

F8926-GW-02 Series LoRaWAN

Indoor Gateway

User Manual

V 1.0.2



Note: There may be differences in accessories and interfaces for different models. Please refer to the actual product for details.

User Manual for F8926-GW-02 Series LoRaWAN Indoor Gateway	Document Version	Security Classification
	V1. 0. 2	
	Droduct Name: E8026-CW-02	Total of 84
	FIGUUEL Mame, F8920-GW-02	pages

This manual is applicable to the following model products:

Model	Product Category
F8926-GW-02433-XXX	LoRa+LTE WIFI Router
F8926-GW-02470-XXX	LoRa+LTE WIFI Router
F8926-GW-02868-XXX	LoRa+LTE WIFI Router
F8926-GW-02915-XXX	LoRa+LTE WIFI Router
F8926-GW-02433-MZZ	LoRa+WIFI Router
F8926-GW-02470-MZZ	LoRa+ WIFI Router
F8926-GW-02868-MZZ	LoRa+ WIFI Router
F8926-GW-02915-MZZ	LoRa+ WIFI Router
Note: XXX represents the 4G module code, MZZ does not include	
cellular module.	



Customer Hotline: 400-8838 -199 Telephone: +86-592-6300320 Fax: +86-592-5912735 Web: <u>www.four-faith.com</u> Address: 11th Floor, Building A06, Phase

III, Xiamen Jimei Software Park



Document Revision History

Date	Version	Specification	Author
2022-08-29	V1.0.0	Initial Version	SGK/HGL/YSL/WSC
2022-11-01	V1.0.1	Change the communication field "devEui" to "devEui"	SGK
2023-08-15	V1.0.2	English Version Update	YYL





Copyright Statement

All materials or content contained in this document are protected by copyright law. All copyrights are owned by Xiamen Four-Faith Communication Technology Co., Ltd., except for content explicitly referenced from other sources. Without written permission from Four-Faith, no one may copy, distribute, reproduce, link, transmit, or otherwise use any content from this document for any commercial purposes. However, downloading or printing for non-commercial, personal use is permitted (provided that the material is not modified and the copyright notice or other ownership notices are retained).

Trademark Statement



Four-Faith、四信、^{Four-Faith}、Four-Faith **山山** 、 **A** All are registered trademarks of Xiamen Four-Faith Communication Technology Co., Ltd. Without prior written permission, no one is allowed to use the name "Four-Faith" and the trademarks or symbols of Four-Faith in any way.

Contents

Chapter 1 Product Introduction	.7
1.1 Product Overview	.7
1.2 Product Features	.7
1.3 Block Diagram of Operation	. 9
1.4 Product Specifications	. 9
Chapter 2 Installation	14
2.1 Overview	14
2.2 Packing List	14
2.3 Installation and Cable Connection	14
2.4 Power Instructions	17
2.5 Indicator Lights Explanation:	18
2.6 Reset Button Instructions	18
Chapter 3 Quick Start Guide	19
3.1 Introduction to Solution Architecture	19
3.1.1 Difference Between Embedded and Non-Embedded	19
3.1.2 System Framework	19
3.2 Accessing the Configuration Interface	20
3.2.1 Accessing the Web Management Platform	20
3.2.2 To add a device in the embedded mode	21
Chapter 4 Detailed Introduction to Function Pages	25
4.1 Interface Management Configuration	25
4.1.1 Web Management Platform	25
4.1.2 Directory Details	25
4.1.3 Management Configuration	26
4.1.3.1 Status	26
4.1.3.2 LoRa Gateway	31
4.1.3.3 LoRa Network Server	37
4.1.3.4 System	49
4.1.4 Data Format	51
4.1.4.1 Data Explanation	51
4.1.4.2 MQTT Data Format	52
4.1.4.3 TCP Data Format	57
4.1.4.4 HTTP Push Data Format	65
4.1.4.5 JavaScript Function Transformation Method	65
4.1.5 Common Platform Integration	66
4.1.5.1 Four-Faith Cloud NS	66
4.1.5.2 ChirpStack Platform (GWMP)	67
4.1.5.3 ChirpStack Platform (LNS)	68
4.1.5.4 AWS Platform (LNS)	70
4.1.5.5 AWS Platform(CPUS)	72
4.1.5.6 TTN Platform(GWMP)	75
4.1.5.7 TTN Platform(LNS)	77
	5



4.1.6 Common Issues	
4.1.6.1 Gateway Status	80
4.1.6.2 Communication Device	
4.1.6.3 Device Joining Abnormality	81
4.1.6.4 Customer Platform Integration	82



Chapter 1 Product Introduction

1.1 Product Overview

The F8926-GW-02 series gateway is a wireless communication gateway based on the LoRaWAN standard protocol. It connects to various types of standard LoRaWAN protocol application nodes, collects information, and transmits it to the cloud server through wired Ethernet/4G/WIFI methods. This product utilizes a high-performance industrial-grade 32-bit communication processor, supported by an embedded real-time operating system as its software platform. It provides 1 Ethernet WAN (POE) port, 1 LAN port, and 1 WIFI interface, supporting WIFI wireless configuration management and online upgrades, with DC and POE+ power inputs.

The F8926-GW-02 gateway complies with the standard LoRaWAN protocol and supports multiple modes, including the embedded Network Server mode (Network Server deployed within the gateway), Basicstation mode (connecting to an external server corresponding to the Basicstation protocol), and Semtech UDP GWMP Protocol mode (connecting to an external NS server via GWMP UDP protocol).

This product has been widely applied in the IoT industry chain, including sectors such as M2M, smart meters, disaster monitoring, smart sensing, smart photovoltaics, smart grids, intelligent transportation, industrial automation, smart buildings, fire protection, public safety, environmental protection, meteorology, digital healthcare, remote sensing surveying, military, space exploration, agriculture, forestry, water management, coal mining, petrochemicals, and more.

1.2 Product Features

Industrial-Grade Application Design

- Utilizes High-Performance Industrial-Grade LoRa Module (SX1302)
- Utilizes High-Performance Industrial-Grade Wireless Module
- Utilizes High-Performance Industrial-Grade 32-bit Communication Processor
- Adopts a metal aluminum casing with an IP30 protection rating, metal casing, and system security isolation, making it particularly suitable for industrial field applications.
- Wide power supply input (DC9~36V), standard: 12V/1.5A
- Supports POE+ (802.3af/at) input

Stable and Reliable

- WDT Watchdog Design, Ensuring System Stability
- Utilizes a Comprehensive Anti-Drop Mechanism to Ensure Data Terminals Stay Online Permanently
- Ethernet Interface with Built-in 1.5KV Electromagnetic Isolation Protection
- SIM/UIM Card Interface with Built-in 15KV ESD Protection
- Power Interface with Built-in Reverse Polarity Protection and Overvoltage Protection



Antenna Interface Lightning Protection (optional)

Standard and User-Friendly

- Provides Standard TYPE-C, 4G, Ethernet, and WiFi Interfaces, Allowing Direct Connection to Serial Devices, Ethernet Devices, and WiFi Devices
- Provides Standard Wired WAN Port (Supports Standard PPPOE Protocol), Allowing Direct Connection to ADSL Devices
- Smart Data Terminal, Enters Data Transmission State Upon Power On
- Provides Powerful Central Management Software for Convenient Device Management (optional)
- Easy to Use, Flexible, Multiple Working Mode Options
- Convenient System Configuration and Maintenance Interfaces (Including Local and Remote WEB and CLI Methods)

Powerful Functionality

- Provides Wired Ethernet, 4G, WiFi, and Other Data Connection Methods
- LoRaWAN Protocol Versions: 1.0.2 and 1.0.3
- ◆ LoRaWAN Protocol: ClassA、ClassC
- WIFI supports 802.11b/g/n
- WiFi supports various encryption methods such as WEP, WPA, WPA2, as well as features like MAC address filtering.
- Supports Semtech UDP GWMP Protocol mode
- Supports embedded Network Server mode, reducing operation and maintenance costs as well as NS deployment costs, for simple and user-friendly management.
- Supports Basicstation mode, with various data encryption methods to ensure data transmission security.
- Supports Platform Connection: LinkWAN, ChirpStack, Tencent Cloud, TTN (The Things Network), AWS, etc.
- Provides HTTP Push, MQTT Subscribe and Publish, and TCP Connection Methods to the Outside
- Supports configuration of MQTT topics for interfacing with the client, and allows data content to be transformed using embedded JavaScript functions.
- Supports multiple WAN connection methods, including static IP, DHCP, L2TP, PPTP, PPPOE, 2.5G/3G/4G.
- Supports intelligent dual-link switching and backup function for wireless cellular and wired WAN (optional).
- Supports VPN client (PPTP, L2TP, OPENVPN, IPSEC, and GRE) (Note: Supported only in the VPN version)
- Supports VPN server (PPTP, L2TP, OPENVPN, IPSEC, and GRE) (Note: Supported only in the VPN version)
- Supports remote management, SYSLOG, SNMP, Telnet, SSHD, HTTPS, and other functions.
- Supports local and remote online upgrades, as well as importing and exporting configuration files.
- Supports NTP and has a built-in RTC.





- Supports various domestic and international DDNS
- Supports MAC address cloning and PPPOE server functionality.
- WiFi supports 802.11b/g/n, and offers various working modes including WiFi AP, AP Client, Repeater, Bridge, and WDS (Wireless Distribution System) (optional)
- WiFi supports various encryption methods including WEP, WPA, WPA2, and offers features like RADIUS authentication and MAC address filtering.
- Supports various online and offline trigger modes, including SMS, ringing, serial data, and network data-triggered online/offline modes.
- Supports APN/VPDN
- Supports multiple DHCP servers and DHCP clients, DHCP binding with MAC addresses, DDNS, firewall, NAT, DMZ host, QoS, traffic statistics, real-time display of data transmission rate, and other functions.
- Supports multiple network protocols including TCP/IP, UDP, FTP (optional), HTTP, and more.
- Supports SPI firewall, VPN passthrough, access control, URL filtering, and other functions.

1.3 Block Diagram of Operation

The block diagram of the router's operation is as follows:



1.4 Product Specifications

Wireless Parameters



Items	Contents		
F8926-GW-02>	F8926-GW-02XXX LoRa+LTE WIFI Router		
Standards			
and	Supports Full Network: LTE FDD、LTE TDD、EVDO、WCDMA、TD-SCDMA、		
Frequency	CDMA1X、GPRS/EDGE		
Bands			
Theoretical Bandwidth	LTE FDD: Downlink Speed 100Mbps, Uplink Speed 50Mbps		
	LTE TDD: Downlink Speed 61Mbps, Uplink Speed 18Mbps		
	DC-HSPA+: Downlink Speed 42Mpbs, Uplink Speed 5.76 Mbps		
	TD-HSPA+: Downlink Speed 4.2Mbps, Uplink Speed 2.2Mbps		
	EVDO Rev. A: Downlink Speed 3.1Mbps, Uplink Speed 1.8Mbps		
Receiver	< 07dPm		
Sensitivity	<-9/dbm		

WIFI Wireless Parameters

Items	Contents
Standards and	
Frequency	Support IEEE802.11b/g/n Standard
Bands	
Theoretical	IEEE802.11b/g: Maximum Speed of 54Mbps
Bandwidth	IEEE802.11n: Maximum Speed of 150Mbps
Security	Supports various encryption methods including WEP, WPA, WPA2, and
Encryption	optional WPS functionality.
Transmit Power	20dBm (11n), 24dBm (11g), 26dBm (11b)
Receiver	< 70dDm@54Maba
Sensitivity	

LoRa Parameters



Items	Contents	
Operational Channels	Uses a simple star topology network and supports blind repeaters.	
LoRaWAN Protocol	ClassA、ClassC	
Urban		
Communication	9km	
Reference Distance		
Reference Distance	16 Eloors@SE12	
for Floor Penetration		
Operating Frequency	EU433、CN470-510、CN779-787、EU863-870、US902-928、AU915-928、 AS923、 KR920-923	
Maximum Transmit Power	26±1dBm	
Maximum Antenna	-140dbm @l oRa	
Receive Sensitivity		
Communication Bandwidth	125kHz、250kHz、500kHz	
Communication	8 Uplink Channels, 1 Downlink Channel	
Channel		
Communication Rate	Adaptive Link Rate	
Communication Mode	Half-Duplex	
Operating Mode	Supports Transceiving on Different Frequencies and Transceiving on	
	the Same Frequency	
Reporting Server	4G Wire Ethernet	
Mode		
Wireless	WiFi Wireless Management and Upgrades	
Management		

Hardware System

Items	Contents
CPU	Industrial-Grade 32-bit Communication Processor
FLASH	32MB (Expandable up to 64MB)
DDR2	128MB

Interface Type

Items	Contents
Power Interface	Standard 3-pin power socket, with built-in reverse polarity protection and
	overvoltage protection.
WAN (POE)	WAN/LAN configurable, with 1 10/100M Ethernet port (RJ45 socket),
	adaptive MDI/MDIX, and built-in 1.5KV electromagnetic isolation protection.
LAN	1 10/100M Ethernet port (RJ45 socket), adaptive MDI/MDIX, and built-in
	1.5KV electromagnetic isolation protection.



Console	Type-C USB
Reset Button	By pressing this button, you can restore the parameter configuration of the
	ROUTER to its factory settings.
TF Card	8GB/32GB, Customizable Support
SIM Card	Supports SIM Cards from the Three Major Carriers (3FF Cards)
Antenna	LoRa、WIFI、4G,3 Antenna Interfaces
Indicator Lights	"PWR", "SYS", "WiFi","LoRa ","4G" 5 Indicator Lights



Note: There may be differences in accessories and interfaces for different models. Please refer to the actual product.

Power Supply

Items	Contents
	DC 12V/1.5A (Recommended), supports power supply voltage range
Power Supply	DC 9~36V
	POE+ (802.3af/at) Power Consumption 25W max

Power Consumption

Operational Status	Power Consumption
Standby	Average Current≤120mA@12V
	Transmit Current≪460mA@12V(with 4G)
Communication	Transmit Current≤143mA@12V(without 4G)
	Receive Current≤120mA@12V

Physical Characteristics

Items	Contents
Casing	Aluminum Casing, IP30 Protection Level
Dimensions	160X105X24 mm (Excluding Antenna and Mounting Accessories)
Weight	450g(Excluding Accessories)

Other Parameters

Items	Contents
Operating	-35~+75°C (-31~+167°F)



Temperature	
Storage	10~+95%C (10~+195°E)
Temperature	-40 [°] + 85 [°] C [°] + 185 [°] F [°]
Relative	0.5% (no condensation)
Humidity	



Chapter 2 Installation

2.1 Overview

The router must be installed correctly in order to achieve its designed functionality. Usually, the installation of the equipment must be carried out under the guidance of authorized and qualified engineers from our company.

> Precautions:

Please do not install the router while it is powered on.

2.2 Packing List

Please keep the packaging materials when you unpack the box, so that they can be used for operating if needed in the future. The list is as follows:

- ♦ 1 Router Host
- ♦ 1 Wireless Cellular Stick Antenna (SMA Male Connector)
- ♦ 1 WiFi Stick Antenna (SMA Female Connector)
- ♦ 1 LoRa Stick Antenna (SMA Male Connector)
- ♦ 1 Power Adapter
- ♦ 1 Ethernet Cable

Note: LoRa suction cup antenna is optional.

2.3 Installation and Cable Connection

Physical Dimensions:

The physical dimensions are shown in the following diagram. (Unit: mm) The specifications for the mounting bracket and router device screws are: M3*5mm countersunk screws.



Bracket Dimensions









Wall Mount Bracket Dimensions











Router Dimensions

Note: When using the mounting bracket to install the router, use M3 screws with a depth of 3-4mm screwed into the router. The mounting bracket and wall mount bracket are optional accessories.

Antenna Installation:

Wireless Wide Area Network (WWAN) antenna interface is an SMA female socket (labeled as "4G"). Screw the provided wireless cellular stick antenna with an SMA male connector into this antenna interface and ensure it is tightened securely to maintain signal quality.

The Wireless Local Area Network (WLAN) antenna interface is an SMA female socket (labeled as "WIFI"). Screw the provided WIFI stick antenna with an SMA male connector into this antenna interface and ensure it is tightened securely to maintain signal quality.

The Long-Range (LoRa) antenna interface is an SMA female socket (labeled as "LoRa"). Screw the provided LoRa stick antenna with an SMA male connector into this antenna interface and ensure it is tightened securely to maintain signal quality.

Note: The wireless cellular 4G antenna, WiFi antenna, and LoRa antenna must not be connected in reverse, otherwise the device will not function properly.

SIM/UIM Card Installation:

When installing the SIM/UIM card, please pay attention to the card's orientation. The golden contacts should face downward, and the cut corner should be positioned at the top-left corner. Gently push the card into the slot until you feel a slight resistance, indicating that the card is secured. To remove the card, simply press the "PUSH" area to release it.





Note: Align the card's cut corner with the printed cut corner, and ensure that the golden contacts are facing downward.

Connect Ethernet Cable:

Insert one end of the Ethernet cable into the LAN port of the Router, and the other end into the Ethernet interface of the user's device. The Ethernet cable connection should be as follows:

RJ45-1	RJ45-2	Wire Color
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown

Connect Console Wire (TYPE-C) :

Simply use a standard Type-C cable, connect one end to the Router device and the other end to a PC, then install the corresponding drivers.

Driver download address: <u>https://www.wch.cn/search?t=all&q=CH340C</u> Installation package:



2.4 Power Instructions

Routers are commonly used in complex external environments. In order to adapt to



these challenging application scenarios and enhance the system's operational stability, advanced power supply technology is employed in the Router. Users can power the Router using the standard configuration of a 12VDC/1.5A power adapter or directly supply it with DC power in the range of 9-36V. When using an external power supply for the Router, it is essential to ensure the stability of the power source (with ripple less than 300mV) and guarantee that momentary voltage doesn't exceed 36V. Additionally, the power supply should provide a power output greater than 8W.

It is recommended to use the standard configuration of a 12VDC/1.5A power adapter or POE+ (802.3af/at) input.

