有人物联网
www.usr.cn

5G 工业无线路由器
USR-G810

说明书

联网找有人

可信赖的智慧工业物联网伙伴

目录

1.产品简介

USR-G810 是一款支持 NSA 和 SA 双模 5G 网络的 5G 工业路由器，向下兼容 4G/3G 网络制式，组网便捷。产品采用工业级设计，具备多重硬件防护，带有外部看门狗电路，即使在严苛环境下也能稳定运行。多天线设计，有效降低同频干扰，提高数据收发能力；2.4GHz 与 5.8GHz 双频 WiFi，用户可以自行选择连接。

该产品已经在物联网产业链中的 M2M 行业广泛应用，为智慧工厂、智慧医疗、新媒体直播、自动驾驶、智能机器人等领域提供高速率、低时延、广覆盖的传输网络。

1.1. 产品特点

稳定可靠

- 全工业设计，金属外壳，防护等级 IP30；
- 宽电压 DC 9-36V 输入，具备电源反向保护；
- 静电、浪涌、电快速脉冲群等多重防护；
- 内置硬件看门狗，故障自检测、自修复，确保系统稳定。

组网灵活

- 提供高速率、低时延、高稳定的 5G 网络；
- 支持 NSA 和 SA 双模 5G 网络，向下兼容 4G/3G 网络制式；
- 配备 4 个千兆以太网口，提供高速连接能力；
- 6 根高增益天线科学布局，有效降低同频干扰，稳定收发数据；
- 支持自动检网、5G/4G/3G 制式切换、支持 APN/VPDN 专网卡；
- 支持有线/5G 多网同时在线、多网智能切换备份功能；
- 支持 2.4GHz 与 5.8GHz 双频 WiFi，自行选择网络连接；
- 支持 VPN（PPTP、L2TP、IPSec、OpenVPN、GRE），并支持 VPN 加密功能。

功能强大

- 支持多种 WAN 连接方式，包括静态 IP、DHCP、PPPoE、3G/4G/5G；
- 支持花生壳内网穿透、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；
- 支持远程升级、远程监控，轻松实现设备远程运维；
- 支持 NTP、支持一键恢复出厂设置；
- 支持 LED 状态监测(PWR、WLAN、NET、SIG),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

USR-G810 路由器的技术参数如下。

5G 千兆工业无线路由器 USR-G810		
无线参数	无线模块	工业级无线模块
	标准及频段	5G NR:n1、n28、n41、n77、n78、n79 LTE:B1、B2、B3、B5、B7、B8、B34、B39、B40、B41 WCDMA：B1、B2、B5、B8
	理论带宽	5G NR:最大上行速率 900Mbp，最大下行速率 2Gbps LTE CAT12：最大上行峰值速率 90.4Mbps ，最大下行峰值速率 600Mbps HSPA+:最大上行速率 5.76Mbps ,最大下行速率 42Mbps
	发射功率	Class 3 (23dBm±1dB)

WiFi 无线参数	标准及频段	支持 IEEE802.11b/g/n，2.4GHz，支持 AP 模式 支持 IEEE802.11ac，5.8GHz，支持 AP 模式
	理论带宽	2.4G:最高速率 300Mbps 5.8G:最高速率 867Mbps
	认证类型	支持 WPA-PSK、WPA2-PSK、MPA3-PSK 认证方式。
	安全加密	支持 TKIP、AES 加密算法
	传输距离	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）
接口类型	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
	指示灯	具有“PWR、WLAN、NET、SIG”四个指示灯
	天线接口	蜂窝：6 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)
	SIM 卡接口	标准 6 针抽屉式卡接口，支持 3V/1.8V SIM 卡，具备 15KV ESD 防护
	电源接口	标准 5.5*2.1 火车头电源座+2P 端子电源，具备电源反向保护
	Reload 按钮	长按 5s 以上松开，恢复出厂设置
	TBD 串口	用于调试和刷机。
供电	标准电源	DC 12V/2A
	供电范围	DC 9 - 36V
	工作电流	平均 524mA，最大 637mA/12V
物理特性	外壳	金属外壳，防护等级 IP30
	尺寸	200.0*140.0*35.0 (L*W*H，不含天线座和安装件)

	EMC 等级	EMC 4 级
其他参数	工作温度	-20℃～+70℃
	存储温度	-40℃～+125℃
	工作湿度	5%～95%RH（无凝露）
	存储湿度	1%～95%RH（无凝露）

功耗参数

数值均在全速工作情况下测试得出，1 个 WiFi 从站接入，1 个 LAN 口接入，5G 访问外网的数据传输速率。

表 1 USR-G810 功耗表

工作方式	供电电压	平均电流（mA）	最大工作电流（mA）	最小工作电流（mA）
LAN+WAN 全速通信（5G 正常+WLAN 正常）	DC12V	524.054	636.746	399.831
单独 LAN 口全速通信（5G 正常+WLAN 正常）	DC12V	512.729	621.289	393.333
LAN+WAN 全速通信（5G 无卡+WLAN 正常）	DC12V	422.714	578.728	288.474
单独 WAN 口全速通信（5G 无卡+WLAN 正常）	DC12V	342.644	505.063	257.435

G810 在 12V 供电并全速工作时，统计得出：

平均功耗 6.3W，最大工作功耗 7.6W。平均电流 524mA，最大工作电流 636.7mA。

注意

- 推荐使用出厂配套的电源适配器。如需自行配置电源，可详询技术工程师相关功耗参数。

1.3. 状态指示灯

共有 4 个状态指示灯，含义如下

表 2 指示灯说明表

名称	说明
PWR	电源指示灯，上电后长亮，显示红色
WLAN	WiFi 灯，WiFi 正常工作时亮起，显示绿色
NET	连接到网络后，NET 灯亮起。红色代表 3G，橙色代表 4G，绿色代表 5G
SIG	信号指示灯，注网后指示灯亮起，红色、橙色、绿色信号由弱到强

1.4. 安装尺寸

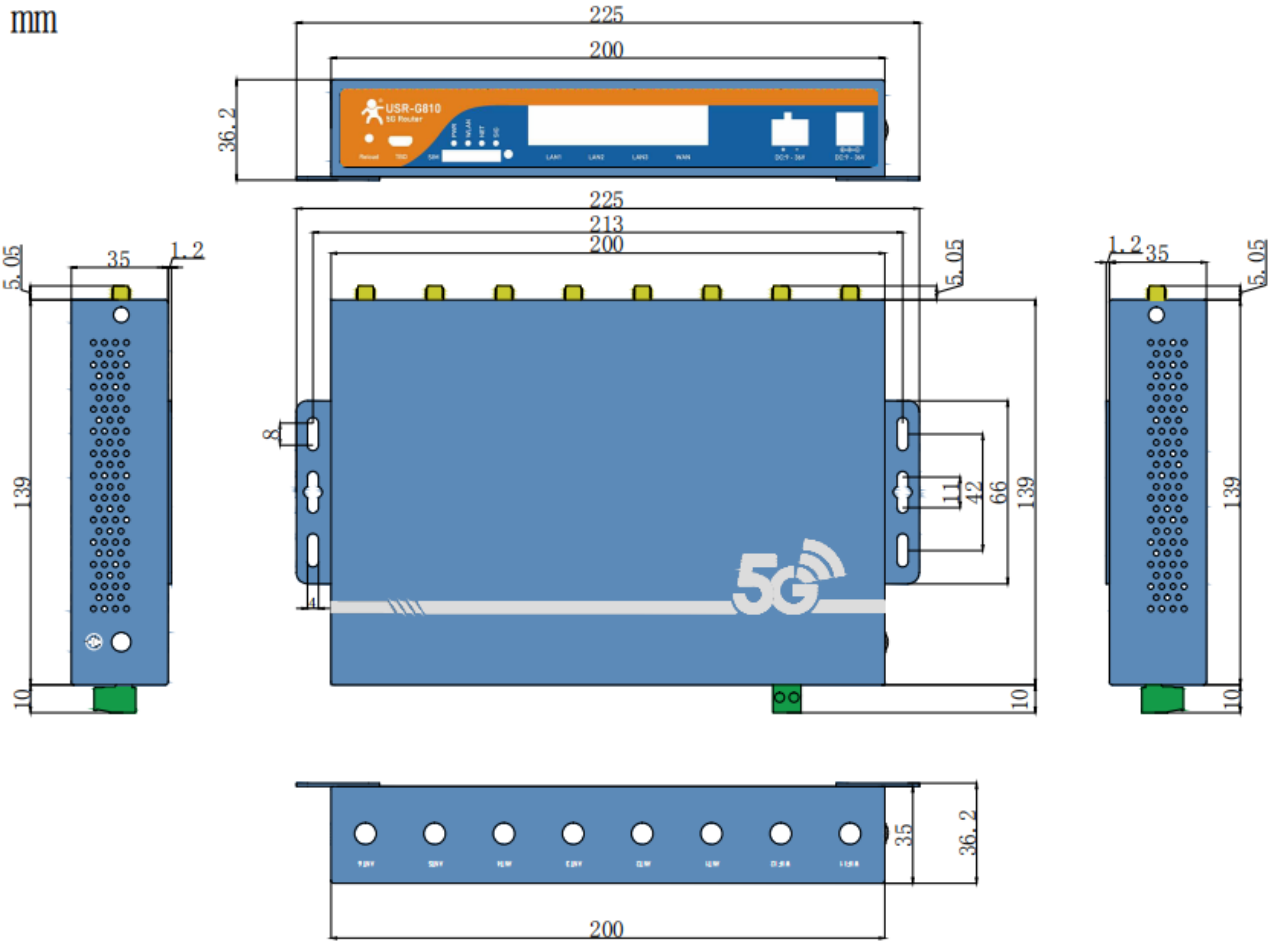


图 1 USR-G810 尺寸图

注意：

- 钣金外壳，两侧固定孔，兼容导轨安装件
- 产品尺寸：200.0*140.0*35.0mm（L*W*H，不含安装件、电源端子及天线座）
- 固定开孔尺寸：213.0*42.0mm(L*W)

2.系统基本功能

本章介绍一下 USR-G810 所具有的功能，下图是产品功能的整体框图。

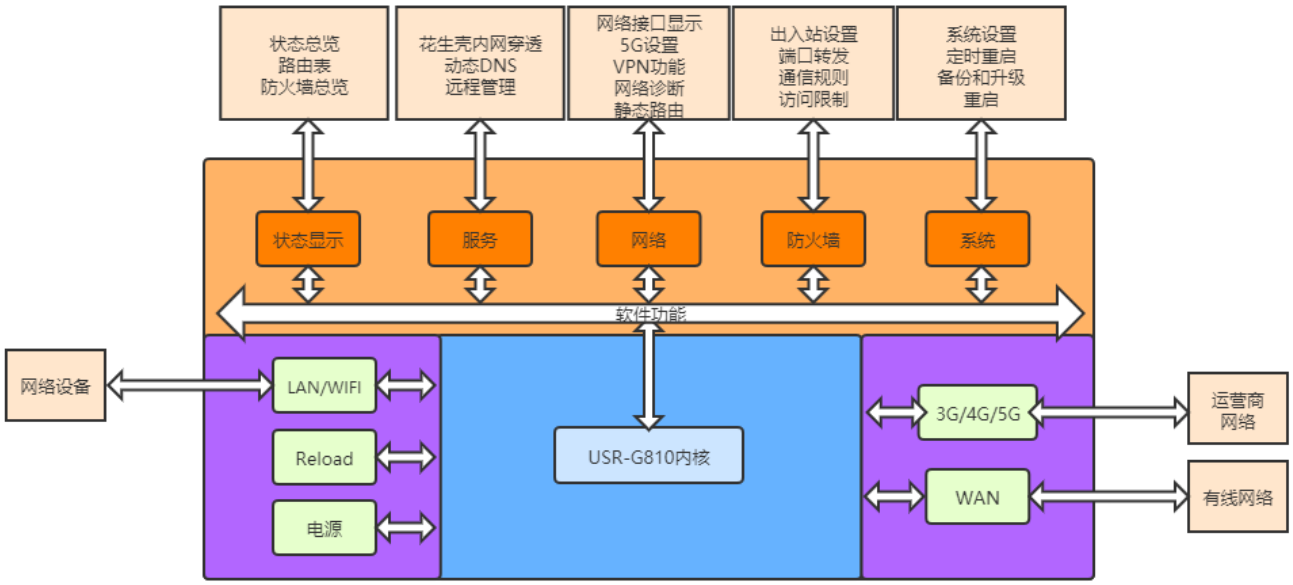


图 2 功能框图

接口对照表：

表 3　　接口对照表

网卡名称	网卡代号	对应的网络接口名称
有线 LAN 口	br-lan	LAN
5G 接口	eth1.2	WAN_5G
有线 WAN 口	eth1.3	WAN_WIRED

2.1. 查询 5G 覆盖

手机浏览器打开 m.speedtest.cn/5g/map，可以观察周围环境是否已经完成 5G 网络覆盖。

本页面显示的蓝色区域为 5G 网络覆盖范围，位置可供参考，具体情况需视当地基站状态。

图 3 Speedtest.cn 查询网络覆盖情况

2.2. Web 页面设置

使用 USR-G810 时，可以通过 PC 连接 USR-G810 的 LAN 口，或者连接上 WLAN 无线，然后用 Web 管理页面配置。默认参数如下。

表 4 USR-G810 网络默认设置表

参数	默认设置
SSID	USR-G810-XXXX、USR-G810-XXXX_5G
LAN 口 IP 地址	192.168.1.1
用户名	root
密码	root

无线密码	www.usr.cn

首先操作电脑加入 USR-G810-xxxx（xxxx 为 MAC 地址后四位），无线连接好后，在浏览器地址栏输入 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，管理页面默认中文。

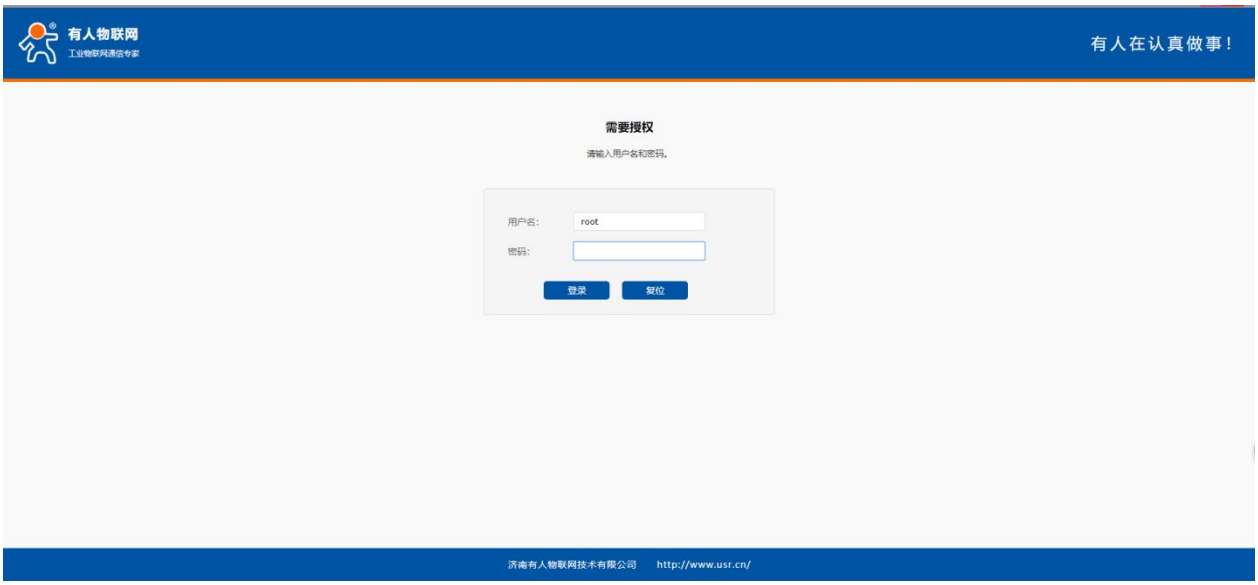


图 4 首页页面

在网页的左边是功能标签页，可以具体设置参数；

- 状态：主要显示设备的名称信息、固件版本、运行状态、当前路由表、防火墙状态等；
- 服务：主要是一些高级功能，包括花生壳内网穿透、动态 DNS、远程管理；
- 网络：设置接口、5G 配置、无线 WIFI、网络诊断、静态路由等信息；
- VPN：搭建 PPTP、L2TP、IPSec、OpenVPN、GRE 的 VPN 网络及查询 VPN 状态；
- 防火墙：设置出入站规则、端口转发、黑名单、白名单等信息；
- 系统：主要是一些基本功能，包括重启、恢复出厂设置、固件升级、本地日志等。

图 5 状态网页

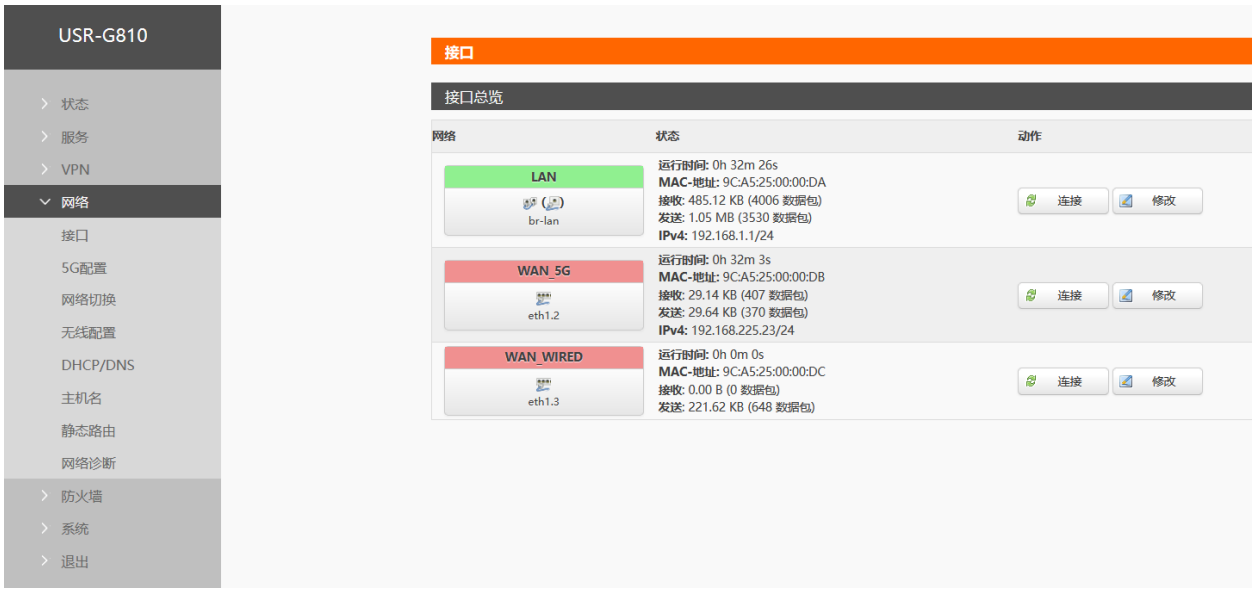


图 6 接口网页

2.3. 主机名与时区

路由器自身主机名默认 USR-G810，时区为北京时区。

图 7 主机名和时区设置页面

2.4. NTP 设置

图 8 NTP 页面

路由器可以进行网络校时，默认启动 NTP 客户端功能。有 NTP 服务器地址设置。

2.5. 用户密码设置

图 9 用户名密码设置页面

默认密码可以设置，默认密码为 root，用户名不可设置。本密码主要用于网页服务器的登录密码。

2.6. 参数备份与上传

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-G810-2020-08-09.tar.gz ，并保存到本地。

参数上传：将参数文件（xxx.tar.gz）上传到路由器内，那么参数文件将会被保存并生效。

图 10　　备份/恢复页面

<注意>

固件恢复配置，仅限在同一版本固件。由于不同版本参数不同会导致问题出现，建议用户在同一版本进行恢复配置。

2.7. 恢复出厂设置

通过网页可以恢复出厂参数设置。点击恢复出厂设置的执行按钮，本功能与硬件的 Reload 按键功能一致。

图 11 恢复出厂页面

通过 Reload 按键（恢复出厂设置按键），可将 G810 路由器恢复到出厂参数。

- 长按 5s 以上然后松开，路由器将自行恢复出厂参数设置并重启
- 重启生效瞬间，所有指示灯都将闪亮 1 次，然后灭掉（电源灯不灭）

2.8. 固件升级

USR-G810 模块支持 web 方式的在线固件升级。

图 12　　升级页面

<说明>

- 固件升级过程会持续 3 分钟，请在 3 分钟之后再次尝试登录网页
- 可以选择是否保留配置，默认不保留参数升级(在不同版本升级时不要保留参数升级)
- 固件升级过程中请不要断电或者拔网线
- 多只路由器组合使用时，需要升级为同一版本最新固件。

2.9. 设备重启

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 90 秒后完全启动成功。

图 13　重启页面

2.10. Log

Log 分为远程日志和本地日志，位于系统-系统功能菜单内。

远程 Log

- 远程 log 服务器：远端 UDP 服务器的 IP 或域名，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 14　远程日志

本地日志

- 内核日志等级：支持调试、信息、注意、警告、错误、关键、告警、紧急，共 8 个等级；按顺序调试最低，紧急最高；应用日志等级：同上；
- 日志（内核、应用、VPN）支持即时查看、清空，支持日志文件导出。遇到应用问题时，在不断电前提下，进入该页面，先点击“生成日志”，再点击“下载日志”导出 Log,以进行问题分析排查。

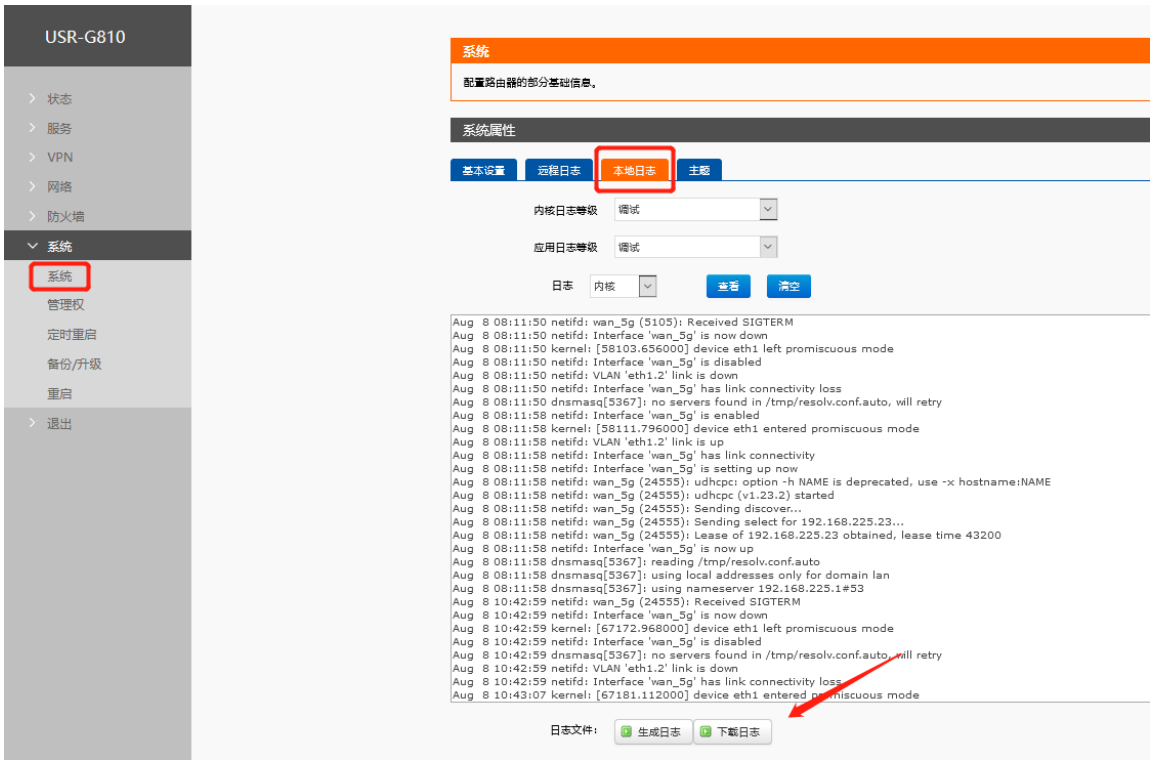


图 15　　生成日志后下载日志

2.11. 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，提高路由器使用稳定性。页面设置如下。

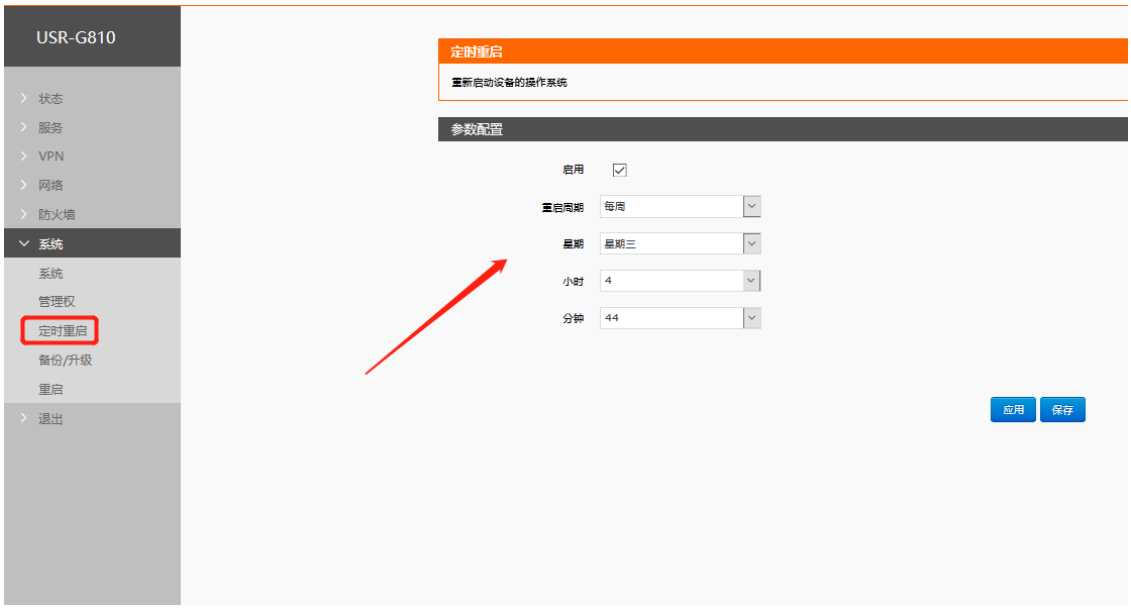


图 16　　定时重启设置页面

3. 网络配置

进入网络--接口界面，可以查看路由器网卡的接口总览，包括网卡运行状态、MAC 地址、IP 地址、收发数据包个数，也可以从该处对 WAN 口、LAN 口、5G 接口进行修改或者重连。

