



有人物联网
www.usr.cn

4G/5G 聚合工业路由器

USR-G810-33

说明书



联网找有人，靠谱

可信赖的智慧工业物联网伙伴

目录

1. 产品简介	4
1.1. 产品特点	4
1.2. 技术参数	5
1.3. 状态指示灯	6
1.4. 产品选型	6
1.5. 尺寸描述	7
2. 系统基本功能	7
2.1. Web 页面设置	7
2.2. 系统	8
2.2.1. 主机名设置	8
2.2.2. 时间参数	9
2.2.3. NTP 校准	9
2.2.4. 日志	10
2.3. 用户名密码设置	11
2.4. 参数备份与上传	12
2.5. 恢复出厂设置	13
2.6. 固件升级	13
2.7. 重启	14
2.8. 定时重启	15
3. 聚合服务	15
3.1. 开启并设置聚合服务	16
3.2. 聚合规则设置（白名单）	17
3.2.1. 规则添加	17
3.2.2. 选择聚合服务器	18
3.3. 聚合服务黑名单设置	19
3.4. 状态与日志	20
3.4.1. 状态	20
3.4.2. 日志	20
4. 网络接口功能	21
4.1. 蜂窝网设置	21
4.1.1. 4G 接口	21
4.1.2. APN 配置	23
4.1.3. 保活探测配置	24
4.1.4. SIM 卡信息显示	24
4.2. 无线配置	25
4.3. LAN 接口	27
4.3.1. DHCP 功能	28
4.4. DHCP/DNS	29
4.5. WAN 口	30
4.5.1. DHCP 客户端	30
4.5.2. 静态 IP	31

4.5.3. PPPoE	31
4.6. 网络切换	32
4.7. 主机名	33
4.8. 静态路由	34
4.9. 网络诊断功能	35
4.10. QoS	36
4.10.1. 接口限速	36
4.10.2. 分类规则	37
4.11. 负载均衡	38
5. VPN 功能	39
5.1. PPTP Client	40
5.2. L2TP Client	41
5.3. IPSec	43
5.4. OpenVPN	44
5.5. GRE	45
6. 防火墙功能	46
6.1. 基本设置	46
6.2. 通信规则	47
6.2.1. IP 地址黑名单	48
6.2.2. IP 地址白名单	50
6.3. NAT 功能	52
6.3.1. IP 地址伪装	52
6.3.2. SNAT	53
6.3.3. 端口转发	56
6.3.4. NAT DMZ	57
6.4. 访问限制	58
6.4.1. 域名黑名单	59
6.4.2. 域名白名单	59
7. 高级服务	60
7.1. 云服务	60
7.1.1. 监控大屏	61
7.1.2. 设备管理	62
7.1.3. 报警联动	66
7.1.4. 数据中心	70
7.1.5. 设备运维	71
7.2. 动态域名解析 (DDNS)	76
7.2.1. 已支持服务商	76
7.2.2. 自定义的服务商	78
8. 免责声明	80
9. 更新历史	80

1. 产品简介

USR-G810-33 是一款和阿里云合作推出的一款双 4G 聚合工业 CPE，采用高性能嵌入式双核 CPU，工作频率高达 880MHz，搭载双高通 4G 模组，并具备丰富的软硬件功能：多链路聚合服务、负载均衡、2.4GHz 和 5.8GHz 双频 WiFi、千兆 LAN/WAN 口、5 种 VPN 加密传输以及免费云管理平台。它在弱网环境以及高速移动场景尤其能够凸显其不断网的优势，为您的数据传输提供稳定可靠的网络组网解决方案。

本产品具有可靠性高、高网络稳定性、零断网等特性以及操作简单的优势，可广泛应用在商超监控、无人车、机器人、ATM 机、自动售货机、充电站等领域。

1.1. 产品特点

稳定可靠

- 全工业设计，金属外壳，防护等级 IP30；
- 支持水平桌面放置、挂壁式、导轨式安装方式；
- 宽电压 DC 9-36V 输入，具备电源反向保护；
- 工业级宽温 -20°C~+70°C 宽温设计、EMC 3 级防护；
- 内置硬件看门狗、故障自检测、自修复，固件备份还原功能，确保系统稳定。

组网灵活

- 提供高速率、低时延、高稳定的多链路聚合网络；
- 支持双高通 4G 全网通，支持 APN/VPDN 专网接入，可定制 eSIM；
- 支持 4 个千兆网口，提供高速连接能力；
- 支持 2.4G 和 5.8G 双频 wifi，提供稳定的 wifi 网络；
- 支持 VPN (PPTP、L2TP、IPSec、OpenVPN、GRE)，并支持 VPN 加密功能；
- 可定制双 5G+有线聚合版/4G+5G+有线聚合版/WIFI+蜂窝网+有线聚合版。

功能强大

- 支持多种 WAN 连接方式，包括静态 IP、DHCP、PPPoE、3G/4G；
- 支持免费云管理：可实现远程打开内置网页、掉电报警、批量可视化配置；
- 支持多路聚合功能、保持设备零断网、低延时网络传输性能；
- 支持负载均衡、QoS、DDNS、静态路由功能；
- 支持防火墙、NAT、访问控制的黑白名单；
- 支持 ssh、telnet、Web 多平台管理配置方式；
- 支持配置参数导入/导出，极大提升大批量应用下的配置效率；
- 支持 NTP、支持一键恢复出厂设置；
- 支持 LED 状态监测(PWR、WLAN、NET1、NET2)，直观查看当前状态；
- 支持链路探测功能，提供防掉线机制，确保数据终端长久在线。

1.2. 技术参数
表 1 基本参数

项目		型号/规格
蜂窝网标准	无线模块	工业级无线模块
	标准频段	LTE:B1/B3/B5/B8/B38/B39/B40/B41 TD-SCDMA:B34/B39 WCDMA:B1/B8 CDMA/GSM:900/1800MHz
	理论速率	LTE :150Mbps (DL) /50Mbps (UL) WCDMA :42Mbps (DL) /5.76Mbps (UL)
WIFI 标准	无线标准	支持 IEEE802.11b/g/n/ac
	理论带宽	2.4G:最高速度 300Mbps 5.8G:最高速度 867Mbps
	认证类型	WPA-PSK、WPA2-PSK、WPA3-PSK
	安全加密	支持 TKIP、AES 加密算法
	覆盖距离	室外空旷/无阻拦, 覆盖半径可达 200 米 室内办公环境/障碍物, 覆盖半径可达 40 米 (受环境影响)
物理特性	工作温度	-20°C ~ +70°C
	存储温度	-40°C ~ +125°C
	工作湿度	5% ~ 95%RH (无凝露)
	存储湿度	1% ~ 95%RH (无凝露)
	供电电压	DC 9-36V
	适配器	12V/3A
	平均功耗	12V@260mA
	尺寸	200.0*140.0*35.0mm (L*W*H, 不含导轨挂耳、天线座以及安装件)
	安装方式	导轨式安装、挂壁式安装、水平桌面放置
	EMC 等级	3 级
硬件接口	WAN 口	1 个 10/100/1000M 以太网口, 自适应 MDI/MDIX, 具备 1.5KV 电磁隔离保护
	LAN 口	3 个 10/100/1000M 以太网口, 自适应 MDI/MDIX, 具备 1.5KV 电磁隔离保护
	SIM 卡接口	2 * (3V/1.8V) 标准自弹式 SIM 卡槽 (双卡可定制内置 eSIM)
	天线接口	蜂窝: 2 个标准 SMA 天线接口(外螺内孔) WiFi: 2 个标准 SMA 天线接口(外螺内孔)
	指示灯	PWR、WLAN、NET1、NET2
	电源接口	直流电源: 筒式 5.5*2.1mm 圆插座或者工业端子供电, 具备反极性保护
	Reload 按键	长按 5-15s 松开恢复出厂

	TBD 接口	调试接口
	接地保护	接地螺丝

<功耗参数>

表 2 功耗表

工作方式	供电电压	平均电流	最大电流
空载运行	DC12V	310mA	480mA
满载运行	DC12V	260mA	600mA

1.3. 状态指示灯

共有 4 个状态指示灯，含义如下

表 3 指示灯说明表

名称	状态	说明
PWR 电源指示灯	常亮	上电状态
	灭	未上电状态
WLAN WIFI 指示灯	常亮	WIFI 开启状态
	灭	WIFI 关闭状态
NET1/2 SIM1/2 指示灯	灭	未插卡/联网异常
	绿色	4G
	双色	3G
	红色	2G

1.4. 产品选型

USR-G810 系列选型表		
选型	双 4G 聚合版	高通单 5G 版
功能 产品图		
蜂窝网	4G 双卡双模	5G 单卡单模
阿里聚合	双 4G 聚合，如插入有线支持有线+双 4G 三路聚合	--
负载均衡	支持	--
免费云平台	支持，远程打开网页、硬件断电报警、可视化批量配置	远程管理平台
网络灾备	双卡无缝切换，零断网	5G/有线自动切换
网口	千兆 1WAN+3LAN	千兆 1WAN+3LAN
WIFI	双频 WIFI5	双频 WIFI5
eSIM	可定制	--
可定制多链路方式聚合	双 5G 聚合版/4G+5G 聚合版/WIFI+蜂窝网聚合版	--

1.5. 尺寸描述

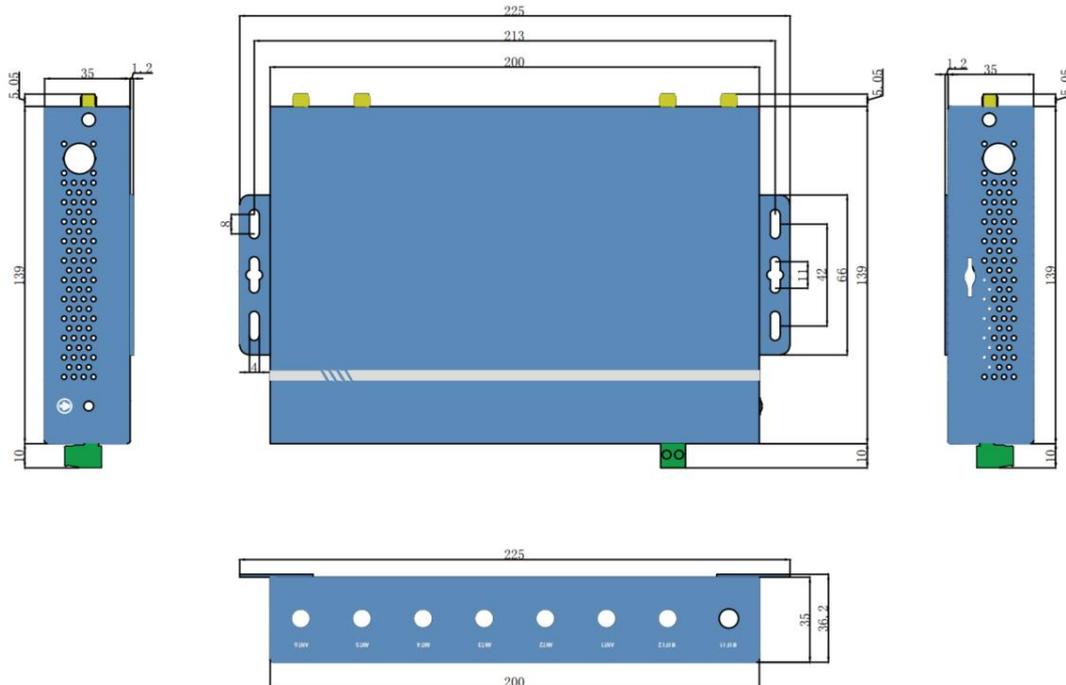


图 1 尺寸图

- 钣金外壳，两侧固定孔，兼容导轨安装件；
- 长宽高分别为 200.0*139*35mm (L*W*H，不含导轨挂耳、天线座以及安装件)。

2. 系统基本功能

2.1. Web 页面设置

首次使用 USR-G810-33 设备时，可以通过 PC 连接 USR-G810-33 的 LAN 口或者连接 G810-33 WIFI，然后用 web 管理页面配置。SSID、IP 地址和用户名、密码如下：

表 4 USR-G810-33 网络默认设置表

参数	默认设置
2.4G SSID	USR-G810-XXXX
5.8G SSID	USR-G810-XXXX_5G
LAN 口 IP 地址	192.168.1.1
用户名	root
密码	root
无线密码	12345678

<说明>

➤ XXXX 代表设备 MAC 后四位。

首先用 PC 的无线网卡或者以太网卡，USR-G810-33 的默认 SSID 为 USR-G810-33-xxxx，操作 PC 加入这个无线网络。等无线连接好后，打开浏览器，在地址栏输入 192.168.1.1 回车。填入用户名和密码（均为 root），然后点击确认登录。网页会出现 USR-G810-33 的管理页面。USR-G810-33 管理页面默认中文。

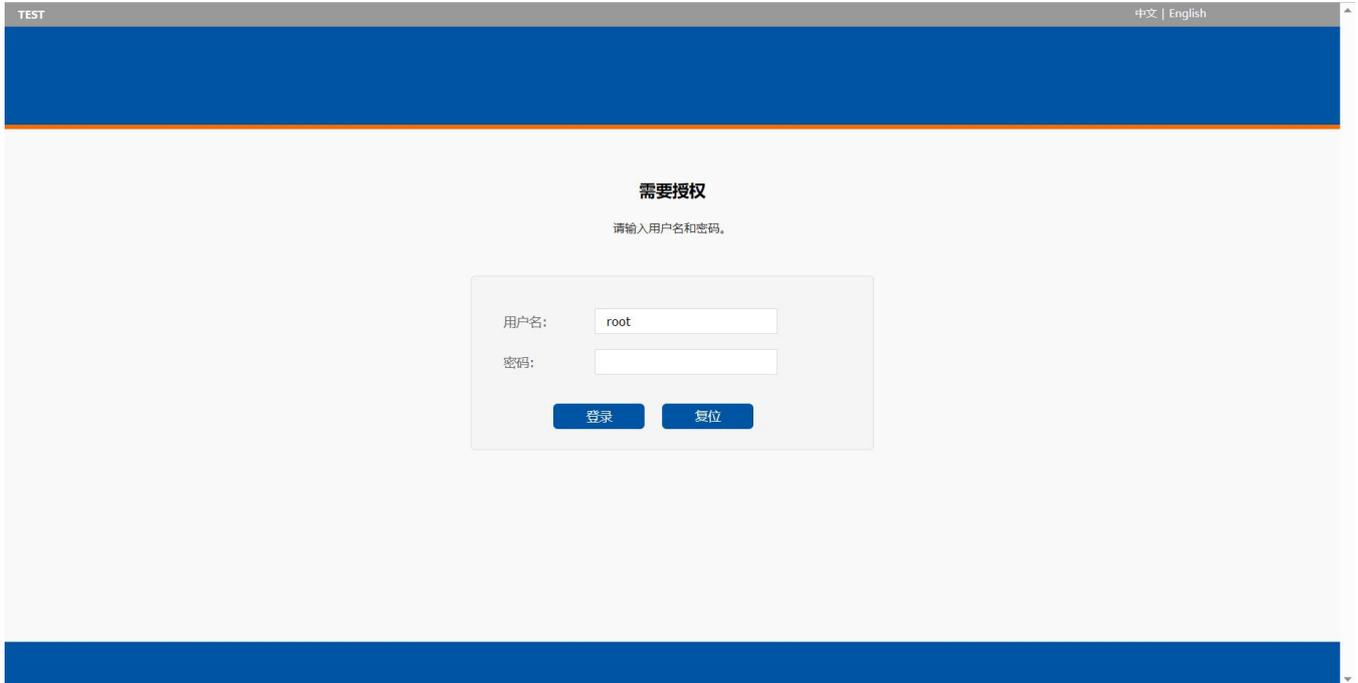


图 2 首页页面

2.2. 系统

2.2.1. 主机名设置

G810-33 路由器可自定义主机名（默认 USR-G810），配置如下：

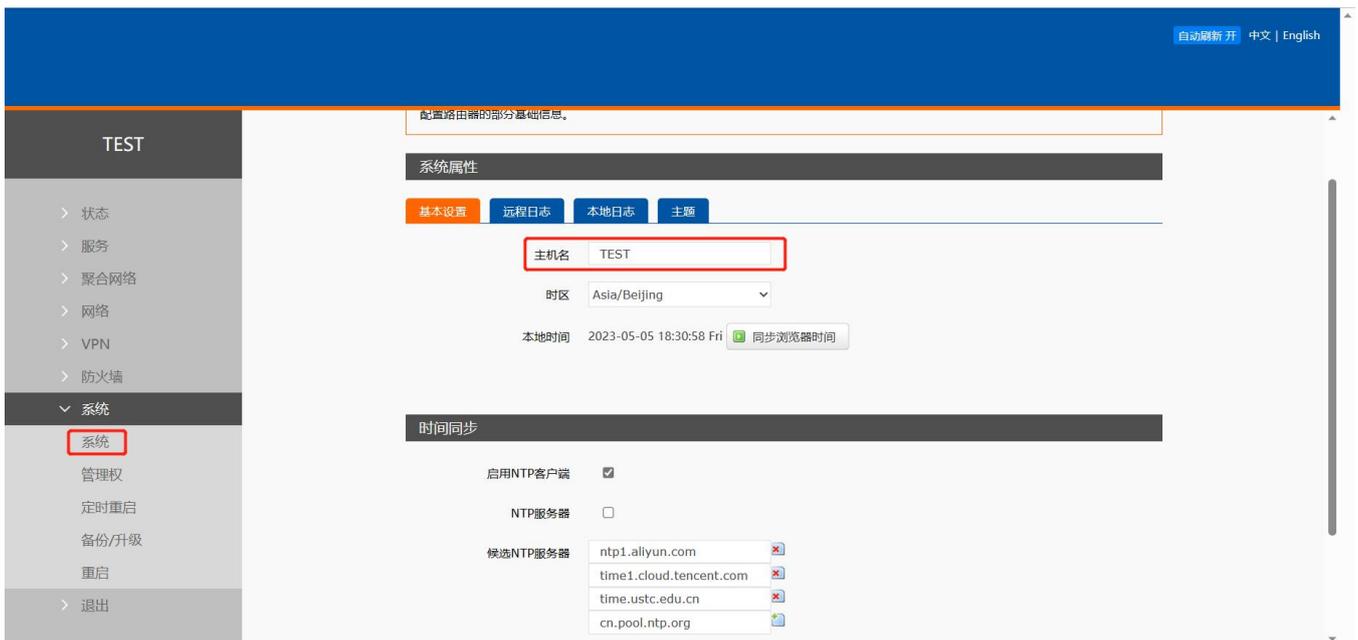


图 3 主机名设置页面

2.2.2. 时间参数

可通过“同步浏览器时间”同步本地时间，可设置路由器默认时区。

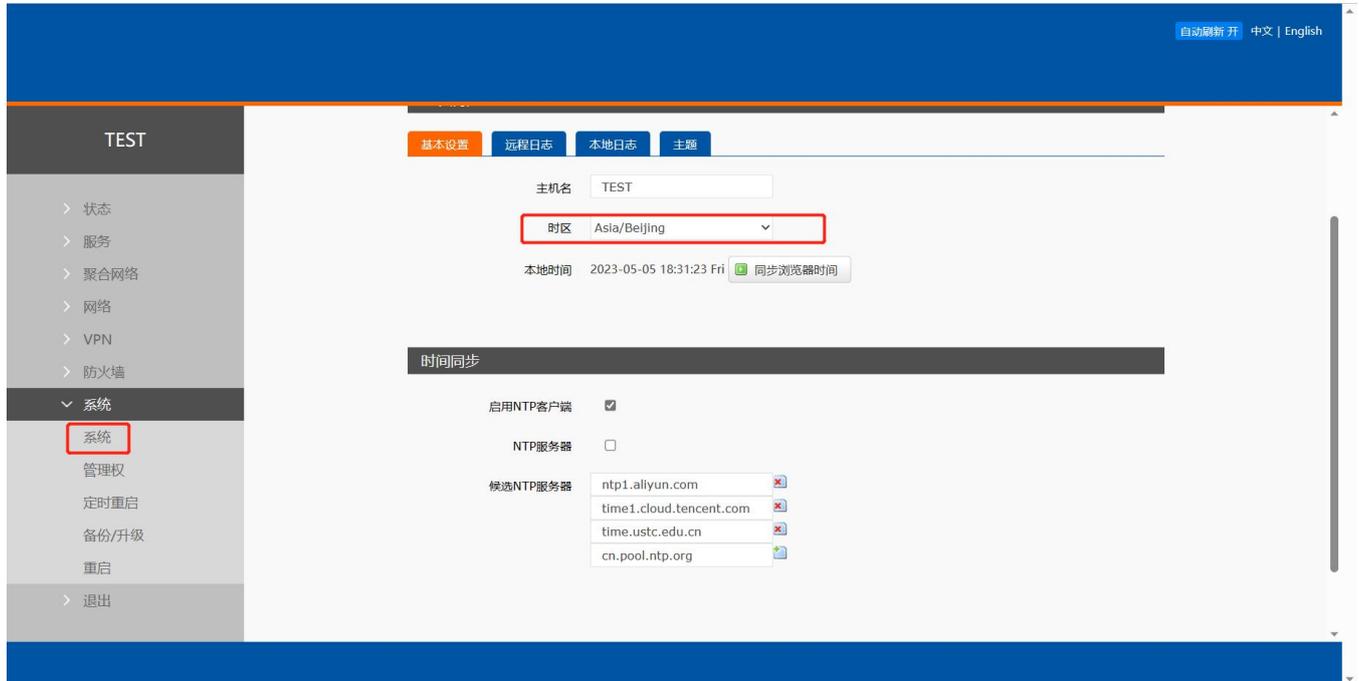


图 4 时区与本地时间同步设置

2.2.3. NTP 校准

路由器可以进行网络校时，默认启动 NTP 客户端功能。

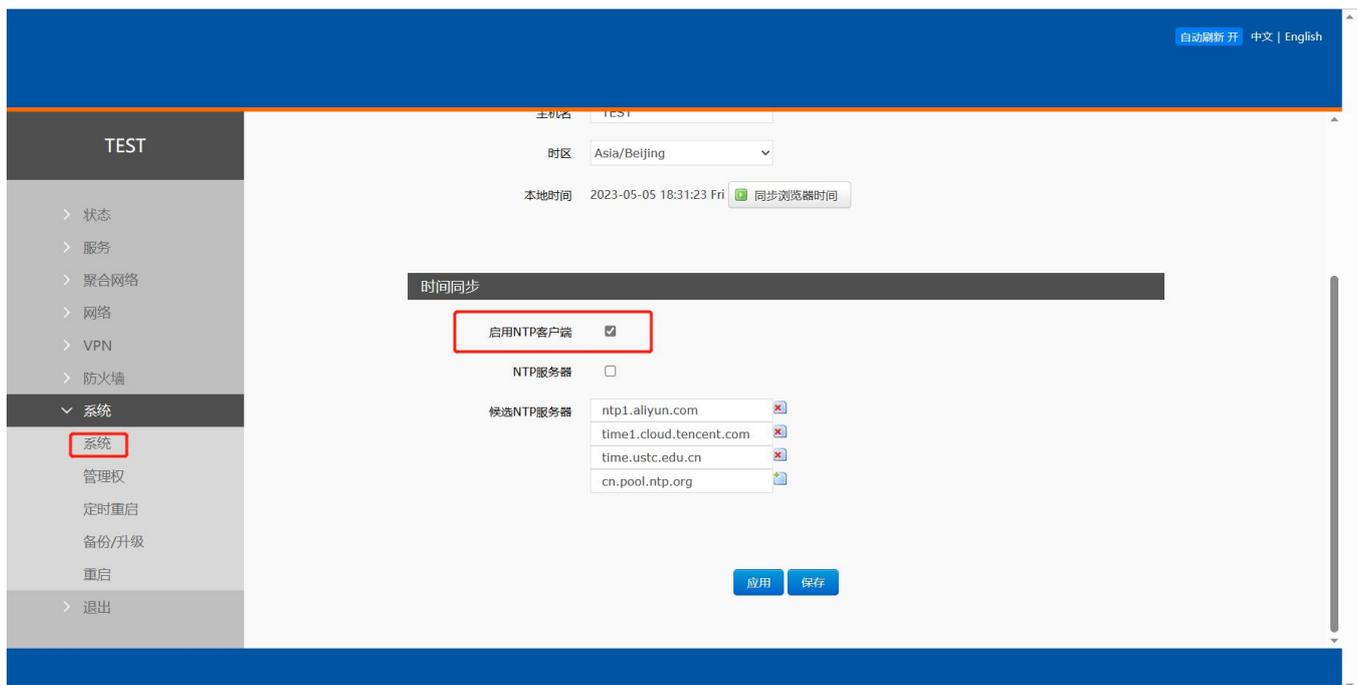


图 5 NTP 页面

2.2.4. 日志

<远程日志>

- 远程 log 服务器：远端 UDP 服务器的 IP，当 IP 为 0.0.0.0 时不启用远程日志；
- 远程 log 服务器端口：远端 UDP 服务器端口。

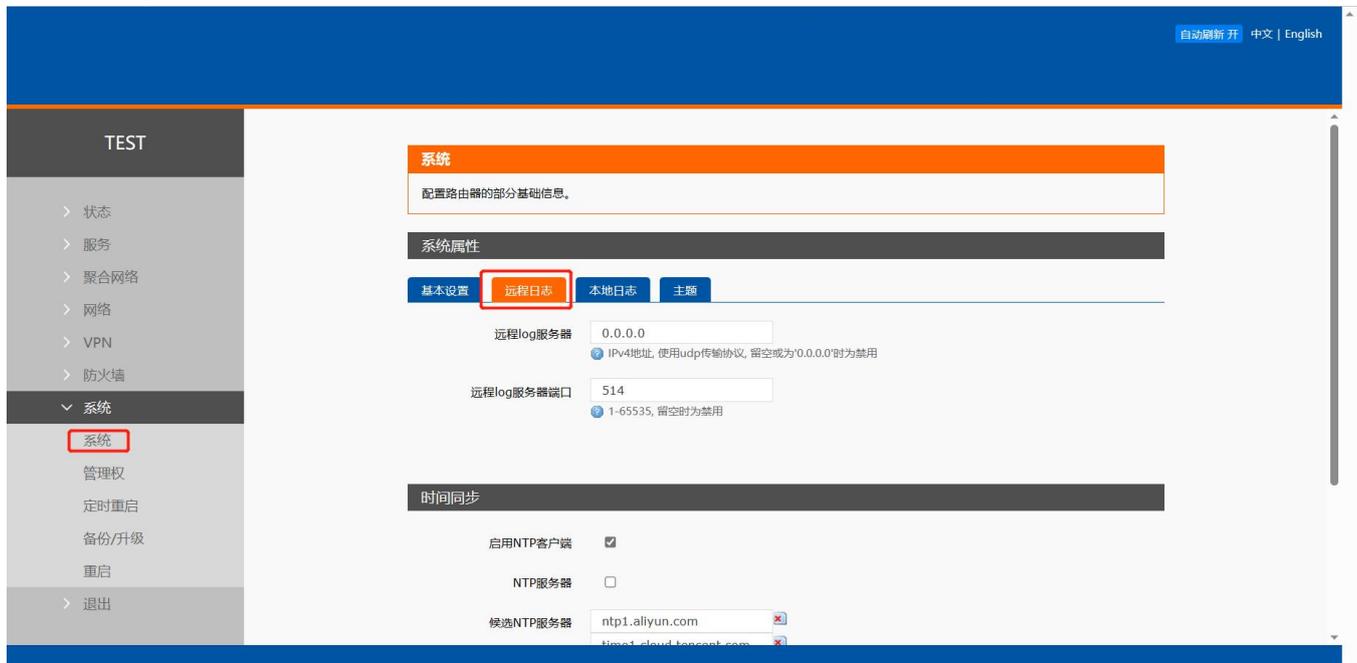


图 6 远程日志

<本地日志>

- 内核/应用日志等级：支持调试/信息/注意/警告/错误/致命错误/警戒/紧急，共 8 个等级；按顺序调试最低，紧急最高；
- 日志（内核、应用、VPN）支持即时查看、清空，支持日志文件导出。

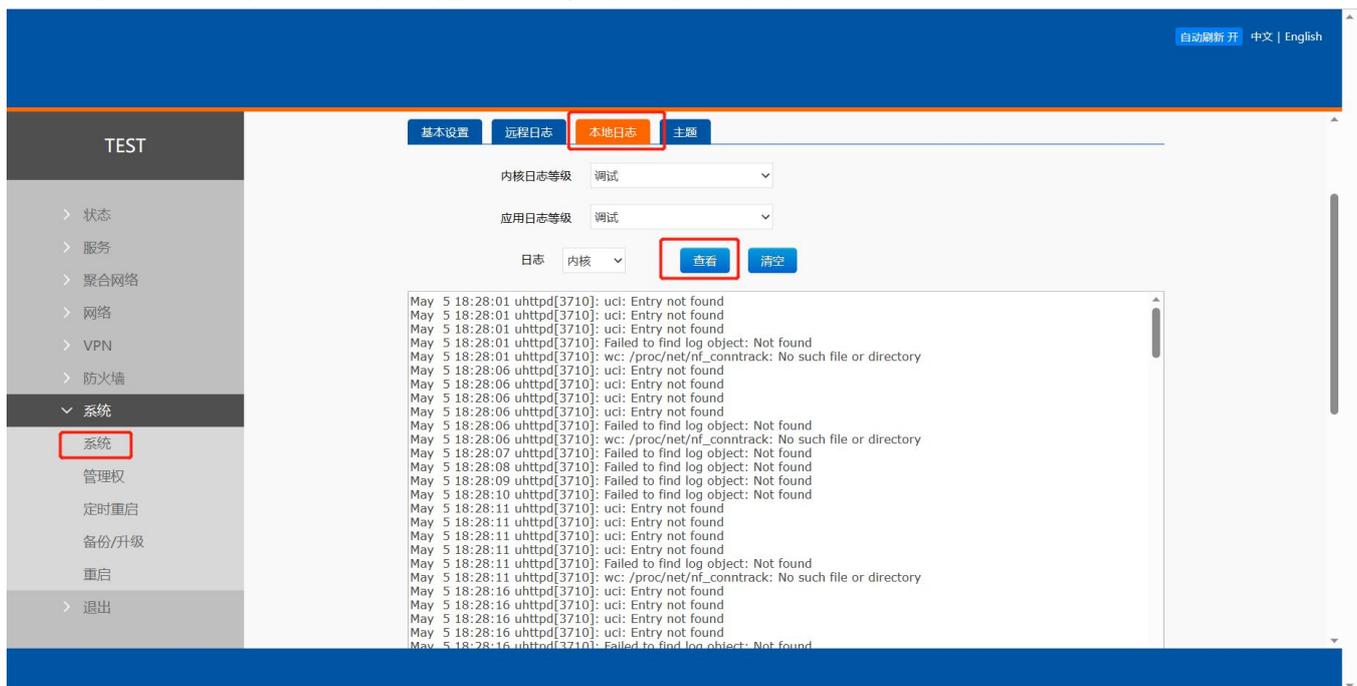


图 7 log 查看

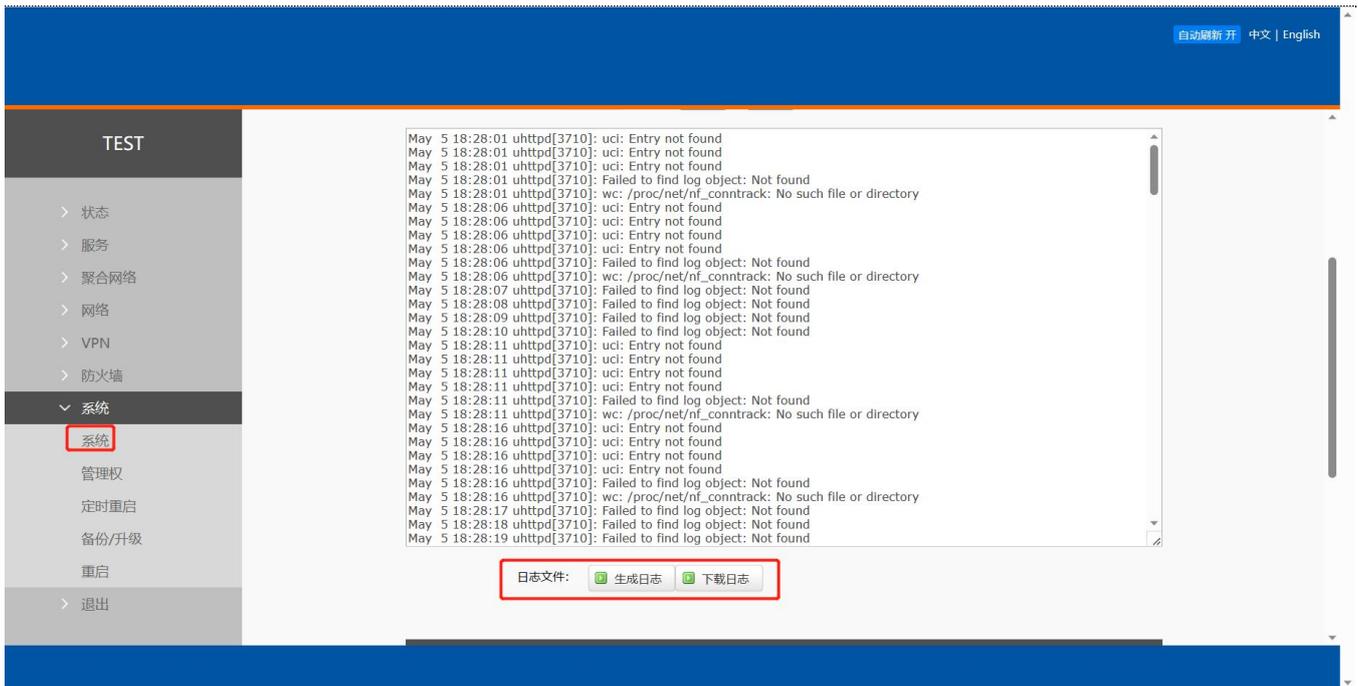


图 8 log 下载

<说明>

- 先生产日志，然后下载日志。

2.3. 用户名密码设置

默认密码可以设置，默认密码为 root，用户名不可设置。本密码为管理密码（网页登录密码）。

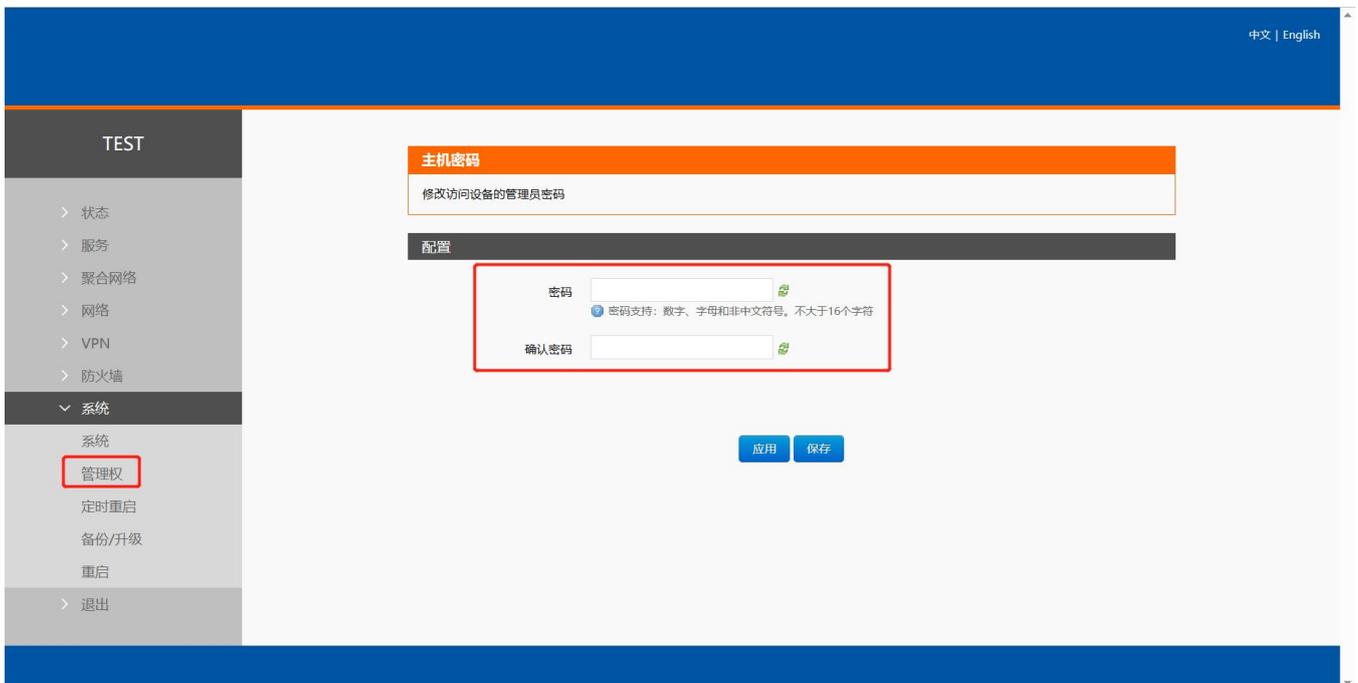


图 9 用户名密码设置页面

2.4. 参数备份与上传



图 10 备份/恢复页面

参数备份：点击“下载备份”按钮，可以将当前参数文件，备份为压缩包文件，比如 backup- USR-G810-2022-04-20.tar.gz ，并保存到本地。



图 11 参数备份上传页面

<说明>

- 必须是 USR-G810-33 的配置文件进行导入，否则将有可能出现配置混乱现象；
- 尽可能是同一版本固件进行导入配置，版本跨越较大有可能出现配置混乱现象。

2.5. 恢复出厂设置

通过网页可以恢复出厂参数设置。



图 12 恢复出厂页面

<说明>

- 在设备正常运行时，长按 Reload 按钮 5-15s 然后松开，路由器将自行恢复出厂参数设置，并自动重启；
- 重启生效瞬间，所有指示灯都将闪亮一下，然后又灭掉（电源灯不灭）；
- 在路由器内置网页界面，点击按钮恢复出厂设置，本功能与硬件的 Reload 按键功能一致；
- 恢复出厂过程持续 3 分钟，期间请不要给设备断电。

2.6. 固件升级

USR-G810-33 模块支持 web 方式的在线固件升级。



图 13 升级页面

<说明>

- 固件升级过程会持续 3-4 分钟左右，请在 4 分钟后再次登录网页；
- 可以选择是否“保留配置”，如版本跨越较大不建议“保留配置”升级；
- 固件烧录过程中请不要断电或者拔网线。

2.7. 重启

点击按钮重启路由器。重启时间与路由器的上电启动时间一致，约为 1 分钟后完全启动成功。

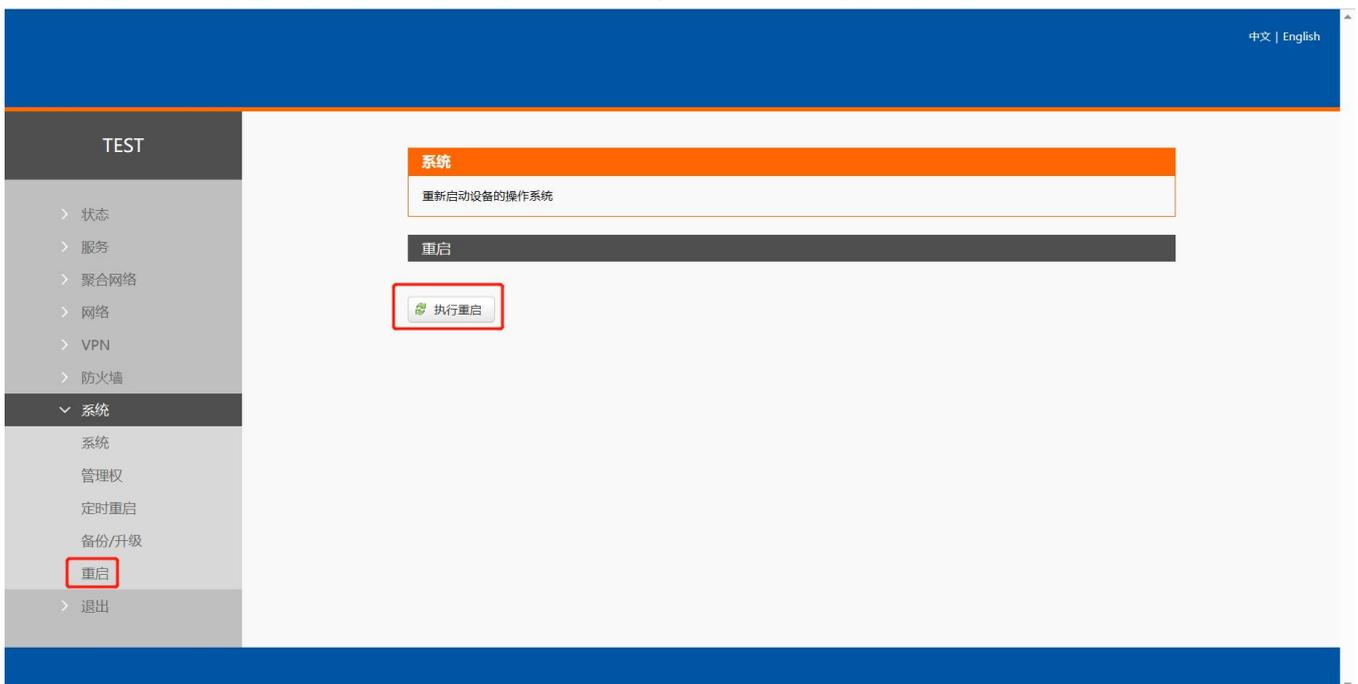


图 14 重启页面

2.8. 定时重启

可以按照每日、每周、每月任意时间的方式对路由器进行定时重启的管理，定期清除运行缓存，提高路由器运行稳定性。页面设置如下。



图 15 定时重启设置页面

3. 聚合服务

本服务是和阿里云合作推出的核心服务，开启聚合可以让多 WAN 网速叠加（包括双蜂窝网、有线、WIFI），让业务传输更加的稳定。在弱网或高速移动场景能够持续保持稳定高速联网。

