

Communication Expert of Industrial

4G Industrial Router Pioneer

USR-G806p

Manual



Be Honest & Do Best

Your Trustworthy Smart Industrial IoT Partner



Content

1. Product introduction	5
1.1. Product features	5
1.2. Hardware interface diagram	7
1.3. Size description	8
2. Operation Instruction	9
2.1. Test	9
3. Network interface function	
3.1. Cellular networks	11
3.1.1. Cellular network configuration	11
3.1.2. SIM	
3.1.3. SIM card information	14
3.2. LAN	
3.2.1. DHCP	16
3.2.2. VLAN	
3.2.3. WAN/LAN Select	17
3.2.4. DHCP	
3.3. WAN	
3.3.1. DHCP	19
3.3.2. Static IP mode	20
3.3.3. PPPoE	20
3.4. Network switching	21
3.5. Wireless configuration	22
3.6. Wireless client	23
3.7. Static routing	25
3.8. Network diagnostic function	27
3.9. TCPDUMP traffic monitoring	27
4. VPN function	28
4.1. PPTP Client	28
4.2. L2TP Client	
4.3. IPSec	
4.4. OpenVPN	
4.4.1. OpenVPN TAP bridge example	43
4.4.2. An example of subnet interworking in OpenVPN TUN mode	47
4.5. GRE	52
5. Firewall	53
5.1. Basic Settings	53
5.2. Communication rules	54
5.2.1. IP address blacklist	55
5.2.2. IP address whitelist	57



USR-G806p Manual

5.3. NAT function	59
5.3.1. IP address spoofing	
5.3.2. SNAT	
5.3.3. DNAT	63
5.3.4. Port forwarding	64
5.3.5. NAT DMZ	65
5.4. Access restrictions	66
5.4.1. Domain blacklists	67
5.4.2. Domain name whitelist	67
6. Service function	
6.1. Dynamic domain name resolution (DDNS)	68
6.1.1. Supported services	
6.1.2. DDNS come into force	
6.1.3. functional characteristics	
6.2. SSH Port	70
6.3. SMS	71
6.4. SNMPD	72
6.5. GNSS	73
7. Serial port server function	
7.1. Serial port Settings	74
7.1.1. Time-triggered mode	75
7.1.2. Length-triggered mode	
7.2. Communication configuration	
7.2.1. MQTT pattern	76
7.2.2. Connect to the Amazon platform	79
7.2.3. Connect to Ali Cloud platform	
7.2.4. HTTPD mode (HTTP Client mode)	82
7.2.5. Registration packet/handshake packet function	84
7.3. advanced setup	
8. system function	86
8.1. host name	86
8.2. Time Settings	
8.3. Username and password Settings	
8.4. HTTP port	
8.5. Parameter backup and upload	
8.6. factory data reset	
8.7. firmware upgrade	
8.8. restart	
8.9. Restart at regular intervals	
8.10. Daily record	
9. AT order set	
9.1. AT code repertory	



USR-G806p Manual

9.1.1. AT order set	
10. Disclaimer	
11. Update log	130



1. Product introduction

The USR-G806p is a flagship industrial router with 5 network ports, built on the industry-leading Qualcomm CPU solution. It features multiple hardware interfaces, including 5 network ports (1WAN + 1 LAN + 3 LAN), dual serial ports (1 RS232 + 1 RS485), Qualcomm enhanced WIFI, and GNSS positioning. Additionally, it supports dual external expansion cards, providing advanced internet connectivity and high-speed data access for terminals. Users can quickly set up their own application networks with this device, which also offers robust software support.

Designed for harsh industrial environments, this device meets industrial-grade standards and is designed for a wide temperature range of -40°C to 75°C. It operates on a wide voltage DC range of 9 to 48V, with hardware EMC protection up to Class 3B. The device has undergone rigorous professional environmental testing and features built-in dual watchdogs for software and hardware, as well as mechanisms for automatic fault recovery. These features ensure robust and reliable operation in various industrial settings, even in harsh and demanding environments.

The product is widely used in meteorological monitoring system, store cashier monitoring system, energy storage power station system, agricultural environment monitoring system, smart water system and other scenarios.

1.1. Product features

♦ Stable and reliable

- Industrial grade design: wide temperature-40°C~75°C, sheet metal shell, IP30 protection;
- Support horizontal desktop placement, wall hanging, rail installation;
- Wide voltage DC 9-48V input, with power reverse protection;
- Static electricity, surge, electric fast pulse group and other multiple hardware protection;
- Built-in hardware and software watchdogs, self-detection and self-repair of faults to ensure system stability.

♦ Flexible networking

- Provide 4G network system;
- Theoretical rate of cellular network: download: 150Mbps/uplink: 50Mbps (interference exists in the real environment, so the actual measurement is taken as the standard);
- Support automatic network inspection, 4G/3G/2G mode switching, support APN/VPDN private network card
- Supports dual SIM cards;
- Support 3LAN+1WAN/LAN+1WAN, 10/100Mbps rate;
- Support network cable /4G/WIFI online at the same time, intelligent switching and backup function;
- Supports 2.4GHz WiFi band and supports AP/STA/routing modes;
- Support 1*RS232+1*RS485;



♦ Powerful

- Supports TCP/UDP/Modbus TCP to Modbus RTU/MQTT data acquisition capability;
- Support GPS positioning service;
- Support PUSR Cloud services to facilitate centralized management of device systems;
- Supports VPN (PPTP, L2TP, IPSec, OpenVPN, GRE) and supports VPN encryption function;
- Support dynamic domain name (DDNS), PPPoE, DHCP, static IP function;
- Supports firewall, NAT, black and white list access restrictions, and supports SNAT and DNAT functions;
- Support SSH, TELNET and Web multi-platform management and configuration;
- Support SNMP, VLAN division, SMS service and other diversified functions;
- Supports one-click restore factory Settings and hardware watchdog;

Project		describe
	Band (-GL)	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
Cellular	Theoretical rate	The download speed of 150Mbps and the uplink speed of 50Mbps are affected by environmental interference, and the on-site measurement is taken as the standard
	Antenna interface	1* Standard SMA-K antenna interface (outer screw and inner hole)
	SIM	2*Nano-SIM
Ethernet	Number of network ports	1* WAN, 1* WAN/LAN , 3* LAN
	Network port specifications	RJ45 interface: IEEE 802.3 compliant
	Network port rate	10/100 Mbps adaptive, Auto MDI/MDIX
Wi-Fi	Wireless standards	IEEE 802.11b/g/n,2.4GHz, AP /STA/AP+STA/repeater
	Theoretical rate	300Mbps; Note: The wireless rate is affected by the environment. Please measure it as the standard.
	МІМО	2×2
	Antenna interface	2* Standard SMA-K interface
	Transmission distance	500 meters; Note: The actual transmission distance depends on the field environment. Please measure according to the actual measurement.
DTU	SOCKET	TCP/UDP/Modbus TCP to RTU/MQTT/HTTPD/AWS/ALI Pass-Through/Modbus RTU
	Heartbeat packet / registration packet	Support
	Serial port baud rate	1200/2400/4800/9600/19200/38400/57600/115200/230400

Tab 1 USR-G806p Specification parameters



	data bit;	7, 8
	stop bit	1, 2
	check bit	NONE,ODD,EVEN
	Serial port type	1*RS232、1*RS485
pilot light;	PWR	The power indicator light is on after power on
	WIFI	WiFi light, which lights up when WiFi is turned on and working properly
	NET	Green-4G
		Orange-3G
		Red-2G
	SIG	Signal 25-31-Green
		Signal 15-25-Orange
		Signal 0-15-Red
Power supply	adapter	DC 12V/1A
specifications	Power	V+、V- 2p terminal, Anti-polarity protection is available
	Power supply range	DC 9-48V
	average current	< 500mA@12V
physical	hull	Sheet metal enclosure,IP30
characteristics	Size	110.0*85.0*30.0mm(L*W*H,)
	way to install	Hang ear installation, horizontal desk placement
	ЕМС	National standard 3B
	working temperature	-40°C~75°C
	Storage temperature	-40℃ ~ 85℃
	Working humidity	5%~95%(No condensation)
other	Reload	Support restore factory
	ground protection	Grounding screws

1.2. Hardware interface diagram





Pic 1 USR-G806p Product interface diagram

1.3. Size description



Pic 2 USR-G806p View size diagram



2. Operation Instruction

2.1. Test

When the USR-G806p is used for the first time, you can connect the LAN port of the USR-G806p to the PC or connect to the WLAN wireless, and then configure it using the web management page.

parameter	default setting
SSID	USR-G806p-XXXX
LAN IP	192.168.1.1
User name	admin
password	admin
Wireless password	www.usr.cn



USR-G806p	English 中文
Communication Expert of Industrial IOT	Be Honest, Do Best!
	Authorization Required Please enter your username and password.
	Username: admin Password: Login Reset
	iNan Usr IOT Technology Limited http://www.pusr.com/

Pic 3 Login page





Pic 4 Status overview

You can query routing information and ARP tables from here.

G806p	Routes					
	The following rules a	re currently active on this system.				
ew	400					
cw.	ARP		MAC-Address	Interface		
s:	192.168.1.136		00.0exc6.72:70:e0	br-lan		
k	1321001100			or ran		
	Active IPv4-Route	25				
rver	Network	Target	<u>IPvd</u> -Gateway	Metric	Table	
	wan6_4g	0.0.0.0/0	10.209.56.102	0	main	
	wan6_4g	0.0.0.0/0	10.209.56.102	15	main	
	wan6_4g	10.209.56.100/30		15	main	
	wan6_4g	10.209.56.102		15	main	
	lan	192.168.1.0/24		0	main	
	Active IPv6-Route	25				
	Network	Target	Source	Metric	Table	
	lan	fd9c:7daf:f2f0::/64		1024	main	
	lan	ff00::/8		256	local	
	(eth1)	ff00::/8		256	local	

Pic 5 ARP

3. Network interface function



3.1. Cellular networks

ial IOT WAN Overview Status Status Actions Network VAN6_4G MAC-Address: 00: RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) 🖉 Connect 🔣 Edit eth2 WAN_4G MAC-Address: 00:0 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) Cellular Network 🖉 Connect 📓 Edit eth2 Network Failover Uptime: 0h 0m 0s MAC-Address: D4:AD:20:BD:77:46 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) AN_WIRED WLAN AP 🖉 Connect 🛃 Edit eth0 WLAN STA DHCP Static Routes Diagnostics Tcpdump VPN Firewall Serial Serve System Logout Nan Usr IOT Technology Limited http://www.pusr.com/

The router supports WAN ports for access to external networks.

Pic 6 4G Set up the interface

Tab 3 state table

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

3.1.1. Cellular network configuration



Communication Egent of Industrial IOT	Ве	Honest, Do Best! AUTO REFRESHON English †文
USR-G806p		í Í
Cellular Network Conf	iguration	
	ers, network priority, SIM card PIN code, network detection and other functions of the mobile network. iority to reduce network search time.	
> Services		
✓ Network Config		
WAN SIM1 Configuration	nfig SIM2 Config Mobile Information	
LAN Dual SIM Switching Mode	Master Standby Mode	
Cellular Network	Set the dual-SIM switchover mode	
Network Failover SIM Switching Cycle	300	
WLAN AP	In the master standby Mode, when using sim2 for internet access, it will attempt to switch to sim1 for internet access after the *SIM Switching Cycle* is reached, Value range:	
WLAN STA	180-86400%	
DHCP Link Detection Enable	Once selected, check the network connect with ping	
Static Routes Interval	10	
Diagnostics	ping interval unit: sec, 1-86400	
Tcpdump Max Ping Tries	3 Perform recovery action after reaching Consecutive failures times, 1-100	
> VPN		
Detection Address 1	119.29.29.29 Set the first address for ping check	
> Serial Server		
Detection Address 2	8.8.8.8 Set the second address for ping check	
> Logout Detection Address 3		
Detection Address 3	Set the third address for ping check	
Recovery Action	Reset Modern	
		*

Pic 7 Cellular network configuration page

Item	function	default
Dual card switching	Master-Backup Mode : SIM1 is the primary. When SIM1	Master-Backup
mode	malfunctions, it automatically switches to SIM2 for internet	Mode
	access.Once SIM1 recovers, it will switch back to SIM1	
	automatically.	
	Mutual Backup Mode : If the current SIM card can access the	
	internet, no card switching will occur.	
	Manual Mode: Lock onto SIM1 or SIM2, disabling automatic card	
	switching.	
Check the cycle	At present, when the card is connected to the network, the	300
	threshold time set here will detect whether SIM1 returns to normal	
	(the cellular network will be disconnected each time). If SIM1 is	
	restored, it will automatically switch to SIM1 access. Unit: seconds	
Fixed SIM card	When the mode is switched to manual mode, select the SIM card	SIM1
	to be locked	
Link probing	Open: Enable the SIM card Ping detection function	Close
enabled	Close: Disable the SIM card Ping detection function	
Detection time	Ping detection interval, unit: seconds	10
interval		
Number of re-tries	Number of ping probe failures	3
for detection		
Probe address 1	A total of 3 Ping addresses are detected. If one of them is	8.8.8.8

Tab 4 Cell network configuration parameter table



	pingable, the link is considered normal		
Probe address 2	A total of 3 Ping addresses are detected. If one of them is	119.29.29.29	
	pingable, the link is considered normal		
Probe address 3	A total of 3 Ping addresses are detected. If one of them is	255.5.5.5	
	pingable, the link is considered normal		
Resume the exercise	Optional: None / Re-dial / Restart module / Restart module /	Restart	the
	Restart device	module	
Signal strength	Checked: detect the interval time once, and switch the SIM card	Unchecked	
detection enabled	when the sub-signal is less than the set trigger threshold for		
	multiple times		
Detection time	Signal detection interval time, unit: second	10	
interval			
Number of re-tries	If the signal value is less than the threshold for several times, the	3	
for detection	card will be cut		
Trigger threshold	Signal threshold, unit: dbm	-80	
Ping delay detection	Checked : The interval time is detected once, and the delay of	Unchecked	
is enabled	multiple probes is greater than the set trigger threshold to switch		
	the SIM card		
Detection time	Detection interval time, unit: seconds	10	
interval			
Number of re-tries	If the detection delay exceeds the threshold, the card will be cut	3	
for detection			
Trigger threshold	Delay threshold, unit: ms	80	

3.1.2. SIM

Set the SIM1/2 card related parameters.

Communication Expert of Industrial KOT			Be Honest, Do Best! ⊮nemennement inglehi≑x
USR-G806p	Cellular Network Conf	guration	
Status Services		s, network priority, SIM card PIN code, network detection and other functions of the mobile net wity to reduce network search time.	vork.
 V Network 	Config		
WAN	Configuration SIM1 Co	fig SIM2 Config Mobile Information	
LAN	APN	Automatic Y	
Cellular Network		Input your APN Name, 0-62 characters	
Network Fallover	Username		
WLAN AP		User name for apn, 0-62 characters	
WLAN STA DHCP	Password	User password for apn, 0-62 characters	
Static Routes	Auth Method	PAP AND CHAP	
Diagnostics		Authentication type for apn	
Tcpdump	Network Type	AUTO 🗸	
> VPN	LTE band selection	auto 🗸	
> Firewall		Enter 'auto' or '1' or '1:2:3:' Supported LTE frequency bands: 1:2:3:4:5:7:8:12:13:18:19:20:25:26:28:38:39:40:41	
> Serial Server	PDP Type	IPV48.V6	
> System	MTU	1500	
> Logout	110	1300 1280~1500	
	Priority Of Network Search	AUTO 👻	
		The priority of network search	
	PIN Enable	If SIM card enable PIN, enable this function to enter the PIN code	-
192.168.1.1/cgi-bin/luci/:stok=b776f1e345d902be0d	325832397d9399/admin/network/cellular?tab.apnset.cfg016a90	liNan Usr IOT Technology Limited http://www.pusr.com/ basicset	

Pic 8 SIM



Item	Description	Default
APN	Please set the correct APN address	Auto
Username	APN username	empty
Password	APN Password	empty
Auth Method	APN authentication type: None/PAP/CHAP	empty
Network Type	Force 4G, 3G or 2G network	Auto
LTE band selection	Lock the frequency band	Auto
PDP Type	IPv4/IPv6/IPv4&v6 are optional	IPv4&v6
MTU	Set the cellular network card MTU	1500
Network search	Auto/2G/3G/4G	Auto
priority		
PIN enable	SIM PIN	Not enabled
PIN	Four to eight digits	1234
	Note: The PIN code is invalid if the PIN enablement item	
	is not enabled	
EHRPD	This option is generally not required when 5G network is	Not enabled
	started	

Tab 5 SIM

3.1.3. SIM card information

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

USR IOT Communication Expert of Industrial IOT		Be Honest, Do B Annamana ru
JSR-G806p	Cellular Network Configuration	
Status	Configure the APN parameters, network priority, SIM ca Configure network search priority to reduce network se	ard PIN code, network detection and other functions of the mobile network. arch time.
services Network	Config	
VAN	Configuration SIM1 Config SIM2 Config	Mobile Information
AN	Modern Version:	EC20CEHDLGR06A09M1G
Cellular Network	IMEI:	869446079133588
LAN AP	Dial SIM:	sim2
AN STA	SIM Status:	READY
CP	SMS Service Center:	+8613334786200
Routes	ICCID:	89861124204041429026
stics	CIMI:	460113453150069
ιp	APN:	ctnet_ctnet@mycdma.cn,vnet.mobi,1
	Attachment Status:	Attached
	Signal Strength:	20(-73dBm)
rver	Network Type:	FDD-LTE(4G)
	BAND:	LTEBAND3
	Network Operator:	CHN-CT
	IP Address:	10.25.130.194
	Location Area Code:	5277
	Cell ID:	8D85F34

Pic 9 SIM Information



3.2. LAN

LAN port is a LAN with 4 wired LAN ports (LAN4 can be set to WAN2 for use).

Skales Skales Nores Nore	Communication Expert of Indu	ны ют		Be	Honest, Do Best! Auto REFRESHON English 412
 Saturation Saturation Saturation Second Methodic March Saturation March Saturation Saturatio	USR-G806p	LAN			
 Vetwork: WAN UAN UAN Cellular Network: Network Failover WLAN STA DHCP Static Routes Diagnottics Ticpdump Verwall Serial Server System 	> Status	LAN Overview			
WAN UAN LAN Cellular Network Network Failover WLAN AP WLAN AP WLAN AP DHCP Static Routes Diagnostics Tcpdump Serial Server Serial Server System	> Services	Network	Status	Actions	
Cellular Network Network Failower WLAN AP WLAN STA DHCP Static Routes Diagnostics Tcpdump > VPN > Firewall > Serial Server > System	WAN	127 (221余)	MAC-Address: D4:AD:20:8D:77:48 RX: 4.65 MB (17212 Pkts.) TX: 3.63 MB (8601 Pkts.) IPv4: 192:168.1.1/24	S Connect	
VLAN AP Enable Vlan WLAN AFA Enable Vlan WLAN STA Apply DHCP Apply Static Routes Save Diagnostics Complete Com			IPV0: T09C/ 08DE200 1/00		
WLAN STA DHCP Static Routes Diagnostics Tcpdump > Firevall > Serial Server > System		Vlan Management			
DHCP Amb/ Save Static Routes Diagnostics Tcpdump > VPN > Finewall > Serfal Server > System		Enable Vlan			
Static Routes Diagnostics Tcpdump > VPN > Firewall > Serial Server > System					
Diagnostics Tcpdump > VPN > Firewall > Serial Server > System				Apply Save	
Tcpdump VPN Firewall Serial Server System					
> VPN > Firewall > Serial Server > System	Diagnostics				
Firewall Serial Server System	Tcpdump				
> Serial Server > System	> VPN				
> System	> Firewall				
	> Serial Server				
> Logout	> System				
	> Logout				

Pic 10 LAN

Tab 6 LAN

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

< Instruction>

- The default static IP address is 192.168.1.1 and the subnet mask is 255.255.255.0. This parameter can be modified, for example, to change the static IP address to 192.168.2.1;
- > The DHCP server function is enabled by default, and the devices connected to the LAN port of the router can automatically obtain IP addresses;



If VLAN division is used, the WIFI interface is bridged to the br-lan port, and the WIFI obtains IP and the same network segment as the br-lan network card.

