WWW.INFOPULSAS.LT / info@infopulsas.lt



UG87-LW

Industrial LoRaWAN Gateway User Guide

Ursalink Technology Co., Ltd.



×

SIRCOM

www.ursalink.com

Preface

Thanks for choosing Ursalink UG87-LW industrial LoRaWAN gateway. The UG87-LW 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 UG87-LW 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 UG87-LW LoRaWAN gateway

Related Documents

Document	Description	
Ursalink UG87-LW Datasheet	Datasheet for the Ursalink UG87-LW industrial LoRaWAN Gateway.	
Ursalink UG87-LW Quick Start Guide	Quick installation guide for the Ursalink UG87-LW industrial LoRaWAN Gateway.	

Declaration of Conformity

UG87-LW 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
Jul. 19, 2018	V.1.0.0	Initial version

Contents

Chapter 1 Product Introduction	8
1.1 Overview	8
1.2 Advantages	8
1.3 Specifications	
Chapter 2 Installation	
2.1 General Packing List	13
2.2 Product Overview	14
2.3 LED Indicators	
2.4 Ethernet Port Indicators	15
2.5 Reset Button	
2.6 PIN Definition	
2.7 SIM Card Installation	16
2.8 Cellular Antenna Installation	
2.9 Mounting the Gateway	
2.10 Connect the Gateway to a Computer	
2.11 Installation of Power Supply and Protective Grounding	
2.11.1 Power Supply Installation	
2.11.2 Protective Grounding Installation	
Chapter 3 Access to Web GUI	21
3.1 PC Configuration for Web GUI Access to gateway	21
3.2 Access to Web GUI of gateway	
Chapter 4 Web Configuration	24
Chapter 4 Web Configuration 4.1 Status	
	24
4.1 Status	24 24
4.1 Status 4.1.1 Overview	24 24 24 25
4.1 Status 4.1.1 Overview 4.1.2 LoRa WAN	24 24 25 27
4.1 Status 4.1.1 Overview 4.1.2 LoRa WAN 4.1.3 Cellular	
4.1 Status 4.1.1 Overview 4.1.2 LoRa WAN 4.1.3 Cellular 4.1.4 Network	
4.1 Status 4.1.1 Overview 4.1.2 LoRa WAN 4.1.3 Cellular 4.1.4 Network 4.1.5 VPN	
 4.1 Status	
 4.1 Status	
4.1 Status.4.1.1 Overview.4.1.2 LoRa WAN.4.1.3 Cellular.4.1.4 Network.4.1.5 VPN.4.1.6 Routing Information.4.1.7 Host List.	24 24 25 27 29 30 31 32 33 33
 4.1 Status	24 24 25 27 29 30 31 31 32 33 33 33
4.1 Status	24 24 25 27 29 30 31 31 32 33 33 33 33 33
4.1 Status	24 24 25 27 29 30 30 31 31 32 33 33 33 33 33 33 33
4.1 Status	
4.1 Status	24 24 25 27 29 30 30 31 31 32 33 33 33 33 33 33 33 33 33 33 33 33
4.1 Status	
4.1 Status. 4.1.1 Overview. 4.1.2 LoRa WAN. 4.1.3 Cellular. 4.1.4 Network. 4.1.5 VPN. 4.1.6 Routing Information. 4.1.7 Host List. 4.2 LoRa 4.2.1 Packet Forwarder. 4.2.1.1 General. 4.2.1.2 Radios. 4.2.1.3 Advanced. 4.2.1.5 Traffic. 4.2.2 Network Server.	24 24 25 27 29 30 31 31 32 33 33 33 33 33 33 33 33 33 33 33 33
4.1 Status4.1.1 Overview	

4.2.2.4 Device	43
4.2.2.5 Packet	
4.3 Network	46
4.3.1 Interface	
4.3.1.1 Port	46
4.3.1.2 WAN	
4.3.1.3 LAN	50
4.3.1.4 VLAN Trunk	51
4.3.1.5 Cellular	
4.3.1.6 Loopback	55
4.3.2 Firewall	56
4.3.2.1 ACL	56
4.3.2.2 DMZ	57
4.3.2.3 Port Mapping	
4.3.2.4 MAC Binding	
4.3.3 QoS	
4.3.4 DHCP	60
4.3.4.1 DHCP Server	60
4.3.4.2 DHCP Relay	62
4.3.5 DDNS	62
4.3.6 Link Failover	63
4.3.6.1 SLA	63
4.3.6.2 Track	64
4.3.6.3 VRRP	65
4.3.6.4 WAN Failover	66
4.3.7 VPN	67
4.3.7.1 DMVPN	67
4.3.7.2 IPSec	69
4.3.7.3 GRE	72
4.3.7.4 L2TP	73
4.3.7.5 PPTP	75
4.3.7.6 OpenVPN Client	77
4.3.7.7 OpenVPN Server	78
4.3.7.8 Certifications	
4.4 System	
- 4.4.1 General Settings	
4.4.1.1 General	
4.4.1.2 Account Management	83
4.4.1.3 System Time	
4.4.1.4 SMTP	
4.4.1.5 Phone	
4.4.2 User Management	
4.4.3 SNMP	
4.4.3.1 SNMP	

	4.4.3.2 MIB View	
	4.4.3.3 VACM	
	4.4.3.4 Trap	
	4.4.3.5 MIB	91
	4.4.4 AAA	91
	4.4.4.1 RADIUS	91
	4.4.4.2 TACACS+	92
	4.3.4.3 LDAP	92
	4.3.4.4 Authentication	93
	4.3.5 Device Management	
	4.3.6 Events	95
	4.3.6.1 Events	95
	4.3.6.2 Events Settings	
	4.5 Industrial Interface	
	4.5.1 I/O	
	4.5.1.1 DI	98
	4.5.1.2 DO	
	4.5.2 Serial Port	100
	4.5.3 Modbus Master	
	4.5.3.1 Modbus Master	
	4.5.3.2 Channel	
	4.6 Maintenance	
	4.6.1 Tools	
	4.6.1.1 Ping	
	4.6.1.2 Traceroute	
	4.6.2 Schedule	
	4.6.3 Log	
	4.5.3.1 System Log	
	4.6.3.2 Log Settings	108
	4.6.4 Upgrade	109
	4.6.5 Backup and Restore	
	4.6.6 Reboot	
	4.7 APP	
	4.7.1 Python	111
	4.7.1.1 Python	111
	4.7.1.2 App Manager Configuration	
	4.7.1.3 Python App	
Cha	apter 5 Application Examples	
	5.1 Application configuration	
	5.2 Device Profiles configuration	
	5.3 Device configuration	117
	5.4 Account Info Management	120
	5.5 Common User Management	
	5.6 System Time Management	

5.7 Backup and Restore Configuration	123
5.8 Restore Factory Defaults	124
5.8.1 Via Web Interface	124
5.8.2 Via Hardware	126
5.9 Firmware Upgrade	126
5.10 Events Application Example	
5.11 Schedule Application Example	130
5.12Logs and Diagnostics	130
5.13 SNMP Application Example	132
5.14 Cellular Connection	135
5.15 Dual SIM Backup Application Example	137
5.17 NAT Application Example	140
5.18 Access Control Application Example	140
5.18 DTU Application Example	141
5.19 PPTP Application Example	145

Chapter 1 Product Introduction

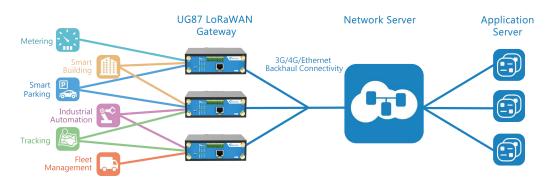
1.1 Overview

Ursalink UG87-LW is an industrial LoRa gateway with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, UG87-LW provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial platform of 64-bit CPU and wireless module, the UG87-LW is capable of providing wire-speed network with a typical 2 W power consumption and ultra-small package to ensure the extremely safe and reliable connection to the wireless network.

Meanwhile, the UG87-LW also supports Gigabit Ethernet port, serial port (RS232), which enables you to scale up M2M application combining data and video in limited time and budget.

The UG87-LW is particularly ideal for smart grid, digital media installations, industrial automation, telemetry equipment, medical device, digital factory, finance, payment device, environment protection, water conservancy and so on.





1.2 Advantages

Benefits

- Built-in industrial strong CPU, big memory;
- Dual SIM cards for backup between multiple carriers networking and global 2G/3G/LTE options make it easy to get connected
- Embed Ursalink SDK (Python 2.7/C) for secondary development
- Flexible modular design provides users with different connection modules like Ethernet, serial port for connecting diverse field assets
- 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
- With embedded hardware watchdog to automatically recover from various failure and ensure highest level of availability
- Establish a secured mechanism on centralized authentication and 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

Cellular Interfaces	
Connectors	$2 \times 50 \Omega$ SMA (Center pin: female)
SIM Slots	2
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 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
Hardware System	
CPU	800MHz, 64-bit ARM Cortex-A53
Memory	4 GB Flash, 512 MB DDR3 RAM
Ethernet	
Ports	1 × RJ-45
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)
Serial Interface	
Ports	1 × RS232
Connector	Terminal Block
Baud Rate	300bps to 230400bps
10	
Connector	(4) pin screw down terminal block
Digital	$2 \times DI + 2 \times DO$
Software	
Network Protocols	PPP, PPPOE, SNMP v1/v2c/v3, TCP, UDP, DHCP,DDNS, VRRP,
	HTTP, HTTPS, DNS, SNTP, Telnet, VLAN, SSH, 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		
AAA	RADIUS, TACACS+, LDAP, Local Authentication		
Multilevel Authority	Multiple levels of user authority		
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	ption		
Connector	2-pin with 5.08 mm terminal block		
Input Voltage	9-48 VDC		
Power Consumption	Typical 2.3 W (Max 3.2 W)		
Physical Characteristics			
Ingress Protection	IP30		
Housing & Weight	Metal, 369 g (0.81 lb)		
Dimensions	100 x 96.1 x 30 mm (3.94 x 3.78 x 1.18 in)		
Mounting	Desktop, wall or DIN rail mounting		
Others			
Reset Button	1 × RESET		
LED Indicators	$1 \times POWER$, $1 \times STATUS$, $1 \times LoRa$, $1 \times VPN$,		
	$1 \times SIM1$, $1 \times SIM2$, $3 \times Signal strength$		
Built-in	Watchdog, RTC, Timer		
Certifications	RoHS, CE, FCC		
EMC	IEC 61000-4-2 Level 3		
	IEC 61000-4-3 Level 4		
	IEC 61000-4-4 Level 3 IEC 61000-4-5 Level 4		
	IEC 61000-4-5 Level 3		
	IEC 61000-4-8 Level 4		
Environmental			
Operating Temperature	-40°C to +70°C (-40°F to +158°F) Reduced cellular		
	performance above 60°C		
Storage Temperature	-40°C to +85°C (-40°F to +185°F)		
Ethernet Isolation	1.5 kV RMS		
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F		

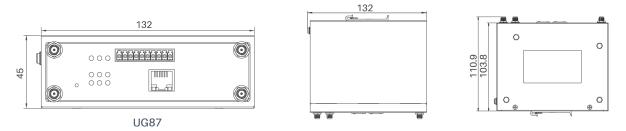
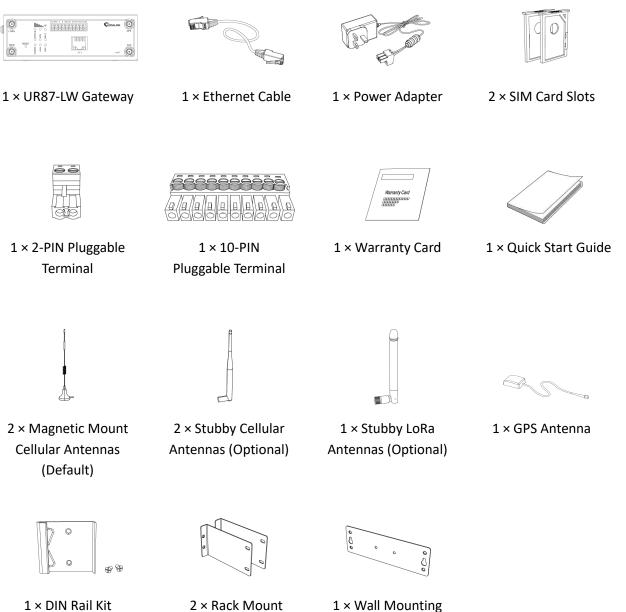


Figure 1-2

Chapter 2 Installation

2.1 General Packing List

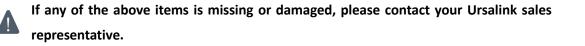
Before you begin to install the UG87-LW, please check the package contents to verify that you have received the items below.



