AI 数采魔方

SL-R621

使用说明书

v1.0.1

本手册适用于以下产品：FNR310 系列产品

四信智慧工业科技有限公司

hwww.findustrials.com/

版本历史

日期	版本	说明	作者
2025-9-4	v1.0.0	初始版本	Jonas
2026.5.27	v1.0.1	产品型号变更，增加 GPS 配置功能	Jonas



注意：配件和接口可能因型号不同而有所差异，具体以实物为准。

著作权声明

本文档所载的所有材料或内容受版权法的保护，所有版权由厦门四信通信科技有限公司拥有，但注明引用其他方的内容除外。未经四信公司书面许可，任何人不得将本文档上的任何内容以任何方式进行复制、经销、翻印、连接、传送等任何商业目的的使用，但对于非商业目的的、个人使用的下载或打印（条件是不得修改，且须保留该材料中的版权说明或其他所有权的说明）除外。

商标声明

四信均系厦门四信通信科技有限公司注册商标，未经事先书面许可，任何人不得以任何方式使用四信名称及四信的商标、标记。

产品适用性说明

本用户手册适用于以下设备的配置说明：FNR310、FNR310-5R、FNR310-C1、FNR310-GNSS、FNR310-NOANT

联系方式

地址:
福建省厦门市集美区软件园三期第 06 号栋 11 层
网站:
www.four-faith.com
电话:
+86-592-5907276 5907277
传真:
+86-592-5912735
邮编:
361021
电子邮件地址:
info@four-faith.com

目录

第一章 参数配置 1

1.1 配置连接图 1

1.2 登录配置页面 1

1.2.1 PC IP 地址地址配置（三种方法） 1

1.2.2 登录配置页面 2

第二章 配置与管理 5

2.1 WEB 界面顶部栏 5

2.2 首页 6

2.2.1 运行信息 6

2.2.2 设备信息 7

2.2.3 网络状态 8

2.2.4 无线信息 8

2.2.5 局域网端口 10

2.2.6 4G/5G 蜂窝网络 11

2.2.7 串口 12

2.3 网络设置 13

2.3.1 广域网 13

2.3.1.1 广域网配置 13

2.3.1.2 全局设置 15

2.3.1.3 运营商限制 15

2.3.1.4 拓扑图 16

2.3.2 局域网 16

2.3.3 WIFI 19

2.3.3.1 WIFI 配置 19
2.3.3.2 虚拟接口 22
2.3.3.3 Chillspot 22

2.3.4 VPN 24

2.3.4.1 PPTP 24
2.3.4.2 L2TP 27
2.3.4.3 OPEN VPN 30
2.3.4.4 IPSEC 34
2.3.4.5 GRE 38
2.3.4.6 EOIP 40
2.3.4.7 FRP 41
2.3.4.8 Zero Tier 43
2.3.4.9 L2tpv3 44
2.3.4.10 WireGuard 45
2.3.4.11 DMVPN 49

2.3.5 NAT 50

2.3.5.1 端口转发 50
2.3.5.2 DMZ 52
2.3.5.3 虚拟 IP 映射 52

2.3.6 IPv6 53

2.3.7 VLAN 56

2.3.8 网桥 56

2.3.8.1 桥接配置 57
2.3.8.2 端口设置 58

2.3.9 高级路由 59

2.3.10 DDNS 60

2.3.11 MAC 认证克隆 61

2.4 数据采集 62

2.4.1 子设备 62

2.4.2 云服务 63

2.4.3 接口设置 64

2.4.4 协议转换 65

2.4.4.1 Modbus TCP 65
2.4.4.2 Modbus RTU 66

2.5 应用设置 67

2.5.1 活动策略 67

2.5.1.1 定时重启 67
2.5.1.2 定时任务 68

2.5.2 安全设置 68

2.5.2.1 IP 地址限制 68
2.5.2.2 URL 地址限制 70
2.5.2.3 MAC 认证限制 70
2.5.2.4 防火墙 71
2.5.2.5 证书管理 72
2.5.2.6 WEB 访问 72

2.5.3 QOS 74

2.5.3.1 QOS 基本设置 74
2.5.3.2 QOS 分类设置 76

2.5.4 位置信息获取设置（GNSS） 78

2.5.4.1 基础配置 78
2.5.4.2 数据上报通道设置 79
2.5.4.3 采集与过滤策略 80
2.5.4.4 高级功能与数据格式 80

2.6 串口应用 81

2.6.1 串口应用 81

2.6.2 短信应用 82

2.7 运维管理 88

2.7.1 诊断 88
2.7.2 网络工具 89
2.7.3 命令调试 90
2.7.4 Profile 管理 90
2.7.5 日志管理 91
2.7.6 防火墙统计 92
2.7.7 流量统计 93
2.7.8 存储设置 94
2.7.9 远程管理 94
2.7.10 I/O 设置 100
2.8 云平台管理 100
2.8.1 设备云 100
2.9 系统设置 101
2.9.1 系统配置 101
2.9.2 登录管理 103
2.9.3 恢复出厂 103
2.9.4 备份 103
2.9.5 固件升级 104
第三章 LED 说明 105
第四章 安装说明 108

第一章 参数配置

1.1 配置连接图

在配置路由器之前，请确保使用出厂附带的网线将路由器正确连接至用于配置的电脑。为建立连接，将网线一端插入路由器上标有“WAN”的以太网接口（下文称为局域网口），另一端连接至电脑的以太网端口。此连接对于访问路由器的配置界面至关重要。

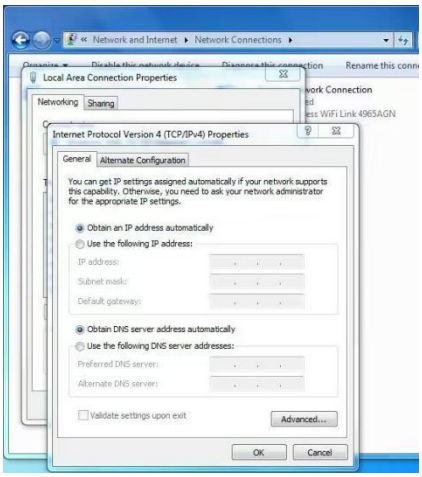


1.2 登录配置页面

1.2.1 配置电脑的 IP 地址（三种方法）

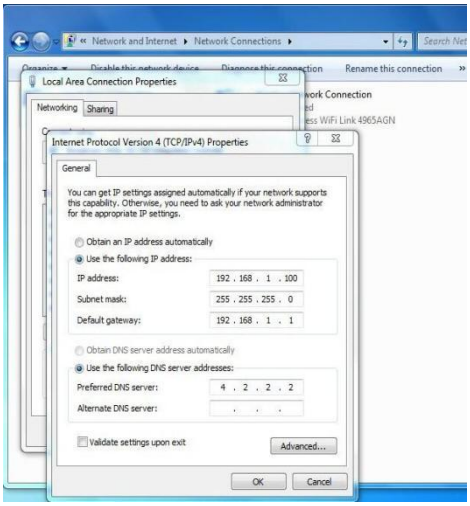
方法一：自动获取 IP 地址

如图所示，将电脑设置为自动获取 IP 地址。当电脑成功获取到 192.168.1.1 子网内的 IP 地址后，在浏览器地址栏输入 192.168.1.1 即可访问路由器的网页配置页面。



方法二：指定 IP 地址

将电脑的网络设置如下：将 IP 地址设置为 192.168.1.100（或 192.168.1 子网内的其他可用 IP 地址），子网掩码设置为 255.255.255.0，默认网关设置为 192.168.1.1，DNS 服务器设置为本地可用的 DNS 服务器。配置完成后，打开网页浏览器，在地址栏输入 192.168.1.1 即可访问路由器的网页配置页面。

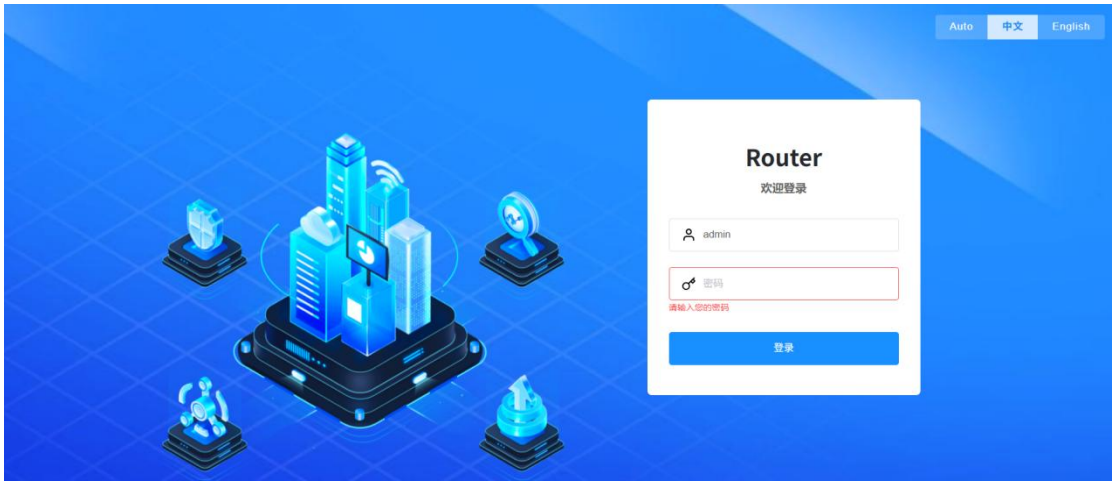


方法三：

将路由器的联网方式设置为静态 IP 地址或自动 DHCP，确保电脑与路由器都连接在与上级路由器相同的网络段内。配置完成后，在网页浏览器地址栏输入路由器广域网口 IP 地址：8088 即可访问路由器的网页管理界面。

1.2.2 登录配置页面

要访问路由器的网页管理界面，请打开 Internet Explorer 浏览器 或任意其他网页浏览器。根据第 1.2.1 节中所述的访问方式，在地址栏中输入相应的网址即可登录。默认用户名和密码均为管理员。



要访问路由器的网页管理界面，请启动 Internet Explorer\Edge 浏览器 或其他任意网页浏览器。参考第 节中的相应访问方式，在地址栏输入对应的网址。使用默认的用户名和密码（均为 管理员）登录，即可对路由器进行设置配置。



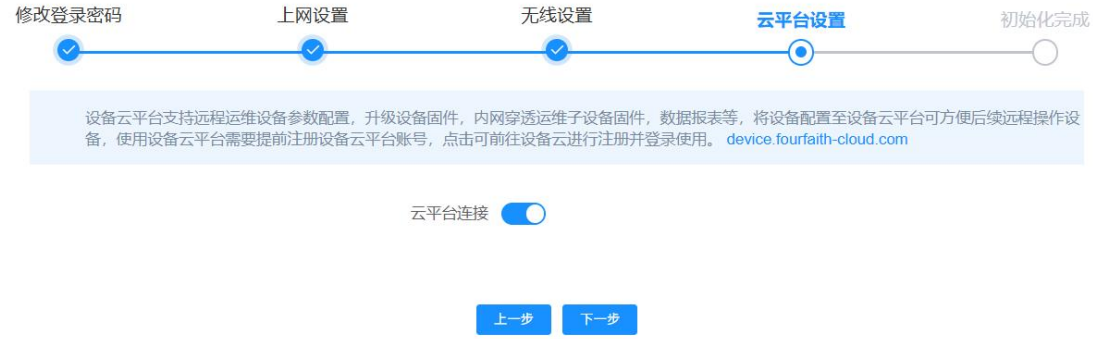
首次登录时，出于网络安全性考虑，系统需要强制输入新密码，且密码长度不少于把个字符，系统也会对应提示密码的强度便于参考。



上网设置可根据当前网络环境选择，以太网（有线）或蜂窝网络连接方式。



首次登录时，系统将引导设置 SSID 名称、安全模式、WPA 算法，并重置 Wi-Fi 密码（不少于 10 位），同时提供密码强度提示供参考。



初次登录时，用户可完成设备的云平台连接设置，实现与四信云的快速对接，从而便于后续的数据管理与远程运维服务。



初始化完成后，系统将跳转至登录页，需输入新密码才能进入设备配置页面。

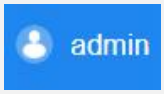
第二章 配置与管理

2.1 网页界面顶部导航栏

每台设备都包含一个网页顶部导航栏。本章将详细介绍该导航栏的主要功能与特点。



网页界面顶部导航栏说明

	点击可收起的菜单栏
	显示当前页面的菜单路径
	SIM 卡 1 和 SIM 卡 2 的连接状态
	有线网络连接状态
	管理平台的连接状态
	重启
	语言切换
	显示当前登录用户



登录管理：修改密码

引导：进入引导页设置

返回旧版：进入上一版本的网页界面

退出登录：用户退出登录

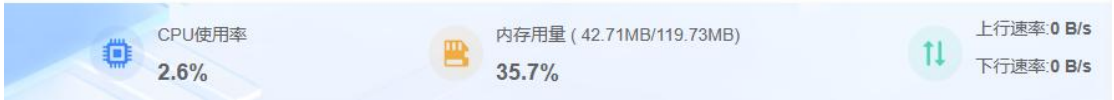
2.2 首页

首页是网站界面的主控制面板，提供关键信息的概览摘要，并包含多个快捷入口，方便快速跳转至其他页面，实现高效导航。



2.2.1 运行信息

本部分概览设备的当前运行状态，展示关键指标，如 CPU 处理器使用率、内存状态以及实时数据的上行和下行速率。这些指标有助于监测设备的运行效率与性能表现。

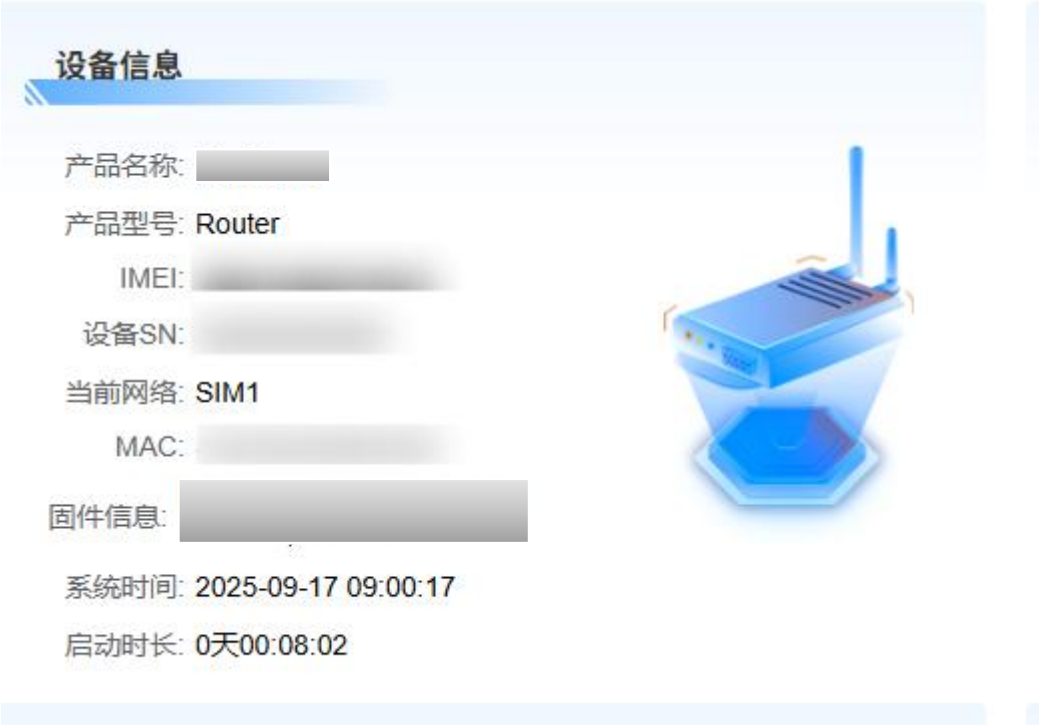


项目	说明
CPU 处理器	CPU 处理器 使用率百分比
内存用量	内存使用率百分比

上行速率	瞬时上传速率
下行速率	瞬时下载速率

2.2.2 设备信息

本部分用于展示设备的基本信息，包括型号、序列号、固件版本以及其他重要参数，便于全面了解设备的身份与配置情况。



项目	说明
产品名称	设备名称
产品型号	设备型号
编号	设备唯一标识符
当前网络	网络连接方式
MAC 认证	设备的 MAC 认证 地址
固件信息	设备的固件版本
系统时间	设备当前的系统时间
启动时长	设备自启动以来的运行时长

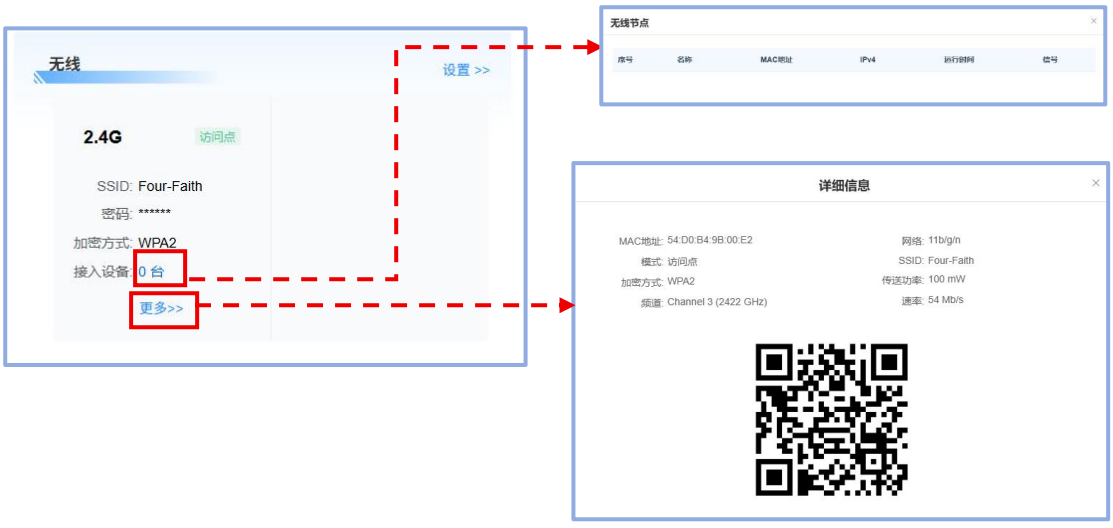
2.2.3 网路状态

本部分可用于查看详细的互联网连接信息。点击“设置”即可进入互联网配置页面。点击无线图标或有线图标可进行切换，查看对应的网络连接信息。此外，点击“诊断”将跳转至网络诊断页面，用于故障排查与分析。



2.2.4 无线信息

本部分提供有关无线网络的详细信息。点击“设置”即可进入无线网络配置页面。“设备数”字段显示当前连接到无线网络的用户数量。点击“数字”可查看无线上网用户的基本信息。此外，点击“更多”可以查看更多无线网络的详细信息，包括信号强度、安全设置以及已连接设备等内容。





项目	说明
SSID 服务	无线网络名称
密码	无线网络密码
加密方式	无线网络加密类型
接入设备	连接到网络的设备数量



项目	说明
MAC 认证地址	设备的 MAC 认证 地址
模式	设备的工作模式
加密方式	无线网络加密类型

频道	当前使用的无线信道
网络	支持的网络标准
传送功率	无线信号的发射功率
速率	无线网络传输速率

2.2.5 局域网端口

本部分提供有关 局域网 和 局域网/WAN 接口的基本信息，帮助您监控网络连接状态。点击“设置”可跳转至 局域网 接口配置页面。网络端口图标直观显示连接状态：绿色表示端口已连接，灰色表示端口当前未连接。此方式提供了一种清晰直观的方式来检查和管理端口连接情况。



项目	说明
MAC 认证地址	设备的 MAC 认证 地址
IP 地址地址	路由器在网络中的地址
子网掩码	接口的子网掩码，用于区分 IP 地址 地址中的网络部分和主机部分
本地 DNS 服务器	用于本地网络域名解析的 DNS 服务器 服务
支持 DHCP 服务	动态主机配置协议（支持 DHCP）的状态。启用时，设备会自动为连接的客户端分配 IP 地址 地址
起始 IP 地址地址	支持 DHCP 可分配的起始 IP 地址 地址
结束 IP 地址地址	支持 DHCP 可分配的结束 IP 地址 地址
设备	连接到该端口的设备数量

2.2.6 4G/5G 蜂窝网络

本部分用于查看蜂窝网络连接的详细信息。点击“设置”可跳转至 广域网 配置页面。您可以点击 “SIM 卡 1” 或 “SIM 卡 2” 在两张 SIM 卡 卡之间切换，以查看每张卡的具体信息。如需了解更深入的蜂窝网络信息，可点击“更多”查看包括信号强度、网络状态以及连接参数等内容的详细信息。



