

UG87 Industrial LoRaWAN Gateway User Guide

Xiamen Ursalink Technology Co., Ltd.

×

SHROSH



www.ursalink.com

Preface

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

Related Documents

Document	Description
Ursalink UG87 Datasheet	Datasheet for the Ursalink UG87 industrial LoRaWAN gateway.
Ursalink UG87 Quick Start Guide	Quick Installation Guide for the Ursalink UG87 industrial LoRaWAN gateway.

Declaration of Conformity

UG87 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
July 13, 2019	V1.1	Initial version
Aug. 6, 2019	V1.2	Add New Function:
		1. Python Development
		2. Send data to LoRaWAN nodes

Contents

Chapter 1 Product Introduction	. 7
1.1 Overview	. 7
1.2 Advantages	.7
1.3 Specifications	. 8
1.4 Dimensions (mm) 1	10
Chapter 2 Access to Web GUI	1
2.1 PC Configuration for Web GUI Access to gateway	
2.2 Access to Web GUI of gateway	L 2
Chapter 3 Web Configuration	14
3.1 Status	14
3.1.1 Overview	14
3.1.2 LoRa	14
3.1.3 Cellular	L7
3.1.4 Network 1	۱9
3.1.5 WLAN (Only Applicable to Wi-Fi Version)	20
3.1.6 VPN	21
3.1.7 Host List	22
3.2 LoRaWAN	23
3.2.1 Packet Forwarder	23
3.2.1.1 General	23
3.2.1.2 Radios	24
3.2.1.3 Advanced	26
3.2.1.4 Custom	27
3.2.1.5 Traffic	27
3.2.2 Network Server	28
3.2.2.1 General	28
3.2.2.2 Application	30
3.2.2.3 Profiles	31
3.2.2.4 Device	32
3.2.2.5 Packets	32
3.3 Network	35
3.3.1 Interface	35
3.3.1.1 Port	35
3.3.1.2 WAN	36
3.3.1.3 LAN	39
3.3.1.4 VLAN Trunk4	10
3.3.1.5 WLAN (Only Applicable to Wi-Fi Version)	11
3.3.1.6 Cellular4	12
3.3.1.7 Loopback	16
3.3.2 Firewall4	17
3.3.2.1 Security	17

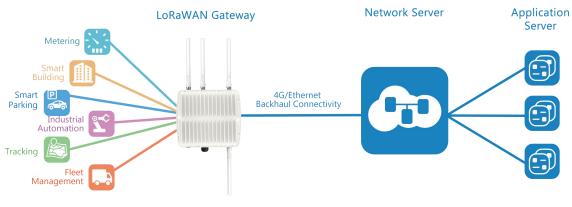
3.3.2.2 ACL	. 47
3.3.2.3 DMZ	49
3.3.2.4 Port Mapping	49
3.3.2.5 MAC Binding	. 50
3.3.3 QoS	. 51
3.3.4 DHCP	. 52
3.3.4.1 DHCP Server	52
3.3.4.2 DHCP Relay	. 53
3.3.5 DDNS	. 54
3.3.6 Link Failover	54
3.3.6.1 SLA	54
3.3.6.2 Track	55
3.3.6.3 VRRP	56
3.3.6.4 WAN Failover	. 58
3.3.7 VPN	59
3.3.7.1 DMVPN	. 59
3.3.7.2 IPSec	60
3.3.7.3 GRE	63
3.3.7.4 L2TP	64
3.3.7.5 PPTP	. 66
3.3.7.6 OpenVPN Client	68
3.3.7.7 OpenVPN Server	69
3.3.7.8 Certifications	. 71
3.4 System	. 73
3.4.1 General Settings	. 73
3.4.1.1 General	. 73
3.4.1.2 System Time	. 74
3.4.1.3 SMTP	. 76
3.4.1.4 Phone	76
3.4.1.5 Email	. 77
3.4.2 User Management	78
3.4.2.1 Account	. 78
3.4.2.2 User Management	79
3.4.3 SNMP	80
3.4.3.1 SNMP	. 80
3.4.3.2 MIB View	. 81
3.4.3.3 VACM	. 81
3.4.3.4 Trap	. 82
3.4.3.5 MIB	83
3.4.4 AAA	. 83
3.4.4.1 RADIUS	83
3.4.4.2 TACACS+	84
3.4.4.2 TACACS+ 3.4.4.3 LDAP	_

3.4.5 Device Management	86
3.4.6 Events	87
3.4.6.1 Events	87
3.4.6.2 Events Settings	88
3.5 Maintenance	
3.5.1 Tools	89
3.5.1.1 Ping	89
3.5.1.2 Traceroute	89
3.5.2 Schedule	90
3.5.3 Log	
3.5.3.1 System Log	91
3.5.3.2 Log Settings	91
3.5.4 Upgrade	92
3.5.5 Backup and Restore	93
3.5.6 Reboot	94
3.6 APP	
3.6.1 Python	95
3.6.1.1 Python	96
3.6.1.2 App Manager Configuration	
3.6.1.3 Python App	
Chapter 4 Application Examples	
4.1 Application Configuration	
4.2 Device Profiles Configuration	102
4.3 Device Configuration	
4.4 Send Data to Device	107
4.5 Restore Factory Defaults	
4.5.1 Via Web Interface	
4.5.2 Via Hardware	
4.6 Firmware Upgrade	
4.7 Cellular Connection	114
4.8 Dual SIM Backup Application Example	116
4.9 Wi-Fi Application Example	
4.9.1 AP Mode	119
4.9.2 Client Mode	

Chapter 1 Product Introduction

1.1 Overview

Ursalink UG87 is an industrial LoRaWAN gateway with embedded intelligent software features designed for multifarious M2M/IoT applications. Options like cellular network or Wi-Fi provide drop-in connectivity for operators and make a giant leap in maximizing uptime. Adopting high-performance industrial platform of 64-bit CPU and wireless module, the UG87 enables you to scale up M2M application combining data within limited time and budget. The UG87 is particularly ideal for smart city, smart agriculture, building automation, digital factory, environment protection, water conservancy and so on.





1.2 Advantages

Benefits

- Built-in industrial CPU and big memory;
- Ethernet, 2.4GHz/5GHz Wi-Fi and global 2G/3G/LTE options make it easy to get connected
- Embedded network server and compliant with several third party network servers
- MQTT, HTTP or HTTPS protocol for data transmission to application server
- Embedded GPS module for high-precision time synchronization
- Rugged enclosure, optimized for wall or pole 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
- Embedded hardware watchdog to automatically recover from various failure and ensure highest level of availability

 Establish a secured mechanism on centralized authentication and features authorization of device access by supporting AAA (TACACS+, RADIUS, LDAP, local authentication) and multiple levels of user authority

Easy Maintenance

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

Hardware System	
CPU	800MHz, 64-bit ARM Cortex-A53
Memory	8 GB Flash, 512 MB DDR3 RAM
Storage	1 × M.2 slot supports SATA M.2 SSD
LoRaWAN	
Connectors	$1 \times 50 \Omega$ N-Type (Center pin: Female)
Channel	8 or 16
Frequency Band	Supports EU 863-870, US 902-928, EU 433, AU 915-928, CN
	470-510 IN865 and KR 920-923 Band
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class C and V1.0.2 Class A/Class C

1.3 Specifications

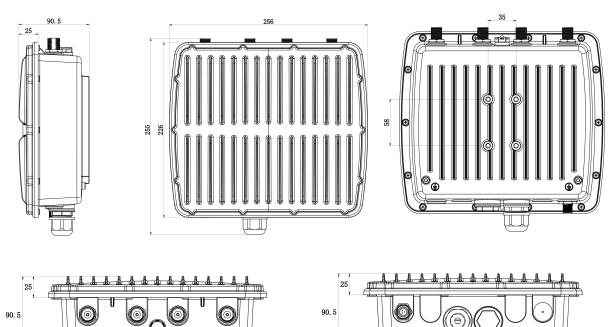
Ethernet	
Ports	1 × RJ-45 (PoE PD Default)
Physical Layer	10/100/1000 Base-T (IEEE 802.3)
Data Rate	10/100/1000 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)
Cellular Interfaces (Optiona	I)
Connectors	$1 \times 50 \Omega$ N-Type (Center pin: Female)
SIM Slots	2
Wi-Fi Interfaces (Optional)	
Connectors	$1 \times 50 \Omega$ N-Type (Center PIN: Female)
Standards	IEEE 802.11 b/g/n/ac
Tx Power	802.11b: 16 dBm +/-1.5 dBm (11 Mbps)
	802.11g: 15 dBm +/-1.5 dBm (54 Mbps)
	802.11n@2.4 GHz: 14 dBm +/-1.5 dBm (MCS7) 802.11n@5
	GHz: 11 dBm +/-2 dBm (MCS7) 802.11ac@5 GHz: 10 dBm
	+/-2 dBm (MCS9)
GPS	
Connectors	$1 \times 50 \Omega$ N-Type (Center PIN: Female)
Software	
Network Protocols	PPP, PPPOE, SNMP v1/v2c/v3, TCP, UDP, DHCP,DDNS, VRRP,
	HTTP, HTTPS, DNS, SNTP, Telnet, VLAN, SSH, MQTT, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding
Management	Web, CLI, SMS, On-demand dial up
Reliability	VRRP, Dual SIM Backup
Power Supply and Consump	otion
Connector	Default: 1 × 802.3af/at PoE input
	Optional: 9-48VDC/220VAC Circular Connector
Consumption	Max 8.2W
Physical Characteristics	
Ingress Protection	IP67
Dimensions	256 x 226 x 90.5 mm

