

UR75

工业路由器 用户手册



前言

Milesight

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
2024.6.12	V1.1	1. 新增 Node-RED/DDNS/IP 穿透/短信/SNMP 功能
		2. modbus mater 更名为 modbus client
		3. 支持配置蜂窝 MTU/IMS/短信中心号码
		4. 支持 NAT 功能
		5. 支持添加自定义 AT 指令
		6. 新增硬重置功能
		7. 更新网页显示效果
		8. 细化蜂窝状态

目录

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	
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	
3.1.3 GPS	
3.1.4 防火墙	16
3.1.5 路由表	17
3.1.6 VPN	
3.2 网络	
3.2.1 接口	
3.2.2 WLAN (仅 Wi-Fi 版本)	
3.2.3 防火墙	
3.2.4 静态路由	
3.2.5 IP 穿透	
3.2.6 DDNS	40
3.2.7 网络诊断	
3.3 VPN	42
3.4 工业	62
3.4.1 串口	63
3.4.2 I/O	
3.4.3 Modbus Clienet	68
3.4.4 GPS	
3.5 APP	
3.6 系统	81
3.6.1 常规	81
3.6.2 密码	82

		3.6.3	设备管理	
		3.6.4	备份还原	85
		3.6.5	重启	87
		3.6.6	日志	87
		3.6.7	调试	89
第四	章	应用案	圣例	91
	4.1	恢复出	出厂设置	91
		4.1.1	通过网页页面	
		4.1.2	硬件上重置	
	4.2	固件チ	升级	93
	4.3	网络连	车接	94
		4.3.1	蜂窝数据连接	
		4.3.2	以太广域网连接	
	4.4	双 SIN	M 故障转移应用案例	
	4.5	Wi-Fi J	应用案例	
	4.6	NAT 应	立用案例	
	4.7	DTU 应	立用案例	

第一章 产品介绍

1.1 概述

Milesight

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。





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

6

- 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

www.milesight.cn

- 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。

単数制面板 原用 検索用の ク 拉利 - 市市時時後後本林県	>	ビリン ビリン ビン ビン ビン ジェル ビン ジェル ビン ジェル ビン ジェル ビン ジェル ビン ジェル ジェル	· 调整计 · · · · · · · · · · · · · · · · · · ·	算机的设置 系统和安全 查看你的计算机状态 通文对历史记录保存例如文件备份副本 备份和起愿(Windows 7) 网络和 Internet 查看网络状态和任务 硬件和声音 查看後都印印机、 添加资备 调整常用移动设置 程序 卸載 <u>周</u> 序	88 19 19 19 19 19 19 19 19 19 19 19 19 19	查看方式 考别 - 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®数字格式 轻松使用 健用 Windows 建议的设置 优化视觉显示
①在 Windov 索"控制面板	vs 10	任务栏单击"搜索框"	以搜	② 单击"控制面标 看网络状态和任务	反"将其 子"	其打开,然后单击"查

更放网络设置 全 设置新公法提成网络 设置大线、贯带、拨号、储时或 VPN 法接; 或设置通由器或访问点。 全 选择更加基础 法接受问题里新法接到无线、有线、接号或 VPN 网络法规。 记得原因组织共享感觉 访问位于其他网般计算机上的文件和打印机,或更改共享设置。	持续时间: 28 天 07:08:48 速度: 1.0 Gbpz 详细信息(2) 活动
20%除音 诊断并作复列炮问题,或获得幼稚排除信息。	(愛麗性 @) (愛慧用 @) (诊断 (G) 关闭 @)

8

网络 共享	常規 金用配置 9 加果网络支持此功能,则可以获取自动指派的 IP 设置。否则,	Internet 初辺版本 4 (TCP/IPv4) 居性 2 世 常規 加里団総支持が竹能、回回以祭町白さ社指海的 TP 沿来。조回4.
Realtek PCIe GBE Family Controller 配置(C) 此连接使用下列项目(0): ● Bpcap Facket Driver (DFCAP) ● Internet 协议版本 6 (CE/IP(4)) ● Internet 协议版本 4 (CE/IP(4)) ● Explorement Driver 4 (CE/IP(4)) ● Explorement Brite Structure (DFCAP) ● Internet 协议版本 4 (CE/IP(4)) ● Explorement Brite Structure (DFCAP) ● Explorement Brite Structure (DFCAP) ● Internet 协议版本 4 (CE/IP(4)) ● Explorement Brite Structure (DFCAP) ● Internet 助议版本 4 (CE/IP(4)) ● Explorement Brite Structure (DFCAP) ● Internet Brite Structure (DFCAP) <td> な需要从网络系統管理员处获得适当的「IP 设置。 自动获得 IP 地址(0) 使用下面的 IP 地址(S): IP 地址(C): 子柯猿岛(0): 最认网头(0): 自动获得 DNS 服务器地址(0) 使用下面的 DDS 服务器地址(2): 首法 TDS 服务器(1): 通出的验证设置(1) 高級 (0)</td> <td> · (法本・日本中・ · (法・ · (法・ ·</td>	 な需要从网络系統管理员处获得适当的「IP 设置。 自动获得 IP 地址(0) 使用下面的 IP 地址(S): IP 地址(C): 子柯猿岛(0): 最认网头(0): 自动获得 DNS 服务器地址(0) 使用下面的 DDS 服务器地址(2): 首法 TDS 服务器(1): 通出的验证设置(1) 高級 (0)	 · (法本・日本中・ · (法・ · (法・ ·
确定即消	福定 取消	确定 取消
双击 "Internet 协议版本 4	方法 1: 单击 "自动获取 IP 7	方法 2:单击"使用以下 IP 地址
(TCP / IPv4) ″ 配置 IP	地址";	在路由器的同一子网内手动分配
地址和 DNS 服务器。	· · · · · · · · · · · · · · · · · · ·	—————————————————————————————————————

(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。
 - Milesiph Friesiph Barrier Barrier Barrier Barrier Barrier
- 2. 输入用户名、密码,然后单击"登录"。

Milesight _{星纵物联}



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	۲
新密码	۲
确认密码	۲
	取造 保友

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。

Milesight	状态 / 概说		自动刷新:开 💄 admin [→
宮 状态 へ	为了您的设备安全,请及时修改款认密码		
概范	系统		
蜂窩网络	主机名	Router	
GPS	型号	UR75-504AE-P-W2	
防火墙	序列号	6019D1875086	
路由表	固件版本	78.0.0.3-r1	
VPN	硬件版本	V1.2	
メ 网络 、	本地时间	2024-06-12 17:03:57	
≢ VPN ~	运行时间	0h 3m 51s	
置服务 、			
🖆 АРР 🗸 🗸	硬件		
⑧ 系统 ~	CPU 温度	39°C	
	平均负载	4.86, 3.09, 1.31	
	内存 (1024 MB)		709.00 MB (69%)
	Flash (1024 MB)		741.95 MB (72%)
	 Several valuation of the state of the state	类型: 静态地址	
		IPv4: 192.168.48.22	
	WAN	IPv6:- IPv4 网关: 192.168.48.1	
	Ø		