2.5 Indicator Lights Explanation:

Indicator Lights	Status	Specification
Power	ON	Device power normal
	OFF	The device is not powered on / in the shutdown period of
	OFF	the scheduled power on/off function.
SYS	Blinking	The system is running normally.
	OFF	The system is not functioning properly.
WIFI	OFF	The WiFi is not active.
	ON	The WiFi is active.
LoPo	ON	LoRa has been detected.
LURA	OFF	LoRa not detected.
4G	ON	Device has logged into the network.
	OFF	The device is not logged into the network.

The Router provides the following indicator lights: "PWR", "SYS", "WiFi", "LoRa", and "4G". The status explanations for each indicator light are as follows:

2.6 Reset Button Instructions

The router is equipped with a reset button labeled "Reset." The function of this button is to restore the router's settings to the factory defaults. The procedure is as follows: Insert a pointed object into the "Reset" hole and gently hold down the reset button for about 15 seconds, then release it. At this point, the router will automatically restore the parameter settings to the factory defaults. After approximately 5 seconds, the router will automatically restart (the automatic restart phenomenon is as follows: the "SYS" indicator light will go off for about 10 seconds and then resume normal operation).



Chapter 3 Quick Start Guide

3.1 Introduction to Solution Architecture

3.1.1 Difference Between Embedded and Non-Embedded



As shown in the diagram above, the main difference between the embedded and non-embedded solutions lies in the position of the Network Server (NS). In the non-embedded solution, the NS is typically deployed on a separate server, while in the embedded solution, the NS is deployed within the gateway itself.

✤ The advantage of the embedded solution (embedded mode) is that there is no need to deploy the Network Server (NS) on an external server, which reduces operational costs and allows for a quick and convenient setup of the entire LoRaWAN system. However, the drawback is that the performance and storage capacity of the gateway system are relatively lower compared to a dedicated server. This limitation affects the number of nodes that can be supported and the ability to cache large amounts of information.

The advantage of the non-embedded solution (external mode) is that servers have stronger performance and larger storage capacity, enabling them to manage a large number of gateways and nodes. This solution can be deployed through clustering to significantly enhance system performance and availability. However, the drawback is the need for additional server deployment to host the Network Server (NS), which requires maintenance and increases project costs. Setting up the system and troubleshooting may also require more time and effort.

3.1.2 System Framework







The gateway communicates with devices or terminals, and the direction of data flow is determined based on web configuration.

✤ In the Basics Station (BasicStation mode), data will be exchanged bidirectionally with the corresponding connected server. The gateway only functions as a data forwarding unit. In this scenario, device management, data encryption/decryption, and integration with customer platforms are all performed on the server side.

In the Semtech UDP GWMP Protocol (external NS mode), data will be communicated with the external Network Server (NS) using the standard UDP protocol. In this scenario, device management, data encryption/decryption, and integration with customer platforms will be handled within the external NS server. For instance, commonly used external NS servers include those provided by Four-Faith Cloud.

In the Built-in LoRa Server (internal NS mode), data will be routed to the NS server that is integrated within the gateway. In this scenario, device management, data encryption/decryption, and integration with customer platforms will be handled within the built-in NS server, also known as the LoRa Network Server. Clients can achieve data push functionality through configuration of an HTTP server (HTTP POST only supports uplink push and doesn't support downlink data), or through MQTT and TCP methods for both uplink and downlink data. The embedded NS serves as the core network for LoRaWAN. This product theoretically supports a large number of gateways and device connections. It manages tasks such as device provisioning, data encryption/decryption, uplink and downlink data transmission, and data pushing. Uplink data from devices, after being decrypted by LoRaWAN, establishes a connection with the customer platform via an interface. Customers can use MQTT for data publishing or TCP for downlink data, which is encrypted by LoRaWAN and sent to the specified device.

3.2 Accessing the Configuration Interface

3.2.1 Accessing the Web Management Platform

1) Method 1: After powering on the gateway, the default WiFi SSID is "Four-Faith," and the default password is blank. Once successfully connected to the WiFi, the LAN IP address of the gateway is 192.168.1.1. You can then access the web management platform by



entering http://192.168.1.1 (or simply 192.168.1.1) into your browser's address bar.

2) Method 2: If you already know the WAN address of the gateway (e.g., set to static IP 192.168.1.88), you can directly access the web management platform by visiting http://192.168.1.88 in your web browser.

3) Login using the default credentials: Username: admin, Password: admin. Click "Login" to access the Web management platform.

Note: Please use Google Chrome browser as other browsers might have compatibility issues.

3.2.2 To add a device in the embedded mode

- 1. Identify the frequency band and corresponding frequencies for your device (e.g., a standard EU868 terminal, frequencies: 868.1MHz, 868.3MHz, 868.5MHz)
- 2. **Confirm if the embedded mode is enabled** (default is embedded mode). If not, change it to embedded mode.

Path: LoRa Gateway → Basic Settings

Ģ	Status ^	Dashboard / LoRa Gateway / LoRa Gateway
	Overview	曽页 × Overview × ● LoRa Gateway ×
	LoRa Packet Logger	Basic Frequency Band Set Packet Filter
	System Log	* Gateway MAC 54D084FFFE9B006C
	Network ~	Protocol Build-In LoRa Server
		Keepalive Interval (s) 10
	LoRa Network Server	Internal UDP Port 1699
	System ~	Save & Modify

3. Check if the gateway's frequency band and frequency points match (default frequency points are determined by regional parameters). If they don't match, modify them to match. Path: LoRa Gateway → Frequency Band Configuration

Status ^	E Dashboard / LoRa Gateway / LoRa Gateway
Overview	首页 × Overview × ● Lota Gateway × Application × Application Detail × LoRa Packet Logger ×
LoRa Packet Logger	Basic Frequency Band Set Packet Filter
System Log	Working Area (Frequency Band MHz) EU955 V RF beard type does not match frequency band (RF board type
🕄 Network 🗸 🗸	Is Customize preset group Custom frequency
🕅 LoRa Gateway	Conform to LoRaWAN The page switching data will not be synchronized, and it will take effect after clicking Save & Modify on the corresponding page.
LoRa Network Server	LoRaWAN Public
☺ System	Multi-SF LoRa Channel (MHz) 867.1 × 867.3 × 867.5 × 867.7 × 867.9 × 868.1 × 868.3 × 868.5 ×
	Save & Modify

Add an application (configure it as automatic device addition mode for network).
 Path: LoRa Network Server => Applications => Add Application

		M	C		C	L D WAN	1.1		
Four-Faith	User	Manua I	TOT F89	20-GW-02	Serles	LORAWAN	Indoor	Gateway	
🖵 Status 🔷	E Dashboard /	LoRa Network	Server / Applicatio	n					
Overview	首页 × Overview	× LoRa Gate	way × • Applicati	× nc					
LoRa Packet Logger	+ New application		New application	n				>	<
System Log	1D	Name							
⊠ Network ~		patest	* Name						
🖗 LoRa Gateway			* AppKEY	16 bytes, or 32	d LaDoWAN Dr	wise will be added	automatically of	default	
I aPa Natwork Server			Auto Add Dev	Application Key	pass verification	n.	automatically a	ter Application Eor and	
Chatra Containe			Description						
Basic							⊙ C:	ancel O Confirm	

In the above figure, both AppKEY and AppEUI are generated by clicking on the "default" on the right side (these values are default values provided by Four-Faith; for non-Four-Faith devices, please modify them accordingly). Choose either ClassA or ClassC based on the device type, then click "Confirm" to proceed with the addition. After adding, the following page will appear:

+ New app	plication					
ID	Name	Device Number	CreateAt	Auto Add Dev	Description	Operate
2	pdtest	1	2022-05-18 13:56:31	true	pulse test	View Delete

5. Device Onboarding

Device Initiation of Network Join Request and Verification of Successful Joining; if Joining Fails, Follow these Troubleshooting Steps:

1) Verify if the gateway can receive the network join request sent by the device (you can use a packet capture tool, path: Status \rightarrow LoRa Packet Logger).

2) If the gateway receives the network join request but does not see the join accept packet (Join Accept), it's usually due to a mismatch between the AppKey or AppEUI configured in the application and the device.

	Time	DataType	Freq.	RSSI	SNR	TxPwr	DataRate	FCnt	DevAddr	FPort	Payload Size	Been Filtered	MAC Command	
>	1970-01-01 05:07:26	Join Accept	868.1	0	D	14	SF12BW125	0		0	17	false		
×	1970-01-01 05:07:26	Join Request	868.1	-75	11	0	SF12BW125	D		D	23	faise	AppEUI: 753890477036668 0 DevEUI: 6E11000000000 000	

6. Upstream Data from Devices

After the device successfully joins the network, instruct the device to send any data. You can then navigate to the corresponding application in the device list to view the data: Path: LoRa Network Server \rightarrow Applications \rightarrow Select the corresponding application (click to view) \rightarrow Find the corresponding device (click to view) \rightarrow Online Debugging

-Faith	User	Manua I	for	F8926-GW-02	Series Lo	oRaWAN	Indoor	Gateway
Application > pdtest > ff20230816165412 (T	EST111)							
Overview Configure Activation	Debug							
Timed conding	10	Up	odate log: 🧲	D				Export
Timed sending	- 10 +	Second	Data ty	pe Receiving time	GatewayID	RSSI	SNR	Data
ED-14			> Uplin	2023-08-16 16:56:31	54d0b4fffe9b006c	-66	7	34 34 34 34 34
FPort - 10 T			> Uplint	2023-08-16 16:56:26	54d0b4fffe9b006c	-65	6.8	33 33 33 33 33 33
Confirm type O UnConfirmed	Confirmed		> Uplini	2023-08-16 16:56:14	54d0b4fffe9b006c	-66	10.3	33 32 31
Data type 🧿 ASCII 🛛 HEX		_						

7. Send Data to Device

Send data to the device on the online debugging page of the device, as shown in the following figure:

Overview	Configure	Activation	Debug	
	Timed s	ending	- 10	+ Second
	FPort -	10 +		
Con	firm type 💿 Un	Confirmed	Confirmed	
C	Data type 💿 AS			
	Data 6666	666		
			-	li

The Four-Faith module receives data as follows:

```
Rec Mac 18:< 60 AD 56 DA 00 AO 08 00 0A B9 7B AC 63 C3 99 30 95 A8 >
MType=3
address=0xda56ad
OnRx2
RxWinCon:Freq=869525000 Dr0=0 SBT=6 DR=0 BW=0 MPL=51
MacSta [->] Flags=0x13 State=0x1 NodeAckReq=1
MacSta [X] Flags=0x13 State=0x0
McpsCon
+ACK
McpsInd
+McpsInd
+McpsInd:UNCON
+RCV:10,12345
```



Precaution:

The device types are divided into ClassA and ClassC, with the following data reception methods:

1. In ClassA mode, after sending data, it won't be directly delivered to the device. The data will be sent to the device only after the device sends an uplink data transmission.

2. In ClassC mode, when sending data, it will be directly delivered to the device. If the device doesn't receive the data, please verify whether the NS configuration type matches the device configuration type. If they don't match, make the necessary changes and rejoin the network before conducting data communication tests.



Chapter 4 Detailed Introduction to Function Pages

4.1 Interface Management Configuration

4.1.1 Web Management Platform

1) Method 1: After the gateway is powered on, the default WiFi name is "Four-Faith" and the default password is blank. Once the WiFi connection is successful, the LAN address of the gateway will be set to 192.168.1.1. You can then log in by visiting http://192.168.1.1 (or simply entering 192.168.1.1) in your web browser.

2) Method 2: If you already know the WAN address of the gateway (for example, if it's set to a static IP like 192.168.1.88), you can directly access it by visiting http://192.168.1.88 in your web browser.

3) Login using the default credentials: Username - admin, Password - admin. Click on "Login" to access the Web Management Platform.

.		
LoRaWAN Gateway	A	
admin	7775	

Note: Please use Google Chrome browser, other browsers may have compatibility issues.

4.1.2 Directory Details

Web: <u>www.four-faith.com</u> Address: Building A06, Phase III, Xiamen Jimei Software Park



Below, we will introduce the functions of each page in the order of the directory:

Status

• Overview: The gateway listens to data statistics and displays system parameter information.

■ LoRa Message Recorder: Display of received data and downstream data on the gateway.

- System Log: Operational logs during runtime.
- Network

■ WAN Interface: Gateway WAN configuration, you can configure network information here, such as setting up DHCP or static IP.

- Wi-Fi: wifi Parameters and Security Configuration
- Network Diagnostics: Includes Ping, Traceroute, and Nslookup commands.
- Firewall: Basic firewall parameter configuration.

• LoRa Gateway: Gateway mode configuration, frequency channel parameter configuration, packet filtering, etc.

- LoRa Network Server
 - Status: Display of embedded NS statistical information.
 - Basic Settings: Configuration of NS-related parameters, such as ADR switch,

RX2 parameter settings, etc.

- Gateway: Display of gateway information.
- Application: Display of application information, including device list and

more.

- Multicast: Multicast management.
- Interfaces: Configuration of protocols for integration with client platforms,

data transformation, heartbeat settings, etc.

- System
 - System: Embedded NS version information, system time settings, etc.
 - Change Password: Modify the password for the Web management platform.
 - Reboot: Restart the gateway button.
 - Factory Reset: Factory reset button.

4.1.3 Management Configuration

4.1.3.1 Status

- 1. Overview
 - > Path: Status -> Overview

> **Function:** Displays communication statistics of the gateway, making it easy to view and analyze the RF environment around the gateway. This helps determine device communication status, identify potential interference, and make assessments regarding device connectivity.

- Details:
 - ♦ Received Packets: The number of packets received since system startup.
 - \diamond Sent Packets: The number of packets sent since system startup.
 - ♦ Active Nodes: The number of uplink nodes received by the gateway.



♦ Busy Nodes: Nodes that have sent uplink data twice within 10 seconds are considered busy nodes. This statistic reflects the count over the past hour.

♦ LoRa Channel Utilization Statistics: Channel utilization status in various time intervals over the past 24 hours.

♦ LoRa Data Rate Utilization Statistics: Data rate utilization status in various time intervals over the past 24 hours.

♦ LoRa Network Server: Includes system startup time, LoRa protocol, device count, NS device uplink count, NS device downlink count, and NS MQTT connection status.

♦ System: Includes host name, LAN MAC address, WAN MAC address, wireless MAC address, WAN IP address, LAN IP address, and WAN protocol.

♦ Wireless: Includes wireless switch, mode, network mode, name, channel, and transmission power.

C Status ^	E Dashboard / Status / Overview	X 🛛 🖻 🗸
Overview	Device × • Overview ×	
LoRa Packet Logger	Receive Count Receive Count Active Node 👽	Busy Node
System Log		1
፼ Network ⊻	LoRa Channel Occupancy Statistics LoRa Rate Occupancy Statistics	
傑 LoRa Gateway	-O- chan0 -O- chan1 -O- chan2 -O- chan3 -O- chan5 -O- chan5 -O- chan7 -O- st7 -O- st8 -O- st9 -O- st10 -O- st11 -O- st	12
LoRa Network Server	25	
Status	2	
Basic	1 15	
Gateway	0.5	
Application	0.5	
Multicast Groups	0 17h 19h 21h 23h 1h 3h 5h 7h 9h 11h 13h 15h 17h 19h 21h 23h 1h 3h 5h 7h 9h	11h 13h 15h
Interface	LoRa Network Server System	
ੰ System ∽	System Startup Time 2023-08-16 16:53:35 Host Name Four-Faith	

Preview:

2. LoRa Message Record

Path: Status -> LoRa Message Recorder

> Function:

■ Display LoRaWAN data received by the gateway and data sent by the gateway.

It can be used to analyze the communication between the gateway and devices, and allows for analysis of issues based on data types, such as unanswered join requests, missing downlink data, communication quality, and more.

> Details:

■ Update Log Switch: It is enabled by default. When disabled, it allows for expanding the view of data. While it's disabled, data is still received normally, and once enabled again, it automatically updates the list.

■ LoRaWAN Data Type Selection: This option is used to facilitate the analysis of communication issues by selecting different LoRaWAN data types.



■ Packet Filter Status: Indicates whether the packet has been filtered. Filtered data will not be reported to the NS server. The filtering configuration can be found in LoRa Gateway → Packet Filter. The options are as follows: All - Displays both filtered and unfiltered data. Unfiltered - Displays only unfiltered data. BeFiltered - Displays only data that has been filtered.

- devAddr: Search by Short Address
- Time: Received Data Time
- DataType: Data Type
 - ♦ ALL
 - ♦ Join Request
 - ♦ Join Accept
 - Unconfirmed Data Up
 - Unconfirmed Data Down
 - Confirmed Data Up
 - Confirmed Data Down
- Freq: Communication Frequency Point
- RSSI: Signal Strength
- SNR: Signal-to-Noise Ratio
- TxPwr: Transmit Power, this value is 0 during uplink
- FCnt: Frame Count, can be used to determine if there are any packet losses or

retransmissions.

> Preview:

	Time												
>	1970-01-01 07:29:35	Unconfirmed Data Down	868.1	-67	1.8	D	SF12BW125	1426	00da56ad	8	12	false	
>	1970-01-01 07:29:33	Unconfirmed Data Down	868.5	D	0	14	SF12BW125	1426	00da56ad	8	12	false	
~	1970-01-01 07:29:33	Confirmed Data Up	868.5	-74	8.3	D	SF12BW125	1387	00da56ad	32	22	false	
a b c c d	ask: 0, Filtered: false, rd: 0, nan: 7, odr: "4/5", sta: "gK1W2gAAawUgI6n8G stab: "gK1W2gA awUgI6n8G	2509X0UYfH9uLQ==",											
d f n r r s s t t t t }	<pre>att: "SF12BH125", 00 cv eq: 508.5, sr: 8.3, dui: "LCRA", fch: 1, ss1: -74, ic: 22, tc: 22, tc: 22, tc: 11, mms: null, mst: null, sst: 1145115140</pre>	(c) 100 00 22 23 09 (c) 34	a c3 00 5e 83	18 7c 7t 6	20,								
d ff l m r r r s s t t t t }	<pre>tr: "SF12BH125", 00 to eq: 508.5, sr: 8.3, dui: "LCRA", fch: 1, ss1: -74, is: call, ss1: -74, is: call, ss1: -74, is: call, ss1: sn11, ss1: sn11, ss</pre>	Unconfirmed Data Up	868.1	-94	4	0	SF128W125	4986	01423761	21	23	false	
d ffl1 mrrrs sttt } >	ttr: "SF120m125", 00 to eq: 000.5, sq: 000.5, sq: 000.7, fch: 1, sg: -null, sg: -null, me: null, me: null, me: 1145115140 1970-01-01 07.28.33 1970-01-01 07.28.29	Unconfirmed Data Up Unconfirmed Data Up	868.1 868.5	-94 -67	4 1.3	D	SF128W125 SF128W125	4986 1425	01423761 00da56ad	21 45	23 12	Tatse Tatse	
<pre>d f f i m r r s s t t t } > > ></pre>	th: 'SriJbm125', 'd 'd 'd ee: 808.5, dd: 'loR*', tig: null, ssi: -74, tig: null, tig: null,	Unconfirmed Data Up Unconfirmed Data Down	868.1 868.1 868.1	-94 -67 0	4 1.3 0	0 0 14	SF128W125 SF128W125 SF128W125	4996 1425 1425	01423761 00da56ad 00da56ad	21 45 45	23 12 12	faise faise faise	

3. LoRa Packet Logger

➢ Path: Status → LoRa Packet Logger

> **Function:** The logs can be used to analyze the overall operation of the gateway, abnormal device communication situations, and other anomalies.

