (package name must be the same asapp)

② For custom packages, there are two ways to start, with the following priorities:

I. Check if there isStopCmd attribute, if there is, execute this attribute RunII. package name stop (package name must be the same asapp)

6. Get program running status:

① Check whether GetRunStateCmd attribute exists. If yes, call the command specified by this attribute to obtain it. The return value of this command is required. If running,return "state=run", otherwise return "state=stop".

②Check whether it is runningby package name>(package name mustbe the sameas app

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

7. start automatically when the system

① After the system is started, it will traverse the installed packages, find the ones that need to be started, and then run them using the above operation logic.

6.1.2.3. CAPI Library

For details, please refer to: 2D Toolkit\C Language 2D API-demo + Dynamic Library + Compiler Toolchain\op_usr_basic. tar. gz\libusr_basic\include\usr_basic. h file description

6.1.2.4. Python API Library

For details, please refer to: Two-Open Toolkit\Python Two-Open API\python Two-Open Interface Description

6.1.2.5. Two-way kit

1. The two-open toolkit contains three dome two-open files.

①usr_oledtest_1_ipq.ipk:

OLED two-on program, after installation and operation, willdisplay the following contentson the O

Hello World Hi OLED
Can be executed after logging in to the web console

usr_oledtest"<Custom Page>""Lines>"<Contents>"ortest_oled.sh"<Custom Page>""Lines>"<Contents>"
such as

usr_oledtest "2" "1" "aaa" AAA will be displayed on the first line of customization page 1

②usr_apptest_1_ipq.ipk:

will always print =====<<<Hello>>=== ======

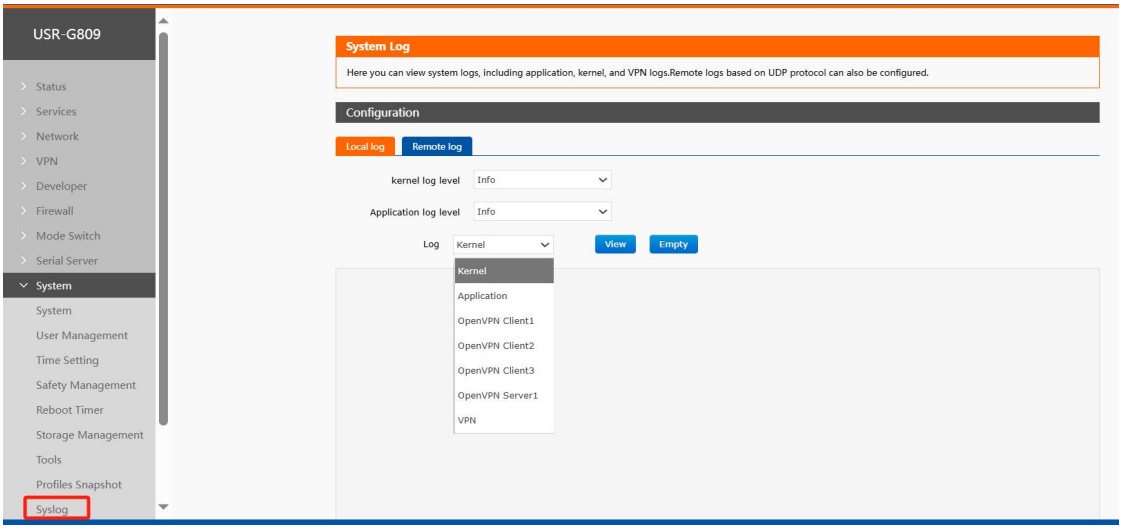


Fig. 117 print content

③python_demo_cmdtest.tar.gz:

After installation and operation, continuously print the IP of WAN1 network card to the file/tmp/python_demo (Note: insert WAN1 network cable, wait for WAN1 network card to have IP and test)



Fig. 118 Print WAN1IP to File

2. C language cross-compiler toolchain
3. Python 2 Open API
4. C language two open API-demo+ dynamic library + compiler tool chain

6.2. Web console

Use account/password: root/root to log in to the router management background to debug the second open program.

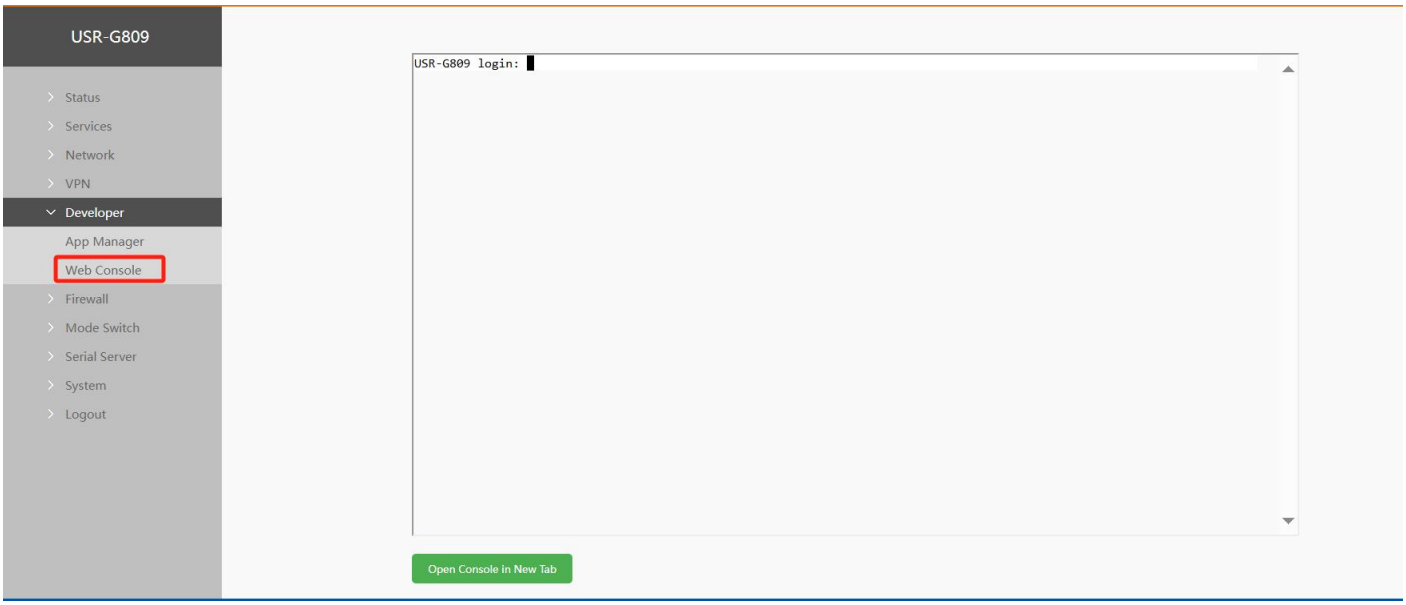


Fig. 119 web console

7. Firewall

7.1. Basic setup

Default to two firewall rules.

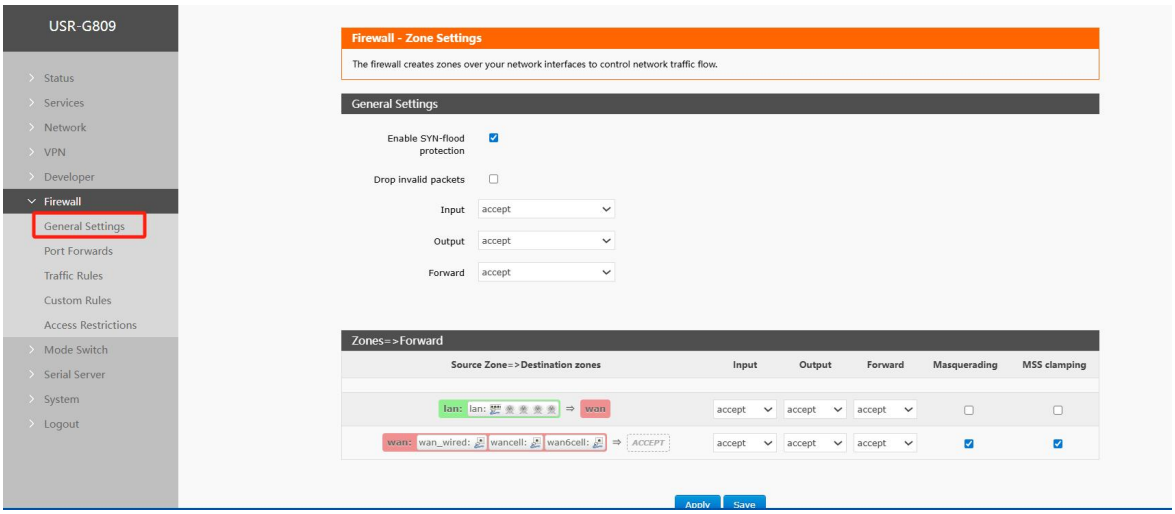


Fig. 120 Firewall Settings Page

<Noun introduction>

- inbound:packets accessing router IP
- outbound:packets to be sent by router IP;
- Forwarding: forwarding data between interfaces without routing itself;
- IP dynamic disguise: only meaningful for WAN port and 4Gport, IP address disguise when accessing external network;
- MSS clamp: limits the message MSS size, usually1460.

<Rule 1>

- LAN port to wired WAN port inbound, and forwarding,are receiving;
- If a data packet comes from the LAN port and is going to access the WAN port, then this rule allows the data packet to beforwarded from the LAN port to the WAN port, which is forwarding;
- You can also open the router web page under the LAN port, which belongs to "inbound";
- The router itself connects to the external network,such as synchronizing time, which is "outbound."

<Rule 2>

- Wired WAN port and 4Gport, accept "inbound", accept "outbound", allow "forwarding";
- If there is an "inbound" packet,such as someone trying tolog into a router web page from a WAN port, it will be allowed;
- If there is an "outbound" packet,such as a router accessing an external network through a WAN port or a 4Gport, this action is allowed;
- If there is a "forward" packet,such asa packet from the WAN port that wants to be forwarded to the LAN port, this action is allowed.

7.2. Communication rules

Communication rules can selectively filter specific Internet data types and block Internet access requests, enhancing network security through these communication rules.Firewall has a wide range of applications. The following is a brief introductionto several common applications.

name	describe	default parameters
start using	Display means enabled Display means disabled	start using
name	This rule name, character type	-
limit-address	Limit IPv4 addresses	IPv4 addresses only
agreement	The protocol type of the restriction rule can be selected as TCP+UDP/TCP/UDP/ICMP.	TCP+UDP
Match ICMP type	Matching ICMP rules, select any	Any
source region	Data flow source area, optional: arbitrary area, WAN ,LANLAN: indicates subnet access to external network rules WAN: Indicates rules for accessing an intranet from an external network	LAN
source MAC address	Source MAC required to match rule null: means match all MAC Note: To match the source MAC address, set the source IP address to null	empty
source IP address	Source IP required to match rule null: means match all IPs Note: To match the source IP address, set the source MAC address to null	empty
source port	Source port to match rule null: means match all ports	empty
Target area	Data flow destination area, optional: arbitrary area, WAN ,LANLAN: indicates subnet access to external network rules WAN: Indicates rules for accessing an intranet from an external network	WAN
Target address	Access destination IP address null: represents all addresses	empty
Target port	Access target port number null: represents all	empty
movement	When receiving such data packets, you can choose: discard, accept,reject, no action Drop: Packets received with this rule will be dropped Accept: Packets received with this rule will be accepted Reject: Packets received with this rule will be rejected No Action: No action will be taken when receiving this rule packet	take in

7.2.1. IP address blacklist

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

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

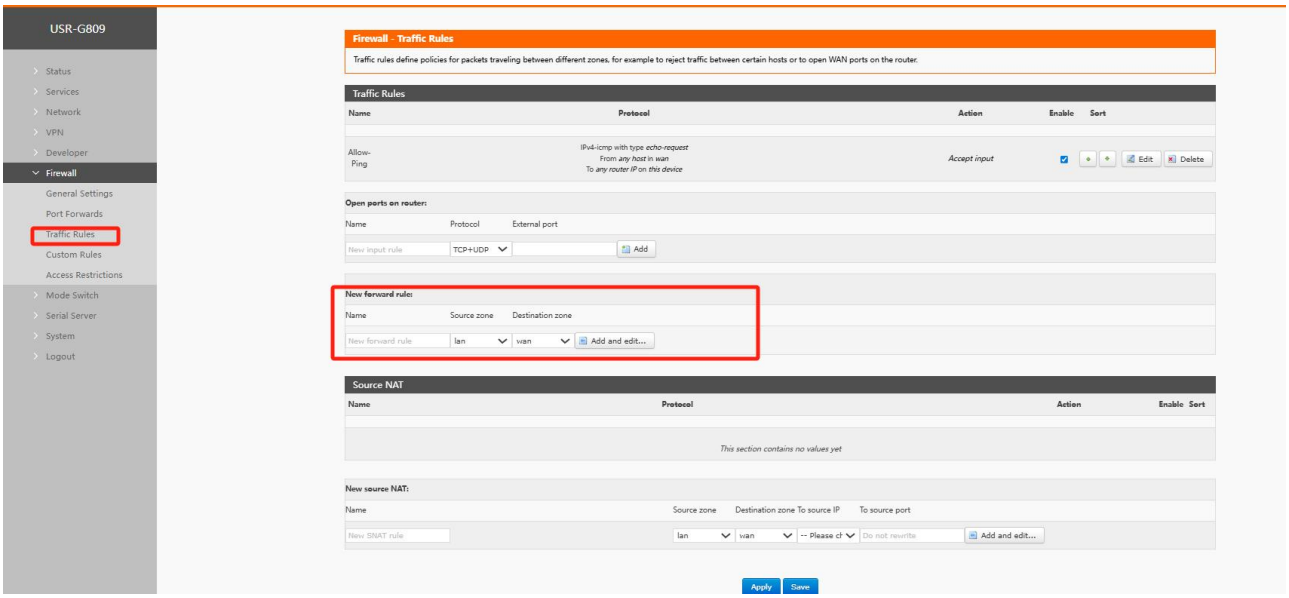


Fig. 121 Firewall Blacklist Figure 1

In the jump page, select lan for the source area,and select all for the source MAC address and source address (if it is a specific IP that only restricts specific IPs in the local area network from accessing the external network,you need to fill in the IP address or MAC address here),as shown in the following figure:

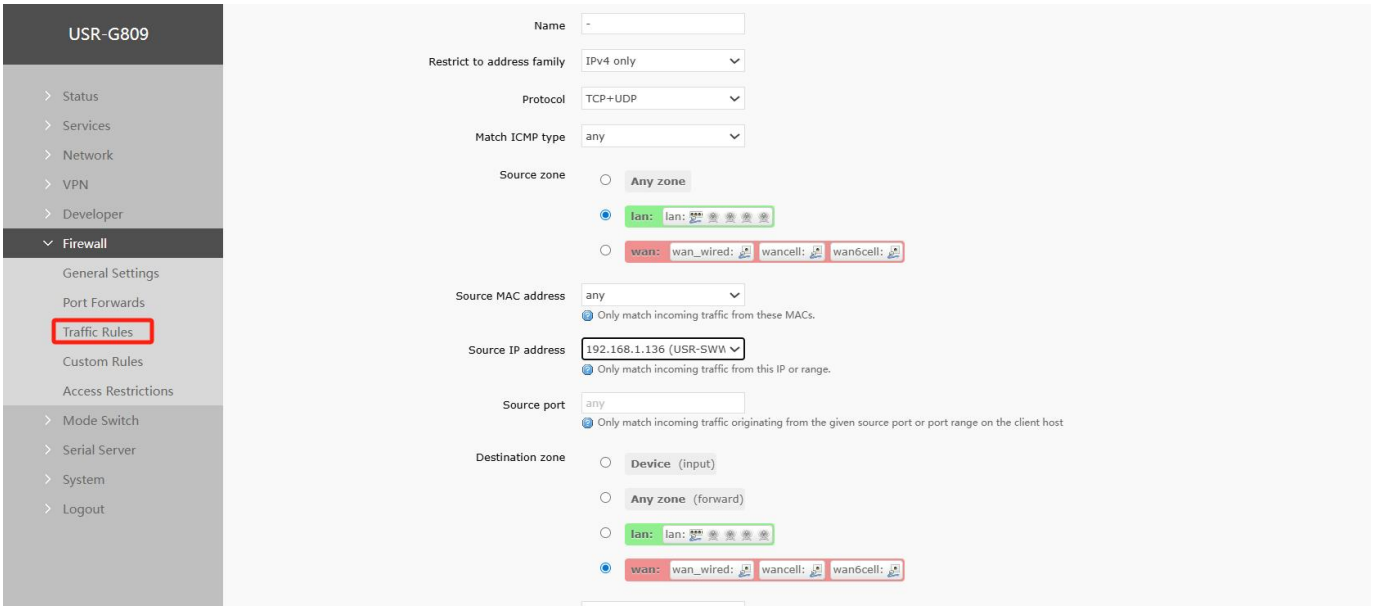


Fig. 122 Firewall Blacklist Figure II

Select WAN in the target area, fill in the IP that is prohibited from accessing the target address, select "Reject" for the action,and click "Apply" after setting. As shown below.

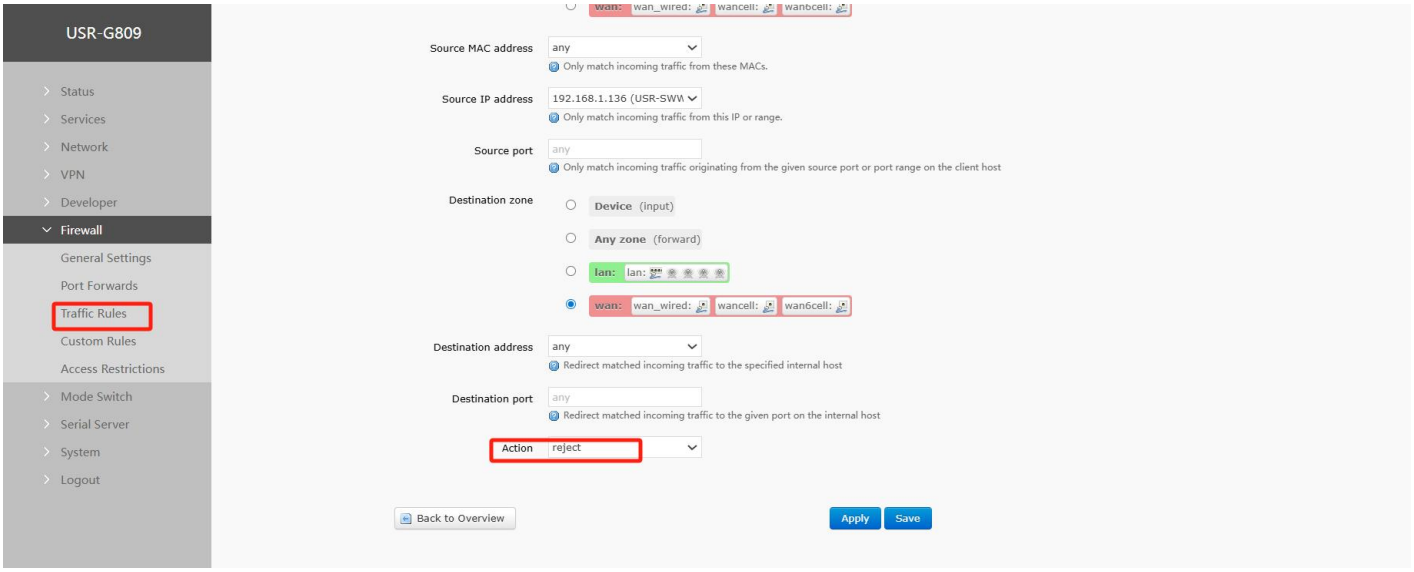


Fig. 123 Firewall Blacklist Figure 3

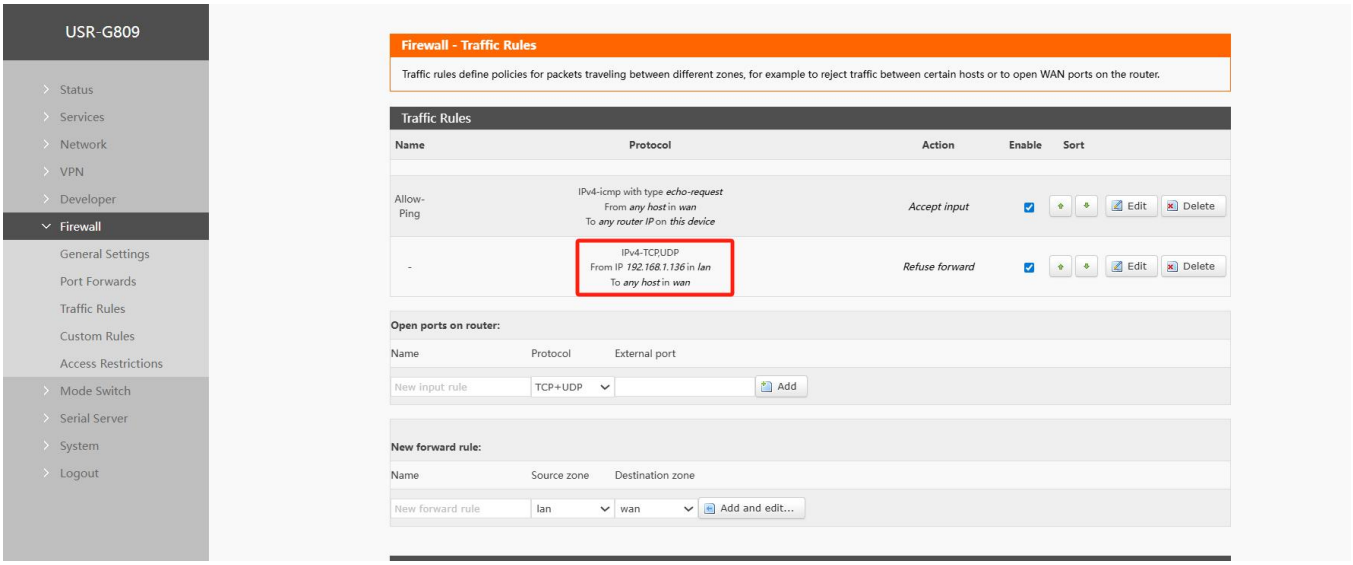


Fig. 124 Firewall Blacklist Figure 4

After this setting is completed, the blacklist function is realized.That is, the IP of the subnet device is 192.168.1.136

7.2.2. IP address whitelist

First add the communication rule of 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.

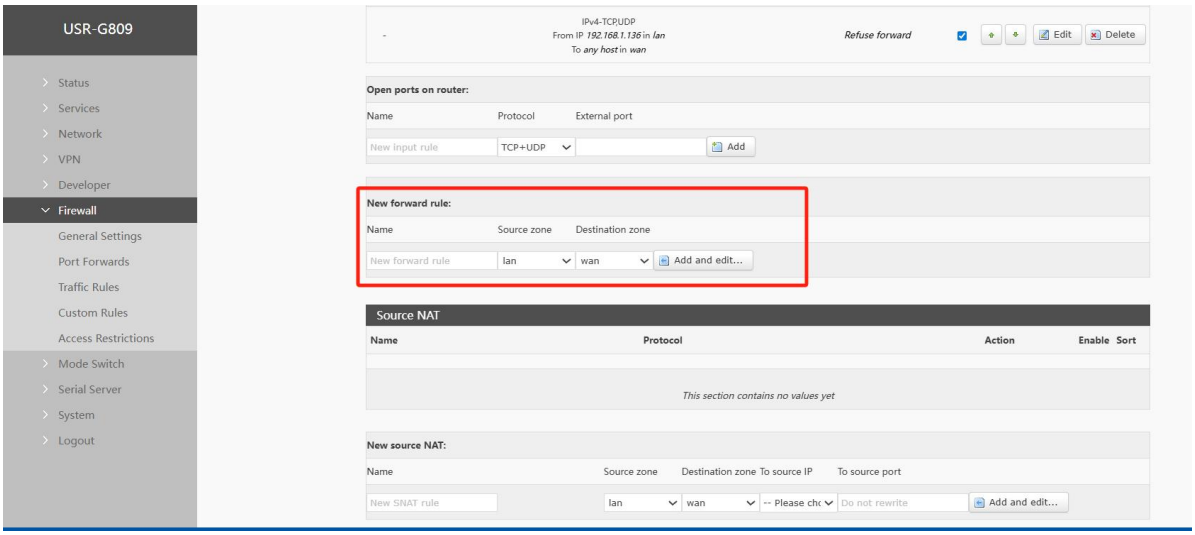


Fig. 125 Firewall Whitelist Figure 1

In the jump page, select lan for the source area,and select all for the source MAC address and source address (if it isa specific IP that allows a specific IP in the local area network to access the external network,you need to fill inthe IP address orMAC address here),as shown in the following figure

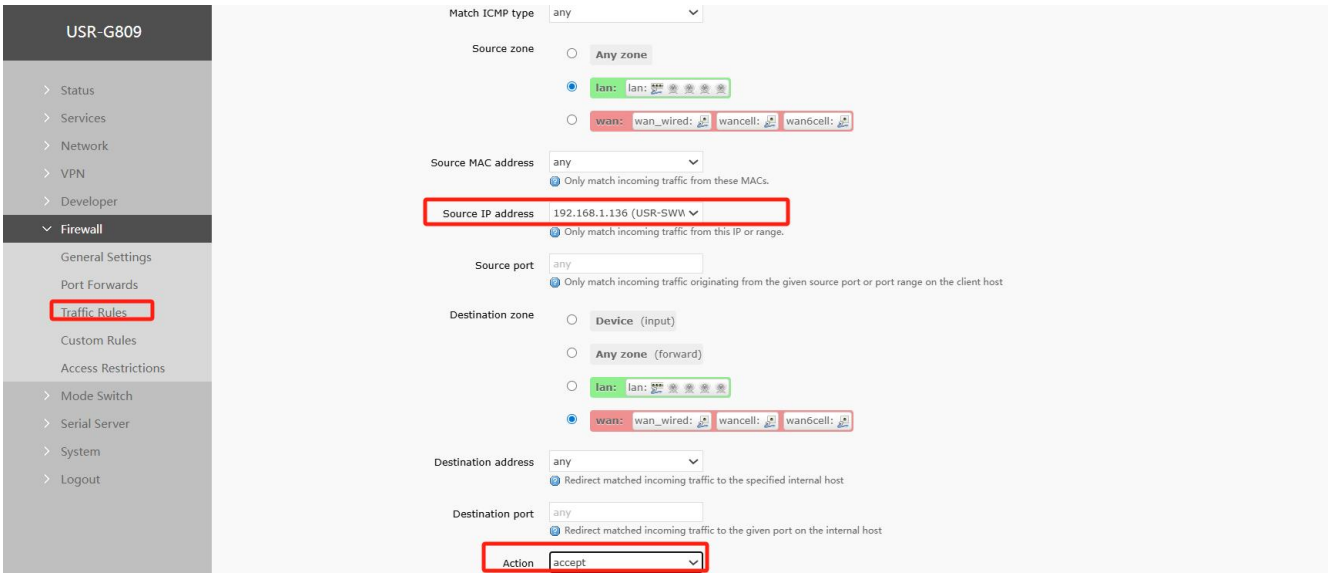
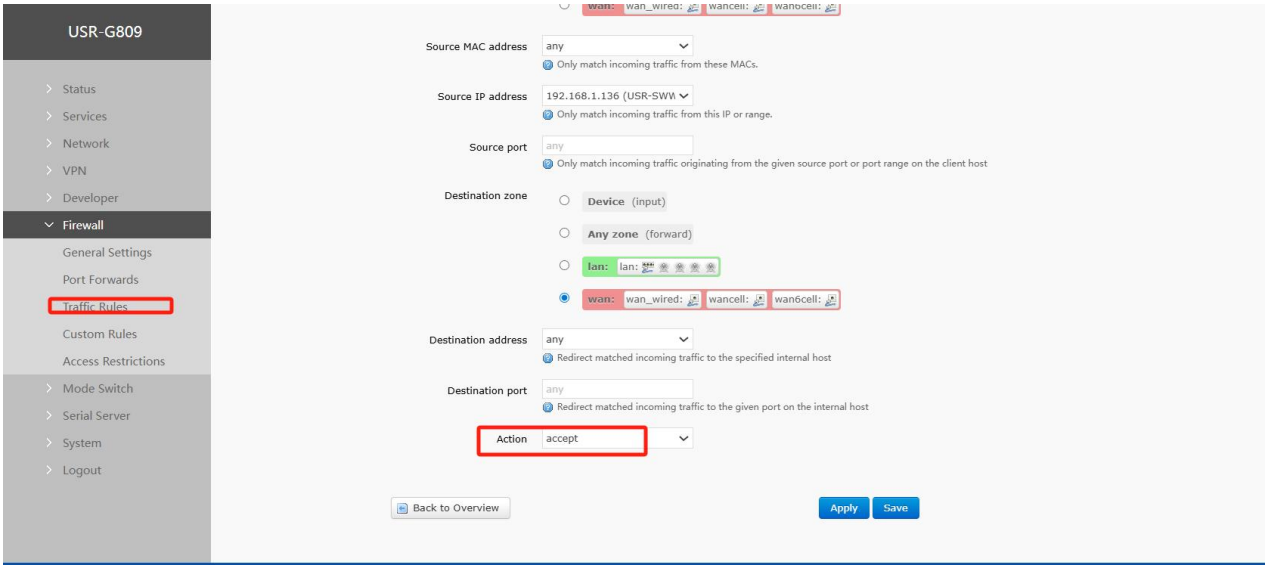


Fig. 126 Firewall Whitelist Figure II

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



Next, set a rule that all communications are rejected, with the source address set to "All", the destination address set to "All", and the action selected "Reject". Notice the order of the two rules. The rule of permission must be first and the rule of refusal must be second. After the overall setting is completed, as shown in the following figure

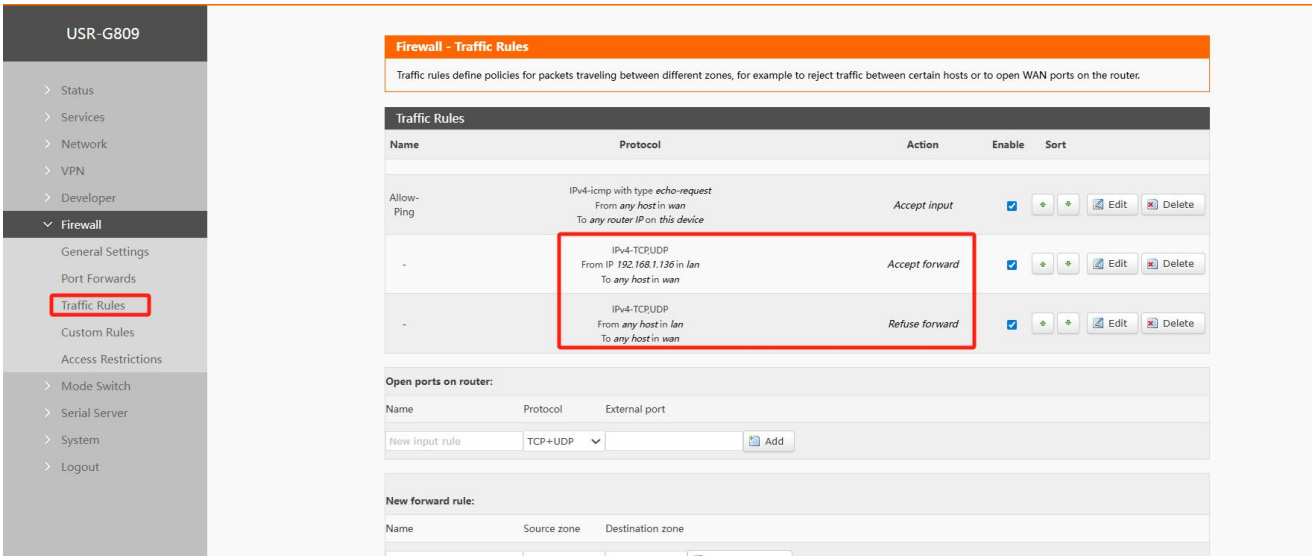


Fig. 128 Firewall Whitelist Figure 3

7.3. Nat function

7.3.1. IP address masquerading

IP address disguise: converts the source IP of the outgoing packet into the IP address of an interface of the router. As shown in the figure, if IP dynamic disguise ischecked, the system will modify the source IP address of the outgoing packet to the IP address of the WAN port.

