



UG67 User Guide

Outdoor LoRaWAN® Gateway



Preface

Milesight

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, 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

© 2011-2024 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: <u>iot.support@milesight.com</u> Support Portal: support.milesight-iot.com Tel: 86-592-5085280 Fax: 86-592-5023065 Address: Building C09, Software Park III, Xiamen 361024, China

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 integration
Aug. 24, 2021	V1.2	2. Delete Package Forward status page
		3. Phone & Email webpage update
		1. Add AS923-3&AS923-4
Dec. 15, 2021	V1.3	2. Change network server channel mask box to channel
		3. Add device channel setting in profile
	V1.4	1. Add batch backup
Feb. 23. 2022		2. Login webpage update
		3. Change default antenna type to external antenna
		4. Adjust time of Class C ACK timeout
	V1.5	1. Support VLAN Trunk client
Jun. 1, 2022		2. Add System Name in SNMP
		3. Add Use L21P Peer DNS option
	V1.6	1. Add BACnet Server feature
Dec.26, 2022		2. Add Payload Codec feature
		3. Add Reset and all flows export feature on Node-RED
		4. Add data retransmission feature on Packet Forward
March 6, 2023	V1.7	1. Delete embedded antenna mode
		2. Add LBT feature
		Compatible with Milesight Development Platform
Fab 01 0004		2. Update default secondary ICMIP and DNS server
red. 21, 2024	νΙ.δ	address
		3. Add cellular IMS and custom MITU feature
		4. Add 8 pre-set device profiles

Contents

Chapter 1 Product Introduction	7
1.1 Overview	7
1.2 Advantages	7
1.3 Specifications	8
1.4 Dimensions (mm)	10
Chapter 2 Access to Web GUI	11
2.1 Wireless Access	11
2.2 Wired Access	12
Chapter 3 Web Configuration	14
3.1 Status	14
3.1.1 Overview	14
3.1.2 Cellular (Cellular Version Only)	15
3.1.3 Network	16
3.1.4 WLAN	17
3.1.5 VPN	19
3.1.6 Host List	20
3.2 LoRaWAN	21
3.2.1 Packet Forwarder	21
3.2.1.1 General	
3.2.1.2 Radios	22
3.2.1.3 Noise Analyzer	24
3.2.1.4 Advanced	25
3.2.1.5 Custom	27
3.2.1.6 Traffic	
3.2.2 Network Server	
3.2.2.1 General	
3.2.2.2 Application	
3.2.2.3 Payload Codec	34
3.2.2.4 Profiles	
3.2.2.5 Device	
3.2.2.6 Multicast Groups	41
3.2.2.7 Gateway Fleet	
3.2.2.8 Packets	44
3.3 Protocol Integration	
3.3.1 BACnet Server	47
3.3.1.1 Server	47
3.3.1.2 BACnet Object	48
3.4 Network	49
3.4.1 Interface	
3.4.1.1 Port	
3.4.1.2 WLAN	52

3.4.1.3 Cellular (Cellular Version Only)	55
3.4.1.4 Loopback	58
3.4.1.5 VLAN Trunk	59
3.4.2 Firewall	59
3.4.2.1 Security	59
3.4.2.2 ACL	60
3.4.2.3 DMZ	62
3.4.2.4 Port Mapping (DNAT)	62
3.4.2.5 MAC Binding	63
3.4.3 DHCP	64
3.4.4 DDNS	65
3.4.5 Link Failover	66
3.4.5.1 SLA	66
3.4.5.2 Track	66
3.4.5.3 WAN Failover	68
3.4.6 VPN	68
3.4.6.1 DMVPN	69
3.4.6.2 IPSec	70
3.4.6.3 GRE	73
3.4.6.4 L2TP	74
3.4.6.5 PPTP	76
3.4.6.6 OpenVPN Client	78
3.4.6.7 OpenVPN Server	79
3.4.6.8 Certifications	82
3.5 System	83
3.5.1 General Settings	83
3.5.1.1 General	83
3.5.1.2 System Time	84
3.5.1.3 SMTP	85
3.5.1.4 Phone	85
3.5.1.5 Email	86
3.5.2 User Management	87
3.5.2.1 Account	87
3.5.2.2 User Management	87
3.5.3 SNMP	88
3.5.3.1 SNMP	88
3.5.3.2 MIB View	89
3.5.3.3 VACM	89
3.5.3.4 Trap	90
3.5.3.5 MIB	91
3.5.4 Device Management	91
3.5.4.1 Auto Provision	91
3.5.4.2 Management Platform	92
3.5.5 Events	93

Milesight

3.5.5.1 Events	93
3.5.5.2 Events Settings	94
3.6 Maintenance	95
3.6.1 Tools	95
3.6.1.1 Ping	95
3.6.1.2 Traceroute	95
3.6.1.3 Qxdmlog	96
3.6.2 Schedule	96
3.6.3 Log	97
3.6.3.1 System Log	97
3.6.3.2 Log Settings	
3.6.4 Upgrade	98
3.6.5 Backup and Restore	
3.6.6 Reboot	100
3.7 APP	100
3.7.1 Python	
3.7.1.1 Python	101
3.7.1.2 App Manager Configuration	101
3.7.1.3 Python App	102
3.7.2 Node-RED	103
3.7.2.1 Node-RED	
Chapter 4 Application Examples	105
4.1 Restore Factory Defaults	105
4.2 Firmware Upgrade	106
4.3 Ethernet Connection	
4.4 Cellular Connection (Cellular Version Only)	
4.5 Wi-Fi Application Example	109
4.5.1 AP Mode	109
4.5.2 Client Mode	110
4.6 Packet Forwarder Configuration	111
4.7 Connect to Milesight IoT Cloud	113
4.8 Application Configuration	115
4.9 Device Configuration	117
4.10 Send Data to Device	118
4.11 Node-RED	121
4.11.1 Start the Node-RED	121
4.11.2 Send Data by Email	

Chapter 1 Product Introduction

1.1 Overview

Milesight

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

1.3 Specifications

Hardware System	
CPU	Quad-core 1.5GHz, 64-bit ARM Cortex-A53
Memory	8 GB eMMC Flash, 512 MB DDR4 RAM
LoRaWAN	
Antenna Connector	$2 \times 50 \Omega$ N-Female External Connectors
Channel	8
	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923-1&2&3
Frequency Band	&4
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class B/Class C and V1.0.2 Class A/Class B/Class C
LBT	Support
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)				
Interface	Auto MDI/MDIX				
Mode	Full or half duplex (auto-sensing)				
Wi-Fi Interfaces					
Antenna	Fully Integrated and Internal Antenna				
Standards	IEEE 802.11 b/g/n, 2.4 GHz				
	802.11b: 18 dBm +/-2.0 dBm (11 Mbps)				
	802.11g: 15 dBm +/-2.0 dBm (6 Mbps)				
	802.11g: 15 dBm +/-2.0 dBm (54 Mbps)				
Tx Power	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS0_HT20)				
	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS7_HT20)				
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS0_HT40)				
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS7_HT40)				
Cellular Interfaces (C	Optional)				
Antenna	Internal Antenna				
SIM Slots	1				
GPS					
Antenna	Internal Antenna				
	-167dBm@Tracking, -149dBm@Acquisition,				
Sensitivity	-161dBm@Re-acquisition				
Position Accuracy	<2.5m CEP				
Software					
	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS,				
Network Protocols	DNS, SNTP, Telnet, SSH, MQTT, BACnet/IP, etc.				
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE				
Firewall	ACL/DMZ/Port Mapping/MAC Binding				
	Web, CLI, SMS, On-demand dial up, DeviceHub, Milesight IoT				
Management	Cloud, Yeastar Workplace Platform, Milesight Development				
	Platform				
Арр	Python SDK, Node-RED				
Power Supply and Co	onsumption				
Deriver Over 1	1. 1 × 802.3 af PoE Input				
Power Supply	2. 12 VDC with M12 Connector				
Consumption	Typical 3.6W, Max 4.8W				

Physical Characteris	stics
Ingress Protection	IP67
Dimensions	240 x 164 x 90.9 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 $+85^{\circ}$ C (-40° F to $+185^{\circ}$ 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

Δ

Milesight

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".

- 6-55	Language English v
Milesight - Granwy -	
A Logn	

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

4. After logging the web GUI, you can view system information and perform configuration of the gateway. It's suggested that you change the password for the sake of security.

Milesigh	t								💄 admin 🔁)
				For yo	our device security, p	lease change ti	he default password			
Status		Overview	Cellular	Network	WLAN	VPN	Host List			?
Packet Forwarder		System Information	lion							
Network Occurs		Model		UG67-L00E	E-868M					
Network Server		Region		EU868						
Protocol Integration	•	Serial Number		6222C4522	2590					
		Firmware Version		60.0.0. <mark>41</mark> -r	4					
Network	×	Hardware Version		V1.4						
	201	Local Time		2023-03-02	11:09:02 Thursday					
System		Uptime		17:11:08						
Maintenance	•	CPU Load		3%						
		RAM (Capacity/Ava	ailable)	512MB/107	'MB(20.9%)					
APP	Þ	eMMC (Capacity/A	Available)	3.0G/2.8G(91.08%)					
		GPS		-						
									Manual Refresh V Refresh	

2.2 Wired Access

Milesight

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).

Network and Sharing Center		- 🗆 ×
← → × ↑ 💺 « Network	and Internet > Network and Sharing Center	✓ ♂ Search Control Panel
Control Panel Home	View your basic network informatic	on and set up connections
Change adapter settings Change advanced sharing	View your active networks Yeastar5G	Access type: Internet
settings	Private network	Connections: M Wi-Fi (Yeastar5G)
	ldentifying	Access type: No network access Connections: Ethernet
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN	connection; Ethernet
	Troubleshoot problems Diagnose and repair network problem	ms, or get troubleshooting information.
See also		
HomeGroup		
Intrared		
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.

nternet Protocol Version 4 (TCP	/IPv4) Properties
General	
You can get IP settings assigned this capability. Otherwise, you r for the appropriate IP settings.	d automatically if your network supports need to ask your network administrator
O Obtain an IP address auto	matically
• Use the following IP addre	ss:
IP address:	192 . 168 . 23 . 200
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 23 . 150
Obtain DNS server address	s automatically
• Use the following DNS serv	ver addresses:
Preferred DNS server:	8.8.8.8
Alternative DNS server:	e - e - >
Validate settings upon exi	t 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, enter the username and password, click "Login".



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, you can view system information and perform configuration of the gateway. It's suggested that you change the password for the sake of security.



Chapter 3 Web Configuration

3.1 Status

Milesight

3.1.1 Overview

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

System Information	
Model	UG67-915M
Region	AU915
Serial Number	6222D3914187
Firmware Version	60.0.0.42-r5
Hardware Version	V1.4
Local Time	2024-02-21 20:25:25 Wednesday
Uptime	1days,05:53:13
CPU Load	3%
RAM (Capacity/Available)	512MB/109MB (21.29%)
eMMC (Capacity/Available)	8.0GB/6.5GB (81.86%)
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 3-1-1-1 System Information

Milesight

When Milesight UPS is connected to the device, the UPS basic information will also show on the Status page. For more details please refer to *Milesight UPS User Guide*.

