

4G 工业路由器

USR-G807

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	6
1.1. 产品特点	6
1.2. 技术参数	7
1.3. 硬件接口说明	8
1.4. 状态指示灯	9
1.5. 尺寸描述	10
2. 系统基本功能	10
2.1. Web 页面设置	10
2.2. Web 功能介绍	11
2.3. 系统功能框图	11
2.4. 主机名与时区	13
2.5. NTP 设置	13
2.6. 用户名密码设置	14
2.7. 参数备份与上传	14
2.8. 恢复出厂设置	15
2.9. 固件升级	16
2.10. 重启	17
2.11. 计划任务	17
3. 网络接口功能	18
3.1. 4G 接口	18
3.2. APN 设置	20
3.2.1. 修改 APN	20
3.2.2. 网络制式选择	21
3.2.3. 4G ping 检测	22
3.2.4. SIM 卡信息显示	22
3.3. LAN 接口	23
3.3.1. DHCP 功能	24
3.3.2. DHCP/DNS	25
3.4. WAN 口	26
3.5. 网络模式选择	26
3.6. WIFI 无线接口	27
3.7. 网络诊断功能	29
3.8. 主机名功能	30
3.9. 接口限速	30
4. VPN Client 功能	31
4.1. 概念介绍	31
4.2. PPTP Client 搭建	32
4.3. L2TP Client 搭建	34
4.4. IPSec 搭建	36
4.4.1. Road Warrior 模式	37
4.4.2. Net-to-Net 模式	39

4.5. OpenVPN 搭建	41
4.6. GRE 搭建	43
4.7. VPN + 端口转发	47
4.8. 静态路由	48
5. 防火墙功能	51
5.1. 基本设置	51
5.2. 通信规则	52
5.2.1. IP 地址黑名单	52
5.2.2. IP 地址白名单	54
5.3. NAT 功能	56
5.3.1. IP 地址伪装	56
5.3.2. SNAT	57
5.3.3. 端口转发	59
5.3.4. NAT DMZ	60
5.4. 自定义规则	61
5.5. 访问限制	62
5.5.1. 域名黑名单	62
5.5.2. 域名白名单	62
5.6. 网速控制	63
6. 高级服务功能	64
6.1. 花生壳内网穿透	64
6.2. 动态域名解析 (DDNS)	68
6.2.1. 已支持的服务	68
6.2.2. 自定义的服务	70
6.2.3. 功能特点	71
6.3. 远程管理	72
6.3.1. 远程平台	72
6.3.2. 远程升级	74
6.3.3. 远程监控	75
7. DTU 功能	76
7.1. 工作模式	76
7.1.1. 网络透传模式	77
7.1.2. HTTPD 模式	79
7.1.3. 协议(UDC)透传模式	81
7.2. 串口	83
7.2.1. 基本参数	83
7.2.2. 成帧机制	84
7.3. 特色功能	85
7.3.1. 注册包功能	85
7.3.2. 心跳包机制	87
7.3.3. 透传云功能	88
8. AT 指令集	91
8.1. AT+VER	92

8.2. AT+MAC	93
8.3. AT+ICCID	93
8.4. AT+IMEI	93
8.5. AT+SYSINFO	93
8.6. AT+APN	94
8.7. AT+CSQ	94
8.8. AT+TRAFFIC	95
8.9. AT+NETMODE	95
8.10. AT+UPTIME	95
8.11. AT+WANN	96
8.12. AT+LANN	96
8.13. AT+WEBU	96
8.14. AT+PLANG	97
8.15. AT+CLEAR	97
8.16. AT+DHCPEN	97
8.17. AT+UPDATE	98
8.18. AT+MONITOR	98
8.19. AT+HEARTPKT	98
8.20. AT+LINUXCMP	99
8.21. AT+UART	99
8.22. AT+UARTFT	99
8.23. AT+UARTFL	100
8.24. AT+SOCKA	100
8.25. AT+SOCKB	100
8.26. AT+SOCKC	101
8.27. AT+SOCKD	101
8.28. AT+SOCKAEN	101
8.29. AT+SOCKBEN	102
8.30. AT+SOCKCEN	102
8.31. AT+SOCKDEN	102
8.32. AT+SOCKALK	103
8.33. AT+SOCKBLK	103
8.34. AT+SOCKCLK	103
8.35. AT+SOCKDLK	103
8.36. AT+SOCKIND	104
8.37. AT+REGEN	104
8.38. AT+REGTP	104
8.39. AT+REGDT	105
8.40. AT+REGSND	105
8.41. AT+CLOUD	105
8.42. AT+HEARTEN	106
8.43. AT+HEARTDT	106
8.44. AT+HEARTSND	106

8.45. AT+HEARTTM	106
8.46. AT+HTPTP	107
8.47. AT+HTPURL	107
8.48. AT+HTPSV	107
8.49. AT+HTPHD	108
8.50. AT+HTPTO	108
8.51. AT+HTPFLT	108
9. 联系方式	109
10. 免责声明	110
11. 更新历史	111

1. 产品简介

USR-G807 是一款带串口的高性能工业 4G 无线路由器，同时具备强大的 DTU 功能，利用公用无线网络，为用户提供了一种工业 4G 路由器和 DTU 的集成解决方案。

产品采用高性能嵌入式 CPU，工作频率高达 580MHz，基于多样的硬件接口+强大的软件功能，用户可以快速组建自己的应用网络。该产品已经在物联网产业链中的 M2M 行业广泛应用，为智能电网、个人医疗、智能家居、自助终端、工业自动化、环保农业、市政服务等领域提供可靠的数据传输组网。

1.1. 产品特点

- 支持 1 个有线 LAN 口，1 个有线 WAN 口（WAN 口可切换成 LAN 口）；
- 支持 2.4GWIFI 无线局域网 AP 功能；
- 支持多个 LED 通信指示灯；
- 支持 SSH、TELNET、Web 多平台管理配置方式；
- 支持一键恢复出厂设置；
- 有线网口均支持 10/100Mbps 速率；
- 支持有线/4G 多网同时在线、多网智能切换备份功能；
- 支持 VPN Client(PPTP/L2TP/IPSec/GRE/OpenVPN)，并支持 VPN 加密和静态 IP 功能；
- 支持 APN 自动检网、2/3/4G 制式切换、SIM 信息显示，支持 APN/VPDN 专网卡；
- 支持有线无线多网同时在线、多网智能切换备份功能；
- 支持远程升级、远程监控；
- 支持花生壳内网穿透、动态域名（DDNS）、静态路由、PPPOE，DHCP，静态 IP 功能；
- 支持防火墙、NAT、DMZ 主机、访问控制的黑白名单、IP 限速、NTP、MAC 限速；
- 支持串口 AT 指令；
- 支持 4 个网络连接同时在线，支持 TCP Server,TCP Client,UDP Server 和 UDP Client；
- 每路连接支持 20KB 串口数据缓存，连接异常时可选择缓存数据不丢失；
- 支持发送注册包/心跳包数据；
- 支持多种工作模式：网络透传模式、HTTPD 模式、UDC 模式、透传云；
- 支持基本指令集；
- 支持外部硬件看门狗设计，保证系统的稳定性。

1.2. 技术参数

USR-G807 路由器参数如下表

表 1 USR-G807 基本参数

项目		型号/规格	
产品名称	4G 无线路由器	USR-G807	
有线网口	有线 WAN 口	1*WAN/LAN	
	有线 LAN 口	1*LAN	
WIFI	WIFI 无线局域网	支持 IEEE802.11b/g/n, 2.4GHz AP 模式	
	天线	1 个/3dbi 输出增益棒状天线	
	覆盖距离	空旷地带 100m	
频段信息	TDD-LTE	下行速率 130Mbps 上行速率 35Mbps Band 38/39/40/41	
		FDD-LTE	下行速率 150Mbps 上行速率 50Mbps Band 1/3/5/8
			WCDMA
	CDMA2000	下行速率 3.1Mbps 上行速率 1.8Mbps CDMA1X/ 1xEV-DO rel.0/ 1xEV-DO rev. A: 800 MHz	
		TD-SCDMA	下行速率 4.2Mbps 上行速率 2.2Mbps Band 34/39
	GSM/GPRS/EDGE		MAX:下行速率 384kbps 上行速率 128kbps 900/1800MHz
		SIM 卡天线	SIM/USIM 卡
	天线		1 个/2.5dbi 棒状天线
	DTU	DTU 模式	NET,HTTPD,UDC 模式
		心跳包/注册包	支持
		波特率	2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
		数据位	8

	停止位	1, 2
	校验位	NONE,ODD,EVEN,MARK
	串口类型	RS485
	SOCKET	支持四路可选择 TCPS (仅 SOCKA 支持) /TCPC/UDPS/UDPC
按键	Reload	一键恢复出厂设置
指示灯	状态指示灯	电源, WIFI,2/3/4G, 信号强度指示灯, WAN 口, LAN 口
温度	工作温度	-20°C ~ +70°C
	存储温度	-40°C ~ +125°C
湿度	工作湿度	5% ~ 95%RH (无凝露)
	存储湿度	1% ~ 95%RH (无凝露)
供电	供电电压	DC9 ~ 36V
	电流消耗	在 DC12V 供电下, 平均电流 270mA, 最大电流 400mA

<注意>

➢ USR-G807 路由器, 支持全网通, 移动、联通、电信的 2G/3G/4G 网络。

<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, 4G 访问外网, 10KByte/s 的数据传输速率。

表 2 USR-G807 功耗表

工作方式	供电电压	平均电流	最大电流
LAN+WAN 全速通信 (4G 正常+WALN 正常)	DC12V	151mA	385mA
单独 LAN 口全速通信 (4G 正常+WALN 正常)	DC12V	270mA	400mA
LAN+WAN 全速通信 (4G 无卡+WALN 正常)	DC12V	130mA	236mA
LAN+WAN 全速通信 (4G 无卡+WALN 正常)	DC12V	128mA	295mA

USR-G807 在 12V 供电并全速工作时, 统计得出:

平均功耗 3.24W, 最大功耗 4.8W。平均电流 270mA, 最大电流 400mA。

1.3. 硬件接口说明

硬件接口描述如下

表 3 接口描述

序号	名称	备注
1	DC 电源座	供电范围 DC:9~36V, 标准 5.5*2.1 电源座
2	DC 电源端子	供电范围 DC:9~36V, 绿色端子座, 端子尺寸 5.08mm-2, 注意正负极性防止接错
3	WAN/LAN 口	1*10/100M RJ45 类型以太网口, 自适应 MDI/MDIX, 具备 1.5KV 电磁隔离保护
4	LAN 口	1*10/100M RJ45 类型以太网口, 自适应 MDI/MDIX, 具备 1.5KV 电磁隔离保护
5	调试串口 TBD	1 个
6	485 串口	1*标准 3.81mm*3 针(A,B,G)接口
7	指示灯	9 路状态指示灯, 说明详见指示灯章节的描述

8	SIM 卡座	抽屉式 SIM 卡卡托。如果需要安装 SIM 卡，需要使用尖锐物顶住一侧的黄色按钮，将卡托退出
9	Reload 按键	Reload: 长按 5s 以上再松开，恢复出厂设置
10	WIFI 天线	2.4G 棒状天线
11	全频天线	全频棒状天线
12	保护接地点	侧面带有接地螺丝，建议使用时将该点与地线连接



<保护接地安装具体步骤如下>

- 将接地螺钉拧下来-->将地线的接地环套进接地螺钉上-->将接地螺钉拧紧-->地线接地；
- 为提高路由器整机抗干扰能力，路由器在使用安装时，需根据具体环境将地线接到路由器接地螺栓上；
- 关于 WIFI 天线跟 4G 天线的区分。在天线的尾端有有相关标识。

1.4. 状态指示灯

共有 9 个状态指示灯，含义如下

表 4 指示灯说明表

名称	说明
PWR	上电后长亮
WAN	WAN 口网线插入时亮起，数据通信时闪烁
LAN	LAN 口网线插入时亮起，数据通信时闪烁
WLAN	WIFI 正常工作时亮起
2G 指示灯	LTE 模块工作在 2G 时亮起
3G 指示灯	LTE 模块工作在 3G 时亮起
信号强度 (1-3)	信号强度指示灯亮起的灯越多，信号越强

<说明>

- 2/3/4G 指示灯，是否亮起反映了 USR-G807 联网成功与否（是最重要的指示灯）；
- WIFI 启动成功后，WLAN（或者叫 WIFI）指示灯长亮；
- WAN 与 LAN 的工作状况，由 WAN 以及 LAN 指示灯来指示；
- 当网线接入，且在对端的网络设备也在工作，这时对应的 WAN/LAN 指示灯才会闪烁；
- 电源灯将一直长亮；
- LTE 模块工作在 4G 时，2G 指示灯和 3G 指示灯都亮起。

1.5. 尺寸描述

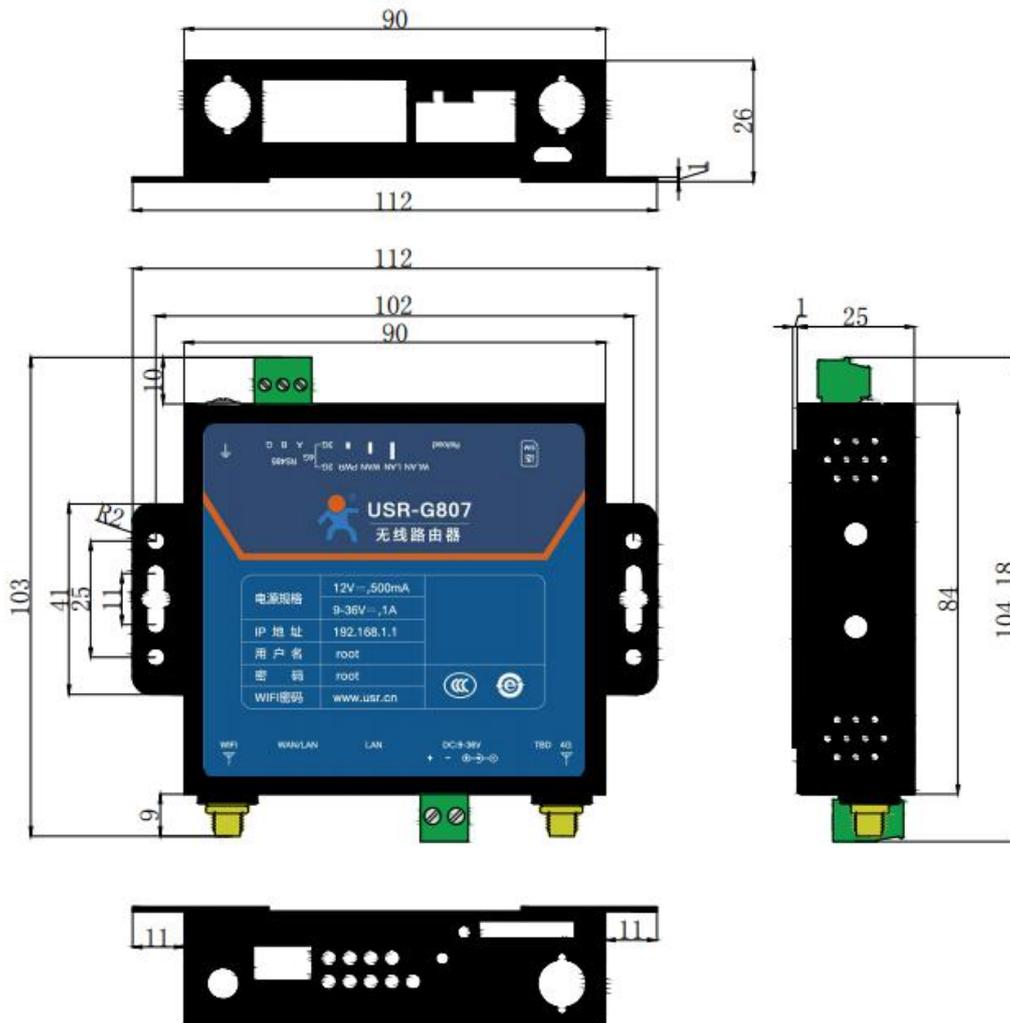


图 1 USR-G807 尺寸图

- 钣金外壳，两侧固定孔，兼容导轨安装件；
- 长宽高分别为 90 * 84.0 * 26.0mm（不含电源端子，RS485 端子，挂耳，天线及天线座）。

2. 系统基本功能

2.1. Web 页面设置

首次使用 USR-G807 设备时，可以通过 PC 连接 USR-G807 的 LAN 口，或者连接上 WLAN 无线，然后用 web 管理页面配置。默认情况下，USR-G807 的 AP 默认名称为 USR-G807-xxxx，IP 地址和用户名、密码如下：

表 5 USR-G807 网络默认设置表

参数	默认设置
SSID	USR-G807-XXXX
LAN 口 IP 地址	192.168.1.1

用户名	root
密码	root
无线密码	www.usr.cn

首先用 PC 的无线网卡，USR-G807 的默认 SSID 为 USR-G807-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-G807 的管理页面。USR-G807 管理页面默认中文。

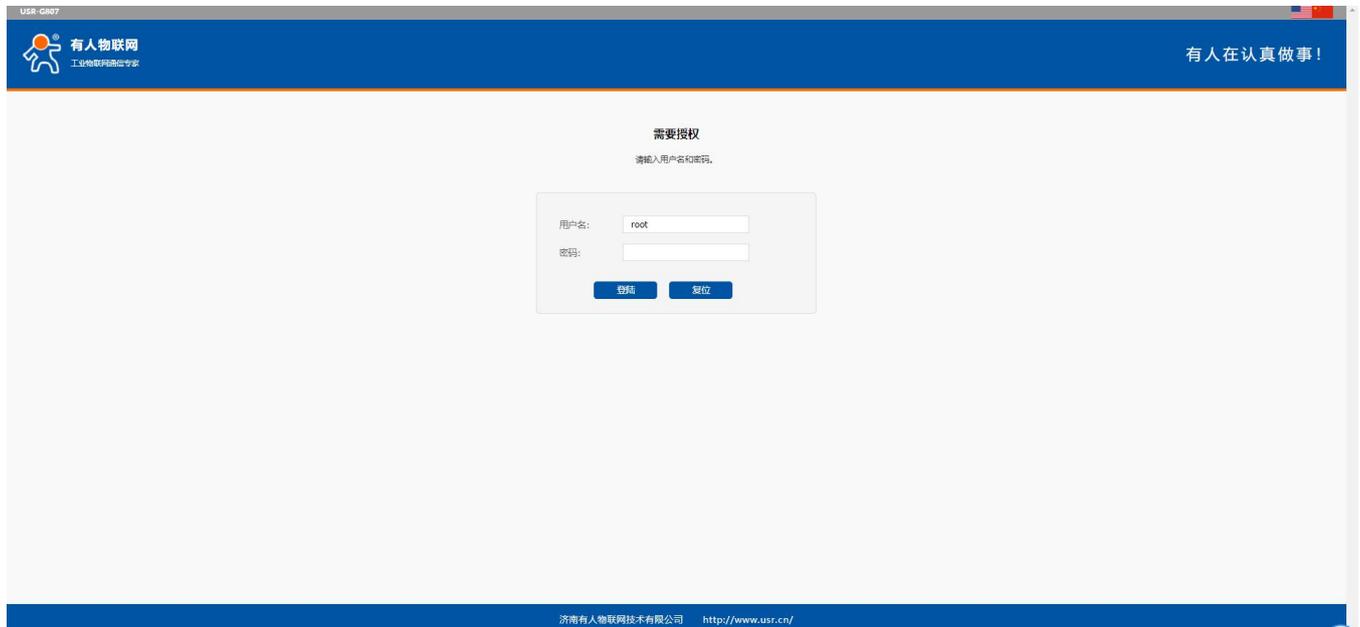


图 2 首页页面

2.2. Web 功能介绍

在网页的左边是标签页，可以具体设置模块的一些参数。

- 状态：主要显示设备的名称信息、固件版本、运行状态等；
- 服务：主要是一些高级功能，包括内网穿透、动态 DNS、强制门户、远程管理、基站信息；
- 网络：设置接口、无线 WiFi、无线客户端、APN、VPN 协议等信息；
- 防火墙：设置出入站规格、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、固件升级等。

2.3. 系统功能框图

本章介绍一下 USR-G807 所具有的功能，下图是模块的功能的整体框图。

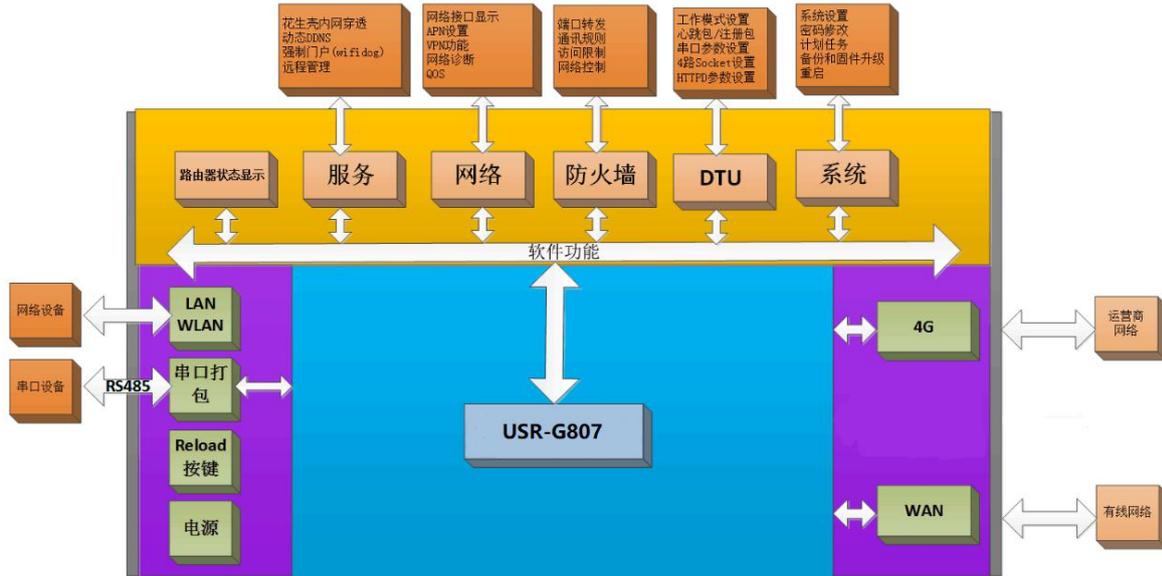


图 3 功能框图

接口对照表：

表 6 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
默认的 WIFI AP 接口	ra0	LAN
有线 WAN 口	eth0.2	WAN_WIRED
4G 接口	eth1	WAN_4G

下图为应用示意图。

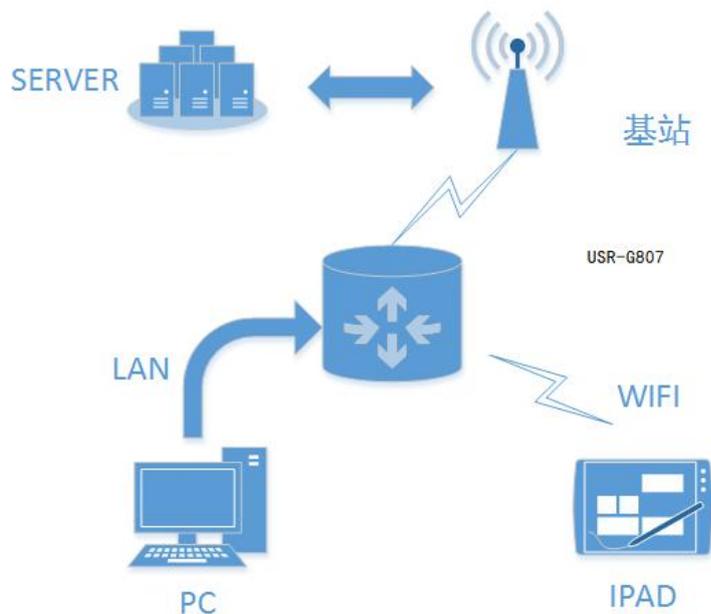


图 4 应用示意图

<说明>

- 用户设备或电脑，可以通过 USR-G807 的有线 LAN 口或者 WIFI 接口，来访问外网；
- 如果使用普通手机卡，无需任何设置，通电即可上外网。

2.4. 主机名与时区

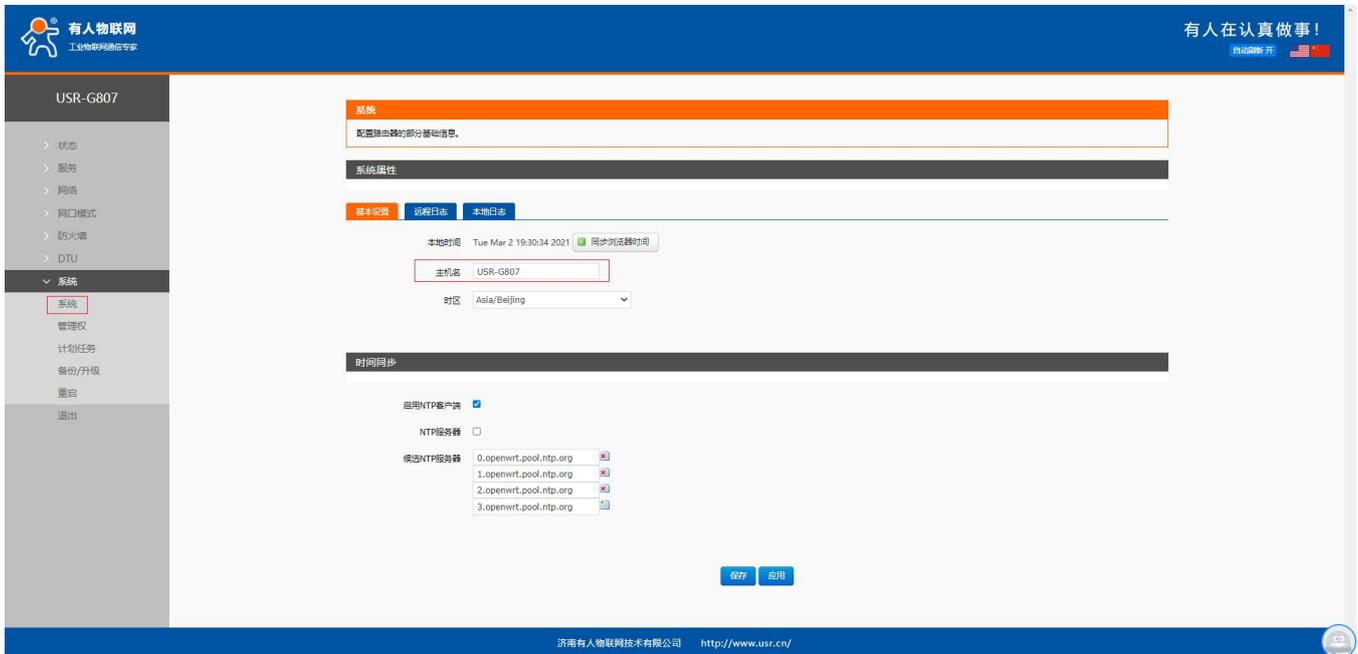


图 5 主机名和时区设置页面

路由器自身主机名默认 USR-G807，时区为北京时区。

2.5. NTP 设置

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。

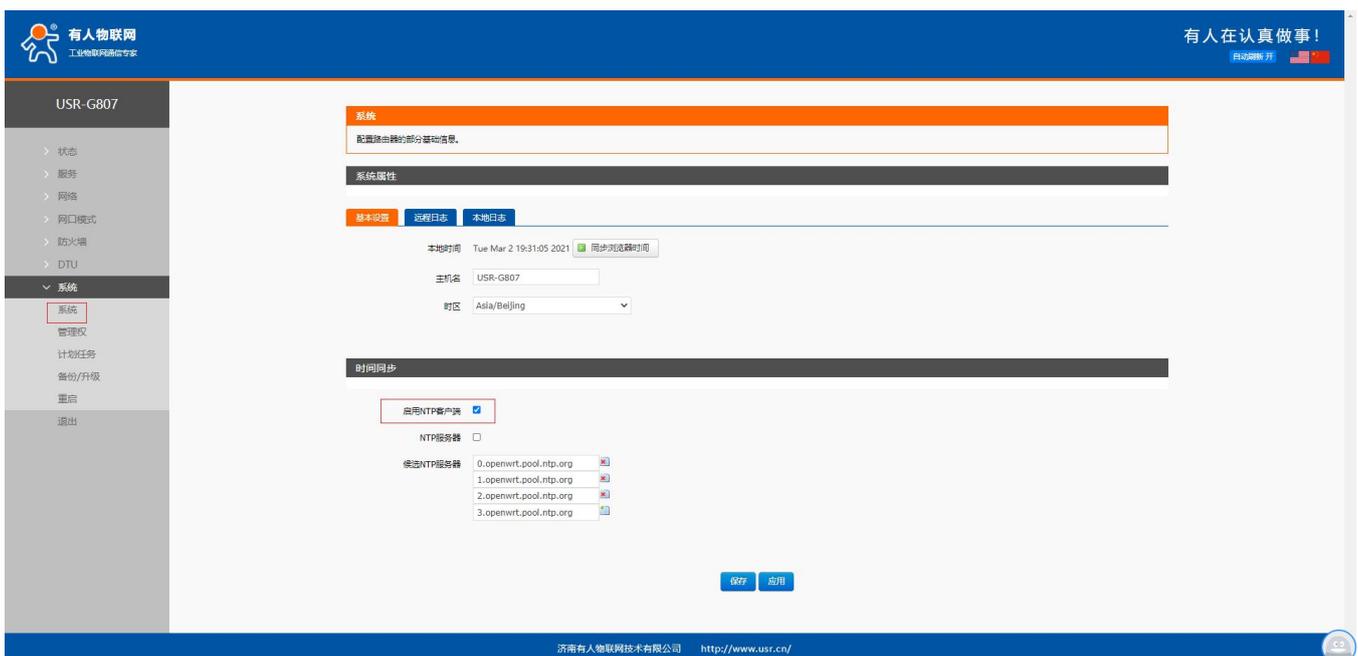


图 6 NTP 页面

2.6. 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）。

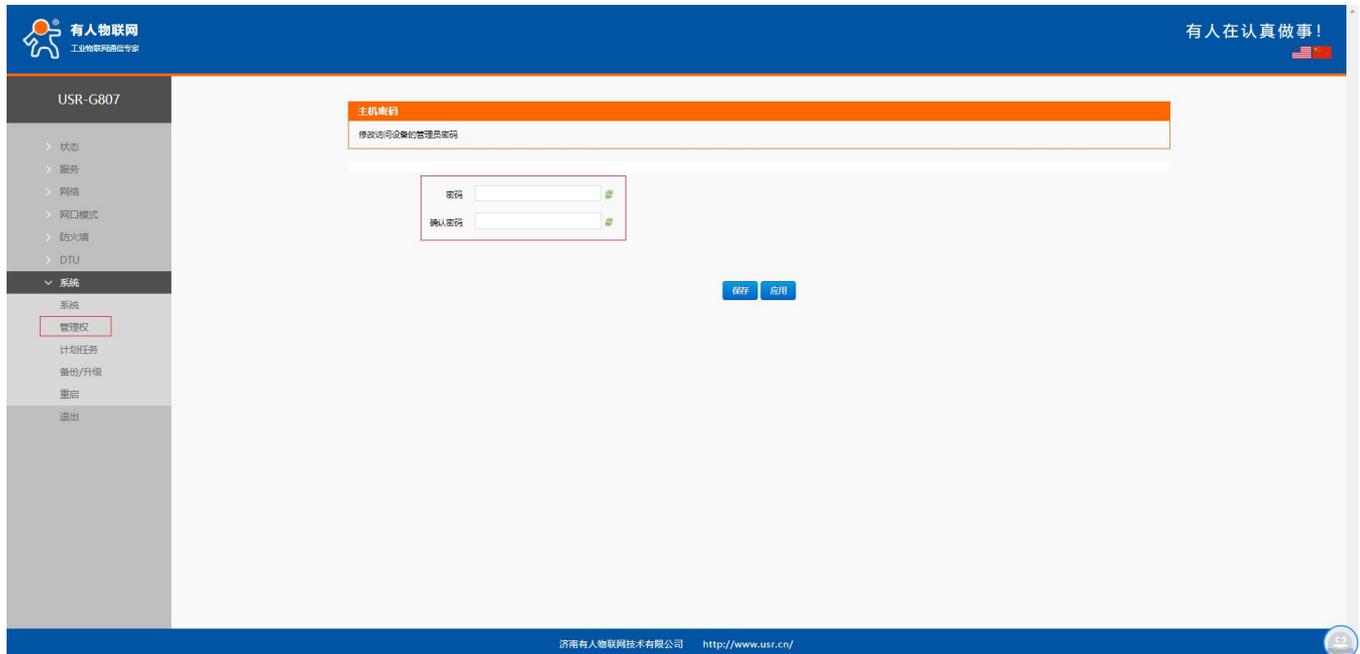


图 7 用户名密码设置页面

2.7. 参数备份与上传

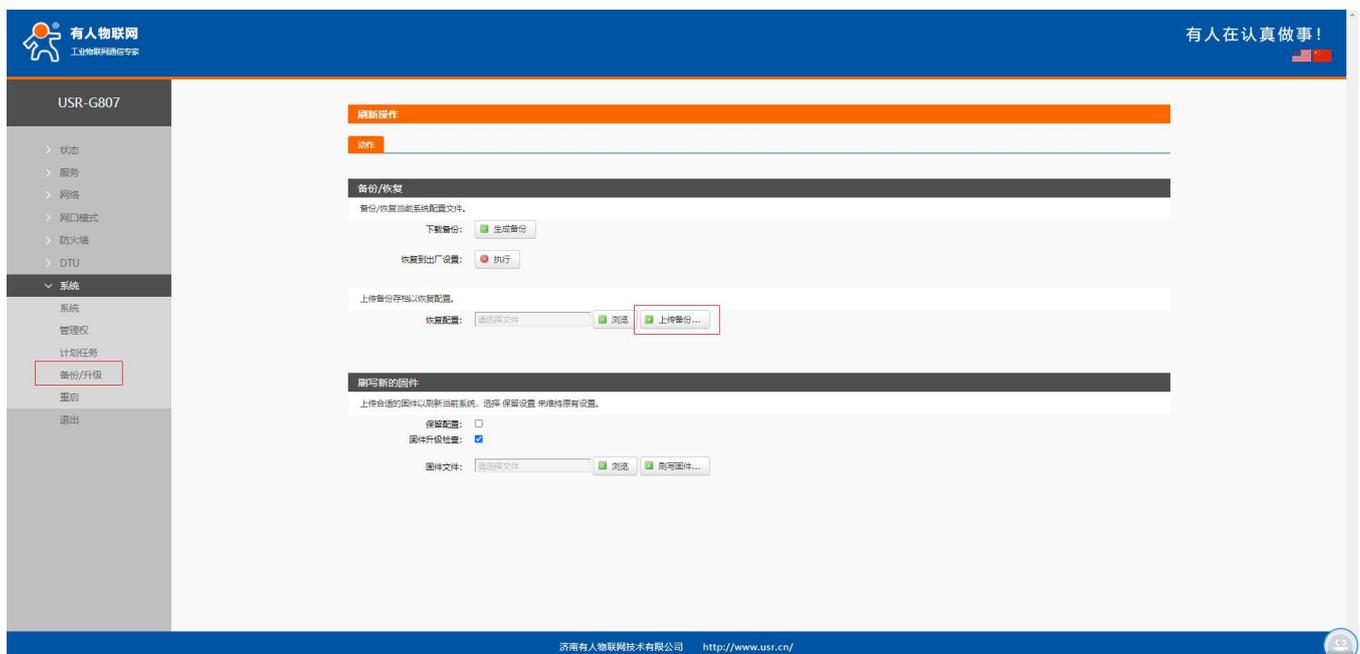


图 8 参数备份上传页面

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。

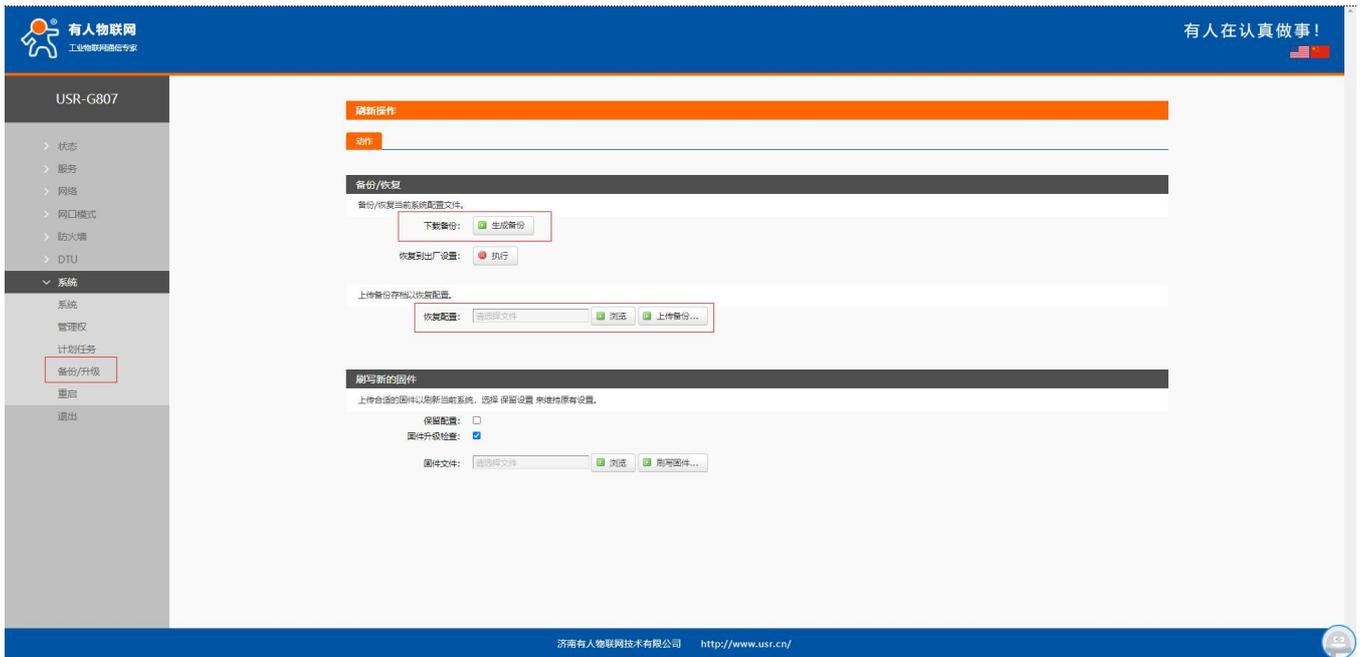


图 9 备份/恢复页面

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-G807-2018-04-20.tar.gz，并保存到本地。

2.8. 恢复出厂设置

通过网页可以恢复出厂参数设置。

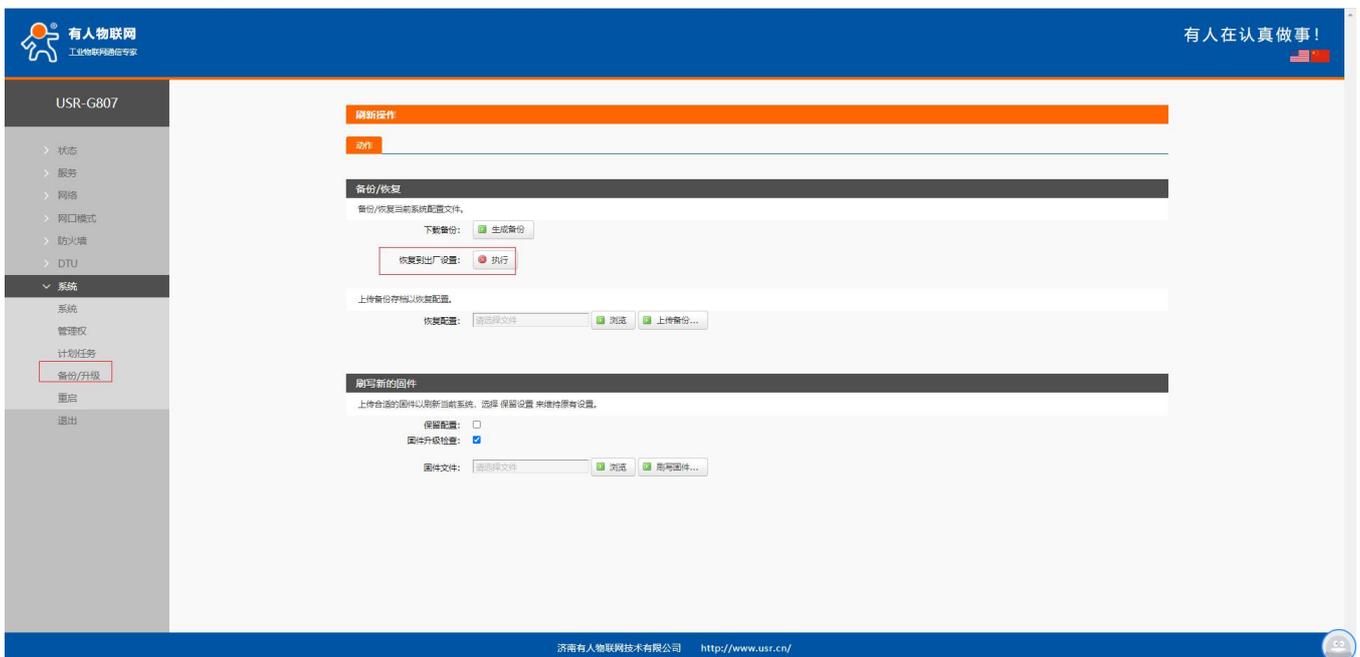


图 10 恢复出厂页面

点击按钮恢复出厂设置，本功能，与硬件的 Reload 按键功能一致。Reload 按键的使用

- 长按 5s 以上然后松开，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 1 次，然后又掉（电源灯不灭）。

2.9. 固件升级

USR-G807 模块支持 web 方式的在线固件升级。

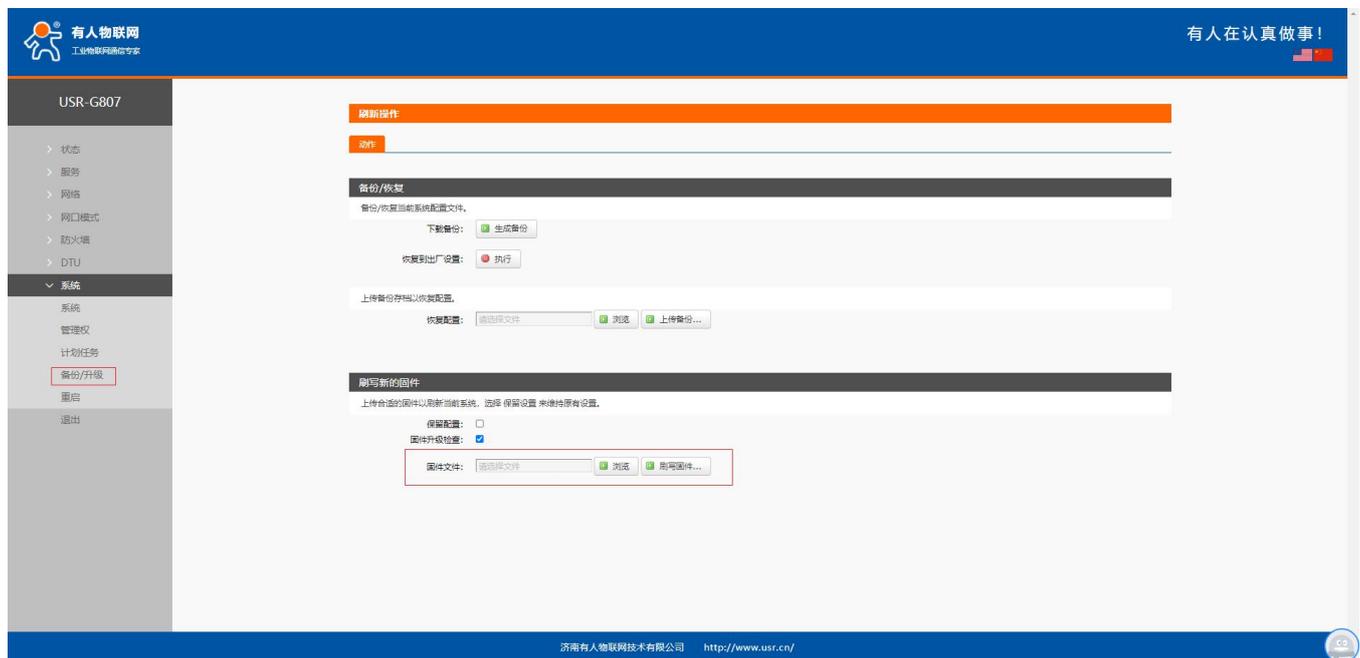


图 11 升级页面

<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”；
- 固件烧录过程中请不要断电或者拔网线。

2.10. 重启

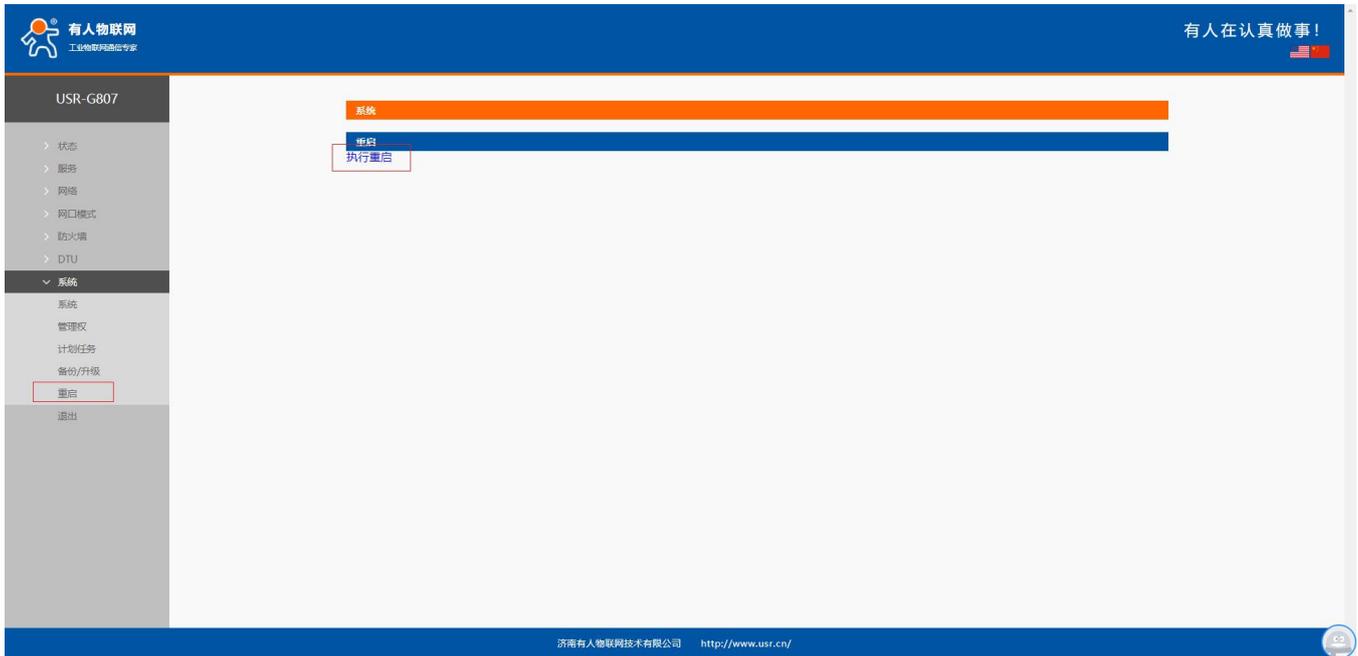


图 12 重启页面

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。

2.11. 计划任务

<注意>

➢ 本功能不可删除原有的计划任务，否则可能导致路由器运行不正常。

本路由器预留了计划任务的接口可以方便用户对路由器进行定时的管理。页面如下

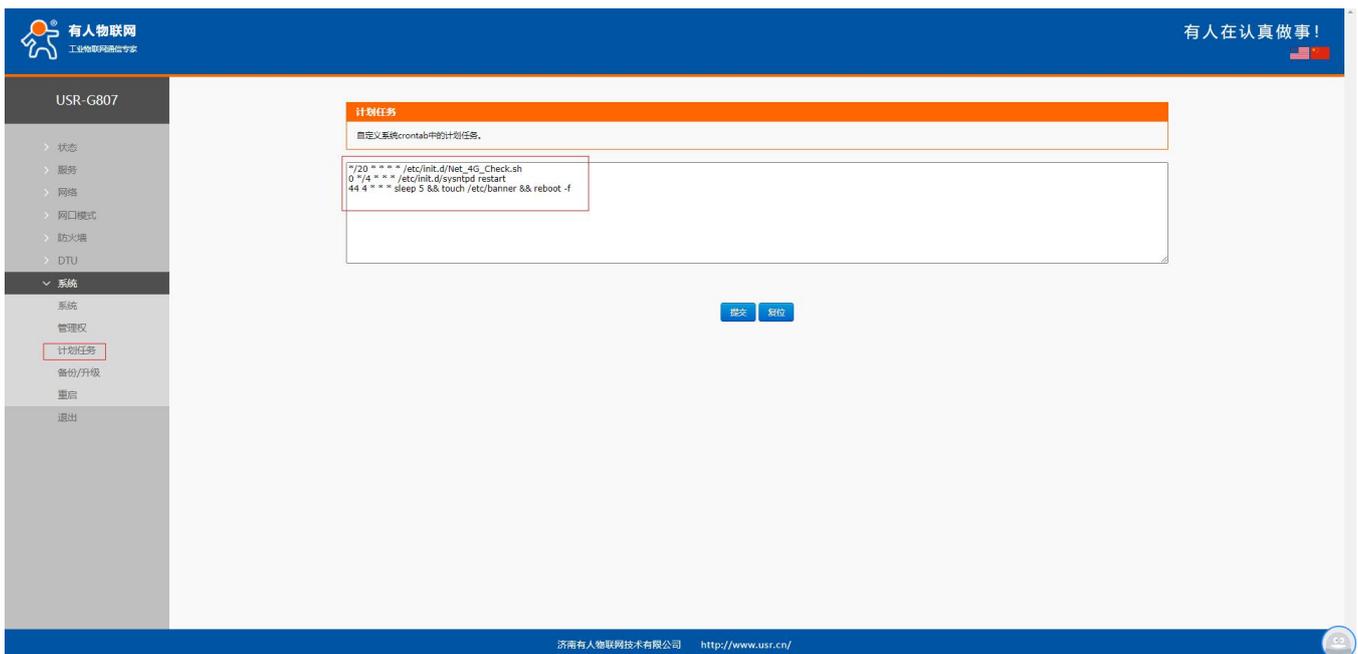


图 13 计划任务设置页面

如需添加定制任务，只需要在输入框内另起一行，输入相关的定时任务指令即可。

计划任务列表的格式：

[minute] [hour] [day of month] [month] [day of week] [program to be run]