Mounting	Wall or Pole Mounting
Others	
Reset Button	1 × RST
LED Indicators	$1 \times PWR$, $1 \times SYS$, $1 \times L1$, $1 \times L2$
Built-in	Watchdog, RTC, Timer
Certifications	RoHS, CE, FCC
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

1.4 Dimensions (mm)

T

 \bigcirc



╧┛┓┓┓┓┓┓┓┓┓┓┓╸╸

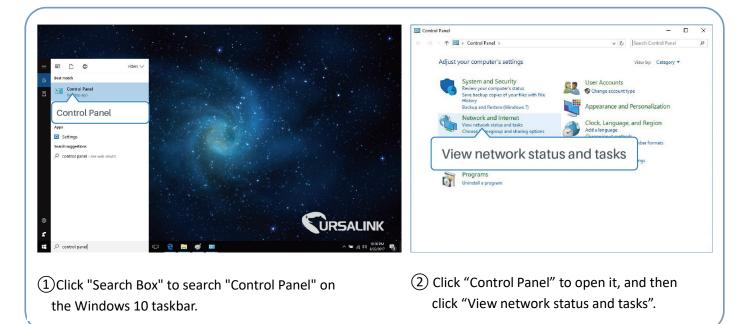
Chapter 2 Access to Web GUI

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

2.1 PC Configuration for Web GUI Access to gateway

Please connect PC to GE port of UG87 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 Sharing Center		- 🗆 X	Ethernet Status	×
← → × ↑ 🛣 « Network	and Internet > Network and Sharing Center	v Ö Search Control Panel P	General	
Control Panel Home	View your basic network informat	ion and set up connections		
	View your active networks		Connection	
Change adapter settings		Access type: Internet	IPv4 Connectivity:	No network access
Change advanced sharing settings	Yeastar5G Private network	HomeGroup: Ready to create	IPv6 Connectivity:	No network access
scange	Private network	Connections: Mi-Fi (Yeastar5G)	Media State:	Enabled
			Duration:	00:01:21
	Identifying	Access type: No network access	Speed:	1.0 Gbos
	identifying	Connections: Q Ethernet	speed:	1.0 6005
			Details	
	Change your networking settings			
	Set up a new connection or netwo			
	Set up a broadband, dial-up, or VF	N connection;	Activity	
	Troubleshoot problems			
	Diagnose and repair network prob	lems, or get troubleshooting information.	t —	Received
			Properties	alt
			210	0
See also				
HomeGroup			Properties Disable	Diagnose
Infrared			- Toperaes	
Internet Options				-
Windows Firewall				Close
\frown				
(3) Click "Fth	ernet" (May have	e different name).	(4) Click "Prope	rtioc"
	iernee (ividy have	anner en	(4) CIICK Prope	rues.

UG87 User Guide

Ethernet	Properties			
Vetworking	Sharing			
Connect us	sing:			
🚽 Intel	(R) 82567LM	Gigabit Network	Connection	
			Config	gure
This conne	ection uses th	e following items:		
	lient for Micro	soft Networks	10.00 M	^
🗹 🟆 Fi	le and Printer	r Sharing for Micro	soft Networks	- 1
🗹 🐙 Q	oS Packet S	cheduler		
	ternet Protoc	11/	1177 12	
and the second second	des supervises en en entre terres	dispersion of the second s	and the second second	
and the second second	des supervises en en entre terres	Adapter Multip	and the second second	
□ <u>∎</u> M	et Prot	dispersion of the second s	olexor Protocol	
Intern	icrosoft Nety et Prot all	ocol Versi	olexor Protocol on 4 (TCP	
Intern	et Prot all on ssion Control a network pr	ocol Versi	olexor Protocol on 4 (TCP Prope Protocol. The de	rties fault
Intern	et Prot all on ssion Control a network pr	Adapter Multip OCOI Versio Uninstall Protocol/Internet totocol that provide	olexor Protocol on 4 (TCP Prope Protocol. The de	rties fault

 (5) Double Click "Internet Protocol Version 4 (TCP/IPv4)" to configure IP address and DNS server.

nternet l	Protocol Version 4 (TCP/IPv4) Propertie	es.		×
General	Alternate Configuration				
this cap	n get IP settings assigned auto bability. Otherwise, you need t appropriate IP settings.				
0	btain an IP address automatica	ally			
OU	se the following IP address:				
IP ac	ddress:		1		
Subr	iet mask:			- Se	
Defa	ult gateway:		14	14	
() ()	btain DNS server address auto	matically			
OU	se the following DNS server ad	dresses:			
Pref	erred DNS server:		100		
Alter	nate DNS server:				
V	alidate settings upon exit			Advance	ed
			OK	(Cancel

6 Method 1: click "Obtain an IP address automatically";

ernet Pi	rotocol Version 4 (TCP/	IPv4) Properties
eneral		
his capa	get IP settings assigned ability. Otherwise, you ne appropriate IP settings.	192.168.1.20 [™] 255.255.255.0
Ob	tain an IP address autor	192.168.1.1
() Use	the following IP address	
IP add	dress:	192.168.1.20
Subne	et mask:	255 . 255 . 255 . 0
Defau	lt gateway:	192.168.1.1
Ob	tain DNS server address a	automatically
() Use	the following DNS serve	r addresses:
Prefer	rred DNS server:	192.168.1.1
Altern	ate DNS server:	
□Va	lidate settings upon exit	192.168.1.1
		OK Cancel

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

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

2.2 Access to Web GUI of gateway

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

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

- 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".

() () () () () () () () () () () () () (×
	URSALINK
2	Jsername
a	Password
	Login

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

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

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

Change Pa	1554010
Old Password	
New Password	
Confirm New Password	
Save	Cancel

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

URSAL	INK											
				For your devi	For your device security, please change the default password							
Status		Overview	LoRa	Cellular	Network	VPN	Host List					
LoRaWAN	•	System Informa	tion									
		Model		UG87								
Network	•	Partnumber		L00E-G-P-E	EU868							
System		Serial Number		6216924973	387							
System		Firmware Version		80.0.0.18	80.0.0.18							
Maintenance	•	Hardware Version		V2.0	V2.0							
		Local Time		2019-07-18	14:36:34							
APP	•	Uptime		00:20:35								
		CPU Load		17%								
		RAM (Capacity/Av	vailable)	512MB/249	MB(48.63%)							
		Flash (Capacity/A	vailable)	64MB/0MB(0%)							
		eMMC (Capacity/	Available)	3.0G/2.6G(8	37.37%)		Man	ual Refresh 🔻	Refresh			

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

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

URSALI	NK										
				For your devi	ce security, please cl	nange the default	password				
Status		Overview	LoRa	Cellular	Network	VPN	Host List				
LoRaWAN	۲	System Information	n								
		Model		UG87							
Network		Partnumber		L00E-G-P-E	L00E-G-P-EU868						
Queters		Serial Number		6216924973	387						
System		Firmware Version		80.0.0.18	80.0.0.18						
Maintenance		Hardware Version		V2.0	V2.0						
		Local Time		2019-07-18	14:36:34						
APP	•	Uptime		00:20:35							
		CPU Load		17%							
		RAM (Capacity/Availa	able)	512MB/2491	MB(48.63%)						
		Flash (Capacity/Avail	able)	64MB/0MB(0%)						
		eMMC (Capacity/Ava	ilable)	3.0G/2.6G(8	37.37%)						

Figure 3-1-1-1

System Information							
Item	Description						
Model	Show the model name of gateway.						
Serial Number	Show the serial number of gateway.						
Firmware Version	Show the currently firmware version of gateway.						
Hardware Version	Show the currently hardware version of gateway.						
Local Time	Show the currently local time of system.						
Uptime	Show the information on how long the gateway has been running.						
CPU Load	Show the current CPU utilization of the gateway.						
RAM (Capacity/Available)	Show the RAM capacity and the available RAM memory.						
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 3-1-1-1 System Information

