

Semi-industrial LoRaWAN[®] Gateway UG65

User Guide



Preface

Milesight

Thanks for choosing Milesight UG65 LoRaWAN[®] gateway. UG65 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 UG65 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
UG65 Datasheet	Datasheet for UG65 LoRaWAN® gateway.
UG65 Quick Start Guide	Quick Installation Guide for UG65 LoRaWAN® gateway.

Declaration of Conformity

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





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	
Aug. 31, 2020	V1.0	Initial version	
Dec. 10, 2020	V2.0	Layout replace	
		1. Support LoRaWAN [®] Class B	
		2. Add Node-RED feature	
Apr. 30, 2021	V2.1	3. Add Noise-Analyzer feature	
		4. Add Multicast Group feature	
		5. Add application examples	
		1. Support Yeastar Workplace platform integration	
Aug. 24, 2021	V2.2	2. Delete Package Forward status page	
		3. Phone & Email webpage update	
		1. Add AS923-3&AS923-4	
Dec. 15, 2021	V2.3	2. Change network server channel mask box to channel	
		3. Add device channel setting in profile	
		1. Add batch backup	
Feb. 18, 2022	V2.4	2. Log in webpage update	
100.10,2022		3. Change default antenna type to external antenna	
		4. Adjust time of Class C ACK timeout	
		1. Support VLAN Trunk client	
Jun. 1, 2022	V2.5	2. Add System Name in SNMP	
		3. Add Use L2TP Peer DNS option	
		1. Add BACnet Server feature	
Dec.26, 2022	V2.6	2. Add Payload Codec feature	
200.20, 2022	12.0	3. Add Reset and all flows export feature on Node-RED	
		4. Add data retransmission feature on Packet Forward	
		1. Compatible with Milesight Development Platform	
	V2.7	2. Update default secondary ICMP and DNS server	
Feb. 21, 2024		address	
,		3. Add cellular IMS and custom MTU feature	
		4. Add 8 pre-set device profiles	
		5. Add beacon time offset setting	
June 7, 2024	V2.8	1. Support to import ovpn file for OpenVPN connection;	
		2. Support packet filter feature;	

3

3. Add default WLAN connection password;
4. Add username on SMTP client setting;
5. Add BACnet object types, support object instance
customization.

Contents

Chapter 1 Product Introduction	8
1.1 Overview	8
1.2 Advantages	8
1.3 Specifications	9
1.4 Dimensions (mm)	11
Chapter 2 Access to Web GUI	12
2.1 Wireless Access	12
2.2 Wired Access	13
Chapter 3 Web Configuration	16
3.1 Status	16
3.1.1 Overview	16
3.1.2 Cellular	17
3.1.3 Network	18
3.1.4 WLAN	19
3.1.5 VPN	21
3.1.6 Host List	22
3.2 LoRaWAN	23
3.2.1 Packet Forwarder	
3.2.1.1 General	
3.2.1.2 Radios	25
3.2.1.3 Noise Analyzer	27
3.2.1.4 Advanced	28
3.2.1.5 Custom	
3.2.1.6 Traffic	
3.2.2 Network Server	31
3.2.2.1 General	31
3.2.2.2 Application	33
3.2.2.3 Payload Codec	
3.2.2.4 Profiles	39
3.2.2.5 Device	41
3.2.2.6 Multicast Groups	43
3.2.2.7 Gateway Fleet	45
3.2.2.8 Packets	46
3.3 Protocol Integration	
3.3.1 BACnet Server	49
3.3.1.1 Server	49
3.3.1.2 BACnet Object	50
3.4 Network	51
3.4.1 Interface	51
3.4.1.1 Port	51
3.4.1.2 WLAN	54

3.4.1.3 Cellular (Cellular Version Only)5	57
3.4.1.4 Loopback6	50
3.4.1.5 VLAN Trunk	j1
3.4.2 Firewall	51
3.4.2.1 Security6	j2
3.4.2.2 ACL	j2
3.4.2.4 Port Mapping (DNAT)6	j4
3.4.2.3 DMZ	55
3.4.2.5 MAC Binding	55
3.4.3 DHCP	56
3.4.4 DDNS	57
3.4.5 Link Failover6	58
3.4.5.1 SLA6	58
3.4.5.2 Track	58
3.4.5.3 WAN Failover	70
3.4.6 VPN	70
3.4.6.1 DMVPN7	/1
3.4.6.2 IPSec7	/2
3.4.6.3 GRE	75
3.4.6.4 L2TP	76
3.4.6.5 PPTP	78
3.4.6.6 OpenVPN Client	30
3.4.6.7 OpenVPN Server	32
3.4.6.8 Certifications8	35
3.5 System	36
3.5.1 General Settings	36
3.5.1.1 General	36
3.5.1.2 System Time	38
3.5.1.3 SMTP	38
3.5.1.4 Phone	39
3.5.1.5 Email	90
3.5.2 User Management9	90
3.5.2.1 Account) 1
3.5.2.2 User Management9) 1
3.5.3 SNMP	
3.5.3.1 SNMP9	92
3.5.3.2 MIB View) 3
3.5.3.3 VACM9	93
3.5.3.4 Trap9) 4
3.5.3.5 MIB	
3.5.4 Device Management9	
3.5.4.1 Auto Provision9	
3.5.4.2 Management Platform9	
3.5.5 Events	

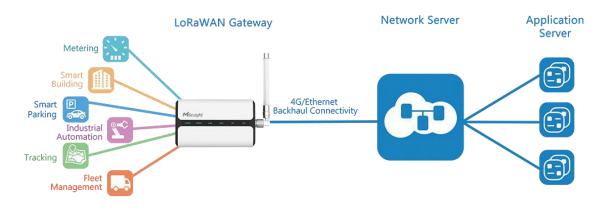
3.5.5.1 Events	97
3.5.5.2 Events Settings	
3.6 Maintenance	
3.6.1 Tools	99
3.6.1.1 Ping	
3.6.1.2 Traceroute	
3.6.1.3 Qxdmlog	100
3.6.2 Schedule	100
3.6.3 Log	101
3.6.3.1 System Log	101
3.6.3.2 Log Settings	101
3.6.4 Upgrade	
3.6.5 Backup and Restore	
3.6.6 Reboot	104
3.7 APP	105
3.7.1 Python	105
3.7.1.1 Python	105
3.7.1.2 App Manager Configuration	106
3.7.1.3 Python App	106
3.7.2 Node-RED	107
3.7.2.1 Node-RED	
Chapter 4 Application Examples	110
4.1 Restore Factory Defaults	110
4.2 Firmware Upgrade	111
4.3 Ethernet Connection	111
4.4 Cellular Connection (Cellular Version Only)	112
4.5 Wi-Fi Application Example	114
4.5.1 AP Mode	114
4.5.2 Client Mode	115
4.6 Packet Forwarder Configuration	117
4.7 Connect to Milesight IoT Cloud	118
4.8 Application Configuration	120
4.9 Device Configuration	123
4.10 Send Data to Device	124
4.11 Node-RED	126
4.11.1 Start the Node-RED	126
4.11.2 Send Data by Email	127

Chapter 1 Product Introduction

1.1 Overview

UG65 is a robust 8-channel indoor LoRaWAN[®] gateway. Adopting SX1302 LoRa chip and high-performance quad-core CPU, UG65 supports connection with more than 2000 nodes. UG65 has line of sight up to 15 km and can cover about 2 km in urbanized environment, which is ideally suited to smart office, smart building and many other indoor applications.

UG65 supports not only multiple back-haul backups with Ethernet, Wi-Fi and cellular, but also has integrated mainstream network servers (such as 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(s) or HTTP(s) protocol for data transmission to application server
- Rugged enclosure, optimized for wall or pole mounting
- 3-year warranty included

Security & Reliability

- Automated failover/failback between Ethernet and Cellular
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN
- Embedded hardware watchdog to automatically recover from various failure and ensure highest level of availability

Easy Maintenance

- Milesight DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and various upgrading options help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve quick configuration and simple management among a large quantity of devices
- Users can efficiently manage the remote devices on the existing platform through the industrial standard SNMP

Capabilities

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial quad core 64-bit ARM Cortex-A53 processor, high-performance operating up to 1.5 GHz with low power consumption, and 8GB eMMC available to support more applications
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

Hardware System	
CPU	Quad-core 1.5GHz, 64-bit ARM Cortex-A53
Memory	8 GB eMMC Flash, 512 MB DDR4 RAM
LoRaWAN	
A .	Fully Integrated and Internal Antenna
Antenna	(Optional: $1 \times 50 \Omega$ N-Female External Connector)
Channel	8
Frequency Band	CN470/IN865/EU868/RU864/US915/AU915/KR920/AS923-1&2&3&
	4
Sensitivity	-140dBm Sensitivity @292bps
Output Power	27dBm Max
Protocol	V1.0 Class A/Class B/Class C and V1.0.2 Class A/Class B/Class C
Ethernet	
Ports	1 × RJ-45 (PoE PD supported)
Physical Layer	10/100/1000 Base-T (IEEE 802.3)

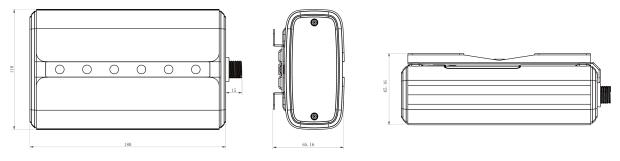
1.3 Specifications

Milesight

Data Rate	10/100/1000 Mbps (auto-sensing)
Interface	Auto MDI/MDIX
Mode	Full or half duplex (auto-sensing)
Wi-Fi Interfaces	
Antenna	Fully Integrated and Internal Antenna
Standards	IEEE 802.11 b/g/n, 2.4 GHz
	802.11b: 18 dBm +/-2.0 dBm (11 Mbps)
	802.11g: 15 dBm +/-2.0 dBm (6 Mbps)
	802.11g: 15 dBm +/-2.0 dBm (54 Mbps)
Tx Power	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS0_HT20)
	802.11n@2.4 GHz: 14 dBm +/-2.0 dBm (MCS7_HT20)
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS0_HT40)
	802.11n@2.4 GHz: 13 dBm +/-2.0 dBm (MCS7_HT40)
Cellular Interfaces	(Optional)
Antenna	Internal Antenna
SIM Slots	1
Software	
Network	PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, DDNS, HTTP, HTTPS,
Protocols	DNS, SNTP, Telnet, SSH, MQTT, MQTTS, BACnet/IP etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Firewall	ACL/DMZ/Port Mapping/MAC Binding
Management	Web, CLI, SMS, On-demand dial up, DeviceHub, Milesight IoT Cloud,
Management	Yeastar Workplace Platform, Milesight Development Platform
Арр	Python SDK, Node-RED
Power Supply and	Consumption
Damar Ormalia	1. DC Jack Connector for 9-24 VDC power supply
Power Supply	2. 1 × 802.3 af PoE input
Consumption	Typical 2.9W, Max 4.2W
Physical Character	istics
Ingress Protection	IP65
Dimensions	180 x 110 x 56.5 mm
Mounting	Desktop, Wall or Pole Mounting
Others	
Reset Button	1 × RST

LED Indicators	1 × POWER, 1 × STATUS, 1 × LoRa, 1 × Wi-Fi, 1 × LTE, 1 × ETH	
Built-in	Watchdog, RTC, Timer	
Environmental		
Operating	-40°C to +70°C (-40°F to +158°F)	
Temperature	Reduced cellular performance above 60°C	
Storage Temperature	-40°C to +85°C (-40°F to +185°F)	
Ethernet Isolation	1.5 kV RMS	
Relative Humidity	0% to 95% (non-condensing) at 25°C/77°F	

1.4 Dimensions (mm)



Chapter 2 Access to Web GUI

This chapter explains how to access to Web GUI of the UG65. Username: **admin** Password: **password**

2.1 Wireless Access

Milesight

Λ

1. Enable Wireless Network Connection on your computer and search for access point **Gateway_******* to connect it, the default Wi-Fi password is **iotpassword**.

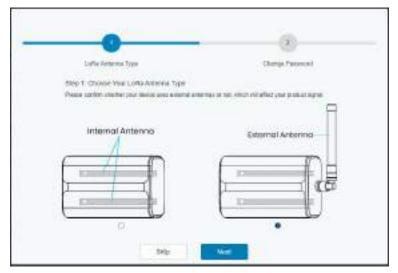
2. Open a Web browser on your PC (Chrome is recommended) and type in the IP address **192.168.1.1** to access the web GUI.

