PUSR®
www.pusr.com

Edge LoRaWAN Gateway

USR-LG270

User Manual



V2.0

Your Trustworthy Smart Industrial IoT Partner

Table

1. Product Overview 4
1.1. Product Introduction 4
1.2. Selection Table 5
1.3. Product Features 6
1.4. Product Parameters 7
1.5. Hardware Structure 10
2. Web Configuration 12
3. System Management 13
3.1. System Time 13
3.2. Local Parameter Settings 14
3.3. Configuration Import/Export 14
3.4. Factory Reset 15
3.5. Firmware Upgrade 16
3.6. Storage Management 16
3.7. Buzzer 17
3.8. Power Failure Alarm 17
4. Network Management 18
4.1. Network Switching 19
4.2. Cellular Network 21
4.3. Wireless WiFi Network 23
4.4. Ethernet Port Management 25
4.5. WAN Port Management 26
4.6. LAN Port Management 27
4.7. Routing 28
4.8. VPN 30
4.8.1. PPTP Client 31
4.8.2. L2TP Client 32
4.8.3. OpenVPN 33
4.8.4. IPSec 34
4.9. Network Diagnostics 35

4.10. Firewall 36
5. LoRaWAN 37
5.1. LoRaWAN Network Introduction 37
5.2. LoRaWAN Network Architecture 38
5.3. LoRaWAN Gateway Frequency Band Settings 39
5.4. Gateway Mode Settings 40
5.4.1. Built-in NS Mode 41
5.4.2. Built-in NS-Edge Mode 55
5.4.3. Packet Forwarding Mode 60
6. Serial Port Management 61
6.1. Serial Port Configuration 61
6.2. Serial Port Framing Mechanism 62
7. Communication Link 63
7.1. Communication Link 63
7.2. Offline Data Caching 64
8. Edge Computing 64
8.1. Data Point Table 66
8.2. Slave Devices and Points 67
8.3. Slave Device Status 71
8.4. Point Data 72
8.5. Import/Export 72
8.6. Edge Data Collection 74
8.7. Edge Computing 75
8.8. Active Reporting 78
8.8.1. Active Reporting 78
8.8.2. JSONTemplate 80
8.9. Protocol Conversion 82
9. Remote Cloud Service 84
9.1. DataConfiguration 85
9.2. Data Monitoring 88
9.3. Device Maintenance 89
10. Contact Information ..... **错误！未定义书签。**
11. Disclaimer 91
12. Update History 91

1. Product Overview

1.1. Product Introduction

USR-LG270 is a high-performance industrial LoRaWAN® edge computing gateway independently developed and designed by USR IoT. It integrates LoRaWAN network access, edge computing, protocol conversion, data collection, and remote management, specifically designed for industrial IoT scenarios. The gateway adopts an industrial-grade RK3506J ARM triple-core processor platform, equipped with Semtech SX1302 8-channel LoRa baseband chip, supporting global mainstream LoRaWAN frequency bands such as CN470, US915, AU915, AS923, and EU868, featuring powerful data processing capabilities and stable communication performance.

The product has a built-in LoRaWAN Network Server (NS), allowing the construction of a private LoRaWAN network without additional server deployment, supporting stable access and management of thousands of LoRaWAN nodes. Meanwhile, the gateway integrates the WukongEdge edge computing engine, supporting local data processing, logical operations, linkage control, and protocol conversion, helping users reduce cloud dependency and improve system response speed and data security.

USR-LG270 provides rich industrial interfaces and multi-network access capabilities, including dual Gigabit Ethernet ports, dual-band Wi-Fi 6, Cat.1 cellular network, RS485/RS232 serial ports, I/O, USB, etc., supporting various communication protocols such as MQTT, HTTP, TCP, Modbus, BACnet, and DLT645. The product adopts industrial-grade wide temperature and wide voltage design, with EMC industrial-grade protection, suitable for complex and harsh industrial environments.

It is widely used in smart industry, smart energy, smart agriculture, smart parks, environmental monitoring, building automation, and other fields, helping users quickly build stable, secure, and efficient IoT systems.



1.2. Selection Table

Model	Frequency Band	Environment	Cellular	WiFi	Ethernet	GNSS
USR-LG270-470	470~510MHz	Indoor	--	Dual-bandWiFi6 2.4G: IEEE 802.11b/g/n/ax 2.4000 - 2.4835GHz 5.8G: IEEE 802.11a/n/ac/ax 5.15 - 5.25GHz; 5.25 - 5.35GHz; 5.47 - 5.73GHz; 5.735 - 5.835GHz	√	--
USR-LG270-470-C1	470~510MHz	Indoor	√		√	--
USR-LG270-470h-C1*	470~510MHz	Outdoor	√		√	√
USR-LG270-915	902~928MHz	Indoor	--		√	--
USR-LG270-915-GL1	902~928MHz	Indoor	√		√	--
USR-LG270-915h-GL1*	902~928MHz	Outdoor	√		√	√

USR-LG270-868	863~870MHz	Indoor	--		√	--
USR-LG270-868-GL1	863~870MHz	Indoor	√		√	--
USR-LG270-868h-GL1*	863~870MHz	Outdoor	√		√	√

1.3. Product Features

■ Hardware System

- RK3506J, industrial-grade main control, 3-core Cortex A7, ARM architecture, 1.2GHz main frequency;
- 1G RAM + 8G EMMC, supports external TF memory card;
- Rich communication interfaces, LoRaWAN, 2 * Ethernet ports (1WAN/LAN + 1LAN), 2 * serial ports (1RS485 + 1RS232/485), IO ports (1DI + 1DO), dual-band WiFi 6 (AP/STA), cellular (Cat 1 dual SIM single standby), USB (Type-A);
- Reserved M.2 interface, expandable to 5G cellular, ZigBee, Bluetooth and other communication methods. Reserved GNSS positioning;

■ LoRaWAN Network

- Supports LoRaWAN® standard protocol,supports CN470, US915, AU915, AS923, EU868 and other frequency bands;
- Uses Semtech SX1302 eight-channel LoRa® chip, supports half-duplex transmission, strong data processing capability;
- Supports access of third-party standard LoRaWAN terminals, supports access of thousands of nodes
- Built-in LoRaWAN NS service
- Compatible with third-party LoRaWAN platforms such as ChirpStack and TTN

■ Edge Computing

- Built-in WukongEdge edge computing engine,supports edge collection, edge computing, grouped reporting, supports collection of 1000 data points
- Rich collection protocols, supports Modbus RTU, Modbus TCP, BACnet, DLT645, etc.

■ Industrial Design

- Wide voltage input 9~48VDC

- Operating temperature -25℃ ~ +75℃
- EMC industrial grade protection
- DIN rail mounting,ear mounting

■ Power-off Alarm

- Continues to work for about 20 seconds after power off
- Automatically report power-off alarms
- Ensure complete upload of critical event data

■ Open Development

- Standard Ubuntu 22.04 operating system
- Supports Node-RED for customer secondary development
- Provides a rich software development environment

1.4. Product Parameters

Category	Item	Specifications
Hardware System	CPU	RK3506J, Triple-Core ARM Cortex-A7, Max Frequency 1.2GHz
	Memory	1GB DDR
	Flash	8GB eMMC
	External Storage	TF Card Expansion Supported
LoRaWAN	LoRa Chip	Semtech SX1302
	LoRa Channels	8 Channels
	Protocol	V1.0 Class A/Class B/Class C and V1.1 Class A/Class B/Class C
	Frequency Bands	CN470, AU915, US915, EU868, AS923-1/2/3/4
	Receive Sensitivity	-140dBm @292bps
	Transmit Power	27dBm Max
	Antenna Interface	1 × Standard SMA Female External Antenna Interface, Characteristic Impedance 50 Ohms

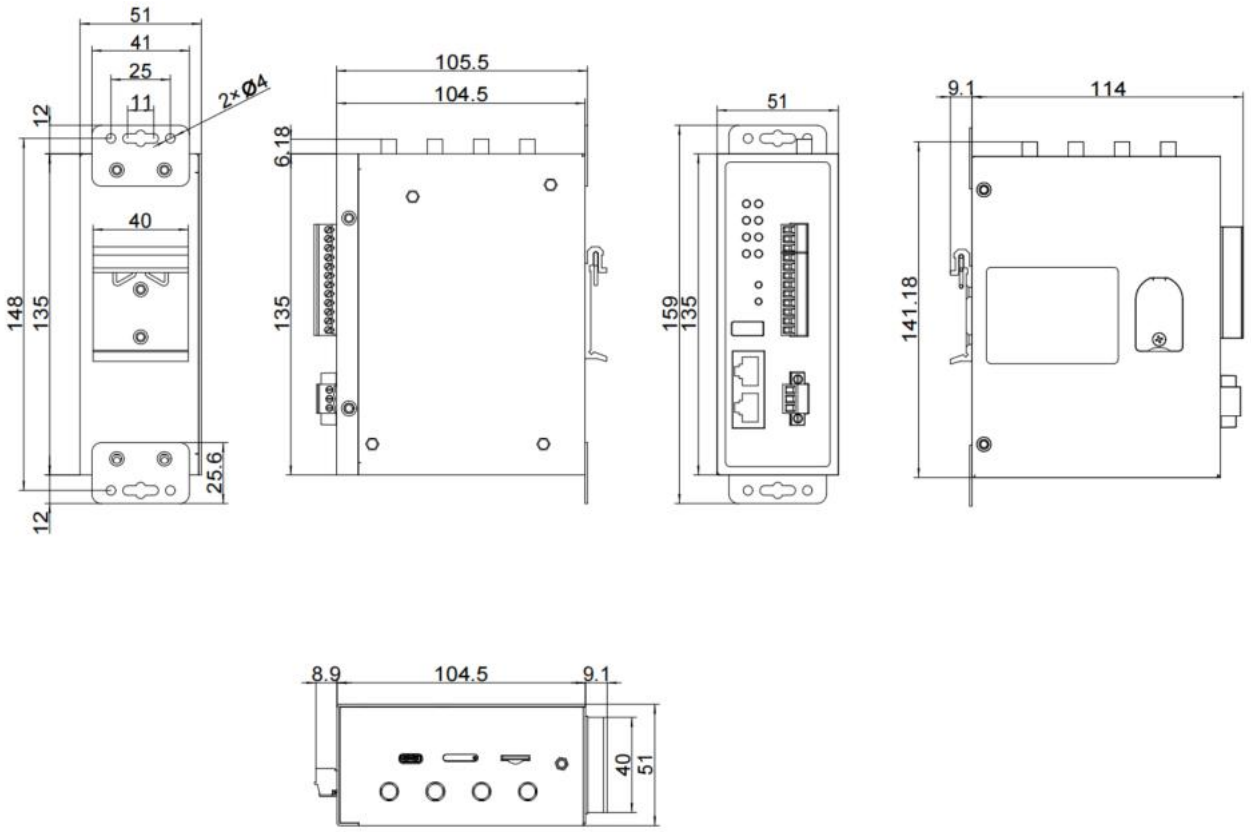
Category	Item	Specifications
	Communication Distance	Based on LoRaWAN® communication, with wide coverage. Transmission distance can reach 15 km in open areas and 5.5 km in urban areas (communication distance is closely related to the actual deployment environment; actual distance depends on specific deployment conditions).
	LoRaWAN Node Capacity	1000+ End Devices
Ethernet Port	Ethernet Interface	2 × 10/100 Mbps RJ45 (1 WAN/LAN + 1 LAN)
Serial Port & I/O	Serial Interface	1 × RS485, 1 × RS232/485
	Digital Input/Output	1 × DI, 1 × DO
WiFi	WiFi Standard	IEEE 802.11b/g/n/ax, 2.4GHz IEEE 802.11a/n/ac/ax, 5GHz
	WiFi Frequency Bands	2.4G: 2.4 - 2.4835GHz (2.4GHz ISM Band) 5.8G: 5.15 - 5.25GHz; 5.25 - 5.35GHz; 5.47 - 5.73GHz; 5.735 - 5.835GHz (5GHz ISM Band)
	Antenna Interface	1 × Standard SMA Female External Antenna Interface, Characteristic Impedance 50 Ohms
	Operating Mode	AP or STA
Cellular Network	Frequency Bands	China/India Region: TDD-LTE: Band 34/38/39/40/41 FDD-LTE: Band 1/3/5/8 Other Regions: TDD-LTE: Band 34/38/39/40/41 FDD-LTE: Band 1/2/3/4/5/7/8/12/13/14/17/18/19/20/25/26/28/66/71
	Antenna Interface	1 × Standard SMA Female External Antenna Interface, Characteristic Impedance 50 Ohms
	SIM Card Slot	2 × Nano SIM Slots, Dual SIM Single Standby
	Theoretical Speed	Max Downlink Speed 10Mbps, Max Uplink Speed 5Mbps
Other Interfaces	USB	1 × USB Type-A, for image upgrade (in secondary development mode, can be used for user customization)

Category	Item	Specifications
	Buttons	Reload Button: Long press for 3-15 seconds to restore factory settings (in secondary development mode, can be used for user customization) REC Button: For image upgrade
	LED Indicators	PWR, WORK, LTE, WiFi, LoRa, User-defined × 3
	Type-C	For device debugging
	Grounding Screw	Grounding Screw
	Reserved Interface	M.2 Slot: Expandable for 5G Cellular, ZigBee, Bluetooth, etc. GNS
	GNSS	Reserved
Software Features	Operating System	Ubuntu Linux
	Edge Computing Engine	WukongEdge
	Edge Computing Points	Up to 1000 Points
	Built-in NS Service	Supported
	LoRaWAN Activation Method	OTAA / ABP
	ADR	Supported
	Third-party LoRaWAN Platform	ChirpStack, TTN
	Northbound Protocol	MQTT, TCP, HTTP
	Industrial Protocol	Modbus RTU, Modbus TCP, BACnet, DLT645, Various PLC Protocols, etc.
	Local Data Storage	Supported

Category	Item	Specifications
	Secondary Development	Supported
	VPN	PPTP, L2TP, OpenVPN
Electrical and Environmental Parameters	Power Supply	9 ~ 48VDC
	Power-off Alarm	Built-in Supercapacitor
	Power-off Backup Time	Max 20 Seconds
	Operating Temperature	-25°C ~ +75°C
	Storage Temperature	-40°C ~ +85°C
	Operating Humidity	5% ~ 95% RH (Non-condensing)
	EMC Protection	Industrial Grade Protection
Mechanical Characteristics	Product Dimensions	135 × 104.5 × 51 mm
	Installation Method	DIN Rail / Ear Mounting
	Enclosure Material	Sheet Metal

1.5. Hardware Structure

LG270 Dimensions: 123.1*141.18*51mm (including terminals/rails)



Indicator Lights

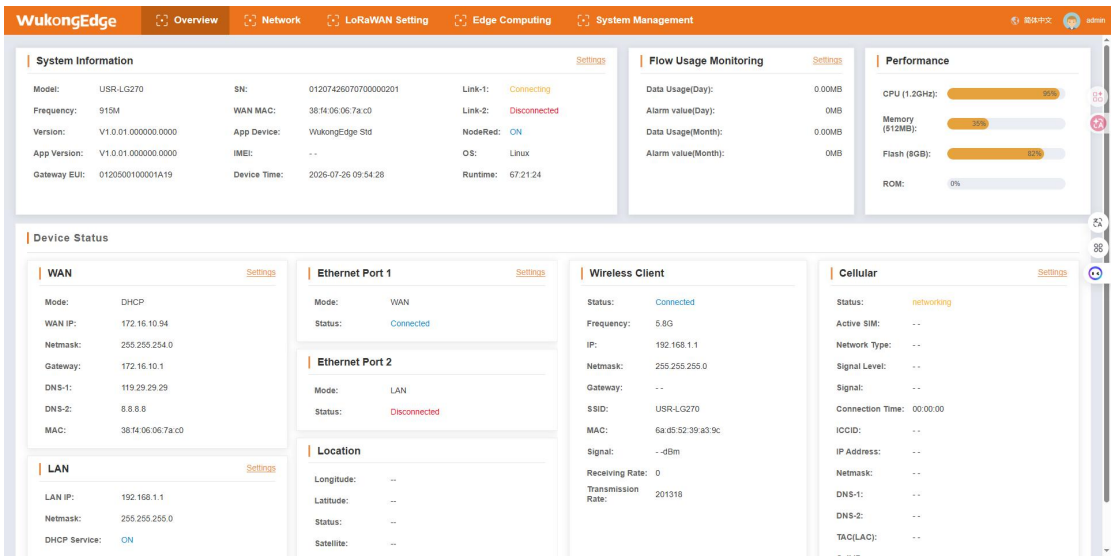
Indicator Light	Label	Status Description
Power Indicator	PWR	Solid on when powered, off when power is lost
Working Indicator	WORK	Blinks once every 1s during normal operation Firmware upgrade, blinks every 400ms
4G Indicator	LTE	Solid on when network registration is successful and signal strength ≥ 22 Blinking when network registration is successful and signal strength < 22 Off when network registration fails
WiFi Indicator	WiFi	Solid on after WiFi starts

LoRa Indicator	LoRa	Blinks when data is being transmitted or received
Custom Indicator	User	3 indicators, for customer custom development

2. Web Configuration

FromThis chapter will provide an in-depth and comprehensive introduction to the various functions of WukongEdge, along with detailed application operation guides for each function, helping you quickly master and utilize these features.

The web configuration system of WukongEdge is designed with extreme convenience as its core concept, simplifying complexity and eliminating redundant steps. Users do not need complex operation processes; they can quickly complete various configurations by simply clicking and setting up on the intuitive web interface, significantly shortening the time cycle from deployment to actual application, helping users integrate WukongEdge into business processes faster and efficiently achieve expected application goals.

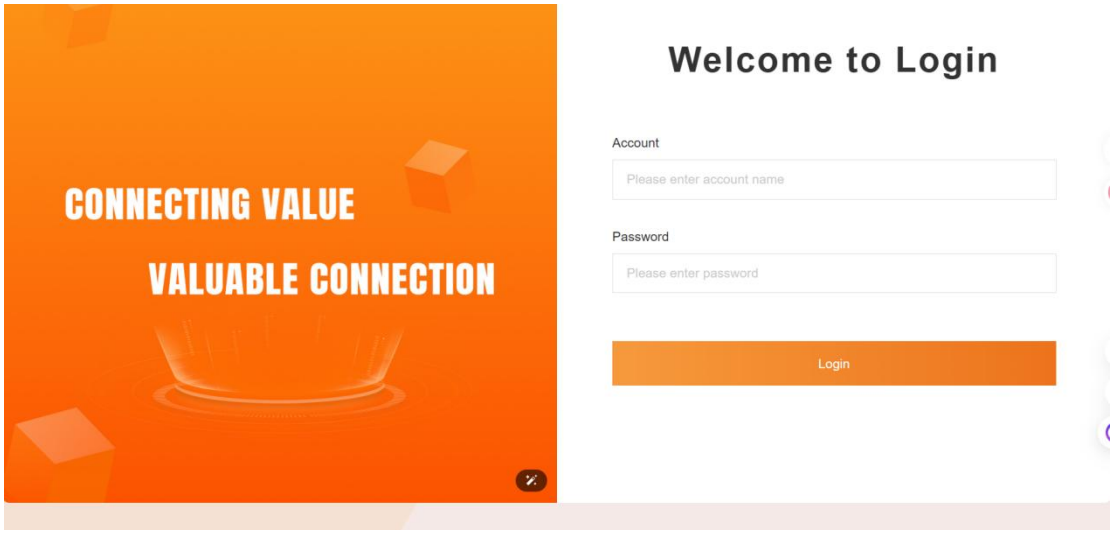


Steps for multi-port devices:

1. After powering on the device, connect the computer and the hardware device via the LAN port. The built-in LAN port of WukongEdge supports DHCP Server function and will assign an IP address to the computer;

2. Open "192.168.1.1" in the computer browser to enter the login interface, and input the default username and password to log in. The default username and password are: admin/admin;

3. After logging in, the overview interface is displayed first, showing the network status of WukongEdge and important device information.



3. SystemManagement

3.1.System Time

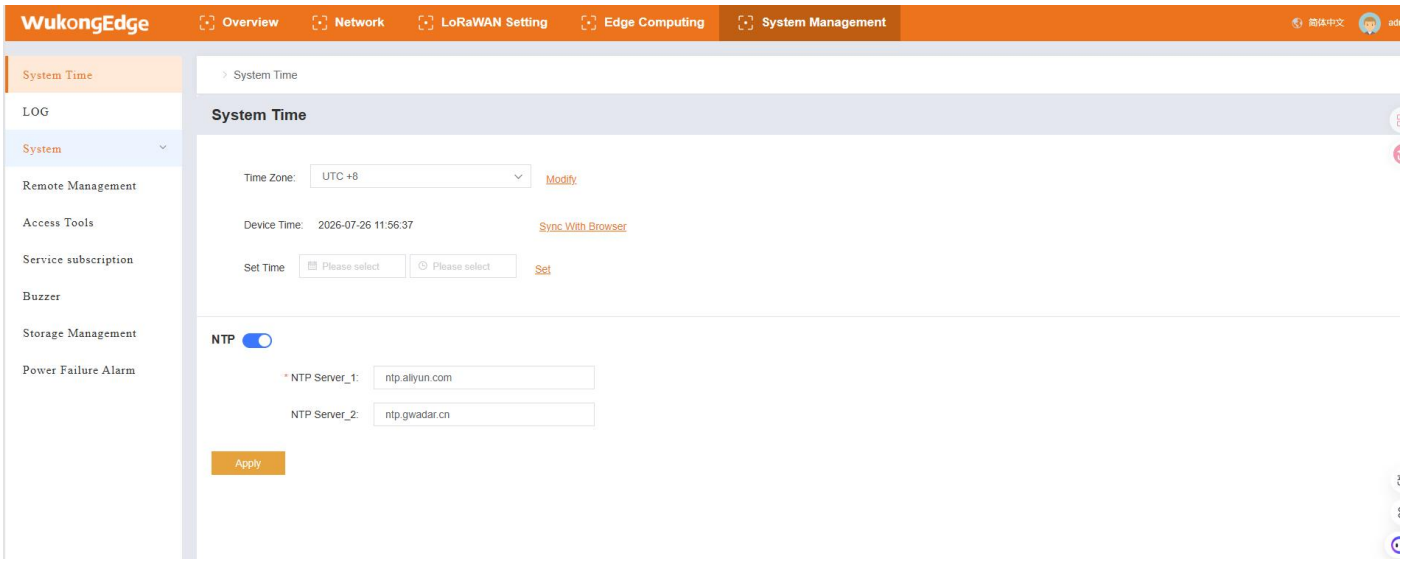
LG270supports two time synchronization functions: NTPsynchronization andsynchronousbrowser synchronization.

When the device cannot connect to the internet, open the built-in web page of the device via PCto manually synchronize time, which will sync the PC's computer time to the device, calibrating the device system time.

When the device can connect to the network, set up an NTPserver and obtain precise network time from the NTPserver to calibrate the device's system time.

LG270's many timing functions require accurate system time. If time cannot be synchronized via NTPor

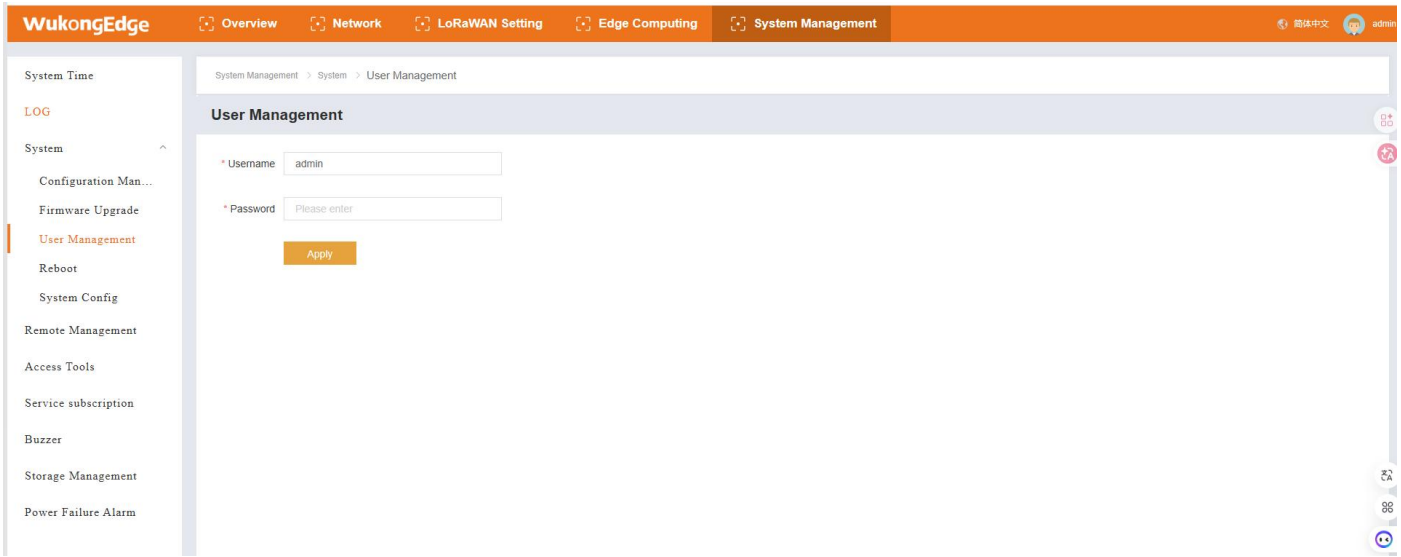
manually, the system time will default to starting from 1970-01-01 00:00:00.



3.2.Local Parameter Settings

USR-LG270comes with a built-in webWebserver. Users can set parameters via the web page and also view module-related statuses. The web server uses port 80 by default. Additionally,LG270provides the function to modify this port. After modification, the built-in web page can be accessed via other ports.

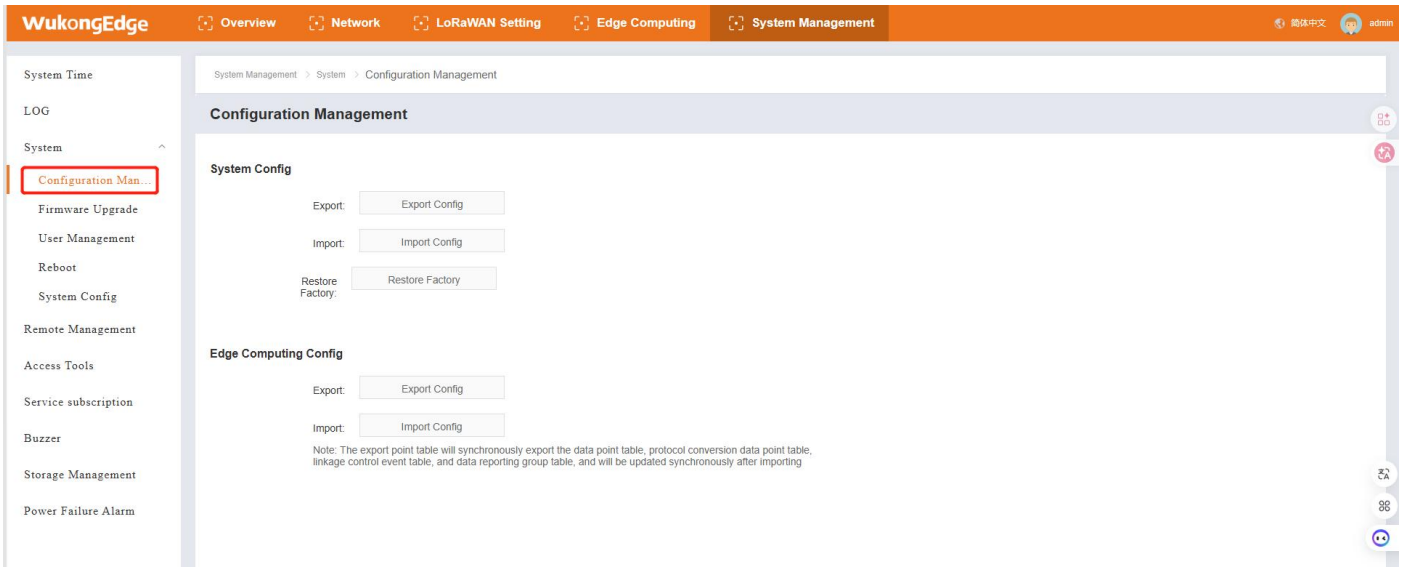
The default username and password for the built-in web page are both admin. You can modify the username and password via the built-in web page.



3.3.Configuration Import/Export

Supportsimport/export of system files/edge computing parameters. For the import function, first select

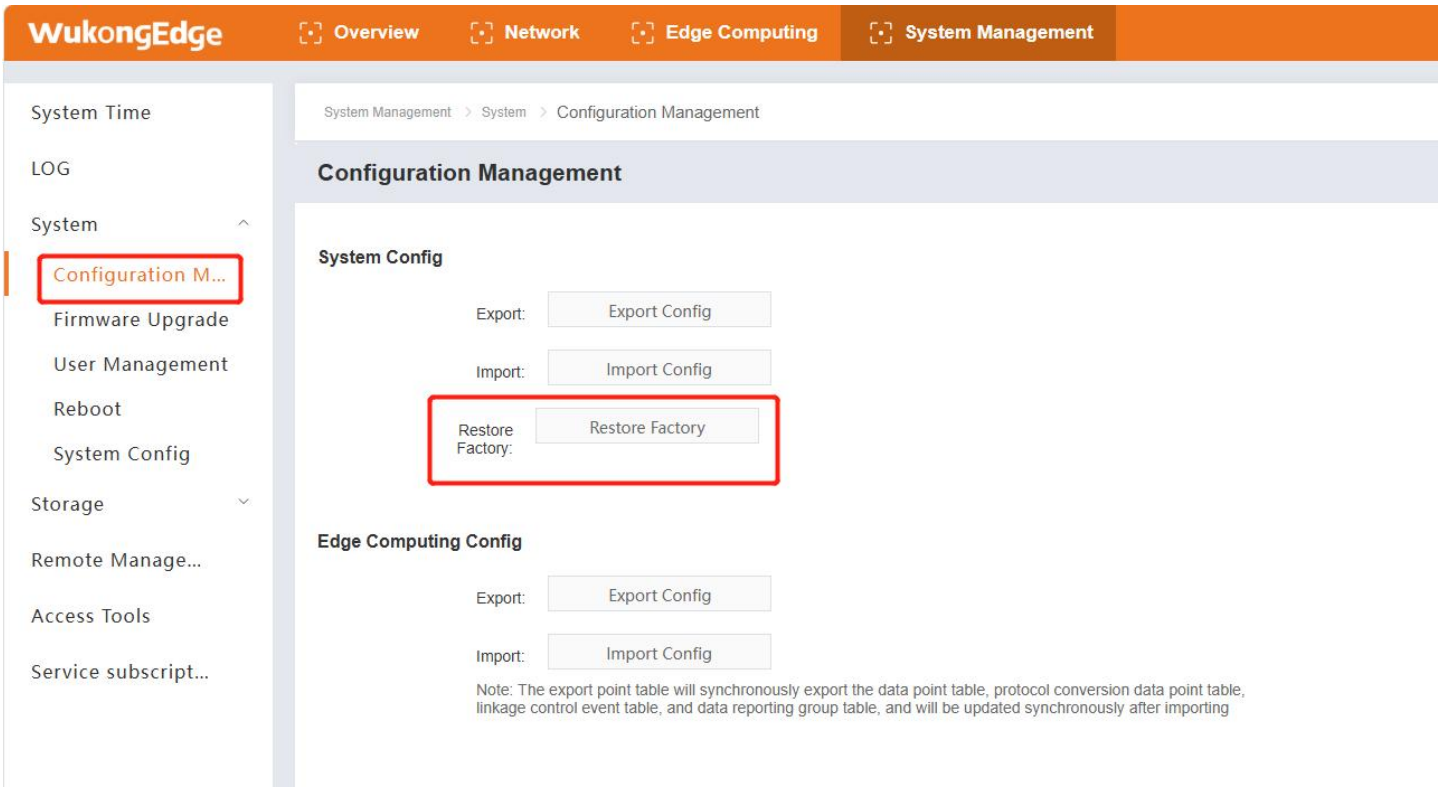
the file to be imported.



3.4.Factory Reset

Hardware Factory Reset: The module can perform a hardware factory reset. In the powered-on state, press and hold the Reload button, and release it after 3-15 seconds to perform a hardware factory reset.

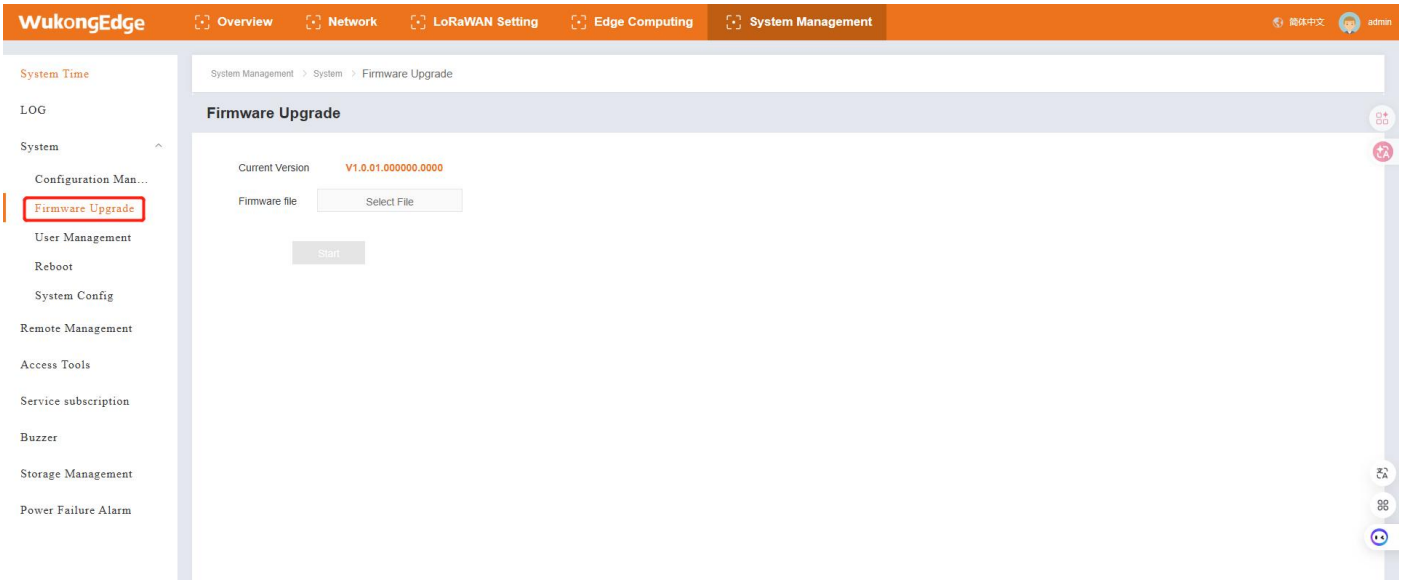
Software Factory Reset: Enter via the web pageSystem Settings--ConfigurationManagement, and click the Factory Reset button to restore factory settings.



3.5.Firmware Upgrade

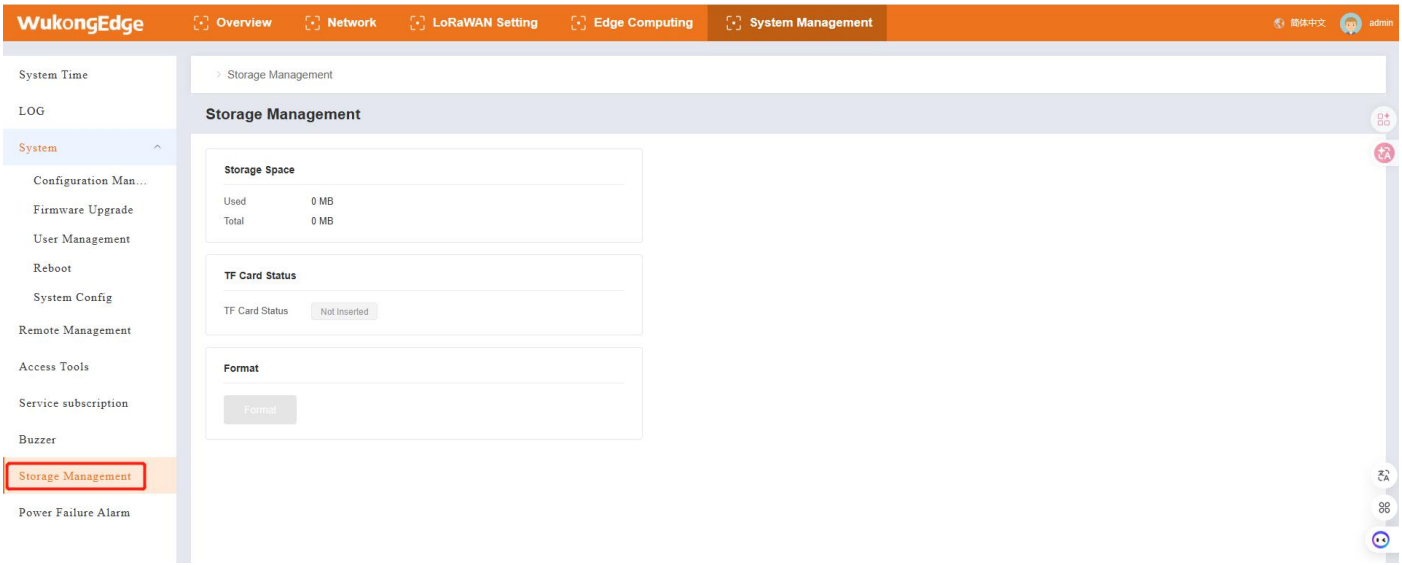
By upgrading the firmware, you can access more advanced applications.Insidethe built-in web page, go to"System Settings--Firmware Upgrade", and select the path where the corresponding firmware file is stored. Double-click the left mouse button, and you will see the path filled into the firmware file box, then click Flash Firmware.

If the firmware download is successful, the following prompt will appear"Firmware download successful, will automatically restart to complete the upgrade", click OK, firmware download successful.



