

# **UG85** Industrial LoRaWAN Gateway User Guide

×

SHROW

Xiamen Ursalink Technology Co., Ltd.



www.ursalink.com

# Preface

Thanks for choosing Ursalink UG85 industrial LoRaWAN gateway. The UG85 industrial LoRaWAN gateway delivers tenacious connection over network with full-featured design such as automated failover/failback, extended operating temperature, dual SIM cards, hardware watchdog, VPN, Gigabit Ethernet and beyond.

This guide shows you how to configure and operate the UG85 industrial LoRaWAN gateway. You can refer to it for detailed functionality and gateway configuration.

### Readers

This guide is mainly intended for the following users:

- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

### © 2017 Xiamen Ursalink Technology Co., Ltd. All rights reserved.

All information in this user guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Ursalink Technology Co., Ltd.

### **Products Covered**

This guide explains how to configure the following devices:

• Ursalink UG85 LoRaWAN gateway

### **Related Documents**

Document	Description
Ursalink UG85 Datasheet	Datasheet for the Ursalink UG85 industrial LoRaWAN Gateway.
Ursalink UG85 Quick Start Guide	Quick installation guide for the Ursalink UG85 industrial LoRaWAN Gateway.

### **Declaration of Conformity**

UG85 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.



For assistance, please contact Ursalink technical support: Email: support@ursalink.com Tel.: 86-592-5023060 Fax: 86-592-5023065

### **Revision History**

Date	Doc Version	Description
Jun. 13, 2019	V.1.1	Initial version
Aug. 6, 2019	V1.2	Add New Function:
		1. Python Development
		2. Send data to LoRaWAN nodes

# Contents

Chapter 1 Product Introduction	7
1.1 Overview	7
1.2 Advantages	7
1.3 Specifications	
1.4 Dimensions (mm)	10
Chapter 2 Access to Web GUI	11
2.1 PC Configuration for Web GUI Access to gateway	
2.2 Access to Web GUI of gateway	12
Chapter 3 Web Configuration	14
3.1 Status	14
3.1.1 Overview	14
3.1.2 LoRa	
3.1.3 Cellular (Only Applicable to Cellular Version)	17
3.1.4 Network	
3.1.5 WLAN (Only Applicable to Wi-Fi Version)	
3.1.6 VPN	21
3.1.7 Host List	22
3.2 LoRaWAN	
3.2.1 Packet Forwarder	23
3.2.1.1 General	23
3.2.1.2 Radios	
3.2.1.3 Advanced	
3.2.1.4 Custom	
3.2.1.5 Traffic	
3.2.2 Network Server	29
3.2.2.1 General	29
3.2.2.2 Application	
3.2.2.3 Profiles	
3.2.2.4 Device	
3.2.2.5 Packets	
3.3 Network	
3.3.1 Interface	36
3.3.1.1 Port	36
3.3.1.2 WAN	
3.3.1.3 LAN	40
3.3.1.4 VLAN Trunk	41
3.3.1.5 WLAN (Only Applicable to Wi-Fi Version)	41
3.3.1.6 Cellular (Only Applicable to Cellular Version)	43
3.3.1.7 Loopback	47
3.3.2 Firewall	48
3.3.2.1 Security	

	3.3.2.2 ACL	. 48
	3.3.2.3 DMZ	.50
	3.3.2.4 Port Mapping	.50
	3.3.2.5 MAC Binding	.51
3.3.	3 QoS	. 52
3.3.	4 DHCP	. 53
	3.3.4.1 DHCP Server	53
	3.3.4.2 DHCP Relay	. 54
3.3.	5 DDNS	. 55
3.3.	6 Link Failover	.55
	3.3.6.1 SLA	55
	3.3.6.2 Track	.56
	3.3.6.3 VRRP	57
	3.3.6.4 WAN Failover	.59
3.3.	7 VPN	.60
	3.3.7.1 DMVPN	. 60
	3.3.7.2 IPSec	.61
	3.3.7.3 GRE	.64
	3.3.7.4 L2TP	.65
	3.3.7.5 PPTP	. 67
	3.3.7.6 OpenVPN Client	.69
	3.3.7.7 OpenVPN Server	70
	3.3.7.8 Certifications	. 72
3.4 Syste	m	.74
3.4.	1 General Settings	. 74
	3.4.1.1 General	. 74
	3.4.1.2 System Time	. 75
	3.4.1.3 SMTP	.77
	3.4.1.4 Phone	.77
	3.4.1.5 Email	. 78
3.4.	2 User Management	.79
	3.4.2.1 Account	.79
	3.4.2.2 User Management	80
3.4.	3 SNMP	81
	3.4.3.1 SNMP	. 81
	3.4.3.2 MIB View	. 82
	3.4.3.3 VACM	. 82
	3.4.3.4 Trap	. 83
	3.4.3.5 MIB	.84
3.4.4 AA	A	84
	3.4.4.1 RADIUS	.84
	3.4.4.2 TACACS+	.85
	3.4.4.3 LDAP	.85
	3.4.4.4 Authentication	86

3.4.5 Device Management	
3.4.6 Events	88
3.4.6.1 Events	88
3.4.6.2 Events Settings	
3.5 Industrial Interface	
3.5.1 I/O	
3.5.1.1 Dl	90
3.5.1.2 DO	
3.5.2 Serial Port	
3.5.3 Modbus Master	
3.5.3.1 Modbus Master	96
3.5.3.2 Channel	96
3.6 Maintenance	99
3.6.1 Tools	
3.6.1.1 Ping	
3.6.1.2 Traceroute	
3.6.2 Schedule	
3.6.3 Log	
3.6.3.1 System Log	100
3.6.3.2 Log Settings	101
3.6.4 Upgrade	102
3.6.5 Backup and Restore	
3.6.6 Reboot	
3.7 APP	105
3.7.1 Python	105
3.7.1.1 Python	
3.7.1.2 App Manager Configuration	
3.7.1.3 Python App	
Chapter 4 Application Examples	
4.1 Application Configuration	108
4.2 Device Profiles Configuration	112
4.3 Device Configuration	
4.4 Send Data to Device	117
4.5 Restore Factory Defaults	
4.5.1 Via Web Interface	
4.5.2 Via Hardware	
4.6 Firmware Upgrade	123
4.7 Cellular Connection	
4.8 Dual SIM Backup Application Example	
4.9 Wi-Fi Application Example	
4.9.1 AP Mode	129
4.9.2 Client Mode	
4.10 NAT Application Example	131
4.11 DTU Application Example	

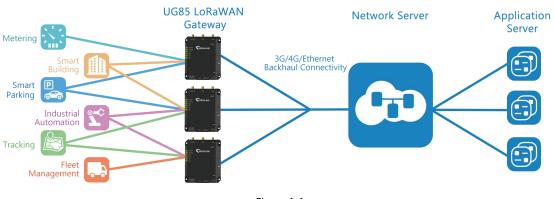
### **Chapter 1 Product Introduction**

#### 1.1 Overview

Ursalink UG85 is an industrial LoRaWAN gateway with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Options like cellular network or WIFI provide drop-in connectivity for operators and make a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial platform of 64-bit CPU and wireless module, the UG85 is capable of providing wire-speed network. Meanwhile, the UG85 also supports Gigabit Ethernet port, serial port (RS232), digital input and output which enable you to scale up M2M application combining data in limited time and budget.

The UG85 is particularly ideal for smart city, smart agriculture, building automation, digital factory, environment protection, water conservancy and so on.





#### 1.2 Advantages

#### Benefits

- Built-in industrial CPU, big memory;
- Ethernet, 2.4GHz/5GHz Wi-Fi or global 2G/3G/LTE options make it easy to get connected
- Embedded network server and compliance with several third party network servers
- MQTT, HTTP or HTTPS protocol for data transmission to application server
- Flexible modular design provides users with different connection options like Ethernet, serial port
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 3-year warranty included

#### Security & Reliability

- Automated failover/failback between Ethernet and Cellular (dual SIM)
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN

- Features embedded hardware watchdog to automatically recover from various failure and ensures highest level of availability
- Establishes a secured mechanism on centralized authentication and features authorization of device access by supporting AAA (TACACS+, RADIUS, LDAP, local authentication) and multiple levels of user authority

#### **Easy Maintenance**

- Ursalink DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and various upgrading options help administrator to manage the device as easy as pie
- WEB GUI and CLI enable the admin to achieve quick configuration and simple management among a large quantity of devices
- Efficiently manage the remote devices on the existing platform through the industrial standard SNMP

### Capabilities

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial 64-bit ARM Cortex-A53 processor, high-performance operating up to 800MHz with low power consumption, and 512 MB memory available to support more applications
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

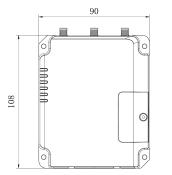
### **1.3 Specifications**

Hardware System	
CPU	800MHz, 64-bit ARM Cortex-A53
Memory	8 GB Flash, 512 MB DDR3 RAM
LoRaWAN	
Connectors	$1 \times 50 \ \Omega$ SMA (Center pin: Female)
Channel	8
Frequency Band	Supports EU 863-870, US 902-928, EU 433, AU 915-928, CN
	470-510 IN865 and KR 920-923 Band
Sensitivity	-140dBm Sensitivity @292bps

Output Power	27dBm Max
Protocol	V1.0 Class A/Class C and V1.0.2 Class A/Class C
Ethernet	
Ports	1 × RJ-45 (PoE PD Optional)
Physical Layer	10/100/1000 Base-T (IEEE 802.3)
Data Rate	10/100/1000 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)
Cellular Interfaces (Optiona	1)
Connectors	$1 \times 50 \Omega$ SMA (Center pin: Female)
SIM Slots	2
Wi-Fi Interfaces (Optional)	
Connectors	$1 \times 50 \Omega$ SMA (Center PIN: SMA Male)
Standards	IEEE 802.11 b/g/n/ac
Tx Power	802.11b: 16 dBm +/-1.5 dBm (11 Mbps)
	802.11g: 15 dBm +/-1.5 dBm (54 Mbps)
	802.11n@2.4 GHz: 14 dBm +/-1.5 dBm (MCS7) 802.11n@5
	GHz: 11 dBm +/-2 dBm (MCS7) 802.11ac@5 GHz: 10 dBm
	+/-2 dBm (MCS9)
GPS (Optional)	
Connectors	$1 \times 50 \Omega$ SMA (Center PIN: SMA Female)
Serial Interface	
Ports	1 × RS232
Connector	Terminal Block
Baud Rate	300bps to 230400bps
10	
Connector	Terminal Block
Digital	$1 \times DI + 1 \times DO$
Console Interface	
Connector	1 × RJ45
Software	
Network Protocols	PPP, PPPOE, SNMP v1/v2c/v3, TCP, UDP, DHCP,DDNS, VRRP,
	HTTP, HTTPS, DNS, SNTP, Telnet, VLAN, SSH, MQTT, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE

Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding
Management	Web, CLI, SMS, On-demand dial up
Reliability	VRRP, Dual SIM Backup
Serial Port	Transparent (TCP Client/Server, UDP), Modbus Gateway
	(Modbus TCP to Modbus RTU), Modbus Master
Power Supply and Consum	otion
Power Input	2-pin with 5.08 mm terminal block
	(Optional: 1 × 802.3 af/at PoE PD )
Input Voltage	9-48 VDC
Power Consumption	Typical 2.3W, Max 6.5W
Physical Characteristics	
Ingress Protection	IP30
Dimensions	108 x 90 x 26 mm (4.25 x 3.54 x 1.02 in)
Mounting	Desktop, wall or DIN rail mounting
Others	
Reset Button	1 × RESET
LED Indicators	$1 \times POWER$ , $1 \times SYSTEM$ , $1 \times LoRa$ , $1 \times WIFI$ , $1 \times LTE$ , $1 \times LAN$
Built-in	Watchdog, RTC, Timer
Certifications	RoHS, CE, FCC
Environmental	
Environmental	
Operating Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular
	-40°C to +70°C (-40°F to +158°F) Reduced cellular
Operating Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular performance above 60°C
Operating Temperature Storage Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular performance above 60°C -40°C to +85°C (-40°F to +185°F)

# 1.4 Dimensions (mm)





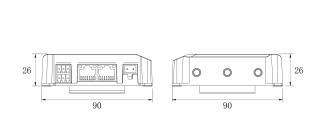


Figure 1-2

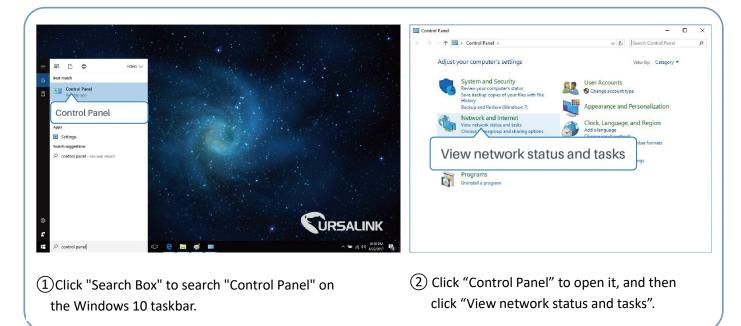
### **Chapter 2 Access to Web GUI**

This chapter explains how to access to Web GUI of the UG85.

### 2.1 PC Configuration for Web GUI Access to gateway

Please connect PC to GE port of UG85 directly. PC can obtain an IP address, or you can configure a static IP address manually. The following steps are based on Windows 10 operating system for your reference.

The following steps are based on Windows 10 operating system for your reference.



← → * ↑ 🛣 « Network	and Internet > Network and Sharing Cente		General	
Control Panel Home	View your basic network info	rmation and set up connections		
Change adapter settings	View your active networks		Connection	
Change advanced sharing	Yeastar5G	Access type: Internet	IPv4 Connectivity:	No network access
settings	Private network	HomeGroup: Ready to create Connections: I Wi-Fi (Yeastar5G)	IPv6 Connectivity:	No network access
		Connections: and Wi-Fi (Teastarbo)	Media State:	Enabled
			Duration:	00:01:21
	Identifying	Access type: No network access Connections: U Ethernet	Speed:	1.0 Gbps
			Details	
	Change your networking settings		o c tuno m	
	Set up a new connection or	ntwork Ethorpot		
	Set up a broadband, dial-up		Activity	
	Troubleshoot problems		neonity -	-
		k problems, or get troubleshooting information.	t	Received
			Properties	alt
			210	0
See also				
HomeGroup			Properties Pisable	Diagnose
Infrared				Diagnose
Internet Options			1	
Windows Firewall				Close
			_	
(3) Click "Ftk	hernet" (May ha	ave different name).	(4) Click "Propert	: II

UG85 User Guide

Networking	Sharing			
Connect us	ing:			
🚽 Intel	(R) 82567LM (	Gigabit Network C	onnection	
			Confi	gure
This conne	ction uses the	following items:		
🗹 🏪 Cli	ient for Micros	oft Networks	10.00	^
🗹 🐙 Fil	e and Printer S	Sharing for Micros	oft Networks	
🗹 🐙 Qa	S Packet Scl	heduler		
	ternet Protoco	Version 4 (TCP/	(Dred)	
million Robie	connect note ee	Version 4 (TCL7	11 V-4)	
Second Second		Adapter Multipl	and the second	
I _ Mi	et Proto	Contraction of the second s	exor Protocol	
Intern	et Proto	Adapter Multipl	exor Protocol	
Intern	et Proto	Adapter Multipl	Protocol. The des	erties efault

O Use the following DNS server addresses: Preferred DNS serve Alternate DNS server: Validate settings upon exit Advanced... OK Cancel

Obtain DNS server address automatically

Internet Protocol Version 4 (TCP/IPv4) Properties

 Obtain an IP address automatically O Use the following IP address:

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

General Alternate Configuration

IP address Subnet mask: Default gateway: ×

- (5) Double Click "Internet Protocol Version 4 (TCP/IPv4)" to configure IP address and DNS server.
- (6) Method 1: click "Obtain an IP address automatically";

nternet P	rotocol Version 4 (TCP/	IPv4) Properties X
General		
this cap	get IP settings assigned ability. Otherwise, you ne appropriate IP settings.	192.168.1.20 <sup>ts</sup> 255.255.255.0
Oob	itain an IP address autor	192.168.1.1
OUs	e the following IP address	
IP ad	dress:	192 . 168 . 1 . 20
Subn	et mask:	255 . 255 . 255 . 0
Defa	ult gateway:	192.168.1.1
OOb	tain DNS server address a	automatically
) Us	e the following DNS serve	r addresses:
Prefe	rred DNS server:	192.168.1.1
Alter	nate DNS server:	
□va	alidate settings upon exit	192.168.1.1
		OK Cancel

Method 2: click "Use the following IP address" to assign a static IP manually within the same subnet of the gateway.

(Note: remember to click "OK" to finish configuration.)

### 2.2 Access to Web GUI of gateway

Ursalink gateway provides Web-based configuration interface for management. If this is the first time you configure the gateway, please use the default settings below.

Username: admin Password: password IP Address: 192.168.1.1 **DHCP Server: Enabled** 

- Start a Web browser on your PC (Chrome and IE are recommended), type in the IP 1. address, and press Enter on your keyboard.
- Enter the username, password, and click "Login". 2.

The second seco
<b>URSALINK</b>
Lisemame
Password
Login

If the SIM card is connected to cellular network with public IP address, you can access WEB GUI remotely via the public IP address when remote access is enabled.

If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

3. When you login with the default username and password, you will be asked to modify the password. It's suggested that you change the password for the sake of security. Click "Cancel" button if you want to modify it later.

Glian	ge Password	
Old Password		
New Password		
Confirm New Password		
Save	Cancel	

4. After you login the Web GUI, you can view system information and perform configuration on the gateway.

URSAL	.INK										
			password								
Status		Overview	LoRa	Cellular	Network	VPN	Host List				
LoRaWAN	×	System Informa	ation								
	-	Model		UG85							
Network		Partnumber		L00E-S1011	L00E-S1011-EU868						
System		Serial Number		621791810	621791810162						
	Firmware Version			80.0.0.6							
Industrial	•	Hardware Version	n	V1.0	V1.0						
		Local Time		2019-06-11	11:30:26						
Maintenance	•	Uptime		00:15:40							
APP	•	CPU Load		28%							
		RAM (Capacity/A	vailable)	512MB/257	MB(50.2%)						
		eMMC (Capacity/	/Available)	6.6G/6.0G(	91.63%)						
							[	Manual Refresh 🔻	Refresh		

# **Chapter 3 Web Configuration**

### 3.1 Status

### 3.1.1 Overview

You can view the system information of the gateway on this page.

Status	Overview	LoRa	Cellular	Network	VPN	Host List				
LoRaWAN 🕨	System Information	n)								
	Model		UG85							
Network	Partnumber		L00E-S1011-EU868							
	Serial Number		621791810162							
System 🕨	Firmware Version		80.0.0.8	80.0.0.8						
Industrial	Hardware Version		V1.0	V1.0						
	Local Time		2019-06-12	19:38:32						
Maintenance										
	Uptime		01:43:58	01:43:58						
APP	CPU Load	56%	56%							
	RAM (Capacity/Availa	RAM (Capacity/Available)			512MB/244MB(47.66%)					
	eMMC (Capacity/Avai	ilable)	6.6G/6.0G(	92.01%)						

Figure 3-1-1-1

System Information						
Item	Description					
Model	Show the model name of gateway.					
Serial Number	Show the serial number of gateway.					
Firmware Version	Show the currently firmware version of gateway.					
Hardware Version	Show the currently hardware version of gateway.					
Local Time	Show the currently local time of system.					
Uptime	Show the information on how long the gateway has been running.					
CPU Load	Show the current CPU utilization of the gateway.					
RAM (Capacity/Available)	Show the RAM capacity and the available RAM memory.					
eMMC (Capacity/Available)	Show the eMMC capacity and the available eMMC memory.					

Table 3-1-1-1 System Information

### 3.1.2 LoRa

You can view the LoRaWAN status of gateway on this page.

Basic		
Mode	Packet Forwarder	
Version	4.0.1	
Status	Running	
Gateway ID	24E124FFFEF0132D	
Region Code	AS923	
Server Address	localhost	
Uplink		
Packet Received	1	
Packets Received State	CRC_OK: 0.00%, CRC_FAIL: 100.00%,	
Packet Forwarded	1 (208 bytes)	
Push Data Datagrams Sent	1 (456 bytes)	
Push Data Acknowledged	0.00%	
Downlink		
Pull Data Sent	3 (0.00% acknowledged)	
Pull Resp Datagrams Received	0 (0 bytes)	
Packets Sent to node	0 (0 bytes)	
Packets Sent Errors	0	

### Figure 3-1-2-1

LoRaWAN Status (Packet Forwarder Mode)								
Item	Description							
Mode	Show the working mode of LoRaWAN.							
Version	Show the version of packet forwarder software.							
Status	Show the status of packet forwarder.							
Status	Value include Running, Disabled.							
Gateway ID	Show the ID of the gateway.							
Region Code	Show the LoRa region code which is based on the gateway's variant							
Server Address	Show the IP address of remote LoRaWAN network server.							
Packet Received	Show the count of data packet from node to gateway.							
	Show the RF packets receiving state:							
Packets received State	CRC_OK: Percentage of CRC verification							
Packets received State	CRC_Fail: Percentage of CRC verification failure							
	NO_CRC: Percentage of abnormal packets without CRC							
Packets forwarded	Packets that CRC verified are sent from gateway to server.							
Push Data Datagrams Sent	The total quantity of packets sent from gateway to server,							
	including the RF packets forwarded and statistics packets.							
Push Data Acknowledged	Percentage of acknowledged packets among Push Data Datagrams Sent.							
Pull Data Sent	Show the number of keepalive packets sent to the server, and							

	percentage of acknowledged packet regarding the keepalive packet from the server.
Pull Resp Datagrams Received	Show the packet counts and size that will be sent from server to gateway.
RF Packets Sent to node	Show the RF packet counts and size that will be sent from gateway to node.
RF Packets Sent Errors	Show the RF packet counts that fail to be sent from server to node.

