

UR75

工业路由器

用户手册



前言

感谢您选择星纵物联 UR75 工业蜂窝路由器。UR75 工业蜂窝路由器具备丰富的功能，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，路由器带有自动网络连接备份/故障恢复，双 SIM 卡，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 UR75 工业蜂窝路由器。 您可以参考它来获取详细路由器功能和配置。

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

© 2011-2023 厦门星纵物联科技有限公司

版权所有。

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：

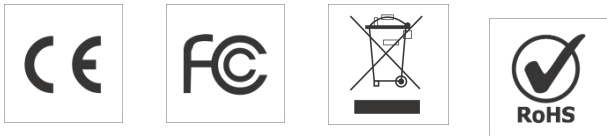
- 星纵物联 UR75 工业路由器

相关文档

文档名称	文档描述
UR75 规格书	星纵物联 UR75 工业路由器规格书

一致性声明

UR75 符合 CE, FCC 和 RoHS 的基本要求和和其他相关规定。



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
地址: 厦门市集美区软件园三期 C09 栋

修订记录

日期	文档版本	文档描述
2023.2.9	V1.0	UR75 初始版本

目录

阅读人群	2
第一章 产品介绍	6
1.1 概述	6
1.2 优势	6
1.3 产品尺寸 (mm)	7
第二章 登录网页端操作界面	8
2.1 配置 PC 以连接路由器	8
2.2 路由器登录	9
第三章 网页端配置	10
3.1 状态	10
3.1.1 概览	10
3.1.2 蜂窝网络	12
3.1.3 GPS	15
3.1.4 防火墙	16
3.1.5 路由表	17
3.1.6 VPN	18
3.2 网络	18
3.2.1 接口	18
3.2.2 WLAN (仅 WiFi 版本)	31
3.2.3 防火墙	32
3.2.4 静态路由	38
3.2.5 网络诊断	38
3.3 VPN	39
3.4 工业	58
3.4.1 串口	59
3.4.2 I/O	62
3.4.3 Modbus Master	64
3.4.4 GPS	66
3.5 系统	69
3.5.1 常规	70
3.5.2 密码	71
3.5.3 设备管理	72
3.5.4 备份还原	74

3.5.5 重启	75
3.5.6 日志	75
3.5.7 调试	77
第四章 应用案例	79
4.1 恢复出厂设置	79
4.1.1 通过网页页面	79
4.1.2 硬件上重置	81
4.2 固件升级	81
4.3 网络连接	82
4.3.1 蜂窝数据连接	82
4.3.2 以太广域网连接	84
4.4 双 SIM 故障转移应用案例	85
4.5 Wi-Fi 应用案例	87
4.6 NAT 应用案例	88
4.7 DTU 应用案例	89

第一章 产品介绍

1.1 概述

星纵物联 UR75 是一款工业级蜂窝路由器，具有嵌入式智能软件功能，专为多种 M2M/IoT 应用而设计。UR75 支持全球 4G LTE 和 5G SA&NSA 网络，为用户提供快速网络接入，同时保障网络连接的稳定与可靠。

UR75 采用高性能，低功耗的工业级 CPU 和无线模块，能够提供低功耗的无线网络和超小型封装，确保与无线网络的安全可靠的连接。同时，UR75 还支持千兆以太网口、串口（RS232/RS485）和 I/O（输入/输出），使您能够在有限的时间和预算内部署将数据和视频业务相结合的 M2M 应用。

UR75 广泛应用于智能电网、数字媒体设备、工业自动化、遥测设备、医疗设备、数字工厂、金融、支付设备、环境保护、水利等行业。

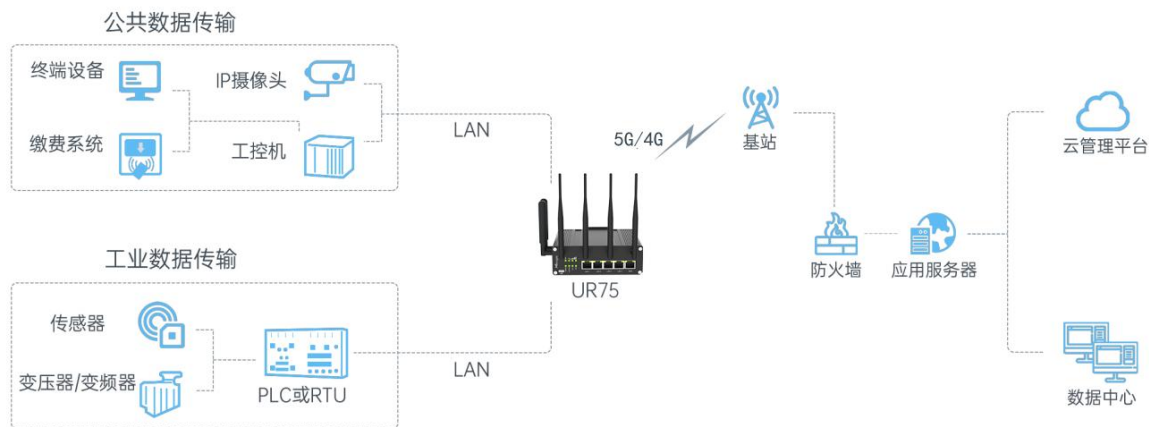


图 1.1 概述-1

1.2 优势

极速网络连接

- 工业级四核 CPU ARM Cortex-A55 大内存，提供高性能的数据传输
- 全球 5G (NSA/SA)/4G LTE 双卡双待网络，支持多运营商网络互通
- 5G Sub-6GHz 支持双载波聚合 (2CC CA)，可实现更宽的信号覆盖范围，下载速度高达 4.67 Gbps
- 支持千兆以太网端口或 USB Type-C 接口提供数据传输，即插即用
- 支持 Wi-Fi 6，允许 2.4G & 5G 双频并发，下载速度高达 1.8 Gbps

安全性和可靠性

- 以太网有线接入、Wi-Fi 和蜂窝网络之间自动连接备份和故障恢复（同时有双 SIM 卡备份）
- 支持 VPN 安全数据传输，如 IPsec/OpenVPN
- 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
- 配备 ACL、DMZ、SYN-Flood 保护、数据过滤等多重安全保护措施，确保网络安全
- 支持路由策略和 NAT，提供更安全的内网访问

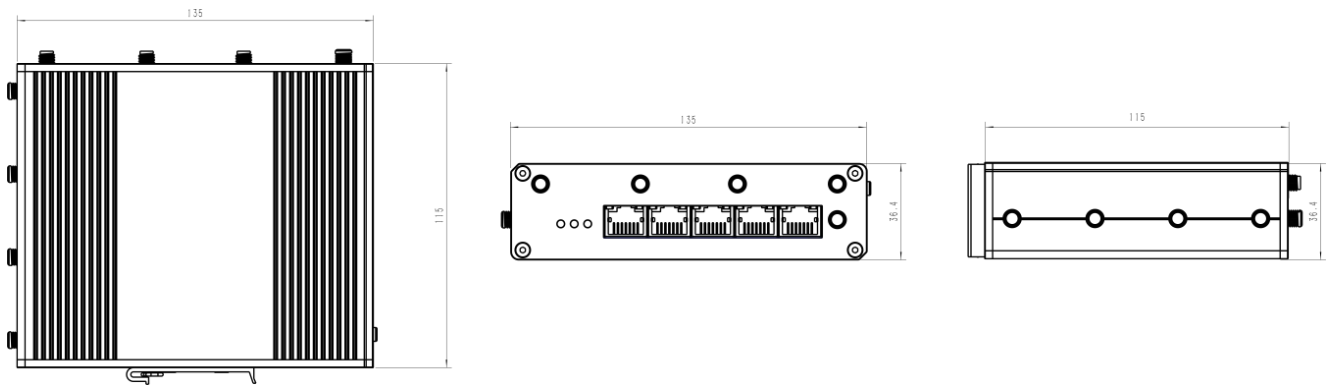
易于维护

- 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
- 支持多级用户权限安全管理

工业级设计

- 针对恶劣环境的工业设计，宽温宽压，支持-30℃ 至 60℃ 的工作温度范围
- IP30 防护等级外壳，支持 DIN 导轨或壁挂等多种安装方式。
- 配备 I/O、串口、GPS，适用于工业传输应用

1.3 产品尺寸 (mm)



第二章 登录网页端操作界面

本章介绍如何访问 UR75 路由器的网页端操作界面。

2.1 配置 PC 以连接路由器

请将 PC 直接连接 UR75 路由器的 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。



调整计算机的设置

查看方式: 类别



系统和安全

查看你的计算机状态
通过文件历史记录保存你的文件备份副本
备份和还原(Windows 7)



网络和 Internet

查看网络状态和任务



硬件和声音

查看设备和打印机



程序

添加设备
调整常用移动设置
卸载程序



用户帐户

更改帐户类型



外观和个性化



时钟和区域

更改日期、时间或数字格式

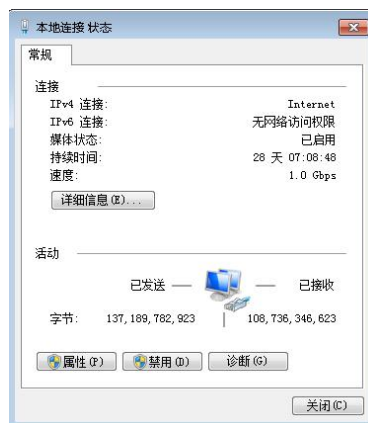


轻松使用

使用 Windows 建议的设置
优化视觉显示

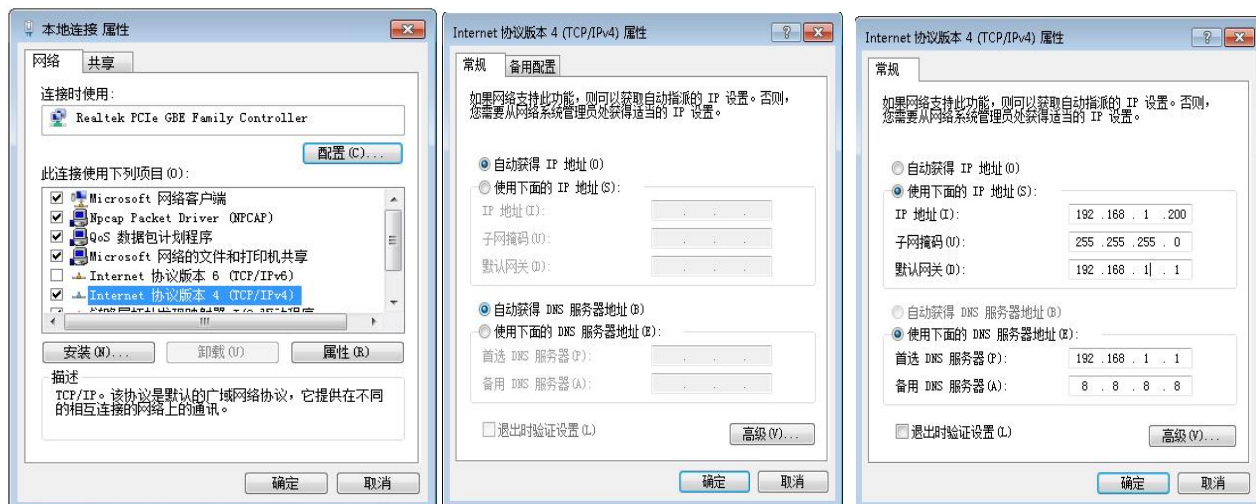
①在 Windows 10 任务栏单击“搜索框”以搜索“控制面板”。

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 路由器登录

星纵物联路由器为配置管理提供了网页端操作界面。如果您第一次使用路由器，默认配置如下：

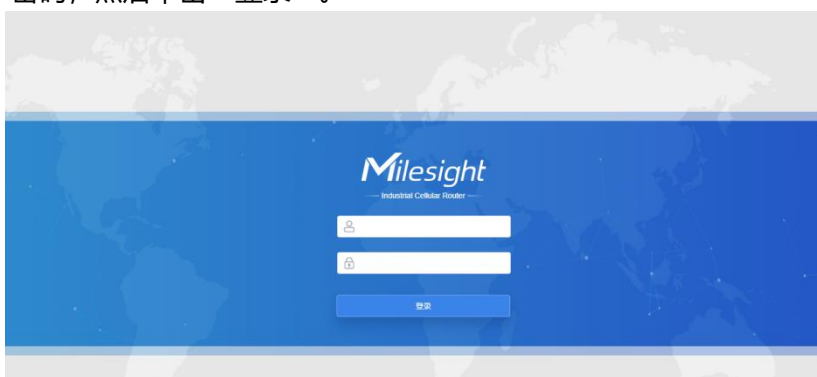
用户名: admin

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”。





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。

The image shows a '修改密码' (Change Password) dialog box. It contains three input fields: '旧密码' (Old Password), '新密码' (New Password), and '确认密码' (Confirm Password). Each field has a toggle icon to the right. At the bottom right, there are two buttons: '取消' (Cancel) and '保存' (Save).