3.2.1. DHCP

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

Communication Expert of Industrial IOT				Be Honest, Do Best! ⊯annamazioni trajaki+n≿
USR-G806p	General Setup			·
	Status	Uptime: 0h 5m 47s MAC-Address: D4:AD:20:8D:77:40		
> Status		B ²⁰ RX: 5.27 MB (19342 Pkts.) br-lan TX: 4.19 MB (9932 Pkts.)		
> Services		IPv4t 192.168.1.1/24		
✓ Network				
WAN	Protocol	Static address 🗸		
LAN	IPv4 address	192.168.1.1		
Cellular Network	IPv4 netmask	255.255.255.0 🗸		
Network Failover	IPv4 gateway			
WLAN AP	IPv4 broadcast			
WLAN STA	Use custom DNS servers	114.114.114.114		
DHCP		8.8.8.8		
Static Routes				
Diagnostics				
Tcpdump	DHCP Server			
> VPN > Firewall	General Setup			
> Serial Server			7	
> System	Ignore interface	Disable <u>DHCP</u> for this interface.		
> Logout	Start Address	100 Lowest leased address as offset from the network address.		
	Limit			
		Maximum number of leased addresses.		
	Leasetime	12h		
		Expiry time of leased addresses, minimum is 2 minutes (2m).		
	Back to Overview		Apply Save	
		JiNan Usr IOT Technology Limit	ed http://www.pusr.com/	

Pic 11 DHCP

< instruction>

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

3.2.2. VLAN

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



USR-G806p	LAN						
itatus	LAN Overview						
ervices	Network	Status		Actions			
letwork VAN AN iellular Network	LAN 8 ³⁷ (time in br-lan	Uptime: 0h 2m 29s MAC-Address: D4AD:20:8D:77:48 RX: 14.8 M8 (6035 Pkts.) TX: 184 M8 (4035 Pkts.) IPv6: 192:163:1.1724 IPv6: fd9c:74afd2f0c:1/60		2 Con	nect 🗹 Edit		
letwork Failover							_
VLAN AP	Vlan Management Enable						
VLAN STA							_
DHCP	Vlan List						
tatic Routes					PORTS		
Diagnostics		Network Interface	LAN1	LAN2	LAN3	LAN4 V	
cpdump		lan(br-lan)			•		
/PN		lan2(br-lan2)		O		0	
irewall		lan3(br-lan3)					
erial Server		lan4(br-lan4)				0	
lystem							
ogout			Apply Sa	ve			



< explain>

- Disable VLAN division by default. If enabled, LAN port IP will be automatically changed to 192.168.1.1, LAN2 to 192.168.2.1 and so on;
- > WIFI is bridged to LAN. When a device connects to the router's WIFI, the device obtains the IP network segment and LAN network interface in the same network segment;
- > LAN2 and LAN3 can be bridged to lan~lan4 network interface at will.

3.2.3. WAN/LAN Select

After the VLAN switch is turned on, LAN4 can be set to WAN.

SR-G806p	LAN						
atus	LAN Overview						
rvices	Network	Status		Actions			
etwork AN IN Ilular Network	LAN 8 ³⁴ G프 등 br-lan	Uptime: 0h 2m 44s MAC-Address: 0-4A2:208D:7748 RX: 1.53 M8 (6840 Pkts.) TX: 1.90 M8 (4374 Pkts.) IIPv6: 192:185.1724 IIPv6: 192:185.1724		<i>₿</i> Conr	nect 🛛 Edit		
etwork Fallover							
LAN AP	Vlan Managemen Enable						
LAN STA		vian u					
НСР	Vlan List						
atic Routes					ORTS		
agnostics		Network Interface	LAN1	LAN2	LAN3	LAN4 V WAN	
pdump		lan(br-lan)			2	LAN4	
2N		lan2(br-lan2)		O		0	
rewall		lan3(br-lan3)					
rial Server		lan4(br-lan4)					
stem							
igout			Apply Sav	re			

Pic 13 VLAN



3.2.4. DHCP

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

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

Communication Expert of Industrial IOT					Be
USR-G806p	DHCP and Static				
Status Services	DHCP list information and S		sstnames to DHCP clients. They are also requi	ired for non-dynamic interface configurations where only hosts with a corr	esponding
✓ Network	Active DHCP Leases				
WAN	Hostname	IPv4-Address	MAC-Address	Leasetime remaining	_
LAN	USR-SV**	192.168.1.136	00:0e:c6:72:70:e0	11h 56m 47s	
Cellular Network	USR-SW/	172.19.0.94	d0:39:57:51:ee:fd	11h 33m 17s	
Network Failover					
WLAN AP	Active DHCPv6 Leases				
WLAN STA	Hostname	IPv6-Address	DUID	Leasetime remaining	
DHCP Static Routes	There are no active leases.				
Diagnostics Tcpdump	Static Leases				
VPN		as multiplier in lease times, as well as time is 100 weeks.	seconds, minutes, hours and days.		
Firewall	Hostna		MAC-Address	IPv4-Address	
Serial Server					
System			This section contains no valu	ies yet	
Logout					
	New rule:				
	Hostname	MAC	-Address	1Pv4-Address	
	New rule		~	~	ڬ Add

Pic 14 DHCP

3.3. WAN

5806p	WAN				
	WAN Overview				
	Network	Status		Actions	
	WAN2_WIR asse eth1.5	Uptime: 0h 0m 0s MAC-Address: D4-AD:20:8D:77:47 RX: 0.00 B (0 Plsts.) TX: 4.97 KB (25 Plsts.)	WAN2	S Connect d Edit	
letwork Failover	WANG_4G	Uptime: 0h 0m 0s MAC-Address: D8:89:84:F3:D3:C5 RX: 806.88 K8 (4566 Pkts.) TX: 1.93 M8 (6390 Pkts.)		S Connect d Edit	
A	WAN 4G	Uptime: 0h 3m 12s MAC-Address: D6:89:84:F3:D3:C5 RX: 806.88 KB (4566 Pks.) TX: 1.93 MB (6390 Pks.) IPv4: 10.192.63.221/30		S Connect	
tes cs	WAN WIRED		WAN1	S Connect d Edit	
ver					

Pic 15 Interface configuration interface



< explain>

- > By default, the 1WAN port is enabled, and the LAN port VLAN division is enabled for WAN2;
- > WAN supports DHCP client, static IP and PPPoE mode;
- > The default IP acquisition method is DHCP Client.

3.3.1. DHCP

Communication Expert of Industrial IOT	Be Honest, Do Be Announcement	
	I - WAN_WIRED	
> Status You car	is page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. In also use <u>VLAN</u> notation INTERFACE. VLANE (e.g.: exist. 1).	
Services Network Comm	mon Configuration	
WAN General	al Setup Advanced Settings	
LAN	Status Uptime: 0h 0m 0s	
Cellular Network	MAC-Address: D4AD:20:8D:77:46	
Network Failover	etho RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	
WLAN AP		
WLAN STA	Protocol DHCP client •	
DHCP Hostn	name to send when USR-G806p	
Static Routes	requesting DHCP	
Diagnostics		
Tcpdump 🖻 Back	k to Overview Apply Save	
> VPN		
> Firewall		
> Serial Server		
> System		
> Logout		



< explain>

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



3.3.2. Static IP mode

USR IOT Communication Expert of Indust		onest, Do Best! илто велезном English фф
USR-G806p Status Services Vetwork	WAN - WAN, WIRED On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use <u>VLAN</u> notation INTERFACE, VLANIR (e.g.; etbl. 1). Common Configuration	
WAN LAN Cellular Network Network Failover WLAN AP	General Setting: Uptime: 0h 0m 0s Status Uptime: 0h 0m 0s MAC-Address: DAA2028D/7746 MAC-Address: DAA2028D/7746 etho FKA.008 (0 Pits.) TK 0.008 (0 Pits.) TK 0.008 (0 Pits.)	
WLAN STA DHCP Static Routes Diagnostics	Protocol Static address IP-4 address IP-4 netmask Please choose	
Tcpdump > VPN > Firewall > Serial Server	IPv4 gateway IPv4 broadcast Use custom DNS servers	
> System > Logout	Back to Overview Save	



< explain>

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

3.3.3. PPPoE

Communication Expert of Industrial KOT	Be Ho	nest, Do Best! AUTO REFRESH ON English লাহ
USR-G806p	WAN - WAN WIRED	
Status Services	On this page you can configure the network interfaces. You can bridge serveral interfaces by ticking the "bridge interfaces" field and enter the names of serveral network interfaces separated by spaces. You can also use <u>YLAR</u> notation INTERFACE. YLARD (<u>a.g.</u>) +30: 1].	
V Network	Common Configuration Conversional Sering: Advanced Serings	
LAN Cellular Network	Status Uptime: 0h 0m 0s Imac. Address: D4AD208027746 Imac. Address: D4AD208027746	
Network Failover WLAN AP	etho RX 0.008 (0 Pics.) TXc 0.008 (0 Pics.)	
WLAN STA DHCP	Protocod PPPOE PAP/CHAP username	
Static Routes Diagnostics	PAD/CHAP password	
Tcpdump > VPN	Back to Overview Save	
Firewall Serial Server		
> System > Logout		
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 18 WAN



< explain >

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

3.4. Network switching

Communication Expert of Indust	utrial וסד Be Honest, Do Bes נדקום אין	
USR-G806p	Network Fallover	
> Status	Configure the network switching function.	
> Services	Configuration	
 Network 		
WAN	Priority WANI3 WANZ>Celliular>ST V	
LAN	Reference Mode Custom Y	
Cellular Network	Primary Server 8.8.8.8 V	
Network Failover	P or Domain, such at 225.6.6.9 or "balductom"	
WLAN AP	Secondary Server 119.29.29.29 V	
WLAN STA	P or Domain, such at 223.6.69 or "baids.com"	
DHCP	Thirdy Server 223.5.5.5 ∨ ● Proma, such at 223.6.5 or ladaccom*	
Static Routes		
Diagnostics	Ping Interval 10 1-4-000econds	
Tcpdump	Package size 0	
> VPN	vacage sze 0 r-1024bytes	
> Firewall	Timeout 2000	
> Serial Server	100-2000/millisecords	
> System		
> Logout		
	Apply Save	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 19 Network switching configuration

Tab 7 Network switching configuration

name	description	Default parame	ter
priority	Set the NIC priority policy here	WAN1	takes
	For example, select: WAN1> WAN2> Cellular> STA. When	precedence	
	the WAN1 network card can detect the target address is		
	open, the WAN1 network card will be used to access the		
	Internet. When the WAN1 network card fails to detect the		
	target address, the WAN2, Cellular, and STA network cards		
	will be used in sequence to detect the target address.		
	Disable: Use the last network		
reference pattern	Customization: Determine the network status based on the	user-defined	
	custom reference address		
	Gateway: Probe the gateway address of each network card		
	to determine the network status		
Reference 1	You can set IP/domain name	8.8.8.8	
Reference 2	You can set IP/domain name	8.26.56.26	
Reference 3	You can set IP/domain name	208.67.222.222	



Detection interval (unit: s)	Set the link detection interval: 1-600s can be set	10
Ping packet size (unit: bytes)	Packet size for link detection: 32-1024 bytes can be set	0
Ping timeout (unit: ms)	Set the ping timeout time: can set 100-20000ms	2000

3.5. Wireless configuration

2.4G wireless LAN (Wi-Fi) function.

USR IOT Communication Expert of Industri	TOI lat			Bel	Honest, Do Best!
USR-G806p	WLAN AP Settings				
> Status	WLAN AP Settings				
Services Network	2.4G Settings Client Int	omation			
WAN LAN	Status	Mode: Master SSID: USR-G806p-7746 BSSID: D4:AD:20:BD:77:49			
Cellular Network Network Failover		Channel: 1 (2.412 GHz) Tx-Power: 20 dBm			
WLAN AP	Enable	8			
WLAN STA	Hide SSID				
DHCP	SSID	USR-G806p-7746			
Static Routes Diagnostics	Encryption	mixed-psk 🗸			
Tcpdump	Key				
> VPN	HW Mode	11ng 🗸			
> Firewall	Channel	auto 🗸			
> Serial Server		If STA is enabled, the configuration is affected by STA.			
> System > Logout	HT Mode	auto			
	Regions	CN - China 👻			
			Δnnlv Save		÷
		JiNan Usr IOT Technology Limited	http://www.pusr.com/		

Pic 20 Wi-Fi configuration intent

< explain >

- Wi-Fi and LAN can simultaneously support up to 30 clients, with a maximum of 20 being Wi-Fi clients. When Wi-Fi and LAN are not simultaneously loading clients, if there are no LAN port clients, Wi-Fi can support up to 20 wireless clients; if there are no Wi-Fi clients, only LAN port clients can support up to 50 clients. When the LAN port is configured with VLAN division, the AP segment and the LAN network share the same subnet;
- The maximum coverage of Wi-Fi is 500m in open areas, and the environment affected by obstacles such as offices can be covered within 50m;
- > The actual connection distance of Wi-Fi is greatly affected by the environment. Please test it as the actual test.

name	description	Windows default
start using	Turn on the WIFI LAN function	check
hide SSID	To enable this function: The device will not be able to search for 806w WIFI, and you need to manually enter the correct WIFI name and password to connect, ensuring the WIFI security	Not selected
WIFI name	The router's WIFI name can be customized The default value of XXXX is the last four bits of the router MAC	USR-G806w-XXXX

Tab 8WiFi configuration parameter



encryption	selectable :	mixed-psk
	No encryption/mixed-psk/psk+ccmp/psk2/psk2-tkip	
password	WIFI password, customizable	www.usr.cn
Network model	Options: 11ng/11n/11g/11bgn/11bg/11b	11ng
channel	Automatic, lockable channel	voluntarily
frequency	Auto/40MHz/20MHz is optional	auto
bandwidth		
Country or region	You can select a country or region	CN-China

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

Communication Expert of Industrial 10T					Be	Honest, Do Best!
USR-G806p	WLAN AP Settings					
> Status	WLAN AP Settings					
> Services						
✓ Network	2.4G Settings Client Information					
WAN	SSID MAC-Address	IPv4-Address	Signal	Noise RX Rate	TX Rate	
LAN	No information available					
Cellular Network	No information available					
Network Failover						
WLAN AP		Ap	ply Save			
WLAN STA		_				
DHCP						
Static Routes						
Diagnostics						
Tcpdump						
> VPN						
> Firewall						
> Serial Server						
> System						
> Logout						

Pic 21 WiFi client list page

3.6. Wireless client

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



USR-G806p Status Status Status Status Status Network Caluar Network Caluar Network Caluar Network Caluar Network Network Failover VLAN STA Caluar Network Caluar Network Caluar Network Caluar Network Failover VLAN STA Caluar Network Caluar Network <th>Communication Expert of Industrial IOT</th> <th>Be Ho</th> <th>AUTO REFRESHON English 4132</th>	Communication Expert of Industrial IOT	Be Ho	AUTO REFRESHON English 4132
> Logout	 Status Services Network WAN LAN Cellular Network Network Failover WLAN AP WLAN AP WLAN AP MULAN STA DHCP Static Routes Diagnostics Tcpdump VPN Firewall Serial Server System 	Z45 Setting: AP Information Enable Scan Scan SSID WIFI-STA Encryption No Encryption Information When selecting the LAN interface, please modify or close the Dr. P configuration of the LAN port address as the address within the upper routing subnet Encaller Ping Check: Increased end, check the wireless connect with ping 	



1 ab 9 WIFI confiduration parameter	Tab 9	WiFi configuration parameter
-------------------------------------	-------	------------------------------

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

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



Communication Expert of Indust		onest, Do Best (AUTO REFRESH ON English #文
USR-G806p	WLAN STA Settings	
> Status	WLAN STA Settings	
> Services		
 Network 	24G Settings AP Information	
WAN	SSID MAC-Address Signal Noise RX Rate TX Rate	
LAN		
Cellular Network	No information available	
Network Failover		
WLAN AP	Apply Save	
WLAN STA	(1400) 2005	
DHCP		
Static Routes		
Diagnostics		
Tcpdump		
> VPN		
> Firewall		
> Serial Server		
> System		
> Logout		

Pic 23 Connect to the AP information page

< explain >

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

3.7. Static routing

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

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 24 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.

Communication Expert of Indus	ны ют					Be Honest, Do Best! AUTO REFRESSION English 中文
USR-G806p	Static Routing					
> Status	To find information	on on static routing configuration, refe	r to the figure and table below			
Services	Static Routing	Routing Table				
✓ Network	Static IPv4 Rou					
WAN	Static IPV4 Kot Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	
LAN			dada			
Cellular Network	This section contain	s no values vet				
Network Failover						
WLAN AP	New Rule:					
WLAN STA	Interface	Target	JPy4-Netmask	IPv4-Gateway	Metric	
DHCP		Host-IP or Network	If target is a network			
Static Routes						
Diagnostics	wan_wired ¥	192.168.1.0	255.255.255.0	192.168.0.202	0	Add
Tcpdump						
> VPN			Apply	Save		
> Firewall						
> Serial Server						
> System						
> Logout						

Pic 25 Route table add page



3.8. Network diagnostic function

Communication Expert of Industrial NOT				Be Honest, Do Best! English Hot
USR-G806p	Diagnostics			
> Status	Network Utilities			
> Services	223.6.6.6	223.6.6.6	www.baidu.com	
✓ Network	IPv4 🗸 auto 🖌 🖬 Ping	IPv4 🗸 auto 🗸 🖬 Traceroute	Nslookup	
WAN				
LAN				
Cellular Network				
Network Failover				
WLAN AP				
WLAN STA				
DHCP				
Static Routes				
Diagnostics				
Tcpdump				
> VPN				
> Firewall				
> Serial Server				
> System				
> Logout				

Pic 26 Network diagnostic interface

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

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

3.9. TCPDUMP traffic monitoring

Packet capture can be performed through the web interface.

USR IOT communication Expect of Industrial IOT				Be H	onest, Do Best!
USR-G806p					2
	Start network capture				
> Status	Interface s	econds, packets	Filter	Actions	
> Services	lo 🗸	seconds 🗸	filter	Start capture	
V Network					
WAN	Output				
LAN	No capture in progress				
Cellular Network					
Network Failover WLAN AP	Capture links				
WLAN AP WLAN STA	Capture file	Modification date	Capture size	Actions	
DHCP					
Static Routes	There are no capture files availa	ble yet.			
Diagnostics					
Tcpdump					
> VPN					
> Firewall					
> Serial Server					
> System					
> Logout					
		JiNan Usr IOT Technology Limited	http://www.pusr.com/		
	r				

Pic 27 TCPDUMP

Tab 11WiFi configuration parameter



name	description	Windows default
joggle	Select the capture interface	Lo
	Br-lan: LAN interface	
	Wan_wired: WAN1 interface	
	Wan2_wir: WAN2 interface	
	Wan_4G: Cellular interface	
	Ath1: WIFI STA interface	
Capture restrictions	Capture duration or number of packets	0 seconds
filter	Fill in the filter conditions for the Tcpdump command,	empty
	such as port 80	

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

4. VPN function

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

4.1. PPTP Client

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

Communication Expert of Indu	serial IOT	Be Honest, Do Best! royani et
USR-G806p	PPTP Setting	
> Status	PPTP Parameters	
Services	PPTP Client 🖲 Enab	O Drable
Network	Server Address 192.168.0	
V VPN	Interface auto	~
PPTP	 Auto refe 	sed default route interface to connect
L2TP	User Name	
IPSec	Password	8
OpenVPN	Remote Subnet 192.168.3	
Certificate Management	@ +g: 192.1	
GRE	Remote Subnet Mask 255.255.2	
VPN Status	🔘 eg: 255.2	550
> Firewall	NAT 💈	
> Serial Server	Enable MPPE Encryption	
> System	MTU 1450	
> Logout	600~145	
	Extra option	
	Append	d options.Non - professional.careful modification
	Enable Static Tunnel IP 🗌 Address	
	Default Gatevray 🗌 🍘 Al	ffic gous to VPN, except WAN pretocol is PPPCE
	Enable Ping 🗌 🥥 Re	nect When Fails to Ping
		Apply Save

Pic 28 Router adds VPN operation diagram 1



Tab 12	PPTP configure
	PPTP configure

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
	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	

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







4.2. L2TP Client

USR IOT	trial IOT	Be	Honest, Do Best! English∣#⊄
USR-G806p	L2TP Setting		
> Status	L2TP Parameters	Ann Ann	
> Services	L2TP Client Server Address	Enable O Disable	
Network VPN	server Address Interface		
PPTP		auto (a) Auto refers used default route interface to connect	
L2TP	User Name		
IPSec	Password	8	
OpenVPN Certificate Management	Tunnel Name		
GRE	Tunnel Password	2 Character(0-50)	
VPN Status	Enable IPsec	0	
> Firewall > Serial Server	Remote Subnet	192.168.35.0	
> Senal Server > System		● ag. 192.168.10.0	
> Logout	Remote Subnet Mask	2255.255.0 @ eg: 255.255.0	
	NAT	8	
	MTU	1450 0 600-1450	
	Extra option		
		Append pppd options.Non - professional.careful modification	
	Enable Static Tunnel IP Address		
	Default Gateway	All traffic goes to VPN, except VAN protocol is PPPOE	
	Enable Ping	Peconnect When Fails to Ping	
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 30 L2TP client Settings interface

Tab 13 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 5G to connect to a VPN	
	Note: If you select a non-automatic interface, such as the	
	selected interface and server address are not accessible,	
	but other interfaces and server addresses are accessible,	
	you cannot connect to the VPN	
	Select the automatic interface. If one interface is	
	disconnected due to an exception, it can automatically	
	switch to other interfaces to try to connect to the VPN	
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-modp1024	
	ESP encryption: des-md5, des-sha1, 3des-md5, 3des-sha1	
end on ID	The ID set on the server side	
To the subnet	Use a static route through the VPN to enable subnet	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
	the VPN channel after the VPN is established	
	Unchecked: Only the VPN channel is established. If you	
	need subnet intercommunication, you need to establish a	
	static route	
	Note: If the WAN port is connected by PPPOE mode, the	
	check here is invalid	
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	Unchecked: Do not enable ping to keep alive function The address that the L2TP network card can ping is usually	empty
Ping address		empty
Ping address Ping period	The address that the L2TP network card can ping is usually	empty 10



not be sent to the set IP address and the VPN will reconnect	will reconnect
--	----------------

< explain >

> The mppe mode is: mppe required, stateless.