(Default)

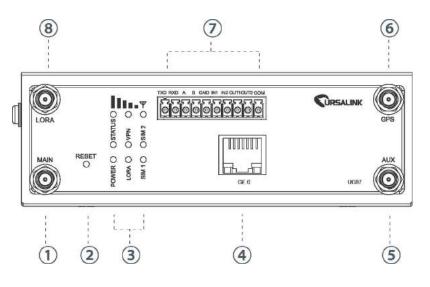
Kits (Optional)

Bracket (Optional)



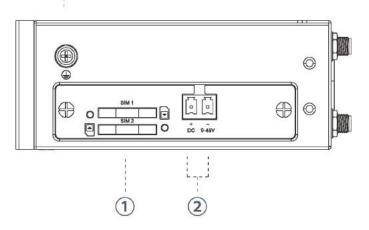
2.2 Product Overview

A. Front Panel



B. Left Panel





- ① Main Cellular Antenna
- 2 Reset Button
- ③ LED Indicator Area
 POWER: Power Indicator
 STATUS: Status Indicator
 平: Signal Strength Indicator
 LORA: LoRa Indicator
 VPN: VPN Indicator
 SIM1: SIM1 Status Indicator
 SIM2: SIM2 Status Indicator
- ④ Ethernet Port Indicator:
 Orange for data transmission;
 Green for network rate
- 5 AUX Cellular Antenna
- 6 GPS Antenna
- ⑦ Serial Port & I/O
- 8 LoRa Antenna

- ① SIM Card Slot
- ② Power Connector
- ③ Grounding Stud

2.3 LED Indicators

LED	Indication	Status	Description		
POWER	Power Status	On	The power is switched on		
		Off	The power is switched off		
		Green Light	Static: Start-up		
STATUS	System Status		Blinking slowly: the system is running properly		
		Off	The system goes wrong		
LoDo	LoRa Status	Green Light	Packet Forwarder mode is running well.		
LoRa	LORA SIdius	Off	Packet Forwarder mode is running off.		
VPN	VPN Status	Green Light	VPN is connected		
VPN	VPIN Status	Off	VPN is disconnected		
		Off	SIM1 or SIM2 is registering or fails to register		
		OII	(or there are no SIM cards inserted)		
		Green Light	Blinking slowly: SIM1 or SIM2 has been		
SIM1/SIM2	SIM Card Status		registered and is ready for dial-up		
51111/51112	SIM Card Status		Blinking rapidly: SIM1 or SIM2 has been registered and is dialing up now		
			Static: SIM1 or SIM2 has been registered and		
			dialed up successfully		
		Off	No signal		
	Signal 1/2/3		Static/Off/Off: weak signals with 1-10 ASU		
			(please check if the antenna is installed		
Signal			correctly, or move the antenna to a suitable		
Strength		Green Light	location to get better signal)		
50,00,000			Static/Static/Off: normal signals with 11-20		
			ASU (average signal strength)		
			Static/Static/Static: strong signals with 21-31		
			ASU (signal is good)		

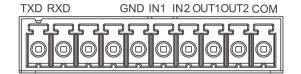
2.4 Ethernet Port Indicators

Indicator	Status	Description	
	On	Connected	
Link Indicator (Orange)	Blinking	Transmitting data	
	Off	Disconnected	
Rate Indicator (Green)	On	1000Mbps mode	
	off	100Mbps mode	

2.5 Reset Button

Function	Description			
FUNCTION	STATUS LED	Action		
Pohoot	Blinking	Press and hold the reset button for about 5-15 seconds.		
Reboot	Static Green	Release the button and wait for system to reboot.		
	Blinking	Press and hold the reset button for more than 15 seconds.		
Reset	Static Green → Rapidly Blinking	Release the button and wait.		
	$Off \rightarrow Blinking$	The gateway is now reset to factory defaults.		

2.6 PIN Definition



PIN	RS232	DI	DO	Description
1	TXD			Transmit Data
2	RXD			Receive Data
3				Data +
4				Data -
5	GND	GND		Ground
6		IN1		Digital Input1
7		IN2		Digital Input2
8			OUT1	Digital Output1
9			OUT2	Digital Output2
10			COM	Common Ground

V+ V-		
	PIN	Description
	11	Positive
	12	Negative

2.7 SIM Card Installation

A. Push the yellow button on left panel of the gateway, and then you will see the SIM card slot popping out directly.



B. Put SIM card onto the slot, and then insert the slot back into the hole.



2.8 Cellular Antenna Installation

A. Rotate the antenna into the Antenna Connector.

The external cellular antenna should be installed vertically always on a site with a good cellular signal.



Note: UG87-LW supports dual antennas with "Main" and "AUX" connectors. "Main" interface is for data receiving and transmission. "AUX" interface is for enhancing signal strength, which cannot be used separately.

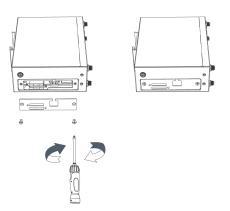
2.9 Mounting the Gateway

The gateway can be placed on a desktop or mounted to a wall or a DIN rail.

2.9.1 Wall Mounting (Measured in mm)

Use 2 pcs of M3×6 flat head Phillips screws to fix the wall mounting kit to the gateway, and then use 2 pcs of M3 drywall screws to mount the gateway associated with the wall mounting kit on the wall.

Recommended torque for mounting is 1.0 N. m, and the maximum allowed is 1.2 N.m.

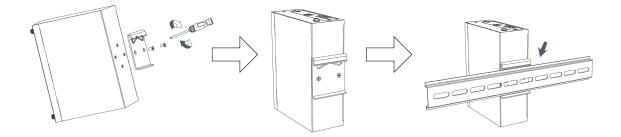


2.9.2 DIN Rail Mounting (Measured in mm)

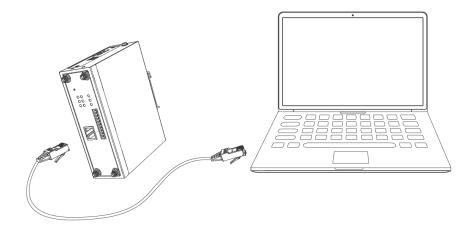
Use 2 pcs of M3×6 flat head Phillips screws to fix the DIN rail to the gateway, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.



Recommended torque for mounting is 1.0 N. m, and the maximum allowed is 1.2 N.m.



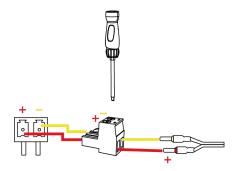
2.10 Connect the Gateway to a Computer



2.11 Installation of Power Supply and Protective Grounding

2.11.1 Power Supply Installation

- A. Take out the terminal from the gateway and unscrew the bolt on terminal.
- B. Screw down the bolt after inserting power cable into the terminal.



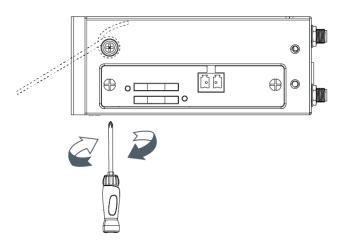
Connecting the Power Cable				
Color	Polarity			
Red	+			
Yellow	-			



If you insert wires into the reverse holes, the gateway will not start and you must switch the wires into the correct holes.

2.11.2 Protective Grounding Installation

- 1. Remove the grounding nut.
- 2. Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.





The gateway must be grounded when deployed. According to operating environment, the ground wire should be connected with grounding stud of gateway.

2.12 Examine

- 1. Double check antenna connection.
- 2. Double check if SIM card is correctly inserted and working perfectly.
- 3. Power on the UG87-LW industrial LoRaWAN gateway and check indicators status.
- (1) If Status LED blinks slowly, the system is running properly.
- (2) If SIM1 or SIM2 indicator is static green, the gateway is connected to network already.

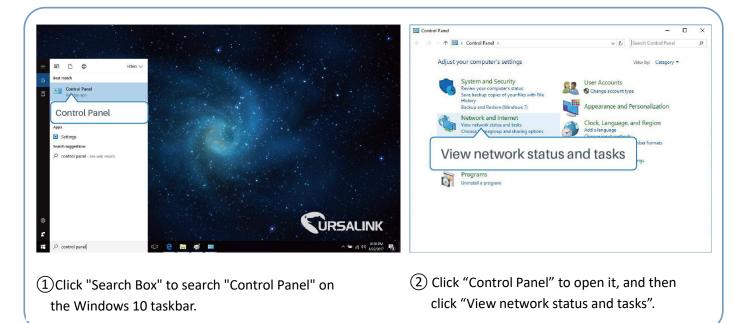
Chapter 3 Access to Web GUI

This chapter explains how to access to Web GUI of the UG87-LW.

3.1 PC Configuration for Web GUI Access to gateway

Please connect PC to GE port of UG87-LW 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 Cent	ter v Ö Search Control Panel P	General	
Control Panel Home	View your basic network infe	ormation and set up connections	- Schelar	
	View your active networks		Connection	
Change adapter settings Change advanced sharing	Yeastar5G	Access type: Internet	IPv4 Connectivity:	No network access
settings	Private network	HomeGroup: Ready to create Connections: an Wi-Fi (Yeastar5G)	IPv6 Connectivity:	No network access
		Connections: and Wi-Fi (Yeastards)	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 —		L'AL BURGET	
	Set up a new connection o	Tthorpot		
	Set up a broadband, dial-u		Activity	
	Troubleshoot problems		Aconty	
		rk problems, or get troubleshooting information.	t — 💵	Received
			Properties 7	5
			210	0
See also				
HomeGroup			Properties Diable Dia	gnose
Infrared				griose
Internet Options			1	-
Windows Firewall				Close
14				
(3) Click "Fth	ernet" (May h	ave different name).	(4) Click "Propertie	- 11

UG87-LW User Guide

Ethernet	Properties			
letworking	Sharing			
Connect us	sing:			
🚽 Intel	(R) 82567LM	1 Gigabit Network	Connection	
			Cor	figure
This conne	ction uses th	ne following items	_	
🗹 🌄 Cli	ient for Micro	osoft Networks	Section 2.	1
		r Sharing for Micn	osoft Networks	
	oS Packet S			
inner Second		col Version 4 (TCI	and the second second second	
inner Second		col Version 4 (TC)	and the second second second	
🗆 🔔 Mi	icrosoft Nety et Prot	and provide the second second second second	iplexor Protocol	
Intern	et Prot	Adapter Mult	iplexor Protocol	P/IPv
Intern	et Prot all on assion Control a network pr	Adapter Mult	iplexor Protocol ion 4 (TC Prot t Protocol. The des communicat	P/IPv perties default
Intern	et Prot all on assion Control a network pr	Adapter Mult	iplexor Protocol ion 4 (TC Prot t Protocol. The des communicat	P/IF perties default

ernet P	rotocol Version 4 (TCP/IPv	4) Propertie	25		×		
eneral	Alternate Configuration	Alternate Configuration					
this cap	get IP settings assigned auto ability. Otherwise, you need appropriate IP settings.						
Ob	otain an IP address automatic	ally					
OUs	e the following IP address:						
IP ac	dress:		5				
Subn	et mask:		a:	3			
Defa	ult gateway:			- 14			
() Ob	tain DNS server address auto	matically					
OUs	e the following DNS server ad	dresses:					
Prefe	rred DNS server:		- (2)				
Alter	nate DNS server:						
V	alidate settings upon exit			Advance	d		
			OK		d		

- (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";

ternet Proto	ocol Version 4 (TCP)	/IPv4) Properties	×
General			
this capabili	IP settings assigned ty. Otherwise, you n opriate IP settings.		
() Obtain	an IP address auton	192.168.1.1	
• Use th	e following IP addres	s.	
IP addres	is:	192 . 168 . 1 . 20	
Subnet m	ask:	255 . 255 . 255 . 0	
Default g	ateway:	192.168.1.1	
Ohtain	DNS server address	automatically	
	e following DNS serv		
Preferred	DNS server:	192.168.1.1	
Alternate	DNS server:		
Valida	te 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.)

3.2 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

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

http:/	//192.168.1	.1	
		Constant for the	
		Lisemania	

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.

Old Password	1	1
Old Password	-	
New Password		
Confirm New Passwor	d	
	-Mi	

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

<i>WRSALINK</i>								
Status	Overview	LoRa	Cellular	Network	VPN	Routing	Host List	
LoRaWAN	System Informa	tion						
Network 🕨	Model Partnumber		UG87-LW LD0E-S1122	GPS				
System 🕨	Serial Number Firmware Version		6216832718 87.1.0.2	73				
Industrial 🕨	Hardware Version		V1.3					
Maintenance +	Local Time Uptime		2018-09-04 1	17:04:49				
APP 🕨	CPU Load RAM (Capacity/A	vailable)	10% 512MB/275A	AB(53.71%)				
	Flash (Capacity/A	wallable)	64MB/37MB	(57 81%)				
	eMMC (Capacity/	Available)	3 66/3 16(9	4%)				

Chapter 4 Web Configuration

4.1 Status

4.1.1 Overview

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

URSALIN	C				
Status		Overview	LoRa	Cellular	Network
LoRaWAN	×	System Information			
		Model		UG87-LW	
Network	•	Partnumber		L00E-S1122	-GPS
System		Serial Number		6216832718	73
		Firmware Version		87.1.0.2	
Industrial		Hardware Version		V1.3	
		Local Time		2018-09-04	17:04:49
Maintenance		Uptime		02:42:41	
APP		CPU Load		10%	
		RAM (Capacity/A	vailable)	512MB/275	MB(53.71%)
		Flash (Capacity/A	vailable)	64MB/37ME	8(57.81%)
		eMMC (Capacity/	Available)	3.6G/3.1G(9	94%)
		eiviivio (Capacity/	Available)	3.00/3.10(5	(470)

Figure 4-1-1-1

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.			
Flash (Capacity/Available)	Show the Flash capacity and the available Flash memory.			
eMMC (Capacity/Available)	Show the eMMC capacity and the available eMMC memory.			

Table 4-1-1-1 System Information

4.1.2 LoRa WAN

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 4-1-4-4

LoRaWAN Status (Packet F	orwarder 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				
Region Code	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				
Fackets 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 4-1-4-4 LoRaWAN Status (Packet Forwarder Mode)

Status		Overview	LoRa	Cellular	Network	VPN	6) - SI	Routing	Host Lis	t				
LoRaMAN	+	Basic												
Network	٠	Mode Version		Net 1.0	work Server									
System	•	Status			ming									
industrial		Gateways												
Maintenance	۲		EU	СЬФ	Ch1	Ch2	Ch3	Ch4	Ch5	Ch6	Ch7	LoRa	FSK	Operation
APP	×	24E12	4FFFE087443	0	29	10	0	0	0	1146	0	0	1145	• =

Figure 4-1-4-5

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

Table 4-1-4-5 LoRa WAN-Status-Network Server

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

Click (I) to view the details of the connected gateway, as the following picture shows.

ateway	Details										
Gateway	EUI				24E124FI	FE0B7443					
IP Addres	s				localhost	E0					
Version					4.0.1						
Uplink					1170						
Downlink					15						
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

LoRa WAN-Network Server-Status-Gateway Detail						
ltem	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					
LUNA	LoRa channel.					
FSK	Show the frequency of FSK channel and number of packets received on FSK					
I JN	channel.					
CRC	Show the total number of packets with CRC error.					
Toal	Show the total number of packets received by the gateway.					

