

UF51

5G CPE

用户手册



前言

感谢您选择星纵物联 UF51 5G CPE。UF51 5G CPE 具备丰富的功能，能为您提供稳定的网络连接，同时能承受工业级的高低温工作环境，CPE 带有自动网络连接备份/故障恢复，硬件看门狗，VPN，快速以太网等功能。

本手册将介绍如何配置和操作 UF51 5G CPE。 您可以参考它来获取详细的功能和配置。

阅读人群

本指南主要面向以下用户：

- 网络工程师
- 现场技术支持和维护人员
- 负责网络配置和维护的网络管理员

版权所有 © 2011-2022 星纵物联

本用户指南中的所有信息均受版权法保护。未经厦门星纵物联科技有限公司书面授权，任何组织和个人不得以任何方式复制或复制本用户指南的全部或部分内容。

产品涵盖

本指南介绍了如何配置以下设备：

- 星纵物联 UF51 5G CPE

相关文档

文档名称	文档描述
UF51 规格书	介绍 UF51 5G CPE 的规格参数
UF51 快速安装手册	介绍 UF51 5G CPE 的安装使用

一致性声明

UF51 符合 CE, FCC 和 RoHS 的基本要求和相关规定。



如需帮助，请联系

星纵物联技术支持:

邮箱: contact@milesight.com

电话: 0592-5023060

传真: 0592-5023065

总部地址: 厦门市集美区软件园三期 C09 栋

深圳: 深圳市南山区高新南一道 TCL 大厦 A709

修订记录

日期	文档版本	文档描述
2021.7.1	V1.0	第一版
2021.12.30	V1.1	更新品牌 Logo

目录

前言	1
阅读人群	1
第一章 产品介绍	8
1.1 概述	8
1.2 优势	8
1.3 技术参数	9
1.4 产品尺寸 (mm)	12
第二章 登录网页端操作界面	13
2.1 配置 PC 以连接 CPE	13
2.2 CPE 登录	14
第三章 网页端配置	16
3.1 状态	16
3.1.1 概况	16
3.1.2 蜂窝	17
3.1.3 网络	19
3.1.4 WLAN	20
3.1.5 VPN	21
3.1.6 路由信息	22
3.1.7 主机列表	23
3.1.8 GPS	23
3.2 网络	24
3.2.1 接口	24
3.2.1.1 链路备份	24
3.2.1.2 蜂窝网络	26
3.2.1.3 端口	29
3.2.1.4 广域网	30
3.2.1.5 网桥	35
3.2.1.6 WLAN	36
3.2.1.7 交换机	39
3.2.1.8 环回	40
3.2.2 DHCP	40
3.2.2.1 DHCP 服务器/DNCHv6 服务器	40
3.2.2.2 DHCP 中继	42

3.2.3 防火墙	43
3.2.3.1 安全	43
3.2.3.2 访问控制列表	44
3.2.3.3 端口映射	46
3.2.3.4 DMZ	46
3.2.3.6 MAC 绑定	47
3.2.3.7 自定义规则	48
3.2.3.8 SPI	48
3.2.4 流量控制	50
3.2.5 VPN	51
3.2.5.1 DMVPN	51
3.2.5.2 IPSec 服务器	54
3.2.5.3 IPSec	59
3.2.5.4 GRE	63
3.2.5.5 L2TP	64
3.2.5.6 PPTP	66
3.2.5.7 OpenVPN 客户端	68
3.2.5.8 OpenVPN 服务器	70
3.2.5.9 证书管理	72
3.2.6 IP 穿透	75
3.2.7 路由	75
3.2.7.1 静态路由	75
3.2.7.2 RIP	76
3.2.7.3 OSPF	79
3.2.7.4 路由过滤	85
3.2.8 VRRP	86
3.2.9 DDNS	87
3.3 系统	88
3.3.1 常规	89
3.3.1.1 常规	89
3.3.1.2 系统时间	90
3.3.1.3 SMTP	92
3.3.1.4 存储	94
3.3.2 电话&短信	94

3.3.2.1 电话	94
3.3.2.2 短信	96
3.3.3 用户管理	97
3.3.3.1 账户	97
3.3.3.2 用户管理	97
3.3.4 SNMP	98
3.3.4.1 SNMP	99
3.3.4.2 MIB 视图	99
3.3.4.3 VACM	100
3.3.4.4 Trap	101
3.3.4.5 MIB	102
3.3.5 AAA	102
3.3.5.1 Radius	102
3.3.5.2 TACACS+	103
3.3.5.3 LDAP	104
3.3.5.4 认证	105
3.3.6 设备管理	106
3.3.6.1 设备管理	106
3.3.6.2 Milesight VPN	107
3.3.7 事件	108
3.3.7.1 事件	108
3.3.7.2 事件设置	109
3.4 工业接口	110
3.4.1 I/O	111
3.4.1.1 数字输入	111
3.4.1.2 数字输出	112
3.4.2 串口	113
3.4.3 Modbus TCP	116
3.4.3.1 Modbus TCP	117
3.4.3.2 Modbus RTU	117
3.4.3.3 Modbus RTU Over TCP	118
3.4.4 Modbus Master	120
3.4.4.1 Modbus Master	120
3.4.4.2 通道设置	121

3.4.5 GPS	123
3.4.5.1 GPS	123
3.4.5.2 GPS IP 转发	123
3.4.5.3 GPS 串口转发	125
3.5 维护	126
3.5.1 工具	126
3.5.1.1 PING 探测	126
3.5.1.2 路由探测	127
3.5.1.3 网络抓包工具	127
3.5.1.4 Qxdmlog	128
3.5.2 调试	129
3.5.2.1 蜂窝 AT 调试	129
3.5.2.2 防火墙 AT 调试	129
3.5.3 日志	130
3.5.3.1 系统日志	130
3.5.3.2 系统日志下载	131
3.5.3.3 系统日志设置	131
3.5.4 升级	132
3.5.5 备份还原	133
3.5.6 重启	134
3.5.6.1 立即重启	134
3.5.6.2 定时重启	134
第四章 应用案例	135
4.1 恢复出厂设置	135
4.1.1 通过网页页面	135
4.1.2 硬件上重置	136
4.2 固件升级	136
4.3 事件应用案例	137
4.4 日志和诊断	139
4.5 SNMP 应用案例	140
4.6 网络连接	143
4.6.1 蜂窝数据连接	143
4.6.2 以太广域网连接	145
4.7 Wi-Fi 应用案例	148

4.7.1 接入点模式	148
4.7.2 客户端模式	149
4.8 NAT 应用案例	149
4.9 访问控制应用案例	150
4.10 流量控制应用案例	151
4.11 DTU 应用案例	153
4.12 PPTP 应用案例	156

第一章 产品介绍

1.1 概述

星纵物联 5G CPE 是一款具备 IP67 高防水防尘等级特性同时兼顾时尚外观的 5G 工业路由设备。内置高性能处理器，采用全网通通信模块与 2 个千兆网口，提供无可比拟的通信能力，同时自带 RS232/RS485 串行接口与数字输入输出(DI/DO)，支持 Python 二次开发，灵活拓展 CPE 功能。

5G CPE 宽温宽压的工业设计，可广泛应用于物联网产业链中的 M2M 行业，如智能交通、电子警察、无人驾驶、智慧办公、智慧医疗、商用机器人、智能家居、金融、移动 POS 终端、供应链自动化、智能建筑、消防、公共安全、环境保护、气象、遥感勘测、农业、林业、水务、煤矿、石化等领域。

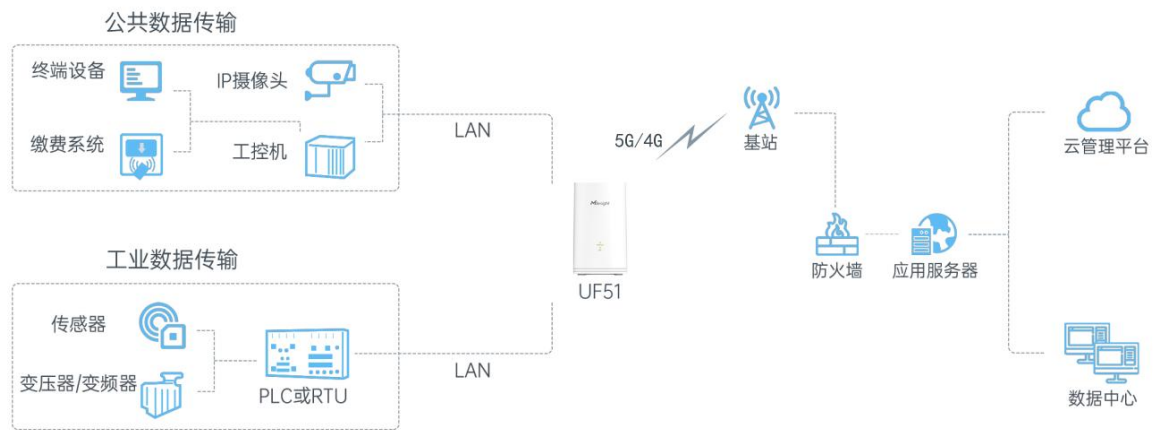


图 1.1 概述-1

1.2 优势

效益

- 使用工业级 NXP CPU，大内存
- 内置 4G/5G 全无线通信模块，支持 NSA 和 SA 网络，兼容各大主流运营商
- 灵活的模块化设计为用户提供不同的连接模块，如以太网、I/O、串口、Wi-Fi、GPS，可用于连接不同类型的终端设备
- 铸铝外壳，支持壁挂、抱杆、桌面放置、底部磁吸/锁付等多种安装方式

安全性和可靠性

- 以太网有线接入和蜂窝网络之间自动连接备份和故障恢复
- 支持多种 VPN，如 IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN

- 嵌入硬件看门狗，能够自动从各种故障中恢复，确保设备运行稳定性
- 进行集中认证和设备授权访问的安全机制，支持 AAA（TACACS +、Radius、LDAP、本地认证）和多级用户权限

易于维护

- 设备管理平台 DeviceHub 提供简便的单台配置、批量配置和远程设备的集中管理
- Web 界面设计和多个升级选项可帮助管理员轻松管理设备
- CLI 指令配置使管理员能够在大量设备之间实现简单的管理和快速配置
- SNMP 有效管理现有平台上的远程 CPE

功能

- 工业级 32 位 ARM Cortex-A7 处理器，512MHz DDR3 RAM，8GB 的内存可支持更多应用
- 支持丰富的协议，如 SNMP、Modbus、RIP、OSPF
- 支持-40°C ~ 70°C/-40°F ~ 158°F工作温度

1.3 技术参数

硬件系统

CPU	高通 4 核 CPU，716.8 MHz，ARM Cortex-A7
内存	8 GB 闪存, 512 MB DDR3 RAM

蜂窝网络

网络	5G / 4G LTE
天线	8 根内置天线
SIM 卡槽	1 个 (2FF)

以太网口

网口数量	2 × 10/100/1000 Mbps
网口类型	1 × WAN + 1 × LAN 或 2 × LAN
传输模式	全双工/半双工自适应
PoE	WAN / LAN 口支持 802.3af 标准 PoE 受电

Wi-Fi 接口

天线	4 根内置天线
标准及频段	IEEE 802.11b/g/n, 2.4 GHz IEEE 802.11a/n/ac, 5.8 GHz

发射功率	2.4 GHz: 最大 26 dBm 5.8 GHz: 最大 26.4 dBm
接收灵敏度	
2.4G	802.11b: $\leq -92\text{dBm}@11\text{Mbps}$ 802.11g: $\leq -78\text{dBm}@54\text{Mbps}$ 802.11ac VHT20: $\leq -91\text{dBm}@MCS0$ 802.11ac VHT20: $\leq -66\text{dBm}@MCS8$ 802.11ac VHT40: $\leq -88.5\text{dBm}@MCS0$ 802.11ac VHT40: $\leq -64\text{dBm}@MCS8$
5.8G	802.11a: $\leq -91\text{dBm}@6\text{Mbps}$ 802.11a: $\leq -76\text{dBm}@54\text{Mbps}$ 802.11ac VHT20: $\leq -90\text{dBm}@MCS0$ 802.11ac VHT20: $\leq -68\text{dBm}@MCS8$ 802.11ac VHT40: $\leq -87\text{dBm}@MCS0$ 802.11ac VHT40: $\leq -65\text{dBm}@MCS9$ 802.11ac VHT80: $\leq -84\text{dBm}@MCS0$ 802.11ac VHT80: $\leq -60\text{dBm}@MCS9$
工作模式	客户端模式, AP 模式
安全加密	WEP/WPA/WPA2 认证, 支持 WEP/TKIP/AES 加密
GPS¹ 接口 (可选)	
天线	1 根内置天线
定位技术	GPS/GLONASS/北斗/Galileo/QZSS
串口	
接口数量	1 × RS232 或 1 × RS485 (可切换)
接口类型	3.5 mm 接线端子
波特率	300 bps ~ 230400 bps
DI/DO	
接口数量	1 × DI (干接点) + 1 × DO (湿接点), 带电隔离
接口类型	3.5 mm 接线端子
最大承受电压/电流	0.3A@30VDC (DO)
其他接口	
复位按钮	1 个
LED 指示灯	1 × 状态指示灯, 1 × 蜂窝网络指示灯

内置 看门狗，定时器

软件功能

网络协议	IPv4/IPv6, PPP, PPPoE, SNMP v1/v2/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QOS, SNTP, Telnet, VLAN, SSH 等
VPN	DMVPN, IPsec, OpenVPN, PPTP, L2TP, GRE
防火墙	SPI 防火墙, 访问控制 (ACL), DMZ, 端口转发, MAC 地址绑定, DoS&DDoS 攻击防御, URL 过滤
设备管理	网页, CLI, 短信, 按需拨号, SNMP v1/v2/v3, 星纵物联设备管理平台
AAA	Radius, Tacacs+, LDAP, 本地认证
多级用户	支持管理员和只读用户两级权限
高可靠性	VRRP, 多重链路备份
串口协议	TCP 客户端/服务端, UDP, Modbus RTU/TCP 主站模式, Modbus 从站模式, Modbus RTU 转 Modbus TCP

供电

供电方式 ²	1. 9-48 VDC, 支持浪涌保护和反极保护 2. 802.3af 标准 PoE 受电
电源接口	2PIN 3.5 mm 接线端子

物理特性

防护等级	IP67
材质	PC+金属外壳
透气阀	1 个
外形尺寸	不带防水接头: $\Phi 105 \times 110 \times 188$ mm 带防水接头: $\Phi 105 \times 110 \times 218$ mm
安装方式	支持抱杆, 壁挂, 桌面放置, 底部磁吸/锁付

环境需求

工作温度	-40°C~70°C
存储温度	-40°C~85°C
电磁隔离保护	1.5 kV RMS
相对湿度	25°C下 0%~95% (无凝结)

1.4 产品尺寸 (mm)

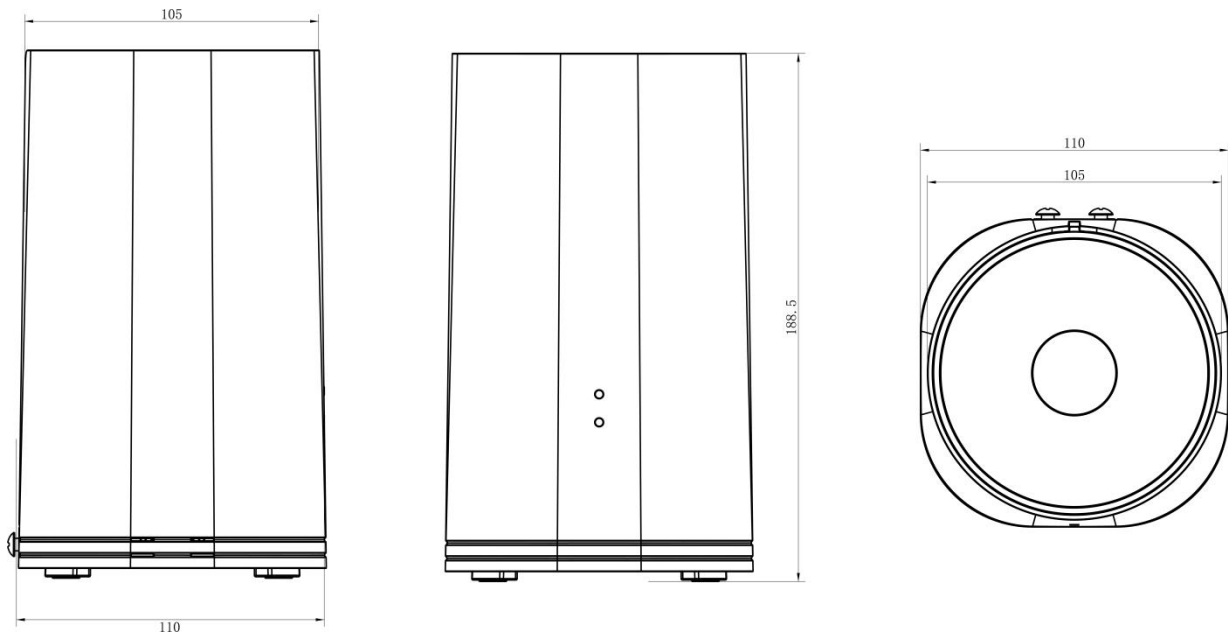


图 1：不带防水接头尺寸图

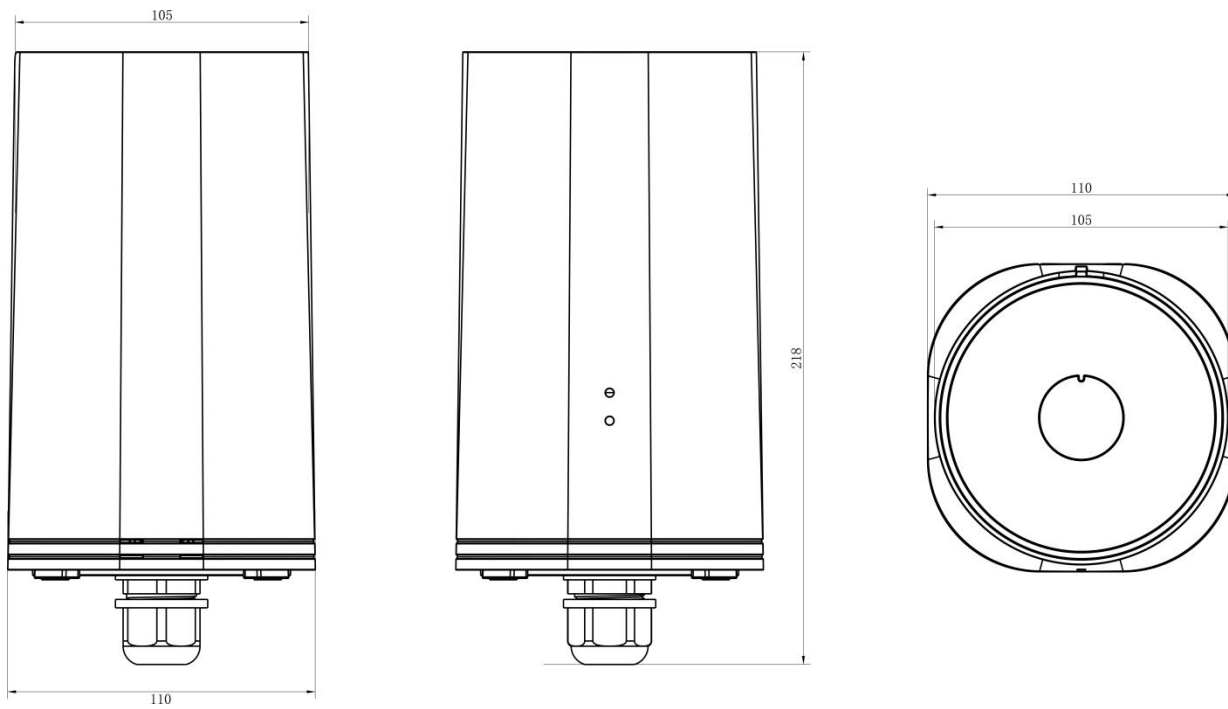


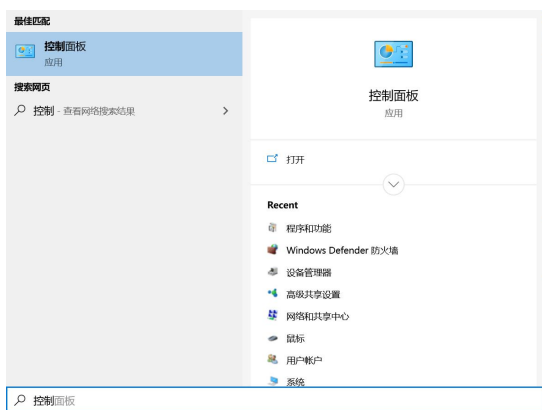
图 2：带防水接头尺寸图

第二章 登录网页端操作界面

本章介绍如何访问 UF51 的网页端操作界面。

2.1 配置 PC 以连接 CPE

请将 PC 直接连接 UF51 的 LAN 端口。PC 可以自动获取 IP 地址，也可以手动配置静态 IP 地址。
以下步骤基于 Windows 10 操作系统供您参考。



① 在 Windows 10 任务栏单击“搜索框”以搜索“控制面板”。

调整计算机的设置

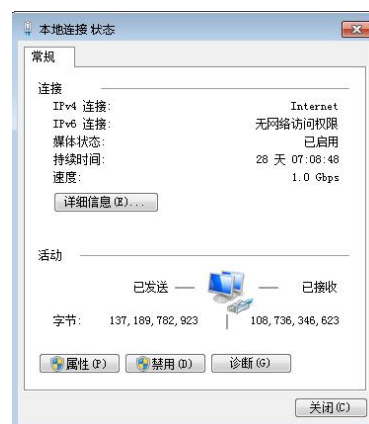
查看方式: 类别



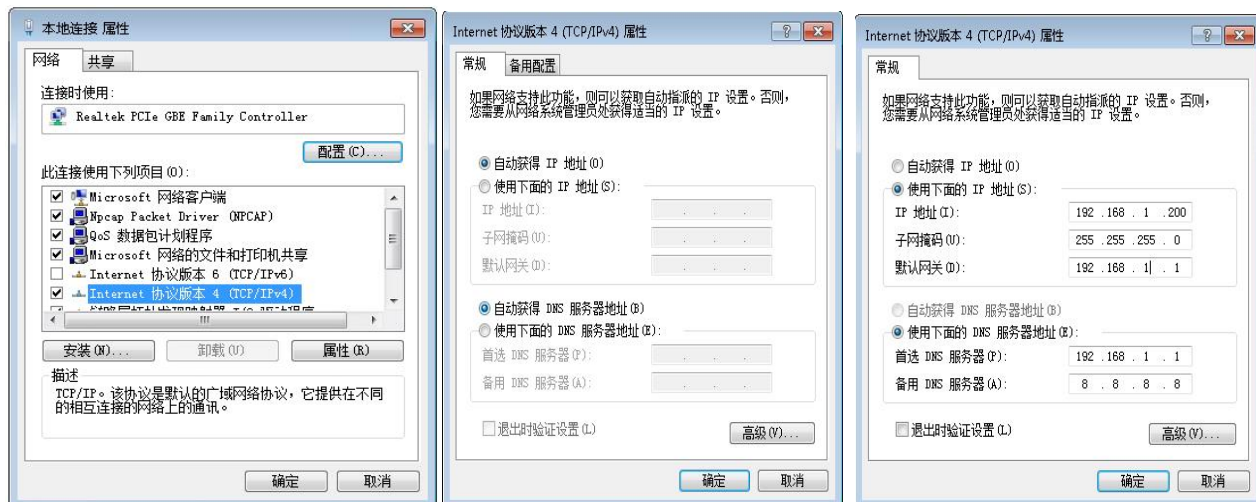
② 单击“控制面板”将其打开, 然后单击“查看网络状态和任务”



③ 单击“本地连接”（可能有不同的名称）。



④ 单击“属性”。



- ⑤ 双击“Internet 协议版本 4 (TCP / IPv4)”配置 IP 地址和 DNS 服务器。
- 方法 1: 单击“自动获取 IP 地址”；
- 方法 2: 单击“使用以下 IP 地址”在路由器的同一子网内手动分配静态 IP。

(注意: 记得单击“确定”完成配置。)

2.2 CPE 登录

星纵 CPE 为配置管理提供了网页端操作界面。如果您第一次使用 CPE，默认配置如下：

用户名: admin

密码: password

IP 地址: 192.168.1.1

DHCP 服务器: 启用

1. 在 PC 上启动 Web 浏览器（建议使用 Chrome 和 IE），输入 IP 地址，然后按键盘上的 Enter 键。
2. 输入用户名、密码，然后单击“登录”。

中文

Milesight

Username

Password

登录

图 2.1 CPE 登录 -1

- !** 如果输入的用户名或密码错误超过 5 次，登录页面将被锁定 10 分钟。
3. 使用默认用户名和密码登录时，系统会要求您修改密码。为了安全起见，建议您更改密码。如果要稍后修改，请单击“取消”按钮。

修改密码 ×

旧密码

新密码

再次输入新密码

保存

取消

图 2.2 CPE 登录 -2

4. 登录 Web GUI 后，您可以在 CPE 上查看系统信息并执行配置。

状态	概况	蜂窝	网络	WLAN	VPN	路由信息	主机列表	GPS
网络	系统信息					系统状态		
系统	型号		UF51-501EU			本地时间		2021-07-15 09:20:29 Thursday
工业	序列号		6223B1372450			正常运行时间		00:01:38
维护	固件版本		76.2.0.2-a6			处理器负荷		41%
APP	硬件版本		V1.0			内存 (可用/全部)		313MB/512MB(61.13%)
						Flash (可用/全部)		2922MB/4096MB(71.34%)
	蜂窝					WAN ● 当前链路		
	状态		Down			状态		在线
	IPv4		0.0.0.0/0			IPv4		192.168.22.69/24
	IPv6		-			IPv6		fe80::26e1:24ff:fe20:2147/64

图 2.2 CPE 登录 -3

第三章 网页端配置

3.1 状态

3.1.1 概况

查看 CPE 的所有接口运行状态

状态

网络

系统

工业

维护

APP

概况

蜂窝

网络

WLAN

VPN

路由信息

主机列表

GPS

系统信息

系统状态

型号

本地时间

UF51-501EU

2021-07-15 09:20:29 Thursday

序列号

正常运行时间

6223B1372450

00:01:38

固件版本

处理器负荷

76.2.0.2-a6

41%

硬件版本

内存 (可用/全部)

V1.0

313MB/512MB(61.13%)

Flash (可用/全部)

2922MB/4096MB(71.34%)

蜂窝

WAN

● 当前链路

状态

状态

Down

在线

IPv4

IPv4

0.0.0.0/0

192.168.22.69/24

IPv6

IPv6

-

fe80::26e1:24ff:fe20:2147/64

连接时长

MAC

0 days, 00:00:00

24:e1:24:20:21:47

数据月度统计

连接时长

0.0 MiB

0 days, 00:00:28

WLAN-2.4G

WLAN-5G

状态

状态

运行

运行

模式

模式

接入点

接入点

SSID

SSID

UF51_2.4G

UF51_5G

已连接客户端数

已连接客户端数

0

0

图 3.1.1 状态-1

系统信息	
项目	描述
系统信息	
型号	显示该设备的型号。
序列号	显示该设备序列号。
固件版本	显示当前固件版本。
硬件版本	显示当前的硬件版本。
蜂窝	
状态	显示当前蜂窝连接状态
当前 SIM 卡	显示当前所使用的 SIM 卡
IPv4/IPv6	显示蜂窝拨号获取的 IPv4/IPv6 地址
连接时长	显示蜂窝拨上号后的连接时长
数据月统计	显示本月当前 SIM 卡已使用数据流量

WLAN	
状态	显示当前 WLAN 运行状态
模式	显示当前 WLAN 运行模式
SSID	当模式为接入点时显示 CPE 的 SSID。当模式为客户端，显示 CPE 连接的接入点的 SSID。
已连接客户端数	当模式为接入点时显示，统计当前接入客户端数量
系统状态	
本地时间	显示 CPE 当前的系统时间
正常运行时间	显示系统从启动到当前的工作时长。
处理器负荷	显示当前 CPE CPU 负载情况
内存（全部/可用）	显示当前的内存总容量和可用容量。
Flash（全部/可用）	显示当前 Flash 总容量和可用容量。
WAN	
状态	显示当前 WAN 口状态
IPv4/IPv6	显示当前 WAN 口的 IPv4/IPv6 地址
MAC	显示 WAN 口的 MAC 地址
连接时长	显示 WAN 口网线连接的时长。当禁用 WAN 功能或断开网线连接后停止计时。
LAN	
IPv4/IPv6	显示局域网中 CPE 地址
已连接设备数	显示当前局域网的设备数量

表 3.1.1 概况-1

3.1.2 蜂窝

查看 CPE 的蜂窝网络状态

状态

网络

系统

工业

维护

APP

概况

蜂窝

网络

WLAN

VPN

路由信息

主机列表

GPS

蜂窝运行状态

网络

状态

Ready

状态

Connected

模块型号

RM500Q-GL

IPv4 地址

172.23.69.64/25

版本

RM500QGLABR11A01M4G

IPv4 网关

172.23.69.65

当前SIM卡

SIM1

IPv4 DNS

218.85.157.99

信号强度

99asu (85dBm)

IPv6 地址

fe80::a470:f2ff:fe52:efdc/64

注册状态

Registered (Home network)

IPv6 网关

::

IMEI

863305040328782

IPv6 DNS

::

IMSI

460115210471226

连接时长

0 days, 00:21:35

ICCID

89860320245922910521

月度数据统计

运营商

CHN-CT

SIM-1

RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB

网络类型

5G NR

SIM-2

RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB

PLMN ID

46011

位置区码

5E3803

Cell ID

0

CQI

0

下行带宽

20 MHz

上行带宽

1.4 MHz

信噪比

26

PCI

795

图 3.1.2 蜂窝-1

蜂窝信息	
项目	描述
状态	显示模块和 SIM 卡的相关检测状态。
模块型号	显示蜂窝模块型号。
当前 SIM 卡	显示当前使用的 SIM 卡。
信号强度	显示蜂窝无线信号强度。
注册状态	显示当前 SIM 卡的注册状态。
IMEI	显示模块 IMEI。
IMSI	显示 SIM 卡的 IMSI。
ICCID	显示 SIM 卡的 ICCID。
运营商	显示注册上的运营商。
网络类型	显示拨号上的网络类型，如 5G NR，LTE，3G 等。
PLMN ID	显示移动国家代码 (MCC)+移动网络代码 (MNC),也显示位置区域码 (LAC)和小区识别码。
位置区码	显示 SIM 卡位置区域码。
Cell ID	显示 SIM 卡所在的蜂窝小区识别号。

表 3.1.2 蜂窝-1

网络状态	
项目	描述
状态	显示蜂窝网络的拨号状态。
IPv4/IPv6 地址	显示蜂窝拨号获取的 IPv4/IPv6 地址。
IPv4/IPv6 网关	显示蜂窝拨号获取的 IPv4/IPv6 网关
IPv4/IPv6 DNS	显示蜂窝拨号获取的 DNS
连接时长	显示蜂窝拨号上线后的连接时长

表 3.1.2 蜂窝-2

月度数据统计	
项目	描述
SIM	显示 SIM 卡当月的流量使用情况

表 3.1.2 蜂窝-3

3.1.3 网络

查看 CPE 的 WAN 和 LAN 状态

状态	概况	蜂窝	网络	WLAN	VPN	路由信息	主机列表	GPS
网络								
系统								
工业								
维护								
APP								

广域网-IPv4								
端口	状态	拨号类型	IP地址	子网掩码	网关	DNS	连接时长	
WAN	上线	静态IP地址	192.168.23.215	255.255.255.0	192.168.23.1	8.8.8.8	53m 33s	
广域网-IPv6								
端口	状态	拨号类型	IP地址	前缀长度	网关	DNS	连接时长	
WAN	上线	静态IP地址	fe80::26e1:24ff:fe00:3ed0	64	-	-	53m 33s	

图 3.1.3 网络-1

广域网状态	
状态	描述
端口	显示 WAN 口的端口名称。
状态	显示 WAN 口的状态。“上线”表示端口已经启用。
拨号类型	显示 WAN 口拨号的类型。
IP 地址	显示 WAN 口的 IPv4 或者 IPv6 地址
子网掩码	显示 WAN 口的 IPv4 子网掩码
前缀长度	显示 WAN 口的 IPv6 前缀长度
网关	显示 WAN 口的网关地址

DNS	显示 WAN 口的 DNS
连接时长	显示 WAN 口网线连接的时长。当禁用 WAN 功能或断开网线连接后停止计时。

表 3.1.3 网络-1

网桥				
名称	STP	IPv4地址	IPv6地址	Members
Bridge0	启用	192.168.1.1/24	-	eth1,WLAN-2.4G,WLAN-5G