聚合路由和普通路由器对比优势



图 16 弱网以及移动环境下对比

<说明>

- 常规出货 WIFI 支持 AP 功能，如需 WIFI WAN 多链路聚合功能需定制；
- 如您需体验聚合服务，可直接联系销售，我司将免费提供试用；
- 如需正式部署聚合服务批量使用，需联系销售购买聚合服务；
- 聚合服务支持 TCP/UDP 协议；
- 开启聚合服务时，负载均衡功能将自动关闭，再次关闭聚合服务时负载均衡自动打开；
- 聚合服务开启时，不影响网络切换功能；
- 服务优先顺序：QoS>聚合服务>负载均衡。

3.1. 开启并设置聚合服务

设置聚合服务请顺序执行：开启聚合服务->设置聚合规则（聚合规则内数据将走聚合服务）->如您需设置聚合黑名单请至聚合网络-黑名单进行设置（黑名单内规则将不走聚合服务）->查看聚合网络-状态与日志查看是否聚合建立成功。



图 17 聚合配置页面

表 5 聚合配置参数表

名称	含义	默认值
聚合网络	开启：开启聚合服务 禁用：禁用聚合服务	禁用
用户名/密码	使用聚合服务，需要设置用户名密码 免费体验版请联系销售提供 正式购买服务需填写正确的用户名密码	空
聚合网卡	选择聚合服务使用的链路，可多选 eth0.2：有线 eth1：SIM1 eth2：SIM2 如您定制 WIFI，聚合网卡将会新增 WIFI 网卡，可将双卡+有线+WIFI 四路聚合上传	eth1+eth2 双 SIM 聚合

服务器地址	聚合服务器的地址：域名或 IP 免费体验版请联系销售提供 正式购买服务需填写正确的服务器地址	空
服务器端口	聚合服务器的端口 免费体验版请联系销售提供 正式购买服务需填写正确的服务器端口	空

<说明>

- 服务器地址端口可最多可填写 10 条，填写多个服务器可实现聚合多 Server 优选、多 Server 灾备；
- 设置多个服务后设备会根据 RTT 值智能选路，选择最佳服务器进行聚合；
- 如最优聚合服务器异常，会自动再您设置的其他多个服务器中再选择最佳服务进行聚合；
- 聚合服务是否设置成功，请至聚合网络-状态与日志进行查看；
- 如您开启了聚合服务，但是未设置聚合规则，所有数据将不走聚合服务；
- 此界面点击应用将重启聚合服务。

3.2. 聚合规则设置（白名单）

3.2.1. 规则添加

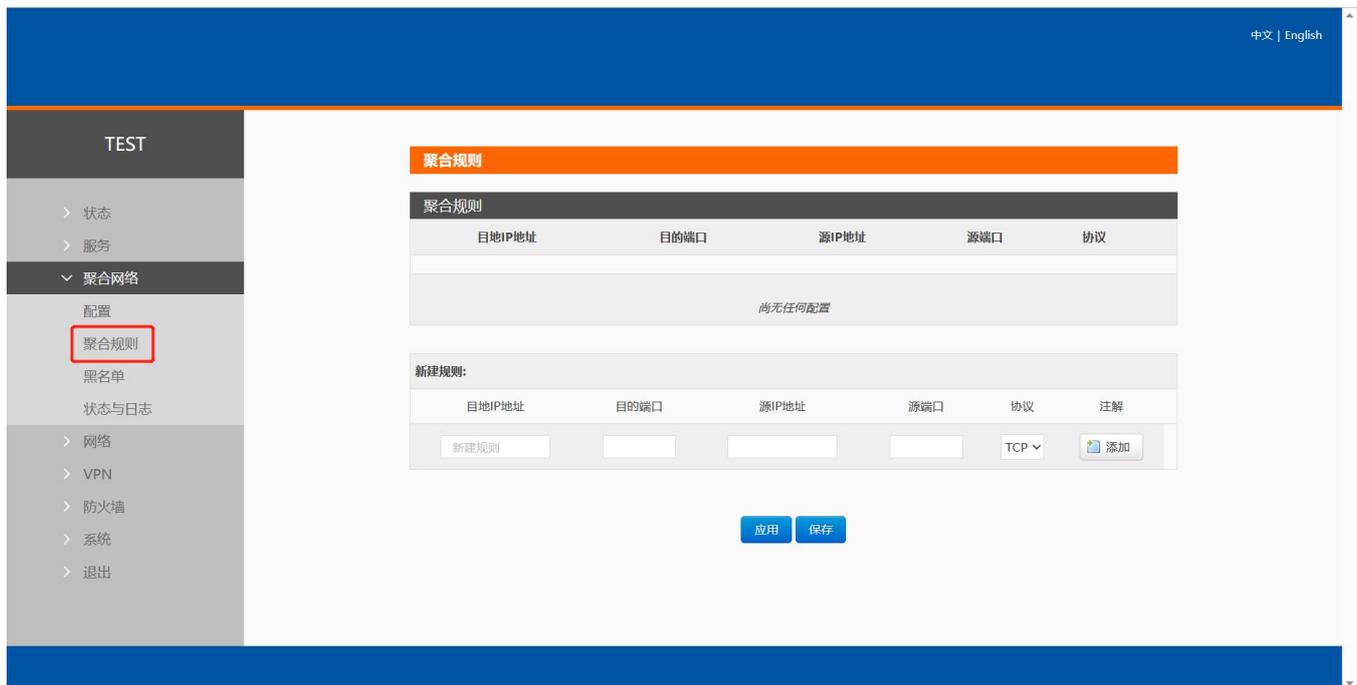


图 18 聚合规则页面

表 6 聚合配置参数表

名称	含义	默认值
目的 IP 地址	访问的目标 IP 地址经过聚合服务 如您需要所有数据都经过聚合，可将目的 IP 地址设置为 0.0.0.0/0	空
目的端口	访问的目标端口经过聚合服务	空

	如您无需限制端口，可直接填空	
源 IP 地址	某子网设备经过聚合服务 如您无需限制具体子网设备可设置为：0.0.0.0/0	空
源端口	某子网设备限制端口经过聚合路由 如您无需限制端口，可直接填空	空
协议	可选择的协议：tcp/udp	tcp

3.2.2. 选择聚合服务器

下图规则解析：所有子网设备无限制，访问所有目标网络并且协议是 tcp 或 udp 均走聚合服务。

点击选择服务器，可为该规则选择需要使用的服务器，对应服务器才会添加该规则，不选中任何服务器时，则该规则不生效。

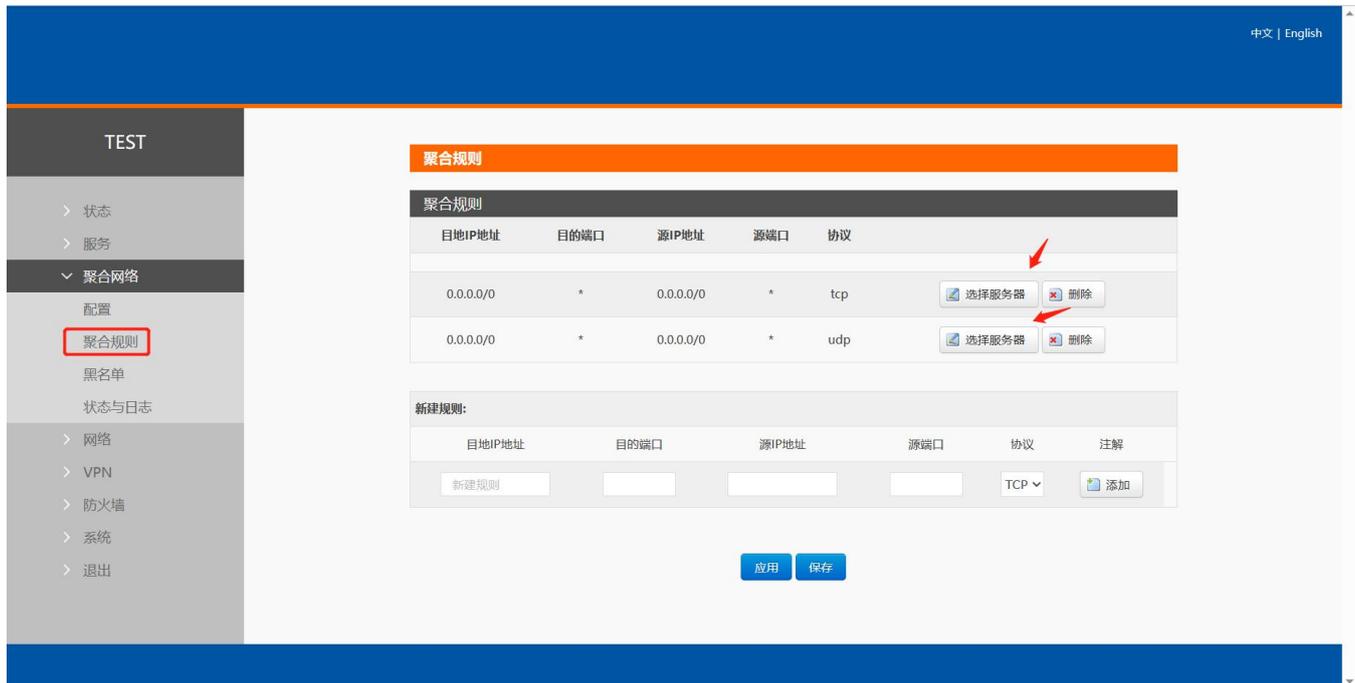


图 19 聚合规则页面

<说明>

- 聚合规则最多可添加 30 条。



图 20 勾选选择聚合服务器页面

<说明>

- 聚合规则如不设置（或删除规则后），相当于未开启聚合服务，所有数据将不走聚合服务器，走原有路由通道；
- 在“聚合网络-配置”界面中配置了几个服务器，在此处选择时，便有几个服务器可以选择，可全选；
- 该规则勾选哪个服务器，哪个服务器才会添加该规则，未勾选的服务器该规则将失效；
- 聚合规则设置完成点击“应用”后仅重新配置规则，不重启聚合服务。

3.3. 聚合服务黑名单设置

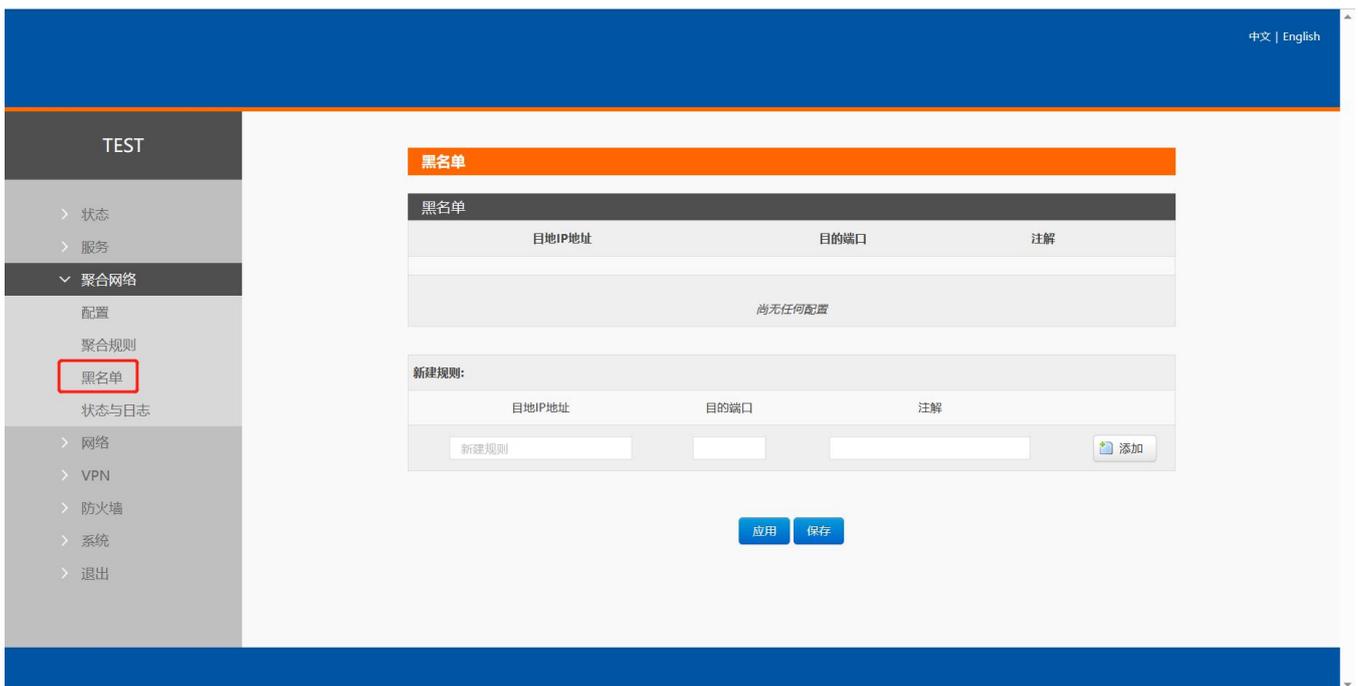


图 21 聚合服务器黑名单设置页面

表 7 聚合服务黑名单参数表

名称	含义	默认值
目的 IP 地址	聚合服务器黑名单 IP 地址	空
目的端口	聚合服务器黑名单端口号 端口为空表示目标黑 IP 的所有端口所有协议数据均不走聚合服务	空
注释	此规则备注	空

<说明>

- 黑名单优先级比聚合规则高，如聚合规则和黑名单 IP 端口冲突时，以黑名单优先；
- 黑名单最多可添加 30 条；
- 黑名单设置完成点击“应用”后仅重新配置规则，不重启聚合服务。

3.4. 状态与日志

3.4.1. 状态

如聚合功能开启成功后，状态将显示“已建立”，也可以看到每个服务器的 RTT 值以及实时速率。

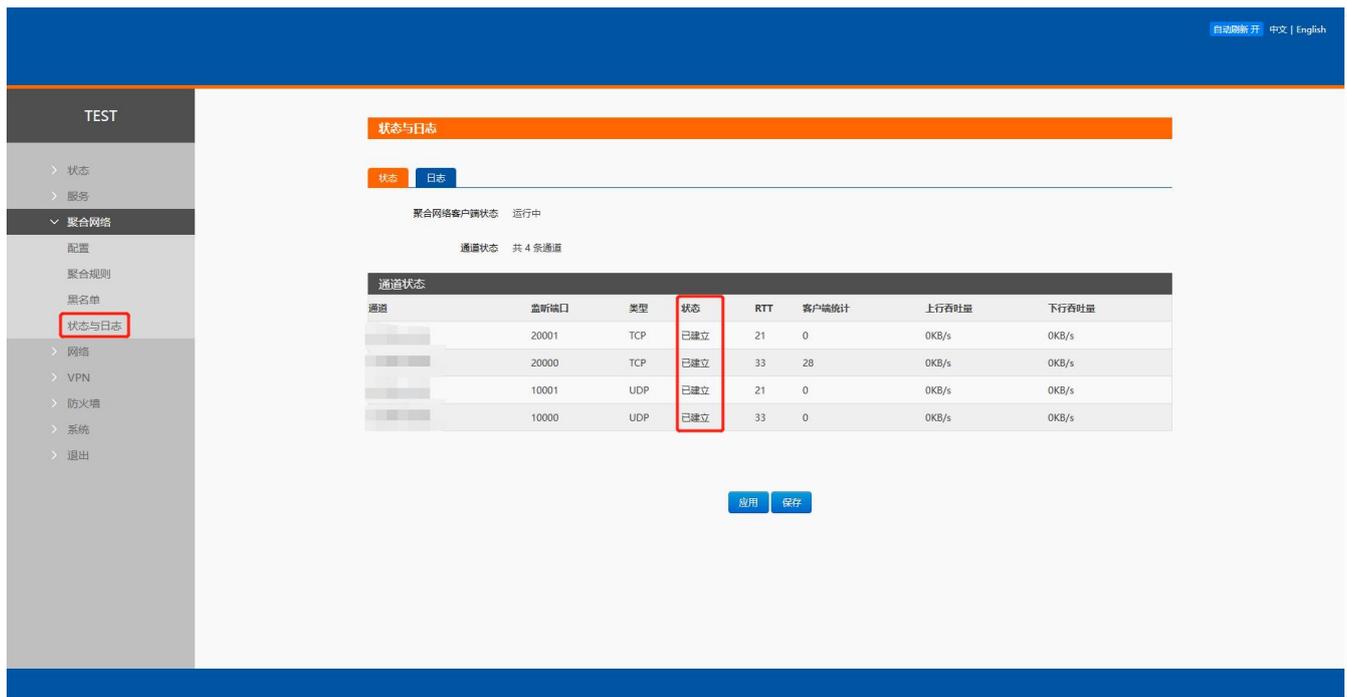


图 22 聚合服务状态显示页面

3.4.2. 日志

可通过日志查看聚合的状态和异常信息，也可在此处下载聚合日志包到电脑。

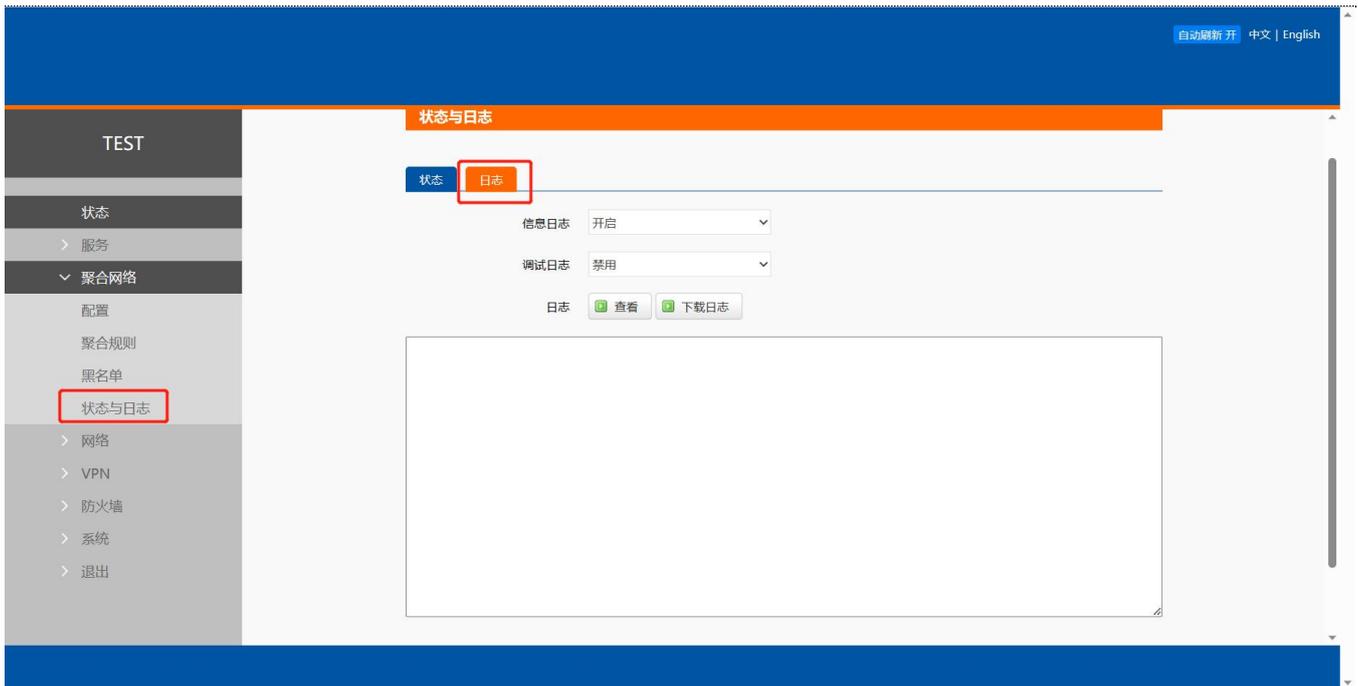


图 23 聚合服务 log 页面

<说明>

- 开启调试日志，日志更加详细；
- 可通过“下载日志”下载到电脑分析；
- 此界面点击应用将重启聚合服务。

4. 网络接口功能

4.1. 蜂窝网设置

4.1.1. 4G 接口

本路由器支持二路 4G 通信模块接口，用来访问外部网络。网页界面如下。



图 24 4G 接口设置页面

对于状态栏的显示如下，如果运行时间为 0，代表本网卡未能联网。

表 8 状态表

名称	含义
运行时间	本接口在网时间
MAC 地址	本网卡接口的 MAC 地址
接收/发送	本网卡累计的接收与发送数据统计
IPv4	代表本网卡使用 IPv4 协议

<说明>

- 路由器默认优先使用有线 WAN 口，可设置 **4G1/4G2/WAN 优先**。

4.1.2. APN 配置

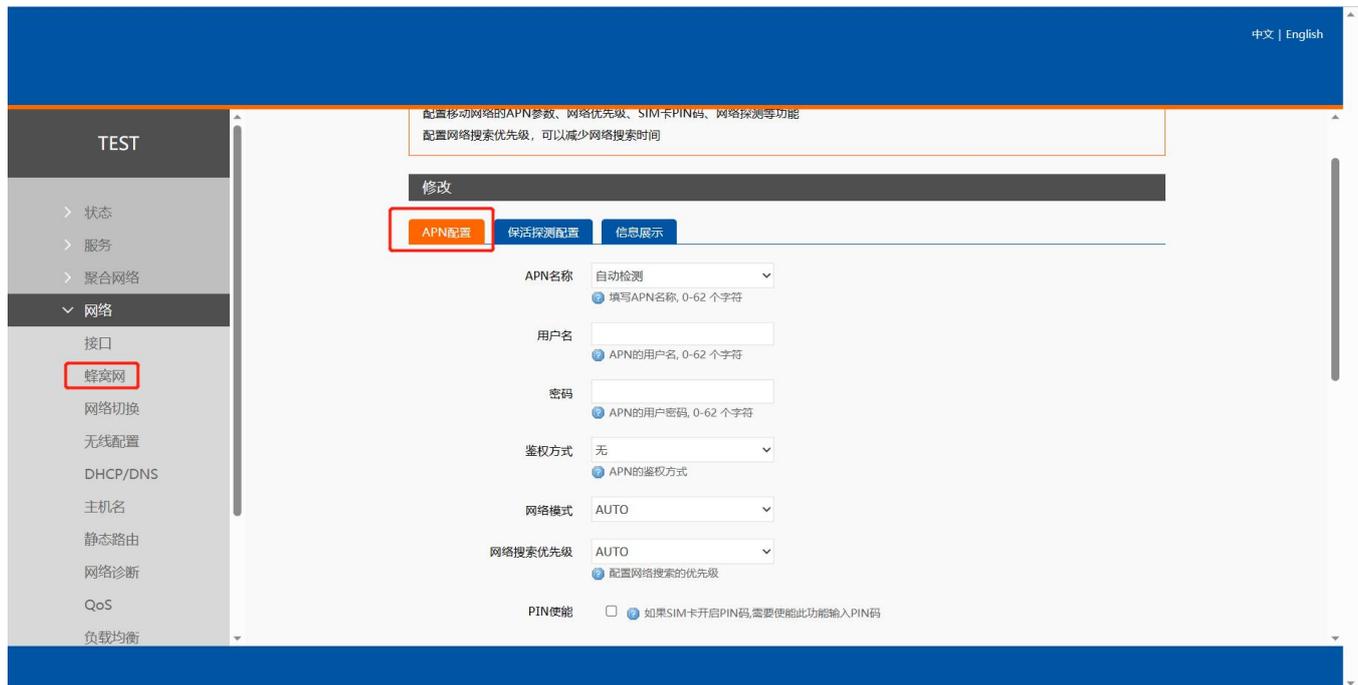


图 25 配置页面

表 9 4GAPN 配置表

名称	含义	默认值
APN 名称	如您使用 APN 卡，请设置正确 APN 如您使用普通物联网卡，默认值即可	自动检测
用户名	如 APN 卡需要用户名，请正确填写	空
密码	如 APN 卡需要密码，请正确填写	空
鉴权方式	如 APN 需要设置鉴权，请正确填写	无
网络模式	可锁 2G/3G/4G 默认自动模式，自动模式当现场无 4G 情况会选择 2G 或 3G 驻网	AUTO
网络搜索优先级	驻网搜网时的优先顺序 可设置 AUTO/4G/3G/2G	AUTO
PIN 使能	如 SIM 卡设置了 PIN 码，请开启 PIN 使能并设置正确 PIN 码	关闭
PIN 码	如 SIM 卡设置了 PIN 码，请开启 PIN 使能并设置正确 PIN 码	1234

<说明>

- 路由器 APN 设置界面上面是 SIM1 的设置，往下拉有一样的配置界面为 SIM2 配置界面。

4.1.3. 保活探测配置

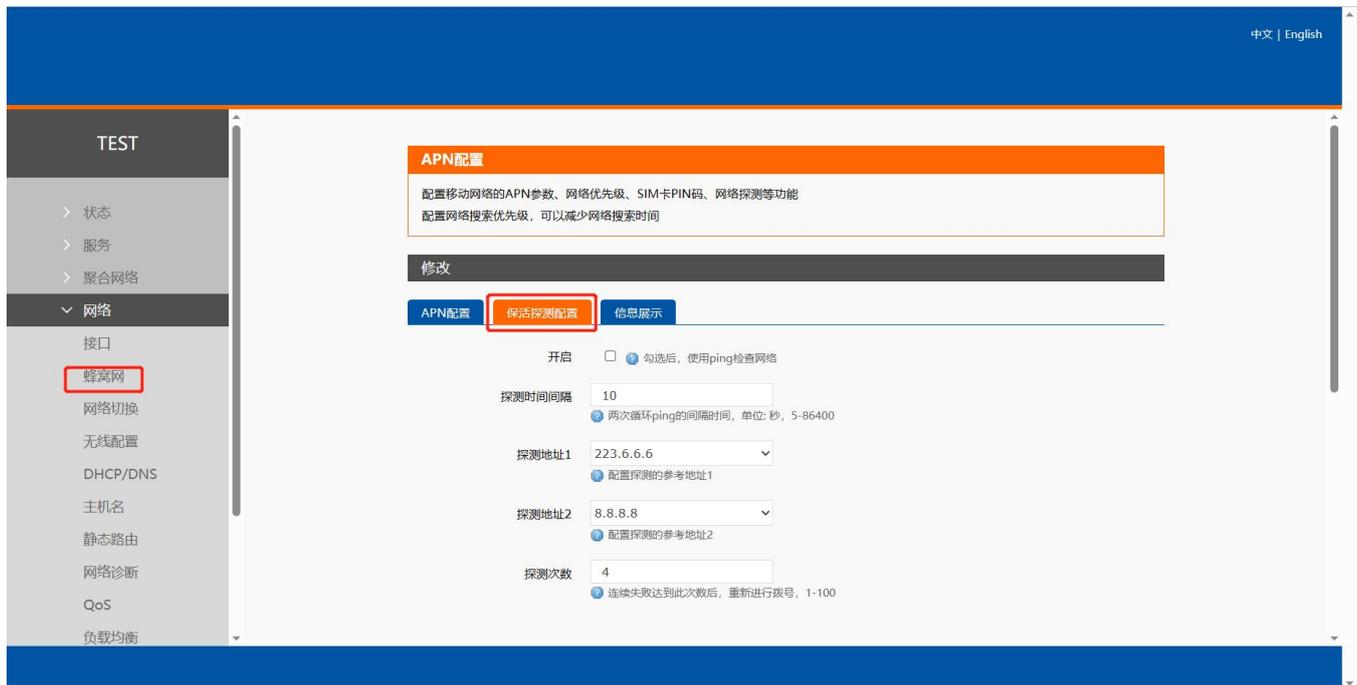


图 26 保活探测配置页面

表 10 保活探测配置表

名称	含义	默认值
开启	勾选: 开启	自动检测
探测时间间隔	ping 的时间间隔,单位:s	10
探测地址 1	ping 探测的地址 其中一个探测地址能 ping 通则表示网络通畅	223.6.6.6
探测地址 2	ping 探测的地址 其中一个探测地址能 ping 通则表示网络通畅	8.8.8.8
探测次数	ping 的次数	AUTO

<说明>

- 路由器保活探测配置界面上面是 SIM1 的设置, 往下拉有一样的配置界面为 SIM2 配置界面;
- 当界面填写的 2 个探测地址和内部预留的 ping 探测地址都不通时则认为网络异常, 将重新驻网拨号。

4.1.4. SIM 卡信息显示

SIM 卡信息显示会详细得显示出 SIM 卡的配置信息, 如果联网出现问题可以在此查看问题的原因。

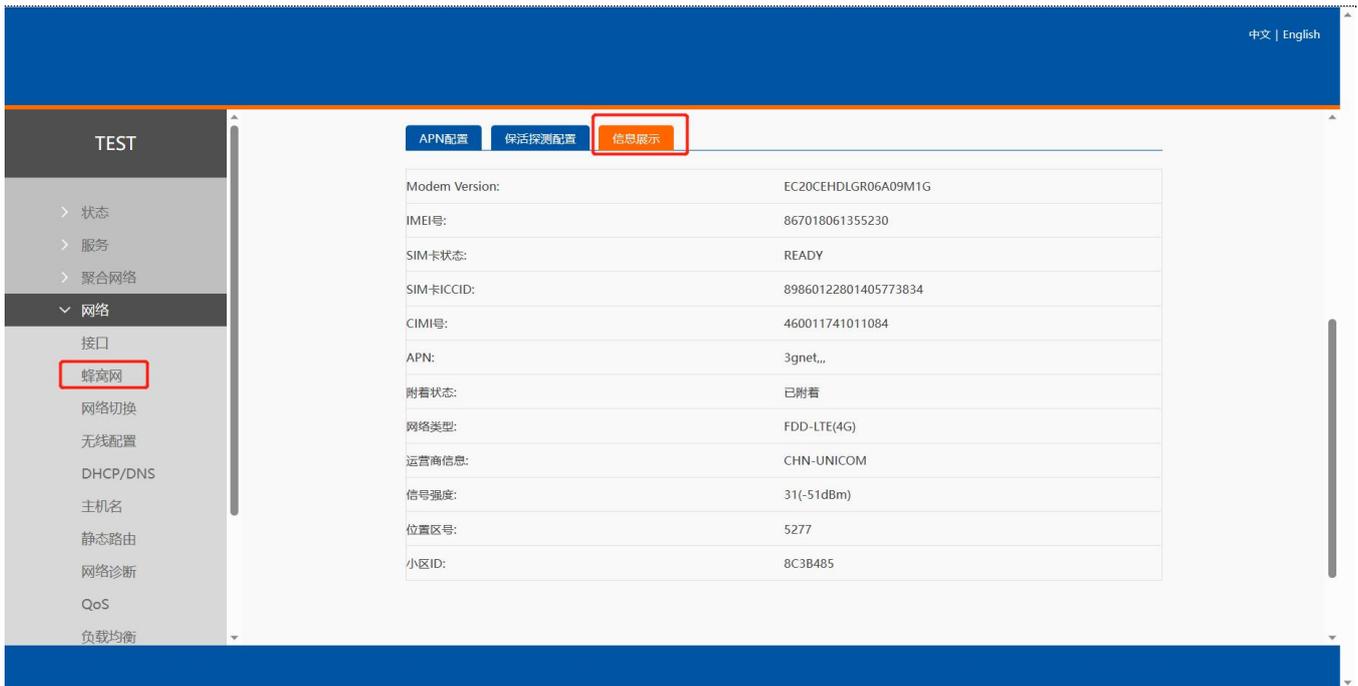


图 27 SIM 卡信息显示

4.2. 无线配置

USR-G810 具备双频 WiFi 功能：2.4GHz 和 5.8GHz 无线网络。可以在基本设置、高级设置里面对双频 WiFi 的参数进行修改。如不需要 WiFi 功能，可直接选择禁用。

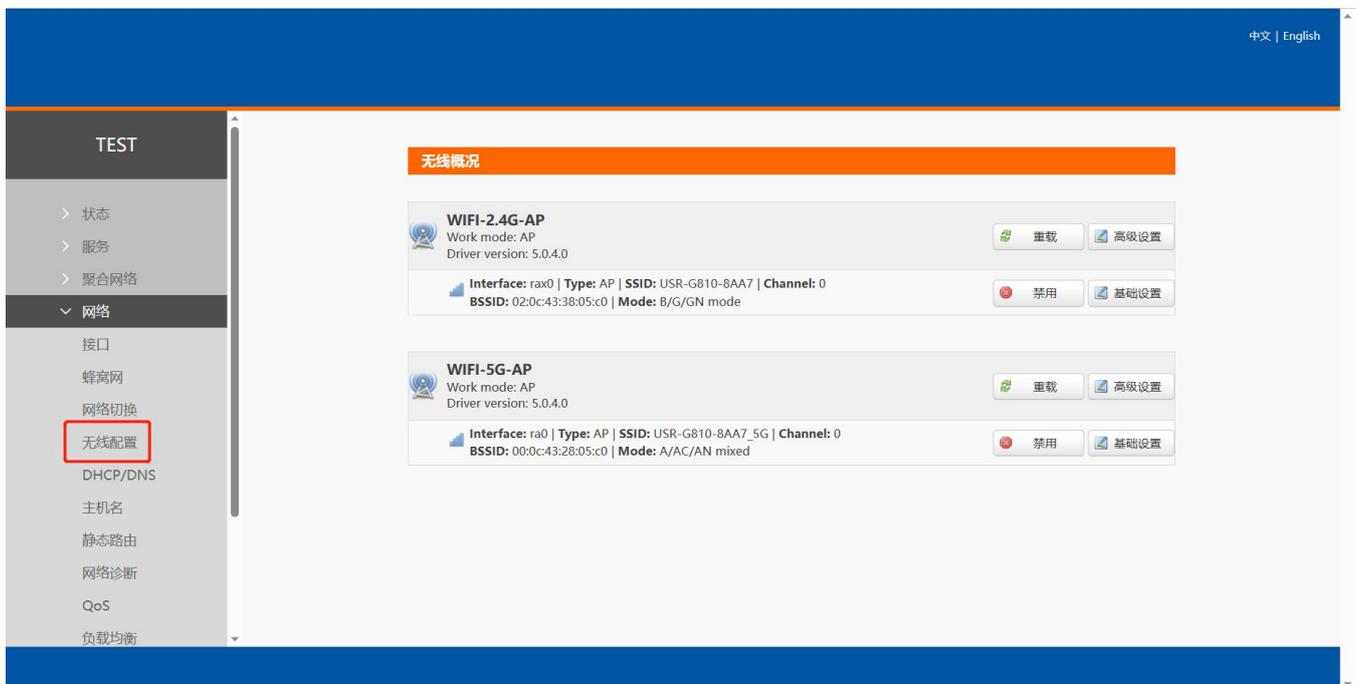


图 28 无线配置界面

<说明>

- G810 路由器本身是一个 AP，其它无线终端可以接入到它的 WLAN 网络。支持最多 24 个无线 STA 连接；

- 本 WLAN 局域网与有线 LAN 口互为交换方式；
- WiFi 最大覆盖范围为空旷地带 200m，办公室等有障碍物地受环境影响可在 40m 内覆盖。

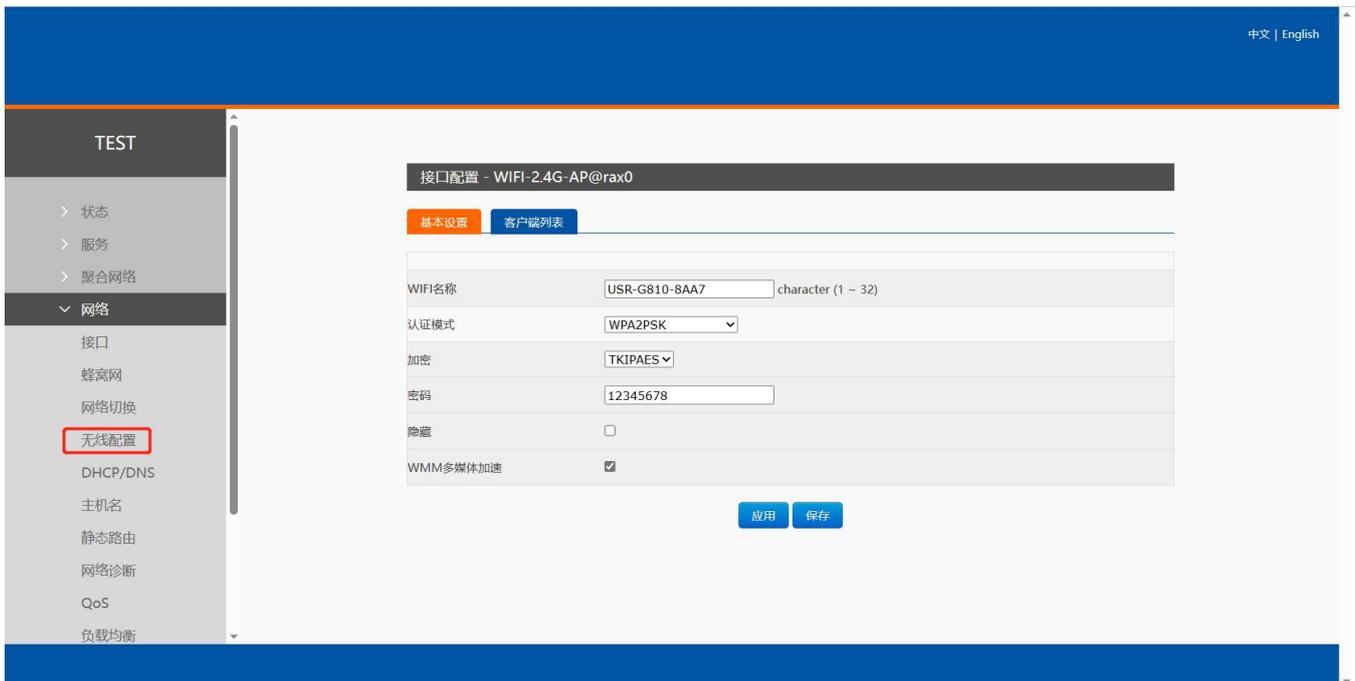


图 29 无线-SSID 设置页面

表 11 无线 WiFi 基本设置参数表

默认参数	说明	默认值
WiFi 名称	WiFi 名称	2.4G:USR-G810-XXXX 5G: USR-G810-XXXX_5G (最后为 MAC 地址后 4 位)
认证模式	WiFi 的认证模式，可设置 Disable/WPA2PSK/WPA3PSK/WPA2PSK/WPA3PSK	WPA2PSK
加密	TKIP/TKIPAES/AES	TKIPAES
密码	WiFi 密码	12345678
隐藏	勾选后客户端搜索不到本 WiFi 名称 连接时需要输入正确 WiFi 名称和密码才可连接	未勾选