4. 登录 Web GUI 后，您可以在路由器上查看系统信息并执行配置。

The screenshot shows the Milesight Web GUI interface. On the left is a sidebar with a '状态' (Status) menu. The main content area displays system information under the '状态' tab. A yellow banner at the top reads: '为了您的设备安全，请及时修改默认密码' (For your device security, please modify the default password in time). The system information table lists details such as device name, model, SN, firmware version, hardware version, local time, uptime, and average load. Below the table, the memory usage is shown with two progress bars: '可用' (Available) at 53% and '已用' (Used) at 47%.

系统	
主机名	Router
型号	UR75-504AE-W
SN	6019C3084044
固件版本	78.0.0.2-a4
硬件版本	V1.1
本地时间	2023-01-16 13:22:25
运行时间	0h 8m 10s
平均负载	3.18, 2.68, 1.43

内存	
可用	348.02 MB / 651.01 MB (53%)
已用	302.99 MB / 651.01 MB (47%)

第三章 网页端配置

3.1 状态

3.1.1 概览

状态中的系统、内存部分主要包含一些路由器的基本信息

状态

系统

主机名	Router
型号	UR75-S04AE-W
SN	6019C3084044
固件版本	78.0.0.2-a4
硬件版本	V1.1
本地时间	2023-02-09 06:53:51
运行时间	3h 51m 13s
平均负载	4.73, 4.14, 3.69

内存

可用数	337.41 MB / 651.01 MB (52%)
已用	313.61 MB / 651.01 MB (48%)

状态

项目

描述

系统

主机名	显示设备的主机名，可以在 系统 > 系统 > 常规设置 中修改。
型号	显示设备的型号名称。
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。
本地时间	显示设备当前系统时间，可在 系统 > 系统 > 常规设置 中修改。
运行时间	显示设备上电运行时间
平均负载	显示设备的平均运行负载情况。显示数值为逐渐延长时间段（1、5 和 15 分钟的平均值）的负载平均值，数值越小越好。

内存

可用数	显示当前内存可用数量
已用	显示当前内存已使用数量

当前网络栏内显示正在使用的链路的基本信息，点击**网络>接口**可查看详情及配置。

当前网络

● 表示可访问Internet的IP地址

蜂窝网络

(?)

● 表示可访问Internet的IP地址

WAN

(?)

当前SIM卡: SIM1
IPv4: 10.18.108.251/29
● IPv6: 240e:465:2134:14b6::1/128
运行时长: 0h 0m 35s

类型: 静态地址
● IPv4: 192.168.48.206
IPv6: -
IPv4 网关: 192.168.48.1
IPv6 网关: -
MAC: 24:E1:24:F5:AF:DE
运行时长: 4h 26m 20s

已分配的 DHCP 租约栏内显示当前已连接设备的基本信息

已分配的 DHCP 租约			
主机名	IPv4 地址	MAC 地址	剩余租期
DESKTOP-JT9JHJ5	192.168.1.100	00:E0:99:01:98:45	23h 3m 36s

已分配的 DHCP 租约	
项目	描述
主机名	显示已连接设备的主机名。
IPv4 地址	显示已连接设备的 IPv4 地址。
MAC 地址	显示连接设备的 MAC 地址。
剩余租期	显示此设备本次租约的剩余时间。

3.1.2 蜂窝网络

在此页面可以查看路由器的蜂窝网络状态

蜂窝运行状态	
状态	Ready
模块型号	RG500L-EU
版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
当前SIM卡	SIM1
蜂窝频段	N78
信号强度	-90dBm
注册状态	Registered(Home network)
IMEI	869263050069412
IMSI	460115210733085
ICCID	89860321245923785517
运营商	CHN-CT
网络类型	5G SA
PLMN ID	46011
位置区域	5E3503
Cell ID	5E46D7005
CQI	-
下行带宽	100MHz
上行带宽	100MHz
信噪比	25dB
PCI	230
RSRP	-85dBm
RSRQ	-11dB
EARFCN	99240

蜂窝运行状态	
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。
版本	显示蜂窝模组当前版本
当前 SIM 卡	显示当前使用的 SIM 卡。
蜂窝频段	显示当前路由器蜂窝注册使用频段
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。
CQI	显示蜂窝网络的信道质量指标。
下行带宽	显示蜂窝网络的下行带宽。
上行带宽	显示蜂窝网络的上行带宽
信噪比	显示蜂窝网络的信号干扰+噪声比。
PCI	显示蜂窝网络的物理层小区标识。
RSRP	显示蜂窝网络的参考信号接收功率。
RSRQ	显示蜂窝网络的参考质量接收功率。
EARFCN	显示载波频点号。

网络

状态	已连接
IPv4 地址	10.18.108.251/29
IPv4 网关	10.18.108.252
IPv4 DNS	218.85.152.99
IPv6 地址	240e:465:2134:14b6::1/128
IPv6 网关	fe80::2
IPv6 DNS	240e:14:6000::1
连接时长	0days, 00:29:56

月度流量统计

流量统计结果仅供参考，实际流量以运营商提供的收费账单为准。

SIM-1	RX: 0.0 MiB	TX: 0.0 MiB	ALL: 0.0 MiB
SIM-2	RX: 0.0 MiB	TX: 0.0 MiB	ALL: 0.0 MiB

网络	
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
月度数据统计	
项目	描述
SIM-1	显示 SIM 卡 1 当月的流量使用情况
SIM-2	显示 SIM 卡 2 当月的流量使用情况

3.1.3 GPS

在开启 GPS 功能并成功获取 GPS 信息后，您可以在本页面查看最新的 GPS 信息，包括 GPS 时间、经纬度、速度等。

GPS 状态

状态	已获取
定位时间	2022/11/23 11:15:57
卫星使用数量	35
可见卫星数量	73
纬度	24.623978 N
经度	118.030707 E
高度	75.9 M
速度	0.000000 km/h

GPS 状态	
项目	描述
状态	显示当前 GPS 状态。
定位时间	显示本地定位时间。
卫星使用数量	显示使用中的卫星数量。
可见卫星数量	显示可见卫星数量。
纬度	显示路由器位置纬度。
经度	显示路由器位置经度。
高度	显示路由器位置高度。
速度	显示路由器移动速度。

3.1.4 防火墙

在此页面上，您可以检查 iptables 的所有 IPv4/IPv6 网络链路。用户可以点击虚线标示的目标，跳转到对应的网络链路。

防火墙状态

IPv4 防火墙IPv6 防火墙

显示空链 复位计数器 重启防火墙

表: Filter

链 INPUT (策略: ACCEPT, 0 B 数据包, 0 B 流量)

数据包	流量	目的网络	协议	入口	出口	源地址	目标地址	选项	备注
5.91 K	487.41 KB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
8.91 K	1.53 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
8.31 K	1.46 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
65	3.38 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
595	67.90 KB	zone_wan_input	all	eth1	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	ccmni2	*	0.0.0.0/0	0.0.0.0/0	-	-
6	433 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-

防火墙状态

项目	描述
表: Filter	显示过滤网络数据包的默认表。
表: NAT	显示修改网络数据包的源/目的 IP 地址或端口链路表。
表: Mangle	显示用于修改网络数据包内报文修改、重新封装链路表。
表: RAW	用于关闭 NAT 表上的链路连接追踪。
显示空链	显示/隐藏无规则的空链路。
复位计数器	重置所有链的流量计数。
重启防火墙	重新启动整个防火墙进程。

3.1.5 路由表

查看路由状态，包括路由表和 ARP 缓存

IPv4 路由

接口	目的网络	IPv4 网关	优先级
wan	0.0.0.0/0	192.168.48.1	0
wan	8.8.8.8	192.168.48.1	0
cellular	8.8.8.8	10.18.108.252	0
cellular	10.18.108.248/29	-	0
cellular	114.114.114.114	10.18.108.252	0
wan	114.114.114.114	192.168.48.1	0
lan	192.168.1.0/24	-	0
wan	192.168.48.0/24	-	0

ARP

IPv4 地址	MAC 地址	接口
192.168.48.205	F4:8E:38:F0:47:26	wan

IPv4/IPv6 路由

项目	描述
接口	显示路由出路接口。
目的地址	显示目标主机或目标网络的 IP 地址和网络掩码。
IPv4/IPv6 网关	显示从中发送数据包的网关的 IP 地址。
优先级	指示接口使用优先级的指标编号。

ARP

项目	描述
IPv4 地址	显示 ARP 池的 IP 地址。
MAC 地址	显示 IP 地址对应的 MAC 地址。
接口	显示 ARP 的绑定接口。

IPv6 网上邻居

项目	描述
IPv6 地址	显示 IPv6 网上邻居的 IP 地址。
MAC 地址	显示 SIP 地址对应的 MAC 地址。
接口	显示网上邻居的绑定接口。

3.1.6 VPN

在该页可以查看 VPN 运行状态

状态	VPN
概览	
蜂窝网络	
GPS	
防火墙	
路由表	
VPN	
网络	
VPN	
工业	
系统	

VPN				
客户端				
名称	状态	本地IP	远端IP	
尚无任何配置				
IPsec 服务器				
状态	服务器IP	已连接客户端IP		
尚无任何配置				
OpenVPN 服务器				
状态	服务器IP	已连接客户端IP		
尚无任何配置				