Table 3-1-2-1 LoRaWAN Status (Packet Forwarder Mode)

Status		Overview	LoRa	Cellular	Network	VP	ч	Routing	Host Lis	t				
LoRaWAN	•	Basic												
Mode Nerwork Server														
Network	· · · ·			1.0.2	2									
System	•	Status		Run	ning									
Industrial	•	Gateways												
Maintenance	•		EUI	Ch0	Ch1	Ch2	Ch3	Ch4	Ch5	Ch6	Ch7	LoRa	FSK	Operation
APP	×	24E124	FFFE0B7443	0	29	10	0	0	0	1146	0	0	1146	•

Figure 3-1-2-2

LoRaWAN Status (Network Server)						
Description						
Show the working mode of LoRaWAN.						
Show the version of installed lora network server file.						
Show the status of network server.						
Value include Running, Disabled.						
Show the identifier of the gateway.						
Show the number of packets received on Ch0.						
Show the number of packets received on Ch1.						
Show the number of packets received on Ch2.						
Show the number of packets received on Ch3.						
Show the number of packets received on Ch4.						
Show the number of packets received on Ch5.						
Show the number of packets received on Ch6.						
Show the number of packets received on Ch7.						
Show the number of packets received on LoRa.						
Show the number of packets received on FSK.						

Table 3-1-2-2 LoRa WAN-Status-Network Server



Click to clean every channel's data, then the packet receive counter will be restarted.

Click

to view the details of the connected gateway, as the following picture shows.

ateway	Details										
Gateway EUI						FE0B7443					
IP Address					localhost						
Version					4.0.1						
Uplink					1170						
Downlink					15						
				1.02000							
Ch0	Ch1	Ch2	Ch3	Ch4	Ch5	Ch6	Ch7	LoRa	FSK	CRC	Total
923.0	923.2	923.4	922.0	922.2	922.4	922.6	922.8	922.1	922.6		
0	29	10	0	0	0	1146	0	0	1146	3	1188

#### Figure 4-1-4-6

LoRaWAN-Net	LoRaWAN-Network Server-Status-Gateway Detail						
Item	Description						
Gateway EUI	Show the identifier of the gateway.						
IP Address	Show the IP address of the gateway.						
Version	Show the version of packet forwarder software.						
Uplink	Show the number of uplink packets which the gateway received.						
Downlink	Show the number of downlink packets which the gateway received.						
Ch0	Show the frequency of Ch0 and number of packets received on Ch0.						
Ch1	Show the frequency of Ch1 and number of packets received on Ch1.						
Ch2	Show the frequency of Ch2 and number of packets received on Ch2.						
Ch3	Show the frequency of Ch3 and number of packets received on Ch3.						
Ch4	Show the frequency of Ch4 and number of packets received on Ch4.						
Ch5	Show the frequency of Ch5 and number of packets received on Ch5.						
Ch6	Show the frequency of Ch6 and number of packets received on Ch6.						
Ch7	Show the frequency of Ch7 and number of packets received on Ch7.						
LoRa	Show the frequency of LoRa channel and number of packets received on						
LOINA	LoRa channel.						
FSK	Show the frequency of FSK channel and number of packets received on FSK						
	channel.						
CRC	Show the total number of packets with CRC error.						
Total	Show the total number of packets received by the gateway.						

Table 4-1-4-6 LoRa WAN-Network Server-Status-Gateway Detail

### 3.1.3 Cellular (Only Applicable to Cellular Version)

You can view the cellular network status of gateway on this page.

Overview	Cellular	Network	VPN	Routing	Host List
Modem					
Status		Ready			
Model		EC25			
Current SIM		SIM1			
Signal Level		15asu (-83dBr	n)		
Register Status		Registered (H	ome network)		
IMSI		460019987103	3071		
		898601178380	019196629		
ISP		CHN-UNICOM	1		
Network Type		LTE			
PLMN ID		46001			
LAC		5922			
Cell ID		812c63d			
IMEI		861107031710	8000		

### Figure 3-1-3-1

Modem Information				
Item	Description			
Status	Show corresponding detection status of module and SIM card.			
Model	Show the model name of cellular module.			
Current SIM	Show the current SIM card used.			
Signal Level	Show the cellular signal level.			
<b>Register Status</b>	Show the registration status of SIM card.			
IMSI	Show IMSI of the SIM card.			
ICCID	Show ICCID of the SIM card.			
ISP	Show the network provider which the SIM card registers on.			
Network Type	Show the connected network type, such as LTE, 3G, etc.			
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.			
LAC	Show the location area code of the SIM card.			
Cell ID	Show the Cell ID of the SIM card location.			
IMEI	Show the IMEI of the module.			

Table 3-1-3-1 Modem Information

#### Network

Status	Connected
IP Address	10.53.241.18
Netmask	255.255.255.252
Gateway	10.53.241.17
DNS	218.104.128.106
Connection Duration	0 days, 00:04:26

### Figure 3-1-3-2

Network Status				
Item	Description			
Status	Show the connection status of cellular network.			
IP Address	Show the IP address of cellular network.			
Netmask	Show the netmask of cellular network.			
Gateway	Show the gateway of cellular network.			
DNS	Show the DNS of cellular network.			
Connection Duration	Show information on how long the cellular network has been connected.			

Table 3-1-3-2 Network Status

### 3.1.4 Network

On this page you can check the LAN status of the gateway.

WAN							
Port	Status	Туре	IP Address	Netmask	Gateway	DNS	Duration
GE 0	up	Static	192.168.23.94	255.255.255.0	192.168.23.1	114.114.114.114	12m 14s

#### Figure 3-1-4-1

LAN Status				
Item	Description			
Port	Show the name of WAN port.			
Status	Show the status of WAN port. "Up" refers to a status that WAN is enabled and Ethernet cable is connected. "Down" means Ethernet cable is disconnected or WAN function is disabled.			
Туре	Show the dial-up type of WAN port.			
IP Address	Show the IP address of WAN port.			
Netmask	Show the netmask of WAN port.			
Gateway	Show the gateway of WAN port.			
DNS	Show the DNS of WAN port.			

	Show the information about how long the Ethernet cable has
Dunation	been connected to WAN port when WAN function is enabled.
Duration	Once WAN function is disabled or Ethernet cable is
	disconnected, the duration will stop.

Table 3-1-4-1 LAN Status

### 3.1.5 WLAN (Only Applicable to Wi-Fi Version)

You can check Wi-Fi status on this page, including the information of access point and client.

Overview	LoRa	Cellular	Network	WLAN	VPN	Host List
WLAN Status						
Wireless Status		Enabled				
MAC Address		24:e1:24:f0:27:85				
Interface Type		AP				
SSID		Ursalink_F02786				
Channel		Auto				
Encryption Type		No Encryption				
Status		Up				
IP Address		192.168.100.1				
Netmask		255.255.255.0				
Connection Duration	1	0 days, 00:08:50				

### Figure 3-1-5-1

WLAN Status				
Item	Description			
Wireless Status	Show the wireless status.			
MAC Address	Show the MAC address.			
Interface Type	Show the interface type, such as "AP" or "Client".			
SSID	Show the SSID.			
Channel	Show the wireless channel.			
Encryption Type	Show the encryption type.			
Status	Show the connection status.			
IP Address	Show the IP address of the gateway.			
Netmask	Show the wireless MAC address of the gateway.			
Gateway	Show the gateway address in wireless network.			
Connection Duration	Show information on how long the Wi-Fi network has been connected.			

Table 3-1-5-1 WLAN Status

Associated Stations		
IP Address	MAC Address	Connection Duration

Figure 3-1-5-2

Associated Stations				
Item	Description			
IP Address	Show the IP address of access point or client.			
MAC Address	Show the MAC address of the access point or client.			
Connection Duration	Show information on how long the Wi-Fi network has been connected.			

Table 3-1-5-2 WLAN Status

### 3.1.6 VPN

You can check VPN status on this page, including PPTP, L2TP, IPsec, OpenVPN and DMVPN.

Overview	Cellular	Network	VPN	Routing	Host List
PPTP Tunnel					
	Name	Status		Local IP	Remote IP
	pptp_1	Disconnected		: 73	
	pptp_2	Disconnected		-	-
	pptp_3	Disconnected			-
L2TP Tunnel					
	Name	Status		Local IP	Remote IP
	l2tp_1	Disconnected		: 28	5
	12tp_2	Disconnected		-	-
	l2tp_3	Disconnected		. 50	-

Figure 3-1-6-1

Overview	Cellular	Network	VPN Rou	ting Host List	
IPsec Tunnel					
	Name	Status	Local	IP	Remote IP
	ipsec_1	Disconnected			: 5
	ipsec_2	Disconnected	-		
	ipsec_3	Disconnected	807		1
OpenVPN Clie	ent				
	Name	Status	Local	IP	Remote IP
	openvpn_1	Disconnected			: 5
	openvpn_2	Disconnected	-		-
	openvpn_3	Disconnected	1		- 21

Figure 3-1-6-2

GRE Tunnel				
	Name	Status	Local IP	Remote IP
	gre_1	Disconnected	~	
	gre_2	Disconnected	-	
	gre_3	Disconnected	2	
DMVPN Tunnel				
	Name	Status	Local IP	Remote IP
	dmvpn	Disconnected	÷	

Figure 3-1-6-3

VPN Status			
Item	Description		
Name	Show the name of the VPN tunnel.		
Status	Show the status of the VPN tunnel.		
Local IP Show the local tunnel IP of VPN tunnel.			
Remote IP	Show the remote tunnel IP of VPN tunnel.		
Table 3-1-6-1 VPN Status			

### 3.1.7 Host List

You can view the host information on this page.

Overview	Cellular	Network	VPN	Routing	Host List	GPS
DHCP Leases						
	IP		MAC		Lease	Remaining Time
MAC Binding						
	IF	0			MAC	

Figure 3-1-7-1

Host List			
Item Description			
DHCP Leases			
IP Address	Show IP address of DHCP client		
MAC Address Show MAC address of DHCP client			
Lease Time Remaining Show the remaining lease time of DHCP client.			
MAC Binding			
IP & MAC	Show the IP address and MAC address set in the Static IP list of		
IF & WIAC	DHCP service.		

Table 3-1-7-1 Host List Description

### 3.2 LoRaWAN

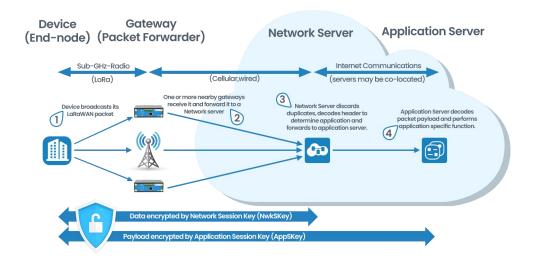


Figure 3-2-1

#### 3.2.1 Packet Forwarder

3.2.1.1 General

#### General Radios Advanced Custom Traffic Status General Setting LoRaWAN Enable Please close the Network Server mode first Packet Forwarder Mode Packet Forwarder Network Server Gateway EUI 24E124FFFE0B6543 Gateway ID 24E124FFFE0B6543 Network D Server Address localhost Server Up Port 1700 System Server Down Port 1700 Industrial Maintenance



General Setting			
ltem	Description	Default	
Enable	Click to enable the Packet Forwarder mode.	Enabled	
		Generated from	
		MAC address of	
Gateway EUI	Show the identifier of the gateway.	the gateway and	
		cannot be	
		changed.	

Gateway ID	Fill in the corresponding ID which you've used for register gateway on the remote network server, such as TTN. It is usually the same with gateway EUI and can be changed.	The default is the same with gateway EUI.
Server Address	Enter the IP address of the LoRaWAN network server.	Null
Server Up Port	Enter the port of the LoRaWAN network server to upload data. Range: 1-65535.	1700
Server Down Port	Enter the port of the LoRaWAN network server to send data to your gateway. Range: 1-65535.	1700

Table 3-2-1-1 General Setting Parameters

### 3.2.1.2 Radios

General	Radios	Advanced	Custom	Traffic		
Radio Channel S	Radio Channel Setting					
Supported Frequer	ісу			AS923 *		
		Name			Center Frequency/MHz	
		Radio 0			923.6	
		Radio 1			922.6	



Radios-Radio Channel Setting			
Item	Description	Default	
	Choose the LoRaWAN frequency plan used for	The default	
Supported	the upstream and downlink frequencies and	frequency is set	
Frequency	datarates. Available channel plans depend on the	based on the	
	gateway's variant.	gateway's variant.	
Name	Show the name of central frequency.		
Center Frequency	Enter the central frequency of Radio 0 which supports transmitting and receiving packet. Enter the center frequency of Radio 1 which only supports receiving packet from nodes.	Null	

Table 3-2-1-2 Radio Channels Setting Parameters

#### Multi Channels Setting

Enable	Index	Radio	Frequency/MHz
	0	Radio 0 🔻	923.2
۲	1	Radio 0 🔻	923.4
۲	2	Radio 0 🔻	923.6
	3	Radio 1 🔻	922.2
	4	Radio 1 🔻	922.4
	5	Radio 1 🔻	922.6
	6	Radio 1 🔻	922.8
۲	7	Radio 1	923.0



Radios-Multi Channel Setting			
Item	Description	Default	
Enable	Click to enable this channel to transmit packets.	Enabled	
Index	Indicate the ordinal of the list.		
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0	
Frequency/MHz	Enter the frequency of this channel. Range: center frequency $\pm$ 0.9.	The default frequency is set based on the supported frequency you have selected.	

### Table 3-2-1-3 Multi Channel Setting Parameters

LoRa Channel Setting

Enable	Radio	Frequency/MHz	Bandwidth/KHz	Spread Factor
2	Radio 0 🔻	923.8	250KHZ •	SF7 •

Figure 3-2-1-4

Radios-LoRa Channel Setting				
Item	Description	Default		
Enable	Click to enable this channel to transmit packets.	Enabled		
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0		
Frequency/MHz	Enter the frequency of this channel. Range: center frequency $\pm$ 0.9.	The default frequency is set based on the supported frequency you have selected.		
Bandwidth/MHz	Enter the bandwidth of this channel. Recommended value: 125KHz, 250KHz, 500KHz	125KHz		
Spread Factor	Choose the selectable spreading factor. The channel with large spreading Factor corresponds to a low rate, while the small one corresponds to a high rate.	The default is based on what is specified in the LoRaWAN regional parameters document.		

Table 3-2-1-4 LoRa Channel Setting Parameters

FSK Channel Setting				
Enable	Radio	Frequency/MHz	Bandwidth/KHz	DataRate
2	Radio 0 🔹	924.0	125KHZ •	50000

Figure	3-2-1-5
inguie	J-Z-I-J

Radios-FSK Chann	Radios-FSK Channel Setting			
Item	Item Description			
Enable	Click to enable this channel to transmit packets.	Disabled		
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0		
Frequency/MHz	Enter the frequency of this channel. Range: center frequency $\pm$ 0.9.	The default frequency is set based on the supported frequency you have selected.		
Bandwidth/MHz	Enter the bandwidth of this channel. Recommended value: 125KHz, 250KHz, 500KHz	500KHz		
Data Rate	Enter the data rate. Range: 500-25000.	500		

Table 3-2-1-5 FSK Channel Setting Parameters

### 3.2.1.3 Advanced

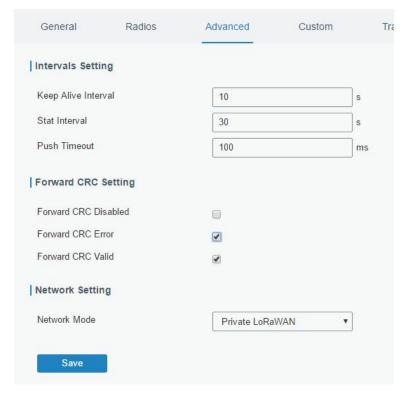


Figure 3-2-1-6

Advanced		
Item	Description	Default
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to LoRaWAN network server to keep the connection stable and alive. Range: 1-3600.	10
Stat Interval	Enter the interval to update the network server with gateway statistics. Range: 1-3600.	30
Push Timeout	Enter the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-3600.	100
Forward CRC Disabled	Enable to send packets received with CRC disabled to the network server.	Disabled.
Forward CRC Error	Enable to send packets received with CRC errors to the network server.	Disabled.
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled
Network Mode	select from "Public LoRaWAN", "Private LoRaWAN". Public LoRaWAN: telecom/operator managed networks, connect multiple applications (multi-tenant) into a single network. Private LoRaWAN: individually managed networks, Network deployed for single application purpose.	Public LoRaWAN

Table 3-2-1-6 Advanced Parameters

#### 3.2.1.4 Custom

General	Radios	Advanced	Custom	Traffic
Custom Config	guration			
Enable				
				Example
"antenna_gain "radio_0": { "enable": true, "type": "SX125 "freq": 922500 "rssi_offset": - "tx_enable": tr "tx_freq_min": "tx_freq_max" },	ic": true, adio_1 provides clo ": 0, /* antenna gair ". 000, 162, ue, 917000000,	ck to concentrator */ n, in dBi */		
"radio 1": {				

Figure 3-2-1-7

When Custom Configuration mode is enabled, you can write your own packet forwarder configuration file in the edit box to configure packet forwarder. Click "Save" to save your custom configuration file content, and click "Apply" to take effect. You can click "Clear" to erase all content in the edit box. If you don't know how to write configuration file, please click "Example" to go to reference page.

### 3.2.1.5 Traffic

When navigating to the traffic page, any recent traffic received by the gateway will display. To watch live traffic, click Start.

Tra	ffic Setting								
	Refresh	Clear							
	Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
	1	up	7	83002508	922.8	SF9BW125	4/5	-103	-13.2
	1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
	1	up	-	35426956	922.8	SF9BW125	4/5	-103	-9.8
	1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5
	1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0
	1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2
	1	up	2	3147851660	922.6	SF9BW125	4/5	-102	-13.8
	1	up	÷	3143888916	922.8	SF9BW125	4/5	-102	-13.2
	1	up		3139922740	922.8	SF9BW125	4/5	-100	-12.2
	1	up		3124065788	922.8	SF9BW125	4/5	-100	-12.8

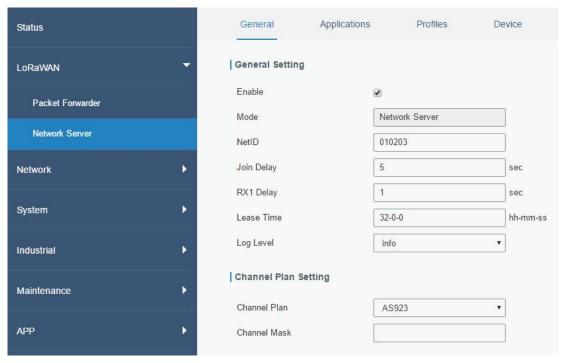
#### Figure 3-2-1-8

Item	Description
Refresh	Click to obtain the latest data.
Clear	Click to clear all data.
Rfch	Show the channel of this packet.
Direction	Show the direction of this packet.
Time	Show the receiving time of this packet.
Ticks	Show the ticks of this packet.
Frequency	Show the frequency of the channel.
Datarate	Show the datarate of the channel.
Coderate	Show the coderate of this packet.
RSSI	Show the received signal strength.
SNR	Show the signal to noise ratio of this packet.

Table 3-2-1-7 Traffic Parameters

### 3.2.2 Network Server







Item	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Disabled
NetID	Enter the network identifier.	01023
Join Delay	Enter the interval time between the end-device sends a Join_request_message to network	5

	server and the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	
RX1 Delay	Enter the interval time between the end-device sends uplink packets and the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time until a successful join expires. The format is hours-minutes-seconds. If the join-type is OTAA, then the end-devices need to join the network server again when it exceeds the lease time.	"744-00-00"
Log level	Choose the log level.	Info
<b>Channel Plan Setti</b>		
Channel Plan	Choose LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's variant.	Depend on the gateway's variant.
Channel Mask	Enabled frequencies are controlled using channel mask. Leave it blank means using the default standard usable channels which are specified in the LoRaWAN regional parameters document. A bit in the ChMask field set to 1 means that the corresponding channel can be used for uplink transmissions if this channel allows the data rate currently used by the end-device. A bit set to 0 means the corresponding channels should be avoided. US and AU 915 have a 80-bit channel mask for 72 usable channels and EU, AS, IN, KR have a 16-	Null. Null means using the default standard usable channels which are specified in the LoRaWAN regional parameters document.