4.3. IPSec

Communication Expert of Industrial IOT		Be Honest, Do Best! English #文
USR-G806p	Connection Configuration	
> Status	sc Parameters	
> Services	195ec 🔹 Enable 🔿 Disable	
> Network	Interface auto Autometer used default route interface to connect	
✓ VPN	Peer Address 192.158.0.2 ● P address or domain or Narykey 1010.158. eg/Sany	
L2TP	Negotiation Method Main 🗸	
OpenVPN	Tunnel Type Site To Site 🗸	
Certificate Management GRE	Local Subnet 192.1681.0/24	
VPN Status	Peer Subnet 192.168.53.0/24	
> Firewall > Serial Server	IXE Version IXE Version IXE's only apports a single somet	
> System IKE	Encryption Algorithm 30EB	
	E Integrity Algorithm MD5	
	DiffierHellman Group Group2(1024bits)	
	IKE LIfe Time 28800	
	Authantication Type Pre-shared Key V	
	Pre-shared Kay Grancher(150)	
	Local Identifier © IP addess or ©domain Character/0-29 eg 10 10.1.80, eg @not	
	Peer Identifier @server	

Pic 31 IPSec Settings interface



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	
	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)	holotype
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	
	You can fill in up to 10 segments	
To the subnet	Fill in the destination subnet segment, and set the	192.168.55.0/24
	destination to be consistent with the destination subnet	
	You can fill in up to 10 segments	
IKE edition	ikev2/ikev1, and the configuration is consistent with that of	ikev2
	the other end	
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 the	@server
	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	
ESP verification algorithm	Select the ESP verification algorithm and configure it to be	SHA-1
	consistent with the other end	
PFS	Select the PFS configuration and match it to the end	DH2
	configuration	
ESP life cycle	ESP life cycle Settings, unit: seconds	3600
DPD overtime	Set the DPD timeout time in seconds	60
DPD detection cycle	DPD detection cycle setting, unit: second	60
DPD activity	Optional: None/removal/maintenance/reboot	restart



4.4. OpenVPN

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

USR-G806p	OpenVPN Configuration							
Status	Enhanced OpenVPN design a	allows 3 OpenVPN Clients and	1 OpenVPN Server					
Services	OpenVPN Configuration	n						
Network	Name	Туре	Description	Enab	le	Status		
/PN PPTP	CLIENT_1	CLIENT		OFF	~	Disconnected	📓 Edit	
.2TP	CLIENT_2	CLIENT		OFF	~	Disconnected	Z Edit	
PSec	CLIENT_3	CLIENT		OFF	~	Disconnected	dit	
Certificate Management	SERVER_1	SERVER		OFF	~	Disconnected	🗷 Edit	
GRE								
VPN Status				Apply				
Firewall								
Serial Server								
System								
Logout								

Pic 32 Open the OpenVPN page

Tab 15	OpenVPN Client parameter table
--------	--------------------------------

name	description	Default parameter	
start using	using Open: Open the openvpn client		
	Close: Disable the openvpn client		
description You can customize the description of this OpenV		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	Tap network cardfill in the IP address of the TAP network card on this end	
Tap the subnet mask	p the subnet mask If the authentication type is no/pre-shared password, fill in	
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,	
	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	
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-MTU/T	Set the data pack length	Air / air / 1450
CP 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	Set the static route target segment established by the	empty
route-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	
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 16 OpenVPN Server parameter table

name	description	Default parameter
start using	Open: Start the openVPN server	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	
protocol	tcp/udp/tcp ipv4/udp ipv4	udp
port	Set the openvpn server port number	1194
Type of certification	None, SSL/TLS, user name and password, pre-shared key,	SSL/TLS
	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 DUCD services Use the rester LAN pert	convice
configuration	Use the device's own DHCP service: Use the router LAN port DHCP service	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	
topology	Net30/p2p/subnet, which is usually the default value	subnet
IPv4 tunnel network	Open the IP subnet assigned to the client for OpenVPN,	
IPV4 turinet network	such as 192.168.100.0	empty
IPv4 tunnel subnet		ompty
mask	Enter the subnet mask assigned to the client by OpenVPN, for example: 255.255.255.0	empty
Local tunnel IP	· · · · · · · · · · · · · · · · · · ·	ampti
Local lunnel IP	When the authentication type is no/pre-shared password, fill in the local TUN tunnel IP	empty
Remote tunnel IP	When the authentication type is no/pre-shared password,	empty
	fill in the end-to-end tunnel IP of this end	empty
begin IP	The TAP bridge mode specifies the starting IP address, such	empty
beginir	as 192.168.100.100	empty
	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	empty
Enter the IP address of	If the authentication type is no/pre-shared password, fill in	empty
the Tap network card	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	
The client	When the client reaches the set value, it will renegotiate	3600
renegotiates the time	and reconnect. This is a security mechanism of openvpn	
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	
Maximum number of	Set the upper limit of the number of clients that can	16
customers	connect to the service	
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 OpenVPN Server	
Redirect gateway	Use openvpn as the default gateway	close
•	It takes effect after you select "None" in "Network	



	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 time interval (seconds)	VPN live heartbeat detection interval	10
Connection detection timeout interval (seconds)	If the heartbeat exceeds the set time without response, reconnect the VPN	120
Enable LZO	Data compression method	No preference
encryption algorithm	Data encryption algorithm	BF-CBC
Hash algorithm	The data's hash algorithm	SHA1
TLS way	Select the TLS authentication method	OFF
LINK-MTU/TUN-MTU/T CP MSS	Set the data pack length	Air / air / 1450
Maximum frame length	The maximum frame length of data is the default without special configuration	empty
Allows remote address changes	Whether to allow remote address change Settings	close
Log grade	Openvpn log level, the larger the number of log is more detailed, generally open a larger level to troubleshoot problems when the connection is abnormal	Warning (3)
Additional configuration	Non-professionals should not configure it. You need to input openvpn recognizable parameters	empty
user	Set the user name and password account for the client connective the user name and password to take effect. Set multiple acco password for each client	·
user name	Set the client connection user name, and you can set multiple user names and passwords	empty
password	Set the client connection password, and you can set multiple user name passwords	empty
The client is assigned	Set the parameters for assigning fixed IP addresses to client	s. 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 value of the client certificate, such as client1 If you use only the form of user name and password: Enter the user name value here	empty
Static IP address	Set the static IP address assigned to the client, such as	empty
	1	1



	192.168.100.2	
subnet mask	Set the subnet mask assigned to the client, for example: 255.255.255.0	empty
Customer subnet	To enable subnet interworking, you need to fill in the subnet	segment of each client, and
	openvpn will automatically push the routing function	
name	Use the certificate form: This is set to the CN corresponding	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 192.168.1.0	empty
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	



Communication Expert of Industrial IOT	Be Hor	nest, Do Bes English 4
USR-G806p	Certificate Management	
> Status	The current page is used to centrally manage various certificate and key files related to OpenVPN	
> Services	Client1 Certificate	
Network VPN	pkcs12(p12) 意思能文明 - 美国指任何文件 例 PCSF12 [17] Risk define an active Ris format for storing cryptographic objects as a single Rie. It means that p12 Rie is able to contain ca & cert & key. Generally if you have a p12 Ris already there is no need to unploaded a & cert & key one by one.	
PPTP L2TP	ca 建建文件 未把择任何文件	
IPSec	cert 逐渐交佳 未退得任何文件	
OpenVPN	key 透明文件,未进明任何文件	
Certificate Management	tls-auth(secret key) 透路定体,未选择任何文件	
GRE	tls-crypt(secret key) 选择文件 未选择任何文件	
VPN Status > Firewall	Pre-shared key(secret key) 送账文件 》来出版任何文件	
> Serial Server	Certificate Password Type 🔹 file 🔿 input	
> System	Certificate Password 建建築文件 未选择任何文件	
> Logout		
	Client2 Certificate	
	pkcs12(p12) 通知任何文件 ④ PHCS+12 1917; Bind defend and a strike file format for storing cryptographic objects as a single file. It means that p12 file is able to contain cs & cert & key. Generally if you have a p12 file altrady, there is no need to upladed cs & cert & key one by one.	
	ca [进程文件] 未退得任何文件	
	cett 透现文件 制造绿任何文件	

Pic 33 OpenVPN certificate page

Tab 17 OpenVPN Server parameter table

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

< explain >

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



4.4.1. OpenVPN TAP bridge example

It is generally used for APN dedicated network card +OpenVPN to realize the function of LAN for multiple terminals. Note: In this scheme, LAN port DHCP should be turned off for each router, and the router configuration should be in the same network segment and the IP address should not conflict.



Pic 34 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.

USR IOT Communication Expert of Industria		Be H	onest, Do Best! AUTO REFRESH ON English 부玟
MUMIC Consectory	General Setup		
USR-G806p	Status	MAC-Address: D4-AD:20:8D:77:48 BY: 16 25 MR (49381 Ptrs.)	
> Status		brian TX: 26.14 MB (45982 Pkts.)	
> Services		IPv4: 192.168.1.1/24	
✓ Network	Protocol	Static address	
WAN	IPv4 address	192.168.10.1	
LAN			
Cellular Network	IPv4 netmask	255.255.255.0 ¥	
Network Failover	IPv4 gateway	192.168.10.1	
WLAN AP	IPv4 broadcast		
WLAN STA		114.114.114	
DHCP	Use custom DNS servers	114.114.114 💌 8.8.8.8 🛍	
Static Routes			
Diagnostics			
Tcpdump	DHCP Server		
> VPN			
> Firewall	General Setup		
> Serial Server	Ignore interface	Disable DHCP for this interface.	
> System	Start Address	100	
> Logout		Q Lowest leased address as offset from the network address.	
	Limit	150 Maximum number of leased addresses.	
	Leasetime	12h Grain time of leased addresses, minimum is 2 minutes (2m).	
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 35 LAN port configuration

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



Communication Expert of Indust	irial IOT	Be Honest, Do Best! English (+x)
USR-G806p	SERVER_1 - OpenVPN Configuration	I Configuration
> Status > Services > Network	Configuration Enable Description	
VPN PPTP L2TP	Enable OpenVPN Config from file Protocol	
IPSec OpenVPN Certificate Management		1194
GRE VPN Status > Firewall	TUN/TAP Bridge Network	
 Serial Server System Logout 	Tap bridging network configuration mode Renegotiation Interval(s)	
	max clients Client to client	Allow a maximum of n simultaneously connected clients.
		JINan Usr IOT Technology Limited http://www.pusr.com/

Pic 36 OpenVPN configuration 1

Set a set of user names and passwords.

Communication Expert of Industrial IOT					Be Honest,
USR-G806p	Extra Option	e content here will be written direct	y to the configuration file. Please fill in carefully	8	
 Status Services Network 	User Username	_	Password		_
V VPN PPTP L2TP	test		test	X Delete	
IPSec OpenVPN Certificate Management GRE	New User: User	name	Password	i 20 A	dd
VPN Status VFN Status > Firewall > Serial Server	Client Static Ip User	Static Ip		Vetmask/P2P IP	
> System > Logout			This section contains no values yet		
	Tunnel static IP: User		Static IP	Netmask/P2P IP	
	JiNar	n Usr IOT Technology Limite	ed http://www.pusr.com/		

Pic 37 OpenVPN configuration 2

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



USR-G806p Certificat	ie Management
Status The current	page is used to centrally manage various certificate and key files related to OpenVPN
Client1 C	ertificate
Network VPN PPTP L2TP IPSec OpenVPN	pks12(p12) 夏夏安使 未認時任何文件 ● PXC5H2 (P12) File define an archive file format for storing crystographic objects as a single file. It means that p12 file is able to contain ca & cert & key. Generally if you have a g12 file alwayd, there is no need to upload ca & cert & key one by one. Ca 夏夏安使 未認知知道 cert 夏夏安使 未認知任何文件 key 夏夏安使 未認知任何文件
icate Management tls-au	th(secret key) 透耀文件 未退埠任何文件
N Status	p(scoret key) 通频交击 未选择任何文件 ex(scoret key) 通频交击 未选择任何文件
	Password Type 🛛 🐵 File 🛛 input
em Certifi	cate Password 逻辑文件 未愿得任何文件
gout	

Pic 38 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 Anno Mersea
	General Setup	
USR-G806p	Status	Uptime: 0h. 29m 13s # MAC-Address: D4A202080:77-88 RK 2: 518 MC (2546 Vets.)
> Status		Drian TX: 38.32 MB (68717 Pkts.) IPv4: 192.168.1.1/24
> Services		
✓ Network	Protocol	Static address 🗸
WAN LAN	IPv4 address	192.168.10.2
Cellular Network	IPv4 netmask	255.255.255.0 🔹
Network Failover	IPv4 gateway	192.168.10.1
WLAN AP	IPv4 broadcast	
WLAN STA		114.114.114
DHCP	Use custom DNS servers	114.114.114.114 A
Static Routes		
Diagnostics		
Tcpdump	DHCP Server	
> VPN		
> Firewall	General Setup	
> Serial Server	Ignore interface	I is able <u>DHCP</u> for this interface.
> System	Start Address	100
> Logout		Lowest leased address as offset from the network address.
	Limit	150 Maximum number of leased addresses.
		12h © Expiry time of leased addresses, minimum is 2 minutes (2m).

Pic 39 LAN port configuration

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



USR IOT	al lor		Be Honest, Do Best! _{English↓‡‡}
USR-G806p	CLIENT_1 - OpenVP V	I Configuration	
> Status	Configuration		
> Services	Enable	0N 🗸	
Network VPN	Description	The maximum length is 50 Bytes.	
PPTP L2TP	Enable OpenVPN Config from file		
IPSec	Protocol	UDP Y	
OpenVPN	Remote Host IP Address	192.168.66.109	
Certificate Management	Port	1194	
GRE VPN Status	Authentication Type	Username/Password	
> Firewall	TUN/TAP	TAP	
> Serial Server	Bridge Network	LAN V	
> System > Logout	User name	test © Username used for authentication to the VPN server. It is needed when Authentication Type contains Username/Password.	
	Password	test # Password used for authentication to the VPN erver. It is needed when Authentication Type contains Username/Password.	
	Renegotiation Interval(s)	3600	-
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 40 OpenVPN configuration 1

Communication Expert of Industr	ы ют			Be Honest,
Communication typert of Indust USR-G806p Status Services Network VPN PPTP L2TP IPSec OpenVPN Certificate Management GRE VPN Status Firewall Serial Server System	Certificate Manageme	centrally manage various certificate and key fil 透祥文件 未选择文件	at for storing cryptographic objects as a single file. It m	nans that p12 file is able to contain ca & cert & key.
> Logout				

Pic 41 OpenVPN configuration 2

Test that PC1 and PC2 can communicate with each other:





4.4.2. An example of subnet interworking in OpenVPN TUN mode



Pic 42 Connect the topology



Router 1 configuration, LAN port setting

USR IOT Communication Expert of In	dustrial IOT	
USR-G806p	LAN - LAN	
> Status		nfigure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and paces. You can also use <u>VLAN</u> notation INTERFACE. VLANRR (e.g.: eth0. 1).
Services Network	Common Configuration	tion
WAN LAN Cellular Network	General Setup Status	MAC-Address: D4:AD:20:BD:77:48
Network Failover WLAN AP		RX: 24.95 MB (57060 Pkts.) br-lan TX: 31.23 MB (55866 Pkts.) IPv4: 192.168.1.1/24
WLAN STA DHCP	Protocol IPv4 address	
Static Routes Diagnostics	IPv4 netmask	
Tcpdump > VPN	IPv4 gateway IPv4 broadcast	
> Firewall > Serial Server	Use custom DNS servers	
> System > Logout	₩ ▼	

Pic 43 Router 1 is configured 1

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

USR IOT Communication Expert of Industrial	ют	Be Honest, Do Best! English ≉∞
USR-G806p	SERVER_1 - OpenVPN Configuration	Configuration
> Services	Enable	on 🖌 🗸
> Network VPN	Description	The maximum length is 50 Bytes.
PPTP L2TP	Enable OpenVPN Config from file	Not Support
IPSec	Protocol	UDP V
OpenVPN	Port	1194
Certificate Management GRE	Authentication Type	ssi,/TLS 🖌 🗸
VPN Status	TUN/TAP	TUN
> Firewall	Тороlоду	Subnet 🗸 🗸
> Serial Server	Client Subnet	100.100.0
> System	Client Netmask	255.255.0 🕊
> Logout	Renegotiation Interval(s)	3600
	max clients	16 Allow a maximum of n simultaneously connected clients.
		JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 44 Router 1 is configured 2

Enter the client subnet information and click "Save"



USR IOT Communication Expert of Industrial IOT							Ве Нс	nest
USR-G806p	User		Static IP		Netmask/P2P IP		🛅 Add	
tatus	Client subnet							
ervices etwork	Name	Subnet		Netmask				
n	client1	192.168.1.0		255.255.255.0		💌 Delete		
TP TP								
	New Client Network:							
ec enVPN	Name		Subnet		Netmask			
rtificate Management	Name		Network		Netmask		bbA 😭	
RE	Local Route - LAN IP add	lross and subnot mask o	of the remote network					
N Status		Subnet	a the remote network		Vetmask			
ewall rial Server								
stem			This section con	tains no values yet				
ogout								
	Local Route:							
		Subnet		Netm	ask			
	Network			Netmask		t	Add	

Pic 45 Router 1 is configured 3

•	F1-3		
USR IOT Communication Expert of Indus			
USR-G806p	Certificate Password		
> Status > Services	Server Certificate pkcs12(.p12)		mat for storing cryptographic objects as a single file. It means that .p12 file is able to con
Network VPN PPTP L2TP	ca cert key	Generally if you have a .p.12 file already, there if 透释文件 未选择文件 选择文件 未选择文件 选择文件 未选择文件	: no need to upload ca & cert & key one by one.
IPSec OpenVPN Certificate Management	DH tis-auth(secret key)	 选择文件 未选择文件 选择文件 选择文件 	
GRE VPN Status > Firewall	tis-crypt(secret key) Pre-shared key(secret key) Certificate Revoke List	透释文件 未选择文件 透释文件 未选择文件 透释文件 未选择文件	
 Serial Server System Logout 	Certificate Revoke List Certificate Password Type Certificate Password	● file ○ input 遠择文件 未选择文件	
		JiNan Usr IOT Technology Limited	Apply Save
		Sinvan Osi ion reciliology Linited	http://www.pusi.com/

Enter the OpenVPN server certificate and click "Apply".

Pic 46 Router 1 is configured for 4

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



USR IOT Communication Expert of Indust	Be Ho
USR-G806p Status Services Network VPN PPTP L2TP IPSec OpenVPN Certificate Management GRE	CLIENT_1 - Op enVPN Configuration Configuration Enable ON V Description • The maximum length is 50 Bytes. Enable OperVPN Config On • Off from file • On • Off Protocol UDP V Remote Host IP Address 192.168.66.109 Port 1194
VPN Status Firewall Serial Server System Logout	Authentication Type SSL/TLS TUN/TAP TUN Topology Subnet Renegotiation Interval(s) 3600 Interface Auto
	JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 47 Router 2 is configured 1

Client adds information to the server subnet.

Communication Expert of Indust	rial IOT		Be Honest, Do
	Fragment	2 Enable internal datagram fragmentation:128~1500.If you are not familiar with this option, please	leave it empty.
USR-G806p	Remote Addr Float	O Allowing the remote end to change its IP address/port	()
> Status	Log Level	warning(3)	
Services Network VPN	Extra Option	Log LevelO-11 The content here will be written directly to the configuration file. Please fill in carefully	
РРТР		 The content rate minute interest or an comparation must have in in containing 	
L2TP	Local Route - LAN IP ad	dress and subnet mask of the remote network.	
IPSec	Subne		
OpenVPN			
Certificate Management	192.168.1	0.0 255.255.255.0	🗷 Delete
GRE VPN Status			
> Firewall	Local Route:		
> Serial Server		Subnet Netmask	
> System	Network	Netmask	Add 😭
> Logout			
	Back to Overview	Apply Save	
		iNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 48 Router 2 is configured 2

Enter the OpenVPN client certificate and click "Apply".



USR IOT Communication Expert of Indust		onest,	Do Best! English 中文	
USR-G806p Status Services Network VPN L2TP L2TP L2TP L2TP L2TP Certificate Management GRE VPN Status Serial Server System Logout	Certificate Management The current page is used to centrally manage various certificate and key files related to OpenVPN Client1 Certificate pics12(:12) BBXCH 未放排文件 PicS412(:12) BBXCH 未放排文件 Certificate BBXCH 未放排文件 Certificate Address USH 未放排文件 Certificate Password BBXCH 未放排文件 USH 未放拌文件 USH 未放拌文件 USH 未放拌文件 USH 未放拌文件 USH 未放拌文件 USH 未放拌文件 OF IDE		Î	
	Client2 Certificate pkcs12(p12) 選擇文件		-	
	JINan Usr IOT Technology Limited http://www.pusr.com/			-

Pic 49 Router 2 is configured 3

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

SR IOT mmunication Expert of Industrial IOT						Be Ho	nest,
806p							_
	OpenVPN Clients Common Name	Virtual Address	Real Address	Bytes Received	Bytes Sent	Connected Since	
				-,	-,		
	VPN						
	VPN Status						
		JiNan Usr IOT Techno	logy Limited http://	www.pusr.com/			

PC1 and PC2 are interconnected





Pic 50 PC1 and PC2 are interconnected

4.5. GRE

USR IOT Communication Expert of Indust	rial for	Be Honest, Do Best! English ⊄α
USR-G806p	GRE Setting	
> Status > Services	GRE Parameters GRE	® Enable O Disable
> Network	Interface Name	gre_gre1 @ unused.egr.gre1
PPTP L2TP	Interface	auto v
IPSec OpenVPN	Peer WAN IP Peer Tunnel IP	192.168.0.10 10.10.10.1
Certificate Management	Peer Subnet	192.168.55.0/24
VPN Status > Firewall	Local Tunnel IP NAT	10.10.2
> Serial Server > System	πι	255 21-255
> Logout	МТU	1450 © 600-1500
	Enable Ping	@ Reconnect When Fails to Ping
		JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 51 GRE basic configuration

< explain >

- > Remote address: WAN port IP address of the remote GRE;
- Local address: The local wan_wired and wan_4g addresses are input according to different networking modes;
- > Remote tunnel address: GRE tunnel IP of the other end;
- > For the subnet: For setting the subnet mask, it can be expressed as follows: 255.255.255.0 can be written as



IP/24, and 255.255.255.255 can be written as IP/32. For example: 172.16.10.1/24 corresponds to IP 172.16.10.1, and the subnet mask is 255.255.255.0;

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

5. Firewall

5.1. Basic Settings

The default is to enable two firewall rules.