VPN 状态

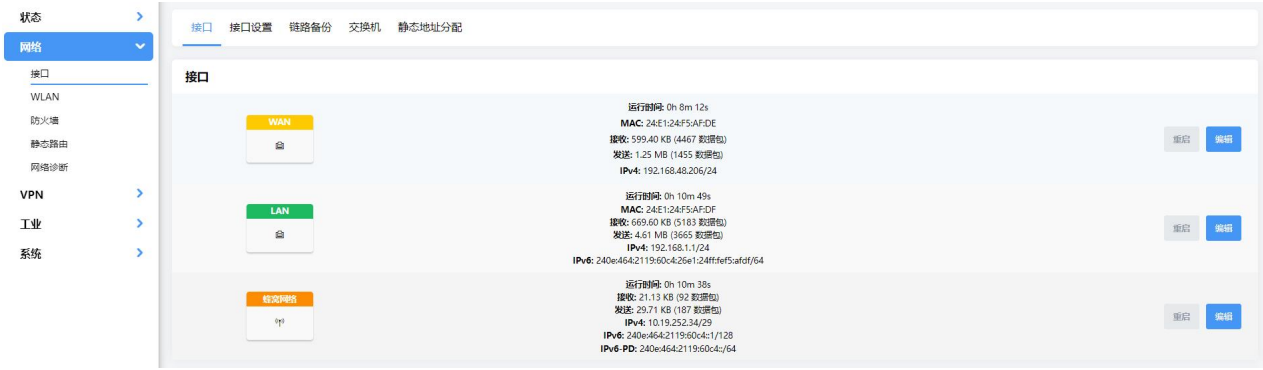
项目	描述
客户端	
名称	显示已经启用的 VPN 客户端的名称。
状态	显示开启的客户端是否与服务器连接。“已连接”表示客户端已连接上服务器。“已断开”表示客户端不再连接服务器。
本地 IP	显示路由器的 IP 地址。
远端 IP	显示隧道的远端真实 IP 地址。
IPsec/OpenVPN 服务器	
状态	显示服务器的状态。
服务器 IP	显示服务器 IP 及 VPN 的隧道 IP
已连接客户端 IP	显示连接到服务器的客户端的 IP 地址。

3.2 网络

3.2.1 接口

在此菜单可以配置蜂窝、WAN 和 LAN 接口的基本设置。

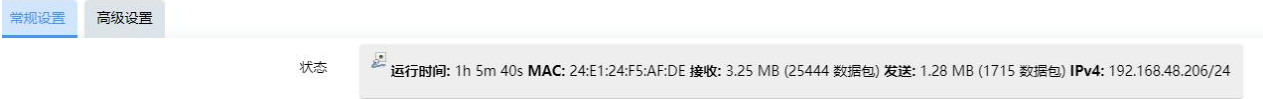
3.2.1.1 接口



端口	
项目	描述
链路优先级	
重启	显示该链路的优先级，越靠前优先级越高
编辑	显示该链路是否启用
全局网络选项	
IPv6 ULA 前缀	
fd21:79aa:79b5::/48	
全局网络选项	
IPv6 ULA 前缀	显示此设备的 IPv6 唯一本地地址（ULA）前缀。

3.2.1.1.1 WAN

- WAN 口可以用网线连接上网。它支持 3 种连接类型，可以同时使用 IPv4 和 IPv6。
- **静态 IP**：配置以太网 WAN 接口的 IPv4 地址、网络掩码和网关。
 - **DHCP 客户端**：将以太网 WAN 接口配置为 DHCP 客户端以自动获取 IPv4 地址。
 - **PPPoE**：将以太网 WAN 接口配置为 PPPoE 或 PPPoEv6 客户端。



WAN-状态	
项目	描述
运行时间	显示 WAN 口运行的时间。
MAC	显示 WAN 口的 MAC 地址。
接收	显示 WAN 口接收的数据包和数据量。
发送	显示 WAN 口发送的数据包和数据量。
IPv4	显示 WAN 口的 IPv4 地址

1. 静态地址

本节介绍如何配置蜂窝网络的相关参数。

协议	静态地址
IP 类型	IPv4
IPv4 地址	192.168.48.206
IPv4 子网掩码	255.255.255.0
IPv4 网关	192.168.48.1
首选IPv4 DNS服务器	114.114.114.114
备选IPv4 DNS服务器	8.8.8.8

静态地址-常规设置		
项目	描述	默认值
IP 类型	固定为 IPv4 地址。	IPv4
IPv4 地址	设置 WAN 口的 IPv4 地址。	--
IPv4 子网掩码	设置 WAN 端口的网络掩码。	255.255.255.0
IPv4 网关	设置 WAN 口 IPv4 地址的网关。	--
首选 IPv4 DNS 服务器	设置主 IPv4 DNS 服务器。	114.114.114.114
备选 IPv4 DNS 服务器	设置辅助 IPv4 DNS 服务器。	8.8.8.8

2. DHCP 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。

常规设置	高级设置
状态	 运行时间: 4h 43m 32s MAC: 24:E1:24:F5:AF:DE 接收: 10.18 MB (79129 数据包) 发送: 1.40 MB (2634 数据包) IPv4: 192.168.48.206/24
协议	DHCP 客户端

接口 » WAN

常规设置 高级设置

自动获取DNS服务器

☒

最大传输单元(MTU)

1500

DHCP 客户端-高级设置

项目	描述
自动获取 DNS 服务器	自动获取对端 DNS。当访问域名时需要 DNS。
最大传输单元 (MTU)	设置最大传输单位。设置范围：68-1500。

3. PPPoE/PPPoEv6

PPPoE 是指以太网上的点对点协议。如果启用 IPv6，路由器可以获得 IPv4 和 IPv6 地址。

接口 » WAN

常规设置 高级设置

状态

运行时间: 4h 58m 27s MAC: 24:E1:24:F5:AF:DE 接收: 10.18 MB (79129 数据包) 发送: 1.40 MB (2634 数据包) IPv4: 192.168.48.206/24

协议

PPPoE

PAP/CHAP 用户名

PAP/CHAP 密码

PPPoE-常规设置

项目	描述
PAP/CHAP 用户名	输入互联网服务供应商提供的用户名。
PAP/CHAP 密码	输入互联网服务供应商提供的密码。

接口 » WAN

常规设置 高级设置

获取 IPv6 地址

启用

在 PPP 链路上启用 IPv6 协商

自动获取DNS服务器

☒

最大重试次数

9

心跳间隔

60

秒

最大传输单元(MTU)

1500

PPPoE-高级设置	
项目	描述
获取 IPv6 地址	在 PPP 链路上启用 IPv6 。
自动获取 DNS 服务器	PPP 拨号时自动获取对端 DNS。 访问域名需要 DNS。
最大重试次数	设置拨号失败后的最大重试次数。 范围：0-9。
心跳间隔（秒）	设置链路检测的心跳间隔。 范围：1-600。
传输单元（MTU）	设置最大传输单位。 范围：68-1500。

3.2.1.1.2 LAN/DHCP 服务器

接口 » LAN

常规设置

高级设置

DHCP服务器

状态

运行时间: 5h 16m 9s MAC: 24:E1:24:F5:AF:DF 接收: 3.46 MB (27167 数据包) 发送: 36.82 MB (23700 数据包) IPv4: 192.168.1.1/24 IPv6: 240e:466:21c3:bfb8:26e1:24ff:fe5:afdf/64

IPv4 地址

192.168.1.1

IPv4 子网掩码

255.255.255.0

IPv6 前缀长度

64

将每个公共 IPv6 前缀的给定长度部分分配给此接口

IPv6 前缀标识

0

将此十六进制子ID前缀分配给此接口。

LAN-常规设置	
项目	描述
状态	运行时间： 显示该端口运行了多长时间。
	MAC： LAN 接口的 MAC 地址。
	接收： 该接口接收到的数据量和包数。
	发送： 该接口发送的数据量和包数。
	IPv4/IPv6： LAN 接口的 IPv4/IPv6 地址。
IPv4 地址	设置 LAN 接口的 IPv4 地址。
IPv4 网络掩码	设置 LAN 接口的网络掩码。
IPv6 前缀长度	将每个公共 IPv6 前缀的给定长度的一部分分配给此接口。
IPv6 前缀标识符	使用此接口的十六进制子前缀 ID 分配前缀部分。

接口 » LAN

常规设置

高级设置

DHCP服务器

最大传输单元(MTU)

1500

LAN-高级设置

项目	描述
----	----

最大传输单元 (MTU)	设置最大传输单位。 设置范围：68-1500。
--------------	-------------------------

基本设置

启用 ☒

开始地址 192.168.1.100

结束地址 192.168.1.199

IPv4 租期 1440 分

IPv4 子网掩码 255.255.255.0

DNS服务器 192.168.1.1

+

DHCP 服务器-基本设置

项目	描述
----	----

启用	启用/禁用此接口 DHCP 服务器。
----	--------------------

开始地址	设置 DHCP 客户端自动获取的 IP 地址池的起始地址。
------	-------------------------------

结束地址	设置 DHCP 客户端自动获取的 IP 地址池的结束地址。
------	-------------------------------

IPv4 租期	设置租用地址的到期时间，最小为 2 分钟（2m）。
---------	---------------------------

IPv4 子网掩码	设置客户端的子网掩码，通常是根据所服务子网计算。
-----------	--------------------------

DNS 服务器	设置客户端 DNS 服务器列表。
---------	------------------

IPv6 设置

启用	☒
路由通告服务	服务器模式
DHCPv6 服务	服务器模式
DHCPv6 模式	无状态的
通告的 DNS 服务器	+

DHCP 服务器-IPv6 设置	
项目	描述
启用	使用蜂窝 IPv6 或 PPPoE v6 时选择启用 DHCPv6 服务器。
路由通告服务	固定为服务器模式。
DHCPv6 服务	固定为服务器模式。
DHCPv6 我是	固定为无状态模式。
通告的 DNS 服务器	设置客户端 DNS 服务器列表。

3.2.1.1.3 蜂窝网络

本节介绍如何配置蜂窝网络的相关参数。

UR75 蜂窝路由器支持双卡备份，一次只有一张 SIM 卡处于激活状态，同时启用两个蜂窝接口时，默认 SIM1 优先。典型的用例是将 SIM1 配置为主蜂窝接口，将 SIM2 配置为备份。当 SIM1 无法连接网络时，将自动切换到 SIM2 作为网络出口。

选择SIM卡	SIM1
未填写则使用SIM卡中自带默认配置	
IP 类型	IPv4/IPv6
接入点	
PIN码	
认证类型	NONE
网络类型	自动
允许漫游	☒
最大传输单元(MTU)	1500
最大可用流量	MB
清算日	1日
蜂窝频段	5G NR 频段: N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78 LTE频段: B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43

蜂窝网络	
项目	描述
选择 SIM 卡	选择需要配置的 SIM 卡。
协议类型	选择协议类型 “IPv4” , “IPv6” , “IPv4/IPv6”
接入点	输入由本地互联网服务提供商提供的蜂窝网络拨号连接的接入点。
PIN 码	输入用于解锁 SIM 卡的 PIN 代码, 4-8 位。
认证类型	可选 “NONE” 、 “PAP” 、 “CHAP” 、 “PAP/CHAP” 。
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” 。 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。
允许漫游	勾选开启漫游功能后路由器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
最大传输单元 (MTU)	设置最大传输单元，范围：68-1500
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
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
蜂窝频段	选择用于注册蜂窝网络的 5G NR 和 4G LTE 频段。可用于通过选择特定频段来优化蜂窝速度。

3.2.1.2 接口设置

本节介绍如何配置以太网端口参数。

UR75 蜂窝路由器支持 1 个 WAN 端口和 4 个 LAN 端口。

接口设置

接口	状态	属性	接口速率	接口模式
LAN1	Up	LAN	Auto	Auto
LAN2	Up	LAN	Auto	Auto
LAN3	Up	LAN	Auto	Auto
LAN4	Up	LAN	Auto	Auto
WAN	Up	WAN	Auto	Auto

接口设置

项目	描述
接口	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。
接口速率	设置以太网口速率，固定 auto。
接口模式	设置以太网口模式，固定 auto。

3.2.1.3 链路备份

本节介绍如何配置链路备份策略、优先级和 ping 设置，默认情况下每条链路都有自己的 ping 规则。路由器会根据优先级选择下一个可用的接口上网。使用前请确保您已启用此处需要使用的链路接口。如果优先级 1 只能使用 IPv4，则 UR75 将选择 IPv6 作为主 IPv6 链路的第二条链路，反之亦然。