在“无线配置→WiFi-2.4G-AP (WiFi-5G-AP) →基础设置→无线客户端”查看客户端的列表信息。

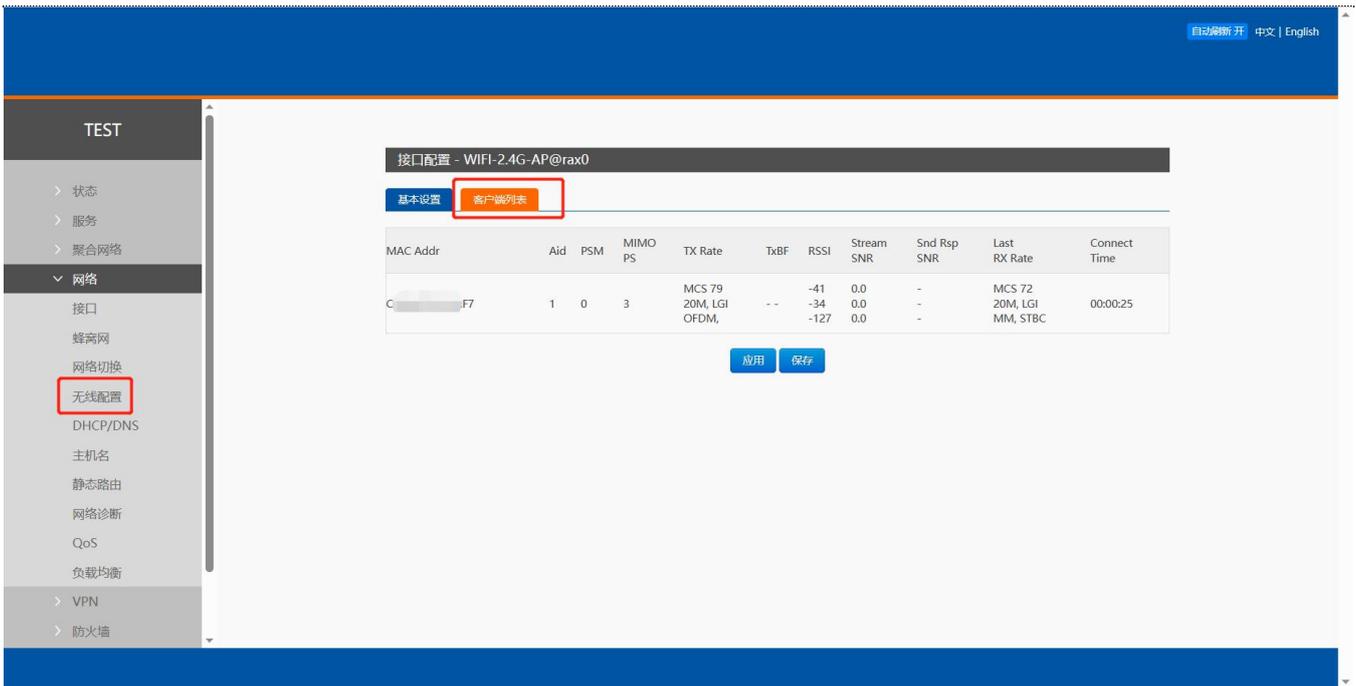


图 30 无线-客户端列表

在“无线配置→WiFi-2.4G-AP (WiFi-5G-AP) →高级设置”修改信道、带宽、发射功率。

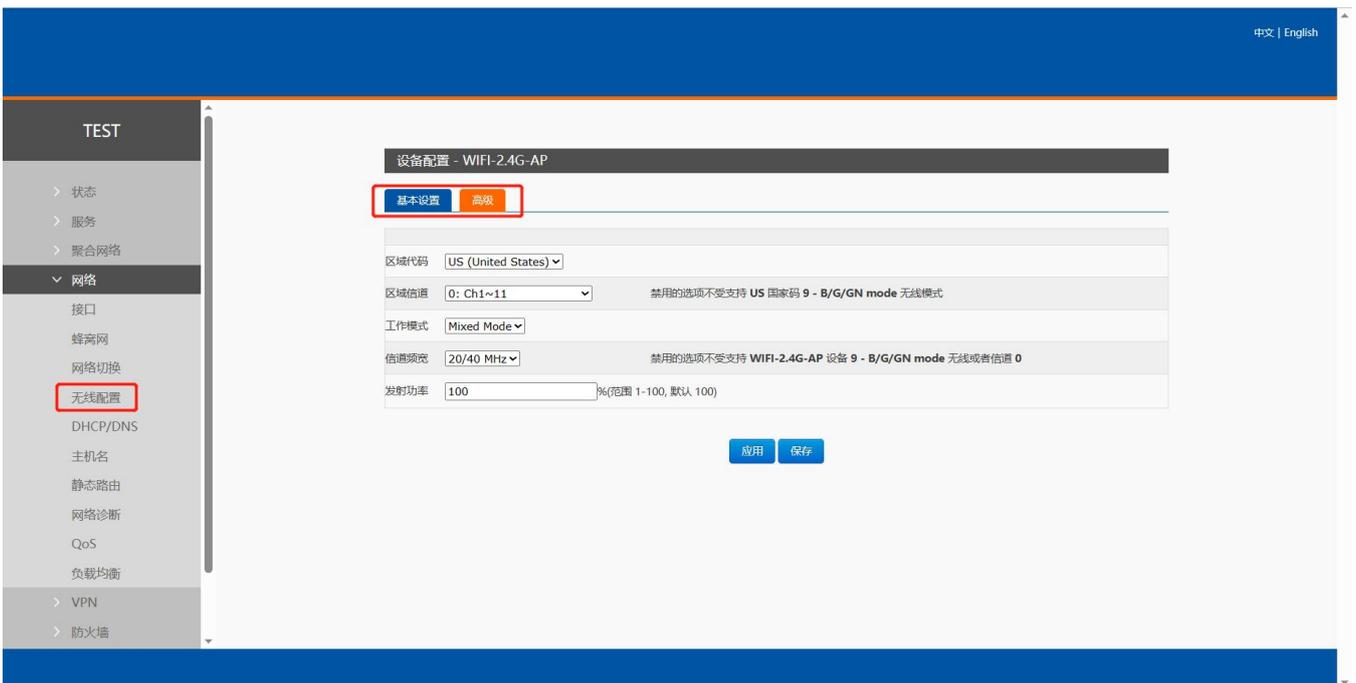


图 31 无线-信道设置页面

4.3. LAN 接口

LAN 口为千兆局域网络，本设备具备 3 个有线 LAN 口。

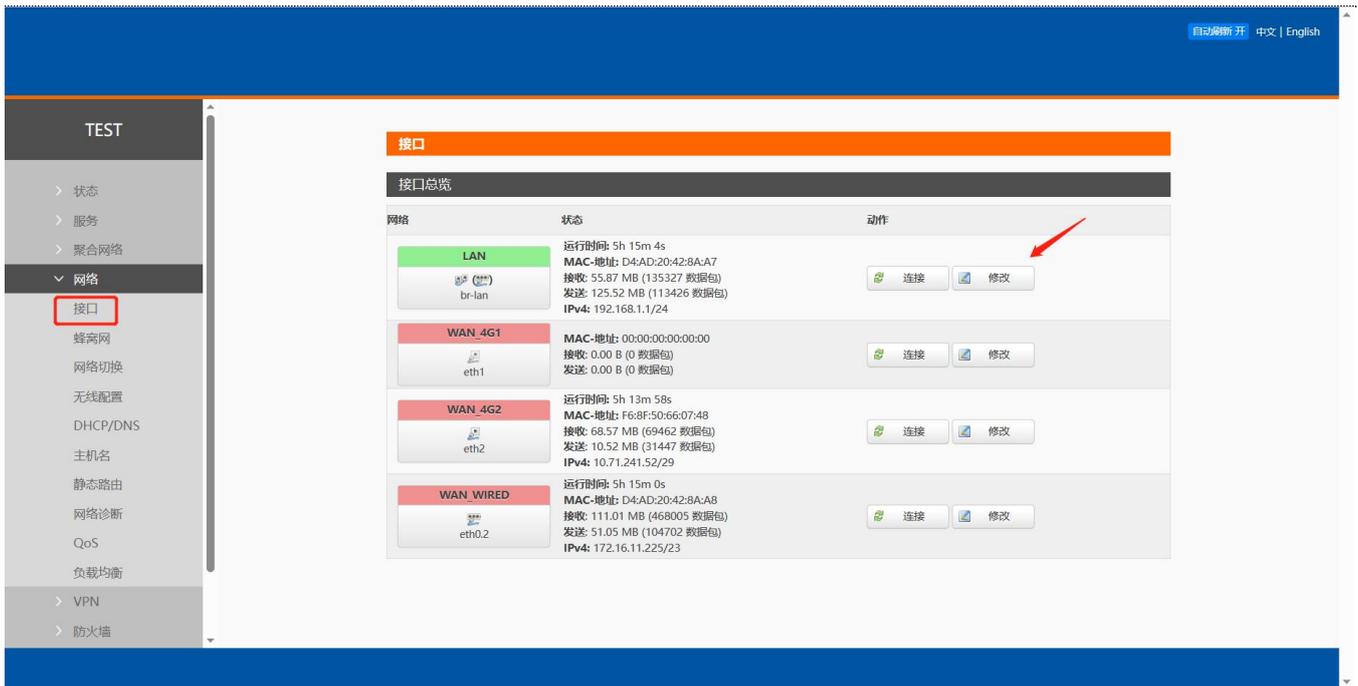


图 32 LAN 口设置页面

<说明>

- 3 个 LAN 口；
- 默认静态的 IP 地址 192.168.1.1，子网掩码 255.255.255.0。本参数可以修改，比如静态 IP 修改为 192.168.2.1；
- WIFI 桥接到了 LAN 口，和 LAN 同网段；
- 默认开启 DHCP 服务器功能，所有接入到路由器 LAN 口的设备均可自动获取到 IP 地址；
- 具备简单的状态统计功能。

4.3.1. DHCP 功能

LAN 口的 DHCP Server 功能默认开启（可以选择关闭），所有接入 LAN 口的网络设备，可以自动获取到 IP 地址。

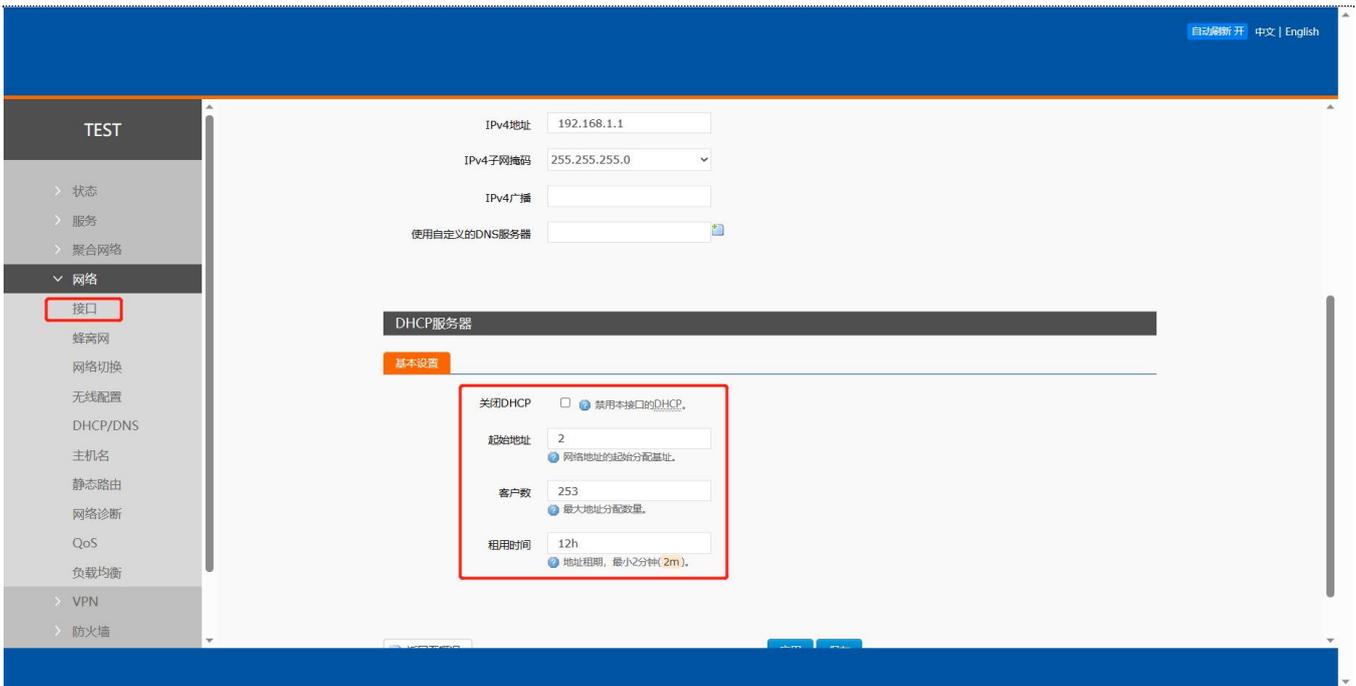


图 33 DHCP 设置页面

<说明>

- 可以调整 DHCP 池的开始地址，以及地址租用时间；
- DHCP 默认分配范围从 192.168.1.2 开始；
- 默认租期 12 小时。

4.4. DHCP/DNS

静态地址分配（IP-MAC 绑定）：该功能是 LAN 接口 DHCP 设置的延伸，用于给 DHCP 客户端分配固定的 IP 地址和主机标识。

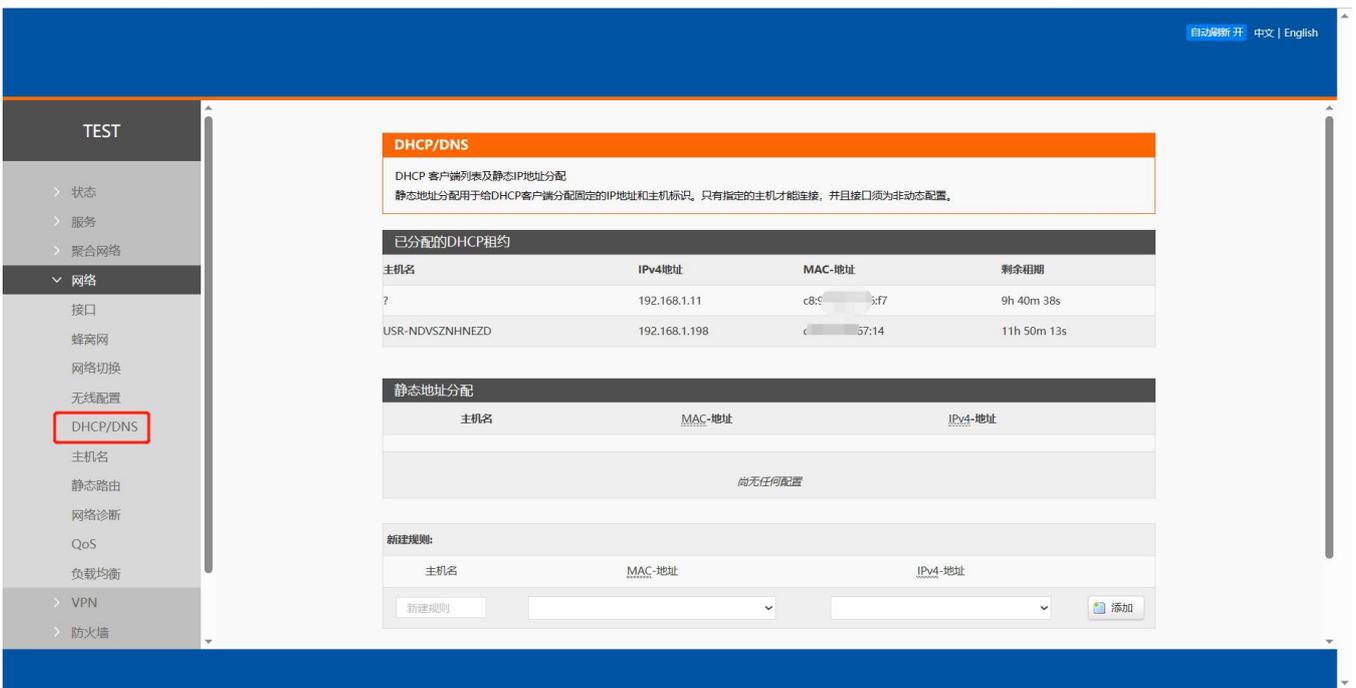


图 34 DHCP/DNS 设置页面

表 12 DHCP/DNS 参数表

默认参数	说明	默认值
主机名	子网设备的名称	空
MAC 地址	子网设备的 MAC 地址	空
IPv4 地址	设置的 IPv4 地址	空

<说明>

- 最多可添加 20 条 DHCP/DNS 规则；
- IPv4 地址请和 LAN 口设置同网段，否则无法正常通信。

4.5. WAN 口

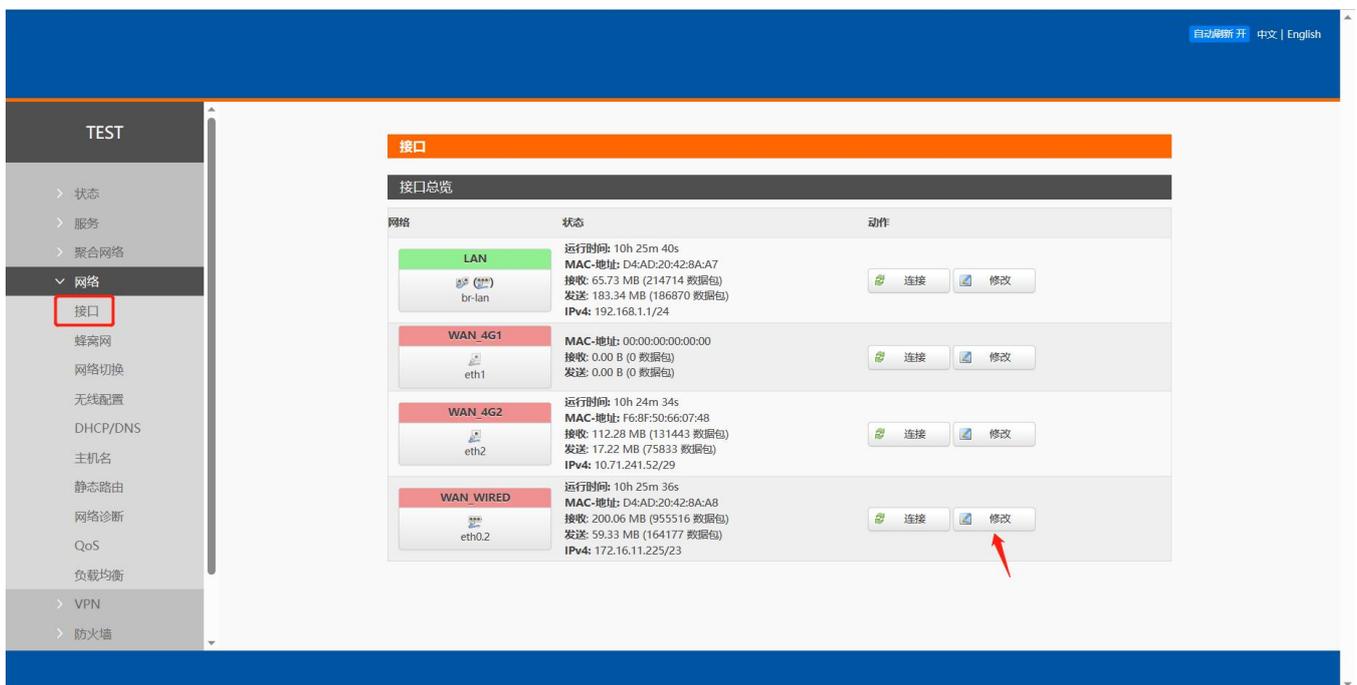


图 35 WAN 口设置页面

<说明>

- 1 个有线 WAN 口，WAN 口为广域网接口；
- 支持 DHCP 客户端，静态 IP，PPPOE 模式；
- 默认 DHCP 客户端；
- WAN 口 IP 不可与 LAN 口 IP 同网段。

4.5.1. DHCP 客户端

上级路由器必须开启 DHCP 服务，用网线插入上级路由器 LAN 和本路由器 WAN，G810-33 才可获取 IP。

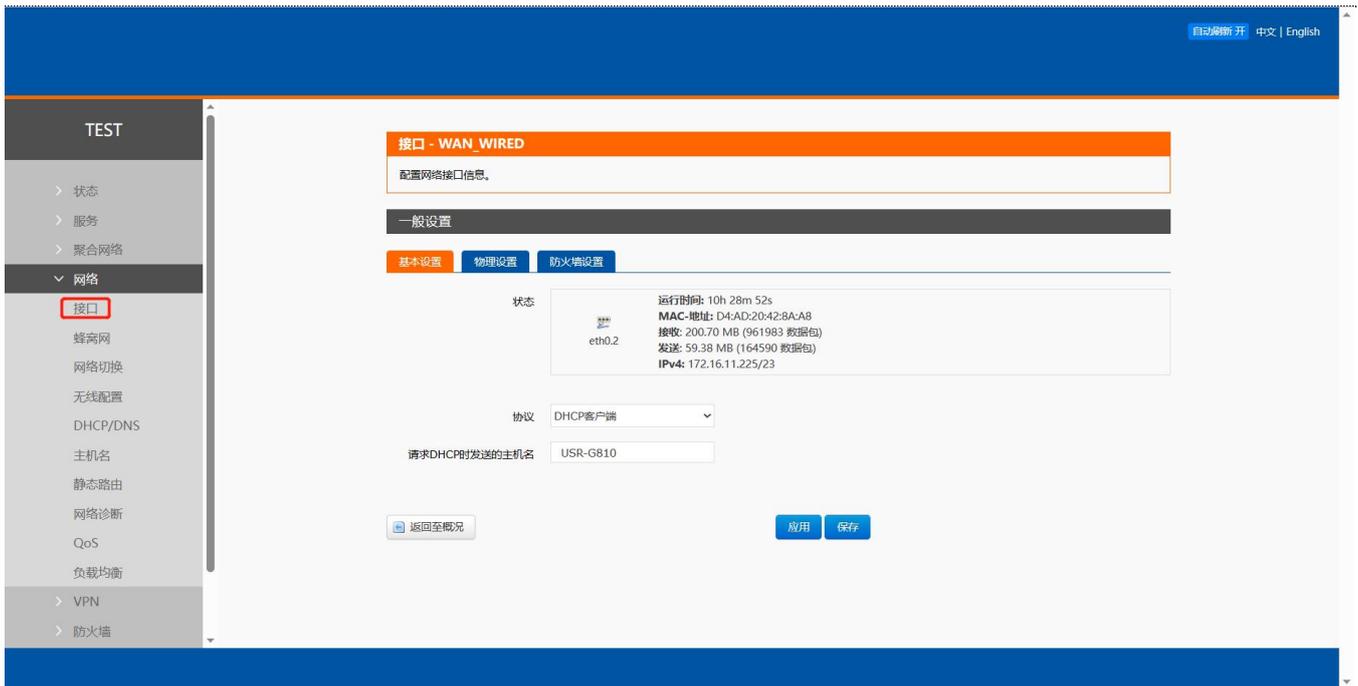


图 36 WAN 口设置-DHCP

4.5.2. 静态 IP

填写和上级路由器同网段 IP，IP、网关和子网掩码需要正确填写，如是专线公网网线，需按照运营商给出的 IP、子网掩码、网关以及 DNS 服务器正确填写。

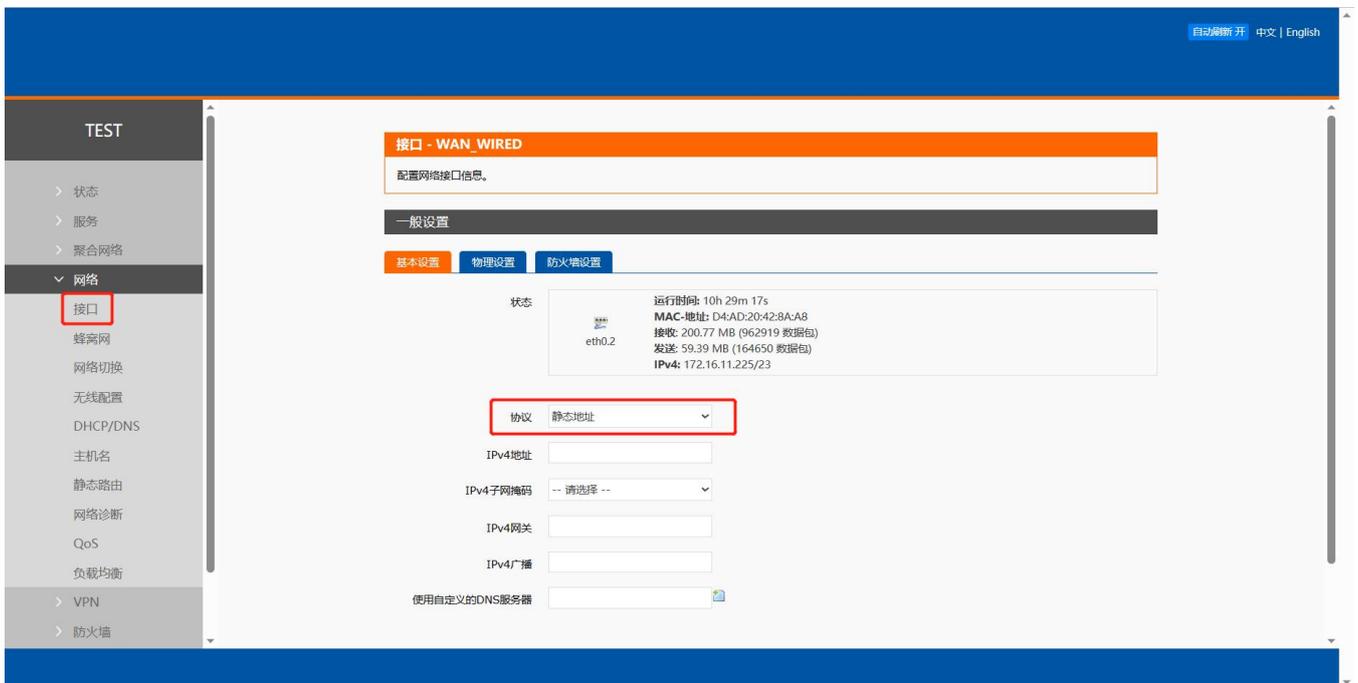


图 37 WAN 口设置-静态 IP

4.5.3. PPPoE

需按照运营商给出的正确用户名和密码填写。

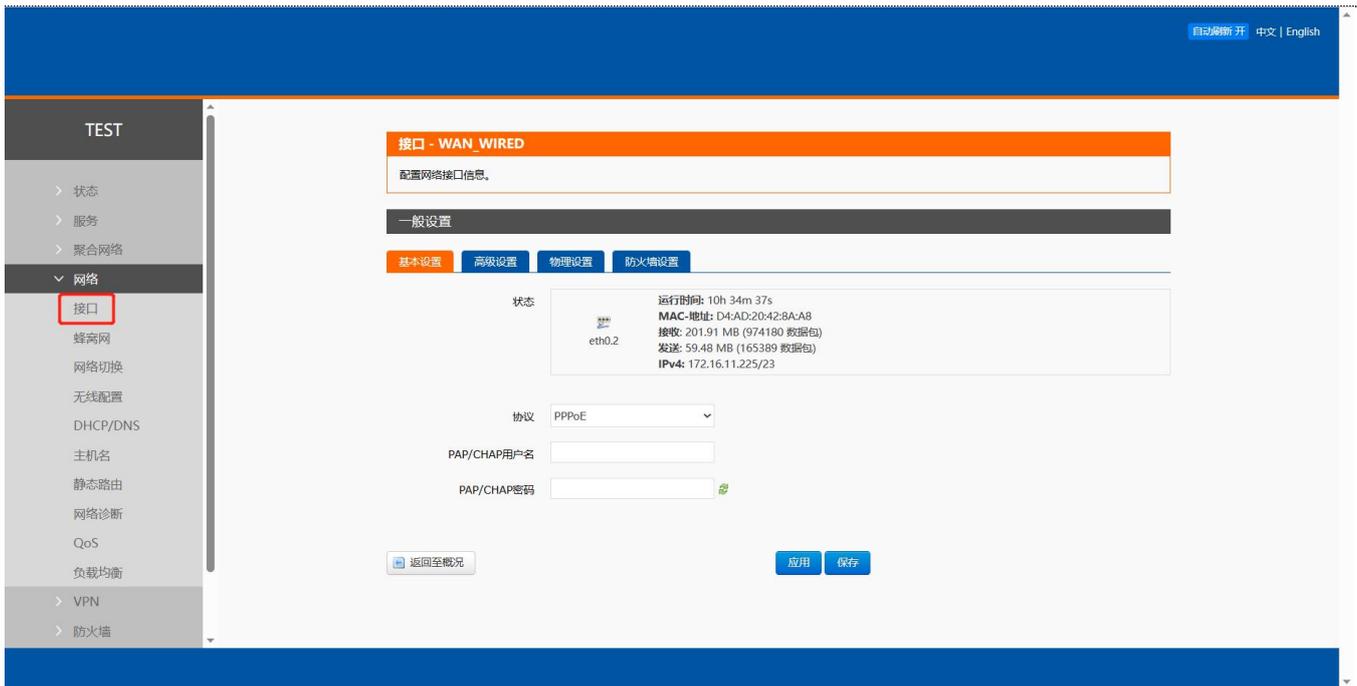


图 38 WAN 口设置-PPPoE

4.6. 网络切换

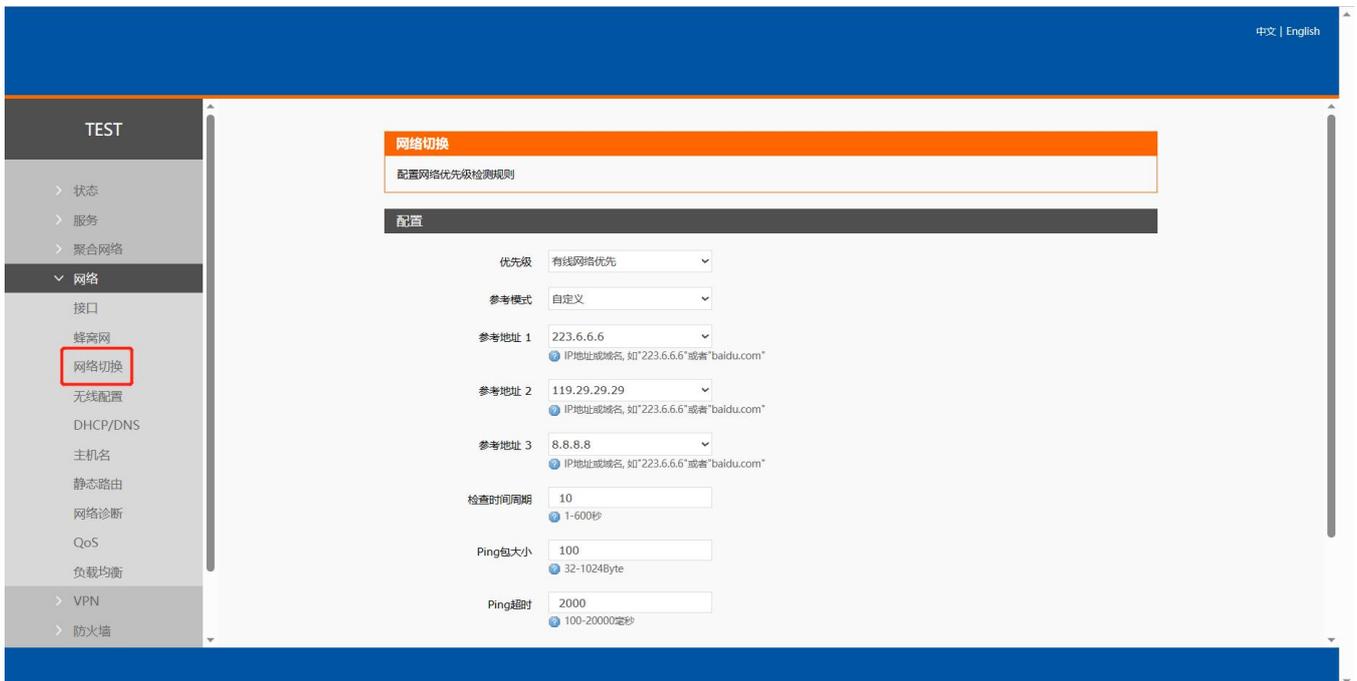


图 39 网络切换配置

表 13 网络切换配置

名称	描述	默认参数
----	----	------

优先级	有线网络优先 4G1 网络优先 4G2 网络优先 禁用：禁用网络切换功能，使用当前上网方式上网	有线网络优先
参考模式	自定义：根据自定义参考地址确定网络状态 网关：参考网关确定网络状态	自定义
参考地址 1	可设置 IP/域名	223.6.6.6
参考地址 2	可设置 IP/域名	119.29.29.29
参考地址 3	可设置 IP/域名	8.8.8.8
检测间隔（单位：s）	设置链路检测间隔：可设置 1-600s	10
ping 包大小（单位：字节）	检测链路时包大小：可设置 32-1024 字节	100
Ping 超时（单位：ms）	设置 ping 超时时间：可设置 100-20000ms	2000

<说明>

- 配置网络优先级检测规则，默认启用，默认切网顺序：有线网络优先；
- 设定 3 组检测联网状态的 IP 地址（也可以设定域名），如能够 ping 通其一，则判断网络正常，不进行任何切网配置；
- 如 3 组检测规则均无法 ping 通，则执行切网操作，继续进行 ping 包检测；
- 如有线网络、蜂窝网络均无法 ping 通，则判断路由器无法连接外网。

4.7. 主机名

主机名功能为自定义挟持域名功能，可将自定义域名对应 IP（需要客户端 DNS 指向本路由生效）。

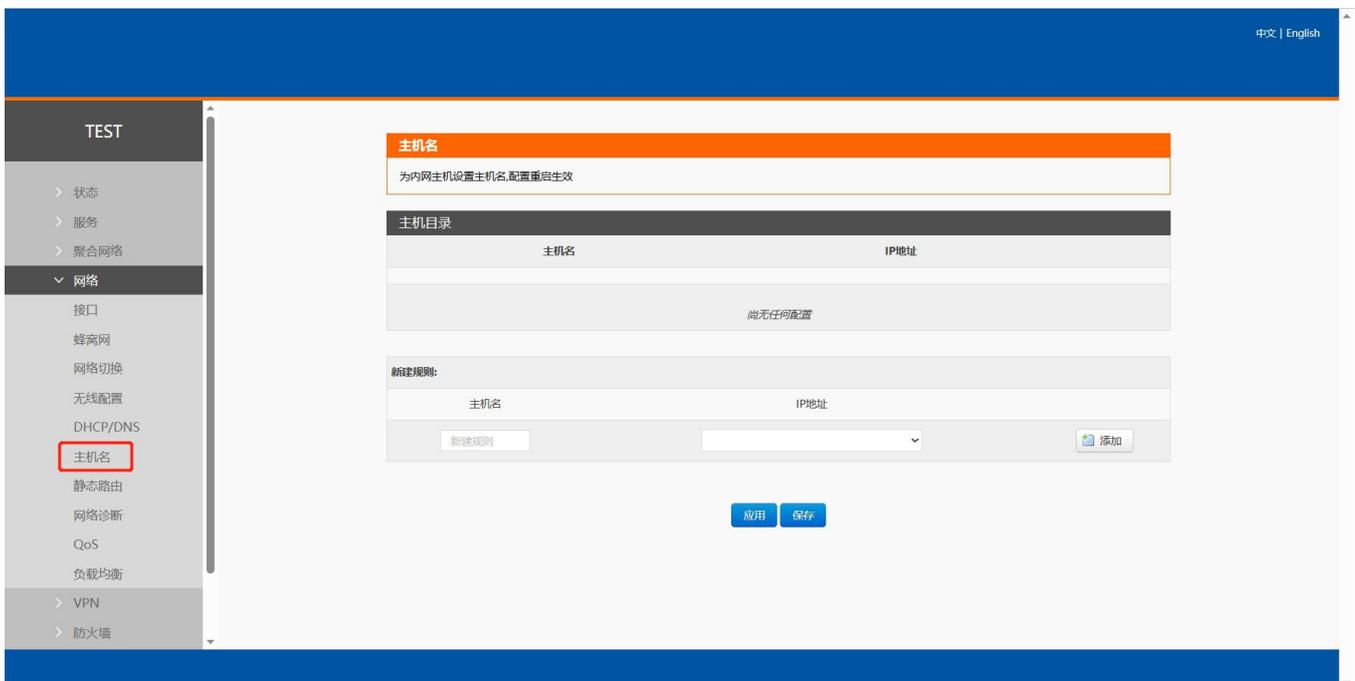


图 40 主机名配置

<说明>

- 主机名最多可设置 20 条。

4.8. 静态路由

静态路由有如下几个参数。

表 14 静态路由参数表

名称	描述	默认参数
接口	lan、wan_4g1、wan_4g2、wan_wired、vpn 接口	lan
对象（目标地址）	要访问的对象的地址或地址范围	空
子网掩码	要访问的对象网络的子网掩码	空
网关（下一跳）	要转发到的地址	空
跃点数（Metric）	包跳跃个数	空

静态路由描述了以太网上数据包的路由规则。

测试示例：测试环境，两个平级路由器 A 和 B，如下图。

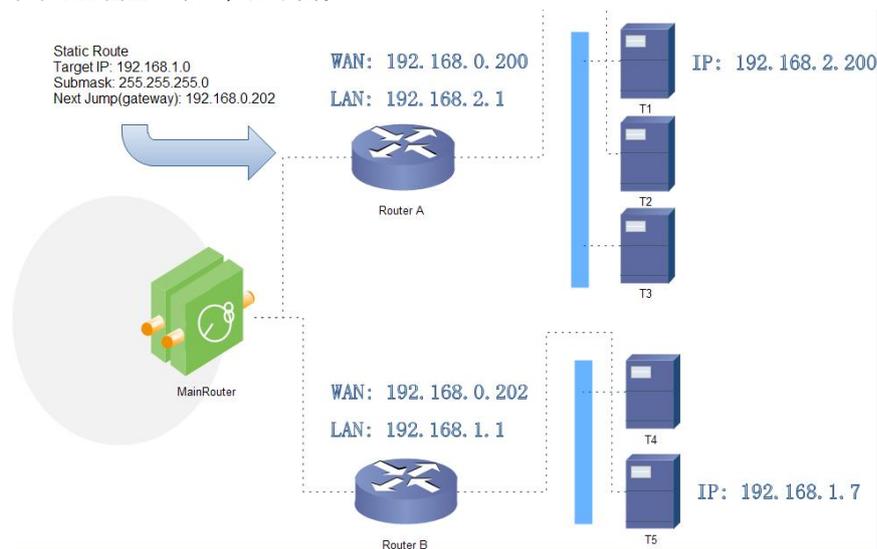


图 41 静态路由表实例图

路由器 A 和 B 的 WAN 口都接在 192.168.0.0 的网络内，路由器 A 的 LAN 口为 192.168.2.0 子网，路由器 B 的 LAN 为 192.168.1.0 子网。

现在，如果我们要在路由器 A 上做一条路由，使我们访问 192.168.1.x 地址时，自动转给路由器 B。

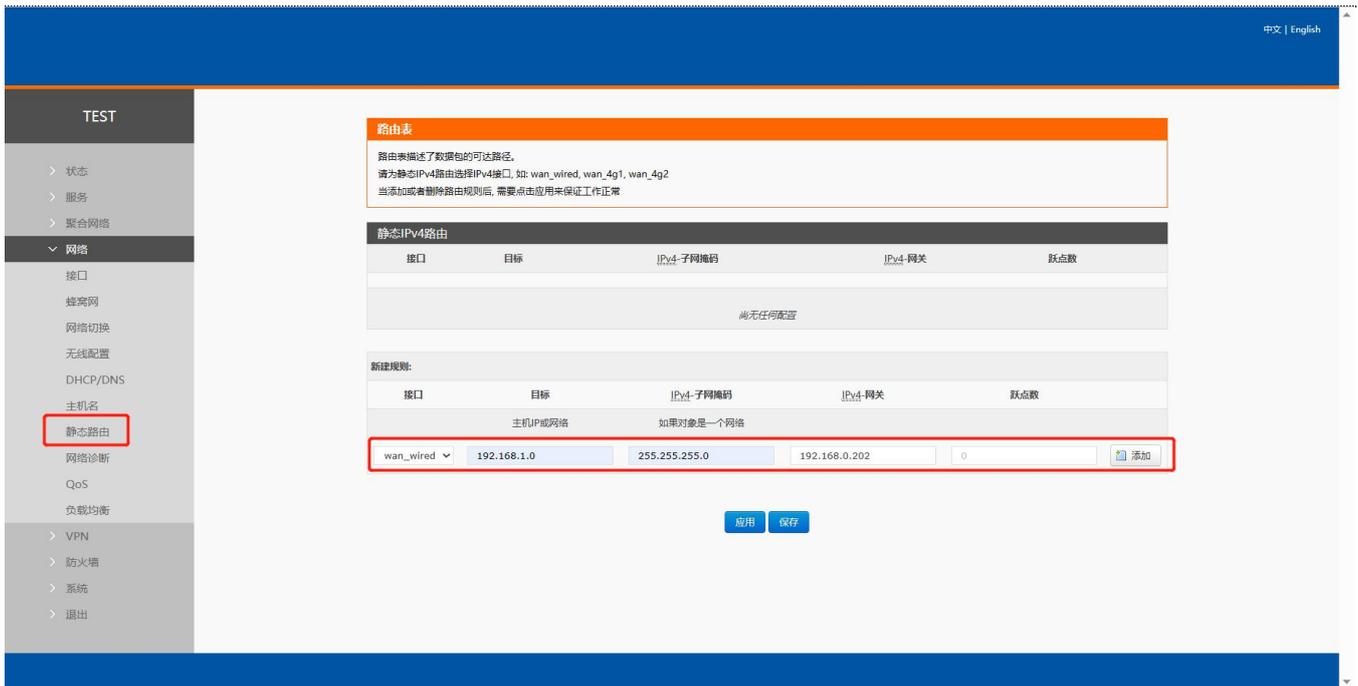


图 42 路由表添加页面

<说明>

- 静态路由最多可添加 20 条规则。

4.9. 网络诊断功能

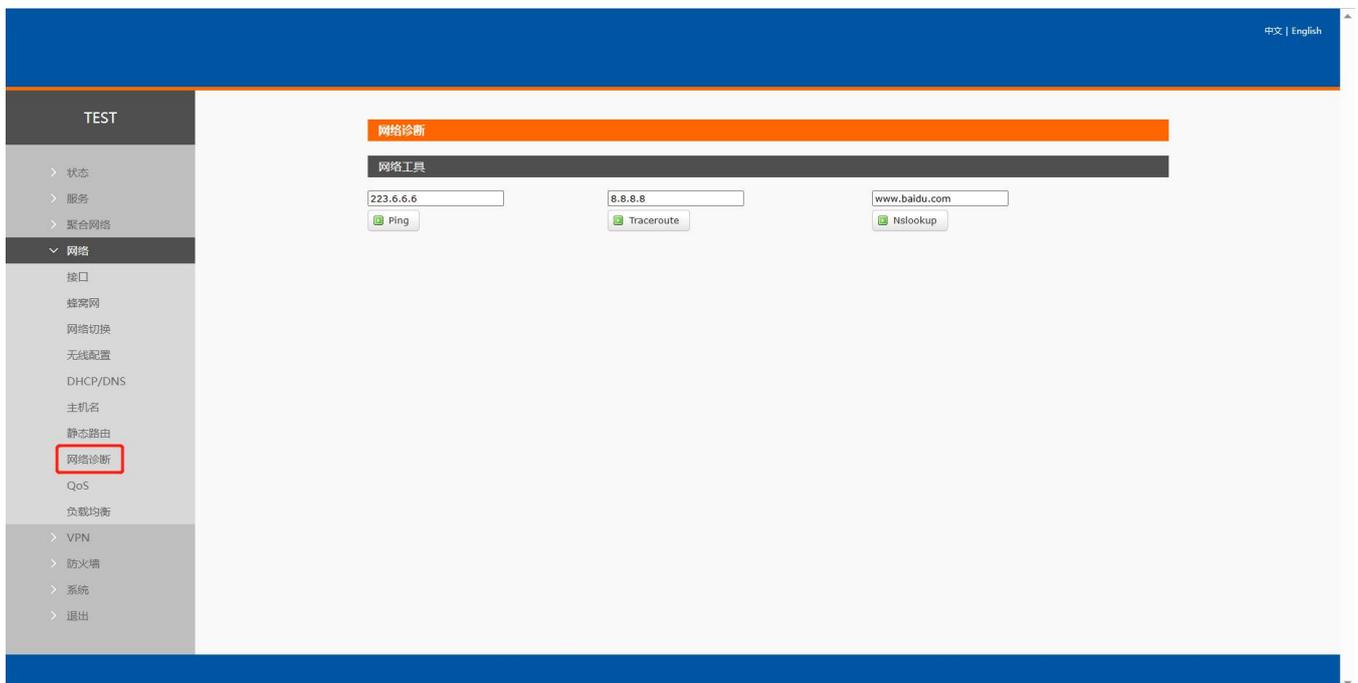


图 43 网络诊断页面

<说明>

- 在线诊断功能，包括 Ping 工具，路由解析工具，DNS 查看工具；
- Ping 是 Ping 工具，可以直接在路由器端，对一个特定地址进行 ping 测试；