项目	说明
运营商	电信服务提供商
网络	表示技术标准和通信模式的网络系统
信号强度	设备接收到的信号强度
Band	设备的通信频段
IMEI	移动设备的唯一国际移动设备识别码（IMEI 号）
ICCID	唯一 SIM 卡卡标识符，用于归属和认证
IMSI	唯一移动用户身份，用于区分网络中的用户
EARFCN	LTE 无线信道标识符（演进绝对无线频率信道编号）
PCI	物理小区标识，用于区分 LTE 基站小区
EARFCN	E-UTRA 绝对无线频点编号，是 LTE 系统中用于标识下行链路或上行链路载波中心频率的编号
CELL ID	特定基站小区的唯一标识符
TAC	LTE 网络中的跟踪区域码，用于移动性管理
RSRP	参考信号接收功率，表示接收到的信号强度

RSRQ	参考信号接收质量，用于衡量信号质量
带宽	通信网络中用于数据传输的频率范围
SINR	信号与干扰加噪声比，反映信号清晰度

2.2.7 串口

本节提供有关控制台的详细信息，便于您管理和监控控制台相关设置。若需查看某个控制台的具体信息，可点击“控制台 1”或“控制台 2”切换至对应控制台的详细页面。若需配置串口参数，可点击“设置”跳转至串口配置页面，在该页面中可调整波特率、数据位等串口通信参数。



项目	说明
波特率	数据传输速率：可根据连接设备进行调整，但必须与所连接设备的波特率一致。
数据位	传输数据中的二进制位数：默认通常为 8 位，可根据连接设备需求进行修改。
校验位	显示当前使用的校验模式
停止位	标志传输数据结束的停止位数量。
名称	串口名称。
使用设备	当前连接的设备数量。

2.3 网络设置

2.3.1 广域网

2.3.1.1 广域网配置

广域网配置页面用于设置广域网网络接口，使设备能够连接到外部网络。通过该配置，可确保设备与广域网络建立通信，实现访问互联网或连接其他远程系统。

- **双链路配置选项**

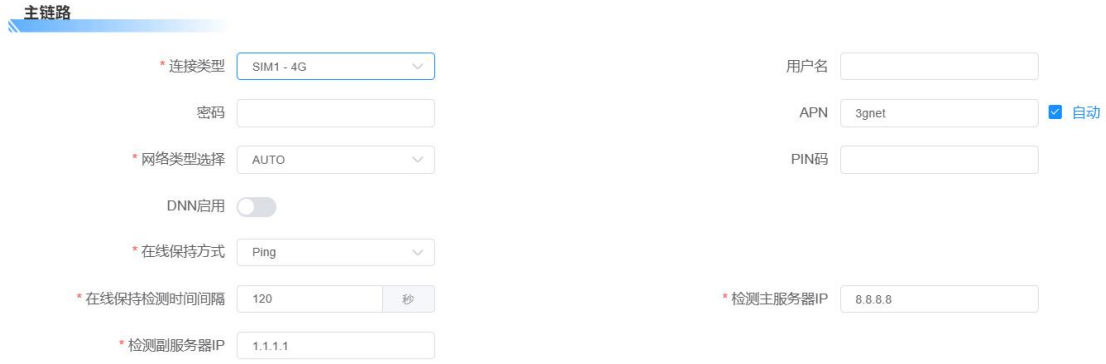
双链路选项用于配置双链路切换设置。该功能可实现设备在两条网络连接之间的管理与切换，提升连接的可靠性与容错能力。当其中一条链路发生故障时，设备可自动切换至备用链路，确保网络服务持续不断。



项目	说明
启用双链路备份功能	**开启**:启用后，当主链路故障时，路由器会自动切换到备用链路。 **关闭**：禁用后，当主链路故障时，路由器将不会切换到备用链路。
双链路同时在线	**开启**：两条链路（如 4G 和有线）可同时保持激活，支持高带宽应用或多链路协同。 **关闭**：同一时间仅保持一条链路激活，避免同时连接。
负载均衡	**开启**：路由器会在可用链路间动态分配网络流量，以优化性能并防止拥塞。 **关闭**：流量不会自动分配，负载均衡已禁用。

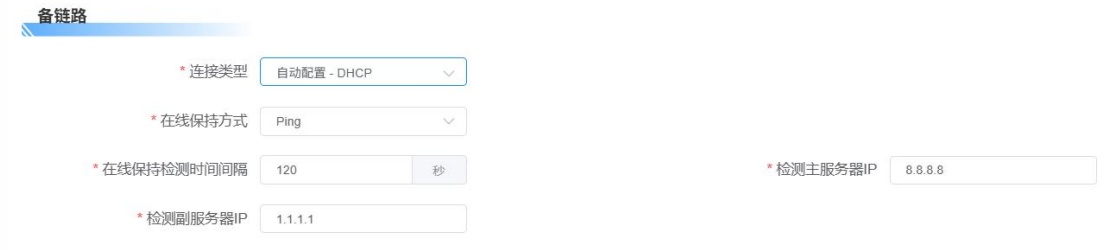
- **主链路**

本页面用于设置主链路的相关参数。



项目	说明
连接类型	选择主链路的连接方式（SIM 卡 1 或 sim2）。
用户名	如需网络认证，请输入用户名。
密码	输入网络认证密码。
APN	指定移动网络的接入点名称（APN）。
PIN 码	SIM 卡的个人识别码（引脚）。
DNN 网络启用	切换以启用或禁用专用网络名称（DNN）功能。
在线保持方式	选择监控和维护网络连接的方式。
在线保持检测时间间隔	设置连接性检查的间隔时间（秒）。
检测主服务器 IP 地址	主服务器 IP 地址 用于网络状态检测。
检测副服务器 IP 地址	备用服务器 IP 地址 用于网络状态检测。

- **备链路**



项目	说明
连接类型	选择主链路的连接方式（SIM 卡 1 或 sim2）。
在线保持方式	选择监控和维护网络连接的方式。
在线保持检测时间间隔	设置连接性检查的时间间隔（秒）。
检测主服务器 IP 地址	主服务器 IP 地址 地址，用于网络状态检测。
检测副服务器 IP 地址	备用服务器 IP 地址 地址，用于网络状态检测。

2.3.1.2 全局设置



项目	说明
强制网卡模式	设置网卡的工作模式。“自动”模式下，系统会自动检测并选择最佳模式。
匹配	定义网络传输的最大数据包大小（字节）。

2.3.1.3 运营商限制

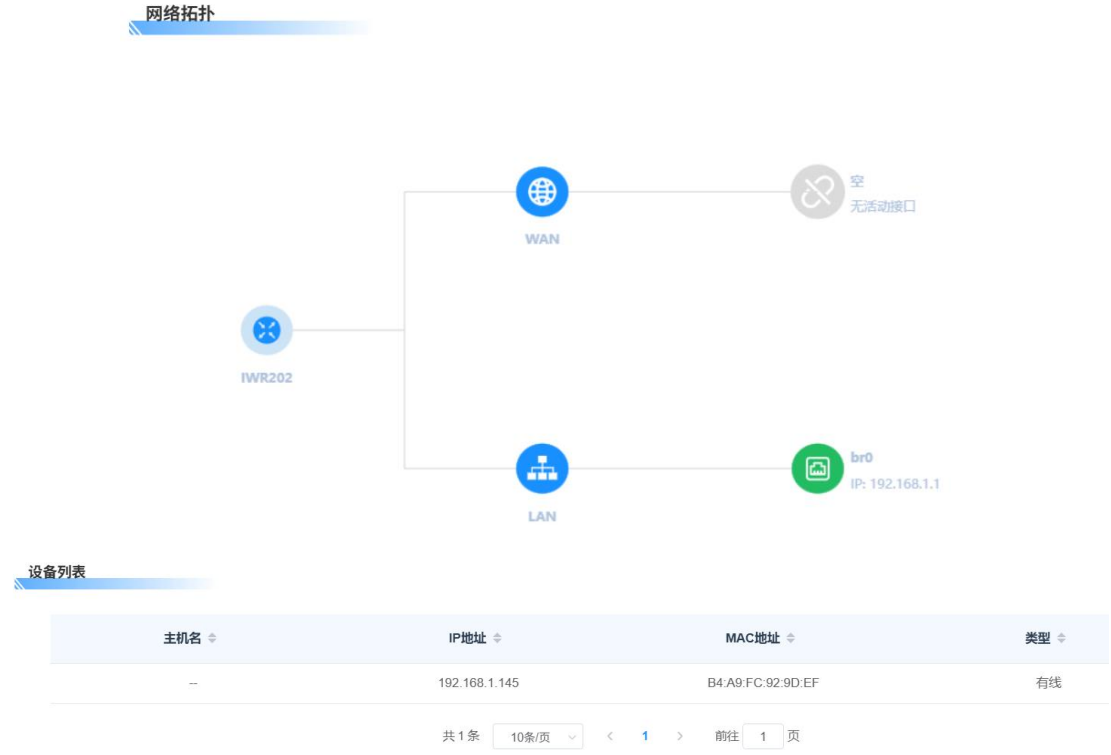


点击“新增”按钮以添加对应的运营商信息。

项目	说明
启用	开关选项：启用时，运营商限制功能根据定义的策略管理网络访问；禁用时，不施加任何限制。
策略	定义运营商限制方式。“黑名单”模式下，被阻止的运营商无法接入网络；“白名单”模式下，仅允许批准的运营商接入。

2.3.1.4 网络拓扑

支持查看设备网络拓扑及已连接设备列表。



2.3.2 局域网

本页面用于配置局域网（局域网）网络接口，使设备能够连接到本地网络。

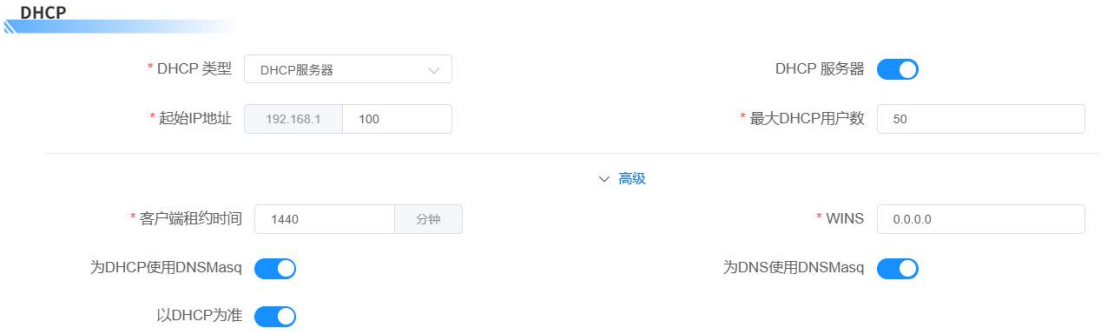
- **路由器 IP 地址**



项目	说明

LAN IP	路由器在本地网络（局域网）中的 IP 地址 地址，使设备能够访问路由器的管理界面。
子网掩码	此接口的子网掩码，用于区分 IP 地址 地址的网络部分和主机部分。
网关	局域网 设备访问外部网络的出口 IP 地址 地址；请确保正确设置网关地址，以便正常访问外部网络。
本地 DNS 服务器	用于将域名解析为 IP 地址 地址，需要填写有效的 DNS 服务器 服务器地址以保证正确解析。

- **DHCP 服务**



项目	说明
DHCP 类型	 选择路由器的 DHCP 服务类型。“DHCP 服务器”允许路由器自动为连接的设备分配网络参数，如 IP 地址。 “DHCP 转发器”充当中继代理来转发 DHCP 消息。选择后，必须手动输入目标 DHCP 服务器地址。
DHCP 服务器	 **开启（默认）：**路由器充当 DHCP 服务器，自动为连接的设备分配 IP 地址、子网掩码、网关和其他网络设置。 **关闭：**路由器不向设备分配网络配置参数。
起始 IP 地址	DHCP 服务器分配给设备的起始 IP 地址。

最大 DHCP 用户数	DHCP 服务器可以为其分配 IP 地址的最大设备数。
客户端租约时间	设备可以使用 DHCP 服务器分配的 IP 地址的持续时间，超过此期限后必须续约。
WINS	用于解析本地网络中的 NetBIOS 名称。
为 DHCP 使用 DNSMasq	**开启：**使用 DNSMasq 管理 DHCP 服务，提供增强的灵活性和配置选项。 **关闭：**禁用 DNSMasq，使用默认的系统 DHCP 管理模式。
为 DNS 使用 DNSMasq	**开启：**使用 DNSMasq 进行域名解析，实现本地域名缓存，解析速度更快。 **关闭：**禁用 DNSMasq，使用默认的系统 DNS 解析方法。
以 DHCP 为准	启用后，路由器具有 IP 地址分配的权威性，任何非权威性 DHCP 服务器都将被忽略。

- **LAN 口多网段**



允许您添加和管理多个 LAN IP 地址和子网掩码，使相应 IP 段内的设备能够连接到网络。

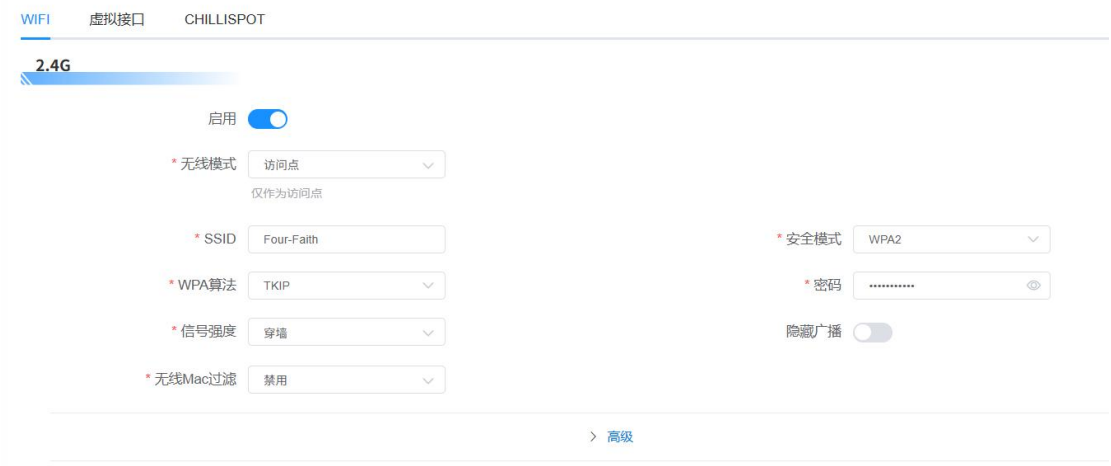
- **静态分配**



允许选择连接设备的 MAC 地址，并可选择自定义其名称、IP 地址和分配的 IP 有效持续时间。

2.3.3 WIFI

Wi-Fi 配置页面允许您设置设备互连和通过 Wi-Fi 访问互联网的无线设置。



2.3.3.1 WIFI 配置

设置无线模式。



项目	说明
启用	**开启：**激活 2.4G 无线网络，允许设备在 2.4G 频段发射信号，供其他设备连接。 **关闭：**关闭 2.4G 无线网络，停止设备在 2.4G 频段发射信号。
无线模式	**访问点：**允许其他设备（例如，手机、计算机）连接到路由器的无线网络以访问互联网。 **客户端：**设备充当无线客户端，连接到其他 WiFi 网络并通过它们访问互联网。

	中继：接收现有的 WiFi 信号并进行重传，扩展当前无线网络的覆盖范围。 **中继桥接：**扩大 WiFi 覆盖范围，在多个网络设备之间创建桥梁，实现同一局域网内不同区域的通信。



项目	说明
SSID	无线网络的名称。
安全模式	设置 4G 路由器无线网络的安全防护类型。  **开放：**不加密，允许对无线网络的开放访问。 **WPA：**一种使用动态密钥生成的无线安全标准。 **WPA/WPA2-PSK：**一种用于家庭网络的常用加密方法，其中设备需要共享密码才能连接。 **WPA2:**WPA 的升级版，通过高级加密协议（例如 AES）提供更强的安全性。 **WPA-Enterprise：**用于大型网络，需要 RADIUS 服务器进行用户身份验证，提供强大的安全性，但设置更复杂。 **WPA2-Enterprise：**通过 RADIUS 服务器将 WPA2 加密与企业级身份验证相结合，适用于高安全性环境。 **WPA/WPA2-Enterprise:WPA/WPA2 加密与企业级身份验证的组合，需要 RADIUS 服务器进行用户验证。**
WPA 算法	用于保护无线网络数据的加密算法。
密码	连接到无线网络时用于验证的 WiFi 密码。
信号强度	WiFi 信号的相关设置选项用于调整 WiFi 信号的输出模式。

	 **穿墙：**增强传输功率，以提高信号穿透墙壁等障碍物的能力，从而扩大覆盖范围，但可能会增加功耗。 **标准：**默认发射功率，平衡信号强度、覆盖和功耗。 **节能：**降低传输功率以节省能源，这可能会减少信号强度和覆盖面积。
隐藏广播	 **开启：**禁用广播无线网络名称（SSID），需要手动输入 SSID 才能连接，增强安全性和网络隐藏性。 **关闭：**主动广播 SSID，方便用户查找和连接网络。
无线 MAC 过滤	禁用后，任何设备都可以尝试连接到网络。 启用后，可以允许或拒绝具有特定 MAC 地址的设备访问，从而改善网络访问控制。



项目	说明
AP 独立	 **开启:**2.4G 无线网络独立工作，不受其他频段或功能的干扰。 **关闭：**2.4G 无线网络可能与其他频段或功能协同工作，具体取决于设备的整体配置。
区域代码	指定适用于无线网络的区域标准。
信道	表示无线网络数据传输的路径。在自动模式下，路由器根据周围的网络环境选择干扰最小的信道进行最佳数据传输。
最大客户端	可同时连接到此 2.4G 无线网络的设备的最大数量。

信道宽带	指的是信道的传输带宽。在自动模式下，路由器根据网络环境和设备能力调整通道带宽，以提高网络性能。
802.11 协议	定义无线网络的通信标准。

2.3.3.2 虚拟接口

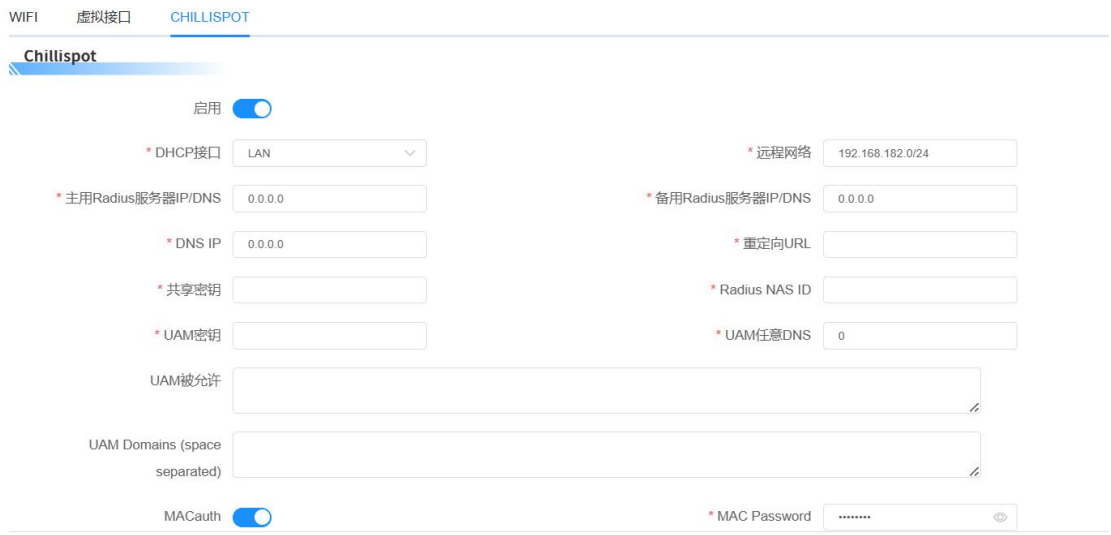
可以创建多个虚拟接口，每个虚拟接口代表不同的子网或网络服务。



项目	说明
新增	用于添加虚拟接口，有关内容设置，请参阅（“WiFi”页面） 
全选	一键选择所有选项
删除	删除所选条目

2.3.3.3 CHILLISPOT

它是一个开源的热点管理系统，用于管理和控制无线网络访问。本页面提供了其配置界面。



项目	说明
启用	**开启：**激活 Chillispot 功能，对路由器的无线网络进行用户管理和认证。 **关闭：**禁用 Chillispot，不通过 Chillispot 处理网络访问管理。
DHCP 接口	定义用于动态主机配置协议（DHCP）的网络接口。
远程网络	远程网络的地址范围，允许在一定范围内控制设备的访问。
主用 Radius 服务器 IP/DNS	设置主 RADIUS 服务器的 IP 或 DNS 地址，该服务器处理用户身份验证、授权和记帐。默认值 0.0.0.0 表示未对其进行配置。
备用 Radius 服务器 IP/DNS	定义备份 RADIUS 服务器的 IP 或 DNS 地址。如果主服务器发生故障，身份验证将切换到备用服务器。默认值 0.0.0.0 表示未对其进行配置。
DNS IP	指定 DNS 服务器的 IP 地址，用于域名解析，使设备能够访问 Internet 资源。
重定向 URL	当身份验证失败或对特定资源（通常是身份验证或通知页）的访问受到限制时，将用户重定向到此 URL。
共享密钥	与 RADIUS 服务器进行加密通信的安全密钥，保证数据的安全和一致传输。
Radius NAS ID	RADIUS 系统中 NAS（Network Access Server，网络接入服务器）的唯一标识，用于设备识别和管理。
UAM 密钥	与用户访问管理器（UAM）关联的安全密钥，用于增强用户访问保护。