- > Details:
 - \diamond Switch: Enabled by default, when paused, new data is stored in the browser



cache and will be updated when re-enabled.新

> Preview:

🖵 Status 🔷	🗉 Dashboard / Status / System Log
Overview	Device × Overview × • System Log ×
LoRa Packet Logger	Update log:
System Log	time-************************************
t23 Network ∽	Imm=*2223-06-16 1659:15" Invert-INT 0 mag/=series to generative, add = 10.1063.1122-8002, type = 1 directs Imm=*2023-06-16 1659:15" Invert-INT 0 mag/=series to generative, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Invert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-16 1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-1659:16" Intervert-INT 0 msg="senit to gateway, add = 10.1863.1123.24802, type = Publicati Imm=*2023-08-1659:16" Intervert-
'№ LoRa Gateway	time="2023-08-16 16:59:16" level=DEBUG msg="Uplink PhyPayload = 40cbc7e30000030015/28de8c3fe8aa5b3db8, Gatewayld = 54d0b4fffe9b006c, Frequency = 868300000, Rssi = -66, LoraSnr = 9.5" time="2023-08-16 16:59:16" level=INFC msg="send to gateway, add = 10.168:1.123:43403, type = PushCR/"
LoRa Network Server	шпе- zиzэлилги тоцо, то текеникто поу- гол полт увлемау, акил – то, тоо, т, гдунунчо, уре – PUSID818

4.1.3.2 Network

1. Network

➢ Path: Network → WAN Interface

Function: Used to configure network parameters, such as setting up static IP,

DHCP, etc.

- > Details:
 - \diamond Configure various modes based on the mode parameters.
- > Preview:

🖵 Status 🔷	E Dashboard / Network / WAN Interface
Overview	Device × Overview × System Log × • WAN Interface ×
LoRa Packet Logger	Connection Type Automatic Configuration - DHCP \checkmark
System Log	Wan Nat Disable C Enable
⊠ Network ^	STP Disable Enable
WAN Interface	Save & Modify
Wi-Fi	

2. WIFI

- ➢ Path: Network → WiFi
- **Function:** wifi Parameter Configuration, Security Configuration
- ➤ Detail:
 - \diamond Configure various modes based on the mode parameters.
- > Preview:

Pur-Faith	Us	er Manua	al for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
🖵 Status 🔷	Ξ Dash	nboard / Netwo	ork / Wi-Fi					
Overview	Device ×	Overview ×	System Log	× WAN Interface ×	• Wi-Fi ×			
LoRa Packet Logger	Basic	Wireless S	ecurity					
System Log				Wireless	Network Dis	sable 🚺 Ena	ble	
Ø Network ∧				Wirele	ess Mode	AP	~	
WAN Interface				Wireless Netwo	ork Mode	Mixed	~	
Wi-Fi				Wireless Network Nam	ne (SSID)	LORAWANEU868		
Diagnose				Wireless	Channel	Auto	~	
Firewall				Chanr	nel Width	Auto 🗸		
[ା] ଅ LoRa Gateway				Wireless SSID B	roadcast Dis	sable 🚺 Ena	able	
a LoRa Network Server∖						🔮 Save & Mo	dify	

3. Network Diagnosis

- ➢ Path: Network → Network Diagnosis
- **Function**: Support Ping, Traceroute, NsLookup Commands
- **Details**:
 - ♦ Ping: A program used to test network connectivity.
- \diamond Traceroute: The command uses the ICMP protocol to trace all the routers between your computer and the target computer.

 \diamond NsLookup: It is a command-line tool for monitoring whether DNS servers in the network can perform proper domain name resolution.

> Preview:

☐ Status ^	Dashboard / Network / Diagnose		
Overview	Device × Overview × System Log × WAN Interfac	2e × WI-FI × Olagnose ×	
LoRa Packet Logger	Network Tool		
System Log	8.8.8.8	120.42.46.98	120.42.46.98
⊠ Network ∧	# Ping	Traceroute	₩ Nslookup
WAN Interface	DING 8 8 8 8 (8 8 8 8): 56 data twice		
Wi-Fi	64 bytes from 8.8.8.8: seq=0 ttl=109 time=191.662 64 bytes from 8.8.8.8: seq=1 ttl=109 time=190.482	! ms 2 ms	
	64 bytes from 8.8.8.8: seq=3 ttl=109 time=191.155	i ms	
Firewall	 8.8.8.8 ping statistics 4 packets transmitted, 3 packets received, 25% pa round-trip min/avg/max = 190.482/191.099/191.66. 	icket loss i2 ms	
🕅 LoRa Gateway			

- 4. Firewall
 - ▶ Path: Network \rightarrow Firewall
 - **Function:** Configuration of Firewall Parameters
 - > Details:
 - \diamond Configure parameters according to the page display.



Preview:

Generation Status	⊒ Dashboard	d / Network / F	Firewall					
Overview	Device × Ove	erview × Syste	em Log 🛛 ×	WAN Interface $\ \times$	WI-FI ×	Diagnose ×	• Firewall ×	
LoRa Packet Logger	Security							
System Log	Firewall Pro	otection						
Network	🗌 SPI Fi	irewall						
WAN Interface	Additional F	Filters						
Wi-Fi	Filter I	Proxy Cookies						
Diagnose	🔲 Filter .	Java Applets						
Firewall	Filter /	ActiveX						
'⊯' LoRa Gateway	Block WAN	Requests						
ᡦ LoRa Network Server∖	☑ Block.☑ Filter I	Anonymous WAI	N Request)	s (ping)				
Status	Block	WAN SNMP acc	ess					
Basic	Impede WA	N DoS/Brutefo	orce					
Gateway	🔲 Limit S	SSH Access						

4.1.3.2 LoRa Gateway

- 1. Basic Settings
 - ▶ Path: LoRa Gateway \rightarrow Basic Settings
- **Function:** Gateway Protocol Configuration, which can be configured as Build-in LoRa Server, Semtech UDP GWMP Protocol, Basics Station mode.
 - > Details:
 - ♦ Semtech UDP GWMP Protocol GWMP Forwarding Mode

■ Gateway MAC: Gateway's unique identifier, with a length of 8 bytes (16 characters), typically not modified.

- Protocol: UDP GWMP Protocol, which connects to an external NS server, with the gateway acting as a data forwarding role.
 - Server Address: IP or Domain Name
 - Server Port: Port Number (e.g. 1700)

Server Timeout Time (milliseconds): The timeout duration for waiting for acknowledgment when sending data reports. Generally, no modifications are needed.

Keepalive Interval (seconds): The interval duration for the "pull_data" command in the protocol. Generally, no modifications are needed.

■ Internal UDP Communication Port: In the case of gateway cascading applications, this port number, configured as the server port for the gateway, should match the server port of the sub-gateway.

Four-Faith	User Manual for F8926-GW-02 Series LoRaWAN In	door Gateway
🖵 Status 🔷	Dashboard / LoRa Gateway / LoRa Gateway	
Overview	Device × Overview × System Log × WAN Interface × WI-FI × Diagnose × Fire	wall × • LoRa Gateway ×
LoRa Packet Logger	Basic Frequency Band Set Beacon Set Packet Filter	
System Log	* Gateway MAC 54D0B4FFFE9B00	60
ຜ Network ^	Protocol Semtech UDP GW	MP Protocol V
WAN Interface	Server Address 47.90.209.17	
Wi-Fi	Server Port(UDP) 27915	
Diagnose	Server Timeout(ms) 100	
Firewall	Keepalive Interval (s) 10	
🕅 LoRa Gateway	Internal UDP Port 1699	
	Save & h	fodify

♦ Build-in LoRa Server - Built-in NS Mode

■ Gateway MAC: Gateway's unique identifier, which is 8 bytes in length (16 bits), is usually not modified.

■ Protocol: Built-in NS mode, equivalent to deploying NS inside the gateway.

• Keepalive Interval(s): The interval time for the pull_data command in the protocol, usually not modified.

■ Internal UDP Communication Port: In gateway cascading applications, configure this port number as the server port of the sub-gateway.

Basic	Frequency Band Set	Packet Filter	
		* Gateway MAC	54D0B4FFFE9B006C
		Protocol	Build-in LoRa Server
		Keepalive Interval (s)	10
		Internal UDP Port	1699
			Save & Modify

♦ Basics Station - More secure and reliable protocols (via WebSocket or HTTP) are used to connect to the Network Server (NS)

■ Gateway MAC: The unique identifier of the gateway, with a length of 8 bytes (16 characters). Generally, it is not modified.

- Protocol: Basicstation Mode
- Server: LNS Protocol (for regular data communication) or CUPS Protocol (for adding gateway upgrade-related protocols).



■ URI: Server Address (IP or domain name) for connection.

■ Port: Server corresponding port.

Authentication Mode: Security authentication mode (detailed

introduction of various modes' application scenarios will be provided later), below is a brief introduction of each mode:

• No Authentication: Establish regular WebSocket or HTTP connections without the need for authentication (e.g. ChirpStack configured in this mode and integrated with TTN platform).

Authentication Mode	No Authentication	~

• TLS Server Authentication: TLS server identity authentication is achieved by establishing TLS connections (wss, https) to authenticate the server (LNS or CUPS) (e.g. ChirpStack configured in this mode).

Authentication Mode	TLS Server Authentication	~	
trust			

• TLS Server and Client Authentication: TLS server and client identity authentication is achieved by the gateway establishing TLS connections (wss, https) to authenticate the server (LNS or CUPS), and the server verifies the gateway by requesting its certificate and a signature with a private key (e.g. when integrating with the AWS platform).

Authentication Mode	TLS Server and Client Authentication \sim	
trust		
		li
certificate		
		h
key		

• TLS Server Authentication and Client Token: The gateway authenticates the server (LNS or CUPS) by establishing a TLS connection (wss, https), and the server verifies the gateway's identity by inspecting the secure token provided by the gateway (e.g. when integrating with TTN platform).

ur-Eaith	User	Manual	for	F8926-GW-C)2 Series	LoRaWAN	Indoor	Gateway
Aut	hentication Mode	TLS Server	Authentic	ation and Client To	ken	~		
	trust							
								,
	tokan							
	token							
Preview	V :							
*	Gateway MAC	54D0B4	FFFE9B0	006C				
	Protocol	Basics S	station					
						~		
	Server	LNS Ser	ver			~		
	Server	LNS Ser	ver			~		
	Server	LNS Ser	ver 9Q4NHF	15TTZ8X.Ins.lora	wan.us-east-1.ai	wazonaws.com		
	Server URI Port	LNS Ser wss://A3	ver 9Q4NHF	15TTZ8X.Ins.lora	wan.us-east-1.a	w mazonaws.com		
	Server URI Port	LNS Ser wss://A3 443	ver 9Q4NHF	45TTZ8X.Ins.lora	wan.us-east-1.ai	wazonaws.com		

2. Frequency Band Configuration

➢ Path: LoRa Gateway → Frequency Band Settings

➤ **Function:** Configuration of Gateway Frequencies, applicable to modes: Semtech UDP GWMP Protocol or Build-in LoRa Server. For Basics Station mode, frequency settings are configured in the NS server.

- > Details:
 - \diamond Frequency configuration is primarily supported through three methods:

■ Custom Frequency Mode: This method provides a straightforward way to visualize the allocated frequency points, as shown in the diagram below. The left-colored frequency points (e.g. 867.1) are deletable, while the right-colored frequency points (e.g. 868.1) are essential and cannot be removed as they represent mandatory fields for the frequency band. To delete a frequency point, simply click the "×" icon next to it. To add a new frequency point, click the "+ Add" button on the far right.

🖵 Status 🛛 🔿	🗉 Dashboard / LoRa Gateway / LoRa Gateway 🕹
Overview	描页 × Overview × ● LoRa Gateway ×
LoRa Packet Logger	Basic Frequency Band Set Packet Filter
System Log	Working Area (Frequency Band MHz) EU865 V RF board type does not match frequency band (RF board type = 470, Bandhame = EU866)
⊠ Network ⊻	Is Customize preset group Custom frequency
'X ^I LoRa Gateway	Conform to LoRaWAN The page switching data will not be synchronized, and it will take effect after cicking Save & Modify on the corresponding page.
LoRa Network Server	LoRaWAN Public 🗾
☺ System ∽	Multi-SF LoRa Channel (MHz) 867.1 × 867.5 × 867.7 × 868.1 × 868.5 ×
	Save & Modify

■ Preset Group Mode: This method is the most convenient. Based on your needs, you can select the corresponding preset group. The displayed frequency



points represent the starting frequency and ending frequency, with a general interval of 0.2MHz between them. There are a total of 8 frequency points in this preset group.

Basic	Frequency Band Set	Packet Filter		
	Work	ing Area (Frequency Ba	nd MHz) EU868	~
		ls Cu	stomize preset group custom frequency	
		Frequency band g	channel 0 ~ channel 7 (867.1MHz ~ 868.5MHz)	~
			Save & Modify	

■ Custom Frequency Points + Conform to LoRaWAN Mode: This method aligns closely with the gateway's configuration file structure and is the most comprehensive configuration approach. When the other two methods cannot meet the requirements, this method should be used for configuration.

Basic	Frequency Ba	nd Set Pa	cket Filter								
		Working Are	a (Frequency E	and MHz)	U868			∼ RF b	oard type does not mat	ch frequency band [RF t	poard type = 470, Bandname = EU868
			ls (customize pres	set group 🚺	custom freque	ncy				
			Conform to	LoRaWAN	The page switching	data will not be synch	onized, and it will take	effect after clicking Si	ive & Modify on the cor	responding page.	
			LoRaW	AN Public							
		Radio	0 Center Freq	uency(Hz) 8	57500000						
		Radio	1 Center Freq	uency(Hz) 8	58500000						
		Mir	nimum Tx Freq	uency(Hz) 8	53000000						
		Ma	ximum Tx Freq	uency(Hz) 8	7000000						
	chan.ID	MultiSF 0	MultiSF 1	MultiSF 2	MultiSF 3	MultiSF 4	MultiSF 5	MultiSF 6	MultiSF 7	LoRa std	FSK
	Enable										
	Radio	Radio 0	Radio 0	Radio 0	Radio 0	Radio 0	Radio 1	Radio 1	Radio 1	Radio 1	Radio 1
	lf(Hz)	-400000	-200000	0	200000	400000	-400000	-200000	0	-200000	300000
	Freq.	867.1MHz	867.3MHz	867.5MHz	867.7MHz	867.9MHz	868.1MHz	868.3MHz	868.5MHz	868.3MHz	868.8MHz
	Bandwidth	125KHz	125KHz	125KHz	125KHz	125KHz	125KHz	125KHz	125KHz	250KHz	125KHz

> Preview:

Working Area (Frequency Band MHz)	EU868		RF board type does n	ot match frequency band [RF board type = 470, Bandname = EU868	J
Is Customize	preset group 🚺 d	ustom frequency			
Conform to LoRaWAN The page switching data will not be synchronized, and it will take effect after clicking Save & Modify on the corresponding page.			the corresponding page.		
LoRaWAN Public					
Multi-SF LoRa Channel (MHz)	867.1 × 867.3	× 867.5 × 867.7	× 867.9 × 868.1 ×	868.3 × 868.5 ×	
	Save & Modify				

3. Beacon Set

Web: <u>www.four-faith.com</u>



▶ **Path:** LoRa Gateway \rightarrow Beacon Set

Function: Configuring the ClassB parameters of the gateway can be done using the Semtech UDP GWMP Protocol mode.

- litech UDP GwMP Protocol h
- Details:
 - \diamond Beacon Period: Period, when set to 0, indicates that it is turned off.
 - ♦ Beacon Frequency (Hz): Frequency Point
 - ♦ Beacon Spreading Factor: Spreading Factor
 - ♦ Beacon Bandwidth: Beacon Packet Bandwidth
 - ♦ Beacon Tx Power: Transmission Power
- > Preview:

		Packet Filter	Beacon Set	Frequency Band Set	Basic
	0	Beacon Period	1		
	869525000	requency (Hz)	Beacon F		
	1	annel Number	Beacon Ch		
	0	ency Step (Hz)	Beacon Frequ		
~	SF9	reading Factor	Beacon Sp		
	125000	con Bandwidth	Bead		
	0	acon Infodesc	Be		
lodify	Save & N				

4. Packet Filter

▶ Path: LoRa Gateway → Packet Filter

> Function: At the gateway side, packets can be filtered based on configured rules to reduce the amount of irrelevant data transmitted to the NS server, thus easing the processing load on the NS. This can be configured using the Semtech UDP GWMP Protocol or Build-in LoRa Server modes.

> Details:

♦ Supports configuring NetID and JoinEUI.

♦ NetID: Network ID filtering, the short address portion allocated during device joining is related to the network ID. By configuring this value, non-joining interference data can be effectively filtered out. In the embedded mode, this value can be configured to the network ID configured for this gateway, thereby effectively avoiding interference from other devices' data.

♦ JoinEUI(AppEUI): JoinEUI filtering, a component of the device's triplet, can be configured with multiple sets of range values here. Once set, JoinEUI values outside the specified ranges will be filtered.