其中各个参数的取值范围是：

minute(0-59)、hour(0-23)、day of month(1-31)、month(1-12)、day of week(0-7,0 or 7 is Sun)

每个参数里的取值可以有 4 种间隔符：

* 表示任意

- 表示范围

, 表示枚举多个值

/ 表示每隔

例如：

周一到周五每天晚上 23:30 执行 ifconfig ra0 down 指令（关掉 wifi 网卡）

```
30 23 * * 1-5 ifconfig ra0 down
```

周一到周五每天晚上 7:30 执行 ifconfig ra0 up 指令（开启 wifi 网卡）

```
30 7 * * 1-5 ifconfig ra0 up
```

每天每隔 10 小时执行 reboot 指令（重启路由器）

```
**/10 *** reboot
```

<说明>

- 原有第 2 条计划任务为每隔 20 分钟进行 4G 联网检测，不可删除，删除后会影响路由器正常使用；
- 原有第 5 条计划任务 44 4 * * * reboot，为每天 4:44 重启路由器
- 每日 04:44 定时重启路由器计划任务，如不需该功能，删除该条后点击“应用”，重启设备即可。
- 计划任务可根据需要自行定义添加，提交修改后重启设备生效；
- 如需添加定制任务，只需要在输入框内另起一行，输入相关的定时任务指令即可。

3. 网络接口功能

3.1. 4G 接口

本路由器支持一路 4G/3G/2G 通信模块接口，用来访问外部网络。

下图为 4G 接口功能框图。

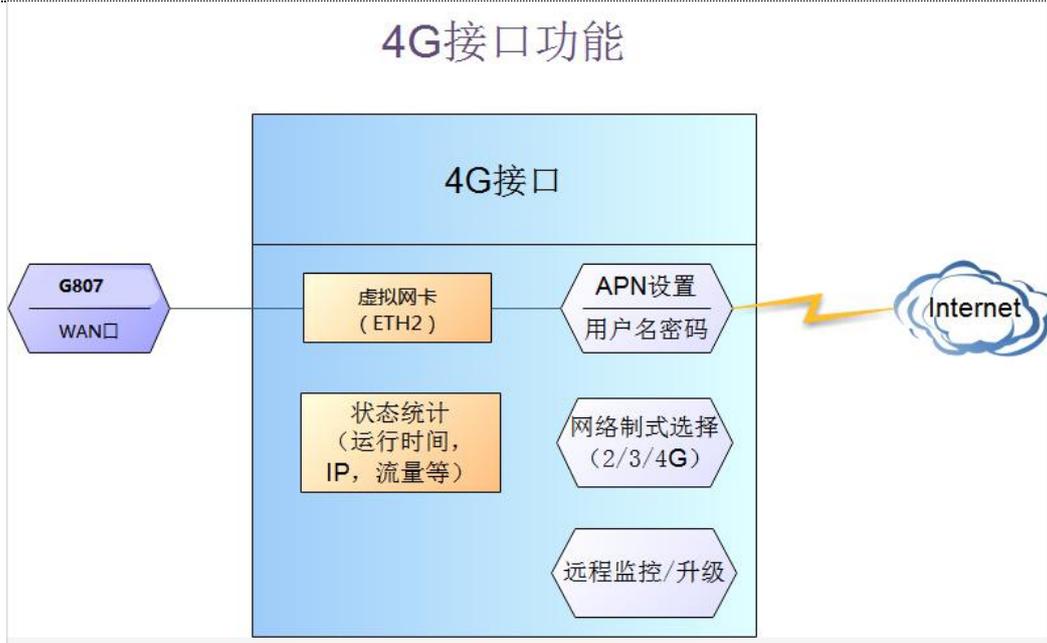


图 14 4G 功能示意图

网页界面如下。

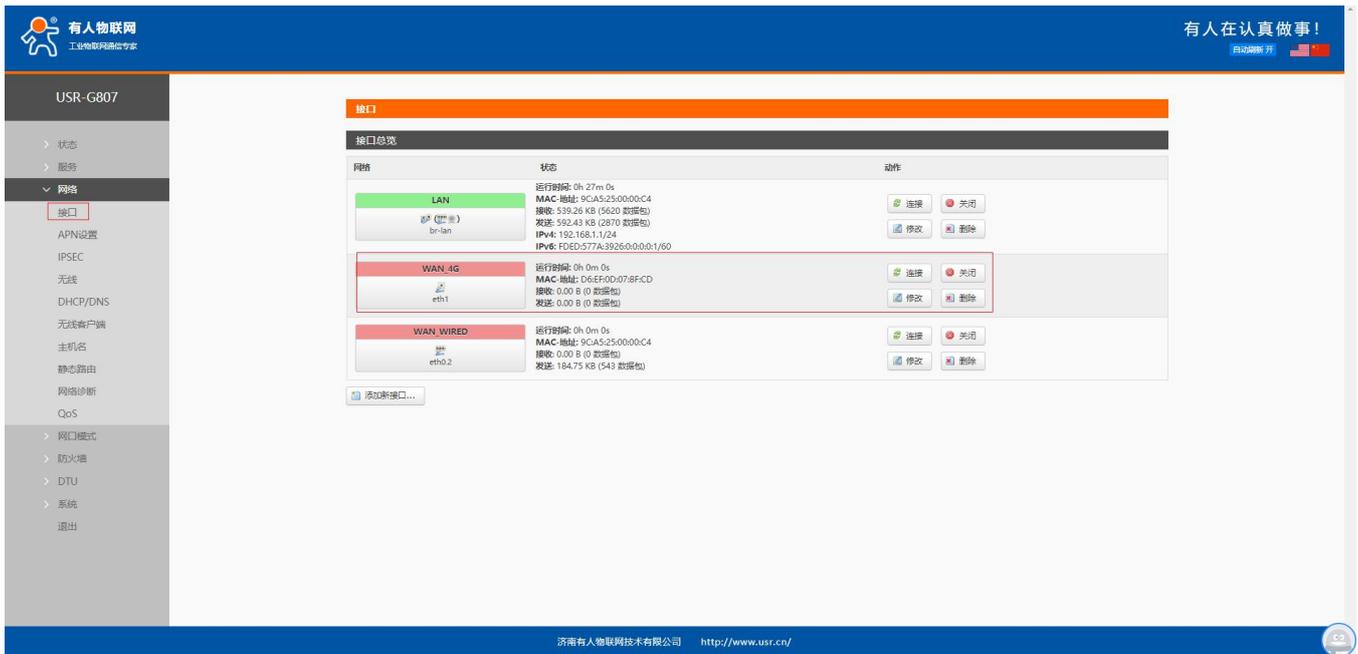


图 15 4G 设置页面

对于状态栏的显示如下，如果运行时间为 0，代表本网卡未能成功运行。

表 7 状态表

序号	名称	含义
1	运行时间	本接口自从最近上电开始的累计运行时间
2	MAC 地址	本网卡接口的 MAC 地址
3	接收/发送	本网卡累计的接收与发送数据统计
4	IPv4	代表本网卡使用 IPv4 协议

<说明>

- 4G 接口的协议：请勿修改，保持默认；
- 路由器将优先使用有线 WAN 口，其次是使用 4G 网络；
- 如果您使用 APN 专网，请参考 APN 章节的介绍。

3.2. APN 设置

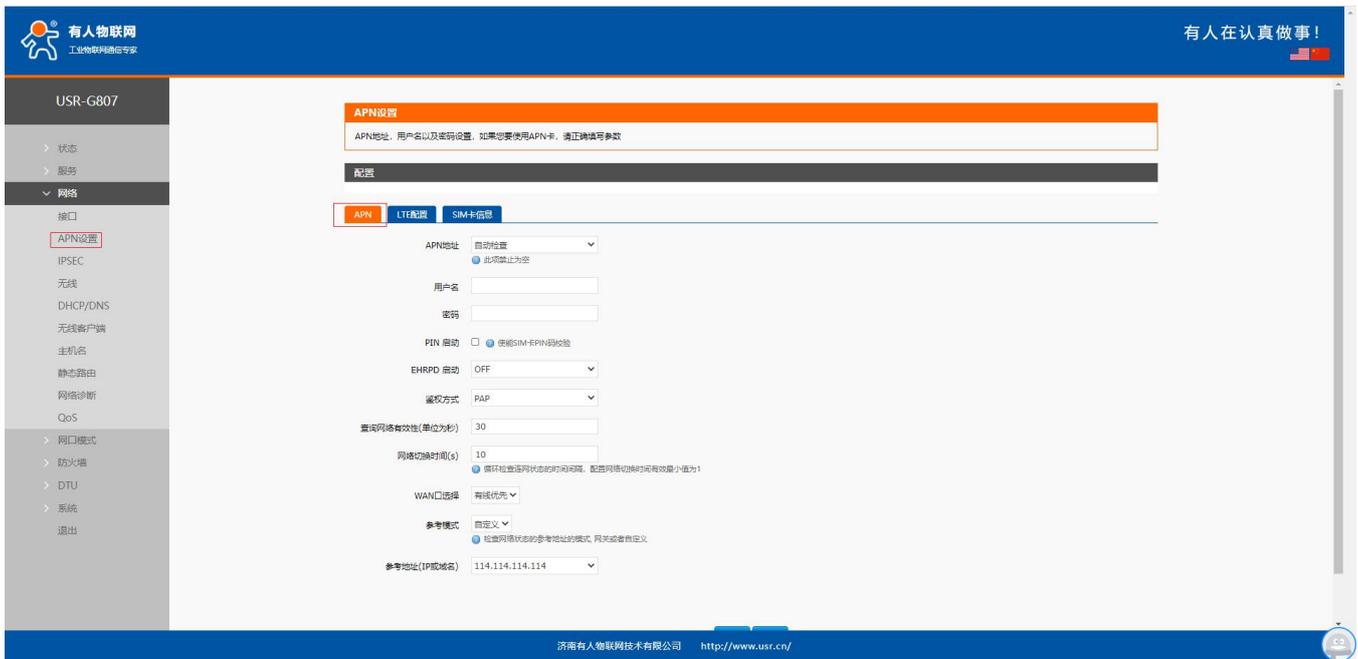


图 16 APN 设置页面

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 8 APN 参数表

参数名称	数值以及功能
APN 地址	请填写正确的 APN 地址
用户名	默认为空。如使用 APN 卡请填写
密码	默认为空。如使用 APN 卡请填写
PDP 类型	默认即可
鉴权方式	默认即可
其他	请保持默认

<注意>

- 普通的 4G 手机卡上网，可不用关心 APN 设置；
- 如果使用了 APN 专网卡，务必要填写 APN 地址，用户名跟密码。

3.2.1. 修改 APN

首先，在 APN 地址处，选择“自定义”选项，然后根据要求填写准确的 APN 地址。设置成功后，重启路由器生效。

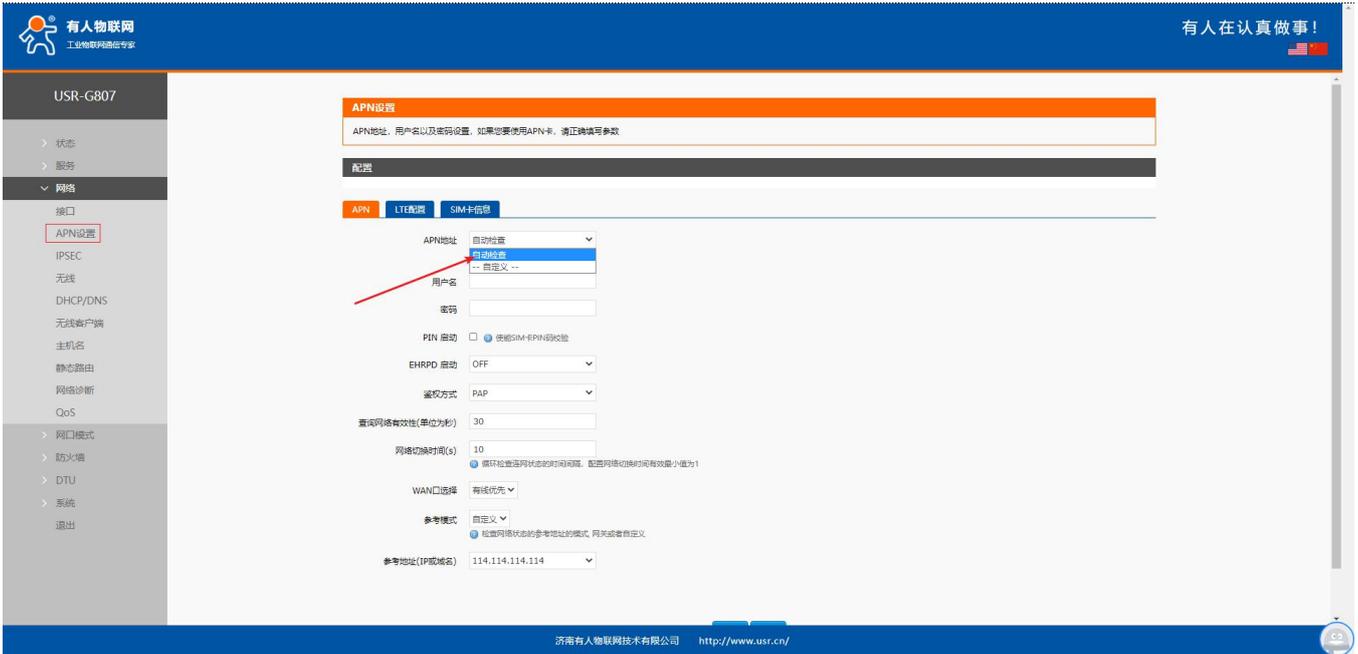


图 17 APN 地址选择页面

3.2.2. 网络制式选择

4G 路由器的联网网络制式，默认设置为自动，也就是 4G->3G->2G 的优先级，自动选择联网。

如果不是 4G 的 SIM 卡，或者网络需要指定(比如您指定要使用 2G 或者 3G 网络)，则需选定网络制式（不然会影响到联网速率等），如下：

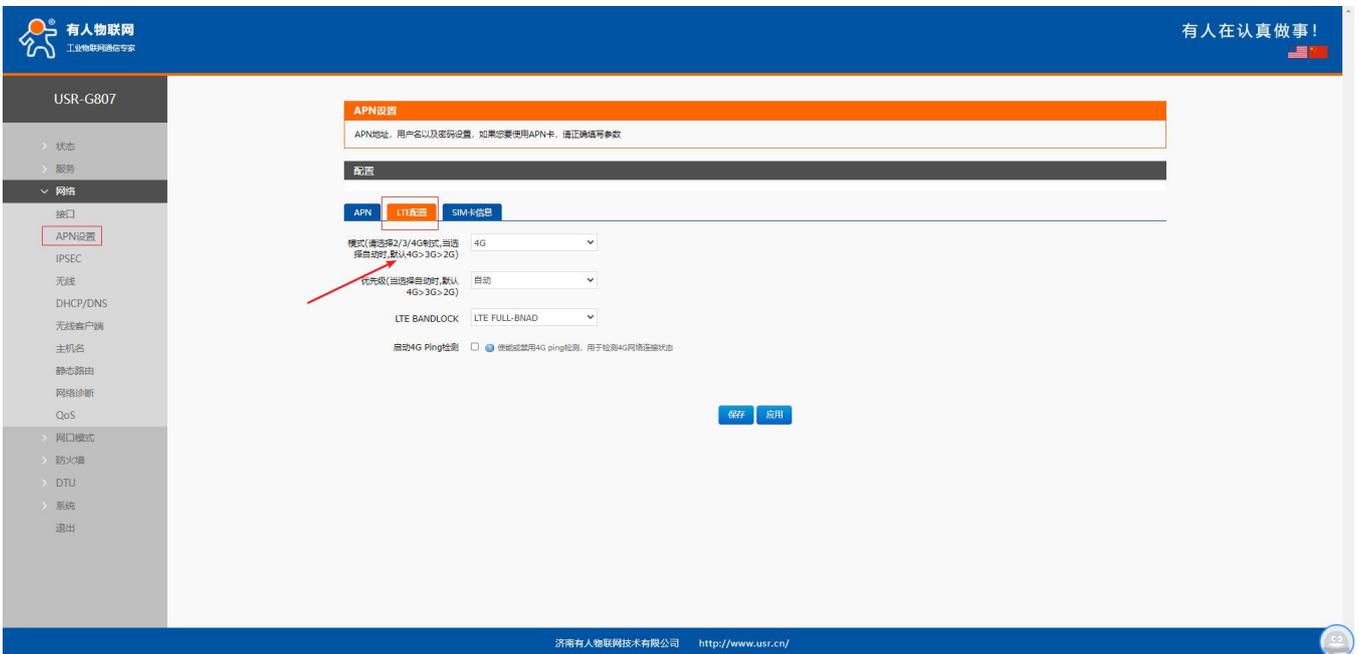


图 18 网络制式选择

例如选择了 3G 模式和 3G 优先时，4G 路由器在联网时，可更准确选择连接相应的 3G 网络。各种选项对应如下：

表 9 制式选择表

选项	解释	切换顺序	备注
自动	自动网络制式选择	4G>3G>2G	默认配置

2G	仅使用 2G 网络	2G>3G>4G	适用于 2G 卡
3G	仅使用 3G 网络	3G>2G>4G	适用于 3G
4G	仅使用 4G 网络	4G>3G>2G	适用于移动/联通/电信 4G

<注意>

➢ 适用于非 4G 卡，以及 2G/3G 的 APN 卡。

3.2.3. 4G ping 检测

实时 ping 检测功能，用于检测 4G 网络连接状态，默认关闭状态。开启 4G ping 检测功能，设备会每隔设定的时间去连接指定的检测地址，当失败次数达到最大时会自动重启设备。

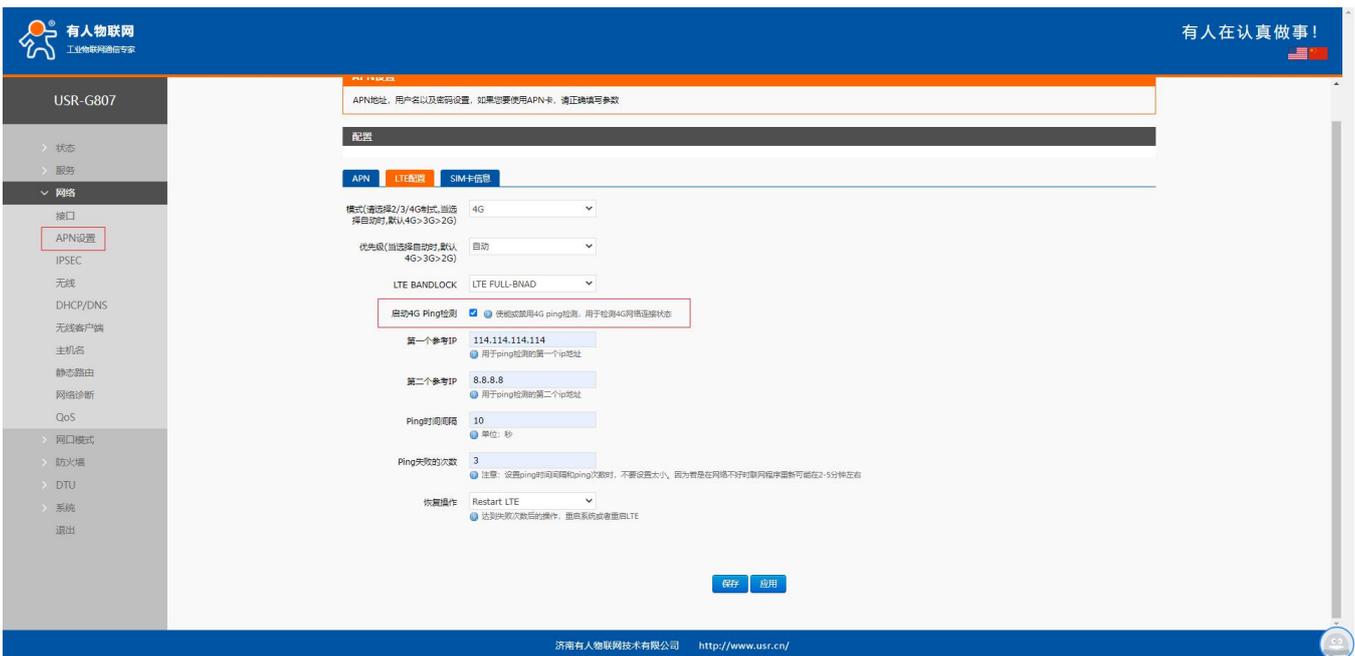


图 19 4G 实时 ping 检测

3.2.4. 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。

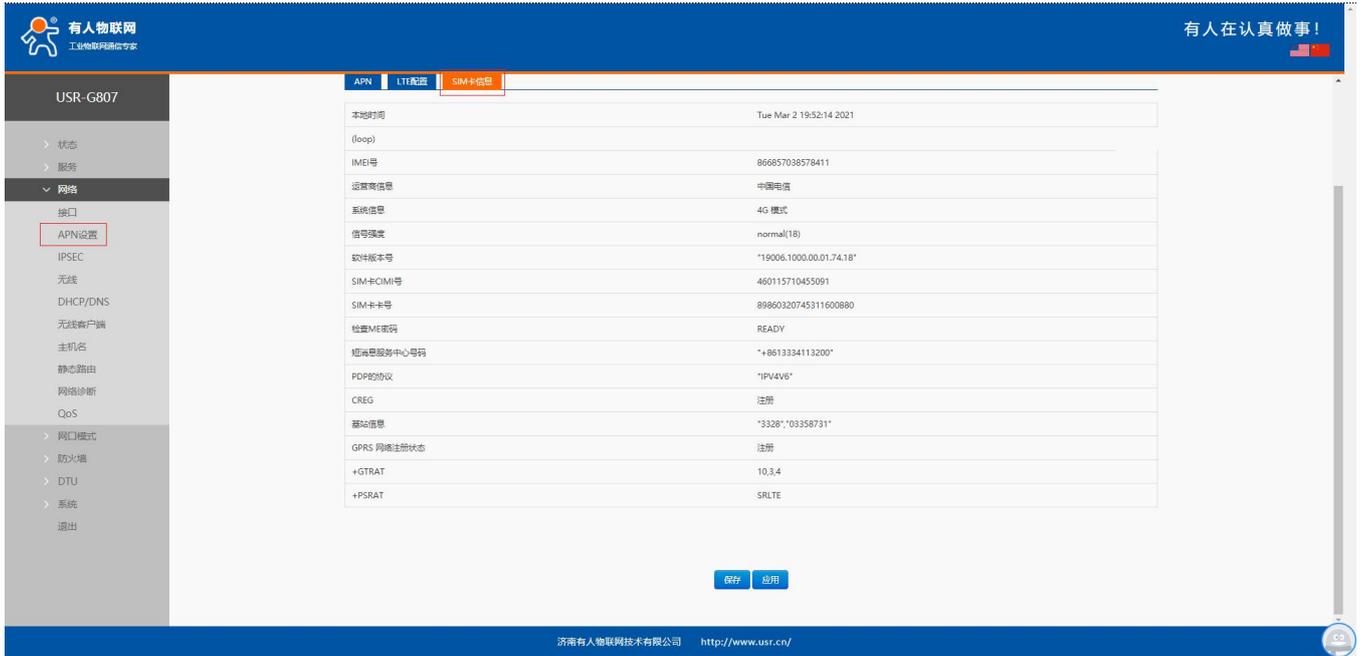


图 20 SIM 卡信息显示

<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-G807 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，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， $dBm \geq -90dBm$ ， $asu \geq 12$ ，信号强度满足覆盖要求，可以据此衡量当前信号是否达标。

3.3. LAN 接口

LAN 口为局域网络，有 1 个有线 LAN 口（WAN 口也可以设置成 LAN 口使用）。

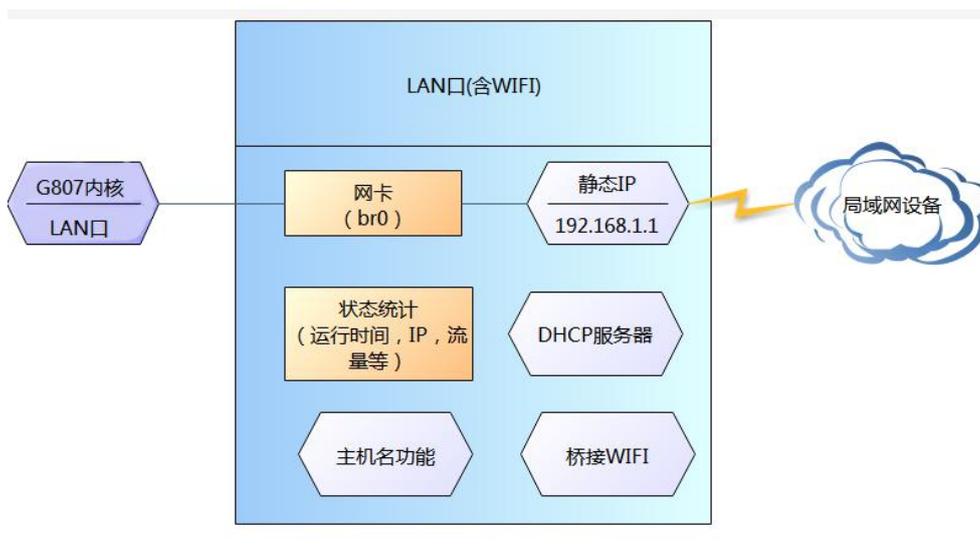


图 21 LAN 口功能示意图

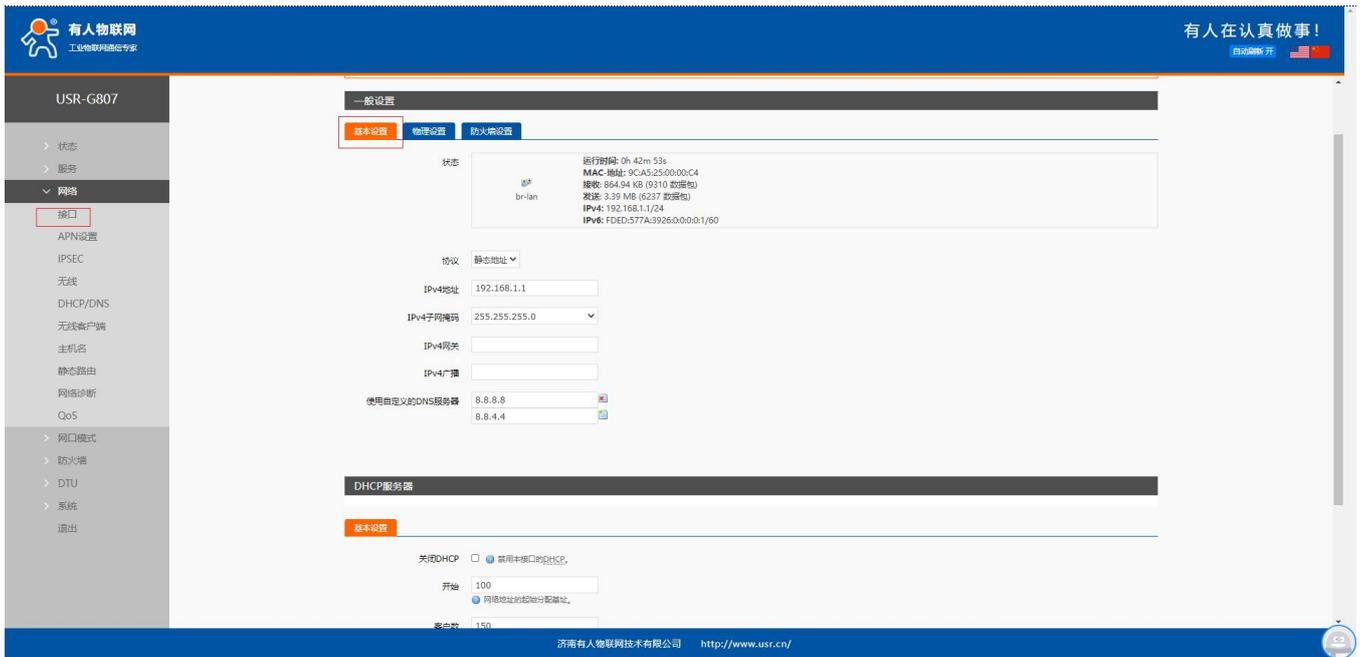


图 22 LAN 口设置页面

<说明>

- 1 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 接口（WLAN 口）桥接到了 LAN 口；
- 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。

3.3.1. 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。

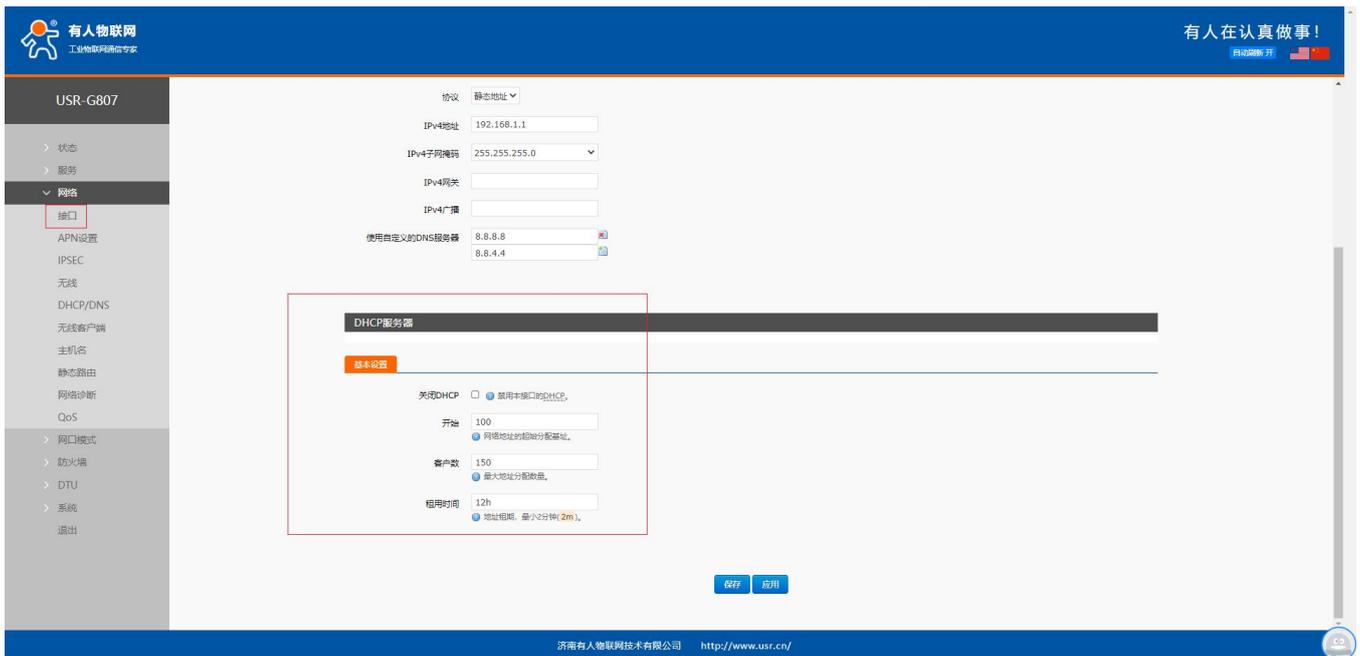


图 23 DHCP 设置页面

<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 192.168.1.100 开始；
- 默认租期 12 小时。

3.3.2. 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。只有指定的主机才能连接，并且接口须为非动态配置。

使用添加来增加新的租约条目。使用 MAC-地址鉴别主机，IPv4-地址分配地址，主机名分配标识。

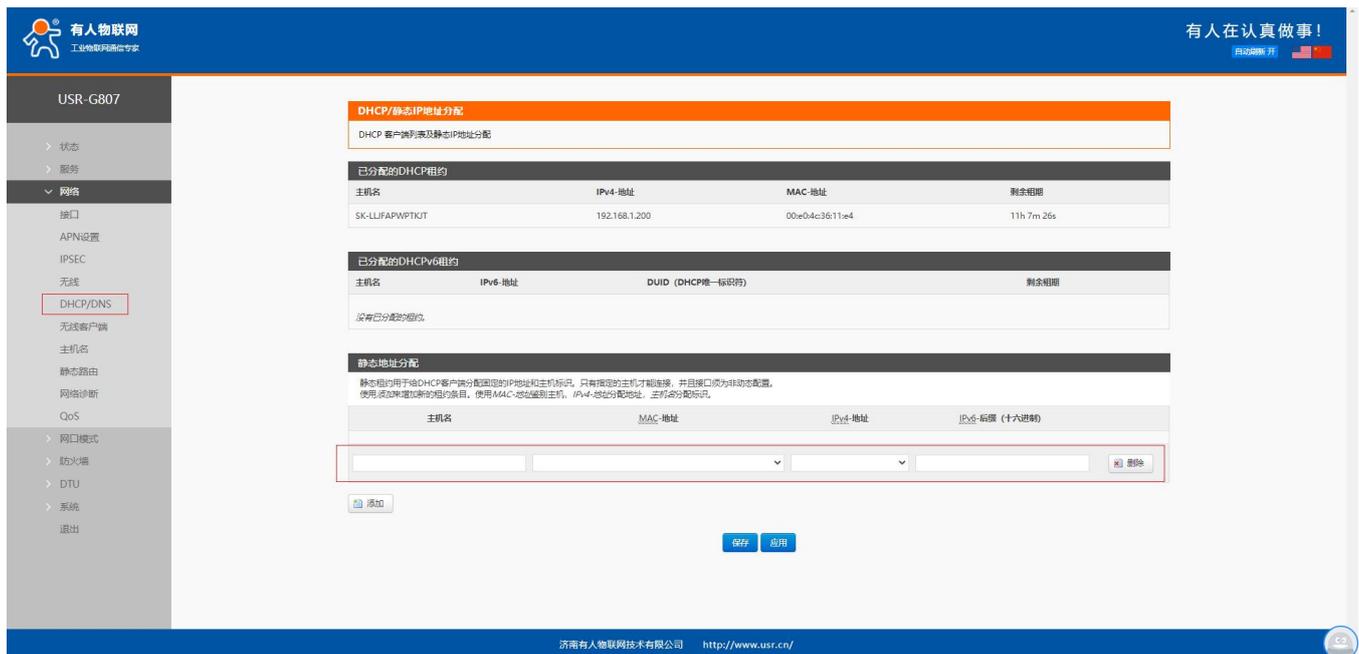


图 24 DHCP/DNS 设置页面

3.4. WAN 口

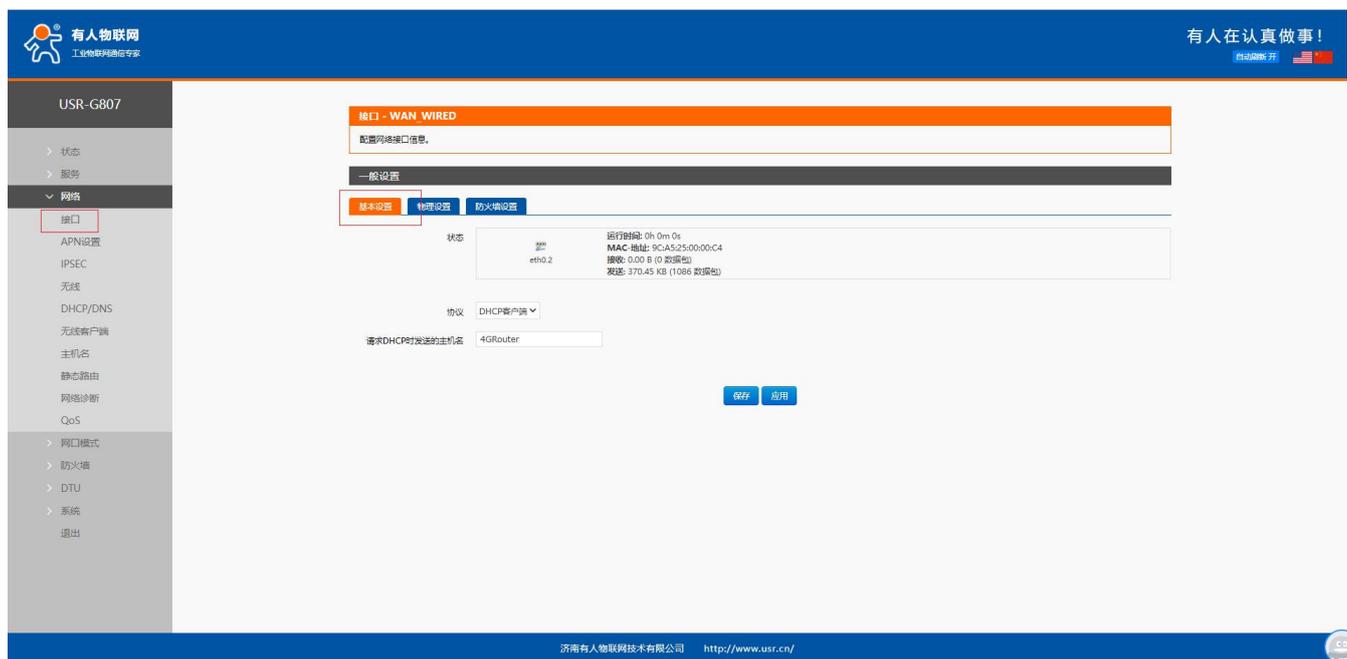


图 25 WAN 口设置页面

<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 等模式；
- 默认 DHCP 客户端；
- 此 WAN 口的网口可以设置成 LAN，方便客户用于局域网多个设备通信，具体设置请参照网口模式配置。

3.5. 网络模式选择

Web 界面左侧依次点击：网口模式--模式选择，进入设置界面。选择 LAN 口后，再依次点击保存---应用。重启生效，实现双 LAN 应用。

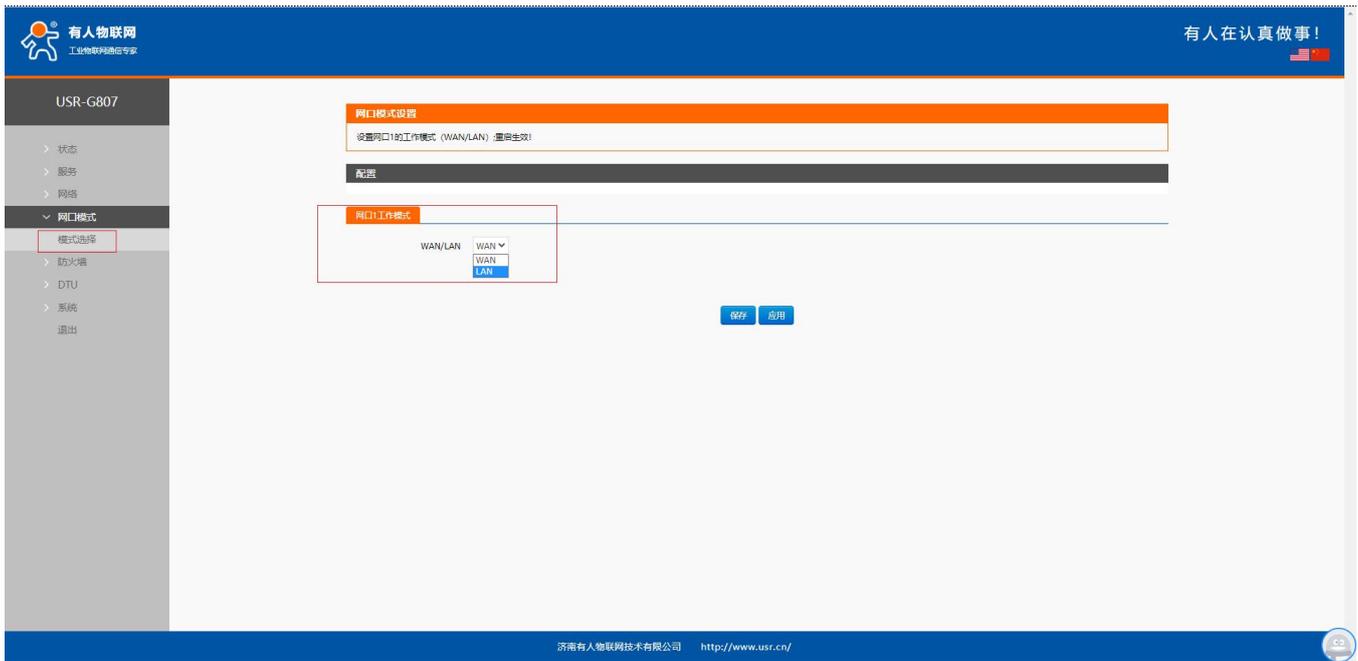


图 26 WAN 口改 LAN 口设置页面

3.6. WIFI 无线接口

无线局域网的功能框图如下图所示：

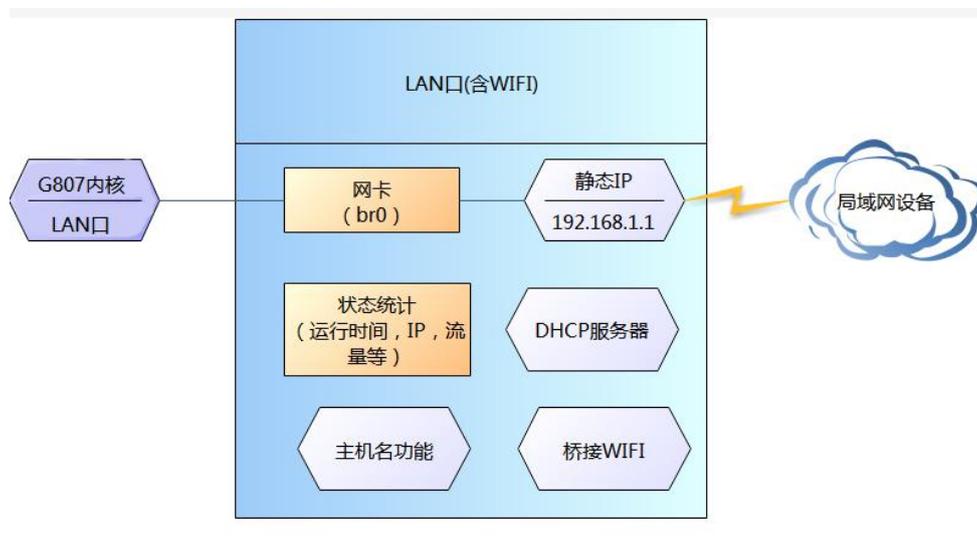


图 27 WIFI 功能示意图

<说明>

- USR-G807 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 100m。

默认参数如下：

表 10 WIFI 默认参数

默认参数	数值
SSID 名称	USR-G807-XXXX (最后为 MAC 地址后 4 位)
无线密码	www.usr.cn
信道	Auto
带宽	40MHz
加密方式	WPA2-PSK