UPS	
Model	-
Serial Number	-
Firmware Version	-
Hardware Version	7 5
Power Status	Unconnected
Remaining Battery	-1

Figure 3-1-1-2

3.1.2 Cellular (Cellular Version Only)

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

Item	Description	
Modem Informati	on	
		Figure 3-1-2-1
Cell ID		340db80
LAC		5922
PLMN ID		
Network Type		LTE
ISP		CHN-UNICOM
ICCID		89860117838009934120
IMSI		460019425301842
IMEI		860425047368939
Reg <mark>ister</mark> Status		Registered (Home network)
Signal Level		26asu (-61dBm)
Version		EC25ECGAR06A07M1G
Model		EC25
Status		Ready
Modem		

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

Table 3-1-2-2 Network Status

3.1.3 Network

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

Overview	C	ellular	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



Network	
Item	Description
Port	Show the name of the Ethernet port.
Statue	Show the status of the Ethernet port. "Up" refers to a status that WAN
Status	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. <mark>1</mark> .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	
Item	Description
IP Address	Show the IP address of access point or client.
MAC Address	Show the MAC address of the access point or client.
Connection Duration	Show information on how long the Wi-Fi network has been

connected.

Table 3-1-4-2 WLAN Status

3.1.5 VPN

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

Overview	Cellular	Network	WLAN VPN	Host List
PPTP Tunnel				
	Name	Status	Local IP	Remote IP
	pptp_1	Disconnected	80 1	2
	pptp_2	Disconnected	-	-
	pptp_3	Disconnected	100	2
L2TP Tunnel				
	Name	Status	Local IP	Remote IP
	12tp_1	Disconnected	20	2
	12tp_2	Disconnected	2	-
	12tp_3	Disconnected	1.00	

Figure 3-1-5-1

IPsec Tunnel					
	Name	Status	Local IP	Remote IP	
	ipsec_1	Disconnected	2 .	2	
	ipsec_2	Disconnected	14 - 1	12	
	ipsec_3	Disconnected	1821	· •	
OpenVPN Client	OpenVPN Client				
	Name	Status	Local IP	Remote IP	
	openvpn_1	Disconnected		2	
	openvpn_2	Disconnected	8 2 4	12	
	openvpn_3	Disconnected	120	: 50	

Figure 3-1-5-2

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

Figure 3-1-5-3

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.

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

Figure 3-1-6-1

Host List			
ltem	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			
	Show the IP address and MAC address set in the Static IP		
	list of DHCP service.		



Table 3-1-6-1 Host List Description

3.2 LoRaWAN



3.2.1 Packet Forwarder

3.2.1.1 General

General	Radios	Advanced	Custom	Traffic		
General Setting						
Gateway EUI	24E124FFF	EF35F39				
Gateway ID	24E124FF	FEF35F39				
Frequency-Sync	Disabled		~			
Data Retransmissio	n 🗌					
Multi-Destination						
ID	Enable	•	Туре	Server Address	Connect Status	Operation
0	Enable	d E	mbedded NS	localhost	Disconnected	
						H

Figure 3-2-1-1

General Settings	
Item	Description
Gateway EUI	Show the unique identifier of the gateway and it's non-editable.
	Fill in the corresponding ID which you've used for registering
Gateway ID	gateway to the remote network server. It is usually the same as
	gateway EUI and can be changed.

Frequency-Sync	Sync frequency configurations from the network server by selecting the corresponding multi-destination ID.
Data Retransmission	When the gateway connects to a single Chirpstack/Semtech/Remote Embedded NS/Basic Station type package forwarder, it supports data storage up to 1 million pieces of data when network is disconnected and re-transmits the data after network recovery.
Multi-Destination	The gateway will forward the data to the network server address that was created and enabled in the list.
Connection Status	Show the connection status of package forwarder.

Table 3-2-1-1 General Setting Parameters

Related Configuration Example

Packet fowarder configuration

3.2.1.2 Radios

Radio Channel Setting			
Region	US915	~	Noise Analyzer 👻
Name		Center F	requency/MHz
Radio 0		904.3	
Radio 1		905.1	



Radios-Radio Channel Setting					
Item	Description	Default			
Region	Choose the LoRaWAN [®] frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Based on the gateway's model			
Center Frequency	Change the frequencies to receive packets from LoRaWAN [®] nodes.	Based on what is specified in the LoRaWAN [®] regional parameters document			

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

1	Multi	Channels	Settin
	wuru	Channels	Settin

wutti Cria	nnels setung				
	Enable	Index	Radio		Frequency/MHz
		0	Radio 0	¥	923.2
	۲	1	Radio 0	T	923.4
		2	Radio 0	¥	923.6
	۲	3	Radio 1	T	922.2
		4	Radio 1	¥	922.4
	۲	5	Radio 1	T	922.6
		6	Radio 1	T	922.8
		7	Radio 1	Ŧ	923.0



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

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

LoRa Channel Setting

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

Figure 3-2-1-4

Radios-LoRa Channel Setting					
ltem	Description	Default			
Enable	Click to enable this channel to transmit packets.	Enabled			
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0			
Frequency/MHz	Enter the frequency of this channel. Range: center frequency±0.9.	Based on the supported frequency			
Bandwidth/MHz	Enter the bandwidth of this channel.	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		
	Radio 0 🔹	924.0	125KHZ 🔻	50000		



Radios-FSK Channel Setting					
Item	Description	Default			
Enable	Click to enable this channel to transmit packets.	Disabled			
Radio	Choose Radio 0 or Radio 1 as center frequency.	Radio 0			
Frequency/MHz	Enter the frequency of this channel. Range: center frequency±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.

ported Freq			US915	~	Noise Analyzer 🔺
Noise Analyzer	Running				
Settings	Sweep Freq	Genaral Freq	~		
	0-63: 902.3-914.9	MHz			
	64-71: 903-914.2 M	MHz			
	Sween Time	Quatara			
	Oweep Time	Custom	•		
		24	h		
		ок			
	-	O→ Current Value → O→ W	eighted Average Value		
RSSI/dBm					
0		1 1	· · · ·	1 1	MHz
-20 -					
10					
*40 -			Δ		
-60 -		\wedge			
-80-	~ ~	\sim			
-100		200			
			8		
-116 -					

Figure 3-2-1-6

Noise Analyzer						
Item	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

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

General	Radios	Advanced	Custom	Traffic
Beacon Settin	g			
Beacon Period		0	~	s
Beacon Freq		508300000		Hz
Beacon Datarat	e	SF10	~	
Beacon Channe	el Number	3	•	
Beacon Freq St	ер	200000		Hz
Beacon Bandwi	dth	125000	¥	Hz
Beacon TX Pow	/er	14		dBm



Advanced-Beacon Setting					
Item	Description	Default			
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons.	0			
Beacon Freq	The frequency of beacons.	Based on the supported			

		frequency
Beacon Datarate	The datarate of beacons.	Based on the supported frequency
Beacon Channel Number	When selecting Custom, it allows users to custom range from 1 to 8.	1
Beacon Freq Step	Frequency interval of beacons.	200000
Beacon Bandwidth	The bandwidth of beacons. Unit: Hz	12500 Hz
Beacon TX Power	The TX power of beacons.	Based on the supported frequency

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



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	Enable to send packets received with CRC errors to	Disabled

Error	the network server.	
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled
	Table 3-2-1-8 Advanced Parameters	

LBT Settings		
Enable		
RSSI Target	-80	dBm

Figure 3-2-1-9

ltem	Description	Default
Enable	Enable or disable LBT feature. Listen before talk (LBT) is used to detect whether the downlink channel is idle and avoid channel access conflicts. Note: AU915 and US915 do not support LBT feature.	Disabled
RSSI Target	Enter the criteria of an idle channel. If actual RSSI of a channel is less than the criteria/target, the channel is considered as idle. Range: -120~0	-80

Table 3-2-1-9 Advanced-LBT Parameters

3.2.1.5 Custom

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

Note: customized configuration will overwrite the packet forward configurations of web GUI.

General	Radios	Advanced	Custom	Traffic	
Custom Confi	guration				
Enable					
				Example	
{ "SX1302_conf "spidev_path": "lorawan_publ "clksrc": 0, "antenna_gain "antenna_cfg" "full_duplex": f "precision_tim "enable": false "max_ts_metri "nb_symbols": }, "radio_0": { "enable": true, "type": "SX125 "for-er", 023000	<pre>": { "/dev/spidev0.0", ic": true, ": 0, /* antenna gair : "ITXIRX", false, estamp": { , ics": 255, 1 50", </pre>	n, in dBi */			

Figure 3-2-1-10

3.2.1.6 Traffic

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

SNR -13.2
SNR -13.2
- <mark>1</mark> 3.2
-13.2
-9.8
-10.5
-13.0
-12.2
-13.8
-13.2
-12.2
-12.8

Figure 3-2-1-11

Item	Description
Refresh	Click to obtain the latest data.
Clear	Click to clear all data.
Rfch	Show the channel of this packet.
Direction	Show the direction of this packet.
Time	Show the receiving time of this packet.
Ticks	Show the ticks of this packet.

Frequency	Show the frequency of the channel.
Datarate	Show the datarate of the channel.
Coderate	Show the coderate of this packet.
RSSI	Show the received signal strength.
SNR	Show the signal to noise ratio of this packet.

Table 3-2-1-10 Traffic Parameters

3.2.2 Network Server

3.2.2.1 General

General Setting		
Enable		
Platform Mode		
NetID	010203	
Join Delay	5	sec
RX1 Delay	1	sec
Lease Time	8760-0-0	hh-mm-ss
Log Level	info	~
Global Channel Plan	Setting	
Channel Plan	US915	~
Channel	8-15	

Figure 3-2-2-1

Item	Description	Default
General Setting		
Enable	Click to enable Network Server mode.	Enabled
Platform Mode	Enabled to connect gateway to Milesight IoT Cloud or Yeastar Workplace platform.	Disabled
NetID	Enter the network identifier.	010203
Join Delay	Enter the interval time between when the end-device sends a Join_request_message to network server and when the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
RX1 Delay	Enter the interval time between when the	1

	end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	
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 Set	tting	
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	Allow end devices to communicate with specific frequency channels. Leave it blank means using all the default standard usable channels specified in the LoRaWAN [®] regional parameters document. It allows to enter the index of the channels. Examples: 1, 40: Enabling Channel 1 and Channel 40 1-40: Enabling Channel 1 to Channel 40 1-40, 60: Enabling Channel 1 to Channel 40 channel 60	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
			Ð



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

The r	ange is based	on what is	specified in	
the	LoRaWAN®	regional	parameters	
docur	nent.			