Table 3-2-2-1 General Parameters

**Note:** For some regional variants, If allowed by your LoRaWAN region, you can use Additional Plan to configure additional channels that are not defined by the LoRaWAN Regional Parameters, like EU868 and KR920, as the following picture shows:

Additional Channels			
Frequency(MHz)	Min Datarate	Max Datarate	Operation
			•

Figure 3-2-2-2

Additional Channels			
Item	Description	Default	
Frequency/MHz	Enter the frequency of the additional plan.	Null.	
Max Datarate	Enter the max datarate for the end-device. The range is based on what is specified in the LoRaWAN regional parameters document.	DR0(SF12,125kHz)	
Min Datarate	Enter the min datarate for the end-device. The range is based on what is specified in the LoRaWAN regional parameters document.	DR3(SF9,125kHz)	

Table 3-2-2-2 Additional Plan Parameters

### 3.2.2.2 Application

Devices can communicate with applications that they've been registered. To register a device, you'll first need to create an application (define the method you want to decode the data sent from end-device ) and a device profile (define the join-type and LoRaWAN classes). You don't have to create new application profile and device profile when you add a new device which its "Payload Codec", "Join Type", "Class Type" are the same with existing device. You can just choose the corresponding profiles.

You can see the information about the application you have created in this page.

Applications

ID	Name	Description	Payload Codec	Operation
1	Ursalink-app	a application for ursalink test	None	
2	AS923	S	Cayenne LPP	2 ×
				<b>H</b>

	Figure	3-2	-2-3
--	--------	-----	------

Item	Description
ID	Show the ID of the application profile already created.
Name	Show the name of the application profile already created.
Description	Show the description of the application profile already created.
Payload Codec	Show the payload codec of the application profile already created.

Table 3-2-2-3 Application Parameters

You can edit the application by clicking  $\blacksquare$  or create a new application by clicking  $\blacksquare$ .



Data Transmission	
Туре	Operation
	8

Figure 3-2-2-4

The data will be sent to your custom server address using the MQTT, HTTP or HTTPS protocol.

#### **Related Configuration Example**

Application configuration

### 3.2.2.3 Profiles

You can view the information about the device profiles which you have created in this page.

Device Profile	95				
	Name	Max TXPower	Join Type	Class Type	Operatio n
	Device-test	0	OTAA	Class A	2X
	Ursalink-test-ABP	0	ABP	Class A	2X
	ninii	0	OTAA	Class A	l ×
					8

#### Figure 3-2-2-5

Item	Description
Name	Show the name of the device profile.
Max Tx power	Show the Tx power of the device profile.
Join Type	Show the join type of the device profile.
Class Type	Show the class type of the device profile.

Table 3-2-2-4 Device profiles setting Parameters

You can edit the device profile by clicking  $\blacksquare$  or create a new device profile by clicking  $\blacksquare$ .



#### **Related Configuration Example**

**Device Profiles Advanced configuraion** 

### 3.2.2.4 Device

Device							
	Device Name	Device EUI	Device-Profile	Application	Last Seen	Actived	Operatio n
	asd	353035308337 <mark>611</mark> 8	ninii	AS923	53 minutes ago	~	<b>∕</b> ×
							<b>H</b>



Item	Description	
Device Name	Show the name of the device.	
Device EUI	Show the EUI of the device.	
Device-Profile	Show the name of the device's device profile.	
Application	Show the name of the device's application.	
Last Seen	Show the time of last packet received.	
Actived Show the status of the device . V means that the device been activated.		
Table 3-2-2-5 Device Parameters		

You can edit the device by clicking  $\square$  or create a new device by clicking  $\square$ .

## **Related Configuration Example**

**Device configuration** 

### 3.2.2.5 Packets

end Data To Device									
Device EUI		Туре			I	Payload		Port	Confirmed
000000000000000000		ASCII	•]						
Send									
letwork Server									
Clear								Search	O,
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
24e1641193199962	865402500	SF11BW125		-	17	0	<b>Jn</b> Acc	2019-08-09T07:18:23+02:00	0
24e1641193199962	865402500	SF11BW125	9.5	-34	18	0	JnReq	2019-08-09T07:18:22+02:00	0
24e1641193199962	865402500	SF8BW125	2	u.	0	2	DnUnc	2019-08-09T07:17:16+02:00	0
24e1641193199962	865402500	SF8BW125	10.8	-42	26	3	UpCnf	2019-08-09T07:17:16+02:00	0
24e1641193199962	865062500	SF7BW125	-	-	0	1	DnUnc	2019-08-09T07:17:01+02:00	0
24e1641193199962	865062500	SF7BW125	8.8	-46	25	2	UpCnf	2019-08-09T07:17:01+02:00	0
24e1641193199962	865402500	SF12BW125	2	2	0	0	DnUnc	2019-08-09T07:16:53+02:00	0
24e1641193199962	865402500	SF12BW125	7.8	-50	3	1	UpCnf	2019-08-0 Manual Refresh	Refres

#### Figure 3-2-2-7

Send Data To Device			
Item	Description	Default	
Device EUI	Enter the EUI of the device to receive the payload.	Null	
Туре	Choose from: "ASCII", "hex", "base64". Choose the payload type to enter in the payload Input box.	ASCII	
Payload	Enter the message to be sent to this device.	Null	
Fport	Enter the LoRaWAN frame port for packet transmission between device and Network Server.	Null	
Confirmed	After enabled, the end device will receive downlink packet and should answer "confirmed" to the network server.	Disabled	

Network Server		
Item	Description	
Device EUI	Show the EUI of the device.	
Frequency	Show the used frequency to transmit packets.	
Datarate	Show the used datarate to transmit packets.	
SNR	Show the signal-noise ratio.	
RSSI	Show the received signal strength indicator.	
Size	Show the size of payload.	
Fcnt	Show the frame counter.	
Туре	<ul> <li>Show the type of the packet:</li> <li>JnAcc - Join Accept Packet</li> <li>JnReq - Join Request Packet</li> <li>UpUnc - Uplink Unconfirmed Packet</li> <li>UpCnf - Uplink Confirmed Packet - ACK response from</li> <li>network requested</li> <li>DnUnc - Downlink Unconfirmed Packet</li> <li>DnCnf - Downlink Confirmed Packet- ACK response from</li> <li>end-device requested</li> </ul>	
Time	Show the time of packet was sent or received.	

Table 3-2-2-6 Packet Parameters



Click to get more details about the packet. As shown:

			30
Pack	kets Details		×
	Dev Addr	068c1b56	*
	GwEUI	24e124fffe0b7443	1
	AppEUI	70b3d57ed0007ac1	(
	DevEUI	3530353083376118	
	Immediately	false	
	TimeSinceGPSEpoch	2	9
	Timestamp	242616788	
	Туре	DnUnc	
	Adr	true	ľ
	AdrAcKReq	false	1
	Ack	true	1
	Fcnt		
	Fport		
			*

Figure 3-2-2-8

Item	Description
Dev Addr	Show the address of the device.
GwEUI	Show the EUI of the gateway.
AppEUI	Show the EUI of the application.
DevEUI	Show the EUI of the device.
	True: Device may transmit an explicit (possibly empty)
Immediately	acknowledgement data message immediately after the reception of a
	data message requiring a confirmation.
TimeSinceGPS Epoch	Show the GPS time.
Timestamp	Show the timestamp of this packet.
Frequency	Show the frequency of this channel.
	Show the type of the packet:
	JnAcc - Join Accept Packet
	JnReq - Join Request Packet
Туре	UpUnc - Uplink Unconfirmed Packet
1,100	UpCnf - Uplink Confirmed Packet - ACK response from network requested
	DnUnc - Downlink Unconfirmed Packet
	DnCnf - Downlink Confirmed Packet- ACK response from end-device
	requested
Adr	True: The end-node has enabled ADR.
	False: The end-node has not enabled ADR.
	In order to validate that the network is receiving the uplink messages,
AdrAcKReq	nodes periodically transmit ADRACKReq message. This is 1 bit long.
	True:Network should respond in ADR_ACK_DELAY time to confirm that it

	is receiving the uplink messages				
	False: Otherwise				
Ack	True: This frame is ACK.				
	False: This frame is not ACK.				
Fcnt	Show the frame-counter of this packet. The network server tracks the				
	uplink frame counter and generates the				
	downlink counter for each end-device.				
FPort	FPort is a multiplexing port field. If the frame payload field is not empty,				
	the port field must be present. If present, a FPort				
	16 value of 0 indicates that the FRMPayload contains MAC commands				
	only.When this is the case, the FOptsLen field must be zero. FOptsLen is				
	the length of the FOpts field in bytes.				
Modulation	LoRa means the physical layer uses the LoRa modulation				
Bandwidth	Show the bandwidth of this channel.				
SpreadFactor	Show the spreadFactor of this channel.				
Bitrate	Show the bitrate of this channel.				
CodeRate	Show the coderate of this channel.				
SNR	Show the SNR of this channel.				
RSSI	Show the RSSI of this channel.				
Power	Show the transmit power of the device.				
Payload (b64)	Show the application payload of this packet.				
Payload (hex)	Show the application payload of this packet.				
MIC	Show the MIC of this packet.MIC is a cryptographic message integrity				
	code, computed over the fields MHDR, FHDR, FPort and the encrypted				
	FRMPayload.				

Table 3-2-2-7 Packets Details Parameters

### **Related Topic**

Send Data to Device

### 3.3 Network

### 3.3.1 Interface

### 3.3.1.1 Port

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
Port Settin	ng				
	Port	Status	Property	Speed	Duplex
	GE 0	up 🔻	wan 🔻 au	uto 🔻 au	ito 🔻

Figure 3-3-1-1

Port Setting	Port Setting				
Item	Description				
Port	Users can define the Ethernet ports according to their needs.				
Status	Set the status of Ethernet port; select "up" to enable and "down" to disable.				
Property	LAN. User cannot change this setting.				
Speed	Set the Ethernet port's speed. The options are "auto", "1000 Mbps", "100 Mbps", and "10 Mbps".				
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".				

Table 3-3-1-1 Port Parameters

# 3.3.1.2 WAN

WAN port can be connected with Ethernet cable to get Internet access. It supports 3 connection types.

- Static IP: configure IP address, netmask and gateway for Ethernet WAN interface.

- **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain IP address automatically.

- **PPPoE**: configure Ethernet WAN interface as PPPoE Client.

<b>VRSALINK</b>								
		For your device security, please	change the default password					
Status	Port WAN	LAN VLAN Trunk	Cellular Loopback					
LoRaWAN	- WAN_1							
Network 👻	Enable	2						
Interface	Port	GE 0	]					
Firewall	Connection Type IP Address	Static IP 192.168.23.141						
QoS	Netmask	255.255.255.0						
DHCP	Gateway	192.168.23.1						
DDNS	MTU	1500						
Link Failover	Primary DNS Server	8.8.8.8						
	Secondary DNS Server	114.114.114	]					
VPN	Enable NAT							



WAN Setting				
Item	Description	Default		
Enable	Enable WAN function	Enable		
Port	The port that is currently set as WAN port.	GE 0		
Connection	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP		

Туре		
MTU	Set the maximum transmission unit.	1500
Primary DNS Server	Set the primary DNS.	Null
Secondary DNS Server	Set the secondary DNS.	Null
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Table 3-3-1-2 WAN Parameters

# 1. Static IP Configuration

If the external network assigns a fixed IP for the WAN interface, user can select "Static IP" mode.

URSAL	INK						
				For your device secur	ity, please change	the default password	
Status		Port WAN	LAN	VLAN Trunk	Cellular	Loopback	
LoRaWAN	۲	Enable		8			
Network	-	Port Connection Type		GE 0 Static IP	Ŧ		
Interface		IP Address		192.168.23.141			
Firewall		Netmask		255.255.255.0			
QoS		Gateway		192.168.23.1			
		MTU		1500			
DHCP		Primary DNS Server		8.8.8.8			
DDNS		Secondary DNS Server		114.114.114.114			
Link Failover		Enable NAT		2			
VPN		Multiple IP Address					
			IP Addres	\$		Netmask	Operation
System	۲						•

Figure 3-3-1-3

Static IP					
Item	Description	Default			
IP Address	Set the IP address which can access Internet. E.g. 192.168.1.2.	192.168.0.1			
Netmask	Set the Netmask for WAN port.	255.255.255.0			
Gateway	Set the gateway's IP address for WAN port.	192.168.0.2			
Multiple IP Address	Set the multiple IP addresses for WAN port.	Null			

Table 3-3-1-3 Static Parameters

# 2. DHCP Client

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, user can select "DHCP client" mode to obtain IP address automatically.

				For your device sec	urity, please change th	re default password	
Status	Port	WAN	LAN	VLAN Trunk	Cellular	Loopback	
LoRaWAN 🕨	— WAN_	1					
Network 🔫	Port			Ø GE 0			
Interface							
Firewall	Conne	Connection Type			DHCP Client		
QoS	Use F	eer DNS					
DHCP	Prima	ry DNS Server		8.8.8.8	8.8.8.8		
DDNS		Secondary DNS Server			114.114.114.114		
Link Failover	Enabl	e NAT		2			
VPN	Save 8						



DHCP Client				
Item	Description			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.			
Table 3-3-1-4 DHCP Client Parameters				

# 3. PPPoE

PPPoE refers to a point to point protocol over Ethernet. User has to install a PPPoE client on the basis of original connection way. With PPPoE, remote access devices can get control of each user.

		For your device sect	urity, please change	the default passwo
Status	Port WAN LAN	VLAN Trunk	Cellular	Loopback
DRaWAN 🕨	— WAN_1			
etwork 🔻	Enable	8		
Interface	Port	GE 0		
Firewall	Connection Type	PPPoE	•	
	Username			
QoS	Password			
DHCP	Link Detection Interval(s)	60		
DDNS	Max Retries	0		
DUNS	МТО	1500		
Link Failover	Use Peer DNS			
VPN	Primary DNS Server	8.8.8.8		
system 🕨	Secondary DNS Server	114.114.114.11	14	
ystem	Enable NAT			



PPPoE				
Item	Description			
Username	Enter the username provided by your Internet Service Provider (ISP).			
Password	Enter the password provided by your Internet Service Provider (ISP).			
Link Detection Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.			
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.			

Table 3-3-1-5 PPOE Parameters

# 3.3.1.3 LAN

LAN setting is used for managing local area network devices connected to LAN port of the UG85, allowing each device to access the Internet.

Click  $\times$  to delete the existing LAN port setting. Click  $\pm$  to add a new LAN port setting.

Port	LAN	VLAN Trunk	Cellular	Loopback		
LAN Settin	Port	IP Address		Netmask	MTU	Operation
GE	٠	192.168.23.47	255.	255.255.0	1500	×
						8

Figure	3-3-1-6
--------	---------

LAN		
Item	Description	Default
Port	Select LAN port.	GE
IP Address	Set IP address of LAN port.	192.168.1.1
Netmask	Set Netmask of LAN port.	255.255.255.0
MTU	Set the maximum transmission unit of LAN port. Range: 68-1500.	1500

Table 3-3-1-6

### 3.3.1.4 VLAN Trunk

VLAN is a kind of new data exchange technology that realizes virtual work groups by logically dividing the LAN device into network segments.

Client 🔀 to delete the current VLAN setting. Click 🕂 to add a new VLAN port.

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback		
VLAN Sett	ings						
1	Enable	Interfac	e	VID	IP Address	Netmask	Operation
	0	GE 0	•			255.255.255.0	×
							•



VLAN Trunk		
Item	Description	
Enable	The gateway can encapsulate or decapsulate the virtual LAN tag when this function is enabled.	
Interface	Select the VLAN interface from the LAN ports.	
VID	Set the label ID of the VLAN. Range: 1-4094.	
IP Address	Set VLAN port's IP address.	
Netmask	Set VLAN port's netmask.	

Table 3-3-1-7 VLAN Trunk Parameters

### 3.3.1.5 WLAN (Only Applicable to Wi-Fi Version)

This section explains how to set the related parameters for Wi-Fi network. UG85 supports 802.11 b/g/n/ac, as AP or client mode.

#### UG85 User Guide

Port	WAN	LAN	VLAN Trunk		WLAN	Cellular	Loopback
WLAN							
Enable							
Work Mode	e	AP		•			
SSID Broa	dcast						
AP Isolatio	n						
Radio Type	e	802	.11ac	•			
Channel		Aut	0	•			
SSID		test					
BSSID		24:e	1:24:f0:00:f3				
Encryption	Mode	No	Encryption	•			
Bandwidth		801	ЛНz				
Max Client	Number	100					
			Figure 3-2-1-8				
IP Setting							
Protocol		Sta	atic IP	٣	]		
IP Address	3	192	. 168.232.1		]		
Netmask		255	255 255 0		]		

### Figure 3-2-1-9

WLAN Settings		
Item	Description	
Enable	Enable/disable WLAN.	
Work Mode	Select gateway's work mode. The options are "Client" or "AP".	
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".	
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can be filled to joint the network.	
SSID	Fill in the SSID of the access point.	
Client Mode		
Scan	Click "Scan" button to search the nearby access point.	
SSID	Show SSID.	
Channel	Show wireless channel.	
Signal	Show wireless signal.	

BSSID	Show the MAC address of the access point.
Security	Show the encryption mode.
Frequency	Show the frequency of radio.
Join Network	Click the button to join the wireless network.
AP Mode	
	When SSID broadcast is disabled, other wireless devices can't not
SSID Broadcast	find the SSID, and users have to enter the SSID manually to access
	to the wireless network.
AP Isolation	When AP isolation is enabled, all users which access to the AP are
AP ISOIdUOII	isolated without communication with each other.
Radio Type	Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g
	(2.4 GHz)", "802.11n (2.4 GHz)", "802.11 n (5 GHz)" and "802.11 ac (5 GHz)".
Channel	Select wireless channel. The options are "Auto", "1", "2""13".
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
Кеу	Fill the pre-shared key of WPA encryption.
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
	Set the maximum number of client to access when the gateway is
Max Client Number	configured as AP.
IP Setting	
Protocol	Set the IP address in wireless network.
IP Address	Set the IP address in wireless network.
Netmask	Set the netmask in wireless network.
Gateway	Set the gateway in wireless network.

Table 3-3-1-8 WLAN Parameters

### **Related Topic**

Wi-Fi Application Example

### 3.3.1.6 Cellular (Only Applicable to Cellular Version)

This section explains how to set the related parameters for cellular network. The UG85 LoRaWAN gateway has two cellular interfaces, namely SIM1 and SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, then SIM1 interface takes precedence by default.

A typical use case would be to have SIM1 configured as the primary cellular interface and SIM2 as a backup. If the UG85 cannot connect to the network via SIM1, it will automatically fail over to SIM2.

Port	WAN	LAN	VLAN Trunk	Cellula	r Lo	oopback
Cellular Se	tting					
		SIM1		SIN	12	
Enable						
Network Typ	be			•		•
APN						
Username						
Password						
Access Nun	nber					
PIN Code						
Authenticati	on Type	Auto		• A	uto	•
Roaming						
SMS Center	r					

Figure 3-3-1-10

0	
8.8.8.8	
114.114.114.114	
5	
20	%
PDU	•
	<ul> <li>8.8.8</li> <li>114.114.114</li> <li>5</li> <li>20</li> </ul>

Figure 3-3-1-11

General Settings			
Item	Description	Default	
Enable	Check the option to enable the corresponding SIM card.	Enable	
Network Type	<ul> <li>Select from "Auto", "4G First", "4G Only", "3G First", "3G</li> <li>Only", "2G First", and "2G Only".</li> <li>Auto: connect to the network with the strongest signal automatically.</li> <li>4G First: 4G network takes precedence.</li> </ul>	Auto	

	4G Only: connect to 4G network only.	
	And so on.	
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.	Null
Username	Enter the username for cellular dial-up connection provided by local ISP.	Null
Password	Enter the password for cellular dial-up connection provided by local ISP.	Null
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.	Null
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.	Null
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".	Auto
Roaming	Enable or disable roaming.	Disable
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.	Null
Enable NAT	Enable or disable NAT function.	Enable
Restart When Dial-up failed	When this function is enabled, the gateway will restart automatically if the dial-up fails several times.	Disabled
ICMP Server	Set the ICMP detection server's IP address.	8.8.8.8
Secondary ICMP Server	Set the secondary ICMP detection server's IP address.	114.114.114.114
PING Times	Set PING packet numbers in each ICMP detection.	5
Packet Loss Rate	Set packet loss rate in each ICMP detection. ICMP detection fails when the preset packet loss rate is exceeded.	20

Table 3-3-1-9 Cellular Parameters

Connection Setting		
Connection Mode	Connect on Demand	•
Redial Interval(s)	5	
Max Idle Time(s)	60	
Triggered by Call		
Triggered by SMS		
Triggered by IO	0	
Dual SIM Strategy		
Primary SIM Card	SIM1	۳
Switch to backup SIM card when ICM detection fails	P	
Swtich to backup SIM card when the connection fails		
Switch to backup SIM card when roaming is detected		

Figure 3-3-1-12

Item	Description	
Connection Mode		
Connection Mode	Select from "Always Online" and "Connect on Demand".	
Connect on	"Connect on Demand" includes "Triggered by Call", "Triggered by	
Demand	SMS", and "Triggered by IO".	
	The gateway will switch from offline mode to cellular network	
Triggered by Call	mode automatically when it receives a call from the specific phone	
	number.	
Call Group	Select a call group for call trigger. Go to "System > General >	
Call Group	Phone" to set up phone group.	
	The gateway will switch from offline mode to cellular network	
Triggered by SMS	mode automatically when it receives a specific SMS from the	
	specific mobile phone.	
SMS Group	Select a SMS group for trigger. Go to "System > General > Phone" to	
Sivis Group	set up SMS group.	
SMS Text	Fill in the SMS content for triggering.	
	The gateway will switch from offline mode to cellular network	
Triggered by IO	mode automatically when the DI status is changed. Go to	
	"Industrial > $I/O$ > DI" to configure trigger condition.	
Dual SIM Strategy		
Current SIM Card	Select between "SIM1" and "SIM2" as a current SIM card used.	
Switch to backup	The gateway will switch to the backup SIM card when packet loss	
SIM card when	The gateway will switch to the backup SIM card when packet loss	
ICMP detection fails	rate in IMCP detection exceeds the preset value.	
Switch to backup	The gateway will switch to the backup SIM card when the primary	

SIM card when the connection fails	one fails to connect with cellular network.
Switch to backup SIM card when roaming is detected	The gateway will switch to the backup SIM card when the primary one is roaming.