Preview:
Basic	Frequency Band Set	Beacon Set	Packet Filter				
				Add NetID Add the netID for uplink data filte	ering, the value can be used LoRa Netwo	ork Server->Basic Settings->Network	ID (e.g. 000001)
			NetID - 1:	g. 000001	Delete		
				Add JoinEUI Add the JoinEUI range for join	n data filtering, fill in the start value in the	front box, and fill in the end value in	the back box. (e.g. 0000000000000000 - 0

4.1.3.3 LoRa Network Server

1. Status

- ➢ Path: LoRa Network Server → Status
- > Function: Display statistics of flow to the embedded NS server.
- > Details:

♦ Basic Information: Mainly includes the number of gateways, the number of devices, and the statistics of device uplink and downlink data counts.

This can be used to analyze the communication quality between gateways and nodes, based on the distribution of RSSI (Received Signal Strength Indicator), SNR (Signal-to-Noise Ratio), and DataRate values.

♦ Communication Distribution: This displays the curve chart of uplink and downlink communication situations, allowing analysis of whether the distribution of uplink and downlink data matches the expected patterns.

> Preview:



Faith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gatewa
Communication distribution (uplink and downlink da	a)						
6.94								
6								
5								
4								
5					20h			
2					odownlink: 0			

2. Basic Setting

- ➢ Path: LoRa Network Server → Basic Setting
- **Function:** Configuring NS Server Parameters
- > Details:

♦ Operating Region: Corresponds to the frequency band in the regional parameter table. This setting cannot be configured here and should remain consistent with the configuration in LoRa Gateway → Frequency Band Configuration → Operating Region.

Enable Dynamic Data Rate Adjustment (ADR): Determines whether the Adaptive Data Rate (ADR) feature is enabled.

♦ ADR Margin: This value affects the sensitivity of ADR adjustment. A larger value makes the adjustment less aggressive, while a smaller value makes the adjustment more aggressive.

- ♦ Minimum Data Rate: The lowest data rate used for ADR adjustment.
- ♦ Maximum Data Rate: The highest data rate used for ADR adjustment.

♦ Network ID: A parameter used to generate the device's short address. It can be configured in the filtering parameters to avoid interference.

- ♦ Rx2 Frequency: Frequency of rx2 Window
- ♦ Rx2 Datarate: Datarate of rx2 Window

♦ Downlink Transmit Power (dBm): The transmit power configuration for downlink messages. When set to -1, it will follow the transmit power specifications defined in the regional parameters table.

> Preview:

Four-Faith	User	Manua I	for	F8926-	GW-02	Series	LoRaWA	N Indoor	Gateway
	Working Area (Frequency Band MH	Iz) EU868							
	AL	DR 🔵							
	ADR margin (d	B) 10							
	Minimum Ra	te LoRa:SF	=12/125kHz				\sim		
	Maximum Ra	te LoRa:SF	-7/125kHz				~		
	Network	ID 000000					Network id	entifier (NetID, 3 bytes) en	coded as HEX (e.g. 010203)
	Rx 2 Frequency (H	lz) 8695250	000						
	Rx 2 Datara	te LoRa:Sf	=12/125kHz				\sim		
			Save & M	lodify					

3. Gateway

➢ Path: LoRa Network Server → Gateway

➢ Function: Gateway Addition, Modification, and Deletion in Embedded NS: Gateways are usually automatically added when they connect and typically do not require manual addition.

> Details:

♦ Displaying the Gateway List: The list shows detailed information for each gateway, including online status and more.

> Preview:

+ Add	⊘ Export								
ID	Gateway MAC	Name	FirstSeenAt	LastSeenAT	Latitude	Longitude	Altitude(m)	is Online	Operrate
1	54d0b4fffe9b006c	54d0b4fffe9b006c	2022-05-16 15:16:48	2023-08-16 17:06:01	0	0	0	true	🖉 Edit 🔲 Delete

4. Application

▶ Path: LoRa Network Server → Application

> **Function:** It is equivalent to the grouping function, where different groups correspond to different application scenarios for easier management.

> Details:

♦ Add Application: After clicking the "Add" button, the following page will open.

■ Name: This is equivalent to the group name, just for identification purposes.

■ AppKEY: The AppKEY corresponding to the terminal, which is used to verify the value when adding devices automatically (clicking on the right side of "default" will change it to the default value of Four-Faith).

■ Auto-Add Devices: When selected, devices can be added automatically without the need to add them in advance. Once the AppKEY and AppEUI validation is successful, devices will be added automatically.

■ AppEUI (JoinEUI): One of the triplets required for device configuration. When enabling auto-add devices, this needs to be configured (clicking on the "default" option will change it to the default value provided by Four-Faith).

Type: The device type corresponding to auto-added devices, either



ClassA or ClassC.

New application

Description: Description information.

Name	pdtest	\odot
* AppKEY	2b7e151628aed2a6abf7158809cf4f3c \odot	default
Auto Add Dev	If enabled, LoRaWAN Device will be added automatically after Application Application Key pass verification.	on EUI and
AppEUI	7538904770366680	default
Туре	Please select V Join automatically adds device types	

♦ Delete: It is not possible to delete the application if devices are associated with
 it. You must delete the devices first before deleting the application.

 \diamond View: Once inside the application, you can access the list of devices and other related information.

• Device Management: Detailed explanation of device addition, deletion, modification, and retrieval.

■ Application Configuration: Similar to the creation process, here you can modify existing applications.

■ Interface Management: Configure HTTP POST, when this feature is enabled, all data from devices under this application will be pushed to the specified address using the HTTP POST method.

Device	e Manage	Application Set Inte	grations						
Please I	nput DevEul	Q Search	+ Add Add In I	Bulk 🗍 Delete In E	Bulk	⊙ Export			
	ID	LastSeenAT 🌩	DevEUI	Name	Туре	Join Mode	Device addr	Description	Operate
	20	2023-08-11 10:53:49	ff00058005000090	#00058005000090	С	OTAA	01e97ee4		View Delete
	22	2023-08-16 16:59:33	ff20230816165412	TEST111	с	OTAA	00e3c7cb		© View 🗐 Delete
	23	2023-08-16 17:01:43	ffddee0000000002	dev_00000002	A	OTAA	01bed7a7	auto join device	View Delete

40

×

Device Manage	Application Set	Integrations					
		HTTP push s	witch				
		Uplink Data		ample: http://192.1	68 1 1 8080/upl	ink	
		Join Notification		ample: http://192.1	68.1.1:8080/ioin		
				New bood parame	tore		
				New nead parame	iters		
				Save 8	s modity		

	Operate
2. pdlest 3 2022-05-18 13:56:31 true pulse test	© View 🗍 Delete

5. Devices

➢ Path: LoRa Network Server → Devices

Function: Device Addition, Deletion, Modification, and Query: Web Entry: LoRa Network Server -> Applications -> View -> Device Management

> Details:

Add New Device: Setting the Basic Parameters of the Device. Joining methods include OTAA (where the device initiates joining) or ABP (where no joining is required). When the AppKEY of this device is different from the AppKEY of the application, you can specify a specific AppKEY here.

New device

* DevEUI	The unique code of the device, the length is 8 bytes, such as: 0102						
Name							
Туре	ClassA						
Join Mode	ode OTAA ~						
MAC Version	1.0.2 🗸						
AppKEY	When empty, application.AppKEY will be used.						
Description	Description						
	(a) Cancel	O Confirm					

■ ABP Mode: In this mode, you need to input the Short Address and Session Keys information as shown in the boxes.

41

×

New device		
* DevEUI	The unique code of the device, the length is 8 bytes, such as	0102
Name		
Туре	ClassA	~
Join Mode	ABP	~
MAC Version	1.0.2	~
Device addr	For example: 01020304	
Application Session Key	For example: 01020304050607080900010203040506	S
Network Session Key	For example: 01020304050607080900010203040506	C
Description	Description	

♦ Bulk Add: The parameters for bulk adding devices are similar to adding a single device. However, it's important to note that bulk adding can only be used for adding OTAA devices.

Start DevEui	ff01020304050607	0
Device Number	- 10	+
Туре	ClassA	~
MAC Version	1.0.2	~
AppKEY	When empty, application AppKEY will be used	d.,

✤ Bulk Delete: To perform a bulk deletion, you need to first check the checkboxes next to the devices you want to delete, and then click on the "Bulk Delete" button.

Four-Faith			User Ma	anual for	F8926-GW-02	Ser	ies L	_oRaWAN I	ndoor Gateway	/
	Device	Manage	Application Set Inte	egrations	In Bulk		Export			
		ID	LastSeenAT 🔶	DevEUI	Name	Туре	Join Mode	Device addr	Description	Operate
		20	2023-08-11 10:53:49	ff00058005000090	ff00058005000090	С	OTAA	01e97ee4		View Delete
		22	2023-08-16 16:59:33	ff20230816165412	TEST111	С	OTAA	00e3c7cb		© View Delete
		23	2023-08-16 17:01:43	ffddee00000000002	dev_00000002	A	OTAA	01bed7a7	auto join device	View Delete

♦ Export: This option allows you to export the device information as an Excel spreadsheet, providing an easy way for backup and management.

♦ Device Details: By clicking on the "View" option next to the corresponding device, you can access the detailed information about that device.

• Overview: This section displays the device's uplink information and relevant statistical data. It can be used to analyze packet loss and other device communication issues.



■ Configuration: Adjust parameters for the device.

ر User Manu ا	al for I						
New device							×
* DevEUI	The unique	code of the de	vice, the length is	8 bytes, such a	as: 010/		
Name							
Туре	ClassA				\sim		
Join Mode	OTAA				~		
MAC Version	1.0.2				\sim		
AppKEY	When empl	ty, application A	AppKEY will be us	ed.			
Description	Description						
Activation Infornetwork. Overview Configure	rmation: D	Display para	ameters after	the device	ioins	the	Confirm
Activation Information network. Overview Configure	mation: D	Display para	ameters after Device addr	the device	joins	the	Confirm
Activation Infornetwork. Overview Configure	Activation	Display para Debug App	ameters after Device addr lication session	the device oss 00e3c7cb	joins	the	024399be
Activation Infornetwork. Overview Configure	Activation	Display para Debug App	ameters after Device addr lication session	the device ss 00e3c7cb (ey cc13949ft (ey e4762cda	; joins ; join	193f795a5	024399be 13b99cdcf
Activation Infornetwork. Overview Configure	Activation	Display para Debug App N	ameters after Device addr lication session letwork session	the device of the device	e joins	193f795a5	024399be 13b99cdcf
Activation Infor network. Overview Configure	Activation	Display para Debug App N U Dow	ameters after Device addr lication session letwork session plink frame-cour	the device the device output of the device	e joins	193f795a5	024399be 13b99cdcf
 Activation Infornetwork. Overview Configure Online Debuggi 	ng: Allow	Display para Debug App N U Dow	ameters after Device addr lication session letwork session plink frame-cour mlink frame-cour downlink (sc	the device the device output of the device output of the device output of the device the device output of the device output o	e joins e joins e730db 3196263 ownlin	the 193f795a5 541349fd ² k) and	024399be 13b99cdcf
Activation Infornetwork. Overview Configure Online Debuggited isplays uplink data for determined to the second seco	Activation Activation	Display para Debug App N U Dow rs for data c purposes.	Device addr Device addr lication session letwork session plink frame-cour mlink frame-cour downlink (sc	the device the device oss 00e3c7cb (ey cc13949ft (ey e4762cda ther 7 ther 1 heduled do	e730db [*] 3196263	the 193f795a5 541349fd k) and	024399be 13b99cdcf
Activation Infornetwork. Overview Configure Online Debuggi displays uplink data for de Overview Configure Activation Debuggi	ng: Allow cbugging I	Display para Debug App N U Dow rs for data o purposes.	ameters after Device addr lication session letwork session lplink frame-cour mlink frame-cour downlink (sc	the device the device output of the device output of the device ter 7 ter 1 heduled do	e joins e joins e730db 3196263	the 193f795a5 541349fd ² k) and	024399be 13b99cdcf
Activation Infornation Activation Infornation Overview Configure Overview Configure Online Debuggin displays uplink data for de Overview Configure Activation Debug Timed sending Debug Timed sending Debugging	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow os for data o purposes.	ameters after Device addr lication session letwork session lplink frame-cour nlink frame-cour downlink (sc	the device the device output of the device the devi	e joins e joins e730db 3196263 ownlin	the 193f795a5 541349fd k) and	Confirm 024399be 13b99cdcf 13b99cdcf
 Activation Infornetwork. Overview Configure Online Debuggit displays uplink data for determing Overview Configure Activation Debug 	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow of for data of purposes.	Device addr Device addr lication session letwork session plink frame-cour mlink frame-cour downlink (sc Receiving time 2023-06-16 17.18.26	the device the device output the device the device	erancel joins oe730db 3196263 ownlin	the 193f795a5 541349fd k) and	024399be 13b99cdcf 13b99cdcf Data 3434343434
 Activation Infornation network. Overview Configure Online Debugging displays uplink data for destruction Online Debugging displays uplink data for destruction 	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow os for data o purposes.	ameters after Device addr lication session letwork session lplink frame-cour nlink frame-cour downlink (sc Receiving time 2023-08-16 17:18-26	the device the device of the device of the device the device tess 00e3c7cb tey cc13949ft tey e4762cda ther 7 ther 1 heduled do	e joins e joins e730db 3196263 ownlin	the 193f795a5 541349fd k) and	Confirm 024399be 13b99cdcf 13b99cdcf 13b3434343434
 Activation Infornation intervents. Overview Configure Configure <l< td=""><td>Activation Activation ng: Allow ebugging p</td><td>Display para Debug App N U Dow ors for data of purposes.</td><td>Device addr Device addr lication session letwork session lplink frame-cour mlink frame-cour downlink (sc 2023-08-16 17:18:26</td><td>the device the device of the device of the device the device the device the device the device the device</td><td>e joins e joins e730db 3196263 ownlin</td><td>the 193f795a5 541349fd⁴ k) and</td><td>Confirm 024399be 13b99cdcf 13b99cdcf 0ata 0ata 34343434</td></l<>	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow ors for data of purposes.	Device addr Device addr lication session letwork session lplink frame-cour mlink frame-cour downlink (sc 2023-08-16 17:18:26	the device the device of the device of the device the device the device the device the device the device	e joins e joins e730db 3196263 ownlin	the 193f795a5 541349fd ⁴ k) and	Confirm 024399be 13b99cdcf 13b99cdcf 0ata 0ata 34343434
 Activation Infornation network. Overview Configure Configure Configure Configure Activation Debugging Configure Activation Debug Timed sending Configure Fired sending Configure Configure Activation Debug Timed sending Configure Configure Activation Debug Fired sending Configure Configure Activation Debug 	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow of for data of purposes.	Device addr Device addr lication session letwork session lplink frame-cour mlink frame-cour downlink (sc Receiving time 2023-06-16 17:18:26	the device the device output output output the device output the device output	e730db 3196263 ownlin	the 193f795a5 541349fd k) and	Confirm 024399be 13b99cdcf 13b99cdcf 0434343434
Activation Infornation Infornation Infornation Information Informatio Information Information Information Information Infor	Activation Activation ng: Allow ebugging p	Display para Debug App N U Dow os for data o purposes.	ameters after Device addr lication session letwork session lplink frame-cour nlink frame-cour downlink (sc exercise 2023-06-16 17:18/26 D: "2", mer: "pittert", "based: "based: "2", "test111", "addbafffebboocc",	the device the device ass 00e3c7cb (ey cc13949ft (ey e4762cda ther 7 ther 1 heduled doc Gateway(D 54004###90006c	e joins e joins be730db 3196263 ownlin	the 193f795a5 541349fd ¹ k) and	Confirm 024399be 13b99cdcf 13b99cdcf 13b34343434

> Preview:

-Fa	® ith		User Manua	al for	F8926-0	GW-02	Series	LoRaWAN	Indoor	Gatewa
Applicati	ion > pdtest									
Devic	e Manage	Application Set Inte	grations							
Please	Input DevEui	Q Search	+ Add Add In Bui	k 🗇 Delete In Bu	lk 🛛 🛇 Expo	tro				
	ID	LastSeenAT 🔶	DevEUI	Name	Туре	Join Mode	Device addr	Descrip	ption	Oper
	20	2023-08-11 10:53:49	#00058005000090	ff00058005000090	c	OTAA	01e97ee4			(D) View
	20	2020-00-11 10:00.45	100000000000000000000000000000000000000			0.0.01				

6. Multicast

22

➢ Path: LoRa Network Server → Multicast

➤ **Function:** In this context, multicast refers to the ability to send data to multiple devices with the same configuration parameters within the NS. Multicast data can be sent using MQTT, and you can also test sending multicast data through the web interface.

> Details:

2023-08-16 17:18:26

♦ Add Multicast: Below are the corresponding values for Four-Faith devices

00e3c7cb

© View Delete

OTAA

Uplink Channel Start Frequency	868700000
Uplink Channel Number	3
Iulticast Param	
Device Address	00:00:01
NwkSKey	00:00:00:00:00:00:00:00:00:00:00:00:00:
AppSKey	00:00:00:00:00:00:00:00:00:00:00:00:00:
X2	
Receive frequency	869525000
Receive speed	0
utomatic reporting of successful ne	etwork addition
Enable	e 🔻

 \diamond Based on the values provided above, configure the multicast parameters.

Edit							
	* Name	mutilcast					
* Multica	ast Address	00000001					S
* Multicast network s	session key	000000000000000000000000000000000000000	0000000000000	2			G
* Multicast application s	session key	000000000000000000000000000000000000000	000000000	3			0
Multicast	-group type	Class-C					
	Data-rate	0					
Free	quency (Hz)	869525000					
After creation Add Wulticast	n, you will b	e able to see the follo	wing mu	lticast	list info	ormatio	n.

SSCOM V5.13.1 Serial/Net data debugger,A PORT COM_Settings Display Send_Data

[17:34:32.986]IN←◆1234|

♦ During actual usage, multicast data can be sent using MQTT or TCP. Please refer to the data format for more details.

③ Cancel

⊘ Confirm

7. Interface

- ➢ Path: LoRa Network Server → Interface
- > Function: Configuration page for integrating the internal NS with a customer



platform is available, supporting both MQTT and TCP communication methods. Data can be transformed using JavaScript functions, and heartbeat configurations are also supported.