图 3.1.3 网络-2

网桥	
项目	描述
名称	显示网桥接口的名称
STP	显示是否启用生成树协议
IPv4/IPv6	显示网桥接口的 IPv4/IPv6 地址和网络位
成员	显示网桥的成员

表 3.1.3 网络-2

3.1.4 WLAN

查看 Wi-Fi 状态，包括接入点和客户端的信息

状态

网络

系统

工业

维护

APP

概况

蜂窝

网络

WLAN

VPN

路由信息

主机列表

GPS

WLAN状态

名称	状态	接口类型	SSID	IPv4地址	IPv6地址
WLAN-2.4G	运行	接入点	Router_F137B8	192.168.1.1/24	-
WLAN-5G	运行	接入点	Router_F137B9	192.168.1.1/24	-

已关联无线用户

SSID名称	MAC地址	IPv4地址	IPv6地址	连接时间
Router_F137B8	94-bf-2d-46-fa-a7	192.168.1.105	-	9 seconds

图 3.1.4 WLAN-1

WLAN 状态

项目	描述
WLAN 状态	
名称	显示 Wi-Fi 的名称。
状态	显示 Wi-Fi 的状态。
接口类型	显示 Wi-Fi 的接口类型。
SSID	当接口类型为接入点时显示 CPE 的 SSID。当接口类型为客户端，显示 CPE 连接的接入点的 SSID。
IPv4/IPv6 地址	当接口类型为接入点时，显示 CPE 的 IPv4/IPv6 地址和网络位。当接口类型为客户端时，显示 CPE 连接的接入点的 IPv4/IPv6 地址和网络位。
已关联无线用户	
SSID	当接口类型为接入点时，显示 CPE 的 SSID。当接口类型为客户端时，显示 CPE 连接的接入点的 SSID。
MAC 地址	当接口类型为接入点时，显示已连接客户端的 MAC 地址。当接口类型为客户端时，显示 CPE 连接的设备的 MAC 地址。
IPv4/IPv6 地址	当接口类型为接入点时，显示已连接客户端的 IPv4/IPv6 地址。当接口类型为客户端时，显示 CPE 连接的设备的 IPv4/IPv6 地址。
连接时间	当接口类型为接入点时，显示设备连接到 CPE 的时间。当接口类型为客户端时，显示 CPE 连接到接入点的时间。

表 3.1.4 WLAN-1

3.1.5 VPN

查看 VPN 运行状态，包括 PPTP，L2TP，IPsec，OpenVPN 和 DMVPN

状态

网络

接口

DHCP

防火墙

流量控制

VPN

IP 穿越

路由

VRRP

概况

蜂窝

网络

WLAN

VPN

路由信息

主机列表

GPS

客户端

名称	状态	本地IP	远端IP
ipsec_1	断开	-	-

服务器

名称	状态
OpenVPN Server	禁用
Ipsc Server	禁用

已连接客户端

服务器类型	客户端IP	连接时间
-------	-------	------

图 3.1.5 VPN-1

VPN 状态	
项目	描述
客户端	

名称	显示已经启用的 VPN 客户端的名称。
状态	显示开启的客户端是否与服务器连接。“已连接”表示客户端已连接上服务器。“已断开”表示客户端不再连接服务器。
本地 IP	显示 CPE 的 IP 地址。
远端 IP	显示隧道的远端真实 IP 地址。
服务器	
名称	显示已经启用的 VPN 服务器的名称。
状态	显示服务器的状态。
已连接客户端	
服务器类型	显示连接的服务器类型。
客户端 IP	显示连接到该服务器的客户端的 IP 地址。
连接时间	显示客户端与服务器的连接时间。当禁用该服务器时或连接断开后停止计时。

表 3.1.5 VPN-1

3.1.6 路由信息

查看路由状态，包括路由表和 ARP 缓存

状态

网络

系统

工业

维护

概况

蜂窝

网络

WLAN

VPN

路由信息

主机列表

路由表

目的地址	子网掩码	网关	接口	度量
0.0.0.0	0.0.0.0	10.39.128.13	Cellular 0	1
10.39.128.12	255.255.255.252	-	Cellular 0	-
127.0.0.0	255.0.0.0	-	Loopback	-
192.168.0.0	255.255.0.0	192.168.23.1	GE 0	1
192.168.1.0	255.255.255.0	-	bridge0	-
192.168.23.0	255.255.255.0	-	GE 0	-
192.168.23.35	255.255.255.255	-	gre_1	-
192.168.100.0	255.255.255.0	-	wlan0	-

ARP Cache

IP	MAC	接口
192.168.23.40	1c:1b:0d:f8:fe:06	GE 0

图 3.1.6 路由信息-1

路由信息	
项目	描述
路由表	
目的地址	显示目的主机或目的网络的 IP 地址。

子网掩码	显示目的主机或目的网络的子网掩码。
网关	显示该静态路由规则网关的 IP 地址。
接口	显示所配置的路由的出站接口。
度量	显示路由的度量值。
ARP Cache	
IP	显示 ARP 池的 IP 地址。
MAC	显示 IP 地址相对应的 MAC 地址。
接口	显示 ARP 记录的绑定接口。

表 3.1.6 路由信息-1

3.1.7 主机列表

查看连接的主机信息



图 3.1.7 主机列表-1

主机列表	
项目	描述
DHCP 租约时间	
IP	显示 DHCP 的租约主机的 IP 地址。
MAC	显示 DHCP 的租约主机的 MAC 地址。
剩余租约时间	显示 DHCP 租约剩余时间。
MAC 绑定	
IP & MAC	显示 DHCP 服务中绑定的静态 IP 和 MAC 地址

表 3.1.7 主机列表-1

3.1.8 GPS

启用 GPS 功能并成功获取 GPS 信息后，查看最新的 GPS 信息，包括 GPS 时间、纬度、经度和速度。

概况	蜂窝	网络	WLAN	VPN	路由信息	主机列表	GPS
GPS状态							
状态	未启用						
定位时间	-						
卫星使用数量	-						
可见卫星数量	-						
纬度	-						
经度	-						
高度	-						
速度	-						

图 3.1.8 GPS -1

GPS 状态	
项目	描述
状态	显示 GPS 的状态
定位时间	显示定位的时间
卫星使用数量	显示可见的卫星数量
可见卫星数量	显示使用的卫星数量
纬度	显示定位的纬度
经度	显示定位的经度
高度	显示 CPE 的高度信息
速度	显示移动的速度

表 3.1.8 GPS -1

3.2 网络

3.2.1 接口

3.2.1.1 链路备份

本节介绍如何配置链路备份。链路备份功能是指当正在使用的链路不可用时，能够自动切换到另一个可用链路，保证网络连接的可靠性。



图 3.2.1.1 链路备份-1

链路备份	
项目	描述
链路优先级	
优先级	显示该链路的优先级，越靠前优先级越高
启用规则	显示该链路是否启用
当前链路	显示当前链路使用状态， ● 代表正在使用的链路
接口	显示该链路使用的接口
连接类型	显示该链路的连接类型
IP	显示该链路所使用的 IP 地址
操作	进入 Ping 探测配置界面； 调整链路优先级
设置	
恢复间隔	指定等待多少秒后尝试切换至优先级更高的链路，设置为 0 时表示不切回。
链路异常则重启	启用后，若当前系统无可用链路，系统将会重启。

表 3.2.1.1 链路备份-1

通过 PING 探测检测该链路是否可用，配置规则如下：



图 3.2.1.1 PING 探测-2

Ping 探测		
项目	描述	默认
启用	启用链路 Ping 探测后，CPE 会阶段性探测链路的连接状态	启用
目的地址（IPV4/IPv6）	CPE ping 主地址/域名来检测当前连接是否存在	IPv4：8.8.8.8 IPv6：2001:4860:4860::8888
备选目的地址（IPV4/IPv6）	CPE ping 备用地址/域名来检测当前连接是否存在	IPv4：114.114.114.114 IPv6：2400:3200::1
Ping 间隔	CPE 每隔一个 Ping 间隔对目的地址进行 Ping 探测	300
Ping 重试间隔	当 Ping 失败后，CPE 每隔一个 Ping 重试间隔再重新 Ping	5
Ping 超时	发送 Ping 命令后等待应答的超时时间	3
最大重试次数	连续 Ping 失败并达到最大重试次数，判定此次 Ping 探测连接失败	3

表 3.2.1.1PING 探测-2

3.2.1.2 蜂窝网络

本节介绍如何配置蜂窝网络的相关参数。

The screenshot shows the '蜂窝网络' (Cellular Network) configuration page. On the left is a sidebar menu with categories: 状态 (Status), 网络 (Network), 接口 (Interface), DHCP, 防火墙 (Firewall), 流量控制 (Traffic Control), VPN, IP 穿透 (IP Penetration), 路由 (Routing), VRRP, DDNS, 系统 (System), 工业 (Industrial), and 维护 (Maintenance). The '网络' category is expanded, showing sub-items like 链路备份 (Link Backup), 蜂窝网络 (Cellular Network), 端口 (Port), 广域网 (WAN), and 网桥 (Bridge). The '蜂窝网络' sub-item is selected. The main configuration area includes fields for: 协议类型 (Protocol Type) set to 'IPv4/IPv6'; 接入点 (Access Point), 用户名 (Username), 密码 (Password), and PIN 码 (PIN Code) as empty text boxes; 拨号中心号码 (Dialing Center Number) as an empty text box; 认证方式 (Authentication Method) set to 'Auto'; 网络类型 (Network Type) set to '自动' (Auto); 短信中心号码 (SMS Center Number) as an empty text box; 启用NAT (Enable NAT) checked; 允许漫游 (Allow Roaming) checked; 最大可用流量 (Maximum Available Traffic) set to 0 MB; 清算日 (Billing Day) set to 每月 1 日 (Monthly 1st); 连接设置 (Connection Settings) section with 连接模式 (Connection Mode) set to '永远在线' (Always Online) and 重拨间隔(秒) (Redial Interval in seconds) set to 5. A '保存' (Save) button is at the bottom.

图 3.2.1.2 蜂窝网络-1

蜂窝网络		
项目	描述	默认
协议类型	选择协议类型 “IPv4” , “IPv6” , “IPv4/IPv6”	IPv4
接入点	输入由本地互联网服务供应商提供的蜂窝网络拨号连接的接入点。	Null
用户名	输入由本地互联网服务供应商提供的蜂窝网络拨号连接的用户名。	Null
密码	输入由本地互联网服务供应商提供的蜂窝网络拨号连接的密码。	Null
PIN 码	输入用于解锁 SIM 卡的 PIN 代码, 4-8 位。	Null
拨号中心号码	输入由本地互联网服务供应商提供的网络拨号号码。	Null
认证方式	可选 “Auto”、“PAP”、“CHAP”、“MS-CHAP”、“MS-CHAPv2”。	Auto
网络类型	选择蜂窝网络类型, 即网络访问顺序。可选 “自动”、“5G-NSA”、“5G-SA”、“仅 4G”、“仅 3G”。	Auto

	自适应：自动连接信号最强的网络。 5G-NSA:仅连接 5G-NSA 网络 5G-SA：仅连接 5G-SA 网络 仅 4G：仅连接 4G 网络。 以此类推。	
启用 NAT	勾选开启 NAT 功能	启用
允许漫游	勾选开启漫游功能后 CPE 会自动搜索并连上信号好的漫游网络；当取消漫游选项，漫游的 SIM 卡不能拨号上网。使用本地卡时，勾选漫游和取消漫游功能都不影响 SIM 卡拨号上网	禁用
短信中心号码	短消息进行存储转发的中心号码。通常依号码归属地不同短信中心的号码亦不同。	Null
最大可用流量	设置每月的最大可使用流量，当数据流量超过设定值时，该 SIM 卡将被禁止使用。0 表示不限制流量	Null
清算日	指定每个月的数据流量结算日。已使用的流量记录将在这一天的 00:00 清零，重新计算。合法值：1-28	Null

表 3.2.1.2 蜂窝网络-1

| 连接设置

连接模式

按需拨号

重拨间隔(秒)

5

最大空闲时间(秒)

60

电话触发

☐

短信触发

☐

IO触发

☐

保存

图 3.2.1.2 蜂窝网络-2

连接设置	
项目	描述
连接模式	可选“永远在线”、“按需拨号”。
按需拨号	按需拨号分为“电话触发”、“短信触发”、“IO 触发”。
电话触发	当 CPE 接到指定电话号码的来电时，CPE 自动从不在线状态转变为连接到蜂窝网络模式。
拨号组别	选择用于电话触发的电话组别。用户通过 Web 页面“系统>常规>电话”来设置电话群组。

短信触发	当 CPE 接到指定电话号码的短信时，CPE 自动从不在线状态转变为连接到蜂窝网络模式。
短信组别	选择用于短信触发的电话组别。用户通过 Web 页面“系统>常规>电话”来设置短信群组。
短信内容	填写触发的短信内容。
IO 触发	当 DI 状态有变化时，CPE 自动从不在线状态转变为连接到蜂窝网络模式。用户通过 Web 页面“工业>I/O>数字输入”来设置 IO 触发条件。

表 3.2.1.2 蜂窝网络-2

相关内容

[蜂窝网络连接](#)
[电话组](#)

3.2.1.3 端口

本节介绍如何配置以太网端口参数。
UF51 支持 2 个 LAN 端口，LAN1 可配置为 WAN 端口。

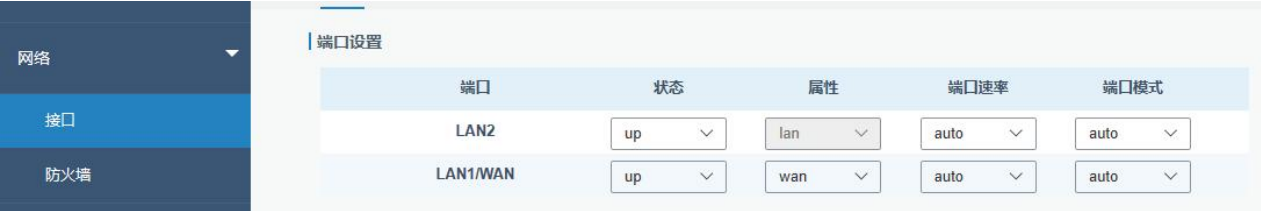


图 3.2.1.3 端口-1

端口设置	
项目	描述
端口	用户可根据自己的需要，对以太网口进行配置。
状态	设置以太网口的状态。“up”表示启用；“down”表示禁用。
属性	设置以太网口的类型，即 LAN 或 WAN。
端口速率	设置以太网口速率，可选择 auto、1000Mbps、100Mbps、10Mbps。
端口模式	设置以太网口模式，可选择 auto、full、half。

表 3.2.1.3 端口-1

3.2.1.4 广域网

WAN 端口可以通过以太网线连接以访问 Internet。它支持 6 种连接类型。

- 静态 IP：为以太网 WAN 口配置 IP 地址，网络掩码和网关。
- DHCP 客户端：将以太网 WAN 口配置为 DHCP 客户端，自动获取 IPv4 地址。
- PPPoE：将以太网 WAN 口配置为 PPPoE Client。
- DHCPv6 客户端：将以太网 WAN 口配置为 DHCP 客户端，自动获取 IPv6 地址。
- PPPoEv6：将以太网 WAN 口配置为 PPPoEv6 Client。
- DS-Lite：使用 IPv4-in-IPv6 隧道将 IPv4 数据包封装在 IPv6 数据包中发送到网络服务提供商。

状态

网络

接口

DHCP

防火墙

流量控制

VPN

IP 穿透

路由

VRRP

DDNS

系统

工业

维护

链路备份

蜂窝网络

端口

广域网

网桥

广域网设置

广域网_1

启用

网口

拨号类型

IPv4地址

子网掩码

IPv4网关

IPv6 地址

前缀长度

IPv6 网关

最大传输单元

首选DNS (IPv4)

备选DNS (IPv4)

首选DNS (IPv6)

备选DNS (IPv6)

启用NAT

☒

WAN

静态IP地址

192.168.22.175

255.255.255.0

192.168.22.1

fe80::26e1:24ff:fe1:37b6

64

1500

8.8.8.8

114.114.114.114

☒

图 3.2.1.4 广域网-1

广域网设置		
项目	描述	默认
启用	启用 WAN 功能	启用
网口	当前设置为 WAN 口的以太网口	--

拨号类型	选择 WAN 口上网的方式。可选“静态 IP 地址”、“DHCP 客户端”、“PPPoE”、“DHCPv6 客户端”、“PPPoEv6”、“Dual-Stack Lite”。	静态 IP 地址
最大传输单元	设置 WAN 口最大传输单元。合法值：68-1500	1500
首选 DNS (IPv4/IPv6)	设置首选的 DNS 服务器。	Null
备用 DNS (IPv4/IPv6)	设置备用的 DNS 服务器。	Null
启用 NAT	启用/禁用 NAT 功能。启用后可以把私网 IP 地址转换成公网 IP 地址。	启用

表 3.2.1.4 广域网-1

1. 配置静态 IP

如果外部网络为 WAN 口分配固定 IP，则用户可以选择“静态 IP 地址”模式。

广域网_1

启用

网口

拨号类型

IPv4地址

子网掩码

IPv4网关

IPv6 地址

前缀长度

IPv6 网关

最大传输单元

首选DNS (IPv4)

备选DNS (IPv4)

首选DNS (IPv6)

备选DNS (IPv6)

启用NAT

☒

WAN

静态IP地址

192.168.22.175

255.255.255.0

192.168.22.1

fe80::26e1:24ff:fe1:37b6

64

1500

8.8.8.8

114.114.114.114

☒

图 3.2.1.4 广域网-2

静态 IP 地址		
项目	描述	默认
IPv4 地址	设置可以访问互联网的 IPv4 地址，如 192.168.1.2	192.168.0.1
子网掩码	设置 WAN 口的子网掩码。如果子网掩码填的是 IPv4 地址 (IPv6)	255.255.255.0

	的格式，则访问网络时优先使用 IPv4（IPv6）的地址。	
IPv4 网关	设置 WAN 口的 IPv4 地址的网关。	192.168.0.2
IPv6 地址	设置可以访问互联网的 IPv6 地址，默认地址为：CPE 根据 WAN 口 MAC 地址生成的 IPv6 地址。	根据 MAC 地址生成
前缀长度	设置 IPv6 前缀长度以标识网段中全局单播 IPv6 地址的位数。如：在 2001:0DB8:0000:000b::/64 中，64 用来标识在该网段中的前 64 位。	64
IPv6 网关	设置 WAN 口的 IPv6 地址的网关。	--
多 IP 地址	除主 IP 以外用户还可以配多个从 IP 地址。	Null

表 3.2.1.4 广域网-2

2. DHCP 客户端/DHCPv6 客户端

外部网络启用了 DHCP 服务器并为以太网 WAN 接口分配了 IP 地址，则用户可以选择“DHCP 客户端”模式自动获取 IP 地址。

The figure displays two screenshots of the WAN configuration interface for '广域网_1' (WAN_1). The top screenshot shows the DHCP client configuration, and the bottom screenshot shows the DHCPv6 client configuration.

Top Screenshot (DHCP Client Configuration):

- 启用: ☒
- 网口: WAN
- 拨号类型: DHCP客户端
- 最大传输单元: 1500
- 使用对端DNS: ☐
- 首选DNS (IPv4): 8.8.8.8
- 备选DNS (IPv4): 114.114.114.114
- 启用NAT: ☒

Bottom Screenshot (DHCPv6 Client Configuration):

- 启用: ☒
- 网口: WAN
- 拨号类型: DHCPv6 Client
- 请求IPv6地址模式: None
- 请求IPv6前缀长度: 0-64
- 最大传输单元: 1500
- 首选DNS (IPv6): 2001:4860:4860::8888
- 备选DNS (IPv6):
- 启用NAT: ☒

图 3.2.1.4 广域网-3

项目	描述
使用对端 DNS	PPP 拨号时自动获取对端 DNS。在访问域名时 DNS 是必需的。
DHCPv6 客户端	
请求 IPv6 地址模式	选择 CPE 从 DHCPv6 服务器获取的 IPv6 地址的方式。可选项为：try、force、none。 Try：服务器优先分配特定的地址； Force：服务器只能分配特定的地址； None：服务器随机分配地址，该特定地址与你设置的前缀长度有关。
请求 IPv6 前缀长度	设置 CPE 期望从服务器获取的 IPv6 地址的前缀长度。

表 3.2.1.4 广域网-3

3. PPPoE/PPPoEv6

PPPoE 是指以太网上的点对点协议，用于 CPE 拨号上网。UF51 支持 PPPoE 和 PPPoEv6 拨号上网。

— 广域网_1

启用	☒
网口	WAN
拨号类型	PPPoE
用户名	
密码	
链路检测间隔 (秒)	60
最大重拨次数	0
最大传输单元	1500
使用对端DNS	☐
首选DNS (IPv4)	8.8.8.8
备选DNS (IPv4)	114.114.114.114
启用NAT	☒

— 广域网_1

启用

☒

网口

WAN

拨号类型

PPPoEv6

用户名

密码

链路检测间隔 (秒)

60

最大重拨次数

0

最大传输单元

1500

使用对端DNS

☐

首选DNS (IPv4)

8.8.8.8

备选DNS (IPv4)

114.114.114.114

首选DNS (IPv6)

2001:4860:4860::8888

备选DNS (IPv6)

启用NAT

☒

图 3.2.1.4 广域网-4

PPPoE	
项目	描述
用户名	输入互联网服务供应商提供的用户名。
密码	输入互联网服务供应商提供的密码。
链路检测间隔 (秒)	PPPOE 建立连接后发送心跳报文时间间隔，合法值：1-600。
最大重拨次数	设置拨号失败后的最大重新连接次数，合法值：0-9。
使用对端 DNS	PPP 拨号时自动获取对端 DNS。在访问域名时 DNS 是必需的。

表 3.2.1.4 广域网-4

4.DS-Lite

DS-Lite 技术可在 IPv6 网络中提供 IPv4 和 IPv6 双栈业务，也支持 IPv6 单栈业务。

— 广域网_1

启用

☒

网口

WAN

拨号类型

Dual-Stack Lite

IPv6 网关

DS-Lite AFTR地址

本地IPv6地址

最大传输单元

1500

首选DNS (IPv4)

8.8.8.8

备选DNS (IPv4)

114.114.114.114

首选DNS (IPv6)

2001:4860:4860::8888

备选DNS (IPv6)

启用NAT

☒

图 3.2.1.4 广域网-5

Dual-Stack Lite	
项目	描述
IPv6 网关	设置 WAN 口的 IPv6 网关
DS-Lite AFTR 地址	设置 DS-Lite AFTR 服务器地址
本地 IPv6 地址	设置 WAN 口的 IPv6 地址

表 3.2.1.4 广域网-5

相关配置案例

[以太网局域网连接](#)

3.2.1.5 网桥

管理连接到 UF51 的 LAN 端口的局域网设备，允许每个设备外网访问。



图 3.2.1.5 网桥-1

网桥		
项目	描述	默认
名称	显示网桥名称。默认为 Bridge0 且不可更改。	Bridge0
STP	开启/关闭 STP。	禁用
IP 地址	设置网桥的 IPv4 地址。	192.168.1.1
子网掩码	设置网桥的子网掩码	255.255.255.0
IPv6 地址	设置网桥的 IPv6 地址。	2004::1/64
最大传输单元	设置网桥的最大传输单元，合法值：68-1500。	1500
多 IP 地址	设置网桥的多个从 IP 地址。	Null

表 3.2.1.5 网桥-1

3.2.1.6 WLAN

本节介绍如何配置 Wi-Fi 的相关参数。
UF51 支持 2.4G 和 5G Wi-Fi，支持接入点或客户端模式。

图 3.2.1.6 WLAN-1

WLAN	
项目	描述
启用	启用/禁用 WLAN 功能。
接口类型	选择 WLAN 工作类型，可选“客户端”和“接入点”。
加密方式	选择加密方式，可选“No Encryption”、“WEP Open System”、“WEP Shared Key”、“WPA-PSK”、“WPA2-PSK”和“WPA-PSK/WPA2-PSK”。
BSSID	填入接入点的 MAC 地址。可以从 SSID 和 BSSID 中选择任意一种方式加入到网络。
SSID	填入接入点 SSID。
客户端模式	
扫描	点击“扫描”搜索附近的接入点。
SSID	显示 SSID。
信道	显示无线信道。
信号	显示无线信号。
BSSID	填入接入点的 MAC 地址。

安全	显示加密方式。
频率	显示射频频率。
加入网络	单击该按钮加入网络。
接入点模式	
射频类型	选择射频类型, 可选 “802.11b (2.4 GHz)”、“802.11g (2.4 GHz)”、“802.11n (2.4 GHz)”、“802.11a (5 GHz)” “802.11n (5 GHz)” “802.11ac (5 GHz)”。
信道	选择无线信道, 可选 “Auto”、“1”、“2” “13”。
加密方式	选择加密方式, 可选 “No Encryption”、“WEP Open System”、“WEP Shared Key”、“WPA-PSK”、“WPA2-PSK”、“WPA-PSK/WPA2-PSK”。
密钥	填写介入无线网络的密钥, 字符长度范围: 8-63 位。
无线频宽	选择无线频宽, 可选 “20MHz”、“40MHz”和 80MHz。
SSID 广播	当禁用 SSID 广播时, 其他无线设备无法找到 SSID, 用户必须手动输入 SSID 才能访问无线网络。
AP 隔离	启用接入点隔离后, 接入点所有用户之间的二层报文相互不能进行转发。
访客模式	该功能启用后, 连接该 SSID 不能访问内网。
最大客户端数量	输入该 SSID 可允许连接的最大客户端数量。合法值: 1-128。
IP 设置	
协议	CPE 作为客户端时, 选择无线网络接入方式, 可选 “DHCP Client”、“Static IP”。
IP 地址	设置无线网络中的 IP 地址。
子网掩码	设置无线网络中的子网掩码。
网关	设置无线网络中的网关。

表 3.2.1.6 WLAN-1

MAC地址过滤

类型

白名单
禁用
白名单
黑名单

MAC	描述	操作
		×
		+

图 3.2.1.6 WLAN-2

MAC 地址过滤	
项目	描述
类型	选择过滤类型
白名单	只有在访问控制列表里面的地址才能访问 CPE AP
黑名单	在访问控制列表里的地址都被拒绝访问 CPE AP。

表 3.2.1.6 WLAN-2

相关内容

[Wi-Fi 应用案例](#)

3.2.1.7 交换机

VLAN 是一种新的数据交换技术，通过将 LAN 设备逻辑划分为网段来实现虚拟工作组。

图 3.2.1.7 交换机-1

交换机	
项目	描述
局域网设置	
名称	设置 VLAN 接口名称。
VLAN ID	选择接口的 VLAN 标签。
IP 地址	设置 LAN 口的 IP 地址。
子网掩码	设置 LAN 口的 IP 子网掩码。
最大传输单元	设置 LAN 口的最大传输单元。合法值：68-1500。
VLAN 设置	

VLAN ID	用户自定义 VLAN 的标签 ID，合法值：1-127。
LAN1, LAN2(, LAN3, LAN4)	把 VLAN 绑定到相应的端口并设置 Ethernet frame 在 trunk link 上的状态，即 “Tagged” ， “Untagged” ， 或 “Close” 。
CPU	控制该 VLAN 和其他网络的互相通信。

表 3.2.1.7 交换机-1

3.2.1.8 环回

环回接口是 CPE 上的虚拟逻辑接口。在默认情况下，CPE 上没有环回接口，但可以根据需要创建。

图 3.2.1.8 环回-1

环回		
项目	描述	默认
IP 地址	用户不可更改	127.0.0.1
子网掩码	用户不可更改	255.0.0.0
多 IP 地址	除以上 IP 地址之外用户可以配其他 IP 地址	Null

表 3.2.1.8 环回-1

3.2.2 DHCP

DHCP 采用客户端/服务器通信模式，由客户端向服务器发起配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

3.2.2.1 DHCP 服务器/DNCHv6 服务器

默认启用 DHCP 服务器，主机连接 CPE 时会自动获取分配的 IP 地址，同时确保为每个主机分配不同的 IP 地址。

状态

网络

接口

DHCP

防火墙

流量控制

VPN

IP 穿透

路由

VRRP

DDNS

DHCP服务器

DHCPv6服务器

DHCP中继

DHCP服务器_1

启用

接口

起始地址

结束地址

子网掩码

有效期(分钟)

首选DNS服务器

备选DNS服务器

Windows名称服务器

静态IP

MAC地址

IP地址

操作

图 3.2.2.1 DHCP 服务器-1

状态

网络

接口

DHCP

防火墙

流量控制

VPN

IP 穿透

路由

VRRP

DDNS

DHCP服务器

DHCPv6服务器

DHCP中继

DHCPv6服务器_1

启用

接口

起始地址

结束地址

前缀长度

有效期(分钟)

首选DNS服务器

备选DNS服务器

静态IP

DUID

IPv6地址

操作

图 3.2.2.1 DHCPv6 服务器-1

DHCP 服务器		
项目	描述	默认
启用	开启/关闭 DHCP 服务器功能。	启用
接口	选择接口，如 Bridge0。	Bridge0
起始地址	设置地址池中分配给客户端设备的起始 IP 地址。	192.168.1.100
结束地址	设置地址池中分配给客户端设备的结束 IP 地址。	192.168.1.199
子网掩码	设置 DHCP 客户端从 DHCP 服务端获取的 IP 地址的子网掩码。	255.255.255.0
前缀长度	设置 DHCP 客户端从 DHCP 服务端获取的 IPv6 地址	64

	的前缀长度	
有效期（分钟）	设置分配 IP 的地址的有效期, 过期 DHCP 服务器将回收分配给客户端的 IP 地址并重新分配 IP 地址。合法值：5-1440，不能为空。	1440
首选 DNS 服务器	设置首选的 DNS 服务器。	192.168.1.1
备选 DNS 服务器	设置备选的 DNS 服务器。	Null
Windows 名称服务器	输入 DHCP 客户端从 DHCP 服务器获取的 Windows Internet 命名服务器对应的地址。通常可以留空。	Null
静态 IP		
MAC 地址	设置一个静态指定的 DHCP 客户端的 MAC 地址（不能与其他 MAC 相同，防止冲突）。	Null
DUID	设置一个静态指定的 DHCPv6 客户端 DUID。（不能与其他 DUID 相同，防止冲突）	Null
IP 地址	设置一个静态指定的 DHCP 客户端的 IP 地址（必须在起始 IP 地址和结束 IP 地址范围外）。	Null

表 3.2.2.1 DHCP 服务器-1

3.2.2.2 DHCP 中继

提供中继隧道，解决 DHCP Client 和 DHCP Server 不在同一子网内的问题。

DHCP服务器DHCPv6服务器DHCP中继

DHCP中继

启用

DHCP服务器

保存

图 3.2.2.2 DHCP 中继-1

DHCP 中继	
项目	描述
启用	开启/关闭 DHCP 中继功能。
DHCP 服务器	设置 DHCP 服务器，最多可以配置 10 个（以空格或 “，” 隔开）。

表 3.2.2.2 DHCP 中继-1

3.2.3 防火墙

本节介绍如何设置防火墙参数，包括安全性、访问控制列表、DMZ、端口映射、MAC 绑定、SPI。

防火墙根据报文的内容特征，如协议样式，源/目的 IP 地址等，实现入口方向（从公网到局域网）和出口方向（从局域网到公网）的相应数据流控制。确保 CPE 在安全的环境中运行并在局域网中托管。