3.1.2 LoRa

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

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

Figure 3-1-2-1

LoRaWAN Status (Packet F	LoRaWAN Status (Packet Forwarder Mode)								
Item	Description								
Mode	Show the working mode of LoRaWAN.								
Version	Show the version of packet forwarder software.								
Status	Show the status of packet forwarder.								
Status	Value include Running, Disabled.								
Gateway ID	Show the ID of the gateway.								
Region Code	Show the LoRa region code which is based on the gateway's								
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 3-1-2-1 LoRaWAN Status (Packet Forwarder Mode)

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

Figure 3-1-2-2

LoRaWAN Status (Network Server)							
Item	Description						
Mode	Show the working mode of LoRaWAN.						
Version	Show the version of installed lora network server file.						
Statuc	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 3-1-2-2 LoRa WAN-Status-Network Server



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

Click

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

ateway	Details										
Gateway	EUI				24E124FF	FE0B7443					
IP Addres	s				localhost						
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

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

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

3.1.3 Cellular

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

Overview	Cellular	Network	VPN	Routing	Host List			
Modem								
Status		Ready	Ready					
Model		EC25						
Current SIM		SIM1						
Signal Level		15asu (-83dBr	n)					
Register Status		Registered (He	Registered (Home network)					
IMSI		460019987103	460019987103071					
		898601 <mark>1</mark> 78380	89860117838019196629					
ISP		CHN-UNICOM	CHN-UNICOM					
Network Type		LTE	LTE					
PLMN ID		46001	46001					
LAC		5922	5922					
Cell ID		812c63d	812c63d					
IMEI		861107031710	861107031710008					

Figure 3-1-3-1

Modem Information	1
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 3-1-3-1 Modem Information

Network

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

Figure 3-1-3-2

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

Table 3-1-3-2 Network Status

3.1.4 Network

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

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

Figure 3-1-4-1

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

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

Table 3-1-4-1 LAN Status

3.1.5 WLAN (Only Applicable to Wi-Fi Version)

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

Overview	LoRa	Cellular	Network	WLAN	VPN	Host List
WLAN Status						
Wireless Status		Enabled				
MAC Address		24:e1:24:f0: <mark>27:85</mark>				
Interface Type		AP				
SSID		Ursalink_F02786				
Channel		Auto				
Encryption Type		No Encryption				
Status		Up				
IP Address		192. <mark>168</mark> .100.1				
Netmask		255.255.255.0				
Connection Duration	1	0 days, 00:08:50				

Figure 3-1-5-1

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

Table 3-1-5-1 WLAN Status

Associated Stations		
IP Address	MAC Address	Connection Duration

Figure 3-1-5-2

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

Table 3-1-5-2 WLAN Status

3.1.6 VPN

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

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

Figure 3-1-6-1

Overview	Cellular	Network	VPN	Routing	Host List
IPsec Tunnel					
	Name	Status		Local IP	Remote IP
	ipsec_1	Disconnected		150	
	ipsec_2	Disconnected			-
	ipsec_3	Disconnected		(a)	1
OpenVPN Clie	ent				
	Name	Status		Local IP	Remote IP
	openvpn_1	Disconnected			: 5)
	openvpn_2	Disconnected			-
	openvpn_3	Disconnected			12

Figure 3-1-6-2

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

Figure 3-1-6-3

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

3.1.7 Host List

You can view the host information on this page.

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

Figure 3-1-7-1

Host List				
Item Description				
DHCP Leases				
IP Address	Show IP address of DHCP client			
MAC Address	dress 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 3-1-7-1 Host List Description

3.2 LoRaWAN

3.2.1 Packet Forwarder

3.2.1.1 General

Status	General	Radios	Advanced	Custom	Traffic	
LoRaWAN	General Setting	1				
	Enable		Please close	e the Network Serve	er mode first	
Packet Forwarder	Mode		Packet Forwa	rder		
Network Server	Gateway EUI		24E124FFFE	DB6543		
	Gateway ID		24E124FFFE	DB6543		
Network •	Server Address		localhost			
System	Server Up Port		1700			
	Server Down Por	t	1700			
Industrial 🕨						
Maintenance >						
APP						

Figure 3-2-1-1

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

Table 3-2-1-1 General Setting Parameters

3.2.1.2 Radios

General	Radios	Advanced	Custom	Traffic	
Radio Channel S	etting				
Supported Frequen	су			AS923 •	
		Name			Center Frequency/MHz
		Radio 0			923.6
		Radio 1			922.6



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

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

1	Multi	Channels	Setting

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

Figure 3-2-1-3

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

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

LoRa	Channel	Setting
------	---------	---------

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

Figure	3-2-1-4

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

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

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



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 3-2-1-5 FSK Channel Setting Parameters

3.2.1.3 Advanced

General	Radios	Advanced	Custom	Tra
Intervals Setting	g			
Keep Alive Interv	al	10	s	
Stat Interval		30	s	
Push Timeout		100	m	s
Forward CRC S	etting			
Forward CRC Dis	abled			
Forward CRC Erro	or			
Forward CRC Vali	d			
Network Setting	1			
Network Mode		Private LoRa	WAN •	
Save				

Figure 3-2-1-6

Advanced					
Item	Description	Default			
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to LoRaWAN network server to keep the connection stable and alive. Range: 1-3600.	10			
Stat Interval	30				
Push Timeout	Sh Timeout the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-3600.				
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	Public LoRaWAN			

(multi-tenant) into a single network.	
Private LoRaWAN: individually managed networks,	
Network deployed for single application purpose.	

Table 3-2-1-6 Advanced Parameters

3.2.1.4 Custom

Custom Config	guration		
Enable			
			Example
{			
"SX1301_conf			
"lorawan_publi		al. to concentrates */	
	adio_1 provides cio ": 0, /* antenna gair	ck to concentrator */	
"radio 0": {	. v, / antenna gan		
"enable": true.			
"type": "SX125	7"		
"freq": 922500			
"rssi offset": -1			
"tx_enable": tru	Je,		
"tx_freq_min":	917000000,		
"tx_freq_max":	923500000		
},			
"radio 1": {			
"enable": true.			



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

3.2.1.5 Traffic

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

Traff	fic Setting								
	Refresh	Clear							
	Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
	1	up	÷	83002508	922.8	SF9BW125	4/5	-103	-13.2
	1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
	1	up	-	35426956	922.8	SF9BW125	4/5	-103	-9.8
	1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5
	1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0
	1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2
	1	up	0	3147851660	922.6	SF9BW125	4/5	-102	-13.8
	1	up	-	3143888916	922.8	SF9BW125	4/5	-102	-13.2
	1	up	-	3139922740	922.8	SF9BW125	4/5	-100	-12.2
	1	up	-	3124065788	922.8	SF9BW125	4/5	-100	-12.8

Figure 3-2-1-8

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

Table 3-2-1-7 Traffic Parameters

3.2.2 Network Server

3.2.2.1 General

Status	General	Applications	Profiles	Device
LoRaWAN 👻	General Settin	g		
	Enable			
Packet Forwarder	Mode	Network	Server	*
Network Server	NetID	010203		
- 112	Join Delay	5		sec
Network 🕨	RX1 Delay	1		sec
System 🕨	Lease Time	744-0-0		hh-mm-ss
	Log Level	info		•
Maintenance				
	Channel Plan	Setting		
APP 🕨	Channel Plan	EU868		*
	Channel Mask			

Figure	3-2-2-1
--------	---------

Item	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Disabled
NetID	Enter the network identifier.	01023
	Enter the interval time between the end-device	
	sends a Join_request_message to network	
	server and the end-device prepares to open	
Join Delay	RX1 to receive the Join_accept_message sent	5
	from network server.	
	Enter the interval time between the end-device	
	sends uplink packets and the end-device	
RX1 Delay	prepares to open RX1 to receive the downlink	1
	packet.	
	Enter the amount of time until a successful join	
	expires. The format is hours-minutes-seconds. If	
Lease Time	the join-type is OTAA, then the end-devices need	"744-00-00"
	to join the network server again when it exceeds	
	the lease time.	
Log level	Choose the log level.	Info
Channel Plan Sett	ing	
	Choose LoRaWAN channel plan used for the	
Channel Plan	upstream and downlink frequencies and	Depend on the
Channel Flan	datarates. Available channel plans depend on	gateway's variant.
	the gateway's variant.	
	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	Null.
	document.	Null means using
		the default standard
Channel Mask	A bit in the ChMask field set to 1 means that	usable channels
	the corresponding channel can be used for	which are specified
	uplink transmissions if this channel allows the	in the LoRaWAN
	data rate currently used by the end-device.	regional parameters
	A bit set to 0 means the server and the	document.
	A bit set to 0 means the corresponding	
	channels should be avoided.	
	US and AU 915 have a 80-bit channel mask for	
	72 usable channels and EU, AS, IN, KR have a	