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

系统		
主机名	Router	
型号	UR75-504AE-P-W2	
序列号	6019D1875086	
固件版本	78.0.0.3-r1	
硬件版本	V1.2	
本地时间	2024-06-12 17:04:42	
运行时间	0h 4m 36s	
硬件		
CPU 温度	39°C	
平均负载	4.61, 3.27, 1.45	
内存 (1024 MB)		708.96 MB (69%)
Flash (1024 MB)		742.09 MB (72%)

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。	
序列号	显示设备的 SN 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。	
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。	
硬件		
CPU 温度	显示当前 CPU 工作温度。	
亚均各共	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	
干均贝轼	和 15 分钟的平均值)的负载平均值,数值越小越好。	
内存	显示当前内存可用数量。	
Flash	显示当前 Flash 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。



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	1 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	
SIM卡状态	Ready
模块型号	RG500L-EU
版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
当前SIM卡	SIM1
蜂窝频段	÷
信号强度	0
注册状态	Not registered
IMEI	869263055068641
IMSI	-
ICCID	۵
运营商	e.
网络类型	÷
PLMN ID	ш. С
位置区码	۵
Cell ID	-
CQI	-
下行带宽	100MHz
上行带宽	100MHz
信曝比	25dB
PCI	230
RSRP	-85dBm
RSRQ	-11dB
EARFCN	99240

蜂窝运行状态	
项目	描述
SIM 卡状态	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。
	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	
流星统计结果仅供参考,实际流星以运营商提供的收费账单为准。	
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
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 SIM-2	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB
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 SIM-2	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB
流晶统计结果仅供参考, 实际流晶以运营商提供的收费账单为准。 SIM-1 SIM-2 网络	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB
 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 SIM-2 网络 项目 	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB
 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 SIM-2 网络 项目 状态 	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB 描述 显示蜂窝网络的拨号状态。
 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 SIM-2 网络 项目 状态 IPv4/IPv6 地址 	RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB RX: 0.0 MiB TX: 0.0 MiB ALL: 0.0 MiB 描述 显示蜂窝网络的拨号状态。 显示蜂窝拨号获取的 IPv4/IPv6 地址。
 流蟲统计结果仅供参考, 实际流晶以运营商提供的收费账单为准。 SIM-1 SIM-2 网络 项目 状态 IPv4/IPv6 地址 IPv4/IPv6 网关 	RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB RX: 0.0 MIB TX: 0.0 MIB ALL: 0.0 MIB 描述 显示蜂窝网络的拨号状态。 显示蜂窝拨号获取的 IPv4/IPv6 地址。 显示蜂窝拨号获取的 IPv4/IPv6 网关

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。

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	
GPS 状	态

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。

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

								显示空链	复位计数器 重启防火墙
IPv4 防火	墙 IPv6 防火	······································							
表: Filter	r								
链 INPUT (作能略: ACCEETT, 0 数据包, 0 B 流量)									
数据包	流量	目的网络	协议	ЛП	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		
8.91 K	1.53 MB	input_rule	all	*	*	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	ctstate RELATED, ESTABLISHED	-
65	3.38 KB	syn_flood	tcp	*	*	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 B	zone wan input	all	ccmni2	*	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		-
防火地	啬状态								
表: F	ilter		显示过	扩滤网络	数据包	的默认表	₹.		
表: N	TAV		显示修	砂网络	数据包	的源/目	的 IP 地址	上或端口链路表。	
表: N	Mangle		显示用	于修改	网络数	据包内报	夏 文修改、	重新封装链路表。	
表: F	RAW		用于关	闭 NA	「表上的	り链路连	接追踪。		
显示	空链		显示/图	急藏无规	则的名	≧链路。			
复位证	复位计数器 重置所有链的流量计数。								
重启网	重启防火墙								

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		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。

在该页可以查看 VPN 运行状态

名称

状态

VPN

客户端

IPsec 服务器

OpenVPN 服务器

>

>

>

>

接口

尚无任何配置

服务器IP

尚无任何配置

远端

18

已连接客户端IP

3.1.6 VPN

2	1	6	\/	D	N

J	د	~	•	-	1

状态

概范 蜂窝网络

GPS

防火墙

路由表 VPN

网络

VPN

Τ₩

系统

	状态	服务器IP 已在建築户端IP
		尚无任何政策
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。
		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
大応		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/Ope	enVPN 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	ı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			
状态 >	接口接口设置链路备份	交換机 静态地址分配	
<u>火山</u> 接口	接口		
WLAN 防火場 静态路由 网络诊断	WAN E	超行時時後 0h 8m 12x MAC: 24.51:24F5AFDE 接触: 599.40 KG (4467 数時面) 発始:: 125 M(1455 数時面) IP+4: 192.168.48.206/24	頭島 実績
VPN > 工业 > 系统 >	LAN Ê	総行時時: 0h 10m 49s MAC: 24年1244F584/DF 持物な: 6630,00 (15 83 影明音の) 総理: 4.61 MB (1665 影明音の) 「Pv4: 192.168.11/24 「Pv6: 24/08.463.21 195.06.42,261:124(ffer5.add/)54	頭启 编辑
	42:2/时代5 0f3	XE行資利用に On 10m 386 Web 21.1 5 KG (22 及回信約) XUE 25.71 KG (22 及回信約) XUE 25.71 KG (27 及回信約) IPVet 10.1525.23.4/2 IPvet 240ex452115600cs1/728 IPVet PD: 240ex4542115600cs1/728	重启编辑
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 fd21:7	¹⁹ aa:79b5::/48	
全局网络选环	页		
IPv6 ULA 前	J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。

接口 » WAN	
常规设置高级设置	
状态	 运行时间: 0h 17m 0s MAC: 24:E1:24:F7:73:70 接收: 15.93 MB (22882 数据包) 发送: 2.92 MB (13370 数据包) IPv4: 192.168.48.22/24
协议	静态地址
IP 类型	IPv4 ~
IPv4 地址	192.168.48.22
IPv4 子网掩码	255.255.255.0
IPv4 网关	192.168.48.1
首选IPv4 DNS服务器	8.8.8.8
备选IPv4 DNS服务器	223.5.5.5

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

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	192.168.48.22	
IPv4 子网掩码	255.255.255.0	~
IPv4 网关	192.168.48.1	
首选IPv4 DNS服务器	8.8.8.8	
备选IPv4 DNS服务器	223.5.5.5	

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。	8.8.8.8		
备选IPv4 DNS 服务器	设置辅助 IPv4 DNS 服务器。	223.5.5.5		

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。

接口 » WAN

常规设置 高级设置

状态	🖉 运行时间: Oh 17m 45s
	MAC: 24:E1:24:F7:73:70
	接收: 16.07 MB (23353 数据包)
	发送: 2.98 MB (13688 数据包)
	IPv4: 192.168.48.22/24

DHCP 客户端

协议

~

接口 » WA	N			
常规设置	高级设置			
		自动获取DNS服务器		
		NAT		
		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。			
网络地址转换(NAT)	启用或禁用 NAT 功能。启用时, 私有 IP 地址可以转换为公共 IP 地址。			
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