UAM 任意 DNS	定义 UAM 是否允许使用任何 DNS 服务器。
UAM 被允许	启用或禁用用户访问管理器（UAM）功能，在输入字段中提供配置选项。
UAM 域（以空格分隔）	指定 UAM 允许进行网络访问的以空格分隔的域列表。
MACauth	**开启：**启用基于 MAC 地址的身份验证，仅允许预先批准的设备连接。 **关闭：**禁用基于 MAC 的身份验证，允许其他连接方法。
MAC 密码	启用 MACauth 时使用的认证密码。
802.1X 验证(EAP)	**开启：**启用 802.1X 和 EAP 认证，实现基于端口的网络访问控制，提高安全性。 **关闭：**关闭 802.1X 和 EAP 认证。
Chillispot 附加选项	允许输入系统所需的其他 Chillispot 配置参数。

2.3.4 VPN

“VPN 配置”页面用于设置虚拟专用网络（VPN），在公共网络上创建安全专用网络。它支持加密通信以进行远程访问和安全数据传输。

2.3.4.1 PPTP

- **PPTP 服务器**



项目	说明
PPTP 服务器	启用或禁用 PPTP 服务器。
广播支持	启用或禁用 PPTP 服务器的广播支持。
强制 MPP 加密	选择是否对 PPTP 数据强制 MPPE 加密。
DNS1 和 DNS2	设置主 DNS 服务器和辅助 DNS 服务器。
WINS1 和 WINS2	设置主要和次要 WINS 服务器地址。
服务器 IP	输入充当 PPTP 服务器的路由器的 IP 地址。此地址必须与 LAN 地址不同。
客户端 IP 范围	以 xxx.xxx.xxx.xxx-xxx 格式指定分配给 PPTP 客户端的 IP 地址范围。
用户列表	单击，进入用户管理界面，可以添加、删除、管理 PPTP 用户账号。 
连接状态	单击可查看当前的 PPTP 服务器连接状态，包括已连接的客户端、连接持续时间和其他详细信息。 

- **PPTP 客户端**



项目	说明
PPTP 客户端选项	**开启：**启用 PPTP 客户端，允许路由器通过 PPTP 协议连接到远程 VPN 服务器。 **关闭：**禁用 PPTP 客户端，防止路由器通过 PPTP 建立 VPN 连接。
服务器 IP 或 DNS 名称	输入 PPTP 服务器的 WAN IP 地址或 DNS 名称。
远程子网	指定远程 PPTP 服务器的本地 IP 地址。
远程子网掩码	定义远程 PPTP 服务器的子网掩码。
MPPE 加密	启用或禁用 MPPE 加密以实现安全通信。
MTU	设置 MTU 值（取值范围：0-1500）
MRU	设置 MRU 值（取值范围：0-1500）。
NAT	**开启：**开启 NAT 功能，允许多个内部设备共享一个公网 IP 进行 VPN 访问。 **关闭：**禁用 NAT，要求内部设备拥有自己的公网 IP 来访问 VPN。
启用手动设置隧道 IP	**开启：**使用固定 IP 地址连接 VPN 服务器。必须在固定 IP 地址中指定 IP。 **关闭:**VPN 服务器动态分配 IP 地址。
隧道 IP 地址	输入启用固定 IP 时要使用的固定 IP 地址。值 0.0.0.0 表示未设置固定 IP。

用户名	输入 PPTP 服务器授权的用户名。
密码	为 PPTP 服务器用户名输入相应的密码。
Ping 检测	**开启：**开启定期 ping 检测，使路由器能够监控 VPN 连接状态。 **关闭：**关闭 Ping 检测功能。
在线保持检测时间间隔	设置 ping 检测的时间间隔（例如，30 秒表示每 30 秒发送一次 ping 请求）。
IP 地址	显示 VPN 服务器分配给路由器的 IP 地址。
重连次数	指定 VPN 连接中断时自动重新连接尝试的次数（例如，10 次尝试）。
连接状态	单击可查看当前的 PPTP 客户端连接详细信息。 

2.3.4.2 L2TP

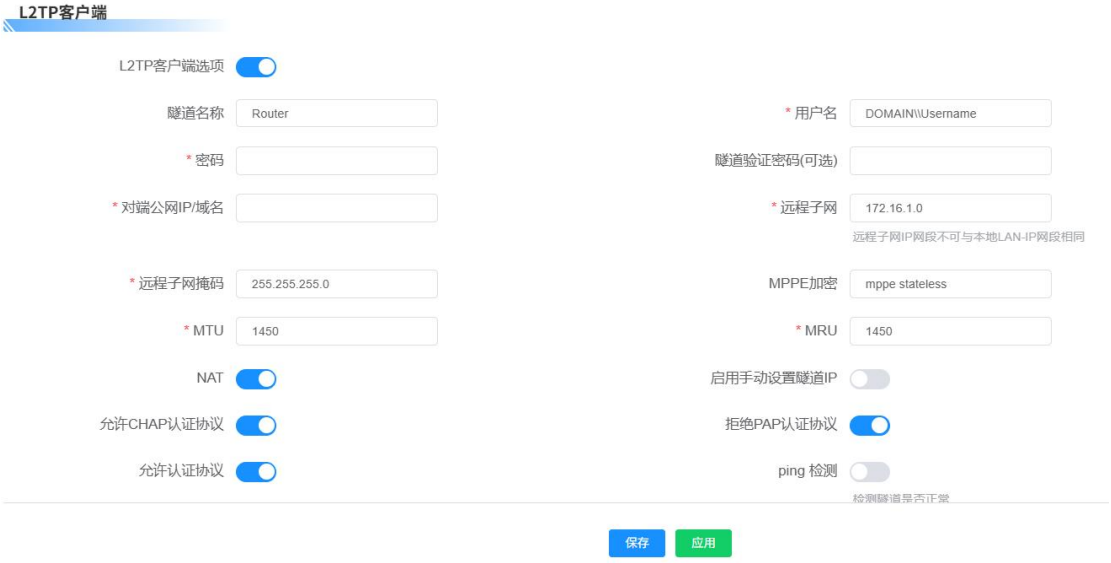
- **L2TP 服务器**



项目	说明
L2TP 服务器选项	**开启：**启用 L2TP 服务器，允许客户端通过 L2TP 协议连接到路由器的 VPN 服务。 **关闭：**禁用 L2TP 服务器，阻止客户端通过 L2TP 连接。
强制 MPPE 加密	**开启：**对 L2TP 连接强制使用 MPPE（微软点对点加密协议），

	通过防止数据被盗或篡改来增强安全性。 **关闭：**不强制进行 MPPE 加密，允许不加密或使用其他加密方法传输数据。
服务器 IP	配置 L2TP 服务器的 IP 地址。客户端使用此地址进行连接。将其保留为空白可能会使服务器无法正常运行。
客户端 IP	指定分配给 L2TP 客户端的 IP 地址范围（格式：xxx.xxx.xxx.xxx-xxx）。
隧道验证密码	配置 L2TP 隧道验证所需的密码。客户端必须提供此密码才能与服务器建立安全连接。
用户列表	单击，进入用户管理界面，可以添加、删除或管理 L2TP 用户账号，包括用户名和密码。
连接状态	单击可查看当前 L2TP 服务器连接详细信息。

- **L2TP 客户端**



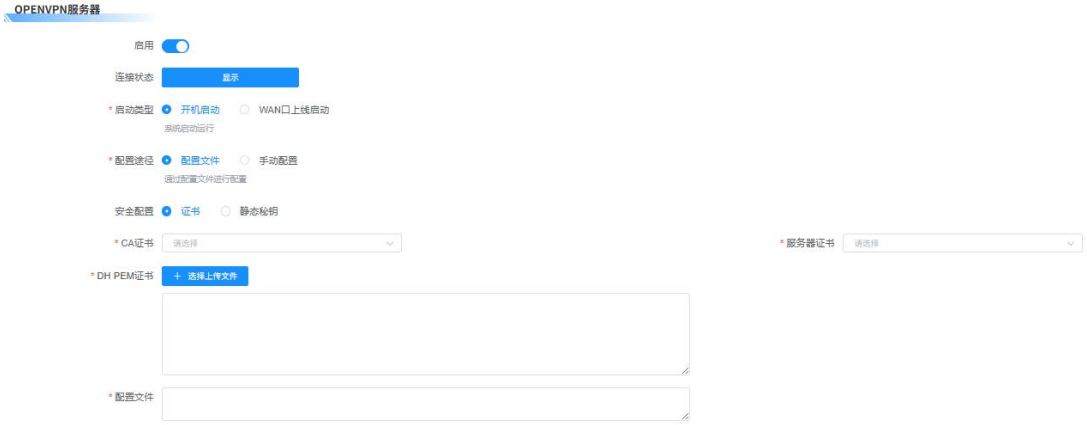
项目	说明
L2TP 客户端选项	 **开启：**启用 L2TP 客户端，允许路由器通过 L2TP 协议连接到远程 VPN 服务器。 **关闭：**关闭 L2TP 客户端，禁止路由器建立 L2TP VPN 连接。
隧道名称	指定 L2TP 隧道的名称以标识此 VPN 连接。
用户名	输入用于连接到远程 L2TP 服务器的用户名，格式为“域\用户名”，其中“域”是域名，“用户名”是帐户名。
密码	输入用户名对应的密码，以便与远程 L2TP 服务器进行身份验证。

隧道验证密码（可选）	建立 L2TP 隧道所需的额外密码，增强连接安全性。
对端公网 IP/域名	输入远程 L2TP 服务器的 IP 地址或域名。
远程子网	指定远程 L2TP 服务器的 IP 地址。
远程子网掩码	指定远程 L2TP 服务器的子网掩码。
MPPE 加密	选择是否为安全数据传输启用 MPPE 加密。
MTU	设置最大传输单位（MTU）（取值范围：0-1500）。
MRU	设置最大接收单元（MRU）（取值范围：0-1500）。
NAT	 **开启：**开启 NAT 功能，允许多个内部设备共享一个公网 IP 进行 VPN 访问。 **关闭:**关闭NAT,要求内部设备使用自己的公网 IP 访问 VPN。
启用手动设置隧道 IP	 **开启：**使用固定 IP 地址进行 VPN 连接。在固定 IP 地址中指定 IP。 **关闭：**VPN 服务器动态分配 IP 地址。
隧道 IP 地址	如果启用了“固定 IP”，请输入固定 IP 地址。0.0.0.0 表示未设置 IP。
允许 CHAP 认证协议	 **开启：**强制使用 CHAP（质询握手验证协议）进行安全验证。 **关闭：**不强制 CHAP。
拒绝 PAP 认证协议	 **开启：**拒绝 PAP（密码认证协议），因为其安全性较低（明文密码传输）。 **关闭：**允许 PAP 认证。
允许认证协议	 **开启：**连接 L2TP 服务器时需要认证。 **关闭：**不强制认证（可能存在安全隐患）。
Ping 检测	 **开启：**开启周期性 ping 请求，以监控 VPN 连接状态。

	关闭：关闭 Ping 检测功能。
检测时间间隔	设置 ping 检测的时间间隔（默认为 30 秒）。
IP 地址	显示从 VPN 连接获得的 IP 地址。
重启次数	设置 VPN 断开连接时的自动重新连接尝试次数（默认：10 次）。
连接状态	单击，查看 L2TP 客户端当前的连接状态。 

2.3.4.3 OPENVPN

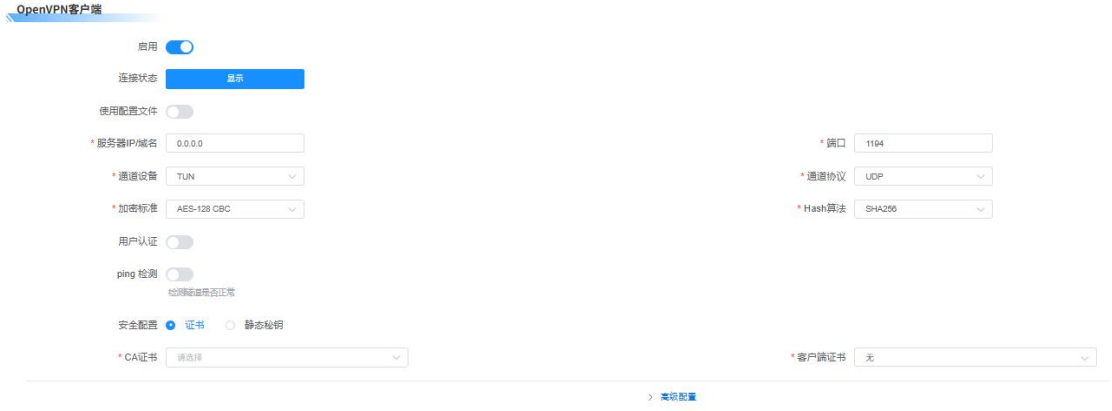
- **OpenVPN 服务器**

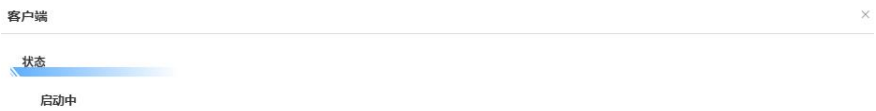


项目	说明
启用	**开启：**激活 OpenVPN 服务器，允许客户端通过 OpenVPN 协议进行连接。 **关闭：**禁用 OpenVPN 服务器，阻止客户端连接。
连接状态	单击“显示”以查看当前 OpenVPN 服务器连接状态。

	
开始类型	**启动时启动：**在路由器启动时自动启动 OpenVPN 服务器。 **从 WAN 开始：**在建立 WAN 连接时启动 OpenVPN 服务器。
通过配置	**手动配置：**手动设置 OpenVPN 服务器参数。 **配置文件：**上传预配置文件以简化设置，在有配置模板时非常理想。
安全保障	**证书：**使用 CA 颁发的证书进行认证，安全性高。 **静态密钥：**使用静态密钥进行认证，配置简单，但安全性较证书低。

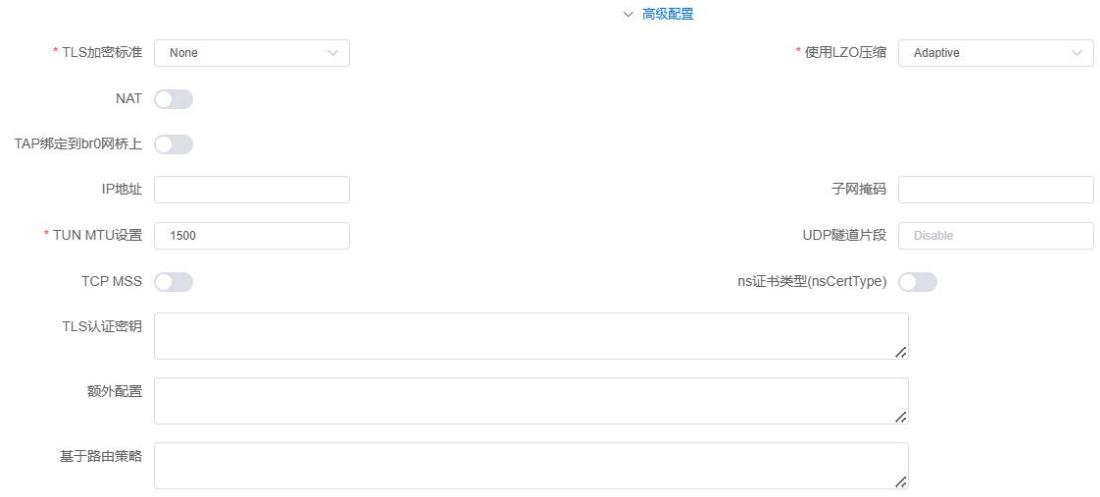
- **OpenVPN 客户端**



项目	说明
启用	 **开启：**激活 OpenVPN 客户端，允许路由器通过 OpenVPN 连接到远程服务器。 **关闭：**禁用 OpenVPN 客户端，阻止连接。
连接状态	单击“显示”以查看当前 OpenVPN 客户端连接状态。 
使用配置文件	 **开启：**导入预配置文件以便于设置。 **关闭：**手动配置各参数。
服务器 IP/名称	输入远程 OpenVPN 服务器的 IP 地址或域名。值“0.0.0.0”表示未设置。

港口	指定用于连接到 OpenVPN 服务器的端口。默认值为 1194,OpenVPN 常用。
隧道设备	**tun：**使用虚拟的 IP 层隧道，适用于大多数基于 IP 的应用。 **TAP：**使用虚拟以太网隧道，模拟以太网接口。
隧道协议	**UDP：**速度快，开销低，是实时应用的理想选择。通常与 OpenVPN 一起使用。 **TCP：**可靠、面向连接，适用于对数据准确性要求较高的场景。
加密密码	指定数据加密算法。
哈希算法	定义数据完整性验证和认证的算法。
用户通过身份验证	**开启：**需要用户名和密码进行身份验证。 **关闭：**禁用用户名-密码身份验证，使用其他方法（如证书）。
Ping 检测	**开启：**开启周期性 ping 请求，以监控连接状态。 **关闭：**关闭 Ping 检测功能。
安全保障	**证书：**使用 CA 颁发的证书进行认证，安全性高。 静态密钥：使用静态密钥进行身份验证，比证书更简单，但安全性较低。
CA 证书	使用证书模式时是必需的。选择现有 CA 证书以验证服务器和客户端凭据。
客户端证书	用于客户端身份验证和加密通信的数字证书。

高级配置：



项目	说明
TLS 加密标准	指定用于 TLS（传输层安全）协议的加密算法。
使用 LZO 压缩	**自适应：**根据网络条件自动调整 LZO 压缩以优化数据传输。 是：强制使用 LZO 压缩进行数据传输。 **禁用：**禁用 LZO 压缩。 **否：**禁用 LZO 压缩（与“禁用”相同）。
NAT	**开启：**开启 NAT 功能，允许内部设备共享公网 IP 进行 VPN 访问。 **关闭：**禁用 NAT，要求内部设备拥有自己的公网 IP 来访问 VPN。
TAP 绑定到 br0 网桥上	**开启：**将 TAP 虚拟以太网设备桥接到 br0 网桥，实现灵活的网络连接和数据转发。 **关闭：**禁用 TAP 到 BR0 桥接。
IP 地址	手动设置 OpenVPN 连接的 IP 地址。
子网掩码	定义分配的 IP 地址的子网掩码，确定网络和主机地址分段。
TUN MTU 设置	设置 tun 虚拟网络设备的最大传输单位（MTU）。默认值为 1500 字节。合理的 MTU 设置可以避免报文分片，提高传输效率。
UDP 隧道片段	**启用：**必要时允许 UDP 分片。 **Disable：**关闭 UDP 分片功能。

TCP MSS	**开启：** 设置 TCP 连接的最大段大小（MSS）以优化性能。 **关闭：** 关闭 TCP MSS 配置。
NS 证书类型	**开启：** 开启证书类型校验，增强连接安全性。 **关闭：** 关闭证书类型验证。
TLS 认证密钥	输入 TLS 验证密钥，用于协议验证和加密。
额外配置	允许根据特定要求输入自定义 OpenVPN 客户端配置参数。
基于路由策略	定义策略路由规则，根据指定的策略对网络流量进行控制。

2.3.4.4 IPSEC

- **全局设置**

配置影响整体 IPsec 的常规参数



项目	说明
NAT 穿越	**开启：**启用NAT 穿越，允许 IPsec 在具有网络地址转换（NAT）的网络中正常运行，确保兼容性。 **关闭：** 关闭 NAT 穿越功能。如果网络中存在 NAT 设备，则 IPsec 连接可能会失败。
日志等级	**基本：** 记录用于初始故障排除的关键调试信息。 **关闭：** 捕获更详细的日志，以便进行深入的调试。
证书管理	单击，进入证书管理界面，可以导入、导出、查看或删除 IPsec 相关证书，以保证连接的安全性。