Note: IP Dynamic Camouflage and MSS Clamp must be enabled on WAN interfaces, and IP Dynamic Camouflage and MSS Clamp must not be enabled on LAN interfaces.

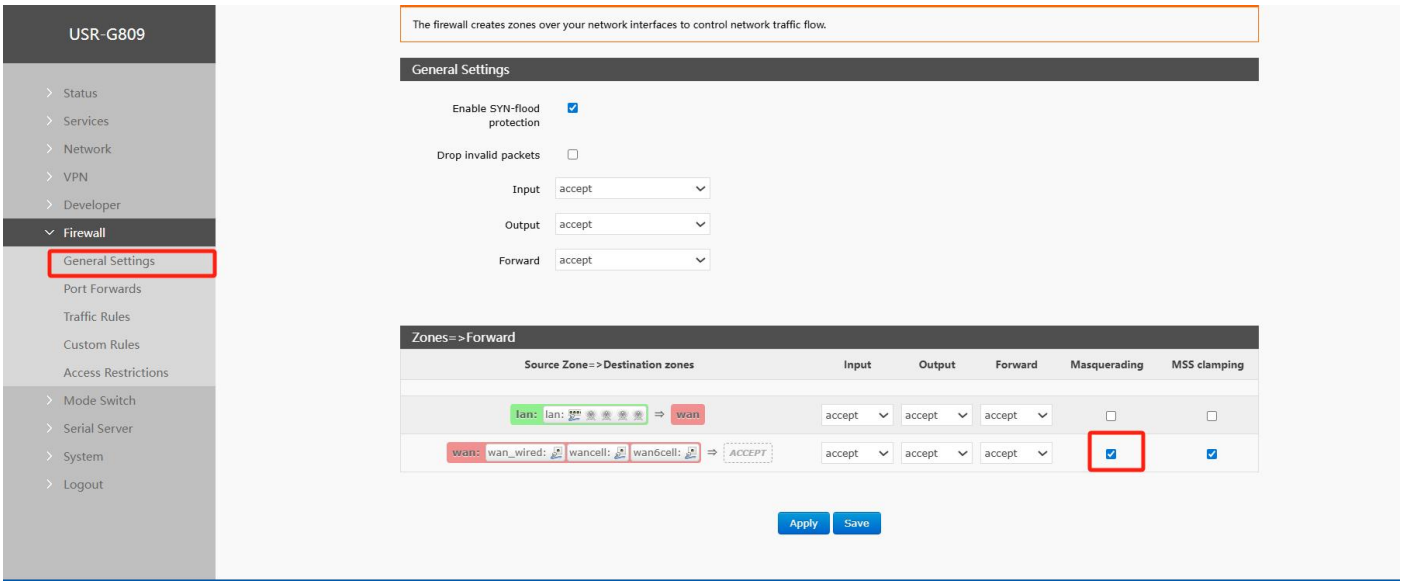


Fig. 129 IP Address Disguise Settings

7.3.2. SNAT

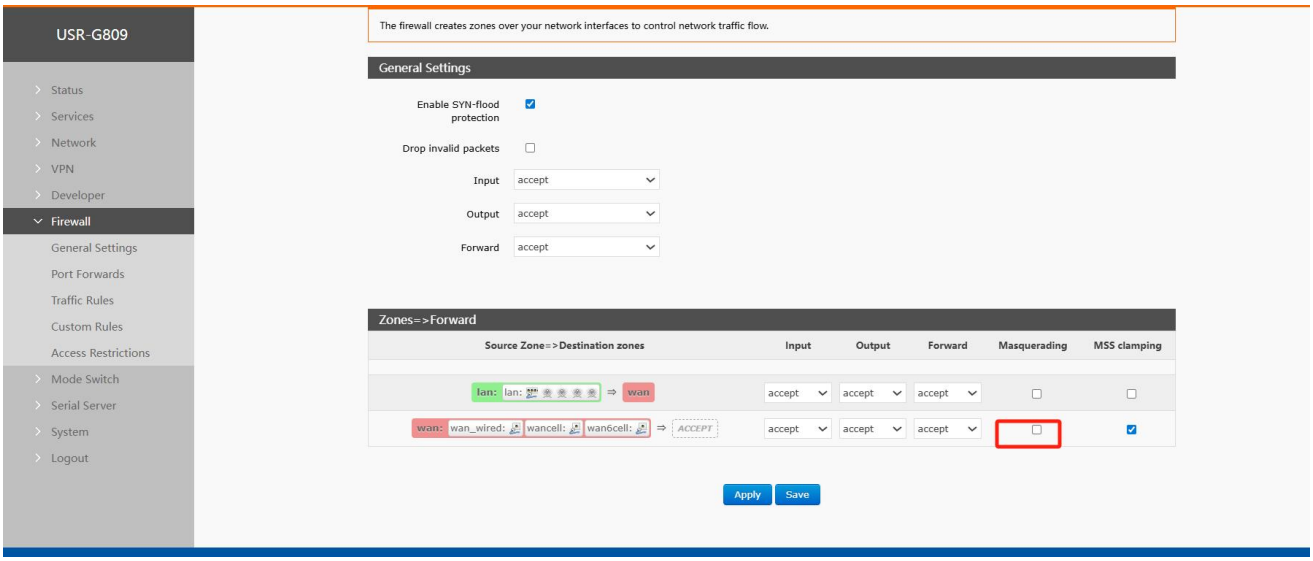
outbound source IP translation capability.

table 41 SNAT parameter table

name	describe	default parameters
enable button	Display indicates enabled status Display indicates disabled state	start using
name	Name of this firewall rule	-
agreement	Can be set: TCP+UDP/TCP/UDP/ICMP	TCP+UDP
source IP address	SourceIPs that need to match inbound traffic are null to match all source IPs	empty
source port	Source ports that need to match inbound traffic are null to match all source ports	empty
destination IP	Destination IPs that need to match inbound trafficare null to match all destination IPs	empty
Target port	Destination port to match inbound traffic required or null to match destination port	empty
SNAT IP address	Change the source address of matching traffic to this address	Custom IP

SNAT port	Change the source port for matching traffic to null for this port to use the source port	empty

Source NAT is a special form of packet disguise that changes the source address of packets leaving the router. When used,theIP dynamic disguise of the wan port is first closed.



Set Source NAT

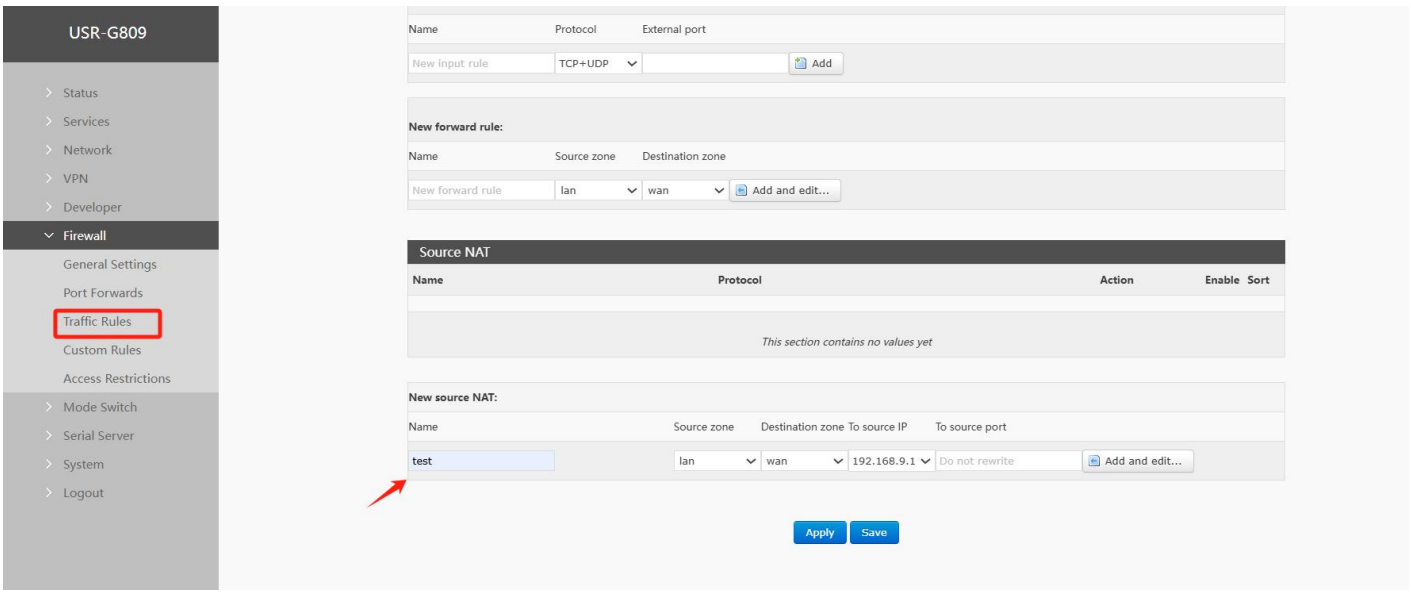


Fig. 130 NAT Settings 1

Click Add and Edit

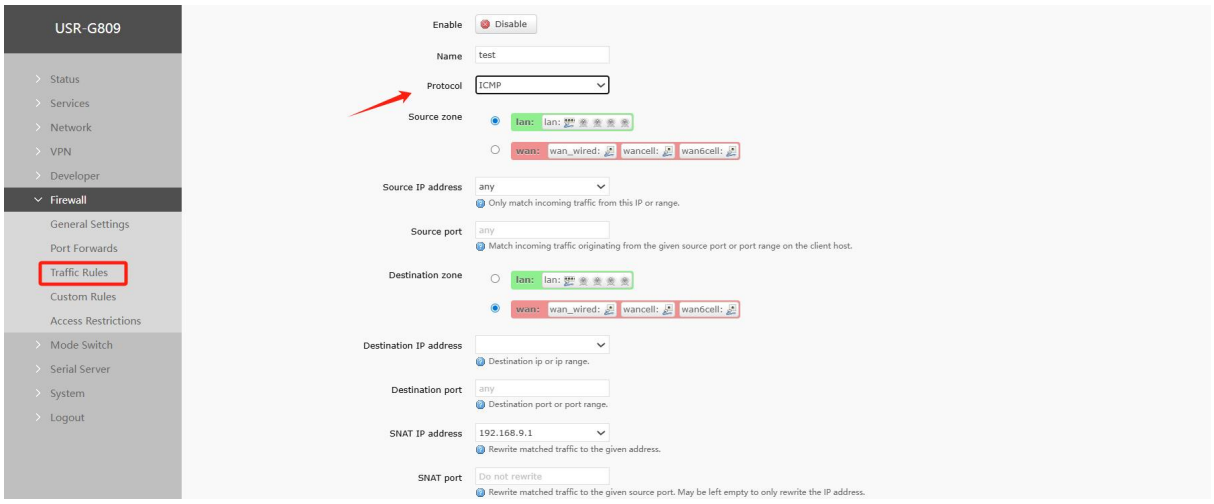


Fig. 131 NAT Settings II

If source IP, source port, destination IP and destination port are not filled in, all IPs and ports are defaulted.Save after setting.

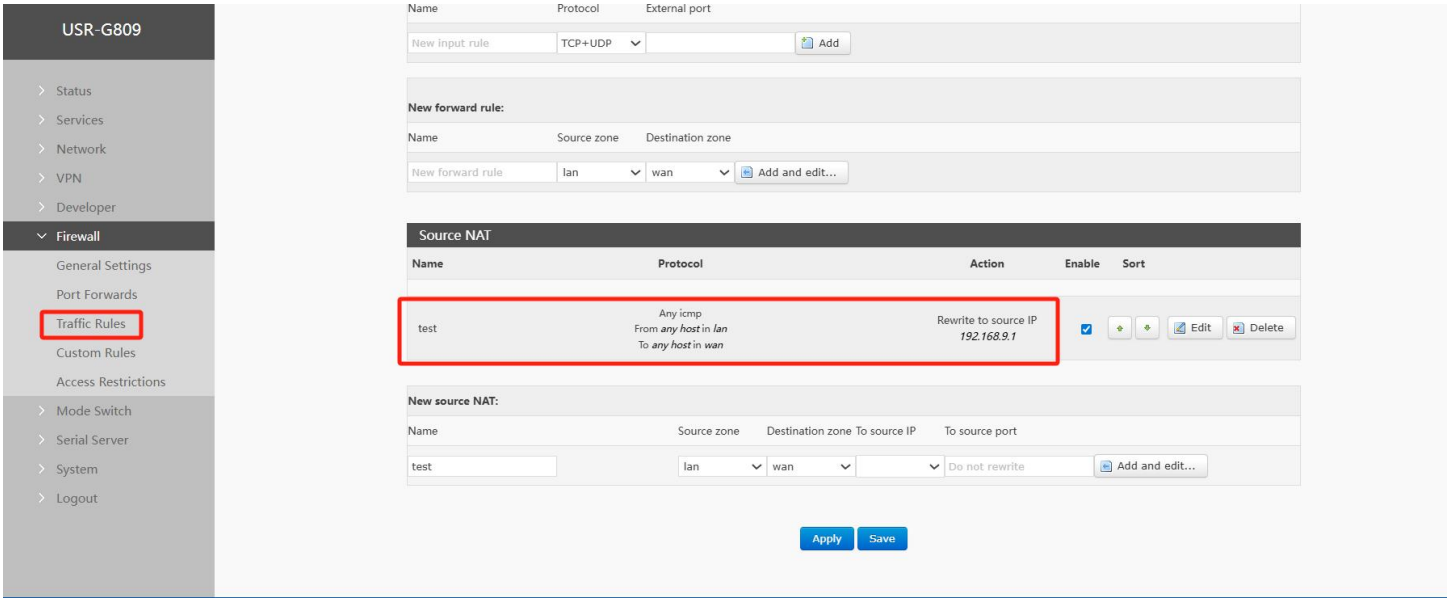


Fig. 132 NAT setting three

Change the source IP address of packets leaving the router to192.168.9.1as shown in the figure. As can be seen,the source address of ICMP packets to192.168.13.4

192.168.9.1instead of192.168.1.114.

Verify that the device (IP: 192.168.1.114)under the router ping the PC(IP: 192.168.13.4)under the same switch as the router.The data captured on the PC is as follows:

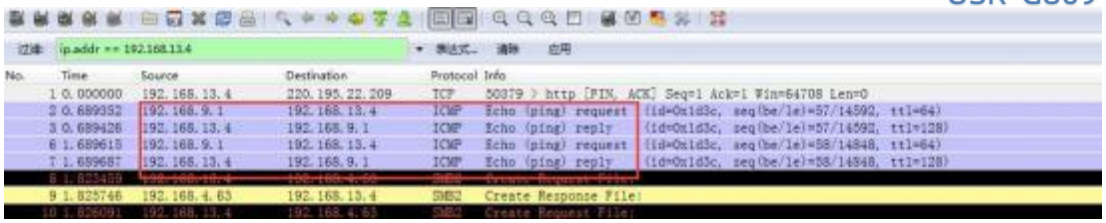


Fig. 133 NAT authentication

7.3.3. Port forwarding

Port forwarding allows computers from the Internet to access computers or services within a private local area network, i.e., map a specified port of a WAN port address to a host on the intranet.

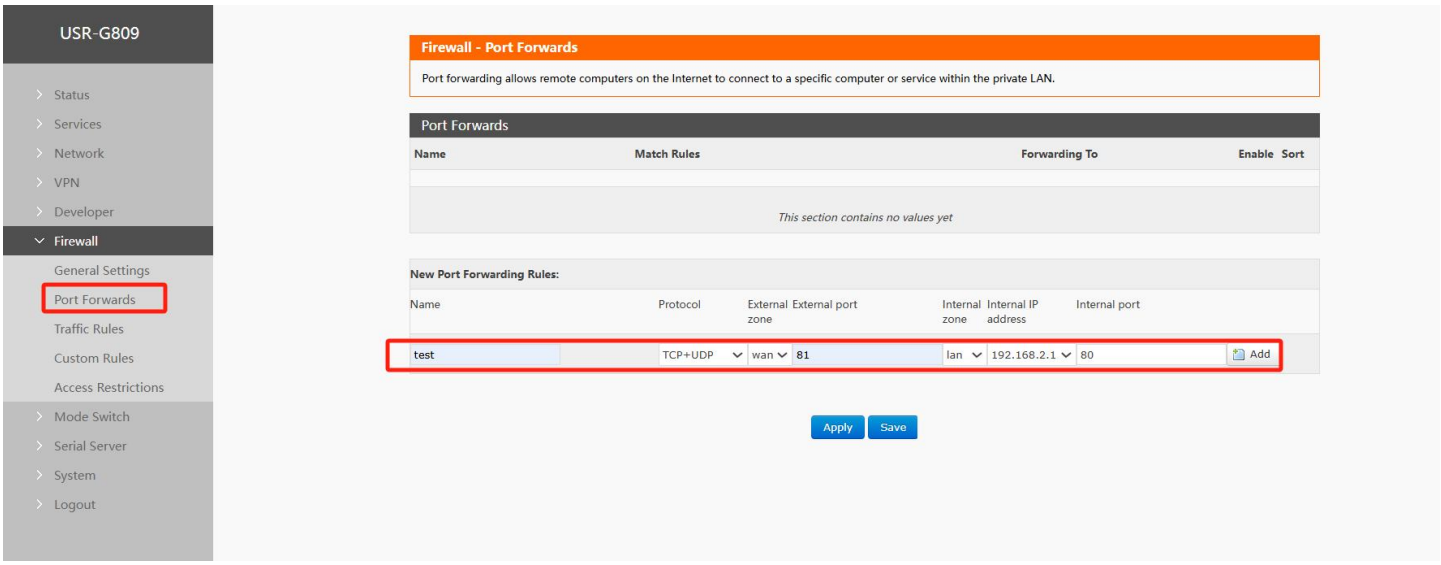


Fig. 134 Port Settings Page 1

- After setting the forwarding rule, click the Add button on the right, and then this rule will be displayed in the rule bar;
- Then click on the "Apply" button in the lower right corner to make the settings take effect;
- The following settings,192.168.2.1:80,are the router's own web server. If we want to access a device in the local area network from the external network, we need to set the mapping from the external network to the internal network,for example, set the external network port to 81,the internal network IP to192.168.2.1, and the internal network port to80;
- When we access port 81 from the WAN port, the access request will be redirected to192.168.2.180.

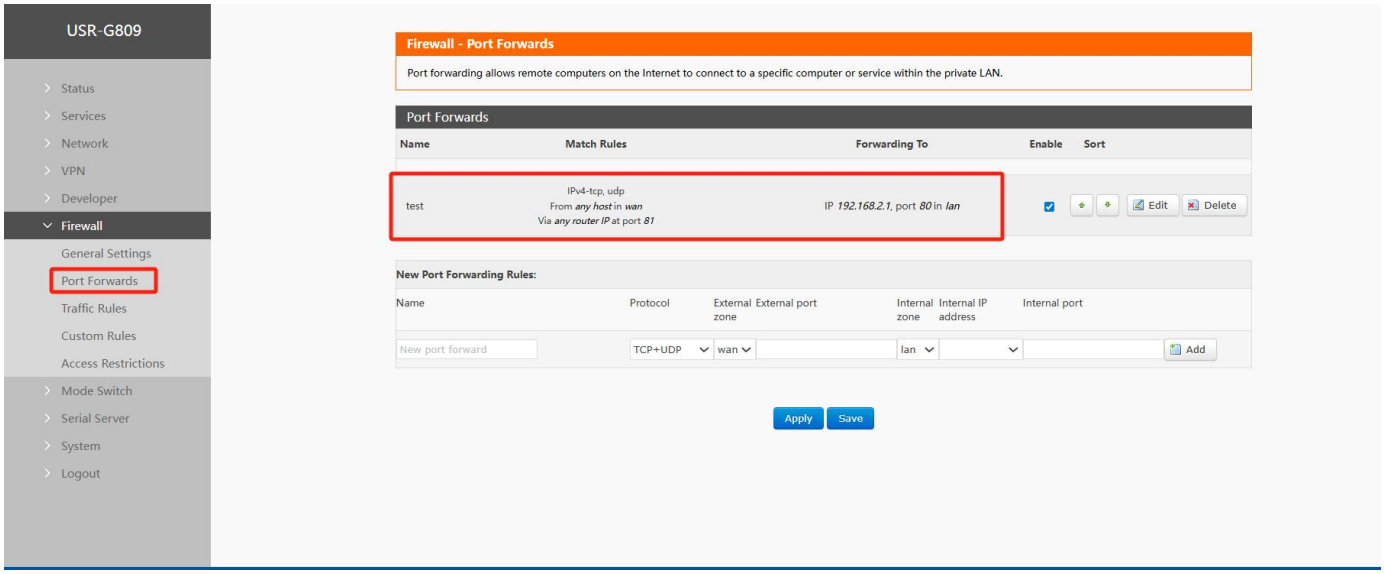


Fig. 135 Port Settings Page II

table 42 Port forwarding parameter table

name	describe	default parameters
name	Name of this port forwarding rule, character type	empty
agreement	Protocol type, settable: TCP+UDP/TCP/UDP	TCP+UDP
exterior zone	Includes Wired WAN, 4G, VPN	wan
external port	Single port or port range can be set, for example: 8000- 9000Description:DMZ function	empty
interior region	router subnet area	lan
internal IP	Router LAN Area IP Address	empty
internal port	Single port or port range can be set, for example: 8000- 9000Description:DMZ function	empty

7.3.4. DNAT

outbound destination address translation.

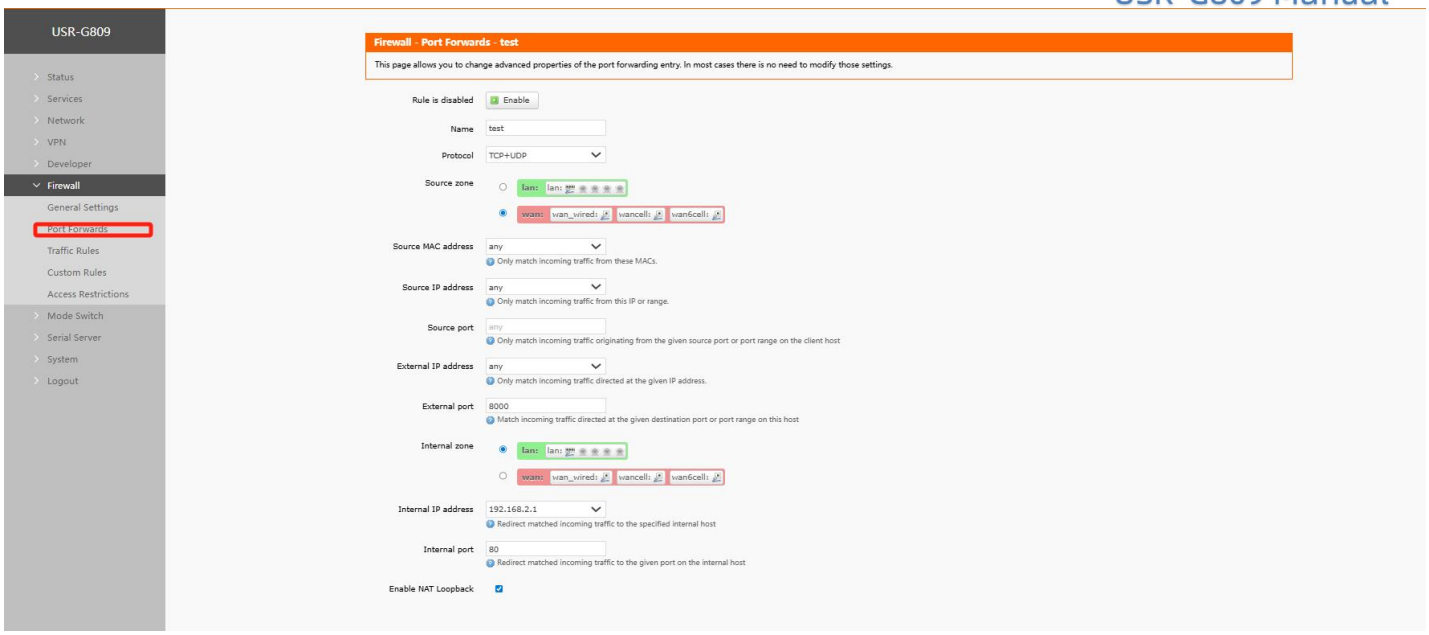


Fig. 136 configuration interface

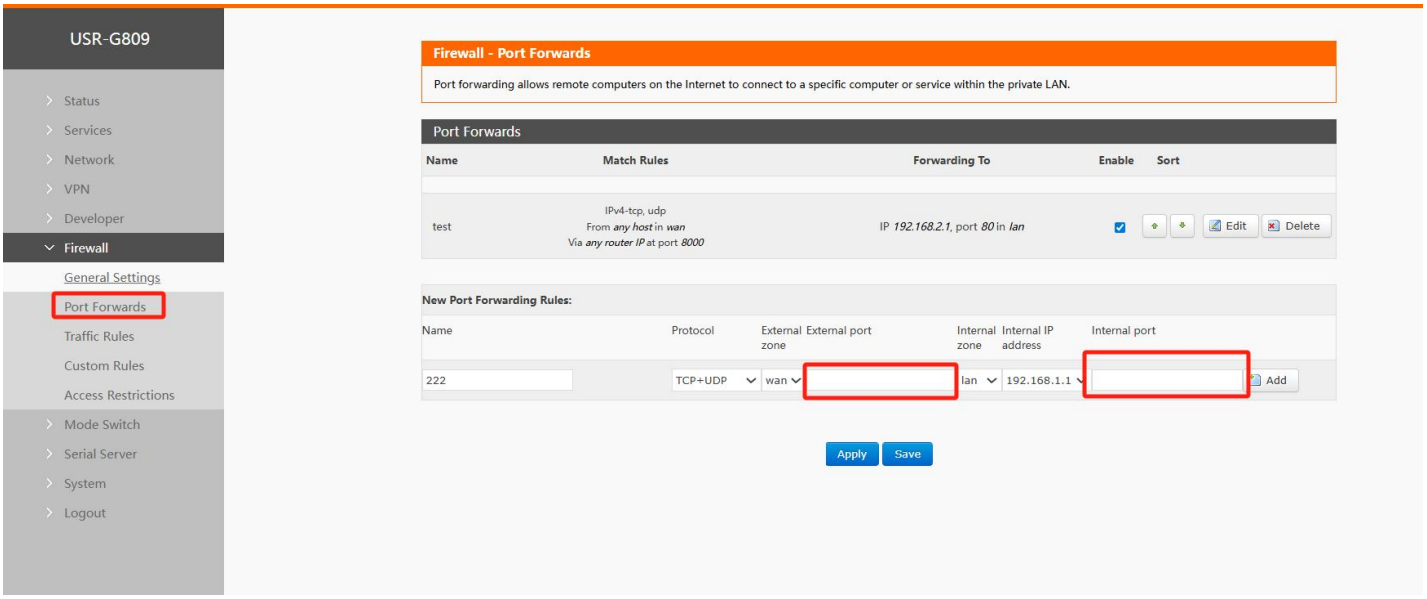
table 43 configuration parameters

name	describe	default parameters
enabled	Enable: Disable Close: Enable	enabled
name	Custom name for this rule	empty
source region	Data inbound zone selection	Wan
source MAC address	Source MAC address filtering	all
source IP address	Source IP address filtering	all
source port	Source port filtering on inbound	all

external IP address	Destination IP address	all
external port	Destination port on inbound	empty
interior region	Exit area after redirection	Lan
internal IP address	Redirect outbound destination address	empty
internal port	Destination port when redirecting outbound	empty
Enable NAT loopback	Check Enable NAT loopback	check

7.3.5. NAT DMZ

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



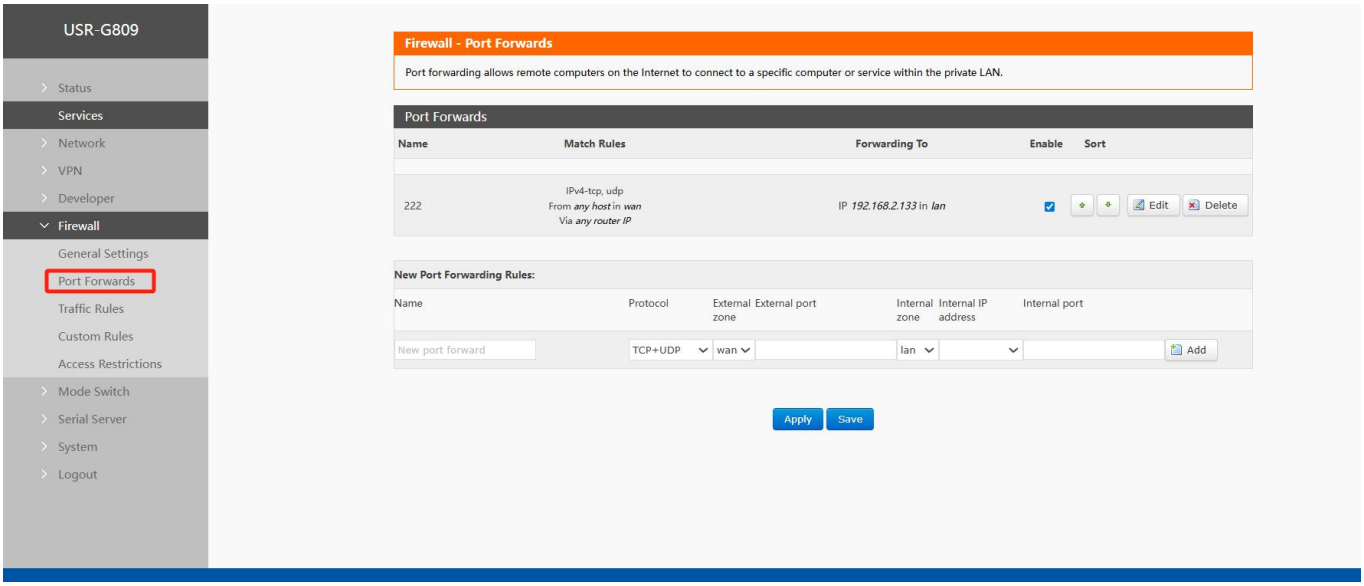


Fig. 138 DMZ Settings II

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

<Attention>

- Port mapping and DMZ cannot be used simultaneously.

