

# × UG65 Indoor LoRaWAN Gateway User Guide SHROM Xiamen Ursalink Technology Co., Ltd. П UG65

www.ursalink.com

# Preface

Thanks for choosing Ursalink UG65 industrial LoRaWAN gateway. The UG65 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 UG65 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 UG65 LoRaWAN gateway

# **Related Documents**

Document	Description				
Ursalink UG65 Datasheet	Datasheet for the Ursalink UG65 industrial LoRaWAN gateway.				
Ursalink UG65 Quick Start Guide	Quick Installation Guide for the Ursalink UG65 industrial LoRaWAN gateway.				

# **Declaration of Conformity**

UG65 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: help@ursalink.com Tel.: 86-592-5023060 Fax: 86-592-5023065

# **Revision History**

Date	Doc Version	Description
Aug. 31, 2020	V1.0	Initial version

# Contents

Chapter 1 Product Introduction	7
1.1 Overview	7
1.2 Advantages	7
1.3 Specifications	8
1.4 Dimensions (mm)	10
Chapter 2 Access to Web GUI	11
2.1 PC Configuration for Web GUI Access to gateway	
2.2 Access to Web GUI of gateway	12
Chapter 3 Web Configuration	14
3.1 Status	14
3.1.1 Overview	
3.1.2 Packet Forwarder	
3.1.3 Cellular	
3.1.4 Network	
3.1.5 WLAN	18
3.1.6 VPN	
3.1.7 Host List	21
3.2 LoRaWAN	
3.2.1 Packet Forwarder	22
3.2.1.1 General	
3.2.1.2 Radios	23
3.2.1.3 Advanced	25
3.2.1.4 Custom	26
3.2.1.5 Traffic	
3.2.2 Network Server	28
3.2.2.1 General	28
3.2.2.2 Application	30
3.2.2.3 Profiles	
3.2.2.4 Device	31
3.2.2.5 Packets	
3.3 Network	35
3.3.1 Interface	35
3.3.1.1 Port	35
3.3.1.2 WLAN	
3.3.1.3 Cellular	41
3.3.1.4 Loopback	44
3.3.2 Firewall	45
3.3.2.1 Security	
3.3.2.2 ACL	46
3.3.2.3 DMZ	47
3.3.2.4 Port Mapping	48

	3.3.2.5 MAC Binding	.48
	3.3.3 DHCP	. 49
	3.3.4 DDNS	. 50
	3.3.5 Link Failover	.51
	3.3.5.1 SLA	51
	3.3.5.2 Track	.52
	3.3.5.3 WAN Failover	.53
	3.3.6 VPN	.54
	3.3.6.1 DMVPN	. 54
	3.3.6.2 IPSec	.55
	3.3.6.3 GRE	.58
	3.3.6.4 L2TP	.59
	3.3.6.5 PPTP	. 61
	3.3.6.6 OpenVPN Client	.63
	3.3.6.7 OpenVPN Server	64
	3.3.6.8 Certifications	. 66
3.4 9	System	. 68
	3.4.1 General Settings	. 68
	3.4.1.1 General	
	3.4.1.2 System Time	. 69
	3.4.1.3 SMTP	
	3.4.1.4 Phone	.71
	3.4.1.5 Email	. 72
	3.4.2 User Management	.73
	3.4.2.1 Account	.73
	3.4.2.2 User Management	74
	3.4.3 SNMP	75
	3.4.3.1 SNMP	. 75
	3.4.3.2 MIB View	. 76
	3.4.3.3 VACM	. 76
	3.4.3.4 Trap	. 77
	3.4.3.5 MIB	.78
	3.4.5 Device Management	. 78
	3.4.6 Events	.79
	3.4.6.1 Events	.79
	3.4.6.2 Events Settings	. 80
3.5	Maintenance	.81
	3.5.1 Tools	. 81
	3.5.1.1 Ping	. 81
	3.5.1.2 Traceroute	.81
	3.5.2 Schedule	82
	3.5.3 Log	. 82
	3.5.3.1 System Log	.83
	3.5.3.2 Log Settings	83

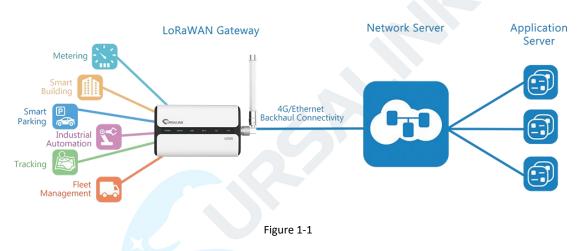
3.5.4 Upgrade	84
3.5.5 Backup and Restore	85
3.5.6 Reboot	85
3.6 APP	
3.6.1 Python	86
3.6.1.1 Python	87
3.6.1.2 App Manager Configuration	
3.6.1.3 Python App	
Chapter 4 Application Examples	
4.1 Packet Forwarder Configuration	
4.2 Application Configuration	
4.3 Device Profiles Configuration	94
4.4 Device Configuration	
4.5 Send Data to Device	
4.6 Restore Factory Defaults	
4.6.1 Via Web Interface	
4.6.2 Via Hardware	
4.7 Firmware Upgrade	
4.8 Cellular Connection	
4.9 Wi-Fi Application Example	
4.9.1 AP Mode	
4.9.2 Client Mode	

# **Chapter 1 Product Introduction**

#### 1.1 Overview

Ursalink UG65 is an affordable 8-channel indoor LoRaWAN gateway. Adopting SX1302 LoRa chip and high-performance quad-core CPU, UG65 supports connection with more than 2000 nodes. UG65 has line of sight up to 10km and can cover about 2km in urbanized environment, which is ideally suited to smart office, smart building and many other indoor applications.

UG65 supports not only multiple back-haul backups with Ethernet, Wi-Fi and cellular and has integrated mainstream LoRa network servers (such as TTN, ChirpStack, etc.), but also built-in network server and Ursalink Cloud for easy deployment.



# 1.2 Advantages

#### Benefits

- Built-in industrial CPU and big memory;
- Ethernet, 2.4GHz 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
- 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

#### **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 quad core 64-bit ARM Cortex-A53 processor, high-performance operating up to 1.5GHz with low power consumption, and 8GB eMMC available to support more applications
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

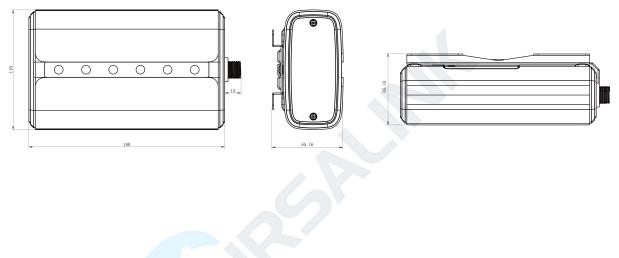
Hardware System	
CPU	Quad-core 1.5GHz, 64-bit ARM Cortex-A53
Memory	8 GB eMMC Flash, 512 MB DDR4 RAM
LoRaWAN	
A . I	Fully Integrated and Internal Antenna
Antenna	(Optional: $1 \times 50 \Omega$ N-Female External Connector)
Channel	8
European Devel	EU433/CN470/IN865/EU868/RU864/US915/AU915/KR920/AS9
Frequency Band	23
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class C and V1.0.2 Class A/Class C
Ethernet	
Ports	1 × RJ-45 (PoE PD supported)
Physical Layer	10/100/1000 Base-T (IEEE 802.3)

#### **1.3 Specifications**

Data Rate	10/100/1000 Mbps (auto-sensing)				
Interface	Auto MDI/MDIX				
Mode	Full or half duplex (auto-sensing)				
Wi-Fi Interfaces					
Antenna	Fully Integrated and Internal Antenna				
Standards	IEEE 802.11 b/g/n				
	802.11b: 18 dBm +/-2.0 dBm (11 Mbps)				
	802.11g: 15 dBm +/-2.0 dBm (6 Mbps)				
	802.11g: 15 dBm +/-2.0 dBm (54 Mbps)				
Tx Power	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS0_HT20)				
	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS7_HT20)				
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS0_HT40)				
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS7_HT40)				
Cellular Interfaces (Opti	onal)				
Antenna	Fully Integrated and Internal Antenna				
SIM Slots	1				
Software					
Network Protocols	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS,				
Network Frotocols	DNS, SNTP, Telnet, SSH, MQTT, etc.				
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE				
VPN Tunnel Access Authentication	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE CHAP/PAP/MS-CHAP/MS-CHAPV2				
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2				
Access Authentication Firewall	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up				
Access Authentication Firewall Management Power Supply and Const	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up				
Access Authentication Firewall Management	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up				
Access Authentication Firewall Management Power Supply and Consu Power Supply Consumption	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up umption 1. DC Jack Connector for 9-24 VDC power supply				
Access Authentication Firewall Management Power Supply and Consu Power Supply	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up <b>umption</b> 1. DC Jack Connector for 9-24 VDC power supply 2. 1 × 802.3 af PoE input				
Access Authentication Firewall Management Power Supply and Consu Power Supply Consumption Physical Characteristics	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up <b>umption</b> 1. DC Jack Connector for 9-24 VDC power supply 2. 1 × 802.3 af PoE input ≤ 4.2W				
Access Authentication Firewall Management Power Supply and Consu Power Supply Consumption Physical Characteristics Ingress Protection	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up <b>umption</b> 1. DC Jack Connector for 9-24 VDC power supply 2. 1 × 802.3 af PoE input ≤ 4.2W				
Access Authentication Firewall Management Power Supply and Consu Power Supply Consumption Physical Characteristics Ingress Protection Dimensions	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up <b>umption</b> 1. DC Jack Connector for 9-24 VDC power supply 2. 1 × 802.3 af PoE input ≤ 4.2W IP65 180 × 110 × 56.5 mm				
Access Authentication Firewall Management Power Supply and Consu Power Supply Consumption Physical Characteristics Ingress Protection Dimensions Mounting	CHAP/PAP/MS-CHAP/MS-CHAPV2 ACL/DMZ/Port Mapping/MAC Binding Web, CLI, SMS, On-demand dial up <b>umption</b> 1. DC Jack Connector for 9-24 VDC power supply 2. 1 × 802.3 af PoE input ≤ 4.2W IP65 180 × 110 × 56.5 mm				

Built-in	Watchdog, RTC, Timer
Certifications	RoHS, CE, FCC
Environmental	
	-40°C to +70°C (-40°F to +158°F)
Operating Temperature	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)



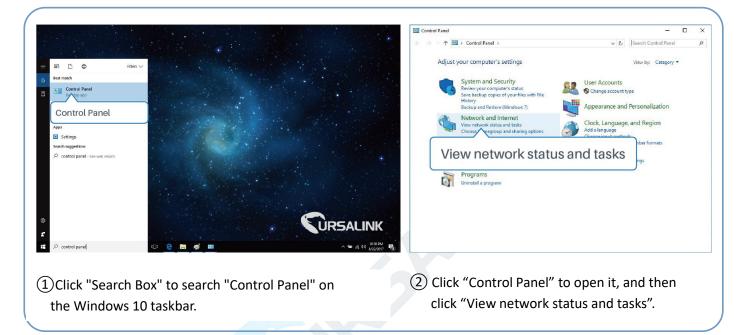
# **Chapter 2 Access to Web GUI**

This chapter explains how to access to Web GUI of the UG65.

