# Semi-industrial LoRaWAN<sup>®</sup> Gateway UG65

User Guide



# Preface

Thanks for choosing Milesight UG65 LoRaWAN<sup>®</sup> gateway. UG65 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 LoRaWAN<sup>®</sup> 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

## ©2011-2023 Xiamen Milesight IoT 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 Milesight lot Co., Ltd.

# **Related Documents**

Document	Description
UG65 Datasheet	Datasheet for UG65 LoRaWAN® gateway.
UG65 Quick Start Guide	Quick Installation Guide for UG65 LoRaWAN® gateway.

# **Declaration of Conformity**

UG65 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.





# **Revision History**

Date	Doc Version	Description
Aug. 31, 2020	V1.0	Initial version
Dec. 10, 2020	V2.0	Layout replace
		1. Support LoRaWAN <sup>®</sup> Class B
		2. Add Node-RED feature
Apr. 30, 2021	V2.1	3. Add Noise-Analyzer feature
		4. Add Multicast Group feature
		5. Add application examples
		1. Support Yeastar Workplace platform integration
Aug. 24, 2021	V2.2	2. Delete Package Forward status page
		3. Phone & Email webpage update
		1. Add AS923-3&AS923-4
Dec. 15, 2021	V2.3	2. Change network server channel mask box to channel
		3. Add device channel setting in profile
		1. Add batch backup
Eab 19 2022	V2.4	2. Log in webpage update
Feb. 18, 2022	٧2.4	3. Change default antenna type to external antenna
		4. Adjust time of Class C ACK timeout
		1. Support VLAN Trunk client
Jun. 1, 2022	V2.5	2. Add System Name in SNMP
		3. Add Use L2TP Peer DNS option
		1. Add BACnet Server feature
Dec.26, 2022	V2.6	2. Add Payload Codec feature
Dec.20, 2022	v 2.0	3. Add Reset and all flows export feature on Node-RED
		4. Add data retransmission feature on Packet Forward

# Contents

Chapter 1 Product Introduction	
1.1 Overview	7
1.2 Advantages	
1.3 Specifications	8
1.4 Dimensions (mm)	
Chapter 2 Access to Web GUI	11
2.1 Wireless Access	11
2.2 Wired Access	
Chapter 3 Web Configuration	
3.1 Status	
3.1.1 Overview	
3.1.2 Cellular	
3.1.3 Network	
3.1.4 WLAN	-
3.1.5 VPN	
3.1.6 Host List	
3.2 LoRaWAN	
3.2.1 Packet Forwarder	
3.2.1.1 General	
3.2.1.2 Radios	
3.2.1.3 Noise Analyzer	
3.2.1.4 Advanced	
3.2.1.5 Custom	
3.2.1.6 Traffic	
3.2.2 Network Server	
3.2.2.1 General	
3.2.2.2 Application	
3.2.2.3 Payload Codec	
3.2.2.4 Profiles	
3.2.2.5 Device	
3.2.2.6 Multicast Groups	
3.2.2.7 Gateway Fleet	
3.2.2.8 Packets	
3.3 Protocol Integration	
3.3.1 BACnet Server	
3.3.1.1 Server	
3.3.1.2 BACnet Object	
3.4 Network	
3.4.1 Interface	
3.4.1.1 Port	
3.4.1.2 WLAN	52

	3.4.1.3 Cellular	55
	3.4.1.4 Loopback	58
	3.4.1.5 VLAN Trunk	58
3.4.	2 Firewall	59
	3.4.2.1 Security	59
	3.4.2.2 ACL	59
	3.4.2.3 DMZ	61
	3.4.2.4 Port Mapping	61
	3.4.2.5 MAC Binding	62
	3 DHCP	
	4 DDNS	
3.4.	5 Link Failover	
	3.4.5.1 SLA	65
	3.4.5.2 Track	
	3.4.5.3 WAN Failover	
3.4.	6 VPN	68
	3.4.6.1 DMVPN	68
	3.4.6.2 IPSec	
	3.4.6.3 GRE	72
	3.4.6.4 L2TP	73
	3.4.6.5 PPTP	
	3.4.6.6 OpenVPN Client	77
	3.4.6.7 OpenVPN Server	78
	3.4.6.8 Certifications	
•	em	
3.5.	1 General Settings	
	3.5.1.1 General	82
	3.5.1.2 System Time	83
	3.5.1.3 SMTP	85
	3.5.1.4 Phone	.85
	3.5.1.5 Email	86
3.5.	2 User Management	87
	3.5.2.1 Account	87
	3.5.2.2 User Management	87
3.5.	3 SNMP	88
	3.5.3.1 SNMP	88
	3.5.3.2 MIB View	89
	3.5.3.3 VACM	.89
	3.5.3.4 Trap	90
	3.5.3.5 MIB	91
3.5.	4 Device Management	91
3.5.	5 Events	92
	3.5.5.1 Events	92
	3.5.5.2 Events Settings	93

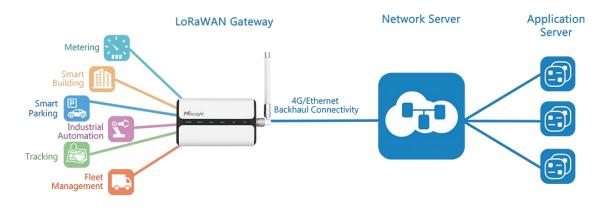
3.6 Maintenance	95
3.6.1 Tools	95
3.6.1.1 Ping	95
3.6.1.2 Traceroute	95
3.6.1.3 Qxdmlog	96
3.6.2 Schedule	96
3.6.3 Log	96
3.6.3.1 System Log	
3.6.3.2 Log Settings	97
3.6.4 Upgrade	98
3.6.5 Backup and Restore	
3.6.6 Reboot	99
3.7 APP	100
3.7.1 Python	
3.7.1.1 Python	100
3.7.1.2 App Manager Configuration	101
3.7.1.3 Python App	102
3.7.2 Node-RED	103
3.7.2.1 Node-RED	
Chapter 4 Application Examples	105
4.1 Restore Factory Defaults	105
4.1.1 Via Web Interface	
4.1.2 Via Hardware	
4.2 Firmware Upgrade	106
4.3 Ethernet Connection	
4.4 Cellular Connection	108
4.5 Wi-Fi Application Example	109
4.5.1 AP Mode	109
4.5.2 Client Mode	111
4.6 Packet Forwarder Configuration	112
4.7 Connect to Milesight IoT Cloud	114
4.8 Application Configuration	115
4.9 Device Configuration	118
4.10 Send Data to Device	119
4.11 Node-RED	121
4.11.1 Start the Node-RED	
4.11.2 Send Data by Email	122

## **Chapter 1 Product Introduction**

## 1.1 Overview

UG65 is a robust 8-channel indoor LoRaWAN<sup>®</sup> 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 15 km and can cover about 2 km 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, but also has integrated mainstream network servers (such as TTI, ChirpStack, etc.) and built-in network server and Milesight IoT 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
- 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**

- Milesight 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 1.5 GHz 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

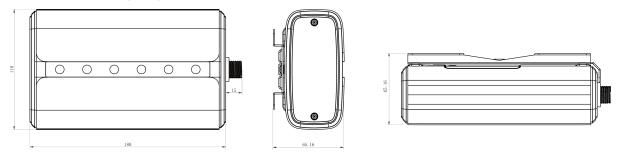
Hardware System	
CPU	Quad-core 1.5GHz, 64-bit ARM Cortex-A53
Memory	8 GB eMMC Flash, 512 MB DDR4 RAM
LoRaWAN	
A	Fully Integrated and Internal Antenna
Antenna	(Optional: $1 \times 50 \Omega$ N-Female External Connector)
Channel	8
	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923-1&2&3&
Frequency Band	4
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class B/Class C and V1.0.2 Class A/Class B/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, 2.4 GHz
	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 (	Optional)
Antenna	Internal Antenna
SIM Slots	1
Software	
Network	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS,
Protocols	DNS, SNTP, Telnet, SSH, MQTT, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Firewall	ACL/DMZ/Port Mapping/MAC Binding
Management	Web, CLI, SMS, On-demand dial up, DeviceHub, Milesight IoT Cloud
Management	Yeastar Workplace Platform
Арр	Python SDK, Node-RED
Power Supply and C	Consumption
	1. DC Jack Connector for 9-24 VDC power supply
Power Supply	2. 1 × 802.3 af PoE input
Consumption	Typical 2.9W, Max 4.2W
Physical Characteris	
Ingress Protection	IP65
Dimensions	180 x 110 x 56.5 mm
Mounting	Desktop, Wall or Pole Mounting
<b>Others</b> Reset Button	1 × RST

LED Indicators	1 × POWER, 1 × STATUS, 1 × LoRa, 1 × Wi-Fi, 1 × LTE, 1 × ETH
Built-in	Watchdog, RTC, Timer
Environmental	
Operating	-40°C to +70°C (-40°F to +158°F)
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. Username: **admin** Password: **password** 

## 2.1 Wireless Access

Δ

1. Enable Wireless Network Connection on your computer and search for access point "Gateway\_\*\*\*\*\*\*" to connect it.

2. Open a Web browser on your PC (Chrome is recommended) and type in the IP address

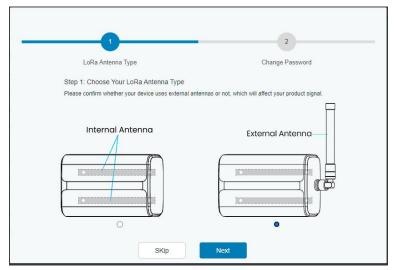
**192.168.1.1** to access the web GUI.

3. Enter the username and password, click "Login".

	Languaga English •
Logn	

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

4. After logging the web GUI, follow the guide to complete the basic configurations. It's suggested that you change the password for the sake of security.





5. You can view system information and perform configuration of the gateway.

		For	your device security.	please change the d	efault password			
Status	Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List	Help
Status								Model
Packet Forwarder	System Inform	ation						Show the model name of router.
	Model		UG65-L00E-470M-	EA				Region Show the Region of router.
Network Server	Region		CN470					Serial Number
Network 🕨	Serial Number		6221A4950760					Show the serial number of router.
	Firmware Versio	n	60.0.3000.26					Firmware Version
System 🕨	Hardware Versio	n	V1.1					Show the current firmware version of router.
	Local Time		2020-12-10 17:57:2	4 Thursday				Hardware Version
Maintenance	Uptime		03:04:04					Show the current hardware version of router.
	CPU Load		6%					Local Time
	RAM (Capacity//	Available)	512MB/65MB(12.7	%)				Show the current local time of system.
	eMMC (Capacity	/Available)	2.0G/1.8G(90.80%)	j				Uptime

## 2.2 Wired Access

Connect PC to UG65 ETH port directly or through PoE injector to access the web GUI of gateway. The following steps are based on Windows 10 system for your reference.

1. Go to "Control Panel"  $\rightarrow$  "Network and Internet"  $\rightarrow$  "Network and Sharing Center", then click "Ethernet" (May have different names).

→ × ↑ 👺 « Network	and Internet > Network and Sharing Center	✓ ♂ Search Control Panel
Control Panel Home	View your basic network informatic	on and set up connections
Change adapter settings Change advanced sharing settings	Yeastar5G Private network	Access type: Internet HomeGroup: Ready to create Connections: MW-Fi (Yeastar5G)
	ldentifying	Access type: No network access Connections: Ethernet
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN Troubleshoot problems Diagnose and repair network problem	
See also		
HomeGroup		
Internet Options		
Windows Firewall		

2. Go to "Properties"  $\rightarrow$  "Internet Protocol Version 4(TCP/IPv4) "and select "Use the following IP address", then assign a static IP manually within the same subnet of the gateway.

ternet Protocol Version 4 (TCI	P/IPv4) Properties
General	
	d automatically if your network supports need to ask your network administrator
O Obtain an IP address auto	omatically
• Use the following IP addre	ess:
IP address:	192 . 168 . 23 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 23 . 150
Obtain DNS server addres	s automatically
• Use the following DNS ser	ver addresses:
Preferred DNS server:	8.8.8.8
Alternative DNS server:	
Validate settings upon ex	it Advanced

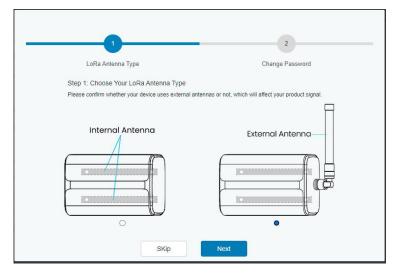
3. Open a Web browser on your PC (Chrome is recommended) and type in the IP address **192.168.23.150** to access the web GUI.

4. Enter the username and password, click "Login".

	Language English 🔍 🗸
Milesight - ustanting -	- 3 <sup>2</sup>

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

5. After logging the web GUI, follow the guide to complete the basic configurations. It's suggested that you change the password for the sake of security.



6. After guide complete, you can view system information and perform configuration of the gateway.

Milesigl	ht								💄 admin 🔁
			Fo	r your device security	, please change the d	lefault password			
Status		Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List	Help
oluluo									Model
Packet Forwarder		System Information	ation						Show the model name of router.
		Model		UG65-L00E-470M-	EA				Region
Network Server		Region		CN470					Show the Region of router.
									Serial Number
Network		Serial Number		6221A4950760					Show the serial number of router.
		Firmware Version	n	60.0.3000.26					Firmware Version
System	•	Hardware Versio	n	V1.1					Show the current firmware version of router.
		Local Time		2020-12-10 17:57:2	24 Thursday				Hardware Version
Maintenance	•	Uptime		03:04:04					Show the current hardware version of router.
APP		CPU Load		6%					Local Time
		RAM (Capacity/A	Available)	512MB/65MB(12.7	%)				Show the current local time of system.
		eMMC (Capacity	/Available)	2.0G/1.8G(90.80%	)				Uptime
							Manual R	efresh 🗸 Refresh	Show the information on how long the router has been running.

