

5G CPE UF51 User Guide



Preface

Thanks for choosing Milesight UF51 5G CPE. The UF51 5G CPE 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 describes how to configure and operate the UF51 5G CPE. You can refer to it for detailed functionality and device 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

© 2011-2022 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 IoT Co., Ltd.

Related Documents

Document	Description
UF51 Datasheet	Datasheet for the UF51 5G CPE.
UF51 Quick Start Guide	Quick Installation guide for the UF51 5G CPE.

Declaration of Conformity

UF51 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.





For assistance, please contact Milesight technical support: Email: iot.support@milesight.com Tel: 86-592-5085280 Fax: 86-592-5023065 Address: Building C09, Software Park III, Xiamen 361024, China

Revision History

Date	Doc Version	Description
June 21, 2021	V 1.0	Initial version

Contents

Chapter 1 Product Introduction	8
1.1 Overview	
1.2 Advantages	
1.3 Specifications	9
1.4 Dimensions (mm)	12
Chapter 2 Access to Web GUI	13
2.1 Wireless Access	13
2.2 Wired Access	14
Chapter 3 Web Configuration	
3.1 Status	
3.1.1 Overview	
3.1.2 Cellular	
3.1.3 Network	
3.1.4 WLAN	
3.1.5 VPN	
3.1.6 Routing	
3.1.7 Host List	
3.1.8 GPS	
3.2 Network	
3.2.1 Interface	
3.2.1.1 Link Failover	
3.2.1.2 Cellular	
3.2.1.3 Port	
3.2.1.4 WAN	
3.2.1.5 Bridge	
3.2.1.6 WLAN	
3.2.1.7 Switch	
3.2.1.8 Loopback	
3.2.2 DHCP	
3.2.2.1 DHCP Server/DHCPv6 Server	
3.2.2.2 DHCP Relay	
3.2.3 Firewall	
3.2.3.1 Security	
3.2.3.2 ACL	
3.2.3.3 Port Mapping	
3.2.3.4 DMZ	
3.2.3.5 MAC Binding	
3.2.3.6 Custom Rules	
3.2.3.7 SPI	
3.2.4 QoS	
3.2.5 VPN	
3.2.5.1 DMVPN	

3.2.5.2 IPSec Server	50
3.2.5.3 IPSec	
3.2.5.4 GRE	56
3.2.5.5 L2TP	57
3.2.5.6 PPTP	59
3.2.5.7 OpenVPN Client	61
3.2.5.8 OpenVPN Server	63
3.2.5.9 Certifications	65
3.2.6 IP Passthrough	67
3.2.7 Routing	68
3.2.7.1 Static Routing	
3.2.7.2 RIP	
3.2.7.3 OSPF	71
3.2.7.4 Routing Filtering	77
3.2.8 VRRP	77
3.2.9 DDNS	79
3.3 System	81
3.3.1 General Settings	
3.3.1.1 General	81
3.3.1.2 System Time	82
3.3.1.3 Email	
3.3.2 Phone&SMS	85
3.3.2.1 Phone	85
3.3.2.2 SMS	
3.3.3 User Management	88
3.3.3.1 Account	88
3.3.3.2 User Management	89
3.3.4 SNMP	
3.3.4.1 SNMP	90
3.3.4.2 MIB View	91
3.3.4.3 VACM	91
3.3.4.4 Trap	
3.3.4.5 MIB	
3.3.5 AAA	93
3.3.5.1 Radius	
3.3.5.2 TACACS+	94
3.3.5.3 LDAP	
3.3.5.4 Authentication	
3.3.6 Device Management	
3.3.6.1 DeviceHub	
3.3.6.2 Milesight VPN	
3.3.7 Events	
3.3.7.1 Events	
3.3.7.2 Events Settings	

3.4 Industrial Interface	
3.4.1 I/O	
3.4.1.1 Dl	
3.4.1.2 DO	103
3.4.2 Serial Port	
3.4.3 Modbus Slave	
3.4.3.1 Modbus TCP	
3.4.3.2 Modbus RTU	
3.4.3.3 Modbus RTU Over TCP	
3.4.4 Modbus Master	
3.4.4.1 Modbus Master	
3.4.4.2 Channel	110
3.4.5 GPS	112
3.4.5.1 GPS	112
3.4.5.2 GPS IP Forwarding	113
3.4.5.3 GPS Serial Forwarding	
3.5 Maintenance	115
3.5.1 Tools	
3.5.1.1 Ping	
3.5.1.2 Traceroute	115
3.5.1.3 Packet Analyzer	
3.5.1.4 Qxdmlog	
3.5.2 Debugger	
3.5.2.1 Cellular Debugger	
3.5.2.2 Firewall Debugger	
3.5.3 Log	118
3.5.3.1 System Log	
3.5.3.2 Log Download	119
3.5.3.3 Log Settings	
3.5.4 Upgrade	
3.5.5 Backup and Restore	
3.5.6 Reboot	
3.6 APP	
3.6.1 Python	
3.6.1.1 Python	
3.6.1.2 App Manager Configuration	
3.6.1.3 Python App	
apter 4 Application Examples	
4.1 Restore Factory Defaults	
4.1.1 Via Web Interface	
4.1.2 Via Hardware	
4.2 Firmware Upgrade	
4.3 Events Application Example	
4.4 SNMP Application Example	

4.5 Network Connection	132
4.5.1 Cellular Connection	132
4.5.2 Ethernet WAN Connection	134
4.6 Wi-Fi Application Example	135
4.6.1 AP Mode	
4.6.2 Client Mode	
4.7 VRRP Application Example	137
4.8 NAT Application Example	140
4.9 Access Control Application Example	141
4.10 QoS Application Example	142
4.11 DTU Application Example	143
4.12 PPTP Application Example	147

Chapter 1 Product Introduction

1.1 Overview

Milesight UF51 5G CPE is designed as a cost-effective solution providing for 5G wireless networking application. Adopting high-performance industrial platform of quad-core CPU and 5G cellular module, UF51 is capable of providing ultra-fast Internet connection and ultra-small packages to ensure the extremely safe and reliable connection to the wireless network. With various kinds of installation methods, IP67 waterproof enclosure and novel design, UF51 is applicable to indoor and outdoor applications.

Meanwhile, the UF51 also supports 2-port Gigabit Ethernet switch, serial port (RS232/RS485) and I/O (input/output), which allow you to scale up M2M application combining data and video in limited time and budget.

The UF51 is particularly ideal for smart offices, video surveillance, digital media implementations, industrial automation, traffic applications, robots and so on.

For details of hardware and installation, please check the UF51 Quick Start Guide.

1.2 Advantages

Benefits

- Built-in Qualcomm quad-core CPU and big memory
- 4G LTE/5G NR (NSA/SA) network with dual SIM cards for backup among multiple carriers networking
- Gigabit Ethernets for fast data transmission
- Equipped with Ethernet, I/O, serial port, Wi-Fi, GPS for connecting diverse field assets
- Embedded Python SDK for second development
- Pole mounting, wall mounting, desktop, bottom magnetic or lock mounting for various applications
- 3-year warranty included

Security & Reliability

- Automated failover/failback among Ethernet, Cellular and Wi-Fi
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN
- Embed hardware watchdog, automatically recovering from various failure, and ensuring highest level of availability
- Establish a secured mechanism on centralized authentication and authorization of device access by supporting AAA (TACACS+, Radius, LDAP, local authentication) and multiple levels of user authority

Easy Maintenance

- Milesight DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and several upgrade options help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve simple management and quick configuration among a large quantity of devices
- 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
- It can be continuously running in a broken or weak network environment, and the latest data can be synchronized to remote server after the network is restored
- Support rich protocols like SNMP, Modbus bridging, RIP, OSPF
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

Hardware System	
CPU	Qualcomm Quad-core ARM Cortex A7, 716.8 MHz
Memory	8 GB Flash, 512 MB DDR3 RAM
Ethernet	
Ports	2 × RJ-45
Physical Layer	10/100/1000 Base-T (IEEE 802.3)
Data Rate	10/100/1000 Mbps (Auto-Sensing)
Interface	Auto MDI/MDIX
Mode	Full or Half Duplex (Auto-Sensing)
PoE	1 × 802.3af PoE PD on WAN/LAN port
Cellular Interfaces	
Network	5G/4G LTE
Antenna	8 × Internal Antennas
SIM Slot	1 (Mini SIM-2FF)

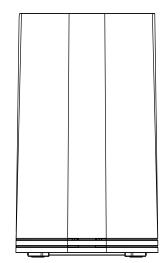
1.3 Specifications

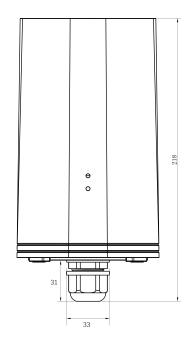
Wi-Fi Interface	
Antenna	4 × Internal Antennas
Standards	IEEE 802.11 a/b/g/n/ac
Tx Power	2.4 GHz: 26dBm(max)
TX Power	5 GHz: 26.4dBm(max)
Rx Sensitivity	
2.4 GHz	802.11b: ≤ -92dBm@11Mbps
	802.11g: ≤ -78dBm@54Mbps
	802.11ac VHT20: ≤ -91dBm@MCS0
	802.11ac VHT20: ≤ -66dBm@MCS8
	802.11ac VHT40: ≤ -88.5dBm@MCS0
	802.11ac VHT40: ≤ -64dBm@MCS8
	802.11a: ≤ -91dBm@6Mbps
	802.11a: ≤ -76dBm@54Mbps
	802.11ac VHT20: ≤ -90dBm@MCS0
5 GHz	802.11ac VHT20: ≤ -68dBm@MCS8
	802.11ac VHT40: ≤ -87dBm@MCS0
	802.11ac VHT40: ≤ -65dBm@MCS9
	802.11ac VHT80: ≤ -84dBm@MCS0
	802.11ac VHT80: ≤ -60dBm@MCS9
Modes	AP and Client Mode
Security	WPA/WPA2 Authentication, WEP/TKIP/AES Encryption
10	
Connector	3.5 mm Terminal Block
Digital	1 × DI (Dry Contact) + 1 × DO (Wet Contact)
Serial Interface	
Ports	1 × RS232 or 1 × RS485 (Switchable)
Connector	3.5 mm Terminal Block
Baud Rate	300bps to 230400bps
GNSS ¹	
Antenna	1 × Internal Antenna
Technology	GPS/GLONASS/Beidou/Galileo/QZSS

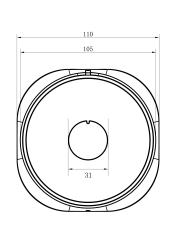
¹ GNSS is under development.

Software	
	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2,
Network Protocols	OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN,
	SSH, etc.
VPN Tunnel	DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE
Access Authentication	CHAP/PAP/MS-CHAP/MS-CHAPV2
Firewall	ACL/DMZ/Port Mapping/MAC Binding/SPI/DoS & DDoS Protection
Firewall	/IP Passthrough
Management	Web, CLI, SMS, On-demand Dial up, DeviceHub
AAA	Radius, TACACS+, LDAP, Local Authentication
Multilevel Authority	Multiple Levels of User Authority
Reliability	VRRP, WAN Failover
Carial Dart	Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to
Serial Port	Modbus TCP)
Power Supply and Cons	umption
Connector	2-pin 3.5 mm Terminal Block
Input Voltage	9-48 VDC or 802.3af PoE PD
Power Consumption	≤ 7 W
Physical Characteristics	
Ingress Protection	IP67
Housing	Polycarbonate + Metal
Dimensions	No Waterproof Connector: φ105 x 110 x 187 mm (φ4.13 x 4.33 x 7.36 in)
	With Waterproof Connector: \$\$\phi105 x 110 x 218 mm (\$\$\phi4.13 x 4.33 x 8.58 in)\$\$
Mounting	Desktop, Wall Mounting, Pole Mounting, Bottom Magnetic/Lock Mounting
Others	
Reset Button	1 × RESET
LED Indicators	1 × STATUS, 1 × Cellular Network
Built-in	Watchdog, 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 UF51 device. Username: **admin** Password: **password**

2.1 Wireless Access

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

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

to access the web GUI.

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

	Milesight	
*	Username	
8	Password	
	Login	

English

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

4. After logging in the web GUI, you can view system information and perform configuration.

			For your device se	curity, please change the default pass	sword	
Status		Overview	Cellular Network	WLAN VPN	Routing Host List	â Help
		-				Model
Network	•	GPS				Show the model name of router.
		System Information	1	System Status		Serial Number
System	×					Show the serial number of router.
		Model	UF51-501EU	Local Time	2021-07-28 10:44:44 Wednesday	Firmware Version
Industrial	•	Serial Number	6901B1901925	Uptime	1days, 13:57:19	Show the current firmware version of router.
		Firmware Version	76.2.0.2	CPU Load	7%	Hardware Version
Maintenance	•	Hardware Version	V1.0	RAM (Available/Capacity)	215MB/512MB(41.99%)	Show the current hardware
				Flash (Available/Capacity)	2911MB/4096MB(71.07%)	version of router.
APP	•					Show the current local time
		Cellular 😑 Link in i	use	WAN		of system.
		Status	Ready, 5G NR, Yill	Status	Online	Uptime Show the information on how
		IPv4	10.2.25.72/28	IPv4	192.168.22.213/24	long the router has been running.
		IPv6	fe80::7cf3:90ff:fe33:6151/64	IPv6	fe80::26e1:24ff:fef1:e38d/64	CPU Load
		Connection Duration	0 days, 23:05:19	MAC	24:e1:24:f1: Manual Refresh 🗸 Refresh	Show the current CPU utilization of the router.

2.2 Wired Access

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

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

A St a Network	and Internet > Network and Sharing Center	5 ~	Search Control Panel	
Control Panel Home View your basic network information and set up co				
Characteriter	View your active networks			
Change adapter settings Change advanced sharing settings	Yeastar5G Private network		Access type: Internet HomeGroup: Ready to create Connections: M Wi-Fi (Yeastar5G)	
	ldentifying	Access t Connect		
	Change your networking settings		Ethernet	
	Set up a broadband, dial-up, or VPN Troubleshoot problems Diagnose and repair network problem			
See also				
HomeGroup				
Infrared Internet Options				
Windows Firewall				

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

Internet Protocol Version 4 (TCP/IPv4) Properties X	Internet Protocol Version 4 (TCP/IPv4) Properties
General Alternate Configuration	General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.	You can get IP settings assigned 192.168.1.20 ts for the appropriate IP settings. 255.255.255.0
Obtain an IP address automatically	Obtain an IP address autor 192.168.1.1
O Use the following IP address:	Use the following IP address:
IP address:	IP address: 192 . 168 . 1 . 20
Subnet mask:	Subnet mask: 255 . 255 . 255 . 0
Default gateway:	Default gateway: 192 . 168 . 1 . 1
Obtain DNS server address automatically	Obtain DNS server address automatically
O Use the following DNS server addresses:	Use the following DNS server addresses:
Preferred DNS server:	Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server:	Alternate DNS server:
Validate settings upon exit Advanced	□ Validate settings upon exit 192.168.1.1
OK	OK Cancel

3. 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.

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

Milesight	
Lusername]
Password]
Login	

English

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

5. After logging in the web GUI, you can view system information and perform configuration of the gateway.

			For your	device security, please cha	inge the default pass	wordl		
Status		Overview	Cellular Networ	k WLAN	VPN	Routing Host	t List	A Help
Network	۰.	GPS						Show the model name of router.
System	•	System Information			m Status		Î	Serial Number Show the serial number of router.
Industrial	•	Model Serial Number	UF51-501EU 6901B1901925	Local Uptim		2021-07-28 10:44:44 Wee 1days, 13:57:19	dnesday	Firmware Version Show the current firmware version of router.
Maintenance	×	Firmware Version Hardware Version	76.2.0.2 V1.0	CPU I	.oad (Available/Capacity)	7% 215MB/512MB(41.99%)		Hardware Version Show the current hardware version of router.
∖ PP	•			Flash	(Available/Capacity)	2911MB/4096MB(71.07%)	Local Time
		Cellular 🔍 Link in u	ise	WAN				Show the current local time of system.
		Status	Ready, 5G NR, YI	Status		Online		Uptime Show the information on how
		IPv4	10.2.25.72/28	IPv4		192.168.22.213/24		long the router has been running.
		IPv6	fe80::7cf3:90ff:fe33:6	151/64 IPv6		fe80::26e1:24ff.fef1:e38d/		CPU Load
		Connection Duration	0 days, 23:05:19	MAC		24:e1:24:f1: Manual Refr	esh 🛩 Refresh	Show the current CPU utilization of the router.

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS		
System Informat	tion					System	n Status		
Model		ι	JF51-501EU			Local T	ime	2021-07-22 13:27:27 Thursd	day
Serial Number		6	901B1901925			Uptime		5days, 23:14:12	
Firmware Version		7	'6.2.0.2-a5			CPU Lo	ad	4%	
Hardware Version		١	/1.0			RAM (A	wailable/Capacity)	204MB/512MB(39.84%)	
						Flash (/	Available/Capacity)	2911MB/4096MB(71.07%)	
Cellular 🕒 Link	in use					WAN			
Status		F	Ready, 5G NR, Yil			Status		Online	
IPv4			0.2.25.72/28			IPv4		192.168.22.213/24	
IPv6		f	e80::7446:73ff.fe43:36	4d/64		IPv6		fe80::26e1:24ff:fef1:e38d/64	
Connection Duration	on	1	days, 18:22:59			MAC		24:e1:24:f1:e3:8d	
Data Usage Month	hly	3	31.1 MiB			Connec	tion Duration	1 days, 20:35:54	
WLAN-2.4G						WLAN-	5G		
Status		c	Connected			Status		Running	
Mode		C	Client			Mode		AP	
SSID		N	/lilesight_HW			SSID		Router_F1E390_5G	
						Connec	ted Clients	0	

Figure 3-1-1-1

System Information	
Item	Description
Model	Show the model name of device.
Serial Number	Show the serial number of device.
Firmware Version	Show the currently firmware version of device.
Hardware Version	Show the currently hardware version of device.
	Table 3-1-1-1 System Information

System Status	
Item	Description
Local Time	Show the currently local time of system.
Uptime	Show the information about how long the device has
optime	been running.
CPU Load	Show the current CPU utilization of the device.
RAM (Available/Capacity)	Show the RAM capacity and the available RAM memory.
Flash (Available/Capacity)	Show the Flash capacity and the available Flash memory.

Table 3-1-1-2 System Status

Cellular	
Item	Description
Status	Show the real-time status of the SIM card.

Milesight IoT	
---------------	--

	·
Data Usage Monthly	Show the monthly data usage of currently used SIM card.
Connection Duration	Show the connection duration of the currently-used SIM card.
IPv4/IPv6	Show the IPv4/IPv6 address obtained from the mobile carrier.
Current SIM	Show the SIM card currently used for the data connection.

Table 3-1-1-3 Cellular Status

WAN	
Item	Description
Status	Show the current status of WAN port.
IPv4/IPv6	The IPv4/IPv6 address of WAN port.
MAC	The MAC address of the Ethernet port.
Connection Duration	Show the connection duration of the WAN port.

Table 3-1-1-4 WAN Status

WLAN	
Item	Description
Status	Show the current status of WLAN.
IP	Show the WLAN mode (AP or client).
SSID	Show the SSID of the WLAN AP or client.
Connected Clients	Show the amount of connected devices when using AP mode.

Table 3-1-1-5 WLAN Status

LAN	
Item	Description
IPv4/IPv6	Show the IPv4/IPv6 address of the LAN port.
Connected Devices	The number of devices that connect to the device's LAN.

