

Outdoor LoRaWAN[®] Gateway UG67 User Guide

Milesight IoT

Preface

Thanks for choosing Milesight UG67 LoRaWAN[®] gateway. UG67 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 UG67 LoRaWAN[®] gateway. You can refer to it for detailed functionality and gateway configuration.

Readers

This guide is mainly intended for the following users:

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

© 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
UG67 Datasheet	Datasheet for UG67 LoRaWAN® gateway.
UG67 Quick Start Guide	Quick Installation Guide for UG67 LoRaWAN [®] gateway.

Declaration of Conformity

UG67 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.







For assistance, please contact Milesight technical support: Email: iot.support@milesight.com Tel: 86-592-5085280 Fax: 86-592-5023065

Revision History

Date	Doc Version	Description
Dec. 31, 2020	V1.0	Initial version
		1. Support LoRaWAN [®] Class B
		2. Add Node-RED feature
Apr. 30, 2021	V1.1	3. Add Noise-Analyzer feature
		4. Add Multicast Groups feature
		5. Add application examples
		1. Support Yeastar Workplace platform
Aug. 04, 0001	V1.2	integration
Aug. 24, 2021	V I.Z	2. Delete Package Forward status page
		3. Phone & Email webpage update

Contents

3.3.2.3 DMZ	57
3.3.2.4 Port Mapping	57
3.3.2.5 MAC Binding	58
3.3.3 DHCP	59
3.3.4 DDNS	60
3.3.5 Link Failover	61
3.3.5.1 SLA	61
3.3.5.2 Track	62
3.3.5.3 WAN Failover	63
3.3.6 VPN	64
3.3.6.1 DMVPN	64
3.3.6.2 IPSec	65
3.3.6.3 GRE	68
3.3.6.4 L2TP	69
3.3.6.5 PPTP	71
3.3.6.6 OpenVPN Client	73
3.3.6.7 OpenVPN Server	74
3.3.6.8 Certifications	76
3.4 System	
3.4.1 General Settings	78
3.4.1.1 General	78
3.4.1.2 System Time	
3.4.1.3 SMTP	
3.4.1.4 Phone	81
3.4.1.5 Email	
3.4.2 User Management	83
3.4.2.1 Account	
3.4.2.2 User Management	
3.4.3 SNMP	
3.4.3.1 SNMP	84
3.4.3.2 MIB View	
3.4.3.3 VACM	85
3.4.3.4 Trap	
3.4.3.5 MIB	87
3.4.5 Device Management	87
3.4.6 Events	
3.4.6.1 Events	
3.4.6.2 Events Settings	
3.5 Maintenance	
3.5.1 Tools	
3.5.1.1 Ping	
3.5.1.2 Traceroute	
3.5.1.3 Qxdmlog	

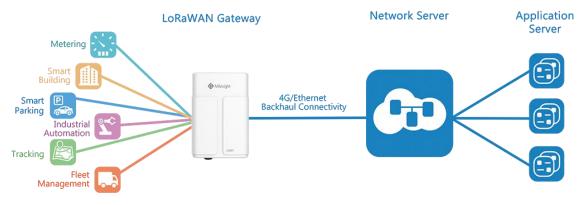
3.5.3 Log	92
3.5.3.1 System Log	92
3.5.3.2 Log Settings	
3.5.4 Upgrade	
3.5.5 Backup and Restore	
3.5.6 Reboot	
3.6 APP	96
3.6.1 Python	96
3.6.1.1 Python	
3.6.1.2 App Manager Configuration	
3.6.1.3 Python App	
3.6.2 Node-RED	
3.6.2.1 Node-RED	
Chapter 4 Application Examples	100
4.1 Restore Factory Defaults	100
4.1.1 Via Web Interface	
4.1.2 Via Hardware	
4.2 Firmware Upgrade	101
4.3 Ethernet Connection	102
4.4 Cellular Connection	103
4.5 Wi-Fi Application Example	
4.5.1 AP Mode	104
4.5.2 Client Mode	106
4.6 Packet Forwarder Configuration	107
4.7 Connect UG67 to Milesight IoT Cloud	
4.8 Application Configuration	
4.9 Device Configuration	113
4.10 Send Data to Device	
4.11 Node-RED	
4.11.1 Start the Node-RED	116
4.11.2 Send Data by Email	117

Chapter 1 Product Introduction

1.1 Overview

UG67 is a robust 8-channel outdoor LoRaWAN[®] gateway. Adopting SX1302 LoRa chip and high-performance quad-core CPU, UG67 supports connection with more than 2000 nodes. UG67 has line of sight up to 15 km and can cover about 2km in urbanized environment, which is ideally suited to smart office, smart building and many other outdoor applications.

UG67 supports not only multiple back-haul backups with Ethernet, Wi-Fi and cellular, but also has integrated mainstream network servers (such as The Things Industries, 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 1.5GHz with low power consumption, and 8GB eMMC available to support more applications
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

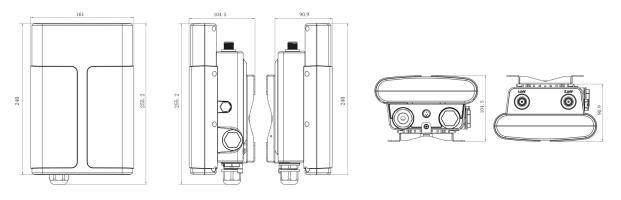
Hardware System	
CPU	Quad-core 1.5GHz, 64-bit ARM Cortex-A53
Memory	8 GB eMMC Flash, 512 MB DDR4 RAM
LoRaWAN	
A	2 × Internal Antennas +
Antenna	$2 \times 50 \Omega$ N-Female External Connectors
Channel	8
Frequency Band	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923/AS923-2
Sensitivity	-140dBm Sensitivity @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)
Data Rate	10/100/1000 Mbps (auto-sensing)

1.3 Specifications

Interface	Auto MDI/MDIX	
Mode	Full or half duplex (auto-sensing)	
Wi-Fi Interfaces		
Antenna	Fully Integrated and Internal Antenna	
Standards	IEEE 802.11 b/g/n	
	802.11b: 18 dBm +/-2.0 dBm (11 Mbps)	
	802.11g: 15 dBm +/-2.0 dBm (6 Mbps)	
	802.11g: 15 dBm +/-2.0 dBm (54 Mbps)	
Tx Power	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS0_HT20)	
	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS7_HT20)	
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS0_HT40)	
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS7_HT40)	
Cellular Interfaces	(Optional)	
Antenna	Internal Antenna	
SIM Slots	1	
GPS		
Antenna	Internal Antenna	
Concitivity	-167dBm@Tracking, -149dBm@Acquisition,	
Sensitivity	-161dBm@Re-acquisition	
Position Accuracy	<2.5m CEP	
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	
Арр	Python SDK, Node-RED	
Power Supply and	Consumption	
Power Supply	1. 1 × 802.3 af PoE Input	
Fower Suppry	2. 12 VDC with M12 Connector	
Consumption	Typical 3.6W, Max 4.8W	
Physical Character	istics	
Ingress Protection	IP67	
Dimensions	250 x 172 x 92 mm	

Mounting	Wall or Pole Mounting
Others	
Reset Button	1 × RST
LED Indicators	1 × SYS, 1 × LoRa, 1 × LTE
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 UG67. Username: **admin** Password: **password**

2.1 Wireless Access

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".

	Milesight	
1	Username	
۵	Password	
	Login	

() English

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. You can also skip the instructions. 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.

		Fo	r your device security.	please change the d	lefault password			
Status	Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List	Help
Status								Model
Packet Forwarder	System Informa	ation						Show the model name of router.
	Model		UG67-L00E-470M					Region Show the Region of router.
Network Server	Region		CN470					Serial Number
Network	Serial Number		6222A3243835					Show the serial number of router.
	Firmware Version	1	60.0.0.23					Firmware Version
System 🕨	Hardware Version	n	V1.0					Show the current firmware version of router.
	Local Time		2020-12-14 17:05:0	15 Monday				Hardware Version
Maintenance	Uptime		4days,05:52:48					Show the current hardware version of router.
APP	CPU Load		2%					Local Time
APP P	RAM (Capacity/A	vailable)	512MB/77MB(15.04	4%)				Show the current local time of system.
	eMMC (Capacity	/Available)	3.0G/2.7G(89.74%)					Uptime
	GPS	Available)	-			Manual R	efresh 🗸 Refresh	Show the information on long the router has been running.

2.2 Wired Access

Connect PC to UG67 ETH port 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).

A Star Network	and Internet > Network and Sharing Center	5 v	Search Control Panel		
Control Panel Home	View your basic network inform				
Change adapter settings	View your active networks				
Change advanced sharing settings	Yeastar5G Private network		Access type: Internet HomeGroup: Ready to create Connections: M Wi-Fi (Yeastar5G)		
	ldentifying	Access t Connect			
	Change your networking settings				
	Set up a new connection or ne Set up a broadband, dial-up, o		Ethernet		
	Troubleshoot problems Diagnose and repair network p	roblems, or get troubles	shooting information.		
See also					
HomeGroup					
Infrared					
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.



General	
	ed automatically if your network supports need to ask your network administrator
O Obtain an IP address auto	omatically
• Use the following IP addr	ess:
IP address:	192 . 168 . 23 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 23 . 150
Obtain DNS server addres	ss automatically
Use the following DNS ser	
Preferred DNS server:	8.8.8.8
Alternative DNS server:	
Validate settings upon ex	kit 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.