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 » WA	N			
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
		NAT		
		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。	
网络地址转换 (NAT)	启用或禁用 NAT 功能。启用时,私有 IP 地址可以转换为公共 IP 地址。	
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

常规设置 高级设置 DHCP服务器 状态	^{脚参} 运行时间: 16h 29m 57s MAC: 24:E1:24:F7:73:71
状态	1997 运行时间: 16h 29m 57s MAC: 24:E1:24:F7:73:71
	接收: 22.99 MB (98816 数据包) 发送: 76.06 MB (102970 数据包) IPV4: 192.168.1.1/24 IPV6: 2409:8d34:2:3b1:26e1:24ff.fef7.737
IPv4 地址	192.168.1.1
IPv4 子网掩码	255.255.255.0
IPv6 前缀长度	64 ✔
IPv6 前缀标识	0

LAN-常规设置		
项目	描述	
	运行时间:显示该端口运行了多长时间。	
	MAC: LAN 接口的 MAC 地址。	
状态	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

MTU

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。

1500

基本设置

启用	0	
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。	

Milesight _{星纵物联}

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。

接口 » 蜂窝网络

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		Ø	
认证类型	NONE	~	
网络类型	自动	~	
允许漫游			
IMS			
短信中心号码			
NAT			
自定义MTU			
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,I LTE频段:	N28,N38,N40,N41,N	77,N78

蜂窝网络	
项目	描述
选择 SIM 卡	选择需要配置的 SIM 卡。
IP 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供应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
IMS	启用或禁用 IMS 功能。
最大传输单元 (MTU)	设置最大传输单元,范围: 1280-1500
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。

Milesight	j õ	路 / 接口					🙎 admin	(→
吕 状态		4)为了您的设备安全,请及时修改默认密码						
X 网络		接口 接口设置 链路备份 交换机 副	净态地址分配					
設口 WLAN		接口设置						
防火墙		接口	状态	属性	接口速率	接口模式		
静态路由		LAN1	Up 🗸	LAN	~ Auto ,	Auto	×	
IP穿透		LAN2	Up	LAN	~ Auto	Auto	~	
DDNS 网络诊断		LAN3	Up	LAN	~ Auto	Auto	~	
≇ VPN		LAN4	Up	LAN	 ✓ Auto 	Auto	Ŷ	
置 服务		WAN	Up	WAN	~ Auto	Auto	~	
d APP	e							
⑧ 系统	-							

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	ŧ					
开启链路备份功 表格从上到下,	b能后,若检测到当前转 优先级从高到低	递路不可用, 将自动切挂	與到下个链路			
优先级	启用规则	当前链路	接口	连接类型	IP	
1		٠	WAN	静态地址	192.168.48.206	三编辑
2		•	Cellular-SIM1	DHCP 客户端	100.115.251.117/29 240e:466:2154:878::1/128	☴編田
3	۵	٠	Cellular-SIM2	DHCP 客户端		三编
设置						
	恢复	夏至高优先级链路				
			勾选后,定时採测局优先级链路	是否能ping通,若可以,则切换至	:优先败吏局的链路	
		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)	去正常使用,系统将会进行重启		

链路备份	
项目	描述
链路优先级	
冶生纲	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
1/1.754/X	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。

Milesight ^{星纵物联}

	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	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
级链路	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。。

启用		
	关闭时,默认ping探测通过	
目的地址(IPv4)	8.8.8.8	
备选目的地址(IPv4)	114.114.114	
目的地址(IPv6)	2001:4860:4860::8888	
备选目的地址(IPv6)	2400:3200::1	
Ping间隔	180	秒
Ping重试间隔	3	秒
Ping超时	5	秒
最大重试次数	3	

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	۵					
VLAN设置							
VLAN ID	LAN 1	LAN 2		LAN 3	LAN 4	CPU	
5	Tagged	✓ Tagged	✓ Tagged	► Tag	ged 🗸	Tagged	▶ 删除
							添加
局域网设置							
名称		VLAN ID	IP地址	7	网掩码	最大传输单元(MTU)	
test	5	•	192.168.3.1	255.255.255.0	1	500	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。			
$ \Delta N 1 \Delta N 2 (\Delta N 2 \Delta N 4)$	把 VLAN 绑定到相应的端口并设置 Ethernet frame 在 trunk link			
LAINT, LAINZ(, LAINS, LAIN4)	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	test	~	
开始地址	192.168.3.100		
结束地址	192.168.3.199		
IPv4 租期	1440		分
IPv4 子网掩码	255.255.255.0		
DNS服务器	114.114.114.114	×	
	8.8.8	×	

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	
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。 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	,只有指 定 的主机才能连接,并且接口须为非动态 值将被固定分配给MAC 地址字段标识的主机,租	配置。 期是一个可选字段,可为每个主机单独设定 DHCP 租期的船	κ.	
主机名	MAC 地址	IPv4 地址	IPv4 租期	
			分	删除
				添加
			· 保	存保存并应用
静态地址分配				
项目	描述			
主机名	设置静态租约	的的主机名。		
MAC 地址	设置 DHCP	客户端的 MAC 地址。		
IPv4 地址	设置分配给智	客户端的 IPv4 地址。		
IPv4 租期	设置客户端的	灼剩余时间。		

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。

and see a second	
启用 🗹	
接口类型	以点 ~
BSSID 24	:e1:24:f5:af:e0
射频类型 8)2.11bgn/ax mixed 🗸
信道 A	uto 🗸
无线频宽 4) MHz 🗸
SSID Ro	uter_F5AFE0_2.4G
加密模式W	'EP 开放式系统 🖌
密钥	
ssiD广播 🕑	
AP隔离	
最大客户端数目 12	8
MAC地址过滤 🕝	
类型 自	名单 ~

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。		
	选择加密方式,可选"无加密"、"WEP开放式系统"、"WEP共享秘钥"、		
加密模式	"WPA-Auto" 、 "WPA-PSK" 、 "WPA2-PSK" 、 "WPA3-PSK" 、		
	"WPA-PSK/WPA2-PSK" 、 "WPA2-PSK/WPA3-PSK" 。		
密钥	填写介入无线网络的密钥。		
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。		
	白名单:只允许设置的 MAC 地址连接到路由器的无线接入点。		
INIAC 追迫	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			
方问控制				
名称	端口	本地	方问	远程访问
нттр	80	C	i	
HTTPS	443	C		
SSH	22		l	
TELNET	23	C	1	
网山过滤				

例:如需过濾www.google.com,请輸入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
ЦТТР	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
нир	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。
网页讨波	

Milesight _{星纵物联}

域名关键字过滤	通过设置域名中的关	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	1.