# **Chapter 3 Web Configuration**

## 3.1 Status

## 3.1.1 Overview

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

System Information	
Model	UG65-L00E-868M-EA
Region	EU868
Serial Number	6221A4968194
Firmware Version	60.0.0.34
Hardware Version	V1.1
Local Time	2021-05-07 15:14:59 Friday
Uptime	31days,04:55:54
CPU Load	4%
RAM (Capacity/Available)	512MB/93MB(18.16%)
eMMC (Capacity/Available)	3.0G/2.7G(89.95%)

Figure 3-1-1-1

System Information			
Item	Description		
Model	Show the model name of gateway.		
Region	Show the LoRaWAN <sup>®</sup> frequency region 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		

Table 3-1-1-1 System Information

## **3.1.2 Cellular**

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

#### Modem

Status	Ready
Model	EC25
Version	EC25ECGAR06A07M1G
Signal Level	26asu (-61dBm)
Register Status	Registered (Home network)
IMEI	860425047368939
IMSI	460019425301842
ICCID	89860117838009934120
ISP	CHN-UNICOM
Network Type	LTE
PLMN ID	
LAC	5922
Cell ID	340db80
	F

Figure 3-1-2-1

Modem Information			
ltem	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 3-1-2-1 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 3-1-2-2

Network Status			
Item	Description		
Status	Show the connection status of cellular network.		
IP Address	Show the IP address of cellular network.		
Netmask	Show the netmask of cellular network.		
Gateway	Show the gateway of cellular network.		
DNS	Show the DNS of cellular network.		
<b>Connection Duration</b>	Show information on how long the cellular network has been connected.		
Table 3-1-2-2 Network Status			

## 3.1.3 Network

On this page you can check the Ethernet port status of the gateway.

Overview	С	ellular	Network	WLAN	VPN	Host List		
WAN								
Port	Status	Туре	IP Address	Netmask		Gateway	DNS	Duration
eth 0	up	Static	192.168.22.32	255.255.254.0	1 8	192.168.22.1	8.8.8.8	10h 52m 03s

Figure 3-1-3-1

Network	
ltem	Description
Port	Show the name of the Ethernet port.
	Show the status of the Ethernet port. "Up" refers to a status that WAN
Status	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 the Ethernet port.
IP Address	Show the IP address of the Ethernet port.
Netmask	Show the netmask of the Ethernet port.

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

Table 3-1-3-1 WAN Status

## 3.1.4 WLAN

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

Overview	Cellular	Network	WLAN	VPN	Host List
WLAN Status					
Wireless Status		Enabled			
MAC Address		24:e1:24:f1:22:58			
Interface Type		AP			
SSID		Gateway_F12258			
Channel		Auto			
Encryption Type		No Encryption			
Status		Up			
IP Address		192.168.1.1			
Netmask		255.255.255.0			
Connection Duratio	n	0 days, 10:52:23			

Figure 3-1-4-1

WLAN Status				
ltem	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.			
<b>Connection Duration</b>	Show information on how long the Wi-Fi network has been connected.			

Table 3-1-4-1 WLAN Status

Associated Stations			
IP Address	MAC Address	Connection Duration	
	Figure 3-1-4-2		
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 3-1-4-2 WLAN Status

## 3.1.5 VPN

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

Overview	Cellular	Network	WLAN VPN	Host List
PPTP Tunnel				
	Name	Status	Local IP	Remote IP
	pptp_1	Disconnected	-	
	pptp_2	Disconnected	-	
	pptp_3	Disconnected	50	*
L2TP Tunnel				
	Name	Status	Local IP	Remote IP
	l2tp_1	Disconnected	-	
	l2tp_2	Disconnected	-	
	l2tp_3	Disconnected	-	

Figure 3-1-5-1

#### IPsec Tunnel

Name	Status	Local IP	Remote IP
ipsec_1	Disconnected	-	( <b>-</b> )
ipsec_2	Disconnected	-	
ipsec_3	Disconnected	-	121

#### OpenVPN Client

Name	Status	Local IP	Remote IP
openvpn_1	Disconnected	-	~
openvpn_2	Disconnected	-	-
openvpn_3	Disconnected	14	199

Figure 3-1-5-2

GRE Tunnel				
	Name	Status	Local IP	Remote IP
	gre_1	Disconnected	-	22
	gre_2	Disconnected	2	-
	gre_3	Disconnected	2	20
DMVPN Tunnel				
	Name	Status	Local IP	Remote IP
	dmvpn	Disconnected	-	



VPN Status			
Item	Description		
Name	Show the name of the VPN tunnel.		
Status	Show the status of the VPN tunnel.		
Local IP Show the local tunnel IP of VPN tunnel.			
Remote IP	Show the remote tunnel IP of VPN tunnel.		

Table 3-1-5-1 VPN Status

## 3.1.6 Host List

You can view the host information on this page.

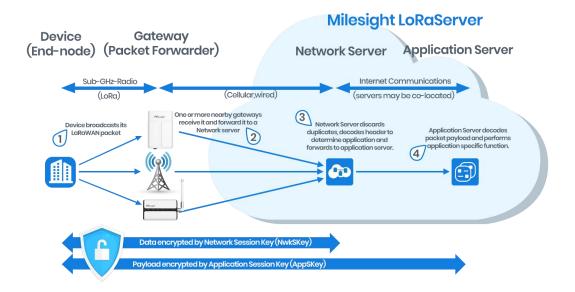
Overview	Cellular	Network	WLAN	VPN	Host List	
DHCP Leases						
	IP		MAC		Lease Remaining Time	
MAC Binding						
	IF	2			MAC	

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

Host List				
Description				
Show IP address of DHCP client				
Show MAC address of DHCP client				
Show the remaining lease time of DHCP client.				
Show the IP address and MAC address set in the Static IP list of DHCP service.				

Table 3-1-6-1 Host List Description

## 3.2 LoRaWAN



## 3.2.1 Packet Forwarder

## 3.2.1.1 General

General	Radios	Advanced	Custom	Traffic		
General Setting						
Gateway EUI	24E124	FFFEF35F39				
Gateway ID	24E12	4FFFEF35F39				
Frequency-Sync	Disab	led	~			
Data Retransmissi	on 🗌					
Multi-Destination						
ID	Er	able	Туре	Server Address	Connect Status	Operation
0	En	abled	Embedded NS	localhost	Disconnected	
						+

Figure 3-2-1-1

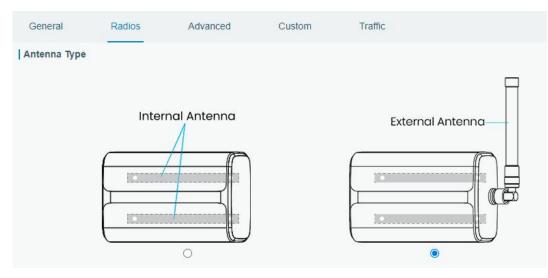
General Settings	General Settings				
Item	Description				
Gateway EUI	Show the unique identifier of the gateway and it's non-editable.				
Gateway ID	Fill in the corresponding ID which you've used for registering gateway to the remote network server, such as TTN. It is usually the same as gateway EUI and can be changed.				
Frequency-Sync	Sync frequency configurations from the network server by selecting the corresponding multi-destination ID.				
Data Retransmission	When the gateway connects to a single Chirpstack/Semtech/Remote Embedd ed NS type package forwarder, it supports data storage up to 1GB w hen network is disconnected and re-transmits the data after network recovery.				
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.				
Connection Status	Show the connection status of package forwarder.				

Table 3-2-1-1 General Setting Parameters

## **Related Configuration Example**

Packet fowarder configuration

## 3.2.1.2 Radios





Radio Channel Setting	
Region	US915 Voise Analyzer -
Name	Center Frequency/MHz
Radio 0	904.3
Radio 1	905.1



Radios-Radio Channel Setting			
Item	Description		
Antenna Type	Select the transmission type of antennas.		
Region	Choose the LoRaWAN <sup>®</sup> frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.		
Center Frequency	Change the frequencies to receive packets from LoRaWAN <sup>®</sup> nodes.		

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

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



**Radios-Multi Channel Setting** 

Item	Description
Enable	Click to enable this channel to transmit packets.
Index	Indicate the ordinal of the list.
Radio	Choose Radio 0 or Radio 1 as center frequency.
Frequency/MHz	Enter the frequency of this channel.
	Range: center frequency $\pm$ 0.4625.

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

1						
	Enable	Radio	Frequency/MHz	Bandwidth/KHz	Spread Factor	
		Radio 0 🔻	923.8	250KHZ •	SF7 •	



Radios-LoRa Channel Setting			
ltem	Description		
Enable	Click to enable this channel to transmit packets.		
Radio	Choose Radio 0 or Radio 1 as center frequency.		
	Enter the frequency of this channel.		
Frequency/MHz	Range: center frequency±0.9.		
Bandwidth/MHz	Enter the bandwidth of this channel.		
Spread Factor	Choose the selectable spreading factor. The channel with large spreading factor corresponds to a low rate, while the small one corresponds to a high rate.		

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

FSK Channel Setting				
Enable	Radio	Frequency/MHz	Bandwidth/KHz	DataRate
×	Radio 0 🔻	924.0	125KHZ <b>v</b>	50000

Figure 3-2-1-6

Radios-FSK Channel Setting			
ltem	Description		
Enable	Click to enable this channel to transmit packets.		
Radio	Choose Radio 0 or Radio 1 as center frequency.		
	Enter the frequency of this channel.		
Frequency/MHz	Range: center frequency±0.9.		
Bandwidth/MHz	Enter the bandwidth of this channel.		
	Recommended value: 125KHz, 250KHz, 500KHz		
Data Rate	Enter the data rate. Range: 500-25000.		

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

## 3.2.1.3 Noise Analyzer

LoRa Channel Setting

Noise analyzer is used for scanning the noise of every frequency channel and giving a diagram for users to analyze the environment interference condition and select best deployment. RSSI indicates the sensitivity for every channel. Lower the RSSI value, better

the signal. It's not suggested to enable this feature when using package forwarder since it will affect the downlink transmission.

Radio Channel Setting		
Supported Freq	US915 ~	Noise Analyzer 🔺
Noise Analyzer C Running		
Settings Sweep Freq Genaral Freq ~	•	
0.63: 902.3.914.9 MHz 64.71: 903.914.2 MHz		
Sweep Time Custom V		
24	h	
ОК		
-O- Current Value -O- Weighted	Average Value	
RSSI/dBm		MHz
-20-	1 1 1	IVINZ
-20 -		
-60 - A	F.	
-80-		
100-		
-116-		
902.3 902.7 903.1 903.5 903.9 904.3 904	4.7 905.1 905.5 905.9 906.	3

Figure 3-2-1-7

Noise Analyzer				
ltem	Description	Default		
Enable	Click to enable noise analyzer feature.	Disabled		
Sweep Freq	Select the frequency sweeping range. <b>General Freq:</b> frequencies based on the LoRaWAN <sup>®</sup> regional parameters document <b>Custom:</b> custom the frequency range	General Feq		
Sweep Time	Enable the noise analyzer continuously or within a period of time. If Custom is selected, the noise analyzer will stop automatically after the pre-configured time. Note: It's suggested to custom the time since noise analyzer feature will affect the normal data transmission.	Custom/24h		

Table 3-2-1-6 Noise Analyzer Setting Parameters

#### 3.2.1.4 Advanced

This section is about settings in details of beacon transmitting and validating.

General	Radios	Advanced	Custom	Traffic
Beacon Settin	g			
Beacon Period		0	~	s
Beacon Freq		508300000		Hz
Beacon Datarat	е	SF10	~	]
Beacon Channe	I Number	3	•	]
Beacon Freq St	ep	200000		Hz
Beacon Bandwi	dth	125000	*	Hz
Beacon TX Pow	ver	14		dBm



Advanced-Beacon Setting				
ltem	Description	Default		
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons.	0		
Beacon Freq	The frequency of beacons.	Based on the supported frequency		
Beacon Datarate	The datarate of beacons.	Based on the supported frequency		
Beacon Channel Number	When selecting Custom, it allows users to custom range from 1 to 8.	1		
Beacon Freq Step	Frequency interval of beacons.	200000		
Beacon Bandwidth	The bandwidth of beacons. Unit: Hz	12500 Hz		
Beacon TX Power	The TX power of beacons.	Based on the supported frequency		

Table 3-2-1-7 Advanced-Beacon Parameters

Intervals Setting		
Keep Alive Interval	10	s
Stat Interval	30	s
Push Timeout	100	ms
Forward CRC Setting		
Forward CRC Disabled		
Forward CRC Error		
Forward CRC Valid		

#### Figure 3-2-1-9

ltem	Description	Default
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to 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: 1-1999.	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 3-2-1-8 Advanced Parameters

## 3.2.1.5 Custom

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.

General	Radios	Advanced	Custom	Traffic	
Custom Config	guration				
Enable					
				Example	
"lorawan_publi "clksrc": 0, "antenna_gain "antenna_cfg": "full_duplex": fi "precision_time "enable": false "max_ts_metri "nb_symbols": }, "radio_0": { "enable": true,	"/dev/spidev0.0", ic": true, "ITXIRX", alse, estamp": { , cs": 255, 1	n, in dBi */			
"type": "SX125					*

Figure 3-2-1-10

## 3.2.1.6 Traffic

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

Traffic Setting								
Refresh	Clear							
Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
1	up	2	83002508	922.8	SF9BW125	4/5	-103	-13.2
1	up	-	71108156	922.6	SF9BW125	4/5	-102	-13.2
1	up	~	35426956	922.8	SF9BW125	4/5	-103	-9.8
1	up	-	3171639508	922.6	SF9BW125	4/5	-100	-10.5
1	up	-	3159744804	922.6	SF9BW125	4/5	-102	-13.0
1	up	-	3155781348	922.6	SF9BW125	4/5	-101	-12.2
1	up	8	3147851660	922.6	SF9BW125	4/5	-102	-13.8
1	up	÷	3143888916	922.8	SF9BW125	4/5	-102	-13.2
1	up	e.	3139922740	922.8	SF9BW125	4/5	-100	-12.2
1	up	-	3124065788	922.8	SF9BW125	4/5	-100	-12.8

Figure 3-2-1-11

ltem	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 3-2-1-9 Traffic Parameters

## 3.2.2 Network Server

Channel

## 3.2.2.1 General

General Setting			
Enable			
Platform Mode			
NetID	010203		
Join Delay	5		sec
RX1 Delay	1		sec
Lease Time	8760-0- <mark>0</mark>		hh-mm-ss
Log Level	info	~	
Giobal Channel Pla	n Setting		
Channel Plan	US915	~	

# Figure 3-2-2-1

8-15

ltem	Description	Default
<b>General Setting</b>		
Enable	Click to enable Network Server mode.	Enabled
Platform Mode	Enabled to connect gateway to Milesight IoT Cloud or Yeastar Workplace platform .	Disabled
NetID	Enter the network identifier.	010203
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	1

	end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	
Enter the amount of time till a successful join expires. The format is hours-minutes-seconds. If the join-type is OTAA, then the end-devices need to join the network server again when it exceeds the lease time.		876000-00-00
Log level	Choose the log level.	Info
Channel Plan Se	tting	
Channel Plan	Choose LoRaWAN <sup>®</sup> channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Depend on the gateway's frequency
Channel	Enabled frequencies are controlled using channel mask. Leave it blank means using all the default standard usable channels specified in the LoRaWAN® regional parameters document. It allows to enter the index of the cahnnels. <b>Examples:</b> 1, 40: Enabling Channel 1 and Channel 40 1-40: Enabling Channel 1 to Channel 40 1-40, 60: Enabling Channel 1 to Channel 40 All: Enabling all channels Null: Indicates that all channels are disabled	Depend on the gateway's frequency

Table 3-2-2-1 General Parameters

**Note:** For some regional variants, if allowed by your LoRaWAN<sup>®</sup> region, you can use Additional Plan to configure additional channels undefined by the LoRaWAN<sup>®</sup> Regional Parameters, like EU868 and KR920, as the following picture shows:

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



Additional Channels		
ltem	Description	
Frequency/MHz	Enter the frequency of the additional plan.	
Max Datarate	Enter the max datarate for the end-device. The range is based on what is specified in the LoRaWAN <sup>®</sup> regional parameters document.	