# 2.1 PC Configuration for Web GUI Access to gateway

Please connect PC to GE port of UG65 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.



	k and Internet > Network and Sharing Center View your basic network information	✓ ♂ Search Control Panel	Q	General	
Control Panel Home		and set up connections		Connection	
Change adapter settings	View your active networks	Access type: Internet		IPv4 Connectivity:	No network access
Change advanced sharing settings	Yeastar5G	Access type: Internet HomeGroup: Ready to create		IPv6 Connectivity:	No network access
secongs	Private network	Connections: Wi-Fi (Yeastar5G)		Media State:	Enabled
				Duration:	00:01:21
	Identifying	Access type: No network access		Speed:	1.0 Gbps
		Connections:			
	Change your networking settings			Details	
	Change your networking settings	Ethe even eth			
	Set up a broadband, dial-up, or VPN co	Ethernet		Activity	
	Troubleshoot problems			riconty	-
	Diagnose and repair network problems,	or get troubleshooting information.		t —	Received
				Properties	alt
				210	0
See also					
HomeGroup				Properties Disable	Diagnose
Internet Options					
Windows Firewall					Close
New York Constraints and Constraints					Close
~					
	hernet" (May have o	different name)		(4) Click "Proper	

U Ethernet Properties ×	Internet Protocol Version 4 (TCP/IPv4) Properties
Networking Sharing	General
Connect using:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Configure This connection uses the following items:	O <u>O</u> btain an IP address automatically
Client for Microsoft Networks	Use the following IP address:
✓ <sup>1</sup> File and Printer Sharing for Microsoft Networks ✓ <sup>1</sup> QoS Packet Scheduler	IP address: 192 . 168 . 23 . 200
✓ Gos Packet Scheduler ✓ Internet Protocol Version 4 (TCP/IPv4)	Subnet mask: 255 . 255 . 255 . 0
Microsoft Nety Adapter Multiplexor Protocol	Default gateway: 192 . 168 . 23 . 150
Internet Protocol Version 4 (TCP/IPv4)	Obtain DNS server address automatically
	• Use the following DNS server addresses:
Install Uninstall Properties	Preferred DNS server: 8 . 8 . 8 . 8
Transmission Control Protocol/Internet Protocol. The default	Alternative DNS server:
wide area network protocol that provides communication across diverse interconnected networks.	Valjdate settings upon exit Advanced
OK Cancel	OK Cancel
5 Double Click "Internet	6 Click "Use the following IP
Protocol Version 4 (TCP/IPv4)"	address" to assign a static IP
to configure IP address and	manually within the same subnet of
DNS server.	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: 192.168.23.150 **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". × + - 8 × C URSALINK ← → C ③ Not secure | 192.168.23.150/login.htm \$ (\*) English URSALINK Lusername Password

0 :

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 Password					
Old Password					
New Password					
Confirm New Password					
Save Can					

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

URSALIN	К								💄 admin 🛛 🔁
For your device security, please change the default peakword									
Status		Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List	Help — Model
Packet Forwarder		System Informa	tion						Show the model name of router.
		Model		UG65-L00E-W-P-C	N470				Serial Number
Network Server		Serial Number		6221A2254974					Show the serial number of router.
Network		Firmware Version		60.0.0.11					Firmware Version Show the current firmware
Network		Hardware Version	1	V1.0					version of router.
System	۶.	Local Time		2020-08-18 09:40:3	4 Tuesday				Hardware Version Show the current hardware
		Uptime		12:51:23					version of router.
Maintenance	×.	CPU Load		4%					Local Time
		RAM (Capacity/A	vailable)	512MB/139MB(27.1	15%)				Show the current local time of system.
APP	•	eMMC (Capacity/	Available)	3.0G/2.8G(90.95%)					Uptime
				,					Show the information on how long the router has been running.
							Manual Re	efresh 🗸 Refresh	CPU Load
									Show the current CPU

# **Chapter 3 Web Configuration**

# 3.1 Status

# 3.1.1 Overview

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

<b>URSALI</b>	NK							
			F	or your device security	, please change the d	efault password		
Status		Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List
Packet Forwarder		System Informa	tion					
		Model		UG65-L00E-W-P-C	CN470			
Network Server		Serial Number		6221A2254974				
Network		Firmware Version		60.0.0.11				
NEWOIK		Hardware Version		V1.0				
System		Local Time		2020-08-18 09:40:	34 Tuesday			
		Uptime		12:51:23				
Maintenance		CPU Load		4%				
APP	•	RAM (Capacity/A	vailable)	512MB/139MB(27	15%)			
		eMMC (Capacity/	Available)	3.0G/2.8G(90.95%	)			
							Manual Ref	resh 🗸 Refresh

Figure 3-1-1-1

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

Table 3-1-1-1 System Information

# 3.1.2 Packet Forwarder

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

Overview	Packet Forward	Cellular	Network	WLAN	
Basic					
Version	4	.0.1			
Status	R	lunning			
Gateway ID	2	4E124FFFEF0C400			
Region Code	E	U868			
Uplink					
Packet Received	5				
Packets Received State	e C	RC_OK: 80.00%, CR	C_FAIL:		
Packet Forwarded	4	(125 bytes)			
Push Data Datagrams	Sent 5	5 (1320 bytes)			
Push Data Acknowledg	ed 1	00.00%			
Downlink					
Pull Data Sent	3	(100.00% acknowled	ged)		
Pull Resp Datagrams R	eceived 0	(0 bytes)			
Packets Sent to node	0	(0 bytes)			
	Fi	igure 3-1-2-1			

Packet Forwarder Status				
Item	Description			
Basic				
Version	Show the version of packet forwarder software.			
Status	Show the status of packet forwarder.			
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.			
Uplink				
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			
	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.
Downlink	
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.
Packets Sent to node	Show the RF packet counts and size that will be sent from gateway to node.
Packets Sent Errors	Show the RF packet counts that fail to be sent from server to node.

Table 3-1-2-1 LoRaWAN Status

# 3.1.3 Cellular

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

Overview	Packet Forward	Cellular	Network	WLAN
Modem				
Status		Ready		
Model		EC25		
Version		EC25ECGAR06A07M1	G	
Sign <mark>a</mark> l Level		26asu (-61dBm)		
Register Status		Registered (Home netw	ork)	
IMEI		860425047368939		
IMSI		460019425301842		
ICCID		8986011783800993412	0	
ISP		CHN-UNICOM		
Network Type		LTE		
PLMN ID				
LAC		5922		
Cell ID		340db80		

Figure 3-1-3-1

Modem Information				
Item	Description			
Status	Show corresponding detection status of module and SIM card.			
Model	Show the model name of cellular module.			
Version	Show the version of cellular module.			
Signal Level	Show the cellular signal level.			
<b>Register Status</b>	Show the registration status of SIM card.			
IMEI	Show the IMEI of the module.			
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.			

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 Ethernet port status of the gateway.

	Overview	P	acket Forward	Cellular	Network	WLAN	VPN	Host List
V	VAN							
	Port	Status	Туре	IP Address	Netmask	Gateway	DNS	Duration
	GE 0	up	Static	192.168.22.228	255.255.255.0	192.168.22.1	192.168.1.1	05h 25m 44s

Figure 3-2	1-4-1
------------	-------

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

Table 3-1-4-1 WAN Status

# 3.1.5 WLAN

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

Overview	Packet Forward	Cellular	Network	WLAN
WLAN Status				
Wireless Status	Enabled			
MAC Address	24:e1:24:f	D:c4:34		
Interface Type	AP			
SSID	Ursalink_F	0C434		
Channel	Auto			
Encryption Type	WPA-PSK	WPA2-PSK		
Cipher	Auto			
Status	Up			
IP Address	192.168.1	1		
Netmask	255.255.2	55.0		
Connection Duration	0 days, 12	:57: <mark>17</mark>		

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.

#### UG65 User Guide

Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List
PPTP Tunnel						
	Name	Status	Local IP		Remote	IP
	pptp_1	Disconnected	15. X		251	
	pptp_2	Disconnected			-	
	pptp_3	Disconnected	( <b>F</b> )		1.73	
L2TP Tunnel						

Name	Status	Local IP	Remote IP
l2tp_1	Disconnected	17.4 1	-
l2tp_2	Disconnected	-	17.
l2tp_3	Disconnected	~	171

Figure 3-1-6-1

IPsec Tunnel

Name	Status	Local IP	Remote IP
ipsec_1	Disconnected	121	20
ipsec_2	Disconnected	-	2
ipsec_3	Disconnected	(T)	2

#### OpenVPN Client

Name	Status	Local IP	Remote IP
openvpn_1	Disconnected	-	2
openvpn_2	Disconnected		- 2-
openvpn_3	Disconnected	175	: 78

Figure 3-1-6-2

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

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.