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

		frame (section)
and the second second	Milesight	
	0.	

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

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



12

Milesight				1.mm (3)
	Serie Islan	Name ALAN UPA Head		But .
Partiel Folgenitie	System Information			The balance and
Terrate Server	Heater .	IN THE ADDRESS OF A		Report Street for September of patients
Prese literature	Pages Annu Pages	to and the		Bend Hander Handrand and and a
-	Printed Street	weinen. mi		Firmup a Western
-	Land Term	(All \$1,47) (7) (8) (8) (8) (8) (8) (8) (8) (8) (8) (8		An and a parameter of the later.
and state	CROSSE	19 (20 30) 204		Local Real
ATT	MMI Capacity Research	A COMPANY OF A COM		Distriction of the second seco
	1074			These free internation of these and the particular factors:
	Heater .			CRULING
	targe for the state			How The large Distance Of the patients
	Preparate Second		Wend School & Connect	Ball Coperty doubling

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

2.2 Wired Access

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

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

$ ightarrow \star \star \star$	and Internet > Network and Sharing Center	✓ ひ Search Control Panel
Control Panel Home	View your basic network inform	ation and set up connections
Change adapter settings Change advanced sharing settings	View your active networks Yeastar5G Private network	Access type: Internet HomeGroup: Ready to create Connections: all Wi-Fi (Yeastar5G)
	ldentifying	Access type: No network access Connections: Up <u>Ethernet</u>
	Change your networking settings Set up a new connection or netw Set up a broadband, dial-up, or Troubleshoot problems Diagnose and repair network pro	EINPINEL
See also HomeGroup Infrared Internet Options Windows Firewall		

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

Internet Protocol Version # (RCP/Pr	4 Prepaties	×
Concret		
Not the pet ${\mathbb R}$ sectory any we will the capability. Otherway, you need for the appropriate ${\mathbb P}$ so from		
O gbiair an P address as innats	ally	
B up for falloung Plada east		
¥ akbosi	182 . 162 . 23 . 200	
Sgnetmeek	285 - 285 - 255 - 0	
Geging Breecold	182.388.22 188	
ing the tires, see you address and	anaticity.	
· · · · · · · · · · · · · · · · · · ·	ddrwesses:	
Environment (DNE conversion	$I \rightarrow I \rightarrow R \rightarrow R$	
gitametrie DIG servers		
🖂 freigheiter verföttigt uppart er ell	Adjusted	
	Car Car	-

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

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

Δ

	Construction of the local data
AMERICA	
Milesight	
8	- 10 C
	1.00

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

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

	9
Loffer Anternon Type	Change, Passecol
555 T. Chouse You Lotta Antonia Type Presa carlier chatter por liaist and anama antenna	n na mar na dha na pala na n
internal Antenno	Edomal Antenna
<u> </u>	<u> </u>

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

Milesight				1.mm 🖯 🖯
	Series Inter-	Innon. MAN 1991 Hottle		And And
Partici Patronia	Spalars Information			The Party States
Names 2014	-	IN THE ADDRESS OF A		Report Story for Support of patients
Preset the star	Pages Annual Annual	ALC: NAME AND		Bend Nander Steel Parister of Anthony
-	Internet Autom	weather .		Fit through it was played.
	institut.	(Algorith 2) (2) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4		an Bill of parson Restaurie visions Transformers for balance
-	e Gio sait	Ma		united of particular Linear Procession and and
ATT.	• MMC Capacity Second	A COMPACT AND A		Des .
).ms			These the conception of these straighter galaxies functions unception
	Manual Victoria			CRULING
	Tana Tanan			Here The last \$1000 all and - of the patients
	Preparate Second		Mercel Bellinet: 4 California	RAW Capacity Sciences

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

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

UG65-L00E-868M-EA
EU868
6221A4968194
60.0.0.42-r5
V1.1
2024-02-21 21 49 38 Wednesday
01:29:39
5%
512MB/47MB (9.18%)
8.0GB/6.4GB (80.32%)

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.		
	Table 2.1.1.1 System Information		

Table 3-1-1-1 System Information

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	34
Serial Number	
Firmware Version	-
Hardware Version	33
Power Status	Unconnected
Remaining Battery	1.

Figure 3-1-1-2

3.1.2 Cellular

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

Modem		
Status	Ready	
Modei	EC25	
Version	EC25ECGAR06A07M1G	
Signal Level	26asu (-61dBm)	
Register Status	Registered (Home network)	
IMEI	860425047368939	
IMSI	460019425301842	
ICCID	89860117838009934120	
ISP	CHN-UNICOM	
Network Type	LTE	
PLMN ID		
LAC	5922	
Cell ID	340dh80	

Figure 3-1-2-1

Modem Information			
Item	Description		
Status	Show corresponding detection status of module and SIM card.		
Model	Show the model name of cellular module.		
Version	Show the version of cellular module.		
Signal Level	Show the cellular signal level.		
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	



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.

Milesight

Oveniev	0	eilular	Network	WLAN	VPN Host List		
WAN							
Port	Status	Туре	IP Address	Netmask	Gateway	DNS	Duration
ath D	up.	Static	192 16B 22 32	255 255 254 0	152 158.22 1	55.5.5	10h 52m 03s



Network				
ltem	Description			
Port	Show the name of the Ethernet port.			
	Show the status of the Ethernet port. "Up" refers to a status that WAN			
Status	is enabled and Ethernet cable is connected. "Down" means Ethernet			
	cable is disconnected or WAN function is disabled.			
Туре	Show the dial-up type of the Ethernet port.			
IP Address	Show the IP address of the Ethernet port.			
Netmask	Show the netmask of the Ethernet port.			
Gateway	Show the gateway of the Ethernet port.			
DNS	Show the DNS of the Ethernet port.			
	Show the information about how long the Ethernet cable has been			
Duration	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	1	24:e1:24:f1:22:58			
Interface Type	3	4P			
SSID	10	3ateway_F12258			
Channel	1	Auto			
Encryption Type	1	Ne Encryption			
Status	1	Up			
IP Address	9	192.168.1.1			
Netmask	1	255 255 255.0			
Connection Duratio	n i) days, 10:52:23			

Figure 3-1-4-1

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

Table 3-1-4-1 WLAN Status

```
Associated Stations
```

IP Address

MAC Address

Connection Duration

Figure 3-1-4-2

Associated Stations				
ltem	Description			
IP Address	Show the IP address of access 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	Celular	Network	WLAN VPN	HestUst
PP1P Tunnel				
	Name	Stature	Local IP	Rameta IP
	pp/p_1	Disconnected	13	
	pptp_2	Documents and	14	
	pptp_3	Damanaciad	13	1
L2TP Tunnel				
	Name	Status	Local IP	Remote IP
	Dp_1	Disconnected	1.54	-
	Dtp_2	Datemedad	3	
	Etp_3	Disconnactad	5 4 .5	

Figure 3-1-5-1

Name	Status	Local IP	Renota IP
ipsec_1	Disconnected	85	3
ipsec_2	Disconnected	9	-
(psec_)	Disconnected	17	10

1.6	2.5	242	-	1.64	100	242
10	-pei	nγ	۳ħ	1.0	80	. 2n

Name	Stature	Local IP	Remote IP
ubewitu_1	Deconnected	12	S.
openvpn_2	Disconnected		
openvpn_3	Disconnected	52	22

Figure 3-1-5-2

Milesight

GRE Tunnel				
	Name	Status	Local IP	Remote IP
	gre_1	Discovercied	Sİ	2
	gre_2	Disconnected	54	2
	gre_3	Disconnoied	12	ž
DMVPN Tur	neł			
	Name	Status	Local IP	Remote IP
	davpn	Disconnected	02	8

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.

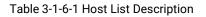
Overview	Cellular	Network	WLAN	VPN	HottList
DHCP Leases					
	IP		MAC		Lease Remaining Time
MAC Binding					
	1				MAC

Figure 3-1-6-1

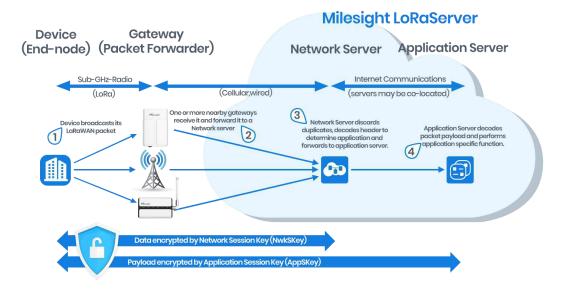
Host List	
ltem	Description
DHCP Leases	
IP Address	Show IP address of DHCP client
MAC Address	Show MAC address of DHCP client
Lease Time Remaining	Show the remaining lease time of DHCP client.
MAC Binding	
IP & MAC	Show the IP address and MAC address set in the Static IP

22

list of DHCP service.



3.2 LoRaWAN



3.2.1 Packet Forwarder

3.2.1.1 General

General	Hades	Advanced	Custon	Tuñc		
General Setting	0					
Gateway EI/II	24E184	FFFEF36F39				
Gatoway (D	24E %	MERFER MERON				
Frequency-Senc	Died					
Data Hutxeen exis						
Multi Destinatio	•2					
o	61	nable	Type	Server Address	Connect Status	Operation
0	. Et	bete	Embedded NS	localitest	Disconnected	
						83

Figure 3-2-1-1

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

23

	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 of up to 1 million pieces of data when the 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 the package forwarder.

Table 3-2-1-1 General Setting Parameters

Packet Filters			
Filters by NetID default mode	White List []		
Proprietary Message Filter	2		
Filters by NetID	White List	~	
Filters by JoinEUI	Black List	~	
		To	.
Filters by DevEUI	White List	~	
		Te	

Figure 3-2-1-2

Packet Filters			
Parameters	Description		
Filters by NetID Default Mode	 Select the filter mode as black list or white list. White List: Only forward the packets on this list to the network server. Black List: Only forward the packets except this list to the network server. 		
Proprietary Message Filter	This only works when the packet forwarder type is Milesight Development Platform LNS or DeviceHub LNS.		
Filters by NetID Filters by JoinEUI	Forward/Not forward the uplink packets that match the NetID. Forward/Not forward the join request packets that match the		

	JoinEUI range.
Filters by DevEUI	Forward/Not forward the join request packets that match the DevEUI range.
List	Set the specific filtering value or range list. Every condition supports to add 5 lists at most.

Table 3-2-1-2 Packet Filters Parameters

Note:

1. When join EUI and dev EUI are both configured, only packets that match both conditions will be forwarded.

2. This feature is not supported when the packet forwarder type is Loriot or Everynet.

3. When a third-party network server assigns filter condition to gateway, the gateway will use network server settings in priority.

Related Configuration Example

Packet forwarder configuration

3.2.1.2 Radios



Figure 3-2-1-3

legion	US915	* Noise Analyzer +
Name		Center FrequencyMHz
Radio II		904.3
Radio 1		905.1

Figure 3-2-1-4

Radios-Radio Channel Setting

ltem	Description
Antenna Type	Select the transmission type of antennas when using EA version.
Region	Choose the LoRaWAN [®] frequency plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.
Center Frequency	Change the frequencies to receive packets from LoRaWAN® nodes.

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

Multi Chancels Setting

- Enable	tedas	Hadio	Fisquery With
×.	F	Redo 0. T	103.2
*	1	Rado 0 •	823.4
*	40 -	Rado 0 *	825.0
*	2	Robit +	8222
*	¥7	Rado I +	922 A
*	52	Rudic 1 +	82.0
*		Rado I +	102.8
	¥.)	Rado F +	453.0

Figure 3-2-1-5

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

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

Channel Balling				
tratile	Refin	Financy Wit	Davind 85/854	Sprood Texture
	Balls E .	101.8	258032 +	587 -

Figure 3-2-1-6

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

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

Enable Radia Forquerry/Mitz Bandwith/Hit	DesiRes

Figure	3-2-1-7
riguie	5217

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

Table 3-2-1-6 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.

