USR-G806 说明手册

文件版本：V1.0.23

目录

1. 快速入门

4G 路由器为用户设备提供一种无线远距离快速联网解决方案，通过内置网页进行参数设置，满足场景应用。

本章是针对 USR-G806 路由器产品的快速入门介绍，建议用户系统的阅读本章并按照指示操作一遍，将会对 4G 路由器产品有一个基本的认识。针对特定的功能细节和说明，请参考后续章节。

如在使用过程中遇到问题，可以提交到我们的客户支持中心：http://h.usr.cn

如需产品的相关资料，可以到官网链接下载对应的产品手册：http://www.usr.cn/Product/182.html

图 1 官网产品页面

1.1. 硬件环境

产品测试数据流拓扑图：

图 2　　入门测试数据流图

- 硬件：PC 机 1 台，路由器 1 套（含天线、电源适配器）、网线 1 根（自备）、4G 的 SIM 卡（自备）

- 接线：电脑通过网线连接 USR-G806 的 LAN 口，WiFi 天线、全频天线依次接在对应的天线接口上
- 联网：在断电状态下插入 SIM 卡（卡槽正面对应“sim”丝印正方向）
- 供电：USR-G806 工作电压为 DC5~36V，建议配套使用出厂提供的 DC 12V/1A 电源适配器
- 上电之后，观察指示灯：PWR 常亮、LAN 闪烁、4G 灯（3G+2G 灯）点亮、信号灯全亮代表信号良好。

1.2. 网络连接

网络连接：配置计算机网卡，选择自动获取 IP 地址

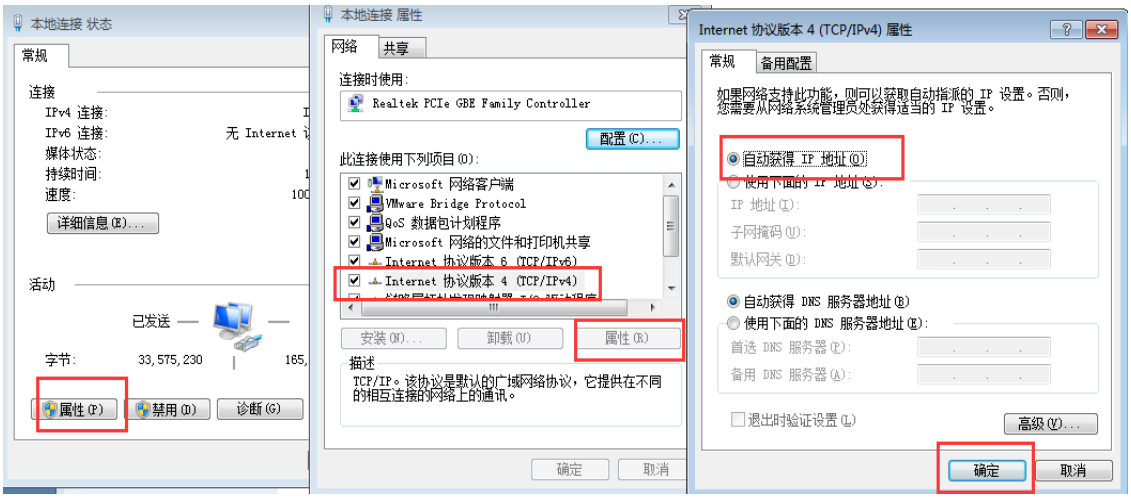


图 3 IP 获取示意图

上网测试：给 USR-G806 上电，等待大约 2 分钟，2/3G 指示灯开始亮起，表明路由器的 4G 联网成功，此时就可以直接上网了。我们先通过 USR-G806 的默认参数进入设置查看下网络状态。

表 1 路由器初始值

参数	初始值
用户名	root
密码	root
自身 IP 地址	192.168.1.1

在电脑的浏览器中输入：192.168.1.1，然后敲回车，下图为路由器登录界面

图 4 登陆首页

用户名与密码均输入 root。左侧菜单栏选择网络=>网络诊断=>Ping 工具，能够 ping 通域名（这里以百度为例），表示联网正常。也可以直接打开浏览器，直接输入想要登陆的网站网址。

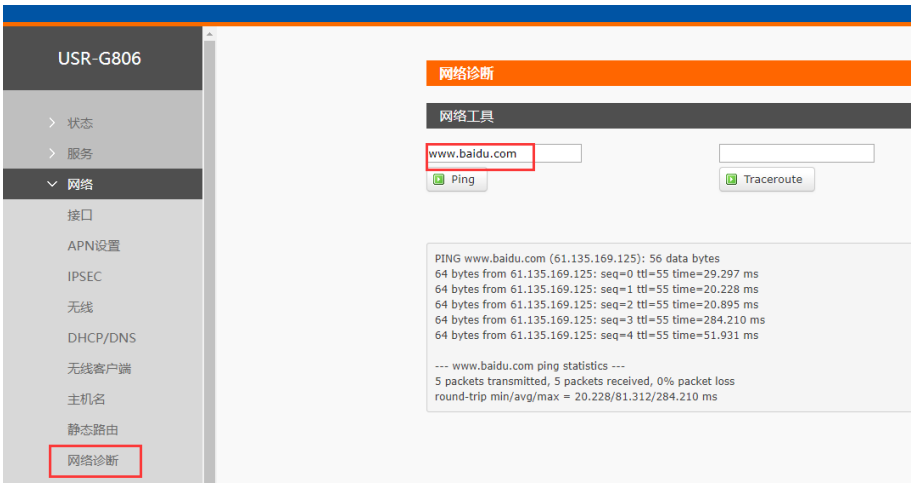


图 5 网络诊断页面

网速测试：使用测速工具测速结果（本测试使用 4G 卡，根据当地网络不同，速度可能有差别，理论最高值应当是上行 50Mbps，下行 150Mbps），如下。

图 6 网络测速

2. 产品简介

USR-G806 是一款高性价比的 4G 路由器，利用公用无线网络，为用户设备提供了快速联网的解决方案。

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、工业自动化等领域提供可靠的数据传输组网。

2.1. 产品特点

- 支持 1 个有线 LAN 口，1 个有线 WAN 口（可切换成 LAN 口），均为 10/100Mbps 速率
- 支持 1 个 WLAN 无线局域网，支持多种 LED 通信指示灯
- 支持有线无线多网同时在线、多网智能切换备份功能
- 支持 APN 自动检网、制式切换、SIM 信息显示，支持 APN/VPDN 专网卡
- 支持花生壳内网穿透、动态域名（DDNS）、PPPoE、DHCP、静态 IP 功能
- 支持 VPN(PPTP、L2TP、IPSec、OpenVPN、GRE、SSTP)等功能
- 支持防火墙、NAT、黑白名单访问限制，支持 SNAT、DNAT 功能，可以自定义通信规则
- 支持流量服务，可以根据需要设定接口限速、IP 限速、MAC 限速
- 支持支持 SSH、TELNET、Web 多平台管理配置方式
- 支持 M2M 远程管理平台，具备远程监控、升级和参数配置等功能
- 支持一键恢复出厂设置，支持硬件看门狗，保证系统的稳定性
- 导轨式或壁挂式安装，适配各种场景

2.2. 技术参数

G806 系列路由器的主要型号及规格如下。

USR-G806：支持移动、联通 2G/3G/4G，电信 4G;

USR-G806-43：支持移动、联通、电信的 2G/3G/4G。

表 2 USR-G806 基本参数

路由器	USR-G806	USR-G806-43
硬件规格		
电源	DC 5.0 ～ 36.0V	
有线 WAN 口	1 个 10/100mbpsT(X)端口	
有线 LAN 口	1 个 10/100mbpsT(X)端口	
网口类型	RJ45，交叉直连自动切换	
电磁隔离保护	1.5kv	
SIM/USIM 卡	普通 SIM 卡	
其他接口	状态指示灯、Reload 键	
WiFi 规格		
无线标准	支持 802.11b/g/n	
天线	1 个/3dbi 输出增益	
天线接口	SMA 接口(外螺内孔)	
2G/3G/4G 规格		
制式标准	TDD-LTE FDD-LTE WCDMA TD-SCDMA GSM/GPRS/EDGE	TDD-LTE FDD-LTE WCDMA TD-SCDMA EVDO/CDMA1X GSM//GPRS/EDGE
天线数量	1 个/全频棒状天线	1 个/全频吸盘天线
天线接口	SMA 接口(外螺内孔)	
频段信息		
TDD-LTE	Band 38/39/40/41	Band 38/39/40/41
FDD-LTE	Band 1/3/8	Band 1/3/5/8
WCDMA	Band 1/8	Band 1/8
CDMA2000	-	BC0
TD-SCDMA	Band 34/39	Band 34/39
GSM/GPRS/EDGE	Band 3/8	Band 3/8
技术规范		
TDD-LTE	3GPP R9 CAT4 下行 150 Mbps 上行 50 Mbps	下行 130 Mbps 上行 35 Mbps
FDD-LTE	3GPP R9 CAT4 下行 150Mbps 上行 50Mbps	下行 150Mbps 上行 50Mbp
WCDMA	HSPA+ 下行 21Mbps 上行 5.76Mbps	3GPP R8 CAT24 DC-HSPA+ 下行 42Mbps 上行 5.76Mbps 3GPP R6 CAT6 HSUPA/HSUPA+ 下行 21Mbps 上行 5.76 Mbps

CDMA2000	-	下行：3.1Mbps 上行：1.8Mbps
TD-SCDMA	3GPP R9 下行 2.8 Mbps 上行 2.2 Mbps	下行 4.2 Mbps 上行 2.2 Mbps
GSM	下行 384kbps 上行 128kbps	下行 384kbps 上行 128kbps
功率等级		
TDD-LTE Band38/39/40/41	23dBm (Power class 3)	23dBm (Power class 3)
FDD-LTE Band 1/3/8	23dBm (Power class 3)	23dBm (Power class 3)
WCDMA Band 1/8	23dBm (Power class 3)	24dBm (Power class 3)
TD-SCDMA Band34/39	24dBm (Power class 3)	24dBm (Power class 3)
CDMA2000	-	24dBm (Power class 3)
GSM Band8	33dBm (Power class 4)	33dBm (Power class 4)
GSM Band3	30dBm (Power class 1)	30dBm (Power class 1)
其他		
尺寸（mm）	110.0*94.0*29.0（L*W*H，不含电源端子，天线及天线座）	
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）	
资质认证		
安规认证	CE 、RoHS、3C	CE、RoHS、3C

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 3 G806 功耗表

工作方式	供电电压	平均电流	最大工作电流
LAN+WAN 全速通信（4G 正常+WLAN 正常）	DC12V	175mA	385mA
单独 LAN 口全速通信（4G 正常+WLAN 正常）	DC12V	147mA	243mA
LAN+WAN 全速通信（4G 无卡+WLAN 正常）	DC12V	126mA	216mA
LAN+WAN 全速通信（4G 无卡+WLAN 正常）	DC12V	98mA	183mA

G806 在 12V 供电并全速工作时，统计得出：

平均功耗 1.8W，最大工作功耗 4.6W。平均电流 175mA，最大工作电流 385mA。

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。

2.3. 接口说明

图 7 G806 外观接口图

硬件接口描述如下

表 4 接口描述

序号	名称	备注
1	DC 电源座	供电范围 DC:5-36V，标准 5.5*2.1 电源座
2	DC 电源端子	供电范围 DC:5-36V，绿色端子座，端子尺寸 5.08mm-2，注意正负极性防止接错
3	WAN 口	广域网接口，10/100Mbps，支持 Auto MDI/MDIX

4	LAN 口	局域网接口，10/100Mbps，支持 Auto MDI/MDIX
5	USB 口	预留
6	指示灯	10 路状态指示灯，说明详见指示灯章节的描述
7	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
8	Reload 按键	Reload：长按 5s 以上再松开，恢复出厂设置
9	WPS 按键	预留（WPS 功能正在做）
10	WiFi 天线	2.4G 棒状天线，156mm
11	全频天线	全频吸盘天线，Φ30*310mm

注意

- **关于 WiFi 天线跟 4G 天线的区分，在天线的尾端有相关标识；**
- **SIM 卡不支持热插拔，安装或更换 SIM 卡时请在断电下进行操作。**

2.4. 状态指示灯

共有 10 个状态指示灯，含义如下

表 5 指示灯说明表

名称	说明
Power	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（1-4）	信号强度指示灯亮起的灯越多，信号越强

<说明>

- WAN 与 LAN 的工作情况，由 WAN 以及 LAN 指示灯来指示；
- 网线插入且对端的网络设备也在工作，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。

2.5. 安装尺寸

单位：mm

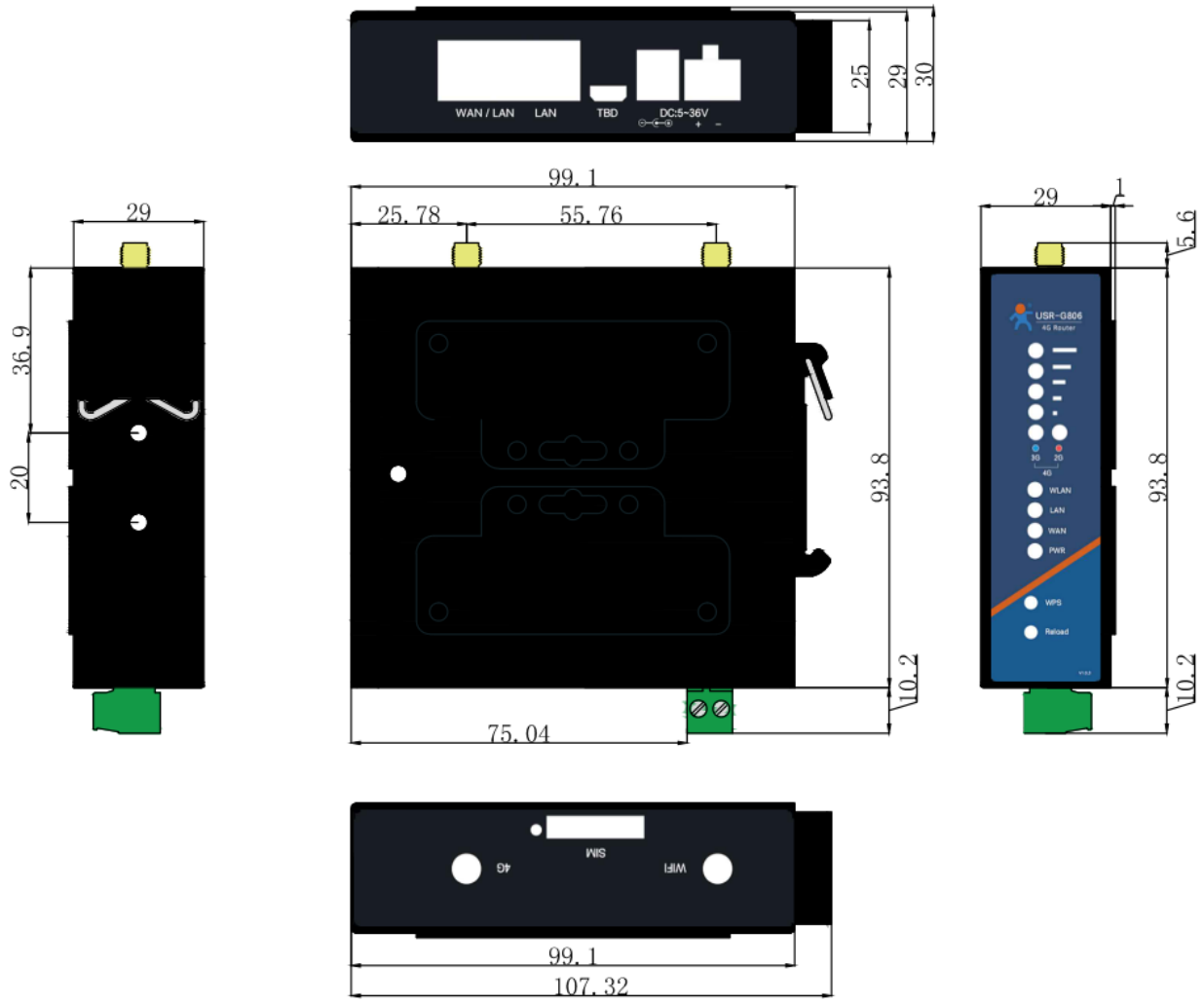


图 8 USR-G806 尺寸图

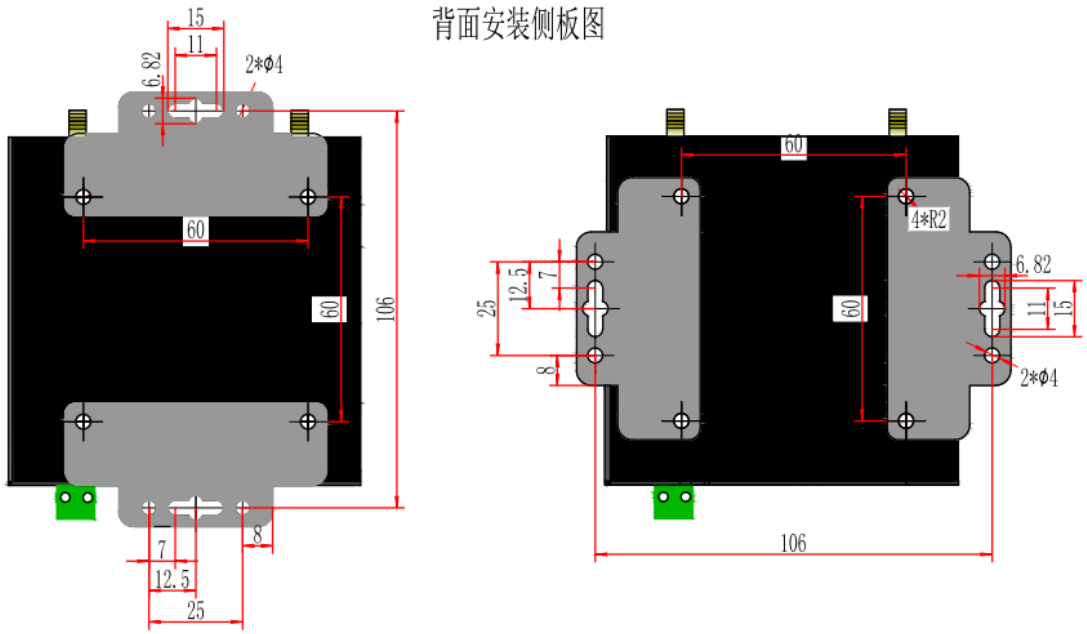


图 9 USR-G806 安装侧板图

注意：

- 钣金外壳，两侧固定孔，兼容导轨安装件
- 长宽高分别为 99.1*93.8*29.0mm（不含电源端子，天线及天线座）
- 安装方式：35mm 导轨式安装、挂耳式安装。挂耳安装尺寸：106.0*25.0mm(L*W)

3. 系统基本功能

本章介绍一下 USR-G806 所具有的功能，下图是模块的功能的整体框图。

图 10　　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 11　　联网示意图

- 用户设备或电脑，可以通过 G806 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。

3.1. Web 页面设置

首次使用 USR-G806 设备时，可以通过 PC 连接 USR-G806 的 LAN 口，或者连接上 WLAN 无线，然后用 web 管理页面配置相关参数。默认参数如下。

表 7 USR-G806 网络默认设置表

参数	默认设置
SSID	USR-G806-XXXX
LAN 口 IP 地址	192.168.1.1
用户名	root
密码	root
无线密码	www.usr.cn