Min Datarate Enter the min datarate for the end-device. The range is based on what is specified in the LoRaWAN<sup>®</sup> regional parameters document.

Table 3-2-2-2 Additional Plan Parameters

## 3.2.2.2 Application

An application is a collection of devices with the same purpose/of the same type. Users can add a series of devices to the same application which needs to send to the same server.

You can edit the ap	oplication by clicking	or create a new application by clicking 🖽	
Applications			
Name	cloud		
Description	cloud		
Data Transmission			
	Туре	Operation	
		Ð	

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

Application	Application		
ltem	Description		
Nomo	Enter the name of the application profile.		
Name	E.g: smoker-sensor-app.		
<b>D</b>	Enter the description of this application.		
Description	E.g: an application for smoker sensor.		
Data	Data will be sent to your custom server using the MQTT, HTTP,		
Transmission	HTTPS or BACnet/IP protocol. One application can add 3 data		
	transmissions at most and every protocol can be selected only once.		

Table 3-2-2-3 Application Parameters

Туре	MQTT	~
Status	-	
General		
Broker Address		
Broker Port		
Client ID		
Connection Timeout/s	30	
Keep Alive Interval/s	60	
User Credentials		
Enable		
Username		
Password		



TLS			
Enable			
Mode	CA signed server certificate		
Торіс			
Data Type	topic		
Uplink data		QoS 0	*
Downlink data		QoS 0	~
Multicast downlink data		QoS 0	~
Join notification		QoS 0	~
ACK notification		QoS 0	~
Error notification		QoS 0	~

## Figure 3-2-2-5

MQTT Settin	MQTT Settings	
Item	Description	
General		
Broker Address	MQTT broker address to receive data.	
Broker Port	MQTT broker port to receive data.	



	Client ID is the unique identity of the client to the server.
Client ID	It must be unique when all clients are connected to the same server, and
	it is the key to handle messages at QoS 1 and 2.
Connection If the client does not get a response after the connection timeou	
Timeout/s	connection will be considered as broken. The Range: 1-65535.
Keep Alive	After the client is connected to the server, the client will send heartbeat
Interval/s	packet to the server regularly to keep alive. Range: 1-65535.
User Creden	tials
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
	Select from "Self signed certificates", "CA signed server certificate".
	CA signed server certificate: verify with the certificate issued by
Mode	Certificate Authority (CA) that pre-loaded on the device.
	Self signed certificates: upload the custom CA certificates, client
	certificates and secret key for verification.
Торіс	
Data Type	Data type sent to MQTT broker.
Торіс	Topic name of the data type used for publishing.
	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
QoS	This level guarantees that the message will be delivered at least once,
003	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.

Table 3-2-2-4 MQTT Settings Parameters

HTTP Header				
	Header Name	Header Value	Operation	
			Œ	
URL				
	Data Type	URL		
	Uplink data		]	
	Join notification		]	
	ACK notification		]	
	Error notification		]	



HTTP/HTTPS Settings		
ltem	Description	
HTTP Header		
Header Name	A core set of fields in the HTTP header.	
Header Value	Value of the HTTP header.	
URL		
Data Type	Data type sent to HTTP/HTTPS server.	
Topic	Topic name of the data type used for publishing.	
URL	HTTP/HTTPS server URL to receive data.	

Table 3-2-2-5 HTTP/HTTPS Settings Parameters

## **Related Configuration Example**

Application configuration

#### 3.2.2.3 Payload Codec

Payload Codec provides the inbuilt payload codec library of Milesight LoRaWAN devices to decode and encode the data easily. Users can also customize the payload codec of other brands of devices or adjust the uplink and downlink contents as requirements.

	Inbuilt	Payload	Codec	Library
--	---------	---------	-------	---------

Library Version

Obtaining Type
Obtain

\_\_\_\_\_

~

1.0.0

Online

Note: Ensure that the Internet access is available.

Name	Payload decoder function	Payload encoder function	Details
AM103 & AM103L	~	$\checkmark$	0
AM104	~	$\checkmark$	0
AM107	$\checkmark$	$\checkmark$	0
AM307	$\checkmark$	$\checkmark$	0
AM308	$\checkmark$	$\checkmark$	0
AM319-HCHO	$\checkmark$	$\checkmark$	0
AM319-HCHO-IR	$\checkmark$	$\checkmark$	0
AM319-O3	$\checkmark$	$\checkmark$	0
EM300-TH	$\checkmark$	$\checkmark$	0
WS101	~	~	0

Figure 3-2-2-7

Inbuilt Payload	Inbuilt Payload Codec Library		
ltem	Description		
Library	Show the version of the Milesight LoRaWAN node payload codec		
Version	library.		
Obtaining Type	Select the type to update the Milesight devices payload codec library. Online: update automatically if gateway detects there is version update every time gateway powers on and accesses the Internet. Users can also click Obtain button to check update status manually. Local Upload: click Browse to upload the zip format payload codec package and click Import to update the library.		
Name	Show the corresponding Milesight product model of the payload codec.		
Payload decoder/enc oder function	Show if decoder and encoder are existed.		
Details	Show the details of decoder and encoder. If this does not meet your requirement, please customize your payload codec.		

Table 3-2-2-6 Inbuilt Payload Codec Library Parameters

Name	
Description	
Template	None 👻
Payload decoder	
Payload decoder function	<pre>1 // Decode decodes an array of bytes into an object. // - + Ppert contains the LoRAWAN PPort number // - bytes is an array of bytes, e.g. [225, 230, 255, 0] // The function must return an object, e.g. {"temperature": 22.5} function Decode(FPort, bytes) { return []; } </pre>
Payload encoder	
Payload encoder function	<pre>1 // Encode encodes the given object into an array of bytes. // - fPort contains the LoRAWAN fPort number // - obj is an object, e.g. ("temperature"; 22.5) // The function must return an array of bytes, e.g. [225, 230, 255, 0] function Encode(fPort, obj) { return []; }</pre>
Payload Codec Test	
	1 // input decoded test payloed or encoded test payload // decoded bytes // 0 175 5C 03 67 34 01 04 68 65 05 6A 49 00 06 65 1C 00 79 00 14 00 07 7D E7 04 08 7D 07 00 09 73 3F 27 // encoded objs // 4



Custom Payload Codec	
ltem	Description
Name	Enter the unique name of the custom payload codec.
Description	Enter the description of this payload codec.
Template	Select an existing inbuilt payload codec as a template.
Payload Decoder/Encoder Function	Customize the device payload decoder or encoder. Note that the function header should be the same as the example on the blanks.
Payload Codec test	Disable or enable payload codec test.
fPort	Application port of LoRaWAN devices. It's 85 by default for Milesight LoRaWAN devices.
Decode	Enter the hex format raw data and click <b>Decode</b> to check the result.
Encode	Enter the JSON format command and check <b>Encode</b> to check the result.

Table 3-2-2-7 Custom Payload Codec Parameters

### 3.2.2.4 Profiles

A Profile defines the device capabilities and boot parameters that are needed by the Netwo rk Server for setting the LoRaWAN<sup>®</sup> radio access service. These information elements shall be provided by the end-device manufacturer.

You can edit	t the device p	rofile by clicking	or create	e a new device	profile by clicking
Device Profiles					
	Name	Max TXPower	Join Type	Class Type	Operation
	OTAA-ClassA-B	0	OTAA	Class A Class B	
	OTAA-ClassC	0	OTAA	Class A Class C	2 ×
	node	0	OTAA	Class A Class C	2 ×
					•



Device Profiles	
Name	
Max TXPower	0
Join Type	OTAA 🗸
Class Type	🔄 Class A 🗌 Class B 🔲 Class C
Advanced	



Device Profiles Settings		
Item	Description	
Name	Enter the name of the device profile.	
	Enter the maximum transmit power.	
Max	The TXPower indicates power levels relative to the Max EIRP level of	
TXPower	the end-device. 0 means using the max EIRP. EIRP refers to the	
	Equivalent Isotropically Radiated Power.	
Join Type	Select from: "OTAA" and "ABP".	
	Device type is Class A by default. Users can check the box of Class	
Class Type	B or Class C to add the class type.	
	Note: Beacon period should be set to nonzero value in "Packet	
	Forwarder"> "Advanced" if you use Class B.	

Table 3-2-2-8 Device Profiles Setting Parameters

Advanced			
MAC Version	1.0.2	~	
Regional Parameters Revision	В	~	
RX1 Datarate Offset	0	~	
RX2 Datarate	DR0 (SF12, 125 kHz)	~	
RX2 Channel Frequency	505300000		Hz
Frequency List			Hz
Device Channel			



Device Profile Advanced Settings				
ltem	Description	Default		
MAC Version	Choose the version of the LoRaWAN <sup>®</sup> 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	The offset which used for calculating the RX1 data-rate, based on the uplink data-rate.	Based on what is specified in		
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window.	the LoRaWAN <sup>®</sup> regional		
RX2 Channel Frequency	RX2 channel frequency which used for the RX2 receive-window.	parameters document		
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN <sup>®</sup> regional parameters document.	Null		
Device Channel	Change this device frequency channel by typing the channel indexs. When configured, it takes precedence over the global channel. This setting only works for CN470/US915/AU915 gateway.	Null		
PingSlot Period	Period of opening the pingslot.	Every Second		
PingSlot DataRate	Datarate of the node receiving downlinks.	Based on the supported frequency		
PingSlot Freq	Frequency of the node receiving downlinks.	Based on the supported frequency		
ACK Timeout	The time for confirmed downlink transmissions. This option is only applicable to class B and class	Class B: 10 Class C: 10		

C.	

 Table 3-2-2-9
 Device Profiles Advanced Setting Parameters

# 3.2.2.5 Device

A device is the end-device connecting to, and communicating over the LoRaWAN® network.

Add Bulk Import	Delete All					
Adu Buik Import	Delete All				Search	
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
24E124414B032563	24E124414B032563	classB	cloud	11 days ago	~	<b>ℤ</b> ×
24E124414A501971	24E124414A501971	OTAA-calssB	cloud	28 days ago	~	
1152-test	24E1612290821375	ClassC-OTAA	cloud	63 days ago	~	2 ×

Showing 1 to 3 of 3 rows

Figure 3-2-2-12
-----------------

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 3-2-2-10 Device Parameters

Device Name	lora-sensor		
Description	a short description of your node		
Device EUI	24e1641194784358		
Device-Profile	ClassC-OTAA 🗸		
Application	cloud 🗸		
Paylod Codec	<b>•</b>		
fPort	1		
Modbus RTU Data Transmission	Modbus RTU over TCP 🗸 🗸		
Modbus RTU Fport			
TCP Port			
Frame-counter Validation			
Application Key			
Device Address			
Network Session Key			
Application Session Key			
Uplink Frame-counter	0		
Downlink Frame-counter	0		



Device Configuration		
ltem	Description	
Device Name	Enter the name of this device.	
Description	Enter the description of this device.	
Device EUI	Enter the EUI of this device.	
Device-Profile	Choose the device profile.	
Application	Choose the application profile.	
Payload Codec	Choose the payload codec existed on Payload Codec page.	
fPort	Enter the downlink port of device, it's 85 by default for Milesight	
TFOIL	devices.	
	Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over	
	TCP". This feature is only applicable to Milesight LoRaWAN®	
Modbus RTU	controllers.(UC501/UC300, etc.)	
Data	Modbus RTU to TCP: TCP client can send Modbus TCP commands	
Transmission	to ask for controller Modbus data.	
	Modbus RTU over TCP: TCP client can send Modbus RTU commands	
	to ask for controller Modbus data.	
Modbus RTU	Enter the LoRaWAN® frame port for transparent transmission	
Fport	between Milesight LoRaWAN <sup>®</sup> controllers and UG65.	

	Range: 2-84, 86-223.
	Note: this value must be the same as the Milesight LoRaWAN <sup>®</sup> controller's fPort.
TCP Port	Enter the TCP port for data transmission between the TCP Client and UG65 (as TCP Server).Range: 1-65535.
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.
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.
Device Address	The device address identifies the end-device within the current network.
Network Session Key	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.
Application Session Key	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.
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.
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 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.

Table 3-2-2-11 Device Setting Parameters

### **Related Configuration Example**

**Device configuration** 

### 3.2.2.6 Multicast Groups

Milesight gateways support for creating Class B or Class C multicast groups to send downlink messages to a group of end devices. A multicast group is a virtual ABP device (i.e. shared session keys), does not support uplink, confirmed downlink nor MAC commands.