- **隧道**

管理 IPsec 隧道配置。



项目	说明
全选	选中当前页面上所有的 IPSec 隧道表项进行批量操作。
新增	打开界面以创建新的 IPsec 通道配置。
删除	删除选定的 IPsec 隧道配置。

新增：

添加 IPsec 隧道配置



类型：

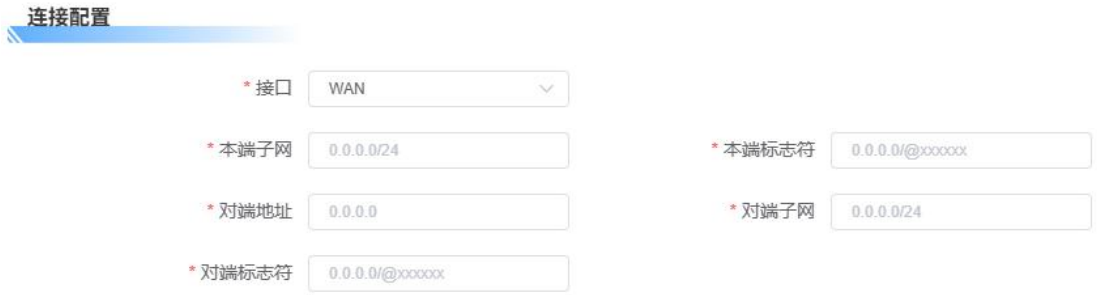
类型配置



项目	说明
启用	**开启：**激活 IPSec 隧道，允许建立安全连接。 **关闭：**禁用隧道，即使配置了隧道，也不能使用隧道。
名称	分配唯一名称以标识和管理 IPsec 隧道。
类型	Net-to-Net：连接两个独立的网络，实现站点到站点的 VPN 通信。 Host-to-Host **虚拟专用网：**在单个设备和另一台主机（通常是企业 VPN 服务器）之间建立安全连接。
功能	**客户端:**隧道作为客户端运行，启动与远程 VPN 服务器的连接 **服务端：**隧道充当服务器，处理传入的客户端连接以实现安全通信

连接配置：

对于连接配置



项目	说明
接口	选择用于 IPsec 连接的网络接口。
本端子网	定义本地网络的子网地址和掩码。
本地标志符	标识 IPsec 连接中用于身份验证和通信的本地设备。
对端地址	输入远程设备（例如 VPN 服务器）的公共 IP 地址以建立 IPsec 连接。
对端子网	指定远程网络的子网地址和掩码。
对端标志符	标识 IPsec 连接中用于身份验证和通信的远程设备。

检测

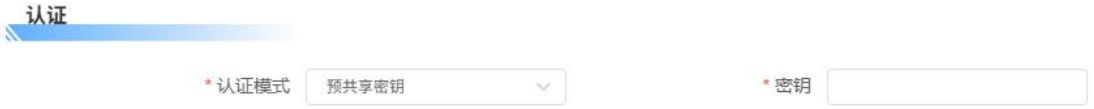
检测配置



项目	说明
启用 DPD 检测	**开启：**激活失效对等体检测（DPD）以监控远程设备的可用性。 **关闭：**关闭 DPD 检测功能。
时间间隔	定义 DPD 检测尝试的时间间隔。
超时时间	设置将对等设备标记为不可访问之前的最长等待时间。
操作	**Hold：**在检测到需要手动干预或进一步检测的问题时保持当前连接状态。 **Restart：**在连接失败时自动尝试重新启动 IPsec 隧道。 **Clear：**清除当前连接状态，以便重新建立连接。 **Restart by peer：**当检测到问题时，请求远程设备重新启动连接。
Ping 检测	**开启：**启用 ping 检测，允许路由器定期发送 ping 请求来监控连通性。 **关闭：**关闭 Ping 检测功能。
在线保持检测时间间隔	设置 ping 检测的频率。
IP 地址	指定 ping 请求的目标 IP 地址。
重连次数	定义连接失败后自动重新连接尝试的次数。

认证：

认证配置



项目	说明
认证模式	**预共享密钥：**使用共享密钥进行身份验证。双方必须配置相同的密钥才能建立安全连接。 **X.509 证书：**使用 X.509 数字证书进行身份验证，确保通过证书颁发机构（CA）颁发的证书进行身份验证。

2.3.4.5 GRE

GRE 是一种隧道协议，用于在 IP 网络中封装多种网络层协议，实现远程网络互联。



项目	说明
GRE 隧道	 **开启：**启用 GRE 隧道功能。 **关闭：**关闭 GRE 隧道功能。
全选	选中显示的所有 GRE 隧道配置表项，进行批量操作。
添加	打开接口以创建新的 GRE 隧道配置。
删除	删除选定的 GRE 隧道配置项。

新增：



项目	说明
名称	为 GRE 隧道指定唯一的名称，便于标识和管理。
启用	**开启：**表示激活 GRE 隧道，允许数据传输。 **关闭：**关闭隧道，即使配置了其他参数，也不发送数据。
通过	**PPP：**通过 PPP(Point-to-Point Protocol)协议封装和传输 GRE 隧道数据。 **LAN：**使用局域网进行数据传输，适合于同一网络中不同子网或设备的连接。 **WAN：**在广域网上建立 GRE 隧道，实现跨区域的网络互通。
对端 WAN IP	输入远程设备的 WAN IP（例如路由器）以建立 GRE 隧道连接。
对端子网	定义远程网络的子网和掩码。
对端隧道 IP	在 GRE 隧道中设置对端设备的 IP 地址。
本端隧道 IP	配置 GRE 隧道内本端设备的 IP 地址。

本地子网掩码	指定本地隧道 IP 的子网掩码以定义网络范围。
NAT	**开启：**开启 NAT 功能，允许多个内部设备共享一个公网 IP，通过 GRE 隧道进行通信。 **关闭：**禁用 NAT，要求内部设备具有单独的公共 IP 用于 GRE 隧道通信。
MTU	配置 GRE 隧道中数据的最大传输单元（报文大小）。
保活	**开启：**开启周期性的保持在线消息，监控和维护隧道连接。 **关闭：**关闭保持在线机制。
Ping 检测	**开启：**定期向目标发送 Ping 请求，以验证 GRE 隧道的连接状态。 **关闭：**关闭 Ping 检测功能。

2.3.4.6 EOIP

EOIP 是一种基于 IP 的隧道协议，用于连接远程局域网，实现跨网络二层通信。



项目	说明
全选	单击，选中当前页面中所有的 EOIP 隧道配置条目，进行批量操作。
新增	单击以打开用于创建新 EOIP 隧道配置的界面。
删除	单击可删除选定的 EOIP 隧道配置条目。

新增：



项目	说明
启用	**开启：**激活 EOIP 通道，允许以太网数据通过 IP 网络传输。 **关闭：**关闭 EOIP 通道。即使设置了其他参数，也不会发生以太网数据传输。
本端 IP 地址	指定 EOIP 通道中的本端设备 IP 地址，用于隧道内的标识。
远程 IP 地址	在 EOIP 通道中输入对端设备的 IP 地址，与本端设备建立通信。
桥接	**开启：**桥接 EOIP 隧道与本地网络，实现无缝数据转发和交互。 **关闭：**禁用桥接，使 EOIP 隧道独立于本地网络。数据交互可能需要额外的路由配置。

2.3.4.7 FRP

FRP 是一种内网穿透工具，可实现远程访问内网设备，支持 TCP/UDP 协议，常用于远程管理与服务映射。



项目	说明

启用	**开启：**启用 FRPC（快速反向代理客户端）功能，允许路由器作为客户端与 FRP 服务器通信，并执行反向代理相关业务。 **关闭：**关闭 FRPC 功能。路由器将不再充当 FRP 客户端，并且无法执行基于 FRP 的反向代理操作。
FRP 服务器地址	输入 FRP 服务器的 IP 地址或域名。此地址使路由器能够与 FRP 服务器建立连接以进行通信。
FRP 服务器端口	指定 FRP 服务器侦听的端口号。路由器将使用此端口进行通信，与服务器上配置的侦听端口相匹配。
FRP 远程访问密钥	FRP 客户端和服务器之间的验证密钥。FRPC 需要使用正确的 token 才能成功连接到 FRP 服务器并执行后续操作。
全选	点击此按钮，选择当前页面中所有与 FRP 相关的配置条目进行批量操作。
新增	单击此按钮将打开添加新的 FRP 相关配置的界面。
删除	单击此按钮将删除所选 FRP 相关配置项。

新增：



项目	说明
名称	为当前 FRP 配置项目指定名称，以便于识别。
本地 IP	指定本地设备（例如，服务器或主机）的 IP 地址。此地址标识本地网络中的本地服务，并允许 FRP 将外部请求转发到正确的设备。
本地端口	设置本地服务侦听的端口号。FRP 将传入的外部请求转发到此端口，并将它们定向到适当的本地服务。
远程端口	定义用于映射本地服务的 FRP 服务器上的端口号。外部用户可以通

	过连接到 FRP 服务器上的此端口来访问本地服务。

2.3.4.8 ZeroTier

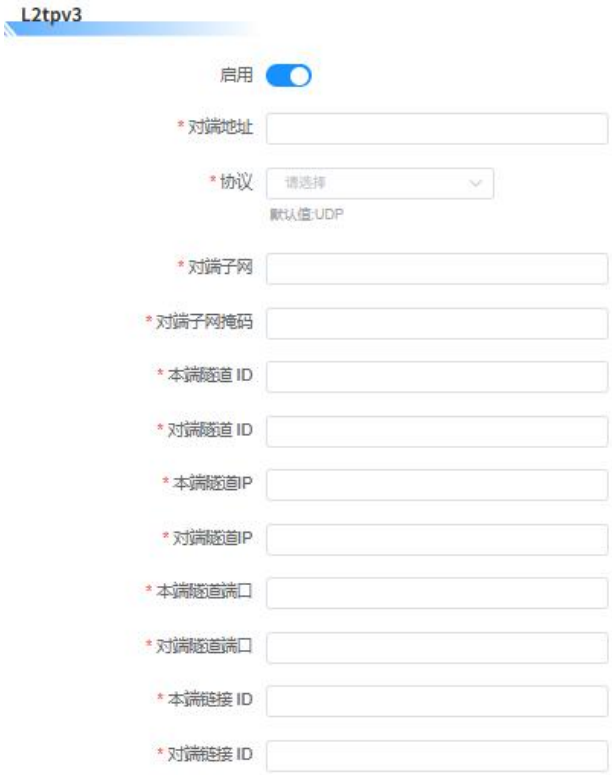
ZeroTier 是一种虚拟组网技术，实现跨地域设备安全互联，支持自动寻址、加密通信与灵活组网管理。



项目	说明
启用	**开启：**激活 ZeroTier 功能，允许路由器通过 ZeroTier 网络进行连接和通信。 **关闭：**禁用 ZeroTier 功能，防止路由器参与任何 ZeroTier 网络操作。
连接状态	显示路由器与 ZeroTier 网络之间的当前连接状态。
地址	指定与 ZeroTier 网络关联的地址。
重置	单击此按钮可将“地址”字段重置为其默认的未填充状态。
端口	定义用于与 ZeroTier 网络通信的端口号。
网络 ID	ZeroTier 网络的唯一标识符，用于区分不同的 ZeroTier 虚拟网络。加入特定网络时，请输入正确的网络 ID。

2.3.4.9 L2tpv3

L2TPv3 是一种隧道协议，用于在 IP 网络上传输二层数据，实现远程局域网互联与透明链路扩展。



项目	说明
启用	**开启：**启用 L2TPv3(Layer 2 Tunneling Protocol version 3)功能，使路由器能够建立安全的隧道连接进行数据传输。 **关闭：**关闭 L2TPv3 功能，禁止路由器进行隧道连接或相关数据传输。
对端地址	输入对等设备（例如远程路由器）的广域网(WAN)IP 地址，以建立 L2TPv3 隧道，这对于两台设备之间的通信是必要的。
协议	选择 L2TPv3 隧道的传输协议，默认选择 UDP。
对端子网	指定对等网络的子网地址，定义哪些对等设备可以通过此隧道进行通信以及对等网络的范围。
对端子网掩码	与“对等子网”一起定义网络掩码，进一步明确对等网络的结构和范围。
本端隧道 ID	本端设备在 L2TPv3 隧道中使用的 IP 地址，用于在隧道内传输数据

	时作为设备的标识。
对端隧道 ID	L2TPv3 隧道中对等设备的唯一标识符，与本地隧道 ID 一起使用，用于管理连接和控制数据传输。
本端隧道 IP	本地设备在 L2TPv3 隧道内使用的 IP 地址，用于在隧道内传输数据时标识设备。
对端隧道 IP	对端设备在 L2TPv3 隧道中使用的 IP 地址，便于与本端设备通信。
本端隧道端口	本端设备在 L2TPv3 隧道中接收和发送数据的端口号。
对端隧道端口	对端设备用于 L2TPv3 隧道连接的端口号，该端口号与本端隧道端口配合使用，实现双方设备之间的数据交互。
本端链接 ID	L2TPv3 隧道链路层本地设备的标识，用于链路层管理和控制数据转发。
对端链接 ID	L2TPv3 隧道链路层对端设备的标识，与本端链路 ID 共同保证链路层数据的正常传输。

2.3.4.10 WireGuard

WireGuard 是一种轻量高效的 VPN 协议，采用先进加密算法，实现安全、快速、简洁的网络通信。

- 服务器



项目	说明
启用	**开启：**激活 WireGuard 服务器功能，允许路由器作为 WireGuard 服务器运行，接受客户端连接并建立安全隧道。 **关闭：**禁用 WireGuard 服务器功能，阻止它接受客户端连接。
状态	显示 WireGuard 服务器的当前运行状态。

端口	设置 WireGuard 服务器侦听传入客户端连接的端口号。
本机地址	指定 WireGuard 服务器在本地网络中的 IP 地址，用于标识其位置。
私钥	WireGuard 服务器的私钥，用于在与客户端通信期间对数据进行加密和解密。它应该安全地存放。单击“生成”按钮将创建一个新的私钥。
公钥	从私钥派生的公钥，用于与客户端进行身份验证和安全密钥交换。
DNS	允许在 WireGuard 隧道内指定用于域名解析的 DNS 服务器地址，方便通过域名访问服务。
全选	单击此按钮将选择列表中的所有客户端配置项进行批量操作。
新增	单击此按钮将打开用于添加新客户端配置的界面。
删除	单击此按钮将删除选定的客户端配置项。

新增：



项目	说明
启用	**开启：**激活 WireGuard 客户端配置，允许它与服务器建立连接。 **关闭：**停用客户端配置，阻止连接到服务器。

名称	设置 WireGuard 客户端配置的名称，以便于识别和管理多个连接。
私钥	客户端的私钥，用于在与服务器通信期间对数据进行加密和解密。单击“生成”按钮将创建一个新的私钥。
公钥	客户端的公钥，用于与服务器进行身份验证和密钥交换。它必须与服务器上的相应配置匹配。
共享密钥	用于其他加密或身份验证方案的共享密钥。单击“生成”按钮将创建一个新的共享密钥。
保活	设置客户端和服务器之间发送 Keepalive 消息的时间间隔，以保持一个稳定的连接。
地址	指定客户端的 IP 地址或域名，由服务器用于标识和连接。
允许的 IP	定义允许客户端访问的 IP 地址或网段，以控制其网络范围。

- 客户端



项目	说明
启用	**开启：**激活 WireGuard 客户端功能，允许路由器与服务器建立安全连接。 **关闭：**禁用 WireGuard 客户端功能，阻止连接到服务器。
全选	单击此按钮可选择批操作的当前列表中的所有条目。
增加	单击此按钮，打开添加 WireGuard 服务器配置界面。
删除	单击此按钮可删除所选条目。

新增：



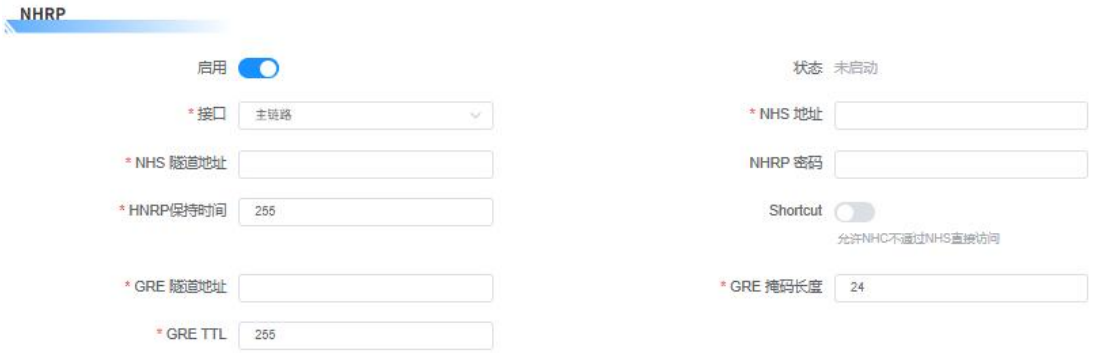
项目	说明
启用	**开启：**激活 WireGuard 服务器配置。 **关闭：**取消激活服务器配置。
从 conf 文件导入	单击“选择”以上传和导入预配置的 WireGuard 服务器配置文件。
ID	为 WireGuard 服务器配置分配唯一标识符。
服务器地址	指定用于建立连接的 FRP（快速反向代理）服务器的地址。
端口	设置 WireGuard 客户端连接到服务器的通信端口。
服务器公钥	输入 WireGuard 服务器的公钥以进行密钥交换和验证。
共享密钥	设置共享密钥以进行其他加密或身份验证。单击“生成”以创建新密钥。
本机私钥	用于加密和解密数据的 WireGuard 客户端的私钥。单击“生成”以生成新密钥。
保活	定义客户端和服务器之间发送 Keepalive 消息的时间间隔。
本机地址	指定 WireGuard 客户端在本地网络中的 IP 地址。
允许的 IP	添加允许客户端访问的 IP 地址或网段。
DNS	为 WireGuard 隧道内的域名解析配置 DNS 服务器。

2.3.4.11 DMVPN

DMVPN 是一种动态多点 VPN 技术，通过 NHRP 与 GRE 实现节点间自动建隧，支持灵活高效的组网通信。

- **NHRP**

NHRP 用于 DMVPN 中动态解析地址，建立直连隧道，提高转发效率，减轻中心负载，实现灵活高效的虚拟专网通信。



项目	说明
启用	开启：激活 NHRP。 关闭：取消 NHRP。
状态	显示 NHRP 的当前运行状态。
接口	选择参与 NHRP 的网络接口，分主链路和备链路
NHS 地址	配置 NHRP 服务器公网地址
NHS 隧道端口	配置 NHRP 服务器的隧道地址
NHRP 密码	输入 NHRP 通信认证密码
NHRP 保持时间	NHRP 映射信息保留时间
Shortcut	允许直连节点间快捷访问
GRE 隧道地址	本地 GRE 隧道虚拟地址
GRE 掩码长度	GRE 报文最大传输长度
GRE TTL	GRE 报文生存时间

2.3.5 NAT

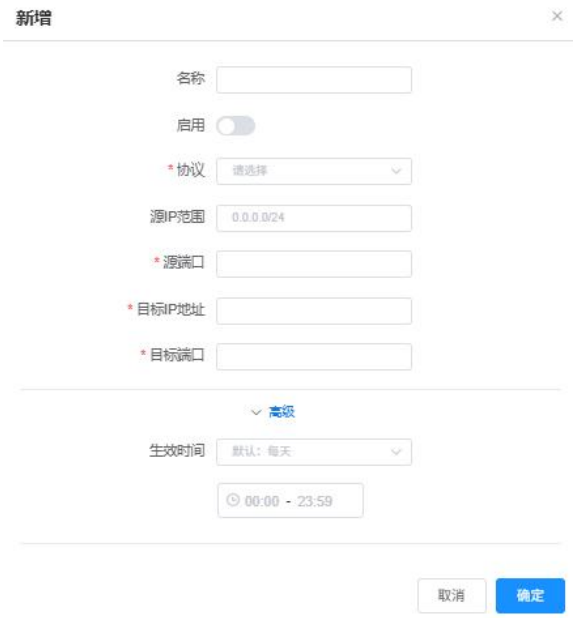
2.3.5.1 端口转发

- **端口转发**

端口转发用于配置公共网络服务，如 Web 服务器、FTP 服务器或其他需要外部访问的基于 Internet 的应用程序。



新增：



项目	说明
名称	输入应用程序的名称。
启用	打开或关闭端口转发。
协议	为应用程序选择 UDP、TCP 或两者。
源 IP 范围	指定 Internet 用户的 IP 地址。对于 IP 范围，请使用类似于 172.168.2.0/24 的格式，其中 172.168.2.0 是网络地址，24 是子网掩码长度。
源端口	输入服务使用的外部端口号。
目标 IP 地址	指定 Internet 用户要访问的服务器的内部 IP 地址。