Table 3-1-1-6 LAN Status

3.1.2 Cellular

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS		
Modem						Netwo	ork		
Status			Ready			Status			Connected
Model			RG500Q-EA			IPv4 A	IPv4 Address		10.2.25.72/28
Version			RG500QEAAAR11A02M4G			IPv4 G	Sateway		10.2.25.73
Signal Level			30asu (-53dBm)			IPv4 D	INS		211.136.17.107
Register Status			Registered (Home net	vork)		IPv6 A	ddress		fe80::7446:73ff.fe43:364d/64
IMEI			866897040051965			IPv6 G	Gateway		
IMSI			460045927703652			IPv6 D	INS		
ICCID			89860439101880723652			Conne	ection Duration		1 days, 18:31:20
ISP			CHINA MOBILE			Data L	Jsage Monthly		
Network Type			5G NR			RX	,		15.6 MIB
PLMN ID			46000			TX			15.6 MIB
LAC			592F			ALL			31.2 MiB
Cell ID			271f848			ALL			51.2 WID
CQI			9						
DL Bandwidth			20 MHz						
UL Bandwidth			20 MHz						
SINR			19						
PCI			170						
RSRP			-83dBm						
RSRQ			-13dB						

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 cellular module firmware version.					
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 5G NR, LTE, 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.					
CQI	Show the Channel Quality Indicator of the cellular network.					
DL Bandwidth	Show the DL bandwidth of the cellular network.					
UL Bandwidth	Show the UL bandwidth of the cellular network.					
SINR	Show the Signal Interference + Noise Ratio of the cellular network.					
PCI	Show the physical-layer cell identity of the cellular network.					
RSRP	Show the Reference Signal Received Power of the cellular network.					
RSRQ	Show the Reference Quality Received Power of the cellular network.					
ECGI	Show the E-UTRAN Cell Global Identifier of the cellular network.					
EARFCN	Show the E-UTRA Absolute Radio Frequency Channel Number.					

ENODEB ID	Show the eNodeB ID of the cellular network.					
Table 3-1-2-1 Modem Information						
Network	Network					
Item	Description					
Status	Show the connection status of cellular network.					
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network.					
IPv4/IPv6 Gateway	Show the IPv4/IPv6 gateway and netmask of cellular network.					
IPv4/IPv6 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

Data Usage Monthly					
Item	Description				
RX	Show monthly downlink data usage.				
ТХ	Show monthly uplink data usage.				
ALL	Show all monthly data usage.				

Table 3-1-2-3 Data Usage Information

3.1.3 Network

On this page you can check the WAN and LAN status of the device.

WAN-IPv4							
Port	Status	Туре	IP	Netmask	Gateway	DNS	Connection Duration
WAN	up	Static	192.168.23.187	255.255.255.0	192.1 <mark>68.23.1</mark>	192.168.1.1	10m 58s
WAN-IPv6							
Port	Status	Туре	IP	Prefix-length	Gateway	DNS	Connection Duration
WAN	up	Static	fe80::26e1:24ff:fef0:3b7 a	64		21	10m 58s



WAN Status	WAN Status					
Item	Description					
Port	Show the name of WAN port.					
Status	Show the status of WAN port. "Up" refers to a status that WAN is enabled and Ethernet cable is connected. "Down" means Ethernet cable is disconnected or WAN function is disabled.					
Туре	Show the dial-up connection type of WAN port.					
IP Address	Show the IPv4 or IPv6 address of WAN port.					
Netmask	Show the IPv4 netmask of WAN port.					
Prefix-length	Show the IPv6 Prefix-length of WAN port.					
Gateway	Show the gateway of WAN port.					

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

Table 3-1-3-1 WAN Status

Bridge				
Name	STP	IPv4	IPv6	Members
Bridge0	Enabled	192.168.1.1/24	2004::1/64	eth1,WLAN-2.4G,WLAN-5G



Bridge					
ltem	Description				
Name	Show the name of the bridge interface.				
STP	Show if STP is enabled.				
IPv4/IPv6	Show the IPv4/IPv6 address and netmask of the bridge interface.				
Members	Show the members of the bridge interface.				

Table 3-1-3-2 Bridge 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	Routing	Host List	GPS	
WLAN Status								
Name	Status	Туре	SSID		IPv4 Addres	55	IPv6 Address	
WLAN-2.4G	Running	AP	UF51-2.4G		192.168.1.1/	24	-	
WLAN-5G	Running	AP	UF51_5G		192.168.1.1/	24		
Associated S	tations							
\$5	GID	MAC Addres	55	IPv4 Address		IPv6 Address	Connection Durati	on

Figure 3-1-4-1

WLAN Status					
Item	Description				
WLAN Status					
Name	Show the name of the Wi-Fi interface .				
Status	Show the status of the Wi-Fi interface.				
Туре	Show the Wi-Fi interface type (AP or client).				
SSID	Show the SSID of AP device.				
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of AP device.				

Associated Stations	
SSID	Show the SSID of AP device.
MAC Address	Show the MAC address of the client which connected to the device when the interface type is AP. Show the MAC address of the AP which the device connected to when the interface type is Client.
IPv4/IPv6 Address	Show the IPv4/IPv6 address of the client which connected to the device when the interface type is AP. Show the IPv4/IPv6 address of the AP which the device connected to when the interface type is Client.
Connection Duration	Show the connection duration between client device and device when the interface type is AP. Show the connection duration between device and the AP when the interface type is Client.

Table 3-1-4-1 WLAN Status

3.1.5 VPN

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List
Clients						
	Name	Status		Local IP		Remote IP
Server						
	Name				Status	
	OpenVPN Server				Disabled	
	Ipsec Sei	ver			Disabled	
Connected List						
	Server Type		Client IP			Duration

Figure 3-1-5-1

VPN Status					
Item	Description				
Clients					
Name	Show the name of the enabled VPN clients.				
Status	Show the status of client. "Connected" refers to a status that client is connected to the server. "Disconnected" means client is disconnected to the server.				
Local IP	Show the local IP address of the tunnel.				

Remote IP	Show the real remote IP address of the tunnel.
Server	
Name	Show the name of the enabled VPN Server.
Status	Show the status of Server.
Connected List	
Server Type	Show the type of the server.
Client IP	Show the IP address of the client which connected to the server.
Duration	Show the information about how long the client has been connected to this server when the server is enabled. Once the server is disabled or connection is disconnected, the duration will stop counting.

Table 3-1-5-1 VPN Status

3.1.6 Routing

You can check routing status on this page, including the routing table and ARP cache.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS			
Routing Table										
	Des	stination	ŀ	letmask/Prefix L	ength	Gateway		Interface	Me	ric
	0	0.0.0.0		0.0.0.0		192.168.22.1		WAN	1	
	12	27.0.0.0		255.0.0.0				Loopback	-	
	192	2.168.1.0		255.255.255.	0			Bridge0	17	
	192.	.168.22.0		255.255.255.	0	÷		WAN	· -	
		11 11 11		0	2	408:844b:1a20:fc0:1d0a: 5a	9a67:4a3:3b	Cellular 0	45	
		::1		128		-		Loopback		
	2001:486	60:4860::8888		128	2	408:844b:1a20:fc0:1d0a: 5a	9a67:4a3:3b	Cellular 0	24	
	2	2004::		64				Bridge0		
	240	0:3200::1		128	2	408:844b:1a20:fc0:1d0a: 5a	9a67:4a3:3b	Cellular 0	1	
	2408:84	14b:1a20:fc0::		64				Cellular 0	5	
ARP Cache										
		IP				MAC			Interface	
	192.	168. <mark>1.1</mark> 13			0	:8:5b:76:b2:56:1f			Bridge0	
	192.1	168.22.127			2	24:e1:24:f0:47:e1			WAN	
	192.	.168.22.1			5	ic:dd:70:6c:46:3d			WAN	
	192.168.22.6					f4:b5:49:f1:1b:1f			WAN	
	192.	168.23.77			2	24:4b:fe:8d:95:ab			WAN	Manual Refresh 🗸 🛛 R

Figure 3-1-6-1

Item	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix	Show the netmask or prefix length of destination host or
Length	destination network.
Gateway	Show the IP address of the gateway.

Interface Show the outbound interface of the route.					
Metric	Show the metric of the route.				
ARP Cache					
IP	Show the IP address of ARP pool.				
MAC	Show the IP address's corresponding MAC address.				
Interface	Show the binding interface of ARP.				

Table 3-1-6-1 Routing Information

3.1.7 Host List

You can view the host information on this page.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS	
DHCP Leases								
		IP			N	AC/DUID		Lease Remaining Time
	192.168.1.113				c8:5	0:76:b2:56:1f		23h 07m 24s
	20	04::20 <mark>0</mark>			00:01:00:01:27:0	c:cf:61:c8:5b:76:b2:5	56:1f	23h 09m 22s
MAC Binding								
			IP					MAC/DUID

Figure 3-1-7-1

Host List					
Item	Description				
DHCP Leases					
IP Address	Show IP address of DHCP client				
MAC/DUID	Show MAC address of DHCPv4 client or DUID of DHCPv6 client.				
Lease Time Remaining	Show the remaining lease time of DHCP client.				
MAC Binding					
IP	Show the IP address set in the Static IP list of DHCP service.				
MAC/DUID	Show the MAC address or DUID set in the Static IP list of DHCP service.				

Table 3-1-7-1 Host List Description

3.1.8 GPS

When GPS function is enabled and the GPS information is obtained successfully, you can view the latest GPS information including GPS Time, Latitude, Longitude and Speed on this page.

GPS Status		
Status	Weak Signal	
Time for Locating	2	
Satellites In Use	-	
Satellites In View	<u>1</u> 2	
Latitude	-	
Longitude	7 5	
Altitude	2	
Speed	÷.	

Figure 3-1-8-1

GPS Status				
ltem	Description			
Status	Show the status of GPS.			
Time for Locating	Show the time for locating.			
Satellites In Use	Show the quantity of satellites in use.			
Satellites In View	Show the quantity of satellites in view.			
Latitude	Show the Latitude of the location.			
Longitude	Show the Longitude of the location.			
Altitude	Show the Altitude of the location.			
Speed	Show the speed of movement.			
•				

Table 3-1-8-1 GPS Status Description

3.2 Network

3.2.1 Interface

3.2.1.1 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its own ping rules by default. UF51 will follow the priority to choose the next available interface to access the internet, make sure you have enable the full interface that you need to use here. If priority 1 can only use IPv4, UF51 will select a second link which IPv6 works as main IPv6 link and vice versa.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Link Priority							
Priority	Enable Rule	Link in use	Interface	Connec	tion Type	IP	Operation
1		٠	Cellular	DI	HCP	2	
2		•	WAN	S	tatic	192.168.22.69	
Settings							
Revert Interval		30		s			
Emergency Reboo	ot						
Save							

Figure 3-2-1-1

Link Failover					
Item	Description				
Link Priority					
Priority	Display the priority of each interface, you can modify it by the operation's up and down button.				
Enable Rule	If enabled, the device will choose this interface into its switching rule. For the Cellular interface, if it's not enabled here, the interface will be disabled as well.				
Link In Use	Mark whether this interface is in use with green icon.				
Interface	Display the name of the interface.				
Connection type	Display how to obtain the IP address in this interface, like static IP or DHCP.				
IP	Display the IP address of the interface.				
Operation	You can change the priority of the rules and configure the ping detection rules here.				
Settings					
Revert Interval	Specify the number of seconds to waiting for switching to the link with higher priority, 0 means to disable the function.				
Emergency Reboot	Enable to reboot the device if no link is available.				

Table 3-2-1-1 Link Failover Parameters

Enable			
IPv4 Primary Server	8.8.8.8		
IPv4 Secondary Server	114.114.114		
IPv6 Primary Server	2001:4860:4860::8888		
IPv6 Secondary Server	2400:3200::1		
Interval	300	s	
Retry Interval	5	s	
Timeout	3	s	
Max Ping Retries	3		

Figure 3-2-1-2

Ping Detection						
Item	Description					
Enable	If enabled, the device will periodically detect the connection status of the link.					
IPv4/IPv6 Primary Server	The device will send ICMP packet to the IPv4/IPv6 address or hostname to determine whether the Internet connection is still available or not.					
IPv4/IPv6 Secondary Server	The device will try to ping the secondary server if primary server is not available.					
Interval	Time interval (in seconds) between two Pings.					
Retry Interval	Set the ping retry interval. When ping failed, the device will ping again in every retry interval.					
Timeout	The maximum amount of time the device will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.					
Max Ping Retries	The retry times of the device sending ping request until determining that the connection has failed.					

Table 3-2-1-2 Ping Detection Parameters

3.2.1.2 Cellular

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN
Cellular Settings					
Protocol Type		IPv4		~	
APN					
Username					
Password					
PIN Code					
Access Number					
Authentication Type		Auto		~	
Network Type		Auto		~	
SMS Center					
Enable NAT					
Roaming					
Data Limit		0		MB	
Billing Day		Day 1	✓ of The Mont	h	
Connection Setting					
Connection Mode		Always O	nline	~	
Re-dial Interval(s)		5			

Figure 3-2-1-3

Cellular Settings						
Item	Description					
Protocol	Select from "IPv4", "IPv6" and "IPv4/IPv6".					
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.					
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.					
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.					
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".					

Network Type	Select from "Auto", "5G NSA", "5G SA", "4G Only" and "3G Only". Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Roaming	Enable or disable roaming.
Data Limit	When you reach the specified data usage limit, the data connection of currently used SIM card will be disabled. 0 means to disable the function.
Billing Day	Choose the billing day of the SIM card, the device will reset the data used to 0.

Table 3-2-1-3 (Cellular	Parameters
-----------------	----------	------------

Connection Setting		
Connection Mode	Connect on Demand	
Re-dial Interval(s)	5	
Max Idle Time(s)	60	
Triggered by Call	Ø	
Call Group	•	
Triggered by SMS	×.	
SMS Group	•	
SMS Text		
Triggered by IO		



Connection Setting						
Item	Description					
Connection Mode	Select from "Always Online" and "Connect on Demand".					
Re-dial Interval(s)	Set the interval to dial into ISP when it lost connection, the default value is 5s.					
Max Idle Times	Set the maximum duration of device when current link is under idle status. Range: 10-3600					
Triggered by Call	The device 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 > Phone&SMS > Phone" to set up phone group.					
Triggered by SMS	The device will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.					

SMS Group	Select an SMS group for trigger. Go to "System > Phone&SMS > SMS" to set up SMS group.
SMS Text	Fill in the SMS content for trigger.
Triggered by IO	The device will switch from offline mode to cellular network mode automatically when the DI status is changed. Go to "Industrial > I/O > DI" to configure trigger condition.

Table 3-2-1-4 Cellular Parameters

Related Topics

<u>Cellular Network Connection</u> <u>Phone Group</u> <u>DI Setting</u>

3.2.1.3 Port

This section describes how to configure the Ethernet port parameters.

UF51 supports 2 Gigabit Ethernet ports.

	Cellular	Port		WAN	Bridge		WLAN	Sw	itch	Loopback
Port Setting										
	Port	Statu	s	Prope	erty	Spee	d	Duple	ex	
1	LAN1/WAN	up	~	wan	~	auto	~	auto	~	
	LAN2	up	~	lan	~	auto	~	auto	~	

Figure 3-2-1-5

Port Setting	
Item	Description
Port	Users can define the Ethernet ports according to their needs.
Status	Set the status of Ethernet port; select "up" to enable and "down" to disable.
Property	Show the Ethernet port's type, as a WAN port or a LAN port.
Speed	Ethernet port speed is fixed as "auto".
Duplex	Ethernet port mode is fixed as "auto".

Table 3-2-1-5 Port Parameters

3.2.1.4 WAN

WAN 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 IPv4 address automatically.

- PPPoE: configure Ethernet WAN interface as PPPoE Client.

- **DHCPv6 Client**: configure Ethernet WAN interface as DHCP Client to obtain IPv6 address automatically.

- **PPPoE v6**: configure Ethernet WAN interface as PPPoEv6 Client.

- **Dual-Stack Lite**: use IPv4-in-IPv6 tunneling to send terminal device's IPv4 packet through a tunnel on the IPv6 access network to the ISP.

Link	Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback			
WAN	Settings										
-	WAN_1										
	Enable										
	Port			LAI	LAN1/WAN						
	Connection Type			DHCP Client V							
	MTU			1500							
	Use Peer DNS										
	IPv4 Primary DNS			114	.114.114.114						
	IPv4 Secondary DNS				8.8.8.8						
	Enable NAT										
Sa	ve & Apply										

Figure 3-2-1-6

WAN Basic Setting					
Item	Description	Default			
Enable	Enable WAN function.	Enable			
Port	The port that is currently set as WAN port.	LAN1/WAN			
Connection Type	Select from "Static IP", "DHCP Client", "DHCPv6 Client", "PPPoE", "DHCPv6 Client", "PPPoEv6", and "Dual-Stack Lite".	Static IP			
MTU	Set the maximum transmission unit.	1500			
IPv4 Primary DNS Server	Set the primary IPv4 DNS server.	114.114.114. 114			
IPv4 Secondary DNS Server	Set the secondary IPv4 DNS server.	8.8.8.8			
IPv6 Primary DNS Server	Set the primary IPv6 DNS server.	2001:4860:4 860:8888			
IPv6 Secondary DNS Server	Set the secondary IPv6 DNS server.				
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable			

Table 3-2-1-6 WAN Parameters

1. Static IP Configuration

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

Enable			
Port	LAN1/WAN		
Connection Type	Static IP	~	
IPv4 Address	192.168.22.69		J
Netmask	255.255.255.0		
IPv4 Gateway	192.168.22.1		
IPv6 Address	fe80::26e1:24ff.fe20:2147		
Prefix Length	64		
IPv6 Gateway			
МТU	1500		
IPv4 Primary DNS	114.114.114.114		
IPv4 Secondary DNS	8.8.8.8		
IPv6 Primary DNS	240C::6666		
IPv6 Secondary DNS			
Enable NAT			
Multiple IP Address			
	IP Address		

Figure 3-2-1-7

Static IP	Static IP					
ltem	Description	Default				
IPv4 Address	Set the IPv4 address of the WAN port.	192.168.0.1				
Netmask	Set the Netmask for WAN port.	255.255.255.0				
IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	192.168.0.2				
IPv6 Address	Set the IPv6 address which can access Internet.	Generated from Mac address				
Prefix-length	Set the IPv6 prefix length to identify how many bits of a Global Unicast IPv6 address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.	64				
IPv6 Gateway	Set the gateway for WAN port's IPv6 address. E.g.2001:DB8:ACAD:4::2.					
Multiple IP Address	Set the multiple IP addresses for WAN port.	Null				

Table 3-2-1-7 Static Parameters

2. DHCP Client/DHCPv6 Client

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

Enable	
Port	LAN1/WAN
Connection Type	DHCP Client 🗸
MTU	1500
Use Peer DNS	
IPv4 Primary DNS	114.114.114.114
IPv4 Secondary DNS	8.8.8.8
Enable NAT	
Figu	re 3-2-1-8
Enable	
Port	LAN1/WAN
Connection Type	DHCPv6 Client 🗸
Request IPv6-address	None 🗸
Request IPv6-prefix of length	0-64
MTU	1500
IPv6 Primary DNS	240C::6666
IPv6 Secondary DNS	
Enable NAT	



DHCP Client				
Item	Description			
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.			
DHCPv6 Client				
Request IPv6-address	Choose the ways to obtain the IPv6 address from the DHCP Server. Select from try, force, none. Try: The DHCP Server will assign specific address in priority. Force: The DHCP Server assigns specific address only. None: The DHCP Server will randomly assign address.The specific address is relevant to the prefix length of IPv6 address you set.			
Request prefix length of IPv6	Set the prefix length of IPv6 address which device is expected to obtain from DHCP Server.			

Table 3-2-1-8 DHCP Client Parameters

3. PPPoE/PPPoEv6

PPPoE refers to a point to point protocol over Ethernet. With PPPoE, remote access devices can get control of each user. If type as PPPoEv6, UF51 can get both IPv4 and IPv6 address.

Enable	
Port	LAN1/WAN
Connection Type	PPPoE 🗸
Username	
Password	
Link Detection Interval(s)	60
Max Retries	0
мти	1500
Use Peer DNS	
IPv4 Primary DNS	114.114.114.114
IPv4 Secondary DNS	8.8.8.8
Enable NAT	



Enable				
Port	LAN1/WAN			
Connection Type	PPPoEv6			
Username				
Password				
Link Detection Interval(s)	60			
Max Retries	0			
мти	1500			
Use Peer DNS				
IPv4 Primary DNS	114.114.114.114			
IPv4 Secondary DNS	8.8.8.8			
IPv6 Primary DNS	240C::6666			
IPv6 Secondary DNS				
Enable NAT				



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

Table 3-2-1-9 PPOE Parameters

4. Dual-Stack Lite

Dual-Stack Lite (DS-Lite) uses IPv4-in-IPv6 tunneling to send a subscriber's IPv4 packet through a tunnel on the IPv6 access network to the ISP. The IPv6 packet is decapsulated to recover the

subscriber's IPv4 packet and is then sent to the Internet after NAT address and port translation and other LSN related processing. The response packets traverse through the same path to the subscriber.