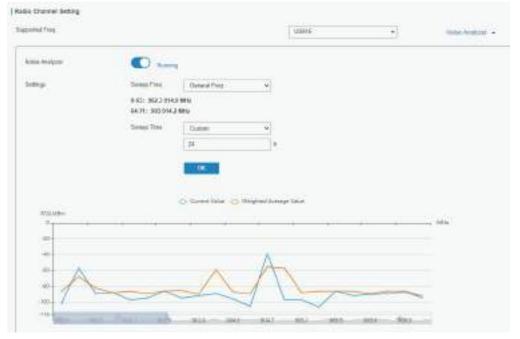


Figure 3-2-1-8

Noise Analyzer			
Item	Description	Default	
Enable	Click to enable noise analyzer feature.	Disabled	
Sweep Freq	Select the frequency sweeping range.	General Feq	

	General Freq: frequencies based on the LoRaWAN [®] regional parameters document Custom: custom the frequency range	
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 3-2-1-7 Noise Analyzer Setting Parameters

3.2.1.4 Advanced

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

Beacon Setting			
Beacon Period	128	×	s
Beacon Freq	869525000		Hz
Beacon Datarate	SF9	×	
Beacon Channel Number	1	*	
Beacon Freq Step	200000		Hz
Beacon Bandwidth	125000	~	Hz
Beacon TX Power	16		dBm
Beacon Time Offset	0		s

Figure 3-2-1-9

Advanced-Beacon Setting			
ltem	Description	Default	
Beacon Period	Interval of gateway sending beacons for Class B device time synchronization. 0 means the gateway will not send beacons.	0	
Beacon Freq	The frequency of beacons.	Based on the supported frequency	
Beacon Datarate	The datarate of beacons.	Based on the supported frequency	
Beacon Channel Number	When selecting Custom, it allows users to custom range from 1 to 8.	1	

Beacon Freq Step	Frequency interval of beacons.	200000
Beacon Bandwidth	The bandwidth of beacons. Unit: Hz	12500 Hz
Beacon TX Power	The TX power of beacons.	Based on the supported frequency
Beacon Time Offset	Add this offset to system time and assign the time result to class B devices. This can avoid the interference when multiple class B devices are close.	0

Table 3-2-1-8 Advanced-Beacon Parameters

Intervals Setting		
Keep Alive Interval	10	s
Stat Interval	30	5
Push Timeout	100	ms
Forward CRC Setting		
Forward CRC Disabled		
Forward CRC Error		
Forward CRC Valid	2	

Figure 3-2-1-10

ltem	Description	Default
Keep Alive Interval	Enter the interval of keepalive packet which is sent from gateway to network server to keep the connection stable and alive. Range: 1-3600.	10
Stat Interval	Enter the interval to update the network server with gateway statistics. Range: 1-3600.	30
Push Timeout	Enter the timeout to wait for the response from server after the gateway sends data of node. Rang: 1-1999.	100
Forward CRC Disabled	Enable to send packets received with CRC disabled to the network server.	Disabled
Forward CRC Error	Enable to send packets received with CRC errors to the network server.	Disabled
Forward CRC Valid	Enable to send packets received with CRC valid to the network server.	Enabled

Table 3-2-1-9 Advanced Parameters

3.2.1.5 Custom

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

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

General	Radios	Advanced	Custom	Traffic	
Custom Confi	guration				
Enable					
				Example	
"lorawan_publ "ciksrc" 0,	"/dev/spidev0.0", itc" true. "TTXIRX", faise. estamp". (ks" 255. 1	i, in dBi ″/			

Figure 3-2-1-11

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**.

artic betting								
(Filmer	Cher							
-	(byrika)	Dec	Tella	Irepany .	Intern	Lotions	16.9	SIR
. +	19		101576	101.0	avanetts.	45	340	+122
			11000.66	2014	APARTON	24	302	163
7	17		Happen	80.8	(material)	15	140	- 44
- 10	14		31712(0000)	82.6	SCHWESS.	-	-40	48.4
11			11073484	40.0	STREET.	40	-82	11.1
1.0	14		DOTADA.	80.4	9700402	- 10	- 101	422
1.1	- 10		114710 1440	82.4	5638mt5	- 85	1912	- 0.0
	-		11.01080110	82.1	arrente.	10	102	112
132	19		1100022746	102.8	seatures.	(99)	240	322
. 4	u		313406798	82.9	5/10/HUE	45	-960-	-41.8

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

Figure 3-2-1-12

Table 3-2-1-10 Traffic Parameters

3.2.2 Network Server

3.2.2.1 General

Enable	2		
Platform Mode			
NetID	010203		
Join Delay	5		sec
RX1 Delay	1		sec
Lease Time	8760-0-0		hh-mm-s
Log Lavel	info	~]
Global Channel Plar	1 Setting		
Channel Plan	US915	v	
Channel	8-15		1

Figure 3-2-2-1

ltem	Description	Default		
General Setting				
Enable	Click to enable Network Server mode.	Enabled		
Platform Mode	Enabled to connect gateway to Milesight IoT	Disabled		

Milesight

	Cloud or Yeastar Workplace platform .	
NetID	Enter the network identifier.	010203
Join Delay	Enter the interval time between when the end-device sends a Join_request_message to network server and when the end-device prepares to open RX1 to receive the Join_accept_message sent from network server.	5
RX1 Delay	Enter the interval time between when the end-device sends uplink packets and when the end-device prepares to open RX1 to receive the downlink packet.	1
Lease Time	Enter the amount of time till a successful join expires. The format is hours-minutes-seconds. If the join-type is OTAA, then the end-devices need to join the network server again when it exceeds the lease time.	876000-00-00
Log level	Choose the log level.	Info
Channel Plan Se	etting	
Channel Plan	Choose LoRaWAN [®] channel plan used for the upstream and downlink frequencies and datarates. Available channel plans depend on the gateway's model.	Depend on the gateway's frequency
Channel	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:

Ional Channels			
Fridgemecy(NIHz)	Mire Detarate	Mox Deterate	Operatio
			8

Additional Channels			
Item	Description		
Frequency/MHz	Enter the frequency of the additional plan.		
Max Datarate	Enter the max datarate for the end-device. The range is based on what is specified in the LoRaWAN [®] regional parameters document.		
Min Datarate	Enter the min datarate for the end-device. The range is based on what is specified in the LoRaWAN [®] regional parameters document.		

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 tl	he application by clicking	or create a new application by clicking 🖽.
Applications		
Nami	dotal	
Description	Opuil	
Data Transmission		
	Type.	Contation
	1999	



Application				
ltem	Description			
Name	Enter the name of the application profile.			
marrie	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,			
Data	HTTPS or BACnet/IP protocol. One application can add 3 data			
Transmission	transmissions at most and every protocol can be selected only once.			

Table 3-2-2-3 Application Parameters

MQTT Integration

Туре	MQTT	×
Status		
General		
Braker Address	-	
Broker Port		
Client ID		
Connection Timeout/s	30	
Keep Alive interval/s	60	
User Credentials		
Enable	-	
Usemame		
Password		



3			
en <u>p</u>			
di CAsgedonve ianko	dan v		
tale CAugrad server certile			
State Type	Net		
Uplicit: data		Gel\$ 8	
Devendink, data	1	Ged I	
Hulkicast downlink data		GelS II	100
Join net/fostion		Qetil II	
ACK notification		Gold II	. 4
Error nettikative		_ 1949 W _	1.0
Responding to the		Good ii	
Kespunse data		(203 #	



MQTT Settings					
Item	Description				
General	General				
Broker Address	MQTT broker address to receive data.				
Broker Port	MQTT broker port to receive data.				
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle messages at QoS 1 and 2.				

Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535.			
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 Credentials				
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.			
Mode	 Select from "Self signed certificates", "CA signed server certificate". CA signed server certificate: verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device. Self signed certificates: upload the custom CA certificates(.crt or .pem), client Certificates(.crt) and secret key(.key) for verification. 			
Торіс				
Data Type	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 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	QoS 0 - Only Once This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode. QoS 1 - At Least Once This level guarantees that the message will be delivered at least once, but may be delivered more than once. QoS 2 - Exactly Once QoS 2 is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS 2 is			
	the safest and slowest quality of service level.			

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				
	Reader Name	fleader Value	Operation	
URL			8	
	Data Type	URL		
	Uplink data]	
	Join notification			
	ACK notification]	
	Error notification			

Figure 3-2-2-6

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

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

Related Configuration Example

Application configuration

3.2.2.3 Payload Codec

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

overy Verbion	1.0.0			
blaining Type	Onine	¥		
Ottain At Crosse that the Internet ago	ees to available :			
Nime		Paytnad decoder function	Payload ancoder function	Depili
AMIST & AV103	i.	¥	~	0
AW104		~	~	0
AM102		~	4	0
AW/207		~	*	0
AW308		~	~	0
AM319-HOHO		4	~	0
AND19-HCHO-I	R.	×	×	0
AM219-03		V	×	0
EM308-TH		¥	~	0
W5494		~	v	.0

Figure 3-2-2-7

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

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

None	
Description	
Template	None
Payload docodor	
Payload decoder function	1 of Narroda residence as some of types Life as sequent. (* - Mort contains the contain Port content (* - Mort contains the contain Port content (* - Mort contains the contain Port of the sequence of the
Payload encoder Payload encoder function	(i) If include modes the given styles, interactions of types.
	<pre>() Other converses on a samada there assume () - Hy D are adjust, h g ("Anderstein", 22.5) () The Function converse on a series of system, n.g. 1220, 120, 200, 41 (setter (samada)Shire, and)) (setter (1))</pre>
Payload Codec Test	2
	1 // maps deviate the payment of anomalies into payment. // Anomalies type: // Anomalies type: // Anomalies type: // Anomalies type: // Anomalies type:



Custom Payload C	odec
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

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. UG65 has pre-configured 8 device files and users can also create a new device profile.

Denesis	Applications Poyless	Collec Polities	Device Multicost Orcas	pe Oservey Pool	Packetts
Onice Profile	e:				
	Name -	Nas TXPeum	Just Type	Class Type	Gaesalius
	Cimil-APP		107	Date A	51 CS
	tianA-056A		idiaa	-Data A	55
	Const-489		320	Films & Cites W	52 (23
	Chanalicology	*	0144	TIME & DATE (1	68
	ChanG-ABP		459	Chever, A. Course Cl.	6883
	Classific PURA		alan	Cherry P. Cherry C.	50
	Class(2)-ADF		ARP	Cierc A Cierc D Chare C	6283
	Ciev(5-076A		0556	Class A Date & Class E	12 43
					0



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



Device Profiles	s Settings
ltem	Description
Name	Enter the name of the device profile.
	Enter the maximum transmit power.
Max	The TXPower indicates power levels relative to the Max EIRP level of
TXPower	the end-device. 0 means using the max EIRP. EIRP refers to the
	Equivalent Isotropically Radiated Power.
Join Type	Select from: "OTAA" and "ABP".
	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

Milesight

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

Figure	3-2-2-11

Device Profile A	dvanced 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	The offset which used for calculating the RX1	Based on what
Offset	data-rate, based on the uplink data-rate.	is specified in
RX2 Datarate	Enter the RX2 datarate which used for the RX2 receive-window.	the LoRaWAN [®] regional
RX2 Channel	RX2 channel frequency which used for the RX2	parameters
Frequency	receive-window.	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.	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

С.		
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.

ARE Discount	Danker HE				Dist-10	
Device Harse	Derita D.R	Desite Proble	Application	Last See	Activent	Openetio
2051242100000483	2061240108032603	und	the	TT BAYS AND	~	50
1401244/1445P1021	3421344164301911	Of 64-calent	thad	25 days ige	4	20
#152-bad	2161612288821375	Cand O'RA	and	AD daywage	14	1213

Figure	3-2-2-12
riguic	02212

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

Table 3-2-2-10 Device Parameters

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



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

	Range: 2-84, 86-223. Note: this value must be the same as the Milesight LoRaWAN [®] controller's fPort.
TCP Port	Enter the TCP port for data transmission between the TCP Client and UG65 (as TCP Server).Range: 1-65535.
Frame-Counter Validation	If disable the frame-counter validation, it will compromise security as it enables people to perform replay-attacks.
Application Key	Whenever an end-device joins a network via over-the-air activation, the application key is used for derive the Application Session key.
Device Address	The device address identifies the end-device within the current network.
Network Session Key	The network session key specific for the end-device. It is used by the end-device to calculate the MIC or part of the MIC (message integrity code) of all uplink data messages to ensure data integrity.
Application Session Key	The AppSKey is an application session key specific for the end-device. It is used by both the application server and the end-device to encrypt and decrypt the payload field of application-specific data messages.
Uplink Frame-counter	The number of data frames which sent uplink to the network server. It will be incremented by the end-device and received by the end-device. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.
Downlink Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server. Users can reset the a personalized end-device manually, then the frame counters on the end-device and the frame counters on the network server for that end-device will be reset to 0.