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>端囗映射>访问 列表优先级:表格从上到下,优先级	控制>ACL规则 从高到低					
名称		DEBASABUT		动作	启用	
test	来自	转发 IPv4, 协议 TCP, UDP, ICMP WAN(WAN, Cellular), IP 0.0.0.0/0 到 LAN, IP 192.168.3.0/24		医芹 转发		
						沃加

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。	
	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	ТСР	UDP	ICMP	•
源接口	WAN(WAN、Cellul	ar)	•
源地址类型	IP			•
源IP地址	0.0.0.0,	/0		
源端口	例:192.1 任意端 可输入端	68.1.1 或 192. 口 口号,或输入2	168.1.1/24 20~300	
目的接口	LAN			~
目的IP地址	0.0.0.0,	/0		
	例:192.1	68.1.1 或 192.	168.1.1/24	
目的端口	任意端			
	可輸入端	口号, 或输入2	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) 列表优先级:表格从上到下,优先级从;	web网站),外部地址发 高到低	起主动连接,由路由繼或省防火墙上的网关接	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			
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		
							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" 、 "UI	OP" 、"Both"	中选择协议。		
外部 IP 地址		定义允许访问	本地 IP 地址的	り主机或网络。	0.0.0.0/0 代表用	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	异范围。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	发的数据包的	「CP 或 UDP 端	口。	
启用		启用或禁用此	端口映射规则	0			
Ξ		拖动该按钮可	以调整端口映	射规则的优先组	及。 列表顶部的	的优先级最高	高。
删除		删除这条规则	0				

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	0
DMZ 主机IP地址	192.168.1.1
源IP地址	0.0.0/0

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。
	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
源IP 地址	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。

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 子网编码	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 IP 穿透

将分配的 IP 地址共享或传输给连接到路由器的单个局域网客户端设备。

Miles	ight	网络 / IP穿透	
8 状态	~	😑 为了您的设备安全,请及时修改默从密码	
24 网络	^		-
接口		19H	
WLAN		穿透模式	固定模式
防火墙		MAC	
静态路由			
IP穿透			
DDNS			
网络诊断			
幸 VPN	~		
圖 服务			
	~		
◎ 系统	~		

IP 穿透	
项目	描述
启用	是否启用 IP 穿透功能。
穿透模式	可选固定模式或动态模式。
MAC	当穿透模式设置为固定模式时,请设置 MAC 地址。

3.2.6 DDNS

动态域名系统(DDNS)是一种自动更新域名系统(DNS)中的名称服务器的方法,它允许用户将动态 IP 地址别名化为静态域名。DDNS 作为客户端工具,需要与 DDNS 服务器配合使用。在开始配置之前, 用户应在合适的域名提供商网站上注册并申请一个域名。

Milesight	网络 / DDNS	
吕 状态 人名法	分了您的设备安全,请及时修改默认密码	
メ 网络 へ		
接口	状态	未连接
WLAN	启用	
防火墙	服务商	自定义
静态路由	田山乞	
IP穿透		
DDNS	账号索引	
网络诊断	密码	Ø
≢ VPN ~	服务器	
■ 服务 ~	服务器路径	
🖾 АРР 🗸		
豪 系统 ~	现法	
	添加IP	
	使用HTTPS	

DDNS	
项目	描述
状态	显示连接状态。
启用	是否启用 DDNS。
服务商	选择 DDNS 服务运营商。
用户名	输入 DDNS 注册的用户名。
账号索引	输入 DDNS 服务器的用户 ID。
密码	输入 DDNS 注册的密码。
服务器	输入 DDNS 服务器的名称。
服务器路径	默认情况下, 主机名会附加到路径上。
域名	输入 DDNS 的域名。
添加 IP	将当前的 IP 附加到 DDNS 服务器的更新路径上
使用 HTTPS	是否启用 HTTPS 功能。

3.2.7 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	
执行各种网络命令以检查与其他系统的连接和名称解析。	
114.114.114.114 IPV4 PING -	openwrLorg IPV4 TRACEROUTE - NSLOOKUP
PING 114.114.114.114 (114.114.114.114): 56 data bytes	
114.114.114.114 ping statistics 5 packets transmitted, 0 packets received, 100% packet loss	
网络诊断	۵
网络诊断 项目	描述
网络诊断 项目 IPv4 Ping	/ 描述 单击以从 IPv4 中的设备 ping 外部网络。
网络诊断 项目 IPv4 Ping IPv6 Ping	/ 描述 单击以从 IPv4 中的设备 ping 外部网络。 单击以从 IPv6 中的设备 ping 外部网络。
网络诊断 项目 IPv4 Ping IPv6 Ping IPv4 Traceroute	描述 单击以从 IPv4 中的设备 ping 外部网络。 单击以从 IPv6 中的设备 ping 外部网络。 IPv4 中要检测的目的主机地址。
网络诊断 项目 IPv4 Ping IPv6 Ping IPv4 Traceroute IPv6 Traceroute	描述 単击以从 IPv4 中的设备 ping 外部网络。 単击以从 IPv6 中的设备 ping 外部网络。 IPv4 中要检测的目的主机地址。 IPv6 中要检测的目的主机地址。

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	翻除

OpenVPN 服务器 - 文件配置			
项目	描述		
金星を	单击以浏览服务器配置 ovpn 格式文件,包括设置和证书内		
心见	容。请根据示例参考服务器配置文件: <u>server.conf</u>		
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			

www.milesight.cn

账户							
		用户省				部時	
				尚无任何配置			
							添加账户
本地路由							
	子间				子同掩码		
				尚无任何配置			
							添加路由
客户端子网							
	各称		子间			子网络码	
				尚无任何酿造			
							添加于网

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。			
	从"tun"和"tap"这两种不同的 OpenVPN 设备接口中选择。tun 与 tap			
网络接口	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"			
以位天王	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。			
	从"NONE"、"BF-CBC"、"DES-CBC"、"DES-EDE3-CBC"、			
加密模式	"AES-128-CBC"、"AES-192-CBC"、"AES-256-CBC"中选择加密			
	算法。			
县十住检험二 (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。			
取入1~期半儿(IMTU)	合法值: 64-1500。			
最大帧长	设置传输的最大帧长度。合法值: 64-1500。			
口十/合自犯则	从低到高选择输出日志级别:"错误"、"提示"、"注意"、"调试"。			
口心后尽纵加	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 编词 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: <u>client.conf</u>
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		
	界面配置	~
协议	UDP	~
端口	1194	
运端地址		
网络接口	tun	~
以证类型	无	~
本地 <mark>IP</mark>		
近種IP		
精简模式	LZO	*
Ping 间隔	60	
Ping 重适	300	
加密模式	无	~
最大传输单元(MTU)	1500	
最大較长	1500	
日志级别	注意	~
专家选项		

本地路由

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。		
	从"tun"和"tap"这两种不同的 OpenVPN 设备接口中选择。tun 与		
网络接口	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。		
认证悉刑	从"无"、"共享静态密钥"、"用户名/密码"、"单客户端证书认证"		
《仙天王	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。		
Ding 青洋 (孙)	如果在这段时间内一直超时,将重新建立 OpenVPN 隧道。合法值:		
Filiy 里瓜(炒)	60-3600.		
加密模式	从"NONE"、"BF-CBC"、"DE-CBC"、"DES-EDE3-CBC"、		

子网掩码

尚无任何能置

	"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。在给定的网络环境中可传输的数据包最大长度的标志符。
取入1 5 制中元(MITU)	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。
生学进行	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
专家远坝	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	対版	
证书	3132 -313	89
私胡	3132 -511	
DH	900 9 31	
TA	3132 433	Dit
证书吊销列表	9192 -932	
预共事密胡	対策	
客户端_1		
CA证书	50 Wit 1994	
(2:4)	3/05 - 644	
私钥		
ТА	31%	
福共重密组	5100 1224	