	Communication Expert of Industrial		onest, Do Best! English 中文
USR-G806p Frewall - Zone Settings > Status The frewall creates zones over your network interfaces to control network traffic flow. > Services General Settings		The firewall creates zones over your network interfaces to control network traffic flow.	
Network Enable SYN-flood VPN Drop Invalid packets Firewall Drop Invalid packets General Settings Input Port Forwards output Port Forwards Output Custom Rules Forward Access Restrictions Serial Server	VPN Firewall General Settings Port Forwards Traffic Rules Custom Rules Access Restrictions	protection Drop invalid packets Input accept cutout	
System > Logout Source Zone=>Destination zones Inn: Inn: Inn: Inn: <th></th> <th>Source Zone=>Destination zones Input Output Forward Masquerading MSS clamping Iant: Ian: :::::::::::::::::::::::::::::::::</th> <th></th>		Source Zone=>Destination zones Input Output Forward Masquerading MSS clamping Iant: Ian: :::::::::::::::::::::::::::::::::	

Pic 52 Firewall Settings page

[Term Introduction]

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

[Rule 1]

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



[Rule 2]

- > The wired WAN port and 4G port accept "incoming", "outgoing" and allow "forwarding";
- If there is an "incoming" packet, such as someone trying to log in to the router's web page from a WAN port, it will be allowed;
- > If there is an "outgoing" packet, such as a router accessing the Internet through a WAN port or 4G port, this action is allowed;
- > If there is a "forwarding" packet, such as a packet coming from the WAN port that wants to be forwarded to the LAN port, this action is allowed.

5.2. Communication rules

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

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

Tab 18 Communication rule parameter table



	LAN: Indicates the rules for subnet access to the Internet	
	WAN: Indicates the rules for accessing the Intranet from	
	the Internet	
destination address	The target IP address to visit	empty
	Empty: Represents all addresses	
Target port	The target port number to visit	empty
	Air: represents all	
movement	Receive such packets with options: discard, accept,	accept
	reject, or no action	
	Discard: This rule packet will be discarded upon receipt	
	Accept: The packet will be accepted if it is received	
	Reject: This rule packet will be rejected upon receipt	
	No action: No action is taken when this rule packet is	
	received	

5.2.1. IP address blacklist



Communication Expert of Industrial IOT					Ве Но	nest, Do Best! English #12
USR-G806p	1	IPv4-ICMP From IP 192 168 1.100 in <i>Ian</i> To IP 47.103.49.100 in wan	Accept forward	••	Edit 🗶 Delete	
 Status Services 	2	IPv4-ICMP From any host in lan To any host in wan	Refuse forward	••	Edit 🗷 Delete	
> Network	Open ports on router:					
> VPN	Name	Protocol External port				
✓ Firewall General Settings	New input rule	TCP+UDP 🗸				
Port Forwards						
	New forward rule:					
Custom Rules	Name	Source zone Destination zone				
Access Restrictions	test	lan 🗸 wan 🗸 🖻 Add and edit	1			
> Serial Server						
> System	Source NAT					
> Logout	Name	Protocol		Action	Enable Sort	
		This section contains no values	; yet			
	New source NAT:					
	Altered	JiNan Usr IOT Technology Limited http://www.pusr.com	n/			

Pic 53 Figure 1 of the firewall blacklist

In the redirected page, select LAN for the source area, and select all for the source MAC address and source address (if you only restrict a specific IP address within the LAN to access a specific IP address outside the LAN, you need to fill in the IP address or MAC address), as shown in the following figure:





Pic 54 Figure 2 of the firewall blacklist

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

USR IOT Communication Expert of Indust	rial IOT	Be Honest, Do
	Source MAC address Source IP address Source ort Destination zone Destination address Destination port Action	wan: wan_wired: wan_4g: wanb_4g: wa
	Back to Overview	Apply Save
		JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 55 Figure 3 of the firewall blacklist



Communication Expert of Industrial IOT					Be Hone	est, Do Best! _{English 中文}
USR-G806p	1	IPv4-ICMP From IP 192.168.1.100 in Ian To IP 47.103.49.100 in wan	Accept forward		dit 🗶 Delete	*
> Status > Services	2	IPv4-ICMP From <i>any host</i> in <i>lan</i> To <i>any host</i> in <i>wan</i>	Refuse forward		dit 🗶 Delete	
> Network > VPN	-	IPv4-TCP,UDP From IP <i>192.168.2.33</i> in <i>lan</i> To <i>any host</i> in <i>wan</i>	Refuse forward		dit 🗙 Delete	
Firewall General Settings	Open ports on router:					
Port Forwards	Name	Protocol External port				
Traffic Rules Custom Rules	New input rule	TCP+UDP 🗸 🗿 Add				
Access Restrictions	New forward rule:					
> Serial Server	Name	Source zone Destination zone				
> System	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit				
> Logout						
	Source NAT					
	Name	Protocol		Action	Enable Sort	
		This section contains i	no values yet			•
		JiNan Usr IOT Technology Limited http://www.p	pusr.com/			

Pic 56 Figure 4 of the firewall blacklist

After this setting is completed, the blacklist function is implemented. That is, the IP address of the subnet device 192.168.2.133 is prohibited from accessing all external networks.

5.2.2. IP address whitelist

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

USR IOT Communication Expert of Industr		lonest, Do Best! _{English} ∣≄x́
Wine continue.	To any host in wan	
USR-G806p	Any TCPUDP test From any host in lan To any host in wan	
> Status		
> Services	Open ports on router:	
> Network	Name Protocol External port	
> VPN	New input rule TCP+UDP V	
✓ Firewall		
General Settings	New forward rule:	
Port Forwards	Name Source zone Destination zone	
Traffic Rules		
Custom Rules	test Ian V wan V 🖻 Add and edit	
Access Restrictions		_
> Serial Server	Source NAT	
> System	Name Protocol Action Enable Sort	
> Logout		
	This section contains no values yet	
	New source NAT:	
	Name Source zone Destination zone To source IP To source port	
	New SNAT rule Ian v wan v - Please cht v Do not rewrite Add and edit	-
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 57 Firewall whitelist Figure 1

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



Communication Expert of Industr	nal IOT	Be Honest,	Do Best! English 中文
	Enable	A Disanis	
USR-G806p	Name	test	
> Status	Restrict to address family	IPv4 only	
> Services	Protocol	TCP+UDP	
> Network	Match ICMP type	any 🗸	
> VPN	Source zone	O Any zone	
Firewall General Settings		Ian: Ian: 翌 魚	
Port Forwards		O wan: wan_wired: 🛃 wan_4g: 🛃 wan6_4g: 🛃	
Traffic Rules Custom Rules	Source MAC address	any Orly match incoming traffic from these MACs.	
Access Restrictions	Source IP address	192.168.2.133	
> Serial Server		Only match incoming traffic from this IP or range.	
> System	Source port		
> Logout		Only match incoming traffic originating from the given source port or port range on the client host	
	Destination zone	O Device (Input)	
		O Any zone (forward)	
		O lan: lan: 💯 🛞	
		wan: wan_wired: 2 wan_4g: wan6_4g: 2	~
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 58 Figure 2 of the firewall whitelist

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

Communication Expert of Industrial IOT		Be Hones	st, Do Best! English 中文
USR-G806p	Source MAC address	Wan: wan_dg: wan_dg:	*
StatusServices	Source IP address	192.168.2.133 O Only match incoming traffic from this IP or range.	
> Network > VPN	Source port	any Only match incoming traffic originating from the given source port or port range on the client host	
 Firewall General Settings Port Forwards Traffic Rules Custom Rules 	Destination zone		
Access Restrictions Serial Server	Destination address	any Redirect matched incoming traffic to the specified internal host	
> System > Logout		Redirect matched incoming traffic to the given port on the internal host accept	
	Back to Overview	Apply Save	
		JINan Usr IOT Technology Limited http://www.pusr.com/	

Pic 59 Figure 3: Firewall whitelist

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



Communication Expert of Industrial IOT				Be H	onest, Do Best! _{English #文}
USR-G806p > Status		or packets traveling between different zones, for example to	reject traffic between certain hosts or	to open WAN ports on the router.	Î
> Services> Network	Traffic Rules	Protocol	Action	Enable Sort	· · · ·
VPN Firewall General Settings	test	IPv4-TCP,UDP From IP <i>192 168.2.133</i> in <i>Ian</i> To <i>any host</i> in <i>wan</i>	Accept forward	🖉 🔹 👻 🛃 Edit 😢 Delete	
Port Forwards Traffic Rules	test1	IPv4-TCPUDP From any fastin lan To any fastin wan	Refuse forward	🛛 🔹 🖉 Edit 🗶 Delete	
Custom Rules Access Restrictions	Open ports on router:				
> Serial Server	Name P	rotocol External port			
> System	New input rule	TCP+UDP 🗸			
> Logout					
	New forward rule:				
	Name S	ource zone Destination zone			
	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit			
					~
	Course NIAT	JINan Usr IOT Technology Limited http://ww	w.pusr.com/		· · · ·

Pic 60 Figure 3 of the firewall whitelist

5.3. NAT function

5.3.1. IP address spoofing

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

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

USR IOT Communication Expert of Indust		nest, Do Best! English∣#文
USR-G806p	Firewall - Zone Settings The firewall creates zones over your network interfaces to control network traffic flow.	
Services Network VPN Firewall	General Settings Enable SYM-flood protection Drop invalid packets	
General Settings Port Forwards Traffic Rules Custom Rules Access Restrictions	Unop invalid packets Imput input accept Output accept Forward accept	
Access restructions Serial Server System Logout	Forward Destination zones Input Output Forward Masquerading MSS clamping Input Input Output Forward Incept v accept v accept v Input Input Input MSS clamping Input Input Input Output Forward Input Inpu	
	Apply Save JiNan Usr IOT Technology Limited http://www.pusr.com/	-

Pic 61 IP address disguise Settings



5.3.2. SNAT

Source IP conversion function.

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

Tab 19 SNAT parameter list

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



USR IOT Communication Expert of Indus		nest, Do Best! _{English 中文}
USR-G806p Status Services	Firewall - Zone Settings The firewall creates zones over your network interfaces to control network traffic flow. General Settings	Î
Network VPN Firewall General Settings Port Forwards Traffic Rules Custom Rules Access Restrictions Setral Server	Enable SYN-flood protection Drop invalid packets Input accept Forward accept	
 Serial Server System Logout 	Zones=>Forward Input Output Forward Masquerading MSS clamping Ian: Image: Second Sec	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Then set up the Source NAT

Communication Expert of Industrial IOT		Be Honest, Do Best! English ≠≿
USR-G806p	Name Protocol External port	
	New input rule TCP+UDP V	
> Status		
> Services	New forward rule:	
> Network	Name Source zone Destination zone	
> VPN	New forward rule Ian v wan v Add and edit	
✓ Firewall		
General Settings	Source NAT	
Port Forwards		
Traffic Rules	Name Protocol	Action Enable Sort
Custom Rules		
Access Restrictions	This section contains no values yet	
> Serial Server		
> System	New source NAT:	
> Logout	Name Source zone Destination zone To source IP To source port	
	test Ian v wan 192.168.9.1 v Do not rewrit	e Add and edit
	Apply Save	
	https://www.	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 62 NAT Settings 1

Click Add and Edit



USR IOT Communication Expert of Indus	rial KOT	Be H	onest, Do Best! _{English 412}
	Firewall - Traffic Rules	- SNAT test	
USR-G806p	This page allows you to char	nge advanced properties of the traffic rule entry, such as matched source and destination hosts.	
> Status	Enable	Ø Disable	
> Services	Name	test	
> Network > VPN	Protocol	ICMP V	
✓ Firewall	Source zone) Ian: Ian: 22 ()	
General Settings		O wan: wan_wired; 2 wan_4g; 3 wan6_4g; 3	
Port Forwards Traffic Rules	Source IP address	any Conly match incoming traffic from this IP or range.	
Custom Rules Access Restrictions	Source port	any Match incoming traffic originating from the given source port or port range on the client host.	
Serial Server System	Destination zone	○ lan: lan:要素	
> Logout		wan: wan_wired: A wan_4g: Wan64g: Wan64g: Wan64g: Man64g: M	
	Destination IP address	Destination ip or ip range.	
	Destination port	any Destination port or port range.	
	SNAT IP address	192.168.9.1	•
		JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 63 NAT Settings 2

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

Communication Expert of Indus	rial IOT			Be H	onest, Do Best! English 中文
1100 0000	Name	Protocol External port			
USR-G806p	New input rule	TCP+UDP 🗸 🖄 Add			
> Status > Services	New forward rule:				
> Network	Name	Source zone Destination zone			
> VPN	New forward rule	lan 🗸 wan 🗸 🖻 Add and edit			
✓ Firewall					
General Settings	Source NAT				
Port Forwards	Name	Protocol	Action	Enable Sort	
Traffic Rules		Any ICMP		1	
Custom Rules	test	From any host in lan	Rewrite to source IP 192.168.9.1	🛛 🔹 🔹 🗹 Edit 💌 Delete	
Access Restrictions		To any host in wan			
> Serial Server	New source NAT:				
> System	Name	Source zone Destination zone	To source IP To source port		
Logout	New SNAT rule	lan 🗸 wan 🗸	Please cht 🗸 Do not rewrite	Add and edit	
		Αρήγ	Save		
		JiNan Usr IOT Technology Limited http://ww	ww.pusr.com/		

Pic 64 NAT Settings 3

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



过滤:	ip.addr == 1	92.168.13.4		▼ 表达式	清除	应用			
No.	Time	Source	Destination	Protocol	Info				
	1 0.000000	192. 168. 13. 4	220. 195. 22. 209	TCP	50379 > 1	ttp [FIN,]	ACK] Seq=1 Ac	k=1 Win=64708 Len=0	
	2 0. 689352	192.168.9.1	192. 168. 13. 4	ICMP	Echo (pin	ng) request	(id=0x1d3c,	seq(be/le)=57/14592,	ttl=64)
	3 0. 689426	192. 168. 13. 4	192. 168. 9. 1	ICMP	Echo (pin	ng) reply	(id=0x1d3c,	seq(be/le)=57/14592,	ttl=128)
	6 1.689615	192. 168. 9. 1	192. 168. 13. 4	ICMP	Echo (pin	ng) request	(id=0x1d3c,	seq(be/le)=58/14848,	ttl=64)
	7 1.689687	192. 168. 13. 4	192. 168. 9. 1	ICMP	Echo (pin	ng) reply	(id=0x1d3c,	seq(be/le)=58/14848,	ttl=128)
	8 1.823459	192. 160. 18. 4	192. 168. 4. 68	53/02	Create R	quest File			
	9 1.825746	192. 168. 4. 63	192. 168. 13. 4	SMB2	Create Re	sponse File	e:		
1	0 1 826091	192 168 13 4	192 168 4 63	CUR2	Create P.	muest File			

Pic 65 NAT test and verify

5.3.3. DNAT

Exit target address translation.





Name	describe	Default Parameters
Enable	Enable	Enable
	Disable: 🔞 Disable	Disable
Name	Customize the name of this rule	Empty
Source area	Data entry area selection	WAN
Source MAC address	Source MAC address filtering at entry	All
Source IP address	Source IP address screening at entry	All
Source port	Source port filtering at entry	All
External IP address	Target IP address at the time of entry	All
External port	Target port at entry	Empty
Interior zone	Redirection to the outbound area	LAN
An internal IP address	Target address when redirecting out of the station	Empty
Internal ports	Redirect the outgoing port to the target port	Empty
Enable NAT loopback	Check to enable NAT loopback	Check

DNAT parameter list

5.3.4. Port forwarding

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

USR IOT Communication Expert of Industrie	al lot			Be Honest, Do Best! English 493
USR-G806p	Firewall - Port F	orwards		
> Status	Port forwarding allo	ws remote computers on the Internet to connect to a specific compute	er or service within the private LAN.	
> Services	Port Forwards			
> Network	Name	Match Rules	Forwarding To	Enable Sort
> VPN				
✓ Firewall		This section contain:	s no values yet	
General Settings				
Port Forwards	New Port Forwarding	Rules:		
Traffic Rules	Name	Protocol External External port zone	Internal Internal IP Internal port zone address	
Custom Rules Access Restrictions	test	TCP+UDP v wan v 81	lan ✔ 192.168.2.1 ✔ 80	bbA 😭
> Serial Server				
> System			Save	
> Logout		Apply	Dave	
		JiNan Usr IOT Technology Limited http://www.p	pusr.com/	
C		Die 66 Deut Cettinge nage		

Pic 66 Port Settings page 1

- > After setting the forwarding rule, you need to click the add button on the right, and then this rule will be displayed in the rule column;
- > Then click the "Apply" button in the lower right corner to make the Settings effective;
- The following Settings: 192.168.2.1:80 is the router's own web server. If we want to access a device in the LAN from the Internet, we need to set up the mapping from the Internet to the LAN, such as setting the



Internet port to 81, the internal IP address to 192.168.2.1, and the internal port to 80;

> When we access port 81 from the WAN port, the access request will be redirected to 192.168.2.1:80.

Communication Expert of Indust	rial IOT			Bel	Honest, Do Best! English 493
USR-G806p > Status > Services			to a specific computer or service within the private LA	N	
 Network VPN Firewall General Settings Port Forwards 	Name test	Match Rules IPv4-TCP, UDP From any host in wan Via any nouter IP at port 81	Forwarding To IP 192.168.2.1, port 80 in <i>Ian</i>	Enable Sort	lete
Traffic Rules Custom Rules Access Restrictions > Serial Server > System > Logout	New Port Forwa	Protocol Exte		Internal port	
		JiNan Usr IOT Technology Limited	i http://www.pusr.com/		

Pic 67 Port Settings page 2

Tab 20	Port forwarding parameter table
--------	---------------------------------

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

5.3.5. NAT DMZ

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



USR IOT Communication Expert of Industr	alor.	Be Honest,	Do Best! English 中文
USR-G806p Status Services	Firewall - Port Forwards Port forwards Port Forwards Port Forwards		
> Network > VPN Firewall General Settings	Name Match Rules Forwarding To Enable Sort IPv4-TCP UDP	Edit 🗷 Delete	
Port Forwards Traffic Rules Custom Rules Access Restrictions > Serial Server	New Port Forwarding Rules: Name Protocol External External port Internal Internal IP Internal port New port forward TCP+UDP wan Ian Image: Compare the second sec	Add	
> System > Logout	Apply Save empty		
	IINan Usr IOT Technology Limited http://www.nusr.com/		

Pic 68 DMZ Settings 1

USR IOT Communication Expert of Industrial IOT				Be H	onest, Do Bes _{English f}
USR-G806p	Firewall - Port Forwa	ards			
> Status		mote computers on the Internet to connect to	a specific computer or service within the private LA	N.	
Services Network	Port Forwards Name	Match Rules	Forwarding To	Enable Sort	
> VPN Y Firewall	test	IPv4-TCP, UDP From any host in wan Via any router IP at port 81	IP 192.168.2.1, port 80 in Ian	🛛 🔹 🔹 🧟 Edit 🗷 Deleta	
General Settings Port Forwards Traffic Rules	New Port Forwarding Rule				
Custom Rules Access Restrictions	Name	Protocol Externa zone	I External port Internal Internal IP zone address	Internal port	
Serial Server	New port forward	TCP+UDP 🗸 wan 🗙	lan 🗸	► Add	
> System > Logout			Apply Save		
		JiNan Usr IOT Technology Limited	http://www.pusr.com/		
	Die	69 DMZ Setting	- 7		

Pic 69 DMZ Settings 2

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

< pay attention to >

> Port mapping and DMZ functions cannot be used simultaneously.