首先操作电脑加入 USR-G806-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。

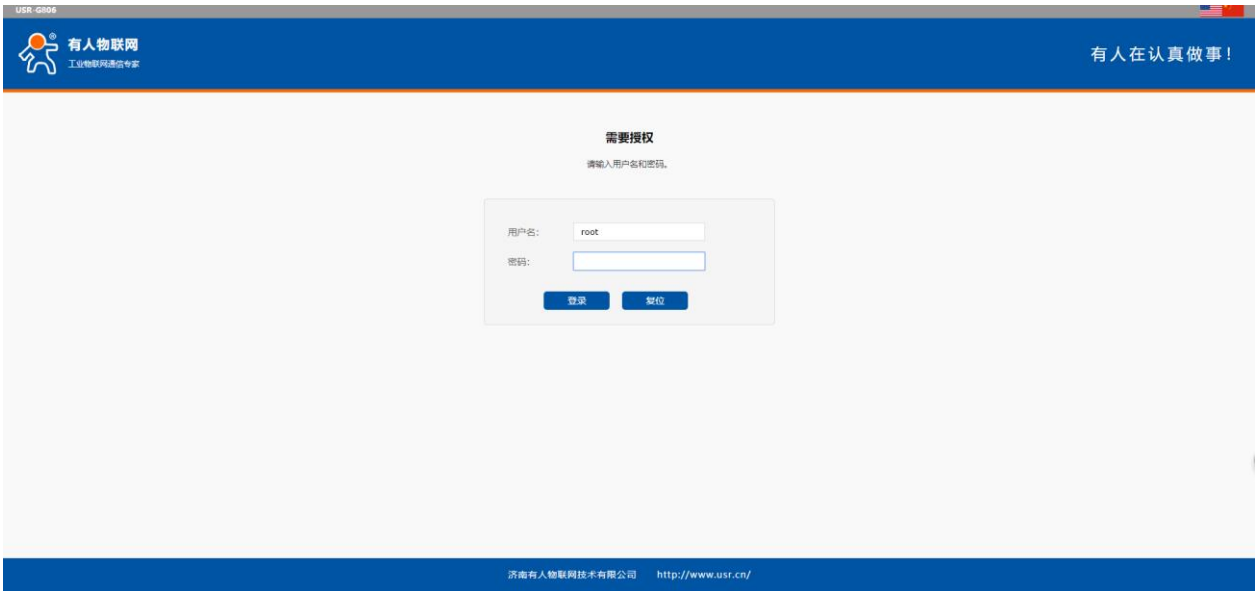


图 12 首页页面

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、固件升级等；

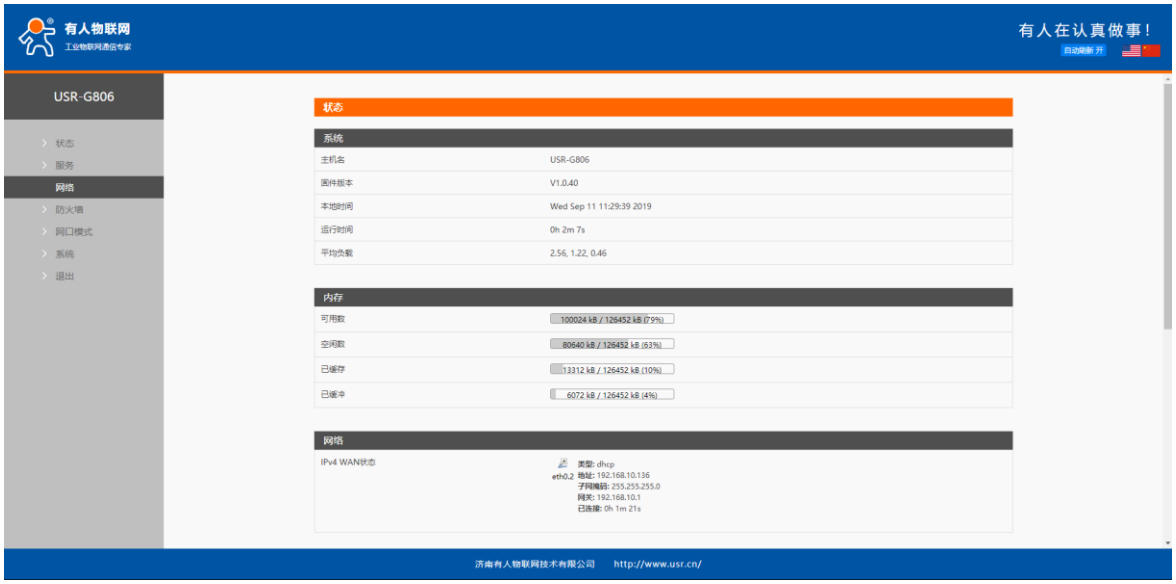


图 13 状态网页

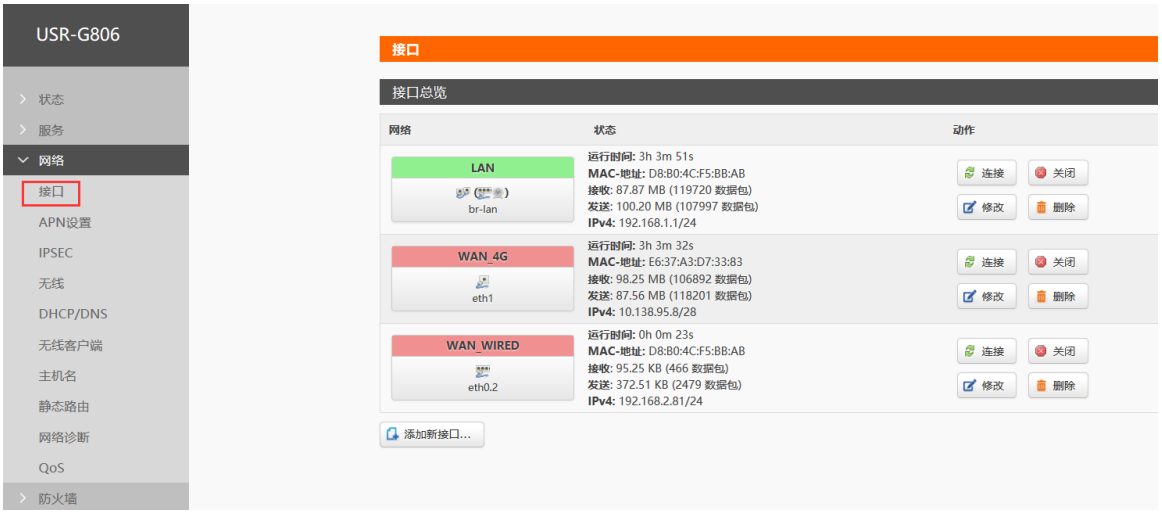


图 14　　接口网页

3.2. 主机名与时区

路由器自身主机名默认 USR-G806，时区为北京时区。

图 15　　主机名和时区设置页面

3.3. NTP 设置

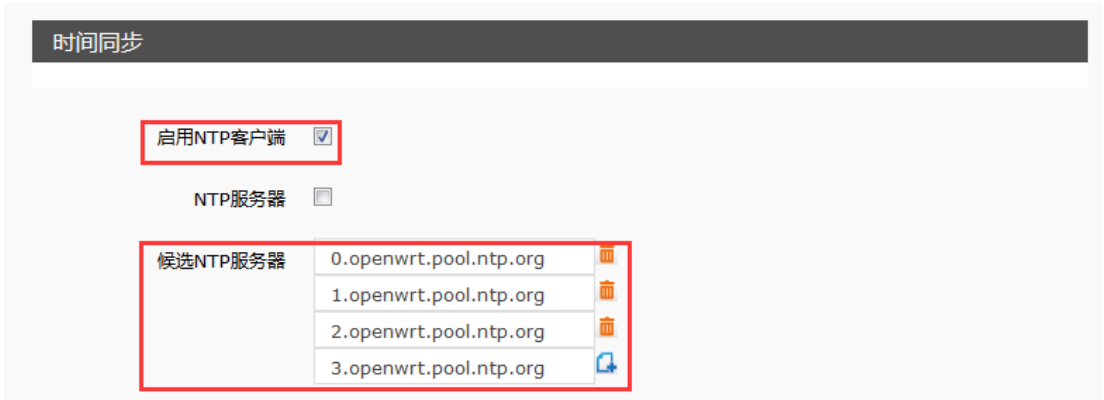


图 16　　NTP 页面

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。

3.4. 用户密码设置

图 17　　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。

3.5. 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-G806-2019-09-09.tar.gz ，并保存到本地。

图 18　　备份/恢复页面

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 19　参数备份上传页面

<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。

3.6. 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 20　恢复出厂页面

通过 Reload 按键（恢复出厂设置按键），可将 G806 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）

3.7. 固件升级

USR-G806 模块支持 web 方式的在线固件升级。

图 21　　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

➢ 固件升级检查按钮，去掉后不再进行固件升级的检测，在升级老版本固件(V1.0.35 之前)时可以去掉

➢ 多只路由器组合使用时，需要升级为同一版本最新固件。

3.8. 设备重启

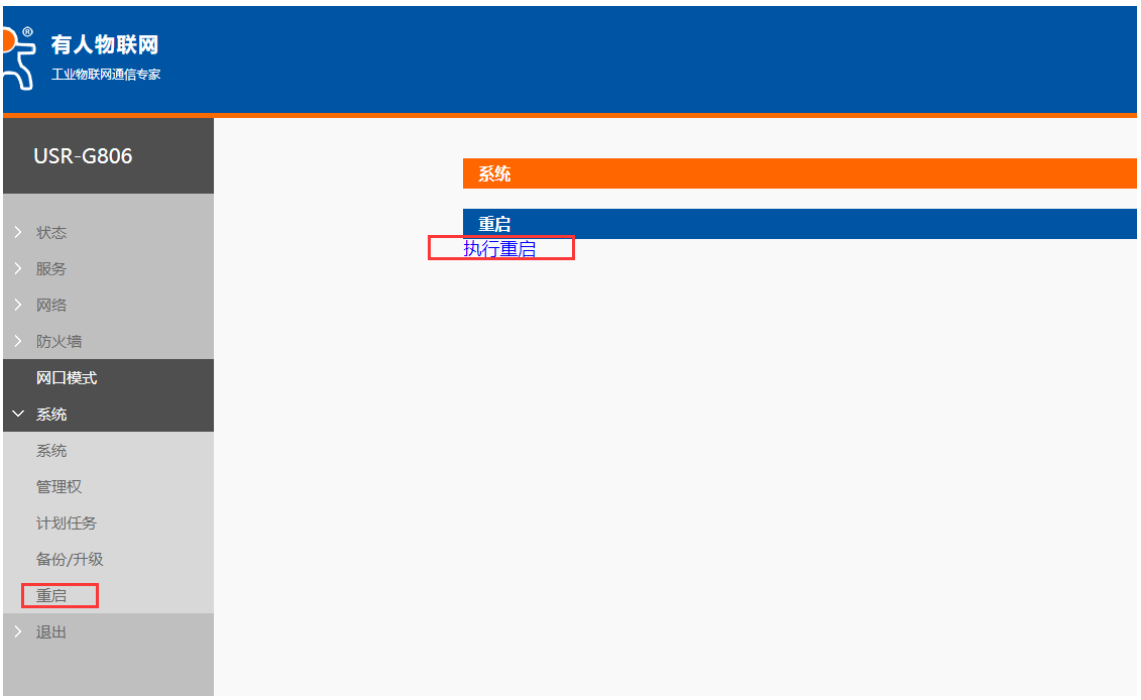


图 22　　重启页面

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 90 秒后完全启动成功。

3.9. 计划任务

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。

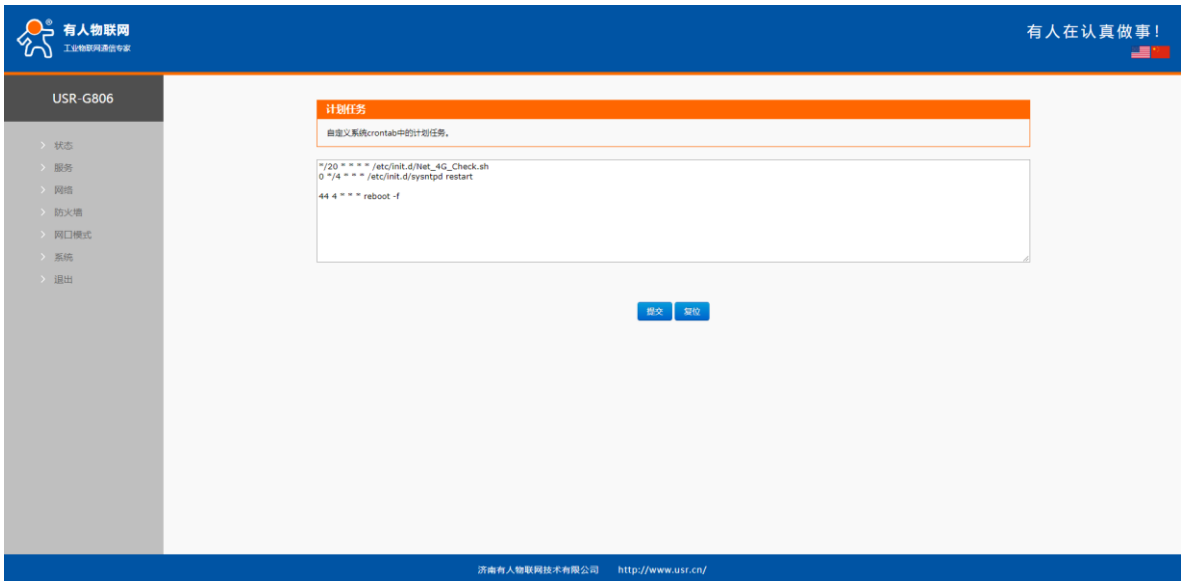


图 23　　计划任务设置页面

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>

- 原有第一条计划任务为每隔 20 分钟进行 4G 联网检测
- 原有第二条计划任务为每 4 个小时重启校准时间进程
- 原有第三条计划任务为每天 4:44 重启路由器
- 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；
- 原有计划任务一和原有计划任务二不可删除，删除后会影响路由器正常使用；
- 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。

3.10. 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；
- 系统日志缓存区大小：默认 128k
- 日志记录等级：默认最低等级，不支持分级；

图 24　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（先生成后下载）。

图 25　内核 log

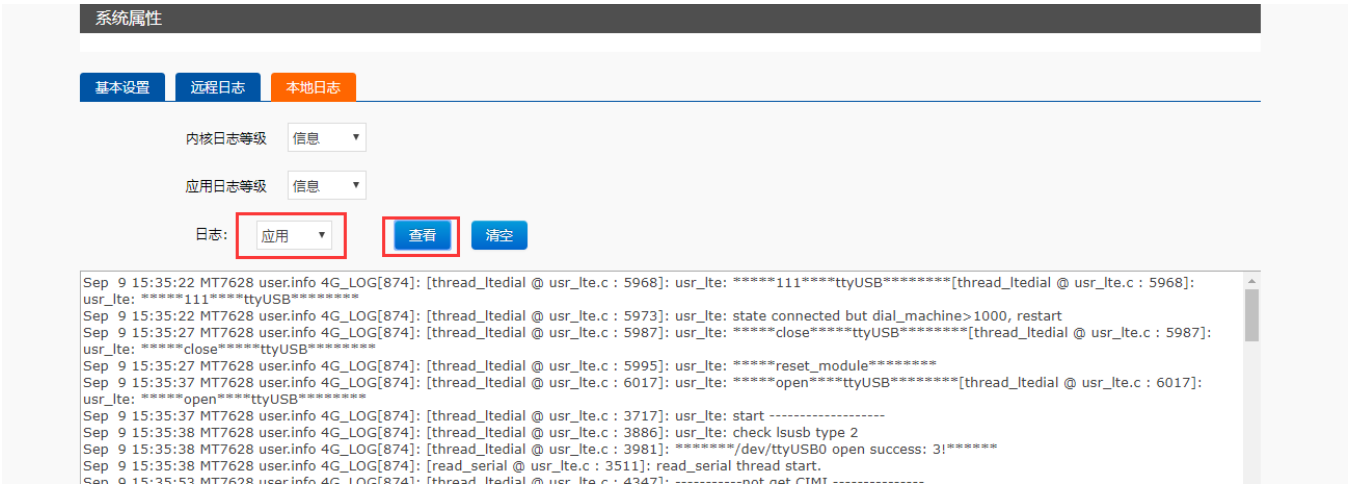


图 26　　应用 log

4. 网络接口功能

4.1. 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。

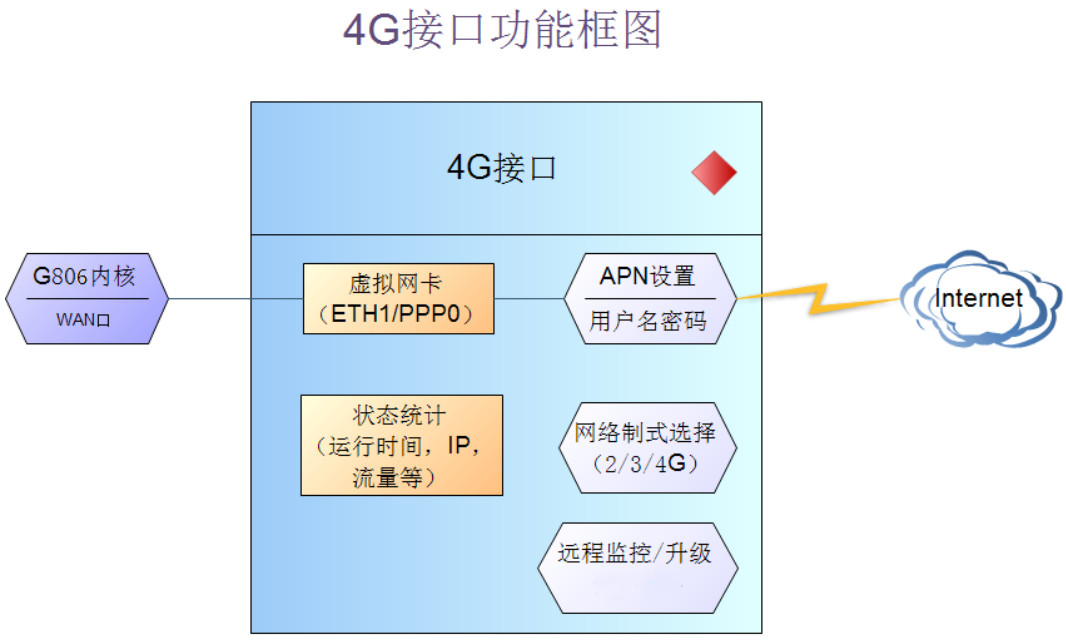


图 27　　4G 功能示意图

网页界面如下。

图 28　　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 8 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>

- USR-G806：支持移动，联通的 2/3/4G 以及电信 4G
- USR-G806-43：支持移动，联通，电信的 2/3/4G，为全网通
- 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，请在一个应用中只使用一种接口
- 如果您使用 APN 专网，请参考 APN 章节的介绍

4.2. APN 设置

4.2.1. APN 设置

APN 参数设置如下。

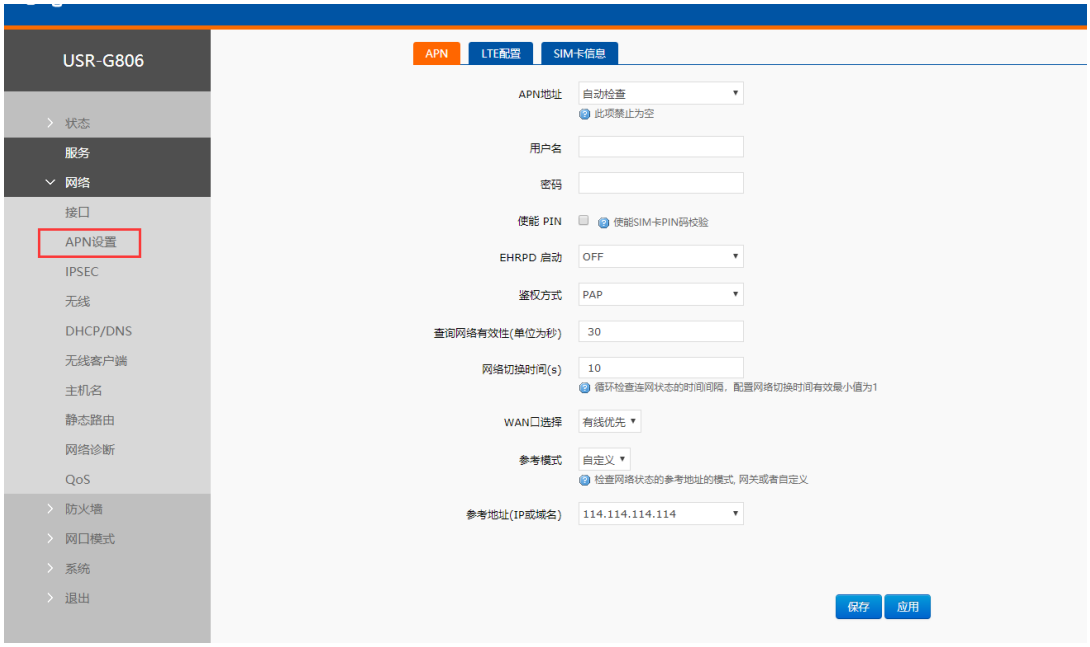


图 29　　APN 设置页面

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 9 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
EHRPD 启动	3.5G 网络时启动
鉴权方式	APN 的鉴权方式，默认即可
查询网络有效性	默认 30 轮询检测网络是否有效
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
- 不同运营商的 APN 专网卡规格不同，APN 地址、用户名和密码（如有），请咨询运营商。

4.2.2. 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：

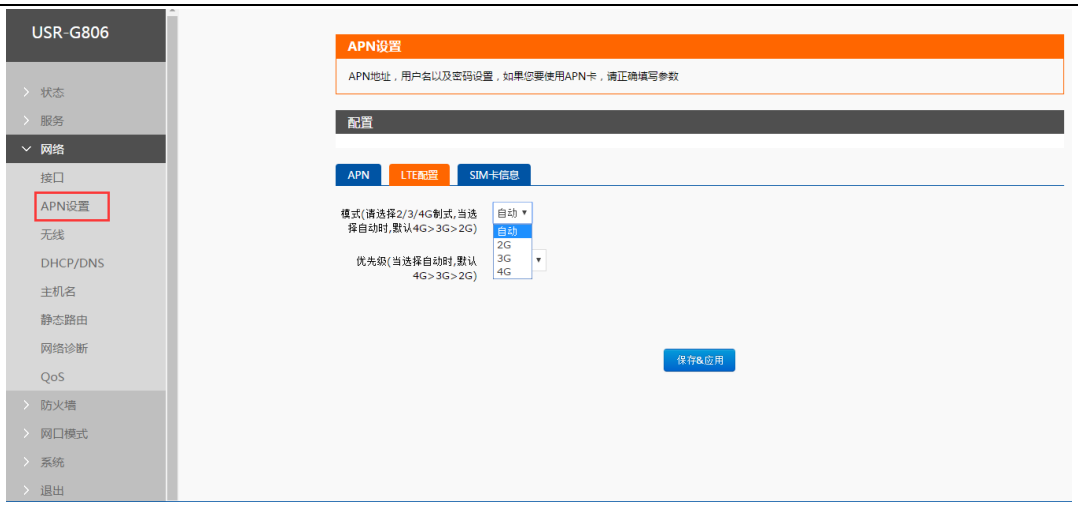


图 30　　网络制式选择

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 10　　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

4.2.3. 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。

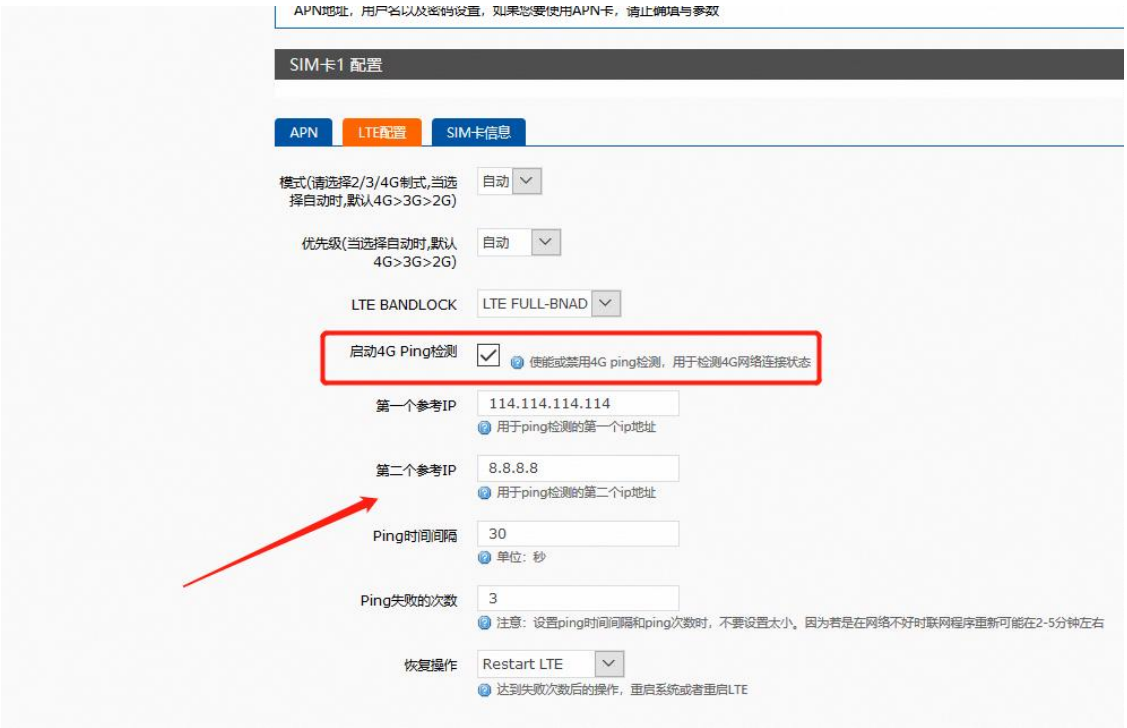


图 31　　4G 实时 ping 检测

4.2.4. 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 32　　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
- 不同产品型号，信号强度有着不同的显示方式。
- 7 模 USR-G806-43 版本使用 asu 值表示；asu 的范围为 1-31，数值越大，信号强度越好；
- 5 模 USR-G806 版本使用 dBm 值表示，不同制式的显示方式不同，需要按照下表进行换算；

制式	取值	信号强度（dBm）
GSM	0-31	dBm=-113dBm+ 信号强度
TD	100-199	dBm=-115dBm+（信号强度-100）
LTE	100-199	dBm=-140dBm+（信号强度-100）
GSM/TD/LTE	99	未知或者不可测

- 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≥-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。