Milesight

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。		
ТА	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。		
ТА	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。

48

启用	•		
IPsec模式		~	
IPsect参议	ESP	~	
本地子网	192.168.1.1		
本地子网搏码	255.255.255.0		
本地ID类型	Default	~	
远端子网	192.168.2.1		
远端子网携码	255.255.255.0		
远端ID类型	Default	~	
SA加密算法	AES128	~	
SAULUE	SHA1	~	
PFS组	NULL	~	
SA生存时间	3600		紗
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。

Milesight ^{星纵物联}

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	0				
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	预共享密钥	~			
XAUTH					
生存时间	10800	ŧ	眇		
PSK列表					
进	**				预共导密钥
				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。
	从"MD5"和"SHA1"中选择认证算法应用在 IKE 协商中。
认证算法	MD5:使用HMAC-SHA1;
	SHA1:使用HMAC-MD5。
	从"MODP768_1"、"MODP1024_2"、"MODP1536_5"选择来应
	用在 IKF(网络密钥交换)协商中。
DH 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。
	从"PSK"、"CA"中选择,应用到 IKE 协商中。
本地认证类型	PSK:预共享密钥;
	CA: 认证机构。
XAUTH	启用后输入 XAUTH 用户名、密码。
	在 IKE 协商中设置生存时间。合法值:60-86400。在 SA 过期之前,IKE
生存时间 (秒)	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。
密码 PSK 列表	输入 XAUTH 认证所需密码。
密码 PSK 列表 选择器	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。
密码 PSK 列表 选择器 预共享密钥	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。
密码 PSK 列表 选择器 预共享密钥 SA 参数	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。
密码 PSK 列表 选择器 预共享密钥 SA 参数	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、
密码 PSK 列表 选择器 预共享密钥 SA 参数	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、 "AES128_MD5"、"AES128_SHA1"、"AES192_MD5"、
密码 PSK 列表 选择器 预共享密钥 SA 参数	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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。
密码 PSK 列表 选择器 预共享密钥 SA 参数	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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。
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	 输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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。 从 "NULL"、"MODP768_1"、"MODP1024_2"、"MODP1536_5"
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	 输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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。 从 "NULL"、 "MODP768_1"、 "MODP1024_2"、 "MODP1536_5" 中选择。
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	 输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 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。 从 "NULL"、"MODP768_1"、"MODP1024_2"、"MODP1536_5" 中选择。 NULL: 禁用 PFS 组;
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	 输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、 "AES128_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。 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;
密码 PSK 列表 选择器 预共享密钥 SA 参数 SA 算法	 输入 XAUTH 认证所需密码。 输入进行 PSK 认证时对应的识别号。 输入预共享密钥。 可以选择 "DES_MD5"、"DES_SHA1"、"3DES_MD5"、"3DES_SHA1"、 "AES128_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。 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;

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。
<i>去</i> 完进顶	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
专 承远坝	用分号分隔字符串。

Milesight 星纵物联 厦门星纵物联科技有限公司

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。

Milesight ⊈纵物联

IPsec 网关地址	输入远端 IPsec 服务器地址(IP/域名) 。
	从"隧道"和"运输"中选择。
IPsec 模式	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。
	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。
IPSeC 阶段	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。
	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。
★主 己 米王	ID:在IKE协商中把IP地址当作ID。
本地で安全	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。
	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。
远端 ID 举型	ID:在IKE协商中把IP地址当作ID。
心地で欠当	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。
	设置 IPsec SA 的生存时间。合法值:60-86400。注意:当协商建立 IPsec
SA 生存时间	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	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	预共享密钥	~	
本地密钥			۲
XAUTH			
生存时间	10800		秒
IPsec高级			
支持压缩			
时间裕度	100		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。
	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。
炒肉快巧	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。
	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;
加密算法	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。
	从 "MD5" 和 "SHA1" 中选择认证算法应用在 IKE 协商中。
认证算法	MD5:使用HMAC-SHA1;
	SHA1:使用HMAC-MD5。
	从"MODP768_1"、"MODP1024_2"、"MODP1536_5"选择来应
	用在 IKF(网络密钥交换)协商中。
DH 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。
	从"PSK"、"CA"中选择,应用到 IKE 协商中。
本地认证类型	PSK: 预共享密钥;
	CA: 认证机构。
XAUTH	启用后输入 XAUTH 用户名、密码。
	在 IKE 协商中设置生存时间。合法值:60-86400。在 SA 过期之前,IKE
生存时间 (秒)	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。
去 家进顶	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
マ豕匹坝	用分号分隔字符串。

3.3.2.3 IPSec 证书

在使用 IPSEC 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。

Psec 服务器		
	CA证书	湖田 田田 武武
	本地证书	が読みませい。
	私钥	親語 野田 一部時
IPsec_1		
	CA证书	浏览 导出 删除
	本地证书	対応 号出 删除
	远端证书	が読 号出 副除
	- 147	

IPsec 服务器		
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。	
私钥	导入/导出私钥文件。	
IPsec 客户端		
IPsec 答尸端		
IPsec 客戶端 项目	描述	
IPsec 客戶端 项目 CA 证书	描述 导入/导出根证书文件。	
IPsec 客戶端 项目 CA 证书 本地证书	描述 导入/导出根证书文件。 导入/导出本地证书文件。	
IPsec 客戶端 项目 CA 证书 本地证书 远端证书	描述 导入/导出根证书文件。 导入/导出本地证书文件。 导入/导出远端证书文件。	

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P地址		
用户名		
空時		۲
以证类型	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	0	
本靖陵道IP地址		
对编随着IP地址		
启用MPPE		
地址/控制压缩		
协议字段压缩		
Asyncmap值		
最大接收堂元(MRU)	1500	
最大传输单元(MTU)	1500	
链路检测间隔时间	60	眇
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
	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。
本地 IF 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	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-ffffffff,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。
	为了检测隧道的链接,客户端和服务器周期性地给彼此发送 PPP 回应。如
链路检测间隔时间(秒)	果在指定时间内,客户端或服务器接收不到对端 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。
土字进西	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
专家选项	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。

60

眉用		
服务器P地址		
用户名		
空码		۲
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	۵	
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/直	******	
最大接收单元(MRU)	1440	
最大传输单元(MTU)	1440	
键路检测间隔时间	60	影
最大重试次数	1	
专家选项		

РРТР	
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
	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。
本地 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-ffffffff。
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。
	为了检测隧道的链接,客户端和服务器周期性地给彼此发送 PPP 回应。如
链路检测间隔时间 (秒)	果在指定时间内, 客户端或服务器接收不到对端 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 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。
	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
专 豕 范 坝	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