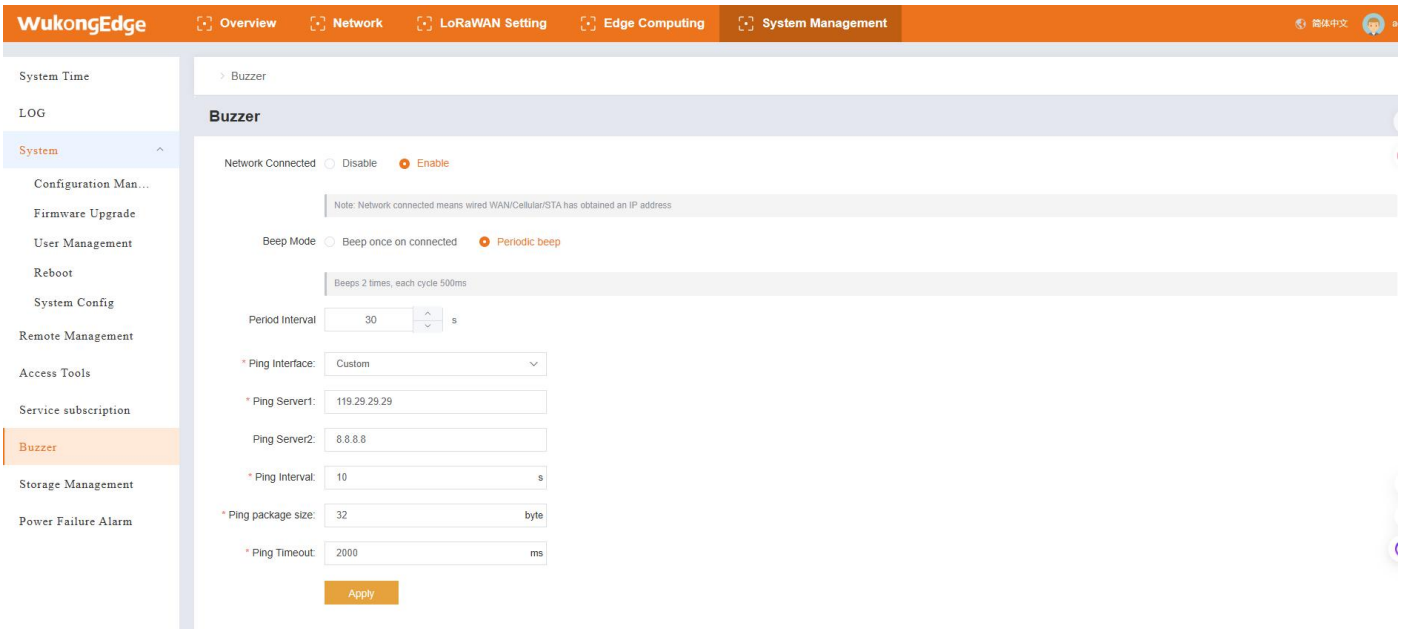
3.6.Storage Management

LG270provides an external TF card slot for customer secondary development. It does not come with a TF card by default; customers need to purchase it separately.



3.7.Buzzer

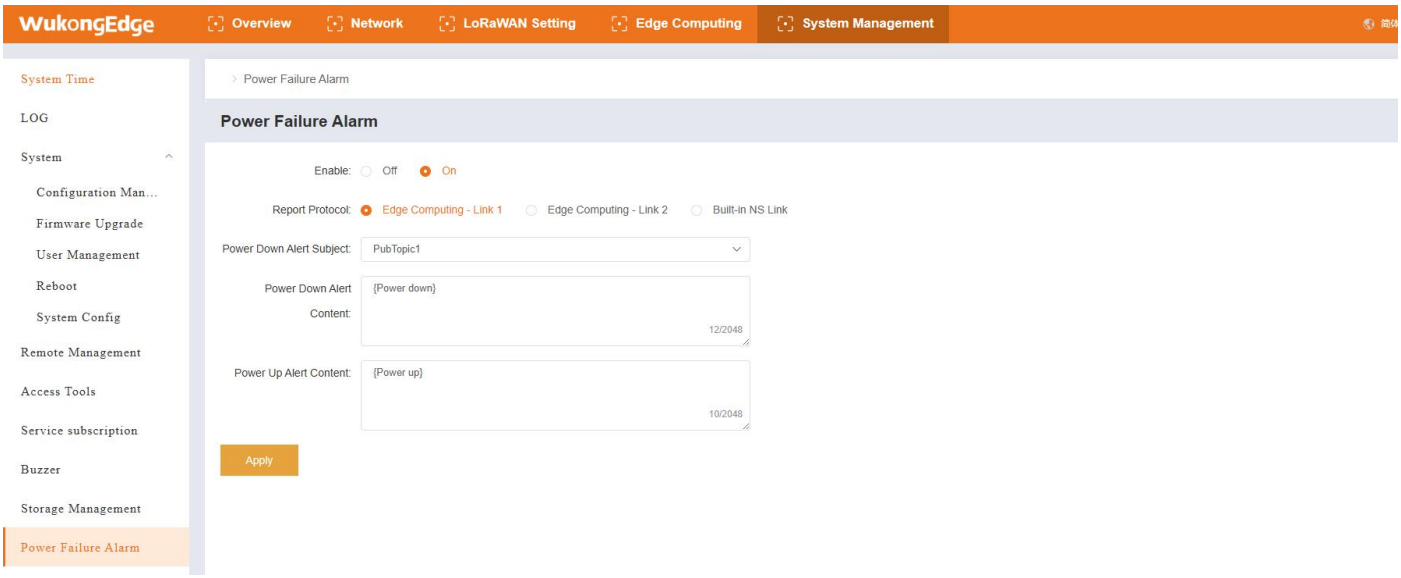
The buzzer is mainly used to indicate the product's network connection status. This function is disabled by default, and users can manually enable it.



3.8.Power-off Alarm

The USR-LG270 has a built-in large-capacity capacitor. After external power is disconnected, the capacitor can continue to supply power for 5-10 seconds. When the power-off alarm is enabled, the device detects the disconnection of external power and actively reports a power-off alarm message to the specified server.

Currently, the reporting links include Edge Computing - Link 1, Edge Computing - Link 2, and the built-in NS link.



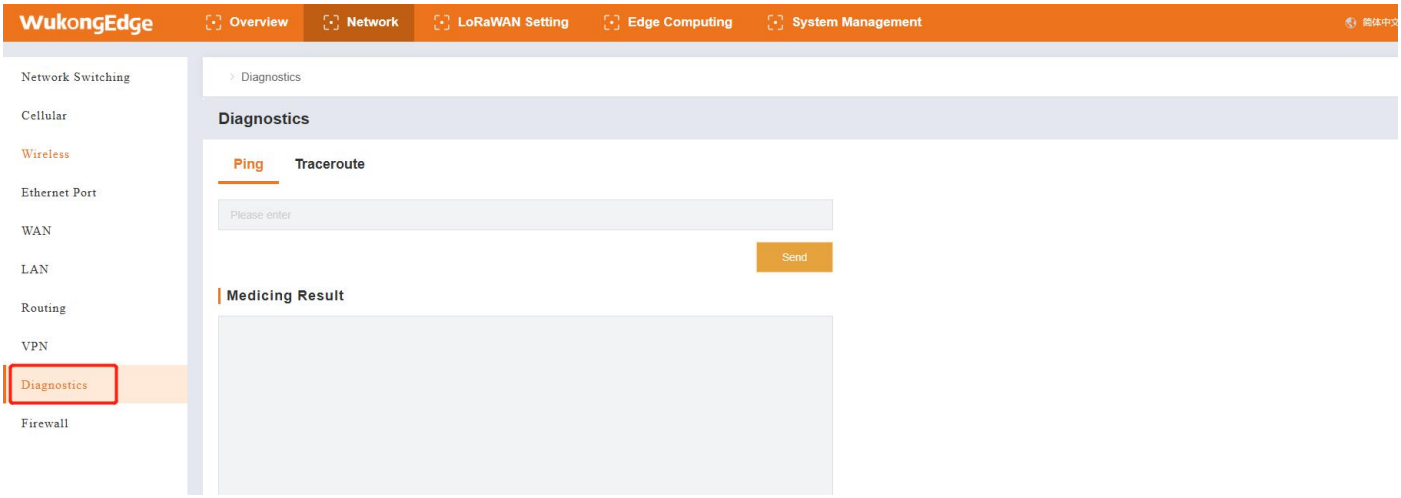
4. Network Management

WukongEdge application offers comprehensive integration of network functions, providing users with ultimate network flexibility and stability.

It supports various access methods including cellular networks, Ethernet, and Wi-Fi, meeting network connection needs in different scenarios. Whether relying on cellular networks for data communication in mobile operations, or achieving high-speed and stable network access through Ethernet or Wi-Fi in fixed locations, it can be easily realized.

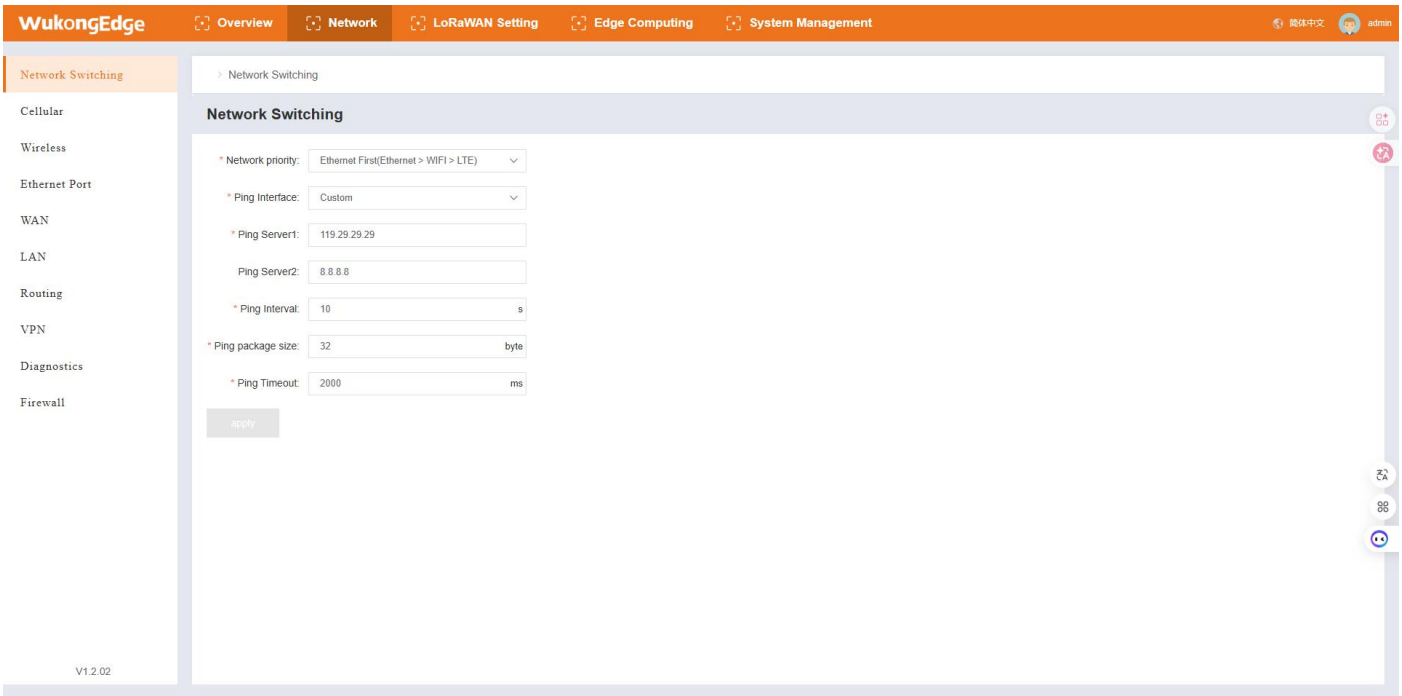
More importantly, its integrated routing, VPN, and firewall functions build a rigorous network security protection system. The routing function ensures efficient data transmission, VPN helps users securely establish private network connections over public networks, and the firewall monitors network traffic in real-time to resist various potential network attacks, comprehensively protecting users' network security.

Furthermore, the WukongEdge application is equipped with powerful network diagnostic functions, supporting multi-network backup and multi-link internet access. When the primary network fails, the system can automatically switch to the backup network link to ensure continuous and stable network connection. Meanwhile, the network diagnostic function can monitor network status in real-time and quickly locate fault points, greatly improving network operation and maintenance efficiency, providing solid guarantee for business continuity.



4.1.Network Switching

The network switching function is mainly used to set the priority order of network usage in multi-network mode. Under this function, the system will prioritize the network with higher priority. Once the high-priority network is disconnected, the system will automatically switch to the lower-priority network in the preset order, thereby ensuring the stability and continuity of the network connection.



Parameter Introduction:

Name	Parameter Description	Default Parameter

Network Priority	The preferred network for connection. If the preferred network cannot connect, it will automatically switch to the alternative network.	Ethernet First
Detection Mode	Custom: Determine network status based on custom detection addresses. Gateway: Detect WAN gateway address to determine network status.	Custom
Detection Address 1	When the detection mode is custom, this address is pinged first for communication detection. A reply indicates normal network, while no communication indicates detection failure.	119.29.29.29
Detection Address 2	When the detection mode is custom, if Detection Address 1 fails, Address 2 will be used for ping operation. A successful ping indicates normal network.	8.8.8.8
Detection Cycle	Set link detection interval: configurable from 1-600s.	10s
Ping Packet Size	Ping packet data size for link detection: configurable from 32-1024 bytes.	32 bytes
Ping Timeout	Ping timeout: configurable from 100-20000ms.	2000ms

Network Priority Description:

Network Priority	**Description**
Ethernet First (Ethernet->WIFI->Cellular)	The device prioritizes Ethernet for networking. If Ethernet detection fails, it switches to WiFi. If WiFi detection fails, it connects to the cellular network. The three networks are attempted in sequence.
Ethernet First (Ethernet->Cellular->WIFI)	The device prioritizes Ethernet for networking. If Ethernet detection fails, it switches to the cellular network. If cellular detection fails, it connects to WiFi. The three networks are attempted in sequence.
WiFi First (WIFI->Ethernet->Cellular)	Same as Ethernet First, only the priority order is different.
WiFi First (WIFI->Cellular->Ethernet)	Same as Ethernet First, only the priority order is different.
Cellular First (Cellular->Ethernet->WIFI)	Same as Ethernet First, only the priority order is different.

Cellular First (Cellular->WIFI->Ethernet)	Same as Ethernet First, only the priority order is different.
Ethernet Only	Communication is only possible via Ethernet; other networks are disabled.
Cellular Only	Communication is only possible via cellular network; other networks are disabled.
WiFi Only	Communication is only possible via WiFi; other networks are disabled.

4.2.Cellular Network

4G/5G Support: WukongEdge supports 4G/5G networks, allowing it to utilize high-speed mobile networks for data transmission and other operations. This provides users with faster data transfer speeds and lower latency, meeting network performance requirements in various scenarios.Device

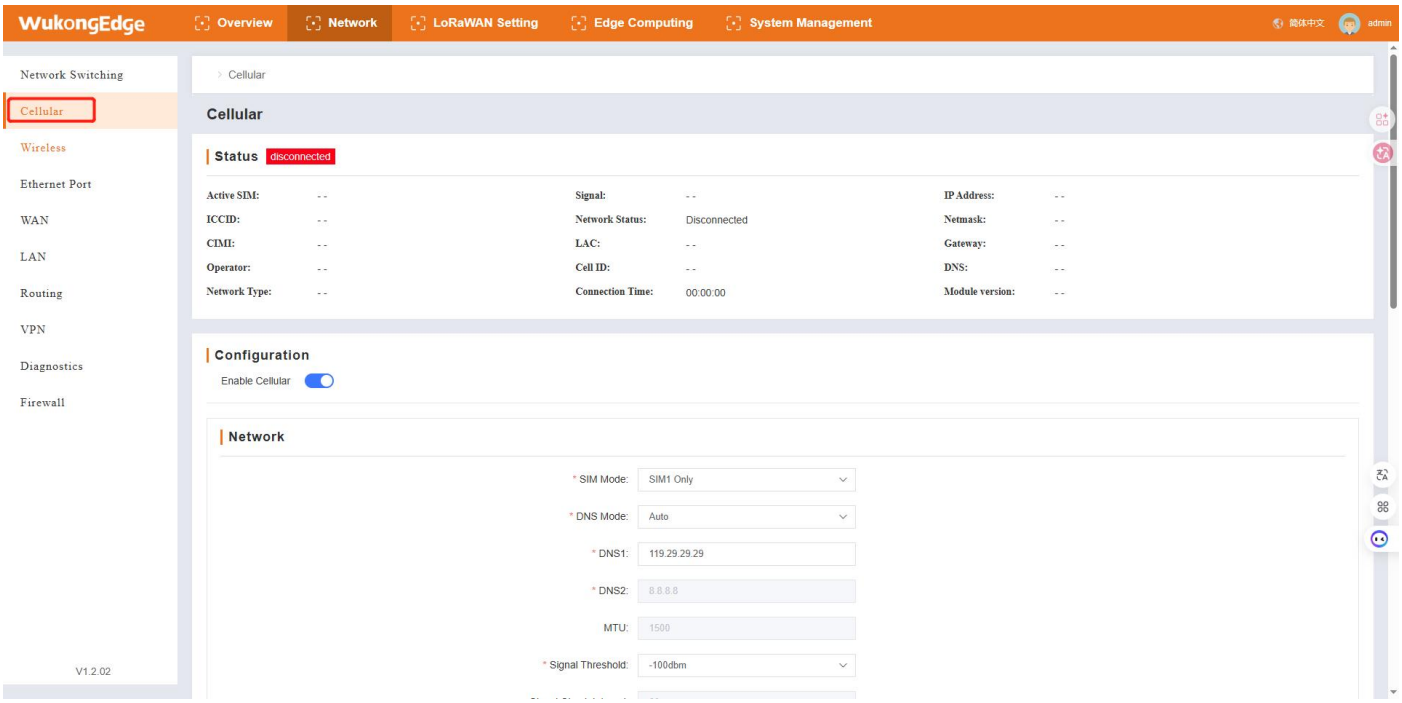
Compatible Modules:Quectel EG800, QuectelEG25, Fibocom NL668, TD Tech MT5710P-CN, USR GM5/G401tf.

Dual SIM Single Standby: The device adopts a dual SIM single standby design, meaning two SIM cards can be inserted, but only one card's network can be used at a time. This design allows users to flexibly choose which card's network service to use based on different needs, such as different data plans or network coverage conditions.

Automatic Detection: It features built-in network and signal detection modes, capable of automatically identifying available network types and signal strength. This enables the device to make intelligent decisions based on actual network conditions, such as automatically attempting to switch to a 5G network (if supported and available) when the 4G signal is poor.

Automatic Switching: Through the automatic switching function, WukongEdge can seamlessly switch between different networks or different signal sources within the same network. This ensures stable cellular network connectivity, reduces connection interruptions caused by signal fluctuations or failures, and improves the user's network experience.

This design and feature set give WukongEdge high flexibility, stability, and adaptability in cellular network connectivity, better meeting the network needs of various application scenarios.



Application Configuration:

- Enter the built-in web page, find "Network->Cellular Network", and enable the cellular network.
- Configure dual SIM mode according to the actual hardware product situation, and configure detection;
- Configure SIM1 and SIM2 parameters such as APN. If single SIM mode is selected, then only the selectedSIM card needs to be configured;
- After configuration is complete, click the "Apply" buttonto complete the configuration. The changes take effect immediately after application.

Parameter Introduction:

Name	Parameter Description	Default Parameter
Dual SIM Mode	Use the preferred SIM card for the first dialing. Supports four modes. "SIM1 Only" and "SIM2 Only" are single-SIM modes.	SIM1 Priority
DNS Acquisition Method	Automatic: Automatically obtain DNS server address from the base station. Manual: Manually set the address of the DNS resolution server.	Automatic
DNS1	Configurable DNS server IP	119.29.29.29
DNS2	Configurable DNS server IP	8.8.8.8
MTU	Maximum Transmission Unit, in bytes, range 128~1500	1500
Signal Threshold	If the average value of the current SIM signal detected within a certain period is less than the set threshold, it will switch to the other card for networking.	-100dbm

Signal Query Interval	The interval between two signal queries for the current SIM, range 1~3600	60s
Max Dial Attempts	When the preferred SIM fails to dial successfully within the set maximum number of attempts, the device will switch to the other SIM for dialing.	3
Link Detection	Detect whether the link is smooth by Ping.	SIM1&SIM2
Detection Interval	Ping time interval, range: 5~86400s	10s
Detection Count	Continuous failure peak. Redial after reaching this count, range 1~100	4
Detection Timeout	Maximum waiting time for a reply in a single detection. If no reply is received after timeout, the detection fails.	5s
Detection Address 1	Ping address 1. If this address can be pinged, it means the network is smooth.	119.29.29.29
Detection Address 2	Ping address 2. If this address can be pinged, it means the network is smooth.	8.8.8.8

SIM card setting parameters are as follows:

Name	Parameter Description	Default Parameter
APN	Used to identify the service type of WCDMA/LTE network, range 0~62 characters	Empty
Username	Specify the username of the user accessing the external PDN network, range 0~62 characters	Empty
Password	Specify the password of the user accessing the external PDN network, range 0~62 characters	Empty
Authentication Method	Authentication method, supports NONE, PAP, CHAP, PAP&CHAP four methods	NONE
Network Type	Supports Auto, 4G, 3G, 2G four networks	Auto
PIN Code	PIN code is the personal identification password of the SIM card. After enabling, the correct PIN code needs to be set to dial normally. PIN code range 4~8 characters	Disabled
Network Mode	Supports Auto, 4G, 3G, 2G four networks	Auto

4.3.Wireless WiFi Network

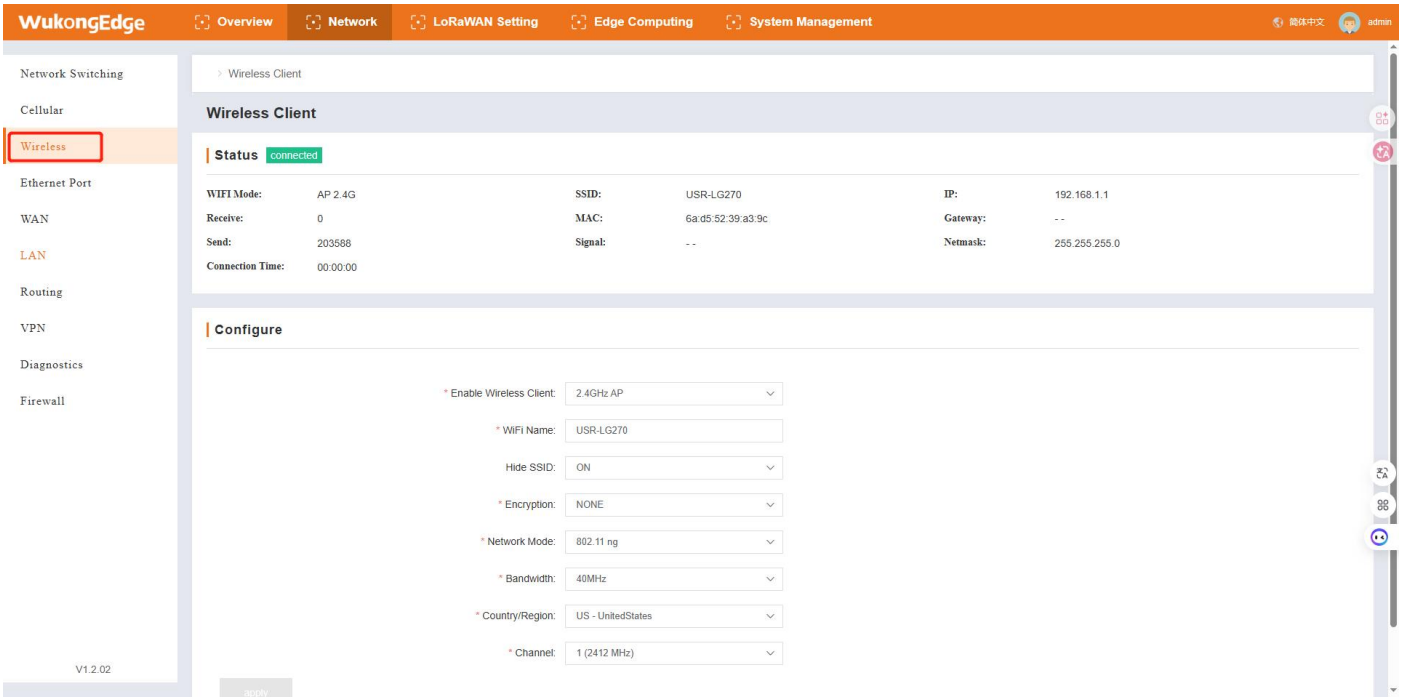
WukongEdge integrates Wi-Fi network management function, supporting AP and STA modes. USR-LG270 integrates dual-band WiFi6 network card, supporting both 2.4G WiFi and 5.8G WiFi.

AP Mode: USR-LG270 emits wifi signal, users can access LG270's network by connecting to WiFi to

configure parameters or communicate data with LG270; Note: 2.4G AP and 5.8G AP cannot be used simultaneously.

STA Mode: USR-LG270 accesses the upper-level network as a WiFi client, realizing the connection between LG270 and the upper-level network.

AP and STA cannot be used simultaneously.



Name	Parameter Description	Default Parameter
WirelessMode	Select WiFi working mode: Off/Wireless Client/2.4G Wireless Hotspot/5.8G Wireless Hotspot	5.8G Wireless Hotspot
Wi Fi Name	In AP mode: Display the wireless WiFi name of the hotspot In STA mode: You can manually enter the WiFi name to connect, or manually click search to select the network name to join	USR-LG270-XXXX (Last four digits of MAC)
Hide SSID	This option is only available in AP mode OFF: The WiFi hotspot broadcasts normally, and users can search for the WiFi signal in nearby networks ON: The WiFi hotspot broadcasts normally, but users cannot search for the WiFi signal in nearby networks. By manually entering the WiFi name, you can connect to the network normally;	OFF
Encryption Method	Two options,NONE/Mixed-psk	NONE
Password	Valid when encryption method isMixed-psk: AP mode: The password required for other WiFi devices to access the network; STA mode: The WiFi password of the upstream network to be accessed needs to be entered;	Empty

Network Mode	5.8G AP: 802.11 a/na/ac/axa 2.4G AP: 802.11 b/g/bg/ng/axg	802.11 ac
Bandwidth	5.8G AP: Auto/20/40/80 2.4G AP: Auto/20/40	80MHz
Country/Region	APmode parameter: AR-KE	US
Channel	2.4G AP mode: Channels 1-13 5.8G AP mode: The displayed channels vary depending on the country code	140
Network Mode	STA mode parameters: DHCP: IP address assigned by the upstream network Static: Manually set IP address	DHCP
DNS Acquisition Method	Auto Configuration/Manual Configuration	Auto Configuration

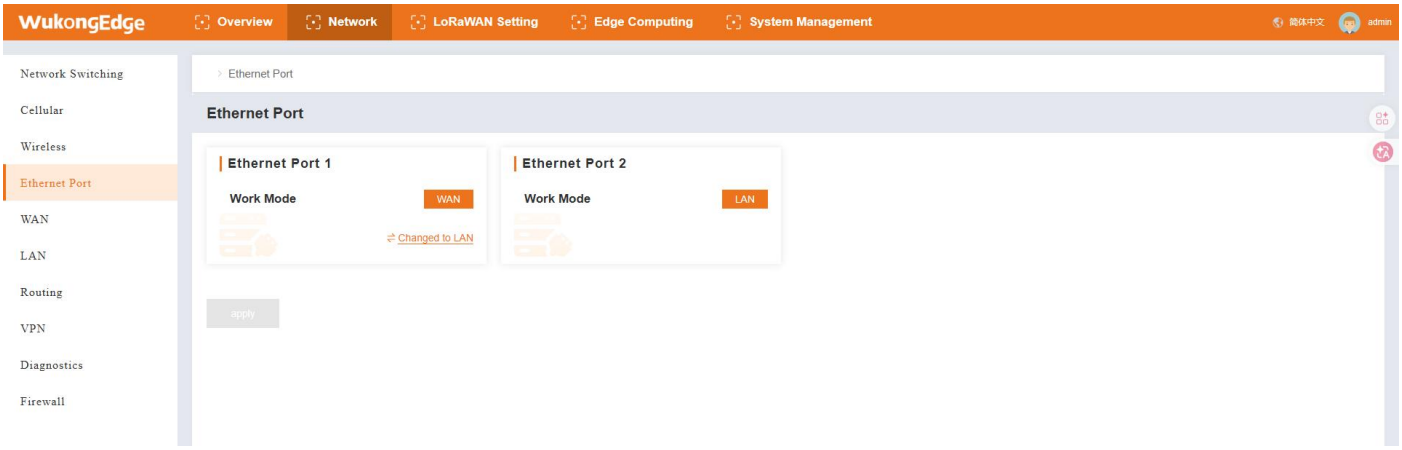
4.4.Ethernet Port Management

Ethernet management covers port mode management, WAN port configuration management, and LAN port management. The interface adaptation is flexible, where the port mode can switch between WAN and LAN modes. The WAN port is responsible for connecting to external networks, such as Internet Service Providers, ensuring device access to the wide area network and enabling data transmission and reception. The LAN port is used to build a local area network, facilitating interconnection of internal devices such as computers and printers, and enabling fast data sharing and exchange. Under the management of WukongEdge, WAN and LAN work together to meet the needs of different network application scenarios.

For dual-port devices, ETH1 is generally defaulted to WAN with DHCP function enabled by default, while the remaining ports are LAN, with a default address of 192.168.1.1 and built-in DHCP Server function. After connecting directly to a computer, it can assign IP addresses to PCs.

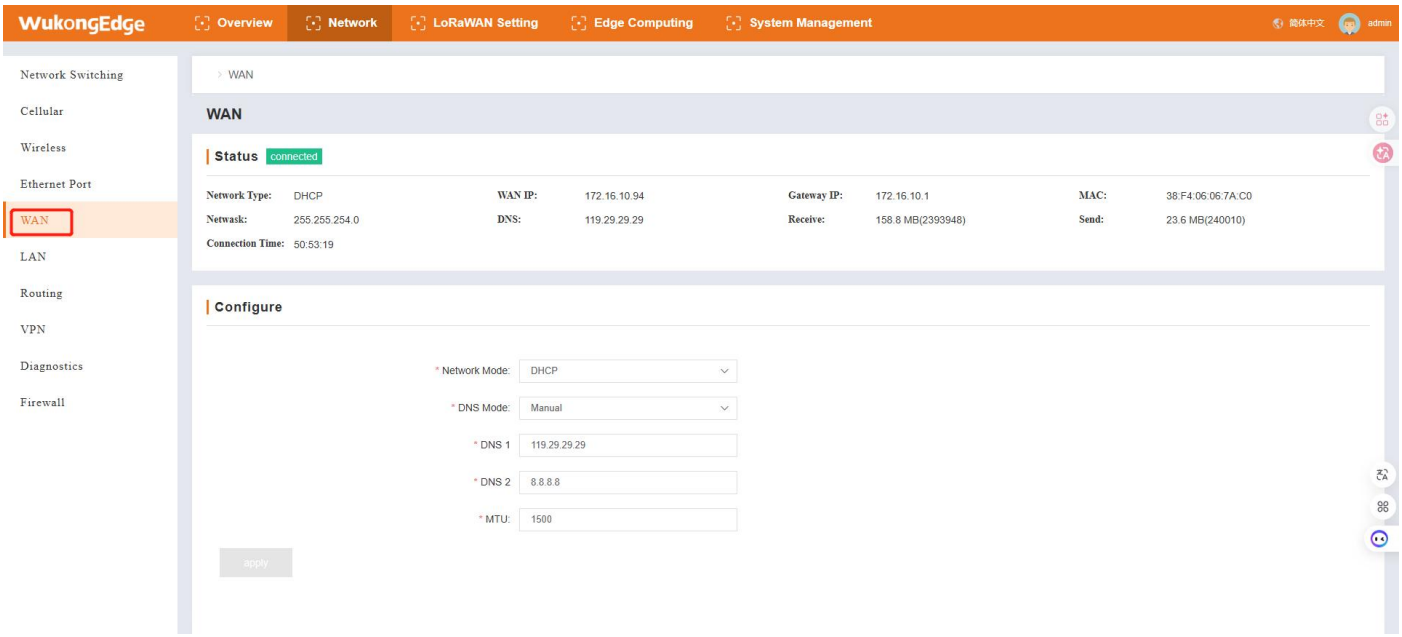
In the built-in web page, switch in the "Network -> Gateway Management" interface. After switching and clicking apply, a restart prompt will appear. This function requires a restart to take effect.

(Hardware port function switching**requires re-initialization**to ensure normal port communication).



4.5.WAN Port Management

The WAN port management built-in interface is divided into status management and parameter configuration. Status displays key information such as connection status and IP address, while parameter configuration is used to set the IP address acquisition method and address configuration. After setting the parameters, click apply to take effect immediately.



Parameter Management:

Name	Parameter Description	Default Parameter

Network Mode	DHCP (Dynamic IP): WAN acts as a DHCP client, using DHCP to obtain an IP address Static IP: Manually configure IP address, subnet mask, and other information for the Ethernet interface	Multi-port: DHCP
Static Address	In Static IP mode, manually configure the device's IP address for network identification	192.168.0.7
Subnet Mask	In Static IP mode, the WAN subnet range	255.255.255.0
Gateway	In Static IP mode, the WAN port gateway address	192.168.0.1
DNS Acquisition Method	Automatic Configuration: Automatically obtain DNS server addresses from the public network Manual Configuration: Manually set DNS server addresses, suitable for LAN communication	Manual Configuration
DNS1	Configurable DNS server IP	119.29.29.29
DNS2	Configurable DNS server IP	8.8.8.8
MTU	Maximum Transmission Unit, in bytes, range 128~1500	1500

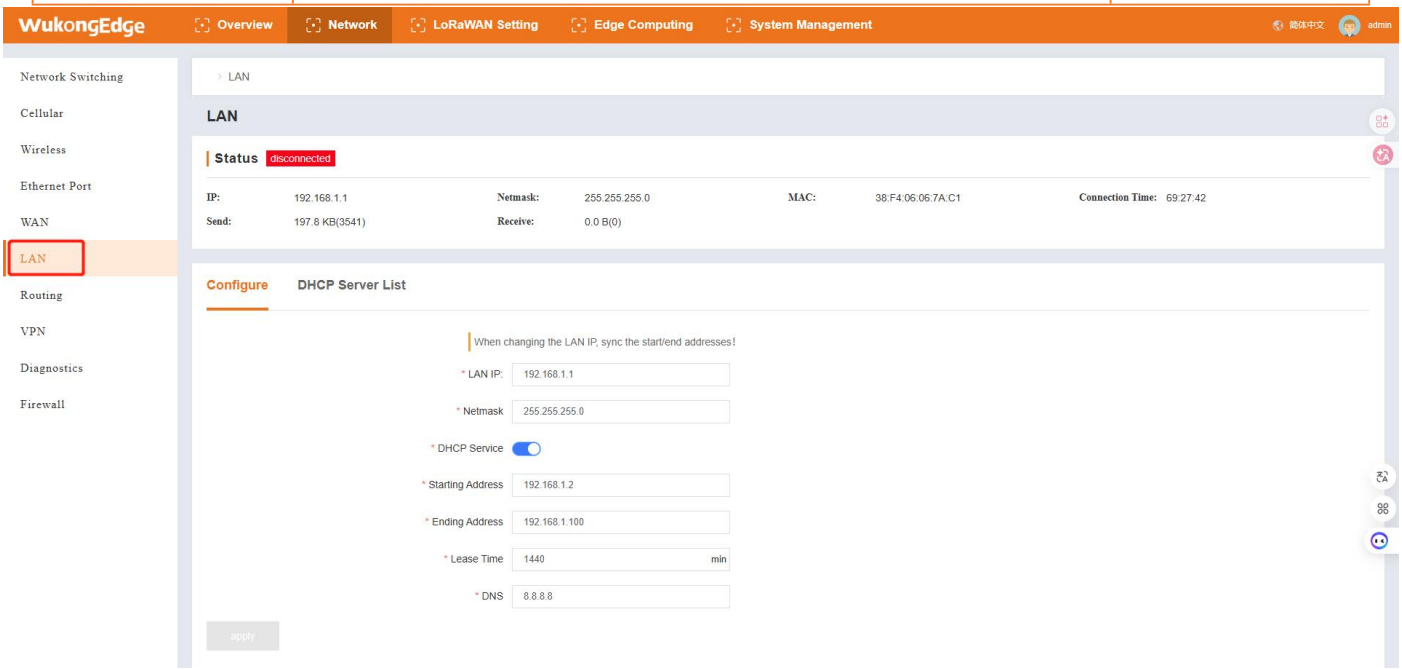
4.6.LAN Port Management

LAN port management covers status display, parameter configuration, and DHCP server. Status display shows real-time status; parameter configuration allows setting relevant parameters as needed; the DHCP server assigns IPs to downstream devices and displays them in a list, and can also assign static addresses to match fixed MAC address devices with fixed IPs. All LAN port configurations take effect immediately after application.

Parameter Description:

Name	Parameter Description	Default Parameter

LAN IP	LAN IP address, which can serve as the gateway for the local area network formed by clients connected to the LAN port	192.168.1.1
Subnet Mask	LAN subnet range	255.255.255.0
DHCP Service	The function of assigning addresses to clients connected to the LAN port, enabled by default, can be disabled	Enabled
Start Address	Set the starting IP address assigned to client devices in the address pool	192.168.1.2
End Address	Set the ending IP address assigned to client devices in the address pool	192.168.1.100
Lease Time	Set the validity period of the assigned IP addresses. Upon expiration, the DHCP server will reclaim the IP addresses assigned to clients and reassign them. This field cannot be empty	1440min
DNS Server Address	DNS server address for domain name resolution for LAN clients. If changed to the gateway, it will use the WAN port proxy DNS by default	8.8.8.8



4.7.Routing

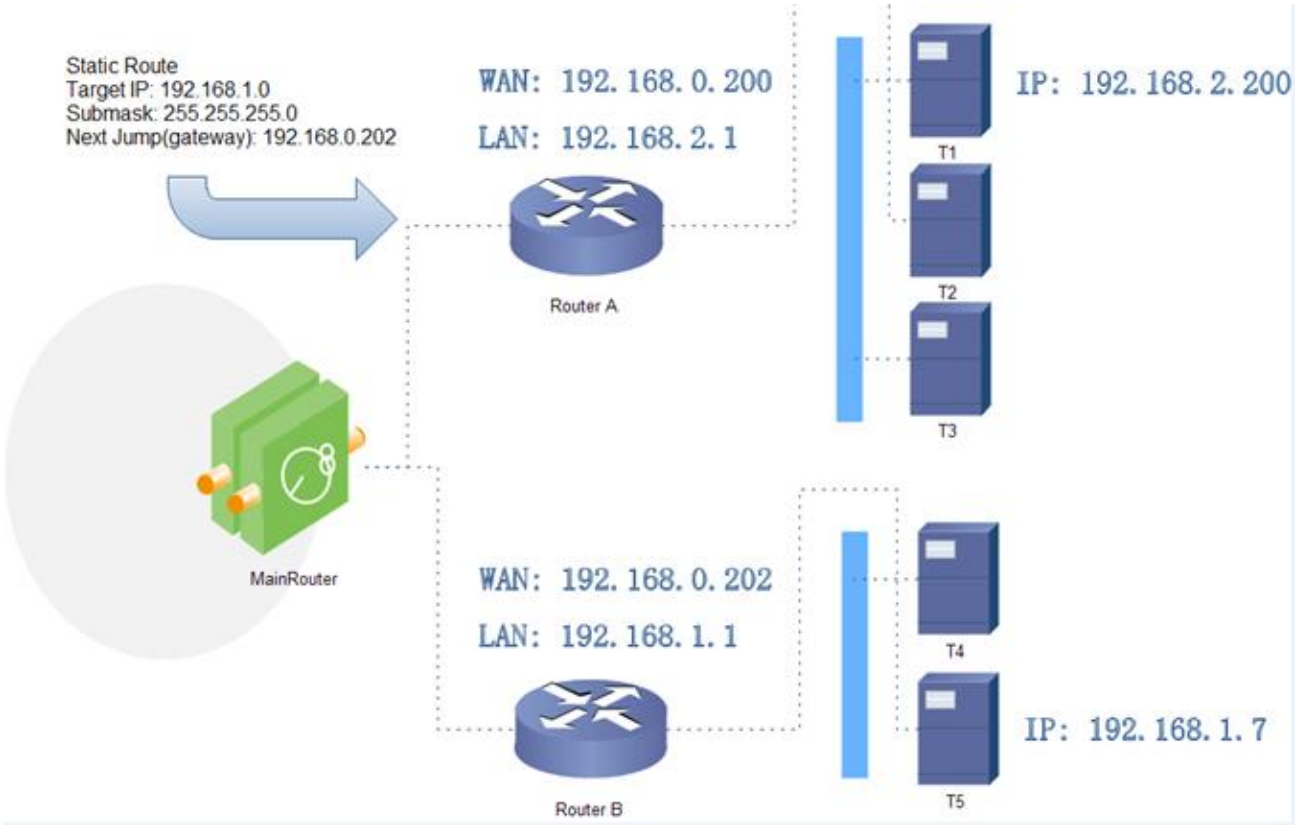
Static routing in the routing function is a key feature. It is easy to operate, and users do not need complex professional knowledge. They can easily complete the configuration and put it into use by filling in

basic information such as destination network address, subnet mask, and next hop address on the device's built-in web page according to their own network needs.