Table 3-2-2-11 Device Setting Parameters

Related Configuration Example

Device configuration

3.2.2.6 Multicast Groups

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

Multicast Groups				
AM			Stath.	0
Multicest Address	Group Nove	Humber of Devices	Open	ilion
	No wratching miss	orde Second		

Figure 3-2-2-14

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

Table 3-2-2-12 Multicast Group Parameters

Multicast Address	
Multicast Network Session Key	
Multicast Application Session Kay	
Сіаза Туре	Class C 🗸 🗸
Datarate	DR8(SF12,500KHz) v
Frequency	923300000
Frame-counter	0
Selected Devices	
Add Device	

Figure 3-2-2-15

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

Class Type	Class B and Class C are optional.
Datarate	Datarate of the node receiving downlinks.
Frequency	Downlink frequency of all devices in this group.
Frame-counter	The number of data frames which received by the end-device downlink from the network server. It will be incremented by the network server.
Ping Slot Periodicity	Period of opening the pingslot. This is only applied to Class B end devices.
Selected Devices	Show all device names in this group.
Add Device	Add devices in the pull-down list.

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

3.2.2.7 Gateway Fleet

Milesight gateways can connect to UG65 network server. A gateway supports to add 100 gateways at most.

Gaterstay (II	Natar	Status	Last Seer	Operative
34E-01#177EP-0263	Local Getwywy	Darreded	2021-04-10 (0:12:21	
				-

Figure 3-2-2-16

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

Table 3-2-2-14 Gateway Fleet Parameters

	1
Name	
Location	
GPS into will be displa	ayed by default or can be changed manually
	ayed by default or can be changed manually Eg.0.026811
GPS into will be displ Latitude Longitude	

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 data it will replace your customized data.

Table 3-2-2-15 Gateway Setting Parameters

3.2.2.8 Packets

Device EUI		Type	Peytoall	Post	Confirmed	
03600336003560035	A	acıı 👻		05	D	Sin
é Data to Multicast C	broup					
Multicast Group		Type	Payload	Port.		
	• A	sca 🗸		85		500
tork Server						
tork Server				Search		

Figure 3-2-2-18

Send Data To	Device/Multicast Group
ltem	Description
Device EUI	Enter the EUI of the device to receive the payload.
Multicast Group	Select the multicast group to send downlinks. Multicast groups can be added under Multicast Groups tab.
Туре	Choose 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.
	Show the type of the packet:
	JnAcc - Join Accept Packet
	JnReq - Join Request Packet
	UpUnc - Uplink Unconfirmed Packet
Туре	UpCnf - Uplink Confirmed Packet - ACK response from
	network requested
	DnUnc - Downlink Unconfirmed Packet
	DnCnf - Downlink Confirmed Packet- ACK response from
	end-device requested
Time	Show the time of packet was sent or received.
	Table 2.2.2.17 Desket Decemeters

Table 3-2-2-17 Packet Parameters

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

P	acket Details		-
1.0		1	
	Dec Add: Multicant Addr	96148591	1
	GwELI	24E124FFFEF0E225	
	AppEUI	24E124C0002A0001	
	Device ELUGroup Name	24E1241266210668	
	Class. Type	Class C	
	Interaclately		
	Timestamp	2721022973	
	Type	UpUnc	- 1
	Adı	inise	
	AdvAcKiReq	talse	
	Ack	talse	
	First	969	
	Part	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	Chow the FUIL of the device (multicent group name
Name	Show the EUI of the device/multicast group name.
Class Type	Show the class type of the device or multicast group.

Immediately	True: Device may transmit an explicit (possibly empty) acknowledgement data message immediately after the reception of a data message requiring a confirmation.
Timestamp	Show the timestamp of this packet.
	Show the type of the packet:
	JnAcc - Join Accept Packet
	JnReg - Join Request Packet
	UpUnc - Uplink Unconfirmed Packet
Туре	UpCnf - Uplink Confirmed Packet - ACK response from network
туре	requested
	DnUnc - Downlink Unconfirmed Packet
	DnCnf - Downlink Confirmed Packet- ACK response from end-device
	requested True: The end-node has enabled ADR.
Adr	
	False: The end-node has not enabled ADR.
	In order to validate that the network is receiving the uplink messages,
	nodes periodically transmit ADRACKReq message. This is 1 bit long.
AdrAcKReq	True: Network should respond in ADR_ACK_DELAY time to confirm that
	it is receiving the uplink messages.
	False: ADR is disabled or Network does not respond in
	ADR_ACK_DELAY.
Ack	True: This frame is ACK.
	False: This frame is not ACK.
F 4	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.
MIC	Show the MIC of this packet. MIC is a cryptographic message integrity
	code, computed over the fields MHDR, FHDR, FPort and the encrypted

FRMPayload.

Table 3-2-2-18 Packets Details Parameters

Related Topic

Send Data to Device

3.3 Protocol Integration

3.3.1 BACnet Server

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

3.3.1.1 Server

Enable		
JDP Port	47808	i.
Device ID	40185	ĺ.
Jevice Name	UG67-6222B4620088	
BMD	2	
P Address		
P Port	47808	

Figure 3-3-1-1

Server Settings	
Item	Description
Enable	Enable or disable BACnet server function.
UDP Port	Set communication port of BACnet/IP. Range: 1-65535.
	The default port is 47808.
Device ID	The unique BACnet device identifier which needs to avoid conflict
Defice ib	with other devices.
Device Name	The device name to represent the device.
BBMD	Enable BBMD(BACnet/IP Broadcast Management Device) if
DDIVID	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	Dub ingent	Hell Days	et. Deter Al	14			(Sept		.0
	bject Name	Object Type	Object Instance Nr	Present Value	Units	Updates	Update tree	COV	Operation
248 (2459)	16302496 tullor_	Anatogrinput	a	15/73822740000.0	no- units	339	2022-12-13 08:52.06	Deatiled	

Figure 3-3-1-2

ltem	Description	
Add	Add a BACnet object. The gateway supports adding 2000	
Auu	objects at most.	
Bulk Import	Download template and import multiple BACnet objects.	
Bulk Export	Export all generated BACnet object settings.	
Delete All	Delete all objects in the list.	
Object Name	Show the name of the BACnet object.	
Object Type	Show the type of this object.	
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	AM308	•
LoRa Object	temperature	•
Object Name	AM308 temperature	
Object Type	Analog-Input	~
The Object Instance	0	
Units	*C(62)	•
Description		Ĩ
COV		

Figure 3-3-1-3

BACnet Object Co	onfiguration
ltem	Description

Device Name	Select the device added on Network Server > Device page.
LoRa Object	Select one of device variables as an object.
Object Name	Customize an unique name for this object.
	Select the object type as binary input/output/value, analog
Object Type	input/output/value, multistate input/output/value and
	charcterString value.
The Object	Questo mains the shirest instance
Instance	Customize the object instance.
Description	Enter the description of this object.
Analog Input/Out	put/Value
Units	Select the unit of this object value.
	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 Increment	Only when the object value reaches or over this increment, the
COV increment	BACnet server (gateway) will send the notification.
Relinquish	If there is no command, the analog output will be set as this
Default	relinquish default value.
Binary Input/Out	put/Value
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 binary output will be set as this
Default	relinquish default value.
MultiState Input/	Output/Value
Number of	Set the number of states and define the name of every state.
States	set the number of states and denne the name of every state.
Relinquish	If there is no command, the multistate output will be set as this
Default	relinquish default value.
	Table 3-3-1-3 BACnet Object Configuration Parameters

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	eth 0 🗸
onnection Type	Static IP 👻
P Address	192,168.23.150
letmask	255.255.255.0
ateway	192.168.23.1
ти	1500
rimary DNS Server	8888
econdary DNS Server	223.5.5.5
nable NAT	

Figure 3-4-1-1

Port Setting		
ltem	Description	Default
Port	The port that is fixed as eth0 port and enabled.	eth 0
Connection Type	Select from "Static IP", "DHCP Client" and "PPPoE".	Static IP
MTU	Set the maximum transmission unit.	1500
Primary DNS Server	Set the primary DNS.	8.8.8.8
Secondary DNS Server	Set the secondary DNS.	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	ethid 👻		
Gamercion Tape	Thefic IP (
P stations	502 168 25 166		
Antoniesk.	200.205.206.0		
Jalenay-	992 100 20 t		
imu	1500		
Printing (DMS Server	8810		
Secondary DNS Server	223.5.5.5		
Erustine NAT	0		
Address P Address			
	Address	Netrosak	Operatio

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	2
Connection Type	DHCP Client	
MTU	1500	
Use Peer DNS		
Primary DNS Server	8,8,8,8	
Secondary DNS Server	223555	

Figure 3-4-1-3

DHCP Client	
ltem	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.

Enable NAT	2 63 11	
Secondary DNS Server	223.5.5.5	
Primary DNS Server	8.8.8.8	
Use Peer DNS	D.	
NTU	1500	
Max Retries	0	
Link Detection Interval(s)	60	
Fasaword		
Usemame		
Connection Type	PPPpE	
Port	oth 0)

Figure 3-4-1-4

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

Table 3-4-1-4 PPOE Parameters

3.4.1.2 WLAN

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

54

Port	WLAN	Cellular Loo	pbáck
WLAN			
Enable			
Work Mode		AP	~
SSID Broad	kcast		
AP Isolation	ų.		
Radio Type		8(2.11n(2.4GHz)	×
Chantel		Auto	÷
SSID			
BSSID			
Encryption	Made	No Encryption	~
Bandwidth		20f/Hz	~
Max Client	Number	10	
IP Setting			
Protocol		Static IP	~
IP Address			
		DHCP Settings	
Netmask			

Figure 3-4-1-5

Enable		
Work Mode	Cliest	- Stan
SSID		
BSBID		
Encryption Mode	WPA-PSK/WPA2-PSK	~
Cipher	Auto	
Key		
IP Setting		
Protocol	Static IP	•
iP Address	1	1
Netmask.	255 255 255 0	1
Gateway	The second	

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".
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID
0330	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
Encryption Mode	Open System" , "WEP Shared Key", "WPA-PSK", "WPA2-PSK" ,
Eneryption mode	"WPA-PSK/WPA2-PSK", "WPA-Enterprise", "WPA2-Enterprise" and
	"WPA-Enterprise/WPA2-Enterprise".
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
Кеу	Fill the pre-shared key of WEP/WPA encryption.
XSupplicant Type	Select from "Peap", "Leap", "TLS" and "TTLS".
User	Fill the user of WPA/WPA2-Enterprise.
Anonymous Identity	Fill the anonymous identity of WPA/WPA2-Enterprise.
Phase2	Fill the phase2 of WPA/WPA2-Enterprise.
Public Server	The public server certificate used for verifying with
Certificate	WPA/WPA2-Enterprise access point.
AP Mode	
	When SSID broadcast is disabled, other wireless devices can't not
SSID Broadcast	find the SSID, and users have to enter the SSID manually to
	access to the wireless network.
AP Isolation	When AP isolation is enabled, all users which access to the AP
	are isolated without communication with each other.
Radio Type	Select Radio type. The options are "802.11b (2.4 GHz)", "802.11g (2.4 GHz)", "802.11n (2.4 GHz)"".
Channel	Select wireless channel. The options are "Auto", "1", "2""11".
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK" and "WPA-PSK/WPA2-PSK".
Cipher	Select cipher. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
Кеу	Fill the pre-shared key of WPA encryption. The default password is iotpassword .
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
Bandwidth Max Client Number	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 maximum number of client to access when the gateway
Max Client Number	Set the maximum number of client to access when the gateway
Max Client Number IP Setting	Set the maximum number of client to access when the gateway is configured as AP.