Table 3-2-2-1 General Parameters

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

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

Figure 3-2-2-2

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

Table 3-2-2-2 Additional Plan Parameters

3.2.2.2 Application

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

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

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

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

Item	Description
ID	Show the ID of the application profile already created.
Name	Show the name of the application profile already created.
Description	Show the description of the application profile already

	created.		
Payload Codec	Show the payload codec of the application profile already created.		
Table 3-2-2-3 Application Parameters			
You can edit the application by clicking \fbox or create a new application by clicking \boxdot			
Data Transmission			
Туре	Operation		
	Œ		



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

Related Configuration Example

Application configuration

3.2.2.3 Profiles

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

Device Profiles

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

Figure	3-2-2-5

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

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

You can edit the device profile by clicking or create a new device profile by clicking



Related Configuration Example

Device Profiles Advanced configuraion

3.2.2.4 Device

Device							
	Device Name	Device EUI	Device-Profile	Application	Last Seen	Actived	Operatio n
	asd	353035308337611 8	ninii	AS923	53 minutes ago	~	<i>[</i>]×
							Ð



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

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

Related Configuration Example

Device configuration

3.2.2.5 Packets

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

Figure 3-2-2-7

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

Network Server					
Item	Description				
Device EUI	Show the EUI of the device.				
Frequency	Show the used frequency to transmit packets.				
Datarate	Show the used datarate to transmit packets.				
SNR	Show the signal-noise ratio.				
RSSI	Show the received signal strength indicator.				
Size	Show the size of payload.				
Fcnt	Show the frame counter.				
Туре	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 3-2-2-6 Packet Parameters



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

Pack	kets Details		×	
				l
	Dev Addr	068c1b56		l
	GwEUI	24e124fffe0b7443		100
	AppEUI	70b3d57ed0007ac1		1
	DevEUI	3530353083376118		
	Immediately	false		
	TimeSinceGPSEpoch	-		
	Timestamp	242616788		
	Туре	DnUnc		1
	Adr	true		I
	AdrAcKReq	false		Í
	Ack	true		
	Font	it.		l
	Fport			
			*	

Figure 3-2-2-8

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

	is receiving the uplink messages
	False: Otherwise
Ack	True: This frame is ACK.
ACK	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 3-2-2-7 Packets Details Parameters

Related Topic

Send Data to Device

3.3 Network

3.3.1 Interface

3.3.1.1 Port

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
Port Settir	ıg				
	Port	Status	Property	Speed	Duplex
	GE 0	up 🔻	wan 🔻	auto 🔻 a	uto 🔻

Figure 3-3-1-1

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

Table 3-3-1-1 Port Parameters

3.3.1.2 WAN

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

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

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

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

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



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

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

Table 3-3-1-2 WAN Parameters

1. Static IP Configuration

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

	INK				
			For your device security, please change the	e default password	
Status	Î	Port WAN LAN	VLAN Trunk Cellular	Loopback	
LoRaWAN	×	Enable	8		
Network	-	Port Connection Type	GE 0 Static IP		
Interface		IP Address	192.168.23.141		
Firewall		Netmask	255.255.255.0		
QoS		Gateway	192.168.23.1		
205		MTU	1500		
DHCP		Primary DNS Server	8.8.8.8		
DDNS		Secondary DNS Server	114.114.114.114		
Link Failover		Enable NAT	8		
VPN		Multiple IP Address			
		IP Ad	dress	Netmask	Operation
System	•				•

Figure 3-3-1-3

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

Table 3-3-1-3 Static Parameters

2. DHCP Client

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

	-			For your device sec	urity, please change ti	te default password
Status	Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
LoRaWAN 🕨	- WAN	L1				
Network 🔫	Enal	ble				
Interface	Port			GE 0		
Firewall	Coni	nection Type		DHCP Client	•	
QoS	Use	Peer DNS				
DHCP	Prim	ary DNS Server		8.8.8.8		
DDNS	Seco	ondary DNS Server		114.114.114.1	114	
Link Failover	Enal	ble NAT		2		
VPN	Save					



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

3. PPPoE

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

				For your device sec	urity, please change t	he default password.
Status	Port	WAN	LAN	VLAN Trunk	Cellular	Loopback
LoRaWAN	- WAN_	1				
Network 👻	Enable	9				
Interface	Port			GE 0		
Firewall	Userna	ection Type		PPPoE	•	
QoS	Passw	ord				
DHCP	Link D	etection Interval	(S)	60		
DDNS	Max R	etries		0		
	MTU			1500		
Link Failover	Use P	eer DNS				
VPN	Primar	y DNS Server		8.8.8.8		
System	Secon	dary DNS Serve	r	114.114.114.1	14	
	Enable	NAT		2		



PPPoE					
Item	Description				
Username	Enter the username provided by your Internet Service Provider (ISP).				
Password	Enter the password provided by your Internet Service Provider (ISP).				
Link Detection	Set the heartbeat interval for link detection. Range: 1-600.				
Interval (s)	Set the heartbeat interval for link detection. Range. 1-000.				
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.				
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.				

Table 3-3-1-5 PPOE Parameters

3.3.1.3 LAN

LAN setting is used for managing local area network devices connected to LAN port of the UG87, 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	LAN	VLAN Trunk	Cellular	Loopback		
LAN Settir	ngs					
	Port	IP Address		Netmask	MTU	Operation
GE	٣	192.168.23.47	255.2	255. <mark>255.0</mark>	1500	×
						B



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

Table 3-3-1-6

3.3.1.4 VLAN Trunk

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

Client \times to delete the current VLAN setting. Click \pm to add a new VLAN port.

Port	WAN	LAN	VLAN Trunk	Cellular	Loopback		
VLAN Sett	ings						
	Enable	Interfa	ice	VID	IP Address	Netmask	Operation
	0	GE 0	•			255.255.255.0	×
							æ



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

Table 3-3-1-7 VLAN Trunk Parameters

3.3.1.5 WLAN (Only Applicable to Wi-Fi Version)

This section explains how to set the related parameters for Wi-Fi network. UG87 supports

802.11 b,	/g/	'n/a	аc,	as	AP	or	client	mode.
-----------	-----	------	-----	----	----	----	--------	-------

Port	WAN	LAN	VLAN Trunk	WLAN	Cellular	Loopback
WLAN						
Enable						
Work Mode		AP		•		
SSID Broad	cast					
AP Isolation						
Radio Type		802	.11ac	•		
Channel		Auto	D	•		
SSID		test				
BSSID		24:e	1:24:f0:00:f3			
Encryption M	Mode	No	Encryption	•		
Bandwidth		80N	1Hz			
Max Client N	Number	100				
			Figure 3-2-1-8			
IP Setting						

Protocol	Static IP 🔹		
IP Address	192.168.232.1		
Netmask	255.255.255.0		

Figure 3-2-1-9

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

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

Table 3-3-1-8 WLAN Parameters

Related Topic

Wi-Fi Application Example

3.3.1.6 Cellular

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

fail over to SIM2.

Port WAN	LAN	VLAN Trunk	Cellular	Loopback
Cellular Setting				
	SIM1		SIM2	
Enable	X			
Network Type			•	
APN				
Username				
Password				
Access Number				
PIN Code				
Authentication Type	Aut	to	▼ Auto	
Roaming	۵			
SMS Center				
		Figure 3-3-1-1	10	
Co	onnection Setting	8		
Du	al SIM Strategy			
Er	able NAT			
Re	estart When Dial-up	failed		
IC	MP Server	8.8	.8.8	
Se	econdary ICMP Ser	ver 114	4.114.114.114	
PI	NG Times	5		
Pa	acket Loss Rate	20		%
SN	IS Settings			
SI	/IS Mode	P	00	T

Figure 3-3-1-11

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 First", and "2G Only". Auto: connect to the network with the strongest signal automatically.	Auto			

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

Table 3-3-1-9 Cellular Parameters

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

Figure 3-3-1-12

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

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

Table 3-3-1-10 Cellular Parameters

Related Topics

Cellular Connection Application Example Dual SIM Backup Application Example Phone Group

3.3.1.7 Loopback

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

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

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

Figure 3-3-1-13

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

Table 3-3-1-11 Loopback Parameters

3.3.2 Firewall

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

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

3.3.2.1 Security

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



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

Table 3-2-2-1 Security Parameters

3.3.2.2 ACL

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

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

UG87 User Guide

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

Figure 3-3-2-2

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

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

Table 3-3-2-2 ACL Parameters

3.3.2.3 DMZ

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

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

Figure 3-3-2-3

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

Table 3-3-2-3 DMZ Parameters

3.3.2.4 Port Mapping

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

Click \blacksquare to add a new port mapping rules.