3.2.3.1 安全

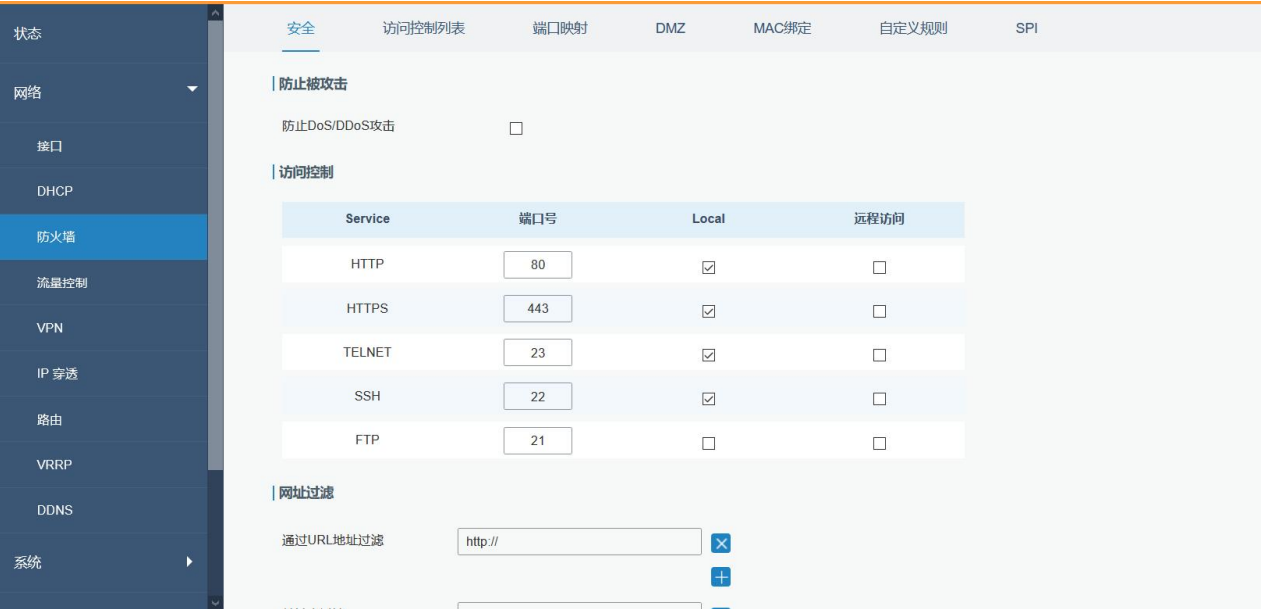


图 3.2.3.1 安全-1

项目	描述	默认
防止攻击		
防止 DoS/DDoS 攻击	启用/禁用防止 DoS/DDoS 攻击	禁用
访问服务控制		
端口号	设置相应服务的端口号。合法值：1-65535。	--
本地访问	本地连接 CPE	启用
远程访问	远程访问 CPE	禁用
HTTP	用户在勾选该选项之后可以通过 HTTP 在本地登录设备，然后通过 Web 进行访问和控制。	80
HTTPS	用户在勾选该选项之后可以通过 HTTPS 本地或远	443

	程登录设备，然后通过 Web 进行访问和控制。	
TELNET	用户在勾选该选项之后可以通过 Telnet 本地或远程登录设备。	23
SSH	用户在勾选该选项之后可以通过 SSH 本地或远程登录设备。	22
FTP	用户在勾选该选项之后可以通过 FTP 本地或远程登录设备。	21
网页过滤		
通过 URL 地址过滤	输入想封锁的 HTTP 地址进行过滤	
关键词过滤	通过输入关键字来封锁部分网络的访问，只能输入字母。最多不超过 64 个字符。	

表 3.2.3.1 安全性-1

3.2.3.2 访问控制列表

访问控制列表，也称为 ACL，是通过配置一系列匹配规则来实现对指定网络流量（例如源 IP 地址）的访问的许可或禁止来达到过滤网络接口流量的目的。当 CPE 收到报文时，将根据应用于当前接口的访问控制规则对该字段进行分析。在识别出特殊分组后，将根据预设策略实现对相应分组的许可或禁止。

ACL 定义的数据包匹配规则也可以由需要流量区分的其他功能使用。

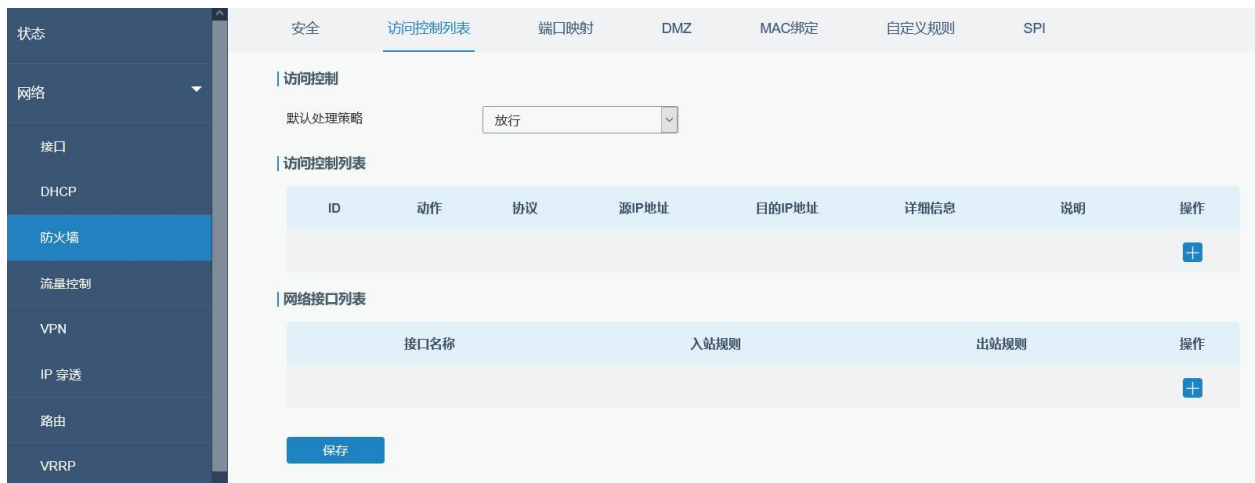


图 3.2.3.2 访问控制列表-1



图 3.2.3.2 访问控制列表-2

项目	描述
访问控制	
默认处理策略	可选“放行”或“拒绝”。对于不满足访问控制列表的报文，采取该默认处理策略。
访问控制列表	
类型	选择“扩展”或“标准”。扩展类型具有更多访问条件。
ID	输入 ACL 规则编号。合法值：1-199。
动作	可选“允许”或“拒绝”。
协议	访问控制协议，可选“ip”、“icmp”、“tcp”、“udp”、“1-255”。
源 IP 地址	输入 ACL 规则的匹配报文的源地址，为空表示所有。
源地址反掩码	输入 ACL 规则匹配报文的源地址反掩码。
目的 IP 地址	输入 ACL 规则匹配报文的地址，为空表示所有。
目的地址反掩码	输入 ACL 规则匹配报文目的地址反掩码。
说明	对同一个 ID 号的组进行统一说明。
ICMP 类型	输入 ICMP 包的类型。合法值：0-255。
ICMP 代码	输入 ICMP 包的代码。合法值：0-255。
源端口类型	选择源端口类型，如指定端口，或端口范围，等等。
源端口	设置源端口号。合法值：1-65535。
起始源端口	设置起始源端口号。合法值：1-65535。
结束源端口	设置结束源端口号。合法值：1-65535。
目的端口类型	选择目的端口类型，如指定端口，或端口范围等等。
目的端口	设置目的端口号。合法值：1-65535。
起始目的端口	设置起始目的端口号。合法值：1-65535。
结束目的端口	设置结束目的端口号。合法值：1-65535。
详细信息	显示端口信息。
网络接口列表	
接口名称	选择访问控制的网络接口。
进站规则	从访问控制列表 ID 中选择作进站过滤。
出站规则	从访问控制列表 ID 中选择规则作出站过滤。

表 3.2.3.2 访问控制列表-1

相关配置案例

访问控制应用案例

3.2.3.3 端口映射

端口映射是网络地址转换（NAT）的应用程序，数据通过网络网关（如 CPE 或防火墙）时将通信请求从地址和端口号的组合重定向到另一个。

单击  添加新端口映射规则。

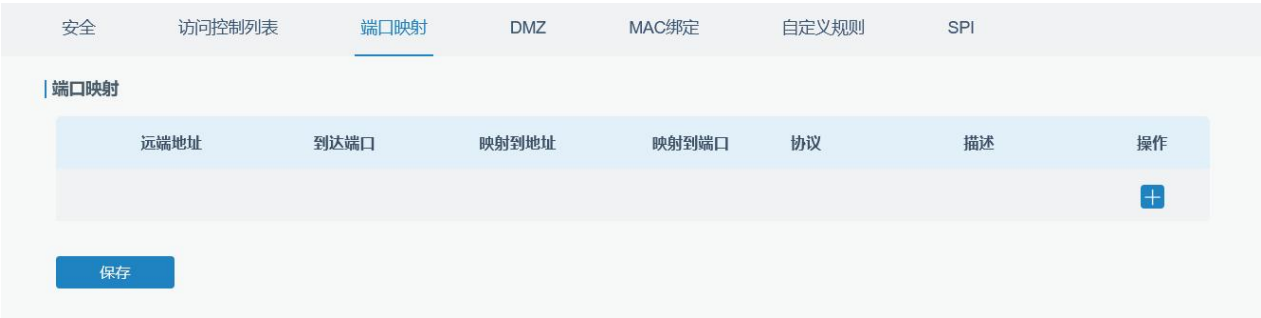


图 3.2.3.3 端口映射-1

端口映射	
项目	描述
远端地址	定义允许访问本地 IP 地址的主机或网络。0.0.0.0/0 代表所有主机或网络。
到达端口	输入外网访问 CPE 的对外端口号或端口号范围。合法值：1-65535。
映射到地址	输入把数据转发到内网的设备的 IP 地址。
映射到端口	输入在传入端口上接收后转发的数据包的 TCP 或 UDP 端口。范围：1-65535。
协议	根据应用从“TCP”、“UDP”、“Both”中选择协议。
描述	输入对该条映射规则的描述。

表 3.2.3.3 端口映射-1

相关配置案例

NAT 应用案例

3.2.3.4 DMZ

DMZ 主机是除了被占用和转发的端口外，其他所有端口都对指定地址开放访问的内网主机。



图 3.2.3.4 DMZ-1

DMZ	
项目	描述
启用	启用/禁用 DMZ 功能。
DMZ 主机 IP 地址	输入内网 DMZ 的 IP 地址。
源 IP 地址	设置可以和 DMZ 主机通话的源 IP 地址。0.0.0.0/0 代表所有的地址都能与 DMZ 主机通话。

表 3.2.3.4 DMZ-1

3.2.3.6 MAC 绑定

MAC 绑定用于通过匹配允许的外部网络访问列表中的 MAC 地址和 IP 地址来指定主机。设置 MAC 绑定后，只有绑定列表里的主机能访问外网。



图 3.2.3.6 MAC 绑定-1

MAC 绑定列表	
项目	描述
MAC 地址	设置绑定的 MAC 地址。

IP 地址	设置绑定的 IP 地址。
说明	便于记录每条 MAC-IP 地址绑定规则的意义。

表 3.2.3.6 MAC 绑定-1

3.2.3.7 自定义规则

自定义规则指通过设置指令来自定义防火墙规则。



图 3.2.3.7 自定义规则-1

自定义规则	
项目	描述
规则	填写防火墙规则指令
描述	方便记录该自定义规则的意义

表 3.2.3.7 自定义规则-1

3.2.3.8 SPI

SPI (Stateful Packet Inspection) 防火墙，全状态数据包检测型防火墙，是指通过对每个连接信息（包括套接字对(socket pairs)：源地址、目的地址、源端口和目的端口；协议类型、TCP 协议连接状态和超时时间等）进行检测从而判断是否过滤数据包的防火墙。



图 3.2.3.8 SPI-1

SPI 防火墙	
项目	描述
启用	启用/禁用 SPI 防火墙功能。
过滤 Proxy	该功能启用后，组织包含 “Host:” 字符串的 HTTP 请求。
过滤 Cookies	识别包含 “Cookie:” 字符串的 HTTP 请求并破坏 cookie。且尝试阻止使用 cookie。
ActiveX 过滤	阻止包含以 “.ocx” 或 “.cab” 结尾的 URL 的 HTTP 请求。
Java Applets 过滤	阻止包含以 “.js” 或 “.class” 结尾的 URL 的 HTTP 请求。
过滤组播包	防止组播数据包到达 LAN。
过滤 IDENT 认证协议	启用该功能可以使 113 端口免于被自己的网络之外的其他设备进行扫描。
阻止广域网的 SNMP 请求	启用该功能可以阻止来自广域网的 SNMP 的请求。
WAN 的重定向过滤	防止 LAN 上的主机使用 CPE 的 WAN 地址联系 LAN 上的服务器(已使用端口重定向配置)
阻止来自 WAN 口的匿名请求	启用该功能，从而防止自己的网络遭受其他的 Internet 用户的 ping 或探测。

表 3.2.3.8 SPI-1

3.2.4 流量控制

流量控制（QoS）是指流量优先级和资源预留控制机制。流量控制旨在为不同的应用程序、用户、数据流提供不同的优先级，保证数据流的合理分配。

图 3.2.3.8 流量控制-1

流量控制	
项目	描述
下行/上行带宽	
启用	开启/关闭流量控制。
默认类别	从服务类别列表中选择默认类别。
总下行/上行带宽	CPE 所连接网络的总下载带宽，单位 kbps。合法值：1-8000000。
服务类别	
名称	用户自定义服务类别的名称。有效字符包括字母、数字、"_"。
比例 (%)	设置服务类别的百分比。合法值：0-100。
最大带宽 (kbps)	当发生阻塞时，实际数据不能超过设置的最大带宽，单位：kbps。需小于总下行带宽。
最小带宽 (kbps)	该服务最小能保证的带宽，单位：kbps。需小于最大带宽。
类别规则	
项目	描述
名称	用户可自定义一个名称。
源地址	流量控制的源地址（空代表所有）。
源端口	流量控制的源端口，合法值：0-65535（空代表所有）。

目的地址	流量控制的目的地址（空代表所有）。
目的端口	流量控制的目的端口。合法值：0-65535（空代表所有）。
协议	选择协议类型，用户可选择“ANY”、“TCP”、“UDP”、“ICMP”、“GRE”。
服务类别	设置该条规则的服务类别。

表 3.2.4 流量控制-1

相关配置案例

[流量控制应用案例](#)

3.2.5 VPN

虚拟专用网络（也称为 VPN）用于将两个专用网络安全地连接在一起，以便设备可以通过安全通道从一个网络连接到另一个网络。

UF51 支持 DMVPN、IPsec、GRE、L2TP、PPTP、OpenVPN，以及 GRE over IPsec 和 L2TP over IPsec。

3.2.5.1 DMVPN

结合 mGRE 和 IPsec 的动态多点虚拟专用网络（DMVPN）是一种安全网络，可在站点之间交换数据，而无需通过组织的总部 VPN 服务器或 CPE 传递流量。

状态	DMVPN	IPsec 服务器	IPsec	GRE	L2TP	PPTP	OpenVPN客户端	OpenVPN服务器	证书管理
网络	启用 ☒								
接口	Hub地址								
DHCP	本地IP地址								
防火墙	GRE Hub IP地址								
流量控制	GRE本地IP地址								
VPN	GRE子网掩码		255.255.255.0						
IP 穿透	GRE密钥								
路由	协商模式		Main						
VRRP	加密算法		DES						
DDNS	认证算法		MD5						
系统	DH组		MODP768-1						
工业	PSK密钥								
维护	本地ID类型		Default						
APP	IKE生存时间(秒)		10800						
	SA算法		DES-MD5						
	PFS组		NULL						
	生存时间(秒)		3600						
	DPD时间间隔(秒)		30						
	DPD超时时间(秒)		150						
	Cisco密钥								
	NHRP保持时间(秒)		7200						

图 3.2.5.1 DMVPN-1

DMVPN 设置	
项目	描述
启用	启用/禁用 DMVPN。
Hub 地址	DMVPN Hub 的 IP 地址或者域名。
本地 IP 地址	DMVPN 本地隧道 IP 地址。
GRE Hub IP 地址	GRE Hub 隧道 IP 地址。
GRE 本地 IP 地址	GRE 本地隧道 IP 地址。
GRE 子网掩码	GRE 本地隧道子网掩码。
GRE 密钥	GRE 隧道密钥
协商模式	从“Main”和“Aggressive”中选择 IKE 协商模式。如果 IPsec 隧道一端的 IP 地址是自动获取的，必须选择“Aggressive”为 IKE 协商模式。在这种情况下，只要用户名和密码正确，就能建立 SAs。
加密算法	从“DES”、“3DES”、“AES128”、“AES192”、“AES256”中选择加密算法应用在 IKE 协商中。 DES：使用 56 位的 DES 加密算法。 3DES：使用 168 位的 3DES 加密算法。 AES128：使用 128 位的 AES 加密算法。

	AES192: 使用 192 位的 AES 加密算法。 AES256: 使用 256 位的 AES 加密算法。
认证算法	从 “MD5” 、 “SHA1” 中选择认证算法应用在 IKE 协商中。
DH 组	从 “MODP768_1” 、 “MODP1024_2” 和 “MODP1536_5” 选择来应用在 IKF 协商中。 MODP768_1: 使用 768-bit Diffie-Hellman 组。 MODP1024_2: 使用 1024-bit Diffie-Hellman 组。 MODP1536_5: 使用 1536-bit Diffie-Hellman 组。
PSK 密钥	输入预共享密钥。
本地 ID 类型	选择 “Default” 、 “ID” 、 “FQDN” 、 “User FQDN” 。 Default: IP 地址。 ID: 在 IKE 协商中把 IP 地址当作 ID。 FQDN: 在 IKE 协商中把正式域名当作 ID。如果选择这一选项, 要把域名中@去掉后再输入, 如 test.user.com。 User FQDN: 在 IKE 协商中把用户正式域名当作 ID。如果选择这一选项, 输入域名时要带上@, 如 test@user.com。
IKE 生存时间 (秒)	在 IKE 协商中设置生存时间。合法值: 60-86400。在 SA 过期之前, IKE 协商出新的 SA。新的 SA 一建立, 它会立即生效。旧的那一个过期后会立即清除。
SA 算法	可以选择 “DES_MD5” 、 “DES_SHA1” 、 “3DES_MD5” 、 “3DES_SHA1” 、 “AES128_MD5” 、 “AES128_SHA1” 、 “AES192_MD5” 、 “AES192_SHA1” 、 “AES256_MD5” 、 “AES256_SHA1” 中选择。注意: 更高的安全性意味着更复杂的实现和更低的速率。DES 能满足一般需求。安全和机密性要求更高是则选用 3DES。
PFS 组	从 “NULL” 、 “MODP768_1” 、 “MODP1024_2” 、 “MODP1536_5” 中选择。 NULL: 禁用 PFS 组。 MODP768_1: 使用 768-bit Diffie-Hellman 组。 MODP1024_2: 使用 1024-bit Diffie-Hellman 组。 MODP1536_5: 使用 1536-bit Diffie-Hellman 组。
生存时间 (秒)	设置 IPSec SA 的生存周期。IPSec 协商建立 SA 时, 采用本端设置的生存周期和对端的生存周期中较小的一个。合法值: 60-86400。

DPD 时间间隔（秒）	设置间隔时间。如果从对端接收不到 IPsec 保护包，过了该间隔时间后，DPD 将会被触发。 DPD：失效对等体检测。DPD 会不定期地检测 IKE 的对端是否失效。本地终端接收到 IPsec 包时，DPD 检测上一次从对端收到 IPsec 包的时间。如果时间超过 DPD 间隔时间，它将发送 DPD hello 包给对端。如果本地终端在 DPD 包回传时间接个内未接到 DPD 确认，它将重传 DPD hello 包。如果本地终端发送 DPD hello 包超过最大重传尝试次数，仍未收到 DPD 确认，就认为对端已经无效，将清除 IKE SA 和基于 IKE SA 的 IPsec SAs。
DPD 超时时间（秒）	设置 DPD（失效对等体检测）包的超时时间。
Cisco 密钥	Cisco NHRP 密钥。
NHRP 保持时间（秒）	NHRP 协议的保持时间。

表 3.2.5.1 DMVPN-1

3.2.5.2 IPsec 服务器

IPsec 对于实现虚拟专用网络以及通过拨号连接到专用网络进行远程用户访问特别有用。IPsec 的一大优点是可以在不需要更改单个用户计算机的情况下处理安全性安排。

IPsec 提供三种安全服务选择：身份验证标头（AH），封装安全负载（ESP）和 Internet 密钥交换（IKE）。AH 本质上允许验证发件人的数据。ESP 支持发送者身份验证和数据加密。IKE 用于密码交换。所有这些都可以保护主机之间、主机和网关之间以及网关之间的一个或多个数据流。

IPsec 是 IETF 制定的一组开放的网络安全协议，在 IP 层通过数据来源认证、数据加密、数据完整性和抗重放功能来保证通信双方 Internet 上传输数据的安全性。减少泄漏和被窃听的风险，保证数据的完整性和机密性，保障了用户业务传输的安全。

状态

网络

接口

DHCP

防火墙

流量控制

VPN

IP 穿透

路由

VRRP

DDNS

系统

DMVPN

IPsec 服务器

IPsec

GRE

L2TP

IPsec 服务器

启用☐

IPsec 模式

隧道

IPsec 协议

ESP

本地子网

本地子网掩码

本地 ID 类型

Default

远端子网

远端子网掩码

远端 ID 类型

Default

IKE 参数☐

SA 参数☐

IPsec 高级☐

保存

图 3.2.5.2 IPsec 服务器-1

IPsec Server	
项目	描述
启用	启用 IPsec 隧道，最大隧道数是 3。
IPsec 模式	从“隧道”和“运输”中选择。隧道：一般用于网关之间或终端到网关之间，网关作为身后主机的代理。运输：用于终端之间或终端和网关之间的通讯。如在工作站到 CPE 之间建立加密的 Telnet 连接。
IPsec 协议	用户可选择 ESP 协议和 AH 认证头协议。AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。AH 协议定义了认证的应用方法，提供数据源认证和完整性保证。ESP：封装安全载荷协议。除提供 AH 认证头协议的所有功能之外，还可对 IP 报文净荷进行加密。ESP 协议允许对 IP 报文净荷进行加密和认证、只加密或者只认证，ESP 没有对 IP 头的内容进行保护。
本地子网	输入 IPsec 保护的本地子网地址。
本地子网掩码	输入 IPsec 保护的本地子网掩码。
本地 ID 类型	从“Default”、“ID”、“FQDN”、“User FQDN”中选择本地 ID 类型应用在 IKE 协商中。 Default：代表 IP 地址。

	ID: 在 IKE 协商中把 IP 地址当作 ID。 FQDN: 在 IKE 协商中把正式域名当作 ID。如果选择这一选项, 要把域名中@去掉后再输入, 如 test.user.com。 User FQDN: 在 IKE 协商中把用户正式域名当作 ID。如果选择这一选项, 输入域名时要带上@, 如 test@user.com。
远端子网	输入 IPsec 远端保护子网地址。
远端子网掩码	输入 IPsec 远端保护子网的子网掩码。
远端 ID 类型	从 "Default" 、 "ID" 、 "FQDN" 、 "User FQDN" 中选择本地 ID 类型应用在 IKE 协商中。 Default: 代表 IP 地址。 ID: 在 IKE 协商中把 IP 地址当作 ID。 FQDN: 在 IKE 协商中把正式域名当作 ID。如果选择这一选项, 要把域名中@去掉后再输入, 如 test.user.com。 User FQDN: 在 IKE 协商中把用户正式域名当作 ID。如果选择这一选项, 输入域名时要带上@, 如 test@user.com。

表 3.2.5.2 IPsec 服务器-1

IKE参数	☒
IKE版本	IKEv1
协商模式	Main
加密算法	DES
认证算法	MD5
DH组	MODP768-1
本地认证类型	PSK
XAUTH	☐
生存时间(秒)	10800

图 3.2.5.2 IPsec 服务器-2

SA参数	☒
SA算法	DES-MD5
PFS组	NULL
生存时间(秒)	3600
DPD时间间隔(秒)	30
DPD超时时间(秒)	150
IPsec高级	>

图 3.2.5.2 IPsec 服务器-3

IKE 参数	
项目	描述
IKE 版本	设置 IKE 协议使用的版本号，支持 IKEv1、IKEv2。
协商模式	设置 IKEv1 的协商模式。 主模式：主模式将密钥交换信息与身份认证信息相分离。这种分离保护了身份信息，从而提供了更高的安全性。 野蛮模式：野蛮模式缺少身份认证，但可以满足某些特定的网络环境需求。如果无法预先知道发起者的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥认证方法来创建 IKE SA，就可以用野蛮模式。
加密算法	用户可选择：DES、3DES、AES128、AES192、AES256。 3DES：使用三个 64bit 的 DES 密钥对明文进行加密； DES：使用 64bit 的密钥对一个 64bit 的明文块进行加密； AES：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。
认证算法	从 “MD5” 和 “SHA1” 中选择认证算法应用在 IKE 协商中。 MD5：使用 HMAC-SHA1； SHA1：使用 HMAC-MD5。
DH 组	从 “MODP768_1”、“MODP1024_2”、“MODP1536_5” 选择来应用在 IKF（网络密钥交换）协商中。 MODP768_1：使用 768-bit Diffie-Hellman 组。 MODP1024_2：使用 1024-bit Diffie-Hellman 组。 MODP1536_5：使用 1536-bit Diffie-Hellman 组。
本地认证类型	从 “PSK”、“CA” 中选择，应用到 IKE 协商中。 PSK：预共享密钥；

	CA: 认证机构。
XAUTH	启用后输入 XAUTH 用户名、密码。
生存时间 (秒)	在 IKE 协商中设置生存时间。合法值: 60-86400。在 SA 过期之前, IKE 协商出新的 SA。新的 SA 一建产, 它会立即生效。旧的那一个过期后会立即清除。
XAUTH 列表	
用户名	输入 XAUTH 认证所需用户名。
密码	输入 XAUTH 认证所需密码。
PSK 列表	
选择器	输入进行 PSK 认证时对应的识别号。
预共享密钥	输入预共享密钥。
SA 参数	
SA 算法	可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、"AES128_MD5"、"AES128_SHA1"、"AES192_MD5"、"AES192_SHA1"、"AES256_MD5"、"AES256_SHA1" 中选择。 注意: 更高的安全性意味着更复杂的实现和更低的速率。DES 能满足一般需求。安全和机密性要求更高是则选用 3DES。
PFS 组	从 "NULL"、"MODP768_1"、"MODP1024_2"、"MODP1536_5" 中选择。 NULL: 禁用 PFS 组; MODP768_1: 使用 768-bit Diffie-Hellman 组; MODP1024_2: 使用 1024-bit Diffie-Hellman 组; MODP1536_5: 使用 1536-bit Diffie-Hellman 组。
生存时间 (秒)	设置 IPsec SA 的生存时间。合法值: 60-86400。注意: 当协商建立 IPsec SAs 时, IKE 将在本地设定生存时间和对端提出的生存之间选择较小的那一个。
DPD 时间间隔 (秒)	设置间隔时间。如果从对端接收不到 IPsec 保护包, 过了该间隔时间后, DPD 将会被触发。 DPD: 失效对等体检测。DPD 会不定期地检测 IKE 的对端是否失效。本地终端接收到 IPsec 包时, DPD 检测上一次从对端收到 IPsec 包的时间。如果时间超过 DPD 间隔时间, 它将发送 DPD hello 包给对端。如果本地终端在 DPD 包回传时间内未接到 DPD 确认, 它将重传 DPD hello 包。如果本地终端发送 DPD hello 包超过最大重传尝试次数, 仍未收到 DPD 确认, 就认为对端已经无效, 将清除 IKE SA 和基于 IKE SA 的 IPsec SAs。

DPD 超时时间（秒）	设置 DPD 包的超时时间。合法值：10-3600。
IPsec 高级	
支持压缩	点击启用后则会压缩 IP 数据包的头部。
基于 IPsec 的 VPN 类型	选择“无”、“GRE”、“L2TP”。在这里可以选择开启 VPN over IPsec 功能。

表 3.2.5.2 IPsec 服务器-2

3.2.5.3 IPsec

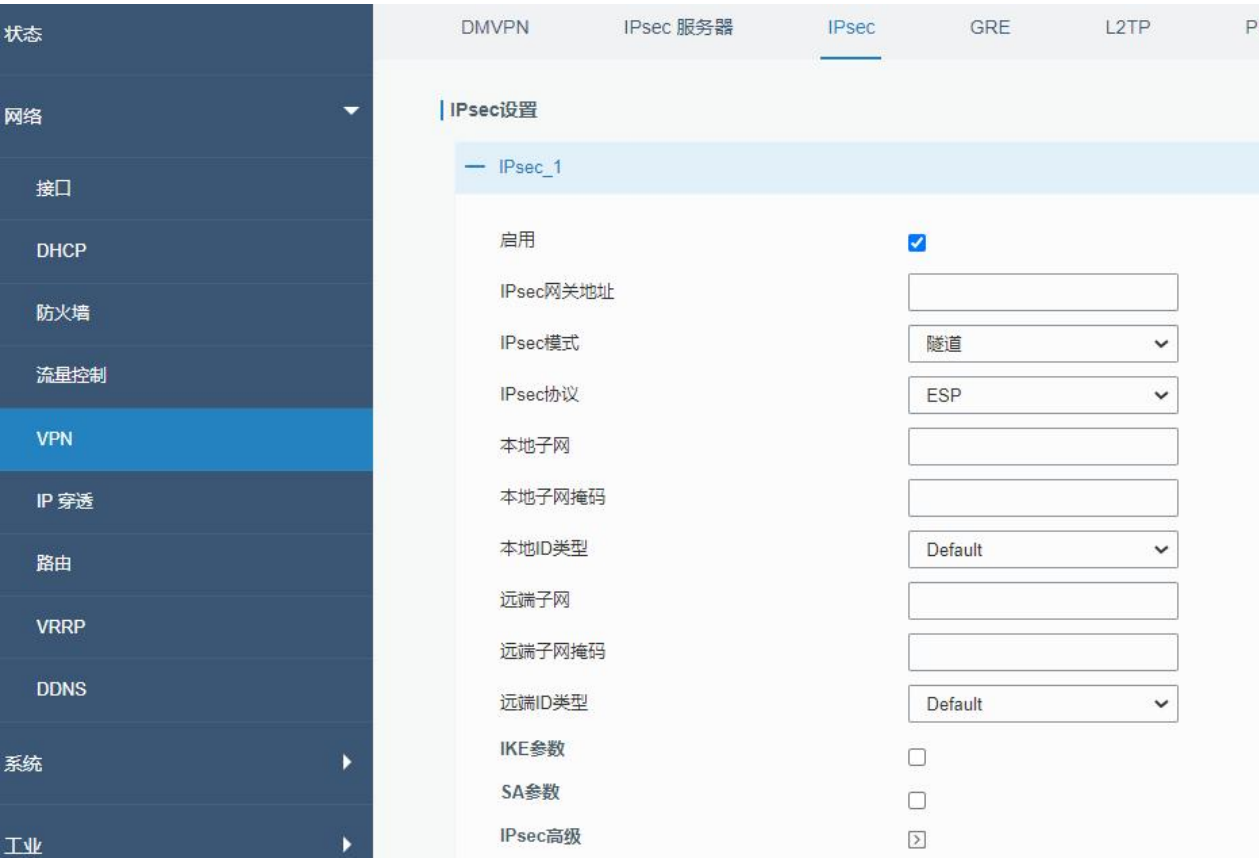


图 3.2.5.3 IPsec-1

IPsec	
项目	描述
启用	启用 IPsec 隧道，最大隧道数是 3。
IPsec 网关地址	输入远端 IPsec 服务器地址(IP/域名)。
IPsec 模式	从“隧道”和“运输”中选择。 隧道：一般用于网关之间或终端到网关之间，网关作为身后主机的代理。

	运输：用于终端之间或终端和网关之间的通讯。如在工作站到 CPE 之间建立加密的 Telnet 连接。
IPsec 协议	用户可选择:ESP 协议和 AH 认证头协议。 AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。AH 协议定义了认证的应用方法，提供数据源认证和完整性保证。 ESP：封装安全载荷协议。除提供 AH 认证头协议的所有功能之外，还可对 IP 报文净荷进行加密。ESP 协议允许对 IP 报文净荷进行加密和认证、只加密或者只认证，ESP 没有对 IP 头的内容进行保护。
本地子网	输入 IPsec 保护的本地子网地址。
本地子网掩码	输入 IPsec 保护的本地子网掩码。
本地 ID 类型	从 Default”、“ID”、“FQDN”、“User FQDN” 中选择本地 ID 类型应用在 IKE 协商中。 Default：代表 IP 地址。 ID：在 IKE 协商中把 IP 地址当作 ID。 FQDN：在 IKE 协商中把正式域名当作 ID。如果选择这一选项，要把域名中@去掉后再输入，如 test.user.com。 User FQDN：在 IKE 协商中把用户正式域名当作 ID。如果选择这一选项，输入域名时要带上@，如 test@user.com。
远端子网	输入 IPsec 远端保护子网地址。
远端子网掩码	输入 IPsec 远端保护子网的子网掩码。
远端 ID 类型	从 “Default”、“ID”、“FQDN”、“User FQDN” 中选择本地 ID 类型应用在 IKE 协商中。 Default：代表 IP 地址。 ID：在 IKE 协商中把 IP 地址当作 ID。 FQDN：在 IKE 协商中把正式域名当作 ID。如果选择这一选项，要把域名中@去掉后再输入，如 test.user.com。 User FQDN：在 IKE 协商中把用户正式域名当作 ID。如果选择这一选项，输入域名时要带上@，如 test@user.com。