Enable	
Port	LAN1/WAN
Connection Type	Dual-Stack Lite 🗸
IPv6 Gateway	
DS-Lite AFTR Address	
Local IPv6 Address	
MTU	1500
IPv4 Primary DNS	114.114.114.114
IPv4 Secondary DNS	8.8.8.8
IPv6 Primary DNS	240C::6666
IPv6 Secondary DNS	
Enable NAT	

Figure 3-2-1-12

Dual-Stack Lite				
Item	Description			
IPv6 Gateway	Set the gateway for WAN port's IPv6 address.			
DS-Lite AFTR Address	Set the DS-Lite AFTR server address.			
Local IPv6 Address	Set the WAN port IPv6 address which use the same subnet as IPv6 gateway.			

Table 3-2-1-10 Dual-Stack Lite Parameters

Related Configuration Example

Ethernet WAN Connection

3.2.1.5 Bridge

Bridge setting is used for managing local area network devices which are connected to LAN ports of the UF51, allowing each of them to access the Internet.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Bridge Setting							
Name	Bri	dge0					
STP	~						
IP Address	192	2. <mark>1</mark> 68.1. <mark>1</mark>					
Netmask	255	5.255.255.0					
IPv6 Address	200	04::1/64	/				
MTU	150	00					
Multiple IP Address							
	IP Add	ress		Netmask		Operation	
						H	

Figure 3-2-1-13

Bridge		
Item	Description	Default
Name	Show the name of bridge. "Bridge0" is set by default and cannot be changed.	Bridge0
STP	Enable/disable STP.	Disable
IP Address	Set the IP address for bridge.	192.168.1.1
Netmask	Set the Netmask for bridge.	255.255.255. 0
IPv6 Address	Set the IPv6 address for bridge.	2004::1/64
MTU	Set the maximum transmission unit. Range: 68-1500.	1500
Multiple IP Address	Set the multiple IP addresses for bridge.	Null

Table 3-2-1-11 Bridge Settings

3.2.1.6 WLAN

This section explains how to set the related parameters for Wi-Fi network. UF51 supports both 2.4 GHz and 5 GHz Wi-Fi and it can work as AP or client mode at the same time.

Milesight M

WLAN1-2.4G	
Enable	
Work Mode	AP
BSSID	24:e1:24:f1:e3:8f
Radio Type	802.11n(2.4GHz)
Channel	Auto
Bandwidth	20MHz
SSID	
Encryption Mode	WPA-PSK/WPA2-PSK
Cipher	Auto
Кеу	
Group Rekey Time	3600
SSID Broadcast	
AP Isolation	
Guest Mode	
MAC Filtering	
Туре	Disabled



WLAN	
ltem	Description
Enable	Enable/disable WLAN.
Work Mode	The options are "Client" or "AP".
SSID	Fill in the SSID of the access point.
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can be filled to joint the network.
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 in the key of access point.

Client Mode	
Scan	Click "Scan" button to search the nearby access point.
SSID	Show SSID.
Channel	Show wireless channel.
Signal	Show wireless signal.
BSSID	Show the MAC address of the access point.
Cipher	Show the cipher 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.
AP Mode	
Radio Type	Select Radio type. 2.4G radio types can only be selected in WLAN 1 and 5G radio types can only be selected in WLAN2.
Channel	Select wireless channel. The options are "Auto", "1", "2""11".
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
Group Rekey Time	Rekeytime is when you select PSK encryption mode.
SSID Broadcast	When SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.
AP Isolation	When AP isolation is enabled, all users that access to the AP are isolated without communication with each other.
Guest Mode	The internal network is not allowed to visit if the guest mode is enabled.
IP Setting	
Protocol	Set the IP address in wireless network.
IP Address	Set the IP address in wireless network.
Netmask	Set the netmask in wireless network.
Gateway	Set the gateway in wireless network.

Table 3-2-1-12 WLAN Parameters

MAC Filtering			
Туре	Allow and Block the Rest		
	MAC Address	Description	Operation
			Ð
Save & Apply			

Figure 3-2-1-15

MAC Filtering	
Item	Description
Туре	In this mode, you can choose the rule according to your security

	policy, which is 'Allow and Block the Rest' and 'Block and Allow the Rest', the default value is Disabled.
Allow and Block the Rest	Only the listed MAC addresses are allowed to connect to the device's wireless access point.
Block and Allow the Rest	The listed MAC addresses are not allowed to connect to the device's wireless access point.

Table 3-2-1-13 MAC Filtering Parameters

Related Topic

Wi-Fi Application Example

3.2.1.7 Switch

VLAN is a kind of new data exchange technology that realizes virtual work groups by logically dividing the LAN device into network segments.

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback	
LAN Settings								
Name		VLAN ID		IP Address	Netma	sk	MTU	Operation
								8
VLAN Settings								
VLAN	ID	LAN 1		L	AN 2		СРИ	Operation
1	U	ntagged	~	Untagged	~	Tagged	~	×
								•

Figure 3-2-1-16

Switch	
Item	Description
LAN Settings	
Name	Set interface name of VLAN.
VLAN ID	Select VLAN ID of the interface.
IP Address	Set IP address of LAN port.
Netmask	Set Netmask of LAN port.
MTU	Set the maximum transmission unit of LAN port. Range: 68-1500.
VLAN Settings	
VLAN ID	Set the label ID of the VLAN. Range: 1-4094.
LAN 1/2	Make the VLAN bind with the corresponding ports and select status
LAN 1/2	from "Tagged", "Untagged" and "Close" for Ethernet frame on trunk link.
CPU	Control communication between VLAN and other networks.

Table 3-2-1-14 VLAN Trunk Parameters

3.2.1.8 Loopback

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

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Loopback Address							
IP Address		127.0.0.1					
Netmask		255.0.0.0					
Multiple IP Address	ses						
	IP Addres	s			Netmask		Operation
							•
Save							

Figure 3-2-1-17

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

Table 3-2-1-15 Loopback Parameters

3.2.2 DHCP

DHCP adopts Client/Server communication mode. The Client sends configuration request to the Server which feeds back corresponding configuration information and distributes IP address to the Client so as to achieve the dynamic configuration of IP address and other information.

3.2.2.1 DHCP Server/DHCPv6 Server

UF51 can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. UF51 only supports stateful DHCPv6 when working as DHCPv6 server.

CP Server	DHCPv6 Server	DHCP Relay		
DHCP Server_1				
Enable				
Interface		Bridge0 🗸		
Start Address		192.168.1.113		
End Address		192.168.1.126		
Netmask		255.255.255.0		
Lease Time(Min)		1440		
Primary DNS Server	<u>f</u>	8.8.8.8		
Secondary DNS Ser	rver	114.114.114		
Windows Name Ser	ver			
Static IP				
	MAC Add	ress	IP Address	Operatio
				8



CP Server	DHCPv6 Server	DHCP Relay		
DHCPv6 Server_	_1			
Enable		۵		
Interface		Bridge0 🗸		
Start Address		2004:0:0:0:0:0:0:100		
End Address		2004:0:0:0:0:0:0:200		
Prefix Length		64		
Lease Time(Min))	1440		
Primary DNS Ser	rver	2001:D0B0:3000:3001::1		
Secondary DNS	Server	2001:4860:4860::8888		
Static IP				
	DUID		IPv6 Address	Operati
				+



DHCP Server/DHCPv6 Server					
Item	Description	Default			
Enable	Enable or disable DHCP server.	Enable			
Interface	Select interface.	Bridge0			
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.2			
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.2 54			
Netmask	Define the subnet mask of IPv4 address obtained by DHCP clients from DHCP server.	255.255.255 .0			

Prefix Length	Set the IPv6 prefix length of IPv6 address obtained by DHCP clients from DHCP server.	64
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	192.168.1.1
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
DUID	Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID 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 3-2-2-1 DHCP Server Parameters

3.2.2.2 DHCP Relay

UF51 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

Figure 3-2-2-2

DHCP Relay	
Item	Description
Enable	Enable or disable DHCP relay.
DHCP Server	Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".

Table 3-2-2-2 DHCP Relay Parameters

3.2.3 Firewall

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

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 device operate in a safe environment and host in local area network.

3.2.3.1 Security

Security	ACL	Port Mapping	DMZ	MAC Binding Custom Rules
Prevent Attack				
DoS/DDoS Prot	ection			
Access Servic	e Control			
Serv	ice	Port	Local	Remote
нтт	ſP	80	×	×
нтт	PS	443	Ø	×
TELN	IET	23	×	×
SSI	н	22		Ø
FTI	Ρ	21		ø
Website Block	ing			
URL Blocking		http://		
Keyword Blockir	ng			

Figure 3-2-3-1

ltem	Description	Default
Prevent Attack		
DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack.	Disable
Access Service Control		
Port	Set port number of the services. Range: 1-65535.	
Local	Access the device locally.	Enable
Remote	Access the device remotely.	Disable
HTTP	Users can log in the device locally via HTTP to	80

	access and control it through Web after the option is checked.	
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 after the option is checked.	23
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22
FTP	Users can log in the device locally and remotely via FTP after the option is checked.	21
Website Blocking		
URL Blocking	Enter the HTTP address which you want to block.	
Keyword Blocking	You can block specific website by entering keyword maximum number of character allowed is 64.	The

Table 3-2-3-1 Security Parameters

3.2.3.2 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 device receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

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

Security	ACL	Port Mappir	ng DMZ	MAC Binding	Custom R	ules SP	
ACL Setting	blicy	Accept	•				
Access Contro	ol List						
ID	Action	Protocol	Source IP	Destination IP	More Detail	Description	Operation 0
							8
Interface List							
	Interface		In /	ACL	Out A	CL.	Operation
							8
Save							

Figure 3-2-3-2

Iter	n	Description
gn ne	micoigne	

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

Table 3-2-3-2 ACL Parameters

Related Configuration Example

Access Control Application Example

3.2.3.3 Port Mapping

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

Security	ACL	Port Mapping	DMZ	MAC Binding	I	Custom Rules	SPI	
Port Mapping								
Sour	ce IP	Source Port	Destination IP	Destination Port	Protocol	Description		Operation
								Ŧ
	_							

Click 🛨 to add a new port mapping rules.

Figure 3-2-3-3

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 3-2-3-3 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.2.3.4 DMZ

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

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
DMZ						
Enable DMZ Host						
Source Address						
Save						

Figure 3-2-3-4

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 3-2-3-4 DMZ Parameters

3.2.3.5 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	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
MAC Binding	List					
	MAC		IP		Description	Operation
						•
Save						

Figure 3-2-3-5

MAC Binding List				
Item	Description			
MAC Address	Set the binding MAC address.			
IP Address	Set the binding IP address.			
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.			
	Table 2.2.2.5 MAC Pinding Decomptore			

Table 3-2-3-5 MAC Binding Parameters

3.2.3.6 Custom Rules

In this page, you can configure your own custom firewall iptables rules.

Security	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
Custom Rules	s					
		Rule			Description	Operation
	Eg: -t filter -I INPU	JT -s 192.168.3.240 -j DR(OP			×
						H



Custom Rules				
ltem	Description			
	Specify an iptables rule like the example shows.			
Rule	Tips: You must reboot the device to take effect after modifying or			
	deleting the iptables rules.			
Description	Enter the description of the rule.			

Table 3-2-3-6 Custom Rules Parameters

3.2.3.7 SPI

Secu	rity	ACL	Port Mapping	DMZ	MAC Binding	Custom Rules	SPI
SPI Fi	rewall						
	Enable						
	Filter Pr	оху					
	Filter Co	pokies					
	Filter Ac	tivex					
	Filter Ja	iva Applets					
	Filter Mi	ulticast					
	Filter ID	ENT(port 113)					
9	Block W	/an SNMP access					
9	Filter W	AN NAT Redirecti	on				
9	Block Ar	nonymous Wan R	equest				
	Save						

Figure 3-2-3-7

SPI Firewall	
Item	Description
Enable	Enable/disable SPI firewall.
Filter Proxy	Blocks HTTP requests containing the "Host": string.
Filter Cookies	Identifies HTTP requests that contain "Cookie": String and mangle the cookie. Attempts to stop cookies from being used.
Filter ActiveX	Blocks HTTP requests of the URL that ends in ".ocx" or ".cab".
Filter Java Applets	Blocks HTTP requests of the URL that ends in ".js" or ".class".
Filter Multicast	Prevent multicast packets from reaching the LAN.
Filter IDENT(port 113)	Prevent WAN access to Port 113.
Block WAN SNMP access	Block SNMP requests from the WAN.
Filter WAN NAT Redirection	Prevent hosts on LAN from using WAN address of device to connect servers on the LAN (which have been configured using port redirection).
Block Anonymous WAN Requests	Stop the device from responding to "pings" from the WAN.

Table 3-2-3-7 SPI Parameters

3.2.4 QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS is engineered to provide different priority for different applications, users, data flows, or to guarantee a certain level of performance to a data flow.

Status	Î.	QoS(Download)	QoS(Upload)						
Network	-	Download Bandwidth							
Interface		Enable	8						
DHCP		Default Category Download Bandwidth	0	• kbits	s				
Firewall		Capacity							
QoS		Service Category							
VPN		Name		Percent(%)	Max BW(F	(bps)	Min BW(kbps)	Operation
IP Passthrough									•
Routing		Service Category Rul	es						
VRRP		Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Category	Operation
DDNS									Đ
System	•	Save							

Figure 3-2-4-1

QoS				
Item	Description			
Download/Upload				
Enable	Enable or disable QoS.			
Default Category	Select the default category from Service Category list.			
Download/Upload	The download/upload bandwidth capacity of the network that the			
Bandwidth Capacity	device is connected with, in kbps. Range: 1-8000000.			
Service Category				
Name	You can use characters such digits, letters and "-".			
Percent (%)	Set percent for the service category. Range: 0-100.			
Max BW(kbps)	The maximum bandwidth that this category is allowed to consume, in kbps. The value should be less than the "Download/Upload Bandwidth Capacity" when the traffic is blocked.			
Min BW(kbps)	The minimum bandwidth that can be guaranteed for the category, in kbps.The value should be less than the "MAX BW" value.			
Service Category Rule	S			
Item	Description			
Name	Give the rule a descriptive name.			
Source IP	Source address of flow control (leaving it blank means any).			
Source Port	Source port of flow control. Range: 0-65535 (leaving it blank means any).			

Destination IP	Destination address of flow control (leaving it blank means any).
Destination Port	Destination port of flow control. Range: 0-65535 (leaving it blank means any).
Protocol	Select protocol from "ANY", "TCP", "UDP", "ICMP", and "GRE".
Service Category	Set service category for the rule.
	Table 3-2-4-1 OoS (Download/Unload) Parameters

Table 3-2-4-1 QoS (Download/Upload) Parameters

Related Configuration Example

QoS Application Example

3.2.5 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. UF51 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.2.5.1 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 router.

Status	DMVPN IPsec	Server IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
Network	DMVPN Settings							
Interface	Enable Hub Address							
DHCP	Local IP Address							
Firewall	GRE HUB IP Address							
QoS	GRE Local IP Address							
VPN	GRE Mask	255.2	255.255.0					
IP Passthrough	GRE Key							
Routing	Negotiation Mode Authentication Algorithm	Main		v v				
VRRP	Encryption Algorithm	MD5		*				
DDNS	DH Group	MOE	DP768-1	Ψ.				
System	Key							
System	Local ID Type	Defa	ault	Ŧ				
Industrial	IKE Life Time(s)	1080	0					
	SAAlgorithm		-MD5	*				
Maintenance	PFS Group	NUL		*				
APP 🕨	Life Time(s)	3600						
	DPD Time Interval(s)	30						
	DPD Timeout(s)	150						
	Cisco Secret							
	NHRP Holdtime(s)	7200						
	Comp.							
	Save							

Figure 3-2-5-1

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".				
DH Group	Select from "MODP768_1", "MODP1024_2" and				
ытыбар	"MODP1536_5".				
Кеу	Enter the preshared key.				
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"				
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.				
	Select from "DES_MD5", "DES_SHA1", "3DES_MD5",				
SA Algorithm	"3DES_SHA1", "AES128_MD5", "AES128_SHA1",				
o, () (gontinin	"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 3-2-5-1 DMVPN Parameters

3.2.5.2 IPSec Server

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

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

DMVPN	IPsec Server	IPsec	GRE	L2TP
IPsec Server				
Enable				
IPsec Mode			Tunnel	~
IPsec Protocol			ESP	~
Local Subnet			2	
Local Subnet M	ask			
Local ID Type			Default	~
Remote Subnet				
Remote Subnet	Mask			
Remote ID Type	a		Default	~
IKE Parameter				
SA Parameter				
IPsec Advance	d		\sum	
Expert Options				

Figure 3-2-5-2

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

Table 3-2-5-2 IPsec Parameters

Save

IKE Parameter				
IKE Version	IKEv1	٣		
Negotiation Mode	Main	•		
Encryption Algorithm	DES	•		
Authentication Algorithm	MD5	Ŧ		
DH Group	MODP768-1	T		
Local Authentication	PSK	T		
XAUTH				
Lifetime(s)	10800			
XAUTH List				
Ŭ	sername		Password	Operation
				•
PSK List				
	Selector		PSK	Operation
		Figure 3-2-	5-3	

SA Parameter		
SAAlgorithm	DES-MD5	~
PFS Group	NULL	~
Lifetime(s)	3600	
DPD Time Interval(s)	30	
DPD Timeout(s)	150	
IPsec Advanced	\bigtriangledown	
Enable Compression		
VPN Over IPsec Type	NONE	~
Expert Options		



IKE Parameter		
Item	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".	
XAUTH	Enter XAUTH username and password after XAUTH is enabled.	

ł.	Milesight IoT
	-

Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
XAUTH List	
Username	Enter the username used for the xauth authentication.
Password	Enter the password used for the xauth authentication.
PSK List	
Selector	Enter the corresponding identification number for PSK authentication.
PSK	Enter the pre-shared key.
SA Parameter	
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1" , "MODP1024_2" and "MODP1536_5".
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time(s)	Set DPD interval time to detect if the remote side fails.
DPD Timeout(s)	Set DPD timeout. Range: 10-3600.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
VPN Over IPsec Type	Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function.
Expert Options	User can enter some other initialization strings in this field and separate the strings with ";". For example, if more local or remote subnet need to be added, users can add contents here.

Table 3-2-5-3 IPsec Server Parameters

3.2.5.3 IPSec

DM	VPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
IPse	c Settings						
-	IPsec_1						
	Enable			1			
	IPsec Gateway	y Address					
	IPsec Mode			Tunnel	~		
	IPsec Protocol	I		ESP	~		
	Local Subnet						
	Local Subnet	Mask					
	Local ID Type			Default	~		
	Remote Subne	et					
	Remote Subne	et Mask					
	Remote ID Typ	pe		Default	~		
	IKE Paramete	۶r					
	SA Parameter	r					
	IPsec Advance	ed	>]			
	Expert Options	S					
+	IPsec_2						
+	IPsec_3						

Figure 3-2-5-5

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

Table 3-2-5-4 IPsec Parameters

IKE Parameter		
IKE Version	IKEv1	~
Negotiation Mode	Main	~
Encryption Algorithm	AES128	~
Authentication Algorithm	SHA1	~
DH Group	MODP768-1	~
Local Authentication	PSK	~
Local Secrets		
XAUTH		
Username		
Password		
Lifetime(s)	28800	
SA Parameter		
IPsec Advanced		
Enable Compression		
VPN Over IPsec Type	NONE	~
Expert Options		

Figure 3-2-5-6

IKE Parameter	IKE Parameter			
Item	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 pre-shared 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", "3DES_SHA1",			
SA Algorithm	"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.		
Expert Option	User can enter some other initialization strings in this field and separate the strings with ";". For example, if more local or remote subnet need to be added, users can add contents here.		

Table 3-2-5-5 IPsec Parameters

3.2.5.4 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 could be transmitted and encapsulation and decapsulation could be realized at both ends.