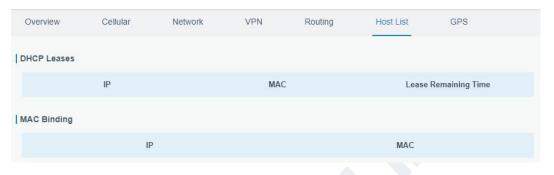
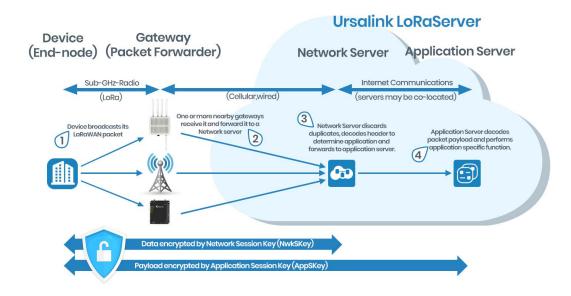


Figure 3-1-7-1

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

Table 3-1-7-1 Host List Description

# 3.2 LoRaWAN



# 3.2.1 Packet Forwarder

# 3.2.1.1 General

General Setting						
General Setting						
Gateway EUI	24E124FFFE	EF027D5				
Gateway ID	24E124FFF	FEF027D5				
Frequency-Sync	Disabled		•			
Multi-Destination						
ID		Enable		Туре	Server Address	Operation
0		Enabled		Ursalink	localhost	2 ×
						Ð

Figure 3-2-1-1

General Settings					
Item	Description	Default			
Gateway EUI		Generated from MAC			
	Show the identifier of the actoway	address of the gateway			
	Show the identifier 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 as gateway EUI and can be changed.	The default is the same as gateway EUI.
Frequency-Sync	Disable: Disable sync frequency configurations from network server, the gateway will use local configurations. Network Server ID: Sync frequency configurations from network server by selecting the corresponding ID.	Disabled
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.	Local host

Table 3-2-1-1 General Setting Parameters

# **Related Configuration Example**

Packet fowarder configuration

# 3.2.1.2 Radios

General	Radios	Advanced	Custom	Traffic		
Antenna Type			2 x Built-in ANT	~	]	
Radio Channe	I Setting					
Supported Freq	uency		EU868	~	]	
	N	ame		Cente	r Frequency/MHz	
	Ra	dio 0		867.5		
	Ra	dio 1		868.5		

Radios-Radio Channel Setting			
ltem	Description	Default	
	Select the transmission type of antennas.		
Antenna Type	Note: Only "2 × Built-in ANT" is valid if there is not	2 × Built-in ANT	
	external antennas.		
	Choose the LoRaWAN frequency plan used for the	The default	
Supported	upstream and downlink frequencies and datarates.	frequency is set	
Frequency	Available channel plans depend on the gateway's	based on the	
	variant.	gateway's variant.	
Name	Show the name of control frequency	Depend on gateway	
Name	Show the name of central frequency.	model.	
Center	Enter the central frequency of Radio 0 which	The default is based	

Frequency	supports transmitting and receiving packet.	on what is specified
	Enter the center frequency of Radio 1 which only	in the LoRaWAN
	supports receiving packet from nodes.	regional parameters
		document.

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

Multi Channels Setting			
Enable	Index	Radio	Frequency/MHz
	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
Ø	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 V

# Figure 3-2-1-4

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

corresponds to a low rate, while the small one	in the LoRaWAN
corresponds to a high rate.	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	Data Rate Enter the data rate. Range: 500-25000.		
	Table 2.2.1 E ECK Channel Catting Devenators		

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

# 3.2.1.3 Advanced

General	Radios	Advanced	Custom	Traffic
Intervals Settin	ng			
Keep Alive Inter	val	10		s
Stat Interval		30		S
Push Timeout		100		ms
Forward CRC	Setting			
Forward CRC D	isabled			
Forward CRC D Forward CRC E				

Advanced		
Item	Description	Default
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to LoRaWAN network server to keep the connection stable and alive. Range: 1-3600.	10
Stat Interval	Enter the interval to update the network server with gateway statistics. Range: 1-3600.	30
Push Timeout	Enter the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-3600.	100
Forward CRC Disabled	Enable to send packets received with CRC disabled to the network server.	Disabled.
Forward CRC Error	Enable to send packets received with CRC errors to the network server.	Disabled.
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled

Table 3-2-1-6 Advanced Parameters

# 3.2.1.4 Custom

General	Radios	Advanced	Custom	Traffic
Custom Config	guration			
Enable				
				Example
	ic": true, adio_1 provides clo ": 0, /* antenna gair "7", 000, 162, Je, 917000000,	ck to concentrator */ n, in dBi */		

Figure 3-2-1-7

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

# 3.2.1.5 Traffic

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

Tra	ffic Setting								
	Refresh	Clear							
	Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
	1	up	e	83002508	922.8	SF9BW125	4/5	-103	-13.2
	1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
	Ť	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	а.	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

General	Applications	Profiles	Device	Packets
General Setting				
Enable				
Ursalink Cloud				
NetID	010203		]	
Join Delay	5		sec	
RX1 Delay	1		sec	
Lease Time	876000-0-0		hh-mm-ss	
Log Level	info	Ţ	]	
Channel Plan Se	etting			
Channel Plan	AU915	Ŧ	]	
Channel Mask			]	
Save & Apply				
	Fig	ure 3-2-2-1		

Item	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Enable
Ursalink Cloud	Enabled to connect gateway to Ursalink Cloud.	Disable
NetID	Enter the network identifier.	01023
Join Delay	Enter the interval time between when the end-device sends a Join_request_message to network server and when the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
RX1 Delay	Enter the interval time between when the end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time till a successful join	"876000-00-00"

-	
to join the network server again when it exceeds	
the lease time.	
Choose the log level.	Info
ing	
Choose LoRaWAN channel plan used for the	
upstream and downlink frequencies and	Depend on the
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 specified in the	
LoRaWAN regional parameters document.	
	Null.
A bit in the ChMask field set to 1 means that	Null means using
the corresponding channel can be used for	the default standard
uplink transmissions if this channel allows the	usable channels
data rate currently used by the end-device.	specified in the
	LoRaWAN regional
A bit set to 0 means the corresponding	parameters
channels should be avoided.	document.
US 915 and AU 915 have a 80-bit channel mask	
channels.	
	Choose the log level. Ing Choose LoRaWAN channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's variant. Enabled frequencies are controlled using channel mask. Leave it blank means using the default standard usable channels specified in the LoRaWAN regional parameters document. A bit in the ChMask field set to 1 means that the corresponding channel can be used for uplink transmissions if this channel allows the data rate currently used by the end-device. A bit set to 0 means the corresponding channels should be avoided. US 915 and AU 915 have a 80-bit channel mask for 72 usable channels and EU, AS, IN, KR frequencies have a 16-bit mask for 16 usable

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 undefined by the LoRaWAN Regional Parameters, like EU868 and KR920, as the following picture shows:

ditional Channels			
Frequency(MHz)	Min Datarate	Max Datarate	Operation
			+



Additional Channe	els	
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	DR0(SF12,125kHz)

	LoRaWAN regional parameters document.	
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.