图 17　　网络接口总览

3.1. WAN 接口

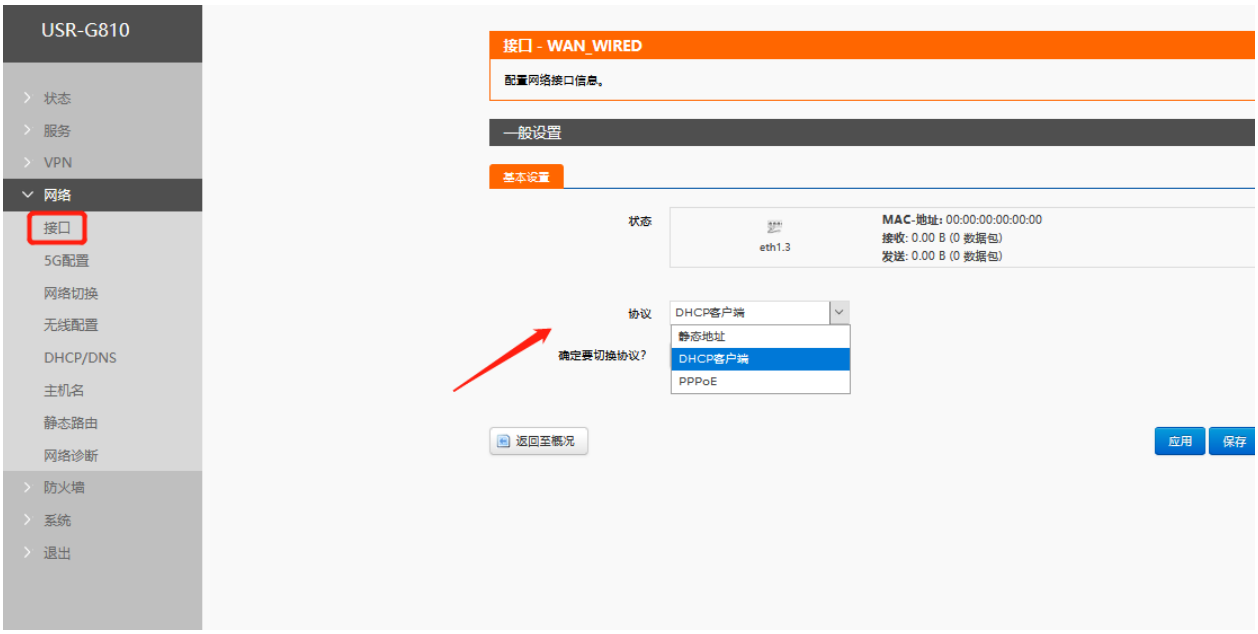


图 18　　WAN 口设置页面

<说明>

- 有线 WAN 口：支持 DHCP 客户端、静态 IP、PPPoE 协议。默认 IP 获取方式为 DHCP 客户端
- WAN 接口-物理设置配置不可随意配置；如若误配导致 WAN 接口不可使用请还原出厂时 WAN 配置。

3.2. LAN 接口

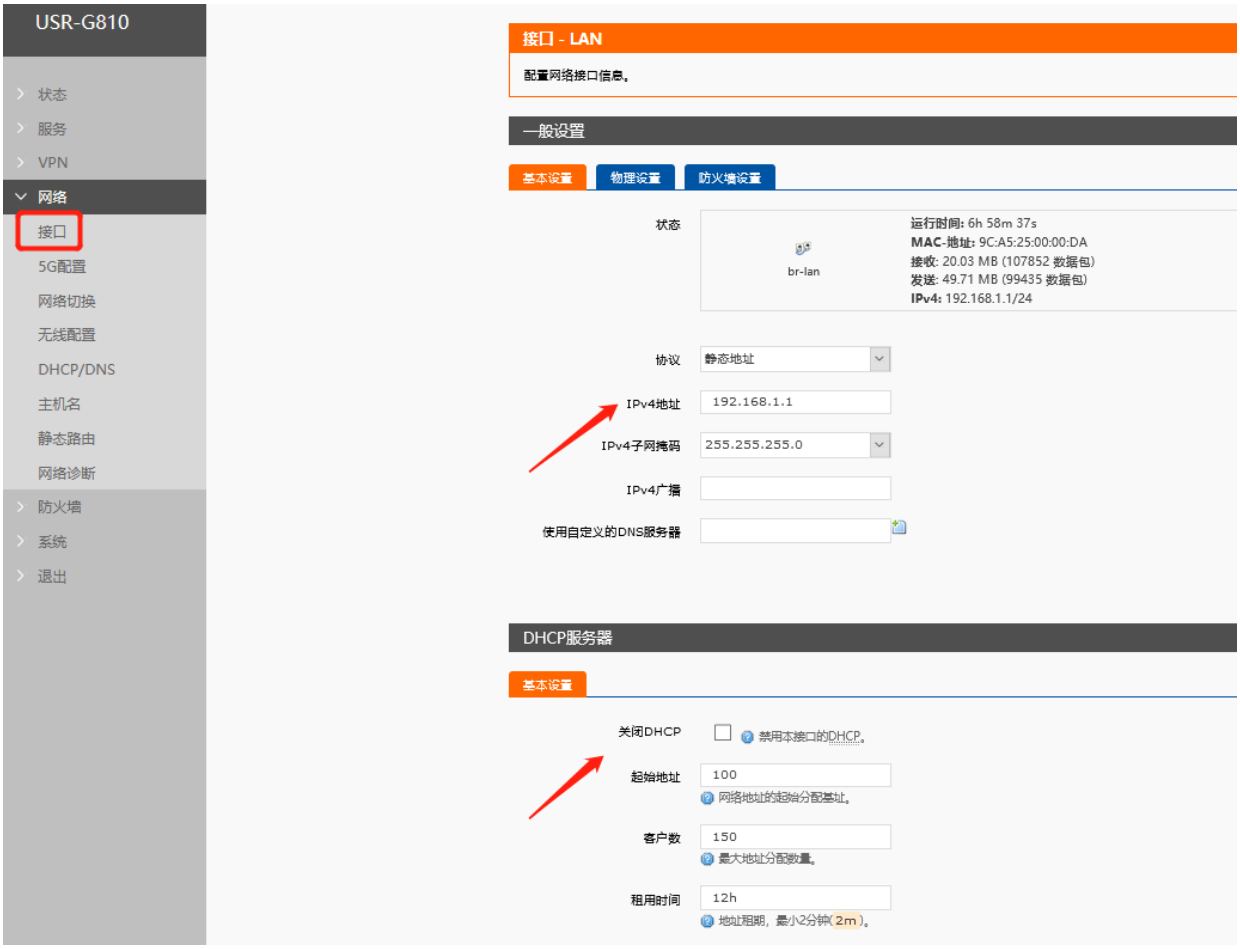


图 19　　LAN 口设置页面

<说明>

- 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（下次登陆路由器即使用该地址）
- WiFi 接口（WLAN）与有线 LAN 口同属 LAN 网络
- 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
- 可以调整 DHCP 池的开始与结束地址，以及地址租用时间。

- DHCP 默认分配范围从 192.168.1.100 ~ 192.168.1.250。默认租期 12 小时；
- LAN 接口-物理设置配置不可随意配置，如若误配导致 LAN 接口不可使用请还原出厂时 LAN 配置

3.3. 5G 配置

本路由器支持一路 5G/4G/3G 通信模块接口，用来访问外部网络。

图 20　　5G 接口页面

表 5　　状态表

序号	名称	含义
1	运行时间	本接口获取网络后的连接时间，无网络则不显示。
2	MAC 地址	本网卡接口的 MAC 地址
3	接收/发送	本网卡自从连接成功后累计的接收与发送数据统计
4	IPv4	代表本网卡使用 IPv4 协议

3.3.1. 5G 配置

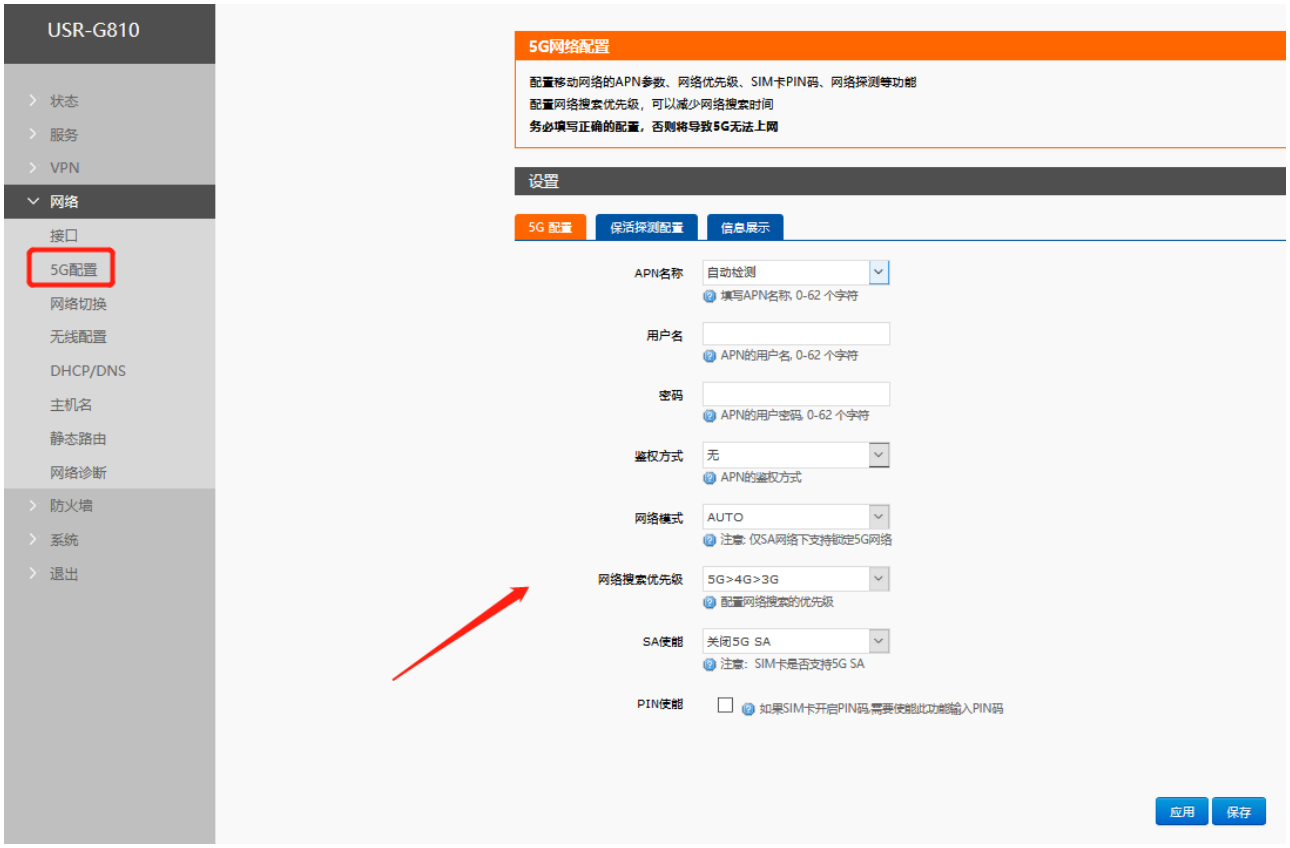


图 21　5G 配置页面

如果您使用的是普通手机卡，APN 设置无需关心，插卡即可联网。

如果您使用了 APN 卡，有特殊的 APN 地址，则需要在此处设置 APN 地址，用户名跟密码。

表 6　APN 参数表

参数名称	功能
APN 地址	请填写正确的 APN 地址。
用户名	默认为空。如使用 APN 卡请正确填写
密码	默认为空。如使用 APN 卡请正确填写
鉴权方式	APN 的鉴权方式，根据实际卡类别选择
网络模式	默认为自动。可强制锁定 5G、4G、3G 网络。

网络搜索优先级	默认 5G 优先。可以自行选择搜网顺序。
SA 使能	默认关闭 5G SA。若 SIM 卡不支持 SA 网络，禁止打开。
PIN 使能	默认未开启。如需开启，则需要输入 SIM 卡的 PIN 码。

<说明>

- 如果您使用的是普通手机卡，APN 设置无需关心，插卡即可联网。
- 如果您使用了 APN 卡，有特殊的 APN 地址，则需要在此处设置 APN 地址、用户名、密码。

3.3.2. 保活探测配置

保活探测配置，用于检测网络连接状态，默认关闭状态。开启网络探测功能，设备会每隔设定的时间去连接指定的探测地址，当失败次数达到设定次数下，会重新进行拨号。

由于基站会定时踢掉空载的设备，若用户使用过程中经常会长时间不传输数据，为避免被基站踢掉，建议开启网络探测。

图 22　保活探测配置

3.3.3. 信息显示

信息展示会详细得显示出 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。

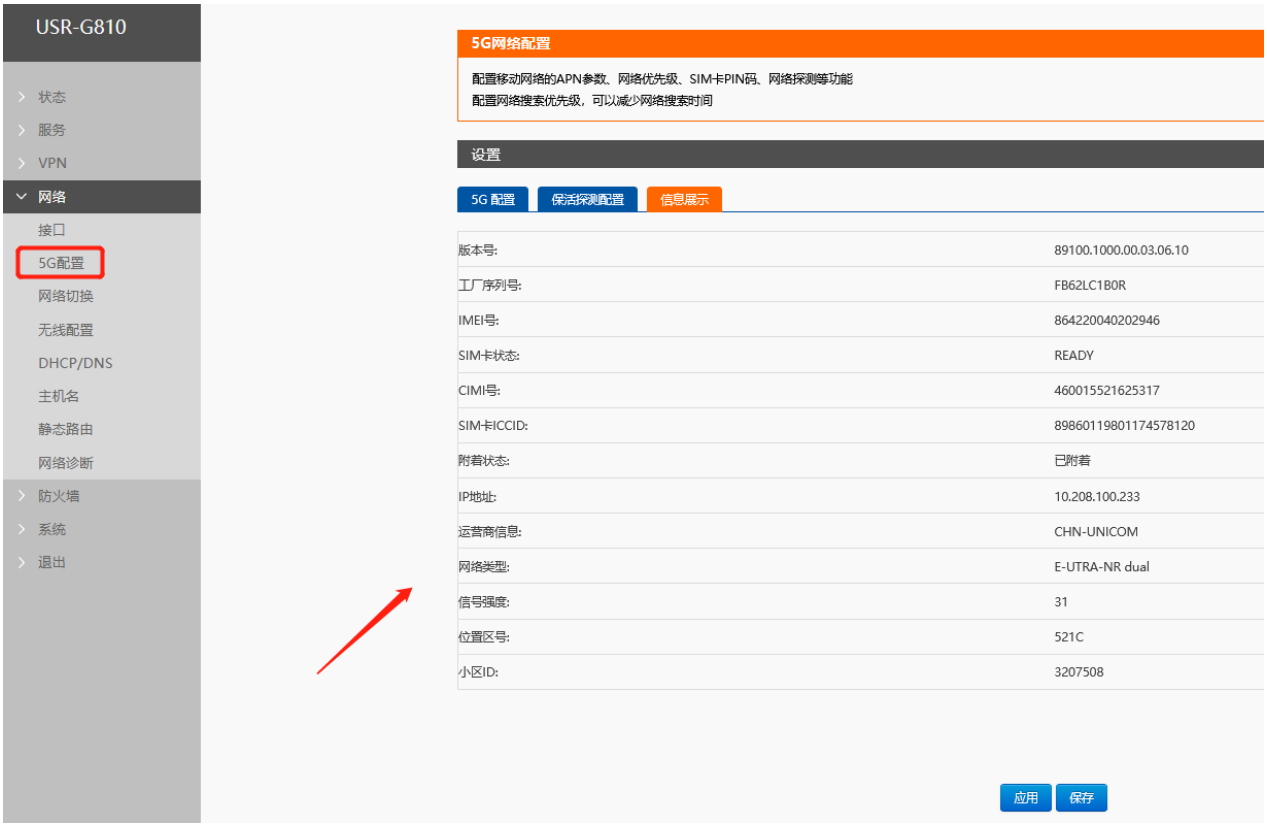


图 23　SIM 卡信息显示

<说明>

- 信号强度，常用有两个表示单位：dBm 和 asu。其换算关系是 dBm =-113+2*asu
- USR-G810 使用 asu 值表示；asu 的范围为 1-31，数值越大，信号强度越好；
- 注册到不同的网络制式或者小区 ID，信号强度的表示值无论是 dBm 还是 asu，都无法直接对比。
- 一般情况下，dBm≥-90dBm，asu≥12，信号强度满足覆盖要求，可以据此衡量当前信号是否达标。

3.4. 网络切换规则

配置网络优先级检测规则，默认启用，默认切网顺序：5G 网络优先，可设置有线网络优先；

设定 3 组检测联网状态的 IP 地址（也可以设定域名），依次进行 ping 包，如能够 ping 通，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 5G 网络、有线网络均无法 ping 通，则判断路由器无法连接外网。

图 24　　网络切换配置

3.5. DHCP/DNS

静态地址分配：在网络-DHCP/DNS 处设置。该功能是 LAN 接口 DHCP 设置的延申，用于给 DHCP 客户端分配固定的 IP 地址和主机标识。

使用添加来增加新的规则。在本功能下可以设定 MAC 和 IP 地址的绑定（最多可添加 20 条），以此实现固定 MAC 在 DHCP 下分配到指定 IP 的目的。

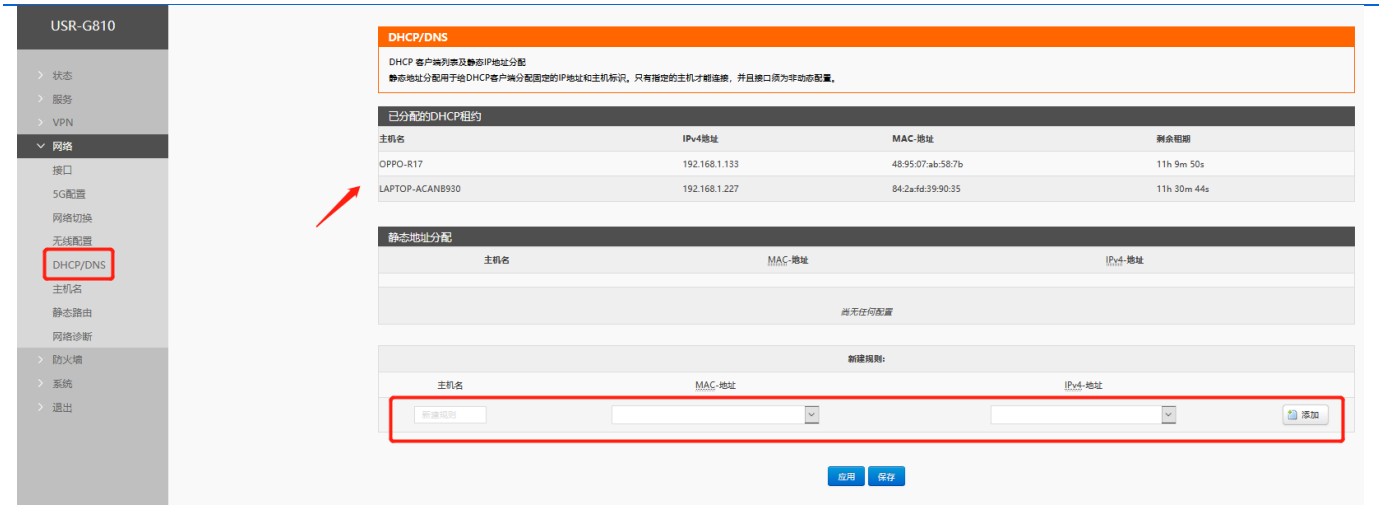


图 25　　DHCP/DNS 设置页面

3.6. 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。

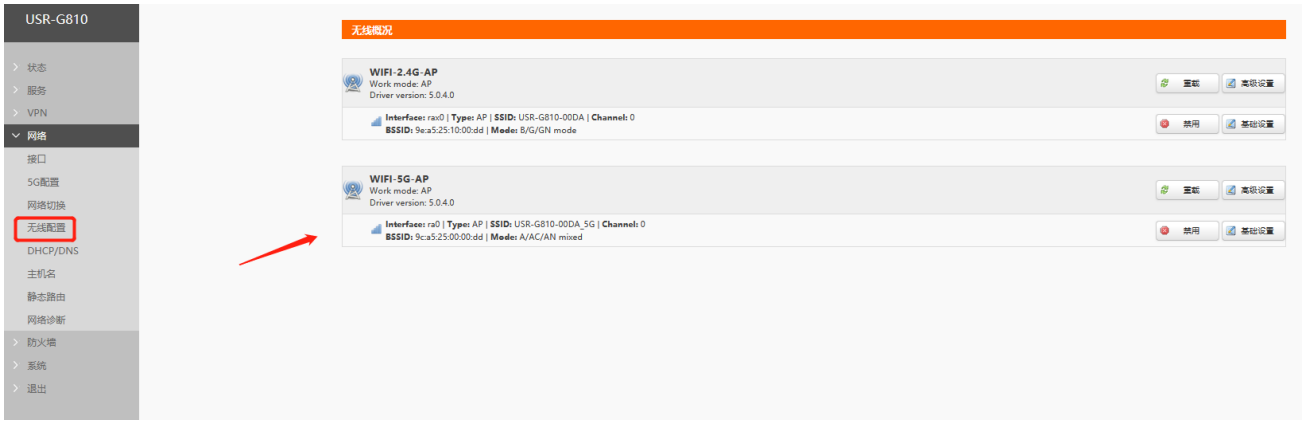


图 26　　无线配置界面

<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

表 7　　无线 WiFi 默认参数

默认参数	数值
SSID 名称	USR-G810-XXXX、USR-G810-XXXX_5G （最后为 MAC 地址后 4 位）
无线密码	www.usr.cn
信道	Auto
加密方式	WPA2-PSK