在如下位置修改 SSID。

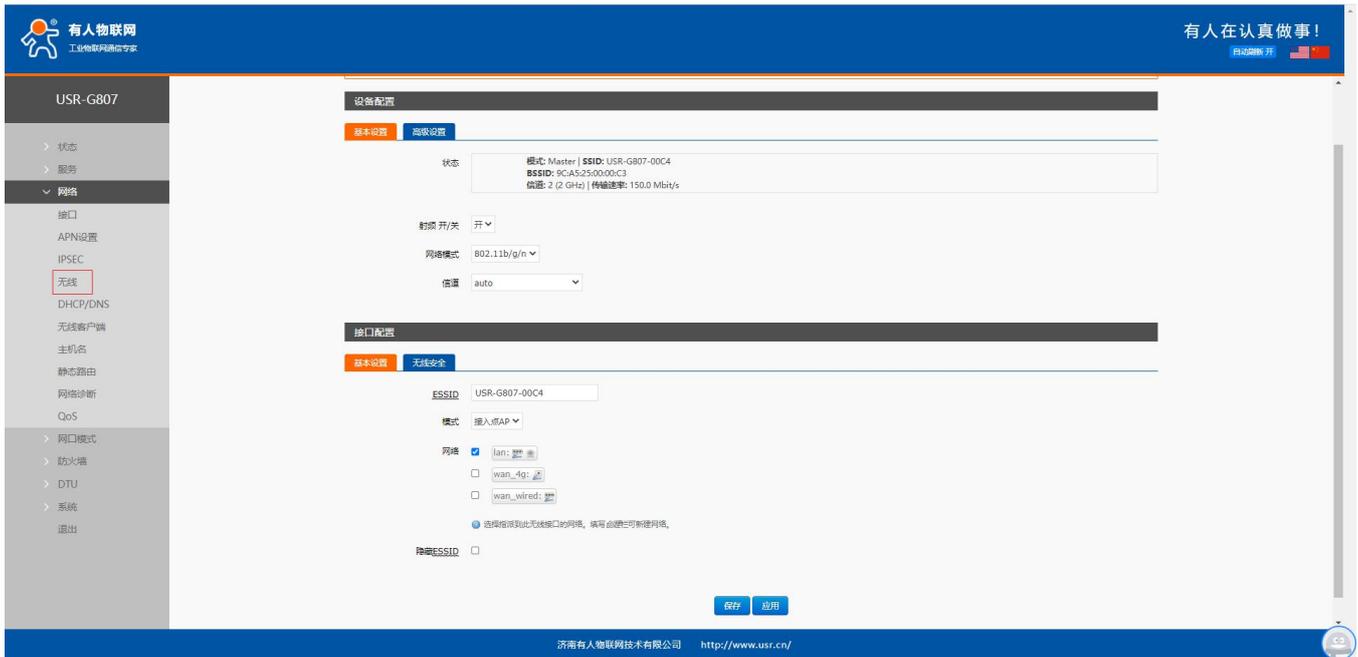


图 28 SSID 设置页面

如下位置修改无线密码。

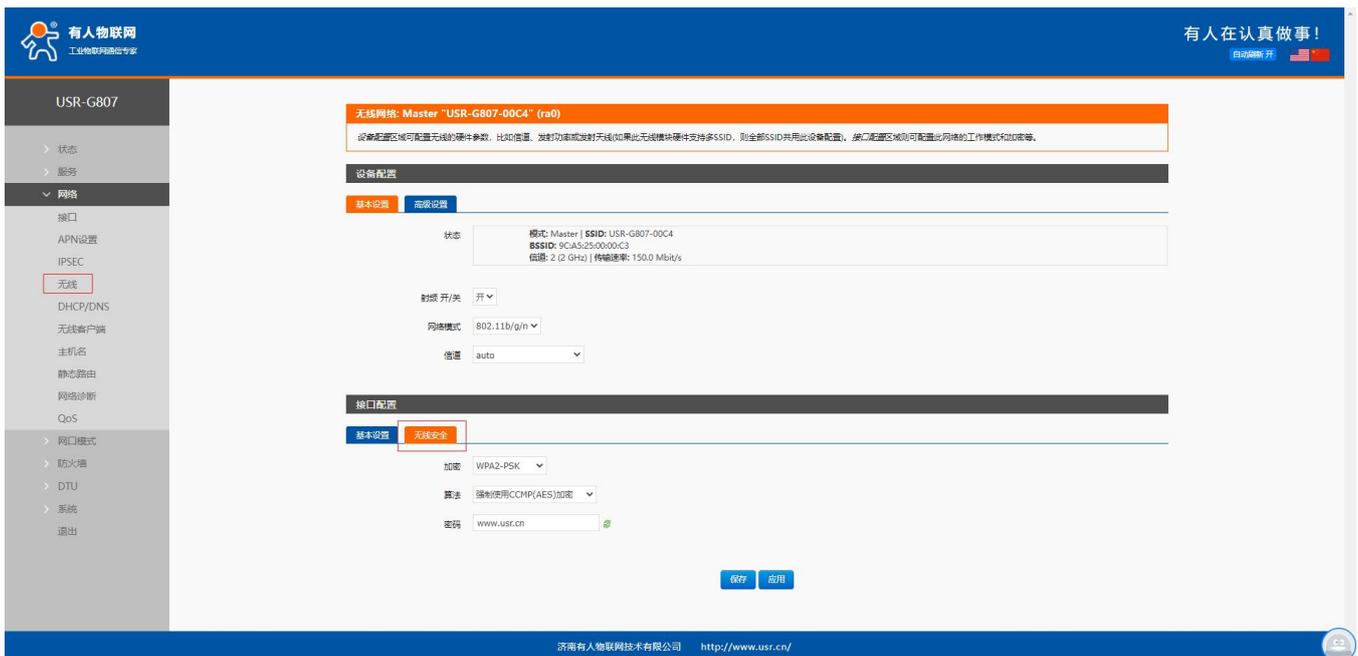


图 29 WIFI 设置页面

在如下位置，修改是否开启无线功能（将射频关闭，如下图，即时生效）。

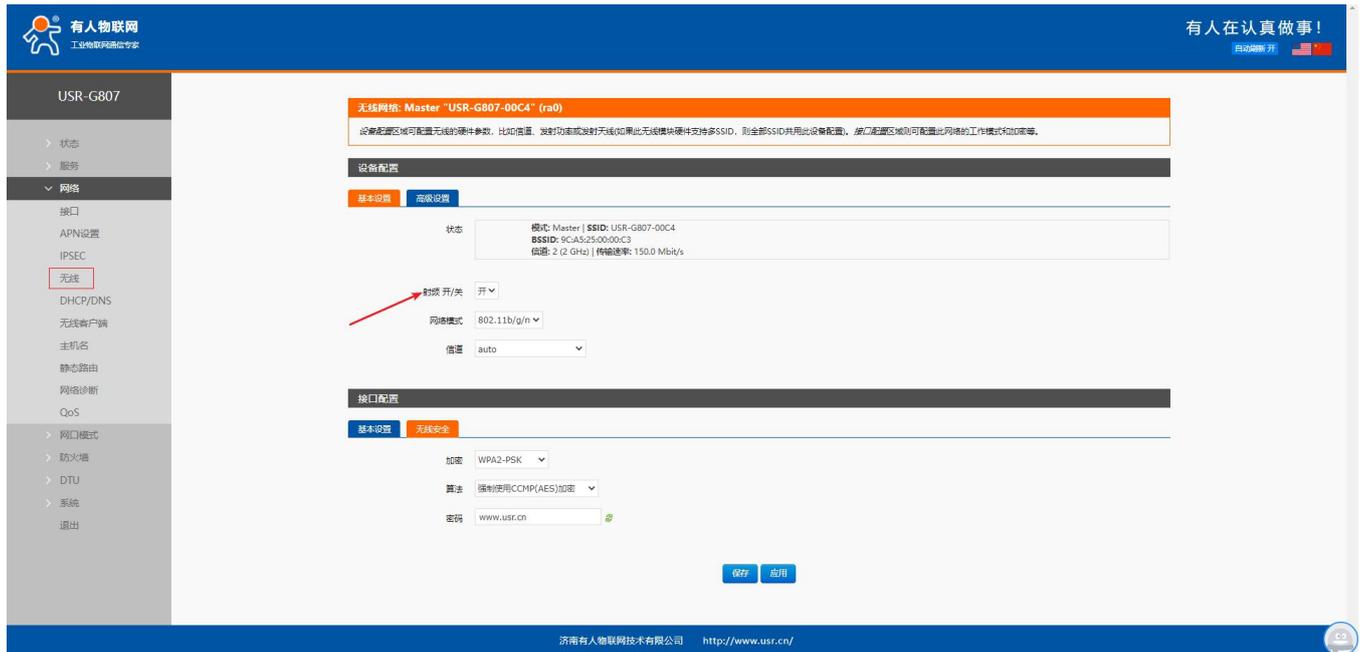


图 30 WIFI 开关设置页面

3.7. 网络诊断功能

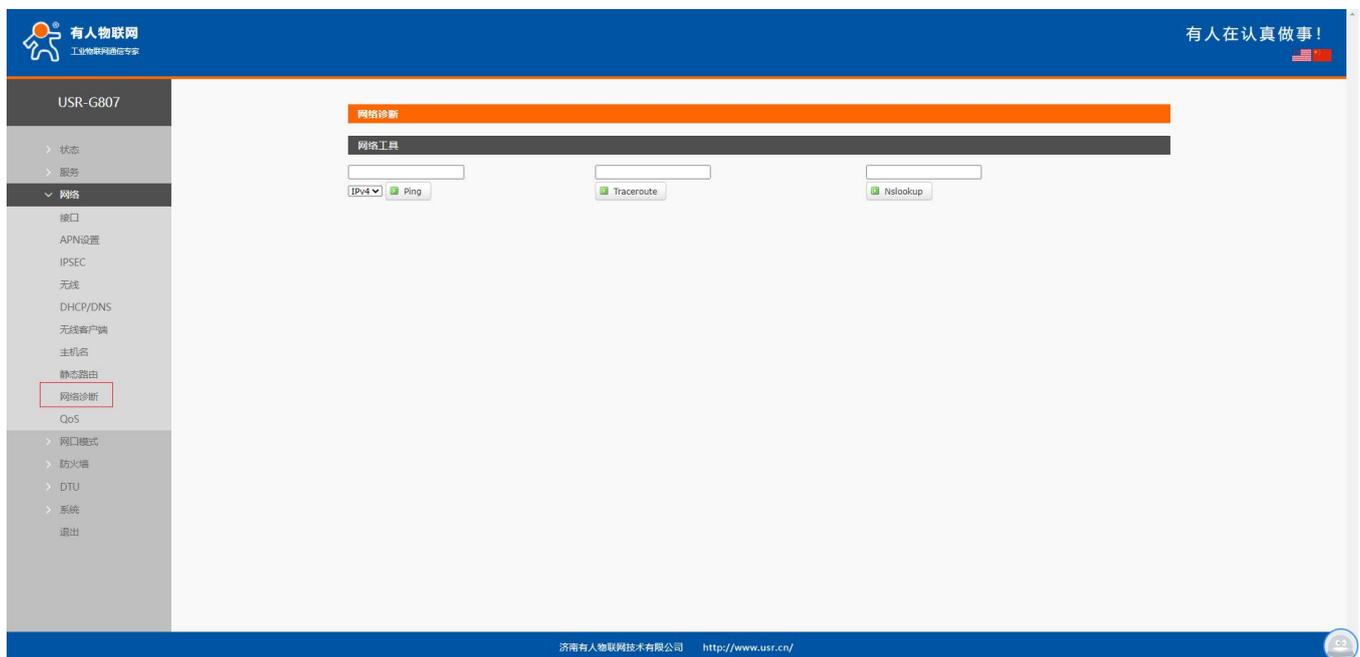


图 31 网络诊断页面

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。

3.8. 主机名功能

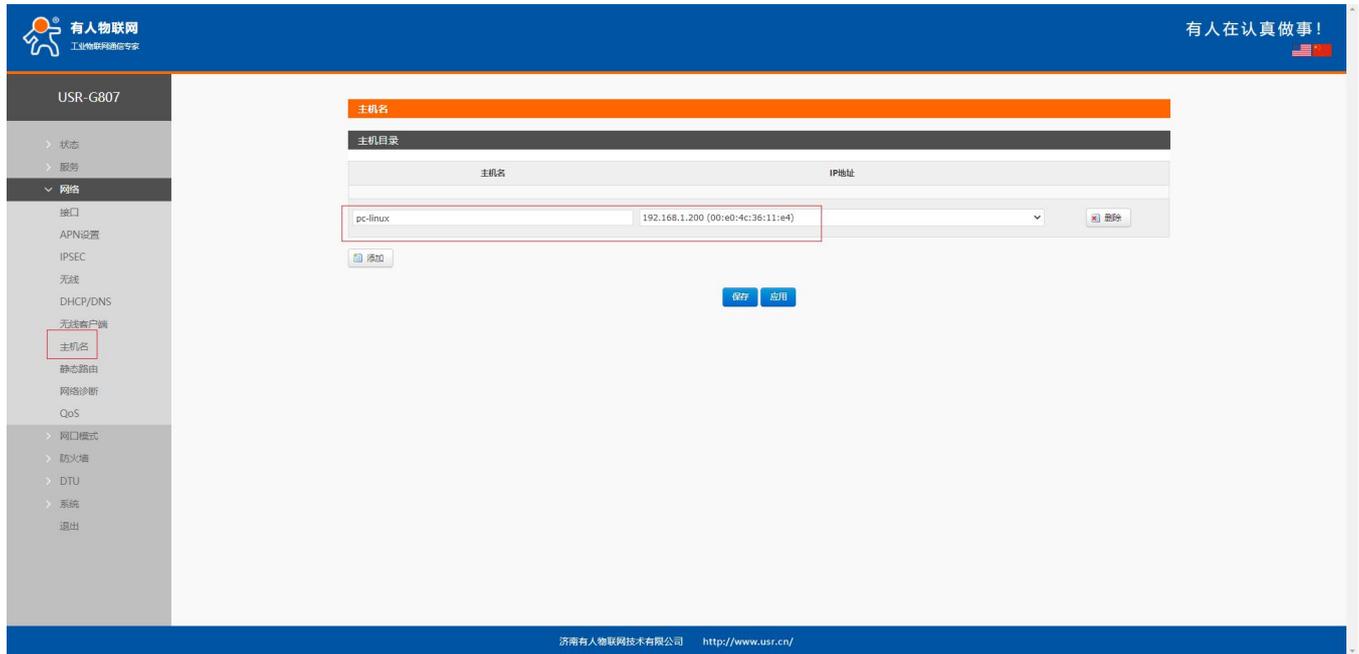


图 32 主机名页面

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“pc-linux”设置为主机名，对应的ip地址192.168.1.200。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。

3.9. 接口限速

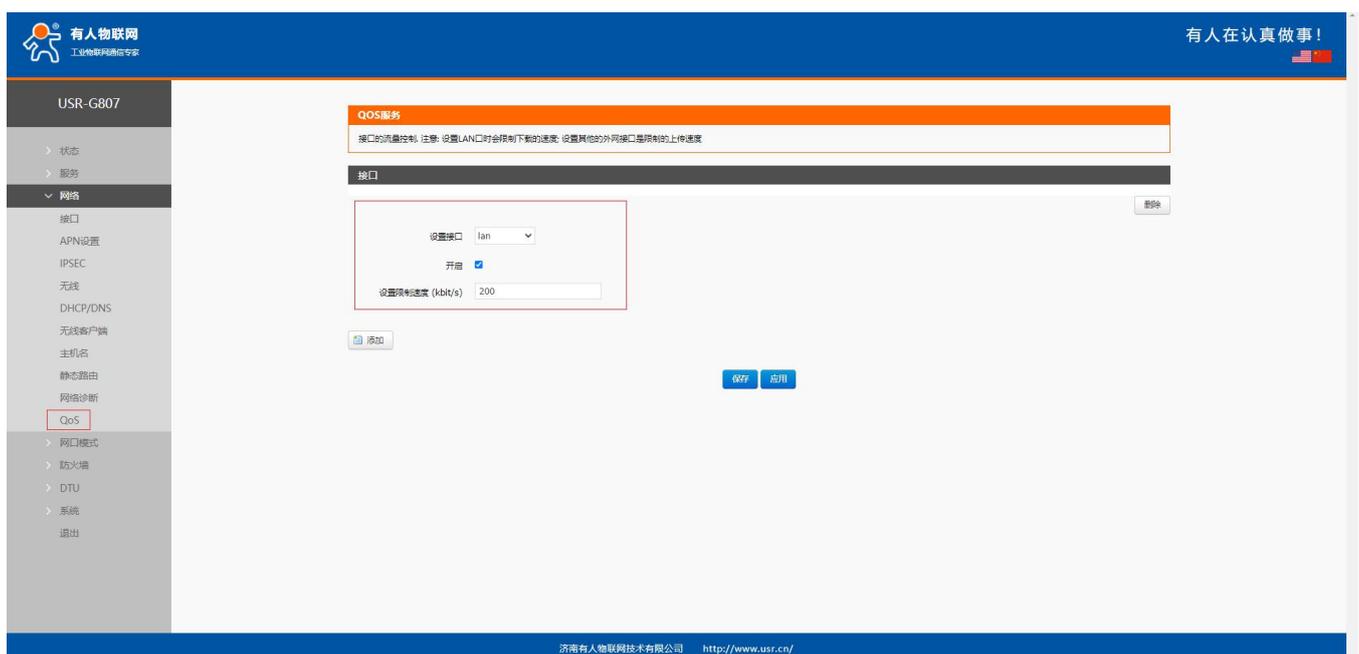


图 33 限速功能设置页面

可以根据路由器每个接口进行限速。添加一个设置如上图, 目标为有线 LAN 口, 限制上下行速度均为 200Kbps(约 20KB/s), 那么使用测速工具测得上网速度如下:



图 34 限速测试图

4. VPN Client 功能

4.1. 概念介绍

VPN (Virtual Private Network) 虚拟专用网, 在协议上又分为 PPTP, L2TP, IPSec, OpenVPN, gre、sstp 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、MS-CHAP V2 或 EAP-TLS 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 USR-G807 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 AH、ESP、IKE 和用于网路认证及加密的一些算法等。其中 AH 协议和 ESP 协议用于提供安全服务, IKE 协议用于密钥交换。

OpenVPN:

是一个基于 Openssl 库的应用层 VPN 实现。其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。

SSTP:

SSTP，又称安全套接字隧道协议，是一种应用于互联网的协议，它可以创建一个在 HTTPS 上传送的 VPN 隧道。SSTP 只适用于远程访问，不能支持站点与站点之间的 VPN 隧道。

<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。

4.2. PPTP Client 搭建

我们新建一个接口，协议选择 PPTP。参数由 VPN 服务器提供，并将参数依次写入。

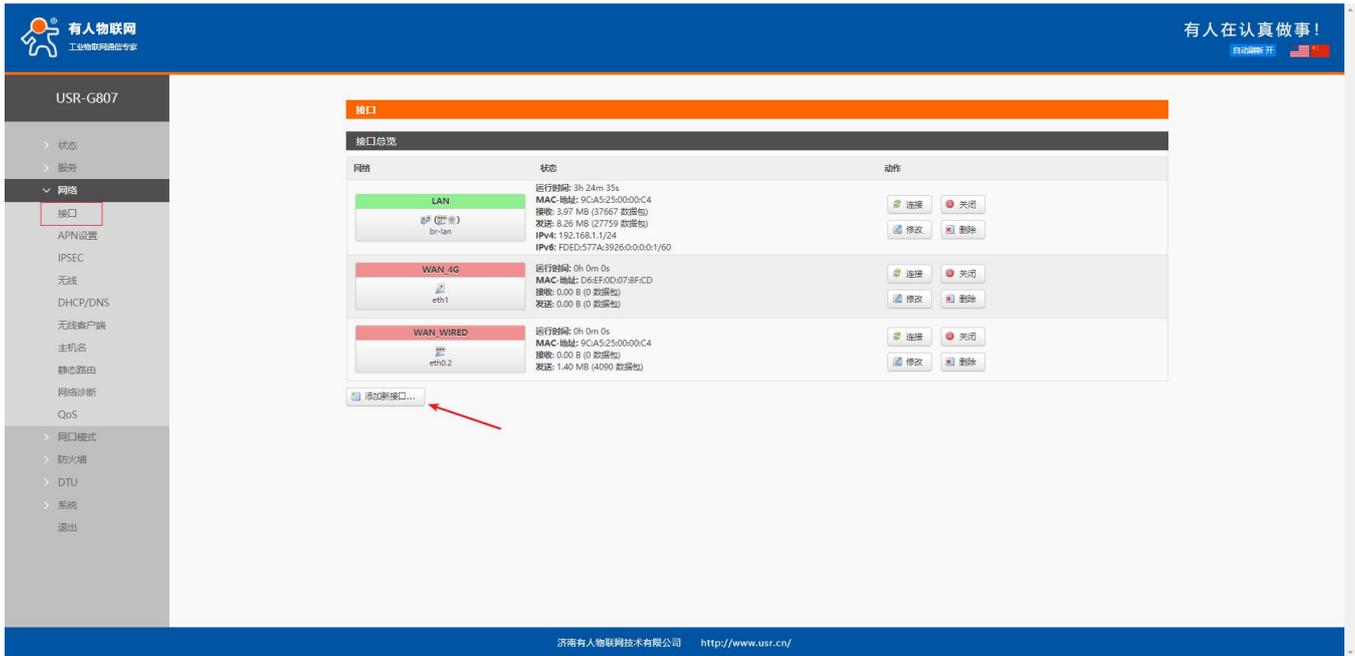


图 35 路由器添加 VPN 操作图一

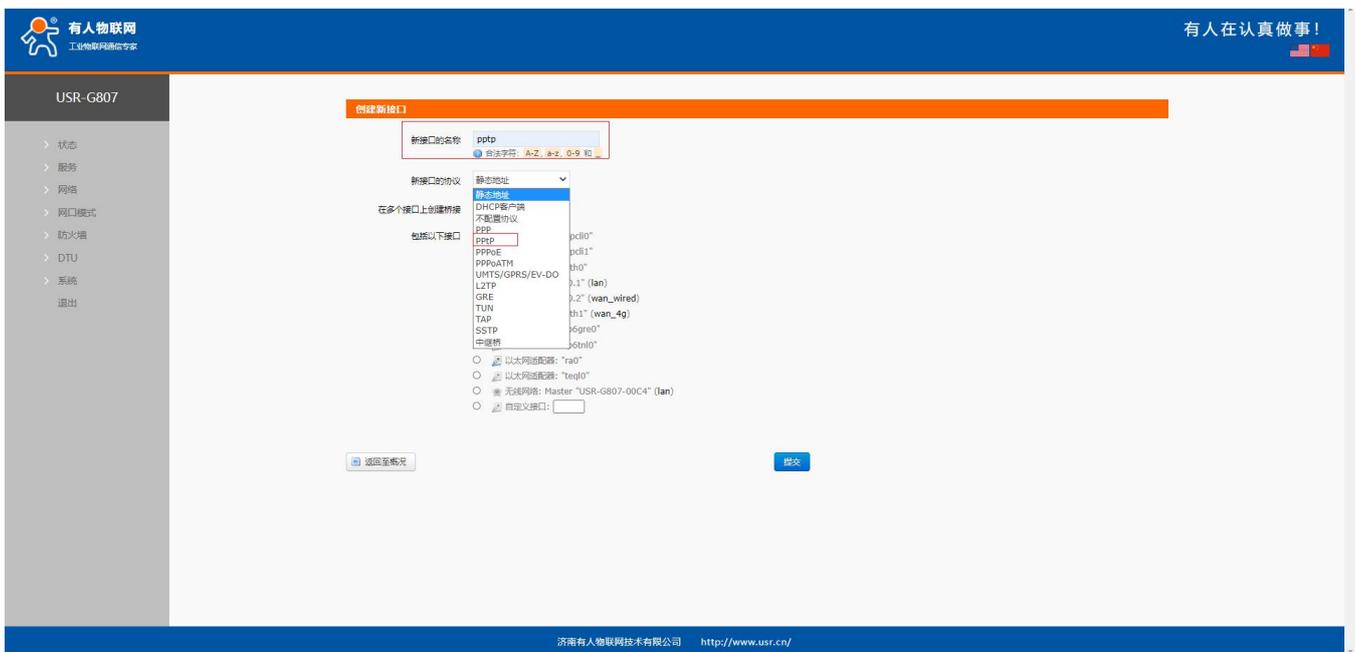


图 36 路由器添加 VPN 操作图二

防火墙区域我们选择 WAN，因为是在 WAN 口进行的拨号，然后点保存并应用

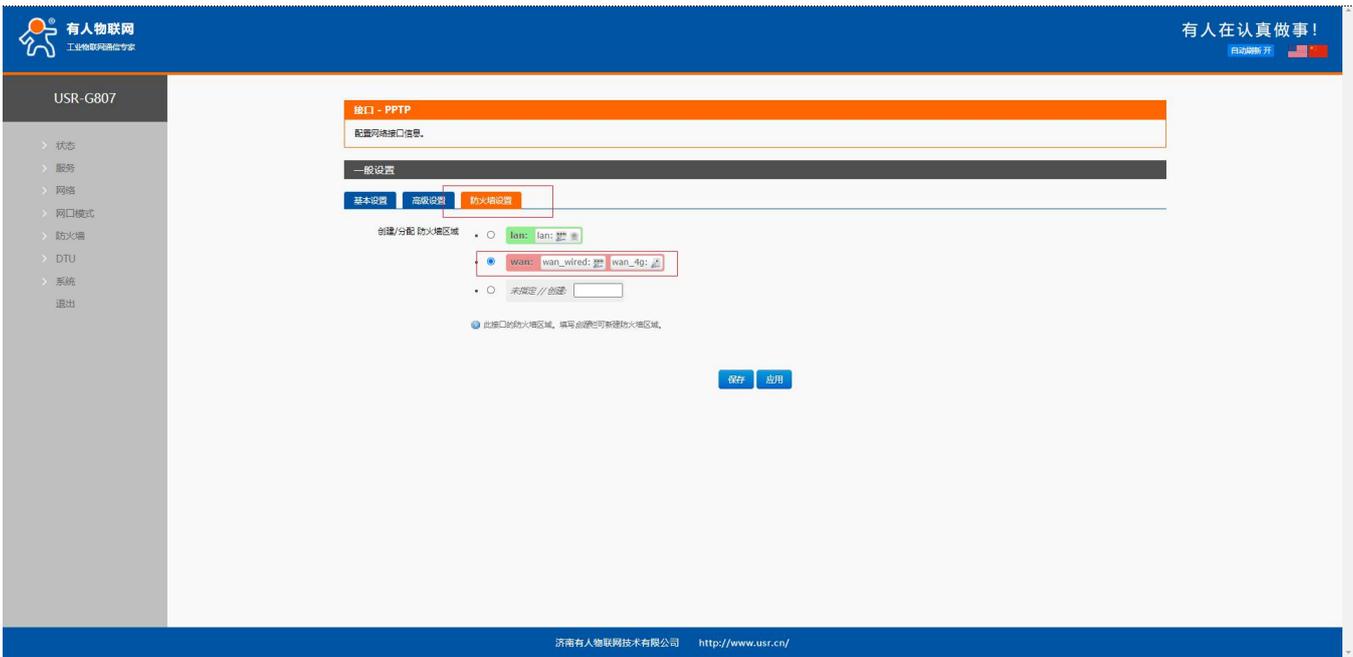


图 37 路由器添加 VPN 操作图三

等 1 分钟或重启路由器，当看到路由器页面中的“VPN”接口，有运行时间（非 0）时，表示当前的 VPN 已经成功启动，可以访问 VPN 网络。

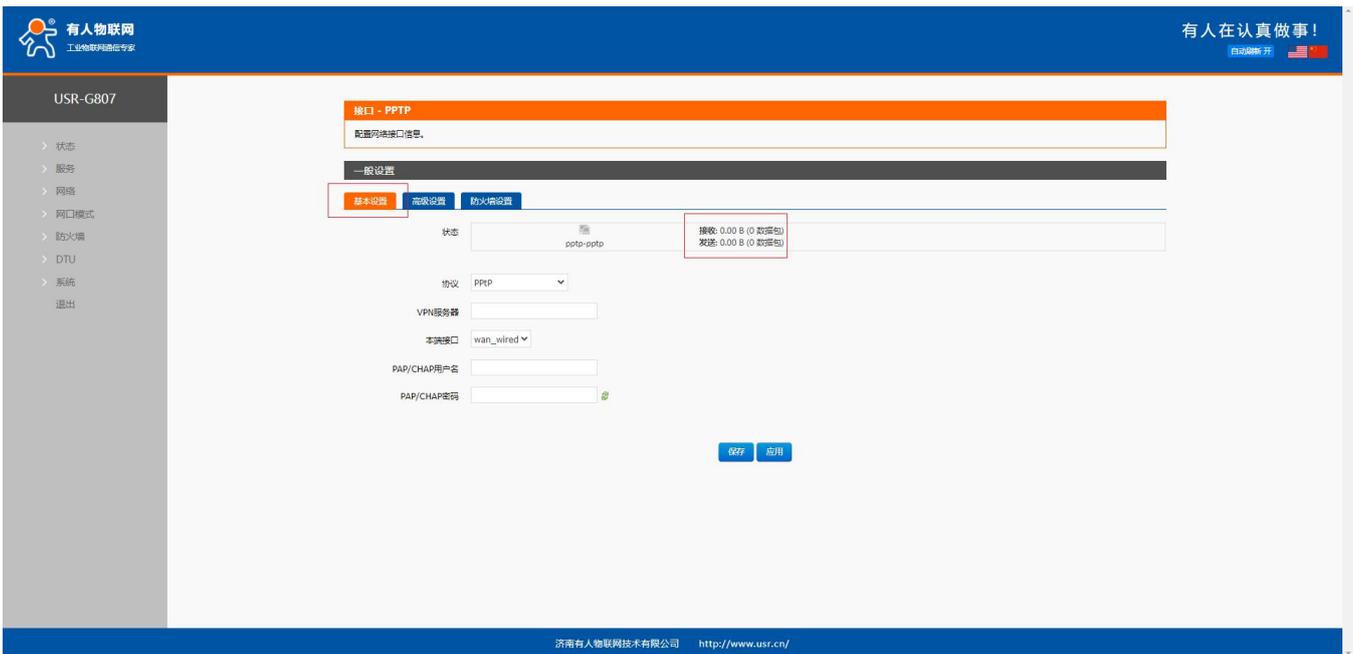


图 38 路由器添加 VPN 操作图四

<注意>

- 目前 PPTP 支持 MPPE 加密，和多种认证方式，具体设置可以在高级设置的身份验证查看；
- Only MSChapV2 表示仅支持 MPPE 加密；
- MSChapV2 EAP PAP CHAP 表示支持 MPPE 加密和多种认证；
- 其他表示不做处理，默认状态，默认情况下只有 CHAP 认证。

4.3. L2TP Client 搭建

L2TP 目前支持多种身份认证(MSCHAPV2、CHAP、EAP、PAP), MPPE 加密, L2TP OVER IPsec 加密。增加了隧道密码认证的方式。

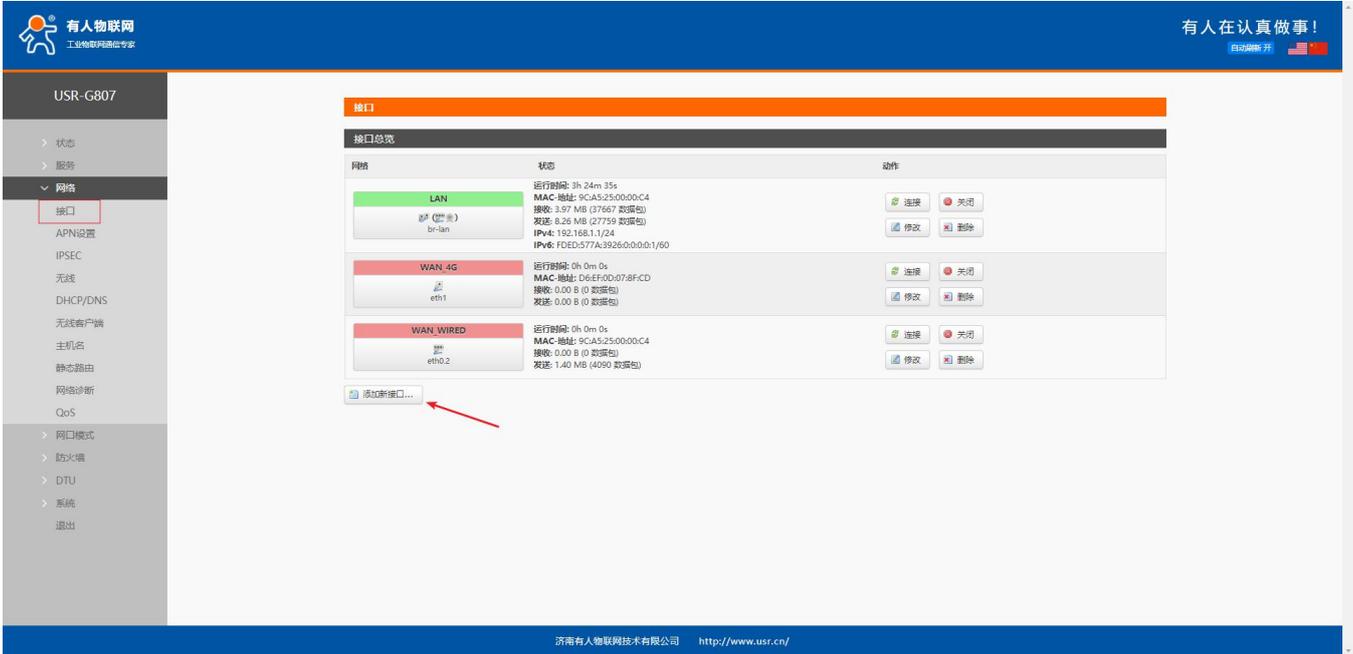


图 39 创建接口

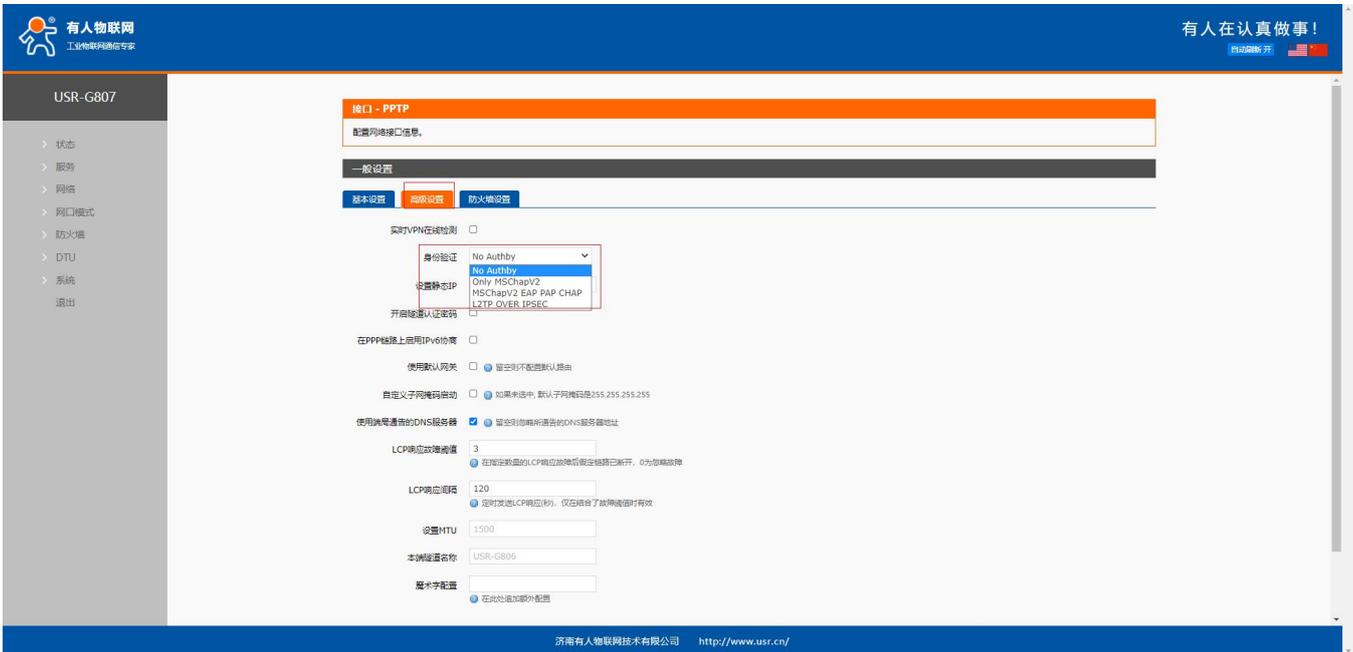


图 40 L2TP 认证方式选择

开启隧道密码认证

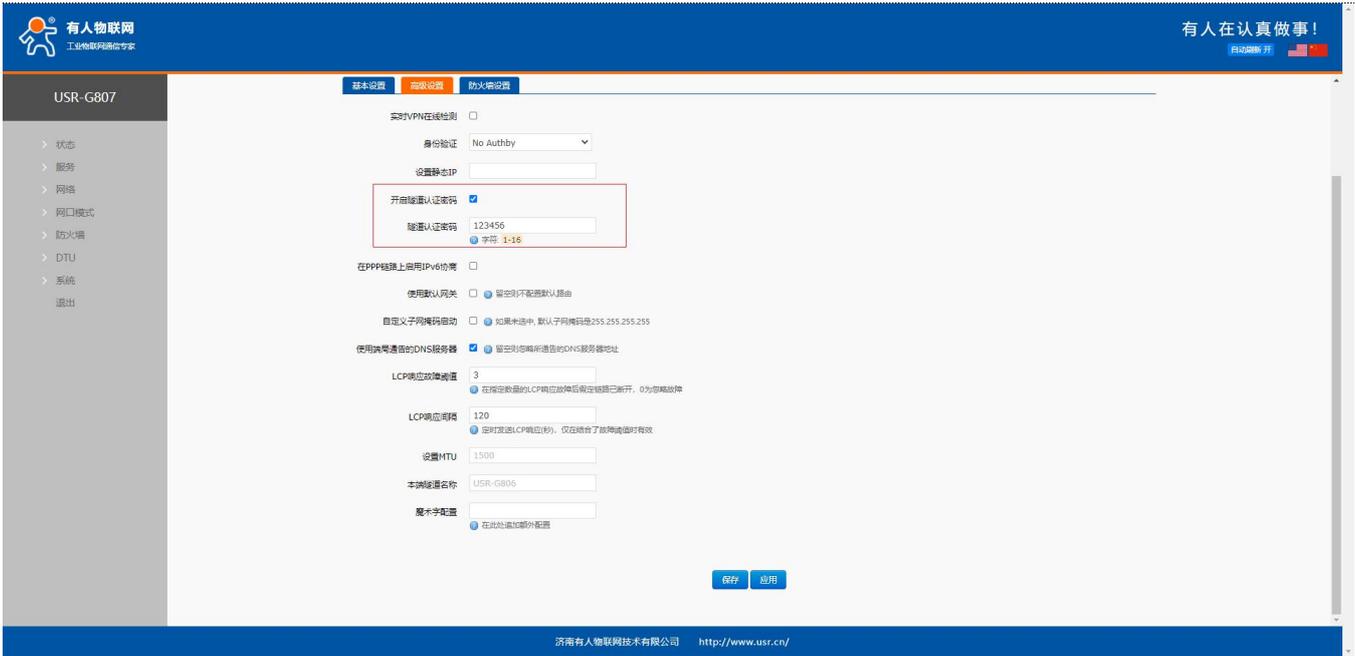


图 41 L2TP 认证方式选择

L2TP OVER IPsec 加密方式配置

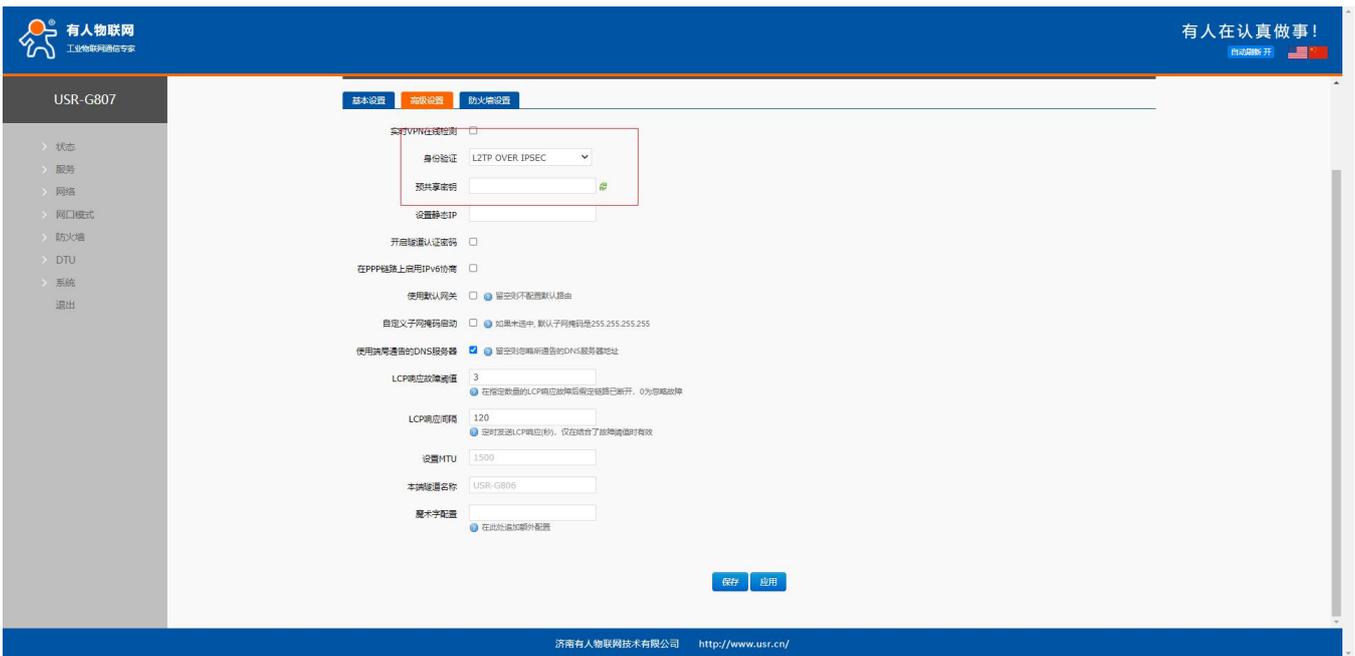


图 42 L2TP OVER IPsec 加密方式配置

4.4. IPSec 搭建

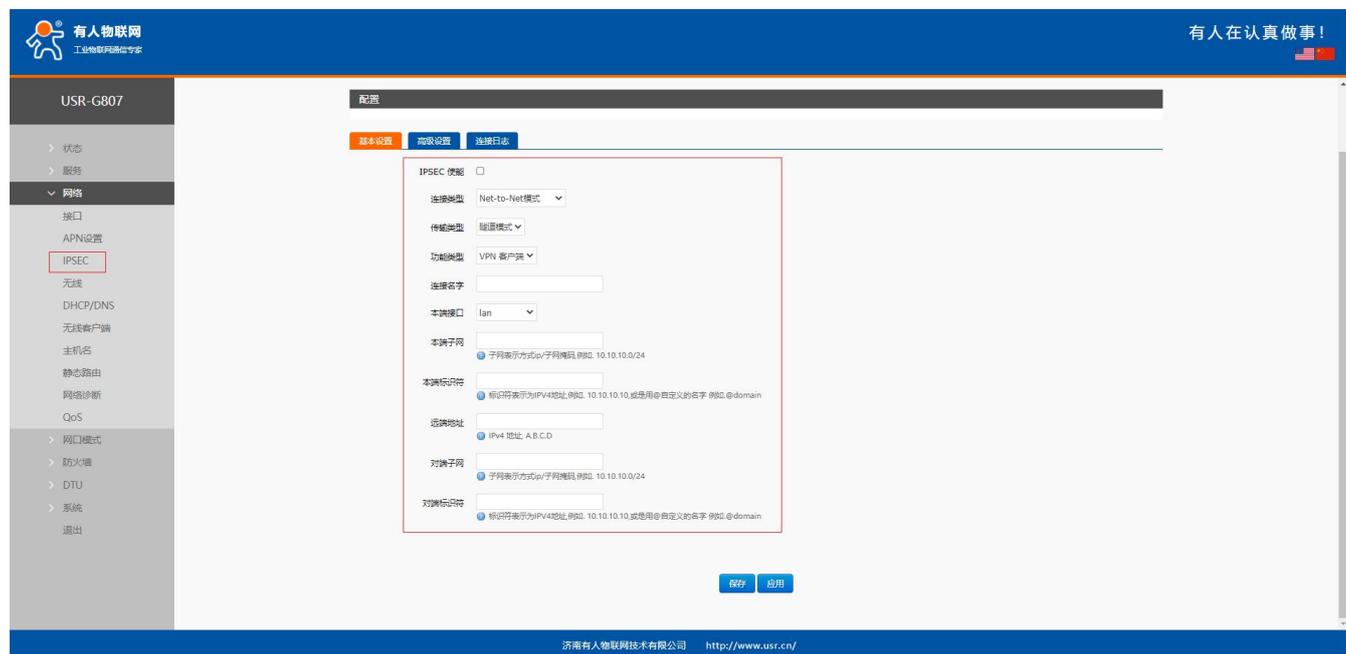


图 43 IPSec 基本设置

- 应用方式选择： Net-to-Net 模式(站点到站点或者网关到网关)、Road Warrior 模式（端到站点或者 PC 到网关）；
- 传输方式选择：可以分为隧道模式和传输模式。可在传输类型中选择；
- 功能类型：可以分为 VPN 客户端和 VPN 服务器；
- 连接名字：用以表示该连接的名字，须唯一，不可使用纯数字；
- 本地接口：通过的本端地址，这个可选择 wan_wried、wan_4g；
- 远程地址：对端的 IP/域名；
- 本端子网：IPSec 本端保护子网及子网掩码，如果选择 Road Warrior 模式的客户端，则不需要填写；
- 对端子网：IPSec 对端保护子网及子网掩码；
- 本端标识符：通道本端标识，可以为 IP 或域名，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 或域名，注意在域名自定义名时加@。