Gateway Set the gateway in wireless network.							
			Table 3-4	4-1-5 WLAN Para	imeters		
WELAN	Other						
sab	Chennel	Signal	Cipher	RSSID	Security	Frequency	
mace_008002	Auto -	94dEte	3400	24.41.24.08.46402	No Encryption	2463872	Autoration State
igh_limi	Adm	a distance in the second s	AES	ac20 as 99.5 co4	WRAPSKWPA2PSK	24578Hz	Alter-
		VILAN Dallake SND Channel mare 200002 Ada	VILAN Cullular Lo SVID Channel Signal max_00000 Auto O460m	VILAN Collular Looptack	Table 3-4-1-5 WLAN Para	Table 3-4-1-5 WLAN Parameters VILAN Colspan="3">Colspan="3">Secondary SND Channel Signal Cipter Bissio Secondary SND Channel Signal Cipter Bissio Secondary max_1000002 Ada Hether Ada 24xe12400486022 No Encrypter	Table 3-4-1-5 WLAN Parameters Table 3-4-1-5 WLAN Parameters VIE.AN Collade Loopteck SND Chennel Signal Optow MSSSD Secontry Programmy next_100002 Ads Adds 24 al 24 05 66:02 No Strengther 246387c



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

Table 3-4-1-6 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	- a ;	
Network Type	Auto	÷
APN		
Usemame		
Password	Ī.	
Access Number		
PIN Code		
Authentication Type	None	~
Roaming	8	
Customize MTU	8	
MTU	1500	
Enable IMS		
SMS Center		



Connection Setting	O	
Enable NAT		
Restart When Dial-up failed	D	
ICMP Server	8.8.8	
Secondary ICMP Server	223.5.5.5	
ICMP Detection Max Retries	3	
ICMP Detection Timeout	5	s
ICMP Detection Interval	15	\$
SMS Settings		
SMS Mode	PDU	v



General Settings		
ltem	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.	

58

	4G Only: connect to 4G network only.
	And so on.
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.
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 MTU	Enable or disable to customize the maximum transmission units. When 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
Dial-up failed	automatically if the 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 Timeout	Set timeout of ICMP detection.
ICMP Detection Interval	Set interval of ICMP detection.
SMS Mode	Select SMS mode from "TEXT" and "PDU".
	1

Table 3-4-1-7 Cellular Parameters

Milesight

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	
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.

60

Loopback	Arthrens			
cooputer :	August 25.0			
IP Address		127.0.0 1		
Natmask		255.0.0.0		
Multiple IP	Addresses			
	₽ Adi		Netmask	Operation
				0

Figure 3-4-1-11

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

Table 3-4-1-9 Loopback Parameters

3.4.1.5 VLAN Trunk

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

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

Pa .	tertace	VO	Question
900 Q	*		

Figure 3-4-1-12

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

Table 3-4-1-10 VLAN Trunk Parameters

3.4.2 Firewall

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

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



Security	ACL	DMZ	Port Mapping	MAC Binding
Website Block	ing by URL Ad	dress		
URL Address		http://		
Makana Pirat				
Website Block	ing by Keywor	a		
Keyword				
		Figure 3-	4-2-1	

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

Table 3-2-2-1 Security Parameters

3.4.2.2 ACL

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

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

ACL Setting						
Default Filter Policy	Accept	÷				
Access Control List						
		туря	erden ded	¥		
		a c				
		Actor	permit	*		
		Prelocal	in .	*		
		Source IP	L	1		
		Source Wildcard Mask	9.0.0			
		Destination IP	-			
		Destrator Widcard Mark	3.0.0.9	_		
		Description	-	_		
		there	Galant			
nterface List						
inte	rtace	In ACL		0	#ACL	Operation
						0

Figure 3-4-2-2

ltem	Description
ACL Setting	
	Select from "Accept" and "Deny".
Default Filter Policy	The packets which are not included in the access control list will be processed by the default filter policy.
Access Control List	
Туре	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
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.		
Port	Set start destination port number. Range. 1-03555.		
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

3.4.2.4 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 Η to add a new port mapping rules.

Security	ACL	CMZ	Poil Mapping	MAC	ainding		
ort Mapping Source IP	ŝ	Source Port	Destination IP	Destination Post	Protocol	Description	Operation
0.0.0.0.0					TCP ¥		

Figure 3-4-2-4

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

Table 3-4-2-4 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.4.2.3 DMZ

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

Security	ACL	DMZ	Port Mapping
Enable			
DMZ Host			
Source Address			

Figure 3-4-2-3

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

Table 3-4-2-3 DMZ Parameters

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.	FortMapping	MAC Binding		
MAC Bindir	ng List					
	MACAddress		IP Address		Description	Operation
						8
						8

Figure 3-4-2-5

MAC Binding List

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

Table 3-4-2-5 MAC Binding Parameters

3.4.3 DHCP

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

DHCP Server_1			
Enable	8		
Interiace	wian0 🗸		
Start Address	192 168 66 100		
End Address	192.168.66.199		
Notmask	255.255.255.0		
Lease Time(Min)	1440		
Primary DNS Server	8.8.8		
Secondary DNS Server			
Windows Name Server			
Static IP			
MAC Ar	ddress	IP Address	Operati
			8

Figure 3-4-3-1

DHCP Server		
ltem	Description	Default
Enable	Enable or disable DHCP server.	Enable
Interface	Only wlan interface is allowed to distribute IP addresses.	wlan0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IP address obtained by DHCP clients from DHCP server.	255.255.255.0
Lease Time	Set the lease time on which the client can use the IP	1440

(Min)	address obtained from DHCP server. Range: 1-10080.	
Primary DNS Server	Set the primary DNS server.	8.8.8.8
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.

NS Metho	d List									
Name	Interface	Service Type	Userrame	UserIU	Password	Server	Server Parth	Nostname	Appe ed IP	Ope atio
	ularð 🗸	DynDl 👻	5 6 C		E 11	a a	12			

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

Table 3-4-4-1 DDNS Parameters

3.4.5 Link Failover

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

Configuration Steps

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

3.4.5.1 SLA

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

ny									
<u>10</u>	144+	Destination Address	Beconthey Destination Address	Debu Sian	(starsa(s)	Three add(me)	Pachet Lass Court	Set See	Operation
	100.070		221515	58	<u>.</u> #	9000	1	3000 ····	

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

Milesight

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						
10	Туре	SLA ID	lminefaco	Negativa Dalay(s)	Positive Delay(s)	Operation
۴.	910	• 1 •	where w		1	

Figure 3-4-5-2

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

switching).	

Table 3-4-5-2 Track Parameters

3.4.5.3 WAN Failover

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

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

AN Failova								
Main linter		Beckup In	Startup Deley(s)	Up Delay(s)	Down De	levis) To	ick ID	Operation
Califia: 0	- 34	ads 8	 36	0	0	1	4	63

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.

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

3.4.6.1 DMVPN

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

DMVPN	IPsec	GRE	1,279	PPTP	OpenVPN Client
OMVPN Settings					
Engola			×		
Hub Address					
Local IP Address					
GRE HUB IP Adds	115		-		
ORE Local IP Add	49.5		E		
GRE Mask	GRE Mask				
GRE Key			Î.		
Negotiation Mode			Main	٠	
Authentication Algo	ritter		DES		
Encryption Algorith	m		MD5	•	
DH Group			MODP768-1	•	
Kay					
Local ID Type			Delaut		
IKE Life Time(s)			10800		
BA Algorithm			DES-NO5	•	
PFS Group			NULL	Ť	
Life Time(s)			3600		

Figure 3-4-6-1

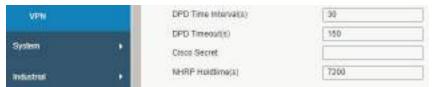


Figure 3-4-6-2

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.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication	Select from "DES", "3DES", "AES128", "AES192" and
Algorithm	"AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
	Select from "MODP768_1", "MODP1024_2" and
DH Group	"MODP1536_5".
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",
SA Algontini	"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.

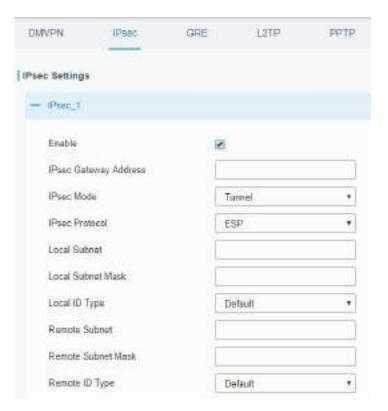


Figure 3-4-6-3

IPsec		
Item	Description	
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.	
IPsec Gateway Address	Enter the IP address or domain name of remote IPsec server.	
IPsec Mode	Select from "Tunnel" and "Transport".	
IPsec Protocol	Select from "ESP" and "AH".	
Local Subnet	Enter the local subnet IP address that IPsec protects.	
Local Subnet Netmask	Enter the local netmask that IPsec protects.	
Local ID Type	be Select from "Default", "ID", "FQDN", and "User FQDN".	
Remote Subnet	Enter the remote subnet IP address that IPsec protects.	
Remote Subnet Mask	Enter the remote netmask that IPsec protects.	
Remote ID type	Select from "Default", "ID", "FQDN", and "User FQDN".	
	Table 2.4.6.2 Daga Davamatara	

Table 3-4-6-2 IPsec Parameters

IKE Parameter	2		
IKE Version	IKEV1	•	
Negatistion Mode	Main	•	
Encryption Algorithm	DES	٠	
Authentication Algorithm	MDS	•]	
DH Group	MODP768-1	•	
Local Authentication	PSK	•	
Local Secrets			
XAUTH	0		
Lifetime(s)	10800		
SA Parameter			
SA Algorithm	DES-MD6	•	
PFS Group	NULL		
Lifetime(s)	3600		
OPD Time Interval(s)	00		
OPD Timeout(s)	150		
IPsec Advanced	2		
Enable Compression			
VPN Over IPsec Type	NONE	•	

Figure 3-4-6-4

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

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

Table 3-4-6-3 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.

DMVPN	IPsec	GRE	L2TP	PPTP
		-		
ORE Settings				
- ORE_1				
Enable		8		
Remote IF	² Address			
Local IP A	ddress	ĺ.		
Local Virt	all IP Address	Ê		
Netmask		2	55.255.255.0	
Peer Virtu	al IP Address	6		
Global Tri	Global Traffic Forwarding			
Remote S	ubnet			
Remote N				
MTU		1	500	
Кау				
Enabla N/	AT			

Figure 3-4-6-5

GRE	
Item	Description
Enable	Check to enable GRE function.

75

Enter the real remote IP address of GRE tunnel.	
Set the local IP address.	
Set the local tunnel IP address of GRE tunnel.	
Set the local netmask.	
Enter remote tunnel IP address of GRE tunnel.	
All the data traffic will be sent out via GRE tunnel when this	
function is enabled.	
Enter the remote subnet IP address of GRE tunnel.	
Enter the remote netmask of GRE tunnel.	
Enter the maximum transmission unit. Range: 64-1500.	
Set GRE tunnel key.	
Enable NAT traversal function.	

Table 3-4-6-4 GRE Parameters

3.4.6.4 L2TP

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

DMVPN	IPsec	GRE	L2TP	PPTP
- L2TP_1				
Enable				
Ramote II	PAddress			
Usemaine	ŧ			
Password	i.	E		
Authentic	Authentication		Auto	*
Global Tra	Global Traffic Forwarding		I	
Remote S	Remote Subnet		10.5.22.0	
Remote Subnet Mask		1	255 255 255 0	
Key		E		
Use L2TP	Use L2TP Peer DNS		i	

Figure 3-4-6-6

L2TP		
Item Description		
Enable	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	0
Protocol Field Compression	0.
Aaynemap Value	01011
MRU	1500
MTO	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.	

77

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 2.4.6.6.1.2TD Decemptors

Table 3-4-6-6 L2TP Parameters

3.4.6.5 PPTP

Milesight

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	IPséc	GRE	12TP	PPTP
PPTP Settings				
- PPTP_1				
Enable		×		
Remote IP	Address			
Username		[
Password				
Authentical	fion		Auto.	٠
Global Traf	fic Fanvarding	10		
Remote Su	ibnet			
Remote Su	ibnet Mask			

Figure 3-4-6-8

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

Remote Subnet Mask	Set the netmask of peer PPTP se	erver.
	Table 3-4-6-7 PPTP Parameters	
Advanced Sattings	2	
Local IP Address		
Peer IP Address		Ŭ.
Enable NAT		
Enable MPPE	×	
Address/Control Comp	pression 📃	
Protocol Field Compre	esion 🗐	
Asyncinap Value	100	
MRU	1500	
MTU	1500	0
Link Detection Interval	(s) 6P	
Max Retries	a	
Expert Options		

Figure 3-4-6-9

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

Table 3-4-6-8 PPTP Parameters

3.4.6.6 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. UG65 supports running at most 3 OpenVPN clients at the same time. You can import the ovpn file directly or configure the parameters on this page to set clients.