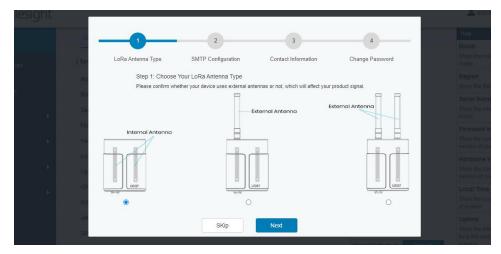
4. Enter the username and password, click "Login".

	Milesight	
1	Username	
A	Password	
	Login	

() English

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. You can also skip the instructions. 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.

		Fo	r your device security,	please change the d	efault password			
Status	Overview	Packet Forward	Cellular	Network	WLAN	VPN	Host List	Help
								Model
Packet Forwarder	System Inform	ation						Show the model name of router.
	Model		UG67-L00E-470M					Region
Network Server	Dealer		CN470					Show the Region of router.
	Region		CN470					Serial Number
Vetwork	Serial Number		6222A3243835					Show the serial number of router.
NEWOIK	Firmware Versio	in	60.0.0.23					
								Firmware Version Show the current firmware
System	Hardware Versio	n	V1.0					version of router.
	Local Time		2020-12-14 17:05:0	5 Monday				Hardware Version
Maintenance	Uptime		4days,05:52:48					Show the current hardware
								version of router.
APP	CPU Load		2%					Local Time
	RAM (Capacity/	Available)	512MB/77MB(15.04	1%)				Show the current local time of system.
	-11110 (0	···(A··111-1-)	2 000 70(00 740)					
	eMMC (Capacity	y/Available)	3.0G/2.7G(89.74%)					Uptime
	GPS		-			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	UG67-L00E-915M
Region	US915
Serial Number	6222A4983306
Firmware Version	60.0.0.33
Hardware Version	V1.1
Local Time	2021-01-06 10:37:17 Wednesday
Uptime	01:12:19
CPU Load	7%
RAM (Capacity/Available)	512MB/146MB(28.52%)
eMMC (Capacity/Available)	3.0G/2.8G(90.66%)
GPS	

Figure 3-1-1-1

System Information				
Item	Description			
Model	Show the model name of gateway.			
Region	Show the LoRaWAN [®] 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.			
GPS	Show GPS data of the gateway.			
	Table 2-1-1-1 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

Figure 3-1-2-1

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

Table 3-1-2-2 Network Status

3.1.3 Network

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

Overview	C	Cellular	Network	WLAN	VPN Host List		
WAN							
Port	Status	Туре	IP Address	Netmask	Gateway	DNS	Duration
eth 0	up	Static	192.168.22.112	255.255.255.0	192.168.22.1	8.8.8.8	02m 14s

Figure 3-1-3-1

Network	Network				
ltem	Description				
Port	Show the name of the Ethernet port.				
Status	Show the status of the Ethernet port. "Up" refers to a status that WAN is enabled and Ethernet cable is connected. "Down" means Ethernet cable is disconnected or WAN function is disabled.				
Туре	Show the dial-up type of 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:f0:e2:26			
Interface Type		AP			
SSID		Gateway_F0E226			
Channel		Auto			
Encryption Type		No Encryption			
Status		Up			
IP Address		192.168.1.1			
Netmask		255.255.255.0			
Connection Duration		4 days, 21:12:11			

Figure 3-1-4-1

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

Table 3-1-4-1 WLAN Status

Associated Stations		
IP Address	MAC Address	Connection Duration
	Figure 3-1-4-2	
Associated Stations		
ltem	Description	
IP Address	Show the IP address of access	s point or client.
MAC Address	Show the MAC address of the	access point or client.
Connection Duration	Show information on how long connected.	g the Wi-Fi network has been

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.

Cellular	Network	WLAN VPN	Host List
Name	Status	Local IP	Remote IP
pptp_1	Disconnected	20	2
pptp_2	Disconnected	2	2
pptp_3	Disconnected	150	2
Name	Status	Local IP	Remote IP
l2tp_1	Disconnected		2
l2tp_2	Disconnected	-	2
l2tp_3	Disconnected	171	2
	Name pptp_1 pptp_2 pptp_3 Name l2tp_1 l2tp_2	Name Status pptp_1 Disconnected pptp_2 Disconnected pptp_3 Disconnected Name Status I2tp_1 Disconnected	Name Status Local IP pptp_1 Disconnected - pptp_2 Disconnected - pptp_3 Disconnected - Mame Status Local IP 1 Disconnected - 1 Disconnected -

Figure 3-1-5-1

IPsec Tunne	el.			
	Name	Status	Local IP	Remote IP
	ipsec_1	Disconnected	22	÷
	ipsec_2	Disconnected	120	12
	ipsec_3	Disconnected	1000	. 5
OpenVPN C	lient			
	Name	Status	Local IP	Remote IP
	openvpn_1	Disconnected	12	÷
	openvpn_2	Disconnected	1 <u>-</u> 1	12
	openvpn_3	Disconnected	125	- 5

Figure 3-1-5-2

GRE Tunnel				
	Name	Status	Local IP	Remote IP
	gre_1	Disconnected	۵.	
	gre_2	Disconnected	-	-
	gre_3	Disconnected		
DMVPN Tunnel				
	Name	Status	Local IP	Remote IP
	dmvpn	Disconnected	-	

Figure 3-1-5-3

VPN Status		
Item	Description	
Name	Show the name of the VPN tunnel.	
Status	Show the status of the VPN tunnel.	
Local IP	Show the local tunnel IP of VPN tunnel.	
Remote IP	Show the remote tunnel IP of VPN tunnel.	
Table 3-1-5-1 VPN Status		

3.1.6 Host List

You can view the host information on this page.

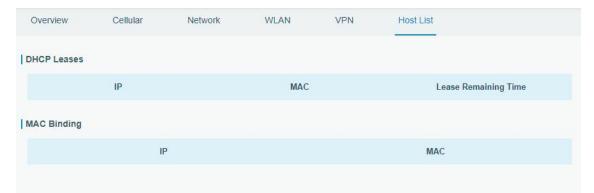
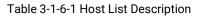


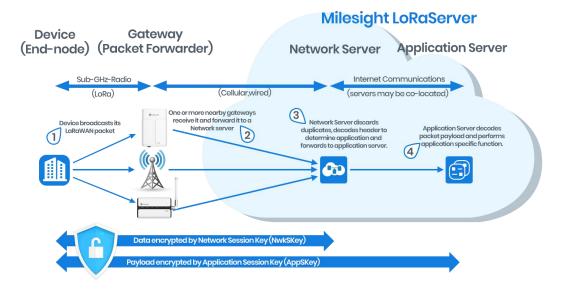
Figure 3-1-6-1

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

list of DHCP service.



3.2 LoRaWAN



3.2.1 Packet Forwarder

3.2.1.1 General

General	Radios	Advanced	1 Cu	stom	Traffic		
General Setting							
Gateway EUI	24E124FFF	EF12257					
Gateway ID	24E124FF	FEF12257					
Frequency-Sync	Disabled		~				
Multi-Destination							
ID	Enable		Туре	Serv	er Address	Connect Status	Operation
0	Enabled	J E	Embedded NS	lo	ocalhost	Connected	2 ×
							E

Figure 3-2-1-1

General Settings			
Item	Description	Default	
		Generated from MAC	
Gateway EUI	Show the identifier of the gateway.	address of the	
		gateway and cannot	

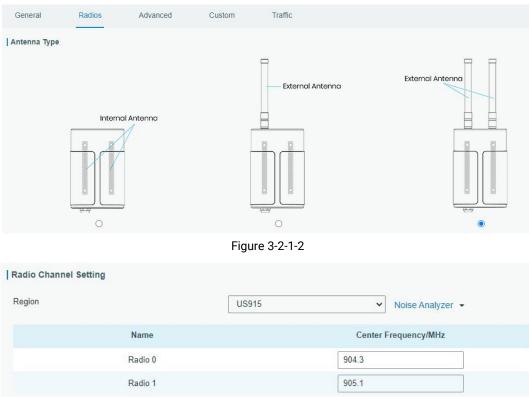
		be changed.
Gateway ID	Fill in the corresponding ID which you've used for register gateway on the remote network server, such as TTN. It is usually the same as gateway EUI and can be changed.	The same as gateway EUI.
Frequency-Sync	Sync frequency configurations from network server by selecting the corresponding ID.	Disabled
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.	Local host
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





Radios-Radio Channel Setting			
ltem	Description	Default	
Antenna	Colort the transmission type of entennes	Internal Antonna	
Туре	Select the transmission type of antennas.	Internal Antenna	

Region	Choose the LoRaWAN [®] frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	
Center Frequency	Radio 0 : supports transmitting and receiving packet. Radio 1 : only supports receiving packet from nodes.	Based on what is specified in the LoRaWAN [®] regional parameters document

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

Multi Channels Setting	
Enable	Index
2	0

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

Figure 3-2-1-4

Radios-Multi Channel Setting			
ltem	Description	Default	
Enable	Click to enable this channel to transmit packets.	Enabled	
Index	Indicate the ordinal of the list.	/	
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0	
Frequency/MHz	Enter the frequency of this channel. Range: center frequency \pm 0.4625.	Based on the LoRaWAN [®] regional document	

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



Figure 3-2-1-5

Radios-LoRa Channel Setting			
Item	Description	Default	
Enable	Click to enable this channel to transmit packets.	Enabled	
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0	
Frequency/MHz	Enter the frequency of this channel.	Based on the	