Table 3-2-2-2 Additional Plan Parameters

3.2.2.2 Application

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

You can edit the app	lication by clicking	or create a new application by clicking	+
Applications			
Name	cloud		
Description	cloud		
Data Transmission			
	Туре	Operati	on
		E	

Figure 3-2-2-3

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

Table 3-2-2-3 Application Parameters

MQTT Integration

Туре	MQTT	~
Status	-	
General		
Broker Address		
Broker Port		
Client ID		
Connection Timeout/s	30	
Keep Alive Interval/s	60	
User Credentials		
Enable		
Username		
Password		
TLS		
Enable		
Mode	CA signed server certificat	e 🗸

Figure 3-2-2-4

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 🗸
Request data	/event/request	QoS 0 🗸
Response data	/event/response	QoS 0 🗸

Figure 3-2-2-5

MQTT Settin	gs
ltem	Description
General	
Broker	MOTT broker address to receive data
Address	NIQ I I DIOKEI address to receive data.
Broker Port	MQTT broker port to receive data.

Milesight

	Client ID is the unique identity of the client to the server.
Client ID	It must be unique when all clients are connected to the same server, and
	it is the key to handle messages at QoS 1 and 2.
Connection	If the client does not get a response after the connection timeout, the
Timeout/s	connection will be considered as broken. The Range: 1-65535
Keep Alive	After the client is connected to the server, the client will send heartbeat
Interval/s	packet to the server regularly to keep alive. Range: 1-65535
User Credent	ials
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
	Select from "Self signed certificates", "CA signed server certificate".
	CA signed server certificate: verify with the certificate issued by
Mode	Certificate Authority (CA) that pre-loaded on the device.
	Self signed certificates: upload the custom CA certificates, client
	certificates and secret key for verification.
Торіс	
	Data type to communicate with MQTT broker:
	Uplink Data: receive device uplink packets
	Downlink Data: send downlink commands to device
	Multicast Downlink Data: send downlink commands to multicast group
Data Type	Join Notification: receive join request packets from devices
	ACK Notification: receive ACK packets from devices
	Error Notification: receive error packets from devices
	Request data: send requests to enquire and configure the gateway NS
	Response data: receive the request responses
Торіс	Topic name of the data type used for publishing.
	QoS 0 – Only Once
	This is the fastest method and requires only 1 message. It is also the
	most unreliable transfer mode.
	QoS 1 – At Least Once
0.05	This level guarantees that the message will be delivered at least once,
000	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

Note: if MQTT broker type is HiveMQ, please enable **TLS** and set the option as **CA signed server certificate.**

HTTP/HTTPS Integration

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

Figure 3-2-2-6

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

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

Related Configuration Example

Application configuration

3.2.2.3 Payload Codec

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

ihaami Maralan	100			
ibrary Version	1.0.0			
Obtaining Type	Online	~		
Obtain				
lote: Ensure that the Internet ac	cess is available.			
Name		Payload decoder function	Payload encoder function	Details
AM103 & AM10)3L	~	~	0
AM104		\checkmark	\checkmark	0
AM107		\checkmark	\checkmark	0
AM307		\checkmark	\checkmark	0
AM308		\checkmark	\checkmark	0
AM319-HCH0	C	\checkmark	\checkmark	0
AM319-HCHO-	-IR	\checkmark	\checkmark	0
AM319-03		~	\checkmark	0
EM300-TH		\checkmark	\checkmark	0
				•

Figure 3-2-2-7

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

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

Name	
Description	
Template	None
Payload decoder	
Payload decoder function	<pre>1 // Decode decodes an array of bytes into an object. // - Prort contains the LORAWAN fPort number // - bytes is an array of bytes, e.g. [22, 280, 255, 0] // The function must return an object, e.g. {"temperature": 22.5} function Decode(fPort, bytes) { return {}; } }</pre>
Payload encoder	
Payload encoder function	<pre>1 // Encode encodes the given object into an array of bytes. // - Port contains the LoRawWW FPort number // - obj is an object, e.g. ("temperature": 22.5) // The function must return an array of bytes, e.g. [225, 230, 255, 0] function Encode(FPort, obj) { return []; }</pre>
Payload Codec Test	
	1 // input decoded test payloed or encoded test payload // decoded bytes // 01 75 5C 03 67 34 01 04 68 65 05 6A 49 00 06 65 1C 00 79 00 14 00 07 7D E7 04 08 7D 07 00 09 73 3F 27 // encoded objs // {



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

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

Milesight

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. UG67 has pre-configured 8 device files and users can also create a new device profile.

General	Applications	Payload Codec	Profiles	Device	Multicast Groups	Gateway Fleet	Packets
Davica Profiles							
Device Fromes							
	Nam	e	Max TXPower		Join Type	Class Type	Operation
	ClassA-	ABP	0		ABP	Class A	ℤ ×
	ClassA-0	AATC	0		OTAA	Class A	\mathbb{Z} ×
	ClassB-	ABP	0		ABP	Class A Class B	\mathbb{Z} ×
	ClassB-0	AATC	0		OTAA	Class A Class B	\mathbb{Z}
	ClassC-	ABP	0		ABP	Class A Class C	\mathbb{Z}
	ClassC-0	AATC	0		OTAA	Class A Class C	ℤ ×
	ClassCB	-ABP	0		ABP	Class A Class B Class C	\mathbb{Z}
	ClassCB-	OTAA	0		OTAA	Class A Class B Class C	
							(m)



Device Profiles		
Name		
Max TXPower	0	
Join Type	ΟΤΑΑ	~
Class Type	🔄 Class A 🗌 Clas	ss B 🔲 Class C
Advanced		



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

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

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

Figure	3-2-2-11
riguie	52211

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 Frequency	RX2 channel frequency which used for the RX2 receive-window.	parameters document			
Frequency List	List of factory-preset frequencies. The range is based on what is specified in the LoRaWAN [®] regional parameters document.	Null			
Device Channel	Change this device frequency channel by typing the channel indexs. When configured, it takes precedence over the global channel. This setting only works for CN470/US915/AU915 gateway.	Null			
PingSlot Period	Period of opening the pingslot.	Every Second			
PingSlot DataRate	Datarate of the node receiving downlinks.	Based on the supported frequency			
PingSlot Freq	Frequency of the node receiving downlinks.	Based on the supported frequency			
ACK Timeout	The time for confirmed downlink transmissions. This option is only applicable to class B and class	Class B: 10 Class C: 10			

C.	Table 2.2.2.0 Device Profiles Advanced Setting Decomptore	
	C.	

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

3.2.2.5 Device

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

Add Bulk Import	Delete All				Search	
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operatio
24E124414B032563	24E124414B032563	classB	cloud	11 days ago	~	<i>[[</i>]×
24E124414A501971	24E124414A501971	OTAA-calssB	cloud	28 days ago	~	2 X
1152-test	24E1612290821375	ClassC-OTAA	cloud	63 days ago	~	<i>l</i> ×

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 . \checkmark means that the device has been activated.			
Operation	Edit or delete the device.			

Table 3-2-2-10 Device Parameters

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



Device Configuration				
Item	Description			
Device Name	Enter the name of this device.			
Description	Enter the description of this device.			
Device EUI	Enter the EUI of this device.			
Device-Profile	Choose the device profile.			
Application	Choose the application profile.			
Payload Codec	Choose the payload codec existed on Payload Codec page.			
fDort	Enter the downlink port of device, it's 85 by default for Milesight			
IFOIL	devices.			
	Choose from: "Disable", "Modbus RTU to TCP", "Modbus RTU over			
	TCP". This feature is only applicable to Milesight LoRaWAN®			
Modbus RTU	controllers.(UC501/UC300, etc.)			
Data	Modbus RTU to TCP: TCP client can send Modbus TCP commands to			
Transmission	ask for controller Modbus data.			
	Modbus RTU over TCP: TCP client can send Modbus RTU commands			
	to ask for controller Modbus data.			
Modbus RTU	Enter the LoRaWAN® frame port for transparent transmission			
Fport	between Milesight LoRaWAN [®] controllers and UG67.			

Milesight

	Range: 2-84, 86-223.
	Note: this value must be the same as the Milesight LoRaWAN®
	controller's Fport.
TOD Dort	Enter the TCP port for data transmission between the TCP Client and
ICP POIL	UG67 (as TCP Server). Range: 1-65535.
Frame-Counter	If disable the frame-counter validation, it will compromise security as
Validation	it enables people to perform replay-attacks.
Application Koy	Whenever an end-device joins a network via over-the-air activation,
Аррисацон кеу	the application key is used for derive the Application Session key.
Dovice Address	The device address identifies the end-device within
Device Address	the current network.
Notwork	The network session key specific for the end-device. It is used by the
Soccion Koy	end-device to calculate the MIC or part of the MIC (message integrity
Session Key	code) of all uplink data messages to ensure data integrity.
	The AppSKey is an application session key specific for the
Application	end-device. It is used by both the application server and the
Session Key	end-device to encrypt and decrypt the payload field of
	application-specific data messages.
	The number of data frames which sent uplink to the network server. It
Unlink	will be incremented by the end-device and received by the end-device.
Frame-counter	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.
	The number of data frames which received by the end-device
	downlink from the network server. It will be incremented by the
Downlink	network server.
Frame-counter	Users can reset the a personalized end-device manually, then the
	frame counters on the end-device and the frame counters on the
	network server for that end-device will be reset to 0.

Table 3-2-2-11 Device Setting Parameters

Related Configuration Example

Device configuration

3.2.2.6 Multicast Groups

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

Mult	icast Groups				
	Add			Search	Q
	Multicast Address	Group Name	Number of Devices	Operat	tion
		No matching reco	irds found		

Figure 3-2-2-14

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

Table 3-2-2-12 Multicast Group Parameters

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

Figure	3-2-2-15
iguic	02210

Multicast Group Configuration					
Item	Description				
Group Name	Enter the name of this multicast group.				
Multicast Address	Device address (Dev Addr) of all devices in this group.				
Multicast Network	The network session key (Netwks Key) of all devices in this				
Session Key	group.				
Multicast	The application session key(AppSKey) of all devices in this				
Application	aroun				
Session Key	group.				
Class Type	Class B and Class C are optional.				
Datarate	Datarate of the node receiving downlinks				
Frequency	Downlink frequency of all devices in this group.				
	The number of data frames which received by the end-device				
Frame-counter	downlink from the network server. It will be incremented by the				
	network server.				

Ping Slot	Period of opening the pingslot. This is only applied to Class B
Periodicity	end devices.
Selected Devices	Show all device names in this group.
Add Device	Add devices in the pull-down list.
	Table 3-2-2-13 Multicast Group Setting Parameters

3.2.2.7 Gateway Fleet

Milesight gateways can connect to UG67 network server. It is suggested to add not more than 5 gateways.

Gateway Fleet				
Gateway ID	Name	Status	Last Seen	Operation
24E124FFFEF12263	Local Gateway	Connected	2021-04-19 16:12:27	2×
				Œ

Figure 3-2-2-16

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

Table 3-2-2-14 Gateway Fleet Parameters

Gateway ID		
Name		
∟ocation		
GPS info will be displa	ayed by default or can be changed manua	ally
GPS info will be displa Latitude	ayed by default or can be changed manual Eg:0.026811	aliy
GPS info will be displi Latitude Longitude	ayed by default or can be changed manual Eg:0.026811 Eg:-18.286764	ally

Figure 3-2-2-17

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
Location	data it will replace your customized data.