- Details:
 - ♦ Protocol Configuration
 - NONE: Not enabled.

■ MQTT: MQTT parameter configuration, specific topics and data formats are detailed in the data format section.

Protocol config	Data conver	Heartbeat config		
		Protocol type	MQTT	
		MQTT Switch	close open	
		Server addr	47.90.209.17	
		Server port	18868	
		ClientID	Ev4gzOBP	
		CleanSession		
		QOS	exactly once 🗸	
		Keepalive(sec)	20	
		User auth		
		User Name	ZSC	
		Password	123456	
		SSL/TLS Mode	Disable	
		Join topic	application/{{application_ID}}/device/{{device_EUI}}/join	default

■ TCP: Integrating with TCP servers allows for simultaneous connections to multiple servers, and the connection status can be used to determine the connection situation.

Protocol config	Data conver	Heartbeat config	
		Protocol ty	ре ТСР 🗸
		TCP -	1: Switch status: close open
			Server addr: ws1.omnicam.com.sg
			Server port: 60000
			Connect status:
			+ Add Connect
		Cache frame numb	er 0 v When the network is abnormal, the galeway caches the latest data quantity and sends if our immediately after the connection is successful. If it is 0, it will not be cached
			(recommended value 100)

 ◇ Data transformation: If no configuration is done here, the default data format will be used for communication. If you need to transform data, you can configure functions for the conversion. After uplink and downlink data reaches the gateway, it can be transformed using specified functions before forwarding.

Uplink transformation



Downlink transformation

C Default template

🖹 Сору

avaScript function	Analog input data
function Encode(obj) { var bytes = []; bytes[0] = 10; // port bytes[1] = 0; // 0-unconfirmed, 1-confirmed	{"devEul": "ff000000000000001", "cmdCode": 1, "heartbeatCycle": 60}
<pre>// bytes 2~9 = devEui. for (var i = 0; i < obj.devEui.length; i+=2) { bytes.push(parseInt(obj.devEui.substr(i, 2), 16));</pre>	↓ Conver
}	Analog output data
<pre>// bytes 10~n Send to device content. bytes[10] = obj.cmdCode; bytes[11] = obj.heartbeatCycle; return bytes;</pre>	01 3c
}	1

🗇 Clear

■ TCP packet generation tool: During the testing phase of using TCP to connect to the server, you can use this tool to generate corresponding data for testing by sending it through the TCP server. In actual projects, you can write a program to generate the data.

Four-Fa	aith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
				TCP pa	ckage tool				
This tool is used Downlink data. (t	to group TCP protocol package (HEX+JSON) vas64 online tool: https://base64.us/)	, copy part of json conte	nt (template in default	data format) t	o JSON content box (modify devEul)	, and the converted re	sult can be sent to gatewa	y through TCP assista	nt to realize \times
JSON Object	{"devEui":"0102030405060708","confirmed	":false, "iPort": 10, "data":	'YWJjZA=="}						default
			↓ Conver						

♦ Heartbeat Configuration: You can configure the heartbeat switch, heartbeat interval time, and heartbeat data format. It supports configuring a custom string as the heartbeat data. Heartbeat is mainly used to periodically report status information. The gateway can also use heartbeats to determine the connection status between itself and the MQTT server.

After the heartbea of heartbeat cycle customization	at is turned on, it will is to not subscribe to	regularly pu heartbeat c	sh the heartbea lata as the basi	at content (M s for judging	QTT/TCP) to the the gateway disc	client pl connectio
Heart	beat switch clo	se 🔵	open			
interv	Heartbeat //		60	+		
Heartbeat	data format def	ault 🔵	customize			

4.1.3.4 System

Conver result

1. System

➢ Path: System → System

➢ Function: View Program Version, Configure Token Duration, Time Settings and Language Switch

> Details:

 \diamond System Program Version: Use this to trouble shoot related issues by checking the version.

 \diamond Token Expiry Time: The shorter the time, the more frequent the need for webpage login.

♦ NTP Time Configuration: Configure NTP

> Preview:

Basic language								
System Params								
System Version								
Token valid	2592000	When the t	oken expires	, you need to log in again.				
time(Sec.)								
Log level	DEBUG	✓ The higher	the log level,	, the more information you can v	riew. For example, D	EBUG- logs of all types	are printed, FATAL-	Logs of only FATAL
	displayed.							

Save & Modify

- 2. Change Password
 - ▶ Path: System → Change Password
 - **Function:** Change the gateway system password, length range 5-32.
 - > Details:

 \diamond Enter the new password and confirm the password. After modification, log out of the system. When logging in again, use the new password.

> Preview:

* New Password	Not less than 5 bits	
* Confirm Password	Same as the new password	

3. Restart

- ▶ Path: System \rightarrow Restart
- ➢ Function: Restart Gateway
- **Details**:
 - \diamond Click to restart the gateway.
- > Preview:

System Reboot

C Execute Reboot

4. Restore to factory settings.

▶ Path: System \rightarrow Restore to factory settings.

Function: Clicking on this will restore the gateway to its factory settings, primarily affecting router-related parameters such as network settings (LoRa-related parameters like device lists, join information, etc., will not be deleted).

- ➢ Details:
 - \diamond Clicking this button will initiate the factory reset process.
- > Preview:

Four-Faith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
System Reboot								
C Execute Reboot								

4.1.4 Data Format

4.1.4.1 Data Explanation

1. Data Format Explanation

Protocol for connecting to the client includes MQTT, TCP, and HTTP. Both MQTT and TCP support two-way communication, while HTTP only supports the gateway pushing data to the client using the POST method and does not support downlink. Below is the data explanation for various protocols:

- MQTT Data: Topic + JSON Content
- TCP Data: Header + JSON Content
- HTTP Data: URL + JSON Content

Note: The JSON content data format is consistent within the same type, and if JavaScript function transformation is applied, it will be applied to all data.

2. MQTT Data Flow



As shown in the diagram, in this mode, you need to deploy an MQTT Broker first. Both the gateway and the client platform establish connections with it and subscribe to relevant topics according to the topic format. If the client needs multiple sets of data, multiple clients can connect and subscribe. In comparison to the TCP mode, this method involves an additional step of setting up an external MQTT server.

3. TCP



As depicted in the diagram above, in this mode, the client platform opens a TCP server, while the gateway is configured in TCP mode and points to the corresponding server's IP and port. This configuration allows for the establishment of multiple TCP connections simultaneously.



As shown in the diagram above, the configuration for this mode is within the interface settings of each application. This mode only supports data pushing and does not support downstream data.

4.1.4.2 MQTT Data Format

1. MQTT Topic and Data Format

• The default MQTT topic format is as follows:



• The MQTT approach primarily consists of topics and data content. Topics are displayed and can be modified within the interface.

The default topic includes {{application_ID}} and {{device_EUI}}

■ {{application_ID}}: Application ID, it will be replaced with the corresponding application ID of the device when reporting data (e.g.,

4. HTTP



application/1/device/6e110000000000/rx). For downlink data, it also needs to be replaced with the actual application ID of the device (e.g., application/1/device/6e110000000000/tx).

■ {{device_EUI}}: Device unique identifier, it will be replaced with the device's EUI when reporting data (e.g., application/1/device/6e110000000000/rx). For downlink data, it also needs to be replaced with the actual device EUI (e.g., application/1/device/6e110000000000/tx). When this field is included in the topic, the JSON content of the downlink data can omit the device's unique identifier.

Modification Description

• You can modify the topic, for example, change it to "lorawan/uplink" or similar.

• $\{\{application_ID\}\}$: This can be removed, and after removal, the topic will only lack the application ID.

■ {{device_EUI}}: If removed, the topic won't be able to identify the corresponding device. Therefore, the JSON content of the downlink data must include the device's unique identifier (as explained in the following content).

Example of Subscribed Topics

■ Subscribe to a Single Device for a Single Event:

application/1/device/6e110000000000/rx

■ Subscribe to All Events for a Single Device: application/1/device/6e110000000000/+

■ Subscribe to a Single Event for All Devices in an Application: application/1/device/+/rx

■ Subscribe to All Events for All Devices in an Application: application/1/device/#

■ Subscribe to a Single Event for All Devices in All Applications: application/+/device/+/rx

■ Subscribe to All Events for All Devices in All Applications: application/+/device/+/+ or application/#

The data content is in JSON format, and the specific format is detailed below. It's important to note that if the {{device_EUI}} placeholder is removed from the downlink topic, the topic won't be able to identify the specific device. In this case, you need to look for the "devEui" field in the data content. If the "devEui" field is also absent, the specific device data will be lost.

2. Uplink Data

Execution Condition: Forward when receiving business data reports from successfully joined devices.

- Default Topic Format: application/{{application_ID}}/device/{{device_EUI}}/rx
- Default Topic Example: application/1/device/6e110000000000/rx
- Default JSON Data Content Example:



ł "applicationID": "1", "applicationName": "temperature", "deviceName": "dev_00000000", "devEui": "6e1100000000000", "rxInfo": [{ "gatewayID": "ff000000000000a", "name": "ff0000000000000a", "time": "", // Only when the gateway can receive GPS signals will there be actual values. "rssi": -76, "loRaSNR": 7.5, "location": { "latitude": 0, "longitude": 0, "altitude": 0 } }], "txInfo": { "frequency": 868100000, "dr": 0 }, "adr": false, "fCnt": 6, "fPort": 32, "data": "MTQ10TYzNTgy" // Base64 encoding, you can refer to the "Base64 Encoding and Decoding" section later for more information.

}

3. Join Data

Execution condition: Pushed upon receiving a device's join request and responding *



to the join accept message.

- Default Topic format: application/{{application_ID}}/device/{{device_EUI}}/join
- Default Topic Example: application/1/device/6e1100000000000/join
- Default Data Content Example:

{

"applicationID": "1",

"applicationName": "temperature",

"deviceName": "dev_00000000",

"devEui": "6e1100000000000",

"devAddr": "01b0e489"

}

4. Downlink Data

- Execution Condition: Sending business data to the device
- Default Topic Format: application/{{application_ID}}/device/{{device_EUI}}/tx
- Default Topic Example: application/1/device/6e110000000000/tx
- Default JSON Data Content Example:

{

"devEui": "6e1100000000000",

"confirmed": true,

"fPort": 12,

"data": "MTIzNA==" // Base64 encoded, please refer to the "Base64 Encoding and Decoding" section

below. This corresponds to "1234".

}

Convenient test data (the data above contains spaces, which might cause transmission failures):

{"devEui":"6e110000000000","confirmed":true,"fPort":12,"data":"MTIzNA=="}

5. Downlink acknowledgment packet response:

• Execution condition: After receiving the downlink acknowledgment packet, push the data when the device responds.

- Default Topic Format: application/{{application_ID}}/device/{{device_EUI}}/ack
- Default Topic Example: application/1/device/6e110000000000/ack
- Default JSON Data Content Example:

{

"applicationID": "1",



"applicationName": "temperature",

"deviceName": "dev_00000000",

"devEui": "6e1100000000000",

"acknowledged": true

}

6. Downlink multicast data.

• Execution condition: When multicast information needs to be sent to devices with the same triplets as the multicast group.

- Default Topic Format: mcast_group/{{mcast_ID}}/tx
- Default Topic Example: mcast_group/1/tx
- Default JSON Data Content Example:

```
{
```

"multicastGroupId": 1,

"fPort": 10,

"data": "YWJjZA==" // base64 Encoding

}

Convenient test data

```
{"multicastGroupId":1,"fPort":10,"data":"YWJjZA=="}
```

7. Heartbeat data

Execution condition: Heartbeat switch is turned on, heartbeat interval > 0, heartbeat content is not empty.

- Default Topic: lorawan/heartbeat
- Default JSON Data Content Example:

{

"gateways": [{

"gatewayID": "ff000000000000a",

"gatewayName": "ff0000000000000a",

```
"lastSeenAt": "2022-04-29 14:18:36",
```

"isOnline": true,

"longitude": 0,

"latitude": 0

}],

Four-Faith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
"applications": [{								
"applicationID": 1,								
"name": "app",								
"deviceNum": 1,								
"activatNum": 1,								
"isAutoJoin": false								
}]								
}								

4.1.4.3 TCP Data Format

1. TCP Data Format

Offset	Byte count	Function	Identifier	Value example
0	1	Frame header	header	0xFE
1	1	Version number (currently V1)	version	0x01
2	2	JSON data length (big-endian)	length	0x0001
4	1	Data Type	type	0x00-Heartbeat Packet
5	2	Random key Random	random	0x1234
		number (big endian)		
7	n	JSON Content	JSON Object	{}

• The first 7 bytes are the TCP data header, and starting from the 7th byte is the JSON content. This JSON content is the same as that used in MQTT and HTTP.

2. Uplink Data

Offset	Byte	Function	Value or Description
	count		
0	1	header	0xFE
1	1	version	0x01
2	2	length	0x018A
4	1	type	0x01



5	2	random	0x1234
7	394	JSON object	{
			"applicationID": "2",
			"applicationName": "app1",
			"deviceName": "dev_00000001",
			"devEui": "ff0000000000001",
			"rxInfo": [
			{
			"gatewayID": "54c345fffed5a1e3",
			"name": "54c345fffed5a1e3",
			"time": "2021-11-19T01:51:01.136686Z",
			"rssi": -107,
			"loRaSNR": 7.5,
			"location": {
			"longitude": 118.03394,
			"latitude": 24.48405,
			"altitude": 89
			}
			}
],
			"txInfo": {
			"frequency": 923400000,
			"dr": 4
			},
			"adr": false,
			"fCnt": 4,
			"fPort": 32,
			"data": "YWJjZA=="



	}		
	,	Description	Туре
	applicationID	Application ID	string
	applicationName	Application Name	string
	deviceName	Device Name	string
	devEui	Device EUI	string
	rxInfo	Information about the receiving gateway	Array of structures
	- gatewayID	Gateway unique identifier	string
	- name	Gateway Name	string
	- time	GPS Time	string
	- rssi	Signal strength	float64
	- loRaSNR	Signal-to-Noise Ratio	float64
	- location	GPS Location (When GPS signal is not available, the value is {})	
	- longitude	Longitude	float64
	- latitude	Latitude	float64
	- altitude	Altitude	float64
	TxInfo	Device Data Transmission Parameters	
	- frequency	Frequency Point	uint32
	- dr	Rate	uint8
	adr	Whether ADR request is enabled	bool
	fCnt	Uplink frame counter	uint32
	fPort	Uplink Port	uint8
	data	Business data (in base64 encoded format)	string

3. Activation data

Offset	Byte Count	Function	Value or Description
0	1	header	0xFE



User Manual	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
-------------	-----	-------------	--------	---------	--------	---------

1	1	version	0x01						
2	2	length	0x007B	0x007B					
4	1	type	0x03						
5	2	random	0x1234						
7	123	JSON	{	{					
		object	"applicationID": "2"	"applicationID": "2",					
			"applicationName":	"applicationName": "app1",					
			"deviceName": "dev	"deviceName": "dev_00000001",					
			"devEui": "ff000000	"devEui": "ff000000000001",					
			"devAddr": "032013	ac"					
			}						
				Description	Туре				
			applicationID	Application ID	string				
			applicationName	applicationName Application Name string					
			deviceName	Device Name	string				
			devEui Device EUI string						
			devAddr	Short address assigned to the device	string				
				during activation					

4. Downlink Data

Offset	Byte	Function	Value or Description
	Count		
0	1	header	0xFE
1	1	version	0x01
2	2	length	0x004D
4	1	type	0x02
5	2	random	0x1234
7	77	JSON	{
		object	"devEui": "ff0000000000001",
			"confirmed": false,

Four-Faith	User Manual for	F8926-GW-O2 Series LoF	RaWAN Indoor Gateway		
	"fPort": 10, "data": "YWJjZA= }	'			
		Description			
	devEui	Device EUI	string		
	confirmed	Confirmation packet flag (de false)	efault: bool		
	fPort	Port (Default 10)	uint8		
	data	Sending business data (base encoded)	64 string		

Convenient test data (the data above may contain spaces, which can sometimes cause sending failures)

{"devEui":"ff000000000001","confirmed":true,"fPort":10,"data":"MTIzNA=="}

Note: You can use the TCP Packet Generator tool available on the web page (Path: LoRa Network Server -> Interfaces -> Data Conversion -> TCP Packet Generator) to generate the corresponding data for testing, as shown below:

	TCP package tool	
This tool is used Downlink data.	to group TCP protocol package (HEX+JSON), copy part of json content (template in default data format) to JSON content box (modify devEul), and the converted result can be sent to gateway through TCP assistant to reali (based online tox) https://based.us/)	ize ×
JSON Object	["dev/Eur":10102030405660708", "confirmed" failse, "IPort":10, "diatat":"YWJ[ZA=="]	default

Among them, the data that can be used for testing when sending downlink data to a TCP server is as follows (during testing, you usually need to modify the devEui):

fe01004b0204427b22646576455549223a2266663030303030303030303030303031222c22636f6e6669726d65642 23a747275652c2266506f7274223a31302c2264617461223a224d54497a4e413d3d227d

5.	Response	for a	Down	link	Cont	firma	tion	Packet
----	----------	-------	------	------	------	-------	------	--------

Offset	Byte Count	Function	Value or Description
0	1	header	0xFE
1	1	version	0x01
2	2	length	0x0000
4	1	type	0x05



5	2	random	0x1234					
7	77	JSON	{					
		object	"applicationID": "1",					
			"applicationName":	"applicationName": "app1",				
			"deviceName": "dev	/_00000000",				
			"devEui": "6e0000000	0000000",				
			"acknowledged": true					
			}					
				Description	Туре			
			applicationID	Application ID	String			
			applicationName	Application Corresponding Name	String			
			deviceName Device Name String					
			devEui	Device EUI	String			
			acknowledged	Response status: Success - true	Bool			

6. Downlink Multicast Data

Offset	Byte Count	Function	Value or Description			
0	1	header	0xFE			
1	1	version	0x01			
2	2	length	0x0000			
4	1	type	0x04			
5	2	random	0x1234			
7	77	JSON	{			
		object	"multicastGroupId":	1,		
			"fPort": 10,			
			"data": "YWJjZA=="			
			}			
				Description	Туре	

Four-Faith	User	Manual	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
		multicastG	roupId	Multicast	ID			int
		fPort		Port (De	fault 10)			uint8
		data		Sending b	ousiness data (Base64		string

Convenient test data

{"multicastGroupId":1,"fPort":10,"data	":"YWJjZA=="}
--	---------------

Note: You can use the TCP packet tool on the web page (Path: LoRa Network Server \rightarrow Interfaces \rightarrow Data Conversion \rightarrow TCP Packet Tool) to generate corresponding data for testing, as shown below:

TCP package tool

JSON Object	{"devEui":"0102030405060708", "confirmed".false, "fF	Port":10,"data":"YWJjZA=="}	default
		↓ Conver	
Comments and the			

The converted result can be used for testing by sending it to the TCP server. The example content above is as follows:

fe01003304341e7b226d756c74696361737447726f75704964223a312c2266506f7274223a31302c2264617461 223a2259574a6a5a413d3d227d



7. Heartbeat Data

Offset	Byte	Function	Value or Description					
	Count							
0	1	header	0xFE					
1	1	version	0x01					
2	2	length	0x01BC					
4	1	type	0x00					
5	2	random	0x1234					
7	n	JSON	{					
		object	"gateways": [{					
			"gateway	yID": "54D0B4FFFE3AB6CE",				
			"lastSee	enAt": "2021-11-18 15:34:02",				
			"isOnlin	ne": true,				
			"longitu	ıde": 118.03394,				
			"latitud	de": 24.48405				
			}],					
			"applications":	[{				
			"applica	"applicationID": 1,				
			"name":	"Smoke Detector",				
			"devicel	Num": 10,				
			"activat	tNum": 7,				
			"isAuto	Join": false				
			}]					
			}					
				Description	Туре			
			gateways	Array of Gateway Information				
			- gatewayID	Gateway Unique Identifier	string			
			- lastSeenAt	Gateway Last Uplink Time	string			
			- isOnline	Online status, true: online, false:	bool			
				offline				
			- longitude	Longitude	float64			
			- latitude	Latitude	float64			
			applications	Application information array				
			- applicationID	Application ID	int			
			- name	Application Name	string			
			- deviceNum	Total number of devices under this	int			
				application				
			- activatNum	Number of devices that are already	int			
				activated (joined)				
			- isAutoJoin	Whether this application allows	bool			
				automatic device provisioning				



4.1.4.4 HTTP Push Data Format

HTTP is configured for each application, configuration path: LoRa Network Server
 -> Applications -> View (corresponding to the APP) -> Interface Management.