5.4. Access restrictions

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



5.4.1. Domain blacklists

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

Communication Expert of Industrial IOT	Be Hones	st, Do Best! English 中文
USR-G806p Status Services Network VPN Firewall General Settings Port Forwards Traffic Rules Custom Rules Access Restrictions Serial Server System Logout	Access Restrictions There 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 restriction: Configurations Method Black List Lest Domain Name Eable Name Domain Name Name Domain Name Exer Firewall Rule: Image: State of the access fails, please of the acc	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 70 Domain blacklists

5.4.2. Domain name whitelist

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



Communication Expert of Indust		est, Do Best! English∣‡文
USR-G806p > Status > Services > Network	Access Restrictions 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. Configurations	
VPN V Firewall General Settings Port Forwards Traffic Rules Custom Rules	Method White List Name Enable test baldu.com I	
Access Restrictions Serial Server System Logout	New Firewall Rule: Name Domain Name Fiew rule Add	
	Apply Save JiNan Usr 10T Technology Limited http://www.pusr.com/	

Pic 71 Domain name whitelist

6. Service function

6.1. Dynamic domain name resolution (DDNS)

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

6.1.1. Supported services

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



Communication Expert of Indu	urial IOT	Be Honest, Do Best! _{Englich 492}
USR-G806p > Status ~ Services	Dynamic DNS Dynamic DNS configuration Configuration	n allows access to a fixed domain for the host, but the corresponding IP may be dynamic.
USR Cloud DDNS SSH Port SNMPD	Enable Event interface	wan_wired Ketwork on which the ddm-updater scripts will be started
GNSS SMS > Network	Service Username	Service provider username
> VPN > Firewall	Password Domain Name	
 Serial Server System Logout 	Sync Time Forced Update Time	300 @ Unit s, 80-85535 86400 @ Unit s, 80-86400
		Apply Save JINan Usr IOT Technology Limited http://www.pusr.com/

Pic 72 DDNS Settings page

Parameter filling requirements are as follows:

Tab 21	DDNS	parameter list
--------	------	----------------

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

6.1.2. DDNS come into force

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

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



C:\Users\Administrator> C:\Users\Administrator>ping fe26203015.zicp.vip
正在 Ping fe26203015.zicp.vip [6 38] 具有 32 字节的数据: 来自 60 38 的回复: 字节=32 时间<1ms TTL=127 来自 60 38 的回复: 字节=32 时间<1ms TTL=127 来自 60 38 的回复: 字节=32 时间<1ms TTL=127 来自 60 38 的回复: 字节=32 时间<1ms TTL=127
9 6()的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = Oms, 最长 = Oms, 平均 = Oms

Pic 73 DDNS test Figure 3

6.1.3. functional characteristics

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

6.2. SSH Port

Enable or disable SSH to manage the router.

USR IOT Communication Expert of Indust	mailor Be Honest, Do Best! mailor
USR-G806p Status Services USR Cloud DONS SSH Port SNMPD GNSS SMS Network VPN Firewall Serial Server System Logout	SSH Access Dropbear firstance Enable port 2222
	JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 74 SSH



6.3. SMS

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

USR IOT Communication Expert of Indust	rial IOT			Be Hon	nest, Do Best! _{English †文}
USR-G806p	Short Message Service	•			î
> Status	SMS AT Enable				
✓ Services	SMS AT Enable	Once selected, the SMS AT function is e	nabled		
USR Cloud	SMS Send				
DDNS SSH Port	Receiver Number				
SNMPD	Content	The phone number must be 1 to 20 digits	ong, optionally starting with a '+' sign to indicate an international number.		
GNSS	Content				
SMS		Please enter your information in this box, Y	ou can input up to 70 characters.		
> Network		Send			
> VPN > Firewall	SMS Receiving Record				
> Serial Server	Sender Number	Time	Content		
> System					
> Logout	SMS Sending Record	Time	Content	Status	
					-
		JiNan Usr IOT Technology Limited	http://www.pusr.com/		

Pic 75 SMS

Tab 22	configuration parameter
--------	-------------------------

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

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





Pic 76 SMS AT

6.4. SNMPD

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

						<u> </u>
Communication Expert of Industrie	нот.			E	3e Honest, D)o Best! English∣#文
USR-G806p	SNMPD Configuration SNMPD is a master daemon/	agent for SNMP, from the net-snmp projec	ct.			Î
> Status						
✓ Services	Enable SNMP					
USR Cloud	Enable SNMP					
DDNS						
SSH Port						
SNMPD	User Info (use for snmp	v3)				
GNSS	username	user				
SMS						
> Network	auth type	auth 🗸				
> VPN	auth mode	SHA 🗸				
> Firewall	auth passwd					
> Serial Server						
> System						
> Logout	System Info					
	sysLocation	JiNan				
	Systocaton					
	sysContact	www.usr.cn				
	sysName	Smart_Router				
		JiNan Usr IOT Technology Limited	http://www.pusr.com/			

Pic 77 SNMP service Settings interface

Tab 23 SNMP parameter list

function	content	Windows default
SNMP switc	h Check to enable SNMP services	Not selected
configuration		
user name	The name assigned to SNMP users	user


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

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

Tab 24 SNMP OID list

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

6.5. GNSS

Supports GPS positioning data reporting to private platforms.



7. Serial port server function

G806p has RS232/RS485, supports TCP, UDP, MODBUS, MQTT, HTTPD and other network protocols, and supports heartbeat packets, registration packets and AT features.

name	functional description	Windows default
Baud rate	Set the baud rate of RS232 or RS485. You can set:	115200
	1200/2400/4800/9600/19200/38400/57600/115200/230400	
	Note: Only RS485 supports 230400	
data bit	Set the data bit of RS232 or RS485. You can set it to 7/8	8
stop bit	The stop bit of RS232 or RS485 can be set to 1/2	1
check bit	The parity bit of RS232 or RS485 can be set to NONE/ODD/EVEN	NONE
Packaging	Set the data packing time for RS232 or RS485	50
time	Unit: ms (range: 10-60000ms)	
Pack length	Set the data packing length of RS232 or RS485	1000
	Unit: bytes (range: 5-1500 bytes)	

7.1. Serial port Settings

In this interface, you can set the baud rate, data bits and other parameters of the serial port.

Communication Expert of Industr	ial IOT						Be Ho	nest, Do Best! _{English 中文}
USR-G806p	Serial Port Se Serial port basic		me can be set in the ra	nge of 0-1000 ms (i) indicates automatic pa	ckaging), package length can be s	set in the range of 5-1460 bytes.	
ServicesNetwork	Basic Configu Name	ration Baud Rate	Data Bits	Stop Bits	Pairty	Packaging Interval	Packaging Length	
> VPN > Firewall > Serial Server	COM1-485 COM2-232	115200 V			NONE V		1000	
Serial Port Settings Communication		prevention Configu			,			
Advanced Settings > System > Logout	485 collision p	orevention OFF	~					
				1	Apply			
		JiNan Usr	IOT Technology Lir	nited http:/,	'www.pusr.com/			

Pic 78 Serial port setting interface

Tab 25	Serial port setting parameter table
--------	-------------------------------------

name	functional description	Windows 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 bit	Set the data bit of RS232 or RS485 to 7/8	8



stop bit	The stop bit of RS232 or RS485 can be set to 1/2	1
check bit	The parity bit of RS232 or RS485 can be set to NONE/ODD/EVEN	NONE
Packaging	Set the data packing time for RS232 or RS485	50
time	Unit: ms (range: 10-60000ms)	
Pack length	Set the data packing length of RS232 or RS485	1000
	Unit: bytes (range: 5-1500 bytes)	

7.1.1. Time-triggered mode

When the G806p receives data from the UART, it continuously checks the interval between adjacent bytes. If the interval is greater than or equal to a specific 'time threshold,' the frame is considered complete. Otherwise, it continues to receive data until the total length reaches or exceeds the packet size (default is 1000 bytes). The frame is then sent to the network as a single packet. The 'time threshold' is the interval between packets, which can be set from 10ms to 60000ms. The default setting is 50ms.



Pic 79 Time-triggered mode

7.1.2. Length-triggered mode

When the 806p receives data from the UART, it continuously checks the number of bytes received. If the number of received bytes reaches a certain 'length threshold,' the frame is considered to have ended. The frame data is then sent as a TCP or UDP packet to the network. The 'length threshold' refers to the packet size, which can be set between 5 and 1500 bytes. The default setting is 1000 bytes.



Pic 80 Length-triggered mode

7.2. Communication configuration

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



Communication Expert of Industri	ial KOT						Be Hone	est, Do Best! _{English ⊕文}
USR-G806p		inication configuration						
StatusServices	Commu	nication configuration						
> Network > VPN	Nar	me Protocol	Enable	Description				
 Firewall Serial Server 	TCPO	C_1 TCPC	ON	TCPC_1		Edit Delete		
Serial Port Settings	New Chann							
Communication Advanced Settings	N	Name	Protocol TCPC V	Enable	Description Description	Add and edit		
> System > Logout				Apply				
				Арруу				
		JiNan Usr IC)T Technology Limited	http://www.pusr.com	I			

Pic 81 Communication configuration

name	functional description	Windows default
name	Set the name of this link	empty
protocol	You can select the following network protocol:	ТСРС
	TCPC/TCPS/UDPC/UDPS/HTTPD/MQTT/AWS/ALI	
start using	Whether this link is enabled, ON (enabled)/OFF (disabled)	start using
description	Set the remarks for this link	empty

 Tab 26
 Communication configuration parameter table

explain :

- > Follow up with different protocol choices, and the "add and edit" interface will vary accordingly;
- > Up to six links can be set.

7.2.1. MQTT pattern

The device supports the MQTT Client function, allowing users to easily connect to their own private MQTT server through simple configuration. Both data publishing and subscription support multi-topic configurations, enabling users to send serial port data to a specific topic or direct the server's pushed data to a bound serial port, thus achieving seamless data transmission between the serial port and the server.



7.2.1.1. MQTT basic configuration

Communication Expert of Industrial IOT		Be Honest, Do Best! ™gitah∣#%
USR-G806p Configuration		
Enable	on 🗸	
> Status Name	112	
> Services Description	MQTT_1	
Network MQTT Vsesion VPN	V3.1.1 🗸	
VPN Firewall Server Address	cloudmqtt.usr.cn	
Server Port	1883	
Serial Port Settings Client ID	01303125040800004300	
Communication Heartbeat Interval Advanced Settings	30 © 0-6000 Seconds	
System Reconnect Walting Logout Interval(s)	5 (a) range: 1-3600	I
Authentication	OFF 🗸	
MQTT Will	off 🗸	
Clean Session	OFF 🗸	
TLS	OFF 🗸	
Offline Data Cache	OFF 🗸	

Pic 82 MQTT configuration interface

Tab 27 MQTT parameter list

name	functional description	Windows default
start using	Whether this link is enabled, ON (enabled) / OFF (disabled)	ON
name	The name of the link	MQTT_X
description	This link notes information	MQTT_X
MQTT edition	You can choose: MQTTV3.1.1/V3.1 version	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
The heartbeat	MQTT protocol heartbeat time, unit: seconds	30
packet time		
Redundancy	The interval between the next reconnection after MQTT	5
detection interval	disconnection. Unit: seconds	
attestation	If the server needs user name and password authentication, it	OFF
	needs to be enabled	
	ON: Enable MQTT user name and password authentication	
	OFF: Disable MQTT user name and password authentication	
words of the	MQTT connection flag, when the network is abnormal and	OFF
deceased	disconnected, the server will publish this will message to other	
	clients who subscribe to this will topic.	
	ON: Enable subscription to the will topic	
	OFF: Turn off the subscription to the will topic	
theme	Testament topic	empty
The contents of	Set the contents of your will	empty



the will		
QOS	QOS Settings can be set for:	0
	0 at most	
	1 At least once	
	2. Get it right the first time	
Keep the	Whether to enable the legacy message retention function	OFF
message	ON: open	
	OFF: close	
Clean up the	MQTT protocol connection flag, used to control the session state	OFF
conversation	lifetime, OFF is off, ON is on	
TLS	The version number can be selected as TLS1.0 or TLS1.2	OFF
	You can choose to verify the certificate, verify the server	
	certificate, and verify the certificate in both directions	
TLS	No certificate verification: that is, only the data layer	Do not verify the
authentication	transmission decryption is implemented, and the identity of the	certificate
method	other party is not checked during the handshake process	
	Verify server certificate: that is, the client verifies the server	
	certificate during the handshake. The client needs to preset the	
	root certificate of the server	
	Two-way authentication: that is, the client and server check	
	each other's identity, which requires the pre-set server root	
	certificate, client certificate and client private key	
Offline data	Data overflow processing mode selection, cache mode, cache	OFF
cache	length setting, etc	

7.2.1.2. Theme subscription/publish

The topic addition feature is primarily used to add topics for publication or subscription. Configuration parameters include the topic name, TOPIC, QOS, and whether to retain messages. The serial port association function links a topic to a specific serial port. When publishing, the original data from the serial port serves as the Payload of the topic. When receiving subscription messages, the Payload of the subscribed topic is sent to the serial port as the original data.



						Be H
on OFF	~					
ill OFF	~					
on OFF	~					
S OFF	~					
e OFF	~					
						_
Name	Торіс	Qos	KeepMsg	сом	Description	
		This section con	tains no values yet			
, т	Горіс	Qos	KeepMsg	COM	Description	
Торіс		0 At most or 🗸	on 🗸	COM1-485 🗸	Description	첩 Add
			Apply Sa	ave		
	II OFF I OFF OFF OFF OFF Name	II OFF · · · · · · · · · · · · · · · · · ·	II OFF · · · · · · · · · · · · · · · · · ·	II OFF OFF OFF OFF OFF OFF OFF OF	III OFF IV INAME Topic Qos KeepMsg COM IV This section contains no values yet IV IV IV IV Topic Qos KeepMsg COM	III OFF III OFF IIII OFF IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

Pic 83 MQTT topic configuration interface

name	functional description	Windows default
type	Theme type: Publish/subscribe is optional	publish
name	The name of the topic	empty
theme	Theme: Theme content	empty
Qos	The quality of the topic message can be set:	0
	0 At most once	
	1 At least once	
	2. Get it right the first time	
Keep the	Set whether to retain messages, ON (retain) / OFF (do not retain)	ON
message		
channel	COM1-485: Use the 485 channel for data communication	COM1-485
	COM2-232: Use channel 232 for data communication	
	COM1+COM2: Use RS232 or RS485 channels to transmit data	
description	Set the remarks information for this topic rule	empty

explain :

> You can set up a maximum of 16 theme rules.

7.2.2. Connect to the Amazon platform

In this mode, the user terminal can send request data to the AWS platform via this device. Data publishing and subscription to the AWS platform can be configured for multiple topics. Users can configure the serial port data to be sent to a specific topic or direct the server-pushed data to the bound serial port, enabling seamless data transmission between the serial port and the server.



Communication Expert of Industr	MIOT			Be Honest, Do	Bes inglish f
USR-G806p	AWS - Communication	n configuration			
> Status	Communication configuration	'n			
> Services	Configuration				
> Network > VPN	Enable	on 🗸			
> VPN	Name	AWS_1			
✓ Serial Server	Description	AWS_1			
Serial Port Settings	Server Address	amazonaws.com.cn			
Communication	Server Port	8883			
Advanced Settings	Client ID	01303125040800004300			
> Logout		30			
	Reconnect Detection Interval(s)	5			
	Clean Session	OFF V			



Tab 29 AWS parameter list

name	functional description	Windows default
start using	Whether the link is enabled, ON (enabled) / OFF (disabled)	ON
name	The name of the AWS platform link	AWS_2
description	AWS platform link remarks	AWS_2
Server address	AWS platform MQTT service server connection address: IP or	amazonaws.com.cn
	domain name	
Server port	AWS platform MQTT server port	1883
client ID	The AWS platform MQTT client identifier	123456
The heartbeat packet time	MQTT protocol heartbeat time, unit: seconds	30
Redundancy	The interval between the next reconnection after MQTT	5
detection interval	disconnection. Unit: seconds	
Clean up the	MQTT protocol connection flag, used to control the session state	OFF
conversation	lifetime, OFF is off, ON is on	
Server root	Select the corresponding file	not have
certificate		
Device signature	Select the corresponding file	not have
certificate		
Device private	Select the corresponding file	not have
key		
Offline data	Data overflow processing mode selection, cache mode, cache	OFF
cache	length setting, etc	



7.2.2.1. Theme subscription/publish

The topic add function is mainly used to add the topic for publishing or subscribing. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages. The serial port association is used to associate a topic with a serial port. Up to 16 topic rules can be set.

7.2.3. Connect to Ali Cloud platform

The Alibaba Cloud IoT Platform is a highly popular public cloud platform. It supports the MQTT protocol for device access, offering both industrial and enterprise instances. The platform supports SSL functions, enabling unencrypted, one-way, and two-way authentication connections to Alibaba Cloud. In this mode, data can be published and subscribed to terminal devices through the Alibaba Cloud platform, supporting multi-topic configuration. Users can configure serial port data to be sent to specific topics or direct server-pushed data to the bound serial ports, facilitating seamless data transmission between the serial port and the server.

USR IOT Communication Expert of Indust	nial KOT					Ве Но	nest, Do Best! _{English 中文}
USR-G806p	ALI - Communication	configuration					
> Status	Communication configuration	n					
> Services	Configuration						
> Network	Enable	ON	~				
> VPN > Firewall	Name	ALI_1					
 Firewall Serial Server 	Description	ALI_1					
Serial Port Settings	Instance Type	Public Instance	~				
Communication	ProductKey	can't be empty					
Advanced Settings System	deviceName	can't be empty					
> Logout	deviceSecret	can't be empty					
	Client ID	can't be empty					
	Region ID	Shang Hai	~				
	Server Port	1883					
	Heartbeat Interval	300 30-1200 Seconds					
	Reconnect Detection Interval(s)	5 i range: 1-3600					
		JiNan Usr IOT Technolog	ogy Limited	http://www.pusr.	.com/		

Pic 85 ALI configuration interface

Tab 30 ALI parameter list

name	functional description	Windows default
start using	Whether the link is enabled, ON (enabled) / OFF (disabled)	ON
name	The name of the ALI platform link	ALI_2
description	ALI platform link remarks	ALI_2
Instance type	Supports Ali Cloud public instances and enterprise instances	Public instance
ProductKey	Device attributes, the triplet ProductKey is added to the device in	not have
	Ali Cloud	
deviceName	Device name, the DeviceName in the triplet added to Aliyun	not have
	devices	
deviceSecret	eviceSecret Device key, the triplet DeviceSecre added to the device in Ali	
	Cloud	



client IDSupports custom customer ID for MQTT client concatenationnot haveregionThe regional code of Ali Cloud, such as East China 2 (Shanghai) is filled in: cn-shanghaiEast China 2-ShanghaiServer portALI platform MQTT server port1883The heartbeat packet timeMQTT protocol heartbeat time, unit: seconds disconnected, unit: seconds300Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsDo not verify the certificateTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOffline cacheData overflow processing mode selection, cache mode, cache length setting, etcOFF			
Image: Server portALI platform MQTT server port1883Server portALI platform MQTT server port1883The heartbeat packet timeMQTT protocol heartbeat time, unit: seconds300Redundancy detection intervalThe interval between the next reconnection after MQTT is disconnected, unit: seconds5Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLS authentication methodNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF	client ID	Supports custom customer ID for MQTT client concatenation	not have
Server portALI platform MQTT server port1883The heartbeat packet timeMQTT protocol heartbeat time, unit: seconds300RedundancyThe interval between the next reconnection after MQTT is disconnected, unit: seconds5Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF	region	The regional code of Ali Cloud, such as East China 2 (Shanghai),	East China 2-Shanghai
The heartbeat packet timeMQTT protocol heartbeat time, unit: seconds300Redundancy detection intervalThe interval between the next reconnection after MQTT is disconnected, unit: seconds5Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsDo not verify the certificateTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate is that is, the client verifies the server certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF		is filled in: cn-shanghai	
packet timeIndependent of the interval between the next reconnection after MQTT is disconnected, unit: seconds5Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedata overflow processing mode selection, cache mode, cacheOFF	Server port	ALI platform MQTT server port	1883
Redundancy detection intervalThe interval between the next reconnection after MQTT is disconnected, unit: seconds5Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate of the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, cand verifoate and client private keyOFF	The heartbeat	MQTT protocol heartbeat time, unit: seconds	300
detection intervaldisconnected, unit: secondsOFFClean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedata overflow processing mode selection, cache mode, cacheOFF	packet time		
Clean up the conversationMQTT protocol connection flag, used to control the session state lifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer other party is not checked during the handshake process Verify server certificate in both directionsDo not verify the certificate during the handshake. The client verifies the server certificate during the handshake. The client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedata overflow processing mode selection, cache mode, cacheOFF	Redundancy	The interval between the next reconnection after MQTT is	5
conversationlifetime, OFF is off, ON is onOFFTLSThe version number can be selected as TLS1.0 or TLS1.2 You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsOFFTLSNo certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF	detection interval	disconnected, unit: seconds	
TLSThe version number can be selected as TLS1.0 or TLS1.2OFFYou can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsDo not verifyTLSNo certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF	Clean up the	MQTT protocol connection flag, used to control the session state	OFF
You can choose to verify the certificate, verify the server certificate, and verify the certificate in both directionsDo not verify the certificateTLS authentication methodNo certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFF	conversation	lifetime, OFF is off, ON is on	
certificate, and verify the certificate in both directionsDo not verify theTLSNo certificate verification: that is, only the data layer transmission decryption is implemented, and the identity of the other party is not checked during the handshake process Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFF	TLS	The version number can be selected as TLS1.0 or TLS1.2	OFF
TLSNo certificate verification: that is, only the data layerDo not verify theauthenticationtransmission decryption is implemented, and the identity of thecertificatemethodother party is not checked during the handshake processverify server certificate: that is, the client verifies the serverVerify server certificate: that is, the client needs to preset the root certificate of the serververify server certificate of the serverTwo-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOFF		You can choose to verify the certificate, verify the server	
authenticationtransmission decryption is implemented, and the identity of the other party is not checked during the handshake processcertificateWerify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the servereach other's identity. It requires the pre-set server root certificate, client certificate and client private keyoFFOfflinedataData overflow processing mode selection, cache mode, cacheOFF		certificate, and verify the certificate in both directions	
methodother party is not checked during the handshake processVerify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOfflinedataData overflow processing mode selection, cache mode, cacheOFF	TLS	No certificate verification: that is, only the data layer	Do not verify the
Verify server certificate: that is, the client verifies the server certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOfflinedataData overflow processing mode selection, cache mode, cacheOFF	authentication	transmission decryption is implemented, and the identity of the	certificate
certificate during the handshake. The client needs to preset the root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private keyOfflineOfflinedataData overflow processing mode selection, cache mode, cacheOFF	method	other party is not checked during the handshake process	
root certificate of the server Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private key<		Verify server certificate: that is, the client verifies the server	
Two-way authentication: that is, the client and server check each other's identity. It requires the pre-set server root certificate, client certificate and client private key Offline data Data overflow processing mode selection, cache mode, cache OFF		certificate during the handshake. The client needs to preset the	
each other's identity. It requires the pre-set server root certificate, client certificate and client private key Each other's identity. It requires the pre-set server root certificate, client certificate and client private key Offline data Data overflow processing mode selection, cache mode, cache OFF		root certificate of the server	
Offline data Data overflow processing mode selection, cache mode, cache OFF		Two-way authentication: that is, the client and server check	
Offline data Data overflow processing mode selection, cache mode, cache OFF		each other's identity. It requires the pre-set server root	
		certificate, client certificate and client private key	
cache length setting, etc	Offline data	Data overflow processing mode selection, cache mode, cache	OFF
	cache	length setting, etc	

7.2.3.1. Theme subscription/publish

The topic add function is mainly used to add the topic for publishing or subscribing. The configuration parameters include basic parameters such as name, TOPIC, QOS, and whether to retain messages. The serial port association is used to associate the topic with a certain serial port. A maximum of 16 topic rules can be set.