Table 3-2-2-15 Gateway Setting Parameters

3.2.2.8 Packets

Milesight

Send Data To Device									
Device EUI		Туре	Payload			Port Confirmed			ł
000000000000000000	AS	cii 🗸				ł	85		Send
Send Data to Multicast G	roup								
Multicast Group		Туре		Payload			Port		
	✓ AS(cii 🗸				1	85		Send
Network Server									
Clear						S	earch		Q
Device EUI/Group	Gateway ID	Frequency	Datarate	RSSI/SNR	Size	Fcnt	Туре	Time	Details
		No	matching recor	rds found					

Figure 3-2-2-18

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

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

Network Server	
Item	Description
Device EUI/Group	Show the EUI of the device or multicast group.
Frequency	Show the used frequency to transmit packets.
Datarate	Show the used datarate to transmit packets.
SNR	Show the signal-noise ratio.
RSSI	Show the received signal strength indicator.
Size	Show the size of payload.
Fcnt	Show the frame counter.
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 3-2-2-17 Packet Parameters

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

Pack	ket Details		×
	Dev Addr/Multicast Addr	0614B991	A.
	GwEUI	24E124FFFEF0E225	
	AppEUI	24E124C0002A0001	
	Device EUI/Group Name	24E124126A210644	
	Class Type	Class C	
	Immediately	17.1	
	Timestamp	2721022973	
	Туре	UpUnc	
	Adr	false	
	AdrAcKReq	false	
	Ack	false	
	Fcnt	969	
	Port	85	-

Figure 3-2-2-19

ltem	Description
Dev	
Addr/Multicast	Show the address of the device/multicast group.
Addr	
GwEUI	Show the EUI of the gateway.
AppEUI	Show the EUI of the application.
DevEUI/Group	Show the FUIL of the device (multicast group name
Name	Show the Eor of the device/multicast group name.
Class Type	Show the class type of the device or multicast group.
	True: Device may transmit an explicit (possibly empty)
Immediately	acknowledgement data message immediately after the reception of a
	data message requiring a confirmation.
Timestamp	Show the timestamp of this packet.
Type	Show the type of the packet:
туре	JnAcc - Join Accept Packet

Milesight

	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
۸dr	True: The end-node has enabled ADR.
Au	False: The end-node has not enabled ADR.
	In order to validate that the network is receiving the uplink messages,
	nodes periodically transmit ADRACKReq message. This is 1 bit long.
A dr A al/Dag	True: Network should respond in ADR_ACK_DELAY time to confirm that
Adlackkeq	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.
Json	Show the data after decoded.
	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 3-2-2-18 Packets Details Parameters

Related Topic

Send Data to Device

3.3 Protocol Integration

3.3.1 BACnet Server

UG67 can work as LoRaWAN to BACnet gateway to integrate with BMS system easily.

3.3.1.1 Server

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



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

Table 3-3-1-1 Server Parameters

3.3.1.2 BACnet Object

Add	Bulk Import	Bulk Expo	Delete All	l i			Searc	ch	С
Object	Name	Object Type	Object Instance Nr	Present Value	Units	Updates	Update time	cov	Operation
24E124592B322	496.button	Analog-Input	0	1670892748800.0	no- units	539	2022-12-13 08:52:06	Disabled	ℓ ×

Figure 3-3-1-2

Item	Description
۸dd	Add a BACnet object. The gateway supports adding 2000
Add	objects at most.
Bulk Import	Download template and import multiple BACnet objects.
Bulk Export	Export all generated BACnet object settings.
Delete All	Delete all objects in the list.
Object Name	Show the name of the BACnet object.
Object Type	Show the type of this object.
Object Instance Nr	Show the instance number of this object.
Present Value	Show the latest value of object.
Units	Show the unit of this object value.
Updates	Show the update times of this object value.
Update time	Show the time for this object to get and update the data.
COV	Show if COV (Change of value) is enabled.
Operation	Edit or delete the object.

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

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



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

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

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

3.4 Network

3.4.1 Interface

3.4.1.1 Port

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

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

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

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

Port_1	
Port	eth 0 🗸
Connection Type	Static IP 🗸
IP Address	192.168.23.150
Netmask	255.255.255.0
Gateway	192.168.23.1
MTU	1500
Primary DNS Server	8.8.8.8
Secondary DNS Server	223.5.5.5
Enable NAT	

Figure 3-4-1-1

Port Setting			
Item	Description	Default	
Port	The port that is fixed as eth0 port and enabled.	eth 0	
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP	
MTU	Set the maximum transmission unit.	1500	
Primary DNS Server	Set the primary DNS.	8.8.8.8	
Secondary DNS Server	Set the secondary DNS.	223.5.5.5	
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable	

Table 3-4-1-1 Port Parameters

Related Configuration Example

Ethernet Connection

1. Static IP Configuration

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



- Port_1			
Port		eth 0	~
Connection Type		Static IP	~
1000			
IP Address		192.168.23.150	
Netmask		255 255 255 0	
		200.200.200.0	
Gateway		192.168.23.1	
MTU		1500	
Primary DNS Server		8888	
		0.0.0.0	
Secondary DNS Server		223.5.5.5	
Enable NAT			
Multiple IP Address			
	IP Address		

Figure 3-4-1-2

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 3-4-1-2 Static IP Parameters

2. DHCP Client

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

Port	eth 0	~
Connection Type	DHCP Client	~
MTU	1500	
Use Peer DNS		
Primary DNS Server	8.8.8.8	
Secondary DNS Server	223.5.5.5	
Enable NAT		

Figure 3-4-1-3

DHCP Client

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

3. PPPoE

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

Port_1		
Port	eth 0	~
Connection Type	PPPoE	~
Username		
Password		
Link Detection Interval(s)	60	
Max Retries	0	
MTU	1500	
Use Peer DNS		
Primary DNS Server	8.8.8.8	
Secondary DNS Server	223.5.5.5	
Enable NAT		

Figure 3-4-1-4

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

Table 3-4-1-4 PPPOE Parameters

3.4.1.2 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 Loopb	ack
WLAN			
Enable			
Work Mode		AP	~
SSID Broad	lcast		
AP Isolation	1		
Radio Type		802.11n(2.4GHz)	~
Channel		Auto	~
SSID			
BSSID			
Encryption I	Mode	No Encryption	~
Bandwidth		20MHz	~
Max Client	Number	10	
IP Setting			
Protocol		Static IP	~
IP Address			
		DHCP Settings	
Netmask			



WLAN		
Enable		
Work Mode	Client	✓ Scan
SSID		
BSSID		7
Encryption Mode	WPA-PSK/WPA2-PSK	~
Cipher	Auto	~
Кеу		
IP Setting		
Protocol	Static IP	~
IP Address		
Netmask	255.255.255.0	
Gateway		

Figure 3-4-1-6

WLAN Settings		
Item	Description	
Enable	Enable/disable WLAN.	

Work Mode	Select gateway's work mode. The options are "Client" or "AP".
DOOLD	Fill in the MAC address of the access point. Either SSID or BSSID
R22ID	can be filled to join 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
Enonyption Mode	Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" ,
Eliciyption Mode	"WPA-PSK/WPA2-PSK", "WPA-Enterprise", "WPA2-Enterprise" and
	"WPA-Enterprise/WPA2-Enterprise".
Ciphor	Select cipher. The options are "Auto", "AES", "TKIP" and
Cipitei	"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	Fill the apopymous identity of WPA (WPA2-Enterprise
Identity	Fin the anonymous identity of WFA/ WFA2-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
SSID Broadcast	find the SSID, and users have to enter the SSID manually to access to the wireless network.
SSID Broadcast	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP
SSID Broadcast AP Isolation	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other.
SSID Broadcast AP Isolation	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g
SSID Broadcast AP Isolation Radio Type	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".
SSID Broadcast AP Isolation Radio Type Channel	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11".
SSID Broadcast AP Isolation Radio Type Channel	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption.
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth	 find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz".
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP.
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting	 find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP.
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting Protocol	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP. Set the protocol in wireless network.
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting Protocol IP Address	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP. Set the protocol in wireless network. Set the IP address in wireless network.
SSID Broadcast AP Isolation Radio Type Channel Encryption Mode Cipher Key Bandwidth Max Client Number IP Setting Protocol IP Address Netmask	find the SSID, and users have to enter the SSID manually to access to the wireless network. When AP isolation is enabled, all users which access to the AP are isolated without communication with each other. Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"". Select wireless channel. The options are "Auto", "1", "2""11". Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK". Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP". Fill the pre-shared key of WPA encryption. Select bandwidth. The options are "20MHz" and "40MHz". Set the maximum number of client to access when the gateway is configured as AP. Set the protocol in wireless network. Set the IP address in wireless network. Set the netmask in wireless network.

Table 3-4-1-5 WLAN Parameters

P	ort WLAN	Cellular	Lo	opback				
< (GoBack							
	SSID	Channel	Signal	Cipher	BSSID	Security	Frequency	
	Vison Sensor_006602	Auto	-94dBm	Auto	24:e1:24:00:66:02	No Encryption	2462MHz	Join Network
	Milesight_Test	Auto	-88dBm	AES	ec:26:ca:99:3a:a4	WPA-PSK/WPA2-PSK	2437MHz	Join Network



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

Table 3-4-1-6 WLAN Scan Parameters

Related Topic

Wi-Fi Application Example

3.4.1.3 Cellular (Cellular Version Only)

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

Cellular Setting		
Enable		
Network Type	Auto	~
APN		
Username		
Password		
Access Number		
PIN Code		
Authentication Type	None	~
Roaming		
Customize MTU		
MTU	1500	
Enable IMS		
SMS Center		



Connection Setting		
Enable NAT		
Restart When Dial-up failed		
ICMP Server	8.8.8.8	
Secondary ICMP Server	223.5.5.5	
ICMP Detection Max Retries	3	
ICMP Detection Timeout	5 s	
ICMP Detection Interval	15 s	
SMS Settings		
SMS Mode	PDU ~	



General Settings	
Item	Description
Enable	Check the option to enable cellular feature.
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.
APN	Enter the Access Point Name for cellular dial-up connection provided by

Milesight

	local ISP.
Username	Enter the username for cellular dial-up connection provided by local ISP.
Password	Enter the password for cellular dial-up connection provided by local ISP.
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.
Authentication Type	Select from "None", "PAP", "CHAP".
Roaming	Enable or disable roaming.
Customized	Enable or disable to customize the maximum transmission units. When
MTU	disabled, the device will use operator's MTU settings.
MTU	Set the maximum transmission units. Range: 68-1500.
Enable IMS	Enable or disable IMS function.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Restart When	When this function is enabled, the gateway will restart automatically if the
Dial-up failed	dial-up fails several times.
ICMP Server	Set the ICMP detection server's IP address.
Secondary ICMP Server	Set the secondary ICMP detection server's IP address.
ICMP Detection Max Retries	Set max number of retries when ICMP detection fails.
ICMP Detection	Cat time a sut of IOMD data stice
Timeout	
ICMP Detection Interval	Set interval of ICMP detection.
SMS Mode	Select SMS mode from "TEXT" and "PDU".