7.4. Access restriction

Access restriction restricts access to specified domain names. Blacklist and whitelist settings for domain names and addresses are supported. When Blacklist is selected, devices connected to the router cannot accessdomain names in Blacklist, while other domain names and addresses can be accessed normally. When Whitelist is selected, devices connected to the router cannot accessdomain names andaddresses normally except domain names and addresses set in Whitelist.Multiple entries can be set in Blacklist and Whitelist. This feature is disabled by default.

7.4.1. Domain name blacklist

First, select the blacklist in the method option, click Add to enter the name of the rule and the correct domain name, and then click Save. The rule will take effect immediately, and devices connected to the router will not be able to access the domain name. If Blacklist is selectedand no rule is added, the default Blacklist is empty, i.e. all domain names are accessible. As shown in the figure, except Baidu, other do main names can be accessed normally.

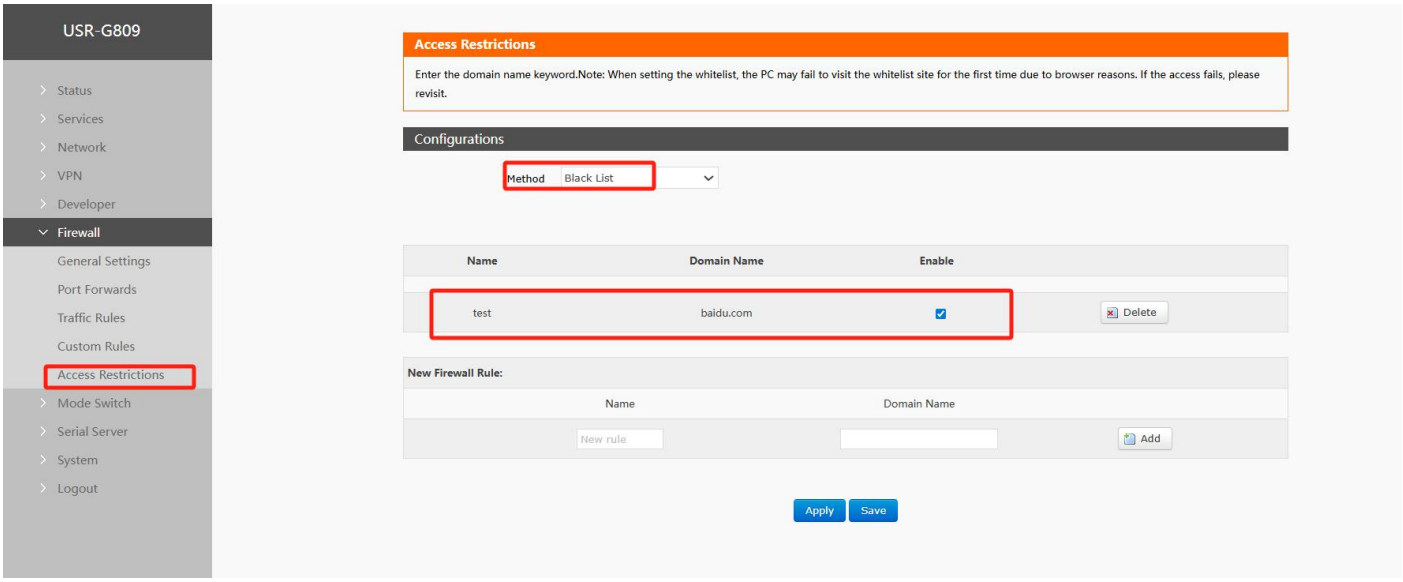


Fig. 139 Domain name blacklist

7.4.2. Domain name white list

First, select the white list in the method option, click Add to enter the name of the rule and the correct domain name, and then click Save. The rule takes effect immediately. Except for the domain name in the rule, other domain names cannot be accessed by the devices connected to the router.If whitelist is selectedand no rule is added, the default whitelist is empty, that is, all domain names are inaccessible. As shown in the figure, the device can access Baidu.

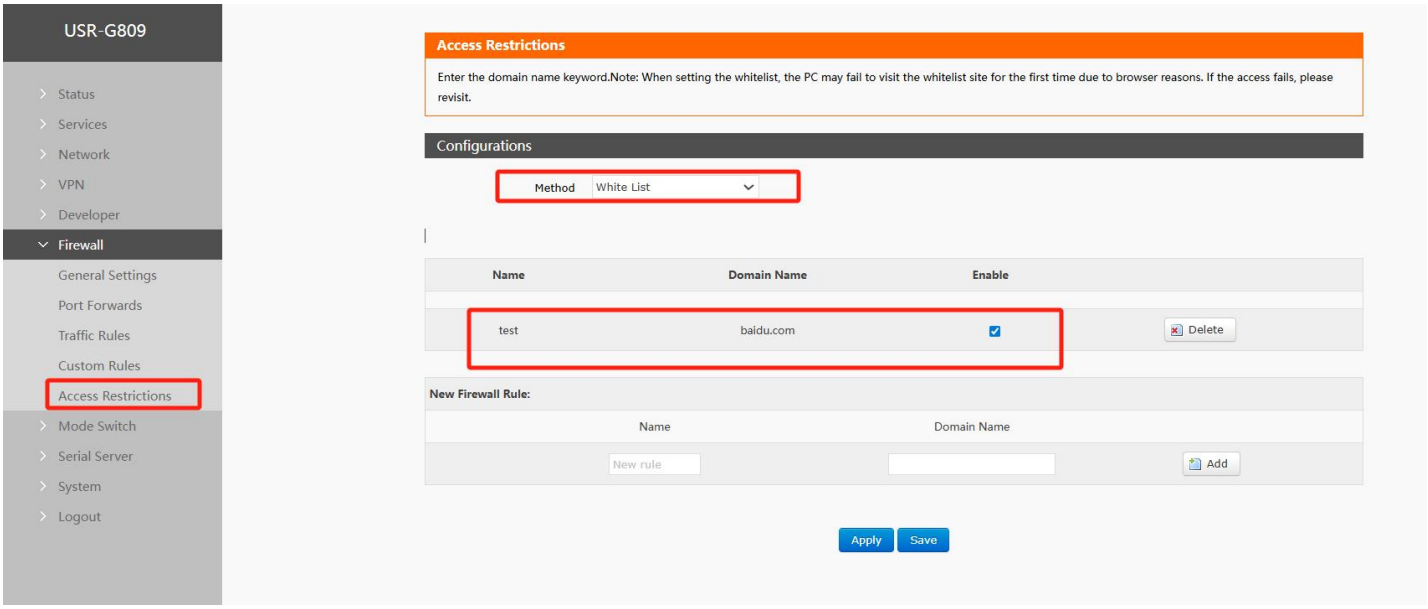


Fig. 140 domain name white list

7.5. custom rules

When the above firewall settings cannot meet the security requirements, you can enter firewall commands through a custom firewall.

Note: Please enter firewall commands correctly under the guidance of operation and maintenance professionals or technical support, otherwise it may lead to abnormal equipment.

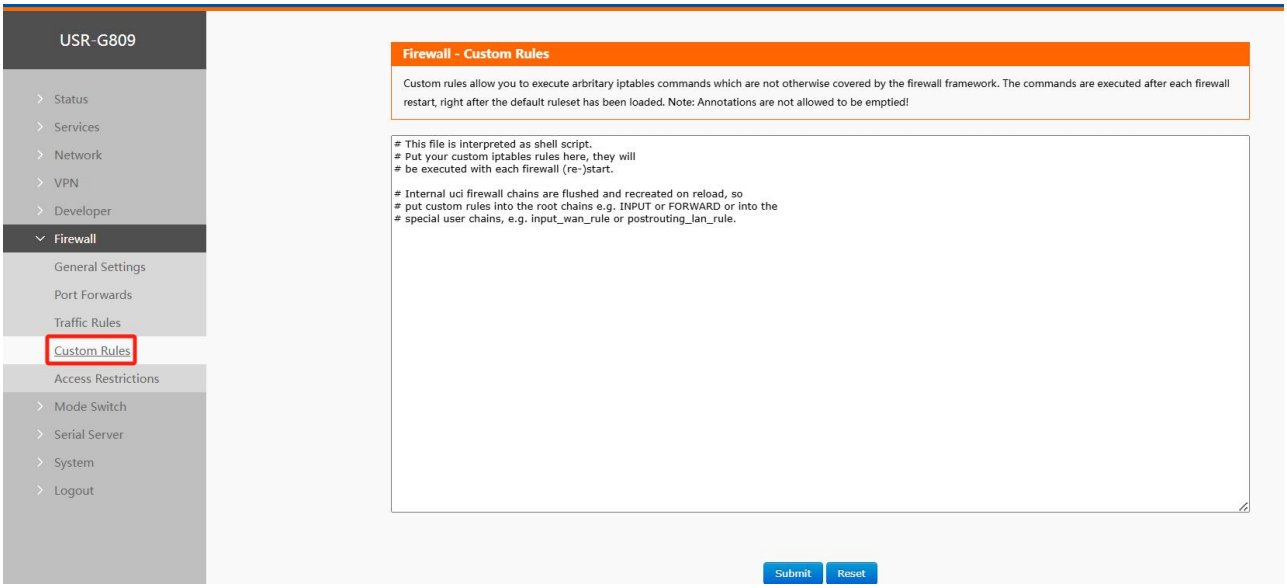


Fig. 141 custom rules

8. Edge computing

Edge computing and serial server functions can only be used in one of two ways,DTU/edge computing mode can be switched by mode, DTU mode can transmit serial data to the target server through TCP, UDP, MQTT, etc., configured through serial server interface; edge computing function mainly refers to G809 as the host, actively issue polling collection command, periodically obtain point data of serial port and network port equipment and data collected by IO interface, calculate the result according to the calculation formula set for each point and save it to the virtual register ofG809, and then actively report the data to the server according to the report grouping, reporting conditions and Json template

Select Edge Computing Mode in Mode Switch, click the button "Switch to Edge Computing Mode Configuration Web Page"toenter the Edge Computing Settings interface.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

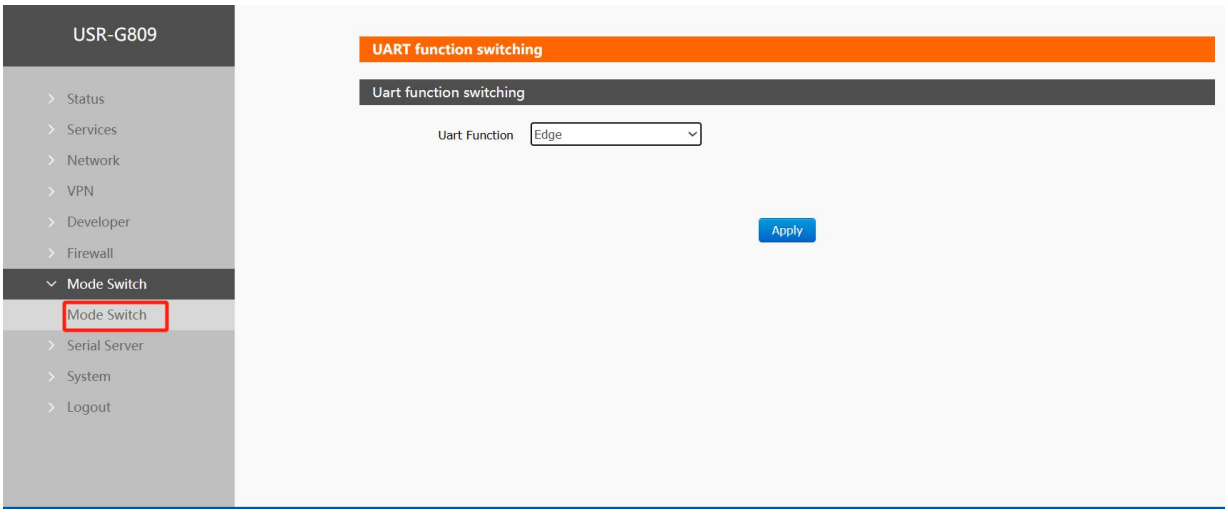


Fig. 142 mode switch

8.1. Data point

Data points are the core database of edge computing functions. Data collection, reporting, data reading and writing,protocol conversion and linkage control data and data-related information are all obtained from this point table. Therefore, in the process of use, it is particularly important to add all the data information that needs to be processed in detail. The data point table contains two main elements, slave and point. The system defaults to 2 fixed slaves, local IO slaves and status slaves.Up to 50 slaves can be added, including up to 20 network slaves and up to 50 serial slaves. You can add them according to your needs.Each slave can add a corresponding data point. Except for virtual slaves, the total number of points under all slaves can be up to 2000. The points under each slave carry out active polling collection from the corresponding interface according to the protocol specified by the slave, and the collected data are stored in the virtual register in the product.

Because the protocol corresponding to each slave is different, the parameters required for adding points are also different, and can be configured according to the actual situation. Compute points can only be added to virtual slaves, where a maximum of 500 compute points can be added. The G809 limits the addition of only one virtual slave for storing compute points.

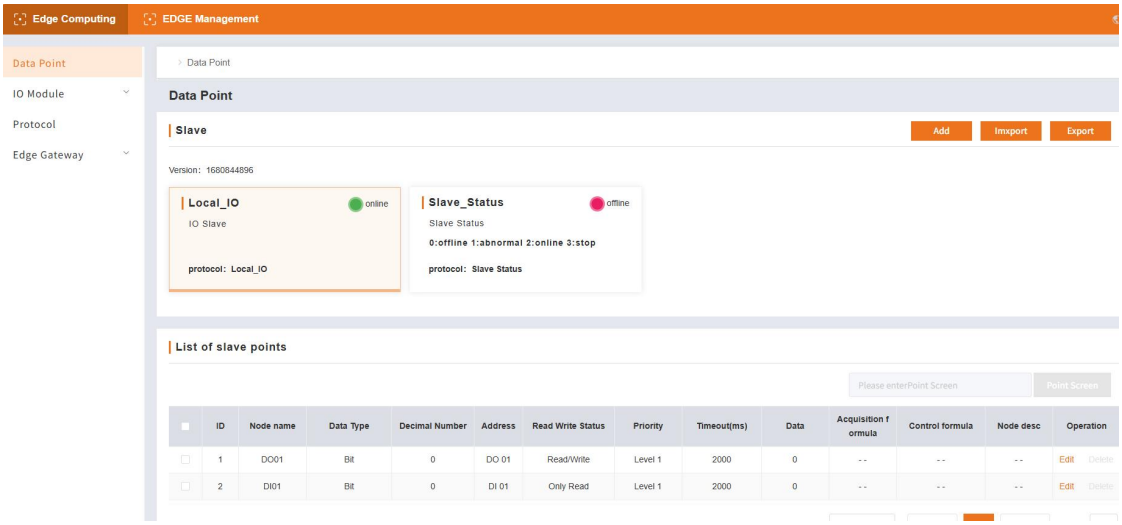


Fig. 143 data point

table 44 configuration parameters

name	describe	point
IO slave	IO interface data acquisition and storage, for edge computing other functions,analog data can be added to the calculation formula	The maximum number of slave points is equal to the number of G809IOpoints, which includes 2000 data points.
state slave	The online status of all addable slaves in the point table	Every time a new slave is added, the status point automatically increases byone, and the status point name directly corresponds to the name of the new slave.
virtual slave	Calculation points are mainly added. The data of multiple collection points are calculated internally by G809and the results are new data. New locations need to be provided for storage. Calculation formulas are customized when virtual points are added	Maximum 500 virtual points, not within 2000 real points

8.1.1. Add Slave

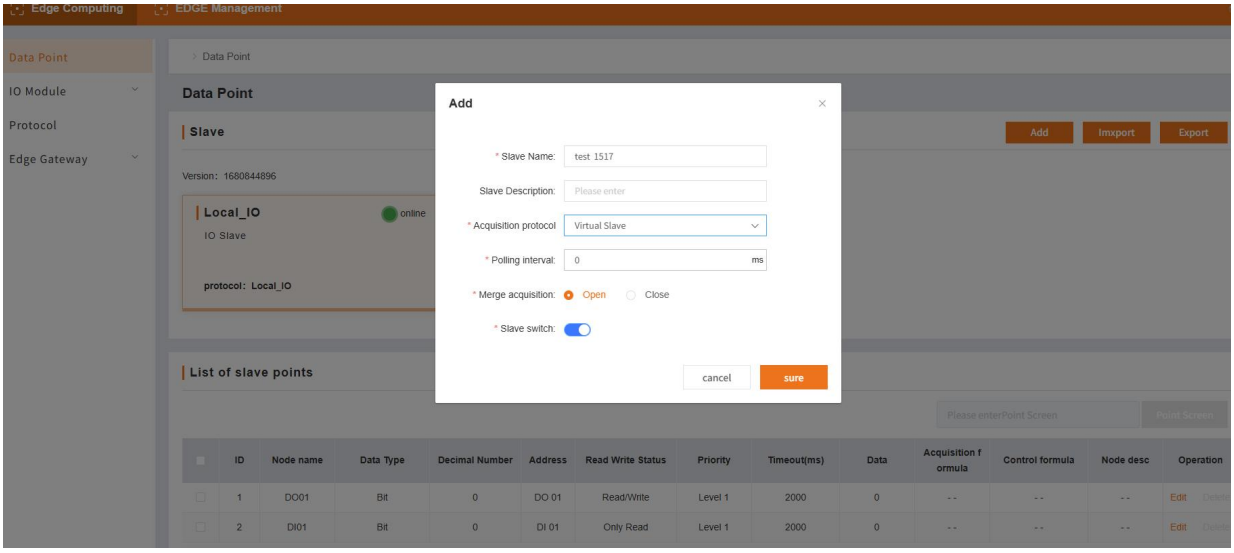


Fig. 144 Add Slave

table 45 configuration parameters

name	describe	default parameters
Slave Name	1-64 byte, used as unique identification of slave, non-repeatable, supporting Chinese	device1
slave description	Support 1-64 bytes, including alphanumeric, Chinese, underlined and connector	empty
acquisition protocol	The protocol used by slave point active polling acquisition, Modbus protocol supported	virtual slave
polling interval	The waiting time before each point acquisition command is sent, ranging from 0 to 65535ms	0ms
combined acquisition	Several consecutive address points in a single slave are combined into one command for acquisition, and a maximum of 32commands are used for acquisition.	open
slave switch	When it is closed, all points under the slave will stop active rotation training and data updating.	open
slave address	Slave code of lower equipment, partial protocol settings	1
Serial serial number	Point acquisition command sends serial serial port serial	1
IP	When collecting the network port, G809 as a Client, need to fill inthe target IP, part of the protocol settings	192.168.1.1
port	When collecting network port, G809 as Client needs to fill in the targetportand some protocol settings	102

8.1.2. Add Point Table

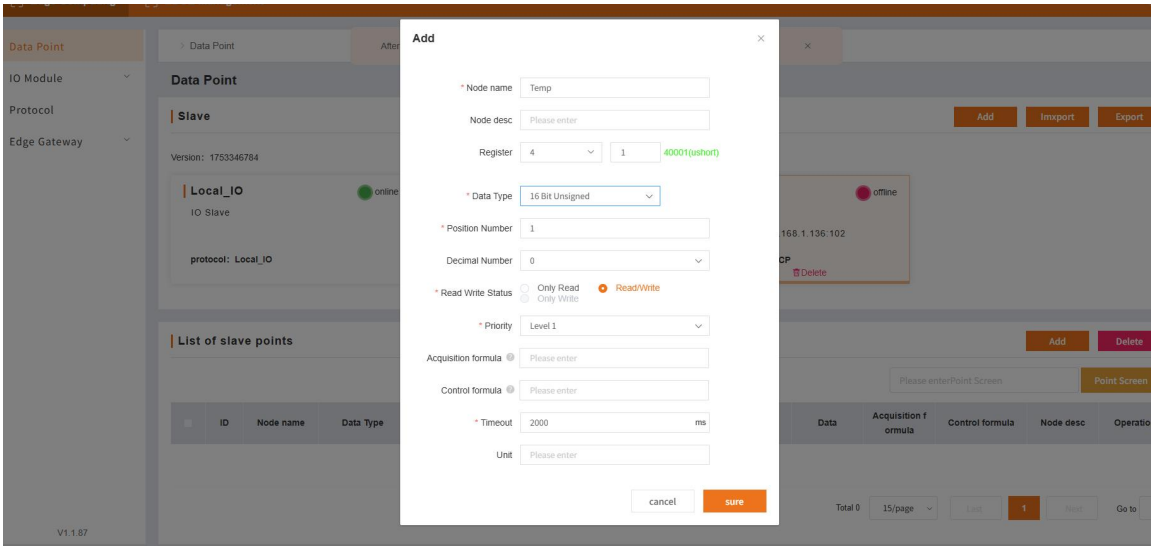


Fig. 145 Add Point Table

table 46 configuration parameters

name	describe	default parameters
Point name	1-64 byte, unique identifier of a point, not repeated with any other point	empty
Point Description	1-64 bytes, supporting characters, numbers and Chinese	empty
register	The storage type and storage address of the point	00001
data type	Selection of Data Type for Point Collection	place
Number of points	Add the total number of consecutive address points at a time under the same slave, add in batches	1
number of decimal places	The number of decimal data displayed when the calculated result of collected data is decimal	0
read-write state	Read/write status of points. Different point types support different read/write types.	read and write
priority	When polling all points, the high-priority points are given priority to ensure that the polling collection is carried out periodically, and the high -priority points are guaranteed to be collected periodically. Real-time acquisition	Grade 1
acquisition formula	Point calculation formula, the collected data is stored and extracted after calculation according to the formula	empty

	For other functions	
control formula	When a write operation is performed on this point,the result is written to the terminal device after calculation	empty
timeout	The longest waiting time for reply after issuing command during point polling acquisition, and this acquisition will be automatically abandonedafter exceeding the time Set, do not update historical data and execute the next acquisition command.Range: 10~3000ms	2000ms
unit	Non-mandatory parameters, set as needed	empty

8.1.3. Edge computing

Edge calculation function is mainly aimed at the calculation of data in point table, which is divided into two kinds: acquisition calculation and control calculation.

8.1.3.1. Collection computing

The collection and calculation of edge calculation mainly refers to the process of calculating the point data collected by the product through serial port or network port according to the formula set in advance and obtaining the result. The calculated data is stored in the virtual register corresponding to the data point table. When the product actively reports or the server actively collects, the data is packaged and sent to the cloud.The G809 integrates edge computing functions, and the data processing moves down from the cloud to the gateway, greatly relieving the pressure of data processing in the cloud.

Calculation method: Edge calculation supports addition, subtraction, multiplication and division and () operation.Calculation format:

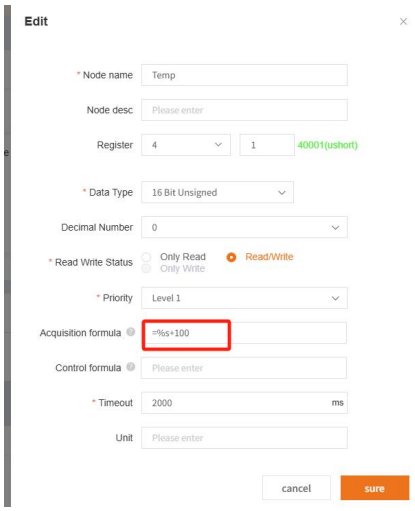


Fig. 146 collection computing

table 47 configuration parameters

calculation point	Example Formula	explain	Formula Add Location
single point	=(%s+10)/2	%s represents the current point value	Current Point Configuration Interface
multi-point	=(%s+10)/%s , node0101, node0102	The first %s representsdata for thepoint name node0101 The second %s representsdata for thepoint name node0102	Add new points separately under virtual slave Add calculation formula when

8.1.3.2. Control calculation

The main function of the edge calculation control formula is that when the north-facing server or APP sends data to the terminal, in order to maintain and actively collect the calculation results to maintain a unifiedmetric, it is necessary to perform certain calculations on the sent data. This type of function generally receives northbound data through protocol conversionand forwards it to the point table. After obtaining the result through the control calculation formula, it sends the data terminal.

Calculation method: The control formula supports addition, subtraction,multiplication and division and () operation.Calculation format:

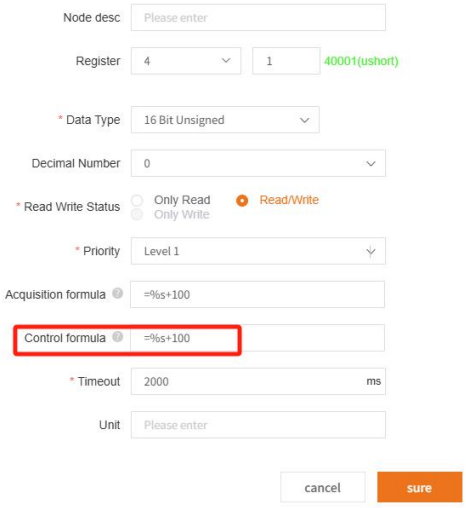


Fig. 147 control calculation

table 48 configuration parameters

calculation point	Example Formula	explain	Formula Add Location
single point	=(%s+10)/2	%s represents the current point value	Current Point Configuration Interface

8.2. IO Management

The G809 supports one DI and one DO.

8.2.1. IO hardware connection

<Description>

- Withstand voltage DC0-30V;
- It has two states: closed and open.
- Polarity, wiring can not be reversed. DO

<Description>

- DO withstand voltageDC0-30V, maximum withstand current 400mA;
- Digital output;
- It has two states: electric and non-electric;
- Polarity, wiring can not be reversed.

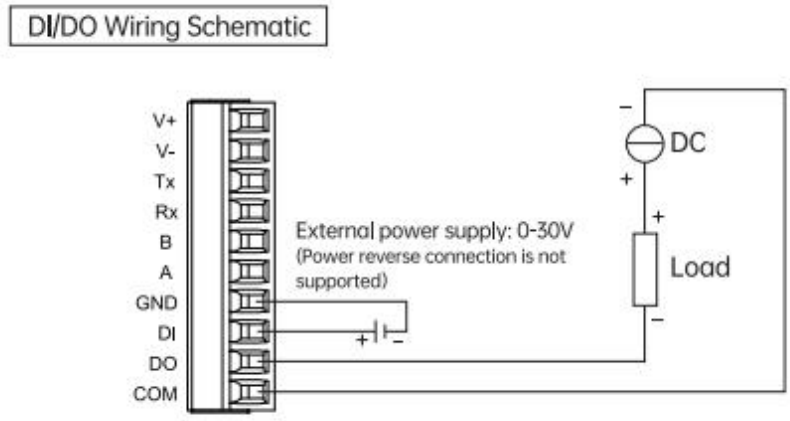


Fig. 148 DIDO Wiring Diagram

8.2.2. IO function

IO functions include DI acquisition mode and filter time, DO restart hold and timing functions.IO functions are configured under the "Edge Computing->IO Management->IO Functions" path on the built-in webpage.