4.3. 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）。

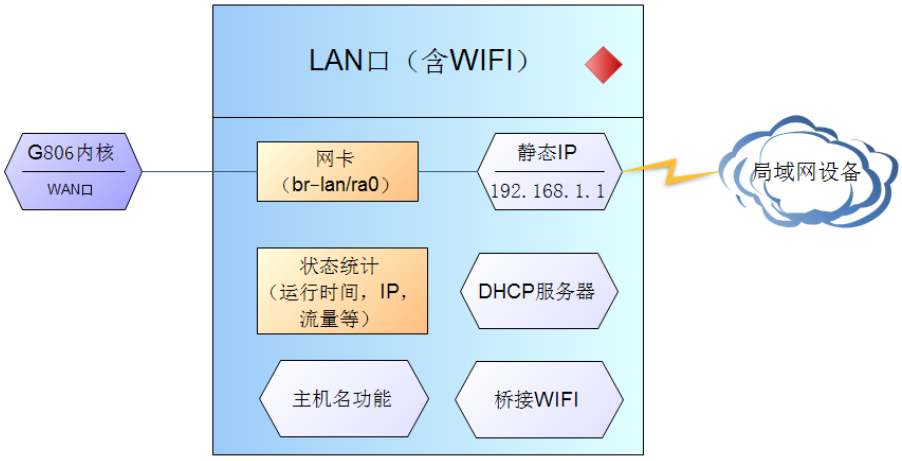


图 33　　LAN 口功能示意图

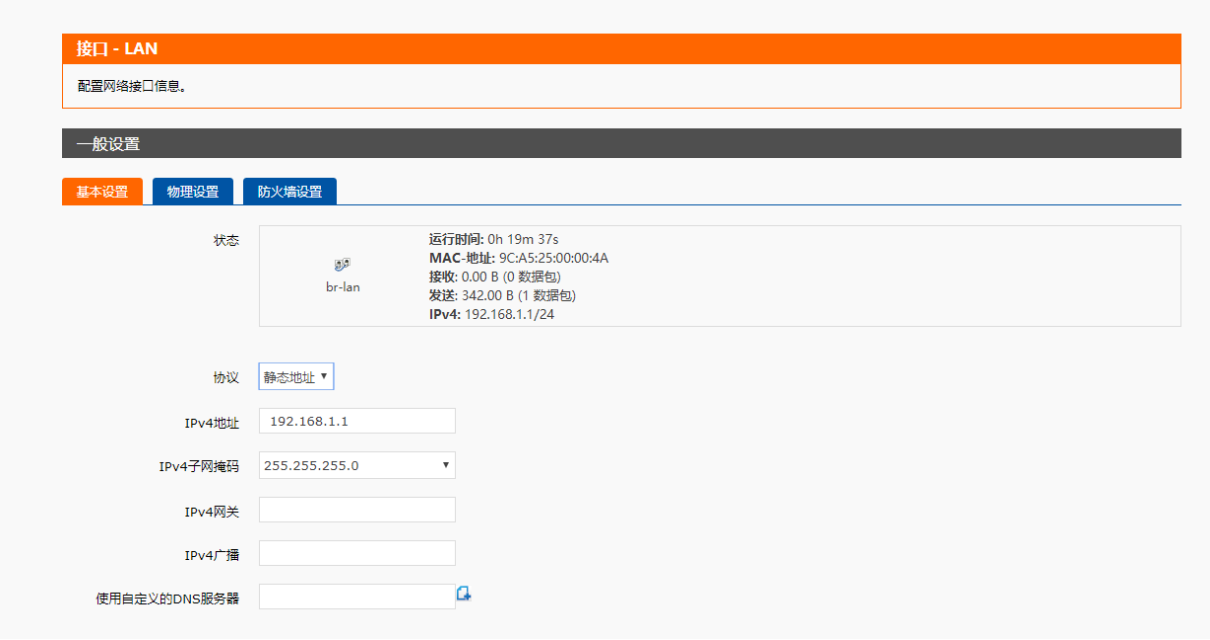


图 34　　LAN 口设置页面

<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（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
- 具备简单的状态统计功能
- LAN 接口-物理设置配置不可随意配置，除 lan(eth0.1)、wan_wired(eth0.2)、wan_4g(eth1)、wwan(apcli0)接口之外都为内部接口；
- 如若误配导致 LAN 接口不可使用请还原出厂时 LAN 配置

4.3.1. DHCP 功能

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

图 35　　DHCP 设置页面

<说明>

- 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

4.3.2. 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 36　　DHCP/DNS 设置页面

4.4. WAN 口

图 37　　WAN 口设置页面

<说明>

- 1 个有线 WAN 口，WAN 口为广域网接口。
- 支持 DHCP 客户端、静态 IP、PPPOE 模式
- 默认 IP 获取方式为 DHCP Client
- WAN 接口-物理设置配置不可随意配置，除 lan(eth0.1)、wan_wired(eth0.2)、wan_4g(eth1)、wwan(apcli0)接口之外都为内部接口；
- 如若误配导致 WAN 接口不可使用请还原出厂时 WAN 配置

4.5. WiFi 无线接口

无线局域网的功能框图如下图所示：

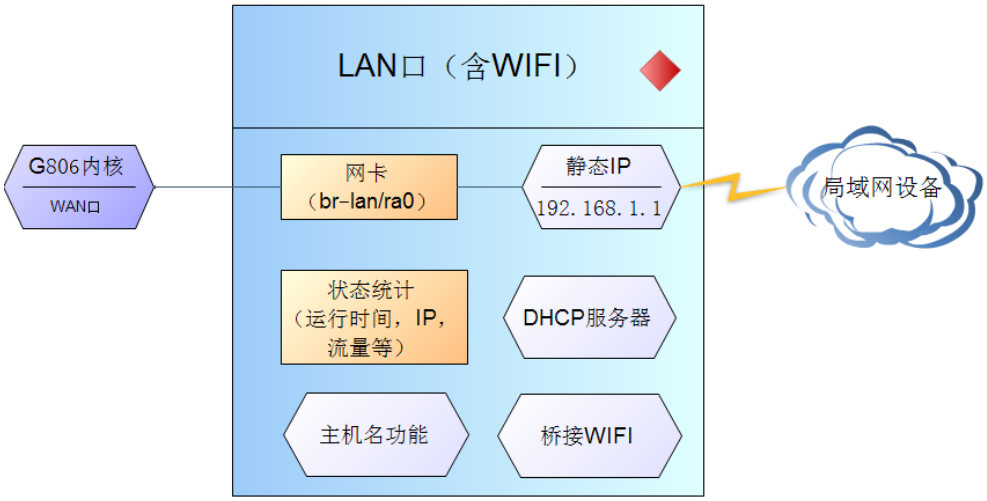


图 38　　WiFi 功能示意图

<说明>

- G806 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，办公室等有障碍物地受环境影响可在 50m 内覆盖

图 39　　WiFi 功能示意图

默认参数如下。

表 11　　WiFi 默认参数

默认参数	数值
SSID 名称	USR-G806-XXXX（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“网络-无线-接口位置”修改 SSID 和无线密码。

图 40　　SSID 设置页面

图 41　　WiFi 密码设置页面

在“网络-无线-设备配置”位置，修改是否开启无线功能（将射频关闭，如下图，即时生效）、网络模式、信道、带宽设置。

图 42　　WiFi 开关设置页面

4.6. 网络诊断功能

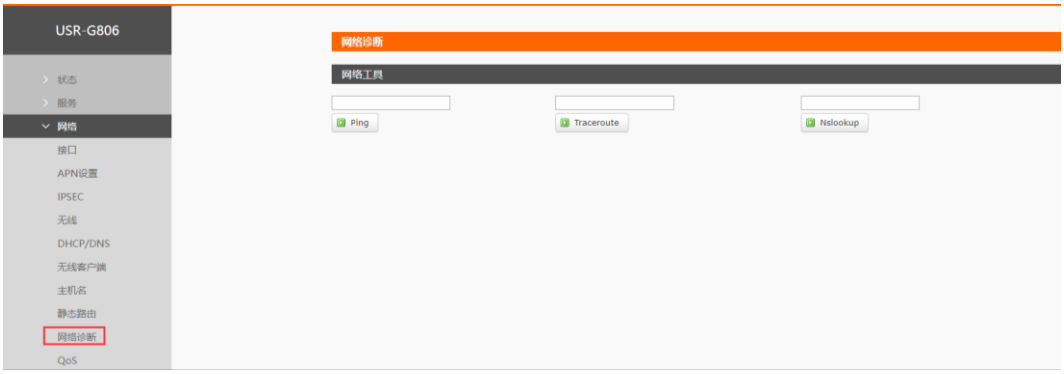


图 43　网络诊断页面

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。

4.7. 主机名功能

图 44　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“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 45　主机名 PING 功能

4.8. 接口限速

图 46　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，限制下行速度为 200Kbps（约 20KB/s），那么使用测速工具测得上网速度如下，

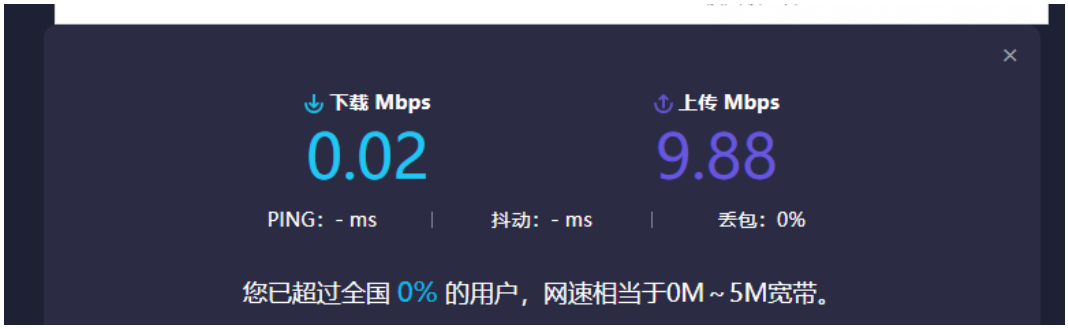


图 47　限速测试图

<说明>

- 设置 LAN 口时会限制下载的速度；设置其他的外网接口是限制的上传速度。

5. VPN Client 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、SSTP。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 G806 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。

下面是这几种协议的具体搭建过程。

5.1. PPTP Client 搭建

5.1.1. PC 端连接 VPN(基于 PPTP 协议)

为了方便理解与测试，本章节我们分两部分来介绍，首先，介绍 windows 端的 VPN Server 与 VPN Client 是如何创建与使用的；最后，再介绍本路由器的 VPN 功能使用。

我们先在服务器上创建 VPN Server。

打开服务器（远程服务器）上的网络连接页面，点击 “文件” -> “新建传入连接”，

然后，选择增加账户，请输入用户名，以及密码等信息。

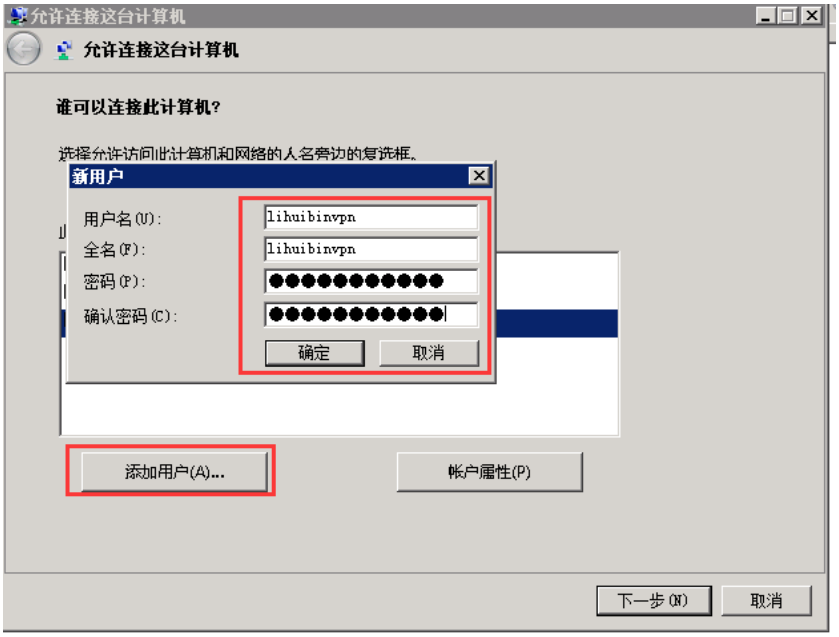


图 48　　PC 连接 VPN 操作一

点击“下一步”，勾选“通过 Internet”来连接到这台计算机。

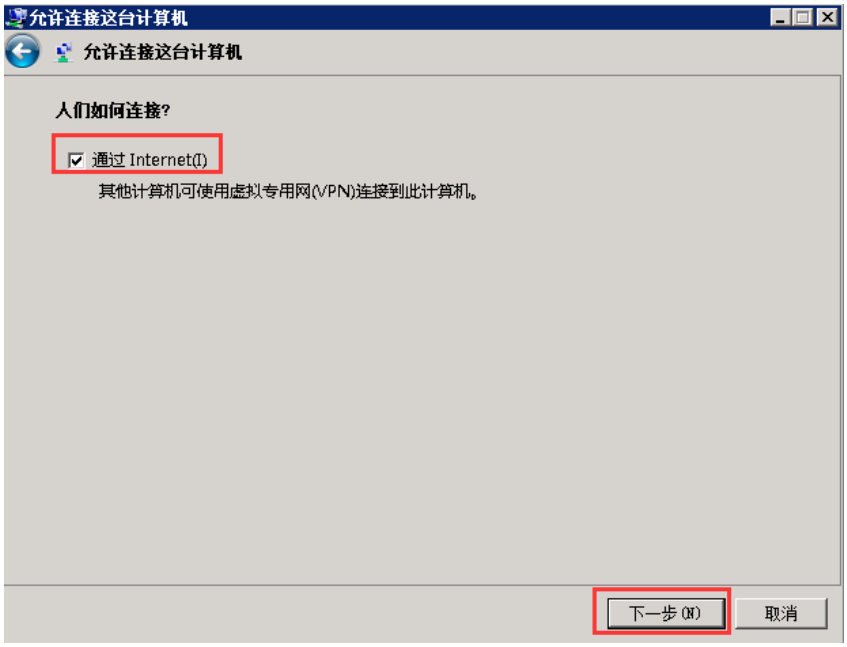


图 49　　PC 连接 VPN 操作二

然后，选择“Internet 协议版本 4”来设置传入 IP 的属性，IP 地址分配选择“指定 IP 地址”，然后选择“确定”以及“允许访问”，设置步骤结束。

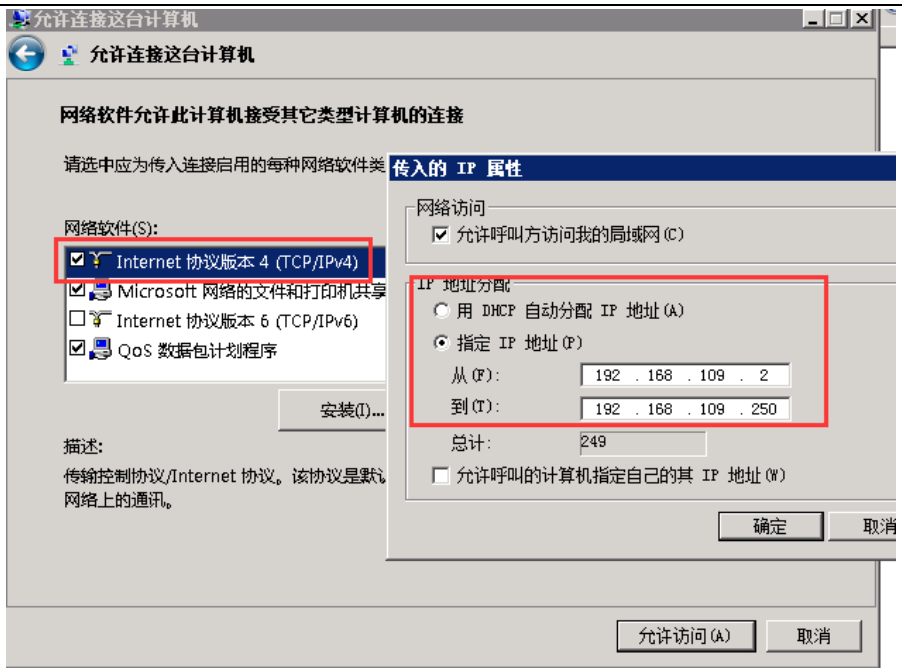


图 50　　PC 连接 VPN 操作三

至此，VPN 服务器端已经设置完毕，我们成功的创建了 VPN Server。

下面来讲述 VPN Client 的使用。我们在局域网内找一台电脑，保证它有能力访问上面的服务器。然后新建一个 VPN 连接，参数如下图

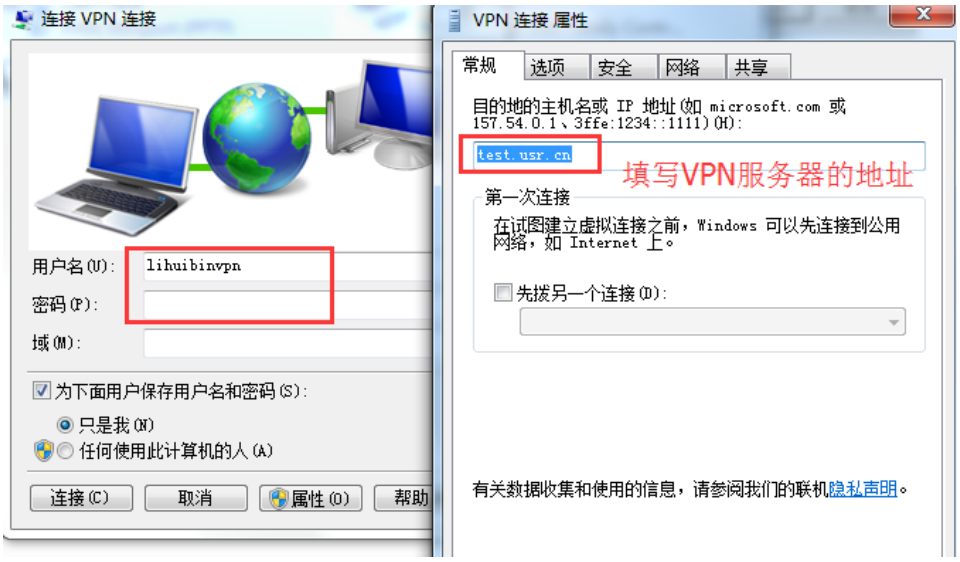


图 51　　PC 连接 VPN 操作四

在连接框中，点击“属性”，选项卡中可以设置目标地址（也就是 vpn 服务器的地址），安全选项中选择“PPTP 协议”，点确定后，输入用户名，密码，

图 52　　PC 连接 VPN 操作五

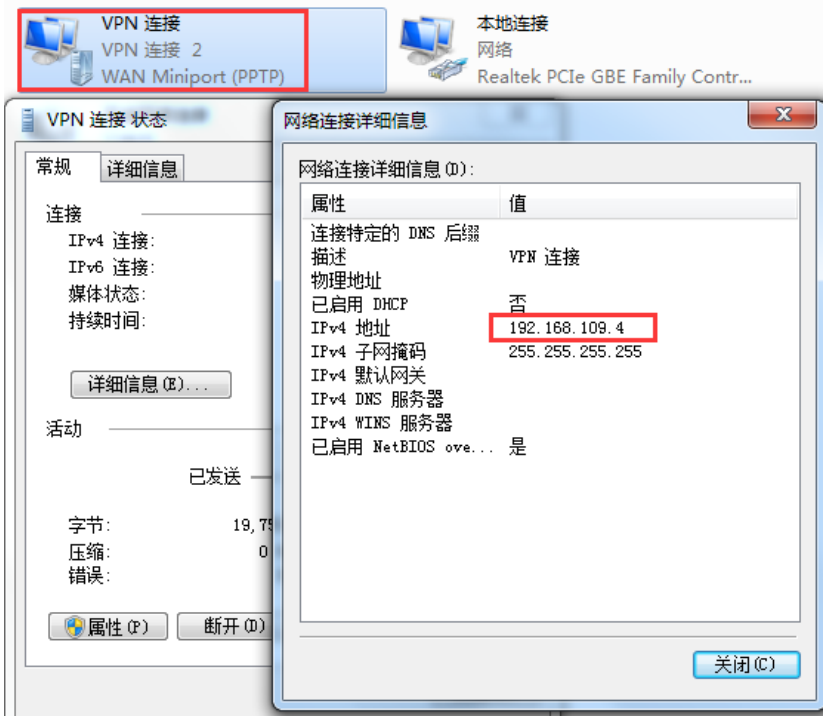


图 53　　PC 连接 VPN 操作六

点击“连接”按钮，连接成功后，可以看到 VPN 的网卡连接，从灰色变成了亮色，代表 VPN 连接已经成功建立。

图 54　　PC 连接 VPN 操作七

上面是服务器上的网卡连接，表明现在已经有 VPN Client 连接上来，我们下面做一个实验，证明在 VPN 网络内，各个 IP 的之间是可以相互访问的（192.168.109.7 为局域网的 VPN 客户端）。

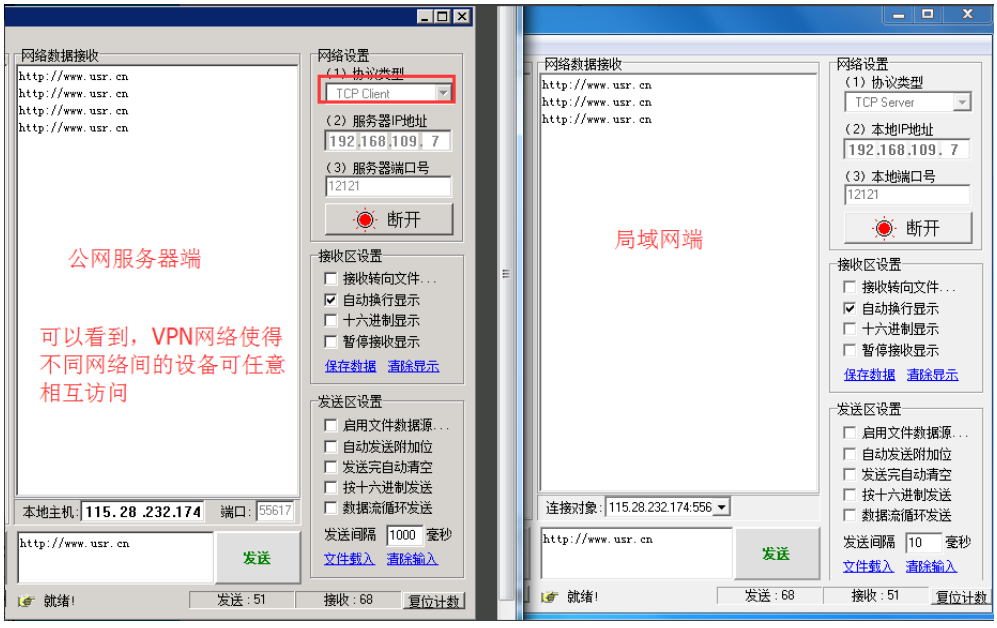


图 55　　VPN 功能测试图

可以看到，在 VPN 网络内，各个网络设备之间点对点直接访问，形成了一个虚拟的，可双向互通的网络。

注意：

VPN 连接有多种属性，如下是两种 PPTP 连接成功后的不同属性，身份验证协议，加密方式等均有不同

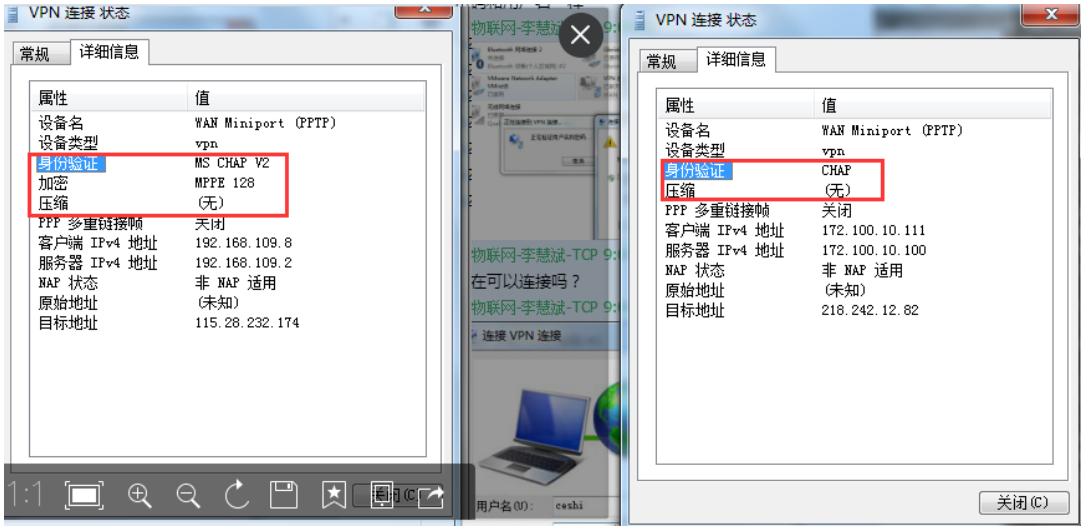


图 56　　VPN 连接状态图

5.1.2. 路由器连接 VPN(基于 PPTP 协议)

