

Communication Expert of Industrial IOT

# **Gigabit Edge Router**

## USR-G809 Flagship

Manual



## **Be Honest & Do Best**

Your Trustworthy Smart Industrial IoT Partner



## Contents

1. Product introduction	
1.1. Product feature	6
1.2. Specification parameters	7
1.3. OLED & indicator display	
1.4. Hardware Interface Diagram	9
2. Size description	11
3. Internet operation instructions	
3.1. Cellular network	
3.1.1. Enabled	15
3.1.2. Configuration	
3.1.3. SIM configuration	
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	
3.2.3. VLAN configuration	
3.2.4. WAN/ LAN selection	
3.2.5. DHCP	
3.3. WAN port	
3.3.1. DHCP mode	
3.3.2. Static IP mode	25
3.3.3. PPPoE mode	
3.4. Network Failover	27
3.5. Wireless configuration	
3.5.1. 2.4G AP1 Configuration	
3.5.2. 5.8G AP1 Configuration	29
3.5.3. 2.4G AP2 Configuration	
3.5.4. 5.8G AP2 Configuration	
3.5.5. MAC-Filter	
3.5.6. Client information	
3.6. WWAN	
3.6.1. 2.4G Settings	32
3.6.2. 5.8G Settings	
3.6.3. AP information	
3.7. Static routing	35
4. Service function	
4.1. Dynamic domain name resolution (DDNS)	
4.1.1. Supported services	
4.1.2. DDNS takes effect	
4.1.3. functional characteristics	
4.2. GNSS	
4.2.1. Report Private Cloud	
4.3. OLED	41
4.3.1. Generalized usage	41



4.3.2. Secondary development OLED	42
4.4. Data monitoring services	
4.4.1. Basic configuration	
4.4.2. Set Link Information	
4.4.3. TCPC Data Monitoring Examples	46
4.5. Event alarm service	
4.6. SMS service	
4.6.1. Basic configuration	49
4.6.2. SMS Service	50
4.6.3. Transmission list	
4.7. SNMPD	51
5 VDN function	52
5.1 DDTD Client	
5.5. Openven TAD Bridge Instance	
5.5.1. Openvpri TAP Bruge Instance	0/
5.5.2. An example of implementing subnet interworking in Openvph ToN	
5.7. wifeguard	/b
6. Developers	81
6.1. Application management	
6.1.1. Custom program upload	81
6.1.2. Back-end implementation logic	
6.2. web console	
7. Firewall	
7.1. Basic setup	
7.2. Communication rules	
7.2.1. IP address blacklist	88
7.2.2. IP address whitelist	
7.3. Nat function	
7.3.1. IP address masquerading	
7.3.2. SNAT	93
7.3.3. Port forwarding	96
7.3.4. DNAT	
7.3.5. NAT DMZ	
7.4. Access restriction	
7.4.1. Domain name blacklist	
7.4.2. domain name white list	
7.5. custom rules	
8. Edge computing	
8.1. data point	
8.1.1. Add Slave	
8.1.2. Add Point Table	
8.1.3 Edge computing	107



8.2. IO Management	
8.2.1. IO hardware connection	109
8.2.2. IO function	
8.2.3. IO status	
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	
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



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



## 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 industrialgrade design, it provides stable and reliable networking solutions for digital upgrades in various industries.

This product adopts industrial standard, wide temperature-40°C~75°C, 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°C~+75°C 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);



#### 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.

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)		
Ethernet	Number of network ports	Version with 10 LAN ports: 2*WAN/LAN+6*LAN+2*SFP; SFP: 1*WAN/LAN+1*LAN		
Interface	Network port specifications	RJ45: 10/100 /1000Mbps, IEEE 802.3 SFP: Gigabit optical port It has 1.5KV network isolation transformer protection		
	V+, V-	Built-in power reverse protection		
	GND	Ground terminal;		
·	Tx	R5232		
Connecting	Rx	R5232		
Terminat	А	RS485		
	В	RS485		
	DI1	Digital input port		
	D01	Digital output port		
	Com	Common teminal		

## 1.2. Specification parameters



		USR-G809 Manual
	Antenna interface	2 * Standard RP-SMA-K interface (External screw and internal pins)
Wi-Fi6	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/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	Antenna interface	1 * Standard SMA-K interface (external screw and internal hole)
Function	Positioning criteria	GPS
Power Supply	Adapter	DC 12V/2.5A
Specifications	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	Hull	Aluminum alloy shell, dustproof grade IP40
Characteristics	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°C ~ +75℃
	Storage temperature	-40°C~+85°C(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	lcon	Description
PWR	ڻ ا	The power is on and always on



	<b>\</b>	Turn on WiFi
WIFI	*	Turn off WiFi
	26	2G Cellular registered
	36	3G Cellular registered
	46	4G Cellular registered
	5G	5G Cellular registered
NET	<u>۲</u> ×	No Signal
	NOT READY	No SIM card detected
	READY	SIM card detected, but not registered on the network
	53	dbm[-51 ~ -63] S3: Strong signal
DCDD	52	dbm[-63 ~ -83] S2: Medium signal
KJKF	S1	dbm[<-83] S1:Weak signal
	2	Turn on GPS
GPS	R	Turn off GPS
	0°0	DI input is in low level state (DI is off)
	~~	DI input is in high level state (DI is on)
DI		
		DO make-and-break
	Ø	DO disconnect state
DO		
DATE	2025-01-01 12:00:00 (+0800)	System date/Time zone
	SIM1:0.00MB	Displays the current month's usage (SIM1 and SIM2)
SIM	SIM2:0.00MB	
Reset	Release button Reset	Restore the release prompt at factory
	is ready	
Starting up	System booting	Device startup prompt
	Please wait	
	Upgrading	Firmware upgrade in progress
Firmware	Please Wait	
upgrade	Upgrade	The firmware upgrade was successful
	Successful	

1.4. Hardware Interface Diagram



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
СОМ	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)
Туре-С	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	No network cable inserted: off
indicator light	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



	USR-G809 Man
Communication Expert of Industrial IOT	Be Honest, Do Best! Automenestow Auto [English] † 42
USR-G809 Status	Î
System	
Overview USR-G809	
Network Status Firmware Version V1.0.03	
Firewall SN 01603125040800001050	
> Services IMEI 865827074532813	
> Network Local Time Mon Jul 21 11:35:46 2025	
> VPN Uptime Oh 31m 16s	
> Developer Load Average 1.74, 1.40, 1.09	
> Firewall	
> Mode Switch Traffic Usage	
> Serial Server sim1 monthly usage: 0 kB	
> System sim2 monthly usage: 7 kB	
> Logout	
Memory	
Total Available 697228 k8 / 923796 k8 (75%)	
Free 667080 k8 / 923796 k8 (72%)	
Cached 23572 kB / 923796 kB (2%)	

#### Query routing information and ARP tables here.

Communication Expert of Indust	rial IOT				ВеНо	onest, Do Best! <sub>Auto   English   中文</sub>
	Network S	Status				
USR-G809	The following	g rules are currently active on this system.				
✓ Status	DHCP Leas	ses				
Overview	Number of dho	cp clients				
Network Status	1					
Firewall	Hostname	IPv4-Address	MAC-Address	Leasetime remaining		
> Services	USR-SWWDN	192.168.1.136	00:0e:c6:72:70:e0	11h 58m 51s		
> Network						
> VPN						
Developer	ARP					
> Firewall	IPv4-Address		MAC-Address	Interface		
> Mode Switch	192 168 1 136		00-0ex6-72-70-e0	br-lan		
> Serial Server	152,100,1,150		00.00.00.72.70.00	LA -TURY		
> System						
> Logout	Active IDv	4 Poutor				
	Network	Target	IPv4-Gateway	Metric	Table	
	wancell	0.0.0/0	10.245.116.213	0	main	
	wancell	0.0.0/0	10.245.116.213	25	main	
	wancell	10.245.116.208/29		25	main	
		JiNan Usr IOT Technol	ogy Limited http://www.pusr.com/			

View firewall list information here.





#### 3.1. Cellular network

This router supports a 4G communication module interfacefor accessing external networks.

Communication Expert of Industrial IOT				Be Honest, Do Best!
USR-G809	WAN			
> Status	WAN Overview			
> Services	Network	Status	Actions	
Vetwork	WAN6CELL eth2	Uptime: 0h 1m 2s MAC-Address: EE4C:0D:2F:A317 RX: 181 M [4710 Pkts.] TX: 2.67 MB (5599 Pkts.) IPv6: 240e844/26:12:448b:8d11:7438:2716/64 IPv6: 240e844/26:12:448b:8d11:7438:2716/64	🖉 Connect 🛛 🗹 Edit	
Cellular Network	WAN_WIRED	Uptime: 0h 0m 0s		
Network Failover	eth0	MAC-Address: D4(AD)20(BF)63(D1) RX: 0.00 B (0 Pkts.)	🦉 Connect 📝 Edit	
Wireless WWAN DHCP Static Routes	WANCELL	Uptime:         0.1 m 12s           Wptime:         0.1 m 12s           MAC-Address:         E4C-0D:2FA317           RX:         1.81 MB (4710 Pkts.)           TX:         2.67 MB (5599 Pkts.)           IPv4:         10.245,145.207/27	S Connect di Edit	
> VPN				
> Developer				
> Firewall				
> Mode Switch				
> Serial Server				
> System				
> Logout				

#### 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



#### 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.

USR IOT Communication Expert of Industrial IOT	Be Hon	est, Do Best! <sub>Auto∣English∣‡1</sub> ≵
USR-G809  Status Services  Network  WAN LAN  Cellular Network Network Failover Wireless WWAN DHCP Static Routes VPN DHCP Static Routes VPN Developer Firewall Mode Switch Serial Server	Cellular Network Configuration         Settings for APN address, usemanne and password, if you goning to use an APN card, please fill in the form correctly.         Effective configuration search priority, can improve the network search time.         Be sure to fill in the correct configuration, otherwise 5G will be unable to access the Internet.         Configuration         Configuration         SM1 Config       SM2 Config         Module Info       AT Test         Enable Cellular       Improve the network	AUD   15(00)   452
> Logout		

## 3.1.2. Configuration

Configuration
Cellular Configuration SIM1 Config SIM2 Config Module Info AT Test
Sim Card Switch Enable
Dual SIM Switching Mode Master Standby Mode
Set the dual-SIM switchover mode
SIM Card Priority Auto
It is to be a selected SIM card, 'Auto' means to record the SIM card dialed last time and uses it.
SIM Switching Cycle 300
 reached, Value range: 180~86400s.
Signal Strength Detection 🛛 🕼 Once selected, when signal blow threshold will send alarm
Enable
Continu Dial Failures 2
Signal value that triggers SIM card switchover(1-50)
Link Detection Enable 🛛 🖉 🎯 Once selected, check the network connect with ping
Interval(s) 10
ping interval unit: sec,1-86400
 Package size 0
O-10248ytes
Detection Address 1 119.29.29.29
Set the first address for ping cneck. It use ipvo, please add [ipvo] address, such as (2400:3200:1)



#### **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.

Configuration	
Cellular Configuration	SIM1 Config SIM2 Config Module Info AT Test
Status APN Name	autocheck
Services	Input your APN Name, 0-62 characters
Network User Name	
WAN	User name for apn, 0-62 characters
LAN Password	
Cellular Network	User password for apn, 0-62 characters
Network Failover	PAP&CHAP 🗸
Weiler	Authentication type for apn
CID	1
WWAN	PDP context identifier
DHCP PDP Type	IPv6 🗸
Static Routes	IPv4
VPN Network Mode	IPv6
Developer	G or 5G network IPv4&IPv6
Firewall Network Search Priority	AUIU
Mode Switch	Configuration search priority, can improve the network search time
Serial Server IMS	Enable 🗸
System	Onfig IMS
Volte	Enable

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	voluntarily
	Settings:Auto/2G/3G/4G	
frequency band	Network Mode	Auto
	Select 4G	
	Active Auto:	
	Unlocked Frequency Input specified frequency band: for example, input 1 lock BAND1 band	
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	1234
	Note: PIN enable item is not open, this PINcode setting is	



	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(l Pv6)	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

## <<u>Attention></u>

> 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



	USR-G809		
_		Version Number:	CC20CEWDLOR00A05MH U
	Status	IMEI Number:	865827074392013
	Services	Dial SIM:	sim2
	Network	SIM Card Status	READY
	WAN	SIM Card ICCID:	8986002++0200000
	LAN	SIM Card IMSI:	46011:11702
. [	Cellular Network	MCC:	460
	Network Failover	MNC:	11
	Wireless	Signal Strength:	13
	WWAN	Operator Information:	CHN-CT
	DHCP	APN Configuration:	ctnet,ctnet@mycdma.cn,vnet.mobi,1
	Static Routes	Network Type:	FDD-LTE(4G)
	VPN	Location Area Code:	5277
	Eirouoll	Band:	LTEBAND1
	Mode Switch	Cell Identifier:	8C6C686
	Serial Server	IP Address:	10.245.145.207
	System	IPv6 Address:	240e:844:42:6c12:ec4c:dff:fe2f:a317/64Global,240e:844:42:6c12:448b:8d11:7438:2716/64Global,
	Logout	Attachment State:	1

#### 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.

USR-G809	Cellular Network Configuration
<ul><li>Status</li><li>Services</li></ul>	Settings for APN address, username and password, if you goning to use an APN card, please fill in the form correctly. Effective configuration search priority, can improve the network search time. Be sure to fill in the correct configuration, otherwise 5G will be unable to access the Internet.
Vetwork WAN LAN	Configuration Cellular Configuration SIM1 Config SIM2 Config Module Info
Cellular Network Network Failover Wireless	Send Cellular AT
WWAN DHCP	W Send
Static Routes	+CPIN: READY OK
Developer     Firewall     Mode Switch	Send at cmd to module
Serial Server     System	Apply Save
> Logout	

#### 3.2. LAN interface

LAN port is a local area network.



atus	LAN Overview			
rvices	Network	Status	Actions	
twork AN	LAN وع (ی <del>ند</del> ی ی ی br-lan	Uptime: 0h 58m 41s MAC-Address: 04AD:208FB3:03 &) TX: 1432 PM (64788 Pkts.) TX: 30.35 MB (48329 Pkts.) IPv4: 1927:168.1.1/24 IPv6: 6497:21bit.2075:1/60	🥙 Connect 🛛 🔣 Edit	
llular Network twork Failover	Vlan Management			
reless	Enable Vlan			
VAN	Global network ontion	ne		
ICP	IPv6 ULA-Prefix	fd97:21bb:2d07::/48		
tic Routes				
N				
veloper		Apply Sav	e	
ewall			-	
de Switch				
ial Server				
iur ber ver				

USR-G809 Common Configuratio	on
General Setup	
> Status Status	s Uptime: 0h 59m 4s
> Services	MAC-Address: D4:AD:20:8F:B3:D3 8/8 RX: 15.27 MB (49688 Pkts.)
✓ Network	br-lan TX: 30.81 MB (49295 Pkts.) IPv4-192.168.1.1/24
WAN	IPv6: fd97:21bb:2d07::1/60
LAN	
Cellular Network Protocol	Static address
Network Failover IPv4 address	s 192.168.1.1
Wireless IPv4 netmask	k 255.255.255.0
WWAN Ind asterior	
DHCP	
Static Routes IPv4 broadcast	
> VPN Use custom DNS servers	s 114.114.114.114 🗶
> Developer	8.8.8.8
Firewall IPv6 assignment length	n 60 🗸
Mode Switch	Ø Assign a part of given length of every public IPv6-prefix to this interface
Serial Server IPv6 assignment hint	t
> System	w ranger preix parts saming sits resolutioning subprens to for unit interfaces
> Logout	

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.	
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



> 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).

	USR-G809	A .		8.8.8.8
			IPv6 assignment length	60 ~
	S (24.4			Assign a part of given length of every public IPv6-prefix to this interface
	Status		IBv6 accionment hint	
	> Services		1PV0 assignment mit	Assign prefix parts using this hexadecimal subprefix ID for this interface.
	✓ Network			
	WAN			
- [	LAN		DHCP Server	
	Cellular Network			
	Network Failover		General Setup IPv6 Set	tings
	Wireless		Ignore interface	Disable DHCP for this interface.
	WWAN		Start Address	100
	DHCP			Dowest leased address as offset from the network address.
	Static Routes		Limit	150
	> VPN			Maximum number of leased addresses.
	Developer		Leasetime	12h
	> Firewall			Opring time of leased addresses, minimum is 2 minutes (2m).
	> Mode Switch	L _		
	> Serial Server		Back to Overview	Looks Com
	> System		Back to overview	ADVA 23AAG
	Locout	-		

## <Description>

> You can adjust the 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	Disable: Disables routing advertisements	relay mode		
Advertisement	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			



		USR-G809 Manua
DHCPv6 Services	Disable: Disable DHCPv6 services	relay mode
	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	
NDP-Agent	Disable: Disable NDP proxy services	relay mode
	Relay mode: Relay NDP(Neighbor Discovery Packet) to cellular interface	
	Mixed mode: Allows devices to use both NDP proxy and standard NDP	
DHCPv6 mode	Stateless: Configure IPv6addresses automatically	stateless + stateful
	Status: DHCP Server assigned address fully enabled	
	Stateless + stateful: devices canobtainIPv6 addresses and	
	other network configuration information through DHCPv6	
	servers, and IPv6 addresses can also be automatically	
	configured through SLAA C.	
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

> 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.

	LAN Overview					
	Network	Status			Actions	
-	LAN 8 <sup>2</sup> (聖神会会会会) br-lan	Uptime: 0h 6 MAC-Addres RX: 16.05 MB TX: 33.53 MB IPv4: 192.168 IPv6: fd97:21	0m 14s (52308 Pkts.) (52771 Pkts.) 3.1.1/24 bb:2d07::1/60	:B3:D3	S Connect	Edit
ork	Vlan Management					
	Enable Vlan 🗹		J			
	Vian List			PORTS		
	Network Interface	LAN1	LAN2	LAN3	LAN4 V	WAN_WIRED ¥
	lan(br-lan)					
	lan2(br-lan2)					
	lan3(br-lan3)					
	lan4(br-lan4)					
	Design and the second second second second second second					



> 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 is turned on, LAN 4can be set to WAN 2\_WIR (shell screen WAN 2/LAN 4), WAN\_WIRED can be set to LAN (shell screen WAN1/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.