DI function: mainly for each channel DI mode setting and related mode parameter configuration, support switching quantity acquisition and counting quantity acquisition.Related parameters are described as follows:

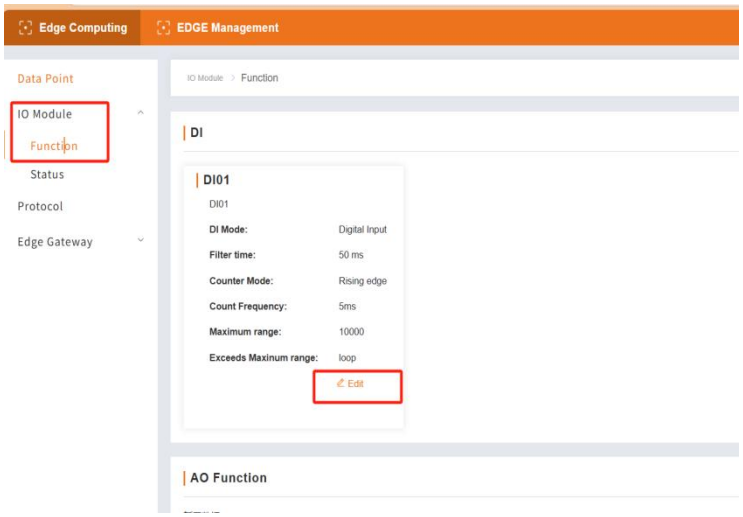


Fig. 149 DI function

table 49 configuration parameters

name	describe	default parameters
DI mode selection	switching quantity/counting quantity	switching value
filtering time	Filter time needs to be set in switching mode	50ms
counting mode	Rising edge trigger/falling edge trigger	rising edge
counting frequency	The speed of counting, the shorter the time, the faster the count	5ms
maximum range of count	The maximum number of counts that can be reached.	10000
Full-scale post-operation	Cycle: Counting from 1 Stop: Stop counting after full scale	circulation

Restart hold function: OFF by default. After ON, all DO status will be restored to pre-restart status after G809 soft restart.This feature does not support power-off restart.

Timed function: Add timed tasks in the form of events, and perform fixed actions of DO according to the set time and cycle.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

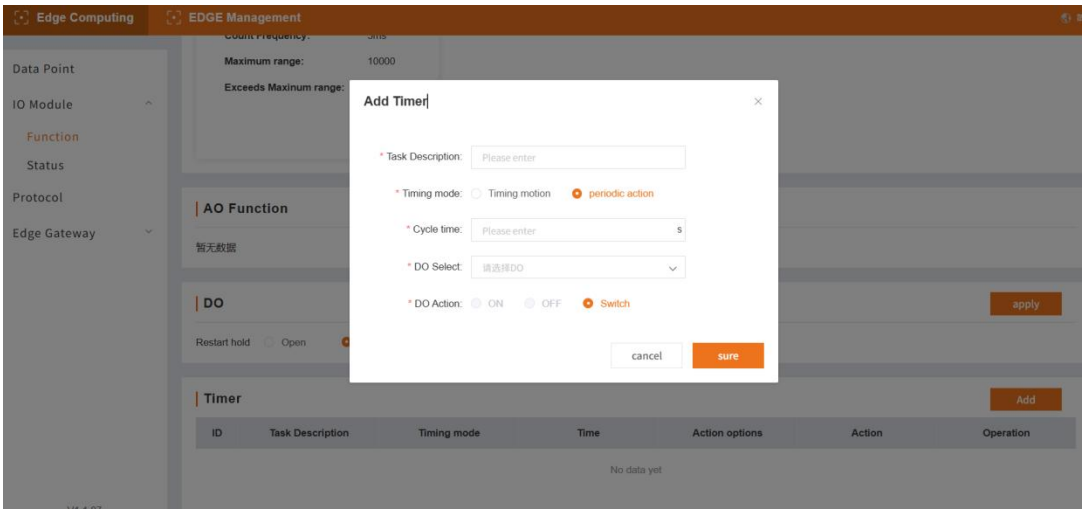


Fig. 150 timing function

table 50 configuration parameters

name	describe	default parameters
timing mode	Timed action: executed at a fixed time every day Periodic action: executed according to a fixed cycle	timed action
Timing Mode Time	In the timed operation mode, it is necessary to set a fixed time of operation every day, and the 24-hour system	empty
periodic action time	In periodic mode, the periodic interval between each action, in s	empty
DO selection	Select the DO interface	empty
DO action	Select the execution operation of the timed task	empty

8.2.3. IO status

Built-in webpage is equipped with local IO status supervision interface, through which DO status query and control, DI status and data view can be realized. IO state boundaries are as follows:

DI state has two modes: counting mode and switching detection mode. In counting mode, the interface displays the actual value of counting, and in switching detection mode, the interface displays the switching state of DI. The status of each DI is displayed independently and does not affect each other.

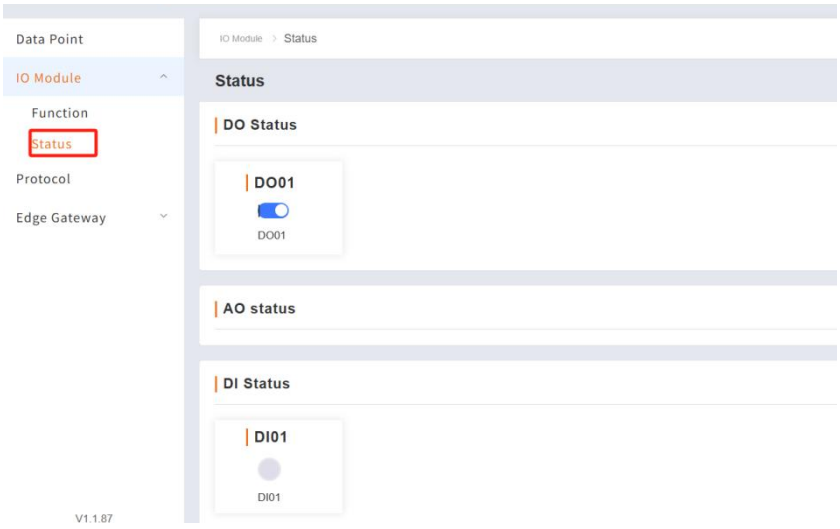


Fig. 151 IO status

8.3. protocol conversion

The protocol conversion function is mainly used in the scenario where the server actively issues protocol commands toobtain data or control points from G809.Because there are many kinds of point collection protocols in the point table, the server cannot fully interface with only one protocol. The protocol conversion can perfectly solve the problem of multiple protocols issued by the server for collection and control.

After the G809 is connected to the server through the protocol conversion link, the server issues standard protocol commands to collect and control all the data points of the G809.at present

Protocol conversion supports three protocol standards, Modbus RTU, Modbus TCP and Json.Different protocol conversions are set independently and can be used simultaneously and in parallel.

8.3.1. Modbus RTU

Modbus RTU protocol conversion function needs to add different protocol points in the data point table to the point mapping table of this function, and assign corresponding points to each point.

Modbus register address, after adding, the corresponding point data will be converted to standard Modbus protocol data. When receiving Modbus RTU from server Command, the corresponding address of the data to form a standard Modbus RTU data packet back to the server, so that the server through the unified data of the G809 point collection and control. Modbus RTU protocol conversion supports two kinds of data channels, one is Socket connection, supporting TCP Client and TCP Server, and the other isRS485 communication, mainly used in the configuration screen of field docking 485 interface.

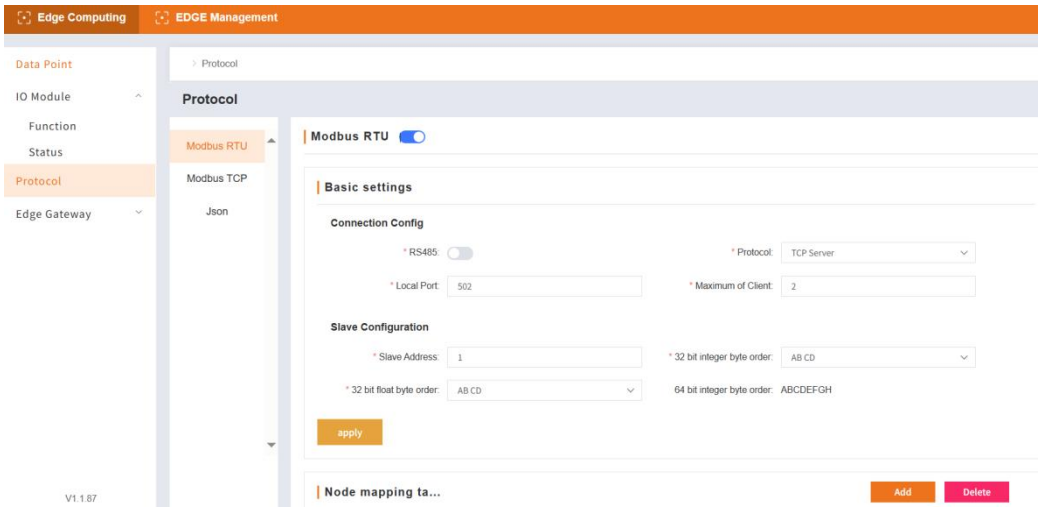


Fig. 152 Modbus RTU

8.3.2. Modbus TCP

Modbus TCP and RTU have the same operation on points, both of which convert the points in the data point table through the point mapping table, but Modbus TCP only supports Socket, TCP Client and TCP Server.

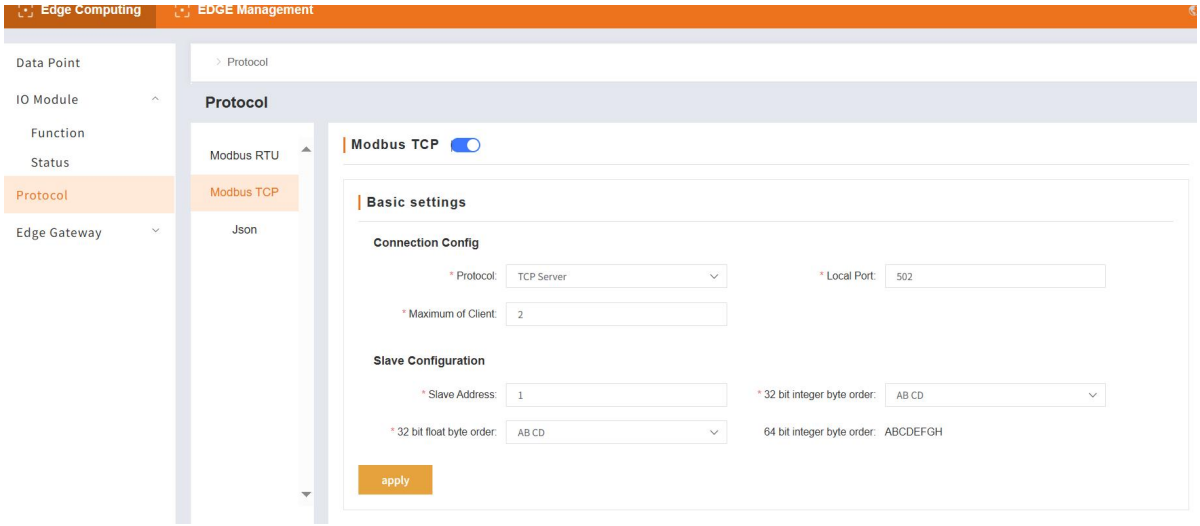


Fig. 153 Modbus TCP

8.3.3. JSON

Json format message is a commonly used message format for Internet of Things Hub. After Json function is enabled, data can be read and written through existing communication links.

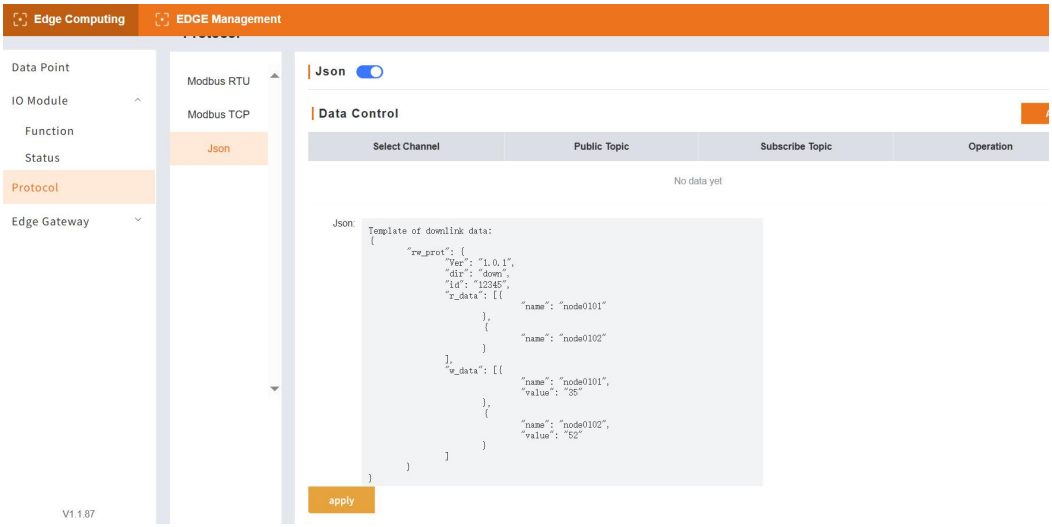


Fig. 154 Json

●Jsondata read and write format

WhenJson protocol conversion or MQTT communication link isenabled, the data points of G809 need to be collected and controlled according to the established format. TheJsoncommand format for reading and writing is as follows:

{"rw_prot": {"Ver":"Protocol Version","dir":"Data Trend","id":"Information Number","r_data":[{"name":"Point Name"}],"w_data":[{"name":"Point Name","value":"data"}]}}

●Jsonread and write command field description:

table 51 configuration parameters

field name	describe	field selection
rw_prot	protocol packet header	
ver	protocol version	1.0.1
dir	Data trend, the server sends a command to fill in down	down: server issues
id	The code of the data delivered by the server can be used as sequence identification.	Customer-defined, device replies No make changes
r_data	data read field	
w_data	data control field	

name	The point name can be substituted into the point if it is consistent with the point name in the point table.	
value	Only value field is written in read/write command, which is valid value written.	

●Jsonread-write reply format:

{"rw_prot": {"Ver":"Protocol Version","dir":"Data Trend","id":"Information Number","r_data":[{"name":"Point Name","value":"data","err":"Error Code"}],"w_data":[{"name":"Point Name","value":"data","err":"Error Code"}]}

●Jsonread and write reply field description:

table 52 configuration parameters

field name	describe	field selection
rw_prot	protocol packet header	
ver	protocol version	1.0.1
dir	Data trend, equipment reply content fill up	up: equipment reply
id	Information identification code, keep consistent with the issued command	
r_data	data read field	
w_data	data control field	
name	Point name, corresponding to the point in the point table	
value	Valid data corresponding to points	Read error, value valid value is nullWrite error, value value historical value
err	error code	0: Data executed normally 1: Data error execution

●Jsonfield error reply:

1) Json format error: device does not reply

2) ver, dir, id three fields, any one error, then reply according to the error protocol.

3) If the other fields are correct and only one error is found in r_data or w_data, the error field is discarded and the correct field is replied; if both fields are wrong,

Reply according to the wrong protocol.

4) Error protocol: "rw_prot":{"Ver":"1.0.1","dir":"up","err":"1"}.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

field name	describe	field selection
rw_prot	protocol packet header	
ver	protocol version	1.0.1
dir	Data trend, reporting and distribution	up: equipment reply
err	error code	0: Normal execution 1: Incorrect execution

Description:

a. When the read/write command is incorrect, the value of the reply content of the read command is null, and the value of the reply content of the write command is the historical data value.

b. The maximum upper limit of read and write operation is to read and write 5 data points simultaneously.

8.4. edge Gateway

The G809 has its own integrated edge gateway function, which realizes edge acquisition, calculation, reporting and linkage through simple parameter setting.Edge gateway function includes serial port management and communication link, data point active acquisition, data reporting and linkage control. In addition, the implementation of edge gateway function needs to be based on the complete configuration of data points.

8.4.1.1. Serial port management

Point data of edge gateway can be acquired through serial port. Before using edge gateway, parameters of each serial port need to be configured to ensure normal serial port communication. G809 supports two serial port configurations, which need to be configured separately.

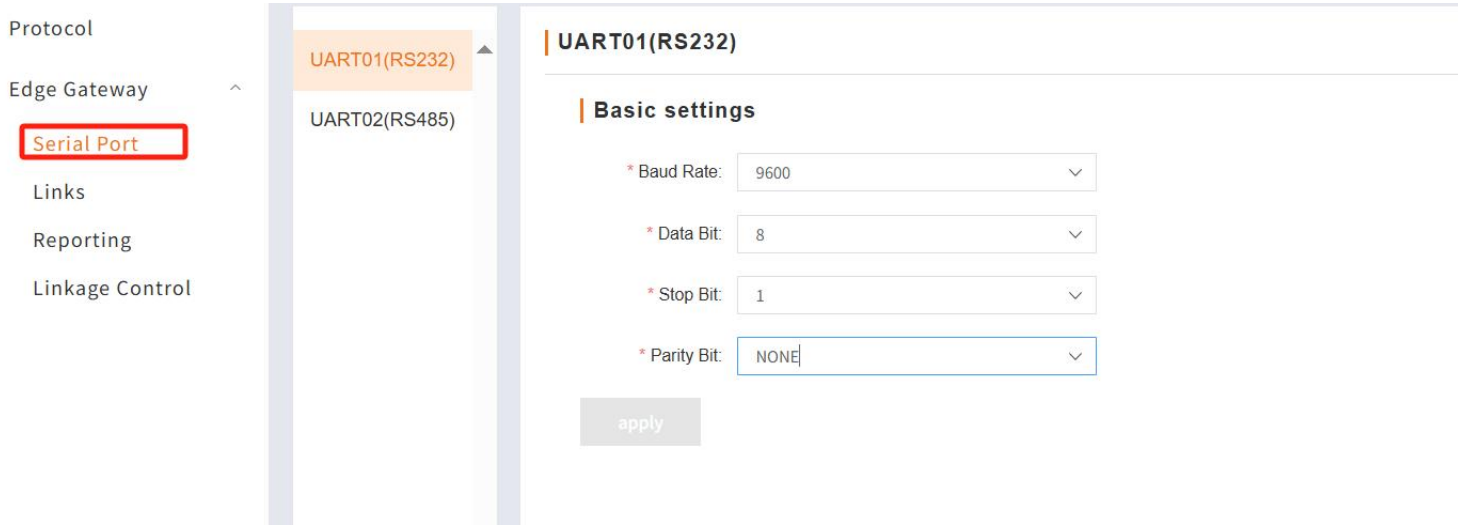


Fig. 155 serial port configuration

table 54 configuration parameters

name	describe	default parameters
RS232		
Baud rate	Can be set to: 600/1200/2400/4800/9600/19200/38400/57600/115200/230400	9600
data bits	Can be set to: 7/8	8
stop bit	Can be set to: 1/2	1
parity bit	Can be set to: NONE/ODD/EVEN	NONE
RS485		
Baud rate	Can be set to: 600/1200/2400/4800/9600/19200/38400/57600/115200/230400	9600
data bits	Can be set to: 7/8	8
stop bit	Can be set to: 1/2	1
parity bit	Can be set to: NONE/ODD/EVEN	NONE
Serial port function	Downward edge acquisition: data acquisition can be set in the data point table Uplink communication interface: as Modbus RTU protocol conversion function interface	downward edge acquisition

8.4.1.2. Communications link

Edge Gateway and Cloud Virtual Machine are channels for data interaction. Two connections are supported. Each connection supports TCP, HTTP and MQTT. Alibaba Cloud provides fast access to the platform. Meanwhile, each connection supports SSL encryption.Different protocol connections can flexibly configure parameters, among which MQTT and Alibaba Cloud can configure multiple subscriptions and publishing topics.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

(Subscribe and publish up to 16 topics).

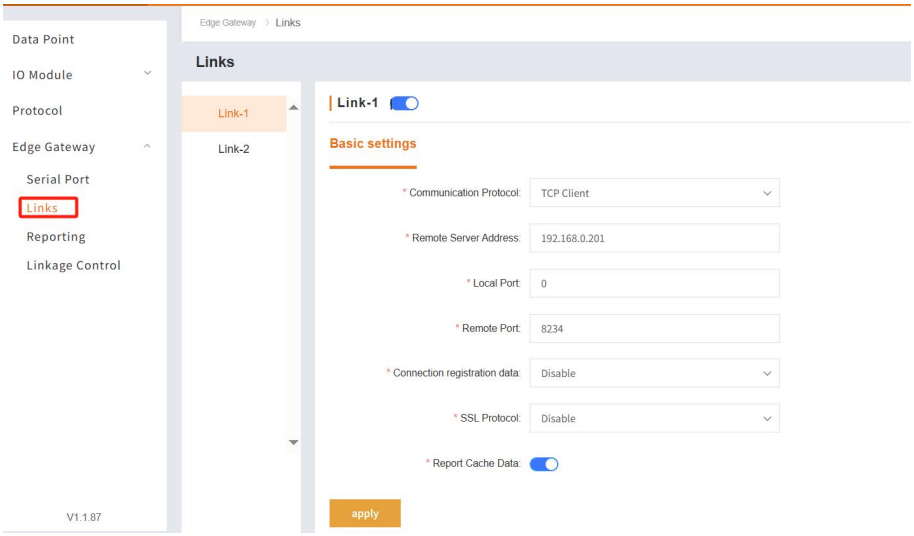


Fig. 156 communications link

8.4.1.3. Network disconnection cache

The two communication links of G809 both support the network disconnection cache function, with a total cache space of 2G. The data of each link is stored separatelyand stored by strip.

The template in the G809 data active report packet determines the size of each report data, so each data can not exceed 8K at most. Although each packet is independent, it is reported through two communication links. The G809data report can support the network disconnection cache function.

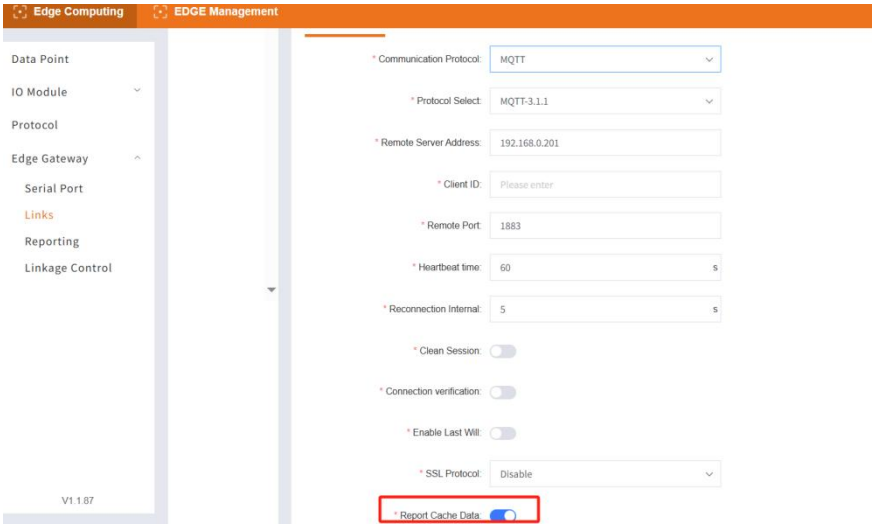


Fig. 157 network disconnection cache

8.4.1.4. Data reporting

The edge function of the G809 performs active collection,actively issues commands to the terminal equipment to obtain data through serial ports and network ports, and stores the data in the storage space inside the G809. There are two ways for these data to interact with the server. One is through protocol conversion. The server actively interacts with G809 to obtain data through a specific protocol. In this way, the server is the active initiator, and G809 is used as the passive reply slave. The other way is thatG809 actively reports to the server according to the set conditions.In this way,G809actively initiates data to the server. The active reporting method can reduce the link for the server to issue commands, thus reducing the pressure on the server to collect colleagues, and saving bandwidth or traffic.

G809's active reporting supports group reporting, each group reports independently, and individual reporting channels, reporting conditions, reporting Json templates, and reporting data points can be configured within the group. A total of 2000 groups can be created for reporting. Multi-group reporting can report different data to the server according to different frequencies or methods according to importance, thus reducing the pressure on the server. The configuration diagram is as follows:

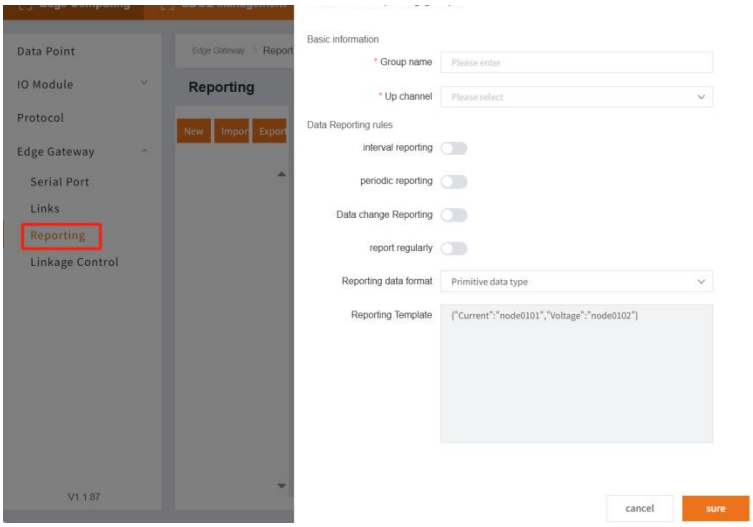


Fig. 158 Create a data escalation group

table 55 Key parameter description

name	describe	default parameters
upward channel	Report the channel of packet connection server. You can choose human cloud/link 1/link 2.	empty
Reporting Rules	Support four reporting conditions (interval/cycle/change/timing reporting), support multiple choices	empty

Reporting data cell type	Original type: Point data is reported to the server according to the original type. Numeric to character: if the point data is of numeric type,"" will be added in the report, and the numeric format will be converted to character string format, and then reported to the platform.	empty

Submission template	CustomJson, need to comply withthe Json format specification, template maximum 8K bytes.	empty
table of points	Each independent reporting group has a point table, and the data points in the data point table that need to be reorganized and reported All points are pulled, so that each group can be independently performed according to the point list Data pull and accurate reporting	empty

8.4.1.5. Json Reporting Template

The data reporting function uploads point data to the server in Json format. The client can customize the Json template according to the server requirements to ensure that the uploaded data format meets the server's parsing requirements.The actual name of the data point can be defined in the Json template. However, Json template configuration needs to pay attention to the following points:

1. The Json template in the grouping is empty by default. It can be designed by itself and meets the requirements of Json format.

2.Valuein Json template is character type, which needs to be filled in data point name. When data is reported, the actual acquisition value corresponding to point name will be substituted for replacement.

3. Examples:

The acquisition values of node0101 and node0102 at the edge are 30 and 20 respectively;

Json template is set to {"Current":"node0101","Voltage":"node0102"};actual report data format is {"Current":30,"Voltage":20}.

Inaddition to the data points, some specific identifiers can also be added to the Json template, such as the firmware version of the product, SN, MAC and other parameters, which can be processed as the unique identifier of the device or device identification information. Directly add the relevant identification name to the value position of the Json template, and the equipment is on the top. In the reporting process, the data corresponding to the identification name will be substituted and

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

reported. For example, when reporting the timestamp, set the Json template to {"time":"sys_local_time"}, andthe actual data reported by the device is {"time":"2023-05-27,22:35:44"}. The list of identifiers that can be populated into the Json template is as follows:

table 56 parameter specification

identification	implication	Example of Reporting Content
sys_ver	Product firmware version number	V1.0.14.000000.0000
sys_imei	IMEI	864452061930390
sys_sn	SN	02700122093000012356
sys_mac	MAC	D4AD20474662
sys_iccid	ICCID	89861122219045577705
sys_local_time	local time	2023-05-27,22:35:44
sys_utc_time	UTC time	2023-01-12T18:15:02Z
sys_timestamp	timestamp	1706167861
sys_timestamp_ms	millisecond timestamp	1601196762389

8.4.1.6. Linkage control

Linkage function is mainly to realize local closed-loop management, rapid alarm and emergency applications. Theproduct can support 50 linkage events. Each linkage control can set the judgment condition, pull the trigger point and set the trigger mode.During the operation process of the product,whether the linkage is to be executed or not is confirmed according to the judgment conditions after the data of the trigger point is calculated and obtained through edge collection, and when the conditions are met, the processing is carried out according to the execution action set by each linkage event.

The parameters are described as follows:

table 57 parameter specification

name	describe	default parameters
event name	Linkage event name, user-defined	event1
event switch	Enabling of linked events	open

minimum trigger interval	When the linkage event meets the trigger condition for many times in a short time, touch The minimum interval between the execution of the trigger and the minimum trigger time. Send no action, directly discard.	1000ms
trigger point	Linkage conditions determine the source of the required data and support multiple points bit selection	empty
trigger condition	The judgment condition of linkage event is satisfied, and the action is executed. 10 conditions supported	empty
trigger mode	When multiple trigger points are selected, trigger logic between multiple points	All points meet the conditions

	compile	
the upper threshold	Maximum range of threshold conditions, range 0~20000	0
the lower threshold	Range minimum of threshold condition, range 0~20000	0
perform an action	After the linkage event meets the trigger conditions, the actions to be executed made	empty

Linkage event trigger conditions support 10, as shown in the following table:

table 58 parameter specification

trigger condition	describe	explain
forward following	DI closed, DO closed; DI open, DO closed break	Trigger points only support switching values
reverse following	DI closed, DO open; DI open, DO close	Trigger points only support switching values
greater than or equal to	Trigger action when detection value is greater than or equal to set threshold	Set lower threshold only

greater than	Trigger action when detection value is greater than set threshold	Set lower threshold only
less than or equal to	Trigger action when detection value is less than or equal to set threshold	Set only the upper threshold
less than	Trigger action when detection value is less than set threshold	Set only the upper threshold
Within the interval (including boundaries)	Detection value triggers action within threshold interval, each entry Trigger an action within an interval	Set upper and lower thresholds
Within the interval (excluding boundaries)	Detection value triggers action within threshold interval, each entry Trigger an action within an interval	Set upper and lower thresholds
Outside the interval (including boundaries)	Detection value outside threshold range triggers action, outgoing interval One action at a time.	Set upper and lower thresholds
Outside the interval (excluding boundaries)	Detection value outside threshold range triggers action, outgoing interval One action at a time.	Set upper and lower thresholds

Linkage events trigger execution of operations in support of 4, as shown in the table below:

table 59 parameter specification

trigger condition	describe	explain
DO action	Select DO interface of equipmentand output corresponding actions (close, open and flip)	DO is single choice
write data point	Write pre-set data to pre-selected points centre	Data points pulled from the data point table
reporting platform	Cloud level that uploads custom alarm messages via link Quick alarm	MQTT requires a separate theme

send short messages	Send custom alarm messages to your hands via SMS Machine, realize fast alarm	SMS content is within 70 bytes

8.5. Edge computing management

8.5.1. configuration management

Import and export files are mainly used for rapid replication of edge computing configurations, so users need to ensure the legitimacy of files during import and export.