Table 3-4-1-7 Cellular Parameters

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

Figure 3-4-1-10

ltem	Description
Connection Mode	

Milesight

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

Table 3-4-1-8 Cellular Parameters

Related Topics

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

3.4.1.4 Loopback

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

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

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

Figure 3-4-1-11

Loopback				
Item	Description	Default		
IP Address	Unalterable	127.0.0.1		
Netmask	Unalterable	255.0.0.0		

Multiple IP	Apart from the IP above, user can configure other IP	Null
Addresses	addresses.	INUII

Table 3-4-1-9 Loopback Parameters

3.4.1.5 VLAN Trunk

Milesight

UG67 gateway supports the Ethernet port working as VLAN Trunk client and be assigned a VLAN ID, which easy to traffic classification. When VLAN ID is set, port on "**Network"** > "**Interface"** > "**Port"** can be chosen as eth0.x with x being VLAN ID. VLAN Setting is blank by

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

Interface	VID	Operation
eth 0 🗸		×
		H



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

Table 3-4-1-10 VLAN Trunk Parameters

3.4.2 Firewall

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

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

3.4.2.1 Security

Security	ACL	DMZ	Port Mapping	MAC Binding
Website Block	ing by URL Ad	dress		
URL Address		http://] 💌
				8
Website Block	ing by Keywor	d		
Keyword] 💌
				Œ

Figure 3-4-2-1

Website Blocking	
URL Address	Enter the HTTP address which you want to block.
Keyword	You can block specific website by entering keyword. The maximum number of character allowed is 64.
	Table 3-2-2-1 Security Parameters

3.4.2.2 ACL

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

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

Security	ACL	DMZ	Port Mapping	MAC Binding			
ACL Setting							
Default Filter Po	blicy	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			Out ACL	Operation
							8

Figure 3-4-2-2

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

Destination Port	Select destination port type, such as specified port, port range,
Туре	etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination	Set start destination port number. Range: 1-65535.
FUIL	
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 3-4-2-2 ACL Parameters

3.4.2.3 DMZ

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

Security	ACL	DMZ	Port Mapping
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 3-4-2-3 DMZ Parameters

3.4.2.4 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published ext ernally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection into the an internal connection. This conversion is called DNAT, which is mainly used for external and interval services.

Click 🛨 to add a new port mapping rules.

Security	ACL	DMZ	Port Mapping	MAC E	Binding		
Port Mapping							
Sourc	e IP S	ource Port	Destination IP	Destination Port	Protocol	Description	Operation
0.0.0/0					TCP 🗸		
							Ð

Figure 3-4-2-4

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

Table 3-4-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.4.2.5 MAC Binding

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

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

Figure 3-4-2-5

MAC Binding Lis	it
ltem	Description
MAC Address	Set the binding MAC address.

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

Table 3-4-2-5 MAC Binding Parameters

3.4.3 DHCP

UG67 can be set as a DHCP server to distribute IP address when Wi-Fi work as AP mode.

]	
]]	
]	
]	
]	

Figure 3-4-3-1

DHCP Server		
Item	Description	Default
Enable	Enable or disable DHCP server.	Enable
Interface	Only wlan interface is allowed to distribute IP addresses.	wlan0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary	Set the primary DNS server.	8.8.8.8

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 3-4-3-1 DHCP Server Parameters

3.4.4 DDNS

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

DDNS										
DDNS Method	List	Service Type	Username	User ID	Password	Server	Server Path	Hostname	Appe nd IP	Oper ation
	wlan0 🗸	DynDl 🗸								×

Figure 3-4-4-1

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

Table 3-4-4-1 DDNS Parameters

3.4.5 Link Failover

Milesight

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

Configuration Steps

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

3.4.5.1 SLA

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

SLA	Tr	ack WA	AN Failover							
SLA Ent	ry									
	ID	Туре	Destination Address	Secondary Destination Address	Data Size	Interval(s)	Timeout(ms)	Packet Loss Count	Start Time	Operation
[1	icmp-echo	♥ 8.8.8.8	223.5.5.5	56	15	5000	3	now 🗸	×
										H

Figure 3-4-5-1

SLA		
ltem	Description	Default
ID	SLA index. Up to 10 SLA settings can be added. Range: 1-10.	1
Туре	ICMP-ECHO is the default type to detect if the link is alive.	icmp-echo
Destination Address	The detected IP address.	8.8.8.8
Secondary Destination Address	The secondary detected IP address.	223.5.5.5
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 3-4-5-1 SLA Parameters

3.4.5.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and Application module. Track setting is located between application module and SLA module

with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

Linkage between Track Module and SLA module

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

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

Linkage between Track Module and Application Module

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

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

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

SLA	Track	WAN Failover				
Track Object						
ID	Туре	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)	Operation
1	sla	▼ 1 ▼	wlan0 🗸	0	1	×
						Ð

Figure 3-4	4-5-2
------------	-------

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

Table 3-4-5-2 Track Parameters

3.4.5.3 WAN Failover

Milesight

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.

S	LA Tr	ack	WAN Fa	ilover				
WA	AN Failover							
	Main Interface	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 3-4-5-3

WAN Failover		
Parameters	Description	Default
Main Interface	Select a link interface as the main link.	
Backup Interface	Select a link interface as the backup link.	
Startup Delay (s)	Set how long to wait for the startup tracking detection policy to take effect. Range: 0-300.	30
Up Delay (s)	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time. Range: 0-180 (0 refers to immediate switching)	0
Down Delay (s)	When the primary interface switches from successful 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 3-4-5-3 WAN Failover Parameters

3.4.6 VPN

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

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

3.4.6.1 DMVPN

Milesight

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client
DMVPN Setting	gs				
Enable					
Hub Address					
Local IP Addres	s				
GRE HUB IP Ac	ldress				
GRE Local IP A	ddress				
GRE Mask			255.255.255.0		
GRE Key					
Negotiation Mod	je –		Main	٣	
Authentication A	Algorithm		DES	•	
Encryption Algo	rithm		MD5	¥	
DH Group			MODP768-1	•	
Key			-		
Local ID Type			Default	•	
IKE Life Time(s))		10800		
SA Algorithm			DES-MD5	•	
PFS Group			NULL	•	
Life Time(s)			3600		
		Fiç	gure 3-4-6-1		



Figure 3-4-6-2

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.

Milesight

Negotiation Mode	Select from "Main" and "Aggressive".
Authentication Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
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.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of Nhrp protocol.

Table 3-4-6-1 DMVPN Parameters

3.4.6.2 IPSec

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

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

DMVPN	IPsec	GRE	L2TP	PPTP
IPsec Settings				
- IPsec_1				
Enable		V		
IPsec Gate	way Address			
IPsec Mod	e	Т	unnel	*
IPsec Proto	ocol	E	SP	•
Local Subr	iet			
Local Subn	iet Mask			
Local ID Ty	/pe	D	efault	*
Remote Su	ibnet			
Remote Su	ibnet Mask			
Remote ID	Туре	D	efault	•

Figure 3-4-6-3

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

Table 3-4-6-2 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	T
Negotiation Mode	Main	•
Encryption Algorithm	DES	•
Authentication Algorithm	MD5	•
DH Group	MODP768-1	•
Local Authentication	PSK	•
Local Secrets		
XAUTH		
Lifetime(s)	10800	
SA Parameter		
SA Algorithm	DES-MD5	۲
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".		
	Select from "NULL", "MODP768_1" , "MODP1024_2" and		
ri S Gloup	"MODP1536_5".		
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.		
DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.		
----------------------	---	--	--
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.		
IPsec Advanced			
Enable Compression	The head of IP packet will be compressed after it's enabled.		
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.		

Table 3-4-6-3 IPsec Parameters

3.4.6.3 GRE

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

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

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

DM	VPN	IPsec	GRE	L2TP	PPTP
GRE	Settings				
-	GRE_1				
	Enable			×	
	Remote IP Ad	dress			
	Local IP Addre	ess			
	Local Virtual I	P Address			
Netmask				255.255.255.0	
	Peer Virtual IF	Address			
	Global Traffic	Forwarding			
	Remote Subn	et			
	Remote Netm	ask			
	MTU			1500	
	Key				
	Enable NAT			v	

Figure 3-4-6-5

GRE	
Item	Description
Enable	Check to enable GRE function.

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

Table 3-4-6-4 GRE Parameters

3.4.6.4 L2TP

Milesight

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

DMVPN	IPsec	GRE	L2TP	PPTP
— L2TP_1				
Enable		V	i	
Remote IF	Address			
Username	•			
Password				
Authentica	ation		Auto	~
Global Tra	ffic Forwarding	C)	
Remote S	ubnet		10.5.22.0	
Remote S	ubnet Mask		255.255.255.0	
Key				
Use L2TP	Peer DNS			

Figure 3-4-6-6

L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.

Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and "MS-CHAPv2".
Global Traffic	All of the data traffic will be sent out via L2TP tunnel after
Forwarding	this function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Key	Enter the password of L2TP tunnel.
Use L2TP Peer DNS	Enable to use the DNS address of peer L2TP server .

Table 3-4-6-5 L2TP Parameters

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

Figure 3-4-6-7

Advanced Settings		
Item	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 (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-4-6-6 L2TP Parameters

3.4.6.5 PPTP

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

DMVPN	IPsec	GRE	L2TP	PPTP
PPTP Settings	i.			
- PPTP_1				
Enable				
Remote IF	^o Address			
Username	•			
Password				
Authentica	ation		Auto	•
Global Tra	affic Forwarding			
Remote S	ubnet			
Remote S	ubnet Mask			

Figure 3-4-6-8

PPTP	
Item	Description
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP
Remote il Address	server.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authoritoption	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and
Authentication	"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	3-4-6-7 PPTP Parameters		
	Advanced Settings				
	Local IP Address				
	Peer IP Address				
	Enable NAT				
	Enable MPPE				
	Address/Control Comp	ression			
	Protocol Field Compres	ssion			
	Asyncmap Value		fffffff		
	MRU		1500		
	MTU		1500		
	Link Detection Interval	(s)	60		
	Max Retries		0		
	Expert Options				

Figure 3-4-6-9

PPTP Advanced Settings			
Item	Description		
Local IP Address	Set IP address of PPTP client.		
Peer IP Address	Enter tunnel IP address of PPTP server.		
Enable NAT	Enable the NAT faction of PPTP.		
Enable MPPE	Enable MPPE encryption.		
Address/Control 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	Set the link detection interval time to ensure tunnel		
(s)	connection. Range: 0-600.		
Max Petries	Set the maximum times of retrying to detect the PPTP		
	connection failure. Range: 0-10.		
Expert Options	User can enter some other PPP initialization strings in this		
	field and separate the strings with blank space.		