Multicast Groups				
Add			Search	Q
Multicast Addre	ss Group Name	Number of Devices	Operation	n
	No matchin	ig records found		

## Figure 3-2-2-14

ltem	Description
Add	Add a multicast group.
Group Name	Show the name of the group.
Number of Devices	Show the device number of the group.
Operation	Edit or delete the multicast group.

Table 3-2-2-12 Multicast Group Parameters

Multicast Address	Group Name	
Multicast Application Session Key       Class Type       Datarate       Drequency       Frequency       Frame-counter	Multicast Address	
Class Type     Class C       Datarate     DR8(SF12,500KHz)       Frequency     923300000       Frame-counter     0	Multicast Network Session Key	
Datarate     DR8(SF12,500KHz)       Frequency     923300000       Frame-counter     0	Multicast Application Session Key	
Frequency     923300000       Frame-counter     0	Class Type	Class C 🗸
Frame-counter 0	Datarate	DR8(SF12,500KHz)
	Frequency	923300000
	Frame-counter	0
Selected Devices	Selected Devices	

### Figure 3-2-2-15

Multicast Group Configuration				
Item	Description			
Group Name	Enter the name of this multicast group.			
Multicast Address	Device address (Dev Addr) of all devices in this group.			
Multicast Network Session Key	The network session key (Netwks Key) of all devices in this group.			
Multicast Application Session Key	The application session key (AppSKey) of all devices in this group.			

Class Type	Class B and Class C are optional.
Datarate	Datarate of the node receiving downlinks.
Frequency	Downlink frequency of all devices in this group.
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.
Ping Slot Periodicity	Period of opening the pingslot. This is only applied to Class B end devices.
Selected Devices	Show all device names in this group.
Add Device	Add devices in the pull-down list.

Table 3-2-2-13 Multicast Group Setting Parameters

# 3.2.2.7 Gateway Fleet

Milesight gateways can connect to UG65 network server. It is suggested to add not more than 5 gateways.

Gateway Fleet				
Gateway ID	Name	Status	Last Seen	Operation
24E124FFFEF12263	Local Gateway	Connected	2021-04-19 16:12:27	[/] ×
				•

Figure 3-2-2-16

ltem	Description
Gateway ID	Show the gateway ID.
Name	Show the name of the gateway.
Status	Show the connection status of the gateway.
Last Seen	Show the time of last packet received.
Operation	Edit or delete the gateway.

Table 3-2-2-14 Gateway Fleet Parameters

Gateway ID		
Name		
Location		
GPS info will be displa	ayed by default or can be changed manu	ally
	ayed by default or can be changed manu Eg:0.026811	Jally
GPS info will be displa Latitude Longitude		Jally



ltem	Description
Gateway ID	Enter the unique gateway ID to recognize the gateway.
Name	Enter the name of this gateway.
Location	GPS data of the gateway can be edited here. If gateway sends GPS data it will replace your customized data.

Table 3-2-2-15 Gateway Setting Parameters

# 3.2.2.8 Packets

end Data To Device									
Device EUI		Туре		Payload			Port	Confirme	d
000000000000000000000000000000000000000	AS	iCII 🗸				(	85		Send
end Data to Multicast G	roup								
Multicast Group		Туре		Payload			Port		
	✓ AS	icii 🗸				[	85		Send
etwork Server									
Clear							Search		
Device EUI/Group	Gateway ID	Frequency	Datarate	RSSI/SNR	Size	Fcnt	Туре	Time	Detail
			matching reco						

Figure 3-2-2-18

Send Data To Device/Multicast Group				
ltem	Description			
Device EUI	Enter the EUI of the device to receive the payload.			
Multicast Group	Select the multicast group to send downlinks. Multicast groups can be added under Multicast Groups tab.			
Туре	Choose from: "ASCII", "hex", "base64". Choose the payload type to enter in the payload Input box.			
Payload	Enter the message to be sent to this device.			
Port	Enter the LoRaWAN <sup>®</sup> frame port for packet transmission between device and Network Server.			
Confirmed	After enabled, the end device will receive downlink packet and should answer "confirmed" to the network server. Multicast feature does not support confirmed downlink.			

Table 3-2-2-16 Send Data to Device Parameters

Network Server	
Item	Description
Device EUI/Group	Show the EUI of the device or multicast group.
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.				
	Show the type of the packet:				
	JnAcc - Join Accept Packet				
	JnReq - Join Request Packet				
	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				
Time	Show the time of packet was sent or received.				

Table 3-2-2-17 Packet Parameters

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

Packet Details		×
Dev Addr/Multicast Addr	0614B991	A
GwEUI	24E124FFFEF0E225	
AppEUI	24E124C0002A0001	
Device EUI/Group Name	24E124126A210644	
Class Type	Class C	
Immediately		
Timestamp	2721022973	
Туре	UpUnc	
Adr	false	
AdrAcKReq	false	
Ack	false	
Fcnt	969	
Port	85	

Figure 3-2-2-19

ltem	Description
Dev Addr/Multicast Addr	Show the address of the device/multicast group.
GwEUI	Show the EUI of the gateway.
AppEUI	Show the EUI of the application.
DevEUI/Group Name	Show the EUI of the device/multicast group name.
Class Type	Show the class type of the device or multicast group.

Immediately	True: Device may transmit an explicit (possibly empty) acknowledgement data message immediately after the reception of a data message requiring a confirmation.
Timestamp	Show the timestamp of this packet.
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
Adr	True: The end-node has enabled ADR. False: The end-node has not enabled ADR.
AdrAcKReq	In order to validate that the network is receiving the uplink messages, nodes periodically transmit ADRACKReq message. This is 1 bit long. True: Network should respond in ADR_ACK_DELAY time to confirm that it is receiving the uplink messages. False: ADR is disabled or Network does not respond in ADR_ACK_DELAY.
Ack	True: This frame is ACK. False: This frame is not ACK.
Fcnt	Show the frame-counter of this packet. The network server tracks the uplink frame counter and generates the downlink counter for each end-device.
FPort	FPort is a multiplexing port field. If the frame payload field is not empty, the port field must be present. If present, a FPort 16 value of 0 indicates that the FRMPayload contains MAC commands only.When this is the case, the FOptsLen field must be zero. FOptsLen is the length of the FOpts field in bytes.
Modulation	LoRa means the physical layer uses the LoRa modulation.
Bandwidth	Show the bandwidth of this channel.
SpreadFactor	Show the spreadFactor of this channel.
Bitrate	Show the bitrate of this channel.
CodeRate	Show the coderate of this channel.
SNR	Show the SNR of this channel.
RSSI	Show the RSSI of this channel.
Power	Show the transmit power of the device.
Payload (b64)	Show the application payload of this packet.
Payload (hex)	Show the application payload of this packet.
Json	Show the data after decoded.
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 3-2-2-18 Packets Details Parameters

# **Related Topic**

Send Data to Device

# **3.3 Protocol Integration**

### 3.3.1 BACnet Server

UG65 can work as LoRaWAN to BACnet gateway to integrate with BMS system easily.

### 3.3.1.1 Server

Server		
Enable		
UDP Port	47808	
Device ID	40185	
Device Name	UG67-6222B4620088	
BBMD		
IP Address		
IP Port	47808	
Time TO Live	60000	

Figure 3-3-1-1

Server Settings	
Item	Description
Enable	Enable or disable BACnet server function.
UDP Port	Set communication port of BACnet/IP. Range: 1-65535. The default port is 47808.
Device ID	The unique BACnet device identifier which needs to avoid conflict with other devices.
Device Name	The device name to represent the device.
BBMD	Enable BBMD(BACnet/IP Broadcast Management Device) if BACnet devices of different network subnets should work together.
IP Address	Fill in the IP address of BBMD device or external device registrar.
IP Port	Fill in the UDP/IP port for external device registration.
Time TO Live	Number of seconds used on external device registration.

Table 3-3-1-1 Server Parameters

# 3.3.1.2 BACnet Object

Add	Bulk Import	Bulk Expo	ort Delete All				Sear	ch	0
Object	t Name	Object Type	Object Instance Nr	Present Value	Units	Updates	Update time	cov	Operation
24E124592B32	2496.button	Analog-Input	0	1670892748800.0	no- units	539	2022-12-13 08:52:06	Disabled	ℓ ×

Figure 3-3-1-2

Item	Description
Add	Add a BACnet object. The gateway supports adding 2000
Auu	objects at most.
Bulk Import	Download template and import multiple BACnet objects.
Bulk Export	Export all generated BACnet object settings.
Delete All	Delete all objects in the list.
Object Name	Show the name of the BACnet object.
Object Type	Show the type of this object.
<b>Object Instance Nr</b>	Show the instance number of this object.
Present Value	Show the latest value of object.
Units	Show the unit of this object value.
Updates	Show the update times of this object value.
Update time	Show the time for this object to get and update the data.
COV	Show if COV (Change of value) is enabled.
Operation	Edit or delete the object.

Table 3-3-1-2 BACnet Object List Parameters

BACnet Object	
Device Name	24E124592B322496 💌
LoRa Object	button_1_ts
Object Name	24E124592B322496.button_1_1
Object Type	Analog-Input 🗸
Units	~
Description	
COV	
COV Increment	1.0



BACnet Object Configuration			
ltem	Description		
Device Name	Select the device added on Network Server > Device page.		

LoRa Object	Select one of device variables as an object.
Object Name	Customize an unique name for this object.
Object Type	Select the object type as binary input/output/value or analog
Object Type	input/output/value.
Unit	Select the unit of this object value.
Description	Enter the description of this object.
	When object value changes, the BACnet server (gateway) will send
COV	notification of new value to BACnet client. This only applies to
	analog type objects.
00)///	Only when the object value reaches or over this increment, the
COV Increment	BACnet server (gateway) will send the notification.
Polarity	Define the binary input/output status as Normal or Reverse.
	Characterize the intended effect of active state of binary type object
Active Text	value. <b>Example:</b> when a button is pressed and binary input is 1,
	active text can be defined as "Pressed".
	Characterize the intended effect of inactive state of binary type
Inactive Text	object value. <b>Example:</b> for a button, inactive text can be defined as
	"Unpressed".
Relinquish	If there is no command, the analog output or binary output will be
Default	set as this relinquish default value.

Table 3-3-1-3 BACnet Object Configuration Parameters

# 3.4 Network

### 3.4.1 Interface

### 3.4.1.1 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	Port eth 0					
	Connec	tion Type	Static IP	~		
Network	IP Addr	ess	192.168.22.112			
Interface	Netmask				255.255.255.0	
Firewall	Gatewa	ау			192.168.22.1	
DHCP	MTU				1500	
	Primary	DNS Server			8.8.8.8	
DDNS	Second	lary DNS Server			114.114.114.114	
Link Failover	Enable	NAT				1

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

Port Setting					
Item	Description	Default			
Port	The port that is fixed as eth0 port and enabled.	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.	8.8.8.8			
Secondary DNS Server	Set the secondary DNS.	114.114.114.1 14			
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable			

Table 3-4-1-1 Port Parameters

## **Related Configuration Example**

**Ethernet Connection** 

## 1. Static IP Configuration

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

Port_1			
Port	eth 0		
Connection Type	Static IP 🗸		
IP Address	192.168.22.112		
Netmask	255.255.255.0		
Gateway	192.168.22.1		
MTU	1500		
Primary DNS Server	8.8.8.8		
Secondary DNS Server	114.114.114		
Enable NAT			
Multiple IP Address			
IP A	ddress	Netmask	Operatio
			E

Figure 3-4-1-2

Static IP					
Item	Description	Default			
IP Address	Set the IP address which can access Internet.	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 3-4-1-2 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.

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

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

DHCP Client			
Item	Description		
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when user visits domain name.		
	Table 3-4-1-3 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	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	114.114.114.114

Figure 3-4-1-4

PPPoE				
ltem	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 3-4-1-4 PPOE Parameters

### 3.4.1.2 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				
Enable				
Work Mode	9	AP		~
SSID Broa	dcast			
AP Isolatio	n			
Radio Type	9	802.11n	(2.4GHz)	~
Channel		Auto		~
SSID				
BSSID				
Encryption	Mode	No Encr	yption	~
Bandwidth		20MHz		~
Max Client	Number	10		
IP Setting				
Protocol		Static IP		~
IP Address	8			
		DHCP Set	tings	
Netmask				



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 3-4-1-6

WLAN Settings			
Item	Description		
Enable	Enable/disable WLAN.		

Work Mode	Select gateway's work mode. The options are "Client" or "AP".				
DOOLD	Fill in the MAC address of the access point. Either SSID or BSSID				
BSSID	can be filled to joint the network.				
SSID	Fill in the SSID of the access point.				
Client Mode					
Scan	Click "Scan" button to search the nearby access point.				
	Select encryption mode. The options are "No Encryption", "WEP				
Encryption Mode	Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" ,				
Liferyption 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					
	When SSID broadcast is disabled, other wireless devices can't not				
SSID Broadcast	find the SSID, and users have to enter the SSID manually to				
	access to the wireless network.				
AP Isolation	When AP isolation is enabled, all users which access to the AP				
AP Isolation	are isolated without communication with each other.				
Radio Type	Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".				
Channel	Select wireless channel. The options are "Auto", "1", "2""11".				
	Select encryption mode. The options are "No Encryption", "WEP				
Encryption Mode	Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and				
	"WPA-PSK/WPA2-PSK".				
Qinhar	Select cipher. The options are "Auto", "AES", "TKIP" and				
Cipher	"AES/TKIP".				
Key	Fill the pre-shared key of WPA encryption.				
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".				
Max Client Number	Set the maximum number of client to access when the gateway				
	is configured as AP.				
IP Setting					
Protocol	Set the protocol in wireless network.				
IP Address	Set the IP address in wireless network.				
Netmask	Set the netmask in wireless network.				
Gateway	Set the gateway in wireless network.				