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

4.1.3 Cellular

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 (-83dBn	ו)		
Register Status		Registered (Ho	ome network)		
IMSI		460019987103	071		
ICCID		89860 <mark>11</mark> 78380	19196629		
ISP		CHN-UNICOM			
Network Type		LTE			
PLMN ID		46001			
LAC		<mark>5922</mark>			
Cell ID		812c63d			
IMEI		861107031710	008		

Figure 4-1-2-1

Modem Information	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.					
Register Status	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 4-1-2-1 Modem Information

Network

Status	Connected
IP Address	10.53.2 <mark>41</mark> .18
Netmask	255.255.255.252
Gateway	10.53.241.17
DNS	218.104.128.106
Connection Duration	0 days, 00:04:26

Figure 4-1-2-2

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 4-1-2-2 Network Status

4.1.4 Network

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

NAN							
Port	Status	Туре	IP Address	Netmask	Gateway	DNS	Duration
GE 0	цр	Static	192.168.23.94	255 255 255 0	192 168 23 1	114.114.114.114	12m 14s

Figure 4-1-3-1

LAN Status	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 IPv 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.					

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

Table 4-1-3-1 LAN Status

4.1.5 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		21	8
	pptp_2	Disconnected		7)	
	pptp_3	Disconnected		1	
L2TP Tunnel					
	Name	Status		Local IP	Remote IP
	l2tp_1	Disconnected		23	5
	l2tp_2	Disconnected		73	
	l2tp_3	Disconnected			



Overview	Cellular	Network	VPN	Routing	Host List
IPsec Tunnel					
	Name	Status		Local IP	Remote IP
	ipsec_1	Disconnected		850	21
	ipsec_2	Disconnected		(7)	172
	ipsec_3	Disconnected			

OpenVPN Client

Name	Status	Local IP	Remote IP
openvpn_1	Disconnected	450	2
openvpn_2	Disconnected		
openvpn_3	Disconnected	~	: #

Figure 4-1-4-2

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



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 4-1-4-1 VPN Status		

4.1.6 Routing Information

You can check routing status on this page, including the routing table and ARP cache.

Overview	Cellular	Network	VPN	Routing	Host List	
Routing Tab	le					
	Destination	Netmask	Gat	eway	Interface	Metric
	0.0.0.0	0.0.0.0	192.1	68.23.1	GE	1
	127.0.0.0	255.0.0.0		5 4	Loopback	-
	192.168.23.0	255.255.255.0			GE	
ARP Cache						
	IP		MAC			Interface
	192.168.23.21		e0:d5:5e:50:b4	4:c0	GE	
	192.168.23.111		00:00:00:00:00		GE	
	192.168.23.40		1c:1b:0d:f8:fe:06		GE	
	192.168.23.1		24:e1:24:f0:01	l:97		GE

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

Item	Description
Routing Table	

Destination	Show the IP address of destination host or destination network.
Netmask	Show the netmask of destination host or destination network.
Gateway	Show the IP address of the gateway.
Interface	Show the outbound interface of the route.
Metric	Show the metric of the route.
ARP Cache	
IP	Show the IP address of ARP pool.
MAC	Show the IP address's corresponding MAC address.
Interface	Show the binding interface of ARP.

Table 4-1-6-1 Routing Information

4.1.7 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	2			MAC	

```
Figure 4-1-7-1
```

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 DHCP service.

Table 4-1-7-1 Host List Description

4.2 LoRa

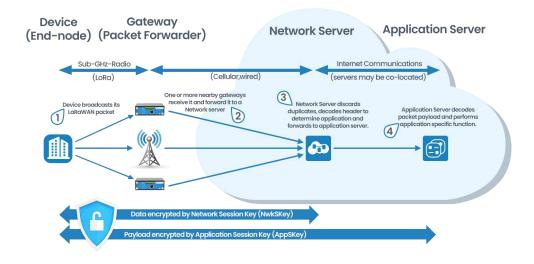


Figure 4-2-1-1

4.2.1 Packet Forwarder

4.2.1.1 General

Status		General	Radios	Advanced	Custom	Traffic
LoRaWAN	-	General Setting	g			
Packet Forwarder		Enable Mode		Please close Packet Forward	se the Network Serve	er mode first
Network Server		Gateway EUI		24E124FFFE	0B6543	
Network	•	Gateway ID		24E124FFFE	0B6543	
HCIWOIN .		Server Address		localhost		
System		Server Up Port		1700		
		Server Down Po	rt	1700		
Industrial	•					
Maintenance						
APP						



General Setting				
Item	Description	Default		
Enable	Click to enable the Packet Forwarder mode.	Enabled		
Gateway EUI	Show the identifier of the gateway.	Generated from MAC address of the gateway and cannot be changed.		
Gateway ID	Fill in the corresponding ID which you've used for	The default is the		

	register gateway on the remote network server, such as TTN. It is usually the same with gateway EUI and can be changed.	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 4-2-1-1 General Setting Parameters

4.2.1.2 Radios

General	Radios	Advanced	Custom	Traffic			
Radio Channe	l Setting						
Supported Frequ	iency			A5923	*		
		Name				Center Frequency/MHz	
		Radio 0				923.6]
		Radio 1				922.6	

Figure 4-2-1-3

Radios-Radio Channels 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 4-2-1-2 Radio Channels Setting Parameters

Multi Channels Setting

Enable	Index	Radio	Frequency/MHz
2	0	Radio 0 🔹	923.2
2	1	Radio 0 🔹	923.4
2	2	Radio 0 *	923.6
e.	3	Radio 1 🔹	922.2
×.	4	Radio 1 🔹	922.4
2	5	Radio 1 🔻	922.6
ø	6	Radio 1 💌	922.8
	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 4-2-1-3 Multi Channel Setting Parameters

LoRa Channel Setting

Enable	Radio	Frequency/MHz	Bandwidth/KHz	Spread Factor
×	Radio 0 🔹	923.8	250KHZ *	SF7 •

Figure 4-2-1-5

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 4-2-1-4 LoRa Channel Setting Parameters

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

Figure	4-2-1-6
1 Barc	

Radios-FSK Channel Setting				
Item	Description	Default		
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 4-2-1-5 FSK Channel Setting Parameters

4.2.1.3 Advanced

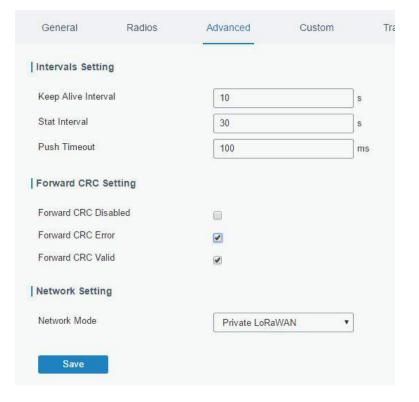


Figure 4-2-1-7

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 4-2-1-6 Advanced Parameters

4.2.1.4 Custom

General	Radios	Advanced	Custom	Traffic
Custom Confi	guration			
Enable				
				Example
"antenna_gain "radio_0": { "enable": true, "type": "SX125 "freq": 922500 "rssi_offset": - "tx_enable": tr "tx_freq_min":	ilc": true, adio_1 provides clo ": 0, /* antenna gair 57", 0000, 162, ue, 917000000,	ck to concentrator */ n, in dBi */		
"tx_freq_max" }, "radio_1": {	: 923500000			



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.

4.2.1.5 Traffic

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

1.5	1.000	20			
Traf	TIC	Set	tti	ne	

Refresh	Clear							
Rich	Direction	Time	Ticks	Frequency	Datarato	Coderate	RSSI	SNR
1	up	<i>7</i> 2	83002508	922 8	SF9BW125	4/5	-103	-13.2
1	up	÷.	71108156	922.6	SF9BW125	4/5	-102	-13.2
1	up	2	35426956	922.8	SF9BW125	4/6	-103	-9.8
1	up	70	3171639508	922.6	SF9BW125	4/5	-100	-10.5
1	up	¥1	3159744804	922.6	SF9BW125	4/5	-102	-13.0
1	up	2	3155781348	922.6	SF9BW125	4/5	-101	-12.2
1	up	÷	3147851660	922 6	SF9BW125	4/5	-102	-13.8
1	up	*	3143888916	922.8	SF9BW125	4/5	-102	-13.2
1	up	52	3139922740	922.8	SF9BW125	4/5	-100	-12.2
. 1	up	*	3124065788	922.8	SF9BW125	4/5	-100	-12.8

Figure 4-2-1-9

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 4-2-1-7 Traffic Parameters

4.2.2 Network Server

4.2.2.1 General

Status		General	Applications	Profiles	Device
LoRaWAN	~	General Settin	g		
Packet Forwarder		Enable	2		
		Mode	Net	work Server	
Network Server		NetID	010	203	
Network		Join Delay	5		sec
		RX1 Delay	1		sec
System	×	Lease Time	32-0	0-0	hh-mm-ss
Industrial	•	Log Level	info	0	
Maintenance		Channel Plan	Setting		
Wantenance	8	Channel Plan	AS	923	¥
APP	×	Channel Mask			

Figure 4-2-2-1

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 server and the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
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 agagin when it exceeds the lease time.	"744-00-00"
Loglevel	Choose the log level.	Info
Channel Plan Setti	ing	
Channel Plan	Choose LoRaWAN channel plan used for the upstream and downlink frequencies and	Depend on the gateway's variant.

	datarates. Available channel plans depend on the gateway's vatiant.	
	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.	Null. Null means using
Channel Mask	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.	the default standard usable channels which are specified in the LoRaWAN regional parameters
	A bit set to 0 means the corresponding channels should be avoided.	document.
	US and AU 915 have a 80-bit channel mask for 72 usable channels and EU, AS, IN, KR have a 16- bit mask for 16 usable channels.	

Table 4-2-2-1 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:

tional Channels			
Frequency(MHz)	Min Datarate	Max Datarate	Operation
			8

Figure 4-2-2-2

Additional Channels				
ltem	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 4-2-2-2 Additional Plan Parameters

4.2.2.2 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.

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

Figure 4-2-2-3

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 4-2-2-3 Application Parameters

You can edit the application by clicking 🖉 or create a new application by clicking 🛅.

Related Configuration Example

Application configuration

4.2.2.3 Profiles

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

Name	Max TXPower	Join Type	Class Type	Operatio n
Device-test	0	OTAA	Class A	
Ursalink-test-ABP	0	ABP	Class A	
ninli	0	OTAA	Class A	2 ×

Figure 4-2-2-4

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 4-2-2-4 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 configuration

4.2.2.4 Device

Device <mark>N</mark> ame	Device EUI	Device-Profile	Application	Last Seen	Actived	Operatio n
asd	353035308337611 8	ninii	AS923	53 minutes ago	~	ZX



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 . we means that the device has
	been activated.

Table 4-2-2-5 Device Parameters

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



Related Configuration Example

Device configuration

4.2.2.5 Packet

Clear									
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Detail
3530353083376118	923200000	SF10BW12 5	51	ਰ	0	0	DnUnc	2018-09- 04T09:05:49+08:00	0
3530353083376118	923200000	SF10BW12 5	10.5	-45	8	0	UpCnf	2018-09- 04T09:05:48+08:00	0
3530353083376118	923400000	SF10BW12 5	÷.	×	17	0	JnAcc	2018-09- 04T09:05:28+08:00	0
3530353083376118	923400000	SF10BW12 5	10.2	-38	18	0	JnReq	2018-09- 04T09:05:28+08:00	0

Figure 4-2-2-6

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	Show the type of the packet: JnAcc - Join Accept Packet JnReq - Join Request Packet UpUnc - Uplink Unconfirmed Packet UpCnf - Uplink Confirmed Packet - ACK response from network requested DnUnc - Downlink Unconfirmed Packet DnCnf - Downlink Confirmed Packet- ACK response from end-device requested
Time	Show the time of packet was sent or received.

Table 4-2-2-6 Packet Parameters

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

Packets Details		×
Dev Addr	068c1b56	*
GwEUI	24e124fffe0b7443	
AppEUI	70b3d57ed0007ac1	
DevEUI	3530353083376118	
Immediately	false	
TimeSinceGPSEpoch	2	
Timestamp	242616788	
Туре	DnUnc	
Adr	true	
AdrAcKReq	false	
Ack	true	1
Fcnt	*	
Fport		-

Figure 4-2-2-7

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
Type	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.
, (d)	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.
АСК	False: This frame is not ACK.
	Show the frame-counter of this packet. The network server tracks the
Fcnt	uplink frame counter and generates the
	downlink counter for each end-device.
	FPort is a multiplexing port field. If the frame payload field is not empty,
	the port field must be present. If present, a FPort
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.
	Show the MIC of this packet.MIC is a cryptographic message integrity
MIC	code, computed over the fields MHDR, FHDR, FPort and the encrypted
	FRMPayload.

Table 4-2-2-7 Packets Details Parameters

4.3 Network

4.3.1 Interface

4.3.1.1 Port

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
Port Settin	9				
	Port	Status	Property	Speed	Duplex
	GE 0	up 🔹	wan 🔻	auto 🔻	auto 🔻
			Figure 4-3	-1-1	

Port Setting	5
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 4-3-1-1 Port Parameters

4.3.1.2 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.

URSALINK			
		For your device security, please	change the default password
Status	Port WAN	LAN VLAN Trunk	Cellular Loopback
LoRaWAN	— WAN_1		
Network 🔻	Enable		
Interface	Port	GE 0]
Firewall	Connection Type IP Address	Static IP •	
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	114.114.114.114]
VPN	Enable NAT	Ø	

Figure 4-3-1-2

WAN Setting						
Item	Description	Default				
Enable	Enable WAN function	Enable				
Port	The port that is currently set as WAN port.	GE 0				
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP				
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 4-3-1-2 WAN Parameters

1. Static IP Configuration

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

	For your device security please manage the defaultmassworth											
Status	Î	Port WAN LAN	VLAN Trunk Cellular	Loopback								
LoRaWAN		Enable	8									
		Port	GE 0									
Network	-	Connection Type	Static IP 🔹									
Interface		IP Address	192.168.23.141									
Firewail		Netmask	255,255,255,0									
		Gateway	192.168.23.1									
QoS		MTU	1500									
DHCP		Primary DNS Server	8888									
DDNS		Secondary DNS Server	114.114.114.114									
Link Failover		Enable NAT	×									
VPN		Multiple IP Address										
		1	P Address	Netmask	Operation							

Figure 4-3-1-3

Static IP	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 4-3-1-3 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 secu	irity, please change th	e default password
Status	Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
LoRaWAN	— WAN_1					
Network 🔫	Enable			v		
Interface	Port	tion Type		GE 0 DHCP Client		
Firewall	MTU	lion Type		1500		
QoS	Use Pe	er DNS				
DHCP	Primary	DNS Server		8.8.8.8		
DDNS		ary DNS Server		114.114.114.1	14	
Link Failover	Enable	NAT		2		
VPN	Save & Apply					

Figure 4-3-1-4

DHCP Client				
Item	Description			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.			