表 3.2.5.3 IPSec-1

IKE参数	☒
IKE版本	IKEv1
协商模式	Main
加密算法	DES
认证算法	MD5
DH组	MODP768-1
本地认证类型	PSK
本地密钥	
XAUTH	☒
用户名	
密码	
生存时间(秒)	10800
SA参数	☒
SA算法	DES-MD5
PFS组	NULL
生存时间(秒)	3600
DPD时间间隔(秒)	30
DPD超时时间(秒)	150
IPsec高级	☒
支持压缩	☐
基于IPsec的VPN类型	无

图 3.2.5.3 IPSec-2

IKE 参数	
项目	描述
IKE 版本	设置 IKE 协议使用的版本号，支持 IKEv1、IKEv2。
协商模式	设置 IKEv1 的协商模式。 主模式：主模式将密钥交换信息与身份认证信息相分离。这种分离保护了身份信息，从而提供了更高的安全性。 野蛮模式：野蛮模式缺少身份认证，但可以满足某些特定的网络环境需求。如果无法预先知道发起者的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥认证方法来创建 IKE SA，就可以用野蛮模式。
加密算法	用户可选择：DES、3DES、AES128、AES192、AES256。 3DES：使用三个 64bit 的 DES 密钥对明文进行加密； DES：使用 64bit 的密钥对一个 64bit 的明文块进行加密； AES：使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密。
认证算法	从 “MD5” 和 “SHA1” 中选择认证算法应用在 IKE 协商中。 MD5：使用 HMAC-SHA1；

	SHA1: 使用 HMAC-MD5。
DH 组	从 "MODP768_1"、"MODP1024_2"、"MODP1536_5" 选择来应用在 IKF (网络密钥交换) 协商中。 MODP768_1: 使用 768-bit Diffie-Hellman 组。 MODP1024_2: 使用 1024-bit Diffie-Hellman 组。 MODP1536_5: 使用 1536-bit Diffie-Hellman 组。
本地认证类型	从 "PSK"、"CA" 中选择, 应用到 IKE 协商中。 PSK: 预共享密钥; CA: 认证机构。
XAUTH	启用后输入 XAUTH 用户名、密码。
生存时间 (秒)	在 IKE 协商中设置生存时间。合法值: 60-86400。在 SA 过期之前, IKE 协商出新的 SA。新的 SA 一建产, 它会立即生效。旧的那一个过期后会立即清除。
IKE 版本	设置 IKE 协议使用的版本号, 支持 IKEv1、IKEv2。
SA 参数	
SA 算法	可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、"AES128_MD5"、"AES128_SHA1"、"AES192_MD5"、"AES192_SHA1"、"AES256_MD5"、"AES256_SHA1" 中选择。 注意: 更高的安全性意味着更复杂的实现和更低的速率。DES 能满足一般需求。安全和机密性要求更高是则选用 3DES。
PFS 组	从 "NULL"、"MODP768_1"、"MODP1024_2"、"MODP1536_5" 中选择。 NULL: 禁用 PFS 组; MODP768_1: 使用 768-bit Diffie-Hellman 组; MODP1024_2: 使用 1024-bit Diffie-Hellman 组; MODP1536_5: 使用 1536-bit Diffie-Hellman 组。
生存时间 (秒)	设置 IPsec SA 的生存时间。合法值: 60-86400。注意: 当协商建立 IPsec SAs 时, IKE 将在本地设定生存时间和对端提出的生存之间选择较小的那一个。
DPD 时间间隔 (秒)	设置间隔时间。如果从对端接收不到 IPsec 保护包, 过了该间隔时间后, DPD 将会被触发。 DPD: 失效对等体检测。DPD 会不定期地检测 IKE 的对端是否失效。本地终端接收到 IPsec 包时, DPD 检测上一次从对端收到 IPsec 包的时间。如果时间超过 DPD 间隔时间, 它将发送 DPD hello 包给对端。如果本地

	终端在 DPD 包回传时间内未接到 DPD 确认，它将重传 DPD hello 包。如果本地终端发送 DPD hello 包超过最大重传尝试次数，仍未收到 DPD 确认，就认为对端已经无效，将清除 IKE SA 和基于 IKE SA 的 IPsec SAs。
DPD 超时时间（秒）	设置 DPD 包的超时时间。合法值：10-3600。
IPsec 高级	
支持压缩	点击启用后则会压缩 IP 数据包的头部。
基于 IPsec 的 VPN 类型	选择“无”、“GRE”、“L2TP”。在这里可以选择开启 VPN over IPsec 功能。

表 3.2.5.3 IPsec-2

3.2.5.4 GRE

通用路由封装（GRE）是一种封装数据包的协议，以便通过 IP 网络路由其他协议。GRE 规定如何用一种网络协议去封装另一种网络协议的方法。GRE 协议的主要用途有两个：企业内部协议封装和私有地址封装。它是一种隧道技术，提供了一个通道然后通过该通道可以传输封装的数据消息，并且可以在两端实现封装和解封装。

图 3.2.5.4 GRE-1

GRE	
项目	描述
启用	勾选后启用 GRE 功能。
远端 IP 地址	输入 GRE 隧道的远端真实 IP 地址。
本地 IP 地址	设置本地 IP 地址。
本地虚拟 IP 地址	设置 GRE 隧道的本地隧道 IP 地址。
子网掩码	设置本地子网掩码。
对端虚拟 IP 地址	输入 GRE 隧道的远端隧道 IP 地址。
全局流量转发	勾选后启用这个功能，所有数据流量都会通过 GRE 隧道发送。
远端子网	输入 GRE 隧道的远端子网 IP 地址。
远端子网掩码	输入 GRE 隧道的远端子网掩码。
最大传输单元	最大传输单元。在给定的网络环境中可传输的数据包最大长度的标志符。合法值：64-150。
密钥	设置 GRE 隧道密钥。
启用 NAT	勾选后为 GRE 启用 NAT 穿越。在 NAT 环境中，必须启用这个选项。

表 3.2.5.4 GRE-1

3.2.5.5 L2TP

第二层隧道协议（L2TP）是因特网服务提供商（ISP）使用的点对点隧道协议（PPTP）的扩展，用于通过因特网实现虚拟专用网络（VPN）的操作。L2TP 是一种工业标准的 Internet 隧道协议，功能大致和 PPTP 协议类似，比如同样可以对网络数据流进行加密。

图 3.2.5.5 L2TP-1

L2TP	
项目	描述
启用	勾选后启用 L2TP 功能。
远端 IP 地址	输入 L2TP 服务器的公网 IP 地址或域名。
用户名	输入 L2TP 服务器提供的用户名。
密码	输入 L2TP 服务器提供的密码。
认证类型	从“自动”、“PAP”、“CHAP”、“MS-CHAPv1”、“MS-CHAPv2”中选择。L2TP 客户端应该和 L2TP 服务器端选择的认证类型一致。当选择“自动”时，CPE 会根据服务器的认证类型自动选择正确的认证类型。
全局流量转发	勾选启用后，所有数据流量都会通过 L2TP 隧道发送。
远端子网	输入 L2TP 远端保护的子网地址。
远端子网掩码	输入 L2TP 远端保护的子网掩码。
密钥	输入 L2TP 隧道密码。

表 3.2.5.5 L2TP-1

启用网络地址转换 (NAT)

☒

启用MPPE

☐

地址/控制压缩

☐

协议字段压缩

☐

Asyncmap值

最大接收单元 (MRU)

最大传输单元 (MTU)

链路检测间隔时间 (秒)

最大重连次数

专家选项

图 3.2.5.5 L2TP-2

高级选项	
项目	描述
本地 IP 地址	设置 L2TP 客户端的隧道 IP 地址。可以输入 L2TP 服务器分配的 IP 地址。

	不填意味着 L2TP 客户端将从 L2TP 服务器的 IP 地址池中自动获取 IP 地址。
对端 IP 地址	输入 L2TP 服务器隧道 IP 地址
启用网络地址转换 (NAT)	点击后启用 L2TP 的 NAT 穿越功能。
启用 MPPE	启用 MPPE 加密。
地址/控制压缩	用于 PPP 初始化。一般保持默认。
协议字段压缩	用于 PPP 初始化。一般保持默认。
Asyncmap 值	PPP 协议初始化字符串之一。合法值：0-ffffff，一般没必要改变这个值。
最大接收单元 (MRU)	最大接收单元。在给定的网络环境中可接收的数据包最大长度的标识符。合法值：64-1500。
最大传输单元 (MTU)	最大传输单元。在给定的网络环境中可传输的数据包最大长度的标识符。合法值：64-1500。
链路检测间隔时间 (秒)	为了检测隧道的链接，客户端和服务端周期性地给彼此发送 PPP 回应。如果在指定时间内，客户端或服务端接收不到对端 PPP 回应，它会重传 PPP 回应。如果超过最大重连次数，服务端或客户端还没从对端接收到答复，将会判定 L2TP 隧道断掉了，会尝试再次和对端建立连接。合法值：0-600。
最大重连次数	指定 L2TP 链接检测失败最大的重试次数。合法值：0-10。
专家选项	可以在此字段中输入一些其他 PPP 初始化的字符串。每个字符串用空格分开。

表 3.2.5.5 L2TP-2

3.2.5.6 PPTP

点对点隧道协议 (PPTP) 是一种允许公司通过公共互联网上的私有“隧道”扩展其自己的公司网络的协议。实际上，公司使用广域网作为单个大型局域网。该协议是在 PPP 协议的基础上开发的一种新的增强型安全协议，支持多协议虚拟专用网 (VPN)，可以通过密码身份验证协议 (PAP)，可扩展身份验证协议 (EAP) 等方法增强安全性。

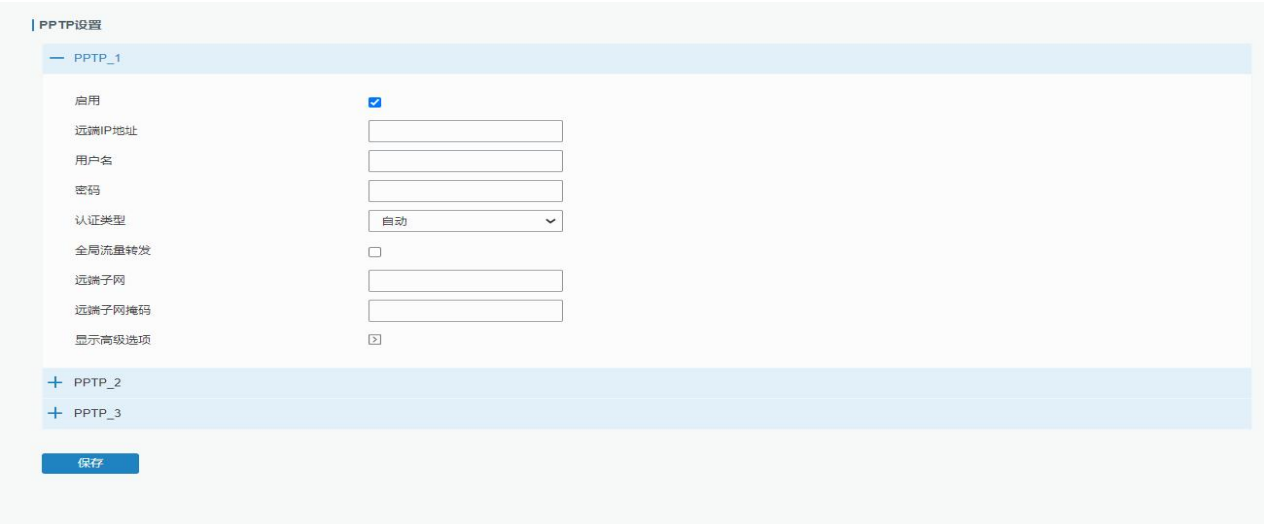


图 3.2.5.6 PPTP-1

PPTP	
项目	描述
启用	启用 PPTP 客户端。最多可建立 3 个虚拟隧道。
远端 IP 地址	输入 PPTP 服务器的公网 IP 或域名。
用户名	输入 PPTP 服务器提供的用户名
密码	输入 PPTP 服务器提供的密码
认证类型	从“自动”、“PAP”、“CHAP”、“MS-CHAPv1”、“MS-CHAPv2”中选择。L2TP 客户端应该和 L2TP 服务器端选择的认证类型一致。当选择“自动”时，CPE 会根据服务器的认证类型自动选择正确的认证类型。
全局流量转发	勾选后启用这个功能，所有数据流量都会通过 PPTP 隧道发送。
远端子网	设置 PPTP 对端子网。
远端子网掩码	设置 PPTP 对端的子网掩码。

表 3.2.5.6 PPTP-1

显示高级选项

本地IP地址

对端IP地址

启用NAT

启用MPPE

地址/控制压缩

协议字段压缩

Asyncmap/值

最大接收单元 (MRU)

最大传输单元 (MTU)

链路检测间隔时间 (秒)

最大重连次数

专家选项

☒

☒

☐

☐

☐

图 3.2.5.6 PPTP-2

PPTP 高级设置	
项目	描述
本地 IP 地址	设置 PPTP 客户端的隧道 IP 地址。可以输入 PPTP 服务器分配的 IP 地址。不填意味着 PPTP 客户端将从 PPTP 服务器的 IP 地址池中自动获取 IP 地址。
对端 IP 地址	输入 PPTP 服务器隧道 IP 地址。
启用 NAT	勾选后启用 NAT 穿越功能。
启用 MPPE	勾选后启用 MPPE 加密。
地址/控制压缩	用于 PPP 初始化。一般保持默认。
协议字段压缩	用于 PPP 初始化。一般保持默认。
Asyncmap 值	PPP 协议初始化字符串之一。一般没必要改变这个值。默认值：0-ffffff。
最大接收单元（MRU）	最大接收单元。在给定的网络环境中可接收的数据包最大长度的标识符。合法值：0-1500。
最大传输单元（MTU）	最大传输单元。在给定的网络环境中可传输的数据包最大长度的标识符。合法值：0-1500。
链路检测间隔时间（秒）	为了检测隧道的链接，客户端和服务端周期性地给彼此发送 PPP 回应。如果在指定时间内，客户端或服务端接收不到对端 PPP 回应，它会重传 PPP 回应。如果超过最大重连次数，服务端或客户端还没从对端接收到答复，将会判定 PPTP 隧道断掉了，会尝试再次和对端建立连接。合法值：0-600。
最大重连次数	指定 PPTP 链接检测失败最大的重试次数。合法值：0-10。
专家选项	可以在此字段中输入一些其他 PPP 初始化的字符串。每个字符串用空格分开。

表 3.2.5.6 PPTP-2

相关配置案例

[PPTP 应用案例](#)

3.2.5.7 OpenVPN 客户端

OpenVPN 是一种开源虚拟专用网络（VPN）产品，提供简化的安全框架，模块化网络设计和跨平台可移植性。

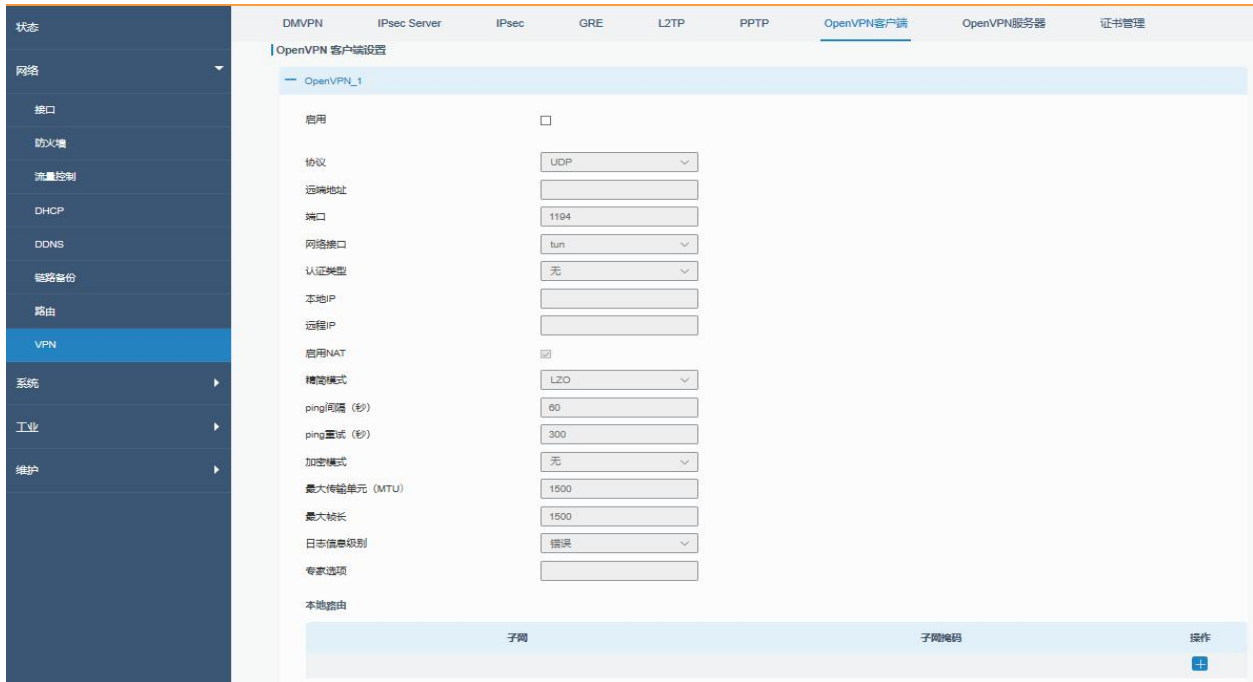


图 3.2.5.7 OpenVPN 客户端-1

OpenVPN 客户端	
项目	描述
启用	启用 OpenVPN 客户端，最多可建立 3 条隧道。
协议	根据应用需求，从“UDP”和“TCP”中选择。
远端 IP 地址	输入远端 OpenVPN 服务器 IP 地址或域名。
端口	输入远端 OpenVPN 服务器的监听端口。合法值：1-65535。
网络接口	从“tun”和“tap”这两种不同的 OpenVPN 设备接口中选择。tun 与 tap 的不同之处是：tun 设备是网络层点到点的虚拟设备，tap 是以太网链路层的虚拟设备。
认证类型	从“无”、“共享静态密钥”、“用户名/密码”、“单客户端证书认证”和“用户/密码+证书认证”中选择。
本地 IP	设置 OpenVPN 隧道的本地隧道地址。
远程 IP	设置 OpenVPN 隧道的远程隧道地址。
全局流量转发	勾选后启用这个功能，所有数据流量都会通过 OpenVPN 隧道发送。
启用 TLS 认证	勾选后启用 TLS 认证功能。
用户名	输入 OpenVPN 服务器提供的用户名。
密码	输入 OpenVPN 服务器提供的密码。
启用 NAT	勾选后启用 NAT 穿越的功能。在 NAT 环境中必须启用该功能。
精简模式	选择“LZO”使用 LZO 压缩库来压缩数据流。

Ping 间隔 (秒)	设置 ping 时间间隔, 以检查隧道是否断开。合法值: 10-1800。
Ping 重试 (秒)	如果在这段时间内一直超时, 将重新建立 OpenVPN 隧道。合法值: 60-3600。
加密模式	从 "NONE"、"BF-CBC"、"DE-CBC"、"DES-EDE3-CBC"、"AES-128-CBC"、"AES-192-CBC"、"AES-256-CBC" 中选择加密算法和服务器匹配。
最大传输单元 (MTU)	最大传输单元。在给定的网络环境中可传输的数据包最大长度的标志符。合法值: 128-1500
最大帧长	设置传输的最大帧长度。合法值: 128-1500。
日志信息级别	从低到高选择输出日志级别: "错误"、"提示"、"注意"、"调试"。级别越高输出的日志信息越多。
专家选项	可以在此字段中输入一些其他 PPP 初始化的字符串。每个字符串用空格分开
本地路由	
子网 IP	设置本地路由 IP 地址。
子网掩码	设置本地路由子网掩码。

表 3.2.5.7 OpenVPN 客户端-1

3.2.5.8 OpenVPN 服务器

UF51 支持 OpenVPN 服务器, 可在路由或桥接配置和远程访问设施中创建安全的点对点或站点到站点连接。

状态	DMVPN	IPsec 服务器	IPsec	GRE	L2TP	PPTP	OpenVPN客户端	OpenVPN服务器
网络	OpenVPN服务器设置							
接口	启用 ☒							
DHCP	协议 UDP							
防火墙	端口 1194							
流量控制	监听IP							
VPN	网络接口 tun							
IP 穿透	认证类型 无							
路由	本地IP							
VRRP	远程IP							
DDNS	启用NAT ☒							
系统	精简模式 LZO							
工业	ping间隔 60							
维护	ping重试 150							
APP	加密模式 无							
	最大传输单元 (MTU) 1500							
	最大帧长 1500							
	日志信息级别 错误							
	专家选项							

图 3.2.5.8 OpenVPN 服务器-1

账号

用户名	密码	操作
		+

本地路由

子网	子网掩码	操作
		+

客户端子网

名称	子网	子网掩码	操作
			+

保存

图 3.2.5.8 OpenVPN 服务器-2

OpenVPN 服务器	
项目	描述
启用	启用/禁用 OpenVPN 服务器。
协议	根据应用需求，选择“UDP”或“TCP”。
端口	输入监听端口，合法值：1-65535。
监听 IP	可以输入移动广域网，以太广域网或以太局域网的 IP 地址。不填代表所有当前活跃的广域网链接、移动广域网或以太广域网。
网络接口	从“tun”和“tap”这两种不同的 OpenVPN 设备接口中选择。tun 与 tap 的不同之处是：tun 设备是网络层点到点的虚拟设备，tap 是以太链路层的虚拟设备。
认证类型	从“无”、“共享静态密钥”、“用户名/密码”、“多客户端用户认证”和“用户/密码+证书认证”。
本地 IP	OpenVPN 的隧道的本地隧道地址。
远程 IP	OpenVPN 的隧道的对端隧道地址。
客户端子网	客户端的本地子网 IP 地址。
客户端子网掩码	客户端的本地子网掩码。
重新协商时间间隔（秒）	重新协商时间间隔。合法值：0-86400。
最大用户数	最大客户端数量。合法值：1-128。
启用证书吊销列表	启用证书吊销列表。
启用客户端到客户端	允许客户端之间互相访问。
启用多用户使用同一证书	允许多个用户使用同一个证书

启用 NAT	勾选后启用 NAT 穿越功能。在 NAT 环境中必须启用该功能。
精简模式	选择“LZO”使用 LZO 压缩库来压缩数据流。
Ping 间隔	设置检查隧道是否断开的 ping 时间间隔。合法值：10-1800
Ping 重试（秒）	设置链路断开超时时间。合法值：60-3600。
加密模式	从“NONE”、“BF-CBC”、“DES-CBC”、“DES-EDE3-CBC”、“AES-128-CBC”、“AES-192-CBC”、“AES-256-CBC”中选择加密算法。
最大传输单元（MTU）	最大传输单元。在给定的网络环境中可传输的数据包最大长度的标志符。合法值：64-1500。
最大帧长	设置传输的最大帧长度。合法值：64-1500。
日志信息级别	从低到高选择输出日志级别：“错误”、“提示”、“注意”、“调试”。级别越高输出的日志信息越多。
专家选项	可以在此字段中输入一些其他 PPP 初始化的字符串。每个字符串用空格分开。
本地路由	
子网	OpenVPN 服务器到客户端的路由，一般填写客户端实际通讯的子网。
子网掩码	OpenVPN 服务器到客户端的路由的子网掩码，一般填写客户端实际通讯的子网掩码。
账号	
用户名与密码	设置 OpenVPN 客户端使用用户名、密码方式验证登陆。

表 3.2.5.8 OpenVPN 服务器-1

3.2.5.9 证书管理

导入证书/密钥文件到 CPE 或导出证书/密钥文件到电脑。

DMVPN
IPsec 服务器
IPsec
GRE
L2TP
PPTP
OpenVPN客户端
OpenVPN服务器
证书管理

OpenVPN客户端

OpenVPN 客户端_1

CA证书		浏览	导入	导出	删除
证书		浏览	导入	导出	删除
私钥		浏览	导入	导出	删除
TA		浏览	导入	导出	删除
预共享密钥		浏览	导入	导出	删除
PKCS12		浏览	导入	导出	删除

+ OpenVPN 客户端_2
+ OpenVPN 客户端_3

图 3.2.5.9 证书管理-1

OpenVPN 客户端	
项目	描述
CA 证书	导入/导出根证书文件。
公钥	导入/导出公钥文件。
私钥	导入/导出私钥文件。
TA	导入/导出 TA 密钥文件。
预共享密钥	导入/导出预共享密钥文件。
PKCS12	导入/导出 PKCS12 证书文件。

表 3.2.5.9 证书管理-1

OpenVPN服务器

OpenVPN 服务器

CA证书

浏览

导入

导出

删除

证书

浏览

导入

导出

删除

私钥

浏览

导入

导出

删除

DH

浏览

导入

导出

删除

TA

浏览

导入

导出

删除

证书吊销列表

浏览

导入

导出

删除

预共享密钥

浏览

导入

导出

删除

图 3.2.5.9 证书管理-2

OpenVPN 服务器	
项目	描述
CA 证书	导入/导出根证书文件。
公钥	导入/导出公钥文件。
私钥	导入/导出私钥文件。
DH	导入/导出 DH 密钥交换文件。
TA	导入/导出 TA 密钥文件。
证书吊销列表	导入/到处证书吊销列表。
预共享密钥	导入/导出预共享密钥文件。

表 3.2.5.9 证书管理-2

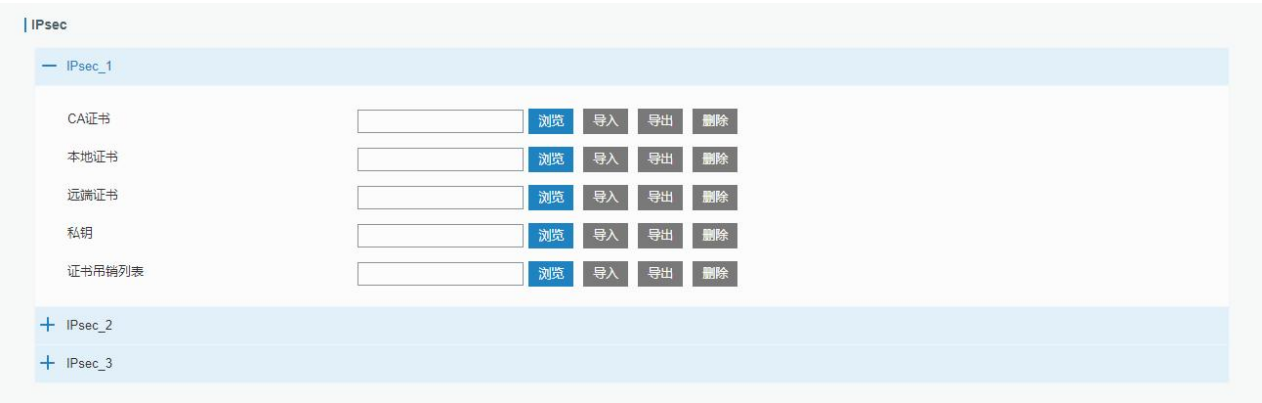


图 3.2.5.9 证书管理-3

IPsec	
项目	描述
CA 证书	导入/导出根证书文件。
本地证书	导入/导出本地证书文件。
远端证书	导入/导出远端证书文件。
私钥	导入/导出私钥文件。
证书吊销列表	导入/导出证书吊销列表。

表 3.2.5.9 证书管理-3



图 3.2.5.9 证书管理-4

IPsec 服务器	
项目	描述
CA 证书	导入/导出 CA 证书。
本地证书	导入/导出本地证书。
私钥	导入/导出私钥。
证书吊销列表	导入/导出证书吊销列表。

表 3.2.5.9 证书管理-4

3.2.6 IP 穿透

IP 穿透，将 CPE 获取到的蜂窝 IP 直接透传给连接在 CPE 下面的终端设备。



图 3.2.6 IP 穿透-1

IP 穿透	
项目	描述
启用	启用/禁用 IP 穿透。
穿透模式	设置穿透模式，可选择 “DHCP Fixed” 、 “DHCP Dynamic” 。
MAC	设置 MAC 地址。

表 3.2.6 IP 穿透-1

3.2.7 路由

3.2.7.1 静态路由

静态路由是指手动配置，手动输入有关路由的信息，而不是从动态路由流量中获取。设置静态路由后，指定目标的包将被转发到用户指定的路径。



图 3.2.7.1 静态路由-1

静态路由	
项目	描述
目的网络	输入需要到达的目的 IPv4/IPv6 地址。
子网掩码/前缀长度	输入需要到达的目的地址的子网掩码/前缀长度。
接口	数据到达目的网络使用的接口。
网关	输入数据在到达目的地之前, 需要经过的下一个 CPEIPv4/IPv6 地址。
距离	即优先权, 数值越小优先级越高。合法值: 1-255。

表 3.2.7.1 静态路由-1

相关内容

[跟踪设定](#)

3.2.7.2 RIP

RIP 主要用于小型网络。RIP 使用跳数来测量到目标地址的距离, 称为度量。在 RIP 中, 从 CPE 到其直连网络的跳数为 0, 通过 CPE 到达的网络跳数为 1, 依此类推。为了限制收敛时间, RIP 的指定度量是 0 到 15 范围内的整数, 大于或等于 16 的跳数被定义为无穷大, 这意味着目标网络或主机不可达。由于此限制, RIP 不适用于大规模网络。为了提高性能并防止路由环路, RIP 支持水平分割功能。RIP 还引入了由其他路由协议获得的路由。

静态路由

RIP

OSPF

路由过滤

RIP设置

启用

☒

更新定时器

30

秒

超时定时器

180

秒

清除定时器

120

秒

版本

v2

▼

显示高级选项

☒

缺省信息发布

☐

缺省度量

1

重分发直连路由

☐

重分发静态路由

☐

重分发OSPF路由

☐

图 3.2.7.2 RIP-1

RIP	
项目	描述
启用	启用/禁用 RIP。
更新定时器	定义了发送路由更新的时间间隔，合法值：5-2147483647（秒）。
超时定时器	超时定时器定义了路由老化时间，如在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16，合法值：5-2147483647（秒）。
清除定时器	定义一条路由从度量值变为 16 开始直到它从路由表里被删除所经过的时间。在垃圾回收时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如垃圾回收超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。合法值：5-2147483647（秒）。
版本	RIP 版本号，用户可选择“默认”、“v1”、“v2”。
显示高级选项	
缺省信息发布	启用后将发布缺省信息。
缺省度量	本 CPE 到达目的地的缺省开销。合法值：0-16。
重分发直连路由	点选启用。
重分发路由度量	启用重分发直连路由后，设置分发直连路由的路由度量。合法值：0-16。
重分发静态路由	点选启用。
重分发路由度量	启用分发静态路由后，设置分发静态路由的路由度量。合法值：0-16。
重分发 OSPF 路由	点选启用
重分发路由度量	启用 OSPF 路由后，此项用于设置分发动态路由的路由度量。合法值：0-16。

表 3.2.7.2 RIP-1

被动接口只接收 RIP 报文，不发送 RIP 报文。

配置邻居后，RIP 包将只发送到邻居 CPE。

距离/度量管理

距离	IP地址	子网掩码	访问列表名	操作

重分发路由度量

重分发路由度量	出入过滤策略	接口	访问列表名	操作

路由过滤策略

策略类型	策略名	出入过滤策略	接口	操作

被动接口

被动接口	操作

接口

接口	RIP发送版本	RIP接收版本	水平分割/毒性翻转	认证方式	密钥	密钥链	操作

邻居

IP地址	操作

网络

IP地址	子网掩码	操作

保存

图 3.2.7.2 RIP-2

项目	描述
距离/度量管理	
距离	设置学习到的某条 RIP 路由的管理距离。合法值：1-255。
IP 地址	需要设置的 RIP 路由的 IP 地址。
子网掩码	需要设置的 RIP 路由的子网掩码。
访问列表名	设置某条路由引用的访问策略。
重分发路由度量	设置接口收到或发送路由的度量值。合法值：0-16。
出/入过滤策略	用户可选择 “in” / “out” 。 in：进入 CPE 的时候访问列表配置生效； out：出 CPE 的时候访问列表配置生效。
接口	选择路由的接口。
访问列表名	用户配置的路由策略的访问列表名称。
路由过滤策略	
策略类型	用户可选择 “access-list” 、 “prefix-list” 。
策略名	用户配置的前缀列表名。
出入过滤策略	用户可选择 “in” 、 “out” 。
接口	用户可选择 “cellular0” 、 “FE1” 、 “FE0” 。
被动接口	
被动接口	用户可选择 “cellular0” 、 “WAN” 、 “Bridge0” 。

接口	
接口	用户可选择 “cellular0” 、 “WAN” 、 “Bridge0” 。
RIP 发送版本	用户可选择 “默认” 、 “v1” 、 “v2” 。
RIP 接收版本	用户可选择 “默认” 、 “v1” 、 “v2” 。
水平分割	启用/禁用水平分割。
认证方式	用户可选择 “text” 、 “md5” 。
密钥	RIPV2 报文交互时使用的验证密钥。
密钥链	RIPV2 报文交互时使用的验证密钥链。
邻居	
IP 地址	手动配置的 RIP 邻居地址。
网络	
IP 地址	RIP 需要发布出去接口的 IP 地址。
子网掩码	RIP 需要发布出去接口的子网掩码。