Milesight _{星級物联}

> 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。

Milesight	服务 / 目			
8 状态	• 9为	了您的设备安全,请及时修改默认密码		
X 网络	~ 串□	1 串口2		
± VPN	~			
2 服务	~	启用	•	
串口		串口类型	RS485	~
I/O Modbus Client		波特率	9600	~
GPS		数据位	8 Bits	~
电话 & 短信		停止位	1 Bits	~
SNMP		校验位	无	~
	~	软件流控		
● 系统	~	串口様式	Modhus Client	v

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 Client"、 "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 Client:选择 Modbus Client 模式,在"工业 > Modbus Client"中配置基本参数和频道。

串口模式	DTU	~	
DTU 协议	TCP 客户端	~	
保活间隔	75	ŧ	6
保活重试次数	9		
重连间隔	10	秒	
指定协议			
串口分帧长度	1024	字	节
串口分帧间隔	100	Ż	秒
注册包内容			

目的IP地址

DTU 设置	
项目	描述
	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。
DTU 协议	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。
(1):1:101111 (1):10111	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
1米沽时隔(杉)	值: 1-3600。
但这手计为数	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
保活里试次敛	数后 TCP 连接将进行重连。合法值:1-16。
串口分帧长度(字	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:
节)	1-1024。
串口分帧间隔 (毫	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。

状态

秒)	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				
	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			
1朱沽间隔(秒)	值: 1-3600。			
们江王之子	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			
保石里以次釵	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	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:			
节)	1-1024。			
	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。			
串口分帧间隔(毫	合法值: 10-65535。			
秒)	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。			
	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			
连接超时时间	有从从设备接收到任何数据,则 TCP 连接将断开。			
	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			
读取间隔	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			
	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			
响小业起的扣扣目	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。

吕 状态	v						
X 网络	~	DI DO					
≢ VPN	~						
38服务	^	启用	0				
串口		模式	高电平	ł		~	
I/O		持续时间	100				豪秒
Modbus	Client						
GPS		动作	DO	SMS	Node-RED	*	
电话&郑	臣信	电话群组				~	
SNMP		+#*+**					
	Ŷ	古名内容。					
◎ 系统	~						
							0/255

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。 DO: 勾选启用 DI 触发控制 DO 输出状态。

SMS:选择电话组以发送短信报警。
Node-RED:当安装了 Node-RED 时,将 DI 状态发送到数字输入节点。

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		* <mark>1</mark> 0 臺秒
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 Clienet

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

3.4.3.1 Modbus Client

在该界面可以配置 Modbus Client 的参数。

启用		
读取间隔	0	秒
最大重试次数	3	
最大响应时间	500	毫秒
命令间隔时间	50	毫秒
通道	请选择	★ 读取

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	数日	指令类型	链路类型	运输设备IP	端口	有符号	小数位	
	1	0	1	保持寄存器 (INT16) ¥	тср 🗸				0	88*
										_

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。	

告警设置 名称

告警条件

描述

尚无任何配置

告警委型

添加告警设置		×
名称	- 満近第	
告醫療件	False 🗸	
短悔	8	
电话群组	¥	
异地名普尔森	教売 FYFAR9ANNEDAY FYME, 地理変列AME的 地址ADDRES (武明県南朝国のALLE, (東南地理 長SCONDTION) 77/255	
异丙酮的后进管约率	設示 SYEARSMONGDAY STME, 以連進SMAMED 地址ADDRESS BIRGIE MRIBSVALLE, (時地市面 含5CONDITION) 777255	
里貝萼告	0	
		取2首 保持
告警设置		

项目

满加

名称	自定义告警设置名称。
告警条件	选择触发报警的条件。
最小阈值	设置触发警报的最小值。当实际值小于此值时,将触发警报。
最大阈值	设置触发警报的最大值。当实际值大于此值时,将触发警报。
短信	当 Modbus 通道满足条件时,启用或禁用短信报警。
电话群组	选择接收报警短信的电话组。
	电话组可以在"服务 > 电话&短信 > 电话"页面添加。
异常告警内容	当实际值满足告警条件时,路由器将自动触发告警,并将设置的异常内容发
	送到指定的电话组。
异常接触后告警内容	当实际值从超出阈值恢复到正常值时,路由器将自动取消异常告警,并将预
	设的正常内容发送到指定的电话组。
重复告警	一旦启用,相同的告警将会持续报告。否则,相同的告警只会报告一次。

TCP转发

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。

尚无任何配置

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。

端口



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。

Milesight ⊈纵物联

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		*
包含RMC信息			
包含GSA信息	۲		
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	服务器法口	状态
		尚无任何就習	

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。



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。		

3.4.4.4 电话&短信

电话

电话设置包括呼叫/短信触发、短信控制和事件的短信报警。

74

Milesight	服务 / 电谱 & 理信			朱尘用記畫	옾 admin	(→
8 #2 v	为了您的设备安全,请及时修改新认	1.8533				
※ 网络	电话设置 短信					
≢ VPN ~						
	电调本					
#0	电适号码		25課			
NO	123456				删除	
Modbus Client					15th	
GPS						
电话 & 短信	电活群组					
SNMP	名称	描述	号码列表			
d App ~			尚无任何配照			
● 凝焼 ~					ntās:	

电话设置		
电话本		
项目	描述	
电话号码	输入电话号码。仅允许数字、"+"和"-"。	
描述	对电话号码进行描述。	
电话群组		
名称	设置电话群组名称。	
描述	对电话群组进行描述。	
号码列表	选择要添加到列表中的电话号码	

电话&短信

短信设置包含远程短信控制、发送短信以及短信接收和发送状态。

电话设置 短信		
常规设置		
	短信模式 PDU	v
短信	远程控制	
	认证类型 电话号码	*
	电话群组	~

短信	
项目	描述
	选择短信模式:
	文本模式 :纯文本模式,主要用于欧洲和美国。从技术上讲,也可以用于发送中文
短信模式	短信。
	PDU 模式: 这是手机的默认编码模式, 符合所有手机的短信格式, 并且可以使用
	任何字符。
短信远程控制	启用/禁用短信远程控制。





短信发送		
项目	描述	
接收号码	填入接收短信的号码。	
内容	短信内容。	
短信接收记录/短信发送记录		
查找	查找短信记录。	
清空记录	清空短信记录。	

3.4.4.5 SNMP

SNMP 广泛用于网络管理中的网络监控。SNMP 以变量形式在被管理系统中公开管理数据。系统组织 在一个管理信息库 (MIB) 中,该库描述了系统状态和配置。这些变量可以被管理应用程序远程查询。 在网络中配置 SNMP 时, NMS 和 SNMP 的管理程序应在管理端设置。为实现从 NMS 查询,配置步 骤如下:

- 1. 启用 SNMP 设置。
- 2. 下载 MIB 文件并将其加载到 NMS 中。
- 3. 配置 MIB 视图。
- 4. 配置 VCAM。

SNMP 设置

电话设置包括呼叫/短信触发、短信控制和事件的短信报警。

Milesight ^{星纵物联}

SNMP设置	MIB视图	VACM	告警设置	MIB下载	
			启用	0	
			端口	161	
			版本	SNMPv2c	~
			位置信息	-	
			联系信息		