- Traceroute 是路由解析工具，可以获取访问一个地址时，经过的路由路径；
- Nslookup 是 DNS 查看工具，可以将域名解析为 IP 地址。

4.10. QoS

QoS (Quality of Service) 即服务质量。在有限的带宽资源下，QoS 为各种业务分配带宽，为业务提供端到端的服务质量保证。例如，语音、视频和重要的数据应用在网络设备中可以通过配置 QoS 优先得到服务。

<说明>

- 开启聚合服务时，负载均衡功能将自动关闭，再次关闭聚合服务时负载均衡自动打开；
- 聚合服务开启后，不影响网络切换功能；
- 服务优先顺序：QoS>聚合服务>负载均衡。

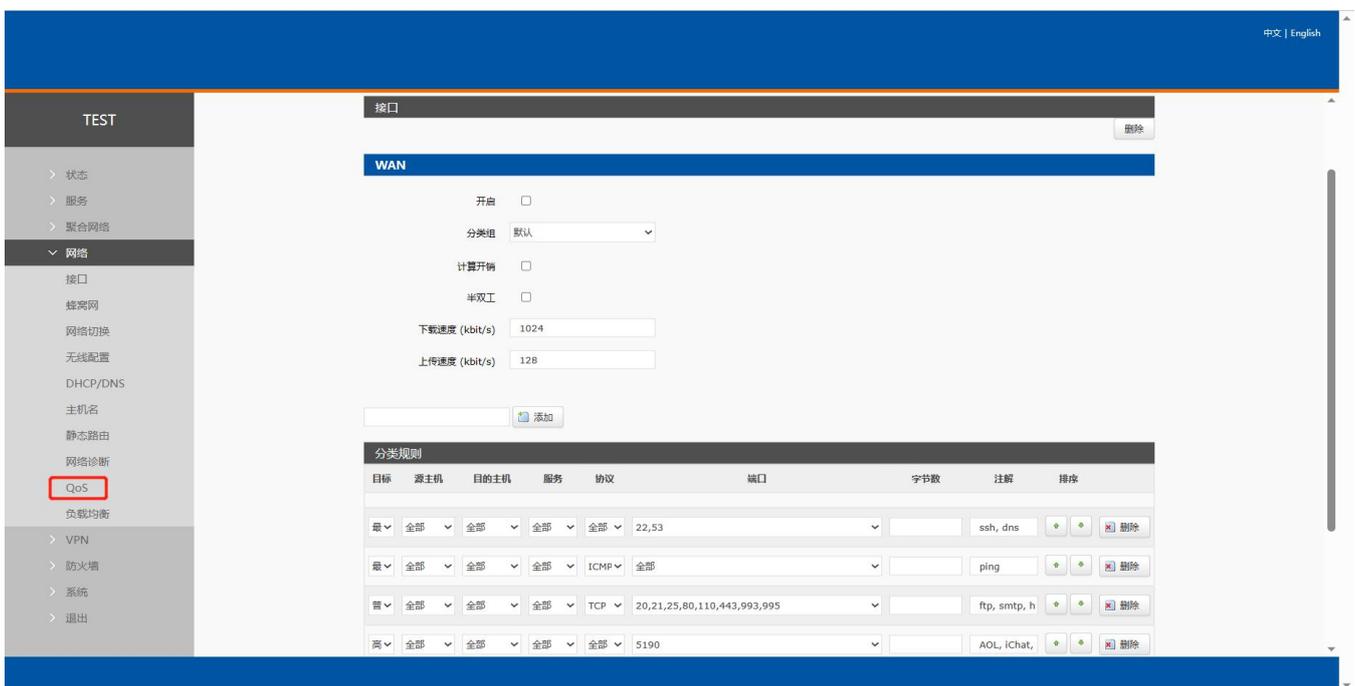


图 44 QoS 设置页面

4.10.1. 接口限速

可以新建一个接口限速，此处的接口与下列一致，添加接口使用小写即可，添加后会自动显示大写格式。

表 15 接口表

名称	网卡名
LAN 接口	lan
有线 WAN 接口	wan_wired
蜂窝 SIM1	wan_4g1
蜂窝 SIM2	wan_4g2

举例：将 WAN 口限速上下行 100kbit/s 左右。

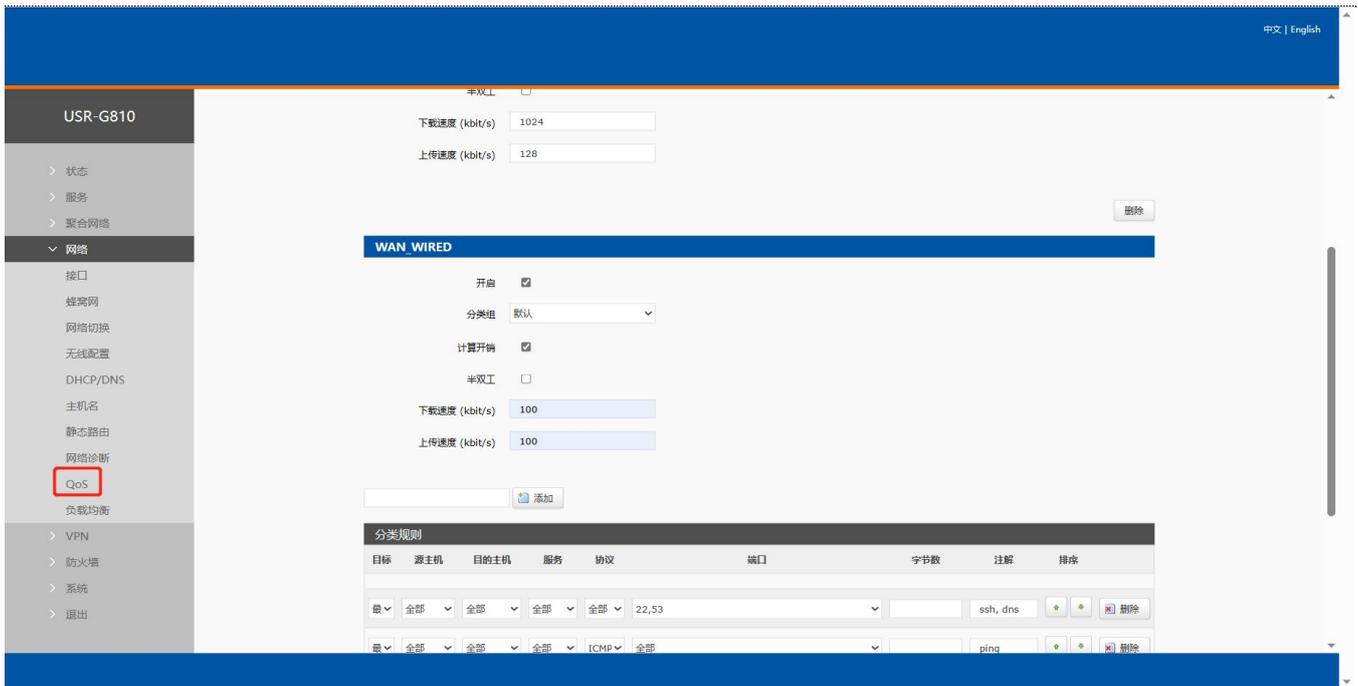


图 45 接口限速设置页面

<说明>

- 开启：是否在此接口启用 QoS，勾选则启用；
- QoS 接口限速如和聚合路由选择的接口并用，首先“接口限速”会作用在该接口，其次“分类规则”也会作用在该接口；
- 上传速度：会将上传的速度限制在此速率附近，单位为 kbit/s，（注意：网上的文章表明此处仅限 TCP）；
- 下载速率：会将下载的速度限制在此速率附近，单位为 kbit/s。

4.10.2. 分类规则

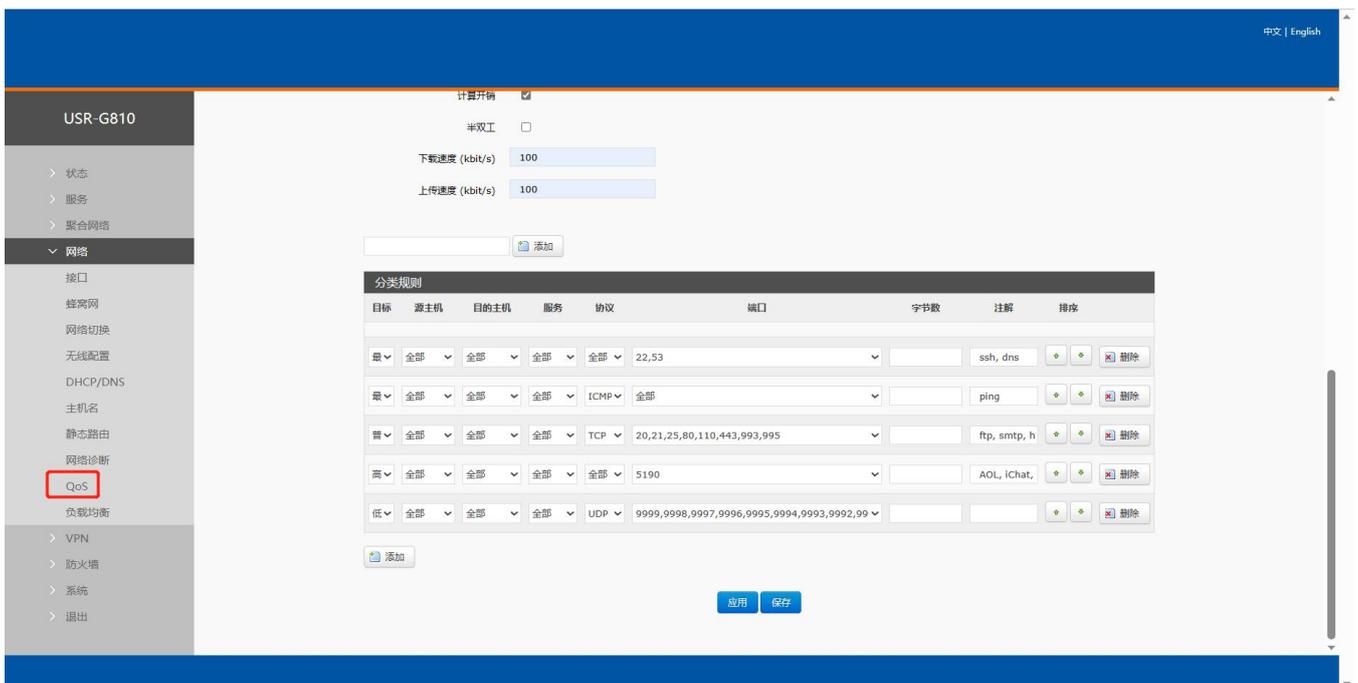


图 46 分类规则设置页面

<说明>

- 目标：一种分类标记，可选项：最高/高/普通/低，QoS 会将符合条件的数据包加上对应的标记；
- 源主机：数据包的源地址，填写 IP 地址；
- 目标主机：数据包的目的地址，填写 IP 地址；
- 服务：可选针对某种网络服务，可选项 aim/bittorrent/edonkey/fasttrack/ftp...
- 协议：TCP/UDP/ICMP/自定义；
- 端口：可选针对不同端口，多个端口使用逗号隔开；
- 包大小：定义需要匹配的字节数大于等于该数值，单位 bytes，如需设置最大长度,匹配小于 50000 字节的包(:50000)，匹配 500-3000 字节内的包(500:3000)；
- 注释：解释文字，用来给人员方便查看的。

4.11. 负载均衡

本设备采用 mwan3 软件，它的作用是把路由器的流量，做路由表级别的负载均衡，按照设置的优先级和权重分配到不同的 WAN 口上，从而起到网速叠加的作用。

<说明>

- 当开启聚合服务时，负载均衡将自动关闭；
- 默认禁用负载均衡，如使用负载均衡功能请正确配置；
- 开启聚合服务时，负载均衡功能将自动关闭，再次关闭聚合服务时负载均衡自动打开；
- 当 QoS 具备接口限速，优先 QoS 限速功能，负载均衡功能仍旧生效，QoS 限速接口数据包速率低；
- 服务优先顺序：QoS>聚合服务>负载均衡。

表 16 各 WAN 接口表

名称	网卡名
有线 WAN 接口	wan_wired
蜂窝 SIM1	wan_4g1
蜂窝 SIM2	wan_4g2

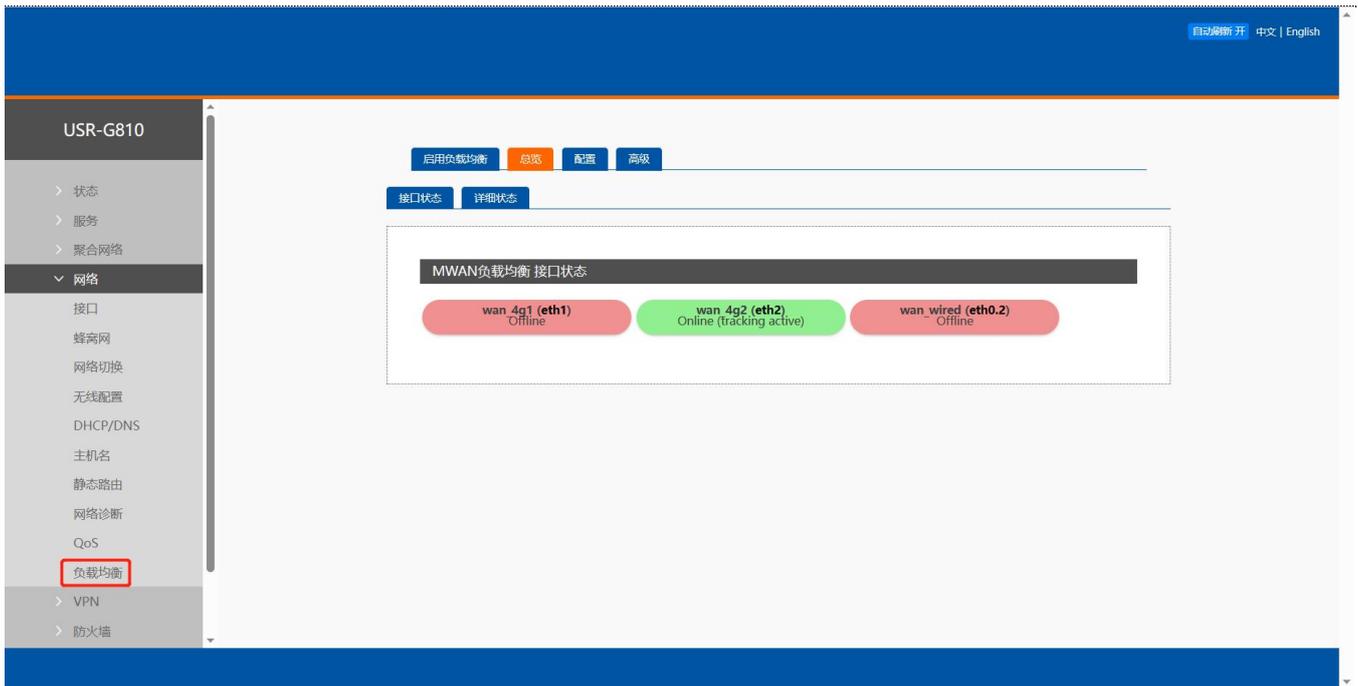


图 47 负载均衡设置页面

5. VPN 功能

VPN (Virtual Private Network) 虚拟专用网，在协议上又分为 PPTP、L2TP、IPSec、OpenVPN、GRE 等。接下来分别介绍一下这几种协议创建 VPN 的原理。

PPTP:

是一种点对点的隧道协议,使用一个 TCP(端口 1723)连接对隧道进行维护,使用通用的路由封装(GRE)技术把数据封装成 PPP 数据帧通过隧道传送,在对封装 PPP 帧中的负载数据进行加密或压缩。其中 MPPE 将通过由 MS-CHAP V2 身份验证过程所生成的加密密钥对 PPP 帧进行加密。

L2TP:

是第二层隧道协议,与 PPTP 类似。目前 G810-33 支持隧道密码认证、用户名密码认证方式,支持 L2TP OVER IPSec 的预共享密钥加密。

IPSec:

协议不是一个单独的协议,它给出了应用与 IP 层上网络数据安全的一整套体系结构,包括网络认证协议 ESP、IKE 和用于网路认证及加密的一些算法等。其中 ESP 协议用于提供安全服务,IKE 协议用于密钥交换。

OpenVPN:

支持基于证书的双向认证,也就是说客户端需认证服务端,服务端也要认证客户端。

GRE:

GRE(Generic Routing Encapsulation、通用路由封装)协议是对某些网络层协议(如 IP 和 IPX)的数据报文进行封装,使这些被封装的数据报文能够在另一个网络层协议(如 IP)中传输。GRE 采用了 Tunnel(隧道)的技术,是 VPN(Virtual Private Network)的第三层隧道协议。

注意:

这几种协议都可以搭建出 VPN,具体可以根据自己的需求来选择比较适合的协议来搭建。

下面是这几种协议的版本号和具体搭建过程:

序号	协议	版本号
----	----	-----

1	PPTP	V1.10.0
2	L2TP	V1.3.15
3	IPSec	V5.3.3
4	OpenVPN	V2.4.7

5.1. PPTP Client

应用前需要获取到 VPN 服务器地址、账户、密码和加密方式，然后启用 PPTP 客户端，其他参数依次写入。

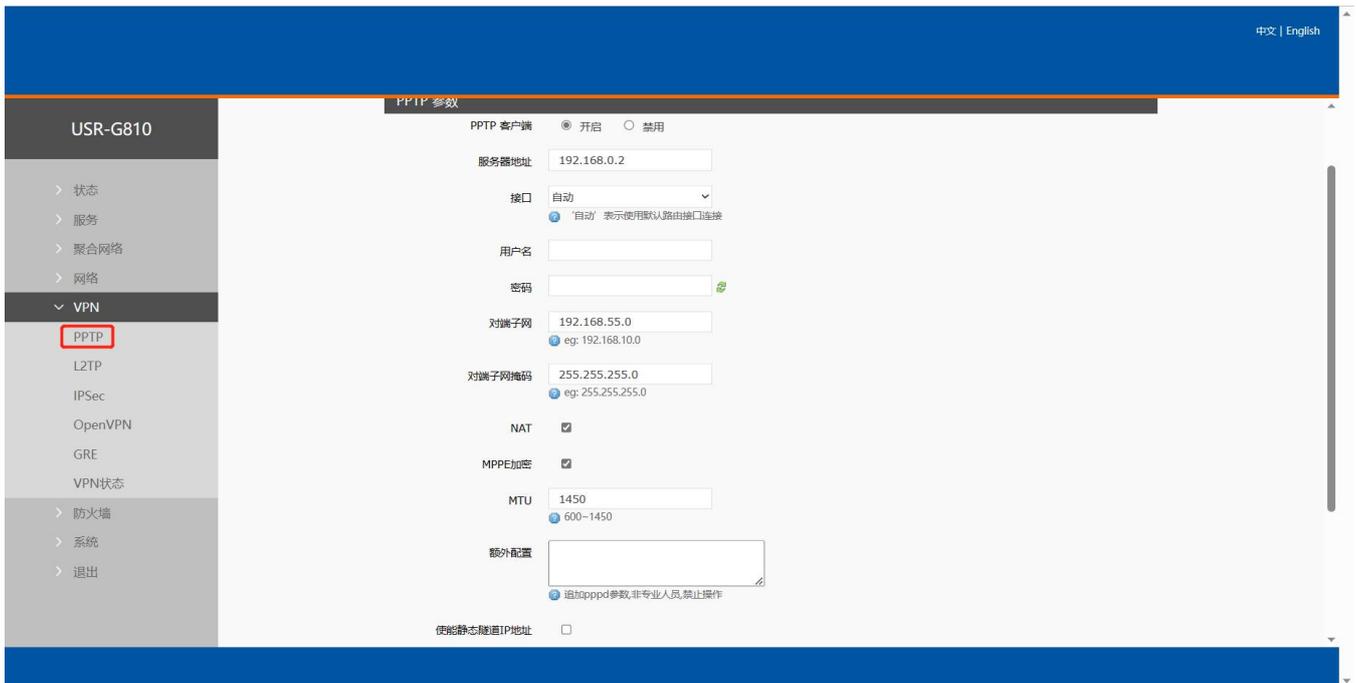


图 48 路由器添加 VPN 操作图一

<说明>

- 服务器地址：填写要连接的 VPN 服务器 IP 或者域名；
- 接口：根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动；
- 用户名/密码：从 VPN 服务器处获取；
- 加密方式：MPPE 加密、无加密，从 VPN 服务器端获取，根据实际情况选择打勾或不打勾；
- MTU 设置：设置通道的 MTU 值，默认 1450，本项设置需和 VPN 服务器对应；
- NAT 设置：该功能默认开启。当内容需要和外部通讯时，将内部地址替换成公用地址。关闭该项，则无法实现网络地址转换功能；
- 对端子网、掩码：填写正确后，在 NAT 功能开启下，可直接实现 VPN 下的子网互通功能；
- 使能静态隧道 IP 地址：默认未使能，服务器端自动分配 IP。可于此处填写静态隧道 IP；
- 额外配置：追加 PPPD 参数、魔术字等，默认不需要进行任何操作；
- 使能 ping:实时 VPN 在线检测及重连机制。通过 ping 自定义 IP 的方式，保证连接稳定。默认未启用。

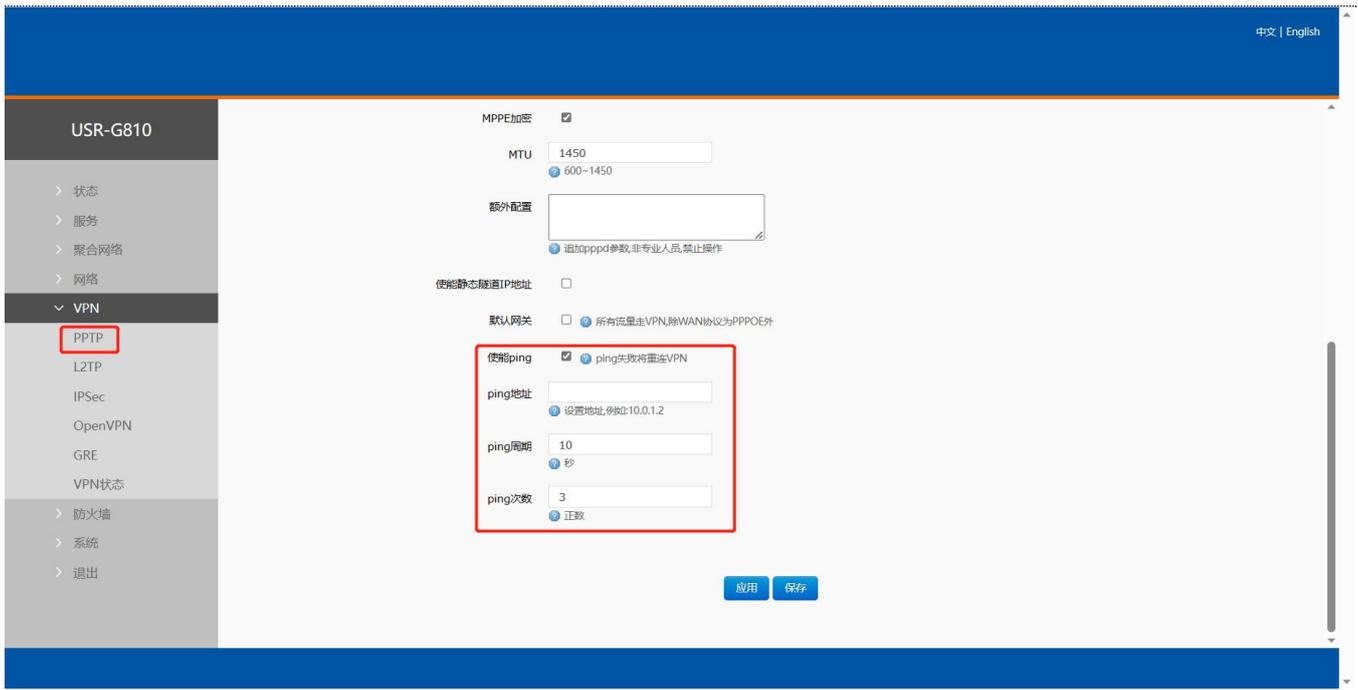


图 49 路由器启用 VPN 状态检测

PPTP 连接成功：完成相关参数的填入后，保存&应用，进入到 VPN--VPN 状态处查看连接状态。

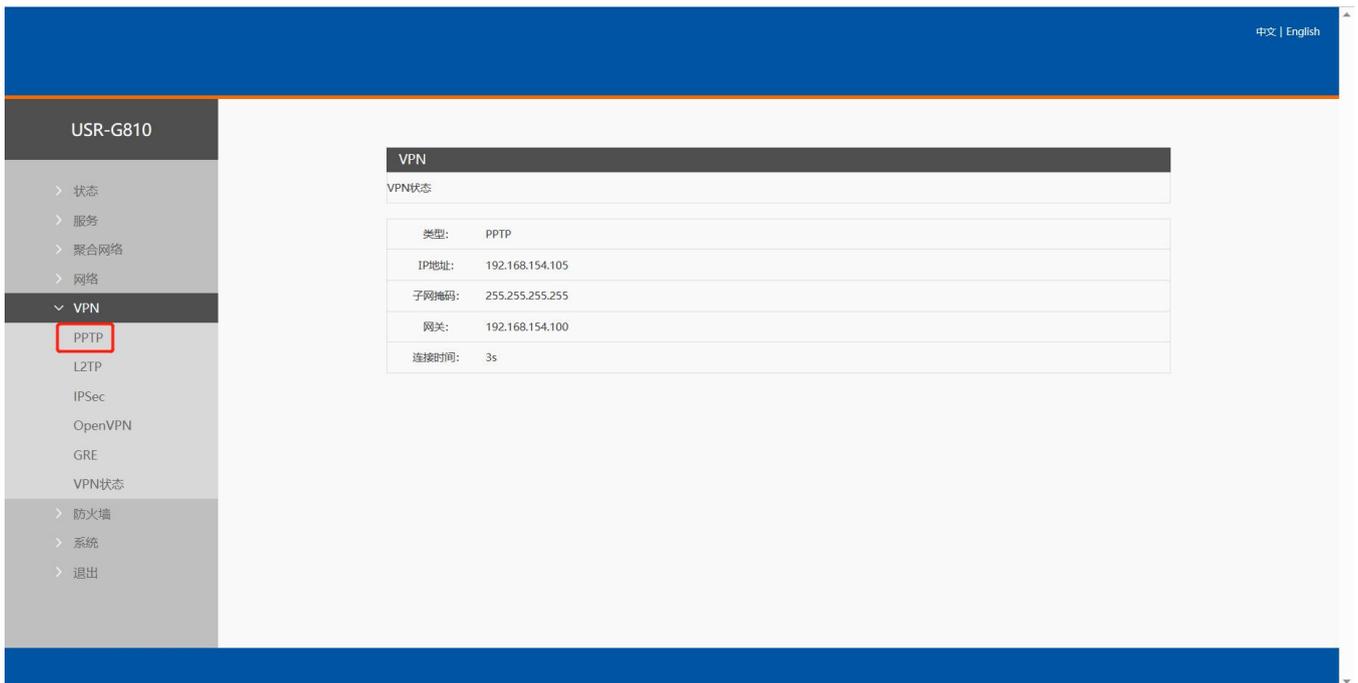


图 50 路由器 VPN 连接状态

5.2. L2TP Client

L2TP 是第二层隧道协议，与 PPTP 类似。目前 G810-33 支持隧道密码认证，支持 L2TP OVER IPsec 的预共享密钥加密方式。进入 VPN--L2TP 界面中，选择启用 L2TP 客户端，依次填入参数。

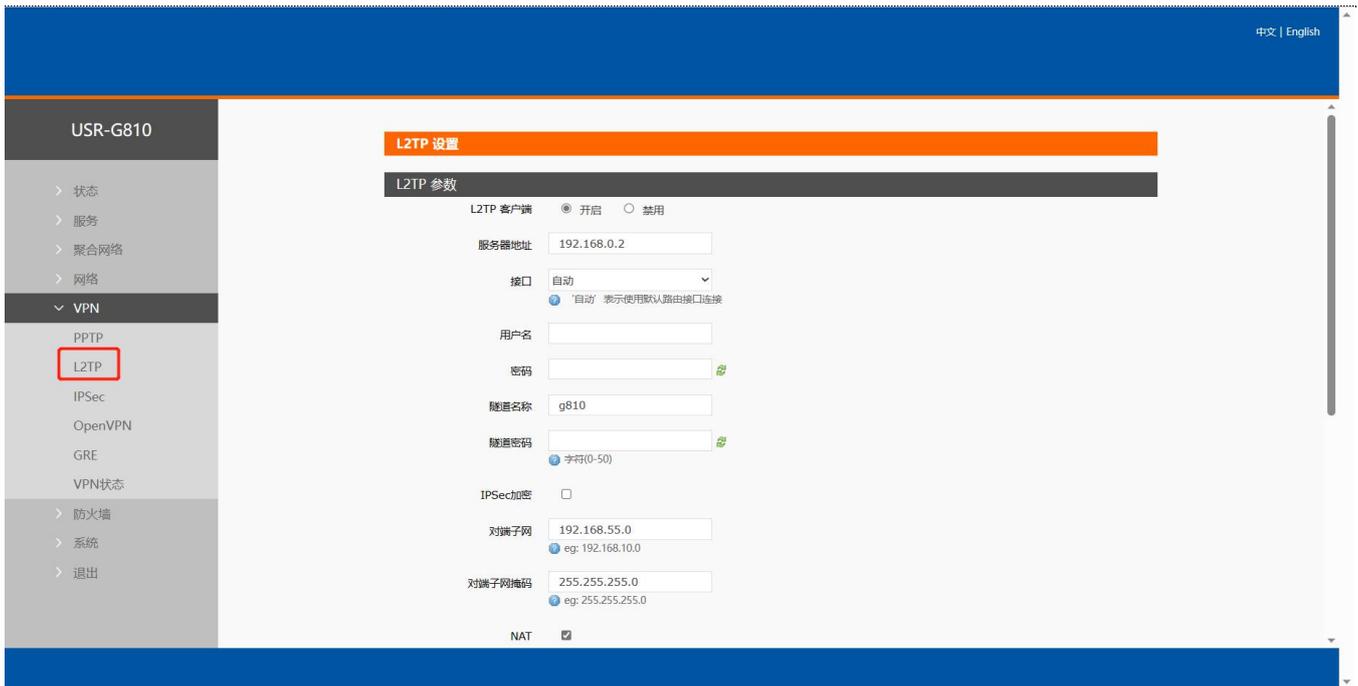


图 51 L2TP 客户端启用设置界面

<说明>

- L2TP 支持隧道密码认证、L2TP OVER IPSec 加密；
- 服务器地址：填写要连接的 VPN 服务器 IP 或者域名；
- 接口：根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动；
- 用户名/密码：从 VPN 服务器处获取；
- 加密/认证：隧道密码认证、IPSec 加密，从 VPN 服务器端获取后正确填入；
- 使能静态隧道 IP 地址：默认未使能，服务器端自动分配 IP。可于此处填写静态隧道 IP；
- 额外配置：追加 PPPD 参数、魔术字等，默认不需要进行任何操作；
- NAT 设置：该功能默认开启。当内容需要和外部通讯时，将内部地址替换成公用地址。关闭该项，则无法实现网络地址转换功能；
- 对端子网、掩码：填写正确后，在 NAT 功能开启下，可直接实现 VPN 下的子网互通功能；
- 使能 ping:实时 VPN 在线检测及重连机制。默认未启用。打勾代表 ping 失败将重连 VPN；
- L2TP 连接成功：完成相关参数的填入后，保存&应用，进入到 VPN--VPN 状态处查看连接状态。

5.3. IPSec

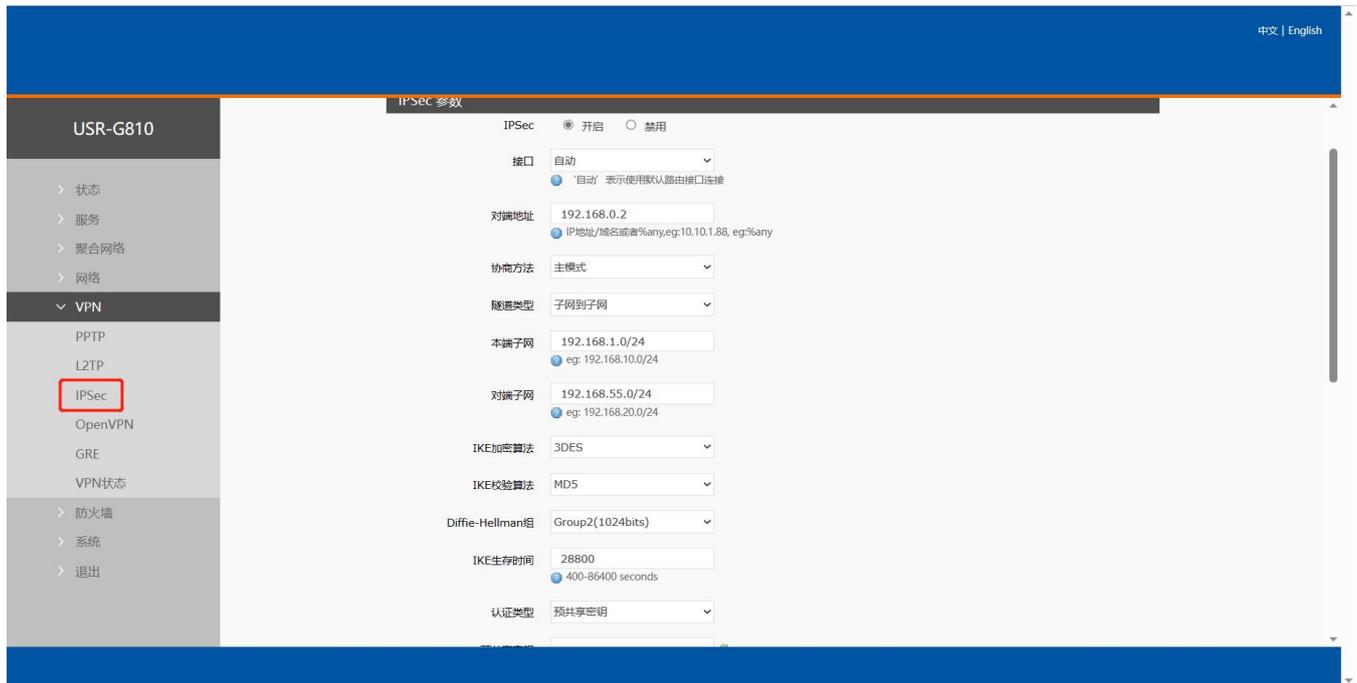


图 52 IPSec 启用后基本设置

<说明>

- 接口：根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动；
- 对端地址：可以分为 VPN 客户端和 VPN 服务器。填入对端的 IP/域名；
- 协商方式：主模式、积极模式（野蛮模式），默认主模式；
- 隧道类型：子网到子网、子网到主机、主机到子网、主机到主机。根据实际应用方式选择；
- 本端子网：IPSec 本端子网及子网掩码；
- 对端子网：IPSec 对端子网及子网掩码；
- 本端标识符：通道本端标识，可以为 IP 或 FQDN，注意在域名自定义名时加@；
- 对端标识符：通道对端标识，可以为 IP 或 FQDN，注意在域名自定义名时加@；
- IKE 的加密：第一阶段包括 IKE 阶段的加密方式、完整性方案、DH 交换算法；
- IKE 生命周期：设置 IKE 的生命周期，单位为秒，默认：28800；
- IKE 加密算法：3DES/AES-128/AES-192/AES-256；
- IKE 校验算法：SHA-1/SHA2-256/SHA2-512/MD5；
- Diffie-Hellman 组：Group1/2/5/14；
- 认证方式：目前支持预共享密钥的认证方式；
- ESP 加密：第二阶段包括 ESP 对应的加密方式、完整性方案；
- ESP 生命周期：设置 ESP 生命周期，单位为秒，默认：3600；
- ESP 加密算法：3DES/AES-128/AES-192/AES-256；
- ESP 校验算法：SHA-1/SH2-256/MD5；
- 会话密钥向前加密(PFS)：None/DH1/DH2/DH5；
- 启动 DPD 检测：当 DPD 声明对等点为死时,应该采取什么行动；
- DPD 检测周期：设置连接检测（DPD）的时间间隔；
- DPD 超时时间：设置连接检测（DPD）超时时间；

- DPD 操作：设置连接检测的操作。包括重启、拆除、保持、无，默认重启；
- IPsec 连接成功：和对端通过 IPsec 连接成功后，进入到 VPN--VPN 状态处查看连接状态。