#### Table 3-4-1-5 WLAN Parameters

Port	WLAN	Cellular	Lo	opback				
< GoBack								
55	SID	Channel	Signal	Cipher	BSSID	Security	Frequency	
Vison Sen:	sor_006602	Auto	-94dBm	Auto	24:e1:24:00:66:02	No Encryption	2462MHz	Join Network
Milesig	ght_Test	Auto	-88dBm	AES	ec:26:ca:99:3a:a4	WPA-PSK/WPA2-PSK	2437MHz	Join Network



<b>Client Mode-Scan</b>					
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 3-4-1-6 WLAN Scan Parameters

# **Related Topic**

## Wi-Fi Application Example

### 3.4.1.3 Cellular

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

Port	WLAN	Cellular	Loopback
Cellular Se	etting		
Enable			
Network Ty	ре	Auto	~
APN			
Username			
Password			
Access Nur	mber		
PIN Code			
Authenticat	ion Type	Auto	~
Roaming			
SMS Cente	r	<u>.</u>	





Connection Setting		
Enable NAT		
Restart When Dial-up failed		
ICMP Server	8.8.8.8	
Secondary ICMP Server	114.114.114.114	
ICMP Detection Max Retries	3	
ICMP Detection Timeout	5	s
ICMP Detection Interval	15	s
SMS Settings		
SMS Mode	PDU	~
	S	



General Settings				
ltem	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: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.	Auto		
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.	Null		
Username	me Enter the username for cellular dial-up connection provided by local ISP.			
Password	Enter the password for cellular dial-up connection provided by local ISP.			
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.	Enable		
SMS Center	SMS Center Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.			
Enable NAT	Enable or disable NAT function.	Enabled		
Restart When	When this function is enabled, the gateway will restart	Disabled		

Dial-up failed	automatically if the dial-up fails several times.	
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.	114.114.11 4.114
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

Table 3-4-1-7 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 3-4-1-10

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 3-4-1-8 Cellular Parameters

# **Related Topics**

Cellular Connection Application Example

### Phone Group

### 3.4.1.4 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
					<b>H</b>
Save					

Figure 3-4-1-11

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 3-4-1-9 Loopback Parameters

#### 3.4.1.5 VLAN Trunk

UG65 gateway supports the Ethernet port working as VLAN Trunk client and be assigned a VLAN ID, which easy to traffic classification. When VLAN ID is set, port on "**Network"** > "Interface" > "Port" can be chosen as eth0.x with x being VLAN ID. VLAN Setting is blank by

default, you can add a new VLAN label to certain interface by clicking

×
•

Figure 3-4-1-12

VLAN Trunk	
ltem	Description
Interface	Select the VLAN interface, it's fixed as eth0.
VID	Set the label ID of the VLAN. Range: 1-4094.

Table 3-4-1-10 VLAN Trunk Parameters

## 3.4.2 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.

# 3.4.2.1 Security

Security	ACL	DMZ	Port Mapping		MAC Binding
Website Block	ing by URL Ad	dress			
URL Address		http://		] 🗵	
				Ŧ	
Website Block	ing by Keywor	d			
Keyword					
				+	

Figure 3-4-2-1

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

### 3.4.2.2 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 Polic	cy	Accept	~				
Access Control	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			
			Description				
			Save	Cancel			
Interface List							
	Interface		In ACL			Out ACL	Operation
							•

Figure 3-4-2-2

ltem	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	Wildcard mask of the source network address.
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	white and mask of destination address.
Description	Fill in a description for the groups with the same ID.
ІСМР Туре	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.

Select source port type, such as specified port, port range, etc.
Set source port number. Range: 1-65535.
Set start source port number. Range: 1-65535.
Set end source port number. Range: 1-65535.
Select destination port type, such as specified port, port range,
etc.
Set destination port number. Range: 1-65535.
Oct start destination next number, Dennes 1 (FEOF
Set start destination port number. Range: 1-65535.
Set end destination port number. Range: 1-65535.
Show information of the port.
Select network interface for access control.
Select a rule for incoming traffic from ACL ID.
Select a rule for outgoing traffic from ACL ID.

Table 3-4-2-2 ACL Parameters

### 3.4.2.3 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
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" means any address.

Table 3-4-2-3 DMZ Parameters

# 3.4.2.4 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	IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0					TCP 🖌		
							•

Figure 3-4-2-4

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 forwarded. Range: 1-65535.				
Destination IP	Enter the IP address that packets are forwarded to after being received on the incoming interface.				
Destination Port	Enter the TCP or UDP port that packets are forwarded to after being received on the incoming port(s). Range: 1-65535.				
Protocol	Select from "TCP" and "UDP" as your application required.				
Description	The description of this rule.				

Table 3-4-2-4 Port Mapping Parameters

## **Related Configuration Example**

NAT Application Example

## 3.4.2.5 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					
Ν	MAC Address		IP Address		Description	Operation
						×
						Ð

Figure 3-4-2-5

MAC Binding List					
ltem	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 3-4-2-5 MAC Binding Parameters

# 3.4.3 DHCP

UG65 can be set as a DHCP server to distribute IP address when Wi-Fi work as AP mode.

wlan0 🗸		
192.168.66.100		
192.168.66.199		
255.255.255.0		
1440		
8.8.8.8		
ess	IP Address	Operat
	wlan0         192.168.66.100         192.168.66.199         255.255.255.0         1440         8.8.8.8	wlan0          192.168.66.100         192.168.66.199         255.255.255.0         1440         8.8.8.8

Figure 3-4-3-1

DHCP Server						
ltem	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.	114.114.114.114
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

Table 3-4-3-1 DHCP Server Parameters

### 3.4.4 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	od List								
Name	Interface	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Oper ation
	wlan0 🗸	DynDI 🗸							×
									Ð

Figure 3-4-4-1

DDNS	DDNS				
ltem	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 3-4-4-1 DDNS Parameters

### 3.4.5 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.

## 3.4.5.1 SLA

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

SLA		Track	WAN Failover								
SLA En	itry										
	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 🗸	×	
										Ð	

Figure	3-4-5-1
--------	---------

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.	114.114.114.11 4
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 probe fails when the preset packet loss count is exceeded.	5

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

Table 3-4-5-1 SLA Parameters

### 3.4.5.2 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	▼ 1 <b>∨</b>	wlan0 🗸 🗸	0	1	×
						•

Figure 3-4-5-2

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 3-4-5-2 Track Parameters

### 3.4.5.3 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	ck	WAN Fa	ilover				
WAN Failo Main Int		Backup Ir	nterface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
Cellular	0 🗸	eth 0	~	30	0	0	1 ~	
								Ð

Figure 3-4-5-3

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	0		

	detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	
Track ID	Track detection, select the defined track ID.	

Table 3-4-5-3 WAN Failover Parameters

# 3.4.6 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.

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

### 3.4.6.1 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 Settin	gs				
Enable					
Hub Address					
Local IP Addres	35				
GRE HUB IP A	ddress				
GRE Local IP A	ddress				
GRE Mask			255.255.255.0		
GRE Key					
Negotiation Mo	de		Main	•	
Authentication /	Algorithm		DES	•	
Encryption Algo	orithm		MD5	•	
DH Group			MODP768-1	•	
Key					
Local ID Type			Default	•	
IKE Life Time(s	)		10800		
SA Algorithm			DES-MD5	•	
PFS Group			NULL	•	
Life Time(s)			3600		
		Fi	aure 3-4-6-1		

Figure 3-4-6-1

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

Eiguro	2162
rigule	3-4-6-2

DMVPN				
ltem	Description			
Enable	Enable or disable DMVPN.			
Hub Address	The IP address or domain name of DMVPN Hub.			
Local IP address	DMVPN local tunnel IP address.			
GRE Hub IP Address	GRE Hub tunnel IP address.			
GRE Local IP Address	GRE local tunnel IP address.			
GRE Netmask	GRE local tunnel netmask.			
GRE Key	GRE tunnel key.			
Negotiation Mode	Select from "Main" and "Aggressive".			
Authentication	Select from "DES", "3DES", "AES128", "AES192" and			
Algorithm	"AES256".			
Encryption Algorithm	Select from "MD5" and "SHA1".			
DH Group	Select from "MODP768_1", "MODP1024_2" and			
ыныныр	"MODP1536_5".			
Key	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",			
o, thigontain	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and			
	"AES256_SHA1".			
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and			
•	"MODP1536-5".			
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.			
DPD Interval Time (s)	Set DPD interval time			
DPD Timeout (s)	Set DPD timeout.			
Cisco Secret	Cisco Nhrp key.			
NHRP Holdtime (s)	The holdtime of Nhrp protocol.			

Table 3-4-6-1 DMVPN Parameters

### 3.4.6.2 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				
- IPsec_1				
Enable				
IPsec Gate	eway Address			
IPsec Mod	e	Т	unnel	•
IPsec Prot	ocol	E	SP	•
Local Subr	net			
Local Subr	net Mask			
Local ID Ty	ype		efault	•
Remote Su	ubnet			
Remote Su	ubnet Mask			
Remote ID	Туре	D	efault	•

Figure 3-4-6-3

Description	
Enable IPsec tunnel. A maximum of 3 tunnels is allowed.	
Enter the IP address or domain name of remote IPsec	
server.	
Select from "Tunnel" and "Transport".	
Select from "ESP" and "AH".	
Enter the local subnet IP address that IPsec protects.	
Enter the local netmask that IPsec protects.	
Select from "Default", "ID", "FQDN", and "User FQDN".	
Enter the remote subnet IP address that IPsec protects.	
Enter the remote netmask that IPsec protects.	
Select from "Default", "ID", "FQDN", and "User FQDN".	

Table 3-4-6-2 IPsec Parameters

IKE Parameter			
IKE Version	IKEv1	•	
Negotiation Mode	Main	¥	
Encryption Algorithm	DES	•	
Authentication Algorithm	MD5	•	
DH Group	MODP768-1	٣	
Local Authentication	PSK	٣	
Local Secrets			
XAUTH			
Lifetime(s)	10800		
SA Parameter			
SA Algorithm	DES-MD5	•	
PFS Group	NULL	•	
Lifetime(s)	3600		
DPD Time Interval(s)	30		
DPD Timeout(s)	150		
IPsec Advanced			
Enable Compression			
VPN Over IPsec Type	NONE	•	



IKE Parameter				
ltem	Description			
IKE Version	Select from "IKEv1" and "IKEv2".			
Negotiation Mode	Select from "Main" and "Aggressive".			
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".			
Authentication Algorithm	Select from "MD5" and " SHA1"			
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".			
Local Authentication	Select from "PSK" and "CA".			
Local Secrets	Enter the preshared key.			
XAUTH	Enter XAUTH username and password after XAUTH is enabled.			
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.			
SA Parameter				
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".			
PFS Group	Select from "NULL", "MODP768_1" , "MODP1024_2" and "MODP1536_5".			
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 3-4-6-3 IPsec Parameters

### 3.4.6.3 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.

PN	IPsec	GRE	L2TP	PPTP
ettings				
GRE_1				
Enable				
Remote IP Add	Iress			
ocal IP Addre	ss		12 	
_ocal Virtual IP	Address			
Netmask			255.255.255.0	
Peer Virtual IP	Address			
Globa <mark>l T</mark> raffic F	orwarding			
Remote Subne	t			
Remote Netma	sk			
UTU			1500	
Key				
Enable NAT				
	Settings SRE_1 Enable Remote IP Addre Local IP Addre Local Virtual IP Netmask Peer Virtual IP Slobal Traffic F Remote Subne Remote Netma MTU Key	Settings SRE_1 Enable Remote IP Address Local IP Address Local Virtual IP Address Local Virtual IP Address Netmask Peer Virtual IP Address Slobal Traffic Forwarding Remote Subnet Remote Netmask MTU Key	Settings SRE_1 Enable Remote IP Address Local IP Address Local IP Address Local Virtual IP Address Local Virtual IP Address Remote Subnet Remote Subnet Remote Netmask MTU Key	SRE_1  Enable  Remote IP Address  Local IP Address  Local IP Address  Local Virtual IP Address



GRE	
ltem	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 3-4-6-4 GRE Parameters

#### 3.4.6.4 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_1				
Enable			i	
Remote IF	PAddress			
Username				
Password				
Authentica	ation		Auto	~
Global Tra	ffic Forwarding	C	)	
Remote S	ubnet		10.5.22.0	
Remote S	ubnet Mask		255.255.255.0	
Key				
Use L2TP	Peer DNS		1	

Figure 3-4-6-6

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
Forwarding	this function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Key	Enter the password of L2TP tunnel.
Use L2TP Peer DNS	Enable to use the DNS address of peer L2TP server .

#### Table 3-4-6-5 L2TP Parameters

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

Figure 3-4-6-7

Advanced Settings				
ltem	Description			
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP 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 Compression	For PPP initialization. User can keep the default option.			
Protocol Field Compression	For PPP initialization. User can keep the default option.			
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.			

MRU	Set the maximum receive unit. Range: 64-1500.		
MTU	Set the maximum transmission unit. Range: 64-1500		
Link Detection Interval	Set the link detection interval time to ensure tunnel		
(s)	connection. Range: 0-600.		
Max Retries	Set the maximum times of retry to detect the L2TP		
Max Relifes	connection failure. Range: 0-10.		
Export Options	User can enter some other PPP initialization strings in this		
Expert Options	field and separate the strings with blank space.		

Table 3-4-6-6 L2TP Parameters

## 3.4.6.5 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 Settings				
- PPTP_1				
Enable				
Remote IP	Address			
Username				
Password				
Authentica	tion	A	Auto	•
Global Trat	ffic Forwarding			
Remote Su	ubnet			
Remote Su	ubnet Mask			

Figure 3-4-6-8

PPTP			
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 Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.		
Remote Subnet	Set the peer subnet of PPTP.		