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

- GRE tunnel could 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 Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
GRE Settings						
— GRE_1						
Enable						
Remote IP	Address					
Local IP Ac	Idress					
Local Virtua	al IP Address					
Netmask			255.2	55.255.0		
Peer Virtua	I IP Address					
Global Traf	fic Forwarding					
Remote Su	bnet				a) a)	
Remote Ne	etmask					
MTU			1500			
Key			6		ē	
Enable NA	Т		ø			

Figure 3-2-5-7

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

Table 3-2-5-6 GRE Parameters

3.2.5.5 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 Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
L2TP Settings						
- L2TP_1						
Enable						
Remote IF	P Address		58.63.	128.250		
Username	e		user2			
Password		•••••				
Authentica	ation		CHAP)	¥	
Global Tra	affic Forwarding					
Key						
Advanced Settings		\triangleright				

Figure 3-2-5-8

L2TP	
Item	Description
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and
	"MS-CHAPv2".
Global Traffic	All of the data traffic will be sent out via L2TP tunnel after
Forwarding	this function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Кеу	Enter the password of L2TP tunnel.

Table 3-2-5-7 L2TP Parameters

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

Figure 3-2-5-9

Advanced Settings		
Item	Description	
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.	
Peer IP Address	Enter tunnel IP address of L2TP server.	
Enable NAT	Enable NAT traversal function.	
Enable MPPE	Enable MPPE encryption.	

Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 64-1500
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-2-5-8 L2TP Parameters

3.2.5.6 PPTP

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

DMVF	PN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client
PPTP S	Settings						
— Р	PTP_1						
E	nable						
R	Remote IP Add	ress					
U	Isername						
P	assword						
A	uthentication			Auto		¥	
G	Global Traffic F	orwarding					
R	lemote Subne	t					
R	lemote Subne	t Mask					
A	dvanced Setti	ings		\geq			



РРТР	
Item	Description
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP server.
Username	Enter the username that PPTP server provides.

Password	Enter the password that PPTP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".
Global Traffic	All of the data traffic will be sent out via PPTP tunnel once
Forwarding	enable this function.
Remote Subnet	Set the peer subnet of PPTP.
Remote Subnet Mask	Set the netmask of peer PPTP server.

Table 3-2-5-9 PPTP Parameters

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

Figure 3-2-5-11

PPTP Advanced Settings			
Item	Description		
Local IP Address	Set IP address of PPTP client.		
Peer IP Address	Enter tunnel IP address of PPTP server.		
Enable NAT	Enable the NAT faction of PPTP.		
Enable MPPE	Enable MPPE encryption.		
Address/Control	For PPP initialization. User can keep the default option.		
Compression			
Protocol Field	For PPP initialization. User can keep the default option.		
Compression			
Asyncmap Value	One of the PPP protocol initialization strings. User can keep		
	the default value. Range: 0-fffffffff.		
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 3-2-5-10 PPTP Parameters

Related Configuration Example

PPTP Application Example

3.2.5.7 OpenVPN Client

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

Advantages of OpenVPN include:

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certificatio
OpenVPN Clin	ent Settings						
- OpenVPI	N_1						
Enable		-					
Protocol				•			
	P Address	UDF		•			
Port	P Address	1194					
Interface		tun					
Authentic		Non	~	•			
Local Tu				•			
	Tunnel IP						
Enable N							
Compres		LZO	9	*			
Link Dete	ection Interval(s)	60					
Link Dete	ection Timeout(s)	300					
Cipher		Non	e	*			
MTU		1500					
Max Frar	ne Size	1500					
Verbose	Level	ERF	OR	•			
Expert O	ptions						
Local Ro	oute						
		Subnet			Subnet Mas	k	Operation
							æ

Figure 3-2-5-12

OpenVPN Client	
Item	Description
Enable	Enable OpenVPN client. A maximum of 3 tunnels is allowed.
Protocol	Select from "UDP" and "TCP".
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port Enter the listening port number of remote OpenVPN server. Range 1-65535.	
Interface Select from "tun" and "tap".	
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert", and "X.509 cert+user".
Local Tunnel IP	Set local tunnel address.
Remote Tunnel IP	Enter remote tunnel address.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Check to enable TLS authentication.
Username	Enter username provided by OpenVPN server.
Password	Enter password provided by OpenVPN server.

Enable NAT	Enable NAT traversal function.	
Compression	Select LZO to compress data.	
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. Range: 10-1800.	
Link Detection Timeout (s) Set link detection timeout. OpenVPN will be reestablished after timeout. Range: 60-3600.		
Cipher	Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".	
MTU	Enter the maximum transmission unit. Range: 128-1500.	
Max Frame Size	Set the maximum frame size. Range: 128-1500.	
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".	
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.	
Local Route		
Subnet	Set the local route's IP address.	
Subnet Mask	Set the local route's netmask.	

Table 3-2-5-11 OpenVPN Client Parameters

3.2.5.8 OpenVPN Server

UF51 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server
OpenVPN Serv	ver Settings					
Enable						
Protocol		UDP		Ŧ		
Port		1194				
Listening IP						
Interface		tun		Ŧ		
Authentication		None		٣		
Local Virtual IP						
Remote Virtual I	Ρ					
Enable NAT		4				
Compression		LZO		٣		
Link Detection Ir	nterval	60				
Cipher		None		v		
MTU		1500				
Max Frame Size		1500				
Verbose Level		ERROR		٣		
Expert Options						

Figure 3-2-5-13

Local Route			
	Subnet	Netmask	Operation
Account			
	Username	Password	Operation
			8



OpenVPN Server	
Item	Description
Enable	Enable/disable OpenVPN server.
Protocol	Select from TCP and UDP.
Port	Fill in listening port number. Range: 1-65535.
Listening IP	Enter WAN IP address or LAN IP address. Leaving it blank refers to all active WAN IP and LAN IP address.
Interface	Select from " tun" and "tap".
Authentication	Select from "None", "Pre-shared", "Username/Password", "X.509 cert" and "X. 509 cert +user".
Local Virtual IP	The local tunnel address of OpenVPN's tunnel.
Remote Virtual IP	The remote tunnel address of OpenVPN's tunnel.
Client Subnet	Local subnet IP address of OpenVPN client.
Client Netmask	Local netmask of OpenVPN client.
Renegotiation Interval(s)	Set interval for renegotiation. Range: 0-86400.
Max Clients	Maximum OpenVPN client number. Range: 1-128.
Enable CRL	Enable CRL
Enable Client to Client	Allow access between different OpenVPN clients.
Enable Dup Client	Allow multiple users to use the same certification.
Enable NAT	Check to enable the NAT traversal function.
Compression	Select "LZO" to compress data.
Link Detection Interval	Set link detection interval time to ensure tunnel connection. Range: 10-1800.
Cipher	Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
MTU	Enter the maximum transmission unit. Range: 64-1500.
Max Frame Size	Set the maximum frame size. Range: 64-1500.
Verbose Level	Select from "ERROR", "WARING", "NOTICE" and "DEBUG".
Expert Options User can enter some other PPP initialization strings in this field separate the strings with blank space.	
Local Route	
Subnet	The real local IP address of OpenVPN client.
Netmask	The real local netmask of OpenVPN client.

Account		
Username & Password	Set username and password for OpenVPN client.	
Table 3-2-5-12 OpenVPN Server Parameters		

3.2.5.9 Certifications

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

DMVPN	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
OpenVPN Clie	nt						
- OpenVPN	client_1						
CA				Browse	Import Export De	lete	
Public Ke	Y			Browse	Import Export De	lete	
Private Ke	∋y <mark>n</mark>			Browse	Import Export De	lete	
TA				Browse	Import Export De	lete	
Preshared	l Key			Browse	Import Export De	lete	
PKCS12				Browse	Import Export De	lete	

Figure 3-2-5-15

OpenVPN Client	OpenVPN Client		
Item	Description		
CA	Import/Export CA certificate file.		
Public Key	Import/Export public key file.		
Private Key	Import/Export private key file.		
ТА	Import/Export TA key file.		
Preshared Key	Import/Export static key file.		
PKCS12	Import/Export PKCS12 certificate file.		

Table 3-2-5-13 OpenVPN Client Certification Parameters

Ope	nVPN Server				
—	OpenVPN Server				
	CA	Browse	Import	Export	Delete
	Public Key	Browse	Import	Export	Delete
	Private Key	Browse	Import	Export	Delete
	DH	Browse	Import	Export	Delete
	ТА	Browse	Import	Export	Delete
	CRL	Browse	Import	Export	Delete
	Preshared Key	Browse	Import	Export	Delete

Figure 3-2-5-16

OpenVPN Server		
Description		
Import/Export CA certificate file.		
Import/Export public key file.		
Import/Export private key file.		
Import/Export DH key file.		
Import/Export TA key file.		
Import/Export CRL.		
Import/Export static key file.		

Table 3-2-5-14 OpenVPN Server Parameters

IPsec					
- 1	Psec_1				
	CA	Browse	Import	Export	Delete
	Client Key	Browse	Import	Export	Delete
	Server Key	Browse	Import	Export	Delete
	Private Key	Browse	Import	Export	Delete
	CRL	Browse	Import	Export	Delete

Figure 3-2-5-17

IPsec	
Item	Description
CA	Import/Export CA certificate.
Client Key	Import/Export client key.
Server Key	Import/Export server key.
Private Key	Import/Export private key.

CRL	Import/Export certificate recovery list.							
Table 3-2-5-15 IPsec Parameters								
IPsec Server								
- IPsec Server								
CA	Browse Import Export Dele	te						
Local Certificate	Browse Import Export Dele	te						
Private Key	Browse Import Export Dele	te						
CRL	Browse Import Export Dele	te						

Figure 3-2-5-18

IPsec Server				
Item	Description			
CA	Import/Export CA certificate.			
Local Certificate	Import/Export Local Certificate file.			
Private Key	Import/Export private key.			
CRL	Import/Export certificate recovery list.			

Table 3-2-5-16 IPsec Server Parameters

3.2.6 IP Passthrough

IP Passthrough mode shares or "passes" the Internet providers assigned IP address to a single LAN

client device connected to the device.

Status	IP Passthrough	
Network	IP Passthrough	
	Enable	
Interface	Passthrough Mode	DHCPS-Fixed *
DHCP	MAC	
Firewall		
QoS	Save	
VPN		
IP Passthrough		
	Figure 3-2-6-1	
IP Passthrough		
Item	Description	

Enable or disable IP Passthrough.

Enable

Passthrough Mode	Select passthrough mode from "DHCPS-Fixed" and "DHCPS-Dynamic".	
MAC	Set MAC address.	
	·	

Table 3-2-6-1 IP Passthrough Parameters

3.2.7 Routing

3.2.7.1 Static Routing

A static routing is a manually configured routing entry. Information about the routing is manually entered rather than obtained from dynamic routing traffic. After setting static routing, the package for the specified destination will be forwarded to the path designated by user.

atic Rou	ting					
	Destination	Netmask/Prefix Length	Interface	Gateway	Distance	Operation
2	2400:3200::1	128	Cellular 🗸	2408:844b:1a30:115a:b94b:	1	×
2	2001:4860:4860::8888	128	Cellular 🗸	2408:844b:1a30:115a:b94b:	1	×
:	1	0	Cellular 🗸	2408:844b:1a30:115a:b94b:	1	×
:		0	·	2408:844b:1a30:126:a02f:68	1	×
	0.0.0	0.0.0.0	WAN 🗸	192.168.22.1	1	×



Static Routing	
Item	Description
Destination	Enter the destination IPv4/IPv6 address.
Netmask/Prefix Length	Enter the subnet mask or prefix length of destination address.
Interface	The interface through which the data can reach the destination address.
Gateway	IPv4/IPv6 address of the next router that will be passed by before the input data reaches the destination address.
Distance	Priority, smaller value refers to higher priority. Range: 1-255.

Table 3-2-7-1 Static Routing Parameters

3.2.7.2 RIP

RIP is mainly designed for small networks. RIP uses Hop Count to measure the distance to the destination address, which is called Metric. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to limit the convergence time, the specified metric of RIP is an integer in the range of 0 - 15 and

the hop count larger than or equal to 16 is defined as infinity, which means that the destination network or host is unreachable. Because of this limitation, the RIP is not suitable for large-scale networks. To improve performance and prevent routing loops, RIP supports split horizon function. RIP also introduces routing obtained by other routing protocols.

Each router that runs RIP manages a routing database, which contains routing entries to reach all reachable destinations.

Static Routing	RIP	OSPF	Routi	ing Filtering	
RIP Settings					
Enable					
Update Timer	30		s		
Timeout Timer	180		s		
Garbage Collection Timer	120		s		
Version	v2		•		
Show Advanced Options					
Default Information Origina	te 📄				
Default Metric	1				
Redistribute Connected					
Redistribute Static					
Redistribute OSPF					



RIP	
Item	Description
Enable	Enable or disable RIP.
Update Timer	It defines the interval to send routing updates. Range: 5-2147483647, in seconds.
Timeout Timer	It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16. Range: 5-2147483647, in seconds.
Garbage Collection Timer	It defines the period from the routing cost of a routing becomes 16 to it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the routing cost for sending routing updates. If Garbage Collection times out and the routing still has not been updated, the routing will be completely removed from the routing table. Range: 5-2147483647, in seconds.
Version	RIP version. The options are v1 and v2.
Advanced Settings	

Default Information Originate	Default information will be released when this function is enabled.			
Default Metric	The default cost for the device to reach destination. Range: 0-16			
Redistribute Connected	Check to enable.			
Metric	Set metric after "Redistribute Connected" is enabled. Range: 0-16.			
Redistribute Static	Check to enable.			
Metric	Set metric after "Redistribute Static" is enabled. Range: 0-16.			
Redistribute OSPF	Check to enable.			
Metric	Set metric after "Redistribute OSPF" is enabled. Range: 0-16.			

Table 3-2-7-2 RIP Parameters

Distance/Metric I	vanagement						
Distance		IP Add	Iress	Netmas	ĸ	ACL Name	Operation
							Ð
Metric		Policy	In/Out	Interface	3	ACL Name	Operation
							Ð
Filter Policy							
Policy Ty	pe	Policy	Name	Policy In/C	Dut	Interface	Operation
							8
Passive Interface	2						
			Passive	Interface			Operation
							•
Interface							
Interface	Send Version	Receive Version	Split- Horizon	Authentication Mode	Authentication String	Authentication Key-chain	Operation
							•
Neighbor							
			IP Ad	Idress			Operation
							Ð
Network							
	IP Addre	\$5			Netmask		Operation
							•



Willesignt 101	

Item	Description				
Distance/Metric Management					
Distance	Set the administrative distance that a RIP route learns. Range: 1-255.				
IP Address	Set the IP address of RIP route.				
Netmask	Set the netmask of RIP route.				
ACL Name	Set ACL name of RIP route.				
Metric	The metric of received route or sent route from the interface. Range: 0-16.				
Policy in/out	Select from "in" and "out".				
Interface	Select interface of the route.				
ACL Name	Access control list name of the route strategy.				
Filter Policy					
Policy Type	Select from "access-list" and "prefix-list".				
Policy Name	User-defined prefix-list name.				
Policy in/out	Select from "in" and "out".				
Interface	Select interface from "cellular0", "WAN" and "Bridge0".				
Passive Interface					
Passive Interface	Select interface from "cellular0" and "WAN", "Bridge0".				
Interface					
Interface	Select interface from "cellular0", "WAN" and "Bridge0".				
Send Version	end Version Select from "default", "v1" and "v2".				
Receive Version	Select from "default", "v1" and "v2".				
Split-Horizon	Select from "enable" and "disable".				
Authentication Mode	Select from "text" and "md5".				
Authentication String	The authentication key for package interaction in RIPV2.				
Authentication Key-chain	The authentication key-chain for package interaction in RIPV2.				
Neighbor					
IP Address	Set RIP neighbor's IP address manually.				
Network					
IP Address	Address The IP address of interface for RIP publishing.				
Netmask The netmask of interface for RIP publishing.					
Table 3-2-7-3					

Table 3-2-7-3

3.2.7.3 OSPF

OSPF, short for Open Shortest Path First, is a link status based on interior gateway protocol

developed by IETF.

If a router wants to run the OSPF protocol, there should be a Router ID that can be manually configured. If no Router ID configured, the system will automatically select an IP address of interface as the Router ID. The selection order is as follows:

- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

Five types of packets of OSPF:

- Hello packet
- DD packet (Database Description Packet)
- LSR packet (Link-State Request Packet)
- LSU packet (Link-State Update Packet)
- LSAck packet (Link-Sate Acknowledgment Packet)

Neighbor and Neighboring

After OSPF router starts up, it will send out Hello Packets through the OSPF interface. Upon receipt of Hello packet, OSPF router will check the parameters defined in the packet. If it's consistent, a neighbor relationship will be formed. Not all matched sides in neighbor relationship can form the adjacency relationship. It is determined by the network type. Only when both sides successfully exchange DD packets and LSDB synchronization is achieved, the adjacency in the true sense can be formed. LSA describes the network topology around a router, LSDB describes entire network topology.

Static Routing	RIP	OSPF	Routing Filtering
OSPF Settings			
Enable			
Router ID			
ABR Type	cisco	6	٣
RFC1583 Compatibility			
OSPF Opaque-LSA			
SPF Delay Time	0		ms
SPF Initial-holdtime	50		ms
SPF Max-holdtime	5000		ms
Reference Bandwidth	100		mbit

Figure 3-2-7-4

Milesight IoT	
---------------	--

OSPF	
Item	Description
Enable	Enable or disable OSPF.
Router ID	Router ID (IP address) of the originating LSA.
ABR Type	Select from cisco, ibm, standard and shortcut.
RFC1583 Compatibility	Enable/Disable.
OSPF Opaque-LSA	Enable/Disable LSA: a basic communication means of the OSPF routing protocol for the Internet Protocol (IP).
SPF Delay Time	Set the delay time for OSPF SPF calculations. Range: 0-6000000, in milliseconds.
SPF Initial-holdtime	Set the initialization time of OSPF SPF. Range: 0-6000000, in milliseconds.
SPF Max-holdtime	Set the maximum time of OSPF SPF. Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

Table 3-2-7-4 OSPF Parameters

Interface	ł	Hello Interval(s)	Dead Interv	ale	Retransmit Interval(s)	Transmit Delay(s)	Operatio
Bridge0	▼ 10		40	5		1	×
terface Advanced	Options	9					
				Authenticat			

Figure 3-2-7-5

Item	Description
Interface	
Interface	Select interface from "cellular0","WAN" and "Bridge0".
Hello Interval (s)	Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established. Range: 1-65535.
Dead Interval (s)	Dead Time. If no Hello packet is received from the neighbours within the dead time, then the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship cannot be established.

Retransmit Interval (s)	When the device notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour. Range: 3-65535.
Transmit Delay (s)	It will take time to transmit OSPF packets on the link. So a certain delay time should be increased before transmission the aging time of LSA. This configuration needs to be further considered on the low-speed link. Range: 1-65535.
Interface Advanced Opt	ions
Interface	Select interface.
Network	Select OSPF network type.
Cost	Set the cost of running OSPF on an interface. Range: 1-65535.
Priority	Set the OSPF priority of interface. Range: 0-255.
Authentication	Set the authentication mode that will be used by the OSPF area. Simple: a simple authentication password should be configured and confirmed again. MD5: MD5 key & password should be configured and confirmed again.
Key ID	It only takes effect when MD5 is selected. Range 1-255.
Кеу	The authentication key for OSPF packet interaction.

Table 3-2-7-5 OSPF Parameters





Item	Description
Passive Interface	
Passive Interface	Select interface from "cellular0", "WAN" and "Bridge0".
Network	
IP Address	The IP address of local network.
Netmask	The netmask of local network.

Area ID	The area ID of original LSA's router.
Area	
Area ID	Set the ID of the OSPF area (IP address).
Area	Select from "Stub" and "NSSA". The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA".
No Summary	Forbid route summarization.
Authentication	Select authentication from "simple" and "md5".