7.2.4. HTTPD mode (HTTP Client mode)

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 port device.

Users do not need to pay attention to the data conversion process between serial port data and network packets. They can realize the data request from serial port device to HTTP server through simple parameter setting.

The device filters the received data by default and only outputs the user data to the serial port. The customer can use the AT command to select whether to filter the HTTPD data.



Communication Expert of Industrial KOT	Be	Honest, Do Best! English 493
Communication configur	ication configuration	Î
Status Services Configuration		- 1
	ble ON 🗸	
> VPN Nam	me HTTPD_1	
Cricevan Descriptio Serial Server	ion HTTPD_1	
Serial Port Settings Request Metho		
Communication Remove Heade Advanced Settings		
System Server Addres	IRL /1.php[3F]	
Logout Remote Por		
Timeou		
	1-3600 Seconds	I
Httpd Heade		
bin	IS OFF	
i.		Ŧ

Pic 86 HTTPD configuration interface

Tab 31 HTTPD parameter list

name	functional description	Windows default
start using	Whether this link channel is enabled: ON (enabled) / OFF	ON
	(disabled)	
name	The name of the link	HTTPD_X
description	Add remarks to this link	HTTPD_X
Request method	The way to request data from an HTTP server	GET
	GET/POST	
Clean the filter	Set whether to filter HTTP header	ON
head	ON (filter) / OFF (no filter)	
HTTP URL	Add the URL you want to access	/1.php[3F]
Server address	HTTP server address, which can be filled with IP or domain	empty
	name	
Remote port	HTTP server port number	empty
overtime	If the server does not actively disconnect the connection	10
	within the timeout time, this end needs to wait for the	
	disconnection time, unit: seconds	
Request header	HTTP header information	Accept:text/html[0D][0A]
information		
Channel binding	COM1-485: Use the 485 channel for data communication	COM1-485
	COM2-232: Use channel 232 for data communication	
	COM1+COM2: Use RS232 or RS485 channels to transmit	
	data	
TLS encryption	Supports TLS1.0\TLS1.2\OFF	OFF



7.2.5. Registration packet/handshake packet function

7.2.5.1. Registration package description

Registration packet: This is used to enable the server to identify the data source device or as a password for obtaining server function authorization. The registration packet can be sent when the device connects to the server, or it can be appended to the beginning of each data packet as part of the data packet. The data in the registration packet can be either a MAC address or custom registration data.

explain :

- > If MAC is selected, the WAN port MAC is used as the content of the registration packet;
- > This function is available only when the link is set to tcpc or udpc mode.

7.2.5.2. Network heartbeat packet description

Network heartbeat packet: sent to the network end, 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.

explain :

> This function is available only when the link is set to tcpc or udpc mode.

7.3. advanced setup

You can configure network AT, serial port heartbeat packets, and no data action conditions.

Communication Expert of Industrial IOT	Be Honest, D	Oo Best! English 中文
USR-G806p	Advanced configuration	Î
> Status	Advanced configuration	
> Services > Network	Transparent AT Configuration Network and serial port transparent AT function, can directly perform AT command operation during data transparent transmission, without the need to configure, where the network AT command is applicable to TCP/CTPS/UDP/CUDP's mode.	
> VPN	Transparent AT Instruction ON	
 Firewall Serial Server 	AT Data Header atnetcmd#	
Serial Port Settings		
Communication Advanced Settings	Serial Heart Configuration If no channel is bound to the serial port, the serial port heartbeat function will not take effect.	
> System > Logout	Serial Heart OFF V	
	No Data Configuration	
	Network Reconnect OFF Without Data Reconnect network channel, Works in non-HTIPD mode.	
	Network Restarting OFF V Without Data Reboot device, Works in non-HTTPD mode.	
	Serial Restarting Without OFF V	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 87 Advanced configuration interface

Tab 32 Advanced configuration interface parameter table

name	functional description	Windows default
Network AT command	ON (enable)/OFF (disable)	ON
Network AT password	The password for the network AT	atnetcmd#



word		
Serial port heartbeat	ON: Enable the function of sending heartbeat	OFF
	packets to serial port	
	OFF: Disable the function of sending heartbeat	
	packets to serial port	
Pacemaker types	HEX: 16-bit type	HEX
	ASCII: Character type	
	The explanation of the heartbeat packet is shown in	
	Chapter 8.2.7.2	
Pacemaker data	Heartbeat packet data content	empty
The heartbeat packet	The time interval at which the heartbeat packet is	60
time	sent, in seconds	
Serial port binding	COM1-485: Use the 485 channel for data	COM1+COM2
	communication	
	COM2-232: Use channel 232 for data	
	communication	
	COM1+COM2: Use RS232 or RS485 channels to	
	transmit data	
The network channel	If no data is received from the network end within	OFF
does not enable data	the setting time, the channel triggers reconnection	
reconnection	It is applicable to non-HTTP protocols. See the	
	following description for details	
Redundancy detection	Set the time interval, unit (seconds)	3600
interval		
The network channel is	If no data is received from the network end within	OFF
not enabled for data	the setting time, all channels will trigger the device	
restart	to restart	
	It is applicable to non-HTTP protocols. See the	
	following description for details	
Restart the detection	Set the time interval, unit (seconds)	36000
interval		
Serial port data restart	The configuration serial port channel does not	OFF
enabled	receive the serial port data, and triggers the DTU to	
	restart	
	If two serial ports are configured, the DTU will be	
	restarted if no serial port data is received within the	
	time of one channel	
Enable serial port	COM1-485/COM2-232/COM1+COM2	COM1-485

explain :

Serial heartbeat packet: This function is only available if there is a link channel (at least one communication configuration);

> No data reconnection of the network channel: TCPC/UDPC/MQTT. If no time is received from the network end



within the set time, the link will be reconnected;

- No data reconnection of network channel: TCPS, if the client does not receive data within the set time, it will kick out the corresponding client;
- > No data reconnection of the network channel: UDPS, if the client data is not received at the set time, the serial port data will not be sent to UDPC;
- Network channel no data restart: all link channels will restart when the set time is reached and no network data is received;
- Network channel restart without data: if the TCPC connection success data is received within the set time, the count is reset;
- > Serial port channel restart without data: if the serial port data is not received at the set time, DTU restarts;

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

8. system function

8.1. host name

The default hostname is USR-G806p.

USR IOT Communication Expert of Indus	Be Hon	est, Do Best! Englikh∣#文
USR-G806p Status Services Network VPN Firewall Serial Server System Administration Reboot Timer NTP Http Port Syslog Backup/Upgrade Reboot Logout	System Here you can configure the basic aspects of your device like its hostname or the timezone. System Properties Cenveral Setting: Design Hostname: USR-GB08p Carpety: Save	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 88 host name



8.2. Time Settings

Communication Expert of Industrial IOT	Be Honest, Do Best! Auto REFRESH ON: English 4-%
Status Services Time Parameter Network Current System Time VPN Firewall Serial Server	a section is used to configure general router time settings, like selecting the local time zone, synchronizing the time and NTP. e 2025-06-27 15:24:43 Fri Sync with browser e Asia/Beijing v
System Time Synchronizatio System	
Administration Enable NTP Clier	t 🖾
Reboot Timer NTP Serve	r D
NTP Alternate NTP Server Http Port Syslog Backup/Upgrade Reboot	r ntp1.aliyun.com a time1.doud.tencent.com a time.ustc.edu.cn a cn.pool.ntp.org a
JiNa	n Usr IOT Technology Limited http://www.pusr.com/



< pay attention to >

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

USR IOT Communication Expert of Industrial IOT	Be Hon	est, Do Best! English 中文
USR-G806p Status Services Network VPN Firewall Serial Server System Administration Reboot Timer NTP Http Port Syslog Backup/Upgrade Reboot	Router Password Changes the administrator password for accessing the device Configuration Password Image: Configuration Image: Configuration Image: Configuration Confirmation Image: Confirmation Image: Confirmation Image: Confirmation Image: Confirmation Image: Confirmation	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 90 Username and password setup page

< pay attention to >

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



8.4. HTTP port

Set the port number of the web	login page and	d on able or disable	the TELNET function
Set the polt number of the web	login paye, and	u enable of ulsable	THE TELINET TUTICUOT.

USR IOT Communication Expert of Industrial IOT		Be Honest, Do Best! English #rx
USR-G806p Status Services Network VPN Firewall Service	HTTP Port Here you can configure the HTTP port number, effective immediately Web server Http Port 80 Image: On the port in use	
System System Administration Reboot Timer NTP Http Port Syslog Backup/Upgrade	Telnet Access Telnet Instance Enable Image: Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2">Colspan="2"	
Reboot	Apply JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 91 HTTP port

8.5. Parameter backup and upload

Communication Expert of Industrial IOT	Be Honest, Do Best English 492
USR-G806p Status Services Network VPN Firewall Serial Server System Administration	Backup / Flash Firmware Backup / Restore Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset". Download backup: ⓐ Generate archive Reset to defaults: @ Perform To restore configuration files, you can upload a previously generated backup archive here. @ Reset to legachts: Restore backup: Pease select file @ Browse
Reboot Timer NTP Http Port Syslog Backup/Upgrade Reboot	Flash new firmware image Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration. Keep settings: Image: Please select file Browse Flash image
	JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 92 Parameter backup upload page

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

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



Parameter backup: Click the "Download Backup" button to backup the current parameter file as a compressed package file, such as backup-USR-G806ps-2019-09-16.tar.gz, and save it to the local.

8.6. factory data reset

You can restore factory parameters through the web page.

- By long pressing and releasing the Reload button (factory reset button) for 5~15 seconds, the USR-G806p router can be restored to the factory parameters;
- > Do not disconnect power to the device during recovery. The factory recovery process lasts about 3 minutes;
- > You can restore factory Settings via the web with the same functionality as follows.

Communication Expert of I		st, Do Best! English 中文
USR-G806p	Backup / Flash Firmware	í
 > Status > Services > Network > VPN > Firewall > Serial Server > System 	Backup / Restore Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset". Download backup: @ Generate archive Reset to defaults: ● Perform To restore configuration files, you can upload a previously generated backup archive here. Restore backup: Please select file @ Browse © Upload archive	
System Administration Reboot Timer NTP Http Port Syslog Backup/Upgrade Reboot	Flash new firmware image Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration. Keep settings: Image: Please select file @ Browse Flash image	
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 93 Restore the factory page

8.7. firmware upgrade

The USR-G806p module supports online firmware upgrade in web mode.



Communication Expert of Industrial IOT	Be Honest, Do Best! English ex
USR-G806p	Backup / Flash Firmware
> Status	Backup / Restore
> Services	Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset".
> Network	Download backup:
> VPN	Reset to defaults: O Perform
> Firewall	
> Serial Server	To restore configuration files, you can upload a previously generated backup archive here.
✓ System	Restore backup: Please select file
System	
Administration	Flash new firmware image
Reboot Timer	Upload a proper image here to replace the running firmware. Check "Keep settings" to retain the current configuration.
NTP	Keep settings:
Http Port	
Syslog	Image: Please select file
Backup/Upgrade	
Reboot	U
	JiNan Usr IOT Technology Limited http://www.pusr.com/

Pic 94 Restore the factory page

< explain >

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

8.8. restart

Communication Expert of Indus	Be Honest	;, Do	Best! English 中文
USR-G806p	System		
> Status	Reboots the operating system of your device		
> Services	Reboot		
> Network			
> VPN	Perform reboot		
> Firewall			
> Serial Server			
∽ System			
System			
Administration			
Reboot Timer			
NTP			
Http Port			
Syslog			
Backup/Upgrade			
Reboot			
	JiNan Usr IOT Technology Limited http://www.pusr.com/		

Pic 95 Restart the page

Click the button to restart the router. The restart time is the same as the power-on start time of the router, which



takes about 50 seconds to complete successfully.

8.9. Restart at regular intervals

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

USR IOT Communication Expert of Industrial IOT			Be Hor	nest,	Best! English 中文
USR-G806p Status Services	Reboot Scheduler Reboots the operating system Parameter Configuration				
> Network > VPN > Firewall	Enable Periodic Reboot	Daily V			
Serial Server System	Random Time	Enable a Randomly generate the restart to required.	ime (hours and minutes) to avoid the device online at the same time. If disabled, custom time is		
System Administration Reboot Timer	Random Range(Start) Random Range(End)	4:00 ~ 5:00 ~			
NTP Http Port Syslog	Reboot Time	4:54			
Backup/Upgrade Reboot			Apply Save		
	JiNan U	Jsr IOT Technology Limited	http://www.pusr.com/		

Pic 96 Restart the Settings page

< explain >

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

8.10. Daily record

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

long-range Log

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



Communication Expert of Industrial IOT	Be Hon	est, Do Best! English∣#文
USR-G806p > Status > Services > Network > VPN > Firewall > Serial Server > System System	System Log Here you can view system logs, including application, kernel, and VPN logs.Remote logs based on UDP protocol can also be configured. Configuration Log Remote log Log Kernel View Empty	
Administration Reboot Timer NTP Http Port Syslog Backup/Upgrade Reboot		
	JiNan Usr IOT Technology Limited http://www.pusr.com/	

Pic 97 log page

Local logs

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

9. AT order set

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

9.1. AT code repertory

order number	name	function
number		
1	AT	The Test AT command is available
2	AT+R	Restart the device
3	AT+H	Help document and list all instructions
4	AT+CLEAR	Restore factory
5	AT+VER	Query the firmware version
6	AT+CMDPW	Query/set SMS password
7	AT+MAC	query LANMAC
8	AT+APN	Query/set APN parameters
9	AT+SN	query SN

Tab 33 Summary of AT instructions



10	AT+CSQ	Query the current signal strength		
11	AT+CPIN	Query SIM card status		
12	AT+IMEI	query IMEI		
13	AT+ICCID	query ICCID		
14	AT+MCCMNC	query CIMI		
15	AT+CNUM	query CUNM		
16	AT+SYSINFO	Query network operators and formats		
17	AT+CELLULAR	Query network mode		
18	AT+WEBU	Query the web user name and password		
19	AT+PLANG	query language		
20	AT+UPTIME	Query the device running time		
21	AT+WANINFO	Query wan information		
22	AT+4GINFO	Query 4G information		
23	AT+LANINFO	Query LAN information		
24	AT+WANN	Query wan configuration		
25	AT+LAN	Query the LAN configuration		
26	AT+PING	Ping check		
27	AT+TRAFFIC	Cellular traffic statistics		
28	AT+WIREDTRAFFIC	Wired traffic statistics		
29	AT+NETSTATUS	Get the default routing interface		
30	AT+ALYSIMSWITCH	Query/set the SIM card operator		
31	AT+DUALSIMMODE	Set dual SIM card switching mode		
Serial port S	Settings			
32	AT+S	Restart the DTU program		
33	AT+UART1	Query/Configure serial port 1 parameters		
34	AT+UART2	Query/Configure port 2 parameters		
35	AT+UART1FT	Query/Configure the serial port 1 packing		
		time		
36	AT+UART1FL	Query/Configure the serial port 1 packet length		
37	AT+UART2FT	Query/Configure the serial port 2 packing		
		time		
38	AT+UART2FL	Query/Configure the serial port 2 packet		
		length		
DTU set up				
39	AT+CHLIST	Query all communication configurations of DTU		
40	AT+CHSET	Set the DTU channel configuration		
41	AT+CHDEL	Verify that the DTU channel configuration		
		exists		
42	AT+CHCLR	Remove all channel configurations of the		
		DTU		
L	1	1		



44 AT+C 45 AT+C 46 AT+C 47 AT+C	HCFG HCACHE HREG HHEART HTLS	Query the DTU specified channel configurationQuery the cache configuration of the specified channelQuery the registration packet attributes of the specified channelQuery the heartbeat packet attributes of the specified channel
45 AT+C 46 AT+C 47 AT+C	HREG HHEART	specified channel Query the registration packet attributes of the specified channel Query the heartbeat packet attributes of
46 AT+C 47 AT+C	HHEART	the specified channel Query the heartbeat packet attributes of
47 AT+C		the specified channel Query the heartbeat packet attributes of
47 AT+C		Query the heartbeat packet attributes of
	HTLS	
	HTLS	
48 AT+C		Query/set the TLS configuration for a
48 AT+C		specified channel
	HMODBUS	Query/set the MODBUS configuration of a
		specified channel
MQTT		1
49 AT+M	IQTTFAMILYVER	Query/set the MQTT version of the
		specified channel
50 AT+M	IQTTFAMILYAUTH	Query/set MQTT authentication
		information for a specified channel
51 AT+M	IQTTFAMILYWILL	Query/set the MQTT legacy information for
		a specified channel
52 AT+M	IQTTFAMILYCLEAN	Query/set the MQTT clean session for a
		specified channel
53 AT+M	IQTTFAMILYRCTM	Query/set the MQTT reconnection interval
		for a specified channel
54 AT+M	IQTTFAMILYHEART	Query/set the MQTT heartbeat time for a
		specified channel
Theme Settings		-
55 AT+T	OPICPUBLIST	Query the list of published topics for the
		specified channel
56 AT+T	OPICPUBADD	Add a publishing topic
57 AT+T	OPICPUBDEL	Delete the topic of the release
58 AT+T	OPICPUBCLR	Clear the release topic
59 AT+T	OPICSUBLIST	Query the list of subscription topics
60 AT+T	OPICSUBADD	Add subscription topics
61 AT+T	OPICSUBDEL	Delete the subscription topic
62 AT+T	OPICSUBCLR	Clear the subscription topic
63 AT+N	IETAT	Query/set network AT configuration
Serial port heartbea	t	
64 AT+H	IEARTEN	Query/set serial port heartbeat enable
65 AT+H	IEARTBIND	Query/set serial heartbeat binding
66 AT+H	IEARTTM	Query/set serial port heartbeat time
67 AT+H	IEARTDT	Query/set serial heartbeat data



69	AT+NETRSTIM	Query/set network timeout reconnection
70	AT+NETRCTIM	Query/set the network timeout restart time
71	AT+COMRSTIM	Query/set the serial port timeout restart time
GNSS		
72	AT+GNSSFUNEN	Query/Configure GNSS enabled information
73	AT+GNSSMOD	Query/Configure location type
74	AT+SOCKGLK	Query GNSS status
75	AT+QHEARTTM	Query/Configure heartbeat packet time
76	AT+QHWVER	Query GNSS hardware version
77	AT+QLOGOUT	Send a logout session signal
78	AT+QONLINE	Send an online session signal
79	AT+SOCKG	Query/set the working mode
80	AT+GHEARTEN	Query/set heartbeat packet enablement
81	AT+GHEARTTM	Query/set the heartbeat packet interval
82	AT+GHEARTCON	Query/set heartbeat packet data
83	AT+GPOSTP	Query/set the location package type
84	AT+GREGEN	Query/set the registration package enablement
85	AT+GREGTP	Query/set the registration package type
86	AT+GREGDT	Query/set the registration package data
87	AT+GCLOUD	Query/set the cloud ID and password
88	AT+GMDBS	Query/set the modbus device ID
89	AT+GPOSUPTM	Query/set the modbus reporting interval
90	AT+GREGSND	Query/set the registration package sending method
91	AT+GPGGA	Query gps gngga data
92	AT+GPRMC	Query gps gnrmc data
93	AT+CELLOCATION	Query the lac and CID information of the base station
94	AT+GNSSINFO	Query the GPS status

9.1.1. AT order set

9.1.1.1. AT

name	AT
function	Test the AT command
query	order : AT
	return : OK



set up	not have
parameter	return : OK
explain	The instruction takes effect immediately, and the return OK
	represents that the AT instruction is in use

9.1.1.2. AT+R

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

9.1.1.3. AT+H

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

9.1.1.4. AT+CLEAR

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



9.1.1.5. AT+VER

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

9.1.1.6. AT+CMDPW

name	AT+CMDPW
function	Query/set SMS AT command password
query	AT+CMDPW
	+CMDPW: <cmdpw></cmdpw>
set up	AT+CMDPW= <cmdpw></cmdpw>
	ОК
parameter	cmdpw:
	The password set, such as test.cn#, can be set to 1-20Byte
explain	The command returns OK if it is executed correctly, and the
	device is restarted with this setting in effect

9.1.1.7. AT+MAC

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

9.1.1.8. AT+APN

name	AT+APN
function	Query or set APN information
query	Command: AT+APN



	Return: +APN: apn_name, user, pw, type		
set up	Command: AT+APN=apn_name, user, pw, type		
	return : OK		
parameter	Apn_name: APN address, which can be empty [0-62] bytes,		
	supports the character range [a-zA-Z0-9#@]		
	User: user name, which can be empty [0-62] bytes, [33-126]		
	ASCII characters		
	PW: Password, which can be empty [0-62] bytes, [33-12		
	ASCII characters		
	Type: authentication mode, none/pap/chap		
give an	Command: AT+APN=autocheck,.,.,none		
example	return : OK		
explain	The command is executed correctly and the configuration		
	takes effect after restarting the device		

9.1.1.9. AT+SN

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

9.1.1.10.AT+CSQ

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

< explain >

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

stan	standard		short-cut	Signal strength (dBm)
		proces	S	
GSM/	CDMA/WCDMA/EVDO/EHRPD/LTE	0-31		dBm= -113dBm + signal strength *2



	Nine of the nine				
	had no signal				
TDSCDMA	100-191	dBm=	-116dBm	+	(signal
	Nine of the nine	strength	-100)		
	had no signal				

> When registered to different network modes, the signal strength can not be directly compared whether it is expressed as dBm or asu.