The data content for HTTP push is in JSON format, and its content is consistent with the JSON content for MQTT and TCP methods (please refer to the previous two sections).

✤ When a JavaScript function is configured for parsing, the JSON data will no longer use the default data format; instead, it will use the transformed data format.

• The HTTP method only supports data pushing and does not support downstream data.

4.1.4.5 JavaScript Function Transformation Method

The purpose of the function transformation method

■ The function transformation method allows for converting hexadecimal or string data reported by devices during uplink transmission into corresponding JSON format field data. This enables seamless integration with specific platforms without requiring customizations.

■ When sending downlink data, the function converts the JSON data sent by the client platform into corresponding hexadecimal data, which is then transmitted to the device.

When this conversion function is not configured, the default data format is used.

The gateway supports function conversion for both uplink and downlink data, and by default, both are in a disabled state.

1. Uplink Data Transformation

✤ When the device reports data as hexadecimal values like "ff 19 08 32 53", you can transform it into the following JSON format:

{"devEui":"ff000000000001","items":[{"label":"temperature","value":25.8},{"label":"hum idity","value":50}]} (where ff is the protocol fixed header, 19 is the temperature integer part, 08 is the temperature decimal part, 32 is the humidity value, and 53 is the checksum). Once this transformation is successfully configured, the JSON-format data received by the client will be as described.

❖ Configuration Path: LoRa Network Server → Interface → Data Transformation
 → Upstream Data Format



Uplink data format

vaScript function	Ana	alog input data
function Decode(bytes,devEui) { var data = { devEui: devEui, items: []};		19 08 32 53 evEui Simulation value:
// bytes check & bytes length check & header check.		000000000001, 10 1660 10 111 11
if (bytes === undefined bytes.length !== 5 bytes[0] !==		
Oxff) {		
data.errMsg = 'basic check failed';		↓ Conver
return data;		
1	An	eteb turtu pole
1		alog output data
// check sum.		'devEui":"ff00000000000001","item
// check sum. if ((bytes[0] + bytes[1] + bytes[2] + bytes[3]) % 255 !==		'devEui":"ff000000000000001","item
// check sum. if ((bytes[0] + bytes[1] + bytes[2] + bytes[3]) % 255 !== bytes[4]) {	S E	'devEui":"ff00000000000001","item ": "fabel":"temperature","value":25.8},
// check sum. if ((bytes[0] + bytes[1] + bytes[2] + bytes[3]) % 255 I== bytes[4]) { data.emMsg = 'check sum failed';		"devEui":"ff000000000000001","item ": "label":"temperature","value":25.8}, "label":"humidity","value":50}]]

2. Downlink Data Transformation

When the device sends data {"devEui": "ff000000000001", "cmdCode": 1,
 "heartbeatCycle": 60} and applies a function transformation ---(function transformation)--->
 01 3c (01-command code for heartbeat cycle configuration, 3c-heartbeat cycle value), it will be transformed into 013c and sent to the terminal.

♦ Configuration Path: LoRa Network Server → Interfaces → Data Transformation
 → Downlink Data Format

Downlink data format

avaScript function	Analog input data
function Encode(obj) { var bytes = []; bytes[0] = 10; // port bytes[1] = 0; // 0-unconfirmed, 1-confirmed	{"devEui": "ff0000000000001", "cmdCode": 1, "heartbeatCycle": 60}
<pre>// bytes 2~9 = devEui. for (var i = 0; i < obj.devEui.length; i+=2) { bytes.push(parseInt(obj.devEui.substr(i, 2), 16)); }</pre>	↓ Conver
<pre>// bytes 10~n Send to device content. bytes[10] = obj.cmdCode; bytes[11] = obj.heartbeatCycle; return bytes;</pre>	01 3c
}	1

4.1.5 Common Platform Integration

4.1.5.1 Four-Faith Cloud NS

The standard network server (NS) used by Four-Faith Cloud adopts the Semtech



UDP GWMP Protocol.

- In this mode, the gateway implements the data forwarding function.
- ♦ Configuration Path: LoRa Gateway → Basic Settings, Main configurations

include protocol selection, server address, and server port (UDP). The specific settings are as follows:

	and Set Beacon Set	Packet Filter	
		* Gateway MAC	54D0B4FFFE9B006C
		Protocol	Semtech UDP GWMP Protocol
		Server Address	47,90,209.17
		Server Port(UDP)	27915
		Server Timeout(ms)	100
	P	Keepalive Interval (s)	10
		Internal UDP Port	1699
			Save & Modify
 Open C Create 	CSTool: <u>http://47.</u>	90.209.17:518	68/#/ns/gateways
 Open C Create Add Gateway * GwID 	CSTool: <u>http://47.</u> Gateway eg: 0102030405060	90.209.17:518 9708	68/#/ns/gateways
 Open C Create Add Gateway * GwID * Name 	CSTool: <u>http://47.</u> Gateway eg: 0102030405060 eg: gateway_1	90.209.17:518 0708	68/#/ns/gateways

• Viewing Gateway Status: As shown in the following image, it is evident that the gateway is currently online.

Keyword	Q Search + Ad	d Gateway				
GwiD	Name	Description	Is Online	First Up Time	Last Up Time	Operate
54d0b4fffe36d12c	54D0B4FFFE36D12C	54D0B4FFFE36D12C	false	2023-07-31 16:19:49	2023-07-31 16:39:19	© View 🗈 Delete

4.1.5.2 ChirpStack Platform (GWMP)

ChirpStack is a versatile open-source Network Server (NS) that supports multiple connectivity methods. One of the commonly used methods for integration is through the GWMP (Gateway Management Protocol) protocol.

♦ Configuration Path: LoRa Gateway → Basic Settings, Main Configuration

Protocol, Server Address, Server Port(UDP), Specific configurations are as follows:

Four-Faith User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
* Gateway MAC	54D0B4FF	FE9B0	06C				
Protocol	Semtech U	JDP GV	VMP Protocol		~		
Server Address	47.90.209	.17					
Server Port(UDP)	27 <mark>91</mark> 5						
Server Timeout(ms)	100						
Keepalive Interval (s)	10						
Internal UDP Port	1699						
	0	Save &	Modify				

4.1.5.3 ChirpStack Platform (LNS)

ChirpStack can be configured to use the Basicstation protocol for integration. This mode of integration is generally referred to as LNS (LoRa Network Server). It supports two modes: No Authentication and TLS Server Authentication. The following examples illustrate the configuration for both modes of integration.

1. LNS - No Authentication

• By configuring the protocol, server protocol type, URI, port, and mode selection, you can make the necessary changes. Once these modifications are successfully applied, the configuration will be updated.

* Gateway MAC	54D0B4FFFE9B006C		
Protocol	Basics Station	~	
Server	LNS Server	\sim	
URI	wss://A39Q4NHH5TTZ8X.Ins.lorawan.us-east-1.a	mazonaws.com	
Port	443		
Authentication Mode	No Authentication		~
	Save & Modify		

✤ The "Last seen at" on the platform indicates the gateway's connection status.

Four-Faith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
Gateways / FF000	000000	00000a						
GATEWAY DETAILS	GATEWA	Y CONFIGU	IRATION	CERTIFIC/	ATE	GATEWAY D	ISCOVERY	
Gateway detai	ls							
Gateway ID				ff000000000000	10a			
Altitude				0 meters				
GPS coordinates				0, 0				
Last seen at				Apr 21, 2022 5:1	3 PM			

2. LNS - TLS Server Authentication

✤ When configuring the gateway, the URI should match the corresponding domain name of the server, and the "trust" content is derived from the server's .pem file content.

* Gateway MAC	54D0B4FFFE9B006C	
Protocol	Basics Station V	
Server	LNS Server	
URI	wss://A39Q4NHH5TTZ8X.lns.lorawan.us-east-1.amazonaws.com	
Port	443	
Authentication Mode	TLS Server Authentication	
trust	BEGIN CERTIFICATE MIIEdTCCA12gAwlBAgIJAKcOSkw0grd/MA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNV BAYTAIVTMSUwlwYDVQQKExxTdGFyZmllbGQgVGVjaG5vbG9naWVzLCBJbmMuMTlw MAYDVQQLEyITdGFyZmllbGQgQ2xhc3MgMiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0 eTAeFw0wOTA5MDIwMDAwMDBaFw0zNDA2MjgxNzM5MTZaMIGYMQswCQYDVQQGEwJV	* *
	Save & Modify	

✤ The "Last seen at" on the platform indicates the gateway's connection status.

Four-Faith	User	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	Gateway
Gateways / FF0000	00000000000a							
GATEWAY DETAILS	GATEWAY CONFIGURATIO	ON CEP	RTIFICATE	GATEWAY DISCO	VERY			
2								
Catoway dotail	c							
Galeway detail	5							
Gateway ID		ff000000	000000a					
Altitude		0 meters						
GPS coordinates		0, 0						
		-		_				
Last seen at		Apr 21, 20	22 5:14 PM	Λ				

4.1.5.4 AWS Platform (LNS)

✤ Create a gateway on the AWS platform.

dd gateway Info	
Gateway details Info	
Gateway's EUI	
54D0B4FFFE9B006C	
Enter the 16-digit alphanumeric EUI code found on your gateway.	
Frequency band (RFRegion)	
EU868	
Choose the LoRa specific frequency band (RFRegion) used where the gateway is deployed. Name - optional	
54D0B4FFFE9B006C	
Give your gateway a descriptive name to make it easier to locate. Description - <i>optional</i>	
aws_test	
Enter a description of the gateway.	

• Download the corresponding keys generated by the gateway and configure the corresponding parameters for the gateway. Choose the mode "TLS Server and Client Authentication." In the following image, boxes with the same color represent matching content.