	Active DHCP Leases				
	Hostname	IPv4-Address	MAC-Address	Leasetime remaining	
	USR-SWWDN	192.168.1.136	00:0e:c6:72:70:e0	11h 27m 37s	
	Active DHCPv6 Lease	es			
	Hostname	IPv6-Address	DUID	Leasetime remaining	
	There are no active leases.				
Network					
Failover	Static Leases				
	Hostnan	10	MAC-Address	IPv4-Address	
			This section contains no val	lues vat	
outes			This section contains no va	ino yer	
	New rule:				
	Hostname	MAC-A	ddress	IPv4-Address	
		III.IE.		man.	
itch	New rule		~	~	Add
erver					
			Apply Save		
<b>T</b>					

#### 3.3. WAN port

G809	WAN			
atus	WAN Overview			
rvices	Network	Status		Actions
etwork	WAN6CELL E eth2	Uptime: 0h 32m 31s MAC-Address: Et-4C:0D:2F:A3:17 RX: 41.63 MB (61779 Pkts.) TX: 17.56 MB (63890 Pkts.) IVv6: 240e:844:42:6c12:448:btd11:7438:2716, IVv6: 240e:844:42:6c12:ec4c:dtffte2fta317/64	Cellular IPv6	🖉 Connect 🔣 Edit
ilular Network stwork Failover ireless	WAN_WIRED	Uptime: 0h 0m 0s MAC-Address: D4:AD:20:BF:B3:D1 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Ethernet WAN	🖉 Connect 🛃 Edit
WAN HCP atic Routes	WANCELL	Uptime: 0h 32m 41s MAC-Address: E:4AC0D:2F:A3:17 RX: 41.63 MB (61779 Pkts.) TX: 17:56 MB (63990 Pkts.) IPv4: 10.245.145.207/27	Cellular IPv4	& Connect
per				
witch				
rver				
-				

## <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

USR-	-G809			_						
			WAN - WAN_WIRED							
> Status	5		interfaces separated by space	es. You can also u	nterfaces, you ca ise <u>VLAN</u> notatio	n Dridge several interface n INTERFACE, VLANNR (e.g.	s by ticking the bridge i : eth0, 1).	nterfaces' field and enti	er the names of severa	I network
> Servio	:es									
✓ Netwo	ork		Common Configuration	1						
WAN			General Setup Advance	ed Settings						
LAN			Status		Uptime: 0h 0	n Os				
Cellula	ar Network			ath0	MAC-Addres	: D4:AD:20:BF:B3:D1				
Netwo	ork Failover			etho	TX: 0.00 B (0	ekts.)				
Wirele	ess									
WWA	N		Protocol	DHCP client	~					
DHCP			Hostname to send when	USR-G809						
Static	Routes		requesting DHCP							
> VPN			Choose the port type (GE/SEP)	GE port	~					
> Develo	oper		(02,011)							
> Firewa	all						-			
> Mode	Switch		Back to Overview				Apply Save			
Serial	Server									
> Systen	m									
Logou	ut	v								

## <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	
--------	----------------	--

USR-G809	interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLAINR (e.g.: etbl. 1).					
	Common Configuration	Common Configuration				
> Status	General Setup Advance	ced Settings				
Services     Network	Status	Uptime: 0h 0m 0s MAC-Address: D4:AD:20:BF:B3:D1				
WAN		eth0 RX: 0.00 B (0 Picts.) TX: 0.00 B (0 Picts.)				
LAN Callular Natwork	Dente and	Entrie address				
Network Failover	Protocol					
Wireless	Choose the port type (GE/SFP)	GE port				
WWAN	IPv4 address					
DHCP	IPv4 netmask	Please choose 🗸				
Static Routes	IPv4 gateway					
> Developer	IPv4 broadcast					
> Firewall	Use custom DNS servers	<u>a</u>				
> Mode Switch						
> Serial Server	Back to Overview	Apply Save				
System						



- Static address mode requires manual input ofIPv4 address, mask andIPv4gateway address;
- Sateway 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

809		
	WAN - WAN_WIKED	
Status	On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE. VLNIRK (e.g.: etb). 1).	network
ervices		
Network	Common Configuration	
WAN	General Setup Advanced Settings	
LAN	Status Uptime: 0h 0m 0s	
Cellular Network	MAC-Address: D4:AD:20:8F:83:D1	
Network Failover	TX: 0.00 B (0 Pkts.)	
Wireless		
WWAN	Protocol PPPoE V	
рнср	Choose the port type GE port	
tatic Routes	(GE/SFP)	
/PN	PAP/CHAP username	
Developer	PAP/CHAP password	
rewall		
Aode Switch		
a le	Back to Overview Apply Save	
mai server		
tem		
ogout		

## <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

USR-G809 Network Failover		
Configure the network switc	hing function.	
Services Configuration		
Network Priority	WAN1>WAN2>STA2.4>ST	
VAN Reference Mode	Custom 🗸	
Cellular Network Primary Server	223.6.6.6 🗸	
Network Failover Wirelass Secondary Server	IP or Domain, such as 223.6.6.0°C 119.29.29.29	f"baidu.com"
WWAN	IP or Domain, such as 223.6.6.6° c	n"baidu.com"
DHCP Thirdly Server	223.5.5.5 V	pr"baidu.com*
Static Routes Ping Interval VPN	10	
Developer Package size	0	
Firewall	O-1024Bytes	
Serial Server	2000 2000 100-20000milliseconds	
System		
Logout		

name	describe	default parameters
priority	Set NIC priority policy here	WAN1>WAN2>STA2.4
	WAN1: Corresponding to WAN/LAN port of shell silkscreen, corresponding to WAN_WIRED network card	>STA5>Cellular
	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	
reference mode	Custom: Determine network status	custom
	according to custom reference address	
	Gateway: Detect gateway address of	
	status	
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.



WiFi theoretical load 2.4G +5.8G: 256 units:

> Wi-Fi coverage is measured as 500m in open area bysome people, 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

SR-G809 24G AP1 24G AP2	5.8G AP1 5.8G AP2 MAC-Filter Client Information
atus Status	Mode:         Master           SSID:         USR-G809-B3D1           BSSID:         DAAD/2000 mol/of           Channel:         CLARATO:           Tx-Power:         27 dBm
IN Enable	2
Ilular Network Edilover SSID	USR-G809-B3D1
reless Encryption WAN Key	mixed-psk v
HCP HW Mode	11axg II STA is enabled, the configuration is affected by STA.
N HT Mode	auto           auto         •           If STA is enabled, the configuration is affected by STA.
rewall Channel Ode Switch	auto  If STA is enabled, the configuration is affected by STA.
rial Server Regions stem AP Isolation	00 - World
igout	

## 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	8888888
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

USR-G809	2.4G AP1 2.4G AP2	S&G AP1 S&G AP2 MAC-Filter Client Information
> Status	Status	Mode: Master SSID: USA-G809-B301_5G BSGID: DuAD-200FBR3D5
Services     Network		Channel: 100 (5.500 GHz) Tx-Power: 24 dBm
WAN	Enable	8
Cellular Network	Hide SSID	
Network Failover Wireless	SSID	USR-G809-B3D1_5G
WWAN	Key	······ ##
DHCP Static Routes	HW Mode	11axa            II is reabled, the configuration is affected by STA.
> VPN > Developer	HT Mode	auto
> Firewall	Regions	00 - World 🗸
Mode Switch     Serial Server	AP Isolation	o.
> System > Logout	•	Apply Save

## 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	8888888
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

	USR-G809
	<b>0</b>
	Status
	> Services
ì	✓ Network
	WAN
	LAN
	Cellular Network
	Network Failover
	Wireless
	WWAN
	DHCP
	Static Routes
	VPN
	Developer
	Circuper
	Maria C. indu
	Mode Switch
	> Serial Server
	System
	> Logout

## 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



					USR-G809	Manual
	USR-G809	Wireless Settings				
	Charles	Wireless Settings				
	Status	×				
	> Services	2.4G AP1 2.4G AP2	5.8G AP1 5.8G AP2 MA	C-Filter Client Information		
``	✓ Network					
	WAN	Statu	SSID: USR-G809-B3D1_5G-1   Mode: Master			
	LAN		Wireless is disabled or not			
	Cellular Network		33003100			
	Network Failover	Enabl	• □			
	Wireless		_			
	WWAN	Hide SSI				
	DHCP	SSI	USR-G809-B3D1_5G-1			
	Static Routes	Encryptio	No Encryption			
	VPN					
	Developer					
	Firewall			Apply Save		
	Mode Switch					
	Serial Server					
	System					
	Logout	<b>*</b>				

## 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

ISR-G809	·			
	Wireless Settings			
	Wireless Settings			
Status		_		
Services	2.4G AP1 2.4G AP2	5.8G AP1 5.8G AP2 MA	C-Filter Client Information	
Network				
WAN	MAC-Address Filter	disable 🗸		
LAN		disable		
Cellular Network		Allow listed only	Apply Save	
Network Failover		Allow all except listed	oppin Date	
Wireless				
WWAN				
DHCP				
Static Routes				
VPN				
Developer				
Firewall				
Mode Switch				
arial Sarvar				
char berver				
iystem				
ogout				



		051 0005 110100
name	describe	default
MAC address filtering	Disabled: All terminals can connect to router WiFi	forbidden
	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	
MAC-List	Fill in MAC-list, maximum support 64 MAC list	empty

#### 3.5.6. Client information

Displays a list of terminals.

	-							
-G809	<b>^</b>	-						
	4) · · · · · · · · · · · · · · · · · · ·	Wireless S	Settings					
Charles		Wireless Set*	tings					
status	51					-		
Services		2.4G AP1	24G AP2 58G AP1	5.8G AP2 MAC-Filter Client	Information			
Network		Latoria						
WAN								
LAN		SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Cellular Network		No information	n available					
Network Failover								
Wireless		SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
WWAN		No informatio	n available					
DHCP								
Static Routes		SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
VPN								
Developer		No information	n available					
Firewall		SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Mode Switch								
Serial Server		No information	n available					
System	1 · · · · · · · · · · · · · · · · · · ·							
Logout	×							

#### 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



03K-0609	WWAN Settings
Status	When enabling the STA, make sure that the AP corresponding to the device is enabled. After the STA is successfully connected, the channel, bandwidth and mode of the AP of the device will be synchronized to the same as the STA.
Services	
<ul> <li>Network</li> </ul>	2.4G Settings 5.8G Settings AP Information
WAN	
LAN	Enable 🗹
Cellular Network	Scan Scanning
Network Failover	SSID WIFI-STA
Wireless	Encryption No Encryption
WWAN	
DHCP	network wwan0 🗸
Static Routes	<ul> <li>The spectra gradient and the spectra of the spectra o</li></ul>
VPN	Enable Ping Check
Developer	
Firewall	
Mode Switch	Apply Save
Serial Server	
System	
Logout	

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	not have
	It takes about 30 seconds to 1 minute to search for hot spots, so wait patiently.	
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	wwan0
	Normal use STA function select	
	wwan0ifyou need to use WIFI	
	bridge mode please select lan	
Forcibly update LAN IP	Check this functionto restart LAN when LAN (bridge	check
address	mode) is	
Enable Ping detection	If checked, enable the detection function to be kept	not checked
	active. If the detection address is notavailable, try to	
	connectto wireless again.	
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



	WWAN Settings	
> Status	When enabling the STA, make sure the device will be synchronized to the	hat the AP corresponding to the device is enabled. After the STA is successfully connected, the channel, bandwidth and mode of the AP of e same as the STA.
> Services		
✓ Network	2.4G Settings 5.8G Settings	AP Information
WAN		1
LAN	Enable 🗹	
Cellular Network	Scan Scar	n 🕊
Network Failover	SSID WIFI-	STA
Wireless	Encryption No En	rcryption 🗸
WWAN	network wwan	
DHCP	(a) Whe	en selecting the LAN interface, please modify or close the DHCP configuration of the LAN port and configure the LAN port address as the address within
Static Routes	the upp	per routing subnet
> VPN	Enable Ping Check 🗌 🌔	Once selected, check the wireless connect with ping
Developer		
> Firewall		
> Mode Switch		Appry Save
> Serial Server		
> System		
> Logout		

## 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	not have
	It takes about 30 seconds to 1 minute to search for hot spots, so wait patiently.	

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.



ISR-G809		MOMANI C	ottings							
		Without St	ettings	D annual an de des de des la anchier	After the CTA is success	e di la constanta di Alexandre	nal baarda iddb aad mada af tha AD af			
> Status		the device v	When enabling the S1A, make sure that the AP corresponding to the device is enabled. Atter the STA is successfully connected, the channel, bandwidth and mode of the AP of the device will be synchronized to the same as the STA.							
> Services		L								
✓ Network		2.4G Setting	s 5.8G Settings AP Info	ormation						
WAN										
LAN		SSID	MAC-Address	Signal	Noise	RX Rate	TX Rate			
Cellular Network		No informatio	n available							
Network Failover										
Wireless										
WWAN				Apply	Save					
DHCP										
Static Routes										
> VPN										
> Developer										
> Firewall										
> Mode Switch										
Serial Server										
System	1									
Logout	r									

#### 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 1Static 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.

SR-G809	Static Routing				
	To find information o	on static routing configurati	on, refer to the figure and table below		
tatus					
Services	Static Routing	Routing Table			
letwork	Static IPv4 Route	s			
VAN	Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric
AN					
Cellular Network	This section contains n	o values vet			
letwork Failover	This section contains in	o values yet			
Vireless	New Rule:				
VWAN	Interface	Target	IPv4-Netmask	<u>IPv4</u> -Gateway	Metric
HCP		Host-IP or Network	If target is a network		
tatic Routes		noot in or notice	in target is a network		
PN	wan_wired 🗸	192.168.1.0	255.255.255.0	192.168.0.202	0
eveloper					
irewall			Apply	Save	
Mode Switch					
erial Server					
ystem					
oqout					



#### 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:

USR-G809			
	Dynamic DNS		
> Status	Dynamic DNS configuration	allows access to a fixed domain fo	r the host, but the corresp
✓ Services	Configuration		
DM Management	Enable	0	
DDNS	Event interface	wan wired	
Data Service	Liten mende	Network on which the ddns-up	later scripts will be started
SMS Service	Service	dyndns.org 🗸	
Event Alarm Service		Service provider	
OLED	Username	username	
SNMPD	Password	•••••	8
Network	Domain Name		
> VPN	Sync Time	300	
> Developer		(a) Unit: s, 30-65535	
> Firewall			
> Mode Switch			
> Serial Server			Apply
> System			
> Logout			

### 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.



C:\Us C:\Us	ers\Administ ers\Administ	crator> crator>ping	fe26203	015.zicp.v	vip	
正来来来来来来	Ping fe26203 60 60 60 60	3015.zicp.v 38 的回复: 38 的回复: 38 的回复: 38 的回复: 38 的回复:	ip [6 字节=32 字节=32 字节=32 字节=32 字节=32	); 日寸(8)<1ms 日寸(8)<1ms 日寸(8)<1ms 日寸(8)<1ms 日寸(8)<1ms	8] 具有 32 <sup>2</sup> TTL=127 TTL=127 TTL=127 TTL=127 TTL=127	字节的数据:
1 60 . 往返 <sup>2</sup>	)的 效据包: 已发道 亍程的估计时[ 灵短 = Oms, 】	Ping 统计 送 = 4, 已搭 目(以毫秒为 最长 = Oms,	信息: 웾文 = 4, 单位): 平均 = (	丢失 = 0 Oms	(0% 丢失),	

#### 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.

		GNSS Configuration		
> Status		Configuration		
✓ Services		GNSS Enable		
DM Manageme	ent	GNSS Type	GPS+BDS	~
DDNS		7		
Data Service		Operating Mode	TCPC	~
SMS Service		Server Address	www.test.com	
Event Alarm Se	rvice	Server Port	2317	
OLED		GNSS Heart Type	NMEA GGA	~
SNMPD				
GNSS		Upload Interval	30 (2) 1-6000 second(s)	
> Network		Pagistar Packat	NONE	~
> VPN		Registi y Packet	NONE	
Developer		Heart Packet	NONE	~
> Firewall		Offline Cache Enable		
> Mode Switch				
> Serial Server				
> System				
> Logout	<b>T</b>			

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



	BDS;	
work pattern	Optional: TCPC/TCPS/UDPC/UDPS	ТСРС
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	Not checked
	Unchecked: positioning data will not be cached during network disconnection	
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



✓ Services	GNSS Enable		
DM Management	GNSS Type	GPS	~
DDNS		TOPO	
Data Service	Operating Mode	TCPC	*
SMS Service	Server Address	47.104.	
Event Alarm Service	Server Port	1517	
OLED	GNSS Heart Type	NMEA GGA	~
SNMPD		1	
GNSS	Upload Interval	1-6000 second(s)	
> Network	Registry Packet	NONE	~
> VPN		HOUT	
> Developer	Heart Packet	NONE	~
> Firewall	Offline Cache Enable		
> Mode Switch			
> Serial Server			
> System			
> Logout	*		

# Fig. 43 GNSS settings

# Report NMEA GGA data through TCPC.

	TCP/UDP Net Assistant	×
Settings	Data log	NetAssist V5.0.1 🗇 🗘
(1) Protocol	[2025-07-29 15:40:33.344]# RECV ASCII FROM 144.12.129.3 :11696>	^
(2) Loopi Host Addr	\$GRGGA, 074031.000, 3640.246396, N, 11706.031266, E, 2, 10, 1.06, 484.3, M, -5.0, M, , *69	
172 31 103 27		
	[2025-07-29 15:40:36.352]# RECV ASCII FROM 144.12.129.3 :11696>	
1523	304000, U14U34, UUU, 304U, 240019, M, 11100, U32124, E, Z, 1U, 1, U0, 405, F, M, ~5, U, M, , *86	
Close	[2025-07-29 15:40:39.343]# RECV ASCII FROM 144.12.129.3 :11696>	
	\$GNGGA, 074037.000, 3640.244804, N, 11706.032729, E, 2, 10, 1.06, 487.4, M, -5.0, M, , *64	
Recy Options		
	[2025-07-29 15:40:42.344]# RECV ASCII FROM 144.12.129.3 :11696>	
🔽 Log Display Mode	\$GNGGA, 074041.000, 3640.243976, N, 11706.032680, E, 2, 09, 1.10, 491.2, M, -5.0, M, , *6A	
🔽 Auto Linefeed		
🔲 Hide Received Data	[2025-07-29 15:40:45.367]# RECV ASCII FROM 144.12.129.3 :11696>	
Save Recv to File	\$GNGGA, 074043.000, 3640.243636, N, 11706.032306, E, 2, 09, 1.10, 493.1, M, -5.0, M, , *69	
AutoScroll Clear		
	[2025-07-29 15:40:48.368]# RECV ASCII FROM 144.12.129.3 :11696>	
AutoReply Themes	\$GNGGA, 074046.000, 3640.242433, N, 11706.034592, E, 2, 09, 1.10, 498.2, M, -5.0, M, , *6F	
Export DonateUs		
	[2025-07-29 15:40:51.367]# RECV ASCII FROM 144.12.129.3 :11696>	
	\$GNGGA, 074049.000, 3640.242113, N, 11706.033099, E, 2, 09, 1.10, 501.1, M, -5.0, M, , *6C	
Send Options	[2025-07-29 15:40.54 352]# RECV ASCIT REOM 144 12 129 3 (11696)	
C ASCIL C HEX	\$GNGGA, 074053.000, 3640.241241, N, 11706.031651, E, 2, 09, 1.11, 505.7, M, -5.0, M, , *63	
Use Escape Chars		
AT CMD auto CRLF		~
T Auto Append Bytes		
Send from File	Data Send Clients: All Connections (1)	🚽 🐺 Clear 🗶 Clear
Cycle 1000 ms	12345	e 1
Shortout <u>History</u>		Send
🝠 Ready!	149/0 RX:7502	TX:0 Reset

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.

