



SLK-RT990 系列

工业级车载 5G CPE

使用说明书

目录

第一章 登录	4
1.1 登录前准备	4
1.2 登录配置页面	6
第二章 网络配置	7
2.1 修改登录页面地址	7
2.2 5G 网络	8
2.2.1 SIM 卡 3/4/5G 方式上网	8
2.2.2 APN 设置表	10
2.3 WAN 口设置	11
2.3.1 动态地址	11
2.3.2 PPPoE 拨号	11
2.3.3 静态地址	11
2.3.4 关联 Lan（将 WAN 口转化为 LAN 口）	12
2.4 DHCP 服务器	12
2.5 WIFI 无线 AP	13
2.6 WIFI 无线客户端(桥接)	14
2.7 WIFI 无线中继	16
2.7.1 修改本地 IP 地址	16
2.7.2 连接主无线 AP	17
2.7.3 关闭 DHCP	18
2.8 定时重启	19
2.9 网络备份	19
2.10 网络自检	20
2.11 网络测试	22
第三章 串口服务(GPS)	23
3.1 设置 GNSS	23
3.2 使用工具和准备	23
3.3 GPS 工具的使用与查看	25
第四章 防火墙及应用	30
4.1 防火墙开启与关闭	30
4.2 DMZ 设置	30
4.3 端口转发	31
4.4 黑白名单	33
4.4.1 白名单	33
4.4.2 黑名单	35
4.5 内网穿透 (frp)	36
4.5.1 连接服务器	37
4.5.2 添加 TCP 代理协议	40
4.5.3 添加 STCP 代理协议	42
4.5.4 添加 UDP 代理协议	49
4.5.5 添加 HTTP 代理协议	51
第五章 VPN（虚拟专用网）	53

5.1 PPTP VPN	53
5.2 L2TP VPN	53
5.3 GRE VPN	54
5.4 OpenVPN	55
第六章 系统（设备管理）	57
6.1 日期和时间	57
6.2 语言设置	57
6.3 修改密码	58
6.4 升级固件	58
6.5 备份/恢复	59
6.6 恢复出厂设置	59
6.7 设备重启	60
6.8 页面退出	60

第一章 登录

1.1 登录前准备

完成硬件安装后，在登录路由器的 Web 设置页面前，您需要确保管理计算机已安装了以太网卡。请将管理 PC 设置成“自动获得 IP 地址”和“自动获得 DNS 服务器地址”（计算机系统的缺省配置），由设备自动为管理 PC 分配 IP 地址。

将管理 PC 的 IP 地址（例如设置为：192.168.2.59）与设备的 LAN 口 IP 地址设置在同一网段内（设备 LAN 口初始 IP 地址为：192.168.2.1，子网掩码均为 255.255.255.0）方法如下。

以 win10 为例，操作如下：

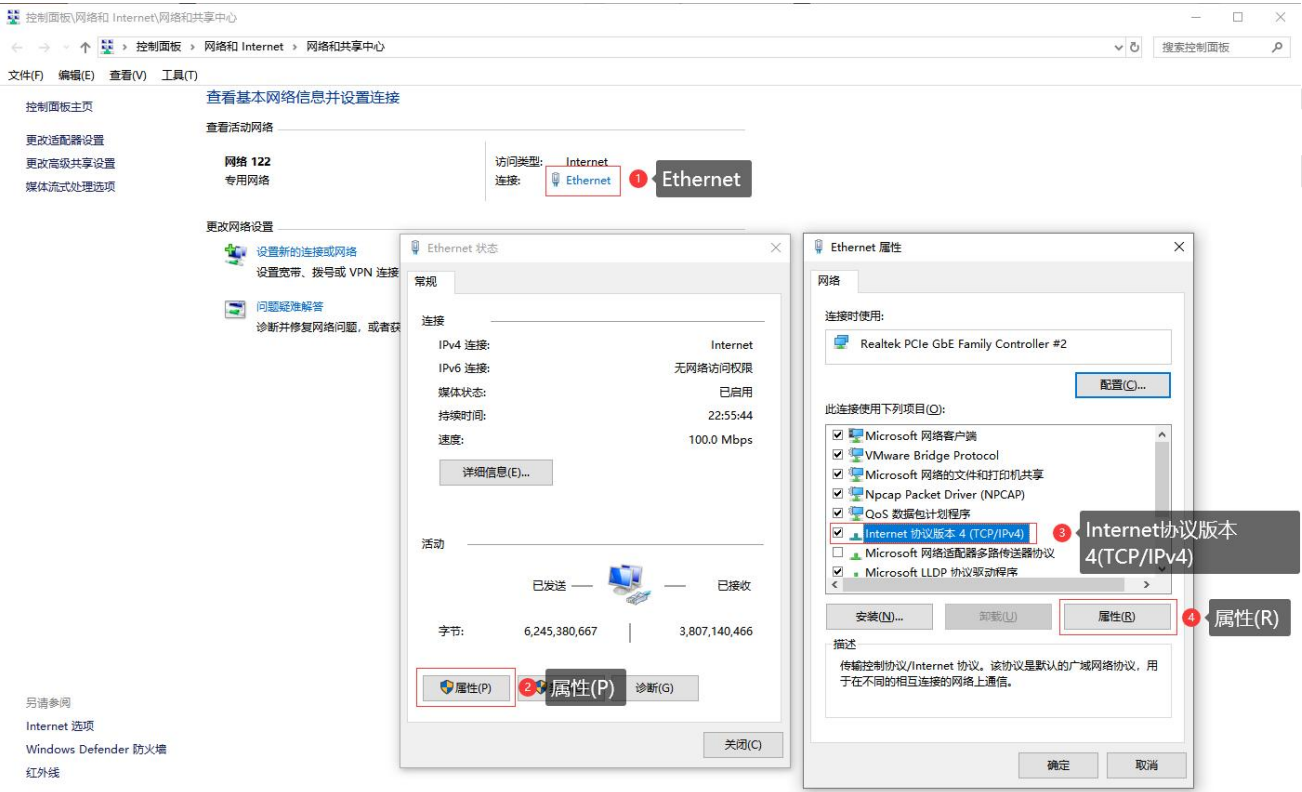
第一步：鼠标右击桌面右下角网络标志（如图），选择打开“网络和 Internet”设置。



第二步：先鼠标点击以太网，再点击网络和共享中心。

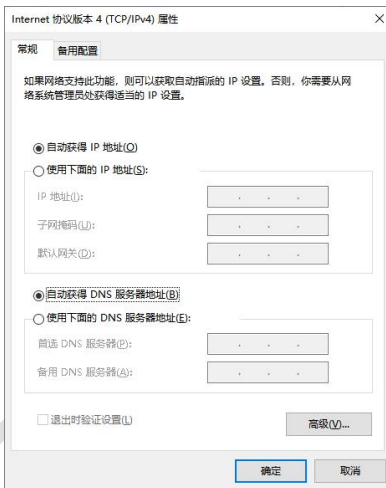


第三步：鼠标点击 **Ethernet**，弹出框(Ethernet 状态)内点击**属性**，弹出框(Ethernet 属性)内选择 **Internet 协议版本 4(TCP/IPv4)**，点击**属性**。