下面我们使用路由器上的 PPTP Client 来替换电脑拨号的方式。

首先假设用户已经获取到了 VPN 服务器地址，账户跟密码，那么我们新建一个接口，协议选择 PPTP，其他参数依次写入。

图 57　　路由器添加 VPN 操作图一

图 58　　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

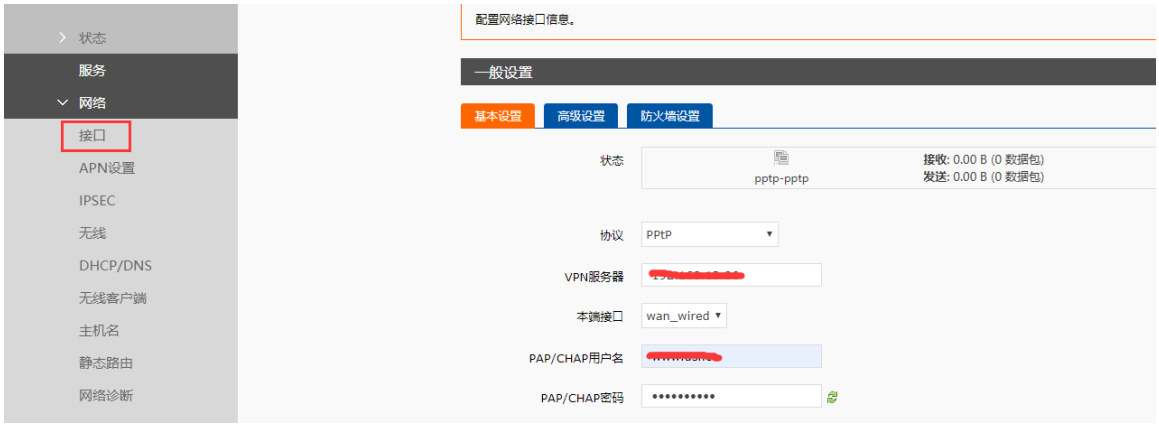


图 59　　路由器添加 VPN 操作图三

本端接口：根据联网方式的不同可选择 wan_4g、wan_wired

用户名：服务器设置的账户

密码：服务器端设置的密码

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 60　　路由器添加 VPN 操作图四

图 61　　路由器添加 VPN 操作图五

<说明>

- VPN 服务器填写服务器 IP/域名。
- 本端接口默认 LAN 口，可根据实际搭建环境选择接口，例如通过有线搭建 VPN 则接口选择 wan_wired
- 服务器搭建好要看一下是否支持仅 MPPE 加密后，可以在客户端高级设置里面选择加密方式。
- 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。
- 当接口页面-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。
- 加密方式：mppe stateful—有状态连接， mppe stateless—无状态连接 ，no mppe—无 mppe 加密
- mppe stateful：会进行频繁更换密钥，且在更换密钥时会出现严重丢包。
- mppe stateless：只有在丢包的时候会进行密钥更改
- no mppe：服务端无 MPPE 加密方式时选择此模式

- 设置静态 IP：空白则是服务端自动分配 IP，可填写静态 IP
- 魔术字：当以上配置不满足配置文件和服务端向匹配时在此添加附加配置，例如服务端 MPPE 认证方式为 only mschapV2，G806 可在魔术字内添加 refuse-eap refuse-chap refuse-pap refuse-mschap 配置

5.2. L2TP Client 搭建

L2TP 是第二层隧道协议，与 PPTP 类似。目前 G806 支持隧道密码认证、CHAP 等多种认证方式，支持 MPPE 的加密方式和 L2TP OVER IPSec 的预共享密钥加密方式。

那么我们新建一个接口，协议选择 L2TP，其他参数依次写入，服务器地址、用户名、密码需要 L2TP Sevser 提供。具体配置说明：在高级设置里面可以在身份认证中选择相应的认证和加密的方式，如下图：

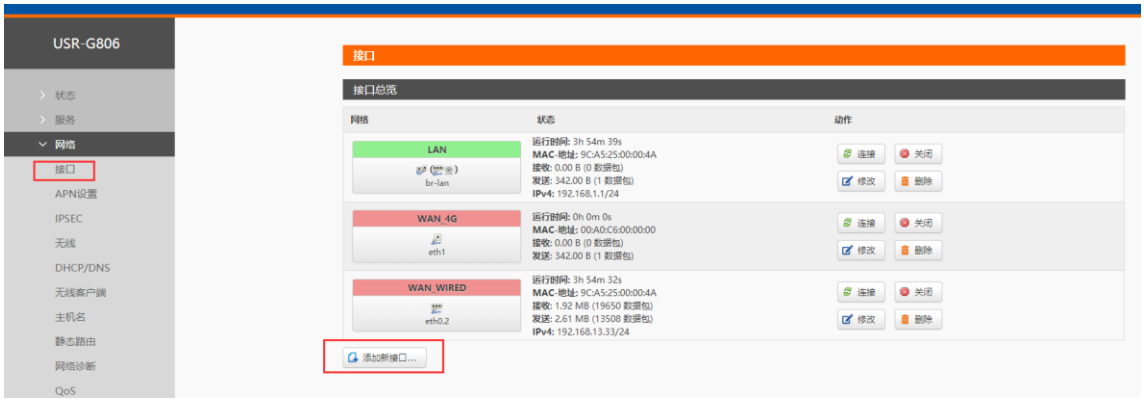


图 62　　创建接口

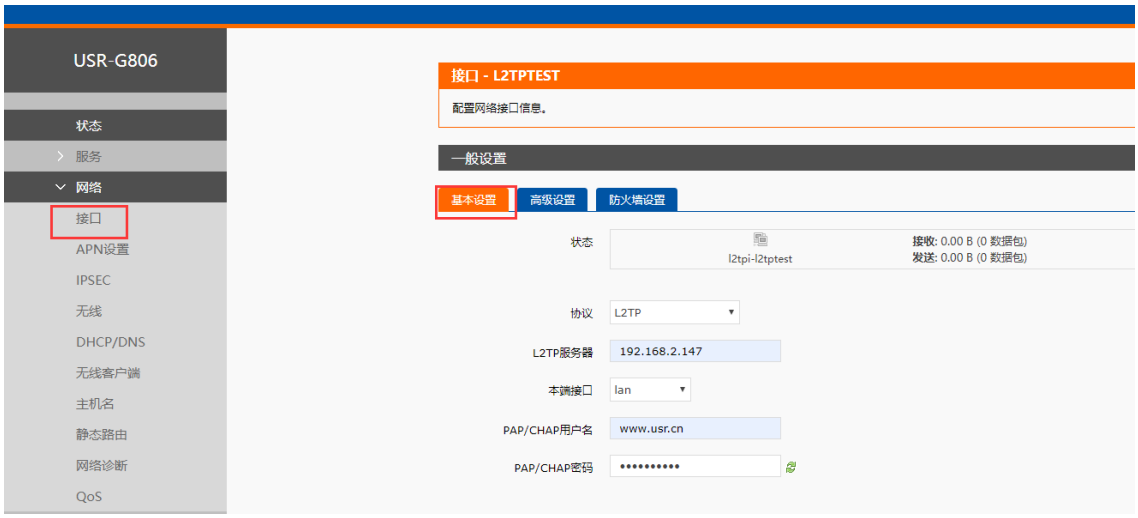


图 63　　配置基本参数

图 64　　L2TP 认证方式选择

图 65　　L2TP 开启隧道密码认证

<说明>

- L2TP 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。
- 增加了可以设置客户端静态 IP 的模式。
- 其他参数建议直接使用默认参数。

5.3. IPSec 搭建

图 66　　IPSec 基本设置

<说明>

- 使能 IPSec：启动 IPSec 功能
- 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，不可使用存数字。
- 本地接口：通过的本端地址，这个可选择 wan_wired、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 67　　IPSec 高级设置

<说明>

- 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。
- 会话秘钥向前加密(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。

注意：

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。

SA类型：ESP						
主模式	ESP加密			野蛮模式	ESP加密	
IKE加密	3DES-SHA1	3DES-MD5		IKE加密	3DES-SHA1	3DES-MD5
3DES-SHA1	pass	pass		3DES-SHA1	pass	pass
3DES-SHA1-DH2	pass	pass		3DES-SHA1-DH2	pass	pass
3DES-SHA1-DH5	pass	pass		3DES-SHA1-DH5	pass	pass
3DES-MD5	pass	pass		3DES-MD5	pass	pass
3DES-MD5-DH2	pass	pass		3DES-MD5-DH2	pass	pass
3DES-MD5-DH5	pass	pass		3DES-MD5-DH5	pass	pass

5.3.1. Road Warrior 模式

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

G806 WAN 口：192.168.13.13

G806 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:~# 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 68　IPSec 测试 1

• 路由器基本配置：

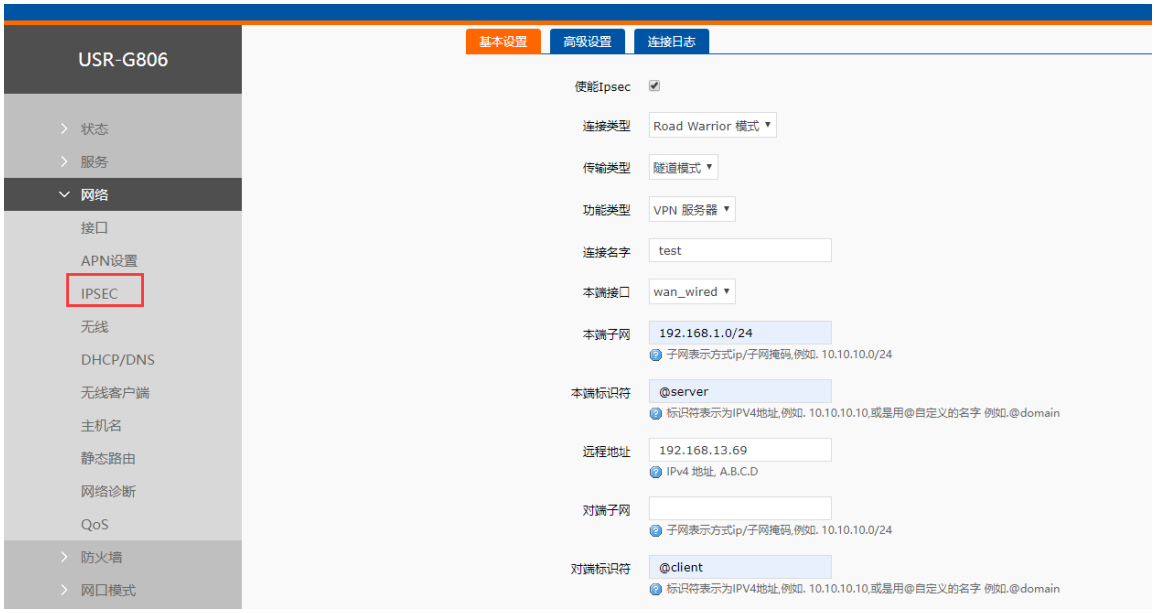


图 69　　IPSec 测试 2

• 路由器 IPSec 高级设置

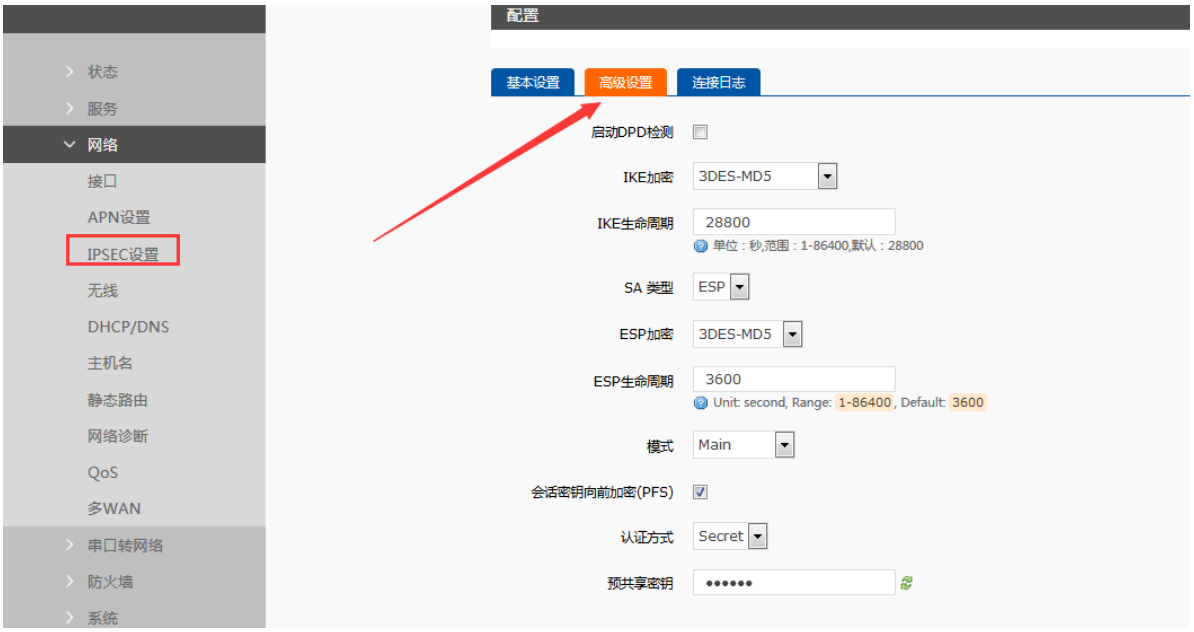


图 70　　IPSec 测试 3

• 在防火墙将 G806 的 WAN 口改为接受

图 71　　IPSec 测试 4

这样 G806 和虚拟机就都配置完成，重启一下 G806，可以用手机连上 G806 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 72　　IPSec 测试 5

5.3.2. Net-to-Net 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。

5.3.2.1. 主模式举例测试：

测试环境：以 1 号 USR-806 作为 IPSec Server，2 号 USR-G806 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-G806（本端）
WAN 口 IP	192.168.13.165	192.168.13.167
LAN 口 IP	192.168.1.1	192.168.20.1
子网下的 PC IP	192.168.1.177	192.168.20.214

2 号 USR-G806 作为 IPSec client，设置界面如下。

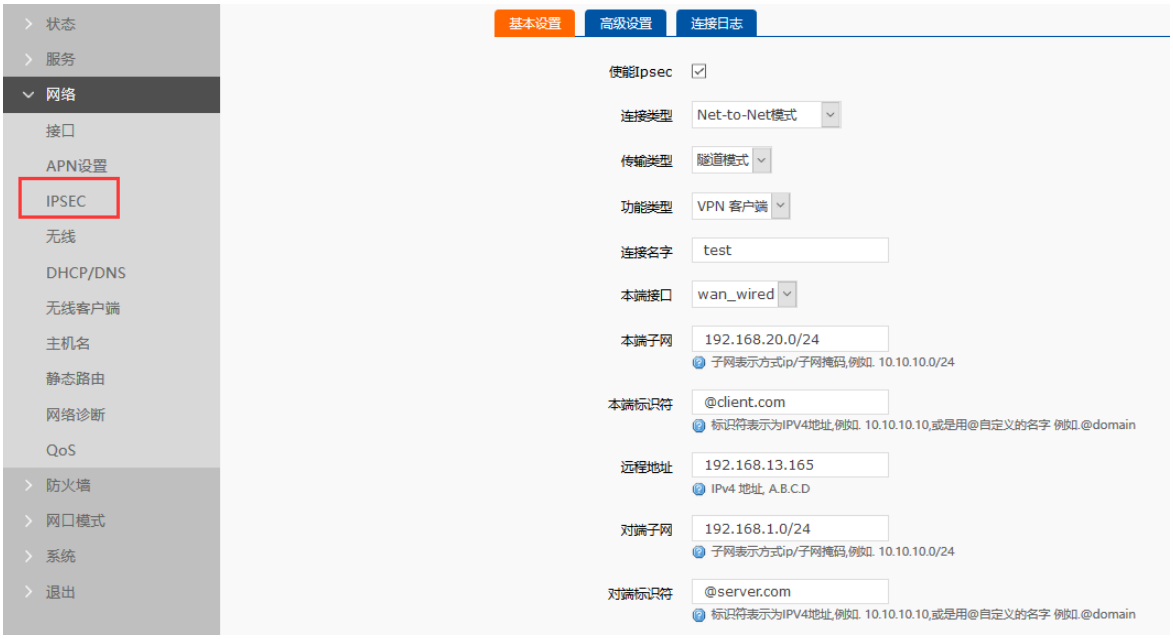


图 73　　IPSec 测试 6

1 号 USB-G806 作为 IPSec server，设置界面如下。

图 74　　IPSec 测试 7

图 75　　IPSec 主模式配置举例

测试结果：

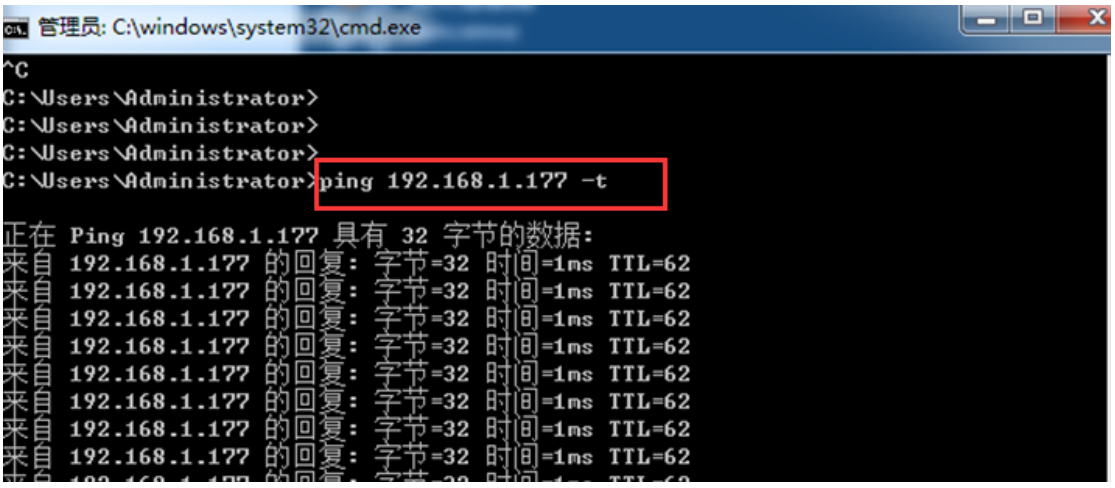


图 76　　G806 下的 pc

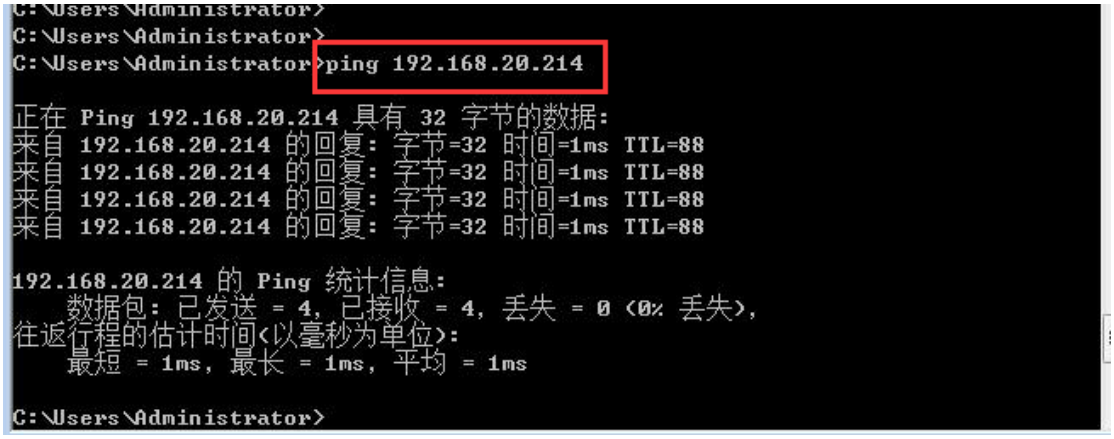


图 77　　另一台 G806 下的 pc

5.3.2.2. h3c 野蛮模式 IPSec server 配置：

1）如图所示点击新建。

图 78　　h3c 配置 1

2）本地网关填写 h3c 的专线地址，设置网线连接的接口 GigabitEthernet0/0，设置共享秘钥，对端 id 类型为 usr，本端 id 类型为 h3c，以上参数要与 G806 一致。

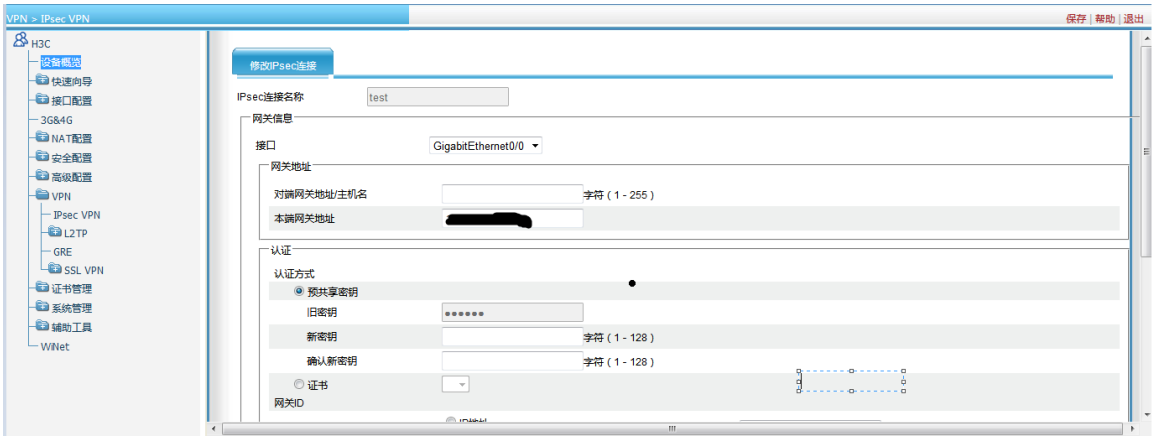


图 79　　h3c 配置 2

3）DH 设置 Diffie-Hellman Group2 与 G806 中 IKE 3DES-MD5-DH2 相对应，选择野蛮模式，其他的按图中所示设置即可。

图 80　　h3c 配置 3

图 81　　h3c 配置 4

4）设置完后，点击右上角的保存。

5.3.2.3. 4G 野蛮模式举例：

对端为 h3c 路由器配置的 server，固定 IP，标识符为@h3c，共享秘钥 123456。

图 82　　4G 野蛮模式配置举例

图 83　　4G 野蛮模式配置举例

- 000 algorithm IKE dh group: id=18, name=OAKLEY_GROUP_MODP8192, bits=8192
- 000 algorithm IKE dh group: id=22, name=OAKLEY_GROUP_DH22, bits=1024
- 000 algorithm IKE dh group: id=23, name=OAKLEY_GROUP_DH23, bits=2048
- 000 algorithm IKE dh group: id=24, name=OAKLEY_GROUP_DH24, bits=2048
- 000
- 000 stats db_ops: {curr_cnt, total_cnt, maxsz} :context={0,2,36} trans={0,2,216} attrs={0,2,288}
- 000
- 000 "test": 192.168.90.0/24===10.5.89.173[@usr]---10.5.89.174...10.5.89.174---[redacted][@h3c]===192.168.10.0/24; erouted; eroute owner: #2
- 000 "test": myip=unset; hisip=unset;
- 000 "test": ike_life: 3600s; ipsec_life: 28800s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
- 000 "test": policy: PSK+ENCRYPT+TUNNEL+UP+AGGRESSIVE+IKEv2ALLOW+SAREFTRACK; prio: 24,24; interface: eth1; kind=CK_PERMANENT
- 000 "test": dpd: action:restart_by_peer; delay:30; timeout:120;
- 000 "test": newest ISAKMP SA: #1; newest IPsec SA: #2; eroute owner: #2;
- 000 "test": IKE algorithms wanted: 3DES_CBC(5)_000-MD5(1)_000-MODP1024(2); flags=-strict
- 000 "test": IKE algorithms found: 3DES_CBC(5)_192-MD5(1)_128-MODP1024(2)
- 000 "test": IKE algorithm newest: 3DES_CBC_192-MD5-MODP1024
- 000 "test": ESP algorithms wanted: 3DES(3)_000-MD5(1)_000; flags=-strict
- 000 "test": ESP algorithms loaded: 3DES(3)_192-MD5(1)_128
- 000 "test": ESP algorithm newest: 3DES_000-HMAC_MD5; pfsgroup=<N/A>
- 000
- 000 #2: "test":4500 IKEv1.0 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 27623s; newest IPSEC; eroute owner; isakmp#1; idle; import:admin initiate
- 000 #2: "test" esp.fbd05857@[redacted]esp.289a4077@10.5.89.173 tun.0@[redacted]tun.0@10.5.89.173 ref=0 refhim=4294901761
- 000 #1: "test":4500 IKEv1.0 STATE_AGGR_I2 (sent AI2, ISAKMP SA established); EVENT_SA_REPLACE in 2417s; newest ISAKMP; lastdpd=30s(seq in:22196 out:0); idle; import:admin initiate