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

```
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.
	Show the description of the application profile already
Description	created.
Devide and Cardaa	Show the payload codec of the application profile already
Payload Codec	created.
	Table 3-2-2-3 Application Parameters
You can edit the app	plication by clicking 🖉 or create a new application by clicking 🖽
Data Transmission	
	Type Operation
	B



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 Profi	les				
	Name	Max TXPower	Join Type	Class Type	Operatio n
	Device-test	0	ΟΤΑΑ	Class A	
	Ursalink-test-ABP	0	ABP	Class A	l ×
	ninii	0	OTAA	Class A	2X
					Œ



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 configuration** 

#### 3.2.2.4 Device

UC11-T1	24e1641094	162145	ClassA-OTAA	cloud	-		2×
Device Name	Device	EUI	Device-Profile	Application	Last Seen	Activated	Operation
Add	Bulk Import	Delete All				Search	(
evice							
General	Applications	Profil	es Device	Packet	5		

Showing 1 to 1 of 1 rows

Figure 3-2-2-6

Item	Description
Add	Add a device.
Bulk Import	Download template and import multiple devices.
Delete All	Delete all devices in the list.
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.
Activated	Show the status of the device .  means that the device has been activated.
Operation	Edit or delete the device.

Table 3-2-2-5 Device Parameters

# **Related Configuration Example**

# **Device configuration**

.2.5 Packets									
Send Data To Device									
Device EU	I	Туре			I	<sup>o</sup> ayload		Port	Confirmed
000000000000000000000000000000000000000		ASCII	•						
Send									
Network Server									
Clear								Search	Q
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
Device EUI 24e1641193199962	Frequency 865402500	Datarate SF11BW125	SNR -	RSSI	Size	Fcnt 0	<b>Type</b> JnAcc	Time 2019-08-09T07:18:23+02:00	Details
24e1641193199962	865402500	SF11BW125	-	-	17	0	JnAcc	2019-08-09T07:18:23+02:00	0
24e1641193199962 24e1641193199962	865402500 865402500	SF11BW125 SF11BW125	- 9.5	-34	17 18	0	JnAcc JnReq	2019-08-09T07:18:23+02:00 2019-08-09T07:18:22+02:00	0
24e1641193199962 24e1641193199962 24e1641193199962	865402500 865402500 865402500	SF11BW125 SF11BW125 SF8BW125	- 9.5 -	- -34 -	17 18 0	0 0 2	JnAcc JnReq DnUnc	2019-08-09T07:18:23+02:00 2019-08-09T07:18:22+02:00 2019-08-09T07:17:16+02:00	0
24e1641193199962 24e1641193199962 24e1641193199962 24e1641193199962 24e1641193199962	865402500 865402500 865402500 865402500	SF11BW125 SF11BW125 SF8BW125 SF8BW125	- 9.5 - 10.8	-34 - -42	17 18 0 26	0 0 2 3	JnAcc JnReq DnUnc UpCnf	2019-08-09T07:18:23+02:00 2019-08-09T07:18:22+02:00 2019-08-09T07:17:16+02:00 2019-08-09T07:17:16+02:00	0
24e1641193199962 24e1641193199962 24e1641193199962 24e1641193199962 24e1641193199962	865402500 865402500 865402500 865402500 865062500	SF11BW125 SF11BW125 SF8BW125 SF8BW125 SF7BW125	- 9.5 - 10.8 -	- -34 - -42 -	17 18 0 26 0	0 0 2 3 1	JnAcc JnReq DnUnc UpCnf DnUnc	2019-08-09T07:18:23+02:00 2019-08-09T07:18:22+02:00 2019-08-09T07:17:16+02:00 2019-08-09T07:17:16+02:00 2019-08-09T07:17:01+02:00	0



Send Data To Device			
Item	Description	Default	
Device EUI	Enter the EUI of the device to receive	Null	
Device EUI	the payload.	INUII	
Tupo	Choose from: "ASCII", "hex", "base64".	ASCII	
Туре	Choose the payload type to enter in the payload Input box.	ASCII	
Payload	Enter the message to be sent to this device.	Null	
Port	Enter the LoRaWAN frame port for packet transmission	Null	

	between device and Network Server.	
Confirmed	After enabled, the end device will receive downlink packet	Disabled
Commed	and should answer "confirmed" to the network server.	Disableu

Table 3-2-2-6 Send Data to Device Parameters

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 3-2-2-7 Packet Parameters

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

Packets Details		×
Dev Addr	068c1b56	
GwEUI	24e124fffe0b7443	
AppEUI	70b3d57ed00007ac1	
DevEUI	3530353083376118	
Immediately	false	
TimeSinceGPSEpoch		
Timestamp	242616788	
Туре	DnUnc	
Adr	true	
AdrAcKReq	false	
Ack	true	
Fcnt		
Fport		
		•

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

Item	Description
Dev Addr	Show the address of the device.
GwEUI	Show the EUI of the gateway.
AppEUI	Show the EUI of the application.
DevEUI	Show the EUI of the device.
	True: Device may transmit an explicit (possibly empty)
Immediately	acknowledgement data message immediately after the reception of a
	data message requiring a confirmation.
TimeSinceGPS Epoch	Show the GPS time.
Timestamp	Show the timestamp of this packet.
Frequency	Show the frequency of this channel.
	Show the type of the packet:
	JnAcc - Join Accept Packet
	JnReq - Join Request Packet
Turne	UpUnc - Uplink Unconfirmed Packet
Туре	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.
Au	False: The end-node has not enabled ADR.
	In order to validate that the network is receiving the uplink messages,
	nodes periodically transmit ADRACKReq message. This is 1 bit long.
AdrAcKReq	True:Network should respond in ADR_ACK_DELAY time to confirm that it
	is receiving the uplink messages
	False: Otherwise
Ack	True: This frame is ACK.
	False: This frame is not ACK.
	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.
MIC	Show the MIC of this packet.MIC is a cryptographic message integrity code, computed over the fields MHDR, FHDR, FPort and the encrypted
	FRMPayload.

Table 3-2-2-8 Packets Details Parameters

# **Related Topic**

Send Data to Device

# 3.3 Network

# 3.3.1 Interface

# 3.3.1.1 Port

The Ethernet 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.

Status	Port WLAN	Cellular Loopback
Packet Forwarder	- Port_1	
Network Server	Enable	
Naturat	Port	eth 0
Network 🔻	Connection Type	Static IP 🗸
Interface	IP Address	192.168.23.66
Firewall	Netmask	255.255.255.0
DHCP	Gateway	192.168.23.1
	MTU	1500
DDNS	Primary DNS Server	8.8.8.8
Link Failover	Secondary DNS Server	114.114.114.114
VPN	Enable NAT	

Figure 3-3-1-1

Port Setting				
Item	Description	Default		
Enable	Enable WAN function	Enable		
Port	The port that is currently set as WAN port.	eth 0		
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP		
MTU	Set the maximum transmission unit.	1500		
Primary DNS Server	Set the primary DNS.	Null		
Secondary DNS Server	Set the secondary DNS.	Null		
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable		

Table 3-3-1-1 Port Parameters

# 1. Static IP Configuration

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

- Port_1			
Enable			
Port	eth 0	]	
Connection Type	Static IP 🗸	•]	
IP Address	192.168.23.66	]	
Netmask	255.255.255.0	]	
Gateway	192.168.23.1	]	
MTU	1500	]	
Primary DNS Server	8.8.8.8	]	
Secondary DNS Server	114.114.114.114	]	
Enable NAT			
Multiple IP Address			
IP Add	Iress	Netmask	Operation

Figure 3-3-1-2

Static IP				
Item	Description	Default		
IP Address	Set the IP address which can access Internet. E.g. 192.168.1.2.	192.168.23.150		
Netmask	Set the Netmask for Ethernet port.	255.255.255.0		
Gateway	Set the gateway's IP address for Ethernet port.	192.168.23.1		
Multiple IP Address	Set the multiple IP addresses for Ethernet port.	Null		

Table 3-3-1-2 Static IP 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.

Enable	
Port	eth 0
Connection Type	DHCP Client V
мти	1500
Jse Peer DNS	
Primary DNS Server	8.8.8.8
Secondary DNS Server	114.114.114.114
Enable NAT	

Figure 3-3-1-3

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

Table 3-3-1-3 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.

Port_1	
Enable	
Port	eth 0
Connection Type	PPPoE 🗸
Username	
Password	
Link Detection Interval(s)	60
Max Retries	0
MTU	1500
Use Peer DNS	
Primary DNS Server	8.8.8.8
Secondary DNS Server	114.114.114
Enable NAT	



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

Table 3-3-1-4 PPOE Parameters

### 3.3.1.2 WLAN

This section explains how to set the related parameters for Wi-Fi network. UG65 supports 802.11 b/g/n, as AP or client mode.

Port	WLAN	Cellular	Loopback	
WLAN	2			
Enable				
Work Mode	9	AP		•
SSID Broa	dcast			
AP Isolatio	n			
Radio Type	•	802.11n	(2.4GHz)	۲
Channel		Auto		•
SSID				
BSSID				
Encryption	Mode	WPA-PS	K/WPA2-PSK	•
Cipher		AES		•
Key		••••••	•••	
Bandwidth		20MHz		•
Max Client	Number	128		
IP Setting				
Protocol		Static IP	ġ.	٣
IP Address				
Netmask		255.255.	255.0	

Figure 3-3-1-5

WLAN			
Enable			
Work Mode	Client	~	Scan
SSID			
BSSID			
Encryption Mode	WPA-PSK/WPA2-PSK	~	
Cipher	Auto	~	
Key			
IP Setting			
Protocol	Static IP	~	
IP Address			
Netmask	255.255.255.0		
Gateway			

Figure 3-3-1-6

WLAN Settings				
Item	Description			
Enable	Enable/disable WLAN.			
Work Mode	Select gateway's work mode. The options are "Client" or "AP".			
	Fill in the MAC address of the access point. Either SSID or BSSID can			
BSSID	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.			
	Select encryption mode. The options are "No Encryption", "WEP			
E	Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" ,			
Encryption Mode	"WPA-PSK/WPA2-PSK", "WPA-Enterprise", "WPA2-Enterprise" and			
	"WPA-Enterprise/WPA2-Enterprise".			
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".			
Кеу	Fill the pre-shared key of WEP/WPA encryption.			
XSupplicant Type	Select from "Peap", "Leap", "TLS" and "TTLS".			
User	Fill the user of WPA/WPA2-Enterprise.			
Anonymous Identity	Fill the anonymous identity of WPA/WPA2-Enterprise.			
Phase2	Fill the phase2 of WPA/WPA2-Enterprise.			
Public Server	The public server certificate used for verifying with			
Certificate	WPA/WPA2-Enterprise access point.			
AP Mode				
AP Mode	When SSID broadcast is disabled, other wireless devices can't not			
AP Mode SSID Broadcast	When SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access			
SSID Broadcast	find the SSID, and users have to enter the SSID manually to access			
	find the SSID, and users have to enter the SSID manually to access to the wireless network.			
SSID Broadcast AP Isolation	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are			
SSID Broadcast	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.			
SSID Broadcast AP Isolation	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".			
SSID Broadcast AP Isolation Radio Type	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g			
SSID Broadcast AP Isolation Radio Type Channel	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> </ul>			
SSID Broadcast AP Isolation Radio Type	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> <li>Fill the pre-shared key of WPA encryption.</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> <li>Fill the pre-shared key of WPA encryption.</li> <li>Select bandwidth. The options are "20MHz" and "40MHz".</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> <li>Fill the pre-shared key of WPA encryption.</li> <li>Select bandwidth. The options are "20MHz" and "40MHz".</li> <li>Set the maximum number of client to access when the gateway is</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> <li>Fill the pre-shared key of WPA encryption.</li> <li>Select bandwidth. The options are "20MHz" and "40MHz".</li> <li>Set the maximum number of client to access when the gateway is</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting	<ul> <li>find the SSID, and users have to enter the SSID manually to access to the wireless network.</li> <li>When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.</li> <li>Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".</li> <li>Select wireless channel. The options are "Auto", "1", "2""11".</li> <li>Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".</li> <li>Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".</li> <li>Fill the pre-shared key of WPA encryption.</li> <li>Select bandwidth. The options are "20MHz" and "40MHz".</li> <li>Set the maximum number of client to access when the gateway is configured as AP.</li> </ul>			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting Protocol	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP. Set the protocol in wireless network.			