5.4. OpenVPN

启用 OpenVPN 搭建 VPN，内部可选 TUN(路由模式)或 TAP(网桥模式)：

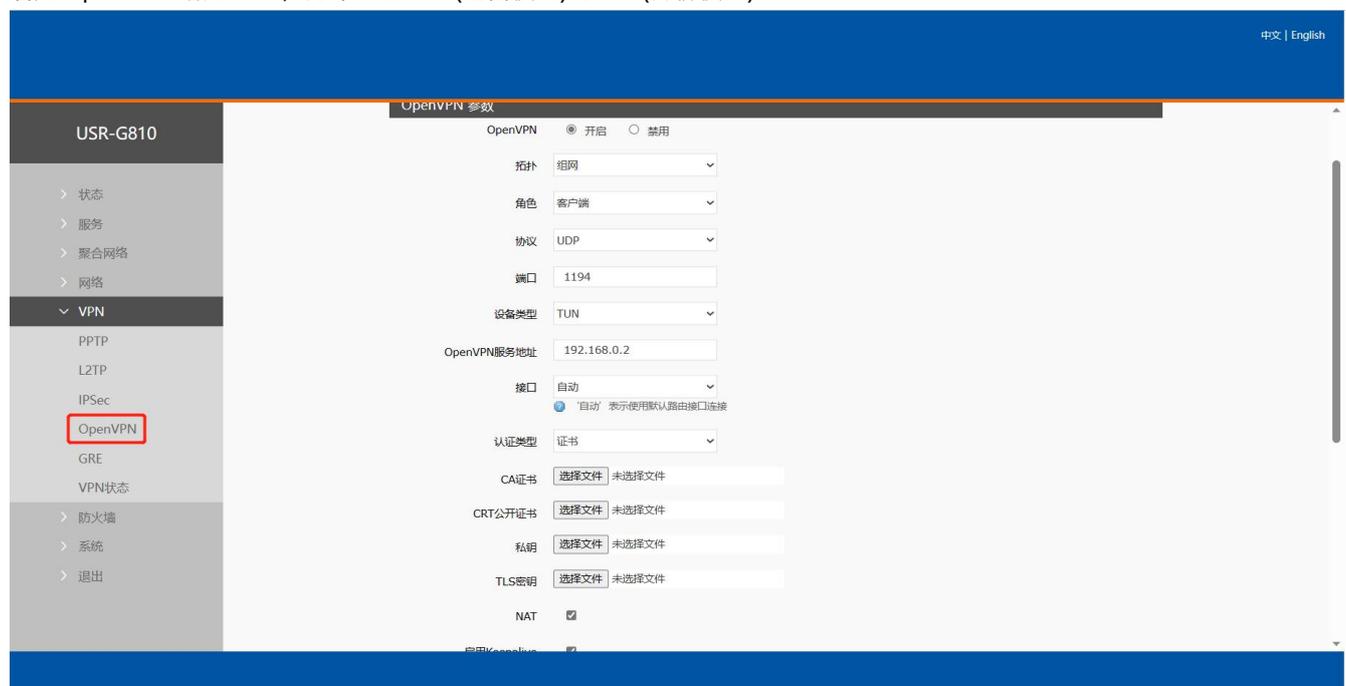


图 53 OpenVPN 启用设置界面

<说明>

- 设备类型：可选择 TUN(路由模式)或 TAP(网桥模式)；
- 通道协议：UDP 或 TCP；
- 端口：OpenVPN 客户端的监听端口；
- VPN 服务器地址：OpenVPN 服务器的 IP/域名；
- 接口：根据联网方式的不同可选择 wan_4g1、wan_4g2、wan_wired、自动；
- CA 证书：服务器和客户端公共的 CA 证书；
- CRT 公开证书：客户端证书；
- 客户端私钥：客户端的密钥；
- TLS 认证密钥：安全传输层的认证密钥；
- 加密算法：无/Blowfish-128/DES-128/3DES-192/AES-128/AES-192/AES-256；
- 哈希算法：无/SHA1/SHA256/SHA512/MD5；
- 加密和哈希算法均需和 VPN 服务器保持一致；
- 使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩；
- NAT 设置：该功能默认开启。当内容需要和外部通讯时，将内部地址替换成公用地址。关闭该项，则无法实现网络地址转换功能；
- 启用 Keepalive：默认启用，默认配置为 keepalive 10 120。本项设置需和 VPN 服务器对应；
- MTU 设置：设置通道的 MTU 值，默认 1500，本项设置需和 VPN 服务器对应；
- TLS 方式：tls-auth/tls-crypt；
- 使能 ping 功能：设定 Ping 检测的地址后，可以保证 vpn 在异常断开下进行重连；

- OpenVPN 连接成功：和 VPN 服务器连接成功后，进入到 VPN--VPN 状态处查看连接状态。
- 注意：
- 客户端与服务器连接前，CA 证书、客户端证书、客户端密钥、TLS 认证密钥，这几个需要服务器提供；
- 得到的证书文件后，将不同的证书内容分别添加到配置界面接口。

附：linux 下 OpenVPN 服务端配置

```
port 1194
proto udp
dev tun
user nobody
group nogroup
persist-key
persist-tun
keepalive 10 120
topology subnet
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
push "redirect-gateway def1 bypass-dhcp"
crl-verify crl.pem
ca ca.crt
cert server_Jz40qi4AWJnZuN8X.crt
key server_Jz40qi4AWJnZuN8X.key
tls-auth tls-auth.key 0
dh dh.pem
auth SHA256
cipher AES-256-CBC
#tls-server
#tls-version-min 1.2
#tls-cipher TLS-DHE-RSA-WITH-AES-128-GCM-SHA256
status openvpn.log
verb 3
```

图 54 Linux 下 OpenVPN 服务端配置

5.5. GRE

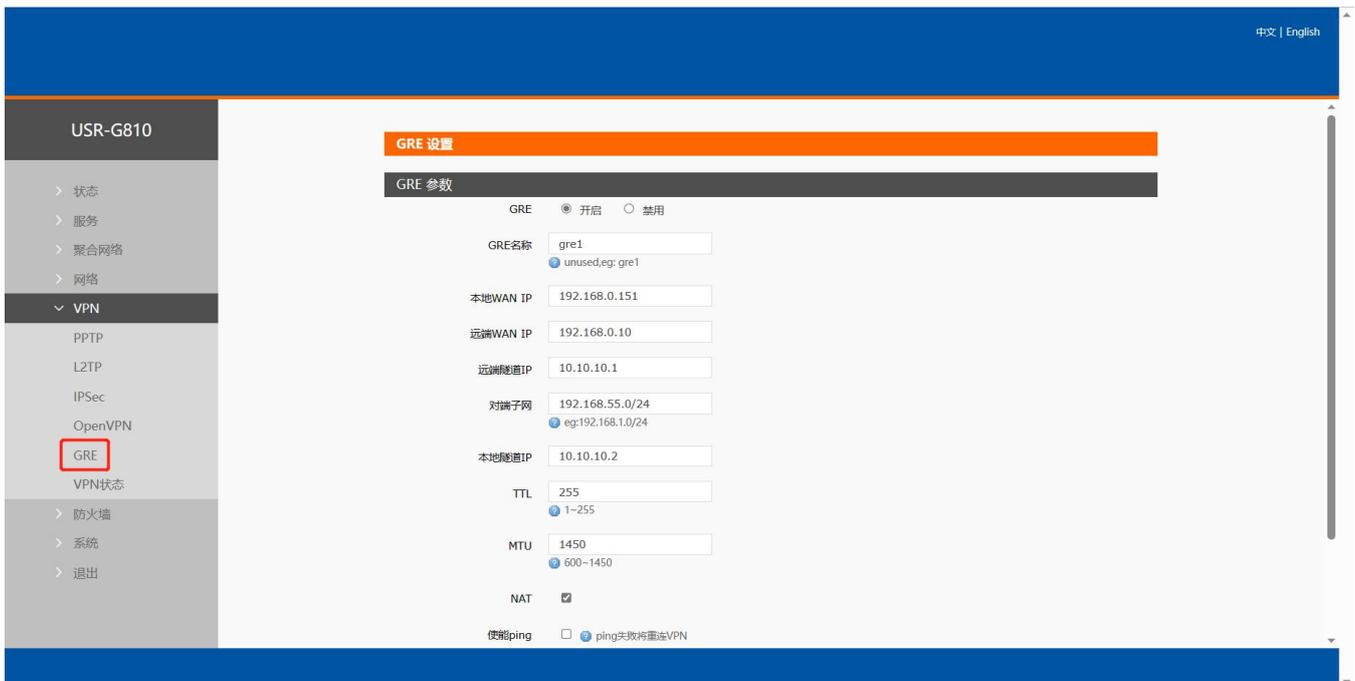


图 55 GRE 基本配置

<说明>

- 远程地址：对端 GRE 的 WAN 口 IP 地址；
- 本端地址：本端的 wan_wired、5G 或者 STA 的地址，根据联网方式不同输入相应本段地址；
- 远端隧道地址：对端的 GRE 隧道 IP；
- 对端子网：对于设置子网掩码可以按照如下规定表示：255.255.255.0 可以写成 IP/24、255.255.255.255 可以写成 IP/32。例如：172.16.10.1/24，对应着 IP 为 172.16.10.1，子网掩码为 255.255.255.0；
- 本端隧道 IP：本地 GRE 隧道 IP 地址；
- NAT：该功能默认开启。当内容需要和外部通讯时，将内部地址替换成公用地址。关闭该项，则无法实现网络地址转换功能；
- TTL 设置：设置 GRE 通道的 TTL，默认 255；
- 设置 MTU：设置 GRE 通道的 MTU，默认 1450。

6. 防火墙功能

6.1. 基本设置

默认两条防火墙规则。

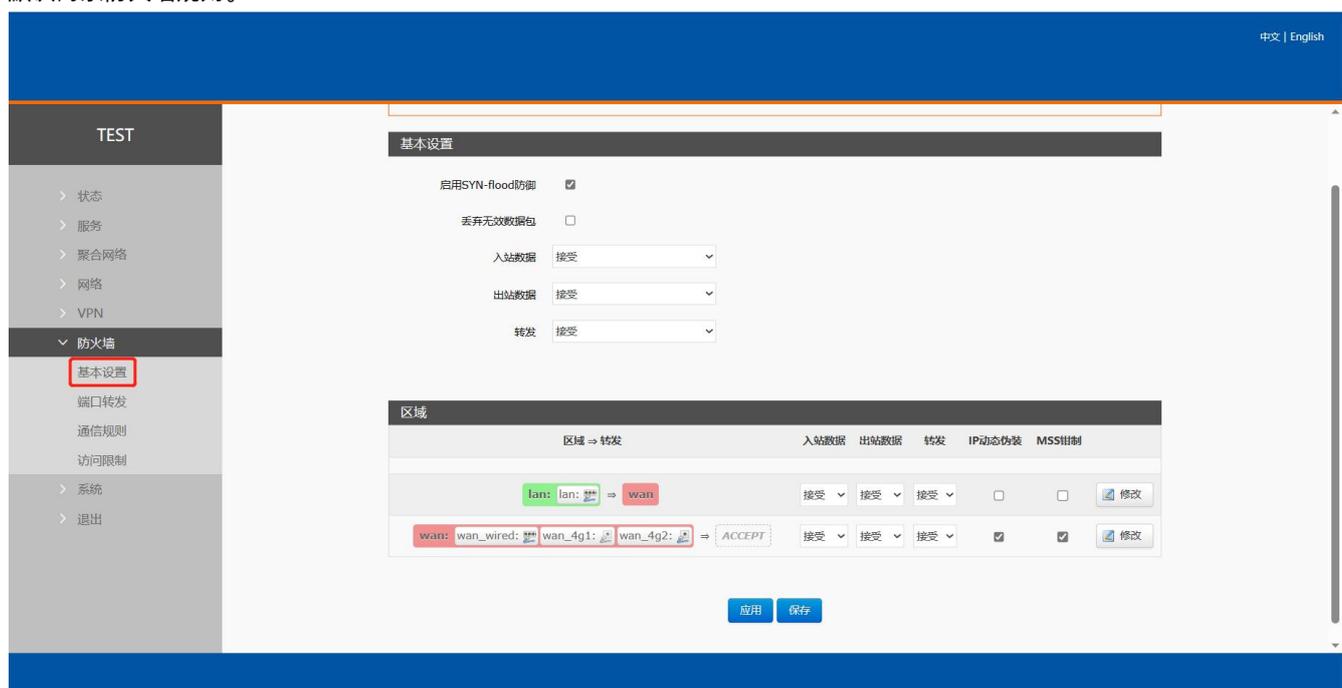


图 56 防火墙设置页面

<名词介绍>

- 入站：访问路由器 IP 的数据包；
- 出站：路由器 IP 要发出的包；
- 转发：接口之间的数据转发，不经过路由自身；
- IP 动态伪装：仅对 WAN 口与 5G 口有意义，访问外网时 IP 地址的伪装；
- MSS 钳制：限制报文 MSS 大小，一般是 1460。

<规则 1>

- LAN 口到有线 WAN 口的入站，以及转发，均为接受；
- 如果有数据包来自于 LAN 口，要去访问 WAN 口，那么本条规则允许数据包从 LAN 口转发到 WAN 口，这属于转发；
- 您也可以在 LAN 口下，打开路由器的网页，这属于“入站”；
- 路由器自身去连接外网，比如同步时间，这属于“出站”。

<规则 2>

- 有线 WAN 口与 5G 口，接受“入站”，接受“出站”，允许“转发”；
- 如果有“入站”数据包，比如有人打算从 WAN 口登录路由器网页，那么将会被允许；
- 如果有“出站”数据包，比如路由器通过 WAN 口或者 5G 口访问外网，此动作被允许；
- 如果有“转发”数据包，比如从 WAN 口来的数据包想转发到 LAN 口，此动作被允许。

6.2. 通信规则

通信规则可以选择性的过滤特定的 Internet 数据类型，以及阻止 Internet 访问请求，通过这些通信规则增强网络的安全性。防火墙的应用范围很广，下面简单介绍下常见的几种应用。

表 17 通信规则参数表

名称	描述	默认参数
启用	显示  表示启用状态 显示  表示禁用状态	启用
名字	此条规则名字，字符类型	-
限制地址	限制 IPv4 地址	仅 IPv4 地址
协议	限制规则的协议类型，可选择： TCP+UDP/TCP/UDP/ICMP	TCP+UDP
匹配 ICMP 类型	匹配的 ICMP 规则，选择 any 即可	Any
源区域	数据流源区域，可选择：任意区域，WAN，LAN LAN：表示子网访问外网规则 WAN：表示外网访问内网规则	LAN
源 MAC 地址	需要匹配规则的源 MAC 空：代表匹配所有 MAC 说明：匹配源 MAC 地址时需将源 IP 地址设置为空	空
源 IP 地址	需要匹配规则的源 IP 空：代表匹配所有 IP 说明：匹配源 IP 地址时需将源 MAC 地址设置为空	空
源端口	需要匹配规则的源端口 空：代表匹配所有端口	空
目标区域	数据流目标区域，可选择：任意区域，WAN，LAN LAN：表示子网访问外网规则 WAN：表示外网访问内网规则	WAN
目标地址	访问的目标 IP 地址 空：代表所有地址	空

目标端口	访问的目标端口号 空：代表所有	空
动作	接受到此类数据包可选择：丢弃，接受，拒绝，无动作 丢弃：收到此规则数据包将丢弃 接受：收到此规则数据包将接受 拒绝：收到此规则数据包将拒绝 无动作：收到此规则数据包将无动作	接受

6.2.1. IP 地址黑名单

首先在新建转发规则中输入规则的名字，然后点击“添加并编辑按钮”

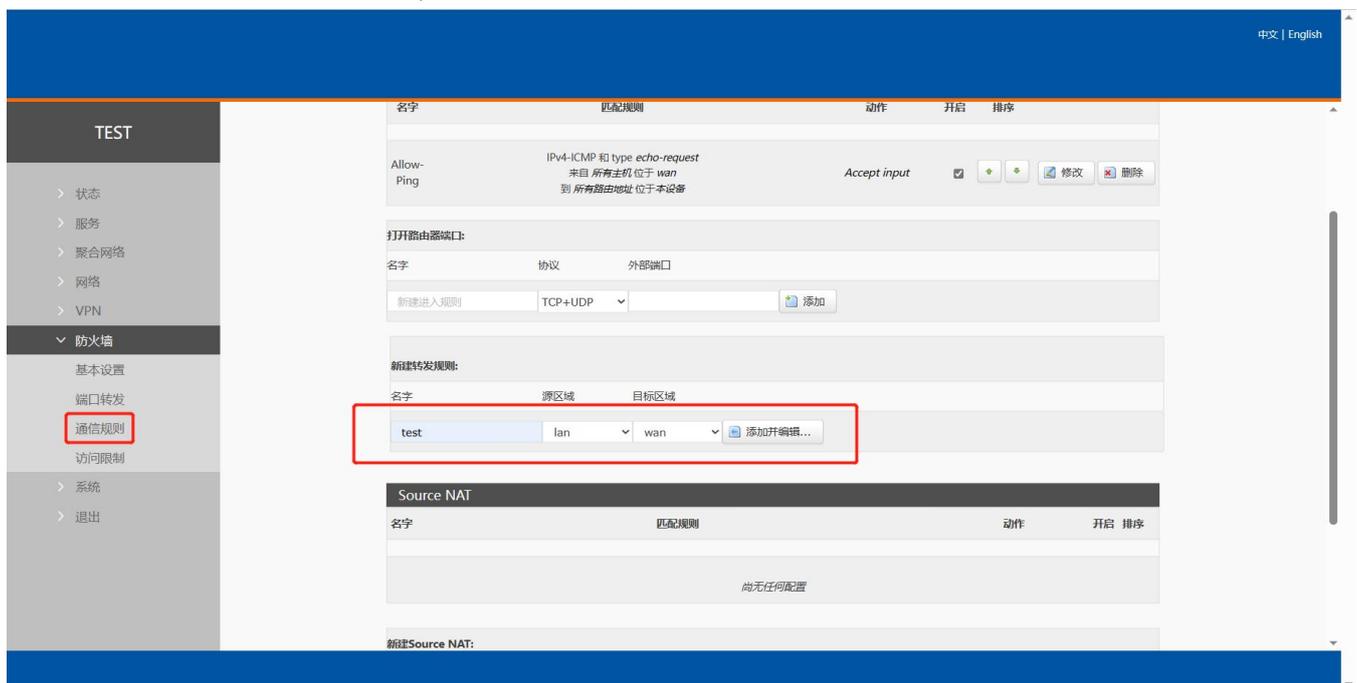


图 57 防火墙黑名单图一

在跳转的页面中，源区域选择 lan，源 MAC 地址和源地址都选择所有（如果是只限制局域网内的特定 IP 访问外网的特定 IP，则此处需填写 IP 地址或是 MAC 地址），如下图：

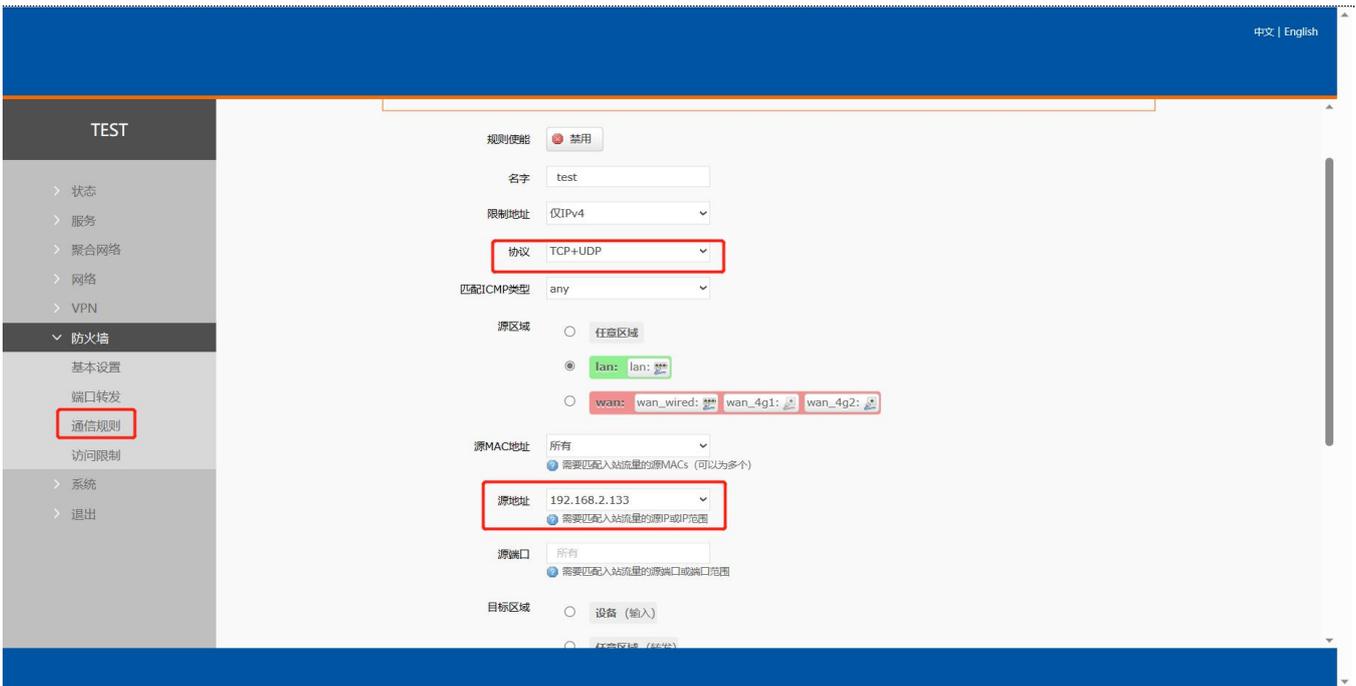


图 58 防火墙黑名单图二

在目标区域选择 WAN，目标地址填写禁止访问的 IP，动作选择“拒绝”设置完成后，点击“应用”。如下图。

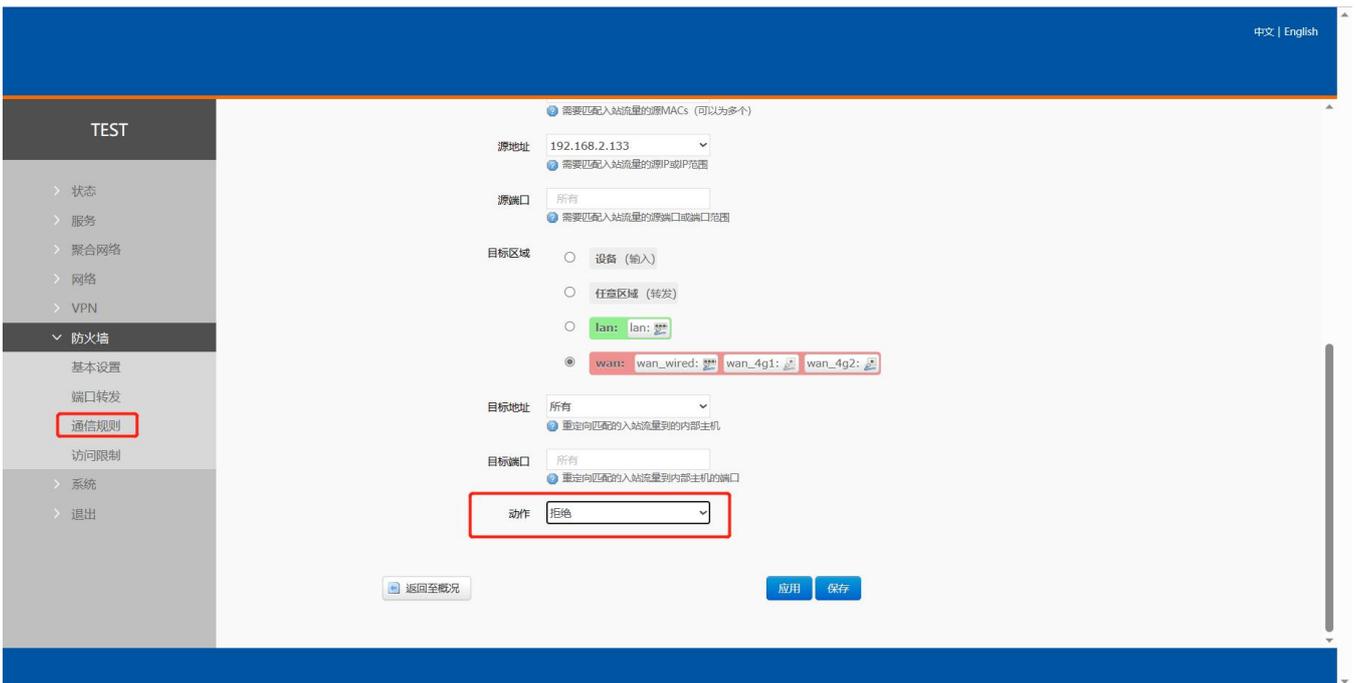


图 59 防火墙黑名单图三

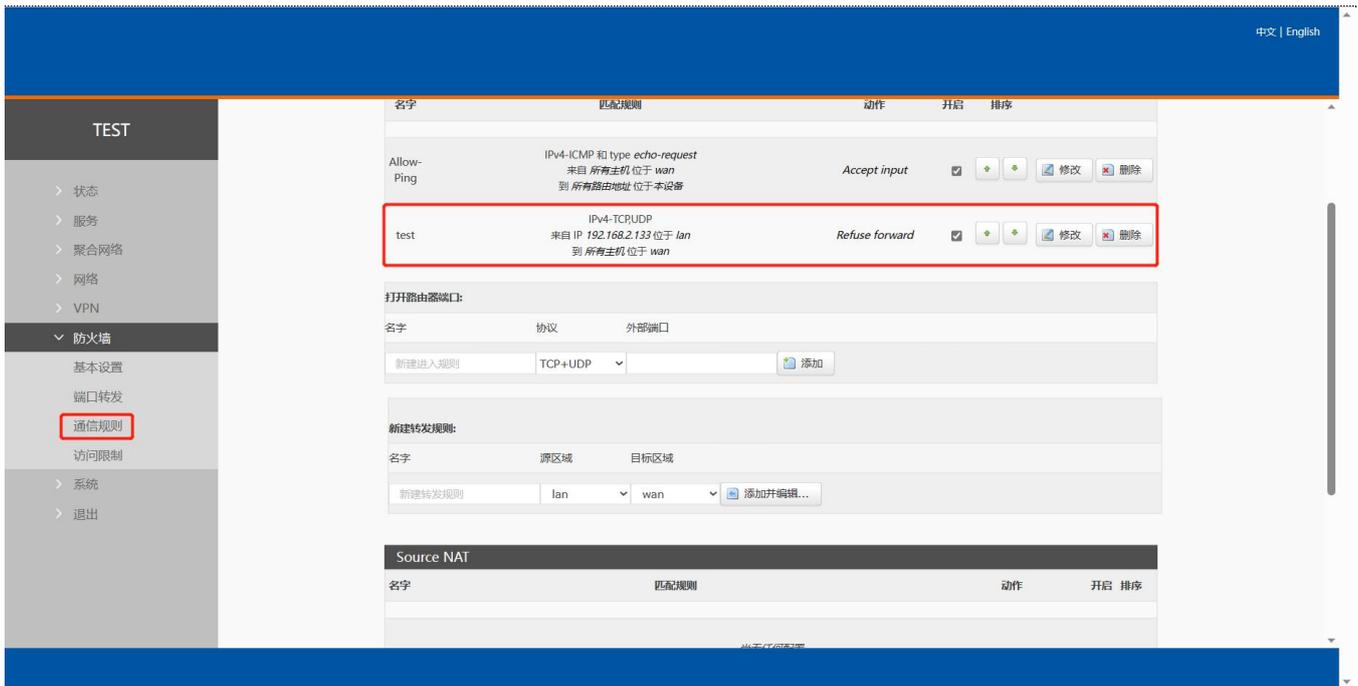


图 60 防火墙黑名单图四

这样设置完成后，就实现了黑名单的功能。即实现子网设备 IP 为 192.168.2.133 的 IP 禁止访问所有外网。

6.2.2. IP 地址白名单

首先添加要加入白名单的 IP 或 MAC 地址的通信规则，在新建转发规则中输入规则的名字，然后点击“添加并编辑按钮”。

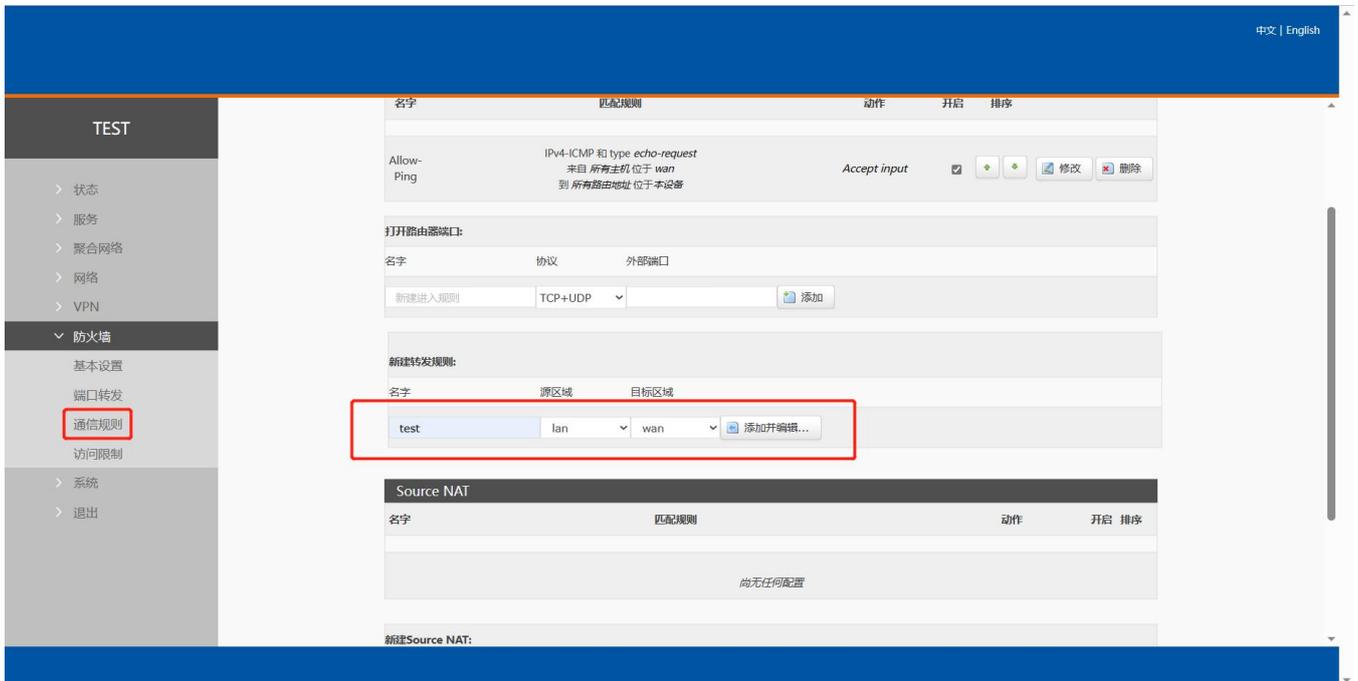


图 61 防火墙白名单图一

在跳转的页面中，源区域选择 lan，源 MAC 地址和源地址都选择所有（如果是允许局域网内的特定 IP 访问外网的特定 IP，则此处需填写 IP 地址或是 MAC 地址），如下图

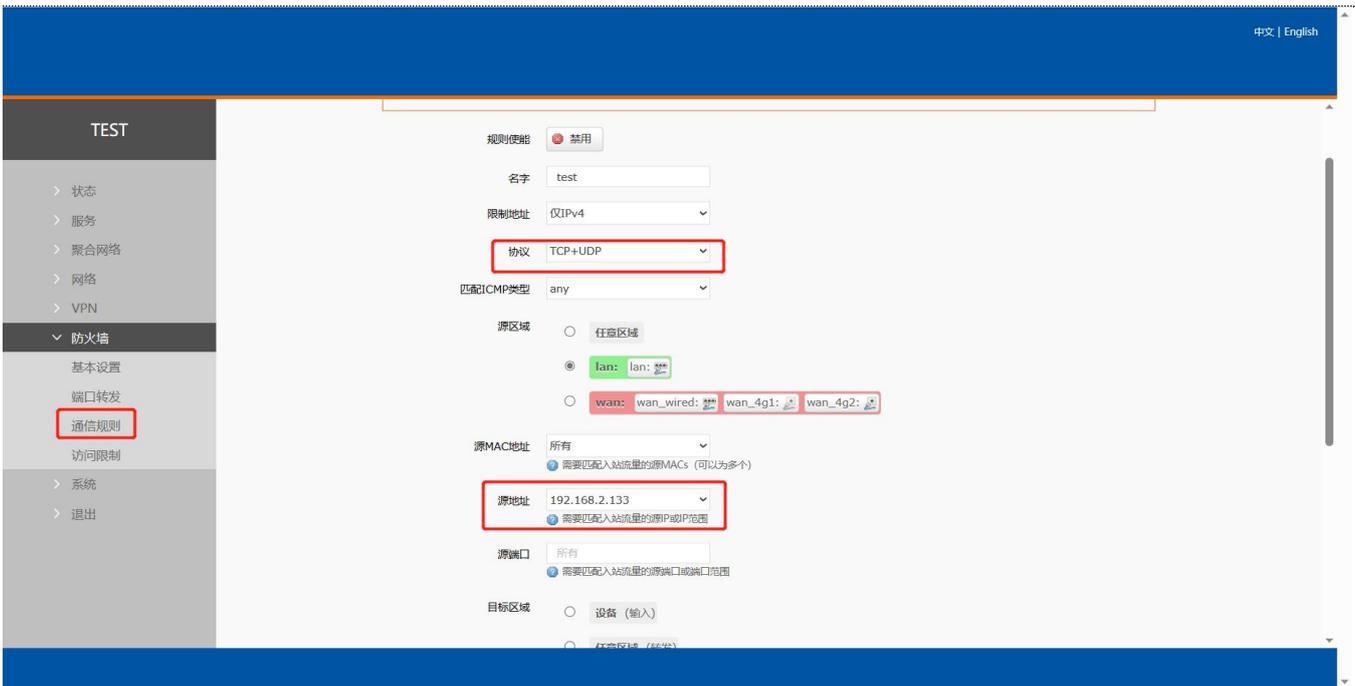


图 62 防火墙白名单图二

在目标区域选择 WAN，目标地址填写允许访问的 IP，动作选择“接受”设置完成后，点击“保存并应用”。如下图。

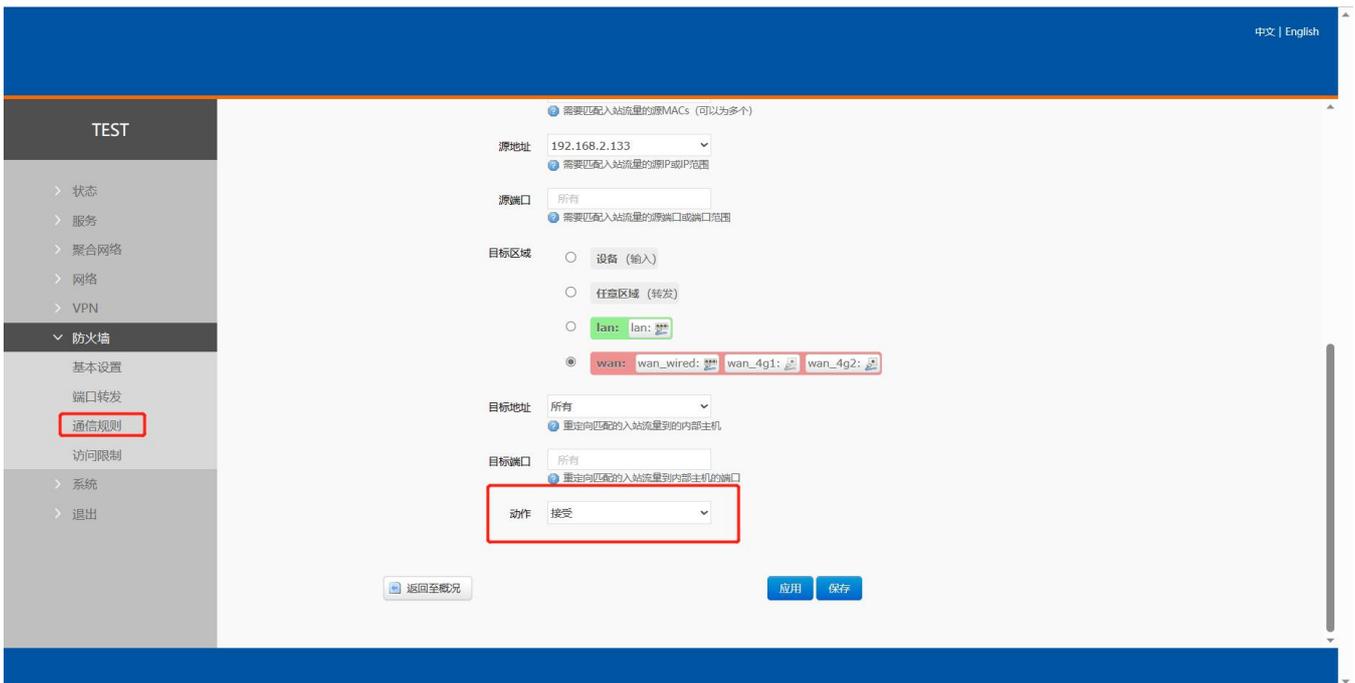


图 63 防火墙白名单图三

接下来再设置一条所有的通信都拒绝的规则，源地址设置为“所有”，目标地址设置为“所有”，动作选择“拒绝”。注意两条规则的先后顺序，一定是允许的规则在前，拒绝的规则在后。总体设置完成后如下图

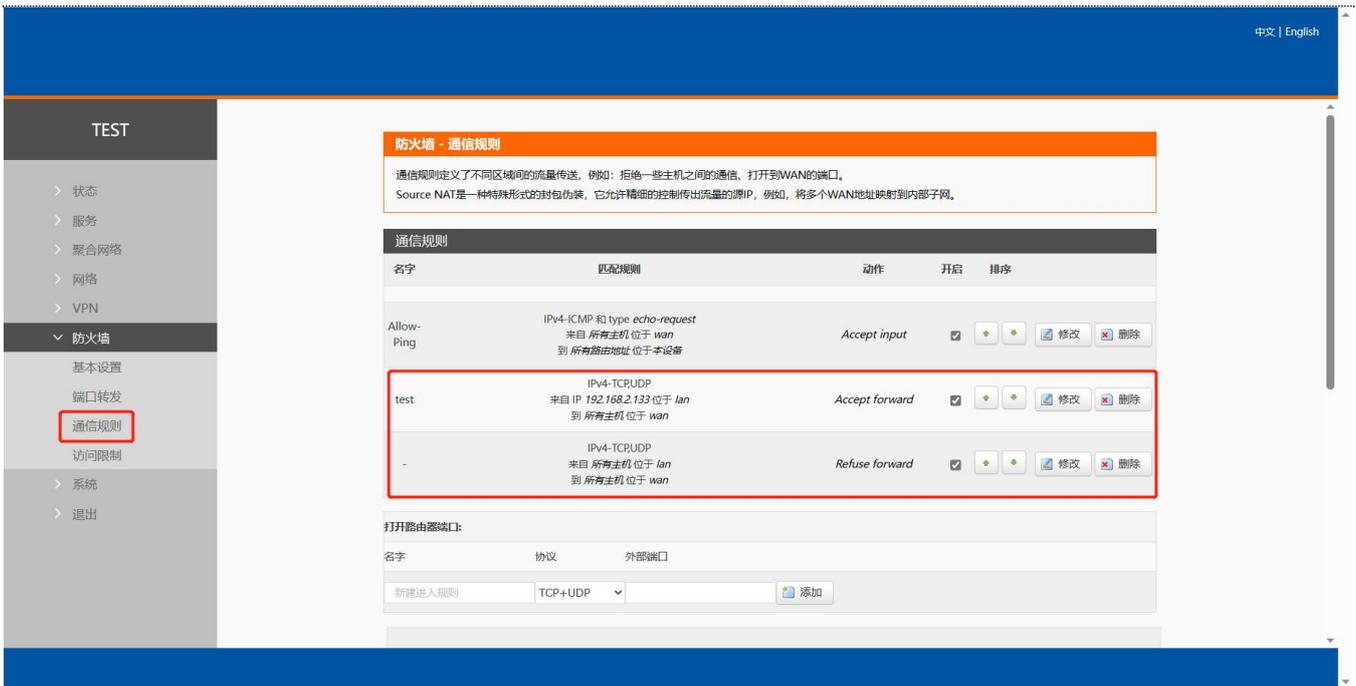


图 64 防火墙白名单图三

<说明>

- 最多可添加 20 条通信规则。

6.3. NAT 功能

6.3.1. IP 地址伪装

IP 地址伪装，将离开数据包的源 IP 转换成路由器某个接口的 IP 地址，如图勾选 IP 动态伪装，系统会将流出路由器的数据包的源 IP 地址修改为 WAN 口的 IP 地址。