Table 3-2--7-6 OSPF Parameters

Area Advanced Options	•							
Area Range								
Area ID	IP Add	ress	Netr	nask	No Advertise	Co	st	Operation
Area Filter								Ð
Area Filler								
Area ID			Filter Type			ACL Name		Operation
								Ð
Area Virtual Link								
Area ID ABR Address	Authentica tion	Key ID	Key	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay	Operation
								H

Figure 3-2-7-7

Area Advanced Options				
Item	Description			
Area Range				
Area ID	The area ID of the interface when it runs OSPF (IP address).			
IP Address	Set the IP address.			
Netmask	Set the netmask.			
No Advertise	Forbid the route information to be advertised among different areas.			
Cost	Range: 0-16777215			
Area Filter				
Area ID	Select an Area ID for Area Filter.			
Filter Type	Select from "import", "export", "filter-in", and "filter-out".			
ACL Name	Enter an ACL name which is set on "Routing > Routing Filtering" webpage.			
Area Virtual Link				
Area ID	Set the ID number of OSPF area.			
ABR Address	ABR is the router connected to multiple outer areas.			
Authentication	Select from "simple" and "md5".			
Key ID	It only takes effect when MD5 is selected. Range 1-15.			
Кеу	The authentication key for OSPF packet interaction.			

Hello Interval	Set the interval time for sending Hello packets through the interface. Range: 1-65535.
Dead Interval	The dead interval time for sending Hello packets through the interface. Range: 1-65535.
Retransmit Interval	The retransmission interval time for re-sending LSA. Range: 1-65535.
Transmit Delay	The delay time for LSA transmission. Range: 1-65535.

Table 3-2-7-7 OSPF Parameters

Redistribution					
Redistribution Type	Metric	Metric Type		Route Map	Operation
connected •		1	•		×
Dedictribution Advanced Options	7				Ð
	•				
Always Redistribute Default Route		_			
Redistribute Default Route Metric	0				
Redistribute Default Route Metric Type	1]			
Distance Management					
Area Type	e		Distance		Operation
					æ

Figure 3-2-7-8

Item	Description
Redistribution	
Redistribution Type	Select from "connected", "static" and "rip".
Metric	The metric of redistribution router. Range: 0-16777214.
Metric Type	Select Metric type from "1" and "2".
Route Map	Mainly used to manage route for redistribution.
Redistribution Advanced C	Options
Always Redistribute Default Route	Send redistribution default route after starting up.
Redistribute Default Route Metric	Send redistribution default route metric. Range: 0-16777214.
Redistribute Default Route Metric Type	Select from "0", "1" and "2".
Distance Management	
Area Type	Select from "intra-area", "inter-area" and "external".
Distance	Set the OSPF routing distance for area learning. Range: 1-255.

Table 3-2-7-8 OSPF Parameters

3.2.7.4 Routing Filtering

Static Routing	RIP	OSPF	Routing F	iltering				
Access Control List								
Name	Ac	tion	Match Any	IP Ad	dress	Netr	nask	Operation
	deny	•						×
								Œ
P Prefix-List								
Name	Sequence Number	Action	Match Any	IP Address	Netmask	GE Length	LE Length	Operation
		deny 🔻						×
								A

Figure 3-2-7-9

Nameare allowActionSelectMatch AnyNo need	efined name, need to start with a letter. Only letters, digits and underline (_)	
Name User-de are allo Action Select Match Any No nee	owed. from "permit" and "deny". ed to set IP address and subnet mask.	
Nameare allowActionSelectMatch AnyNo need	owed. from "permit" and "deny". ed to set IP address and subnet mask.	
Match Any No nee	ed to set IP address and subnet mask.	
,		
P Address User-de	efined.	
Netmask User-de	efined.	
IP Prefix-List		
Name User-de are allo	efined name, need to start with a letter. Only letters, digits and underline (_) owed.	
· ·	x name list can be matched with multiple rules. One rule is matched with quence number. Range: 1-4294967295.	
Action Select	from "permit" and "deny".	
Match Any No nee	ed to set IP address, subnet mask, FE Length, and LE Length.	
IP Address User-de	efined.	
Netmask User-de	efined.	
FE Length Specify	y the minimum number of mask bits that must be matched. Range: 0-32.	
LE Length Specify	y the maximum number of mask bits that must be matched. Range: 0-32.	

Table 3-2-7-9 Routing Filtering Parameters

3.2.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections in

an IP sub-network.

Increasing the number of exit gateway is a common method for improving system reliability. VRRP adds a group of routers that undertake gateway function into a backup group so as to form a virtual router. The election mechanism of VRRP will decide which router undertakes the forwarding task, and the host in LAN is only required to configure the default gateway for the virtual router.

In VRRP, routers need to be aware of failures in the virtual master router. To achieve this, the virtual master router sends out multicast "alive" announcements to the virtual backup routers in the same VRRP group.

The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

VRRP has the following characteristics:

- The virtual router with an IP address is known as the Virtual IP address. For the host in LAN, it is only required to know the IP address of virtual router, and set it as the address of the next hop of the default route.
- The network Host communicates with the external network through this virtual router.
- A router will be selected from the set of routers based on its priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in the case of any malfunction, so as to guarantee uninterrupted communication between the host and external network.

When interface connected with the uplink is at the state of Down or Removed, the router actively lowers its priority so that priority of other routers in the backup group will be higher. Thus the router with the highest priority becomes the gateway for the transmission task.

Status	VRRP	
Network	VRRP Status Status	DISABLE
Interface	VRRP Settings	
DHCP	Enable	
Firewall	Interface	Bridge0 •
i iicwaii	Virtual Router ID	1
QoS	Virtual IP	
VPN	Priority	100
IP Passthrough	Advertisement Interval (s)	1
	Preemption Mode	
Routing	IPV4 Primary Server	8.8.8.8
VRRP	IPV4 Secondary Server	114.114.114.114
DDNS	Interval	300 s
	Retry Interval	5 s
System •	Timeout	3 s
	Max Ping Retries	3
Industrial		
Maintenance	Save	

Figure 3-2-8-1

VRRP				
Item	Description	Default		
Enable	Enable or disable VRRP.	Disable		
Interface	Select the interface of Virtual Router.			
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.			
Virtual IP	Set the IP address of Virtual Router.			
Priority	The VRRP priority range is 1-254 (a bigger number indicates a higher priority). The device with higher priority will be more likely to become the gateway.			
Advertisement Interval (s)	Heartbeat package transmission time interval between devices in the virtual ip group. Range: 1-255.	1		
Preemption Mode	If the device works in the preemption mode, once it finds that its own priority is higher than that of the current gateway, it will send VRRP notification package, resulting in re-election of gateway and eventually replacing the original gateway. Accordingly, the original gateway will become a Backup device.	Disable		
IPV4 Primary Server	The device will send ICMP packet to the IP address or host name to determine whether the Internet connection is still a vailable or not.	8.8.8.8		
IPV4 Secondary Server	The router will try to ping the secondary server name if prim ary server is not available.	114.114. 114.114		
Interval	Time interval (in seconds) between two Pings.	300		
Retry Interval	Set the ping retry interval. When ping failed, the device will p ing again every retry interval.	5		
Timeout	The maximum amount of time the device will wait for a res ponse to a ping request. If it does not receive a response fo r the amount of time defined in this field, the ping request w ill be considered as failure.			
Max Ping Retries	The retry times of the device sending ping request until dete rmining that the connection has failed.	3		

Table 3-2-8-1 VRRP Parameters

Related Configuration Example

VRRP Application Example

3.2.9 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name.

DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

DDNS Status		
Status	()	
DDNS Method List		
Enable		
Name		
Service Type	DynDNS	~
Username		
User ID		
Password		
Server		
Server Path		
Hostname		
Append IP		
Use HTTPS		

Figure 3-2-9-1

DDNS	
Item	Description
Status	Show connection status of DDNS.
Enable	Enable/disable DDNS.
Name	Give the DDNS a descriptive name.
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.
Server Path	By default the hostname is appended to the path.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.
Use HTTPS	Enable HTTPS for some DDNS providers.

Table 3-2-9-1 DDNS Parameters

3.3 System

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

3.3.1 General Settings

3.3.1.1 General

General settings include system info and HTTPS certificates.

General	System Time	Email			
System					
Hostname		ROUTER			
Web Login Timeout(s)		1800			
Encrypting Cleartext Passwords					
HTTPS Certifi	cates				
Certificate	https.crt	Browse	Import	Export	Delete
Key	https.key	Browse	Import	Export	Delete

```
Figure 3-3-1-1
```

General				
Item	Description	Default		
System				
Hostname	User-defined device name, needs to start with a letter.	ROUTER		
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800		
Encrypting Cleartext Passwords	This function will encrypt all of cleartext passwords into ciphertext passwords.	Enable		
HTTPS Certificates				
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into device. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.			
Кеу	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into device. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.			

Table 3-3-1-1 General Setting Parameters

3.3.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type. Note: to ensure that the device runs with the correct time, it's recommended that you set the system time when configuring the device.

General	System Time	Email	
System Time Set	tings		
Current Time		2021-07-22 16:13:17 Thur	
Time Zone		8 China (Beijing)	~
Sync Type		Sync with NTP Server	~
Primary NTP Serve	r	pool.ntp.org	•
Secondary NTP Se	rver		•
NTP Server			
Enable NTP Server			
	Figure 3	3-3-1-2	
General	System Time	Email	
System Time Set	tings		
Current Time		2021-07-22 16:13:43 Thur	
Time Zone		8 China (Beijing)	~
Sync Type		Set up Manually	~
Date		2021-07-22	
Time		16 v 13 v 42	~

Figure 3-3-1-3



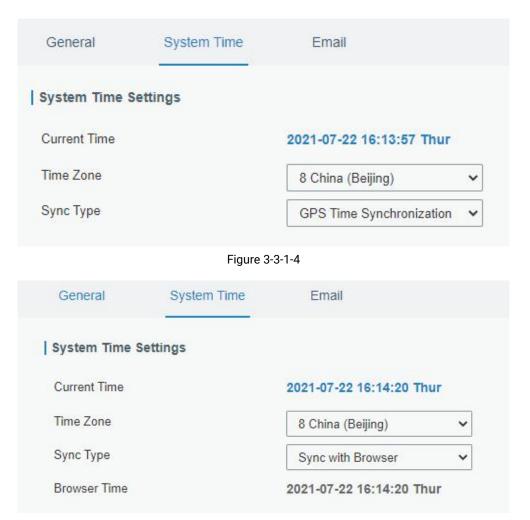


Figure 3-3-1-5

System Time	
Item	Description
Current Time	Show the current system time.
Time Zone	Click the drop down list to select the time zone you are in.
Sync Type	Click the drop down list to select the time synchronization type.
Sync with Browser	Synchronize time with browser.
Browser Time	Show the current time of browser.
Set up Manually	Manually configure the system time.
GPS Time	Synchronize time with GPS.
Synchronization	Synchronize time with Gr 3.
Primary NTP Server	Enter primary NTP Server's IP address or domain name.
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.
NTP Server	
Enable NTP Server	NTP client on the network can achieve time synchronization with device
	after "Enable NTP Server" option is checked.

Table 3-3-1-2 System Time Parameters

3.3.1.3 Email

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 and add email groups for alarms and events.

General	System Time	Email	
SMTP Client S	ettings		
Enable			
Email Address			
Password			
SMTP Server A	ddress		
Port		25	
Encryption		STARTTLS	~
Test			
Test			

Figure 3-3-1-6

SMTP Client Settings			
Item	Description		
Enable	Enable or disable SMTP client function.		
Email Address	Enter the sender's email account.		
Password	Enter the sender's email password.		
SMTP Server Address	Enter SMTP server's domain name.		
Port	Enter SMTP server port. Range: 1-65535.		
Encryption	Select from: None, TLS/SSL, STARTTLS. None: No encryption. The default port is 25. STARTTLS: STARTTLS is a way to take an existing insecure connection and upgrade it to a secure connection by using SSL/TLS. The default port is 587. TLS/SSL: SSL and TLS both provide a way to encrypt a communication channel between two computers (e.g. your computer and our server). TLS is the successor to SSL and the terms SSL and TLS are used interchangeably unless you're referring to a specific version of the protocol.The		

Table 3-3-1-3 SMTP Setting

E	ma	il I	List

Em	ail Address		Description	Operatio
				0
nail Group List				
	Group ID			
	Description			
	List		Selected	
				*
		▼		*

Figure 3-3-1-7

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

Table 3-3-1-4 Email Settings

Related Topics

DI Setting Events Setting Events Application Example

3.3.2 Phone&SMS

3.3.2.1 Phone

Phone settings involve in call/SMS trigger, SMS control and SMS alarm for events.

Phone	SMS						
Phone Num	ber List						
	Nun	nber			Description		Operation
							×
							8
Phone Grou	p List						
		Group ID					
		Description					
		List			Selected		
			*			*	
			*			*	
			Save	Cancel			

Figure 3-3-2-1

Phone	
Item	Description
Phone Number List	
Number	Enter the telephone number. Digits, "+" and "-" are allowed.
Description	The description of the telephone number.
Phone Group List	
Group ID	Set number for phone group. Range: 1-100.
Description	The description of the phone group.
List	Show the phone list.
Selected	Show the selected phone number.
	Table 2.2.2.1 Phane Catting

Table 3-3-2-1 Phone Settings

Related Topic

Connect on Demand

3.3.2.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status.

Status	Phone SMS	
Network	General Setting	
	SMS Mode	PDU v
System 👻	SMS Remote Control	
General Settings	Authentication Type	Password+Phone •
2	Password	
Phone & SMS	Phone Group	
User Management		
SNMP	Save	

Figure 3-3-2-2

SMS Settings	
Item	Description
SMS Mode	Select SMS mode from "TEXT" and "PDU".
SMS Remote Control	Enable/disable SMS Remote Control.
Authentication Type	You can choose "phone number" or "password + phone number". Phone number: Use phone number for authentication. Password + phone number: Use both ""Password"" and ""Phone number"" for authentication.
Password	Set password for authentication.
Phone Group	Select the Phone group which used for remote control. User can click the Phone Group and set phone number.

Table 3-3-2-2 SMS Remote Control Parameters

Send SMS						
Phone Number						
Content						
Send						
Inbox						
From		То		Sender		Search
	Sender		Time		Content	
< > 10 •	Go to: GO	1				
		J				
Outbox		J				
		То		Recipient]	Search
Outbox	Recipient	то	Time	Recipient	Status	Search

Figure 3-3-2-3

SMS	
Item	Description
Send SMS	
Phone Number	Enter the number to receive the SMS.
Content	SMS content.
Inbox/Outbox	
Sender	SMS sender from outside.
Recipient	SMS recipient which UF51 send to.
From	Select the start date.
То	Select the end date.

Table 3-3-2-3 SMS Settings

3.3.3 User Management

3.3.3.1 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.

Status		Account User Ma	nagement
Network	•	Change Account Info	
		Username	admin
System	-	Old Password	
General Settings		New Password	
General Settings		Confirm New Password	
Phone & SMS			
User Management		Save	



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

Table 3-3-3-1 Account Settings

3.3.3.2 User Management

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

Account	User Management			
User List				
	Username	Password	Permission	Operation
			Read-Only 🗸	×
				•

Figure 3-3-3-2

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

Table 3-3-3-2 User Management

3.3.4 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.

Related Configuration Example

SNMP Application Example

3.3.4.1 SNMP

UF51 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

161	
SNMPv2	*
225_location	
225_Contact	
	161 SNMPv2 225_location



SNMP Settings			
Item Description			
Enable	Enable or disable SNMP function.		
Port	Set SNMP listened port. Range: 1-65535.		
FUIL	The default port is 161.		
SNMP Version Select SNMP version; support SNMP v1/v2c/v3.			
Location Information	Fill in the location information.		

Contact Information	Fill in the contact information.

Table 3-3-4-1 SNMP Parameters

3.3.4.2 MIB View

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

SNMP	MIB View	VACM	Trap	MIB	
View List					
Vi	iew Name	View	Filter	View OID	Operation
All		Included	Ŧ] [1	×
system		Included	Ŧ	1.3.6.1.2.1.1	
					+

Figure 3-3-4-2

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

Table 3-3-4-2 MIB View Parameters

3.3.4.3 VACM

This section describes how to configure VCAM parameters.

SNMP	MIB View	VACM	Тгар	MIB		
SNMP v1 & v2	2 User List					
Con	nmunity	Permissio	n	MIB View	Network	Operation
private		Read-Write	• Al	8	▼ 0.0.0.0/0	×
public		Read-Write	• All	1	▼ 0.0.0.0/0	×
						8

Figure 3-3-4-3

VACM				
Item		Description		
SNMP v1 & v2 User List				
Community	Set the community	Set the community name.		
Permission	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 Gro	pup				
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.				
SNMP v3 User Lis	t				
Username	Set the name of SNMPv3 user.				
Group Name	Select a user group to be configured from the user group.				
Authentication	Select from "MD5", "SHA", and "None".				
Authentication	The password should be filled in if authentication is "MD5" and "SHA".				
Password	The password should be filled if it addieffication is 1000 and 511A.				
Encryption	Select from "AES", "DES", and "None".				
Encryption Password	The password should be filled in if encryption is "AES" and "DES".				

Table 3-3-4-3 VACM Parameters

3.3.4.4 Trap

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

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



SNMP Trap				
Item	Description			
Enable	Enable or disable SNMP Trap function.			
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.			
Server Address	Fill in NMS's IP address or domain name.			
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.			
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.			

Auth/Priv Mode Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".

Table 3-3-4-4 Trap Parameters

3.3.4.5 MIB

This section describes how to download MIB files. The last MIB file "LTE-ROUTER-MIB.txt" is for the UF51 device.

SNMP	MIB View	VACM	Тгар	MIB
MIB Download				
MIB File		LTE-ROU	TER-MIB.b 🔻	Download

Figure 3-3-4-5

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

3.3.5 AAA

AAA access control is used for visitors control and the available corresponding services once access is allowed. It adopts the same method to configure three independent safety functions. It provides modularization methods for following services:

- Authentication: verify if the user is qualified to access to the network.
- Authorization: authorize related services available for the user.
- Charging: record the utilization of network resources.

3.3.5.1 Radius

Using UDP for its transport, Radius is generally applied in various network environments with higher requirements of security and permission of remote user access.

Radius	Tacacs+	LDAP	Authentication
Radius Settin	gs		
Enable			
Server IP Addr	ess		
Server Port		18 <mark>1</mark> 2	
Shared Secret			
Save			



Description
Enable or disable Radius.
Fill in the Radius server IP address/domain name.
Fill in the Radius server port. Range: 1-65535.
Fill in the key consistent with that of Radius server in order to get connected with Radius server.

Table 3-3-5-1 Radius Parameters

3.3.5.2 TACACS+

Using TCP for its transport, TACACS+ is mainly used for authentication, authorization and charging of the access users and terminal users by adopting PPP and VPDN.

Radius	Tacacs+	LDAP	Authentication
Tacacs+ Sett	ings		
Enable			
Server IP Add	ress		
Server Port		49	
Shared Secret	t		
	_		
Save			

Figure 3-3-5-2

TACACS+	
ltem	Description
Enable	Enable or disable TACACS+.
Server IP Address	Fill in the TACACS+ server IP address/domain name.
Server Port	Fill in the TACACS+ server port. Range: 1-65535.
Кеу	Fill in the key consistent with that of TACACS+ server in order to get connected with TACACS+ server.

Table 3-3-5-2 TACACS+ Parameters

3.3.5.3 LDAP

A common usage of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect the LDAP server to validate users.

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite as well.

Radius	Tacacs+	LDAP	Authentication
LDAP Setting	IS		
Enable			
Server IP Addr	ess		
Server Port		389	
Base DN			
Security		None	٣
Username			
Password			



LDAP	
Item	Description
Enable	Enable or Disable LDAP.
Server IP Address	Fill in the LDAP server's IP address/domain name. The maximum count is 10.
Server Port	Fill in the LDAP server's port. Range: 1-65535
Base DN	The top of LDAP directory tree.
Security	Select secure method from "None", "StartTLS" and "SSL".

Username	Enter the username to access the server.	
Password	Enter the password to access the server.	

Table 3-3-5-3 LDAP Parameters

3.3.5.4 Authentication

AAA supports the following authentication ways:

- None: uses no authentication, generally not recommended.
- Local: uses the local username database for authentication.
 - Advantages: rapidness, cost reduction. \triangleright
 - Disadvantages: storage capacity limited by hardware. ≻
- Remote: has user's information stored on authentication server. Radius, TACACS+ and LDAP supported for remote authentication.