That May	5
Developmention Mathematic	Pik-Configuration -
Exelipantics File	server, Learner been been been been

Figure 3-4-6-10

OpenVPN Client - File Configuration		
ltem	Description	
Browse	Click to browse the client configuration ovpn format file including the settings and certificate contents. Please refer to the client configuration file according to sample: <u>client.conf</u>	
Edit	Click to edit the imported file.	
Export	Export the server configuration file.	
Delete	Click to delete the configuration file.	

Table 3-4-6-9 OpenVPN Client Parameters

تصب تصترفت	ingo toxigormoi	
himsel .	404	
nen i		
	(1944	
e etas dastate	40.	
	4.00	
a hote #		
man hannel (F		
inch/f		
generation in the local sectors of the local sector	148	
Constant operation	-00	
Talenter Terres(i)	100	
~	Suine	
F	1441	
a free las	+000	
insis Liveli	.0101038	
munt Optimi-		
and Biote		
	birm.	Line Ref.

Figure 3-4-6-11

OpenVPN Client - Page Configuration		
Item	Description	
Protocol	Select a transport protocol used by connecting UDP and TCP.	
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.	

Milesight

Port	Enter the TCP/UCP service number of remote OpenVPN server. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	 Select authentication type used to secure data sessions. Pre-shared: use the same secret key as server to complete 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	Set local tunnel address when authentication type is None or Pre-shared .
Remote Virtual IP	Set remote tunnel address when authentication type is None or Pre-shared .
Global Traffic	All the data traffic will be sent out via OpenVPN tunnel when this function
Forwarding	is enabled.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to Network > VPN > Certifications page to import a ta.key to TA field. 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
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
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: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. Example: ncp-ciphers AES-128-GCM; key direction 1
Local Route	
Subnet	Set the local route's IP address.

Subnet Mask Set the local route's netmask.

Table 3-4-6-10 OpenVPN Client Parameters

3.4.6.7 OpenVPN Server

UG65 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can import the ovpn file directly or configure the parameters on this page to set this server.

OpenVPN Server Settings	
Enable	8
Configuration Method	File Configuration 👻
Configuration File	Browse Import Export Delete

Figure 3-4-6-12

OpenVPN Server - File Configuration		
ltem	Description	
Browse	Click to browse the server configuration ovpn format file including the settings and certificate contents. Please refer to the server configuration file according to sample: <u>server.conf</u>	
Edit	Click to edit the imported file.	
Export	Export the server configuration file.	
Delete	Click to delete the configuration file.	

Table 3-4-6-11 OpenVPN Server Parameters

Enable	•	
Configuration Method	Page Configuration	*
Protocol	UDP	~
Port	1194	
istening IP		
nterface	tun	~
Authentication	None	¥
ocal Virtual IP		
Remote Virtual IP		
nable NAT	2	
Compression	LZO	~
ink Detection Interval	60	
ink Detection Timeout	150	
Sipher	Nane	~
đτu	1500	
Aax Frame Size	1500	
/erbose Level	ERROR	¥
opert Options		

Figure 3-4-6-13

Accostl	Deres		Farment	Country of
con Roma				
	Sec.		NOTION	-Docomen.
				0
Tert futured				
	Note	Balant	Webrand.	Densities



OpenVPN Server - Page Configuration				
Item	Description			
Protocol	Select a transport protocol used by connection from UDP and TCP.			
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN			

83

	server will bind to all interfaces.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. Pre-shared: use the same secret key as server to complete the authentication. After select, 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 select, 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	Set local tunnel address when authentication type is None or Pre-shared .
Remote Virtual IP	Set remote tunnel address when authentication type is None or Pre-shared .
Client Subnet	Define an IP address pool for openVPN client.
Client Netmask	Set the client subnet netmask to limit the IP address range.
Renegotiation Interval	Renegotiate data channel key after this interval. 0 means disable.
Max Clients	Limit server to a maximum of concurrent clients, range: 1-20. Note: please adjust log severity to Info if you need to connect many clients.
Enable CRL	Enable or disable CRL verify.
Enable Client to Client	When enabled, openVPN clients can communicate with each other.
Enable Dup Client	Allow multiple clients to connect with the same common name or certification.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to Network > VPN > Certifications page to import a ta.key to TA field. 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
<u> </u>	Select to enable or disable LZO to compress data.
Compression	
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Interval	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the

	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.
	User can enter some initialization strings in this field and separate the
Expert Options	strings with semicolon.
	Example: ncp-ciphers AES-128-GCM; key direction 1
Account	
Username & Password	Set username and password for OpenVPN client when authentication type
Userianie & Passworu	is username/password.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
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.

Table 3-4-6-12 OpenVPN Server Parameters

3.4.6.8 Certifications

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.

OpenVPN Client	
- OpenMM clear_1	
CA	BIONSE Munet Examt Examt
Public Rey	Browse Browse Easter Database
Privata Kay	Browye Provent Examine
TA.	Biowe Report Examination
Ponsheated Key	Browge Water Export Delite
P802512	Ennove munt Ennot Coldar
+ OpenVPN clock_E	
+ OperAPN clare_3	

Figure 3-4-6-15

OpenVPN Server							
- OpunVPN Ben	w.						
CA			Browse	Import	Export	Delete	
Public Key			Browse	Import	Export	Delate	
Private Key			Browse	Import	Export	Delete	
DH	[]		Browse	Import	Export	Delete	
TA.			Browse	Import	Export	Doiste	
CRL			Browse	Import	Export	Delete	
Preshared Key			Browsel	Import	Export	Defetu	
		Figure 3-4-6-16					
IPsec							
- IPsec_1							
CA			Browsie	Amport.	Export	Dateta	
Client Key			Browne	Import	Export	Doleta	
Press Val.			Section of the	PROPERTY.	N CONTRACTO	In the second	

[Erowse	Import	Export	Delete
	Browner	Import	Export	Dolete
	Browse	Import	Expot	Beleta
	Browso	Import	Export	Defete
1	Browse	Import	Export	Delete
		Browse Browse	Erowser Import Browse Import Browse Import	Erowan Import Export Browai Import Export Browai Import Export

Figure 3-4-6-17

3.5 System

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

3.5.1 General Settings

3.5.1.1 General

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

System					
Hostname		GATEWAY			
Web Login Time	out(s)	1800			
Access Servic	•				
	Enable	Servi	ce		Port
		нтт	P	6	Ø.
		HTTP	5	4	43
	0	TELN	ET	2	3
	8	SSF	ť	2	2
HTTPS Certifi	ates				
Certificate	https.crt	Browse	Import Export	Delete	

Figure 3-5-1-1

General				
ltem	Description	Default		
System				
Hostname	User-defined gateway name, needs to start with a letter.	GATEWAY		
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800		
Access Servic	e			
Port	Set port number of the services. Range: 1-65535.			
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80		
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443		
TELNET	Users can log in the device locally and remotely via TELNET to access and control it through Web after option is checked.	23		
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22		
HTTPS Certificates				
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.			

Keythen click "Import" button to upload the file into gateway. Click "Export" button will export file to the PCClick "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	lettings			
Current Time		2019-06-12 20:3		
Time Zone		8 China (Beijing	•	
Sync Type		Sync with Brows	var 🔹	
Browser Time		2019-06-12 20:3	4:32 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.		
	Click the drop down list to select the time synchronization		
	type.		
Sync 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		
LIIADIE NIF SEIVEI	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.

Enable	2
Email Address	
Jsername	
Password	
SMTP Server Address	
Port	25
Enable TLS	o

Figure 3-5-1-3

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

Table 3-5-1-3 SMTP Setting

Related Topics

Events Setting

3.5.1.4 Phone

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

	1141		-		
bute Name	ruse				
	Ren	÷.		Nardov	Operatio
	List			654321.123456	8



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

Table 3-5-1-4 Phone Settings

Related Topic

Connect on Demand

3.5.1.5 Email

Email settings involve email alarm for events.

well live			-		
	Nac			Email Address	Operation
	Not .	1		sam@umm.com.htt@priet.com	8
					0



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

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.

Usemame	admin	
Old Password		
New Password		
Confirm New Password		



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. You can use any ASCII characters except blank.
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 Managem	ert,			
Jser List				
Userneme	Password	Permission		Operation
stave		Read-Write	۲	
test		Read-Only		

Figure 3-5-2-2

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

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

Table 3-5-2-2 User Management

3.5.3 SNMP

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

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

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

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

3.5.3.1 SNMP

UG65 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

Status	Î	SNMP	MIB View	VACM	Ттар	MIB
Packet Forwarder		SNMP Settin	82			
		Enable				
Network Server		Port		161		
		System Name		24E124FF	FEF24660	
Network	•	SNMP Version		SNMPv2		~
System	-	Location Infon	nation			Ť
		Contact Inform	vation			
General Settings						
Liser Management		Save				
SNMP						

Figure 3-5-3-1

SNMP Settings			
Description			
Enable or disable SNMP function.			
Set SNMP listened port. Range: 1-65535.			
The default port is 161.			
Fill in the system name to represent the gateway.			
Select SNMP version; support SNMP v1/v2c/v3.			
Fill in the location 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	MB	
View List					
	iew Narnu	View	e Filter	View OID	Operation
All		Included] [1	
system		Included	14	1.36.1.2.1.1	
					0

Figure 3-5-3-2

MIB View			
ltem	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.

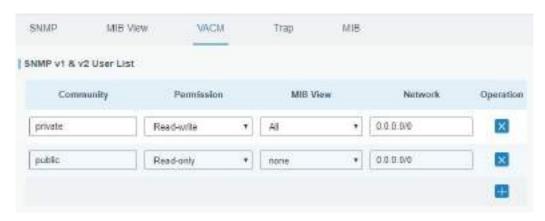


Figure 3-5-3-3

VACM			
ltem	Description		
SNMP v1 & v2 User List			
Community	Set the community name.		
Permission	Select from "Read-Only" and "Read-Write".		
MIB View	Select an MIB view to set permissions from the MIB view list.		
Network	The IP address and bits of the external network accessing the MIB view.		
Read-Write	The permission of the specified MIB node is read and write.		
Read-Only	The permission of the specified MIB node is read only.		
SNMP v3 User Lis	st		
Group Name	Set the name of SNMPv3 group.		
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and " Auth/Priv".		
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.		
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.		
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.		
	Table 3-5-3-3 VACM Parameters		

3.5.3.4 Trap

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

SNMP	MIB View	VACM	Trap	M	8
SNMP Trap					
Enable					
SNMP Version		SNMPv2			
Server Addres	16				
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 "Auth & Priv".	

Table 3-5-3-4 Trap Parameters

3.5.3.5 MIB

This section describes how to download MIB files.

SNIMP	MIB View	VACM	Trap	MIB
MIB Downloa	d			
MIEI Fila		AGENTX	MIB.6xt +	Download

Figure 3-5-3-5

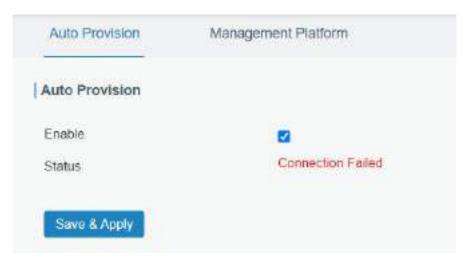
Download Click "Download" button to download the MIB file to PC.	

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 or Milesight Development Platform on this page so as to manage the gateway centrally and remotely.

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

Figure 3-5-4-1

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.	

96

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.	
	T 0 5 4 4	

Table 3-5-4-1

3.5.5 Events

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

3.5.5.1 Events

You can view alarm messages on this page.

Status	Events	Events Setting	6		
Lorawan +	Mark as Reat	Delote	Mark All as Read	Delote All Alama	
Notwork +		Sianas T	lype Tio	ie .	Message
System -	< × 10	• Go to	G0		
General Settings					
Soor Management					
AAA					
Device Management					
Events					

Figure 3-5-5-1

Events	
Item	Description
Mark as Read	Mark the selected event alarm as read.
Delete	Delete the selected event alarm.
Mark All as Read	Mark all event alarms as read.
Delete All Alarms	Delete all event alarms.