Table 3-3-1-10 Cellular Parameters

# **Related Topics**

Cellular Connection Application Example Dual SIM Backup Application Example Phone Group

### 3.3.1.7 Loopback

Loopback interface is used for replacing gateway's ID as long as it is activated. When the interface is DOWN, the ID of the gateway has to be selected again which leads to long convergence time of OSPF. Therefore, Loopback interface is generally recommended as the ID of the gateway.

Loopback interface is a logic and virtual interface on gateway. Under default conditions, there's no loopback interface on gateway, but it can be created as required.

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback	
Loopback	Address					
IP Address		127.	0.0.1			
Netmask		255.	0.0.0			
Multiple IP	Addresses					
	IP A	ddress		Netm	ask	Operation
			]	255.255.255.255		×
						B

Figure 3-3-1-13

Loopback					
Item	Description	Default			
IP Address	Unalterable	127.0.0.1			
Netmask	Unalterable	255.0.0.0			
Multiple IP Addresses	Apart from the IP above, user can configure other IP addresses.	Null			

Table 3-3-1-11 Loopback Parameters

# 3.3.2 Firewall

This section describes how to set the firewall parameters, including website block, ACL, DMZ, Port Mapping and MAC Binding.

The firewall implements corresponding control of data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of packets, such as protocol style, source/destination IP address, etc. It ensures that the gateway operate in a safe environment and host in local area network.

# 3.3.2.1 Security

URSALIN	IK					
Status	Security	ACL	DMZ	Port Mapping	MAC Bindin	ıg
LoRaWAN		king by URL Ac	ldress			
Network	URL Address		http://		× +	
Interface	Website Bloc	king by Keywor	rd			
Firewall	Keyword			2	×	
QoS					Ŧ	
DHCP	Save					



Website Blocking	
URL Address	Enter the HTTP address which you want to block.
Keyword	You can block specific website by entering keyword. The maximum number of character allowed is 64.

Table 3-2-2-1 Security Parameters

### 3.3.2.2 ACL

Access control list, also called ACL, implements permission or prohibition of access for specified network traffic (such as the source IP address) by configuring a series of matching rules so as to filter the network interface traffic. When gateway receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.

#### UG85 User Guide

Status		ACL	DMZ	Port Mapping	MAC Binding		
LoRaWAN	Þ	ACL Setting		Accept	¥		
Network	•	Access Co		Ассерг			
Interface				Туре	extended	•	
Firewall				ID			
BUGB				Action	permit	*	
DHCP				Protocol	ip	T	
DDNS				Source IP			
Link Failover				Source Wildcard Mask	0.0.0.0		
VPN				Destination IP			
VI IN				Destination Wildcard Mas	.k 0,0.0,0		
System	•			Description			
Industrial	۲			S	ave Cancel	U)	
Maintenance	Þ	Interface Li	st				
маппепапсе			Interface	h	ACL	Out ACL	Operation
APP	Þ						•

Figure 3-3-2-2

Item	Description
ACL Setting	
	Select from "Accept" and "Deny".
Default Filter Policy	The packets which are not included in the access control list will be
	processed by the default filter policy.
Access Control List	
Туре	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ІСМР Туре	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.

Start Destination Port Set start destination port number. Range: 1-65535.				
End Destination Port Set end destination port number. Range: 1-65535.				
More Details	bre Details Show information of the port.			
Interface List				
Interface	Select network interface for access control.			
In ACL	Select a rule for incoming traffic from ACL ID.			
Out ACL	Select a rule for outgoing traffic from ACL ID.			

Table 3-3-2-2 ACL Parameters

# 3.3.2.3 DMZ

DMZ is a host within the internal network that has all ports exposed, except those forwarded ports in port mapping.

ACL	DMZ	Port Mapping	MAC Binding	
DMZ				
Enable				
DMZ Host				
Source Add	ress			

Figure 3-3-2-3

DMZ	
Item	Description
Enable	Enable or disable DMZ.
DMZ Host	Enter the IP address of the DMZ host on the internal network.
Source Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

Table 3-3-2-3 DMZ Parameters

### 3.3.2.4 Port Mapping

Port mapping is an application of network address translation (NAT) that redirects a communication request from the combination of an address and port number to another while the packets are traversing a network gateway such as a gateway or firewall.

Click  $\blacksquare$  to add a new port mapping rules.

ACL	DMZ	Port	Mapping	MAC Bindin	g		
Port M	lapping						
	Source IP	Source Port	Destination IP	Destinati on Port	Protocol	Description	Operation
0.0.0	0.0/0				TCP T		
							•



Port Mapping	Port Mapping				
Item Description					
Source IP	Specify the host or network which can access local IP address.				
	0.0.0/0 means all.				
Source Port	Enter the TCP or UDP port from which incoming packets are				
Source Fort	forwarded. Range: 1-65535.				
Destination IP	Enter the IP address that packets are forwarded to after being				
Destination iP	received on the incoming interface.				
Destination Port	Enter the TCP or UDP port that packets are forwarded to after				
Destination Port	being received on the incoming port(s). Range: 1-65535.				
Protocol	Select from "TCP" and "UDP" as your application required.				
Description	The description of this rule.				

Table 3-3-2-4 Port Mapping Parameters

# **Related Configuration Example**

NAT Application Example

# 3.3.2.5 MAC Binding

MAC Binding is used for specifying hosts by matching MAC addresses and IP addresses that are in the list of allowed outer network access.

ACL	DMZ	Port Mapping	MAC Binding		
MAC Bi	inding List				
	MAC Address	IP Ad	dress	Description	Operation
					×
					Œ

Figure 3-3-2-5

MAC Binding List						
Item	Description					
MAC Address	Set the binding MAC address.					
IP Address	Set the binding IP address.					
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.					

Table 3-3-2-5 MAC Binding Parameters

# 3.3.3 QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS is engineered to provide different priority for different applications, users, data flows, or to guarantee a certain level of performance to a data flow.

URSALI	NK								
				For your device sec	urity, please change the	default password			
Status	Î	QoS(Download)	QoS(Upload)						
LoRaWAN	•	Download Bandwidth							
Network	-	Enable Default Class		Ŧ					
Interface		Download Bandwidth Capacity	0	kbits/s					
Firewall		Service Class							
QoS		Name		Percent(%)	Max BW(I	(bps)	Min BW(	(bps)	Operation
DHCP									
DDNS		Service Class Rules							
Link Failover		Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Class	Operation
VPN									•

Figure 3-3-3-1

QoS			
Item	Description		
Download/Upload			
Enable	Enable or disable QoS.		
Default Class	Select default class from Service Class list.		
Download/Upload The download/upload bandwidth capacity of the network			
Bandwidth Capacity	the gateway is connected with, in kbps. Range: 1-8000000.		
Service Classes			
Name	Give the service class a descriptive name.		
Percent (%)	The amount of bandwidth that this class should be guaranteed		
	in percentage. Range: 0-100.		
	The maximum bandwidth that this class is allowed to		
Max BW(kbps)	consume, in kbps. The value should be less than the		
	"Download/Upload Bandwidth Capacity".		

Min BW(kbps)	The minimum bandwidth that can be guaranteed for the class, in kbps. The value should be less than the "MAX BW" value.
Service Class Rules	
Item	Description
Name	Give the rule a descriptive name.
Source IP	Source address of flow control (leaving it blank means any).
Source Port	Source port of flow control. Range: 0-65535 (leaving it blank means any).
Destination IP	Destination address of flow control (leaving it blank means any).
Destination Port	Destination port of flow control. Range: 0-65535 (leaving it blank means any).
Protocol	Select protocol from "ANY", "TCP", "UDP", "ICMP", and "GRE".
Service Class	Set service class for the rule.

Table 3-3-3-1 QoS (Download/Upload) Parameters

# 3.3.4 DHCP

DHCP adopts Client/Server communication mode. The Client sends configuration request to the Server which feeds back corresponding configuration information and distributes IP address to the Client so as to achieve the dynamic configuration of IP address and other information.

### 3.3.4.1 DHCP Server

The UG85 can be set as a DHCP server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent.

Status	Î	HCP Server	DHCP Relay				
LoRaWAN	•	DHCP Server_1  Enable		ø			
Network	-	Interface		GE 0	¥		
Interface		Start Address		192.168.23.100			
Firewall		End Address Netmask		192.168.23.199 255.255.255.0			
QoS		Lease Time(Min)		1440			
DHCP		Primary DNS Serve	er	114.114.114.114			
DDNS		Secondary DNS Se					
Link Failover		Static IP					
VPN		State IP	MAC Addres	s		IP Address	Operation
System	•						

Figure 3-3-4-1

DHCP Server		
ltem	Description	Default
Enable	Enable or disable DHCP server.	Enable
Interface	Select interface, e.g. GE.	GE
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	114.114.114.114
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

Table 3-3-4-1 DHCP Server Parameters

# 3.3.4.2 DHCP Relay

The UG85 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

DHCP Server	DHCP Relay	
DHCP Relay		
Enable		
DHCP Server		

Figure 3-3-4-2

DHCP Relay	
Item	Description
Enable	Enable or disable DHCP relay.
DHCP Server	Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".

Table 3-3-4-2 DHCP Relay Parameters

### 3.3.5 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name.

DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

Status	Î	DDNS										
LoRaWAN		DDNS Method	List									
Network	-	Name	Interface	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Appe nd IP	
Interface												•
Firewall		Save										
QoS												
DHCP												
DDNS												

#### Figure 3-3-5-1

DDNS	
Item	Description
Name	Give the DDNS a descriptive name.
Interface	Set interface bundled with the DDNS.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.

Table 3-3-5-1 DDNS Parameters

### 3.3.6 Link Failover

This section describes how to configure link failover strategies, such as VRRP strategies.

### **Configuration Steps**

- 1. Define one or more SLA operations (ICMP probe).
- 2. Define one or more track objects to track the status of SLA operation.
- 3. Define applications associated with track objects, such as VRRP or static routing.

### 3.3.6.1 SLA

SLA setting is used for configuring link probe method. The default probe type is ICMP.

	SLA	Track	VRRP	WAN Failover							
Interface	SLA Entry										
Firewall				Secondary					Packet		
QoS	ID	Туре	Destination Address	Destination Address	Data Size	Interval(s)	Timeout( ms)	PING Times	Loss Rate	Start Time	Operatio
онср	1	icmp-echo 🔻	114.114.114.114	8.8.8.8	56	30	5000	5	20	now 🔻	×
DDNS											Ð
Link Failover											
	Save										

Figure	3.	3-	6-1
i igui c	-	-	• •

SLA					
Item	Description	Default			
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1			
Туре	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo			
Destination Address	The detected IP address.	114.114.114.114			
Secondary Destination Address	The secondary detected IP address.	8.8.8.8			
Data Size	User-defined data size. Range: 0-1000.	56			
Interval (s)	User-defined detection interval. Range: 1-608400.	30			
Timeout (ms)	User-defined timeout for response to determine ICMP detection failure. Range: 1-300000.	5000			
PING Times	Define PING packet numbers in each SLA probe. Range: 1-1000.	5			
Packet Loss Rate	Define packet loss rate in each SLA probe. SLA probe fails when the preset packet loss rate is exceeded.	20			
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA detection doesn't start.	now			

Table 3-3-6-1 SLA Parameters

### 3.3.6.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and Application module. Track setting is located between application module and SLA module with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

### Linkage between Track Module and SLA module

Once you complete the configuration, the linkage relationship between Track module and SLA module will be established. SLA module is used for detection of link status, network performance and notification of Track module. The detection results help track status change

timely.

- For successful detection, the corresponding track item is Positive.
- For failed detection, the corresponding track item is Negative.

### Linkage between Track Module and Application Module

After configuration, the linkage relationship between Track module and Application module will be established. When any change occurs in track item, a notification that requires corresponding treatment will be sent to Application module.

Currently, the application modules like VRRP and static routing can get linkage with track module.

If it sends an instant notification to Application module, the communication may be interrupted in some circumstances due to routing's failure like timely restoration or other reasons. Therefore, user can set up a period of time to delay notifying application module when the track item status changes.

SLA	Track	VRRP	WAN Failover			
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	• <u>1</u> •	cellular0 •	0	1	×
						æ

Figure 3-3-6-2

Item	Description	Default
Index	Track index. Up to 10 track settings can be configured. Range: 1-10.	1
Туре	The options are "sla" and "interface".	SLA
SLA ID	Defined SLA ID.	1
Interface	Select the interface whose status will be detected.	cellular0
Negative Delay (s)	When interface is down or SLA probing fails, it will wait according to the time set here before actually changing its status to Down. Range: 0-180 (0 refers to immediate switching).	0
Positive Delay (s)	When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate switching).	1

Table 3-3-6-2 Track Parameters

#### 3.3.6.3 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating

hosts. This increases the availability and reliability of routing paths via automatic default gateway selections in an IP sub-network.

URSALI	NK						
					For your device secur	ity, please change the default passv	word
	-	SLA	Track	VRRP	WAN Failover		
Interface		2012/2012					
Firewall		VRRP Statu Status	S	DISA	01 F		
QoS				DISA	BLE		
405		VRRP Settir	igs				
DHCP		Enable					
DDNS		Virtual Route	15	GE	0	*	
	_		riD				
Link Failover		Virtual IP					
VPN		Priority		100			
		Advertiseme	nt Interval(s)	1			
System		Preemption I	Node				
1 4 44 1		Track ID				Ŧ	
Industrial							
Maintenance	•	Save	-1				

Figure 3-3-6-3

VRRP		
Item	Description	Default
Enable	Enable or disable VRRP.	Disable
Interface	Select the interface of Virtual Router.	None
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.	None
Virtual IP	Set the IP address of Virtual Router.	None
	The VRRP priority range is 1-254 (a bigger number indicates a	
Priority	higher priority). The router with higher priority will be more likely to become the gateway router.	100
Advertisement Interval (s)	Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.	1
Preemption Mode	If the gateway works in the preemption mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Disable
Track ID	Trace detection, select the defined track ID or blank character.	None

Table 3-3-6-3 VRRP Parameters

#### 3.3.6.4 WAN Failover

WAN failover refers to failover between Ethernet WAN interface and cellular interface. When service transmission can't be carried out normally due to malfunction of a certain interface or lack of bandwidth, the rate of flow can be switched to backup interface quickly. Then the backup interface will carry out service transmission and share network flow so as to improve reliability of communication of data equipment.

When link state of main interface is switched from up to down, system will have the pre-set delay works instead of switching to link of backup interface immediately. Only if the state of main interface is still down after delay, will the system switch to link of backup interface. Otherwise, system will remain unchanged.

URSALINK									
					For your device secur	ity, please change the de	efault password		
2442 Bi	•	SLA	Track	VRRP	WAN Failover				
Interface		WAN Failove			-				
Firewall									
QoS		Main Inte	rface B	ackup Interface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
		Cellular 0	▼ G	E0 T	30	0	0	1 •	×
DHCP									•
DDNS									
Link Failover		Save							
VPN									

Figure	3-3-6-4
--------	---------

WAN Failover		
Parameters	Description	Default
Main Interface	Select a link interface as the main link.	Cellular0
Backup Interface	Select a link interface as the backup link.	GE0
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	3
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0
Down Delay (s)	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0
Track ID	Track detection, select the defined track ID.	1

Table 3-3-6-4 WAN Failover Parameters

# 3.3.7 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.

The UG85 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

### 3.3.7.1 DMVPN

A dynamic multi-point virtual private network (DMVPN), combining mGRE and IPsec, is a secure network that exchanges data between sites without passing traffic through an organization's headquarter VPN server or gateway.

				For your	device see
tatus	DMVPN	IPsec	GRE	L2TP	PPTP
	DMVPN Set	ttings			
oRaWAN	Enable			8	
letwork	Hub Addres	S			
	Local IP Ad	dress			
Interface	GRE HUB I	P Address			
Firewall	GRE Local	IP Address			
	GRE Mask			255.255.255.0	
QoS	GRE Key				
DHCP	Negotiation	Mode		Main	,
	Authenticat	ion Algorithm		DES	,
DDNS	Encryption	Algorithm		MD5	,
Link Failover	DH Group			MODP768-1	,
	Key				
VPN	Local ID Ty	pe		Default	
/stem	IKE Life Tin	ne(s)		10800	
	SA Algorith	m		DES-MD5	,
dustrial )	PFS Group			NULL	,

Figure 3-3-7-1

VPN	DPD Time Interval(s)	30
	DPD Timeout(s)	150
System	Cisco Secret	
Industrial	NHRP Holdtime(s)	7200



DMVPN	
Item	Description
Enable	Enable or disable DMVPN.
Hub Address	The IP address or domain name of DMVPN Hub.
Local IP address	DMVPN local tunnel IP address.
GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Algorithm	
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and
ынаюцр	"MODP1536_5".
Кеу	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",
	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and
	"AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and
	"MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of Nhrp protocol.

Table 3-3-7-1 DMVPN Parameters

# 3.3.7.2 IPSec

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that

security arrangements can be handled without requiring changes to individual user computers.

IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code exchange. All of them can protect one and more data flows between hosts, between host and gateway, and between gateways.

DMVPN	IPsec	GRE	L2TP	PPTP
IPsec Settings	5			
- IPsec_1				
Enable				
IPsec Gat	teway Address			
IPsec Mo	de	Т	unnel	•
IPsec Pro	tocol	E	SP	•
Local Sub	onet			
Local Sub	onet <mark>Ma</mark> sk			
Local ID 1	Гуре	D	efault	•
Remote S	Subnet			
Remote S	Subnet Mask			
Remote II	D Type	D	efault	•

Figure 3-3-7-3

IPsec	
Item	Description
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.
IPsec Mode	Select from "Tunnel" and "Transport".
IPsec Protocol	Select from "ESP" and "AH".
Local Subnet	Enter the local subnet IP address that IPsec protects.
Local Subnet Netmask	Enter the local netmask that IPsec protects.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN".
Remote Subnet	Enter the remote subnet IP address that IPsec protects.
Remote Subnet Mask	Enter the remote netmask that IPsec protects.
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".
	Table 2 2 7 2 IDeac Darameters

Table 3-3-7-2 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	•
Negotiation Mode	Main	•
Encryption Algorithm	DES	•
Authentication Algorithm	MD5	•
DH Group	MODP768-1	¥
Local Authentication	PSK	•
Local Secrets		
XAUTH		
Lifetime(s)	10800	
SA Parameter		
SA Algorithm	DES-MD5	×
PFS Group	NULL	•
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced		
Enable Compression		
VPN Over IPsec Type	NONE	•



IKE Parameter		
Item	Description	
IKE Version	Select from "IKEv1" and "IKEv2".	
Negotiation Mode	Select from "Main" and "Aggressive".	
<b>Encryption Algorithm</b>	Select from "DES", "3DES", "AES128", "AES192" and "AES256".	
Authentication Algorithm	Select from "MD5" and " SHA1"	
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".	
Local Authentication	Select from "PSK" and "CA".	
Local Secrets	Enter the preshared key.	
XAUTH	Enter XAUTH username and password after XAUTH is enabled.	
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.	
SA Parameter		
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",	
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5",	
	"AES192_SHA1", "AES256_MD5" and "AES256_SHA1".	
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and	
	"MODP1536_5".	
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.	

DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.

Table 3-3-7-3 IPsec Parameters

### 3.3.7.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message can be transmitted and encapsulation and decapsulation can be realized at both ends.

In the following circumstances the GRE tunnel transmission can be applied:

- GRE tunnel can transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.

	DMVPN	IPsec	GRE	L2TP	PPTP
Þ	GRE Settings				
	- GRE_1				
	Enable				
	Remote IF	<sup>D</sup> Address			
	Local IP A	Address	1		
	Local Virt	ual IP Address			
	Netmask		2	255.255.255.0	
	Peer Virtu	al IP Address			
	Global Tra	affic Forwarding			
	Remote S	Subnet			
	Remote N	letmask			
	MTU		1	1500	
	Key				
	Enable N/	AT			

Figure 3-3-7-5

GRE	
Item	Description
Enable	Check to enable GRE function.