	Range: center frequency±0.9.	supported frequency
Bandwidth/MHz	Enter the bandwidth of this channel. Recommended value: 125KHz, 250KHz, 500KHz	500KHz
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.	Based on what is specified in the LoRaWAN [®] regional parameters document

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

FSK Channel Setting

Enable	Radio	Frequency/MHz	Bandwidth/KHz	DataRate
2	Radio 0 🔻	924.0	125KHZ 🔻	50000

Figure 3-2-1-6

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

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

3.2.1.3 Noise Analyzer

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.

pported Freq			US915	~	Noise Analyzer
Noise Analyzer	Runnin	g			
Settings	Sweep Freq	Genaral Freq	~		
	0-63: 902.3-914.	9 MHz			
	64-71: 903-914.2	2 MHz			
	Sweep Time	Custom	~		
		24			
		24	h		
		ОК			
		-O- Current Value -O- Weighter	d Average Value		
					- MHz
RSSI/dBm					141112
0	· · ·				
	, ,				
0			Â		
-20 -	, ,	· · · ·	A		
-20	, ,				
-20 -40 -60					

Figure 3	3-2-1-7
----------	---------

Noise Analyzer			
ltem	Description	Default	
Enable	Click to enable noise analyzer feature.	Disabled	
Sweep Freq	Select the frequency sweeping range. General Freq: frequencies based on the LoRaWAN [®] regional parameters document Custom: 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

General	Radios	Advanced	Custom	Traffic
Beacon Setting	g			
Beacon Period		0	~	s
Beacon Freq		508300000		Hz
Beacon Datarate	e	SF10	~]
Beacon Channe	l Number	3	•	
Beacon Freq St	ер	200000		Hz
Beacon Bandwi	dth	125000	~	Hz
Beacon TX Pow	er	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.	14	

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

General	Radios	Advanced	Custom	Traffic	
Custom Confi	guration				
Enable					
				Example	
{					
"SX1302_conf					
	"/dev/spidev0.0",				
"lorawan_publ	ic": true,				
"clksrc": 0,					
	i": 0, /* antenna gair	n, in dBi */			
"antenna_cfg"					
"full_duplex": f					
"precision_tim "enable": false					
"max ts metri					
"nb_symbols":					
},	1				
"radio_0": {					
"enable": true,					
"type": "SX125					
"K" 022000					*

Figure 3-2-1-10

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

3.2.1.6 Traffic

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

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

Figure 3-2-1-11

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

3.2.2.1 General

General	Applications	Profiles	Device
General Settin	g		
Enable			
Cloud Mode			
	Milesight	IoT Cloud	~
NetID	010203		
Join Delay	5		sec
RX1 Delay	1		sec
Lease Time	8760-0-0		hh-mm-s
Log Level	info		~
Channel Plan	Setting		
Channel Plan	CN470		~
Channel Mask			

Figure 3-2-2-1

ltem	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Enabled
Cloud 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 end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time till a successful join 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 S	etting	
Channel Plan	Choose LoRaWAN [®] 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 Mask	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. A bit in the ChMask field set to 1 means that the corresponding channel can be used for uplink transmissions if this channel allows the data rate currently used by the end-device. A bit set to 0 means the corresponding channels should be avoided. US 915 and AU 915 have a 80-bit channel mask for 72 usable channels and EU, AS, IN, KR frequencies have a 16-bit mask for 16 usable channels.	Depend on the gateway's frequency

Table 3-2-2-1 General Parameters

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

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

Figure 3-2-2-2

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

Table 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. All devices with the same "Payload Codec" and data transmission destination can be added under the same application.

General Applications Profiles Device Multicast Groups Gateway Fleet Packets	
General Applications Fronces Device Multicast Gloups Gateway Freet Fackets	
Applications Name Smoke-sensor-app Description a application for smoke sensor Payload Codec None Data Transmission	
Type Operation	
+ Save Cancel	

Figure 3-2-2-3

ltem	Description
Name	Enter the name of the application profile.
INdifie	E.g Smoker-sensor-app.
Description	Enter the description of this application.
Description	E.g a application for smoker sensor.
	Select from: "None", "Cayenne LPP", "Custom".
	None: This mode enables devices not to encode data.
Payload Codec	Cayenne LPP: This mode enables devices to encode data with the
Fayload Codec	Cayenne Low Power Payload (LPP).
	Custom: This mode enables devices to encode data with the decoder
	function and the encoder function which you have entered the code.
Data	Data will be sent to your custom server using the MQTT,HTTP or
Transmission	HTTPS protocol.

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		

Figure 3-2-2-4

TLS			
Enable			
Mode	CA signed server certificate 🗸		
Topic			
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 Settings				
ltem	Description	Default		
General				
Broker Address	MQTT broker address to receive data.			
Broker Port	MQTT broker port to receive data.			
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle message at QoS 1 and 2.			
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535	30		
Keep Alive Interval/s	After the client is connected with the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535	60		
User Creden	tials			
Enable	Enable user credentials.			
Username	The username used for connecting to MQTT broker.			
Password	d The password used for connecting to MQTT broker.			
TLS				
Enable	Enable the TLS encryption in MQTT communication.			
Mode	Select from "Self signed certificates", "CA signed server certificate". CA signed server certificate:verify with the certificate issued by Certificate Authority (CA) that pre-loaded on 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.
Topic	Topic name of the data type using for publish.
	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,
	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
			+
URL			
	Data Type	URL	
	Uplink data		
	Join notification		
	ACK notification		
	Error notification		

Figure 3-2-2-6

HTTP/HTTPS Settings			
Description			
A core set of fields in HTTP header.			
Value of the HTTP header.			
Data type sent to HTTP/HTTPS server.			
Topic name of the data type using for publish.			
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 Profiles

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

You can e	dit the device	e profil	e by clicking	or creat	e a new devic	e profile by clicking
±.						
General	Applications	Profiles	Device	Multicast Groups	Gateway Fleet	Packets
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	
	node		0	OTAA	Class A Class C	
						H

Figure 3-2-2-7

Device Profiles		
Name		
Max TXPower	0	
Join Type	OTAA	~
Class Type	Class A 🗌 Class	B 🗌 Class C
Advanced		



Device Profiles Settings			
ltem	Description	Default	
Name	Enter the name of the device profile. E.g. Smoker-sensor-app.	Null	
Max TXPower	Enter the maximum transmit power. The TXPower indicates power levels relative to the Max EIRP level of the end-device. 0 means using the max EIRP. EIRP refers to the Equivalent Isotropically Radiated Power.	0	
Join Type	Select from: "OTAA" and "ABP". OTAA:Over-the-Air Activation.	ΟΤΑΑ	

	For over-the-air activation, end-devices must follow a join procedure prior to participating in data exchanges with the network server. An end-device has to go through a new join procedure every time as it has lost the session context information. ABP: Activation by Personalization. Under certain circumstances, end-devices can be activated by personalization. Activation by personalization directly ties an end-device to a specific network bypassing the join request - join accept procedure.	
Class Type	Device type is Class A by default. Users can check the box of Class 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 3-2-2-6 Device Profiles Setting Parameters

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



Device Profile Advanced Settings			
ltem	Description	Default	
MAC Version	Choose the version of the LoRaWAN [®] supported by the end-device.	1.0.2	
Regional Parameter Revision	Revision of the Regional Parameters document supported by the end-device.	В	
RX1 Datarate Offset	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 [®] regional	
RX2 Channel	RX2 channel frequency which used for the RX2	parameters document	

Frequency	receive-window.	
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN [®] regional parameters document.	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 C.	Class B: 10 Class C: 0

Table 3-2-2-7 Device Profiles Advanced Setting Parameters

3.2.2.4 Device

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

General	Applications	Profiles Devic	Ce Multicast Groups	Gateway Fleet	Packets		
evice							
Add	Bulk Import	Delete All				Search	(
D	evice Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
24E1	24414B032563	24E124414B032563	classB	cloud	11 days ago	~	2 ×
24E1	124414A501971	24E124414A501971	OTAA-calssB	cloud	28 days ago	\checkmark	2 ×
	1152-test	24E1612290821375	ClassC-OTAA	cloud	63 days ago	~	2 ×

Figure 3-2-2-10

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 3-2-2-8 Device Parameters

Device Name	lora-sensor
Description	a short description of your node
Device EUI	24e1641194784358
Device-Profile	ClassA-OTAA 🗸
Application	cloud 🗸
Modbus RTU Data Transmission	Modbus RTU to TCP 🗸
Fport	
TCP Port	
Frame-counter Validation	
Application Key	
Device Address	
Network Session Key	
Application Session Key	
Uplink Frame-counter	0
Downlink Frame-counter	0

Figure	3-2-2-11
--------	----------

Device Configuration				
ltem	Description	Default		
Device Name	Enter the name of this device.	Null		
Description	Enter the description of this device.	Null		
Device EUI	I Enter the EUI of this device. Null			
Device-Profile	vice-Profile Choose the device profile.			
Application Choose the application profile.		Null		
Modbus RTU Data Transmission	Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over TCP". This feature is only applicable to Milesight class C type LoRaWAN® controllers.(UC501/UC1152, etc.) -Modbus RTU to TCP: TCP client can send Modbus TCP commands to ask for controller Modbus data. -Modbus RTU over TCP: TCP client can send Modbus RTU commands to ask for controller Modbus data.	Disable		
Fport	Enter the LoRaWAN [®] frame port for transparent transmission between Milesight LoRaWAN [®] controllers and UG67.	Null		

	Range: 2-84, 86-223.	
	Note: this value must be the same as the Milesight	
	LoRaWAN [®] controller's Fport.	
TCP Port	Enter the TCP port for data transmission between the TCP Client and UG67 (as TCP Server). Range: 1-65535.	Null
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.	Enabled
Application Key	Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key.	Null
Device Address	The device address identifies the end-device within the current network.	Null
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.	Null
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.	Null
Uplink Frame-counter	The number of data frames which sent uplink to the network server. It will be incremented by the end-device and received by the end-device. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	Null
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.	Null

Table 3-2-2-9 Device Setting Parameters

Related Configuration Example

Device configuration

3.2.2.5 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.