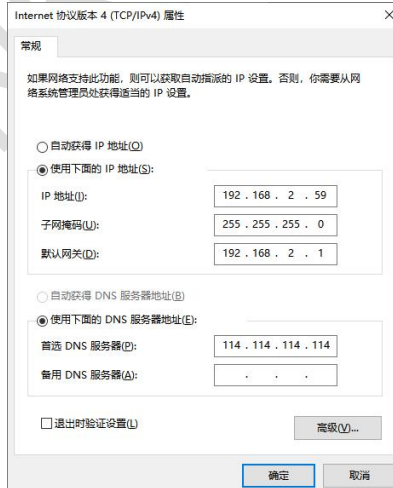


第四步：有三种设置方法。

方法 1



方法 2



方法 3

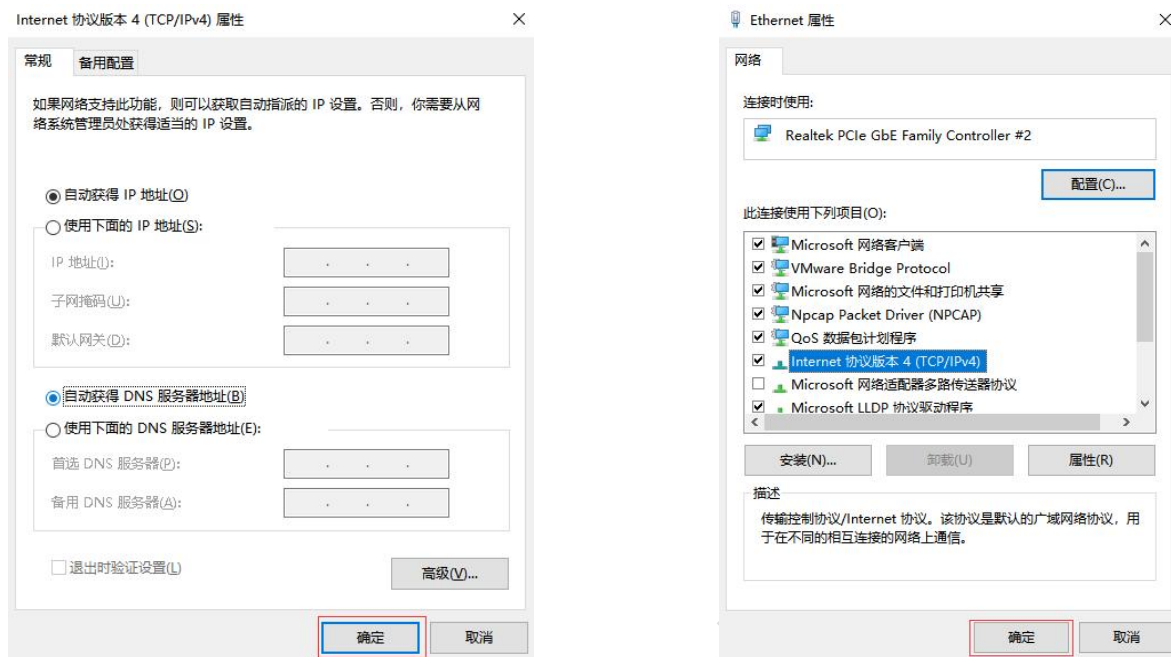


方法 1：可以用于配置设备并访问外网，推荐使用（注意：如果当前环境下有多台不同网段的路由，可能造成电脑获取的 IP 不能连接设备，这时可选用方法 2）；

方法 2：可以用于配置设备并访问外网,IP 地址设置为设备 IP（设备默认 192.168.2.1）同网段 IP：192.168.2.X（X 是 2 到 254 之间的任意数，例如 192.168.2.2），默认网关设置为设备 IP：192.168.2.1，DNS 可设置为 114.114.114.114(国内)和 8.8.8.8(国外)等通用的 DNS；

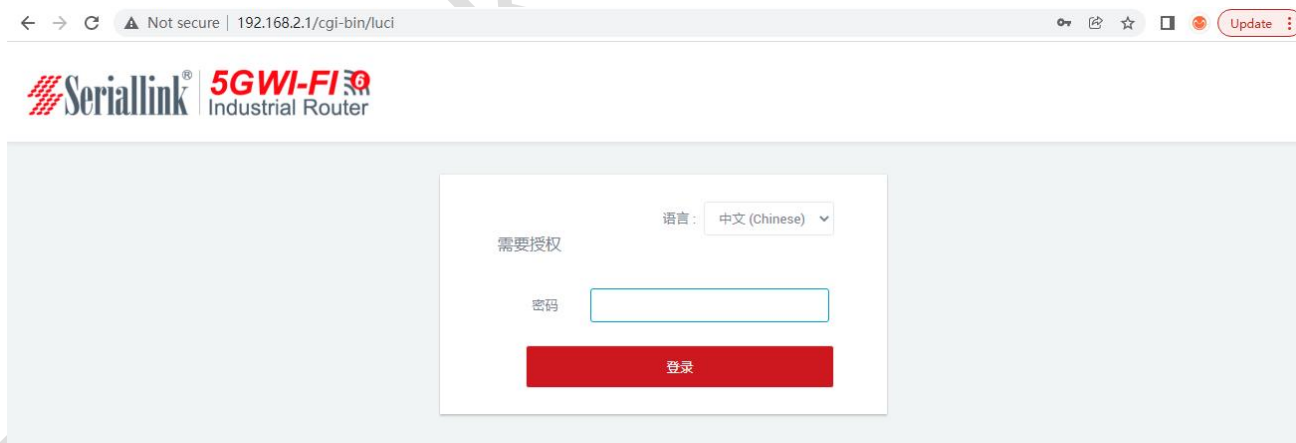
方法 3：仅连接设备，用于配置使用，电脑不能通过设备网络访问外网，IP 地址设置如方法 2；

第五步：鼠标点击**确认**，以保存第三步和第四步的修改（不点击确认直接关闭其中任何一个窗口都将不会生效）。



1.2 登录配置页面

打开 IE 或者其它浏览器，在地址栏中输入 192.168.2.1，连接建立后，在弹出的登录界面，以系统管理员（admin）的身份登录，即在该登录界面输入密码（密码出厂默认设置为 admin）。



登录默认密码都为 admin。若是用户需要保护配置界面，避免被他人修改，可以修改登录密码，依次点击“系统”——“修改密码”，然后填入将要修改的密码，然后“保存&应用”，具体参考章节 5.3。

第二章 网络配置

2.1 修改登录页面地址

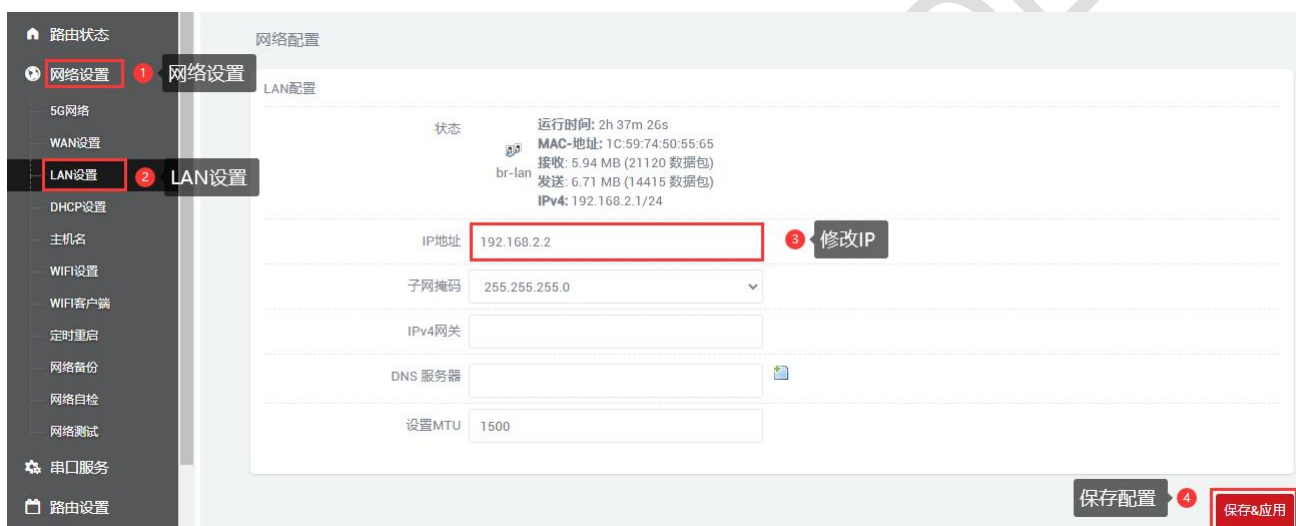
路由器默认地址为 192.168.2.1，在导航栏“网络设置”——“LAN 设置”可以修改静态的 ip 地址，修改后将用新的 ip 地址登录进页面。