目标端口	输入服务使用的内部端口号。
生效时间	设置规则处于活动状态的时间段。

- **端口范围转发**

某些应用程序需要转发特定范围的端口才能正常运行。当外部请求指向指定的端口范围时，路由器会将数据转发到指定的设备。出于安全原因，请将端口转发限制为仅必要的端口。如果不再需要配置，取消选中“启用”选项将暂时禁用转发规则。



新增：



项目	说明
名称	输入应用程序的名称。
启用	启用或禁用端口范围转发。
协议	根据需要选择 UDP、TCP 或两者。
开始端口	指定转发范围的起始端口。
结束端口	指定转发范围的结束端口。
目标 IP 地址	输入目标服务器的内部 IP 地址。
生效时间	设置转发规则的有效时间。

2.3.5.2 DMZ

DMZ 功能允许将网络上的指定设备暴露在 Internet 上以获得特定服务。DMZ 主机将所有端口转发到一台计算机，从而可以从 Internet 访问该计算机。虽然端口转发是一种更安全的选项，因为它只打开必要的端口，但启用 DMZ 会将设备暴露给所有传入的连接，从而增加安全风险。



项目	说明
使用 DMZ	**开启：**启用 DMZ，将指定的主机暴露在 Internet 上。 **关闭：**禁用 DMZ，使网络更安全。
DMZ 主机 IP 地址	指定被指定为 DMZ 主机的设备的 IP 地址，将其置于内部网络和外部网络之间，以便直接访问 Internet。

2.3.5.3 虚拟 IP 映射

虚拟 IP 映射将客户端访问的统一虚拟 IP，动态或静态映射到后端真实 IP，实现负载均衡、高可用性及流量透明转发。



新增：



项目	说明
虚拟 IP	指定在 NAT 过程中暴露给外部网络的 IP 地址。它映射到内部服务器的真实 IP，允许外部访问内部服务。
启用	**开启：**激活虚拟 IP 功能。 **关闭：**关闭虚拟 IP 功能。
实际 IP	内部服务器的实际 IP 地址。在 NAT 转换过程中，它被映射到虚拟 IP，使外部网络可以访问内部服务器。
目的 IP	需要访问的外部网络中的服务器或设备的目标 IP 地址。NAT 设置可以通过虚拟 IP 将内部请求路由到此目标。
接口	选择用于地址转换的网络接口： **lo**：Loopback 接口，主要用于内部设备通信和测试。 **br0**：桥接接口，用于连接局域网中的多个网络。 **WAN**：广域网接口，连接到外部网络（如 Internet），方便内部网络和外部网络之间的通信。

2.3.6 IPv6

IPv6 提供 128 位地址、内置安全、自动配置及高效路由，解决 IPv4 地址不足，实现可扩展、高效、安全的下一代互联网连接。

- IPV6 支持

支持 IPv6，包括路由器地址配置、128 位地址分配、自动或手动配置、高效路由与内置安全，实现可扩展、高效、安全的网络连接。



项目	说明
启用	**开启：**激活 IPv6 支持，允许路由器处理和传输 IPv6 网络数据。 **关闭：**禁用 IPv6 支持，将路由器限制为 IPv4 网络或排除

IPv6 类型	与 IPv6 相关的服务。 **来自 ISP 的本地 IPv6：**直接从 Internet 服务提供商（ISP）获取用于网络通信的本地 IPv6 地址。 **6in4 静态隧道：**将 IPv6 数据包封装在 IPv4 数据包中，实现 IPv4 网络上的 IPv6 通信。
前缀长度	定义 IPv6 地址前缀的长度。
静态 DNS1	指定用于 IPv6 网络中域名解析的主静态 IPv6 DNS 服务器的地址。
静态 DNS2	指定备用静态 IPv6 DNS 服务器的地址，当第一个服务器不可用时，用作域名解析的备份。
路由器 IPv6 地址	支持路由器 IPv6 地址配置，实现自动或手动地址分配与管理。
分配/路由前缀	输入 ISP 分配的或用于路由的 IPv6 地址前缀，这对于地址管理和网络配置至关重要。
MTU	设置允许在 IPv6 网络中传输的最大数据包大小。典型值为 1452 字节，有助于防止数据包分片，优化传输效率。

- WAN IPV6 地址配置

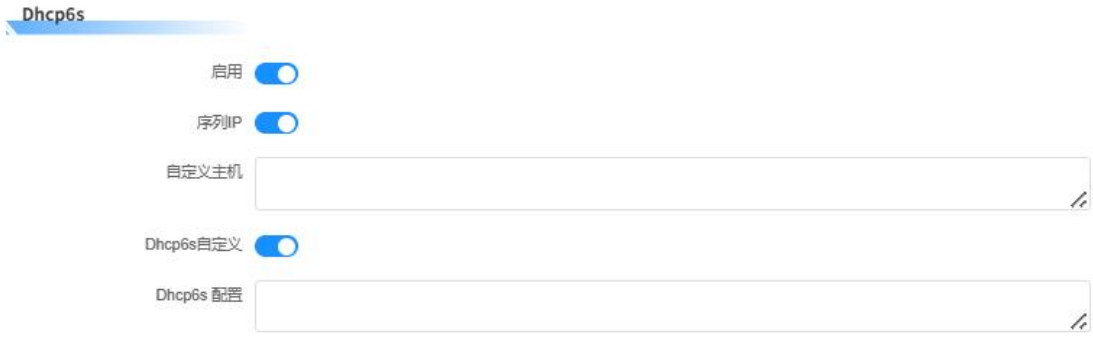
支持 WAN IPv6 地址配置，提供自动或手动分配、高效路由及内置安全，实现 IPv6 网络的可扩展、高效、安全连接。



项目	说明
WAN IPV6 地址配置	**使用 Autoconf：**通过 IPv6 协议自动获取 WAN IPv6 地址。路由器将从 ISP 检索地址信息，而无需手动配置。 **使用静态：**路由器使用无状态地址自动配置（SLAAC）来获取网络前缀信息并生成 IPv6 地址，通常是通过组合设备的 MAC 地址。这样就不需要手动配置地址。
获取 WAN IPV6 的方法	**使用 DHCPv6 客户端：**将路由器配置为 DHCPv6 客户端，以动态接收来自 DHCPv6 服务器的 WAN IPv6 地址和相关设置。此方法速度快，适用于支持 DHCPv6 的网络，类似于通过 DHCP 获取 IPv4 地址。 **使用 RS（路由器请求）：**路由器发送路由器请求消息，从网络中的其他路由器请求网络前缀和配置信息。然后，作为无状态地址自动配置过程的一部分，它使用获得的信息生成其 IPv6 地址。

- Dhcp6s

DHCPv6（dhcp6s）支持 IPv6 地址及网络参数自动分配，实现状态或无状态配置，简化网络管理并提升连接自动化与可靠性。



项目	说明
启用	**开启：**开启 DHCPv6 服务器，4G 工业路由器可以为局域网内的设备分配 IPv6 地址和网络参数。 **关闭：**禁用 DHCPv6 服务器，阻止路由器分配 IPv6 地址。
序列 IP	**开启：**启用 IPv6 地址的顺序分配，以便更好地管理和规划。 **关闭：**禁用顺序分配；可以根据其他规则分配地址。
自定义主机	允许为固定地址分配或设备标识指定自定义主机名到 IPv6 地址映射。
Dhcp6s 自定义	**开启：**启用自定义 DHCPv6 设置，允许个性化参数配置。 **关闭：**使用缺省 DHCPv6 配置。

- Radvd

RADVD 在 IPv6 网络中通过路由器通告广播前缀和网关，实现终端无状态自动地址配置及网络参数自动化管理。

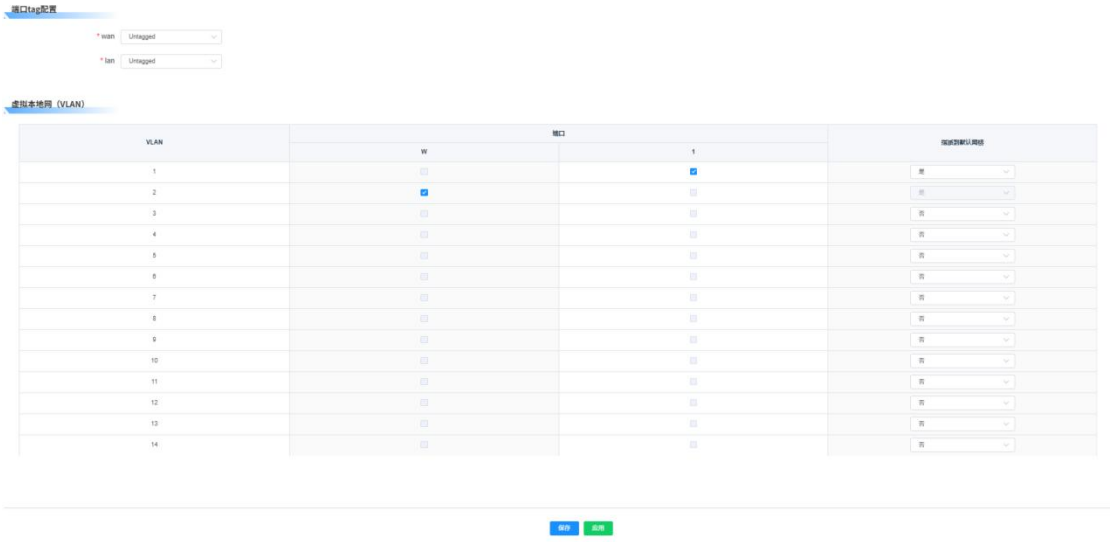


项目	说明
启用	**开启：**激活 Radvd（路由器通告守护程序），允许路由器

Radvd 已开启	在 IPv6 网络中发送路由器通告消息，通知设备网络前缀和路由信息。 **关闭**：关闭 Radvd 功能，路由器停止发送通告消息。 **开启**：启用自定义 Radvd 设置，允许对广告频率和内容等参数进行个性化调整。 **关闭**：使用默认 Radvd 配置，不进行自定义。

2.3.7 VLAN

VLAN 功能使用户可以根据自己的喜好对端口进行分段。系统最多支持 15 个 VLAN 端口（VLAN1 到 VLAN15），但只能配置两个端口：一个用于 WAN，一个用于 LAN。可以根据需要将这些端口分配给不同的 VLAN，但 LAN 和 WAN 端口不能属于同一个 VLAN。



2.3.8 网桥

网桥（Bridge）是一种二层网络设备，用于连接多个局域网（LAN），转发数据帧，实现不同网络段间通信与流量隔离。网桥连接多个局域网，按 MAC 地址转发数据，实现网络互通、流量隔离与局域网扩展。

2.3.8.1 网桥配置



点击“添加”按钮，将打开添加新网桥配置的界面，可以创建网桥并设置相关参数。



项目	说明
网桥名称	设置新桥的名称。
STP	**开启：**启用 STP(Spanning Tree Protocol)，通过阻塞某些端口来防止网络环路，从而确保无环路拓扑结构，从而实现稳定的网络通信。 **关闭：**关闭 STP 功能，如果网络中存在物理环路，可能会导致广播风暴等问题。
优先级	设置网桥的优先级，范围为 0-65535。值越小，网桥在路由计算中的优先级就越高。
MTU	指定网桥中允许的最大数据包大小，以优化网络性能并防止过大的数据包产生碎片。
IP 地址	定义网桥的 IP 地址，以便在网络中识别网桥。

子网掩码	与 IP 地址一起定义网络和主机范围，指定网桥所属的子网。
指派接口	允许将现有接口分配给已创建的网桥。

2.3.8.2 端口设置

网桥端口可配置为桥接或非桥接模式，支持加入/移除网桥，实现流量转发、隔离及网络拓扑灵活管理。



编辑：



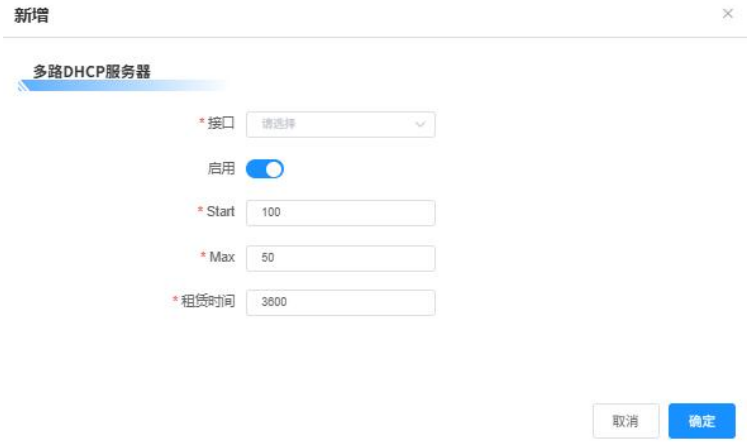
项目	说明
网络配置 eth2	**非桥接：**接口工作在非桥接模式，独立传输网络数据，不与其他接口桥接。这对于需要单独管理或隔离网络连接的情况非常理想。 **默认：**接口使用默认网络配置。
MTU	指定最大传输单位，它定义了可以传输的最大数据包大小。
组播转发	启用或禁用多播转发功能。
Masquerade/NAT	启用或禁用网络地址转换的伪装/NAT。
IP 地址	设置 ra0 接口的 IP 地址，确保与其他端口或网桥不冲突。
子网掩码	配置端口的子网掩码。

- **DHCPD**

DHCPD 自动分配 IP 地址及网络参数，支持 IPv4/IPv6，实现客户端地址管理自动化和网络连接简化。



新增：



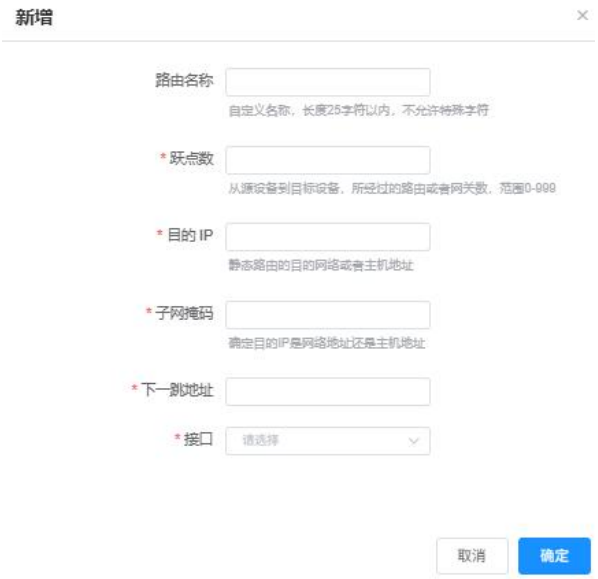
项目	说明
接口	选择启用多 DHCP 服务器功能的网口。必须选择正确的接口，才能允许 DHCP 服务器将 IP 地址分配给连接到此接口的设备。
启用	**开启：**激活当前的多 DHCP 服务器配置，允许路由器为选定接口上的设备分配网络参数（如 IP 地址）。 **关闭：** 禁用此配置，停止路由器通过此接口提供 DHCP 服务。
Start	定义 DHCP 范围的起始 IP 地址。
Max	指定可以分配 IP 地址的 DHCP 客户端的最大数量。
租赁时间	设置 DHCP 客户端的租用时间（以分钟为单位）。

2.3.9 高级路由

在“高级路由”页面上，您可以配置工作模式和静态路由。对于大多数用户，建议使用默认网关模式。



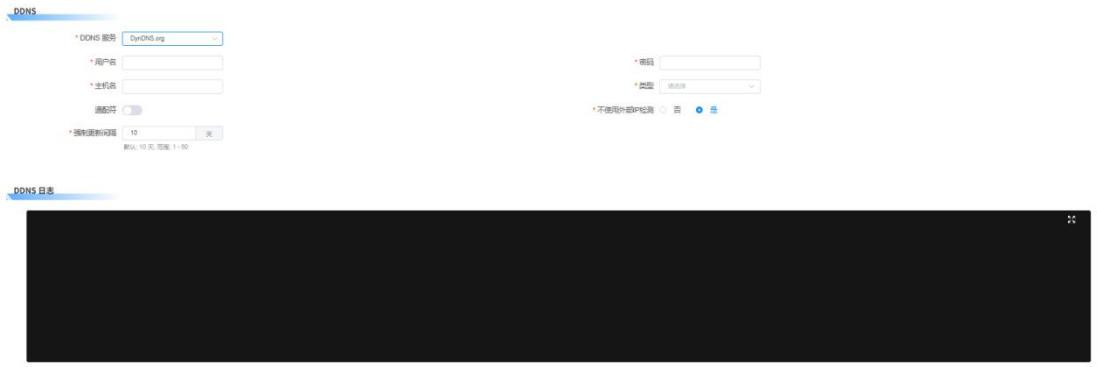
点击“新增”，添加静态路由相关配置



项目	说明
路由名称	路由的用户定义名称（最多 25 个字符）。
跃点数	从源到目的的跳数（范围：0-9999）。
目的 IP	静态路由的目标网络或主机 IP 地址。
子网掩码	定义目标 IP 的网络和主机部分的子网掩码。
下一跳地址	启用与目标通信的网关设备的 IP 地址。
接口	根据目标 IP 位置选择适当的接口（LAN、无线、WAN 或其他端口）。

2.3.10 DDNS

DDNS（动态域名服务）将动态变化的 IP 地址绑定到固定域名，实现远程访问、主机定位和网络服务持续可用性。



项目	说明
DDNS 服务	支持多种 DDNS 提供商，包括 DynDNS、FreeDNS、ZoneEdit、No-IP、3322、easyDNS、TZO 和 DynSIP。还可以配置自定义 DDNS 服务器。
用户名	DDNS 服务的注册用户名（最多 64 个字符）。
密码	密码与 DDNS 帐户相关联（最多 32 个字符）。
主机名	主机名由 DDNS 提供程序分配（没有特定的长度限制）。
类型	DDNS 服务类型，因提供商而异。
通配符	启用通配符支持（默认值：OFF）。如果设置为 ON,*.host.3322.org 将被视为 host.3322.org。
不使用外部 IP 检测	启用或禁用外部 IP 检测。
强制更新间隔	强制在指定的天数内更新 DDNS。

2.3.11 MAC 地址克隆

某些 ISP 要求 MAC 地址注册。为了避免重新注册，您可以克隆路由器的 MAC 地址，以匹配已在 ISP 注册的 MAC 地址。



MAC 地址克隆可以应用于 LAN 和 WAN 端口。关键注意事项：

1. MAC 地址是 48 位，不能是多播地址，这意味着第一个字节必须是偶数。
2. MAC 地址必须是合法的，不能随意分配。

2.4 数据采集

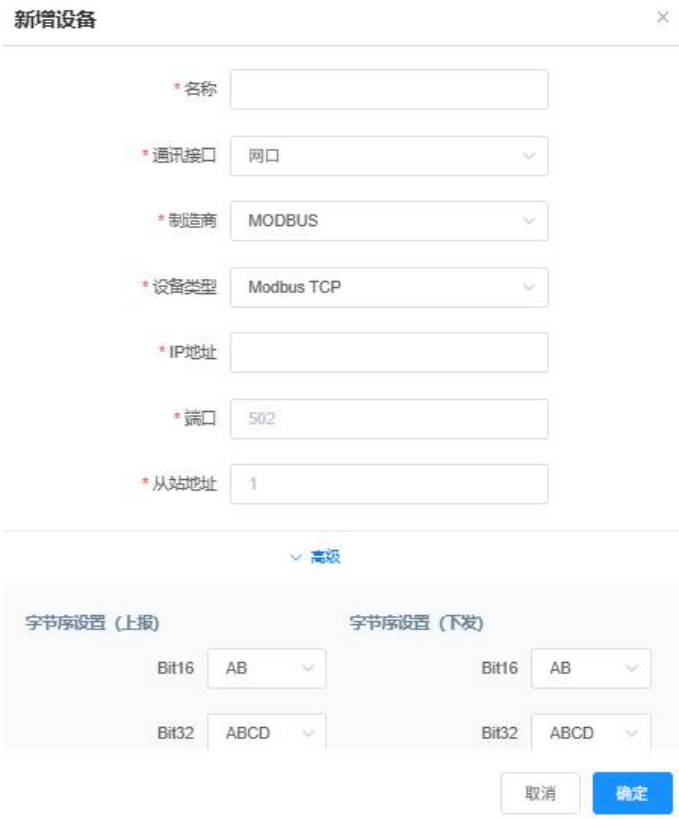
FNR310 支持各种工业设备的运行数据采集。本章概述了工业设备的数据采集和配置。