Communication Expert of Industrial IOT			Be Honest, Do Best! Auto∣English∣#☆
USR-G809	OLED Configuration Configure the page cutting	node and display time of the screen.	
✓ Services DM Management	Display mode		
DDNS Data Service	Switching mode Lock page	System Info	
SMS Service Event Alarm Service		System Info IO	
OLED SNMPD		Cellular Apply Save	
GNSS Network		Custom1 Custom2	
> VPN > Developer		Custom3 Custom4	
Firewall     Mode Switch		Custom5	
Serial Server     System			
> Logout			

### 4.3.1. Generalized usage

Fig. 45 OLED

table 24	configuration	parameters
table 24	configuration	parameters

name	describe	default parameters
switching mode	Configure screen cut mode	scroll display
	Scroll display: interval multi-screen content rotation displaylock display: lock a screen long 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
	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	

# <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:



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:

```
usr oledtest "1" "2" "Hi OLED"
    test_oled.sh
    1
   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 "$text" ] && text="Hello World"
  P[ -z "$page" -o -z "$line" -o -z "$text" ] && {
       echo "param error, page=$1, line=$2, text=$3"
       exit 1
   - }
   uci set custom_oled.custom<mark>S(page)</mark>.line<mark>S(line)</mark>="$(text)" -c /tmp
  B#while true
   #do
        echo "test"
   #
   #
        sleep 1
```

Step 3: compress the data.tar.gz and control files into xxx.tar.gz (rename the compressed package usr\_oledtest\_ipq.ipk) Step 4: Upload and install the application on the router developer.

USR IOT Communication Expert of Industr	lior Be Hor	nest, Do Best! <sub>Auto   English   中文</sub>
Commanication Expert of Industr USR-G809  Status Services Network VPN Developer Cpp Manager Web Console Firewall	App Manager         The application management interface is mainly used for uploading secondary development packages and displaying their status.         App Upload         Upload App:         Upload App:         Install app    Note: <ol> <li>Pesse make sure the uploaded file format is targe or ipk.</li> </ol>	Auto   English   ⊕≵
Mode Switch     Serial Server     System     Logout	<ol> <li>The uploaded secondary development package must comply with specific standards, Please refer to the manual for detailed instructions on how to create it.</li> <li>The uploaded file size cannot exceed 512MB.</li> <li>After the upload is successful, you will enter the package information confirmation page for confirmation. After confirmation, it will be automatically installed and the installation result will be displayed.</li> </ol>	

#### 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.



#done

#### 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.



A					
G809	Data Service				
	The DataService Provide access to syste	em information and statu	s.		
tus					
ervices	Configurations				
M Management	Enable 🗌				
DNS					
Data Service					
SMS Service	Communication configuration				
Event Alarm Service	Service Name		Protocol	Description	Enable
LED					
NMPD			This section contains no values	vet	
GNSS					
etwork	New Service				
/PN	Service Name	Protocol	Description	Enable	
Developer		7000		-	
irewall		ICPC V		UN V	Add and edit
tode Switch					
rial Server			Apply		
stem					
ogout 👻					

# Fig. 48Data monitoring servicestable 25configuration 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	ТСРС
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



	tcpc_1 - Communicati	on configuration			
	The DataService Provide acc	ess to system information and status.			
Status		[max			
Services	Enable	on 🗸			
DM Management	Name	tcpc_1			
DDNS	Description				
Data Service	Protocol	тсрс			
SMS Service					
Event Alarm Service	Server Address	test.cn			
OLED	Server Port	8000			
SNMPD	Enable AT				
GNSS	Aoto Report				
Network	Denet Televel	1			
VPN	Report Interval	1-1440 minute			
Developer	Registry Packet	NONE			
Firewall					
Aode Switch					
Serial Server	Data Rule				
System	Data Nam	e DataType	Format	Instruction	Batch Delete
Logout					

# Fig. 49 link information

table 26 configuration parameters

name	describe	default parameters
enabled	Enable: Open this link	open
	Disable: Disable this link	
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

USR-G809		Enable	ON 🗸			
		Name	tcpc_1			
> Status		Description				
<ul> <li>Services</li> <li>DM Management</li> </ul>	1	Protocol	TCPC 🗸			
DDNS		Server Address	47.104.23			
Data Service		Server Port	1518			
SMS Service		Enable AT				
Event Alarm Service						
OLED		Aoto Report				
SNMPD		Report Interval	1			
GNSS			I-1440 minute			
> Network		Registry Packet	NONE			
VDN						
Developer		Data Rule				
> Firewall		Data Name	DataType	Forma	Instruction	🗴 Batch Delete
> Mode Switch						
> Serial Server		112	base	✓ json	112	X Delete
> System		test123	network	✓ json	234	💌 Delete
> Logout	*					



	TCP/UDP Ne	et Assistant	
Settings	Data log	Net/	Assist V5.0.1 🗇
(1) Protocol			
(2) Local Host Addr 172.31.103.27	[2025-07-24 16:00:53.925]# RE {"loopback": {"proto": "static" ["127.0.0.1/8"]. "ipaddr6": [":	CV ASCII FROM 144.12.0.98 :11080) , "ifname": "lo", "ipaddr4": :1/128"], "uptime": 321}, "lan":	8
(3) Local Host Port 1518	{"proto": "static", "ifname": "b ["fd32:f31f:6389::1/60", "fe80 red": {"proto": "dhcp", "ifname"	r-lan", "ipaddr4": ["192.168.1.1/24 ::d6ad:20ff:febf:b3d3/64"], "uptim :"eth0", "ipaddr4": [], "ipaddr6": []	1"], "ipaddr6": ne":321}, "wan_wi  }, "wancell":
· Close	{"proto":"dhcp", "ifname":"eth ["24De:844:2:2fe3:d9b5:1e1:67 64", "fe80::c870:caff:fef9:b64	2", "ipaddr4": ["10.23.49.183/28"], od:5d6/64", "240e:844:2:2fe3:c870: e/64"], "uptime":296], "wan6cell":	"ipaddr6": caff:fef9:b64e/
Recy Options	{"proto":"dhcpv6","ifname":"e ["240e:844:2:2fe3:d9b5:1e1:67 64","fe80::c870:caff:fef9:b64	<pre>th2", "ipaddr4":["10.23.49.183/28" od:5d6/64", "240e:844:2:2fe3:c870: e/64"], "uptime":296}}</pre>	'], "ipaddr6": caff:fef9:b64e/
Auto Linefeed		Sec. 1286 17	
Hide Received Data	[2025-07-24 16:00:53.957]# RE {"imei":"865827074532813","re CT","csq":"72","ops_net_type"	CV ASCII FROM 144.12.0.98 :11080) gister":"Attached","operator":"CH ':"FDD-LTE	) 01-
AutoScroll <u>Llear</u>	(4G)", "cimi": "460111117537048 "cell ci": "8C6C686", "cell lac	", "apn_cfg": "ctnet, ctnet@mycdma.c ": "5277", "arfcn": "300", "pci": "270	n, vnet. mobi, 1", )", "band": "LTEBA
Send Options • ASCII  • HEX	ND1", "ip": "10.23.49.183", "ine 240e:844:2:2fe3:c870:caff:fef	t6":"240e:844:2:2fe3:d9b5:1e1:67o 9:b64e/64Global,"}	d:5d6/64Global,
Use Escape Chars	Ľ		

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.

US	R-G809
Charles	
	status
	Services
	DM Management
DDN	45
Data	a Service
SMS Se	rvice
Event Ala	Irm Service
OLED	
SNMP	D
GNSS	
Network	
VPN	
Developer	
Firewall	
Mode Switch	
Serial Server	
System	
Logout	×



#### 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

USR-G809	SMS Service configuration	n			
Status	Configurations				
✓ Services	Enable 🗸	2			
DM Management	auth nacswd	2			
DDNS	dddi passina				
Data Service					
SMS Service	SMS Service Receive List	Send List			
Event Alarm Service	Phone Number configuration	on .			
OLED	Phone Number	,	Name Descri	ption	Enable
SNMPD					
Network	This section contains no values yet				
VPN					
Developer	New Number				
Firewall	Phone Number	Name	Description	Enable	
Mode Switch	Phone Number	Name	Description	on 🗸	Add and edit
Serial Server					
System			Apply		
Logout					

# Fig. 59 Authorized mobile phone number settings table 27 configuration parameters

Name	Describe	default parameters
note	Enable: Enable SMS service	enabled
	Disable: Turn off SMS	
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
nabled ON: Authorize the mobile phone number to send query/set router information		ON
	OFF: do not accept the mobile phone number information	

# <Description>

> Up to 6 mobile phone numbers can be authorized.



#### 4.6.2. SMS Service

03K-0009	444 - SMS Action conf	iguration				
> Status	Phone Number	13245				
✓ Services	Enable	on 🗸				
DM Management	Name	444				
DDNS	Description					
Data Service	Description					
SMS Service	Enable AT					
Event Alarm Service						
OLED	Action Rule List					
SNMPD		Action	SMS Content	Reply	Enable	🗷 Batch Delete
GNSS						
> Network			This section contains r	no values vet		
> VPN						
> Developer	New Rule					
Firewall	Action		SMS Content	Reply	Enable	
> Mode Switch						
> Serial Server	reboot	✓ SMS	Content	ON V	ON	Add
System						
> Logout	Back to Overview			Apply Save		

# 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	ON
	OFF: do not accept the mobile phone number information	
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



ι	JSR-G809	SMS Servi	ce configuration			
> 5	Status	Configurat	tions			
✓ 9	Services DM Management DDNS		Enable 🗹 auth passwd 🚥			
	Data Service GMS Service Event Alarm Service	SMS Service	Receive List			
S	DLED	SMS Send	elver Number 132454	20 digits long, optionally starting with a "+" sign to indicate ar	n international number.	
)     (	INSS Network /PN		Content test123	his box You can input up to 70 characters		
> t > F	Developer		Send	na box, rou can input up to ro characters.		
1 <	Mode Switch Serial Server	SMS Sendi Index	Receiver Number	Time	Content	Status
> 5	System	1	1324540	2025-07-24 04:11:23	test123	F ure
> L	.ogout	2	1324540	2025-07-24 04:11:35	test123	Fa re

#### 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.

USR-G809	SNMPD configuration SNMPD is a master daemon/	agent for SNMP, from the net-sn	mp project.
> Status	Enable SNMP		
✓ Services DM Management	Enable SNMP		
DDNS			
Data Service	User Info (use for snmp	v3)	
Event Alarm Service	username	user	
OLED	auth type	auth 🗸	
GNSS	auth mode	SHA 🗸	
> Network	auth passwd	•••••	
> VPN	6-1-1-5		
> Firewall	System Info	liblan	
> Mode Switch	sysLocation	www.test.com	
> System	sysName	Smart_Router	
> Logout			



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.





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	forbidden
	Disable: Close the PPTP client	
Server address	Enter the IP address or domain name of the VPN server to	192.168.0.2
	connect to	
joggle	Automatic: Connect to the VPN using the default routing	voluntarily
	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	
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	192.168.55.0
	communication between the client and the server. Enter	
	the server subnet segment here	
For the subnet mask	Use a static route through the VPN to enable subnet	255.255.255.0
	communication between the client and the server. Enter	
	the subnet mask of the server subnet here	
NAT	Check: Data passing through the VPN will be sent after NAT	check
	No line: Data passing through a VPN does not go through	
	NAT	
MPPE encryption	After checking, it is: mppe required, stateless	check



	l	JSR-G809 Manual
	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	empty
	the client interface does not have these parameters,	
	configure them here. Do not operate by non-professionals	
Enable static tunnel IP	Customize PPTP client IP. Note that if the IP server is	Not enabled
addresses	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	
Static tunnel IP address	Customize PPTP client IP. Note that if the IP server is	empty
	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	
default gateway	After checking: All data traffic will be transmitted through	Not selected
	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	
enable ping	Check: Enable VPNping ping alive detection, and reconnect	Not selected
	to the VPN if ping fails	
	Unchecked: Do not enable ping to keep alive	
Ping address	PPT The address that the PPTP network card can ping is	empty
	usually filled with the PTP address	
Ping period	Ping maintenance interval period, unit: seconds	10
Ping number of times	After the Ping failure upper threshold is exceeded, ping will	3
	not be sent to the set IP address, and the VPN will	
	reconnect	
		1

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



JSR-G809	<u>^</u>					
	OpenVPN Client	is Info				
Status	Common Name	Virtual Address	Real Address	Bytes Received	Bytes Sent	Connected Since
Services						
Network	VPN					
VPN	VPN Status					
РРТР						
L2TP						
IPSec						
VXLAN						
OpenVPN						
Certificate						
MARE						
Wireguard						
VPN Status						
Developer						
Firewall						
Mode Switch						
Serial Server						
	*					

# 5.2. L2TP Client

		L2TP Parameters		
	03/ 0003	L2TP Client	● Enable ○ Disab	в
	Statue	Server Address	192.168.0.2	
	Services	Interface	auto	~
	Network		Auto refers used default re	ute inter
		User Name		
	PPTP	Password		4
1				
	IDCos	Tunnel Name		
	IPSEC	Tunnel Password	Character(0, 50)	8
	VALAN		(a) chalacter(0-50)	
	OpenVPN	Enable IPsec		
	Certificate	Remote Subnet	192.168.55.0	
lanager	nentRE		eg: 192.108.10.0	
	Wireguard	Remote Subnet Mask	255.255.255.0	
	VPN Status		Con conconconto	
	Developer	NAT		
	Firewall	MTU	1450	
	Mode Switch		1430 GUU~ 1430	
3	Serial Server	Extra option		
	System		Append pppd options,Nor	- profess

Fig. 67	L2TP Client Settings Interface
table 32	L2TP Configuration Parameters

name	description	Default parameter
L2TP client enabled	Enable: Start the L2TP client	forbidden
	Disable: Close the L2TP client	
Server address	Enter the IP address or domain name of the VPN server to	192.168.0.2
	connect to	
joggle	Automatic: Connect to the VPN using the default routing	voluntarily
	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	



		<u>JSR-G809 Manual</u>
	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	empty
	be correct	
The Tunnel Code	Fill in the correct tunnel password	empty
IPSec encryption	Check: Enable L2TP over IPSec function	Not selected
	Not checked: Single L2TP function	
	After IPSEC encryption is enabled	
	IKE encryption: 3des-md5-modp1024 3des-sha1-	
	modn1024	
	ESD encryption: des-md5_des-sha1_3des-md5_3des-sha1	
	The ID set on the converside	
To the subhet	Use a static route through the VPN to enable subnet	192.168.55.0
	communication between the client and the server. Enter	
	the server subnet segment here	
For the subnet mask	Use a static route through the VPN to enable subnet	255.255.255.0
	communication between the client and the server. Enter	
	the subnet mask of the server subnet here	
NAT	Check: Data passing through the VPN will be sent after NAT	check
	No line: Data passing through a VPN does not go through	
	NAT	
MTU	Set the PPTP MTU value to the default value	1450
Additional configuration	Special parameters are usually configured for the server. If	empty
	the client interface does not have these parameters,	
	configure them here. Do not operate by non-professionals	
Enable static tunnel IP	Customize the L2TP client IP address. Note that if the IP	Not enabled
addresses	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	
Static tunnel IP address	Customize the L2TP client IP. Note that if the IP server is	empty
	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	
default gateway	After checking: All data traffic will be transmitted through	Not selected
acraatt gateway	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 part is connected by DDDOF made, the	
	Note. If the wait port is connected by PPPOE mode, the	



		<u>JSR-G809 Manual</u>
	check here is invalid	
enable ping	Check: Enable VPNping ping alive detection, and reconnect	Not selected
	to the VPN if ping fails	
	Unchecked: Do not enable ping to keep alive function	
Ping address	The address that the L2TP network card can ping is usually	empty
	filled in as the PTP address	
Ping period	Ping maintenance interval period, unit: seconds	10
Ping number of times	After the Ping failure upper threshold is exceeded, ping will	3
	not be sent to the set IP address and the VPN will reconnect	

< explain >

The mppe mode is: mppe required, stateless.