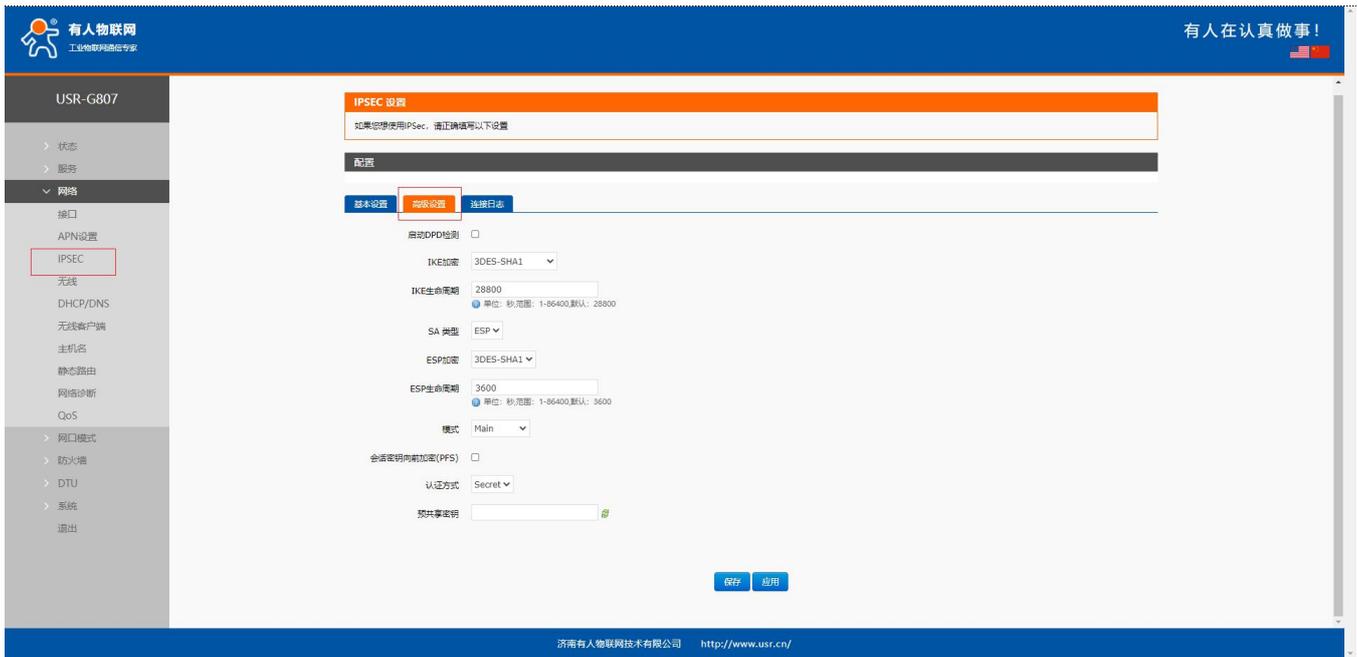


图 44 IPsec 高级设置

- 启动 DPD 检测：是否启用该功能，打钩表示启用；
- DPD 时间间隔：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；
- 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；
- SA 类型：第二阶段可以选择 ESP 和 AH；
- ESP 加密：选择对应的加密方式、完整性方案；
- ESP 生命周期：设置 ESP 生命周期，单位：s，默认：3600；
- 模式：协商模式默认主模式，可选择野蛮模式；
- 会话密钥向前加密(PFS)：如果打钩，则启用 PFS，否则不启用；
- 认证方式：目前支持预共享密钥的认证方式；
- 配置成功后，可先在连接日志里面有 ISAKMP SA established 标志，表示创建 IPsec VPN 成功。

4.4.1. Road Warrior 模式

Road Warrior 模式下的应用，该应用一般是在一个外地人员例如用笔记本访问总公司的内部网络。

网络环境：

虚拟机 IP: 192.168.13.66

USR-G807 WAN 口: 192.168.13.13

USR-G807 LAN 口: 192.168.1.1

虚拟机配置 需要配置/etc/IPsec.conf 和/etc/IPsec.secrets，配置完后，重启虚拟机。

```

root@edu-virtual-machine:~#
root@edu-virtual-machine:~# vi /etc/ipsec.conf

config setup
#interfaces=%defaultroute
protostack=netkey
plutodebug=all
plutostderrlog=/var/log/pluto.log
nat_traversal=yes
virtual_private=%v4:192.168.5.0/24
oe=off

#include /etc/ipsec.d/examples/no_oe.conf

conn    road
left=192.168.13.66
leftid=@left
leftnexthop=%defaultroute

right=192.168.13.13
rightid=@right
rightsubnet=192.168.1.0/24
rightnexthop=%defaultroute

authby=secret
ike=3des-md5
## phase 1 ##
keyexchange=ike
## phase 2 ##
phase2=esp
phase2alg=3des-md5
compress=no
pfs=no
type=tunnel
auto=add

root@edu-virtual-machine:~#
root@edu-virtual-machine:~# vi /etc/ipsec.secrets

#: RSA /etc/ipsec.d/private/client.key "123456"
#: RSA /etc/ipsec.d/private/client.key "123456"
192.168.13.66 %any: PSK "123456"

```

图 45 IPsec 测试 1

路由器基本配置：

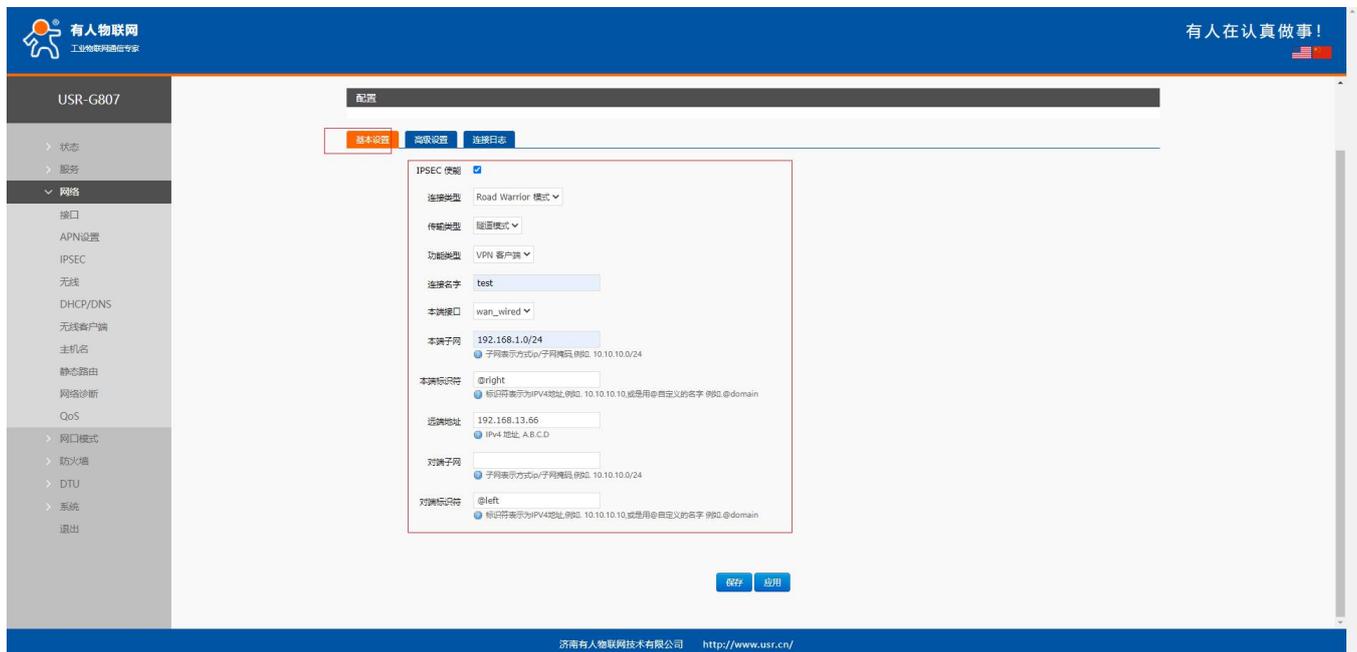


图 46 IPsec 测试 2

路由器 IPsec 高级设置

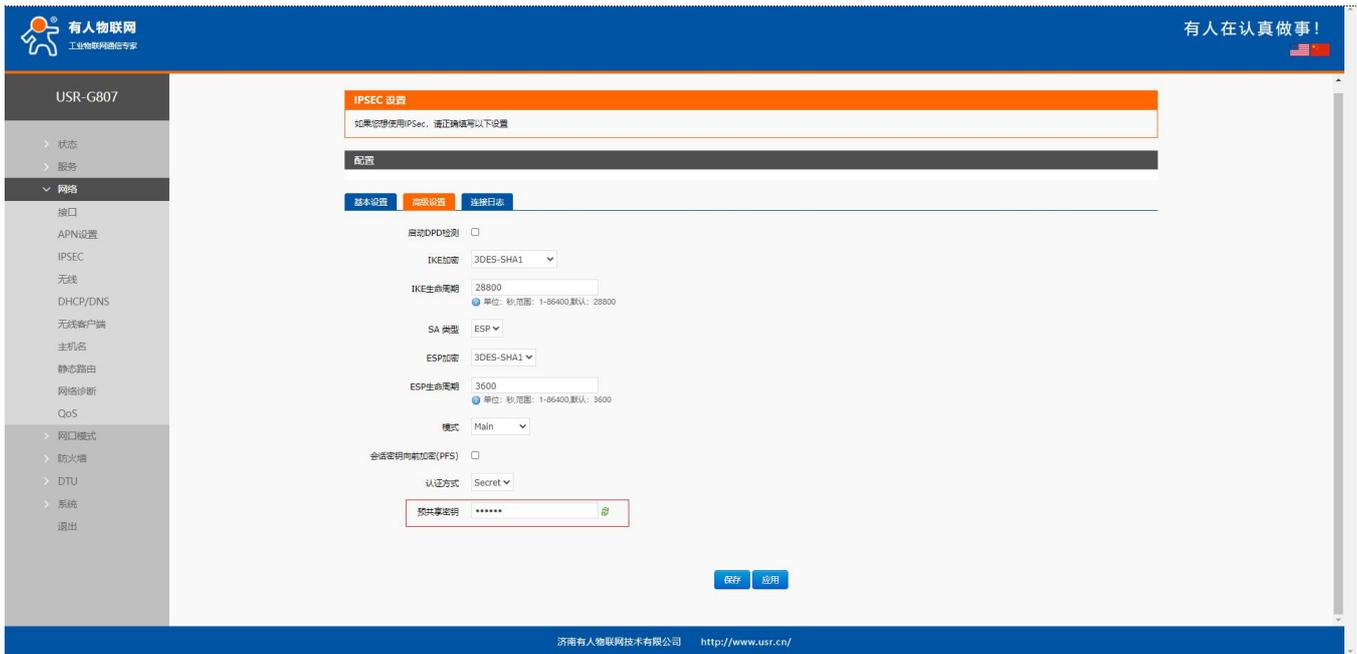


图 47 IPsec 测试 3

这样 USR-G807 和虚拟机就都配置完成，重启一下 USR-G807，可以用手机连上 USR-G807 的 wifi，然后在虚拟机 ping 手机的 IP，能 ping 通，既搭建 Road Warrior 模式搭建成功。例如：我手机获取的 IP: 192.168.1.114

```

root@edu-virtual-machine:~# ping 192.168.1.114
PING 192.168.1.114 (192.168.1.114) 56(84) bytes of data:
 64 bytes from 192.168.1.114: icmp_req=1 ttl=63 time=486 ms
 64 bytes from 192.168.1.114: icmp_req=2 ttl=63 time=202 ms
 64 bytes from 192.168.1.114: icmp_req=3 ttl=63 time=643 ms
 64 bytes from 192.168.1.114: icmp_req=4 ttl=63 time=1784 ms
 64 bytes from 192.168.1.114: icmp_req=5 ttl=63 time=777 ms
 64 bytes from 192.168.1.114: icmp_req=6 ttl=63 time=1501 ms
 64 bytes from 192.168.1.114: icmp_req=7 ttl=63 time=503 ms
 64 bytes from 192.168.1.114: icmp_req=8 ttl=63 time=619 ms
 64 bytes from 192.168.1.114: icmp_req=9 ttl=63 time=8.62 ms
^C
--- 192.168.1.114 ping statistics ---
 9 packets transmitted, 9 received, 0% packet loss, time 8045ms
 rtt min/avg/max/mdev = 8.623/725.247/1784.277/541.355 ms, pipe 2
root@edu-virtual-machine:~#
    
```

图 48 IPsec 测试 5

4.4.2. Net-to-Net 模式

Net-to-Net 模式下的应用，该应用一般两个不同地域间相互通信，例如我们总公司在济南，分公司在深圳，我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：准备一个交换机、两个 USR-G807，一个 USR-G807 叫 USR-G807A，另一个叫 USR-G807B

1、USR-G807A:

WAN 口 IP: 192.168.4.115

Lan 口: 172.16.50.0/24

2、USR-G807B:

WAN 口 IP: 192.168.4.129

Lan 口: 172.16.40.0/24

用电脑连接到 USR-G807B 的 LAN 口上，电脑 ip: 172.16.40.214

用手机连接到 USR-G807A 的 wifi 上：手机 wifi 的 ip: 172.16.50.114

测试结果：用 IPsec 的 net-to-net 模式实现电脑和手机这两个内网就可以相互 ping 通。

USR-G807B 的 IPsec 配置

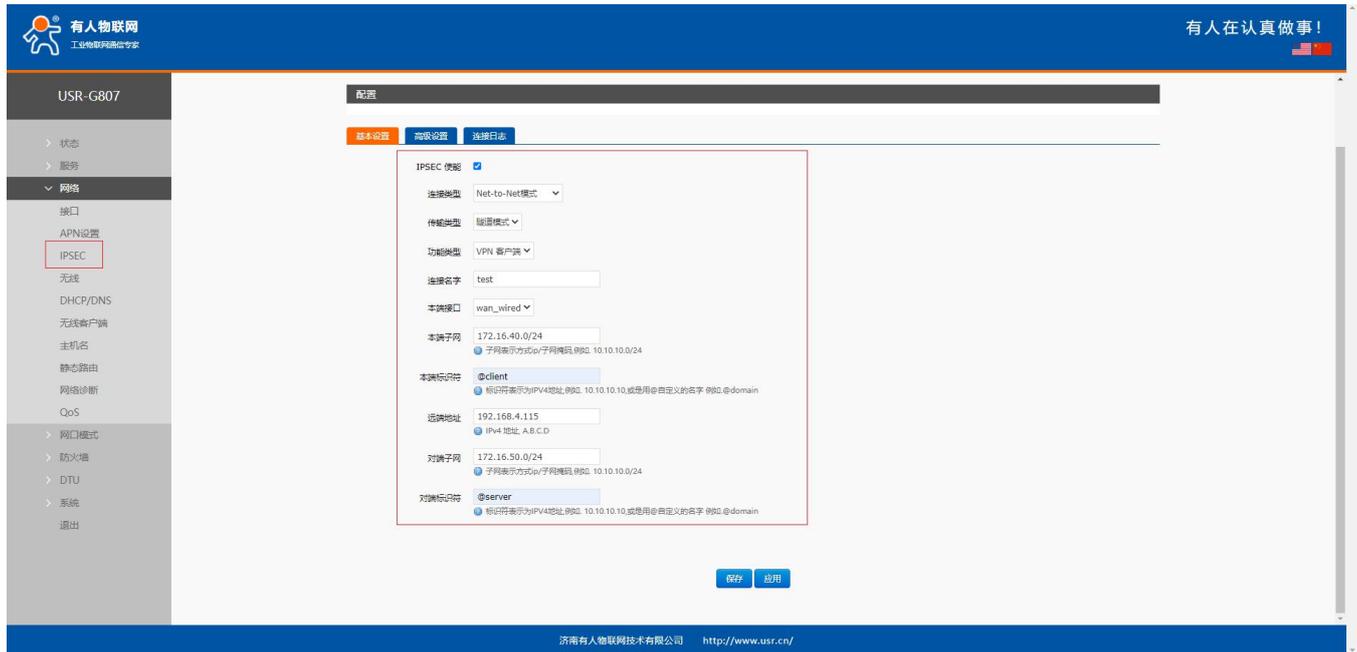


图 49 IPsec 测试 6

测试结果，在子网是 192.168.40.214 的 PC 上 ping 手机 IP 192.168.50.114。

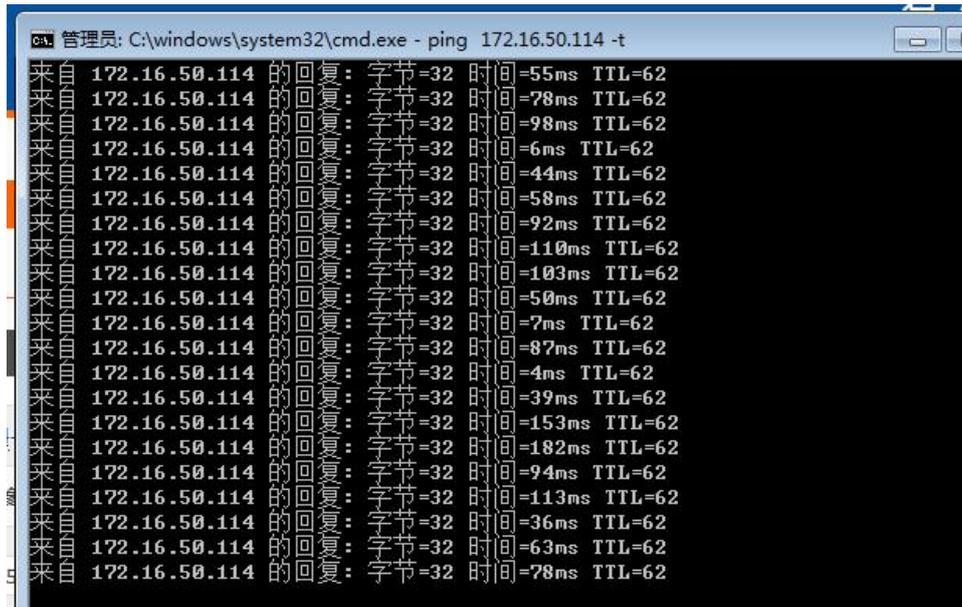


图 50 IPsec 测试 8



图 51 IPsec 测试 9

4.5. OpenVPN 搭建

创建接口，可选 TUN(路由模式)或 TAP(网桥模式):

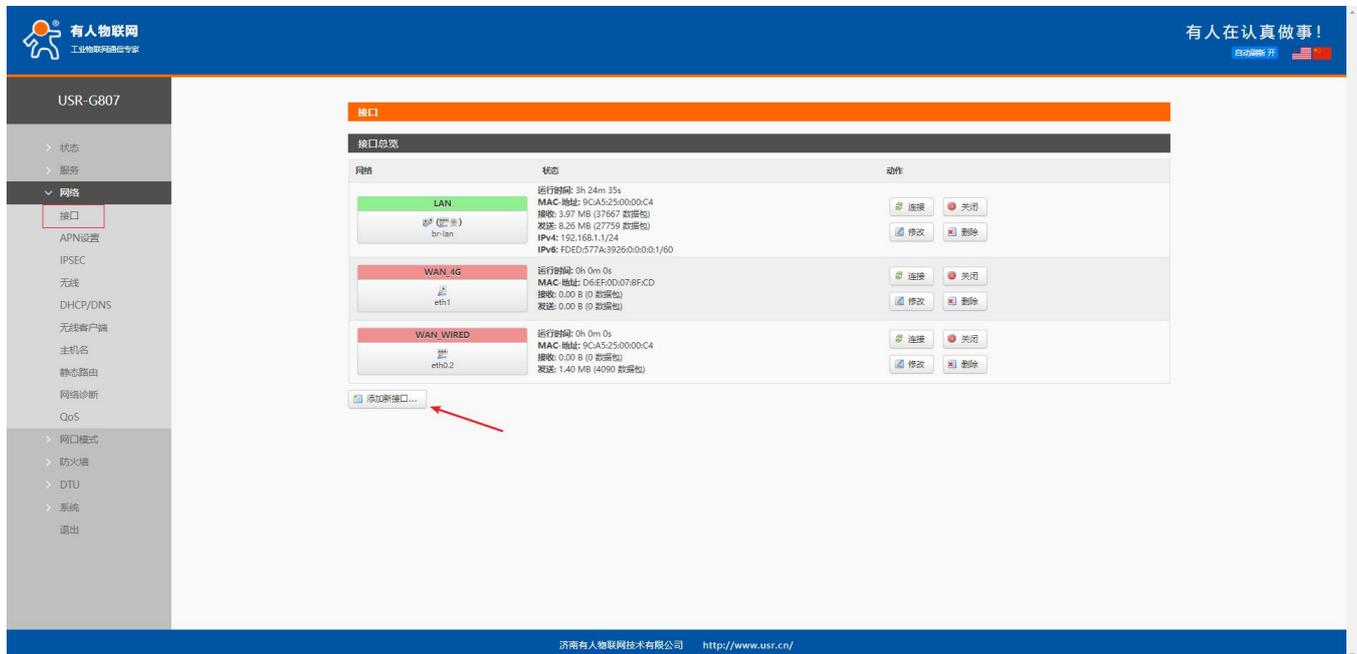


图 52 创建接口

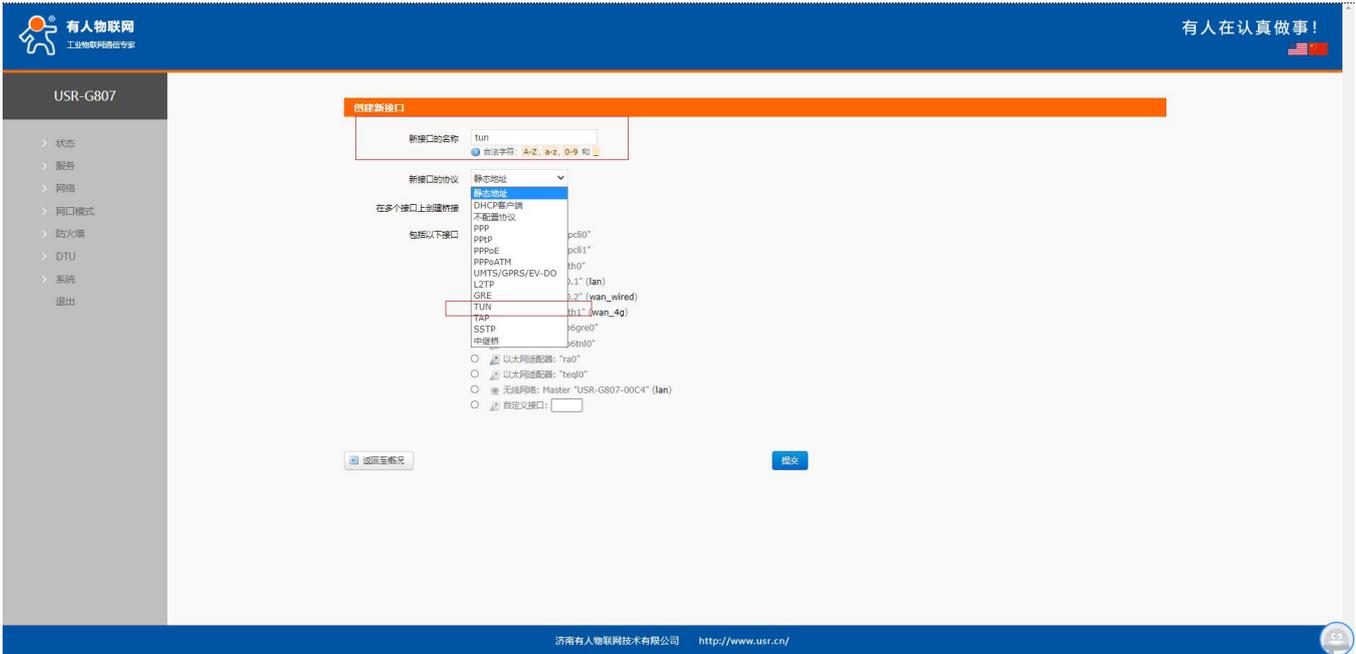


图 53 创建 OpenVPN 接口

基本设置配置参数解释：

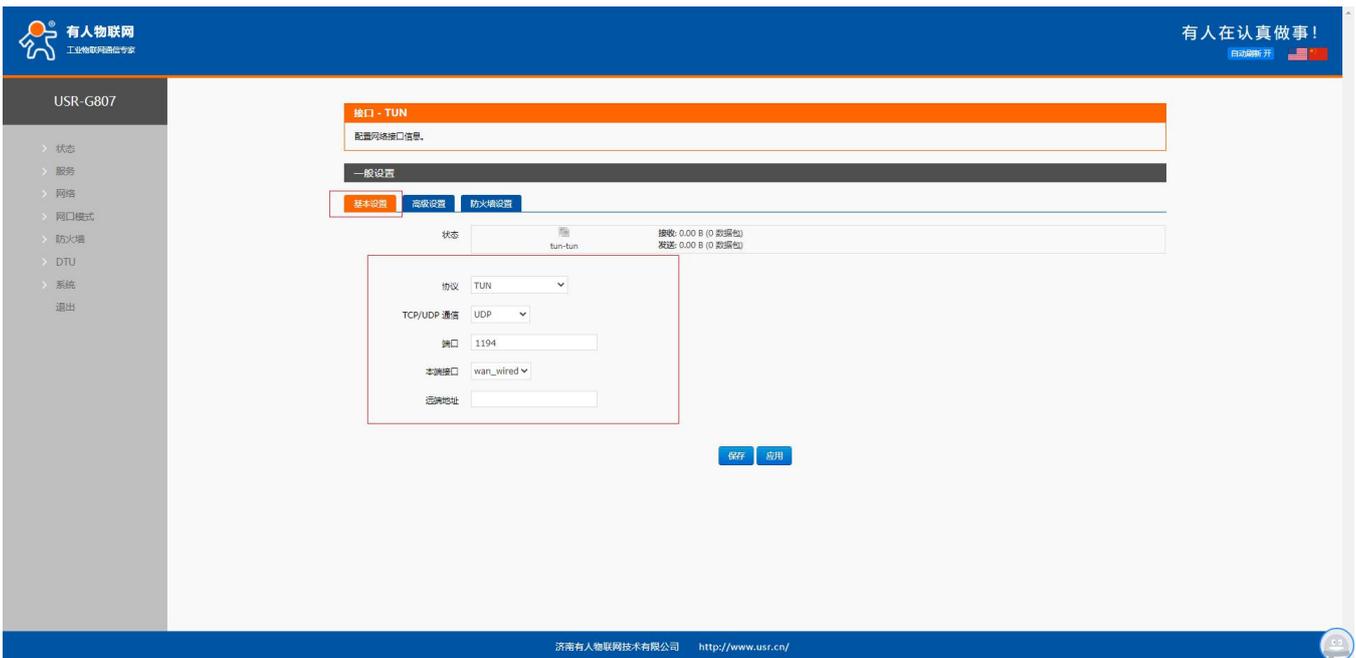


图 54 基本设置

- 协议：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；
- 本端接口：可以是 wan_wired、wan_4g；
- 远程地址：服务器的 IP/域名；
- 本地隧道地址：可以设置本端的隧道地址，如：192.168.10.1，不填默认服务器自动分配；
- 远端隧道地址：可以设置对端的隧道地址，如：192.168.10.1，不填默认服务器自动分配。

高级设置配置参数解释：

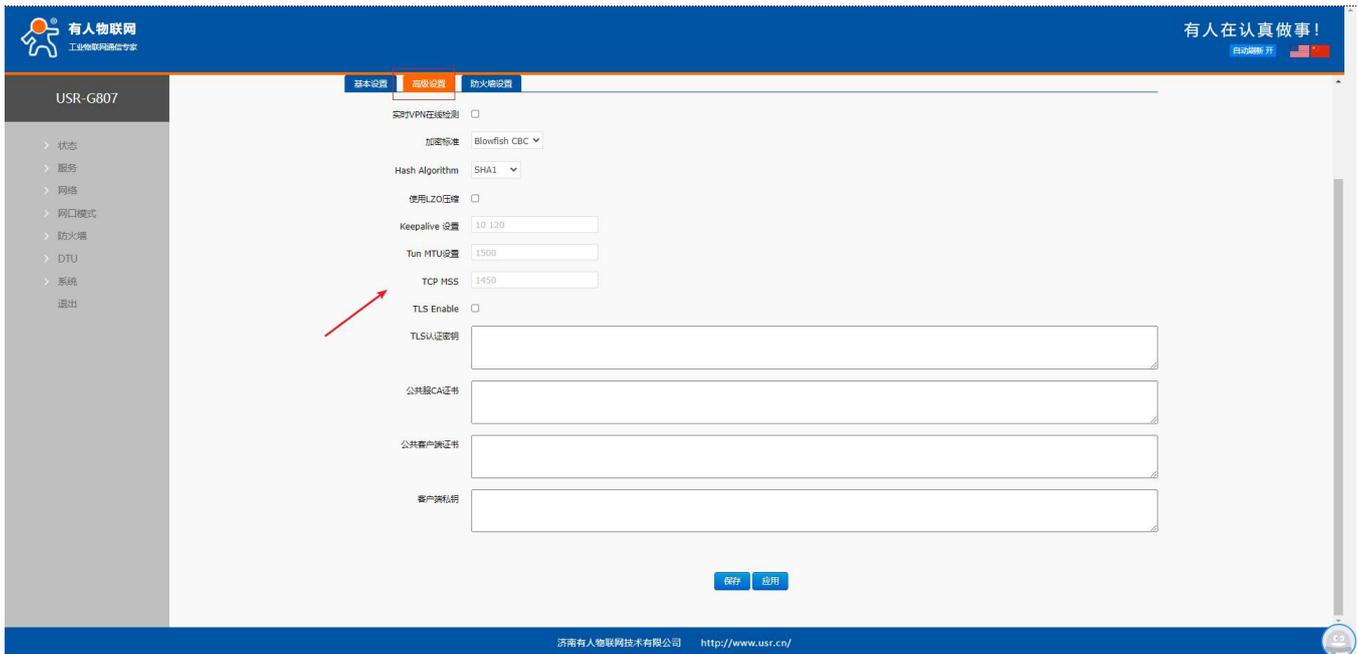


图 55 OpenVPN 高级设置

<说明>

- 加密标准：通道加密标准包括：Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC 五种加密。
- 使用 LZO 压缩：启用或禁用传输数据使用 LZO 压缩。
- Keepalive 设置：默认为 10 120
- TUN MTU 设置：设置通道的 MTU 值。该项需和 VPN 服务器端保持一致。
- TCP MSS：TCP 数据的最大分段大小
- TLS 认证密钥：安全传输层的认证密钥。
- 公共服 CA 证书：服务器和客户端公共的 CA 证书
- 公共客户端证书：客户端证书
- 客户端私钥：客户端的密钥
- 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复制到配置界面对应的编辑框中即可。

4.6. GRE 搭建

创建接口

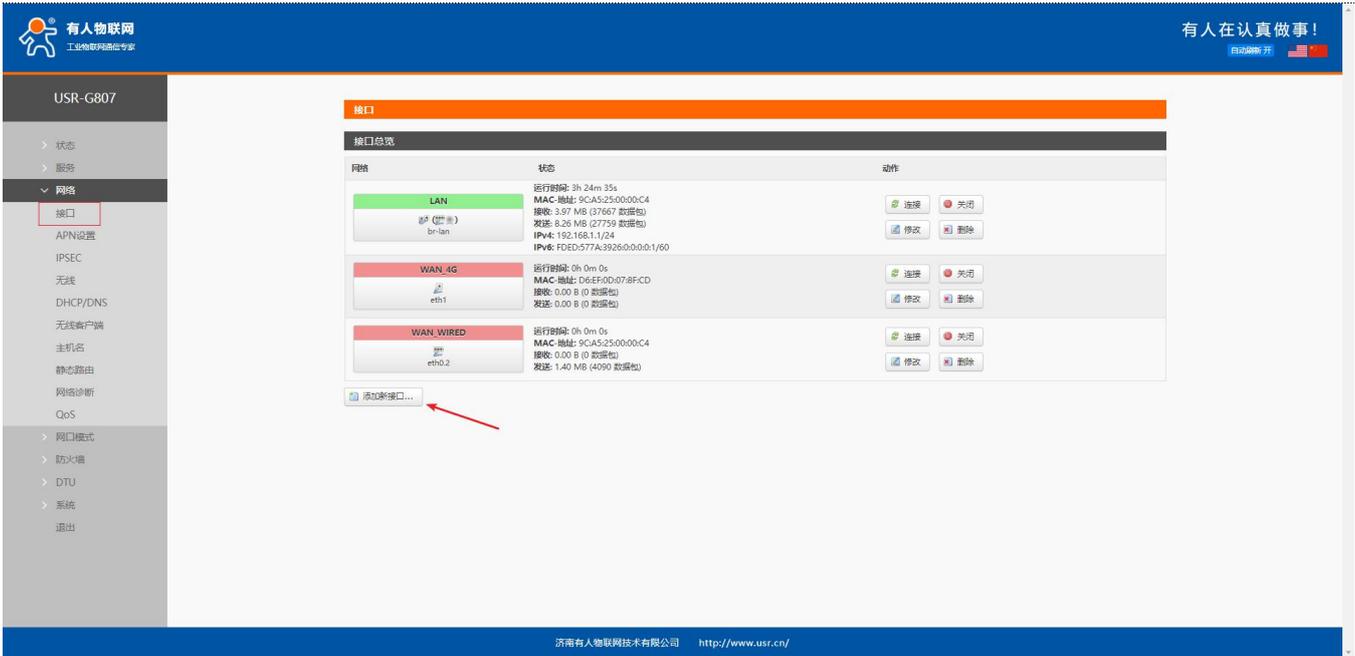


图 56 创建接口

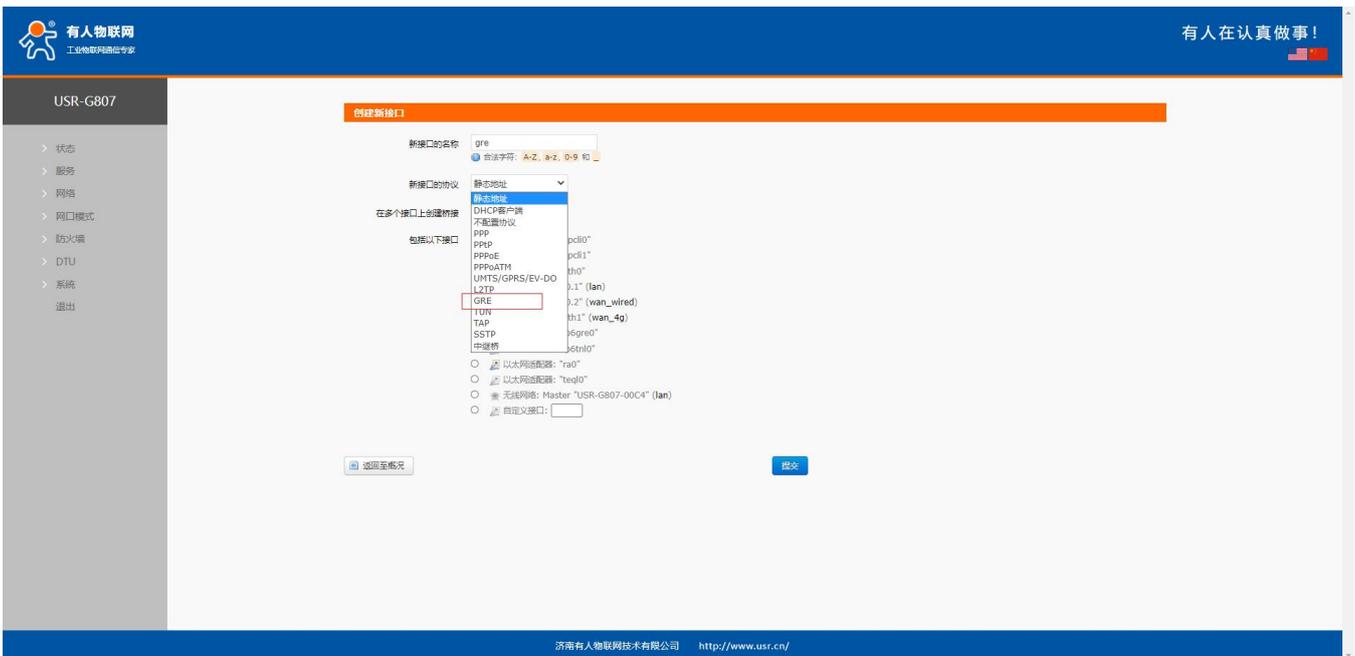
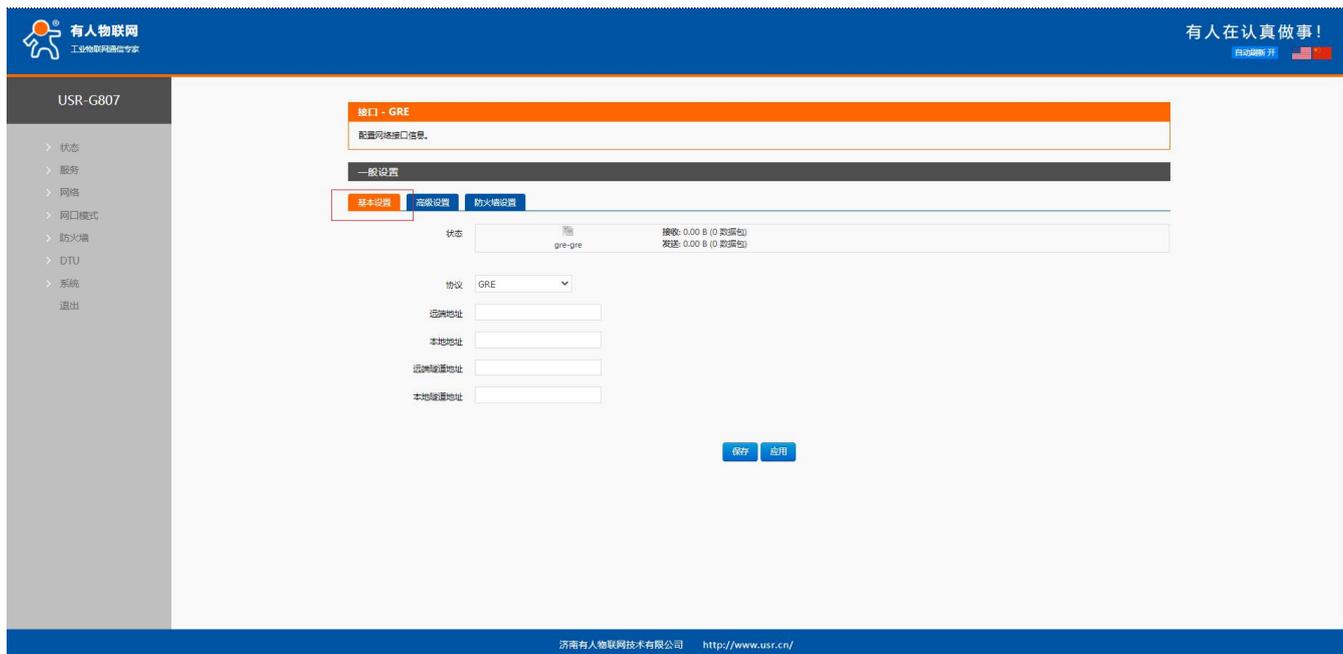


图 57 创建 GRE 接口

基本设置参数解释:



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_wried、wan_4g 的地址，两者根据需要输入；
- 远端隧道地址：对端的 GRE 隧道 IP，对与设置子网掩码可以按照如下规定表示：
- 255.0.0.0 可以写成 IP/8、255.255.0.0 可以写成 IP/16、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。

高级设置参数解释

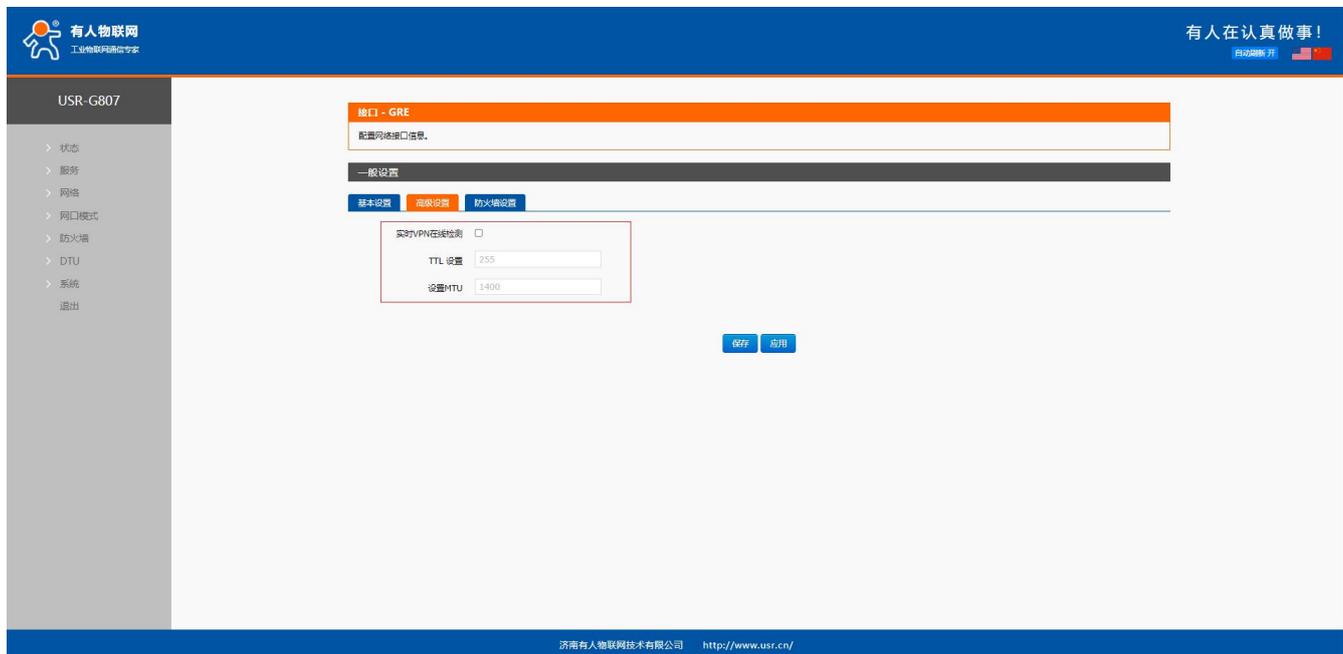


图 58 GRE 高级配置

- 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.例如首先我在虚拟机创建一个 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

```
root@edu-virtual-machine:~# ifconfig
eth0      Link encap:以太网  硬件地址 00:0c:29:ff:1f:d5
          inet 地址:192.168.13.66 广播:192.168.13.255 掩码:255.255.255.0
          inet6 地址: fd79:1a72:ee3d:0:d158:a02f:5442:1169/64 Scope:Global
          inet6 地址: fd79:1a72:ee3d:0:20c:29ff:feff:1fd5/64 Scope:Global
          inet6 地址: fe80::20c:29ff:feff:1fd5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  跃点数:1
          接收数据包:1455  错误:0  丢弃:9  过载:0  帧数:0
          发送数据包:545  错误:0  丢弃:0  过载:0  载波:0
          碰撞:0  发送队列长度:1000
          接收字节:135430 (135.4 KB)  发送字节:85191 (85.1 KB)
          中断:19  基本地址:0x2024

gre-test  Link encap:未指定  硬件地址 C0-A8-0D-42-00-00-00-00-00-00-00-00-00-00-00-00
          inet 地址:10.10.10.2 点对点:10.10.10.1 掩码:255.255.255.255
          inet6 地址: fe80::5efe:c0a8:d42/64 Scope:Link
          UP POINTOPOINT RUNNING NDARP  MTU:1476  跃点数:1
          接收数据包:0  错误:0  丢弃:0  过载:0  帧数:0
          发送数据包:3  错误:0  丢弃:0  过载:0  载波:0
          碰撞:0  发送队列长度:0
          接收字节:0 (0.0 B)  发送字节:168 (168.0 B)

lo        Link encap:本地环回
          inet 地址:127.0.0.1 掩码:255.0.0.0
          inet6 地址: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  跃点数:1
          接收数据包:118  错误:0  丢弃:0  过载:0  帧数:0
          发送数据包:118  错误:0  丢弃:0  过载:0  载波:0
          碰撞:0  发送队列长度:0
          接收字节:8932 (8.9 KB)  发送字节:8932 (8.9 KB)

root@edu-virtual-machine:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
```