2.4.1 子设备

数据采集子设备用于连接各类传感器或终端设备，采集实时数据，通过路由器上传，实现远程监控、分析与智能管理。



新增：



项目	说明
名称	添加的子设备（通常是工业设备）的可自定义名称。
通讯接口	选择连接类型，包括以太网、RS232/A1B1 或 TTL232。

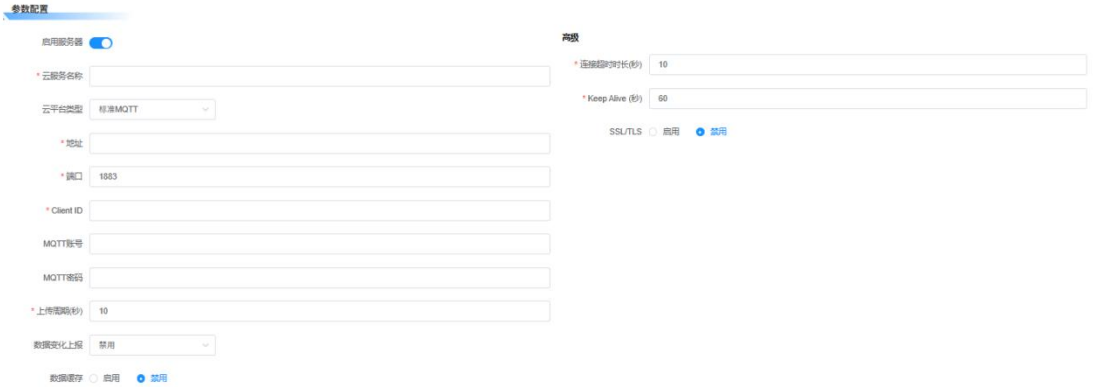
制造商	选择设备制造商或协议。
设备类型	指定设备的通信协议。
IP 地址	输入设备的 IP 地址以进行网络识别。
端口	指定设备通信的端口号。
从站地址	在 Modbus 通信中，它标识设备号。设备通过站号进行区分，默认设置为“1”。
高级	设置字节序上报和下发的类型

2.4.2 云服务

云服务支持添加云服务器、管理变量列表，自动上传采集数据，支持历史数据存储、远程监控、固件升级及安全加密传输。



添加云服务器参数配置：

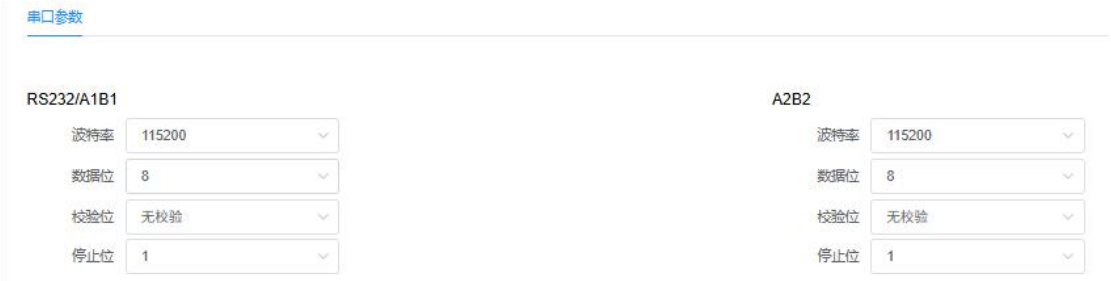


项目	说明
启用	**开启：**启用云服务功能 **关闭：**关闭云服务功能

云服务名称	输入云服务的名称。
云平台类型	选择云平台类型，包括 MQTT、HTTP、TCP/UDP 或第三方平台。当前设置为“标准 MQTT”。
地址	输入云平台的网络地址。
端口	指定云通信的端口号。
客户端 ID	云平台上设备的唯一标识，用于设备管理。
MQTT 账号	用于登录云平台的帐户。
MQTT 密码	MQTT 身份验证的相应密码。
上传周期(s)	定义将数据上载到云的时间间隔（以秒为单位）。
数据变化上报	启用时，设备将向云报告数据更改；禁用时，设备不报告。
数据缓存	启用时，设备会临时存储数据；禁用时，会关闭缓存。
连接超时时长（秒）	设置云连接的超时时间。
Keep Alive(s)	定义 MQTT 心跳间隔，以保持连接的稳定性。
SSL/TLS	启用时，激活 SSL/TLS 加密以确保数据传输安全；禁用时，不使用加密。

2.4.3 接口设置

接口设置支持配置 RS232 和 RS485 串口参数，包括波特率、数据位、校验位和停止位，实现串口设备的灵活连接与通信管理。



项目	说明
波特率	定义串行通信中的数据传输速率，以波特为单位。设置为 115200，表示每秒传输 115200 个符号。两个通信设备必须使用相同的波特率才能正常通信。
数据位	指定每个数据帧中的有效数据位数。
校验位	数据传输中的错误检测方法。“无”表示不执行奇偶校验。

停止位	指示串行通信中数据帧的结束。

2.4.4 协议转换

协议转换功能支持 MODBUS TCP/RTU、IEC104、IEC101、DNP3.0、OPC UA、HJ212，可配置各协议参数，实现不同工业设备和系统间的数据互通与集成。

2.4.4.1 Modbus TCP

MODBUS TCP 是一种基于以太网的工业通信协议，用于主从设备间数据传输，实现实时监控与控制。



- **从站配置**

MODBUS TCP 从站可配置 TCP 模式、监听端口和从站 ID，实现主站访问、数据响应与实时通信管理。



项目	说明
启用	**开启：**启用从站配置功能 **关闭：**关闭从站配置功能
TCP 模式	定义设备在 Modbus TCP 通信中的角色。在“TCP 服务器”模式下，设备侦听传入的连接请求。在“TCP 客户端”模式下，设备主动向指定的服务器发起连接。
监听端口	在“TCP 服务器”模式下运行时，此选项设置用于侦听连接请求的端口号。默认值为 502，即 Modbus TCP 的标准端口。
站号	识别 Modbus 通信中的从机设备。每个从机都有一个唯一的站号，允许主设备识别并与之正确通信。

- **映射变量**

MODBUS TCP 映射变量功能支持将设备寄存器与系统变量对应，实现数据采集、监控及控制的实时映射与管理。



单击“新增”以配置映射变量。



2.4.4.2 Modbus RTU

Modbus RTU 是一种串行通信协议，支持主从设备间数据传输，实现工业设备实时监控与控制。



- **从站配置**

Modbus RTU 从站可配置通讯接口和站号，实现主站访问和设备数据实时响应管理。



项目	说明
启用	**开启：**启用从站配置功能

	关闭：关闭从站配置功能
通讯接口	选择设备通信的物理通道。
站号	用于设备识别、安全验证或启用特定功能的配置参数。

- **映射变量**

Modbus RTU 映射变量功能将设备寄存器与系统变量对应，实现数据采集、实时监控及控制管理。



单击“新增”允许您配置映射变量。



2.5 应用设置

应用设置功能包含活动策略、安全策略与 QOS 管理。活动策略支持定时重启和定时任务；安全策略可设置 IP、URL、MAC 限制、防火墙、证书及 WEB 访问；QOS 支持主备链路及上下行带宽配置，并可按 NETMARK 和 MAC 优先级分类管理。

2.5.1 活动策略

2.5.1.1 定时重启

定时重启功能可设置设备在指定时间自动重启，提升系统稳定性并防止长期运行导致性能下降。



项目	说明
定时重启	用于启用或禁用路由器的定时重新启动功能的切换。如果启用，路由器将根据指定的计划重新启动；如果禁用，路由器将不会自动重新启动。
选择方式	选择定时重新启动的触发方法。下拉菜单中提供了各种触发选项： **间隔若干秒后重启：**选择此选项，使路由器以指定的间隔（以秒为单位）循环重新启动。 **定时重启：**设置路由器重新启动的特定日期和时间。
间隔（秒）	设置定时重启的间隔时间，单位为秒

2.5.1.2 定时任务

用户可以在此处添加计划任务，例如自动重启任务。



2.5.2 安全策略

安全策略支持设置 IP、URL、MAC 限制，配置防火墙、证书管理及 WEB 访问控制，提升网络访问安全性与设备防护能力。

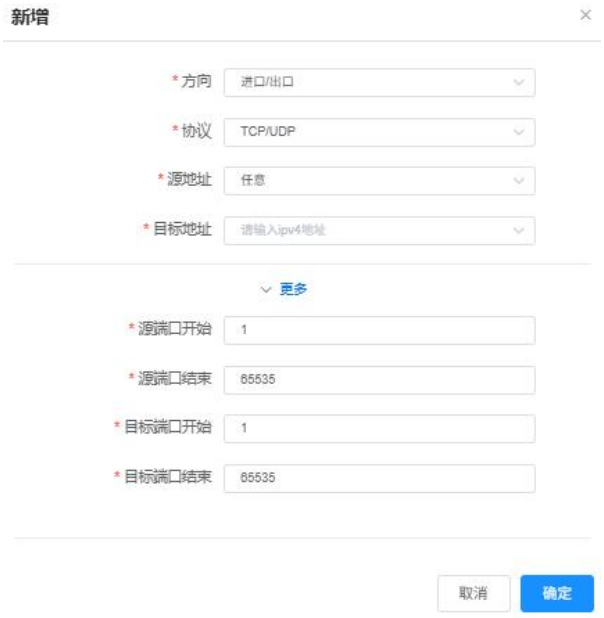
2.5.2.1 IP 限制

IP 限制功能可设置允许或禁止的 IP 地址范围，控制访问权限，保障网络安全与设备防护。



项目	说明
启用	一个开关选项。启用时，IP 限制功能被激活，根据配置的规则限制 IP 相关的访问。禁用时，将关闭 IP 限制，并且不应用任何限制规则。
策略	选择 IP 限制的策略模式。

单击“新增”允许您配置 IP 限制。



项目	说明
新增	单击此按钮，打开增加新的 IP 限制规则界面。
方向	定义数据传输的方向。
协议	选择要应用限制规则的网络协议。
源地址	定义发起访问的设备 IP
目标地址	指定被访问的设备或服务器 IP
源端口开始	设置源端口范围的起始端口号。
源端口结束	设置源端口范围的结束端口号。
目标端口开始	设置目标端口范围的起始端口号。

目标端口结束	设置目标端口范围的结束端口号。

2.5.2.2 URL 限制

URL 限制功能可设置允许或禁止访问的网页地址，实现精确访问控制，保障网络使用安全。



项目	说明
启用	一个开关选项。启用时，URL 限制功能被激活。禁用时，URL 限制将关闭。
策略	选择 URL 限制的策略模式。
新增	单击此按钮，打开添加新 URL 限制规则的界面。
URL 地址	输入限制的 URL 或策略链接。

2.5.2.3 MAC 限制

MAC 限制功能可设置允许或禁止的设备 MAC 地址，实现基于物理地址的访问控制，提升网络安全性。



项目	说明
启用	一个开关选项。启用时，MAC 限制功能被激活。禁用时，“MAC 限制”将关闭。
策略	选择 MAC 限制的策略模式。
新增	单击此按钮，打开添加新的 MAC 限制规则界面。
MAC	输入要应用策略的 MAC 地址。

2.5.2.4 防火墙

防火墙功能提供 SPI 防火墙和 DDOS 防护，支持附加过滤器设置，可阻止来自 WAN 口的非法请求，并限制 WAN 侧 DOS 及暴力破解攻击，保障网络安全稳定。



项目	说明
SPI 防火墙	一个开关选项。启用时，SPI（状态数据包检测）防火墙被激活。禁用时，防火墙功能关闭。
DDoS 防御	选择 DDoS（分布式拒绝服务）防御的策略模式，以防止潜在的 DDoS 攻击。
过滤器代理	单击按钮，打开增加新的 MAC 限制规则界面，可以增加新的 MAC 限制规则。
过滤 Cookie	启用后，路由器将阻止包含 Cookie 的网络流量，以防止隐私泄露或恶意跟踪。
过滤 Java Applets	启用后，路由器会阻止包含 Java 小程序的网络流量，以防止潜在的安全风险，例如恶意代码执行。
过滤 ActiveX	启用后，路由器会阻止包含 ActiveX 控件的网络流量，以防止未经授权的系统访问等安全问题。
阻止来自 WAN 口的匿名请求(ping)	启用后，路由器会阻止来自广域网的匿名 ping 请求，从而防止网络探测和潜在攻击。
过滤 DENT（端口 113）	启用后，路由器会通过端口 113 过滤与 ident 协议相关的流量，以防止安全威胁，例如未经授权的用户身份查询。
阻止 WAN SNMP 访问	启用后，路由器会阻止对简单网络管理协议（SNMP）的广域网访问，防止未经授权的访问或篡改网络管理信息。

限制 SSH 访问	启用后，路由器会限制 SSH（安全外壳协议）访问。您可以设置规则，例如限制对特定 IP 的访问或限制连接频率，以防止暴力破解 SSH 攻击。
限制 Telnet 访问	启用后，路由器会限制 Telnet（远程登录协议）访问，您可以设置规则以防止未经授权的远程登录，因为 Telnet 由于其未加密的数据传输而不太安全。
限制 PPTP 服务器访问	启用后，路由器会限制对 PPTP（点对点隧道协议）服务器的访问，以防止未经授权的用户建立隧道连接。
限制 L2TP 服务器访问	启用后，路由器会限制对 L2TP（第 2 层隧道协议）服务器的访问，防止未经授权的用户建立隧道连接并增强网络的安全性。

2.5.2.5 证书管理



本节主要介绍证书管理和相关参数的配置。

2.5.2.6 WEB 访问

WEB 访问功能支持本地与远程 WEB 访问，可配置管理协议，实现设备界面管理与远程 HTTP 控制。

- **WEB**

WEB 功能支持 HTTP/HTTPS 协议、端口及证书管理，并可设置登录超时、异常登录限制与安全策略，保障访问安全。





项目	说明
Web 界面管理	**开启：**启用 WEB 界面管理，实现设备通过网页进行配置和管理。 **关闭：**关闭 WEB 界面管理
协议	选择用于访问路由器 Web 管理页面的协议。"HTTP"是标准协议，而"HTTPS"使用 SSL/TLS 加密提供安全连接。如果选择了 HTTPS，则必须选择有效的证书（可在证书部分中管理）。
HTTP 端口	配置用于通过 HTTP 访问路由器网页的端口，默认情况下通常设置为端口 80。
HTTPS 端口	配置用于通过 HTTPS 访问路由器网页的端口，默认情况下通常设置为端口 443。
证书	选择用于安全 Web 访问的 HTTPS 证书。
用户自动登出时间设置	设置用户无操作自动登出时间，防止会话滥用。
登录间隔限制	限制连续登录间隔，防止频繁登录攻击。
异常次数判断	设置异常登录次数阈值，触发安全防护措施。
异常登录间隔限制	设置异常登录的最小间隔，防止暴力破解攻击。
异常登录重置时间	设置异常登录计数重置时间，恢复正常登录尝试。

- **远程WEB**



项目	说明
远程 HTTP 管理	开启：启用远程 HTTP 管理 关闭：关闭远程 HTTP 管理

2.5.3 QOS

QOS 功能支持主备链路及 HTB 上下行带宽配置，并可按 NETMARK 和 MAC 优先级分类管理，实现流量优化与网络性能保障。

2.5.3.1 QOS 基本设置

QOS 基本功能支持配置主链路与备链路，并设置 HTB 上下行带宽，实现带宽分配管理与网络流量优化。

- **主链路**

表示主链路配置



项目	说明
启用	打开或关闭主链路的 QoS 功能。启用后，它将根据设置的参数管理网络流量。禁用时，QoS 功能处于非活动状态。
端口	选择主链路的端口。默认选项是“WAN”（广域网）。
数据包调度器	选择用于管理和调度数据包的算法。HTB(Hierarchical Token Bucket)常用于分层流量控制。
最高上传(kbps)	输入上行链路带宽值，通常为最大可用带宽的 80%到 90%。

最高下载(kbps)	输入下行带宽值，一般为最大带宽的 80%~90%。

- **备链路**

表示备份链路配置



项目	说明
启用	打开或关闭备链路的 QoS 功能。启用后，它将根据设置的参数管理网络流量。禁用时，QoS 功能处于非活动状态。
端口	选择备链路的端口。默认选项是“WAN”（广域网）。
数据包调度器	选择用于管理和调度数据包的算法。HTB(Hierarchical Token Bucket)常用于分层流量控制。
最高上传(kbps)	输入上行链路带宽值，通常为最大可用带宽的 80%到 90%。
最高下载(kbps)	输入下行带宽值，一般为最大带宽的 80%~90%。

- **HTB优先级设置上行**

通过 HTB 算法设置上行流量的优先级。



- **HTB优先级设置下行**

通过 HTB 算法设置下行流量的优先级。



2.5.3.2 QOS 分类设置

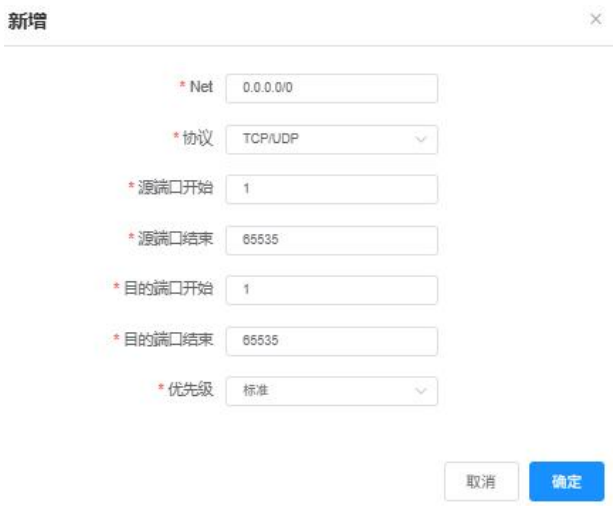
QOS 分类功能可按 NETMASK 和 MAC 优先级对流量进行分类管理，实现数据包优先处理与网络性能优化。

- **NETMASK 优先顺序**

NETMASK 优先顺序功能可根据数据包标记设置优先级，实现不同类型流量的优先处理与网络带宽优化管理。



点击“新增”，添加 NETMASK 优先顺序相关配置



项目	说明
NET	指定 IP 地址范围。“0.0.0.0/0”匹配所有 IP 地址。
协议	选择应用 QoS 规则的网络协议。
源端口开始	设置源端口范围的起始端口号（1-65535）。

源端口结束	设置源端口范围的结束端口号（1-65535）。
目的端口开始	设置目的端口范围的起始端口号（1-65535）。
目的端口结束	设置目的端口范围的结束端口号（1-65535）。
优先级	设置网络流量的优先级。

- **MAC 优先顺序**

MAC 优先顺序可根据设备 MAC 地址设置流量优先级，实现关键设备数据优先传输和网络带宽优化管理。



点击“新增”，添加 MAC 优先顺序相关配置



项目	说明
MAC 地址	指定 MAC 地址。
优先级	设置网络流量的优先级。

优先级说明：

该系统提供了五个优先级。“不受限”优先级独立于其他四个优先级，即：高级（高优先级）、快速（优先）、标准和低（低优先级）。

不受限：

处于不受限优先级的数据流仅受硬件功能的限制。不受限带宽与其他四个优先级的关系如下：

- Max_Up：上传总带宽
- Max_Down：下载总带宽
- 上行：“QoS设置”中的上传限制
- 下行：“QoS设置”中的下载限制

- Exempt_Rate_Up:Exempt数据流的上传流量速率
- Exempt_Rate_Do：表示Exempt数据流的下载流量速率

那么其他优先级的上传总带宽为：
min（Max_Up-Exempt_Rate_Up，上行链路）
其他优先级的总下载带宽为：
min（Max_Down-Exempt_Rate_Do，下行）

在分配豁免数据流之后，剩余带宽将在其他优先级之间分配。例如，如果剩余的上传和下载带宽为 1000 kbps，并且存在四个优先级分别为“高优先”、“优先”、“标准”和“低”的数据流，则分配如下：

- 高优先：（75/100）*上行链路，（75/100）*下行链路
- 优先：（15/100）*上行链路，（15/100）*下行链路
- 标准：（10/100）*上行，（10/100）*下行
- 低：1000位（接近0）;1000位（接近0）