Parameter Description:

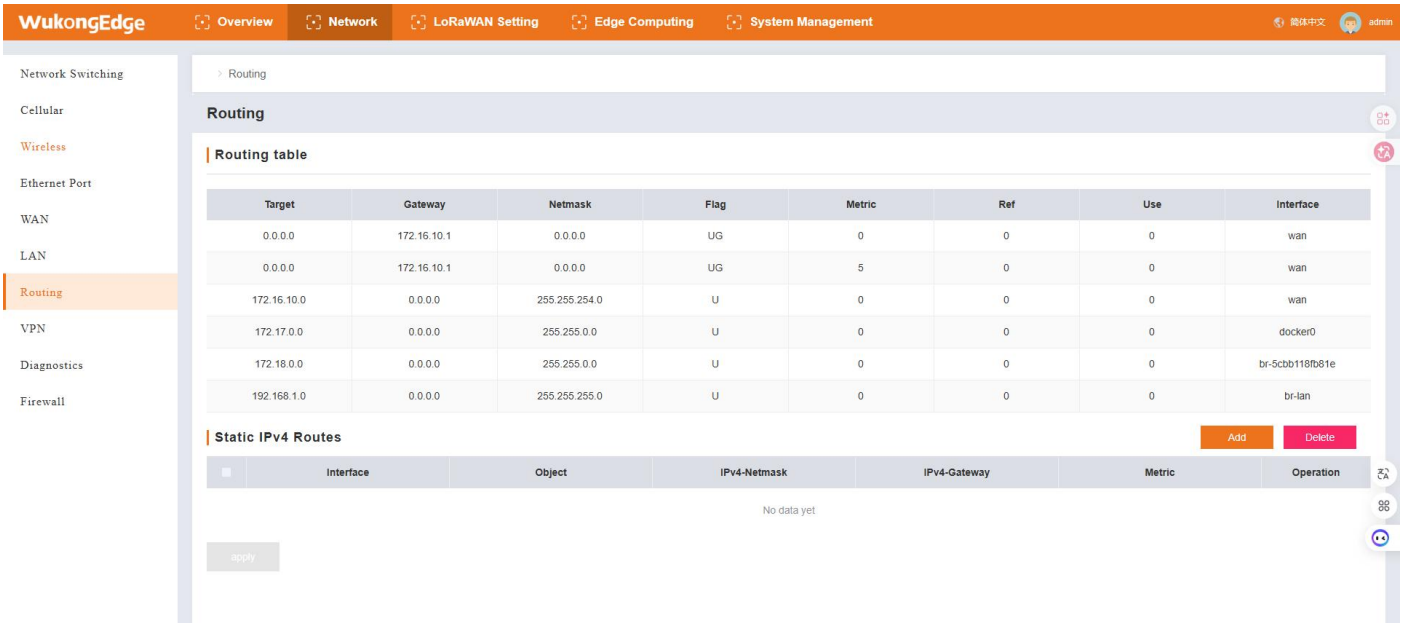
Name	Parameter Description	Default Parameter
Interface	The interface used for data to reach the destination network	Empty
Destination Network	The destination IP address to be reached	Empty
IPv4 Subnet Mask	The subnet mask of the destination address to be reached	Empty
IPv4 Gateway	The IP address of the next router that data must pass through before reaching the destination address	Empty
Metric	That is, priority. The smaller the value, the higher the priority. Range: 0-255	0

Static routes can be illustrated by the following example to show how routing is used. The example diagram is as follows:



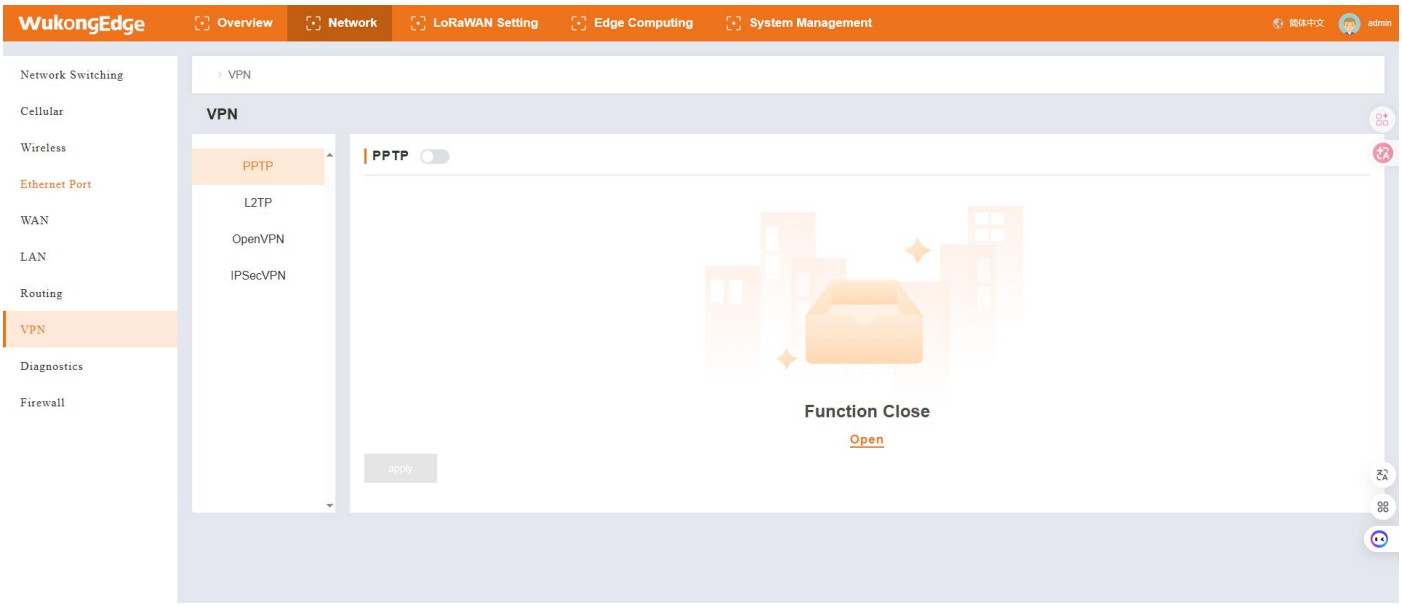
The WAN ports of Router A and B are both connected to the 192.168.0.0 network. The LAN port of Router A is in the 192.168.2.0 subnet, and the LAN of Router B is in the 192.168.1.0 subnet. Now, if we want to create a route on Router A so that when we access 192.168.1.x addresses, they are automatically forwarded to

Router B. Since we want to forward to all 192.168.1.x subnets, the subnet mask should be set to 255.255.255.0 when adding the route. If the target IP is set to a fixed IP address, such as 192.168.1.7, the subnet mask should be set to 255.255.255.255.



4.8.VPN

The VPN function plays a key role in networking scenarios, supporting four mainstream protocols: PPTP, L2TP, OpenVPN, and IPSec VPN. Each protocol has its own advantages, meeting diverse networking needs for network security, stability, and compatibility.



Operation Steps:

Enter the built-in web page, find the "Network -> VPN" interface, and select the corresponding VPN connection method.

For example, if you select PPTP, after selecting PPTP, enter the PPTP parameter interface and first enable

it.

After enabling, the status information bar and parameter configuration will appear. Fill in the required parameters accordingly, and then click the "Apply" button.

After applying, it will take effect immediately. Check the connection status in the status bar. When the corresponding connection information is displayed, it proves that the VPN has been successfully connected.

4.8.1. PPTP Client

PPTP, as a Point-to-Point Tunneling Protocol, maintains the tunnel via a TCP (port 1723) connection. It uses Generic Routing Encapsulation (GRE) technology to encapsulate data into PPP frames for transmission through the tunnel. It can also encrypt or compress the payload data within the encapsulated PPP frames; for instance, MPPE uses encryption keys generated by MS-CHAP V2 authentication to encrypt PPP frames.

Before use, you need to obtain the VPN server address, username, password, and encryption method. After enabling the PPTP client function, fill in these parameters accurately. Once the VPN is active, you can check its status in the status information section.

Parameter Description:

Name	Parameter Description	Default Parameter
Server Address	Enter the IP address or domain name of the VPN server to connect to	192.168.0.2
Interface	Depending on the networking method, you can choose Auto, WAN, or LTE 4G	Auto
Username/Password	Obtain this information from the VPN server; limited to 1~50 characters	username/password
Remote Subnet & Mask	If filled correctly, subnet communication under VPN can be directly achieved when NAT is enabled	192.168.55.0/255.255.25.0
NAT	When content needs to communicate with the outside, replace internal addresses with public addresses. If this item is disabled, Network Address Translation functionality will not be available	Disabled
MPPE Encryption	Encrypts and decrypts data between both parties to prevent unauthorized access and changes.	Disabled
MTU	Maximum Transmission Unit, in bytes, range 128~1500, should be the same as the VPN server	1500
Additional Configuration	Append PPPD parameters, magic numbers, etc. No operation is required by default, 0~500 characters	Empty
Static Tunnel IP Address	The server automatically assigns an IP; you can fill in the static tunnel IP here	Disabled

Ping Check	Real-time VPN online detection and reconnection mechanism. Ensures stable connection by cyclically pinging a custom IP. Disabled by default	Disabled

4.8.2. L2TP Client

L2TP is a Layer 2 Tunneling Protocol, similar to PPTP. In the M300 device, it supports multiple authentication methods such as tunnel password authentication and CHAP, while using L2TP OVER IPSec pre-shared key encryption. Users only need to go to "Network" -> "VPN" -> "L2TP", fill in the corresponding settings, and once the VPN is active, they can view the VPN status in the status information section.

Parameter Description:

Name	Parameter Description	Default Parameter
Server Address	Enter the IP address or domain name of the VPN server to connect to	192.168.0.2
Interface	Depending on the networking method, you can choose Auto, WAN, or LTE 4G	Auto
Username/Password	Obtain this information from the VPN server; limited to 1~50 characters	username/password
Tunnel Name/Password	Obtain from the VPN server and fill in correctly	Empty
Remote Subnet & Mask	If filled correctly, subnet communication under VPN can be directly achieved when NAT is enabled	192.168.55.0/255.255.25.0
NAT	When content needs to communicate with the outside, replace internal addresses with public addresses. If this item is disabled, Network Address Translation functionality will not be available	Disabled
MTU	Maximum Transmission Unit, in bytes, range 128~1500, should be the same as the VPN server	1500
Additional Configuration	Append PPPD parameters, magic numbers, etc. No operation is required by default, 0~500 characters	Empty
Static Tunnel IP Address	The server automatically assigns an IP; you can fill in the static tunnel IP here	Disabled
Ping Check	Real-time VPN online detection and reconnection mechanism. Ensures stable connection by cyclically pinging a custom IP. Disabled by default	Disabled

4.8.3. OpenVPN

OpenVPN is an application-layer VPN solution built on the OpenSSL library, innovatively integrating virtual network cards with the SSL protocol. This unique design not only easily achieves networking goals but also significantly enhances connection security through the encryption features of the SSL protocol. Moreover, the operation process is extremely simple, making it easy for users to get started and highly practical.

Parameter Description:

Name	Parameter Description	Default Parameter
Tunnel Protocol	TCP, UDP	UDP
Remote Host IP Address	OpenVPN Server IP/Domain Name	192.168.1.102
Port	OpenVPN Server Listening Port	1194
Authentication Type	NONE, Username/Password, Pre-shared Key, SSL/TLS, SSL/TLS+Username/Password	
Topology	Subnet, Point-to-Point, Net30	Subnet
Interface	Depending on the networking method, you can choose Ethernet Port, 4G, or Auto	Auto
Redirect Gateway	Append PPPD parameters, magic words, etc. No operation is required by default, 0~500 characters	Empty
NTA	This function is enabled by default. When content needs to communicate with the outside, the internal address is replaced with a public address. If this item is disabled, the Network Address Translation function cannot be realized	Enabled
Keepalive	Enabled by default, requires setting the detection interval and timeout period	Enabled
LZO	Enable or disable LZO compression for data transmission	Adaptive
Encryption Algorithm	None/Blowfish-128/DES-EDE/DES-EDE3/AES-128/AES-192/AES-256	Blowfish-128
Hash Algorithm	None/SHA1/SHA256/SHA512/MD5	SHA1
TLS Method	tls-auth/tls-crypt/OFF	OFF

4.8.4. IPSec

IPSec VPN is a network-layer VPN solution built on the IETF standard protocol suite. It deeply integrates AH and ESP protocols and innovatively combines the IKE key exchange mechanism. This mature architecture not only easily implements end-to-end secure tunnels but also significantly enhances communication confidentiality through the data encryption and integrity verification features of the ESP protocol. Moreover, leveraging the advantage of native operating system support, the configuration process is standardized, making enterprise deployment efficient and highly practical.

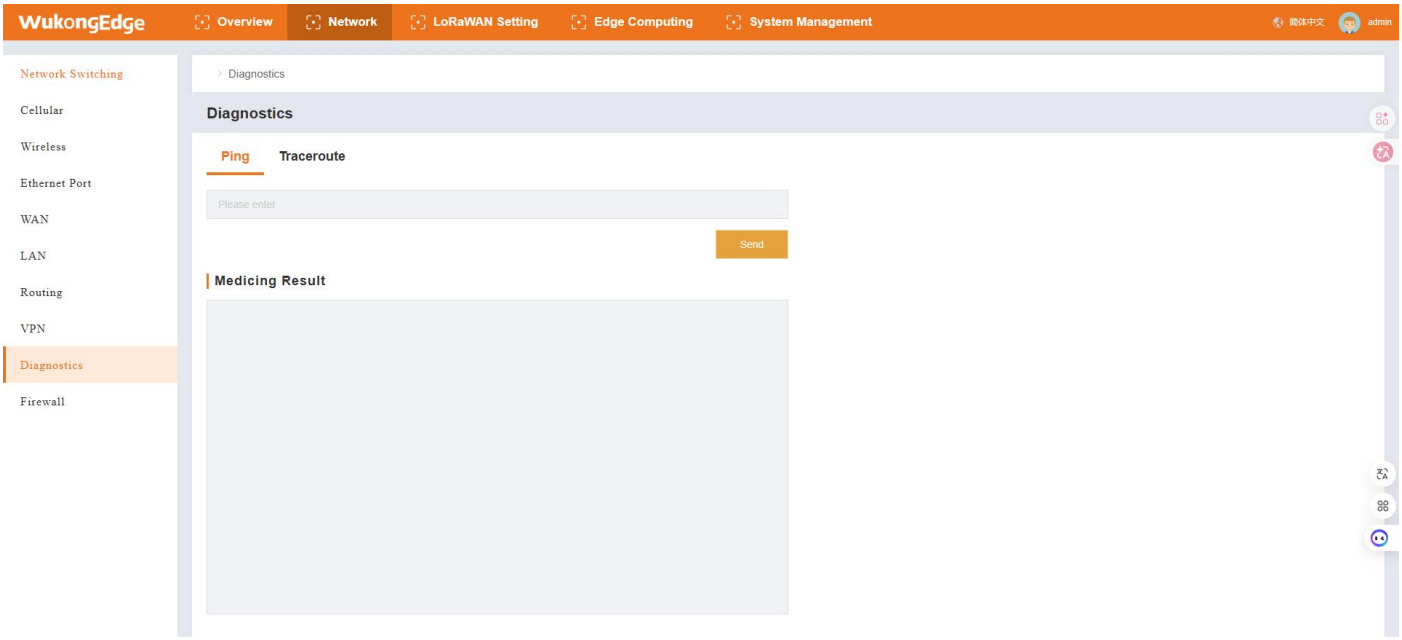
Parameter Description:

Name	Parameter Description	Default Parameter
Interface	Select Auto, Ethernet Port, 4G, or WiFi based on the networking method. Automode: If the currentinterface disconnects abnormally, it can automatically switch to another interface to attempt connection.	Auto
Peer Address	Enter the peer IP address or domain name.	192.168.4.173
Negotiation Mode	Select Main Mode or Aggressive Mode (Wild Mode).	Main Mode
Local Subnet Count	The number of local subnet segments, maximum 4, range 1-4 integer.	1
Local Subnet	Enter the local subnet segment, consistent with the remote subnet setting on the peer side. The maximum number of entries depends on the Local Subnet Count limit.	192.168.3.0/24
IKE Version	ikev2/ikev1, consistent with the peer configuration.	ikev1
IKE Encryption Algorithm	Select the IKE encryption algorithm, consistent with the peer configuration.	AES-128
IKE Authentication Algorithm	Select the IKE authentication algorithm, consistent with the peer configuration.	MD5
Diffie-Hellman Group	Select the DH group, consistent with the peer configuration.	Group2(1024bits)
IKE Lifetime	IKE lifetime setting, range 400~86400,unit: seconds	28800
Authentication Type	Pre-shared Key Type	Pre-shared Key
Pre-shared Key	Consistent with the peer configuration.	123456abc

Local ID	Consistent with the Remote ID setting on the peer side,range 1~63bytes	@client
Remote ID	Consistent with the Remote ID setting on the peer side,range 1~63bytes	@server
ESP Encryption Algorithm	Select the ESP encryption algorithm, consistent with the peer configuration.	AES-128
ESP Authentication Algorithm	Select the ESP authentication algorithm, consistent with the peer configuration.	SHA-1
PFS	Select PFS configuration, consistent with the peer configuration.	DH2
ESP Lifetime	ESP lifetime setting, range 400~86400,unit: seconds	3600
DPD Timeout	DPD timeout setting, range 1-3706,unit: seconds	60
DPD Check Interval	DPD check interval setting, range 1-3706,unit: seconds	60
DPD Action	Options: None/Delete/Hold/Restart	None

4.9.Network Diagnostics

The network diagnostics function covers the Ping tool and the route resolution tool. Through the router's Ping tool, you can directly perform ping tests on specific addresses to determine network connectivity and latency. Traceroute, as a route resolution tool, can obtain the routing path that data transmission passes through when accessing an address, helping to troubleshoot network faults.



4.10.Firewall

The firewall is a key line of defense for ensuring network security. It cleverly integrates various security management and filtering tools, constructing a relatively isolated protection barrier between the gateway's internal network and external network, thereby effectively safeguarding the data within the gateway. It possesses the following main tools:

Port Filtering: It can finely control ports entering and leaving the network based on preset rules, allowing only compliant port communications to pass and blocking illegal port access, greatly reducing the risk of network attacks.

Port Mapping: By mapping specific internal network ports to specified ports on the external network IP, it enables external users to access internal network services while hiding the real internal network IP, enhancing network security.

Port Forwarding: It can forward network traffic from specific ports to other specified IP addresses and ports, flexibly adjusting network data flow to meet the needs of different business scenarios.

DMZ (Demilitarized Zone): Establishes a special area between the internal network and the external network to place servers that need to provide services externally. This ensures external access to these services while restricting their access to the internal network, effectively isolating potential threats.

Operation Steps:

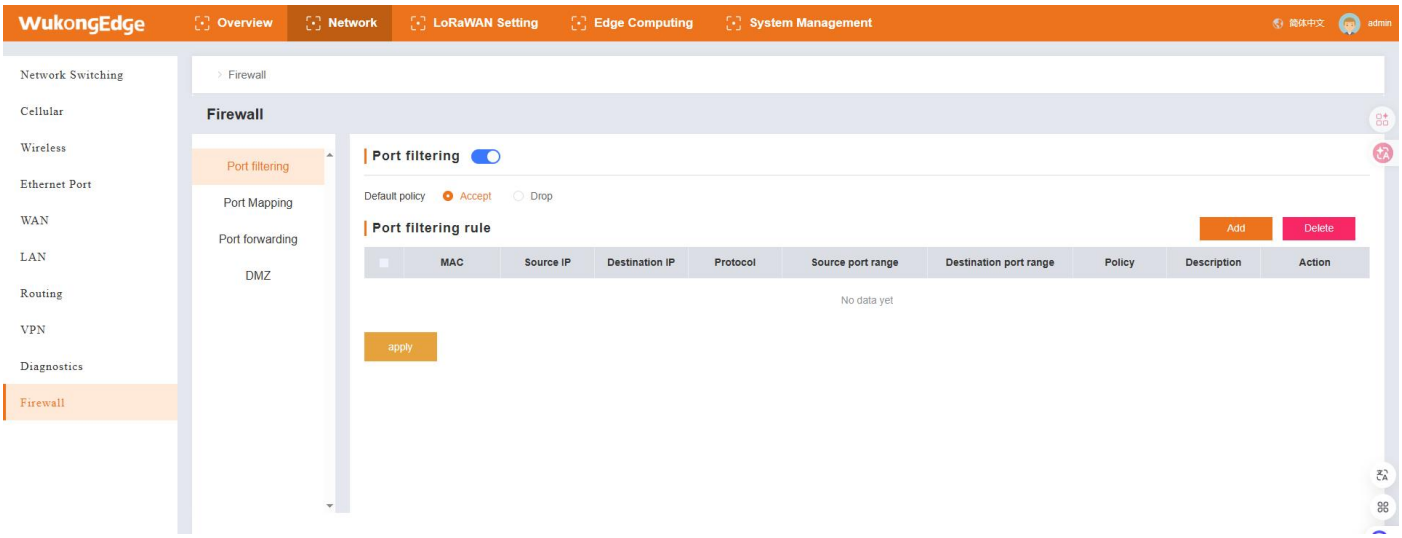
Enter the built-in web page, find the "Network -> Firewall" interface, and select the firewall option to configure;

For example, to configure port mapping, select Port Mapping. After entering the interface, enable it first, and the rule addition interface will appear.

In the parameter configuration interface, click the "Add" button to add a mapping rule;

After adding the parameters, click OK to complete the addition of one rule. Use the same method to add multiple rules;

After completing all rule settings, click the Apply button, and the application will take effect immediately.



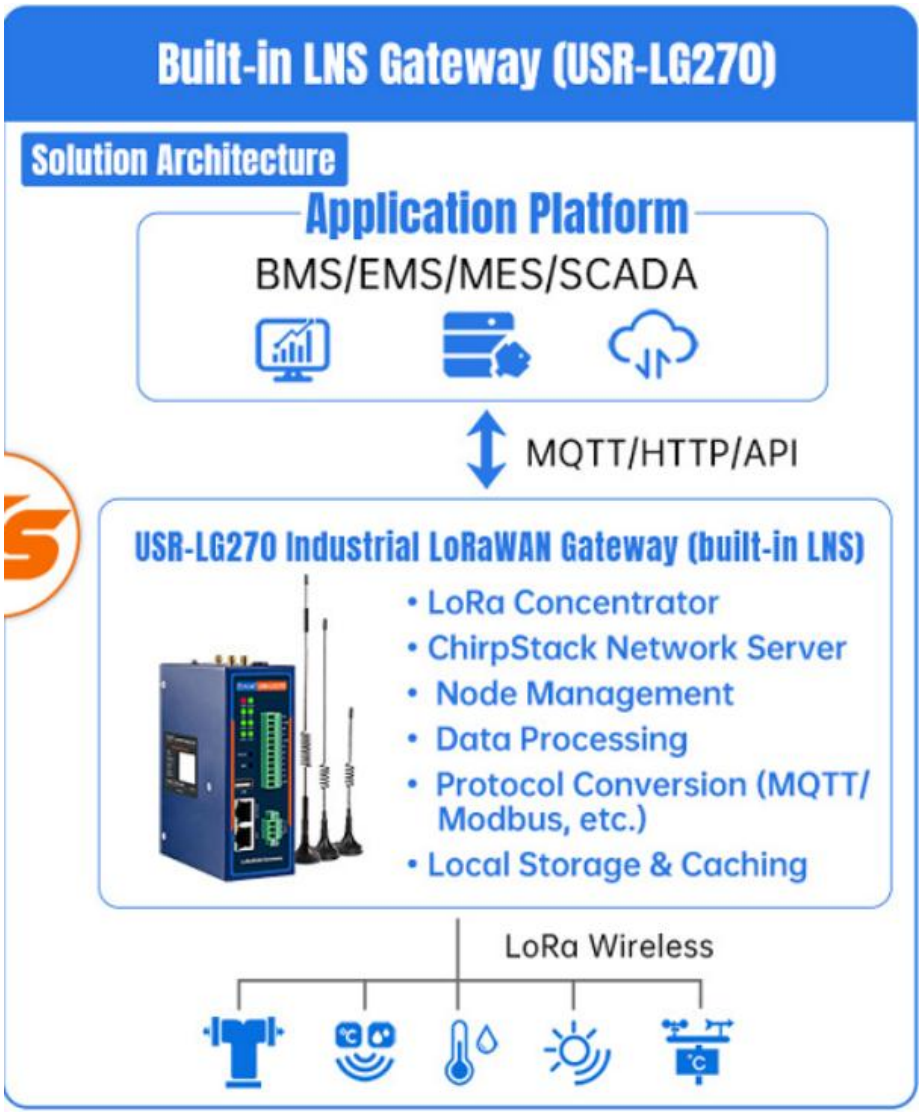
5. LoRaWAN

5.1.LoRaWAN Network Introduction

LoRaWAN (Long Range Wide Area Network) is a low-power wide-area network communication protocol oriented towards IoT applications. Based on LoRa wireless modulation technology, it is designed for large-scale, long-distance, low-power IoT device connections. LoRaWAN supports bidirectional communication, end-to-end security encryption, device management, and remote control functions, and can be widely used in industrial monitoring, smart cities, smart agriculture, energy management, and other fields.

Traditional LoRaWAN networks adopt a star-of-stars topology, consisting of End Devices, LoRaWAN Gateways, Network Servers, and Application Servers. LoRaWAN gateways usually serve only as wireless data forwarding devices (Packet Forwarders), responsible for receiving LoRa data sent by terminal nodes and uploading it to a remote Network Server via Ethernet, cellular networks, or Wi-Fi for device management, data parsing, and network control. This architecture relies on cloud servers, making system deployment complex, and has certain limitations in industrial environments where the network is unstable or public network access is unavailable.

USR-LG270 breaks through traditional gateway design by directly integrating the LoRaWAN Network Server (LNS)**within the industrial gateway**. Combined with powerful edge computing capabilities, the device can not only complete LoRa wireless access but also handle LoRaWAN protocol processing, device management, data analysis, and intelligent control locally, realizing an integrated industrial IoT solution of "Connectivity + Computing + Management", simplifying the LoRaWAN system architecture and reducing deployment costs.



5.2.LoRaWAN Network Components

From the introduction above, we know that the entire LoRaWAN network consists of End Devices, LoRaWAN Gateways, Network Servers, and Application Servers. The specific functions of each component are introduced below.

- LoRaWAN Nodes

LoRaWAN nodes are typically deployed on-site for: sensor data acquisition,industrial equipment status monitoring,environmental parameter detection,remote control execution, etc. Common LoRaWAN nodes include: temperature and humidity sensors, electricity meters, water meters, pressure sensors, industrial IO controllers, etc. LoRaWAN nodes communicate with nearby LoRaWAN gateways via LoRa wireless links.

- LoRaWAN Gateway

The LoRaWAN gateway is the bridge connecting the LoRa wireless network and the IP network. Its main functions are: receiving LoRa node data, forwarding LoRaWAN packets, issuing server control commands, and

managing wireless communication links. LoRaWAN gateways use multi-gateway collaborative communication. If there are multiple LoRaWAN gateways near a node and they share the same NS server, multiple gateways may receive data from the same node simultaneously, and all gateways will upload the received LoRaWAN data to the NS server.

- Network Server

The Network Server is the core management platform of the LoRaWAN network.It is mainly responsible for: device management, data processing, network optimization, and other functions.

Device Management:Node registration,OTAA network access authentication,DevEUI management, etc.;

Data Processing:Data validation,Data decryption,Data deduplication,Data forwarding, etc.;

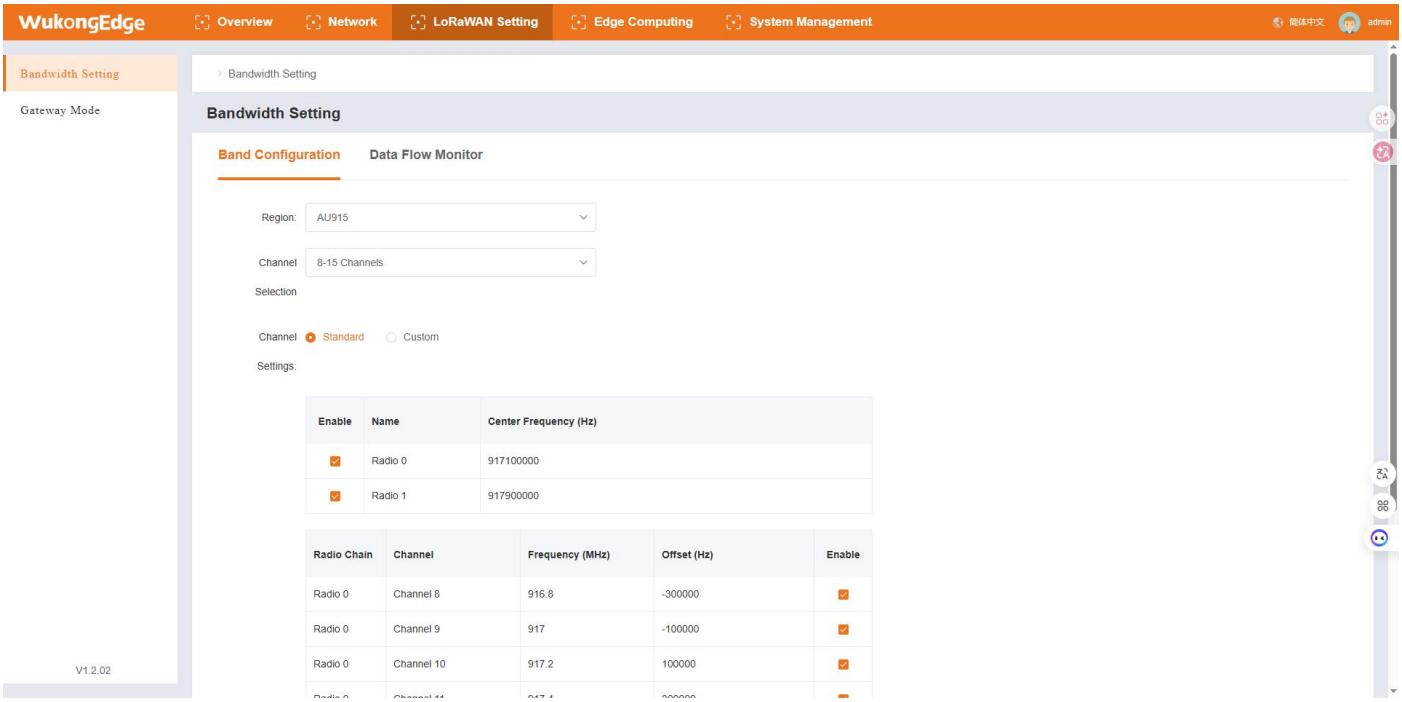
Network Optimization:ADR rate adjustment,Channel management,Downlink scheduling, etc.

- Application Server

The Application Server is responsible for handling user business logic. Main functions: Data storage,Data analysis,Visualization,Alarm management,Device control, etc. The Network Server and Application Server usually communicate data via MQTT(s), HTTP, TCP(s) protocols.

5.3.LoRaWAN Gateway Frequency Band Settings

Because the frequency bands and protocols used by the LoRaWAN protocol vary in different regions, you need to select the corresponding protocol based on the region.



Name	Parameter Description	Default Parameter
Region Selection	Options include: CN470/EU868/US915/AU915/AS923_1/AS923_2/AS923_3/AS923_4	CN470

Channel Selection	Some regions use multiple uplink channels, and LoRaWAN divides channels into multiple sub-bands. Gateways and end devices must be configured to the same sub-band to successfully complete device network access and data communication.	Channel 0-7
Channel Settings	Standard/Custom Standard: Different countries and regions have different regulations on the use of wireless spectrum, so the LoRaWAN Alliance has formulated corresponding Regional Parameters for different global regions. Standard mode means that each channel uses the frequency defined by this regional parameter specification. It is recommended that customers use standard channels for normal communication. Custom: Users can manually set the frequency of each channel to adapt to their application scenarios.	Standard

5.4.Gateway Mode Settings

USR-LG270 supports 3 different working modes: Built-in NS - Edge, Built-in NS, and Packet Forwarding.

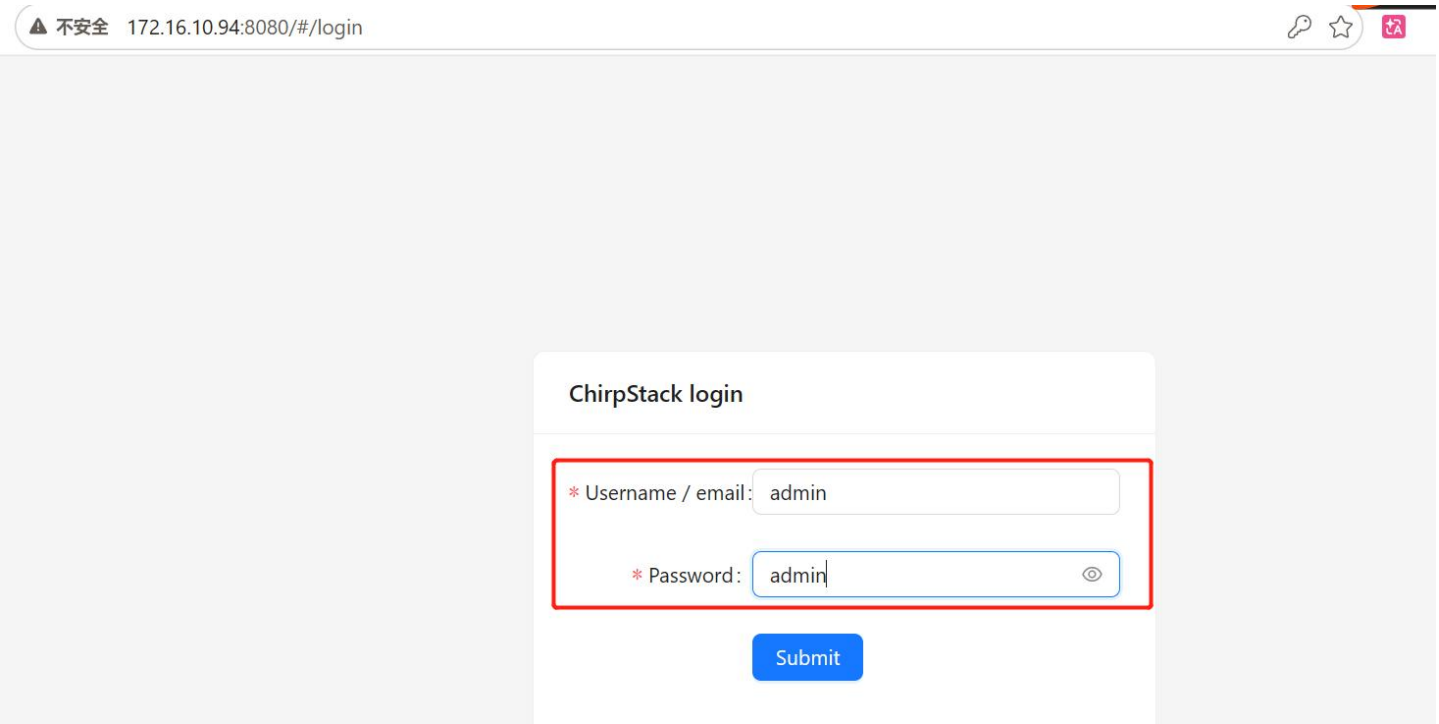
Built-in NS - Edge: Uses the built-in Chirpstack service of USR-LG270, and USR-LG270 acts as the host to actively issue commands to query data from terminal nodes. It implements localized processing based on the acquired data and can also report the collected data to external application servers.

Built-in NS: Uses the built-in Chirpstack server of USR-LG270 to connect to external application servers for data transmission.

Packet Forwarding: Does not use the built-in Chirpstack server, but connects to external NS servers (such as TTN, etc.) through packet forwarding to implement terminal node network access management, etc.