ACL	DMZ	Port I	Mapping	MAC Bindin	9		
Port Mapp	oing						
Sou	Irce IP	Source Port	Destination IP	Destinati on Port	Protocol	Description	Operation
0.0.0.0/0			-		TCP 🔻		×
							0



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

Table 3-3-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.3.2.5 MAC Binding

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

ACL	DMZ	Port Mapping	MAC Binding		
MAC E	Binding List				
	MAC Address	IP Addr	ess	Description	Operation
					×
					•

Figure 3-3-2-5

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

Table 3-3-2-5 MAC Binding Parameters

3.3.3 QoS

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

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

Figure 3-3-3-1

QoS					
Item	Description				
Download/Upload					
Enable	Enable or disable QoS.				
Default Class	Select default class from Service Class list.				
Download/Upload	The download/upload bandwidth capacity of the network 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.				
	The maximum bandwidth that this class is allowed to				
Max BW(kbps)	consume, in kbps. The value should be less than the				
	"Download/Upload Bandwidth Capacity".				

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

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

3.3.4 DHCP

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

3.3.4.1 DHCP Server

The UG87 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 Re	lay		
LoRaWAN >	DHCP Server_1			
Network 👻	Enable	ØE 0 ▼		
Interface	Start Address	192.168.23.100		
Firewall	End Address Netmask	192.168.23.199 255.255.255.0		
QoS	Lease Time(Min)	1440		
DHCP	Primary DNS Server	114.114.114.114		
DDNS	Secondary DNS Server			
Link Failover	Windows Name Server			
VPN	Static IP	Idress	IP Address	Operation
System			n martid	

Figure 3-3-4-1

DHCP Server		
ltem	Description	Default
Enable	Enable or disable DHCP server.	Enable
Interface	Select interface, e.g. GE.	GE
Start	Define the beginning of the pool of IP addresses which	192.168.1.100
Address	will be leased to DHCP clients.	192110011100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	114.114.114.114
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

Table 3-3-4-1 DHCP Server Parameters

3.3.4.2 DHCP Relay

The UG87 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

DHCP Server	DHCP Relay	
DHCP Relay		
Enable		
DHCP Server		

Figure 3-3-4-2

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

Table 3-3-4-2 DHCP Relay Parameters

3.3.5 DDNS

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

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

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

Figure 3-3-5-1

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

Table 3-3-5-1 DDNS Parameters

3.3.6 Link Failover

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

Configuration Steps

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

3.3.6.1 SLA

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

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

Figure	3-3-6	5-1

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

Table 3-3-6-1 SLA Parameters

3.3.6.2 Track

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

Linkage between Track Module and SLA module

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

timely.

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

Linkage between Track Module and Application Module

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

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

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

SLA	Track	VRRP	WAN Failover			
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	• <u>1</u> •	cellular0 •	0	1	×
						8

Figure 3-3-6-2

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

Table 3-3-6-2 Track Parameters

3.3.6.3 VRRP

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

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

		For your device security, please cl	nange
Status	SLA Track	VRRP WAN Failover	
LoRaWAN	VRRP Status		
Network	Status	DISABLE	
	Enable		
Interface	Interface	GE 0	•
Firewall	Virtual Router ID		
QoS	Virtual IP		
DHCP	Priority	100	
DDNS	Advertisement Interval(s)	1	
DDNS	Preemption Mode		
Link Failover	Track ID		•
VPN	Save		

Figure 3-3-6-3

VRRP		
Item	Description	Default
Enable	Enable or disable VRRP.	Disable
Interface	Select the interface of Virtual Router.	None
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.	None
Virtual IP	Set the IP address of Virtual Router.	None
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	None

character.

Table 3-3-6-3 VRRP Parameters

3.3.6.4 WAN Failover

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

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

					For your device security	please change the det	ault password		
Interface	^	SLA	Track	VRRP	WAN Failover				
		WAN Failow	er						
Firewall		Main In	terface	Backup Interface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operatio
QoS		Cellular	•	GE 0 V	30	0	0	1 *	\mathbf{x}
DHCP									
DDNS									
Link Failover		Save							
VPN									

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

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

Table 3-3-6-4 WAN Failover Parameters

3.3.7 VPN

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

The UG87 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.3.7.1 DMVPN

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

				For your	device see
Status	DMVPN	IPsec	GRE	L2TP	PPTP
	DMVPN Setti	ngs			
oRaWAN	Enable		5	8	
etwork	Hub Address		[
	Local IP Addr	ess	[
Interface	GRE HUB IP	Address	[
Firewall	GRE Local IP	Address	[
	GRE Mask		[255.255.255.0	
QoS	GRE Key		[
DHCP	Negotiation N	lode	[Main	•
	Authentication	n Algorithm	[DES	•
DDNS	Encryption Al	gorithm	[MD5	•
Link Failover	DH Group		[MODP768-1	•
	Key		[
VPN	Local ID Type		[Default	•
/stem	IKE Life Time	(s)	[10800	
	SA Algorithm		[DES-MD5	•
dustrial 🕨	PFS Group			NULL	•
	Life Time(s)		Γ	3600	

Figure 3-3-7-1

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



DMVPN	
Item	Description
Enable	Enable or disable DMVPN.
Hub Address	The IP address or domain name of DMVPN Hub.
Local IP address	DMVPN local tunnel IP address.
GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Algorithm	
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and "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 3-3-7-1 DMVPN Parameters

3.3.7.2 IPSec

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

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

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

DMVPN	IPsec	GRE	L2TP	PPTP
IPsec Settings				
- IPsec_1				
Enable		V		
IPsec Gat	eway Address			
IPsec Mod	de	T	unnel	•
IPsec Pro	tocol	E	SP	*
Lo <mark>c</mark> al Sub	net			
Local Sub	net <mark>Mas</mark> k			
Local ID T	уре	D	efault	•
Remote S	ubnet			
Remote S	ubnet Mask			
Remote II) Туре	D	efault	•

Figure 3-3-7-3

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

Table 3-3-7-2 IPsec Parameters

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



IKE Parameter		
Item	Description	
IKE Version	Select from "IKEv1" and "IKEv2".	
Negotiation Mode	Select from "Main" and "Aggressive".	
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	
rrs dioup	"MODP1536_5".	
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.	

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

Table 3-3-7-3 IPsec Parameters

3.3.7.3 GRE

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

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

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

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

Figure 3-3-7-5

GRE	
Item	Description
Enable	Check to enable GRE function.

Enter the real remote IP address of GRE tunnel.	
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 3-3-7-4 GRE Parameters

3.3.7.4 L2TP

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

DMVPN	IPsec	GRE	L2TP	PPTP
L2TP Settings				
— L2TP_1				
Enable				
Remote IF	Address			
Username				
Password				
Authentica	ation	A	uto	•
Global Tra	ffic 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.	

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

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

Figure 3-3-7-7

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

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

Table 3-3-7-6 L2TP Parameters

3.3.7.5 PPTP

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

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



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

Table 3-3-7-7 PPTP Parameters

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

Figure 3-3-7-9

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

Table 3-3-7-8 PPTP Parameters

3.3.7.6 OpenVPN Client

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

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

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

Figure 3-3-7-10

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

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	Check to enable TLS authentication.
Authentication	Check to enable its 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 3-3-7-9 OpenVPN Client Parameters

3.3.7.7 OpenVPN Server

The UG87 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 Ser	ver Settings					
Enable						
Protocol		UDP		*		
Port		1194				
Listening IP						
Interface		tun		v		
Authentication		None		*		
Local Virtual IP						
Remote Virtual	IP					
Enable NAT		1				
Compression		LZO		*		
Link Detection I	nterval	60				
Cipher		None		¥		
MTU		1500				
Max Frame Size	e	1500				
Verbose Level		ERROR		•		
Expert Options						



Local Route			
	Subnet	Netmask	Operation
Account			
	Username	Password	Operation
			•

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

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

Remote Virtual IP	The remote tunnel address of OpenVPN's tunnel.
Client Subnet	Local subnet IP address of OpenVPN client.
Client Netmask	Local netmask of OpenVPN client.
Renegotiation Interval(s)	Set interval for renegotiation. Range: 0-86400.
Max Clients	Maximum OpenVPN client number. Range: 1-128.
Enable CRL	Enable CRL
Enable Client to Client	Allow access between different OpenVPN clients.
Enable Dup Client	Allow multiple users to use the same certification.
Enable NAT	Check to enable the NAT traversal function.
Compression	Select "LZO" to compress data.
Link Detection Interval	Set link detection interval time to ensure tunnel connection.
LINK Detection Interval	Range: 10-1800.
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",
Cipiter	"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".
Export Options	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 3-3-7-10 OpenVPN Server Parameters

3.3.7.8 Certifications

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

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

Figure 3-3-7-13

OpenVPN Client	
ltem	Description
CA	Import/Export CA certificate file.