Remote Subnet Mask	Set the netmask of peer PPTP server.	
	Table 3-4-6-7 PPTP Parameters	
Advanced Settings		
Local IP Address		
Peer IP Address		
Enable NAT		
Enable MPPE		
Address/Control Co	mpression	
Protocol Field Com	pression	
Asyncmap Value	fffffff	
MRU	1500	
MTU	1500	

#### Figure 3-4-6-9

60

0

Link Detection Interval(s)

Max Retries

Expert Options

PPTP Advanced Settings			
Item	Description		
Local IP Address	Set IP address of PPTP client.		
Peer IP Address	Enter tunnel IP address of PPTP server.		
Enable NAT	Enable the NAT faction of PPTP.		
Enable MPPE	Enable MPPE encryption.		
Address/Control Compression	For PPP initialization. User can keep the default option.		
Protocol Field	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	Set the link detection interval time to ensure tunnel		
(s)	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 3-4-6-8 PPTP Parameters

#### 3.4.6.6 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).

IVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifica
enVPN Clie	nt Settings				· · · · · · · · · · · · · · · · · · ·		
• OpenVPN	_1						
Enable		<b>S</b>					
Protocol			5	•			
Remote IF	Address						
Port		1194	ļ				
Interface		tun		•			
Authentica	ation	Nor	e	•			
Local Tun	nel IP						
Remote T	unnel IP						
Enable N/	AT						
Compress	sion	LZC	)	•			
Link Dete	ction Interval(s)	60					
Link Deteo	ction Timeout(s)	300					
Cipher		Nor	e	•			
мти		1500	)				
Max Fram	le Size	1500	)				
Verbose L	evel	ERI	ROR	v			
Expert Op	otions						
Local Ro	ute						
		Subnet			Subnet Mas	k	Operation
							E

Figure 3-4-6-10

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 initialization strings in this field and separate the strings with semicolon.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
	Table 3-1-6-9 OpenVPN Client Parameters

Table 3-4-6-9 OpenVPN Client Parameters

## 3.4.6.7 OpenVPN Server

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 Ser	ver Settings					
Enable						
Protocol		UDP		Ŧ		
Port		1194				
Listening IP						
Interface		tun		Ŧ		
Authentication		None		*		
Local Virtual IP						
Remote Virtual	IP					
Enable NAT		4				
Compression		LZO		¥		
Link Detection I	nterval	60				
Cipher		None		Ŧ		
MTU		1500				
Max Frame Size	e	1500				
Verbose Level		ERROR		¥		
Expert Options						



Local Route			
	Subnet	Netmask	Operation
			8
Account			
	Username	Password	Operation
			<b>H</b>

Figure 3-4-6-12

OpenVPN Server				
Item	Description			
Enable	Enable/disable OpenVPN server.			
Protocol	Select from TCP and UDP.			
Port Fill in listening port number. Range: 1-65535.				
Listoning 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",			
Authentication	"X.509 cert" and "X. 509 cert +user".			
Local Virtual IP	The local tunnel address of OpenVPN's tunnel.			

Remote Virtual IP	The remote tunnel address of OpenVPN's tunnel.
Client Subnet	Local subnet IP address of OpenVPN client.
Client Netmask	Local netmask of OpenVPN client.
Renegotiation Interval(s)	Set interval for renegotiation. Range: 0-86400.
Max Clients	Maximum OpenVPN client number. Range: 1-128.
Enable CRL	Enable CRL
Enable Client to Client	Allow access between different OpenVPN clients.
Enable Dup Client	Allow multiple users to use the same certification.
Enable NAT	Check to enable the NAT traversal function.
Compression	Select "LZO" to compress data.
Link Detection Interval	Set link detection interval time to ensure tunnel connection.
	Range: 10-1800.
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",
Cipilei	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 64-1500.
Max Frame Size	Set the maximum frame size. Range: 64-1500.
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".
Expert Options	User can enter some other initialization strings in this field
	and separate the strings with semicolon.
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 3-4-6-10 OpenVPN Server Parameters

## 3.4.6.8 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 Clie	nt						
- OpenVPN	client_1						
CA				Browse	Import Export De	lete	
Public Ke	y			Browse	Import Export De	lete	
Private Ke	∋y <mark>n</mark>			Browse	Import Export De	lete	
TA				Browse	Import Export De	lete	
Preshared	d Key			Browse	Import Export De	lete	
PKCS12				Browse	Import Export De	lete	

#### Figure 3-4-6-13

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

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

Table 3-4-6-11 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 3-4-6-14

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 3-4-6-12 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 3-4-6-15

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 3-4-6-13 IPsec Parameters

## 3.5 System

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

## 3.5.1 General Settings

## 3.5.1.1 General

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

General	System Time	SMTP	Phone	Email	
System					
Hostname		GATEWAY			
Web Login Time	out(s)	1800			
Access Servic	e				
	Enable	Sen	vice	Port	
		нт	TP	80	
		HTT	PS	443	
		TELI	NET	23	
		SS	θH	22	
HTTPS Certific	ates				
Certificate	https.crt	Browse	Import Expo	t Delete	
Key	https.key	Browse	Import Expo	t Delete	

Figure 3-5-1-1

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



Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800			
Access Servic	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 Certifi	cates				
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 3-5-1-1 General Setting Parameters

## 3.5.1.2 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	)	
Sync Type		Sync with Brows	ser 🔹	
Browser Time		2019-06-12 20:3	4:32 Wed	

Figure 3-5-1-2

General	System Time	SMTP	Phone	Email
System Time Se	ettings			
Current Time		2019-06-12 20:3	33:59 Wed	
Time Zone		8 China (Beijin	g) 🔻	
Sync Type		Set up Manuall	y 🔹	
Date		2019-06-12		
Time		20 🔻 33	▼ 59 ▼	
	Fi	gure 3-5-1-3		
General	System Time	SMTP	Phone	Email
System Time S	ettings			
Current Time		2019-06-12 20:33	3:36 Wed	
Time Zone		8 China (Beijing)	) 🔻	
Sync Type		Sync with NTP S	berver 🔻	

General	System Time	SMTP	Phone	Email
System Time	Settings			
Current Time		2019-06-12 20:3	3:36 Wed	
Time Zone		8 China (Beijing	a) 🔹	
Sync Type		Sync with NTP	Server •	
NTP Server Ad	dress	1.cn.pool.ntp.org	9	
Enable NTP Se	rver			

Figure 3-5-1-4

System Time			
Item	Description		
Current Time	Show the current system time.		
Time Zone	Click the drop down list to select the time zone you are in.		
Sync Type	Click the drop down list to select the time synchronization type.		
Sync with Browser	Synchronize time with browser.		
Browser Time	Show the current time of browser.		
Set up Manually	Manually configure the system time.		
Sync with NTP Server	Synchronize time with NTP server so as to achieve time 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 3-5-1-2 System Time Parameters

#### 3.5.1.3 SMTP

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

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

Figure 3-5-1-5

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 3-5-1-3 SMTP Setting

#### **Related Topics**

**Events Setting** 

#### 3.5.1.4 Phone

Phone settings involve in call/SMS trigger and SMS alarm for events. This is only applied to gateway with cellular feature.

General	System Time	SMTP	Phone	Email		
Phone <mark>N</mark> umbe	r List					
	Nam	le			Number	Operation
	List1				654321;123456	×
						<b>+</b>

Figure 3-5-1-6

Phone		
Item	Description	
Phone Number List		
Name	Set phone group name.	
Number	Enter the telephone number. Digits, "+" and "-" are allowed. You can divide multiple numbers by ";".	

Table 3-5-1-4 Phone Settings

## **Related Topic**

Connect on Demand

## 3.5.1.5 Email

Email settings involve email alarm for events.

General	System Time	SMTP	Phone	Email		
Email List						
	Nam	е			Email Address	Operation
	list1				sam@user.com;hot@gmail.com	×
						<b>H</b>
Save	l,					

Figure 3-5-1-7

Email	
ltem	Description
Email List	
Name	Set Email group name.
Email Address	Enter the Email address. You can divide multiple Email addresses by ";".

Table 3-5-1-5 Email Settings

#### 3.5.2 User Management

#### 3.5.2.1 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.

Username		admin	
Old Password			
New Password			
Confirm New Passwo	rd		



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

Table 3-5-2-1 Account Information

#### 3.5.2.2 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 •	×
				H

Figure 3-5-2-2

User Management					
ltem	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.				



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

Table 3-5-2-2 User Management

### 3.5.3 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.

#### 3.5.3.1 SNMP

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	Trap	MIB	
Packet Forwarder	SNMP Setting	js				
	Enable					
Network Server	Port		161			
	System Name		24E124FFFEF24660			
Network 🕨	SNMP Version		SNMPv2		~	
Custom 🔻	Location Inform	nation				
System 🔻	Contact Inform	ation				
General Settings						
User Management	Save					
SNMP						

Figure 3-5-3-1

SNMP Settings	SNMP Settings				
ltem	Description				
Enable	Enable or disable SNMP function.				
Port	Set SNMP listened port. Range: 1-65535.				
FUIL	The default port is 161.				
System Name	Fill in the system name to represent the gateway.				
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.				
Location Information	Fill in the location information.				
Contact Information	Fill in the contact information.				

Table 3-5-3-1 SNMP Parameters

## 3.5.3.2 MIB View

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

SNMP	MIB View	VACM	Trap	MIB	
View List					
v	iew Name	View	Filter	View OID	Operation
All		Included	•	] [1	×
system		Included	Ţ	1.3.6.1.2.1.1	
					Đ



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 3-5-3-2 MIB View Parameters

## 3.5.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
SNMP v1 & v2	User List					
Commu	inity	Permission	MIB Vie	ew	Network	Operation
private	Read	l-write	All	•	0.0.0/0	×
public	Read	l-only 🔹	none	•	0.0.0/0	

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

VACM				
Item	Description			
SNMP v1 & v2 Use	er List			
Community	Set the community name.			
Permission	Select from "Read-Only" and "Read-Write".			
MIB View	Select an MIB view to set permissions from the MIB view list.			
Network	The IP address and bits of the external network accessing the MIB view.			
Read-Write	The permission of the specified MIB node is read and write.			
Read-Only	The permission of the specified MIB node is read only.			
SNMP v3 User Lis	t			
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 v				
	list.			
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.			
Table 3-5-3-3 VACM Parameters				

## 3.5.3.4 Trap

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

SNMP	MIB View	VACM	Тгар	MIB
SNMP Trap				
Enable				
SNMP Version		SNMPv2		•
Server Address				
Port				
Name				

Figure 3-5-3-4

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 162.			
NameFill in the group name when using SNMP v1/v2c; fillthe username when using SNMP v3.			
Auth/Priv ModeSelect from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".			

Table 3-5-3-4 Trap Parameters

#### 3.5.3.5 MIB

This section describes how to download MIB files.

SNMP	MIB View	VACM	Trap	MIB
MIB Downloa	d			
MIB File		AGENTX	MIB.txt 🔻	Download

Figure 3-5-3-5

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

Table 3-5-3-5 MIB Download

## 3.5.4 Device Management

You can connect the device to the DeviceHub on this page so as to manage the gateway centrally and remotely. For details refer to DeviceHub User Guide.

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

Figure 3-5-4-1

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

Table 3-5-4-1

## 3.5.5 Events

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

## 3.5.5.1 Events

You can view alarm messages on this page.

Status		Events	Events Setti	ngs		
LoRaWAN		Mark as Read	Delete	Mark Al	as Read De	lete All Alarms
Network	•	St	atus	Туре	Time	Message
System	•	< > 10 •	Go to:	GO		
General Settings						
User Managemei	nt					
AAA						
Device Managem	ient					
Events						

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

Events			
Item	Description		
Mark as Read	Mark the selected event alarm as read.		
Delete	Delete the selected event alarm.		
Mark All as Read	Mark all event alarms as read.		
Delete All Alarms	Delete all event alarms.		
Status	Show the reading status of the event alarms, such as "Read" and "Unread".		
Туре	Show the event type that should be alarmed.		
Time	Show the alarm time.		
Message	Show the alarm content.		

Table 3-5-5-1 Events Parameters

## 3.5.5.2 Events Settings

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

Events	Events Settings	
Events Settings		
Enable		

Phone for Notification	~
Email for Notification	~

Events	Record	Email Email Setting	SMS SMS Setting
Cellular Up			
Cellular Down			
WAN Up			
WAN Down			
VPN Up			
VPN Down			
Power On			

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

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.
Power On	The gateway has powered on.
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 option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure
Linan Setting	the Email group.
SMS	The relevant content of event alarm will be sent out via SMS if
31013	this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to
Sivio Setting	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 3-5-5-2 Events Parameters

#### **Related Topics**

Email Setting Phone Setting

## 3.6 Maintenance

This section describes system maintenance tools and management.

#### 3.6.1 Tools

Troubleshooting tools includes ping and traceroute.

## 3.6.1.1 Ping

Ping tool is engineered to ping outer network.

IP Ping	
Host Ping S	ор

Figure 3-6-1-1

PING		
ltem	Description	
Host	Ping outer network from the gateway.	

Table 3-6-1-1 IP Ping Parameters

## 3.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Ping	Traceroute	Qxdmlog		
Traceroute				
Host			Trace	Stop

Figure 3-6-1-2

Traceroute		
ltem	Description	
Host	Address of the destination host to be detected.	
	Table 3-6-1-2 Traceroute Parameters	

Table 3-6-1-2 Traceroute Parameters

#### 3.6.1.3 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.



Figure 3-6-1-3

## 3.6.2 Schedule

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

Status	<u>^</u>	Schedule				
LoRaWAN	•	Schedule				
		Schedule	Frequency	Hour	Minute	Operation
Network	·					•
System	•	Save				
Maintenance	-					
Tools						
Schedule						

Figure 3-6-2-1

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

Table 3-6-2-1 Schedule Parameters

## 3.6.3 Log

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

#### 3.6.3.1 System Log

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

Download		
File	Log File	Download
Log		
View recent(lines)	20	Ŧ
Thu Jul 18 15:01:25 2019 us	er.notice redis[1859]: Background savi	ing terminated with success
Thu Jul 18 15:06:26 2019 us	er.notice redis[1859]: 10 changes in 30	00 seconds. Saving
Thu Jul 18 15:06:26 2019 us	ser.notice redis[1859]: Background savi	ing started by pid 11683
	ser.notice redis[11683]: DB saved on dis	
	er.notice redis[1859]: Background savi	
Thu Jul 18 15:11:27 2019 us	er.notice redis[1859]: 10 changes in 30	
		ng started by pid 16776
Thu Jul 18 15:11:27 2019 us		
Thu Jul 18 15:11:27 2019 us	er.notice redis[15776]: DB saved on dis	sk
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us	er.notice redis[15776]: DB saved on dis er.notice redis[1859]: Background savi	sk ng terminated with success
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[15776]: DB saved on dis er.notice redis[1859]: Background savi ser.notice redis[1859]: 10 changes in 30	sk ing terminated with success 00 seconds. Saving
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us Thu Jul 18 15:16:28 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[15776]: DB saved on dis er.notice redis[1859]: Background savii ser.notice redis[1859]: 10 changes in 30 ser.notice redis[1859]: Background savi	sk ing terminated with success 00 seconds. Saving ing started by pid 19899
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[15776]: DB saved on dis er.notice redis[1859]: Background savi ser.notice redis[1859]: 10 changes in 30	sk ing terminated with success 00 seconds. Saving ing started by pid 19899 sk

Figure 3-6-3-1

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 3-6-3-1 System Log Parameters

## 3.6.3.2 Log Settings

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

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address			an Al	]
Port		514		
Local Log File				
Storage		local	Ţ	]
Size		1024		КВ
Log Severity		Info	v	]

Figure 3-6-3-2

Log Settings	
Item	Description
Remote Log Server	

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

Table 3-6-3-2 System Log Parameters

## 3.6.4 Upgrade

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

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

Upgrade			
Upgrade			
Firmware Version	60.0.0.33		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade



Upgrade			
Item	Description		
Firmware Version	Show the current firmware version.		
Reset Configuration to	When this option is checked, the gateway will be reset to		
Factory Default	factory defaults after upgrade.		
Upgrade Firmware	Click "Browse" button to select the new firmware file, and		
opgrade Filliware	click "Upgrade" to upgrade firmware.		