在“无线配置→WiFi-2.4G-AP（WiFi-5G-AP）→基本设置”修改 SSID 和无线密码。

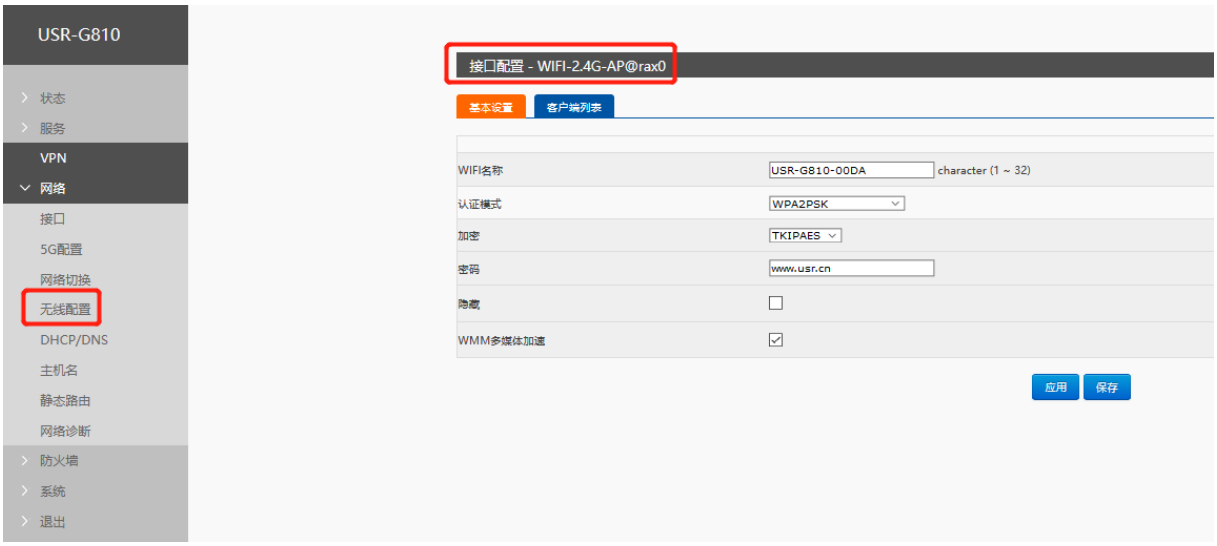


图 27　　无线-SSID 设置页面

在“无线配置→WiFi-2.4G-AP（WiFi-5G-AP）→基本设置”查看客户端的接入信息。

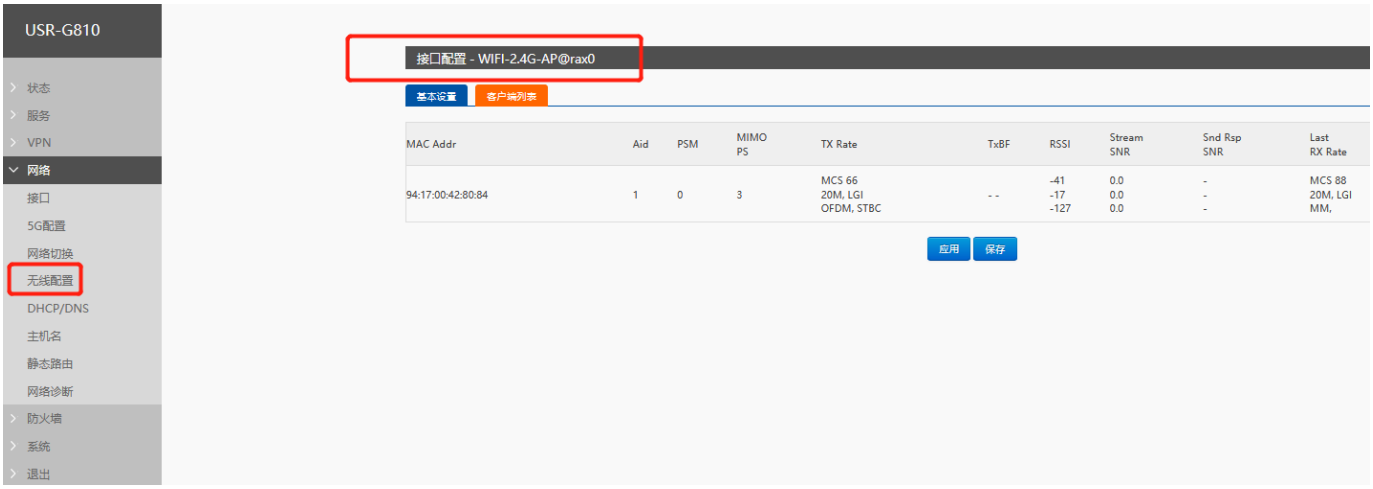


图 28　　无线-客户端列表

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 29　　无线-信道设置页面

3.7. 主机名功能

路由器可以实现自定义的域名解析。将你想要填写的主机名（域名），比如“usr-pc-linux”设置为主机名，对应的 ip 地址 192.168.0.9。这样就可以实现主机名到 IP 地址的映射关系。

注意：对应的 IP 地址外网地址也可以实现映射（需为唯一的公网地址）。该功能需重启生效。DHCP/静态地址的主机名不支持仅填写数字。

图 30　　主机名设置页面

图 31　　主机名 PING 功能

3.8. 网络诊断功能

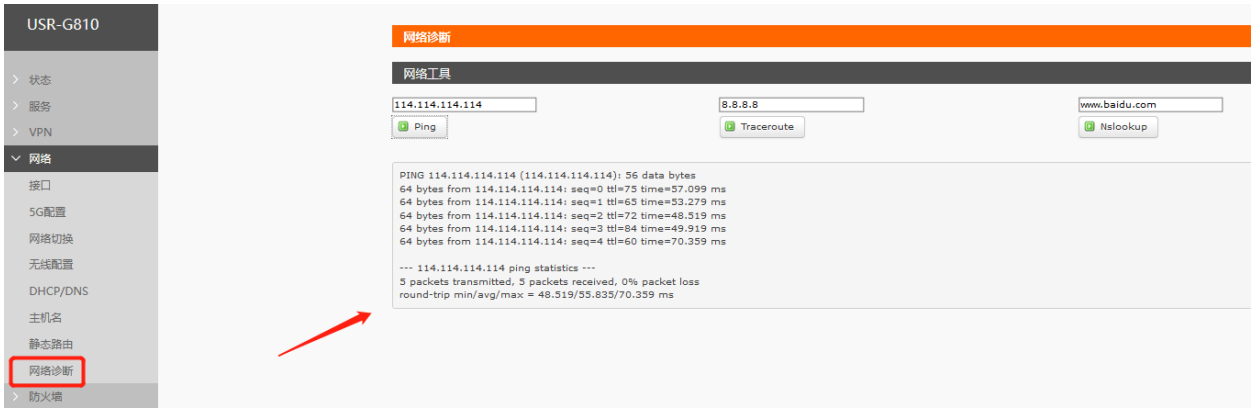


图 32　　网络诊断页面

路由器的在线诊断功能，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。

3.9. 静态路由

静态路由有如下几个参数。默认静态路由最多可添加 20 条。

表 8　　静态路由参数表

名字	含义	备注

接口	路由规则执行的端口	lan、wan_5G、wan_wired
对象（目标地址）	要访问的对象的地址或地址范围	192.168.1.0
子网掩码	要访问的对象网络的子网掩码	255.255.255.0
网关（下一跳）	要转发到的地址	192.168.0.202
跃点数（Metric）	包跳跃个数	根据实际情况填写

静态路由描述了以太网上数据包的路由规则。

- 静态路由使用举例

测试环境，两个平级路由器 A 和 B，如下图。

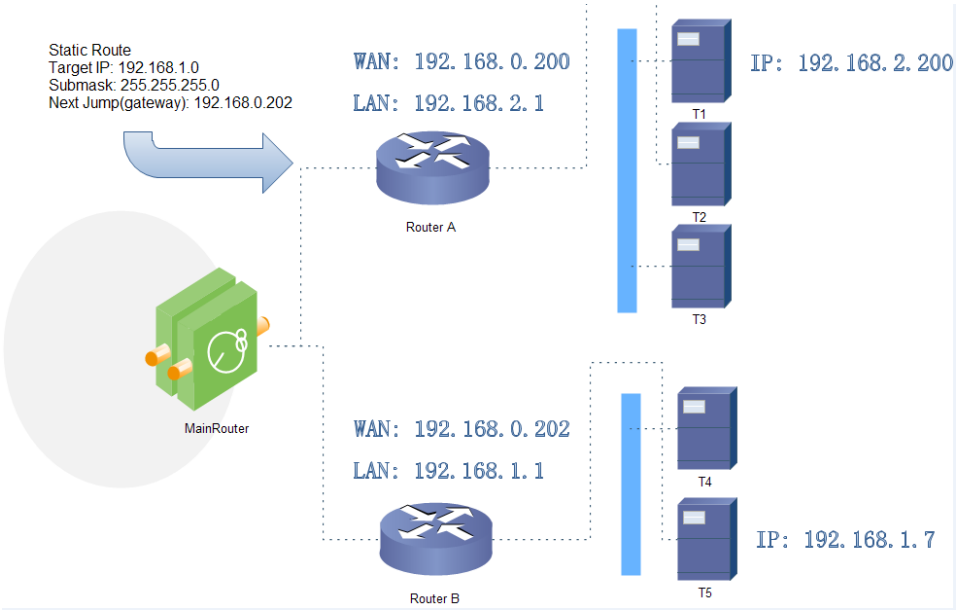


图 33　静态路由表实例图

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。

先在路由器 A 上设置静态路由

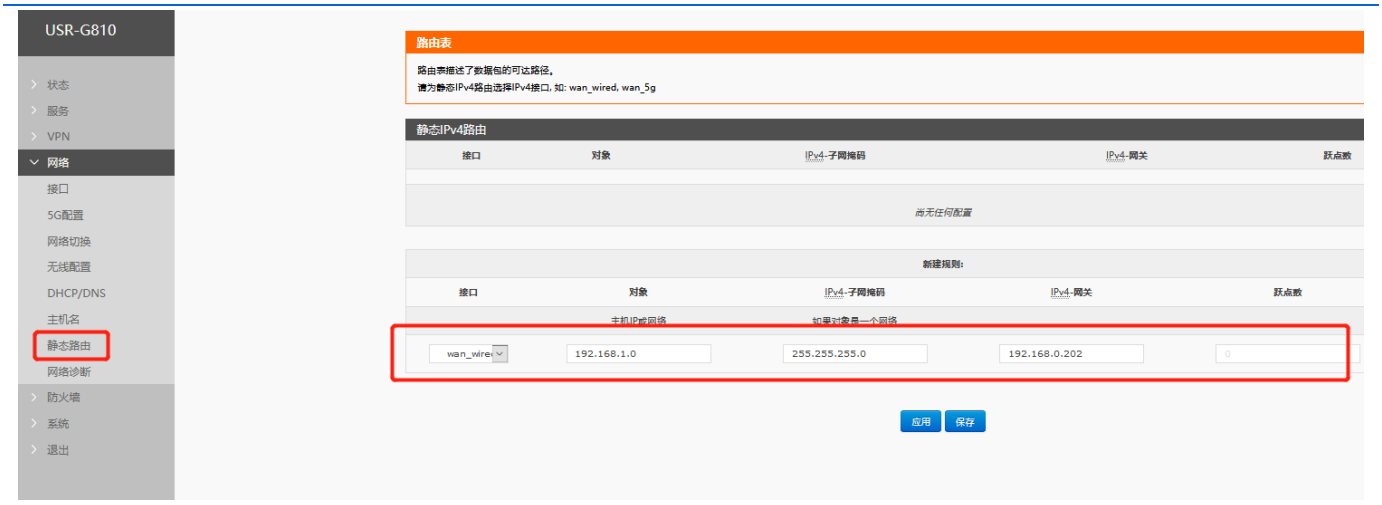


图 34　　路由表添加页面

在 T1（我们用一台 PC 做 T1），用 ping 命令去访问 192.168.1.1（也就是路由器 B 的 LAN 口 IP），

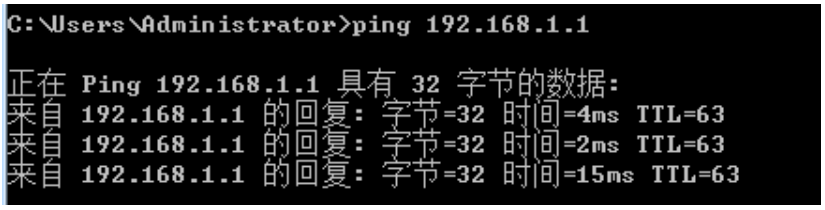


图 35　　路由表功能测试

可以看到，静态路由已经生效，不然是无法从 T1 处访问到路由器 B 的 LAN 口。

4.VPN 功能

VPN（Virtual Private Network）虚拟专用网，分 Client 与 Server，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 支持隧道密码认证、CHAP 等多种认证方式，加密方式支持 MPPE 加密和 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）的数据报进行封装，使这些被封装的数据报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	V2.3.18

4.1. PPTP Client 搭建

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

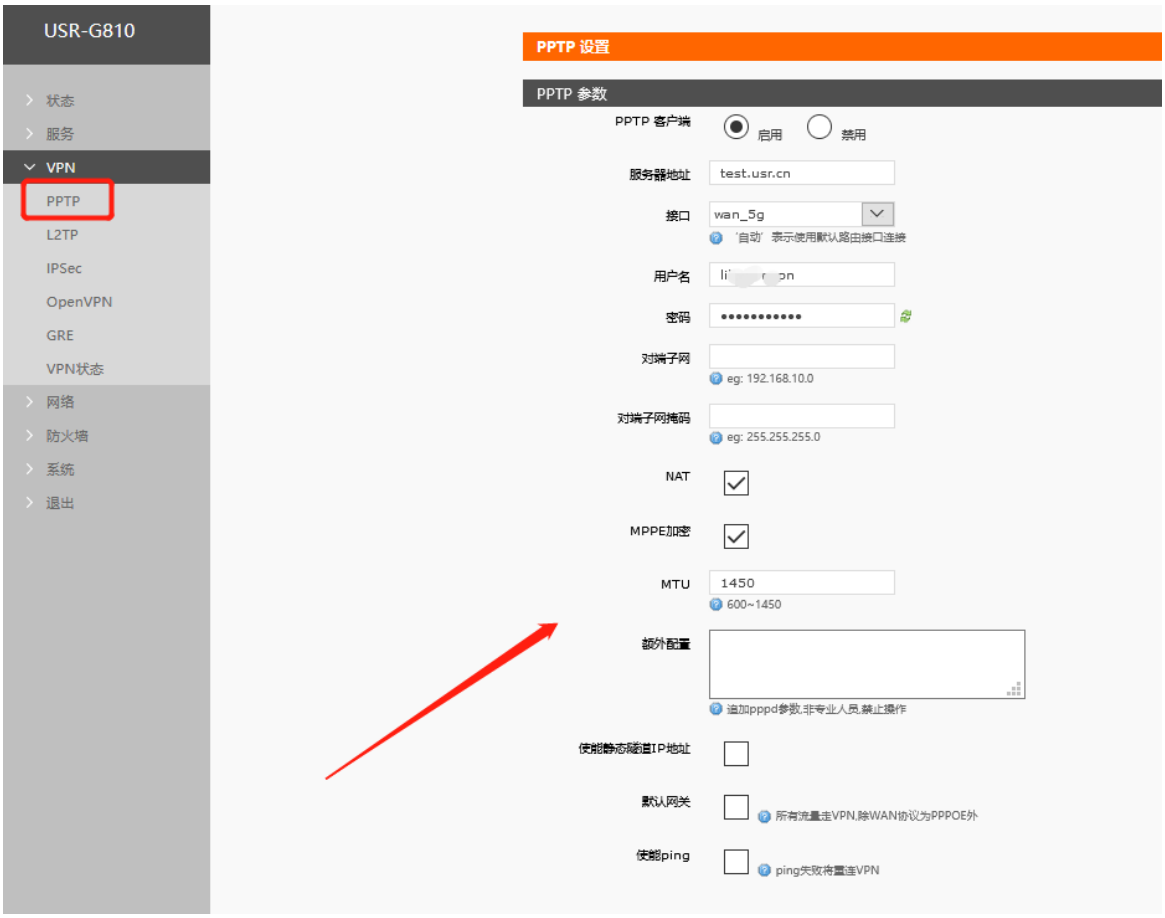


图 36　路由器添加 VPN 操作图一

<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_5g、wan_wired、自动；
- 用户名/密码：从 VPN 服务器处获取。该两处设置可以为空。
- 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 37　　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。

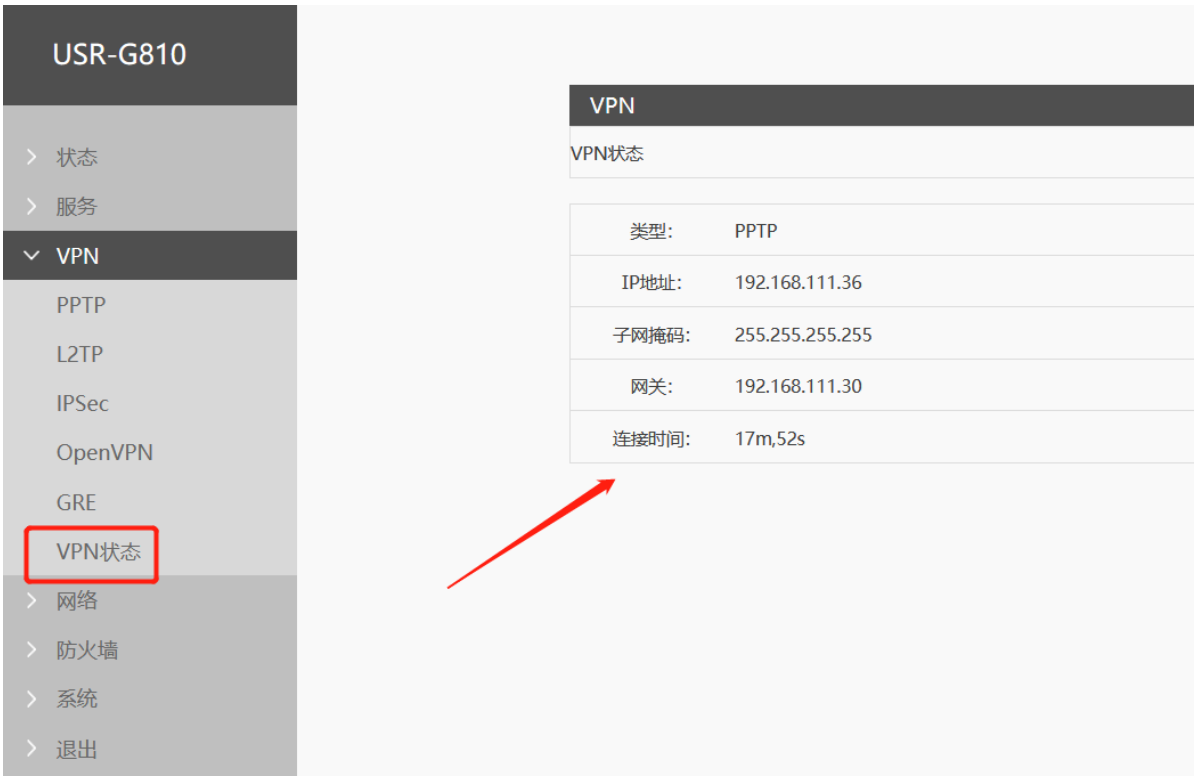


图 38　路由器 VPN 连接状态

4.2. L2TP Client 搭建

L2TP 是第二层隧道协议,与 PPTP 类似。目前 G810 支持隧道密码认证,支持 MPPE 的加密方式和 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

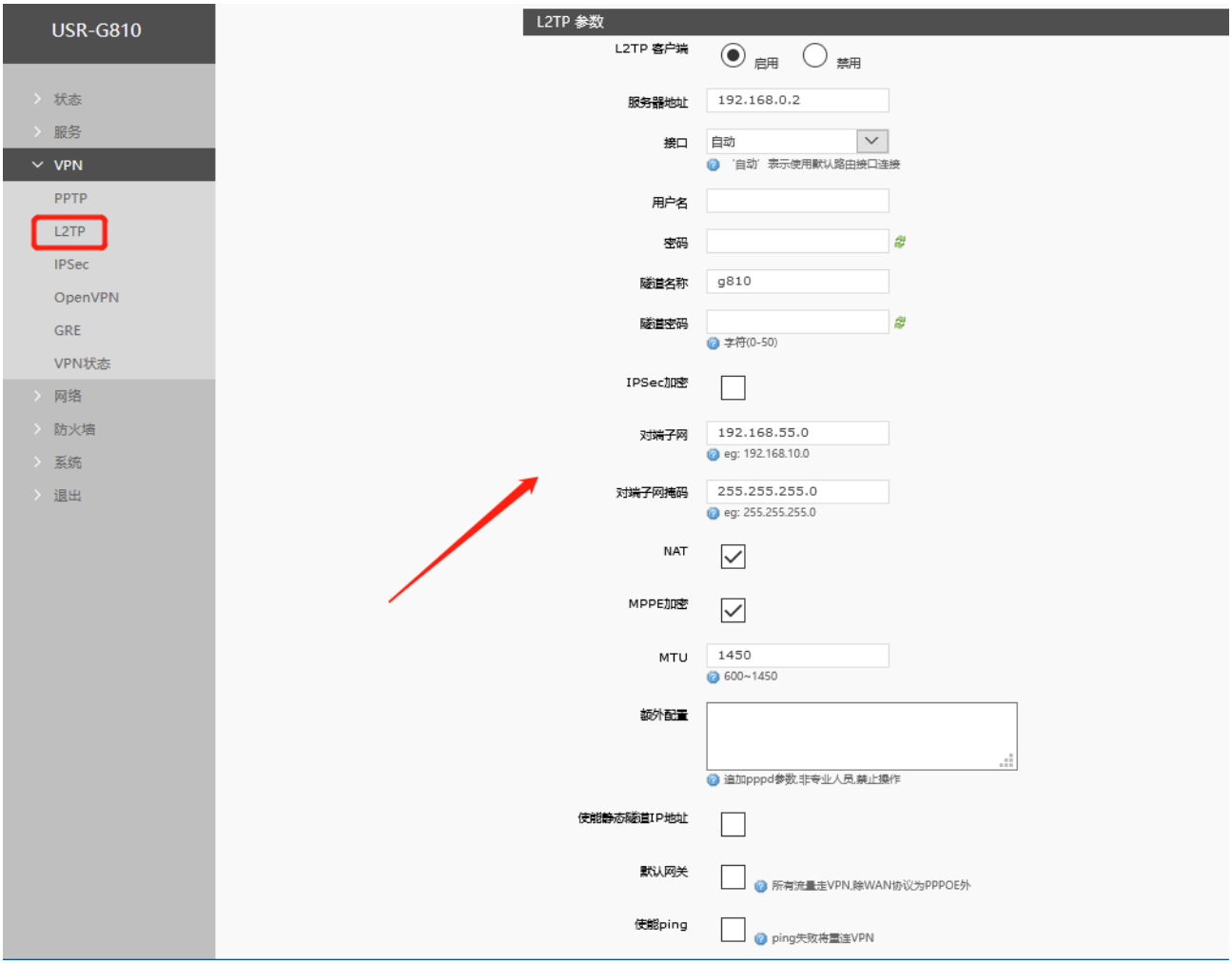


图 39　L2TP 客户端启用设置界面

<说明>

- L2TP 支持隧道密码认证、MPPE 加密、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_5g、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、MPPE 加密、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。