➤ In general, dBm≥-90dBm and asu≥12. The signal strength meets the coverage requirements, which can be used to measure whether the current signal meets the standards.

9.1.1.11.AT+CPIN

name	AT+CPIN
function	Check the status of the device SIM card
query	Command: AT+CPIN
	Return: +CPIN: cpin
set up	not have
parameter	Cpin: SIM card status value
	NOTREADY: Card status is not recognized
	READY: Identify card status
	SIM PIN: Lock the PIN status
	SIM PUK: Lock the PUK state
explain	not have

9.1.1.12.AT+IMEI

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

9.1.1.13.AT+ICCID

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



paramet	er	ICcid: SIM card ICCID number
explain		not have

9.1.1.14.AT+MCCMNC

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

9.1.1.15.AT+CNUM

name	AT+CNUM
function	Query the SIM card phone number
query	AT+CNUM
	+CNUM: <cnum></cnum>
set up	not have
parameter	CNUM: SIM card phone number
explain	

9.1.1.16.AT+SYSINFO

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

9.1.1.17.AT+CELLULAR

name

AT+CELLULAR



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

9.1.1.18.AT+WEBU

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

9.1.1.19.AT+PLANG

name	AT+PLANG
function	Query the web login language
query	AT+PLANG
	+PLANG: <plang></plang>
set up	AT+PLANG= <plang></plang>
	ок
parameter	plang:zh_cn/en
	zn_cn: the Chinese language
	en: English
explain	

9.1.1.20.AT+UPTIME

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



9.1.1.21.AT+WANINFO

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

9.1.1.22.AT+4GINFO

name	AT+4GINFO
function	Query cellular network card information
query	AT+4GINFO
	+4GINFO: <mac> <ip> <mask> <rx_packets> <tr_packets><rx_byt< td=""></rx_byt<></tr_packets></rx_packets></mask></ip></mac>
	es> <tx_bytes></tx_bytes>
set up	not have
parameter	Mac: 4G network card mac
	IP: IP of 4G network card
	Mask: Subnet mask of 4G network card
	rx_packets: Number of received packets
	Tr_packets: Number of packets sent
	rx_bytes: Receive traffic
	tx_bytes: Send traffic
explain	

9.1.1.23.AT+LANINFO

name	AT+LANINFO
function	Query LAN network card information
query	AT+LANINFO
	+LANINFO: <mac> <ip> <mask> <rx_packets> <tr_packets><rx_b< td=""></rx_b<></tr_packets></rx_packets></mask></ip></mac>
	ytes> <tx_bytes></tx_bytes>
set up	not have



parameter	Mac: LAN network card mac
	IP: LAN network card IP
	Mask: Subnet mask of LAN network card
	rx_packets: Number of received packets
	Tr_packets: Number of packets sent
	rx_bytes: Receive traffic
	tx_bytes: Send traffic
	pour :
	If VLAN is configured, this command returns the LAN
	information
explain	

9.1.1.24.AT+WANN

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

9.1.1.25.AT+LAN

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



9.1.1.26.AT+PING

name	AT+PING
function	Run the ping command
query	not have
set up	AT+PING= <ip></ip>
	PING IP(IP): 56 data bytes
parameter	IP: IP or domain name, which cannot be empty. Ping is carried,
	and the parameter is invalid
	For example, c1 is invalid limit [1-200)
	Note: Parameters can only be IP or domain names. Other
	parameters will be judged according to the address and return
	results
explain	

9.1.1.27.AT+TRAFFIC

name	AT+TRAFFIC
function	Query 4G traffic for the time period
query	AT+TRAFFIC
	+TRAFFIC: <rx>,<tx>,<pro_time>,<at_time></at_time></pro_time></tx></rx>
set up	not have
parameter	rx: The number of bytes received in the time period between
	the last query and this query
	Tx: Number of bytes sent between the last query and this
	query
	Protime: The last time this instruction was used
	at_time: The time stamp of this instruction is used
explain	

9.1.1.28.AT+WIREDTRAFFIC

name	AT+WIREDTRAFFIC
function	Query the wan traffic period
query	AT+WIREDTRAFFIC
	+WIREDTRAFFIC: <rx>,<tx>,<pro_time>,<at_time></at_time></pro_time></tx></rx>
set up	not have
parameter	rx: The number of bytes received in the time period between
	the last query and this query



	Tx: Number of bytes sent between the last query and this
	query
	Pro_time: The last time this instruction was used
	at_time: The time stamp of this instruction is used
explain	

9.1.1.29.AT+NETSTATUS

name	AT+NETSTATUS
function	Query the default route usage of the network card
query	AT+NETSTATUS
	+NETSTATUS: <net></net>
set up	not have
parameter	Net: The status of the network card at this time
explain	

9.1.1.30.AT+ALYSIMSWITCH

name	AT+ALYSIMSWITCH
function	Query the SIM card operator
query	AT+ALYSIMSWITCH
	+NETSTATUS: <net></net>
set up	not have
parameter	net:
	CHN-CT Telecom
	CMCC shift
	CUCC log-in
explain	

9.1.1.31.AT+DUALSIMMODE

name	AT+DUALSIMMODE
function	Query/set dual SIM card switching mode
query	AT+DUALSIMMODE
	+DUALSIMMODE: <mode></mode>
set up	AT+DUALSIMMODE= <mode></mode>
	ОК
parameter	mode:
	Master is the master
	Mutual backup
	Manual
explain	Restart the dtu service to make the configuration effective



9.1.1.32.AT+S

name	AT+S
function	Restart the dtu service to make the configuration effective
query	not have
set up	AT+SOK
parameter	not have
explain	Restart the dtu service to make the configuration effective

9.1.1.33.AT+UART1

name	AT+UART1
function	Set/Query the parameters of the 485 interface
query	AT+UART1
	+UART1: <baudrate>,<data_bit>,<stop_bit>,<parity></parity></stop_bit></data_bit></baudrate>
set up	AT+UART1= <baudrate>,<data_bit>,<stop_bit>,<parity> OK</parity></stop_bit></data_bit></baudrate>
parameter	<baudrate>: baud rate, 230400/115200 (default)</baudrate>
	/57600/38400/19200/9600/4800/2400/1200. <data_bit>: data bit,</data_bit>
	7/8
	<stop_bit>: Stop bit, 1/2</stop_bit>
	<parity>: Check bit, NONE/EVEN/ODD.</parity>
explain	

9.1.1.34.AT+UART2

name	AT+UART2
function	Set/Query the 232 interface parameters
query	AT+UART2
	+UART2: <baudrate>,<data_bit>,<stop_bit>,<parity></parity></stop_bit></data_bit></baudrate>
set up	AT+UART2= <baudrate>,<data_bit>,<stop_bit>,<parity> OK</parity></stop_bit></data_bit></baudrate>
parameter	<baudrate>: baud rate, 115200 (default)</baudrate>
	/57600/38400/19200/9600/4800/2400/1200. <data_bit>: data bit,</data_bit>
	7/8
	<stop_bit>: Stop bit, 1/2</stop_bit>
	<parity>: Check bit, NONE/EVEN/ODD.</parity>
explain	



9.1.1.35.AT+UART1FT

name	AT+UART1FT
function	Set/Query the 485 packaging time interval
query	AT+UART1FT?
	+UART1FT: <time></time>
set up	AT+UART1FT= <time> OK</time>
parameter	<time>: Packing time Range [0,1000] 0 (default)</time>
explain	

9.1.1.36.AT+UART1FL

name	AT+UART1FL
function	Set/Query the 485 package length
query	AT+UART1FL
	+UART1FL: <length></length>
set up	AT+UART1FL= <length> OK</length>
parameter	<length>: Packing length Range [5,1460] 1000 (default)</length>
explain	

9.1.1.37.AT+UART2FT

name	AT+UART2FT
function	Set/Query 232 Pack length
query	AT+UART2FT
	+UART2FT: <time></time>
set up	AT+UART2FT= <time> OK</time>
parameter	<time>: Packing time Range [0,1000] 0 (default)</time>
explain	

9.1.1.38.AT+UART2FL

name	AT+UART2FL
function	Set/Query 232 Pack length



query	AT+UART2FL
	+UART2FL: <length></length>
set up	AT+UART2FL= <length> OK</length>
parameter	<length>: Packing length Range [5,1460] 1000 (default)</length>
explain	

9.1.1.39.AT+CHLIST

name	AT+CHLIST
function	Query the list of communication channels
query	AT+CHLIST
	+AT+CHLIST: <ch>,<protocol>,<enable>,<description></description></enable></protocol></ch>
set up	not have
parameter	<ch>: Channel name</ch>
	<protocol>: Channel protocol</protocol>
	TCPC/TCPS/UDPC/UDPS/MQTT/HTTPD/AWS/ALI <enable>: Channel</enable>
	enable
	ON (default)/ OFF
	<description>: Channel description</description>
explain	

9.1.1.40.AT+CHSET

name	AT+CHSET
function	Query the communication channel list
query	not have
set up	AT+CHSET= <ch>,<protocol>,<enable>,<description> OK</description></enable></protocol></ch>
parameter	<ch>: Channel name</ch>
	<protocol>: Channel protocol</protocol>
	TCPC/TCPS/UDPC/UDPS/MQTT/HTTPD/AWS/ALI <enable>: Channel</enable>
	enable
	ON (default)/ OFF
	<description>: Channel description, range [1,32] bytes</description>
explain	


9.1.1.41.AT+CHDEL

name	AT+CHDEL
function	Delete the communication channel
query	not have
set up	AT+CHDEL= <ch> OK</ch>
parameter	<ch>: Channel name range [1,32] bytes</ch>
explain	

9.1.1.42.AT+CHCLR

name	AT+CHCLR
function	Clear the communication channel
query	not have
set up	AT+CHCLR OK
parameter	not have
explain	Delete all added channels

9.1.1.43.AT+CHCFG

name	AT+CHCFG
function	Modify or query channel parameters
query	AT+CHCFG= <ch>?</ch>
	+OK= <ch>, <protocol>, <variable 'protocol'="" based="" on="" parameters=""></variable></protocol></ch>
set up	AT+CHCFG= <ch>, <protocol>, <variable based="" on<="" parameters="" td=""></variable></protocol></ch>
	'Protocol'>



parameter	<ch>: Channel name</ch>
	<protocol>: Protocol</protocol>
	TCPC/TCPS/UDPC/UDPS/HTTPD/MQTT/Ali/AWS <variable< td=""></variable<>
	parameter section>
	TCPC: <server>,<re-port>,<lo-port>,<trans>,<bindcom></bindcom></trans></lo-port></re-port></server>
	<pre><server>: Remote server address range [0-63] bytes <re-port>:</re-port></server></pre>
	Server port range [1-65535]
	<lo-port>: Local port range [0-65535].0 is random</lo-port>
	<trans>: Transmission mode</trans>
	TRANS-Transparent transmission (default) MODBUS-ModBUSRTU
	<bindcom> Channel binding (ALL is not supported in MODBUS)</bindcom>
	485-COM1-485 (default)
	COM1-485 (default)
	232 - COM2-232
	ALL - COM1&COM2
	UDPC: <server>,<re-port>,<lo-port>,<checkport>,<bindcom></bindcom></checkport></lo-port></re-port></server>
	<server>: Remote server address range [0-63] test.cn (default)</server>
	<re-port>: Server port range [1-65535] <lo-port>: Local port range</lo-port></re-port>
	[0-65535]
	0 (default) -0 indicates random
	<checkport>: Port check ON (default) / OFF</checkport>
	<bindcom> Channel binding</bindcom>
	485-COM1-485 (default)
	232 - COM2-232
	ALL - COM1&COM2
	UDPS: <lo-port>,<bindcom></bindcom></lo-port>
	<lo-port>: Local port range [0-65535]. <bindcom>: Channel</bindcom></lo-port>
	binding
	485-COM1-485 (default)
	232 - COM2-232
	ALL - COM1&COM2
	MQTT: <server>,<re-port>,<id></id></re-port></server>
	<pre><server>: Remote server address range [1-128] character</server></pre>
	cloudmqtt.usr.cn (default)
	<re-port>: Server port range [1-65535] 1883 (default)</re-port>
	<id>: Client ID range [1-128] characters 123456 (default)</id>
	AWS: <server>,<re-port>,<id></id></re-port></server>
	<pre><server>: Remote server address Range [1-128] character</server></pre>
	amazonaws.com.cn (default)
	<re-port>: Server port range [1-65535] 8883 (default)</re-port>
	<id>: Client ID range [1-128] characters 123456 (default)</id>
	ALI: <re-< td=""></re-<>



	<re-port>: Server port range [1-65535] 1883 (default)</re-port>
	<type>: Instance type</type>
	PUBLIC-Public instance (default) ENTERPRISE-Enterprise instance
	<key>: ProductKeye Range [1-128] characters</key>
	<name>: devicename, range [1-128] character <secret>:</secret></name>
	deviceSecret range [1-128] character <cli_id>: client ID range</cli_id>
	[1-128] character
	123456 (default)
	<id>: A geographical ID</id>
	cn-hangzhou/cn-shanghai/cn-qingdao/cn-beijing/cn-
	zhangjiakou/cn-huhehaote/cn-shenzhen/cn-chengdu/cn-
	hongkong/ap-southeast-1/ap-southeast-3/ap-southeast-5/eu-
	central-1
	When the instance type is an enterprise instance
	<server>: The server address range [1-128] characters</server>
	HTTPD:
	<server>,<port>,<tp>,<chd>,<url>,<to>,<hd>,<bindcom></bindcom></hd></to></url></chd></tp></port></server>
	<server>: Remote server address range [0-63] characters <port>:</port></server>
	Server port range [1-65535] characters
	<tp>: Request method</tp>
	GET (default)/POST <chd>: Enable filtering packet header ON</chd>
	(default) / OFF
	<url>: HTTP URL range [1-128] bytes "/1.php[3F]" (default)</url>
	<to>: Time-out range [1-3600 seconds] 10 (default)</to>
	<hd>: Request header information range [1-128] bytes</hd>
	"Accept: text/html[0D][0A]" (default)
	<bindcom> Channel binding</bindcom>
	485-COM1-485 (default)
	232 - COM2-232
	ALL - COM1&COM2
explain	The protocol is inconsistent with the existing channel protocol and
	an error is returned
	When polling MODBUS, the serial port binding parameter is not
	allowed to be ALL

9.1.1.44.AT+CHCACHE

name	AT+CHCACHE
function	Query/set channel data cache function
query	AT+CHCACHE
	+CHCACHE: <ch>,<enable>,<cure>,<mode></mode></cure></enable></ch>
set up	AT+CHCACHE OK



parameter	<ch>: Channel name</ch>
	<enable>: Enable authentication when connecting to the server ON</enable>
	/ OFF (default)
	<cure>: Measures to deal with data overflow</cure>
	DISOLD-Discard old data DISNEW-Discard new data <mode>: Cache</mode>
	mode
	PCKLEN-Cache length limit
	PCKCNT-Cache packet limit
explain	You do not need to enter other parameters after closing
	Supported channel protocols: TCPC/TCPS/MQTT/AWS/ Ali Cloud

9.1.1.45.AT+CHREG

name	AT+CHREG
function	Query/set channel data cache function
query	AT+CHREG= <ch></ch>
	+CHREG: <ch>,<mode>,<type>[,<datatype>][,<data>] OK</data></datatype></type></mode></ch>
set up	AT+CHREG= <ch>,<mode>,<type>[,<datatype>][,<data>] OK</data></datatype></type></mode></ch>
parameter	<ch>: Channel name (HTTPD and MQTT are not supported)</ch>
	<mode>: Registration package mode</mode>
	NONE-Close USER-Custom SN
	МАС
	<type>: Sending method</type>
	First-Send a packet when connecting to the server
	EVERY-Add the registration packet to the front of each packet sent
	When the registration package mode is customized
	[<datatype>] Custom registration package data type (only when</datatype>
	the custom mode is selected)
	HEX-Custom registration packet data type is hexadecimal string
	range [2-64] ACSII-Custom registration packet data type is ascii
	string range [1-32] [" <data>"]: Custom registration packet data</data>
	content
explain	Supported channel protocol: TCPC/UDPC
	You do not need to enter any other parameters when you close the
	registration package

9.1.1.46.AT+CHHEART

name	AT+CHHEART
function	Query/set heartbeat packet function
query	AT+CHHEART= <ch></ch>
	+CHHEART: <ch>,<mode>,<type>[,<datatype>][,<data>] OK</data></datatype></type></mode></ch>
set up	AT+CHHEART= <ch>,<mode>,<type>[,<datatype>][,<data>] OK</data></datatype></type></mode></ch>



parameter	CH>: Channel name (HTTPD and MQTT are not supported)
	<mode>: Registration package mode</mode>
	NONE-Close USER-Custom SN
	MAC
	<type>: Sending method</type>
	First-Send a packet when connecting to the server
	EVERY-Add the registration packet to the front of each packet sent
	when the registration packet mode is custom
	[DataType] Custom registration package data type (only when the
	custom mode is selected) HEX-Custom registration package data
	type is a hexadecimal string Range [2-64]
	ASCII-Custom registration package data type is an ascii string
	range [1-32] [<data>]: Custom registration package data content</data>
explain	Supported channel protocol: TCPC/UDPC
	You do not need to enter any other parameters when you close the
	registration package

9.1.1.47.AT+CHTLS

name	AT+CHTLS
function	Query/set heartbeat packet function
query	AT+CHTLS= <ch></ch>
	+CHTLS: <ch>,<enable>,<method> OK</method></enable></ch>
set up	AT+CHTLS= <ch>,<enable>,<method>OK</method></enable></ch>
parameter	<ch>: Channel name</ch>
	<enable>: Authentication enabled when connecting to the server is</enable>
	OFF-Off (default)
	TLS10 - TLS1.0
	TLS12 - TLS1.2
	<method>: Certificate authentication mode NONE-Do not verify the</method>
	certificate (default) SERVER-Verify the server certificate
	BOTH-Two-way authentication
explain	You do not need to enter other parameters after closing
	Supported channel protocols:MQTT,All,TCPC,HTTPD [Note: AWS
	supports TLS by default and does not support AT command query
	configuration]

9.1.1.48.AT+CHMODBUS

name	AT+CHMODBUS
function	Query/set heartbeat packet function



AT+CHMODBUS= <ch>,<enable>,<ack>,<time></time></ack></enable></ch>
+CHMODBUS: <ch>,<enable>,<ack>,<time></time></ack></enable></ch>
ок
AT+CHMODBUS= <ch>,<enable>,<ack>,<time> OK</time></ack></enable></ch>
<ch>: Channel name</ch>
<enable>: Host polling enables the status OFF-off (default)</enable>
ON- open
Ack: Overdue response OFF-Off (default)
ON- open
<time>: Time out range [10-6000] milliseconds 200 (default)</time>
No other parameters need to be input when closing. Channel
protocols supported: TCPC, TCPS
If the protocol transmission mode is not MODBUS, an error is
returned

9.1.1.49.AT+MQTTFAMILYVER

name	AT+MQTTFAMILYVER
function	Query/set MQTT, version information
query	AT+MQTTFAMILYVER= <ch></ch>
	+MQTTFAMILYVER: <ch>,<ver></ver></ch>
	ок
set up	AT+ MQTTFAMILYVER = <ch>,<ver> OK</ver></ch>
parameter	<ch>: Channel name</ch>
	<ver>: MQTT version V3.1-V3.1</ver>
	V3.1.1-V3.1.1 (default)
explain	Supported channel protocol: MQTT