# 5.3. IPSec

	Stra	IPSec Parameters		
	USR-G809	IPSec	Enable O Disable	
		Interface	auto 🗸	
	> Status		Auto refers used default route	nterfa
	> Services	Peer Address	192.168.0.2	
	Network		IP address or domain or %any,	g:10
``	V VPN	Negotiation Method	Main 🗸	
	PPTP		100.150.1.0/04	•
	L2TP	Local Subnet	() eg: 192.168.10.0/24	
	IPSec	Due Calent	102 168 55 0/24	•
	VYLAN	Peer Subnet	@ eg: 192.168.20.0/24	
	OpenV/PN	IKE Version	ikav2	
	Openvers	THE VERSION	10072	
	Certificate	IKE Encryption Algorithm	3DES 🗸	
anager	mendirRE	IKE Integrity Algorithm	MD5 V	
	Wireguard		Course (1004blbs)	
	VPN Status	Diffie-Hellman Group	Group2(1024bits)	
	Developer	IKE Life Time	28800	
	Firewall		400-86400 seconds	
	> Mode Switch	Authentication Type	Pre-shared Key 🗸	
	> Serial Server	Pre-shared Key	•••••	-
	System	▼	② Character(1-50)	

# Fig. 69 IPSec Settings Interface

# table 33 IPSec Configuration Parameters

name	description	Default parameter
IPSec enable	Enable: Enable IPSec	forbidden
	Disable: Disable IPSec	
joggle	Automatic: Use the default route to connect to the VPN	voluntarily
	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	



	l	<u>JSR-G809 Manual</u>
	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	192.168.0.2
	Fill in:%any for passive server mode	
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	192 168 1 0/24
	consistent with the subnet set at the other end	172.1001110721
	You can fill in up to 10 segments	
To the subpot	Fill in the dectination subnet comment, and set the	102 169 55 0/24
	destination to be consistent with the destination subnet	192.100.55.0/24
	Volu can fill in un to 10 comments	
	iles 2 (iles 1, and the configuration is consistent with thet of	11
IKE Edition	Rev2/Rev1, and the configuration is consistent with that of	IKEVZ
IKE encryption algorithm	Select the IKE encryption algorithm and configure it to be	3DES
	consistent with the other end	
IKE verification algorithm	Select the IKE verification algorithm and configure it to be	MD5
	consistent with the other end	
Diffie-Hellman group	Select the DH group and configure it to be consistent with	Group2(1024bits)
	the other end	
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	@client
	peer identifier set on the peer	
End identification	It can be FQDN or IP type, and should be consistent with	@server
	the local identifier set on the other end	
ESP encryption algorithm	Select the ESP encryption algorithm and configure it to be	AES-128
	consistent with the other end	
FSP verification algorithm	Select the FSP verification algorithm and configure it to be	SHA-1
	consistent with the other end	
PES	Select the PES configuration and match it to the end	DH2
	configuration	
ESD life cyclo	ESD life cycle Settings unit: coconds	3600
	Cot the DDD timeout time in seconds	60
		60
UPD detection cycle	טייט aetection cycle setting, unit: second	60
DPD activity	Optional: None/removal/maintenance/reboot	restart



#### 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.

	<b>A</b>										
1009		VXLAN									
		vxlan cor	figure.								
		Config	ration								
		enable	type	Remote IPv4 address	Tunnel IPv4 address/netmask	Group IPv4 address	Bridge interface	Destination port	VNI	Bind interface	
l	TI	OFF 🛩	Grou 🗸			224.1.1.1	lan 🗸	4789	1	wan_wire 🗸	*
		Add 🔝									
						Apply					
н.											
	P.										

#### 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.

USR-G809	OpenVPN Configu	ration					
Chattan .	Enhanced OpenVPN de	sign allows 3 OpenVPN Cli	ents and 1 OpenVPN Server				
Services	OpenVPN Configu	ation					
> Network	Name	Туре	Description	Enal	ble	Status	
V VPN							
РРТР	CLIENT_1	CLIENT		OFF	~	Disconnected	🗹 Edit
TP	CLIENT_2	CLIENT		OFF	~	Disconnected	🛃 Edit
Sec		0.075.07					
AN	CLIENT_3	CLIENT		OFF	~	Disconnected	Edit
nVPN	SERVER_1	SERVER		OFF	~	Disconnected	🛃 Edit
ertificate							
RE				Apply			
Vireguard				Obbil			
PN Status							
veloper							
wall							
e Switch							
al Server							
System							



name	description	Default parameter
start using	Open: Open the openvpn client	close
	Close: Disable the openvpn client	
description	You can customize the description of this OpenVPN path,	empty
	but you don't have to fill it in	
Use the OpenVPN	Open: You can import the OpenVPN configuration	open
configuration file	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	
OpenVPN	The configuration file is passed to OpenVPN	not have
configuration file		
protocol	tcp/udp/tcp ipv4/udp ipv4	udp
Remote host IP	Set the openvpn server address: domain name or IP	192.168.0.2
address		
port	Set the openVPN server port number	1194
Type of certification	None, SSL/TLS, user name and password, pre-shared key,	SSL/TLS
	SSL/TLS+ user name and password	
TUN/TAP	tun/tap	tun
topology	Net30/p2p/subnet	subnet
bridge pattern	Tap bridges LAN and implements layer 2 interaction point	not have
	to point	
user name	When the authentication type is selected with a user name	empty
	and password, you must enter the correct user name	
password	When the authentication type is selected with a user name	empty
	and password, you must enter the correct password	
Local tunnel IP	When the authentication type is no/pre-shared password,	empty
	fill in the TUN tunnel IP of this end	
Remote tunnel IP	When the authentication type is no/pre-shared password,	empty
	fill in the end-to-end tunnel IP of this end	
Enter the IP address of	When the authentication type is no/pre-shared password,	empty
the Tap network card	fill in the IP address of the TAP network card on this end	
Tap the subnet mask	If the authentication type is no/pre-shared password, fill in	empty
of the network card	the TAP network card mask of this end	
joggle	Automatic: Connect to the VPN using the default routing	voluntarily
	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,	
	you connect connect to the VPN	
	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	
Redirect gateway	Use openvpn as the default gateway	close
	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	
Nat	Whether the data on the VPN network card is NAT	open
Enable Keepalive	Enable the live detection mechanism	open
Connection detection	VPN live heartbeat detection interval	10
time interval		
(seconds)		
Connection detection	If the heartbeat exceeds the set time without response,	120
timeout interval	reconnect to the VPN	
(seconds)		
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-	Set the data pack length	Air / air / 1450
MTU/TCP MSS		
Maximum frame	The maximum frame length of data is the default without	empty
length	special configuration	
Allows remote	Whether to allow remote address change Settings	close
address changes		
Log grade	Openvpn log level, the larger the number, the more	Warning (3)
	detailed the log is. Generally, open a higher level to	
	troubleshoot problems when the connection is abnormal	
Additional	Non-professionals should not configure it. You need to	empty
configuration	input openvpn recognizable parameters	
Local route-	Set the static route target segment established by the	empty
destination	openvpn network card on this end	
Local route-Network	Set the subnet mask of the static route target established	empty
mask	by the openvpn network card on this end	
СА	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,	not have
	you do not need to upload the certificate here	
Pre-shared key	Upload the pre-shared key. You can upload the certificate	not have
	only when you select the authentication type as pre-shared	
	key	
	Tab 2 OpenVPN Server parameter table	

#### USR-G809 Manual description Default parameter name Open: Start the openVPN server start using close Close: Disable the openvpn client description You can customize the description of this OpenVPN path, empty but you don't have to fill it tcp/udp/tcp ipv4/udp ipv4 protocol udp 1194 port Set the openvpn server port number Type of certification None, SSL/TLS, user name and password, pre-shared key, SSL/TLS SSL/TLS+ user name and password TUN/TAP Select the network communication mode, tun/tap tun Bridge the network The Tap mode can bridge LAN and realize two-layer not have interaction point to point Bridge network mode TAP bridge network mode Settings Use the device's own DHCP configuration Use the device's own DHCP service: Use the router LAN port service 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 Net30/p2p/subnet, which is usually the default value subnet topology IPv4 tunnel network Open the IP subnet assigned to the client for OpenVPN, empty such as 192.168.100.0 IPv4 tunnel subnet Enter the subnet mask assigned to the client by OpenVPN, empty mask for example: 255.255.255.0 Local tunnel IP When the authentication type is no/pre-shared password, empty fill in the local TUN tunnel IP Remote tunnel IP When the authentication type is no/pre-shared password, empty fill in the end-to-end tunnel IP of this end The TAP bridge mode specifies the starting IP address, such begin IP empty as 192.168.100.100 The LAN port of the router needs to be set to the same subnet as the network segment finish IP The TAP bridge mode specifies the end IP address, such as empty 192.168.100.200 Enter the IP address of If the authentication type is no/pre-shared password, fill in empty the IP address of the TAP network card on this end the Tap network card Tap the subnet mask If the authentication type is no/pre-shared password, fill in empty of the network card the TAP network card mask of this end The client When the client reaches the set value, it will renegotiate 3600 and reconnect. This is a security mechanism of openvpn renegotiates the time interval 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



		16		
Maximum number of	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	check		
	Unchecked: Data is only exchanged between the client and			
	the server not between clients			
Multiple clients use	Check: Allow multiple clients to use the same client	Not selected		
the same certificate	certificate to connect to the Open//PN Server	Not selected		
Redirect gateway	Lise openyon as the default gateway	close		
Redirect 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			
Nat	Whether the data on the VPN network card is NAT	open		
Enable Keepalive	Enable the live detection mechanism	open		
Connection detection	VPN live heartbeat detection interval	10		
time interval				
(seconds)				
Connection detection	If the heartbeat exceeds the set time without response,	120		
timeout interval	reconnect the VPN			
(seconds)				
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-	Set the data pack length	Air / air / 1450		
MTU/TCP MSS				
Maximum frame	The maximum frame length of data is the default without	empty		
length	special configuration			
Allows remote	Whether to allow remote address change Settings	close		
address changes				
Log grade	Openvpn log level, the larger the number of log is more	Warning (3)		
	detailed, generally open a larger level to troubleshoot			
	problems when the connection is abnormal			
Additional	Non-professionals should not configure it. You need to	empty		
configuration	input openvpn recognizable parameters			
user	Set the user name and password account for the client conne	ection. Select the option with		
	the user name and password to take effect. Set multiple acco	ounts to set a user name and		
	password for each client			
user name	Set the client connection user name, and you can set	empty		
	multiple user names and passwords			
password	Set the client connection password, and you can set	empty		
	multiple user name passwords			
The client is assigned	Set the parameters for assigning fixed IP addresses to clients. You can set multiple fixed			



a static IP address	IP addresses for multiple clients, and each client's fixed IP ad	dress cannot be repeated
user	Use the certificate form: This is set to the CN corresponding	empty
	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	
Static IP address	Set the static IP address assigned to the client, such as	empty
	192.168.100.2	
subnet mask	Set the subnet mask assigned to the client, for example:	empty
	255.255.255.0	
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	empty
	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	
subnet	The subnet segment corresponding to the client, such as	empty
	192.168.1.0	
subnet mask	The subnet mask corresponding to the client subnet	empty
	segment, such as: 255.255.255.0	
Local routing	Set up a static route created by the openvpn network card	
target	Set the static route target segment established by the	empty
	openvpn network card on this end	
Network mask	Set the subnet mask of the static route target established	empty
	by the openvpn network card on this end	
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,	not have
	you do not need to upload the certificate here	
Pre-shared key	Upload the pre-shared key. You can upload the certificate	not have
	only when you select the authentication type as pre-shared	
	key	

 Tab 3
 OpenVPN Server parameter table

name	description	Default parameter	
Client certificate	Openvpn Settings with SSL/TLS or user name and password i	require the corresponding	
	certificate to be passed		
	e client 1 certificate list,		
Pkcs12(.p12)	This certificate type is a file archiving format. If the	empty	
	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		
Ca	If you choose to authenticate with a user name and	empty	



	password or SSL, the CA certificate must be sent	
Cert	Enter the client certificate and select the SSL authentication	empty
	type. This certificate must be sent	
Кеу	Enter the client key and select the SSL authentication type.	empty
	This certificate must be sent	
Tls-auth (key)	If the openvpn TLS mode is set to tls-auth, you need to	empty
	enter the TLS key here	
Tls-crypt (key)	If the openvpn TLS mode is set totls-crypt, the TLS key must	empty
	be passed here	
Pre-share the key	When the authentication type is selected to pre-share the	empty
	key, enter the pre-shared key certificate here	
Certificate password	If a certificate password is generated, it must be set	document
input type	according to the file or manually entered type	
Certificate password	The password of the PEM certificate can be entered or	empty
	uploaded (the password is in the file). If the certificate is	
	generated without a password, do not fill in this field	
Server certificate	Openyon server Settings with SSL/TLS or user name and pass	word require the
	corresponding certificate to be passed	
Pkcs12(.p12)	This certificate type is a file archiving format. If the	empty
	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	
(a	If you choose to authenticate with a user name and	empty
	nassword or SSL the CA certificate must be sent	empty
Cert	Pass the client certificate, if you select authentication type	empty
cen	with user name and nassword or SSL this certificate must	empty
	he nassed	
Kov	Dece the client secret key, if you select the authentication	ompty
Ксу	type with user name and password or set this cortificate	empty
	must be bassed	
	To transfer the DU cortificate, if you coloct an	
Л	authentication type with a user name and password or SSI	
	this cortificate must be passed	
	If the energy TLC mode is get to the puth you need to	ometri
rts-autri (key)	anter the TLS key here	empty
rts-crypt (key)	If the open vph TLS mode is set to its-crypt, you need to	emply
Pre-share the key	when the authentication type is selected to pre-share the	empty
	key, enter the pre-shared key certificate here	
Certificate revocation		
list		
Certificate password	If a certificate password is generated, it must be set	document
input type	according to the file or manually entered type	
Certificate password	The password of the PEM certificate can be entered or	empty
	I i i i i i i i i i i i i i i i i i i i	



 	USR-G809 Manual
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.

Communication Expert of Industrial IOT	Be H	lonest, Do Best! אוזס אבאדבאוסא English   איז
General Setup		
USR-G806p Status	Uptime: 0h 18m 20s MAC-Address: 0440028D7748 WF V 168 M UPDI 014-01	
> Status	br-fan TX: 26.1.4 M8 (4598.2 Pkts.) IP44: 192.168.1.1/24	
> Services		
V Network Protocol	Static address	
VAN IPv4 address	192.168.10.1	
Cellular Network IPv4 netmask	255.255.255.0	
Network Failover IPv4 gateway	192.168.10.1	
WLAN AP		
WLAN STA		
DHCP Use custom DNS servers	114.114.114.114 8.8.8.8	
Static Routes		
Diagnostics		
Tcpdump DHCP Server		
> VPN	4	
Firewall		
> Serial Server Ignore interface	I was a state of the state of t	
> System Start Address	100	
> Logout	O Lowest leased address as offset from the network address.	
Umit	150 Maximum number of leased addresses.	
Leasetime	12h Q Expiry time of lessed addresses, minimum is 2 minutes (2m).	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 4 LAN port configuration



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

Communication Expert of Industrial IOT		Be H	onest, Do Best! <sub>English   #文</sub>
USR-G806p	SERVER_1 - OpenVPN	N Configuration	Î
> Status	Configuration		
> Services	Enable	e ON 🗸	
Network     VPN	Description	<ul> <li>The maximum length is 50 Bytes.</li> </ul>	
PPTP L2TP	Enable OpenVPN Config from file	Not Support	
IPSec	Protocol	I UDP V	
OpenVPN	Port	t 1194	
Certificate Management	Authentication Type	username/Password V	
GRE	TUN/TAP		
> Firewall	Bridge Network		
> Serial Server	Tap bridging network configuration mode	use your own dhcp servici 🗸	
> Logout	Renegotiation Interval(s)	3600	
	max clients	16     Allow a maximum of n simultaneously connected clients.	
	Client to client	🖬 💿 Internally route client-to-client traffic.	
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 5 OpenVPN configuration 1

#### Set a set of user names and passwords.

Communication Expert of Industrial IOT			Be Hones
USR-G806p	Extra Option	pe written directly to the configuration file. Please fill in carefully	
<ul><li>&gt; Status</li><li>&gt; Services</li></ul>	User		
> Network	Username	Password	
PPTP L2TP	test	test	🗷 Delete
IPSec OpenVPN Cartificate Management	New User: Username	Password	
GRE VPN Status	User	Password	1 Add
> Firewall	Client Static Ip User Static	: Ip Netmask/	22P IP
System		This section contains no values vet	
	Tunnel static IP-		
	User	Static IP Ne	tmask/P2P IP
	JiNan Usr IOT Techn	ology Limited http://www.pusr.com/	

### 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.

R-G806p	Certificate Manageme	ent	
tus	The current page is used to	o centrally manage various certificate and key files related to OpenVPN	
vices	Client1 Certificate		
work 1	pkcs12(.p12)	建築文化   実現存任何文件 ● FKSF12 (P12) files define an archive file format for storing crystographic objects as a single file. It means that p12 file is able to contain ca & cent & key. Generally if yo file already, there is no need to updoad ca & cent & key one by one.	ı have a .p12
	ca	医躁文性 未选择任何文件	
ec	cert	[选择文件] 未选择任何文件	
enVPN	key	透釋文件 未选择任何文件	
icate Management	tls-auth(secret key)	[ 遗 <b>择文件</b> ] 未逃得任何文件	
	tls-crypt(secret key)	[选择文件] 未选择任何文件	
itatus	Pre-shared key(secret key)	[ 遗 <b>探文件</b> ] 未选择任何文件	
l Server	Certificate Password Type	● file ○ input	
em	Certificate Password	[透釋文件] 未选择任何文件	
ut			

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.

Communication Expert of Industrial IOT			Be Honest, D Autometers
	General Setup		
USR-G806p	Status Uptime 85 MAC-Ac brian TK-25.1 IPv4:19	: 0h 29m 13: ddresc: D4AD208D:77-48 Is MB (37349 Pks.) 2.8 (68717 Pks.) 2.168.1.1/24	
✓ Network			
WAN	Protocol Static address	_	
LAN	IPv4 address 192.168.10.2		
Cellular Network	IPv4 netmask 255.255.2		
Network Failover	IPv4 gateway 192.168.10.1		
WLAN AP	IDu4 broadcast		
WLAN STA			
DHCP	Use custom DNS servers 114.114.114.114	1	
Static Routes			
Diagnostics			
Tcpdump	DHCP Server		
> VPN			
> Firewall	General Setup		
> Serial Server	Ignore interface 🛛 🖉 💿 Disable <u>DHCP</u> for this interf	face.	
> System	Start Address 100		
> Logout	Lowest leased address as offset from the second	om the network address.	
	Limit 150 Maximum number of leased addre	sses.	
	Leasetime 12h  Description Descripti Description Description Description Description Descr	inimum is 2 minutes ( <mark>2m</mark> ).	