表 3.2.7.2 RIP-2

3.2.7.3 OSPF

OSPF 是开放最短路径优先的简称，是基于 IETF 开发的内部网关协议的链路状态。

如果 CPE 想要运行 OSPF 协议，则应该有一个可以手动配置的 CPEID。如果没有配置 CPE ID，系统会自动选择接口的 IP 地址作为 CPE ID。选择顺序如下：

- 如果配置了 Loopback 接口地址，则最后配置的 Loopback 接口 IP 地址将作为 CPE ID；
- 如果没有配置 Loopback 接口地址，系统将选择 IP 地址最大的接口作为 CPE ID。

OSPF 的五种类型的数据包：

- **Hello 包**
- **DD 包**（数据库描述包）
- **LSR 包**（链路状态请求包）
- **LSU 数据包**（链路状态更新数据包）
- **LSAck 数据包**（Link-Sate 确认数据包）

建立邻居关系

OSPF CPE 启动后，将通过 OSPF 接口发出 Hello 报文。收到 Hello 报文后，OSPF CPE 将检查报文中定义的参数。如果它是一致的，将形成邻居关系。并非邻居关系中的所有匹配方都可以形成邻接关系。

它由网络类型决定。只有当双方成功交换 DD 报文并实现 LSDB 同步时，才能形成真正意义上的邻接。LSA 描述了 CPE 周围的网络拓扑，LSDB 描述了整个网络拓扑。

链路状态广播（LSA），是链接状态协议使用的一个分组，它包括有关邻居和本通道成本的信息。LSA 被 CPE 接收用于他们的路由选择表。

静态路由

RIP

OSPF

路由过滤

OSPF设置

启用

☒

路由ID

ABR类型

CISCO

RFC1583兼容性

☒

OSPF可选LSA

☐

SPF延时时间

0

毫秒

SPF初始化时间

50

毫秒

SPF最大时间

5000

毫秒

参考带宽

100

兆比特

接口

图 3.2.7.3 OSPF-1

OSPF 设置	
项目	描述
启用	启用/禁用 OSPF。
路由 ID	始发 LSA 的路由 ID（即 IP 地址）。
ABR 类型	用户可选择 “cisco” 、 “ibm” 、 “standard” 、 “shortcut” 。
RFC1583 兼容性	启用/禁用
OSPF 可选 LSA	启用/禁用。
SPF 延时时间	设置 OSPF SPF 计算的延时时间。合法值：0-6000000（毫秒）。
SPF 初始化时间	设置 OSPF SPF 初始化时间。合法值：0-6000000（毫秒）。
SPF 最大时间	设置 OSPF SPF 最大时间。合法值：0-6000000（毫秒）。
参考带宽	合法值：1-4294967（Mb）。

表 3.2.7.3 OSPF-1

接口

接口	Hello 定时器 (秒)	Dead 定时器 (秒)	重传LSA延迟定时器 (秒)	传送LSA延迟定时器 (秒)	操作

接口高级选项 ☒

接口	网络	接口开销值	协议优先级	认证方式	密钥ID	密钥	操作

图 3.2.7.3 OSPF-2

项目	描述
接口	
接口	需要配置 OSPF 参数的接口，用户可选择 “cellular0” 、 “Bridge0” 。
Hello 定时器 (秒)	发送 Hello 报文的时间间隔。如果相邻两台 CPE 的 Hello 时间间隔不同，则不能建立邻居关系。合法值：1-65535。
Dead 定时器 (秒)	失效时间。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台 CPE 的失效时间不同，则不能建立邻居关系。合法值：1-65535。
重传 LSA 延迟定时器 (秒)	CPE 向他的邻居通告一条 LSA 后，需要对方进行确认。若在重传间隔期间内没有收到对方的确认报文，就会向邻居重传这条 LSA。合法值：3-65535。
传送 LSA 延迟定时器 (秒)	OSPF 报文在链路上发送时也需要花费时间，所以 LSA 的老化时间 (age) 在传送之前要增加一定的延迟时间，在低速链路上需要对该项配置进行重点考虑。合法值：1-65535
接口高级选项	
接口	选择接口。
网络	选择 OSPF 网络类型。
接口开销值	设置接口运行 OSPF 时的开销值。缺省情况下，OSPF 会依据接口的带宽自动计算开销值。合法值：1-65535。
协议优先级	配置 CPE 接口的 OSPF 优先级。合法值：0-255。
认证方式	设置 OSPF 区域所使用的认证模式。如果选择 Simple 认证模式，则还需要配置简单认证密码以及对该密码再进行一次确认。如果选择 MD5 认证模式，则还需要配置 MD5 键值和密码以及对该密码再进行一次确认。
密钥 ID	只在选择 MD5 认证模式时生效，合法值：1-255。
密钥	OSPF 报文交互时的验证密钥。

表 3.2.7.3 OSPF-2

被动接口				
被动接口				操作
				+
网络				
IP地址	子网掩码	域ID	操作	
				+
邻居				
IP地址	优先级	间隔	操作	
				+
域				
域ID	域	禁止路由汇总	认证方式	操作
				+

图 3.2.7.3 OSPF-3

项目	描述
被动接口	
被动接口	用户可选择 “cellular0” 、 “Bridge0” 。
网络	
IP 地址	本地网络的 IP 地址。
子网掩码	本地网络的子网掩码。
域 ID	始发 LSA 的 CPE 所在的区域 ID。
域	
域 ID	设置 OSPF 区域的 ID 号（值为 IP 格式）。
域	设置 OSPF 区域为 Stub 或 NSSA 区域。骨干区域（区域 ID 为 0.0.0.0 的区域）不能被设置为 Stub 或 NSSA 区域。
禁止路由汇总	禁止路由汇总。
认证方式	用户可选择 “simple” 、 “md5” 。

表 3.2.7.3 OSPF-3

域高级选项



域地址汇总

域ID	IP地址	子网掩码	禁止域间路由信息	接口开销值	操作
					

域过滤策略

域ID	路由过滤策略	访问列表名	操作
			

域间虚链路

域ID	ABR地址	认证方式	密钥ID	密钥	Hello定时器	Dead定时器	重传LSA延迟定时器	传送LSA延迟定时器	操作
									

路由重分发

路由重分发类型	指定重分发路由度量	外部路由的类型	路由映射	操作
				

图 3.2.7.3 OSPF-4

域高级选项	
项目	描述
域地址汇总	
域 ID	接口运行 OSPF 时所属的区域 ID 号。
IP 地址	设置接口所在网段 IP 地址。
子网掩码	设置接口所在网段子网掩码。
禁止域间路由信息	禁止 OSPF 域内路由信息在不同域之间传播。
接口开销值	合法值：0-16777215。
域过滤策略	
域 ID	选择过滤策略应用的 OSPF 域号。
路由过滤策略	用户可选择：“import”、“export”、“filter-in”、“filter-out”。
访问列表名	根据配置的访问列表名（在“路由过滤”页面配置）来控制域的路由过滤。只有在配置的访问列表里的路由才生效。
域间虚链路	
域 ID	设置 OSPF 区域的 ID 号。
ABR 地址	连接多外区域的 CPE 是 ABR，配置 ABR 与此域连接的接口地址。
认证方式	用户可选择“simple”、“md5”。
密钥 ID	只在选择 MD5 认证模式时生效，合法值：1-15。
密钥	OSPF 报文交换时的验证密钥。
Hello 定时器	设置接口发送 Hello 报文的时间间隔。合法值：1-65535。

Dead 定时器	发送 Hello 报文的超时时间，合法值：1-65535。
重传 LSA 延迟定时器	当 LSA 传输失败后重新发送 LSA 的时间，合法值：1-65535。
传送 LSA 延迟定时器	LSA 发送时的延时时间，合法值：1-65535。

表 3.2.7.3 OSPF-4

重分发高级选项

☒

总是重分发默认路由

☐

默认路由重分发度量值

0

默认路由重分发度量类型

1

管理距离

域类型	距离	操作

图 3.2.7.3 OSPF-5

项目	描述
路由重分发	
路由重分发类型	用户可选择 “connected” 、 “static” 、 “rip” 。
指定重分发路由度量	设备发送重分发路由时指定的度量值。合法值： 0-16777214。
外部路由的类型	设置引入的外部路由的路由类型。其中， Type1 外部路由表示此类路由的可信度较高。Type2 外部路由表示此类路由的可信度较低。
路由映射	主要用于管理重发布的时候的路由
重分发高级选项	
总是重分发默认路由	设备启动后发送重分发默认路由。
默认路由重分发度量值	发送重分发默认路由的度量值。合法值： 0-16777214。
默认路由重分发度量类型	用户可选择 “0” 、 “1” 、 “2” 。
距离管理	
域类型	用户可选择 “intra-area” 、 “inter-area” 、 “external” 。
距离	设置域学习的 OSPF 路由距离。合法值： 1-255。

表 3.2.7.3 OSPF-5

3.2.7.4 路由过滤



图 3.2.7.4 路由过滤-1

路由过滤	
项目	描述
访问控制列表	
访问列表名	用户自定义名称，字母或下划线开头，只允许字母、数字、下划线。
行动	用户可选择“permit”、“deny”。
任意匹配	不需要再配地址和子网掩码。
IP 地址	用户自定义。
子网掩码	用户自定义。
前缀列表	
前缀列表名	用户自定义名称，字母或下划线开头，只允许字母、数字、下划线。
序号	一个前缀列表名可以配置多个规则，一个规则对应一个序号。合法值：1-4294967295。
行动	用户可选择“permit”、“deny”。
任意匹配	不需要再配地址、子网掩码、大于前缀长度、小于前缀长度。
IP 地址	用户自定义。
子网掩码	用户自定义。
大于前缀长度	填写子网掩码的网络标示位长度，限制 IP 段的最小 IP 地址。合法值：0-32。
小于前缀长度	填写子网掩码的网络标示位长度，限制 IP 段的最大 IP 地址。合法值：0-32。

表 3.2.7.4 路由过滤-1

3.2.8 VRRP

虚拟 CPE 冗余协议（VRRP）是一种计算机网络协议，可为参与的主机自动分配可用的互联网协议（IP）CPE。IP 子网中选择自动默认网关增加了路由路径的可用性和可靠性。

增加出口网关的数量是提高系统可靠性的常用方法。VRRP 将一组承担网关功能的 CPE 添加到备份组中，形成虚拟 CPE。VRRP 的选举机制将决定哪个 CPE 承担转发任务，而局域网中的主机只需要配置虚拟 CPE 的默认网关。

在 VRRP 中，CPE 需要了解虚拟主 CPE 中的故障。为此，虚拟主 CPE 向同一 VRRP 组中的虚拟备份 CPE 发送组播“alive”通告。

编号最大的 VRRPCPE 将成为虚拟主 CPE。VRRPCPE 的编号范围为 1 到 255，通常我们使用 255 表示最高优先级，100 表示 备份。

如果当前虚拟主 CPE 从具有更高优先级的组成员（CPEID）接收到通告，则后者将抢占并成为虚拟主 CPE。

VRRP	
VRRP状态	
状态	禁用
VRRP设置	
启用	☒
接口	Bridge0
虚拟路由器ID	1
虚拟IP地址	
优先级	100
通告间隔(秒)	1
抢占模式	☐
目的地址(IPv4)	8.8.8.8
备选目的地址(IPv4)	114.114.114.114
Ping间隔	300 s
Ping重试间隔	5 s
Ping超时	3 s
最大重试次数	3
<button>保存</button>	

图 3.2.8 VRRP-1

VRRP 设置		
项目	描述	默认值
启用	启用/禁用 VRRP 功能。	禁用
接口	设置虚拟 CPE 的接口。	None
虚拟 CPEID	用户自定义虚拟 CPEID，合法值：1-255。	None
虚拟 IP 地址	设置虚拟 CPEIP 地址。	None
优先级	VRRP 优先级的取值范围为 1-254（数值越大表明优先级越高），优先级越高则越有可能成为网关 CPE。	100
通告间隔（秒）	虚拟 IP 组内 CPE 之间的心跳报文发送时间间隔，合法值：1-255。	1
抢占模式	抢占模式下 CPE 一旦发现自己的优先级比当前的网关 CPE 的优先级高，就会对外发送 VRRP 通告报文。导致重新选举网关 CPE，并最终取代原有的网关 CPE。相应的，原来的网关 CPE 将会变成备用 CPE。	禁用
Track 标识	跟踪探测，选择定义过的 Track 标识或为空	None

表 3.2.8 VRRP-2

3.2.9 DDNS

动态域名（DDNS）是一种自动更新域名系统中名称服务器的方法，允许用户将动态 IP 地址别名为静态域名。

动态域名作为客户端工具，需要与动态域名服务器协调。在开始配置之前，用户应在适当的域名提供商的网站上注册并申请域名。

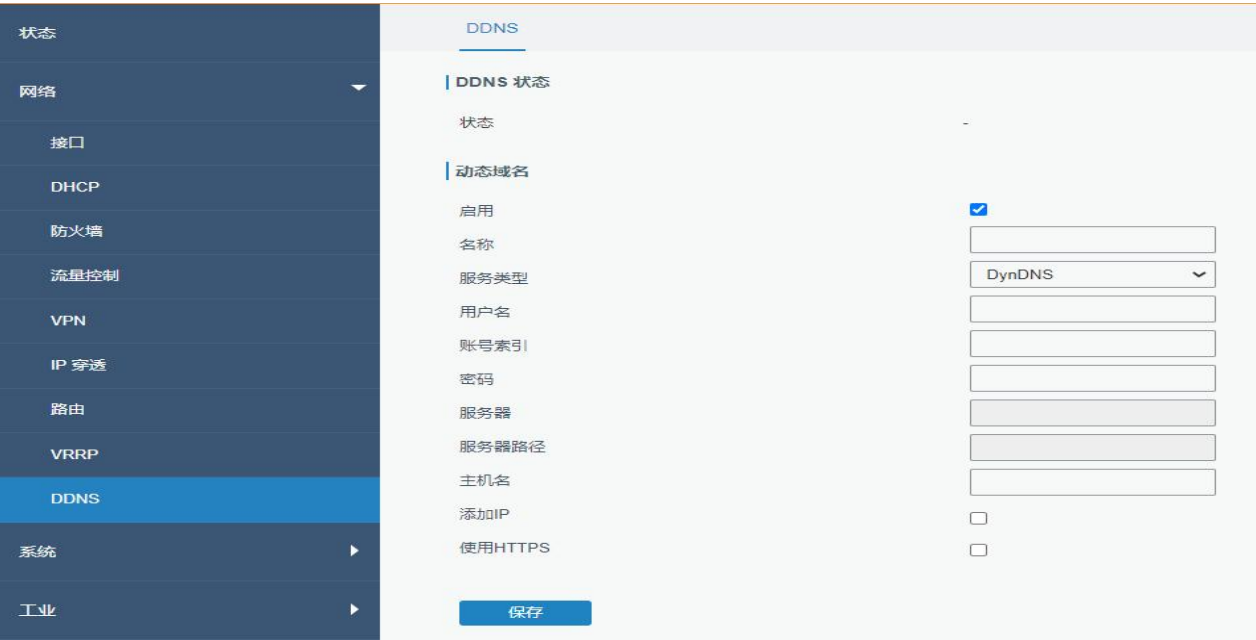


图 3.2.9 DDNS-1

动态域名	
项目	描述
启用	勾选后启用 DDNS。
名称	用户自定义 DDNS 的名称。
服务类型	选择提供动态服务的服务商。
用户名	输入申请注册动态域名的用户名。
账号索引	输入自定义 DDNS 服务器的账号索引。
密码	输入申请注册动态域名的密码。
服务器	输入自定义的 DDNS 服务器名称。
服务器路径	默认情况下主机名会添加到服务器路径。
主机名	输入申请的主机名。
添加 IP	添加当前 IP 到 DDNS 服务器更新路径。

表 3.2.9 DDNS-1

3.3 系统

本节介绍如何配置常规设置，如管理帐户、访问服务、系统时间、通用用户管理、SNMP、AAA、事件警报等。

3.3.1 常规

3.3.1.1 常规

常规设置中有系统信息和 HTTPS 证书。



图 3.3.1.1 常规-1

常规		
项目	描述	默认值
系统		
主机名	用户可自定义 CPE 主机名称，以字母开头，只允许字母、数字、“-”或“_”。	CPE
网页登陆超时时间 (秒)	超时后需要重新登陆网页。合法值：100-3600。	1800
明文密码加密	启用后设备在 WEB 上配置的所有带密码的参数都会以加密的方式显示，提高密码的安全性。	启用
HTTPS 证书		
证书	单击“浏览”从电脑中选择证书文件，再单击“导入”从电脑中导入文件到 CPE；单击“导出”从 CPE 导出文件到电脑；单击“删除”从 CPE 删除文件	--
密钥	单击“浏览”从电脑中选择密钥文件，再单击“导入”从电脑中导入文件到 CPE；单击“导出”从 CPE 导出文件到电脑；单击“删除”从 CPE 删除文件	--

表 3.3.1.1 常规-1

3.3.1.2 系统时间

本节介绍如何设置系统时间，包括时区和时间同步类型。

注意：为确保 CPE 以正确的时间运行，建议您在配置 CPE 时设置系统时间。

状态	常规	系统时间	邮箱	存储
网络	系统时间设置			
系统	当前时间 2021-01-21 02:29:30 星期四			
常规	时区 0 United Kingdom (London)			
电话 & 短信	同步类型 从浏览器同步			
用户管理	浏览器时间 2021-01-21 10:29:31 星期四			
SNMP	保存			

图 3.3.1.2 系统时间-1

状态	常规	系统时间	邮箱	存储
网络	系统时间设置			
系统	当前时间 2021-01-21 02:29:39 星期四			
常规	时区 0 United Kingdom (London)			
电话 & 短信	同步类型 手动设置			
用户管理	日期 2021-01-21			
SNMP	时间 10 29 40			
	保存			

图 3.3.1.2 系统时间-2

图 3.3.1.2 系统时间-3

系统时间	
项目	描述
当前时间	显示 CPE 的当前时间。
色器	选择本地时间，如 “8 China(beijing)” 。
同步类型	选择时间同步类型。
从浏览器同步	从浏览器同步时间。
浏览器时间	显示浏览器时间。
手动设置	手动设置系统时间为任意期望值。
从 NTP 服务器同步	从 NTP 服务器同步时间来对网络内所有具有时钟的设备进行时钟同步。
从 NTP 服务器同步	
NTP 服务器地址	设置 NTP 服务器地址（域名/IP）
启用 NTP 服务器	启用/禁用 NTP 服务器功能，勾选后，网络中的 NTP 客户端即可与 CPE 在时间上实现同步。

表 3.3.1.2 系统时间-1

3.3.1.3 SMTP

SMTP 是简单邮件传输协议的缩写，是用于发送和接收电子邮件的 TCP / IP 协议。SMTP 功能支持将事件推送以电子邮件的方式发送到指定的收件人，本节介绍如何配置电子邮件设置。

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

设备管理

常规

系统时间

邮箱

存储

SMTP客户端设置

启用

邮箱地址

密码

SMTP服务器地址

端口号

加密方式

☒

STARTTLS

测试

图 3.3.1.3 SMTP-1

SMTP	
项目	描述
SMTP 客户端设置	
启用	启用/禁用 SMTP 客户端功能。
邮箱地址	输入发件人的邮件账号。
密码	输入发件人的邮箱密码。
SMTP 服务器地址	输入 SMTP 服务器域名。
端口号	输入 SMTP 服务器端口。合法值：1-65535。
加密方式	选择加密方式。可选项为：None、TLS/SSL、STARTTLS。其中默认选项为 STARTTLS。 选择 None：不加密。在端口 25 上登录服务器。 选择 STARTTLS：STARTTLS 是一种把已经存在的一条不安全的链接，用 SSL/TLS 的加密方法，把这条不安全的连接升级成安全的连接。在端口 587 上登录服务器。默认登录端口为 587。 TLS/SSL：SSL 和 TLS 都提供了加密 2 台计算机（如服务器和客

	户端) 之间通信的办法。TLS 是 SSL 的继任者, 所以除非提到具体协议的版本, TLS 和 SSL 这 2 个词是可以混用的, 在大多数情况下的意思相近。默认登录端口为 465。
--	--

表 3.3.1.3 SMTP-1

邮件设置中可设置事件的电子邮件警报。

1. 添加邮箱列表
2. 选择邮箱地址并添加到邮件群组
3. 进入“系统” - “事件” - “事件设置” - “邮件群组” 并选择需要的邮件群组。

邮箱列表

邮箱地址

描述

操作

✕

+

邮箱群组

组别ID

描述

列表

选中的邮箱地址

➤

➤

➤

➤

➤

保存

取消

图 3.3.1.3 SMTP-2

邮箱	
项目	描述
邮箱列表	
邮箱地址	输入邮箱地址。
描述	对邮箱添加描述。
邮箱群组	
组别 ID	设置邮箱群组的编号。合法值：1-100。
描述	对邮箱群组添加描述。
列表	显示已添加的邮箱地址。
选中的邮箱地址	显示已选中的邮箱地址。

表 3.3.1.3 SMTP-2

相关内容

[DI 设置](#)

[事件设置](#)

[事件应用案例](#)

3.3.1.4 存储

查看外部接入的 SSD 信息



图 3.3.1.4 存储-1

存储	
项目	描述
状态	显示 SSD 的状态，例如“可用”或“未插入”。
容量（总容量/可用容量）	SSD 的总容量。
格式化	格式化 SSD。

表 3.3.1.4 存储-1

3.3.2 电话&短信

3.3.2.1 电话

电话设置涉及呼叫/短信触发，短信控制和事件短信报警。

1. 添加电话本。
2. 选择电话号码并加入电话组。

3. 进入“网络” - “接口” - “蜂窝数据” - “连接模式” - “按需连接” - “电话触发” / “短信触发”或“系统” - “事件” - “事件设置” - “短信”，然后选择电话群组。

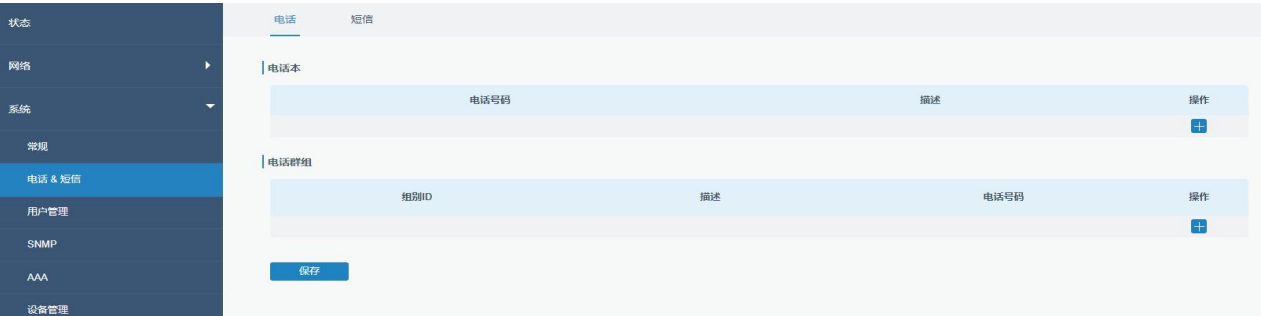


图 3.3.2.1 电话-1

电话	
项目	描述
电话本	
电话号码	输入电话号码。注意：部分国家要求采用国际格式填写电话号码才能正常收发短信，如“+8613859200000”。
描述	对电话号码添加描述。
电话组	
组别 ID	设置电话组编号。合法值：1-100。
描述	对电话组添加描述。
列表	显示已添加的电话本。
选中的电话号码	显示已选中的电话号码。

图表 3.3.2.1 电话-1

3.3.2.2 短信

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

设备管理

事件

工业

维护

APP

电话短信

常规设置

短信模式PDU

短信远程控制

保存

发送短信

接收方号码

内容

发送

短信接收记录

开始时间

结束时间

发送方号码

搜索

发送方号码

时间

内容

< > 10

Go to

GO

图 3.3.2.2 短信-1

SMS	
项目	描述
发送短信	
接收方号码	请输入接收短信的手机号。
内容	请输入短信内容。
短信接收/发送记录	
开始时间	请选择历史记录中要查询的开始时间。
结束时间	请选择历史记录中要查询的结束时间。
发送方号码	例如，输入 123456，点击搜索，则可以查看该号码发送的短信历史记录。
接收方号码	例如，输入 123456，点击搜索，则可以查看该号码发送的短信历史记录。

表 3.3.2.2 短信-1

相关内容

[按需连接](#)

3.3.3 用户管理

3.3.3.1 账户

更改管理员的登录用户名和密码。

注意：出于安全考虑强烈建议修改默认密码。

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

账户

用户管理

修改账户信息

用户名

admin

旧密码

新密码

再次输入新密码

保存

图 3.3.3.1 账户-1

账户	
项目	描述
用户名	输入新用户名。您可以使用 a-z、0-9、“_”、“-”、“\$”等字符。第一个字符不能是数字。
旧密码	输入旧密码。
新密码	输入新密码。
再次输入新密码	再一次输入新密码以确认。

表 3.3.3.1 账户-1

3.3.3.2 用户管理

本节介绍如何创建公共帐户。

通用用户权限包括只读和读写，创建或修改或删除普通用户账户，最大普通用户数为 5。

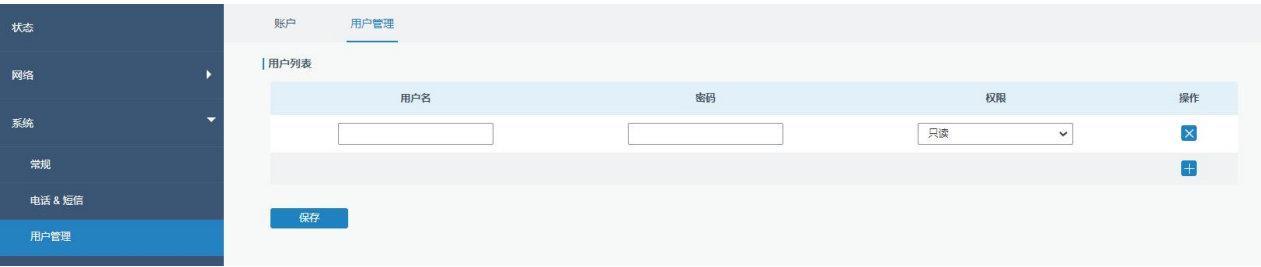


图 3.3.3.2 用户管理-1

用户管理	
项目	描述
用户名	输入新用户名。您可以使用 a-z、0-9、"_"、"- "、"\$" 等字符。第一个字符不能是数字。
密码	设置密码。
权限	从“只读”和“读写”中选择用户权限。 - 只读：用户只能查看此级别的 CPE 配置。 - 读写：用户可以在此级别查看和设置 CPE 的配置。

表 3.3.3.2 用户管理-1

3.3.4 SNMP

SNMP（简单网络管理协议）是一种互联网标准协议，用于收集和组织有关 IP 网络上受管设备的信息，以及修改该信息以更改设备行为。SNMP 广泛用于网络监控的网络管理，且用户可通过 SNMP 利用可自定义的格式查看受管系统中的数据。该系统依从管理信息库（MIB）框架组织、描述系统的状态与配置。网络管理员可以利用 SNMP 远程管理和配置系统中的下属设备，并对这些设备进行实时监控，也可以通过管理应用程序来远程查询变量内容。

SNMP 关于网络、NMS 和 SNMP 管理程序的相关配置应在 Manager 中完成。

为了实现 NMS 的查询，下面列出了配置步骤：

1. 启用 SNMP 设置。
2. 下载 MIB 文件并载入 NMS。
3. 配置 MIB 视图。
4. 配置 VCAM。

相关配置案例

[SNMP 应用案例](#)

3.3.4.1 SNMP

UF51 支持 SNMPv1，SNMPv2c 和 SNMPv3 版本。SNMPv1 和 SNMPv2c 使用社区名称身份验证，SNMPv3 使用用户名和密码进行身份验证加密。

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

SNMPMIB视图VACMTrapMIB

SNMP设置

启用

端口

版本

本地信息

联系信息

☐

161

SNMPv2

保存

图 3.3.4.1 SNMP-1

SNMP 设置	
项目	描述
启用	启用/禁用 SNMP 功能。
端口	设置 SNMP 监听端口，合法值：1-65535，默认为 161。
版本	选择 SNMP 版本，支持 SNMP v1/v2c/v3。
本地信息	填写本地位置信息。
联系信息	填写联系信息。

表 3.3.4.1 SNMP-1

3.3.4.2 MIB 视图

本节介绍如何为对象配置 MIB 视图。

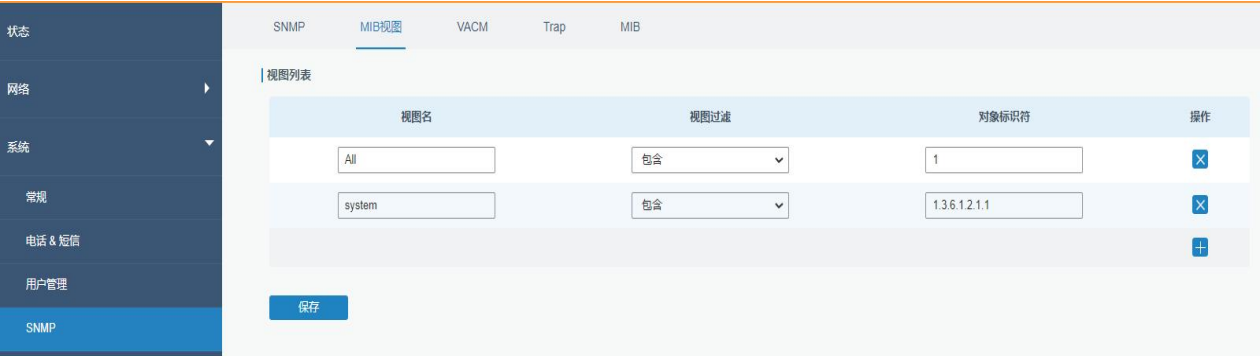


图 3.3.4.2 MIB 视图-1

MIB 视图	
项目	描述
视图名	设置 MIB 视图名称。
视图过滤	用户可选择“包含”和“过滤”。
对象标识符	输入对象标识符。
包含	可查询指定 MIB 节点以内的所有节点。
排除	可查询除指定 MIB 节点以外的所有节点。

表 3.3.4.2 MIB 视图-1

3.3.4.3 VACM

本节介绍如何配置 VACM 参数。

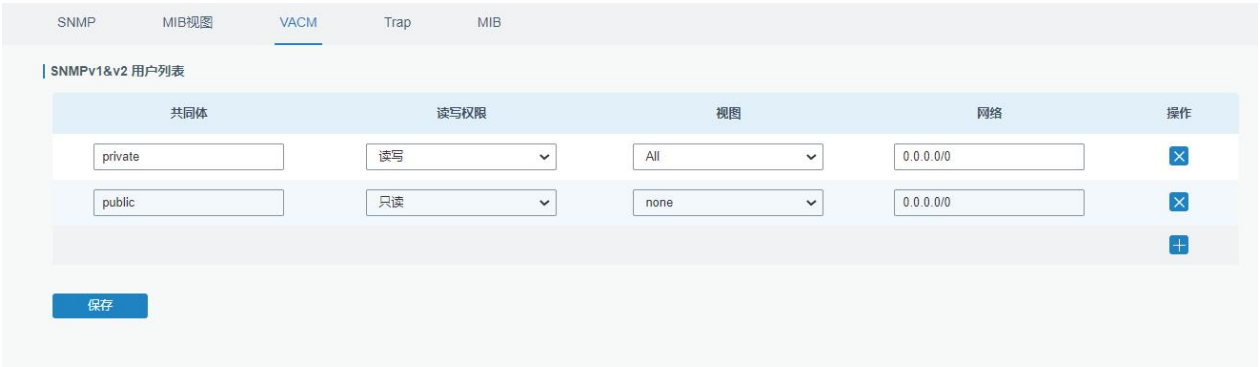


图 3.3.4.3 VACM-1

VACM	
项目	描述
SNMP v1 & v2 用户组	
共同体	设置共同体名称。

读写权限	用户可选择“只读”或“读写”。
视图	从 MIB 视图列表中选择一个要设置权限的 MIB 视图。
网络	访问 MIB 视图的外部网络的 IP 地址及位数。
读写	指定 MIB 节点的用户权限为读写。
只读	指定 MIB 节点的用户权限为只读。
SNMP v3 用户组	
组名	设置用户组组名。
安全级别	选择该组的安全级别，用户可选“无鉴别/无加密”、“鉴别/无加密”、“鉴别/加密”。
只读视图	从 MIB 视图列表中选择一个要设置为只读权限的 MIB 视图。
读写视图	从 MIB 视图列表中选择一个要设置为读写权限的 MIB 视图。
通知视图	从 MIB 视图列表中选择一个要设置为通知视图的名称。