4.3. IPSec 搭建

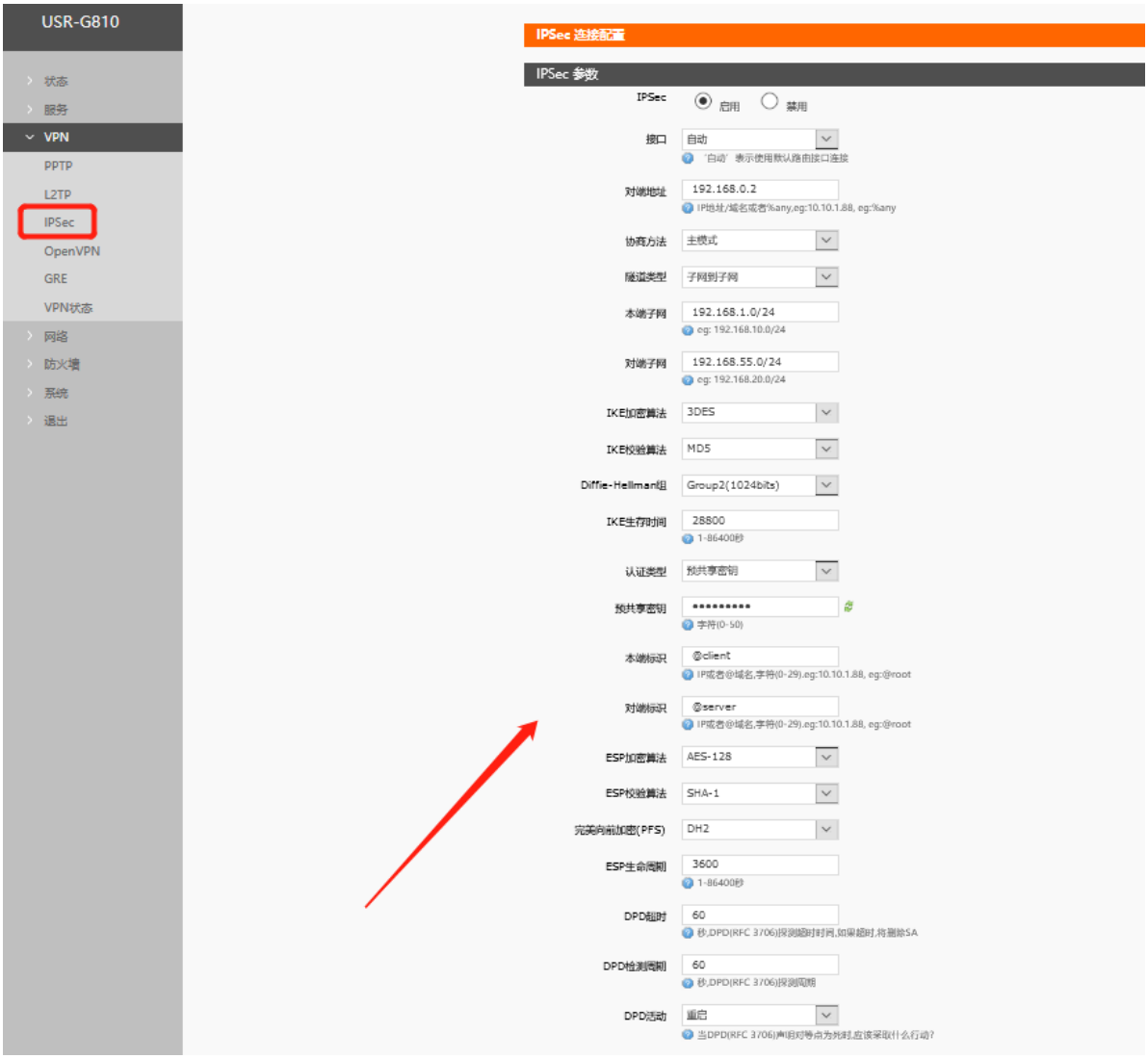


图 40　　IPSec 启用后基本设置

<说明>

- 接口：根据联网方式的不同可选择 wan_5g、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。
- 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
- 会话密钥向前加密(PFS)：提供不启用、DH1、DH2、DH5 共 4 个选项。本项设置需保证本段和对端一致。
- 启动 DPD 检测：是否启用该功能，打钩表示启用。
- 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。

4.3.1. 子网对子网模式

该应用一般两个不同地域间相互通信，例如总公司在济南，分公司在深圳，想实现济南的子网和深圳的子网之间通信，即可用该方式。

测试环境：以 1 号 USR-806 作为 IPSec Server，2 号 USR-G810 作为 IPSec client，以如下参数进行设置。

类别	VPN 服务器	VPN 客户端

设备	USR-G806（对端）	USR-G810（本端）
WAN 口 IP	172.16.14.4	172.16.14.171
LAN 口 IP	192.168.12.1	192.168.1.1
子网下的 PC IP	192.168.12.235	192.168.1.141

1 号 USB-G806 作为 IPSec server，设置界面如下。

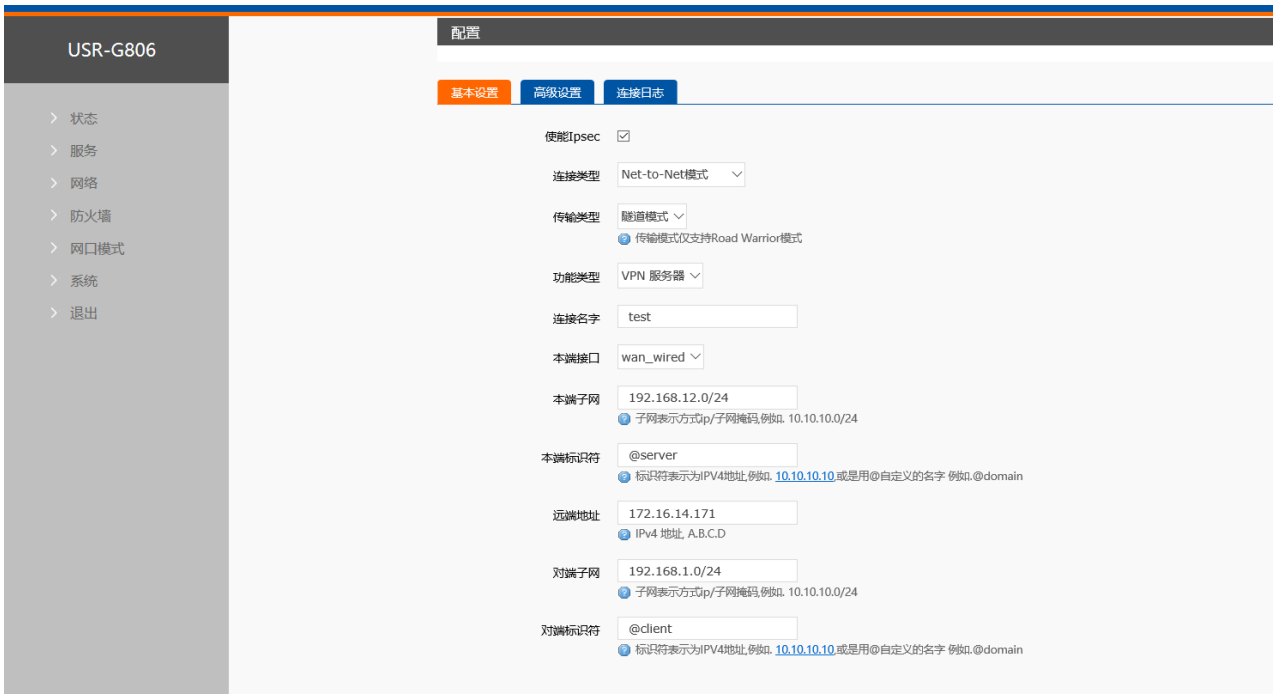
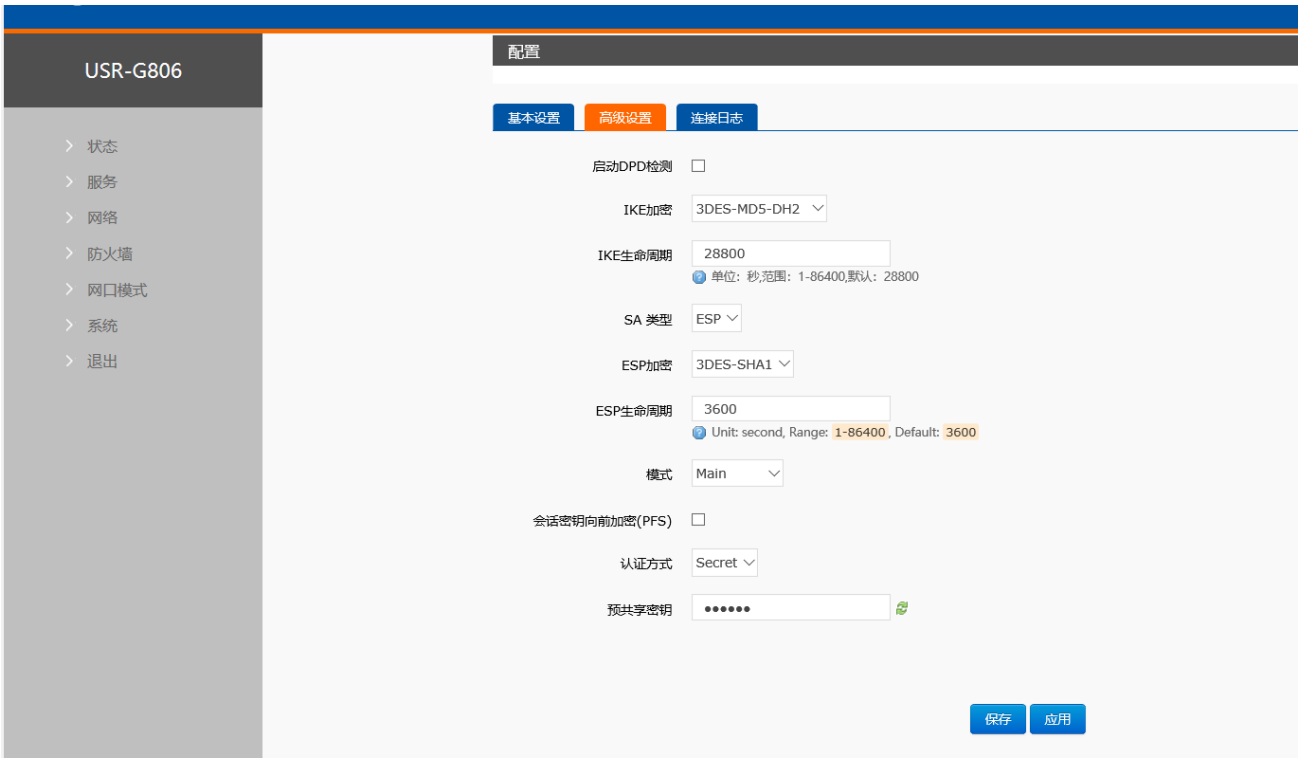


图 41　　IPSec 测试配置举例



2

2 号 USR-G810 作为 IPSec client，设置界面如下。IPSec 测试配置举例

图 42　IPSec 测试配置举例 3

图 43　　IPSec 测试配置举例 4

测试结果：在 VPN 状态处可查看到“IPSec 已连接”提示。此时互相 ping 对端子网也是连通状态。

图 44　　IPSec 测试配置举例 5

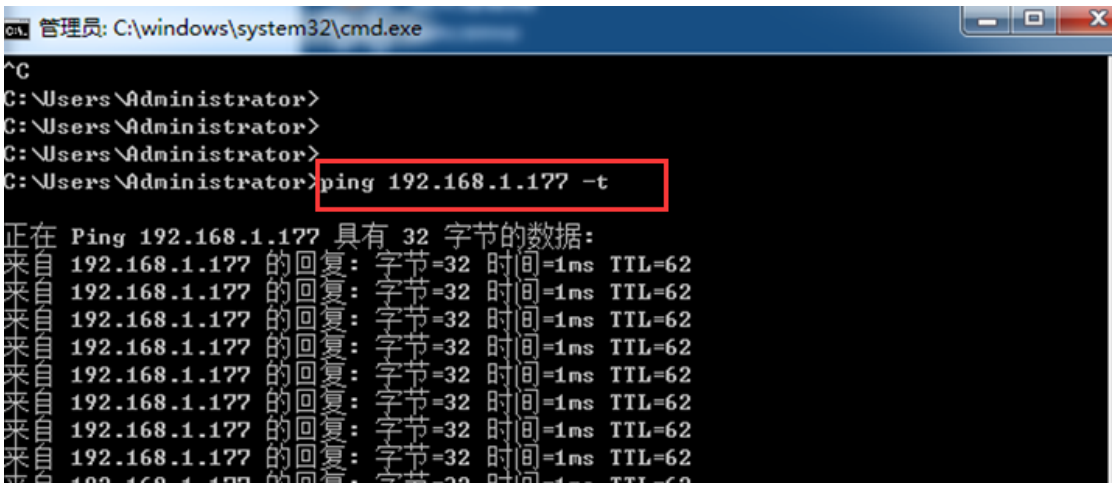


图 45　　2 号 G810 下的 pc

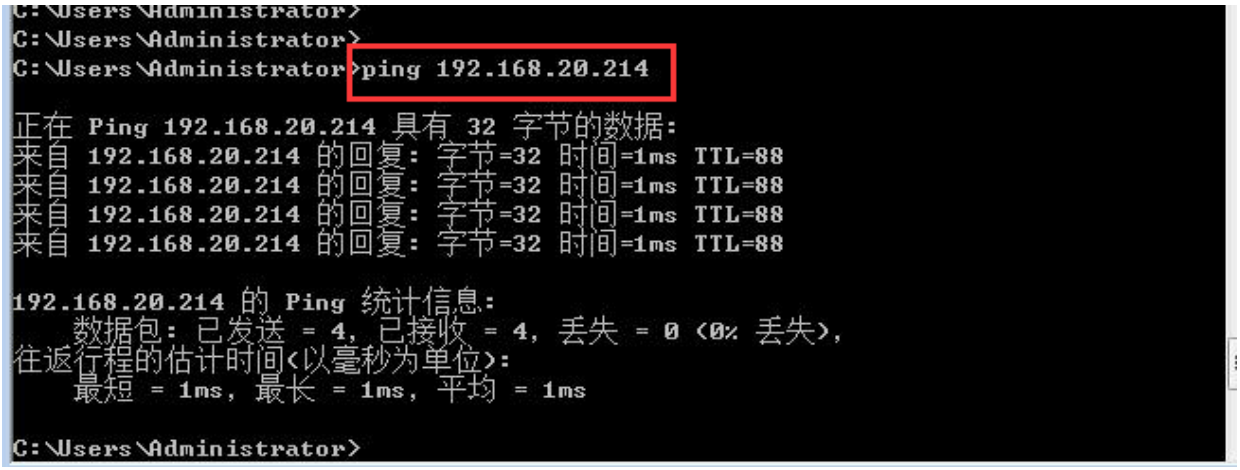


图 46　　1 号 G806 下的 pc

4.4. OpenVPN 搭建

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

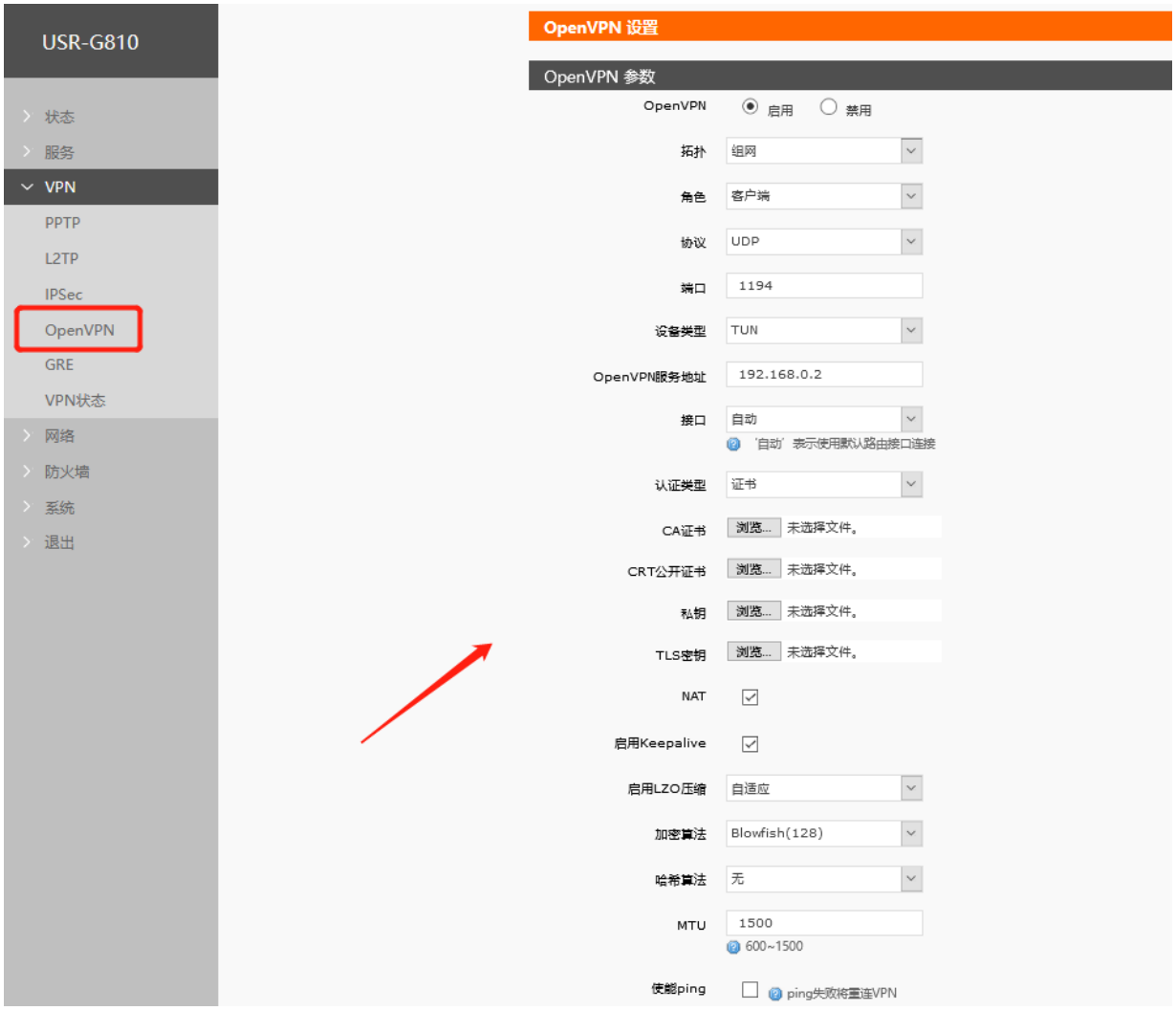


图 47　　OpenVPN 启用设置界面

- 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_5g、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；
- 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_Jz4Oqi4AWJnZuN8X.crt
key server_Jz4Oqi4AWJnZuN8X.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 48　Linux 下 OpenVPN 服务端配置

4.5. GRE 搭建

图 49　GRE 基本配置

- 远程地址：对端 GRE 的 WAN 口 IP 地址
- 本端地址：本端的 wan_wired、wan_5g 的地址，两者根据联网方式不同输入
- 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

- 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 1400

搭建举例：

1）、例如首先在虚拟机创建一个 GRE 的服务器：

ip tunnel add gre-test mode gre remote 192.168.13.13 local 192.168.13.66 ttl 255

ip link set gre-test up

ip addr add 10.10.10.2 peer 10.10.10.1 dev gre-test

执行完后，ifconfig 看一下已经出先一个 gre-test 网卡，但是这个 ping 10.10.10.1 是不通的

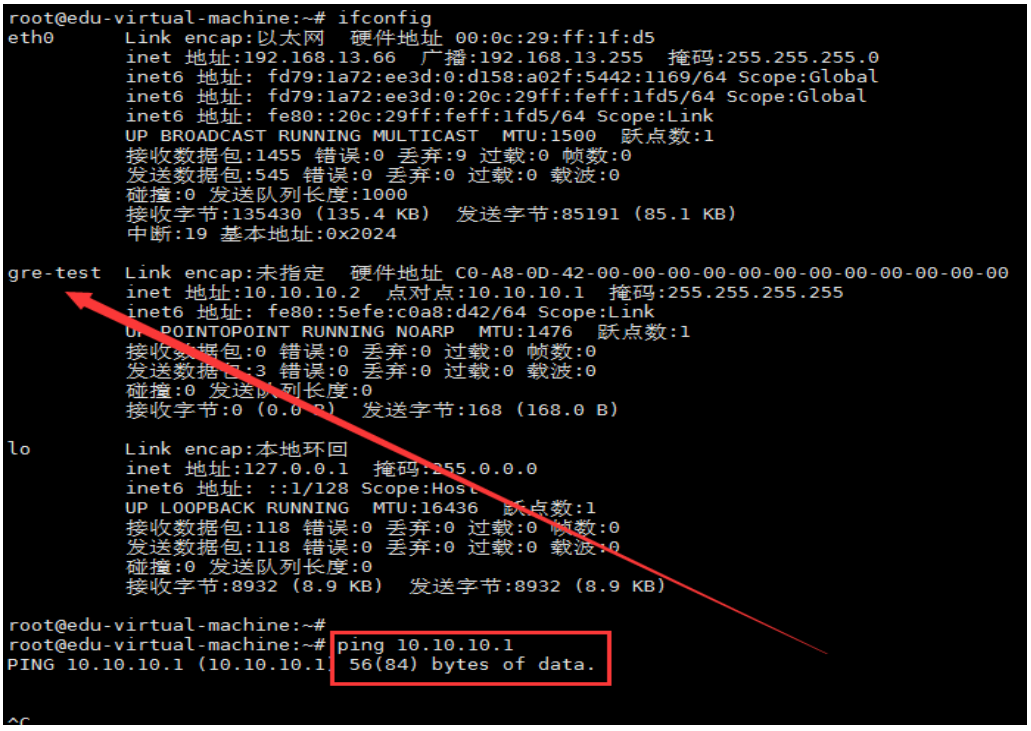


图 50 GRE 测试 1

2）、服务器搭建好之后，在 G810 的 GRE 配置界面做相应的配置。点击保存&应用后，看得到 IP、数据、时间均不为空表示搭建成功。

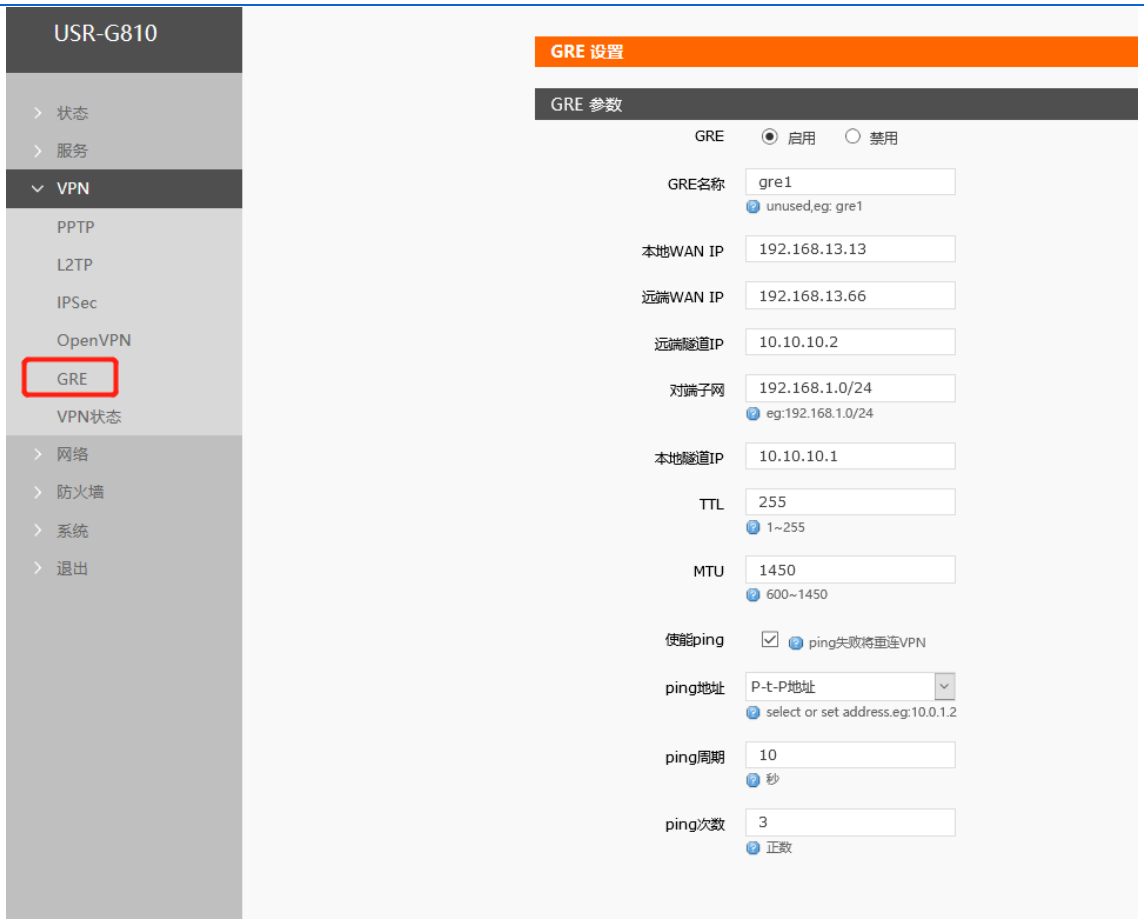


图 51　　GRE 测试 2

·然后在虚拟机上在看，这时也可以 ping 通客户端的隧道了。

```
root@edu-virtual-machine:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=1.03 ms
64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=1.03 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=1.03 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=1.03 ms (DUP!)
^C
--- 10.10.10.1 ping statistics ---
2 packets transmitted, 2 received, +6 duplicates, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.037/1.143/1.249/0.104 ms
root@edu-virtual-machine:~#
```