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting Protocol IP Address	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP.			

Ursalink_F0C425 Yeastar-VPN Yeastar-VPN Ursalink_F0D908	Channel Auto Auto	Cellular Signal -74dBm	Lo Cipher Auto	BSSID	Security	Frequency	
SSID Ursalink_F0C425 Yeastar-VPN Yeastar-VPN Ursalink_F0D908	Auto				Security	Frequency	
Ursalink_F0C425 Yeastar-VPN Yeastar-VPN Ursalink_F0D908	Auto				Security	Frequency	
Yeastar-VPN Yeastar-VPN Ursalink_F0D908		-74dBm	Auto	24-o1-24-f0-o4-25			
Yeastar-VPN Ursalink_F0D908	Auto			24.61.24.10.04.20	No Encryption	2412MHz	Join Network
Ursalink_F0D908		-76dBm	Auto	48:7a:da:40:83:d1	No Encryption	2462MHz	Join Network
	Auto	-70dBm	Auto	48:7a:da:40:76:91	No Encryption	2412MHz	Join Network
11	Auto	-72dBm	Auto	24:e1:24:f0:d9:08	No Encryption	2462MHz	Join Network
Ursalink_F0C419	Auto	-66dBm	Auto	24:e1:24:f0:c4:19	No Encryption	2412MHz	Join Network
Yeastar-VPN	Auto	-84dBm	Auto	48:7a:da:40:7c:d1	No Encryption	2437MHz	Join Network
Ursalink_F02F77	Auto	-58dBm	Auto	24:e1:24:f0:2f:77	No Encryption	2447MHz	Join Network

#### Table 3-3-1-5 WLAN Parameters

Figure 3-3-1-7

Client Mode-Scan	
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.
	Table 3-3-1-6 WLAN Scan Parameters

# **Related Topic**

Wi-Fi Application Example

## 3.3.1.3 Cellular

This section explains how to set the related parameters for cellular network.

Port	WLAN	Cellular	Loopback	
Cellular Se	etting			
Enable				
Network Ty	pe	Auto	~	-
APN				Ĩ
Username				Ī
Password				Ī
Access Nur	mber			Ĩ
PIN Code				7
Authenticat	ion Type	Auto		-
Roaming				
SMS Cente	r			
				4
	F	igure 3-3-1-8		
Connectio	on Setting			
Enable NA	AT			
Restart W	hen Dial-up failed			
ICMP Ser	ver	8.8.8.8		
Secondary	/ ICMP Server	114.114.114.1	114	
ICMP Dete	ection Max Retries	3		
ICMP Dete	ection Timeout	5	S	
ICMP Dete	ection Interval	15	S	
SMS Sett	ings			
SMS Mod	e	PDU	~	



General Settings				
Item	Description	Default		
Enable	Check the option to enable the corresponding SIM card.	Enable		
Network Type	Select from "Auto", "Auto 3G/4G", "4G Only" and "3G Only".	Auto		

	Auto: connect to the network with the strongest signal	
	automatically.	
	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
ICMP Detection Max Retries	Set max number of retries when ICMP detection fails.	3
ICMP Detection Timeout	Set timeout of ICMP detection.	5
ICMP Detection Interval	Set interval of ICMP detection.	15
SMS Mode	Select SMS mode from "TEXT" and "PDU".	PDU
		1

Table 3-3-1-7 Cellular Parameters

Connection Setting	
Connection Mode	Connect on Demand 🗸
Redial Interval(s)	5
Max Idle Time(s)	60
Triggered by Call	
Triggered by SMS	

Figure 3-3-1-10

Item	Description
Connection Mode	
Connection Mode	Select from "Always Online" and "Connect on Demand".
Redial Interval(s)	Set the time interval between redials. Range: 0-3600.
Max Idle Time(s)	Set the maximum duration of the gateway when current link is under idle status. Range: 10-3600.
Triggered by Call	The gateway will switch from offline mode to cellular network 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 Settings > Phone" to set up phone group.
Triggered by SMS	The gateway will switch from offline mode to cellular network 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 Settings > Phone" to set up SMS group.
SMS Text	Fill in the SMS content for triggering.

Table 3-3-1-8 Cellular Parameters

### **Related Topics**

<u>Cellular Connection Application Example</u> <u>Phone Group</u>

### 3.3.1.4 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	WLAN	Cellular	Loopback		
Loopback	Address				
IP Address		127.0.0.1			
Netmask		255.0.0.0			
Multiple IP	Addresses				
	IP	Address		Netmask	Operation
					Đ
Save					

#### Figure 3-3-1-11

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

Table 3-3-1-9 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

Status	Security	ACL	DMZ	Port Mapping	MAC Binding
LoRaWAN	Website Block	ing by URL Ac	ldress		
Network 🔫	URL Address	[	http://		
Interface	Website Block	ing by Keywo	rd		
Firewall	Keyword	[			×
QoS					æ
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.

Security	ACL	DMZ	Port Mapping	MAC Binding			
ACL Setting							
Default Filter Po	blicy	Accept	~				
Access Contro	ol List						
			Туре	extended	~		
			ID				
			Action	permit	~		
			Protocol	ip	~		
			Source IP				
			Source Wildcard Mask	0.0.0.0			
			Destination IP				
			Destination Wildcard Mask	0.0.0.0			
			Description				
			Save	Cancel			
Interface List							
	Interface		In ACL			Out ACL	Operation
							æ

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	Wildcard mask of destination address.		

Mask			
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.

Security	ACL	DMZ	Port Mapping
DMZ			
Enable			
DMZ Host			
Source Address			



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  $\pm$  to add a new port mapping rules.

Security	ACL	DMZ	Port Mapping	MAC E	Binding		
Port Mapping							
Source I	Р	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0					TCP 🗸		
							Ð

Figure 3-3-2-4

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

Table 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.

Security	ACL	DMZ	Port Mapping	MAC Binding		
MAC Binding	List					
	MAC Address		IP Address		Description	Operation
						<b>H</b>

#### 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 DHCP

The UG65 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.

DHCP Server			
DHCP Server_1			
Enable			
Interface	wlan0	~	
Start Address	192.168.66.100		
End Address	192.168.66.199		
Netmask	255.255.255.0		
Lease Time(Min)	1440		
Primary DNS Server	8.8.8.8		
Secondary DNS Server			
Windows Name Server			
Static IP			
MAC Ad	dress	IP Address	Operation
			Ð

Figure 3-3-3-1

DHCP Server							
Item	Description	Default					
Enable	Enable or disable DHCP server.	Enable					
Interface	Only wlan interface is allowed to distribute IP addresses.	wlan0					
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100					
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199					

Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	114.114.114.11 4
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 3-3-3-1 DHCP Server Parameters

#### 3.3.4 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.

DDNS DDNS Metho	d List									
Name	Interface	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Appe nd IP	Oper ation
	wlan0 🗸	DynDI 🗸								×
										Đ



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 3-3-4-1 DDNS Parameters

#### 3.3.5 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.

# 3.3.5.1 SLA

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

SLA	Track	WAN Failover							
SLA Entry									
ID	Туре	Destination Address	Secondary Destination Address	Data Size	Interval(s )	Timeout( ms)	Packet Loss Count	Start Time	Operation
1	icmp-ech 🖌	114.114.114.1	8.8.8.8	56	15	5000	3	nov 🗸	×
									8

Figure 3-3-5-1

SLA		
ltem	Description	Default
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1
Туре	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo
Destination Address	The detected IP address.	114.114.114.114
Secondary Destination Address	The secondary detected IP address.	8.8.8.8
Data Size	User-defined data size. Range: 0-1000.	56
Interval (s)	User-defined detection interval. Range: 1-608400.	30
Timeout (ms)	User-defined timeout for response to determine ICMP detection failure. Range: 1-300000.	5000
Packet Loss Count	Define packet loss count in each SLA probe. SLA	5

	probe fails when the preset packet loss count is exceeded.	
Start Time	Detection start time; select from "Now" and blank character. Blank character means this SLA	now
	detection doesn't start.	

Table 3-3-5-1 SLA Parameters

#### 3.3.5.2 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	WAN Failover				
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	<b>v</b> 1 <b>v</b>	wlan0 🗸 🗸	0	1	
						•

Figure 3-3-5-2

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 3-3-5-2 Track Parameters

#### 3.3.5.3 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.

SLA	Trac	k _	WAN Fai	lover				
WAN Failo		Backup Int	rerface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track II	D Operation
Cellular		eth 0	<b>~</b>	30	0		1	<ul> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>
								•

Figure 3-3-5-3

WAN Failover						
Parameters	Description	Default				
Main Interface	Select a link interface as the main link.					
Backup Interface	Select a link interface as the backup link.					
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	30				
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.	

Table 3-3-5-3 WAN Failover Parameters

#### 3.3.6 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 UG65 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

#### 3.3.6.1 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.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client
DMVPN Setting	js				
Enable					
Hub Address					
Local IP Addres	S				
GRE HUB IP Ad	Idress				
GRE Local IP A	ddress				
GRE Mask			255.255.255.0	•	
GRE Key					
Negotiation Mod	le		Main	•	
Authentication A	Igorithm		DES	Ŧ	
Encryption Algo	rithm		MD5	٣	
DH Group			MODP768-1	•	
Key					
Local ID Type			Default	Ŧ	
IKE Life Time(s)			10800		
SA Algorithm			DES-MD5	•	
PFS Group			NULL	•	
Life Time(s)			3600		

Figure 3-3-6-1

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

Figuro	3-3-6-2
Figure	3-3-6-2

DMVPN			
Item	Description		
Enable	Enable or disable DMVPN.		
Hub Address	The IP address or domain name of DMVPN Hub.		
Local IP address	DMVPN local tunnel IP address.		
GRE Hub IP Address	GRE Hub tunnel IP address.		
GRE Local IP Address	GRE local tunnel IP address.		
GRE Netmask	GRE local tunnel netmask.		
GRE Key	GRE tunnel key.		
Negotiation Mode	Select from "Main" and "Aggressive".		
Authentication			
Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".		
Encryption Algorithm	Select from "MD5" and "SHA1".		
DH Group	Select from "MODP768_1", "MODP1024_2" and		
рн бібир	"MODP1536_5".		
Кеу	Enter the preshared key.		
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"		
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.		
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",		
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",		
SA Algorithm	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and		
XC	"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 3-3-6-1 DMVPN Parameters

### 3.3.6.2 IPSec

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

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

DMVPN	IPsec	GRE	L2TP	PPTP
IPsec Settings	5			
- IPsec_1				
Enable				
IPsec Gat	teway Address			
IPsec Mo	de	Т	unnel	•
IPsec Pro	tocol	Æ	SP	•
Local Sub	net			
Local Sub	onet Mask			
Local ID 1	Гуре	C	)efault	¥
Remote S	Subnet			
Remote S	Subnet Mask			
Remote II	О Туре	Ē	)e <mark>fault</mark>	•



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 3-3-6-2 IPsec Parameters

IKE Parameter			
IKE Version	IKEv1	•	
Negotiation Mode	Main	T	
Encryption Algorithm	DES	T	
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	T	
Lifetime(s)	3600		
DPD Time Interval(s)	30		