Remote IP Address	Enter the real remote IP address of GRE tunnel.
Local IP Address	Set the local IP address.
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.
Netmask	Set the local netmask.
Peer Virtual IP Address	Enter remote tunnel IP address of GRE tunnel.
Global Traffic	All the data traffic will be sent out via GRE tunnel when this
Forwarding	function is enabled.
Remote Subnet	Enter the remote subnet IP address of GRE tunnel.
Remote Netmask	Enter the remote netmask of GRE tunnel.
MTU	Enter the maximum transmission unit. Range: 64-1500.
Кеу	Set GRE tunnel key.
Enable NAT	Enable NAT traversal function.

Table 3-3-7-4 GRE Parameters

# 3.3.7.4 L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

DMVPN	IPsec	GRE	L2TP	PPTP
L2TP Settings				
— L2TP_1				
Enable				
Remote IP	Address			
Username				
Password				
Authentica	tion	A	uto	•
Global Trat	ffic Forwarding			
Remote Su	ıbnet			
Remote Su	ıbnet Mask			
Key				



L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and

	"MS-CHAPv2".
Global Traffic	All of the data traffic will be sent out via L2TP tunnel after this
Forwarding	function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Кеу	Enter the password of L2TP tunnel.

Table 3-3-7-5 L2TP Para	ameters
-------------------------	---------

Advanced Settings	
Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-3-7-7

Advanced Settings		
Item	Description	
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP	
Local IP Address	address automatically from the server when it's null.	
Peer IP Address	Enter tunnel IP address of L2TP server.	
Enable NAT	Enable NAT traversal function.	
Enable MPPE	Enable MPPE encryption.	
Address/Control	For PPP initialization. User can keep the default option.	
Compression	For FFF initialization. Oser can keep the default option.	
Protocol Field	For PPP initialization. User can keep the default option.	
Compression		
Asyncmap Value	One of the PPP protocol initialization strings. User can keep	
	the default value. Range: 0-ffffffff.	
MRU	Set the maximum receive unit. Range: 64-1500.	
MTU	Set the maximum transmission unit. Range: 64-1500	
Link Dotaction Interval (c)	Set the link detection interval time to ensure tunnel	
Link Detection Interval (s)	connection. Range: 0-600.	
Max Retries	Set the maximum times of retry to detect the L2TP connection	

	failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-3-7-6 L2TP Parameters

# 3.3.7.5 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network.

DMVPN	IPsec	GRE	L2TP	PPTP
PPTP Settings	5			
- PPTP_1				
Enable				
Remote II	P Address			
Username	е			
Password	I			
Authentic	ation	Ą	Auto	•
	affic Forwarding			
Remote S				
Remote S	Subnet Mask			



РРТР				
Item	Description			
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.			
Remote IP Address	Enter the public IP address or domain name of PPTP server.			
Username	Enter the username that PPTP server provides.			
Password	Enter the password that PPTP server provides.			
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".			
Global Traffic	All of the data traffic will be sent out via PPTP tunnel once			
Forwarding	enable this function.			
Remote Subnet	Set the peer subnet of PPTP.			
Remote Subnet Mask	Set the netmask of peer PPTP server.			

Table 3-3-7-7 PPTP Parameters

Advanced Settings	
Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-3-7-9

PPTP Advanced Settings				
Item	Description			
Local IP Address	Set IP address of PPTP client.			
Peer IP Address	Enter tunnel IP address of PPTP server.			
Enable NAT	Enable the NAT faction of PPTP.			
Enable MPPE	Enable MPPE encryption.			
Address/Control Compression	For PPP initialization. User can keep the default option.			
Protocol Field Compression	For PPP initialization. User can keep the default option.			
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.			
MRU	Enter the maximum receive unit. Range: 0-1500.			
MTU	Enter the maximum transmission unit. Range: 0-1500.			
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.			
Max Retries	Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.			
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.			

Table 3-3-7-8 PPTP Parameters

### 3.3.7.6 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. Advantages of OpenVPN include:

- Security provisions that function against both active and passive attacks.
- Compatibility with all major operating systems.
- High speed (1.4 megabytes per second typically).
- Ability to configure multiple servers to handle numerous connections simultaneously.
- All encryption and authentication features of the OpenSSL library.
- Advanced bandwidth management.
- A variety of tunneling options.
- Compatibility with smart cards that support the Windows Crypt application program interface (API).

MVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifica
enVPN Clien	t Settings						
- OpenVPN_	1						
Enable							
Protocol		UDF	•	¥			
Remote IP	Address						
Port		1194					
Interface		tun		•			
Authenticat	tion	Non	e	¥			
Local Tunn	el IP						
Remote Tu	nnel IP						
Enable NA	т						
Compressi	on	LZC		٣			
Link Detect	tion Interval(s)	60					
Link Detect	tion Timeout(s)	300					
Cipher		Non	e	×			
MTU		1500	1				
Max Frame	Size	1500	1				
Verbose Le	evel	ERF	OR	Ŧ			
Expert Opti	ions						
Local Rou	te						
		Subnet			Subnet Mas	;k	Operation
							8

Figure 3-3-7-10

OpenVPN Client	
Item	Description
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.

Protocol	Select from "UDP" and "TCP".				
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.				
Remote in Address	Enter the listening port number of remote OpenVPN server.				
Port	Range: 1-65535.				
Interface	Select from "tun" and "tap".				
	Select from "None", "Pre-shared", "Username/Password",				
Authentication	"X.509 cert", and "X.509 cert+user".				
Local Tunnel IP	Set local tunnel address.				
Remote Tunnel IP	Enter remote tunnel address.				
Global Traffic	All the data traffic will be sent out via OpenVPN tunnel when				
Forwarding	this function is enabled.				
Enable TLS	Check to enable TLS authentication.				
Authentication					
Username	Enter username provided by OpenVPN server.				
Password	Enter password provided by OpenVPN server.				
Enable NAT	Enable NAT traversal function.				
Compression	Select LZO to compress data.				
Link Detection Interval	Set link detection interval time to ensure tunnel connection.				
(s)	Range: 10-1800.				
Link Detection Timeout	Set link detection timeout. OpenVPN will be reestablished after				
(s)	timeout. Range: 60-3600.				
Cipher	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC",				
cipiici	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".				
MTU	Enter the maximum transmission unit. Range: 128-1500.				
Max Frame Size	Set the maximum frame size. Range: 128-1500.				
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".				
Expert Options	User can enter some other PPP initialization strings in this field				
	and separate the strings with blank space.				
Local Route					
Subnet	Set the local route's IP address.				
Subnet Mask	Set the local route's netmask.				

Table 3-3-7-9 OpenVPN Client Parameters

# 3.3.7.7 OpenVPN Server

The UG85 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server
OpenVPN Ser	ver Settings					
Enable						
Protocol		UDP		*		
Port		1194				
Listening IP						
Interface		tun		Ŧ		
Authentication		None		*		
Local Virtual IP						
Remote Virtual	IP					
Enable NAT		1				
Compression		LZO		¥		
Link Detection I	nterval	60				
Cipher		None		¥		
MTU		1500				
Max Frame Size	e	1500				
Verbose Level		ERROR		•		
Expert Options						



Local Route			
	Subnet	Netmask	Operation
			•
Account			
	Username	Password	Operation
			<b>H</b>

Figure	3-3-7-12
i igui c	55712

OpenVPN Server			
Item	Description		
Enable	Enable/disable OpenVPN server.		
Protocol	Select from TCP and UDP.		
Port	Fill in listening port number. Range: 1-65535.		
Listening IP	Enter WAN IP address or LAN IP address. Leaving it blank		
	refers to all active WAN IP and LAN IP address.		
Interface	Select from " tun" and "tap".		
Authentication	Select from "None", "Pre-shared", "Username/Password",		
	"X.509 cert" and "X. 509 cert +user".		
Local Virtual IP	The local tunnel address of OpenVPN's tunnel.		

Remote Virtual IP	The remote tunnel address of OpenVPN's tunnel.		
Client Subnet	Local subnet IP address of OpenVPN client.		
Client Netmask	Local netmask of OpenVPN client.		
Renegotiation Interval(s)	Set interval for renegotiation. Range: 0-86400.		
Max Clients	Maximum OpenVPN client number. Range: 1-128.		
Enable CRL	Enable CRL		
Enable Client to Client	Allow access between different OpenVPN clients.		
Enable Dup Client	Allow multiple users to use the same certification.		
Enable NAT	Check to enable the NAT traversal function.		
Compression	Select "LZO" to compress data.		
Link Detection Interval	Set link detection interval time to ensure tunnel connection.		
	Range: 10-1800.		
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",		
	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".		
MTU	Enter the maximum transmission unit. Range: 64-1500.		
Max Frame Size	Set the maximum frame size. Range: 64-1500.		
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".		
Expert Options	User can enter some other PPP initialization strings in this		
	field and separate the strings with blank space.		
Local Route			
Subnet	The real local IP address of OpenVPN client.		
Netmask	The real local netmask of OpenVPN client.		
Account			
Username & Password	Set username and password for OpenVPN client.		

Table 3-3-7-10 OpenVPN Server Parameters

# 3.3.7.8 Certifications

User can import/export certificate and key files for OpenVPN and IPsec on this page.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
OpenVPN Clier	nt						
- OpenVPN	client_1						
CA				Browse	Import Export Delet	e	
Public Key	1			Browse	Import Export Delet	e	
Private Ke	У			Browse	Import Export Delet	e	
TA				Browse	Import Export Delet	e	
Preshared	Кеу			Browse	Import Export Delet	e	
PKCS12				Browse	Import Export Delet	e	

Figure 3-3-7-13

OpenVPN Client		
Item	Description	
СА	Import/Export CA certificate file.	

Public Key	Import/Export public key file.		
Private Key	Import/Export private key file.		
ТА	Import/Export TA key file.		
Preshared Key	Import/Export static key file.		
PKCS12	Import/Export PKCS12 certificate file.		

Table 3-3-7-11 OpenVPN Client Certification Parameters

#### OpenVPN Server

-	OpenVPN Server				
	CA	Browse	Import	Export	Delete
	Public Key	Browse	Import	Export	Delete
	Private Key	Browse	Import	Export	Delete
	DH	Browse	Import	Export	Delete
	ТА	Browse	Import	Export	Delete
	CRL	Browse	Import	Export	Delete
	Preshared Key	Browse	Import	Export	Delete

#### Figure 3-3-7-14

OpenVPN Server			
Item	Description		
СА	Import/Export CA certificate file.		
Public Key	Import/Export public key file.		
Private Key	Import/Export private key file.		
DH	Import/Export DH key file.		
ТА	Import/Export TA key file.		
CRL	Import/Export CRL.		
Preshared Key	Import/Export static key file.		

Table 3-3-7-12 OpenVPN Server Parameters

IPsec				
- IPsec_1				
CA	Browse	Import	Export	Delete
Client Key	Browse	Import	Export	Delete
Server Key	Browse	Import	Export	Delete
Private Key	Browse	Import	Export	Delete
CRL	Browse	Import	Export	Delete

Figure 3-3-7-15

IPsec			
Item Description			
CA	Import/Export CA certificate.		
Client Key	Import/Export client key.		
Server Key	Import/Export server key.		
Private Key	Import/Export private key.		
CRL	Import/Export certificate recovery list.		

Table 3-3-7-13 IPsec Parameters

# 3.4 System

This section describes how to configure general settings, such as administration account, access service, system time, common user management, SNMP, AAA, event alarms, etc.

## 3.4.1 General Settings

## 3.4.1.1 General

General settings include system info, access service and HTTPS certificates.

Status		General	System Time	SMTP	Phone	Email	
LoRaWAN		System					
Network	Þ	Hostname Web Login Timeout(s)		ROUTER 1800			
System	•	Access Servio	ce				
General Settings		Sen	vice	Port	Local		Remote
User Management		HT	TP	80	۲		Ø
		НТТ	PS	443			Ø
SNMP		TEL	NET	23	•		
AAA		SS	6H	22	Ø		Ø
Device Management		HTTS Certific	ates				
Events		Certificate	https.crt	Browse	Import Export	Delete	
Industrial		Key	https.key	Browse	Import Export	Delete	
Maintenance		Save					
APP	×.						



General					
ltem	Default				
System					
Hostname	User-defined gateway name, needs to start with a letter. URSA				
Web Login	You need to log in again if it times out. Range: 100-3600.	1800			
Timeout (s)	Tou need to log in again in it times out. Nange. 100-5000.	1800			
Access Service					
Local	Access the gateway locally.	Enable			

Port	Set port number of the services. Range: 1-65535				
Remote	Access the gateway remotely.	Disable			
НТТР	HTTP Users can log in the device locally via HTTP to access and control it through Web after the option is checked.				
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	8088			
TELNET		8023			
SSH Users can log in the device locally and remotely via SSH after the option is checked.		8022			
HTTPS Certific	HTTPS Certificates				
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.				
Кеу	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.				

Table 3-4-1-1 General Setting Parameters

#### 3.4.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type.

Note: to ensure that the gateway runs with the correct time, it's recommended that you set the system time when configuring the gateway.

General	System Time	SMTP	Phone	Email
System Time S	Settings			
Current Time		2019-06-12 20:34:3	2 Wed	
Time Zone		8 China (Beijing)	¥	
Sync Type		Sync with Browser	•	
Browser Time		2019-06-12 20:34:3	2 Wed	

Figure 3-4-1-2

General	System Time	SMTP	Phone	9	Email
System Time S	ettings				
Current Time		2019-06-12 20:	33:59 Wed		
Time Zone		8 China (Beijin	ig)	•	
Sync Type		Set up Manual	lly	•	
Date		2019-06-12			
Time		20 🔻 33	• 59	•	
	Fi	gure 3-4-1-3			
General	System Time	SMTP	Phone		Email

# System Time Settings

Current Time	2019-06-12 20:33:36 Web	ł
Time Zone	8 China (Beijing)	٣
Sync Type	Sync with NTP Server	•
NTP Server Address	1.cn.pool.ntp.org	
Enable NTP Server		



System Time				
Item	Description			
Current Time	Show the current system time.			
Time Zone	Click the drop down list to select the time zone you are in.			
Sync Type	Click the drop down list to select the time synchronization type.			
Sync with Browser Synchronize time with browser.				
Browser Time Show the current time of browser.				
Set up Manually Manually configure the system time.				
Sync with NTP Server	Synchronize time with NTP server so as to achieve time			
Sync with MTP Server	synchronization of all devices equipped with a clock on network.			
Sync with NTP Server				
NTP Server Address Set NTP server address (domain name/IP).				
Enable NTP Server	NTP client on the network can achieve time synchronization with gateway after "Enable NTP Server" option is checked.			

Table 3-4-1-2 System Time Parameters

#### 3.4.1.3 SMTP

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving e-mail. This section describes how to configure email settings.

General	System Time	SMTP	Phone	Email
SMTP Client S	Settings			
Enable				
Email Address				
Password				
SMTP Server A	ddress	smtp.exmail.qq.	com	
Port		25		
Enable TLS				
	<u></u> .			
Save	Test			

Figure 3-4-1-5

SMTP		
Item	Description	
SMTP Client Settings		
Enable	Enable or disable SMTP client function.	
Email Address	Enter the sender's email account.	
Password	Enter the sender's email password.	
SMTP Server Address	Enter SMTP server's domain name.	
Port	Enter SMTP server port. Range: 1-65535.	
Enable TLS	Enable or disable TLS encryption.	

Table 3-4-1-3 SMTP Setting

#### **Related Topics**

**Events Setting** 

#### 3.4.1.4 Phone

Phone settings involve in call/SMS trigger and SMS alarm for events.

- 1. Add phone list.
- 2. Select phone numbers and add them to the phone group.
- 3. Go to "Network > Interface > Cellular > Connection Mode > Connect on Demand > Trigger by Call / Trigger by SMS" or go to "System > Events > Event Settings > SMS" and then select the phone group ID.

General	System Time	SMTP	Phone	Email		
Phone Numbe	er List					
	Number			Description		Operation
	1234567890			test		×
						Ð
Phone Group	Gro	up ID cription	1 test			
	ř	List		Selected 1234567890		
		_	Save	Cancel	Ŧ	

Figure 3-4-1-6

Phone		
Item	Description	
Phone Number List		
Number	Enter the telephone number. Digits, "+" and "-" are allowed.	
Description	The description of the telephone number.	
Phone Group List		
Group ID	Set number for phone group. Range: 1-100.	
Description	The description of the phone group.	
List	Show the phone list.	
Selected	Show the selected phone number.	

Table 3-4-1-4 Phone Settings

## **Related Topic**

Connect on Demand

#### 3.4.1.5 Email

Email settings involve email alarm for events.

- 1. Add email list.
- 2. Select email addresses and add them to the phone group.
- 3. Go to "System > Events > Event Settings > Email" and then select the email group ID.

General	System Time	SMTP	Phone	Email		
Email List						
	Email Address			Description		Operation
	support@ursalink.com			test		×
						Ð
Email Group		up ID	1		]	
	Des	cription	test		]	
		List		Selected		
				support@ursalink.com	Ŧ	
			Save	Cancel		

Figure 3-4-1-7

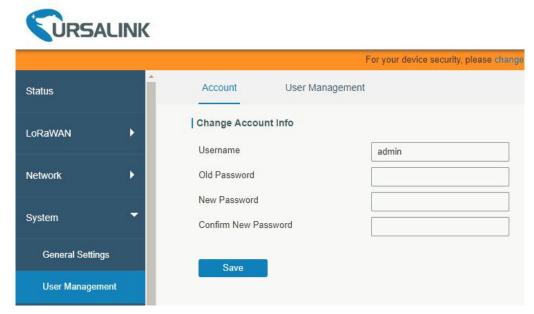
Email		
Item	Description	
Email List		
Email Address	Enter the Email address.	
Description	The description of the Email address.	
Email Group List		
Group ID	Set number for email group. Range: 1-100.	
Description	The description of the Email group.	
List	Show the Email address list.	
Selected	Show the selected Email address.	

Table 3-4-1-5 Email Settings

## 3.4.2 User Management

# 3.4.2.1 Account

Here you can change the login username and password of the administrator. Note: it is strongly recommended that you modify them for the sake of security.





Account		
Item Description		
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "\$". The first character can't be a digit.	
Old Password	Enter the old password.	
New Password	Enter a new password.	
Confirm New Password	Enter the new password again.	

Table 3-4-2-1 Account Information

#### 3.4.2.2 User Management

This section describes how to create common user accounts. The common user permission includes Read-Only and Read-Write.

Account	User Management			
User List				
	Username	Password	Permission	Operation
steve			Read-Write •	×
test		•••••	Read-Only •	×
				•



User Management		
Item	Description	
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "\$". The first character can't be a digit.	
Password	Set password.	
Permission	Select user permission from "Read-Only" and "Read-Write".	

<ul> <li>Read-Only: users can only view the configuration of gateway in this level.</li> </ul>
- Read-Write: users can view and set the configuration of gateway in this level.

Table 3-4-2-2 User Management

#### 3.4.3 SNMP

SNMP is widely used in network management for network monitoring. SNMP exposes management data with variables form in managed system. The system is organized in a management information base (MIB) which describes the system status and configuration. These variables can be remotely queried by managing applications.

Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

Configuration steps are listed as below for achieving query from NMS:

- 1. Enable SNMP setting.
- 2. Download MIB file and load it into NMS.
- 3. Configure MIB View.
- 4. Configure VCAM.

#### 3.4.3.1 SNMP

The UG85 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

Status	SNMP	MIB View	VACM	Тгар	MIB
LoRaWAN	SNMP Settin	gs			
	Enable				
Network	Port		161		
System	SNMP Versior	n	SNMPv2		•
System	Location Inform	mation			
General Settings	Contact Inform	nation			
User Management	Save				
SNMP					

Figure 3-4-3-1

SNMP Settings		
Item	Description	
Enable	Enable or disable SNMP function.	
	Set SNMP listened port. Range: 1-65535.	
Port	The default port is 161.	
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.	

Location Information	Fill in the location information.
Contact Information	Fill in the contact information.

Table 3-4-3-1 SNMP Parameters

# 3.4.3.2 MIB View

This section explains how to configure MIB view for the objects.

SNMP	MIB View	VACM	Trap	MIB	
View List					
Vi	ew Name		Filter	View OID	Operation
All		Included	•	1	×
system		Included		1.3.6.1.2.1.1	
L					

Figure 3-4-3-2

MIB View		
Item	Description	
View Name	Set MIB view's name.	
View Filter	Select from "Included" and "Excluded".	
View OID	Enter the OID number.	
Included	You can query all nodes within the specified MIB node.	
Excluded	You can query all nodes except for the specified MIB node.	

Table 3-3-3-2 MIB View Parameters

# 3.4.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Тгар	MIB		
SNMP v1 & v2	2 User List					
Comm	unity	Permission	MIB Vi	ew	Network	Operation
private	Re	ad-write 🔻	All	•	0.0.0.0/0	×
public	Re	ad-only 🔻	none	•	0.0.0/0	×
						Ŧ



VACM	
Item	Description
SNMP v1 & v2 Use	er List
Community	Set the community name.
Permission	Select from "Read-Only" and "Read-Write".
MIB View	Select an MIB view to set permissions from the MIB view list.
Network	The IP address and bits of the external network accessing the MIB view.
Read-Write	The permission of the specified MIB node is read and write.
Read-Only	The permission of the specified MIB node is read only.
SNMP v3 User List	
Group Name	Set the name of SNMPv3 group.
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and "Auth/Priv".
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.