对于低优先级，其上传和下载速率最低，仅在其他优先级数据流处理完毕后才提供服务。当只有一个数据流处于活动状态时，其带宽仅由“QoS 设置”中的上传和下载限制控制。

注意：如果连接同时满足 MAC 优先级和网络掩码优先级的控制条件，则首先添加的规则优先。

2.5.4 位置信息获取设置（GNSS）

本页面用于配置设备的 GNSS（全球导航卫星系统）数据采集、上报策略及输出格式。通过此设置，设备可将位置信息通过网络或串口实时上传至服务器或本地终端。

2.5.4.1 基础配置

- **位置信息获取设置：**



开启或关闭设备的 GPS 位置信息采集功能。开启后，设备开始解析 GPS 信号；关闭则停止所有位置数据处理。

2.5.4.2 数据上报通道设置

- **上报至网络:**



开启后，设备将通过网络（TCP/UDP）将 GPS 数据发送至指定的服务器。

项目	说明
数据传输协议	设置传输协议，支持 TCP 或 UDP。
中心服务器地址	填写接收数据的服务器 IP 地址。
中心监听端口	填写服务器的监听端口。

- **上报至串口:**



开启后，设备将通过本地串口输出 GPS 数据。当开启此项时，需配置以下参数以确保数据传输正常：

项目	说明
波特率	设置数据传输速率（如 115200）
数据位	设置数据位的长度（通常为 8）
停止位	设置停止位长度（如 1）
校验位	设置校验方式（如 None）
流控	设置流控制方式（如 None）

2.5.4.3 采集与过滤策略

- **信息更新间隔：**



设置 GPS 数据的上报时间间隔（单位：秒）。数值越小，实时性越高，但会增加流量消耗。

- **位移速度阀值：**



设置最低速度过滤阈值。设备会将解析出的 RMC 数据中的速度与此值进行比较。若当前速度低于该阈值，则视为静止状态，设备将停止上报数据，以节省流量。

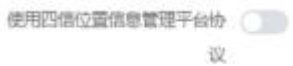
2.5.4.4 高级功能与数据格式

- **信息中添加设备 ID：**



开启后，在每个发送的 GPS 数据包尾部自动附加设备唯一 ID，便于服务器侧进行多设备区分与管理。

- **使用四信位置信息管理平台协议：**



开启后，设备将采用四信 7113 通信协议格式进行 GPS 数据打包及上报。

- **GNSS 信息类型选择：**



支持勾选所需的 NMEA 语句类型，包括 RMC、GGA、VTG、GSA、GSV、GLL。系统将仅根据您的勾选内容生成数据包，提高数据处理效率。

注意事项：

1. 请确保“中心地址”与“中心端口”配置正确，否则网络上报将无法到达服务器。
2. 串口参数（波特率、数据位等）必须与接收终端的设置完全一致，否则会导致乱码或无法通讯。
3. 若您有特定的平台对接需求，请优先确认是否需要开启“使用四信位置信息管理平

台协议”功能。

2.6 串口应用

2.6.1 串口应用

该设备具有一个 RS-485 串行端口和一个 RS-232 串行端口，均用于数据传输。它包括一个内置的串行到 TCP/IP 程序，并支持多服务器中心功能，使来自 COM1 和 COM2 的数据可以定向到任何指定的数据中心。

- **串口应用**

串口应用功能支持添加删除配置，并设置协议类型、服务端地址端口、心跳包间隔及设备号码。



点击“新增”，添加串口应用相关配置



项目	说明
协议类型	选择协议类型。
服务器地址	输入数据服务中心的 IP 地址或域名，以便与路由器的 Serial-to-TCP 程序进行通信。
服务器端口	指定数据服务中心程序监听的端口。
设备号码	设置设备的 11 字节 ID 号。此选项仅在协议类型设置为“UDP(DTU)”或“TCP(DTU)”时适用。
心跳包间隔	设置发送心跳报文的时间间隔。此选项仅在协议类型设置为“UDP(DTU)”或“TCP(DTU)”时适用。

- **接口选择及模式选择**

串口应用接口与模式支持配置 RS232/RS485 数据位、波特率、停止位、流控、校验及通信中心绑定。



项目	说明
通信中心绑定	连接通信中心，对应于串行应用程序中设置的通信中心。
波特率	指定数据传输速度（以字节/秒为单位）。常见的波特率有 115200、57600、38400、19200 等。
数据位	定义每个字符中的位数，通常为 7 或 8。它通常以 ASCII 表示，并从最低有效位开始传输，由时钟同步。
停止位	指示字符数据的结束，通常设置为 1 或 2 个高电平位。
检验	指数据集的错误检查方法。选项包括奇偶校验或奇偶校验。
流控	流量控制，包含管理数据流的硬件和软件方法。

2.6.2 短信应用

短信应用功能支持应用设置、规则配置及定时管理，支持短信发送、转发至 HTTP、短信或 Email，兼容 SMPP 协议，并可监控数据流量。

- **短信应用**

短信应用功能支持新增和删除接收短信的手机号码，可设置对应名称及手机号码，实现灵活管理和消息发送目标设置。



单击“新增”以包括应接收短信的电话号码。



- **短信规则**

短信规则功能支持新增和删除规则，设置规则名称、触发机制及发送内容，实现自动化短信通知管理。



单击“新增”以设置短信的除非动作及相关内容设置。



项目	说明
名称	设置短信规则的名称
动作	选择将触发短信通知的事件。
短信内容	输入短信通知的内容。
启用	启用改短信规则

- **短信转发 HTTP**

短信转发 HTTP 功能支持配置转发标识、URL 和方式，并可新增或删除相关手机号码及名称，实现短信自动 HTTP 转发。



项目	说明
短信转发 HTTP	用于通过 HTTP 协议启用或禁用 SMS 转发的切换选项。启用时，路由器根据设置将短信内容转发到目标服务器；禁用时，关闭短信转发功能。

URL	输入将接收转发 SMS 内容的目标服务器的 URL。
方法	选择短信转发的 HTTP 请求方法。
消息值名称	为短信内容定义自定义参数名称，帮助接收服务器识别和处理短信相关数据。
转发 HTTP 标识符	指定 SMS 转发中使用的 HTTP 请求的标识符。这可用于区分不同的转发任务或有效地管理它们。

单击“新增”以包括应接收短信的电话号码。



- **短信转发短信**

短信转发短信功能可将接收短信自动转发至指定号码，支持同步设置手机号码、名称及接收者，禁用时关闭转发。



项目	说明
短信转发短信	用于启用或禁用短信转发的切换选项。启用时，路由器会根据设置将接收到的短信转发到指定号码；禁用时，短信转发将关闭。
短信转发标记	输入自定义标识符，以区分特定的短信转发任务，帮助管理和识别。
收件人电话号码	用于启用或禁用收件人电话号码设置的切换选项。启用时，可以指定收件人；禁用时，此设置处于非活动状态。

单击“新增”以包括应接收短信的电话号码。



- **短信转发电子邮件**

路由器可将接收到的短信通过电子邮件转发，支持设置 SMTP 服务器、端口、用户名、密码、发件邮箱及收件邮箱等参数。



项目	说明
SMTP 服务器	输入用于发送邮件的 SMTP 服务器地址，该地址是短信转邮件功能所需的。
SMTP 服务器端口	指定 SMTP 服务器的端口号。
用户名	SMTP 服务器的登录用户名。
密码设置	SMTP 登录用户名对应的密码，保证邮件传输安全。
电子邮件来自	指定用于转发 SMS 消息的发件人电子邮件地址。
发送电子邮件至	输入收件人的电子邮件地址，用于发送转发的 SMS 消息。
接收名称	（可选）输入要在电子邮件中显示的收件人姓名。
电子邮件主题	指定电子邮件的主题行，以便为收件人摘要其内容。
电子邮件标记	（可选）输入自定义标识符以区分特定的 SMS 到电子邮件转发任务。

- **短信定时管理**

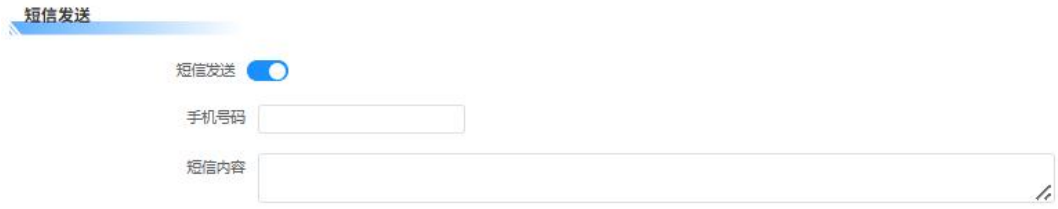
路由器支持短信定时发送功能，可设置短信发送间隔、定时发送内容，并可新增接收短信的手机号码及名称。



项目	说明
间隔(s)	设置发送 SMS 消息的时间间隔（以秒为单位），以确定调度 SMS 传输的频率。
定时短信内容	输入要在定义的时间间隔发送的预定 SMS 消息的文本内容。

- **短信发送**

路由器支持手动发送短信功能，可设置短信内容及接收短信的手机号码。



项目	说明
手机号码	输入 SMS 收件人的手机号码。
短信内容	输入要发送的短信。

- **短信白名单**

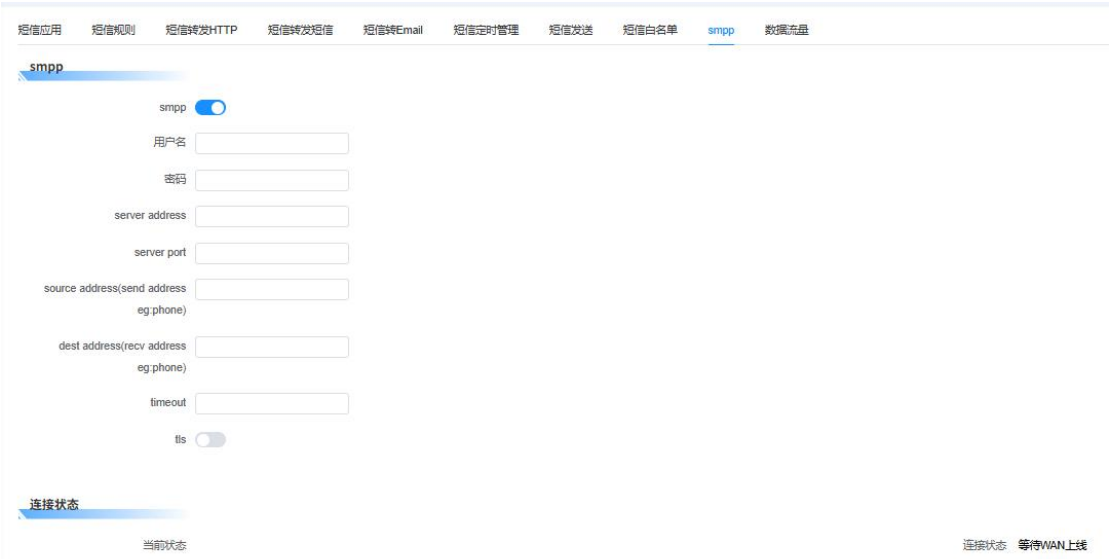
路由器支持短信白名单功能，可新增或删除白名单中的手机号码，用于限制或允许特定号码的短信通信。



项目	说明
短信白名单	切换选项。启用后，只有白名单中的号码才能进行短信相关的操作（如发送和接收短信）。禁用时，SMS 操作不受限制。

- SMPP

路由器支持 SMPP 协议，可设置用户名、密码、服务器地址、服务器端口、源地址及超时时间等参数，用于实现短信的远程发送与接收。



项目	说明
用户名	SMPP 服务器的登录用户名，用于身份验证。
密码	登录 SMPP 服务器的相应密码，以确保鉴权。
服务器地址	输入 SMPP 服务器的 IP 地址或域名，建立连接。
服务器端口	指定连接到 SMPP 服务器的端口号。
源地址（发送地址，例如：电话）	用作 SMS 消息发送者的电话号码。
接收地址（例如：电话号码）	目标地址，如接收号码或电话号码。
超时时间	设置在将请求视为超时之前等待来自 SMPP 服务器的响应的最长时间。
TLS 协议	切换选项。启用时，TLS 加密可保护与 SMPP 服务器的通信；禁用时，不应用加密。

连接状态

可显示当前 SMPP 连接状态及详细连接信息。



- **数据流量**

可对路由器数据流量进行限制设置，设定流量计算周期，并可添加或删除接收流量提醒短信的电话号码。



项目	说明
数据流量限制	**开启：**启用流量限制功能，实现设备流量限制管理。 **关闭：**关闭流量限制功能。
流量限制（MB）	可自定义限制流量阈值，单位为 MB。
计算周期	可选择流量计算周期，可选当日或本月进行流量计算周期的单位。
流量关闭功能	**开启：**启用流量关闭功能，路由器可在达到设定流量或手动触发时关闭数据流量，防止超额使用。 **关闭：**关闭流量关闭功能。

单击“新增”以包括应接收流量短信的电话号码。



2.7 运维管理

路由器支持全面运维管理，包括设备诊断、网络工具、命令调试、Profile 管理、日志管理、防火墙与流量统计、存储设置、远程管理及 I/O 配置。

2.7.1 诊断

路由器可对网络进行全面诊断，快速检测连接状态、网络性能及潜在故障。



项目	说明
诊断内容	单击“开始诊断”以分析设备的相关信息。诊断完成后，您可以导出诊断报告。

2.7.2 网络工具

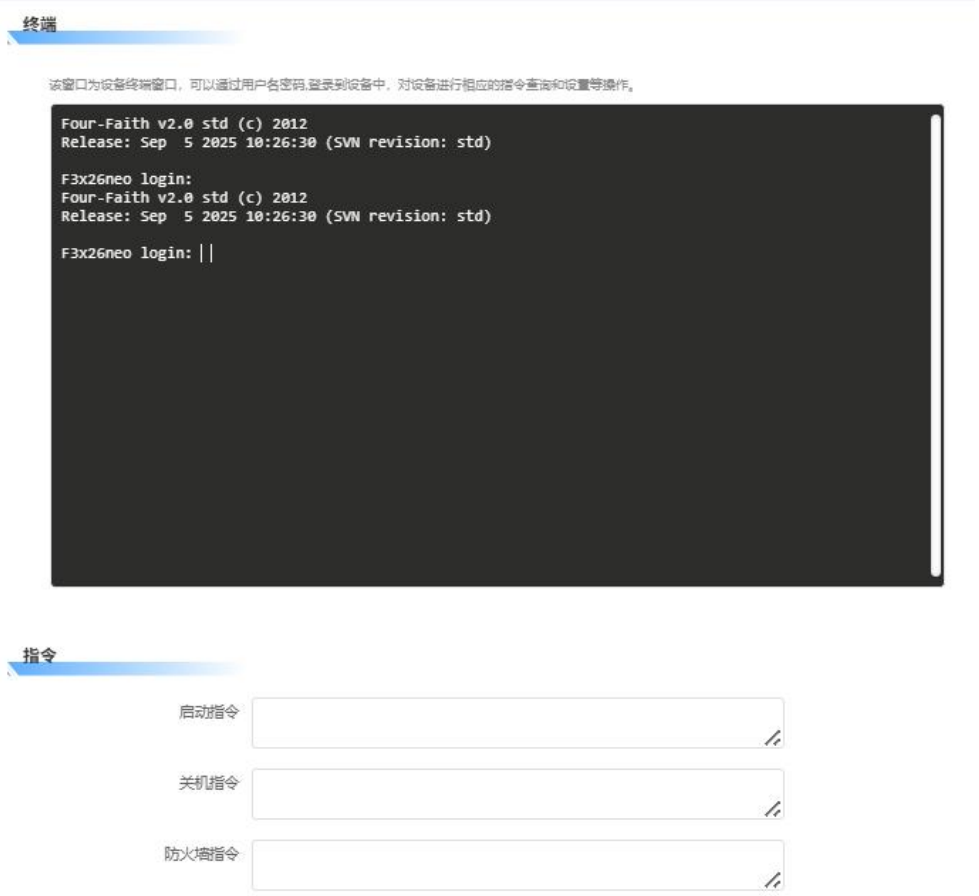
路由器支持网络测试，可设置模式（ping、traceroute、nslookup）及目的 IP 地址或域名。



项目	说明
模式	选择网络测试模式，包括 Ping、Traceroute 和 NSLookup。
目的 IP 地址或域名	输入目标 IP 地址或域名。

2.7.3 命令调试

终端可通过用户名和密码登录路由器，对设备执行指令查询和设置，并支持启动、关机及防火墙指令下发调试。



项目	说明
终端	在“终端”界面执行设备维护命令。
启动命令	保存命令行指令，以便在路由器启动时自动执行。
关机命令	保存命令行指令，以便在路由器关闭时自动执行。
防火墙命令	每次防火墙启动时运行自定义 iptables 命令。

2.7.4 Profile 管理

路由器可查看存储器状态，并支持 Profile 管理，包括新增和导入操作。



单击“导入/应用”来选择对应模式、以及选择导入的 Profile 文件，并开始导入至设备。



单击“新增”来配置 Profile 内容

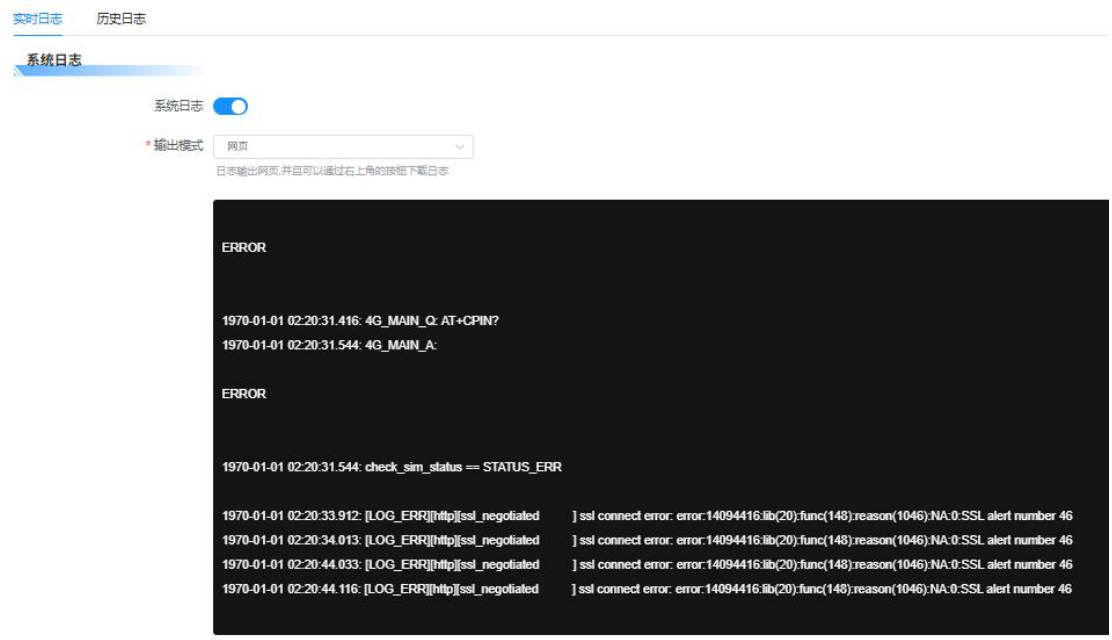


2.7.5 日志管理

路由器可查看实时系统日志，并支持查询和管理历史日志记录。

- **实时日志**

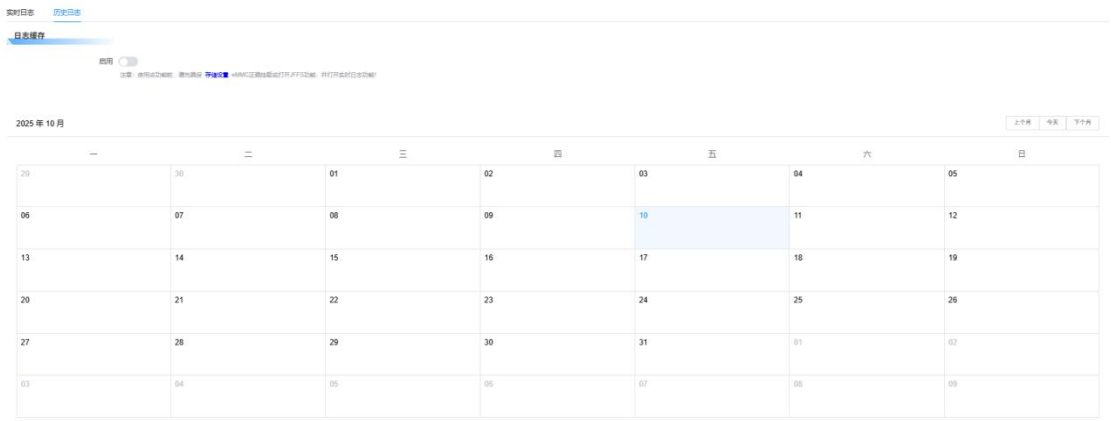
路由器可查看实时系统日志，并可设置日志输出模式（串口、网络、网页）；网页模式下可通过右上角按钮下载日志。



项目	说明
系统日志	一个开关选项。启用时，系统记录操作事件和日志；禁用时，日志记录停止。
输出模式	**串口：**日志将显示在设备的控制台中，供本地查看。 **网络：**将日志通过网络传输到指定的日志服务器，实现远程管理。 **网页：**通过 Web 界面访问日志，允许用户通过浏览器查看日志。