Table 3-4-6-8 PPTP Parameters

3.4.6.6 OpenVPN Client

Milesight

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. UG67 supports running at most 3 OpenVPN clients at the same time.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certificatio
OpenVPN CI	ient Settings						
— OpenVF	PN_1						
Enable							
Protoco	1	UDF	>	¥			
Remote	IP Address						
Port		1194					
Interface	е	tun		•			
Authent	ication	Non	e	T			
Local Tu	unnel IP						
Remote	Tunnel IP						
Enable	NAT						
Compre	ession	LZC		•			
Link De	tection Interval(s)	60					
Link De	tection Timeout(s)	300					
Cipher		Non	e	•			
MTU		1500	r.				
Max Fra	ame Size	1500	1				
Verbose	e Level	ERF	ROR	•			
Expert (Options						
Local R	loute						
		Subnet			Subnet Mas	ĸ	Operation
							8

Figure 3-4-6-10

OpenVPN Client	
Item	Description
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.
Protocol	Select from "UDP" and "TCP".
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Dort	Enter the listening port number of remote OpenVPN server.
Poll	Range: 1-65535.
Interface	Select from "tun" and "tap".
	Select authentication type used to secure data sessions.
Authoptication	Pre-shared: use the same secret key as server to complete
Authentication	the authentication. After selecting, go to Network > VPN >
	Certifications page to import a static.key to PSK field.

	Username/Password: use username/password which is
	preset in server side to complete the authentication.
	X.509 cert: use X.509 type certificate to complete the
	authentication. After selecting, go to Network > VPN >
	Certifications page to import CA certificate, client certificate
	and client private key to corresponding fields.
	X.509 cert + user: use both username/password and X.509
	cert authentication type.
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.
	Disable or enable TLS authentication when authentication
	type is X.509 cert. After being enabled, go to Network >
Enable TLS	VPN > Certifications page to import a ta.key to TA field.
Authentication	Note: this option only supports tls-auth. For tls-crypt, please
	add this format string on expert option: tls-crypt
	/etc/openvpn/openvpn-client1-ta.key
Username	Enter username provided by OpenVPN server.
Password	Enter password provided by OpenVPN server.
Enable NAT	Enable NAT traversal function.
Compression	Select LZO to compress data.
Link Detection Interval	Set link detection interval time to ensure tunnel connection.
(s)	Range: 10-1800.
Link Detection Timeout	Set link detection timeout. OpenVPN will be reestablished
(s)	after timeout. Range: 60-3600.
Ciphor	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC",
Cipilei	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".
Export Optiono	User can enter some other initialization strings in this field
Expert Options	and separate the strings with semicolon.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.

Table 3-4-6-9 OpenVPN Client Parameters

3.4.6.7 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 Serve	r Settings					
Enable						
Protocol		UDP		*		
Port		1194				
Listening IP						
Interface		tun		v		
Authentication		None		¥		
Local Virtual IP						
Remote Virtual IP						
Enable NAT						
Compression		LZO		*		
Link Detection Inte	erval	60				
Cipher		None				
MTU		1500				
Max Frame Size		1500				
Verbose Level		ERROR		•		
Expert Options						



Local Route			
	Subnet	Netmask	Operation
			8
Account			
	Username	Password	Operation
			H

Figure 3-4-6-12

OpenVPN Server	
Item	Description
Enable	Enable/disable OpenVPN server.
Protocol	Select from TCP and UDP.
Port	Fill in listening port number. Range: 1-65535.
Listoping ID	Enter WAN IP address or LAN IP address. Leaving it blank
Listening iP	refers to all active WAN IP and LAN IP address.
Interface	Select from " tun" and "tap".
	Select authentication type used to secure data sessions.
Authoptication	Pre-shared: use the same secret key as server to complete
Authentication	the authentication. After selecting, go to Network > VPN >
	Certifications page to import a static.key to PSK field.

	Username/Password: use username/password which is
	preset in server side to complete the authentication.
	X.509 cert: use X.509 type certificate to complete the
	authentication. After selecting, go to Network > VPN >
	Certifications page to import CA certificate, client
	certificate and client private key to corresponding fields.
	X.509 cert + user: use both username/password and X.509
	cert authentication type.
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.
	Renegotiate data channel key after this interval. 0 means
Renegotiation Interval(s)	disable. Range: 0-86400.
Max Clients	Maximum OpenVPN client number, Range: 1-128.
	Disable or enable TLS authentication when authentication
	type is X.509 cert. After being enabled, go to Network >
Enable TLS	VPN > Certifications page to import a takey to TA field.
Authentication	Note: this option only supports tls-auth. For tls-crypt, please
	add this format string on expert option: tls-crvpt
	/etc/openypn/openypn-client1-ta.key
Enable CRL	Enable or disable CRL verify.
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 "I 70" to compress data
Compression	Set link detection interval time to ensure tunnel connection
Link Detection Interval	Range: 10-1800.
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC",
	"AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 64-1500.
Max Frame Size	Set the maximum frame size. Range: 64-1500.
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".
Export Optiono	User can enter some other initialization strings in this field
Expert Options	and separate the strings with semicolon
Local Route	
Subnet	The real local IP address of OpenVPN client.
Netmask	The real local netmask of OpenVPN client.
Account	
Username & Password	Set username and password for OpenVPN client.
Client Subnet	
Name	Set the name as OpenVPN client certificate common name.
Subnet	Set the subnet of OpenVPN client.

Subnet Mask	Set the subnet netmask of OpenVPN client.
Т	able 3-4-6-10 OpenVPN Server Parameters

3.4.6.8 Certifications

Milesight

When working as OpenVPN server, OpenVPN client or IPsec Server, user can import/export necessary certificate and key files to this page according to the authentication types.

Oper	VPN Client						
—	OpenVPN client_1						
	CA	Browse	Import	Export	Delete		
	Public Key	Browse	Import	Export	Delete		
	Private Key	Browse	Import	Export	Delete		
	ТА	Browse	Import	Export	Delete		
	Preshared Key	Browse	Import	Export	Delete		
	PKCS12	Browse	Import	Export	Delete		
+	OpenVPN client_2						
+	OpenVPN client_3						



OpenVPN	Server				
— Oper	VPN Server				
CA		Browse	Import	Export	Delete
Publ	ic Key	Browse	Import	Export	Delete
Priva	te Key	Browse	Import	Export	Delete
DH		Browse	Import	Export	Delete
TA		Browse	Import	Export	Delete
CRL		Browse	Import	Export	Delete
Pres	hared Key	Browse	Import	Export	Delete



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

Figure 3-4-6-15

3.5 System

Milesight

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

3.5.1 General Settings

3.5.1.1 General

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

General	System Time	SMTP	Phone	Email	
System					
Hostname		GATEWAY			
Web Login Time	eout(s)	1800			
Access Servic	e				
	Enable	Serv	vice		Port
		нт	TP	[80
		HTT	PS	[443
		TELI	NET	[23
		SS	Η	[22
HTTPS Certific	cates				
Certificate	https.crt	Browse	Import Expo	rt Delete	
Key	https.key	Browse	Import Expo	rt Delete	

Figure 3-5-1-1

General						
Item	Description	Default				
System						
Hostname	User-defined gateway name, needs to start with a letter.	GATEWAY				
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800				
Access Servic	Access Service					
Port	Set port number of the services. Range: 1-65535.					
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80				
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443				
TELNET	Users can log in the device locally and remotely via	23				

83

	TELNET to access and control it through Web after option is checked.	
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.	
Key	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into gateway. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.	

Table 3-5-1-1 General Setting Parameters

3.5.1.2 System Time

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

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

General	System Time	SMTP	Phone	Email
System Time S	ettings			
Current Time		2019-06-12 20:34	:32 Wed	
Time Zone		8 China (Beijing)	¥	
Sync Type		Sync with Browse	ır ∎ ▼	
Browser Time		2019-06-12 20:34	:32 Wed	



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. Sync with NTP Server: Synchronize time with NTP Server. Set up Manually: configure the time manually.
Sync with NTP Server	
NTP Server Address	Set NTP server address (domain name/IP).

Enable NTP Server	After checked, NTP client on the network can achieve time				
	synchronization with gateway.				

Table 3-5-1-2 System Time Parameters

3.5.1.3 SMTP

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

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

Figure 3-5-1-3

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

Table 3-5-1-3 SMTP Setting

Related Topics

Events Setting

3.5.1.4 Phone

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

85

gateway with cellular feature.

General	System Time	SMTP	Phone	Email		
Phone Number Lis	t					
	Name				Number	Operation
	List1				654321;123456	
Save						



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

Table 3-5-1-4 Phone Settings

Related Topic

Connect on Demand

3.5.1.5 Email

Email settings involve email alarm for events.

General	System Time	SMTP	Phone	Email		
Email List						
	Nam	9			Email Address	Operation
	list1				sam@user.com;hot@gmail.com	\mathbf{x}
						Ð
Save	í.					

Figure 3-5-1-5

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

Table 3-5-1-5 Email Settings

3.5.2 User Management

3.5.2.1 Account

Milesight

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

Table 3-5-2-1 Account Information

3.5.2.2 User Management

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

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

Figure 3-5-2-2

User Management	
Item	Description
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.
Password	Set password.

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

Table 3-5-2-2 User Management

3.5.3 SNMP

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

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

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

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

3.5.3.1 SNMP

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	Trap	MIB
Packet Forwarder	SNMP Settin	gs			
	Enable				
Network Server	Port		161		
	System Name		24E124FF	FEF24660	
Network 🕨	SNMP Versior	1	SNMPv2		~
Sustam 🔻	Location Inform	mation			
System	Contact Inform	nation			
General Settings			, <u>.</u>		
User Management	Save				
SNMP					

Figure 3-5-3-1

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

Table 3-5-3-1 SNMP Parameters

3.5.3.2 MIB View

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

SNMP	MIB View	VACM	Тгар	MIB	
View List					
V	iew Name	View	Filter	View OID	Operation
All		Included	٣	1	×
system		Included	Ŧ	1.3.6.1.2.1.1	
					Ŧ



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

Table 3-5-3-2 MIB View Parameters

3.5.3.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Trap	MIB		
NMP v1 & v2 U	ser List					
Commun	ity	Permission	MIB Vie	w	Network	Operation
private	Read	-write 🔻	All	•	0.0.0/0	×
public	Read	-only 🔻	none	•	0.0.0.0/0	×

Figure 3-5-3-3

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

3.5.3.4 Trap

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

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

Figure 3-5-3-4

SNMP Trap		
Item	Description	
Enable	Enable or disable SNMP Trap function.	
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.	
Server Address	Fill in NMS's IP address or domain name.	
Port	Fill in UDP port. Port range is 1-65535. The default 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	
	AULII & MIV .	

Table 3-5-3-4 Trap Parameters

3.5.3.5 MIB

This section describes how to download MIB files.

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

Figure 3-5-3-5

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

Table 3-5-3-5 MIB Download

3.5.4 Device Management

3.5.4.1 Auto Provision

Users can customize and select the configuration profile from Milesight Development Platform. When Auto Provision is enabled and the device is connected to Internet, the device will receive the profile to achieve initial configuration. This feature will work even the device does not configure to connect Milesight Development Platform.