Chirpstack login address:http://192.168.1.1:8080/#/login, where 192.168.1.1 refers to the gateway address of USR-LG270

Login username/password: admin/admin



5.4.1. Built-in NS Mode

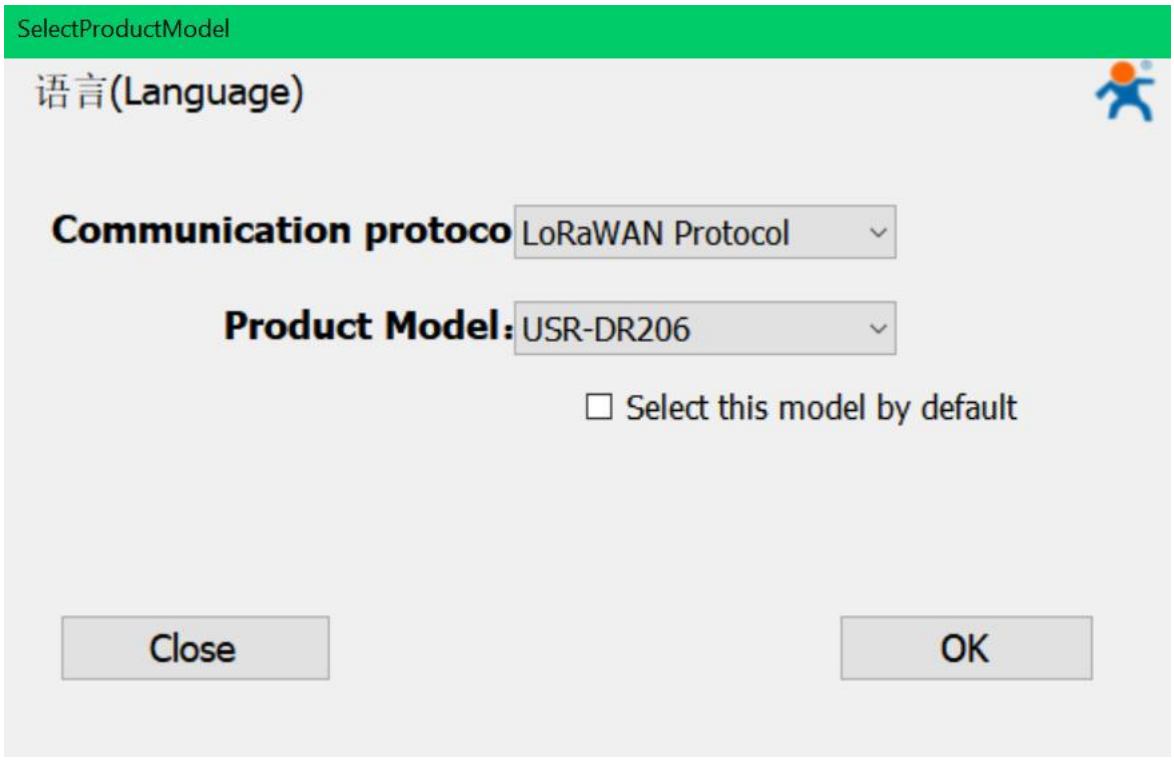
Temperature and Humidity Sensor -- LoRaWAN DTU -- LoRaWAN Gateway (Built-in Chirpstack) -- Application Server

5.4.1.1. LoRaWAN Node Settings

LoRaWAN DTU Network Access Settings: This article takes USR-IoT's USR-DR206-AU915 model as an example for explanation,

Setting software download:https://www.pusr.com/wiki/puba/PEN8h10uV?lang=en_US#top

Open the setting software and select the model



The regional protocol/frequency band of DR206 must match that of LG270 for successful network access

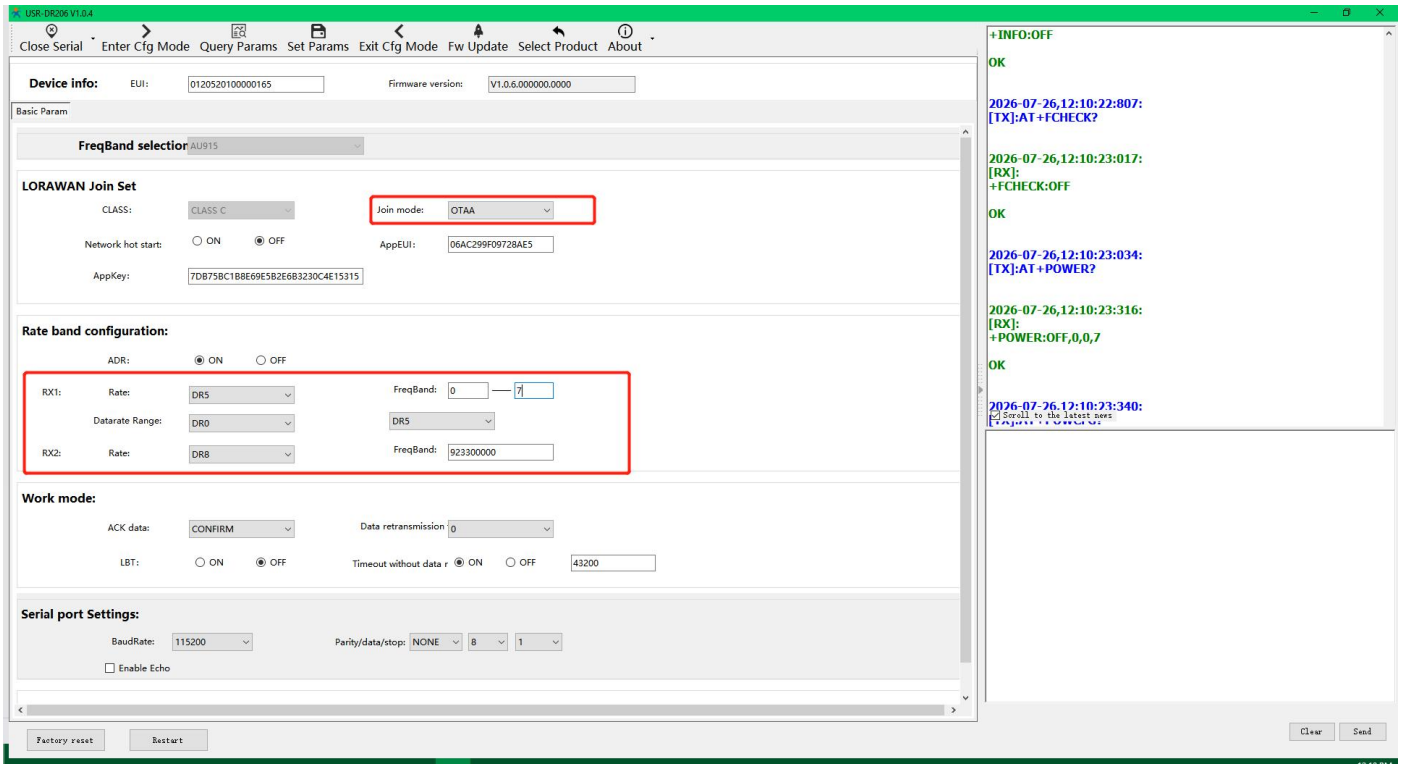
Several key parameters:

Regional Protocol: LoRaWAN nodes, LoRaWAN gateways, and NS servers must be consistent to access the network and communicate normally;

Frequency Band: LoRaWAN nodes, LoRaWAN gateways, and NS servers must be consistent to access the network and communicate normally;

Network Access Method: Must be consistent with the NS server

In this example, the LoRaWAN node regional protocol is AU915, frequency band is 0-7, and network access method is OTAA

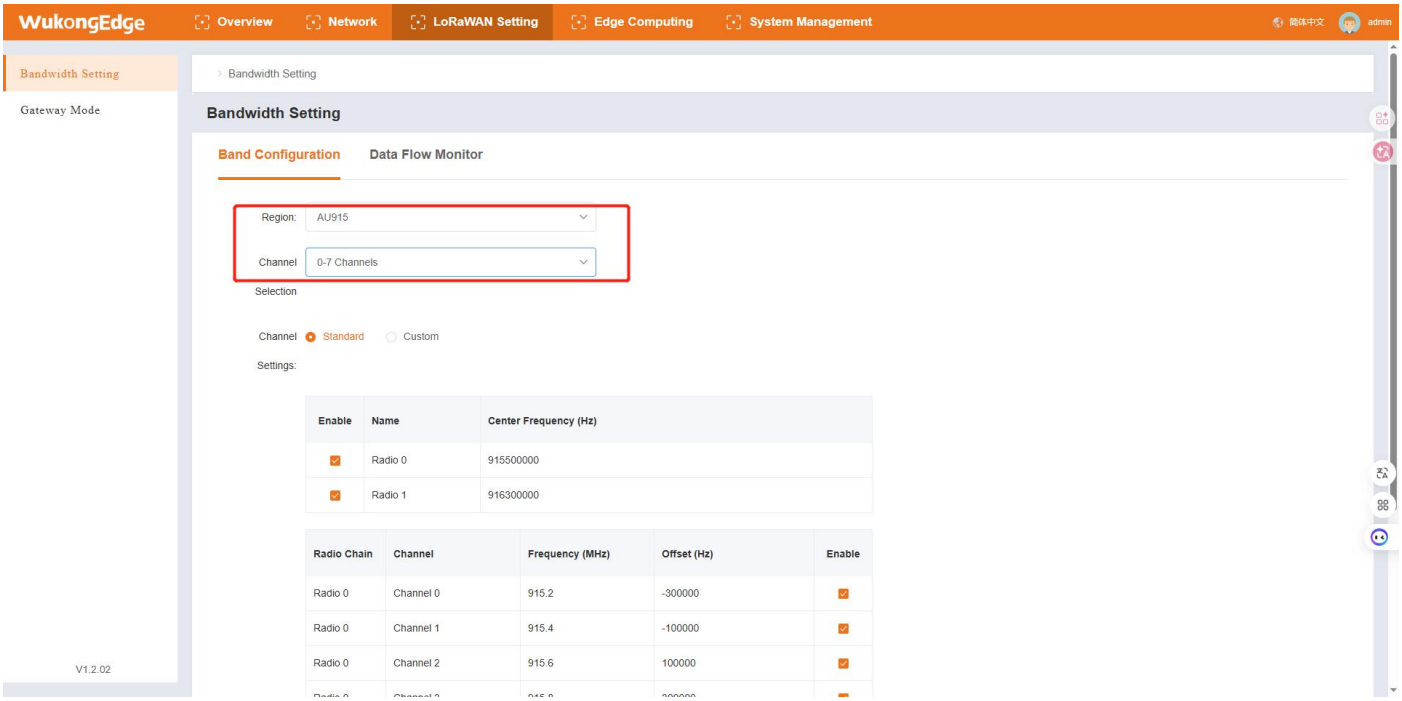


5.4.1.2. LoRaWAN Gateway Configuration

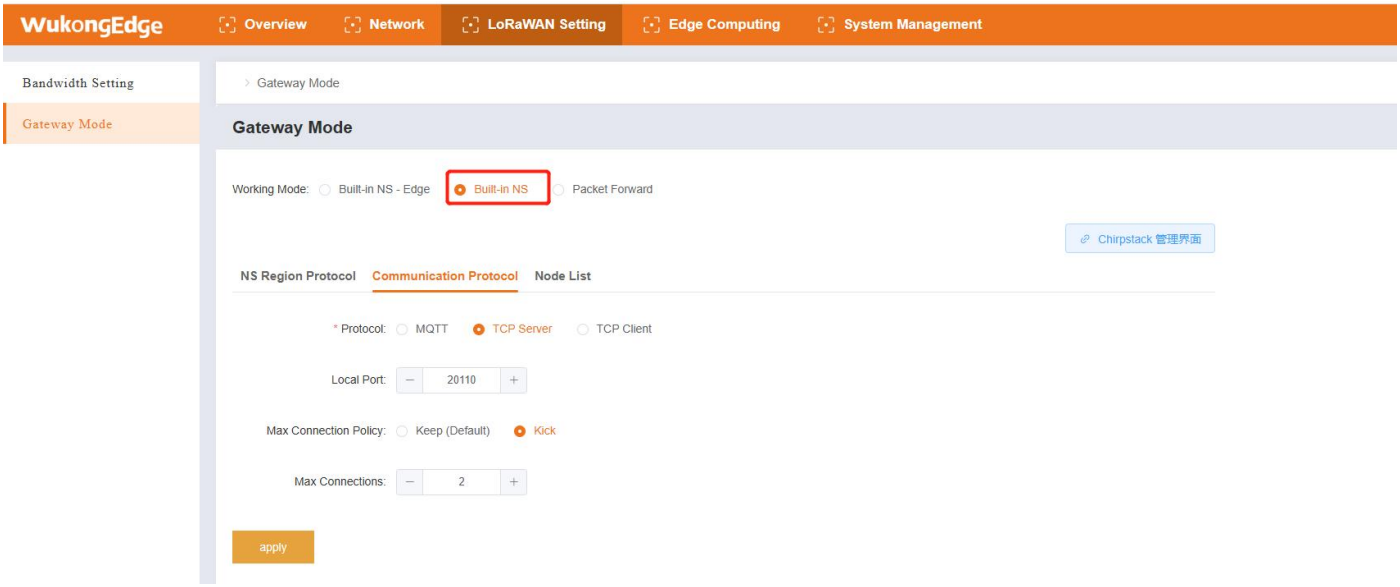
Regional Protocol: AU915, consistent with the LoRaWAN node

Channel Selection: 0-7, consistent with the LoRaWAN node

Channel Settings: Standard

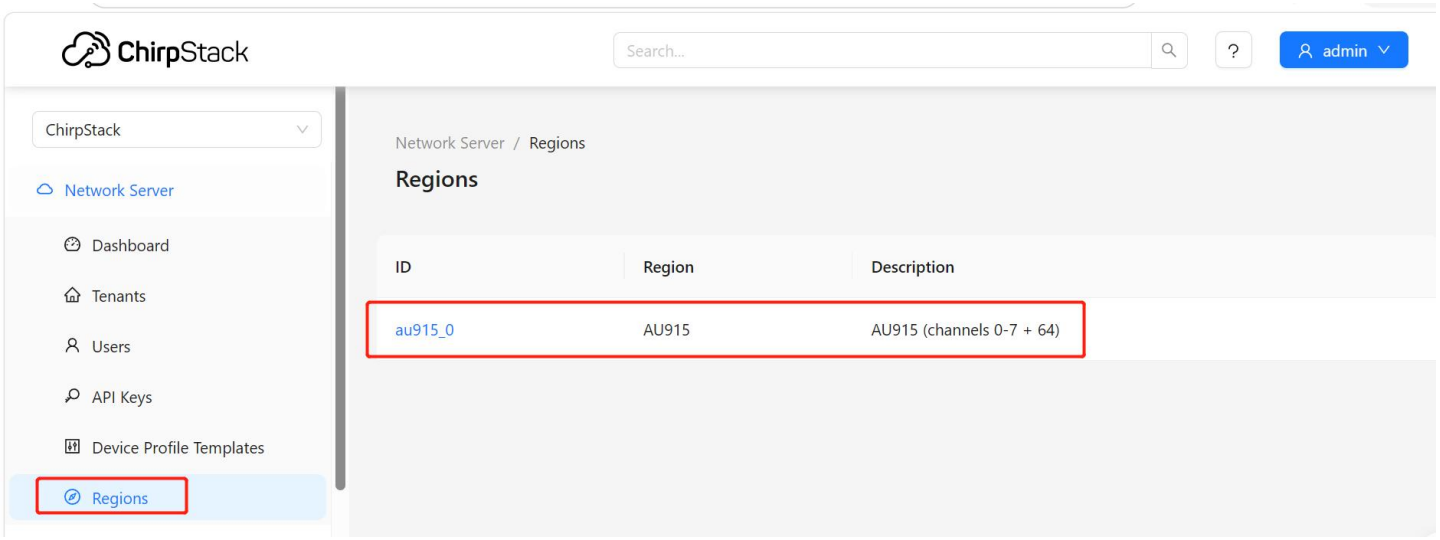


Mode Selection: Select Built-in NS, then click**Chirpstack Management Interface**

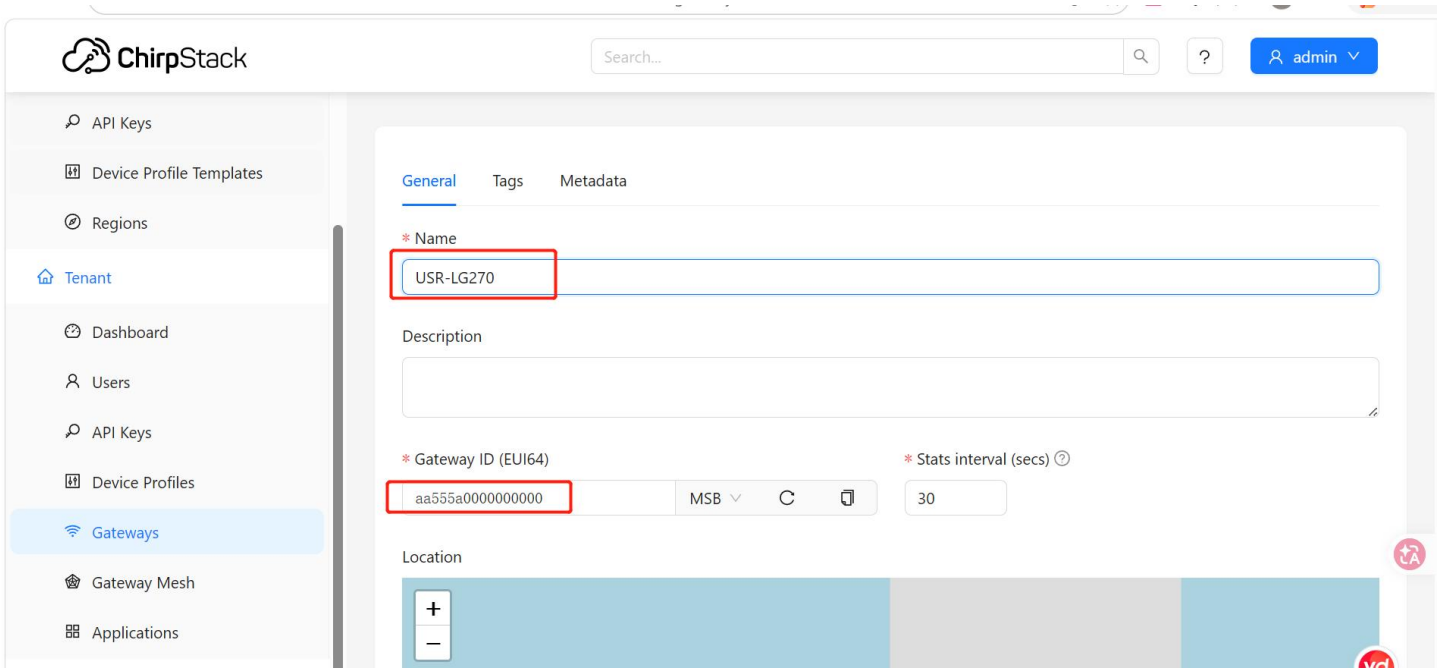


5.4.1.3. Chirpstack Configuration:

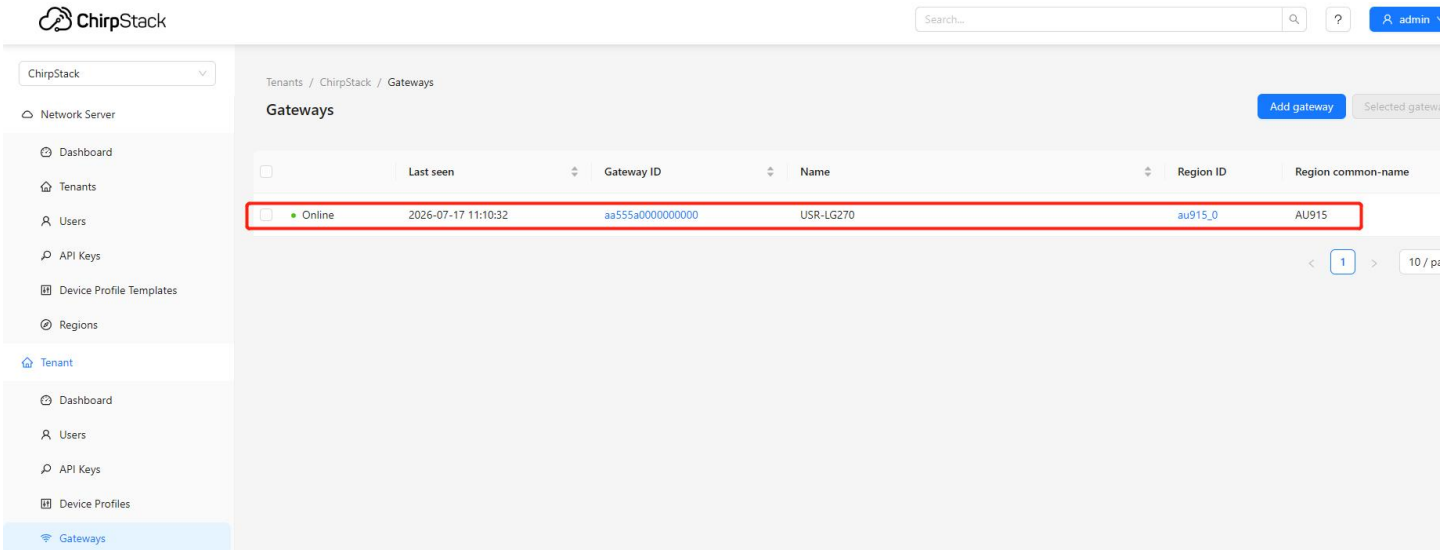
1. View Region: The regional protocol here must include the regional protocols of the gateway and the node, In this example: Both the LoRaWAN node and LoRaWAN gateway are in the AU915 region, channels 0-7, and the NS region server is also AU915_0 (representing AU915 protocol, channels 0-7)



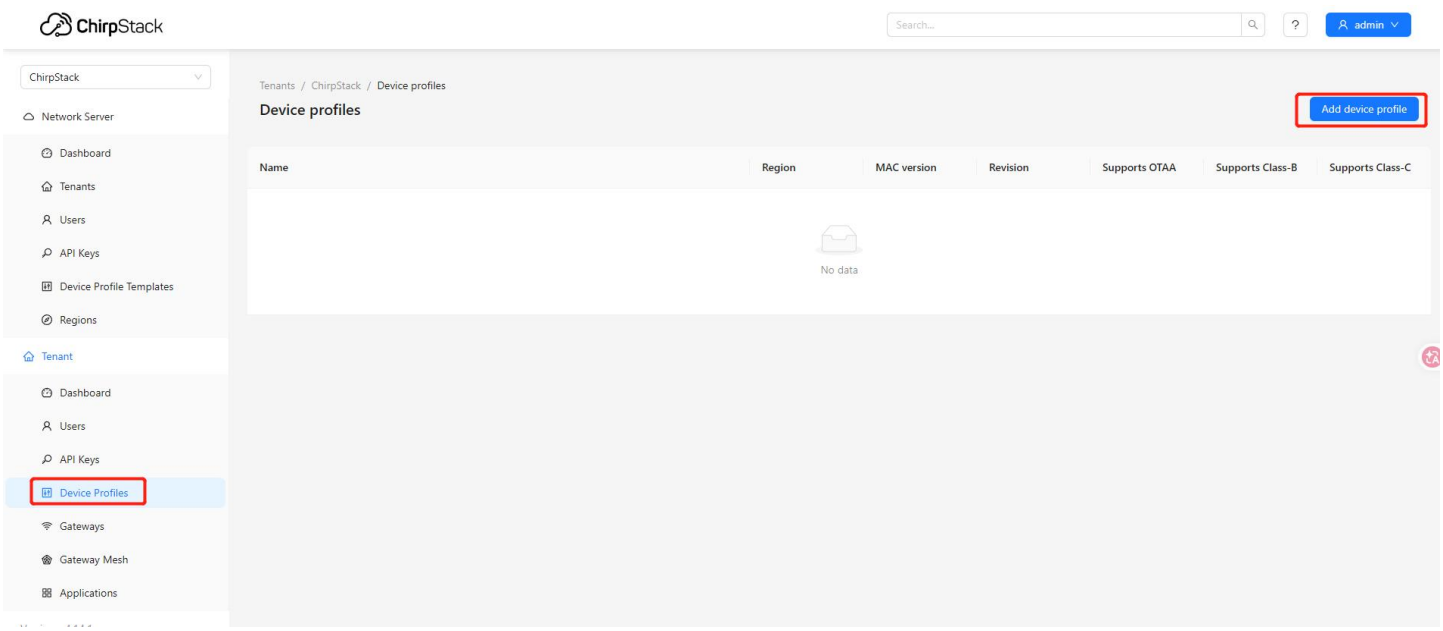
2. Add Gateway: Name can be customized by the user, Gateway ID is the EUI of the LoRaWAN gateway, which can be viewed on the product label or the overview interface of the built-in web page.



Gateway added successfully and online



3. Add Device Profile: The device profile is associated with a specific LoRaWAN node, so parameters such as regional protocol, frequency band, network access method, and keys in the device profile must match the LoRaWAN node, otherwise the LoRaWAN node cannot successfully access the network for data communication.

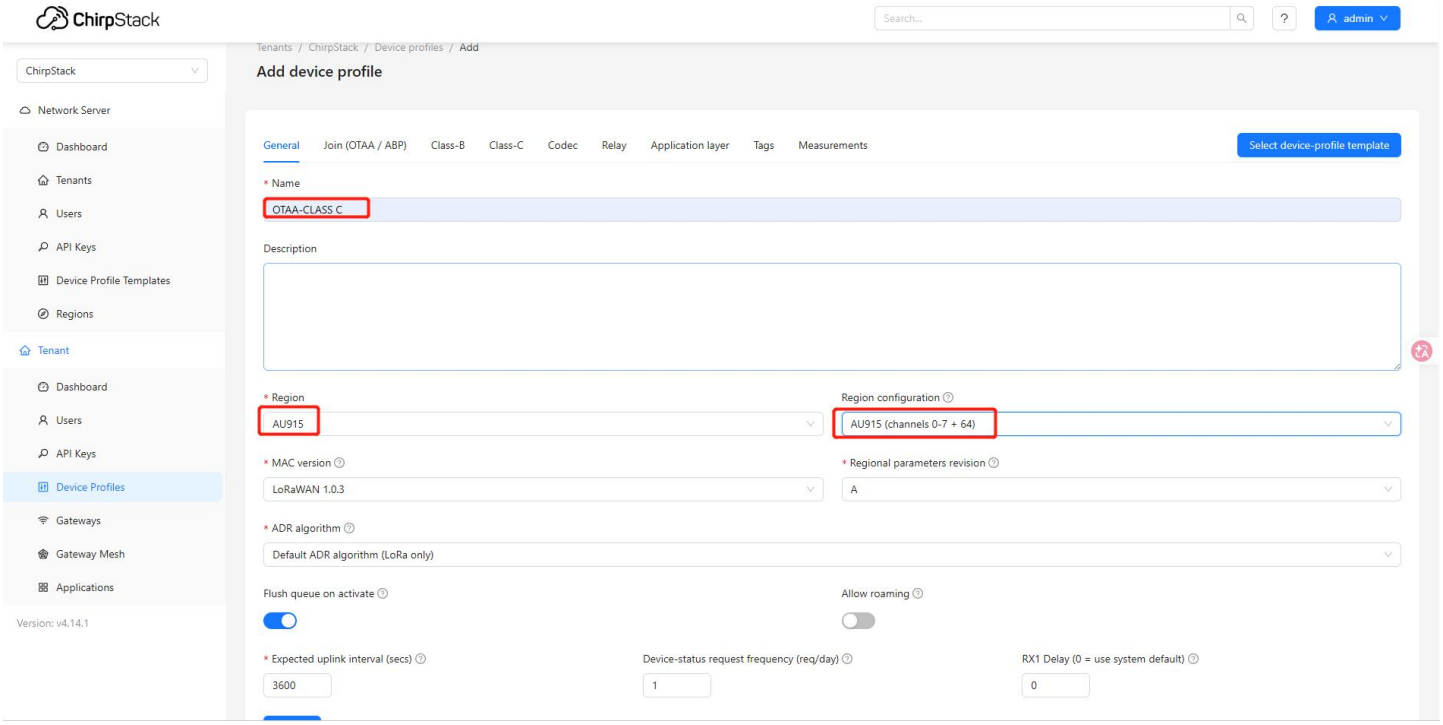


Device Profile Basic Settings:

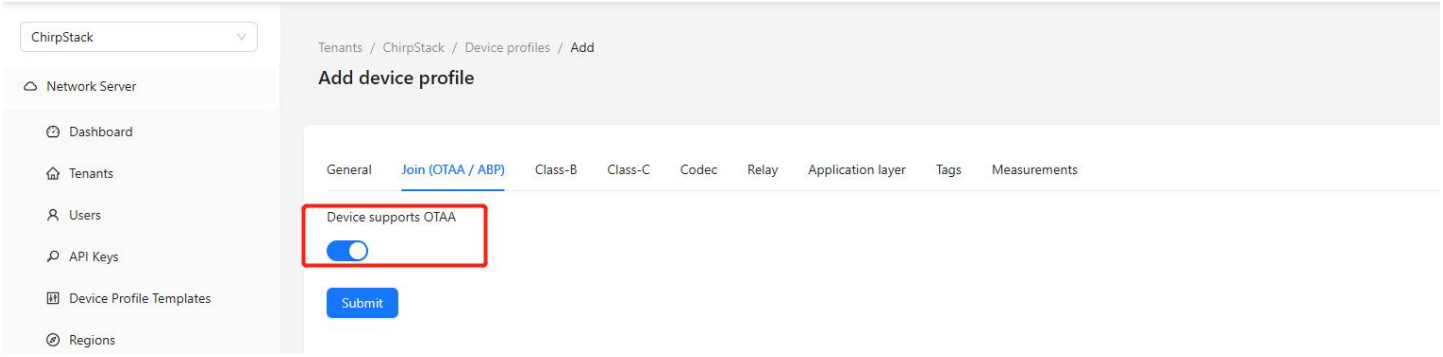
File Name: Custom

Region Selection: Must be consistent with the LoRaWAN node

Region Configuration: i.e., channel, must be consistent with the LoRaWAN node

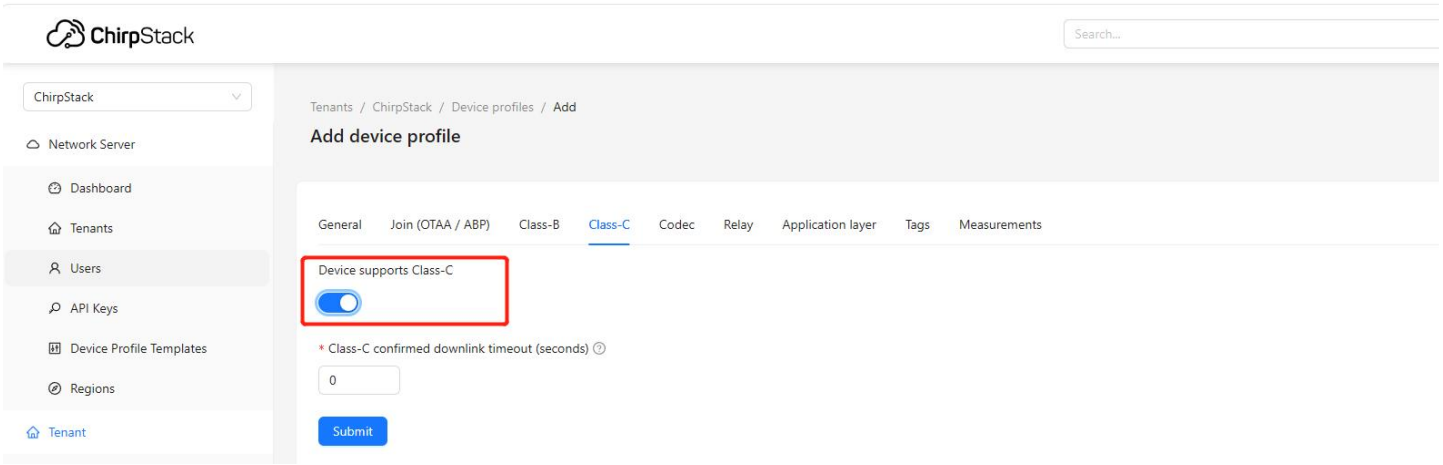


Select device support for OTAA, because the node is set to OTAA network access. If the node uses ABP network access, OTAA does not need to be enabled.

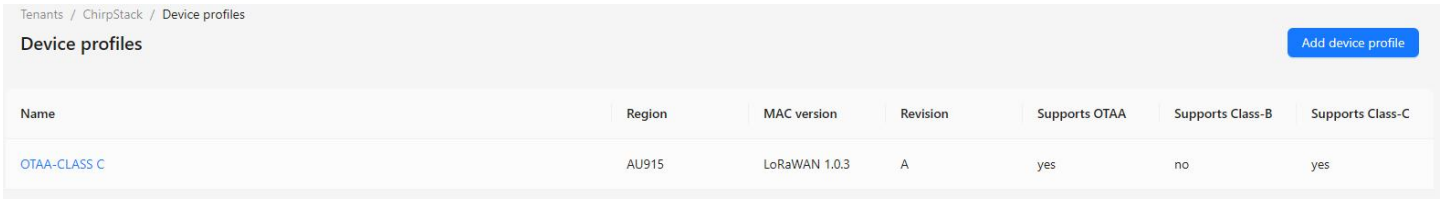


Enable CLASS C: Since USR-DR206 is a CLASS C device, it must be enabled here

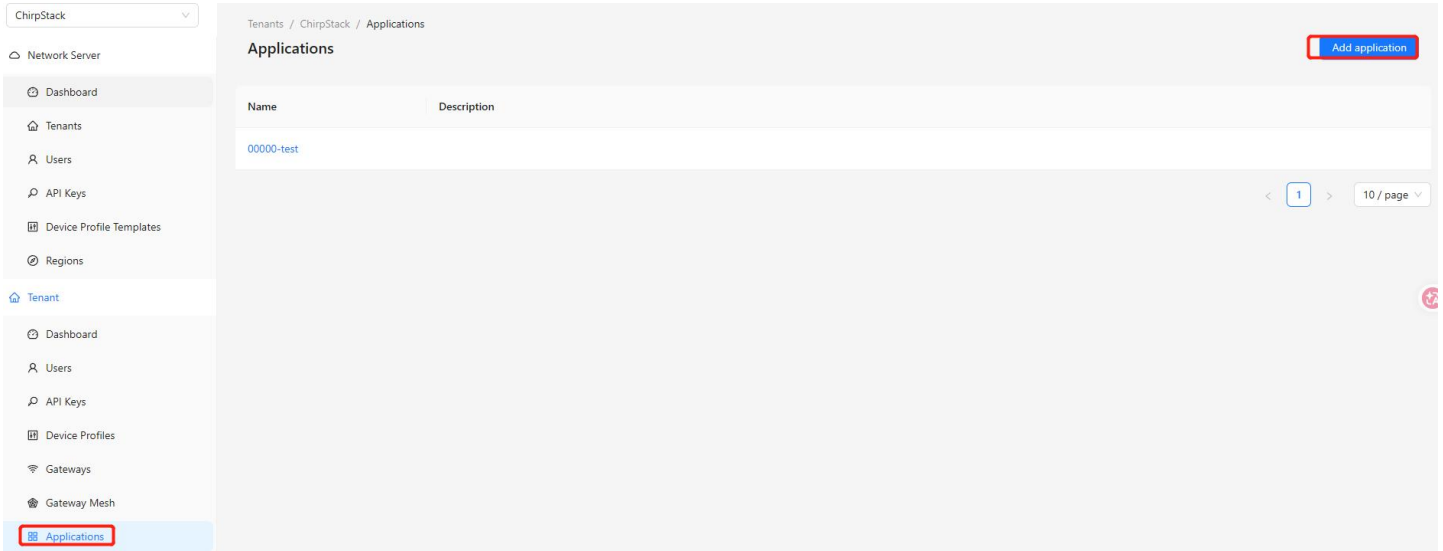
The Chirpstack service supports CLASS A devices by default. CLASS B and CLASS C devices need to be enabled separately.



Device profile added successfully



4. Add Application



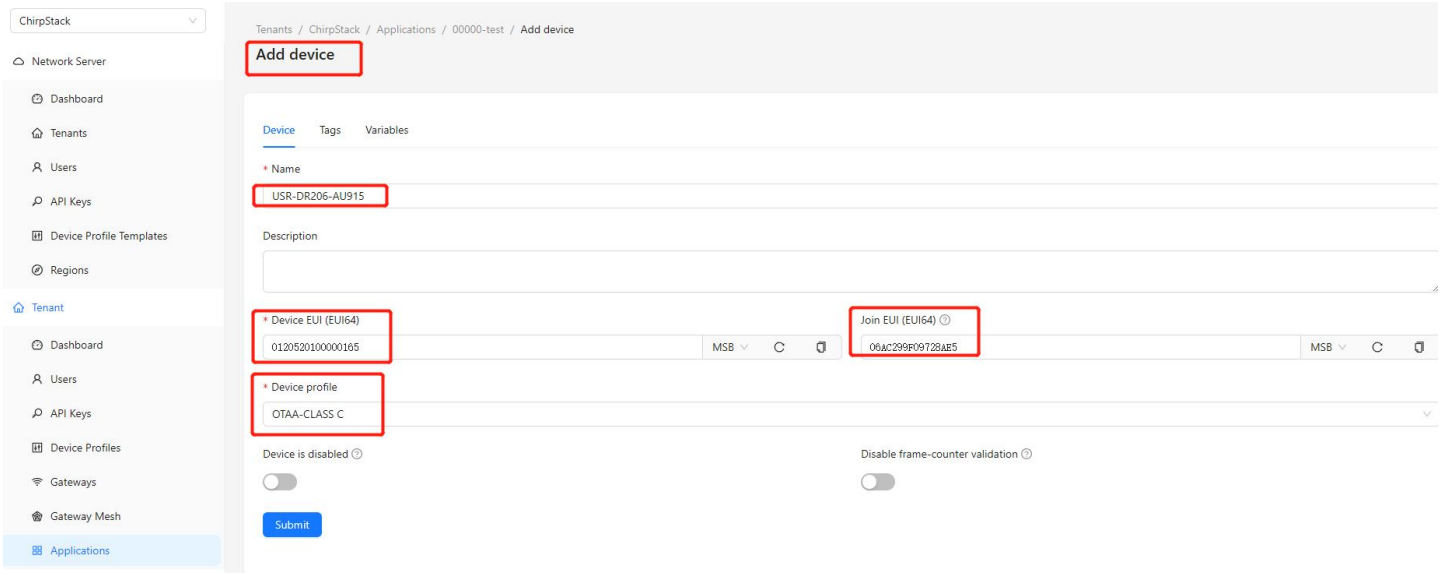
Enter the application and add a device

Name: User-defined

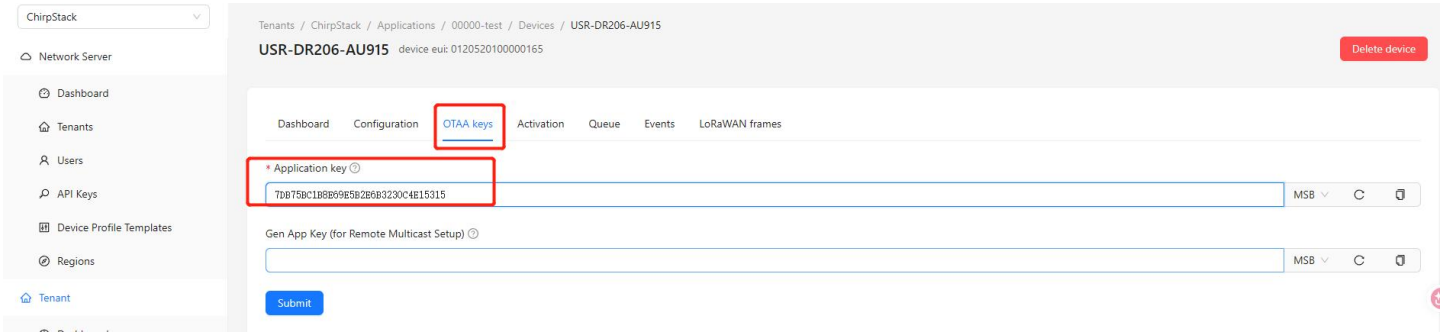
Device EUI: Usually can be found on the device label

Join EUI: Also known as AppEUI. This parameter exists only for OTAA nodes; ABP nodes do not have this parameter.