When radius, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

adius	Tacacs+	LDAP	Authentication	
uthenticatio	on Settings			
Se	rvice	1	2	3
Сог	nsole	None •	None •	None •
V	Veb	None •	None 🔻	None 🔻
Te	Inet	None •	None 🔻	None 🔻
S	SH	None 🔻	None 🔻	None 🔻

Figure 3-3-5-4

Authentication		
Item	Description	
Console	Select authentication for Console access.	
Web	Select authentication for Web access.	
Telnet	Select authentication for Telnet access.	
SSH	Select authentication for SSH access.	

Table 3-3-5-4 Authentication Parameters

3.3.6 Device Management

3.3.6.1 DeviceHub

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

Device Management	Milesight VPN
Device Management	
Status	Disconnected
Server Address	
Activation Method	By Authentication Code 🗸
Authentication Code	

Figure 3-3-6-1

DeviceHub	
Item	Description
Status	Show the connection status between the device and the DeviceHub.
Disconnected	Click this button to disconnect the device from the DeviceHub.
Server Address	IP address or domain of the device management server.
Activation Method	Select activation method to connect the device to the DeviceHub server, options are "By Authentication Code" and "By Account name".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account Name	Fill in the registered DeviceHub account (email) and
Password	password.

Table 3-3-6-1

3.3.6.2 Milesight VPN

You can connect the device to the Milesight VPN on this page so as to manage the device and connected devices centrally and remotely. For more details please refer to *MilesightVPN User Guide*.

Device Management	Milesight VPN
Milesight VPN Setting	
Server	
Port	18443
Authorization Code	
Device Name	
Connect	
Milesight VPN Status	
Status	Disconnected
Local IP	122 ¹
Remote IP	-
Duration	17



Milesight VPN	
Item	Description
Milesight VPN Setting	gs
Server	Enter the IP address or domain name of Milesight VPN.
Port	Enter the HTTPS port number.
Authorization Code	Enter the authorization code which generated by Milesight VPN.
Device Name	Enter the name of the device.
Milesight VPN Status	;
Status	Show the connection information about whether the device is
Status	connected to the Milesight VPN.
Local IP	Show the virtual IP of the device.
Remote IP	Show the virtual IP of the Milesight VPN.
Duration	Show the information on how long the device has been
Duration	connected to the Milesight VPN.

Table 3-3-6-2

3.3.7 Events

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

3.3.7.1 Events

You can view alarm messages on this page.

Status		Events	Events Settin	igs		
Network	•	Mark as Read	Delete	Mark All as	Read Delete All Ala	arms
System	-	St	atus	Туре	Time	Message
General Setting	IS	< > 10 ▼	Go to:	GO		
User Managem	ent					
SNMP						
AAA						
Events						

Figure 3-3-7-1

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

Table 3-3-7-1 Events Parameters

3.3.7.2 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.

System Time Update

VPN Up

VPN Down

WAN Up

WAN Down

Link switch

Weak Signal

Cellular Up

Events	Events Sett	ings				
Events Settings						
Enable Phone Group List Email Group List			•]		
E	Events		Record	Email 🔲 Email Group List	SMS 🗖 Phone Group List	
Syste	em Startup					
Syste	em Reboot					

Figure 3-3-7-2

.

Cellular Down		
Cellular Data Stats Clear		
Cellular Data Traffic is running out		
Cellular Data Traffic Overflow		
WLAN Up(AP)		
WLAN Down(AP)		•
WLAN Up(Client)		
WLAN Down(Client)		

Figure 3-3-7-3

Event Settings		
Item	Description	
Enable	Check to enable "Events Settings".	
Phone Group List	Select phone group to receive SMS alarm.	
Email Group List	Select email group to receive alarm.	
Record	The relevant content of event alarm will be recorded on	
Record	"Event" page if this option is checked.	
Email	The relevant content of event alarm will be sent out via email	
EIIIdii	if this option is checked.	

Milesight IoT

Email Setting	Click and you will be redirected to the page "Email" to configure email group list.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.
VPN Up	VPN is connected.
VPN Down	VPN is disconnected.
WAN Up	Ethernet cable is connected to WAN port.
WAN Down	Ethernet cable is disconnected to WAN port.
Link Switch	Switch to use other interface for Internet access.
Weak Signal	The signal level of cellular is low.
Cellular Up	Cellular network is connected.
Cellular Down	Cellular network is disconnected.
Cellular Data Stats Clear	Zero out the data usage of the main SIM card.
Cellular Data Traffic Is Running Out	The main SIM card is reaching the data usage limit.
Cellular Data Traffic Over Flow	The main SIM card has exceeded the data usage plan.
WLAN Up(AP)	The WLAN(AP) is enabled.
WLAN Down(AP)	The WLAN(AP) has stopped working.
WLAN Up(Client)	The WLAN(Client) is enabled.
WLAN Down(Client)	The WLAN(Client) has stopped working.
	Table 4-3-7-2 Events Parameters

Related Topics

Email Setting

Events Application Example

3.4 Industrial Interface

UF51 is capable of connecting with terminals through industrial interfaces so as to realize wireless communication between terminals and remote data center.

There are two types of industrial interface: serial port (RS232 and RS485) and I/O (digital input and digital output).

RS232 adopts full-duplex communication. It's generally used for communication within 20m.

RS485 adopts half-duplex communication to achieve transmission of serial communication data with distance up to 120m.

Digital input of I/O interface is a logical variable or switch variable with only two values of 0 and 1. "0" refers to low level and "1" refers to high level .

3.4.1 I/O

3.4.1.1 DI

This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.

Status	DI DO		
Network	DI Setting		
	Enable		
System 🕨	Mode	High Level 🔻	
	Duration(ms)	100	
Industrial 🔻	Action	SMS Email DO	Cellular UP
I/O	Save		
Serial Port	Jave		



DI	
Item	Description
Enable	Enable or disable DI.
Mode	Options are "High Level", "Low Level", and "Counter".
Duration (ms)	Set the duration of high/low level in digital input. Range: 1-10000.
Condition	Select from "Low->High", and "High-> Low".
Low->High	The counter value will increase by 1 if digital input's status changes from low level to high level.
High->Low	The counter value will increase by 1 if digital input's status changes from high level to low level.
Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration.
SMS	Check to enable SMS alarm.
Phone Group	Set phone group to receive SMS alarm.
SMS Content	Set the content of SMS alarm.
Email	Check to enable Email alarm.
Email Group	Set phone group to receive email alarm.
Email Content	Set the content of email alarm.
DO	Control output status of DO.
Cellular UP	Trigger the device to switch from offline mode to cellular network mode.

Table 3-4-1-1 DI Parameters

Related Topics

DO Setting

Email Setting

Connect on Demand

3.4.1.2 DO

This section describes how to configure digital output mode.

Status	Î	DI DO		
Network	•	DO Setting		
		Enable		
System	•	Mode	High Level	•
		Duration(*10ms)	100	
Industrial				
I/O		Save		



DO		
Item	Description	
Enable	Enable or disable DO.	
Mode	Select from "High Level", "Low Level", "Pulse" and "Custom" .	
Duration (*10ms)	Set duration of high/low level on digital output. Range: 1-10000.	
Initial Status	Select high level or low level as the initial status of the pulse.	
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.	
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.	
The Number of Pulse	Set the quantity of pulse. Range: 1-100.	
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.	

Table 3-4-1-2 DO Settings

Related Topics

DI Setting

3.4.2 Serial Port

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data center, so as to achieve two-way communication between serial terminals and remote data center.

Status	Serial		
Network	Serial Settings		
	Enable		
System	Serial Type	RS232	~
	Baud Rate	9600	~
Industrial	Data Bits	8bits	~
VO	Stop Bits	1bits	~
Serial Port	Parity	None	~
	Software Flow Control		
Modbus Slave	Serial Mode	Modbus Master	~
Modbus Master			
GPS	Save & Apply		

Figure 3-4-2-1

Serial Settings			
Item	Description	Default	
Enable	Enable or disable serial port function.	Disable	
Serial Type	RS232 or RS485 is optional.	RS232	
Baud Rate	Range is 300-230400. Same with the baud rate of the connected terminal device.	9600	
Data Bits	Options are "8" and "7". Same with the data bits of the connected terminal device.	8	
Stop Bits	Options are "1" and "2". Same with the stop bits of the connected terminal device.	1	
Parity	Options are "None", "Odd" and "Even". Same with the parity of the connected terminal device.	None	
Software Flow Control	Enable or disable software flow control.	Disable	
Serial Mode	Select work mode of the serial port. Options are "DTU Mode" , "Modbus Master", "Modbus Slave" and "GPS".	Disable	
DTU Mode	In DTU mode, the serial port can establish communication with the remote server/client.		
GPS	In GPS mode, go to "Industrial > GPS > GPS Serial Forwarding" to select corresponding Serial Type, then GPS data will be forwarded to this serial port.		
Modbus Master	In Modbus Master mode, go to "Industrial > Modbus Master" to configure basic parameters and channels.		
Modbus Slave	In Modbus Slave mode, go to "Industrial > Modbus Slave" to configure basic parameters.		

Table 3-4-2-1 Serial Parameters

Serial Mode	DTU Mode	•	
DTU Protocol	Transparent	v	
Protocol	ТСР	٣	
Keepalive Interval	75		s
Keepa <mark>live Retry Times</mark>	9		
Packet Size	1024		Bytes
Serial Frame Interval	100		ms
Reconnect Interval	10		s
Specific Protocol			
Register String			

Destination IP Address

Destination IP Address			
Server Address	Server Port	Status	Operation
			H

Figure 3-4-2-2

DTU Mode	DTU Mode			
ltem	Description	Default		
DTU Protocol	 Select from "None", "Transparent", "Modbus", "UDP server" and "TCP server". Transparent: the routed is used as TCP client/UDP and transmits data transparently. TCP server: the device is used as TCP server and transmits data transparently. UDP server: the device is used as UDP server and transmits data transparently. Modbus: the device will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP. 			
TCP/UDP Server				
Listening Port	Set the device listening port. Range: 1-65535.	502		
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600 in seconds.	75		
Keepalive Retry Times	When TCP heartbeat times out, device will resend heartbeat. After it reaches the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9		
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The size range is 1-1024. The unit is byte.	1024		
Serial Frame Interval	The interval that the device sends out real serial data stored in the buffer area to public network. The range is 10-65535, in	100		

milliseconds.	
Note: data will be sent out to public network when real serial data	
size reaches the preset packet size, even though it's within the serial	
frame interval.	

Table 3-4-2	2 DTU Parameters

Item	Description	Default
Transparent		
Protocol	Select "TCP" or "UDP" protocol.	ТСР
Keepalive Interval	After TCP client is connected with TCP server, the client will send	
· ·	heartbeat packet by TCP regularly to keep alive. The interval range	75
(s)	is 1-3600, in seconds.	
Keepalive Retry	When TCP heartbeat times out, the device will resend heartbeat.	
Times	After it reaches the preset retry times, device will reconnect to TCP	9
Times	server. The range is 1-16.	
Packet Size	Set the size of the serial data frame. Packet will be sent out when	1024
racket Size	preset frame size is reached. The range is 1-1024. The unit is byte.	1024
	The interval that the device sends out real serial data stored in the	
	buffer area to public network. The range is 10-65535, in	
Serial Frame	milliseconds.	100
Interval	Note: data will be sent out to public network when real serial data	100
	size reaches the preset packet size, even though it's within the	
	serial frame interval.	
Reconnect	After connection failure, device will reconnect to the server at the	10
Interval	preset interval, in seconds. The range is 10-60.	
Specific Protocol	By Specific Protocol, the device will be able to connect to the	
	TCP2COM software.	
Heartbeat	By Specific Protocol, the device will send heartbeat packet to the	
Interval	server regularly to keep alive. The interval range is 1-3600, in	30
	seconds.	
ID	Define unique ID of each device. No longer than 63 characters	
	without space character.	
Register String	Define register string for connection with the server.	Null
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null
Status	Show the connection status between the device and the server.	
Modbus		
Local Port	Set the device listening port. Range: 1-65535.	502
Maximum TCP	Specify the maximum number of TCP clients allowed to connect th	32
Clients	e device which act as a TCP server.	
Connection	If the TCP server does not receive any data from the slave device w	
Timeout	ithin the connection timeout period, the TCP connection will be bro	60
. inteedt	ken.	
Reading Interval	Set the interval for reading remote channels. When a read cycle end	100

	s, the new read cycle begins until this interval expires. If it is set to 0, the device will restart the new read cycle after all channels have been read.	
Response Timeout	Set the maximum response time that the device waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out.	3000
Maximum Retries	Set the maximum retry times after it fails to read.	3

Table 3-4-2-3 DTU Parameters

Related Configuration Example

DTU Application Example

3.4.3 Modbus Slave

This section describes how to achieve I/O status via Modbus TCP, Modbus RTU and Modbus RTU over TCP.

3.4.3.1 Modbus TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus TCP protocol.

Status	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network	Modbus TCP		
	Enable		
System	Port	502	
	DI Address	0	
Industrial 🔻	DO Address	0	
I/O			
	Save		
Serial Port			
Modbus Slave			



Modbus TCP			
ltem	Description	Default	
Enable	Enable/disable Modbus TCP.	Disable	
Port	Set the device listening port. Range: 1-65535.	502	
DI Address	Define the address of DI, range: 0-255.	0	
DO Address	Define the address of DO, range: 0, 2-255.	0	

Table 3-4-3-1 Modbus TCP Parameters

3.4.3.2 Modbus RTU

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU protocol.

Status	Modbus TCP	Modbus RTU	Modbus RTU Over TCP
Network 🕨	Modbus RTU		
	Enable		
System 🕨	Serial Port	serial	Ŧ
	Slave ID	1	
Industrial 🔻	DI Address	0	
I/O	DO Address	0	
Serial Port	Save		
Modbus Slave			

Figure 3-4-3-2

Modbus RTU					
Item	Description	Default			
Enable	Enable/disable Modbus RTU.	Disable			
Serial Port	Select the corresponding serial port.	serial			
Slave ID	Set slave ID is used for distinguishing different devices on the same link.	1			
DI Address	Define the address of DI, range: 0-255.	0			
DO Address	Define the address of DO, range: 0, 2-255.	0			

Table 3-4-3-2 Modbus RTU Parameters

3.4.3.3 Modbus RTU Over TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU over TCP.

Status		Modbus TCP	Modbus RTU	Modbus RTU Over TCP		
Network	٠	Modbus RTU Over T				
System	٠	Slave ID Device ID	1			
Industrial	•	Reconnect Interval	10	s		
VO		DI Address DO Address	0			
Serial Port			0			
Modbus Slave		Server List				
Modbus Master		IF	5	Port	Status	Operation
CDR						+

Figure 3-4-3-3

Modbus RTU Over TCP			
Item	Description	Default	
Enable	Enable/disable Modbus RTU over TCP function.	Disable	
Slave ID	Set slave ID is used for distinguishing different devices on the same link.	1	
Device ID	Set device ID. The server will get the device ID to the server for identifying identity so that the server can manage multiple devices.		
Reconnection Interval	The reconnection interval when the device and the server fails to establish connection or disconnected.	10	
DI Address	Define the address of DI, range: 0-255.	0	
DO Address	Define the address of DO, range: 0, 2-255.	0	
Server List			
IP	Enter the IP address of the server.		
Port	Enter the port of the server.Range: 0-65535.		
Status	Show the connection status between the device and t	he server.	
	Table 2.4.2.2 Madbue DTU Over TOD Dever store		

Table 3-4-3-3 Modbus RTU Over TCP Parameters

3.4.4 Modbus Master

UF51 can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

3.4.4.1 Modbus Master

You can configure Modbus Master's parameters on this page.

Status	Modbus Master	Channel	
Network 🕨	Modbus Master Setti	ng	
	Enable	*	
System 🕨	Read Interval	0	s
	Max. Retries	3	
Industrial 🔻	Max. Response Time	500	ms
VO	Execution Interval	50	ms
Serial Port	Channel Name		Read
Modbus Slave	Save & Apply		
Modbus Master			

Figure 3-4-4-1

Modbus Master			
Item	Description	Default	
Enable	Enable/disable Modbus master.		
Read Interval/s	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set to 0, the device will restart the new read cycle after all channels have been read. Range: 0-600.	0	
Max. Retries	Set the maximum retry times after it fails to read, range: 0-5.	3	
Max. Response Time/ms	Set the maximum response time that the device waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000.	500	
Execution Interval/ms	The execution interval between each command. Range: 10-1000.	50	
Channel Name	Select a readable channel form the channel list.		

Table 3-4-4-1

3.4.4.2 Channel

You can add the channels and configure alarm setting on this page, so as to connect the device to the remote Modbus Slave to poll the address on this page and receive alarms from the device in different conditions.

Modbus Ma	ster	Cha	nnel							
Channel Set	ting									
Channel Sett	ing									
Name	Slave ID	Addres s	Numbe r	Туре	Link	IP Address	Port	Sign	Decima I Place	Operation
	1	0	1	Holding R	TCP 🔻				0	×
										H



Channel Setting		
ltem	Description	
Name	Set the name to identify the remote channel. It cannot be blank.	
Slave ID	Set Modbus slave ID.	
Address	The starting address for reading.	
Number	The address number for reading.	
Туре	Read command, options are "Coil", "Discrete", "Holding Register (INT16)", "Input Register (INT16)", "Holding Register (INT32)" and "Holding Register (Float)".	

Link	Select TCP for transportation.
IP address	Fill in the IP address of the remote Modbus device.
Port	Fill in the port of the remote Modbus device.
Sign	To identify whether this channel is signed. Default: Unsigned.
Decimal Place	Used to indicate a dot in the read into the position of the channel. For example: read the channel value is 1234, and a Decimal Place is equal to 2, then the actual value is 12.34.

т	ah	le	3-4-4-2
	ab	IC.	J 4 4 Z

Name	tunnel1
Condition	GE(>)
Max. Threshold	0
Alarm	🕑 SMS 🛛 Email
Phone Group	
Email Group	,
Normal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get NORMAL data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
Abnormal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get ABERRANT data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
Continuous Alarm	

Figure 3-4-4-3

Alarm Setting	
ltem	Description
Name	Set the same name with the channel name to identify the remote channel.
Condition	The condition that triggers alert.
Min.	Set the min. value to trigger the alert. When the actual value is less
Threshold	than this value, the alarm will be triggered.
Max.	Set the max. value to trigger the alert. When the actual value is more
Threshold	than this value, the alarm will be triggered.
Alarm	Select the alarm method, e.g SMS.
SMS	The preset alarm content will be sent to the specified phone number.
Phone	Select the phone group to receive the alarm SMS.
Group	Select the phone group to receive the alarm SWS.
Email Group	Select the Email group to receive the alarm Email.
Normal	When the actual value is restored to the normal value from exceeding
Content	the threshold value, the device will automatically cancel the abnormal

	alarm and send the preset normal content to the specified phone group.
Abnormal Content	When the actual value exceeds the preset threshold, the device will automatically trigger the alarm and send the preset abnormal content to the specified phone group.
Continuous Alarm	Once it is enabled, the same alarm will be continuously reported. Otherwise, the same alarm will be reported only one time.

Table 3-4-4-3

TCP Forwading

Name	IP	Port	Operation
All 🔻			×

Figure 3-4-4-4

TCP Forwarding		
ltem	Description	
Name	The name of Modbus Master's channel.	
IP	The IP address of the server which the packets are forwarded to.	
Port	The port of the server's which the packets are forwarded to.	

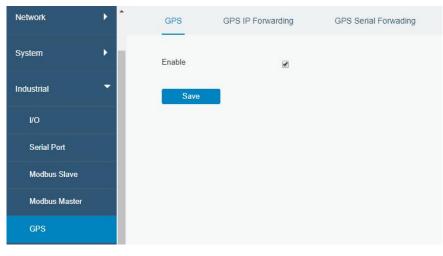
Table 3-4-4-4

3.4.5 GPS

This section give you a detailed introduction to GPS settings, including GPS IP forwarding and GPS serial forwarding.

3.4.5.1 GPS

When you want to receive GPS data, you should enable GPS function on this page.





Milesight Miles

Milesight IoT

3.4.5.2 GPS IP Forwarding

GPS G	GPS IP Forwarding		erial Forwading
Enable			
Туре	Client	Ŧ]
Protocol	TCP Protocol	۲]
Keepalive Interval	75		s
Keepalive Retry	9		times
Reconnect Interval	10		s
Report Interval	30		s
Include RMC			-
Include GSA			
Include GGA			
Include GSV			
Message Prefix]
Message Suffix			

GPS IP forwarding means that GPS data can be forwarded over the Internet.