Table 3-6-4-1 Upgrade Parameters

## **Related Configuration Example**

Firmware Upgrade

#### 3.6.5 Backup and Restore

This section explains how to create a backup of the whole system configurations to a file, replicate parts of important configuration only for batch backup, restore the config file to the gateway and reset to factory defaults.

Backup and Restore			
Restore Config			
Config File		 Browse	Import
Backup Running-cont	ïg		
Full Backup Ba	tch Backup		
Restore Factory Defa	ults		
Reset			

#### Figure 3-6-5-1

Backup and Restore			
ltem	Description		
Config Tilo	Click "Browse" button to select configuration file, and then click "Import"		
Config File	button to upload the configuration file to the gateway.		
Full Backup	Click "Full Backup" to export the current configuration file to the PC.		
	Click "Batch Backup" to export current configuration except gateway ID		
Batch	of packet forwarder, all embedded NS settings, static IP address of		
Backup	WAN, WLAN settings, user management settings, DeviceHub		
	authentication code, all APP settings.		
Reset	Click "Reset" button to reset factory default settings. gateway will		
πεδει	restart after reset process is done.		

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

#### **Related Configuration Example**

Restore Factory Defaults

#### 3.6.6 Reboot

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

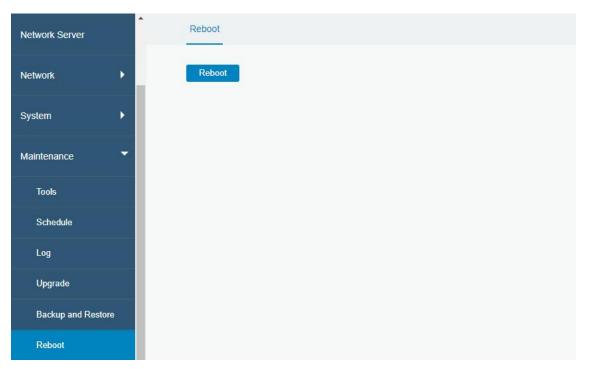


Figure 3-6-6-1

## 3.7 APP

## 3.7.1 Python

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

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

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

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

## 3.7.1.1 Python

Python	AppManager Configuration		Python APP		
Python					
AppManager St	atus	Uninstalled			
SDK Version					
SDK Path					
Available Storag	je	local	~		
SDK Upload				Browse	Install

## Figure 3-7-1-1

Python			
Item Description			
AppMapagar Statua	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 3-7-1-1 Python Parameters

## 3.7.1.2 App Manager Configuration

Python	AppManager Configuration	Python APP	
AppManager			
Enable			
App Managemer	t		
ID	Арр С	ommand Logfile Size(MB	) Uninstall
App Status			
Δ	pp Name	App Version	SDK Version

Figure 3-7-1-2

AppManager Configuration			
Item	Description		
Enable	After enabling Python AppManager, user can click "View" button or 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 3-7-1-2 APP Manager Parameters		

#### Table 3-7-1-2 APP Manager Parameters

# 3.7.1.3 Python App

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

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

Python APP	
Item	Description
App Package	Select App package and import.
App Name	Select App to import configuration.
App Configuration	Select configuration file and import.

Debug File	Export script file.	
Debug Script	Select Python script to be debugged and import.	

Table 3-7-1-3 APP Parameters

## 3.7.2 Node-RED

Node-RED is a flow-based development tool for visual programming and wiring together hardware devices, APIs and online services as part of the Internet of Things. Node-RED provides a web-browser-based flow editor, which can easily wire together flows using the wide range of nodes in the palette. Besides basic nodes, Milesight gateways provide following customized nodes:

- LoRa Input: receive the LoRa data, please ensure the network server mode is enabled before using this node
- LoRa Output: send downlinks to LoRaWAN<sup>®</sup> nodes
- Device Filter: filter out the data of one or more specific LoRaWAN® nodes
- Decoder: decode the Milesight LoRaWAN® end nodes data
- GW Info: monitor alarm messages of gateway, please ensure the event detection is enabled in "General -> Events -> Events Settings"
- Email Output: send LoRa data or gateway alarms via email
- SMS Input: receive SMS message. This only works when cellular is connected
- SMS Output: send SMS message. This only works when cellular is connected

Status		Node-RED		
Packet Forwarder		Node-RED		
Network Server		Enable Node-RED Version	1.2.9	Launch
Protocol Integration	•	Node Library Version Upgrade Node Library	1.0.11	Browse Upgrade
Network	۲	All Flows	Export	
System	•	Restore Factory Defaults Save	Reset	
Maintenance	۲	Save		
APP	-			
Python				
Node-RED				

## 3.7.2.1 Node-RED

Figure 3-7-2-1

Node-RED					
Item	Description				
Enable	Enable the Node-RED.				
Launch	Click to launch the web GUI of Node-RED.				
Node-RED Version	Show the version of the Node-RED. The Node-RED version				
	can be upgraded only when you upgrade the gateway.				
Node Library Version	Show the version of the node library.				
Upgrade Node Library	Upgrade the node library by importing the library package.				
All Flows Export	Export all flows as a JSON format file.				
Restore Factory Default	Erase all flows data of Node-RED.				

Table 3-7-2-1 Node-RED Parameters

## **Related Configuration Example**

Node-RED

# **Chapter 4 Application Examples**

## **4.1 Restore Factory Defaults**

### 4.1.1 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.

Backup and Re	store			
Restore Config				
Config File			Browse	e Import
Backup Runnin	g-config			
Full Backup	Batch Backu	p		
Restore Factory	/ Defaults			
Reset				
Backup Running-config				
Backup				
Restore Factory Defaults				
Reset			×	
	Reset operation will era:	se all configuration data	a on Router and	
	reset the system	n to factory defaults. Co	ontinue?	
	Rese	t 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 SYS light staticly and the login page pops up again, which means the gateway has already been reset to factory defaults successfully.

#### **Related Topic**

**Restore Factory Defaults** 

#### 4.1.2 Via Hardware

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

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

## 4.2 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade gateway firmware. Gateway firmware file suffix is ".bin".

After getting firmware file 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.

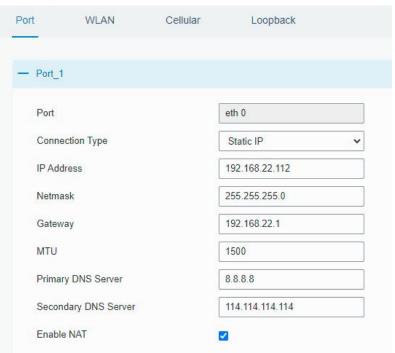
Upgrade			
Upgrade			
Firmware Version	60.0.0.33		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade
Please keep	the power on during upgrade.		
	l i i i i i i i i i i i i i i i i i i i		

#### **Related Topic**

<u>Upgrade</u>

#### **4.3 Ethernet Connection**

- 1. Go to "Network > Interface > Port" page to select the connection type and configure Ethernet port configuration.
- 2. Click "Save & Apply" for configuration to take effect.



3. Connect Ethernet port of gateway to devices like router or modem.

4. Log in the web GUI via the newly assigned IP address and go to "Status -> Network" to check Ethernet port status.

(	Overview	Packet	Forward		Network	WLAN	VPN	Host List		
l w	AN									
	Port	Status	Туре	IP Address	Ne	tmask	Gateway		DNS	Duration
	eth 0	up	Static	192.168.22.112	255.2	255.255.0	192.168.22	.1	8.8.8.8	1days,02h 34m 22s

#### **Related Topic**

Port Setting

## **4.4 Cellular Connection**

1. Go to "Network > Interface > Cellular > Cellular Setting" and configure the cellular info.

2. Choose relevant network type.

Port	WLAN	Cellular	Loopback
Cellular S	etting		
Enable			
Network Type		Auto	~
APN			
Username			
Password		73	
Access Nu	mber		
PIN Code			
Authentication Type		Auto	~
Roaming			
SMS Cente	er		
Connectio	on 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		EC25EC	GAR06A07M1	IG	
Signal Level		23asu (-6	67dBm)		
Register Status		Registere	ed (Home netv	v <mark>or</mark> k)	
IMEI		8604250	47368939		
IMSI		4600194	25301842		
ICCID		8986011	78380099341	20	
ISP		CHN-UN	ICOM		
Network Type		LTE			
PLMN ID					
LAC		5922			
Cell ID		340db83			
Network					
Status		Connecte	ed		
IP Address		10.132.1	32.59		
Netmask		255.255.	255.240		
Gateway		10.132.1	32.60		

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

# 4.5 Wi-Fi Application Example

#### 4.5.1 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		AP	~
SSID Broad	cast		
AP Isolation			
Radio Type		802.11n	(2.4GHz) 🗸
Channel		Auto	~
SSID		Gateway	_F1200F
BSSID		24:e1:24	:f1:20:0f
Encryption N	Node	No Encr	yption 🗸
Bandwidth		20MHz	~
Max Client N	lumber	10	

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

2. Use a smart phone to connect the access point of gateway. 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
WLAN Status					
Wireless Status		Enabled			
MAC Address		24:e1:24:f1:20:0f			
Interface Type		AP			
SSID		Gateway_F1200F			
Channel		Auto			
Encryption Type		No Encryption			
Status		Up			
IP Address		<mark>1</mark> 92.168.1.1			
Netmask		255.255.255.0			
Connection Duration		0 days, 02 <mark>:40:52</mark>			

## 4.5.2 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	Loop	back			
< GoBack								
SSID		Channel	Signal	Cipher	BSSID	Security	Frequency	
AAA		Auto	-61dBm	AES	24:e1:24:f0:c4:13	WPA-PSK/WPA2-PSK	2412MHz	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	r.	Client	~	Scan
SSID		AAA		
BSSID		24:e1:24:t	f0:c4:13	
Encryption	Mode	WPA-PSI	K/WPA2-PSK V	
Cipher		AES	~	
Key		*******		
IP Setting				
Protocol		DHCP CI	lient 🗸	

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:de:14		
Interface Type		Client		
SSID		AAA		
Channel		Auto		
Encryption Type		WPA-PSK/WPA2-PSK		
Cipher		AES		
Status		Connected		
IP Address		192.168.1.145		
Netmask		255.255.255.0		
Connection Duration		0 days, 02:44:45		

## **Related Topic**

WLAN Setting

WLAN Status

# 4.6 Packet Forwarder Configuration

UG65 gateway has installed multiple packet forwarders including Semtech, Basic station, Chirpstack-Generic MQTT broker, etc. Before connecting make sure the gateway has connected to network.

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

General	Radios	Advanced	Custom	Traffic		
General Setting						
Gateway EUI	24E124FFFE	F12257				
Gateway ID	24E124FFF	EF12257				
Frequency-Sync	Disabled	*				
Multi-Destination						
ID	Enable	Туре		Server Address	Connect Status	Operation
0	Enabled	Embedde	d NS	localhost	Connected	
						æ

2. Click 💻 to add a new network server. Fill in the network server information and

enable this server.

Туре	Semtech 🗸
Server Address	eu1.cloud.thethings.network 💌
Port Up	1700
Port Down	1700

3. Go to "Packet Forwarder -> Radio" page to configure antenna type, center frequency and channels. The channels of the gateway and network server need to be the same.

egion		US915		~
	Name			Center Frequency/MHz
	Radio 0		[	904.3
	Radio 1			905.0
Multi Channels Settin	g			
Enable	Index	Radio		Frequency/MHz
	0	Radio 0	~	903.9
	1	Radio 0	~	904.1
	2	Radio 0	~	904.3
	3	Radio 0	~	904.5
	4	Radio 1	~	904.7
	5	Radio 1	~	904.9
	6	Radio 1	*	905.1
				905.3

4. Add the gateway on network server page. For more details about the network server connection please refer to <u>Milesight IoT Support portal</u>.