IP 地址：修改设备的 ip 地址（默认是 192.168.2.1）。

子网掩码：一般是 255.255.255.0，可以根据需要进行修改。

IPv4 网关、DNS 服务器、设置 MTU：无特殊情况不需要设置。

配置完成后点击“保存&应用”，使其生效，生效后需要用新的 ip 地址才能访问到设备的配置页面。



路由状态 网络配置

网络设置 1 网络设置

5G网络

WAN设置

LAN设置 2 LAN设置

DHCP设置

主机名

WiFi设置

WiFi客户端

定时重启

网络备份

网络自检

网络测试

串口服务

路由设置

LAN配置

状态 运行时间: 2h 37m 26s

MAC-地址: 1C:59:74:50:55:65

br-lan 接收: 5.94 MB (21120 数据包)

发送: 6.71 MB (14415 数据包)

IPv4: 192.168.2.1/24

IP地址 192.168.2.2 3 修改IP

子网掩码 255.255.255.0

IPv4网关

DNS 服务器

设置MTU 1500

保存配置 4

保存&应用

← → ↻ Not secure 192.168.2.2/cgi-bin/luci



语言: 中文 (Chinese)

需要授权

密码

登录

2.2 5G 网络

2.2.1 SIM 卡 3/4/5G 方式上网

路由器默认是使用 SIM 卡 3/4/5G 上网，在导航栏“路由状态”——“状态”可以看到 SIM 卡的信息，右上角可以查看网络是 3/4/5G 以及手机卡信号。

The screenshot shows the Seriallink 5GWI-FI Industrial Router web interface. The left sidebar has a menu with '路由状态' (Routing Status) selected, and '状态' (Status) is highlighted. The main area displays '注网状态' (Network Status) with a table of SIM card information. A red box highlights the table content.

SIM卡	已插入卡
运行商	中国联通
当前蜂窝网络	NR5G_SA
频段	78
绝对射频信道	627264
小区ID	365
网络注册信息	GPRS: 0,0 / EPS: 0,0 / 5GS: 0,1
信号质量	RSRQ: -11.0 dB / RSRP: -87 dBm
蜂窝数据	SIM2
IMEI	866355051041425
IMSI	460019468644297
ICCID	89860122801942568077

如果使用普通手机流量卡，APN 设置的位置可以不用关心，默认为空即可。如果您使用了 APN 卡，需要在“网络设置”——“5G 网络”——“基本设置”设置 APN。

The screenshot shows the Seriallink 5GWI-FI Industrial Router web interface. The left sidebar has a menu with '网络设置' (Network Settings) selected, and '5G网络' (5G Network) is highlighted. The main area displays '5G网络' (5G Network) settings. A red box highlights the 'APN' field in the '基本设置' (Basic Settings) tab. A callout box points to the 'APN' field with the text '输入APN配置' (Input APN configuration).

5G网络

基本设置 高级设置 物理设置

状态 运行时间: 0h 7m 29s
MAC-地址: 02:50:F4:00:00:01
接收: 5.16 KB (43 数据包)
发送: 9.14 KB (65 数据包)
IPv4: 10.3.229.242/30
IPv6: 2408:8459:3430:4bd9:dd80:c675:9817:6645/64

应用 ☒

APN

用户名

密码

认证类型 无

PIN码

5G网络异常处理

5G网络异常处理: 开启功能后将每隔5s检测一次目标IP地址。如果超出异常次数后仍然无法PING通目标IP地址, 会选择以下的操作模式之一应对4G网络异常状况 (例如: 飞行模式, 切换SIM卡或者重启路由器)。

启用 ☐

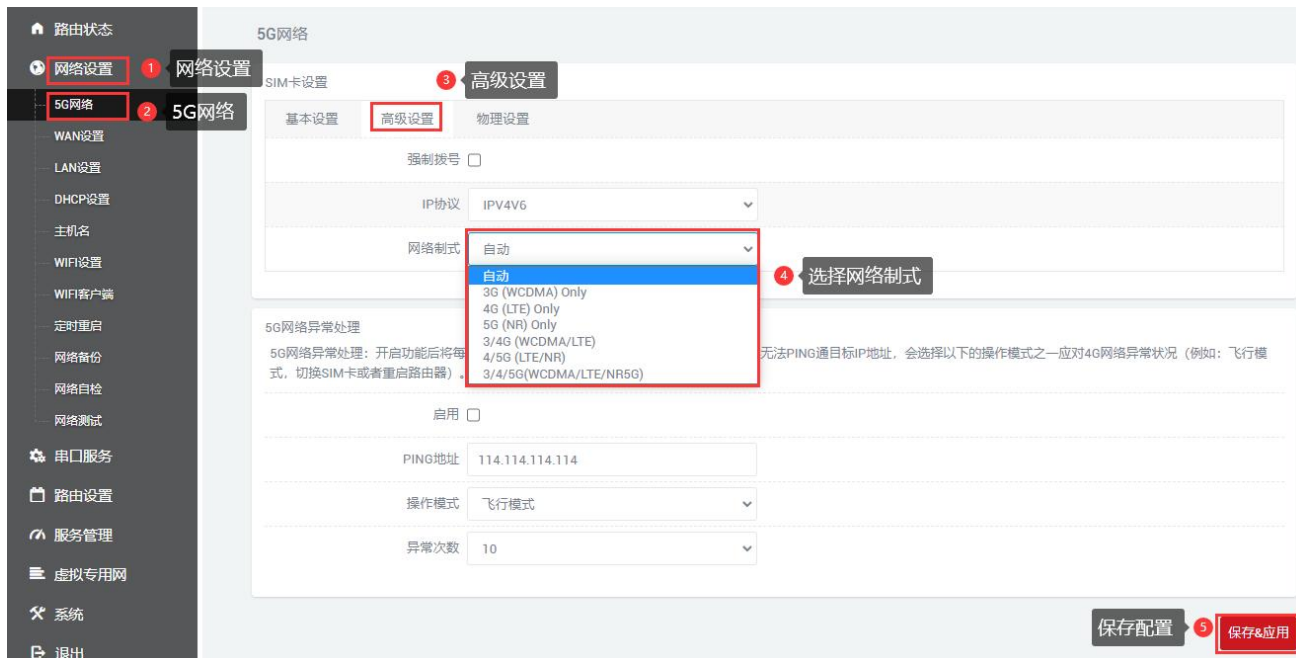
PING地址 114.114.114.114

操作模式 飞行模式

异常次数 10

保存配置 保存&应用

“网络设置”——“5G 网络”——“高级设置”可以对 3/4/5G 进行绑定，如果服务类型选择了 5G (NR) Only，代表只用 5G 的网，附近没有 5G 网络会自动没有网络。默认是 3/4/5G 都有，那个网络信号比较强先用哪一个，优先使用 5G。锁定频段是自动的，优先选择信号好的频段，也可以根据自己需要锁定频段，如果锁定的频段不成功，说明模块暂时不支持这个频段。设置完成后点击“保存&应用”。