图 59 GRE 测试 1

2.服务器搭建好之后，在 USR-G807 的 GRE 配置界面做相应的配置。点击保存&应用后，看到到看 IP、数据、时间均不为空表示搭建成功。



图 60 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。

```

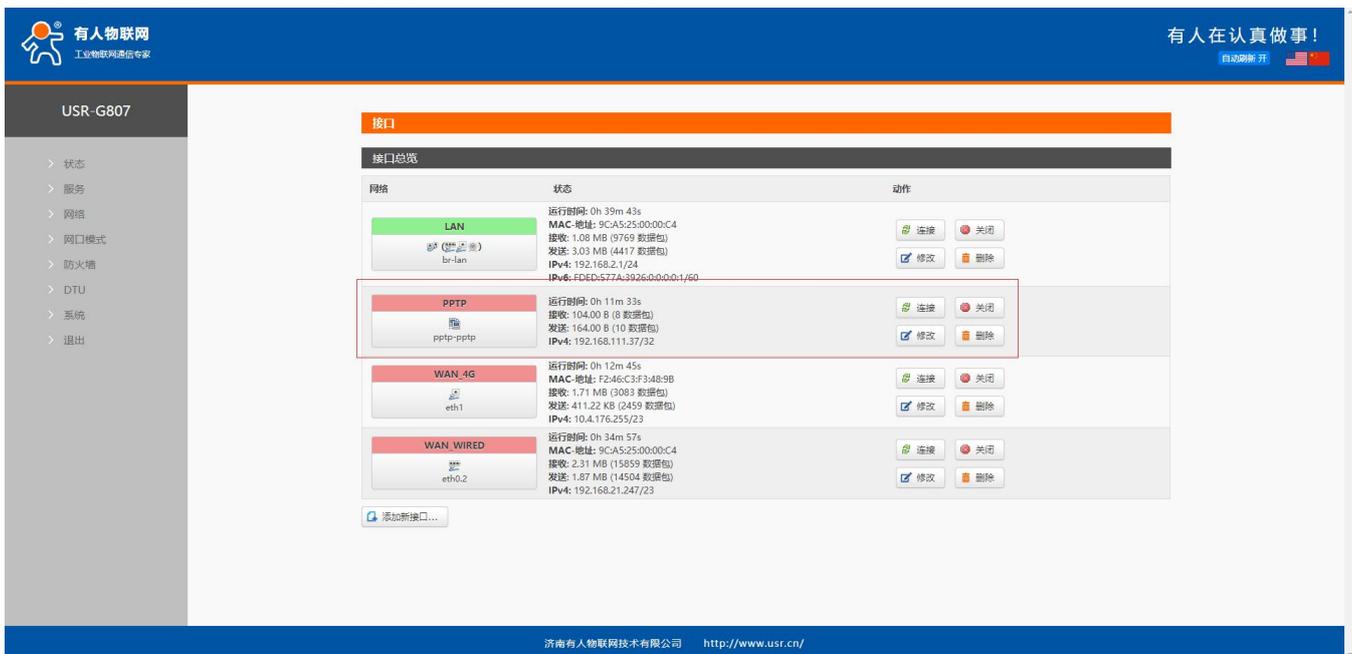
root@edu-virtual-machine:~# ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms (DUP!)
64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=1.24 ms (DUP!)
64 bytes from 10.10.10.1: 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 61 GRE 测试 3

4.7. VPN + 端口转发

VPN + 端口转发，可实现 4G 路由器之间的异地访问。

在路由器下的设备，可以通过端口转发直接进行 socket 通信。



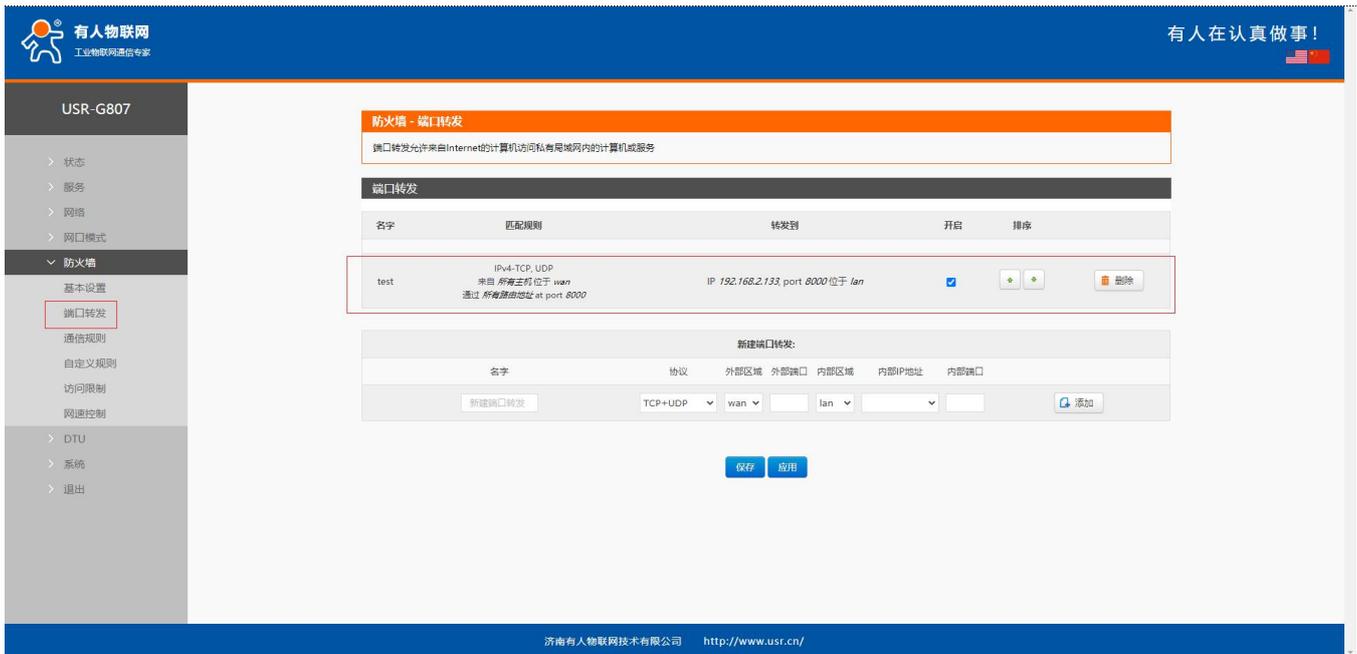


图 62 端口转发设置页面

WAN 口网线没插，只使用 4G 接口。PC 两台，4G 路由器一台（使用 4G 接口）

路由器连接 PPTP Server, 设置端口转发，外部端口 8000，内网 IP 地址 192.168.2.133（PC1），内网端口 8000 在 192.168.2.133 上，创建 TCP Server，监听端口 8000。

在电脑 PC2 上连接同一 PPTP Server（注意 PC2 位于其他网络，不在本路由器下），创建 TCP Client，目标 IP 地址 192.168.111.37，目标端口 8000，应当能够连接到 4G 路由器下的 TCP Server 并通信。

4.8. 静态路由

静态路由有如下几个参数

表 11 静态路由参数表

名字	含义	备注
接口	路由规则执行的端口	eth0.2（有线 WAN 口）
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	填 0 即可
MTU	最大传输单元	1500

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：

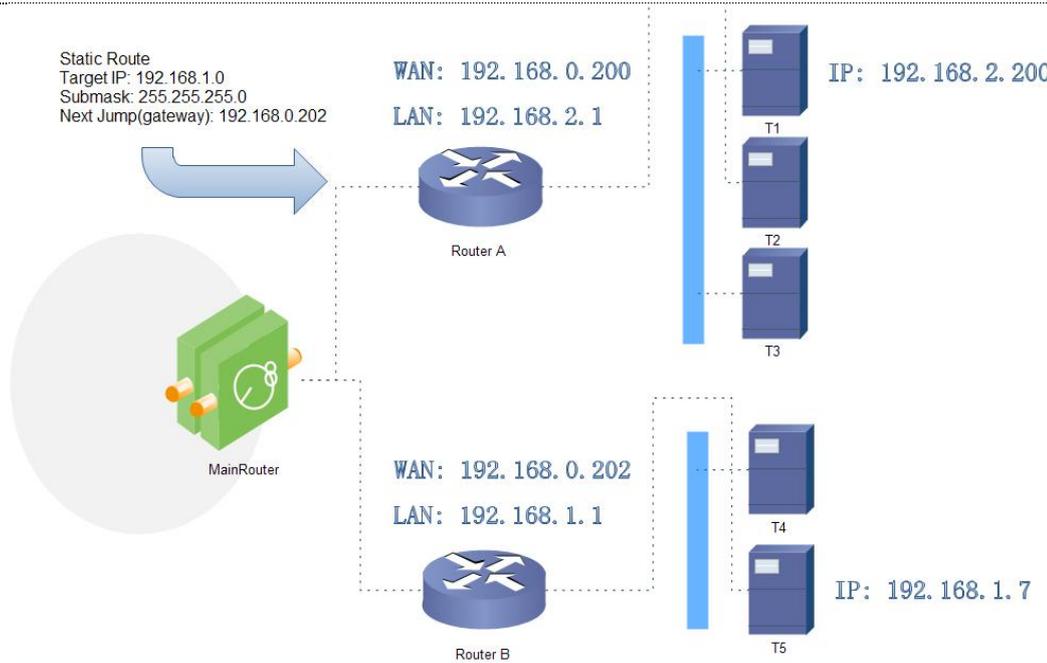


图 63 静态路由表实例图

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：

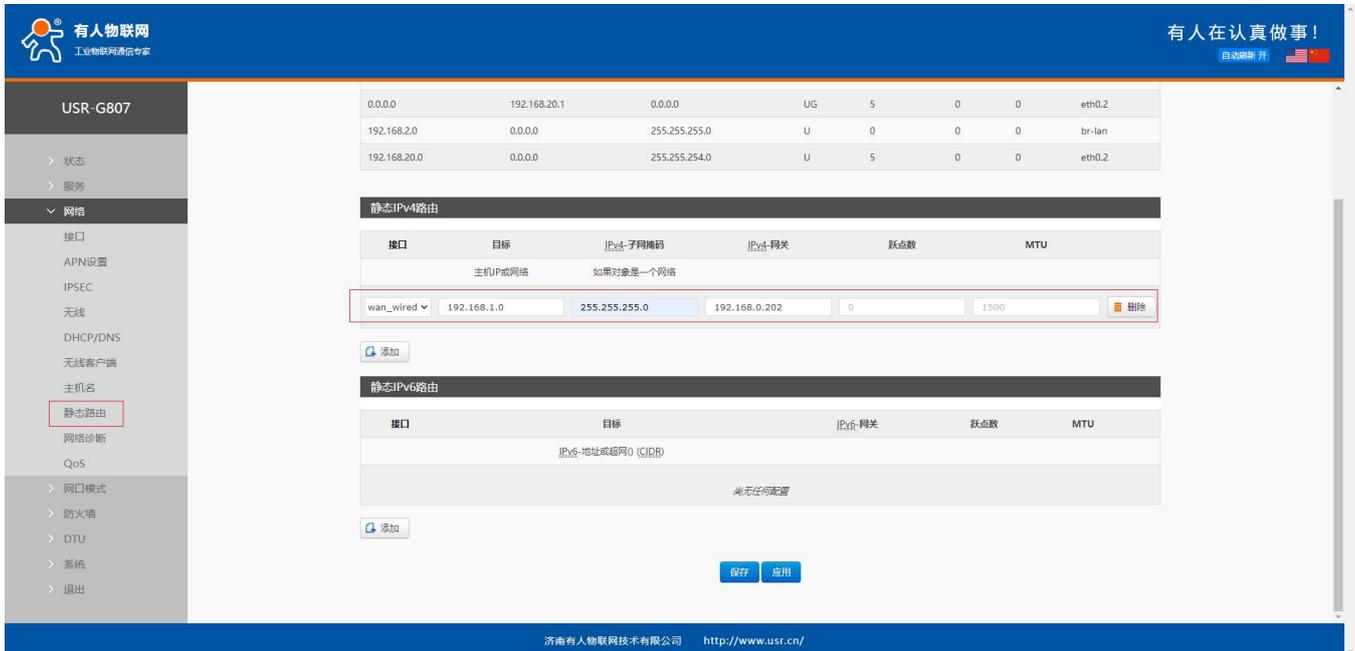


图 64 路由表添加页面

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）。

```
C:\Users\Administrator>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=4ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=63
来自 192.168.1.1 的回复: 字节=32 时间=15ms TTL=63
```

图 65 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 口的。如果我们还想去访问 B 下的设备，比如 T5，还需要做如下处理。

在路由器 B 的防火墙设置，打开 WAN 口到 LAN 口的转发，这样从 WAN 口来的数据包，也可以转发到路由器 B 的 LAN 网络（下图指出了两种路由器的防火墙设置，前者为 USR-G807 的设置，后者为 TP-Link）。

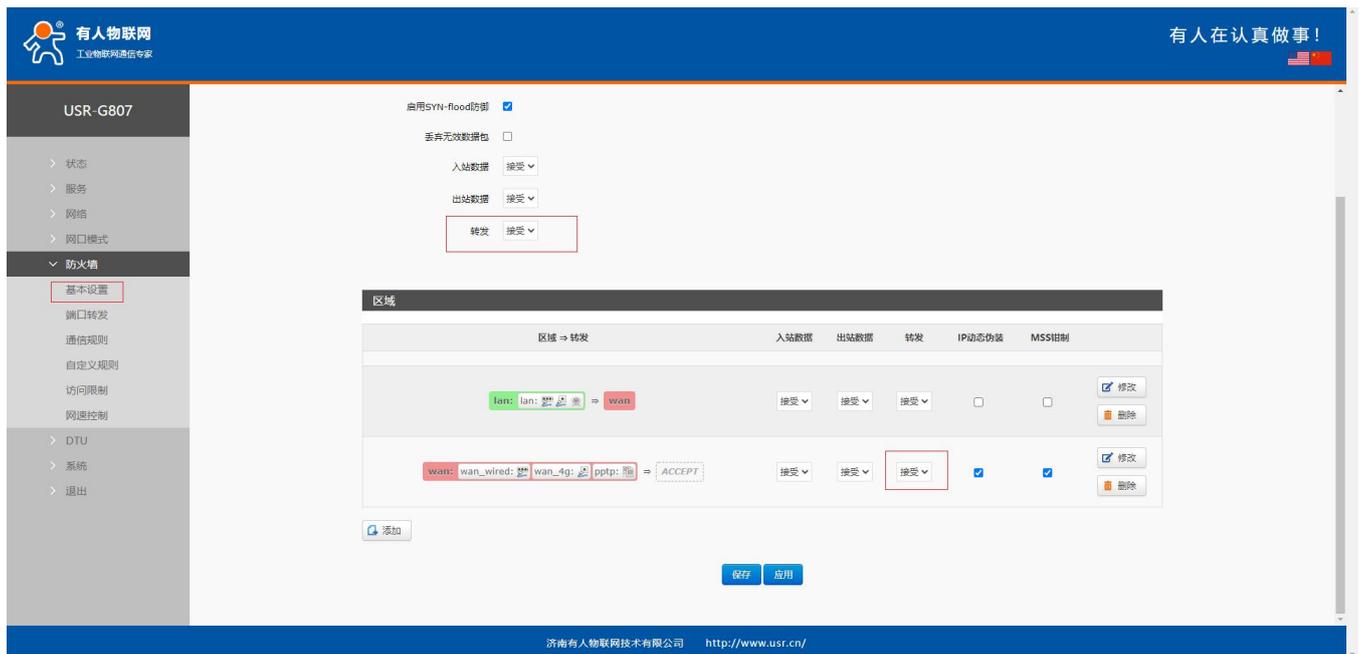


图 66 路由表实例图二

当路由器 B 的防火墙规则设置好后，就可以访问 T5 了。下图表示可以访问路由器 B 下的 T5（192.168.1.7）。