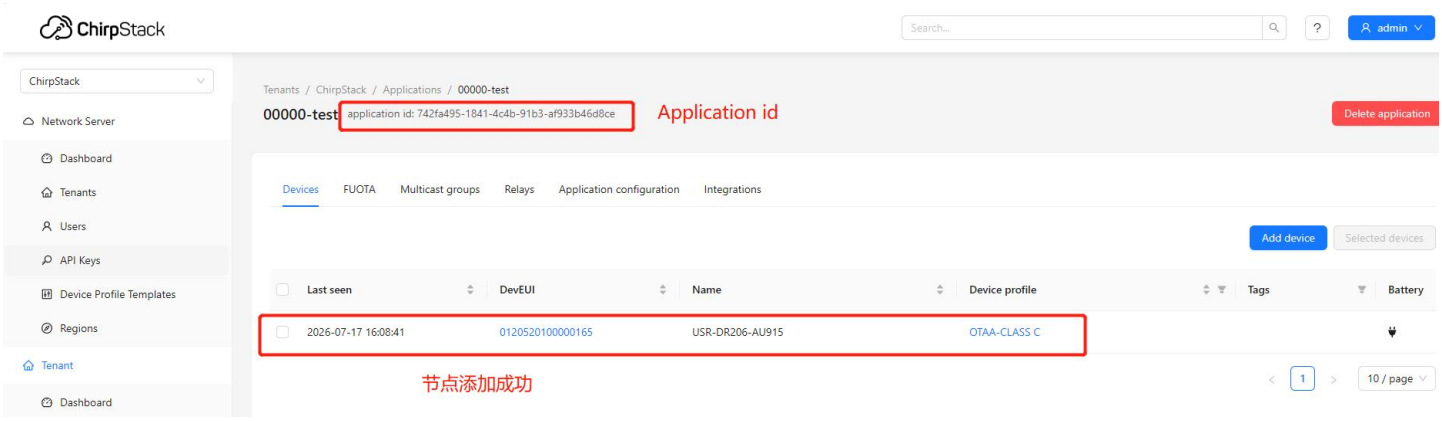
Device Profile: Select the device profile added above. Note: The parameters in this device profile are closely related to the node. Please ensure that the LoRaWAN node parameters match the parameters in the device profile.



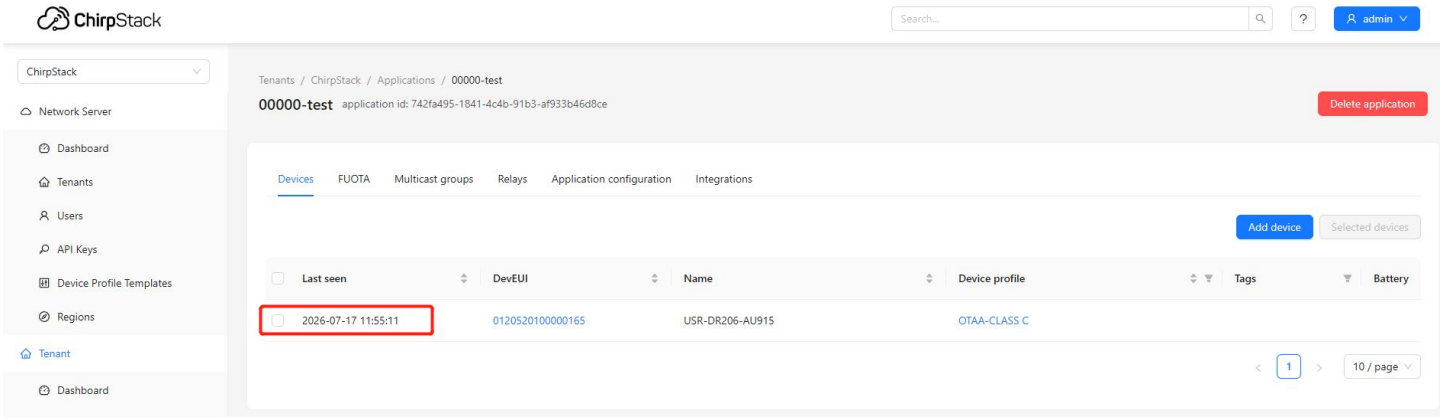
AppKey: After clicking submit, the AppKey interface pops up. Enter the AppKey of the LoRaWAN node.



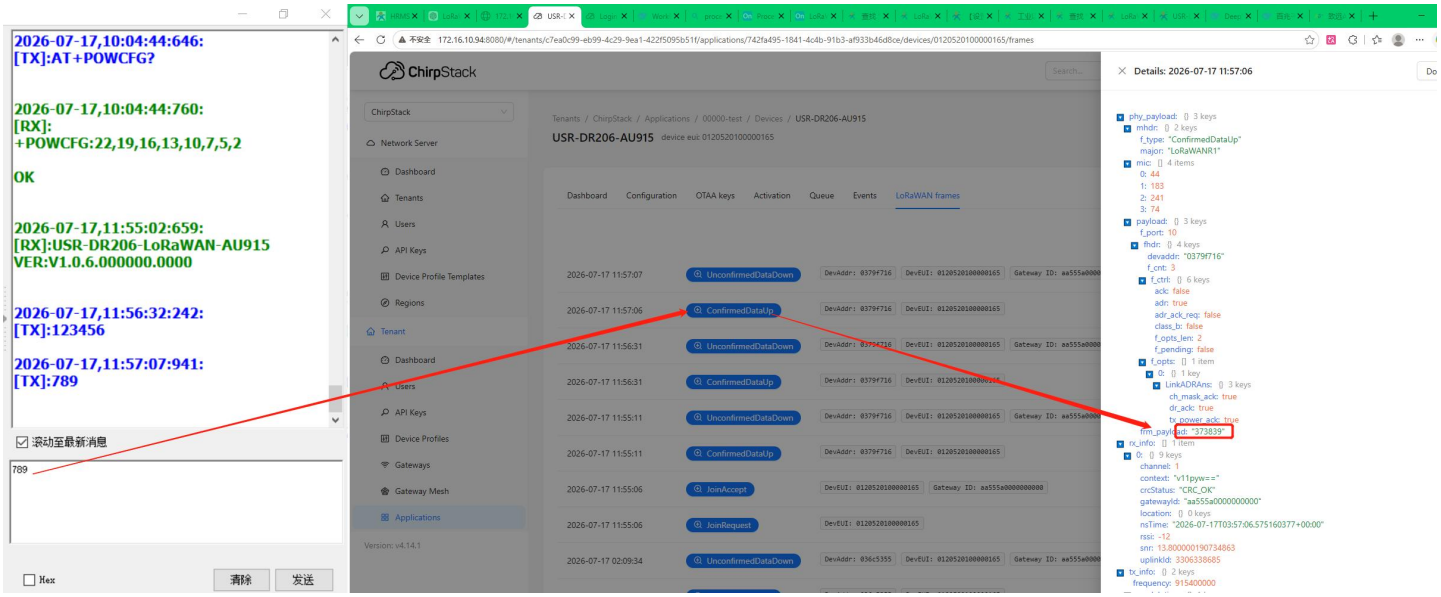
LoRaWAN node added successfully: Note that there is an Application ID here, which will be used in subsequent data communication.



Power on the LoRaWAN node, and the node comes online successfully.



At this point, the Node-Gateway-NS service connection is established. When sending data from the serial port, uplink data can be seen in the NS server's data flow monitoring.



5.4.1.4. MQTT Integration with Application Server

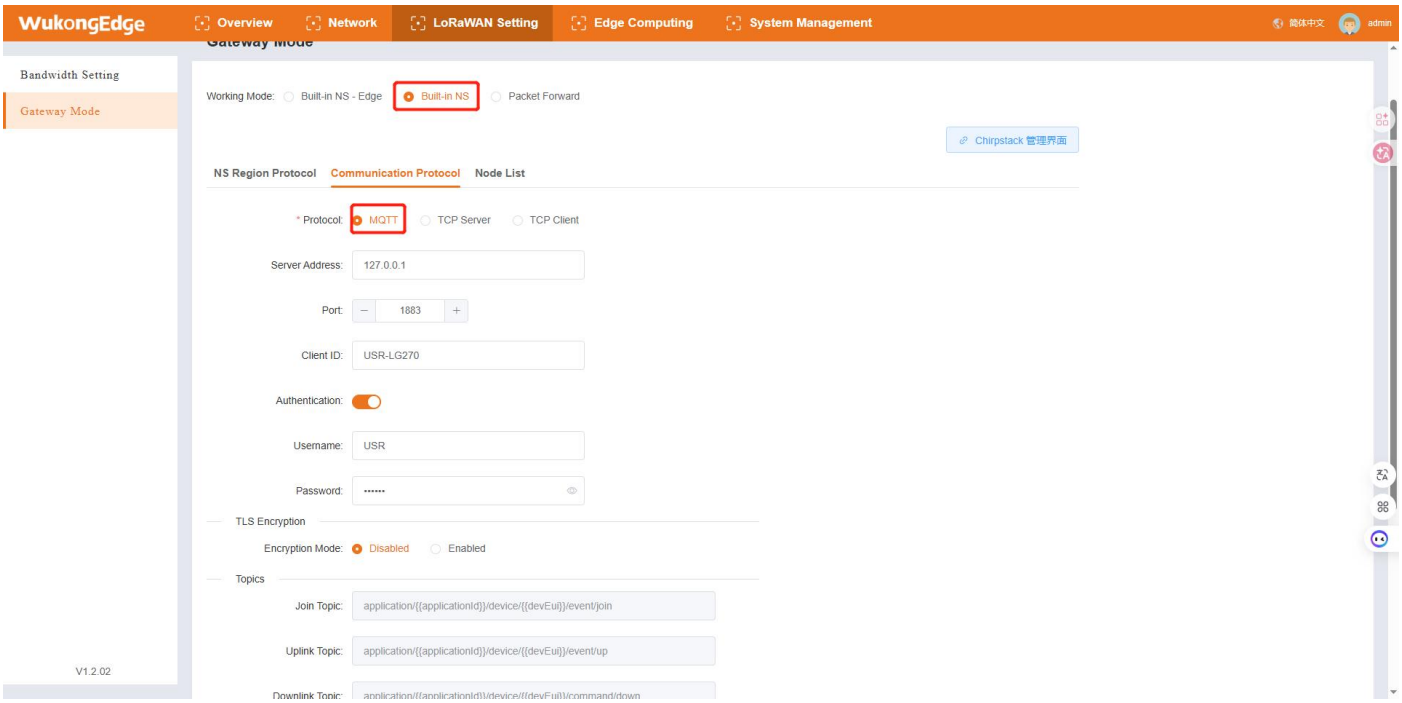
Through the steps above, the NS server has normally received the data sent by the node. Now, this data needs to be sent to the application server for data analysis and application. In built-in NS mode, USR-LG270 supports connecting to the application server via MQTT, TCP, and UDP. Users can choose the appropriate connection method according to their business needs. In addition, to ensure the security of data transmission,

the communication link supports TLS/SSL encryption, and provides various encryption methods for users to choose, further enhancing the confidentiality and integrity of data transmission.

MQTT Communication Protocol Parameter Description:

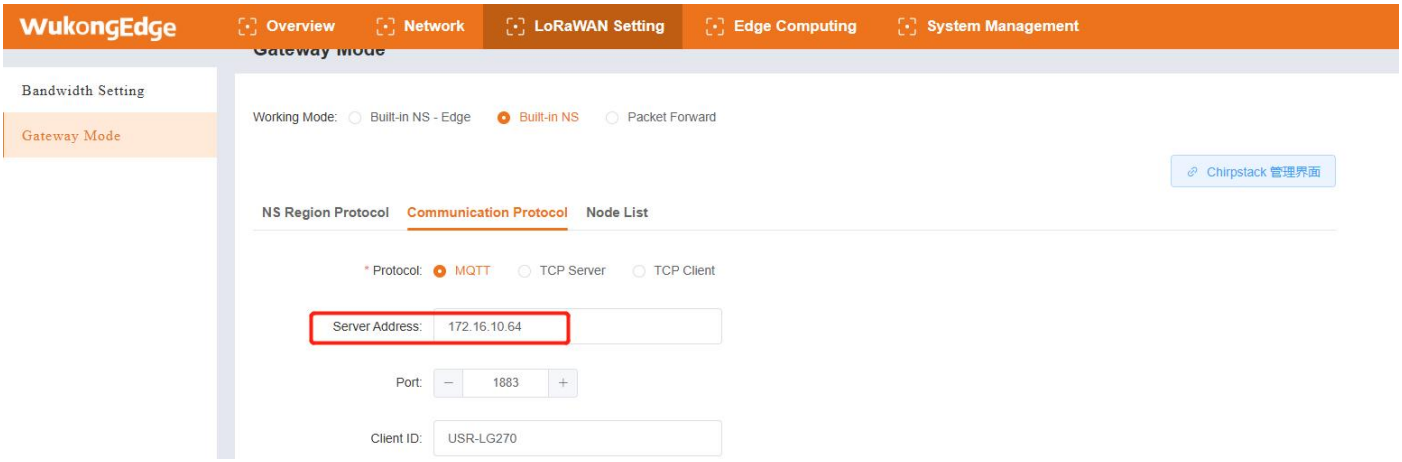
Name	Parameter Description	Default Parameter
Server Address	The IP address or domain name of the remote MQTT Broker If the server address is set to 127.0.0.1, USR-LG270 can act as an MQTT Broker. MQTT client tools on computers within the LAN can directly connect to the USR-LG270's IP address to communicate with the node.	127.0.0.1
Port Number	The listening port number of the remote MQTT Broker or the listening port number when acting as an MQTT Broker itself	1883
Client ID	The unique identity identifier of the current client on theMQTTserver	chirpstack
Authentication	When enabled, username and password verification is required	OFF
Username/Password	Credentials used by the server to verify identity after authentication is enabled. Must be filled in correctly to connect successfully.	Empty
TLS Encryption	If TLS encryption is required, enable encryption mode	Disabled
Authentication Mode	No Certificate Verification / Verify Server / Mutual Authentication	No Certificate Verification

Topic	USR-LG270 uses the topic rules defined by Chirpstack Join Topic: application/{{applicationId}}/device/{{devEui}}/event/join Uplink Topic: application/{{applicationId}}/device/{{devEui}}/event/up Downlink Topic: application/{{applicationId}}/device/{{devEui}}/command/down Acknowledgment Topic: application/{{applicationId}}/device/{{devEui}}/event/ack Status Topic: application/{{applicationId}}/device/{{devEui}}/event/status applicationId: You can see the ID information corresponding to different applications in the Chirpstack Application interface devEui: Node information of the LoRaWAN node Actual Topic Example: application/742fa495-1841-4c4b-91b3-af933b46d8ce/device/0120520100000165/event/up	
Status Information Interval	The interval time for the LoRaWAN gateway to report status information to the application server Range: 30-65535s MQTT clients can subscribe to the topic: +/gateway/#	30s
Clean Session	Enable/Disable Enable: After the device disconnects, the MQTT server does not retain subscription information and unfinished messages Disable: After the device disconnects, the MQTT server retains subscription information and unfinished messages	Disabled



MQTT Protocol Uplink and Downlink Communication Test:

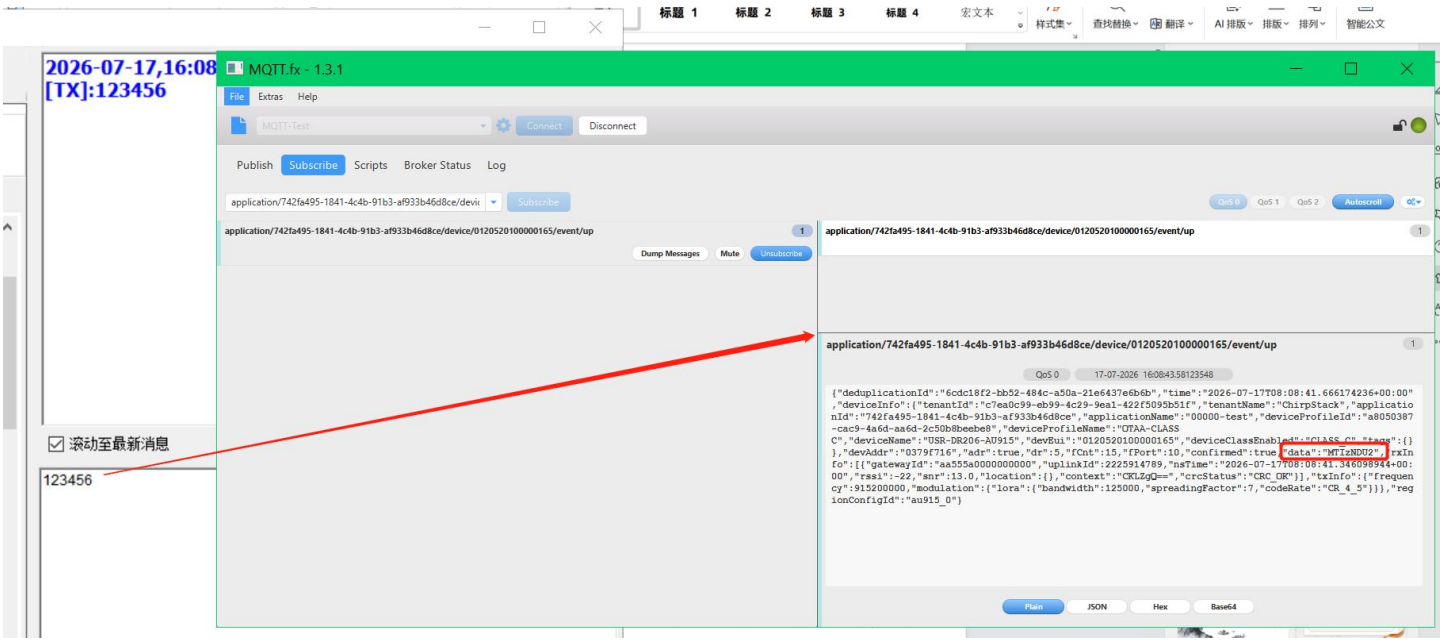
Configure the LoRaWAN industrial gateway to connect to the MQTT server:



Uplink Data:

MQTT subscribes to the uplink topic:

application/742fa495-1841-4c4b-91b3-af933b46d8ce/device/0120520100000165/event/up



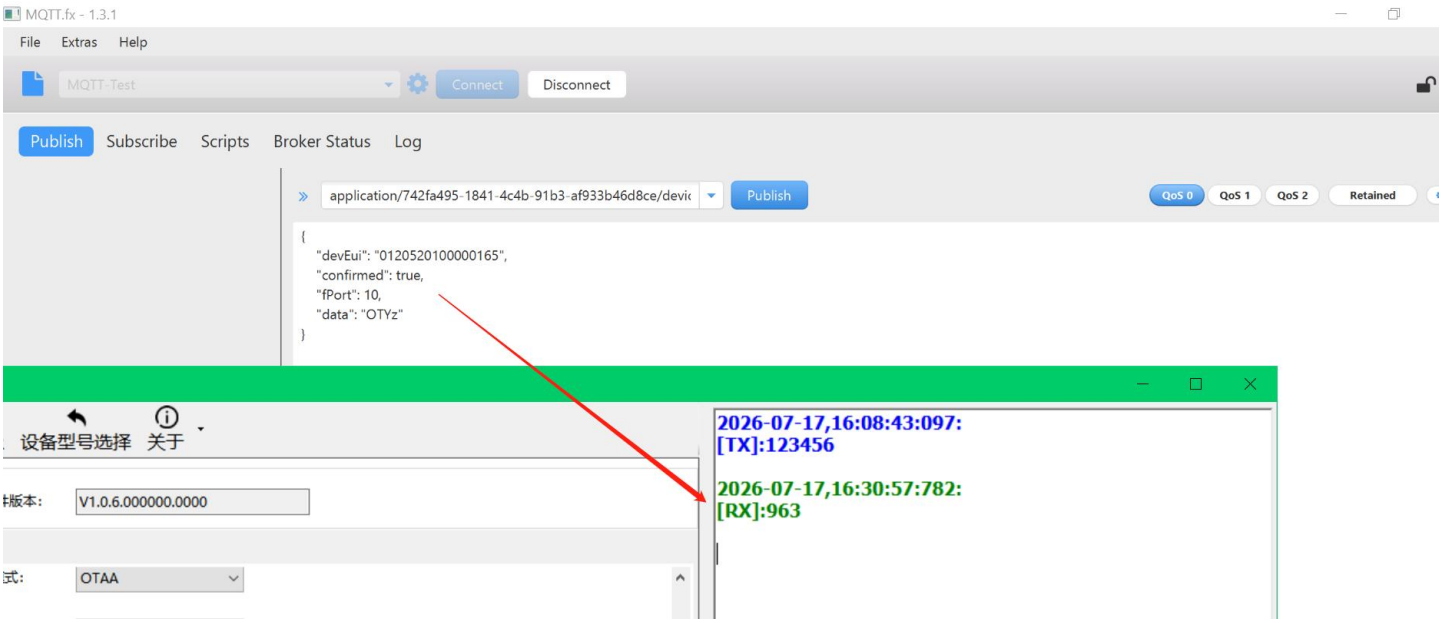
Downlink Data Test:

Push Topic:

application/742fa495-1841-4c4b-91b3-af933b46d8ce/device/0120520100000165/command/down

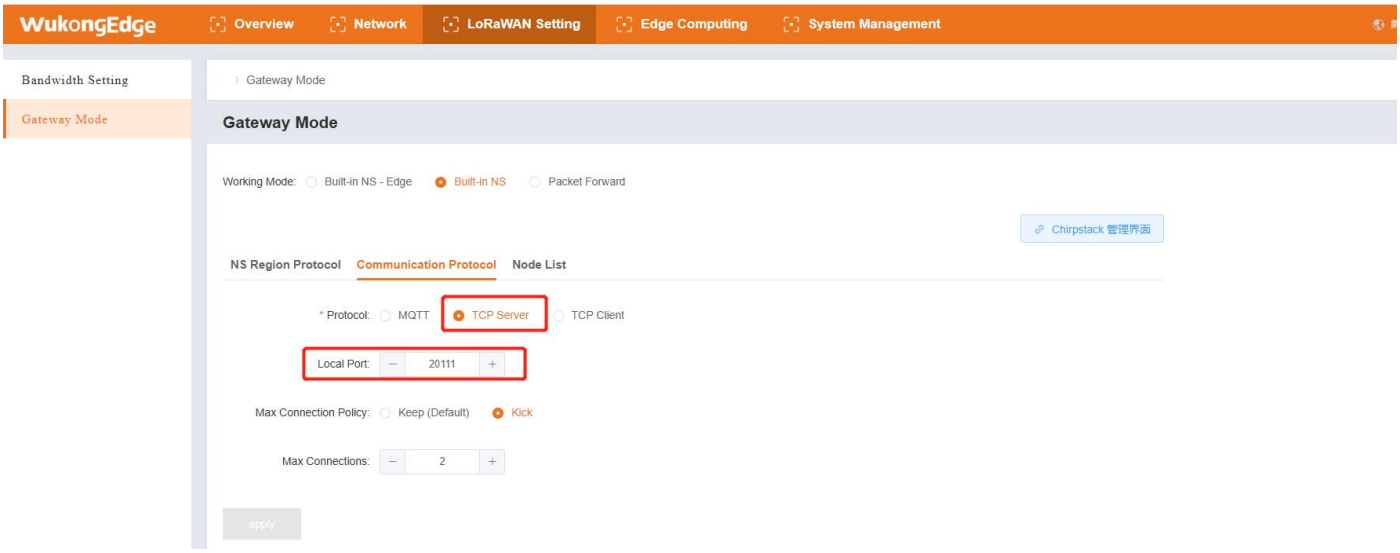
Pushed data format:

```
{
    "devEui": "0120520100000165",        // Must be consistent with the devEui in the MQTT topic
    "confirmed": true,                   // Whether downlink data is confirmed
    "fPort": 10,                         // fport of the LoRaWAN node, DR206-AU915 is 10
    "data": "OTYz"                       // Must be base64 encoded characters
}
```



5.4.1.5. TCP Protocol Integration with Application Server

The LoRaWAN gateway operates inTCP servermode, allowing the network side to receive information reported by LoRaWAN nodes and join information.



Data communication between USR-DR206's serial port and TCP Server. Since there are no subscription and publication topics in the TCP protocol, all data pushed by the Chirpstack server can be received on the application server via the TCP protocol.

In the figure below, the server side receives multiple data packets, where

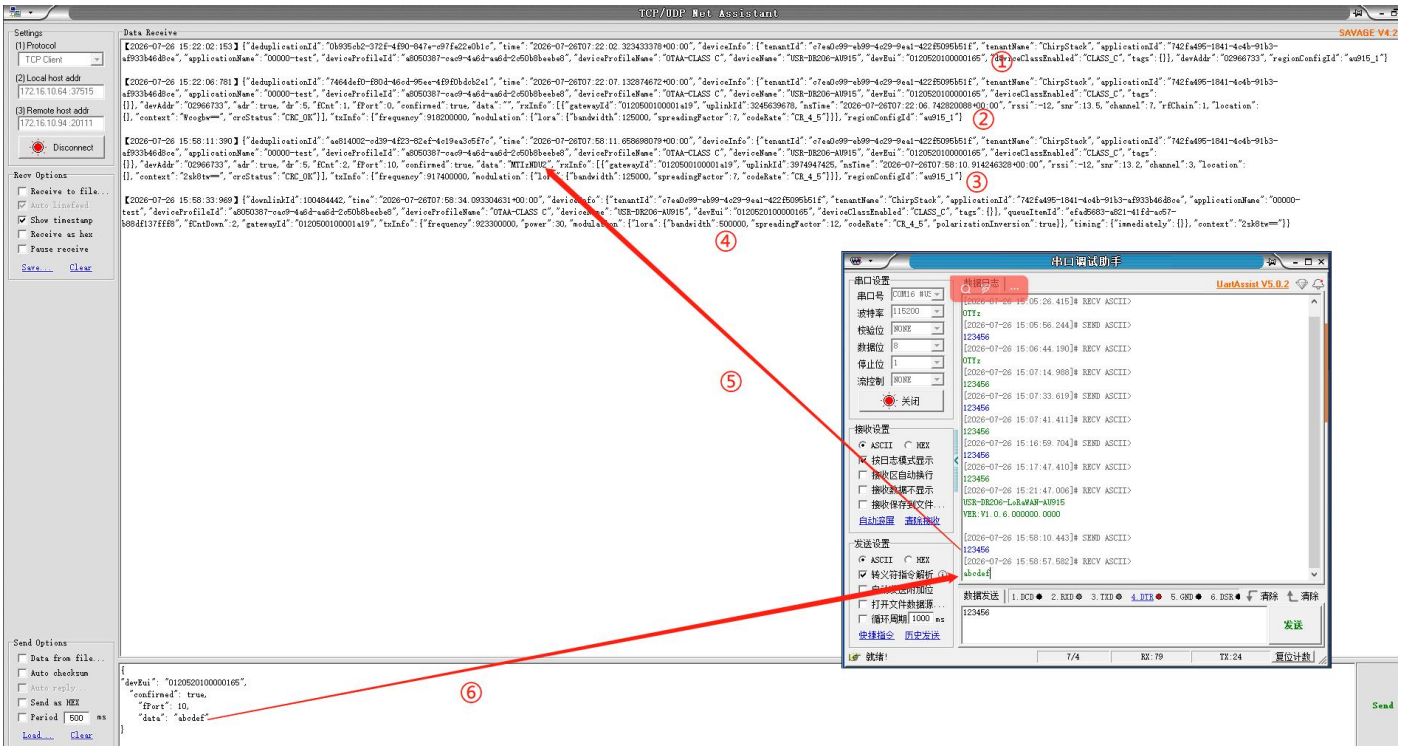
①: Join information for node USR-DR206 joining the network,

②: After node USR-DR206 successfully joins the network, it will actively report an empty packet (this is the mechanism of USR-DR206/216, not applicable to other LoRaWAN nodes)

③ A packet of data reported by node DR206 (123456), ⑤ is the data sent by the serial debugging assistant to the application server side

④ Gateway sends confirmation event data (`txack`), because ⑥ is a packet of data sent by the application server side to the node. When the gateway receives this command, it will immediately reply with a txack message to ChirpStack, indicating "I have received the command and am ready to transmit"

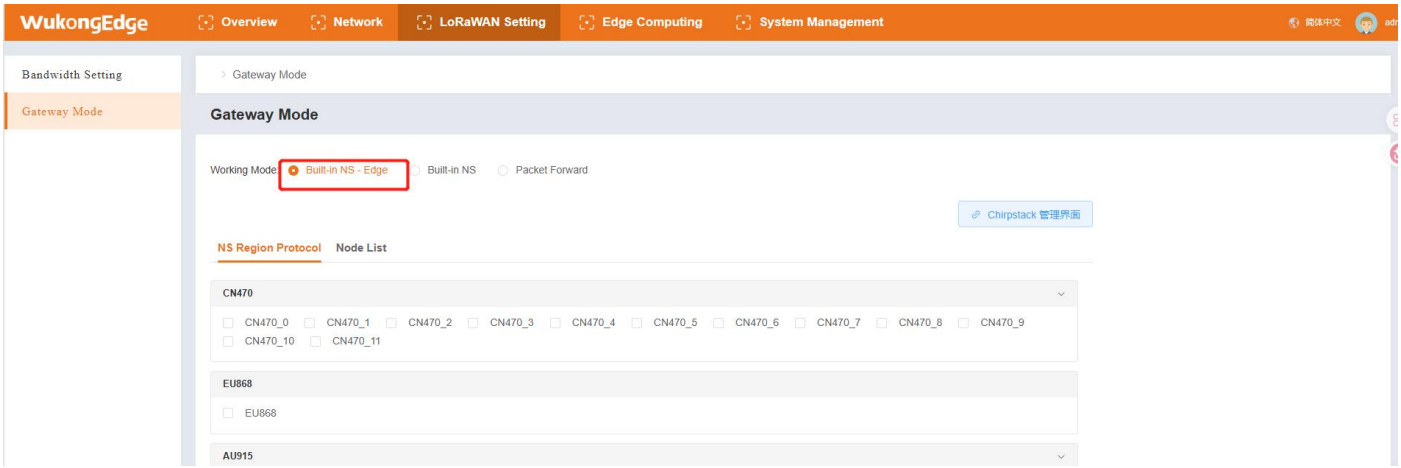
⑥ Application server side sends a packet of data to DR206



5.4.2. Built-in NS - Edge Mode

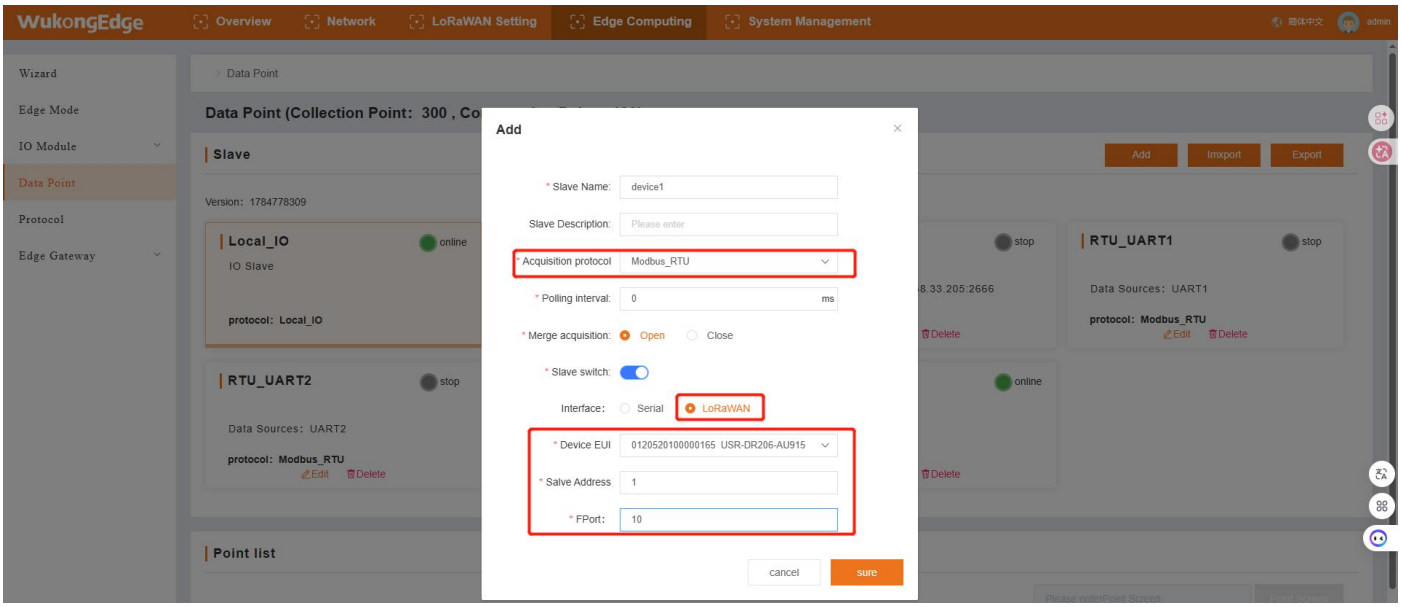
In this mode, the configuration on the Chirpstack side is the same as that of the built-in NS. This section mainly introduces the configuration for connecting to customer application servers and collecting node parameters.

Enable Built-in NS - Edge Mode

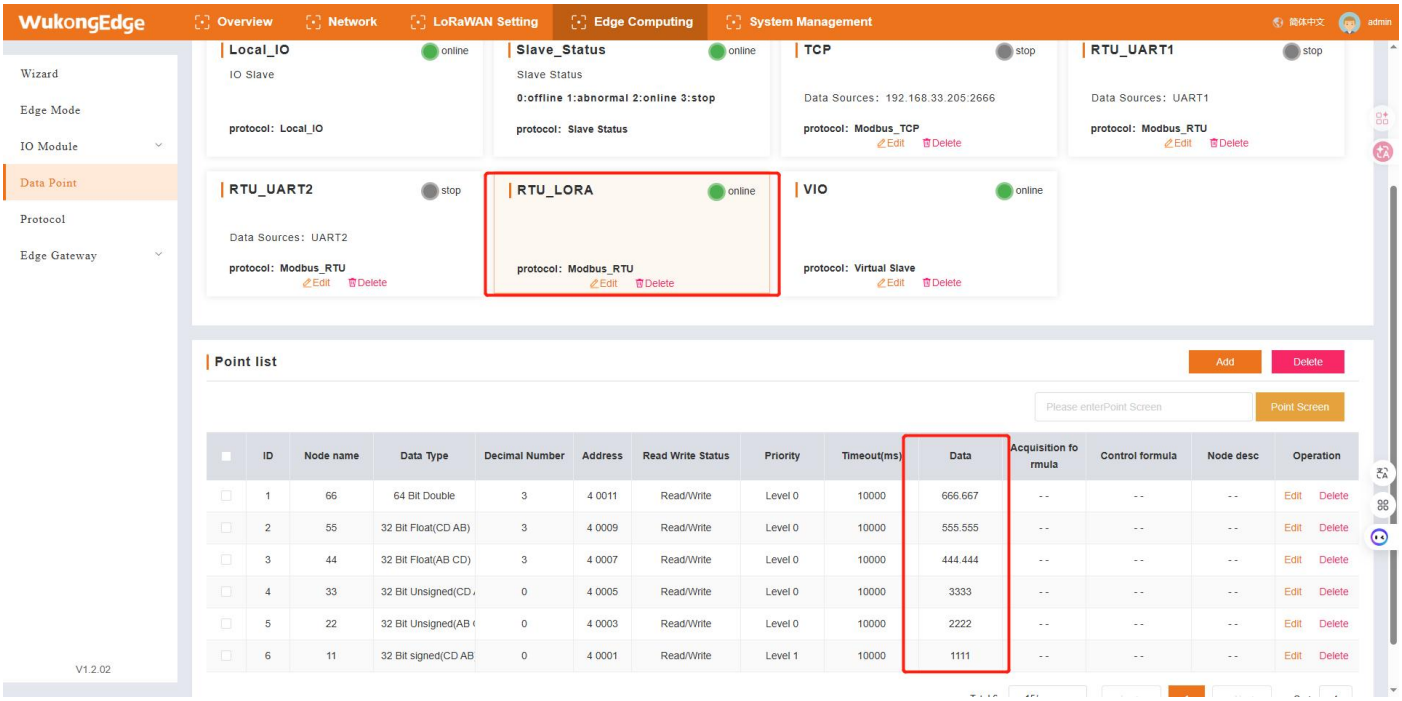


Add slave device, select LoRaWAN for the interface.

Note: Protocols and interface descriptions are detailed in the Edge Computing chapter. This chapter mainly introduces parts related to LoRaWAN settings.



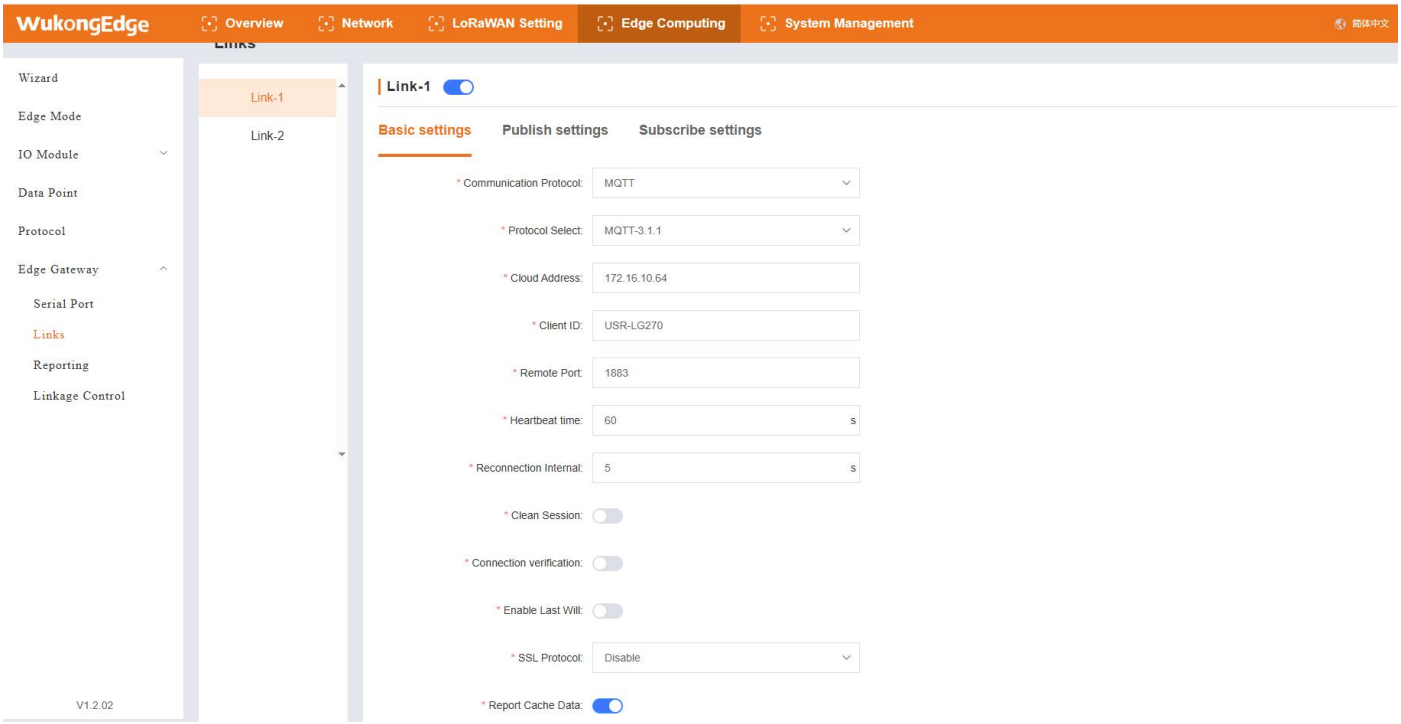
Add data points: If the slave address, register, and Fport settings are correct, normal data collection can be seen on the web page.