“网络设置”——“5G 网络”——“物理设置”可以对默认 SIM 卡进行修改，如果只插入一张卡，则默认使用，不需要修改这里的配置。

跃点数(默认值：30)：一般不用修改，值越小，使用网络优先级越高(网络包括：wifi 客户端、WAN 口、4G 网络等)。

MTU(默认值：1400)：最大传输单元，一般不用修改，影响网络速度。



异常重启：是对网络异常进行处理，每 5s ping 一次设置的 ip 地址 (114.114.114.114)，ping 完异常的次数后还是不能 ping 通，将根据选择进行设置（断网重启网络、飞行模式（默认）、切换 SIM 卡）。在“基本设置”和“高级设置”、“物理设置”都可以设置网络诊断，默认不启用，如果需要启用网络诊断，将启用勾选即可。

异常重启

网络异常处理：5秒钟循环检查网络连接，如果Ping IP地址没有成功，网络超过异常次数后重启，重新搜索注册网络。

启用 ☒

PING地址 114.114.114.114

操作模式 飞行模式

异常次数 10

注意：

- 普通的 5G 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（如有请参考 APN 设置表章节）或请咨询运当地营商。

2.2.2 APN 设置表

下列中是各运营商公网的相关拨号参数，专用拨号参数具体请以运营商给出的专用卡信息为准。

1、国内物联网卡 APN 参数

运营商	APN	用户名	密码	拨号
电信 4G	ctm2m	*.m2m(定向用户)	vnet.mobi	*99#
物理网卡		m2m (普通用户)	vnet.mobi	*99#
联通 4G	unim2m.njm2mapn	空（不填）	空（不填）	*99#
物联网卡				

2、普通流量 4G 卡 APN，一般无需任何设置都可以正常上网：

三大运营商 4G 卡通用卡 APN：

运营商	APN	用户名	密码	拨号
移动 4G	cmnet	card	card	*99#
联通 4G	3gnet	card	card	*99#
电信 4G	ctlte	ctnet@mycdma.cn 或者 card	card	*99#

3、通用 3G 网络 APN 参考如下：（如果您是 3G 卡必须按照如下表格设置）

运营商	APN	用户名	密码	拨号
移动	cmnet	card	card	*99#
联通	3gnet	空（不填）	空（不填）	*99#
电信 3G	ctnet	ctnet@mycdma.cn	vnet.mobi	#777

2.3 WAN 口设置

2.3.1 动态地址

导航栏“网络设置”——“wan 设置”，WAN 口默认协议是动态地址（即 DHCP 客户端），需要上级设备能够为 wan 口分配 ip，无特殊情况，MTU 的值不需要改变(默认值：1500)。



2.3.2 PPPoE 拨号

如果 wan 口需要拨号才能上网的，需要选择 PPPoE 拨号，根据实际情况填写用户名和密码，无特殊情况，MTU 的值不需要改变(默认值：1500)。



2.3.3 静态地址

wan 口也可以选择自己手动设置 ip 地址，需要设置与上级网段相同的 IP 地址，子网掩码，网关填写上级设备的 IP 地址，DNS 可与网关相同，一般有 114.114.114.114(国内)和 8.8.8.8(国外)等通用的 DNS，无特殊情况，MTU 的值不需要改变(默认值：1500)。



2.3.4 关联 Lan（将 WAN 口转化为 LAN 口）

如果要将 WAN 口转化为 LAN 口，将 wan 设置的协议改为“关联 LAN”，点击“保存&应用”，就可以将 wan 口转化为 lan 口（关联 LAN 的情况下，请注意不要将 WAN 口、LAN 口一起接到交换机或同一电脑上），无特殊情况，MTU 的值不需要改变(默认值：1500)。



2.4 DHCP 服务器

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

DHCP 客户端配置（默认启用）：依次选择“网络设置”——“DHCP 设置”，“保存&应用”即可。

关闭 DHCP：勾选关闭 DHCP 服务器。

开始：分配的 dhcp 服务器的起始地址，比如 100，代表从 192.168.2.100 开始分配。

客户数：分配的 ip 个数。

租用时间：分配的 IP 的时间长短。



2.5 WIFI 无线 AP

WIFI AP 支持 WIFI 双频 2.4G+5.8G，WIFI 默认开启，wifi 名称：SLK-Router_2G-XXXX、SLK-Router_5G-XXXX(为避免不同设备之间 wifi 同名，“XXXX”部分会有不同)，密码：slk100200(密码需要满足 8 个字符或以上)。导航栏“网络设置”——“WIFI 无线 AP”，可以更改 WIFI 基本配置。



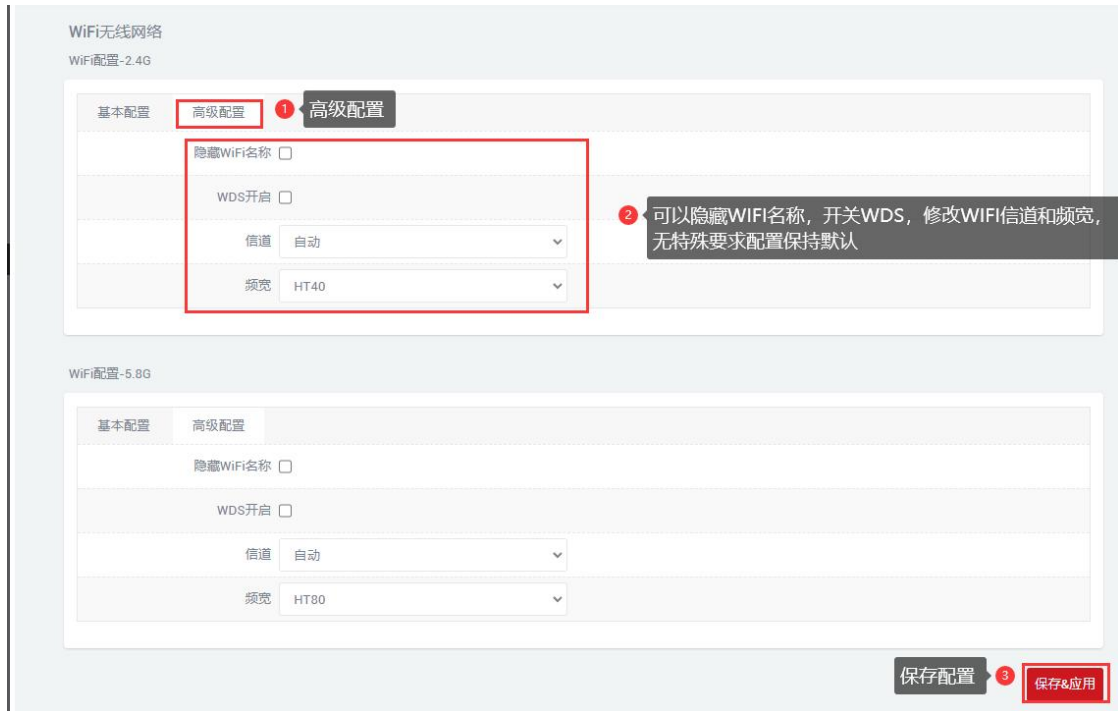
导航栏“网络设置”——“WIFI 无线 AP”——“高级”，一般情况下不需要修改。