图 84　　隧道建立成功

同上，建立成功后，可以 ping 通各自局域网的 pc。

5.4. OpenVPN 搭建

- 创建接口，可选 TUN(路由模式)或 TAP(网桥模式)：

图 85　　创建接口

图 86　　创建 OpenVPN 接口

• 基本设置配置参数解释：

图 87　　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。

• 高级设置配置参数解释：

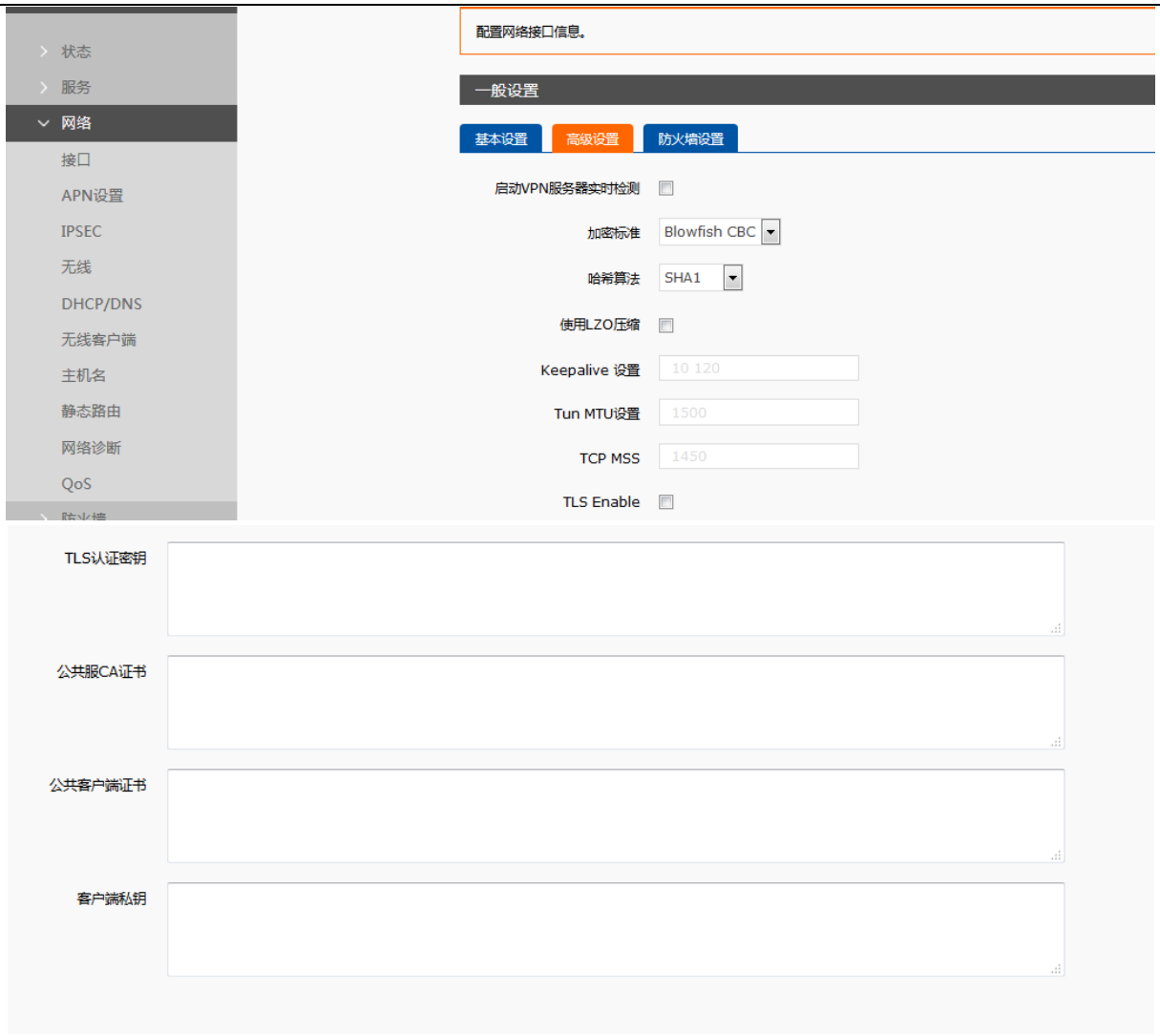


图 88　　OpenVPN 高级设置

- 启用 VPN 服务器实时检测：可以保证 vpn 在异常断开下进行重连。
- 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。
- 哈希算法：SHA1、SHA256、SHA512、MD5
- 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 Enable：是否启用带 TLS 的方式。如不启用，TLS 认证密钥则不需要填写。
- 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

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复制到配置界面对应的编辑框中即可。

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 89　　linux 下 OpenVPN 服务端配置

5.5. GRE 搭建

创建接口

图 90　　创建接口

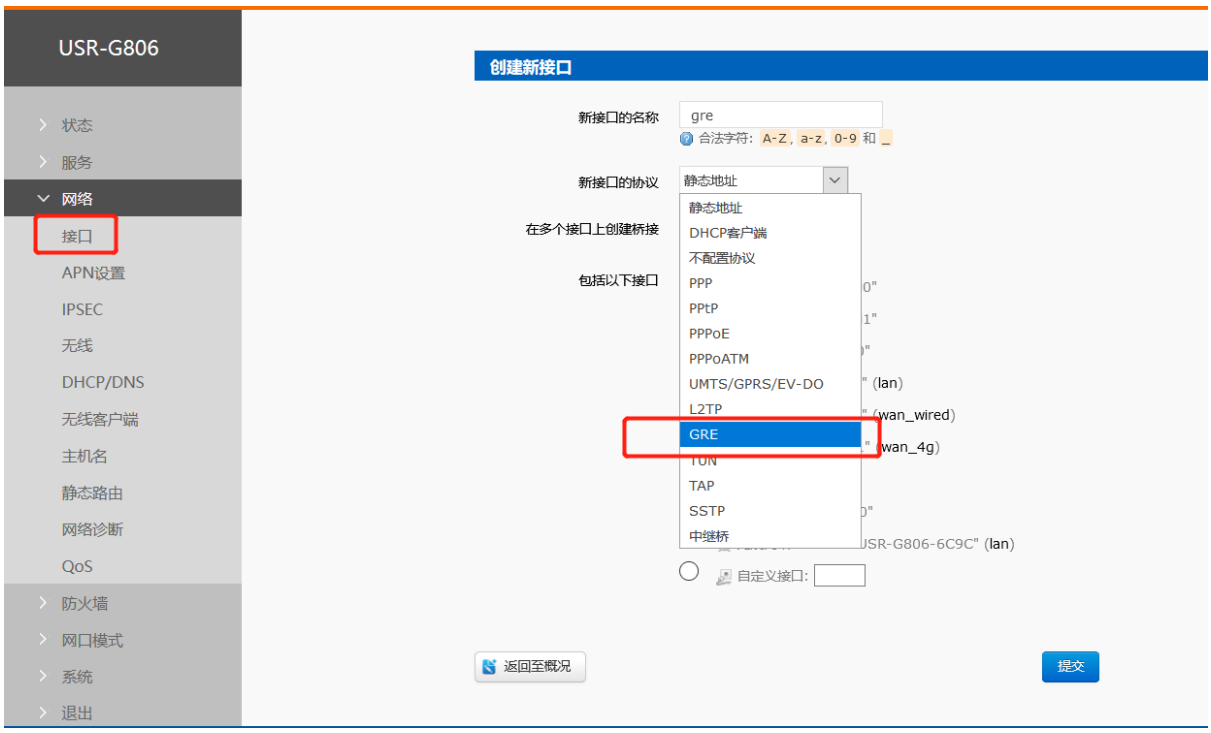


图 91　　创建 GRE 接口

• 基本设置参数解释：

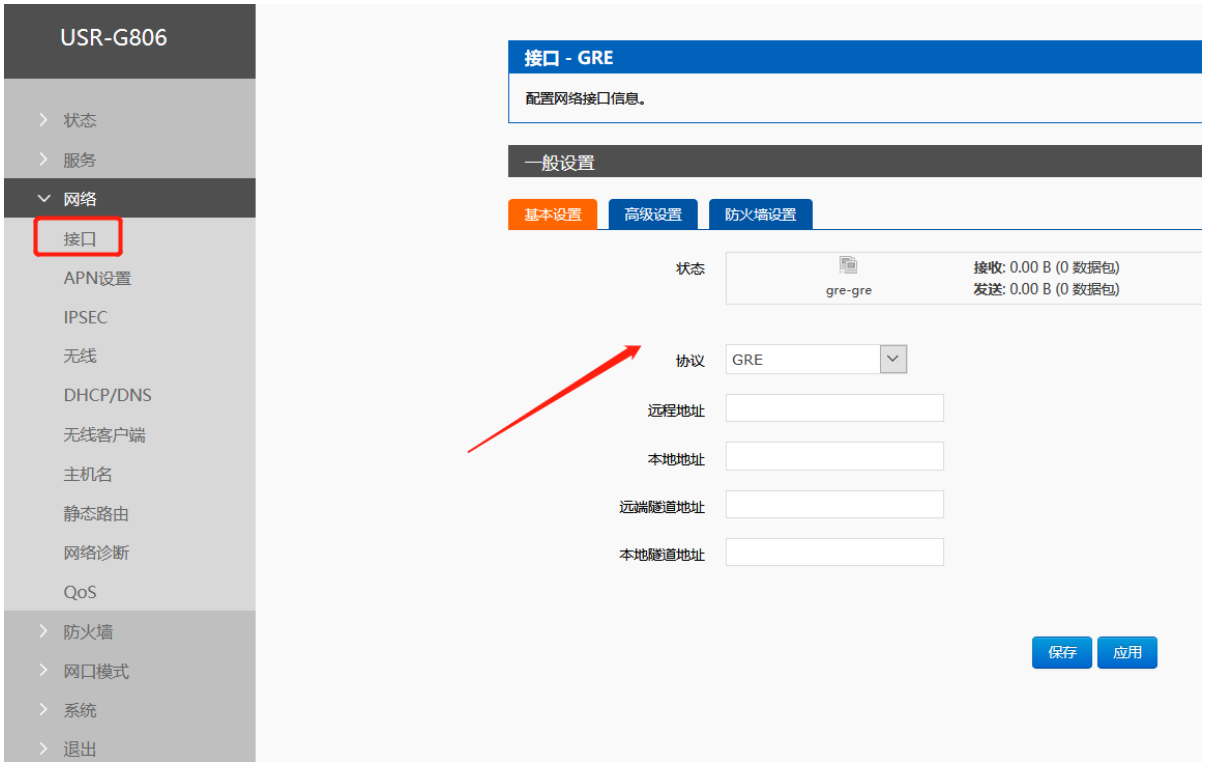


图 92　　GRE 基本配置

- 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，两者根据联网方式不同输入。

➢ 远端隧道地址：对端的 GRE 隧道 IP，对于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

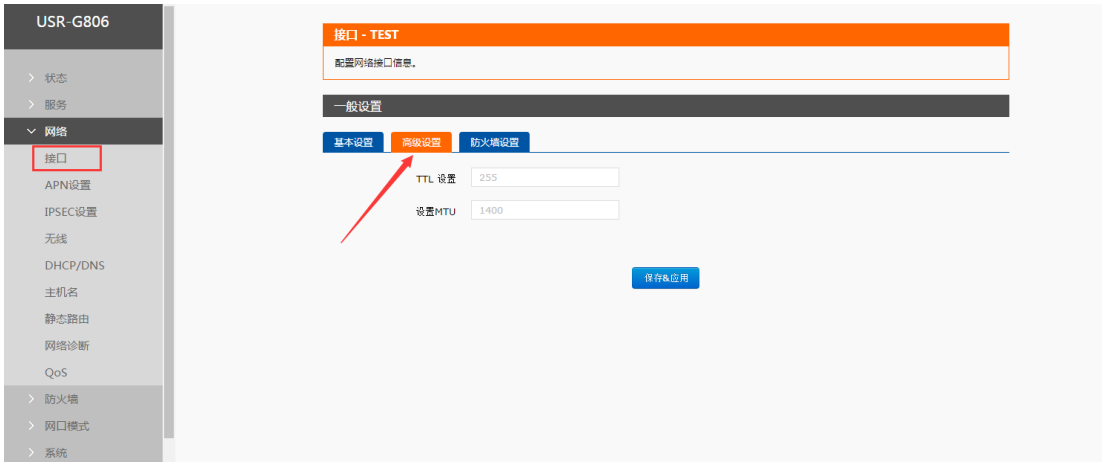


图 93 GRE 高级配置

➢ 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。本项需和 VPN 服务器保持一致。

• 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

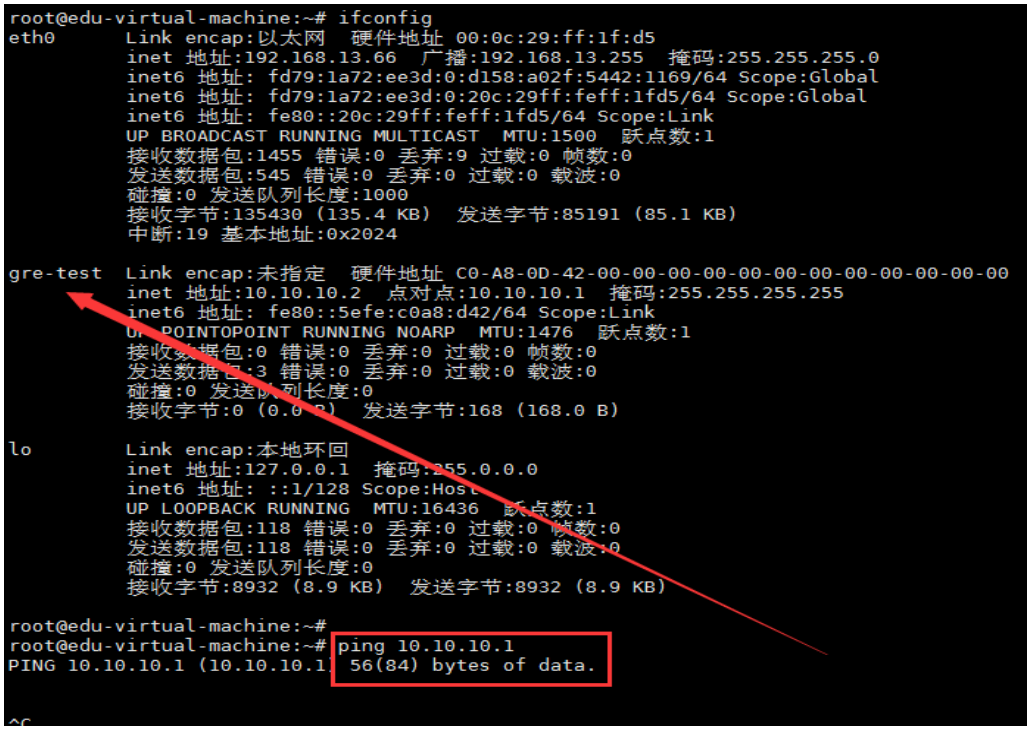


图 94 GRE 测试 1

2、服务器搭建好之后，在 G806 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 95 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 96　　GRE 测试 3

5.6. SSTP Client 搭建

创建 SSTP VPN 接口

图 97　　SSTP VPN 接口创建

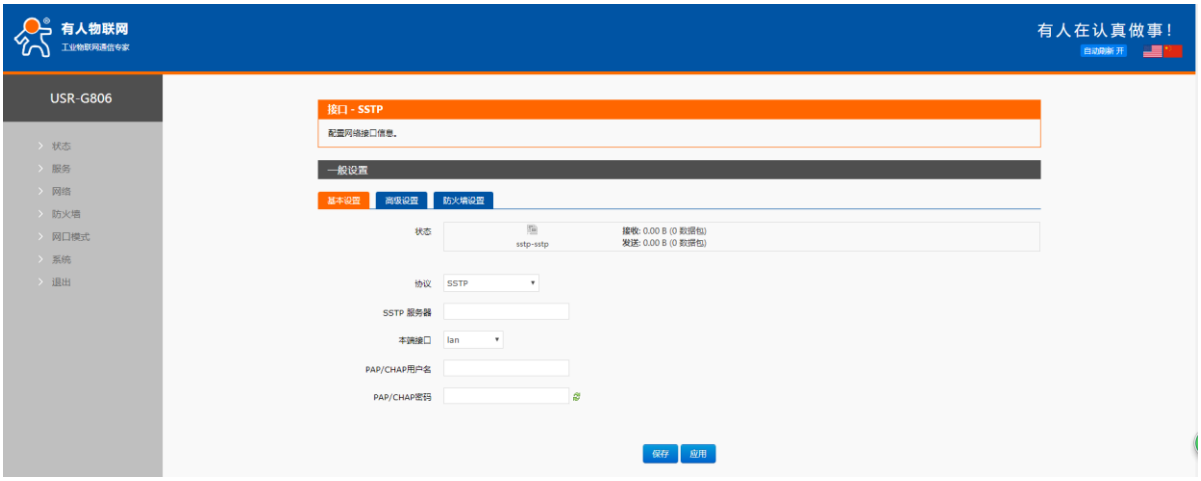


图 98　SSTP 基本设置

- SSTP 服务器：SSTP 服务器的 IP 或域名
- 本端接口：可根据上网方式选择 wan_wired/wan_4g
- PAP/CHAP 用户名：SSTP 的用户名
- PAP/CHAP 密码：SSTP 的密码

注意：

高级设置可参考 PPTP 的高级设置。

5.7. 静态路由

静态路由有如下几个参数

表 12　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，

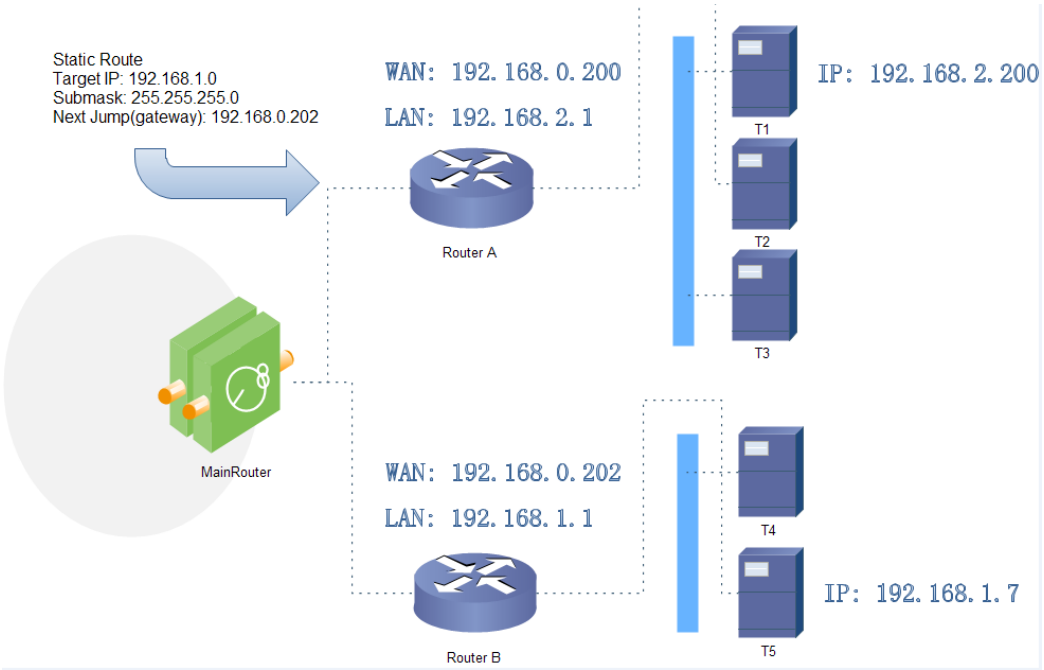


图 99　静态路由表实例图

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

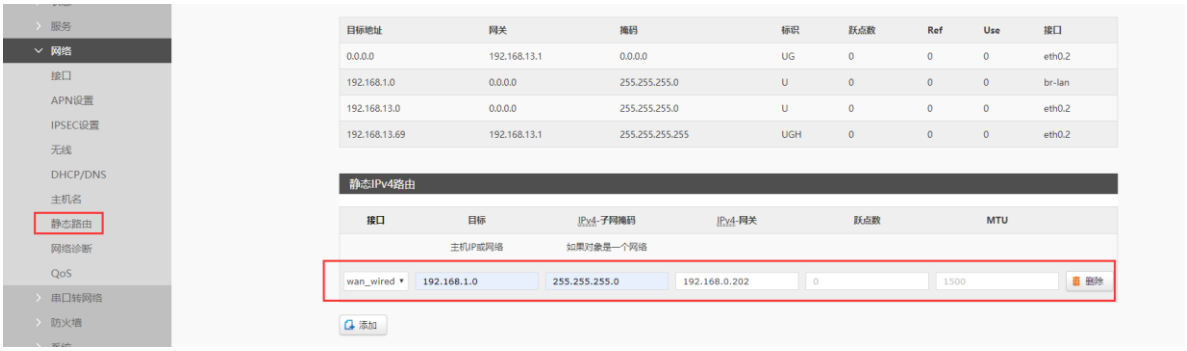


图 100　路由表添加页面

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），

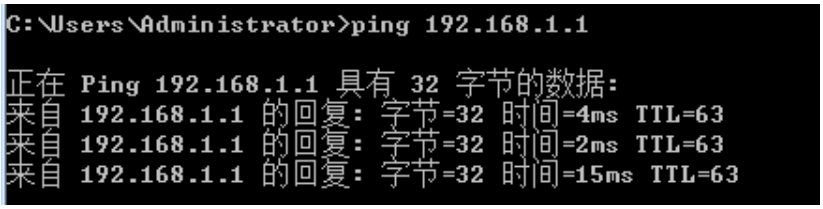


图 101　路由表功能测试

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-G806 的设置，后者为 TP-Link）。

图 102　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）。

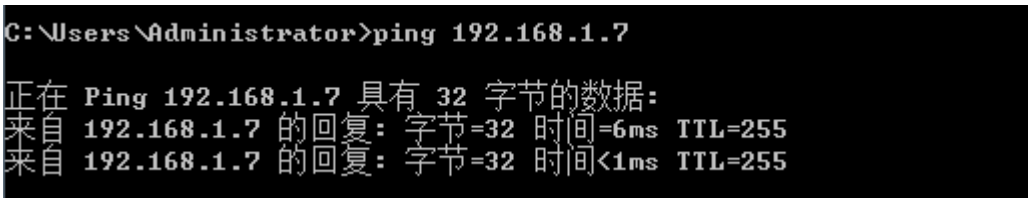


图 103　路由表功能测试二

6. 防火墙功能

6.1. 基本设置

默认两条防火墙规则。

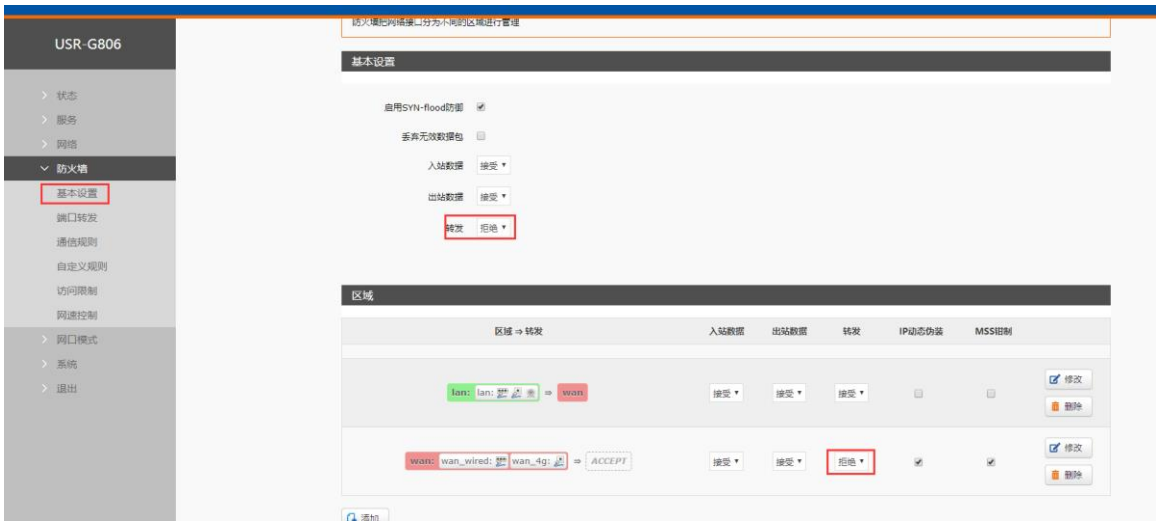


图 104　防火墙设置界面

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 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

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

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：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）。

图 105　防火墙设置页面二

6.2. NAT 功能

6.2.1. 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。

IP 地址伪装设置位于“防火墙-基本设置”界面。

图 106　IP 地址伪装设置

6.2.2. 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，将离开路由器的数据包的源 IP 地址固定成一个特定 IP 向外发送。使用时首先将 wan 口的 IP 动态伪装关闭。

图 107　SNAT 设置 1

然后设置 Source NAT，将离开路由器的数据包的源 IP 地址修改为固定 IP，位于“防火墙-通信规则”下。将源 IP 地址固定修改为 192.168.9.1，其设置界面如下。

图 108　SNAT 设置 2

点击添加并编辑

图 109　SNAT 设置 3

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 110　SNAT 设置 4

如图将离开路由器的数据包的源 IP 地址改变为 192.168.9.1，

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

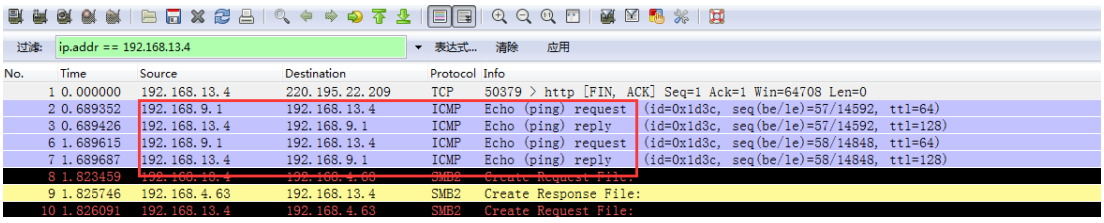


图 111　NET 验证

如同可以看到，到 192.168.13.4 的 IPCMP 包的源地址是 192.168.9.1，而不是 192.168.1.114.