Figure 3-4-5-2

Destination IP Address			
Server Address	Server Port	Status	Operation
			æ

Figure 3-4-5-3

GPS IP Forwarding				
Item	Description	Default		
Enable	Forward the GPS data to the client or server.	Disable		
Туре	Select connection type of the device. The options are "Client" and "Server".	Client		
Protocol	Select protocol of data transmission. The options are "TCP" and "UDP".	ТСР		
Keepalive Interval	After it's connected with server/client, the device will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600, in seconds.	75		
Keepalive Retry	When TCP heartbeat times out, the device will resend heartbeat. After it reaches the preset retry times, device will reconnect to TCP server. The range is 1-16.	9		
Local Port	Set the device listening port. Range: 1-65535.			
Reconnect Interval	After connection failure, device will reconnect to the server at the preset interval, in seconds. The range is 10-60.	10		

Milesight IoT	
---------------	--

Report Interval	device will send GPS data to the server/client at the preset interval, in seconds. The range is 1-60.		
Include RMC	Whether include RMC in GPS data.		
Include GSA	Whether include GSA in GPS data.		
Include GGA	Whether include GGA in GPS data.		
Include GSV	Whether include GSV in GPS data.		
Message Prefix	Add a prefix to the GPS data.	Null	
Message Suffix	Add a suffix to the GPS data.		
Destination IP A	ddress		
Server Address	Fill in the server address to receive GPS data (IP/domain name).		
Server Port	Fill in the port to receive GPS data. Range: 1-65535.		
	Show the connection status between the device and the server.		

Table 3-4-5-1 GPS IP Forwarding Parameters

3.4.5.3 GPS Serial Forwarding

GPS IP forwarding means that GPS data can be forwarded to the serial port.

GPS	GPS GPS IP Forwarding		Forwading
GPS Serial F	Forwading		
Enable			
Serial Type		Serial	~
Tra <mark>p In</mark> terval		30	
Include RMC			
Include GSA			
Include GGA			
Include GSV			



GPS Serial Forwarding				
Item	Description	Default		
Enable	Forward the GPS data to the preset serial port.	Disable		
Serial Type	Select the serial port to receive GPS data. Serial			
Report Interval	The device will forward the GPS data to the serial port at the preset interval, in seconds. The range is 1-60.	30		
Include RMC	Whether include RMC in GPS data.			

Include GSA	Whether include GSA in GPS data.	
Include GGA	Whether include GGA in GPS data.	
Include GSV	Whether include GSV in GPS data.	

Table 3-4-5-2 GPS Serial Forwarding Parameters

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping, traceroute, packet analyzer and qxdmlog.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

System	•	Ping	Traceroute	Packet Analyzer	Qxdmlog
Industrial	•	IP Ping			Ping Stop
Maintenance	-	TIOSE			Ping Stop
Tools					

Figure 3-5-1-1

PING	
Item	Description
Host	Ping outer network from the device.

Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Ping	Traceroute	Packet Analyzer	Qxdn	nlog
Traceroute Host			Trace	Stop
		Figure 3-5-1-2		
Traceroute				
Item	Descript	ion		
Host	Address	Address of the destination host to be detected.		
	Table 3.	5-1-2 Traceroute Parameter	c	

Table 3-5-1-2 Traceroute Parameters

3.5.1.3 Packet Analyzer

Packet Analyzer is used for capturing the packet of different interfaces.

Ping	Traceroute	Packet Analyzer	Qxdmlog
Packet Ana	alyzer		
Ethernet Int	erface	Any	T
IP Address			
Port			
Advanced			
Start	Stop	Download	

Figure 3-5-1-3

Packet Analyzer		
Item	Description	
Ethernet Interface	Select the interface to capture packages.	
IP Address	Set the IP address that the device will capture.	
Port	Set the port that the device will capture.	
Advanced	Set the rules for sniffer. The format is tcpdump.	

Table 3-5-1-3 Packet Analyzer Parameters

3.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.



3.5.2 Debugger

3.5.2.1 Cellular Debugger

This section explains how to send AT commands to device and check cellular debug information.

Cellular Debugger	Firewall Debugger		
Cellular Debugger			
Command	Eg: AT+CGREG? Send		
View Recent Logs (lines)	20 •		
Result	2020-05-08 19:23:38: [SEQ2,ID2]<<< OK 2020-05-08 19:23:38: [SEQ3,ID3]>>> ATE0 2020-05-08 19:23:38: [SEQ3,ID3]<<< ATE0	Manual Refresh V	Refresh

Figure 3-5-2-1

Cellular Debugger		
Item	Description	
Command	Enter the AT command that you want to send to cellular modem.	
View Recent Logs (lines)	View the specified lines of the result.	
Result	Show the response result from cellular modem.	
	Table 2 E 2 1 Callular Daburrar Devenators	

Table 3-5-2-1 Cellular Debugger Parameters

3.5.2.2 Firewall Debugger

This section explains how to send commands to device and check firewall information.

Cellular Debugger	Firewall Debugger
Firewall Debugger	
Command	Eg: -t nat -nvL INPUT Send
Result	
	Clear Log Download

Figure 3-5-2-2

Firewall Debugger	
Item	Description
Command	Enter the iptables command to send to check firewall information.
Result	Show the response result from firewall module.

Table 3-5-2-2 Firewall Debugger Parameters

3.5.3 Log

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

3.5.3.1 System Log

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

/iew recent(lines)		20 🔻		
Fri May 8 19:32:32	2020 daemon.debug vt	ysh_ubus[1631]: ubus_lib.c:428 call com	mand 'end'	
		3107]: finish yruo_log.get		2.67
Fri May 8 19:32:35	2020 user.info : Failed t	o open GPS device.		
Fri May 8 19:32:35	2020 user.info : STA	RT COLLECTION		
Fri May 8 19:32:36	2020 user.debug httpd[3107]: ==call yruo_log.get		
Fri May 8 19:32:36	2020 daemon.debug vt	ysh_ubus[1631]: ubus_lib.c:428 call com	mand 'end'	1111
Fri May 8 19:32:37	2020 user.debug httpd[3107]: finish yruo_log.get		
Fri May 8 19:32:38	2020 daemon.info dhcli	ent: No DHCPOFFERS received.		
Fri May 8 19:32:38	2020 daemon.info dhcli	ent: No working leases in persistent data	abase - sleeping.	
Fri May 8 19:32:40	2020 user.info : Failed t	o open GPS device.		
Fri May 8 19:32:40	2020 user.info : STA	RT COLLECTION		
Fri May 8 19:32:42	2020 user.debug httpd[3107]: ==call yruo_log.get		
Fri May 8 19:32:42	2020 daemon.debug vt	ysh_ubus[1631]: ubus_lib.c:428 call com	imand 'end'	*

Figure 3-5-3-1

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

Table 3-5-3-1 System Log Parameter

3.5.3.2 Log Download

This section describes how to download log files.

System Log	Log Download	Log Settings		
Download				Developed All
				Download All
File	Name	File Size/KB	Creation Time	Operation
vpr	n.log	1	2020/04/30 14:37:55	.↓
syste	m.log	872	2020/05/08 19:35:03	.↓
http	d.log	645	2020/05/08 19:34:12	↓
firew	all.log	0	2020/04/30 14:37:09	↓
cellu	lar.log	1619	2020/05/08 19:35:01	.↓

Figure 3-5-3-2

Log Download	
Item	Description
Download All	Download all log files.

File Name	Show the name of log files.
File Size/KB	Show the size of log files.
Creation Time	Show the creation time of log files.
Operation	Click to download every log file.
	Table 3-5-3-2 System Log Parameter

3.5.3.3 Log Settings

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

Log Download		Log Settings		
]
	514]
	Local		v]
	2048			KB
	Debug	1		1
	Log Download	514 Local 2048	514 Local 2048	□ 514 Local ▼ 2048

Figure 3-5-3-3

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

Table 3-5-3-3 Log Settings Parameters

3.5.4 Upgrade

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

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

Upgrade			
Upgrade			
Firmware Version	76.2.0.2		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade

Figure 3-5-4-1

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

Table 3-5-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.5.5 Backup and Restore

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

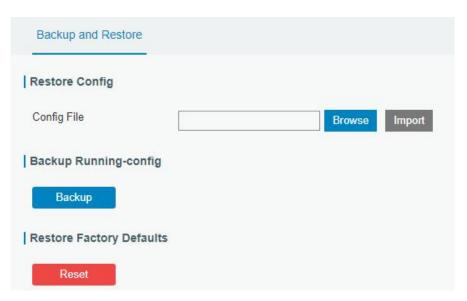


Figure 3-5-5-1

Backup and Restore		
Description		
Click "Browse" button to select configuration file, and then click		
"Import" button to upload the configuration file to the device.		
Click "Backup" to export the current configuration file to the PC.		
Click "Reset" button to reset factory default settings. UF51 will		
restart after reset process is done.		

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

Related Configuration Example

Restore Factory Defaults

3.5.6 Reboot

On this page you can reboot the device immediately or regularly. We strongly recommend clicking "Save" and "Apply" button before rebooting the device so as to avoid losing the new configuration.

Reboot					
Reboot Device					
Reboot Now					
Schedule					
Enable					
Cycles	Every Day	¥	0	: [0
	Every Day Every Week				
Save	Every Month				



Reboot		
Item	Description	
Reboot Now Reboot the device immediately.		
Schedule		
Enable	Reboot the device at a scheduled frequency.	
Cycles	Select the date and time to execute the schedule.	
Table 3-5-2-1 Schedule Parameters		

3.6 APP

3.6.1 Python

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

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

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

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

3.6.1.1 Python

Python	AppMana	ager Configuration	Python Al	pp	
Python					
AppManager S	Status	Uninstalled			
SDK Version					
SDK Path					
Available Store	age	eMMC	~		
SDK Upload				Browse	Install

Figure 3-6-1-1

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

Table 3-6-1-1 Python Parameters

3.6.1.2 App Manager Configuration

Python	AppManager Configuration	Python APP	
AppManager			
Enable			
App Management	:		
ID	App Command	Logfile Size(MB)	Uninstall
App Status			
Ap	op Name	App Version	SDK Version



AppManager Configuration		
Item	Description	
Frabla	After enabling Python AppManager, user can click "View" button on the	
Enable	"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	DK Version Show the SDK version which the imported App is based on.	

Table 3-6-1-2 APP Manager Parameters

3.6.1.3 Python App

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



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 3-6-1-3 APP Parameters

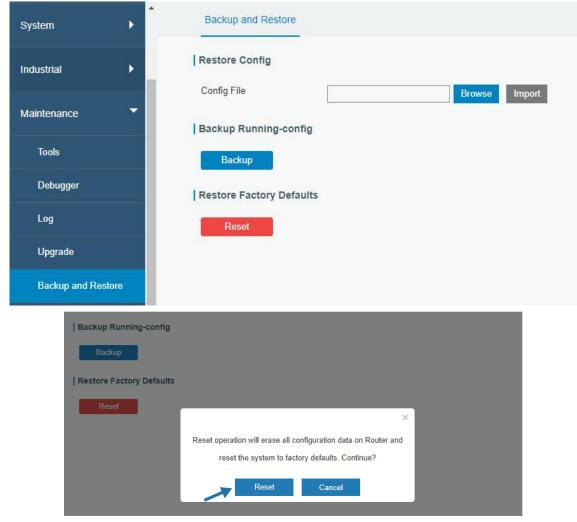
Chapter 4 Application Examples

4.1 Restore Factory Defaults

4.1.1 Via Web Interface

- 1. Log in web interface, and go to "Maintenance > Backup and Restore".
- 2. Click "Reset" button under the "Restore Factory Defaults".

You will be asked to confirm if you'd like to reset it to factory defaults. Then click "Reset" button.



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

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

Please wait till the STATUS LED blinks slowly and login page pops up again, which means the device has already been reset to factory defaults successfully.

Related Topic

Restore Factory Defaults

4.1.2 Via Hardware

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

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

4.2 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade device firmware. 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 device will check if the firmware file is correct. If it's correct, the firmware will be imported to the device, and then the device will start to upgrade.

Note: It is recommended to check the box of Reset Configuration to Factory Default before upgrade.

Upgrade			
Upgrade			
Firmware Version	76.2.0.2		
Reset Configuration to Factory Default			
Upgrade Firmware		Browse	Upgrade

Related Topic

Upgrade

4.3 Events Application Example

Example

In this section, we will take an example of sending alarm messages by email when the following events occur and recording the event alarms on the Web GUI.

Events	Actions to make events occur (for test)
UF51 system start up.	Plug the power supply of the router.
UF51 system time update.	Set up system time manually.

Configuration Steps

- 1. Go to "System > Events > Events Settings" and enable Event settings.
- 2. Check corresponding events for record and email alarm, and then click "Save" button as below.

Events	Events Settings				
Events Settings					
Enable					
Phone Group List			•		
Email Group List	1		T		
Ever	nts	Record	Email Email Setting	SMS SMS Setting	SNMP
System S	Startup				
System F	Reboot				
System Tim	e Update				

3. Configure the corresponding parameters including email sending settings and email groups as below. Click "Save" and "Apply" button to make the changes take effect.

General	System Time	Email	Storage
SMTP Client Settin	gs		
Enable			
Email Address	contact@milesig	ght.com	
Password	•••••		
SMTP Server Addres	s smtp.milesight.c	com	
Port	25		
Encryption	STARTTLS	~	
Test			

Email List				
	Email Address		Description	Operation
	iot.contact@milesight.com		support	×
				Đ
Email Group	o List			
	Group ID	Description	Email Address	Operation
	1	support	iot.contact@milesight.com	2 ×
				H

4. To test the functionality of Alarm, please take the corresponding actions listed above. It will send an alarm e-mail to you when the relevant event occurs.

Refresh the web GUI, go to "Events > Events", and you will find the events records.

Events	Events Settin	gs		
Mark as Read	Delete	Mark All as Read	Delete All Alarms	
	Status	Туре	Time	Message
	Unread	System Time Update	2019-05-15 09:39:08	system time update
	Unread	System Startup	2019-05-09 11:48:25	system startup
< 1 > 10	Go to:	GO		

Related Topics

Events

Email Setting

4.4 SNMP Application Example

Before you configure SNMP parameters, please download the relevant "MIB" file from the UF51's WEB GUI first, and then upload it to any software or tool which supports standard SNMP protocol. Here we take "ManageEngine MibBrowser Free Tool" as an example to access the device to query cellular information.

1. Go to "System > SNMP > MIB" and download the MIB file "LTE-ROUTER-MIB.txt" to PC.

System 🔻	SNMP	MIB View	VACM	Тгар	MIB	
General Settings	MIB Downloa	ad				
Phone & SMS	MIB File		LTE-ROU	ITER-MIB.b 🔻	Download	
User Management						
SNMP						
АЛА						

2. Start "ManageEngine MibBrowser Free Tool" on the PC. Click "File > Load MIB" on the menu bar. Then select "LTE-ROUTER-MIB.txt" file from PC and upload it to the software.

HarageEngine MibBron File Edit View Operations		🏹 🕸 🛅	🛫 🔤 🧕	b 🖬 🔒 🚝) 🧇	Download More Free Tools	× נ
♣ Loaded MibModules	Community	localhost	~	Port Write Community	161		~
	Set Value Device Type Device Type Ider Suggested OIDs	ntified Not Available None	~		~	C Reload	
	Object ID	led: Jsers\Ursalink\Desktop\L		D tvt			^
	Loading MIBs Fail						~

Click the "+" button beside "LTE-ROUTER-MIB", which is under the "Loaded MibModules" menu, and find "usCellularinfo". And then you will see the OID of cellular info is ".1.3.6.1.4.1.50234", which will be filled in the MIB View settings.

ManageEngine MibBrowser Free Tool							
<u>File Edit View Operations Help</u>							
🗞 🍓 🗉 🚳 🤷 🐚 📾 🦛	🔊 🔨 🖄	III 👹	e 🛫 🚥	@ 🔁	日 🔁 🖉	Oownload More Free Tools	
Loaded MibModules	Host Community Set Value Device Type – Device Type Id Suggested OIE Object ID Loading MIBs Fa Loading MIBs C Loading MIBs C Done.	Ds N net.privat ailed: :\Users\Urs ailed:	Available None .e. enterprise salink/Deskto	p\LTE-ROU	TER-MIB.txt	161 C Rela	
% rtCelluarNetPr % rtCelluarNetTy % rtCelluarNetw(% rtCelluarNetw(Description Mu Syntax Access	ultiVer			Status Reference		
<	Index Object ID	1.3.6.1.4.	1. 50234. 1. 1	3			
Global View 🗌	Description						

3. Go to "System > SNMP > SNMP" on the device's WEB GUI. Check "Enable" option, then click "Save" button.

SNMP	MIB View	VACM	Trap	MIB
SNMP Setting	gs			
Enable				
Port		161		
SNMP Versior	1	SNMPv2		~
Location Inform	mation	Xiamen_C	China	
Contact Inform	nation	Xiamen_N	Ailesight	
	-			
Save				

4. Go to "System > SNMP > MIB View". Click + to add a new MIB view and define the view to be accessed from the outside network. Then click "Save" button.

	View Name		View Filter	View	OID	Operation
cellular		Included	3	• 1.3.6.1.4.1.502	34.1.3	×
						H

5. Go to "System > SNMP > VACM". Click 🛨 to add a new VACM setting to define the access authority for the specified view from the specified outside network. Click "Save" and "Apply" to make the changes take effect.

NMP v1 & v2	2 User List					
Con	nmunity	Permission	ı	MIB View	Network	Operation
public		Read-Write	•	cellular	▼ 0.0.0.0/0	

6. Go to MibBrowser, enter host IP address, port and community. Right click "usCellular CurrentSim"

and then click "FET". Then you will get the current SIM info on the result box. You can get other cellular info in the same way.

ManageEngine MibBrowser Free Tool <u>File Edit V</u> iew <u>Operations H</u> elp										-		×
🗞 🎂 🗈 ጰ 🖻 🖷 🗊 ;	🔊 🔨 🖄		۱	STOP	@ ₀] -		3 <		O Mo	Download re Free Tool:	S	
aded MibModules	Host Community Set Value		68.22.225 ●●●●	5	public	100000000 11	Commun		161			~
ArrouterInfos ArrouterInfo ArrouterInfo	Device Type	Device Type Device Type Identified Not Available C Reload Suggested OIDs None										
rtCellularModel	Object ID	. i so. or	rg. <mark>dod</mark> . int	ternet.	private.	enterpris	es.ltero	outer	. <mark>rt</mark> Route	Managemen	t.rtRou	terIn
	Loading MIBs Failed: Loading MIBs C:\Users\Ursalink\Desktop\LTE-ROUTER-MIB.bt Done. Sent GET request to 192.168.22.225 : 161						^					
	rtCellularCurr	entSim.0		Res	sult							~
rtCelluarNetProvider	Description	MultiVar										
rtCelluarNetworkStat	Syntax	OCTET ST	RING			State	us c	urre	nt			
rtCelluarNetworkNeti	Access	read-onl	у			Refe	erence					
< >>	Object ID		. 4. 1. 5023			ar						
Global View	Description	The c	current	SIM ca	ard used							

Related Topic

<u>SNMP</u>

4.5 Network Connection

4.5.1 Cellular Connection

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

Status	Link Failover	Cellular	Port	WAN	Bridge	WLAN
Network 👻	Cellular Settings					
Interface	Protocol Type		IPv4		~	
DHCP	Username					
Firewall	Password					
QoS	PIN Code					
VPN	Access Number Authentication Type		Auto		~	
IP Passthrough	Network Type		Auto		~	
Routing	PPP Preferred					
VRRP	SMS Center					
DDNS	Enable NAT Roaming					

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

2. Go to "Network > Interface > Link Failover" to enable correspond SIM and change link priority.

Status	Link Failover	Cellular	Port	WAN	Bridge	WLAN	Switch	Loopback
Network	Link Priority							
Interface	Priority	Enable Rule	Link in use	Interface	Connec	ction Type	IP	Operation
DHCP	1		•	Cellular	DI	HCP	10.2.25.72	
Firewall	2		٠	WLAN-2.4G	DI	HCP	192.168.3.147	
QoS	3		۰	WAN	s	tatic	192.168.22.213	
VPN								

3. Click \square to configure ICMP ping detection information.

Enable		
IPv4 Primary Server	8.8.8.8	
IPv4 Secondary Server	114.114.114.114	
IPv6 Primary Server	2001:4860:4860::8888	
IPv6 Secondary Server	2400:3200::1	
Interval	300	s
Retry Interval	5	s
Timeout	3	s
Max Ping Retries	3	

4. Check the cellular connection status by WEB GUI of device.

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

Status		Overview	Cellular	Network	WLAN	VPN	N Routing	Но	ost List	GPS
Network	•	Modem					Network			
		Status		Ready			Status		Connected	
System	×.	Model		RG500Q-EA			IPv4 Address		10.2.25.72/2	8
		Version		RG500QEAAAR11A	02M4G		IPv4 Gateway		10.2.25.73	
Industrial	•	Signal Level		30asu (-53dBm)			IPv4 DNS		0.0.0.0	
Maintenance	•	Register Status		Registered (Home ne	etwork)		IPv6 Address		fe80::7446:7	3ff:fe43:364d/64
		IMEI		866897040051965			IPv6 Gateway			
APP	•	IMSI		460045927703652			IPv6 DNS			
		ICCID		89860439101880723	3652		Connection Duration		1 days, 21:2:	3:34
		ISP		CHINA MOBILE			Data Usage Monthly	,		
		Network Type		5G NR						
		PLMN ID		46000			RX		16.3 MiB	
		LAC		592F			TX		16.4 MiB	Manual Refresh V Refresh
		0.00		374046			ALL		32.8 MiB	

5. Check out if network works properly by browser on PC.

Open your preferred browser on PC, type any available web address into address bar and see if it is able to visit Internet via the UF51 device.