```
C:\Users\Administrator>ping 192.168.1.7

正在 Ping 192.168.1.7 具有 32 字节的数据:
来自 192.168.1.7 的回复: 字节=32 时间=6ms TTL=255
来自 192.168.1.7 的回复: 字节=32 时间<1ms TTL=255
```

图 67 路由表功能测试二

<注意>

本功能为静态路由的图形界面，等同于指令接口（指令接口暂不开放！）。

5. 防火墙功能

5.1. 基本设置

默认两条防火墙规则。

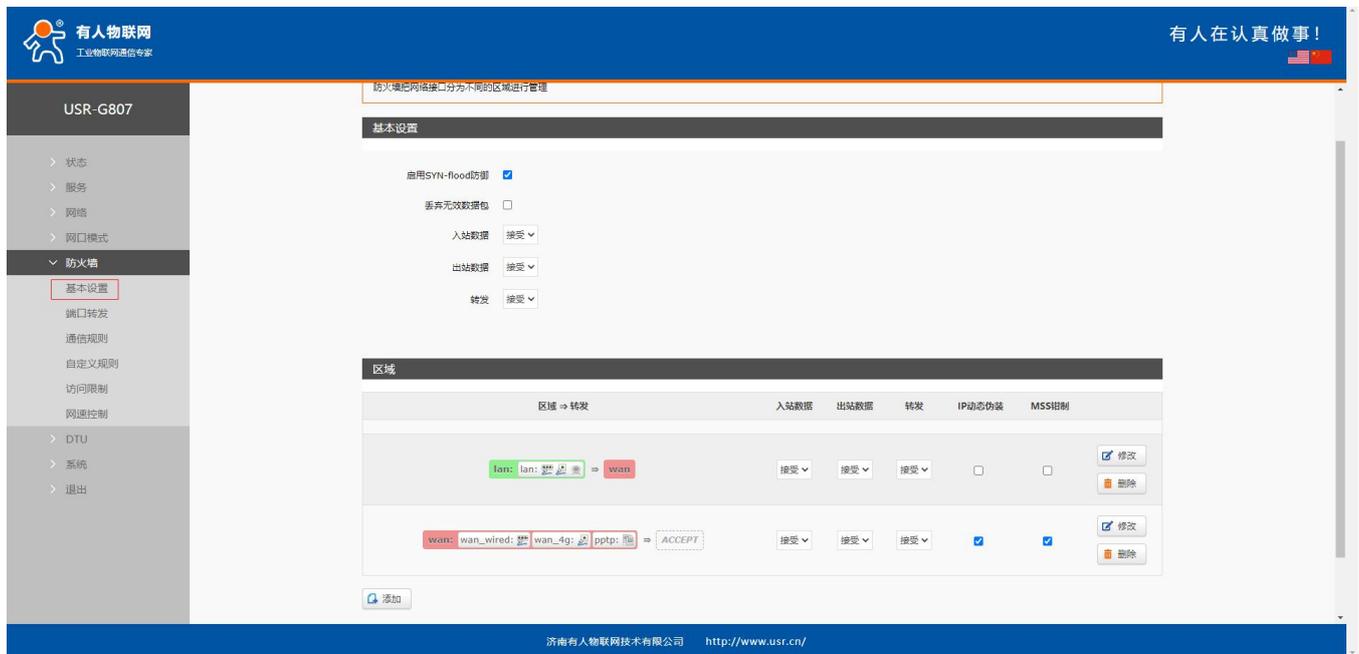


图 68 防火墙设置页面

<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 4G 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 4G 口，接受“入站”，接受“出站”，拒绝“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 4G 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 4G 口，此动作被拒绝。

举例：如果新增了一个网络接口，比如创建了一个 VPN 接口，那么，需要增加一条访问外网的规则，如下：

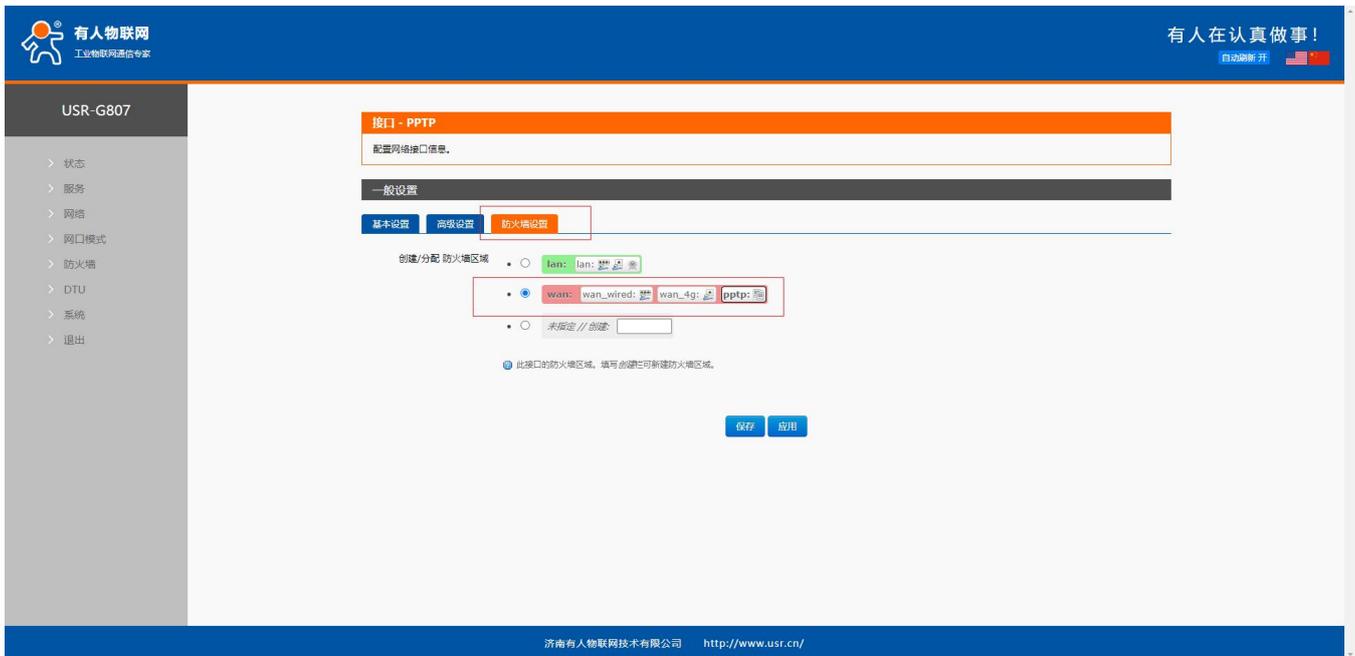


图 69 防火墙设置页面二

5.2. 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。

5.2.1. 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”

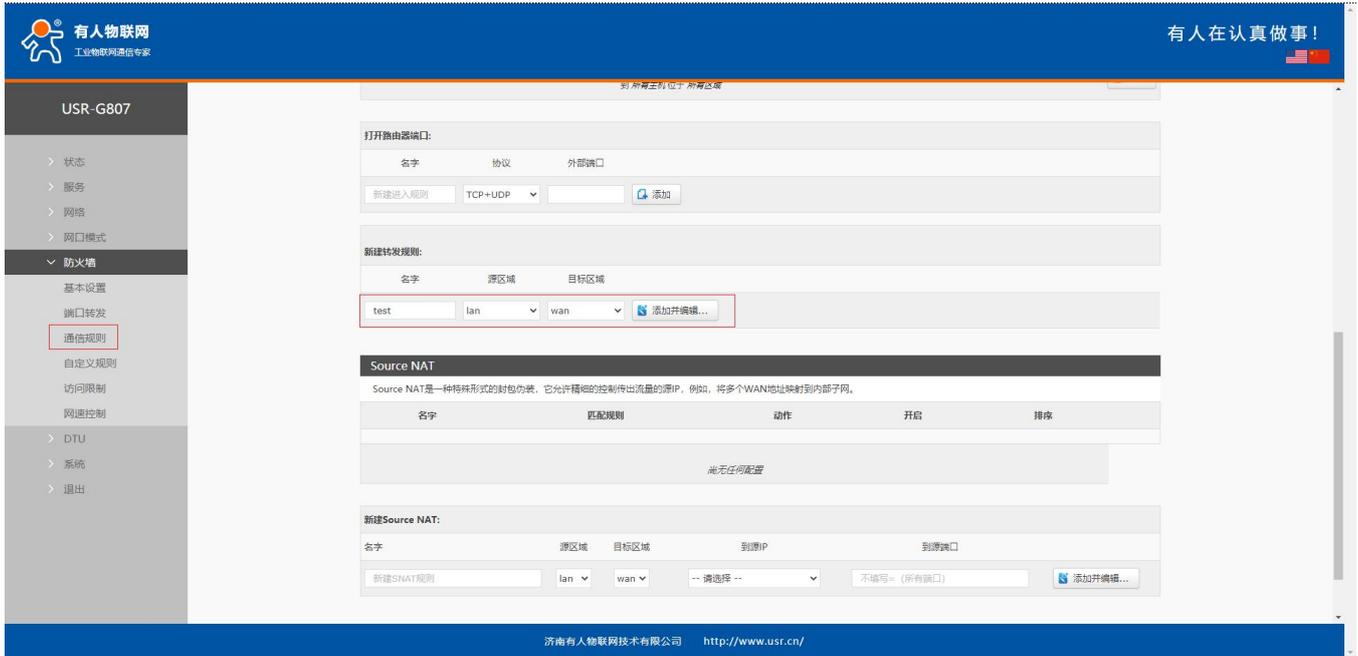


图 70 防火墙黑名单图一

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：

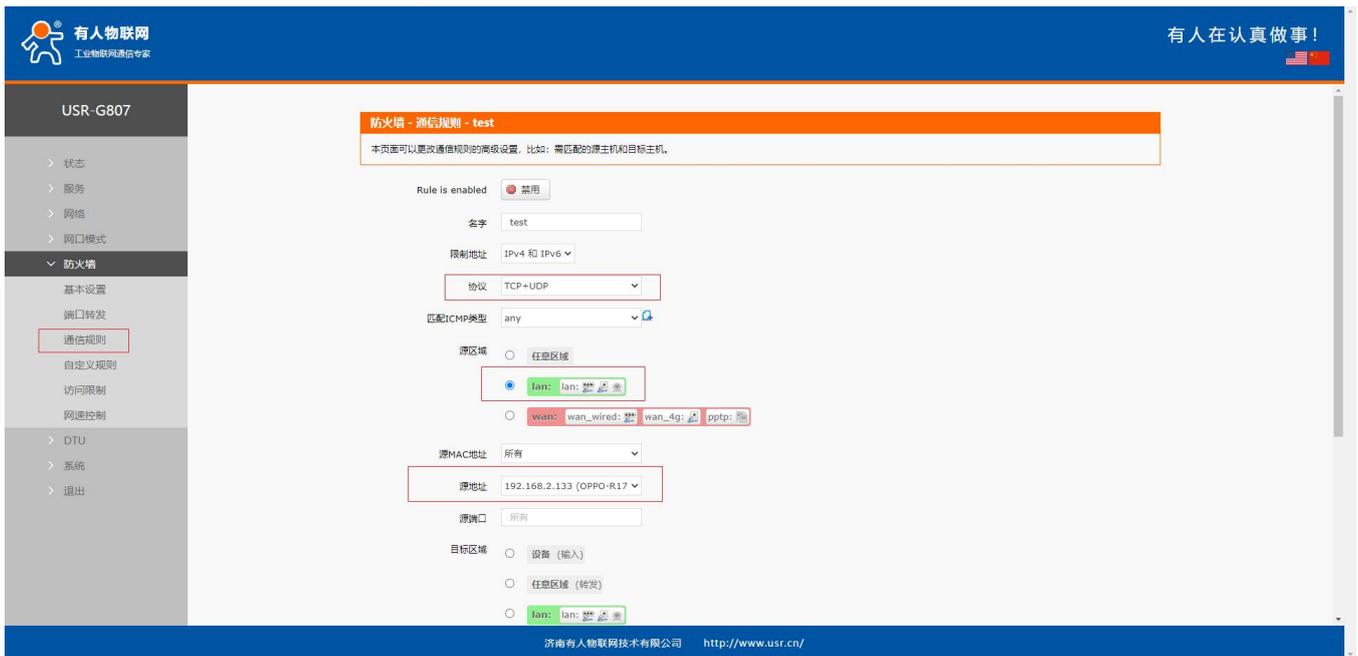


图 71 防火墙黑名单图二

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。

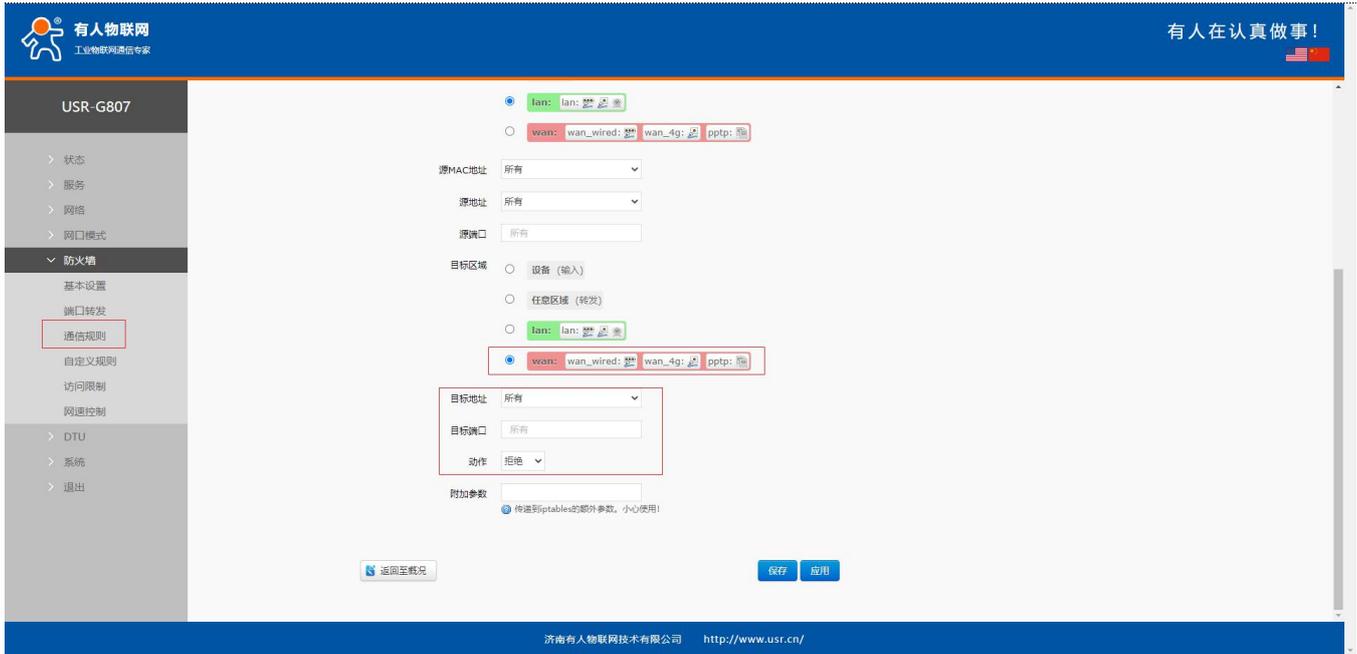


图 72 防火墙黑名单图三

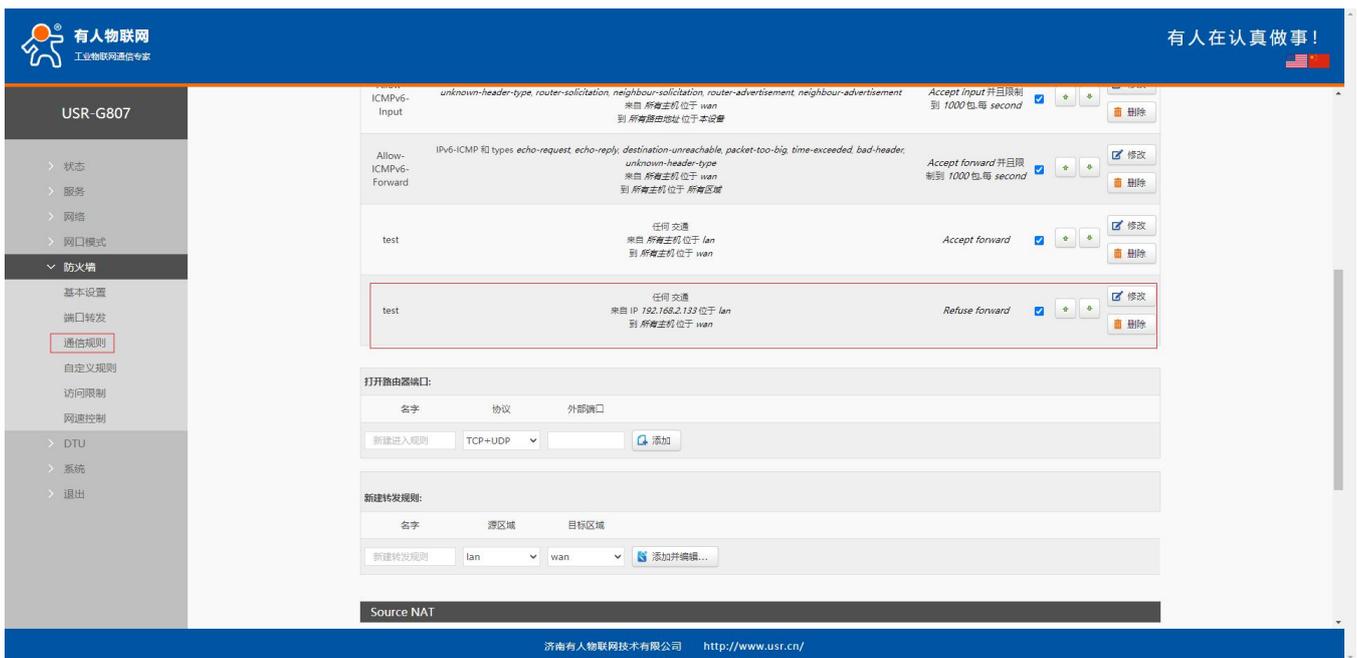


图 73 防火墙黑名单图四

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。

5.2.2. 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”。

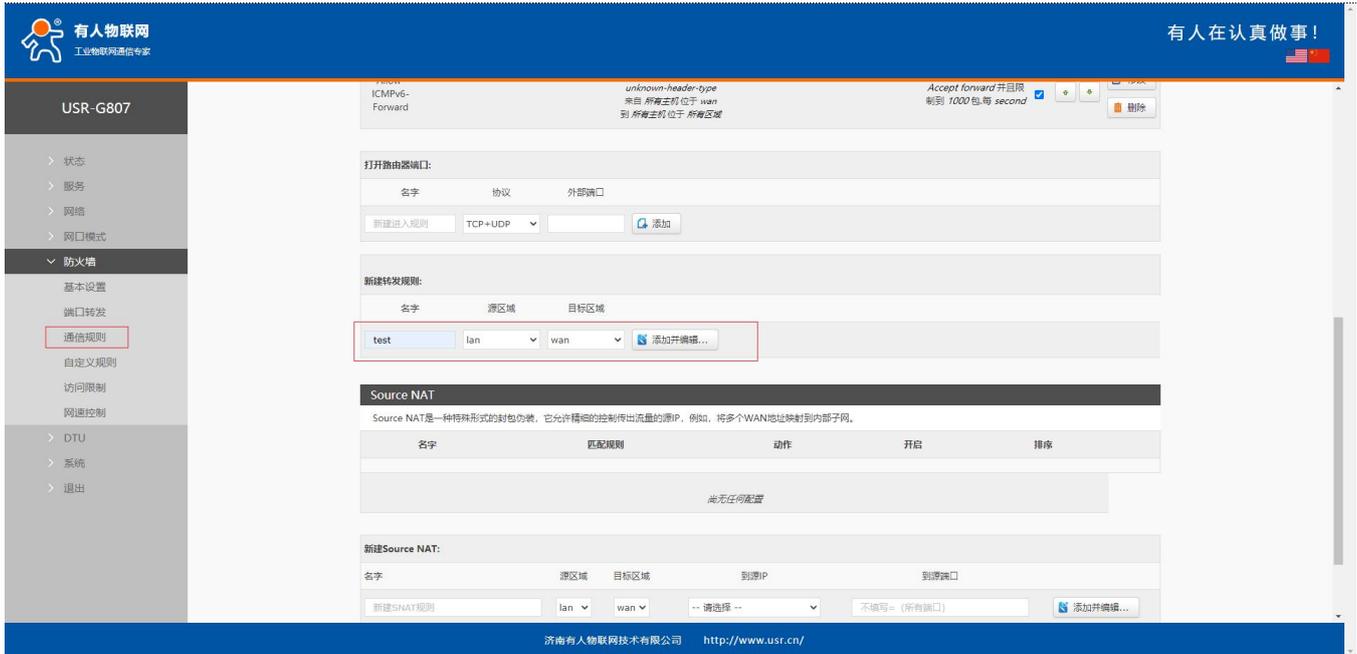


图 74 防火墙白名单图一

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 75 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 76 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

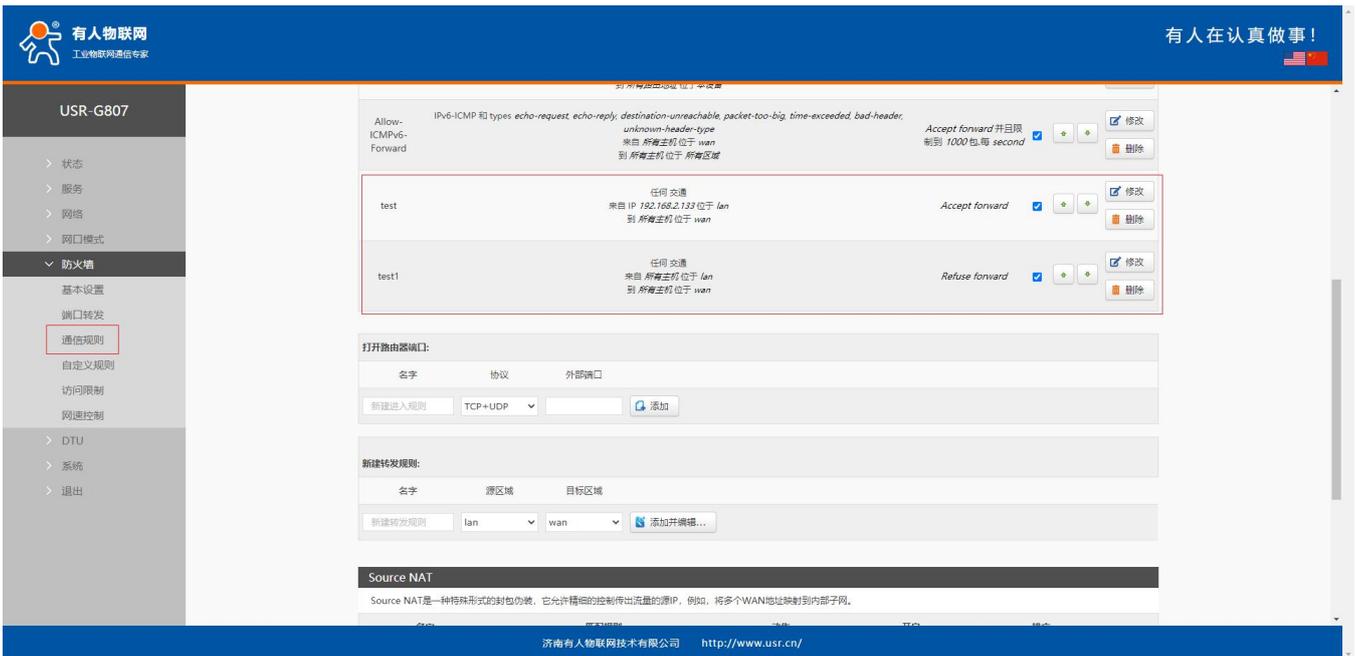


图 77 防火墙白名单图三

5.3. NAT 功能

5.3.1. 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。

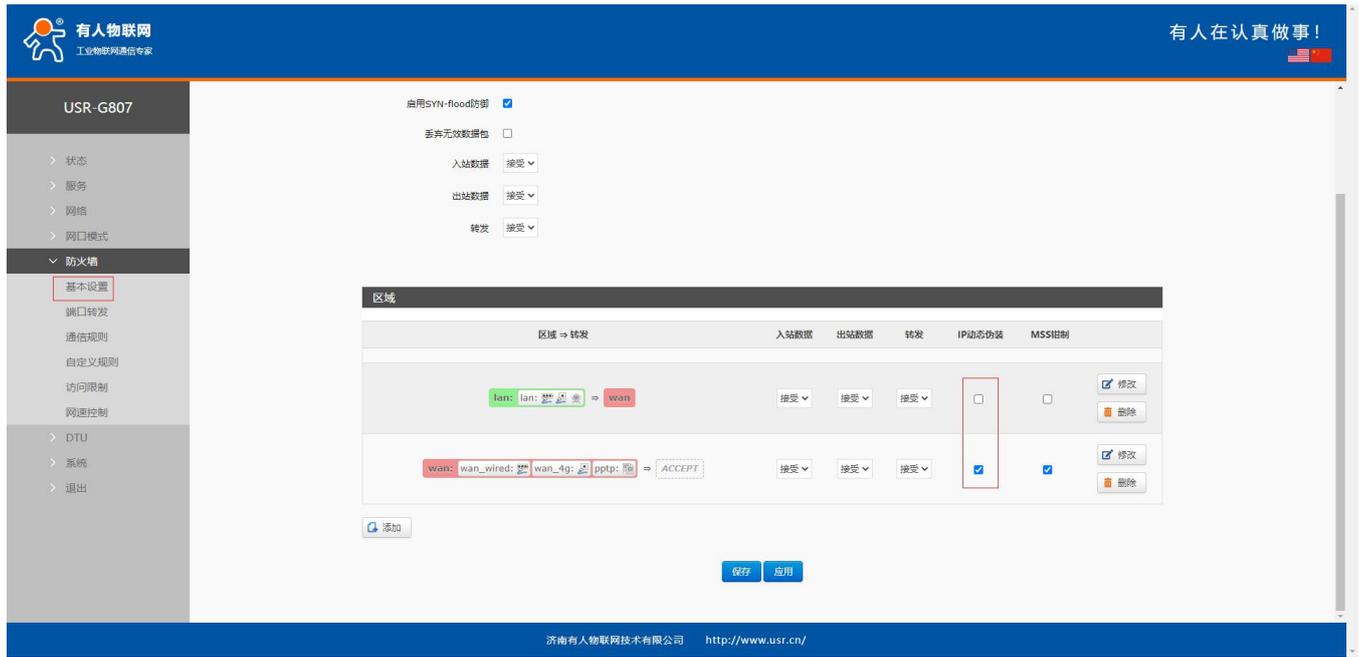
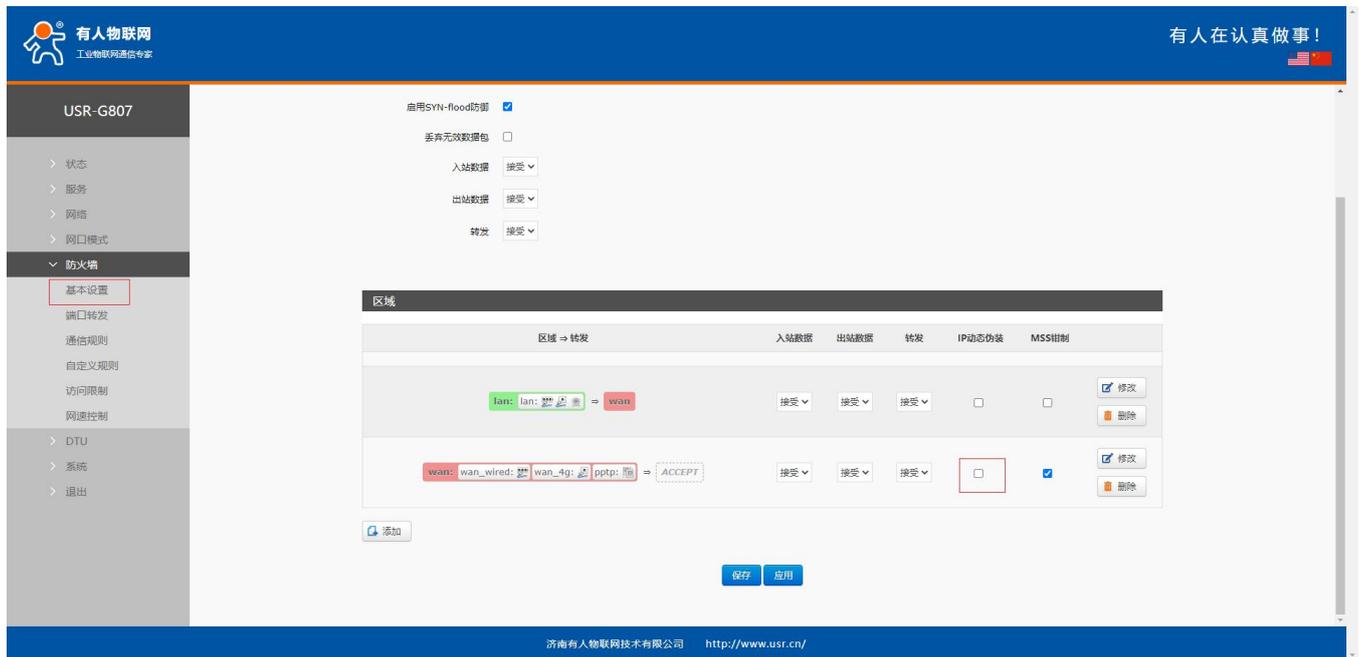


图 78 IP 地址伪装设置

5.3.2. SNAT

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

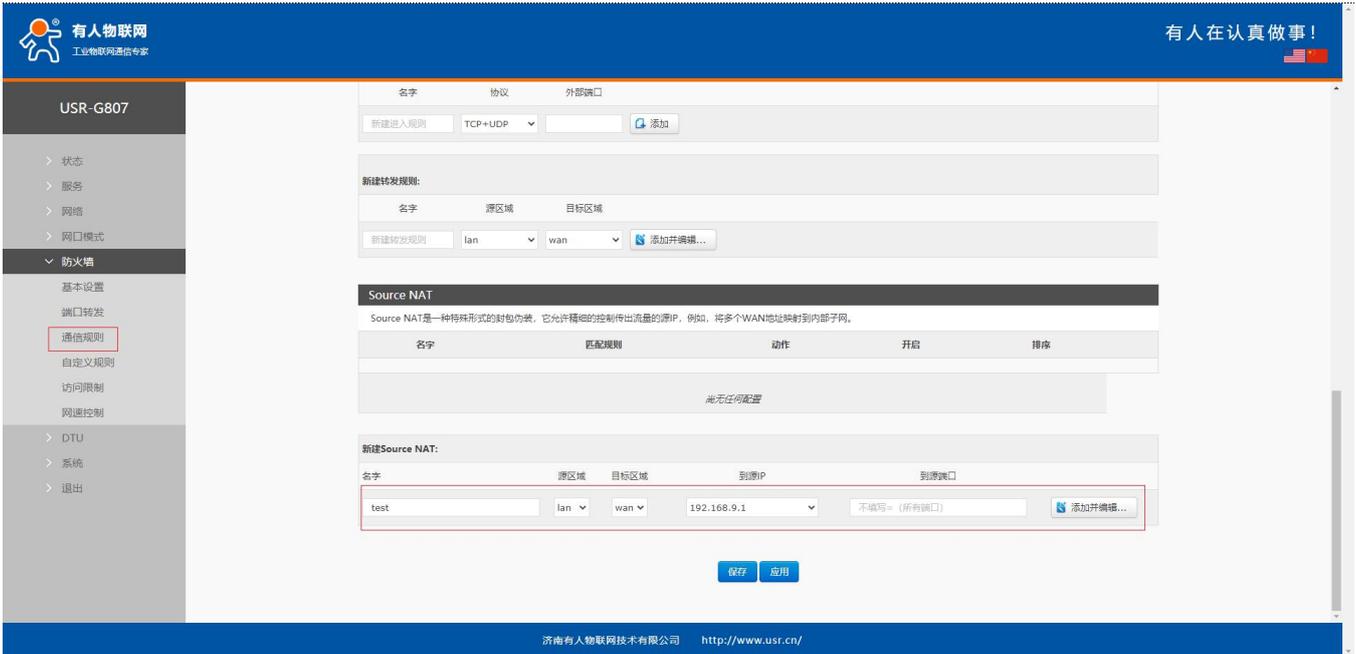


图 79 NAT 设置一

点击添加并编辑



图 80 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。

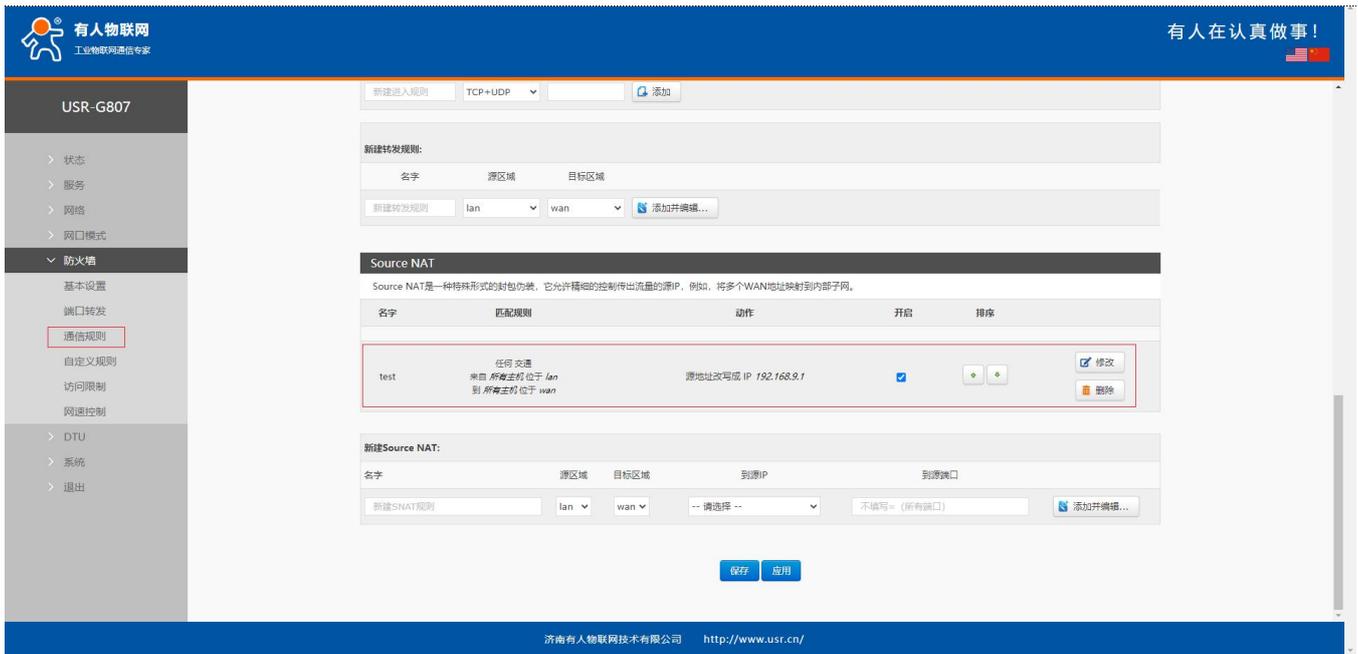


图 81 NAT 设置三

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：

The screenshot shows a network traffic capture tool interface. The filter is set to 'ip.addr == 192.168.13.4'. The table below shows the captured traffic:

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 82 NAT 验证

5.3.3. 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。

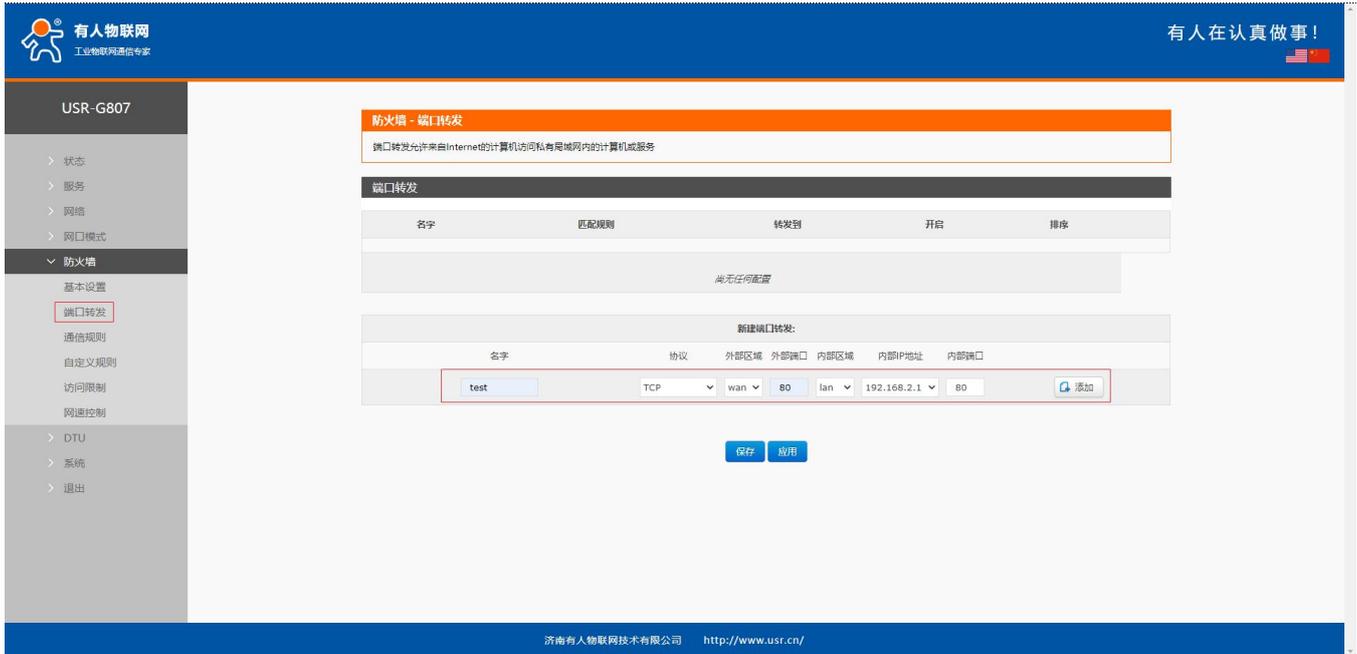


图 83 端口设置页面一

- 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；
- 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。

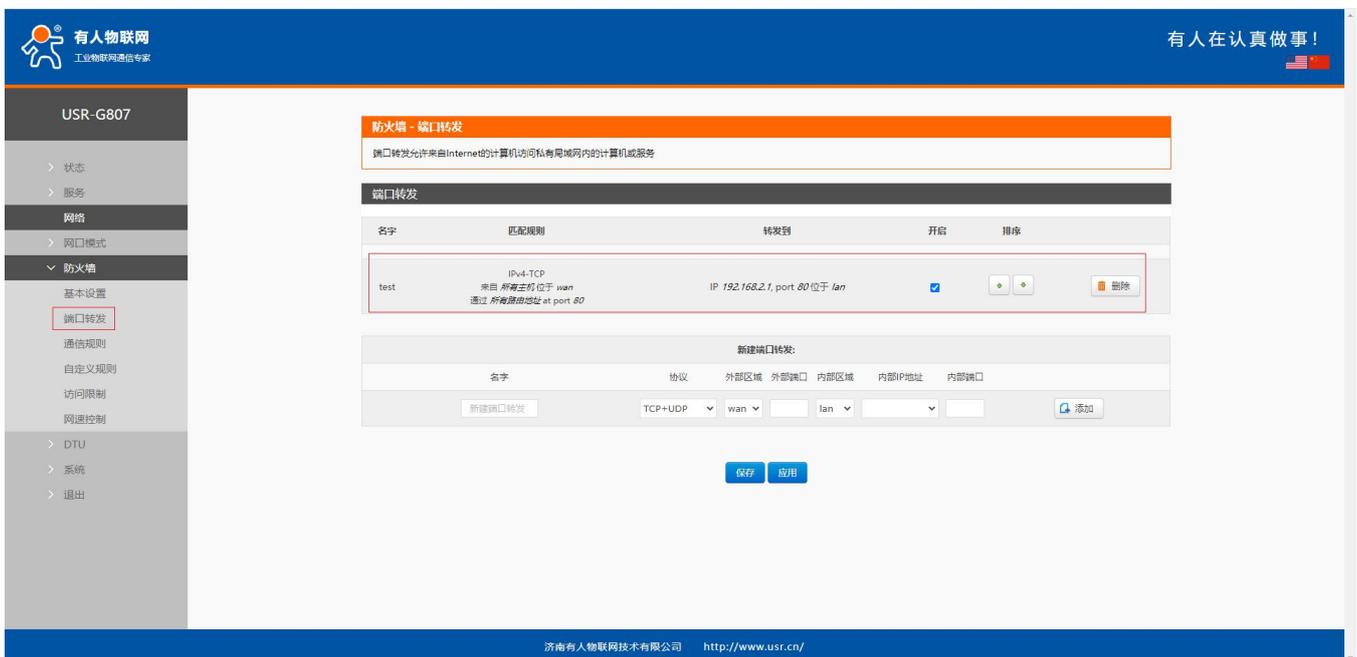


图 84 端口设置页面二

5.3.4. 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。

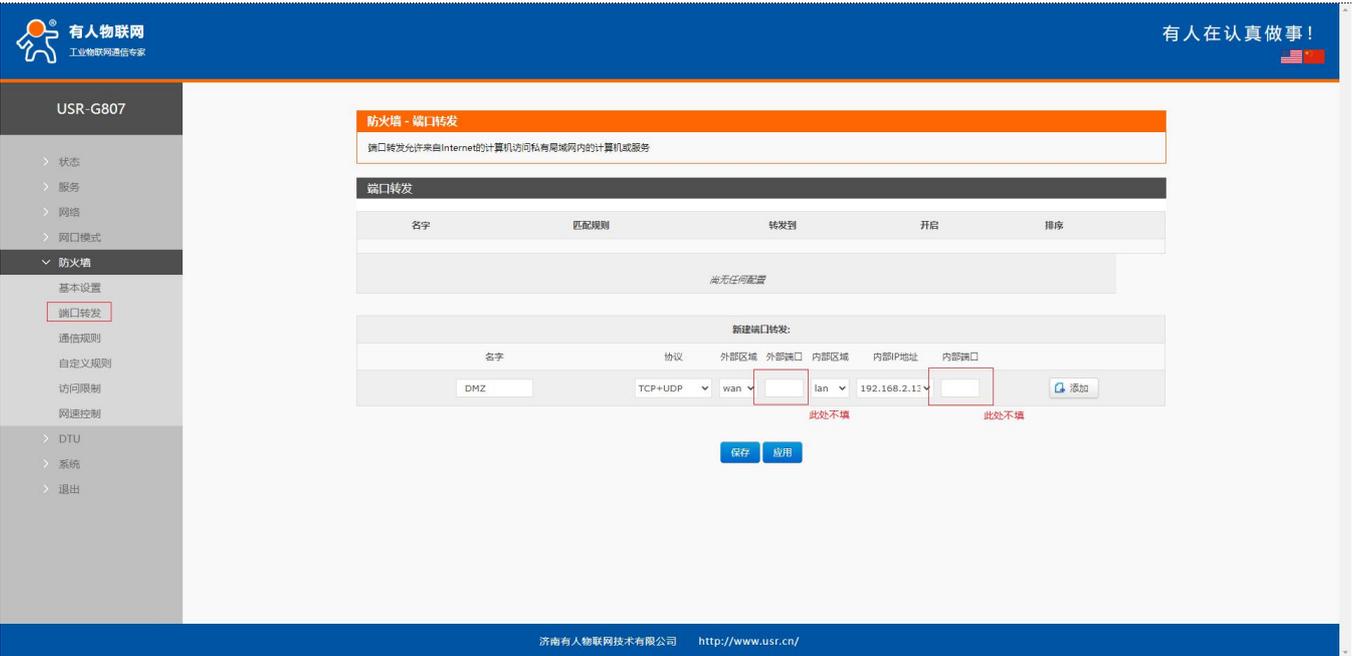


图 85 DMZ 设置一

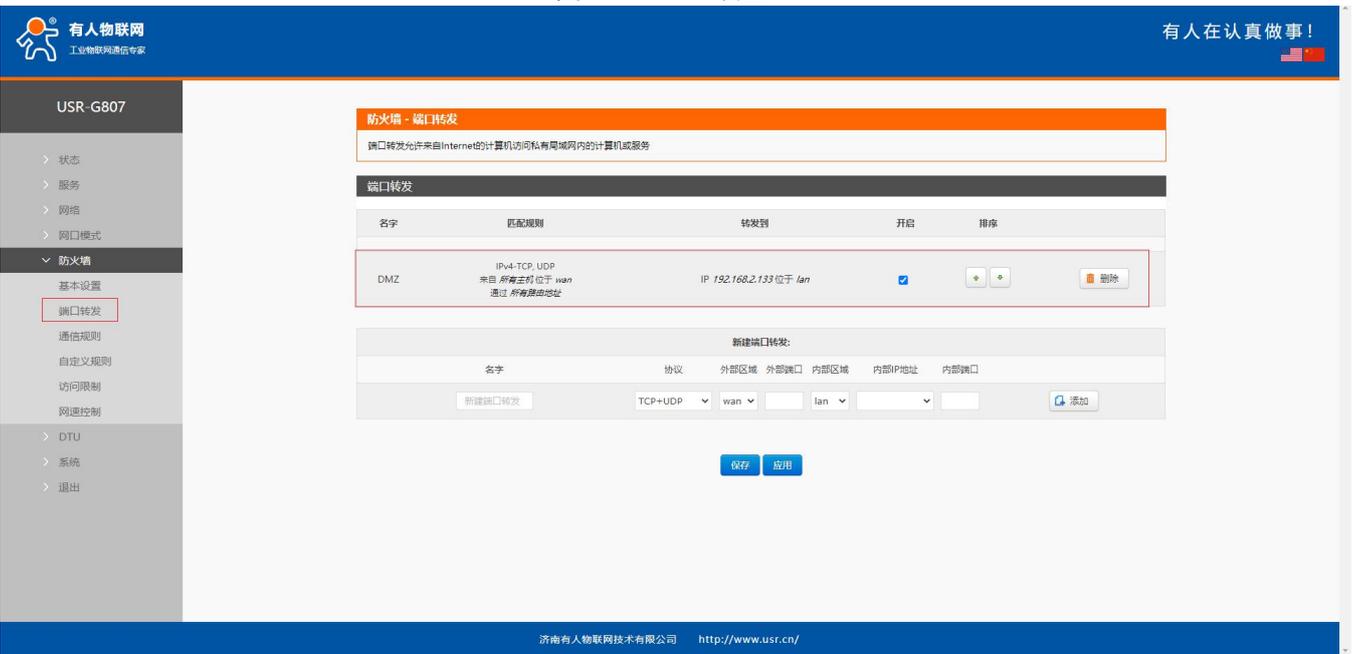


图 86 DMZ 设置二

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。

5.4. 自定义规则

自定义规则可以实现前面的功能，只不过需要写入指令运行。目前支持 Iptables 指令。如果需要可以查阅 linux Iptables 的相关指令说明。

5.5. 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，和白名单都可以设置多条，此功能默认关闭。

5.5.1. 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。

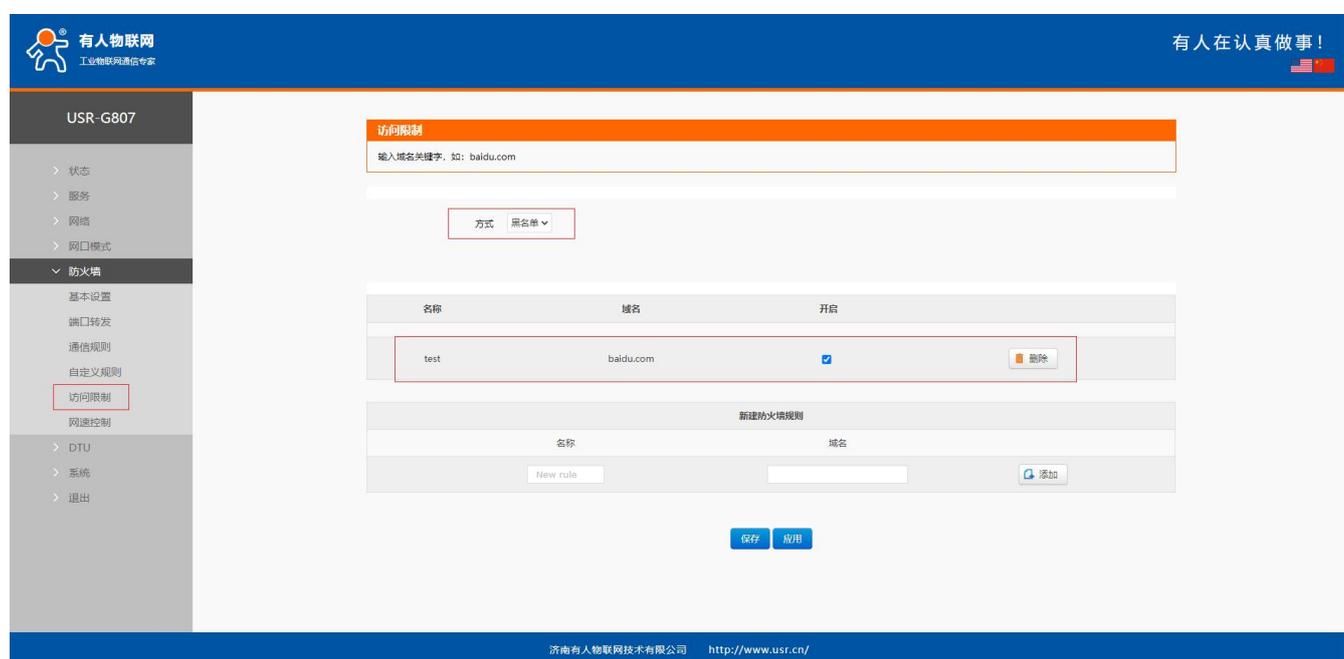


图 87 域名黑名单

5.5.2. 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。

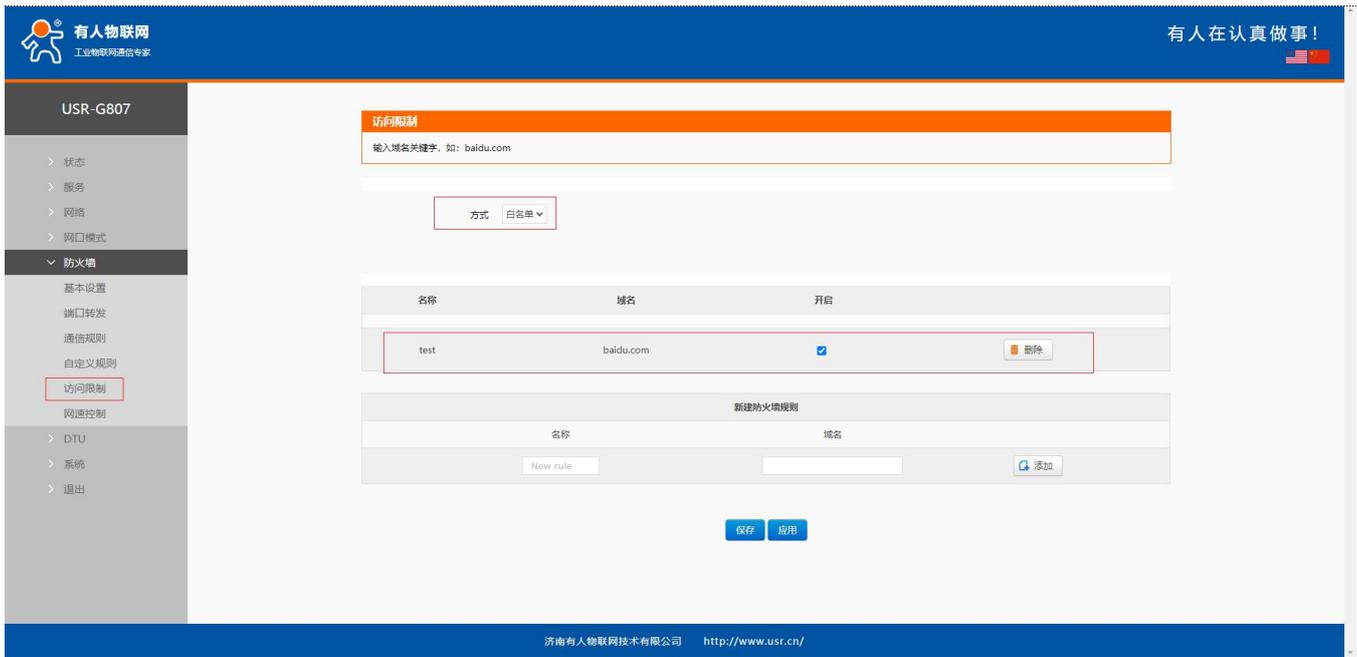


图 88 域名白名单

5.6. 网速控制

网速控制可以限制连接路由器的设备访问网络的上下速率，支持 IP 段地址限速和 MAC 地址限速，规则可以同时添加多条。IP 段限速，需要填写起始 IP 地址、终止 IP 地址、下行速率、上行速率，MAC 地址限速，需要选择 MAC，填写上行速率、下行速率，规则规则设置点击应用保存立即生效。限制上下行速率最低为 10KB/S，若设置的数值小于 10 的，按 10 处理。如图 192.168.1.10-192.168.1.100 网段限制访问网络的最高上行和下行速率为 100KB/S，MAC 地址：00:25:AB:84:66:6E 对应的设备限制访问网络的最高上行和下行速率为 200KB/S。设置时下行速率一般要大于上行速率。

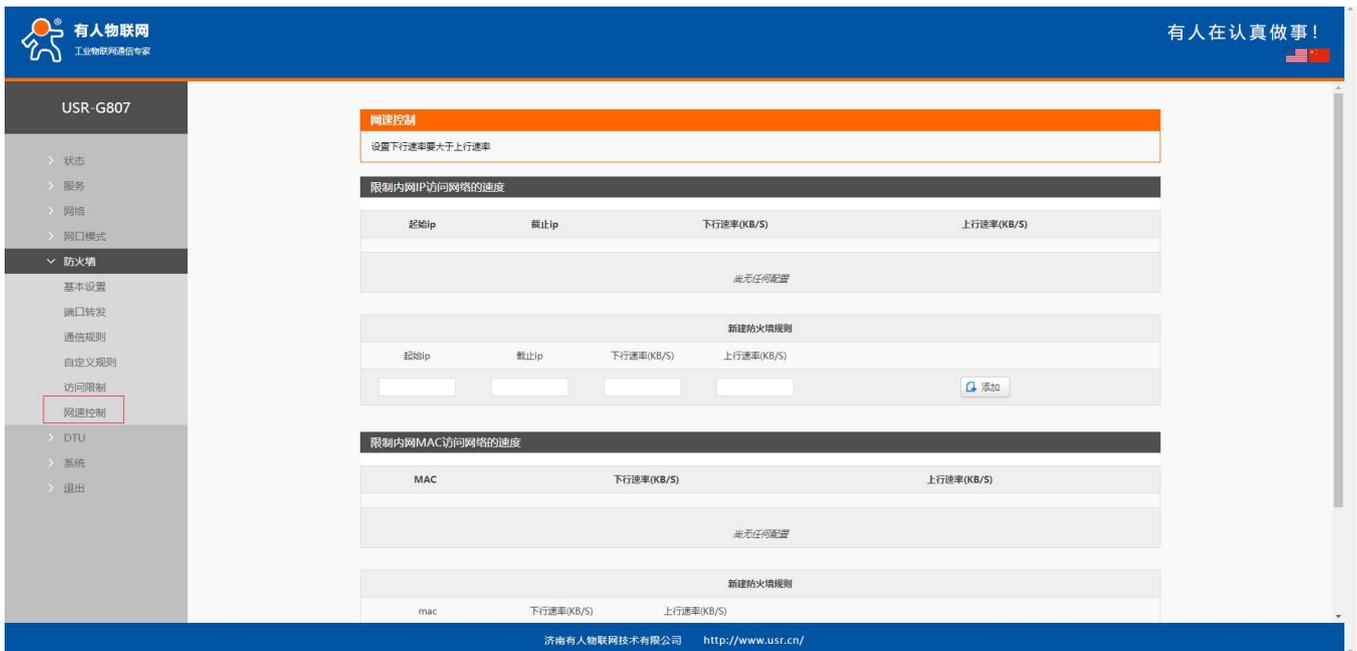


图 89 网速控制

参数列表：

表 12 网上控制参数表

功能	参数设置（如果要使用）	备注
起始 IP	限速网段的起始 IP	IPV4
截止 IP	限速网段的截止 IP	IPV4
上行速率	限制最大上行速率	单位 字节每秒
下行速率	限制最大下行速率	单位 字节美妙
MAC	限速的 MAC	设备 mac 地址

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，可以实现路由器或终端设备的远程登录与管理，设置步骤：

1、选择开启，先保存，再应用，页面会显示 SN 码和服务设备状态

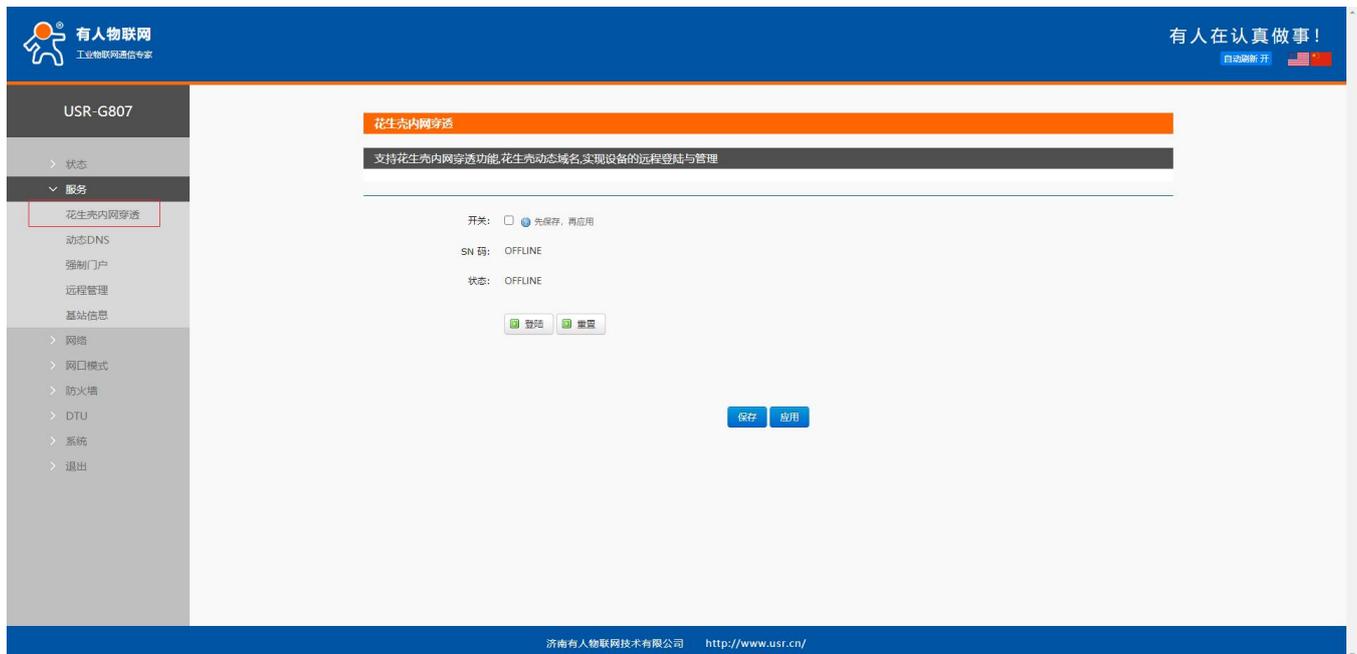


图 90 花生壳内网穿透启动前

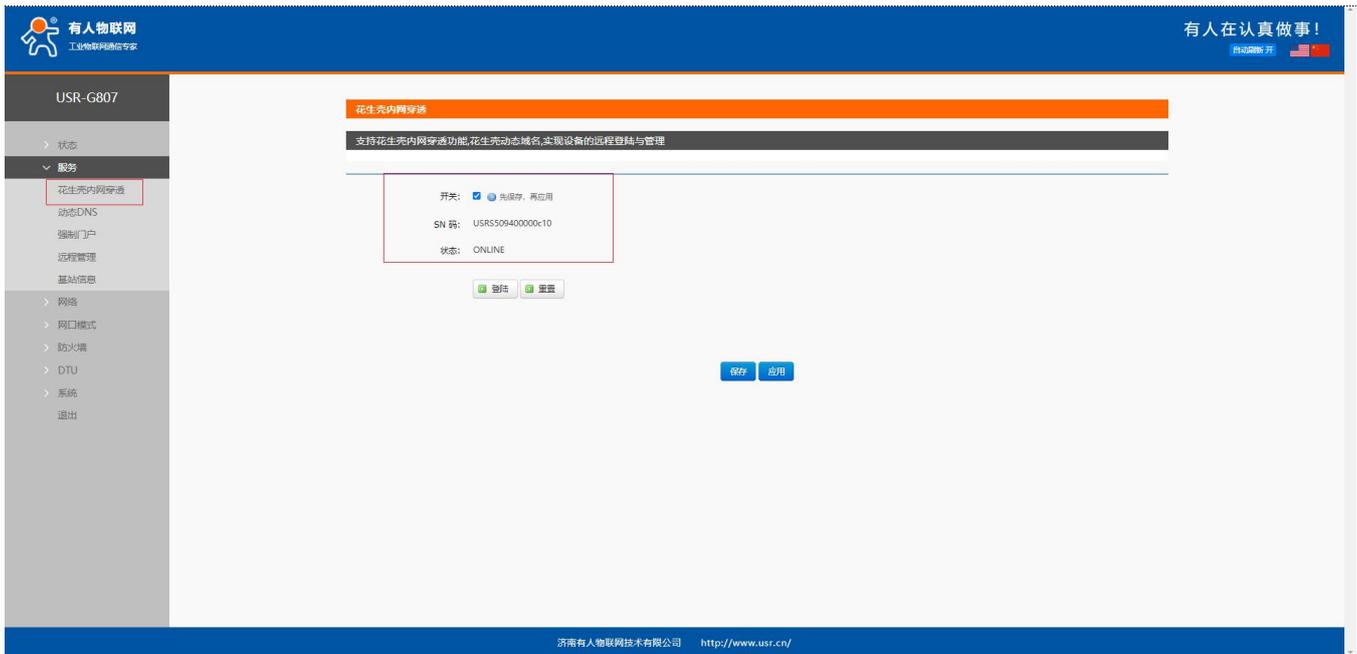


图 91 花生壳内网穿透启动后

2、点击“登录管理”，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，选择 SN 码登录。

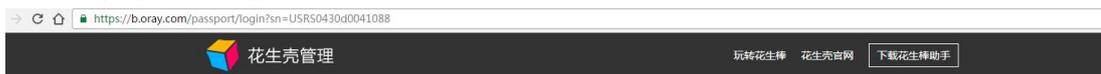


图 92 花生壳内网穿透 SN 码登陆

3、初次登录需要设置以后账号的密码，和验证手机号。

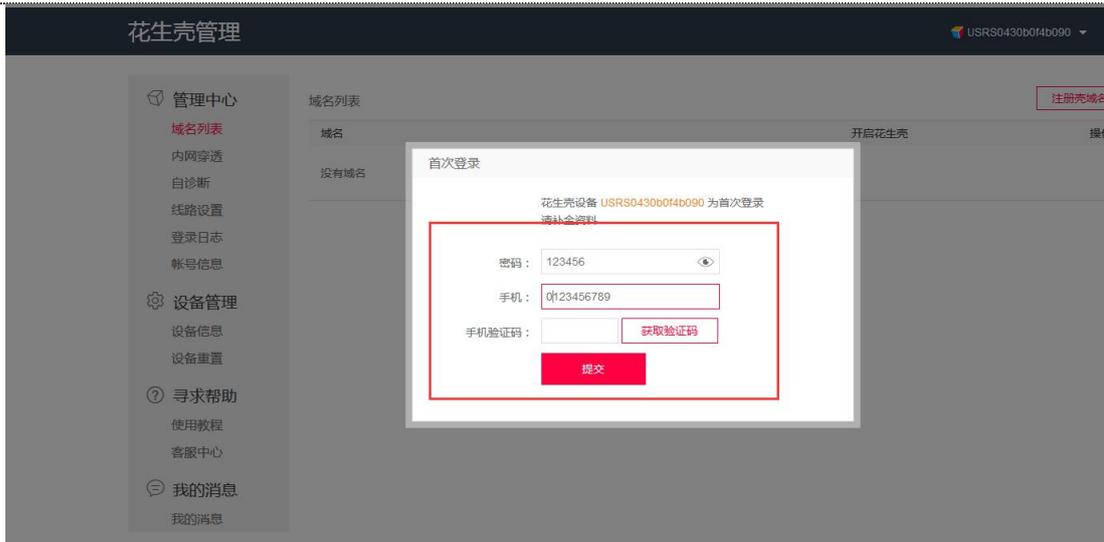


图 93 花生壳内网穿透手机验证

4、登录成功后需要切换账号，关联到花生壳的账号登录，点击图中上方的 SN 码选择切换账号



图 94 花生壳内网穿透切换账号

5、选择账号登录

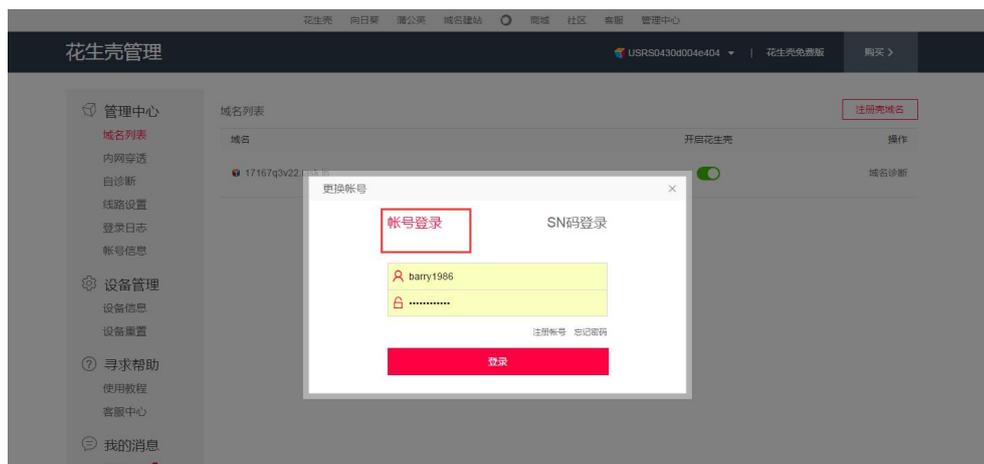


图 95 花生壳内网穿透账号登陆

6、切换到账号登录点击左侧的内网穿透



图 96 花生壳内网穿透设置

7、点击添加映射



图 97 花生壳内网穿透设置

8、设置映射

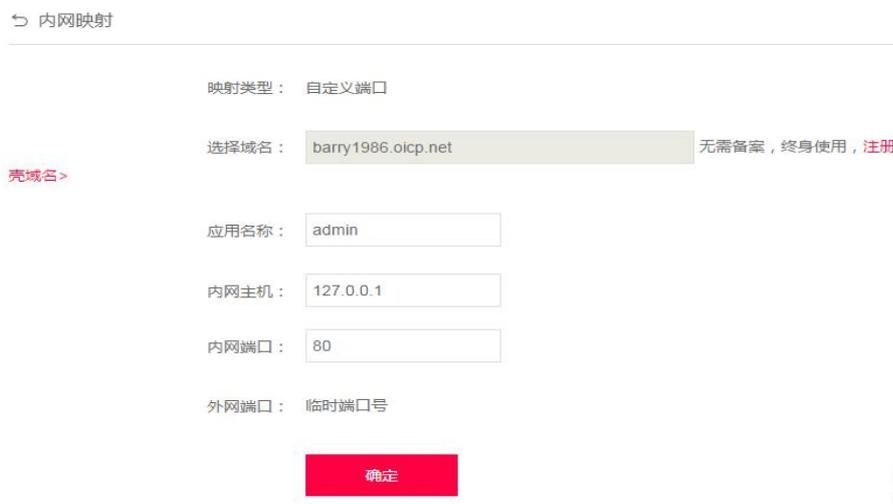


图 98 花生壳内网穿透设置

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，如果是本机填写 127.0.0.1，内网端口填写内网设备中的网络端口，本机填写 80，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 13 端口映射参数表

功能	参数设置（如果要使用）	备注
映射端口类型	选择自定义端口	选择自定义端口
限制域名	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临时端口

9、测试域名



直接在浏览器输入该域名即可访问路由器。

图 99 花生壳内网穿透域名测试

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。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

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（在“服务”下拉框中查看，选择对应的 DDNS 服务商，这里使用花生壳 ddns.oray.com），设置方法如下：

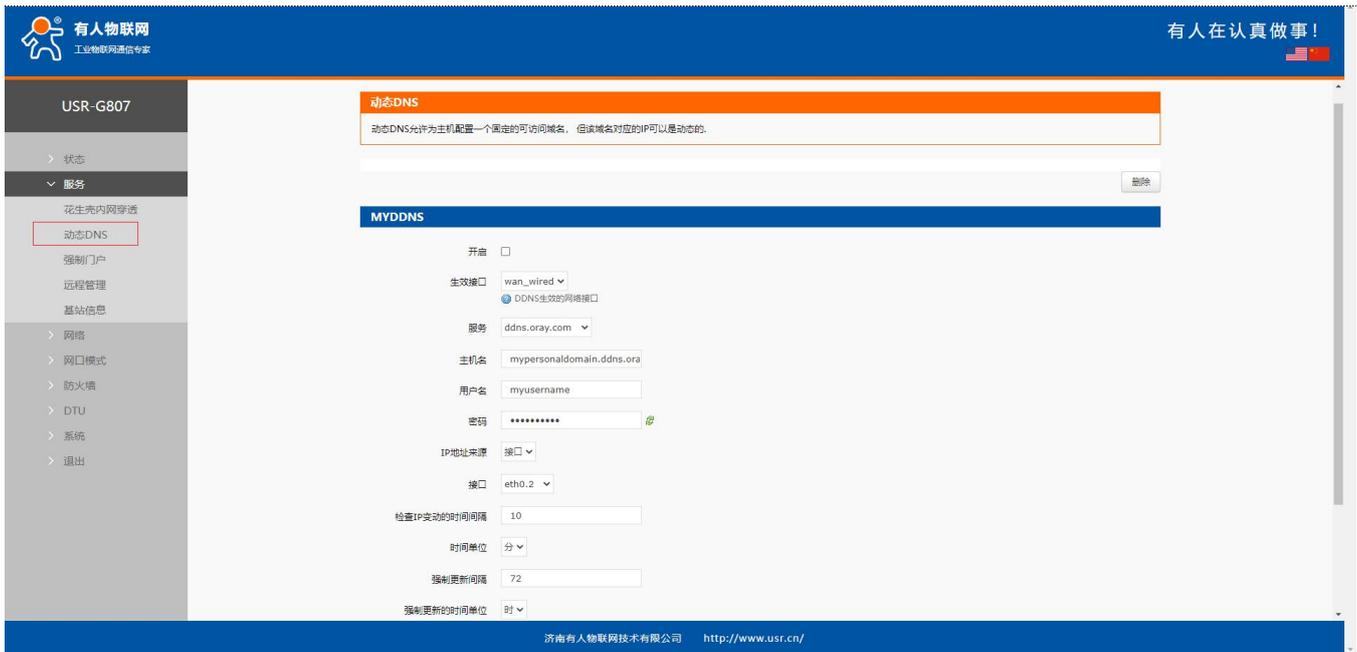


图 100 DDNS 设置页面

参数填写要求如下：

表 14 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：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 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：

```
C:\Users\Administrator>ping 1a516r1619.iask.in

正在 Ping 1a516r1619.iask.in [123.101.125.124] 具有 32 字节的数据:
来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254
来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254
来自 123.101.125.124 的回复: 字节=32 时间<1ms TTL=254
来自 123.101.125.124 的回复: 字节=32 时间=1ms TTL=254

123.101.125.124 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

图 101 DDNS 测试图

6.2.2. 自定义的服务

第二种情况,路由器自身不支持的 DDNS 服务(需要在“服务”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:

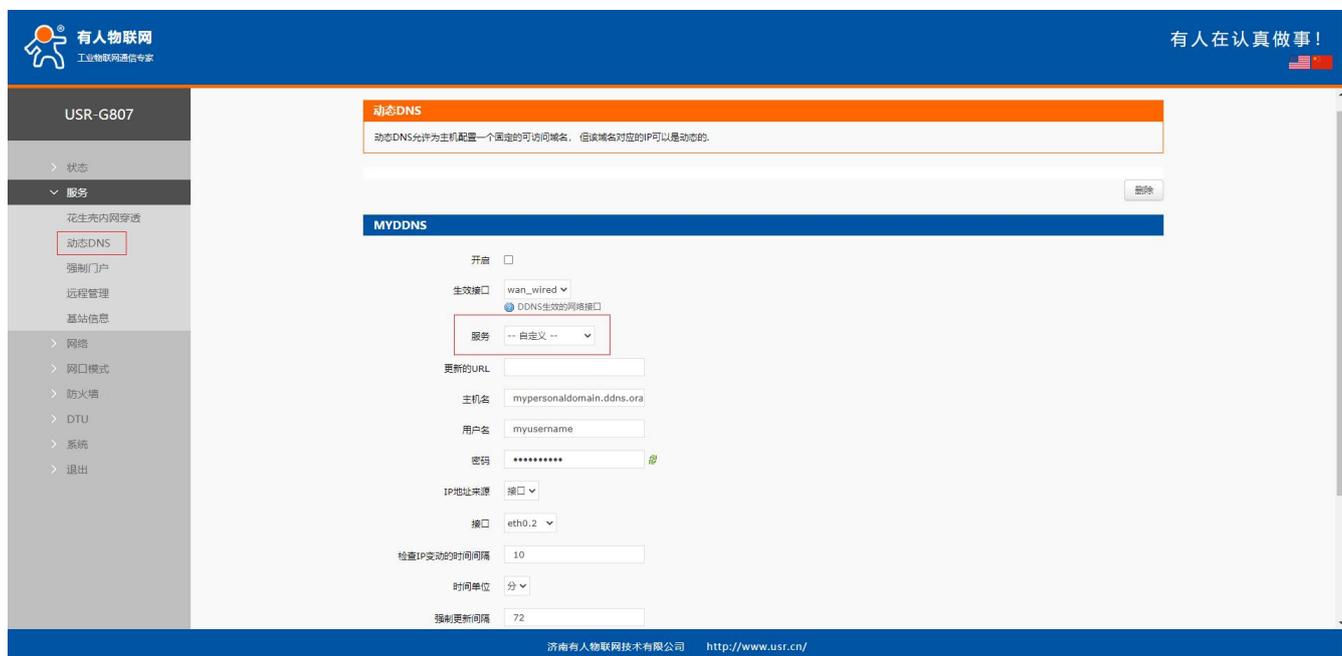


图 102 DDNS 自定义服务参数设置页面

- 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),我申请的动态域名为 1a516r1619.iask.in,用户名 ouclihuibin123,密码 ouclihuibin1231。

表 15 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: oulihuibin123
密码	花生壳密码	举例: oulihuibin1231
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 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 103 DDNS 测试图二

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



图 104 DDNS 测试图三

6.2.3. 功能特点

- 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；
- 即便做为子网下的路由器，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；
- 可以为本路由器添加多个 DDNS 域名。

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：

设备注册界面，将远程平台注册码填入 mac 输入框中，其它选根据需要进行选择，然后点击添加。

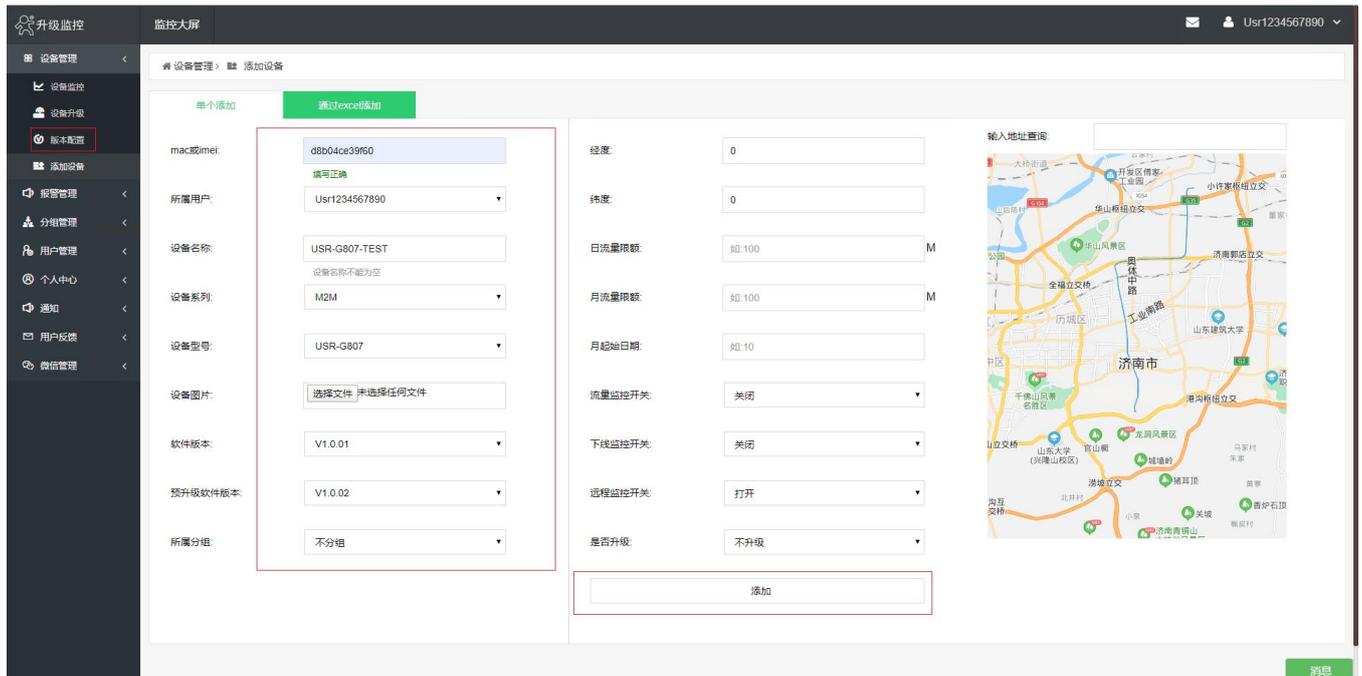


图 105 设备注册

远程监控界面，会显示当前在线的设备，点设备对应的 mac_imEI 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(目前支持路由器相关的 AT)。