6.2.3. 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 112　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 113　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。

上面的设置，192.168.1.1:80 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 192.168.1.1，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 192.168.1.1:80 上面。

6.2.4. 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，即可，

图 114　DMZ 设置一

点击添加然后保存

图 115　DMZ 设置二

如图，WAN 口地址的所有端口都映射到内网 192.168.1.100 这台主机上。

注意：端口映射和 DMZ 功能不能同时使用

6.3. 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。

6.3.1. 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”

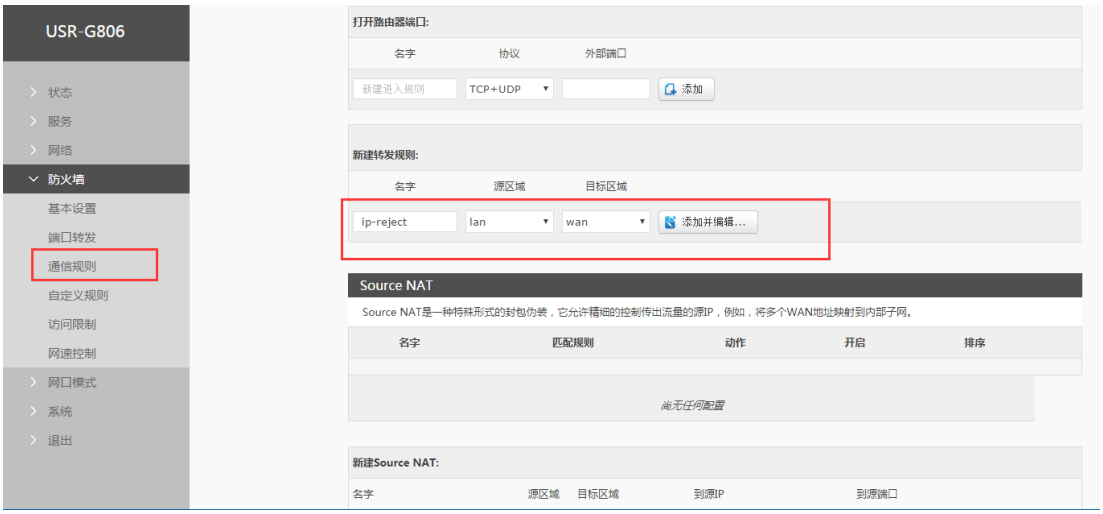


图 116　防火墙 IP 黑名单图一

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 117　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 118　防火墙 IP 黑名单设置图三

图 119　防火墙黑名单设置图四

这样设置完成后，就实现了黑名单的功能。

6.3.2. 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 120　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 121　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 122　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 123　防火墙 IP 白名单图三

6.3.3. 拒绝某子网设备访问某指定 IP

首先添加一条转发规则

图 124　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。
- 协议选择 All protocols，则为指定源 IP 无法 ping 通指定目标 IP,无法建立 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（或不可访问指定目标 IP 的某端口口），协议不可选择 All protocols 或者 ICMP。

此例子选择 TCP 协议

图 125　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 48:95:07:AB:58:7B 的设备的 8899 端口（端口不填即为默认所有端口）

禁止与目的地址为 192.168.0.166 端口为 9999（端口不填即为默认所有端口）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 48:95:07:AB:58:7B 的设备与目的地址为 192.168.0.166 建立 TCP 连接。

图 126　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。

图 127　防火墙设置四

6.3.4. 禁 Ping 功能

首先添加一条转发规则。

图 128　防火墙设置一

协议选择 ICMP。

图 129　防火墙设置二

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 192.168.1.133 到目的地址为 192.168.0.100 的设备 ping 动作。

图 130　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，将右边对勾去掉后点击应用即可，再次使用时将对勾勾线后点击应用即可。

图 131　防火墙设置四

禁 ping 功能生效。

图 132　防火墙设置五

6.4. 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。

6.5. 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。

6.5.1. 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。

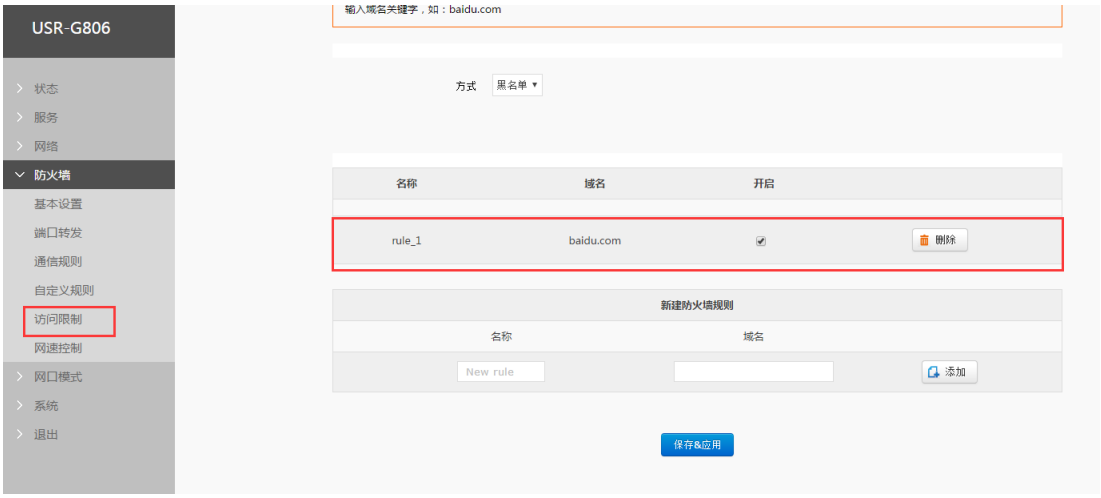


图 133　域名黑名单

6.5.2. 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。

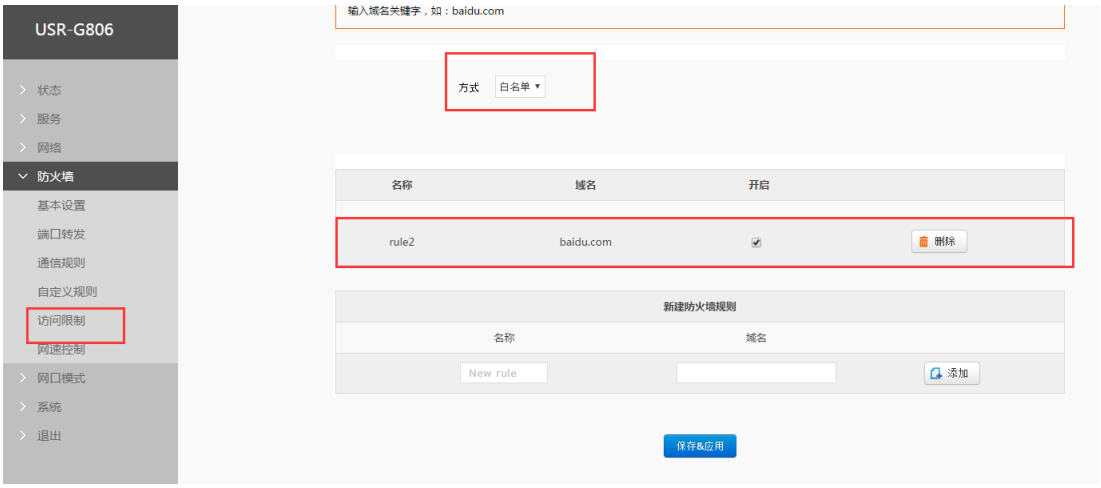


图 134　域名白名单

6.6. 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 135　网速控制

参数列表：

表 13　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 字节每秒
MAC	限速的 MAC	设备 mac 地址

7. 高级服务功能

7.1. 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，点击保存，页面会显示 SN 码和服务设备状态

图 136 花生壳内网穿透启动前

图 137 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。

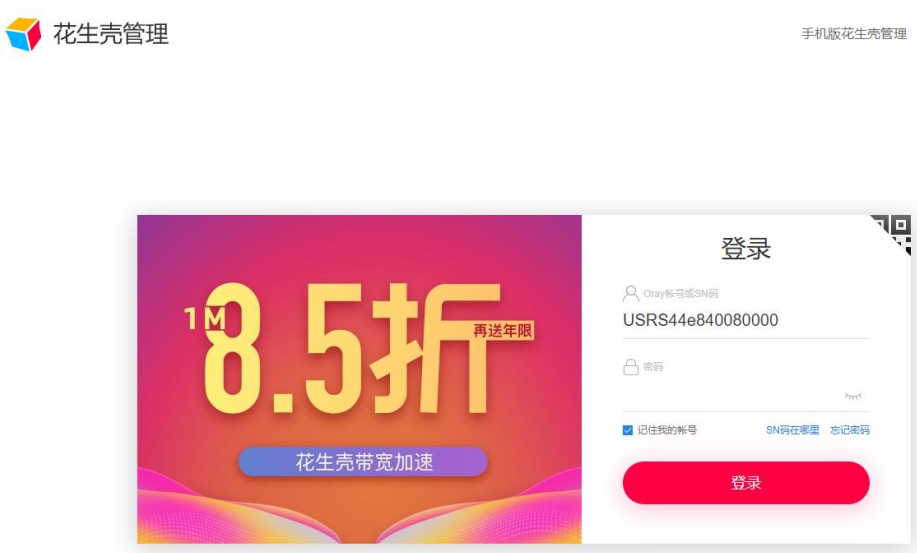


图 138　花生壳内网穿透 SN 码登陆

3、初次登录需要绑定，微信扫描激活。

图 139　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

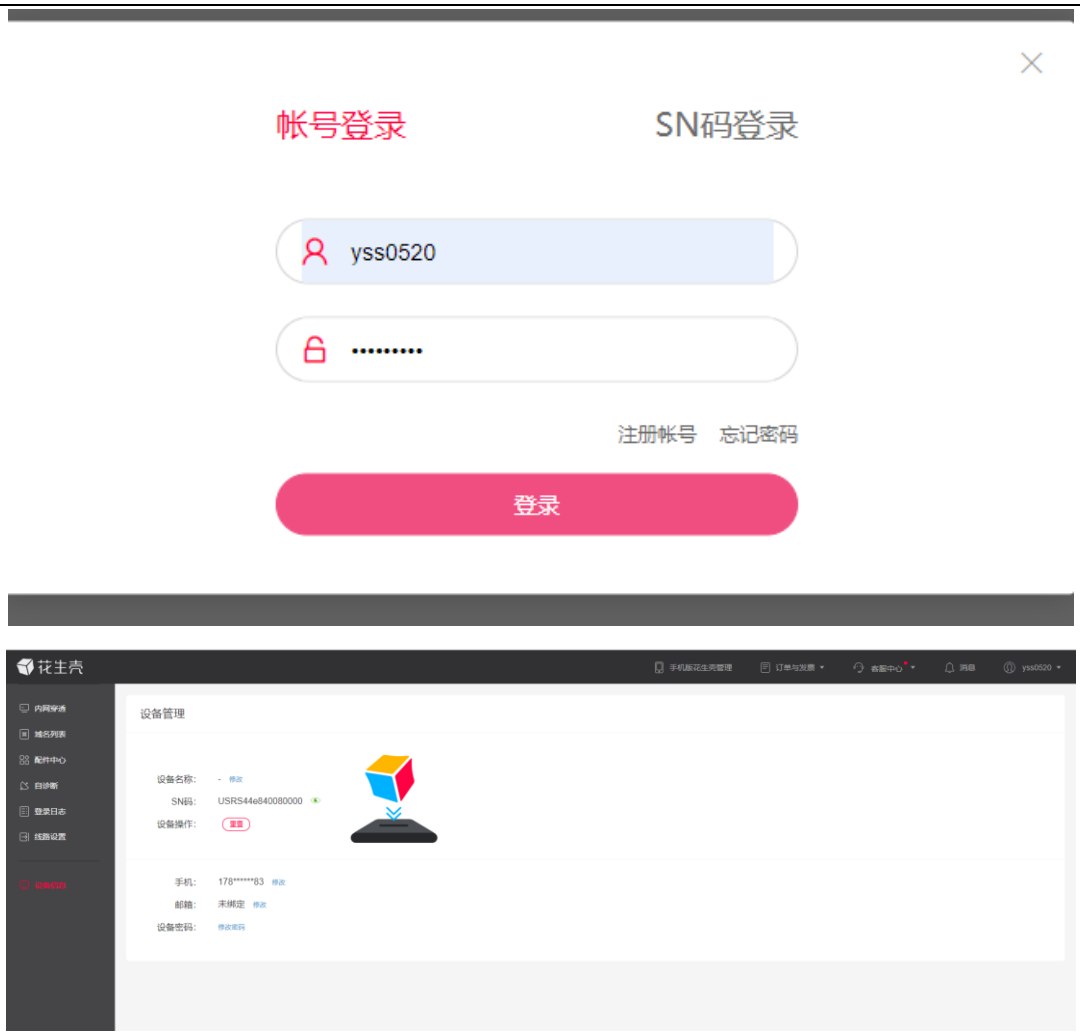


图 140　花生壳内网穿透切换账号

5、切换到账号登录点击左侧的内网穿透

图 141　花生壳内网穿透设置

6、点击“+”号添加映射

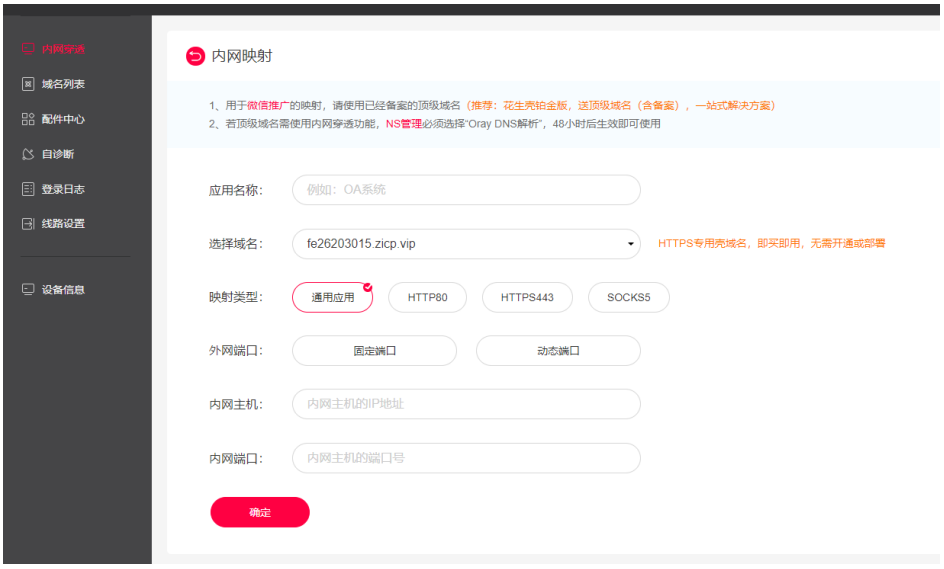


图 142　花生壳内网穿透设置

7、设置映射

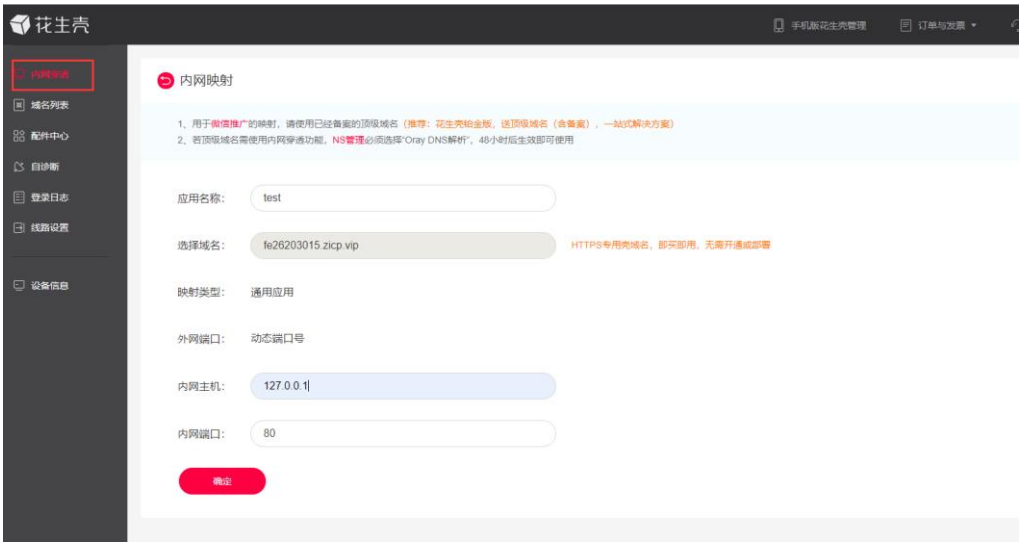


图 143　花生壳内网穿透设置

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 14　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

8、测试域名

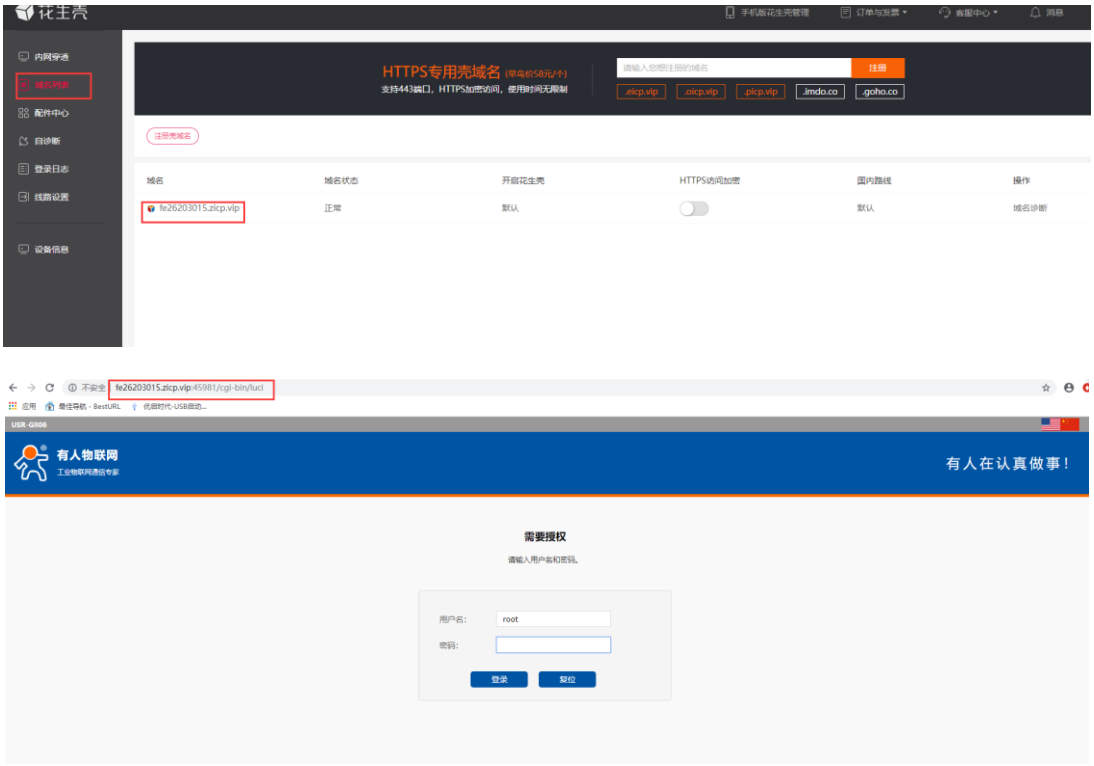


图 144　花生壳内网穿透域名测试

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。

7.2. 动态域名解析（DDNS）

7.2.1. 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 145　DDNS 设置页面

参数填写要求如下，

表 15　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，

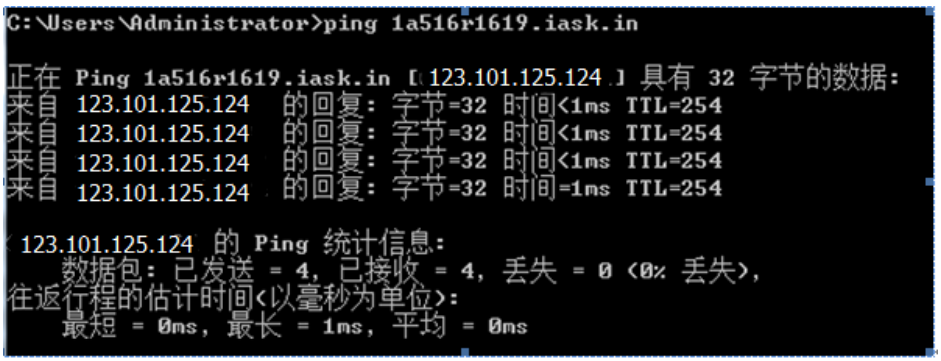


图 146　DDNS 测试图

7.2.2. 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 147　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 16　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 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 148　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。