Pic 8 LAN port configuration

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

USR IOT Communication Expert of Industrie	a lot	Be Honest, Do Best! ma∯ak∣+oc
USR-G806p	CLIENT_1 - OpenVP	4 Configuration
Status     Services     Network     VPN	Enable	ON V The maximum length is 50 Bytes.
PPTP L2TP IPSec	Enable OpenVPN Config from file Protocol	O on ® off
OpenVPN Certificate Management	Remote Host IP Address Port	192.168.66.109 1194
VPN Status > Firewall	Authentication Type	Username/Password V TAP V
Serial Server     System     Logout	Bridge Network User name	test © Username used for authentication to the VPP server. It is needed when Authentication Type contains Username/Password.
	Password	test  Pessword used for authentication to the VPN serves: It is needed when Authentication Type contains Username/Password.
	Renegotiation Interval(s)	JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 9 OpenVPN configuration 1



USR IOT Communication Expert of Indust	лы ют			Be Honest,
USR-G806p	Certificate Manageme	ent		
> Status	The current page is used to	centrally manage various certificate and key fil	es related to OpenVPN	
> Services	Client1 Certificate			
> Network <b>VPN</b>	pkcs12(.p12)	选择文件 录选择文件 @ PKCS#12 (P12) files define an archive file form Generally if you have a .p12 file already, there is 1	nat for storing cryptographic objects as a single file. It means that .p12 file is able to no need to up <u>land to</u> X cert & key one by one.	contain ca & cert & key.
PPTP L2TP	ca	选择文件未选择文件		
IPSec	cert	选择文件未选择文件		
OpenVPN	key	选择文件未选择文件		
Certificate Management	tls-auth(secret key)	选择文件未选择文件		
GRE VPN Status	tis-crypt(secret key)	选择文件 未选择文件		
> Firewall	Pre-shared key(secret key)	选择文件未选择文件		
> Serial Server	Certificate Password Type	● file ○ input		
> System	Certificate Password	选择文件 未选择文件		
Logout				

#### Pic 10 OpenVPN configuration 2

Test that PC1 and PC2 can communicate with each other:





#### 5.5.2. An Example of Implementing Subnet Interworking in Openvpn TUN



Pic 11 Connect the topology



Communication Expert of Industrial IOT		
USR-G806p	LAN - LAN On this page you can configure the ne	etwork interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field.
Status     Services	interfaces separated by spaces. You ca	n also use <u>VLAN</u> notation INTERFACE. VLANNR ( <u>e.g.</u> : eth0. 1).
WAN	General Setup	
Cellular Network Network Failover	Status	Uptime:         Uh 44m 20s           MAC-Address:         D4:AD:20:BD:77:48           br-lan         RX: 24.95 MB (57060 Pkts.)           TX: 31.23 MB (55866 Pkts.)         IPv4: 192.168.1.1/24
WLAN AP WLAN STA DHCP	Protocol Static a	address 🗸
Static Routes Diagnostics	IPv4 address 192.16 IPv4 netmask 255.25	8.10.1 5.255.0 ×
Tcpdump VPN	IPv4 gateway IPv4 broadcast	
Firewall     Serial Server	Use custom DNS servers 114.11 8.8.8.8	4.114.114
> System > Logout		

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



Communication Expert of Industrial IOT			in a start s
USR-G806p	SERVER_1 - OpenVPN	Configuration	
Status	Configuration		
> Services	Enable	0N 🗸	
Network     VPN	Description	The maximum length is 50 Bytes.	
PPTP L2TP	Enable OpenVPN Config from file	Not Support	
IPSec	Protocol	UDP 🗸	
OpenVPN	Port	1194	
Certificate Management GRE	Authentication Type	SSL/TLS 🖌 🗸	
VPN Status	TUN/TAP	TUN	
Firewall	Topology	Subnet 🗸	
Serial Server	Client Subnet	100.100.100.0	
System	Client Netmask	255.255.255.0	
Logout	Renegotiation Interval(s)	3600	
	max clients	16	

Pic 13 Router 1 is configured 2

Enter the client subnet information and click "Save"

Communication Expert of Industrial IOT						Be H	onest, Do
USR-G806p	User		Static IP		Netmask/P2P IP	Add 😭	
Status     Services	Client subnet Name	Subnet		Netmask			
Network     VPN     PPTP	client1	192.168.1.0	2	55.255.255.0		N Delete	
L2TP IPSec OpenVPN Certificate Management	New Client Network:	Name	Subnet Network		Netmask Netmask	Add 📫	
GRE VPN Status > Firewall	Local Route - LAN	N IP address and subnet mask o Subnet	of the remote network.	Net	tmask		
> Serial Server > System > Logout			This section contains	no values yet			
	Local Route:	Subnet		Netmask	k	Add	
		JiNan Usr IOT Technolog	y Limited http://www.j	pusr.com/			

Pic 14 Router 1 is configured 3

Enter the OpenVPN server certificate and click "Apply".


USR IOT Communication Expert of Industrial	ют		
USR-G806p	Certificate Passivoru	<u>2014A11</u> **2014A11	
Status     Services	Server Certificate pkcs12(.p12)	透择文件         未选择文件           ③ PKCS#12 (P12) files define an archive file for	mat for storing cryptographic objects as a single file. It means that .p12 file is able to con
<ul> <li>УРМ</li> <li>РРТР</li> <li>L2TP</li> </ul>	ca cert	Generally if you have a _p12 line already, there is           透择文件           未选择文件           透择文件	no need to upload ca a contra key one by one.
IPSec OpenVPN Certificate Management	key DH tis-auth(secret key)	<ul> <li>选择文件 未选择文件</li> <li>选择文件 未选择文件</li> <li>选择文件 未选择文件</li> </ul>	
GRE VPN Status	tis-crypt(secret key) Pre-shared key(secret key)	选择文件         未选择文件           选择文件         未选择文件	
<ul> <li>&gt; Firewaii</li> <li>&gt; Serial Server</li> <li>&gt; System</li> </ul>	Certificate Revoke List Certificate Password Type	选择文件   未选择文件     ● file   ○ input	
> Logout	Certificate Password	□选择文件 未选择文件	
		JiNan Usr IOT Technology Limited	Apply Save

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).

Communication Expert of Indus	sial IOT	Be Hone
USR-G806p	CLIENT_1 - OpenVPN	PN Configuration
Status Services Network VPN	Configuration Enable Description	on The maximum length is 50 Bytes.
PPTP L2TP IPSec	Enable OpenVPN Config from file Protoco	fig O on ® off
OpenVPN Certificate Management GRE	Remote Host IP Address Port	ss 192.168.66.109 ht 1194
VPN Status Firewall Serial Server	TUN/TAP	AP TUN V gy Subnet V
> system > Logout	Renegotiation Interval(s) Interface	s) 3600 ce Auto a Auto refers used default route interface to connect
	redirect-gateway	ay D JINan Usr IOT Technology Limited http://www.pusr.com/

Pic 16 Router 2 is configured 1

Client adds information to the server subnet.



# USR-G809 Manual

			OSIC GOOP HUT
			Be Honest, Do
Communication Expert of Industrial IOT			
	Fragment		
USR-G806p	② Enable internal datagram	n fragmentation:128~1500.If you are not familiar with this option, ple	ease leave it empty.
	Remote Addr Float	te end to channe its IP address/port	
Chattan			
status	Log Level warning(3)	~	
Services	tog tovero i i		
> Network	Extra Option	4	
✓ VPN	(2) The content here will be	written directly to the configuration file. Please fill in carefully	
РРТР			
L2TP			
IPSec	Local Route - LAN IP address and subnet ma	sk of the remote network.	
OpenVPN	Subnet	Netmask	
Certificate Management	102.178.10.0	255 255 255 0	20 Delete
GRE	192,100,10,0	255.255.255.0	× Delete
VPN Status			
> Firewall	Local Route:		
Carial Conver	Subnet	Netmask	
Schol School	Network	Netmask	bba 🕼
System			
> Logout			
	Back to Overview	Apply Save	
	JiNan Usr IOT Techno	ogy Limited http://www.pusr.com/	

Pic 17 Router 2 is configured 2

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

USR-G8	309
> Status	
> Services	
Network	ł.
V VPN	
PPTP	
L2TP	
IPSec	
VXLAN	
OpenVPI	4
Certificat	e
gementaRE	
Wiregua	ď
VPN Stat	us
> Develope	er
> Firewall	
> Mode Sw	vitch
> Serial Ser	ver
> System	

PC1 and PC2 are interconnected

1an









#### 5.6. GRE

	USR-G809
	Status
	Services
	Services
	Network
~	VPN
	PPTP
	L2TP
	IPSec
	VXLAN
	OpenVPN
	Castificate
	certificate
ageme	enderRE
	Wireguard
	VPN Status
	Developer
	Firewall
	Mode Switch
	Serial Server
	Sustam

Fig. 106GRE Basic Configurationtable 38configuration parameters



name	describe	default parameters
GRE	Enable: Start GRE	forbidden
	Close: Close GRE	
port	Automatic: Connect VPN using default routing interface	voluntarily
	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.	
	disconnected, you can automatically switch toanother interface to try	
	to connect to VPN.	
connection	NIC is the default route	not checked
	Unchecked: If the specified NIC hasIPand is not the default route, it will not connect to VPN.	
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	not checked
	Unchecked: ping keepalive function is	
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.



	USR-G809
	Status
	Services
	Network
~	<ul> <li>VPN</li> </ul>
_	РРТР
	L2TP
	IPSec
	VXLAN
	OpenVPN
	Certificate
Managen	ner@IRE
	Wireguard
	VPN Status
	Developer
	Firewall
	Mode Switch
	Serial Server
	System

Fig. 107 Wireguard

table 39 configuration parameters

name	describe	default parameters
Wireguard Client	Enable: Start Wireguard	close
	Close: Close Wireguard	
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	voluntarily
	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.	
	disconnected, you can automatically switch toanother interface to try to connect to VPN.	
Default NIC connection	Check: Use the specified NIC to connect toVPN when the specified NIC is the default route	not checked
	Unchecked: If the specified NIC hasIPand is not the default route, it will not connect to VPN.	
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



pre-shared key	Can be blank, if necessary fill in this peer	empty
	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=	
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	not checked
	Unchecked: ping keepalive function is	
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



USR-G809	Wireguard	
	Wireguard Parameters	
> Status	Wireguard Client	Enable O Disable
> Services	PrivateKev	<i>a</i>
Network		
VPN	PublicKey	
PPTP	Click Generate Key	3 Generate Key
L2TP		
IPSec	Interface Setting	
VXLAN		
OpenVPN	Interface	wan_wired V
Certificate Management		Auto refers used default route interface to connect
CDF	Default NIC connection	$\Box$ @ A VPN connection is established only when the selected interface is the defaul
Winsmund	Address	10.10.10.1/24
VPN Status	ListenPort	51820
VPN Status		
Developer	MTU	1420
> Firewall		
Mode Switch	Peer Setting	
> Serial Server		
System	Peer Public Key	
Logout	Peer Preshared Key	
	Endpoint Host	192.168.66.132
	Endpoint Port	51820
	Endpoint Subnet	192.168.88.0/24
	AllowedIPs	10.10.10.0/24 Pls or subnets for example: 10.0.0.1,192.168.55.0/24
	PersistentKeepalive	25

Fig. 109 Router 1 Settings Page



Wireguard Cli	ent 🖲 Enable: 🔾 Disable
JSR-G809 Private	Key 🖉
Publich	(ey
atus	
rvices Cick Generate F	ey 🧧 Generate Key
stwork	
N Interface Setting	
TP	are wan wired
TP	Auto refers used default route interface to connect
Sec Default NIC connect	ion 🔹 🔯 A VPN connection is established only when the selected interface is the default route
(LAN	
Addr	20.10.10.2/24
rtificate Management ListenP	ort 51920
RE M	TU 1420
ireguard	
N Status Peer Setting	
veloper	
ewall Peer Public H	Key
ode Switch Peer Preshared H	(ey
rial Server Endpoint H	ost 192.168.66.102
stem	54000
gout	
Endpoint Sub	net 192.168.1.0/24
Allowed	IPs 10.10.10.0/24
	It's or subnets, for example: 10.0.0.1,192,156,55.0/24
PersistentKeepa	ive 25
4	TAT D
Enable P	ing 🛛 🔞 Reconnect When Fails to Ping



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.



SP-G809	
	App Manager
	The application management interface is mainly used for uploading secondary development packages and displaying their status.
tatus	
ervices	App App Upload
letwork	1-1
/PN	Opicad App: Example Acaretic A
Developer	Install ann
App Manager	
Web Console	
Firewall	Note:
Mode Switch	<ol> <li>Please make sure the uploaded file format is targe or ipk.</li> <li>The updated decompany development perkape wet complex with exciting character. Please refer to the manual fee detailed instructions on how to send to it</li> </ol>
erial Server	2. The updated secondary deterophine package index comply with specific standards, rises relet to the manual for detailed instructions on row to cleare it. 3. The updated file size cannot exceed \$12M8.
ystem	4. After the upload is successful, you will enter the package information confirmation page for confirmation. After confirmation, it will be automatically installed and the installation result will be displayed.
Logout	

#### 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".

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



#### 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>>=== ======



	USR-G809
	Statue
	> Services
	Network
	> VPN
	Developer
	> Firewall
	> Mode Switch
	> Serial Server
2	∽ System
	System
	User Management
	Fime Setting
	Reboot Timer
	Storage Management
	Tools
	Profiles Snapshot
	Syslog

#### 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)

Astyn Hansell angel Barter war_oledtest "2" "1" "awa" angel Barter war_oledtest "2" "1" "awa" model Barter war angel Barter war angel Barter wal f /tmp/python,demo bells python,war 1p=127,108,46,103 bells python,war 1p=132,108,46,103 bells python,war 1p=132,108,46,108 bells python,war 1p=	-		
bello python.Wan ip-192.168.66.182			
Hells python.Wan ip-102/108.00.102			
belle python.War 5p=192.168.66:362			

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.

USR-G809		
	USR-G809 login:	
Status		
Services		
Network		
VPN		
Developer		
App Manager		
Web Console		
Firewall		
Mode Switch		
Serial Server		
System		
Logout		
		<b>*</b>

Fig. 119 web console

## 7. Firewall

## 7.1. Basic setup

Default to two firewall rules.



Firewall - Zone Setting The firewall creates zones ov	15 er your network interfaces to control network traffi	: flow.				
The firewall creates zones ov	er your network interfaces to control network traffic	c flow.				
Conserved Contractor						
General Settings						
Enable SYN-flood						
protection						
Drop invalid packets						
Input	accept 🗸					
Output	accept 🗸					
Forward	accept 🗸					
Zones=>Forward						
Sour	ce Zone=>Destination zones	Input	Output	Forward	Masquerading	MSS clamping
lan: la	an: ഈ 衆 ★ ★ ★ → wan	accept 🗸	accept 🗸	accept 🗸		
wan: wan_wired:	wancell: 🛃 wan6cell: 🛃 ⇒ ACCEPT	accept 🗸	accept 🗸	accept 🗸		
	Drop invalid packets Input Output Forward Zones=>Forward Sour Inn: Veen: wan_whred:	Drop invalid packets         Input         accept         Output         accept         Forward         accept             Zones=>Forward             Zones=>Destination zones             Ian:       Image: Rest Rest Rest Rest Rest Rest Rest Rest	processor         Output       accept         Output       accept         Forward       accept         Zones=>Forward       >         Zones=>Destination zones       Input         Image: an: 22 **********************************	Drop invalid packets         Input         accept         Output         Forward         accept         Vane         accept         Input         Source Zone=> Destination zones         Input         Output         Ian:         Ian: </td <td>Drop invalid packets:         Input         Qutput:         accept         Output:         accept         Forward         Zones=&gt;Forward         Source Zone=&gt; Destination zones         Input:         Inn:         Source Zone=&gt; Destination zones         Input:         accept v         accept v</td> <td>Drop invalid packets:       Input         Input       accept         Output       accept         Forward       accept             Zones=&gt;Forward       Input             Zones=&gt;Forward       Input             Input       accept             Imput       accept             Young:       yearseling 2 words             Imput       accept             Imput       Output             Young:       yearseling 2 words             Imput       Accept</td>	Drop invalid packets:         Input         Qutput:         accept         Output:         accept         Forward         Zones=>Forward         Source Zone=> Destination zones         Input:         Inn:         Source Zone=> Destination zones         Input:         accept v         accept v	Drop invalid packets:       Input         Input       accept         Output       accept         Forward       accept             Zones=>Forward       Input             Zones=>Forward       Input             Input       accept             Imput       accept             Young:       yearseling 2 words             Imput       accept             Imput       Output             Young:       yearseling 2 words             Imput       Accept

#### 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 as a 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 introduction to several common applications.



name	describe	default parameters
start using	Display means enabled	start using
	Display means disabled	
name	This rule name, character type	-
limit-address	Limit IPv4 addresses	IPv4 addresses only
agreement	The protocol type of the	TCP+UDP
	restriction rule can be	
	selected as	
Match ICMD turne	Matching ICMD rules coloct any	4.524
матст ісме туре		Ally
source region	Data flow source area, optional: arbitrary	LAN
	area, WAN ,LANLAN: indicates subnet	
	access to external network rules	
	external network	
source MAC address	Source MAC required to match rule null: means match	empty
	all MAC	
	Note: To match the source MAC address, set the source	
	IP address to null	
source IP address	Source IP required to match rule null: means match all	empty
	IPs	
	Note: To match the source IP address, set the source	
	MAC address to null	
source port	Source port to match rule null: means match all ports	empty
Target area	Data flow destination area, optional: arbitrary area,	WAN
	WAN ,LANLAN: indicates subnet access to external	
	network rules	
	WAN: Indicates rules for accessing an intranet from an	
	external network	
Target address	Access destination IP address null: represents all	empty
	addresses	
Target port	Access target port number null: represents all	empty
movement	When receiving such data packets, you can choose: discard, accept,reject, no action	take in
	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	

## 7.2.1. IP address blacklist

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



G809						
	Firewall - Traffic Rules					
	Traffic rules define policies for pack	ets traveling between different zones, for example to reject traffic between ce	rtain hosts or to open WAN ports on the router.			
	Traffic Rules					
	Name	Protocol		Action	Enable Sort	
	Allow-	IPv4-icmp with type echo-request From any host in wan		Accept input	💋 🔹 🔹 📈 Edit	X Delete
		To any router IP on this device				
	Open ports on router:					
	Name Protoco	External port				
	100000					
	New input rule ICP+C					
	New forward rule:					
	Name Source	zone Destination zone				
	New forward rule lan	✓ wan ✓ Add and edit				
	Source NAT					
	Name	Protocol			Action	Enable Sort
		This sect	ion contains no values yet			
	New source NAT:					
	Name	Source zone Dest	ination zone To source IP To source port			