TypeShow the event type that should be alarmed.TimeShow the alarm time.	
Time Show the alarm time.	
Message Show the alarm content.	

Table 3-5-5-1 Events Parameters

3.5.5.2 Events Settings

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

Enable			
Phone for Notification	v		
Email for Notification	v		
Events	Record	Email Email Setting	SMS SMS Setting
Cellular Up		a	D
Cellular Down		a	
WAN Up		a	
WAN Down		0	
VPN Lip		a	
VPN Down	0	Q	
Power On	2		
Connect to UPS External Power Supplies		a	D
Connect to UPS Internal Battery	D	a	D
UPS Low Power (20%)	0	a	
UPS Abnormal Charging			
Disconnect the UPS			

Figure 3-5-5-2

Event Settings	
Item	Description
Enable	Check to enable "Events Settings".
Phone for	Salast phone group to reasive SMS alarm
Notification	Select phone group to receive SMS alarm.
Email for	Select Email group to receive Email alarm.
Notification	Select 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.
Emoil Cotting	Click and you will be redirected to the page "Email" to configure
Email Setting	the Email group.
0140	The relevant content of event alarm will be sent out via SMS if
SMS	this option is checked.
CMC Catting	Click and you will be redirected to the page of "Phone" to
SMS Setting	configure phone group list.
Phone Group List	Select phone group to receive SMS alarm.
Email Group List	Select Email group to receive Email alarm.

Table 3-5-5-2 Events Parameters

Related Topics

Email Setting Phone Setting

3.6 Maintenance

This section describes system maintenance tools and management.

3.6.1 Tools

Troubleshooting tools includes ping and traceroute.

3.6.1.1 Ping

Ping tool is engineered to ping outer network.

Ping	Ð	raceroute	Gxdmlog		
IP Ping					
Host		27) 27)		Ping	Stop
		Fi	gure 3-6-1-1		
	PING				
	ltem	Description			
	Host	Ping outer net	work from the	gateway.	
		Table 3-6-1	1 IP Ping Parame	eters	

Table 3-6-1-1 IP Ping Parameters

3.6.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Ping	1	raceroute Oxdimios	0
Tracero	oute		
Host			Trace Stop
		Figure 3-6-1	-2
	Tracer	ute	
	ltem	Description	
	Host	Address of the destina	tion host to be detected.
		Table 3-6-1-2 Tracerout	e Parameters

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.

5404	i	Benedate				
Location		schieles				
		Schedule	Frequency	These	Maste	Operation
NOWIN.	· •					
Bystem	- De -	Tare				
Mantonance	•					
(Real)						
Schedule						



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 2.6.2.1 Cabadula Daramatara

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	Lợg File	Download	
Log			
Vev ison(lites)	20		
	r notice redb(1959) 10 change c notice redb(1959) Backgrour		

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		0	
Sysleg Server Address			
Port		514	
Local Log File			
Storage		local	la la
Size		1024	108
Log Severity		inte.	1

Figure 3-6-3-2

Log Settings		
ltem	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.

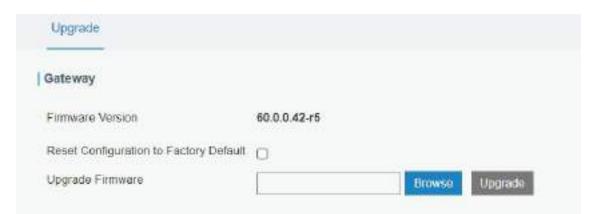


Figure 3-6-4-1

Upgrade		
ltem	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 2.6.4.1.Un grade Devenantere	

Table 3-6-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.6.5 Backup and Restore

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

Backup and Restore			
Restore Config			
Config File		Browse	Import
Backup Running-col	nfig		
Full Backup	Batch Backup		
Restore Factory Def	aults		
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.	
Batch Backup	Click "Batch Backup" to export current configuration except gateway ID of packet forwarder, all embedded NS settings, static IP address of WAN, WLAN settings, user management settings, DeviceHub authentication code, all APP settings.	
Reset	Click "Reset" button to reset factory default settings. gateway will restart after reset process is done.	

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

Related Configuration Example

Restore Factory Defaults

3.6.6 Reboot

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



Figure 3-6-6-1

3.7 APP

Milesight

3.7.1 Python

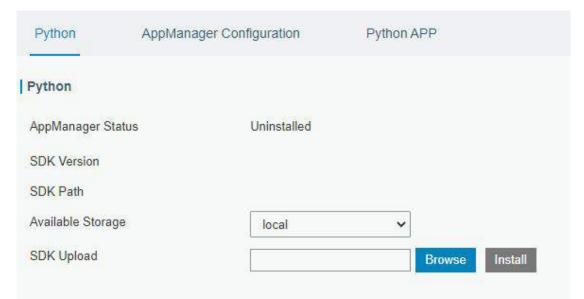
Python is an object-oriented programming language that has gained popularity because of its clear syntax and readability.

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

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

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

3.7.1.1 Python





Python	
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 Co	onfiguration	Python APP		
AppManager					
Enable					
App Managem					
ì	D	App Command	Logfile Size(Mi	B) Uninstall	
App Status					
	App Name		App Version	SDK Version	

Figure 3-7-1-2

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

Python	AppManager Configuration	Python APP	
Import App F	Package		
App Package		Browse	Import
lmport App C	Configuration		
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. For more guidance and documentation please refer to Node-RED official website.

3.7.2.1 Node-RED

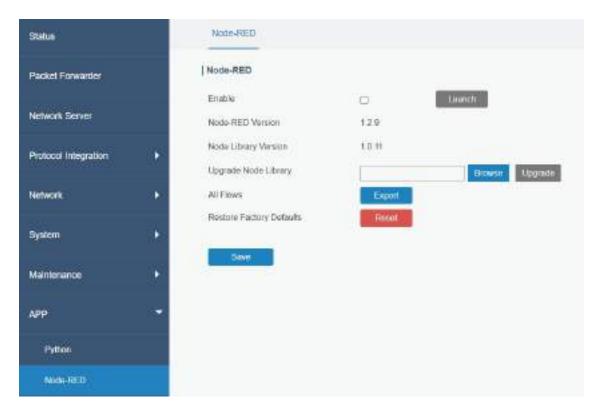


Figure 3-7-2-1

Node-RED	
ltem	Description
Enable	Enable the Node-RED.
Launch	Click to launch the web GUI of Node-RED.
Node-RED Version	Show the version of the Node-RED. The Node-RED version
	can be upgraded only when you upgrade the gateway.
Node Library Version	Show the version of the node library.
Upgrade Node Library	Upgrade the node library by importing the library package.
All Flows Export	Export all flows as a JSON format file.
Restore Factory Default	Erase all flow data of Node-RED.
Table 3-7-2-1 Node-RED Parameters	

Milesight provides a customized node library to use the interfaces of the gateway.

Milesight



Figure 3-7-2-2

Node Library	Node Library						
Node	Description						
LoRa Input	Receive LoRaWAN [®] packets from the gateway. This only works when the network server is enabled.						
LoRa Output	Send downlink commands to LoRaWAN® nodes.						
Device Filter	Filter out the data of one or more specific LoRaWAN [®] nodes via device EUIs.						
GW Info	Monitor events of gateway, this needs to ensure the event detection is enabled in General > Events > Events Settings .						
Email Output	Send an Email. If you select STMP option as "Same as the gateway", it is necessary to go to System > General Settings > SMTP page to configure SMTP client settings.						
SMS Input	Receive SMS message. This only works when the cellular is connected.						
SMS Output	Send an SMS message. This only works when the cellular is connected.						

Table 3-7-2-2 Node Library Parameters

Related Configuration Example

Node-RED

Chapter 4 Application Examples

4.1 Restore Factory Defaults

Method 1:

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.

Materia Server		Basicip and Kancow
Provide Strangestern	÷	Carely File
Nitheon		Bickus Running-carrily
	4	The formation of the second se
w.newm-	-	Rentiste Factury Defaults and texes the system in factory behavity. Continue?
Nieto.		Rent Canel
Service 1		
- 100		
1.000000		
Saidly and Uniters		

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

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

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

Related Topic

Restore Factory Defaults

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	0
Upgrade Firmware	Browse Upgrade
Please keep	p 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.

Milesight

Port	WLAN	Cellular	Loopback	VLAN Trunk		
- Port_	t					
Port			eth 0	~		
Conn	ection Type		Static IP	÷		
IP Ad	dress		192.168.44.186			
Nətm	ask		255.255.255.0			
Gater	way		192.168.44.1			
MTU			1500			
Primary DNS Server			8.8.8.8			
Secondary DNS Server			223.5.5.5			
Enab	ie 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	Oxemiog		
Protocol Integration		IP Ping	www.gov	with cours	Pire	5820
Network	*	PING www	rgoogia .com (172.217. om 172.217.25.4. sog-	75 4): 58 data byli	ni	SHY.
System	•	64 bytes fri 64 bytes fri	om 172 217 25 4 1995 om 172 217 25 4 1995 om 172 217 25 4 1995	1 8=117 time=19. 2 8=117 time=19.	705 mis 707 mis	
Memonance	•	-4 pielkats t	ogle com ping statistic renamified, 4 packata	eceived, this pack		
Tech			neolavgimetr = 19.750/			

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.

Enable	63	
Network Type	Auto	ų
AFN		
Username		
Password	1	
Access Number		
PIN Code		
Authentication Type	None	~
Roaming	8	
Customize MTU	8	
мты	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 Porward	Celular	Network	WLAN
Modern				
Status		Randy		
Nodel		EC26		
Version		EC25ECOARMAN7M	10	
Signal Level	2	23asu (+07dBm)		
Register Status		Registered (Home mit	valo	
IMEI	4	880425047368939		
iM81)	480010425301842		
ICOD	3	093801178300000341	29	
199	2	CHNHANCOM		
DRIVEOUTSpe	1	LTE		
#LMN ID				
EAC:	e e e e e e e e e e e e e e e e e e e	5022		
Cell ID	2	3496583		
Network				
Statue	9	Connedeti		
IP Address		10.132.132.59		
Notesaak		259,255,255,240		
Galeyrey		10 132 132 00		

Related Topic Cellular Setting

Cellular Status

4.5 Wi-Fi Application Example

4.5.1 AP Mode

Application Example

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

Configuration Steps

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

WLAN	Cellular	Loopback	
	AP	~	
c <mark>a</mark> st			
	802.11n	(2.4GHz) 🗸	
	Auto		
	Gateway_F1200F		
	24:e1:24	:f1:20:0f	
Mode	No Encr	yption 🗸	
	20MHz	~	
Number	10		
	cast	cast Cast Cast Cast Cast Cast Cast Cast C	

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	WEAN	VPN
WLAN Status					
Wineless Status		Enabled			
MAC Address		24 e1 24 f1 20 0f			
Interface Type		AP			
SSID		Gateway_F1200F			
Chennel		Auto			
Encryption Type		No Encryption			
Status		Up			
IP Address		192,168,1,1			
Netmask		255 255 255 0			
Connection Duration	1	0 days, 02:40:52			

4.5.2 Client Mode

Application Example

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

Configuration Steps

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

ort WL	AN	Cellular	Loc	oback.			
laBack							
SSID	Channel	Signal	Cipher	BSSID	Security	Frequency	
AAA	Auto	-61dBm	AES	24.e1.24;f0.c4;13	WPA-PSK/WPA2-PSK		Join Network

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

point.