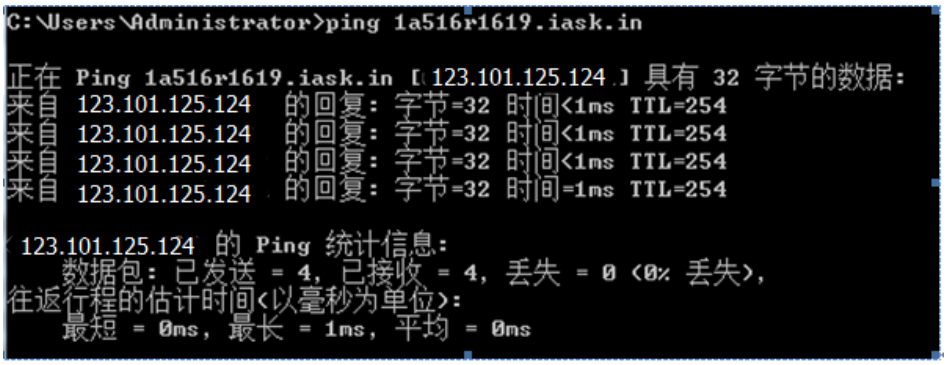


图 149　DDNS 测试图三

7.2.3. 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

7.3. 强制门户（WiFidog）

强制门户功能（WiFiDog），可以将接入路由器网络的设备，在首次浏览外网网页时，首先登录一个认证页面，只有当认证成功后，才可以访问外网。

强制门户功能的意义，一个在于局域网网络的安全，记录使用公共网络进行网络攻击等非法行为；另外，

也可以用于广告用途，它在经过当前宽带使用者的默许下，收集客户信息，方便厂家进行营销推广。

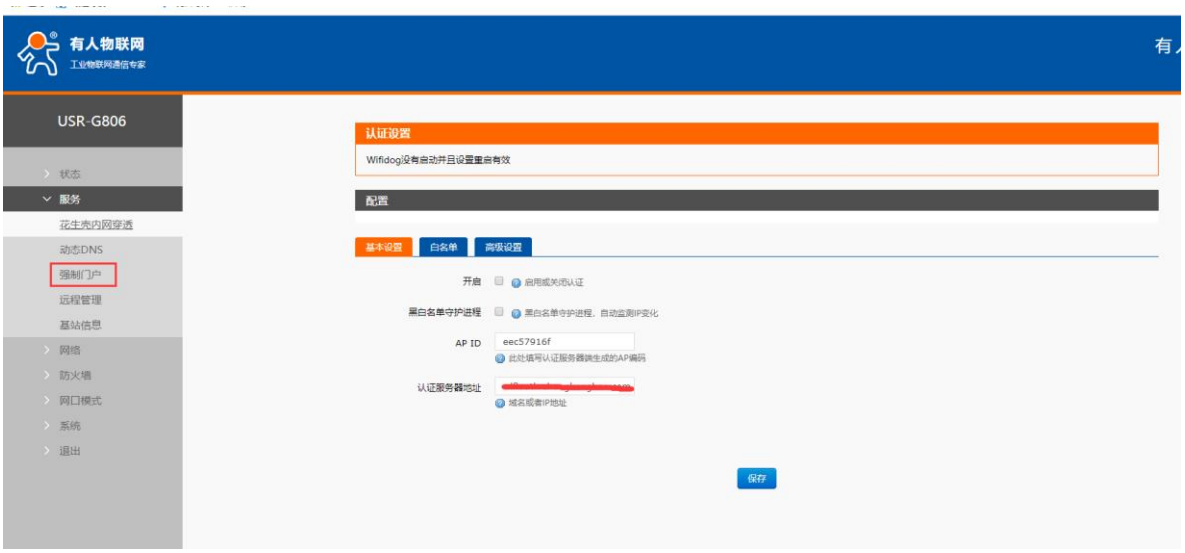


图 150　WiFiDOG 设置页面

如上为参数设置界面，启用认证选项默认不勾选，这样每个客户在收到产品后，都可以正常使用常规的路由功能；当此选项勾选后，将会启用强制门户认证，如下，

图 151　WiFiDOG 设置页面二

其中有几个关键参数，要求如下，

表 17　WiFiDOG 参数表

功能	参数设置（如果要使用）	备注
启用认证	勾选	如果使用请勾选
守护进程	勾选	如果使用请勾选
AP 编码	nfuoId700	AP 编码
认证服务器地址	www.xxx.cn（举例）	协助认证的服务器地址
内网接口	br-lan	LAN 口名称
外网接口	eth0.2	有线 WAN 口名称（如果您想经由 4G 上网，请填写 eth1）
认证服务器路径	/apps/WiFiguanjia/	认证服务器上的路径

然后我们打开浏览器，随便输入一个网址，可出现认证界面，需要输入手机号才可以进入（示例）。

图 152　WiFiDOG 登陆页面

可以配合服务器实现短信验证登录，微信以及 QQ 登录功能，当然需要定做服务器软件。

注意

- 本路由器的强制门户功能为演示示例，如果您要正式使用，需要配合服务器定制
- 定制申请-济南有人物联网技术有限公司官网：
  http://www.usr.cn/Custom/index.html
- 如果您不打算用这个功能，请解除勾选，否则会导致在路由器下无法访问外网（认证后才可以）
  实际的应用效果如下

图 153　WiFiDOG 认证页面

输入手机号，然后点“发送”按钮，来获取验证码。

图 154　WiFiDOG 认证页面二

获取到验证码之后，请输入并提交认证，

图 155　WiFiDOG 认证页面三

认证通过！

注意，每个访客（通过特定接口访问的）都需要经过认证之后才可以访问外网。

7.4. 远程管理

7.4.1. 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，将远程平台注册码填入 mac 或 imei 输入框中，其它选根据需要选择，然后点击添加

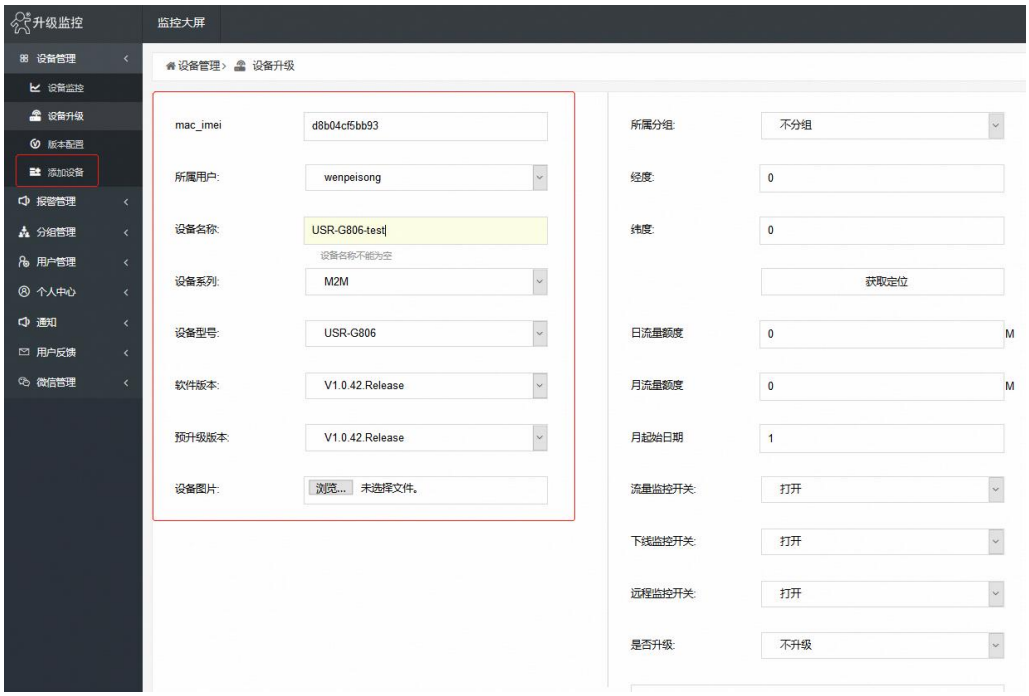


图 156　设备注册

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。

详细 AT 指令可参见《AT 指令集》。

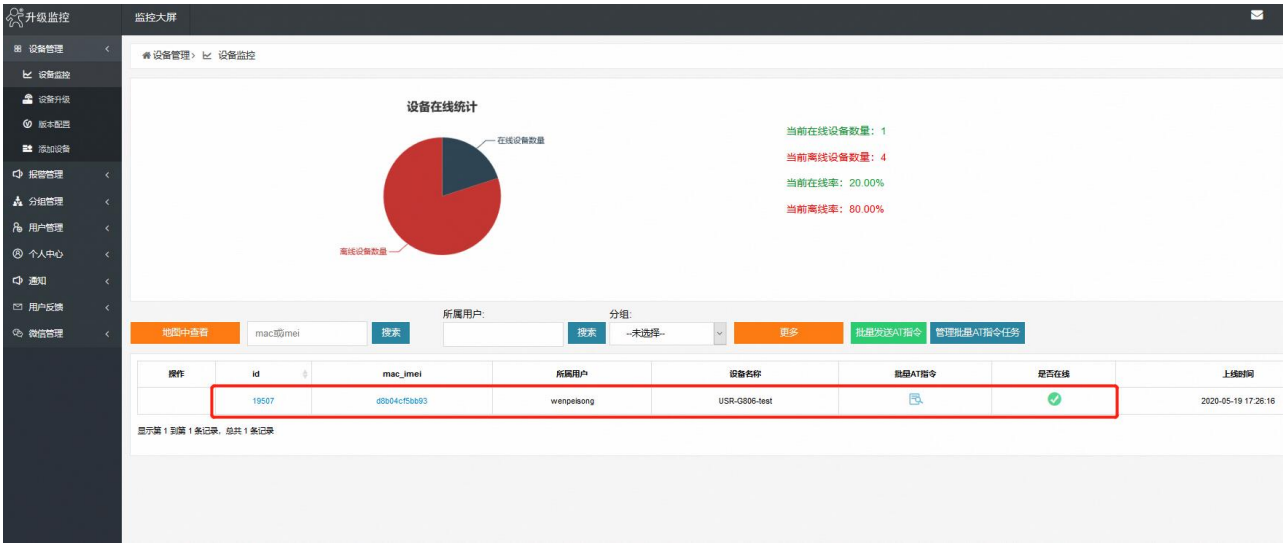


图 157　设备监控一

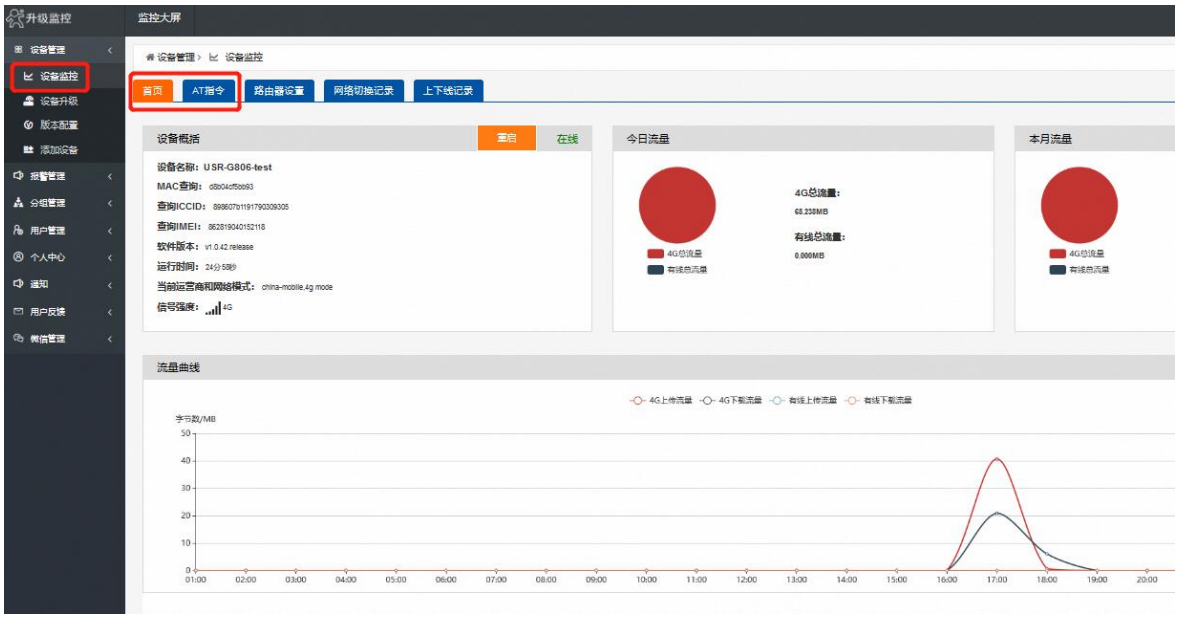


图 158　设备监控二

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。

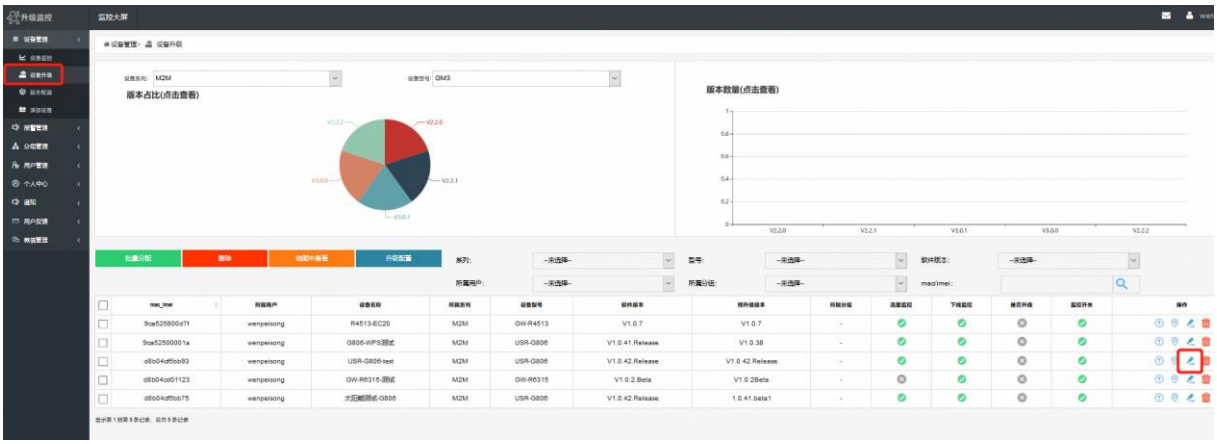


图 159　设备升级一

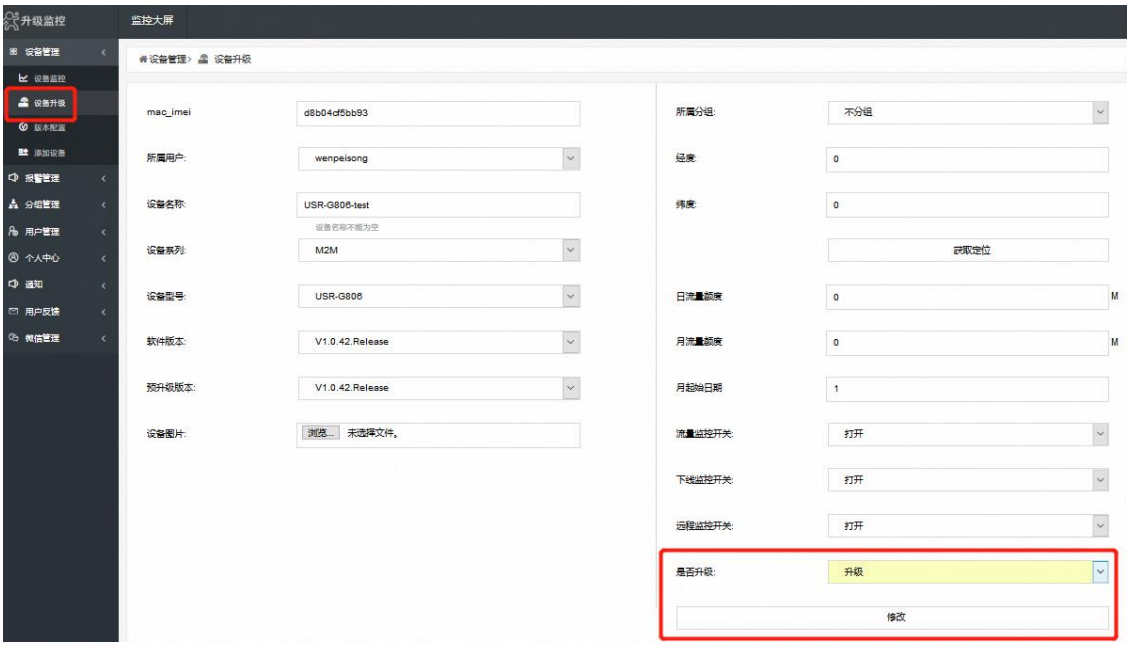


图 160　设备升级二

<说明>

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。

7.4.2. 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。

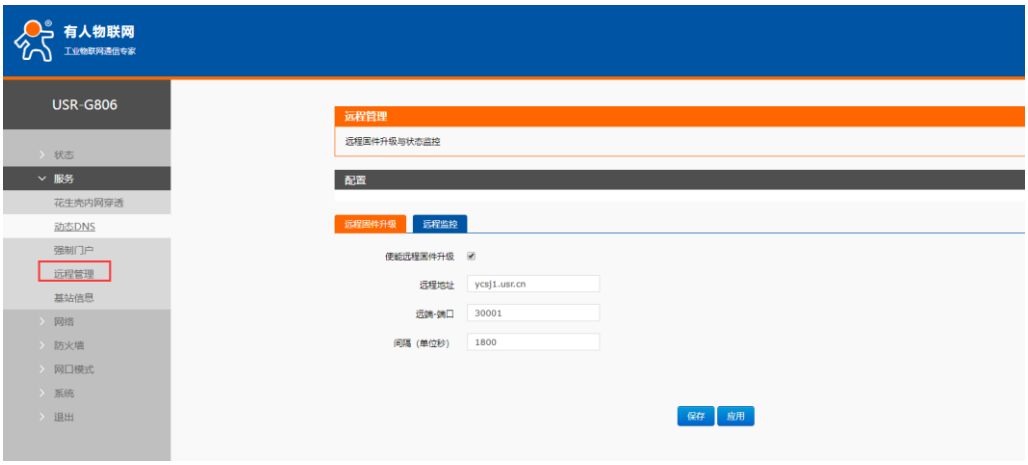


图 161　远程升级

参数列表：

表 18　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；
- 多只路由器组合使用时，需要升级为同一版本最新固件；

7.4.3. 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 162　远程监控

参数列表：

表 19　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

注意：详细的远程监控和远程升级的使用，请登陆 ycsj1.usr.cn

8. 常见组网应用

8.1. WAN+LAN+4G 组网

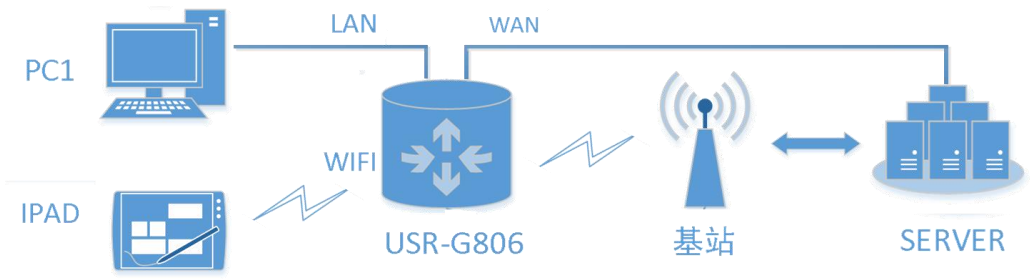


图 163　WAN 口加 4G 组网示意图

该组网方式同时拥有两个可以连接到广域网的接口(以太网口的 WAN 口和 M2M 网络的 4G 口),两路通道形成互补及备份。以太网口的 WAN 口优先，保证数据的流畅，当 WAN 口出现异常时，路由器可以通过 4G 连通服务器。从而保证了数据的完整、可靠、稳定。

本组网方式最大程度的减少了客户的设置过程，路由器自带的 WiFi 的功能也可以同时工作，最大程度的增加用户的局域网的接入数量。主要应用在对网络的稳定性要求高；布网时，现场环境中已有可以连接广域网的网线；并且要求数据有备份线路的场合。已经在工厂厂房、智能楼宇、智慧城市等相关行业广泛应用。

8.2. 双 LAN+4G 组网

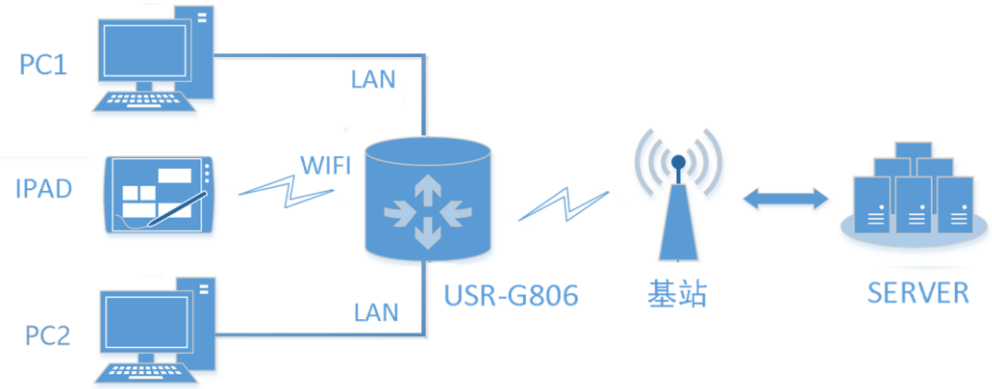


图 164　双 LAN 口加 4G 组网示意图

本组网方式，将两个网口都设成 LAN 口，这样局域网内的可以尽量多的接入网口设备同时使用 4G 网络又省去了网线布线的繁琐，是工程中架设网络的最方便高效的途径，节省了网线布线的材料成本和人力成本。

本方式进行组网网时只需要进行一步设置即可达到该组网的要求，只需要在内置网页中将网口的 WAN 口工作模式改成 LAN 口，具体页面请参照下图。

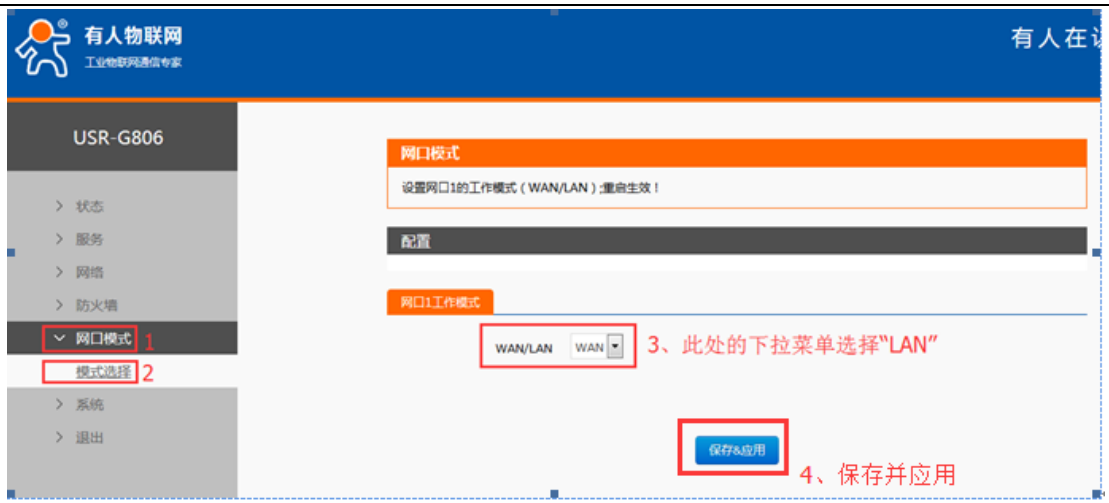


图 165　网口模式修改页面

本组网方式适合于无法布设网线连接广域网的场合，仅通过 4G 进行与广域网服务器的通信，由于仅使用 4G 网络，所以购买 4G 网络套餐时请适当增加流量防止流量超出，造成不必要的后期维护。主要应用于智能公交、农业物联网等领域。