图 52　　GRE 测试 3

5.防火墙功能

5.1. 基本设置

默认两条防火墙规则。

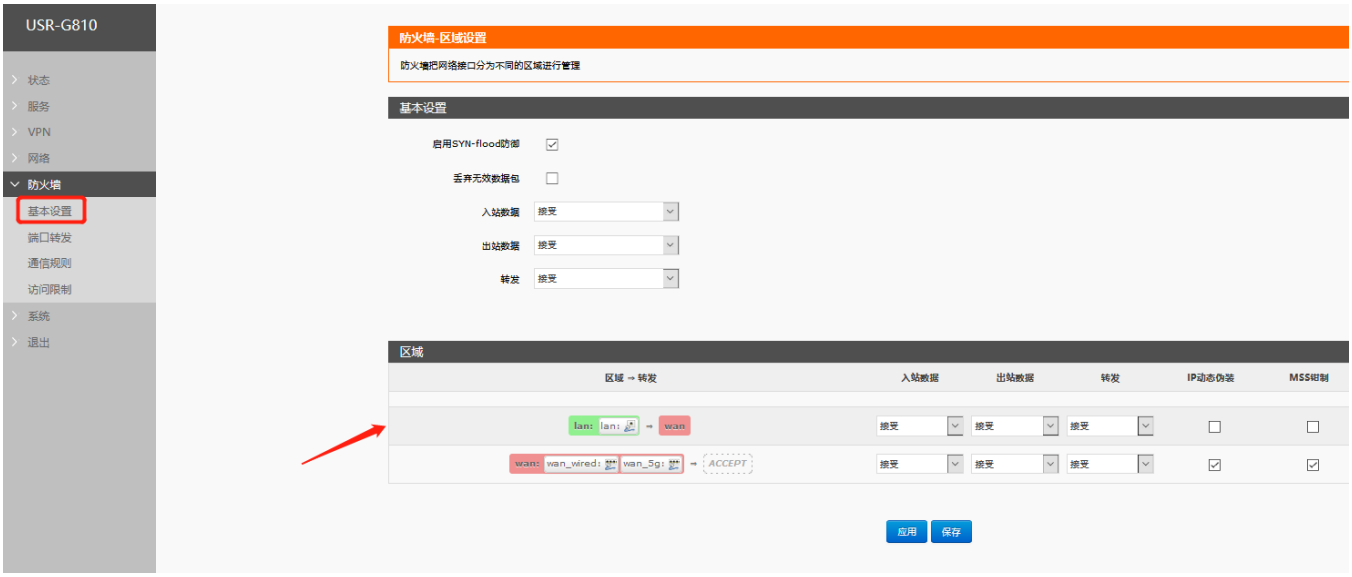


图 53　　防火墙设置界面

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

A、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，允许数据包从 LAN 口转发到 WAN 口，这属于转发

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”

B、规则 2

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 5G 口，此动作被允许

举例：应用场景中 LAN 口需要访问路由器设置，路由器也可以连接外网，但是不允许 LAN 口下的设备连接外网，此时就可以将 LAN 到 WAN 的转发规则设置为拒绝或者丢弃（丢弃即无反馈信息）。

5.2. NAT 功能

5.2.1. IP 动态伪装

IP 动态伪装，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。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。

IP 动态伪装设置位于“防火墙-基本设置”界面。

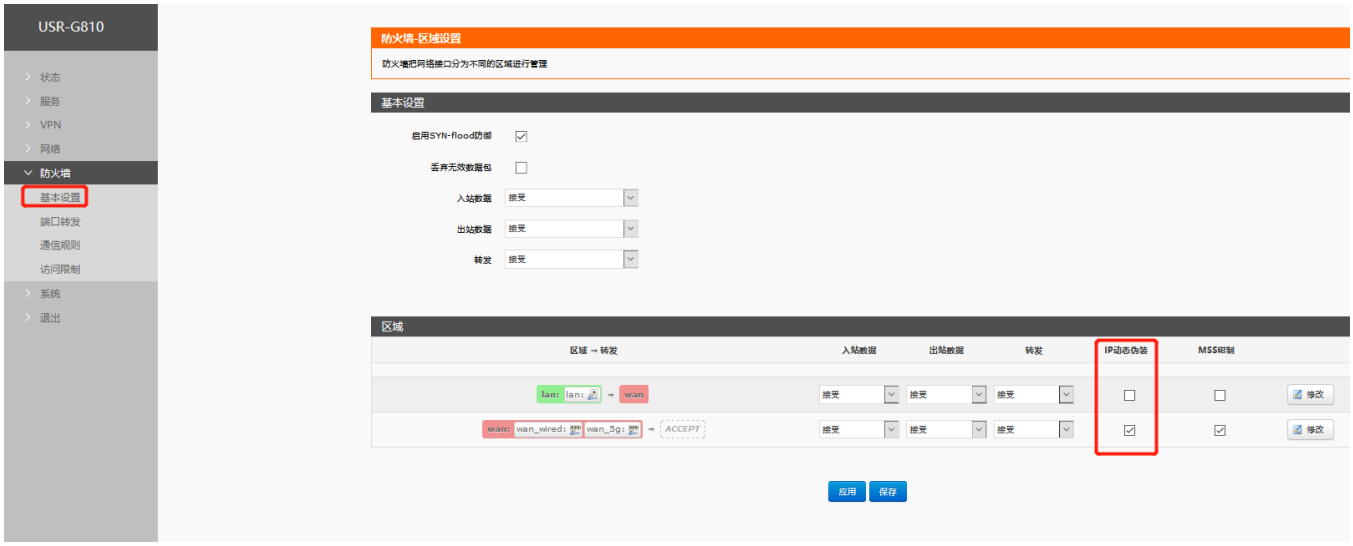


图 54　　IP 地址动态伪装设置

5.2.2.　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。

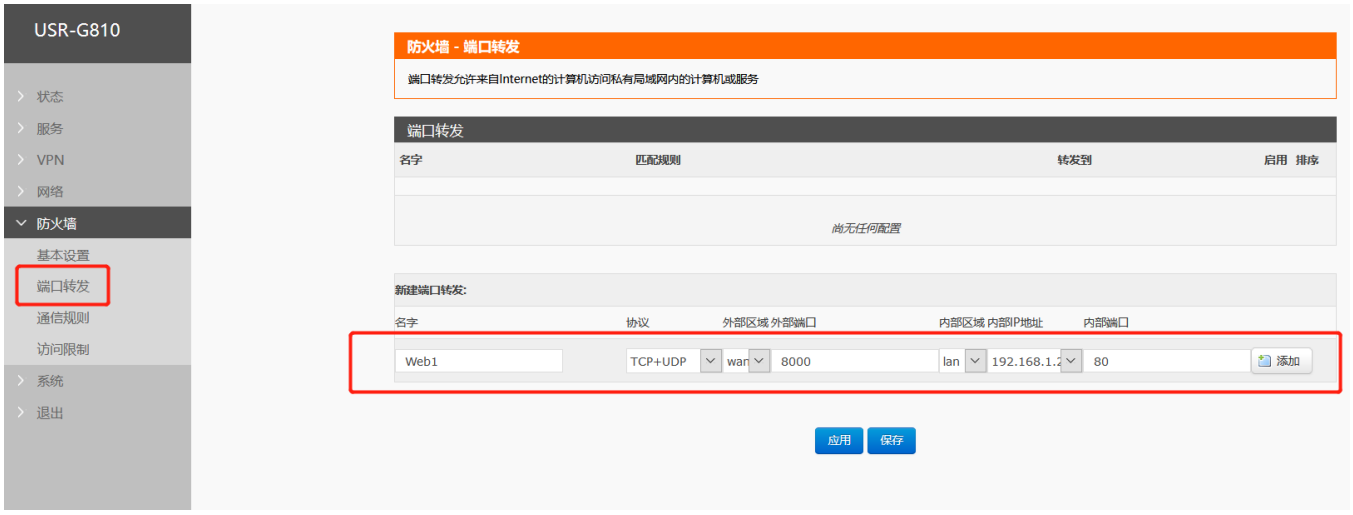


图 55　　端口设置界面一

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。

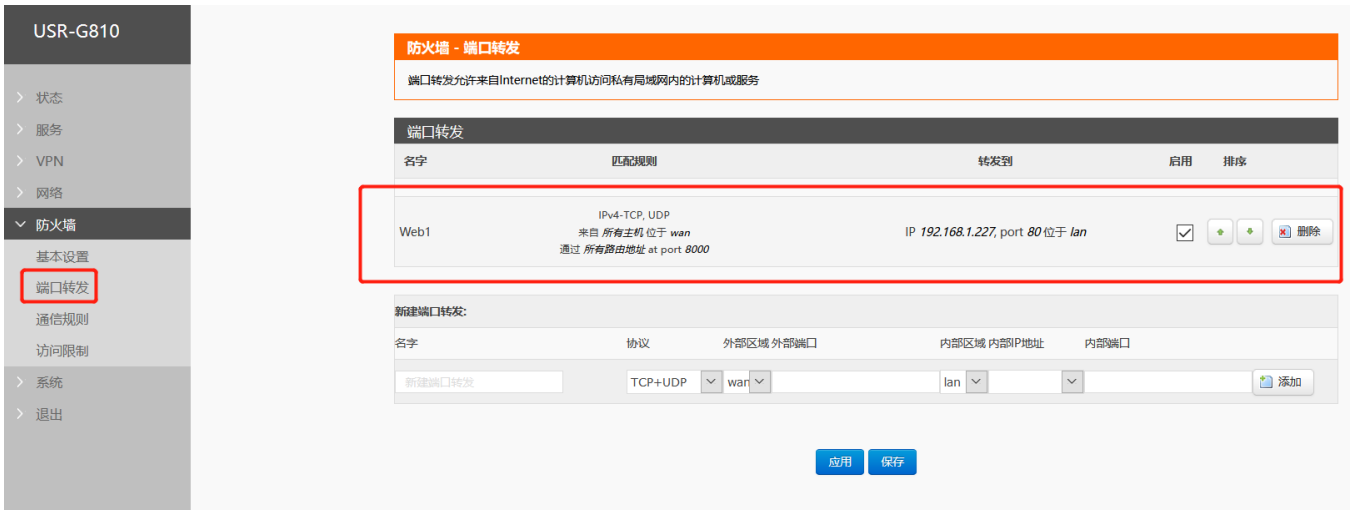


图 56　　端口设置界面二

然后点击右下角的“保存&应用” 按钮，使设置生效。

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。例如，139.224.114.36:

8000 端口转发 192.168.1.227：80，即代表我们从 WAN 口访问 8000 端口时，访问请求将会被映射到 192.168.1.227:80 上面。

5.2.3. 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，即可.

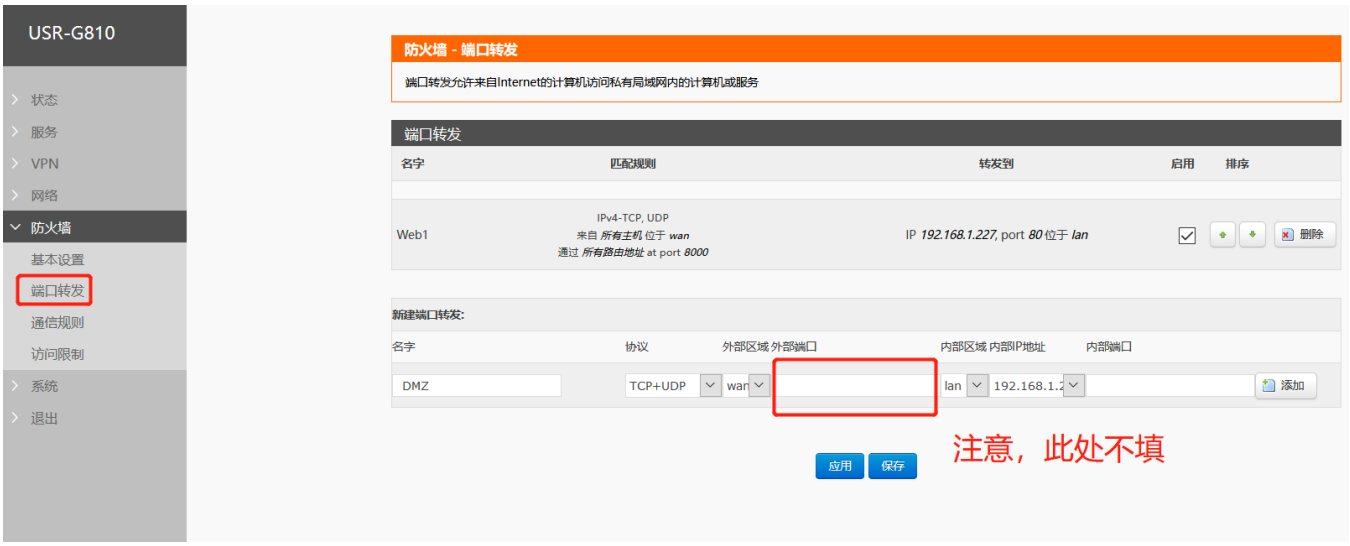


图 57 DMZ 设置一

点击添加然后进行保存&应用。

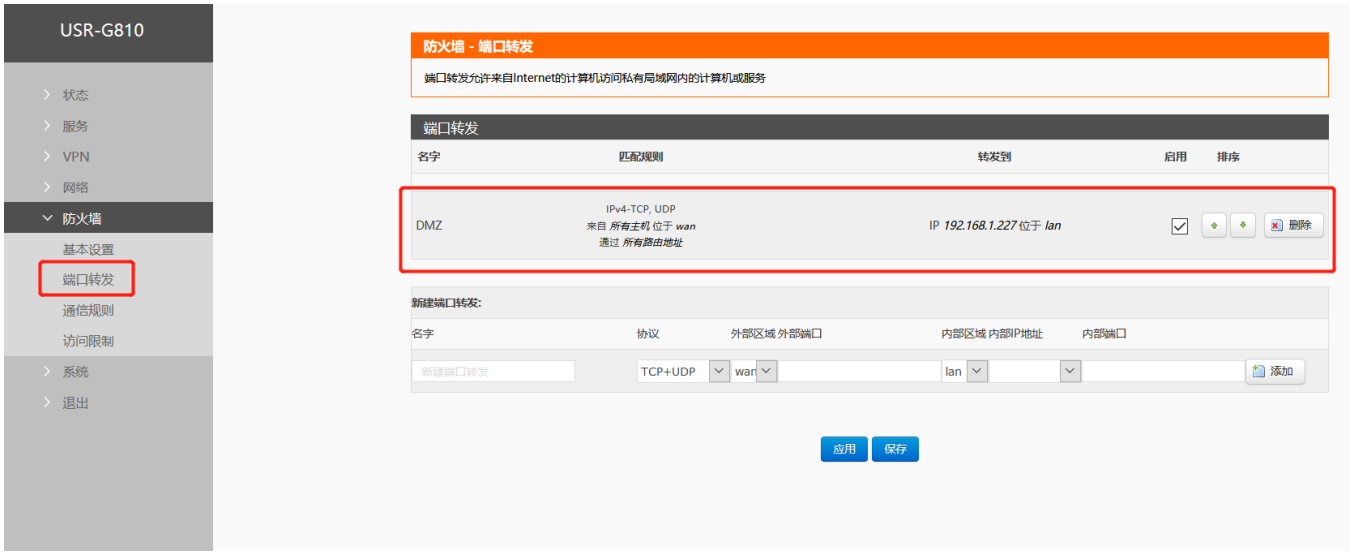


图 58 DMZ 设置二

如图，WAN 口地址的所有端口都映射到内网 192.168.1.227 这台主机上。

注意：端口映射和 DMZ 功能不能同时使用

5.3. 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。

5.3.1. 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”

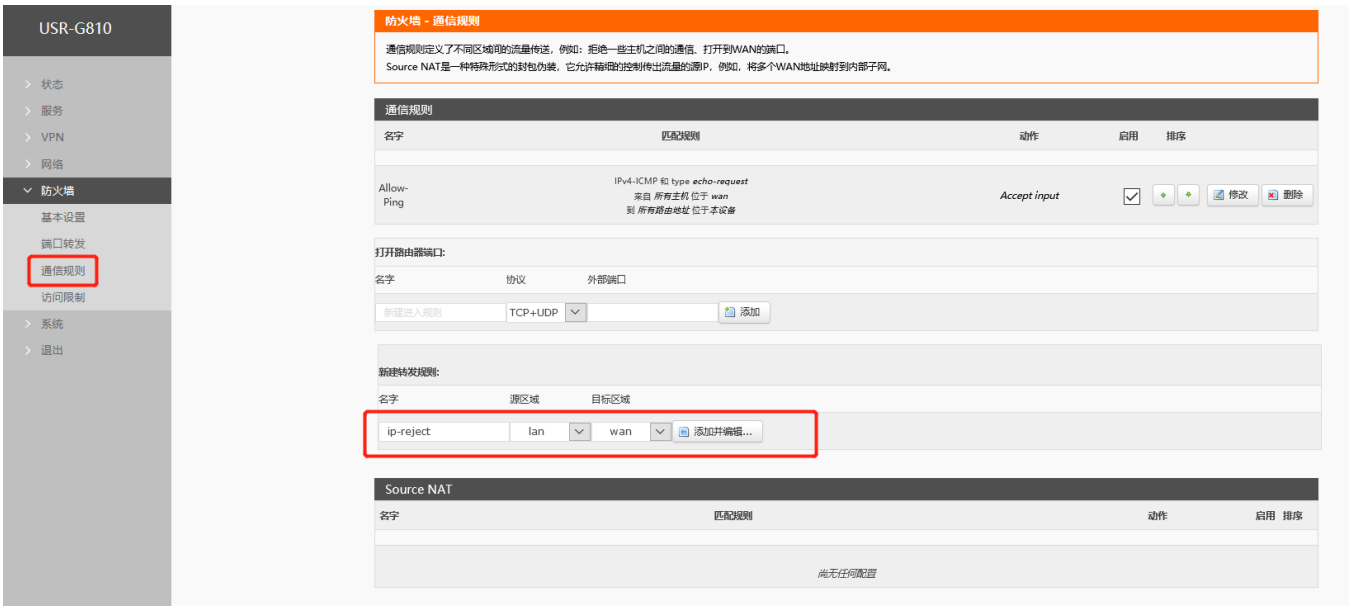


图 59　防火墙 IP 黑名单图一

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，其中一项为“全部”或者 IP 地址与 MAC 地址相对应，否则不生效），如下图

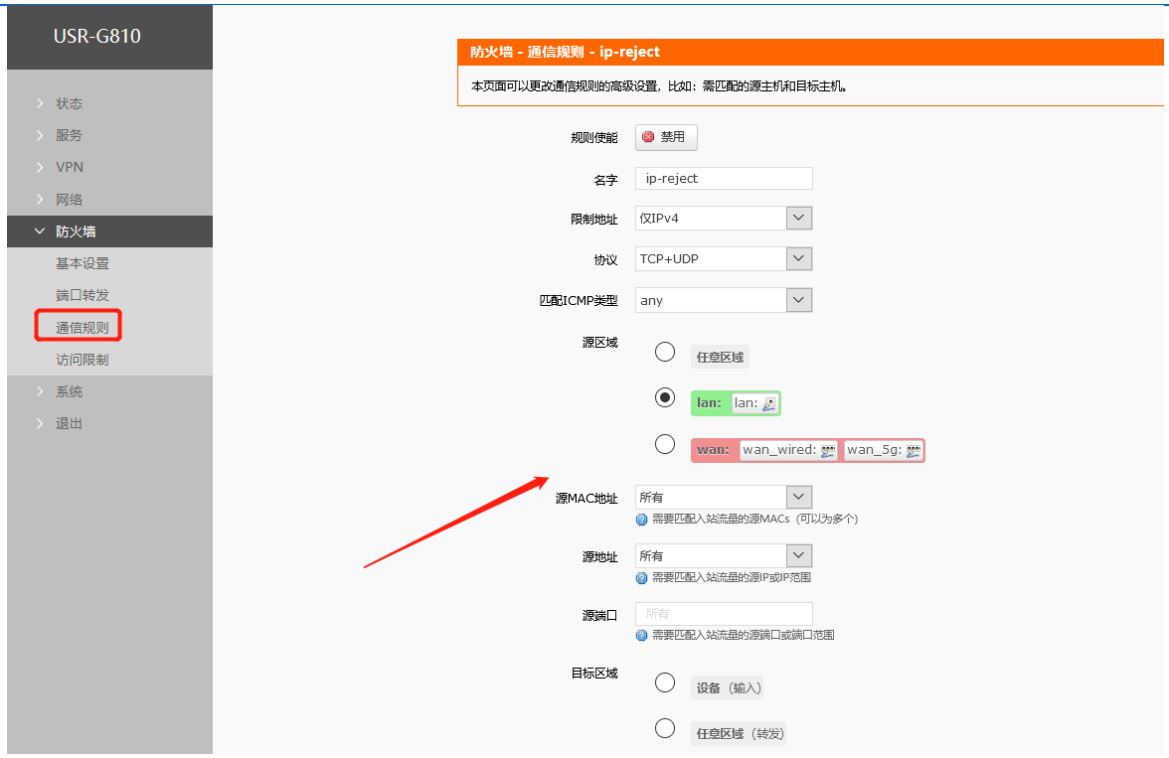


图 60　　防火墙 IP 黑名单图二

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“保存并应用”。如下图。

图 61　　防火墙 IP 黑名单设置图三

图 62　　防火墙黑名单设置图四

这样设置完成后，就实现了 IP 黑名单的功能。

5.3.2.　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 63　　防火墙 IP 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，其中一项为“全部”或者 IP 地址与 MAC 地址相对应，否则不生效），如下图