Figure 3-2-2-12

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 3-2-2-10 Multicast Group Parameters

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

Figure	3-2-2-13
i iguic	02210

Multicast Group Configuration				
ltem	Description Default			
Group Name	Enter the name of this multicast group.	Null		
Multicast	Device address (Dev Addr) of all devices in this group.	Null		

AddressIdenceIdenceMulticast Network Session KeyThe network session key (Netwks Key) of all devices in his group.NullMulticast Application Session KeyThe application session key(AppSKey) of all devices in his group.NullClass TypeClass B and Class C are optional.Class CDatarateDatarate of the node receiving downlinksBased on the supported frequencyFrequencyDownlink frequency of all devices in this group.Based on the supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.Every secondPing Slot Period of opening the pingslot. This is only applied to Class B end devices.Every secondSelected DevicesAdd devices in the pull-down list.Null			
Network Session KeyThe network session key (Netwks Key) of all devices in this group.NullMulticast Application Session KeyThe application session key(AppSKey) of all devices in this group.NullClass TypeClass B and Class C are optional.Class CDatarateDatarate of the node receiving downlinksBased on the supported frequencyFrequencyDownlink frequency of all devices in this group.Based on the supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.0Ping Slot Period cityPeriod of opening the pingslot. This is only applied to Class B end devices.Every 4 secondSelected DevicesShow all device names in this group.Null	Address		
Application Session KeyThe application session key(AppSKey) of all devices in this group.NullClass TypeClass B and Class C are optional.Class CDatarateDatarate of the node receiving downlinksBased on the supported frequencyFrequencyDownlink frequency of all devices in this group.Based on the supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.0Ping Slot PeriodicityPeriod of opening the pingslot. This is only applied to Class B end devices.Every secondSelected DevicesShow all device names in this group.Null	Network		Null
DatarateBased on the supported frequencyFrequencyDownlink frequency of all devices in this group.Based on the supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.0Ping Slot PeriodicityPeriod of opening the pingslot. This is only applied to class B end devices.Every secondSelected DevicesShow all device names in this group.Null	Application		Null
DatarateDatarate of the node receiving downlinkssupported frequencyFrequencyBased on the supported frequency of all devices in this group.Based on the supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.0Ping Slot Period of opening the pingslot. This is only applied to Class B end devices.Every 4 secondSelected DevicesShow all device names in this group.Null	Class Type	Class B and Class C are optional.	Class C
FrequencyDownlink frequency of all devices in this group.supported frequencyFrame-count erThe number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.0Ping Slot PeriodicityPeriod of opening the pingslot. This is only applied to Class B end devices.Every second4 secondSelected DevicesShow all device names in this group.Null	Datarate	Datarate of the node receiving downlinks	supported
Frame-count erend-device downlink from the network server. It will be incremented by the network server.0Ping SlotPeriod of opening the pingslot. This is only applied to Class B end devices.Every second4Selected DevicesShow all device names in this group.Null	Frequency	Downlink frequency of all devices in this group.	supported
PeriodicityClass B end devices.secondSelected DevicesShow all device names in this group.Null		end-device downlink from the network server. It will be	0
Devices Show all device names in this group. Null	-		-
Add Device Add devices in the pull-down list. Null		Show all device names in this group.	Null
	Add Device	Add devices in the pull-down list.	Null

Table 3-2-2-11 Multicast Group Setting Parameters

3.2.2.6 Gateway Fleet

Milesight gateways can connect to UG67 network server. At most 4 gateways can be added to one gateway.

General	Applications	Profiles	Device	Multicast Groups	Gateway Fleet	Packets	
Gateway Fleet							
Gat	teway ID	1	Name	Status	La	st Seen	Operation
24E124	FFFEF12263	Loca	I Gateway	Connected	2021-04-19 16:12:27		[<i>l</i>] ×]
							H

Figure 3-2-2-14

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 3-2-2-12 Gateway Fleet Parameters

Gateway ID		
Name		
Location		
Location		
	ayed by default or can be changed ma	anually
GPS info will be displa	ayed by default or can be changed ma	anually
		anually

Figure 3-2-2-15

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 3-2-2-13 Gateway Setting Parameters

3.2.2.7 Packets

Send Data To Device									
Device EUI		Туре		Payload			Port	Confirme	ł
000000000000000000000000000000000000000	AS	CII 🗸					85		Send
Send Data to Multicast G	roup								
Multicast Group		Туре		Payload			Port		
	✓ AS	CII 🗸					85		Send
Network Server									
Clear							Search		Q
Device EUI/Group	Gateway ID	Frequency	Datarate	RSSI/SNR	Size	Fcnt	Туре	Time	Details
		No	matching reco	rds found					

Figure 3-2-2-16

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

Table 3-2-2-14 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.		
Туре	Show the type of the packet: JnAcc - Join Accept Packet JnReq - Join Request Packet UpUnc - Uplink Unconfirmed Packet UpCnf - Uplink Confirmed Packet - ACK response from network requested DnUnc - Downlink Unconfirmed Packet DnCnf - Downlink Confirmed Packet- ACK response from end-device requested		
Time	Show the time of packet was sent or received.		

Table 3-2-2-15 Packet Parameters

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

Packet Details		×
Dev Addr/Multicast Addr	0614B991	<u>^</u>
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 3-2-2-17

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

Table 3-2-2-16 Packets Details Parameters

Related Topic

Send Data to Device

3.3 Network

3.3.1 Interface

3.3.1.1 Port

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

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

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

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

Status	Port	WLAN	Cellular	Loopback		
Packet Forwarder	- Port_1					
Network Server	Port				eth 0	
	Conne	ection Type			Static IP	~
Network	IP Add	IP Address			192.168.22.112	
Interface	Netmask		255.255.255.0			
Firewall	Gateway		192.168.22.1			
DHCP	MTU				1500	
	Prima	ry DNS Server			8.8.8.8	
DDNS	Secon	dary DNS Server			114.114.114.114	
Link Failover	Enable	e NAT			2	25



Port Setting		
ltem	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 3-3-1-1 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	eth 0		
Connection Type	Static IP 🗸		
P Address	192.168.22.112		
letmask	255.255.255.0		
Gateway	192.168.22.1		
ЛТU	1500		
Primary DNS Server	8.8.8.8		
Secondary DNS Server	114.114.114		
nable NAT			
Iultiple IP Address			
IP A	ddress	Netmask	Ope

Figure 3-3-1-2

Static IP		
ltem	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 3-3-1-2 Static IP Parameters

2. DHCP Client

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

Port	eth 0
, on	Guro
Connection Type	DHCP Client V
мти	1500
Use Peer DNS	
Primary DNS Server	8.8.8.8
Secondary DNS Server	114.114.114

Figure 3-3-1-3

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

3. PPPoE

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

Port	eth 0
Connection Type	PPPoE V
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 3-3-1-4

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 3-3-1-4 PPPOE Parameters

3.3.1.2 WLAN

This section explains how to set the related parameters for Wi-Fi network. UG67 supports 802.11 b/g/n, as AP or client mode.

Port	WLAN	Cellular	Loopback
WLAN			
Enable			
Work Mode		AP	~
SSID Broad	lcast		
AP Isolation	1		
Radio Type		802.11n(2.4	GHz) 🗸
Channel		Auto	~
SSID			
BSSID			
Encryption	Mode	No Encryptic	on 🗸
Bandwidth		20MHz	~
Max Client	Number	10	
IP Setting			
Protocol		Static IP	~
IP Address			
		DHCP Settings	3
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 3-3-1-6

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" ,
LICIYPTION 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".
Key	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
	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".
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and
Key	"AES/TKIP".
	"AES/TKIP". Fill the pre-shared key of WPA encryption.
	Fill the pre-shared key of WPA encryption.
Bandwidth	Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz".
	Fill the pre-shared key of WPA encryption.
Bandwidth	Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway
Bandwidth Max Client Number	Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway
Bandwidth Max Client Number IP Setting	Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP.
Bandwidth Max Client Number IP Setting Protocol	Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP. Set the protocol in wireless network.

Table 3-3-1-5 WLAN Parameters

Port	WLAN	Cellular	Lo	opback				
< GoBack								
	SSID	Channel	Signal	Cipher	BSSID	Security	Frequency	
Vison Se	nsor_006602	Auto	-94dBm	Auto	24:e1:24:00:66:02	No Encryption	2462MHz	Join Network
Miles	sight_Test	Auto	-88dBm	AES	ec:26:ca:99:3a:a4	WPA-PSK/WPA2-PSK	2437MHz	Join Network



Client Mode-Scar	n
SSID	Show SSID.
Channel	Show wireless channel.
Signal	Show wireless signal.
BSSID	Show the MAC address of the access point.
Security	Show the encryption mode.
Frequency	Show the frequency of radio.
Join Network	Click the button to join the wireless network.