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:

	USR-G809	Name	-
		Restrict to address family	IPv4 only 🗸
>	Status	Protocol	TCP+UDP 🗸
>	Services	Match ICMP type	any
>	Network		
>	VPN	Source zone	O Any zone
>	Developer		● Ian: 提 贵 贵 贵
~	/ Firewall		O wan: wan_wired: 🔊 wancell: 🖉 wan6cell: 👰
	General Settings		
	Port Forwards	Source MAC address	any v
	Traffic Rules		Unly match incoming traffic from these MACs.
	Custom Rules	Source IP address	192.168.1.136 (USR-SWW V
	Access Pestrictions		Unly match incoming traffic from this iP of range.
		Source port	any
e e e	Mode Switch		Only match incoming traffic originating from the given source port or port range on the client host
>	Serial Server	Destination zone	O Device (input)
>	System		
>	Logout		O Any zone (forward)
			〇 lan: lan: 要 魚 魚 魚
			wan: wan_wired: 2 wancell: 2 wan6cell: 2

## 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.



		O wan: wan_wired: 🔬 wancell: 🍇
USK-G609	Source MAC address	any 🗸
		Only match incoming traffic from these MACs.
> Status		
Cardina	Source IP address	192.108.1.136 (USR-SWW V
Services		Only instant meaning up to runge.
> Network	Source port	any
> VPN		Only match incoming traffic originating from the given source port or port range on the client host
> Developer	Destination zone	O Device (input)
V. Eirowall		
<ul> <li>Firewall</li> </ul>		O Any zone (forward)
General Settings		
Port Forwards		
Traffic Rules		wan: wan_wired: 2 wancell: 2 wan6cell: 2
Custom Rules		
	Destination address	any V
Access Restrictions		Technice materice meeting during to and specifical meeting max
> Mode Switch	Destination port	any
> Serial Server		Redirect matched incoming traffic to the given port on the internal host
> System	Action	reject
Logout		
	Back to Overview	Apply Save

Fig. 123 Firewall Blacklist Figure 3

Status	Traffic rules defin	e policies for packets traveling between different zones, for example to	reject traffic between certain hosts o	r to open W	/AN ports on the router.
Services	Traffic Rules				
Network	Name	Protocol	Action	Enable	Sort
VPN					
Developer	Allow- Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input		🔹 🔹 🗾 Edit 🗷 Delete
General Settings		IPv4-TCPUDP			
Port Forwards		From IP 192.168.1.136 in Ian To any host in wan	Refuse forward		🔹 🔹 🗷 Edit 💌 Delete
Traffic Rules					
Custom Rules	Open ports on rou	ter:			
Access Restrictions	Name	Protocol External port			
Mode Switch	New input rule	TCP+UDP 🗸 🖄 Add			
Serial Server					
System	New forward rule:				
Logout	Name	Source zone Destination zone			
	New General sule				

## 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.



USR-G809		IPv4-TCP,UDP From IP 192.168.1.136 in Ian To any host in wan	Refuse forward	🗹 🔹 💌 🗷 E	dit 💌 Delete
> Status	Open ports on router:				
> Services	Name	Protocol External port			
> Network	New input rule	TCR_LIDR X			
> VPN					
> Developer					
✓ Firewall	New forward rule:				
General Settings	Name	Source zone Destination zone			
Port Forwards	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit			
Traffic Rules					
Custom Rules	Source NAT				
Access Restrictions	Name	Protocol		Action	Enable Sor
> Mode Switch					
> Serial Server		This section contains no value	is vet		
> System					
> System > Logout	New source NAT:				
> System > Logout	New source NAT: Name	Source zone Destination zone To source IF	To source port		

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 is a specific IP that allows a specific IP in the local area network to access the external network, you need to fill inthe IP address or MAC address here), as shown in the following figure

	Match ICMP type	any 🗸
02K-G809	Source zone	O Any zone
Statue		● Ian: Ian: <sup>1011</sup> ● ● ● ● ●
Status		
Services		o wan: wan_wired: 🖉 wancell: 🖉 wancell:
> Network	Source MAC address	any 🗸
2 VPN		Only match incoming traffic from these MACs.
Developer	Source IP address	192.168.1.136 (USR-SWW 🗸
✓ Firewall		Ø Only match incoming traffic from this IP or range.
General Settings	Source port	any
Port Forwards		(2) Only match incoming traffic originating from the given source port or port range on the client host
Traffic Rules	Destination zone	O Device (input)
Custom Rules		
Access Restrictions		Any zone (torward)
> Mode Switch		〇 Ian: Ian: 2
> Serial Server		wan: wan_wired: 2 wancell: 2 wancell: 2
> System	Destination editors	
> Logout	Desunation address	<ul> <li>Redirect matched incoming traffic to the specified internal host</li> </ul>
	Destination port	any
		@ Redirect matched incoming traffic to the given port on the internal host
	Action	accept
	Fig	126 Eirowall Whitelist Figure II

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.



			Walke wall_wheel. 2: Walkell. 2:
	USR-G809	Source MAC address	any
			Only match incoming traffic from these MACs.
	Status	Course ID address	102 160 1 126 (IICD_CIMM ++
	Services	Source in address	<ul> <li>Only match incoming traffic from this IP or range.</li> </ul>
	Network	Source port	any
	VPN		ony match incoming transconginating nom the given source port or port range on the client nost
	Developer	Destination zone	O Device (input)
~	<ul> <li>Firewall</li> </ul>		
	General Settings		O Any zone (torward)
	General settings		○ lan: lan: デ 条 条 条
	Port Forwards		
	Traffic Rules		wan: wan_wired: A wancell: A wancell:
	Custom Rules	Destination address	any
	Access Restrictions		Redirect matched incoming traffic to the specified internal host
	Mode Switch	Destination post	
		Destination port	Redirect matched incoming traffic to the given port on the internal host
	Serial Server		
	System	Action	accept
	Logout		
		Back to Overview	Apply Save

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

USR-G809	Firewall - Traffic R	ıles				
Status	Traffic rules define polic	ies for packets traveling between different zones, for example to	reject traffic between certain hosts o	r to open V	/AN ports on the router.	
Services	Traffic Rules					
Network	Name	Protocol	Action	Enable	Sort	
VPN Developer Firewall	Allow- Ping	IPv4-icmp with type echo-request From any host in wan To any router IP on this device	Accept input		• • Zedit	X Delete
General Settings Port Forwards		IPv4-TCP,UDP From IP <i>192,168,1.136</i> in <i>Ian</i> To <i>any host</i> in <i>wan</i>	Accept forward		🔹 🔹 🛃 Edit	X Delete
Traffic Rules	-	IPv4-TCP,UDP From <i>any host in lan</i> To <i>any host in wan</i>	Refuse forward		🔹 🔹 🛃 Edit	X Delete
Access Restrictions	Open ports on router:					
Mode Switch Serial Server System	Name New input rule	Protocol External port				
Logout	New forward rule:					
	Name	Source zone Destination zone				

## 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.

USR-G809	The firewall creates zones over your network interfaces to control network traffic flow.						
	General Settings						
Status     Services	Enable SYN-flood protection						
> Network	Drop invalid packets						
> VPN	Input	accept 🗸					
Developer     Firewall	Output	accept 🗸					
General Settings	Forward	accept 🗸					
Port Forwards							
Traffic Rules							
Custom Rules	Zones=>Forward						
Access Restrictions	Sourc	e Zone=>Destination zones	Input	Output	Forward	Masquerading	MSS clamping
> Mode Switch	lan: la	n: ₩	accent M	accent	accent V	_	
> Serial Server	Idit. Ia		accept 🗸	accept 🔹	accept 🗸		
> System	wan: wan_wired:	wancell: 🛃 wan6cell: 🛃 ⇒ ACCEPT	accept 🗸	accept 🗸	accept 🗸		
> Logout							
		Apply	Save				

Fig. 129 IP Address Disguise Settings

## 7.3.2. SNAT

outbound source IP translation capability.

table 41	SNAT	parameter	table
	2147 11	purumeter	ubic

name	describe	default parameters
enable button	Display indicates enabled status	start using
	Display indicates disabled state	
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	empty
	matching traffic to null for	
	this port to use the source	
	port	

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

USR-G809	The firewall creates zones over your network interfaces to control network traffic flow.						
	General Settings						
Status	Enable SYN-flood						
Services	protection						
Network	Drop invalid packets						
VPN	Input	accept 🗸					
Developer	Output	accent					
Firewall	Output	accept					
General Settings	Forward	accept 🗸					
Port Forwards							
Traffic Rules							
Custom Rules	Zones=>Forward						
Access Restrictions	Source	e Zone=>Destination zones	Input	Output	Forward	Masquerading	MSS clamping
Mode Switch							25 E W
Serial Server	lan: la	in: 🚰 轰 轰 轰 ⇒ wan	accept 🗸	accept 🗸	accept 🗸		
System	wan: wan_wired:	wancell: 🖉 wan6cell: 🛃 ⇒ 🛛 ACCEPT	accept 🗸	accept 🗸	accept 🗸		
Logout							
			Apply Save				

#### Set Source NAT

USR-G809	Name	Protocol External port
	New input rule	TCP+UDP 🗸
Status		
ervices	New forward rule:	
work	Name	Source zone Destination zone
	New forward rule	lan v wan V R Add and edit
per		
all	Course NAT	
ll Settings	Source NAI	Destand Asian Facility
ds	Name	Protocol Action Enable 5
es		This section contains no values yet
ictions		
1	New source NAT:	
	Name	Source zone Destination zone To source IP To source port
	test	lan 🗸 wan 🗸 192.168.9.1 V Do not rewrite 🖻 Add and edit
		Apply Save

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.

	Name	Protocol External port		
USR-G809	New input rule	TCP+UDP 🗸		
> Status				
> Services	New forward rule:			
> Network	Name	Source zone Destination zone		
> VPN	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit		
> Developer				
✓ Firewall	Source NAT			
General Settings	Name	Protocol	Action	Enable Sort
Port Forwards				
Traffic Rules	test	Any icmp From <i>any host</i> in <i>lan</i>	Rewrite to source IP	🗸 🔹 🔹 🏹 Edit 💌 Delete
Custom Bules		To any host in wan	192.168.9.1	
custom nuics				
Access Restrictions				
Access Restrictions	New source NAT:			
Access Restrictions Mode Switch Serial Server	New source NAT: Name	Source zone Destination zone To source II	• To source port	
Access Restrictions Mode Switch Serial Server System	New source NAT: Name test	Source zone Destination zone To source II	To source port	🝙 Add and edit
Access Restrictions Access Restrictions Mode Switch Serial Server System Logout	New source NAT: Name test	Source zone Destination zone To source II	To source port     Do not rewrite	Add and edit
Access Restrictions Mode Switch Serial Server System Logout	New source NAT: Name test	Source zone Destination zone To source II	• To source port	Add and edit
Access Restrictions Mode Switch Serial Server System Logout	New source NAT: Name test	Source zone Destination zone To source II	To source port     Do not rewrite	Add and edit

#### 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:



				US	R-G809 Manual
izie	ip.addr == 1	92.168.13.4		<ul> <li>第二日本</li> <li>日本</li> <li>日本</li></ul>	
No.	Time	Source	Destination	Protocol Info	
	1 0.000000	192, 168, 13, 4	220, 195, 22, 209	TCF 50379 > http [FIN, ACK] Seg=1 Ack=1 Win=64708 Len=0	
	2 0.689352	192.168.9.1	192, 168, 13, 4	ICMP Echo (ping) request (id=Ox183c, seq(be/le)=57/14592, tt1=64)	
- 8	3 0. 689426	192, 168, 13, 4	192.165.9.1	ICMP Echo (ping) reply (id=Ox1d3c, seq(be/le)=57/16592, tt1=128)	and the second
	6 1.689615	192.168.9.1	192.168.13.4	ICMP Scho (ping) request (id=Ox1d3c, seq(he/le)=58/14848, tt1=64)	
1	1 1.659687	192. 168. 13. 4	192.168.9.1	ICMP Echo (ping) reply (id=0x1d3c, seq0be/le)=58/14848, tt1=128)	
	6 1.823469	100-100-10-4	108-168-4-50	- SiB& - Ortuge Regenst Frite-I	
	9 1.825746	192, 168, 4, 63	192, 168, 13, 4	SMB2 Create Response File:	and the second se
	0 1.626091	192, 168, 13, 4	192.168.4:63	SNE2 Create Request File;	

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.

USR-G809				
	Firewall - Port Forv	vards		
> Status	Port forwarding allows n	emote computers on the Internet to connect to a specific comp	uter or service within the private LAN.	
> Services	Port Forwards			
> Network	Name	Match Rules	Forwarding To	Enable Se
> VPN				
> Developer		This section cont	ains no values yet	
✓ Firewall				
General Settings	New Port Forwarding Rul	les:		
Port Forwards	Name	Protocol External External port	Internal Internal IP Internal port	
Traffic Rules		zone	zone address	
Custom Rules	test	TCP+UDP V wan V 81	lan 🗸 192.168.2.1 🗸 80	🛅 Add
Access Restrictions				
> Mode Switch				
> Serial Server		Арріу	Save	
> System				
> Logout				

#### 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 to 192.168.2.1, and the internal network port to 80;

When we access port 81 from the WAN port, the access request will be redirected to192.168.2.180.



R-G809						
	Firewall - Port F	orwards				
ltatus	Port forwarding allo	ws remote computers on the Internet to	o connect to a specific computer o	service within the private LAN		
Services	Port Forwards					
Vetwork	Name	Match Rules		Forwarding To	Enable Sort	
/PN						
Developer	test	IPv4-tcp, udp From any bost in wan	IP 192	168.2.1 port 80 in Jan		Z Edit 💌 Delete
Firewall		Via any router IP at port 81				
General Settings					·	
Port Forwards	New Port Forwarding	Rules:				
Fraffic Rules	Name	Protocol	External External port zone	Internal Internal IP zone address	Internal port	
Custom Rules	New work for several	700.000		lan an		10 444
Access Restrictions		TCP+0DP	V wan V	ian 🗸	v	Add
Mode Switch						
Serial Server			Apply Sa	/e		
System						
ogout						

## 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.



# USR-G809 Manual

R-G809	nde toet
This pape allows you to d	nue van
IS I	a da analiza hohe na o na horronal anih a unih ana na
ces Rule is disabled	Enable
vork	her
Protoco	TCP+UDP V
Source zone	C lanz lan: 27 + + + +
eral Settings	vran: vran: vran: // vrancell: // vrancell: //
Forwards	
ic Rules Source MAC address	
om Rules	Only insumisation of the second seco second second sec
ss Restrictions Source IP address	any V Scheric from this IP or range.
e Switch	
I Server	(arry) © Only match incoming traffic originating from the given source port or port range on the client host
em External IP address	any 🗸
ut	Only match incoming traffic directed at the given IP address.
External port	8000
	Match incoming traffic directed at the given destination port or port range on this host
Internal zone	Ian: Ian: 27 * * * * *
	water was wired if washell if washell if
Internal IP address	192.168.2.1
	esurest matched incoming trains to the specified internal nost
Internal port	80 Redirect matched incoming traffic to the given port on the internal host
Factor Matterstein	
Enable NAI Loopback	

## Fig. 136 configuration interface

## table 43 configuration parameters

name	describe	default parameters
enabled	Enable: Disable	enabled
	Close: Enable	
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".

1158-6809				
031( 0009	Firewall - Port Forwar	ds		
Status	Port forwarding allows rem	ote computers on the Internet to conne	ect to a specific computer or service within the private	LAN.
ervices	Port Forwards			
etwork	Name	Match Rules	Forwarding To	Enable Sort
PN				
eveloper	test	IPv4-tcp, udp From <i>any host</i> in <i>wan</i>	IP 192.168.2.1, port 80 in Ian	🕑 🔹 🔹 🜌 Edit 💌 Delete
rewall	v	ia any router IP at port 8000		
eneral Settings				
ort Forwards	New Port Forwarding Rules:			
affic Rules	Name	Protocol Ex	ternal External port Internal Internal one zone address	IP Internal port
ustom Rules	222	TCDUUDD		0111
cess Restrictions	222			AUG
ode Switch				
rial Server			Apply Save	
stem				
gout				



Port Forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.     Port Forwarding   Name Match Rules   Porty port port port port port port port port	809	Firewall - Port	Forwards			
Port Forwards   er   222   IP-4-tcp, udp   222   Form any host in wan Via any router IP   Protocol External External port zone Internal Internal IP and internal IP internal port Internal Internal IP zone Internal Internal IP and internal I		Port forwarding all	ows remote computers on the Internet to conn	ect to a specific computer or service within the priv	vate LAN.	
Name Match Rules   Port Arbon data   122   123   123   124   124   125   126   126   126	s	Port Forwards				
Perf   22   Point reprint repri	k	Name	Match Rules	Forwarding To	Enable Sort	
Al Settings   brwards   kules   n kules   new port forward   rew port forward   TCP+UDP v wan v     Ian v v     Add	per	222	IPv4-tcp, udp From <i>any host</i> in <i>wan</i> Via <i>any router IP</i>	IP <i>192.168.2.133</i> in <i>lan</i>	<ul> <li>*</li> <li>*</li> <li></li> <li>&lt;</li></ul>	dit 💌 Delete
Name     Protocol     External External port zone     Internal Internal IP zone     Internal Internal IP zone     Internal IP address       New port forward     TCP+UDP     wan     Ian     Image: Comparison of the second of the seco	l Settings	New Port Forwardin	a Rules:			
Rules Rew part forward TCP+UDP Van	ules	Name	Protocol E	xternal External port Internal Inter one zone addi	mai IP Internal port	
vitch rver Apply Save	Rules	New port forward	TCP+UDP 🗸	wan 🗸 🛛 lan 🗸	~	📩 Add
Apply Save	Restrictions					
	rver			Apply Save		

#### 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 and addresses 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 selected and 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.



USR-G809	Access Restrictions
Status Services	Enter the domain name keyword.Note: When setting the whitelist, the PC may fail to visit the whitelist site for the first time due to browser reasons. If the access fails, please revisit.
letwork PN	Configurations
veloper ewall	Num Danie Nam
senerai settings Port Forwards Traffic Rules	test baidu.com 🗹 🕅 Delete
stom Rules cess Restrictions	New Firewall Rule:
ode Switch erial Server	Name Domain Name
System Logout	
	Apply Save

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 selected and 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.