DPD Timeout(s)	<mark>1</mark> 50		
IPsec Advanced			
Enable Compression			
VPN Over IPsec Type	NONE	•	

Figure 3-3-6-4

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

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

Table 3-3-6-3 IPsec Parameters

### 3.3.6.3 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
0	GRE Settings				
	- GRE_1				
	Enable		V		
	Remote IF	Address			
	Local IP A	ddress			
	Local Virtu	ual IP Address			
	Netmask		2	55.255.255.0	
	Peer Virtu	al IP Address			
	Global Tra	ffic Forwarding			
	Remote S	ubnet			
	Remote N	etmask			
	MTU		1	500	
	Key				
	Enable N/	AT			



GRE	
Item	Description
Enable	Check to enable GRE function.

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

Table 3-3-6-4 GRE Parameters

### 3.3.6.4 L2TP

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

DMVPN	IPsec	GRE	L2TP	PPTP
L2TP Settings				
— L2TP_1				
Enable				
Remote IF	Address			
Username	1			
Password				
Authentica	ation	A	uto	•
Global Tra	affic 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 3-3-6-5 L2TP Parameters

•
fffffff
1500
1500
60
0

Figure 3-3-6-7

Advanced Settings		
Item	Description	
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP	
Local IP Audress	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 DDD initialization. User can keep the default ention	
Compression	For PPP initialization. User can keep the default option.	
Protocol Field	For DDD initialization. User can keen the default option	
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	Set the maximum receive unit. Range: 64-1500.	
MTU	Set the maximum transmission unit. Range: 64-1500	
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel	
	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 3-3-6-6 L2TP Parameters

### 3.3.6.5 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 Setting	s			
- PPTP_1				
Enable				
Remote	IP Address			
Usernam	ie			
Passwor	d			
Authentio	cation		Auto	•
Global Ti	raffic Forwarding			
Remote	Subnet			
Remote	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 3-3-6-7 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	

Expert Options			
	Figure 3-3-6-9		
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	For PPP initialization. User can keep the default option.		
Compression			
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	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 3-3-6-8 PPTP Parameters

### 3.3.6.6 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 Clier	nt Settings						
- OpenVPN	_1						
Enable							
Protocol		UDF	•	Ŧ			
Remote IP	Address						
Port		1194					
Interface		tun		•			
Authentica	tion	Non	e	v			
Local Tunr	nel IP						
Remote Tu	innel IP						
Enable NA	т						
Compress	ion	LZC		Ŧ			
Link Detec	tion Interval(s)	60					
Link Detec	tion Timeout(s)	300					
Cipher		Non	e	•			
MTU		1500					
Max Fram	e Size	1500	1				
Verbose L	evel	ERF	OR	•			
Expert Opt	ions						
Local Rou	te						
		Subnet			Subnet Mas	k	Operation
							Ð

Figure 3-3-6-10

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

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

Table 3-3-6-9 OpenVPN Client Parameters

### 3.3.6.7 OpenVPN Server

The UG65 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

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



Local Route			
	Subnet	Netmask	Operation
			Ð
Account			
	Username	Password	Operation
			E

Figure 3-3-6-12

OpenVPN Server		
Item	Description	
Enable	Enable/disable OpenVPN server.	
Protocol	Select from TCP and UDP.	
Port	Fill in listening port number. Range: 1-65535.	
Listoping ID	Enter WAN IP address or LAN IP address. Leaving it blank	
Listening IP	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.
	Set link detection interval time to ensure tunnel connection.
Link Detection Interval	Range: 10-1800.
Cinhan	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",
Cipher	"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 3-3-6-10 OpenVPN Server Parameters

# 3.3.6.8 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	'			Browse	Import Export Delet	e	
Private Ke	У			Browse	Import Export Delet	e	
TA				Browse	Import Export Delet	e	
Preshared	Key			Browse	Import Export Delet	e	
PKCS12				Browse	Import Export Delet	e	

Figure 3-3-6-13

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

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

Table 3-3-6-11 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 3-3-6-14

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 3-3-6-12 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 3-3-6-15

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 3-3-6-13 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, event alarms, etc.

### 3.4.1 General Settings

### 3.4.1.1 General

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

General	System Time	SMTP	Phone	Email	
System					
Hostname		ROUTER			
Web Login Time	ou <mark>t</mark> (s)	1800			
Access Service	e				
	Enable	Sen	vice		Port
		нт	TP	80	)
		HTT	PS	44	43
		TELI	NET	23	3
		SS	θH	22	2
HTTS Certifica	tes				
Certificate	https.crt	Browse	Import Export	Delete	
Key	https.key	Browse	Import Export	Delete	
		Figure 3	8-4-1-1		

General		
Item	Description	Default
System		
Hostname	User-defined gateway name, needs to start with a letter.	URSA

Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	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
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443
TELNET	Users can log in the device locally and remotely via TELNET to access and control it through Web after option is checked.	23
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22
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 Se	ettings			
Current Time		2019-06-12 20:3	4:32 Wed	
Time Zone		8 China (Beijing	j) <b>v</b>	
Sync Type		Sync with Brow	ser 🔻	
Browser Time		2019-06-12 20:3	4:32 Wed	

Figure 3-4-1-2

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

General	System Time	SMTP	Phone	Email
System Time	Settings			
Current Time		2019-06-12 20:33:36	Wed	
Time Zone		8 China (Beijing)	•	
Sync Type		Sync with NTP Serve	ər 🔻	
NTP Server Add	dress	1.cn.pool.ntp.org		
Enable NTP Se	rver			



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.			
Superwith NTD Server	Synchronize time with NTP server so as to achieve time			
Sync with NTP 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.

			Phone	Email
SMTP Client Set	tings			
Enable				
Email Address				
Password				
SMTP Server Add	ress	smtp.exmail.qq.	com	
Port		25		
Enable TLS				

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			Descrip	tion	Operation
	1234567890			test		×
						<b>H</b>
Phone Group	List					
	Grou	JD qu	1			
	Des	cription	test			
	[	List		Select 1234567890	ted	
				1204007000		
			× «			
			<b>▼</b>		-	
			Save	Cancel		
			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 Ti Email List Support@ursalia	ddress	Phone	Email Description		Operation
Email A support@ursali					
support@ursali					
	ık.com		test		
Email Group List			7		× +
	Group ID Description List	1 test 2 2 2 3 2 3 3 4 5 3 2 4 5 4 5 4 5 4 5 4 5 1 5 5 5 6 7 5 7 6 7 7 7 7 7 7 7 7 7 7 7 7	Selected support@ursalink.com	×	

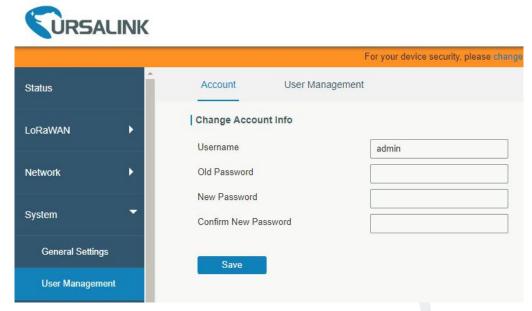
Email		
Item	Description	
Email List		
Email Address	Enter the Email address.	
Description	Description The description of the Email address.	
Email Group List		
Group ID	Set number for email group. Range: 1-100.	
Description	The description of the Email group.	
List	Show the Email address list.	
Selected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

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

Table 3-4-2-2 User Management

### 3.4.3 SNMP

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

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

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

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

### 3.4.3.1 SNMP

The UG65 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	IS			
	Enable				
Network •	Port		161		
Quatam	SNMP Version		SNMPv2		Ŧ
System	Location Inform	nation			
General Settings	Contact Inform	ation			
User Management	Save				
SNMP					



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

Location Information	Fill in the location information.
<b>Contact Information</b>	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	View	Filter	View OID	Operation
All		Included	•	1	×
system		Included	•	1.3.6.1.2.1.1	
					+

### 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 3-4-3-2 MIB View Parameters	

# 3.4.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB Viev	VACM	Тгар	MIB		
SNMP v1 & v2	2 User List					
Comm	unity	Permission	MIB Vi	ew	Network	Operation
private		Read-write	• All	¥	0.0.0.0/0	×
public		Read-only	• none	•	0.0.0.0/0	×



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.

SNMP	MIB View	VACM	Trap	MIB
SNMP Trap				
Enable				
SNMP Version	ı	SNMPv2		T
Server Addres	s			
Port				
Name				

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 UG65.

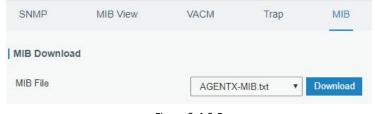


Figure 3-4-3-5

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

3.4.5 Device Management

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

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



DeviceHub	
Item	Description
Status	Show the connection status between the gateway and the DeviceHub.
Disconnected	Click this button to disconnect the gateway from the DeviceHub.

Activation Server Address	IP address or domain of the DeviceHub.
DeviceHub Server	The URL address for the device to connect to the DeviceHub,
Address	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.

Status	Events	Events Sett	ings		
RaWAN	Mark as Re	ad Delete	Mark All	as Read Delete	All Alarms
letwork	F .	Status	Туре	Time	Message
stem	▼	• Go to:	GO		
neral Settings					
ser Management					
<b>AAA</b>					
Device Managemer					
Events					



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	Events Se	ttings			
Events Settin	gs				
Enable					
Phone Group L	ist	1	•	]	
Email Group Li	st	2	•	]	
	Events		Record	Email Email Setting	SMS SMS Setting
	Cellular Up				
	Cellular Down				
	WAN Up				
	WAN Down				
	VPN Up				
	VPN Down		•		

Figure 3-4-6-2

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

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

#### UG65 User Guide

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

#### Figure 3-5-1-2

Traceroute		
Description		
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	Þ	Schedule				
1111-11-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-		Schedule	Frequency	Hour	Minute	Operation
Network						
System	۲	Save				
Maintenance	-					
Tools						
Schedule						

#### Figure 3-5-2-1

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

Table 3-5-2-1 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.

		Download			
LoRaWAN	•	File	Log File	Download	
Network	×	Log			
System	•	View recent(lines)	20	τ	
Maintenance	-	Thu Jul 18 15:01:25 2019 use Thu Jul 18 15:06:26 2019 use Thu Jul 18 15:06:26 2019 use Thu Jul 18 15:06:26 2019 use	r.notice redis[1859]: 10 change r.notice redis[1859]: Backgroun	nd saving started by pid 11683	•
Tools			r.notice redis[1859]: Backgroun	nd saving terminated with success	
Schedule		Thu Jul 18 15:11:27 2019 use Thu Jul 18 15:11:27 2019 use	notice redis[1859]: Backgroun notice redis[15776]: DB saved	id saving started by pid 15776 I on disk	
Log		Thu Jul 18 15:11:27 2019 user.notice redis[1859]: Background saving terminated with success Thu Jul 18 15:16:28 2019 user.notice redis[1859]: 10 changes in 300 seconds. Saving Thu Jul 18 15:16:28 2019 user.notice redis[1859]: Background saving started by pid 19899			