链路优先级

开启链路备份功能后，若检测到当前链路不可用，将自动切换到下一个链路
表格从上到下，优先级从高到低

优先级	启用规则	当前链路	接口	连接类型	IP		
1	☒		WAN	静态地址	192.168.48.206		编辑
2	☒		Cellular-SIM1	DHCP 客户端	100.115.251.117/29 240e:466:2154:878::1/128		编辑
3	☒		Cellular-SIM2	DHCP 客户端	-		编辑

设置

恢复至高优先级链路

☒

勾选后，定时探测高优先级链路是否能ping通，若可以，则切换至优先级更高的链路

恢复间隔

180

秒

链路异常则重启

☐

启用后，若检测到所有接口都无法正常使用，系统将会进行重启

链路备份	
项目	描述
链路优先级	
优先级	显示各个接口的优先级，越靠前优先级越高。可以通过长按 上下拖动修改链路优先级。
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。
	长按拖动此按钮可调整网络链接的优先级。 列表顶部的优先级最高。
编辑	单击可编辑每个网络链接的 ping 探测设置。
设置	
恢复至高优先级链路	启用后，系统将周期性检测是否能 ping 通高优先级链路，若能 ping 通则切换优先级高的链路。
恢复间隔	显示切换到优先级更高的链路的等待秒数，范围：1 - 21600s。。

链路异常则重启	启用后，如果没有任何链接可用，启用重启设备。
---------	------------------------

启用 ☒

关闭时，默认ping探测通过

目的地址(IPv4)

备选目的地址(IPv4)

目的地址(IPv6)

备选目的地址(IPv6)

Ping间隔 秒

Ping重试间隔 秒

Ping超时 秒

最大重试次数

Ping 探测	
项目	描述
启用	启用链路 Ping 探测后，路由器会阶段性探测链路的连接状态。
目的地址 (IPV4/IPv6)	路由器 ping 主地址/域名来检测当前连接是否存在。
备选目的地址 (IPV4/IPv6)	路由器 ping 备用地址/域名来检测当前连接是否存在。
Ping 间隔	路由器每隔一个 Ping 间隔对目的地址进行 Ping 探测
Ping 重试间隔	当 Ping 失败后，路由器每隔一个 Ping 重试间隔再重新 Ping
Ping 超时	发送 Ping 命令后等待应答的超时时间
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

3.2.1.4 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。

VLAN

启用 ☒

VLAN设置

VLAN ID	LAN 1	LAN 2	LAN 3	LAN 4	CPU	
5	Tagged	Tagged	Tagged	Tagged	Tagged	删除
						添加

局域网设置

名称	VLAN ID	IP地址	子网掩码	最大传输单元(MTU)	
test	5	192.168.3.1	255.255.255.0	1500	删除

DHCP服务器

名称	接口	地址	IPv4 租期	IPv4 子网掩码	
DHCP_3	test	开始地址: 192.168.3.100 结束地址: 192.168.3.199	1440分	255.255.255.0	编辑

交换机	
项目	描述
VLAN	设置 VLAN 功能的开关
VLAN 设置	
VLAN ID	用户自定义 VLAN 的标签 ID，合法值：3-4094。
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。
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（MTU）	设置 LAN 口的最大传输单元。合法值：68-1500。

启用 ☒

接口

开始地址

结束地址

IPv4 租期 分

IPv4 子网掩码

DNS服务器

DHCP 服务器-基本设置	
项目	描述
启用	启用/禁用此 VLAN 接口 DHCP 服务器，只有删除相应局域网才能删除此 DHCP 服务器。
接口	显示 DHCP 服务器的 VLAN 接口名称。
开始地址	设置 DHCP 客户端自动获取的 IP 地址池的起始地址。
结束地址	设置 DHCP 客户端自动获取的 IP 地址池的结束地址。
IPv4 租期	设置租用地址的到期时间，最小为 2 分钟（2m）。
IPv4 子网掩码	设置客户端的子网掩码，通常是根据所服务子网计算。
DNS 服务器	设置客户端 DNS 服务器列表。

3.2.1.5 静态地址分配

当 LAN/VLAN 接口作为 DHCP 服务器时，用户可以为具有固定 MAC 地址的设备分配固定的 IP 地址和符号主机名。

静态地址分配

静态租约用于给 DHCP 客户端分配固定的 IP 地址和主机标识。只有指定的主机才能连接，并且接口须为非动态配置。
使用添加按钮来增加新的租约条目。IPv4 地址和主机名字段的值将被固定分配给MAC 地址字段标识的主机，租期是一个可选字段，可为每个主机单独设定 DHCP 租期的时长。

主机名

MAC 地址

IPv4 地址

IPv4 租期

分

删除

添加

保存

保存并应用

项目	描述
主机名	设置静态租约的主机名。
MAC 地址	设置 DHCP 客户端的 MAC 地址。
IPv4 地址	设置分配给客户端的 IPv4 地址。
IPv4 租期	设置客户端的剩余时间。

3.2.2 WLAN（仅 Wi-Fi 版本）

本节介绍如何配置 Wi-Fi 的相关参数。 UR75 支持 2.4G 和 5G Wi-Fi 同时工作。

启用☒

接口类型

接入点

BSSID

24:e1:24:f5:af:e0

射频类型

802.11bgn/ax mixed

信道

Auto

无线频宽

40 MHz

SSID

Router_F5AFE0_2.4G

加密模式

WEP 开放式系统

密钥

SSID广播☒

AP隔离☐

最大客户端数目

128

MAC地址过滤☒

类型

白名单

MAC 地址

描述

尚无任何配置

WLAN	
项目	描述
启用	启用/禁用 WLAN 功能。
接口类型	WLAN 工作类型，固定“接入点”。
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。
射频类型	选择射频类型。
信道	选择无线信道，可选“Auto”、“1”、“2”……“13”。
无线频宽	选择无线频宽，可选“20MHz”、“40MHz”和80MHz（5G）。
SSID	填入接入点 SSID。
加密模式	选择加密方式，可选“无加密”、“WEP 开放式系统”、“WEP 共享秘钥”、“WPA-Auto”、“WPA-PSK”、“WPA2-PSK”、“WPA3-PSK”、“WPA-PSK/WPA2-PSK”、“WPA2-PSK/WPA3-PSK”。
密钥	填写接入无线网络的密钥。
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。
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。
MAC 地址过滤	
MAC 地址过滤	启用或禁用 Wi-Fi 客户端 MAC 地址的过滤器。
MAC 地址	白名单：只允许设置的 MAC 地址连接到路由器的无线接入点。 黑名单：设置的 MAC 地址不允许连接到路由器的无线接入点。

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、自定义规则。

3.2.3.1 常规设置

安全配置

启用 SYN-flood 防御 ☒

默认使用 HTTPS 登陆 ☒

访问控制

名称	端口	本地访问	远程访问
HTTP	80	☒	☒
HTTPS	443	☒	☒
SSH	22	☒	☒
TELNET	23	☒	☒

网址过滤

域名关键字过滤

请输入域名中的关键字

+

例：如需过滤www.google.com，请输入google

项目	描述
安全配置	
启用 SYN-flood 防御	启用/禁用 SYN-flood 防御。
默认使用 HTTPS 登陆	启用/禁用默认使用 HTTPS 登陆。
访问控制	
端口号	设置相应服务的端口号。合法值：1-65535。
本地访问	设置本地连接路由器
远程访问	设置远程访问路由器
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。
HTTPS	用户在勾选该选项之后可以通过 HTTPS 本地或远程登录设备，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。
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。
网页过滤	

域名关键字过滤	通过设置域名中的关键字来阻止特定网站。过滤后，LAN 口下的设备无法访问相应的网站。 允许的最大字符数为 64。
---------	--

3.2.3.2 ACL 规则

ACL 规则，也称为访问控制列表，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。当路由器收到报文时，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。

ACL规则

默认处理策略

接受

规则优先级: DMZ>端口映射>访问控制>ACL规则

列表优先级: 表格从上到下, 优先级从高到低

名称	匹配规则	动作	启用
test	转发 IPv4 协议 TCP, UDP, ICMP 来自 WAN/WAN, Cellular IP 0.0.0.0/0 到 LAN IP 192.168.3.0/24	丢弃 转发	☒

三

编辑

删除

添加

ACL 规则	
项目	描述
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。
启用	启用该条访问控制规则。
三	长按拖动可调整访问控制的优先级。
编辑	单击可进入配置编辑访问控制规则界面。
删除	删除该条访问控制规则。

名称	
IP 类型	IPv4 ▼
协议	TCP UDP ICMP ▼
源接口	WAN(WAN、Cellular) ▼
源地址类型	IP ▼
源IP地址	0.0.0.0/0 例:192.168.1.1 或 192.168.1.1/24
源端口	任意端口 可输入端口号, 或输入20~300
目的接口	LAN ▼
目的IP地址	0.0.0.0/0 例:192.168.1.1 或 192.168.1.1/24
目的端口	任意端口 可输入端口号, 或输入20~300
动作	接受 ▼

项目	描述
访问控制	
名称	为该 ACL 规则定义一个唯一名称。
IP 类型	设置类型作为 IPv4 或 IPv6。
协议	设置访问控制协议, 可选 “icmp” 、 “tcp” 、 “udp” 。
源接口	设置访问控制源接口类型。
源地址类型	设置访问控制源输出接口地址。使用 IPv4 类型时, 选择地址类型为 IP、MAC 或 IP+MAC。
源 IP 地址	输入 ACL 规则的匹配报文的源地址, 为空表示所有。(0.0.0.0/0 表示全

	部) 。
源端口	设置特定的源端口号或端口范围，例如：20-300。
目的接口	设置访问控制目的接口类型。
目的 IP 地址	设置目标网络地址（0.0.0.0/0 表示全部）。
目的端口	设置特定的源端口号或端口范围，例如：20-300。
动作	选择满足条件操作，接受或丢弃。

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（如路由器或防火墙）时将通信请求从地址和端口号的组合重定向到另一个。

端口映射(DNAT)

内部需要提供对外服务时（如对外发布web网站），外部地址发起主动连接，由路由器或者防火墙上网关接收这个连接，然后将连接转换到内部，此转换称为DNAT，主要用于内部服务对外发布。
列表优先级：表格从上到下，优先级从高到低

名称	协议	外部IP地址	外部端口	内部IP地址	内部端口	启用
test	TCP UDP	0.0.0.0/0	8080	192.168.1.1	6000	☒

三

删除

添加

端口映射	
项目	描述
名称	设置对该条映射规则的名。
协议	根据应用从“TCP”、“UDP”、“Both”中选择协议。
外部 IP 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。
外部端口	输入外网访问路由器的对外端口号或端口号范围。合法值：20-300。
内部 IP 地址	输入把数据转发到内网的设备的 IP 地址。
内部端口	输入在传入端口上接收后转发的数据包 TCP 或 UDP 端口。
启用	启用或禁用此端口映射规则。
三	拖动该按钮可以调整端口映射规则的优先级。 列表顶部的优先级最高。
删除	删除这条规则。

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。

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。启用DMZ后，路由器收到的所有来源为`源IP地址`的数据，都会转发到所填写的`DMZ主机IP地址`。