3.5.4.2 Management Platform

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.

Management Platform		
Enable		
Platform Type	DeviceHub 1.0	~
Activation Server Address		
Device Management Server Ac	Idress	
Activation Method	By ID	~
ID		
Password		
Status	Disconnected	

Figure 3-5-5-1

Management Platform		
Item	Description	
Enable	Enable or disable to connect gateway to management platform.	
Platform Type	Milesight DeviceHub 1.0 or Milesight Development Platform is optional.	
Status	Show the connection status between the gateway and the management platform.	

DeviceHub 1.0	
Activation Server Address	IP address or domain of the DeviceHub.
DeviceHub Management Address	The URL address for the device to connect to the DeviceHub, e.g. http://220.82.63.79:8080/acs.
Activation Method	Select activation method to connect the gateway to the DeviceHub server, options are "By Authentication ID" and "By ID".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
ID Password	Fill in the registered DeviceHub account (email) and password.

Table 3-5-5-1

3.5.5 Events

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

3.5.5.1 Events

You can view alarm messages on this page.

tatus	Events	Events Setti	ings			
LoRaWAN	Mark as Rea	ad Delete	Mark All	as Read	elete All Alarms	
Network		Status	Туре	Time	Me	ssage
System 🔻	< > 10	Go to:	GO			
General Settings						
User Management						
AAA						
Device Management						
Events						

Figure 3-5-6-1

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

Time Sr	how the alarm time.
Message Sh	show the alarm content.

Table 3-5-6-1 Events Parameters

3.5.5.2 Events Settings

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

Events Settings			
Enable			
Phone for Notification	~]	
Email for Notification	~		
Events	Record	Email Email Setting	SMS SMS Setting
Cellular Up			
Cellular Down			
WAN Up			
WAN Down			
VPN Up			
VPN Down			
Power On			
Power Off			
Connect to UPS External Power Supplies			
Connect to UPS Internal Battery			
UPS Low Power (20%)			
UPS Abnormal Charging			
Disconnect the UPS			

Figure 3-5-6-2

Event Settings		
Item	Description	
Enable	Check to enable "Events Settings".	
Phone for	Salaat ahana group ta raasiya SMS alarm	
Notification	Select phone group to receive SMS alarm.	
Email for	Salaat Email group to roopiyo Email alarm	
Notification	elect Email group to receive Email alarm.	
Events	Event type the gateway supports to record.	

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.

Table 3-5-6-2 Events Parameters

Related Topics

Email Setting

Phone Setting

3.6 Maintenance

This section describes system maintenance tools and management.

3.6.1 Tools

Troubleshooting tools includes ping and traceroute.

3.6.1.1 Ping

Ping tool is engineered to ping outer network.

Ping	Traceroute	Qxdmlog		
IP Ping				
Host			Ping	Stop

Figure 3-6-1-1

Description
Ping outer network from the gateway.

Table 3-6-1-1 IP Ping Parameters

3.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.



3.6.1.3 Qxdmlog

This section allow collecting diagnostic logs of cellular module via QXDM tool.



Figure 3-6-1-3

3.6.2 Schedule

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

Status		Schedule				
LoRaWAN	۲	Schedule				
Network	۲	Schedule	Frequency	Hour	Minute	Operation
System	Þ	Save				
Maintenance	-					
Tools						
Schedule						

Figure 3-6-2-1

Schedule	
Item	Description
Schedule	Select schedule event:

	Reboot: Reboot the gateway regularly.	
Frequency	Select the frequency to execute the schedule.	
Hour & Minute Select the time to execute the schedule.		

Table 3-6-2-1 Schedule Parameters

3.6.3 Log

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

3.6.3.1 System Log

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

Download			
File	Log File	Download	
Log			
View recent(lines)	20	•	
Thu Jul 18 15:01:25 2019 us	er.notice redis[1859]: Background	saving terminated with success	
Thu Jul 18 15:06:26 2019 us	er.notice redis[1859]: 10 changes	in 300 seconds. Saving	
Thu Jul 18 15:06:26 2019 us	er.notice redis[1859]: Background	saving started by pid 11683	
Thu Jul 18 15:06:26 2019 us	er.notice redis[11683]: DB saved	n disk	
Thu Jul 18 15:06:26 2019 us	er.notice redis[1859]: Background	saving terminated with success	
1110 001 10 10.00.20 2010 00	er.notice redis[1859]: 10 changes	n 300 seconds. Saving	
Thu Jul 18 15:11:27 2019 us			
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us	er.notice redis[1859]: Background	saving started by pid 15776	
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us	er.notice redis[1859]: Background er.notice redis[15776]: DB saved	saving started by pid 15776 n disk	
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:11:27 2019 us	er.notice redis[1859]: Background er.notice redis[15776]: DB saved er.notice redis[1859]: Background	saving started by pid 15776 •n disk saving terminated with success	
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[1859]: Background er.notice redis[15776]: DB saved er.notice redis[1859]: Background er.notice redis[1859]: 10 changes	saving started by pid 15776 n disk saving terminated with success in 300 seconds. Saving	
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[1859]: Background er.notice redis[15776]: DB saved er.notice redis[1859]: Background er.notice redis[1859]: 10 changes er.notice redis[1859]: Background	saving started by pid 15776 n disk saving terminated with success in 300 seconds. Saving saving started by pid 19899	
Thu Jul 18 15:11:27 2019 us Thu Jul 18 15:16:28 2019 us Thu Jul 18 15:16:28 2019 us Thu Jul 18 15:16:28 2019 us	er.notice redis[1859]: Background er.notice redis[18776]: DB saved. er.notice redis[1859]: Background er.notice redis[1859]: 10 changes er.notice redis[1859]: Background er.notice redis[19899]: DB saved	saving started by pid 15776 n disk saving terminated with success in 300 seconds. Saving saving started by pid 19899 in disk	

Figure 3-6-3-1

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

Table 3-6-3-1 System Log Parameters

3.6.3.2 Log Settings

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

System Log	Log Settings			
Remote Log Server				
Enable				
Syslog Server Address			1 1]
Port		514]
Local Log File				
Storage		local	v]
Size		1024		КВ
Log Severity		Info	•]

Figure 3-6-3-2

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

Table 3-6-3-2 System Log Parameters

3.6.4 Upgrade

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

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

Milesight

Upgrade			
Gateway			
Firmware Version	60.0.0.42-r5		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade

Figure 3-6-4-1

Upgrade	
Item	Description
Firmware Version	Show the current firmware version.
Reset Configuration to Factory Default	When this option is checked, the gateway will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade" to upgrade firmware.
	Table 0.6.4.1 University Demonstrate

Table 3-6-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.6.5 Backup and Restore

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

Backup and Restore			
Restore Config			
Config File		Browse	Import
Backup Running-con	fig		
Full Backup Ba	atch Backup		
Restore Factory Defa	ults		
Reset			

Figure 3-6-5-1

Backup and R	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.		
Full Backup	Click "Full Backup" to export the current configuration file to the PC.		
	Click "Batch Backup" to export current configuration except gateway ID		
Batch	of packet forwarder, all embedded NS settings, static IP address of		
Backup	WAN, WLAN settings, user management settings, DeviceHub		
	authentication code, all APP settings.		
Pocot	Click "Reset" button to reset factory default settings. gateway will		
neoet	restart after reset process is done.		

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

Related Configuration Example

Restore Factory Defaults

3.6.6 Reboot

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

Reboot		
Reboot		
	Figure 3-6-6-1	

3.7 APP

3.7.1 Python

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

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

Users can use Python to quickly generate the prototype of the program, which can be the

final interface of the program, rewrite it with a more appropriate language, and then encapsulate the extended class library that Python can call.

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

3.7.1.1 Python

Milesight

Python	AppManag	er Configuration	Python APP		
Python					
AppManager S	itatus	Uninstalled			
SDK Version					
SDK Path					
Available Stora	ige	local	~		
SDK Upload			Br	owse	Install

Figure 3-7-1-1

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

Table 3-7-1-1 Python Parameters

3.7.1.2 App Manager Configuration

Python /	AppManager Configuration	Python APP	
AppManager			
Enable			
App Management			
ID	App Comm	and Logfile Size(MB)	Uninstall
App Status			
Арр	Name	App Version	SDK Version

Figure 3-7-1-2

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

Table 3-7-1-2 APP Manager Parameters

3.7.1.3 Python App

Milesight

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

Figure 3-7-1-3

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

Table 3-7-1-3 APP Parameters

3.7.2 Node-RED

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

- LoRa Input: receive the LoRa data, please ensure the network server mode is enabled before using this node
- LoRa Output: send downlinks to LoRaWAN[®] nodes
- Device Filter: filter out the data of one or more specific LoRaWAN® nodes
- 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

3.7.2.1 Node-RED

Status		Node-RED		
Packet Forwarder		Node-RED		
letwork Server		Enable Node-RED Version	1.2.9	Launch
otocol Integration	•	Node Library Version	1.0.11	
etwork	•	All Flows	Export	Browse
stem	•	Restore Factory Defaults	Reset	
intenance	•	Save		
P	-			
Python				
Node-RED				

Figure 3-7-2-1

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

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

Related Configuration Example

Node-RED

Chapter 4 Application Examples

4.1 Restore Factory Defaults

Method 1:

Milesight

Log in web interface, and go to **Maintenance > Backup and Restore**, click **Reset** button, you will be asked to confirm if you'd like to reset it to factory defaults. Then click **Reset** button.

Network Server	Î	Backup and Restore	
Protocol Integration	•	Config File	Browse Import
Network	•	Backup Running-config	~
System	•	Full Backup Batch Backup	Reset operation will erase all configuration data on Gateway
Maintenance	-	Restore Factory Defaults	and reset the system to factory defaults. Continue?
Tools		_	Reset Califier
Schedule			
Log			
Upgrade			
Backup and Restore			

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



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

Related Topic

Restore Factory Defaults

Method 2:

Locate the reset button on the gateway, press and hold the reset button for more than 5s until the SYS LED blinks.

4.2 Firmware Upgrade

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

After getting firmware file please refer to the following steps to complete the upgrade.

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

Upgrade			
Gateway			
Firmware Version	60.0.0.42-r5		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade
Please keep	the power on during upgrade.		

Related Topic

4.3 Ethernet Connection

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

Port	WLAN	Cellular	Loopback	VLAN Trunk
- Port_1	t.			
Port			eth 0	~
Conne	ection Type		Static IP	~
IP Add	dress		192.1 <mark>6</mark> 8.44.186	
Netma	ask		255.255.255.0	
Gatew	vay		192.168.44.1	
MTU			1500	
Prima	ry DNS Server		8.8.8.8	
Secon	ndary DNS Server		223.5.5.5	
Enabl	e NAT			

- 2. Connect Ethernet port of gateway to devices like router or modem.
- 3. Go to "Maintenance > Tools > Ping" to check network connectivity.