8.3. WAN+VPN+LAN 组网

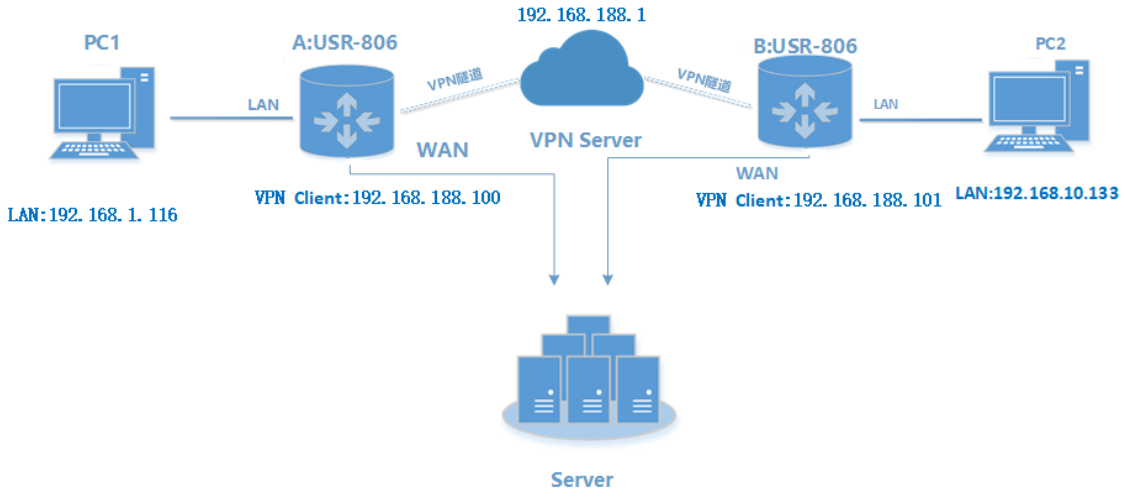


图 166　WAN+VPN+LAN 组网方式

USR-G806 路由器支持 PPTP、L2TP、IPSec、OpenVPN、GRE、SSTP 等多样 VPN 服务，G806 通过 WAN 或者 4G 或者 WIFI 的方式联网后搭建 VPN 服务实现在不同局域网内的设备互通。本组网方式适合于子公司内网访问总部内网以及不同局域网互通的各场景应用。实现安全、便捷的子网互通。

8.4. VPN + 端口映射

连接 VPN 网络后，相当于建立了一份虚拟的局域网网络。VPN 网络下的电脑可以实现对 4G 路由器的远程登陆访问，可以通过设置端口映射，对 4G 路由器下的设备进行 socket 通信。

测试环境：PC 两台（接入同 VPN server），USR-G806 一台（使用 4G 接口）；

- VPN 服务器：使用我司测试 VPN 服务器，test.usr.cn
- USR-G806：采用 4G 接口连接外网，创建 PPTP 接口连接 VPN；
- PC1:通过 PPTP 协议连接 VPN
- PC2：接入 USR-G806 的 LAN，作为子网设备；

8.4.1. VPN+远程登陆

USR-G806-G VPN 及防火墙设置（具备步骤参见 PPTP Client 搭建章节）：

- 添加 VPN 接口：网络---接口---添加接口---协议选择 PPTP
- 设置对应的服务器和测试用户名和密码，可以看到拨号以后获取到的 IP 为 192.168.111.38/32

图 167　SSTP 基本设置

PC1 连接 VPN（具备步骤参见 PPTP Client 搭建章节）：

- 建立 VPN 连接，设置对应的服务器和测试用户名和密码，获取到的 IP 为 192.168.111.32/32

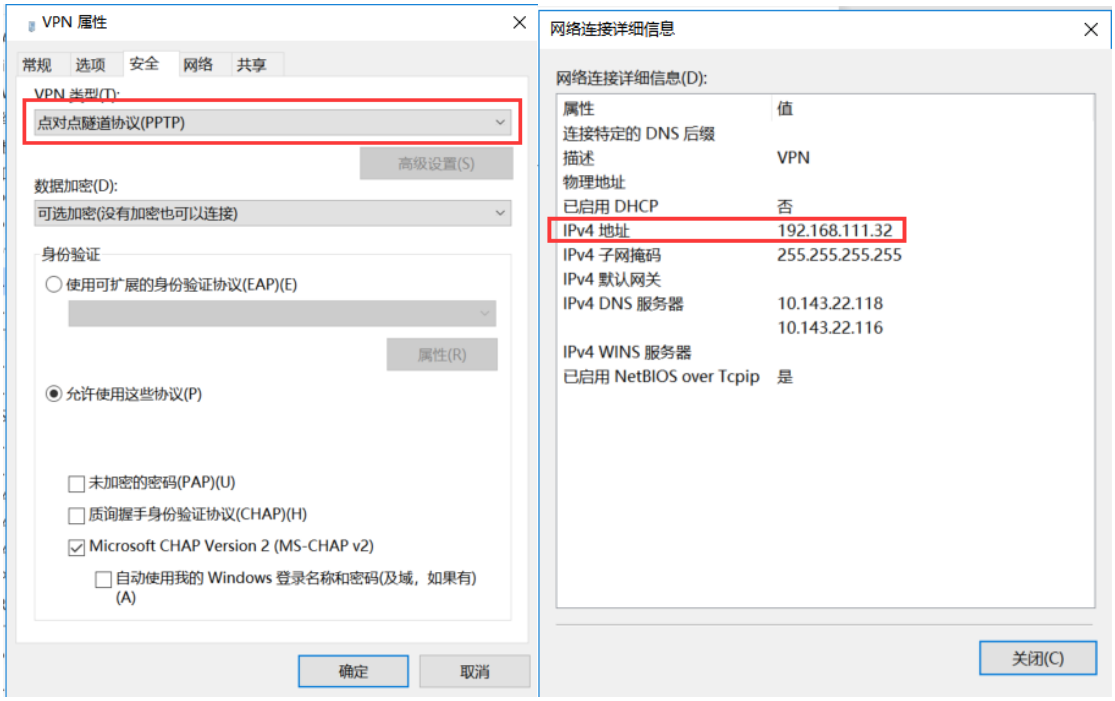


图 168　SSTP 基本设置

PC1 远程登陆访问 4G 路由器 IP：192.168.111.38

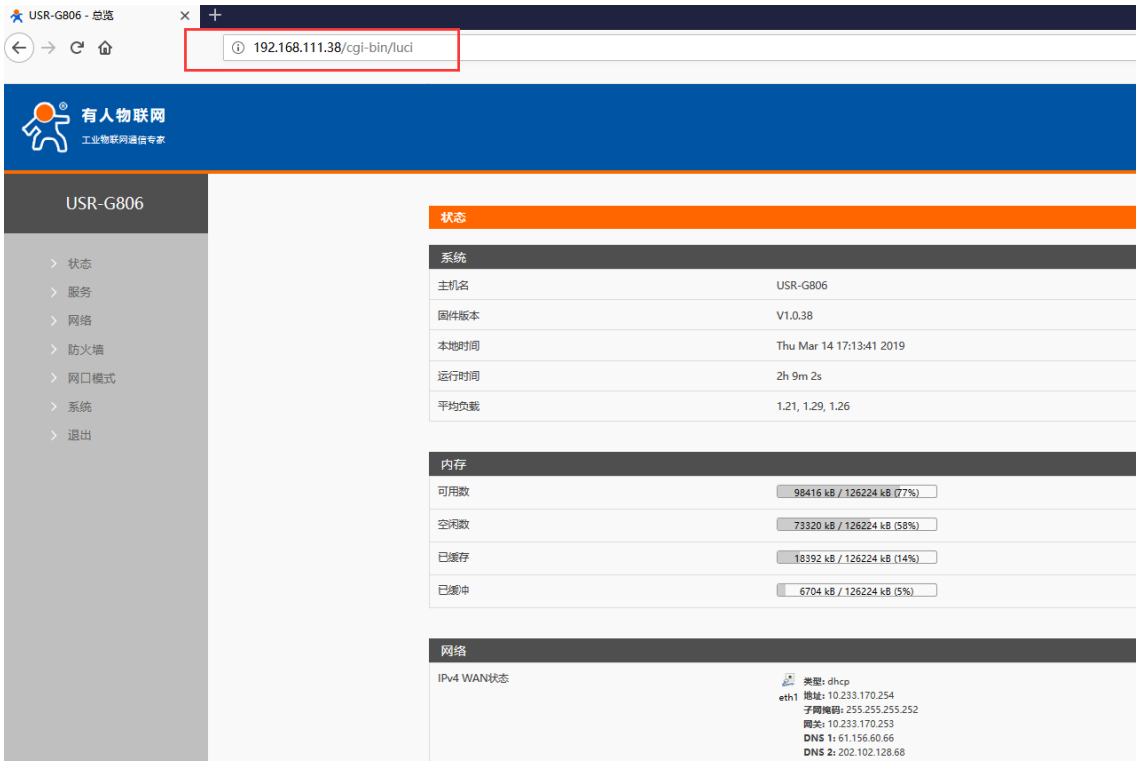


图 169　VPN+远程访问路由器

8.4.2. VPN+端口映射

VPN 下的端口映射数据流拓扑图如下，通过 USR-G806 的端口映射，实现 PC1 到 PC2 的数据收发。

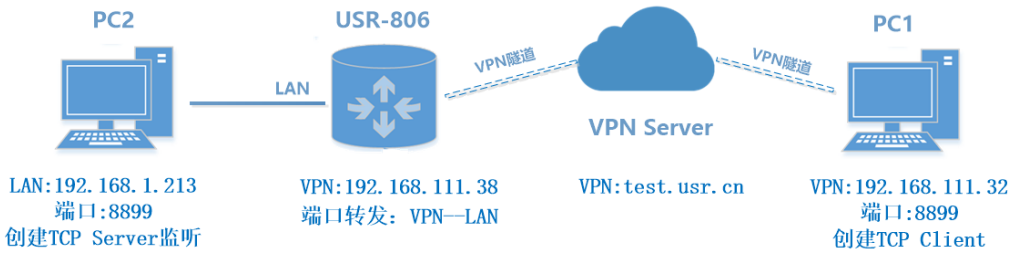


图 170　VPN+端口转发测试图

USR-G806 设置端口转发：

图 171　端口映射设置页面

在电脑 PC1 上（注意 PC1 位于其他网络，不在本路由器下），创建 TCP Client，目标 IP 地址 192.168.111.38，目标端口 8899，能够连接到 4G 路由器下的 TCP Server 并通信。

测试时，在 PC1 的 TCP Client 中发送 www.usr.cn，PC2 能够接收到端口转发数据。

图 172　端口映射成功

8.5. VPN+静态路由

VPN+静态路由拓扑图如下，通过 VPN+静态路由实现子网互通，实现 PC1 到 PC2 的数据收发。

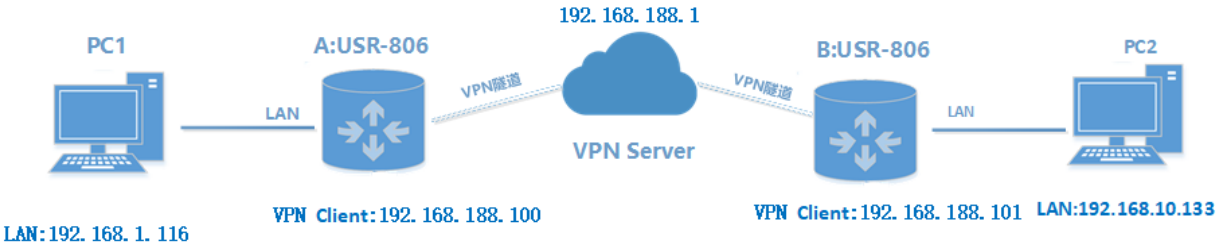


图 173　VPN+静态路由拓扑图

测试环境，两个平级路由器 A 和 B，VPN 服务器， PC 两台，以 PPTP VPN 为例

服务器 IP:192.168.188.1

路由器 A:VPN 地址 192.168.188.100 子网：192.168.1.0

路由器 B:VPN 地址 192.168.188.101 子网：192.168.10.0

在路由器 A 添加静态路由：

接口：所对应的 VPN 名称

目标：如果目标对象是子网，则填写 X.X.X.0 也可填写具体某主机 IP

IPv4-子网掩码：如果目标是子网，则填写子网掩码，若为具体 IP，可不填写

跃点数：一般不需要填写

MTU:发送接收上限，可不填

图 174　添加静态路由

在路由器 B 添加静态路由：

图 175　添加静态路由

在 VPN 服务器添加静态路由

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.188.100
route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.188.101
```

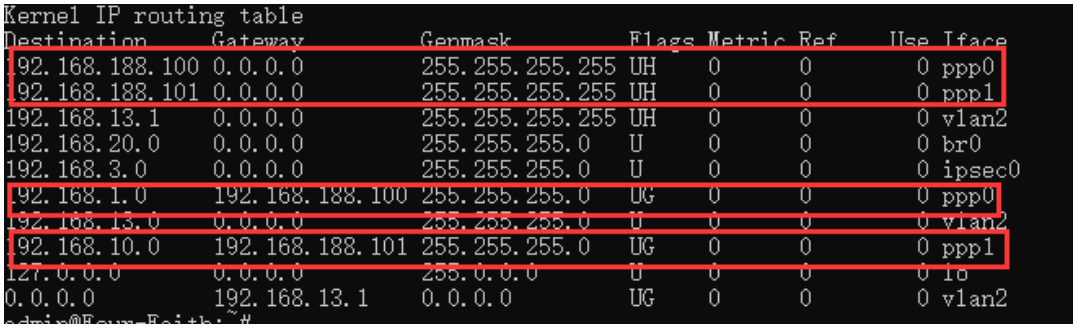
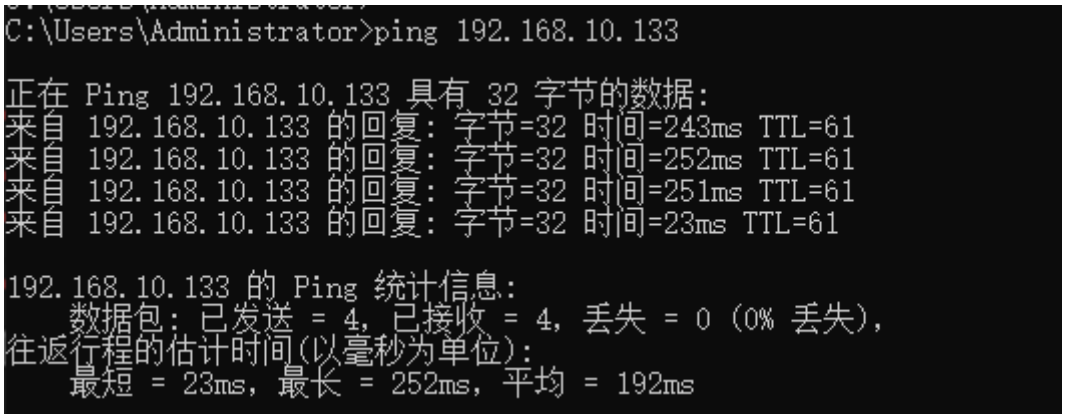


图 176　VPN 服务器添加静态路由

搭建完成后子网可互通



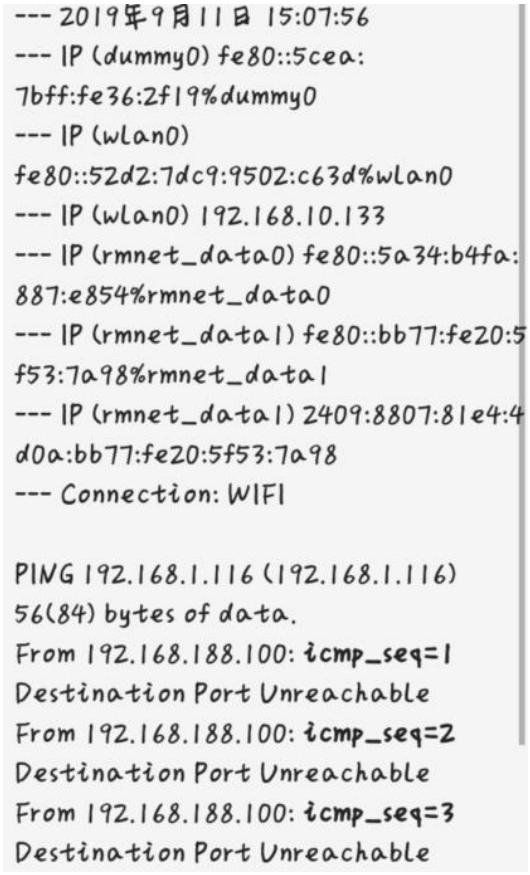


图 177　子网互通

当然 G806 子网想访问 VPN 下子网添加静态路由方式一致。

9. 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 ycsjl.usr.cn，功能参见“远程管理-远程监控”章节介绍。远程 AT 指令如下图：

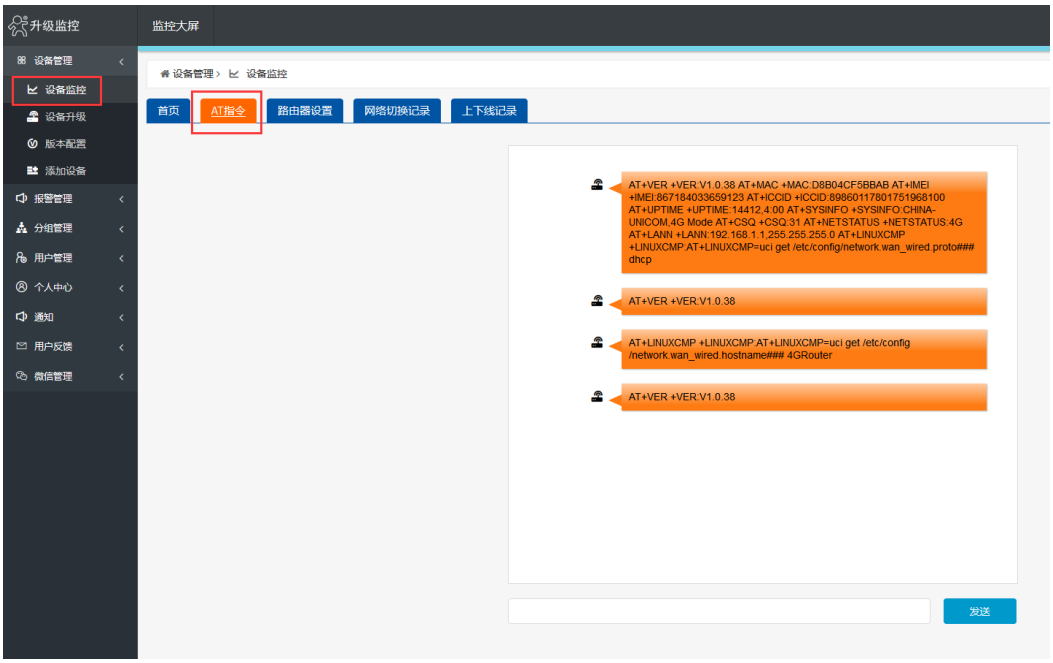


图 178　远程 AT 指令发送页面

AT 指令表汇总参见下表

表 20　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
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）
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
12	AT+WEBU	设置/查询网页登陆名称密码
13	AT+RELD	恢复到模块出厂设置

14	AT+Z	重启指令，备注：要回复+ok
远程监控与升级相关		
15	AT+UPDATE	查询/设置远程升级相关参数
16	AT+MONITOR	查询/设置远程监控相关参数
17	AT+HEARTPKT	查询/设置远程监控心跳包相关参数
系统 shell 指令相关		
28	AT+LINUXCMP	执行系统 shell 指令

9.1. 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

格式为：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:V1.0.38

9.2. 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

9.3. 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}

参数：

code：ICCID 码。

举例

发送：AT+ICCID

返回：+ICCID:898600161515AA709917

9.4. 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}OK{CR}{LF}

参数：

code：IMEI 码。

举例

发送：AT+IMEI

返回：+IMEI:868323023238378

9.5. 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}

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)： 2G Mode

3G Mode

4G Mode

举例，

发送：AT+SYSINFO

返回：+SYSINFO: CHINA-MOBILE,4G Mode

9.6. 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}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

9.7. 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

注意：不同产品型号下信号质量根据当前的 2/3/4G 网络制式的不同，请区分显示。

- USR-G806-43　7 模产品参数
  - rssi：接收信号强度指示

  使用 asu 值表示；asu 的范围为 1-31，数值越大，信号强度越好；

- USR-G806　5 模产品参数
  - rssi：接收信号强度指示

表 21　GSM 制式映射关系

取值	含义

0	小于或等于-113 dBm
1	-111 dBm
2…30	-109…-53 dBm
31	大于或等于-53 dBm
99	未知或不可测

表 22　TD 制式映射关系（减去 100 后）

取值	含义
0	小于-115 dBm
1…90	-115…-26 dBm
91	大于或等于-25 dBm
99	未知或不可测

表 23　LTE 制式映射关系（减去 100 后）

取值	含义
0	小于-140 dBm
1…96	-140…-45 dBm
97	大于或等于-44 dBm
99	未知或不可测

9.8. 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

9.9.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:2096,34

9.10. AT+WANN

功能：查询模块获取到的 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+WWAN

返回：+WANN:DHCP,10.1.179.202,255.255.255.252,10.1.179.201

9.11. 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

9.12. AT+WEBU

功能：查询/设置查询登录密码

查询：

AT+WEBU<CR>

<CR><LF>+WEBU:username,passwd<CR><LF>

举例：发送：AT+WEBU

返回：+WEBU:root,root

设置：

AT+WEBU=username,passwd<CR>

<CR><LF>+WEBU:ok<CR><LF>

9.13. 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

9.14. 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

9.15. 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,30001,20

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,30001,20

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

9.16. 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

9.17. 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: 20,heartpkt

9.18. AT+LINUXCMP

CMP :linux 命令

功能：执行 linux 命令并且返回执行信息

格式

AT+LINUXCMP=cmp<CR>

<CR><LF>+LINUXCMP: result<CR><LF>

举例：

发送：AT+LINUXCMP=pwd

返回：+LINUXCMP：/bin

注：1.返回信息大于 10 行只显示前 10 行的内容

10. 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

11. 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。

12. 更新历史

时间	版本	修改内容
2016-10-17	V1.0.0	创立
2017-3-8	V1.0.4	增添花生壳动态域名、远程管理、防火墙、VPN 功能
2017-7-24	V1.0.5	增添 VPN、DMZ、NAT、短信 AT 指令的说明
2017-7-31	V1.0.6	修改 V1.0.5 中的错误
2017-8-08	V1.0.7	修改 V1.0.6 中的错误
2017-8-13	V1.0.8	修改 V1.0.7 中的错误
2018-10-08	V1.0.10	增加 log 和参数说明
2019-03-07	V1.0.11	增加无线客户端功能介绍，增加常见组网方式，修改排版，修改内容错误
2019-03-18	V1.0.12	增加 VPN+远程登陆、修改内容错误
2019-06-18	V1.0.13	修改错误内容
2019-09-09	V1.0.14	基于 V1.0.40 固件补充修改说明
2020-02-12	V1.0.15	删除短信 AT 指令介绍，修改远程管理介绍; 修改内容错误
2020-03-25	V1.0.16	修改远程平台的图片错误
2020-04-03	V1.0.17	优化排版，合并说明书和软件设计手册
2020-04-14	V1.0.18	修复错误内容，增加安装孔间距、增加常见组网方式、增加防火墙通信规则案例
2020-06-16	V1.0.19	修改远程平台截图、修改 AT+WEBU 指令 增加 SIM 卡信号强度显示说明
2020-08-19	V1.0.20	修改产品安装尺寸描述，修改 AT 指令集格式错误内容
2020-09-05	V1.0.21	校正启动时间错误，修改 AT 指令格式错误
2020-10-27	V1.0.22	修改个别标点符号错误，修改 AT 指令格式错误 修改 ipsec 名称提示、替换 GRE 截图；修改错误内容
2020-11-12	V1.0.23	去掉 WWAN 无线客户端功能。