	0301	Manua I	for	F8926-GW-02	Series	LoRaWAN	Indoor	G
Gateway certifica	ite							
Create a certificate so that	your gateway can co	mmunicate sec	curely with	AWS IoT. Download th	e certificate fil	les so that you ca	n upload	
them to your gateway.								
	O Certificate	e created and	1 associat	ted with your gatew	av			
Create certificate	0			j j				
These certificate files	were created. Dov	wnload them	n and sav	ve them to upload t	o your gate	way.		
Colores (Process)	11 -				4622 02			
Gateway certificate n	ne			90008100-0050	-4622-9200-	046006551410	o.cert.pem	
Private key file				96bb8f00-db5c-4	622-92ee-b4	4600653f41b.p	orivate.key	
N Download certi	ificate files							
E boundad cert	incare mes							
Provisioning cross	lentials							
Choose the endpoint that	your gateway support	ts. Then, copy f	the endpo	int and download the s	erver trust cer	tificate so that yo	u can add	
them to your gateway.								
	nd Hedata Casual	radaalat						
https://A3904	NHHSTTZ8X.cups.	endpoint lorawan.us-	-past-1.	amazonaws.com:44	13	- Ta Co	av.	
	d. C					L co	<i>,</i> ,,	
LNS (LORAWAN Netwo	INCETT28X 105 10	t mawan us-a	ast-1 a	53700 aus com 662		5		
1001111000	110112001210120	n anan . us - e	036-110	1020100310001 445		Dr col	<i>y</i>	
Download your server	trust certificate so er trust certificat	you can uple	oad the o	ertificate for the er	dpoint your	gateway suppo	orts.	
Download your server	trust certificate so er trust certificat 54D0B4FFFE9B0	you can uple	oad the o	ertificate for the er ins.trust	dpoint your	gateway suppo	orts.	
Download your server	trust certificate so er trust certificat 54D0B4FFFE9B0	you can uple	oad the o	ertificate for the er ins.trust	dpoint your	gateway suppo	orts.	
Download your server Download serv * Gateway MAC Protocol	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station	you can uplo	oad the o	ertificate for the er ins.trust	dpoint your	gateway suppo	orts.	
Download your server Download server Gateway MAC Protocol Server	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server	you can uple es	oad the o	ertificate for the er ins.trust v	dpoint your	gateway suppo	orts.	
Download your server Download server * Gateway MAC Protocol Server	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server	you can uple es	oad the c	ertificate for the er ins.trust	dpoint your	gateway suppo	orts.	
Download your server Download server Gateway MAC Protocol Server URI	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF	you can uple es 006C	oad the c	ertificate for the er ins.trust ~ ~ -east-1.amazonaws.co	dpoint your	gateway suppo	orts.	
Download your server Download server * Gateway MAC Protocol Server URI Port	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH	you can uple es 006C H5TTZ8X.Ins.Ic	oad the o	ertificate for the er ins.trust ~ ~	dpoint your	gateway suppo	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF 443 TLS Server and 0	you can uple es 0006C 15TTZ8X.Ins.k	orawan.us	ertificate for the er ins.trust ~ -east-1.amazonaws.co	dpoint your	gateway suppo	orts.	
Download your server Download server * Gateway MAC Protocol Server URI Port Authentication Mode	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF 443 TLS Server and 0	you can uple es 006C H5TTZ8X.Ins.Ic	oad the o	ertificate for the er ins.trust ~ -east-1.amazonaws.co	om	gateway suppo	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT	you can uple es 006C 15TTZ8X.Ins.kc Client Authenti	orawan.us	ertificate for the er ins.trust ~ -east-1.amazonaws.co	m	gateway suppo	orts.	
Download your server Download server * Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF 443 TLS Server and C BEGIN CERT MILEdTCCA12gA BAYTAIVTMSUW	you can uple es 006C 15TTZ8X.Ins.k Client Authenti ITFICATE WIBAgIJAKCC IWYDVQQKES	cation	ertificate for the er ins.trust ~ -east-1.amazonaws.co MA0GCSqGSIb3DQE mIIbGQgVGVjaG5vbc	bm BCwUAMGgx S9naWVzLCB.	gateway suppo gateway suppo czajBgNV JomMuMTIw	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificate 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT MILEdTCCA129A BAYTAI/TASUM MAYDVQQLEyIT eTAEFw0w0TA5	you can uple es 0006C H5TTZ8X.Ins.Ic Client Authentia TIFICATE WIBAGJJAKCD IWYDVQQKED MDIWMDAWM	cation Cation	ertificate for the er ins.trust	BCwUAMGgx S9naWVzLCB F0aW9uIEF10 MIGYMGswC	gateway suppo gateway suppo CzAJBgNV JbmMuMTIw dGhvcmI0 QYDVQQGEwJN	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF 443 TLS Server and O BEGIN CERT MILEdTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAEFw0w0TA5	you can uple es 006C 15TTZ8X.Ins.Ic Client Authenti TIFICATE wkBAgIJAKcC IWYDVQQKE idGFyZmIIbGC MDIWMDAwM	cation Skw0grd/ xxTdGFyZ gQ2xhc3 DBaFw0z	ertificate for the er ins.trust -east-1.amazonaws.cr MA0GCSqGSIb3DQE (mIIbGQgVGVjaG5vbC MgMiBDZXJ0aWZPY2 NDA2MjgxN2M5MT22	BCwUAMGgx BCwUAMGgx SanaWvzLCB. F0aW9uIEF10 MIGYMQswC	gateway suppo gateway suppo CzAJBgNV JomMuMTIw dGhvcmI0 QYDVQQGEwJN	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT MILEdTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAeFw0w0TA5	you can uple es 006C 45TTZ8X.Ins.Ic Client Authenti TIFICATE WIBAgIJAKcC MDIWMDAWM TIFICATE	cation Skw0grd/	ertificate for the er ins.trust	BCwUAMGgx BBCwUAMGgx 90naWVzLCB, 2F0aW9uIEF10 MIGYMQswC	gateway suppo gateway suppo czAJBgNV ////////////////////////////////////	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificate 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT MIEdTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAEFW0WOTA55 BEGIN CERT MIDWTCCAKGg BQAWTTFLMEK0	you can uple es 006C 45TTZ8X.Ins.lc Client Authenti TIFICATE WMBAGJAKCC MWBAGJAKCC MUYDVQQKEs 1GGFyZmIBGG MDIWMDAWM	oad the contraction orawan.us cation oxtdGFy2 QQ2xhc3 DBaFw0z SWNYHp7E 2W1hem9	ertificate for the er ins.trust	BCwUAMGgxi BCwUAMGgxi SanaWvzLCB. F0aW9uEF10 MIGYMQswC DQYJKoZINvc (BPPUFtYXpv	gateway suppo gateway suppo CzAJBgNV JomMuMTIw dGhvcmI0 QYDVQQGEwJV	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust certificate	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHF 443 TLS Server and O BEGIN CERT MILEdTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAEFW0WOTA5 BEGIN CERT MILDWTCCAKGg BQAWTTFLMEKG SW5JLIBMPVNIY QFoXDTO5MTI-	you can uple es 006C 15TTZ8X.Ins.Ic Client Authenti TIFICATE WMBAgIJAKCC MDIWMDAWM TIFICATE YaWIBAgIUHC3 GATUECWXC0 XR0bGUgUTC XR0bGUgUTC	oad the contraction	ertificate for the er ins.trust -east-1.amazonaws.cr MA0GCSqGSIb3DQE milbGQgVGVjaG5vbC MgMiBDZXJ0aWZpY3 NDA2MjgxN2M5MT22 G0Yy/rVHHAT1jj8q14w ulFdIyJ3RvbiBDPVVTME GJuZ3RvbiBDPVVTME GJuZ3RvbiBDPVVTME	bm BCwUAMGgxi SanaWvzLCB, POaW9uIEF1 MIGYMQswC DQYJKoZIhvo (BPPUFYXpv 4XDTIyMDUXi	gateway suppo gateway suppo CzAJBgNV JomMuMTIw dGhvcmI0 QYDVQQGEwJV iNAQEL bi5jb20g MjA0NDk0 jaWZpV2F0	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust	trust certificate so er trust certificate 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT MILEdTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAeFw0w0TA5 BEGIN CERT MILDWTCCAkGg BQAwTTFLMEkK SW5jLIBMPVNIY OFoXDTQ5MTIZ	you can uple es 006C H5TTZ8X.Ins.Ic Client Authenti TIFICATE WIBAgIJAKCC WYDVQQKED 'dGFyZmIIbGG MDIWHDAWM MDIWHDAWM MDIWHDAWM MDIWHDAWM MDIWHDAWM MDIWHDAWM MDIWHDAWM MDIWHDAWM	cation cation Skw0grd/	ertificate for the er ins.trust	BCwUAMGgxi BCwUAMGgxi BCwUAMGgxi BDaVVzLCB, 2F0aW9uIET10 MIGYMQswC DQYJKoZIhvc /8PPUFtYXpv 4XDTIyMDUXI EIVVCBDZXJ0	gateway suppo gateway suppo CzAJBgNV DomMuMTIw dGhvcmI0 QYDVQQGEwJV dGhvcmI0 QYDVQQGEwJV SNAQEL bi5jb20g MJAONDKO DawZpY2F0	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port tuthentication Mode trust certificate key	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server wss://A39Q4NHH 443 TLS Server and 0 BEGIN CERT MILEdTCCA12gA BAYTAI/TIMSUW MAYDVQQLEyIT eTAeFw0w0TA50 BEGIN CERT MIDWTCCAKGg BQAWTTFLMEK0 SW5JLIBMPVNIY OFoXDTQ5MTIZ	you can uple es 006C 15TTZ8X.Ins.lc Client Authenti TIFICATE WIBAGIJAKCC MWBAGIJAKCC MUYDVQQKEy 'dGFyZmIBGG MDIwMDAWM TIFICATE AWIBAGIUHC3 GA1UECwxCC XR0bGUgU10 MTIzNTK10VC	orawan.us cation DSkw0grd/ xxTdGFy2 gQ2xhc3 DBaFw0z DBaFw0z DW1hem9 Q9V2FzaC DW1hem9 Q9V2FzaC	ertificate for the er ins.trust -east-1.amazonaws.co MA0GCSqGSIb3DQE mIbGQgVGVjaG5vbC MgMiBDZXJ0aWZpY2 NDA2MjgxNzM5MTZa 30Yy/rvHHAT1jj8q14w ulFdIYIBTZXJ2aWNIc SluZ3RvbIBDPVVTMB 30GA1UEAwwTQVdT	bm BCwUAMGgxi S9naWvzLCB, F0aW9uIEF11 MIGYMQswC DQYJKoZIhvo /BPPUFtYXpv 4XDTIJMDUxI EIvVCBDZXJ0	gateway suppo gateway suppo CzAJBgNV JomMuMTIw dGhvcmI0 QYDVQQGEwJV SNAQEL bi5jb20g MjA0NDk0 JoaWZpY2F0	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port tuthentication Mode trust certificate key	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server WSS://A39Q4NHF 443 TLS Server and O BEGIN CERT MILEDTCCA129A BAYTAIVTMSUW MAYDVQQLEyIT eTAEFW0W0TA5 BEGIN CERT MILDWTCCAKG BQAWTTFLMEKC SW5JLIBMPVNIY OFoXDTQ5MT2 BEGIN RSAT MILEOWIBAAKCA nMmBISTOI42FF	you can uple es 006C 15TTZ8X.Ins.Ic 15TTZ8X.Ins.Ic Client Authenti TIFICATE	orawan.us cation Diskw0grd/ xxTdGFyZ DgQ2xhc3 DBaFw0z DyV1FpCN DgV2FzaC DwHjECNB DyV2FzaC DwHjECNB	ertificate for the er ins.trust	bm BCwUAMGgxi SinaWVzLCB, POAVSUEF11 MIGYMQswC DQYJKoZIhvo (BPPUFYXpv 4XDTIyMDUxI EIVVCBDZXJC COPPUFYXpv AXDTIYMDUxI EIVVCBDZXJC	gateway suppo gateway suppo CzAJBgNV JomMuMTIw dGhvcmI0 QYDVQQGEwJV GhvcmI0 QYDVQQGEwJV iXAQEL bi5jb20g MjA0NDk0 JawZpY2F0	orts.	
Download your server Download server Gateway MAC Protocol Server URI Port Authentication Mode trust certificate key	trust certificate so er trust certificat 54D0B4FFFE9B0 Basics Station LNS Server WSS://A39Q4NHH 443 TLS Server and O BEGIN CERT MILEDTCCA12gA BAYTAIVTMSUW MAYDVQQLEyIT eTAEFW0WOTA51 BEGIN CERT MIIDWTCCAKGg BQAWTTFLMEKO SW5JLIBMPVNIY OFOXDTQ5MTIZ	you can uple es 006C 15TTZ8X.Ins.Ic Client Authenti TIFICATE	cation cation	ertificate for the er ins.trust -east-1.amazonaws.co -east-1.amazonaws.co MA0GCSqGSIb3DQE milbCQgVGVjaCSvbC MgMiBDZXJ0aWZpY2 NDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 30YY/rVHHAT1jj8q14w ulFdIYIBTZXJ2aWNic SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MJgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MJgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ2 SuDA2MjgxNzM5MTZ	bm BCwUAMGgx BCwUAMGgx BDaWyzLCB, SP0aW9uIET10 MIGYMQswC BPPUFYXpv 4XDTIyMDUXI EIVVCBDZXJC BPPUFYXpv 4XDTIyMDUXI EIVVCBDZXJC CDQYJKOZINvc 4XDTIYMDUXI EIVVCBDZXJC CDQYJKOZINvc 4XDTIYMDUXI EIVVCBDZXJC CDQYJKOZINvc 4XDTIYMDUXI EIVVCBDZXJC	gateway suppo gateway suppo CzAJBgNV ////////////////////////////////////		· · · · · · · · · · · · · · · · · · ·



Continuing Gateway Creation:

Connect to your gateway's local network	Enter your gateway and server trust certificates	Enter the endpoint into your gateway's user interface
Using the getting started guide from your gateway's vendor, connect to your gateway directly using its Ethernet port, or its local Wi-Fi.	If you created a certificate for your gateway earlier, upload it by using the gateway's user interface. If your vendor provided a certificate with your gateway, you can skip this step.	Copy your endpoint to your gateway to direct messages from your gateway to your console.

After successful configuration, you can observe the gateway's connection status on the AWS platform.

6bb8t00-db5c-4622-92ee-b46	00653f41b info		Edit Dele
Details			
Gateway ID 96bb8f00-db5c-4622-92ee-b4600653f41b Associated thing name 1e2fef23-5b33-4b4b-9177-665a208a2556 LORAWAN details Position Tags	Name 540084FFFE98006C Description aws_test	Firmware -	
LoRaWAN specific details			
LoRaWAN specific details	LastUplinkReceivedAt	NetIdFilters	
LoRaWAN specific details GatewayEUI 54d0b4fffe9b006c	LastUplinkReceivedAt August 21, 2023, 15:07:38 (UTC+08:00)	Net/Filters -	
LoRaWAN specific details GatewayEUI 54d0b4fffe9b006c RFRegion	LastUplinkReceivedAt August 21, 2023, 15:07:38 (UTC+08:00) Connection status	NetJdFilters - JoinEulFilters	
LoRaWAN specific details GatewayEUI 54d0b4fffe9b006c RFRegion EU868	LastUplinkReceivedAt August 21, 2023, 15:07:38 (UTC+08:00) Connection status Connected	NetldFilters - JoinEulFilters -	

4.1.5.5 AWS Platform (CPUS)

• Create a gateway on the AWS platform.


Add gateway Info

Sateway's EUI 54D0B4FFFE9B006C inter the 16-digit alphanumeric EUI code found on your gateway.
54D0B4FFFE9B006C
nter the 16-digit alphanumeric EUI code found on your gateway.
requency band (RFRegion)
EU868
hoose the LoRa specific frequency band (RFRegion) used where the gateway is deployed. Name - <i>optional</i>
54D0B4FFFE9B006C
ive your gateway a descriptive name to make it easier to locate. Description – <i>optional</i>
aws_test
inter a description of the external

• Download the corresponding keys generated by the gateway, and configure the corresponding parameters of the gateway. Select the TLS Server and Client Authentication mode. In the diagram below, boxes with the same color indicate the same content.

Gateway certificate Create a certificate so that your gateway can commun them to your gateway.	nicate securely with AWS IoT. Download the certificate	files so that you can upload
Create certificate	ated and associated with your gateway	
These certificate files were created. Downloa	ad them and save them to upload to your ga	teway.
Gateway certificate file	96bb8f00-db5c-4622-92e	e-b4600653f41b.cert.pem
Private key file	96bb8f00-db5c-4622-92ee-	b4600653f41b.private.key
Download certificate files		
Choose the endpoint that your gateway supports. The them to your gateway.	en, copy the endpoint and download the server trust o	ertificate so that you can add
https://A39Q4NHH5TTZ8X.cups.lora	wan.us-east-1.amazonaws.com:443	🗗 Сору
LNS (LoRaWAN Network Server) endpoint	n.us-east-1.amazonaws.com 443	🗇 Сору
Server trust certificates	ran unload the contificate for the order inter-	

aiui							
* Gateway MAC	54D0B4FFFE9B00	06C					
Protocol	Basics Station			~			
Server	CUPS Server			~			
URI	wss://A39Q4NHH	5TTZ8X.Ins.lorav	/an.us-east-1	l.amazonaws.com			
Port	443				88 s		
uthentication Mode	TLS Server and C	lient Authenticati	on		~		
trust	BEGIN CERTI MIIEdTCCA12gAv BAYTAIVTMSUWI MAYDVQQLEyITd eTAeFw0wOTA5M	FICATE VIBAGIJAKCOSKV WYDVQQKExxTo IGFyZmIIbGQgQ IDIWMDAWMDB2	v0grd/MA0G IGFyZmIIbG(2xhc3MgMiE IFw0zNDA2I	CSqGSlb3DQEB(QgVGVjaG5vbG9 3DZXJ0aWZpY2F MjgxNzM5MTZaM	CwUAMGgxCz/ naWVzLCBJbn DaW9uIEF1dGI IGYMQswCQY	AJBgNV nMuMTIw hvcmI0 ′DVQQGEwJV	* * //
certificate	BEGIN CERTI MIIDWJCCAKKGAW CwUAME0XSZBJE IEIuYy4gTD1TZW NDRaFw00OTEyN	FICATE vIBAgIVAKKihOu 3gNVBAsMQkFt F0dGxIIFNUPVd 4zEyMzU5NTIaN	eTBUwAvPi /XpvbiBXZW hc2hpbmd0l 1B4xHDAaBe	zPXVvu+Eiw56M /lgU2VydmljZXMg p24gQz1VUzAeFv gNVBAMME0FXU	A0GCSqGSlb3 Tz1BbWF6b24 v0yMzA4MjEw1 yBJb1QgQ2Vy	DQEB JuY29t NjU3 rdGimaWNh	•
key	BEGIN RSA P MIIEowIBAAKCAC xrR7gyJXqPeWIKY KTnuG6dHErB/6V jq0kXEYe3s7mWw	RIVATE KEY QEAnyJis5PZnyl- (4BMs2RDFZj73) VzNXFiQgeaFmji vQ+oNMbHuBjL	+VdqpGTZO 70j5MXINfBi uiTYeBOKBE ′aPYhR9hB\	QrWdkOxJ+LldL6 BqREk2mwByjlyt\ 3Btt0wfpqURh94v /KRmC7HhuKPny	jpXBvzcwnX0fr /H6ywcyHv73S n1lofJiDSjLA+y XLE2eEAOYm	r4 85 1N4m55+i	* //
	Save &	Modify					
 Continu 	ing the gates	way creati	on:				
Connect your	gateway Info						

Connect to your gateway's Enter your gateway and server trust certificates Using the getting started guide from If you created a certificate for your your gateway's vendor, connect to

gateway earlier, upload it by using the gateway's user interface. If your vendor provided a certificate with your gateway, you can skip this step. Enter the endpoint into your gateway's user interface

)0-

Copy your endpoint to your gateway to direct messages from your gateway to your console.

Ifter you add the gateway, it can take a while for it to complete its configuration. To view your gateways, open the Gateway page. You can also add more devices while you wait for your gateway.

* After successfully configuring the gateway, you can view the gateway's connection

status on the AWS platform.

your gateway directly using its

Ethernet port, or its local Wi-Fi.

local network

74

×

	llser	Manual	for	F8926-GW-02	Series	l oRaWAN	Indoor	Gateway
Faith	0301	Mariaar	101	10/20 01 02	001103	Lonannin	maoor	dacoway
96bb8f00-db5c-46	22-92ee-b4600	653f41b 🖬	0					Edit Del
Details								
Gateway ID	CE7641L	Name	FFF0B006C			Firmware		
96008100-005C-4622-9288-046000	5551410	540084	FFE5B006C			-		
Associated thing name 1e2fef23-5b33-4b4b-9177-665a20	08a2556	Descripti aws_test	on					
LoRaWAN details Position	Tags							
GatewayEUI		LastUpli	nkReceivedAt			NetIdFilters		
54d0b4fffe9b006c		August 2	1, 2023, 15:0	7:38 (UTC+08:00)		-		
RFRegion		Connect	ion status			JoinEuiFilters		
EU868		Connect	ed			-		
						CubDondo		

4.1.5.6 TTN Platform (GWMP)

- ✤ The TTN platform supports GWMP and Basicstation modes of access.
- ↔ When using the GWMP protocol, it is consistent with other platforms. You only

need to configure the server IP and port.

Protocol	Semtech UDP GWMP Protocol	~
Server Address	eu1.cloud.thethings.network	-
Server Port(UDP)	1700	
Server Timeout(ms)	100	
Keepalive Interval (s)	10	
Internal UDP Port	1699	

• The server address and port can be obtained from the "global_conf.json" file which can be downloaded from the TTN platform.

gw_000a	00000a		
• Other cluster ⊘			
General information			
Gateway ID	ff0000000000000		
Gateway EUI	FF 00 00 00 00 00 00 0A	<>	
Gateway description	test gateway		
Created at	Apr 22, 2022 09:49:59		
Last updated at	Apr 22, 2022 09:49:59		
Gateway Server address	eu1.cloud.thethings.netwo	rk	•
LoRaWAN information			

 \clubsuit The server address and port can be found at the end of the file.



After successfully configuring the gateway, you can see the connection information on the TTN platform.

Four-F	¶ [®] aith	User	Manua I	for	F8926	-GW-02	Series	LoRaWAN	Indoor	Gateway
	gw_000a ID: ff00000000000 Other cluster ③)a							🗮 1 Col	llaborator 🛛 🗸 1 API key
	General information					• Live data				See all activity →
	Gateway ID	ff0000000000000				10:44:	39 Disconnect	gateway Connect	tion expired	
	Gateway EUI	FF 00 00 00 00 00 00	0 QA		↔ 🖺	✤ 10:40:	50 Receive ga	teway status Mei	trics: { ackr:	0, rxfw: 0, rxin: 0,
	Gateway description	test gateway				L				
	Created at	Apr 22, 2022 09:49:59								
	Last updated at	Apr 22, 2022 09:49:59								

4.1.5.7 TTN Platform (LNS)

• The TTN platform also supports connection using the Basicstation LNS protocol, with the mode being TLS Server Authentication and Client Token.

✤ Add Gateway

Add	gateway
-----	---------

General settings

Owner*	
sugk	~
Gateway ID 💮 *	
ff000000000000a	
Gateway EUI 🗇	
FF 00 00 00 00 00 00 0A	
Gateway name	
gw_000a	
Gateway description ⑦	
test gateway	
Optional gateway description; can also be used to save not	es about the gate
Gateway Server address	
eu1.cloud.thethings.network	

The address of the Gateway Server to connect to



Require authenticated connection ⑦

Enabled

Controls whether this gateway may only connect if it uses an authenticated Basic Station or MQTT connection

Gateway status ⑦

🗹 Make status public

The status of this gateway may be visible to other users

Gateway location ⑦

✓ Make location public

When set to public, the gateway location may be visible to other users of the network

Attributes 🕐

+ Add attributes

Attributes can be used to set arbitrary information about the entity, to be used by scripts, or simply for your own organization

LoRaWAN options

Frequency plan ⑦*

Europe 863-870 MHz (SF12 for RX2)	
-----------------------------------	--

Schedule downlink late ⑦

Enabled

Enable server-side buffer of downlink messages

Enforce duty cycle ⑦



Recommended for all gateways in order to respect spectrum regulations

Schedule any time delay ⑦*

530	milliseconds	\sim	

Configure gateway delay (minimum: 130ms, default: 530ms)

Obtaining the Token Value



✤ Adding API key



• Follow the diagram below, and create an API key.