隐藏 WiFi 名称：勾选，将在手机、电脑等设备上搜索不到这个 WiFi。

信道：如果知道附近其他 wifi 的信道，可以将此设备设置成不同的信道，以提升 wifi 速度和信号。

频宽：WiFi 速度 HT80(5.8G 专有) > HT40 > HT20，WiFi 稳定性 HT20 > HT40 > HT80(5.8G 专有)，受距离和隔离物（如墙壁）影响，近距离用大频宽，远距离用小频宽。

发射功率：功率越高，wifi 性能越好。



注意：国内 WiFi 5.8G 暂不支持的信道 165、100、104、108、112、116、120、124、128、136、140、144，WiFi-5.8G 启动较慢，请稍等片刻。

2.6 WIFI 无线客户端(桥接)

WIFI 无线客户端默认是不启用的，需要在导航栏“网络设置”——“WIFI 无线客户端”，勾选启用。



然后选择客户端无线接口模式：2.4G 客户端、5.8G 客户端，搜索对应的 WIFI 列表，在 SSID 列表选择 WIFI，根据有无密码更改安全性选项，无（无密码），加密（加密混合模式 Mixed WPA/WPA2-PSK），WDS 默认不勾选。

基本设置

状态  **MAC-地址:** 00:00:00:00:00:00
接收: 0.00 B (0 数据包)
发送: 0.00 B (0 数据包)

启用 ☒

无线接口 5.8G客户端 4 选择客户端接口

搜索 搜索 5 点击搜索

SSID __TEST_AP

安全 __TEST_AP 6 选择WIFI

WDS 赛诺联克

高级设置

基本设置

状态  **MAC-地址:** 00:00:00:00:00:00
接收: 0.00 B (0 数据包)
发送: 0.00 B (0 数据包)

启用 ☒

无线接口 5.8G客户端

搜索 搜索

SSID 赛诺联克

安全 加密 7 安全选择无或者加密

密码 ***** 8 选择加密则需要输入密码

WDS ☐

高级设置

协议 动态地址

☒ 桥接Lan口需与上游设备同一网段

保存&应用

9 保存&应用

成功连接到 WIFI 就会显示 WIFI 状态。

状态  运行时间: 0h 0m 7s
MAC-地址: 06:03:7F:12:32:0B
Client "赛诺联克" 接收: 5.08 KB (55 数据包)
发送: 1.20 KB (6 数据包)
IPv4: 192.168.16.60/24

注意：无线接口 2.4G 客户端搜索需要 WIFI 无线 AP WiFi-2.4G 在已启动状态，无线接口 5.8G 客户端搜索需要 WIFI 无线 AP WiFi-5.8G 在已启动状态，不然不会显示搜索结果（保存 WIFI 无线 AP 和 WIFI 无线客户端的页面配置后，WiFi-5.8G 启动较慢，请稍等片刻）。

WIFI 无线客户端高级设置协议选择：

动态地址（默认）：WiFi 客户端自动获取上级路由的分配的 IP 地址。

静态地址：WiFi 客户端使用用户配置的 IP 地址、子网掩码、网关、DNS。



桥接 Lan 口：使用 Lan 口配置的 IP 地址、子网掩码、网关、DNS，Lan 口配置参考 WIFI 无线客户端



高级设置静态地址(中继模式选择此项)。

2.7 WIFI 无线中继

此部分描述如何通过中继的方式实现无线信号长度延长。在此配置模式下，接入到 SLK-R680 上的电脑终端，是和主无线网网络处在相同的 IP 地址段的。

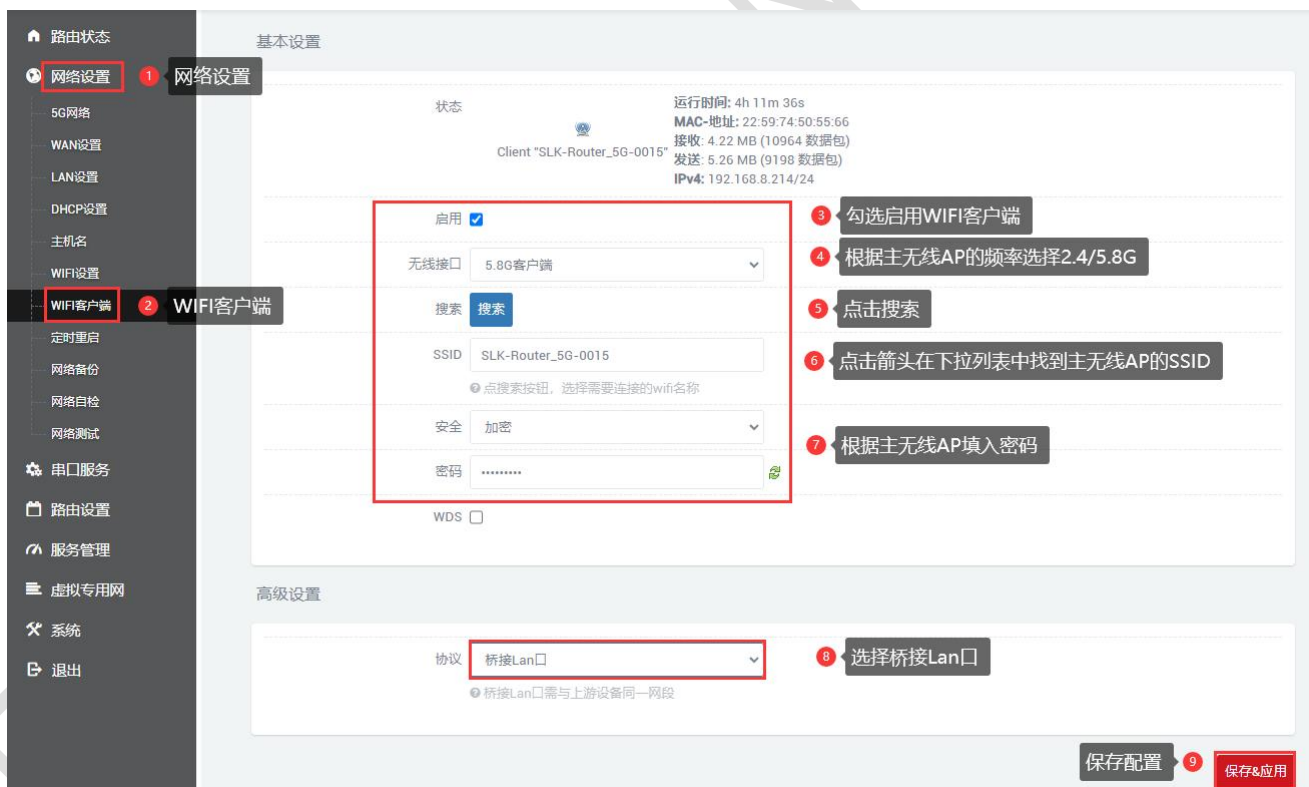
2.7.1 修改本地 IP 地址

需要先将 SLK-R680 的本地 IP 地址修改与主无线 AP 同一网段下，例如要连接的主无线 AP 的 IP 地址是 192.168.1.1，则修改 SLK-R680 的 IP 地址为 192.168.1.100。要注意的是，LAN 口网关默认为空，在使用中继模式设置后，如果日后需要以 WAN 口接线上网，需要再在 LAN 设置删除网关信息，避免发生无法上网的情况。