☒ 启用

DMZ 主机IP地址

源IP地址

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。

3.2.3.5 自定义规则

自定义规则指通过设置 lux 指令来自定义防火墙规则。

防火墙 - 自定义规则

自定义规则允许您执行防火墙的iptables命令，请注意使用URL过滤命令无法生效。

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule
```

3.2.3.6 证书

在此页面中，您可以导入用于路由器 Web GUI 安全访问的 HTTPS 证书。

HTTPS证书

证书		浏览	导出	删除
密钥		浏览	导出	删除

3.2.4 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。

静态 IPv4 路由

接口	目的网络	IPv4 子网掩码	IPv4 网关	优先级	最大传输单元(MTU)
尚无任何配置					

添加

静态 IPv6 路由

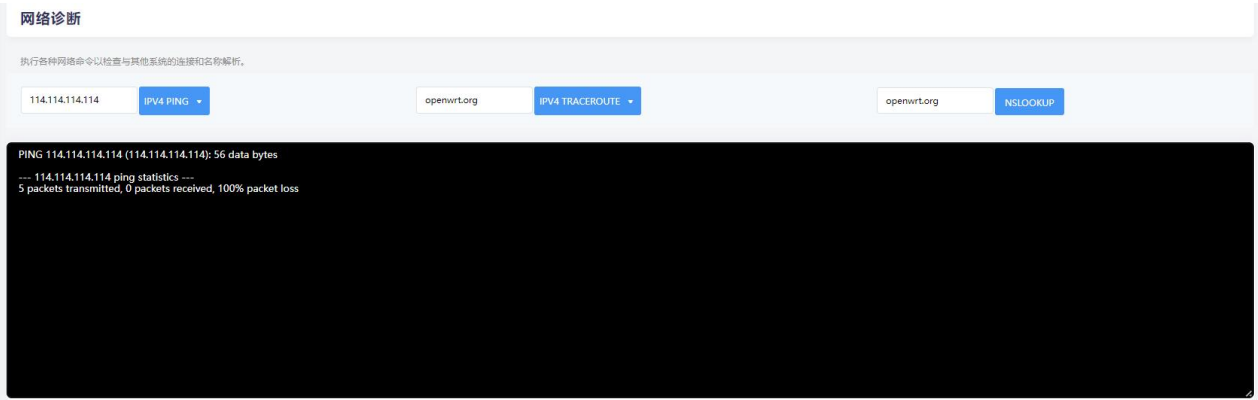
接口	目的网络	IPv6 网关	优先级	最大传输单元(MTU)
尚无任何配置				

添加

静态路由	
项目	描述
接口	数据到达目的网络使用的接口。
目的网络	输入需要到达的目的 IPv4/IPv6 地址。
IPv4 子网掩码	输入需要到达的目的地址的子网掩码/前缀长度。
IPv4/IPv6 网关	输入数据在到达目的地之前，需要经过的下一个路由器 IPv4/IPv6 地址。
优先级	即优先权，数值越小优先级越高。合法值：1-255。
最大传输单元（MTU）	设置最大传输单位。 范围：68-1500。

3.2.5 网络诊断

网络诊断包括 IPv4/IPv6 ping、IPv4/IPv6 traceroute、nslookup 命令行工具。



网络诊断	
项目	描述
IPv4 Ping	单击以从 IPv4 中的设备 ping 外部网络。
IPv6 Ping	单击以从 IPv6 中的设备 ping 外部网络。
IPv4 Traceroute	IPv4 中要检测的目的主机地址。
IPv6 Traceroute	IPv6 中要检测的目的主机地址。
Nslookup	点击获取域名与 IP 地址的映射关系，或其他 DNS 记录。

3.3 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。

3.3.1 OpenVPN

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。UR75 的默认 OpenVPN 版本是 2.5.3。

3.3.1.1 OpenVPN 服务器

启用

☒

配置方式

文件配置

配置文件

浏览

编辑

导出

删除

OpenVPN 服务器 - 文件配置

项目	描述
浏览	单击以浏览服务器配置 ovpn 格式文件，包括设置和证书内容。 请根据示例参考服务器配置文件： server.conf
编辑	单击以编辑导入的配置文件。
导出	导出服务器配置文件。
删除	单击删除配置文件。

启用

☒

配置方式

界面配置

▼

协议

UDP

▼

端口

1194

监听IP

网络接口

tun

▼

认证类型

无

▼

本地IP

10.8.0.1

远程IP

10.8.1.1

精简模式

LZO

▼

Ping 间隔

60

秒

Ping 重试

300

秒

加密模式

无

▼

最大传输单元(MTU)

1500

最大帧长

1500

日志级别

注意

▼

专家选项

账户

用户名	密码
尚无任何配置	

添加账户

本地路由

子网	子网掩码
尚无任何配置	

添加路由

客户端子网

名称	子网	子网掩码
尚无任何配置		

添加子网

OpenVPN 服务器-界面配置

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。
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。
账户	
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。
本地路由	
子网	设置本地路由的 IP 地址。
子网掩码	设置本地路由的网络掩码。
客户端子网	
名称	设置 OpenVPN 客户端证书名称。
子网	设置 OpenVPN 客户端的子网。
子网掩码	设置 OpenVPN 客户端的子网掩码。

3.3.1.2 OpenVPN 客户端

UR75 最多支持同时运行 3 个 OpenVPN 客户端。您可以直接导入 ovpn 文件,也可以在此页面配置参数来设置客户端。

客户端_1

启用

☒

配置方式

文件配置

配置文件

openvpn-custom-client1.conf

浏览

编辑

导出

删除

OpenVPN 客户端 - 文件配置	
项目	描述
浏览	单击以浏览选择客户端配置 ovpn 格式文件, 包括设置和证书内容。 请根据示例参考服务器配置文件: client.conf
编辑	单击以编辑导入的配置文件。
导出	导出配置文件。
删除	单击删除配置文件。

启用 ☒

配置方式 界面配置

协议 UDP

端口 1194

远端地址

网络接口 tun

认证类型 无

本地IP

远端IP

精简模式 LZO

Ping 间隔 60 秒

Ping 重试 300 秒

加密模式 无

最大传输单元(MTU) 1500

最大帧长 1500

日志级别 注意

专家选项

本地路由

子网

子网掩码

尚无任何配置

OpenVPN 客户端-界面配置	
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。
端口	输入远端 OpenVPN 服务器的监听端口。合法值：1-65535。
远端 IP 地址	输入远端 OpenVPN 服务器 IP 地址或域名。
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。
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端匹配。
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。每个字符串用分号分开。
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。

3.3.1.3 证书

在使用 OpenVPN 服务器或客户端的页面配置时，用户可以根据认证类型导入/导出必要的证书和密钥文件到该页面。

服务器

CA证书		浏览	导出	删除
证书		浏览	导出	删除
私钥		浏览	导出	删除
DH		浏览	导出	删除
TA		浏览	导出	删除
证书吊销列表		浏览	导出	删除
预共享密钥		浏览	导出	删除

客户端_1

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

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。
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。

3.3.2 IPSec

3.3.2.1 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 用于密钥交换。所有这些都保护主机之间、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。

启用 ☒

IPsec模式 隧道

IPsec协议 ESP

本地子网 192.168.1.1

本地子网掩码 255.255.255.0

本地ID类型 Default

远端子网 192.168.2.1

远端子网掩码 255.255.255.0

远端ID类型 Default

SA加密算法 AES128

SA认证算法 SHA1

PFS组 NULL

SA生存时间 3600 秒

DPD时间间隔 30 秒

IKE参数 ☐

IPsec高级 ☐

专家选项

IPsec 服务器	
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。如在工作站到路由器之间建立加密的 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。
SA 加密算法	从 “AES128” 、 “AES192” 、 “AES256” 中选择。
SA 认证算法	从 “SHA1” 、 “SHA2-256” 中选择。
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。
SA 生存时间	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	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。

IKE参数 ☒

IKE版本

协商模式

加密算法

认证算法

DH组

本地认证类型

XAUTH ☐

生存时间 秒

PSK列表

选择器	预共享密钥
尚无任何配置	

IPsec高级 ☐

专家选项

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。
时间裕度	在生存期到期之前设置提前时间以开始重新协商。
专家选项	用户可以在此字段中输入一些其他的初始化字符串以添加额外的设置, 使用分号分隔字符串。

3.3.2.2 IPSec 客户端

启用

☒

IPsec网关地址

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

SA加密算法

AES128

SA认证算法

SHA1

PFS组

NULL

SA生存时间

3600

秒

DPD时间间隔

30

秒

IKE参数

☐

IPsec高级

☐

专家选项

IPsec-客户端	
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。如在工作站到路由器之间建立加密的 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。
SA 加密算法	从“AES128”、“AES192”、“AES256”中选择。
SA 认证算法	从“SHA1”、“SHA2-256”中选择。
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。
SA 生存时间	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	设置 DPD 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。

IKE 参数 ☒

IKE 版本

协商模式

加密算法

认证算法

DH 组

本地认证类型

本地密钥

XAUTH ☐

生存时间 秒

IPsec 高级 ☒

支持压缩 ☐

时间裕度 秒

专家选项

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。
IPsec 高级	
支持压缩	点击启用后则会压缩 IP 数据包的头部。
时间裕度	在生存期到期之前设置提前时间以开始重新协商。
专家选项	用户可以在此字段中输入一些其他的初始化字符串以添加额外的设置，使用分号分隔字符串。