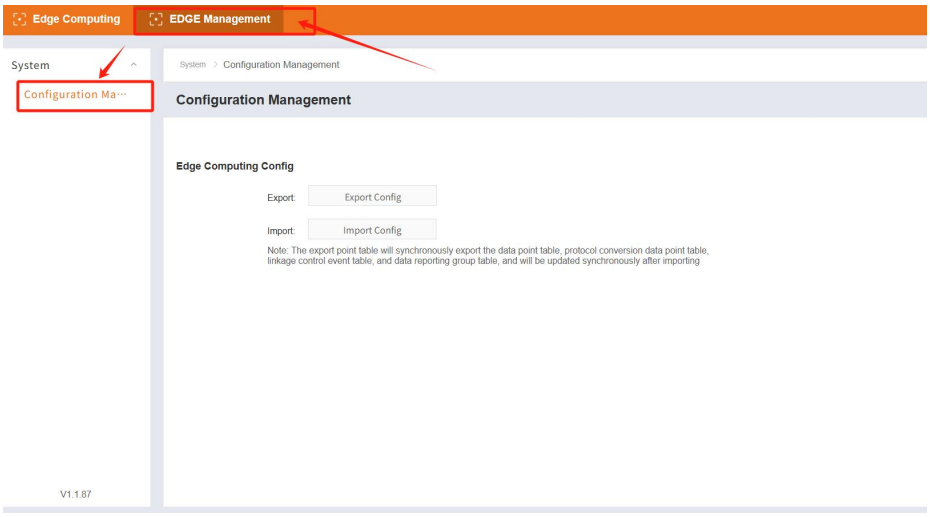


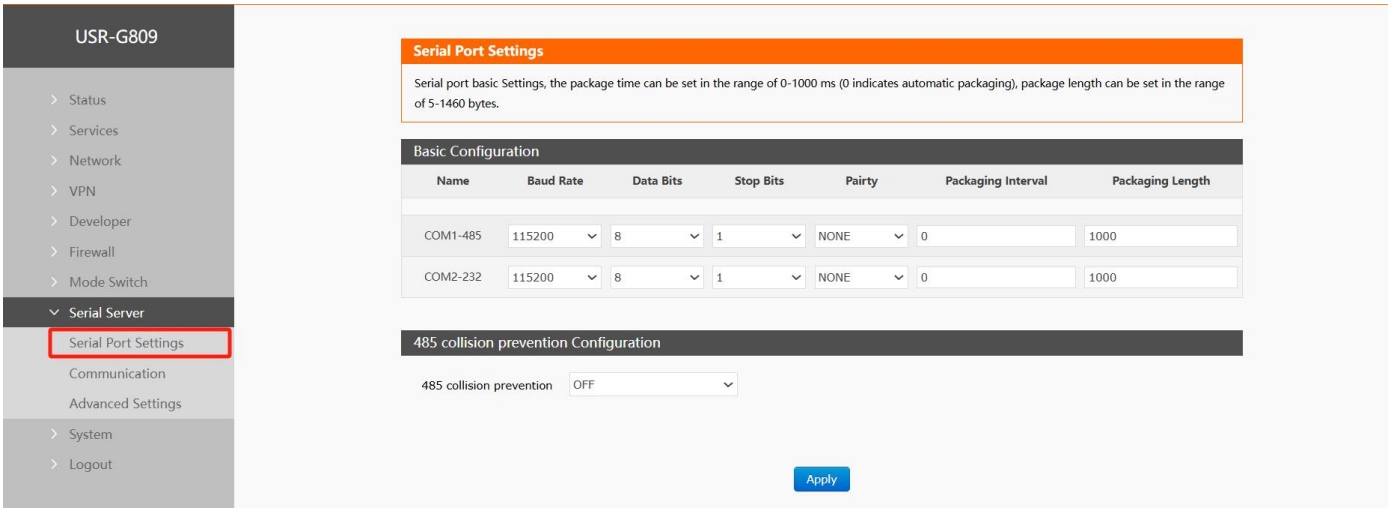
Fig. 159 configuration management

9. Serial server

809 hasRS232/RS485, supports TCP, UDP, MODBUS, MQTT, HTTPD and other network protocols, and supports heartbeat packets, registration packets and AT and other special features.

9.1. Serial port settings

In this interface, you can set parameters such as baud rate and data bit of serial port.



map 208 Serial port setting interface

table 61 Serial port setting parameter table

name	functional description	default
Baud rate	Set the baud rate of RS232 or RS485, you can set: 1200/2400/4800/9600/19200/38400/57600/115200/230400	115200
data bits	Set RS232 or RS485 data bits, settable: 7/8	8
stop bit	Set RS232 or RS485 stop bit, settable: 1/2	1
parity bit	Set the check bit of RS232 or RS485, you can set: NONE/ODD/EVEN	NONE
Packing time	SetRS232orRS485data packing time unit: ms (range: 10-60000ms)	0
packing length	SetRS232orRS485data packet length Unit: bytes (range: 5-1500 bytes)	1000

9.1.1. Time triggered mode

When receiving data from UART,the interval between adjacent 2 bytesis constantly checked. If the interval time is greater than or equal to a certain "time threshold", it is considered that aframe is over, otherwise the data is received until it is greater than or equal to the packet length (default is1000 bytes). This frame of data is sent as a packet to the network. The "time threshold" here is the packing interval time. The settable range is10ms to 60000ms. Factorydefault50 ms.

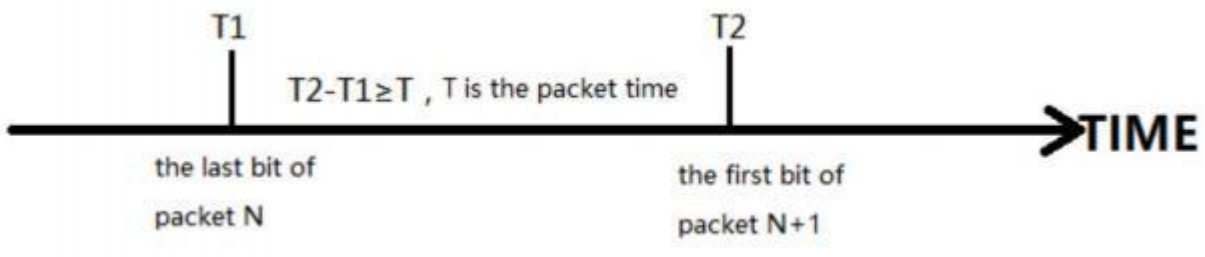
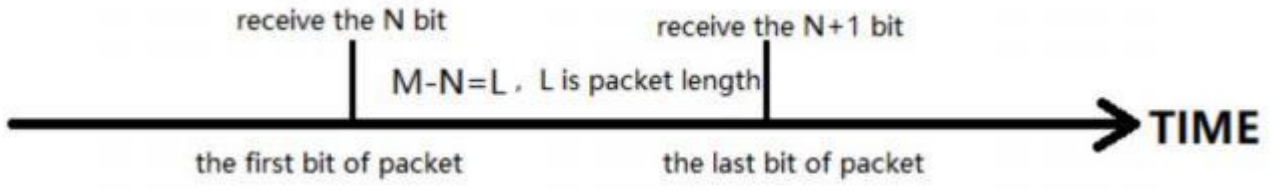


Fig. 209 Time triggered mode

9.1.2. Length Trigger Mode

When receiving data from UART, it constantly checks the number of bytes received.If the number of bytes received reaches a certain "length threshold," a frame is considered to have ended.This frame of data is sent to the network as a TCP or UDP packet.The "length threshold" here is the packing length.The configurable range is5 to1500bytes. Factory default1000 bytes.



graph 210 Length Trigger Mode

9.2. communication configuration

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

9.2.1. TCPC mode (TCP Client mode)

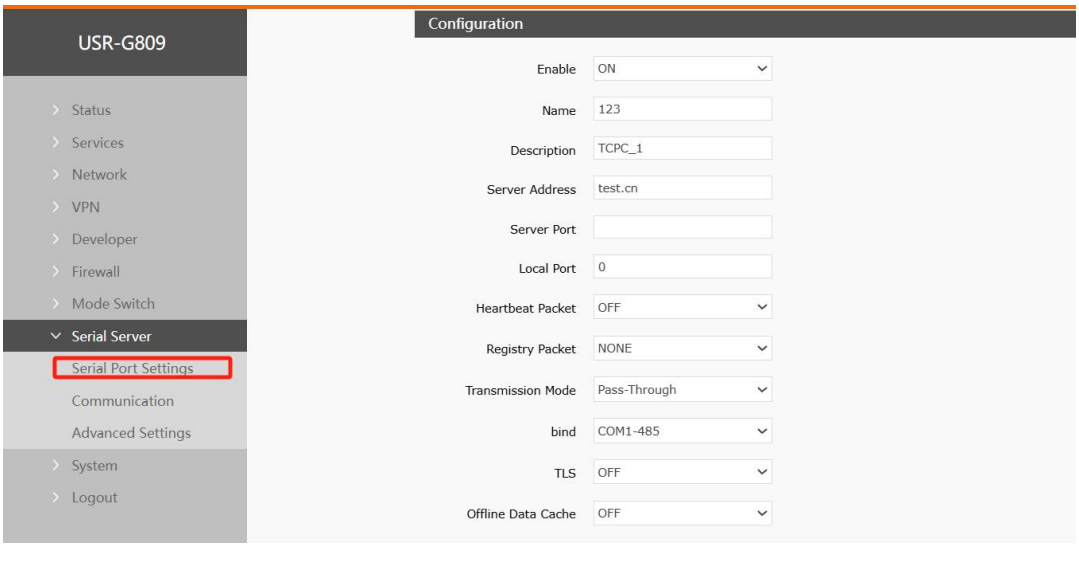


Fig. 212 TCPC Configuration Interface

table 63 TCPC parameter table

name	functional description	default
start using	Is this link enabled, ON/OFF	ON
name	Set the name of this link	123
describe	Set this link comment information	TCPC_1
server address	Server address: IP or domain name form	test.cn
server port	server port number	empty
local port	Fill in the local port number. If it is set to 0,the local port will be automatically assigned.	0
heartbeat packet	Set whether to enable heartbeat packet function, ON/OFF	OFF
Heartbeat packet type	HEX: hexadecimal type ASCII: Character type	HEX
heartbeat packet	Heartbeat packet data content	empty

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

data		
heartbeat time	The time interval between heartbeat packets sent, in seconds	60
Registration packet	NONE: Close Heartbeat Package Custom: Customize registration package content MAC: Include device WAN MAC as registration package content	NONE
Register Package Type	Custom Registry Type HEX: Hex Type ASCII: Character Type	HEX
Register package data	Register package data content	empty
Register package sending method	Send a registration packet when connecting to the server Add registration packets to the front of every packet sent to the server	Send once on connection
transmission mode	Pass-Through: pass-through mode	Pass-Through

host polling	OFF: Modbus RTU and Modbus TCP interconversion;ON: multi-host polling	OFF
channel binding	COM1-485:Data transmission using RS485 channel onlyCOM2-232:Data transmission using RS232 channel COM1+COM2:Data transmission using RS232 or	COM1-485
TLS	Version number: TLS1.0 and TLS1.2 The authentication mode can be selected from non-authentication certificate, authentication server certificate and bidirectional authentication certificate	OFF
TLS authentication method	Do not verify certificate: that is, only implement data layer transmission decryption, and do not verify the identity of the other party during the handshake process Verify server certificate: that is, the client will verify the server certificate during handshake, and the client needsto preset the root certificate of the server. Two-way authentication: that is, the client and the server verify each other's identity, and the server root certificate, client certificate, and client private key need to be preset.	Do not verify certificates
Offline data cache	Cache the data after the Socket network is disconnected, and automatically report the cached data after waiting for the network to be available	OFF
data overflow handling mode	Discard old data: Discard the oldest cached data and roll the newest cached data Discard new data: new data will not be cached when the cache space is full	Discard old data
cache system	Length limit: maximum storage 7300 bytes Packet limit: maximum storage of 10 packets	length limit

Description:

- TCP Client mode can be used in conjunction with the USR custom indicator, which lights up when TCP Client is connected to the server.
- Support TLS encryption transmission, offline data cache function

9.2.2. TCPS mode (TCP Server mode)

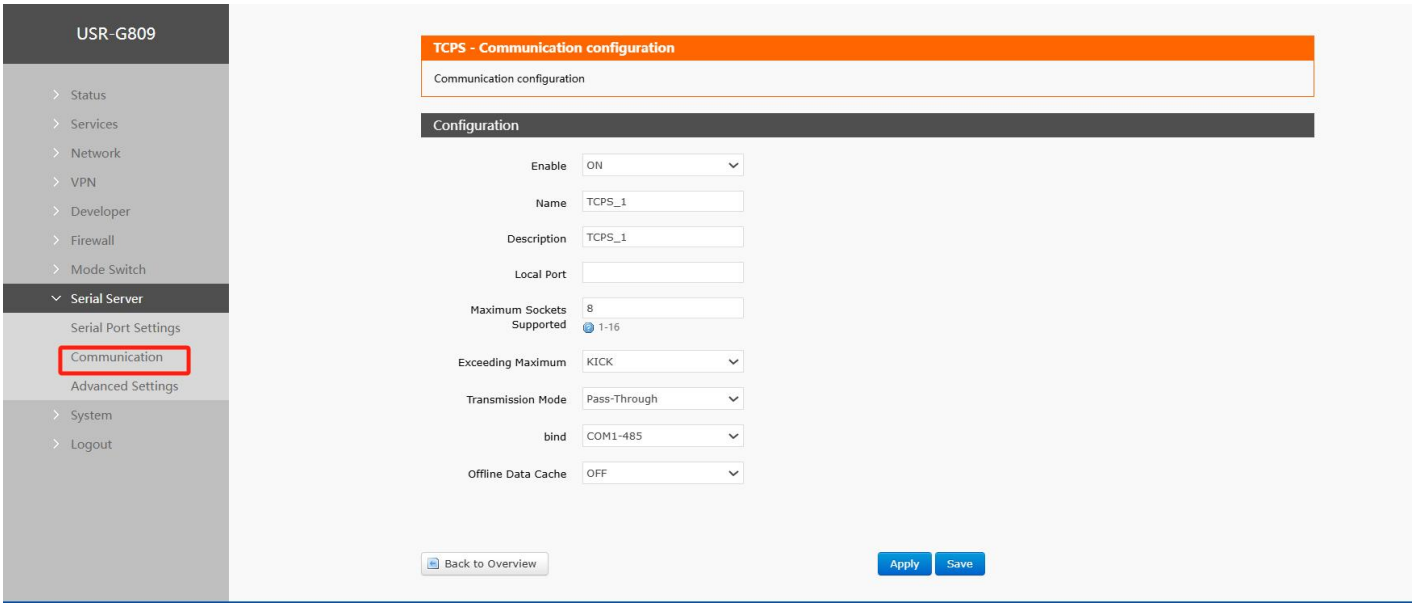


Fig. 213 TCPS configuration interface

table 64 TCPS parameter table

name	functional description	default
start using	Is this link enabled, ON/OFF	ON

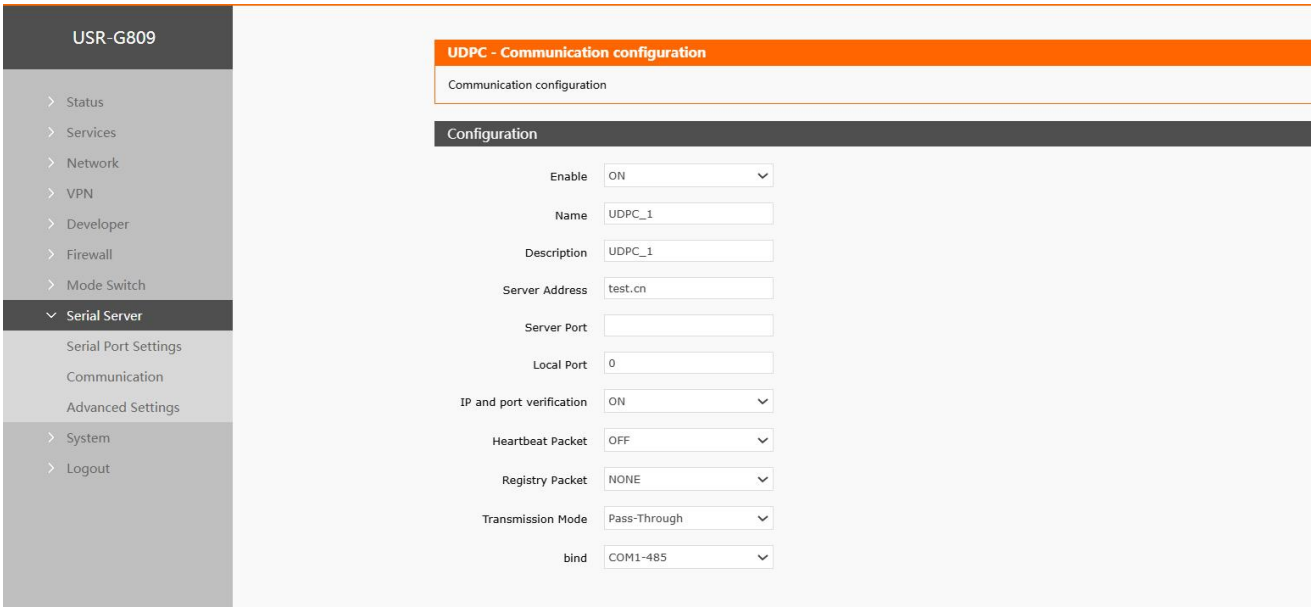
name	Set the name of this link	TCPS_X
describe	Set this link comment information	TCPS_X
port	local port number	empty
Maximum number of client connections supported	Number of clients accepted, 1-16	Default 8
transmission mode	Pass-Through: pass-through mode	Pass-Through
Number of connections exceeded	KICK: kick out of range;KEEP: keep connected	KICK
channel binding	COM1-485:Data transmission using RS485 channel onlyCOM2-232:Data transmission using RS232 channel COM1+COM2: Transfer data using RS232 or	COM1-485
Offline data cache	Data overflow handling mode selection, cache mode, cache length setting, etc.	OFF

Description:

- TCP Server mode can be used in conjunction with a USR custom indicator, which lights up when a client is connected to the service
- Up to 16 clients can connect to this TCP Server at the same time, such as the 17th client connection is not connected.

9.2.3. UDPC mode (UDP Client mode)

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



graph 214 UDPC configuration interface

table 65 UDPC parameter setting table

name	functional description	default
start using	Is this link enabled, ON/OFF	ON
name	Set the name of this link	UDPC_X
describe	Set this link comment information	UDPC_X
server address	Server address: IP or domain name form	empty
server port	server port number	empty
local port	local port number	0
check port	Check port, no check port	check port
heartbeat packet	Set whether to enable heartbeat packet function, ON/OFF	OFF
Heartbeat packet type	HEX: hexadecimal type ASCII: Character type	HEX
heartbeat packet data	Heartbeat packet data content	empty
heartbeat time	The time interval between heartbeat packets sent, in seconds	60
Registration packet	NONE: Close Heartbeat Package Custom: Customize registration package content MAC: Include device WAN MAC as registration package content	NONE
Register Package Type	Custom Registry TypeHEX: Hex TypeASCII: Character Type	HEX
Register package data	Register package data content	empty
Register package sending method	Send a registration packet when connecting to the server Add registration packets to the front of every packet sent to the server	Send once on connection
transmission mode	Pass-Through: pass-through mode	Pass-Through

channel binding	COM1-485:Data transmission using RS485 channel onlyCOM2-232:Data transmission using RS232 channel COM1+COM2:Data transmission using RS232 or	COM1-485

Description:

- UDP Client mode can be used in combination with USR custom indicator,USR indicator lights up when connected to server

9.2.4. UDPS mode (UDP Server mode)

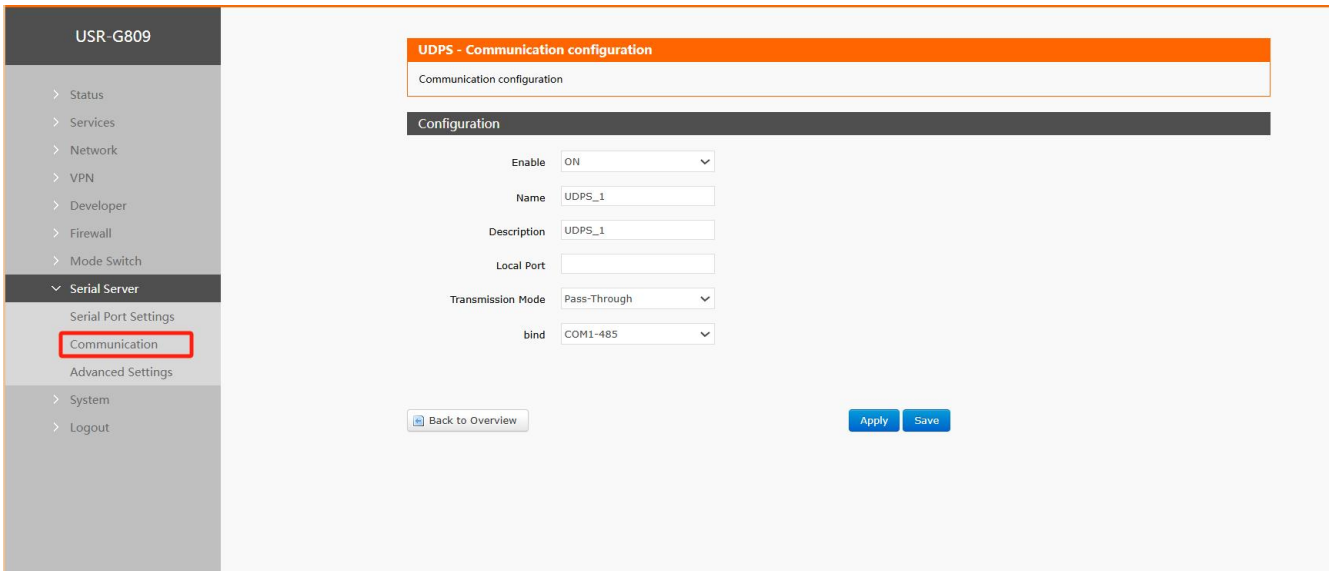


Fig. 215 UDPS configuration interface

table 66 UDPSparameter table

Name	functional description	default
start using	Is this link enabled, ON/OFF	ON
name	Set the name of this link	UDPS_X
describe	Set this link comment information	UDPS_X
local port	local port number	empty
transmission mode	Pass-Through: pass-through mode	Pass-Through
channel binding	COM1-485:Data transmission using RS485 channel onlyCOM2-232:Data transmission using RS232 channel COM1+COM2:Data transmission using RS232 or	COM1-485

Description:

- UDP Server mode can be used in conjunction with a USR custom indicator, which lights up when a client is connected to theservice;
- Use the client that last connected to this service as the actual client.

9.2.5. MQTT mode

The device supports MQTT Client function, users can easily access their own private MQTT server through simple configuration. Data publishing and data subscription support multi-topic adding configuration. Users can send serial data to a certain topic through configuration, or send data pushed by the server to the bound serial port, so as to realize data transmission between serial port and server.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

9.2.5.1. MQTT Basic Configuration

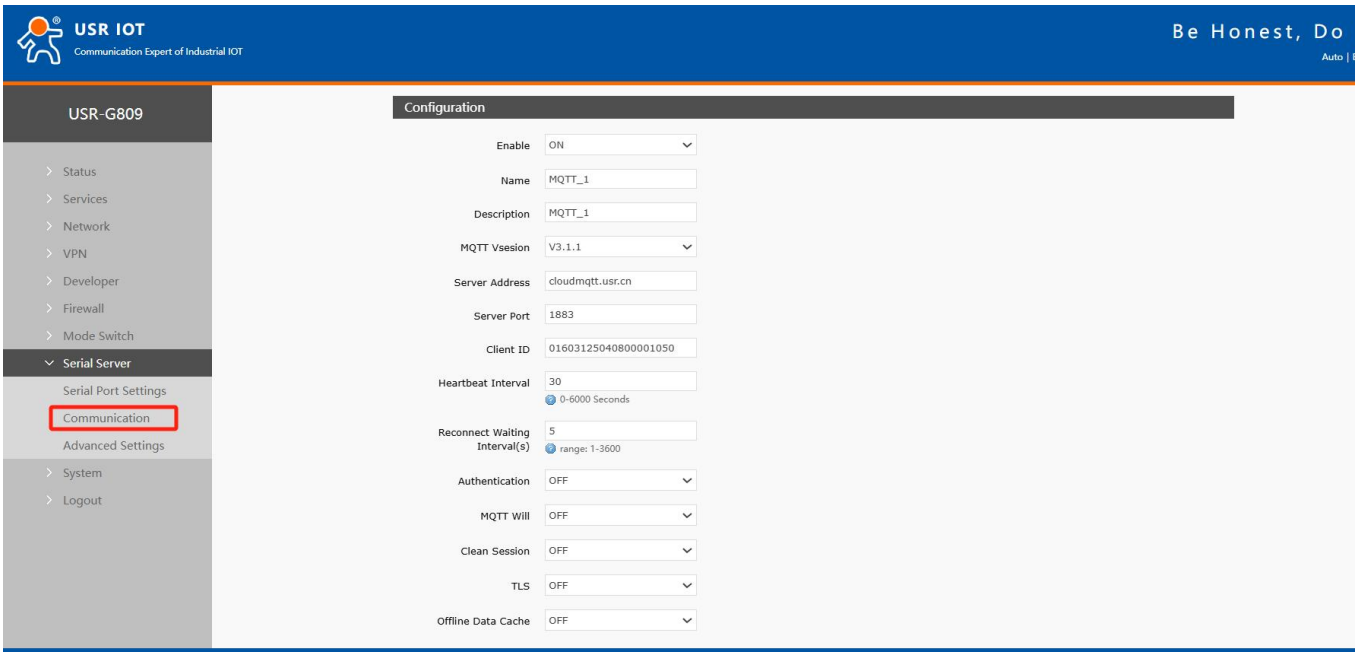


Fig. 216 MQTT configuration interface

table 67 MQTTparameter table

name	functional description	default
start using	Is this link enabled, ON/OFF	ON
name	Name of this link	MQTT_X
describe	Comments for this link	MQTT_X

MQTT version	You can choose:MQTTV3.1. Version 1/V3.1	V3.1.1
server address	MQTT server address: IP or domain name	cloudmqtt.usr.cn
server port	MQTT Server Port	1883
client ID	MQTT client identifier	123456
heartbeat time	MQTT protocol heartbeat time, unit: seconds	30
Reconnection detection interval	Next reconnection interval after MQTT disconnection, unit: seconds	5
authentication	If the server requires username and password authentication,ON: Turn on MQTT username and password authentication OFF: Disable MQTT username password authentication	OFF
last words	MQTT connection flag. When the network is disconnected abnormally, the server will publish this will message toother clients who subscribe to this will topic. ON: Enable Subscriptions to Wills Topics OFF: Close subscription to Wills topic	OFF
theme	Last words topic	empty
Last words	Set Last Words	empty

QOS	To set QOS of will, you can set: 0 at most once 1 at least once 2 exactly once.	0
reservation message	Turn on message function ON: ON OFF: OFF	OFF
cleanup session	MQTT protocol connection flag bit, used to control the lifetime of the session state, OFF,ON	OFF
TLS	Version number: TLS1.0 and TLS1.2 The authentication mode can be selected from non-authentication certificate, authentication server certificate and bidirectional authentication certificate	OFF
TLS authentication method	Do not verify certificate: that is, only implement data layer transmission decryption, and do not verify the identity of the other party during the handshake process Verify server certificate: that is, the client will verify the server certificate during handshake, and the client needs to preset the root certificate of the server. Two-way authentication: that is, the client and the server verify each other's identity, and the server root certificate, client certificate, and client private key need to be preset.	Do not verify certificates
Offline data cache	Data overflow handling mode selection, cache mode, cache length setting, etc.	OFF

9.2.5.2. Subscribe/Publish

The topic adding function is mainly used to add published or subscribed topics. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages.Serial port association is used to associate a topic with a serial port. When publishing, the original data of serial port will be used as the Payload of this topic. When receiving the subscription message, the Payload of the subscription topic will be sent to serial port as the original data.