Add API key

ights* Grant all Grant in Grant in Select al Delete	l current and future rights dividual rights Il e gateway				
Grant all Grant in Select al	l current and future rights dividual rights Il e gateway				
Grant in Select al	dividual rights Il e gateway				
Select al	ll e gateway				
Delete	e gateway				
View					
	gateway information				
🔽 Link a	is Gateway to a Gateway Se	erver for traffic exc	change, i.e. write uplin	ık and read downlink	
View	gateway location				
Retrie	eve secrets associated with	a gateway			
View a	and edit gateway API keys				
Edit b	asic gateway settings				
View a	and edit gateway collabora	itors			
View	gateway status				
Write	downlink gateway traffic				
Read	gateway traffic				
Store	secrets for a gateway				

协议	Basics Station	Please copy newly	created API key
Server	LNS Server	You won't be able to view the key aft	erward
URI	eul.cloud.thethings.network	rigi	
Port	8887	Granted rights	Your API key has been created
uthentication Mode	TLS Server Authentication and Client Token $\qquad \lor$	Y ✓ Link as Gateway to a infi Gateway Server for traffic	successfully. Note: After closing this window, the value of the key secret will not be accessible anymore.
trust	BEGIN CERTIFICATE MIIIsacCA10gAwiBAgiRAIQ27DSQONZRGPgu2OGiwAwDQYIKoZIfiveNAQELBQAw TELMAKGAUBEMMCVIVAKITAnBqNVBAoTEludGVybmV0FNII23VyaXR5FI/L2Vh	exchange, i.e. write uplink and read downlink	Make sure to copy and store it in a safe place now.
	cmNoIEdyb3VwMRUwEwYDVQQDEwxJUIJHIEJvb3QgWDEwHhcNMTUwNjA0MTEwNDM4 WhcNMzUwNjA0MTEwNDM4WjBPMQswCQYDVQQGEwJVUzEpMCcGA1UEChMgSW50ZXJu	ets a	API key
token	Bearer NNSXS.ZLC3OBWR2Q4NJPEB52AQ8MJ3ZZSG47XFZF3L4MQ.PTPW5YFB57LNXDD6FGWQL2'	gat	NNSXS.ZLC30BWR 🚡 🗞
	• 保存 & 传改 token = Bearer NNSXS.ZLC30BWR	gat	
		sta	✓ I have copied the key

 Trust Explanation: This content is from the downloaded file "isrgrootx1.pem" from the TTN platform. The file download path is:

Faith					10720	-GW-02	Series		Indoor	Gatewa
https://www.	thethingsindus	stries.con	n/docs/re	eference/	root-co	ertificates/	#lets-e	ncrypt		
个网关MAC 协议 Server	ff00000000000a Basics Station LNS Server				ſ	LoRaWAN Specificati and Regio Parameter	bility on nal s	Baltimore CyberT Amazon Root CA The Things Indus Download the minima	Trust Root 1, 2, 3 and 4 stries Root CA al certificate list here.	
URI	eu1.cloud.thethings.network					Networkin	g	Let's Encryp	ot	
Port	8887					Packet Bro Routing	oker	ISDG Doot VI		
Authentication Mode	TLS Server Authentication and Cl	ient Token				Packet	0	Many The Things Sta	ck deployments use	the Let's Encrypt I
trust	BEGIN CERTIFICATE					Purging Er	tities	X1 Trust. If using Let's	s Encrypt to secure y	our domain, you m
	MIIFazCCA1OgAwIBAgIRAIIQz7D TzELMAkGA1UEBhMCVVMxKTAn	SQONZRGPgu2OCiw BgNVBAoTIEludGVyb	AwDQYJKoZIhvcNAC mV0IFNIY3VyaXR5IF	QELBQAw FJlc2Vh		Rate Limiti	ng	download the ISRG R	oot XT Trust file nere	- 二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、
	cmNoIEdyb3VwMRUwEwYDVQQ WhcNMzUwNjA0MTEwNDM4Wj	DEwxJU1JHIFJvb3Qg1 BPMQswCQYDVQQGI	WDEwHhcNMTUwNj EwJVUzEpMCcGA1U	A0MTEwNDM4 EChMgSW50ZXJu	-	Resource		← Resource Limitin	g	Tele
token	Bearer NNSXS.ZYS3SEEQSETHCO	6EXSK6HGEKDOC4W	5G6Y22XZXI.2FKB4C	26GQDF22KCNPNYWE	Xe	Root Certi	ficates			
	◎ 保存 & 修改					Telemetry			Was this article help	
						Tenant	/			
						Tenant Manageme	ent		•	
						Tenant Manageme	ent. .em ^		•	•
・RR先MAC り取な Server	JRI Configurat 100000000000 Basics Station LNS Server	ion				Tenant Managem Isrgrootk1,p Isrgrootk1,p gw_000a Its: freeseeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	ent , em ^		•	€ ±t 1 Collaborator •
・同XMAC ・同XMAC 助収 Server UR	JRI Configurat 19000000000 Basics Station LNS Server euledouditethingsnetwork	ion			51 0 0 ↑ 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Tenant Managemu Isrgroobd.‡ Byw_0000a ID: ff000000000 80 ↓0 ◆ Last activ neral Information	ent em ^		•	▲ 1 Collaborator
・同关MAC 「同关MAC 助议 Server UR UR Dort	JRI Configurat H0000000000 Basics Station LNS Server eutcloudthethings.network 8887	ion				Tenant Managemu Isrgroobil p gw_000a ID: ff000000000 80 ↓0 Last activ neral Information terray ID	ent . em ^	ffsoossossa	•	♣ 1 Collaborator
・ 岡夫MAQ ・ 岡夫MAQ 助议 Server URI Port Authentication Mode	JRI Configurat H00000000000 Basics Station LNS Server eut.cloud.thethings.network B887 TIS Server Authentication and Cli	ion ~ ·			••••••••••••••••••••••••••••••••••••••	Tenant Managemu Isrgroobil; gw_000a ID: frococococo 80 0 • Last activ neral information teway ID neral settings	ent. em ^	f1000000000000000000000000000000000000	•	₩ 1 Collaborator d
・ 陽光Mac ・ 陽光Mac 助政 Server URI Port Authentication Mode trust	JRI Configurat F00000000000 Basics Station LVS Server eut Lobud thethingsnetwork BB87 TLS Server Authentication and Clin BEGIN CERTIFICATE	ion v				Tenant Managemu isrgrootx1.p gw_000a ID: frococococo 80 \u0 elast activ neral information tervay ID neral settings tervay description	ent. em ^	ff900000000000000000000000000000000000	•	x 1 Collaborator
خ الالجيمية المحافظة محافظة محافظة محافظة محافظة المحافظة المحافظة محافظة محافظة محاف المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة المحافظة محافظة محاف محافظة محافظة محافظة محافظة محافظة محافظة المحافظة محافظة محافية محافظة محافظة محافظة محافظة محافي محافظة محافي محافظة محافظة محافظة محافظة محافظة محافظة محافظة محافظة م	JRI Configurat 10000000000 Basis Station LVS Server euLedoudthethingsnetwork 5827 TLS Server Authentication and Cli 	ion	2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	LBQAw 22/h		Tenant Managemu isrgrootx1.p gw_000a ID: fr00000000 80 \0 \colored last activ neral information teway ID neral settings teway description teway description teated at	ent iem ^	ff000000000000 Ff 00 50 00 00 00 00 Ff 00 50 00 00 00 00 test gateway Apr 22, 2020 (40:59	•	▲ 1 Collaborator d
الالتحديث العالم المحديث المحدي المحديث المحديث الم محديث المحديث المح محديث المحديث ال مدامث المحديث المحديث المحديث المحديث المحديث المحديث الم	JRI Configurat 100000000000 Basics Station LVS Server eut_doudthethings.network 5827 TLS Server Authentication and Cli BEGIN CERTIFICATE RHIB-colorDig-National-007020 	tion	wCQVIAc2TinetAQB DeatherthougAption	LBQAw 22/h MTEwNDM4 MM5QV5022/Ju		Tenant Managemu isrgrootx1; gw_000a D:: fr000000000 80 ↓ 0 • tr000000000 teway t0 neral settings teway description tated at ti updated at	ent eem ^	ff00000000000 Ff 00 50 00 00 00 00 ff 00 50 00 00 00 00 fet galeway Apr 22, 2022 00:49:59 Apr 22, 2022 00:49:59	•	▲ 1 Collaborator d
・ 同关Mac ・ 同关Mac 助议 Server URI Port Authentication Mode trust	IRI Configurat 10000000000 Basis Sation LVS Server euLedoudthethingsnetwork 5827 TIS Server Authentication and Cli 	ion	MOQUIACIII-NARGE	LBQAw ZVh MTEwDM4 MTEWDM4 GQDF22KCNPNYWDX/		Tenant Managemu isrgrootx1.g Br frocococco 80 V0 Last activ neral information teway ID neral settings teway description sated at it updated at texay Server address	ent eem ^	Ef9000000000000 Fr 00 50 000 00 00 00 Lest gateway Apr 22, 2022 0040559 Apr 22, 2022 0040559 es1.cloud.thethIngs.n	*tozt	x 1 Collaborator

Port Configuration: Fixed to 8887

After successfully configuring the gateway, you can check the gateway's connection status to determine whether the connection has been established.

Overview	Applications	🝶 Gateways	Corganizations		
	Gateways (2)			Q Search	Claim gateway + Add gateway
	ID 👻		Name ¢	Gateway EUI 🗢	Status
	ff00000000000000	a	gw_000a	FF 00 00 00 00 00 00 0A	Connected •

4.1.6 Common Issues

4.1.6.1 Gateway Status

1. Troubleshooting the internal program status of the gateway

✤ For Semtech UDP GWMP Protocol or Build-in LoRa Server, you can troubleshoot by checking whether the logs show "PullData" and "PullACK" messages. If there is no response within 30 seconds, it indicates a potential issue with the gateway.

time="2022-05-05 11:22:10" level=INFO msg="send to gateway, addr = 192.168.9.238:34111, type = PullACK" time="2022-05-05 11:22:10" level=DEBUG msg="rcv from gateway: addr = 192.168.9.238:34111, type = PullData"

✤ When using the Basicstation mode, you can determine by checking whether the logs appear.



2022-05-05 11:31:56.101 [SYN:VFKb] Time sync rejected: quality=2.100 trieshold=2.136 2022-05-05 11:31:23:477 [SYN:INFO] Time sync qualities: min=2055 q90=2136 max=2219 (previous q90=2334) 2022-05-05 11:31:06.631 [SYN:INFO] Mean MCU drift vs SX130X#0: -5.0ppm 2022-05-05 11:31:06.631 [SYN:INFO] MCU/SX130X drift stats: min: -1.0ppm q50: -7.1ppm q80: -19.9ppm max: -48.9ppm - threshold q90: -36.7ppm

2. Can the gateway receive RF data

• Open the LoRa Packet Logger and use a device with the same frequency configuration as the gateway to send data or initiate joining. As long as the LoRa module can capture logs, it indicates that the RF module is working properly.

	Time	DataType	Freq.	RSSI	SNR	TxPwr	DataRate	FCnt
>	2022-05-05 11:33:24	Unconfirmed Data Down	867.3	0	0	14	SF12BW125	8
>	2022-05-05 11:33:24	Confirmed Data Up	867.3	-81	-11.3	0	SF12BW125	6
>	2022-05-05 11:33:24	Confirmed Data Up	868.3	-16	8.3	0	SF12BW125	6

4.1.6.2 Communication Device

1. Abnormal reception of uplink data

Antenna confirmation, are the antenna frequency bands of the gateway and terminal correct? Is the antenna properly installed? Is the gateway feed line correctly installed?

• Frequency confirmation, compare the frequency points configured on the device with the frequency points configured on the gateway to see if they match.

• Open the LoRa packet logger on the gateway, have the terminal send data or initiate the joining process, and check if the gateway can listen to the terminal's data.

2. Cannot receive downlink data

Antenna Confirmation: Is the antenna frequency band of the gateway and terminal correct? Is the antenna properly installed? Is the gateway's feeder line correctly installed?

Check Packet Logger: Verify if there are logs of downlink data in the packet logger.

■ Class A devices need to wait for an uplink from the device before sending downlink data.

Class C devices will send data immediately.

Make sure that the frequency and data rate you are sending on match the frequency and data rate the device is listening on. (For the Four-Faith modules, you can set DBL=2 to view this information.)

Is the device type consistent?

■ For devices in Class A, if the server is in Class C and sends data immediately, but the device is not in its receive window, this can result in data loss.

■ For devices in Class C, if the server is in Class A and sends data, the device won't immediately receive it. The server needs to wait for the device to send an uplink before it can transmit the downlink. If the device doesn't send an uplink, it won't receive the downlink. After adjusting the device or server's class type, the device needs to be rejoined to synchronize the settings.

4.1.6.3 Device Joining Abnormality



First, check whether the gateway can receive the joining request packet initiated by the device. If it cannot be received, please refer to the "Communication with Devices Troubleshooting" section.

Embedded NS

• Check whether the device has been registered in the embedded NS or if the automatic device addition feature has been enabled.

• Automatic device addition requires verifying whether the AppEUI and AppKey match.

• For devices that have already been registered, it's necessary to check if the AppKey matches.

Non-Embedded NS Server

- Check if the device has been added to the platform.
- Verify if the device's AppEUI and AppKey match. The AppKey is a

mandatory validation field, while the validation of AppEUI depends on the platform's requirements.

If the gateway can see the Join Accept downlink packet but the device doesn't receive it, verify whether the device's frequency band matches that of the Network Server (NS). If they don't match, it can result in a mismatch between the listened frequency or data rate and the downlink, causing the data to not be received properly.

Note: The failure of joining is not related to the inconsistency in device types. For example, if the device is classA and the server is classC, the joining can still succeed.

4.1.6.4 Customer Platform Integration

♦ You can use the gateway's network diagnostic tool to ping the server IP and check if the gateway's network is functioning properly (Path: Network → Network Diagnostics → Ping).

 $\bigstar MQTT Type (Path: LoRa Network Server \rightarrow Interfaces \rightarrow Protocol Configuration)$

- Check if the MQTT switch is turned on.
- Verify the server's IP and port.
- Check the connection status of MQTT
- TCP Type
 - Check if the corresponding TCP connection switch is turned on.
 - Verification of the server's address and port
 - Check Corresponding Connection Status

4.1.6.5 base64 Encoding and Decoding

✤ Online tool address: <u>https://base64.us/</u>

Eann		User	Manual	for	F8926-GW	-02 Seri	es	LoRaWAN	Indoor	Gate
i ultili										
Base64.us	Base64	online	encod	ing a	nd deco	ding (the	best	t Base64 onl	line tool)	
Please enter ti	he characters	to be Base6	4 encoded	or decor	het					
1234		to be based	+ encoded	or decou	leu					
1204										
		[(and in	a obortou						
Encoding	Decode	1 exchange		ig shorter	ut key: Ctrt+	Enter)				
The result of E	3ase64 encodi	ng or decod	ing:			A.	itoma	atically select	all after end	coding/o
EjQ=										
After encodi a permalink	ing, the numbe	er of bytes in	the origina	ıl text: 2,	and the numb	er of bytes af	ter er	ncoding: 4. Co	opy the resul	t to gen
After encodi a permalink	ing, the numbe	er of bytes in	the origina	ıl text: 2,	and the numb	er of bytes af	ter er	ncoding: 4. Cc	opy the resul	t to gen
After encodi a permalink You can als	ing, the numbe o select an im	er of bytes in age file to ge	the origina	il text: 2,	and the numb	er of bytes af orm: 选择文件	ter er]未近	ncoding: 4. Cc 选择任何文件	opy the resul	t to gen
After encodi a permalink You can als	ing, the numbe to select an im	er of bytes in age file to ge	the origina	il text: 2, 64–encoc	and the numb	er of bytes af orm: 选择文件	ter er]未述	ncoding: 4. Cc 选择任何文件 Type Cor	opy the resul	t to gen
After encodi a permalink You can als	ing, the numbe	er of bytes in age file to ge	the origina	al text: 2, 64-encoc	and the numb	er of bytes af orm. 选择文件	ter er	ncoding: 4. Cc 选择任何文件 Type Cor	opy the resul	t to gene

It mainly involves different data types, resulting in different encoding and decoding * outcomes, such as text (strings) or Hex (hexadecimal). The configuration for encoding and decoding can be found in the advanced settings shown in the above image.

Encoding: (When sending downlink data, the data needs to be encoded in base64 $\dot{\mathbf{v}}$ format.)

Text Type $(1234 \rightarrow MTIzNA==)$ Code by @ | Duoji cloud video on demand, CDN, object storage, traffic starts at ¥0.05/GB Implementation methods in each language Settings (we use cookies to remember your advanced settings, these cookies are not logged or used for tracking) character set Set character set encoding, GB2312 cannot use the UTF-8 GB2312 encoding hexadecimal output function. Automatic Set whether to automatically encode or decode when the closure automatic coding encoding/decoding content of the original text box is changed. automatic decoding codec shortcut Set in the original text box, the shortcut key for Ctrl+Enter Enter key encoding/decoding. If set to one, the other is the hotkey for line feed. The action to perform after pressing the above shortcut key. After pressing coding decoding the shortcut key Set the format of the output after Base64 decoding. decoded output text H \x \u {...} If the character set encoding is set to GB2312, this setting will format be invalid. 🗹 When outputting non-plain text, add Add space: $u5728u4F7Fu7528 \rightarrow u5728u4F7Fu7528$ spaces Encoded input Sets the form of Base64 encoded input. text H {...} If the character set encoding is set to GB2312, this setting will format be invalid. Hex Type (0x1234 \rightarrow EjQ=)



• Decoding: (The content of the 'data' field in the upstream push data needs to be decoded from base64 to actual content)