Table 3-4-3-3 VACM Parameters

## 3.4.3.4 Trap

This section explains how to enable network monitoring by SNMP trap.

MIB View	VACM	Тгар	MIB
ı	SNMPv2		•
s			
	1	I SNMPv2	SNMPv2

Figure 3-4-3-4

SNMP Trap		
Item	Description	
Enable	Enable or disable SNMP Trap function.	
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.	
Server Address	Fill in NMS's IP address or domain name.	
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.	
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.	
Auth/Priv Mode	Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".	

Table 3-4-3-4 Trap Parameters

#### 3.4.3.5 MIB

This section describes how to download MIB files. The last MIB file "URSA-gateway-MIB.txt" is for the UG85.

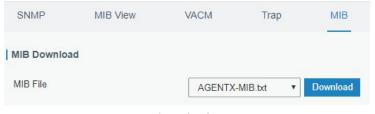


Figure 3-4-3-5

MIB	
Item	Description
MIB File	Select the MIB file you need.
Download	Click "Download" button to download the MIB file to PC.
L	Table 3-4-3-5 MIB Download

#### 3.4.4 AAA

AAA access control is used for visitors control and the available corresponding services once access is allowed. It adopts the same method to configure three independent safety functions. It provides modularization methods for following services:

- Authentication: verify if the user is qualified to access to the network.
- Authorization: authorize related services available for the user.
- Charging: record the utilization of network resources.

#### 3.4.4.1 RADIUS

Using UDP for its transport, RADIUS is generally applied in various network environments with higher requirements of security and permission of remote user access.

Status	Radius	Tacacs+	LDAP	Authentication
LoRaWAN	Radius Settin	igs		
	Enable			
Network	Server IP Addr	ess		
Quelen V	Server Port		1812	
System	Key			
General Settings				
User Management	Save			
SNMP				
ААА				

Figure 3-4-4-1

RADIUS		
Item	Description	
Enable	Enable or disable RADIUS.	
Server IP Address	Fill in the RADIUS server IP address/domain name.	
Server Port	Fill in the RADIUS server port. Range: 1-65535.	
Кеу	Fill in the key consistent with that of RADIUS server in order to get connected with RADIUS server.	

Table 3-4-4-1 RADIUS Parameters

#### 3.4.4.2 TACACS+

Using TCP for its transport, TACACS+ is mainly used for authentication, authorization and charging of the access users and terminal users by adopting PPP and VPDN.

Radius	Tacacs+	LDAP	Authentication
Tacacs+ Setting	gs		
Enable			
Server IP Addres	s		
Server Port		49	
Key			

Figure	3-4-4-2
--------	---------

TACACS+				
Item	Description			
Enable	Enable or disable TACACS+.			
Server IP Address	Fill in the TACACS+ server IP address/domain name.			
Server Port	Fill in the TACACS+ server port. Range: 1-65535.			
Кеу	Fill in the key consistent with that of TACACS+ server in order to get connected with TACACS+ server.			

Table 3-4-4-2 TACACS+ Parameters

## 3.4.4.3 LDAP

A common usage of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect the LDAP server to validate users.

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite as well.

Radius	Tacacs+		Authentication
LDAP Setting	js		
Enable			
Server IP Add	ress		
Server Port		389	
Base DN			
Security		None	*
Username			
Password			

Figure 3-4-4-3

LDAP				
Item	Description			
Enable	Enable or Disable LDAP.			
Server IP Address	Fill in the LDAP server's IP address/domain name. The maximum count			
Server IP Address	is 10.			
Server Port	Fill in the LDAP server's port. Range: 1-65535			
Base DN	The top of LDAP directory tree.			
Security	Select secure method from "None", "StartTLS" and "SSL".			
Username	Enter the username to access the server.			
Password	Enter the password to access the server.			

Table 3-4-4-3 LDAP Parameters

#### 3.4.4.4 Authentication

AAA supports the following authentication ways:

- None: uses no authentication, generally not recommended.
- Local: uses the local username database for authentication.
  - > Advantages: rapidness, cost reduction.
  - > Disadvantages: storage capacity limited by hardware.
- Remote: has user's information stored on authentication server. RADIUS, TACACS+ and LDAP supported for remote authentication.

When RADIUS, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

Radius	Radius Tacacs+ LDAP		Authentication				
Authenticatio	n Settings						
Se	rvice	1		2		3	
Cor	nsole	None	•	None	٣	None	¥
V	/eb	None	T	None	¥	None	
Te	Inet	None	•	None	۳	None	
S	SH	None	¥	None	¥	None	w



Authentication				
Item	Description			
Console	Select authentication for Console access.			
Web	Select authentication for Web access.			
Telnet	Select authentication for Telnet access.			
SSH	Select authentication for SSH access.			

Table 3-4-4-4 Authentication Parameters

## 3.4.5 Device Management

You can connect the device to the DeviceHub on this page so as to manage the gateway centrally and remotely.

Status	Device Management	
LoRaWAN •	Device Management	
	Status	Disconnected
Network •	Activation Server Address	
Queter:	Device Management Server Address	
System	Activation Method	By Authentication Code
General Settings	Authentication Code	
User Management	Connect	
ААА		
Device Management		



DeviceHub	
Item	Description
Status	Show the connection status between the gateway and the

	DeviceHub.
Disconnected	Click this button to disconnect the gateway from the DeviceHub.
Activation Server Address	IP address or domain of the DeviceHub.
DeviceHub Server Address	The URL address for the device to connect to the DeviceHub, e.g. http://220.82.63.79:8080/acs.
Activation Method	Select activation method to connect the gateway to the DeviceHub server, options are "By Authentication ID" and "By ID".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
ID	Fill in the registered DeviceHub account (email) and password.
Password	Fin in the registered Devicendo account (email) and password.

Table 3-4-5-1

# 3.4.6 Events

Event feature is capable of sending alerts by Email when certain system events occur.

# 3.4.6.1 Events

You can view alarm messages on this page.

atus	Events	Events Setti	ngs			
oRaWAN	Mark as Re	ad Delete	Mark All as	Read Delet	te All Alarms	
letwork	•	Status	Туре	Time	Me	sage
System	< > 10	Go to:	GO			
General Settings						
User Management						
AAA						
Device Managemer						
Events						

Figure 3-4-6-1

Events				
Item	Description			
Mark as Read	Mark the selected event alarm as read.			
Delete	Delete the selected event alarm.			
Mark All as Read	Mark all event alarms as read.			
Delete All Alarms	Delete all event alarms.			
Status	Show the reading status of the event alarms, such as "Read" and			

	"Unread".
Туре	Show the event type that should be alarmed.
Time	Show the alarm time.
Message	Show the alarm content.

Table 3-4-6-1 Events Parameters

## 3.4.6.2 Events Settings

In this section, you can decide what events to record and whether you want to receive email and SMS notifications when any change occurs.

Events Ev	rents Settings			
Events Settings				
Enable				
Phone Group List	1	•		
Email Group List	2	¥		
Ever	its	Record	Email Email Setting	SMS SMS Setting
Cellula	r Up			
Cellular	Down			
WAN	Up			
WAN D	lown			
VPN	Up			
VPN D	own			

Figure 3-4-6-2

Event Settings			
Item	Description		
Enable	Check to enable "Events Settings".		
Cellular Up	Cellular network is connected.		
Cellular Down	Cellular network is disconnected.		
WAN Up	Ethernet cable is connected to WAN port.		
WAN Down	Ethernet cable is disconnected to WAN port.		
VPN Up	VPN is connected.		
VPN Down	VPN is disconnected.		
The relevant content of event alarm will be recorded on "Ev			
Record	page if this option is checked.		
Email	The relevant content of event alarm will be sent out via email if this		

	option is checked.
Empil Cotting	Click and you will be redirected to the page "Email" to configure the
Email Setting	Email group.
CNAC	The relevant content of event alarm will be sent out via SMS if this
SMS	option is checked.
SNAC Cotting	Click and you will be redirected to the page of "Phone" to configure
SMS Setting	phone group list.
Phone Group List	Select phone group to receive SMS alarm.
Email Group List	Select Email group to receive Email alarm.

Table 3-4-6-2 Events Parameters

#### **Related Topics**

Email Setting Phone Setting

3.5 Industrial Interface

# The UG85 is capable of connecting with terminals throug

The UG85 is capable of connecting with terminals through industrial interface so as to realize wireless communication between terminals and remote data center.

There are two types of the gateway's industrial interface: serial port RS232 and I/O(digital input and digital output).

RS232 adopts full-duplex communication. It's generally used for communication within 20 m.

Digital input of I/O interface is a logical variable or switch variable with only two values of 0 and 1. "0" refers to low level and "1" refers to high level .

# 3.5.1 I/O

#### 3.5.1.1 DI

This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.

<b>URSALINK</b>					
Status	DI DO				
LoRaWAN 🕨	DI Setting				
Network 🕨	Enable Mode	✓ High Level ▼			
System 🕨	Duration(ms) Action	100 SMS 🕑 Email 🕑 DO	Cellular UP		
Industrial 🔻	Email	2 *			
VO	Save				

Figure 3-5-1-1

DI	
Item	Description
Enable	Enable or disable DI.
Mode	Options are "High Level", "Low Level", and "Counter".
Duration (ms)	Set the duration of high/low level in digital input. Range: 1-10000.
Condition	Select from "Low->High", and "High-> Low".
Low->High	The counter value will increase by 1 if digital input's status changes from low level to high level.
High->Low	The counter value will increase by 1 if digital input's status changes from high level to low level.
Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration.
SMS	Check to enable SMS alarm.
Phone	Set phone number to receive SMS alarm.
Content	Set the content of SMS alarm.
Email	Check to enable Email alarm.
DO	Control output status of DO.
Cellular UP	Trigger the gateway to switch from offline mode to cellular network mode.

Table 3-5-1-1 DI Parameters

# **Related Topics**

DO Setting Email Setting Connect on Demand

#### 3.5.1.2 DO

This section describes how to configure digital output mode.

<b>VRS</b>	LINK			
Status	Î			
LoRaWAN	•	DO Setting		
		Enable		
Network	•	Mode	Pulse	Ŧ
		Initial Status	High Level	•
System	•	Duration of High Level (*10ms)	100	
Industrial	-	Duration of Low Level (*10ms)	100	
		The Number of Pulse	3	
I/O		Alarm Source	☑ DI	
Serial Port				

Figure 3-5-1-2

DO			
Item	Description		
Enable	Enable or disable DO.		
Mode	Select from "High Level", "Low Level", "Pulse" and "Custom".		
Duration (*10ms)	Set duration of high/low level on digital output. Range: 1-10000.		
Initial Status	Select high level or low level as the initial status of the pulse.		
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.		
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.		
The Number of Pulse	Set the quantity of pulse. Range: 1-100.		
Alarm Source	Select alarm source.		
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.		

Table 3-5-1-2 DO Settings

#### 3.5.2 Serial Port

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data center, so as to achieve two-way communication between serial terminals and remote data center.

URSALIN	K		
Status	Serial		
LoRaWAN	Serial Settings		
	Enable		
Network 🕨	Serial Type	RS232	¥
	Baud Rate	9600	•
System 🕨	Data Bits	8	•
Industrial 🔻	Stop Bits	1	•
	Parity	None	T
VO	Software Flow Contr	rol 📋	
Serial Port	Serial Mode	DTU Mode	•
	DTI I Protocol	- ·	

Figure 3-5-2-1

Serial Settings			
Item	Description	Default	
Enable	Enable or disable serial port function.	Disable	
Serial Type	RS232		
Baud Rate	Range is 300-230400. Same with the baud rate of the connected terminal device.	9600	
Data Bits	Options are "8" and "7". Same with the data bits of the connected terminal device.	8	
Stop Bits	Options are "1" and "2". Same with the stop bits of the connected terminal device.	1	
Parity	Options are "None", "Odd" and "Even". Same with the parity of the connected terminal device.	None	
Software Flow Control	Enable or disable software flow control.	Disable	
Serial Mode	The option are "DTU Mode" and "Modbus Master". The serial port can establish communication with the remote server/client.	DTU Mode	
DTU Mode	In DTU mode, the serial port can establish communication with the remote server/client.		
Modbus Master	In Modbus Master mode, go to "Industrial > Modbus Master" to configure basic parameters and channels.		

Table 3-5-2-1 Serial Parameters

Serial Mode	DTU Mode	•		
DTU Protocol	Transparent	•		
Protocol	ТСР	•		
Keepalive Interval	75	s		
Keepalive Retry Times	9			
Packet Size	1024	Bytes		
Serial Frame Interval	100	ms		
Reconnect Interval	10	s		
Specific Protocol				
Register String				
Destination IP Addres	S			
Server Ac	Idress	Server Port	Status	Op

#### Figure 3-5-2-2

DTU Mode		
Item	Description	Default
DTU Protocol	<ul> <li>Select from "Transparent", "Modbus", and "TCP server".</li> <li>Transparent: the routed is used as TCP client/UDP and transmits data transparently.</li> <li>TCP server: the gateway is used as TCP server and transmits data transparently.</li> <li>Modbus: the gateway will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP.</li> </ul>	
TCP Server		
Listening port	Set the gateway listening port. Range: 1-65535.	502
Keepalive Interval	After TCP connection is established, gateway will send heartbeat packet to the client regularly by TCP to keep alive. The interval range is 1-3600 in seconds.	75
Keepalive Retry Times	When TCP heartbeat times out, gateway will resend heartbeat. After it reaches the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The size range is 1-1024. The unit is byte.	1024
Serial Frame Interval	The interval that the gateway sends out real serial data stored in the buffer area to public network. The range is 10-65535, in milliseconds. Note: data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within	100

Table 3-5-2-2 DTU Parameters			
Item	Description	Default	
Transparent			
Protocol	Select "TCP" or "UDP" protocol.	ТСР	
Keepalive Interval (s)	After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600, in seconds.	75	
Keepalive Retry Times	When TCP heartbeat times out, the gateway will resend heartbeat. After it reaches the preset retry times, gateway will reconnect to TCP server. The range is 1-16.	9	
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024. The unit is byte.	1024	
Serial Frame Interval	The interval that the gateway sends out real serial data stored in the buffer area to public network. The range is 10-65535, in milliseconds. Note: data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100	
Reconnect Interval	After connection failure, gateway will reconnect to the server at the preset interval, in seconds. The range is 10-60.	10	
Specific Protocol	By Specific Protocol, the gateway will be able to connect to the TCP2COM software.		
Heartbeat Interval	By Specific Protocol, the gateway will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600, in seconds.	30	
ID	Define unique ID of each gateway. No longer than 63 characters without space character.		
Register String	Define register string for connection with the server.	Null	
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null	
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null	
Status	Show the connection status between the gateway and the server.		
Modbus			
Local Port	Set the gateway listening port. Range: 1-65535.	502	

the serial frame interval.

Table 3-5-2-3 DTU Parameters

# **Related Configuration Example**

DTU Application Example

#### 3.5.3 Modbus Master

UG85 can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

#### 3.5.3.1 Modbus Master

You can configure Modbus Master's parameters on this page.

Status	Modbus Master	Channel	
LoRaWAN	Modbus Master Setting	U.	
	Enable		
Network	Read Interval	0	s
	Max. Retries	3	
System 🕨	Max. Response Time	500	ms
Industrial	Execution Interval	50	ms
muusmai	Channel Name		▼ Read
I/O			
Serial Port	Save & Apply		
Modbus Master			

#### Figure 3-5-3-1

Modbus Master						
ltem	Description	Default				
Enable	Enable/disable Modbus master.					
Read Interval/s	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set to 0, the device will restart the new read cycle after all channels have been read. Range: 0-600.	0				
Max. Retries	Set the maximum retry times after it fails to read, range: 0-5.	3				
Max. Response Time/ms	Set the maximum response time that the gateway waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000.	500				
Execution Interval/ms	The execution interval between each command. Range: 10-1000.	50				

Table 3-5-3-1

#### 3.5.3.2 Channel

You can add the channels and configure alarm setting on this page, so as to connect the gateway to the remote Modbus Slave to poll the address on this page and receive alarms

# from the gateway in different conditions.

Мо	dbus Ma	aster		Cha	nnel							
Cha	nnel Se	tting										
Cha	nnel Se	tting										
	Name	Slav ID	e	Addres s	Numbe r	Туре	Link	IP Address	Port	Sign	Decima I Place	Operation
		1		0	1	Holding R	TCP •				0	×
												<b>H</b>

Figure 3-5-3-2

Channel Se	Channel Setting						
Item	Description						
Name	Set the name to identify the remote channel. It cannot be blank.						
Slave ID	Set Modbus slave ID.						
Address	The starting address for reading.						
Number	The address number for reading.						
Туре	Read command, options are "Coil", "Discrete", "Holding Register (INT16)", "Input Register (INT16)", "Holding Register (INT32)" and "Holding Register						
	(Float)".						
Link	Select TCP for transportation.						
IP address	Fill in the IP address of the remote Modbus device.						
Port	Fill in the port of the remote Modbus device.						
Sign	To identify whether this channel is signed. Default: Unsigned.						
Decimal Place	Used to indicate a dot in the read into the position of the channel. For example: the channel value is 1234, and a Decimal Place is equal to 2, then the actual value is 12.34.						

Table 3-5-3-2

Modbus Master	Channel	
larm Setting		
	Name	
	Condition	GE(>)
	Alarm	🔲 SMS 📄 Email
	Normal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get NORMAL data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
	Abnormal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get ABERRANT data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
	Continuous Alarm	

Figure 3-5-3-3

Alarm Setting	
Item	Description
Name	Set the same name with the channel name to identify the remote
Name	channel.
Condition	The condition that triggers alert.
Min.	Set the min. value to trigger the alert. When the actual value is less than
Threshold	this value, the alarm will be triggered.
Max.	Set the max. value to trigger the alert. When the actual value is more
Threshold	than this value, the alarm will be triggered.
Alarm	Select the alarm method, e.g SMS.
SMS	The preset alarm content will be sent to the specified phone number.
Phone Group	Select the phone group to receive the alarm SMS.
Email	The preset alarm content will be sent to the specified Email address.
Email Group	Select the Email group to receive the alarm Email.
Normal	When the actual value is restored to the normal value from exceeding the
Content	threshold value, the gateway will automatically cancel the abnormal
	alarm and send the preset normal content to the specified phone group.
Abnormal	When the actual value exceeds the preset threshold, the gateway will
Content	automatically trigger the alarm and send the preset abnormal content to
	the specified phone group.
Continuous	Once it is enabled, the same alarm will be continuously reported.
Alarm	Otherwise, the same alarm will be reported only one time.

# 3.6 Maintenance

This section describes system maintenance tools and management.

#### 3.6.1 Tools

Troubleshooting tools includes ping and traceroute.

## 3.6.1.1 Ping

Ping tool is engineered to ping outer network.

Status		Ping	Traceroute
LoRaWAN	٠	IP Ping	
Network	۲	Host	Ping Stop
System	۲		
Industrial	۲		
Maintenance	•		
Tools			

#### Figure 3-6-1-1

PING	
Item	Description
Host	Ping outer network from the gateway.

Table 3-6-1-1 IP Ping Parameters

#### 3.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Status		Ping	Traceroute
LoRaWAN	×	Traceroute	
Network	×	Host	Trace Stop
System	•		
Industrial	•		
Maintenance	-		
Tools			

Figure 3-6-1-2

Traceroute					
Item	Description				
Host	Address of the destination host to be detected.				

Table 3-6-1-2 Traceroute Parameters

# 3.6.2 Schedule

This section explains how to configure scheduled reboot on the gateway.

Status			Schedule				
LoRaWAN	•	9	Schedule				
Network	•		Schedule	Frequency	Hour	Minute	Operatio n
Network							•
System	•		Save				
Industrial	•						
Maintenance	-						
Tools							
Schedule							

#### Figure 3-6-2-1

Schedule	
Item	Description
Schedule	Select schedule type.
Reboot	Reboot the gateway regularly.
Frequency	Select the frequency to execute the schedule.
Hour & Minute	Select the time to execute the schedule.

Table 3-6-2-1 Schedule Parameters

#### 3.6.3 Log

The system log contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data contained in the log, an administrator or user troubleshooting the system can identify the cause of a problem or whether the system processes are loading successfully. Remote log server is feasible, and gateway will upload all system logs to remote log server such as Syslog Watcher.

#### 3.6.3.1 System Log

This section describes how to download log file and view the recent log on web.