Table 4-3-1-4 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 t	ne default password
Status	Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
LoRaWAN	- WAN_	1				
Network -	Enabl	e		۲		
Interface	Port			GE 0		
Firewall	Usern	ection Type Iame		PPPoE		
QoS	Passv	vord				
DHCP	Link D	etection Interval	(s)	60		
DDNS	Max F	Retries		0		
	MTU			1500		
Link Failover	Use F	eer DNS				
VPN	Prima	ry DNS Server		8.8.8.8		
System	Secon	ndary DNS Serve	er	114.114.114.11	14	
Jacin	Enabl	e NAT				

Figure 4-3-1-5

РРРОЕ					
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	Set the heartbeat interval for link detection. Range: 1-600.				
Interval (s)					
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 4-3-1-5 PPOE Parameters

4.3.1.3 LAN

LAN setting is used for managing local area network devices connected to LAN port of the UG87-LW, allowing each device to access the Internet.

Click \blacksquare to delete the existing LAN port setting. Click \boxplus to add a new LAN port setting.

Port		VLAN Trunk	Cellular	Loopback		
	Port	IP Address		Netmask	MTU	Operation
GE	Ŧ	192.168.23. <mark>47</mark>	255	255.255.0	1500	×
						8



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 4-3-1-6

4.3.1.4 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 4-3-1-7 VLAN Trunk Parameters

4.3.1.5 Cellular

This section explains how to set the related parameters for cellular network. The UG87-LW 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 UG87-LW cannot connect to the network via SIM1, it will automatically fail over to SIM2.

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
Cellular Se	etting				
		SIM1		SIM2	
Enable					
Network Ty	pe			•	•
APN					
Username					
Password					
Access Nu	mber				
PIN Code					
Authenticat	tion Type	Auto	2	▼ Auto	۲
Roaming		0			
SMS Cente	¥r				

Figure 4-3-1-8

Connection Setting	8	
Dual SIM Strategy		
Enable NAT		
Restart When Dial-up failed		
ICMP Server	8.8.8.8	
Secondary ICMP Server	114.114.114.114	
PING Times	5	
Packet Loss Rate	20	%
SMS Settings		
SMS Mode	PDU	•

Figure 4-3-1-9

General Settings		
Item	Description	Default
Enable	Check the option to enable the corresponding SIM card.	Enable
Network Type	 Select from "Auto", "4G First", "4G Only", "3G First", "3G Only", "2G Frist", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G First: 4G network takes precedence. 4G Only: connect to 4G network only. 	Auto
	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 4-3-1-8 Cellular Parameters

Connection Setting	
Connection Mode	Connect on Demand
Redial Interval(s)	5
Max Idle Time(s)	60
Triggered by Call	0
Triggered by SMS	
Triggered by IO	8
Dual SIM Strategy	2
Primary SIM Card	SIM1
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 4-3-1-10

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

Table 4-3-1-9 Cellular Parameters

Related Topics

Cellular Connection Application Example Dual SIM Backup Application Example Phone Group

4.3.1.6 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		Netma	ask	Operation
]	255.255.255.255		×
						8

Figure 4-3-1-11

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 4-3-1-10 Loopback Parameters

4.3.2 Firewall

This section describes how to set the firewall parameters, including 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.

4.3.2.1 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.

Status		ACL	DMZ	Port Mapping	MAC Bi	nding		
LoRaWAN		ACL Setting	l.					
		Default Filter	Policy	Accept	•			
Network	-	Access Con	trol List					
Interface				Туре	[extended	*	
Firewall				ID				
DHCP				Action		permit		
				Protocol	L	ip	•	
DDNS				Source IP	[
Link Failover				Source Wildcard Mask		0.0.0.0		
VPN				Destination IP				
				Destination Wildcard M	ask [0000		
System	. •			Description				
Industrial	. •				Save	Cancel		
		Interface Li	st					
Maintenance	2		Interface		In ACL		Out ACL	Operation
APP	×							8

Figure 4-3-2-1

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.
ICMP Type	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	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 4-3-2-1 ACL Parameters

Related Configuration Example

Access Control Application Example

4.3.2.2 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
Enable			
DMZ Host			
Source Add	ress		

Figure 4-3-2-2

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 4-3-2-2 DMZ Parameters

4.3.2.3 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 🛨 to add a new port mapping rules.

ACL	DMZ	Port M	Mapping	MAC Bindin	9		
Port Mapp	bing						
Sou	urce IP	Source Port	Destination IP	Destinati on Port	Protocol	Description	Operation
0.0.0/0)				TCP 🔹		×
							Œ

Figure 4-3-2-3

Port Mapping				
Item	Description			
Source IP	Specify the host or network which can access local IP address.			
Jource II	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	received on the incoming interface.			
Destination Port	Enter the TCP or UDP port that packets are forwarded to after			
Destination Fort	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 4-3-2-3 Port Mapping Parameters

Related Configuration Example

NAT Application Example

4.3.2.4 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 Bir	nding List				
	MAC Address	IP Ad	dress	Description	Operation

Figure	4-3-2-4
inguic	7 5 2 7

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 4-3-2-4 MAC Binding Parameters

4.3.3 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.

	102			For your device s	ecurity, please change the	detault password			
Status	ĵ.	QoS(Download)	QoS(Upload)						
oRaWAN	•	Download Bandwidth							
Network	-	Enable Default Class		*					
Interface		Download Bandwidth	0	kbilse	5				
Firewall		Capacity Service Class							
QuS		Name		Percent(%)	Max BW	kbps)	Min BW(kbos)	Operation
DHCP									8
DDNS		Service Class Rules							
Link Failover		Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Class	Operation
VPN						Poit		Chass	

Figure 4-3-3-1

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 that		
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.		
Max BW(kbps)	The maximum bandwidth that this class is allowed to 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.		
Classification 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 4-3-3-1 QoS (Download/Upload) Parameters

4.3.4 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.

4.3.4.1 DHCP Server

The UG87-LW 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	DHCP Server DHCP Rel	ay		
LoRaWAN 🕨	DHCP Server_1			
Network 👻	Enable	GE 0 V		
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 Server	114.114.114.114		
DDNS	Secondary DNS Server Windows Name Server			
Link Failover	Static IP			
VPN	Static IP MAC Ac	Idress	IP Address	Operation
System				E

Figure 4-3-4-1

DHCP Server		
Item	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 4-3-4-1 DHCP Server Parameters

4.3.4.2 DHCP Relay

The UG87-LW 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		



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 4-3-4-2 DHCP Relay Parameters

4.3.5 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 1D	Password	Server	Server Path	Hostname	Appe nd IP	
Interface												
Firewall		Save										
QuS												
внср												
DDNS												



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 4-3-5-1 DDNS Parameters

4.3.6 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.

4.3.6.1 SLA

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

interface	SLA	Track	VRRP	WAN Failover							
	SLA Entry										
Firewall			-	Secondary			Timesouth	DING:	Packet		
QuS	ID	Туре	Destination Address	Destination Address	Data Size	Interval(s)	Timeout(ms)	PING Times	Loss Rate	Start Time	Operatio
DHCP	1	icmp-echo 🔹	114.114.114.114	8.8.8.8	58	30	5000	5	20	now 🔻	\mathbf{x}
DDNS											8
Link Failover											

Figure 4-3-6-1

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	20

	exceeded.	
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA	now
	detection doesn't start.	

Table 4-3-6-1 SLA Parameters

4.3.6.2 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 4-3-6-2

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 4-3-6-2 Track Parameters

4.3.6.3 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.

				For your device security	y, please change the default passw
	SLA	Track	VRRP	WAN Failover	
Interface					
Firewall	VRRP Stat	tus			
	Status		DISA	BLE	
QoS	VRRP Set	tings			
DHCP	Enable				
	Interface		GE	0	¥
DDNS	Virtual Rou	iter ID			
Link Failover	Virtual IP		1		
VPN	Priority		100		
	Advertisen	nent Interval(s)	1		
ystem 🕨	Preemption	n Mode			
	Track ID				Ŧ
ndustrial 🕨 🕨			L		



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	

Priority	The VRRP priority range is 1-254 (a bigger number indicates a 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 4-3-6-3 VRRP Parameters

4.3.6.4 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.

					For your device security	, please criange the d	efault cases with		
	^	SLA	Track	VRRP	WAN Failover				
Interface		100005-0			-				
Firewall		WAN Failove							
QoS		Main Int	erface	Backup Interface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operatio
		Cellular 0	•	GE Ø	30	0	0	1 *	×
DHCP									Ð
DDNS									Brass ()
Link Failover		Save							
Lans Francisco									
VPN									



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 4-3-6-4 WAN Failover Parameters

4.3.7 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 UG87-LW supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

4.3.7.1 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.

CURSALINK

Status	DMVPN	IPsec	GRE	L2TP	PPTP
	DMVPN Settin	ngs			
LoRaWAN	Enable			8	
Network	Hub Address				
	Local IP Addr	ess		[
Interface	GRE HUB IP	Address			
Firewall	GRE Local IP	Address		Ċ.	
	GRE Mask			255.255.255.0	
QoS	GRE Key			[
DHCP	Negotiation M	lode		Main	•
	Authentication	n Algorithm		DES	٣
DDNS	Encryption Ale	gorithm		MD5	Ŧ
Link Failover	DH Group			MODP768-1	Ţ
	Key			(
VPN	Local ID Type			Default	•
System I	IKE Life Time	(s)		10800	
	SA Algorithm			DES-MD5	٠
ndustrial	PFS Group			NULL	Ţ
	Life Time(s)			3600	

Figure 4-3-7-1

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

Figure 4-3-7-2

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 Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and "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.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "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 4-3-7-1 DMVPN Parameters

4.3.7.2 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.

IPsec	000		
	GRE	L2TP	PPTP
5			
teway Address			
de	T	unnel	•
tocol	E	SP	•
onet			
onet Mask			
Гуре	D	efault	•
Subnet			
Subnet Mask			
D Type	D	efault	•
	eway Address de tocol met Mask ype ubnet ubnet Mask	eway Address	eway Address de Tunnel tocol ESP net net Mask U Upefault ubnet ubnet

Figure 4-3-7-3

IPsec		
ltem	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 4-3-7-2 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	T
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	Ŧ
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".		
Encryption Algorithm	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 4-3-7-3 IPsec Parameters

4.3.7.3 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.

DMVP	N	IPsec	GRE	L2TP	PPTP
GRE Se	ettings				
— GI	RE_1				
Er	nable			V	
R	emote IP Ad	dress			
Lo	cal IP Addre	ess		1	
Lo	ocal Virtual II	^o Address			
Ne	etmask			255.255.255.0	
Pe	eer <mark>Virtual</mark> IP	Address		[
GI	lobal Traffic l	Forwarding		8	
R	emote Subn	et			
Re	emote Netm	ask			
М	TU			1500	
Ke	∋y				
Er	nable <mark>N</mark> AT				

Figure 4-3-7-5

GRE		
Item	Description	
Enable	Check to enable GRE function.	

Enter the real remote IP address of GRE tunnel.
Enter the real remote if address of GRE turnel.
Set the local IP address.
Set the local tunnel IP address of GRE tunnel.
Set the local netmask.
Enter remote tunnel IP address of GRE tunnel.
All the data traffic will be sent out via GRE tunnel when this
function is enabled.
Enter the remote subnet IP address of GRE tunnel.
Enter the remote netmask of GRE tunnel.
Enter the maximum transmission unit. Range: 64-1500.
Set GRE tunnel key.
Enable NAT traversal function.

Table 4-3-7-4 GRE Parameters

4.3.7.4 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 IF	Address			
Username				1
Password				
Authentica	ation	A	uto	¥
Global Tra	iffic Forwarding			
Remote S	ubnet			
Remote S	ubnet 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.

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

Figure 4-3-7-7

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 Detection Interval (s)	Set the link detection interval time to ensure tunnel
LINK DELECTION INTERVAL(S)	connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection

User can enter some other PPP initializa	
Export Options	ation strings in this
Expert Options field and separate the strings with blan	k space.

Table 4-3-7-6 L2TP Parameters

4.3.7.5 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 IF	^o Address			
Username	э			
Password	l.			
Authentic		1	Auto	•
	affic Forwarding			
Remote S	Subnet Subn <mark>et</mark> Mask			
Remote S	oubliet Wask			



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 4-3-7-7 PPTP Parameters

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

Figure 4-3-7-9

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 4-3-7-8 PPTP Parameters

Related Configuration Example

PPTP Application Example

4.3.7.6 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).

IVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certific
enVPN Clier	nt Settings						
OpenVPN	1						
Enable							
Protocol		UDF	2	Ŧ			
Remote IP	Address						
Port		1194					
Interface		tun		•			
Authentica	tion	Non	e	¥			
Local Tunr	nel IP						
Remote Tu	innel IP						
Enable NA	π						
Compressi	on	LZC		•			
Link Detec	tion Interval(s)	60					
Link Detec	tion Timeout(s)	300					
Cipher		Non	e	•			
MTU		1500	1				
Max Frame	e Size	1500	1				
Verbose Le	evel	ERF	ROR	•			
Expert Opt	ions						
Local Rou	te						
		Subnet			Subnet Mas	;k	Operation
							H

Figure 4-3-7-10

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

Destand					
Protocol	Select from "UDP" and "TCP".				
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.				
Port	Enter the listening port number of remote OpenVPN server.				
	Range: 1-65535.				
Interface	Select from "tun" and "tap".				
Authentication	Select from "None", "Pre-shared", "Username/Password",				
Admentication	"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	Chack to onable TLS authentication				
Authentication	Check to enable TLS 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",				
Cipitei	"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".				
Export Options	User can enter some other PPP initialization strings in this field				
Expert Options	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 4-3-7-9 OpenVPN Client Parameters

4.3.7.7 OpenVPN Server

The UG87-LW 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 Serve
OpenVPN Serv	ver Settings					
Enable						
Protocol		UDP		*		
Port		1194				
Listening IP						
Interface		tun		Ŧ		
Authentication		None		*		
Local Virtual IP						
Remote Virtual I	P					
Enable NAT		×				
Compression		LZO		*		
Link Detection I	nterval	60				
Cipher		None		*		
MTU		1500				
Max Frame Size	1	1500				
Verbose Level		ERROR		•		
Expert Options						



Local Route			
	Subnet	Netmask	Operation
Account			
	Username	Password	Operation
			(H)

Figure	1 2 7 1 2
riguie	4-3-7-12

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",				
Authentication	"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".
	User can enter some other PPP initialization strings in this
Expert Options	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 4-3-7-10 OpenVPN Server Parameters

4.3.7.8 Certifications

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVP	N Server	Certifications
OpenVPN Clie	nt							
- OpenVPN	l client_1							
CA				Browse	Import Export	Delete		
Public Ke	у			Browse	Import Export	Delete		
Private Ke	ву 📕			Browse	Import Export	Delete		
TA				Browse	Import Export	Delete		
Preshare	d Key			Browse	Import Export	Delete		
PKCS12				Browse	Import Export	Delete		
				Figure 4-3-	-7-13			
	Open\	PN Client	t					
	Item		Descript	tion				

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 4-3-7-11 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
	TA	Browse	Import	Export	Delete
	CRL	Browse	Import	Export	Delete
	Preshared Key	Browse	Import	Export	Delete

Figure 4-3-7-14

OpenVPN Server				
Item	Description			
CA	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 4-3-7-12 OpenVPN Server Parameters

IPse	c				
-	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 4-3-7-15

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 4-3-7-13 IPsec Parameters

4.4 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.

4.4.1 General Settings

4.4.1.1 General

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

Status	General	System Time	SMTP	Phone	Email	
Lorawan	System					
Network	Hostname Web Login Tim	eout(s)	ROUTER 1800			
System	Access Servi	ce				
General Settings	Ser	vice	Port	Local		Remote
	H	ТР	80			N
User Management	HT	(PS	443	2		2
SNMP	TEL	NET	23			8
ллл	S	бН	22	×		X
Device Management	HTTS Certific	ates				
Events	Certificate	https.crt	Browse	Import Export	Delete	
ndustrial	Key	https:key	Browse	Import Export	Delete	
Maintenance	Save					
APP						



General					
Item	Item Description				
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)		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 4-3-1-1 General Setting Parameters

4.4.1.2 Account Management

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.

General	Account	System Time	SMTP	Phone	Storage
Change Acco	unt Info				
Username		admin			
Old Password					
New Password					
Confirm New P	assword				



Account	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 4-4-1-2 Account Information

Related Configuration Example

Account Info Management

4.4.1.3 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	Account	System Time	SMTP	Phone	Storage
System Time S	ettings				
Current Time		2017-11-14 10:18	:14 Tues		
Time Zone		8 China (Beijing)	•		
Sync Type		Sync with Browse	er 🔻		
Browser Time		2017-11-14 10:18	:30 Tues		
		Figure 4-4-1	-3		
General	Account	System Time	SMTP	Phone	Storage
System Time S	ettings				
Current Time		2017-11-14 10:18	54 Tues		
Time Zone		8 China (Beijing)	¥		
Sync Type		Set up Manually	¥		
Date		2017-11-14			
Time		10 🔻 19	▼ 10 ▼		
		Figure 4-4-1	-4		
General	Account	System Time	SMTP	Phone	Storage
System Time S	ettings				
Current Time		2017-11-14 10:19	:25 Tues		
Time Zone		8 China (Beijing)	•		
Sync Type		Sync with NTP S	erver 🔻		
NTP Server Add	ress	1.cn.pool.ntp.org			
Enable NTP Ser	ver				

Figure 4-4-1-5

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 4-4-1-3 System Time Parameters

Related Configuration Example

System Time Management

4.4.1.4 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	Account	System Time	SMTP	Phone	Storage
SMTP Client S	Settings				
Enable					
Email Address					
Password					
SMTP Server A	ddress	smtp.exmail.qq.co	om		
Port		587			
Enable TLS					
Email Recipie	nts				
Email Address					
Save	Test				
		Figure 4-4-1-6			

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.
Email Recipients	
Email Address	Add recipients' email address.
Test	Check if the recipients can get the mail from sender.

Table 4-4-1-4 SMTP Setting

Related Topics

Events Setting Events Application Example

4.4.1.5 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	Account	System Time	SMTP	Phone	Storage
Phone Numbe	r List				
	Number		Des	cription	Operation
+86	13409876543		adm		
					(H
Phone Group	List				
	Group	ID	1		
	Descri	iption	sms		
	Lis			Selected	
	+861340987654	3			*
		Save	Cancel		

Figure 4-4-1-7

Phone				
Item	Description			
Phone Number List				
Number	Enter the telephone number. Digits, "+" and "-" are allowed.			
Description	The description of the telephone number.			
Phone Group				
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 4.4.1.5 Dhana Cattinga			

Table 4-4-1-5 Phone Settings

Related Topic

Connect on Demand

4.4.2 User Management

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

Status		Account User Mana	agement
LoRaWAN	•	Change Account Info	
		Username	admin
Network	►	Old Password	
		New Password	
System		Confirm New Password	
General Settings		Save	
User Management		Jure.	

Figure	4-4-2-1
--------	---------

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". Read-Only: users can only view the configuration of gateway in this level. Read-Write: users can view and set the configuration of gateway in this level.

Table 4-4-2-1 User Management

Related Configuration Example

Common User Management

4.4.3 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.

Related Configuration Example

SNMP Application Example

4.4.3.1 SNMP

The UG87-LW 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 Setting	js.			
	Enable		8		
Network	Port		161		
System	SNMP Version		SNMPv2		¥
System	Location Inform	nation			
General Settings	Contact Inform	ation			
User Management	Save				
SNMP					

Figure 4-4-3-1

SNMP Settings		
Item	Description	
Enable	Enable or disable SNMP function.	
Port	Set SNMP listened port. Range: 1-65535.	
FUIL	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 4-4-3-1 SNMP Parameters

4.4.3.2 MIB View

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

SNMP	MIB View	VACM	Trap	MIB	
View List					
v	iew Name	View	Filter	View OID	Operation
All		Included] [1	
system		Included		1.3.6.1.2.1.1	
					H

Figure 4-4-3-2

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 4-3-3-2 MIB View Parameters

4.4.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
NMP v1 & v2	User List					
Comm	unity	Permission	MIB Vi	ew	Network	Operation
private	Rea	ad-write 1	• All	•	0.0.0/0	
public	Rea	ad-only	• none	•	0.0.0/0	

Figure 4-3-3-3

Description
r List
Set the community name.
Select from "Read-Only" and "Read-Write".
Select an MIB view to set permissions from the MIB view list.
The IP address and bits of the external network accessing the MIB view.
The permission of the specified MIB node is read and write.
The permission of the specified MIB node is read only.
Set the name of SNMPv3 group.
Select from "NoAuth/NoPriv", "Auth/NoPriv", and "Auth/Priv".
Select an MIB view to set permission as "Read-only" from the MIB view list.
Select an MIB view to set permission as "Read-write" from the MIB view list.
Select an MIB view to set permission as "Inform" from the MIB view list.

Table 4-4-3-3 VACM Parameters

4.4.3.4 Trap

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

SNMP	MIB View	VACM	Trap	MIB
SNMP Trap				
Enable				
SNMP Version		SNMPv2		•
Server Addres	s			
Port				1
Name				

Figure 4-4-3-4

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 4-4-3-4 Trap Parameters

4.4.3.5 MIB

This section describes how to download MIB files. The last MIB file "URSA-gateway-MIB.txt" is for the UG87-LW.

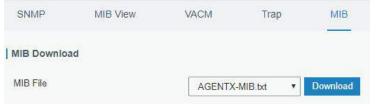


Figure 4-4-3-5

MIB	
ltem	Description
MIB File	Select the MIB file you need.
Download	Click "Download" button to download the MIB file to PC.

Table 4-4-3-5 MIB Download

4.4.4 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.

4.4.4.1 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	gs		
	Enable			
Network •	Server IP Addr	ess		
	Server Port		1812	
System 🔻	Key			
General Settings	Save			
User Management	Jave			
SNMP				
ААА				

Figure 4-3-4-1

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 4-4-4-1 RADIUS Parameters

4.4.4.2 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	js		
Enable			
Server IP Addres	s		
Server Port		49	
Key			0

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

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 4-3-4-2 TACACS+ Parameters

4.3.4.3 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+	LDAP A	uthentication
DAP Setting	js		
E <mark>nable</mark>			
Server IP Add	ress		
Server Port		389	
Base DN			
Security		None	۲
Jsername			
assword		[

Figure 4-3-4-3

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 4-3-4-3 LDAP Parameters

4.3.4.4 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 Tacacs+		LDAP		Authentication				
Authenticatio	on Settings							
Se	rvice	1			2		3	
Co	nsole	None	•	Nor	ne	٣	None	٣
V	Veb	None	•	Nor	10	•	None	v
Те	Inet	None	•	Nor	1e	*	None	•
S	SH	None	•	Nor	1e	w	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 4-3-4-4 Authentication Parameters

4.3.5 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	
	Device Management Server Address	
System	Activation Method	By Authentication Code
General Settings	Authentication Code	
User Management	Connect	<u></u>
AAA		
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 pacculard		
Password	Fill in the registered DeviceHub account (email) and password.		

Table 4-3-5-1

4.3.6 Events

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

4.3.6.1 Events

You can view alarm messages on this page.

Status	Events	Events Settings		
.oRaWAN	Mark as Read	Delete Mark A	Il as Read Delete	All Alarms
Network	Stat	us Type	Time	Message
System 🔻	< > 10 •	Go to: GO		
General Settings				
User Management				
AAA				
Device Management				
Events				

Figure 4-3-6-1

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 4-3-6-1 Events Parameters

4.3.6.2 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	Events Settings				
Events Settings					
Enable					
Phone Group Lis	t		,		
	Events		Record	Email Email Setting	SMS SMS Setting
C	Cellular Up				
Ce	ellular Down				
	WAN Up				
V	VAN Down				
	VPN Up				
N	PN Down				

Figure 4-3-6-2

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.	
Record	The relevant content of event alarm will be recorded on "Event"	
	page if this option is checked.	
Fmail	The relevant content of event alarm will be sent out via email if this	
Linan	option is checked.	

Email Setting	Click and you will be redirected to the page "SMTP" to configure the sender's & recipients' info.
SMS The relevant content of event alarm will be sent out via SMS option is checked.	
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.
Phone Group List Select phone group to receive SMS alarm.	

Table 4-3-6-2 Events Parameters

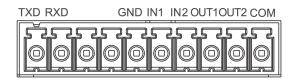
Related Topics

Email Setting Events Application Example

4.5 Industrial Interface

The UG87-LW 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).



PIN	RS232	DI	DO	Description
1	TXD			Transmit Data
2	RXD			Receive Data
3				Data +
4				Data-
5	GND	GND		Ground
6		IN1		Digital Input1
7		IN2		Digital Input2
8			OUT1	Digital Output1
9			OUT2	Digital Output2
10			COM	Common Ground

Figure 4-5-1 Pinouts

Table 4-5-1 Pinouts Definition

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 .

4.5.1 I/O

4.5.1.1 DI

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

CURSAL	_INK		
			For your device security, please change the default password
Status			
LoRaWAN		DI_1 Setting	
Network		Enable Mode	High Level
System		Duration(ms) Action	100 SMS Email DO1 DO2 Cellular UP
Industrial	-	DI_2 Setting	
I/O		Enable	
Serial Port		Mode	High Level 🔻
		Duration(ms)	100
Modbus Master		Action	SMS Email DO1 DO2 Cellular UP

Figure 4-5-1-1

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.
DO1	Control output status of DO1.
DO2	Control output status of DO2.
Cellular UP	Trigger the gateway to switch from offline mode to cellular network mode.

Table 4-5-1-1 DI Parameters

Related Topics

DO Setting Email Setting Connect on Demand

4.5.1.2 DO

This section describes how to configure digital output mode.

DI	DO			
DO_1 Set	tting			
Enable				
Mode		High Level		•
Duration(*	10ms)	100		
Alarm Sou	urce	DI1	🔲 DI2	
DO_2 Set	tting			
Enable		Ø		
Mode		High Level		•
Duration(*	'10ms)	100		
Alarm Sou	urce	DI1	DI2	

Figure 4-5-1-2

DO	
Item	Description
Enable	Enable or disable DO.
Mode	Select from "High Level", "Low Level", and "Pulse".
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 between "DI1" and "DI2".

Table 4-5-1-2 DO Settings

4.5.2 Serial Port

Serial 1 is used for RS232.

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.

Status		Serial 1		
LoRaWAN	Þ.	Serial Settings		
		Enable		
Network	×	Serial Type	RS232	
	12	Baud Rate	9600	*
System	×	Data Bits	8	•
Industrial	-	Stop Bits	1	Ŧ
		Parity	None	*
VO		Software Flow Control		
Serial Port		Serial Mode	DTU Mode	¥

Figure 4-5-2-1

Serial Settings						
ltem	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 is "DTU Mode". The serial port can establish communication with the remote server/client.	DTU Mode				

Table 4-5-2-1 Serial Parameters

Serial Mode	DTU Mode	•		
DTU Protocol	Transparent	•		
Protocol	ТСР	T		
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 Ad	ddress	Server Port	Status	(

Figure 4-5-2-2

DTU Mode					
ltem	Description	Default			
DTU Protocol	 Select from "None", "Transparent", "Modbus", and "TCP server". Transparent: the routed is used as TCP client/UDP and transmits data transparently. TCP server: the gateway is used as TCP server and transmits data transparently. Modbus: the gateway will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP. 				
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.				
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.				
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.				
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 4-5-2-2 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	Modbus						
Local Port	Set the gateway listening port. Range: 1-65535.	502					

the serial frame interval.