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

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

OpenVPN Server

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

Figure 3-3-7-14

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

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

Figure 3-3-7-15

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

Table 3-3-7-13 IPsec Parameters

3.4 System

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

3.4.1 General Settings

3.4.1.1 General

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

Status	General	System Time	SMTP	Phone	Email	Storage
LoRaWAN 🕨	System					
Network 🕨	Hostname Web Login Time	out(s)	ROUTER 1800			
System 👻	Access Service	e				
General Settings		Enable	Servi	се		Port
		2	HTT	P		80
User Management			HTTH	PS		443
SNMP			TELN	ET		23
ААА			SSI	4		22
Device Management	HTTS Certifica	tes				
Events	Certificate	https.crt	Browse	Import Export	Delete	
Maintenance	Key	https.key	Browse	Import Export	Delete	



General			
Item	Item Description I		
System			
Hostname	User-defined gateway name, needs to start with a letter.	URSA	
Web Login	You need to log in again if it times out. Range: 100-3600.	1800	
Timeout (s)	Tou need to log in again in it times out. Nange. 100-5000.	1800	
Access Service			
Port	Set port number of the services. Range: 1-65535.		

HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80
	Users can log in the device locally and remotely via	
HTTPS	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	ates	
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.	
Кеу	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.	

Table 3-4-1-1 General Setting Parameters

3.4.1.2 System Time

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

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

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

Figure 3-4-1-2

General	System Time	SMTP	Phone	Email
System Time S	Settings			
Current Time		2019-06-12 20	:33:59 Wed	
Time Zone		8 China (Be <mark>i</mark> ji	ng) 🔻	
Sync Type		Set up Manua		
Date		2019-06-12		
Time		20 🔻 3	3 🔻 59 🔻	
	Fi	gure 3-4-1-3		
General	System Time	SMTP	Phone	Email
System Time	Settings			

Current Time	2019-06-12 20:33:36 Web	1
lime Zone	8 China (Beijing)	۲
Sync Type	Sync with NTP Server	٠
ITP Server Address	1.cn.pool.ntp.org	
nable NTP Server		



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

Table 3-4-1-2 System Time Parameters

3.4.1.3 SMTP

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

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

Figure 3-4-1-5

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

Table 3-4-1-3 SMTP Setting

Related Topics

Events Setting

3.4.1.4 Phone

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

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

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

Figure 3-4-1-6

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

Table 3-4-1-4 Phone Settings

Related Topic

Connect on Demand

3.4.1.5 Email

Email settings involve email alarm for events.

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

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

Figure 3-4-1-7

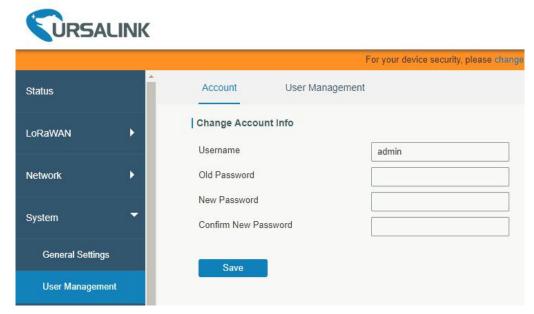
Email	Email				
Item Description					
Email List					
Email Address	Enter the Email address.				
Description The description of the Email address.					
Email Group List					
Group ID	Set number for email group. Range: 1-100.				
Description The description of the Email group.					
List	Show the Email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

Table 3-4-1-5 Email Settings

3.4.2 User Management

3.4.2.1 Account

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





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

Table 3-4-2-1 Account Information

3.4.2.2 User Management

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

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



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 3-4-2-2 User Management

3.4.3 SNMP

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

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

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

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

3.4.3.1 SNMP

The UG87 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	gs			
	Enable				
Network •	Port		161		
System	5.0 2330 53 234		SNMPv2		•
	Location Inform	nation			
General Settings	Contact Inform	ation			
User Management	Save				
SNMP					

Figure 3-4-3-1

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

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

Table 3-4-3-1 SNMP Parameters

3.4.3.2 MIB View

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

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

Figure 3-4-3-2

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

Table 3-3-3-2 MIB View Parameters

3.4.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
SNMP v1 & v2	2 User List					
Comm	unity	Permission	MIB Vi	ew	Network	Operation
private		Read-write	All	•	0.0.0/0	×
public		Read-only	• none	•	0.0.0/0	×
						+



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

Table 3-4-3-3 VACM Parameters

3.4.3.4 Trap

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

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

Figure 3-4-3-4

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

Table 3-4-3-4 Trap Parameters

3.4.3.5 MIB

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

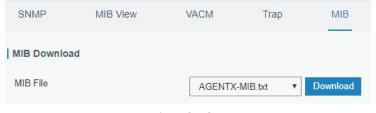


Figure 3-4-3-5

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

3.4.4 AAA

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

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

3.4.4.1 RADIUS

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

Status	Radius	Tacacs+	LDAP	Authentication
LoRaWAN 🕨	Radius Settir	ngs		
	Enable			
Network •	Server IP Add	ress		
System	Server Port		1812	
Gystem	Key			
General Settings	Save			
User Management	Save			
SNMP				
АЛА				

Figure 3-4-4-1

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

Table 3-4-4-1 RADIUS Parameters

3.4.4.2 TACACS+

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

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

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

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

Table 3-4-4-2 TACACS+ Parameters

3.4.4.3 LDAP

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

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

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

Figure 3-4-4-3

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

Table 3-4-4-3 LDAP Parameters

3.4.4.4 Authentication

AAA supports the following authentication ways:

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

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

Radius	Tacacs+	LDAP		Authentication			
Authenticatio	n Settings						
Ser	vice	1		i.	2	3	
Cor	nsole	None	T	None		None	Ŧ
W	/eb	None	T	None	•	None	
Te	Inet	None	•	None	*	None	۳
S	SH	None	v	None	Ŧ	None	w



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

Table 3-4-4-4 Authentication Parameters

3.4.5 Device Management

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

Status	Device Management	
LoRaWAN •	Device Management	
	Status	Disconnected
Network •	Activation Server Address	
Quality	Device Management Server Address	
System	Activation Method	By Authentication Code
General Settings	Authentication Code	
User Management	Connect	
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 password.
Password	Fin in the registered Devicendo account (email) and password.

Table 3-4-5-1

3.4.6 Events

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

3.4.6.1 Events

You can view alarm messages on this page.

us	Events	Events Setti	ngs			
awan	Mark as Re	ad Delete	Mark All as	s Read De	lete All Alarms	
letwork	•	Status	Туре	Time		Message
system	< > 10	Go to:	GO			
General Settings						
User Management						
ААА						
Device Management						
Events						

Figure 3-4-6-1

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

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

Table 3-4-6-1 Events Parameters

3.4.6.2 Events Settings

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

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

Figure 3-4-6-2

Event Settings	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"		
RECOLU	page if this option is checked.		
Email	The relevant content of event alarm will be sent out via email if this		

	option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure the
Email Setting	Email group.
SMS	The relevant content of event alarm will be sent out via SMS if this
21/12	option is checked.
SMC Cotting	Click and you will be redirected to the page of "Phone" to configure
SMS Setting	phone group list.
Phone Group List	Select phone group to receive SMS alarm.
Email Group List	Select Email group to receive Email alarm.

Table 3-4-6-2 Events Parameters

Related Topics

Email Setting

Phone Setting

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping and traceroute.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

Status		Ping Traceroute
LoRaWAN	•	IP Ping
Network	•	Host Ping Stop
System	•	
Maintenance	-	
Tools		
		Figure 3-5-1-1
	PING	
	Item	Description
	Host	Ping outer network from the gateway.

Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

UG87 User Guide

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

Figure 3-5-1-2

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

Table 3-5-1-2 Traceroute Parameters

3.5.2 Schedule

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

Status		Schedule				
LoRaWAN	•	Schedule				
Network	•	Schedule	Frequency	Hour	Minute	
System	•	Save				
Maintenance	•					
Tools						
Schedule						



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

Table 3-5-2-1 Schedule Parameters

3.5.3 Log

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

3.5.3.1 System Log

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

Status			og Settings		
LoRaWAN		Download			
		File	Log File	Download	
Network	•	Log			
System	•	View recent(lines)	20	T	
Maintenance	-	Thu Jul 18 15:06:26 2019 Thu Jul 18 15:06:26 2019	user.notice redis[1859]: Backgrou user.notice redis[1859]: 10 change user.notice redis[1859]: Backgrou user.notice redis[11683]: DB save	nd saving started by pid 11683	*
Tools		Thu Jul 18 15:06:26 2019 Thu Jul 18 15:11:27 2019	user.notice redis[1859]: Backgrou user.notice redis[1859]: 10 change	nd saving terminated with success as in 300 seconds. Saving	
Schedule		Thu Jul 18 15:11:27 2019	user.notice redis[1859]: Backgroun user.notice redis[15776]: DB save user.notice redis[1859]: Backgroun		
Log		Thu Jul 18 15:16:28 2019 Thu Jul 18 15:16:28 2019	user.notice redis[1859]: 10 change user.notice redis[1859]: Backgrou	es in 300 seconds. Saving nd saving started by pid 19899	
			user.notice redis[19899]: DB save	d on disk nd saving terminated with success	

Figure 3-5-3-1

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 3-5-3-1 System Log Parameters

3.5.3.2 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	Ţ]
Size		1024		КВ
Log Severity		Info	•	

Figure 3-5-3-2

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

Table 3-5-3-2 System Log Parameters

3.5.4 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.

UG87 User Guide

Status	Î	Upgrade		
LoRaWAN	•	Upgrade		
Network	•	Firmware Version Reset Configuration to Factory Default	80.0.0.18	
System	•	Upgrade Firmware		Browse Upgrade
Maintenance	-			
Tools				
Schedule				
Log				
Upgrade				

Figure 3-5-4-1

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 "Upgrade" to upgrade firmware.	

Table 3-5-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.5.5 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.

LoRaWAN	* *	Backup and Restore
Network		Restore Config
System	•	Config File Browse Import
Maintenance	•	Backup Running-config
Tools		Restore Factory Defaults
Schedule		Reset
Log		
Upgrade		
Backup and Rest	tore	

Figure 3-5-5-1

Backup and Restore			
ltem	Description		
Config Filo	Click "Browse" button to select configuration file, and then click "Import"		
Config File	button to upload the configuration file to the gateway.		
Backup	Click "Backup" to export the current configuration file to the PC.		
Decet	Click "Reset" button to reset factory default settings. gateway will restart		
Reset	after reset process is done.		

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

Related Configuration Example

Restore Factory Defaults

3.5.6 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.

UG87 User Guide

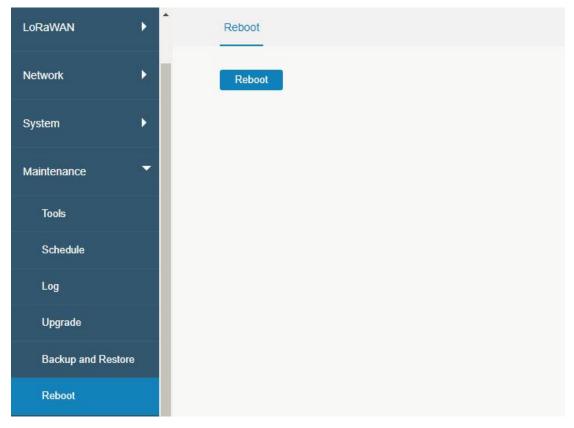


Figure 3-5-6-1

3.6 APP

3.6.1 Python

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

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

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

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

3.6.1.1 Python

URSA	LINK				
			For your de	vice security, please chan	ge the default passw
Status		Python	AppManager Configuration	Python APP	
LoRaWAN	•	Python			
Network	•	AppManager Status	Running		View
NELWOIK		SDK Version	1.1.12		Uninstall
System	•	SDK Path	eMMC		
	~	Available Storage	eMMC	•	
Industrial		SDK Upload		Browse	e Install
Maintenance	•				
APP	-				
Python					

Figure 3-6-1-1

Python				
Item	Description			
AppManager Status	Show AppManager's running status, like "Uninstalled", "Running" or "Stopped".			
SDK Version	Show the version of the installed SDK.			
SDK Path	Show the SDK installation path.			
Available Storage	Select available storage to install SDK.			
SDK Upload	Upload and install SDK for Python.			
Uninstall	Uninstall SDK.			
View	View application status managed by AppManager.			

Table 3-6-1-1 Python Parameters

3.6.1.2 App Manager Configuration

Python	AppManager Configuration	Python APP	
AppManager			
Enable			
App Managemen	t		
ID	App Comman	d Logfile Size(MB)	Uninstall
App Status			
А	pp Name	App Version	SDK Version

Figure 3-6-1-2

AppManager Configuration				
Item	Description			
Enable	After enabling Python AppManager, user can click "View" button on the "Python"			
	webpage to view the application status managed by AppManager.			
App Management				
ID	Show the ID of the imported App.			
App Command	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 3-6-1-2 APP Manager Parameters

3.6.1.3 Python App

Python	AppManager Configuration	Python APP
Import App P	ackage	
App Package		Browse Import
Import App C	onfiguration	
App Name		•
App Configura	tion	Browse Import
Debug Script		
Debug File		• Export
Debug Script		Browse Import



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

Table 3-6-1-3 APP Parameters

Chapter 4 Application Examples

4.1 Application Configuration

1

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

The configuration procedures are listed as below.

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

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

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

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

Туре	HTTP	•
------	------	---

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

TTP Header			
	Header Name	Header Value	Operation
			\mathbf{X}
			H

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

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

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

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

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

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

Step 1: select the transmission protocol as MQTT.

	Туре	MQTT	T
Step 2: Fill	in general settings.		
	General		
	Broker Address		
	Broker Port		
	Client ID		
	Connection Timeout/s	30	
	Keep Alive Interval/s	60	

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

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

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

User Credentials	
Enable	
Username	
Password	

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

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

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

QoS 0 – Only Once

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

QoS 1 – At Least Once

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

QoS 2 – Exactly Once

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

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

4.2 Device Profiles Configuration

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

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

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

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

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

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

4.3 Device Configuration

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

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

Device		
General		
Device Name	asd	
Description	s	
Device EUI	3530353083376118	
Device-Profile	ninii	•
Application	AS923	٣
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 Personalisation	
Device is pre-programmed with a DevAddr, an AppSKey and a NwkSKey. No join procedure is necessary.	The Network Server is also pre- configured with the device's DevAddr, AppSkey and NwkSkey so it recognises its
	transmissions.

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

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

Activate Device(OTAA)

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

	Over-The	-Air Activation	
Device sends join-request with pre-programmed DevEU , AppEU and AppKey , as well as a random DevNonce.	UG87-LW manages packet and then for its networ	rwards it to	The Network Server receives request and consults the entity associated with the AppEU to ralidate the request. If permission is granted, it responds with a join-accept message.
	The device stores the NetID , DevAddr and network settings,	The join-accept response contains a NetID , a DevAddr	and
(5)	and then uses the AppNonce to generate its session keys, NwkSKey and AppSKey.	a AppNonce , as well as sor network settings like DLSetti RxDelay and an optional CF	ngs,

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.

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

4.4 Send Data to Device

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

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

UG87 User Guide

1122612191	8681	00000 SF7BW12	5	13	17	0	JnAcc	2019-08-06T	09:22:29+08:00	0
112261219	8681	00000 SF7BW12	5 9.5	-77	18	0	JnReq	2019-08-06T	09:22:29+08:00	0
ь	h									
tep 2: Fill t	nese inpu	it box.								
Send Data To D	evice									
De	evice EUI	Тур	e			Payload			Fport	Confirmed
1122612191	3	ASCII	×	[15	1004			15	
				L						٣
tep 3: Click	"Send".									
			in the second			÷				
			end		sen	d suc	cess			

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

Note: please enable the "confirmed".

Send Data To Device				
Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII 🔻	15	15	۲

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

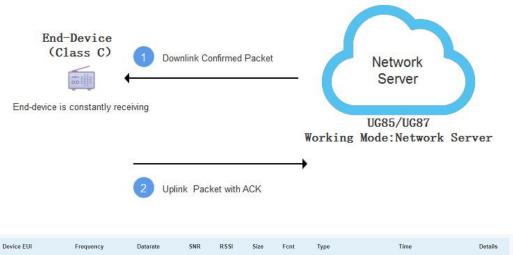
This packet's type is DnCnf (Downlink Confirmed Packet) and if the packet's color is gray, then it means the packet cannot be transmitted now because at least one message has been in the queue.

11226121912 0	6 2 DnCnf	0
---------------	-----------	---

This is the data packet has been delivered successfully.