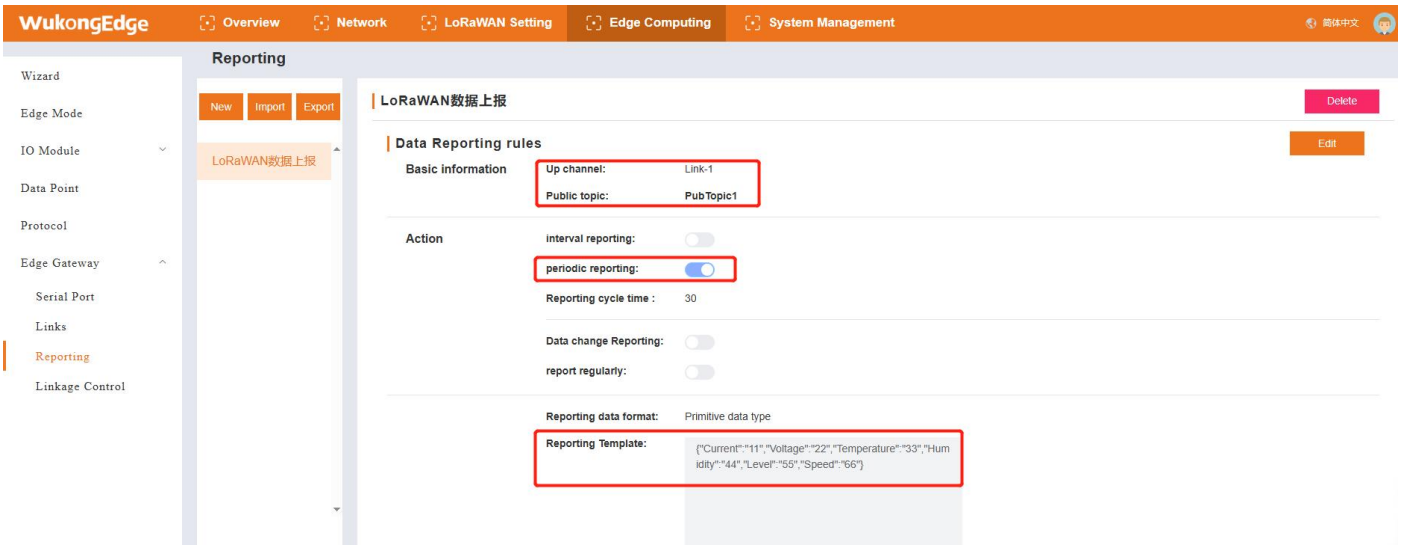
Connect to Application Server:

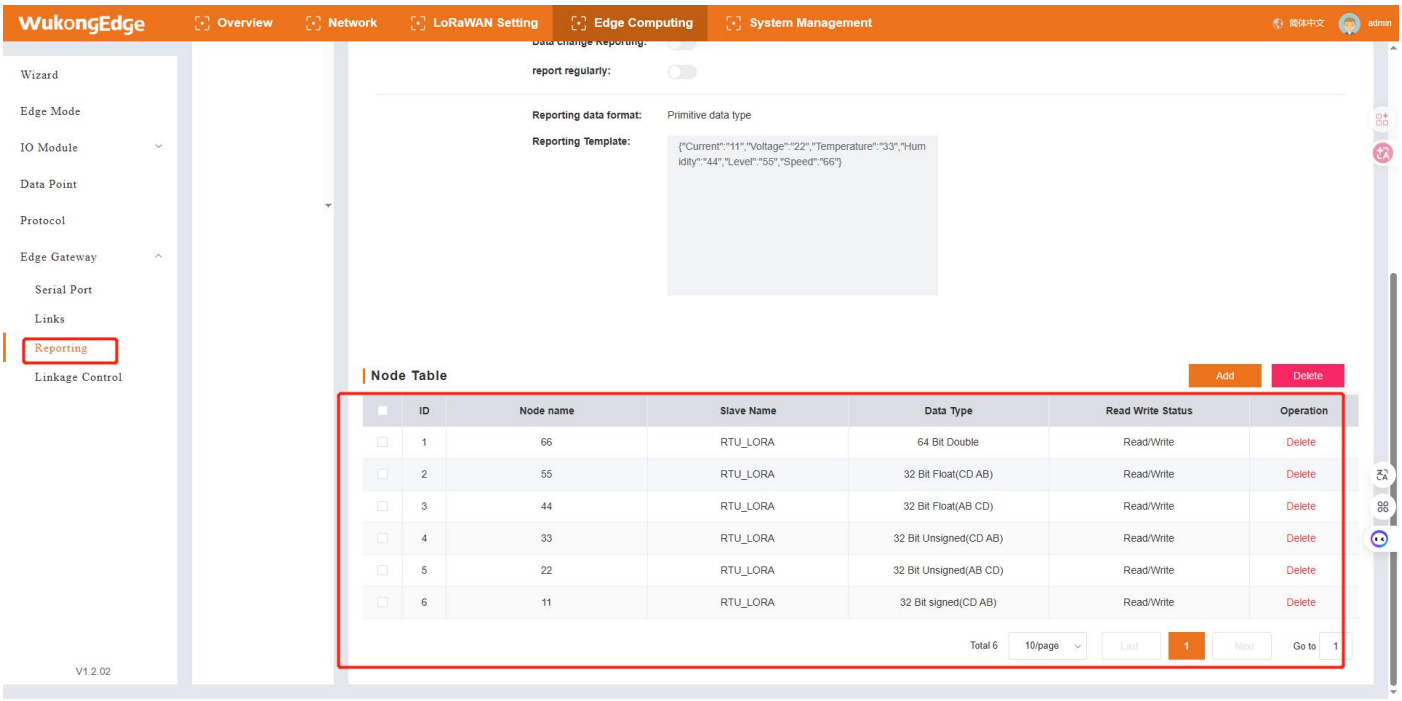
In Built-in NS - Edge Mode, USR-LG270 supports two independent Socket links to connect to customer application servers. The uplink protocol supports TCP Server, TCP Client, HTTP, and MQTT, adapting to common protocol servers to the greatest extent, allowing customers to get started quickly.

This case uses MQTT communication as an example: Set server parameters and subscription/publication topics.

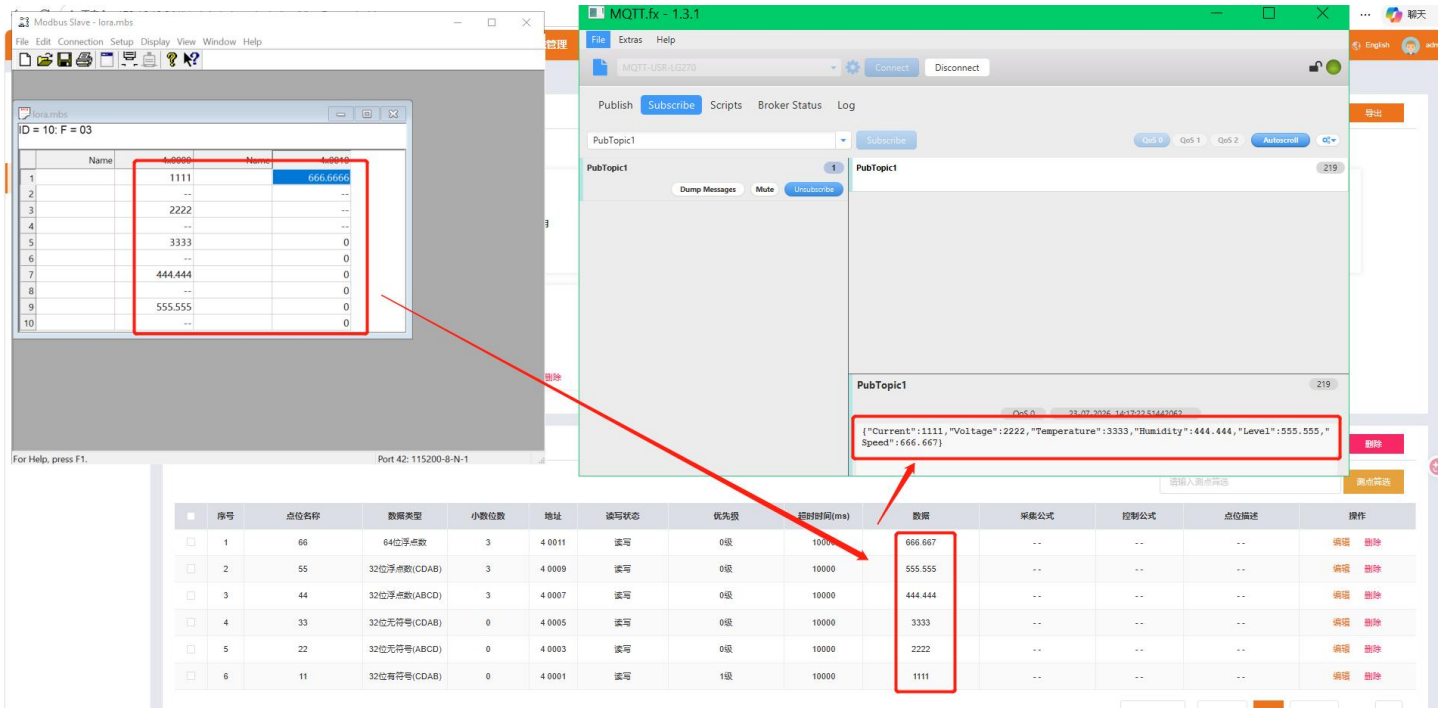


Set Data Reporting Rules:



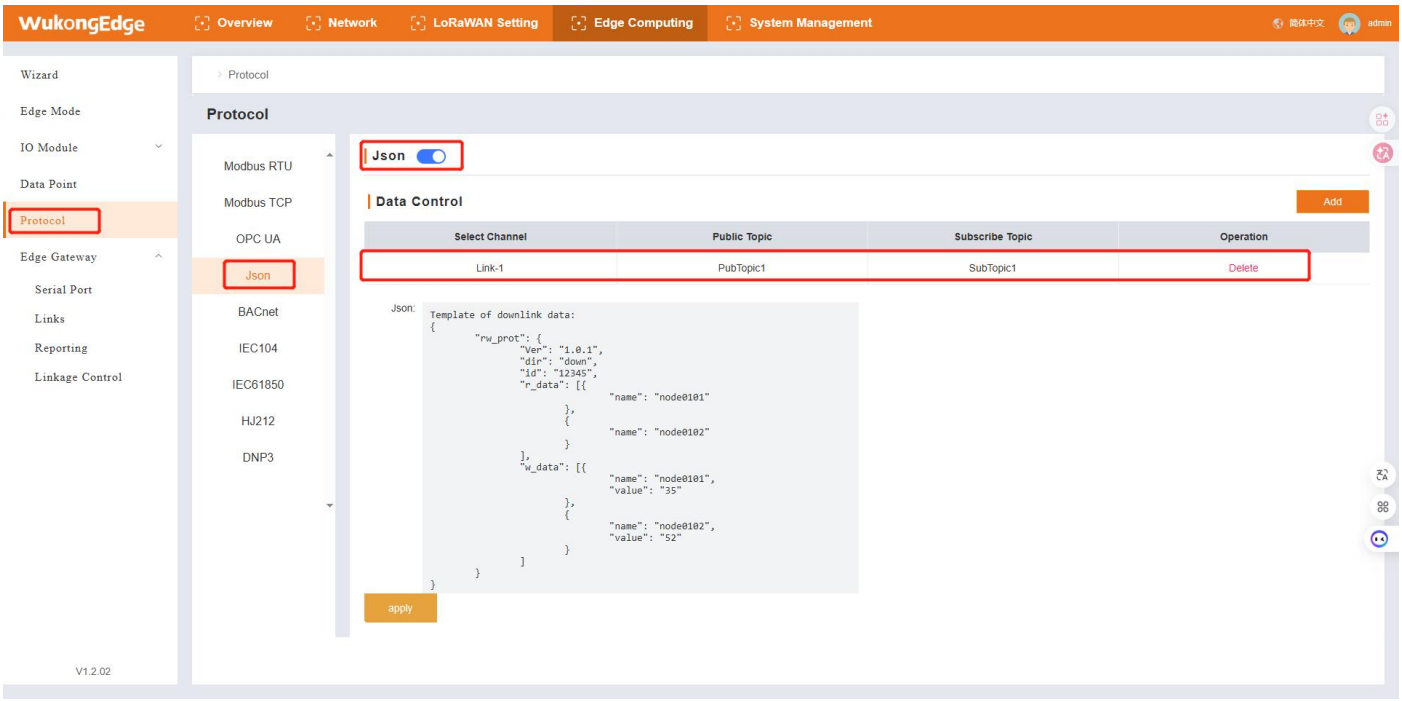


MQTTFX receives reported data, showing that terminal data has been successfully reported. At this point, the uplink is established.



Data Downlink

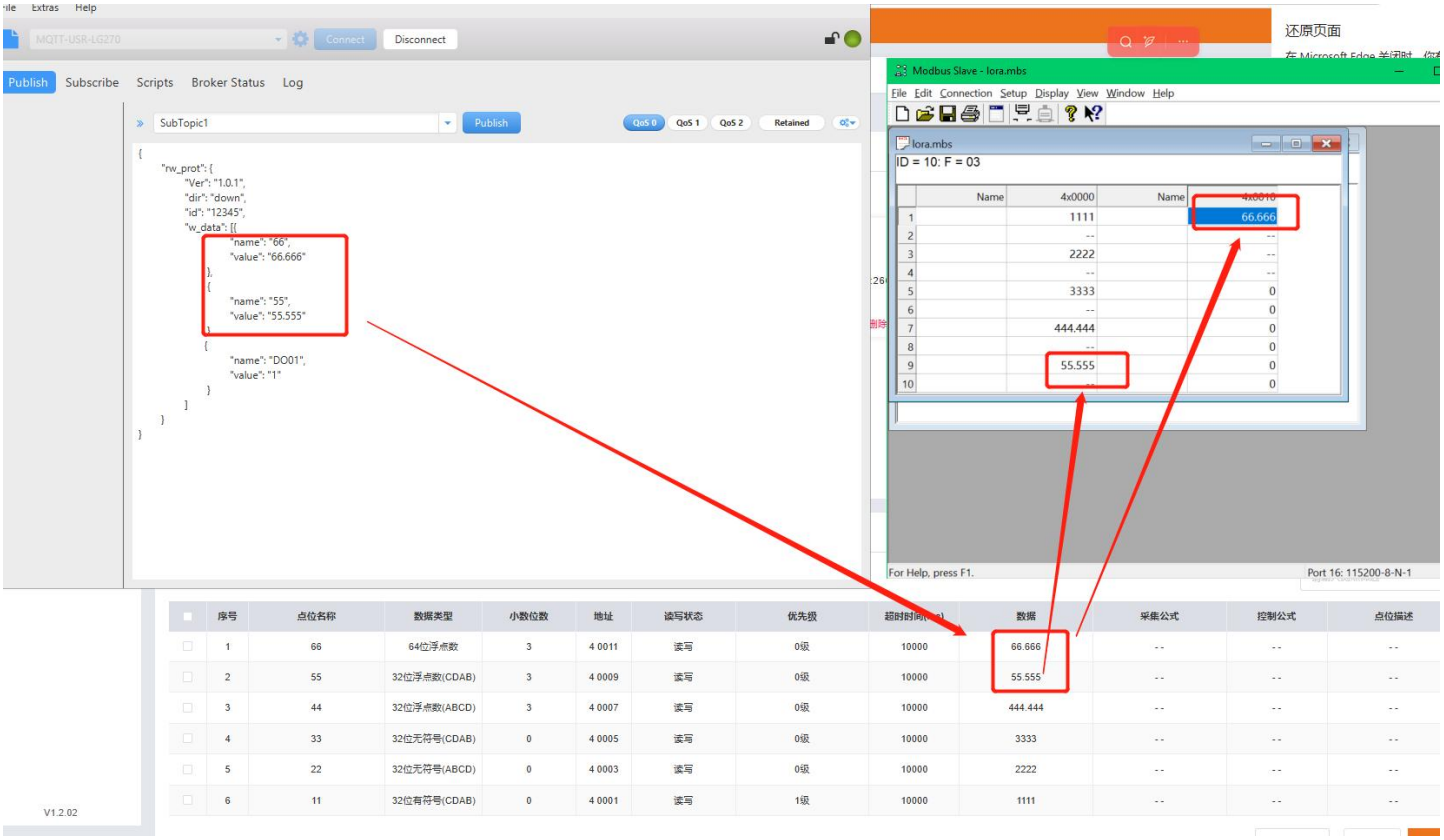
Protocol Conversion -- Enable Json function, add read/write configuration



After setting up Json protocol conversion, send control commands via MQTTFX to disconnect DO, and data points 66 and 55. The protocol format for sending data points can be copied directly from the interface shown in the image above. Using the protocol below, you can remotely control DO01 to disconnect and modify the data of terminal Modbus data points.

```
{
    "rw_prot": {
        "Ver": "1.0.1",
        "dir": "down",
        "id": "12345",
        "w_data": [{
                "name": "66",      Note: Name corresponds to the point name in the point list
                "value": "66.666"
            },
            {
                "name": "55",
                "value": "55.555"
            },
                    {
                "name": "DO01",
                "value": "1"
            }
```

```
        ]
    }
}
```



序号	点位名称	数据类型	小数位数	地址	读写状态	优先级	超时时间(ms)	数据	采集公式	控制公式	点位描述
1	66	64位浮点数	3	4 0011	读写	0级	10000	66.666	--	--	--
2	55	32位浮点数(CDAB)	3	4 0009	读写	0级	10000	55.555	--	--	--
3	44	32位浮点数(ABCD)	3	4 0007	读写	0级	10000	444.444	--	--	--
4	33	32位无符号(CDAB)	0	4 0005	读写	0级	10000	3333	--	--	--
5	22	32位无符号(ABCD)	0	4 0003	读写	0级	10000	2222	--	--	--
6	11	32位有符号(CDAB)	0	4 0001	读写	1级	10000	1111	--	--	--

5.4.3. Packet Forwarding Mode

Packet Forwarding is the basic function of a LoRaWAN gateway. The LoRaWAN gateway is responsible for receiving wireless packets (Uplink) sent by terminal devices and forwarding the data to the LoRaWAN Network Server via the IP network; at the same time, it receives downlink data (Downlink) from the Network Server and sends it to the corresponding terminal devices via the LoRa wireless link. During the entire communication process, the gateway itself does not participate in business data processing but acts as a bridge connecting the LoRa wireless network and the IP network, achieving bidirectional transparent data transmission.This mode is mainly suitable for customers who want to use external NS servers such as TTN, Chirpstack, etc.

Take accessing the TTN platform as an example to introduce the application of packet forwarding mode: For details, refer toUSR-LG270 Connection to TTN Platform Settings Instructions V1.0.0.pdf

6. Serial Port Management

6.1.Serial Port Configuration

Data acquisition is achieved through hardware interfaces, mainly network portsandserial port interfaces. This chapter mainly introduces serial ports. The parameter configuration operations are as follows:

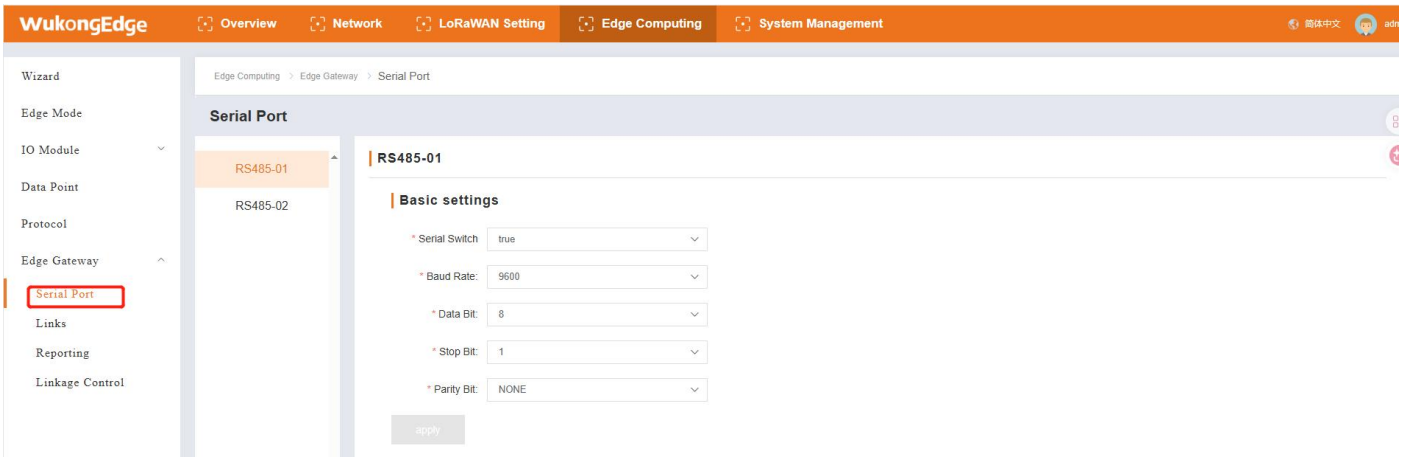
1. Enter the built-in web page, select the used serial port in the "Edge Computing -> Edge Gateway -> Serial Port Management" interface;
2. In the configuration interface of the selected serial port, after enabling the serial port, set the baud rate, data bits, stop bits, and parity bits;
3. After configuration, click Apply and**restart the device for changes to take effect**.

When hardware devices are connected to a serial screen, the screen and hardware device often need to interact via serial protocol to obtain data from the data point table. At this time, the serial port will be used as an uplink communication interface. WukongEdge also reserves a "Serial Port Function" option at the export end, allowing users to freely switch the communication direction of the serial port to meet different data transmission needs.

UplinkTransparent TransmissionInterface:Mainly used in combination with protocol conversion/serial transparent transmissionfunctions, providing serial channels for northbound protocols/bidirectional transparent transmissiondata collection;

Downlink Edge Collection:Mainly used in combination with edge collection functions, providing serial channels for southbound data collection.

Link Selection:A single serial portcan create 2 Socket links in transparent transmission mode, associated with the "Edge Gateway -- Communication Link" function.



6.2.Serial Port Framing Mechanism

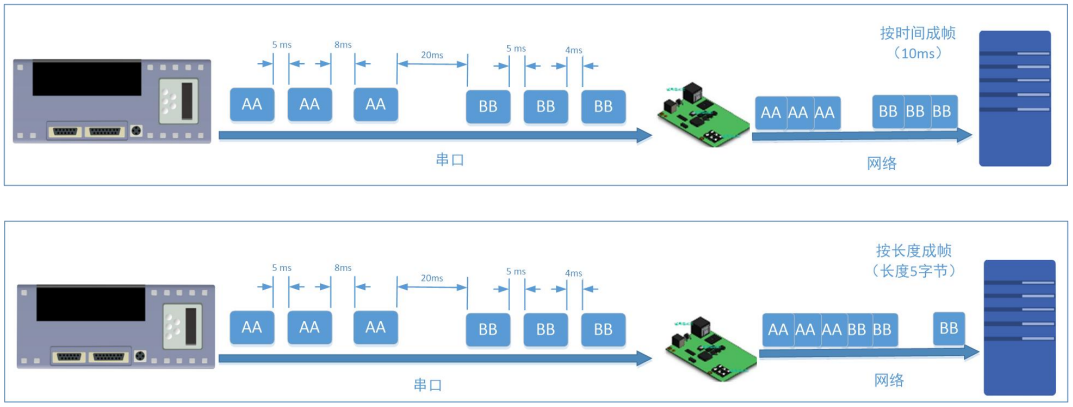


图 1. Serial Port Framing Description

LG270's serial data reception requires packetization and forwarding according to certain rules. The packaging rules mainly include packaging time and packaging length. When serial data entersLG270, if either the packaging time or packaging length condition is met, the data will be packaged and forwarded to the network.

Examples of packaging time and length determination:

1. If the packaging time is set to 10ms and the packaging length is 1460, when the serial port receives data, if the interval between received data exceeds 10ms, or the data length is greater than or equal to 1460, the data will be packaged and sent to the network.

2. If the packaging length is set to 0, only the packaging time takes effect.

3. When the packaging time is set to 0ms,LG270uses a default 4-byte packaging time. That is, when the interval between received serial data exceeds the time it takes to send four bytes,LG270executes data packaging. For example, at a baud rate of 115200, the four-byte packaging time is: T=0.4ms. If the calculated value is less than 0.1ms, the packaging time is calculated as 0.1ms.

$$T = \frac{1}{Baud\ Rate} * 10 * 4$$

WhenLG270receives network data and forwards it to the serial port, due to the limitations of serial speed, users need to control the sending traffic to avoid serial port data overflow. Therefore, when sending data from the network, data traffic needs to be calculated.

Calculation example:

Network data sends m bytes of data every n seconds. The method to check for potential overflow is: (assuming good network conditions and negligible network transmission time)

To avoid overflow, m bytes of data must be transmitted within n seconds. The transmission time for M bytes of data is:

$$T = \frac{1}{Baud\ Rate} * 10 * m$$

If n>2T, it indicates that data will not overflow, and theLG270server can work normally. If the baud rate is below 9600, maintaining n>T is sufficient.

7. Communication Link

7.1.Communication Link

As a network channel for reporting data to the server, communication links provide diverse connection methods to meet different user needs. It supports TCP, MQTT, and HTTP connections, allowing users to choose the appropriate connection method based on their business requirements. Additionally, to ensure data transmission security, communication links support TLS/SSL encryption and offer various encryption methods for users to choose from, further enhancing data confidentiality and integrity. During the configuration of reporting groups, the corresponding communication link needs to be selected, so the communication link configuration must be completed first. The specific operations are as follows:

1. Enter the built-in web page, and in the "Edge Computing -> Edge Gateway -> Communication Link" interface, enable the required communication links;

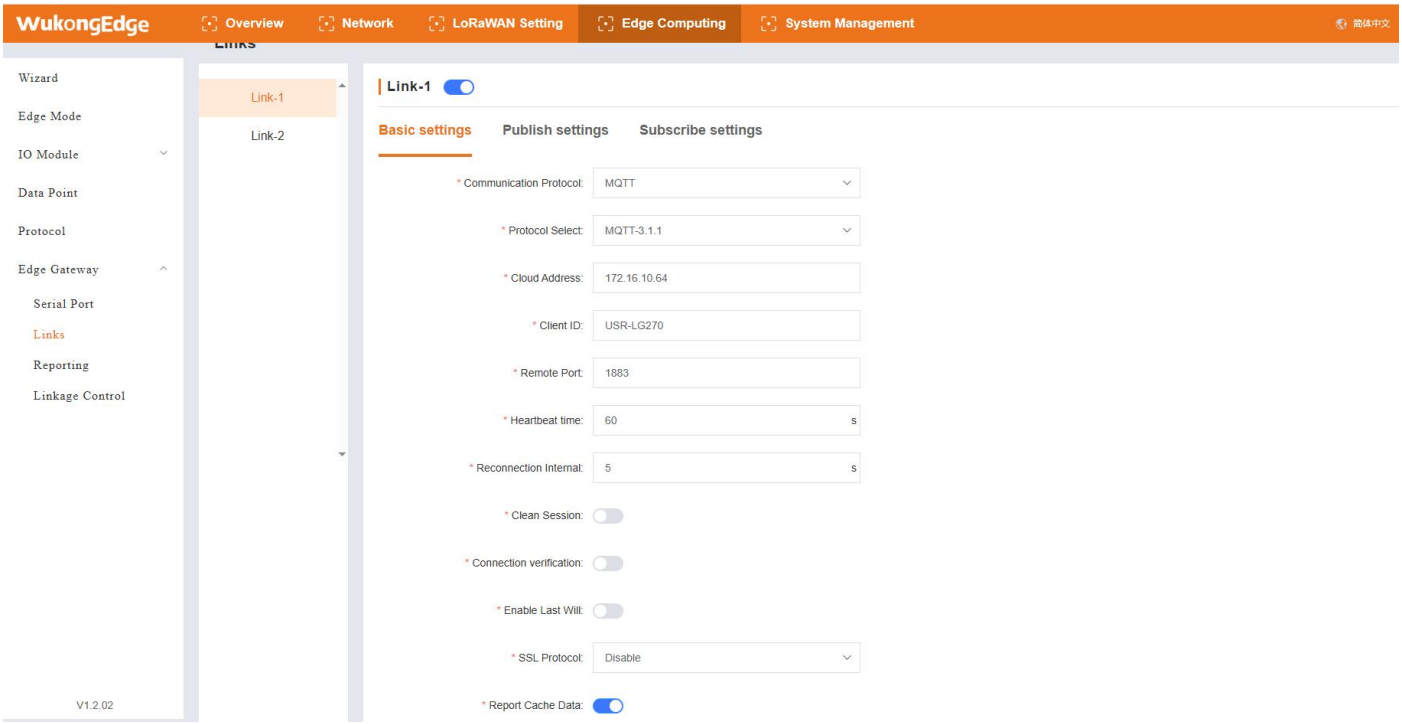
2. Configure the parameters of the enabled communication links. The communication protocol can be selected from TCP, UDP, HTTP,MQTTand other working modes;

3. Configure the encryption method, upload certificates, and enable offline caching;

4. After configuration, click the "Apply" button to save;

5. If MQTT communication is selected, configure the corresponding publish and subscribe topics after completing the basic parameter configuration;

6．After all communication link parameters are configured,**the device needs to be restarted for the changes to take effect**.



7.2.Offline Caching

WukongEdge has a built-in offline caching function in its communication links, which is crucial. Once a network failure occurs, it can quickly store the data being reported to prevent data loss due to disconnection. When the network recovers, it will automatically report the cached data to the server accurately, ensuring data integrity.

The offline caching function stores complete data packets during active reporting, not just single data points. When the network recovers, the cached data is reported to the server following the First-In-First-Out (FIFO) principle, achieving fast and accurate reporting.

When configuring communication links, the offline caching function needs to be enabled simultaneously.

8. Edge Computing

In the industrial field, edge computing plays an irreplaceable key role, covering four core functions: data acquisition, real-time computation and processing, result reporting, and visualization. In terms of data acquisition, edge computing devices can quickly and accurately collect massive amounts of data from various

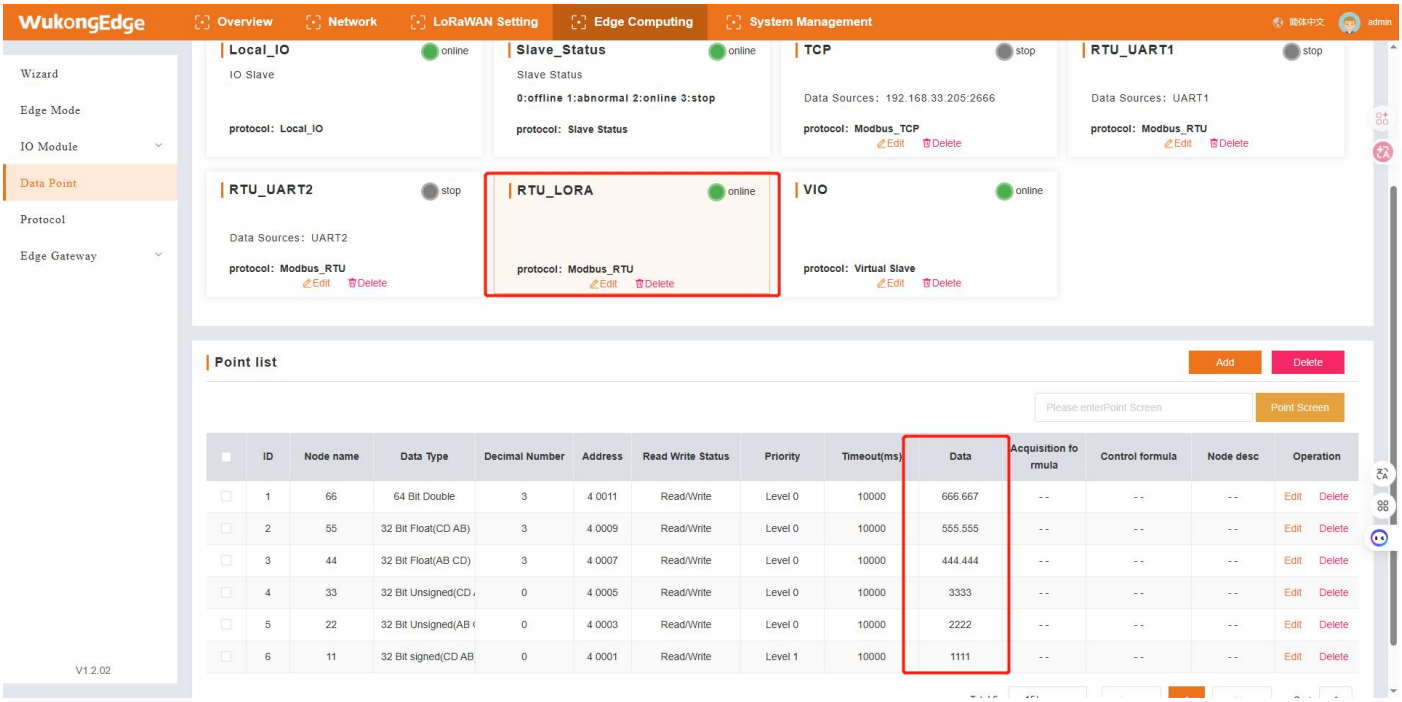
sensors and production equipment at the industrial production site, including operating parameters such as temperature, pressure, and vibration, as well as product quality data on the production line.

In the real-time computation and processing phase, leveraging powerful local computing capabilities, collected data can be analyzed instantly. For example, real-time monitoring and analysis of equipment operation data can predict potential equipment failures in advance, enabling preventive maintenance, ensuring production continuity and stability, and significantly reducing downtime losses caused by equipment failures.

Key processed data is promptly reported to industrial cloud platforms or enterprise management central systems, providing decision-making basis for management. Finally, through intuitive visualization interfaces, key information such as production progress, equipment status, and quality indicators is clear at a glance, allowing managers to grasp production dynamics in real-time, make scientific decisions quickly, optimize production processes, and improve overall production efficiency and quality.

WukongEdge applications integrate these powerful edge computing functions, meeting current industrial data processing requirements with their high integration and efficient processing capabilities, providing strong technical support for the digital transformation of industrial enterprises.

8.1.Data Point Table



As the data cornerstone of the gateway, the data point table occupies a core position in the entire data acquisition and transmission system. It is like a dense information network, with each data point being a key node in this network. The number of data points directly determines the breadth and depth of the gateway's data acquisition; the denser the points, the more massive the data the gateway can capture, providing rich raw materials for subsequent analysis and processing.

With the increasing demand for data volume, the performance of the gateway has also significantly enhanced. A large amount of data not only enriches the gateway's information reserve but also provides richer basis for judgment when the gateway performs data analysis. Meanwhile, supported by abundant data, the gateway can make more precise judgments in aspects such as equipment status monitoring, production process control, and abnormal situation warning, thereby ensuring the efficient and stable operation of the entire industrial system.

WukongEdge application integrates the point table system, which can flexibly adjust the amount of point data according to different adapted hardware. Meanwhile, the configuration interface is simple, adapting to numerous acquisition protocols, making it suitable for more data acquisition scenarios.

8.2.Slave Devices and Points

As a key part of data acquisition, the point table system includes two important components: slave devices and points. Slave devices represent the equipment being acquired, such as various production machinery and sensors, while points represent specific data in the acquired equipment, such as equipment temperature, rotation speed, and other parameters. Both slave devices and points are configured with detailed information, which acts as precise navigation to help the gateway accurately obtain data from the acquired equipment through fixed interfaces, providing a solid data foundation for subsequent data analysis and processing. The slave devices in the point table system are divided into fixed slave devices and configurable slave devices.

The point data obtained by fixed slave devices are mainly equipment parameters themselves, so no configuration is needed. The main types are as follows:

System Slave Device: Mainly obtains the system parameters of the gateway itself, and stores and displays each parameter as a point.

Status Slave Device: For each additional configurable slave device, an online status point will be automatically generated under that slave device.

Configurable slave devices represent the acquired equipment, so users need to manually add them, configure the corresponding hardware interfaces, acquisition protocols, and other related information of the acquired equipment, and add corresponding point information under the slave device. Configurable slave devices support multi-protocol selection, and the parameters corresponding to each protocol are different. The specific parameter descriptions are as follows:

Name	Parameter Description	Default Parameter
Slave Name	1-64 bytes, serves as the unique identifier for the slave, cannot be duplicated, supports Chinese characters	device1
Slave Description	Supports 1-64 bytes, including letters, numbers, Chinese characters, underscores, and hyphens	Empty

Collection Protocol	The protocol used for active polling collection of slave data points, supports Modbus and various PLC protocols	Virtual Slave
Polling Interval	The waiting time before sending each data point collection command, range 0~65535ms	0ms
Merged Collection	Several consecutive address data points in a single slave are merged into one command for collection, up to 32 points per command	On
Slave Switch	When disabled, all data points under the slave will stop active polling collection and data updates	Enabled
Slave Address	The slave code of the downstream device, setting for some protocols	1
Serial Port Number	The number of the serial port used by the serial device to send data point collection commands, setting for some protocols	1
Device EUI	When collecting LoRaWAN nodes via LoRaWAN network, the EUI information of the LoRaWAN node needs to be entered,setting for some protocols	Empty
Fport	When collecting LoRaWAN node data, the port number corresponding to the node needs to be entered, otherwise data cannot be collected normally,setting for some protocols	10
IP	When collecting via network port, M300 acts as Client, target IP needs to be filled in, setting for some protocols	192.168.1.1
Port	When collecting via network port, M300 acts as Client, target port needs to be filled in, setting for some protocols	102

List of acquisition protocols for slave devices:

Acquisition Protocol	Protocol Description	Applicable Scope

Virtual-point (Virtual Slave)	Calculation points independent of acquisition points	Virtual points, also known as calculation points, are new data obtained after calculating multiple acquisition points within the point table system. A maximum of 1000 virtual points can be stored (varies by hardware; please confirm based on the specific product selection table).
Modbus RTU	Generic serial bus protocol	Acquisition via serial communication buses such as RS485/RS232 Applicable to certain models of PLCs from Delta, ABB, HollySys, Modicon, etc.
Modbus TCP	Generic network bus protocol	Suitable for acquisition via network protocols such as Ethernet
DVP_RTU	Delta PLC protocol	Acquisition for Delta DVR series PLCs
FATEK_COM	Fatek PLC protocol	Fatek FATEK series (Serial Port)
FX Protocol	Mitsubishi PLC protocol	FX2N (1N) / FX1S / FX3U
FX5U	Mitsubishi PLC protocol (MC 3C/3E)	Mitsubishi FX5U series (Ethernet and Serial Port)
FX3U_ADP_TCP	Mitsubishi FX3U_MC_ADP	FX3U-ENET-ADP
Q_TCP	Mitsubishi PLC protocol (MC_TCP)	Mitsubishi Q series PLCs
H3_5U_TCP	Inovance PLC protocol	Inovance H3U, H5U
S7_200 Smart	Siemens PLC protocol	S7-200 Smart
S7_200_PPI	Siemens PLC protocol	S7-200
S7_1200	Siemens PLC protocol	S7-1200
S7_1500	Siemens PLC protocol	S7-1500
S7_300	Siemens PLC protocol	S7-300 (Ethernet)
S7_400	Siemens PLC protocol	S7-400 (Ethernet)

FINS_TCP	Omron	CP Series
FINS_COM	Omron	CP Series
DL/T 645-2007	Communication protocol for multi-function energy meters	Various types of energy meters
IEC104	Power industry protocol	Power data transmission DL/T 634.5104-2009
IEC61850	Power industry protocol	Communication protocol for power system automation
DNP3.0	Distributed Network Protocol 3.0	Communication protocol for power automation
Bacnet IP	Building automation protocol	Data communication protocol for building automatic control networks
EtherNET/IP	Industrial Ethernet communication protocol	Industrial Ethernet communication protocol

After adding the slave device, add the corresponding point information under the slave device.