3.3.3 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。

启用☒

服务器IP地址

用户名

密码

认证类型

自动

全局流量转发☐

远端子网

远端子网掩码

隧道密钥

显示高级选项☒

本端隧道IP地址

对端隧道IP地址

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

专家选项

图 3.2.5.5 L2TP-1

L2TP	
项目	描述
启用	勾选后启用 L2TP 功能。
服务 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，路由器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。
隧道密钥	输入 L2TP 隧道密码。
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，服务器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。
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。

3.3.4 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。

启用	☒
服务器IP地址	
用户名	
密码	
认证类型	MS-CHAP
全局流量转发	☐
远端子网	
远端子网掩码	
显示高级选项	☒
本端隧道IP地址	
对端隧道IP地址	
启用MPPE	☐
地址/控制压缩	☐
协议字段压缩	☐
Asyncmap值	ffffff
最大接收单元(MRU)	1440
最大传输单元(MTU)	1440
链路检测间隔时间	60 秒
最大重试次数	1
专家选项	

PPTP	
项目	描述
启用	启用 PPTP 客户端。最多可建立 3 个虚拟隧道。
服务器 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，路由器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。
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。

3.4 工业

UR75 路由器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。

路由器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 串口

本节介绍如何根据与路由器相连的终端设备的串口参数设置路由器串口的参数，实现路由器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。

启用

☒

串口类型

RS485

▼

波特率

9600

▼

数据位

8 Bits

▼

停止位

1 Bits

▼

校验位

无

▼

软件流控

☐

串口模式

Modbus Master

▼

串口设置	
项目	模式
启用	启用/禁用串口功能。
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。
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"。
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"。
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。

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。
串口模式	选择串口的工作模式，可选“DTU”、“Modbus Master”、“GPS”。 DTU：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。

串口模式

DTU 协议

保活间隔 秒

保活重试次数

重连间隔 秒

指定协议 ☐

串口分帧长度 字节

串口分帧间隔 毫秒

注册包内容

目的IP地址

服务器地址	服务器端口	状态
尚无任何配置		

DTU 设置	
项目	描述
DTU 协议	从以下协议中选择： TCP Client：路由器作为 TCP 客户端，向 TCP 服务器透传数据。 UDP Client：路由器作为 UDP Client，向 UDP Server 透传数据。 TCP 服务器：路由器作为 TCP 服务器等待轮询数据。 UDP 服务器：路由器作为 UDP 服务器等待轮询数据。 Modbus：路由器将作为 Modbus 网关，实现 Modbus RTU 和 Modbus TCP 之间的转换。
TCP/UDP 服务器	
本地端口	设置 TCP 服务器的本地端口。合法值：1-65535。
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。
保活重试次数	TCP 心跳超时后，路由器重发送心跳包，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。
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。
串口分帧间隔（毫秒）	路由器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。
TCP/UDP 客户端	
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。
保活重试次数	TCP 心跳超时后，路由器重发送心跳包，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。
重连间隔（秒）	设置客户端连接失败时，重连服务器的时间间隔。合法值 10-60s。
指定协议	设置协议格式，路由器将能够使用特定协议连接到 TCP2COM 软件。
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。
串口分帧间隔（毫秒）	路由器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。
注册包内容	设置注册包内容，设备连接服务器成功后将会发送该内容至服务器中
服务器地址	设置 TCP/UDP 服务器地址。
服务器端口	设置 TCP/UDP 服务器端口。合法值：1-65535。
状态	显示与所设置服务器的连接状态。
Modbus	
本地端口号	设置路由器监听端口。合法值：1-65535。
最大 TCP 客户端数目	设置充当路由器作为 TCP 服务器时，连接的 TCP 客户端的最大数量。
连接超时时间	设置连接超时时间，当路由器作为 TCP 服务器时，连接超时期限内没有从设备接收到任何数据，则 TCP 连接将断开。
读取间隔	设置读取远程通道的时间间隔。 当一个读取周期结束时，新的读取周期开始，直到该间隔期满。 如果它设置为 0，则设备将在读取所有频道后重新启动新的读取周期
响应超时时间	设置路由器等待命令响应的最大响应时间。 如果设备在最大响应时间

	后仍未得到响应，则确定该命令已超时。
最大重试次数	设置读取失败后的最大重试次数。

3.4.2 I/O

3.4.2.1 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。

启用

☒

模式

高电平

▼

持续时间

100

毫秒

动作

☐ DO

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	选择当数字输入满足预设模式的触发条件或时间后作出的动作。 DO： 勾选启用 DI 触发控制 DO 输出状态。

3.4.2.2 数字输出

本节介绍如何配置数字输出。

启用	☒
模式	脉冲
初始状态	高电平
高电平持续时间	100 *10 毫秒
低电平持续时间	100 *10 毫秒
脉冲个数	10

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，同时也是路由器重启后 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。

3.4.3 Modbus Master

UR75 路由器设置为 Modbus Master 来轮询远程 Modbus Slave 并发送至 TCP 服务器。

3.4.3.1 Modbus Master

在该界面可以配置 Modbus Master 的参数。

启用 ☒

读取间隔 秒

最大重试次数

最大响应时间 毫秒

命令间隔时间 毫秒

通道

Modbus Master		
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
命令间隔时间 (毫秒)	每个指令之间的执行间隔。合法值：10-1000。	50
通道	选择一个可读取的远程通道。	--

3.4.3.2 通道设置

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

通道设置

名称	Slave ID	寄存器地址	数目	指令类型	链路类型	远端设备IP	端口	有符号	小数位	
	1	0	1	保持寄存器 (INT16)	TCP			☐	0	删除
										添加

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。
寄存器地址	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	设置链路类型，可选类型“TCP”、“串口 1”、“串口 2”。
远端设备 IP	设置远端 Modbus 设备 IP 地址。
端口	设置远端 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。

TCP转发

名称	IP	端口
尚无任何配置		

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

3.4.4 GPS

本节详细介绍 GPS 设置，包括 GPS IP 转发和 GPS 串行转发。

3.4.4.1 GPS

用户可以在该页面启用 GPS 功能。勾选启用 GPS 日志后，系统将会打印跟多 GPS 相关的调试日志。



3.4.4.2 GPS IP 转发

GPS IP 转发意味着 GPS 数据可以通过互联网转发。

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
重连间隔	10 秒
上报信息间隔	30 秒
稳定上报间隔	120 秒
稳定判定阈值	25 米
包含RMC信息	☒
包含GSA信息	☒
包含GGA信息	☒
包含GSV信息	☒
包含VTG信息	☒
消息前缀	
消息后缀	

目的地址

服务器地址	服务器端口	状态
尚无任何配置		

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	选择路由器的连接类型。 选项是 “客户端” 和 “服务器” 。	客户端
协议	选择数据传输协议。 选项是 “TCP” 和 “UDP” 。	TCP 协议

保活间隔 (秒)	在与服务器/客户端连接后, 路由器将定期向服务器/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, 路由器将重新发送心跳。达到预设的重试次数后, 路由器将重新连接到 TCP 服务器。合法值: 1-16。	9