Network Server	Ping Traceroute Qxdmlog		
Protocol Integration	Host www.google.com Ping Stop		
Network	PING www.google.com (172.217.25.4): 56 data bytes 64 bytes from 172.217.25.4: seq=0 ttl=117 time=20.090 ms		
System	64 bytes from 172.217.25.4: seq=1 ttl=117 time=19.786 ms 64 bytes from 172.217.25.4: seq=2 ttl=117 time=19.797 ms 64 bytes from 172.217.25.4: seq=3 ttl=117 time=19.750 ms		
Maintenance	www.google.com ping statistics 4 packets transmitted, 4 packets received, 0% packet loss		
Tools	round-trip min/avg/max = 19.150/19.855/20.090 ms		

Related Topic

Port Setting

4.4 Cellular Connection (Cellular Version Only)

1. Go to "Network > Interface > Cellular > Cellular Setting" and configure the necessary cellular info of SIM card, lick "Save" and "Apply" for configuration to take effect.

Cellular Setting		
Enable		
Network Type	Auto	~
APN		
Username		
Password		
Access Number		
PIN Code		
Authentication Type	None	~
Roaming		
Customize MTU		
MTU	1500	
Enable IMS		
SMS Center		

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

Overview	Packet Forward	Cellular	Network	WLAN
Modem				
Status		Ready		
Model		EC25		
Version		EC25ECGAR06A07N	/1G	
Signal Level		23asu (-67dBm)		
Register Status		Registered (Home ne	twork)	
IMEI		860425047368939		
IMSI		460019425301842		
ICCID		89860117838009934	120	
ISP		CHN-UNICOM		
Network Type		LTE		
PLMN ID				
LAC		5922		
Cell ID		340db83		
Network				
Status		Connected		
IP Address		10.132.132.59		
Netmask		255.255.255.240		
Gateway		10.132.132.60		

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.

WLAN	Cellular	Loopback
	AP	~
cast		
	802.11n	(2.4GHz) 🗸
	Auto	~
	Gateway	_F1200F
	24:e1:24	:f1:20:0f
Mode	No Encr	yption 🗸
	20MHz	~
Number	10	
	WLAN cast Mode	WLAN Cellular AP AP Cast Image: Second stress Sold stress Mode No Encr 20MHz 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	E	Enabled			
MAC Address	2	24:e1:24:f1:20:0f			
Interface Type	4	\P			
SSID		Gateway_F1200F			
Channel	A	Auto			
Encryption Type	1	No Encryption			
Status	t	Jp			
IP Address		192.168.1.1			
Netmask	2	255.255.255.0			
Connection Durati	on () 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	1	Cellular	Loop	back			
< GoBa	ack								
	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-PSK/	WPA2-PSK V	
Cipher		AES	~	
Key		•••••		
IP Setting				
Protocol		DHCP Clier	nt 🗸	

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
1	WLAN Status				
	Wireless Status		Enabled		
	MAC Address		24:e1:24:f0:de:14		
	Interface Type		Client		
	SSID		AAA		
	Channel		Auto		
	Encryption Type		WPA-PSK/WPA2-PSK		
	Cipher		AES		
	Status		Connected		
	IP Address		192.168.1.145		
	Netmask		255.255.255.0		
	Connection Duration		0 days, 02:44:45		

Related Topic

WLAN Setting

WLAN Status

4.6 Packet Forwarder Configuration

UG67 gateway has installed multiple packet forwarders including Semtech, Basic station, Chirpstack-Generic MQTT broker, etc. Before connecting make sure the gateway has

111

connected to network.

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

General	Radios	Advanced	Cust	om Traffi	c		
General Setting							
Gateway EUI	24E124FFF	EF12257					
Gateway ID	24E124FF	FEF12257					
Frequency-Sync	Disabled	N.	~				
Multi-Destination							
ID	Enable	•	Туре	Server Add	ress Connec	ct Status	Operation
0	Enabled	d Er	nbedded NS	localhos	st Conr	nected	
							Ħ

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

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

3. Go to "Packet Forwarder > Radio" page to configure 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		90	4.3	
	Radio 1		90	5.0	
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.

General	Radi	os Adv	anced	Custom	Traffic			
Traffic Set	ting							
Stop	C	lear						
Rfch	Direction	Time	Ticks F	requency	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 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	24E124FFFE 24E124FFF	EF12257 EEF12257				
Network	•	Frequency-Sync	Disabled		•			
System	۲	Multi-Destination						
		ID	Enable	Ту	pe	Server Address	Connect Status	Operation
Maintenance		0	Enabled	Embed	lded NS	localhost	Connected	
APP	×							æ

2. Go to "Packet Forwarder > Radio" page to configure center frequency and channels. The channels of the gateway and nodes need to be the same.

egion		US915		~
	Name			Center Frequency/MHz
	Radio 0		90	4.3
	Radio 1		90	5.0
lulti Channels Settin	g			
Enable	Index	Radio		Frequency/MHz
2	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	Padio 1	~	905 3

3. Go to "Network Server > 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	►		Milesight	IoT Cloud 🗸]
		NetID	010203]
System	۲	Join Delay	5		sec
Maintenance		RX1 Delay	1		sec
maintenance		Lease Time	8760-0-0		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.

114

Dashboard	Device	s	Gate	ways	listory	+					
My Devices	Search	1	٩		Normal 1	🛱 Alarm 1	M Offline 1	⊗ Inact	ive 3		+ New Device
Map Triggers		\otimes	真实设备-EN 6136A39023	Add Device				×		÷	@ LV (I)
Reports		\otimes	UC3X52-虚 61151109	* SN:				500	iated with your		@ <u>~</u> ()
Event Center 30		38(UC3X5 6123A124	Name.						15 minutes ago	@ № 0
Me		当	AM102- 6128A2175=	CO2	TVOC	Cancel	Confirm Barometric Pressure	ux lina	tion	a few seconds ago	<u>ن</u> ال
			4	27℃ Temperature	51% Humidity		D Activity Level (PIR)	2lux Illumina	tion		
≡•											

5. The gateway is online on Milesight IoT Cloud.

🕐 Dashboard	Devices	Gateways	+		
My Devices	Search	Q,	⊘ Normal 1 🔐 Offline 0 ⊗ Inactiv	e 0	+ New Devices
Map	Statu	is Name	Associated Devices (Joined /Not Joined /Failed)	Last Updated	
Reports	al al	UG Gateway 621793129987	0 / 1 / 0 Detail	2 minutes ago	<u>ک اما</u> ک
Event Center 94					····· ·

4.8 Application Configuration

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

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

2. Click to enter the configuration page, displayed as the following picture:

Applications	
Name	cloud
Description	cloud

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

HTTP or HTTPS:

Step 1: select HTTP or HTTPS as transmission protocol.

Туре	HTTP	•

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

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
			Œ

MQTT:

Step 1: select the transmission protocol as 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.



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

TLS		
Enable	۲	
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	device/test	QoS 0 ~
Downlink data		QoS 0 🗸
Multicast downlink data		QoS 0 🗸
Join notification		QoS 0 🗸
ACK notification		QoS 0 ~
Error notification		QoS 0 🗸
Request data	/event/request	QoS 0 🗸
Response data	/event/response	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.

Add	Bulk Import	Delete All			Search	Q
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
		No matc	hing records found			

Device Name	lora-sensor
Description	a short description of your node
Device EUI	00000000000000
Device-Profile	ClassA-OTAA 🗸
Application	cloud 🗸
Paylod Codec	•
fPort	1
Frame-counter Validation	
Application Key	
Device Address	
Network Session Key	
Application Session Key	
Uplink Frame-counter	0
Downlink Frame-counter	0
	Save & Apply

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

Import File	Browse	Import	Template Download	

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

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

Import this file to add bulks of devices.

4.10 Send Data to Device

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

1122612191	868100000	SF7BW125	-	1.75	17	0	JnAcc	2019-08-06T09:22:29+08:00	0
112261219	868100000	SF7BW125	9.5	-77	18	0	JnReq	2019-08-06T09:22:29+08:00	0

2. Fill in the device EUI or select the multicast group which you need to send downlinks.

Туре	Payload	Fport	Confirmed
ASCII 🔻	15	15	
Orred			
Send	send success		
	Type ASCII • Send	Type Payload ASCII	Type Payload Fport ASCII 15 15 Send send success

Then fill in the downlink commands, ports.

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.

Туре	Payload	Fport	Confirmed
ASCII 🔻	15	15	۲
	Type ASCII 🔻	Type Payload ASCII • 15	TypePayloadFportASCII1515

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	~	-	SF12BW125	869525000	1122612191311123
Pending 🕕	DnCnf	2	6				0	1122612191311123

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

Device EUI	Frequency	Datarate	SNR	RSSI	Size	Fcnt	Туре	Time	Details
11226121913	868300000	SF10BW125		-	0	3	DnUnc	2019-08-06T09:23:44+08:00	0
1122612191	868300000	SF10BW125	10.5	-75	64	2	UpCnf	2019-08-06T09:23:44+08:00	
112261219	869525000	SF12BW125		12	6	2	DnCnf	2019-08-06T09:22:55+08:00	0
112261219	0				6	2	DnCnf		0
112261219	868500000	SF10BW125	0.00	-	0	1	DnUnc	2019-08-06T09:22:49+08:00	0

Packets Details		
Dev Addr	07e7	A
GwEUI	24e124ff	
AppEUI	557240	
DevEUI	1122612191311123	
6 Immediately	128	
⁶ⁱ Timestamp	874346044	
6 Туре	UpCnf	
Adr	false	
6 AdrAcKReq	false	
Ack	true	
Fcnt	21	
Fport	55	
6 Modulation	LORA	

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.



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

Reference in the second s			_
	Node-RED	Usemame: 1 Password: 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 Filter node		
				Delete		Cancel Done
				© Properties		• 2 1
				Name	AM100	
				Device EUI	24E124127A270222	+
	LoRa Input	-AM100				

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

harry	test1	test	chenpan	Edit Decoder node					
				Delete			Cancel Done		
	, i i i i i i i i i i i i i i i i i i i	© Properties			• • •				
	LoPa Inout	484100	AM 100 Decoder	Name AM 10	00 Decoder				
	Lorda mpar			Device Type AM10	00 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		test	chenpan	Edit Email Outpu	ut node			
				Delete		Cancel	Done	e
				© Properties			•	Þ
				Name	AM100 Data to Email			
LORa	input y	Амтоо 9	AM 100 Decoder	SMTP Option	Custom 🗸			
				User ID	@milesight.com			
			msg.payload	Password				
				SMTP Server Address	smtp.exmail.qq.com			
				Port [1-65535]	25			
				Enable TLS				
	WAN UP			То	@milesight.com	+		
				Торіс	AM100 Data			
				Payload	The time is {{time}} Deveui is {{deveui}} counter is {{payload humidity}}	ß		

Note:

1) 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.



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

M100 Data ★		
		2021-0
From	@milesight.com>	
То	@milesight.com>	
Time: 2021年	4月30日 (周五) 17:13 🔊	
Size: 2 KB		

Related Topic

Node-RED

[END]