2019-08-06T09:22:55+08:00 Success 🌗	DnCnf	2	6	- 21	1.00	SF12BW125	869525000	1122612191311123
Pending 🕛	DnCnf	2	6				0	1122612191311123

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



Device E01	Frequency	Datarate	JUN	11331	3120	Full	Type	Time	Details
11226121913	868300000	SF10BW125	(-)	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	-0
112261219	869525000	SF12BW125		-	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125	-	-	0	1	DnUnc	2019-08-06T09:22:49+08:00	0

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

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

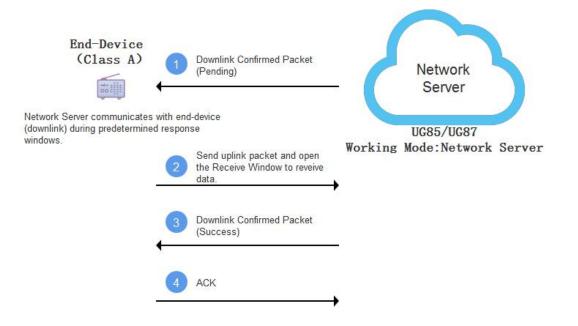
If the device's class type is Class A, then the Network Server communicates with end-device (downlink) during predetermined response windows.

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

1122612191 ²⁻ 0 6 2 DnCnf	0
--------------------------------------	---

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

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



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

Packets

4.5 Restore Factory Defaults

4.5.1 Via Web Interface

- 1. Log in web interface, and go to "Maintenance > Backup and Restore".
- 2. Click "Reset" button under the "Restore Factory Defaults".

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

Status	Backup and Restore
LoRaWAN	Restore Config
Network	Config File Browse Import
System	Backup Running-config
Industrial	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 Import
Backup Running-config	
Backup	Reset, please do not power off
Restore Factory Defaults	
Reset	

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



Related Topic Restore Factory Defaults

4.5.2 Via Hardware

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

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

4.6 Firmware Upgrade

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

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

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

LoRaWAN	× ^	Upgrade	
Network	•	Upgrade	
System	•	Firmware Version Reset Configuration to Factory Default	80.0.0.18
Maintenance	-	Upgrade Firmware	Browse Upgrade
Tools			
Schedule			
Log			
Upgrade			

Upgrade	
Upgrade	
Firmware Version	2.0.0.19
Reset Configuration to Factory Default	
Upgrade Firmware	C:\fakepath\2.0.0.19.bin Browse Upgrade 2 Importing firmware. Please stay on this page till upgrade is finished.
Please kee	ep the power on during upgrade.

<u>Upgrade</u>

4.7 Cellular Connection

The UG87 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 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	I LAN	VLAN Trunk	Cellular	Loopback	
LoRaWAN	Cellular Setting			2 Cellular		
		SIM1		SIM2		
Network	Enable					
Interface	Network Type	Auto		▼ Auto	•	
Firewall (1) Interface	APN Usemame	4G Fi 4G O	nly			
рнср	Password	3G Fi 3G O 2G Fi	nly	o" or others		
DDNS	Access Number	2G O				
	PIN Code					
Link Failover	Authentication Type	Auto		Auto	•	
VPN	Roaming					
System	SMS Center					
	Connection Setting					
Status P	ort WAN LAN	N VLAN Trunk	Cellular	Loopback	Apply 5 Apply	Ladmin Ə
olatus	issword					Enable ^
LoRaWAN	ccess Number					enable the corresponding SIM card.
Network - Pil	N Code					Network Type
	thentication Type	Auto	• Auto)	•	Select from "Auto", "4G First", "4G Only", "3G First", "3G Only", "2G
Interface Ro	paming					Frist", and "2G Only". Auto: connect to the
Firewall SN	/IS Center					network with the strongest signal
UNCP	onnection Setting					automatically. 4G First: 4G network has priority
DDNS	ial SIM Strategy nable NAT					to be connected. 4G Only: connect to 4G network only. And so on.
Link Failover						APN
VPN	MP Server	8.8.8.8				Enter the Access Point Name for cellular dial-up
Se	econdary ICMP Server	114.114.114				connection provided by local ISP.
oystem v	NG Times icket Loss Rate	5				Username Enter the username for
Industrial	IS Settings	20	%			cellular dial-up connection provided by local ISP.
Maintenance SM						Password
	/IS Mode	PDU	•			Enter the password for

Click "Save" and "Apply" for configuration to take effect. **Note:**

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

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

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

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

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
Modem							
Status		Ready					
Model		U9300C					
Current SIM		SIM1					
Signal Level		29asu (-56dBm)					
Register Status		Registered (Home r	network)				
IMSI		460070615219248					
ICCID		898602E613153201	19248				
ISP		CHINA MOBILE					
Network Type		LTE					
PLMN ID		46007					
LAC		fffe					
Cell ID		f700e28					
IMEI		862808032459987					
Network							
Status		Connected	Connected				
IP Address		10.39.128.14					
Netmask		255.255.255.252					
Gateway		10.39.128.13					
DNS		211.143.147.120					
Connection Duration		0 days, 00:15:35			N	Aanual Refresh 🔻	Refresh

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.

Related Topic

Cellular Setting Cellular Status

4.8 Dual SIM Backup Application Example

Example

In this section we will take an example of inserting two SIM cards into the UG87. When one SIM fails, gateway will try to connect with the other SIM as backup link.

Configuration Steps

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

				Apply
Status	Port WAN	LAN VLAN Tru	nk Cellular 2	Loopback
LoRaWAN	Cellular Setting			
		SIM1	SIM2	
Network 🔻	Enable	3 .	Ø	
Interface ①	Network Type	Auto	▼ Auto	Ŧ
E	APN			
Firewall				
	Username			
DHCP	Password			
DDNS	Access Number			
	PIN Code			
Link Failover	Plin Code			
1/DN	Authentication Type	Auto	 Auto 	T
VPN	Roaming			

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

	8 Apply
Status	Port WAN LAN VLAN Trunk Cellular Loopback
LoRaWAN	Connection Setting Dual SIM Strategy 5
Network	Primary SIM Card SIM1
Interface	Switch to backup SIM card when ICMF @ detection fails
Firewall	Swtich to backup SIM card when the connection fails
DHCP	Switch to backup SIM card when
DDNS	Enable NAT
Link Failover	
VPN	ICMP Server 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 V
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.

Ove	rview	Cellular	Network	VPN	Routing			
Mode	em							
Statu	IS		Ready					
Mode	el		EC25					
Curre	ent SIM		SIM1					
Signa	al Level		15asu (-83dBm)					
Register Status			Registered (Home network)					
IMSI			460019987103071					
ICCID			89860117838019196629					
ISP			CHN-UNICOM					
Netw	ork Type		LTE					
	Network							
	Status		C	onnected				
	IP Addres	S	1(0.105.39.33				

 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 (-83dBn	1)	
Register Status		Registered (Ho	me network)	
IMSI		460019987103	071	
ICCID		898601178380	19196629	
Network	ſ			
Status			Connected)
IP Addre	SS		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.

Cellular Setting

Cellular Status

4.9 Wi-Fi Application Example

4.9.1 AP Mode

Application Example

Configure UG87 as AP to allow connection from users or devices.

Configuration Steps

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

URSAL	INK							
					For your device set	curity, please change	e the default passwo	rd
Status	1	Port	WAN	LAN	VLAN Trunk	WLAN	Cellular	Loopback
LoRaWAN	F	WLAN Enable						
Network	-	Work Mode		☑		•		
Interface		SSID Broad						
Firewall		Radio Type		802	11g(2.4GHz)	•		
QoS		Channel SSID		Aut	o alink_support	•		
DHCP		BSSID						
DDNS		Encryption M	Vlode	WP	A2-PSK	v		
Link Failover		Cipher		AES	6	¥		
		Key		•••••				
VPN		Bandwidth		201	ЛНz	*		
System		Max Client 1	Number	128	6			

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

2. Use a smart phone to connect by SSID "Ursalink_F0257A". Go to "Status > WLAN", and

you can check the AP settings and information of the connected client/user.

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

4.9.2 Client Mode

Application Example

Configure UG87 as Wi-Fi client to connect to an access point to have Internet access.

Configuration Steps

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

		For your device security	y, please change	the default passwork	E.
Status	Port WAN	LAN VLAN Trunk	WLAN	Cellular	Loopback
LoRaWAN 🕨] WLAN				
Network 🝷	Enable Work Mode	☑ Client ▼	Scan		
Interface	SSID	Meeting Room]		
Firewall	BSSID	24:e1:24:f0:01:77			
r ii ciwaii	Encryption Mode	WPA2-PSK			
QoS	Cipher	AES 🔻]		
DHCP	Key]		
DDNS	IP Setting				
Link Failover	Protocol	DHCP Client •]		

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

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

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

WLAN Setting

WLAN Status

[END]