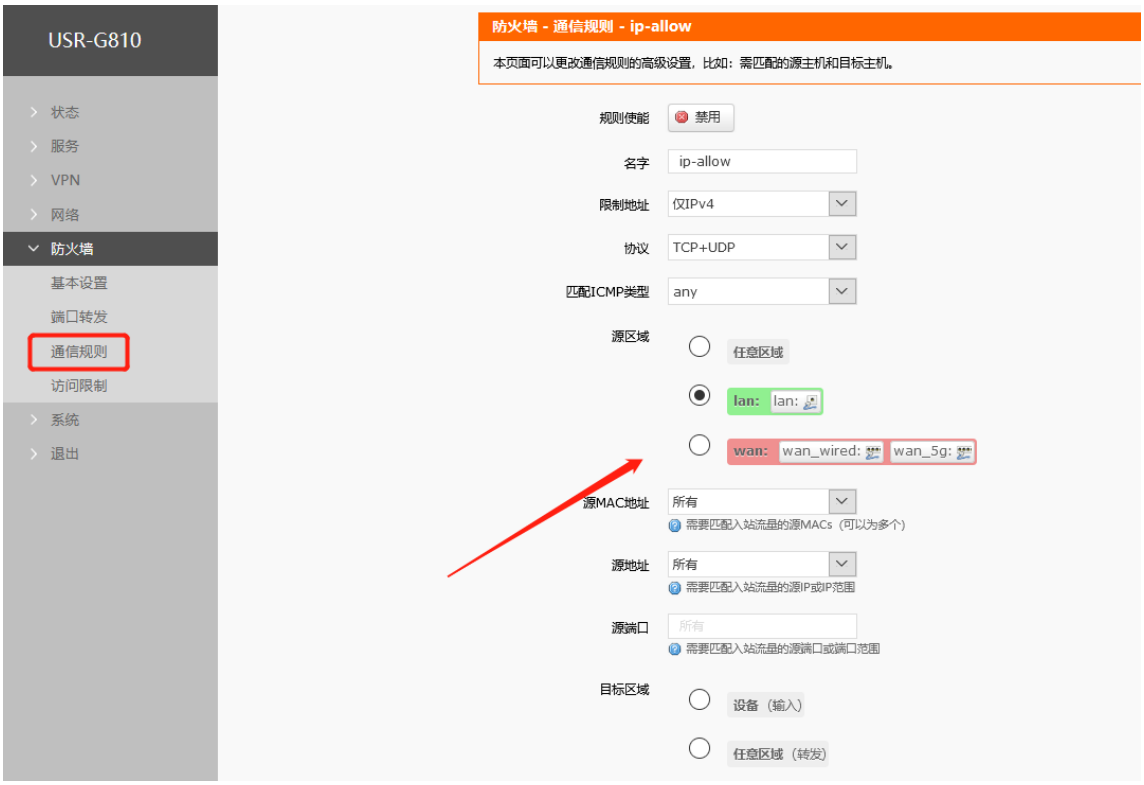


图 64　　防火墙 IP 白名单图二

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。

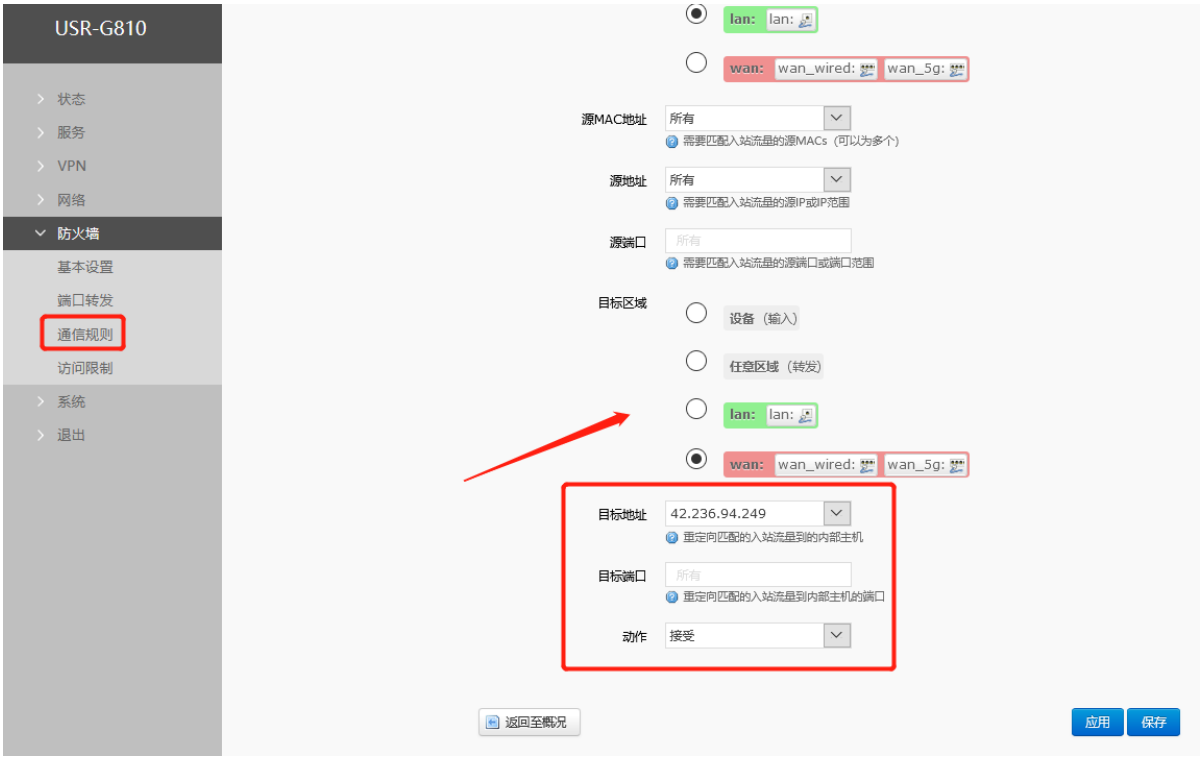


图 65　防火墙 IP 白名单图三

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 66　防火墙 IP 白名单图三

5.3.3. 拒绝某子网设备访问某指定 IP

首先添加一条转发规则

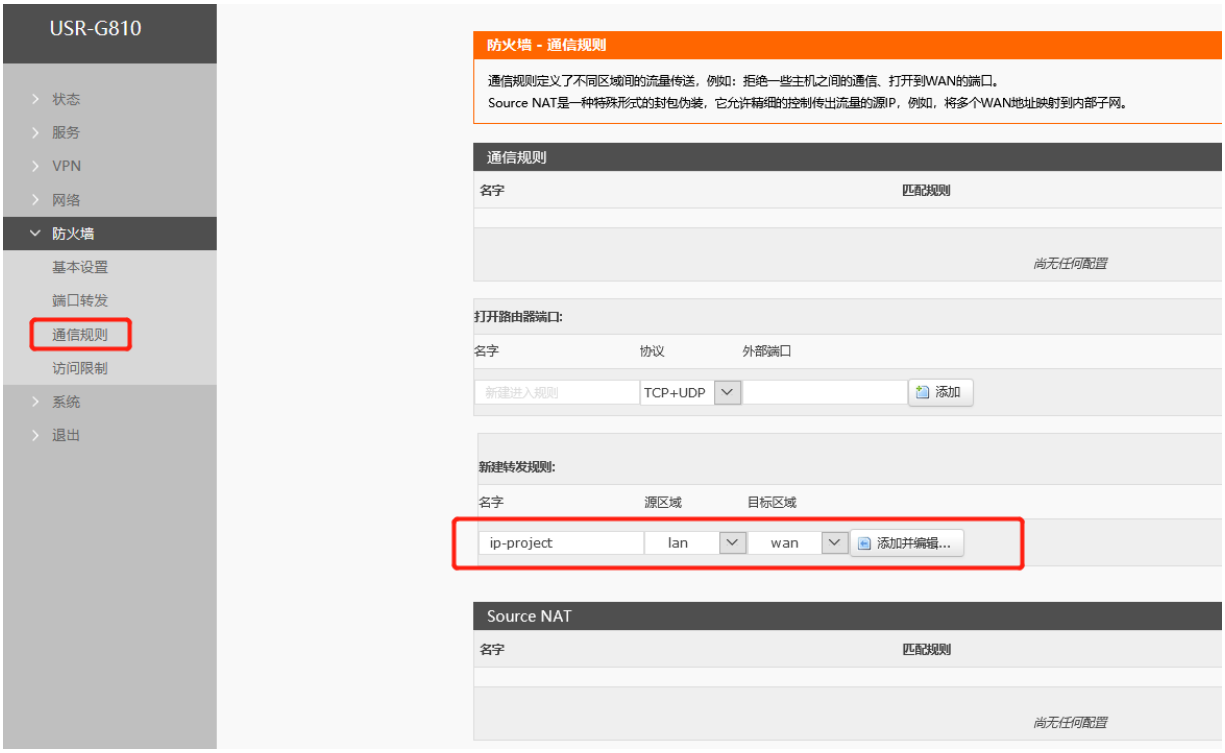


图 67 防火墙设置一

- 协议选择 TCP+UDP，则为指定源 IP 可 ping 通指定目标 IP，建立不了 TCP/UDP 连接。
- 协议选择 ICMP，则为指定源 IP 无法 ping 通指定目标 IP,可建立 TCP/UDP 连接。

注意：

如果想禁止某子网设备某端口不可访问指定目标 IP，此例子选择 TCP 协议。

图 68　　防火墙设置二

源区域目的区域请保持默认，源 MAC 以及源 IP 选择填写其中一个，如果都填写，请保持 MAC 与 IP 相对应，否则将不生效。

以下例子为禁止源 MAC 为 84:2A:FD:39:90:35 的设备的 8800 端口,与目的地址为 192.168.1.1 端口为 8899 建立 TCP 连接。如果源端口与目的端口均不填则为禁止源 MAC 为 84:2A:FD:39:90:35 的设备与目的地址为 192.168.1.1 建立 TCP 连接。

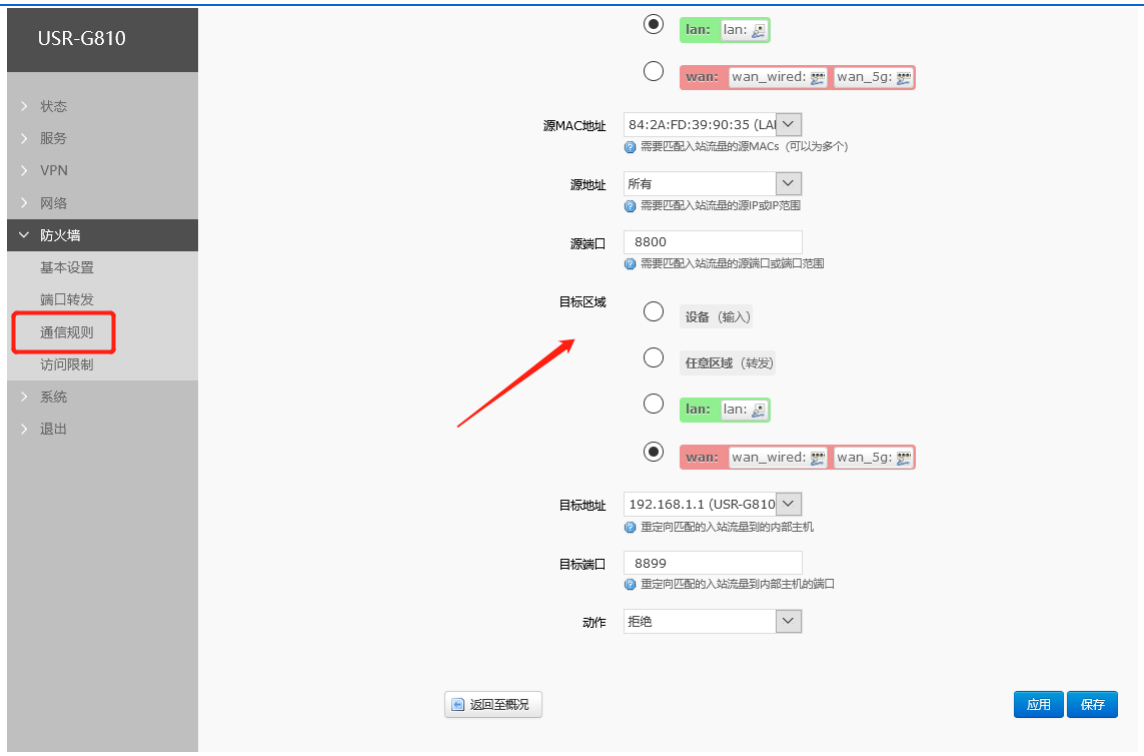


图 69　　防火墙设置三

注意：附加参数请慎用，如果以上配置不能满足您的需求，请联系我司技术支持。

5.3.4.　禁 PING 功能

设备默认是允许被 ping 的，可以通过修改默认规则，实现禁 ping 功能。

图 70　　防火墙设置一

源区域、目标区域默认即可。源 MAC、IP 选择所有即可（根据需求是否需要所有子网设备禁 ping 来选择），

源端口号无需填写。目的 IP 选择所有、根据需求可填禁止到某 IP 的 ping 还是禁止到所有 IP 的 ping 检测。目的端口无需填写。

举例如下：此例为禁止子网设备 IP 为 192.168.1.227 到目的地址为 192.168.225.23 的设备 ping 动作。

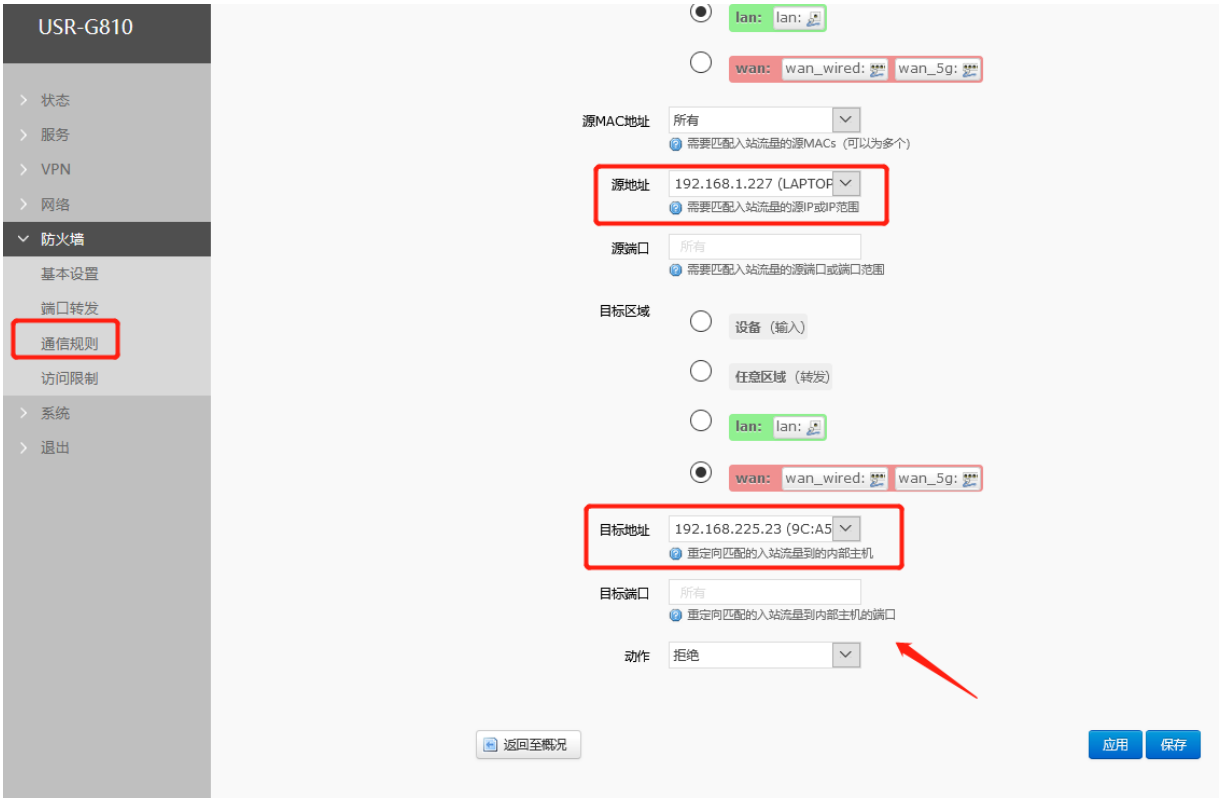


图 71　防火墙设置三

设置完成后点击应用即刻生效。把禁 ping 功能或者其他设置防火墙策略暂时不使用时，将右边“启用”下面的勾选去掉后点击应用即可，再次使用时将启用框勾选，再点击应用即可。

图 72　防火墙设置四

5.4. 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，只能访问白名单内的域名地址。黑名单和白名单都可以设置多条，此功能默认关闭。

5.4.1. 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，然后点击报保存，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。

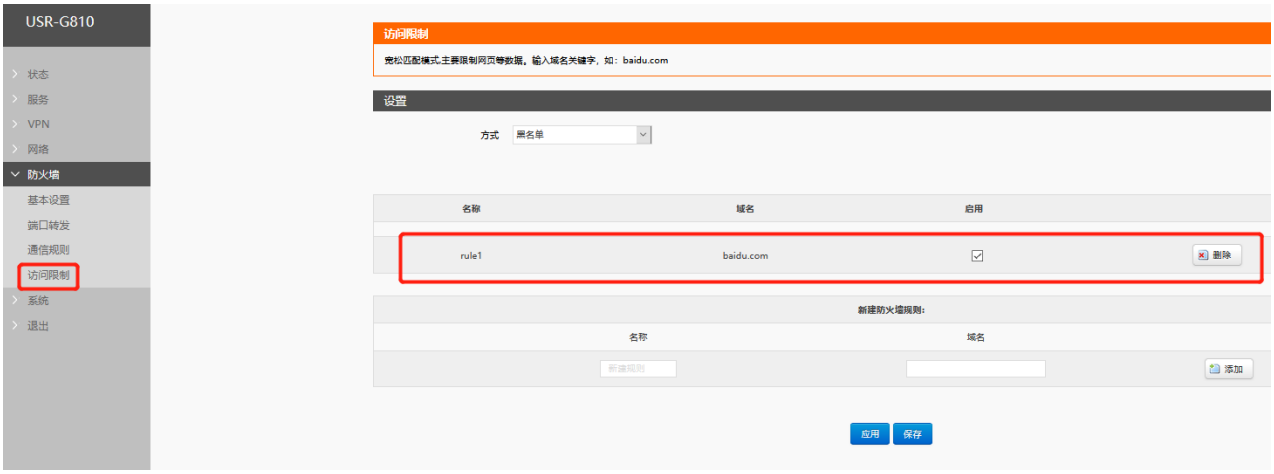


图 73　域名黑名单

5.4.2. 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，然后点击报保存，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。

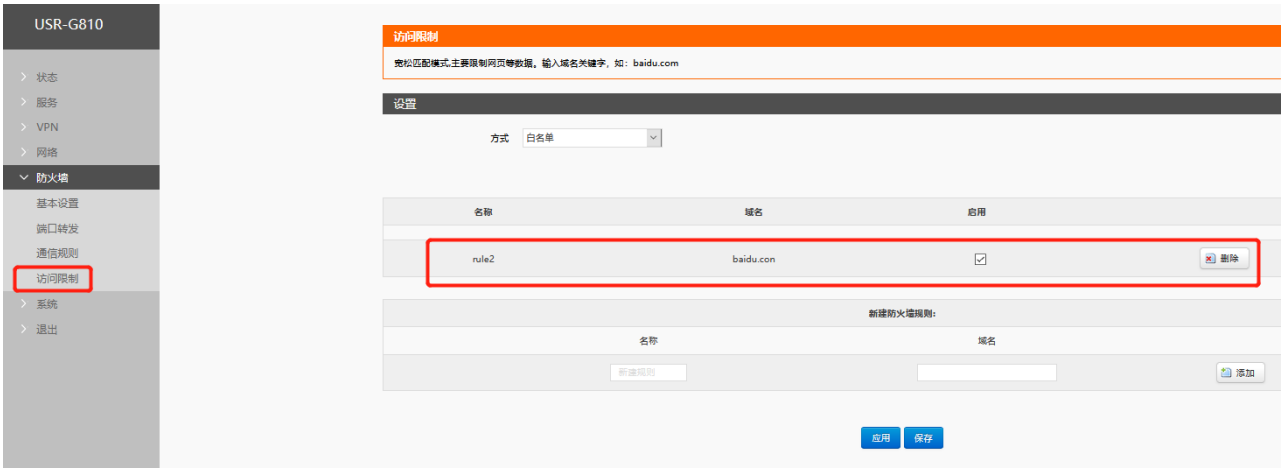

USR-G810
状态
服务
VPN
网络
防火墙
基本设置
端口转发
通信规则
访问限制
系统
退出
访问限制
宽松匹配模式,主要限制网页等数据，输入域名关键字，如：baidu.com
设置
方式
白名单
名称
域名
启用
rule2
baidu.con
删除
新建防火墙规则:
名称
域名
添加
应用
保存

图 74　　域名白名单

6. 高级服务功能

6.1. 花生壳内网穿透

设备支持花生壳内网穿透功能，花生壳动态域名内网穿透版支持内网穿透，可以实现设备的远程登录与管理，

设置步骤：

1、选择开启，点击“保存”后再点击“应用”，页面会显示 SN 码和服务设备状态

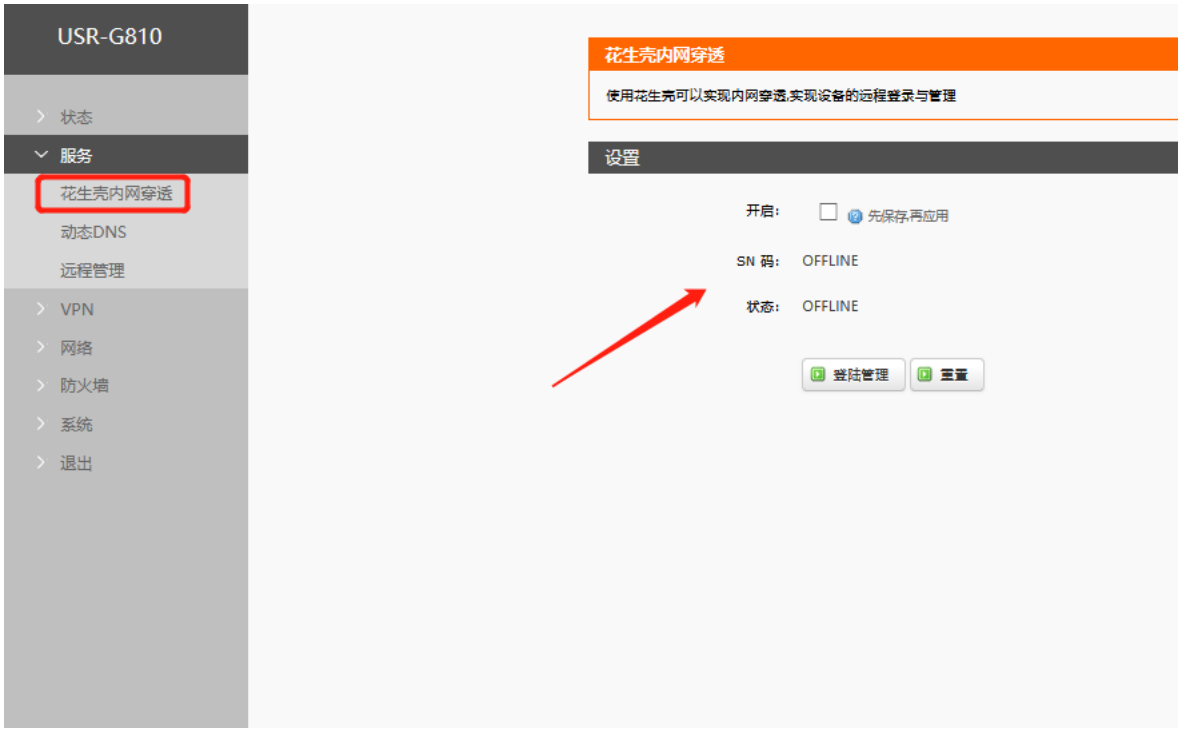


图 75　花生壳内网穿透启用前

图 76　　花生壳内网穿透启动后

2、点击“登陆管理”，登录到花生壳的网站，（如果不能够跳转的到花生壳的登录界面，请检查浏览器，选择允许弹出式窗口），初始登录密码为 admin。

图 77　　花生壳内网穿透 SN 码登陆

3、初次登录需要绑定，微信扫描激活。

图 78　　花生壳内网穿透激活

4、激活成功后需要切换账号，关联到花生壳的账号登录

图 79　　花生壳内网穿透切换账号

5、切换到账号登录点击左侧的内网穿透

图 80　　花生壳内网穿透设置（一）

6、点击“+”号添加映射,设置相关参数

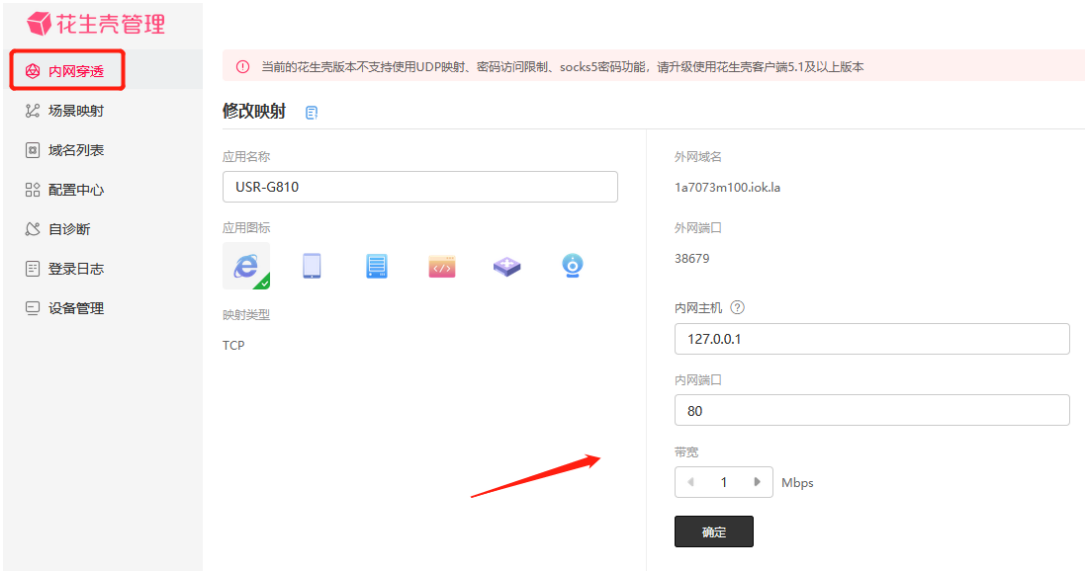


图 81　　花生壳内网穿透设置（二）

网络类型选择自定义端口，域名选择选项选择要映射的域名（申请免费版的或购买付费版），应用名称项填写次条映射的名称（任意），内网主机项填写需要映射的设备的 IP 地址，外网端口选项固定端口需要购买，再次选择临时端口，然后点击确认。