Table 3-3-1-6 WLAN Scan Parameters

Related Topic

Wi-Fi Application Example

3.3.1.3 Cellular

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

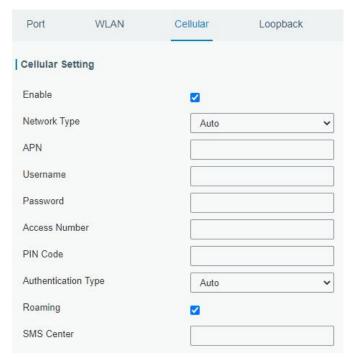


Figure 3-3-1-8

Connection Setting		
Enable NAT		
Restart When Dial-up failed		
ICMP Server	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	~

Figure 3-3-1-9

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	Enter the username for cellular dial-up connection provided by local ISP.	Null			
Password	Enter the password for cellular dial-up connection provided by local ISP.	Null			
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.	Null			
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.	Null			
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".	Auto			
Roaming	Enable or disable roaming.	Disable			
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.	Null			
Enable NAT	Enable or disable NAT function.	Enable			
Restart When Dial-up failed	When this function is enabled, the gateway will restart automatically if the dial-up fails several times.	Disabled			
ICMP Server	Set the ICMP detection server's IP address.	8.8.8.8			

Secondary ICMP Server	Set the secondary ICMP detection server's IP address.	114.114.11 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 3-3-1-7 Cellular Parameters

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

Figure 3-3-1-10

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

Table 3-3-1-8 Cellular Parameters

Related Topics

Cellular Connection Application Example Phone Group

3.3.1.4 Loopback

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

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

Port	WLAN	Cellular	Loopback		
Loopback	Address				
IP Address		127.0.0.1			
Netmask		255.0.0.0			
Multiple IP	Addresses				
	IP	Address		Netmask	Operation
					•
Save					

Figure 3-3-1-11

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

Table 3-3-1-9 Loopback Parameters

3.3.2 Firewall

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

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

3.3.2.1 Security

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

Figure 3-3-2-1

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 2.2.2.1 Coourity Deremeters				

Table 3-2-2-1 Security Parameters

3.3.2.2 ACL

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

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

Security	ACL	DMZ	Port Mapping	MAC Binding			
ACL Setting							
Default Filter Po	licy	Accept	~				
Access Contro	l List						
			Туре	extended	~		
			ID				
			Action	permit	~		
			Protocol	ip	~		
			Source IP				
			Source Wildcard Mask	0.0.0.0			
			Destination IP				
			Destination Wildcard Mask	0.0.0.0			
			Description				
			Save	Cancel			
Interface List							
	Interface		In ACL	8		Out ACL	Operation
							•

Figure 3-3-2-2

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	
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ІСМР Туре	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.

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

Table 3-3-2-2 ACL Parameters

3.3.2.3 DMZ

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

Security	ACL	DMZ	Port Mapping
DMZ			
Enable			
DMZ Host			
Source Address			



DMZ			
Item	Description		
Enable	Enable or disable DMZ.		
DMZ Host	Enter the IP address of the DMZ host on the internal network.		
Source Address	Set the source IP address which can access to DMZ host. "0.0.0/0" means any address.		

Table 3-3-2-3 DMZ Parameters

3.3.2.4 Port Mapping

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

Click 🛨 to add a new port mapping rules.

Security	ACL	DMZ	Port Mapping	MAC E	Binding		
Port Mapping							
Sourc	ce IP	Source Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0					TCP 🗸		
							Ŧ

Figure 3-3-2-4

Port Mapping				
Item	Description			
Source IP	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.			
Source Port Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.				
Destination IP	Enter the IP address that packets are forwarded to after being received on the incoming interface.			
Destination Port	Enter the TCP or UDP port that packets are forwarded to after being received on the incoming port(s). Range: 1-65535.			
Protocol	Select from "TCP" and "UDP" as your application required.			
Description	The description of this rule.			

Table 3-3-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.3.2.5 MAC Binding

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

Security	ACL	DMZ	Port Mapping	MAC Binding		
MAC Binding	List					
I	MAC Address		IP Address		Description	Operation
						×
						•

Figure 3-3-2-5

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 3-3-2-5 MAC Binding Parameters

3.3.3 DHCP

UG67 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		
	wlan0 192.168.66.100 192.168.66.199 255.255.255.0 1440	wlan0 192.168.66.100 192.168.66.199 255.255.255.0 1440

Figure 3-3-3-1

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	Set the primary DNS server.	114.114.114.114		

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

Table 3-3-3-1 DHCP Server Parameters

3.3.4 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name. DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

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

Figure 3-3-4-1

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 3-3-4-1 DDNS Parameters

3.3.5 Link Failover

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

Configuration Steps

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

3.3.5.1 SLA

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

	SLA	Track	WAN Failover							
9	LA Entry									
	ID	Туре	Destination Address	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	Packet Loss Count	Start Time	Operation
	1	icmp-ech 🗸	114.114.114.1	8.8.8.8	56	15	5000	3	no\ 🗸	×
										æ

Figure 3-3-5-1

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

Table 3-3-5-1 SLA Parameters

3.3.5.2 Track

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

Linkage between Track Module and SLA module

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

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

Linkage between Track Module and Application Module

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

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

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

SLA	Track	WAN Failover				
Track Objec	t					
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	v 1 v	wlan0 🗸 🗸	0	1	
						Ŧ

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

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

Positive Delay (s)	When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate switching).	1
--------------------	---	---

Table 3-3-5-2 Track Parameters

3.3.5.3 WAN Failover

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

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

SLA	Trac	k	WAN Fai					
WAN Failo	ver							
Main Int	terface	Backup I	nterface	Startup Delay(s)	Up Delay(s)	Down Delay(s)	Track ID	Operation
Cellular	0 🗸	eth 0	~	30	0	0	1	~ ×
								Ð

Figure 3-3-5-3

WAN Failover					
Parameters	Description	Default			
Main Interface	Select a link interface as the main link.				
Backup Interface	Select a link interface as the backup link.				
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	30			
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching)	0			
Down Delay (s)	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching).	0			
Track ID	Track detection, select the defined track ID.				

Table 3-3-5-3 WAN Failover Parameters

3.3.6 VPN

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

UG67 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.3.6.1 DMVPN

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client
DMVPN Settin	gs				
Enable					
Hub Address					
Local IP Addres	ŝS				
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	Ŧ	
Encryption Algo	orithm		MD5	٣	
DH Group			MODP768-1	T	
Key					
Local ID Type			Default	Ŧ	
IKE Life Time(s)		10800		
SA Algorithm			DES-MD5	•	
PFS Group			NULL	•	
Life Time(s)			3600		
		Fi	gure 3-3-6-1		
				_	



Figure 3-3-6-2

DMVPN			
Item	Description		
Enable	Enable or disable DMVPN.		
Hub Address	The IP address or domain name of DMVPN Hub.		
Local IP address	DMVPN local tunnel IP address.		

GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication	Select from "DES", "3DES", "AES128", "AES192" and
Algorithm	"AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DUCroup	Select from "MODP768_1", "MODP1024_2" and
DH Group	"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",
CA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",
SA Algorithm	"AES192_MD5", "AES192_SHA1", "AES256_MD5" and
	"AES256_SHA1".
	Select from "NULL", "MODP768_1", "MODP1024_2" and
PFS Group	"MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of Nhrp protocol.

Table 3-3-6-1 DMVPN Parameters

3.3.6.2 IPSec

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

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

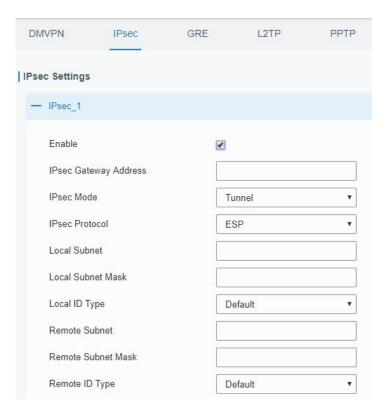


Figure 3-3-6-3

IPsec		
Item	Description	
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.	
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.	
IPsec Mode	Select from "Tunnel" and "Transport".	
IPsec Protocol	Select from "ESP" and "AH".	
Local Subnet	Enter the local subnet IP address that IPsec protects.	
Local Subnet Netmask	Enter the local netmask that IPsec protects.	
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN".	
Remote Subnet	Enter the remote subnet IP address that IPsec protects.	
Remote Subnet Mask	Enter the remote netmask that IPsec protects.	
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".	
	Table 2.2.6.2 IDaga Davamatara	

Table 3-3-6-2 IPsec Parameters

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



IKE Parameter			
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			
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",		
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5",		
	"AES192_SHA1", "AES256_MD5" and "AES256_SHA1".		
PFS Group	Select from "NULL", "MODP768_1" , "MODP1024_2" and "MODP1536_5".		
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.		

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

Table 3-3-6-3 IPsec Parameters

3.3.6.3 GRE

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

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

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

DM	VPN	IPsec	GRE	L2TP	PPTP
GRE	Settings				
-	GRE_1				
	Enable			•	
	Remote IP Ad	dress			
	Local IP Addre	ess			
	Local Virtual IF	^o Address			
	Netmask			255.255.255.0	
	Peer Virtual IP	Address			
	Global Traffic I	Forwarding			
	Remote Subne	et			
	Remote Netma	ask			
	MTU			1500	
	Key				
	Enable NAT				

Figure 3-3-6-5

GRE	
Item	Description
Enable	Check to enable GRE function.

1	
Remote IP Address	Enter the real remote IP address of GRE tunnel.
Local IP Address	Set the local IP address.
Local Virtual IP	Set the local tunnel IP address of GRE tunnel.
Address	Set the local tailler in address of one tailler.
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.
Key	Set GRE tunnel key.
Enable NAT	Enable NAT traversal function.