表 3.3.4.3 VACM-1

3.3.4.4 Trap

本节介绍如何通过 SNMP trap 启动网络监视。

SNMPMIB视图VACMTrapMIB

SNMP Trap

启用

☐

SNMP版本

SNMPv2

服务器地址

端口

名字

private

保存

图 3.3.4.4 Trap-1

SNMP Trap	
项目	描述
启用	启用/禁用 SNMP Trap 功能。
SNMP 版本	选择 SNMP 版本，支持 SNMP v1/v2c/v3。
服务器地址	填写管理站（NMS）的 IP 地址或域名。
端口	填写端口号。合法值：1-65535，默认端口为 162。
名字	版本 v1 或 v2c 时填写相应的团体名，版本为 v3 时填写相应的用户名。

权限模式	选择该组的安全级别，用户可选“无鉴别/无加密”、“鉴别/无加密”、“鉴别/加密”。
------	---

表 3.3.4.4 Trap-1

3.3.4.5 MIB

本节介绍如何下载 MIB 文件。最后一个 MIB 文件“URSA-CPE-MIB.txt”用于 UF51。

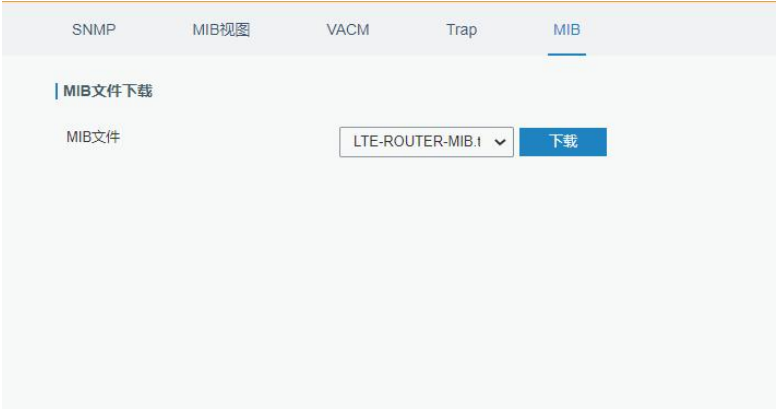


图 3.3.4.5 MIB-1

MIB	
项目	描述
MIB 文件	选择需要的 MIB 文件。
下载	点击“下载”以下载选中的 MIB 文件到电脑上。

表 3.3.4.5 MIB-1

3.3.5 AAA

AAA 访问控制是用来控制允许何种人访问服务器，以及一旦他们能够访问该服务器，允许他们使用何种服务的方法。AAA 为以下服务提供模块化方法：

- 身份验证：验证用户是否有资格访问网络。
- 授权：授权用户使用的相关服务。
- 计费：记录网络资源的利用率。

3.3.5.1 Radius

使用 UDP 进行传输时,Radius 通常应用于具有更高安全性和远程用户访问权限的各种网络环境中。

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

Radius

Tacacs+

LDAP

认证

Radius设置

启用

服务器IP地址

端口

认证密钥

保存

图 3.3.5.1 Radius-1

Radius	
项目	描述
启用	启用/禁用 Radius。
服务器 IP 地址	填写 Radius 服务器的地址（域名/IP）。
端口	填写 Radius 服务器端口号。合法值：1-65535。
认证密钥	与 Radius 服务器建立连接时候需要验证的认证密钥。只有认证密钥一致才能与 Radius 服务器建立连接。

表 3.3.5.1 Radius-1

3.3.5.2 TACACS+

TACACS +使用 TCP 进行传输，主要用于接入用户和终端用户的认证，授权和计费，采用 PPP 和 VPDN。

状态

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

Radius

Tacacs+

LDAP

认证

Tacacs+设置

启用

服务器IP地址

端口

认证密钥

保存

图 3.3.5.2 TACACS+-1

TACACS+	
项目	描述
启用	启用/禁用 TACACS+。
服务器 IP 地址	填写 TACACS+服务器地址（域名/IP）。
端口	填写 TACACS+服务器端口号。合法值：1-65535。
认证密钥	与 TACACS+ 服务器建立连接时候需要验证的认证密钥。只有认证密钥一致才能与 TACACS+ 服务器建立连接

表 3.3.5.2 TACACS+-1

3.3.5.3 LDAP

LDAP 的一个常见用法是提供存储用户名和密码的中心位置，这允许许多不同的应用程序和服务连接 LDAP 服务器以验证用户。

LDAP 是一个基于 X.500 标准但更简单的标准。由于这种关系，LDAP 有时也称为 X.500-lite。

The screenshot displays the 'LDAP设置' (LDAP Settings) configuration page. On the left is a dark sidebar menu with items: 状态 (Status), 网络 (Network), 系统 (System), 常规 (General), 电话 & 短信 (Phone & SMS), 用户管理 (User Management), SNMP, and AAA. The main content area has tabs for Radius, Tacacs+, LDAP (selected), and 认证 (Authentication). Under the 'LDAP设置' heading, there are several configuration fields: '启用' (Enable) with a checkbox, '服务器IP地址' (Server IP Address) with a text input, '端口' (Port) with a text input containing '389', '基准DN' (Base DN) with a text input, '安全' (Security) with a dropdown menu showing 'None', '用户名' (Username) with a text input, and '密码' (Password) with a text input. A blue '保存' (Save) button is located at the bottom of the configuration area.

图 3.3.5.3 LDAP-1

LDAP	
项目	描述
启用	启用/禁用 LDAP。
服务器 IP 地址	填写 LDAP 服务器地址（域名/IP）。

端口	填写 LDAP 服务器的服务端口号，合法值：1-65535。
基准 DN	LDAP 目录树的最顶部。
安全	选择加密方式，共 3 种选择：“None”、“StartTLS”、“SSL”。
用户名	访问服务器的用户名。
密码	访问服务器的密码。

表 3.3.5.3 LDAP-1

3.3.5.4 认证

AAA 支持以下几种认证方式：

- 不认证 (None)：不使用认证，一般不推荐。
- 本地认证 (Local)：使用本地用户名数据库进行认证
 - 优点：快速、成本低。
 - 缺点：存储总容量受硬件限制。
- 远端认证 (Remote)：用户信息存储于认证服务器上，Radius、TACACS+、LDAP 都支持远端认证。

当同时配置 radius、TACACS+、本地认证的情况下，优先级为 1 > 2 > 3。

服务	1	2	3
Console	None	None	None
Web	None	None	None
Telnet	None	None	None
SSH	None	None	None

图 3.3.5.4 认证-1

认证	
项目	描述
Console	选择 Console 访问的认证方式。

Web	选择 Web 访问的认证方式。
Telnet	选择 Telnet 访问的认证方式。
SSH	选择 SSH 访问的认证方式。

表 3.3.5.4 认证-1

3.3.6 设备管理

3.3.6.1 设备管理

星纵物联设备管理平台连接配置，用于远程管理 CPE。



图 3.3.6.1 设备管理-1

设备管理	
项目	描述
状态	显示 CPE 和设备管理平台的连接状态。
断开连接	点击该按钮使设备和设备管理平台的连接断开。
服务器地址	设备管理服务器的地址（IP 或域名）。
激活方式	选择设备与云管理平台的连接方式,可选“通过授权码”和“通过 ID”。

授权码	填写由设备管理平台生成的授权码。
ID	填写已注册的云管理账户（Email）和密码。
密码	

表 3.3.6.1 设备管理-1

3.3.6.2 Milesight VPN

作为 Openvpn 客户端连接到 Milesight VPN，通过 VPN 实现对终端设备的远程访问。

图 3.3.6.2 Milesight VPN-1

Milesight VPN	
项目	描述
Milesight VPN 设置	
服务器	输入 Milesight VPN 的 IP 地址或者域名。
端口	输入 HTTPS 端口号
授权码	输入由 Milesight VPN 产生的授权码。

设备名称	输入设备名称
星纵物联 VPN 状态	
状态	显示 CPE 和 Milesight VPN 的连接状态。
本地 IP	显示 CPE 的虚拟 IP 地址。
远程 IP	显示 Milesight VPN 的虚拟 IP 地址。
连接时长	显示 CPE 和 Milesight VPN 的连接时长。

表 3.3.6.2 Milesight VPN-1

3.3.7 事件

事件功能能够在发生某些系统事件时通过电子邮件和短信形式发送警报。

3.3.7.1 事件

查看警报信息。

状态

网络

系统

常规

用户管理

SNMP

AAA

设备管理

事件

工业

维护

事件

事件设置

标记为已读

删除

全部标为已读

删除全部

	状态	类型	时间	消息
☐	未读	蜂窝网络上线	2018-01-17 10:30:00	蜂窝开启
☐	未读	蜂窝网络掉线	2018-01-17 10:29:51	蜂窝关闭
☐	已读	蜂窝网络上线	2018-01-16 15:08:37	蜂窝开启
☐	已读	蜂窝网络掉线	2018-01-16 15:07:30	蜂窝关闭
☐	已读	蜂窝网络上线	2018-01-16 05:33:03	蜂窝开启
☐	已读	蜂窝网络掉线	2018-01-16 05:31:50	蜂窝关闭
☐	已读	蜂窝网络上线	2018-01-15 20:01:43	蜂窝开启
☐	已读	蜂窝网络上线	2018-01-15 20:00:20	蜂窝开启
☐	已读	蜂窝网络掉线	2018-01-15 20:00:20	蜂窝关闭
☐	已读	蜂窝网络上线	2018-01-15 19:42:40	蜂窝开启

图 3.3.7.1 事件-1

事件	
项目	描述
标记为已读	把选中的事件告警标记为已读。
删除	删除选中的事件告警。

全部标为已读	把全部事件告警标记为已读。
删除全部	删除全部事件告警。
状态	显示需告警信息的阅读状态。
类型	显示需告警的事件类型。
时间	显示告警的时间。
消息	显示告警的内容。
未读	该事件告警为未读状态。
已读	该事件为已读状态。

表 3.3.7.1 事件-1

3.3.7.2 事件设置

设置记录的事件以及是否要在发生任何更改时接收电子邮件和 SMS 通知。

事件	记录 ☒	邮件 ☐ 邮件群组	短信 ☐ 电话群组	SNMP ☐
系统启动	☒	☐	☐	☐
系统重启	☒	☐	☐	☐
系统时间更新	☒	☐	☐	☐
VPN上线	☒	☐	☐	☐
VPN掉线	☒	☐	☐	☐
WAN 连接成功	☒	☐	☐	☐
WAN 连接失败	☒	☐	☐	☐
链路切换	☒	☐	☐	☐
信号质量差	☒	☐	☐	☐
蜂窝网络上线	☒	☐	☐	☐

图 3.3.7.2 事件设置-1

事件设置	
项目	描述
启用	勾选启用事件告警。
电话群组	选择接收短信告警的电话群组。
邮件群组	选择接收邮件告警的邮件群组。

记录	勾选后将在“事件”页面记录事件发生的时间和内容。
邮件	勾选后将事件告警以邮件的形式发送给指定的收件人。
邮件设置	点击后，将跳转至“SMTP”设置页面，以使用户设置发件人及收件人信息。
短信	勾选后将事件告警以短信的形式发送给指定的电话号码。
短信测试	点击后，将跳转至“系统”>“常规”>“电话”设置页面，以使用户设置电话组。
VPN 上线	VPN 已连接上。
VPN 掉线	VPN 断开连接。
WAN 上线	以太网线已连接广域网接口。
WAN 掉线	以太网线已断开广域网接口。
链路切换	CPE 用来上网的接口发生切换。
信号质量差	蜂窝的信号强度低。
蜂窝网络上线	蜂窝网络已拨号成功。
蜂窝网络掉线	蜂窝网络掉线。
蜂窝统计数据清除	主 SIM 卡使用的流量记录清零。
蜂窝网流量临近阈值	主 SIM 卡使用流量即将超过阈值。
蜂窝网流量超出阈值	主 SIM 卡使用流量超出阈值。
WLAN 成功启用（作为接入点）	WLAN 作为接入点已成功启用。
WLAN 停止运行（作为接入点）	WLAN 作为接入点已停止运行。
WLAN 成功启用（作为客户端）	WLAN 作为客户端已成功启用。
WLAN 停止运行（作为客户端）	WLAN 作为客户端已停止运行。

表 3.3.7.2 事件设置-1

相关内容

[邮件设置](#)[事件应用案例](#)

3.4 工业接口

UF51 能够通过工业接口与终端连接，实现终端与远程数据中心之间的无线通信。

CPE 的工业接口有两种类型：串行端口（RS232 和 RS485）和 I/O（数字输入和数字输出）。

RS232 采用全双工通信，它通常用于 20 米范围内的通信。

RS485 采用半双工通信，实现距离可达 120m 的串行通信数据传输。

I/O 接口的数字输入是逻辑变量或开关变量，只有两个值 0 和 1。“0”表示低电平，“1”表示高电平。

3.4.1 I/O

3.4.1.1 数字输入

本节介绍如何配置数字输入，以及数字输入触发时对应的动作。

状态

网络

系统

工业

I/O

串口

Modbus Slave

数字输入

数字输出

数字输入设置

启用

☐

模式

高电平

持续时间(毫秒)

100

动作

☐ 短信

☐ 邮件

☐ DO

☐ 触发蜂窝网络连接

保存

图 3.4.1.1 数字输入-1

数字输入	
项目	描述
启用	启用/禁用数字输入。
模式	用户可选择“高电平”、“低电平”、“计数器”。 高电平：数字输入状态为高电平。 低电平：数字输入状态为低电平。
持续时间（毫秒）	定义维持高/低电平状态的时间。合法值：1-10000。
触发条件	仅在当数字输入在计数器模式时下可用。用户可选择“低->高”，和“高->低”。
低->高	每当数字输入的状态由低电平变为高电平时，计数器值增加 1。

高->低	每当数字输入的状态由高电平变为低电平时，计数器值增加 1。
计数器	在计数器模式下，输入 1-100。当计数器数值达到设定的触发值时，系统就会作出相应的动作，并且计数器将重新计数。
动作	选择当数字输入口满足预设模式的触发条件或时间后作出的动作。
短信	勾选启用 DI 触发短信告警。
电话组	设置接收 SMS 告警信息的电话号码。
短信内容	设置 SMS 告警的内容。
邮件	勾选启用 DI 触发邮件告警。
邮箱组	设置接收邮件告警信息的邮箱。
邮件内容	设置邮件告警的内容。
数字输出	勾选启用 DI 触发控制 DO 输出状态。
蜂窝数据上线	勾选启用触发蜂窝网络连接。

表 3.4.1.1 数字输入-1

相关内容

- 数字输出设置
- 邮件设置
- 按需连接

3.4.1.2 数字输出

本节介绍如何配置数字输出。



图 3.4.1.2 数字输出-1

数字输出	
项目	描述

启用	启用/禁用数字输出启用 or 禁用 DO.
模式	用户可选择“高电平”、“低电平”、“脉冲”和“自定义”。 高电平：数字输出为高电平。 低电平：数字输出为低电平。 脉冲：数字输出为脉冲。
持续时间 (*10 毫秒)	定义维持高/低电平状态的持续时间。合法值：1-10000。
初始状态	设置自定义模式启用时 DO 的初始状态,同时也是 CPE 重启后 DO 的状态。
高电平持续时间 (*10 毫秒)	定义维持脉冲高电平的时间。合法值：1-10000。
低电平持续时间 (*10 毫秒)	定义维持脉冲低电平的时间。合法值：1-10000。
脉冲个数	定义形成完整脉冲的个数。合法值：1-100。
电话组	请选择有配置 I/O 权限的电话组，用户可点击号码组跳转到相关页面设置号码。

表 3.4.1.2 数字输出-1

相关内容

[数字输入设置](#)

3.4.2 串口

本节介绍如何根据与 CPE 相连的终端设备的串口参数设置 CPE 串口的参数，实现 CPE 与终端设备的正常通信；如何配置工作模式实现与远程数据中心的通信，并实现串口与远端数据中心的双向通信。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus Master

串口1

串口2

串口设置

启用

串口类型

波特率

数据位

停止位

校验位

软件流控

串口模式

DTU协议

☒

RS232

9600

8bits

1bits

None

☐

DTU模式

透明传输

图 3.4.2.1 串口-1

串口设置		
项目	模式	默认值
启用	启用/禁用串口功能。	禁用
串口类型	串口 1 类型为 RS232；串口 2 类型为 RS485。	--
波特率	选择串口波特率，它表示每秒钟传送的符号的个数。与已连接的终端设备的波特率相同。范围：300-230400。	9600
数据位	选择串口数据位。与已连接的终端设备的串口数据位相同。用户可选择"7"和"8"。	8
停止位	用于表示单个包的最后一位。与已连接的终端设备的停止位相同。用户可选择"1"和"2"。	1
校验位	在串口通信中的检错方式，支持“None”，“Odd”，“Even”。与已连接的终端设备的校验位相同。	None
软件流控	流控可以使数据接收设备在不能接收数据时通知数据发送设备，使其停止发送启用。	禁用
串口模式	选择串口的工作模式，可选“DTU 模式”、“Modbus Master”、“Modbus Slave”。	禁用
DTU 模式	选择该模式，串口可以和远端服务器或客户端进行通信。	--
GPS	选择该模式，同时在“工业 > GPS > GPS 串口转发”页面选择相应的串口类型后可以将 GPS 信息转发到该串口。	--
Modbus Master	选择 Modbus Master 模式，在“工业 > Modbus Master”中配置基本参数和频道。	--
Modbus Slave	选择 Modbus Slave 模式，在“工业 > Modbus Slave”中配置基本参数和频道。	--

表 3.4.2.1 串口-1

串口模式	DTU模式
DTU协议	透明传输
协议	TCP
保活间隔	75 秒
保活重试次数	9
串口分帧长度	1024 字节
串口分帧间隔	100 毫秒
重连间隔	10 秒
指定协议	☐
注册包内容	
目的IP地址	

服务器地址	服务器端口	状态	操作
			+

图 3.4.2.2 串口-2

DTU 模式		
项目	描述	默认值
DTU 协议	可选“透明传输”、“Modbus”、“UDP 服务器”、“TCP 服务器”。 - 透明传输：路由用作 TCP 客户端/UDP 并透明地传输数据。 - TCP 服务器：路由用作 TCP 服务端并透明地传输数据。 - UDP 服务器：路由用作 UDP 服务端并透明地传输数据。 - Modbus：路由用作带有 Modbus 网关功能的 TCP 服务端，从而实现 Modbus RTU 和 Modbus TCP 之间的通信。	--
TCP/UDP 服务器		
监听端口	设置 CPE 的监听端口。合法值：1-65535。	502
保活间隔（秒）	TCP 连接建立后，客户端会照 TCP 协议定时发送心跳包以保活。合法值：1-3600。	75
保活重试次数	TCP 心跳超时后，CPE 重发送心跳包，发送次数超过预设的重试次数后 TCP 连接将进行重连。合法值：1-16。	9
串口分帧长度（字节）	设置串口分帧长度。串口长度达到预设分帧长度后发送数据包。合法值：1-1024。	1024
串口分帧间隔（毫秒）	CPE 将存储在缓冲区中的实际串行数据发送到公共网络的时间间隔。合法值：10-65535。 注意：当实际串行数据大小达到预设数据包大小时，即使仍在串行分帧间隔内，数据也将被发送到公共网络。	100

表 3.4.2.2 串口-2

项目	描述	默认值
透明传输		
协议	选择 TCP 或 UDP 协议。	TCP
保活间隔（秒）	TCP 连接建立后，客户端会照 TCP 协议定时发送心跳包以保活。合法值：1-3600。	75
保活重试次数	TCP 心跳超时后，CPE 重发送心跳包，发送次数超过预设的重试次数后 TCP 连接将进行重连。合法值：1-16。	9
串口分帧长度（字节）	设置串口分帧长度。串口长度达到预设分帧长度后发送数据包。合法值：1-1024。	1024
串口分帧间隔（毫秒）	CPE 将存储在缓冲区中的实际串行数据发送到公共网络的时间间隔。合法值：10-65535。 注意：当实际串行数据大小达到预设数据包大小时，即使仍在串行分帧间隔内，数据也将被发送到公共网络。	100
重连间隔（秒）	连接断开后 CPE 将在此间隔时间后再次尝试连接，合法值：10-60。	10
指定协议	通过指定协议，设备可以与 TCP2COM 软件对接。	--
心跳间隔（秒）	启用指定协议后，设备向服务器定期发送心跳报文的时间。合法值：1-3600。	30
ID	用户自定义设备标识符作为设备的唯一标识。不允许空格，最大长度为 63 个字符。	--
注册包内容	用户自定义设备登录到服务器的注册包内容。	Null
服务器地址	填写 TCP 或 UDP 服务器地址（IP/域名）。	Null
服务器端口	填写 TCP 或 UDP 服务器端口。合法值：1-65535。	Null
状态	显示设备和服务器的连接状态。	--
Modbus		
本地端口号	设置 CPE 监听端口。合法值：1-65535。	502

表 3.4.2.2 串口-3

相关配置案例

[DTU 应用案例](#)

3.4.3 Modbus TCP

本节介绍如何通过 TCP 上的 Modbus TCP、Modbus RTU 和 Modbus RTU over TCP 实现 I/O 状态。

3.4.3.1 Modbus TCP

定义数字输入和数字输出端口的地址，以便轮询数字输入口的状态并通过 Modbus TCP 协议控制数字输出的状态。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus TCP

Modbus RTU

Modbus RTU Over TCP

Modbus TCP

启用

端口

数字输入地址

数字输出地址

☒

保存

图 3.4.3.1 Modbus TCP-1

Modbus TCP		
项目	描述	默认值
启用	启用/禁用 Modbus TCP。	禁用
端口	设置 CPE 监听的端口。合法值：1-65535。	502
数字输入地址	用户自定义数字输入地址，数字输入地址。合法值：0-255。	0
数字输出地址	用户自定义数字输出地址，数字输出地址。合法值：0-255。	0

表 3.4.3.1 Modbus TCP-1

3.4.3.2 Modbus RTU

定义数字输入和数字输出端口的地址，以便轮询数字输入口的状态并通过 Modbus RTU 协议控制数字输出的状态。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus TCP

Modbus RTU

Modbus R

Modbus RTU

启用

串口模式

Slave ID

数字输入地址

数字输出地址

保存

图 3.4.3.2 Modbus RTU-1

Modbus RTU		
项目	描述	默认值
启用	启用/禁用 Modbus RTU。	禁用
串口	选择对应的串口。	serial
Slave ID	CPE 作为从站利用从站 ID 区分同一链路上的不同设备，用户自定义从站 ID，合法值：1-247。	1
数字输入地址	用户自定义数字输入地址，数字输入地址。合法值：0-255。	0
数字输出地址	用户自定义数字输出地址，数字输出地址。合法值：0-255。	0

表 3.4.3.2 Modbus RTU-1

3.4.3.3 Modbus RTU Over TCP

定义数字输入和数字输出端口的地址，以便轮询数字输入口的状态并通过 Modbus RTU over TCP 协议控制数字输出的状态。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus Master

维护

Modbus TCP

Modbus RTU

Modbus RTU Over TCP

Modbus RTU Over TCP

启用

Slave ID

设备名称

重连时间

数字输入地址

数字输出地址

服务器列表

IP地址

端口

状态

操作

保存

图 3.4.3.3 Modbus RTU Over TCP-1

Modbus RTU Over TCP		
项目	描述	默认值
启用	启用/禁用 Modbus RTU over TCP 功能	禁用
Slave ID	CPE 作为从站利用从站 ID 区分同一链路上的不同设备，用户自定义从站 ID，合法值：1-247。	1
设备 ID	设置设备 ID。服务器会获取此项标识给服务器，便于服务器管理多台设备。	--
重连间隔	当设备与服务器连接失败或连接中断时，两次尝试连接的间隔时间。	10
数字输入地址	用户自定义数字输入地址，数字输入地址。合法值：0-255。	0
数字输出地址	用户自定义数字输出地址，数字输出地址。合法值：0-255。	0
服务器列表		
IP 地址	输入要连接的服务器 IP 地址。	
端口	输入要连接的服务器端口号。合法值：0-65535。	
状态	显示设备和服务器的连接状态。	

表 3.4.3.3 Modbus RTU Over TCP-1

3.4.4 Modbus Master

UF51 设置为 Modbus Master 来轮询远程 Modbus Slave 并设置阈值发送报警。

3.4.4.1 Modbus Master

配置 Modbus Master 的参数。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus Master

Modbus Master

通道

Modbus Master设置

启用

☒

读取间隔

秒

最大重试次数

最大响应时间

毫秒

间隔时间命令

毫秒

通道

▼

保存&应用

图 3.4.4.1 Modbus Master-1

Modbus Master 设置		
项目	描述	默认值
启用	启用/禁用 Modbus master 功能。	--
读取间隔 (秒)	设置执行远程通道读操作的周期时间间隔。当一个周期结束时,设备会等待一段时间,才重新开始新的读操作周期。当读取间隔设置为 0 时,表示读取全部指令后设备将立即重新开始新的读操作周期。合法值: 0-604800。	0
最大重试次数	读取失败时,最大重试次数。合法值: 0-5。	3
最大响应时间 (毫秒)	设置设备等待执行一个读指令后的最大响应时间。如果超过最大响应时间后,设备都没有获取到指令的响应,就认为此指令读超时。合法值: 10-1000。	500
间隔时间命	每个指令之间的执行间隔。合法值: 10-1000。	50

令（毫秒）		
通道	选择一个可读取的远程通道。	--

表 3.4.4.1 Modbus Master-1

3.4.4.2 通道设置

添加通道并配置阈值告警，以便将 CPE 连接到远程 Modbus 从站以轮询此页面上的地址。

通道设置

通道设置

名称	Slave ID	地址	数目	指令类型	链路类型	IP地址	端口	有符号	小数位	操作
tunnel1	1	0	10	保持寄存器 ▾	TCP ▾	192.168.23.4	65535	☐	1	
tunnel2	2	0	10	保持寄存器 ▾	TCP ▾	192.168.23.4	65534	☐	0	

图 3.4.4.2 通道设置-1

通道设置	
项目	描述
名称	用于标识远程通道,该字段不能为空。
Slave ID	设置 Modbus 从地址。
地址	执行读取指令时要读取的起始地址。
数目	读取指令的数目。
指令类型	读指令，可以选择“线圈”、“离散”、“保持寄存器（INT16）”、“输入寄存器（INT16）”、“保持寄存器（INT32）”、“保持寄存器（Float）”。
链路类型	选择 TCP。
IP 地址	远端 Modbus 设备 IP 地址。
端口	远端 Modbus 设备端口。
有符号	用于标识此信道值是有符号。
小数位	用于指示小数点在读取到的远程通道的值的位置。例如：读取到此远程通道的值为 1234，且小数位等于 2，那么实际的值为 12.34。

表 3.4.4.2 通道设置-1

告警设置			
名称	条件	告警方式	操作
tunnel1	> 10	邮箱	 
tunnel2	(5,6)	邮箱	 
			

图 3.4.4.2 通道设置-2

告警设置	
项目	描述
名称	用于标识远程通道，与指令名称一致。
条件	触发告警的条件。
最小阈值	设置触发告警的最小值。当实际接收值小于该设定值时，触发告警。
最大阈值	设置触发告警的最大值。当实际接收值大于该设定值时，触发告警。
告警方式	选择告警方式，如短信，邮件。
短信	通过发送短信到指定号码告警。
电话群组	选择接收告警的电话组。
邮箱群组	选择接受告警的邮箱群组。
正常告警内容	实际接收值由原来的超过设定的阈值重新恢复到正常值时，CPE 将自动消除异常告警，并通过 SMS 的形式，将设定的正常告警内容发送到指定电话群组。
异常告警内容	实际接收值超过设定的阈值时，CPE 将自动触发告警，并通过 SMS 的形式，将设定的异常告警内容发送到指定电话群组。
连续警告	开启此功能后，相同的告警会不断地上报。即，发生多少次告警，CPE 就会上报多少次。若不开启此功能，多次相同的告警只会上报一次。

表 3.4.4.2 通道设置-2

TCP转发			
名称	IP	端口	操作
			

图 3.4.4.2 通道设置-3

TCP 转发	
项目	描述
名称	Modbus Master 通道名称。
IP 地址	要转发到的服务器的 IP 地址。
端口	远端服务器接收数据的端口。

表 3.4.4.2 通道设置-3

3.4.5 GPS

本节详细介绍 GPS 设置，包括 GPS IP 转发和 GPS 串行转发。

3.4.5.1 GPS

启用 GPS 功能

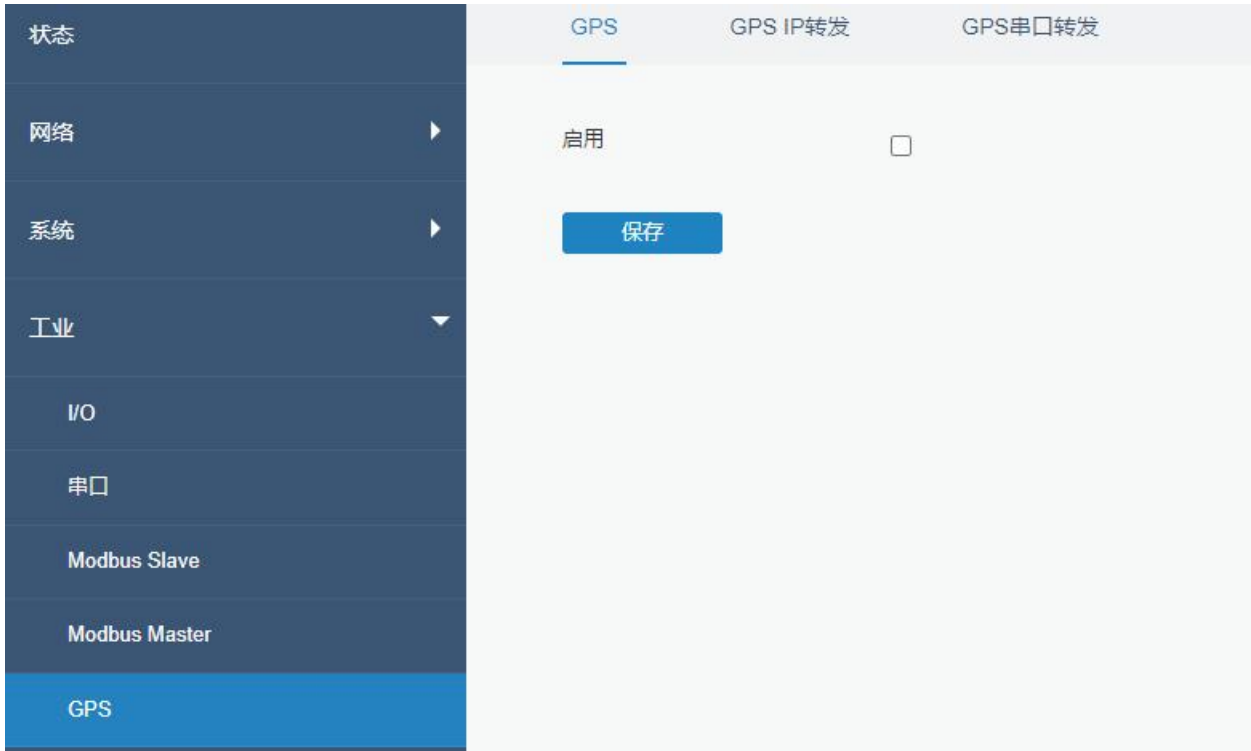


图 3.4.5.1 GPS-1

3.4.5.2 GPS IP 转发

GPS IP 转发意味着 GPS 数据可以通过互联网转发。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus Master