The point parameters are described as follows:

Name	Parameter Description	Default Parameter
Point Name	1-64 bytes, unique identifier when reporting the point, cannot be duplicated with any other point	Empty
Point Description	1-64 bytes, supports characters, numbers, and Chinese	Empty
Register	Storage type and storage address of the point	
Data Type	Type selection for point collected data	
Number of Points	Total number of points with consecutive addresses added in a single batch under the same slave device	1
Decimal Places	Number of decimal places displayed when the calculated result of collected data is a decimal	0

Read/Write Status	Read/write status of the point; different point types support different read/write types	Read/Write
*Priority	When polling all points, high-priority points are guaranteed to be polled according to the cycle first, ensuring real-time collection of high-priority points	Empty
Collection Formula	Point calculation formula. The collected data is calculated internally by the device according to the formula, then stored and provided for use by other functions	Empty
Control Formula	When performing a write operation on this point, the result is written to the terminal device after being calculated by the control formula	Empty
Timeout	During point polling collection, the maximum time to wait for a response after sending a command. If timed out, this collection is automatically abandoned, historical data is not updated, and the next collection command is executed. Range: 10~60000ms. Note: Since LoRa wireless data collection is affected by rate, the default timeout value is 10000ms	2000ms
Unit	Non-mandatory parameter, set as needed	Empty

Note: Priority feature is under development.

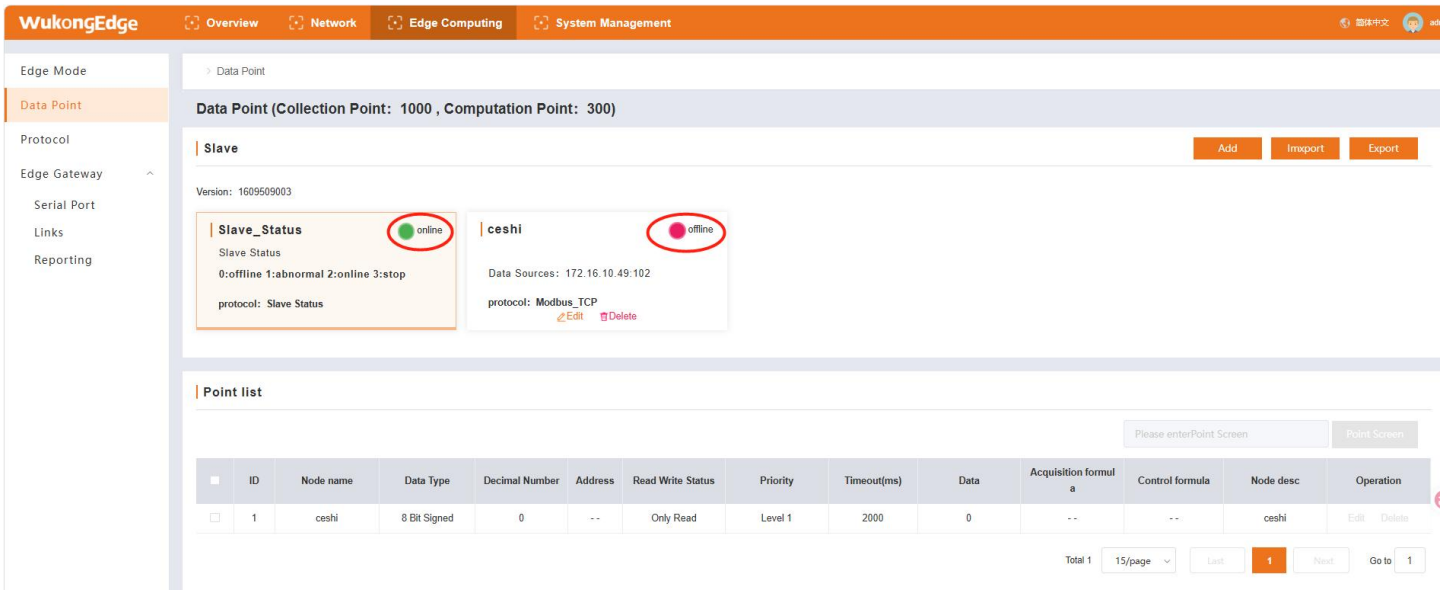
8.3.Slave Status

The data point status display feature allows users to intuitively view the online status of slaves from the built-in web page. Slave statuses are categorized as Online, Offline, and Abnormal.

Online: All data points in the slave have been successfully collected; the corresponding slave status point value in the slave is 2;

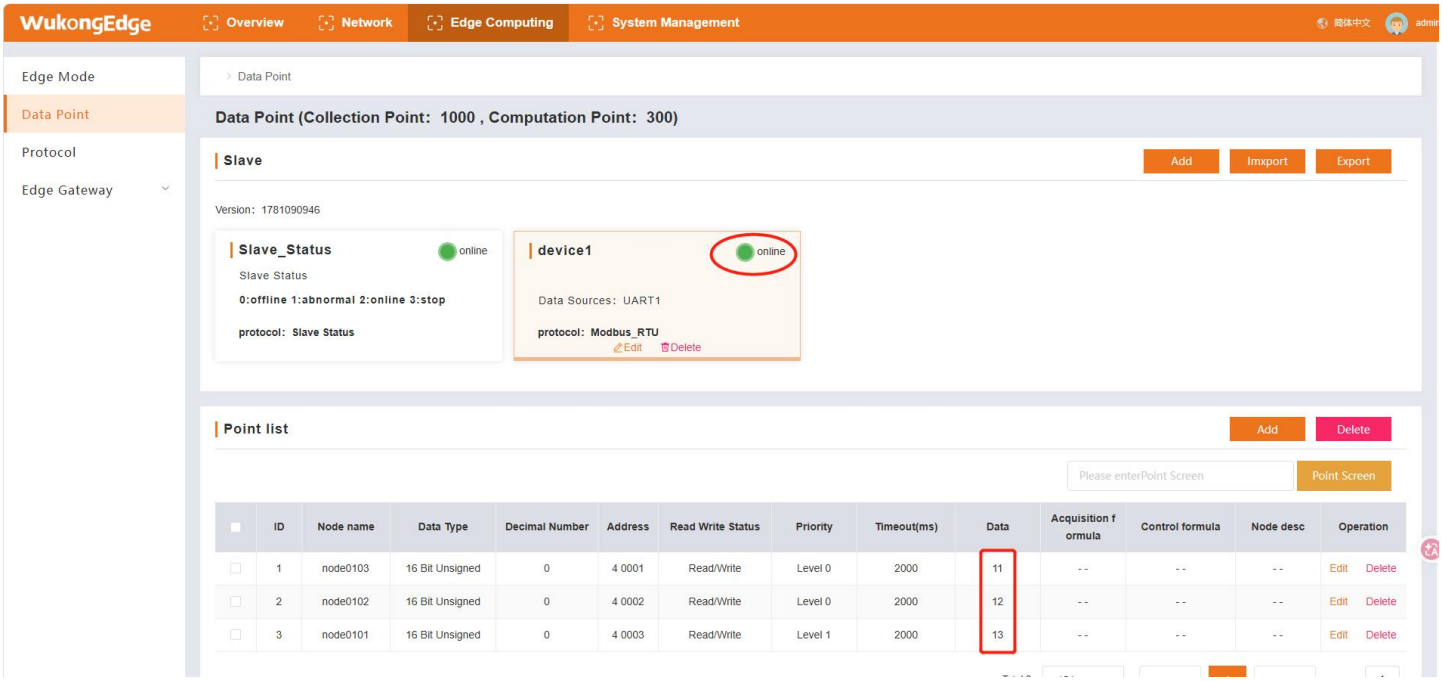
Offline: All data point collections in the slave have failed; the corresponding slave status point value in the slave is 0;

Abnormal: Some data points in the slave have been successfully collected; the corresponding slave status point value in the slave is 1.



8.4.Point Data

After data is obtained for the slave points in the data point table, it can be displayed on the built-in web page. The data updates continuously with collection, allowing users to directly observe the data within the device.



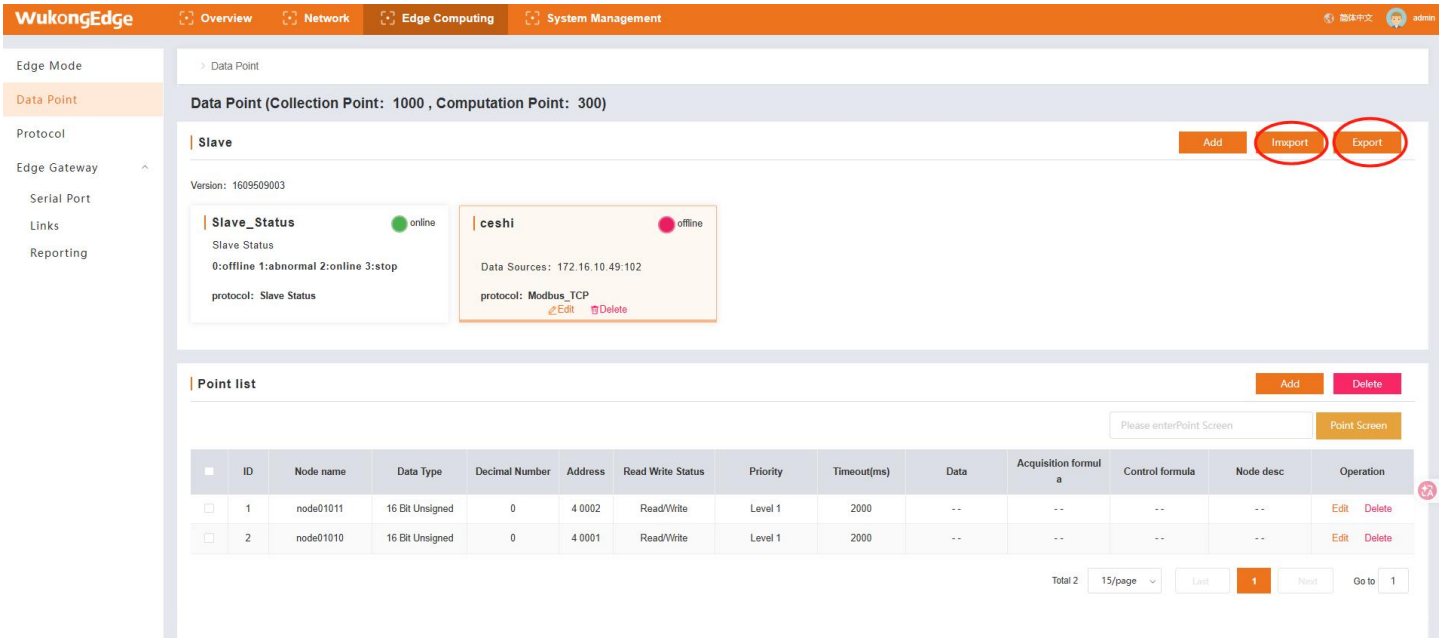
8.5.Import/Export

In the WukongEdge point system, point information in the data point table needs to be added manually. When only some information of certain points differs, using spreadsheet tools like Excel for editing can greatly

improve efficiency. To this end, the WukongEdge point system thoughtfully integrates point export and import functions. Users can first export a point template, quickly edit point information in a familiar spreadsheet environment, and then import the edited file into the device. This allows for more efficient and convenient completion of point addition tasks, significantly saving labor and time costs.

Operation steps:

1. For first-time use, it is recommended to add a slave and points in the device first, then export. The file will show corresponding addition examples;
2. Go to the "Edge Computing - Data Points" interface, find the "Export" button, and click to download the point table template file;
3. In the downloaded CSV file, fill in the relevant parameters for slaves and points according to the headers, and save the file after completion;
4. Go to the "Edge Computing - Data Points" interface, find the "Import" button, click it, and select the saved file to upload;
5. After the device recognizes the file, it will automatically display the corresponding slaves and points, and prompt to restart the device;
6. The device restarts and executes the data collection function after startup.

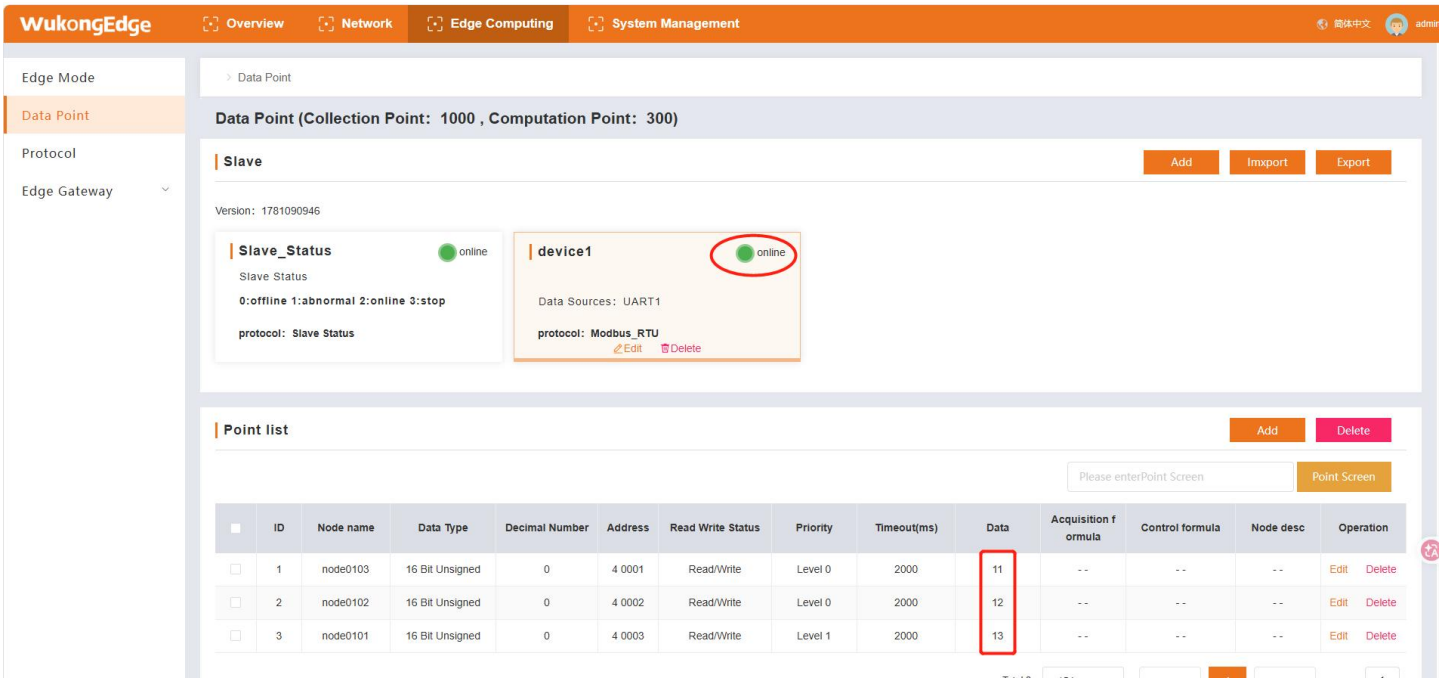


8.6.Edge Collection

The edge collection function mainly relies on hardware gateway devices. When actively collecting sensor data, you first need to enter the data information of the collected device into the gateway device, which is the addition of the data point table. Then, the gateway can automatically obtain data from the collected device based on this information and store the acquired data.

The edge collection process involves point table configuration and collection interface configuration. The steps for active collection are as follows:

1. Enter the built-in web page, go to the "Edge Computing -> Data Points" interface to add a slave, and select the corresponding communication interface;
2. Under the added slave, add the corresponding point information and complete the addition of all points;
3. After configuration is complete, restart the device;
4. After the device restarts, it will actively send data collection commands to the collected device via the corresponding interface, receive the response content, and parse the data;
5. In the point table system, the latest data obtained for each point will be displayed.



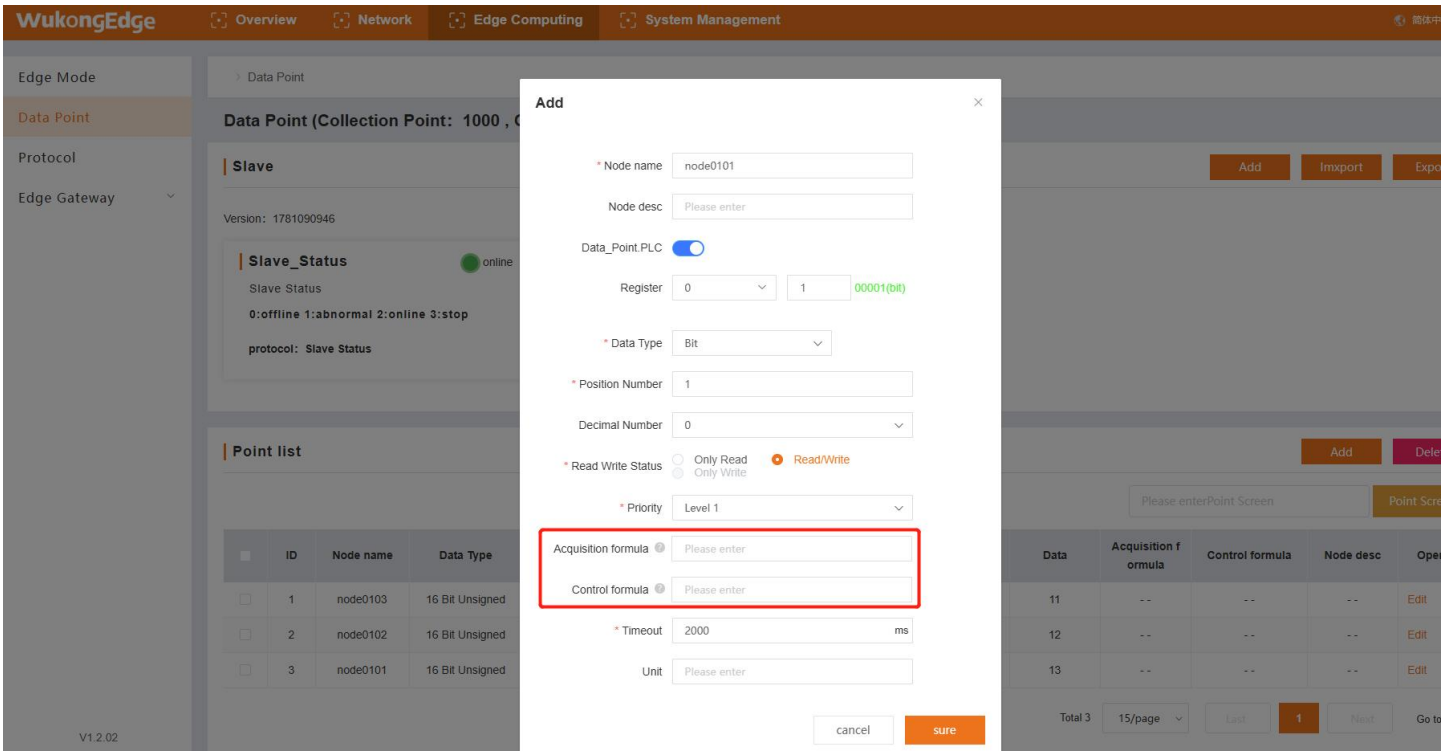
8.7.Edge Computing

After data collection is complete, preliminary data processing is performed leveraging the high-speed computing capability of the chip, significantly accelerating data processing speed. Moreover, since data is processed locally, it reduces the risk of data exposure during network transmission, effectively ensuring data security. Additionally, performing preliminary processing on large amounts of data locally reduces the volume of data uploaded to the server, thereby lowering the server's load pressure and making the entire system run more efficiently and stably.

WukongEdge integrates two methods of data calculation: single-point calculation and multi-point calculation. Both methods are implemented through calculation formulas, supporting five operations: addition, subtraction, multiplication, division, and parentheses (). Data calculation is configured individually for each point during the addition of points in the point table.

Single-point calculation: Single-point calculation targets collection points, where data is obtained through active collection. When adding a collection point, fill in the corresponding formula in the point collection calculation and control calculation parameters. The single-point calculation formula only pulls data for the current point, calculates the result according to the formula, and fills the result into the storage location of that point.

Parameter	Function	Formula Style	Parameter Description
Collection Formula	Calculates the collected data to derive a result and stores it, waiting for upload to the server	=(%s+10)/2	%s represents the current point data
Control Formula	Receives control data issued by the server, calculates the result, and sends it down to the collected device to achieve parameter control	=(%s*2)-10	%s represents the current point data



Multi-point Calculation: Virtual slave devices need to be added, and virtual points need to be added under the virtual slave devices. When adding, fill in the corresponding formula in the collection formula. In the multi-point calculation formula, data from multiple collection points will be pulled for calculation, and the calculated results will be filled into the virtual point.

Parameter	Function	Formula Style	Parameter Description
Collection Formula	Calculate the results from multiple collected data and store them, waiting to be reported to the server	=(%s+10)/%s,node0101,node0102	The first %s represents the data collected by point node0101; The second %s represents the data collected by point node0102.

Steps to Add Virtual Slave Devices and Calculation Points are as follows:

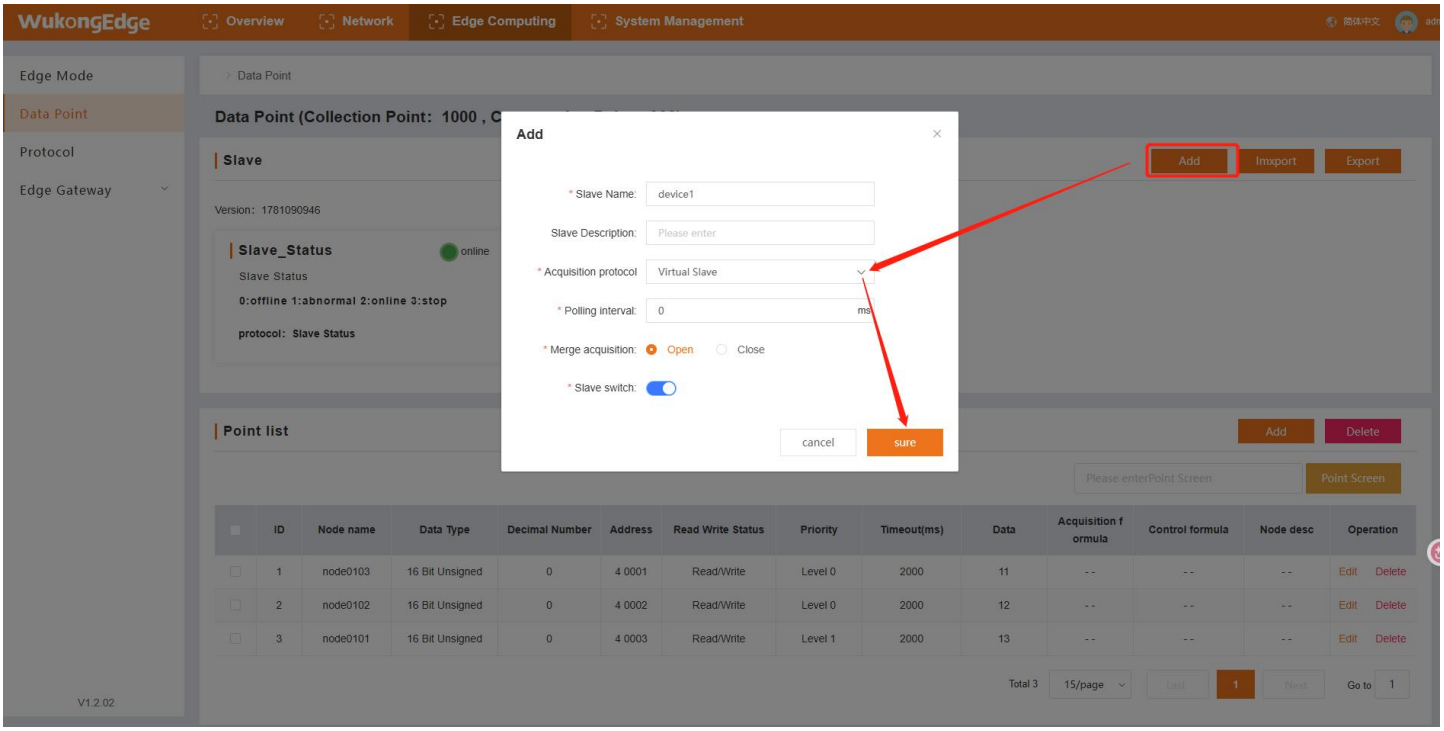
1. Enter the built-in web page, and add slave devices in the "Edge Computing -> Data Points" interface, selecting "Virtual Slave Device" as the collection protocol;
2. After adding the slave device, select the virtual slave device and add virtual points, setting the

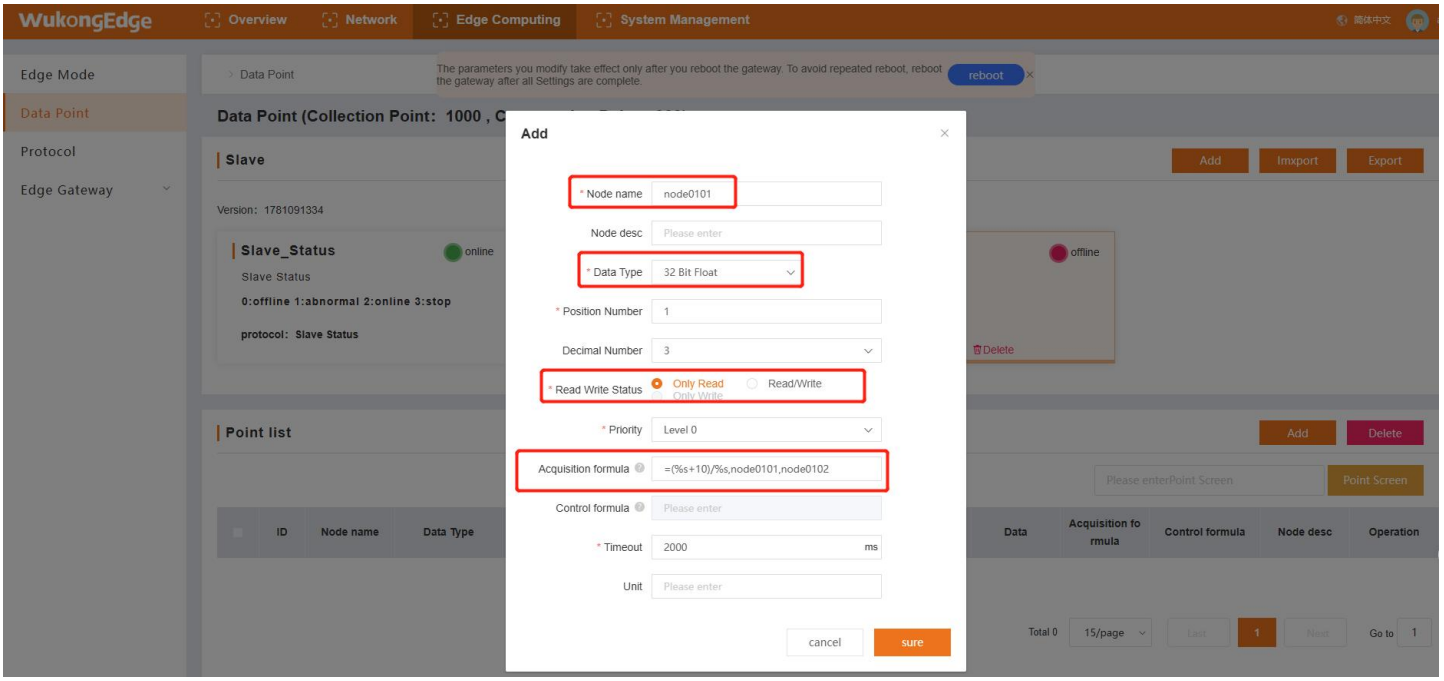
data type and collection formula, etc.;

3. Set the control formula of the virtual point to empty, and set the read/write status to read-only;

4. After configuration, restart the device;

5. After the device restarts, when the points involved in the virtual point collection formula complete data collection, the corresponding virtual point will display the calculated data.





8.8.Active Reporting

The reporting function is a key final step in edge computing. After completing data collection and local calculation, the resulting data is transmitted to the server. These data, initially processed by edge computing, provide a foundation for subsequent complex analysis, processing, and visualization on the server. Active reporting means that after edge computing is completed, the system actively encapsulates the data in Json format and then accurately reports the data to the server via the network. This method not only ensures the standardization of data transmission format but also improves the autonomy and efficiency of data transmission, strongly supporting deep data applications on the server side.

In the WukongEdge application, the active reporting function is divided into two parts: communication link and data reporting, which will be introduced separately.

8.8.1. Active Reporting

The active reporting built into WukongEdge adopts a grouped reporting mode. Users can independently choose different communication links and points for different groups according to actual needs, thereby flexibly reporting data to different servers, easily achieving multi-link and multi-platform data sharing.

Parameter Introduction

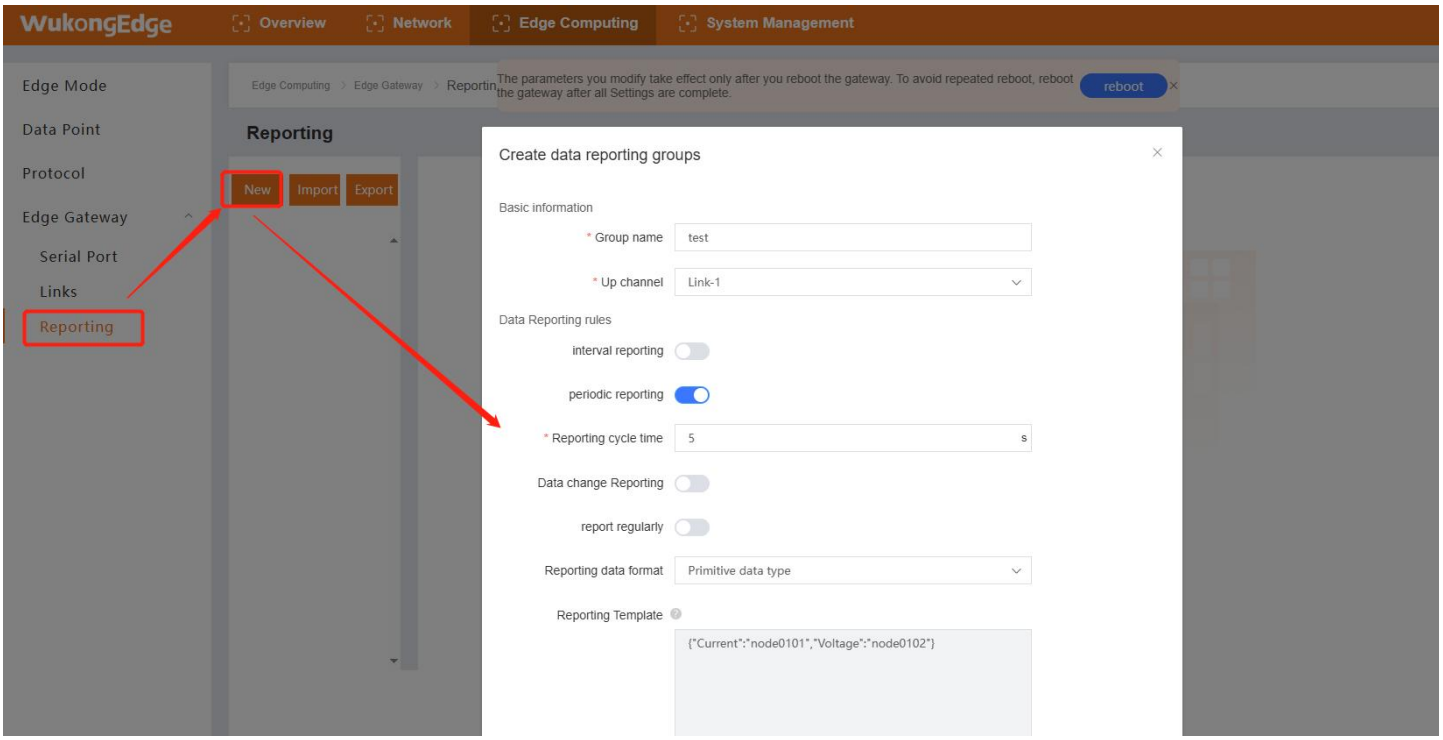
Name	Parameter Description	Default Parameter
Uplink Channel	The data network channel for active reporting, options includePUSR Cloud/Link 1/Link 2	Empty
Reporting Rules	Supports four reporting conditions (range/periodic/change/timed reporting), multiple selection supported	Empty
Reporting Data Format	Original Type: Point data is reported to the server according to the original type Number to String: If the point data is of number type, "" will be added during reporting to convert the number format to string format, and then report to the platform	Empty

Reporting Template	Custom Json, must comply with Json format specifications, maximum template size is 8K bytes.	Empty
Point Table	Each active reporting group acts as an independent entity, pulling the points needed for reporting from the overall data point table to serve as the point table used exclusively by that group.	Empty

The specific operational steps for group active reporting are as follows:

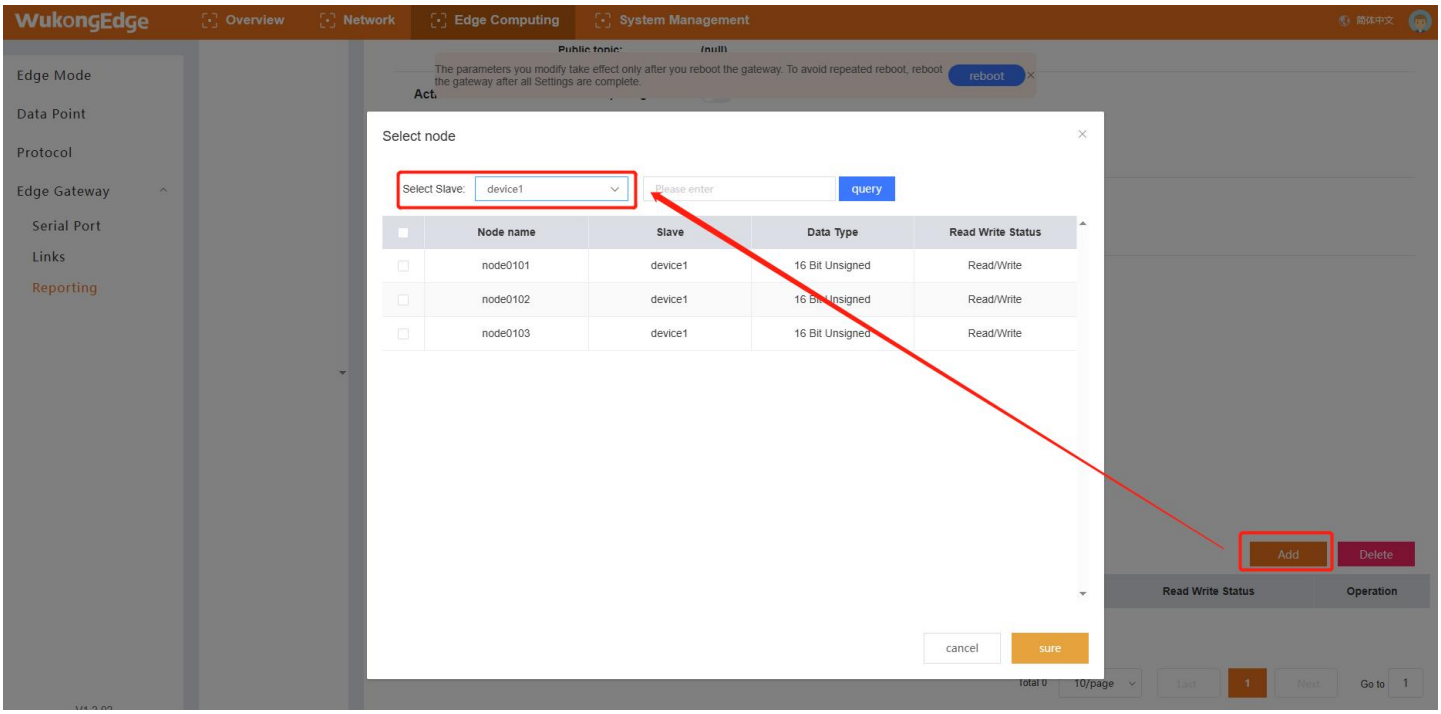
1. Enter the built-in web page, click the "Create" button in the "Edge Computing -> Edge Gateway -> Data Reporting" interface to create a reporting group;

2. Select the reporting channel and configure parameters such as the reporting Json template and reporting conditions;



3. After completing the group addition, find the point table within the group and click the "Add" button, a pop-up window will appear;

4. Select the corresponding slave device and points, then click OK (when there are many points in the slave device, you can select the slave device and directly search for the point name);



5. After selection is complete, finish adding the reporting group. The reporting group will take effect after restarting the device;

6. Wait for the device to successfully connect to the server, then check the data reporting status.

8.8.2. JSONTemplate

The data format for active reporting is a custom Json template. Therefore, before introducing active reporting, let's first understand the configuration method for the reporting Json template. As long as the active reporting data format complies with the Json format, configuration can be achieved, generally configured by customers according to server requirements. However, please note the following points when configuring the Json template:

1. The Json template in the group is empty by default and can be designed by yourself, as long as it meets the Json format requirements

2. In the Json template, the Value is of character type and requires filling in the data point name. During data reporting, the actual collected value corresponding to the point name will be substituted;

3. Example: The collected values for edge points node0101 and node0102 are 30 and 20 respectively;

4. **Set the Json template to {"Current":"node0101","Voltage":"node0102"};**

5. **The actual reported data format is: {"Current":30,"Voltage":20}.**

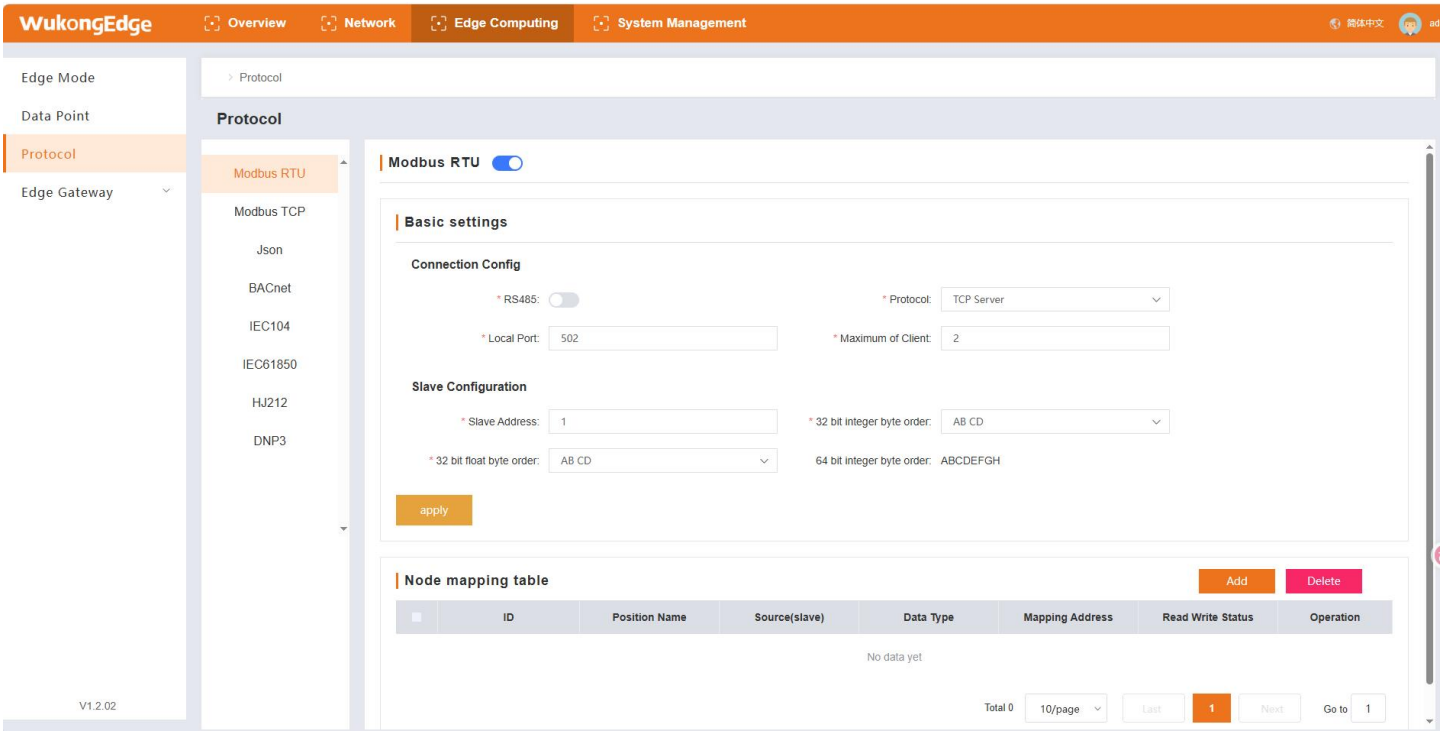
6. **System points can be reported as data points.**

Identifier	Meaning	Report Content Example
sys_utc_time	UTC Time	2026-05-08T10:59:07Z
sys_local_time	Local Time	2026-05-08,19:00:02
sys_local_time2	Local Time (without comma)	2026-05-08 19:05:22
sys_unix_time	Millisecond Timestamp	1778238033186
sys_sn	SN	02700122093000012356
sys_mac	MAC	D4AD20474662
sys_imei	IMEI	864452061930390
sys_iccid1	ICCID (SIM1)	89861122219045577705
sys_iccid2	ICCID (SIM2)	89861122219045577705
sys_ver	Product Firmware Version	V1.0.14.000000.0000
sys_csq	4G/5G Signal	29
sys_longitude	Longitude (+ for East, - for West)	+117.09974683
sys_latitude	Latitude (+ for North, - for South)	+36.66520733
sys_speed	Ground Speed	0.00000000
sys_satellite	Number of Satellites	5
sys_gps_state	Positioning Status	A/V
sys_timestamp	Timestamp (32-bit unsigned ABCD format)	1706167861
sys_timestamp_str	Timestamp (string format)	1778238427
sys_timestamp_ms	Millisecond Timestamp	1601196762389

8.9.Protocol Conversion

The protocol conversion function of WukongEdge establishes a standardized protocol interaction channel between data and the server. Through edge computing capabilities, hardware interfaces can collect data from various different protocols. Under the operation of the protocol conversion function, these data are uniformly converted into a fixed protocol, thereby achieving smooth interaction with the server.