			r.notice redis[19899]: DB saved	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			a) al	]
Port		514		]
Local Log File				
Storage		local	•	]
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		
LIIdDIE	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		

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.

Upgrade			
Upgrade			
Firmware Version	60.0.0.8		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	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.		
	Click "Browse" button to select the new firmware file, and click		
Upgrade Firmware	"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
Maintenance	-	Backup Running-config
Tools		Restore Factory Defaults
Schedule		Reset
Log		
Upgrade		
Backup and Resto	pre	

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

Table 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.

#### UG65 User Guide

LoRaWAN	۲	*	Reboot
Network	۲		Reboot
System	۲		
Maintenance	-		
Tools			
Schedule			
Log			
Upgrade			
Backup and Rest	оге		
Reboot			

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

Python	AppManager Co	nfiguration	Python A	PP	
Python					
AppManager Sta	itus	Uninstalled			
SDK Version					
SDK Path					
Available Storag	е	local	~		
SDK Upload				Browse	Install

# Figure 3-6-1-1

	Figure 3-6-1-1			
Python				
Item	Description			
AppMapagar Status	Show AppManager's running status, like "Uninstalled",			
AppManager Status	"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 Command	Logfile Size(MB)	Uninstall
App Status			
A	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



Description
Select App package and import.
Select App to import configuration.
Select configuration file and import.
Export script file.
Select Python script to be debugged and import.

Table 3-6-1-3 APP Parameters

# **Chapter 4 Application Examples**

# 4.1 Packet Forwarder Configuration

You create multi-destination on this page. So the gateway will forward the data to multiple network server address created and enabled in the list.

The configuration procedures are listed as below.

1. Go to "Packet Forwarder" > "General".

URSALIN	К							
				For your	device security, please	change the defaul	t password	
Status		General	Radios	Advanced	Custom	Traffic		
Packet Forwarder		General Setting	2454	4FFFEF027ED				
Network Server		Gateway ID		124FFFEF027ED				
Network	•	Frequency-Sync		abled	T			
System	×	Multi-Destination						
aintenance			ID	Enable	Туре	Ser	ver Address	Operation
umenumee			0	Enabled	Ursalink		localhost	$\mathscr{Q}$
(pp	•	Save & Apply						•
		Jave & Apply						

2. Click to add a new network server address, displayed as the following picture:

Multi-Destination Configuration						
Item	Description	Default				
Туре	Select "Ursalink" if you need to forward data to the Ursalink Network Server. Select "Semtech" if you need to forward data by Semtech packet forwarder. Select "TTN" if you need to forward data to The Things Network. Select "Loriot" if you need to forward data to Loriot. Select "ChirpStack-Generic" if you need to forward data to ChirpStack with Generic MQTT broker. Note: When the packet forwarder is enabled as Loriot, TTN and ChirpStack-Generic type, data will not be forwarded to other server addresses.	Semtech				
Server Address	Select or enter a server address of the LoRaWAN network server.	ttn.thingsco nnected.ne t				
Port Up	Enter the port of LoRaWAN network server for uploading data. Range: 1-65535.	Ursalink: 1883 Semtech: 1700				

		Loriot: 1780
Port Down	Enter the port of LoRaWAN network server for sending data to your gateway. Range: 1-65535.	Ursalink: 1883 Semtech: 1700 Loriot: 1780
Gateway Key	If the type is "TTN", you need to enter the gateway key for authentication.	Null
User Credentials	When you select user credentials for authentication, you need to enter the username and password required for authentication.	Null
TLS Authentication	Select from "CA signed server certificate" and "Self signed certificates". CA signed server certificate: Verify with the certificate issued by Certificate Authority (CA) that pre-loaded on device. Self signed certificates: In this mode, users have to upload the custom certificate and secret key for verification.	Self signed certificates

# 4.2 Application Configuration

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

The procedures are listed as below.

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

General	Applications	Profiles	Device	Packets	
Applications					
Name		Smoke-sensor-app			
Description	1	a application for smoke se	ensor		
Payload Codec		None	•		
Data Transmissio	n				
	Тур	e		Operation	
				•	
Save	Cancel				

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

3. Click to add a data transmission type of HTTP or HTTPS:

Step 1: select HTTP or HTTPS as transmission protocol.

Туре	HTTP	¥
------	------	---

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

HTTP Header				
	Header Name	Header Value	Operation	

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: 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.

Data Type	URL
Uplink data	
Join notification	
ACK notification	
Error notification	

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

Step 1: select the transmission protocol as MQTT.

Туре		MQTT	Ŧ
Step 2: Fill in general settin	igs.		
General			
Broker Addres	ss		
Broker Port			
Client ID			
Connection Ti	meout/s	30	
Keep Alive Int	terval/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		
Mode	Self signed certificates	
CA File	Browse	nport Delete
Client Certificate File	Browse	nport Delete
Client Key File	Browse	mport 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.

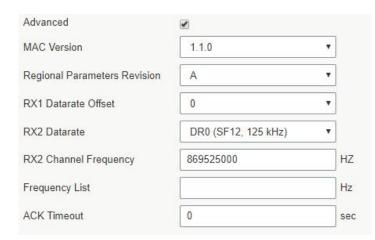
Торіс			
Data Type	topic		
Uplink data		QoS 0	v
Join notification		QoS 0	•
ACK notification		QoS 0	•
Error notification		QoS 0	•

# 4.3 Device Profiles Configuration

Name	device_pro	
Max TXPower	0	
Join Type	OTAA	•
Class Type	Class C	
Advanced		
MAC Version	1.0.2	•
Regional Parameters Revision	В	,
ACK Timeout	0	

Device Profiles Settings			
Item	Description	Default	
Name	Enter the Name of the application profile.	Null	
	E.g. Smoker-sensor-app.	NUII	

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 accept procedure.	ΟΤΑΑ
Class Type	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 transmission. 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.	A



Device Profile Advanced Settings						
ltem	Description	Default				
MAC Version	Choose the version of the LoRaWAN supported by the end-device.	1.0.2				
Regional Parameter Revision	Revision of the Regional Parameters document supported by the end-device.	В				
RX1 Datarate Offset	Enter the offset which used for calculate the RX1 data-rate, based on the uplink data-rate. The range is based on what is specified in the LoRaWAN regional parameters document.	The default offset is based on what is specified in the LoRaWAN regional parameters document.				
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window. The range is based on what is specified in the LoRaWAN regional parameters document.	The default offset is based on what is specified in the LoRaWAN regional parameters document.				
RX2 Channel Frequency	Enter the RX2 channel frequency which used for the RX2 receive-window. The range is based on what is specified in the LoRaWAN regional parameters document.	Null				
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN regional parameters document.	Null				
ACK Timeout	Enter the time for confirmed downlink transmissions. Only applicable to class C.	5				

96

# 4.4 Device Configuration

Go to "Network Server" > "Device".

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

Device		
General		
Device Name	asd	
Description	s	
Device EUI	3530353083376118	
Device-Profile	ninii	•
Application	AS923	Ŧ
Frame-counter Validation	2	

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				

Device Name	UC11-N1-EU868					
Description	Smart environment monitoring					
Device EUI	24e1612292182726					
Device-Profile	ClassA-OTAA	•				
Application	cloud	۲				
Modbus RTU Data Transmission	Modbus RTU to TCP	•				
Fport						
TCP Port						
Frame-counter Validation						



ltem	Description	Default				
Device Name	Name Enter the name of this device.					
Description	Enter the description of this device.	Null				
Device EUI	Enter the EUI of this device.	Null				
Device-Profile	Choose the device profile.	Null				
Application	Choose the application profile.	Null				
Modbus RTU Data Transmission	<ul> <li>Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over TCP".</li> <li>-Disable: This feature is not enabled.</li> <li>-Modbus RTU to TCP: With the this function enabled, you can connect UC11-N1 or UC1152 to TCP networks while converting Modbus message to Modbus TCP Protocol.</li> <li>-Modbus RTU over TCP: With the this function enabled, you can connect UC11-N1 or UC1152 to TCP networks without actually changing any of the bytes in the Modbus message.</li> </ul>	Disable				
Fport	Enter the LoRaWAN frame port for transparent transmission between UC11-N1 and UG65. Range: 2-84, 86-223. Note: this value must be the same as the UC11-N1/UC1152's Fport.	Null				
TCP Port	Enter the TCP port for data transmission between the					
Frame-Counter Validation If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.						

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

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

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

Device Configuration-Activate Device-OTAA						
Item	Description	Default				
Application Key	Enter the application key. Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key.	Null				
Device Address	Show the device address when the device has been activated. The device address identifies the end-device within the current network. It will be cleared when the node has not been activated yet or device has been inactive for a long time.	Null				
Network Session Key	Show the network session key of the device when the device has been activated. The network session key specific for the end-device. It is used by the end-device to calculate 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	Null				

	counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	
	The number of data frames which received by the end-device downlink from the network server. It will be	
Downlink Frame-counter	-counter 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.	

### 4.5 Send Data to Device

Go to "Network Server" > "Packets".

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

1122612191	868100000	SF7BW125	17	: 24	17	0	JnAcc	2019-08-06T09:22:29+08:00	0
112261219	868100000	SF7BW125	9.5	-77	18	0	JnReq	2019-08-06T09:22:29+08:00	0
Step 2: Fill t	hese input bo	DX.							
Send Data To De	evice								
De	vice EUI	Туре				Payload		Fport	Confirmed
1122612191	3	ASCII	•	1	5			15	۲
Step 3: Clicl	k "Send".								
		Sen	d		sen	d succ	ess		

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

Note: p	lease	check	the	"confirme	d" .
---------	-------	-------	-----	-----------	------

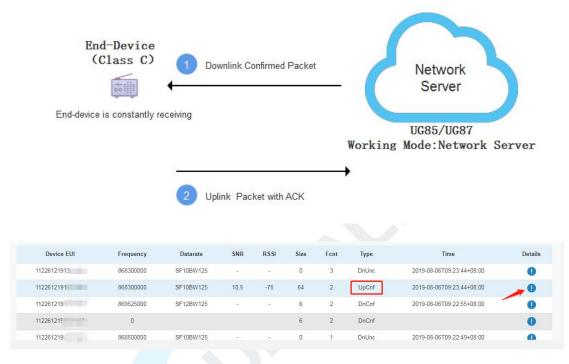
Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII	15	15	

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

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

11226121912	0				6	2	DnCnf	9
his is the data	packet ha	s been del	ivered	l succ	essfu	lly.		
1122612191311123	869525000	SF12BW125	1.00	~	6	2	DnCnf	2019-08-06T09:22:55+08:00 Success ()