GPS

维护

APP

GPSGPS IP 转发GPS 串口转发

GPS IP 转发

启用☒

类型

客户端

协议

TCP 协议

心跳间隔

75

秒

心跳重试次数

9

times

重连间隔

10

秒

上报信息间隔

30

秒

包含RMC☒

包含GSA☒

包含GGA☒

包含GSV☒

消息前缀

消息后缀

图 3.4.5.2 GPS IP 转发-1

目的IP地址			
服务器地址	服务器端口	状态	操作
			+

图 3.4.5.2 GPS IP 转发-2

GPS IP 转发		
项目	描述	默认值
启用	将 GPS 数据转发到客户端或服务器。	禁用
类型	选择 CPE 的连接类型。 选项是 “客户端” 和 “服务器” 。	Client
协议	选择数据传输协议。 选项是 “TCP” 和 “UDP” 。	TCP
保活间隔（秒）	在与服务器/客户端连接后，CPE 将定期向服务器/客户端发送心跳包以保活。合法值：1-3600。	75
保活重试次数	当 TCP 心跳超时，CPE 将重新发送心跳。达到预设的重试次数后，CPE 将重新连接到 TCP 服务器。合法值：1-16。	9
本地端口	设置 CPE 监听端口。合法值：1-65535。	
重连间隔（秒）	连接失败后，CPE 将以预设的时间间隔重新连接到服务器。合法值：10-60。	10
上报间隔（秒）	CPE 将以预设的时间间隔向服务器/客户端发送 GPS 数据。合法值：1-60。	30

www.milesight.cn

124

包含 RMC	是否在 GPS 数据中包含 RMC。	--
包含 GSA	是否在 GSA 数据中包含 RMC。	--
包含 GGA	是否在 GGA 数据中包含 RMC。	--
包含 GSV	是否在 GSV 数据中包含 RMC。	--
消息前缀	给 GPS 数据添加消息前缀。	Null
消息后缀	给 GPS 数据添加消息后缀。	Null
目标 IP 地址		
服务器地址	填写服务器地址以接收 GPS 数据（IP 地址/域名）。	--
服务器端口	填写端口以接收 GPS 数据。合法值：1-65535。	--
状态	显示 CPE 和服务器之间的连接状态。	--

表 3.4.5.2 GPS IP 转发-1

3.4.5.3 GPS 串口转发

GPS 串口转发意味着 GPS 数据可以转发到串口。

状态

网络

系统

工业

I/O

串口

Modbus Slave

Modbus Master

GPS

GPSGPS IP 转发GPS 串口转发

GPS 串口转发

启用☐

串口类型Serial 1

上报间隔30

包含RMC☒

包含GSA☒

包含GGA☒

包含GSV☒

保存

图 3.4.5.3 GPS 串口转发-1

GPS 串口转发		
项目	描述	默认值
启用	将 GPS 数据转发到预设串行端口。	禁用

串行端口类型	选择串行端口以接收 GPS 数据。	serial
上报间隔（秒）	CPE 将以预设的时间间隔将 GPS 数据转发到串行端口。合法值：1-60。	30
包含 RMC	是否在 GPS 数据中包含 RMC。	--
包含 GSA	是否在 GSA 数据中包含 RMC。	--
包含 GGA	是否在 GGA 数据中包含 RMC。	--
包含 GSV	是否在 GSV 数据中包含 RMC。	--

表 3.4.5.3 GPS 串口转发-1

3.5 维护

3.5.1 工具

故障排除工具包括 ping 探测、路由探测、网络抓包工具和 Qxdmlog。

3.5.1.1 PING 探测

PING 工具用来检测 CPE 的网络状态。



图 3.5.1.1 PING 探测-1

PING	
项目	描述
主机	从 CPEping 外网。

表 3.5.1.1 PING 探测-1

3.5.1.2 路由探测

路由探测工具用于排除网络路由故障。



图 3.5.1.2 路由探测-1

路由探测	
项目	描述
主机	要检测的目标主机的地址。

表 3.5.1.2 路由探测-1

3.5.1.3 网络抓包工具

网络抓包工具用于捕获不同接口的数据包。



图 3.5.1.3 网络抓包工具-1

网络抓包工具	
项目	描述
网口	选择要进行抓包动作的网口。下拉框选项有：ANY/LAN/WAN/Cellular/br-lan1/gre0/gretap0/Loopback/WLAN2/tepl0/tunl0/WLAN1（默认为 ANY）。
IP 地址	设置要进行抓包的 IP 地址。
端口	设置要进行抓包的端口号。
高级	设置抓包的规则，格式为 tcpdump 的参数。

表 3.5.1.3 网络抓包工具-1

3.5.1.4 Qxdmlog

用于抓取蜂窝模块运行日志。



图 3.5.1.4 Qxdmlog-1

3.5.2 调试

3.5.2.1 蜂窝 AT 调试

用户可以下发 AT 指令调试蜂窝模块并查看蜂窝模块运行日志。

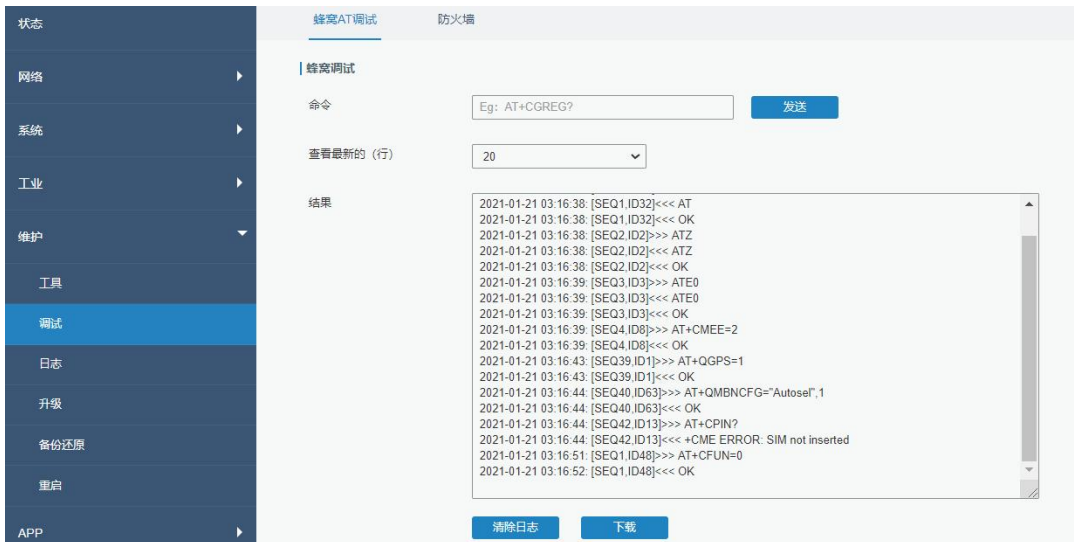


图 3.5.2.1 蜂窝 AT 调试-1

3.5.2.2 防火墙 AT 调试

用户可以下发命令进行防火墙调试。

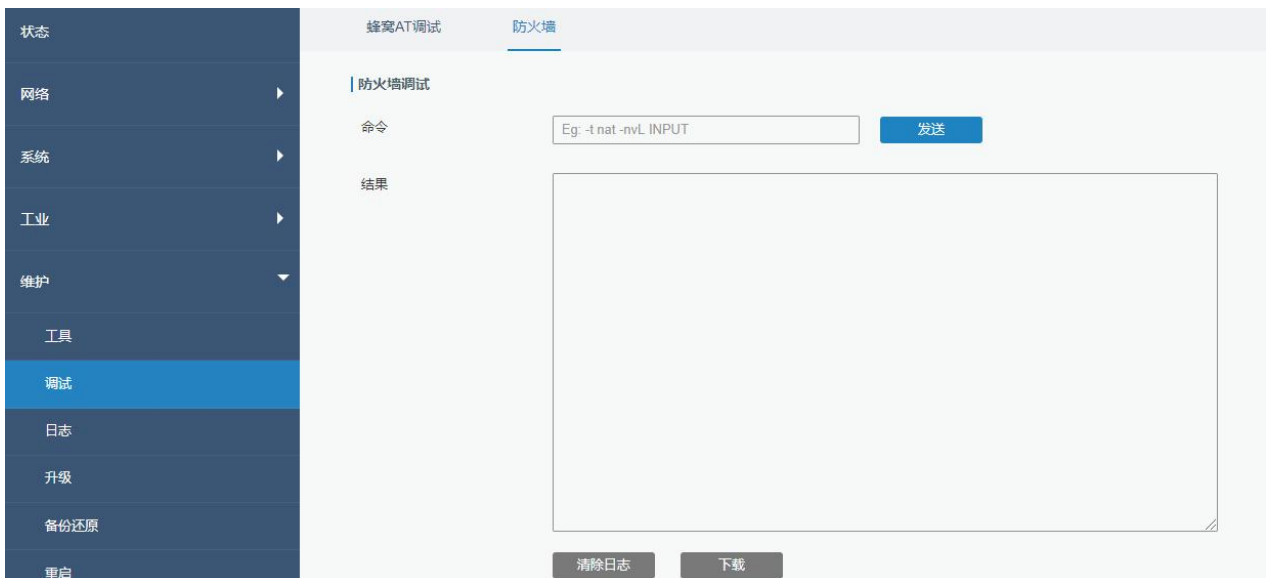


图 3.5.2.2 防火墙调试-1

3.5.3 日志

系统日志包含指示系统如何处理的信息、错误和警告事件的记录。通过查看日志中包含的数据，管理员或用户对系统进行故障排除可以确定问题的原因或系统进程是否成功加载。支持远程查看，CPE 可将所有系统日志上传到远程日志服务器，如 Syslog Watcher。

相关配置案例

日志与诊断

3.5.3.1 系统日志

本节介绍如何查看近期 Web 上的登录情况。系统日志包含了网络和设备的大量信息，包括运行状态、配置变化等。



图 3.5.3.1 系统日志-1

系统日志	
项目	描述
查看最新的（行）	查看最新指定行数的系统日志。
清楚日志	清除当前系统的日志信息。

表 3.5.3.1 系统日志-1

3.5.3.2 系统日志下载

本节介绍如何下载日志至本地。选择想要下载的日志并点击  进行下载



文件名	文件大小/KB	创建时间	操作
vpn.log	1	2021/01/20 07:06:32	
system.log	682	2021/01/21 03:22:46	
httpd.log	268	2021/01/21 03:22:16	
firewall.log	0	2021/01/20 07:06:10	
cellular.log	1470	2021/01/21 03:22:44	

图 3.5.3.2 系统日志下载-1

3.5.3.3 系统日志设置

本节介绍如何启用远程日志服务器和本地日志设置。设置远程日志服务器，CPE 将会把所有的系统日志上传到远程日志服务器。



远程日志服务器

启用 ☒

系统日志服务器地址

端口

本地存储日志

存储位置

大小 KB

日志严重等级

图 3.5.3.3 系统日志设置-1

系统日志设置	
项目	描述
远程日志服务器	
启用	启用“远程日志服务器”后，CPE 会将所有系统日志发送到远程服务器。
系统日志服务器地址	填写远程系统日志服务器地址（IP/域名）。
端口	填写远程日志服务器端口。
本地存储日志	
存储位置	用户可以将日志文件存储在内存或 TF 卡中。
大小	设置本地存储日志文件的大小
日志严重等级	日志严重等级列表遵循标准的 Syslog 协议

表 3.5.3.3 系统日志设置-1

3.5.4 升级

本节介绍如何通过 Web 升级 CPE 固件。
在固件升级过程中不允许在网页上进行任何操作，否则升级将中断，甚至影响设备正常使用。



图 3.5.3.3 系统日志设置-2

升级	
项目	描述
固件版本	显示当前的固件版本。
恢复到出厂设置	若勾选了这个选项，升级后 CPE 会恢复到出厂设置。

升级文件	点击“浏览”选择需要升级的固件文件，再点击“升级”进行固件升级。
------	----------------------------------

表 3.5.3.3 系统日志设置-2

相关配置案例

固件升级

3.5.5 备份还原

本节介绍如何为文件创建系统配置的完整备份，将配置文件还原到 CPE 并重置为出厂默认设置。

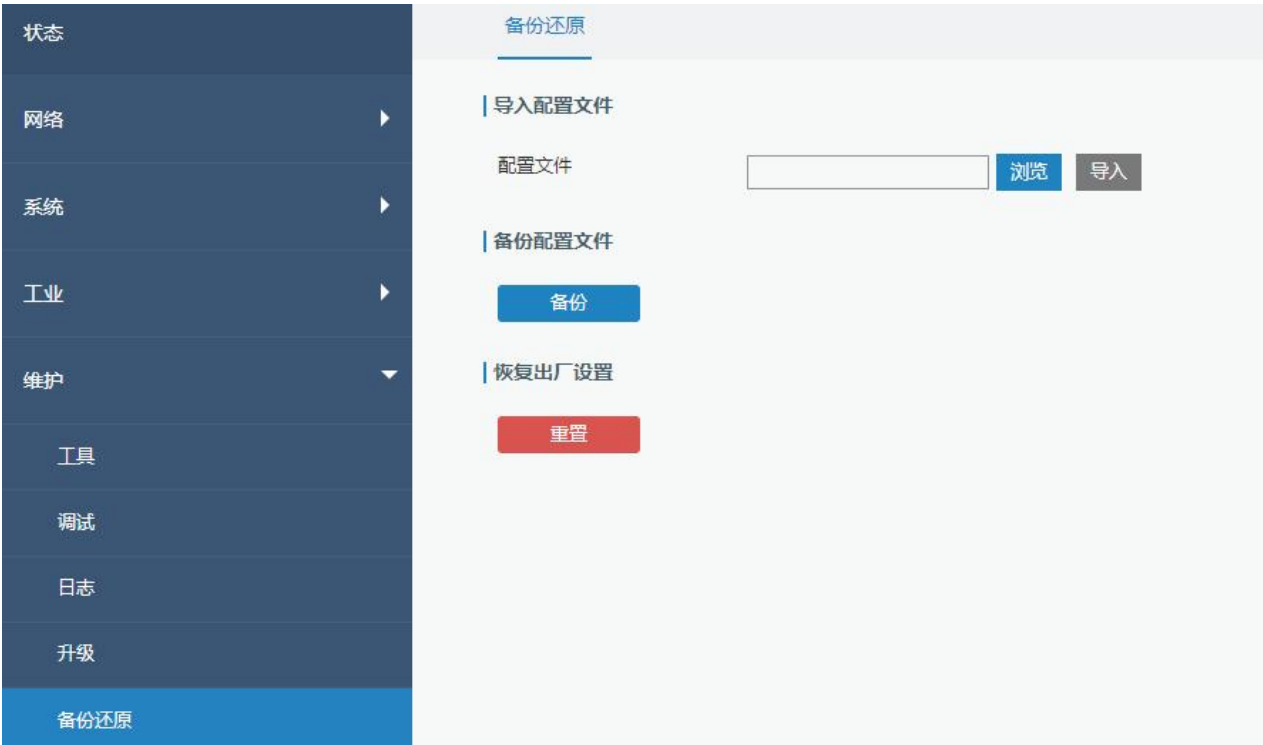


图 3.5.3.3 系统日志设置-3

备份还原	
项目	描述
配置文件	点击“浏览”从电脑选择将要导入到 CPE 的配置文件。点击“导入”把选中的配置文件导入到 CPE。
备份	点击“备份”把当前配置文件备份到电脑。
重置	点击“Reset”使 CPE 恢复出厂设置。恢复出厂后，设备会重启。

表 3.5.3.3 系统日志设置-3

相关配置案例

恢复出厂设置

3.5.6 重启

在此页面上，您可以重新启动 CPE 并返回登录页面。我们强烈建议在重新启动 CPE 之前单击“保存”按钮，以避免丢失新配置。

3.5.6.1 立即重启

点击立即重启，设备会立即重启并返回登录页面

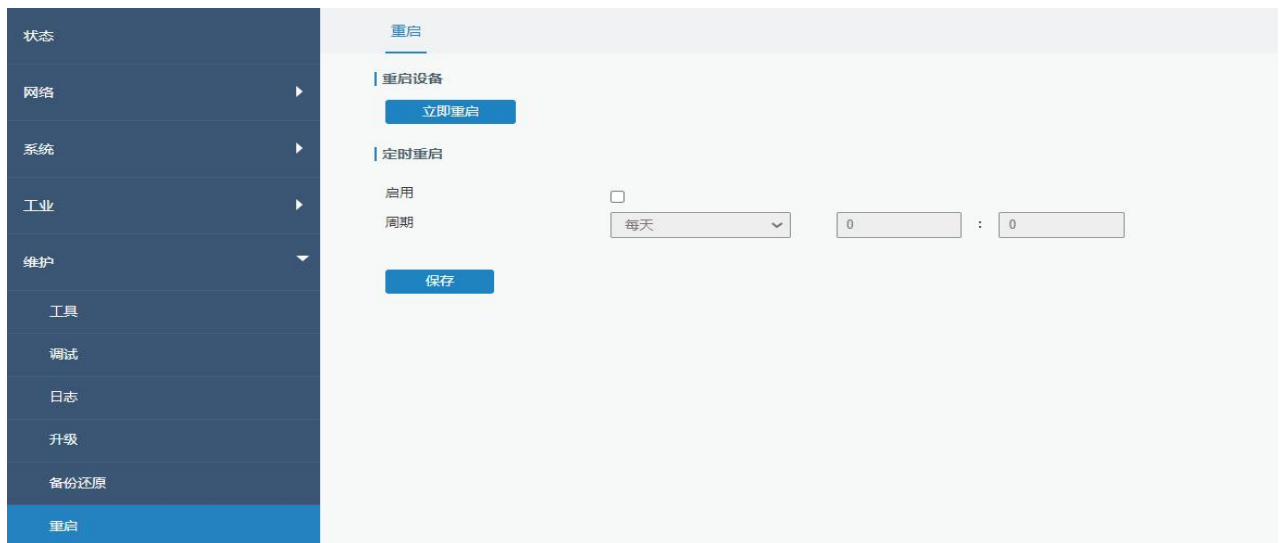


图 3.5.6.1 立即重启-1

3.5.6.2 定时重启

启用定时重启并设置重启周期及时间。每当满足设置周期条件时重启设备

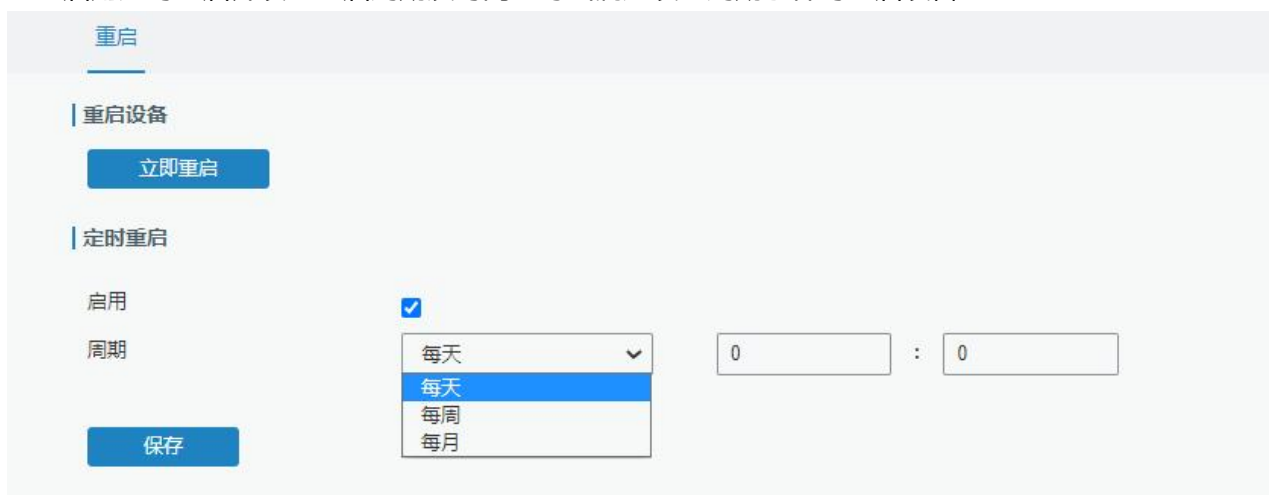


图 3.5.6.2 定时重启-1

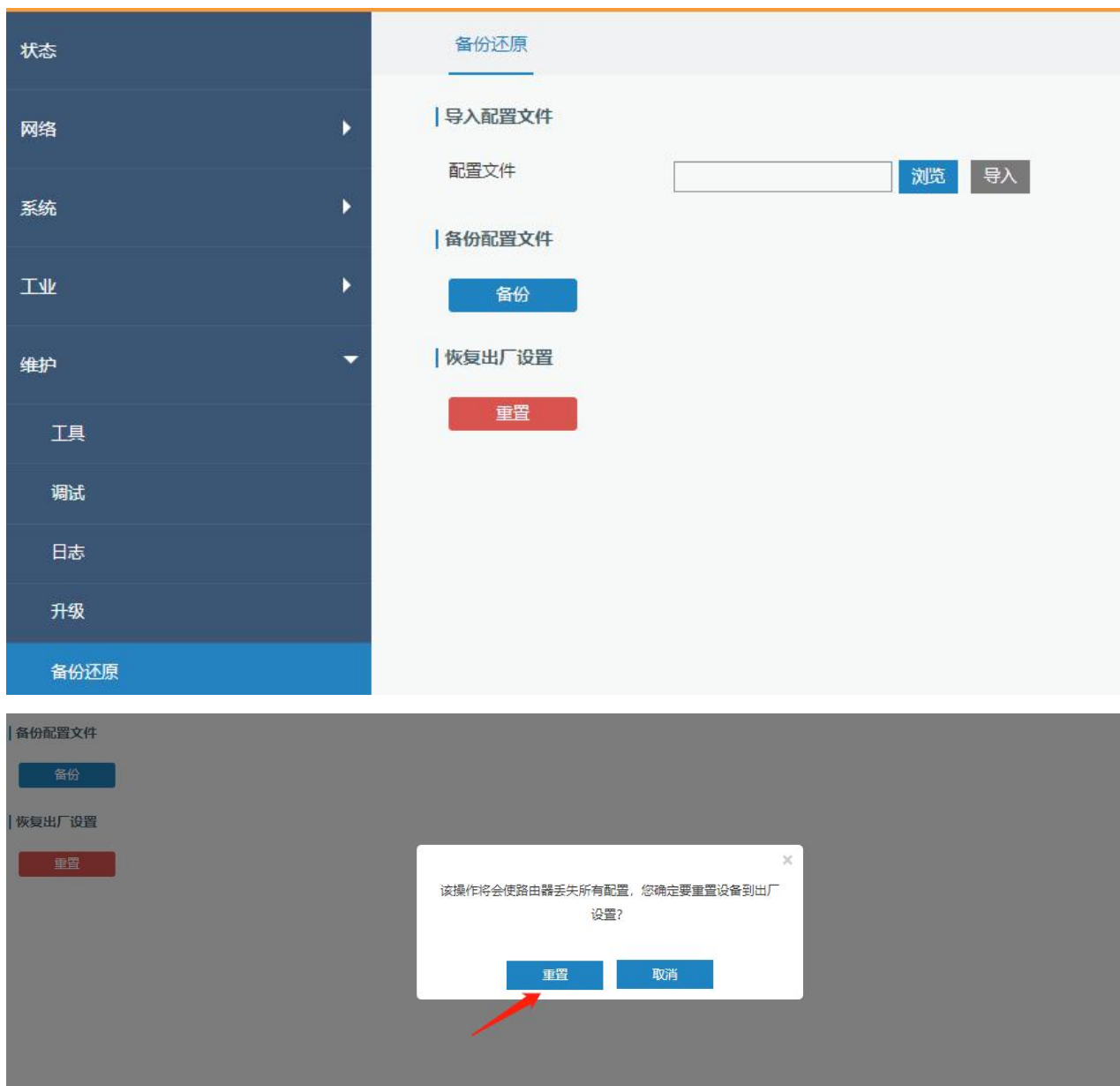
第四章 应用案例

4.1 恢复出厂设置

4.1.1 通过网页页面

1. 登录设备页面，进入“维护>备份还原”。
2. 单击“恢复出厂设置”下的“重置”按钮。

系统会询问您是否确认重置为出厂设置，然后单击“重置”按钮



然后 CPE 设备将重启并立即恢复出厂设置。



登录页面弹出则表示 CPE 设备已被成功恢复出厂设置，请在此页面再次弹出前耐心等待。

中文



 Username

 Password

登录

相关内容

[恢复出厂设置](#)

4.1.2 硬件上重置

找到 CPE 上的重置按钮，根据下表中给出的系统灯状态执行相应动作。

系统灯状态	动作
闪烁	长按重置按钮 15 秒以上
常亮→快速闪烁	松开按钮，等待
重新开始闪烁	CPE 已恢复出厂设置

4.2 固件升级

我们建议您在升级 CPE 固件之前首先咨询星纵物联技术支持。
星纵物联技术支持向您发送固件文件之后，请按照以下步骤进行升级。

1. 进入 “维护>升级”

- 单击“浏览”选择您的个人电脑上要安装的固件文件，勾选恢复到出厂设置时升级完成后设备将恢复出厂默认配置
- 单击“升级”，CPE 将会检查固件文件是否正确。若是，导入固件后 CPE 将开始升级。



相关内容

[升级](#)

4.3 事件应用案例

案例 1

本节中我们将举通过邮件发送告警信息为例，并展示如何在网页页面查看告警。

状态	准备动作（测试中）
CPE 系统启动	给 CPE 电源上电
更新 CPE 时间	手动设置 CPE 时间

配置步骤

- 进入“系统>事件>事件设置”，启用事件设置。
- 勾选想要收到邮件告警的事件，单击最下面的“保存”按钮。

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

设备管理

事件

事件 事件设置

事件设置

启用 ☒

电话群组

邮件群组

事件	记录 ☒	邮件 ☐ 邮件群组	短信 ☐ 电话群组	SNMP ☐
系统启动	☒	☒	☐	☐
系统重启	☒	☒	☐	☐
系统时间更新	☒	☐	☐	☐
VPN上线	☒	☐	☐	☐

3. 如下图配置参数，如邮件发送设置、邮箱群组等。单击“保存”、“应用”使配置生效。

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

设备管理

事件

常规 系统时间 邮箱 存储

SMTP客户端设置

启用 ☒

邮箱地址

密码

SMTP服务器地址

端口号

加密方式

测试

网络

系统

常规

电话 & 短信

用户管理

SNMP

AAA

设备管理

事件

工业

维护

APP

常规 系统时间 邮箱 存储

加密方式

测试

邮箱列表

邮箱地址	描述	操作
support@ursalink.com	1	☒ ☐
		+

邮箱群组

组别ID	描述	邮箱地址	操作
1	1	support@ursalink.com	☒ ☐
			+

保存

4. 为更好地测试告警功能，我们希望您执行上述步骤。

对应事件发生时，系统将向您发送一个告警邮件。

刷新页面，进入“事件>事件”，查看事件记录。



相关内容

[事件](#)

[邮件设置](#)

4.4 日志和诊断

UF51 的系统日志支持 3 种查看方式——网页、下载、远程日志服务器。

案例 1

在网页上获取系统日志。

进入“维护>日志>系统日志”，方框内显示日志。



案例 2

将系统日志发送到远程日志系统。

服务器 IP: 110.22.14.43; 端口: 514

进入“维护>日志>日志设置”，如下图配置对应参数。

状态

网络

系统

工业

维护

工具

调试

日志

升级

系统日志 系统日志下载 系统日志设置

远程日志服务器

启用 ☒

系统日志服务器地址 110.22.14.43

端口 514

本地存储日志

存储位置 本地

大小 2048 KB

日志严重等级 信息

保存

单击“保存”和“应用”按钮。

相关内容

[系统日志](#)

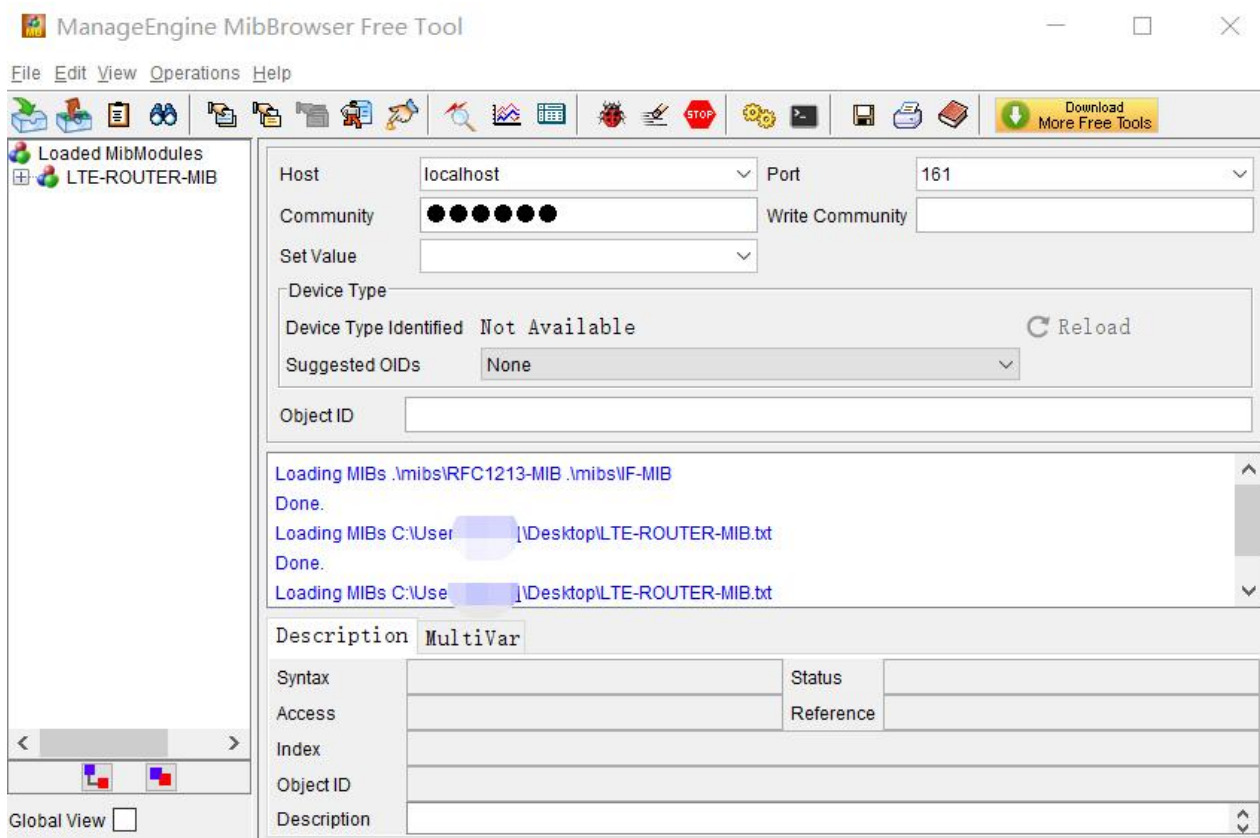
4.5 SNMP 应用案例

在配置 SNMP 参数之前，请先从 CPE 的网页上下载相关的“MIB”文件，然后将其上传到支持标准 SNMP 协议的任何软件或工具。这里我们以“ManageEngine MibBrowser Free Tool”为例，访问 CPE 查询蜂窝信息。

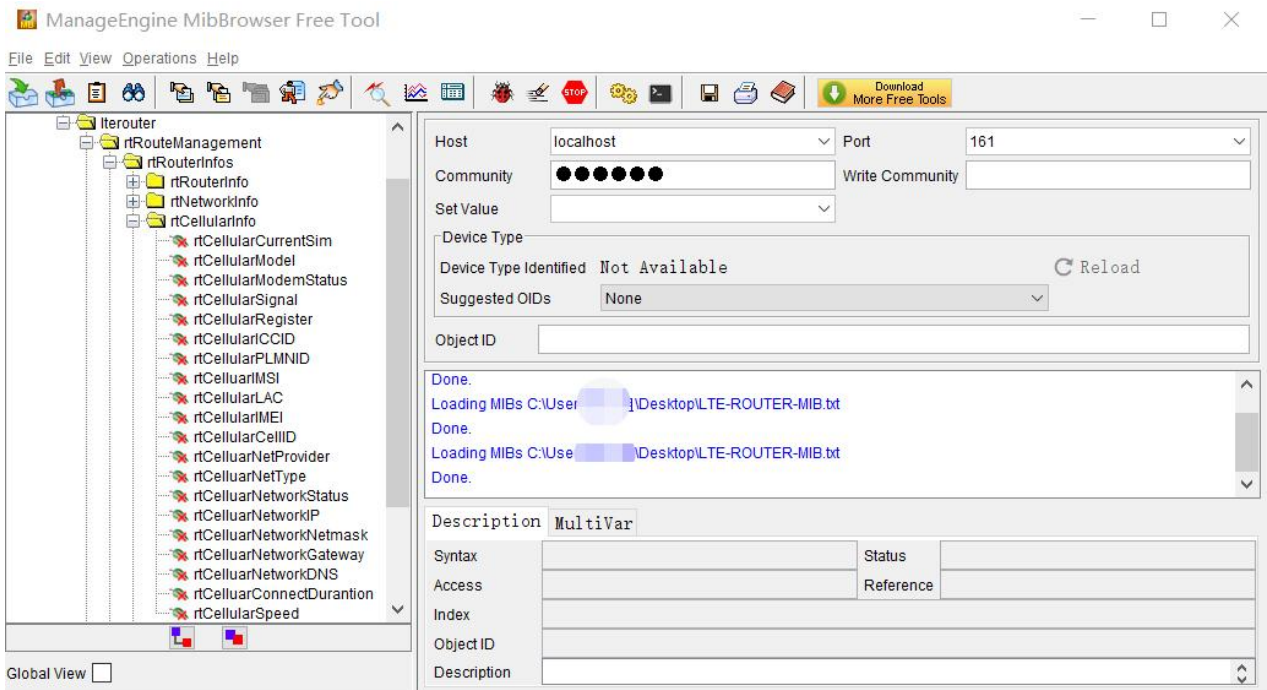
1. 进入“系统>SNMP>MIB”并将 MIB 文件“URSA-CPE-MIB.txt”下载到电脑。