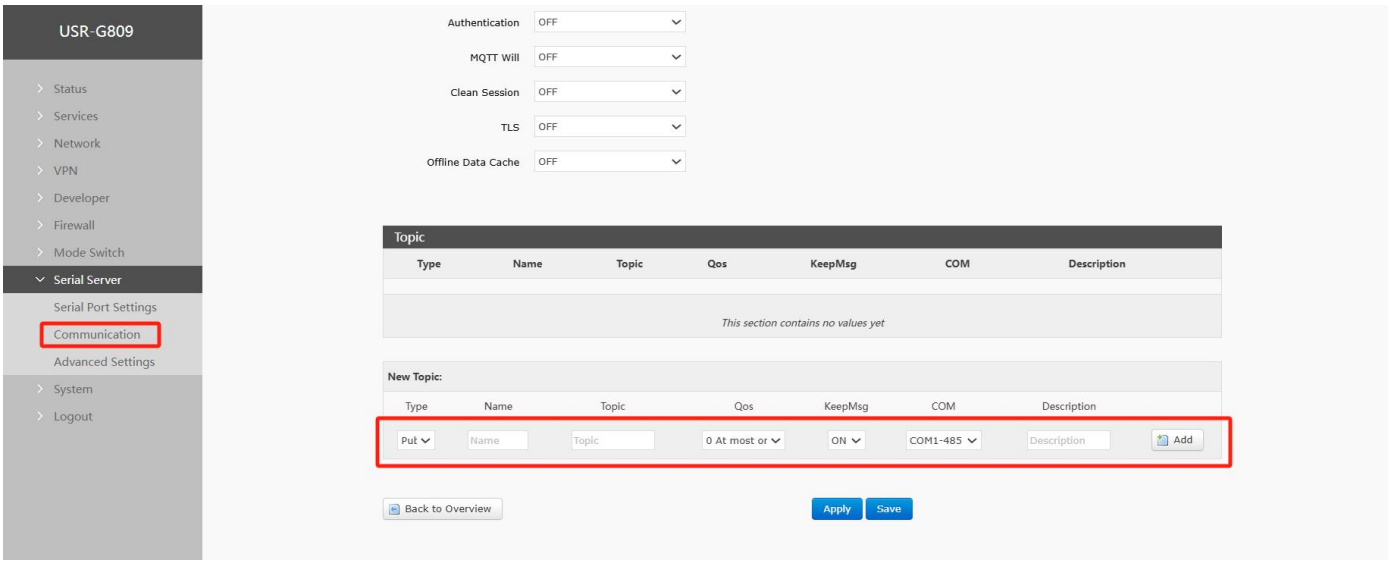


Fig. 217 MQTT Theme Configuration Interface

table 68 MQTT theme parameter table

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

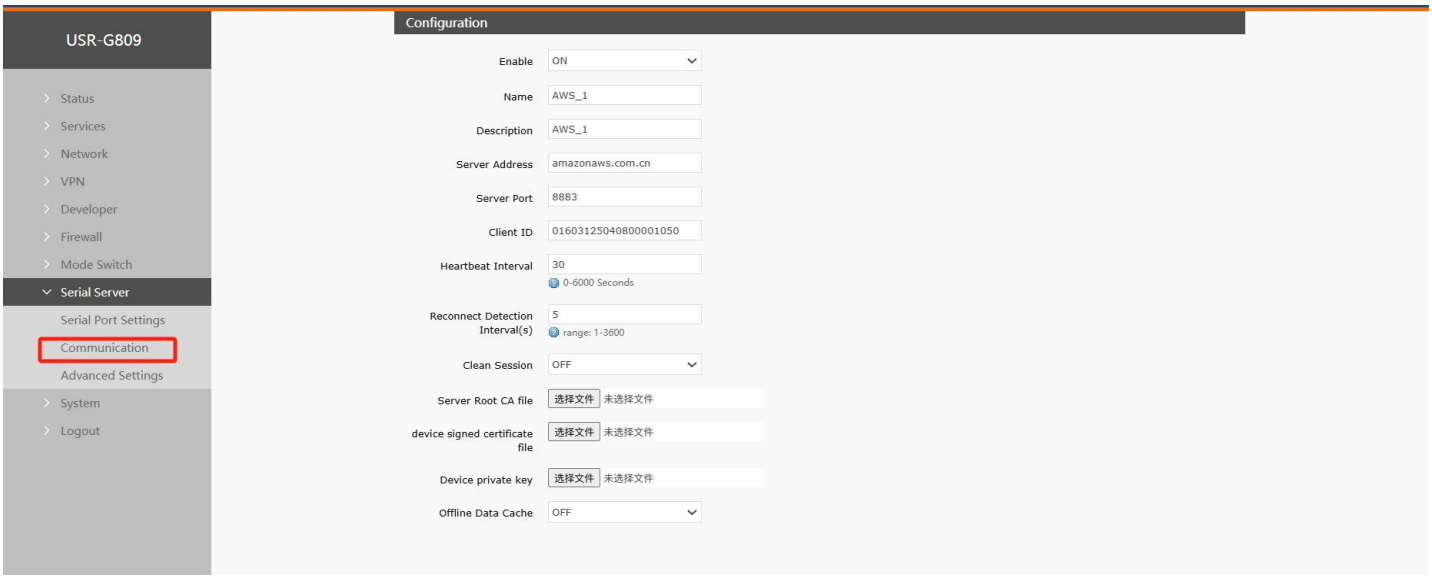
name	functional description	default
type	Topic type: optional publish/subscribe	issue
name	the name of the topic	empty
theme	Subject: Subject Content	empty
Qos	Subject message quality, settable: 0 at most once 1 at least once 2 exactly once.	0
reservation message	Set whether to keep messages, ON/OFF	ON
aisle	COM1-485: Data communication using 485 channelsCOM2-232:Data communication using 232 channels COM1+COM2:Data transmission using RS232 or	COM1-485
describe	Set comments for this theme rule	empty

Description:

- Up to16 theme rules can be set.

9.2.6. Connect to Amazon

In this mode, user terminal data can send request data to AWS platform through this device. Datapublishing and data subscription with terminal devices can be performed on the AWS platform. Both support multi-theme addition configuration. Users can send serial data to a certain theme through configuration, or send data pushed by the server to the bound serial port, so as to realize data transmission between serial port and server.



graph 218 AWS Configuration Interface

table 69 AWS parameter table

name	functional description	default
start using	Link enabled, ON/OFF	ON
name	Name of AWS Platform Link	AWS_2

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

describe	AWS Platform Link Remarks	AWS_2
server address	AWS platform MQTT server connection address: IP or domain name	amazonaws.com.cn
server port	AWS Platform MQTT Server Port	1883
client ID	AWS Platform MQTT Client Identifier	123456
heartbeat time	MQTT protocol heartbeat time, unit: seconds	30
Reconnection detection interval	Next reconnection interval after MQTT disconnection, unit: seconds	5
cleanup session	MQTT protocol connection flag bit, used to control the lifetime of the session state, OFF,ON	OFF
server root certificate	Select corresponding file	not have
Equipment Signature Certificate	Select corresponding file	not have
device private key	Select corresponding file	not have
Offline data cache	Data overflow handling mode selection, cache mode, cache length setting, etc.	OFF

9.2.6.1. Subscribe/Publish

The topic adding function is mainly used to add published or subscribed topics. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages.Serial port association is used to associate a topic with a serial port.Up to 16 theme rules can be set.

9.2.7. Connect to Alibaba Cloud Platform

Alibaba Cloud IoT Platform is a very popular public cloud platform at present. Devices support MQTT protocol to access Alibaba Cloud IoT Platform, support industrialand enterprise instances,support SSL function, and support certificateless, one-way authentication and two-way authentication to access Alibaba Cloud. In this mode, data publishing and data subscription with terminal devices can be performed on the Alibaba Cloud platform. Both support multi-theme addition configurations. Users can send serial port data to a certain theme through configuration, or flow data pushed by the server to The bound serial port enables transparent data transmission between the serial port and the server.

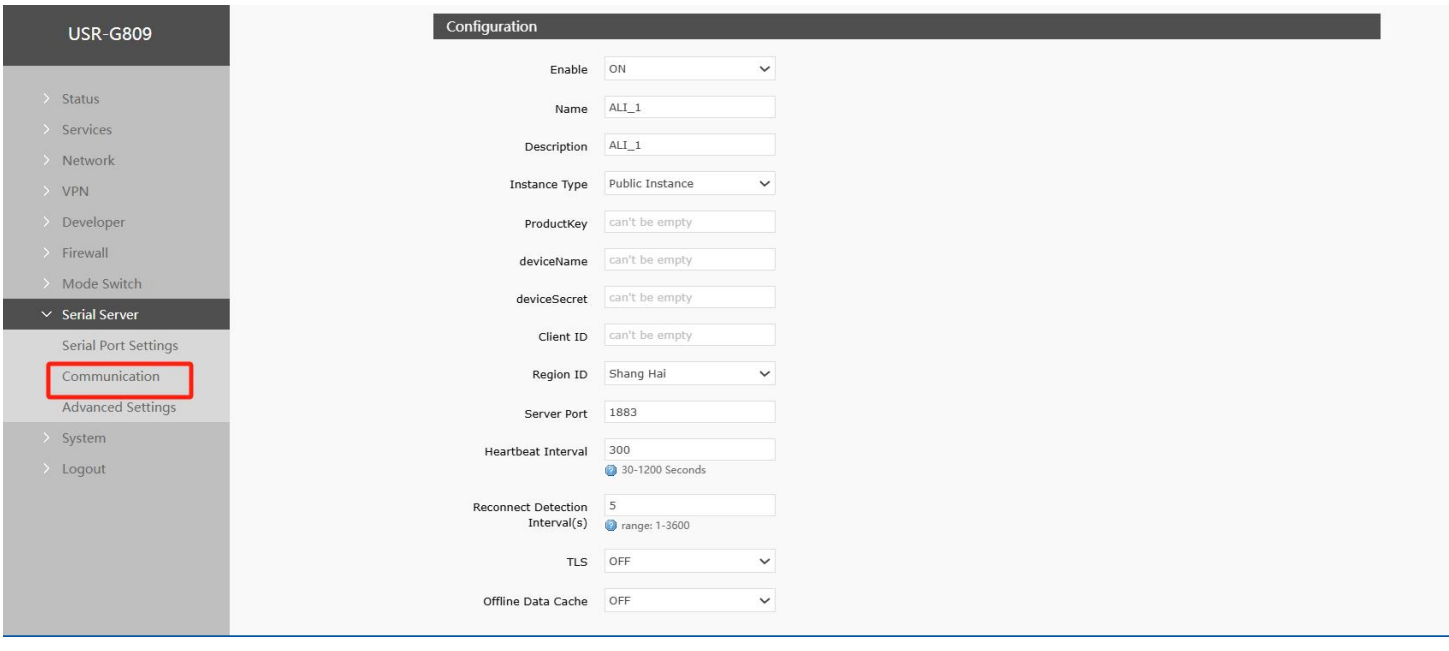


Fig. 219 ALI configuration interface

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

table 70 ALI parameter table

name	functional description	default
start using	Link enabled, ON/OFF	ON
name	Name ofALI platform link	ALI_2
describe	ALIPlatform Link Remarks	ALI_2
instance type	Support Alibaba Cloud public instances and enterprise instances	public instance
ProductKey	Device properties, Alibaba Cloud adds ProductKey of triplet in device	not have
deviceName	DeviceName of the triplet in the device added by Alibaba Cloud	not have
deviceSecret	Device Key, Alibaba Cloud Add DeviceSecre of the triplet in the device	not have
client ID	Support custom client ID for splicing MQTT clients	not have
territory	Alibaba Cloud area code, for example, East China 2 (Shanghai): cn-shanghai	East China 2-Shanghai
server port	ALI Platform MQTT Server Port	1883
heartbeat time	MQTT protocol heartbeat time, unit: seconds	300
Reconnection detection interval	Next reconnection interval after MQTT disconnection, unit: seconds	5
cleanup session	MQTTprotocol connection flag bit, used to control the lifetime of the session state, OFF,ON	OFF
TLS	Version number: TLS1.0 and TLS1.2 The authentication mode can be selected from non-authentication certificate, authentication server certificate and bidirectional authentication certificate	OFF
TLS authentication method	Do not verify certificate: that is, only implement data layer transmission decryption, and do not verify the identity of the other party during the handshake process Verify server certificate: that is, the client will verify the server certificate during handshake, and the client needs to preset the root certificate of the server. Two-way authentication: that is, the client and the server verify each other's identity, and the server root certificate, client certificate, and client private key need to be preset.	Do not verify certificates
Offline data cache	Data overflow handling mode selection, cache mode, cache length setting, etc.	OFF

9.2.7.1. Subscribe/Publish

The topic adding function is mainly used to add published or subscribed topics. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages.Serial port association is used to associate a topic with a serial port.Up to 16 theme rules can be set.

9.2.8. HTTPD mode (HTTP Clientmode)

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

Users do not need to pay attention to the data conversion process between serial data and network data packets, and only need to set simple parametersto realize the data request from serial devices to HTTP servers.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

By default, the device filters the received data and outputs only part of the user data to the serial port. The customer can choose whether to filter HTTPD data using the AT command.

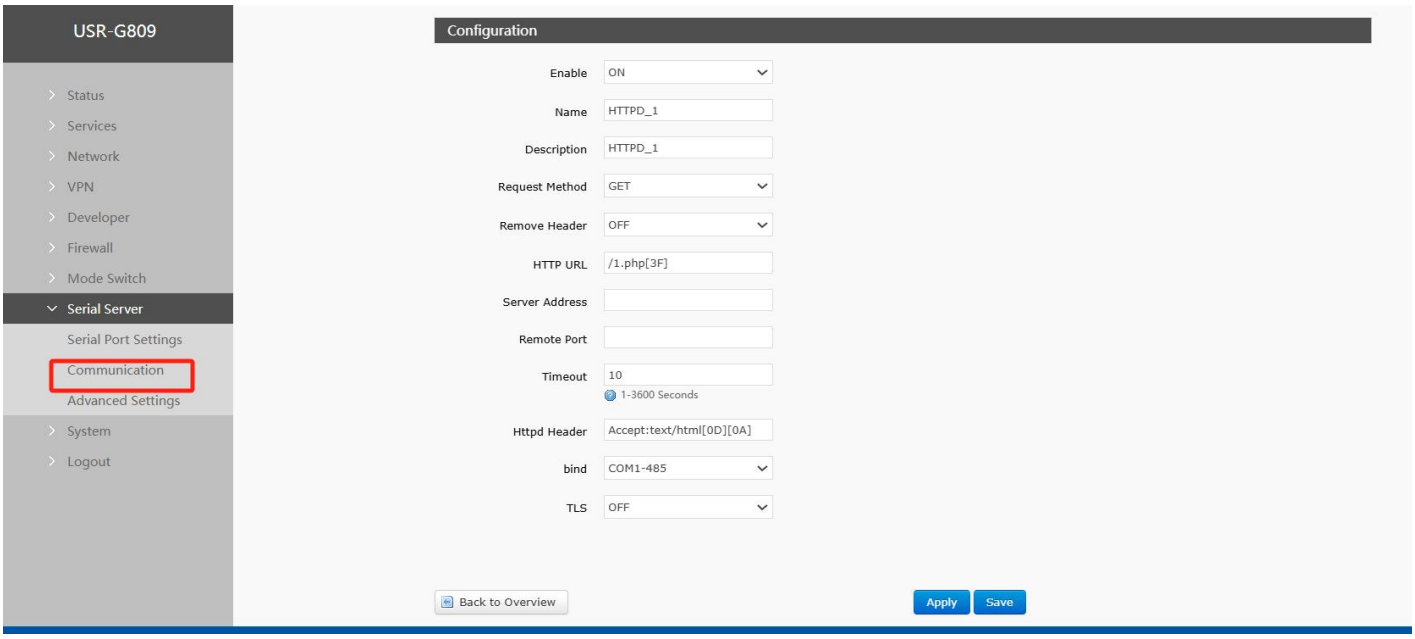


diagram 220 HTTPD configuration interface

table 71 HTTPD parameter table

name	functional description	default
start using	Enable this link channel: ON/OFF	ON
name	Name of this link	HTTPD_X
describe	Remarks for this link	HTTPD_X
request method	How to request data from	GET
	GET/POST	
filter head	Set whether to filter HTTP headers ON(filtered)/OFF (unfiltered)	ON
HTTP URL	Add the URL	/1.php[3F]
server address	HTTP server address, IP or domain name	empty
remote port	HTTP Server Port Number	empty
overtime	If the server does not actively disconnect within the timeout period, the local end needs to wait for the disconnection time, unit: seconds	10
Request header information	HTTP header information	Accept:text/html[0D][0A]
channel binding	COM1-485: Data communication using 485 channelsCOM2-232:Data communication using 232 channels COM1+COM2:Data transmission using RS232 or	COM1-485
TLS encryption	Support TLS1.0\TLS1.2\OFF	OFF

9.2.9. Registration Package/Heartbeat Package Features

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

9.2.9.1. Registration package description

Registration package: A password used to enable the server to identify the device from which the data originated, or as authorization for server functionality.Registration packets can be sent when the device establishes a connection with the server

It is also possible to splice the registration packet data at the forefront of each packet as a packet.The registration packet data can beMAC or custom registration data. Description:

- Select MAC, then WAN port MAC as registration packet content;
- This function is available only when the link is set to tcpc and udpc mode.

9.2.9.2. Network heartbeat packet description

Network heartbeat packet: sent to the network, the main purpose is to let the server know that the terminal W630S is online, so as to maintain a long connection with the server.Description:

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

9.3. Advanced settings

Can configure network AT, serial heartbeat packet and no data action.

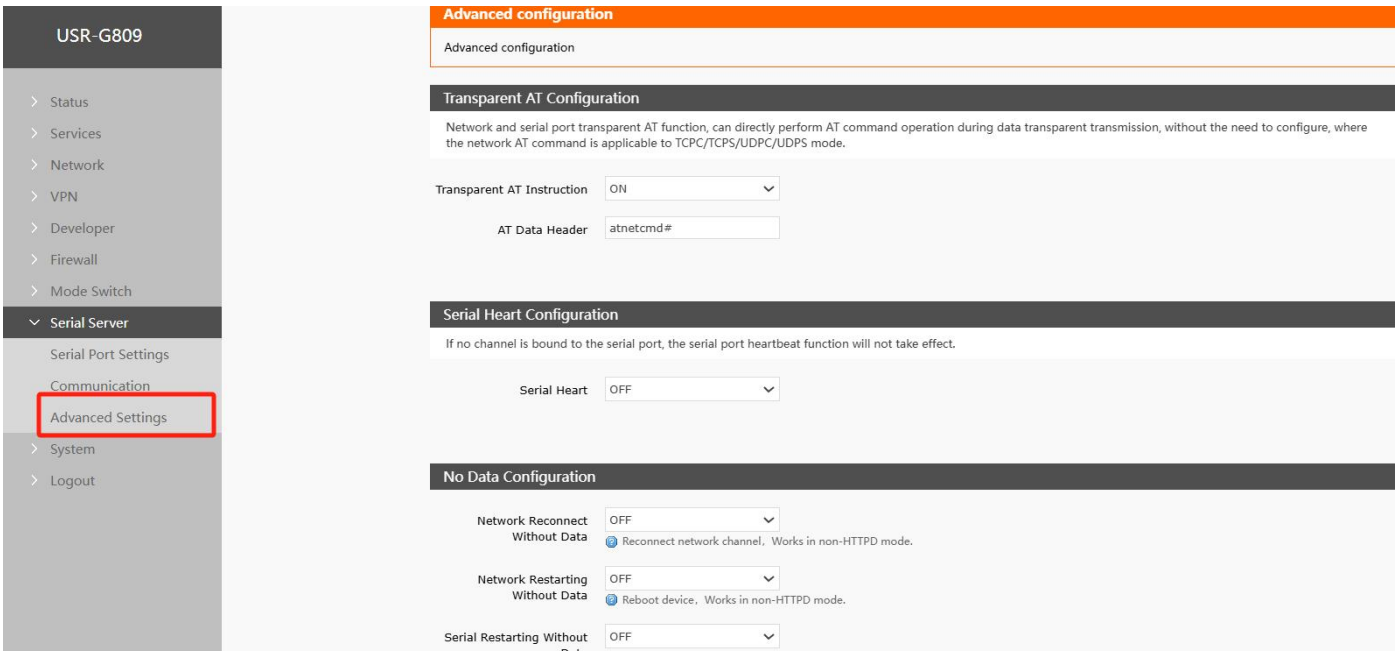


Fig. 221 Advanced Configuration Interface

table 72 Advanced Configuration Interface Parameter Table

name	functional description	default
network AT command	ON/OFF	ON
Network AT cipher word	Network AT password	atnetcmd#
Serial heartbeat	ON: Enable sending heartbeat packet to serial port OFF: Disable sending heartbeat packets to serial port	OFF
Heartbeat packet type	HEX: hexadecimal type ASCII: Character type Heartbeat package description refer to 8.2.7.2 section	HEX
heartbeat packet data	Heartbeat packet data content	empty

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

heartbeat time	The time interval between heartbeat packets sent, in seconds	60
Serial port binding	COM1-485: Data communication using 485 channels COM2-232: Data communication using 232 channels COM1+COM2:Data transmission using RS232 or	COM1+COM2
Network Channel No Data Reconnection Enable	Each channel does not receive network data within the set time, triggering reconnectionis applicable to non-HTTP protocols. For details, see the following description.	OFF
Reconnection detection interval	Set time interval in seconds	3600
Network Channel No Data Restart Enable	All channels do not receive network data within the set time,triggering device restart Applicable to non-HTTP protocols, see the following description for details	OFF
restart detection interval	Set time interval in seconds	36000
Serial port no data restart enable	Configure serial port channel No serial port data received, trigger DTU restart If dual serial ports are configured,DTU restart will be triggered if	OFF
Effective serial port	COM1-485/COM2-232/COM1+COM2	COM1-485

Description:

- Serial Heartbeat Package: Link channel (at least one communication configuration)must existforthis feature to take effect;
- Network channel no data reconnection: TCPC/UDPC/MQTT, when the set time expires and the network endtime isnot received, it will trigger its own link reconnection;
- Network channel no data reconnection:TCPS, when the set time expires, if no data is received from a client, the corresponding client will be kicked off actively;
- Network channel no data reconnection: UDPS, when the set time expires, no client data is received, serial data will not be sent to UDPC;
- Network channel no data restart: all link channels in the set time, did not receive the network end data, then the device restart;
- Network channel no data restart: if the TCPC connection success data is received within the set time, the count is reset;
- Serial port channel no data restart: in the set time, no serial port data received, DTU restart;

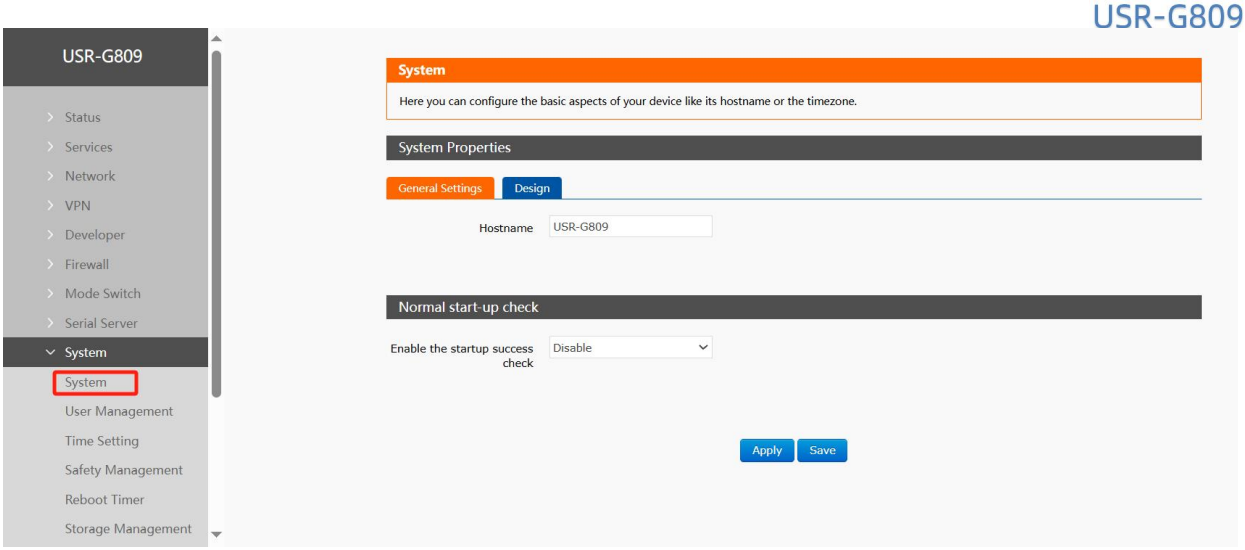
Restart the serial channel without data: If the COM1 + COM2 dual channels are set, one of the channels will not receive serial data after the set time expires, and the DTU will restart.

10. System function

10.1. host name

Default host name USR-G809.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000



10.2. Time setting

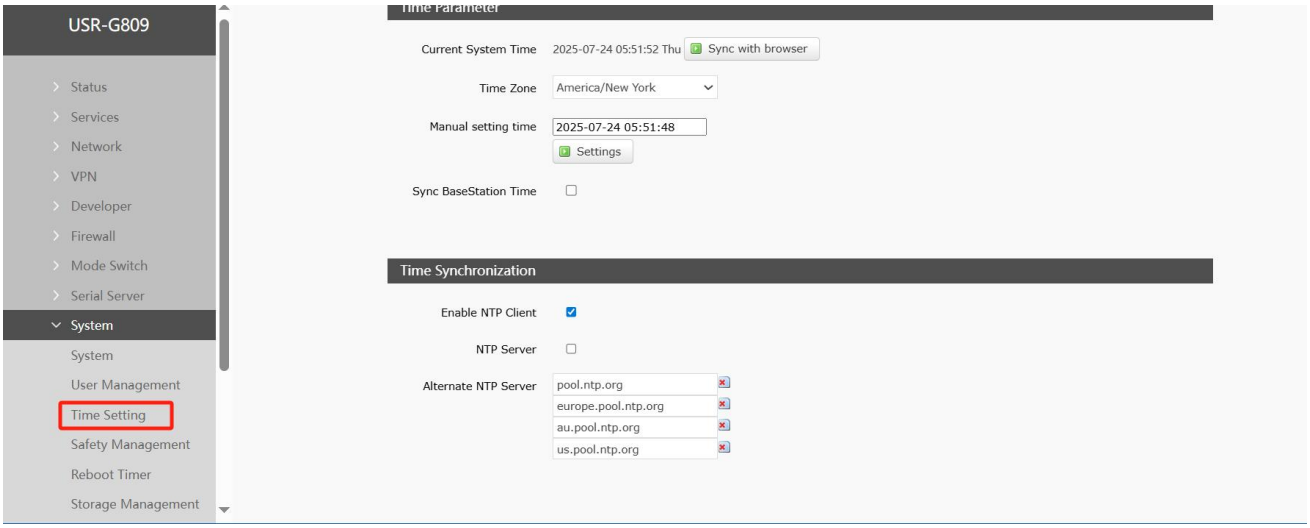


Fig. 223 NTP page

<Attention>

➢ Routers can perform network timing, and NTP client functions are enabled by default. There areNTP server address settings.

10.3. Username Password Settings

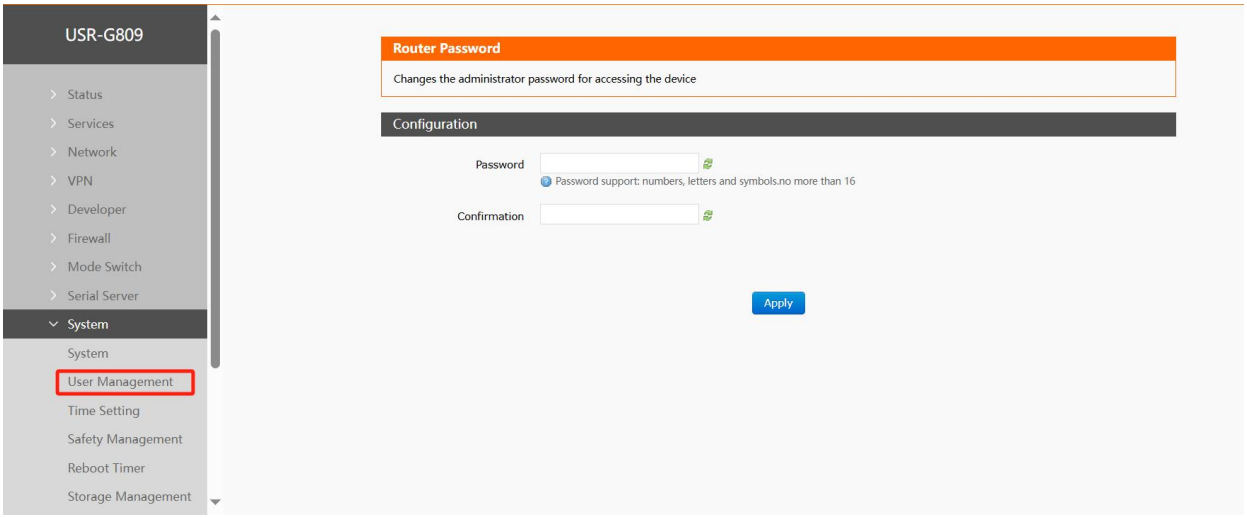


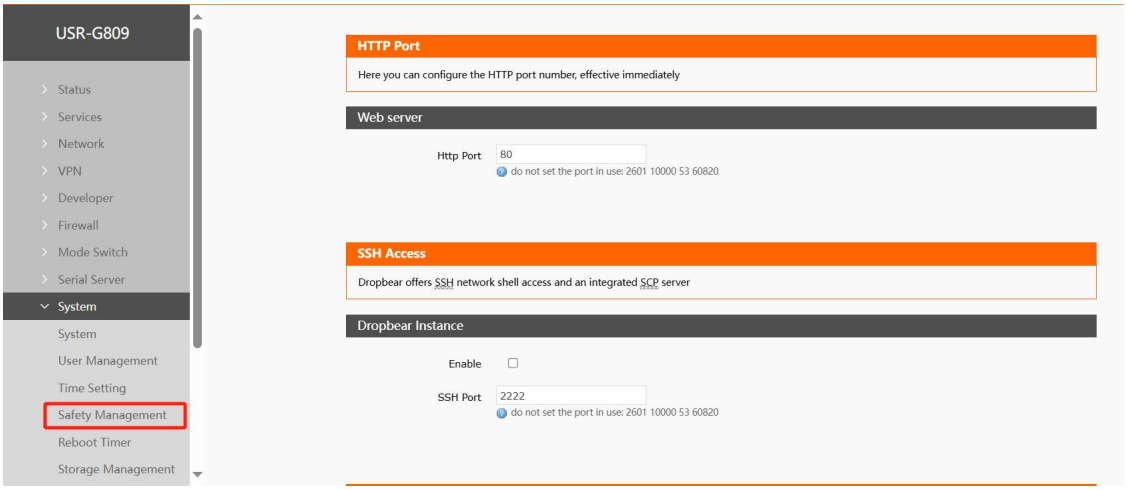
Fig. 224 Username Password Settings Page

<Attention>

- Default password can be set, default password is admin, user name can not be set.This password is the management password (web login password).