注意：WAN 接口必须开启 IP 动态伪装和 MSS 钳制，lan 接口禁止开启 IP 动态伪装和 MSS 钳制。

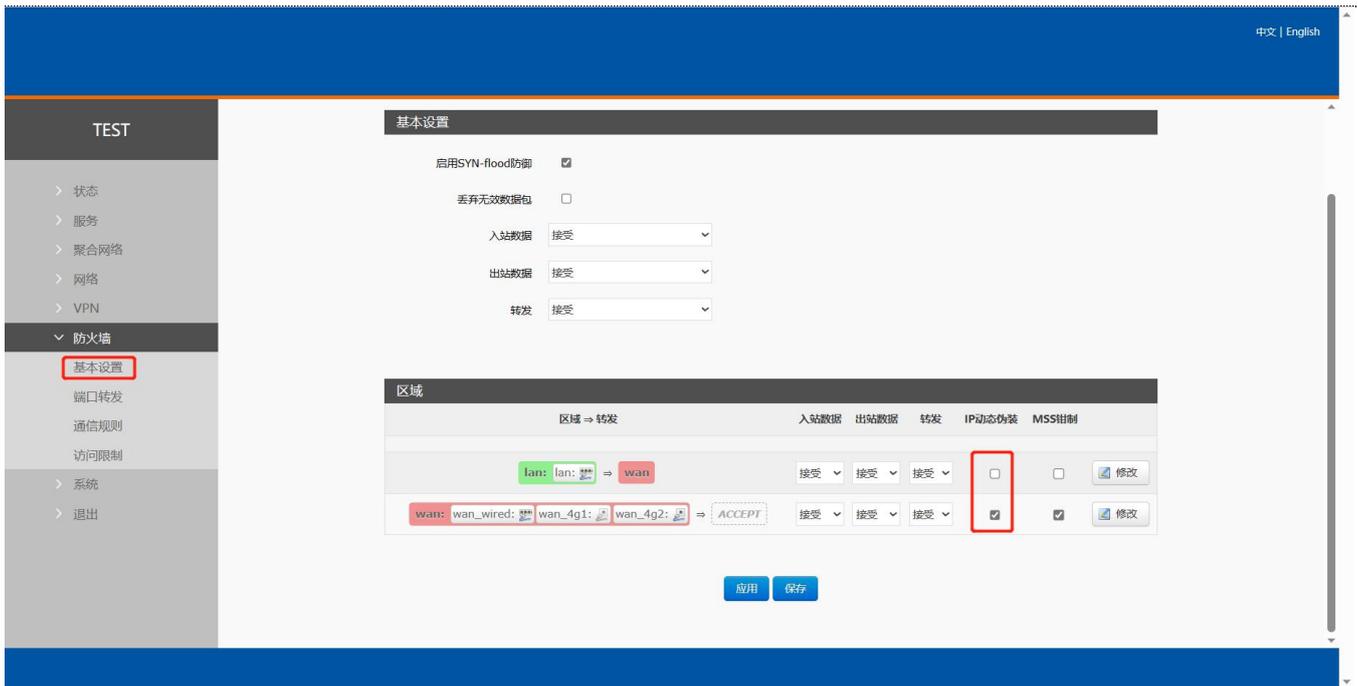


图 65 IP 地址伪装设置

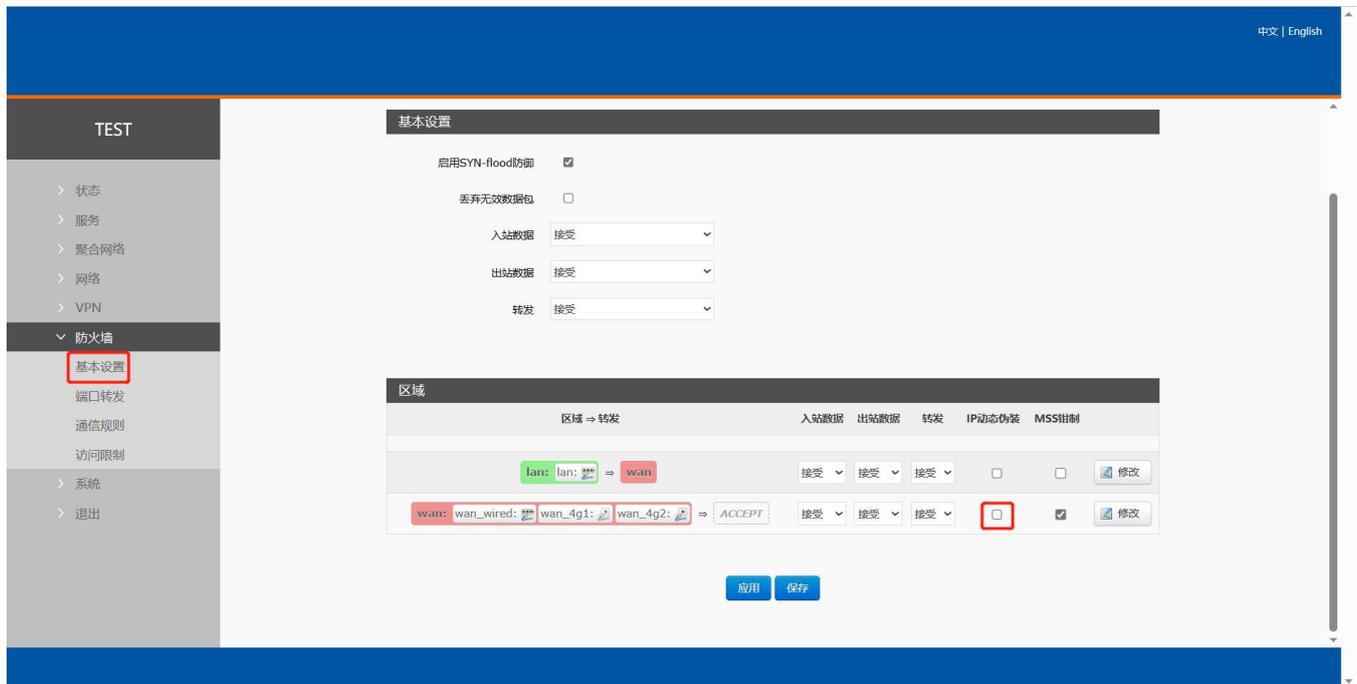
6.3.2. SNAT

表 18 SNAT 参数表

名称	描述	默认参数
启用按钮	显示  表示启用状态 显示  表示禁用状态	启用
名字	此条防火墙规则的名称	-
协议	可设置： TCP+UDP/TCP/UDP/ICMP	TCP+UDP
源 IP 地址	需要匹配入站流量的源 IP 例如一个 IP:192.168.1.100 为空表示匹配所有源 IP	空
源端口	需要匹配入站流量的源端口 例如一个端口:9999 为空表示匹配所有源端口	空
目标 IP	需要匹配入站流量的目标 IP 例如一个 IP:192.168.2.100 为空表示匹配所有目标 IP	空
目标端口	需要匹配入站流量的目标端口 例如一个端口:9999 为空表示匹配所目标端口	空
SNAT IP 地址	将匹配流量的源地址改成此地址	添加时自定义的 IP

SNAT 端口	将匹配流量的源端口改为此端口 为空表示使用源端口	空
---------	-----------------------------	---

Source NAT 是一种特殊形式的封包伪装，改变离开路由器数据包的源地址，使用时首先将 wan 口的 IP 动态伪装关闭



然后设置 Source NAT

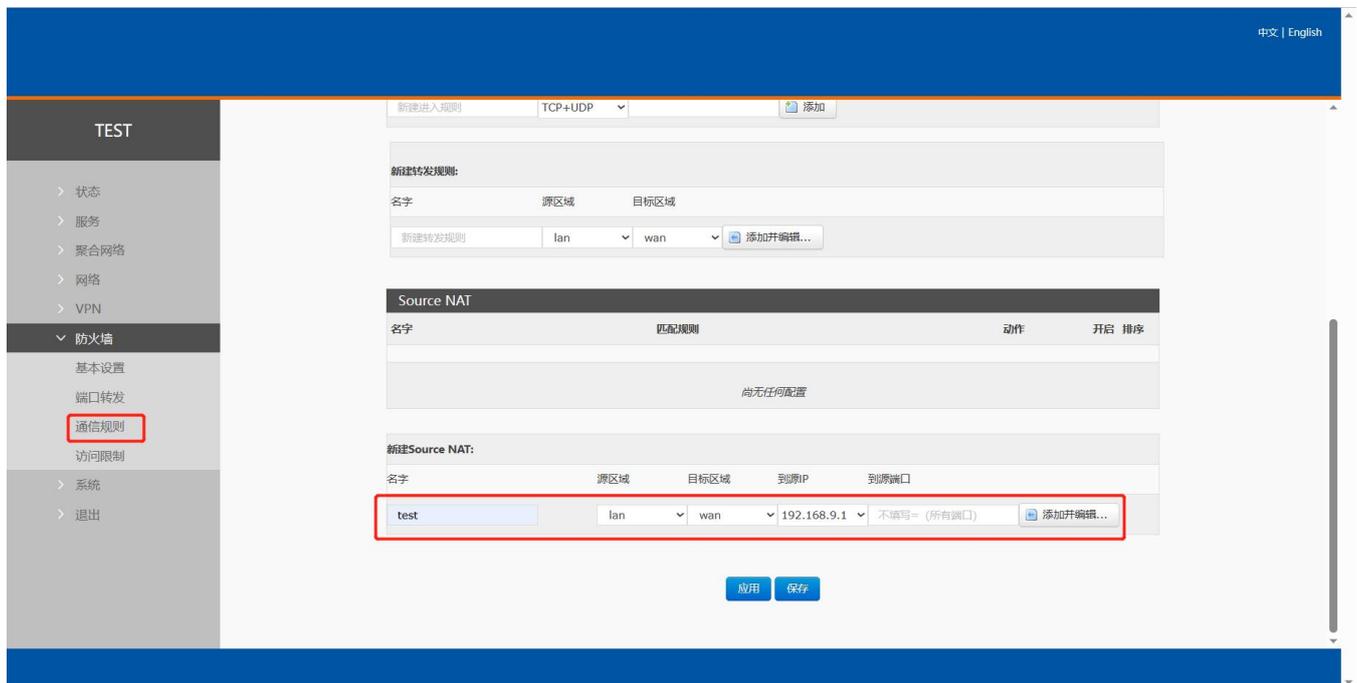


图 66 NAT 设置一

点击添加并编辑

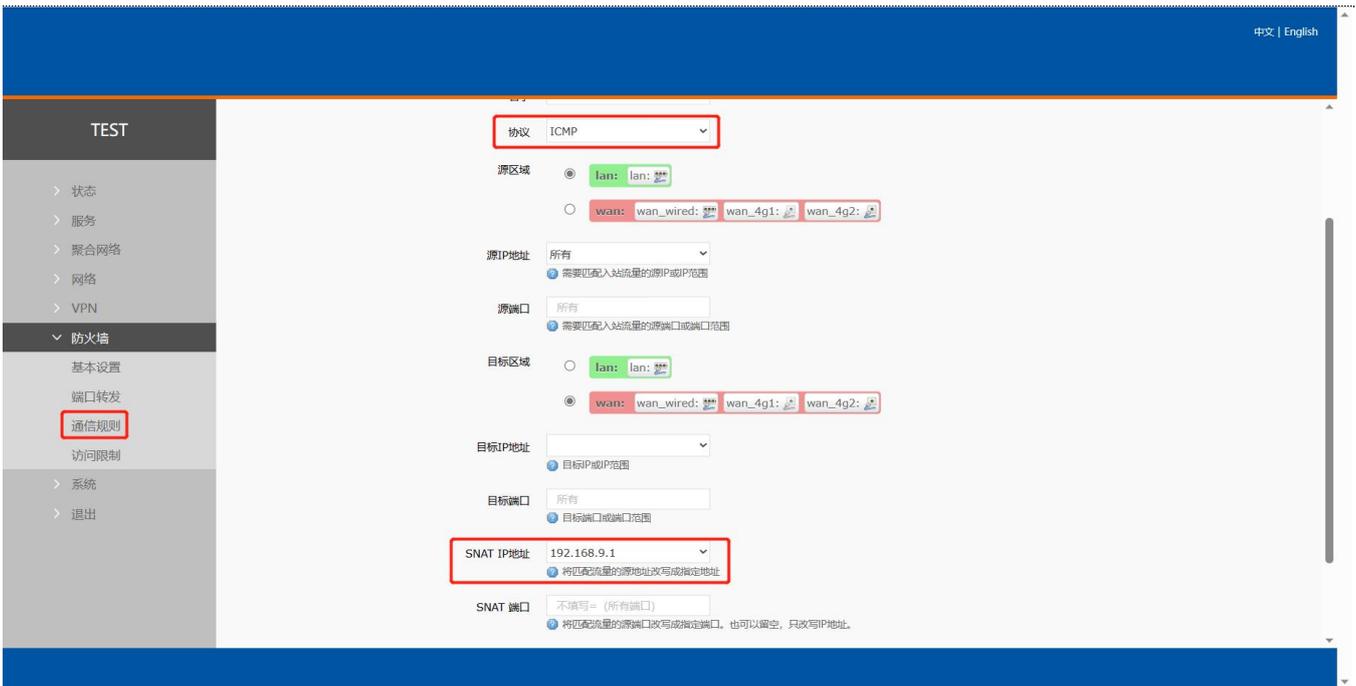


图 67 NAT 设置二

若源 IP、源端口和目的 IP、目的端口不填，默认所有 ip 与端口。设置完之后保存。

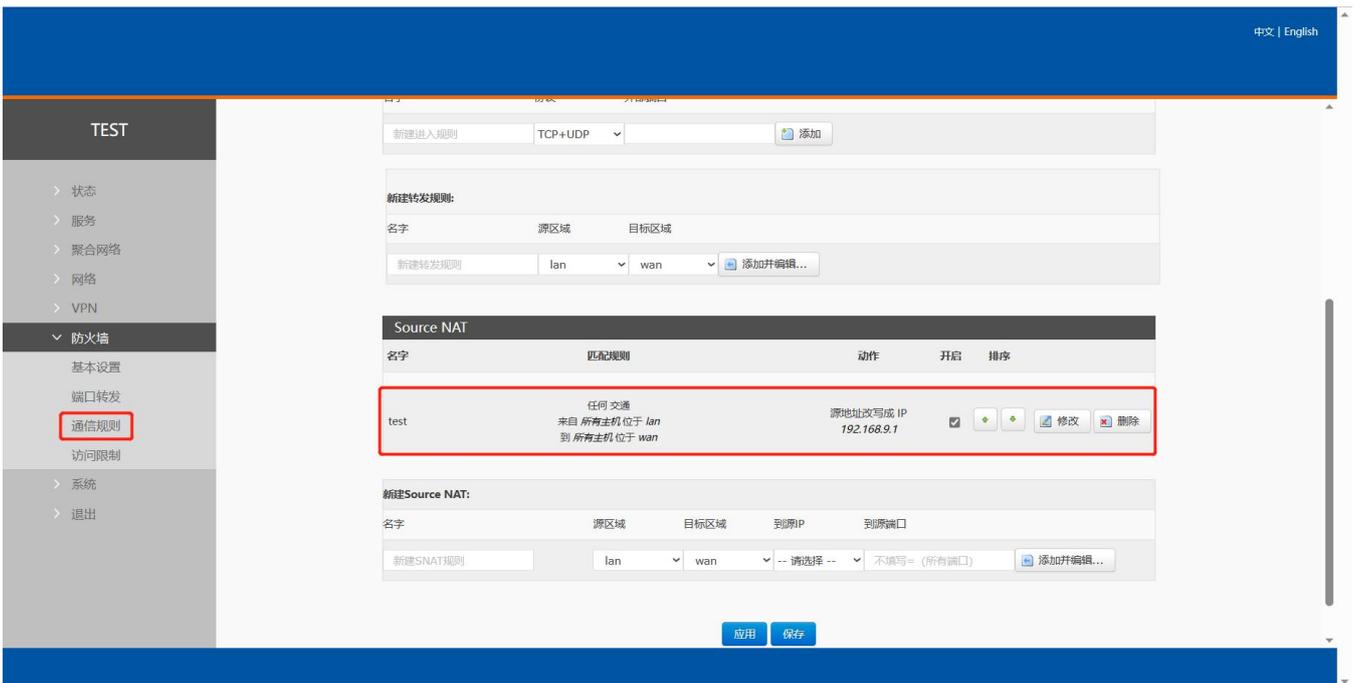


图 68 NAT 设置三

如图将离开路由器的数据包源 IP 地址改变为 192.168.9.1，如图可以看到，到 192.168.13.4 的 ICMP 包的源地址是 192.168.9.1，而不是 192.168.1.114。

验证用路由器下的设备(IP:192.168.1.114)ping 与路由器在同一个交换机下的 PC(IP:192.168.13.4)，在 PC 上抓包的数据如下：

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.13.4	220.195.22.209	TCP	50379 > http [FIN, ACK] Seq=1 Ack=1 Win=64708 Len=0
2	0.689352	192.168.9.1	192.168.13.4	ICMP	Echo (ping) request (id=0x1d3c, seq(be/le)=57/14592, ttl=64)
3	0.689426	192.168.13.4	192.168.9.1	ICMP	Echo (ping) reply (id=0x1d3c, seq(be/le)=57/14592, ttl=128)
6	1.689615	192.168.9.1	192.168.13.4	ICMP	Echo (ping) request (id=0x1d3c, seq(be/le)=58/14848, ttl=64)
7	1.689687	192.168.13.4	192.168.9.1	ICMP	Echo (ping) reply (id=0x1d3c, seq(be/le)=58/14848, ttl=128)
8	1.823459	192.168.13.4	192.168.4.63	SMB2	Create Request File:
9	1.825746	192.168.4.63	192.168.13.4	SMB2	Create Response File:
10	1.826091	192.168.13.4	192.168.4.63	SMB2	Create Request File:

图 69 NAT 验证

<说明>

- 最多可添加 20 条 SNAT 规则。

6.3.3. 端口转发

端口转发允许来自 Internet 的计算机访问私有局域网内的计算机或服务，即将 WAN 口地址的一个指定端口映射到内网的一台主机。

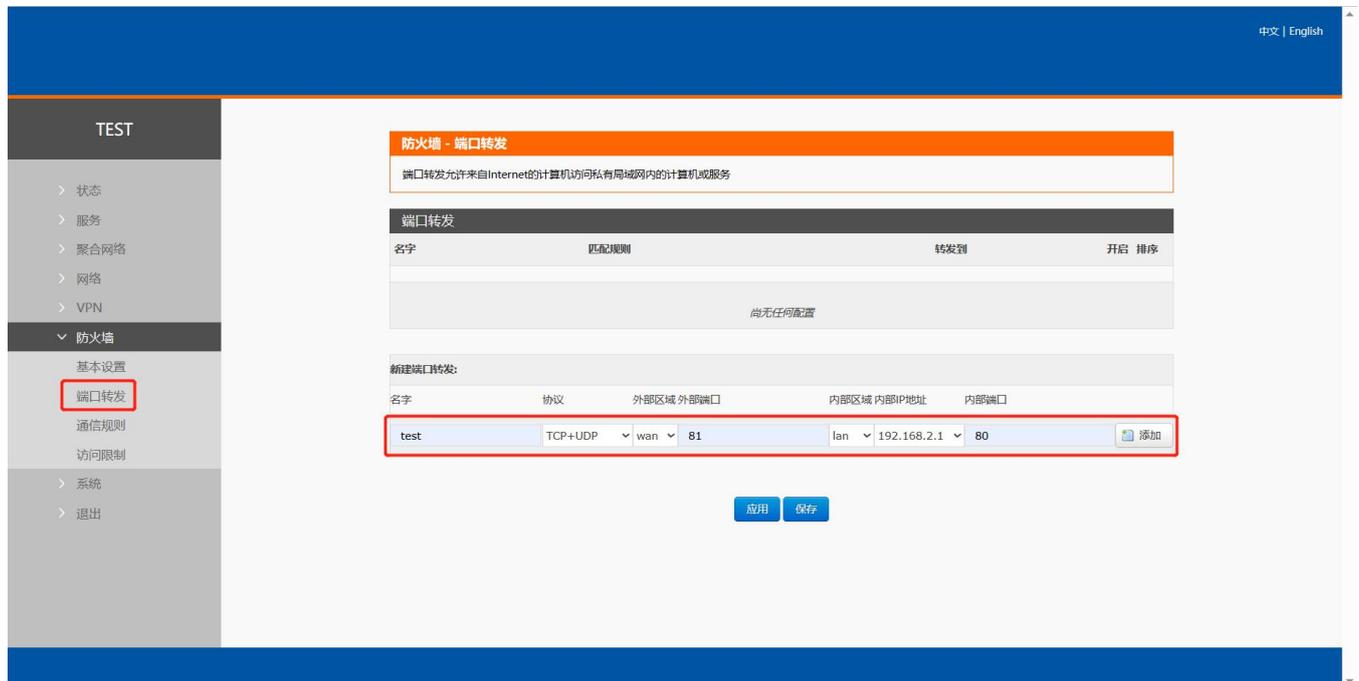


图 70 端口设置页面一

<说明>

- 设置好转发规则后，需要点击右侧的添加按钮，然后本条规则会显示在规则栏内；
- 然后点击右下角的“应用”按钮，使设置生效；
- 以下的设置，192.168.2.1:80 为路由器自身的网页服务器。如果我们想从外网去访问局域网内的某个设备，那么需要设置外网到内网的映射，比如设置外网端口为 81，内网 IP 为 192.168.2.1，内网端口为 80；
- 当我们从 WAN 口访问 81 端口时，访问请求将会被转移到 192.168.2.1:80 上面。

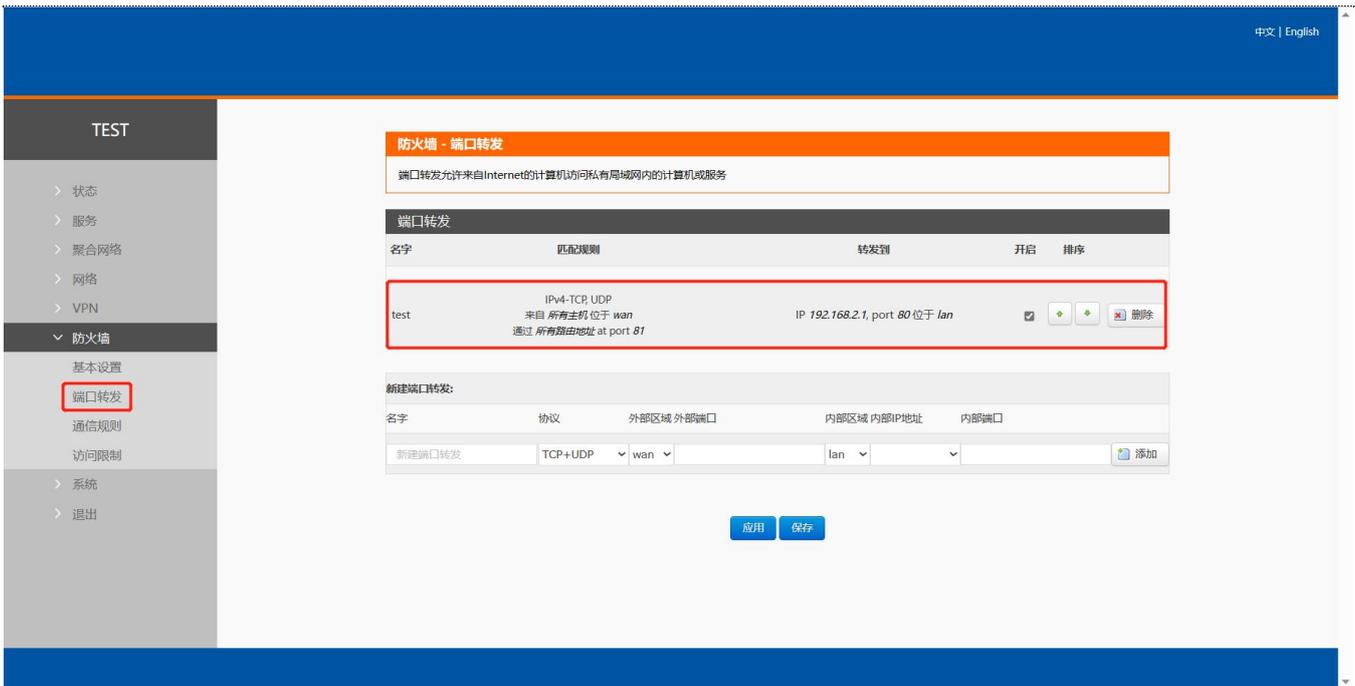


图 71 端口设置页面二

表 19 端口转发参数表

名称	描述	默认参数
名字	此条端口转发规则名称，字符类型	空
协议	协议类型，可设置：TCP+UDP/TCP/UDP	TCP+UDP
外部区域	包括有线 wan、5G、VPN、STA	wan
外部端口	可设置端口范围，例如：8000-9000 说明：当外部端口以及内部端口为空时为 DMZ 功能	空
内部区域	路由器子网区域	lan
内部 IP	路由器 LAN 区域 IP 地址	空
内部端口	可设置端口范围，例如：8000-9000 说明：当外部端口以及内部端口为空时为 DMZ 功能	空

<说明>

- 最多可添加 20 条端口转发规则。

6.3.4. NAT DMZ

端口映射是将 WAN 口地址的一个指定端口映射到内网的一台主机，DMZ 功能是将 WAN 口地址的所有端口都映射到一个主机上，设置界面和端口转发在同一个界面，设置时外部端口不填，点击“添加”即可。

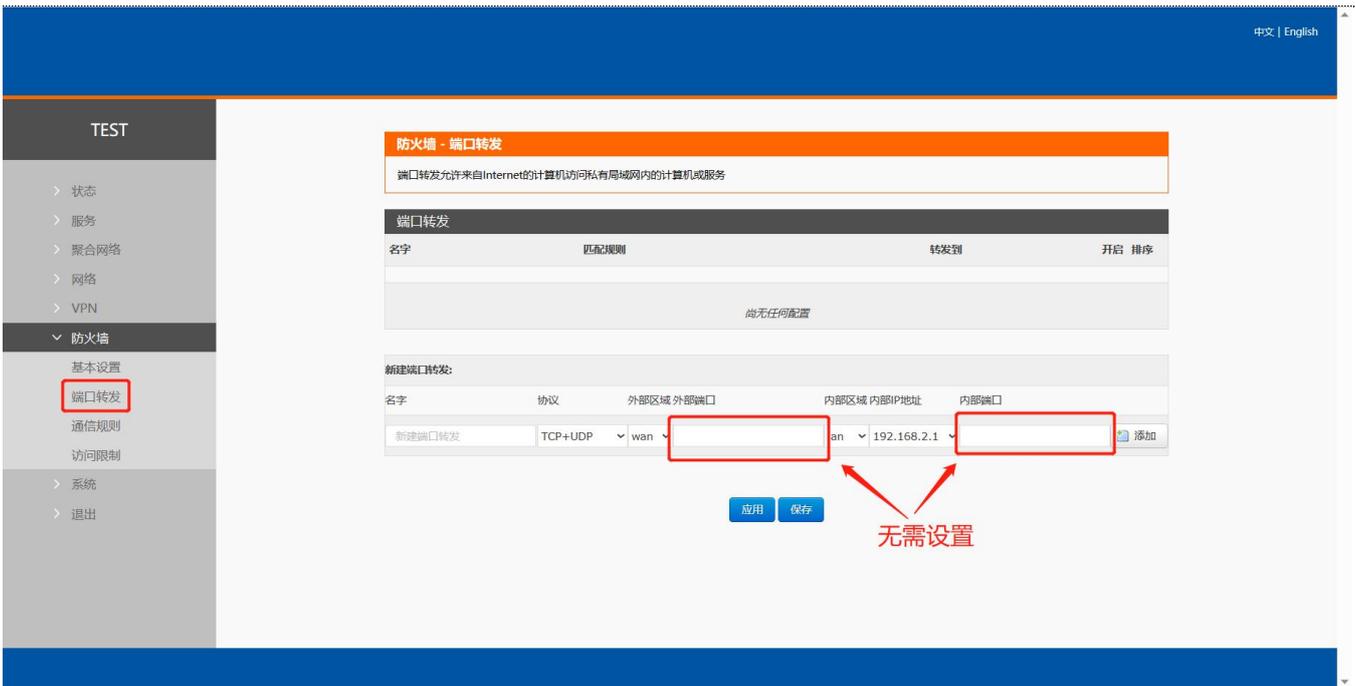


图 72 DMZ 设置一

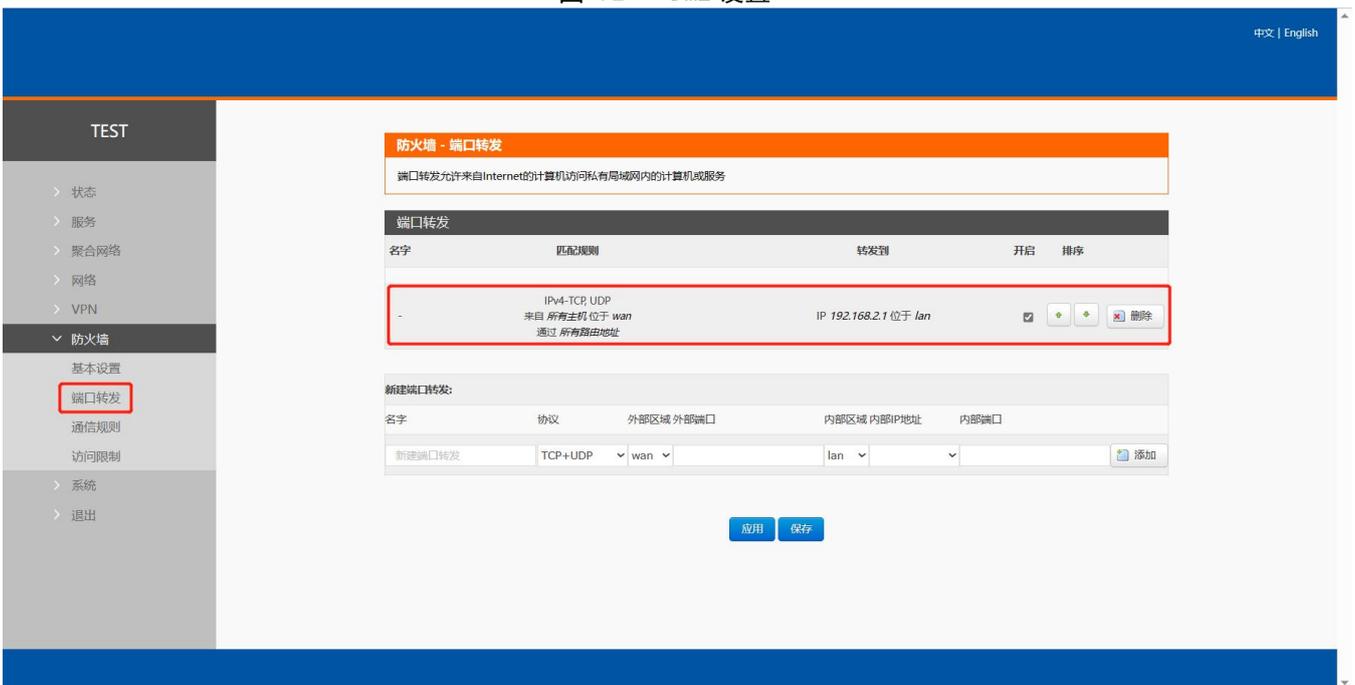


图 73 DMZ 设置二

如图，WAN 口地址的所有端口都映射到内网 192.168.2.133 这台主机上。

<注意>

- 端口映射和 DMZ 功能不能同时使用；
- DMZ 功能仅可建立一条规则使用。

6.4. 访问限制

访问限制实现对指定域名的访问限制，支持域名地址的黑名单和白名单设置，选择黑名单时，连接路由器的设备无法访问黑

名单的域名，其它域名地址可以正常访问，选择白名单时，连接路由器的设备除白名单设置的域名地址可以访问外，其它域名地址都不能够正常访问，黑名单和白名单都可以设置多条，此功能默认关闭。

6.4.1. 域名黑名单

首先，在方式选项中选择黑名单，点击添加输入该条规则的名称和正确的域名，然后点击保存，规则立即生效，连接路由器的设备将无法访问该域名。如果选择黑名单，而未添加规则，默认黑名单为空，即所有域名都可以访问。如图，除百度外，其他域名均可以正常访问。

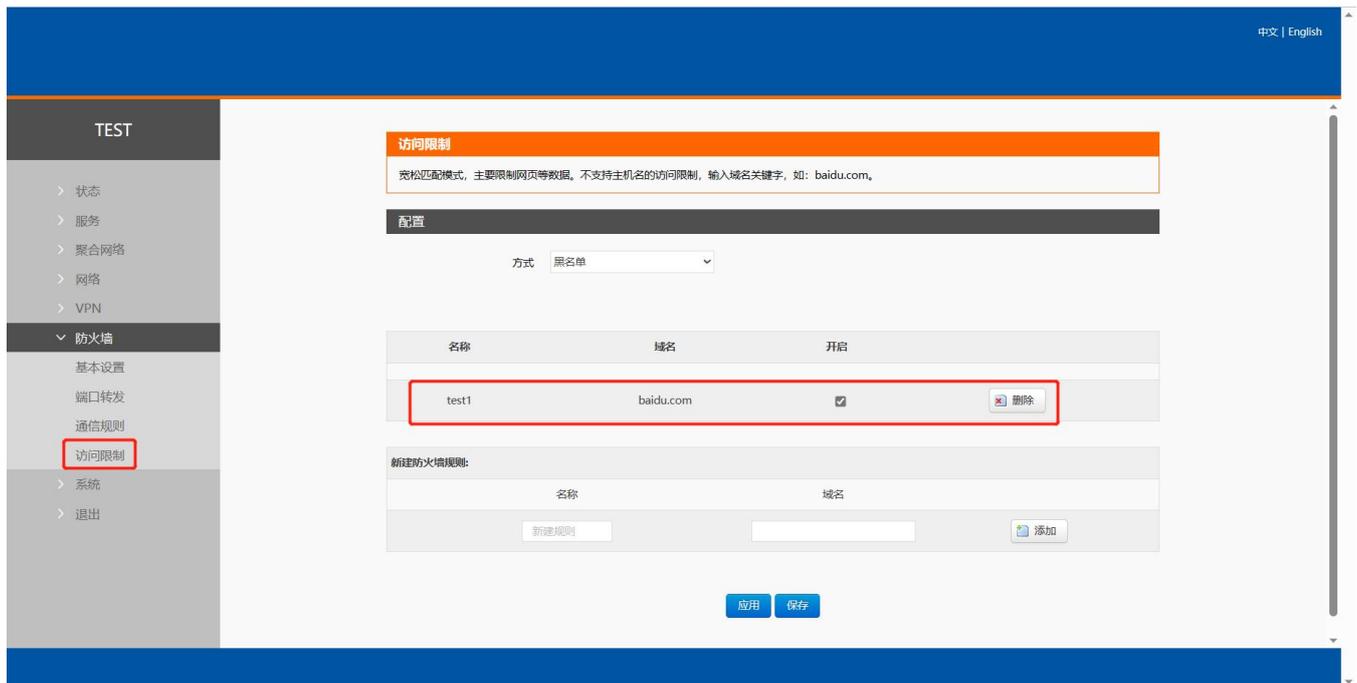


图 74 域名黑名单

6.4.2. 域名白名单

首先，在方式选项中选择白名单，点击添加输入该条规则的名称和正确的域名，然后点击保存，规则立即生效，连接路由器的设备除规则中的域名可以访问外，其他域名都不能够访问。如果选择白名单，而未添加规则，默认白名单为空，即所有域名都不能够访问。如图，设备能够访问百度。

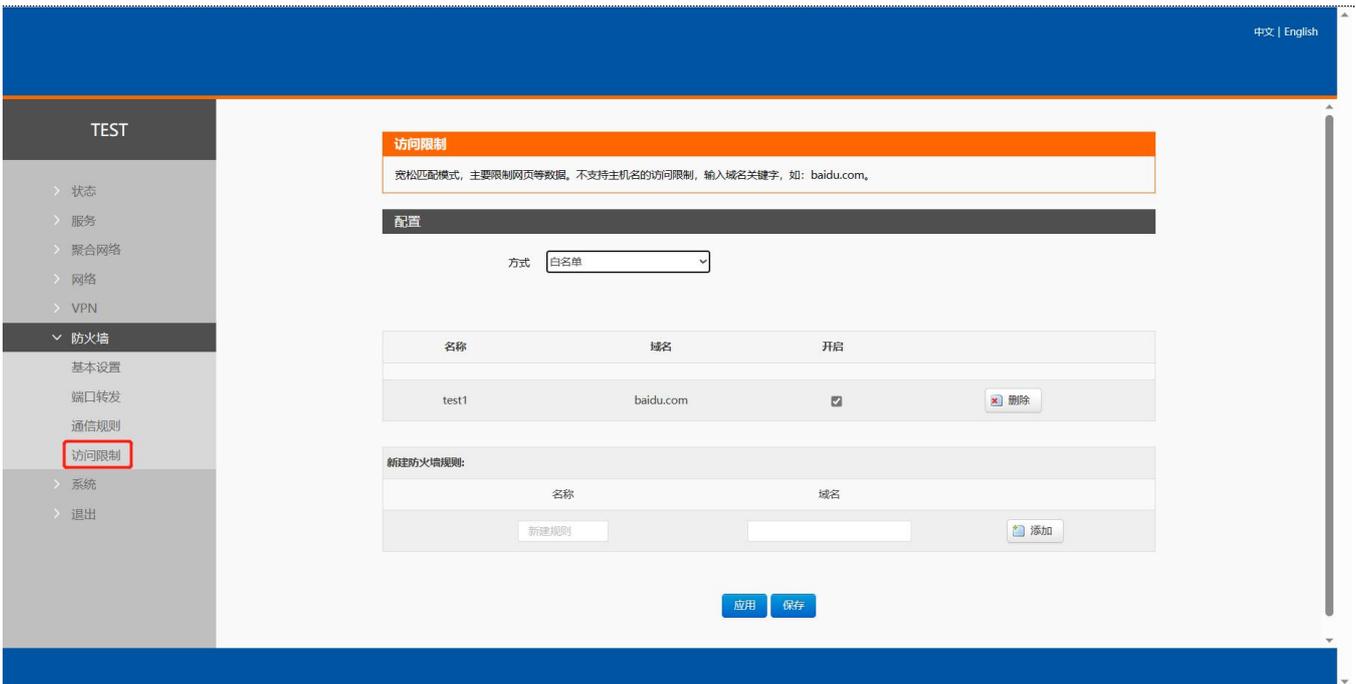


图 75 域名白名单

<说明>

- 最多可添加 20 条访问限制规则。

7. 高级服务

7.1. 云服务

路由器远程管理平台服务地址：[路由器远程管理平台](#)，可以将路由器设备在路由器远程管理平台进行：监控、控制、批量配置、统计、硬件断电报警等高效率、统一化的管理。

<说明>

- USR-G810-33 默认未开启云服务功能。路由器 Web 界面可以配置统计流量、网络状态、心跳包的上报参数；同时支持数据上报到私有部署。
- 设备如需上路由器管理平台，请将私有化部署勾选，并设置私有云设备接入地址：106.14.191.33，端口设置：7100；
- 请登录路由器远程管理平台，注册账号，添加设备后管理。

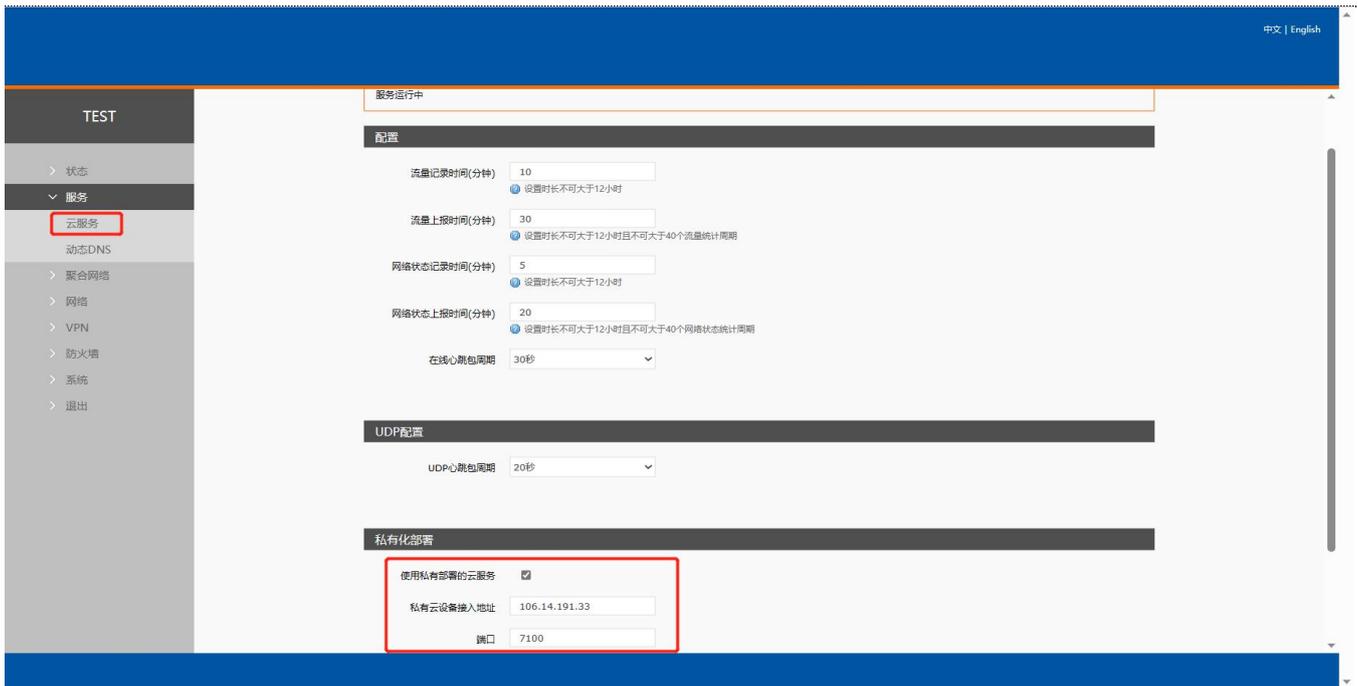


图 76 USR-G810-33 有人云服务界面

7.1.1. 监控大屏

监测大屏，可以按照项目以及设备系列展示设备在线情况、位置信息等信息。



图 77 监测中心

7.1.2. 设备管理

7.1.2.1. 添加设备

点击“添加设备”