2.7.2 连接主无线 AP

导航栏“网络设置”——“WIFI 无线客户端”中，勾选启用 WIFI 无线客户端，配置连接主无线 AP，例如这里要连接的主无线 AP 的 SSID 为 SLK-Router_E60011，密码 slk100200，按照下图操作搜索并选择 SSID，填写密码，“协议”选择“关联 Lan 口”，点击“保存&应用”。



要注意的是，此模式下，主无线 AP 不再为此 SLK-R680 分配 IP 地址。所以“状态”中不会更新获取的 IP 地址，可通过图标颜色和 MAC 地址确认是否连接成功。如下图即为成功的。

基本设置

状态

运行时间: 0h 0m 0s
MAC-地址: 06:03:7F:12:14:CF
Client "WIFI6-2G" 接收: 0.00 B (0 数据包)
发送: 0.00 B (0 数据包)

启用 ☒

无线接口 2.4G客户端

搜索

SSID WIFI6-2G

安全 加密

密码 *****

WDS ☐

2.7.3 关闭 DHCP

关闭 SLK-R680 的 DHCP 服务器功能。这样 SLK-R680 不再为接入的设备分配 IP 地址，所有接入局域网的设备均有主无线分配 IP 地址，实现同网段通信。

路由状态 DHCP服务器设置

网络设置 1 网络设置

5G网络

WAN设置

LAN设置

DHCP设置 2 DHCP设置

主机名

WIFI设置

WIFI客户端

定时重启

网络备份

网络自检

网络测试

串口服务

路由设置

关闭DHCP ☒ 3 关闭DHCP

禁用本接口的DHCP。

静态地址分配

静态租约用于给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。

主机名	MAC-地址	IPv4-地址	IPv6-后缀（十六进制）
尚无任何配置			

添加

保存配置 4 保存&应用

2.8 定时重启

导航栏“网络设置”——“定时重启”，用户可以勾选启用并设置每天重启的时间，注意查看设备时间是否正确，修改正确时间：“系统”——“时间和日期”，具体查看章节 5.1。



2.9 网络备份

此部分为新增功能，主要用于上网优先使用有线（即 wan 口）还是蜂窝网络或者 wifi 客户端，优先使用主链路的网络，当主链路没有网的时候使用备份路线的网络。

网络备份默认的是关闭的，需要将启用勾选，然后根据实际情况进行配置。



常规设置@链路管理		
项目	说明	默认
PING 地址	测试网络连通性的地址	114.114.114.114
主链路	可选择“WAN”或“WIFI”或“5G”。 5G：使用 5G 作为主要的有线链路 WAN：使用 wan 作为主要的有线链路 WIFI：使用 wifi 客户端作为主要的无线链路 注：wifi 链路仅当开启 wifi 的客户端模式后才可用。详情情况请参阅“2.6”	WAN
备份链路	可选择“WAN”、“WIFI”、“5G”、“无”。 5G：使用 5G 作为备份的有线链路 WAN：使用 wan 作为备份的有线链路 WIFI：使用 wifi 客户端作为备份的无线链路 无：代表不使用这备份链路 注：wifi 链路仅当开启 wifi 的客户端模式后才可用。详情情况请参阅“2.6”	无
线路切换模式	‘主线路优先’模式下，网络会主动切换到主线路 注：当主线路恢复正常。	主线路优先
恢复间隔	当备份链路“主线路优先”模式下使用时，指定等待多少分钟切回主链路用以检测主链路是否恢复正常。 注：此功能仅当选择“主线路优先”模式时才显示。	1

2.10 网络自检

导航栏“网络设置”——“网络自检”，网络自检功能默认关闭，网络自检允许设置周期性的重启 或者 网络异常时重启。

需要启动该功能则点击添加，输入配置后点击“保存并应用”。



强制重启延时：当重启系统的时候网络自检将会触发一个软重启，在这里输入一个非 0 的值，如果软重启失败将会触发一个延迟的硬重启。输入秒数启用，输入 0 禁止功能。

周期：当没有网络连接情况下到执行重启的最长时间间隔。默认单位为秒，您可以使用'm'作为后缀表示分钟，'h'表示小时'd'表示天。

ping 主机：ping 主机地址。

1、网络异常重启模式

网络自检

网络自检允许设置周期性的重启 或者 网络异常时重启。

删除

操作模式	网络异常重启
强制重启延时	30
周期	5m
ping主机	8.8.8.8

添加

④ 选择网络异常重启，根据提示配置

保存&应用

⑤ 保存&应用

2、定期重启模式

网络自检

网络自检允许设置周期性的重启 或者 网络异常时重启。

删除

操作模式	定期重启
强制重启延时	30
周期	5m

添加

④ 选择定时重启，根据提示配置

保存&应用

⑤ 保存&应用

2.11 网络测试

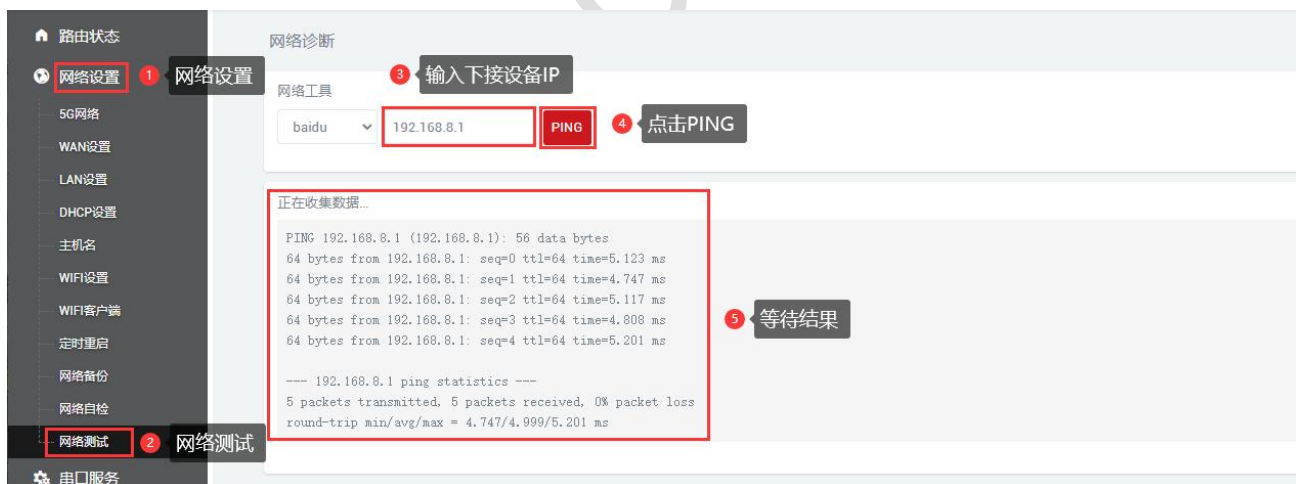
通过网络诊断可以判断路由器与下接设备之间是否能够通信，设备是否能够上网，设备连接 VPN 是否成功。还可以用来测试别的方面，根据自己的需求进行测试即可。