9.1.1.50.AT+MQTTFAMILYAUTH

name	AT+MQTTFAMILYAUTH
function	Query/set MQTT, version information
query	AT+ MQTTFAMILYAUTH= <ch></ch>
	+MQTTFAMILYAUTH: <ch>,<enable>,<usrname>,<password> OK</password></usrname></enable></ch>
set up	AT+MQTTFAMILYAUTH= <ch>,<enable>,<usrname>,<password> OK</password></usrname></enable></ch>
parameter	<ch>: Channel name</ch>
	<enable>: Enable the authentication status ON (default) / OFF</enable>
	when connecting to the server
	<usrname>: The user name required for authentication when</usrname>
	connecting to the server [1-128 bytes] <password>: The password</password>
	required for authentication when connecting to the server [1-128
	bytes]
explain	No other parameters need to be entered when closing. Channel
	protocol is supported:MQTT

9.1.1.51.AT+MQTTFAMILYWILL

name	AT+ MQTTFAMILYWILL
function	Query/set MQTT, last message
query	AT+ MQTTFAMILYWILL= <ch></ch>
	+MQTTFAMILYWILL: <ch>,<enable>,<topic>,<qos>,<payload> OK</payload></qos></topic></enable></ch>
set up	AT+MQTTFAMILYWILL = <ch>,<enable>,<topic>,<qos>,<payload> OK</payload></qos></topic></enable></ch>
parameter	<ch>: Channel name</ch>
	<enable>: Switch status ON / OFF (default)</enable>
	<topic>: The name of the legacy topic. Scope [1-128 bytes] <qos>:</qos></topic>
	The quality of service guarantee level for the legacy
	0-At most once
	1-At least once
	2-Get it right the first time
	<payload>: Content of the will [1-128 bytes]</payload>
explain	No other parameters need to be entered when closing. Channel
	protocol is supported:MQTT



9.1.1.52.AT+MQTTFAMILYCLEAN

name	AT+MQTTFAMILYCLEAN
function	Query/set MQTT clean session function
query	AT+ MQTTFAMILYCLEAN= <ch></ch>
	+MQTTFAMILYCLEAN: <ch>,<enable> OK</enable></ch>
set up	AT+ MQTTFAMILYCLEAN = <ch>,<enable> OK</enable></ch>
parameter	<ch>: Channel name</ch>
	<enable>: Switch status ON / OFF (default)</enable>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.53.AT+MQTTFAMILYRCTM

name	AT+ MQTTFAMILYRCTM
function	Query/set MQTT reconnection detection interval
query	AT+ MQTTFAMILYRCTM= <ch></ch>
	+MQTTFAMILYRCTM: <ch>,<ctim> OK</ctim></ch>
set up	AT+ MQTTFAMILYRCTM = <ch>,<ctim> OK</ctim></ch>
parameter	<ch>: Channel name</ch>
	<rctim>: Reconnection detection interval range [1-3600] 5</rctim>
	(default)
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.54.AT+MQTTFAMILYHEART

name	AT+MQTTFAMILYHEART
function	Query/set MQTT, heartbeat time
query	AT+MQTTFAMILYHEART = <ch>,<ctim> +MQTTFAMILYHEART</ctim></ch>
	= <ch>,<ctim></ctim></ch>
	ОК
set up	AT+ MQTTFAMILYHEART = <ch>,<ctim> OK</ctim></ch>
parameter	<ch>: Channel name</ch>
	<heart>: Heartbeat packet time</heart>
	MQTT/AWS: 30 (default) (0-6000 seconds) ALI: 300 (default)
	(30-1200 seconds
explain	Supported channel protocols: MQTT/All/AWS



9.1.1.55.AT+TOPICPUBLIST

name	AT+TOPICPUBLIST
function	Query the MQTT pre-release topic list
query	AT+ TOPICPUBLIST= <ch></ch>
	+TOPICPUBLIST: <ch>,<name>,<topic>,<qos>,<retained>,<bindc< td=""></bindc<></retained></qos></topic></name></ch>
	OM>, <description></description>
	ок
set up	not have
parameter	<ch>: Channel name <name>: Name</name></ch>
	<topic>: Publish the topic name</topic>
	<qos>: Service quality assurance level 0-up to one time</qos>
	1-At least once
	2-Get it right the first time
	<retained>: Whether to retain the message ON (default) / OFF</retained>
	<bindcom>: Bind channel</bindcom>
	485 - COM1-485
	232 - COM2-232
	ALL-COM1&COM2 <description>: Description</description>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.56.AT+TOPICPUBADD

name	AT+TOPICPUBADD
function	Add new topics to the preset release topic
query	not have
set up	AT+TOPICPUBADD
	= <ch>,<name>,<topic>,<qos>,<retained>,<bindcom>,<descripti< td=""></descripti<></bindcom></retained></qos></topic></name></ch>
	on>
	ок
parameter	<ch>: Channel name</ch>
	<name>: Name</name>
	<topic>: Publish the topic name</topic>
	<qos>: Service quality assurance level 0-up to once</qos>
	1-At least once
	2-Get it right the first time
	<retained>: Whether to retain the message ON (default) / OFF</retained>
	<bindcom>: Bind channel</bindcom>
	485 - COM1-485
	232 - COM2-232
	ALL-COM1&COM2 <description>: Description</description>
explain	Supported channel protocols: MQTT/All/AWS



9.1.1.57.AT+TOPICPUBDEL

name	AT+TOPICPUBDEL
function	Delete the topic with this name from the preset release topics in the
	specified channel
query	not have
set up	AT+ TOPICPUBDEL = <ch>,<name> OK</name></ch>
parameter	<ch>: Channel name</ch>
	<name>: Publish the name of the topic [1-128 bytes]</name>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.58.AT+TOPICPUBCLR

name	AT+TOPICPUBCLR
function	Clear the preset release topic for the specified channel
query	not have
set up	AT+TOPICPUBCLR= <ch> OK</ch>
parameter	<ch>: Channel name</ch>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.59.AT+TOPICSUBLIST

name	AT+TOPICSUBLIST
function	Query the MQTT pre-subscribed topic list
query	AT+TOPICSUBLIST= <ch></ch>
	+TOPICSUBLIST: <ch>,<name>,<topic>,<qos>,<bindcom>,<descripti< td=""></descripti<></bindcom></qos></topic></name></ch>
	on> OK
set up	not have
parameter	<ch>: Channel name <name>: Name</name></ch>
	<topic>: Publish the topic name</topic>
	<qos>: Service quality assurance level 0-up to once</qos>
	1-At least once
	2-Get it right the first time
	<retained>: Whether to retain the message ON (default) / OFF</retained>
	<bindcom>: Bind channel</bindcom>



	485 - COM1-485
	232 - COM2-232
	ALL-COM1&COM2 <description>: Description</description>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.60.AT+TOPICSUBADD

name	AT+TOPICSUBADD
function	Add a new topic to the preset subscription topic
query	not have
set up	AT+TOPICSUBADD
	= <ch>,<name>,<topic>,<qos>,<bindcom>,<description> OK</description></bindcom></qos></topic></name></ch>
parameter	<ch>: Channel name <name>: Name</name></ch>
	<topic>: Publish the topic name</topic>
	<qos>: Service quality assurance level 0-up to once</qos>
	1-At least once
	2-Get it right the first time
	<retained>: Whether to retain the message ON (default) / OFF</retained>
	<bindcom>: Bind channel</bindcom>
	485 - COM1-485
	232 - COM2-232
	ALL-COM1&COM2 <description>: Description</description>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.61.AT+TOPICSUBDEL

name	AT+TOPICSUBDEL
function	Delete the topic in the preset subscription topic that specifies the
	channel
query	not have
set up	AT+TOPICSUBDEL= <ch>,<name> OK</name></ch>
parameter	<ch>: Channel name</ch>
	<name>: The name of the topic to be deleted</name>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.62.AT+TOPICSUBCLR

name	AT+TOPICSUBCLR
function	Clear the preset subscription topic for the specified channel
query	not have



set up	AT+TOPICSUBCLR= <ch> OK</ch>
parameter	<ch>: Channel name</ch>
explain	Supported channel protocols: MQTT/All/AWS

9.1.1.63.AT+HEARTEN

name	AT+HEARTEN
function	Enable or disable the heartbeat packet function
query	AT+HEARTEN
	+HEARTEN: <heart_enable></heart_enable>
set up	AT+HEARTEN= <heart_enable></heart_enable>
	ОК
parameter	heart_enable: ON/OFF
explain	The command is executed correctly and the configuration
	takes effect after restarting the DTU

9.1.1.64.AT+HEARTBIND

name	AT+HEARTBIND
function	Query/set the serial heartbeat packet binding port
query	AT+HEARTBIND?
	+HEARTBIND: <bindcom> OK</bindcom>
set up	AT+ HEARTBIND= <bindcom> OK</bindcom>
parameter	<bindcom>: Bind the serial port</bindcom>
	485 - COM1-485
	232 - COM2-232
	ALL - COM1&COM2
explain	

9.1.1.65.AT+HEARTTM

name	AT+HEARTTM
function	Set/Query heartbeat time
query	AT+HEARTTM?
	+HEARTTM: <heart_times> OK</heart_times>
set up	AT+HEARTTM= <heart_times> OK</heart_times>
parameter	<heart_times>: Heartbeat time, range [1,6000] seconds</heart_times>
explain	



9.1.1.66.AT+HEARTDT

name	AT+HEARTDT
function	Query or set heartbeat packet data
query	AT+HEARTDT
	+HEARTDT: <data></data>
set up	AT+HEARTDT= <data></data>
	ОК
parameter	Data: [2-512] hexadecimal number: 0-9, a-f, A-F, even bits
explain	The command is executed correctly and the configuration
	takes effect after restarting the DTU

9.1.1.67.AT+HEARTDTHEX

name	AT+HEARTDTHEX
function	Query/set the serial heartbeat packet content
query	AT+HEARTDTHEX?
	+HEARTDTHEX: <heartbeat> OK</heartbeat>
set up	AT+ HEARTDTHEX = <heartbeat> OK</heartbeat>
parameter	<heartbeat>: Custom heartbeat packet content (HEX)</heartbeat>
explain	

9.1.1.68.AT+NETRSTIM

name	AT+NETRSTIM
function	Set/Query the restart time without data
query	AT+NETRSTIM?
	+NETRSTIM: <enable>,<timeout_restart> OK</timeout_restart></enable>
set up	AT+NETRSTIM= <enable>[,<timeout_restart>] OK</timeout_restart></enable>
parameter	<enable>: Enable ON/OFF (default)</enable>
	<timeout_restart>: Restart time without data, range [60-36000]</timeout_restart>
	seconds 36000 (default) (60-36000 seconds)
explain	You do not need to enter any other parameters after closing this
	function

9.1.1.69.AT+NETRCTIM

name	AT+NETRCTIM
function	Set/Query no data reconnection time
query	AT+NETRCTIM?
	+NETRCTIM: <enable>,<timeout_restart> OK</timeout_restart></enable>
set up	AT+NETRCTIM= <enable>[,<timeout_restart>] OK</timeout_restart></enable>



parameter	<enable>: Enable ON/OFF (default)</enable>
	<timeout_restart>: No data restart time, range [60-3600] seconds</timeout_restart>
	3600 (default) (60-3600 seconds)
explain	You do not need to enter any other parameters after closing this
	function

9.1.1.70.AT+COMRSTIM

name	AT+COMRSTIM
function	Set/reset the serial port restart time without data
query	AT+COMRSTIM?
	+COMRSTIM: <enable>,<bindcom>,<timeout_restart> OK</timeout_restart></bindcom></enable>
set up	AT+COMRSTIM= <enable>[,<bindcom>,<timeout_restart>] OK</timeout_restart></bindcom></enable>
parameter	<enable>: Enable</enable>
	ON (default)/ OFF
	<bindcom>: Bind the serial port</bindcom>
	485 - COM1-485
	232 - COM2-232
	ALL - COM1&COM2
	<timeout_restart>: No data restart time, range [60-3600] seconds</timeout_restart>
	3600 (default) (60-3600 seconds)
explain	You do not need to enter any other parameters to close this
	function

9.1.1.71.AT+GNSSFUNEN

name	AT+GNSSFUNEN
function	Turn on/off GNSS function
query	Q: AT+GNSSFUNEN?
	Answer: +GNSSFUNEN: <enable></enable>
set up	Q: AT+GNSSFUNEN= <enable></enable>
	answer : OK
parameter	Enable: 1 means open, 0 means close, default is off
explain	

9.1.1.72.AT+GNSSMOD

name	AT+GNSSMOD
function	Select GNSS working mode
query	Q: AT+GNSSMOD?
	Answer: +GNSSMOD: <mode></mode>
set up	Q: AT+GNSSMOD= <mode></mode>
	answer : OK



parameter	mode:
	NET: Private cloud mode
	CLOUD: Someone's cloud model
	Default working mode: NET
explain	

9.1.1.73.AT+SOCKGLK

name	AT+SOCKGLK
function	Query the status of the location server connection
query	Q: AT+SOCKGLK?
	Answer: +SOCKGLK: <state></state>
set up	
parameter	<state>:</state>
	OFF: ununited
	ON: Connected
explain	

9.1.1.74.AT+QHEARTTM

name	AT+QHEARTTM
function	Query/set the heartbeat sending interval
query	Q: AT+QHEARTTM?
	A: +QHEARTTM <time></time>
set up	Q: AT+QHEARTTM= <time></time>
	answer : OK
parameter	<time>: Send interval, [1-6000]s</time>
	The default is 30s
explain	

9.1.1.75.AT+QHWVER

name	AT+QHWVER
function	Query/set hardware version number
query	Q: AT+QHWVER?
	Answer: +QHWVER: <ver></ver>
set up	Q: AT+QHWVER= <ver></ver>
	answer : OK
parameter	<ver>: Hardware version number, string type, up to 20 bytes</ver>
	supported by default: GNSS-v1.0
explain	



9.1.1.76.AT+QLOGOUT

name	AT+QLOGOUT
function	Log out of the terminal in Qianxun mode
query	Q: AT+QLOGOUT
	answer : OK
set up	
parameter	
explain	Qianxun platform does not support this instruction, and it is
	mainly adapted to JT808 standard protocol for reservation

9.1.1.77.AT+QONLINE

name	AT+QONLINE
function	The terminal is logged off and online in the Qianxun mode
query	Q: AT+QONLINE
	answer : OK
set up	
parameter	
explain	Qianxun platform does not support this instruction, and it is
	mainly adapted to JT808 standard protocol for reservation

9.1.1.78.AT+SOCKG

name	AT+SOCKG
function	Third-party cloud server related parameters
query	Q: AT+SOCKG?
	Answer: +SOCKG: <protocol>, <address>, <port></port></address></protocol>
set up	Q: AT+SOCKG= <protocol>, <address>, <port></port></address></protocol>
	answer : OK
parameter	<protocol>: Communication protocol, TCPC or TCPS</protocol>
	<address>: Server address, domain name or IP. The default is</address>
	test.usr.cn. In TCPS, this field can be empty
	<port>: Server port, range [1~65535], default: 2317</port>
explain	

9.1.1.79.AT+GHEARTEN

	name	AT+GHEARTEN
t	function	Heartbeat packet enablement control is enabled in the
		third-party cloud mode



query	Q: AT+GHEARTEN?
	A: +GHEARTEN: <enable></enable>
set up	Q: AT+GHEARTEN= <enable></enable>
	answer : OK
parameter	<enable>: Enable control, ON means on, OFF means off,</enable>
	default is off
explain	

9.1.1.80.AT+GHEARTCON

name	AT+GHEARTCON
function	Heartbeat packet content in the third-party cloud mode
query	Q: AT+GHEARTCON?
	A: +GHEARTCON: <content></content>
set up	Q: AT+GHEARTCON= <content></content>
	answer : OK
parameter	<content>: Heartbeat packet content, character type, length</content>
	[1-512], default is 123456
explain	

9.1.1.81.AT+GHEARTTM

name	AT+GHEARTTM
function	Query/set the heartbeat sending interval in third-party cloud
	mode
query	Q: AT+GHEARTTM?
	A: +GHEARTTM <time></time>
set up	Q: AT+GHEARTTM= <time></time>
	answer : OK
parameter	<time>: Sending interval, [1~6000]s, default is 30s</time>
explain	

9.1.1.82.AT+GPOSTP

name	AT+GPOSTP
function	Query/set the heartbeat sending type in third-party cloud
	mode
query	Q: AT+GPOSTP?
	Answer: +GPOSTP <type></type>
set up	Q: AT+GPOSTP= <type></type>
	answer : OK
parameter	<type>:</type>
	RMC: The original field of RMC in the GNSS information report



	GGA: The original GGA field in the GNSS information reported
	MDBS: The MODBUS46 function code is reported. Default:
	MDBS
explain	

9.1.1.83.AT+GREGEN

name	AT+GREGEN
function	Query/set the heartbeat sending type in third-party cloud
	mode
query	Q: AT+GREGEN?
	A: +GREGEN: <enable></enable>
set up	Q: AT+GREGEN= <enable></enable>
	answer : OK
parameter	<enable>: Enable control, ON means open, OFF means close,</enable>
	default is off
explain	

9.1.1.84.AT+GREGTP

name	AT+GREGTP
function	Query/set the package type registered under third-party
	cloud mode
query	Q: AT+GREGTP?
	Answer: +GREGTP: <type></type>
set up	Q: AT+GREGTP= <type></type>
	answer : OK
parameter	<type>: [ICCID, IMEI, USER, IMSI, SN], default value: USER</type>
explain	

9.1.1.85.AT+GREGDT

name	AT+GREGDT
function	Query/set the package type registered under third-party
	cloud mode
query	Q: AT+GREGDT?
	A: +GREGDT: <data></data>
set up	Q: AT+GREGDT= <data></data>
	answer : OK
parameter	<data>: User-defined registration packet data in hexadecimal</data>
	string format with a maximum length of 256 bytes (after
	conversion), 2 to 512 even bytes, and a default of
	7777772E7573722E636E



explain

9.1.1.86.AT+GCLOUD

name	AT+GCLOUD
function	Query/set the content of human cloud parameters in
	third-party cloud mode
query	Q: AT+GCLOUD?
	Answer: +GCLOUD: <id>, <password></password></id>
set up	Q: AT+GCLOUD= <id>, <password></password></id>
	answer : OK
parameter	<id>: The registered ID of the cloud function is passed by</id>
	someone. It is 20 bytes long and defaults to empty
	<password>: The communication password of the cloud</password>
	function is passed by someone. The length is 8 bytes and the
	default is empty
explain	

9.1.1.87.AT+GMDBS

name	AT+GMDBS
function	Query/set MODBUS parameters in third-party cloud mode
query	Q: AT+GMDBS?
	Answer: +GMDBS: <id>, <address></address></id>
set up	Q: AT+GMDBS= <id>,<address></address></id>
	answer : OK
parameter	<id>: From the machine number, [0-255], default value: 1</id>
	<address>: Register address, [0-65535]. Default value: 0</address>
explain	

9.1.1.88.AT+GPOSUPTM

name	AT+GPOSUPTM
function	Query/set the interval of sending location information
query	Q: AT+GPOSUPTM?
	A: +GPOSUPTM: <time></time>
set up	Q: AT+GPOSUPTM= <time></time>
	answer : OK
parameter	<time>: Sending interval, [1~6000]s, default is 30s</time>
explain	



9.1.1.89.AT+GREGSND

name	AT+GREGSND
function	Query/set the sending method of registration package under
	third-party cloud mode
query	Q: AT+GREGSND?
	Answer: +GREGSND <type></type>
set up	Q: AT+GREGSND= <type></type>
	answer : OK
parameter	<type>: <link data=""/>, default value: LINK</type>
explain	

9.1.1.90.AT+GPOSSND

name	AT+GPOSSND		
function	Query/set the heartbeat sending direction in private cloud		
	mode		
query	Q: AT+GREGSND?		
	Answer: +GREGSND <type></type>		
set up	Q: AT+GREGSND= <type></type>		
	answer : OK		
parameter	<type>:</type>		
	NET: Position the heartbeat packet to the network [default]		
	COM: Position the heartbeat packet to the serial port		
	DOUBLE: It is sent to both the network and the serial port		
explain			

9.1.1.91.AT+GPGGA

name	AT+GPGGA
function	Query the original GPGGA information
query	Q: AT+GPGGA?
	Answer: +GPGGA: <gpgga></gpgga>
set up	
parameter	Gpgga>: GPGGA raw information
explain	

9.1.1.92.AT+GPRMC

name	AT+GPRMC
function	Query the original GPRMC information
query	Q: AT+GPRMC?



	Answer: +GPRMC: <gprmc></gprmc>
set up	
parameter	GPRMC: Original GPRMC information
explain	

9.1.1.93.AT+CELLOCATION

name	AT+CELLOCATION
function	Query base station information
query	Q: AT+CELLOCATION?
	Answer: + CELLOCATION <lac>, <cid></cid></lac>
set up	
parameter	LAC: Location code
	<cid>: Cell ID</cid>
explain	

9.1.1.94.AT+GNSSINFO

name	AT+GNSSINFO	
function	Query GNSS information	
query	Q: AT+GNSSINFO?	
	Answer: +GNSSINFO: <status>, <longitude_hem>, <longitude>,</longitude></longitude_hem></status>	
	<latitude_hem>, <latitude></latitude></latitude_hem>	
set up		
parameter	<pre><state>: Positioning status: A: valid positioning, V: inva</state></pre>	
	positioning	
	<longitude_hem>: Longitude hemisphere: E and W</longitude_hem>	
	<longitude>: Longitude (in degrees)</longitude>	
	<latitude_hem>: Latitude hemisphere: N and S</latitude_hem>	
	<latitude>: Latitude (in degrees)</latitude>	
explain		



10. 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.

11. Update log

Version	Update content	Refresh time
V1.0.0	Create documents and complete relevant function descriptions	2025-06-30







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