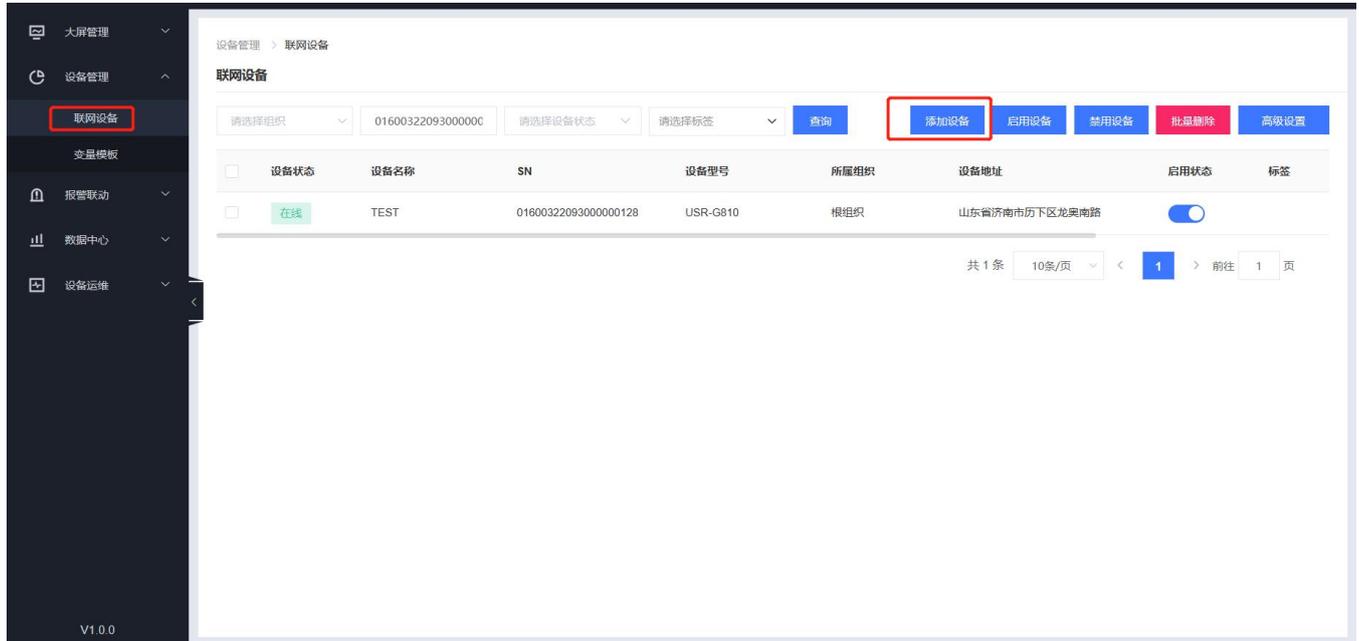


图 78 有人云—添加设备界面一

USR-G810-33 出厂标签上提供设备的 MAC、SN；有人云添加设备时需要填入这些参数。

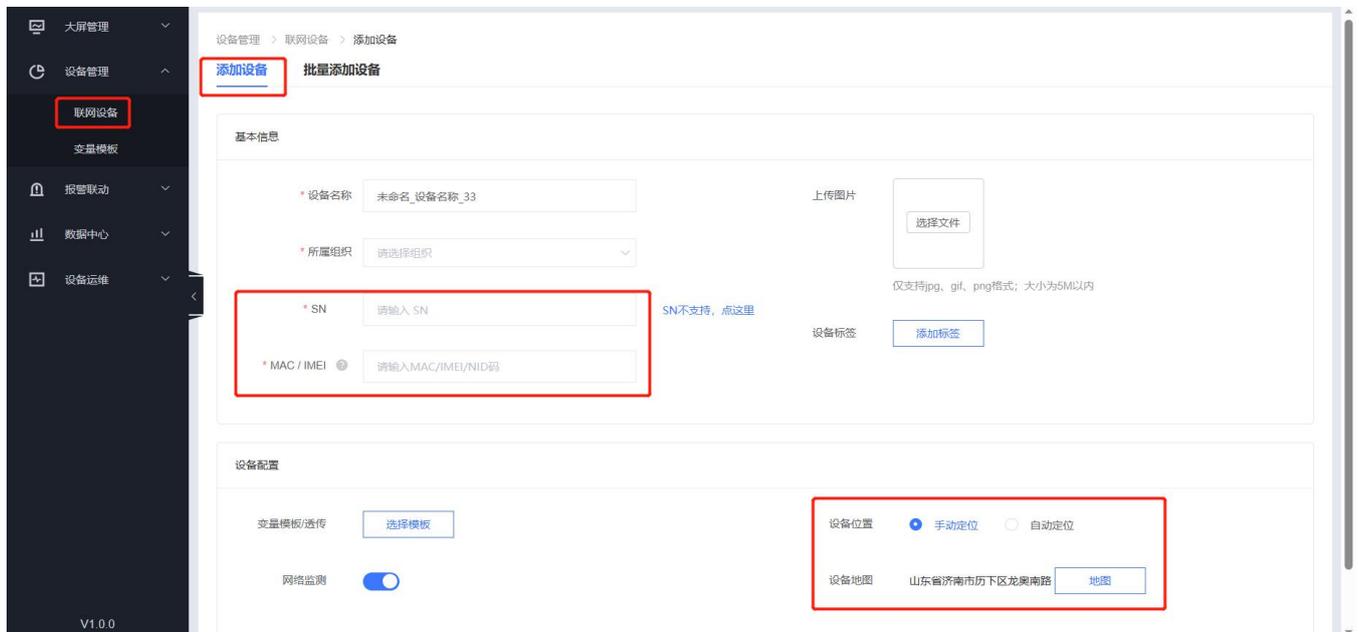


图 79 有人云—添加设备

表 20 有人云添加设备参数表

名称	描述	默认参数
----	----	------

设备名称	给此设备设置一个名称，必填项	未命名_设备名称_XX
所属组织	设备所属于的分组，可作为设备查询筛选项，必选项 例如：此设备属于山东-济南	无
SN	设备 SN 号，必填项 路由器可通过查看小标签 SN 填入	无
MAC/IMEI	可通过田 MAC/IMEI/NID，必填项 路由器可通过查看小标签 MAC 或者 IMEI 填入	无
变量模板/透传	可设置变量模板	无
网络监测	开启：网络监测开启 关闭：将不再监测此设备	开启
上传图片	可以上传设备或者现场图片	无
设备标签	可以给此设备设置标签，可通过标签筛选同一标签设备	无
设备位置	手动定位：可通过“设备地图”设置此设备的具体位置 自动定位：需要设备支持基站定位或 GPS 定位功能	手动定位
设备地图	可手动设置设备具体位置	山东省济南市历下区龙奥南路

<说明>

- 设备亦可批量添加，需按照指定格式将信息填写正确；
- 批量添加模板可在批量添加设备处“下载 Excel 模板”；
- USR-G810-33 不支持基站和 GPS 定位，如需支持需沟通定制。

7.1.2.2. 数据查看

在“设备管理” - “联网设备” - “设备列表”下，找到相应设备，点击“数据查看”可查看设备基本信息。



图 80 有人云一数据查看

7.1.2.3. 设备运维

在“设备管理” - “联网设备” - “设备运维”下，找到相应设备，点击“设备运维”可查看设备基本信息以及发送 AT 配置。

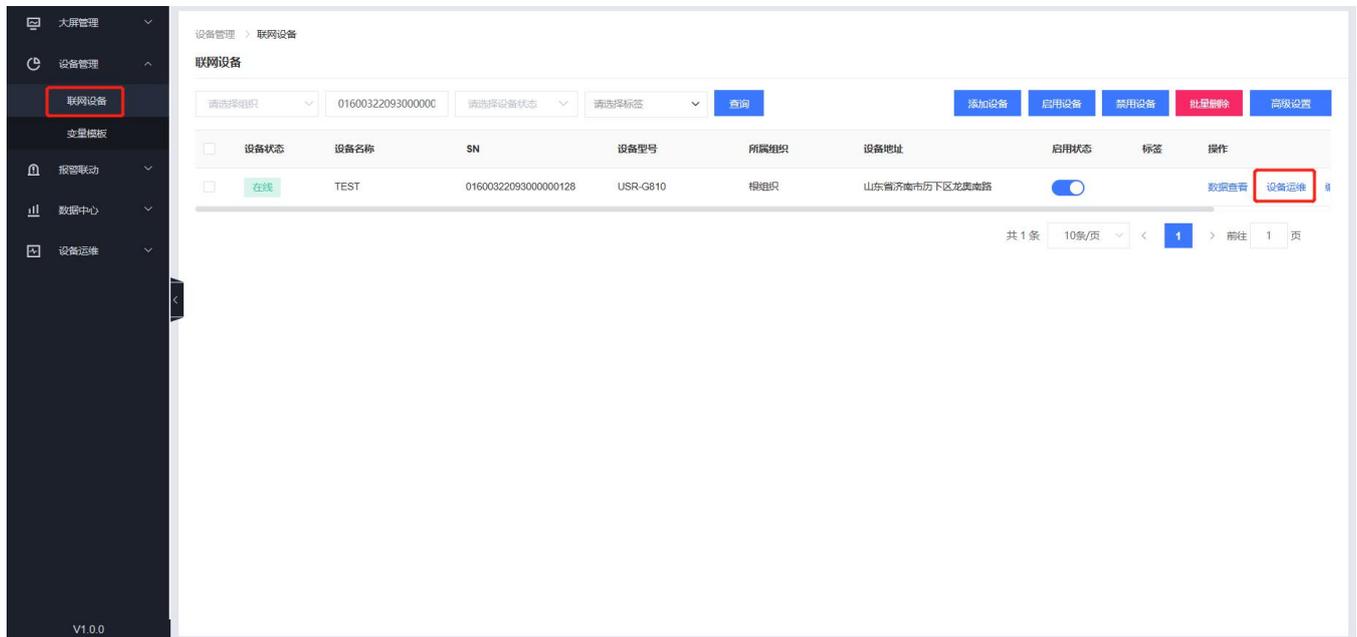


图 81 有人云—设备运维

7.1.2.4. 设备概况

可以查看设备一些基本信息，如图所示：

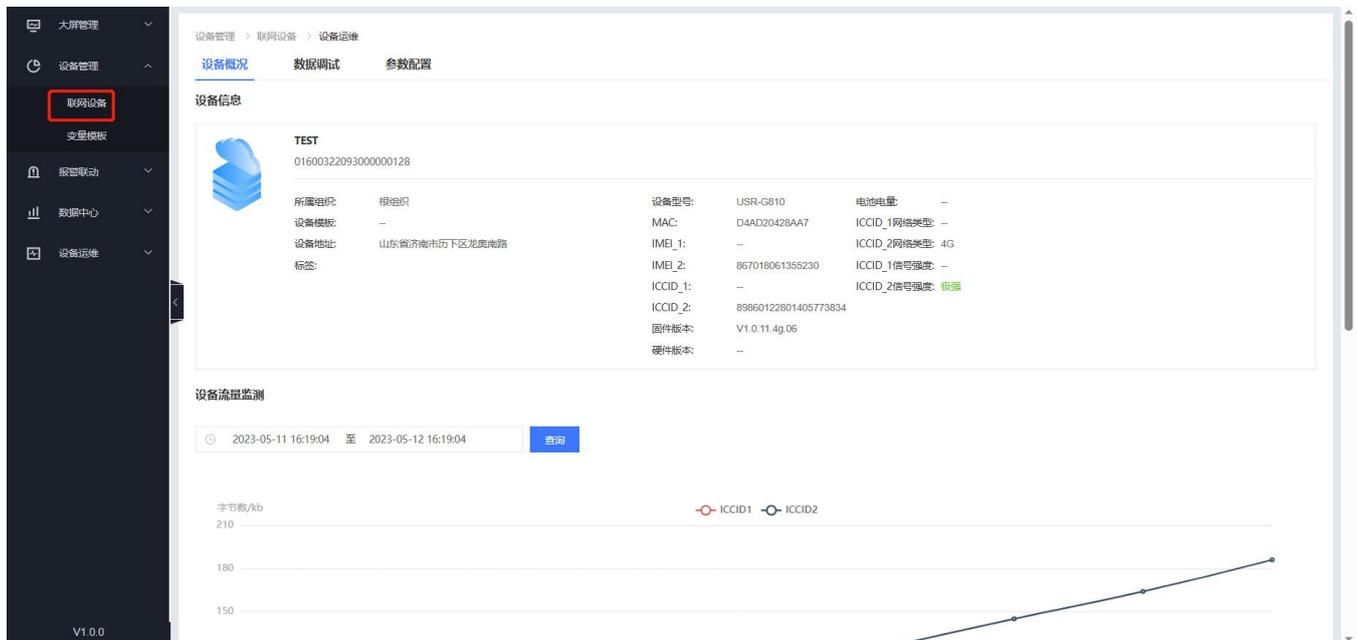


图 82 设备概况

<说明>

➤ 设备如使用 SIM 卡上网，设备流量监测和信号质量监测将生效。

7.1.2.5. 参数配置

在参数配置界面，可以输入 AT 指令来进行配置设备的某些参数，或者读取设备的某些参数，并且参数的返回也会显示在平台上面。本款路由器支持批量可视化配置以及远程打开内置网页，无需复杂的 AT 配置查看路由器参数。

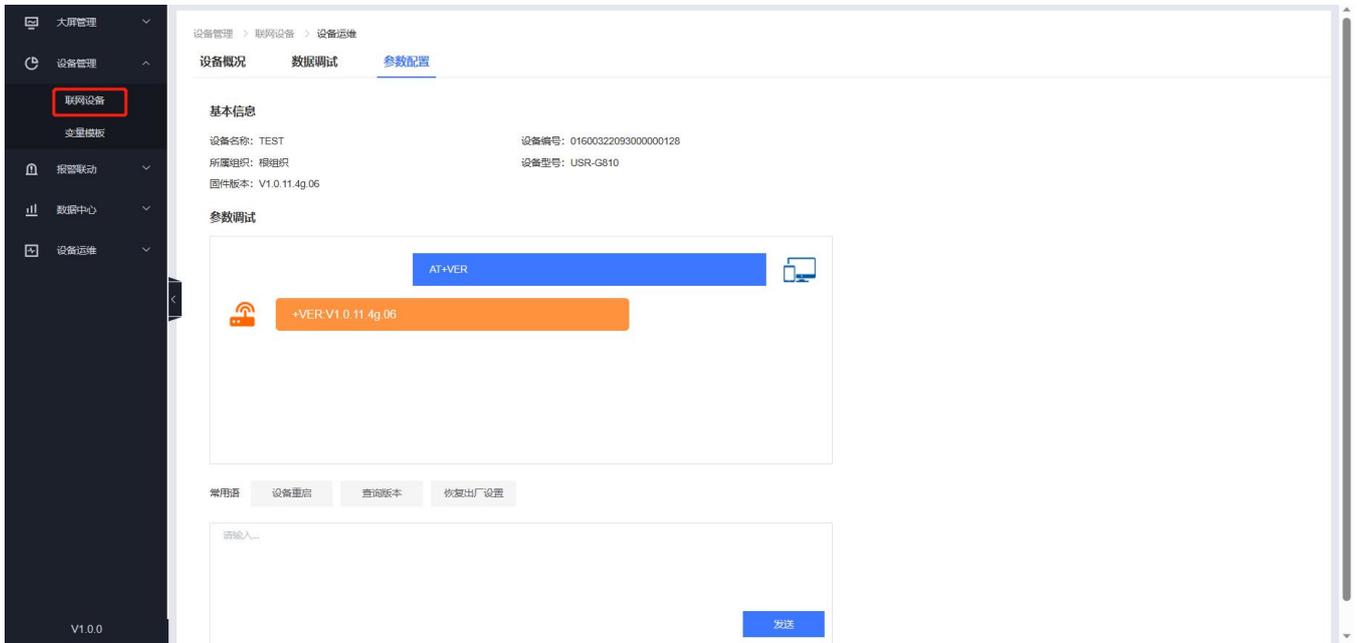


图 83 参数配置

7.1.2.6. 配置网页

G810-33 支持有人云配置远程登录设备网页进行配置操作。

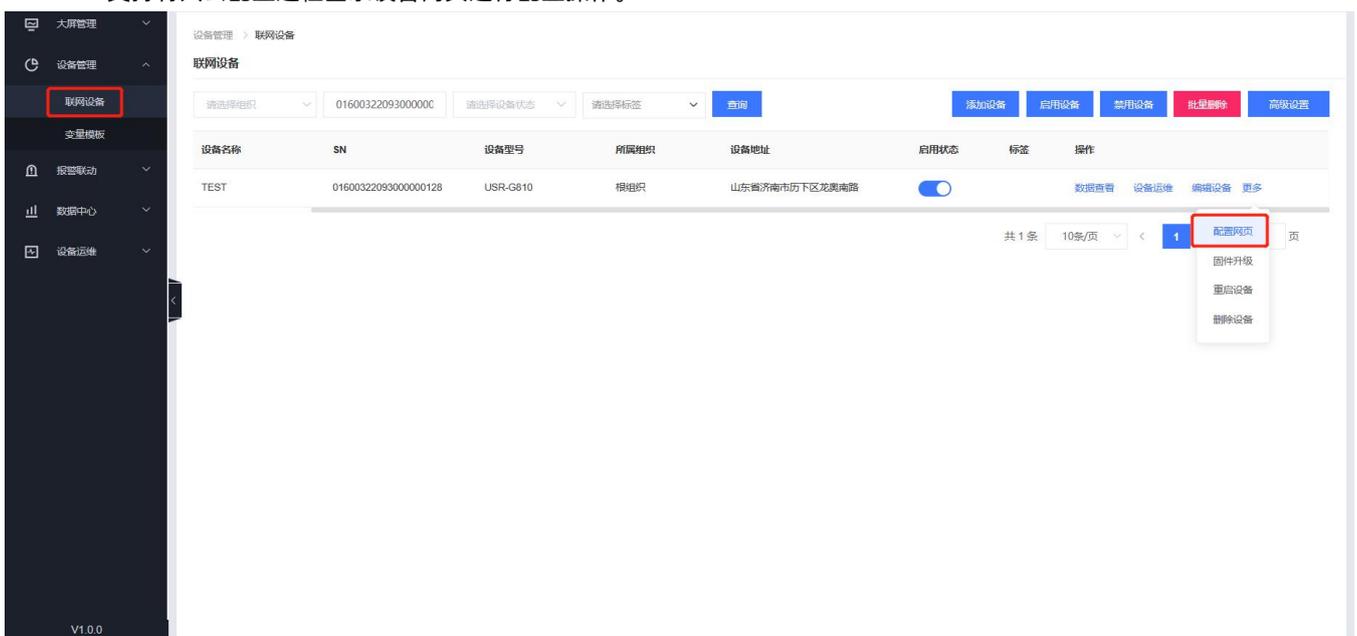


图 84 配置网页（一）

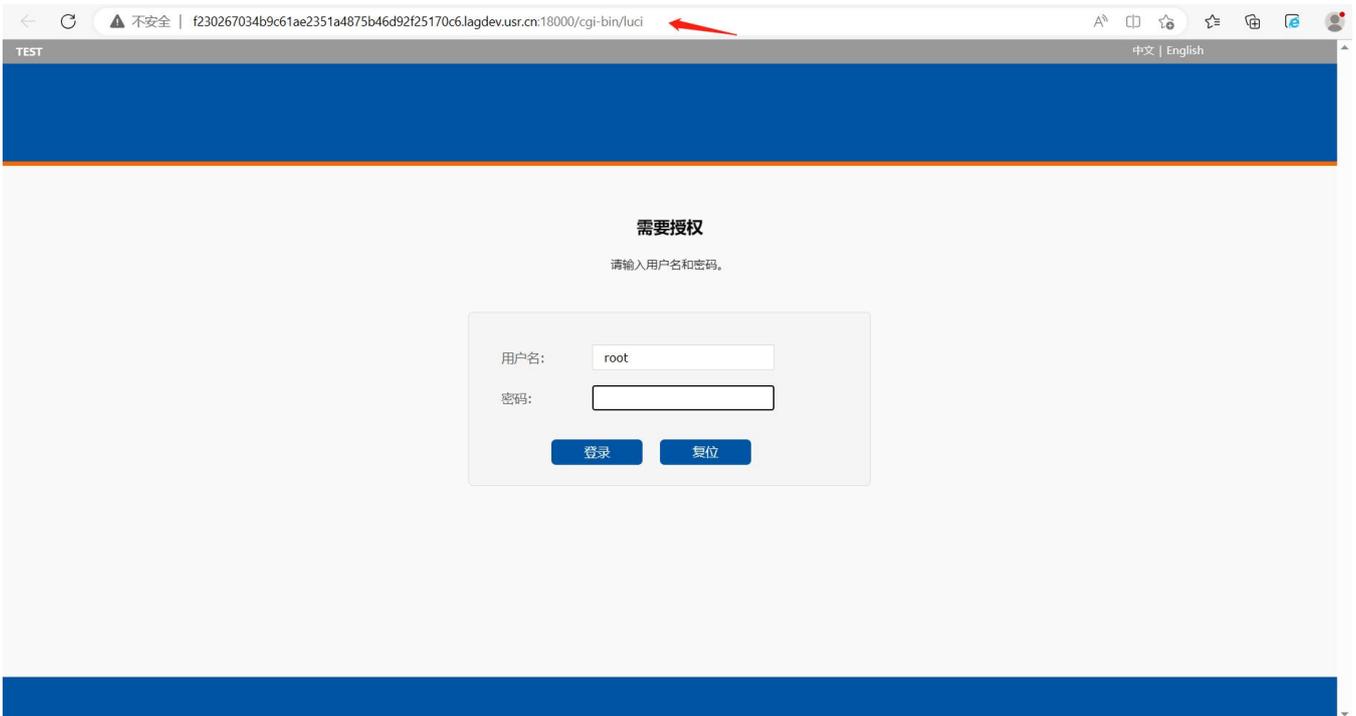


图 85 配置网页（二）

<说明>

- 点击配置网页弹出本设备网页如上图，登录网页进行配置；
- 如出现链接打不开内置网页情况请在有人云，选择对应设备的“配置网页”直接打开。

7.1.3. 报警联动

7.1.3.1. 配置报警联系人

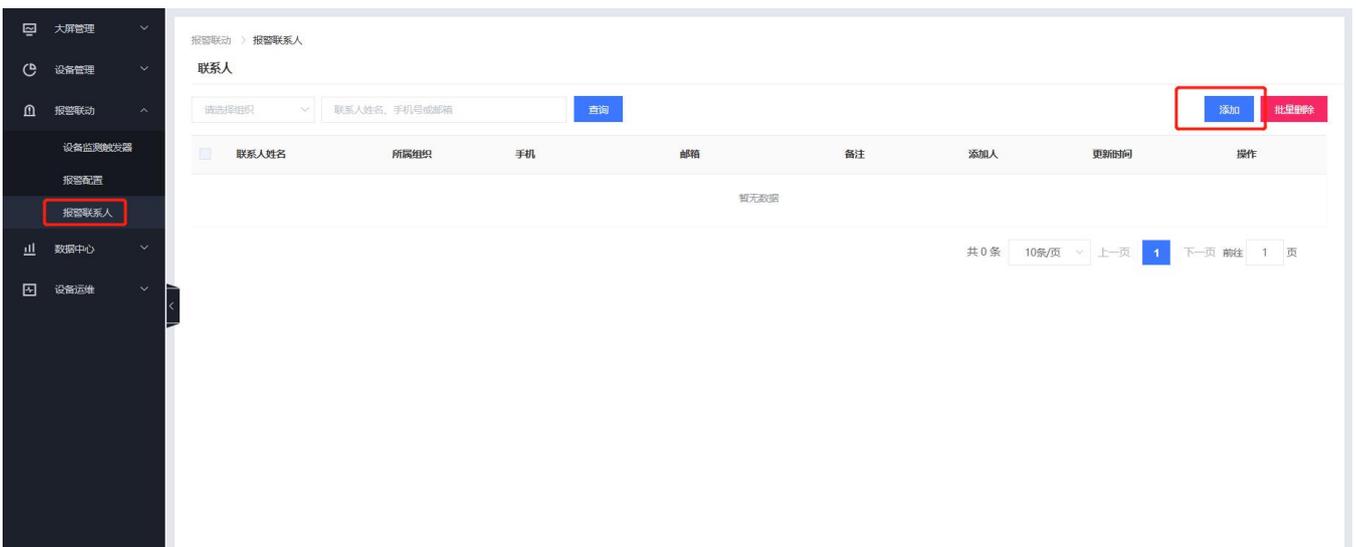


图 86 添加报警联系人（一）

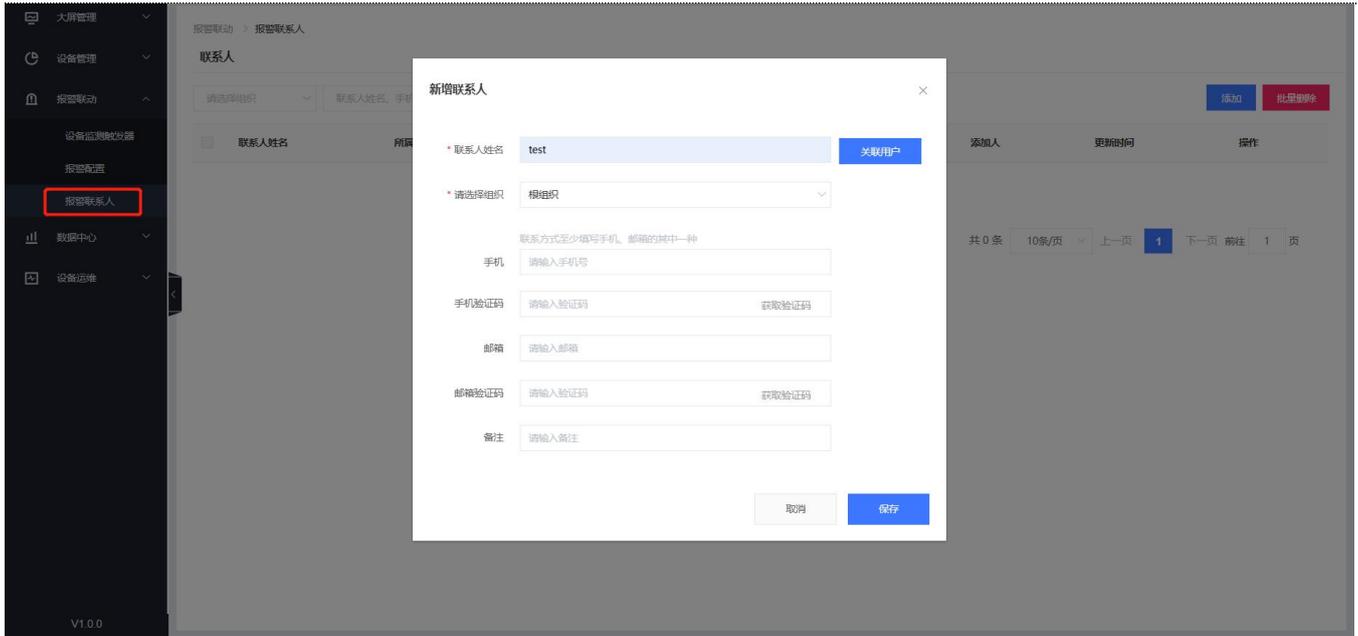


图 87 添加报警联系人 (二)

7.1.3.2. 设置监控触发器

路由器出发什么条件会报警的配置界面。

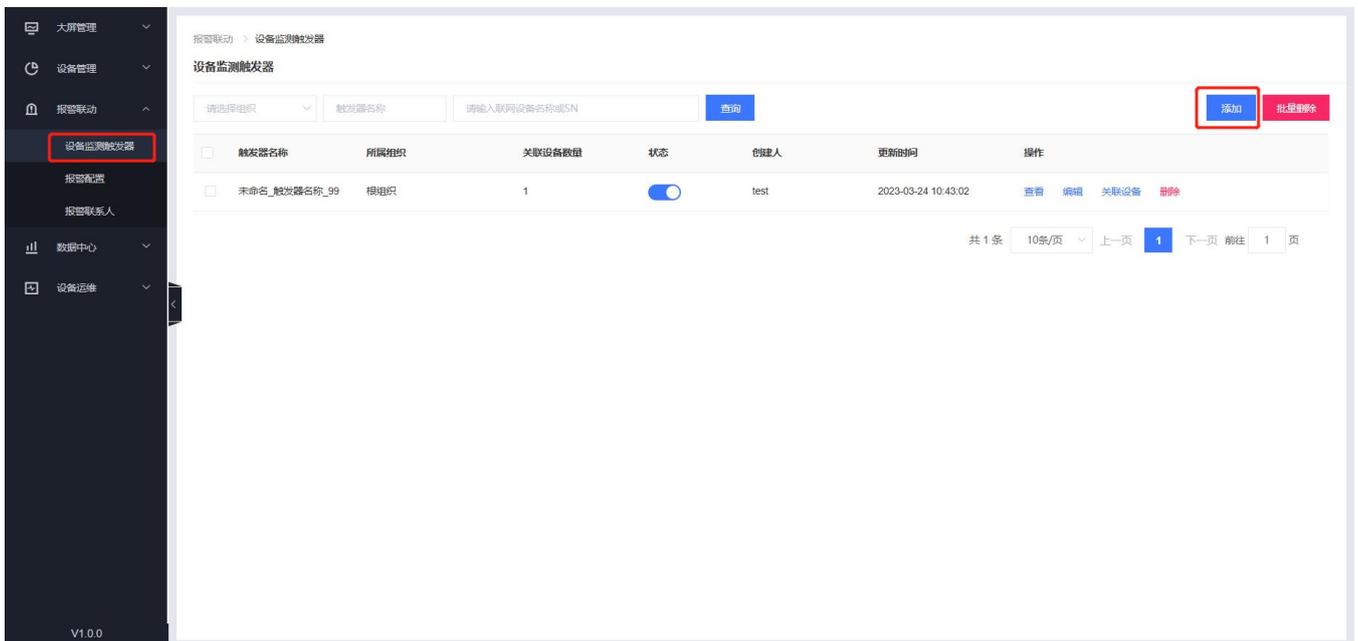


图 88 添加设备监测触发器 (一)

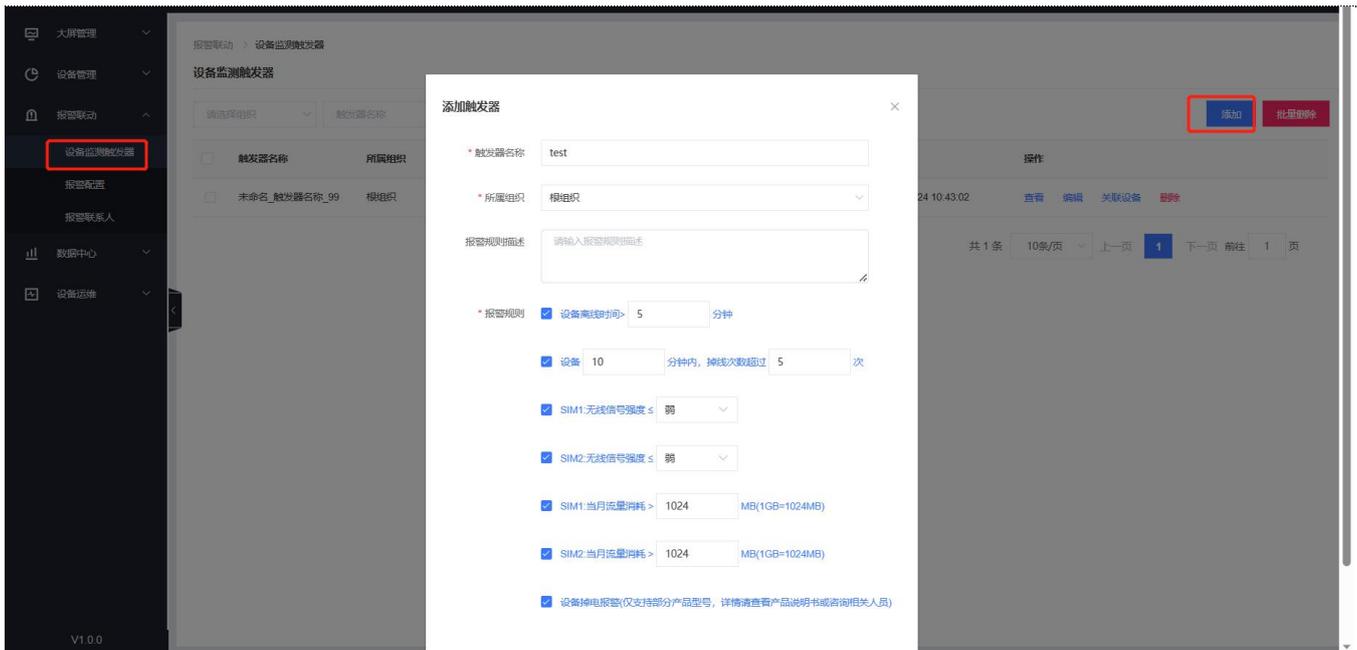


图 89 添加设备监测触发器 (二)

关联设备，那些设备触发以上条件会报警的配置。

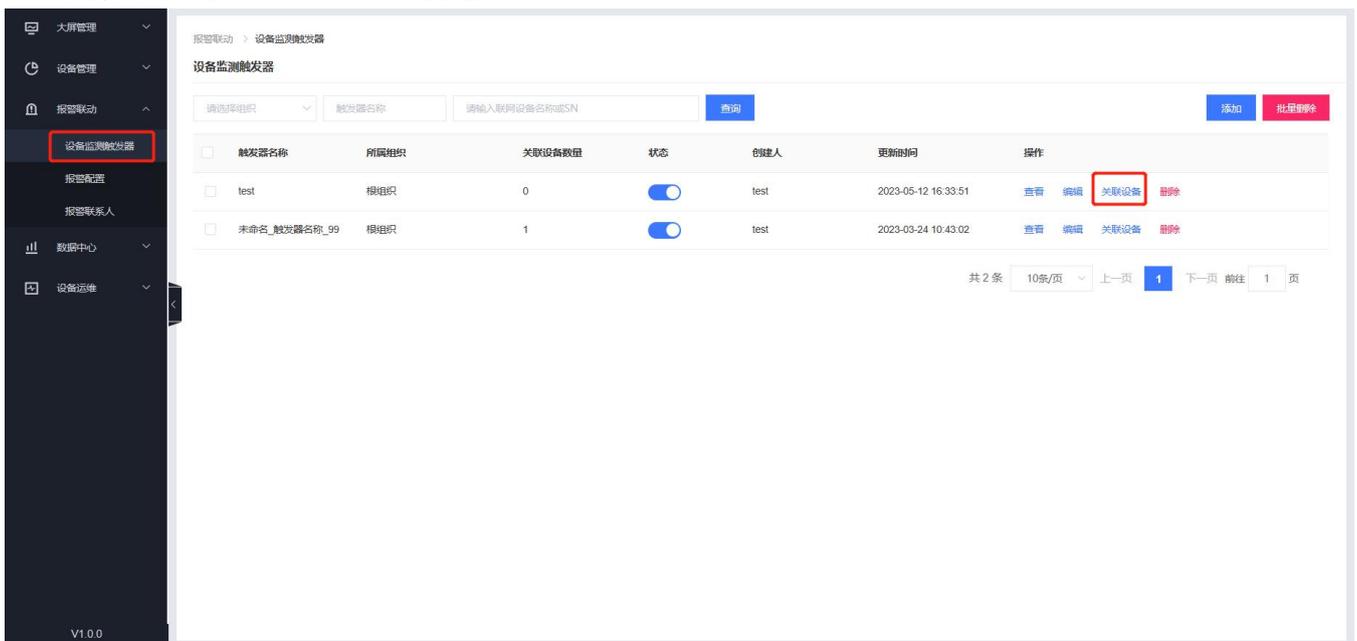


图 90 关联设备

7.1.3.3. 报警配置

将设备检测触发器和报警联系人关联，某台设备触发了某些触发条件将报警信息发给那位报警联系人。

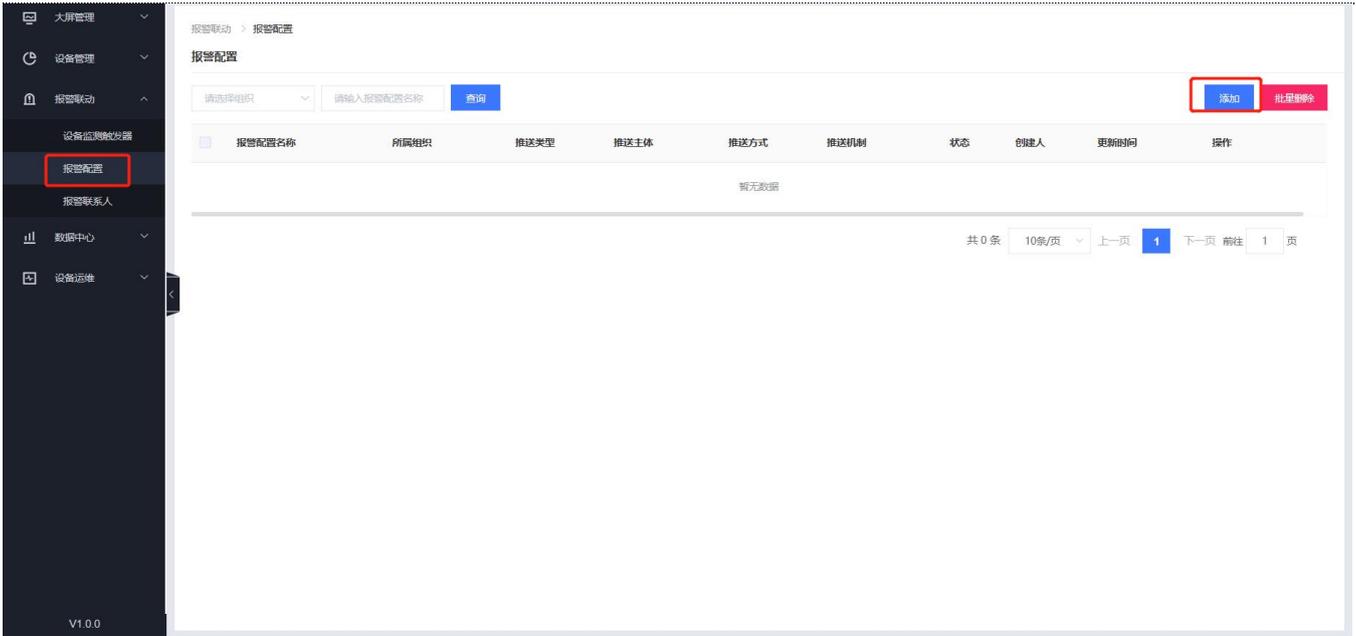


图 91 配置报警



图 92 配置报警

7.1.3.4. 报警验证

以硬件断电举例



图 93 邮件报警信息举例

7.1.4. 数据中心

7.1.4.1. 设备上下线

可 SN 查询某台设备一段时间的上下线情况。

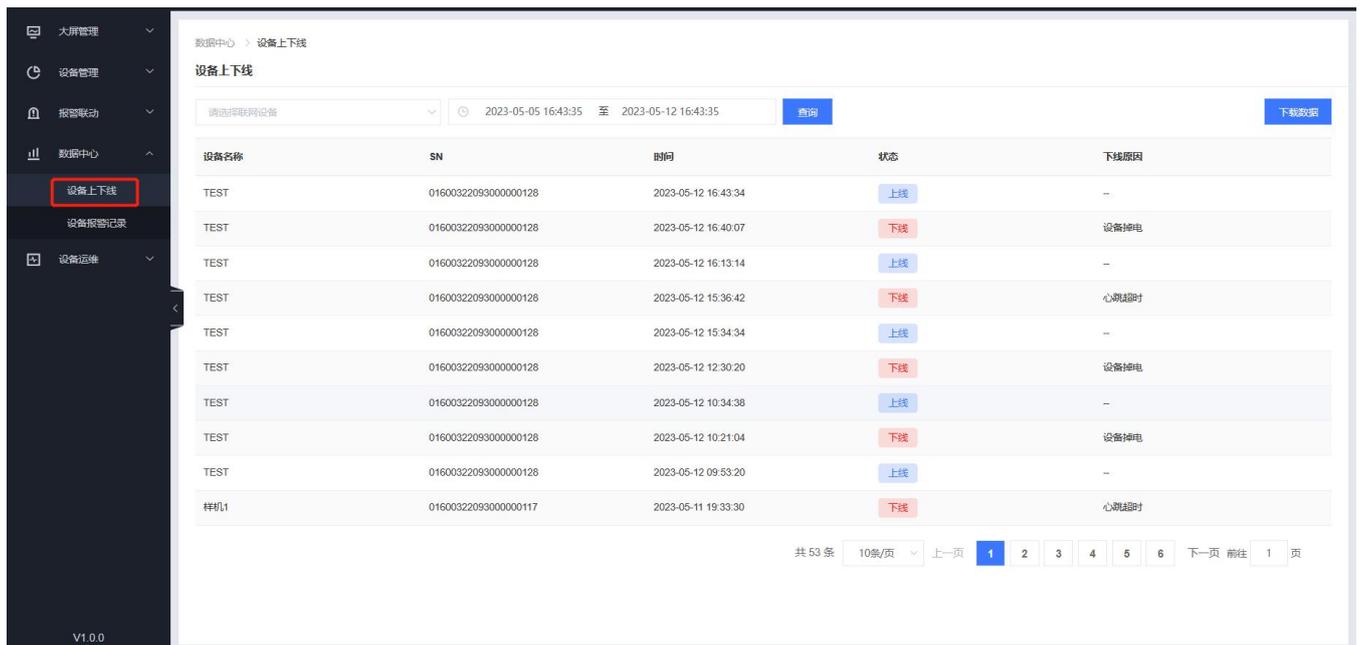


图 94 设备上下线统计

7.1.4.2. 设备报警记录

看看所有的设备报警记录，也可通过时间、SN 等精确查看报警记录。

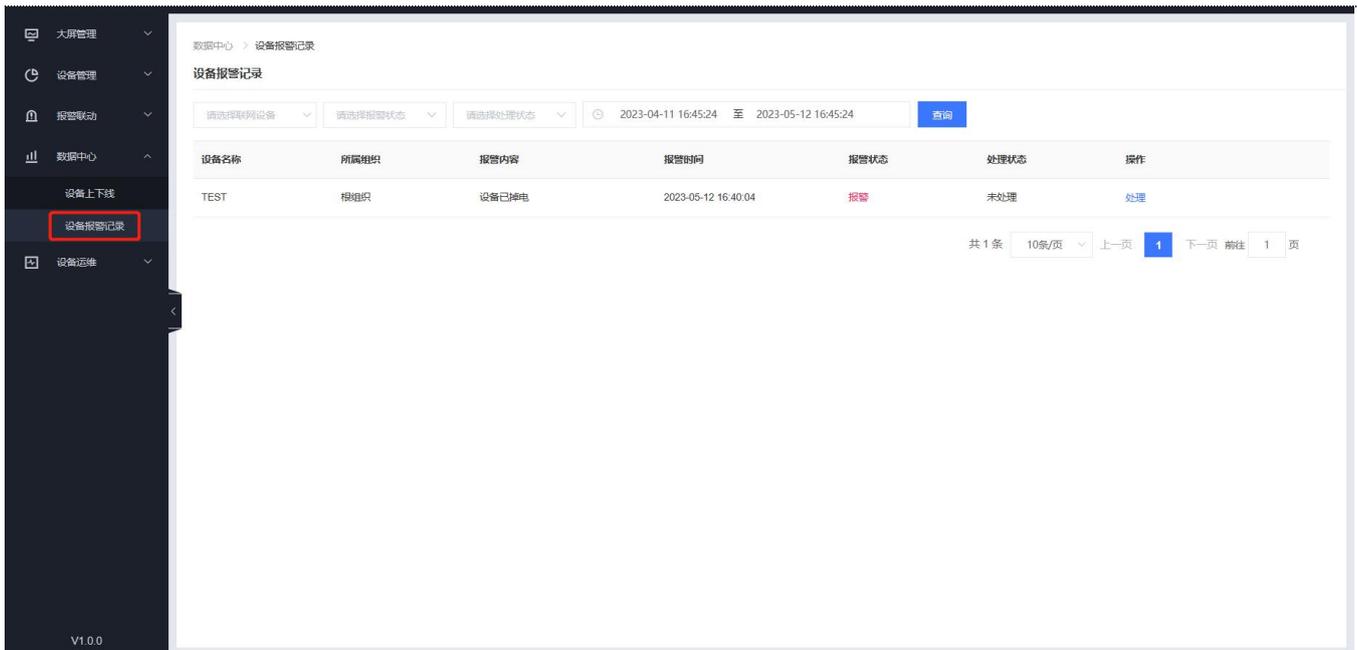


图 95 设备报警记录统计

7.1.5. 设备运维

7.1.5.1. 远程配置

G810-33 支持远程可视化批量配置路由器，无需繁琐 AT 批量配置。轻松快速完成配置任务。

可视化的平台批量配置，免去繁琐的配置每台设备，也免去您需定制默认参数的烦恼，高效运维。

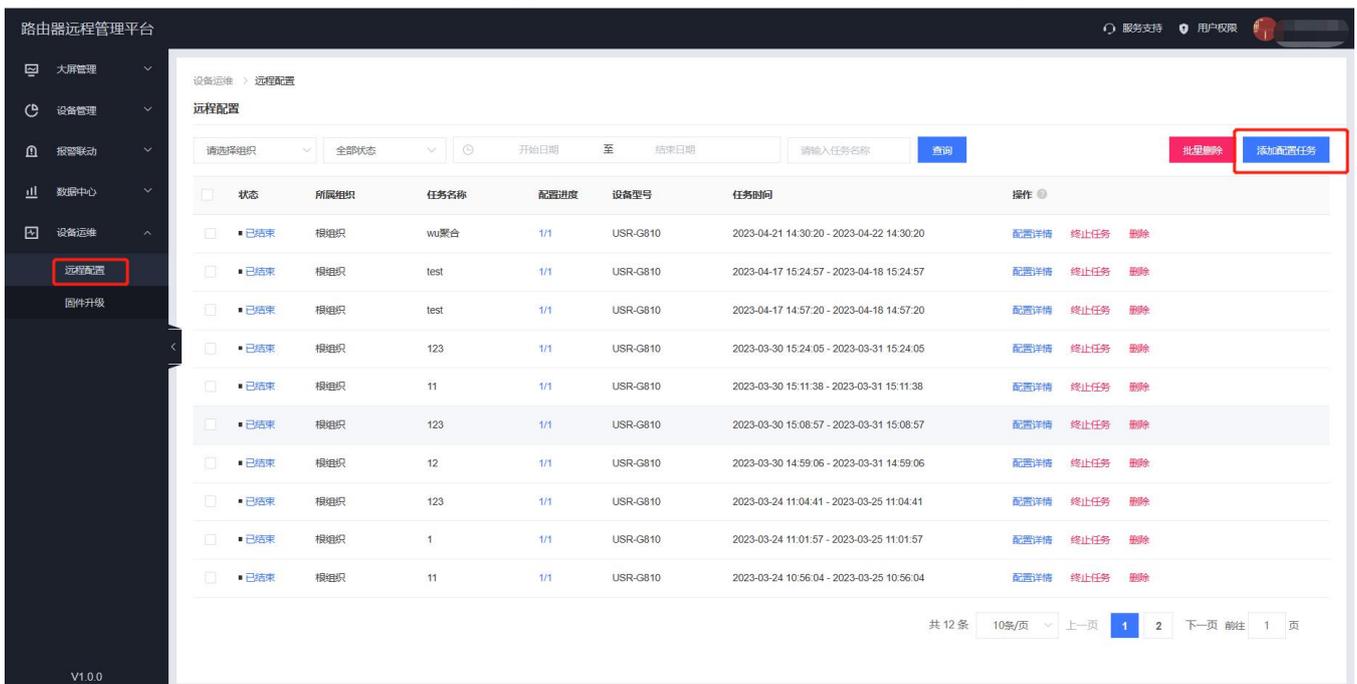


图 96 远程配置 (一)