Table 4-5-2-3 DTU Parameters

Related Configuration Example

DTU Application Example

4.5.3 Modbus Master

UG87-LW can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

4.5.3.1 Modbus Master

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

Status	Modbus Master	Channel	
LoRaWAN	Modbus Master Setting	1	
	Enable	0	
Network	Read Interval	0	s
	Max. Retries	3	
System 🕨	Max. Response Time	500	ms
Industrial	Execution Interval	50	ms
mousman	Channel Name	1	Read
VO			
Serial Port	Save & Apply		
Modbus Master			

Figure 4-5-3-1

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 4-5-3-1

4.5.3.2 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.

Modbus Master		Channe	1						
Channel Setting									
Channel Setting									
Name	Slave ID	Addres s	Number	Туре	Туре	IP Address	Port	Sign	Operation
test1	1	40	1	Holding Regis	тср	▼ 192.168.23.3	500		×
									æ

Figure 4-5-3-2

Channel Set	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.				

Table 4-5-3-2

Modbus Master	Channel			
Alarm Setting				
		Name	test1	¥
		Condition	GE(>)	•
		Max. Threshold	0	
		Alarm	SMS	
		Phone Group		•
		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	1	

Figure 4-5-3-3

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

Table 4-5-3-3

4.6 Maintenance

This section describes system maintenance tools and management.

4.6.1 Tools

Troubleshooting tools includes ping and traceroute.

4.6.1.1 Ping

Ping tool is engineered to ping outer network.

Status		Ping	Traceroute	
LoRaWAN		IP Ping		
Network	Þ	Host	Ping Stop	
System	×			
Industrial	×			
Maintenance	-			
Tools				

Figure 4-6-1-1

PING	
Item	Description
Host	Ping outer network from the gateway.

Table 4-6-1-1 IP Ping Parameters

4.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Status		Ping	Traceroute		
LoRaWAN	F	Traceroute	<u>.</u>		
Network	F	Host		Trace	Stop
System	×				
Industrial	۲				
Maintenance	-				
Tools					

Figure 4-6-1-2

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

Table 4-6-1-2 Traceroute Parameters

4.6.2 Schedule

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

Status		Schedule				
LoRaWAN	•	Schedule				
Network	•	Schedule	Frequency	Hour	Minute	Operation n
						H
System	•	Save				
Industrial	•					
Maintenance	-					
Tools						
Schedule						

Figure 4-6-2-1

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 4-5-2-1 Schedule Parameters

Related Configuration Example

Schedule Application Example

4.6.3 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.

Related Configuration Example

Logs and Diagnostics

4.5.3.1 System Log

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

Status		System Log	Log Settings					Help —
Sidius								System Log
LoRaWAN	M	Download						System Log includes massive information about network and
Network	۲	File Log		Log File	D	awnload		devices, including operating status, configuration changes and so on
System	۲	View recent(lines)		20	9	•		Download Download log file.
Industrial	۲	packet to application Tue Sep 4 09 16:59	n-server error" error= 2018 daemon.err for	"rpc error: code = Im raserver[16451]: time	temal desc = g =="2018-09-04	1T09:16:59+08:00" level- get device error: object d 1T09:16:59+08:00" level-	oes not exist" error msg="processing	View the specified lines
Maintenance	-	Tue Sep 4 09:17:02 Tue Sep 4 09:17:02	2018 daemon.wam . 2018 daemon.wam .	zebra[6050]. (15360 zebra[6050]. (ibgsm/	23822.121124 gsm.c:423 yea	/IBCoBTAIgBUzMyKg2U] GSM Event: sim failed astar_mobile_handle_ev 018-09-04T09: 17:04+08	ent: fail_count 2!	Clear Log Clear the current system
Tools		received udp packet	t from gateway" addr	="127.0.0.1:49158"	protocol_versik	on=2 type=PullData		10-9.
Schedule		sending udp packet Tue Sep 4 09:17:11	to gateway" addr="1 2018 daemon err lor	27.0.0.1.49158" prot a-gateway-bridge[21	tocol_version= (323); time="2	018-09-04T09:17:04+08 2 type=PullACK 018-09-04T09:17:11+08 on=2 type=PushData	7.7	
Log		Tue Sep 4 09:17:11	2018 daemon err lor	a-gateway-bridge[21	[323] time="2	018-09-04T09-17-11+08 BUzOemv0pksU=" mac=		
Upgrade		publishing packet" q	os=0 topic=gateway	(24e124ffe0b7443/n	x	018-09-04T09:17:11+08	10-2019-01000-7000	
Backup and Res	tore	packet received"				109:17:11+08:00" level= 018-09-04T09:17:11+08	entre conservation	
Reboot		Clear Log						
APP	Þ							

System Log				
Item	Description			
Download	Download log file.			
View recent (lines)	View the specified lines of system log.			
Clear Log	Clear the current system log.			

Table 4-6-3-1 System Log Parameters

4.6.3.2 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				
Port		514]
Local Log File				
Storage		local	•	
Size		1024]кв
Log Severity		Info	7	

Figure 4-6-3-2

Log Settings				
Item	Description			
Remote Log Server				
Enable	With "Remote Log Server" enabled, gateway will send all			
Enable	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 4-6-3-2 System Log Parameters

4.6.4 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	Upgrade
LoRaWAN	Upgrade Firmware Version 87.1.0.2
Network	Reset Configuration to Factory Default
System I	Upgrade Firmware Upgrade
Industrial I	
Maintenance	
Tools	
Schedule	
Log	
Upgrade	

Figure 4-6-4-1

Upgrade	
Item	Description
Firmware Version	Show the current firmware version.
Reset Configuration to	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 i i i i wale	"Upgrade" to upgrade firmware.

Table 4-5-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

4.6.5 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
		Backup Running-config	
System	×	Backup	
Industrial	×	Restore Factory Defaults	
Maintenance	-	Reset	
Tools			
Schedule			
Log			
Upgrade			
Backup and Re	store		

Figure 4-6-5-1

Backup and R	estore
ltem	Description
Config File	Click "Browse" button to select configuration file, and then click "Import" 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 after reset process is done.

Table 4-5-5-1 Backup and Restore Parameters

Related Configuration Example

Backup and Restore Configuration Restore Factory Defaults

4.6.6 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.

Status	
LoRaWAN	F
Network	×
System	×
Industrial	×
Maintenance	•
Tools	
Schedule	
Log	
Upgrade Backup and Re	estore
Reboot	

Figure 4-5-6-1

4.7 APP

4.7.1 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.

4.7.1.1 Python

Status		Python	AppManager Cor	nfiguration	Python	APP		
LoRaWAN		Python						
Network		AppManager Statu SDK Version	S	Uninstalled				
System		SDK Path Available Storage		eMMC	T			
Industrial		SDK Upload				Browse	Install	
Maintenance								
APP	•							
Python								

Figure 4-7-1-1

Description
Show AppManager's running status, like "Uninstalled",
"Running" or "Stopped".
Show the version of the installed SDK.
Show the SDK installation path.
Select available storage such as Micro SD or SSD to install SDK.
Upload and install SDK for Python.
Uninstall SDK.
View application status managed by AppManager.

Table 4-7-1-1 Python Parameters

4.7.1.2 App Manager Configuration

Python	AppManager Config	uration P	Python APP	
AppManager				
Enable				
App Managem	ent			
	ID	App Command	Logfile Size(MB)	Uninstall
App Status				
	App Name	A	pp Version	SDK Version
		Figu	ure 4-7-1-2	

AppManager Configuration	on
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	Show the name of the imported App.
Logfile 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 4 7 1 2 ADD Managar Darameters

Table 4-7-1-2 APP Manager Parameters

4.7.1.3 Python App

Python	AppManager Configuration	Python APP
Import App P	ackage	
App Package		Browse Import
Import App C	onfiguration	
App Name		*
App Configurat	ion	Browse Import
Debug Script		
Debug File		Export
Debug Script		Browse Import



escription lect App package and import.
lect App to import configuration.
lect configuration file and import.
port script file.
lect Python script to be debugged and import.

Table 4-7-1-3 APP Parameters

Chapter 5 Application Examples

5.1 Application configuration

You can create a new application on this page, mainly used for defining the method to decode the data sent from end-device.

The configuration procedures are listed as below.

- 1. Go to "LoRaWAN" > "Network Server" > "Application".
- 2. Click to enter the configuration page, as the following picture shows:

	Applications	Profiles	Device	Packets	
pplications					
lame		Ursalink-app			
Description		a application for ursalink	test		
ayload Codec		Custom	•		
ayload decod	ler function				
	odes an array of byt ains the LoRaWAN f				
// - bytes is ar	n array of bytes, e.g.		5		
 // - bytes is ar // The function function Deco 	n array of bytes, e.g.	[225, 230, 255, 0] ct, e.g. {"temperature": 22	2.5}		
// - bytes is ar // The function	n array of bytes, e.g. n must return an obje		2.5}		
 // - bytes is ar // The function function Decoreturn {}; 	n array of bytes, e.g. n must return an obje		2.5}		
// - bytes is ar // The function function Deco- return {}: }	n array of bytes, e.g. n must return an obje de(fPort, bytes) {		2.5}		
// - bytes is ar // The function function Deco- return {}; } Payload encod	n array of bytes, e.g. must return an obje de(fPort, bytes) { der function	ct, e.g. ("temperature": 22	2.5}		
// - bytes is ar // The function function Deco- return {}; } Payload encod	n array of bytes, e.g. must return an obje de(fPort, bytes) { der function	ct, e.g. ("temperature": 22	2.5}		
// - bytes is ar // The function function Deco- return {; } Payload encod // Encode encod // - fPort conta // - obj is an o	n array of bytes, e.g. n must return an obje de(fPort, bytes) { der function odes the given objec ains the LoRaWAN f object, e.g. { tempera	ct, e.g. ("temperature": 22 st into an array of bytes. Port number iture": 22.5)			
// - bytes is ar // The function function Deco- return {; } Payload encod // Encode enc // - fPort conta // - obj is an o // The function function Enco-	n array of bytes, e.g. n must return an obje de(fPort, bytes) { der function odes the given objec ains the LoRaWAN f object, e.g. { tempera	ct, e.g. ("temperature": 22 st into an array of bytes. Port number			
// - bytes is ar // The function function Deco- return {; } Payload encod // Encode enc // - fPort contt // - obj is an o // The function	n array of bytes, e.g. n must return an obje de(fPort, bytes) { der function codes the given objec ains the LoRaWAN f bbject, e.g. {"tempera n must return an arra	ct, e.g. ("temperature": 22 st into an array of bytes. Port number iture": 22.5)			

Save	11	Cancel
		- AP-0411 - Y-9-14-

Application Config	lication 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	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.		

5.2 Device Profiles Configuration

√ame	Device-test	
Max TXPower	0	
Join Type	OTAA	Ŧ
Class Type	Class A	•
Advanced		
MAC Version	1.0.2	٠
Regional Parameters Revision	В	

Device Profiles Set	Device Profiles Setting		
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 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 by-passing the join request - join	ΟΤΑΑ	

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

Check Advanced

to show the advanced settings.

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	F	
ACK TIMEOUL	transmissions. Only class C.	5	

5.3 Device Configuration

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

You can edit the device configuration by clicking to r create a new device by clicking, as shown:

Device		
General		
Device Name	asd	
Description	s	
Device EUI	3530353083376118	
Device-Profile	ninii	
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

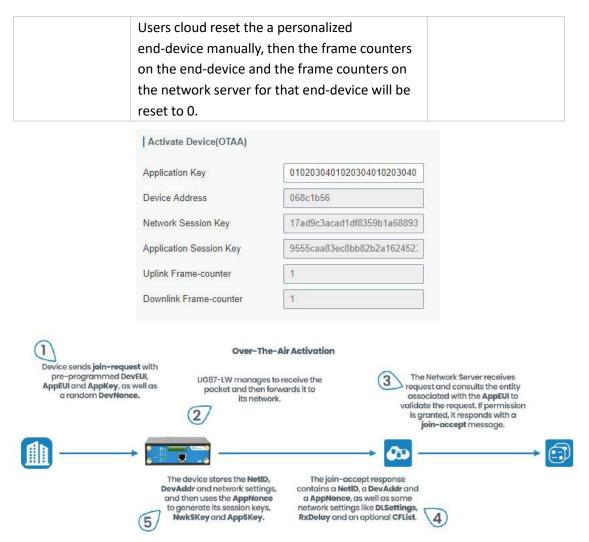
Activate Device(ABP)	
Device Address	068c1b56
Network Session Key	17ad9c3acad1df8359b1a68893
Application Session Key	9555caa83ec8bb82b2a162452;
Uplink Frame-counter	1
Downlink Frame-counter	1

Activation By Personalis	ation	
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.	
	→ 😰	(]

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			
ltem	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. 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.	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.	Null	



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 network via over-the-air activation, the application key is used for derive the Application Session key.	Null
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	Null

	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.	
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

5.4 Account Info Management

It is strongly recommended that you change the default username and password of the administrator account when you log in Ursalink gateway's WEB GUI page at first time for the sake of security.

Example: change the username and password of administrator account to "uradmin" and "URpassword".

The configuration procedures are listed as below.

- 1. Go to "System > User Management> Account".
- 2. Modify the username to "uradmin", fill in the old Password "password", and set the new Password "URpassword".

Click "Save" button, and then you will be asked to login again with the new username and password.

UG87-LW User Guide

Status		Account User Mana	igement
LoRaWAN		Change Account Info	
		Username	admin
Network	T.€	Old Password	
		New Password	
System	~	Confirm New Password	
General Settings		Save	
User Management			

Related Topic

Account Management

5.5 Common User Management

The UG87-LW is capable of creating up to 5 common user accounts that have different authorities, including "Read-Only" and "Read-Write" to manage the gateway.

"Read-Only" refers to the authority that user is only allowed to view the configuration;

"Read-Write" refers to the authority that user can view and modify all the parameters.

Example: create 2 common user accounts listed below.

Username	Password	Permission
ur_user1	UR_password1	Read-Only
ur_user2	UR_password2	Read-Write

Configuration procedures are listed as blow.

- 1. Go to "System > User Management > User Management".
- 2. Click " \pm " to add a new common user.
- 3. Set "Username", "Password", and "Permission" as below.