1122612191311123	0				6	2	DnCnf	Pending 🕕

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



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

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

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

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

11226121912 0 6 2	DnCnf ()
-------------------	----------

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

Device EUI         Frequency         Datarate         SNR         RSSI         Size         Fcnt         Type         Time         Details           1122612191311123         868300000         \$F108W125         -         -         0         19         Duvice         2019-08-06T09.49.38+08.00         0         5         Stow the size of packet.         Fcnt         Stow the size of packet.         Fcnt         Show the size of packet.         Jacket.	twork Server										Show the signal-noise ratio.
End-Device (Class A)       12       74       64       19       Update (Loc)       219:06:0719 4:33:46:00       0       0       10       Disk       219:06:0719 4:33:46:00       <	Clear								Search	Q	Show the received signal stren
Internet initial       6 6 0 0       19       Dubre       2019 48 64709 49 38-06 0       0         Internet initial       6 6 0 0       10       Dubre       2019 48 64709 49 38-06 0       0         Internet initial       6 6 0 0       10       Dubre       2019 48 64709 49 38-06 0       0         Internet initial       6 0 0       0       Dubre       2019 48 64709 49 38-06 0       0         Internet initial       6 0 0       0       Dubre       2019 48 64709 49 38-06 0       0       0         Internet initial       6 0 0       0       Dubre       2019 48 64709 48 34-06 0       Dubre       2019 48 64709 48 34-06 0       Dubre	Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details	
Notice	1122612191311123	868300000	SF10BW125	(2)	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0	
112212191311122       86830000       SF108W125       1       76       64       21       Upcm       201948-06719-94.84:00       0         11221512191311123       86810000       SF108W125       -       -       6       18       Direct       201948-06719-94.84:00       <	1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0	Show the frame counter.
High 1123 8 8610000 SF108W125 0 0 0 17 0 0 17 0 0 16 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	0	
1122812191311123       0       6       20194040109 40.4340.00       0         1122812191311123       0       6       10       Direct       Pending       0         1122812191311123       0       5       10       Direct       Pending       0       ACK response from relevék requested         1122812191311123       86800000       5F10BW125       -       0       11       Dufect       20194040109.47.38+08.00       0         1122812191311123       868100000       5F10BW125       -       0       16       Dufect       20194040109.47.38+08.00       0       0         112261219131123       868100000       5F10BW125       11.2       -74       64       18       Upcdt       20194040109.46.34+08.00       0       0         112261219131123       868100000       5F10BW125       11.2       -74       64       18       Upcdt       20194040109.46.34+08.00       0 <td>1122612191311123</td> <td>868100000</td> <td>SF10BW125</td> <td>-</td> <td>5</td> <td>6</td> <td>18</td> <td>DnCnf</td> <td>2019-08-06T09:48:43+08:00</td> <td>Success</td> <td>JnAcc - Join Accept Packet JnReq - Join Request Packet</td>	1122612191311123	868100000	SF10BW125	-	5	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success	JnAcc - Join Accept Packet JnReq - Join Request Packet
It22812191311123       0       6       18       Deterf       Pending       0       17       ACK response from network         I122812191311123       68800000       \$F10BW125       -       0       17       Dutke       20194846109473.39:08:00       0	1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0	Packet
1122812191311123       66850000       SF108W125       -       -       0       17       Dulne       2019-86-86709 47.38+08.00       0         1122612191311123       668100000       SF108W125       -       0       16       Dulne       2019-86-86709 47.38+08.00       0         1122612191311123       668100000       SF108W125       -       0       16       Dulne       2019-08-06709 47.38+08.00       0       0         1122612191311123       668100000       SF108W125       11.2       -74       64       18       UpCord       2019-08-06709 46.38+08.00       0       0         Method Servers         Control formed Packet         Method Servers         Method Servers         Method Servers         Method Server	1122612191311123	0				6	18	DnCnf	Pending	0	
1122612191311123       86650000       \$F108W125       -       -       0       16       DnUnc       2019-08-06109 46:38-08:00       0       Dnucc       Dnucc       2019-08-06109 46:37-08:00       0       Dnucc       Dnucc       Dnucc       Dnucc       2019-08-06109 46:37-08:00       0       Dnucc	1122612191311123	868500000	SF10BW125	-	-	0	17	DnUnc	2019-08-06T09:47:38+08:00	0	DnUnc - Downlink Unconfirmed
1122612191311123       86810000       SF10BW125       -       0       16       Dulue       2019-08-06709.46.38+08.00       Image: Constraint of the constraint of	1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0	DnCnf - Downlink Confirmed
End-Device (Class A) (Downlink Confirmed Packet (Pending) Network Server communicates with end-device (downlink) during predetermined response windows.	1122612191311123	868100000	SF10BW125	12	2	0	16	DnUnc	2019-08-06T09:46:38+08:00	0	
End-Device (Class A) (1) Downlink Confirmed Packet (Pending) Network Server communicates with end-device (downlink) during predetermined response windows. (2) Send uplink packet and open the Receive Window to reveive data. (3) Downlink Confirmed Packet	1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0	
(downlink) during predetermined response windows. 2 Send uplink packet and open the Receive Window to reveive data. 3 Downlink Confirmed Packet											
	2.25	Class	100 E				nfirme	ed Packet	_ {		Sector Sector

Clear								Search	Q
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	ceived 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	•
1122612191311123	0				6	18	DnCnf		0
1122612191311123	868500000	SF10BW125	-	-	0	17	DnUnc	2019-08-06T09:47:38+08:00	0
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0
1122612191311123	868100000	SF10BW125	2	12	0	16	DnUnc	2019-08-06T09:46:38+08:00	0
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0

### **Related Topic**

Packets

# 4.6 Restore Factory Defaults

# 4.6.1 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.

Stat	us	
LoR	awan	Þ
Netw	vork	×
Syst	em	
Indu	istrial	Þ
Mair	ntenance	-
Ţ	Tools	
:	Schedule	
I	Log	
l	Upgrade	
I	Backup and Restore	

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

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

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

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



Related Topic Restore Factory Defaults

### 4.6.2 Via Hardware

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

STATUS LED	Action
Blinking	Press and hold the reset button for more than 5 seconds.
Static Green → Rapidly Blinking	Release the button and wait.
$Off \rightarrow Blinking$	The gateway is now reset to factory defaults.

# 4.7 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.

Network •	Upgrade
System 🕨	Upgrade Firmware Version 60.0.0.11
Maintenance 👻	Reset Configuration to Factory Default
Tools	Upgrade Firmware Browse Upgrade
Schedule	
Log	
Upgrade	
Backup and Restore	
Reboot	
	Please keep the power on during upgrade.

# **Related Topic**

### <u>Upgrade</u>

# 4.8 Cellular Connection

# Example

We are about to take an example of inserting a SIM card into SIM slot of the UG65 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. Choose relevant network type. "Auto", "Auto 3G/4G", "4G Only", "3G Only" are optional.

Port	WLAN	Cellular	Loopback
Cellular S	etting		
Enable			
Network Ty	/pe	Auto	~
APN			
Username			
Password			
Access Nu	mber		
PIN Code			
Authentica	tion Type	Auto	~
Roaming			
SMS Cente	er		
Connectio	n Setting		
Enable NA	т		

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

3. 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', SIM has dialed up successfully.

Overview	Packet Forward	Cellular	Network	WLAN
Modem				
Status		Ready		
Model		EC25		
Version		EC25ECGAR06A07N	M1G	
Signal Level		23asu (-67dBm)		
Register Status		Registered (Home ne	etwork)	
IMEI		860425047368939		
IMSI		460019425301842		
ICCID		89860117838009934	120	
ISP		CHN-UNICOM		
Network Type		LTE		
PLMN ID				
LAC		5922		
Cell ID		340db83		
Network				
Status		Connected		
IP Address		10.132.132.59		
Netmask		255.255.255.240		
Gateway		10.132.132.60		

4. 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 UG65.

# **Related Topic**

Cellular Setting Cellular Status

# 4.9 Wi-Fi Application Example

### 4.9.1 AP Mode

# **Application Example**

Configure UG65 as AP to allow connection from users or devices.

# **Configuration Steps**

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

Port	WLAN	Cellular	Loopback	
WLAN				
Enable				
Work Mode	e.	AP		
SSID Broad	dcast			
AP Isolation	ı			
Radio Type		802.11n(2.4GHz)		
Channel		Auto		
SSID		Ursalink_F0C434		
BSSID		24:e1:24:f0:c4:34		
Encryption	Mode	WPA-PSI	K/WPA2-PSK 🗸	
Cipher		Auto		
Key		•••••		
Bandwidth		20MHz	~	
Max Client	Number	128		

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

2. Use a smart phone to connect by SSID "Ursalink\_F0C434". Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List
WLAN Status						
Wireless Status	Enabled					
MAC Address	24:e1:24:	f0:c4:34				
Interface Type	AP					
SSID	Ursalink_I	F0C434				
Channel	Auto					
Encryption Type	WPA-PSK	WPA2-PSK				
Cipher	Auto					
Status	Up					
IP Address	<mark>192.168</mark> .1	.1				
Netmask	255.255.2	55.0				
Connection Duration	0 days, 01	1:00:11				

# 4.9.2 Client Mode

### **Application Example**

Configure UG65 as Wi-Fi client to connect to an access point to have Internet access.

### **Configuration Steps**

1. Go to "Network > Interface > WLAN" and click "Scan" to search for WiFi access point.

Port	WLAN		Cellular	Loo	opback			
GoBack								
SSID	- 0	Channel	Signal	Cipher	BSSID	Security	Frequency	
Ursalink_F0DC	CAF	Auto	-68dBm	Auto	24:e1:24:f0:dc:af	No Encryption	2437MHz	Join Network
Ursalink_F0C4	422	Auto	-6 <mark>4</mark> dBm	Auto	24:e1:24:f0:c4:22	No Encryption	2437MHz	Join Network
Ursalink_F0DE	E8C	Auto	-66dBm	Auto	24:e1:24:f0:de:8c	No Encryption	2462MHz	Join Network

2. Select one access point and click "Join Network", then type the password of the access point.

Port	WLAN	Cellular	Loopback	
WLAN				
Enable				
Work Mode		Client	~	Scan
SSID		Ursalink_T	Гес	
BSSID		24:e1:24:f	0:2c:4b	
Encryption	Mode	WPA-PSk	K/WPA2-PSK 🗸	
Cipher		AES	~	
Key		•••••		
IP Setting				
Protocol		DHCP Cli	ient 🗸	

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

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

Overview	Packet Forward	Cellular	Network	WLAN
WLAN Status				
Wireless Status	Enabled			
MAC Address	24:e1:24:	f0:c4:34		
Interface Type	Client			
SSID	Ursalink_	Tec		
Channel	Auto			
Encryption Type	WPA-PSK	WPA2-PSK		
Cipher	AES			
Status	Connecte	d		
IP Address	192.168.2	50.146		
Netmask	255.255.2	55.0		
Connection Duration	n 0 days, 00	):00:05		

# **Related Topic**

WLAN Setting

WLAN Status

[END]