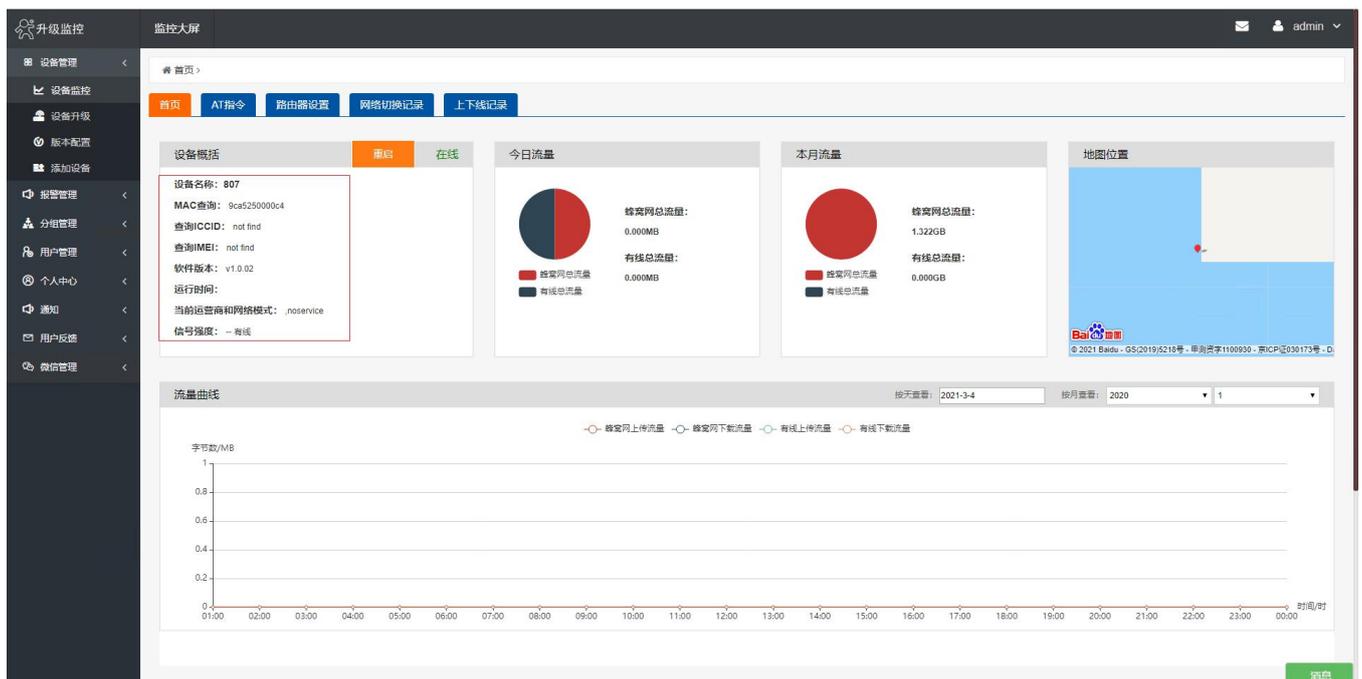


图 106 设备监控一

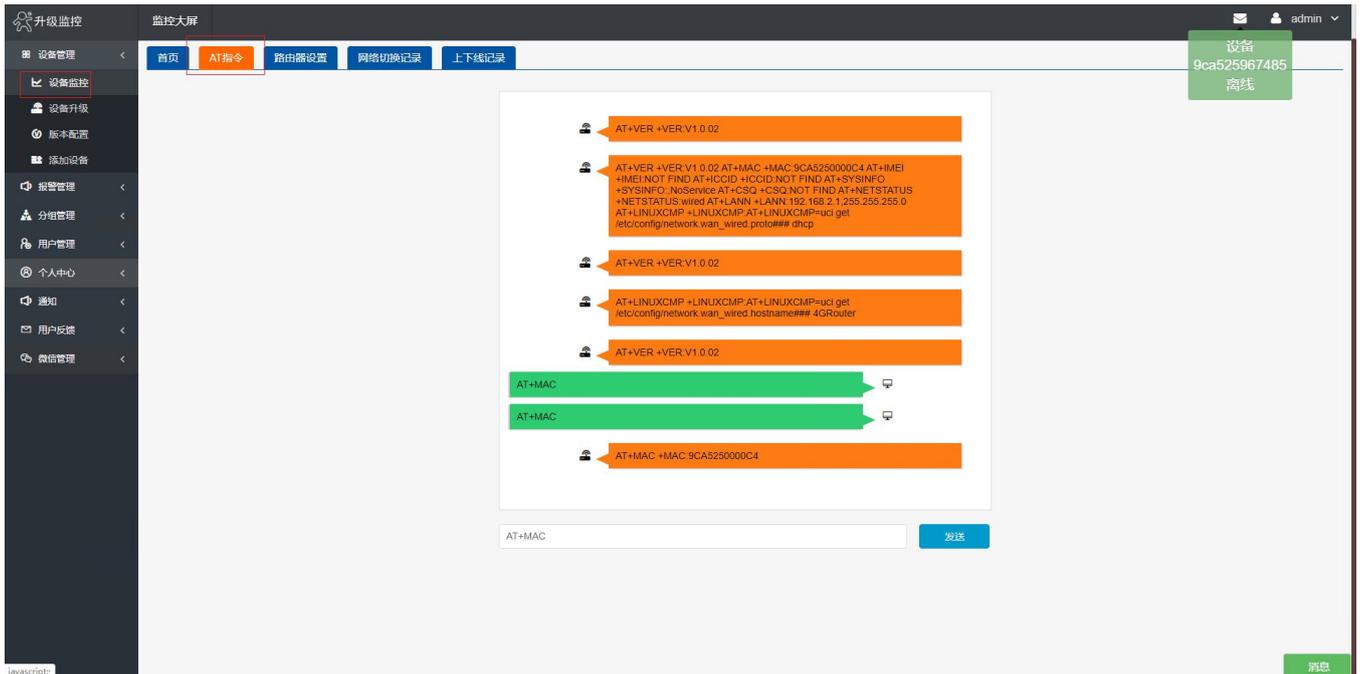


图 107 设备监控二

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。

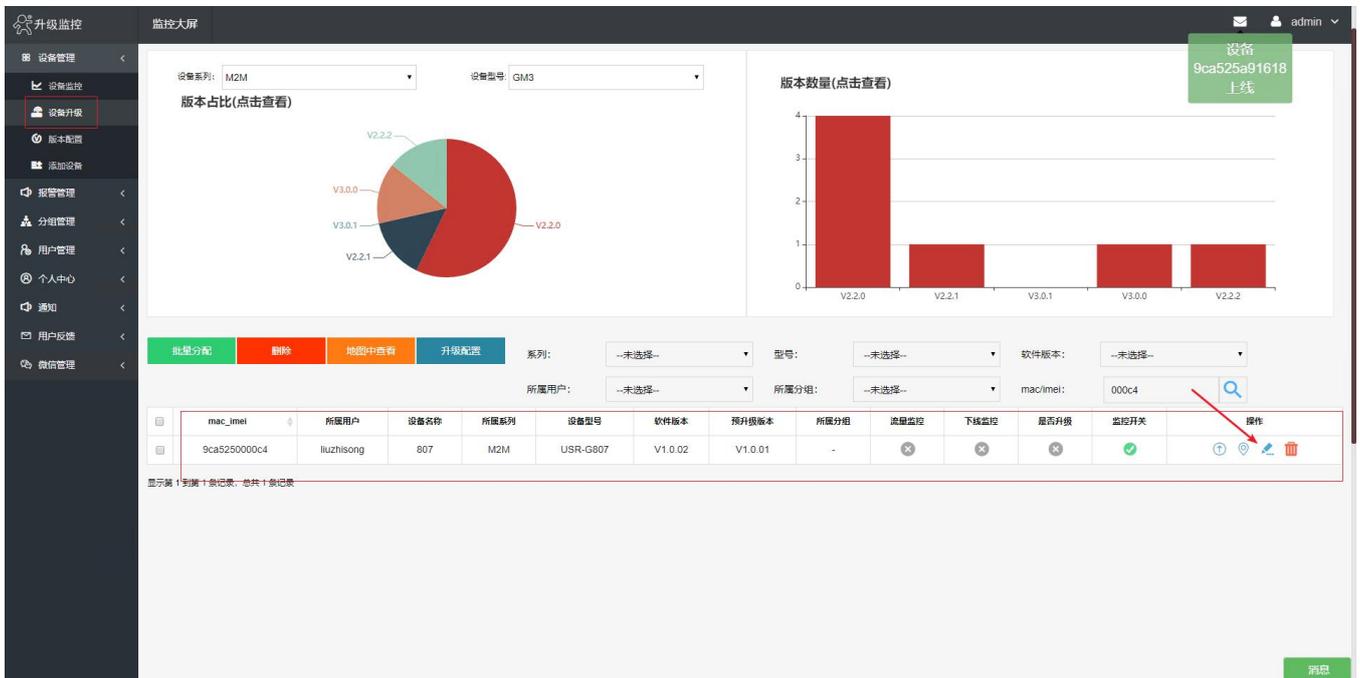


图 108 设备升级一

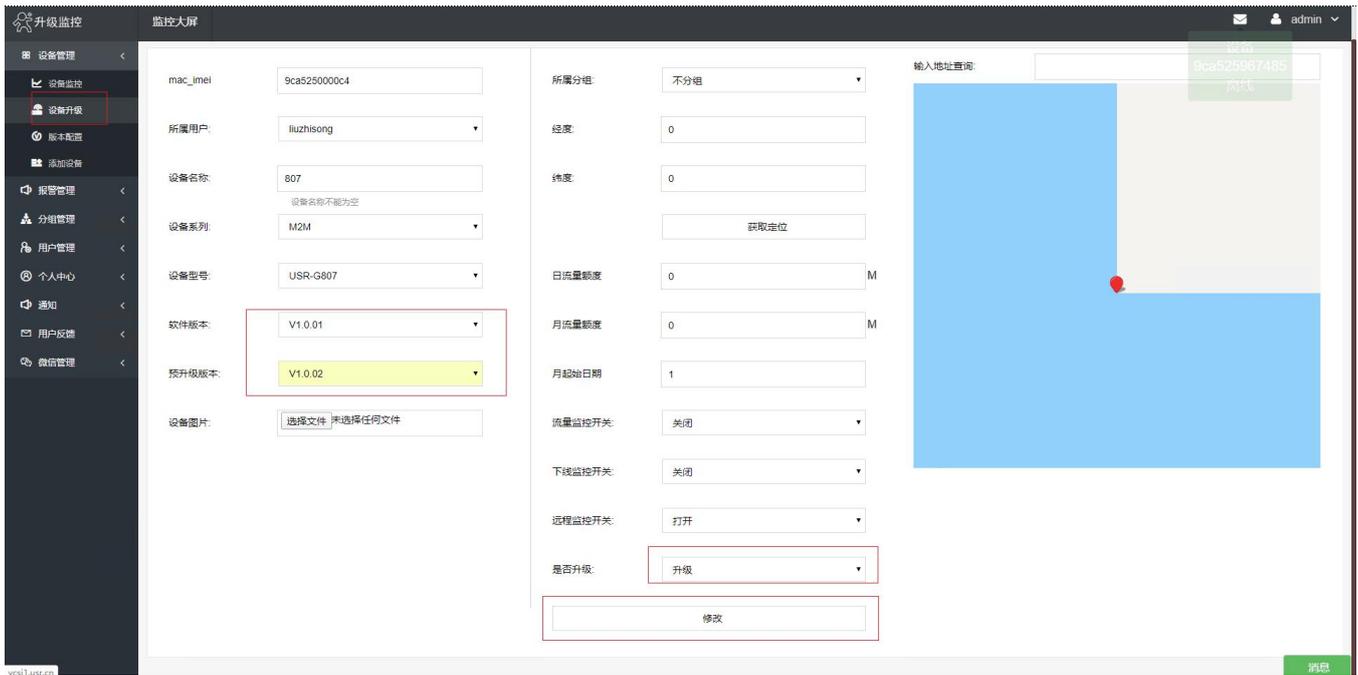


图 109 设备升级二

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时间，默认为 1800 秒，远程升级功能默认打开。

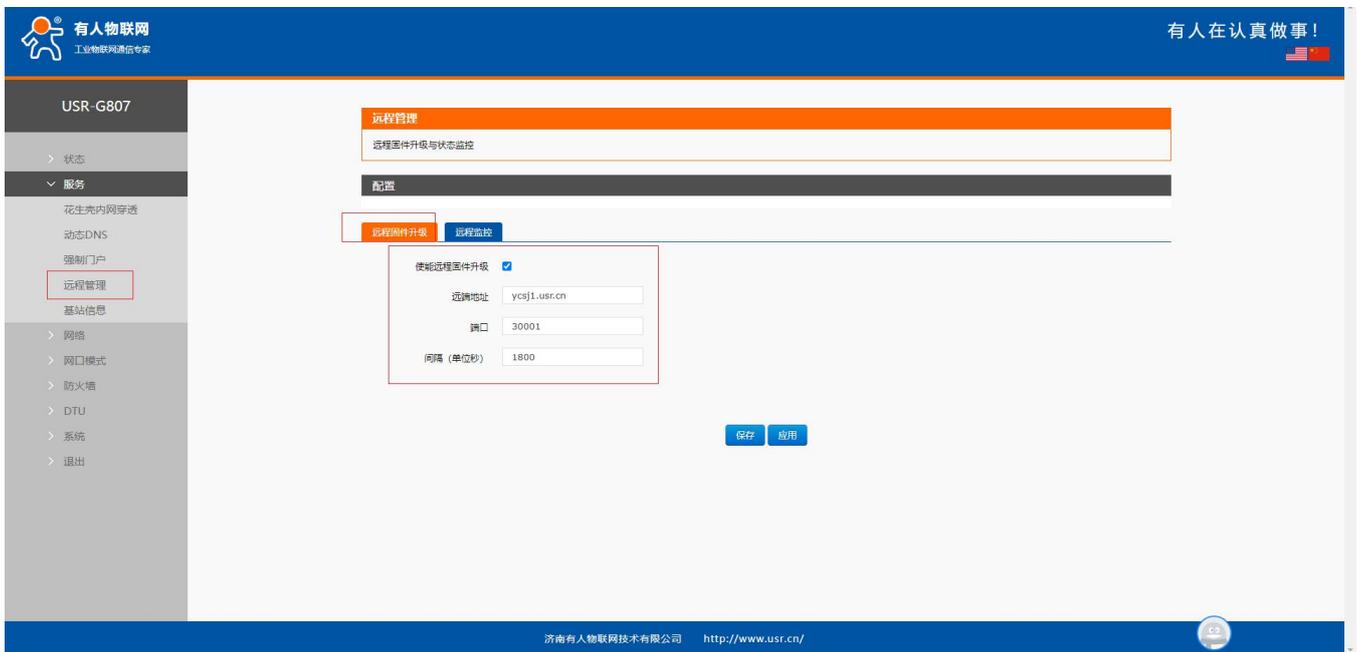


图 110 远程升级

表 16 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

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、WAN 口 IP）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：

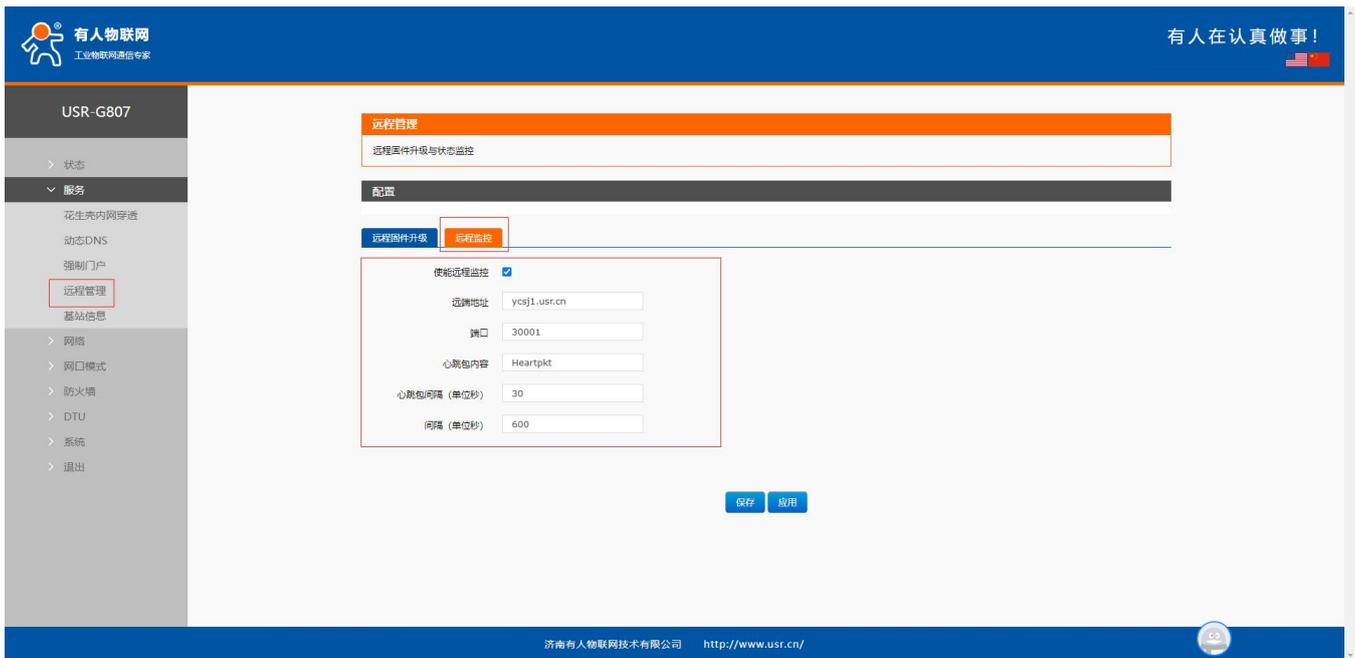


图 111 远程监控

表 17 远程监控参数表

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
心跳包内容	设备向远程监控服务器发送心跳包的内容	默认 heartpkt
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

7. DTU 功能

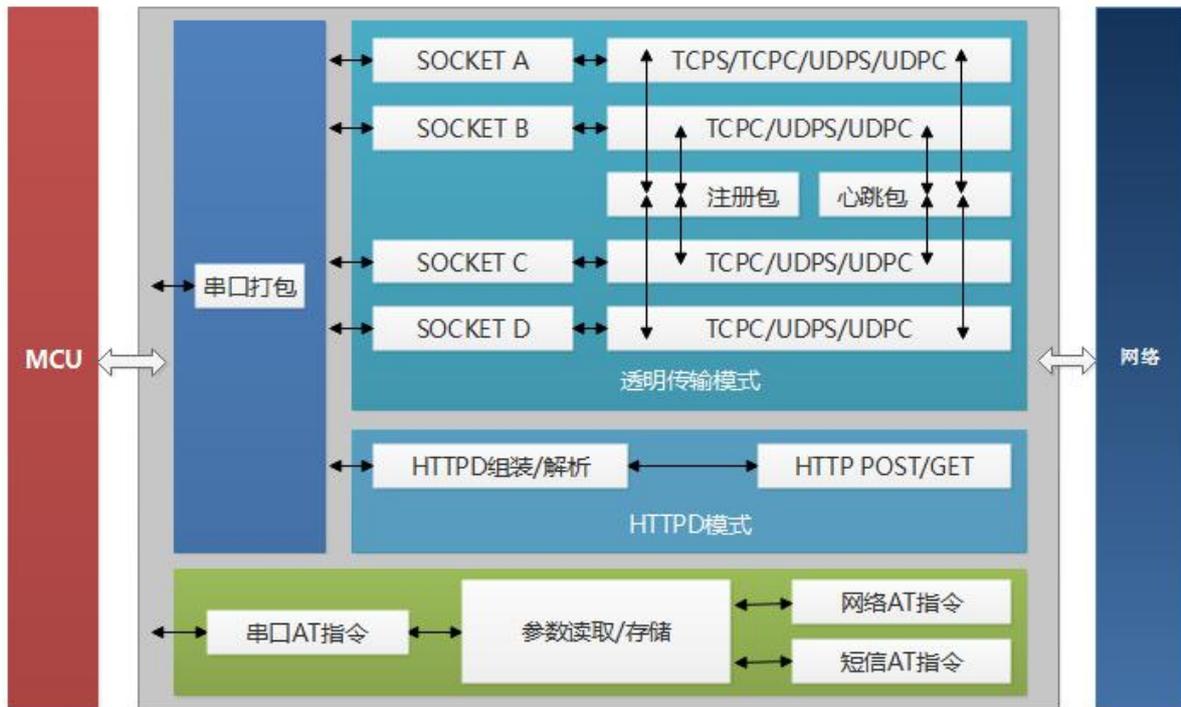


图 112 DTU 功能框图

7.1. 工作模式

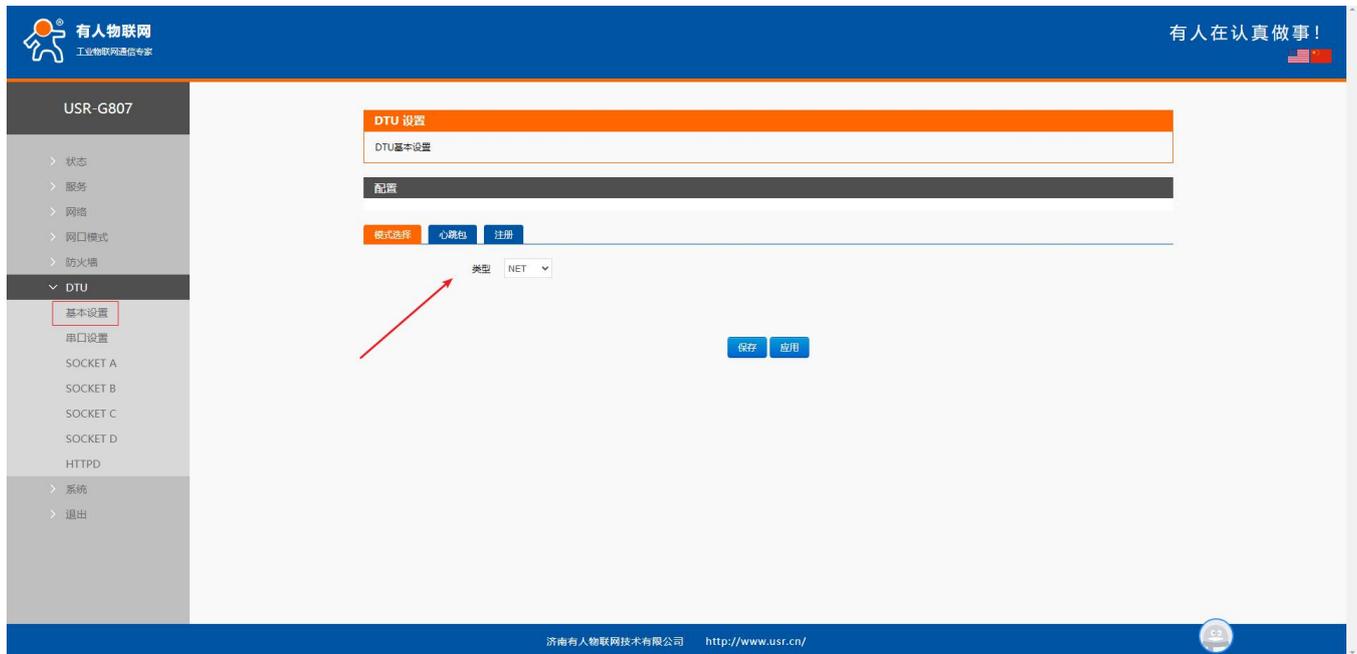


图 113 模式选择

7.1.1. 网络透传模式

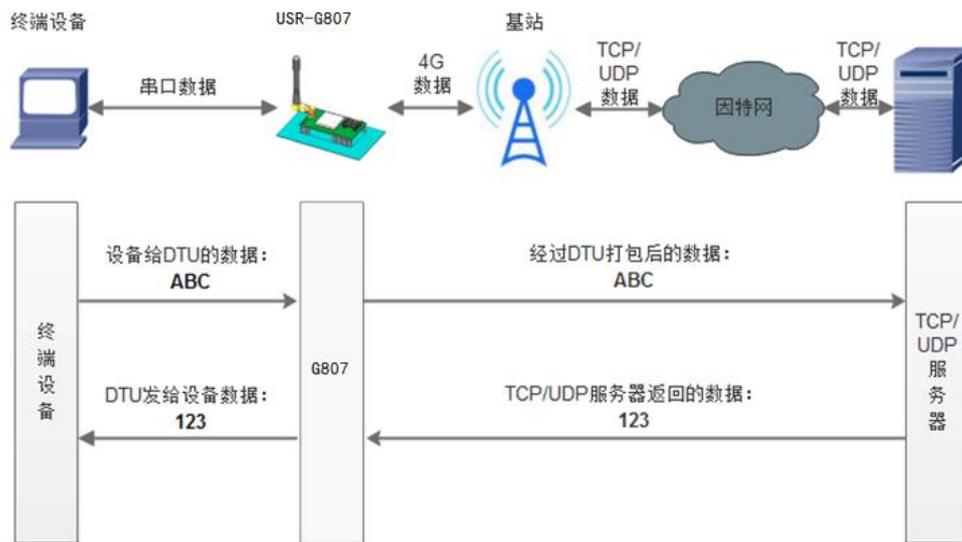


图 114 网络透传模式

<说明>

- 在此模式下，用户的串口设备，可以通过 USR-G807 发送数据到网络上指定的服务器。USR-G807 也可以接受来自服务器的数据，并将信息转发至串口设备；
- 用户不需要关注串口数据与网络数据包之间的数据转换过程，只需通过简单的参数设置，即可实现串口设备与网络服务器之间的数据透明通信；
- 本设备支持四路 SOCKET 连接，分别为 SOCKET A，SOCKET B，SOCKET C 和 SOCKET D，它们是相互独立的；
- SOCKET A 支持 TCP Server、TCP Client、UDP Server、UDP Client 四种模式；
- SOCKET B、SOCKET C 和 SOCKET D 支持 TCP Client、UDP Server、UDP Client 三种模式。

AT 指令设置方法：

1. 设置工作模式为网络透传：

AT+WKMOD=NET

2. 设置 socket A 为使能状态：

AT+SOCKAEN=ON

3. 设置 socket A 为 TCP Client：

AT+SOCKA=TCPC,test.cn,2317

4. 重启：

AT+Z

设置软件示意图：

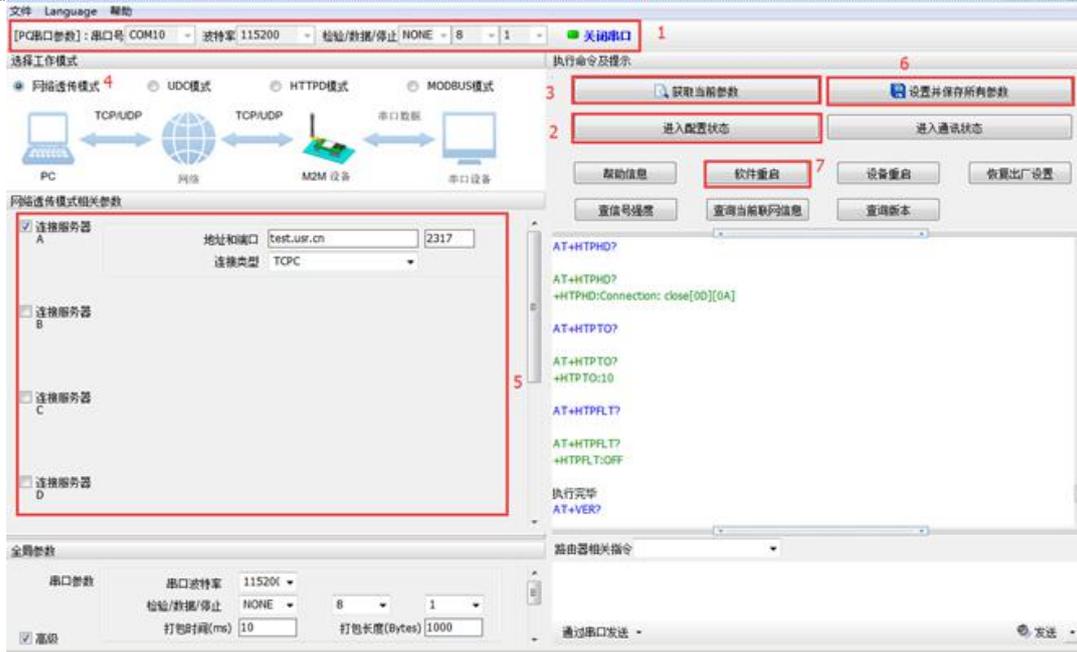


图 115 设置软件示意图

- 1、打开专用设置软件“USR-G807”。根据实际情况设置串口参数并点击“打开串口”。
- 2、点击“进入配置状态”，等待设备进入 AT 指令配置模式。
- 3、点击“获取当前参数”，等待获取所有当前参数完毕。
- 4、在“选择工作模式”一栏中，选中“网络透传模式”。
- 5、设置“地址和端口”为 test.cn 和 2317。
- 6、点击“设置并保存所有参数”。
- 7、保存完毕后，点击“软件重启”按钮。

7.1.2. HTTPD 模式

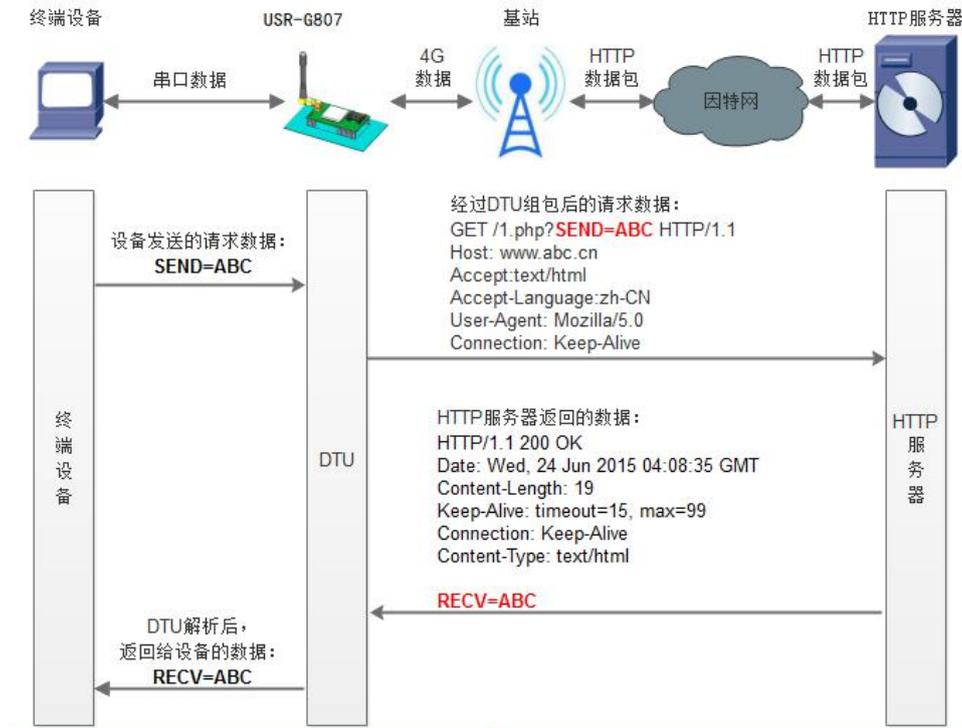


图 116 HTTPD 模式

<说明>

- 在此模式下，用户的终端设备，可以通过本设备发送请求数据到指定的 HTTP 服务器，然后设备接收来自 HTTP 服务器的数据，对数据进行解析并将结果发至串口设备。
- 用户不需要关注串口数据与网络数据包之间的数据转换过程，只需通过简单的参数设置，即可实现串口设备向 HTTP 服务器的数据请求。
- 设备默认会过滤接收到的数据，只将用户数据部分输出到串口，客户可以使用 AT 指令选择是否过滤 HTTPD 数据。

AT 指令设置方法：

1. 设置工作模式为 HTTPD:
AT+WKMOD=HTTPD
2. 设置 HTTP 的请求方式:
AT+HTPTP=GET
3. 设置 HTTP 的请求 URL:
AT+HTPURL=/1.php[3F]
4. 设置 HTTP 的请求服务器:
AT+HTPSV=test.cn,80
5. 设置 HTTP 的请求头信息:
AT+HTPHD=Connection: close[0D][0A]
6. 设置 HTTP 的请求超时时间:
AT+HTPTO=10
7. 设置是否过滤回复信息包头:
AT+HTPFLT=ON
8. 重启:

AT+Z

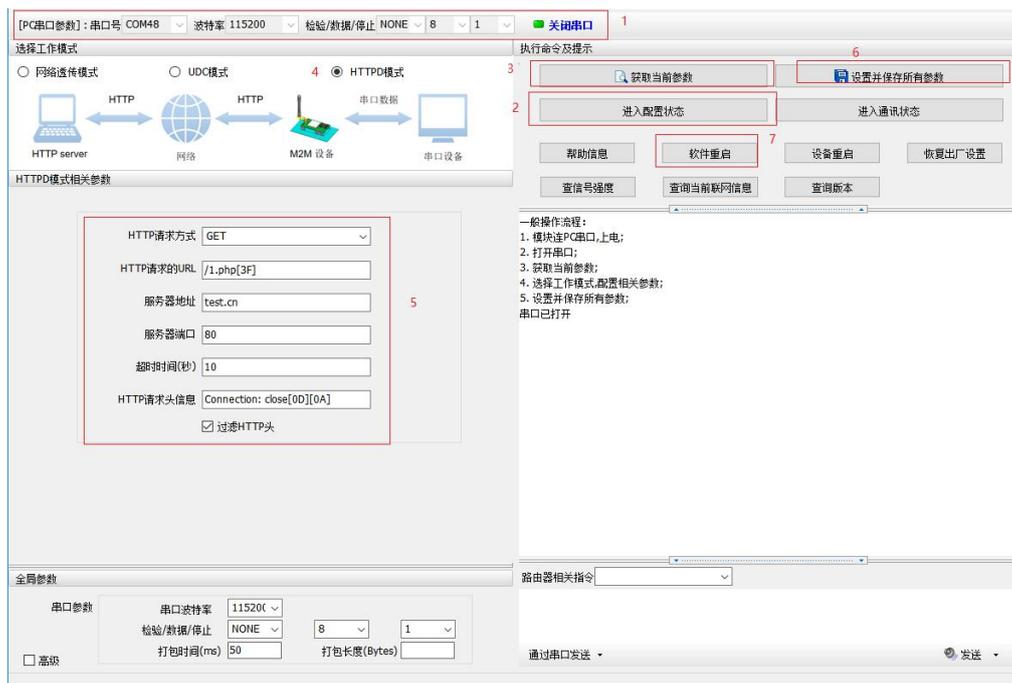
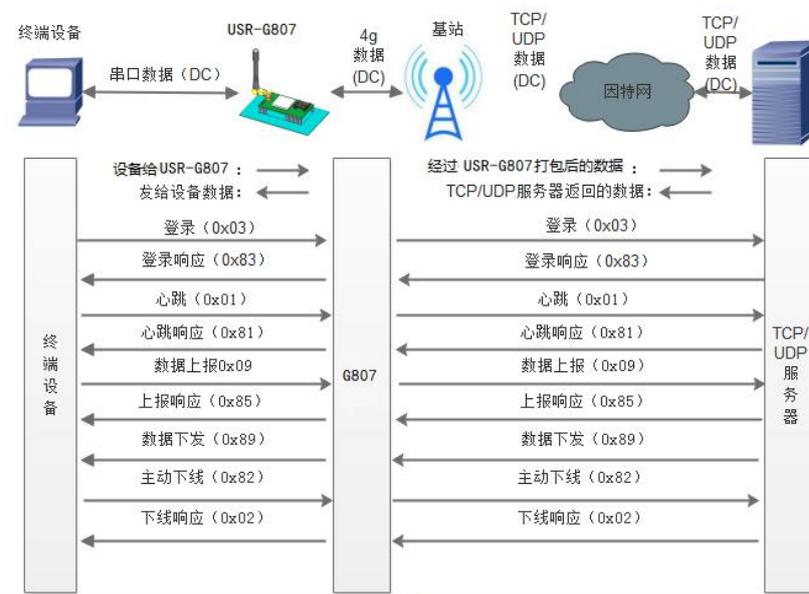


图 117 设置软件示意图

1. 打开专用设置软件“USR-G807”。根据实际情况设置串口参数并点击“打开串口”。
2. 点击“获取当前参数”，等待获取所有当前参数完毕。
3. 点击“进入配置状态”，等待设备进入 AT 指令配置模式。
4. 在“选择工作模式”一栏中，选中“HTTPD 模式”。
5. 设置“HTTP 请求方式”为 GET。设置“HTTP 请求的 URL”为“/1.php[3F]”。设置“服务器地址”为“test.cn”。设置“服务器端口”为 80，设置“超时时间”为 10 秒。设置“HTTP 请求头信息”为“Connection: close[0D][0A]”，选中“过滤 HTTP 头信息”。
6. 点击“设置并保存所有参数”。
7. 保存完毕后，保存完毕后，点击“软件重启”按钮。

7.1.3. 协议(UDC)透传模式



此模式在网络透传模式上增加特定的注册包和心跳包，并且对数据进行组包。这种模式更方便用户使用和二次开发，用户可以理解成加入 UDC 协议的网络透传模式。此模式下，我们提供了服务器端二次开发包，用户在将链接库加入到自己的工程后，就可以通过调用我们提供的接口，快速开发自己的服务端，好处在于设备的上线情况和数据传输既能被用户所掌握，也可以由用户来控制，既方便了用户开发，也提高了服务器端的统一性，稳定性和可靠性。

设置软件示意图：

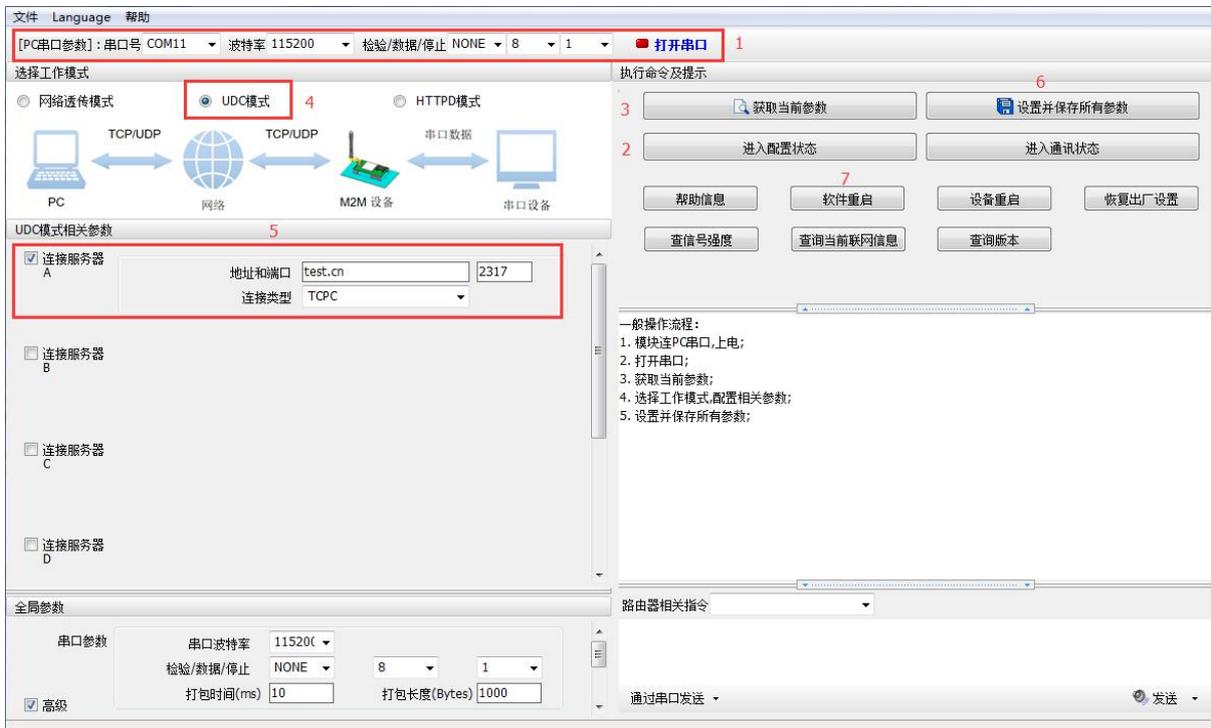


图 118 设置软件示意图

协议透传对比网络透传模式有什么不同？

- 设备端设置更加简单，协议透传模式下你不需要关注心跳包怎么写，注册包怎么设置，只需要按照要求设置服务器地址，端口号，TCP/UDP 和设备 ID 即可(注意：设备 ID 的长度为 11 位，不全会自动补零)：



➤ 重头戏还是服务器端的简化，首先我们看下我们提供的服务器演示程序，当设备上线时会是这样：



➤ 我们通过终端登录号码也就是设置软件上输入的 **UDC ID** 来区分不同的设备，可以拿到这个设备详细的信息，同时还可通过这种方式向设备发送数据：



➤ 还可以对设备进行管理操作：



- 通常服务器程序开发时需要针对开发语言掌握 Socket 的创建方法、线程管理、数据解析等等，开发程序的工程师不一定对设备的工作机制了解，所以开发过程中对注册包心跳包理解不到位，使得发挥不出应有的效果，导致整个项目运行不稳定。
- 针对这种情况我们提供了服务器端二次开发包给客户使用，可以利用开发包并参考我们提供的 demo 就可以十分便捷的开发出稳定的服务器程序。
- 开发包是 windows 下的动态链接库文件，封装了与我们 DTU 设备通讯所需要的全部 API 接口，包括服务的启动，数据发送，数据接收和关闭服务等。

指令设置：

- (1) 设置工作模式为网络透传模式
AT+WKMOD=UDC
- (2) 使能 socket A
AT+SOCKAEN=ON
- (3) 设置 socket A 为 TCP 客户端，服务器地址为 test.usr.cn，服务器端口号为 2317。
AT+SOCKA=TCPC,test.cn,2317
- (4) 使能心跳包
AT+HEARTEN=ON
- (5) 设置心跳包发送间隔
AT+HEARTTM=30
- (6) 使能注册包

	ODD (奇校验)
	MARK
485	NFC: 无硬件流控 485:485 通信
打包时间	10, 50, 可自定义打包时长
打包长度	1000, 可自定义打包长度

注：流控一项暂时不支持

7.2.2. 成帧机制

7.2.2.1. 时间触发模式

USR-G807 在接收来自 UART 的数据时，会不断的检查相邻 2 个字节的间隔时间。如果间隔时间大于等于某一“时间阈值”，则认为一帧结束，否则一直接收数据直到大于等于打包长度（默认是 1000）字节。将这一帧数据作为一个 TCP 或 UDP 包发向网络端。这里的“时间阈值”即为打包间隔时间。可设置的范围是 10ms~60000ms。出厂默认 10ms。

这个参数可以根据 AT 命令来设置，AT+UARTFT=10。

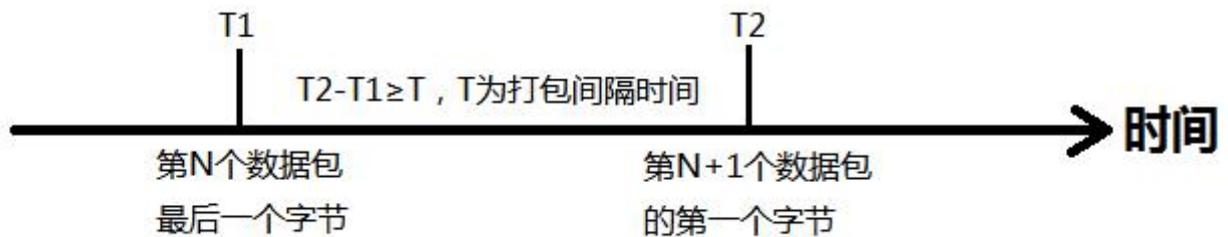


图 120 时间触发模式

7.2.2.2. 长度触发模式

USR-G807 在接收来自 UART 的数据时，会不断的检查已接收到的字节数。如果已接收到的字节数达到某一“长度阈值”，则认为一帧结束。将这一帧数据作为一个 TCP 或 UDP 包发向网络端。这里的“长度阈值”即为打包长度。可设置的范围是 1~4096。出厂默认 1000。