Table 3-3-6-4 GRE Parameters

3.3.6.4 L2TP

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

DMVPN	IPsec	GRE	L2TP	PPTP
L2TP Settin	gs			
— L2TP_	1			
Enable	0			
Remot	e IP Address			
Userna	ime			
Passw	ord			
Auther	tication	A	uto	Ŧ
Global	Traffic Forwarding			
Remot	e Subnet			
Remot	e Subnet Mask			
Key				

Figure 3-3-6-6

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.	
Кеу	Enter the password of L2TP tunnel.	

Table 3-3-6-5 L2TP Parameters

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

Figure 3-3-6-7

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	

Expert Options	(s)	connection. Range: 0-600.
Expert Options	Max Retries	-
nord and opparate the othinge man plant op door	Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-3-6-6 L2TP Parameters

3.3.6.5 PPTP

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

DMVPN	IPsec	GRE	L2TP	PPTP
PPTP Settings				
- PPTP_1				
Enable				
Remote IP	Address			
Username				
Password				
Authentica	ition	· /	Auto	•
Global Tra	ffic Forwarding			
Remote S	ubnet			
Remote S	ubn <mark>et Mask</mark>			

Figure 3-3-6-8

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

Table 3-3-6-7 PPTP Parameters

Advanced Settings	2
Local IP Address	
Peer IP Address	
Enable NAT	
Enable MPPE	
Address/Control Compression	
Protocol Field Compression	
Asyncmap Value	fffffff
MRU	1500
MTU	1500
Link Detection Interval(s)	60
Max Retries	0
Expert Options	

Figure 3-3-6-9

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

Table 3-3-6-8 PPTP Parameters

3.3.6.6 OpenVPN Client

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

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certificatio
OpenVPN Clie	nt Settings						
- OpenVPN	_1						
Enable Protocol Remote If Port	P Address	UDF		Y			
Interface Authentic Local Tun Remote T	nel IP	Non	e	Temperature			
Enable N	AT						
Compress Link Dete	sion ction Interval(s)	60)	•			
Link Dete Cipher	ction Timeout(s)	300	•	•			
MTU		1500					
Max Fram		1500	1				
Verbose L Expert Op		ERF	ROR	•			
Local Ro	ute						
		Subnet			Subnet Mas	k	Operation

Figure 3-3-6-10

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

Protocol	Select from "UDP" and "TCP".
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port	Enter the listening port number of remote OpenVPN server. Range: 1-65535.
Interface	Select from "tun" and "tap".
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert", and "X.509 cert+user".
Local Tunnel IP	Set local tunnel address.
Remote Tunnel IP	Enter remote tunnel address.
Global Traffic	All the data traffic will be sent out via OpenVPN tunnel when
Forwarding	this function is enabled.
Enable TLS Authentication	Check to enable TLS authentication.
Username	Enter username provided by OpenVPN server.
Password	Enter password provided by OpenVPN server.
Enable NAT	Enable NAT traversal function.
Compression	Select LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. Range: 10-1800.
Link Detection Timeout (s)	Set link detection timeout. OpenVPN will be reestablished after timeout. Range: 60-3600.
Cipher	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
	Table 3-3-6-9 OpenVPN Client Parameters

Table 3-3-6-9 OpenVPN Client Parameters

3.3.6.7 OpenVPN Server

UG67 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

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



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

Figure	3-3-6-12
гiyure	3-3-0-12

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

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

Table 3-3-6-10 OpenVPN Server Parameters

3.3.6.8 Certifications

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

DMVPN	IPsec	GRE	L2TP	PPTP	Open	VPN Client		OpenVPN Server	Certifications
OpenVPN Clie	nt								
- OpenVPN	client_1								
CA				Browse	Import	Export	Delete		
Public Key	y			Browse	Import	Export	Delete		
Private Ke	ey 📕			Browse	Import	Export	Delete		
TA				Browse	Import	Export	Delete		
Preshared	d Key			Browse	Import	Export	Delete		
PKCS12				Browse	Import	Export	Delete		

Figure 3-3-6-13

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

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

Table 3-3-6-11 OpenVPN Client Certification Parameters

OpenVPN Server

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

Figure 3-3-6-14

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

Table 3-3-6-12 OpenVPN Server Parameters

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

Figure 3-3-6-15

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

Table 3-3-6-13 IPsec Parameters

3.4 System

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

3.4.1 General Settings

3.4.1.1 General

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

General	System Time	SMTP	Phone	Email	Storage
System					
Hostname		GATEWAY			
Web Login Tim	eout(s)	1800			
Access Servio	ce				
	Enable	Servi	ice		Port
		НТТ	Р		80
		HTT	PS		443
		TELN	ET		23
		SSI	Н		22
HTTS Certifica	ates				
Certificate	https.crt	Browse	Import Expo	rt Delete	
Key	https.key	Browse	Import Expo	rt Delete	

Figure	3-4-1-1
riguic	0 - 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	e de la companya de l	
Port	Set port number of the services. Range: 1-65535.	
НТТР	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 3-4-1-1 General Setting Parameters

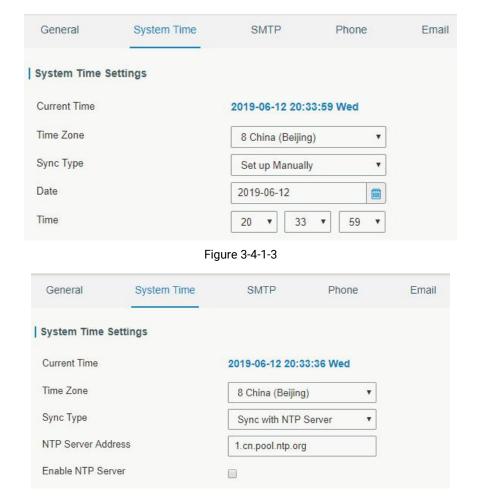
3.4.1.2 System Time

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

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

General	System Time	SMTP	Phone	Email
System Time Se	ttings			
Current Time		2019-06-12 20:3	4:32 Wed	
Time Zone		8 China (Beijing	J) *	
Sync Type		Sync with Brow	ser 🔹	
Browser Time		2019-06-12 20:3	4:32 Wed	

Figure 3-4-1-2





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 3-4-1-2 System Time Parameters

3.4.1.3 SMTP

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

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

Figure 3-4-1-5

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

Table 3-4-1-3 SMTP Setting

Related Topics

Events Setting

3.4.1.4 Phone

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

General	System Time	SMTP	Phone	Email		
^o hone Numbe	r List					
	Nam	le			Number	Operation
	List1				654321;123456	×
						-

Figure 3-4-1-6

Phone				
ltem	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 3-4-1-4 Phone Settings

Related Topic

Connect on Demand

3.4.1.5 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	×
						H
Save						
Save						

Figure 3-4-1-7

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

Table 3-4-1-5 Email Settings

3.4.2 User Management

3.4.2.1 Account

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

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 3-4-2-1 Account Information

3.4.2.2 User Management

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

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

Figure 3-4-2-2

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 3-4-2-2 User Management

3.4.3 SNMP

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

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

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

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

3.4.3.1 SNMP

UG67 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

Status	SNMP	MIB View	VACM	Тгар	MIB
LoRaWAN 🕨	SNMP Settin	gs			
	Enable				
Network •	Port		161		
Quintom 🔻	SNMP Versior	ı	SNMPv2		Ŧ
System	Location Infor	mation			
General Settings	Contact Inform	nation			
User Management	Save				
SNMP					

Figure 3-4-3-1

SNMP Settings				
ltem	Description			
Enable	Enable or disable SNMP function.			
Port	Set SNMP listened port. Range: 1-65535.			
	The default port is 161.			

SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.			
Location Information	Fill in the location information.			
Contact Information	Fill in the contact information.			

Table 3-4-3-1 SNMP Parameters

3.4.3.2 MIB View

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

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

Figure 3-4-3-2

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

Table 3-4-3-2 MIB View Parameters

3.4.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
NMP v1 & v2	User List					
Commu	inity	Permission	MIB Vie	9W	Network	Operation
private	Rea	ad-write	All	•	0.0.0/0	×
public	Rea	ad-only	none	•	0.0.0.0/0	×

Figure 3-4-3-3

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

Table 3-4-3-3 VACM Parameters

3.4.3.4 Trap

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

SNMP	MIB View	VACM	Тгар	MIB
SNMP Trap				
Enable				
SNMP Version	I.	SNMPv2		•
Server Addres	s			
Port				
Name				



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

		"Auth & Priv".
--	--	----------------

Table 3-4-3-4 Trap Parameters

3.4.3.5 MIB

This section describes how to download MIB files.

SNMP	MIB View	VACM	Тгар	MIB
MIB Downloa	d			
MIB File		AGENTX	-MIB txt T	Download

Figure 3-4-3-5

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

3.4.5 Device Management

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

Status	Device Management	
LoRaWAN 🕨	Device Management	
	Status	Disconnected
Network	Activation Server Address	
Q	Device Management Server Address	
System	Activation Method	By Authentication Code •
General Settings	Authentication Code	
User Management	Connect	
AAA		
Device Management		

Figure 3-4-5-1

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

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

Table 3-4-5-1

3.4.6 Events

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

3.4.6.1 Events

You can view alarm messages on this page.