The protocol conversion function supports multiple protocols, including Modbus RTU, Modbus TCP, OPC UA, JSON, Bacnet, IEC104, IEC61850, HJ212, and DNP3.0. The protocol conversion function allows multiple protocols to communicate in parallel simultaneously, with each protocol having an independent operating mechanism that does not interfere with others. Moreover, each protocol has an independent data mapping table, which ensures that the protocol conversion process runs stably and efficiently, providing solid and reliable technical support for various complex industrial scenarios and diverse data interaction needs.



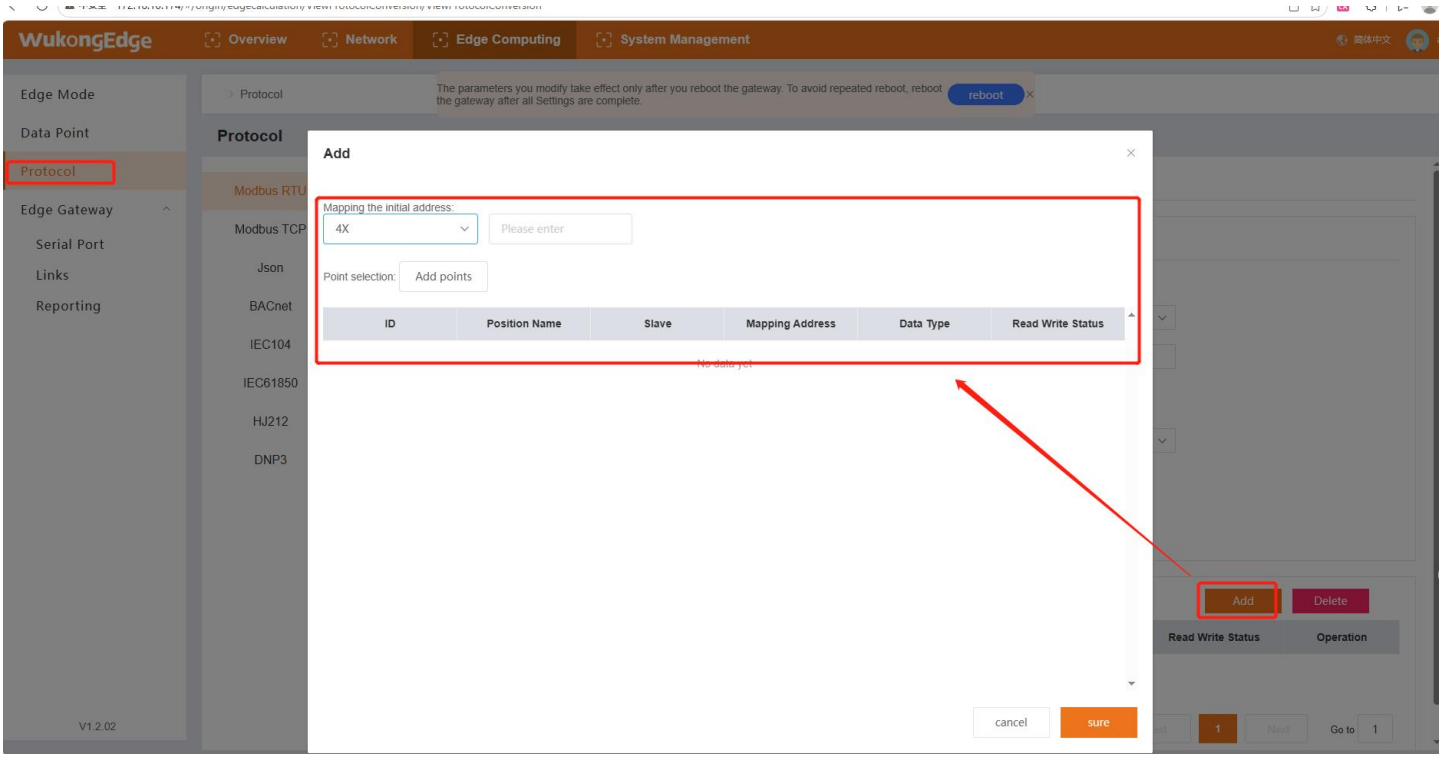
The logic for using the protocol conversion function is to perform the following operations based on the completion of the data point table configuration:

1. **Enter the built-in web page, go to "Edge Computing -> Protocol Conversion", and select the matching protocol for configuration**

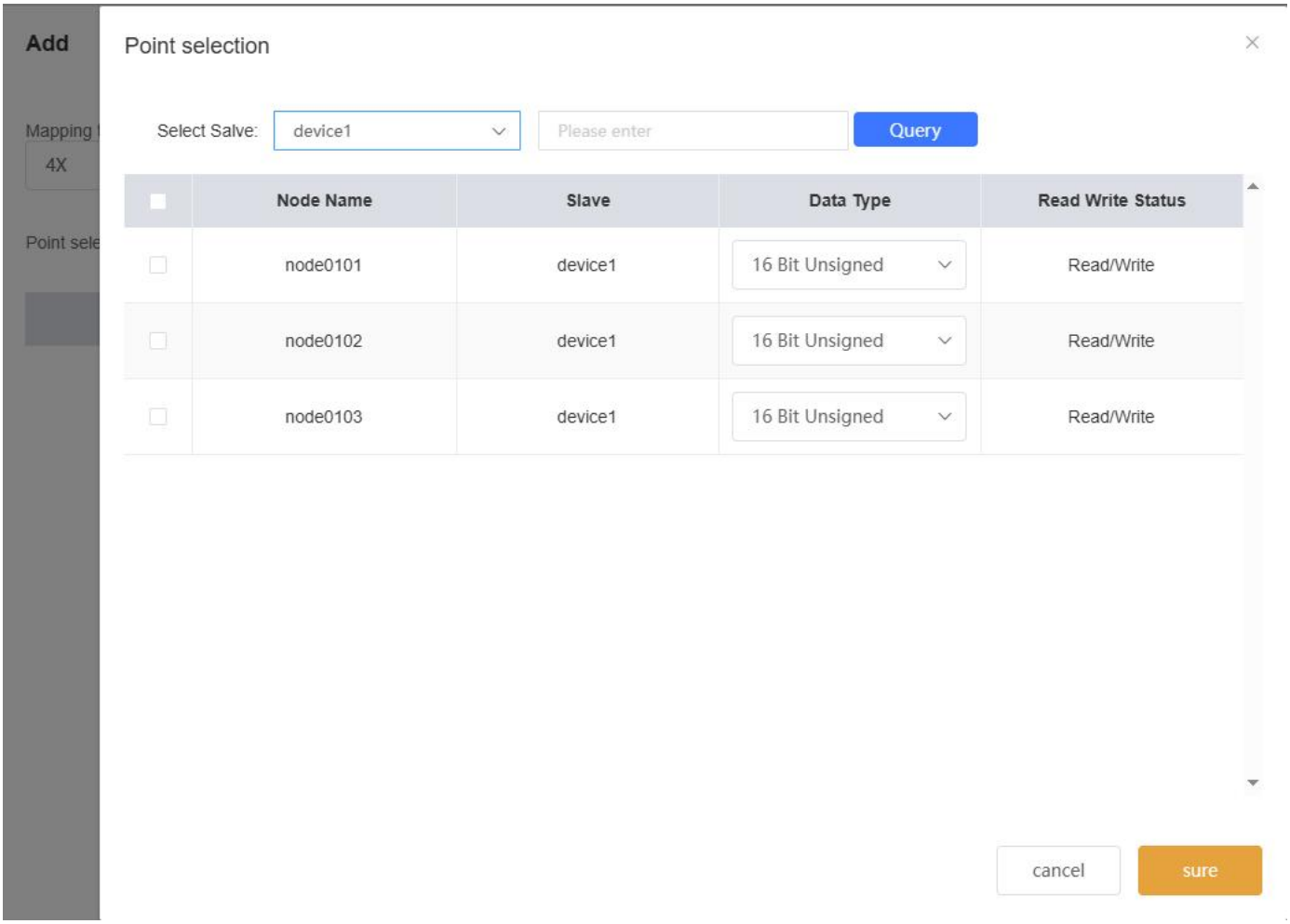
2. Enter the selected protocol interface, configure the protocol enablement, and set related parameters;

3. After parameter configuration is complete, click the "Apply" button to save the parameters;

4. Add point mapping. In the selected protocol interface, find the "Point Mapping Table", click the "Add" button, a pop-up window will appear, set the mapping address for the corresponding protocol;



5. In the pop-up window, set the mapping address, click the "Add Point" button, and the point selection pop-up window will appear;



6. Select the slave device and points, configure the point data type, and after confirmation, click the "OK" button to return to the previous level;

7. After returning to the mapping address configuration pop-up window, confirm that everything is correct, then click the "Confirm" button to complete the addition of the mapping address;

8. After all basic parameters and point mappings are set and saved, restart the device for the changes to take effect;

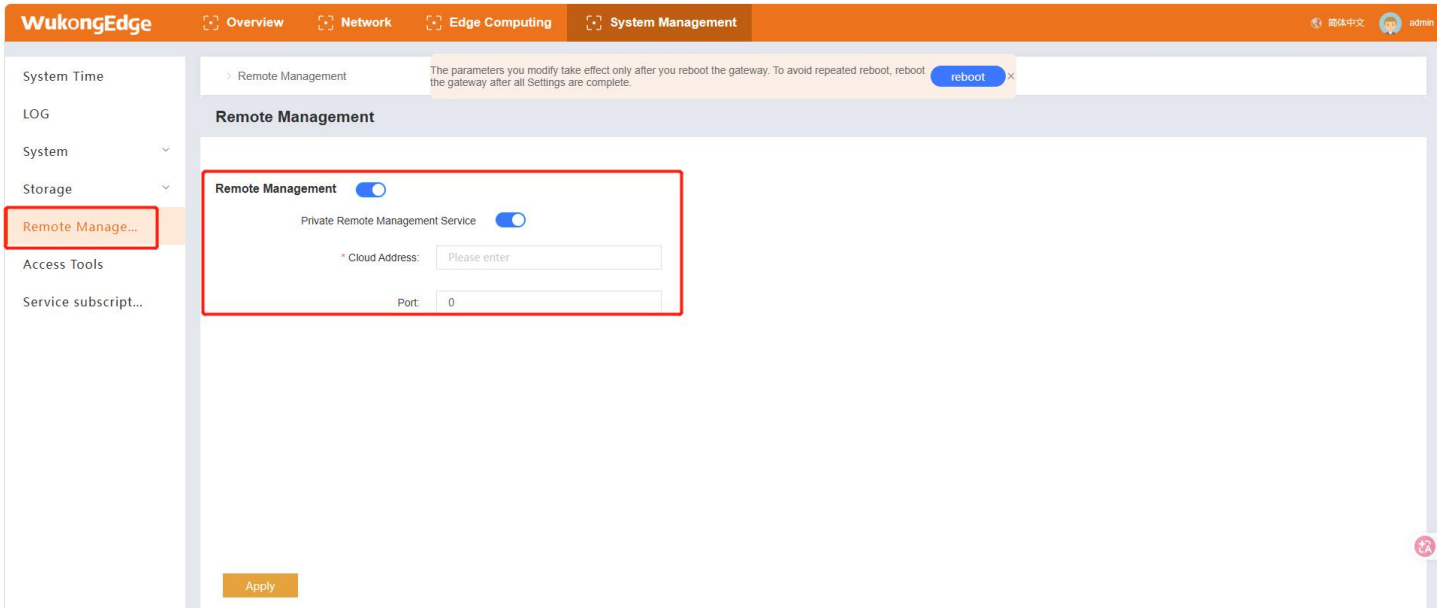
9. After the device restarts, wait for the device to connect to the server, and normal protocol communication will be achieved.

9. Remote Cloud Service

LG270canachieve remote management and maintenance of devices through thePUSR Cloudplatform,performingoperations such as remote device supervision, firmware upgrades, and remote

built-in web page management.

Remote management viaPUSR Cloudis enabled by default. If it is a private deployment, you need to configure the IP address and port of the corresponding private deployment platform; otherwise, the connection to the remote management platform will fail. Devices that require remote management only need to be added to thePUSR Cloudplatform to be operable.



PUSR Cloud, as our company's proprietary IoT platform, is more suitable for product usage.PUSR Cloudprovides enterprises with one-stop software and hardware solutions, empowering many niche industries. It offers core functions such as secure and reliable device access, application development, SCADA services, operation and maintenance management, data statistics and analysis, fully opening platform capabilities. With modular, component-based, and systematic capabilities, it helps enterprises build their own IoT systems at low cost and high efficiency.

9.1.DataConfiguration

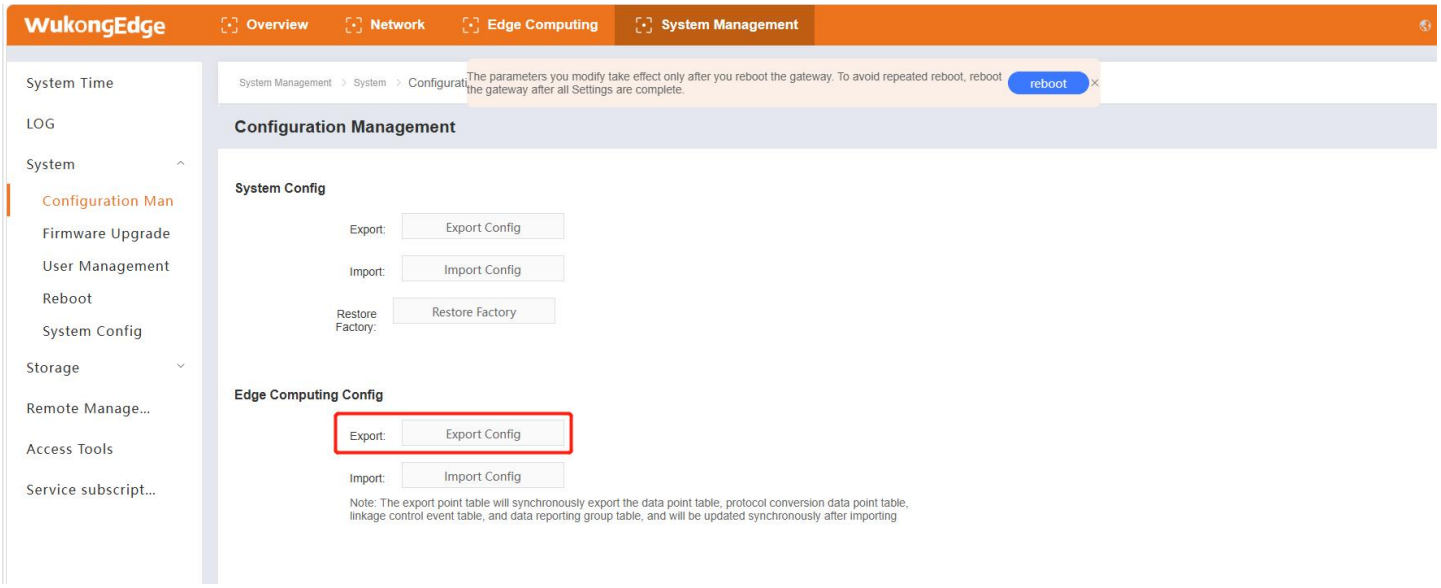
PUSR Cloudcan not only serve as a remote management platform but also manage and display data, as well as implement SCADA functions. However, these functions require the use of thePUSR CloudIoTsubmodule. This requires adding device data templates in the cloud while adding devices, to better facilitate data display and SCADA calls.

PUSR CloudandLG270integration will differ from other products, so detailed instructions on usage will be

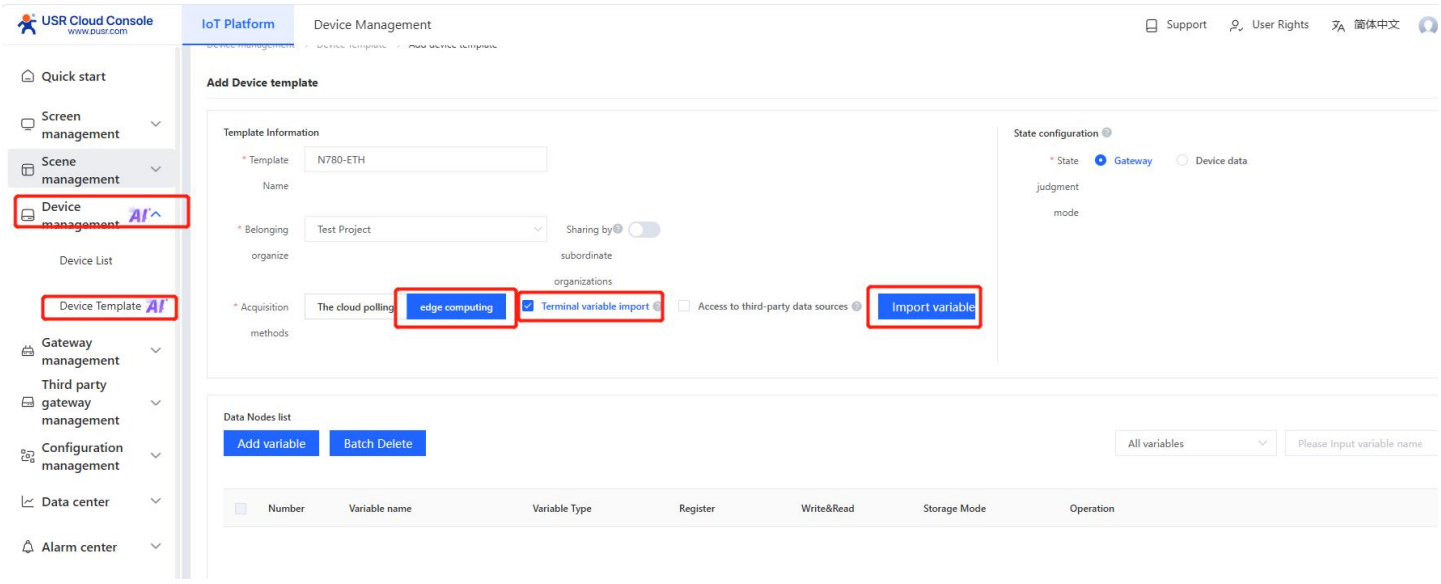
provided:

1） First,LG270needs to enablePUSR Cloudand restart for it to take effect (enabled by default for device supervision).

2） Configure the data point table, export the configured point table, select "To Cloud", and obtain the corresponding .ued file.

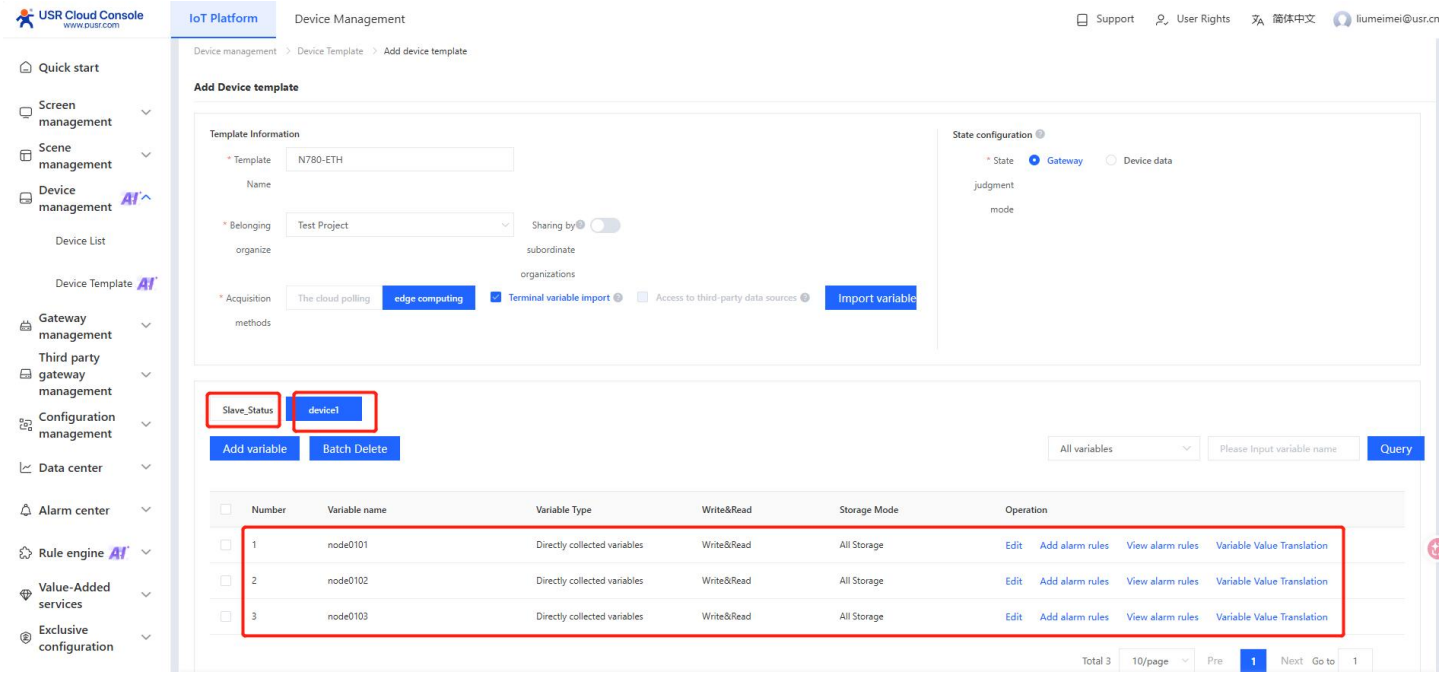


3） Log in to thePUSR Cloudaccount, add a new template in Device Management -> Device Templates, select Edge Computing as the collection method and check Terminal Variable Import, then import the edge computing configuration file exported fromLG270. The cloud will automatically generate the corresponding variable template based on the imported file.



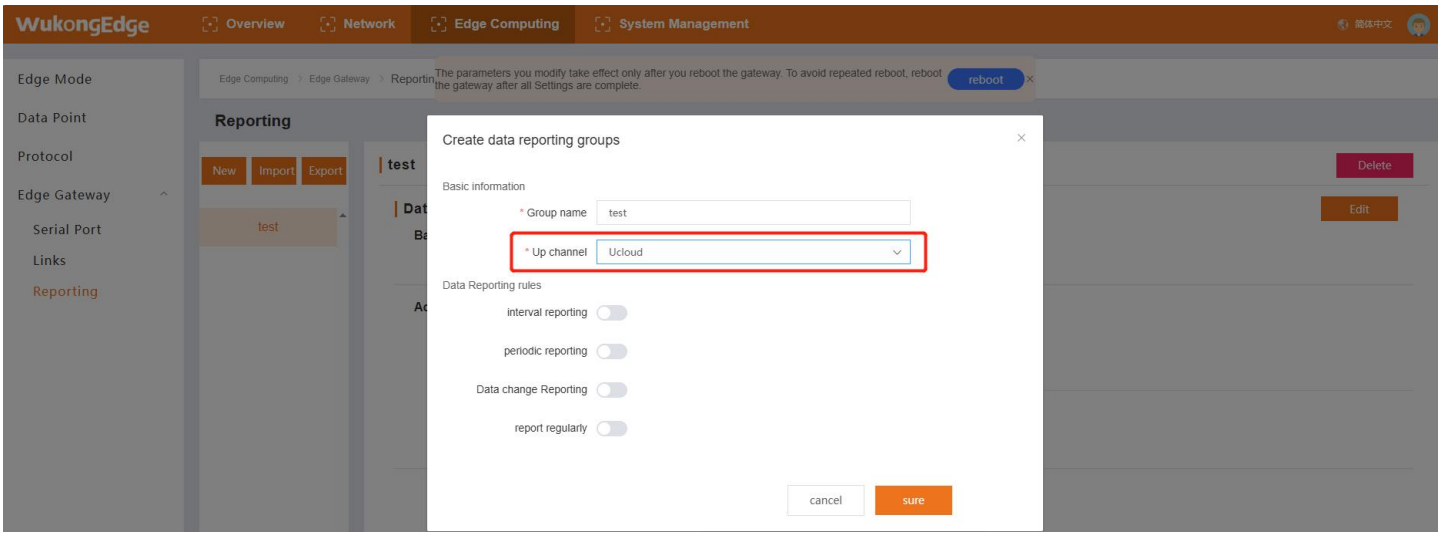
4） Users can add additional features they want in the generated template, such as calculation formulas, and can also add 联动 alarm functions in the cloud based on the collected data.

5） After the template is added, you can proceed to add devices and associate the template with the devices.



6） Ensure that each added device has the same configuration as the edge computing file uploaded with the current template. If they are different, you need to export the file from the device, create a new template, and then associate the product with the template..

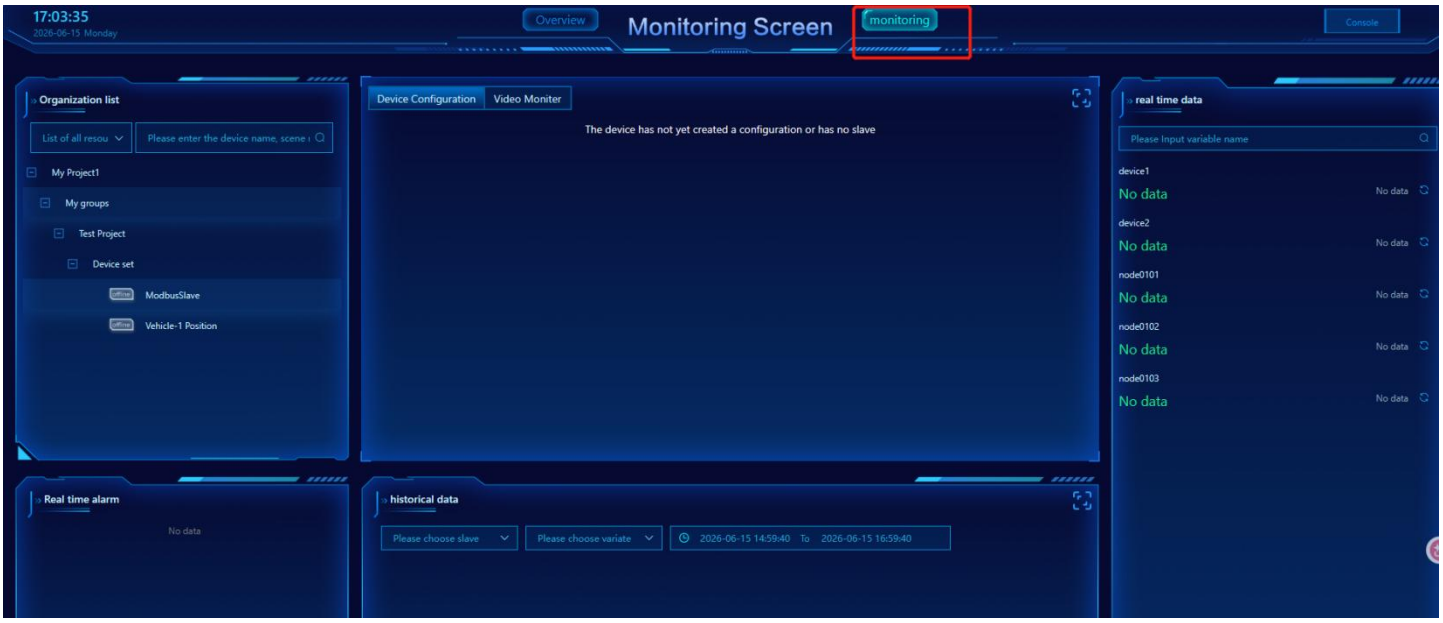
Note: To use PUSR Cloud to receive data, you also need to create a group in "Edge Gateway" -> "Data Reporting" and select PUSR Cloud for reporting.



9.2.Data Monitoring

You can view device details through Monitoring Dashboard > Device Monitoring. This page displays: real-time data, historical data, SCADA screens, alarm information, etc.

Note: The monitoring dashboard can only display device template SCADA, not independent SCADA.



Click on Monitoring Dashboard in the left navigation bar. The monitoring dashboard can display the distribution of devices under the account on the map, as well as device overview, alarm information, etc.



9.3.Device Operation and Maintenance

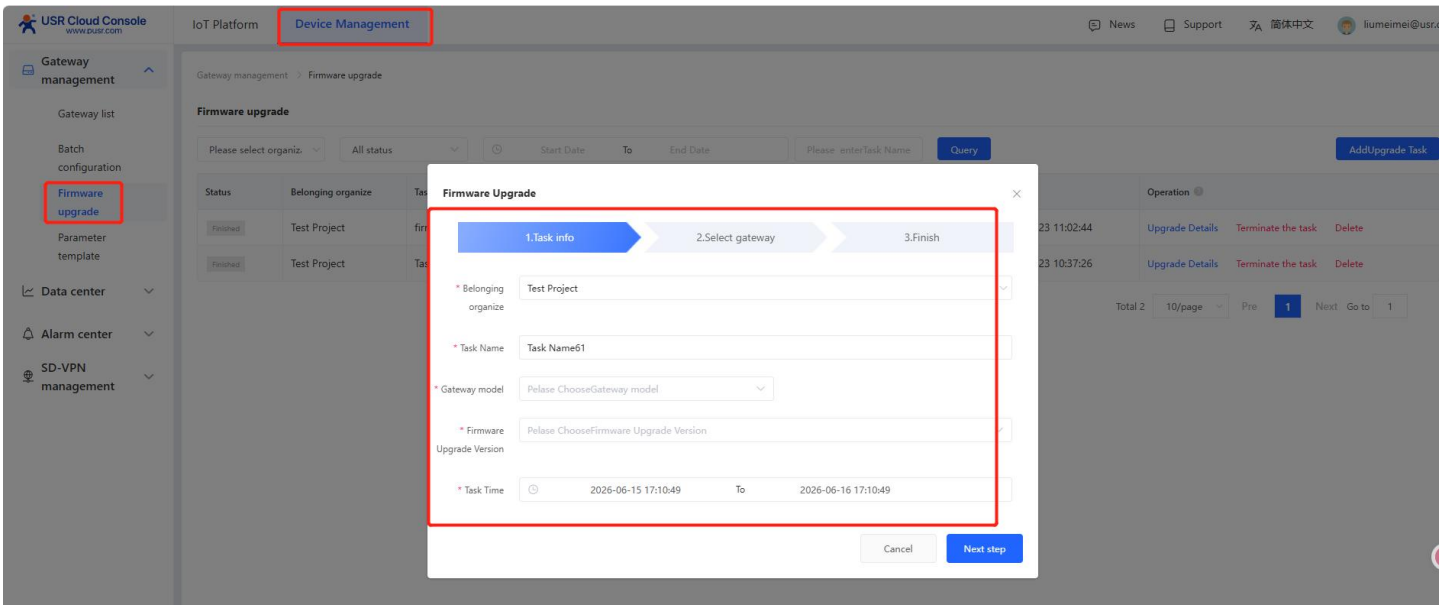
1） Device Status

Device Status	Description
Online	The device is powered, connected to the network, and successfully connected to the cloud.
Offline	The device failed to connect to the cloud. This may be due to lack of power, no network connection, or incorrect IP address/port configuration.
Upgrading	PUSR CloudIoT firmware upgrade function. This status is displayed when the device is undergoing a firmware upgrade.
Template Trigger Alarm	This status is displayed when the monitored device variable data exceeds the threshold. For example, in temperature and humidity collection, an alarm is triggered when the temperature or humidity exceeds the specified alarm threshold.
Model Trigger Alarm	This status is displayed when the device variable data under the monitored product/scene exceeds the threshold. For example, in temperature and humidity collection, an alarm is triggered when the temperature or humidity exceeds the specified alarm threshold.
Device Monitoring Trigger Alarm	This status is displayed when a communication device malfunction occurs. For example, if the communication device's data usage exceeds the set warning value, an alarm will be triggered, displaying this status.

Error	Failed to synchronize the edge computing template with the device. The selected variable template or device does not support the selected edge computing variable template.

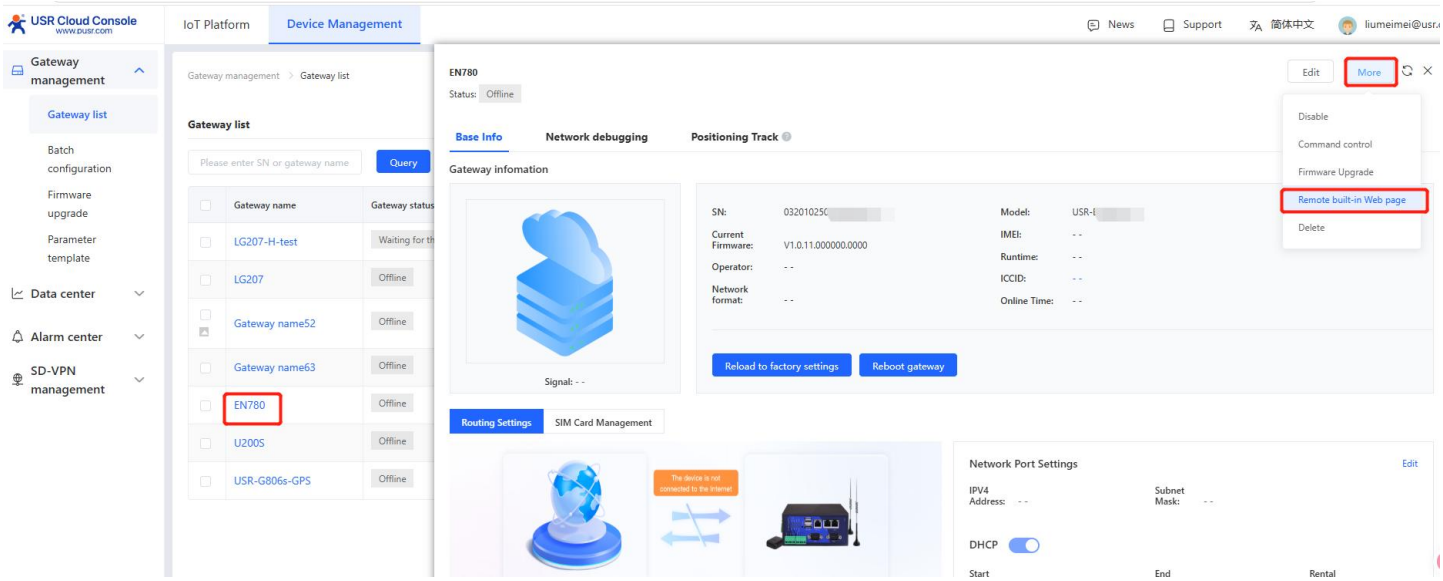
2） Firmware Upgrade

Firmware design allows upgrading the firmware version of networked devices, supporting batch operations. You can create a firmware upgrade task, preset the execution time, and the firmware upgrade for networked devices will be completed on schedule at the specified time.



3） Remote Configuration

PUSR CloudsupportsLG270built-in web page mapping. You can find the corresponding device in theDM-PUSR Cloudgateway management interface, enter its built-in web page, and configure parameters to achieve remote management.



10.Disclaimer

This document provides information about theUSR-LG270product. This document does not grant any license to intellectual property rights, either expressly, by implication, by estoppel, or otherwise. Except for the liabilities stated in the sales terms and conditions of its products, our company assumes no other liability. Furthermore, our company makes no express or implied warranties regarding the sale or use of this product, including but not limited to warranties of fitness for a particular purpose, merchantability, or non-infringement of any patent, copyright, or other intellectual property rights. We reserve the right to modify product specifications and descriptions at any time without prior notice.

11.Update History

File Version	Update Content	Update Time
V1.0	Initial Release	2026-06-03

可信赖的智慧工业物联网伙伴

Official Website: www.pusr.com

Official Shop: shop.usriot.com

Technical Support: h.usriot.com

Inquiry Email: inquiry@usriot.com

Skype & WhatsApp: +86 13405313834

Click to view more: Product Catalog & Facebook & Youtube

Follow USR IOT Wechat Official Account

Log in to the mall for quick ordering