Status		System Log Log Settings	Help —
Status			System Log
LoRaWAN	۲	Download	System Log includes massive information about network and
Network	۲	Lug i ile Download	devices, including operating status, configuration changes and so on.
System	Þ	View recent(lines) 20	Download
		20 ,	Download log file.
Industrial	۲	Tue Sep 4 09:16:59 2018 daemon.err loraserver[16451]: time="2018-09-04T09:16:59+08:00" level=error msg="processing	View the specified lines
Maintenance	•		Clear Log Clear the current system
Tools		Tue Sep 4 09:17:04 2018 daemon.err lora-gateway-bridge[21323]: time="2018-09-04T09:17:04+08:00" level=info msg="gi received udp packet from gateway" addr="127.0.0.1:49158" protocol_version=2 type=PullData Tue Sep 4 09:17:04 2018 daemon.err lora-gateway-bridge[21323]: time="2018-09-04T09:17:04+08:00" level=info msg="gi	log.
Schedule		sending udp packet to gateway" addr="127.0.0.1:49158" protocol_version=2 type=PullACK Tue Sep 4 09:17:11 2018 daemon.err lora-gateway-bridge[21323]: time="2018-09-04T09:17:11+08:00" level=info msg="ge	
Log		received udp packet from gateway" addr="127.0.0.1;53444" protocol_version=2 type=PushData Tue Sep 4 09:17:11 2018 daemon.err lora-gateway-bridge[21323]: time="2018-09-04T09:17:11+08:00" level=info msg="g packet received" addr="127.0.0.1;53444" data="AAqHBgUEAwIBCoBTAigBUzOemv0pksU=" mac=24e124fffe0b7443	
Upgrade		Tue Sep 4 09:17:11 2018 daemon.err lora-gateway-bridge[21323]; time="2018-09-04T09:17:11+08:00" level=info msg="bc publishing packet" gos=0 topic=gateway/24e124fffe0D7443/rx	
Backup and Restore	•	Tue Sep 4 09:17:11 2018 daemon.err loraserver[16451]: time="2018-09-04T09:17:11+08:00" level=info msg="backend/gal packet received" Tue Sep 4 09:17:11 2018 daemon.err lora-gateway-bridge[21323]: time="2018-09-04T09:17:11+08:00" level=info msg="ge	
Reboot		Clear Log	
APP	Þ		

Figure 3-6-3-1

Description
Download log file.
View the specified lines of system log.
Clear the current system log.

Table 3-6-3-1 System Log Parameters

# 3.6.3.2 Log Settings

This section explains how to enable remote log server and local log setting.

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address			9) 14	]
Port		514		
Local Log File				
Storage		local	Ŧ	]
Size		1024		КВ
Log Severity		Info	•	

Figure 3-6-3-2

Log Settings		
Item	Description	
Remote Log Server		
Enable	With "Remote Log Server" enabled, gateway will send all system logs to the remote server.	
Syslog Server Address	Fill in the remote system log server address (IP/domain name).	
Port	Fill in the remote system log server port.	
Local Log File		
Storage	User can store the log file in memory or TF card.	
Size	Set the size of the log file to be stored.	
Log Severity	The list of severities follows the syslog protocol.	

Table 3-6-3-2 System Log Parameters

# 3.6.4 Upgrade

This section describes how to upgrade the gateway firmware via web. Generally you don't need to do the firmware upgrade.

Note: any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.

Status	Î	Upgrade	
LoRaWAN	•	Upgrade	
Network	•	Firmware Version Reset Configuration to Factory Default	80.0.0.8
System	•	Upgrade Firmware	Browse Upgrade
Industrial	•		
Maintenance	-		
Tools			
Schedule			
Log			
Upgrade			

Figure 3-6-4-1

Upgrade	
Item	Description
Firmware Version	Show the current firmware version.

<b>Reset Configuration to</b>	When this option is checked, the gateway will be reset to
Factory Default	factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click
Opgrade Firmware	"Upgrade" to upgrade firmware.

Table 3-6-4-1 Upgrade Parameters

## **Related Configuration Example**

Firmware Upgrade

## 3.6.5 Backup and Restore

This section explains how to create a complete backup of the system configurations to a file, restore the config file to the gateway and reset to factory defaults.

Status		Backup and Restore	
LoRaWAN	•	Restore Config	
Network	×.	Config File	Browse Imp
System	×	Backup Running-config	
Industrial	۲	Restore Factory Defaults	
Maintenance	-	Reset	
Tools			
Schedule			
Log			
Upgrade			
Backup and Re	estore		

Figure 3-6-5-1

Backup and Restore		
Item Description		
Config File	Click "Browse" button to select configuration file, and then click "Import"	
Config File	button to upload the configuration file to the gateway.	
Backup	Click "Backup" to export the current configuration file to the PC.	

Reset	Click "Reset" button to reset factory default settings. gateway will restart
Resel	after reset process is done.

Table 3-6-5-1 Backup and Restore Parameters

## **Related Configuration Example**

**Restore Factory Defaults** 

#### 3.6.6 Reboot

On this page you can reboot the gateway and return to the login page. We strongly recommend clicking "Save" button before rebooting the gateway so as to avoid losing the new configuration.

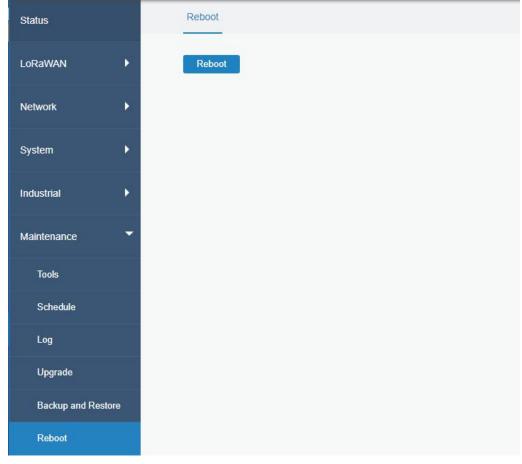


Figure 3-6-6-1

#### 3.7 APP

#### 3.7.1 Python

Python is an object-oriented programming language that has gained popularity because of its clear syntax and readability.

As an interpreted language, Python has a design philosophy that emphasizes code readability, notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords, and a syntax that allows programmers to express concepts in fewer lines of code than it's used in other languages such as C++ or Java. The language provides constructs and intends to enable writing clear programs on both small and large scale.

Users can use Python to quickly generate the prototype of the program, which can be the final interface of the program, rewrite it with a more appropriate language, and then encapsulate the extended class library that Python can call.

This section describes how to view the relevant running status such as App-manager, SDK version, extended storage, etc. Also you can change the App-manager configuration, and import the Python App package from here.

#### 3.7.1.1 Python

URSAU					
			For your de	evice security, please chang	e the default passv
Status		Python	AppManager Configuration	Python APP	
LoRaWAN	۲	Python			
	10017	AppManager Statu	s Running		View
Network	•	SDK Version	1.1.12		Uninstall
System	۲	SDK Path	eMMC		
	~	Available Storage	eMMC	•	
Industrial	•	SDK Upload		Browse	Install
Maintenance	۲				
APP	-				
Python					

#### Figure 3-7-1-1

Python	
Item	Description
AppManager Status	Show AppManager's running status, like "Uninstalled", "Running" or "Stopped".
SDK Version	Show the version of the installed SDK.

SDK Path	Show the SDK installation path.
Available Storage	Select available storage to install SDK.
SDK Upload	Upload and install SDK for Python.
Uninstall	Uninstall SDK.
View	View application status managed by AppManager.

Table 3-7-1-1 Python Parameters

# 3.7.1.2 App Manager Configuration

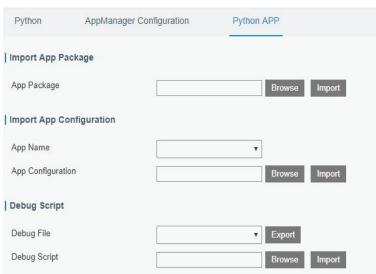
Python	AppManager Configuration	Python APP			
AppManager					
Enable					
App Management					
ID	App Command	Logfile Size(MB)	Uninstall		
App Status					
A	op Name	App Version	SDK Version		



AppManager Conf	AppManager Configuration		
Item	Description		
Enable	After enabling Python AppManager, user can click "View" button on the "Python" webpage to view the application status managed by AppManager.		
App Management			
ID	Show the ID of the imported App.		
App Command	pp Command Show the name of the imported App.		
Logfile Size(MB)	file Size(MB) User-defined Logfile size. Range: 1-50.		
Uninstall	Uninstall APP.		
App Status			
App Name	Show the name of the imported App.		
App Version	Show the version of the imported App.		
SDK Version	Show the SDK version which the imported App is based on.		

Table 3-7-1-2 APP Manager Parameters

# 3.7.1.3 Python App





Python APP		
Item	Description	
App Package	Select App package and import.	
App Name	Select App to import configuration.	
App Configuration	Select configuration file and import.	
Debug File	Export script file.	
Debug Script	Select Python script to be debugged and import.	

Table 3-7-1-3 APP Parameters

# **Chapter 4 Application Examples**

# 4.1 Application Configuration

1

You can create a new application on this page, mainly used for defining the method of decoding the data sent from end-device and choose the data transport protocol to send data to another server address. The data will be sent to your custom server address using the MQTT, HTTP or HTTPS protocol.

The configuration procedures are listed as below.

1. Go to "LoRaWAN" > "Network Server" > "Application".

2.	Click 🔜 to	enter the	configuration page	e, displayed	l as the following	picture:	
	General	Applications	Profiles	Device	Packets		
	Applications						
	Name		Smoke-sensor-app				
	Description		a application for smoke sense	or			
	Payload Codec		None	•			
	Data Transmission						
		Тур	0e		Operation		
					<b>H</b>		
	Save	Cancel					

Application Configuration				
Item	Description	Default		
Name	Enter the name of the application profile.			
Name	E.g Smoker-sensor-app.			
Description	Enter the description of this application.			
Description	E.g a application for smoker sensor.			
	Select from: "None", "Cayenne LPP", "Custom".			
	None: This mode enables devices not to encode data.			
	Cayenne LPP: This mode enables devices to encode			
Payload Codec	data with the Cayenne Low Power Payload (LPP).	None		
	Custom: This mode enables devices to encode data			
	with the decoder function and the encoder function			
	which you have entered the code.			

3. Click to add a data transmission type of HTTP or HTTPS: Step 1: select HTTP or HTTPS as transmission protocol.

Туре	HTTP	•
------	------	---

#### Step 2: Enter the header name and header value as needed.

HTTP Header			
	Header Name	Header Value	Operation
			<b>H</b>

Headers are name/value pairs that appear in both request and response messages. The name of the header is separated from the value by a single colon.

For example, this request message provides a header called User-Agent whose value is Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko. The purpose of this particular header is to supply the web server with information about the type of browser making the request.

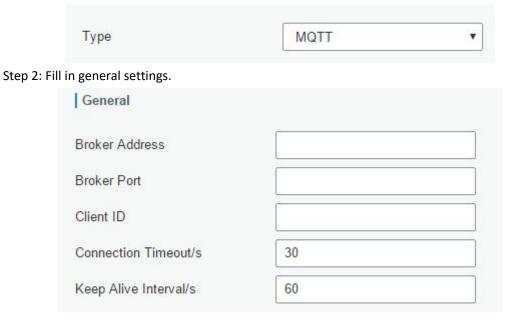
User-Agent: M	Mozilla/5.0	(Windows	NT 6.3;	WOW64;	Trident/7.0;	rv:11.0)	like Gecko
---------------	-------------	----------	---------	--------	--------------	----------	------------

### Step 3: Enter the destination URL. Different types of data can be sent to different URLs.

RL		
	Data Type	URL
	Uplink data	
	Join notification	
	ACK notification	
	Error notification	

4. Click to add a data transmission type of MQTT:

## Step 1: select the transmission protocol as MQTT.



MQTT General Settings			
ltem	Description	Default	
Broker Address	Please enter the broker address to receive data.		
Broker Port	Please enter the broker port to receive data.		
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle message at QoS 1 and 2.		
Connection Timeout	Set the maximum response time when the client waits for the response from the server. If the client does not get a response after the maximum response time, the connection will be considered as broken. The interval range is 1-65535 in second.	30	
Keep Alive Interval	After the client is connected with the server, the client will send heartbeat packet to the server regularly to keep alive. The interval range is 1-65535 in second.	60	

Step 3: Select the authentication method required by the server.

If you select user credentials for authentication, you need to enter the username and password for authentication.

User Credentials	
Enable	
Username	
Password	

If certificate is necessary for verification, please import CA certificate, client certificate and client key file for authentication.

TLS			
Enable			
CA	Browse	Import	Delete
Client Certificate	Browse	Import	Delete
Client Key	Browse	Import	Delete

Step 4: Enter the topic to receive data and choose the QoS.

QoS 0 – Only Once

This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode.

QoS 1 – At Least Once

This level guarantees that the message will be delivered at least once, but may be delivered more than once.

QoS 2 – Exactly Once

QoS 2 is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS 2 is the safest and slowest quality of service level.

Торіс			
Data Type	topic		
Uplink data		QoS 0	•
Join notification		QoS 0	•
ACK notification		QoS 0	•
Error notification		QoS 0	•

# 4.2 Device Profiles Configuration

Device Profiles		
Name	device_pro	
Max TXPower	0	
Join Type	ΟΤΑΑ	•
Class Type	Class C	T
Advanced		
MAC Version	1.0.2	۲
Regional Parameters Revision	В	T
ACK Timeout	0	se

Device Profiles Se	Device Profiles Settings					
Item	Description	Default				
Name	Enter the Name of the application profile. E.g. Smoker-sensor-app.	Null				
Max TXPower	Enter the maximum transmit power. O means using the max EIRP.	0. The TXPower indicates power levels relative to the Max EIRP level of the end-device. 0 means using the max EIRP. EIRP refers to the Equivalent Isotropically Radiated Power.				
Join Type	Select from: "OTAA" and "ABP". OTAA:Over-the-Air Activation. For over-the-air activation, end-devices must follow a join procedure prior to participating in data exchanges with the network server. An end-device has to go through a new join procedure every time as it has lost the session context information. ABP: Activation by Personalization. Under certain circumstances, end-devices can be activated by personalization. Activation by personalization directly ties an end-device to a specific network bypassing the join request - join	ΟΤΑΑ				

	accept procedure.	
	Select from: "Class A" and "Class C".	
	A: Class A operation has the lowest power	
	consumption for applications that require	
	downlink communication from the server shortly	
	after the end-device has sent an uplink	
Class Type	transmission.	A
	C: End-device of Class C will continuously open	
	receive windows, only closed when transmitting.	
	Class C end-device will spend more power than	
	Class A or Class B but they offer the lowest	
	latency for server to end-device communication.	

Advanced			
MAC Version	1.1.0	٠	]
Regional Parameters Revision	A	۲	]
RX1 Datarate Offset	0	٠	]
RX2 Datarate	DR0 (SF12, 125 kHz)	۲	]
RX2 Channel Frequency	869525000		] HZ
Frequency List			Hz
ACK Timeout	0		sec

Device Profile Advanced Settings			
Item	Description	Default	
MAC Version	Choose the version of the LoRaWAN supported by the end-device.	1.0.2	
Regional Parameter Revision	Revision of the Regional Parameters document supported by the end-device.	В	
RX1 Datarate Offset	Enter the offset which used for calculate the RX1 data-rate, based on the uplink data-rate. The range is based on what is specified in the LoRaWAN regional parameters document.	The default offset is based on what is specified in the LoRaWAN regional parameters document.	
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window. The range is based on what is specified in the LoRaWAN regional parameters document.	The default offset is based on what is specified in the LoRaWAN regional parameters	

		document.
RX2 Channel Frequency	Enter the RX2 channel frequency which used for the RX2 receive-window. The range is based on what is specified in the LoRaWAN regional parameters document.	Null
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN regional parameters document.	Null
ACK Timeout	Enter the time for confirmed downlink transmissions. Only applicable to class C.	5

# 4.3 Device Configuration

Go to "LoRaWAN" > "Network Server" > "Device".

You can edit the device configuration by clicking  $\blacksquare$  or create a new device by clicking  $\blacksquare$ .

Device		
General		
Device Name	asd	
Description	s	
Device EUI	3530353083376118	}
Device-Profile	ninii	۲
Application	AS923	Ŧ
Frame-counter Validation		

Device Configuration-General		
Item	Description	Default
Device	Enter the name of this device.	Null
Description	Enter the description of this device.	Null
Device EUI	Enter the EUI of this device.	Null
Device-Profile	Choose the device profile from created device profiles.	Null
Application	Choose the application profile from created application.	Null
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.	Enabled

114

Activate Device(ABP)	
Device Address	068c1b56
Network Session Key	17ad9c3acad1df8359b1a68893
Application Session Key	9555caa83ec8bb82b2a162452
Uplink Frame-counter	1
Downlink Frame-counter	1

Activation By Personalisation	
Device is pre-programmed with a DevAddr, an AppSKey and a NwkSKey. No join procedure is necessary.	The Network Server is also pre- configured with the device's DevAddr, AppSKey and NwkSKey so it recognises its transmissions.
$\blacksquare \longrightarrow \bigcirc \frown \bigcirc$	

ABP stands for Authentication By Personalisation. It means that the encryption keys are configured manually on the device and can start sending frames to the Gateway without needing a 'handshake' procedure to exchange the keys (such as the one performed during an OTAA join procedure).

With ABP the encryption keys enabling communication with the network are preconfigured in the device. The network will need to provide you with a Device Address, Network Session Key and Application Session Key.

Device Configuration-Activate Device-ABP		
Item	Description	Default
Device Address	Enter the device address. The device address identifies the end-device within the current network.	Null
Network Session Key	Enter the network session key of the device. The network session key specific for the end-device. It is used by the end-device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity.	Null
Application Session Key	Enter the application session key of the device. The AppSKey is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages.	Null
Uplink Frame-counter	The number of data frames which sent uplink to the network server. It will be incremented by the end-device and received by the end-device.	Null

	Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. Users cloud reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	Null

Activate Device(OTAA)

Application Key	0102030401020304010203040
Device Address	068c1b56
Network Session Key	17ad9c3acad1df8359b1a68893
Application Session Key	9555caa83ec8bb82b2a162452:
Uplink Frame-counter	1
Downlink Frame-counter	1

	Over-The-Air Ac	tivation	
Device sends <b>join-request</b> with pre-programmed DevEUI, <b>AppEUI</b> and <b>AppKey</b> , as well as a random <b>DevNonce</b> .	UG87-LW manages to receiv packet and then forwards i its network.	it to as valid	he Network Server receives juest and consults the entity sociated with the <b>AppEUI</b> to date the request. If permission granted, it responds with a <b>join-accept</b> message.
$\textcircled{1} \longrightarrow $			$\longrightarrow$
De	ind then uses the <b>AppNonce</b> to generate its session keys, n	The join-accept response ontains a <b>NetID</b> , a <b>DevAddr</b> and a <b>AppNonce</b> , as well as some etwork settings like <b>D2settings</b> <b>RxDelay</b> and an optional <b>CFList</b>	$\sim$

OTAA stands for Over The Air Activation. With this method the end-device sends a Join request to the gateway using the Application Key, Application Key is a shared secret key unique to your device to generate the session keys that prove its identity to the network. If the keys are correct, the gateway will reply to the end-device with a join accept message, and from that point on the end-device is able to send and receive packets to/from gateway. If the keys are incorrect, no response will be received.

Device Configuration-Activate Device-OTAA			
Item	Description	Default	
Application Key	Enter the application key. Whenever an end-device joins a	Null	

	network via over-the-air activation, the application key is used for derive the Application Session key.	
Device Address	Show the device address when the device has been activated. The device address identifies the end-device within the current network.It will be cleared when the node has not been activated yet or device has been inactive for a long time.	Null
Network Session Key	Show the network session key of the device when the device has been activated. The network session key specific for the end-device. It is used by the end-device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity. It will be cleared when the node has not been activated yet or device has been inactive for a long time.	Null
Application Session Key	Show the application session key of the device when the device has been activated. The AppSKey is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages. It will be cleared when the node has not been activated yet or device has been inactive for a long time.	Null
Uplink Frame-counter	The number of data frames which sent uplink to the network server. It will be incremented and received by the end-device. After a JoinReq -JoinAccept message exchange, the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	Null
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. After a JoinReq -JoinAccept message exchange, the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	Null

## 4.4 Send Data to Device

Go to "LoRaWAN" > "Network Server" > "Packets".

Step 1: Please check the packet in the network server list to make sure that the device has joined the network successful.

1122612191	868100000	SF7BW125	17	175	17	0	JnAcc	2019-08-06T09:22:29+08:00	0
112261219	868100000	SF7BW125	9.5	-77	18	0	JnReq	2019-08-06T09:22:29+08:00	0

#### Step 2: Fill these input box.

Device EUI	Туре	Payload	Fport	Confirme
11226121913	ASCII 🔻	15	15	×
		,		

<b>n</b> 1	
Send	send success

Step 4: Check the packet in the network server list to make sure that the device has received this message successful.

Send Data To Device				
Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII	15	15	

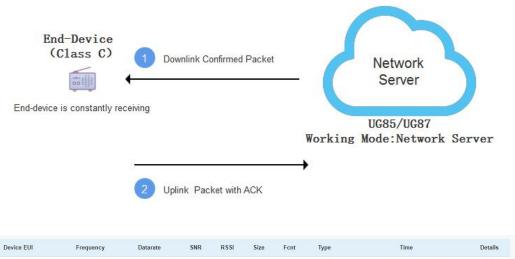
You can click "Refresh" to refresh the list or set automatic refreshing frequency for the list. If the device' s class type is Class C, then the device will be constantly receiving packet.

This packet's type is DnCnf (Downlink Confirmed Packet) and if the packet's color is gray, then it means the packet cannot be transmitted now because at least one message has been in the queue.