Status		Account User Manag	pement		
LoRaWAN	•	User List			
		Username	Password	Permission	Operation
Network	•	tesi1		Read-Only	• 🛛
System	•	test2		Read-Write	•
General Setting	53				
User Manageme	ent	Save			

Click "Save" button, and then click "Apply" on the top-right corner to make the changes take effect.

Related Topic

User Management

5.6 System Time Management

There are 3 ways to synchronize the system time: "Sync with Browser", "Set up Manually", and "Sync with NTP Server".

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

In the following part we take UTC+8 time zone as an example.

A. Synchronize time with browser

Go to "System > General Settings > System Time", set time zone as "8 China (Beijing)" and Sync Type as "Sync with Browser". And Click "Save" button.

System Time Settings	
Current Time	2017-11-09 09:17:40 Thur
Time Zone	8 China (Beijing)
Sync Type	Sync with Browser
Browser Time	2017-11-09 09:18:29 Thur
Save (2)	

B. Set up time by manual

- Go to "System > General Settings > System Time", set time zone as "8 China (Beijing)" and Sync Type as "Set up Manually".
- 2. Select the correct local time. And click "Save" button.

System Time Settings	
Current Time	2017-11-09 09:18:16 Thur
Time Zone	8 China (Beijing)
Sync Type	Set up Manually
Date	2017-11-09
Time	9 v 19 v 4 v
Save 3	

C. Synchronize time with NTP server

 Go to "System > General Settings > System Time", set time zone as "8 China (Beijing)" and Sync Type as "Sync with NTP Server". 2. Configure an available NTP server address such as "time.windows.com". Click "Save" button.

System Time Settings	
Current Time	2017-11-09 09:19:27 Thur
Time Zone	8 China (Beijing)
Sync Type	(1) Sync with NTP Server
NTP Server Address	time.windows.com
Enable NTP Server	
Save 3	

Related Topic

System Time Setting

5.7 Backup and Restore Configuration

A. Backup Configuration

- 1. Go to "Maintenance > Backup and Restore > Backup and Restore".
- 2. Click "Backup" button under "Backup running-config".

Then the current configuration file will be downloaded to the "Downloads" folder of the PC.

Status		Backup and Restore
LoRaWAN	•	Restore Config
Network	٠	Config File Browse Import Backup Running-config
System	•	Backup (3)
Industrial		Restore Factory Defaults
Maintenance	-	Reset
Tools		
Schedule		
Log		
Upgrade		
Backup and Restore	1	

B. Restore Configuration

- 1. Go to "Maintenance > Backup and Restore > Backup and Restore".
- 2. Click "Browse" button under the "Restore" to select configuration file from PC.
- 3. Click "Import" to import the selected configuration file to the gateway.

Status	Backup and Restore
LoRaWAN	Restore Config 3 4
Network	Config File Browse Import
System	Backup
Industrial	Restore Factory Defaults
Maintenance	- Reset
Tools	
Schedule	
Log	
Upgrade	
Backup and Restore	\mathbb{D}

Related Topic

Backup and Restore

5.8 Restore Factory Defaults

5.8.1 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	Backup and Restore
Lorawan 🕨	Restore Config
Network	Config File Import
System 🕨	Backup Running-config
Industrial 🕨	Backup Restore Factory Defaults
Maintenance	Reset
Tools	
Schedule	
Log	
Upgrade	
Backup and Restore	
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
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

5.8.2 Via Hardware



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

STATUS 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 → Blinking	The gateway is now reset to factory defaults.

5.9 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.

Status	Upgrade
LoRaWAN 🕨	Upgrade
Network	Firmware Version 87.1.0.2
System	Reset Configuration to Factory Default Upgrade Firmware Upgrade Default Upgrade Vpgrade
Industrial 🕨	
Maintenance	
Tools	
Schedule	
Log	
Upgrade Upgrade Firmware Version Reset Configuration Upgrade Firmware	2.0.0.19 n to Factory Default C:\fakepath\2.0.0.19.bin Browse Upgrade 2 Importing firmware. Please stay on this page till upgrade is finished.
	Please keep the power on during upgrade.

Related Topic

<u>Upgrade</u>

5.10 Events Application Example

Example

In this section, we will take an example of sending alarm messages by email when the following events occur and recording the event alarms on the Web GUI.

Events	Actions to make events occur (for test)
Cellular network is connected.	Insert SIM card.
Cellular network is disconnected.	Remove SIM card.
WAN cable is connected.	Plug WAN cable.
WAN cable is disconnected.	Unplug WAN cable.

Configuration Steps

- 1. Go to "System > Events > Events Settings" and enable Event settings.
- Check corresponding events for record and email alarm, and then click "Save" button as below. Click "Email Settings" and go to SMTP settings.

Status	Events	Events Settings)		
LoRaWAN	► Events Settings				
Network	Enable Phone Group List	× 3			
System	Email Group List		•		
General Settings		Events	Record	Email Email Setting (6)	SMS SMS Setting
User Management	c	ellular Up			
SNMP	Cel	lular Down		2	
AAA	· · · · · · · · · · · · · · · · · · ·	VAN Up	4	2	
Device Management	W	AN Down		2	
Events	1	/PN Up			
	v	PN Down	0	•	
Industrial	> Save	5			

Configure the corresponding parameters including email sending settings and recipients as below. Click "Save" and "Apply" button to make the changes take effect.

Status	General	System Time	SMTP 8 P	hone Email	
LoRaWAN	SMTP Client Sett	lings			
Network	Enable		9		
System	Email Address Password		upport@ursalick.com		
General Settings	SMTP Server Addr		mtp.ursalink.com		
User Management	Port Enable TLS	17	78		
SNMP	Save	Test			
AAA		1931			
Device Management					
Status	General System Time	SMTP Phone	Email (1)		
LoRaWAN					
Network	Email List 🕖 Email Addre	55	Des	cription	Operation
System	adm@ursalink.com		example		×
General Settings	Email Group List				
User Management	Group ID	Description	1	Email Address	Operation
SNMP					8
Device Management	Save				
Events					

 To test the functionality of Alarm, please take the corresponding actions listed above. It will send an alarm e-mail to you when the relevant event occurs. Refresh the web GUI, go to "Events > Events", and you will find the events records.

Events Sett	ngs			
Mark as Read Delete	Mark All a	as Read Delete All Al	arms	
Status	Туре	Time	Message	
< > 10 ▼ Go to:	GO			

Related Topics

<u>Events</u>

Email Setting

5.11 Schedule Application Example

Through schedule configuration, the UG87-LW can be set to reboot at preset time every day.

Example

Configure gateway to reboot at 0:00 every day.

Configuration Steps

- 1. Go to "Maintenance > Schedule > Schedule".
- 2. Click "
 "
 to set up a new schedule task as below.
- 3. Click "Save" and "Apply" button.

URS		IK								🉎 adr	nin 🔁
Status		Sche	dule								
LoRaWAN	×	Sched	lule								
Network			Schedule		Frequenc	/	Hour		Minute		Operation
INCINCIN		reb	oot	•	Every Day	• 0		• 0		٠	×
System	•										0
Industrial	۲		Save								
Maintenance	•										
Tools											
Schedule											

Related Topic

Schedule Setting

5.12Logs and Diagnostics

System log of the UG87-LW supports 2 types of output method, including Web, Remote Log Server and Console.

Application 1

Obtain system log on Web.

Go to "Maintenance > Log > System log", and you will see the log is listed in the box.

Status	System Log Settings
LoRaWAN	Download
Network	File. Log File Download
System	Log
Industrial	View recent(lines) 20 • Tue Sep 4 10:34:04/2018 daemon em loraserver[12437]: time="2018-09-04T10:34:04+08:00" level=info msg="gateway updated"
Maintenance	mac=24e124fffe0b6543 Tue Sep 4 10:34:06 2018 daemon debug lora_gateway_ubus[11507]: lora_gateway_ubus.c:1459 append_uplink_data: insert a uplink packet.count: 60
Tools	Tue Sep 4 10:34 06 2018 daemon err lora-gateway-bridge[12404]; time="2018-09-04710:34-06+08:00" level=info mag="gateway: received udp packet from gateway" addre"127 0.0.1:54454* protocol_version=2 type=PushData Tue Sep 4 10:34 06 2018 daemon.err lora-gateway-bridge[12404]; time="2018-09-04710:34-06+08:00" level=info mag="gateway: rxpk
Schedule	packet received" addr="127.0.0.1:54454" data="AAgHBgUEAwiBCoBTAigBUzN5CUZcCqk=" mac=24e124fffe0b5543 Tue Sep 4 10.34.06 2018 daemon.err lora-gateway-bridge[12404]: time="2018-09-04T10:34:06+08:00" level=info msg="backend:
Log	publishing packet" qos=0 topic=gateway/24e1(24ffe0b6543/rx Tue Sep 4 10:34:06 2018 daemon err loraserver(12437) time="2018-09-04T10:34:06+08:00" level=info msg="backend/gateway: rx packet received"
Upgrade	Tue Sep 4 10:34:06 2018 daemon em tora-gateway-bridge[12404]; time="2018-09-04710:34:06E408:00" level=into msg="gateway: sending udp packet to gateway" addr="127.0.0.1:54454" protocol_version=2 type=PushACK Tue Sep 4 10:34:07 2018 daemon em toraserver[12437]; time="2016-09-047110:34:07+08:00" level=info msg="packet(s) collected"
Backup and Restore	dev_eui=335301280253800a gw_count=1 gw_macs=24e124fffe0b6543 mtype=JoinRequest Tue Sep 4 10.34.07 2018 daemon.em loraserver[12437]; time="2018-09-04T10.34.07+08.00" level=error msg="finished client unary
Reboot	Leall' amen' ma amen anda = Internal daes = ant device amen object daes ant aviat' ame code=Internal Clear Log

Application 2

Send the system log to the remote syslog server. Server IP: 110.22.14.43; Port: 514

Go to "Maintenance > Log > Log Settings" to configure the parameters as below.

Status	System Log	Log Settings		
LoRaWAN	Remote Log	Server		
Network	> Enable		2	
	Syslog Server	Address	110.22.14.43	
System	Port		514	
Industrial	Local Log Fil	e		
	Storage		local	•
Maintenance	Size		1	
	Size		5120	КВ
Tools	Log Severity		Debug	•
Schedule	Save			
Log				

Then click "Save" and "Apply" button.

Related Topic

System Log

5.13 SNMP Application Example

Before you configure SNMP parameters, please download the relevant "MIB" file from the UG87-LW's WEB GUI first, and then upload it to any software or tool which supports standard SNMP protocol. Here we take "ManageEngine MibBrowser Free Tool" as an example to access the gateway to query cellular information.

 Go to "System > SNMP > MIB" and download the MIB file "URSA-gateway-MIB.txt" to PC.

Status		SNMP	MIB View	VACM	Trap	MIB
LoRaWAN	•	MIB Download				
Network	•	MIB File		AGENTX-M	∕/IB.txt ▼	Download
System	-					
General Settings						
User Management						
SNMP						
AAA						

 Start "ManageEngine MibBrowser Free Tool" on the PC. Click "File > Load MIB" on the menu bar. Then select "BURSA-gateway-MIB.txt" file from PC and upload it to the software.

ManageEngine MibBrowser Free Tool - 🗆 🗙											Х
<u>F</u> ile Edit <u>V</u> iew <u>O</u> perations <u>H</u> elp											
日 🕺 🖻 🎂 🍝	🎒 🖻 🖷 1	n 🗊 🂈	<u>و</u> ھ	🏹 🖄 🛅	I 🍯	🛫 🚥	٩	X	More I	wnload Free Tools	
& Loaded MibModules ⊞…& URSA-ROUTER-MIB	Host	localhost		V	Port		161				~
	Community	******			Write	Community					
	Set Value			~	·						
	Device Type-										
	Device Type Ide	ntified Not	Available					C	🕇 Reload		
	Suggested OID:	s No	ine					\sim			
	Object ID										
	Loading MIBs "E:URSA MIBURSA-ROUTER-MIB.txt"								^		
	MIB(s) Loaded S	MIB(s) Loaded Successfully									

Click the "+" button beside "URSA-gateway-MIB", which is under the "Loaded MibModules"

menu, and find "usCellularinfo". And then you will see the OID of cellular info is

".1.3.6.1.4.1.50234", which will be filled in the MIB View settings.

🕌 ManageEngine MibBrowser Free Tool	📓 ManageEngine MibBrowser Free Tool - 🗆 🗙										
<u>File Edit View Operations H</u> elp											
🗞 🍰 🗉 🤲 🖬 🎒 🗞	🗄 🐃 🖈 🔊 🧠 🏹 🕸 🛅 🕷 🛫 🔤 🧇 🔯 🚺 Download										
Loaded MibModules URSA-ROUTER-MIB enterprises ussaveConfig usRebotDevice usRebotDevice usRebotDevice usCellularInfo usCellularSmsSer usCellularModems usCellularModems usCellularNetwork usCellularNetwork usCellularNetwork usCellularNetwork usCellularNetwork usCellularNetwork usCellularNetwork usCellularNetwork usCellularSignalL usCellularNetwork usCellularNetwork usCellularNetwork usCellularSignalL usCellularNetwork usCellularServer	Host localhost Port 161 Community ****** Write Community Set Value Image: Community Set Value Device Type Device Type Identified Not Available Image: Community Device Type Image: Community Image: Community Image: Community Object ID .iso.org. dod internet. private. enterprises. ursa. usManage. usCellularInfo Loading MIBs "E:URSA MIB/URSA-ROUTER-MIB.bd" MIB(s) Loaded Successfully Description MultiVar Symtax Status Access Reference Index .1.3.6.1.4.1.50234.1.6										
Global View 🗌	Description										

 Go to "System > SNMP > SNMP" on the gateway's WEB GUI. Check "Enable" option, then click "Save" button.

	K		Apply
Status	SNMP MIB View	VACM Trap MIB	
LoRaWAN 🕨	SNMP Settings		
	Enable		
Network 🕨	Port	161	
	SNMP Version	SNMPv2 T	
System 🔻	Location Information	Xiamen_China	
General Settings	Contact Information	Xiamen_Urslaink_Co,Ltd	
User Management	Save		
SNMP			

4. Go to "System > SNMP > MIB View". Click + to add a new MIB view and define the view to be accessed from the outside network. Then click "Save" button.