5. Go to "Traffic" page to view the data communication of UG65.

eneral	Radi	ios Adv	anced	Custom	Traffic			
ffic Sett	ing							
Stop	c	lear						
Rfch	Direction	Time	Ticks	Frequency	Datarate	Coderate	RSSI	SNR
0	up	05:57:30	212136749 3	903.9	SF10BW125	4/5	-51	13.2
0	up	05:57:29	211944923 1	904.5	SF7BW125	4/5	-95	8.5
0	up	05:57:13	210431205 7	904.6	SF8BW500	4/5	-51	11.5
0	up	05:57:06	209699855 6	903.9	SF7BW125	4/5	-65	14.2
	ffic Sett Stop Rfch 0 0	ffic Setting       Stop     C       Rfch     Direction       0     up       0     up       0     up	Stop     Clear       Rfch     Direction     Time       0     up     05:57:30       0     up     05:57:29       0     up     05:57:13	Stop         Clear           Rfch         Direction         Time         Ticks           0         up         05:57:30         212136749         3           0         up         05:57:29         211944923         3           0         up         05:57:29         211944923         1           0         up         05:57:13         210431205         7           0         up         05:57:06         209699855	Clear         Clear         Rfch       Direction       Time       Ticks       Frequency         0       up       05:57:30       212136749 3       903.9         0       up       05:57:29       211944923 1       904.5         0       up       05:57:13       210431205 7       904.6         0       up       05:57:06       209699855       903.9	Stop         Clear           Rfch         Direction         Time         Ticks         Frequency         Datarate           0         up         05:57:30         212136749 3         903.9         SF10BW125           0         up         05:57:29         211944923 1         904.5         SF7BW125           0         up         05:57:13         210431205 7         904.6         SF8BW500           0         up         05:57:06         209699855         903.9         SF7BW125	Stop         Clear           Rfch         Direction         Time         Ticks         Frequency         Datarate         Coderate           0         up         05:57:30         212136749 3         903.9         SF10BW125         4/5           0         up         05:57:29         211944923 1         904.5         SF7BW125         4/5           0         up         05:57:13         210431205 7         904.6         SF8BW500         4/5           0         up         05:57:13         209699855 903.9         903.9         SF7BW125         4/5	Stop         Clear           Rfch         Direction         Time         Ticks         Frequency         Datarate         Coderate         RSSI           0         up         05:57:30         212136749 3         903.9         SF10BW125         4/5         -51           0         up         05:57:29         211944923 1         904.5         SF7BW125         4/5         -95           0         up         05:57:13         210431205 7         904.6         SF8BW500         4/5         -51           0         up         05:57:06         209699855         903.9         SF7BW125         4/5         -65

# 4.7 Connect to Milesight IoT Cloud

1. Go to "Packet Forwarder->General" page to enable the embedded network server.

Status		General	Radios	Advanced	Custom	Traffic		
Packet Forwarder		General Setting						
Network Server		Gateway EUI Gateway ID	24E124FFF 24E124FF		]			
Network	•	Frequency-Sync	Disabled		•			
System	۲	Multi-Destination						
		ID	Enable	Ту	ре	Server Address	Connect Status	Operation
Maintenance	<b>`</b>	0	Enabled	Ember	ded NS	localhost	Connected	$\mathscr{U}$ $\times$
APP	×							8

2. Go to "Packet Forwarder-> Radio" page to select the antenna type, center frequency and channels. The channels of the gateway and nodes need to be the same.

Region		US915	~
	Name		Center Frequency/MHz
	Radio 0		904.3
	Radio 1		905.0
Multi Channels Settin	g		
Enable	Index	Radio	Frequency/MHz
	0	Radio 0	♥ 903.9
	1	Radio 0	♥ 904.1
	2	Radio 0	904.3
	3	Radio 0	904.5
	4	Radio 1	♥ 904.7
	5	Radio 1	904.9
	6	Radio 1	905.1
	7	Radio 1	♥ 905.3

3. Go to "Network Server"  $\rightarrow$  "General" page to enable the network server and "Cloud mode", then select "Milesight IoT Cloud".

Status	General	Applications	Profiles	Device
Packet Forwarder	General Setting			
Network Server	Enable Cloud Mode			
Network •	NetID	Milesight	t IoT Cloud 🗸 🗸	]
System	Join Delay	5		] ] sec
Maintenance	RX1 Delay	8760-0-0		] sec ] hh-mm-ss
APP >	Log Level	info	v	]

4. Log in the Milesight IoT Cloud. Then go to "My Devices" page and click "+New Devices" to add gateway to Milesight IoT Cloud via SN. Gateway will be added under "Gateways" menu.

Dashboard	Devic	es	Gat	eways	History	+				
My Devices	Searc	sh	C	(	⊘ Normal 1	Alarm 1	≥ 1 ⊗	Inactive 3		+ New Device
Map Triggers		$\otimes$	真实设备-EN 6136A39023	Add Device			×		e	© M ()
Reports		$\otimes$	UC3X52-虚 61151109	* SN * Name				sociated with your	-	@ M @
Event Center 30 Sharing Center		.HG	UC3X5 6123A124	* Name					15 minutes ago	© <u>v</u> ©
Me		ä	AM102- 6128A2175	CO2	TVOC	Cancel Confirm Barometric Pres		ux ination	a few seconds ago	@ k ()
			4	27℃ Temperature	<b>51%</b> Humidity	<b>O</b> Activity Level (F		<b>lux</b> umination		
≡										

5. The gateway is online on Milesight IoT Cloud.

<li>② Dashboard</li>	Devices	Gatewa	ys +			
My Devices	Search	٩		⊘ Normal 1 🕅 Offline 0 ⊗ Inact	tive 0	+ New Devices
Map		Status	Name	Associated Devices (Joined /Not Joined /Failed)	Last Updated	
Reports			UG Gateway 21793129987	0/1/0 Detail	2 minutes ago	© <u>M</u> ©
Event Center 94						

# 4.8 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.

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

Applications		
Name	cloud	
Description	cloud	

- 3. Click "Save" to create this application.
- 4. Click 🛄 to add a data transmission type.

## **HTTP or HTTPS:**

URL

Step 1: select	HTTP or HTTPS	as transmission	protocol.
----------------	---------------	-----------------	-----------

Туре	HTTP	•

Step 2: Enter the destination URL. Different types of data can be sent to different URLs.

Enter the header name and header value if there is user credentials when accessing the HTTP(s) server.

HTTP Header			
	Header Name	Header Value	Operation
			×
			e

## MQTT:

Step 1: select the transmission protocol as MQTT.

Tuno	MOTT	
туре	MQTI	

Step 2: Fill in MQTT broker general settings.

General	
Broker Address	
Broker Port	
Client ID	
Connection Timeout/s	30
Keep Alive Interval/s	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 select mode and import CA certificate, client certificate and client key file for authentication.

TLS	
Enable	2
Mode	Self signed certificates
CA File	Browse Import Delete
Client Certificate File	Browse Import Delete
Client Key File	Browse Import Delete

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

Data Type	topic		
Uplink data	devices/UR67/messages/event:	QoS 0	~
Downlink data		QoS 0	~
Multicast downlink data		QoS 0	~
Join notification		QoS 0	~
ACK notification		QoS 0	~
Error notification		QoS 0	~

# 4.9 Device Configuration

Go to "Device" page and click "Add" to add LoRaWAN<sup>®</sup> node devices. Please select correct device profile according to device type.

General	Applications	Profiles	Device G	Sateways	Packets	
Device						
Add	Bulk Import D	lelete All			Search	Q
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
		No mate	ching records found			
	Device Name					
			lora-sens			
	Description Device EUI			escription of you	Ir node	
	Device-Profile			00000000		
	Application		ClassA-C		~	
	Paylod Codec		cloud		-	
	fPort		1			
	Frame-counter	Validation				
	Application Key					
	Device Address					
	Network Sessio	n Key				
	Application Ses	sion Key				
	Uplink Frame-co	punter	0			
	Downlink Frame	e-counter	0			
			Save & Ap	nlv		

You can also click "Bulk Import" if you want to add many nodes all at once.

Import File	Browse	Import	Template Download

Click "Template Download" to download template file and add device information to this file. Application and device profile should be the same as you created on web page.

- 24	A	В	C	D	E	F	G	Н	1
1	name	description	deveui	application	deviceprofile	appkey	devaddr	appskey	nwkskey
2	24e1242191323266		24e1242191323266	cloud	ClassC-OTAA	112233445566778899aa112233445566			
3									
4									
5									

Import this file to add bulks of devices.

## 4.10 Send Data to Device

1. Go to "Network Server" > "Packets", check the packet in the network server list to make sure that the device has joined the network successful.

1122612191	868100000	SF7BW125		1.75	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

2. Fill in the device EUI or select the multicast group which you need to send downlinks. Then fill in the downlink commands, ports.

Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII 🔻	15	15	V



4. Check the packet in the network server list to make sure that the device has received this message successful. It's suggested to enable "Confirmed". Multicast feature does not support confirmed downlinks.

Device EUI	Туре	Payload	Fport	Confirme
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 constantly receive packets.

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. If the packet record is white, it means the packet has been delivered successfully.

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

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

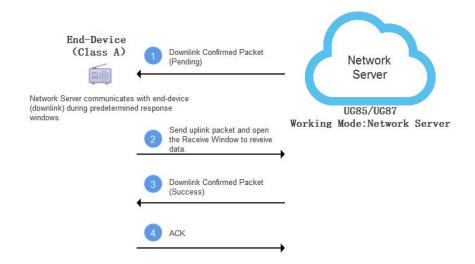
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
11226121913	868300000	SF10BW125		-	0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	, 0
112261219	869525000	SF12BW125	1	-	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125		-	0	1	DnUnc	2019-08-06T09:22:49+08:00	0

P	ackets Details		×
re	Dev Addr	07e7	Î
6	GwEUI	24e124ff	
61	AppEUI	557240	
	DevEUI	1122612191311123	
61	Immediately	23	
64	Timestamp	874346044	
61	Туре	UpCnf	
	Adr	false	
6	AdrAcKReq	false	
61	Ack	true	
6	Fcnt	21	
	Fport	55	
6	Modulation	LORA	<b>*</b>

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

twork Server										Show the signal-noise ratio.
Clear								Search	Q	RSSI Show the received signal strength indicator.
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details	Size Show the size of packet.
1122612191311123	868300000	SF10BW125	1	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0	Font
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0	Show the frame counter.
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	0	Type Show the type of the paceket:
1122612191311123	868100000	SF10BW125	-	70	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success	JnAcc - Join Accept Packet JnReq - Join Request Packet
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0	UpUnc - Uplink Unconfirmed Packet
1122612191311123	0				6	18	DnCnf	Pending	0	UpCnf - Uplink Confirmed Packet ACK response from network requested
1122612191311123	868500000	SF10BW125	1		0	17	DnUnc	2019-08-06T09:47:38+08:00	0	DnUnc - Downlink Unconfirmed Packet
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0	DnCnf - Downlink Confirmed Packet- ACK response from end-
1122612191311123	868100000	SF10BW125	-	2	0	16	DnUnc	2019-08-06T09:46:38+08:00	0	device requested
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0	Time Show the time of packet was sen
								Manual Refre	ch v Refrech	or received

# If the device's class type is Class A, only after the device sends out an uplink packet will the



Clear								Search	O,
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
1122612191311123	868300000	SF10BW125	2	12	0	19	DnUnc	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0
1122612191311123	868300000	SF10BW125	10.8	-76	64	1	UpCnf	2019-08-06T09:49:38+08:00	0
1122612191311123	868100000	SF10BW125	means	the d	evice	has re	ceived t	2019-08-06T09:48:43+08:00 he packet you send.	0
11226 <mark>1219131112</mark> 3	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0
1122612191311123	0				6	18	DnCnf		0
11226 <mark>1</mark> 2191311123	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	10	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

# 4.11 Node-RED

#### 4.11.1 Start the Node-RED

1. Go to "App > Node-RED" to enable the Node-RED feature.

2. After enabled, click "Launch" to go to the Node-RED web GUI and to log in with the same

username and password as gateway.

RED				
		Usemame:		
	Node-RED		Login	

# 4.11.2 Send Data by Email

## **Application Example**

Send AM104 device data by Email.

ha	пу	test1	test	chenpan	test2	Flow 1	+ 😑	∰ debug	i i	<i>∎</i> ¥	٥
							<b></b>		<b>▼</b> s	elected node	es 🛍
								2021/4/30下午4: msg.payload : str "A4L//w=="		5034ec07.ffa	a3c4
	() LoRa Input	<b>A</b> M		AM 100 Decoder	AM100 Data to Email			2021/4/30 T f 4: msg.payload : O * object temperatur humidity: * illuminar 0: 1 1: 6 2: 1 actuation:	bject e: 30.7 52.5 e_sensor:		91754
								2021/4/30下午4: Email msg : string[8] "successs"	33:15 node:	AM100 Data	i to

## **Configuration Steps**

1. Add a "LoRa Input" node. Before adding please ensure network server mode is enabled and LoRaWAN devices have joined the network.

2. If you add many devices and only need one device data, add "Device Filter" node behind the "LoRa Input" and type the device EUI.

harry	test1	test	chenpan	Edit Device Filte	er node	
				Delete		Cancel Done
				Properties		• 2 12
				Name	AM100	
				Device EUI	24E124127A270222	) +
(	LoRa Input					

3. Add a "Decoder" node to decode the Milesight sensor data.

harry	test1	test	chenpan	Edit Decoder no	ode	
				Delete		Cancel Done
				© Properties		• 6 11
	LoRa Input	AM100		Name	AM 100 Decoder	
	Lord input y		100 D00000	Device Type	AM100 Series 🗸	

4. Add an "Email Output" and type the SMTP client settings, destination email address and contents. Example content:

*The time is {{time}} Deveui is {{deveui}} Humidity is {{payload.humidity}}* 

harry	test1	test	chenpan	Edit Email Outpo	ut node		
				Delete		Cancel	Done
				© Properties		¢	8 19
				Name	AM100 Data to Email		
	LoRa Input	AM100 9-	AM 100 Decoder	SMTP Option	Custom ~		
				User ID	@milesight.com		
			msg.payload	Password			
				SMTP Server Address	smtp.exmail.qq.com		
				Port [1-65535]	25		
				Enable TLS			
	WAN Up			То	@milesight.com	+	
				Topic	AM100 Data		
				Payload	The time is {{time}} Deveui is {{deveui}} counter is {{payload.humidity}}	<i>b</i>	

## Note:

When you select SMTP Option as "Same as Gateway", go to "System -> General Settings
 -> SMTP" to configure the SMTP clients.

2) Basic format to call LoRaWAN node data is *{{property name}}*, you can click "Help" page for more info about the Email or SMS payload format.

3) If you need to check the output content in every node, please add debug node.

5. After completing the configuration, click "Deploy" to save all your configuration.

harry	test1	test chenpan test2	test2	Flow 1	+ ≔ # de	∰ debug	8	i 🖉	<u>Ř</u> 0			
							-			r selected	nodes	8
								2021/4/30下午4: msg.payload:str "A4L//w=="		ide: 5034e	:07.ffa3c4	
III LoRa Inpi	ut ç Al	M100 9 000	AM 100 Decoder	AM100 Data to Email								
		m	sg.payload									

6. When AM104 sends data to gateway, gateway will transfer the data to email.

## AM100 Data 📩

```
From @milesight.com>
To @milesight.com>
Time: 2021年4月30日 (周五) 17:13 ①
Size: 2 KB
```

The time is 2021-04-30T09:13:13.872942Z Deveui is 24e124127a270222 Temperature is 30.4 Humidity is 52

2021-04

# **Related Topic**

Node-RED

[END]