10.4. Safety management

Set the port number of the built-in webpage login, and enable and disable TELN ET and SSH functions.



graph 225 safety management

10.5. Memory management

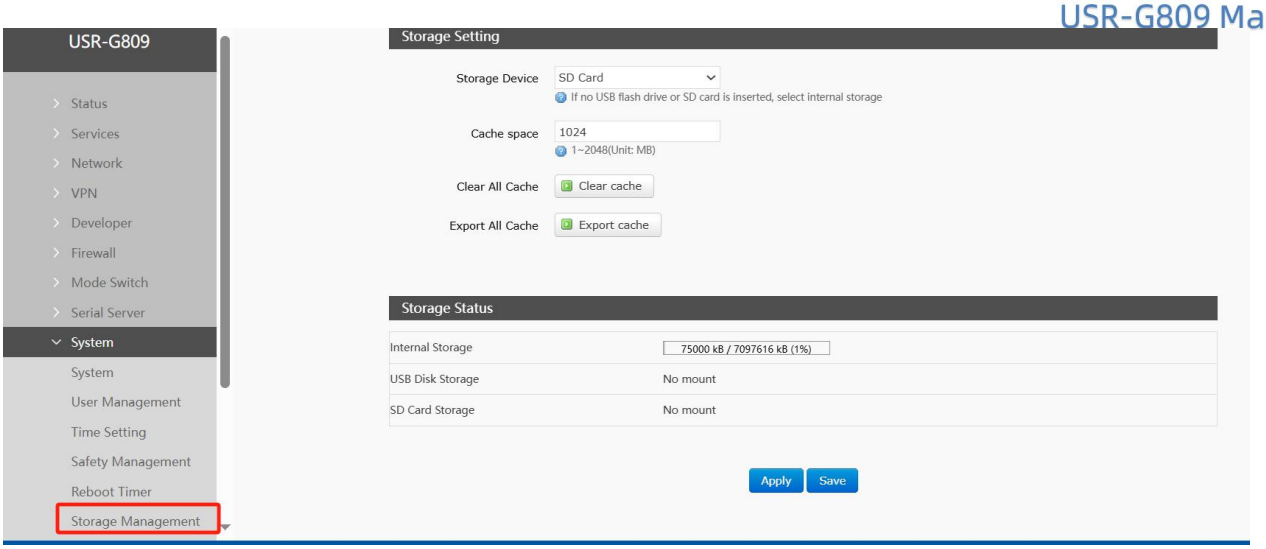


table 73 Storage management parameter table

name	functional description	default
storage device	Select cache data storage space Optional: Internal storage/USB flash drive/SD card	internal storage
cache space	Set the maximum cache space for network disconnection, unit: MB	1024
Clear all caches	Click to clear all caches in the currently selected storage device	not have
Export all caches	Click to export all caches in the currently selected storage device as compressed packages	not have

<Attention>

- Unplug USB,SD card after the need to restart the router effective.

10.6. configuration snapshot

The router can save the current configuration in the router as a snapshot. To use the configuration later, click Use Restore Configuration here.

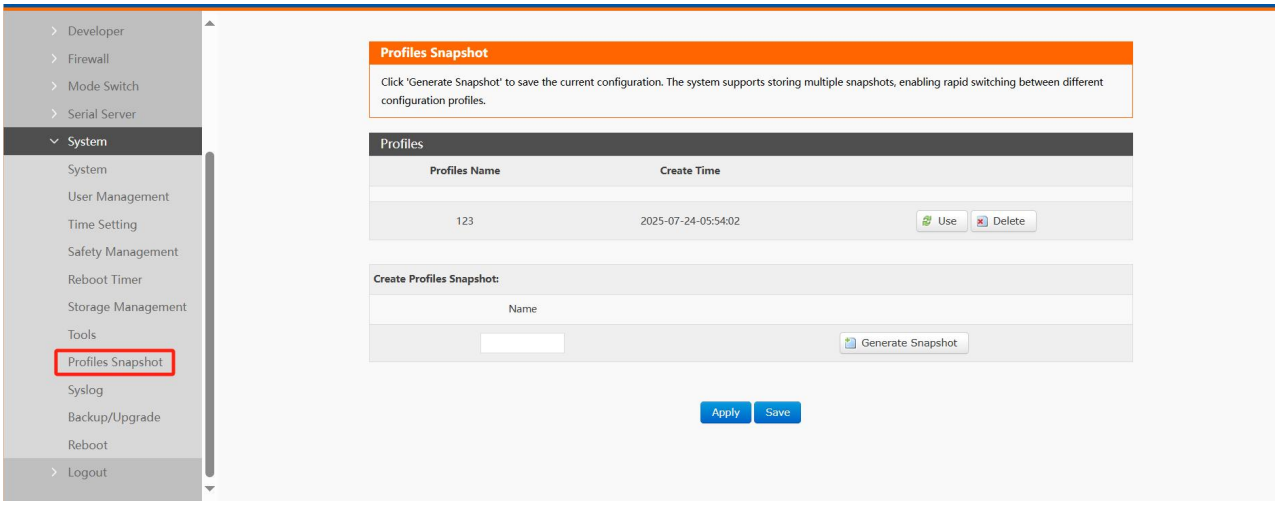


Fig. 227 configuration snapshot

<Attention>

- Snapshots will only be deleted when factory restoration, firmware upgrade without parameters, and manual click delete. Import configuration and parameter upgrade will not be deleted.
- The router supports 4snapshots.

10.7. Parameter backup and upload

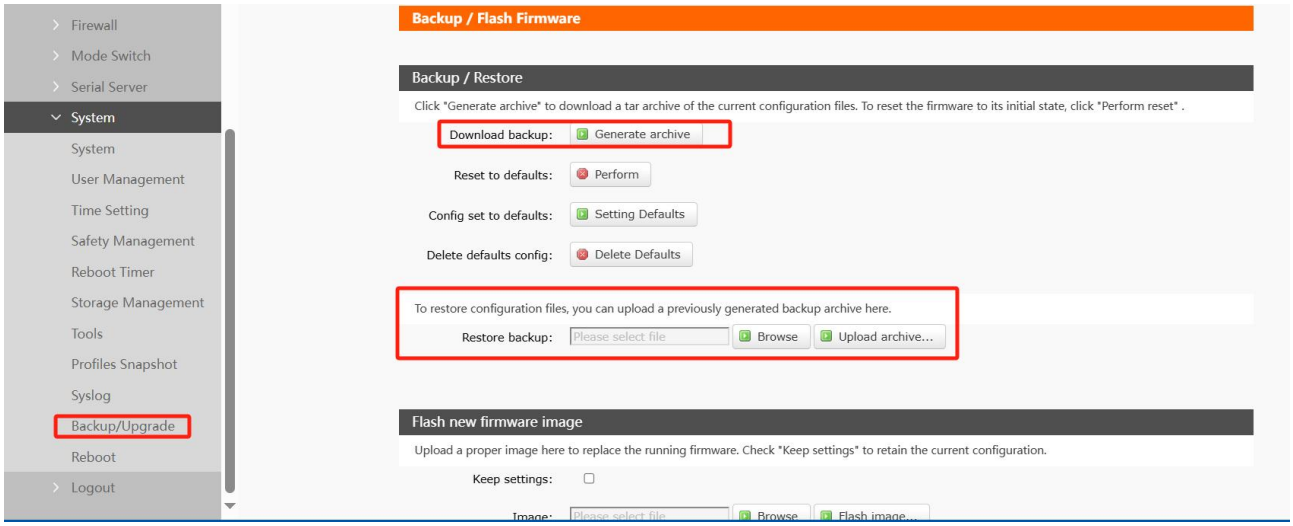


Fig. 228 Parameter Backup Upload Page

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

Note: Firmware recovery configuration is limited to the same version of firmware.Because different version parameters will cause problems, it is recommended that users restore the configuration in the same version.

Parameter backup: Click the Download Backupbuttonto backup the current parameter file as a compressed package file, such asbackup-USR-G809s-2019-09-16.tar.gz,and save it locally.

10.8. Factory data reset

The factory settings can be restored through the web page.

- The USR-G809 router can be restored to factory parameters by pressing and releasing the Reload key (factory reset key)for 5~15 seconds
- Do not power off the equipment during the recovery process, which lasts about 3 minutes;
- Factory settings can be restored through the web page, with the same functions, as follows.

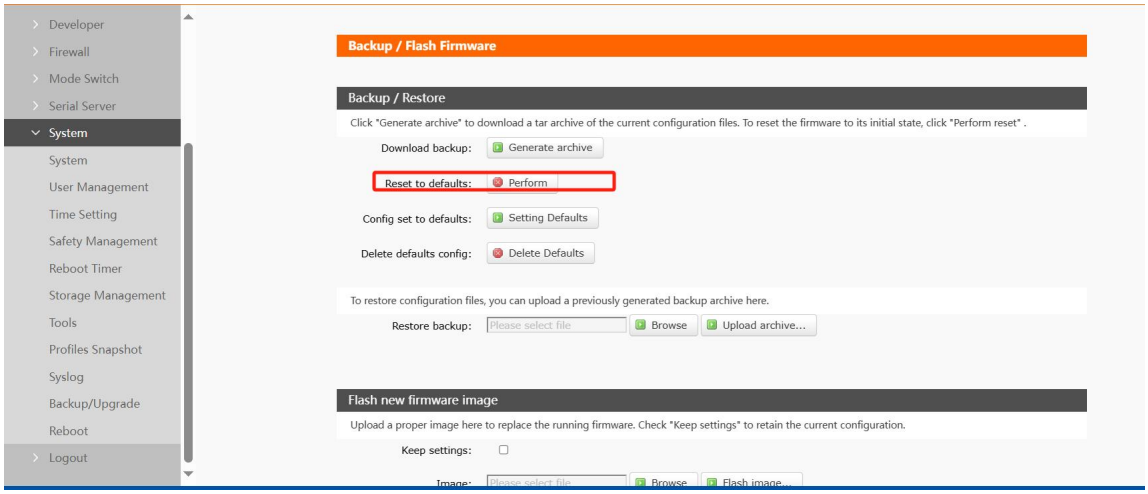
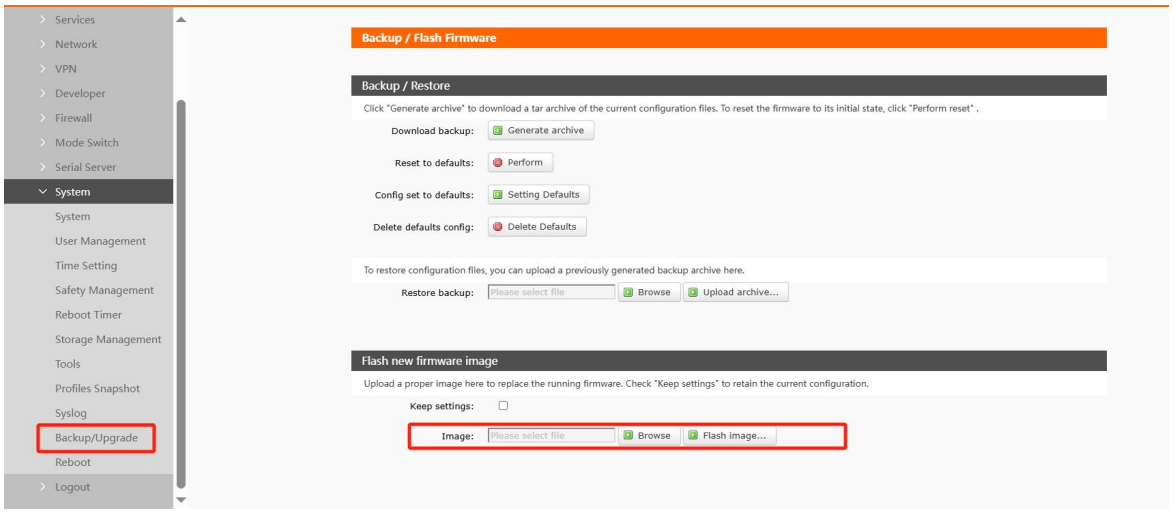


Fig. 229 Restore factory page

10. 9. Firmware upgrade

The USR-G809 module supports web-based firmware upgrades online.



<Description>

- The firmware upgrade process will take5 minutes. Please try to log in again after 5 minutes.
- You can choose whether to keep the configuration. By default, parameter upgrades are not kept (it is recommended not to keep parameter upgrades when upgrading different versions);
- Please do not turn off the power or unplug the network cable during the firmware upgrade process, otherwise the device may crash.

10.10. Set built-in web pages to neutral

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

1. Export configuration

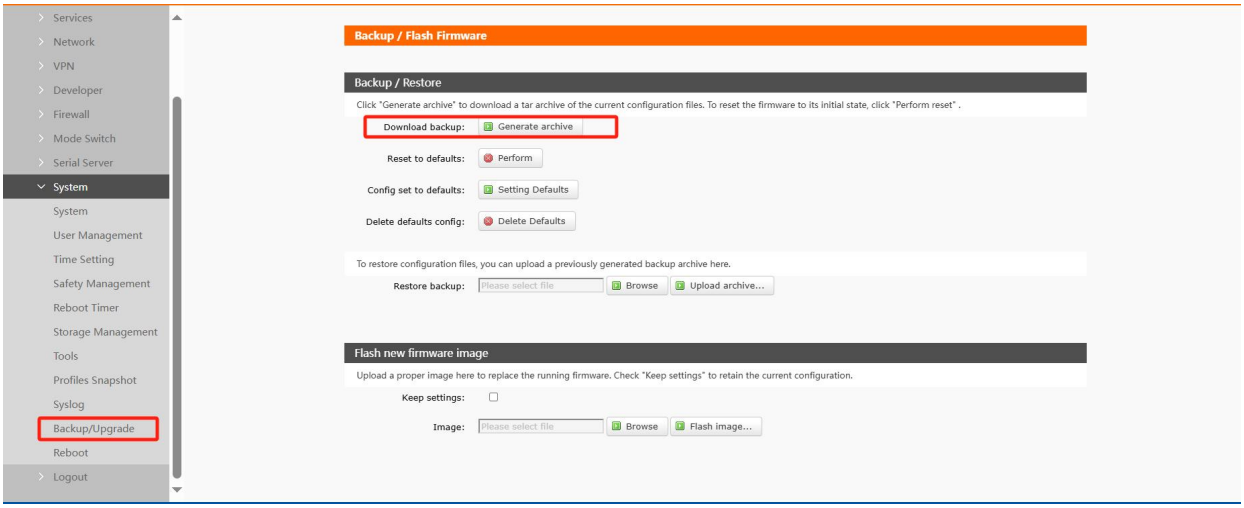


Fig. 232 export configuration

2. Unpack the configuration file and modify the configuration

The requested URL/erc/config/was not found on this server.

① Set the neutral flag bit to 1

② Customize the host name, the case is: 4G Router

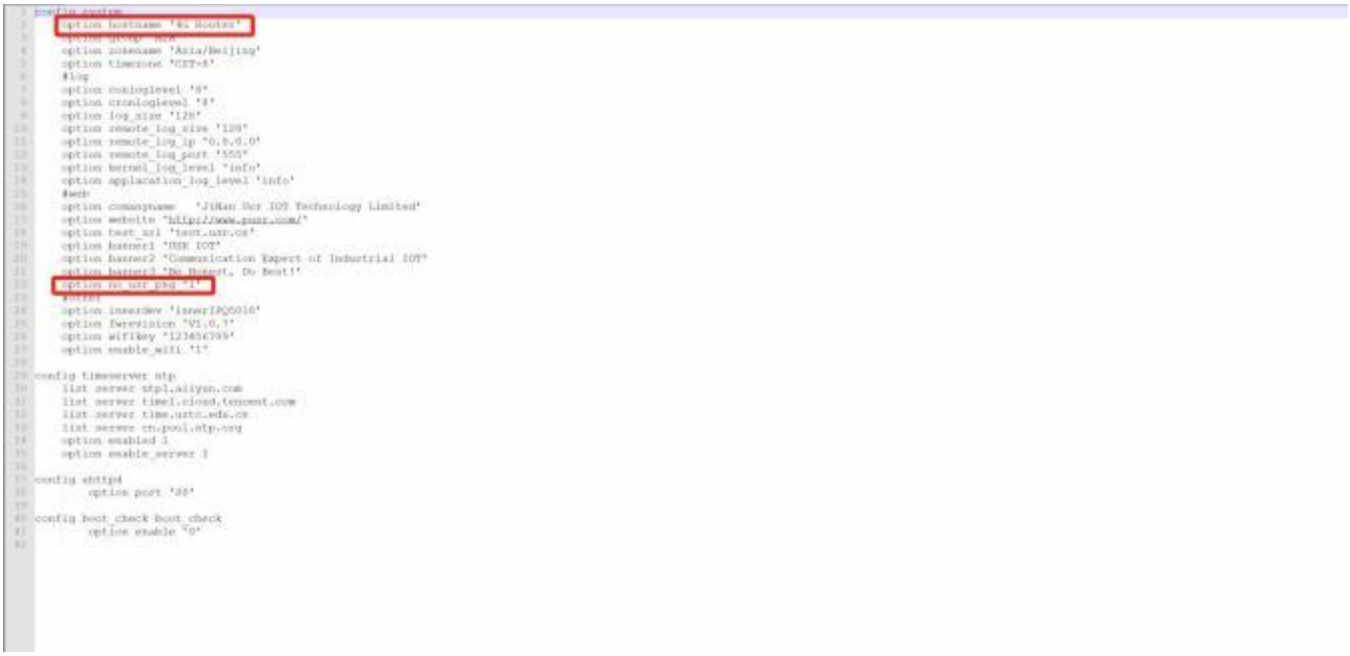


Fig. 233 modify neutral flag bit

Find the/erc/config/wireless file and open it, and modify the names of 2.4G2 + 5.8G 2SSID names. The case is modified as follows: 4G Router-MAC rear four bits-2G/5G as an example.

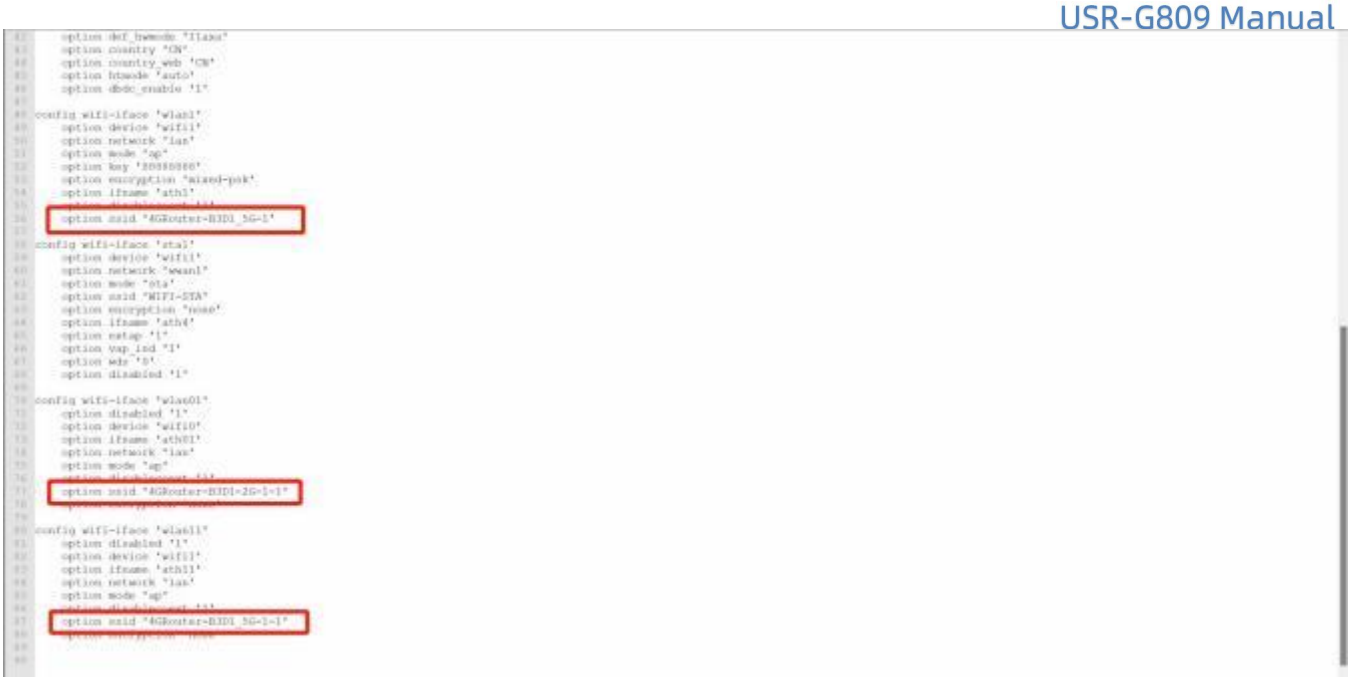


Fig. 234 modified SSID

3. Compress the modified file, note that the compression is: tar.gz suffix file.

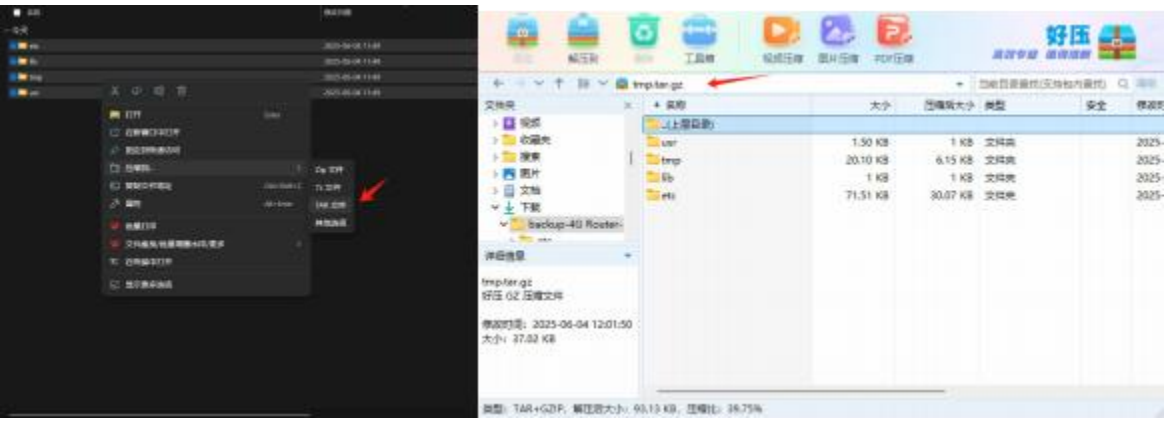
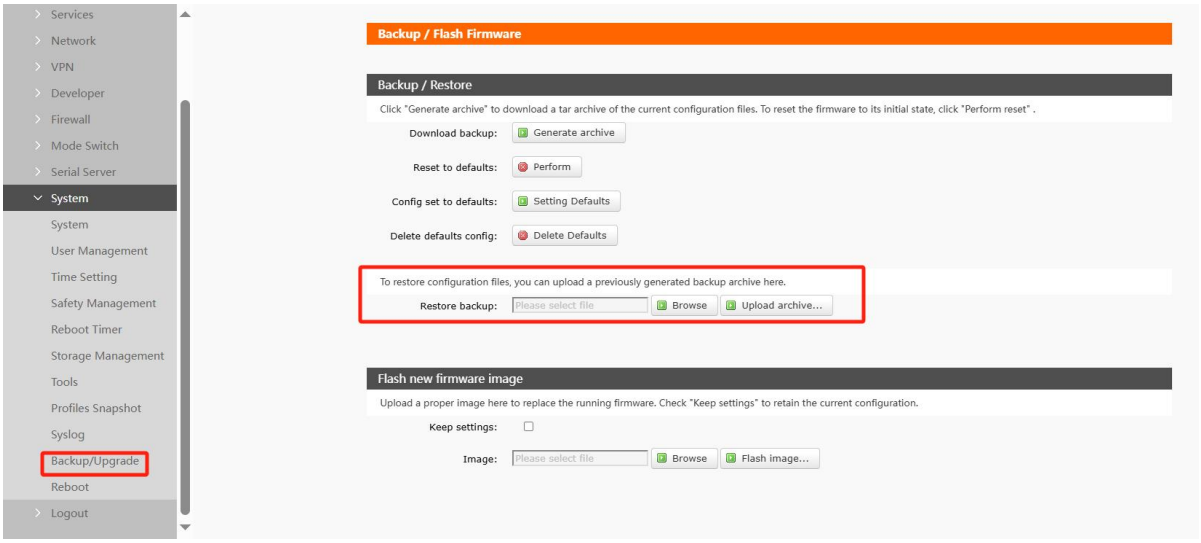


Fig. 235 compressed configuration file

4. import configuration



map 236 import configuration

5. Click Upload Backup, wait formore than 5 minutes, and log in to the router again.

<Note>

- All interfaces of this document are screenshots after neutral settings;
- If the login interface is still not neutral after being set to neutral, please try to login after clearing all browser caches.

10.11. Restart

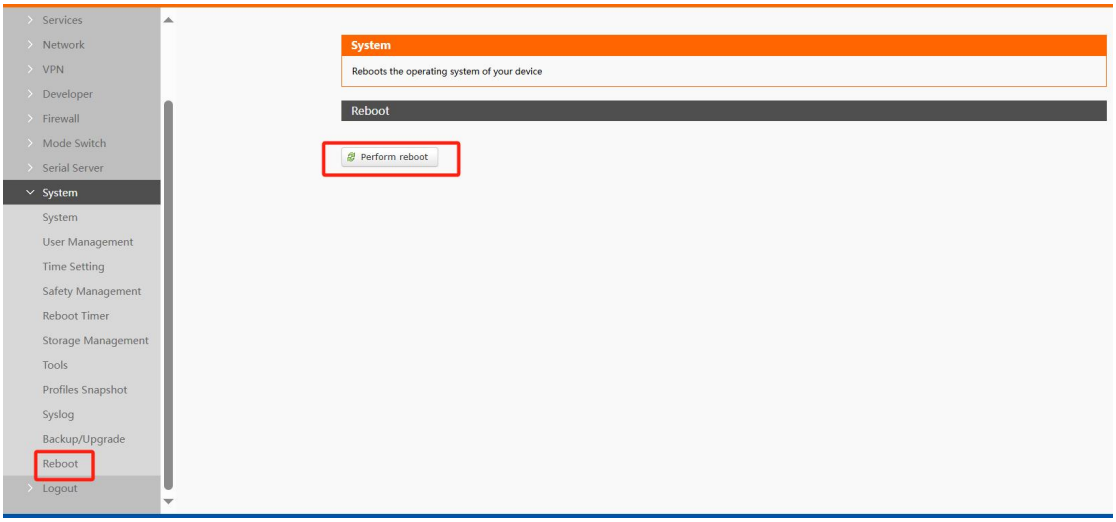


Fig. 237 Restart page

Click the button to restart the router. The restart time is consistent with the power-on startup time of the router, which is about 5 minutes after the complete startup.

10.12. Timed restart

To ensure the stability of the router operation, it is recommended to enable the scheduled restart function.This function allows users to manage the router regularly.

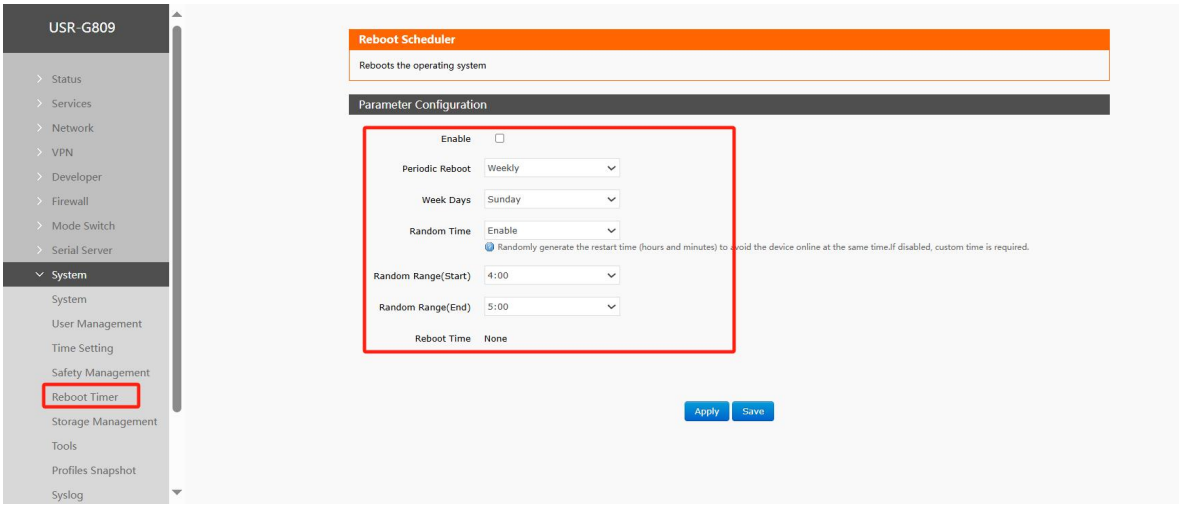


Fig. 238 Timer Restart Settings Page

<Description>

- By default, the timer restart function is turned off;
- According to the actual application, you can set up a regular restart plan that meets the conditions, such as restarting on a fixed number of days per month or a fixed number of weeks per week;
- For example:if Monday is selected in the "week", thescheduled restart task will be executed randomly at 4 - 5 o 'clock every Monday by default.