Status		Events	Events Set	tings		
LoRaWAN		Mark as Read	Delete	Mark A	ll as Read D	elete All Ala
Network	•	Sta	atus	Туре	Time	
System	-	< > 10 •	Go to:	GO		
General Settin	gs					
User Manager	nent					
AAA						
Device Manag	ement					
Events						



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

Message	Show the alarm content.
	Table 2.4.6.1 Events Devendence

Table 3-4-6-1 Events Parameters

3.4.6.2 Events Settings

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

Events	Events Settings			
Events Setting	5			
Enable				
Phone for Notific	ation	*		
Email for Notifica	tion	~		
	Events	Record	Email Email Setting	SMS SMS Setting
(Cellular Up			
Ce	ellular Down			
	WAN Up			
٧	VAN Down			
	VPN Up			
N.	/PN Down			
	Power On			
	Power Off			

Figure 3-4-6-2

Event Settings	Event Settings		
ltem	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.		
Power Off	The gateway has powered off.		
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 the Email group.			
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.		
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.		
Phone Group List	st Select phone group to receive SMS alarm.		
Email Group List	Select Email group to receive Email alarm.		

Table 3-4-6-2 Events Parameters

Related Topics

Email Setting

Phone Setting

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping and traceroute.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

Ping	Traceroute	Qxdmlog		
IP Ping				
Host			Ping	Stop

Figure 3-5-1-1

PING	
ltem	Description
Host	Ping outer network from the gateway.
	Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Ping	Traceroute	Qxdmlog		
Traceroute				
Host			Trace	Stop



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

Table 3-5-1-2 Traceroute Parameters

3.5.1.3 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.

Ping	Traceroute	Packet Analyzer	Qxdmlog
Start	Stop	Download	
		Figure 3-5-1-3	

3.5.2 Schedule

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

Status	Î	Schedule			
LoRaWAN	×	Schedule			
Network		Schedule	Frequency	Hour	Minute
0	•				
System		Save			
Maintenance	-				
Tools					
Schedule					
			Figure 3-5-2-1		
Schedule	•				

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

Table 3-5-2-1 Schedule Parameters

3.5.3 Log

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

3.5.3.1 System Log

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

Download			
File	Log File	• Download	
Log			
View recent(lines)	20	T	
Thu Jul 18 15:01:25 2019 user	.notice redis[1859]; Backgroun	saving terminated with success	
Thu Jul 18 15:06:26 2019 user	.notice redis[1859]: 10 change	in 300 seconds. Saving	
Thu 141 40 45 00 00 0040	notice redis[1859]: Backgroun		
1 nu Jul 18 15:06:26 2019 usel	induce redis[1055]. Dackgroun	I saving started by pid 11683	
Thu Jul 18 15:06:26 2019 user			
Thu Jul 18 15:06:26 2019 user	notice redis[11683]: DB saved		
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user	r.notice redis[11683]: DB saved r.notice redis[1859]: Backgroun r.notice redis[1859]: 10 change:	on disk I saving terminated with success in 300 seconds. Saving	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun notice redis[15776]: DB saved	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun notice redis[15776]: DB saved notice redis[1859]: Backgroun	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776 on disk I saving terminated with success	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:01:27 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:11:27 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun notice redis[1859]: Backgroun notice redis[1859]: 10 change	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776 on disk I saving terminated with success in 300 seconds. Saving	
Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:06:26 2019 user Thu Jul 18 15:11:27 2019 user Thu Jul 18 15:16:28 2019 user	notice redis[11683]: DB saved notice redis[1859]: Backgroun notice redis[1859]: 10 change notice redis[1859]: Backgroun notice redis[1859]: Backgroun notice redis[1859]: O change notice redis[1859]: Backgroun	on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 15776 on disk I saving terminated with success in 300 seconds. Saving I saving started by pid 19899	

Figure 3-5-3-1

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

Table 3-5-3-1 System Log Parameters

3.5.3.2 Log Settings

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

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address			i) L	
Port		514		
Local Log File				
Storage		local	v	
Size		1024		КВ
Log Severity		Info	•	

Figure 3-5-3-2

Log Settings				
Item	Description			
Remote Log Server				
Enable	With "Remote Log Server" enabled, gateway will send all system logs to the remote server.			
Syslog Server Address	Fill in the remote system log server address (IP/domain name).			
Port	Fill in the remote system log server port.			
Local Log File				
Storage	User can store the log file in memory or TF card.			
Size	Set the size of the log file to be stored.			
Log Severity	The list of severities follows the syslog protocol.			
	Table 2 F 2 2 System Lag Decemptore			

Table 3-5-3-2 System Log Parameters

3.5.4 Upgrade

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

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

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

Figure 3-5-4-1

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

Table 3-5-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.5.5 Backup and Restore

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

Backup and Restor	e		
Restore Config			
Config File		Browse	Import
Backup Running-co	onfig		
Backup			
Restore Factory De	faults		
Reset			

Figure 3-5-5-1

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

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

Related Configuration Example

Restore Factory Defaults

3.5.6 Reboot

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

Network Server		Reboot		
Network		Reboot		
System)				
Maintenance	-			
Tools				
Schedule				
Log				
Upgrade				
Backup and Restore				
Reboot				

Figure 3-5-6-1

3.6 APP

3.6.1 Python

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

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

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

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

3.6.1.1 Python

Python	AppManag	AppManager Configuration		PP	
Python					
AppManager S	tatus	Uninstalled			
SDK Version					
SDK Path					
Available Stora	ge	local	~		
SDK Upload				Browse	Install



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

View	View application status managed by AppManager.
	Table 3-6-1-1 Python Parameters

3.6.1.2 App Manager Configuration

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

Figure 3-6-1-2

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

Table 3-6-1-2 APP Manager Parameters

3.6.1.3 Python App

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

Figure 3-6-1-3

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

Table 3-6-1-3 APP Parameters

3.6.2 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[®] 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

3.6.2.1 Node-RED

Status	Node-RED		
Packet Forwarder	Node-RED		
	Enable		Launch
Network Server	Node-RED Version	1.2.9	
	Node Library Version	1.0.2	
Network •	Upgrade Node Library		Browse Upgrade
System 🕨			
	Save		
Maintenance			
APP 🔻			
Python			
Node-RED			

Figure 3-6-2-1

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. Node-RED version can
NOUE-RED VEISION	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.
	Table 3-6-2-1 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	estore
Restore Config	1
Config File	Browse Import
Backup Runnir	ng-config
Backup	
Restore Factor	y Defaults
Reset	
Backup Running-config	
Backup	
Restore Factory Defaults	
Reset	×
	Reset operation will erase all configuration data on Router and reset the system to factory defaults. Continue?
	Reset Cancel

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

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

Please wait till 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 SYS LED.

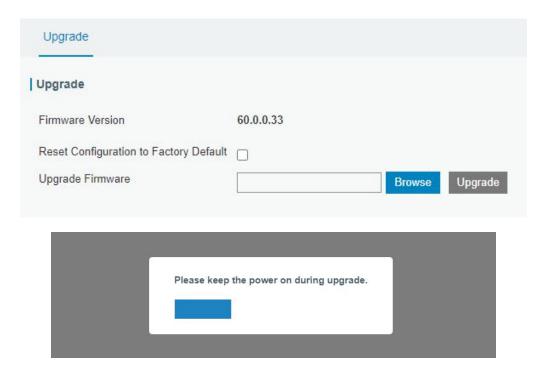
SYS LED	Action
Static Green	Press and hold the reset button for more than 5 seconds.
Static Green → Rapidly Blinking	Release the button and wait.
Off \rightarrow Static Green	The gateway is now reset to factory defaults.

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.

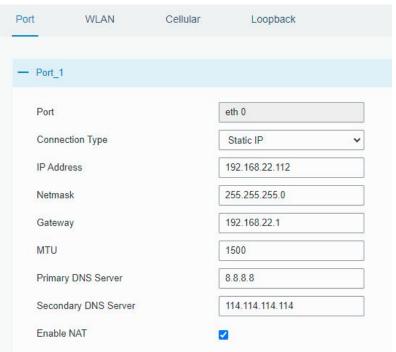


Related Topic

<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	Cellular	Network	WLAN	VPN	Host List		
WAN									
Port	Status	Туре	IP Address	Net	mask	Gateway	/	DNS	Duration
eth 0	up	Static	192.168.22.112	255.25	55.255.0	192.168.22	2.1	8.8.8.8	1days,02h 34m 22s

Related Topic

Port Setting

4.4 Cellular Connection

- 4. Go to "Network > Interface > Cellular > Cellular Setting" and configure the cellular info.
- 5. Choose relevant network type.

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

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

6. 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.



7. 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 UG67.

Related Topic

Cellular Setting Cellular Status

4.5 Wi-Fi Application Example

4.5.1 AP Mode

Application Example

Configure UG67 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	Loopbac	k
WLAN				
Enable				
Work Mode	3	AP		~
SSID Broa	dcast			
AP Isolatio	n			
Radio Type	9	802.11n(2.4GHz)		~
Channel		Auto		~
SSID		Gateway_F1200F		
BSSID		24:e1:24	:f1:20:0f	
Encryption	Mode	No Encr	yption	~
Bandwidth		20MHz		~
Max Client	Number	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		192.168.1.1			
Netmask		255.255.255.0			
Connection Duration	n	0 days, 02:40:52			

4.5.2 Client Mode

Application Example

Configure UG67 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	oback			
< 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		Client		~	Scan
SSID		AAA			
BSSID		24:e1:24:	f0:c4:13		
Encryption	Mode	WPA-PS	K/WPA2-PSK	~	
Cipher		AES		~	
Key		••••••			
IP Setting					
Protocol		DHCP C	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-PS	К	
Cipher		AES		
Status		Connected		
IP Address		192.168.1.145		
Netmask		255.255.255.0		
Connection Duratio	n	0 days, 02:44:45		

Related Topic

WLAN Setting

WLAN Status

4.6 Packet Forwarder Configuration

UG67 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	e	Server Address	Connect Status	Operation
0	Enabled	Embedde	ed NS	localhost	Connected	
						•
F B						

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

enable this server.