本地端口	设置路由器监听端口。合法值: 1-65535。	
重连间隔 (秒)	连接失败后, 路由器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)	路由器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
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	显示路由器和服务器之间的连接状态。	--

3.4.4.3 GPS 串口转发

GPS 串口转发意味着 GPS 数据可以转发到串口。

启用

☒

串口类型

-- 请选择 --

上报信息间隔

30

秒

包含RMC信息

☒

包含GSA信息

☒

包含GGA信息

☒

包含GSV信息

☒

包含VTG信息

☒

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）	路由器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。	--
包含 VTG	是否在 GSV 数据中包含 VTG。	--

3.5 系统

本节介绍如何配置常规设置和调试，例如管理帐户、系统时间、用户管理、设备管理、下载日志等。

3.5.1 常规

主机名

Router

本地时间

2023/03/17 20:58:07

时区

UTC

时间同步

与NTP服务器同步

系统-常规设置	
项目	描述
主机名	用户可自定义路由器主机名称，以字母开头，只允许字母、数字、“-”或“_”。
本地时间	显示当前系统时间。
时区	单击下拉列表以选择您所在的时区。
时间同步	同步浏览器时间： 与浏览器同步时间。 与 NTP 服务器同步： 与 NTP 服务器同步时间。 与 GPS 时间同步： 每小时与 GPS 时间同步。确保在工业 > GPS >GPS 上启用 GPS。 手动： 手动配置时间。

作为 NTP 服务器提供服务 ☐

候选 NTP 服务器

pool.ntp.org

×

cn.pool.ntp.org

×

time.nist.gov

×

+

系统-NTP 设置	
作为 NTP 服务器提供服务	启用/禁用 NTP 服务器功能，勾选后，网络中的 NTP 客户端即可与路由器在时间上实现同步。
候选 NTP 服务器	设置 NTP 服务器地址（域名/IP）

表 3.3.1.2 系统时间-1

3.5.2 密码

在此页可以修改访问设备的管理员密码。

用户名	admin
旧密码	
新密码	
确认密码	

密码	
项目	描述
用户名	固定为 admin。
旧密码	输入旧密码验证权限。
新密码	输入新的密码。
确认密码	再次输入新密码。

3.5.3 设备管理

3.5.3.1 设备管理

星纵物联设备管理平台连接配置，用于远程管理路由器。

设备管理

状态

未连接

服务器地址

激活方式

通过授权码

授权码

连接

图 3.3.6.1 设备管理-1

设备管理	
项目	描述
状态	显示路由器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	

3.5.3.2 Cloud 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。

设置

服务器	
端口	18443
授权码	
设备名称	
连接	

状态

状态	未连接
本地IP	--
远端IP	--
连接时长	--

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	显示路由器和 Milesight VPN 的连接状态。
本地 IP	显示路由器的虚拟 IP 地址。
远程 IP	显示 Milesight VPN 的虚拟 IP 地址。
连接时长	显示路由器和 Milesight VPN 的连接时长。

3.5.4 备份还原

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

备份

点击“生成备份”下载当前配置文件的 tar 存档。

下载备份

生成备份

恢复

上传备份存档以恢复配置。要将固件恢复到初始状态，请单击“执行重置”

恢复到出厂设置

执行重置

恢复配置

上传备份...

自定义文件（证书、脚本）会保留在系统上。若无需保留，请先执行恢复出厂设置。

刷写新的固件

从这里上传一个镜像以更新正在运行的固件。

固件文件

刷写固件...

备份/升级	
项目	描述
生成备份	点击“备份”把当前配置文件备份到电脑。
执行重置	点击“Reset”使路由器恢复出厂设置。恢复出厂后，设备会重启。
上传备份	点击“浏览”从电脑选择将要导入到路由器的配置文件。点击“导入”把选中的配置文件导入到路由器。
刷写固件	在此处上传文件以进行固件替换。

3.5.5 重启

在此页面上，您可以重新启动路由器或设置路由器的重启规则。

重启设置系统

立即重启

定时重启

启用

☒

周期

每天

时间

--:--

重启	
项目	描述
立即重启	点击可以立即重启设备。
定时重启	
启用	点击启用定时重启。
周期	设置设备的重启周期。
时间	设置重启的时间点。

3.5.6 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，路由器可将所有系统日志上传到远程日志服务器，如 Syslog Watcher。

3.5.6.1 常规设置

外部系统日志服务器地址	0.0.0.0
外部系统日志服务器端口	514
外部系统日志服务器协议	UDP
Cron 日志级别	调试
AP 日志	开始
开始或停止 MD 日志	结束
MD 日志保存模式	USB
MD 日志级别	调试

日志-常规设置	
项目	描述
外部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）。
外部系统日志服务器端口	填写远程日志服务器端口。
外部系统日志服务器协议	填写远程日志服务器协议，可选 UDP，TCP。
Cron 日志级别	用户可以将日志文件存储在内存或 TF 卡中。
AP 日志	设置 AP 日志打印级别，可选“调试”、“正常”“警告”
开始或停止 MD 日志	选择开始或停止记录蜂窝模块日志。
MD 日志保存模式	选择 MD 日志的保存输出方式。
MD 日志级别	设置 MD 日志打印的级别，可选“调试”、“信息”、“注意”、“警告”、“错误”、“致命错误”、“警戒”、“紧急”。

3.5.6.2 高级设置



日志-高级设置	
项目	描述
AP 日志	
下载	点击下载记录的最新 AP 日志。
Tcpdump 日志	
开始	点击开始记录 Tcpdump 日志。
结束	点击结束记录 Tcpdump 日志。
下载	点击下载记录的 Tcpdump 日志。

3.5.7 调试

3.5.7.1 蜂窝调试

该工具可以用 AT 命令进行蜂窝调试信息。 可以通过按黑框上方常用指令进行直接执行测试操作。也可以自行输入 AT 指令，回车后即可发送给蜂窝模块。

输入您要发送给蜂窝模块的AT命令，按 Enter 执行。

Eg: AT+COPS?

AT+CSQ

AT+ECELL

AT+ERAT?

AT+EPBSEH?

AT+CREG?

AT+COPS?

清除

常用指令描述

AT+CSQ?-----获取蜂窝网络信号

AT+ECELL?-----获取当前蜂窝信息

AT+ERAT?-----获取 *RAT* 状态和网络类型

AT+EPBSEH? ----获取使用带宽

AT+CREG?-----获取网络注册状态

AT+COPS?-----获取运营商和接入点信息

3.5.7.2 防火墙调试

该工具可以使用 *iptables* 命令来检查防火墙信息。

命令

Eg: -t nat -nvL INPUT

清除

下载

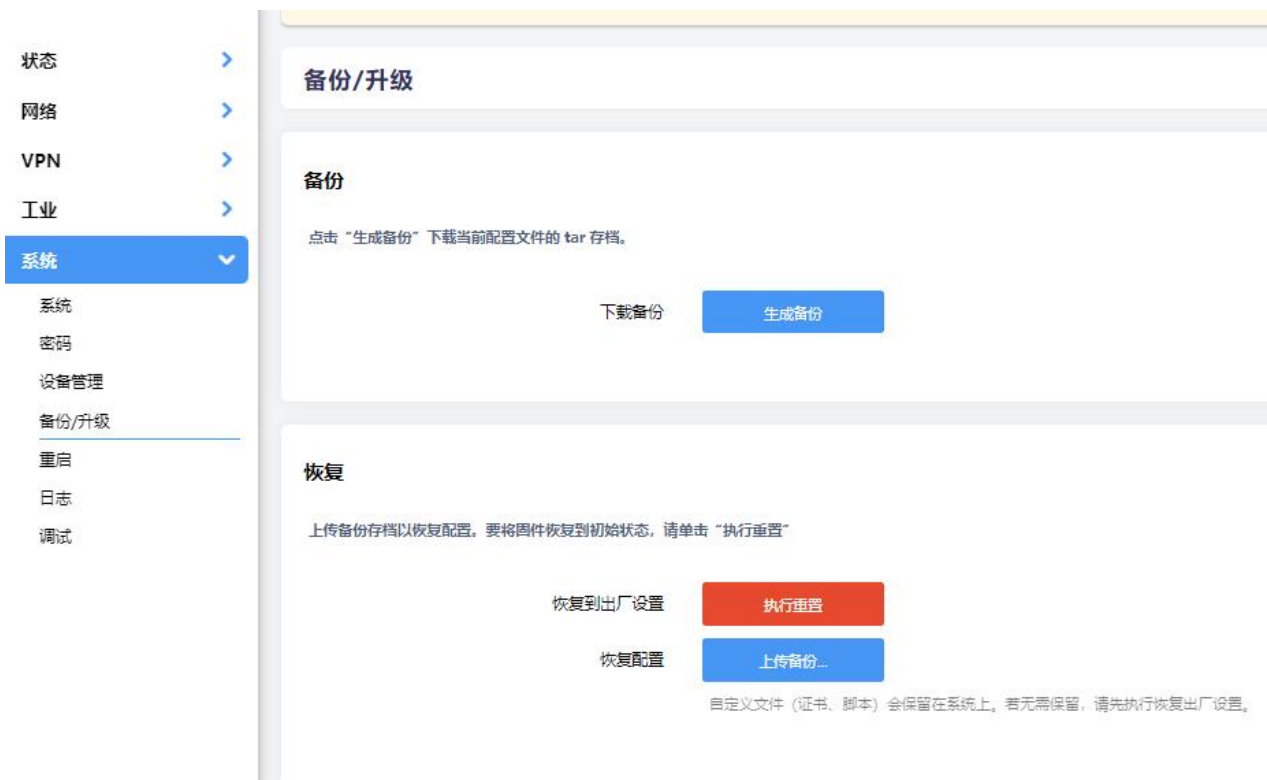
第四章 应用案例

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“系统>备份/升级”。
2. 单击“恢复”下的“执行重置”按钮。

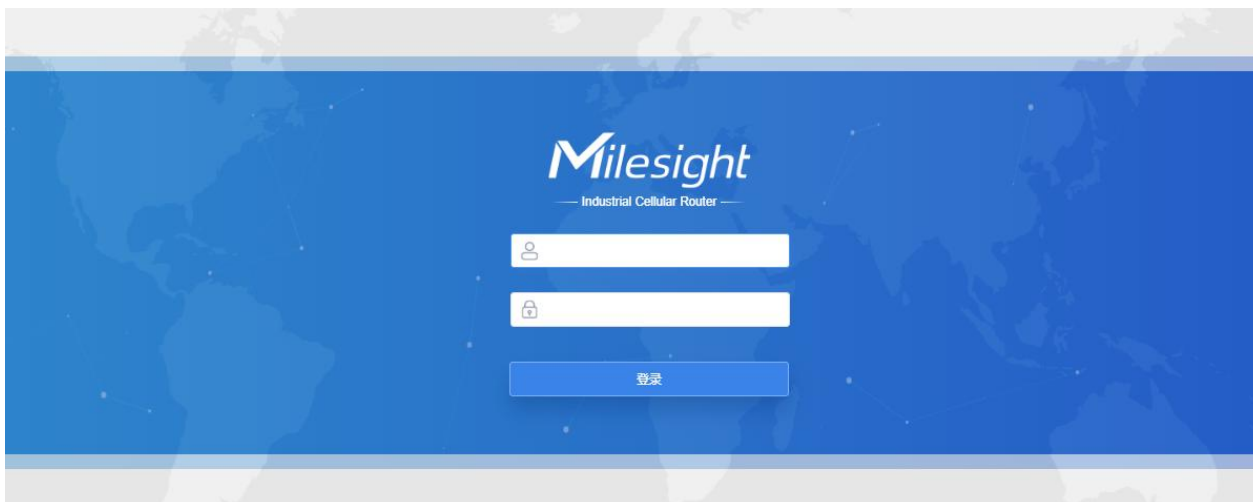
系统会询问您是否确认重置为出厂设置，然后单击“确定”按钮



然后路由器设备将重启并立即恢复出厂设置。



登录页面弹出则表示路由器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。



4.1.2 硬件上重置

找到路由器上的重置按钮，根据下表中给出的系统灯状态执行相应动作。

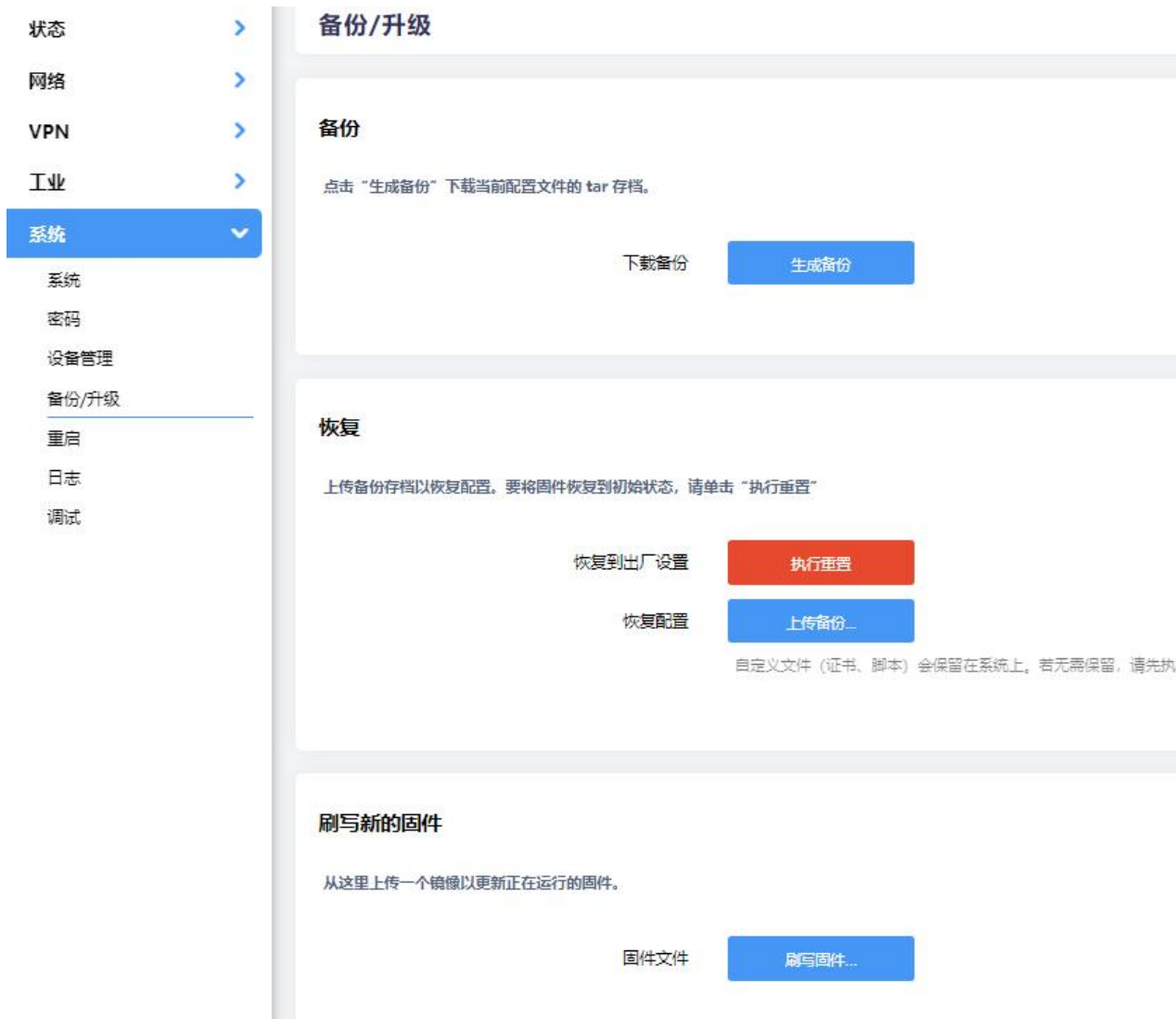
系统灯状态	动作
闪烁	长按重置按钮 15 秒以上
常亮→快速闪烁	松开按钮，等待
重新开始闪烁	路由器已恢复出厂设置

4.2 固件升级

我们建议您在升级路由器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“备份/升级”
2. 单击“刷写固件”后并单击“浏览”选择您的个人电脑上要安装的固件文件。
3. 单击“上传”，路由器将会检查固件文件是否正确。若是，导入固件后路由器将开始升级。



4.3 网络连接

4.3.1 蜂窝数据连接

UR75 路由器都有两个蜂窝接口，命名为 SIM1 和 SIM2。一次只有一个蜂窝接口可以接入使用。如果同时启用了两个蜂窝接口，则 SIM1 接口优先作为默认接口。

案例

我们将举例说明如何将 SIM 卡插入 UR75 的 SIM 2 插槽，并配置路由器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>编辑”并配置蜂窝信息。
2. 选择 SIM2。
3. 选择蜂窝网络类型，即网络访问顺序。可选“自动”、“仅 5G”、“仅 4G”、“仅 3G”。

选择SIM卡	SIM2
未填写则使用SIM卡中自带默认配置	
IP 类型	IPv4/IPv6
接入点	
PIN码	
认证类型	NONE
网络类型	自动
允许漫游	☒
最大传输单元(MTU)	1500
最大可用流量	MB
清算日	1日
蜂窝频段	5G NR 频段: N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78 LTE频段: B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43

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”查看路由器页面上的蜂窝连接状态是否连接，如果显示“Ready”，则 SIM2 已成功拨号上网。

状态	Ready
模块型号	RG500L-EU
版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
当前SIM卡	SIM2
蜂窝频段	B1
信号强度	7asu (-99dBm)
注册状态	Registered(Home network)
IMEI	869263050069412
IMSI	460115210733084
ICCID	89860321245923785509
运营商	CHN-CT
网络类型	4G
PLMN ID	46011
位置区码	5F0C
Cell ID	E0B70B

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 UR75 路由器上网。

4.3.2 以太广域网连接