10.13. Instrument

10.13.1. Network diagnostic function

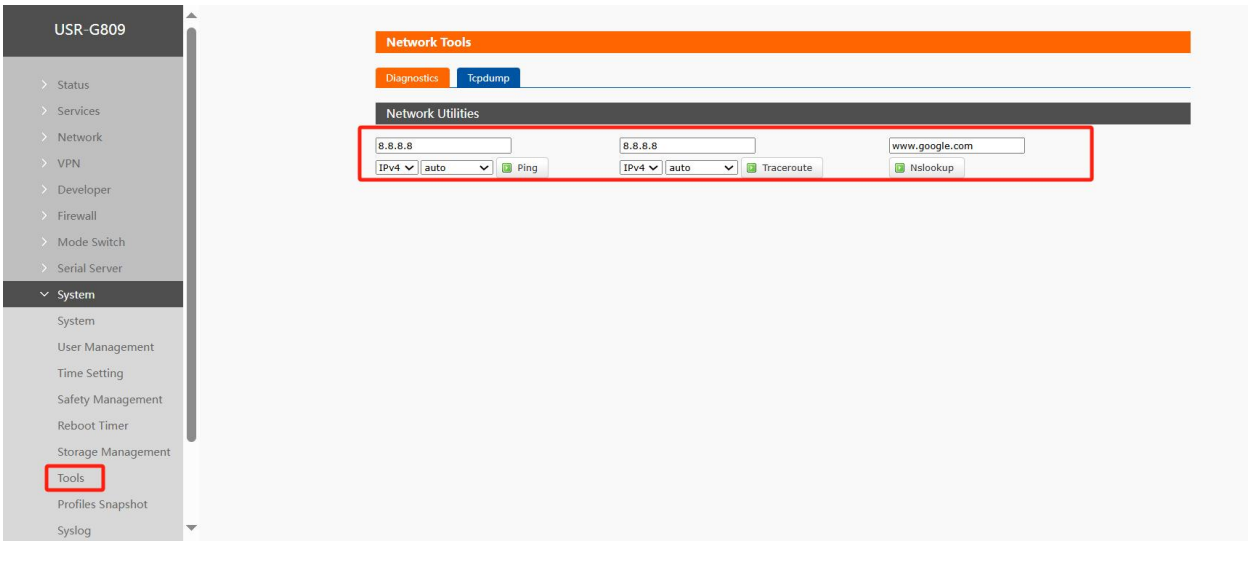


Fig. 239 Network diagnostic interface

Router online diagnostic features, including Ping tools, routing resolution tools, DNS lookup tools.

- Ping isa Ping tool that can ping a specific address directly on the router side;
- Trace route is a routing analysis tool that can obtain the routing path through which an address is accessed;
- Nslookup is a DNS viewer that resolves domain names to IP addresses.

10.13.2. TCPUDMP Traffic Monitoring

It can be accessed via the web interface.

capture limit	Capture duration or number of packets	0s
filtration	Fill in the filter conditions of the Tcpdump command, for example:port 80	empty

- Captured packets are purged after the router restarts.

10.14. log

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

Remote Log

- Remotelog server:IP of remote UDP server,remote log is not enabled when IP is 0.0.0.0
- Remotelog server port: Remote UDP server port.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

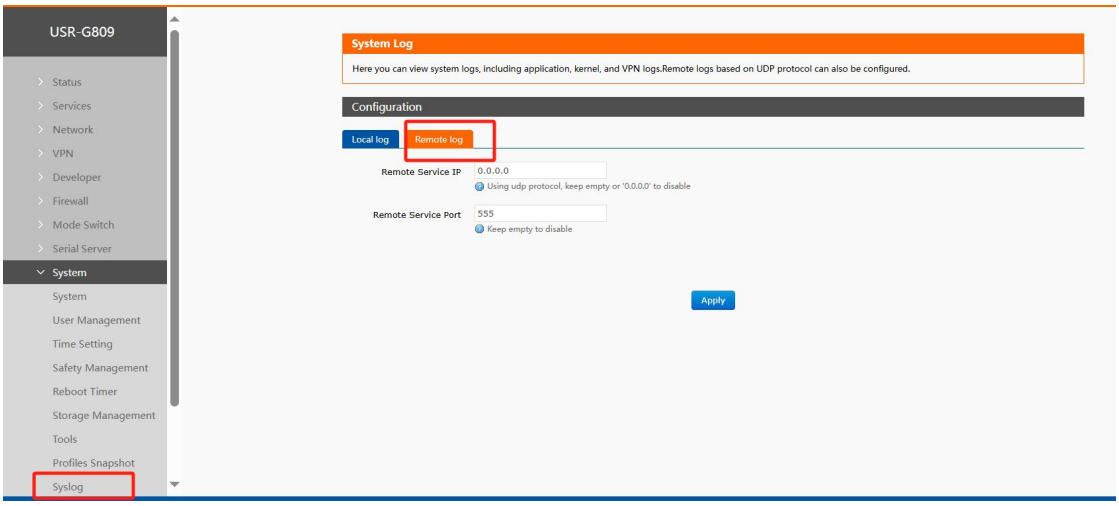
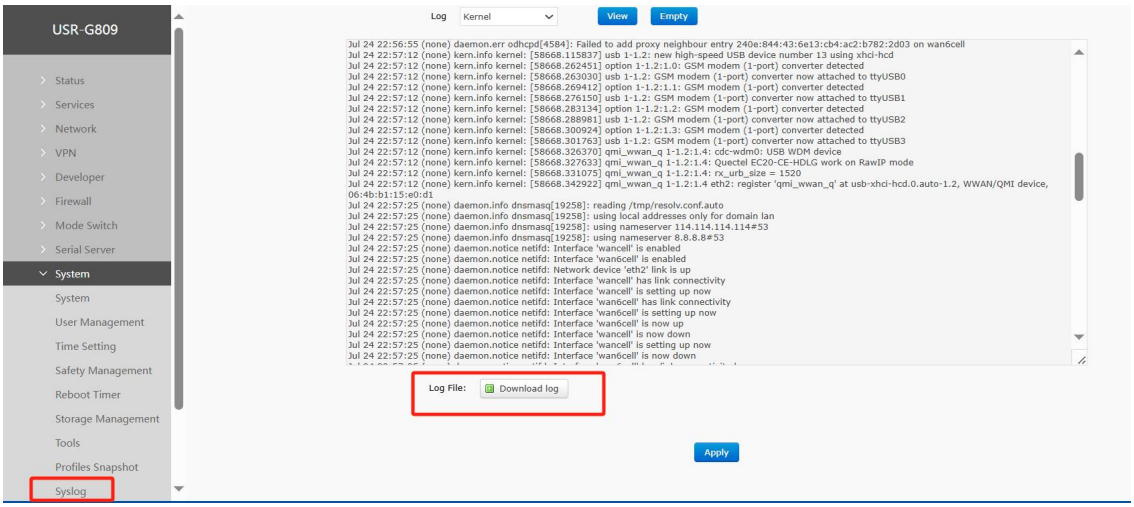


Fig. 241 Remote log page

local log

- Kernel log levels: debug, information, caution, warning, error, critical,alarm, emergency, a total of8 levels; in order, debug is the lowest, emergency is the highest;
- Application log level:same as above;
- Log (kernel, application, VPN) support instant view, empty, support log file export.



map 242 Application log page

11. AT command set

AT instruction set of router is applicable to SMS, DM platform, network and serial port.

11.1. AT instruction list

table 75 AT command summary

serial number	name	function
1	AT	Test AT command available
2	AT+REBOOT	restart the device
3	AT+CLEAR	restore the factory
4	AT+VER	Query firmware version
5	AT+MAC	Query LAN MAC
6	AT+APN1	Query/Set SIM1 APN Parameters
7	AT+APN2	Query/Set SIM2 APN Parameters
8	AT+SN	Query SN
9	AT+CSQ	Query current signal strength
10	AT+CPIN	Inquiry sim card status
11	AT+IMEI	Query IMEI
12	AT+ICCID	Query current SIM card ICCID
13	AT+CNUM	Query CUNM
14	AT+MCCMNC	Query CIMI
15	AT+SYSINFO	Query network operators and standards
16	AT+CELLULAR	Query network format
17	AT+NETMODE	Query resident network mode
18	AT+WEBU	Searchwebusername password
19	AT+PLANG	ql
20	AT+UPTIME	Query device runtime
21	AT+WANINFO	Inquiry Wan Information
22	AT+DIALINFO	Query cellular information
23	AT+LANINFO	Query LAN information
24	AT+WANN	query wan configuration
25	AT+LANN	Query/Set LAN Configuration
26	AT+LAN	Query lan configuration
27	AT+PING	Ping detection
28	AT+NETSTATUS	Get Default Routing Interface
29	AT+CMDPW	Query/set DTU transparent AT password
30	AT+DUALSIM	Query current SIM card priority
31	AT+OPVNON	Settings Open OPENVPN
32	AT+OPVNOFF	Set to turn off OPENVPN
33	AT+WIREGUARD	Set Wireguard VPN On/Off
34	AT+IPSEC	Set IPSEC VPN
35	AT+GRE	Set GRE VPN
36	AT+PPTP	Set PPTP VPN

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

37	AT+L2TP	Set L2TP VPN
38	AT+VXLANON	Settings Open VXLAN VPN
39	AT+VXLANOFF	Set VXLAN VPN OFF
40	AT+TRAFFIC	cellular traffic statistics
41	AT+WIREDTRAFFIC	Cable traffic statistics
42	AT+CLOUDPRIVATE	Query/Set DM Private Cloud Address
43	AT+AUTOREBOOT	Query/set automatic restart time
44	AT+WAP	Query 2.4G AP1 information
45	AT+WAP5G	5.8G AP1 information query
46	AT+LANMAC	Query LAN MAC
47	AT+WANMAC	Query WAN MAC
48	AT+WIFIMAC	Query 2.4G WIFI MAC
49	AT+WIFI5MAC	Query 5.8G WIFI MAC
50	AT+Z	Restart DTU
51	AT+UART	Query/Set UART Configuration
52	AT+UARTFT	Set serial port packing time
53	AT+UARTFL	Set serial port package length
54	AT+GZ	Restart location services
55	AT+GNSSFUNEN	Query/Set Location Report Enable
56	AT+GNSSMOD	Query/Set Location Reporting Mode
57	AT+SOCKGLK	Query location and report connection status
58	AT+GWKMOD	Query or set the location report type. Only independent servers can be reported.
59	AT+GHEARTEN	Query/set heartbeat type or disable heartbeat
60	AT+GHEARTTM	Query/Set Heartbeat Frequency
61	AT+GHEARTCON	Query/Set Heartbeat Packet Data Content
62	AT+GPOSTP	Query/Set Location Package Type
63	AT+GREGEN	Query/set heartbeat type or disable registry package
64	AT+GREGTP	Query/set heartbeat type or disable registry package
65	AT+GREGDT	Query/Set Registration Package Contents
66	AT+GPOSUPTM	Query/set positioning data reporting frequency
67	AT+GREGSND	Query/Set Registration Package Send Mode
68	AT+GPGGA	Querythe original dataof gga format positioning data
69	AT+GPRMC	Query the original data of rmc format positioning data
70	AT+CELLOCATION	Query base station location
71	AT+SENDSMS	send text message
72	AT+DATAUSED	Inquiry sim card traffic usage
73	AT+CELLPING	Query/Set Cellular ping Enable/Disable
74	AT+SWICHWAN	Switch optical WAN and electrical WAN
75	AT+SWICHSIM	Cut and lock SIM card

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

76	AT+GNSSINFO	Query current location information

11.1.1. AT command set

11.1.1.1. AT

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

11.1.1.2. AT+REBOOT

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

11.1.1.3. AT+CLEAR

name	AT+CLEAR
function	factory data reset
inquire	not have
set	AT+CLEAR OK
parameter	not have
explain	This command is executed correctly to restore the factory restart equipment.

11.1.1.4. AT+VER

name	AT+VER

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

11.1.1.5. AT+MAC

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

11.1.1.6. AT+APN1

name	AT+APN1
function	Query or set APN information of SIM1 card
inquire	AT+APN1 +APN:<apn_name>,<user>,<pw>,<type>
set	AT+APN1=<apn_name>,<user>,<pw>,<type> OK
parameter	apn_name:apn address, can be empty [0-62]field,supportcharacterrange [a-zA-Z0-9-.#@] user: username, can be empty [0-62] bytes, ASCII characters within [33-126] pw: password, can be empty [0-62] bytes, ASCII characters within [33-126] type: Authentication method, none/pap/chap
explain	This command is executed correctly, and the configuration takes effect after the device is restarted.

11.1.1.7. AT+APN2

name	AT+APN2
function	Query or set APN information of SIM2 card
inquire	AT+APN2 +APN:<apn_name>,<user>,<pw>,<type>
set	AT+APN2=<apn_name>,<user>,<pw>,<type> OK

parameter	apn_name:apn address, can be empty [0-62]field,supportcharacterrange [a-zA-Z0-9-.#@] user: username, can be empty [0-62] bytes, ASCII characters within [33-126] pw: password, can be empty [0-62] bytes, ASCII characters within [33-126] type: authentication mode, none/pap/chap
explain	This command is executed correctly, and the configuration takes effect after the device is restarted.

11.1.1.8. AT+SN

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

11.1.1.9. AT+CSQ

name	AT+CSQ
function	Query device cellular signal strength
inquire	AT+CSQ +CSQ:<csq>
set	not have
parameter	csq: cellular signal value
explain	

11.1.1.10. AT+CPIN

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

11.1.1.11. AT+IMEI

name	AT+IMEI

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

11.1.1.12. AT+ICCID

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

11.1.1.13. AT+CNUM

name	AT+CNUM
function	Query the current SIM card CNUM i.e. telephone number
inquire	AT+CNUM +CNUM:<cnum>
set	not have
parameter	cnum:SIM card cnum number, SIM card without number only returns+CNUM:
explain	

11.1.1.14. AT+MCCMNC

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

11.1.1.15. AT+SYSINFO

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

11.1.1.16. AT+CELLULAR

name	AT+CELLULAR
function	Query resident network mode (personal cloud only)
inquire	AT+CELLULAR +CELLULAR:<ops_net_type>
set	not have
parameter	ops_net_type: network mode
explain	

11.1.1.17. AT+NETMODE

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

11.1.1.18. AT+WEBU

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

11.1.1.19. AT+PLANG

name	AT+PLANG
function	Query web landing language
inquire	AT+PLANG +PLANG:<plang>
set	AT+PLANG=<plang> OK
parameter	plang:zh_cn/en/auto zn_cn: Chinese en: English auto: It is determined according to the current language of the browser. If the browser bit is Chinese, it will be Chinese. In other cases,it will be English.
explain	

11.1.1.20. AT+UPTIME

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

11.1.1.21. AT+WANINFO

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

11.1.1.22. AT+DIALINFO

name	AT+DIALINFO
function	Query cellular network card information
inquire	AT+DIALINFO +DIALINFO:<mac>|<ip>|<mask>|<rx_packets>|<tr_packets><rx_bytes>|<tx_bytes>
set	not have
parameter	mac: cellular network cardmacip: cellular network cardIP mask: subnet mask of cellular network cardrx_packets: number of packets received tr_packets: Number of packets sent rx_bytes: receive traffic tx_bytes: send traffic
explain	

11.1.1.23. AT+LANINFO

name	AT+LANINFO
function	Query LAN card information
inquire	AT+LANINFO +LANINFO:<mac>|<ip>|<mask>|<rx_packets>|<tr_packets><rx_bytes>|<tx_bytes>
set	not have
parameter	mac:LANcardmaci p:LANcardIP mask:LANcard subnet maskrx_packets: Number of packets received tr_packets: number of packetssent rx_bytes: received traffic tx_bytes: send traffic Note: If VLAN is configured, this command returns LAN information
explain	

11.1.1.24. AT+WANN

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

11.1.1.25. AT+LANN

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

11.1.1.26. AT+LAN

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

11.1.1.27. AT+PING

name	AT+PING
function	Execute ping command

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

11.1.1.28. AT+NETSTATUS

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

11.1.1.29. AT+CMDPW

name	AT+CMDPW
function	Query/set DTU transparent AT password
inquire	Send: AT+CMDPW Return to: cmd>
set	AT+CMDPW=<cmd>
parameter	Return OK means successful setting
explain	

11.1.1.30. AT+DUALSIM

name	AT+DUALSIM
function	Query current SIM card priority
inquire	Send: AT+DUALSIM Return: SIM1/SIM2
set	not have
parameter	SIM card currently in use
explain	

11.1.1.31. AT+OPVNON

name	AT+OPVNON
function	Open OpenVPN
inquire	AT+OPVNON= index> Return: OK
set	
parameter	Index:openvpn serial number, i.e. thenumber of openvpnreturnOK means successful setting
explain	

11.1.1.32. AT+OPVNOFF

name	AT+OPVNOFF
function	Set OpenVPN Off
inquire	not have
set	Send: AT+OPVNOFF= index> Return: OK
parameter	Index: indicates the openvpn serial number, i.e.the numberof openvpnreturnOK means successful setting
explain	

11.1.1.33. AT+WIREGUARD

name	AT+WIREGUARD
function	Set Wireguard VPN On/Off
inquire	not have
set	Send: AT+WIREGUARD= enable> Return: OK
parameter	enable:ON/OFF
explain	

11.1.1.34. AT+IPSEC

Name	AT+IPSEC
function	Set IPSEC VPN
inquire	not have
set	Send: AT+IPSEC= enable> Return: OK
parameter	enable:ON/OFF
explain	

11.1.1.35. AT+GRE

name	AT+GRE
function	Set GRE VPN
inquire	not have
set	Send: AT+GRE= enable> Return: OK
parameter	enable:ON/OFF
explain	

11.1.1.36. AT+PPTP

name	AT+PPTP
function	Set PPTP VPN
inquire	not have
set	Send: AT+PPTP= enable> Return: OK
parameter	enable:ON/OFF
explain	

11.1.1.37. AT+L2TP

name	AT+L2TP
function	Set L2TP VPN
inquire	not have
set	Send: AT+L2TP= enable> Return: OK
parameter	enable:ON/OFF
explain	

11.1.1.38. AT+VXLANON

name	AT+VXLANON
function	Settings Open VXLAN VPN
inquire	not have
set	AT+VXLANON= index> Return: OK
parameter	Index:vxlan serial number, i.e. the number of vxlanreturnOK means successful setting
explain	

11.1.1.39. AT+VXLANOFF

name	AT+VXLANOFF
function	Set VXLAN VPN OFF
inquire	not have
set	Send: AT+VXLANOFF= index> Return: OK
parameter	Index: indicates the vxlan serial number, i.e. the number of vxlanreturnedOK means successful setting
explain	

11.1.1.40. AT+TRAFFIC

name	AT+TRAFFIC
function	Check cellular speed
inquire	Send: AT+TRAFFIC Return: +TRAFFIC: rx>, tx>, timespan>, time>
set	not have
parameter	rx: sample download flowtx: sample report flow timespan: sampling time time: Current time
explain	

11.1.1.41. AT+WIREDTRAFFIC

name	AT+WIREDTRAFFIC
function	Query WAN network card speed
inquire	Send: AT+WIREDTRAFFIC Return: +TRAFFIC: rx>, tx>, timespan>, time>
set	not have
parameter	rx: sample download flowtx: sample report flow timespan: sampling time time: Current time
explain	

11.1.1.42. AT+CLOUDPRIVATE

name	AT+CLOUDPRIVATE
function	Query/Set DM Private Cloud Address
inquire	Send: AT+CLOUDPRIVATE Return: +CLOUDPRIVATE: private_en>, host>, port>
set	AT+CLOUDPRIVATE= private_en>, host>, port>Return: OK
parameter	private_en: Private Cloud Enabled 1/Disabled 0 host: private cloud IP address or domain name, query result canbe blank port: private cloud port, 0 if not set Return OK means successful setting
explain	

11.1.1.43. AT+AUTOREBOOT

name	AT+AUTOREBOOT
function	Query/set automatic restart time
inquire	Send: AT+AUTOREBOOT return answer : +AUTOREBOOT:<reboot_en>,[type],[day],[random],[time1],[time2]
set	AT+AUTOREBOOT=<reboot_en>,<type>,<day>,<random>,[time1],[time] returns an OK

parameter	reboot_en: Auto reboot enabled 1, disabled 0 type: Restart mode Weekly,monthly, dailyday, optional parameter, whenthis parameter is available, the last 4 parameters are required; without this parameter, the last 4 parameters are not required random: random time, 1 enables random, 0 disables random; when random is enabled, the last two parameters represent hours random range, whenrandom is disabled, thelast two parameters representhours and minutes time1: When random is enabled, it means random start range; when random is disabled, it means random end range; when random is disabled, it means scorereturnsOK, which means setting is successful
explain	

11.1.1.44. AT+WAP

name	AT+WAP
function	Query 2.4G AP1 WiFi SSID and password
inquire	Send: AT+WAP Return: +WAP: ssid>, pwd>
set	
parameter	ssid: SSID of pwd:2.4G1 WiFi password
explain	

11.1.1.45. AT+WAP5G

name	AT+WAP5G
function	5.8G AP1 WiFi SSIDand password
inquire	Send: AT+WAP5G Return: +WAP: ssid>, pwd>
set	
parameter	ssid: SSID of pwd:5.8G WiFi password
explain	

11.1.1.46. AT+LANMAC

name	AT+LANMAC
function	inquire
inquire	Send: AT+LANMAC Return: +LANMAC: mac>

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

set	
parameter	mac:LAN port MAC address
explain	

11.1.1.47. AT+WANMAC

name	AT+WANMAC
function	inquire
inquire	Send: AT+WANMAC Return: +WANMAC: mac>
set	
parameter	<mac>: WAN port MAC address
explain	

11.1.1.48. AT+WIFIMAC

name	AT+WIFIMAC
function	Find 2.4G WiFi MAC address
inquire	Send: AT+WIFIMAC Return: +WIFIMAC: mac>
set	not have
parameter	<mac>: WIFI MAC address
explain	

11.1.1.49. AT+WIFI5MAC

name	AT+WIFI5MAC
function	5.8G WiFi MAC Address
inquire	Send: AT+WIFI5MAC Return: +WIFI5MAC: mac>
set	not have
parameter	<mac>: WIFI MAC address
explain	

11.1.1.50. AT+Z

name	AT+Z
function	Restart DTU

inquire	Send: AT+Z Return: OK
set	
parameter	
explain	

11.1.1.51. AT+UART

name	AT+UART
function	Query/Set UART Configuration
inquire	Send: AT+UART= uart_id> Back to: +UART: uart_name>, baud>, bit>, stop>, parity>
set	AT+UART= uart_id>, baud>, bit>, stop>, parity> Return: OK
parameter	uart_id: serial number, two serial ports in total,value0 or1 uart_name: serial port name returned during querybaud: baud rate, values are as follows: 1200/2400/4800/9600/19200/38400/57600/115200/230400 bit: Data bit value 7/8 stop: stop bit value 1/2 parity: parity bit, value NONE, ODD, EVEN
explain	

11.1.1.52. AT+UARTFT

name	AT+UARTFT
function	Set serial port packing time
inquire	AT+UARTFT= uart_id> Return: +UARTFT: ft>
set	AT+UARTFT= uart_id>, ft> Return: OK means success, return others means failure
parameter	uart_id: serial number, values0 and1ft: packing time
explain	

11.1.1.53. AT+UARTFL

name	AT+UARTFL
function	Set serial port package length
inquire	Send: AT+UARTFL Return: +UARTFL: fl>
set	Send: AT+UARTFL= uart_id>, fl> Return: OK means success, return others means failure
parameter	uart_id: serial number, values 0 and 1 fl: package length
explain	

11.1.1.54. AT+GZ

name	AT+GZ
function	Restart location services
inquire	Send: AT+GZ Return: OK
set	
parameter	
explain	

11.1.1.55. AT+GNSSFUNEN

name	AT+GNSSFUNEN
function	Query/Set Location Escalation Enable/Disable
inquire	Send: AT+GNSSFUNEN Return: +GNSSFUNEN: enable>
set	Send: AT+GNSSFUNEN= enable> Return: OK
parameter	enable:0 means disable, 1 means enable
explain	

11.1.1.56. AT+GNSSMOD

name	AT+GNSSMOD
function	Query or set positioning report mode

inquire	Send: AT+GNSSMOD Return: +GNSSMOD: mode>
set	AT+GNSSMOD= mode>Return: OK
parameter	mode: reporting mode, the value is NET, only NET is
explain	

11.1.1.57. AT+SOCKGLK

name	AT+SOCKGLK
function	Query location and report connection status
inquire	Send: AT+SOCKGLK Return: +SOCKGLK: state>
set	not have
parameter	state:ON connected, OFF disconnected
explain	

11.1.1.58. AT+GWKMOD

name	AT+GWKMOD
function	Query or set the location report type. Only independent servers can be reported.
inquire	Send: AT+GWKMOD Return: +GWKMOD: type>
set	AT+GWKMOD= type>Return: OK
parameter	type: reporting type, only INDE is
explain	

11.1.1.59. AT+GHEARTEN

name	AT+GHEARTEN
function	Query/set heartbeat type or disable heartbeat
inquire	Send: AT+GHEARTEN Return: +GREGTP: type>
set	AT+GHEARTEN= type> Return: OK
parameter	type:

	ValuesUSER,ICCID, IMEI,MAC, SN,IMSI,NONE, whereNONEindicates disabled heartbeat
explain	

11.1.1.60. AT+GHEARTTM

name	AT+GHEARTTM
function	Query/Set Heartbeat Frequency
inquire	Send: AT+GHEARTTM Return: +GHEARTTM: time>
set	Send: AT+GHEARTTM= time> Return: OK
parameter	time: heartbeat frequency in s seconds
explain	

11.1.1.61. AT+GHEARTCON

name	AT+GHEARTCON
function	Query/Set Heartbeat Packet Data Content
inquire	Send: AT+GHEARTCON Return: +GHEARTCON: heart_data>
set	AT+ HEARTCON = heart_data> Return: OK
parameter	heart_data: heartbeat packet data content
explain	

11.1.1.62. AT+GPOSTP

name	AT+GPOSTP
function	Query/Set Location Package Type
inquire	Send: AT+GPOSTP Return: +GPOSTP: pos_type>
set	Send: AT+GPOSTP= pos_type> Return: OK
parameter	pos_type: positioning data type, value: RMC or GGA
explain	Set the type of positioning data reported

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

11.1.1.63. AT+GREGEN

name	AT+GREGEN
function	Query/set heartbeat type or disable registry package
inquire	Send: AT+GREGEN Return: +GREGEN: type>
set	AT+GREGEN= type> Return: OK
parameter	type: ValuesUSER,ICCID, IMEI,MAC, SN,IMSI,NONE, whereNONErepresents a disabled registration package
explain	

11.1.1.64. AT+GREGTP

name	AT+GREGTP
function	Query/set heartbeat type or disable registry package
inquire	Send: AT+GREGTP Return: +GREGTP: type>
set	AT+GREGTP= type> Return: OK
parameter	type: ValuesUSER,ICCID, IMEI,MAC, SN,IMSI,NONE, whereNONErepresents a disabled registration package
explain	

11.1.1.65. AT+GREGDT

name	AT+GREGDT
function	Query/Set Registration Package Contents
inquire	Send: AT+GREGDT Return: +GREGDT: reg_data>
set	Send: AT+GREGDT= reg_data> Return: OK
parameter	

11.1.1.66. AT+GPOSUPTM

name	AT+GPOSUPTM
function	Query/set positioning data reporting frequency
inquire	Send: AT+GPOSUPTM Return: +GPOSUPTM: interval>
set	Send: AT+GPOSUPTM= interval> Return: OK
parameter	interval: positioning data reporting frequency, unit s seconds
explain	

11.1.1.67. AT+GREGSND

name	AT+GREGSND
function	Query/Set Registration Package Send Mode
inquire	Send: AT+GREGSND Return: +GREGSND: send_type>
set	AT+GREGSND= send_type> Return: OK
parameter	send_type: sending method, valueLINK connection successfully sent once orDATA registrationpacket added to the front of each report data
explain	

11.1.1.68. AT+GPGGA

name	AT+GPGGA
function	Querythe original dataof gga
inquire	Send: AT+GPGGA Return: +GPGGA: gga>
set	not have
parameter	gga: raw data of gga format positioning data
explain	

11.1.1.69. AT+GPRMC

name	AT+GPRMC
function	Query the original data of rmc format positioning data
inquire	Send: AT+GPRMC Return: +GPRMC: rmc>
set	not have
parameter	rmc: raw data of positioning data in rmc format
explain	

11.1.1.70. AT+CELLOCATION

name	AT+CELLOCATION
function	Query base station location
inquire	Send: AT+CELLOCATION Return: +CELLOCATION: lac>, ci>
set	not have
parameter	lac: Location area code ci: cell number
explain	You need to stay online to get it.

11.1.1.71. AT+SENDSMS

name	AT+SENDSMS
function	send text message
inquire	not have
set	Send: USRPD AT+SENDSMS= phone_num>,<sms> Return: OK
parameter	phone_num: the other party's phone number SMS: Text message content
explain	

11.1.1.72. AT+DATAUSED

name	AT+DATAUSED
function	Inquiry sim card traffic usage
inquire	Send: AT+DATAUSED

	Return: +DATAUSED: kb>
set	not have
parameter	kb: SIM card usage traffic
explain	

11.1.1.73. AT+CELLPING

name	AT+CELLPING
function	Query/Set Cellular ping Enable/Disable
inquire	Send: AT+CELLPING Return: +CELLPING: enable>
set	Send: AT + CELLPING = enable> Return: OK
parameter	enable: OFF/0 disabled, ON/1 enabled
explain	

11.1.1.74. AT+SWICHWAN

name	AT+SWICHWAN
function	Switch optical WAN and electrical WAN
inquire	Send: AT+SWICHWAN Return: +SWICHWAN: wan_index>
set	AT+SWICHWAN= wan_index> Return: OK
parameter	wan_index: 1 electrical WAN, 2 optical WAN
explain	

11.1.1.75. AT+SWICHSIM

name	AT+SWICHSIM
function	Cut and lock SIM card
inquire	not have
set	AT+SWICHSIM= sim_index> Return: OK
parameter	sim_index: sim card serial number, value 1or2
explain	

11.1.1.76. AT+GNSSINFO

name	AT+GNSSINFO
function	Query current location information
inquire	Send: AT+GNSSINFO Return: +GNSSINFO: enable>, gplon>, lon>, gplat>,lat>
set	
parameter	enable: whether positioning is valid, valid A, invalid V gplon: longitude direction, E east longitude, W west longitude lon: longitude gplat: latitude direction, N north, S south lat: latitude
explain	

12. 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.

13. Update history

Manual version	update content	turnover time
V1.0.0	Create documentation and complete functional descriptions	2025-07-28

Your Trustworthy Smart IOT Partner

PUSR®
www.pusr.com

Official Website: www.pusr.com
Official Shop: shop.usriot.com
Technical Support: h.usriot.com
Inquiry Email: inquiry@usriot.com
Skype & WhatsApp: +86 13405313834
Click to view more: Product Catalog & Facebook & Youtube

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000