Milesight

Port	WLAN	Cellular	Loophack
WLAN			
Enable		•	
Work Mode		Client	✓ Sonn
S510		AAA	
BSSID		24:e1:24:10:c4	13
Encryption N	Aode	WPA-PSK/WP	A2-PSK 🖌
Clpher		AES	~
Key			
P Setting			
Protocol		DHCP Client	~

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

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

Overview	Packet Forward	Cellular	Network	WLAN
WLAN Status				
Wireless Status	51	Enabled		
MAC Address	4	24 e1 24 f0 de 14		
Interface Type		Client.		
SSID	3	AAA		
Channel		Auto		
Encryption Type	3	NPA-PSK/NPA2-PS#	¢	
Cipher		AES		
Status	0	Connected		
IP Address	3	192,168,1,145		
Netmask	1	255 255 255 0		
Connection Duratio	n (0 days, 02 44:45		

Related Topic

WLAN Setting

WLAN Status

4.6 Packet Forwarder Configuration

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

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

General	Radios	Advanced	Custom	Traffic		
General Setting						
Gataway EUI	24E124FFFE	F12257				
Gateway ID	240124017	CF12257				
Frequency-Sync	Disabled	*				
Multi-Destination						
10	Enable	Тур		Server Address	Connect Status	Operation
0	Enabled	Embedde	d NS	localhost	Connected	

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

Туре	Samtach v
Server Address	eut cloud thethings network
Port Up	1700
Port Down	1700

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

gios		US915		~		
	Name			Certor Frequency/MHz		
	Fade 0		90	0		
	Radie 1		90	905.0		
Multi Channels Settin	a					
Enable	Index	Radio		Frequency/MHz		
2	0	Radio D	÷	903.9	- 21	
	1	Radia II	(e)	904.1		
2	2	Rado 6	.*	904.3		
2	3	Radio 0	~	904.6		
8		Radio 1		901.7		
2	5	Radio 1	v	904.9	11	
	6	Radio 1	4	905.1		
				905.3		

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

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

Senaral	Radio		encea	Custom	Tiatio			
affic Set	ting							
Skip Rich	Gioctice	time	Ticks	Енцинску	Datacote	Coderate	H551	SNIE
÷		857.M	212136745 3	903.5	6F100/0125	45	-51	13.2
÷.	w	85.57.29	211944523	904.8	s#76W125	41	-01	81
э	ω	15 57 13	218431286 T	904.E	19F-86W500	46	-61	на
	Sie:	\$5.57.08	2006908905 6	903.5	SF7SW125	45	-85	14.2

4.7 Connect to Milesight IoT Cloud

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

Status		flemenar	Rates	Advanced	Custom	Total		
Partici Fernanda		Oververal SetSing						
Network Server		Gateway/ID	24E124FFF					
Network		Fraguency-Synt	Clivabled					
System .	•	Multi Destination						
	30	ID.	Easthi	Typ	•	Server Address	Connect Status	Operations
Mathematica		P.	Erabled	Embods	ed NS	localitest	Convected	
APP	÷							

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

egioe		U8915		~
	Name			Center Frequency/MHz
	Radie 0		904	3
	Radie 1		905	0
Aulti Channels Settin	a.			
Enable	Index	Radio		Frequency/MHz
2	0	Radio D		905.9
8	1	Radio II		914.1
23	2	Radio 6	.*	904.3
2	3	Radio 0	*	904.6
8		Radio 1	÷	904.7
23	5	Radio 1	•	904.9
	6	Radio 1	~	995.1
				A Real Providence of the second se

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

Status		General	Applications	Profiles	Device
Packet Forwarder		General Setting			
Network Server		Enable Cloud Mode	8		
Network			Miasigh	t lo7 Claud 🗸 🗸	1
		NotiD	010203		
System		Join Delay	5		Bec
		RX1 Delay	1		560
Maintenance		Lease Time	8760-0-0		hh-mm-sa
APP	E.	Log Level	ktfo	v	1

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.

TATION C	(inside a	Gro	100	TRATING .	+				
Ad. Cherry	Pres.	1		1.1-1-1	2.444 (10.000	() mittig (1 martine
ton Tapat		REDR-0.	Add Denial						市区市
Reports	0	destroite	+5kr				mandad peter proc		010
anni ini ta 🧑 Shariy (arse		4014.04	Trans.					1	10 In (1)
lan,	о д	AMPROX CONSTITUTION		102	-	Contra	-	a ha anna agu	0100
		200	irc	\$T%		0 Andrew (1997)	Itas		
Ξ.									

5. The gateway is online on Milesight IoT Cloud.

	5	D beend it has prove to 1 the seal	ne 0	A state of the local division of
1.94	e) here	Associated Deense Invest Ann Johnson Association	Lottanee	
5 14	an real sectors	101110 See	1.00000032	0 M (0
	i (see	and they	all attended to a set of the set	all strate and strate to a strate str

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		
Nama	doud	
Description	clouid	

- 3. Click "Save" to create this application.
- 4. Click ២ to add a data transmission type.

HTTP or HTTPS:

Milesight

Step 1: select HTTP or HTTPS as transmission protocol.

Type	HTTP	•
	16.000	

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

Data Type	URL	
Uplink data		
Join nettification		
ACK notification		
Error notification		

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

HTTP Header			
	Hender Name	Header Value	Operation
			8

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.

User Credentials	
Enable	
Usemame	
Password	

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

TLS	
Enable	*
Mode	Self signed certificates *
CA File	Browsor Import Dolate
Client Certificate File	Browse Import Solute
Client Key File	Browse Import Delete

Step 4: Enter the	e topic to	receive	data ai	nd cl	hoose t	the	QoS.
-------------------	------------	---------	---------	-------	---------	-----	------

Data Type	topic		
Uplink data	descentient	QeS 0	
Downlink data		QoS 0	2
Multicast downlink data		QuS 0	5
Join notification		QeS 9	
ACK notification		QoS 0	
Error solification		QUS 1	
Request data	www.minequest	Q05 0	
Response data	Aventibesponse	DetS 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 D	olate All			Snech	
Device Name	Device EUI	Device-Profile	Application	Last Seen	Activated	Operation
		No mate	hing records found			
	Device Name		lora-sens	DC.		
	Description		a shorî de	actiption of you	r node	
	Device EUI		0000000	00000000		
	Device-Profile		ClassA-C)TAA.	~	
	Application		cloud		~	
	Paylod Codec				-	
	fPort.		1			
	Frame-counter \	/alidation			-	
	Application Key Device Address		1			
	Network Session	n Key				
	Application Ses	ion Key				
	Uplink Frame-co	ounter	Ø			
	Downlink Frame	-counter	0			

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.

	6 K.	-11	0	-D-	8.		6	HE .	1
- Sin	24e1242151323366	description	deretii 24e1262131323266	application cloud	deviceprofile ClassC-0744	appley 112233445566778899aa112233445569	devaddr	appolary	mekakay
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.

112	781715	1000 m	8/2012	-		1T	ste .	2015-08-001917229+00-00	0
++12	21210	000100000	#18+3	98	22	**	2006	000 - 00 - 00 TREESED - 00 CR	0

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

Device Eth	Type	Payload	Fport	Confirmed
11228121915	ASOI .	15	16	



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.

Owice ESI	Type	Payload	Filen	Conterna
112201319013	A508 +	15	15	

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

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

11226121210111123	989625257	SP-SSW-SS	17, 17,	+	2	BADat	stress arrester and Success
H12812H9HWH03	¥.			- 36	2	DeCH	Pending 0

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

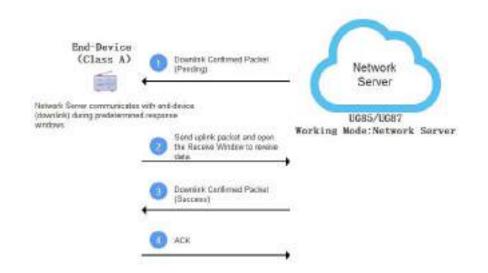
Denne 201	Esquerry	Datastas	948	859	- 694	fea.	Type	Tene	Deam
H220-019-13	0000000	1011020-02				1.	Delare	2010-00-00100-23-444-00-001	0
1123012101010	91420008	REMARKS.	188	35	16	- 21	NOR.	2816-06-08T80.23-48680-80	
112201210	WINGSNOE	SP1394-03	-	-	8	2	Urce!	38154-04-02189-23-54-60180	0
m2003110	1				10	- E.	Bille		0
H2851299	washing	senseira					littire.	2814-09-08132.22 49-405.00	a

Packets Details		×
Dev Aiddr	0747	1
GwEUI	2401240	
AppEUI	55724C	
DevEUI	1122612191311123	
Immediately	The second s	
Timestamp	874346044	
Type	UpCnf	
Adr	fatso	
AdrAcKReq	falso	
ACK	Billio	
Fore	21	
Eport	35	
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.

Nativore Derver										Show the pipel miles with
Die .								hour la	0	HEB They be seen at signed intergal bedrater
Derica EUF	Disparsy	Determine	186	855	240	108	Tom	Tmi	Dealto	Base There the plan of plantse
HURDINGENGE	80120200	071801/105				10	Online.	30.0-04718-40.50-08.00		Post
HEROPHICH	1012000	SF1MINUS	1418	-16	141	- 24	305	2010/06/07 09 09 10 10 10 10	0	This this harts counter
HEROPHINHON	and below.	SENSIVE	164	- 78	44.	.21	UpOH ::	2010-08-0703-08-08-08-08	0	Type Discording type of the parameter of
minimumin	0001100000	SPIRINGS.					DADA	2010-08-00109-08-00-08-08	Success	Artisten - Add Accupy Dacholt Artisten - Add Responsi Pacitist
imprintation	801005	221303/329	10.0	112	- 14	10	UpDel	2010-02-01111-0110-0210	0	Value - lageral deconfinitient - Value
margonnes					18		THOP	Pending	0	UpDif - Tailet Castlenael Packet ACK response transitionil research
1026019011028	Ministeriess-	881189725	-			ų.	Order .	3010-00-00T0E-0130-00:00	0	Ditter - Operank (Jaconfirme) Placket
manasema	money	stieves	41	-18	- 94		UpCar	management of product	0	Dico-
нажанные	101110100	01100108			. *		Online .	30-0-06-06109-48 56-(400)	0	disc in a subjective of
itta dibidetta	800130000	571854125	412	-114	54		UpOnt	30-9-00-00122 40:37-08:90	0	Them there we take of participant part of
								144	A REPORT OF	



Chevron 1								Teach	0
Device EU	Esquercy	Detects	SNR	855	Stat	Fire	Type	Time	October
122012101210121	660380080	\$11003105			÷ ĝ	40	DeLieu	2015-06-06739 89 39+06 18	0
11228-1216/1317 123	8083 00000	19189025	10.8	100	- 39	11	ACH	2010-08-06130-49-38+08-08	0
1122612191311123	898380080	3F1851/125	10.8	-76	-64	1	(I)C/H	2015-06-06705-49-38+08.00	0
12241031031031	809180080	SF 1830-55	means	the di	evice	has re	ceived t	he packet you send.	0
1122612181511125	808190080	571351155	9.8	-77	54	28	UpOrt	2010/08-08/189 48 43408 08	0
022642161301123	1				- 0	10	Driver		0
12201210-01022	80868080	SF1000128		14	.0	12	Deller	2819-08-06739-87-38+06.08	0
1122512101311123	8030.000000	SF189/55	3.1	-74	-04	30	UpOrt	2010/05/05129 47:35+08:08	0
1122612191011125	803180080	8F1890125		10	10	19.	D40ec	2019-06-06739.46.38+06.09	0
CONTRACTOR CONCERN	800180080	GE VALUE OF	.112	.78	- 64	10	IDON .	2010/06-00130-00 37+08-08	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.



4.11.2 Send Data by Email

Application Example

Send AM104 device data by Email.

-	40	- 10	rangest	and .	Filme 1	+ =	4.14mg	1.1	4.4	
		(144)	er minum		440m []	l		1 and		1 H
			200000 () ×					And Administration (1)		

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.

100.00	4.01	1.000	 Cott Service Film	ernola	
			10.00		time in the
			0 Properties		· 01 10
			19836	AMAGE	
			(00010)	Lan La DO Muntaga	+
	Concer 5-	(1991)			

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



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}}

Cont.	401	100		Build Brown Charge	ut moint		
				2444		100	1 How
							• 10 m
-				Nate	Add top (2 and its Down)		
-	()move)-	Con .	- Carton and Carton	EMTP Optox	tpatel. +		
				(Aug 10)	armogram.		
			C.Zmanne T3	Photos			
				ADAMA AND	Setting repeating com		
				Per	(e)		
				(1404) (10	D		
		2.7			Description		
				1qm	ANY DESIGN OF		
				Involt	(contexts of Stational ((contexts (Stational)) (contexts (Stational))		

Note:

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

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

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

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

100	-		1000	-	Pice 1	(+)(=	1.000		4		•
								-		120	1
		() (mm)	Arminist	- Caura							

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

AM100 Data

From ②milesight.com> To ③milesight.com> Time: 2021年4月30日(死五)17:13 ④ Size: 2 KB

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

Related Topic

Node-RED

[END]

2021-04