SNMP 设置		
项目	描述	
启用	是否启用 SNMP 功能。	
端口	默认端口为:161,范围:1-65535。	
版本	可选: SNMPV1, SNMPV2c或SNMPV3。	
位置信息	填写位置信息。	
联系信息	填写联系信息。	

MIB 视图

本节解释了如何为对象配置 MIB 视图。

SNMP设置 MB积图 VACM 告答设置 MIB下载			
MIB视图			
初盟各称	101521407U	OID	
All	Include	v [1	
System	Include	▼ 1.3.6.1.2.1.1	删除
			and the second se

MIB 视图		
项目	描述	
视图名称	设置视图名称。	
	从"包含"和"排除"中选择。	
视图规则	包含: 查询指定 MIB 节点内的所有节点。	
	排除: 查询除指定 MIB 节点外的所有节点。	
OID	输入 OID 编号。	
添加/删除	点击以添加或删除 MIB 视图。	

VACM

本节介绍如何配置 VCAM 参数。

Wine 第6日 第1日 Wine 新聞 Wine Wine Wine Wine Wine Wine Wine Wine			
SNMP 共同体			
共同体 支持网络	8 MBR08 68877		
VACM			
项目	描述		
支持 SNMP v1	和 v2c 的网络		
共同体	设置共同体名称。		
支持网络	访问此 MIB 视图的外部 IP 地址范围。		
MIB 视图	从 MIB 视图列表中选择一个 MIB 视图以设置权限。		
视图权限	从"只读"和"读写"中选择。		
SNMP v3 User			
用户名	设置 SNMPv3 用户的名称。		
安全等级	可选:无,认证/无加密和认证/加密中选择。		
认证算法	可选: MD5或 SHA。		
认证密码	填入认证密码。		
加密算法	当选择"认证/加密"时,从"AES"或"DES"中选择。		
加密密码	填入加密密码。		
只读视图	从 MIB 视图列表中选择一个 MIB 视图,将权限设置为"只读"。		
读写视图	从 MIB 视图列表中选择一个 MIB 视图,将权限设置为"读写"。		
通知视图	从 MIB 视图列表中选择一个 MIB 视图,将权限设置为"通知"。		

告警设置

本节解释了如何通过 SNMP 告警启用网络监控。

SNMP设置	MIB视图	VACM	告警设置 	MIB下载	
			启用	0	
			用户名	无	~
			服务器地址		
			端口		

告警设置	
项目	描述
启用	是否启用 SNMP 告警设置。

共同体	选择 SNMP v1/v2c 的共同体。
用户名	选择 SNMPv3 的用户。
服务器地址	填写 NMS 的 IP 地址或域名。
端口	填写 UDP 端口。端口范围是 1-65535。

MIB 下载

本节描述了如何下载 MIB 文件。

SNMP设置	MIB视图	VACM	告警设置	MIB下载
			MIB文件	Open_Router_MIB.txt

3.5 APP

Node-RED 是一种基于流程的开发工具,用于可视化编程和将硬件设备、API 和在线服务连接在 一起,作为物联网的一部分。Node-RED 提供了一个基于网络浏览器的流程编辑器,可以使用调色板 中的各种节点轻松地将流程连接在一起。有关更多指导和文档,请参阅<u>Node-RED 官方网站。</u>

如果尚未安装 Node-RED, 请从 Milesight 网站下载 Node-RED 应用并将其安装到设备上。

	为了您的设备安全。	请及时修改默认密	商		
		Node	RED安装	浏览	
安装完成后,将	将显示以下状态。				
		启用		操作界面	
		Node-RED 版本	3.0.2		
		组件库版本	1.0.1		
		升级组件库	湖武		
		所有流程	导出		
		恢复出厂设置	重置		
		卸載	卸載		

Node-RED	
项目	描述
启用	是否启用 Node-RED。
	安装完成后,将显示以下状态。
操作界面	点击启动 Node-RED 的 Web GUI, Node-RED Web GUI 的登录权限与
	Web GUI 的管理员帐户相同。
Node-RED 版本	显示 Node-RED 版本。
组件库版本	显示 Milesight 提供的 Node 库的版本。
升级组件库	通过导入库包来升级组件库。
所有流程	将所有数据流导出为 JSON 格式的文件。
恢复出厂设置	清除 Node-RED 中的所有数据流。
卸载	从此设备中卸载 Node-RED 应用程序。

Milesight 提供了一个自定义的节点库,用于使用路由器的接口。



Node-RED			
项目	描述		
Router Event	监控设备的告警事件。		
	接收短信消息。		
SIMS Input	仅在蜂窝网络连接时有效。		
SMS Output	发送短信消息。		

	仅在蜂窝网络连接时有效。
	接收 DI 状态。
Digital Input	仅在 DI 已启用且动作在 服务 > I/O > DI 的网页 GUI 上设置为 Node-RED 时
	有效。
Distal Quitaut	发送 DO 状态。
Digital Output	仅在 服务 > I/O > DO 的网页 GUI 上启用 DO 时有效。
	接收串口数据。
Serial Input	仅在串口已启用, 串口模式为 DTU 且 DTU 协议在 服务 > 串口 > 串口 的网页
	GUI 上设置为 Node-RED 时有效。
	发送命令到串口。
Serial Output	仅在串口已启用, 串口模式为 DTU 且 DTU 协议在 服务 > 串口 > 串口 的网页
	GUI 上设置为 Node-RED 时有效。
CDC Dood	接收 GPS 数据。
GPS Keau	仅在 GPS 在 服务 > GPS > GPS 的网页 GUI 上启用时有效。

3.6 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。

3.6.1 常规

主机名	Router	
本地时间	2023/03/17 20:58:07	
时区	ИТС	~
时间同步	与NTP服务器同步	~

系统-常规设置	
项目	描述
十四夕	用户可自定义路由器主机名称,以字母开头,只允许字母、
土机名	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。		
	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。			
时间同步	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	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
服务	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

82

3.6.2 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		۲
新密码		۲
确认密码		۲

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。

3.6.3 设备管理

3.6.3.1 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	





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		
密码	俱与C注册的工官理账户(Email)和密码。	

3.6.3.2 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。



 Milesight VPN

 项目
 描述

 Milesight VPN 设置

www.milesight.cn

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。
本地 IP 远程 IP	显示路由器的虚拟 IP 地址。 显示 Milesight VPN 的虚拟 IP 地址。

3.6.4 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。	
下部各份	生成新公
	土地用以
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。	
固性文性	同時間性
-1120	

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。

3.6.5 重启

中/回路20日11756505		1//0//50
立即面肩		
定时重启		
	启用 🕑	
	周期每天	~

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··································	
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。

3.6.6 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。

Milesight ^{星纵物联}

3.6.6.1 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	~

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"。	

3.6.6.2 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。

3.6.7 调试

3.6.7.1 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。

輸入您要发送	给蜂窝模块的AT	命令,按 Enter 拐	¥7.				
Eg: AT+CC	PS?						
AT+CSQ	AT+ECELL	AT+ERAT?	AT+EPBSEH?	AT+CREG?	AT+COPS?		
清除							