表 9　　端口映射参数表

功能	参数设置（如果要使用）	备注
映射类型	选择通用端口	选择通用端口
选择域名	选择要进行映射的域名	需要申请或购买
应用名称	此条映射的名称	可以任意填写
内网主机	需要添加映射的设备的 ip	本机填写 127.0.0.1
内网端口	内网设备的端口	本机填写 80
外网端口	使用域名登陆时的端口	可购买固定端口或选择动态端口

7、测试域名。注意：花生壳内网穿透规则配置后，由于 dns 解析需要时间，可能出现无法立即生效，若没

有立即生效，一般等待 1-2 分钟内可以生效。

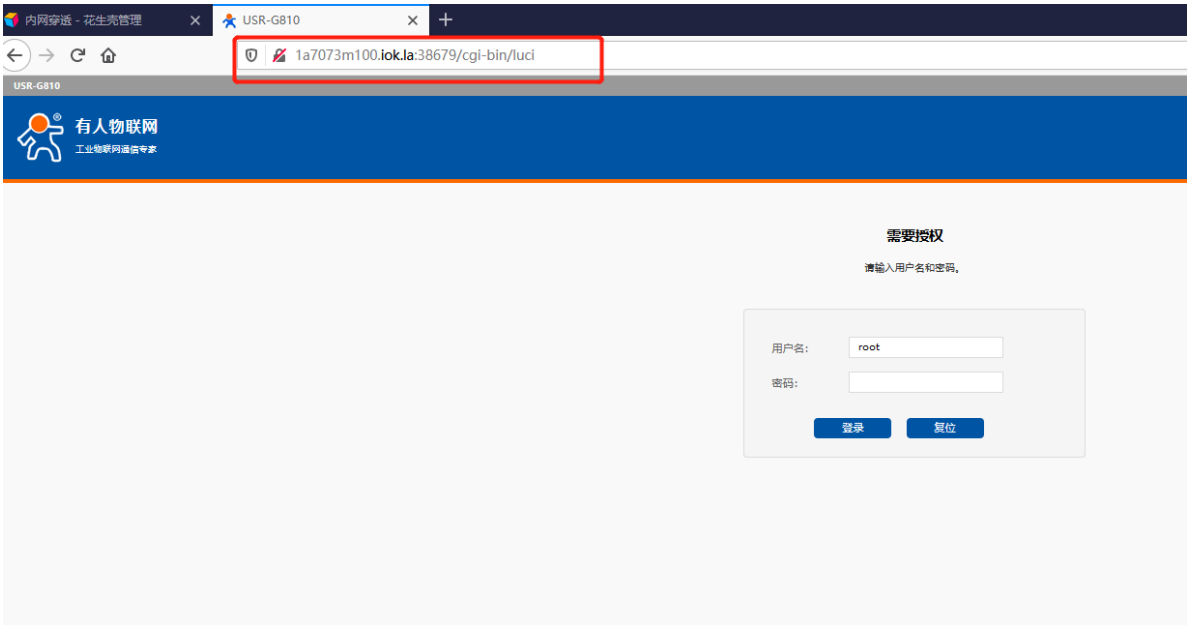


图 82　　花生壳内网穿透域名测试

使用设置内网映射的域名（注意加上端口号），即可实现 PC、手机、平板的远程登陆与管理

6.2. 动态域名解析（DDNS）

6.2.1. 已支持的服务商

动态域名的使用分为两种情况，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：

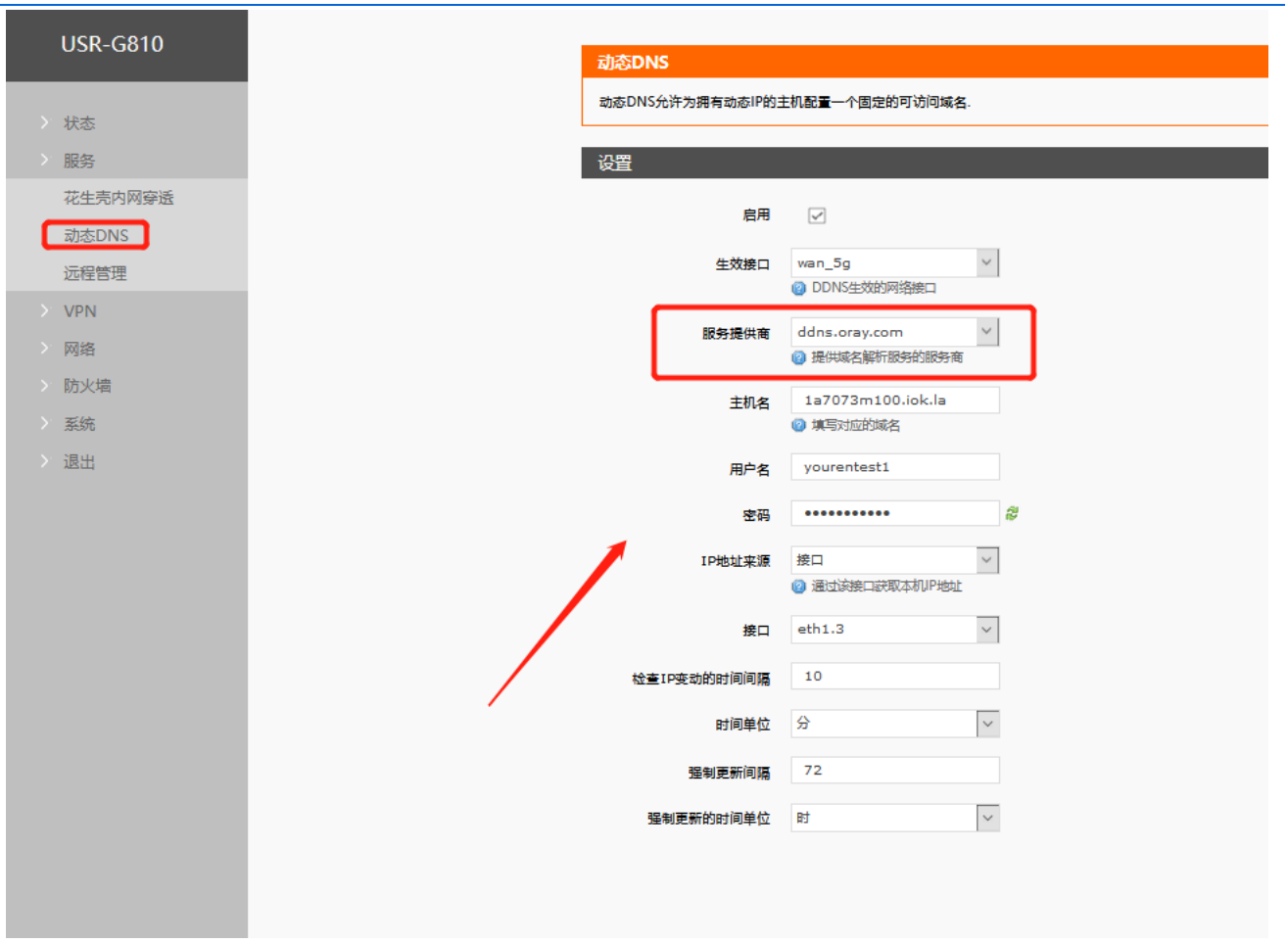


图 83　　DDNS 设置页面

参数填写要求如下：

表 10　　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：1a7073m100.iok.la
用户名	花生壳账户名	举例：yourentest1
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 eth1.3，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。

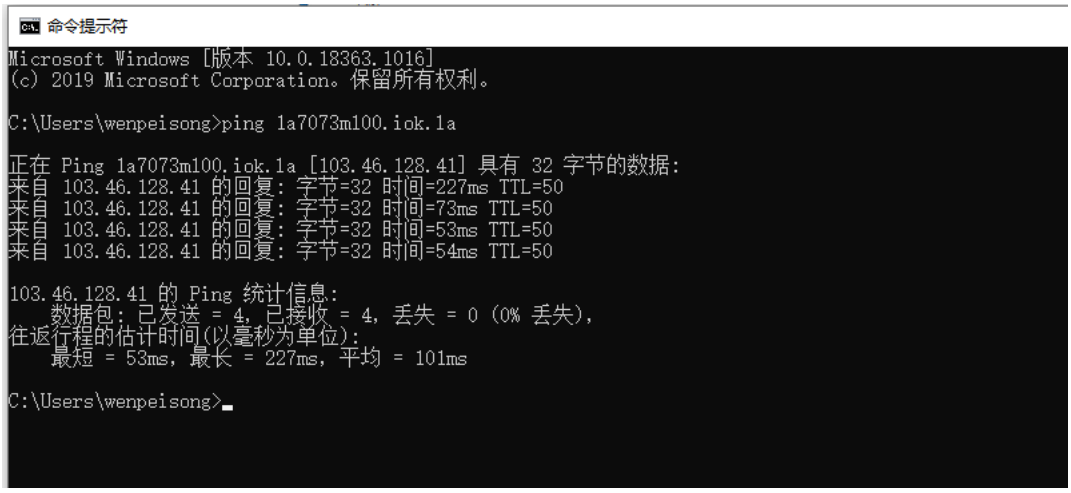


图 84　　DDNS 测试图

6.2.2.　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：

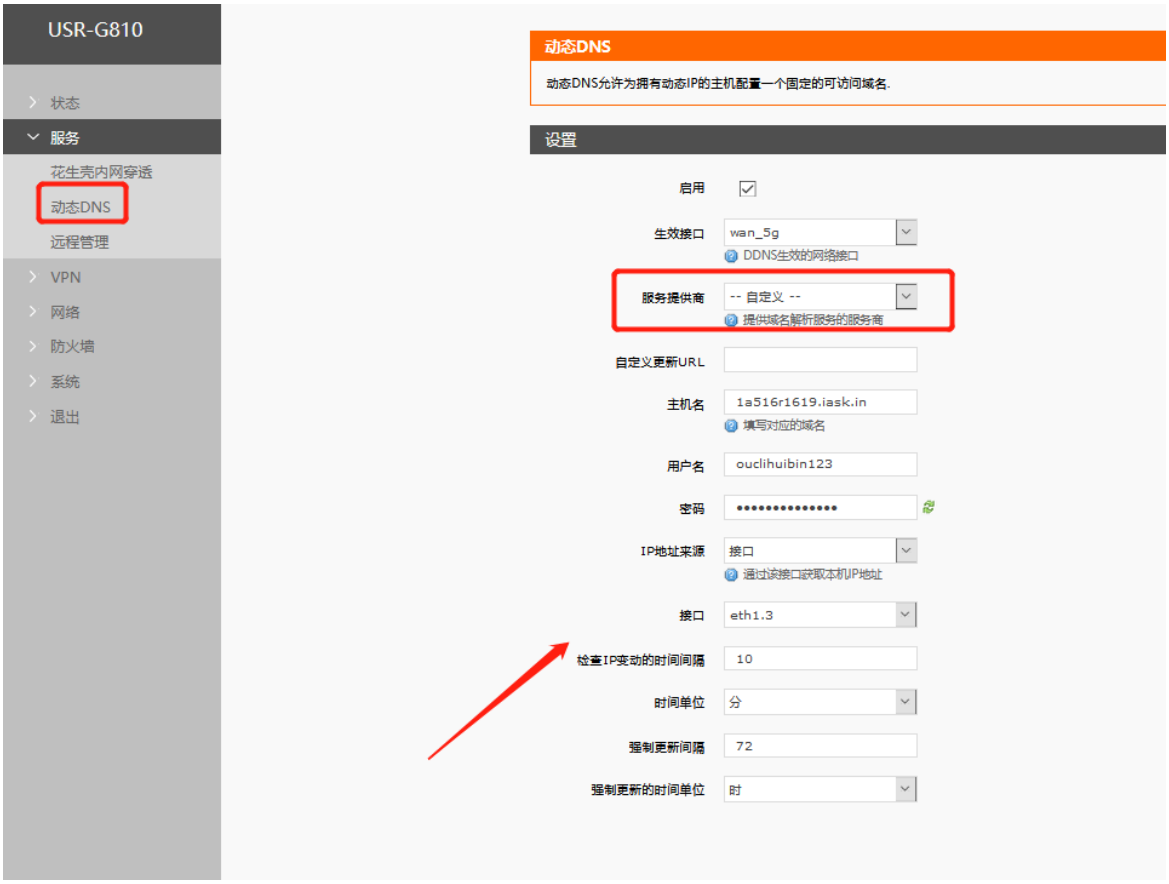


图 85 DDNS 自定义服务参数设置页面

DDNS 功能，为路由器自身在外网中提供一个动态的域名解析功能，为自己申请一个域名来指向自己的 WAN 口的 IP 地址。本功能允许异地通过域名的方式直接访问到路由器。

参数需要如下填写（以花生壳为例），申请的动态域名为 1a516r1619.iask.in，用户名 ouclihuibin123，密码 ouclihuibin1231 。

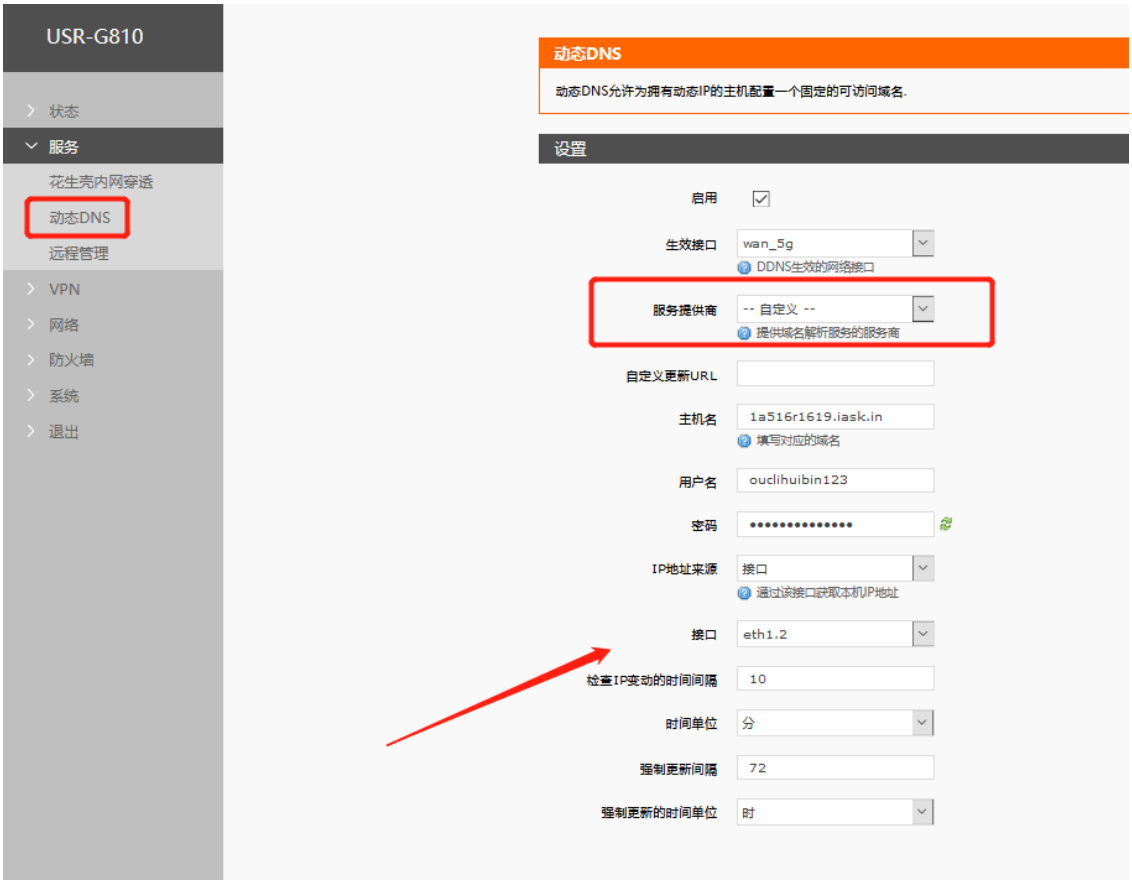


表 11　DDNS 自定义服务参数表

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://ouclihuibin123:ouclihuibin1231@ddns.oray.com/ph/update?hostname=1a516r1619.iask.in
主机名	请填写您申请号的域名	举例：1a516r1619.iask.in
用户名	花生壳账户名	举例：ouclihuibin123

密码	花生壳密码	举例：ouclihuibin1231
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 eth1.2，也就是 5G 接口
检查 IP 变动的时间间隔	检测 IP 地址变动的时间间隔，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

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 86　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。

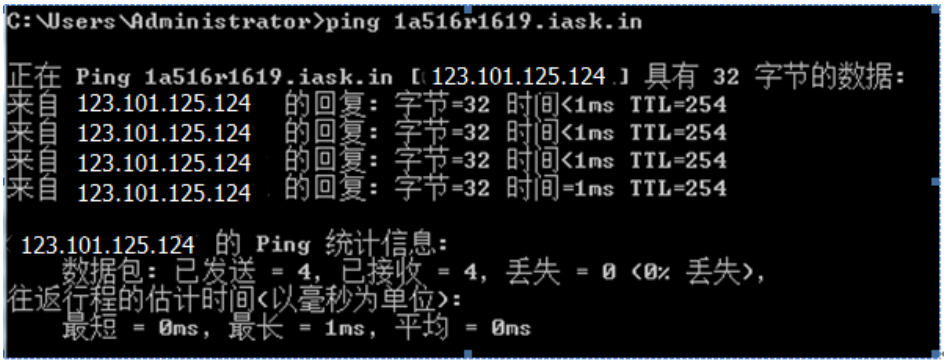


图 87　DDNS 测试图三

- 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

6.3. 远程管理

6.3.1. 远程平台

远程平台是远程监控和升级的设备管理平台，其地址是 ycsj1.usr.cn。如需使用远程管理平台，请先行注册后，将账号通过工单或业务人员提交给技术工程师授权后方可使用。其具体使用方式如下：

设备添加界面，将小写 mac 输入框中，其它选根据需要选择，然后点击添加

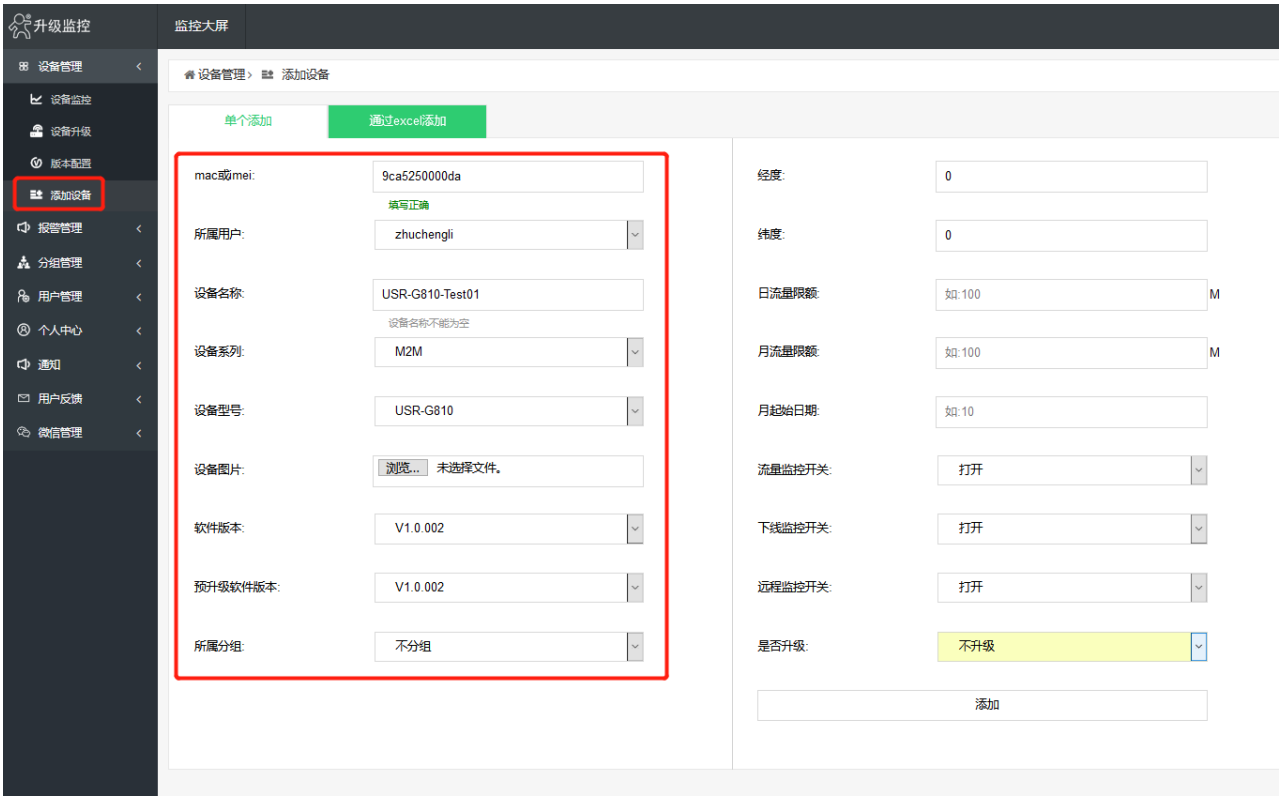


图 88　设备注册

远程监控界面，会显示当前在线的设备，点设备对应的 mac 会进入具体设备的监控页面，此界面可以监控流量信息，运行时间，还可以发送 AT 指令查询路由器具体的运行参数信息。