导航栏“网络设置”——“网络测试”。

Baidu、seriallink、8.8.8.8：一般用来测试设备是否能够上网，能 ping 通说明设备能够上网，不能 ping 通说明设备不能上网。



自定义输入框：一般用来测试能否 ping 通下接设备。



第三章 串口服务(GPS)

3.1 设置 GNSS

依次选择“串口服务”>>>“GNSS”，这里网络协议选择 **TCP Server** 为例，数据类型根据需要选择，一般选择都是 **Raw data**，本地端口设置后要注意，建立 **TCP** 连接的时候要用到串口服务器的 **IP** 地址和端口号，通过串口配置栏对串口的波特率，数据位，停止位以及校验位根据自己的需要进行配置。配置完成后点击保存并应用。

网络配置	
启用	☒
网络协议	TCP Server
数据类型	Raw data
本地端口	4000
最大连接数	6
超时 (秒)	300

串口配置	
波特率	115200
数据位	8
停止位	1
校验位	无

保存&应用

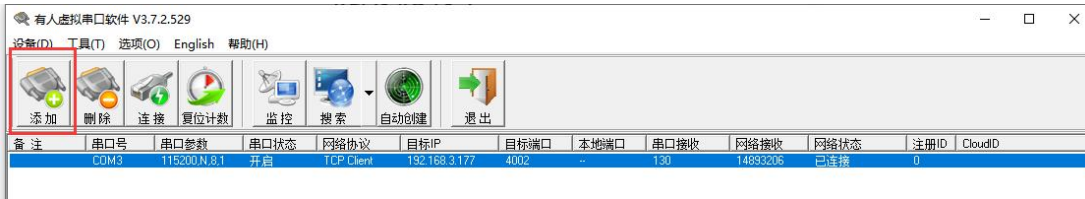
最大连接数：默认为 **6**，表示最多支持 **6** 个 **TCP Client** 去连接同一个串口。

超时(秒)：默认为 **300**，表示 **TCP Server** 建立连接后，没有数据的情况下，**300** 秒之后断开连接，需要永久在线连接可以把值设置为 **0**。

3.2 使用工具和准备

依次选择“串口服务”>>>“GNSS”，根据自己需求配置某个端口。需要虚拟串口工具(这里以 **USR-VCOM** 为例)将设备上的端口虚拟成电脑上的 **com** 口。进入到 **USR-VCOM** 软件。

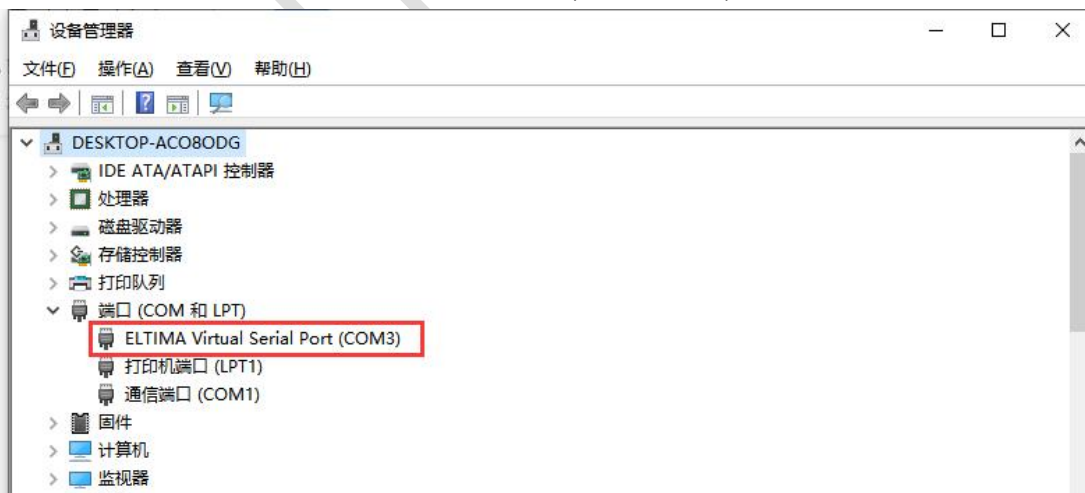
点击添加



- ①选择虚拟的串口(COM)。
- ②网络协议根据设备配置页面设置，(设备)TCP server - TCP Clientn(软件)、(设备)TCP Client- TCP Server(软件)、(设备)UDP- UDP(软件)。
- ③目标 IP/域名填写路由器的 IP 地址(192.168.2.1)。
- ④目标端口填写路由器的“串口服务”>>>“GNSS”中设置的本地端口(默认 4002)。
- ⑤点击确认即可将端口虚拟成电脑的 com 口



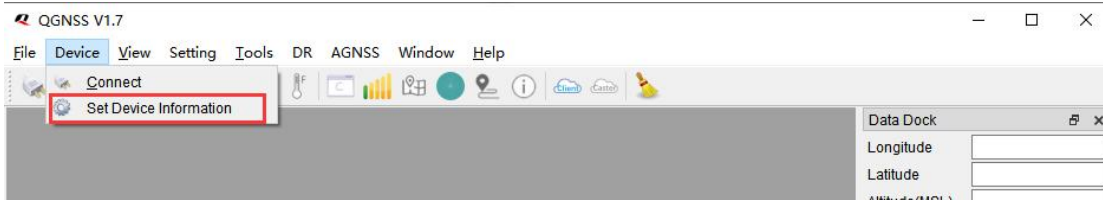
虚拟完成后在电脑打开设备管理器，查看“端口(COM 和 LPT)”中虚拟口是否成功。