如下，点击进行下一步。可以看到当前设备型号下，已经存在的设备，并选择需要对其进行配置的设备，然后点击下一步。

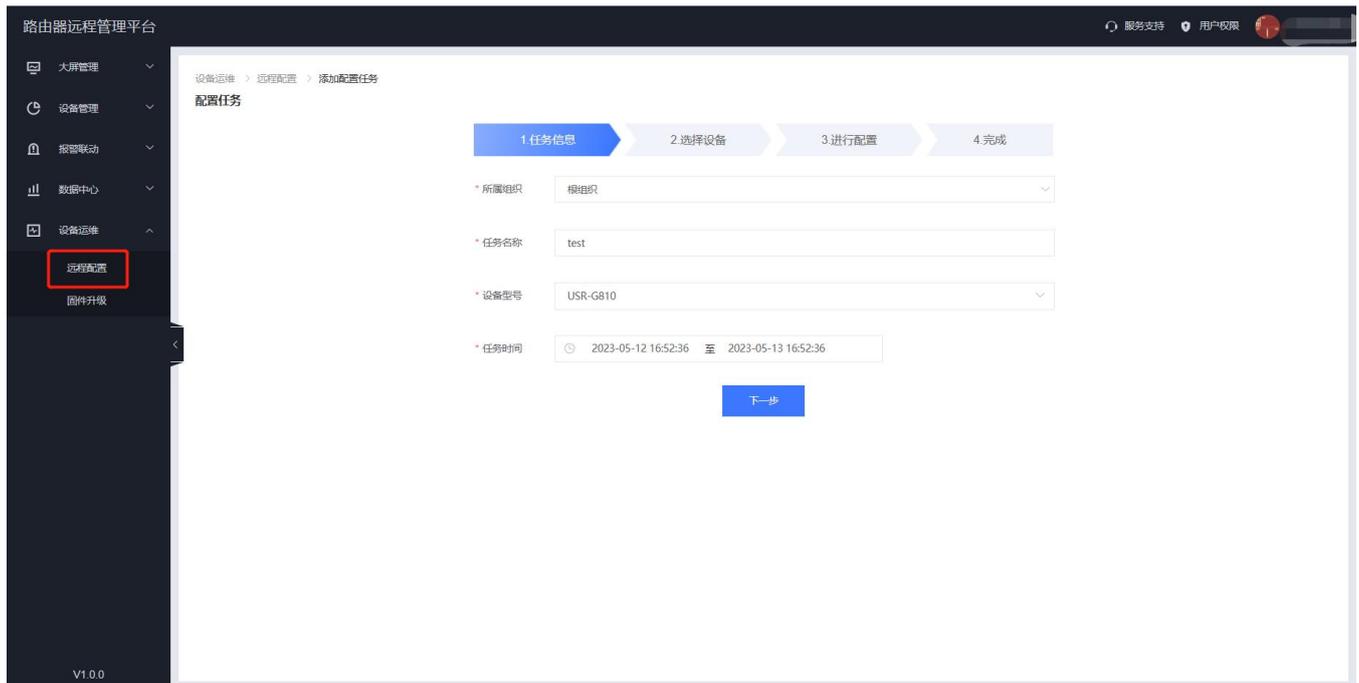


图 97 远程配置 (二)

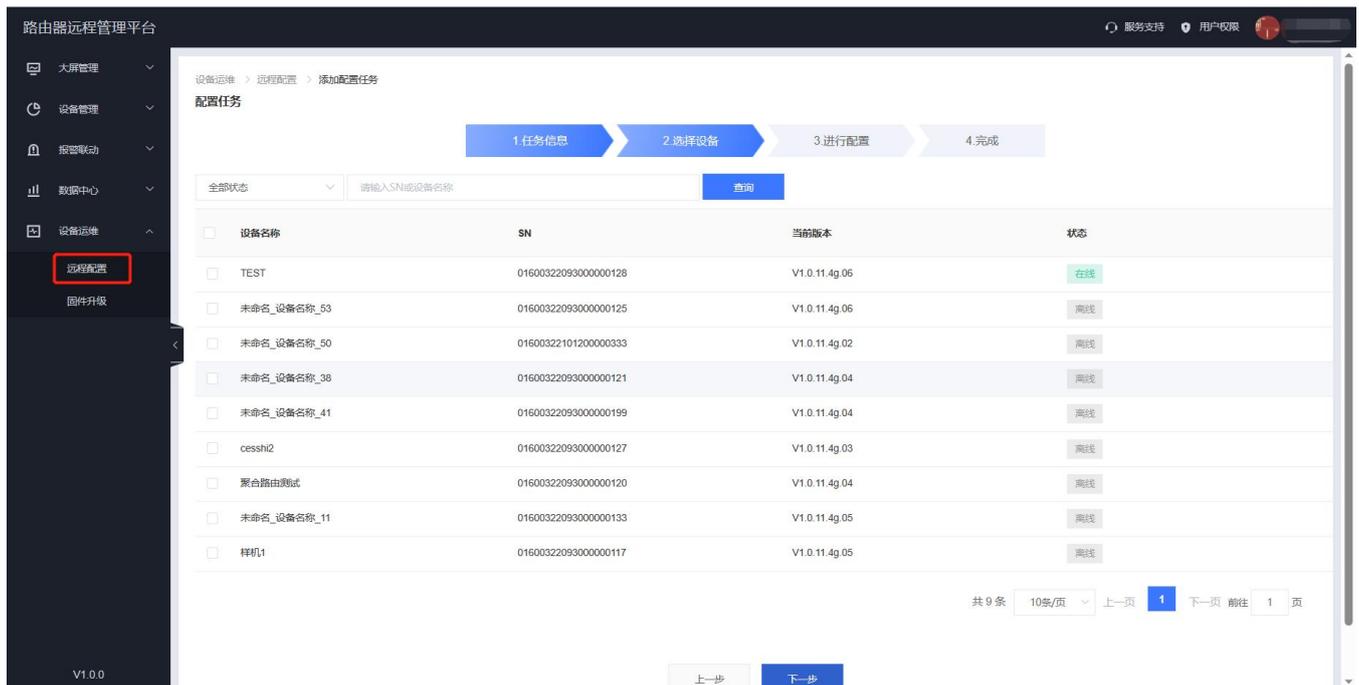


图 98 远程配置-选择批量的设备

可以进行常用参数配置，也可在高级设置中进行设置其他参数，设置完成后点击“确认”。

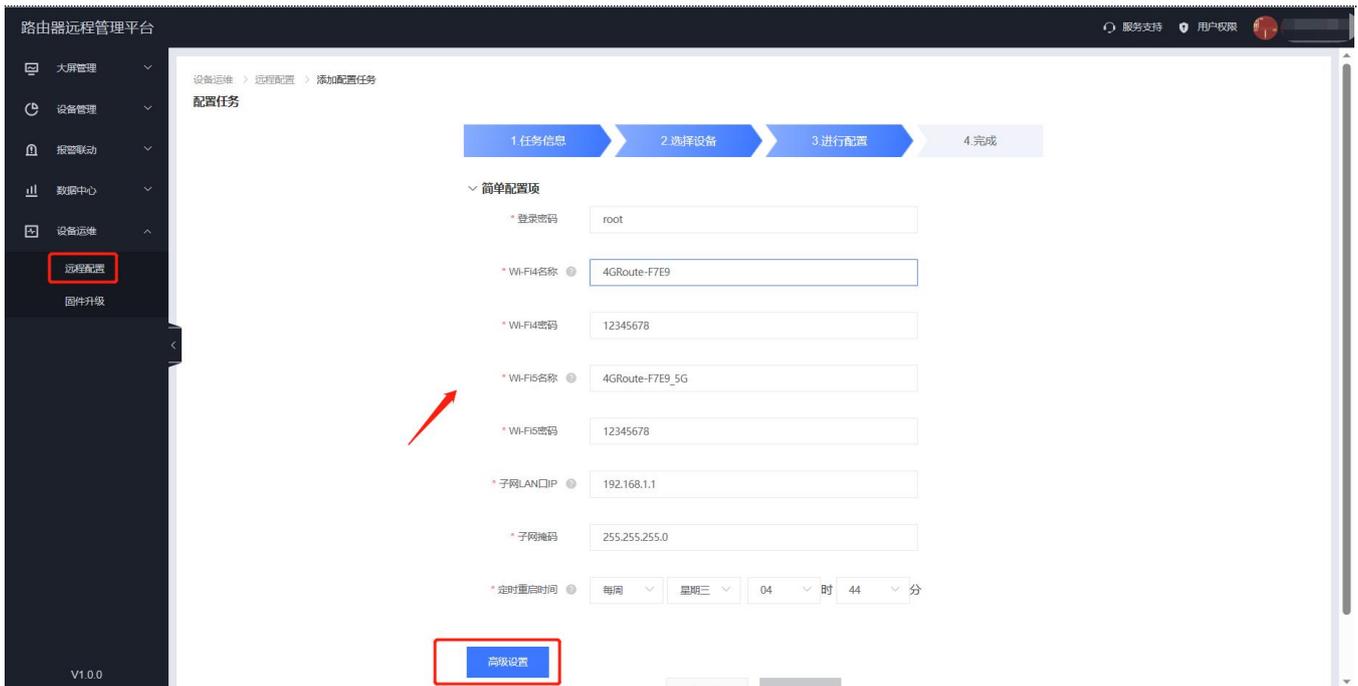


图 99 远程配置-可以设置基本的参数

将您需要设置的参数设置好后，任务添加完成，会将您在平台设置的参数，在您勾选的所有设备进行配置。配置完成后路由器将自动重启。

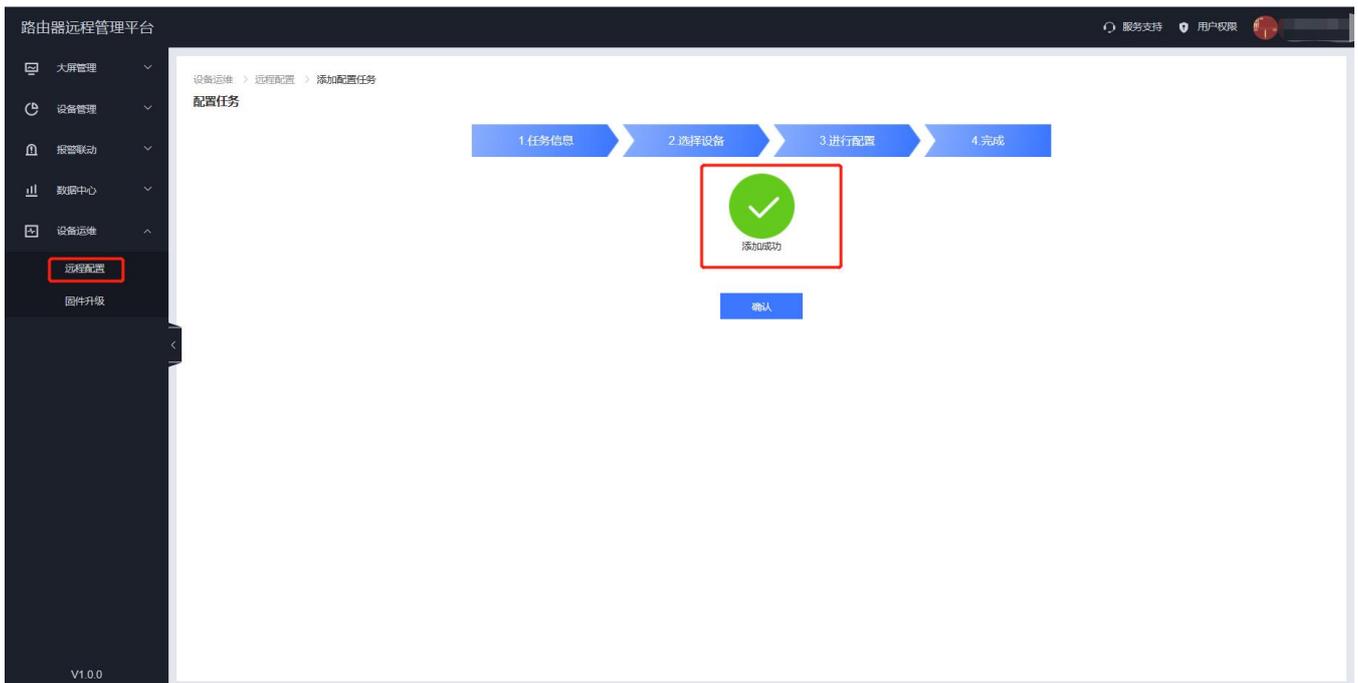


图 100 远程配置任务添加成功

7.1.5.2. 固件升级

平台支持对路由器自身设备进行固件升级。注意：这里的固件升级不是给下端客户设备升级。在“设备管理”“联网设备”-“更多”下，找到想要进行固件升级的设备，选择“固件升级”。

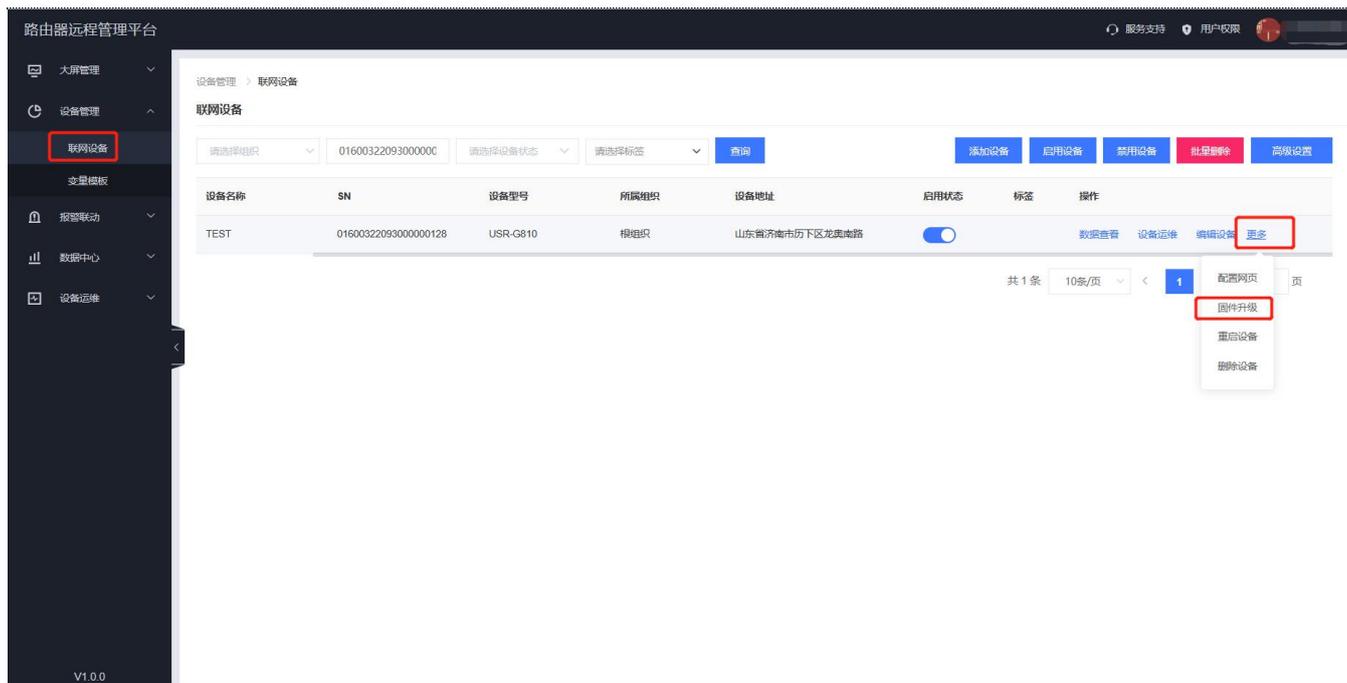


图 101 固件升级（一）

也可以在“设备运维”-“固件升级”下，点击“添加升级任务”。

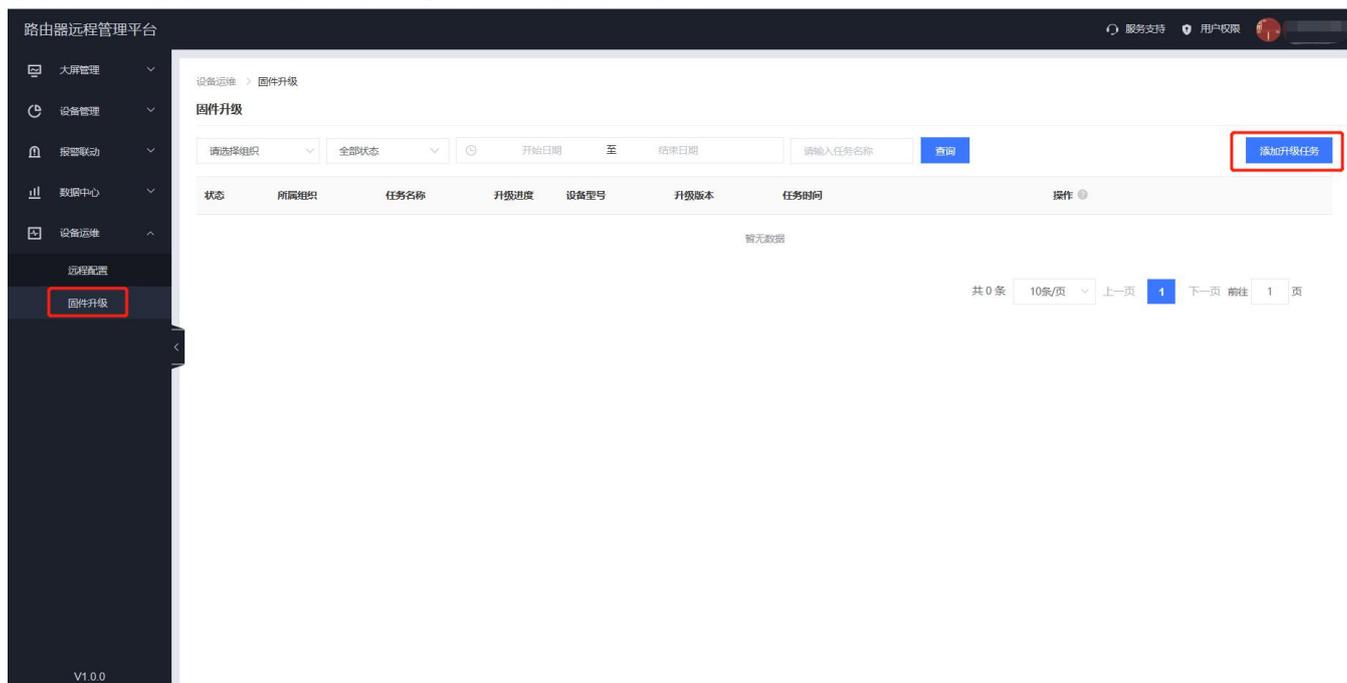


图 102 固件升级（二）

填写上本次固件升级的“任务名称”，选择“固件升级版本”，填写“任务时间”，点击“确认”后进行下一步。

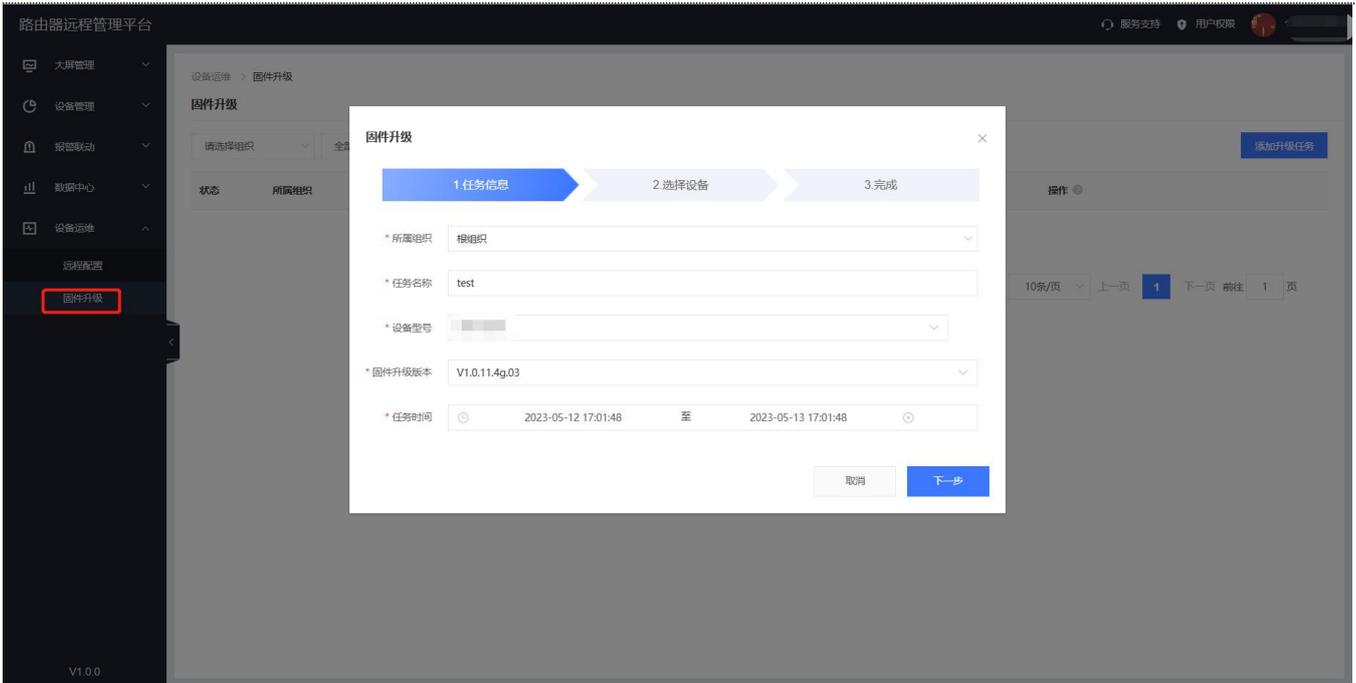


图 103 有人云—固件升级（三）

在“选择设备”里选择需要升级的设备，勾选需要升级的设备后可从界面看到当前版本号以及将要升级版本号。

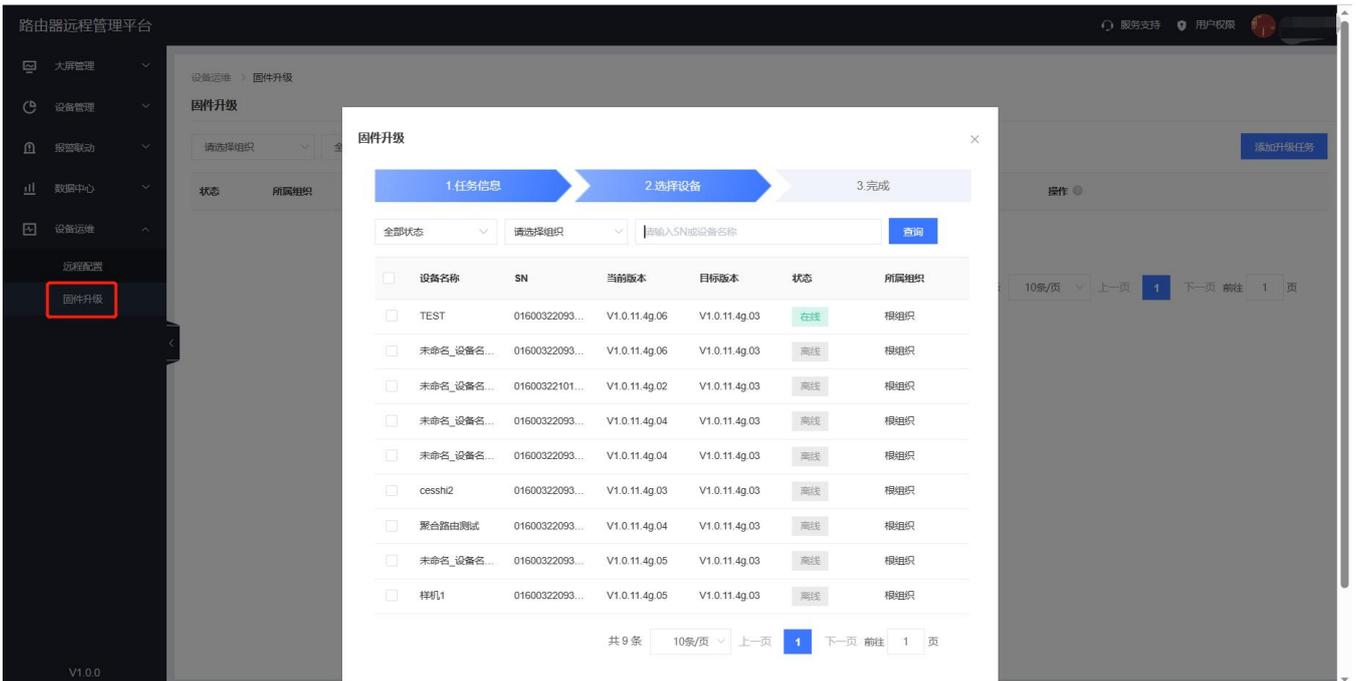


图 104 固件升级（四）

在“升级详情”里面查看当前固件升级进度，并且可以在“查看日志”里面查看详细信息。



图 105 固件升级（五）

7.2. 动态域名解析（DDNS）

DDNS（Dynamic Domain Name Server，动态域名服务）是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。动态域名的使用分为两种情况。

7.2.1. 已支持服务商

第一种，路由器自身支持这种服务商（在“服务提供商”下拉框中查看并选择，这里使用花生壳 ddns.oray.com），设置方法如下：

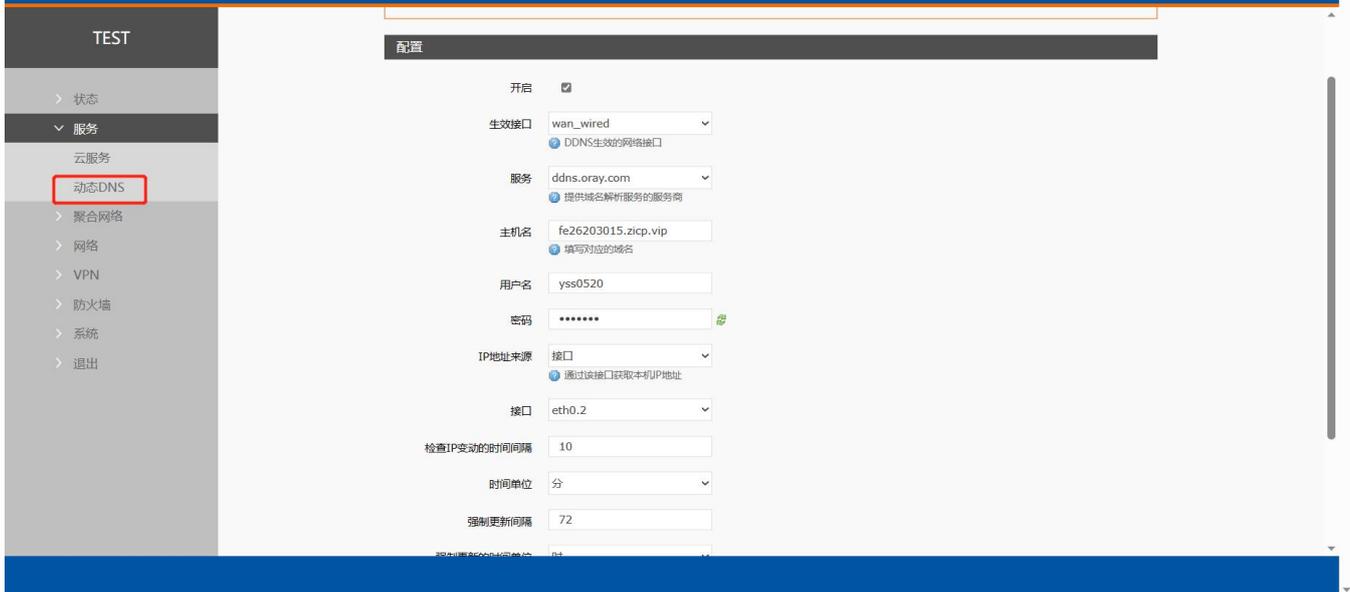


图 106 DDNS 设置页面

表 21 DDNS 参数列表

功能	内容	备注
开启	勾选使能 DDNS 功能	默认不开启，请开启以生效
事件接口	根据需求选择哪个 WAN 口	举例：选择 wan_wired
服务/URL	请填写 DDNS 的服务地址（这里以花生壳为例，服务地址选择 ddns.oray.com）	举例：ddns.oray.com
主机名	请填写您申请号的域名	举例：fe26203015.zicp.vip
用户名	花生壳账户名	举例：yss0520
密码	花生壳密码	举例：*****
IP 地址来源	这里选择接口	选择接口
接口	选择接口名	举例：这里选择 eth0.2 也就是有线 WAN 口
检查 IP 变动的时间间隔 / 时间单位	检测 IP 地址变动的的时间间隔，域名指向的 IP 可能会经常变动，数值越小检测越频繁	举例：1 分钟
强制更新间隔 / 强制更新时间单位	强制更新时间间隔	举例：72 小时

测试申请的域名地址如下。



图 107 DDNS 测试图

7.2.2. 自定义的服务商

第二种情况，路由器自身不支持的 DDNS 服务商（需要在“服务提供商”下拉框中，选择“自定义”，我们这里仍然填写 ddns.oray.com），使用方法如下：

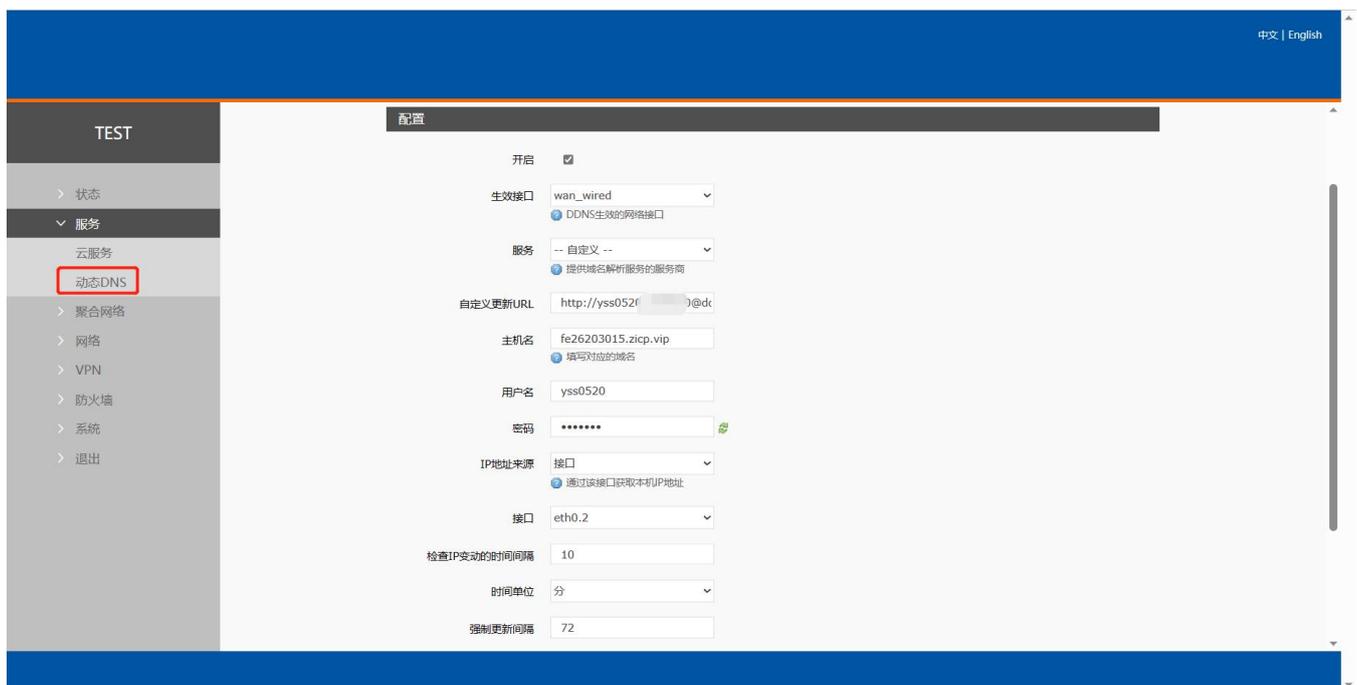


图 108 DDNS 自定义服务参数设置页面

表 22 DDNS 自定义服务参数表

功能	内容	备注
开启	勾选使能 DDNS 功能	默认不开启，请开启以生效
事件接口	根据需求选择哪个 WAN 口	举例：选择 wan_wired
服务/URL	请填写 DDNS 的服务地址（这里以花生壳为例，服务选择自定义），需要以 http://username:password@ddns.oray.com/ph/update?hostname=花生壳的动态域名的格式填写	举例： http://ysss0520:***@ddns.oray.com/ph/update?hostname=fe26203015.zicp.vip

主机名	请填写您申请号的域名	举例: fe26203015.zicp.vip
用户名	花生壳账户名	举例: yss0520
密码	花生壳密码	举例: ***
IP 地址来源	这里选择接口	选择接口
接口	选择接口名	举例: 这里选择 eth0.2, 也就是 WAN 接口
检查 IP 变动的间隔	检测 IP 地址变动的间隔, 域名指向的 IP 可能会经常变动, 数值越小检测越频繁	举例: 1 分钟
强制更新间隔 / 强制更新时间单位	强制更新时间间隔	举例: 72 小时

下面确认 DDNS 设置是否生效（路由器必须重启才可以使设置生效）。首先我们先看一下自己所在网络的公网 IP 地址。



图 109 DDNS 测试图二

然后，我们在 PC 上 ping 域名 1a516r1619.iask.in，可以 ping 通，说明 DDNS 已经生效。



图 110 DDNS 测试图三

<说明>

- 修改设置后，请重启路由器确保生效；
- 请按照表格说明严格填写参数，服务/URL、申请的域名、用户名密码、接口等参数确保正确；
- 即便作为子网下的路由器，本功能也应可以使动态域名生效；
- DDNS + 端口映射可以实现异地访问本路由器内网；
- 如果路由器所在的网络，没有分配到独立的公网 IP，那么本功能无法使用。

8. 免责声明

本文档未授予任何知识产权的许可，并未以明示或暗示，或以禁止发言或其它方式授予任何知识产权许可。除在其产品的销售条款和条件声明的责任之外，我公司概不承担任何其它责任。并且，我公司对本产品的销售和/或使用不作任何明示或暗示的担保，包括对产品的特定用途适用性，适销性或对任何专利权，版权或其它知识产权的侵权责任等均不作担保。本公司可能随时对产品规格及产品描述做出修改，恕不另行通知。

9. 更新历史

说明书版本	更新内容	更新时间
V1.0.0	创立文档，完成相关功能描述	2023-05-12



可信赖的智慧工业物联网伙伴

天猫旗舰店: <https://youren.tmall.com>

京东旗舰店: <https://youren.jd.com>

官方网站: www.usr.cn

技术支持工单: im.usr.cn

战略合作联络: ceo@usr.cn

软件合作联络: console@usr.cn

电话: 4000 255 652

地址: 山东省济南市历下区茂岭山三号路中欧校友产业大厦 12、13 层有人物联网