此外,点击编辑以自定义常用的 AT 命令,然后直接按黑框顶部的按钮来执行常用命令。

「指令	
AT+CSQ	删除
AT+ECELL	删除
AT+ERAT?	删除
AT+EPBSEH?	删除
AT+CREG?	删除
AT+COPS?	删除

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

3.6.7.2 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		
瀞		

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"。
- 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

状态 > 网络 >	备份/升级
VPN >	备份
工杯 >	
系统 🗸	
系统	下數智份 生成备份
出版	
後日日2月 各份/升级	
	恢复
调试	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"
	恢复到出厂设置的新作用置
	恢复配置 上传承份
	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。
192.168	48 206 显示
该操作将:	会使设备去失所有配置,您确定要重置设备到出厂设置?
	确定取消

然后路由器设备将重启并立即恢复出厂设置。

	重置中, 请不要断电		

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。

状态	>	备份/升级
网络	>	
VPN	>	备份
Т¥	>	点击"生成备份"下载当前配置文件的 tar 存档。
系统	~	
系统		下载备份生成备份
密码		
设备管理		
备份/升级		恢复
里后日末		
调试		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
		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 扇写固件

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

94

- 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			۲
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			МВ
清算日	1日	~	
蜂寬频段	5G NR 频段: N1,N3,N5,N7,N8,N20,N28,N38 LTE频段: B1,B3,B5,B7,B8,B20,B28,B32	,N40,N41,N ,B38,B40,B	77,N78 41,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。

dD ×		状态	Ready
概約	, in the second se	模块型号	RG500L-EU
蜂窝网络		版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
GPS		当前CIM-F	 SIM2
防火墙		2010/P476(2)	81
路由表 VPN		A260709X	7
MA			van (-annu)
Mist.		注册状态	Registered(Home network)
VPN	2	IMEI	869263050069412
工杯	>	IMSI	460115210733084
系统	>	ICCID	89860321245923785509
		运营商	CHN-CT
		网络类型	4G
		PLMN ID	46011
		位置区码	SFOC
		Cell ID	E0870B

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 ^Ξ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 表操从上到下,优先级从	1检测到当前链路不可用,将自; 高到低	动切换到下一个链路				
优先级	启用规则	当前链路	按口	连接类型	IP.	
1			WAN	Bench	192.168.48.206	
2	۵	•	Cellular-SIM1	DHCP 客户请		= 978
3	۵	•	Cellular-SIM2	DHCP 客户请	240e:466:2152:147e::1/128	= 568

- 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

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			

(2) DHCP 客户端



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。

れる /	接口	接口设置	的 交换机 射	态地址分配				
接口 WLAN 防火増	链路	优先级						
静态路由	开启组表	688番份功能后,若相 人上到下,优先级从3	创测到当前链路不可用,将自3 1991低	的規劃下一个链路				
网络诊断		优先极	启用规则	当前抵抗	接口	连接关型	IP	
		3	•	•	Cellular-SIM2	DHCP 查户跳	240e:466:2152:147e:1/128	= •
系统 >		2		٠	Cellular-SIM1	DHCP 螯户跳		≡ ***
		1	۵	•	WAN	静态地址	192.168.48.206	= 555
选择	SIM‡	SIM			~	选择SIM卡	SIM2	~
		未填写	则使用SIM卡中	自带默认配置			未填写则使用SIM卡中自带默	从配置
I	P 类型	IPv4	/IPv6		~	IP 类型	IPv4/IPv6	~
1	接入点					接入点		
	PIN码				۲	PIN码		۲
认	证类型	NON	١E		~	认证类型	NONE	
t [oct	络类型	自动			~	网络类型	自动	~
允	许漫游					允许漫游		
最大传输单元	(MTU)	1500				最大传输单元(MTU)	1500	
最大可	用流量				МВ	最大可用流量		МВ
j	清算日	1日			~	清算日	1日	~
蜂	寬 频段	5G NF N1,N3 LTE频 B1,B3	8 频段: 3,N5,N7,N8,N 段: 3,B5,B7,B8,B	20,N28,N38,N4 20,B28,B32,B3	0,N41,N77,N7 8,B40,B41,B4	3 蜂寬频段 2,843	5G NR 频段: N1,N3,N5,N7,N8,N20,N2 LTE频段: B1,B3,B5,B7,B8,B20,B2	8,N38,N40,N41,N77,N78 8,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	~	状态	Ready
概览		橋块型号	RG500L-EU
蜂窝网络		版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
GPS		当前SIM卡	SIM1
防火墙路由表		蜂寬頻段	N78
VPN		信号强度	-115dBm
网络	>	注册状态	Registered(Home network)
VPN	>	IMEI	869263050069412
Т₩	>	IMSI	460115210733084
系统	>	ICCID	89860321245923785509
		运营商	CHN-CT

Milesight _{星纵物联}

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

上內。			
状态	~	蜂窝网络	
概览		an ra ra an	
蜂窝网络		蜂窝运行状态	
GPS 防火墙		状态	Ready
路由表		機快型号	RG500L-EU
VPN	12.1	版本	RG500LEUACR04A01M8G_OCPU_20.001.20.001
网络	>	当前SIM卡	SIM2
VPN	>	韓黨颁發	878
ТЖ	>	信号摄度	6asu (-101dBm)
系统	>	注册状态	Registered(Home network)
		IMEI	869263050069412
		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	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	无加密	~
SSID广播	•	
AP隔离		
最大客户端数目	128	
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)									
内部需要提供对外服务时(如对外发布 列表优先级:表格从上到下,优先级从	īweb网站) ,外部 【高到低	也业发起主动	连接,自	I銷由器或者防火境上的网关操收这个连接。:	然后将连接转换到内部,此转换称为DNAT,主要	要用于内部服务对外发布。			
名称		协议		外部IP地址	外部满口	内部IP地址	内部防病口	启用	
test	TCP	UDP	•	0.0.0.0/0	8000	192.168.1.2	8000		=
									830
									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。

状态	串□1 串□2			
网络				
VPN		定田	P	
I N N			-	
串口		串口类型	RS232	~
I/O Modbus Master		波特率	9600	~
GPS		数据位	8 Bits	~
系统		_		
		停止位	1 Bits	~
		校验位	无	~
		软件流控		

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"。

串口模式	DTU	~
DTU 协议	TCP 客户端	~
保活间隔	75	秒
保活重试次数	9	
重连间隔	10	秒
指定协议		
串口分帧长度	1024	字节
串口分帧间隔	100	毫秒
注册包内容		

3. 配置 TCP 服务器 IP 地址和端口。

目的IP地址			
服务器地址	服务器第口	状态	
110.87.98.58	7087	大连接	893

- 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。

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

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。

<u>PC 端</u>

SSCOM3.2	_		×
testtesttesttesttesttesttesttesttest			~
	1		~
UpenFile FileNm SendFile SaveData	UIe:	ar	HexUata
ComNum COM13 💌 🍘 CloseComHelp			EXT
BaudRa 9600 - DTR RTS			
DataBi 8 🔽 🗖 Send eve 1000 ms/Time			
StopBi 1 SendHEX SendNew			
Verify None V Data input: SLAD			
	OTO .		0.01

TCP 服务器端



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。 8.

相关内容

串口