USR-G809				
	Access Restrictions			
> Status	Enter the domain name keyword.Note: When revisit.	n setting the whitelist, the PC may fail to	o visit the whitelist site for the first time due	to browser reasons. If the access fails, p
> Services				
> Network	Configurations			
> VPN	Method White List	~		
> Developer				
✓ Firewall	l			
General Settings	Name	Domain Name	Enable	
Port Forwards				
Traffic Rules	test	baidu.com		🗴 Delete
Custom Rules				
Access Restrictions	New Firewall Rule:			
> Mode Switch	Name	e	Domain Name	
> Serial Server	New rule			Add
> System				
> Logout		_		
		Арр	bly Save	





#### 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.

Firewall - Custom Rules         Custom rules allow you to execute arbitrary lptables commands which are not otherwise covered by the firewall framework. The commands are executed after each fire restart, right after the default ruleset has been loaded. Note: Annotations are not allowed to be emptied!         * This file is interpreted as shell script.         * Dut your custom lptables rules here, they will         * be executed with each firewall (re-start.)         * Internal uci firewall chains are flushed and recreated on reload, so         * put custom rules lints the root chains e.g. INPUT or FORWARD or into the         * special user chains, e.g. input_wam_rule or postrouting_lam_rule.	2800	
Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each fire restart, right after the default ruleset has been loaded. Note: Annotations are not allowed to be emptied!         # This file is interpreted as shell script.         # Dut your custom (ptables rules here, they will         * executed with each firewall (re-instance)         # Internal uci firewall chains are flushed and recreated on reload, so         # pat custom rules into the root chains e.g. JNPUT or FORWARD or into the         # petial user chains, e.g. input_war_rule or postrouting_lam_rule.		Firewall - Custom Rules
This file is interpreted as shell script. P ut your custom liptables rules here, they will b executed with each firewall (result) is start. I nternal uci firewall chains are flushed and recreated on reload, so p pt custom rules into the root chains e.g. INPUT or FORWARD or into the # special user chains, e.g. Input_wan_rule or postrouting_lan_rule.		Custom rules allow you to execute arbritary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each fire restart, right after the default ruleset has been loaded. Note: Annotations are not allowed to be emptied!
		<ul> <li>* This file is interpreted as shell script.</li> <li>* Put your custom iptables rules here, they will</li> <li>* be executed with each firewall (re-)start.</li> <li>* Internal uci firewall chains are flushed and recreated on reload, so</li> <li># put custom rules into the root chains e.g. INPUT or FORWARD or into the</li> <li># special user chains, e.g. input_wan_rule or postrouting_lan_rule.</li> </ul>



## 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.



USR-G809	UART function switching
> Status	Uart function switching
> Services	Uart Function Edge
> Network	
> VPN	
> Developer	Apply
> Firewall	
✓ Mode Switch	
Mode Switch	
> Serial Server	
> System	
> Logout	



#### 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

L'J Euge Company														
	> Da	ta Point												
IO Module	Data	Point			Add				×					
Protocol	Slav	е										Add	Imxport	Export
Edge Gateway	Version:	: 168084	4896		* Slav	e Name:	test 1517							
		ocal IC	, ,	online	Slave De	scription:	Please enter							
	10	Slave		- Chanto	* Acquisition	protocol	Virtual Slave		~					
					* Polling	interval:	0		ms					
	pro	stocol: L	.ocal_IO		* Merge ac	quisition: 🧕	Open Oclose							
					* Slav	e switch:								
	List	ofsla	ve points					cancel	sure					
														Point Screen
		ID	Node name	Data Type	Decimal Number	Address	Read Write Status	Priority	Timeout(ms)	Data	Acquisition f ormula	Control formula	Node desc	Operation
		1	D001	Bit	0	DO 01	Read/Write	Level 1	2000	0				Edit Delete
		2	DI01	Bit	0	DI 01	Only Read	Level 1	2000	0				Edit Delete

# 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	Oms
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

Data Point	> Data Point After	Add		×××					
IO Module	Data Point	* Node name	Temp						
Protocol	Slave	Node desc	Please enter				Add	Imxport	Export
Edge Gateway 👋	Version: 1753346784	Register	4 ~ 1 40001(ushort)						
	Local_IO	* Data Type	16 Bit Unsigned 🗸			offline			
	IO Slave	* Position Number	1	168.1.136	:102				
	protocol: Local_IO	Decimal Number	0 ~	CP 图 Deleti					
		* Read Write Status	Only Read O Read/Write						
	List of slave points	* Priority	Level 1 V				1	Add	Delete
		Acquisition formula 0							
		Control formula 0	Please enter						Point Screen
	ID Node name Data Type	* Timeout	2000 ms	D	ata	Acquisition f ormula	Control formula	Node desc	Operatio
		Unit	Please enter						
			cancel sure		Total 0	15/page ~	.tas 1	Nest	Go to
V1.1.87									

# 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



		<u>USR-G809 Manual</u>
	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	2000ms
	Set, do not update historical data and execute the next acquisition command.Range: 10~3000ms	
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:

Temp	
Please enter	
4 ~ 1	40001(ushort)
16 Bit Unsigned V	
0	~
Only Read Only Write	
Level 1	~
=%s+100	
Please enter	
2000	ms
Please enter	
	Temp Please enter 4   1 16 Bit Unsigned  0  On On Read  0 Read/Wite Cevel 1  Please enter 2000 Please enter 2000 Please enter



## USR-G809 Manual

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,	The first %s representsdata for thepoint name node0101	Add new points separately under virtual slave
		The second %s representsdata for thepoint name node0102	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:

Node desc	Please enter		
Register	4 ~	1	40001(ushor
* Data Type	16 Bit Unsigned	~	
Decimal Number	0		$\sim$
Read Write Status	Only Read Only Write	Read/Write	
* Priority	Level 1		¥
uisition formula 🕚	=%s+100		
Control formula 🔘	=%s+100		
* Timeout	2000		ms
Unit			

# 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.


## <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:



🕃 Edge Computing	EDGE Management		
Data Point	to Mediate > Function		
IO Module	DI		
Status	DI01		
Protocol	DI01		
Edge Gateway	DI Mode:	Digital Input	
rafe oneway	Filter time:	50 ms	
	Counter Mode:	Rising edge	
	Count Frequency:	5ms	
	Maximum range:	10000	
	Exceeds Maxinum range:	loop	
		∉ Edit	
	-		
	AO Function		

# 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.



Edge Computing	EDGE Management					\$) a
Data Point	Maximum range:	10000				
IO Module	Exceeds Maxinum range:	Add Timer		×		
Function		* Task Description:				
Protocol	AO Function	* Timing mode:	Timing motion			
Edge Gateway	暂无数据	* Cycle time:	Please enter 5	5		
		* DO Select:	请选择DO 🗸			_
	DO	* DO Action:	O ON OFF O Switch			apply
	Restart hold Open C		cancel	sure		
	Timer					Add
	ID Task Description	Timing mod	de Time	Action options	Action	Operation
14 127			No data yet			

# Fig. 150 timing function table 50 configuration parameters

name	describe	default parameters	
timing mode	Timed action: executed at a fixed time every day	timed action	
tining mode	Periodic action: executed according to a fixed cycle		
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 DL. The status of each DI is displayed independently and does not affect each other.



Data Point		iO Module 🔿 Status
IO Module	^	Status
Function Status		DO Status
Protocol		D001
Edge Gateway	~	D001
		AO status
		DI Status
		DI01
V1.1.87		DI01



#### 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.



Data Point	> Protocol					
IO Module ^	Protocol					
Function Status	Modbus RTU	Modbus RTU 💽				
Protocol	Modbus TCP	Basic settings				
dge Gateway 🛛 👋	Json	Connection Config				
		" RS485:		* Protocol:	TCP Server	~
		* Local Port.	502	* Maximum of Client:	2	
		Slave Configuration				
		* Slave Address:	1	* 32 bit integer byte order:	AB CD	~
		* 32 bit float byte order.	AB CD 🗸	64 bit integer byte order:	ABCDEFGH	
	-	apply				
V1.1.87		Node mapping ta				Add Delete
V1.1.87		I Note mapping ta				Add Delete

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.

Edge Computing	e.	j EDGE Management					\$
Data Point		> Protocol					
IO Module	^	Protocol					
Function Status		Modbus RTU	Modbus TCP 🚺				
Protocol		Modbus TCP	Basic settings				
Edge Gateway	~	Json	Connection Config				
			* Protocol:	TCP Server	<ul> <li>Local Port:</li> </ul>	502	
			* Maximum of Client:	2			
			Slave Configuration				
			* Slave Address:	1	* 32 bit integer byte order:	AB CD 🗸	
			* 32 bit float byte order:	AB CD	64 bit integer byte order:	ABCDEFGH	
		Ŧ	арріу				

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.



[·] Edge Computing	💽 EDGE Manag	ement						
Data Point	Modbus RTU	*	Json	•				
IO Module	Modbus TCP		Data C	ontrol				
Status	Json			Select Channel	Public Topic		Subscribe Topic	Operation
Protocol						No data yet		
Edge Gateway 🛛 🗸		÷	Json:	Tomplate of downlink data: {     "rw_pret": {         "rw_pret": [             "fur", rdom,             "ld": "ddm,             "ld": "lddm,             "ld": "lddm,	", "name": "node0101" "name": "node0102" "name": "node0102" "value": "55" "value": "52"			
V1.1.87			apply					

## 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. The Json command 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	