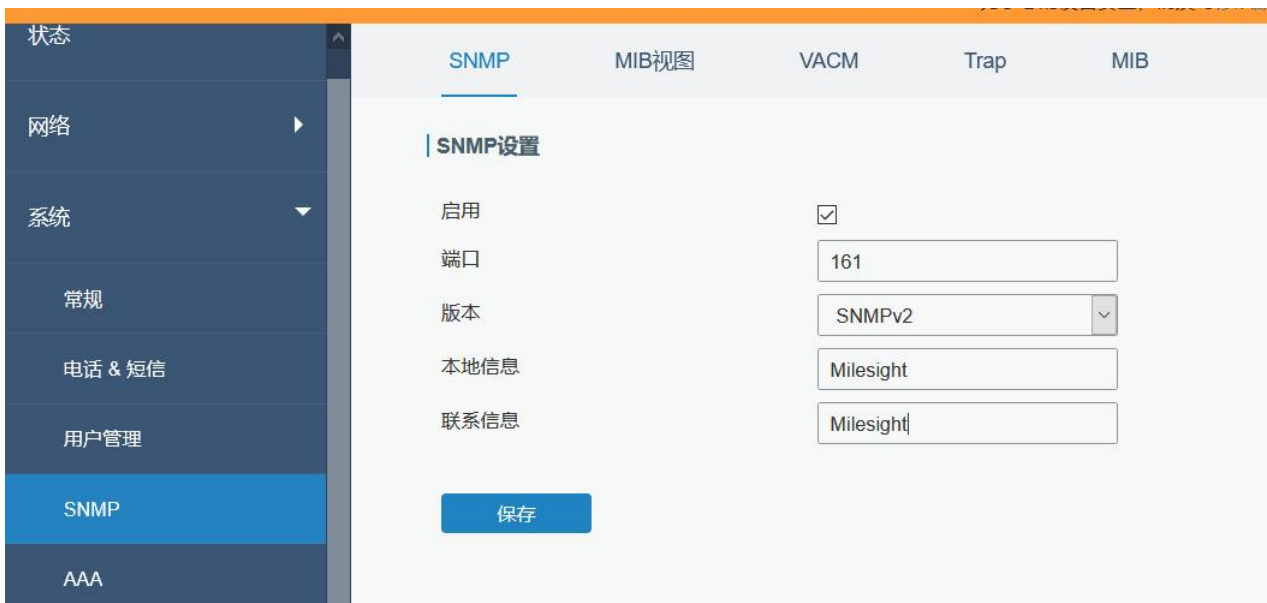
2. 启动电脑上的“ManageEngine MibBrowser Free Tool”，单击菜单栏“文件>载入 MIB”，选中电脑上的“BURSA-CPE-MIB.txt”文件，将其载入软件。



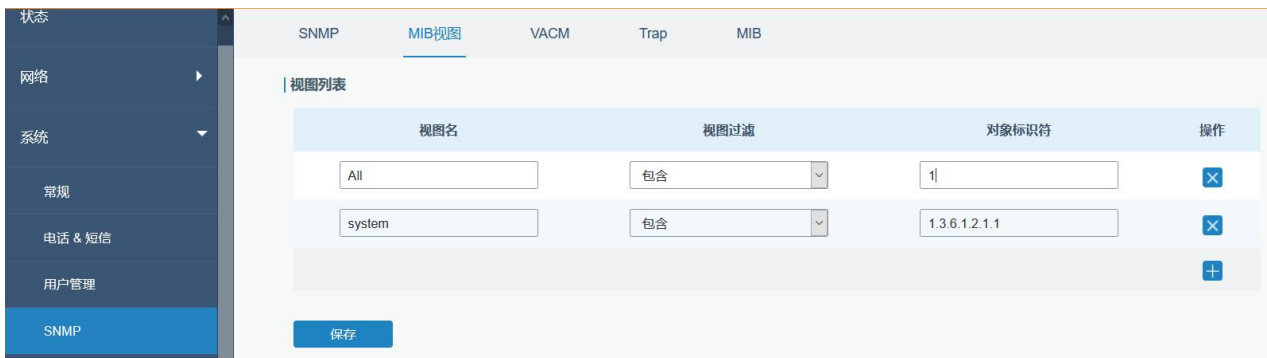
单击菜单栏下“Loaded MibModules”下方“URSA-CPE-MIB”旁的“+”按钮，找到“usCellularinfo”，此处显示蜂窝信息 OID 为“.1.3.6.1.4.1.50234”。



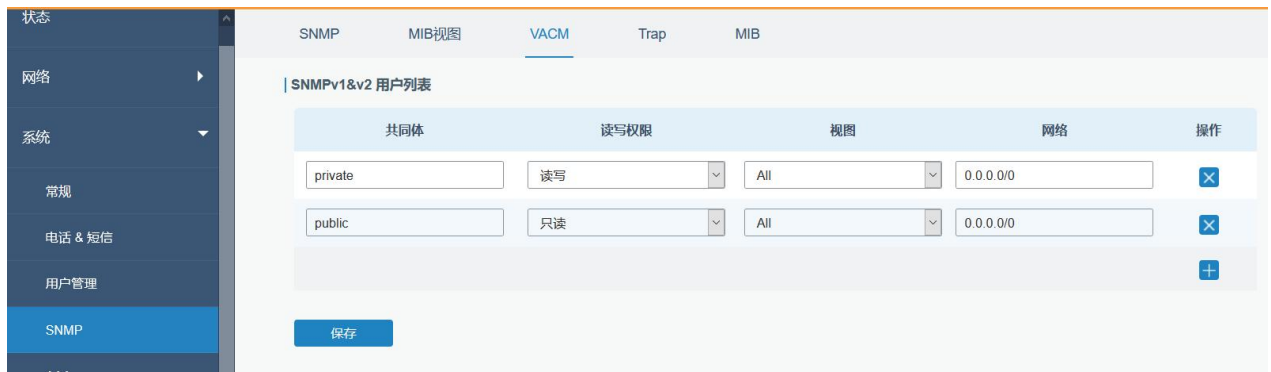
3. 进入网页页面“系统>SNMP>SNMP”，勾选“启用”选项，单击“保存”按钮。



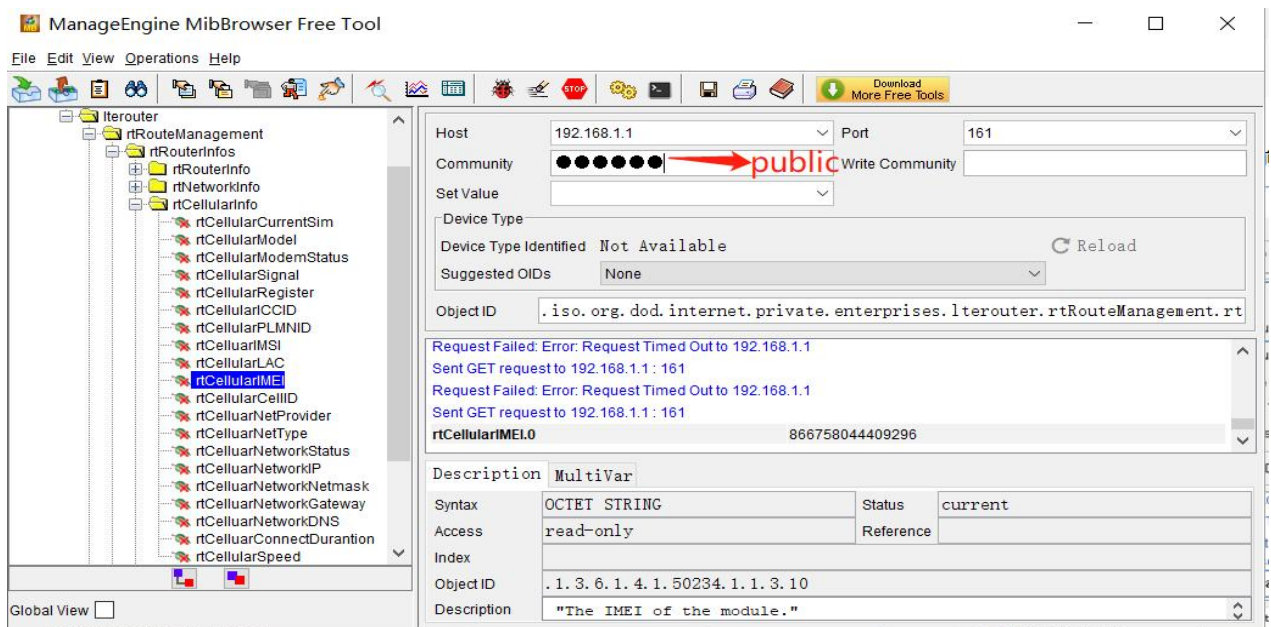
4. 进入“系统>SNMP>MIB 视图”，单击  添加新 MIB 视图并定义为连接外网，单击“保存”按钮。



5. 进入“系统>SNMP>VACM”，单击  添加新的 VACM 设置并指定的外部网络作为视图的访问权限，单击“保存”和“应用”使配置生效。



6. 进入 MibBrowser，输入 Host、port、community。右键单击“usCellular CurrentSim”然后单击“FET”，在下方框中您就能看到当前 SIM 卡信息了。您也能按照这个步骤看到其他蜂窝信息。



相关内容

[SNMP](#)

4.6 网络连接

4.6.1 蜂窝数据连接

案例

我们将举例说明如何将 SIM 卡插入 UF51 的 SIM 插槽，并配置 CPE 以通过蜂窝网络访问互联网。

配置步骤

1. 进入“网络>接口>蜂窝网络>蜂窝设置”并配置蜂窝信息。
2. 启用 SIM。
3. 选择蜂窝网络类型，即网络访问顺序。可选“自动”、“5G-NSA”、“5G-SA”、“仅 4G”、“仅 3G”。

状态	链路备份	蜂窝网络	端口	广域网	网桥	WLAN	交换机	环回
网络	蜂窝设置							
接口	协议类型	IPv4						
DHCP	接入点							
防火墙	用户名							
流量控制	密码							
VPN	PIN码							
IP 穿透	拨号中心号码							
路由	认证方式	Auto						
VRRP	网络类型	自动						
DDNS	PPP优先	☐						
系统	短信中心号码							
工业	启用NAT	☒						
维护	允许漫游	☒						
APP	最大可用流量	0 MB						
	清算日	每月 1 日						
	连接设置							
	连接模式	永远在线						
	重拨间隔(秒)	5						
	保存							

单击“保存”和“应用”使配置生效。

4. 检查蜂窝状态是否已连接

单击“状态>蜂窝”查看 CPE 页面上的蜂窝连接状态是否连接，如果显示“Connected”，则 SIM 已成功拨号上网。

状态	概况	蜂窝	网络	WLAN	VPN	路由信息	主机列表	GPS
网络	蜂窝运行状态					网络		
系统	状态	Ready			状态	Connected		
	模块型号	RM500Q-GL			IPv4 地址	10.41.247.136/28		
工业	版本	RM500QGLABR11A01M4G			IPv4 网关	10.41.247.137		
	当前SIM卡	SIM1			IPv4 DNS	218.85.157.99		
维护	信号强度	99asu (85dBm)			IPv6 地址	fe80::74c0:15ff:fe6:c983/64		
	注册状态	Registered (Home network)			IPv6 网关	::		
APP	IMEI	863305040328782			IPv6 DNS	::		
	IMSI	460115210471226			连接时长	0 days, 00:44:35		
	ICCID	89060320245922910521			月度数据统计			
	运营商	CHN-CT			SIM-1	RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB		
	网络类型	5G NR			SIM-2	RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB		
	PLMN ID	46011						
	位置区码	5E3803						
	Cell ID	0						
	CQI	0						

5. 在电脑上打开浏览器检查是否可以成功上网。

在 PC 上打开您常用的浏览器，输入任意网址尝试是否能通过 UF51 上网。

相关内容

[蜂窝设置](#)

[蜂窝状态](#)

4.6.2 以太网连接

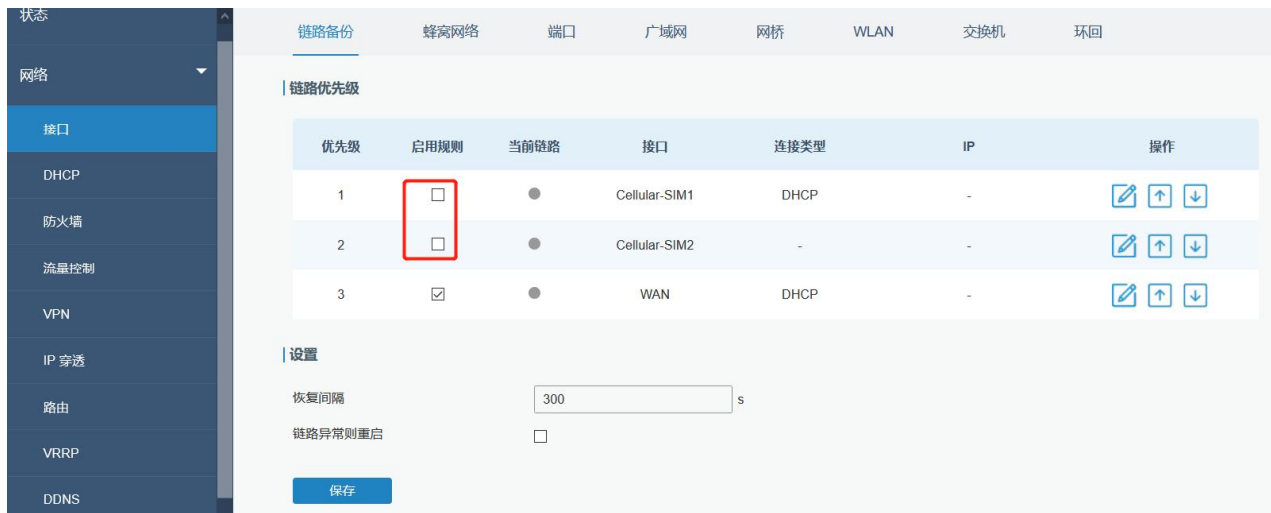
同时启用了“WAN”和“蜂窝”且两者都可用时，默认启用蜂窝接口。

案例

以太网线连接 UF51 的 WAN 口上网。

配置步骤

1. 进入“网络>接口>链路备份”然后禁用“SIM”，单击“保存”。



2. 进入“网络>接口>广域网”配置 WAN 口参数。下面分别为静态 IP 地址、DHCP 客户端、PPPoE 的配置案例。

(1) 静态 IP 地址



(2) DHCP 客户端

状态	链路备份	蜂窝网络	端口	广域网	网桥	WLAN	交换机	环回
网络	广域网设置							
接口	广域网_1							
DHCP	启用	☒						
防火墙	网口	WAN						
流量控制	拨号类型	DHCP客户端						
VPN	最大传输单元	1500						
IP 穿透	使用对端DNS	☒						
路由	启用NAT	☒						
VRRP	保存&应用							

(3) PPPoE

状态	链路备份	蜂窝网络	端口	广域网	网桥
网络	广域网设置				
接口	广域网_1				
DHCP	启用	☒			
防火墙	网口	WAN			
流量控制	拨号类型	PPPoE			
VPN	用户名				
IP 穿透	密码				
路由	链路检测间隔 (秒)	60			
VRRP	最大重拨次数	0			
DDNS	最大传输单元	1500			
系统	使用对端DNS	☐			
	首选DNS	8.8.8.8			
	备用DNS				
	启用NAT	☒			
	保存&应用				

注意：如果您选择 PPPoE 类型，请检查本地 ISP 的“用户名”和“密码”。

单击“保存并应用”按钮以使更改生效。

相关内容

[WAN 设置](#)

WAN 状态

4.7 Wi-Fi 应用案例

4.7.1 接入点模式

应用案例

将 UF51 配置为接入点，允许用户或设备连接。

配置步骤

1. 进入“网络>接口>WLAN”，如下图配置无线参数。

状态	链路备份	蜂窝网络	端口	广域网	网桥	WLAN	交换机	环回
网络	WLAN1-2.4G							
接口	启用	☒						
DHCP	接口类型	接入点						
防火墙	BSSID	24:e1:24:f1:37:b8						
流量控制	射频类型	802.11n(2.4GHz)						
VPN	信道	自动						
IP 穿透	无线频宽	40MHz						
路由	SSID	Router_F137B8						
VRRP	加密方式	No Encryption						
DDNS	SSID广播	☒						
	AP隔离	☐						
	游客网络	☐						
	MAC地址过滤							

在所有配置完成之后单击“保存”和“应用”按钮。

2. 将智能手机连接到您在页面上看到的 SSID，这里如图为“Router_F137B8”。进入“状态>WLAN”，可以查看接入点设置和已连接的客户端、用户。

状态	概况	蜂窝	网络	WLAN	VPN	路由信息	主机列表	GPS
网络	WLAN状态							
系统	名称	状态	接口类型	SSID	IPv4地址	IPv6地址		
工业	WLAN-2.4G	运行	接入点	Router_F137B8	192.168.1.1/24	-		
维护	WLAN-5G	运行	接入点	Router_F137B9	192.168.1.1/24	-		
APP	已关联无线用户							
	SSID名称	MAC地址	IPv4地址	IPv6地址	连接时间			
	Router_F137B8	94:bf:2d:46:fa:a7	192.168.1.105	-	0 seconds			

4.7.2 客户端模式

应用案例

将 UF51 配置为 Wi-Fi 客户端，连接到接入点以进行 Internet 访问。

配置步骤

1. 进入“网络>接口>WLAN”如图配置无线网络。



在所有配置完成之后单击“保存”和“应用”。

2. 进入“状态>WLAN”，可以查看客户端的连接状态。



名称	状态	接口类型	SSID	IPv4地址	IPv6地址
WLAN-2.4G	已连接	客户端	Milesight_HW	192.168.3.148/24	-
WLAN-5G	运行	接入点	Router_F137B9	192.168.1.1/24	-

SSID名称	MAC地址	IPv4地址	IPv6地址	连接时间
Milesight_HW	24:31:54:83:6e:c8	192.168.3.1	-	870 seconds

相关内容

[WLAN 设置](#)

[WLAN 状态](#)

4.8 NAT 应用案例

案例

UF51 可以通过蜂窝接入互联网。LAN 端口与 Web 服务器连接,其 IP 地址为 192.168.1.2,端口为 8000。配置 CPE 使公共网络访问服务器。

配置步骤

进入 “防火墙



>端口映射” 配置端口映射参数。

单击 “保存” 和 “应用” 按钮。

相关内容

[端口映射](#)

4.9 访问控制应用案例

应用案例

UF51 的 LAN 端口设置为 IP 192.168.1.0/24。然后配置 CPE 以拒绝从 IP 地址为 192.168.1.12 的本地设备访问 Google IP 198.98.108.64。

配置步骤

1. 进入 “网络>防火墙>访问控制列表” 配置访问控制列表。单击 “” 按钮如下图配置参数, 然后单击 “保存” 按钮。

ID	动作	协议	源IP地址	目的IP地址	说明
100	拒绝	ip	192.168.1.12	198.98.108.64	google

2. 配置接口列表，配置结束之后单击“保存”和“应用”按钮。

ID	动作	协议	源IP地址	目的IP地址	详细信息	说明	操作
100	拒绝	ip	192.168.1.12/0.0.0.255	198.98.108.64/0.0.0.255		google	✕
+							

接口名称	入站规则	出站规则	操作
Bridge0	100		✕
+			

[保存](#)

相关内容

[ACL](#)

4.10 流量控制应用案例

案例

配置 UF51，将本地优先级分配给不同的 FTP 下载通道。总下载带宽为 75000 kbps。

注意：“总下载带宽”应小于 WAN 或蜂窝接口的实际最大带宽。

FTP 服务器 IP 及 Port	比例	最大带宽 (kbps)	最小带宽 (kbps)
-------------------	----	-------------	-------------

110.21.24.98:21	40%	30000	25000
110.32.91.44:21	60%	45000	40000

配置步骤

1. 进入“网络>流量控制>下行带宽控制”，启用流量控制并设置总下行带宽。

2. 找到“服务类别”，单击“+”设置服务类别。

注意：比例加起来必须为 100%。

3. 找到“服务类别规则”，单击“+”设置规则。

注意：

IP 地址/端口为空则指任意 IP 地址/端口。

单击“保存”、“应用”按钮。

相关内容

[流量控制设置](#)

4.11 DTU 应用案例

案例



可编程逻辑控制器通过 RS232 与 UF51 连接。然后启动 UF51 的 DTU 功能，使远程 TCP 服务器与 PLC 通信。请参阅以下拓扑图。

PLC 串口参数	
波特率	9600
数据位	8
停止位	1
校验位	None

配置步骤

1. 进入“工业>串口>串口”配置串口参数，必须与可编程逻辑控制器的参数保持一致，如下图所示。

The screenshot shows the '串口' (Serial Port) configuration page. On the left is a sidebar with menu items: 状态, 网络, 系统, 工业, I/O, and 串口 (highlighted). The main area is titled '串口设置' (Serial Port Settings) for '串口1'. It includes a '启用' (Enable) checkbox which is checked. Below it are dropdown menus for '串口类型' (Serial Port Type) set to RS232, '波特率' (Baud Rate) set to 9600, '数据位' (Data Bits) set to 8bits, '停止位' (Stop Bits) set to 1bits, and '校验位' (Parity) set to None. At the bottom is a '软件流控' (Software Flow Control) checkbox which is unchecked.

2. 配置串口模式为“DTU 模式”。UF51 作为客户端接入的协议选择“透明传输”。

This screenshot shows the configuration page for '串口1' in DTU mode. The sidebar on the left includes additional options: Modbus Slave, Modbus Master, and GPS. The '串口设置' section now includes '软件流控' (unchecked), '串口模式' (DTU模式), 'DTU协议' (透明传输), and '协议' (TCP). It also features input fields for '保活间隔' (75 秒), '保活重试次数' (9), '串口分帧长度' (1024 字节), '串口分帧间隔' (100 毫秒), and '重连间隔' (10 秒). There are checkboxes for '指定协议' and a text field for '注册包内容'.

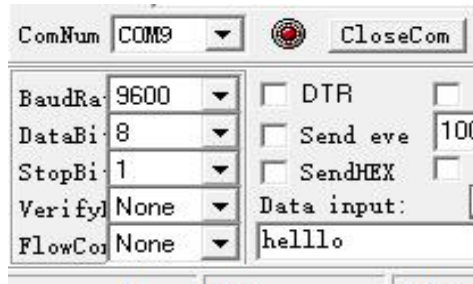
3. 配置 TCP 服务器 IP 地址和端口。

The screenshot shows the '目的IP地址' (Destination IP Address) configuration section. It contains a table with the following columns: 服务器地址 (Server Address), 服务器端口 (Server Port), 状态 (Status), and 操作 (Action). One entry is shown with the server address '110.87.98.58' and port '7087'. The status is a dash '-', and the action column has 'X' and '+' icons. Below the table is a '保存&应用' (Save & Apply) button.

4. 结束所有配置之后，单击“保存”和“应用”按钮。
5. 在 PC 上开启 TCP 服务器。
用“Netassist”测试软件举例，确保端口映射已完成。

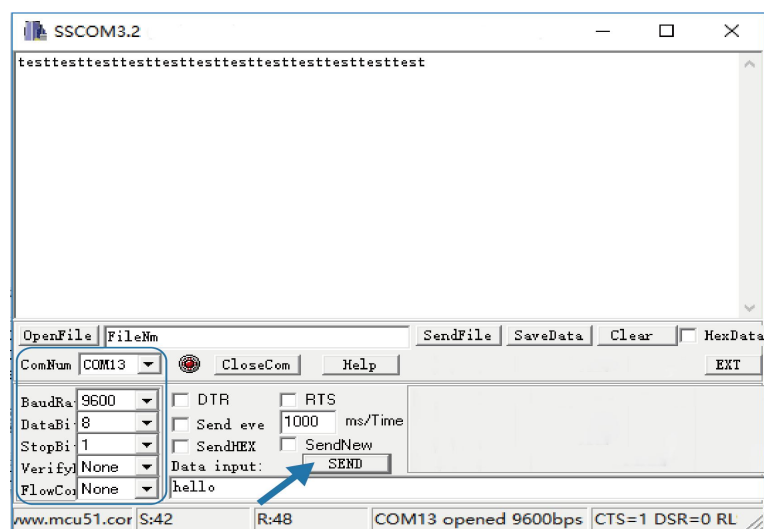


6. UF51 通过 RS232 串口线连接到电脑，启动电脑上的“sscom”软件以测试串口通信。

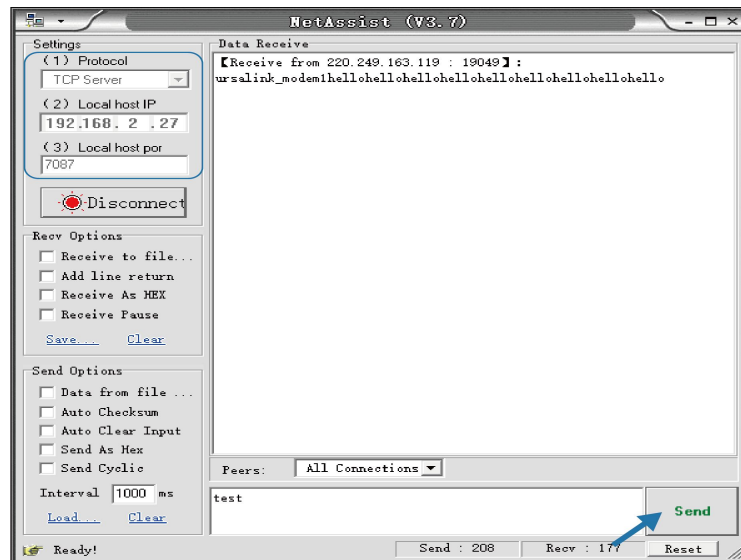


7. UF51 和 TCP 服务器的通信连接成功之后，可以在 sscom 和 Netassit 之间传输数据。

PC 端



TCP 服务器端



8. 串口通信测试完成之后，连接可编程逻辑控制器 PLC 到 UF51 的 RS232 端口进行测试。

相关内容

[串口](#)

4.12 PPTP 应用案例

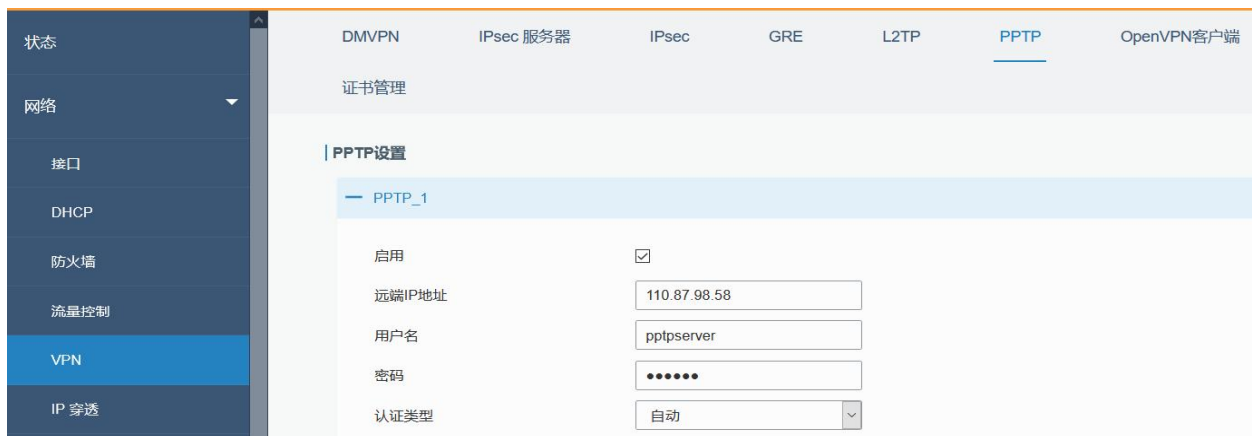
案例



将 UF51 配置为 PPTP 客户端以连接到 PPTP 服务器，以便安全地传输数据。请参阅以下拓扑图。

配置步骤

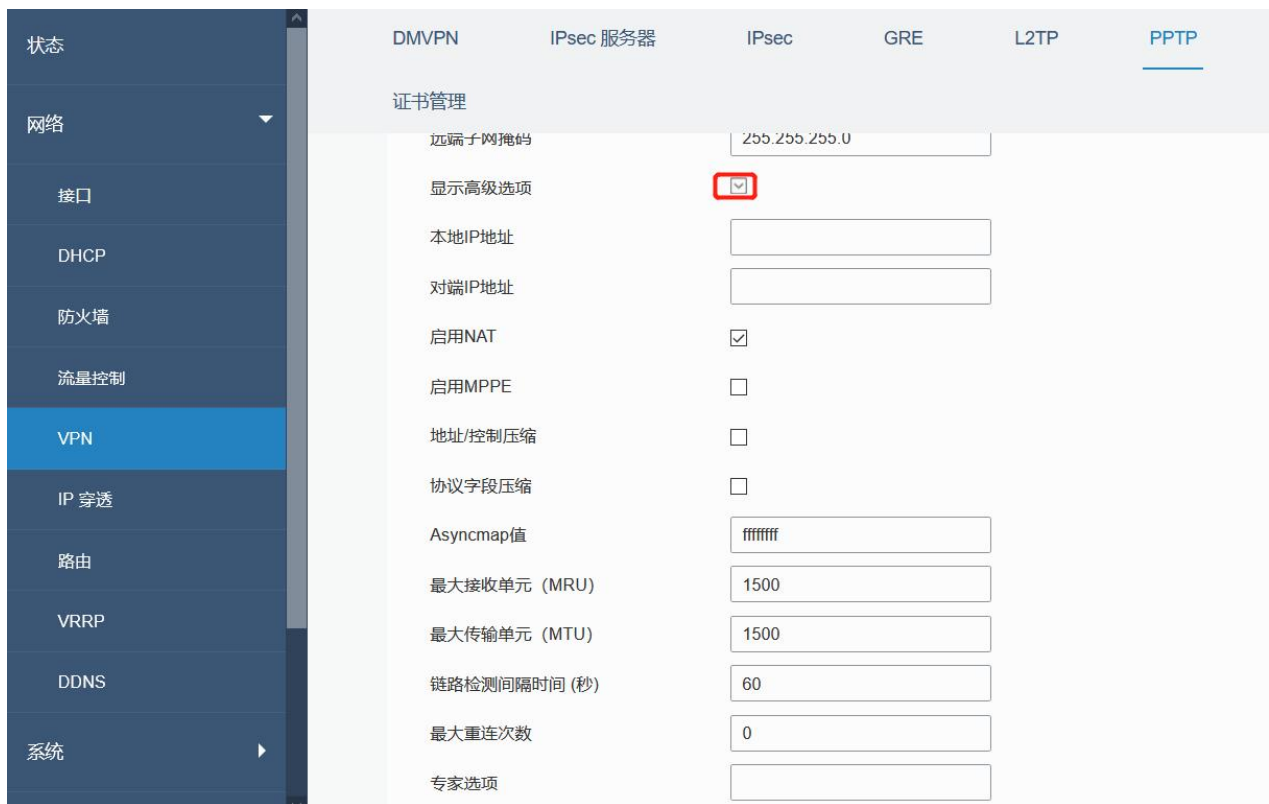
1. 进入“网络>VPN>PPTP”，根据 PPTP 服务器提供的 IP 地址、用户名、密码配置 PPTP 服务器。
注意：如果你希望所有数据都通过 VPN 隧道传播，勾选“全局流量转发”选项。



如果想要访问对端子网，举 192.168.3.0/24 为例，需要将子网和子网掩码加入路由。

全局流量转发	☐
远端子网	192.168.3.0
远端子网掩码	255.255.255.0
显示高级选项	➤

2. 勾选“显示高级选项”，查看高级设置。



如果 PPTP 服务器需要 MPPE 加密，勾选“启用 MPPE”。

启用MPPE
☒

如果 PPTP 服务器分配了固定隧道 IP 给客户端，可将本地隧道 IP 和对端隧道 IP 填入，如下图所示。

显示高级选项 ☒

本地IP地址

对端IP地址

否则 PPTP 服务器将随机分配隧道 IP。

完成所有设置之后单击“保存”按钮，高级选项将折叠起来。然后单击“应用”按钮使配置生效。

3. 进入“状态>VPN”查看 PPTP 连接状况。

相关内容

[PPTP 设置](#)

[PPTP 状态](#)