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 UR75 的 WAN 口上网。

配置步骤

1. 进入“网络>接口>链路备份”然后拖动  将 WAN 口的优先及调整至最高后，单击“保存并应用”。

链路优先级

开启链路备份功能后，若检测到当前链路不可用，将自动切换到下一个链路
表格从上到下：优先级从高到低

优先级	启用规则	当前链路	接口	连接类型	IP	
1	☒		WAN	静态地址	192.168.48.206	 
2	☒		Cellular-SIM1	DHCP 客户端	-	 
3	☒		Cellular-SIM2	DHCP 客户端	240e:4662:152:147e::1/128	 

2. 进入“网络>接口>WAN>编辑”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

状态	 运行时间: 7h 5m 8s MAC: 24:E1:24:F5:AF:DE 接收: 21.00 MB (153830 数据包) 发送: 14.55 MB (16824 数据包) IPv4: 192.168.48.206/24
协议	静态地址
IP 类型	IPv4
IPv4 地址	192.168.48.206
IPv4 子网掩码	255.255.255.0
IPv4 网关	192.168.48.1
首选IPv4 DNS服务器	114.114.114.114
备选IPv4 DNS服务器	8.8.8.8

(2) DHCP 客户端

状态	 运行时间: 7h 5m 23s MAC: 24:E1:24:F5:AF:DE 接收: 21.03 MB (153998 数据包) 发送: 14.64 MB (16932 数据包) IPv4: 192.168.48.206/24
协议	DHCP 客户端

(3) PPPoE

状态	 运行时间: 7h 5m 33s MAC: 24:E1:24:F5:AF:DE 接收: 21.03 MB (154073 数据包) 发送: 14.71 MB (16987 数据包) IPv4: 192.168.48.206/24
协议	PPPoE
PAP/CHAP 用户名	
PAP/CHAP 密码	

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。

4.4 双 SIM 故障转移应用案例

案例

本节中我们将举 UR75 插有两张 SIM 卡的情况为例，当一张 SIM 拨号上网失败，路由器将尝试通过另一张 SIM 作为备用链路。

配置步骤

1. 进入“网络>接口>链路备份”启用 SIM1 和 SIM2，网络类型保持默认“Auto”不变。

网络

接口

WLAN

防火墙

静态路由

网络诊断

VPN

工业

系统

接口

接口设置

链路备份

交换机

静态地址分配

链路优先级

开启该功能后，若检测到当前链路不可用，将自动切换到下一个链路。
按照从上下下，优先级从高到低。

优先级	启用	当前链路	接口	连接类型	IP		
3	☒		Cellular-SIM2	DHCP 客户端	240e:4602:152:147e:1/128		保存
2	☒		Cellular-SIM1	DHCP 客户端	-		保存
1	☒		WAN	静态地址	192.168.48.206		保存

选择SIM卡

SIM1

未填写则使用SIM卡中自带默认配置

IP 类型

IPv4/IPv6

接入点

PIN码

认证类型

NONE

网络类型

自动

允许漫游

☒

最大传输单元(MTU)

1500

最大可用流量

MB

清算日

1日

蜂窝频段

5G NR 频段:
N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78
LTE频段:
B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43

选择SIM卡

SIM2

未填写则使用SIM卡中自带默认配置

IP 类型

IPv4/IPv6

接入点

PIN码

认证类型

NONE

网络类型

自动

允许漫游

☒

最大传输单元(MTU)

1500

最大可用流量

MB

清算日

1日

蜂窝频段

5G NR 频段:
N1,N3,N5,N7,N8,N20,N28,N38,N40,N41,N77,N78
LTE频段:
B1,B3,B5,B7,B8,B20,B28,B32,B38,B40,B41,B42,B43

然后单击“保存”和“应用”按钮。

2. 进入“状态>蜂窝”，可以看到路由器通过 SIM1 上网。

状态	Ready
模块型号	RG500L-EU
版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
当前SIM卡	SIM1
蜂窝频段	N78
信号强度	-115dBm
注册状态	Registered(Home network)
IMEI	869263050069412
IMSI	460115210733084
ICCID	89860321245923785509
运营商	CHN-CT

3. 拔出 SIM1 使路由器不能再使用 SIM1 上网。再次进入“状态>蜂窝”，可以看到路由器通过 SIM2 上网。

状态	蜂窝网络
概览	蜂窝运行状态
蜂窝网络	状态 Ready
GPS	模块型号 RG500L-EU
防火墙	版本 RG500LEUACR04A01M8G_OCPU_20.001.20.001
路由表	当前SIM卡 SIM2
VPN	蜂窝频段 B78
网络	信号强度 6asu (-101dBm)
VPN	注册状态 Registered(Home network)
工业	IMEI 869263050069412
系统	IMSI 460115210733084
	ICCID 89860321245923785509
	运营商 CHN-CT

SIM2 变成了主 SIM，而 SIM1 变成了备用。

除非 SIM2 失联，否则路由器不会再通过 SIM1 上网。

4.5 Wi-Fi 应用案例

应用案例

将 UR75 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。

启用 ☒

接口类型

BSSID

射频类型

信道

无线频宽

SSID

加密模式

SSID广播 ☒

AP隔离 ☐

最大客户端数目

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_F5AFE0_2.4G”。

4.6 NAT 应用案例

案例

UR75 路由器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。配置路由器使公共网络访问服务器。

配置步骤

进入“网络>防火墙>端口映射”配置端口映射参数。

端口映射(DNAT)

内部需要访问对外服务时（如对外发布web网站），外部地址发起主动连接，由路由器或者防火墙上网关接收这个连接，然后将连接转发到内部，此转发称为DNAT，主要用于内部服务对外发布。
列表优先级：表格从上到下，优先级从低到高

名称	协议	外部IP地址	外部端口	内部IP地址	内部端口	启用	
test	TCP UDP	0.0.0.0/0	8000	192.168.1.2	8000	☒	删除

添加

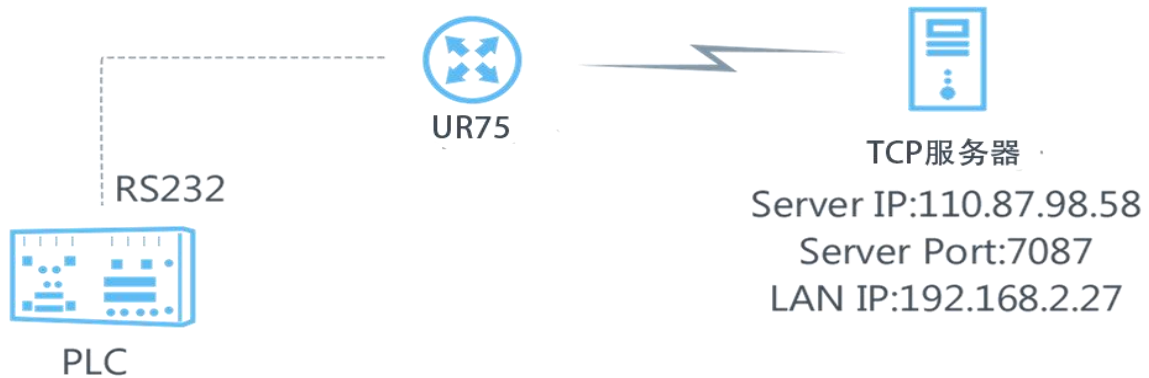
保存

保存并应用

单击“保存并应用”按钮，完成配置。

4.7 DTU 应用案例

案例



可编程逻辑控制器通过 RS232 与 UR75 连接。然后启动 UR75 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 '工业' (Industrial) menu in the left sidebar, with '串口' (Serial Port) selected. The main panel displays settings for '串口1' (Serial Port 1). The '启用' (Enable) checkbox is checked. The '串口类型' (Serial Port Type) is set to 'RS232'. The '波特率' (Baud Rate) is '9600', '数据位' (Data Bits) is '8 Bits', '停止位' (Stop Bits) is '1 Bits', and '校验位' (Parity Bits) is '无' (None). The '软件流控' (Software Flow Control) checkbox is unchecked.

2. 配置串口模式为“DTU 模式”。UR75 作为客户端接入的 DTU 协议选择“TCP 客户端”。

The screenshot shows the DTU configuration settings. '串口模式' (Serial Port Mode) is set to 'DTU'. 'DTU 协议' (DTU Protocol) is set to 'TCP 客户端' (TCP Client). '保活间隔' (Keep-alive Interval) is '75' seconds. '保活重试次数' (Keep-alive Retries) is '9'. '重连间隔' (Reconnect Interval) is '10' seconds. '指定协议' (Specify Protocol) is unchecked. '串口分帧长度' (Serial Port Framing Length) is '1024' bytes. '串口分帧间隔' (Serial Port Framing Interval) is '100' milliseconds. '注册包内容' (Registration Packet Content) is empty.

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 table. The table has columns for '服务器地址' (Server Address), '服务器端口' (Server Port), and '状态' (Status). The first row shows '110.87.98.58' for the server address and '7087' for the server port. The status is '未连接' (Not Connected). There are '删除' (Delete) and '添加' (Add) buttons at the bottom right.

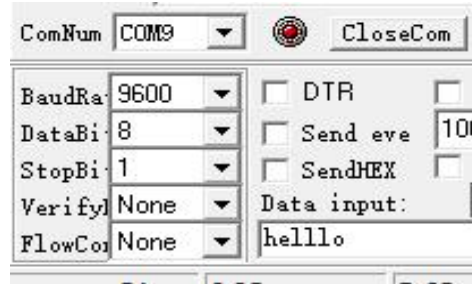
4. 结束所有配置之后，单击“保存”和“应用”按钮。

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。

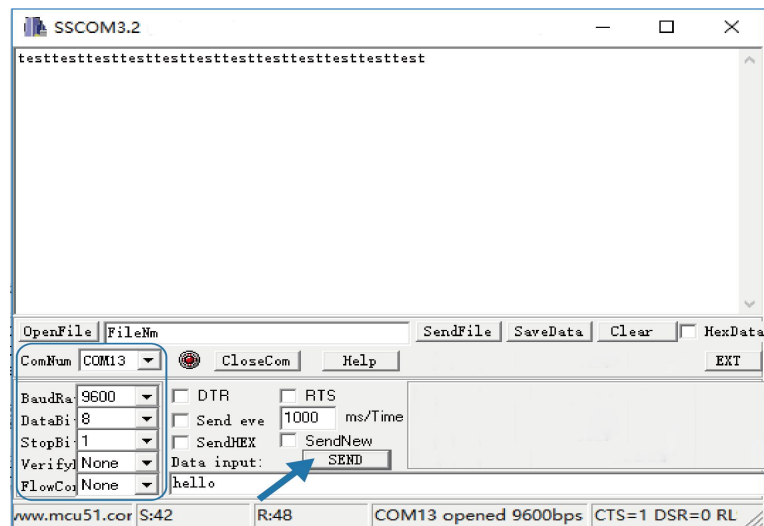


6. UR75 通过 RS232 串口线连接到电脑，启动电脑上的“sscom”软件以测试串口通信。

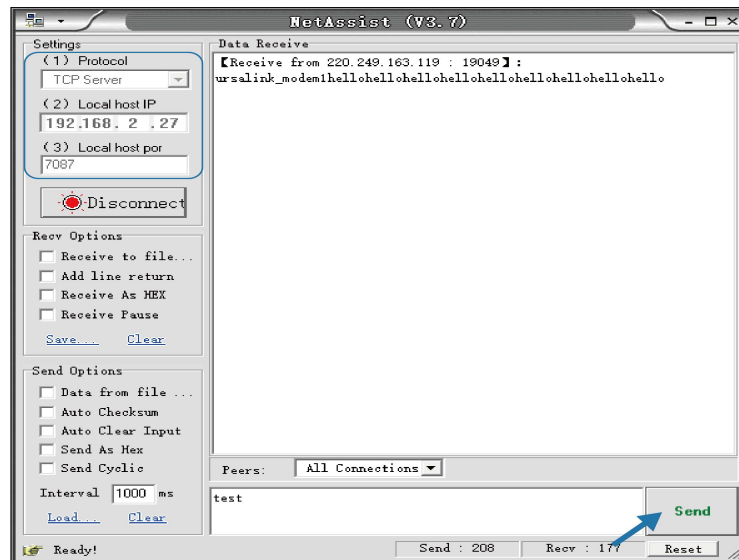


7. UR75 和 TCP 服务器的通信连接成功之后，可以在 sscom 和 Netassit 之间传输数据。

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 UR75 的 RS232 端口进行测试。

相关内容

[串口](#)