Гуре	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.

Region		US915		~	
	Name			Center Frequency/MHz	
	Radio 0		9	04.3	
	Radio 1		9	05.0	
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	

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 UG67.

Ge	eneral	Rad	tios Adv	anced	Custom	Traffic			
Traf	fic Sett	ing							
	Stop		Clear						
	Rfch	Direction	Time	Ticks I	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

4.7 Connect UG67 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	EF12257	_			
Network		Frequency-Sync	Disabled		*			
System	۲	Multi-Destination						
		ID	Enable		Гуре	Server Address	Connect Status	Operation
Maintenance	•	0	Enabled	l Embe	edded NS	localhost	Connected	
APP	•							H

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		C	enter Frequency/MHz
	Radio 0		904.3	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" mode.

Status	General	Applications	Profiles	Device
Packet Forwarder	General Setting			
	Enable			
Network Server	Cloud Mode			
Network		Milesigh	t IoT Cloud	~
	NetID	010203		
System 🕨	Join Delay	5		sec
Maintenance	RX1 Delay	1		sec
	Lease Time	8760-0-0	ien i	hh-mm-ss
APP 🕨	Log Level	info		~

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.

My Devices									Concernance of
	Searc		٩		Normal 1 🖄 Alarm	n 1 🕅 Offline 1	⊗ Inactive 3		+ New Devio
Map Triggers		\otimes	<u>真实设备-EN</u> 6136A39023	Add Device			×	e	@ M @
Reports		\otimes	UC3X52-虚 61151109	* SN : * Name:			sociated with your		@ <u>~</u> 0
Event Center 30 Sharing Center		<u>}</u>	UC3X5 6123A124	• Name.				15 minutes ago	@ <u>M</u> ()
Me		邕	AM102- 6128A2175		Cance	Confirm	ux ination	a few seconds ago	@ <u>~</u> 0
				CO2	TVOC	Barometric Pressure			
			4	27℃ Temperature	51% Humidity	O Activity Level (PIR)	2lux Illumination		

5. The gateway is online on Milesight IoT Cloud.

② Dashboard	Devices		Gateways	+			
My Devices	Search		Q		⊘ Normal 1 🕅 Offline 0 ⊗ Inacti	ve O	+ New Devices
🖄 Map		Status	Name		Associated Devices (Joined /Not Joined /Failed)	Last Updated	
If Triggers		all	UG Gateway 621793129987		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:

Status	General	Applications	Profiles	Device
Packet Forwarder	Applications			
	Name	clou	d	
Network Server	Description	clou	d	
Network 🕨	Payload Codec	Nor	ie	~

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

HTTP or HTTPS:

Step 1: select HTTP or HTTPS as transmission protocol.

Type	HTTP	*
------	------	---

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

URL

Data Type	URL
Uplink data	
Join notification	
ACK notification	
Error notification	

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
[×
			Ŧ

MQTT:

Step 1: select the transmission protocol as MQTT.

(¹	
MQTT	•

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				
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/events	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[®] node devices. Please select correct device profile according to device type.

General	Applications	Profiles	Device	Gateways	Packets			
Device								
Add	Bulk Import	Delete All			Search	Q		
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation		
		No ma	atching records found	i				
	Device Name			or				
	Description			a short description of your node				
	Device EUI		0000000000000000					
	Device-Profile		OTAA-ClassC 🗸					
	Application				~			
	Frame-counter	r Validation						
	Application Ke	у						
	Device Addres	s						
	Network Sessi	ion Key						
	Application Se	ssion Key						
	Uplink Frame-	counter	0					

0

Save & Apply

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

Downlink Frame-counter



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		12	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.

Send Data To Device				
Device EUI	Туре	Payload	Fport	Confirmed
11226121913	ASCII	15	15	
. Click "Send".				
	Send	send success		

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	Confirmed
11226121913	ASCII	15	15	

You can click "Refresh" to refresh the list or set automatic refreshing frequency for the list. If the device's class type is Class C, then the device will 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	 1970	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.

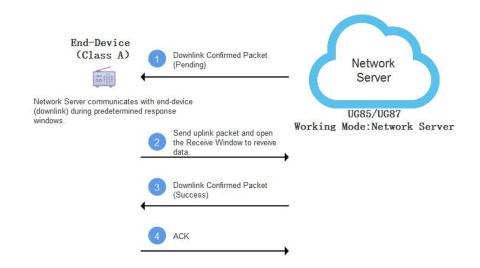
Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fent	Туре	Time	Details
11226121913	868300000	SF10BW125	100	-	0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	- 0
112261219	869525000	SF12BW125	12	121	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125		-	0	1	DnUnc	2019-08-06T09:22:49+08:00	0

Packets Details		×
Dev Addr	07e7	Â
GwEUI	24e124ff	
AppEUI	557240	
DevEUI	1122612191311123	
Immediately	123	
Timestamp	874346044	
Туре	UpCnf	
Adr	false	
AdrAcKReq	false	,
Ack	true	
Fcnt	21	
Fport	55	
Modulation	LORA	
in o datation	2010	-

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

If the device's class type is Class A, only after the device sends out an uplink packet will the network server sends out data to the device.

Network Serv	er										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.
112261219	01311123	868300000	SF10BW125	122	2	0	19	DnUnc	2019-08-06T09:49:38+08:00	0	Font
112261219	91311123	868300000	SF10BW125	10.8	-76	64	21	ACK	2019-08-06T09:49:38+08:00	0	Show the frame counter.
112261219)1311123	868300000	SF10BW125	10.8	-76	64	21	UpCnf	2019-08-06T09:49:38+08:00	0	Type Show the type of the paceket:
112261219	91311123	868100000	SF10BW125	-	51	6	18	DnCnf	2019-08-06T09:48:43+08:00	Success	JnAcc - Join Accept Packet JnReq - Join Request Packet
112261219	91311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	•	UpUnc - Uplink Unconfirmed Packet
112261219	91311123	0				6	18	DnCnf	Pending	0	UpCnf - Uplink Confirmed Packet - ACK response from network requested
112261219	01311123	868500000	SF10BW125	1		0	17	DnUnc	2019-08-06T09:47:38+08:00	0	DnUnc - Downlink Unconfirmed
112261219	91311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0	Packet DnCnf - Downlink Confirmed Packet- ACK response from end-
112261219)1311123	868100000	SF10BW125	-	2	0	16	DnUnc	2019-08-06T09:46:38+08:00	0	device requested
112261219	91311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	D Refresh	Time Show the time of packet was sent



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	•
1122612191311123	868100000	SF10BW125	means	the d	evice	has re		2019-08-06T09:48:43+08:00 he packet you send.	0
1122612191311123	868100000	SF10BW125	9.8	-77	64	20	UpCnf	2019-08-06T09:48:43+08:00	0
1122612191311123	0				6	18	DnCnf		0
1122612191311123	868500000	SF10BW125	~	×	0	17	DnUnc	2019-08-06T09:47:38+08:00	0
1122612191311123	868500000	SF10BW125	8.0	-76	64	19	UpCnf	2019-08-06T09:47:38+08:00	0
1122612191311123	868100000	SF10BW125	2	12	0	16	DnUnc	2019-08-06T09:46:38+08:00	0
1122612191311123	868100000	SF10BW125	11.2	-74	64	18	UpCnf	2019-08-06T09:46:37+08:00	0

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.

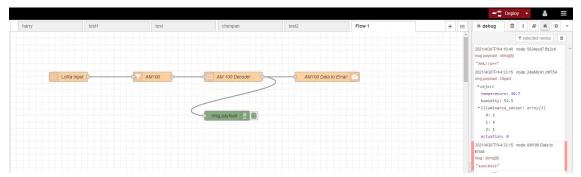


RED.				
	Node-RED	Usemame: [1 Password:		
	Node-RED		Login	

4.11.2 Send Data by Email

Application Example

Send AM104 device data by Email.



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 1
				Name	AM100	
				Device EUI	24E124127A270222	+
	10 LoRa Input	-{T AM100				

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



harry	test1	test	chenpan	Edit Decoder node
				Delete Cancel Done
				🌣 Properties 🔹 🖻 🕅
LoRa Input		A100	AM 100 Decoder	Name AM 100 Decoder
Lord apper			Ann 100 Decouch	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 Outpu	ut node		
				Delete		Cancel	Done
				© Properties			
				Name	AM100 Data to Email		
	LoRa Input	- AM100	AM 100 Decoder	SMTP Option	Custom		
				User ID	@milesight.com		
			msg.payload	Password	(10) (10)		
				SMTP Server Address	smtp.exmail.qq.com		
				Port [1-65535]	25		
				Enable TLS			
	WAN	Up 9		То	@milesight.com	+	
				Topic	AM100 Data		
				Payload	The time is {{time}} Deveui is {{deveui} counter is {{payload.humidity}}	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	Flow 1	+	1	∰ debug	8	i g	ŵ	٥
	III LoRa Input	ç	M100	AM 100 Decoder	AM100 Data to Email				▼ selected nodes 2021/4/30下午4.19.40 node: 5034ec07.fta3 msg.pay/odd: string[8] **A4L//w==*				
				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 ④
Size: 2 KB
```

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

Related Topic

Node-RED

[END]

2021-04