详细 AT 指令可参见《AT 指令集》。

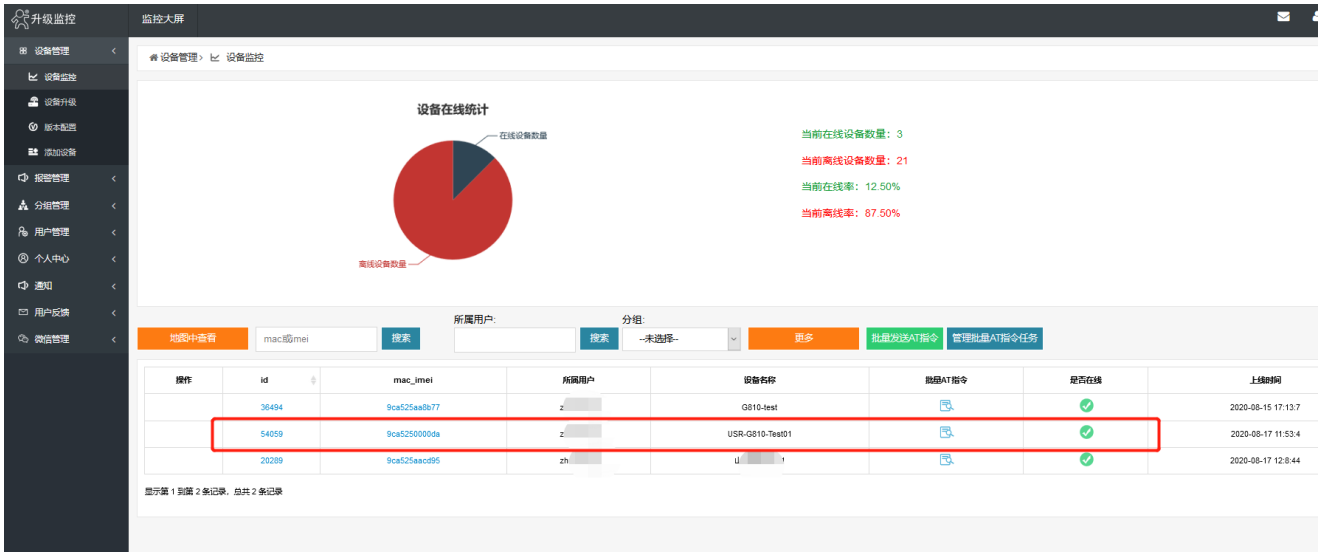


图 89　　设备监控一

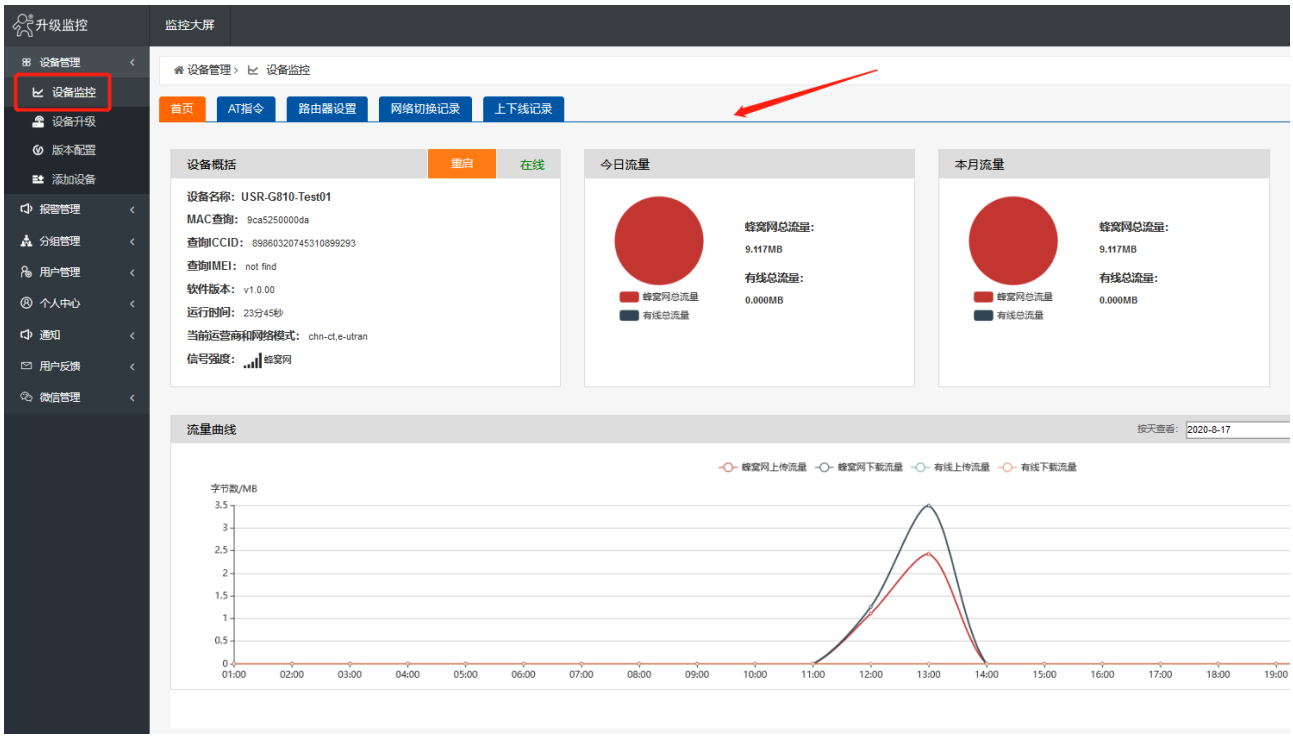


图 90　　设备监控二

远程升级界面，点击 按钮进行版本配置，选择好软件版本和预升级版本，是否升级选项选择升级，

点击修改，设备就可以实现自动升级了。

图 91　　设备升级一

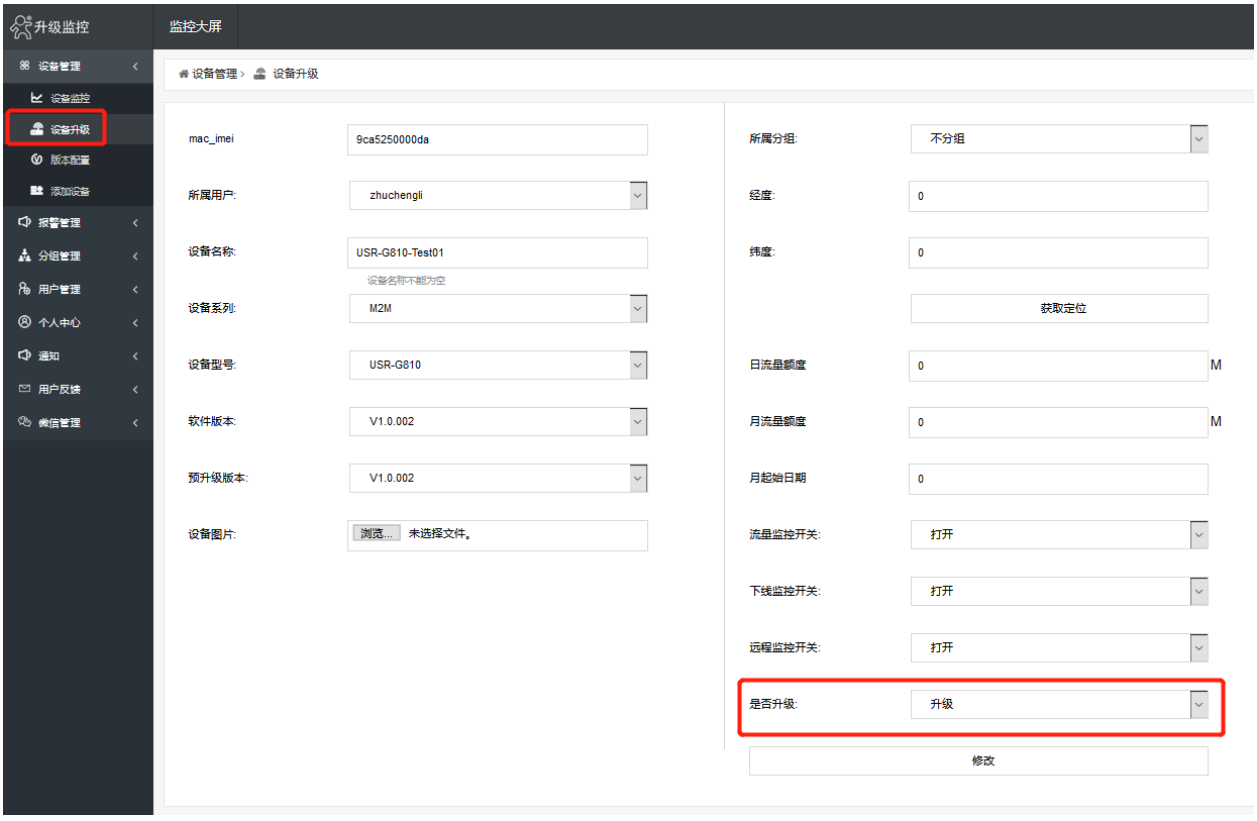


图 92　　设备升级二

平台可定制短信 AT 指令功能：编辑短信到路由器设备的 SIM 卡查询路由器的运行信息并且设置路由器的参数，使用此功能的前提是 SIM 卡支持短信功能。

6.3.2. 远程升级

远程升级功能支持设备连接远程服务器实现远程固件升级的功能，远程地址为远程服务器的地址默认为ycsj1.usr.cn，远程端口默认为 30001，间隔是设备上报信息给远程服务器的将时间，默认为 1800 秒，远程升级功能默认打开。

图 93 远程升级

参数列表：

表 12 远程升级参数表

功能	参数设置（如果要使用）	备注
使能远程固件升级	勾选	如果使用请勾选
远程地址	远程固件升级服务器地址	默认 ycsj1.usr.cn
端口	远程升级服务器端口	默认 30001
间隔时间	设备向服务器发送设备信息的间隔时间	默认 1800 秒

注意：

➢ 详细远程升级的使用，请登陆 ycsj1.usr.cn。远程地址、端口请使用默认设置。

6.3.3. 远程监控

远程监控功能支持设备运行信息（流量、运行时间、固件版本、信号强度、APN）上报给远程监控服务器，远程服务器可以通过下发指令控制设备的运行，设置页面如下：

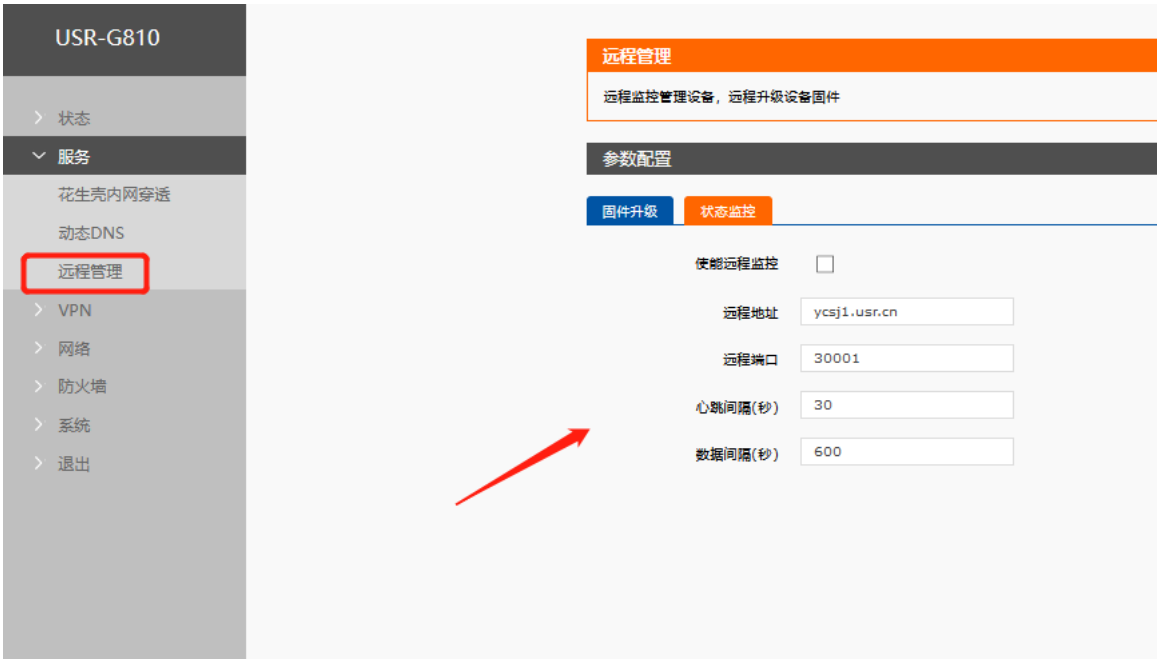


图 94 远程监控

参数列表：

表 13 端口映射参数表

功能	参数设置（如果要使用）	备注
使能远程监控	勾选	如果使用请勾选
远程地址	远程固件升级服务器地址	默认 ycsj1.usr.cn
端口	远程监控服务器端口	默认 30001
心跳包间隔	设备发送心跳包的时间间隔	默认 30 秒
间隔	设备上报运行信息的时间将	默认 600 秒

注意：

详细的远程监控和远程升级的使用，请登陆 ycsj1.usr.cn

当在远程平台添加设备后，如果勾选了远程监控功能，再设备远程升级或恢复出厂设置后，设备也会自动开启远程监控服务。

7.AT 指令集

设备支持远程 AT 指令集，在使用远程监控平台时，可使用 AT 指令查询相关信息。

远程监控请登陆 ycsj1.usr.cn，功能参见“远程管理-远程监控”章节介绍。

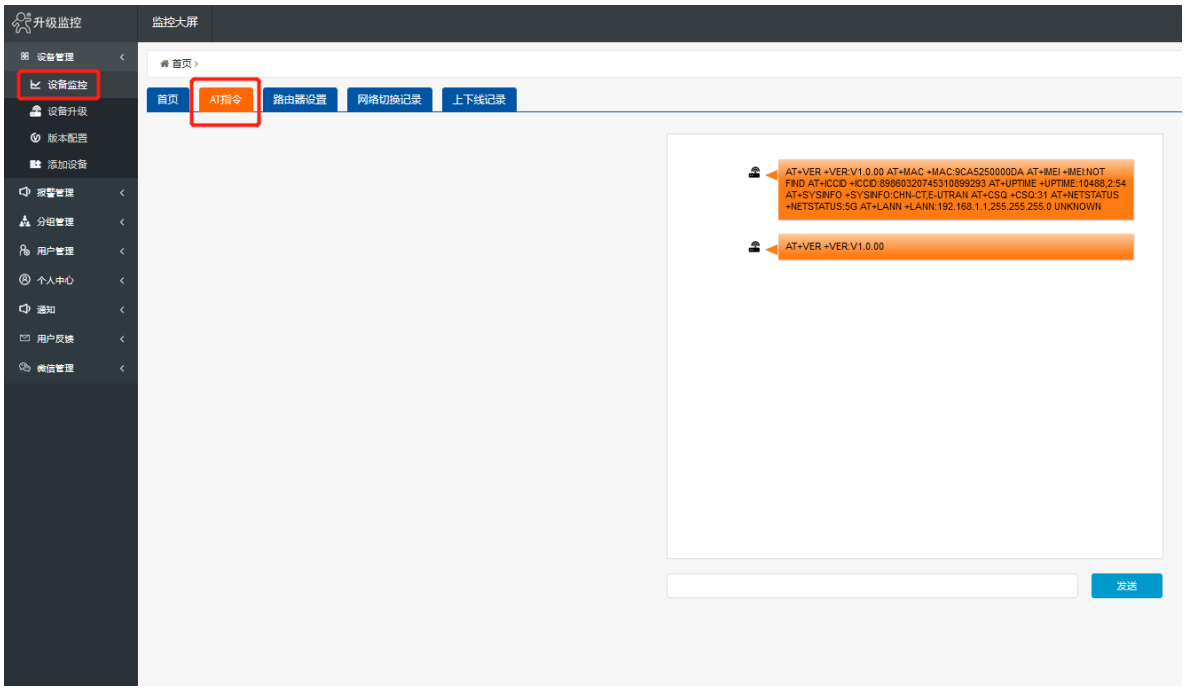


图 95　远程 AT 指令发送页面

AT 指令表汇总参见下表。AT 指令应用方式参加具体 AT 指令收发格式。

表 14　AT 指令汇总表

序号	名称	功能
版本相关		
1	AT+VER	版本查询
2	AT+MAC	MAC 查询
3	AT+ICCID	查询 iccid
4	AT+IMEI	查询 imei
5G 相关		

5	AT+NETSTATUS	查询网络连接方式
6	AT+SYSINFO	查询设备网络信息
7	AT+APN	APN 地址
8	AT+CSQ	信号质量
9	AT+MCCMNC	运营商信息(识别码)
10	AT+TRAFFIC	查询流量信息（上下行）
系统相关		
11	AT+UPTIME	查询运行时间
13	AT+WANN	查询设备 WAN 口 IP 地址
14	AT+LANN	设置/查询设备 LAN 口 IP 地址
15	AT+RELD	恢复到模块出厂设置
16	AT+Z	重启指令，备注：要回复+ok
远程监控与升级相关		
17	AT+UPDATE	查询/设置远程升级相关参数
18	AT+MONITOR	查询/设置远程监控相关参数
19	AT+HEARTPKT	查询/设置远程监控心跳包相关参数
系统 shell 指令相关		
20	AT+LINUXCMD	执行系统 shell 指令

7.1. AT+VER

功能：查询模块固件版本

格式：

查询：AT+VER<CR>

<CR><LF>+VER:<ver><CR><LF>

参数：

ver:查询模块固件版本，冒号后无空格，下同

格式：AA.BB.CC；AA 代表大版本，BB 代表小版本号，CC 代表硬件版本 C.C

举例

发送：AT+VER

返回：+VER:V1.0.2

7.2. AT+MAC

功能：查询模块 MAC

格式：

查询：AT+MAC<CR>

<CR><LF>+MAC=<mac><CR><LF>

参数：

mac：模块的 MAC（例如 01020304050A）

举例：

发送：AT+MAC

返回：+MAC:D8B04CD01234

7.3. AT+ICCID

功能：查询设备的 ICCID 码。

格式：

查询当前参数值：

AT+ICCID{CR}

{CR}{LF}+ICCID:code{CR}{LF}{CR}{LF}

参数：

code：ICCID 码。

举例

发送：AT+ICCID

返回：+ICCID:898600161515AA709917

7.4. AT+IMEI

功能：查询设备的 IMEI 码。

格式：

查询当前参数值：

AT+IMEI{CR}或 AT+IMEI?{CR}

{CR}{LF}+IMEI:code{CR}{LF}{CR}{LF}OK{CR}{LF}

参数：

code：IMEI 码。

举例

发送：AT+IMEI

返回：+IMEI:868323023238378

7.5. AT+NETSTATUS

功能：查询设备网络连接方式

格式：

查询当前参数值：

AT+NETSTATUS{CR}

{CR}{LF}+NETSTATUS:STATUS {CR}{LF}{CR}{LF}

参数：

STATUS(网络类型)：wired、5G

举例：

发送：AT+NETSTATUS

返回：+NETSTATUS: 5G

7.6. AT+SYSINFO

功能：查询设备网络信息

格式：

查询当前参数值：

AT+SYSINFO{CR}

{CR}{LF}+SYSINFO:operator,mode {CR}{LF}{CR}{LF}

参数：

openrator(运营商)： CHINA-MOBILE 中国移动

CHINA-UNICOM 中国联通

CHN-CT、CHINA-TELECOM 中国电信

mode(网络制式)： 3G Mode

4G Mode

5G Mode

举例，

发送：AT+SYSINFO

返回：+SYSINFO: CHINA-MOBILE,4G Mode

7.7. AT+APN

功能：查询/设置 APN 码。

格式：

查询当前参数值：

AT+APN{CR}

{CR}{LF}+APN:code,user_name,password{CR}{LF}{CR}{LF}OK{CR}{LF}

参数：

code：APN

user_name：用户名

password：密码

举例：

发送：AT+APN

返回：+APN:3gnet

7.8. AT+CSQ

功能：查询设备当前信号强度信息。

格式：

AT+CSQ{CR}

{CR}{LF}+CSQ: rssi<CR><LF>

举例：

发送：AT+CSQ

返回：+CSQ:31

7.9. AT+MCCMNC

功能：查询设备当前运营商信息（识别码）。

格式：

AT+MCCMNC{CR}

{CR}{LF}+MCCMNC: code<CR><LF>

举例：

发送：AT+MCCMNC

返回：+MCCMNC:460015521625317

7.10. AT+TRAFFIC

功能：查询流量信息

格式

AT+TRAFFIC<CR>

<CR><LF>+TRAFFIC:< dev_down，dev_up，pro_time，at_time>，<CR><LF>

参数：

dev_down：两时间戳之间的下行流量，以字节为单位

dev_up：两时间戳之间的上行流量，以字节为单位

pro_time：上次上报时间戳

at_time：本次上报时间戳

举例：

发送：AT+TRAFFIC

返回：+TRAFFIC: 111000000B、2000000B,1486379553,1486380161

两时间戳之间的下行流量 111MB，两时间戳之间的上行流量 2MB，上次上报的时间戳 1486379553

本次上报的时间戳：1486380161

7.11. AT+UPTIME

功能：查询模块启动时间（上电运行时间）

格式：

AT+UPTIME<CR>

<CR><LF>+UPTIME:<seconds,time><CR><LF>

参数：

seconds： 系统运行的总秒数

time ： 系统运行的 天、时 、分

举例：

发送：AT+UPTIME

返回：+UPTIME:14191,3:56

7.12. AT+WANN

功能：查询设备获取到的 WAN 口 IP（DHCP/STATIC）

格式：

AT+WANN<CR>

<CR><LF>+WANN=<mode,address,mask,gateway><CR><LF>

参数：

mode：网络 IP 模式。static：静态 IP； DHCP：动态 IP

address： IP 地址。

mask：子网掩码。

gateway：网关地址。

举例：

发送：AT+WANN

返回：+WANN:DHCP,192.168.225.23,255.255.255.0,192.168.225.1

7.13. AT+LANN

功能：查询设置 lan 口网关，掩码

格式：

AT+LANN<CR>

<CR><LF>+LANN:ip,netmask<CR><LF>

举例：

发送：AT+LANN

返回：+LANN:192.168.1.1,255.255.255.0

设置：

AT+LANN=ip,netmask<CR>

<CR><LF>+LANN:OK<CR><LF>

举例：

发送：AT+LANN=192.168.2.1,255.255.255.0

返回：+LANN:OK

7.14. AT+RELD

功能：恢复默认设置

格式：

AT+RELD<CR>

<CR><LF>+RELD:ok<CR><LF>

举例：

发送：AT+RELD

返回：+RELD:OK

7.15. AT+Z

功能：重启

格式：

AT+Z<CR>

<CR><LF>+Z:OK<CR><LF>

举例：

发送：AT+Z

返回：+Z:OK

7.16. AT+UPDATE

功能：设置查询远程升级参数

查询：

AT+UPDATE <CR>

<CR><LF>+UPDATE:status,ip,point,interval<CR><LF>

举例：

发送：AT+UPDATE

返回：+UPDATE:on,ycsj1.usr.cn,30001,1800

设置：

AT+UPDATE=status,ip,point,interval <CR>

<CR><LF>+UPDATE:OK<CR><LF>

举例：

发送：AT+UPDATE=on,ycsj1.usr.cn,30001,1800

返回：+UPDATE:OK

参数：

status： on(打开)，off(关闭)

ip： 远程升级服务器地址

point： 远程升级服务器端口

interval：状态信息上报时间

7.17. AT+MONITOR

功能：设置查询远程监控参数

查询：

AT+MONITOR<CR>

<CR><LF>+MONITOR:status,ip,point,interval<CR><LF>

举例：

发送：AT+MONITOR

返回：+MONITOR:on,ycsj1.usr.cn,30001,600

设置：

AT+MONITOR=status,ip,point,interval<CR>

<CR><LF>+MONITOR:OK<CR><LF>

举例：

发送：AT+MONITOR=on,ycsj1.usr.cn,30001,600

返回：+MONITOR:OK

参数：

status:on(打开)，off(关闭)

ip：远程监控服务器地址

point：远程监控服务器端口

interval：状态信息上报时间

7.18. AT+HEARTPKT

功能：设置查询远程监控心跳包参数

查询

AT+HEARTPKT<CR>

<CR><LF>+HEARTPKT:interval,data<CR><LF>

举例：

发送：AT+HEARTPKT

返回：+Heartpkt:30,Heartpkt

7.19. AT+LINUXCMD

CMP :linux 命令

功能：执行 linux 命令并且返回执行信息

格式

AT+LINUXCMD=cmd<CR>

<CR><LF>+LINUXCMD: result<CR><LF>

举例：

发送：AT+LINUXCMD=pwd

返回：+LINUXCMD：/bin

注：1.返回信息大于 10 行只显示前 10 行的内容

2.使用 cd 命令切换目录

8.联系方式

公 司：济南有人物联网技术有限公司

地 址：山东省济南市高新区新泺大街 1166 号奥盛大厦 1 号楼 11 层

网 址：http://www.usr.cn

客户支持中心：http://h.usr.cn

邮 箱：sales@usr.cn

企 业 QQ：8000 25565

电 话：4000-255-652 或者 0531-88826739

有人愿景：成为工业物联网领域生态型企业

公司文化：有人在认真做事!

产品理念：简单 可靠 价格合理

有人信条：天道酬勤 厚德载物 共同成长 积极感恩

9.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。

10. 更新历史

固件版本	更新内容	更新时间
V1.0.1	创立文档，完成相关功能描述	2020-08-01
V1.0.2	完善远程管理平台 AT 指令集、修改 AT 指令集格式错误、修改错误内容	2020-09-05
V1.0.3	修改 IPSec 案例、OpenVPN 描述说明、替换尺寸图 添加 PPTP、L2TP、OpenVPN 界面的 MTU、NAT、对端子网释义	2020-10-10
V1.0.4	添加 VPN 版本号、修改花生壳内网穿透截图、修改 AT 指令错误内容 新增 WiFi 传输距离、替换错误截图、修改错误内容 修改 5G 频段及上下行速率，新增 WCDMA 频段	2020-11-10

有人物联网 www.usr.cn | 联网找有人

模块 终端 云平台 物联网方案

可信赖的智慧工业物联网伙伴

山东有人信息技术有限公司

济南总部
地址：山东省济南市高新区新泺大街1166号奥盛大厦1号楼11层
电话：4000 255 652　0531-88826739
Email：sales@usr.cn

上海子公司
地址：上海市闵行区秀文路898号西子国际五号楼607、610室
电话：021-52960996　021-52960879

深圳办事处
地址：深圳市福田区华强北华强广场A座8G
电话：0755-27210561

武汉办事处
地址：武汉市高新大道426号华新大厦1901
电话：17754448760

北京办事处
地址：北京市海淀区上地十街1号院（辉煌国际广场）5号楼11层1114
电话：18653122839

成都办事处
地址：成都市高新区天府二街138号蜀都中心一期三号楼2805
电话：19915569197

销售联系方式
华东大区：房召猛　15553138586
华北大区：韩　彬　19953126860
华中大区：雷　爽　17754448760
华南大区：周万平　18665818916

关注有人微信公众号　登录商城快速下单