Related Topic

Cellular Setting Cellular Status

4.5.2 Ethernet WAN Connection

Example

WAN port of the UF51 is connected with Ethernet cable to get Internet access.

Configuration Steps

1. Go to "Network > Interface > WAN" to select connection type and configure WAN parameters.

Status	Link Failover	Cellular	Port	WAN	Bridge	WLAN
Network 🗸	WAN Settings					
Interface	— WAN_1					
DHCP	Enable					
Firewall	Port			LAN1/WAN		
QoS	Connection Type			Static IP 192.168.22.213	~	
VPN	Netmask			255.255.255.0		
IP Passthrough	IPv4 Gateway			192.168.22.1		
Routing	IPv6 Address			fe80::26e1:24ff.f	ef1:e38d	
VRRP	Prefix Length			64		
DDNS	IPv6 Gateway]	
	МТО			1500		
System	IPv4 Primary DN	S		114.114.114.114		
	IPv4 Secondary	DNS		3.3.3.3		
Industrial >	IPv6 Primary DN	S				
Maintenance •	IPv6 Secondary	DNS				
	Enable NAT					

Note: if you select PPPoE type, please check the "Username" & "Password" with your local ISP. Click "Save & Apply" button to make the changes take effect.

2. Go to "Network > Interface > Link Failover" to change the WAN priority to 1.

L	ink Failover	Cellular	Port	WAN Bridge	WLAN Sw	itch Loopback	
Lir	nk Priority						
	Priority	Enable Rule	Link in use	Interface	Connection Type	IP	Operation
	1		•	WAN	Static	192.168.22.213	
	2		٠	Cellular	DHCP	10.2.25.72	
	3			WLAN-2.4G	DHCP	192.168.3.147	

Related Topic

WAN Setting

WAN Status

4.6 Wi-Fi Application Example

4.6.1 AP Mode

Application Example

Configure UF51 as AP to allow connection from users or devices.

Configuration Steps

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN
WLAN1-2.4G					
Enable					
Work Mode	AP	a.	~		
BSSID	24:6	e1:24:f0:d9:40			
Radio Type	802	2.11n(2.4GHz)	~		
Channel	Aut	0	~		
Bandwidth	201	MHz	~		
SSID	Rou	iter_F0D940			
Encryption Mode	WF	A-PSK/WPA2-PSI	< v		
Cipher	Aut	0	~		
Key	•••••	••••			
SSID Broadcast					
AP Isolation					
Guest Mode					

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

 Use a smart phone to connect the access point of UF51. Go to "Status > WLAN", and you can check the AP settings and information of the connected client/user.

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GP
WLAN Status							
Name	Status	Туре	SSID	IP A	Address	Netmask	
WLAN1	Running	AP	Router_F0D940	192.	168.10.1	255.255.255.0	
WLAN2	Running	AP	Router_F0D941	192.168.10.1		255.255.255.0	
Associated Static	ons						
SSI	SSID M		MAC Address		ess	Connection Duration	n
Router_F	Router_F0D940		3c:cd:5d:47:10:8e		0.100	6 seconds	

4.6.2 Client Mode

Application Example

Configure UF51 as Wi-Fi client to connect to an access point to have Internet access.

Configuration Steps

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

Link Failover	Cellular	Port	WAN	Bridge	WLAN
WLAN1-2.4G					
Enable					
Work Mode	Clie	ent	~	Scan	
SSID	WIF	I TEST			
BSSID	3C:	CD:5D:47:10:8E			
Encryption Mode	WF	PA2-PSK	~		
Cipher	AE	S	~		
Key	•••••				
IP Setting					
Protocol	DH	CP Client	~		

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

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

Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
WLAN Status							
Name	Status	Туре	SSID	IP A	Address	Netmask	
WLAN1	Connected	Client	WIFI TEST	192.1	168.43.10	255.255.255.0	
WLAN2	Running	AP	Router_F0D941	192.	168.10.1	255.255.255.0	
Associated Static	ons						
SSI	D	MAC Ad	ldress	IP Addro	ess	Connection Duration	n
WIFI T	EST	3c:cd:5d:4	17:10:8e	192.168.43.1		3 seconds	

Related Topic

WLAN Setting

WLAN Status

4.7 VRRP Application Example

Application Example

A Web server requires Internet access through the UF51 device. To avoid data loss caused by device breakdown, two UF51 devices can be deployed as VRRP backup group, so as to improve network reliability.

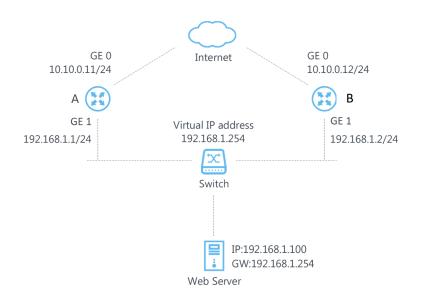
VRRP group:

WAN ports of the UF51 A and UF51 B are connected to the Internet via wired network. And LAN ports of them are connected to a switch.

Virtual IP is 192.168.1.254/24.

UF51 CPE	Virtual Router ID (Same for A and B)	Port connected with switch	LAN IP Address	Priority	Preemption Mode
А	1	LAN2	192.168.1.1	110	Enable
В	1	LAN2	192.168.1.2	100	Disable

Refer to the topological below.



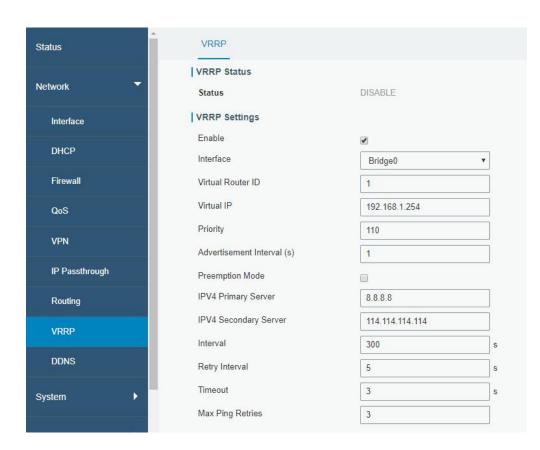
Configuration Steps

A Configuration

1. Go to "Network > Interface > WAN" and configure wired WAN connection as below.

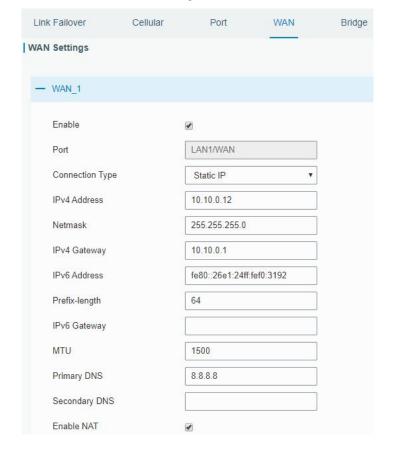
Link Failover	Cellular	Port	WAN	Bridge
WAN Settings			0	
— WAN_1				
Enable				
Port		LAN1/WAN		
Connection Type	1	Static IP	•	
IPv4 Address		10.10.0.11		
Netmask		255.255.255.0		
IPv4 Gateway		10.10.0.1		
IPv6 Address		fe80::26e1:24ff:	fef0:3192	
Prefix-length		64		
IPv6 Gateway				
MTU		1500		
Primary DNS		8.8.8.8		
Secondary DNS				
Enable NAT				

2. Go to "Network > VRRP > VRRP" and configure VRRP parameters as below.



B Configuration

1. Go to "Network > Interface > WAN" and configure wired WAN connection as below.



Status	VRRP		
Network 🗸	Status	DISABLE	
Network	VRRP Settings		
Interface	Enable		
DHCP	Interface	Bridge0	•
UHCP	Virtual Router ID	1	
Firewall	Virtual IP	192.168.1.254	
QoS	Priority	100	
VPN	Advertisement Interval (s)	1	
	Preemption Mode		
IP Passthrough	IPV4 Primary Server	8.8.8.8	
Routing	IPV4 Secondary Server	114.114.114.114	
VRRP	Interval	300	s
	Retry Interval	5	s
DDNS	Timeout	3	s
System 🕨	Max Ping Retries	3	

2. Go to "Network > Link Failover > VRRP" and configure VRRP parameters as below.

Once you complete all configurations, click "Apply" button on the top-right corner to make changes take effect.

Result: normally, A is the master device, used as the default gateway. When the power of UF51 A is down or UF51 A suffers from failure, UF51 B will become the master device, used as the default gateway. With Preemption Mode enabled, UF51 A will be master and UF51 B will demote back to be the backup once UF51 A can access the Internet again.

Related Topics

VRRP Setting

4.8 NAT Application Example

Example

UF51 can access Internet via cellular. LAN port is connected with a Web server whose IP address is 192.168.1.2 and port is 8000. Configure the device to make public network access the server.

Configuration Steps

Go to "Firewall > Port Mapping" and configure port mapping parameters.

Milesight

		For your device security, please	e change the default password!		
Status	Security ACL	Port Mapping 2 DMZ	MAC Binding	Custom Rules	SPI
Network 🔫	Port Mapping				
Interface	Source IP	Source Port Destination IP	Destination Port Protocol	Description	Operation
DHCP	3 0.0.0/0	8000 192.168.1.2	800 TCP 🗸		
Firewall (1)					æ
QoS	Save (4)				

Click "Save" and "Apply" button.

Related Topic

Port Mapping

4.9 Access Control Application Example

Application Example

LAN port of the UF51 is set with IP 192.168.1.0/24. Then configure the device to deny accessing to Google IP 172.217.160.100 from local device with IP 192.168.1.12.

Configuration Steps

1. Go to "Network > Firewall > ACL" to configure access control list. Click "+" button to set

parameters as below. Then click "Save" button.

Security	ACL	Port Mapping	DMZ	MAC Binding	Cu	stom Rules	SPI
ACL Setting							
Default Filter Po	licy	Accept	•				
Access Contro	ol List						
		Туре	[extended	×		
		ID	[100			
		Action	[deny	¥		
		Protocol	[ip	Ŧ		
		Source IP	[192.168.1.12			
		Source Wildcard Mask	[0.0.0.255			
		Destination IP	[172.217.160.100			
		Destination Wildcard Mas	k [0.0.0.255			
		Description	[google			
		Sa	ive	Cancel			

(5) Apply

2. Configure interface list. Then click "Save" and "Apply" button.

Securi	ty	ACL	Port	Mapping	DMZ	MAC Binding	Custom Rules	SPI
ACL Se	Filter Po		Accep	t	•			
Access	Contro	ol List						
ID	þ	Action	Protocol	Source IP	Destination IF	More Detail	Description	Operation
10	0	deny	ip	192.168.1.12/0.0.0. 255	172.217.160.100 0.0.255	/0.	google	×
								8
Interfac	e List							
		Interface		In /	ACL	C	out ACL	Operation
В	Bridge0		¥	100	¥		¥	×

Related Topic

<u>ACL</u>

4.10 QoS Application Example

Example

Configure the UF51 to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

Note: the "Total Download Bandwidth" should be less than the real maximum bandwidth of WAN or cellular interface.

FTP Server IP & Port	Percent	Max Bandwidth(kbps)	Min Bandwidth(kbps)
110.21.24.98:21	40%	30000	25000
110.32.91.44:21	60%	45000	40000

Configuration Steps

1. Go to "Network > QoS > QoS(Download)" to enable QoS and set the total download bandwidth.

Download Bandwidth	n	
Enable		
Default Category]
Download Bandwidth	75000	kbits/s
Capacity	·	1

2. Please find "Service Category" option, and click "
"
to set up service classes.

Note: the percents must add up to 100%.

Name	Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
	40	30000	25000	
	60	45000	40000	×

3. Please find "Service Category Rules" option, and click "+" to set up rules.

Service Category Rules

Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Category	Operation
ftp1	110.21.24.98	21			ANY •	1 •	×
ftp2	110.32.91.44	21			ANY 🔻	2 •	×

Note:

IP/Port: null refers to any IP address/port.

Click "Save" and "Apply" button.

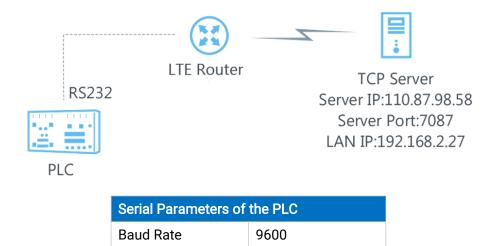
Related Topic

QoS Setting

4.11 DTU Application Example

Example

PLC is connected with the UF51 via RS232. Then enable DTU function of the UF51 to make a remote TCP server communicate with PLC. Refer to the following topological graph.



Data Bit	8
Stop Bit	1
Parity	None

Configuration Steps

1. Go to "Industrial > Serial Port > Serial" and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.

Status		Serial		
Network	×	Serial Settings		
		Enable		
System	۲	Serial Type	RS232	~
	_	Baud Rate	9600	~
Industrial		Data Bits	8bits	~
<i>l</i> /O		Stop Bits	1bits	~
Serial Port		Parity	None	~
		Software Flow Control		

2. Configure Serial Mode as "DTU Mode". The UF51 is connected as client in "Transparent" protocol.

System	ľ.	Serial Mode	DTU Mode	•
Industrial	-	DTU Protocol	Transparent	•
		Protocol	ТСР	•
I/O		Keepalive Interval	75	s
Serial Port		Keepalive Retry Times	9	
Modbus TCP		Packet Size	1024	Bytes
		Serial Frame Interval	100	ms
GPS		Reconnect Interval	10	s
Maintenance		Specific Protocol		
		Register String	modem1	

3. Configure TCP server IP and port.

Server Address	Server Port	Status	Operatio
110.87.98.58	7087		×
			Ŧ

4. Once you complete all configurations, click "Save" and "Apply" button.

Destination IP Address			
Server Address	Server Port	Status	Operation
110.87.98.58	7087	Connected	×

5. Start TCP server on PC.

Take "Netassist" test software as example. Make sure port mapping is already done.

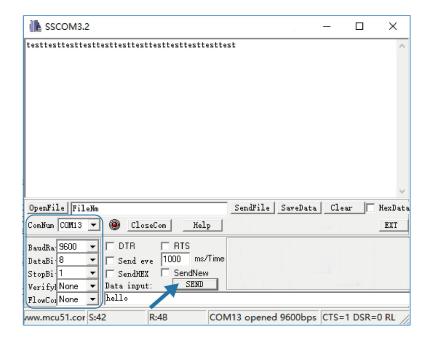
	Protocol Server		7
2)	Local host	IP	
192	.168.2	. 2	7
3) 7087	Local host	por	
		nne	

6. Connect the UF51 to PC via RS232 for PLC simulation. Then start "sscom" software on the PC to test communication through serial port.

ComNum	COM9	•	0	Close	Com
BaudRa	9600	•	D	TR	
DataBi	8	-	∏ Se	nd eve	100
StopBi	1	-	∏ Se	endHEX	Г
Verifyl	None	-	Data	input:	[
FlowCon	None	•	hellI	.0	
				0	

7. After connection is established between the UF51 and the TCP server, you can send data between sscom and Netassit.

PC side



TCP server side

₽ • /	NetAssist (V3.7)
Settings	Data Receive
(1) Protocol	【Receive from 220.249.163.119 : 19049】:
TCP Server 🗾	ursalink_modem1hellohellohellohellohellohellohellohell
(2) Local host IP 192.168, 2, 27	
(3) Local host por 7087	
-@-Disconnect	
Recv Options	
🔽 Receive to file	
🗌 Add line return	
🔲 Receive As HEX	
🗖 Receive Pause	
<u>Save</u> <u>Clear</u>	
Send Options	
🔽 Data from file	
🔲 Auto Checksum	
🗌 Auto Clear Input	
🗌 Send As Hex	
🥅 Send Cyclic	Peers: All Connections -
Interval 1000 ms	test
Data from file Auto Checksum Auto Clear Input Send As Hex Send Cyclic Interval 1000 ms Load Clear	Send
🍯 Ready!	Send : 208 Recv : 177 Reset

8. After serial communication test is done, you can connect PLC to RS232 port of the UF51 for test.

Related Topic

Serial Port

4.12 PPTP Application Example

Example



Configure the UF51 as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.

Configuration Steps

1. Go to "Network > VPN > PPTP", configure PPTP server IP address, username and password provided by PPTP server.

Note: If you want to have all data transferred through VPN tunnel, check "Global Traffic Forwarding" option.

DMVPN	IPsec	GRE	L2TP	PPTP
Certifications				
PPTP Settings				
— PPTP_1				
Enable			•	
Remote IP A	ddress		110.87.98.58	
Username			pptpserver	
Password			•••••	
Authenticatio	n		Auto	•
Global Traffic	: Forwarding			
Remote Subr	net			
Remote Subr	net Mask			
Advanced Se	ettings			

If you want to access peer subnet such as 192.168.3.0/24, you need to configure the subnet and mask to add the route.

Remote Subnet	192.168.3.0	
Remote Subnet Mask	255.255.255.0	

2. Check "Show Advanced" option, and you will see the advanced settings.

DMVPN	IPsec	GRE	L2TP	PPTP
Show Adv	vanced			
Local IP A	Address			
Peer IP A	ddress			
Enable N/	AT			
Enable M	PPE			
Address/0	Control Compressio	on		
Protocol F	Field Compression			
Asyncma	p Value		fffffff	
MRU			1500	
MTU			1500	
Link Dete	ction Interval (s)		60	
Max Retri	es		0	
Expert Op	otions			

If the PPTP server requires MPPE encryption, then you need to check "Enable MPPE" option.

Enable MPPE

1

If the PPTP server assigns fixed tunnel IP to the client, then you can fill in the local tunnel IP and remote tunnel IP, shown as below.

Local IP Address	205.205.0.100	
Peer IP Address	205.205.0.1	

Otherwise PPTP server will assign tunnel IP randomly.

Click "Save" button when you complete all settings, and then the advanced settings will be hidden again. Then click "Apply" button to have the configurations take effect.

3. Go to "Status > VPN" and check PPTP connection status.

PPTP is established as shown below.

Local IP: the client tunnel IP.

Remote IP: the server tunnel IP.

Status		Overview	Cellular	Network	WLAN	VPN	Routing	Host List	GPS
Network	Þ	Clients							
			Name	Status		Local IP		Remote IP	
System			pptp_1	Connected		120.205.0.100	20	5.205.0.1/32	
Industrial	Þ		ipsec_1	Disconnected		-		-	

Related Topics
PPTP Setting
PPTP Status

[END]