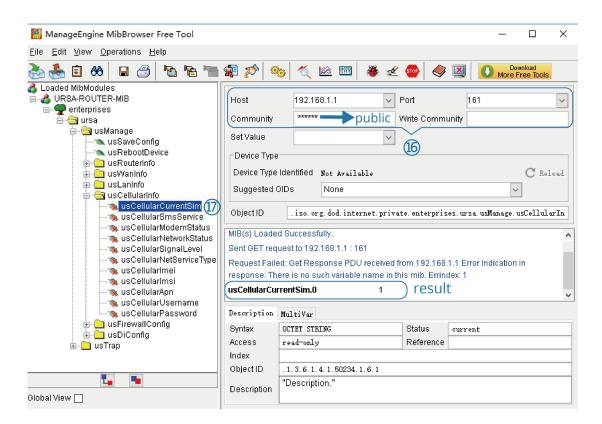
Status	SNMP	MIB View	VACM	Trap	MIB	
LoRaWAN 🕨	View List					
Network	v	iew Name	View	Filter	View OID	Operation
System 🔻	Cellular		Included	8	▼ 1.3.6.1. <u>4</u> .1.50234.1.6	
oyacın						
General Settings		-				
User Management	Save					
SNMP						

5. Go to "System > SNMP > VACM". Click \pm to add a new VACM setting to define the

access authority for the specified view from the specified outside network. Click "Save" and "Apply" to make the changes take effect.

Status		SNMP	MIB View	VACM	Trap MIB		
LoRaWAN		SNMP v1 & v	2 User List				
Network	×	Comn	nunity	Permission	MIB View	Network	Operation
System	÷	public	Re	ead-Only 🔻	Cellular	0.0.0/0	
General Settings			28				
User Management		Save					
SNMP							

6. Go to MibBrowser, enter host IP address, port and community. Right click "usCellular CurrentSim" and then click "GET". Then you will get the current SIM info on the result box. You can get other cellular info in the same way.



Related Topic

<u>SNMP</u>

5.14 Cellular Connection

The UG87-LWs 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 UG87-LW 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.

Status	Port WAN	N LAN VLAN	Trunk Cellular	Loopback	
LoRaWAN	Cellular Setting	SIM1	2 Cellula	r	
Network	Enable	<i>.</i>	✓		
Interface	Network Type	Auto	▼ Auto	T	
Firewall	APN	4G First			
1 Interfac		3G First 3G Only 2G First	3 "Auto" or others		
DDNS	Password Access Number	2G Only			
Link Failover	PIN Code				
	Authentication Type	Auto	 Auto 	•	
VPN	Roaming				
System	SMS Center				
Industrial	Connection Setting Dual SIM Strategy				
				Apply	🛓 admin 🛛 🔁
Status	Port WAN LAN		Cellular Loopback	5 Apply	Enable
LoRaWAN 🕨	Password Access Number				Check the option to enable the corresponding SIM card.
Network 🔻	PIN Code Authentication Type	Auto 🔻	Auto	·	Network Type Select from "Auto", "4G First", "4G Only", "3G
Interface	Roaming				First", "3G Only", "2G Frist", and "2G Only".
Firewall	SMS Center				Auto: connect to the network with the strongest signal
DHCP	Connection Setting				automatically. 4G First: 4G network has priority
DDNS	Dual SIM Strategy Enable NAT				to be connected. 4G Only: connect to 4G network only. And so on.
Link Failover					APN
VPN	ICMP Server Secondary ICMP Server	8.8.8.8			Enter the Access Point Name for cellular dial-up connection provided by
System	PING Times	5			local ISP.
Industrial	Packet Loss Rate	20	%		Enter the username for cellular dial-up connection provided by
Maintenance	SMS Settings	2201			local ISP. Password
	Save (4) Save	PDU T			Enter the password for cellular dial-up connection provided by local ISP.
					Access Number 🗸

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',

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
Modem							
Status		Ready					
Model		U9300C					
Current SIM		SIM1					
Signal Level		29asu (-56dBm)				
Register Status		Registered (Ho	me network)				
IMSI		460070615219	248				
ICCID		898602E61315	32019248				
ISP		CHINA MOBILE	E				
Network Type		LTE					
PLMN ID		46007					
LAC		fffe					
Cell ID		f700e28					
IMEI		862808032459	987				
Network							
Status		Connected <	Connec	ted			
IP Address		10.39.128.14	<u> </u>				
Netmask		255 255 255 25	2				
Gateway		10.39.128.13					
DNS		211.143.147.12	0				
Connection Duration		0 days, 00:15:3	5				

SIM1 has dialed up successfully.

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 UG87-LW.

Related Topic

Cellular Setting Cellular Status

5.15 Dual SIM Backup Application Example

Example

In this section we will take an example of inserting two SIM cards into the UG87-LW. 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 Trunk	Ce	ellular (2)	Loopback	
LoRaWAN	Cellular Settir	g						
Network	Enable		sim1 ③			SIM2 ✔		
Interface (1)	Network Type		Aut	0	•	Auto	•	•
Firewall	APN]
	Username							
DHCP	Password							
DDNS	Access Numbe	r						
Link Failover	PIN Code							
VPN	Authentication	Гуре	Aut	0	•	Auto	•	•
	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	
Network	Primary SIM Card SIM1 SIM1	
Interface	Switch to backup SIM card when ICMP detection fails	
Firewall	Swtich to backup SIM card when the connection fails	
DHCP	Switch to backup SIM card when roaming is detected	
DDNS	Enable NAT	
Link Failover		
VPN	ICMP Server 8.8.8.8	
	Secondary ICMP Server 114.114.114	
System	PING Times 5	
	Packet Loss Rate 20 %	
Industrial	SMS Settings	
Maintenance	SMS Mode PDU •	
APP	Save 🕜	

Then click "Save" and "Apply" button.

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

Overview	Cellular	Network	VPN	Routing
Modem				
Status		Ready		
Model		EC25		
Current SIM		SIM1		
Signal Level		15asu (-83dBm)	
Register Status		Registered (Ho	me network)	
IMSI		460019987103	071	
ICCID		898601178380	19196629	
ISP		CHN-UNICOM		
Network Type		LTE		
Networ	k			
Status			Connected	
IP Addr	ess		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 (-83dBr	n)	
Register Status		Registered (He	ome network)	
IMSI		460019987103	3071	
ICCID		898601178380	019196629	
Network				
Status			Connected)
IP Addres	ŝS		10.63.223.44	ł

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

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

Related Topic

<u>Cellular Setting</u> <u>Cellular Status</u>

5.17 NAT Application Example

Example

An UG87-LW 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.

URSAL	_INK								5 Apply
Status			ACL DMZ	Port M	apping 2 MAC	Binding			
LoRaWAN	Þ	1)	Port Mapping						
Network	•		Source IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
Interface		3<	0.0.0/0	8000	192.168.1.2	8000	TCP •	Server	
Firewall	1								
DHCP			Save (4)					
DDNS									

Click "Save" and "Apply" button.

Related Topic

Port Mapping

5.18 Access Control Application Example

Application Example

GE port of the UG87-LW is set as LAN with IP 192.168.1.0/24. Then configure the gateway to deny accessing to Google IP 198.98.108.64 from local device with IP 192.168.1.12.

Configuration Steps

 Go to "Network > Firewall > ACL" to configure access control list. Click "
 the button to set parameters as below. Then click "Save" button.

Status	ACL 2 DMZ	Port Mapping MAC Bi	inding		
LoRaWAN	ACL Setting				
	Default Filter Policy	Accept •			
Network 🔻	Access Control List				
Interface		Туре	extended •		
Firewall (1)		ID	100		
		Action	deny		
DHCP		Protocol	ip v		
DDNS	3<	Source IP	192.168.1.12		
Link Failover		Source Wildcard Mask	0.0.0.0		
VPN		Destination IP	198.98.108.64		
VPN		Destination Wildcard Mask	0.0.0.0		
System 🕨		Description	google		
Industrial 🕨 🕨		4 Save	Cancel		

2. Configure interface list. Then click "Save" and "Apply" button.

	.INK								(7	Apply
Status			ACL	DMZ	Port Ma	apping N	IAC Binding			
LoRaWAN	۲		ACL Setting Default Filter P	olicy	Accep	t	¥			
Network	•	14	Access Contr	ol List						
Interface			ID	Action	Protocol	Source IP	Destination IP	More Detail	Description	Operation
Firewall			100	deny	ip	192.168.1.12/0.0.0. 0	198.98.108.64/0.0. 0.0		google	×
DHCP										Ð
DDNS		þ	nterface List							
Link Failover				Interface		In	ACL	Out	ACL	Operation
VPN		5	GE 0		•	100	¥		Ŧ	
System	►									
Industrial	•		Save	6						

Related Topic

<u>ACL</u>

5.18 DTU Application Example

Example

PLC is connected with the UG87-LW via RS232. Then enable DTU function of the UG87-LW 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		Serial 1			
LoRaWAN		Serial Settings			
		Enable			
Network		Serial Type	RS232	*	
		Baud Rate	9600	•	
System		Data Bits	8	•	
Industrial	-	Stop Bits	1	•	
		Parity	None	•	
٧O		Software Flow Cont	trol		
Serial Port		Serial Mode	DTU Mode	▼	

2. Configure Serial Mode as "DTU Mode". The UG87-LW is connected as client in "Transparent" protocol.

System		DTU Protocol	Transparent	•
Industrial	-	Protocol	ТСР	•
		Keepalive Interval	75	s
l 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	
NPF	- A			

3. Configure TCP server IP and port.

Destination IP Address

Server Address	Server Port	Status	Operation
		172	×
			H
Save			

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

	Apply	admin	Ð	
Destination IP Address				
Server Address	Server Po	ort	Status	Operation
110.87.98.58	7087		Connected	×
				+

5. Start TCP server on PC.

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

TC	^o Server	
(2)	Local hos	tIP
192	.168.2	. 27
(3) 7087	Local hos	t por
7087		

6. Connect the UG87-LW to PC via RS232 for PLC simulation. Then start "sscom" software

on the PC to test communication through serial port.

ComNum	Сомэ	•		Close	Com
BaudRa	9600	•	🗆 D.	TR	Г
DataBi	8	-	∏ Se	nd eve	100
StopBi	1	-	∏ Se	ndHEX	Γ
Verifyl	None	-	Data	input:	
FlowCon	None	-	hellI	.0	
			u=		

7. After connection is established between the UG87-LW and the TCP server, you can send data between sscom and netassit.

PC side

SSCOM3.2	-		×
testtesttesttesttesttesttesttest			< >
OpenFile FileNm SendFile SaveDate	L Clea	ur	HexData
ComNum COM13 💌 🛞 CloseComHelp			EXT
BaudRa 9600 V DTR RTS DataBi 8 V Send eve 1000 ms/Time StopBi 1 V SendHEX SendNew VerifyNone V Data input: SEND FlowConNone V hello			
ww.mcu51.cor S:42 R:48 COM13 opened 9600bps	CTS=	1 DSR=	0 RL

TCP server side

	NetAssist (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		
• 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	
<u>Load</u> <u>Clear</u>		Send
🍯 Ready!	Send : 208 Recv : 177 F	Reset

8. After serial communication test is done, you can connect PLC to RS232 port of the UG87-LW for test.

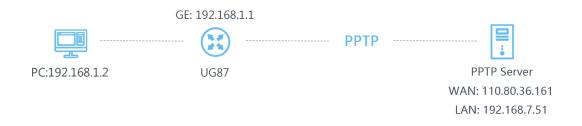
Related Topic

Serial Port

5.19 PPTP Application Example

Example

Configure the UG87-LW as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.



Configuration Steps

1. Go to "Network > VPN > PPTP", configure PPTP server IP address, username and password provided by PPTP server.

Note: If you want to have all data transferred through VPN tunnel, check "Global Traffic Forwarding" option.

Vetwork 🗸	PPTP Settings	
	— PPTP_1	
Interface	Enable	
Firewall	25 St 60 St 76 St	
PUOD	Remote IP Address	110.87.98.58
DHCP	Username	pptpclient
DDNS	Password	
Link Failover	Authentication	Auto
VPN	Global Traffic Forwarding	
	Remote Subnet	
rstem 🕨	Remote Subnet Mask	
	Advanced Settings	
dustrial 🕨 🕨		
	+ PPTP_2	
aintenance	+ PPTP_3	

If you want to access peer subnet such as 192.168.3.0/24, you need to configure the subnet and mask to add the route.

Remote Subnet	192.168.3.0	
Remote Subnet Mask	255.255.255.0	

2. Check "Show Advanced" option, and you will see the advanced settings.

DMVPN IPsec	GRE L2TP	PETE	OpenVPN Client	OpenVPN Server	Certifications
Show Advanced	×				
Local IP Address					
Peer IP Address	[
Enable NAT	×				
Enable MPPE					
Address/Control Compression					
Protocol Field Compression					
Asyncmap Value	mmm				
MRU	1500				
MTU	1500				
Link Detection Interval (s)	60				
Max Retries	0				
Expert Options					

If the PPTP server requires MPPE encryption, then you need to check "Enable MPPE" option.

Enable MPPE



If the PPTP server assigns fixed tunnel IP to the client, then you can fill in the local tunnel IP and remote tunnel IP, shown as below.

Local IP Address	205.205.0.100		
Peer IP Address	205.205.0.1		

Otherwise PPTP server will assign tunnel IP randomly.

Click "Save" button when you complete all settings, and then the advanced settings will be hidden again. Then click "Apply" button to have the configurations take effect.

3. Go to "Status > VPN" and check PPTP connection status.

PPTP is established as shown below.

Local IP: the client tunnel IP.

Remote IP: the server tunnel IP.

Overview	Cellular	Network	VPN	Routing	Host List
PPTP Tunnel					
	Name	Status	Local IP	i	Remote IP
	pptp_1	Connected 120.205.0.100		100	205.205.0.1/32
	pptp_2	Disconnected			
pptp_3		Disconnected			

Related Topics
PPTP Setting
PPTP Status