This is the data packet has been delivered successfully.

2019-08-06T09:22:55+08:00 Success ()	DnCnf	2	6	 -	SF12BW125	869525000	1122612191311123
Pending 🕚	DnCnf	2	6			0	1122612191311123

If the device receives this downlink confirmed packet, then the device will reply "ACK" when delivering next.



11226121913	868300000	SF10BW125	1.00	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	-0
112261219	869525000	SF12BW125		-	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125			0	1	DnUnc	2019-08-06T09:22:49+08:00	0

kets Details		
Dev Addr	07e7	
GwEUI	24e124ff	
AppEUI	557240	
DevEUI	1122612191311123	
Immediately		
Timestamp	874346044	
Туре	UpCnf	
Adr	false	
AdrAcKReq	false	
Ack	true	
Fcnt	21	
Fport	55	
Modulation	LORA	

Ack is "true" means that the device has received this packet.

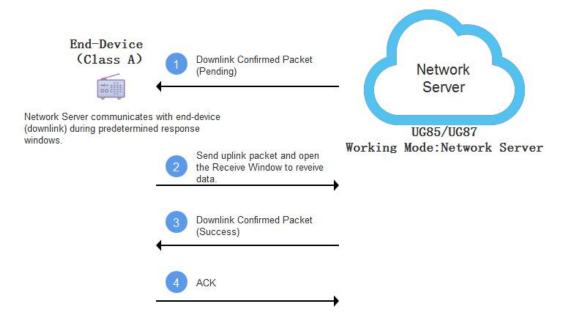
If the device's class type is Class A, then the Network Server communicates with end-device (downlink) during predetermined response windows.

This packet's type is DnCnf (Downlink Confirmed Packet) and if the packet's color is gray, then it means that the packet cannot be transmitted now because at least one message has been in queue.

11226121912-	0	6 2 DnC	1
--------------	---	---------	---

Only after the device sends out an uplink packet will the network server sends out data to the device.

Network Server										Show the signal-noise ratio.
Clear								Search	0	RSSI Show the received signal strength
								L		indicator.
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details	Size Show the size of packet.
1122612191311123	868300000	SF10BW125	121	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0	Font
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0	Show the frame counter.
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	0	Type Show the type of the paceket:
1122612191311123	868100000	SF10BW125	-	5	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success	JnAcc - Join Accept Packet JnReq - Join Request Packet UpUnc - Uplink Unconfirmed
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0	Packet
1122612191311123	0				6	18	DnCnf	Pending	0	UpCnf - Uplink Confirmed Packet ACK response from network requested
1122612191311123	868500000	SF10BW125	-	-	0	17	DnUnc	2019-08-06T09:47:38+08:00	0	DnUnc - Downlink Unconfirmed Packet
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0	DnCnf - Downlink Confirmed Packet- ACK response from end-
1122612191311123	868100000	SF10BW125	-	22	0	16	DnUnc	2019-08-06T09:46:38+08:00	0	device requested
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	D Refresh	Time Show the time of packet was service



Clear								Search	Q
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcn	t Type	Time	Details
1122612191311123	868300000	SF10BW125	2	12	0	19	DnUnc	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	1	UpCnf	2019-08-06T09:49:38+08:00	0
1122612191311123	868100000	SF10BW125	means	the c	device	has	received	the packet you send.	0
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0
1122612191311123	0				6	18	DnCnf		0
1122612191311123	868500000	SF10BW125		-	0	17	DnUnc	2019-08-06T09:47:38+08:00	0
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0
1122612191311123	868100000	SF10BW125	2	12	0	16	DnUnc	2019-08-06T09:46:38+08:00	0
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0

## **Related Topic**

Packets

## 4.5 Restore Factory Defaults

#### 4.5.1 Via Web Interface

1. Log in web interface, and go to "Maintenance > Backup and Restore".

2. Click "Reset" button under the "Restore Factory Defaults".

You will be asked to confirm if you'd like to reset it to factory defaults. Then click "Reset" button.

Status	
LoRaWAN	۲
Network	۲
System	Þ
Industrial	Þ
Maintenance	-
Tools	
Schedule	
Log	
Upgrade	
Backup and Restore	9

Backup Running-config	
Backup	
Restore Factory Defaults	
Reset	×
	Reset operation will erase all configuration data on Router and
	reset the system to factory defaults. Continue?
	Reset Cancel

Then the gateway will reboot and restore to factory settings immediately.

Restore Config	
Config File	Browse Import
Backup Running-config	
Backup	Reset, please do not power off
Restore Factory Defaults	
Reset	

Please wait till the login page pops up again, which means the gateway has already been reset to factory defaults successfully.



Related Topic Restore Factory Defaults

#### 4.5.2 Via Hardware

Locate the reset button on the gateway, and take corresponding actions based on the status of SYSTEM LED.

SYSTEM LED	Action
Blinking	Press and hold the reset button for more than 15 seconds.
Static Green $ ightarrow$	Release the button and wait.
Rapidly Blinking	
$Off \rightarrow Blinking$	The gateway is now reset to factory defaults.

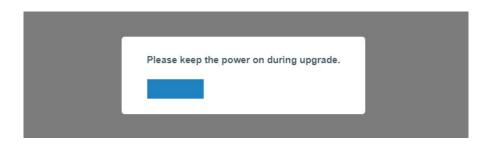
#### 4.6 Firmware Upgrade

It is suggested that you contact Ursalink technical support first before you upgrade gateway firmware.

After getting firmware file from Ursalink technical support, please refer to the following steps to complete the upgrade.

- 1. Go to "Maintenance > Upgrade".
- 2. Click "Browse" and select the correct firmware file from the PC.
- 3. Click "Upgrade" and the gateway will check if the firmware file is correct. If it's correct, the firmware will be imported to the gateway, and then the gateway will start to upgrade.

System	Upgrade	
Industrial 🕨	Upgrade Firmware Version	80.0.0.8
Maintenance 🔻	Reset Configuration to Factory Default Upgrade Firmware	Browse Upgrade
Tools		Dionse Opgrade
Schedule		
Log		
Upgrade		
Upgrade Upgrade		
Firmware Version	n <b>2.0.0.1</b> 9	
Reset Configurat	ion to Factory Default	
Upgrade Firmwa	0.11akepatriz.0.0.15	
	importing firmware.	Please stay on this page till upgrade is finished.



## **Related Topic**

<u>Upgrade</u>

## 4.7 Cellular Connection

The UG85 have two cellular interfaces, named SIM1 & SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, SIM1 interface takes precedence as default.

#### Example

We are about to take an example of inserting a SIM card into SIM1 slot of the UG85 and configuring the gateway to get Internet access through cellular.

#### **Configuration Steps**

- 1. Go to "Network > Interface > Cellular > Cellular Setting" and configure the cellular info.
- 2. Enable SIM1.
- 3. Choose relevant network type. "Auto", "4G First", "4G Only", "3G First", "3G Only", "2G First" and "2G only" are optional.

URSALINK					
Status	Port WAN	LAN VLAN Trur	ik Cellular	Loopback	
LoRaWAN 🕨	Cellular Setting	SIM1	2 Cellular		
Network 🔻	Enable	3im1 ₹	<i>∎</i>		
Interface	Network Type	Auto	▼ Auto	¥	
Firewall (1) Interface	APN Username	Auto 4G First 4G Only 3G First	Auto" or others		
DHCP	Password	3G Only 2G First 2G Only			
DDNS	Access Number				
Link Failover	PIN Code				
VPN	Authentication Type	Auto	▼ Auto	T	
	Roaming				
System 🕨	SMS Center				
	Connection Setting				
Industrial 🕨 🕨	Dual SIM Strategy				

	<								A	pply		💄 admin 🛛 🔁
Status		Port	WAN	LAN	VLAN Trunk		Cellular	Loopback	5	Apply		Help —
LoRaWAN I		Password Access Num	ber								*	Enable Check the option to enable the corresponding SIM card.
Network	•	PIN Code Authenticatio	n Type	A	to	-	Auto		•			Network Type Select from "Auto", "4G First", "4G Only", "3G
Interface		Roaming					0					First", "3G Only", "2G Frist", and "2G Only".
Firewall		SMS Center									1	Auto: connect to the network with the strongest signal
DHCP		Connection	Setting									automatically. 4G First: 4G network has priority
		Dual SIM Str	ategy									to be connected. 4G Only: connect to 4G
DDNS		Enable NAT		Image: A start of the start								network only. And so on.
Link Failover												APN Enter the Access Point
VPN		ICMP Server			.8.8							Name for cellular dial-up connection provided by
		Secondary IC	MP Server	114	. 114. 114. 114							local ISP.
System		PING Times		5								Username
Industrial I		Packet Loss		20			%				l	Enter the username for cellular dial-up connection provided by local ISP.
Maintenance		SMS Mode		PI	N I	•						Password
АРР І		Save	•	Save								Enter the password for cellular dial-up connection provided by local ISP.

Click "Save" and "Apply" for configuration to take effect.

Note:

If you select "Auto", the gateway will obtain ISP information from SIM card to set APN, Username, and Password automatically. This option will only be taken effect when the SIM card is issued from well-known ISP.

If you select "4G First" or "4G Only", you can click "Save" to finish the configuration directly.

If you select "3G First", "3G Only", "2G First" or "2G Only", you should manually configure APN, Username, Password, and Access Number.

4. Check the cellular connection status by WEB GUI of gateway.

Click "Status > Cellular" to view the status of the cellular connection. If it shows 'Connected', SIM1 has dialed up successfully.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
Modem							
Status		Ready					
Model		U9300C					
Current SIM		SIM1					
Signal Level		29asu (-56dBm)					
Register Status		Registered (Home r	network)				
IMSI		460070615219248					
ICCID		898602E61315320	19248				
ISP		CHINA MOBILE					
Network Type		LTE					
PLMN ID		46007					
LAC		fffe					
Cell ID		f700e28					
IMEI		862808032459987					
Network							
Status		Connected	Connected				
IP Address		10.39.128.14					
Netmask		255.255.255.252					
Gateway		10.39.128.13					
DNS		211.143.147.120					
Connection Duration		0 days, 00:15:35			N	Aanual Refresh 🔻	Refresh
						2011	

5. Check out if network works properly by browser on PC.

Open your preferred browser on PC, type any available web address into address bar and see if it is able to visit Internet via the UG85.

#### **Related Topic**

Cellular Setting Cellular Status

## 4.8 Dual SIM Backup Application Example

#### Example

In this section we will take an example of inserting two SIM cards into the UG85. When one SIM fails, gateway will try to connect with the other SIM as backup link.

#### **Configuration Steps**

1. Go to "Network > Interface > Cellular" to enable SIM1 and SIM2. Leave the network type as "Auto" by default.

				Apply
Status	Port WAN	LAN VLAN Tru	nk Cellular 2	Loopback
LoRaWAN 🕨	Cellular Setting			
		SIM1	SIM2	
Network 🔻	Enable	3 .	Ø	
Interface ①	Network Type	Auto	<ul> <li>Auto</li> </ul>	•
<b>E</b>	APN			
Firewall				
	Username			
DHCP	Password			
DDNS	Access Number			
	PIN Code			
Link Failover	PIN Code			
	Authentication Type	Auto	▼ Auto	•
VPN	Roaming			

2. Enable "Dual SIM Strategy", and configure the corresponding options as below. ICMP server can be configured as any reachable IP address.

	8 Apply
Status	Port WAN LAN VLAN Trunk Cellular Loopback
LoRaWAN	Connection Setting  Dual SIM Strategy  (5)
Network	Primary SIM Card SIM1
Interface	Switch to backup SIM card when ICMF  detection fails
Firewall	Swtich to backup SIM card when the connection fails
DHCP	Switch to backup SIM card when
DDNS	Enable NAT
Link Failover	
VPN	ICMP Server
	Secondary ICMP Server 114.114.114
System	PING Times 5
	Packet Loss Rate 20 %
Industrial	SMS Settings
Maintenance	SMS Mode PDU •
APP	Save (7)

Then click "Save" and "Apply" button.

 Go to "Status > Cellular", and you will see the gateway is connected to the network via SIM1.

Ove	erview	Cellular	Network	VPN	Routing
Mode	em				
Statu	IS		Ready		
Mode	el		EC25		
Curre	ent SIM		SIM1		
Signa	al Level		15asu (-83dBm)		
Regi	ster Status		Registered (Home I	network)	
IMSI			460019987103071		
ICCII	D		8986011783801919	96629	
ISP			CHN-UNICOM		
Netw	ork Type		LTE		
	Network				
	Status		C	onnected	
	IP Addres	s	10	).105.39.33	

 You can remove SIM1 to make the gateway fail to connect to network via it. Go to "Status > Cellular" again, and you will see the gateway is connected to the network through SIM2.

Overview	Cellular	Network	VPN	Routing
Modem				
Status		Ready		
Model		EC25		
Current SIM		SIM2		
Signal Level		15asu (-83dBm	1)	
Register Status		Registered (Ho	me network)	
IMSI		460019987103	071	
ICCID		898601178380	19196629	
Network	¢			
Status			Connected	)
IP Addre	SS		10.63.223.44	ŀ

Now SIM2 becomes the main SIM, and SIM1 runs as the backup.

The gateway won't reconnect via SIM1 until SIM2 fails.

#### Related Topic

Cellular Setting

Cellular Status

## 4.9 Wi-Fi Application Example

## 4.9.1 AP Mode

#### **Application Example**

Configure UG85 as AP to allow connection from users or devices.

#### **Configuration Steps**

1. Go to "Network > Interface > WLAN" to configure wireless parameters as below.

URSAL	INK							
					For your device set	curity, please change	e the default passwo	rd
Status	1	Port	WAN	LAN	VLAN Trunk	WLAN	Cellular	Loopback
LoRaWAN	F	WLAN						
Network				AP	e AP			
Interface		SSID Broad						
Firewall		Radio Type		802	11g(2.4GHz)	•		
QoS		Channel SSID		Aut	o alink_support	•		
DHCP		BSSID						
DDNS		Encryption M	Vlode	WP	WPA2-PSK			
Link Failover		Cipher		AES	6	¥		
	_	Key		•••••				
VPN		Bandwidth		201	ЛНz	*		
System		Max Client M	Number	128	6			

Click "Save" and "Apply" button after all configurations are done.

2. Use a smart phone to connect by SSID "Ursalink\_F0257A". Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

Overview	LoRa	Cellular	Network	WLAN	VPN	Host List
WLAN Status						
Wireless Status		Enabled				
MAC Address		24:e1:24:f0:27	:85			
Interface Type		AP				
SSID		Ursalink_supp	ort			
Channel		Auto				
Encryption Type		WPA2-PSK				
Cipher		AES				
Status		Up				
IP Address		192.168.100.1				
Netmask		255.255.255.0				
Connection Durat	tion	0 days, 03:16:	08			

## 4.9.2 Client Mode

#### **Application Example**

Configure UG85 as Wi-Fi client to connect to an access point to have Internet access.

## **Configuration Steps**

1. Go to "Network > Interface > WLAN" to configure wireless as below.

		For your device securit	y, please chang	e the default passwo	d
Status	Port WAN	LAN VLAN Trunk	WLAN	Cellular	Loopback
LoRaWAN 🕨	<b> </b> WLAN				
Network 👻	Enable Work Mode	Client •	Scan	l,	
Interface	SSID	Meeting Room			
Firewall	BSSID	24:e1:24:f0:01:77			
	Encryption Mode	WPA2-PSK T			
QoS	Cipher	AES 🔻	]		
DHCP	Key	••••••	]		
DDNS	IP Setting				
Link Failover	Protocol	DHCP Client	]		

Click "Save" and "Apply" button after all configurations are done.

2. Go to "Status > WLAN", and you can check the connection status of the client.

Overview	LoRa	Cellular	Network	WLAN	VPN	Host List
WLAN Status						
Wireless Status		Enabled				
MAC Address		24:e1:24:f0:27	:85			
Interface Type		Client				
SSID		Meeting Room	l.			
Channel		Auto				
Encryption Type		WPA2-PSK				
Cipher		AES				
Status		Connected				
IP Address		0.0.0.0				
Netmask		0.0.0.0				
Connection Durat	tion	0 days, 00:00:	00			

## **Related Topic**

WLAN Setting

WLAN Status

## 4.10 NAT Application Example

#### Example

An UG85 can access Internet via cellular. GE port is connected with a Web server whose IP address is 192.168.1.2 and port is 8000. Configure the gateway to make public network access the server.

## **Configuration Steps**

Go to "Firewall > Port Mapping" and configure port mapping parameters.

URSA	LINK										5	Apply
Status			ACL	DMZ	Port Ma	<sup>pping</sup> (2)	MAC Bi	nding				
LoRaWAN	•	ļF	Port Mapping	I								
Network	-		Sour	ce IP	Source Port	Destinatio	on IP	Destination Port	Protocol	Description		Operation
Interface		3	0.0.0/0		8000	192.168.1.2		8000	TCP 🔻	Server		×
Firewall	1										_	Ŧ
DHCP			Save	4								
DDNS												

Click "Save" and "Apply" button.

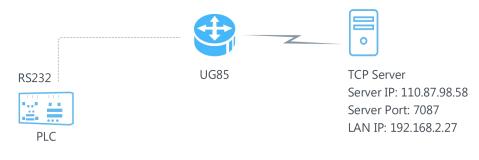
#### **Related Topic**

Port Mapping

## 4.11 DTU Application Example

#### Example

PLC is connected with the UG85 via RS232. Then enable DTU function of the UG85 to make a remote TCP server communicate with PLC. Refer to the following topological graph.



Serial Parameters of the PLC				
Baud Rate	9600			
Data Bit	8			
Stop Bit	1			
Parity	None			

## **Configuration Steps**

1. Go to "Industrial > Serial Port" and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.

Status	Î	Serial		
LoRaWAN	•	Serial Settings		
		Enable		
Network	•	Serial Type	RS232	٣
		Baud Rate	9600	•
System		Data Bits	8	•
Industrial	-	Stop Bits	1	•
		Parity	None	•
I/O		Software Flow Con	trol	
Serial Port		Serial Mode	DTU Mode	¥

2. Configure Serial Mode as "DTU Mode". The UG85 is connected as client in "Transparent" protocol.

System	<b>`</b>	DTU Protocol	Transparent	T
Industrial	-	Protocol	ТСР	•
		Keepalive Interval	75	S
VO		Keepalive Retry Times	9	
Serial Port		Packet Size	1024	Bytes
Modbus Master		Serial Frame Interval	100	ms
		Reconnect Interval	10	s
Maintenance	×	Specific Protocol		
APP	•	Register String	ursalink_modern1	

#### 3. Configure TCP server IP and port.

Destination IP Address

Server Address	Server Port	Status	Operation
		199	×
Save			

4. Once you complete all configurations, click "Save" and "Apply" button.

	Apply 2 admir	Ð	
Destination IP Address			
Server Address	Server Port	Status	Operation
110.87.98.58	7087	Connected	×
			<b>H</b>

5. Start TCP server on PC.

Take "Netassist" test software as example. Make sure port mapping is already done.

(2) Local host IP	_
27 LOCALNOST IF	
192.168.2.2	27
3) Local host por 7087	
Disconne	

6. Connect the UG85 to PC via RS232 for PLC simulation. Then start "sscom" software on

the PC to test communication through serial port.

ComNum	COM9	•	۲	Close	Com
BaudRa	9600	-	ΓD	TR	
DataBi	8	•	∏ Se	end eve	100
StopBi	1	-	T Se	endHEX	Γ
Verifyl	None	-	Data	input:	[
FlowCon		-	hell	lo	
			-	-	

**7.** After connection is established between the UG85 and the TCP server, you can send data between sscom and NetAssit.

## PC side

SSCOM3.2	-		$\times$
testtesttesttesttesttesttesttesttesttes			~
			$\sim$
OpenFile FileNm SendFile SaveDate	a Clear	r	HexDats
ComNum COM13 💌 🛞 CloseCom Help			EXT
BaudRa 9600 - DTR RTS			
DataBi 8 🔽 🔽 Send eve 1000 ms/Time			
StopBi 1 🔽 🗖 SendHEX 🗖 SendNew			
Verify None V Data input: SEND			
ww.mcu51.cor S:42 R:48 COM13 opened 9600bp	s  CIS=1	DSR=	ORC

## TCP server side

	Net∆ssist (V3.7) - □ ×
Settings	Data Receive
(1) Protocol	[Receive from 220.249.163.119 : 19049]:
TCP Server 📃	ursalink_modem1hellohellohellohellohellohellohellohell
(2) Local host IP	
192.168.2.27	
(3) Local host por	
7087	
1 And 1	
- Disconnect	
Recv Options	
🔽 Receive to file	
🗖 Add line return	
🔲 Receive As HEX	
🗖 Receive Pause	
<u>Save</u> <u>Clear</u>	
Send Options	
🔲 Data from file	
🔲 Auto Checksum	
🦳 Auto Clear Input	
🔲 Send As Hex	
🔽 Send Cyclic	Peers: All Connections
Interval 1000 ms	test
Load Clear	Send
💣 Ready!	Send : 208 Recv : 177 Reset

8. After serial communication test is done, you can connect PLC to RS232 port of the UG85 for test.

# **Related Topic**

Serial Port

[END]