- **历史日志**

可以通过选择相应的日期来查看历史日志。



2.7.6 防火墙统计

用于查看多个防火墙规则表类型（如筛选器、Nat、Mangle、Raw）的相关数据。



项目	说明
链式	表示组织防火墙规则的不同链。
流量（字节）	显示通过相应链的网络流量大小（以字节为单位），表示链中数据包使用的带宽。
数据包数量	统计通过相应链的数据包数量。
策略	指定对应链的默认处理策略。
规则	指示当前链中的活动规则数。

2.7.7 流量统计

通过可视化图表查看主备链路的流量。



2.7.8 存储设置

查看 JFFS 存储的状态，可格式化 JFFS 文件系统以擦除所有数据并重新初始化，也可进行相

关文件管理。



2.7.9 远程管理

路由器支持远程管理，可配置 SSH、TELNET、SNMP、TR069、VRRP 及 NFS 客户端功能。

- SSH 协议



项目	说明
启用	**开启：**启用 SSH 功能 **关闭：**关闭 SSH 功能。
SSH TCP 转发	启用或禁用 SSH TCP 转发的开关选项。启用时，TCP 流量可以通过 SSH 隧道转发；禁用时，不允许基于 SSH 的 TCP 转发。
密码登录	允许或限制使用用户名和密码进行 SSH 登录的开关选项。禁用时，可能需要其他身份验证方法，例如基于密钥的登录。
端口	路由器的 SSH 端口默认为 22，用于安全远程登录和管理。

授权密钥	允许为 SSH 身份验证添加公钥。
SSH 远程管理	启用 SSH 相关的管理功能，包括远程端口配置。
SSH 远程端口	路由器的 SSH 远程端口设置，用于安全远程登录和管理。

SSH 白名单

路由器支持 SSH 白名单管理，可新增或删除白名单中的 IP 地址，实现访问控制。



项目	说明
启用	**开启：**启用 SSH 白名单功能 **关闭：**关闭 SSH 白名单功能。
策略	固定为白名单策略

单击“新增”来配置 SSH 白名单内容



- TELNET

路由器支持 Telnet，可开启远程管理以进行设备配置和监控。



项目	说明
Telnet	**开启：**开启设备的 Telnet 服务。 **关闭：**关闭设备的 Telnet 服务。
Telnet 远程管理	允许通过 Telnet 进行远程管理。

TELNET 白名单

路由器支持 TELNET 白名单管理，可新增或删除白名单中的 IP 地址，实现访问控制。



项目	说明
启用	**开启：**启用 TELNET 白名单功能 **关闭：**关闭 TELNET 白名单功能。
策略	固定为白名单策略

单击“新增”来配置 TELNET 白名单内容



- **SNMP**

路由器支持 SNMP 协议，可实现设备状态监控、网络管理及远程数据采集。



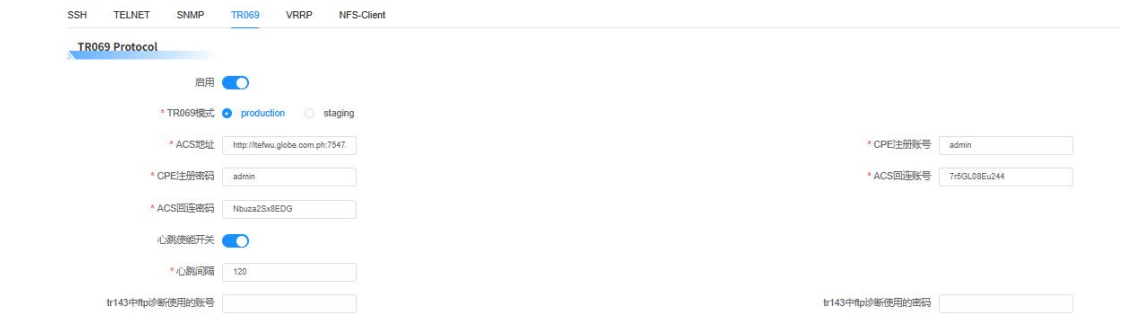
项目	说明
启用	开启：启用 SNMP 功能 关闭：关闭 SNMP 功能。
位置	指定设备的物理位置，以帮助管理员识别其位置。
联系	定义设备的联系信息，默认为“root”。
名称	自定义 SNMP 管理的设备名称，默认为“snmp”。
只读团体字	SNMP 的只读身份验证字符串。具有此团体名称的管理站只能查看设备信息，但不能对其进行修改。默认值：“public”。
读写团体字	SNMP 的读写身份验证字符串。具有此团体名称的管理站可以读取和修改设备信息。默认值：“private”。
SNMP v3	激活 SNMP 版本 3 功能。

单击“新增”来添加与 SNMP 相关的详细信息



- **TR069**

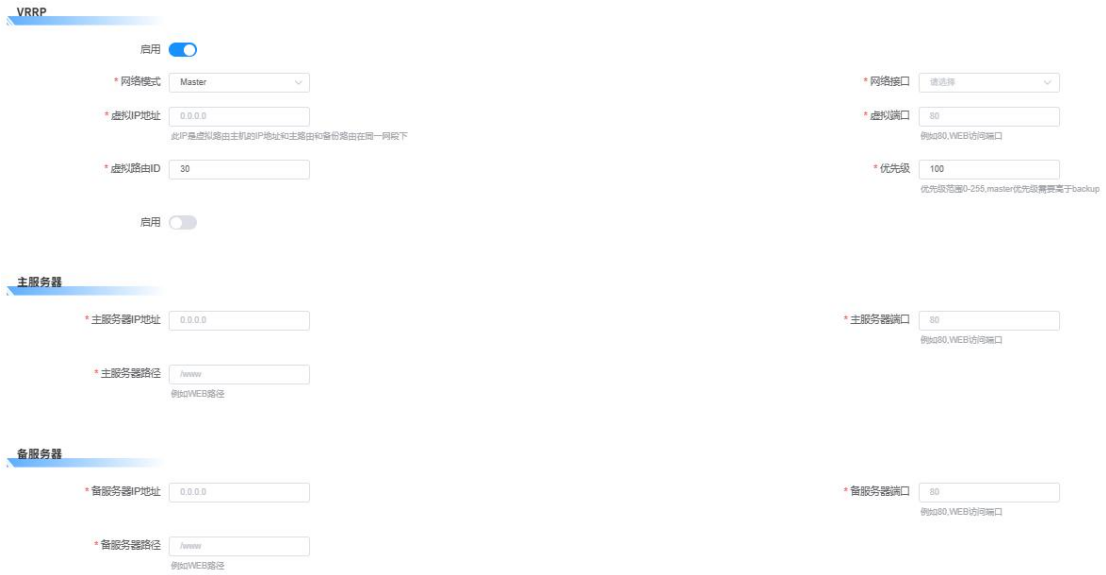
路由器支持 TR069 协议，可实现远程自动配置、管理和监控设备。



项目	说明
启用	**开启：**启用 TR069 功能。 **关闭：**关闭 TR069 功能。
TR069 模式	选择 TR069 协议的工作模式。“生产”用于正式运营环境，而“试运行”用于测试和预部署。
ACS 地址	设置 TR069 远程管理服务器的访问地址。
CPE 注册密码	设置设备向 ACS 注册的密码。
ACS 回连密码	设置 ACS 回连设备时使用的密码。
心跳使能开关	启用后，路由器会定期向管理服务器发送心跳消息，以维护连接并报告其状态。禁用时，此功能停止。
心跳间隔	设置设备向 ACS 发送心跳的时间间隔。
TR143 中用于 FTP 诊断的账号	TR143 下 FTP 相关诊断操作的登录帐号。
TR143 中用于 FTP 诊断的密码	指定 TR143 下 FTP 诊断的登录密码，与认证帐户一起使用。

- VRRP

路由器支持 VRRP 功能，可配置主备服务器地址、路径及端口，实现网关冗余与自动切换。



项目	说明
启用	**开启：**启用 VRRP 功能。 **关闭：**关闭 VRRP 功能。
网络模式	定义 VRRP 设备在网络中的角色。
网络接口	为 VRRP 操作选择网络接口。
虚拟 IP 地址	设置 VRRP 虚拟路由器的共享 IP 地址，主备路由器对外提供服务都使用该 IP 地址。
虚拟端口	指定与虚拟 IP 地址关联的用于网络通信的端口。
虚拟路由器 ID	VRRP 虚拟路由器的标识，一般取值范围为 0.255。同一 VRRP 备份组中的设备必须具有相同的 ID。
优先级	确定设备在 VRRP 组中的优先级。值越高，成为主路由器的可能性就越大（范围：1-254，默认值：150）。
主服务器 IP 地址	主服务器的 IP 地址。
主服务器端口	设置连接到主服务器的端口号。
主服务器路径	定义与主服务器相关的路径。
备份服务器 IP 地址	指定备用服务器的 IP 地址，如果主服务器发生故障，则会接管该服务器。
备份服务器端口	设置连接到备份服务器的端口号。
备份服务器路径	定义与备份服务器相关的路径。

- NFS-Client

路由器支持 NFS 客户端功能，可在系统中设置服务器地址，实现远程文件共享与访问。



2.7.10 I/O 设置

路由器的 I/O 设置功能允许用户配置 HTTP 地址和端口、查看数字输入（DI）状态、设置定时输出、选择输出方式（如延迟若干秒后输出高电平或定时高电平）、设置高电平输出持续时间，并可开启 DI 功能控制，同时配置触发动作及触发方式。



项目	说明
I/O Set	**开启：**启用 I/O SET 功能。 **关闭：**关闭 I/O SET 功能。
DO（水平）	控制数字输出功能的开关选项。使能时，它允许控制输出电平状态。当前 DI 状态显示为“高电平”。”禁用时，数字输出功能关闭。
HTTP 协议	用于启用或禁用通过 HTTP 协议进行的 IO 管理和访问。启用时，可以通过 HTTP 管理 IO 设置；禁用时，基于 HTTP 的操作不可用。
定时	设置高电平方式及高电平输出时间
DI 功能控制	启用或禁用数字输入功能控制的开关选项。使能时，它允许监控和管理输入信号；禁用时，数字输入控制关闭。

2.8 云平台管理

2.8.1 设备云

设备云平台支持远程运维设备参数配置，升级设备固件，内网穿透运维子设备固件，数据报表等，将设备配置至设备云平台可方便后续远程操作设备，使用设备云平台需要提前注册设

备云平台账号，点击可前往设备云进行注册并登录使用。



2.9 系统管理

2.9.1 系统设置

- **系统设置**

您可以在系统设置中修改路由器的名称和主机名。



- **NTP 客户端**

启用 NTP 客户端可以配置时区、夏令时和服务器 IP/名称。



- **时间设置**

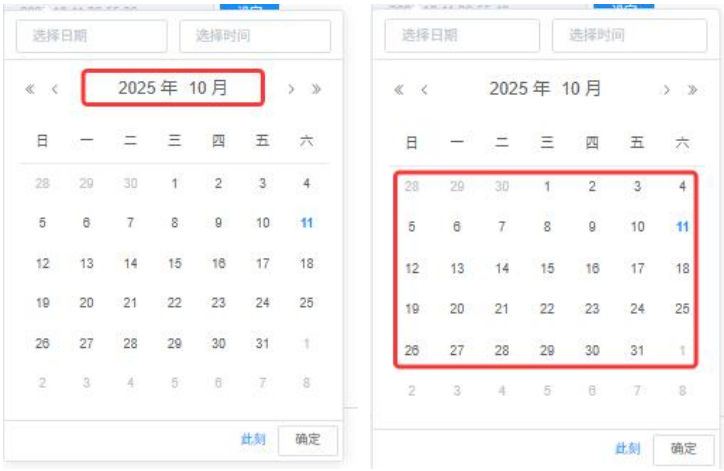
您可以通过选择正确的月份、日期和时间来配置路由器的系统时间，以确保准确的同步。



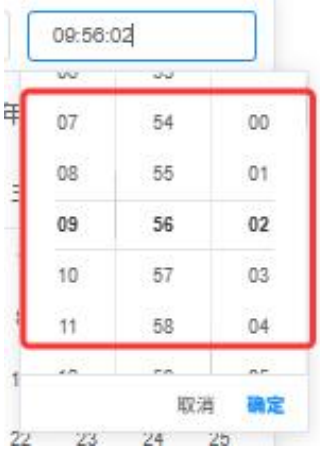
单击该框。



选择月份和日期。



选择所需的时间，然后单击“确定”。



然后，单击“设置”按钮以应用所选日期和时间。



2.9.2 登录管理

- **账号登录**

您可以修改路由器的用户名和密码。这使您可以通过设置强密码和管理用户访问来增强安全性。建议使用字母、数字和特殊字符的组合以获得更好的保护。



2.9.3 恢复出厂

- **出厂默认**

此操作会将路由器恢复为出厂默认设置，同时清除所有自定义配置，包括网络设置、密码和用户首选项。建议在继续之前备份重要设置。



2.9.4 备份

- **备份配置**

创建当前路由器配置的备份以保护您的设置。这样可以确保在路由器重置为出厂默认值或遇到意外问题时快速恢复它们。



- **配置备份**

只能上传相同路由器型号和固件版本的配置备份文件进行恢复。上传不兼容的文件或不是通

过此界面创建的文件可能会导致错误或系统不稳定。请确保使用正确的备份文件以避免潜在问题。



2.9.5 固件升级

- **升级**

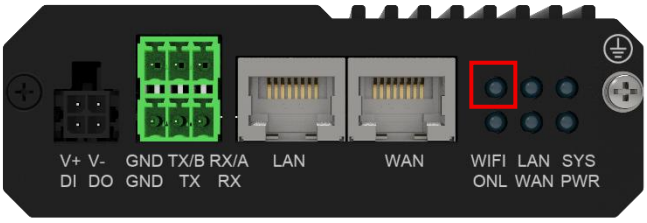
要升级路由器的固件，请首先从本地存储中获取相应的软件文件。选择文件后，单击“升级”按钮开始升级过程。升级过程中，请确保路由器没有断电，避免出现问题。建议在升级前备份当前配置，以防止数据丢失。



第 3 章 LED 说明

- **Wifi LED**

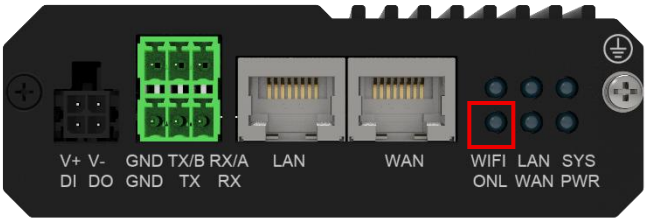
WiFi 指示灯位于前面板右侧左上角的 LED 指示灯区域。



动作	描述
LED 已打开	WIFI 开启，WIFI 功能可用。
LED 关闭	WIFI 已禁用。

- **Online LED**

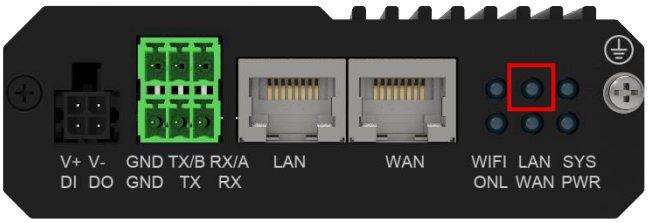
Online 指示灯位于前面板右侧的 LED 指示灯区域，位于左下角。



动作	描述
LED 已打开	连接到 3G/4G 蜂窝网络
LED 关闭	无 SIM 卡或 PIN 码错误

- **LAN LED**

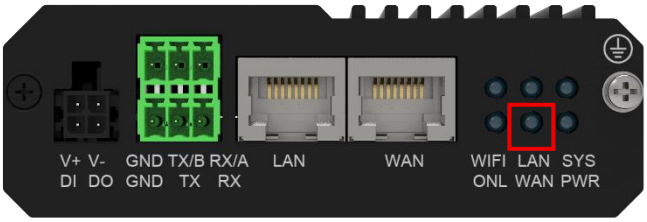
LAN LED 位于前面板右侧的 LED 指示灯区域，位于中间向上。



动作	描述
LED 已打开	作为 LAN 的 10/100 Mbps 连接运行
LED 闪烁	连接已建立，并且此端口上有活动（正在传输数据）
LED 关闭	未建立链接

- **WAN LED**

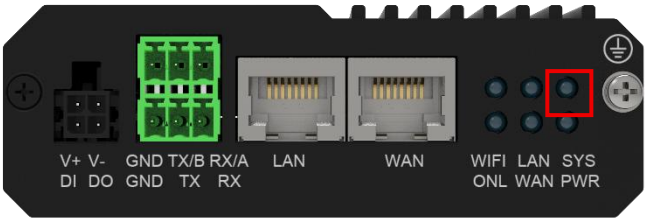
WAN LED 位于前面板右侧的 LED 指示灯区域，位于中间下方。



动作	描述
LED 已打开	作为 WAN 的 10/100 Mbps 连接运行
LED 闪烁	连接已建立，并且此端口上有活动（正在传输数据）
LED 关闭	未建立链接

- **系统 LED**

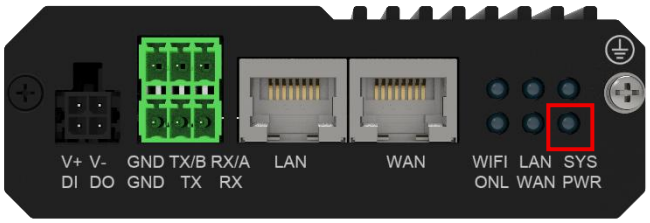
系统指示灯位于前面板右侧的 LED 指示灯区域中，位于右上方。



动作	描述
LED 每 1 秒闪烁一次	设备运行正常。
LED 关闭	设备未上电或已关闭。

- **电源 LED**

系统指示灯位于前面板右侧右下方的 LED 指示灯区域。



动作	描述
LED 已打开	路由器已通电
LED 关闭	路由器未通电

第 4 章 安装说明

DIN 导轨安装 1(背部)



步骤 1： 将路由器主机翻到背面，从导轨工具包中取出 DIN 导轨支架和两颗螺丝。



步骤 2： 将 DIN 导轨支架的两个安装孔与主机背面的卡槽对齐，并放置到位。



步骤 3： 使用随附螺丝固定支架并拧紧，完成安装。

DIN 导轨安装 2(侧部)



步骤 1： 准备路由器主机和导轨工具包，从工具包中取出 DIN 导轨支架及两颗螺丝。



步骤 2： 路由器主机两侧均设有导轨凹槽，可根据需要选择一条凹槽进行安装。



步骤 3： 将 DIN 导轨支架的安装孔与所选凹槽对齐并放置到位。

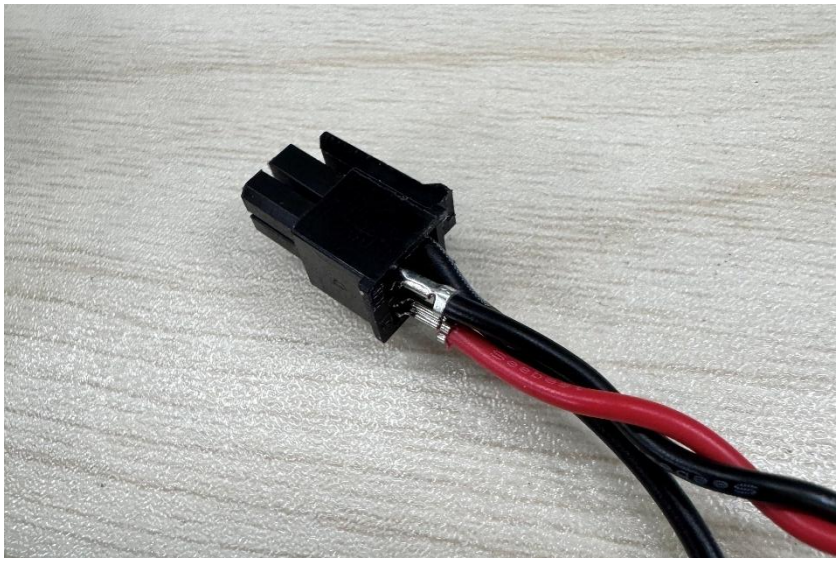


步骤 4：使用随附螺丝固定支架并拧紧，完成安装。

DI/DO 连接线安装



步骤 1： 安装前，准备好电源线、DI/DO 信号线及主设备，确保所有线缆和连接器完好。



步骤 2： 将红线作为 DO 信号插入电源连接器右下端子，将黑线作为 DI 信号插入左下端子。插入后轻轻拉动线缆，确保固定牢靠。



步骤 3： 将带有 DI/DO 线缆的电源端子连接到主设备对应的电源接口，并检查连接是否紧固、无松动。最后，确认所有连接正确且稳固，然后为设备通电，DI/DO 功能即可使用。