		USR-G809 N	Ianual
name	The point name can be substituted into the point if it is consistent with the point name in the point table.		
/alue	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"}.
```



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
		0: Normal execution
err	error code	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.



Protocol		UART01(RS232)	UART01(RS232)			
Edge Gateway	^	UART02(RS485)	Basic setting	IS		
Links			* Baud Rate:	9600	~	
Reporting			* Data Bit:	8	~	
Linkage Control			* Stop Bit:	1	$\sim$	
			* Parity Bit:	NONE	~	

# Fig. 155serial port configurationtable 54configuration parameters

name	describe	default parameters
RS232		
	Can be set to:	
Baud rate	600/1200/2400/4800/9600/19200/38400/57600/115200/2304 00	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		
	Can be set to:	
Baud rate	600/1200/2400/4800/9600/19200/38400/57600/115200/2304 00	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	downward edge
	conversion function interface	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.



#### (Subscribe and publish up to 16 topics).

Data Point	Edge Gateway > Links			
IO Modulo	Links			
Protocol	Link-1	Link-1 🔼		
dge Gateway ^	Link-2	Basic settings		
Serial Port		* Communication Protocol:	TCP Client ~	
Reporting		* Remote Server Address:	192.168.0.201	
Linkage Control		* Local Port:	0	
		* Remote Port:	8234	
		* Connection registration data:	Disable ~	
		* SSL Protocol:	Disable ~	
	Ť	* Report Cache Data:		
V1.1.87		apply		

#### 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.

Data Point			* Communication Protocol:	MOTT	~
				1.081	
O Module	×		* Protocol Select:	MQTT-3.1.1	~
Protocol					
dge Gateway	^		* Remote Server Address:	192.168.0.201	
Serial Port			* Client ID:	Please enter	
Links			Denote Det		
Reporting			* Remote Port	1883	
Linkage Control			* Heartbeat time:	60	s
		-			
			<ul> <li>Reconnection Internal:</li> </ul>	5	s
			Clean Session.		
			* Connection verification:		
			* Enable Last Will:		
			* SSL Protocol:	Disable	~

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:

Data Point	Edge Gateway > Report	Basic information	Please enter	
O Module	Reporting	* Up channel		~
Protocol	New Import Export	Data Reporting rules		
idge Gateway		interval reporting		
Serial Port	-	periodic reporting		
Links		Data change Reporting		
Reporting		report regularly		
Linkage Control		Reporting data format	Primitive data type	~
		Reporting Template	{"Current":"node0101","Voltage":"node0102"}	
	-			

# Fig. 158Create a data escalation grouptable 55Key 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	Original type: Point data is reported to the server according to the original type.	
data cell		empty
<b>h</b>	Numeric to character: if the point data is of numeric type,""	
type	will be added in the report, and the numeric format will be	
	converted to character string format, and then reported to the	
	platform.	

Submission template	CustomJson, need to comply withthe Json format specification, template maximum <mark>8K</mark> 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	empty
	All points are pulled, so that each group can be independently performed according to the point list Data pull and accurate reporting	

## 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



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	МАС	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

#### table 56 parameter specification

#### 8.4.1.6. Linkage control

follows:

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	When the linkage event meets the trigger condition for many times in a short time, touch	1000ms
interval	The minimum interval between the execution of the trigger and the minimum trigger time.	
	Send no action, directly discard.	
trigger point	Linkage conditions determine the source of the required data and support multiple points	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	
Maximum range of threshold conditions, range 0~20000	0
Range minimum of threshold condition, range 0~20000	0
After the linkage event meets the trigger conditions, the actions to be executed	empty
	compileMaximum range of threshold conditions, range 0~20000Range minimum of threshold condition, range 0~20000After the linkage event meets the trigger conditions, the actions to be executedmade

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	Set upper and lower thresholds
	One action at a time.	

Outside the interval (excluding boundar	Detection value outside threshold range triggers action, outgoing interval	Set upper and lower thresholds
	One action at a time.	

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	SMS content is within 70 bytes
	Machine, realize fast alarm	

## 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.

C Edge Computing	EDGE Management	
System	System > Configuration Mana	gement
Configuration Ma	Configuration Manag	gement
	Edge Computing Config	
	Export:	Export Config
	Import	Import Config
	Note: The linkage co	export point table will synchronously export the data point table, protocol conversion data point table, ntrol event table, and data reporting group table, and will be updated synchronously after importing
V1.1.87		

## 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.

Serial Port S	ettings								
Serial port basic of 5-1460 bytes	: Settings, the packa	ige time can b	e set in	the range	of 0-100	00 ms (0 indic	ates au	tomatic packaging), package	length can be set in the ran
Basic Config	uration								
Name	Baud Rate	Data B	its	Stop	Bits	Pairty		Packaging Interval	Packaging Length
	-	11						_	
COM1-485	115200 ~	8	~	1	~	NONE	~	0	1000
COM2-232	115200 ~	8	~	1	~	NONE	~	0	1000
485 collision	prevention Con	figuration							
495 collision	OFF			~					
465 (01151011	prevention								

## 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:	115200
	1200/2400/4800/9600/19200/38400/57600/115200/230400	
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.







## 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 is 5 to 1500 bytes. Factory default 1000 bytes.

recei	ve the N bit	receive the N+1 bit	
	M-N=L, L	is packet length	>
the first	bit of packet	the last bit of packet	

#### 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)

1150-0809	Configuration		
038 0009	Enable	ON	~
> Status	Name	123	
> Services	Description	TCPC_1	
> Network	Server Address	test.cn	
> VPN	Server Port		
> Developer	Local Port	0	
Mode Switch	Heartheat Dacket	OFF	~
✓ Serial Server	ilear bear Packet	NONE	
Serial Port Settings	Registry Packet	NONE	~
Communication	Transmission Mode	Pass-Through	~
Advanced Settings	bind	COM1-485	~
> System	TLS	OFF	~
> Logout	Offline Data Cache	OFF	~

## 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	HEX: hexadecimal type	HEX
type	ASCII: Character type	
heartbeat packet	Heartbeat packet data content	empty



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

nost poting	polling	OFF
channel binding	COM1-485:Data transmission using	COM1-485
	RS485 channel onlyCOM2-232:Data	
	transmission using RS232 channel COM1+COM2:Data transmission using RS232 or	
TLS	Version number: TLS1.0 and TLS1.2	OFF
	The authentication mode can be selected from non- authentication certificate, authentication server certificate and bidirectional authentication certificate	
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	Do not verify certificates
	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.	
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 old data
	Discard new data: new data will not be cached when the cache space is full	
cache system	Length limit: maximum storage 7300 bytes	length limit
	Packet limit: maximum storage of 10 packets	

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



USR-G809	TCPS - Communicatio	n configuration				
	Communication configuration	n				
> Status	Configuration					
> Network	Enable	ON	~			
VPN	Name	TCPS_1				
Firewall	Description	TCPS_1				
Mode Switch	Local Port					
Serial Server	Maximum Sockets Supported	8				
Communication	Exceeding Maximum	кіск	~			
Advanced Settings	Transmission Mode	Pass-Through	~			
System	bind	COM1-485	~			
5	Offline Data Cache	OFF	~			
	Back to Overview			Apply Save		



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	COM1-485		
	RS485 channel onlyCOM2-232:Data			
	transmission using RS232 channel COM1+COM2: Transfer data using RS232 or			
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)



USR-G809
Chabus
Status
Services
Network
VPN
Developer
Firewall
Mode Switch
✓ Serial Server
Serial Port Settings
Communication
Advanced Settings
Advanced Settings
System
Logout



table 65 UDPC parameter setting table

name	functional description	default
start using	Is this link enabled, ON/OFF	ON
name	e Set the name of this link	
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	HEX: hexadecimal type	HEX
type	ASCII: Character type	
heartbeat packet data	Heartbeat packet data content	empty
heartbeat time	The time interval between heartbeat packets sent, in seconds	60
Registration	NONE: Close Heartbeat Package	NONE
packet	Custom: Customize registration package content	
	MAC: Include device WAN MAC as registration package content	
Register Package	Custom Registry	HEX
Туре	TypeHEX: Hex	
	TypeASCII:	
	Character Type	
Register package data	Register package data content	empty
Register package	Send a registration packet when connecting to the server	Send once on
sending method	Add registration packets to the front of every packet sent to the server	connection
transmission mode	Pass-Through: pass-through mode	Pass-Through



		<u>USR-G809 Manual</u>
channel binding	COM1-485:Data transmission using	COM1-485
	RS485 channel onlyCOM2-232:Data	
	transmission using RS232 channel	
	COM1+COM2:Data transmission using RS232 or	

## 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)

Status Services Network	ion	configuration			
Status Services Configuration	ion				
Services Configurat	ion				
Network					
I CHOIR	Enable C	DN	~		
VPN					
Developer	Name U	UDPS_1			
Firewall	Description U	UDPS_1			
Mode Switch	Local Port				
Serial Server	alasian Mada	Page-Through			
Serial Port Settings	hission Mode	Pass-Infougn	*		
Communication	bind C	COM1-485	~		
Advanced Settings					
System					
Back to Ov	review			Apply Save	

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

## 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.



# 9.2.5.1. MQTT Basic Configuration

Communication Expert of Industri	ial lot		Be Honest,	D o <sub>Auto</sub>
USR-G809	Configuration			
	Enable	on 🗸		
> Status	Name	MQTT_1		
> Services	Description	MQTT_1		
> VPN	MQTT Vsesion	V3.1.1 🗸		
> Developer	Server Address	cloudmqtt.usr.cn		
> Firewall	Server Port	1883		
> Mode Switch	Client ID	01603125040800001050		
Serial Port Settings	Heartbeat Interval	30		
Communication	Reconnect Waiting	5		
Advanced Settings	Interval(s)	i range: 1-3600		
> System	Authentication	OFF 🗸		
Logour	MQTT WIII	OFF 🗸		
	Clean Session	OFF 🗸		
	TLS	OFF 🗸		
	Offline Data Cache	OFF 🗸		

# 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
	0 at most once	
	1 at least once	
	2 exactly once.	
reservation	Turn on message	OFF
message	function ON: ON 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	OFF
	The authentication mode can be selected from non- authentication certificate, authentication server certificate and bidirectional authentication certificate	
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	Do not verify certificates
	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.	
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.

R-G809	Authenticatio	n OFF	F 🗸					
	MQTT W	III OFF	F 🗸					
Status	Clean Sessio	n OFF	F 🗸					
Services	т	S OFF	F V					
Network								
VPN	Offline Data Cach	e OFF	F Y					
Developer								
Firewall	Tonic							
Mode Switch	Тупе	Name	Topic	Qos	KeenMsa	COM	Description	
Serial Server	.,,-							
Serial Port Settings								
Communication				This section cor	itains no values yet			
Advanced Settings								
System	New Topic:					244027 (b		
Logout	Type Name		Topic	Qos	KeepMsg	COM	Description	
	Put 🗸 Name		Торіс	0 At most or $\checkmark$	on 🗸	COM1-485 🗸	Description	👌 Add
	Back to Overview				Apply Sav	/P		





		USR-G809 Manua
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
	0 at most once	
	1 at least once	
	2 exactly once.	
reservation message	Set whether to keep messages, ON/OFF	ON
aisle	COM1-485: Data communication	COM1-485
	using 485 channelsCOM2-232:Data	
	communication using 232 channels COM1+COM2:Data transmission using RS232 or	
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.

	Configuration	
038-0009	Enable	ON ~
> Status	Name	AWS_1
> Services	Description	AWS_1
> Network	Server Address	amazonaws.com.cn
> VPN	Server Port	8883
> Firewall	Client ID	01603125040800001050
> Mode Switch	Heartbeat Interval	30
✓ Serial Server		O-6000 Seconds
Serial Port Settings	Reconnect Detection Interval(s)	5 range: 1-3600
Communication	Clean Session	OFF 🗸
Advanced Settings	Server Root CA file	选择文件未选择文件
> Logout	device signed certificate	选择文件未选择文件
	file	
	Device private key	选择文件
	Offline Data Cache	OFF 🗸

## 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



		USR-G809 Manual
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.

USR-G809 Configuration	ì		
	Enable	ON	~
tatus	Name	ALT 1	
25	Name	ne_+	
De	escription	ALI_1	
Insta	ance Type	Public Instance	~
veloper Pr	oductKey	can't be empty	
irewall dev	viceName	can't be empty	
ode Switch dev	riceSecret	can't be empty	
ial Server			
Serial Port Settings	Client ID	can't be empty	
Communication	Region ID	Shang Hai	~
dvanced Settings Se	erver Port	1883	
ystem		200	
Logout	t Interval	200 20-1200 Seconds	
Reconnect I	Detection	5	
Ir	nterval(s)	I range: 1-3600	
	TLS	OFF	~
Offline Da	ata Cache	OFF	~





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	OFF
	The authentication mode can be selected from non- authentication certificate, authentication server certificate and bidirectional authentication certificate	

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	Do not verify certificates
	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.	
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 parameters realize the data request from serial devices to HTTP servers.



USR-G809 Manual 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.

USR-G809	Configuration		
	Enable	ON	✓
> Status	Name	HTTPD_1	
> Services	Description	HTTPD 1	
> Network			
> VPN	Request Method	GET	v
> Developer	Remove Header	OFF	~
> Firewall		(1 =h=[0]]	
> Mode Switch	HTTP ORL	/i.pnp[3F]	
✓ Serial Server	Server Address		
Serial Port Settings	Remote Port		
Communication	Timeout	10	
Advanced Settings		1-3600 Seconds	
> System	Httpd Header	Accept:text/html[0D][0A]	[A
> Logout	bind	COM1-485	×
	7.0	OFF	
	ILS	UFF	×
	Back to Overview		Apply Save

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

# 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.

1997 - 1997 - 1991
USR-G809
Status
Services
Network
VPN
Developer
Eirowall
ritewali
Mode Switch
<ul> <li>Serial Server</li> </ul>
Serial Port Settings
Communication
Advanced Settings
System
Logout
Logour





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



heartbeat time	The time interval between heartbeat packets sent, in seconds	60
Serial port binding	COM1-485: Data communication	COM1+COM2
	using 485 channels COM2-232: Data	
	communication using 232 channels COM1+COM2:Data transmission using RS232 or	
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	OFF
	If dual serial ports are configured,DTU restart will be triggered if	
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.



	03K-0009
-	Statuc
	Services
	Notwork
	VDNI
	Developer
	> Firewall
	Mode Switch
	> Serial Server
	∽ System
	System
	User Management
	Time Setting
	Safety Management
	Reboot Timer
	Storage Management

# 10.2. Time setting

52 Thu Sync with browser k
k 1:48
1:48
1:46
2 2
x)       org       x)
x rg x x x x
:р.с



# <Attention>

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

10.3. Username Password Settings



USR-G809	
	Router Password
> Status	Changes the administrator password for accessing the device
Services	Configuration
Network	Dereved 6
VPN	Password with a start of the st
Developer	Confirmation
Firewall	
Mode Switch	
Serial Server	Apply
System	
ystem	
ser Management	
ne Setting	
Management	
oot Timer	
torage Management	<b>*</b>

#### 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.

USR-G809	
	HTTP Port
	Here you can configure the HTTP port number, effective immediately
> Status	
> Services	Web server
> Network	Http Port 80
> VPN	a do not set the port in use: 2601 10000 53 60820
> Developer	
> Firewall	
> Mode Switch	SSH Access
> Serial Server	Dropbear offers SSH network shell access and an integrated SCP server
∽ System	
System	Dropbear Instance
User Management	Enable 🗌
Time Setting	SCH Port 2222
Safety Management	@ do not set the port in use: 2601 10000 53 60820
Reboot Timer	
Channes Management	



## 10.5. Memory management



		US	SR-G809 Manual
USR-G809	Storage Setting		
Chabus	Storage Device	e SD Card  G fino USB flash drive or SD card is inserted, select internal storage	
Services	Cache space	e 1024	
Network VPN	Clear All Cache	a 🛛 Clear cache	
Developer	Export All Cache	2 Export cache	
Firewall Mode Switch			
Serial Server	Storage Status		
System	Internal Storage	75000 kB / 7097616 kB (1%)	
System	USB Disk Storage	No mount	
User Management	SD Card Storage	No mount	
Time Setting			
Safety Management			
Reboot Timer		Apply Save	
Storage 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.

Firowall	Profiles Snapshot		
> Mode Switch	Click 'Generate Snapshot' to save the cu configuration profiles.	urrent configuration. The system supports storing mult	iple snapshots, enabling rapid switching between different
> Serial Server			
∽ System	Profiles		
System	Profiles Name	Create Time	
User Management			
Time Setting	123	2025-07-24-05:54:02	🐉 Use 🗷 Delete
Safety Management			
Reboot Timer	Create Profiles Snapshot:		
Storage Management	Name		
Tools			1 Generate Snapshot
Profiles Snapshot			
Syslog			
Backup/Upgrade		Apply Save	
Reboot			
Logout			



## <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

> Firewall	Backup / Flash Firmware
> Mode Switch	
> Serial Server	Backup / Restore
✓ System	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
System	Download backup:  Generate archive
User Management	Reset to defaults: <a> </a> Perform
Time Setting	Config set to defaults:
Safety Management	Delete defaults config:
Reboot Timer	
Storage Management	To restore configuration files, you can upload a previously generated backup archive here.
Tools	Restore backup: Please select file 🛛 Browse 🖓 Upload archive
Profiles Snapshot	
Syslog	
Backup/Upgrade	Flash new firmware image
Reboot	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
> Logout	Keep settings:
<b>•</b>	Image · Please select file III Browse III Flash image

#### 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.



> Developer	2
> Firewall	Backup / Flash Firmware
> Mode Switch	
> Serial Server	Backup / Restore
✓ System	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
System	Download backup:      I Generate archive
User Management	Reset to defaults: O Perform
Time Setting	Config set to defaults:
Safety Management	Delete defaulte config: 👩 Delete Defaulte
Reboot Timer	Delete deladits comig:
Storage Management	To restore configuration files, you can upload a previously generated backup archive here.
Tools	Restore backup: Please select file 🔯 Browse 🔯 Upload archive
Profiles Snapshot	
Syslog	
Backup/Upgrade	Flash new firmware image
Reboot	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
> Logout	Keep settings:
<b>•</b>	Image: Please select file Browse B. Elash image



#### 10. 9. Firmware upgrade

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

> Services	
> Network	Backup / Flash Firmware
> VPN	
> Developer	Backup / Restore
> Firewall	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
> Mode Switch	Download backup: 📴 Generate archive
> Serial Server	Reset to defaults: 🕘 Perform
✓ System	Config out to defaulte:
System	
User Management	Delete defaults config:   Delete Defaults
Time Setting	
Time Setting	To restore configuration files, you can upload a previously generated backup archive here.
Safety Management	Restore backup: Please select file II Browse III Upload archive
Reboot Timer	
Storage Management	
Tools	Flash new firmware image
Profiles Snapshot	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
Syslog	Keep settings:
Backup/Upgrade	Image: Please select file 🕼 Browse 🕼 Flash image
Reboot	
> Logout	
<b>v</b>	

# <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

1. Export configuration



	Services	A
;	Network	Backup / Flash Firmware
;	VPN	
	Developer	Backup / Restore
;	Firewall	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
;	Mode Switch	Download backup: 📑 Generate archive
;	Serial Server	Reset to defaults: 🛛 🕲 Perform
×	∕ System	Config set to defaults:
	System	Delete defaults config: Delete Defaults
	User Management	
	Time Setting	To restore configuration files, you can upload a previously generated backup archive here.
	Safety Management	Restore backup: Please select file  Browse  Upload archive
	Reboot Timer	
	Storage Management	
	Tools	Flash new firmware image
	Profiles Snapshot	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
	Syslog	Keep settings:
	Backup/Upgrade	Image: Please select file
	Reboot	
3	Logout	
		*

#### 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

> Services	*
> Network	System
> VPN	Reboots the operating system of your device
> Developer	
> Firewall	Rebot
> Mode Switch	
> Serial Server	Petrum report
✓ System	
System	
User Management	
Time Setting	
Safety Management	
Reboot Timer	
Storage Management	
Tools	
Profiles Snapshot	
Syslog	
Backup/Upgrade	
Reboot	
> Logout	0 ~

#### 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.

5809	1			
	Reboot Scheduler			
	Reboots the operating syste	m		
ces	Parameter Configuration	on		
rk	Enable	0		
per	Periodic Reboot	Weekly	~	
all	Week Days	Sunday	~	
Switch	Bandom Time	Enable	×	
erver		(a) Randomly generate the second s	ne restart time (hours and minut	es) to avoid the device online at the same time.If disabled, custom time is required.
	Random Range(Start)	4:00	~	
	Random Range(End)	5:00	~	
lanagement	Report Time	None		
etting				
Management				
ot Timer			_	
e Management			Ap	ply Save
Snapshot				
-				



## <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

USR-G809
> Status
> Services
> Network
> VPN
> Developer
> Firewall
> Mode Switch
Serial Server
∽ System
System
User Management
Time Setting
Safety Management
Reboot Timer
Storage Management
Profiles Snapshot
Contract Strapshot

#### 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.



R-G809		
	System Log	
atus	Here you can view system lo	ogs, including application, kernel, and VPN logs.Remote logs based on UDP protocol can also be configured
atus	Confirmation	
rvices	Configuration	
etwork	Local log Remote log	
PN	Remete Service IR	0000
eveloper	Remote Service IP	<ul> <li>Using udp protocol, keep empty or '0.0.0.0' to disable</li> </ul>
rewall	Romoto Convico Port	222
ode Switch	Remote Service Port	<ul> <li>Keep empty to disable</li> </ul>
erial Server		
stem		
stem		Apply
ser Management		
me Setting		
fety Management		
poot Timer		
rage Management		
s		
files Spanshot		
ones oneponor		

#### 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.

	Log Kernel V View Empty
USK-0609	Jul 24 22:56:55 (none) daemon.err odhcod[4584]: Failed to add proxy neighbour entry 240e:844:43:6e13:cb4:ac2:b782:2d03 on wan6cell
	Jul 24 22:57:12 (none) kern.info kernel: [58668.115837] usb 1-1.2: new high-speed USB device number 13 using xhcl-hcd
	Jul 24 22:57:12 (none) kern.info kernel: [58668.262451] option 1-1.2:1.0: GSM modem (1-port) converter detected
Status	Jul 24 22:57:12 (none) kern.info kernel: [58668.263030] usb 1-1.2: GSM modem (1-port) converter now attached to ttyUSB0
	Jul 24 22:57:12 (none) kern.info kernel: [58668.269412] option 1-1.2:1.1: GSM modem (1-port) converter detected
Convicos	Jul 24 22:57:12 (none) kern.info kernel: [58668.276150] usb 1-1.2: GSM modem (1-port) converter now attached to ttyUSB1
Services	Jul 24 22:57:12 (none) kern.info kernel: [58668.283134] option 1-1.2:1.2: GSM modem (1-port) converter detected
ALC: I	Jul 24 22:57:12 (none) kern.info kernel: [58668.288981] usb 1-1.2: GSM modem (1-port) converter now attached to ttyUSB2
Network	Jul 24 22:57:12 (none) kern.info kernel: [58668.300924] option 1-1.2:1.3: GSM modem (1-port) converter detected
	Jul 24 22:57:12 (none) kern.info kernel: [\$8668.301763] usb 1-1.2: GSM modem (1-port) converter now attached to ttyUSB3
VPN	Jul 24 22:57:12 (none) kern.info kernel: [58668.326370] qmi_wwan_q 1-1.2:1.4: cdc-wdm0: USB WDM device
	Jul 24 22:57:12 (none) kern.info kernel: [58668.327633] qmi_wwan_q 1-1-2:1.4: Quectel EC20-CE-HDLG work on RawIP mode
Developer	Jul 24 22:57:12 (none) kem.info kemel: [58668.331075] qmi_wwan_q 1-1.2:1.4: rx_urb_size = 1520
	Jul 24 22:57/12 (none) kern.info kernel: [58668.342922] qml_wwan_q 1-1.2:1.4 etn2: register 'qml_wwan_q' at usb-xnci-ncd.0.auto-1.2, wwan/QMI device,
Firewall	06:4b:b1:15:e0:d1
	Jul 24 22:37/25 (none) daemon.into dismasq[19258]: reading (tmp/resolv.com.auto
Mode Switch	Jul 24 22:37/25 (none) daemon.into dismasq[19258]; using local addresses only for domain lan
Wode switch	Jul 24 22:37/25 (none) daemon into distinast[19258]; using nameserver 114:114:114:114:13
0.110	Jul 24 22:37/25 (none) daemon antie patient attended Istanting and the patient of the state of t
Serial Server	Jul 24 22:37:25 (none) deemon notice nettice watcher is enabled
	Jul 24 22:57:25 (none) daemon notice helio, intervent davice labela
System	Jul 24 22:57:25 (none) daemon notice netica netica netica netica factoria de la conscriuto
	Jul 24 22:57:25 (none) deemon notice netific Interface warcall' is satting up now
System	Jul 24 22:57:25 (none) deemon notice netifici. Interface wanefcell' has link connectivity
	Jul 24 22:57:25 (none) daemon notice netifici. Interface WanGcoll' is setting un now
User Management	Jul 24 22:57:25 (none) daemon notice netifit. Interface wanticell is now un
	Jul 24 22:57:25 (none) daemon.notice netifd: Interface 'wancell' is now down
Time Setting	Jul 24 22:57:25 (none) daemon.notice netifd: Interface 'wancell' is setting up now
rine setting	Jul 24 22:57:25 (none) daemon.notice netifd: Interface 'wan6cell' is now down
Cafety Managament	states essed for an antistic state and an and a state
Safety Management	
D I I I I	Log File: II Download log
Reboot Timer	
Storage Management	
IOOIS	and the second se
0.01.0.1.	stellink
LICOTHON & DODODOT	
Promes shapshot	



# 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



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



		USR-G80	9 Manual
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></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></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></type></pw></user></apn_name>
set	AT+APN1= <apn_name>,<user>,<pw>,<type></type></pw></user></apn_name>
	ОК
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></type></pw></user></apn_name>
set	AT+APN2= <apn_name>,<user>,<pw>,<type> OK</type></pw></user></apn_name>



r		_
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></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></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></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></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></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></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></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></ops_net_type></ops_operate>
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></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></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></pw></user>
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></plang>
set	AT+PLANG= <plang></plang>
	ОК
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></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&gt; <tx_bytes></tx_bytes></rx_ </tr_packets></rx_packets></mask></ip></mac>
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_b ytes&gt; <tx_bytes></tx_bytes></rx_b </tr_packets></rx_packets></mask></ip></mac>
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_b ytes&gt; <tx_bytes></tx_bytes></rx_b </tr_packets></rx_packets></mask></ip></mac>
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></gateway></mask></ip></type>
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></mask></ip>
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></mask></ip>
set	AT+LAN= <ip>,<mask></mask></ip>
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></ip>
	PING IP(IP): 56 data bytes
parameter	ip:IP or domain name, cannot be null, invalidpingparameter,e.gc1 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></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></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],[tim e2]</reboot_en>
set	AT+AUTOREBOOT= <reboot_en>,<type>,<day>,<random>,[time 1],[time] returns an OK</random></day></type></reboot_en>



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>



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</mac>
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</mac>
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</mac>
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



#### 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></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







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