这个参数可以根据 AT 命令来设置，AT+UARTFL=<length>。

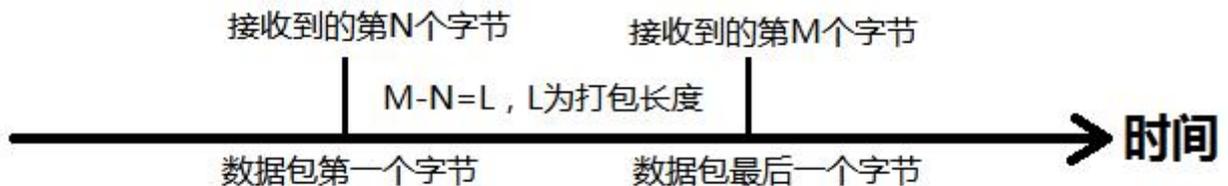


图 121 长度触发模式

7.3. 特色功能

7.3.1. 注册包功能

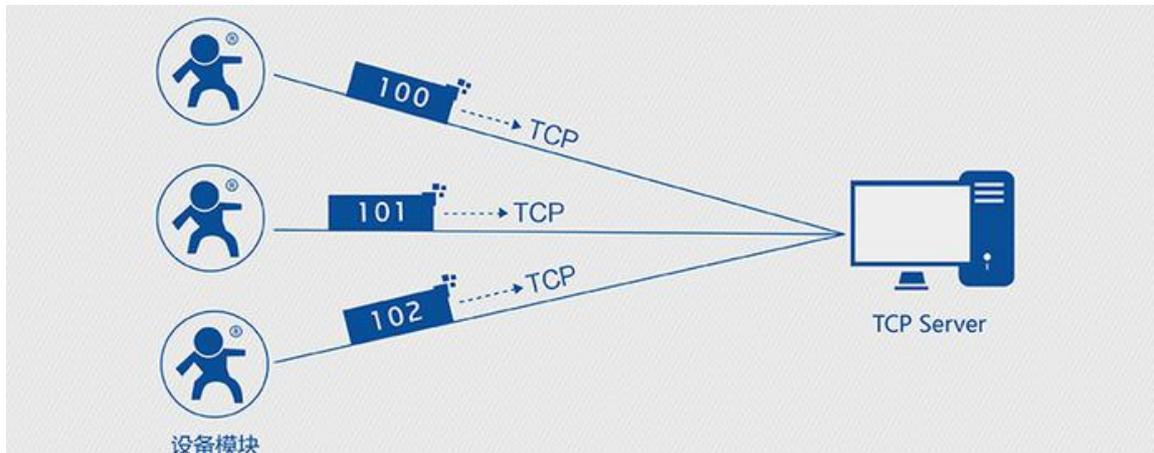


图 122 注册包功能示意图

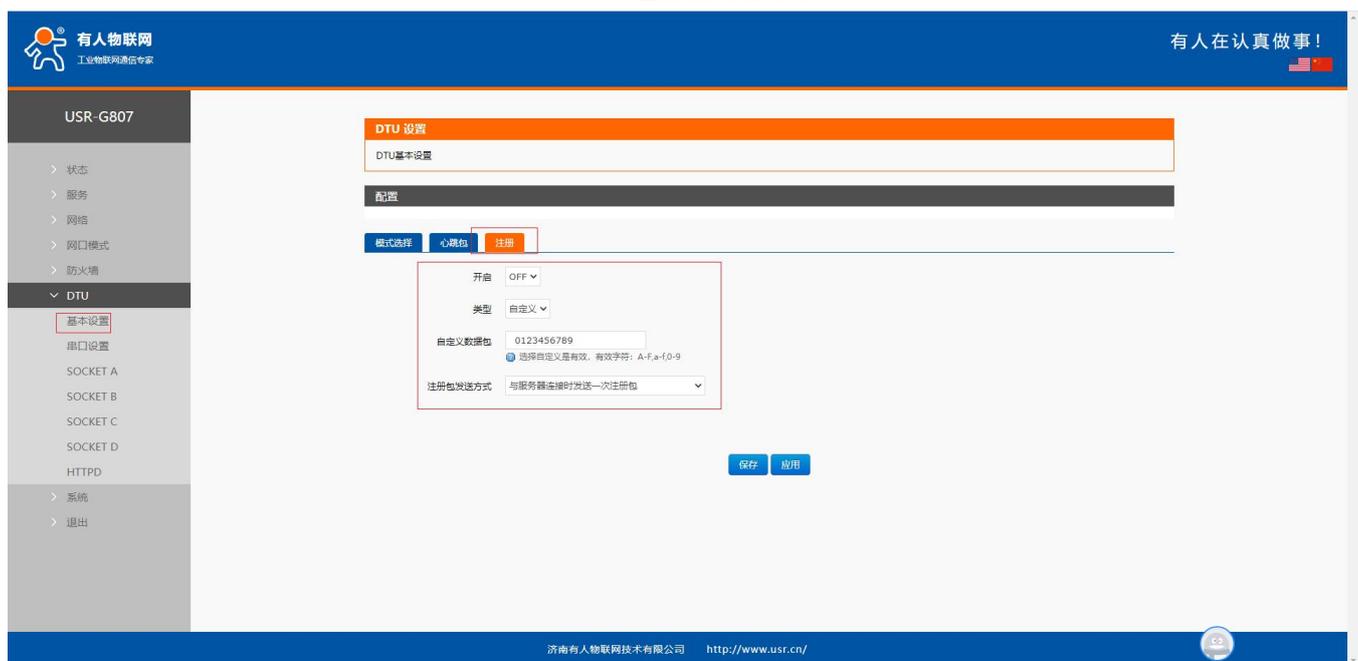


图 123 注册包设置

在网络透传模式下，用户可以选择让设备向服务器发送注册包。注册包是为了让服务器能够识别数据来源设备，或作为获取服务器功能授权的密码。注册包可以在设备与服务器建立连接时发送，也可以在每个数据包的最前端拼接注册包数据，作为一个数据包。注册包的数据可以是 ICCID 码，IMEI 码，或自定义注册数据。

- ICCID，SIM 的唯一识别码，适用于基于 SIM 卡识别的应用。
- IMEI，DTU 设备内上网 DTU 唯一识别码，适用于基于设备识别的应用，与其内安装的 SIM 卡无关。
- CLOUD，基于有人透传云应用的识别码，通过设置的已获取权限的相关参数，即可轻松使用有人透传云服务。
- USER，用户自定义数据，可应用于用户自定义的注册数据。

表 19 参考 AT 指令集

指令名称	指令功能	默认参数
------	------	------

AT+ REGEN	查询/设置是否使能注册包	OFF
AT+ REGTP	查询/设置注册包内容类型	USER
AT+ REGDT	查询/设置自定义注册信息	0123456789
AT+ REGSND	查询/设置注册包发送方式	DATA

AT 指令设置方法：

1. 开启注册包功能：
AT+ REGEN=ON
2. 设置注册包内容类型为自定义：
AT+ REGTP=USER
3. 设置自定义注册包数据：
AT+REGDT=123456789
4. 设置注册包发送方式为将注册数据作为每包数据的头：
AT+ REGSND=DATA
5. 重启：

AT+ Z

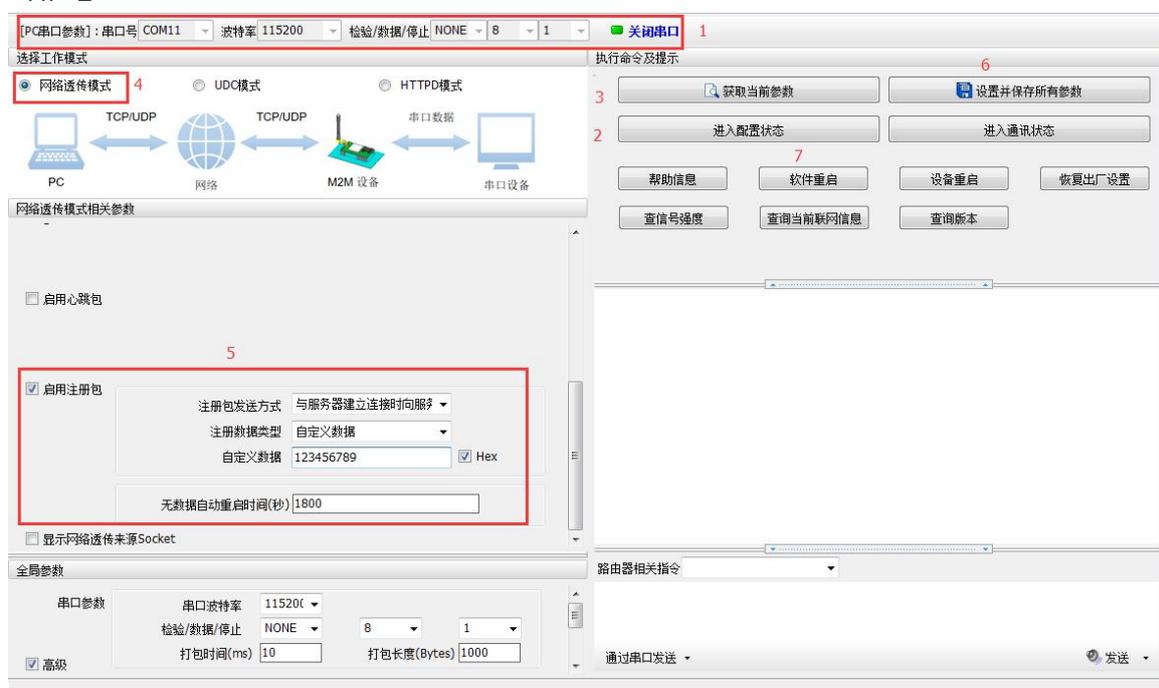


图 124 设置软件示意图

1. 打开专用设置软件“USR-G807”。根据实际情况设置串口参数并点击“打开串口”。
2. 点击“获取当前参数”，等待获取所有当前参数完毕。
3. 点击“进入配置状态”，等待设备进入 AT 指令配置模式。
4. 在“选择工作模式”一栏中，选中“网络透传模式”并设置 socket 的参数。
5. 开启注册包功能，并设置各项参数。
6. 点击“设置并保存所有参数”。
7. 保存完毕后，点击“软件重启”按钮。

7.3.2. 心跳包机制

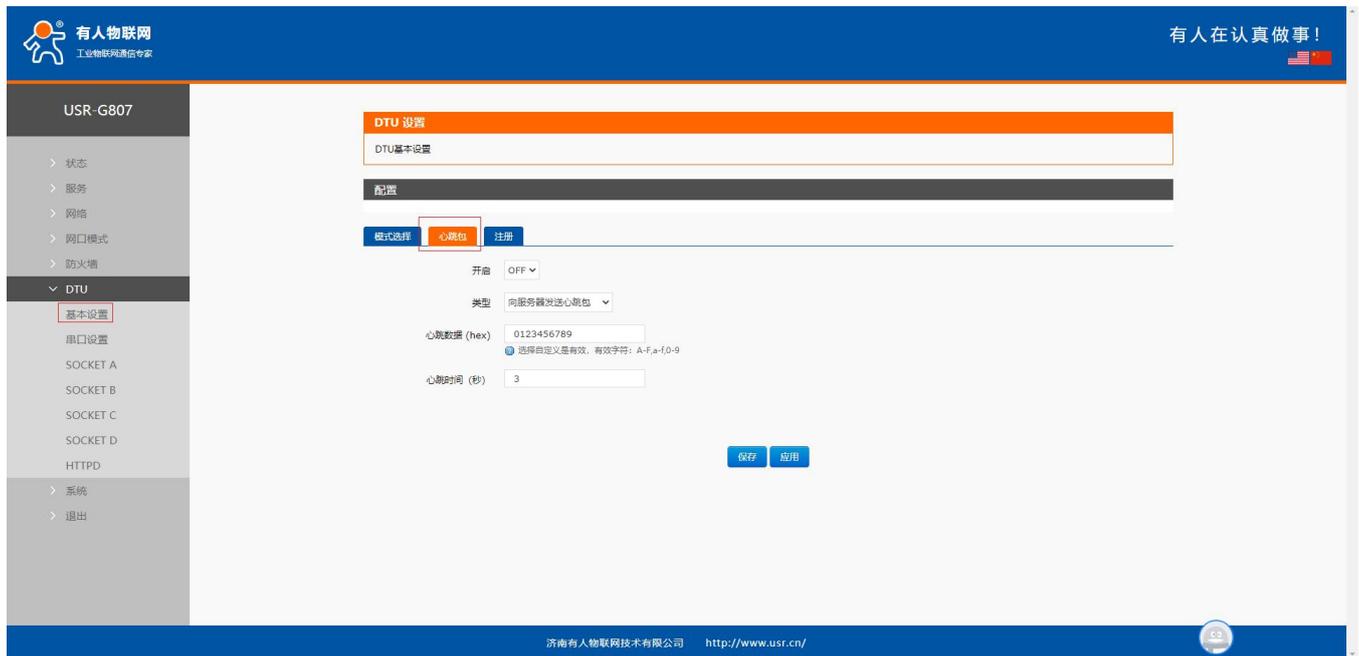


图 125 心跳包设置

在网络透传模式下，用户可以选择让 DTU 发送心跳包。心跳包可以向网络服务器端发送，也可以向串口设备端发送。向网络端发送主要目的是为了与服务器保持连接，和让长时间空闲（很长时间内不会向服务器发送数据）的 DTU 保持与服务器的连接。

在服务器向设备发送固定查询指令的应用中，为了减少通信流量，用户可以选择，用向串口设备端发送心跳包（查询指令），来代替从服务器发送查询指令。

表 20 参考 AT 指令集

指令名称	指令功能	默认参数
AT+ HEARTEN	查询/设置是否使能心跳包	OFF
AT+ HEARTDT	查询/设置心跳包数据	0123456789
AT+ HEARSND	查询/设置心跳包的发送方式	NET
AT+ HEARTTM	查询/设置心跳包发送间隔	30

AT 指令设置方法：

1. 开启心跳包功能：

AT+ HEARTEN=ON

2. 设置心跳包数据：

AT+ HEARTDT=123456789

3. 设置心跳包发送方式为发向网络端：

AT+ HEARTTP=NET

4. 设置心跳包的发送间隔时间：

AT+ HEARTTM=30

5. 重启：

AT+ Z

设置软件示意图：

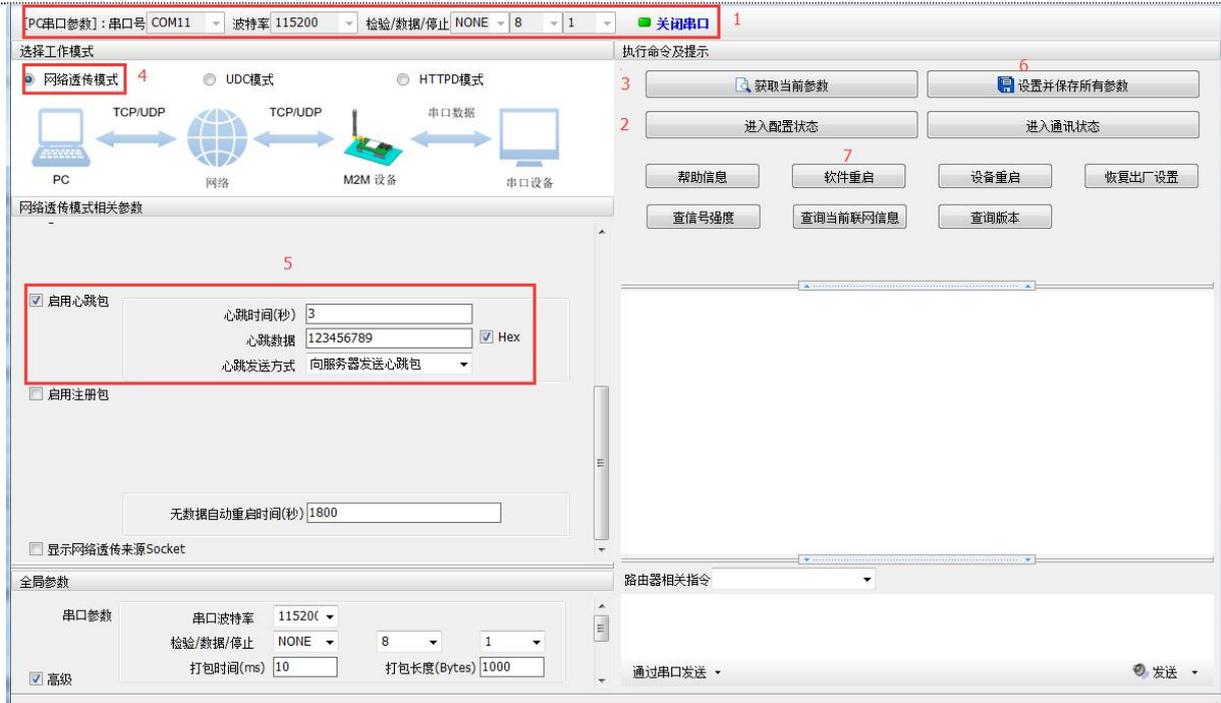


图 126 设置软件示意图

1. 打开专用设置软件“USR-G807”。根据实际情况设置串口参数并点击“打开串口”。
2. 点击“获取当前参数”，等待获取所有当前参数完毕。
3. 点击“进入配置状态”，等待设备进入 AT 指令配置模式。
4. 在“选择工作模式”一栏中，选中“网络透传模式”，并设置 socket 的参数。
5. 开启心跳包功能，并设置各项参数。
6. 点击“设置并保存所有参数”。
7. 保存完毕后，点击“软件重启”按钮。

7.3.3. 透传云功能



图 127 透传云功能示意图

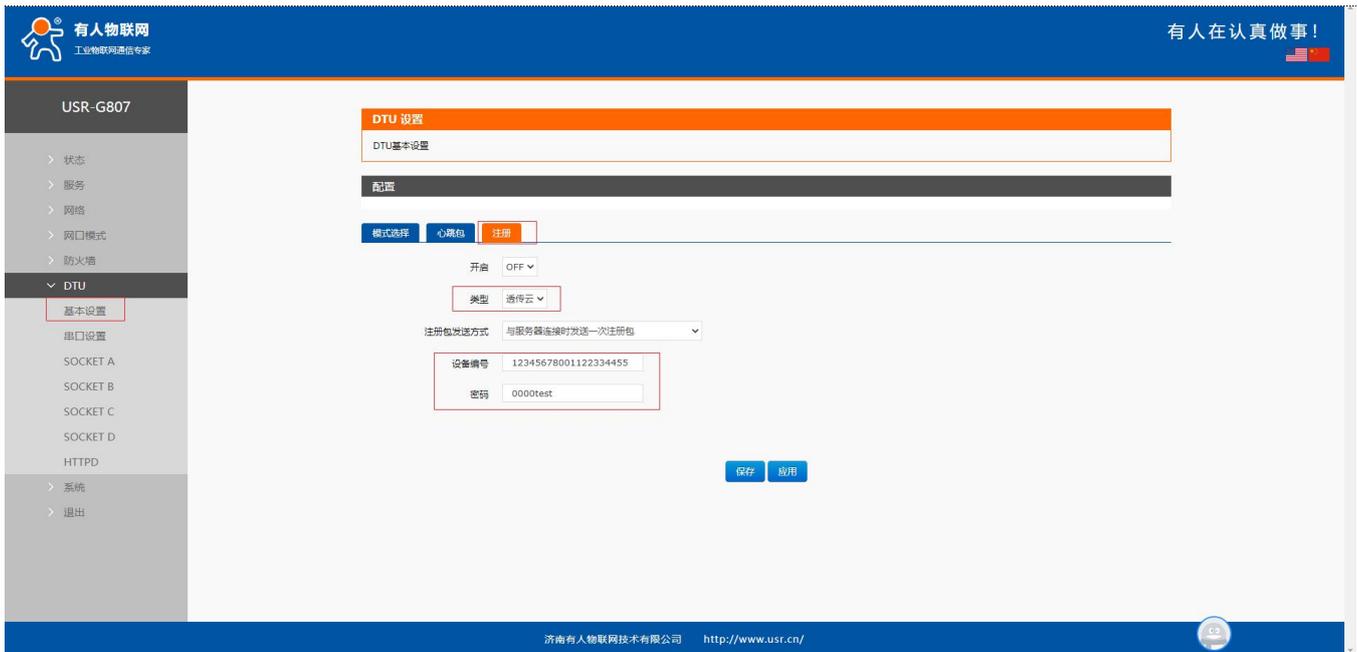


图 128 透传云参数设置

有人透传云主要是为解决设备与设备、设备与上位机（Android、IOS、PC）之间相互通信而开放的平台。透传云主要用来透传数据，接入设备几乎不需做修改便可接入实现远程透传数据。透传云适用于远程监控、物联网、车联网、智能家居等领域，所以我们的 USR-G807 也支持接入透传云。关于透传云的相关信息请浏览 cloud.usr.cn 获取更多资料。注意：本功能仅在 sockA 的 TCP Client 模式下支持。

表 21 参考 AT 指令集

指令名称	指令功能	默认参数
AT+ CLOUD	设置透传云的通信设备编号和密码	无效参数，不必关心
AT+ REGEN	查询/设置是否使能注册包	OFF
AT+ REGTP	查询/设置注册包内容类型	USER
AT+ REGSND	查询/设置注册包发送方式	DATA

AT 指令设置方法：

1. 开启注册包功能：
AT+ REGEN=ON
2. 设置注册包内容类型为透传云：
AT+ REGTP=CLOUD
3. 设置 socketA 参数：
AT+SOCKA=TCPC,cloud.usr.cn,15000
4. 设置注册包发送方式为建立连接时发送：
AT+ REGSND=LINK
5. 设置透传云 ID 和密码：
AT+ CLOUD=XXXXXXXXXXXXXX, XXXXXXXX
6. 重启：
AT+ Z

设置软件示意图：

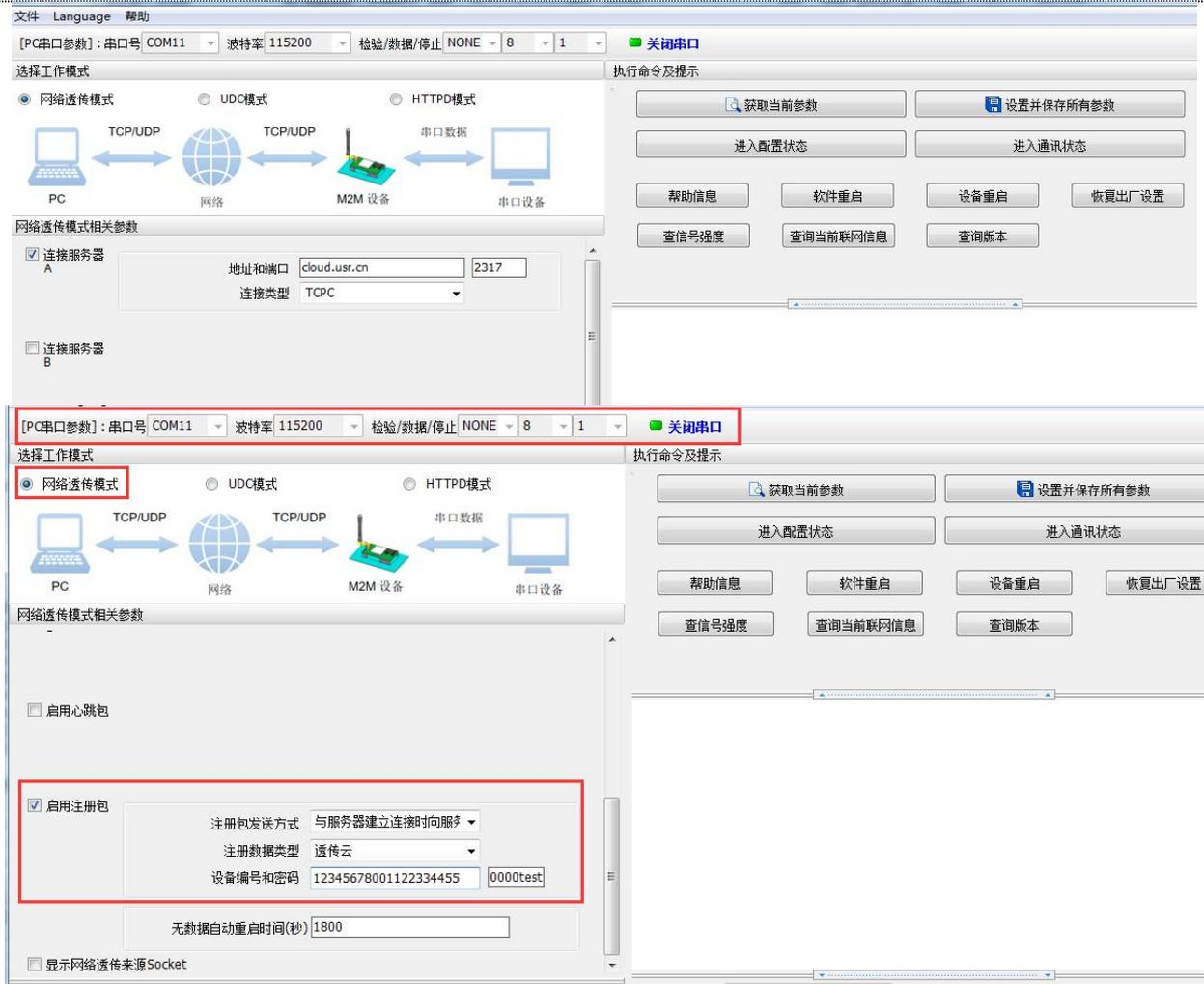


图 129 设置软件示意图

1. 打开专用设置软件“USR-G807”。根据实际情况设置串口参数并点击“打开串口”。
2. 点击“获取当前参数”，等待获取所有当前参数完毕。
3. 在“选择工作模式”一栏中，选中“网络透传模式”，并设置 sockA 的参数。
4. 开启注册包功能，并设置各项参数。
5. 点击“设置并保存所有参数”。
6. 保存完毕后，点击“软件重启”按钮。

8. AT 指令集

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
4G 相关		
5	AT+SYSINFO	查询设备网络信息
6	AT+APN	APN 地址
7	AT+CSQ	信号质量
8	AT+TRAFFIC	查询流量信息（上下行）
	AT+NETMODE	查询当前网络模式
系统相关		
9	AT+UPTIME	查询运行时间
10	AT+WWAN	查询设备 IP 地址
11	AT+LANN	设置/查询模块做网关时的 IP（仅在模块具有路由功能时有效）
12	AT+WEBU	设置/查询网页登陆名称密码
13	AT+PLANG	设置/查询 web 默认语言（中英文）
14	AT+CLEAR	恢复到模块出厂设置
15	AT+Z	重启指令，备注：要回复+ok
16	AT+DHCOPEN	打开/关闭 DHCP Server
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+LINUXCMP	执行系统 shell 指令
串口参数指令		
21	UART	查询/设置串口参数
22	UARTFT	查询/设置串口打包间隔时间
23	UARTFL	查询/设置串口打包数据长度
网络指令		
24	SOCKA	查询/设置 socket A 参数
25	SOCKB	查询/设置 socket B 参数
26	SOCKC	查询/设置 socket C 参数
27	SOCKD	查询/设置 socket D 参数
28	SOCKAEN	查询/设置是否使能 socket A

29	SOCKBEN	查询/设置是否使能 socket B
30	SOCKCEN	查询/设置是否使能 socket C
31	SOCKDEN	查询/设置是否使能 socket D
32	SOCKALK	查询 socket A 连接状态
33	SOCKBLK	查询 socket B 连接状态
34	SOCKCLK	查询 socket C 连接状态
35	SOCKDLK	查询 socket D 连接状态
36	SOCKIND	查询/设置是否使能指示透传数据来源 socket
注册包指令		
37	REGEN	查询/设置是否使能注册包
38	REGTP	查询/设置注册包内容类型
39	REGDT	查询/设置自定义注册信息
40	REGSND	查询/设置注册包发送方式
41	CLOUD	查询/设置透传云注册参数
心跳包指令		
42	HEARTEN	查询/设置是否使能注册包
43	HEARTDT	查询/设置注册包内容类型
44	HEARTSND	查询/设置自定义注册信息
45	HEARTTM	查询/设置注册包发送方式
HTTPD 指令		
46	HTPTP	查询/设置 HTTP 工作方式
47	HTPURL	查询/设置 URL
48	HTPSV	查询/设置目标服务器地址和端口
49	HTPHD	查询/设置 HTTP 协议 HEAD 信息
50	HTPTO	查询/设置超时时间
51	HTPFLT	查询/设置是否使能过滤包头

8.1. AT+VER

名称	AT+VER
功能	查询软件版本号
查询	命令: AT+VER 返回: +VER:ver
设置	无
参数	ver: 软件版本号 例如: +VER:V1.0.02
说明	无

8.2. AT+MAC

名称	AT+MAC
功能	查询 WAN 口 MAC
查询	命令: AT+MAC 返回: +MAC:mac
设置	无
参数	mac: WAN 口 MAC 例如: +MAC:9CA525000C4
说明	无

8.3. AT+ICCID

名称	AT+ICCID
功能	查询 SIM 卡 ICCID 号
查询	命令: AT+ICCID 返回: +ICCID:iccid
设置	无
参数	iccid: SIM 卡 ICCID 号 例如: +ICCID:898600161515AA709917
说明	无

8.4. AT+IMEI

名称	AT+IMEI
功能	查询设备 IMEI 号
查询	命令: AT+IMEI 返回: +IMEI:imei
设置	无
参数	imei: 设备 IMEI 号 例如: +IMEI:868323023238378
说明	无

8.5. AT+SYSINFO

名称	AT+SYSINFO
功能	查询设备网络信息
查询	命令: AT+SYSINFO 返回: +SYSINFO:operator,mode
设置	无
参数	operator: 运营商信息 CHINA-MOBILE 中国移动

	CHINA-UNICOM 中国联通 CHN-CT、CHINA-TELECOM 中国电信 mode: 驻网网络模式 2G Mode 3G Mode 4G Mode
举例	命令: AT+SYSINFO 返回: +SYSINFO:CHINA-TELECOM,4G Mode
说明	无

8.6. AT+APN

名称	AT+APN
功能	查询/设置 APN 信息
查询	命令: AT+APN 返回: +APN:code,name,password,type
设置	命令: AT+APN=code,name,password,type 返回: OK
参数	code: APN 地址, 可设置为自动 (autocheck 表示自动模式) 或者专网卡 APN 地址 name:apn 用户名 password: apn 密码 type: 鉴权方式 PAP/CHAP/0(0 表示无鉴权方式)
举例	命令: AT+APN 返回: +APN:autocheck,,PAP
说明	apn 卡必要情况需设置 apn 信息, 一般普卡与物联网卡保持默认配置即可驻网成功。

8.7. AT+CSQ

名称	AT+CSQ
功能	查询设备信号强度
查询	命令: AT+CSQ 返回: +CSQ:asu
设置	无
参数	csq:4G 信号值 GSM/CDMA/WCDMA/EVDO/EHRPD/LTE:[0-31] 换算 dBm 公式: $-113+2*csq=dBm$ csq=99:未知或不可测
	信号值范围: TDSCDMA:[100-191] 换算 dBm 公式: $-116-100+csq=dBm$ csq=199:无信号

说明	无
----	---

8.8. AT+TRAFFIC

名称	AT+TRAFFIC
功能	查询设备流量信息
查询	命令: AT+TRAFFIC 返回: +TRAFFIC:dev_down, dev_up, pro_time, at_time
设置	无
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	命令: AT+TRAFFIC 返回: +TRAFFIC:0B,0B,1614854914,1614854927
说明	无

8.9. AT+NETMODE

名称	AT+NETMODE
功能	查询当前网络模式
查询	命令: AT+NETMODE 返回: +NETMODE:mode
设置	无
参数	mode:网络模式 2G Mode 3G Mode 4G Mode
举例	命令: AT+NETMODE 返回: +NETMODE:4G Mode
说明	无

8.10. AT+UPTIME

名称	AT+UPTIME
功能	查询系统运行时间
查询	命令: AT+UPTIME 返回: +UPTIME:time
设置	无
参数	time:系统运行时间 例如: +UPTIME:16001,4:26 表示运行 16001s, 运行 4h26m

说明	无
----	---

8.11. AT+WANN

名称	AT+WANN
功能	查询 WAN 口信息
查询	命令: AT+WANN 返回: +WANN:mode,address,mask,gateway
设置	无
参数	mode: 网络 IP 模式。 static: 静态 IP DHCP: 动态 IP (address,mask,gateway 参数省略) address: IP 地址。 mask: 子网掩码。 gateway: 网关地址。
举例	命令: AT+WANN 返回: +WANN:DHCP,192.168.1.158,255.255.255.0,192.168.1.1
说明	无

8.12. AT+LANN

名称	AT+LANN
功能	查询/设置 LAN 口信息
查询	命令: AT+LANN 返回: +LANN:address,mask
设置	命令: AT+LANN=address,mask 返回: +LANN:OK
参数	address: IP 地址。 mask: 子网掩码。
举例	命令: AT+LANN 返回: +LANN:192.168.1.1,255.255.255.0
说明	无

8.13. AT+WEBU

名称	AT+WEBU
功能	查询/设置 Web 登陆用户名密码
查询	命令: AT+WEBU 返回: +WEBU:username,passwd
设置	命令: AT+WEBU=username,passwd 返回: +WEBU:OK

参数	username: 登陆用户名 passwd: 登陆密码
举例	命令: AT+WEBU 返回: +WEBU:root,root
说明	无

8.14. AT+PLANG

名称	AT+PLANG
功能	查询/设置默认语言
查询	命令: AT+PLANG 返回: +PLANG:type
设置	命令: AT+PLANG=type 返回: +PLANG:OK
参数	type: 默认语言 zh_cn 中文 En 英文
举例	命令: AT+PLANG=zh_cn 返回: +PLANG:OK
说明	无

8.15. AT+CLEAR

名称	AT+CLEAR
功能	恢复出厂设置
查询	无
设置	命令: AT+CLEAR 返回: +CLEAR:OK
参数	无
说明	无

8.16. AT+DHCPEN

名称	AT+DHCPEN
功能	打开关闭 DHCP 服务器
查询	无
设置	命令: AT+DHCPEN=status 返回: +DHCPEN:OK
参数	status: ON: 打开 OFF: 关闭
说明	无

8.17. AT+UPDATE

名称	AT+UPDATE
功能	设置/查询远程升级参数
查询	命令: AT+UPDATE 返回: +UPDATE:status,ip,point,interval
设置	命令: AT+UPDATE=status,ip,point,interval 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
举例	命令: AT+UPDATE=on,ycsj1.usr.cn,30001,1800 返回: +UPDATE:OK
说明	无

8.18. AT+MONITOR

名称	AT+MONITOR
功能	设置/查询远程监控参数
查询	命令: AT+MONITOR 返回: +MONITOR:status,ip,point,interval
设置	命令: AT+MONITOR=status,ip,point,interval 返回: +MONITOR: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
举例	命令: AT+MONITOR=on,ycsj1.usr.cn,30001,600 返回: +MONITOR:OK
说明	无

8.19. AT+HEARTPKT

名称	AT+HEARTPKT
功能	设置/查询远程监控心跳包参数
查询	命令: AT+HEARTPKT 返回: +HEARTPKT:interval,data
设置	命令: AT+HEARTPKT=interval,data 返回: +HEARTPKT:OK
参数	interval: 心跳包发送间隔 data: 心跳包数据
举例	命令: AT+HEARTPKT=30,Heartpkt

	返回: +HEARTPKT:OK
说明	无

8.20. AT+LINUXCMP

名称	AT+LINUXCMP
功能	执行后台命令
查询	无
设置	命令: AT+LINUXCMP=cmd
参数	cmd:后台命令
举例	命令: AT+LINUXCMP=ls /tmp/module_info 返回: /tmp/module_info
说明	无

8.21. AT+UART

名称	AT+UART
功能	查询/设置串口基本参数
查询	命令: AT+UART 返回: +UART:baud,uart_data,stop_data,parity
设置	命令: AT+UART=baud,uart_data,stop_data,parity 返回: OK
参数	baud:串口波特率, 可设置: 2400/4800/9600/19200/57600/115200/230400 uart_data: 数据位, 可设置: 8 stop_data: 停止位, 可设置: 1/2 Parity: 校验位, 可设置: NONE/ODD/EVEN
举例	命令: AT+UART=115200,8,1,NONE 返回: OK
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.22. AT+UARTFT

名称	AT+UARTFT
功能	查询/设置 DTU 打包时间
查询	命令: AT+UARTFT 返回: +UARTFT:uartft
设置	命令: AT+UARTFT=uartft 返回: OK
参数	uartft:DTU 打包时间, 可设置: 10-60000s
举例	命令: AT+UARTFT=10 返回: OK



说明	该命令正确执行，回复 OK 需重启 DTU 后配置生效
----	-----------------------------

8.23. AT+UARTFL

名称	AT+UARTFL
功能	查询/设置 DTU 打包长度
查询	命令：AT+UARTFL 返回：+UARTFL:uartfl
设置	命令：AT+UARTFL=uartfl 返回：OK
参数	uartft:DTU 打包长度，可设置： 5-4096 单位：Byte
说明	该命令正确执行，回复 OK 需重启 DTU 后配置生效

8.24. AT+SOCKA

名称	AT+SOCKA
功能	查询/设置 SOCKA
查询	命令：AT+SOCKA 返回：+SOCKA:type,address,port
设置	命令：AT+SOCKA=type,address,port 返回：OK
参数	type:可设置为：TCPC/TCPS/UDPC/UDPS address:可设置为 IP/域名 port:端口号，可设置为 1-65535
举例	命令：AT+SOCKA=TCPC,192.168.88.100,9999 返回：OK
说明	该命令正确执行，回复 OK 需重启 DTU 后配置生效

8.25. AT+SOCKB

名称	AT+SOCKB
功能	查询/设置 SOCKB
查询	命令：AT+SOCKB 返回：+SOCKB:type,address,port
设置	命令：AT+SOCKB=type,address,port 返回：OK
参数	type:可设置为：TCPC/UDPC/UDPS address:可设置为 IP/域名 port:端口号，可设置为：1-65535
举例	命令：AT+SOCKB=TCPC,test.cn,2137

	返回: OK
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.26. AT+SOCKC

名称	AT+SOCKC
功能	查询/设置 SOCKC
查询	命令: AT+SOCKC 返回: +SOCKC:type,address,port
设置	命令: AT+SOCKC=type,address,port 返回: OK
参数	type:TCPC/UDPC/UDPS address:IP 或域名 port:1-65535
举例	命令: AT+SOCKC=TCPC,test.cn,2137 返回: OK
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.27. AT+SOCKD

名称	AT+SOCKD
功能	查询/设置 SOCKD
查询	命令: AT+SOCKD 返回: +SOCKD:type,address,port
设置	命令: AT+SOCKD=type,address,port 返回: OK
参数	type:TCPC/UDPC/UDPS address:IP 或域名 port:1-65535
举例	命令: AT+SOCKD=TCPC,test.cn,2137 返回: OK
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.28. AT+SOCKAEN

名称	AT+SOCKAEN
功能	查询/设置 SOCKA 使能
查询	命令: AT+SOCKAEN 返回: +SOCKAEN:enable
设置	命令: AT+SOCKAEN=enable 返回: OK
参数	enable: ON/OFF ON:开启 SOCKA

	OFF: 关闭 SOCKA
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.29. AT+SOCKBEN

名称	AT+SOCKBEN
功能	查询/设置 SOCKB 使能
查询	命令: AT+SOCKBEN 返回: +SOCKBEN:enable
设置	命令: AT+SOCKBEN=enable 返回: OK
参数	enable: ON/OFF ON:开启 SOCKB OFF: 关闭 SOCKB
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.30. AT+SOCKCEN

名称	AT+SOCKCEN
功能	查询/设置 SOCKC 使能
查询	命令: AT+SOCKCEN 返回: +SOCKCEN:enable
设置	命令: AT+SOCKCEN=enable 返回: OK
参数	enable: ON/OFF ON:开启 SOCKC OFF: 关闭 SOCKC
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.31. AT+SOCKDEN

名称	AT+SOCKDEN
功能	查询/设置 SOCKD 使能
查询	命令: AT+SOCKDEN 返回: +SOCKDEN:enable
设置	命令: AT+SOCKDEN=enable 返回: OK
参数	enable: ON/OFF ON:开启 SOCKD OFF: 关闭 SOCKD
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.32. AT+SOCKALK

名称	AT+SOCKALK
功能	查询 SOCKA 连接状态
查询	命令: AT+SOCKALK 返回: +SOCKALK:state
设置	无
参数	state: ON/OFF ON:已连接 OFF:未连接
说明	无

8.33. AT+SOCKBLK

名称	AT+SOCKBLK
功能	查询 SOCKB 连接状态
查询	命令: AT+SOCKBLK 返回: +SOCKBLK:state
设置	无
参数	state: ON/OFF ON:已连接 OFF:未连接
说明	无

8.34. AT+SOCKCLK

名称	AT+SOCKCLK
功能	查询 SOCKC 连接状态
查询	命令: AT+SOCKCLK 返回: +SOCKCLK:state
设置	无
参数	state: ON/OFF ON:已连接 OFF:未连接
说明	无

8.35. AT+SOCKDLK

名称	AT+SOCKDLK
功能	查询 SOCKD 连接状态
查询	命令: AT+SOCKDLK 返回: +SOCKDLK:state
设置	无

参数	state: ON/OFF ON:已连接 OFF:未连接
说明	无

8.36. AT+SOCKIND

名称	AT+SOCKIND
功能	查询/设置 SOCKET 标识
查询	命令: AT+SOCKIND 返回: +SOCKIND:enable
设置	命令: AT+SOCKIND=enable 返回: OK
参数	enable: ON/OFF ON:开启 SOCKET 标识 OFF:关闭 SOCKET 标识
说明	串口接收到的数据以 SOCKET 标识开头, 例如通过 SOCKA 的数据 data, 发送到串口端接收到的数据是 A+data。 该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.37. AT+REGEN

名称	AT+REGEN
功能	查询/设置启用 DTU 注册包功能
查询	命令: AT+REGEN 返回: +REGEN:enable
设置	命令: AT+REGEN=enable 返回: OK
参数	enable: ON/OFF ON:开启 DTU 注册包功能 OFF:关闭 DTU 注册包功能
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.38. AT+REGTP

名称	AT+REGTP
功能	查询/设置启用 DTU 注册包类型
查询	命令: AT+REGTP 返回: +REGTP:type
设置	命令: AT+REGTP=type 返回: OK
参数	type: ICCID/IMEI/CLOUD/USER ICCID:注册包为设备 ICCID

	IMEI:注册包为设备 IMEI CLOUD:注册包为透传云设备号与密码, 需设置设备号与密码 USER:自定义注册包类型
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.39. AT+REGDT

名称	AT+REGDT
功能	查询/设置 DTU 自定义类型注册包
查询	命令: AT+REGDT 返回: +REGDT:date
设置	命令: AT+REGDT=date 返回: OK
参数	date:设置的注册包数据, 以 16 进制数据表示, 长度为偶数位
举例	命令: AT+REGDT=0123456789 返回: OK
说明	该命令正确执行, 回复 OK 需重启 DTU 后配置生效

8.40. AT+REGSND

名称	AT+RESND
功能	查询/设置 DTU 注册包发送方式
查询	命令: AT+REGSND 返回: +REGSND:type
设置	命令: AT+REGSND=type 返回: OK
参数	type: DATA/LINK DATA:将注册包添加在每次发往服务器数据前面 LINK:与服务器连接时发送一次注册包
说明	该命令正确执行, 需重启 DTU 后配置生效

8.41. AT+CLOUD

名称	AT+CLOUD
功能	查询/设置有人云设备编号和密码
查询	命令: AT+CLOUD 返回: +CLOUD:cloud_id,cloud_psw
设置	命令: AT+CLOUD=cloud_id,cloud_psw 返回: OK
参数	cloud_id: 有人云设备号[1-20]位数字或字母 cloud_psw: 有人云密码 [1-8]位数字或字母 数字: 0-9 字母: a-z A-Z

举例	命令：AT+CLOUD=01234567890123456789,testtest 返回：OK
说明	该命令正确执行，需重启 DTU 后配置生效

8.42. AT+HEARTEN

名称	AT+HEARTEN
功能	启用/禁用心跳包功能
查询	命令：AT+HEARTEN 返回：+HEARTEN:heart_enable
设置	命令：AT+HEARTEN=heart_enable 返回：OK
参数	heart_enable: ON/OFF ON: 启用心跳包功能 OFF: 关闭心跳包功能
说明	该命令正确执行，需重启 DTU 后配置生效

8.43. AT+HEARTDT

名称	AT+HEARTDT
功能	查询/设置心跳包数据
查询	命令：AT+HEARTDT 返回：+HEARTDT:data
设置	命令：AT+HEARTDT=data 返回：OK
参数	date: 设置的心跳包数据，以 16 进制数据表示，长度为偶数位
说明	该命令正确执行，需重启 DTU 后配置生效

8.44. AT+HEARTSND

名称	AT+HEARTSND
功能	查询或设置心跳包发送方向
查询	命令：AT+HEARTSND 返回：+HEARTSND:data
设置	命令：AT+HEARTSND=data 返回：OK
参数	data: NET/COM NET: 发往网络断 COM: 发往串口端
说明	该命令正确执行，需重启 DTU 后配置生效

8.45. AT+HEARTTM

名称	AT+HEARTTM
----	------------

功能	查询或设置心跳包时间
查询	命令: AT+HEARTTM 返回: +HEARTTM:tm
设置	命令: AT+HEARTTM=tm 返回: OK
参数	tm: 心跳包发送间隔时间, 可设置为[1-6000] 单位: s
说明	该命令正确执行, 需重启 DTU 后配置生效

8.46. AT+HTPTP

名称	AT+HTPTP
功能	查询或设置 HTTP 请求类型
查询	命令: AT+HTPTP 返回: +HTPTP:type
设置	命令: AT+HTPTP=type 返回: OK
参数	type: POST/GET POST:HTTP 请求类型是 POST GET: HTTP 请求类型是 GET
说明	该命令正确执行, 需重启 DTU 后配置生效

8.47. AT+HTPURL

名称	AT+HTPURL
功能	查询或设置 HTTP 请求 URL
查询	命令: AT+HTPURL 返回: +HTPURL:url
设置	命令: AT+HTPURL=url 返回: OK
参数	url:必须以[3F]结尾,[5-100]字符,字符类型不做限制
说明	该命令正确执行, 需重启 DTU 后配置生效

8.48. AT+HTPSV

名称	AT+HTPSV
功能	查询或设置 HTTP 请求服务器地址端口号
查询	命令: AT+HTPSV 返回: +HTPSV:ip,port
设置	命令: AT+HTPSV=ip,port 返回: OK
参数	ip:IP 或域名 port:端口号[1-65535]

说明	该命令正确执行，需重启 DTU 后配置生效
----	-----------------------

8.49. AT+HTPHD

名称	AT+HTPHD
功能	查询或设置 HTTP 请求头
查询	命令：AT+HTPHD 返回：+HTPHD:head
设置	命令：AT+HTPHD=head 返回：OK
参数	head:[9-250]字节，必须以[0D][0A]结尾
说明	该命令正确执行，需重启 DTU 后配置生效

8.50. AT+HTPTO

名称	AT+HTPTO
功能	查询或设置 HTTP 请求超时时间
查询	命令：AT+HTPTO 返回：+HTPTO:tm
设置	命令：AT+HTPTO=tm 返回：OK
参数	tm:[1-60]单位：S
说明	该命令正确执行，需重启 DTU 后配置生效

8.51. AT+HTPFLT

名称	AT+HTPFLT
功能	查询或设置 HTTP 请求过滤头部
查询	命令：AT+HTPFLT 返回：+HTPFLT:filter
设置	命令：AT+HTPFLT=filter 返回：OK
参数	filter:ON/OFF ON：设置为过滤 HTTP 请求头部 OFF：设置为不过滤 HTTP 请求头部
说明	该命令正确执行，需重启 DTU 后配置生效

9. 联系方式

公 司：济南有人物联网技术有限公司

地 址：山东省济南市历下区茂岭山三号路中欧校友产业大厦 12 层、13 层

网 址：<http://www.usr.cn>

客户支持中心：<http://h.usr.cn>

邮 箱：sales@usr.cn

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

10. 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。

11. 更新历史

说明书版本	更新内容	更新时间
V1.0.1	创立文档，完成相关功能描述	2021-03-04



 **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

山东有人物联网股份有限公司

济南总部

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
电话：4000 255 652 0531-88826739
Email: sales@usr.cn

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

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

销售联系方式

华东大区：房召猛 15553138586
华中大区：雷爽 17754448760

华北大区：张永增 18653122839
华南大区：周万平 18665818916

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

武汉办事处

地址：武汉市高新大道426号华新大厦1901
电话：17754448760

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



关注有人微信公众号



登录商城快速下单