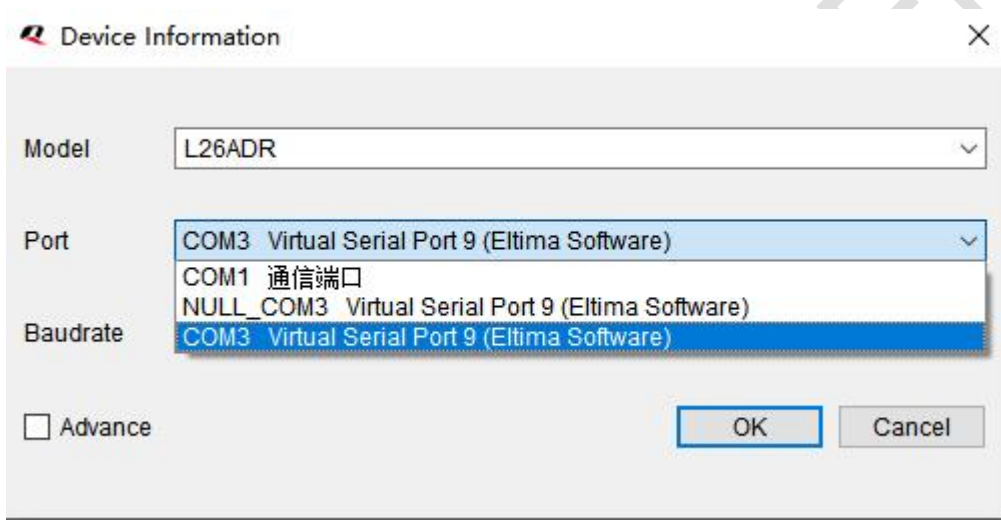
3.3 GPS 工具的使用与查看

3.1.1 连接设备

①打开 QGNSS 软件，点击 Device，选择 SetDevice Information。

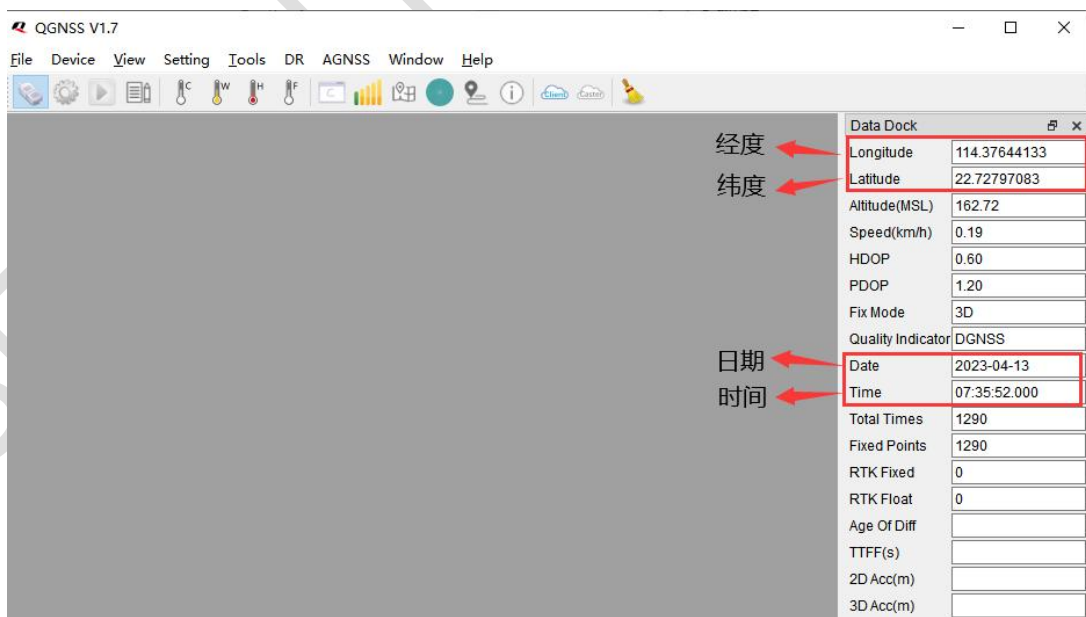


②在 Device Information，根据 USR-VCOM 虚拟出来的 COM 口选择相应的 Port，点击 ok 即可连接



3.1.2 经纬度查看

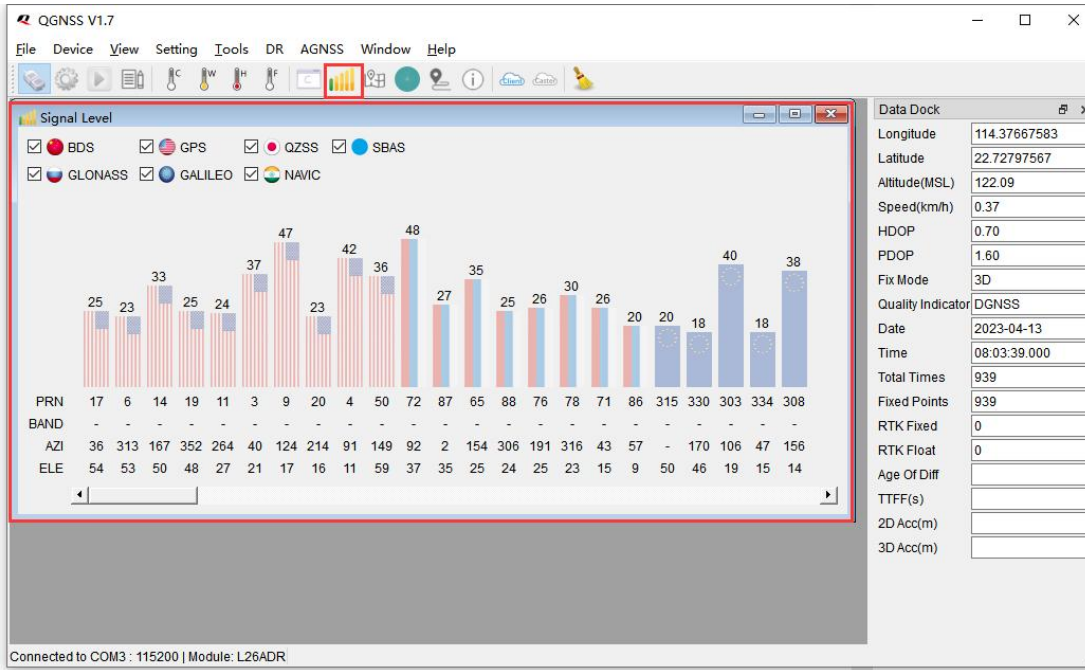
连接成功后，Data Dock 中就会显示出设备所在的经纬度和日期时间等数据。



3.1.3 GNSS 卫星信号

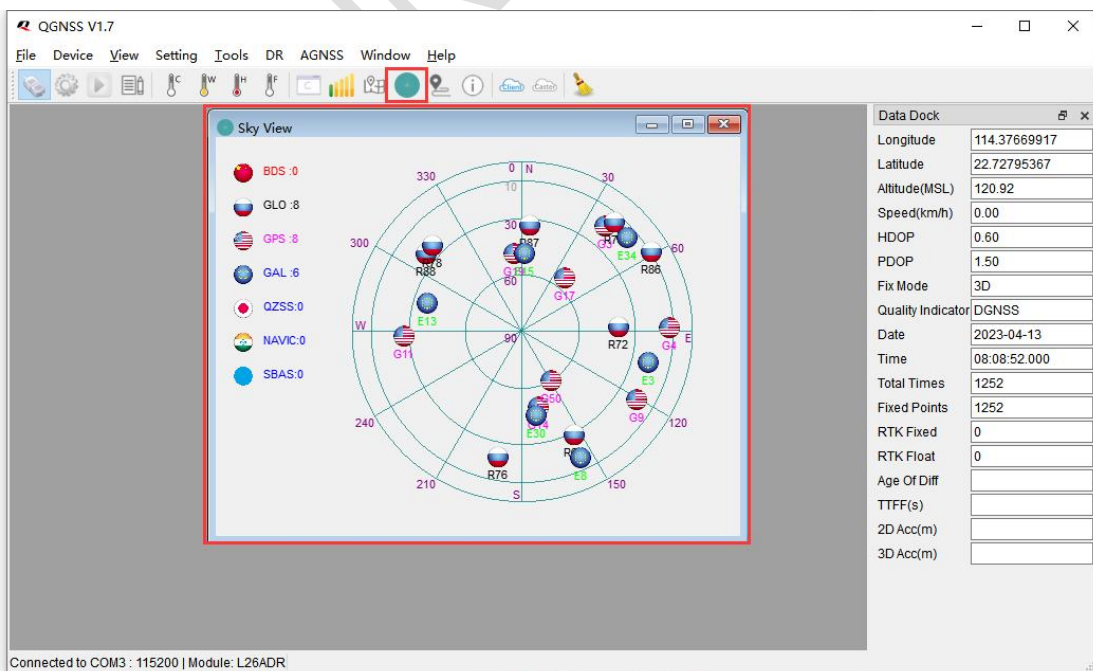
点击 GNSS 信号窗口  按钮，将显示以下界面。每个标志上方显示的数字是 C/No 值。下面显示的信息包括 PRN、卫星使用的频带 (“band”)、方位角 (“AZI”) 和卫星的高程 (“ELE”)。

卫星数目越多定位数据越准。



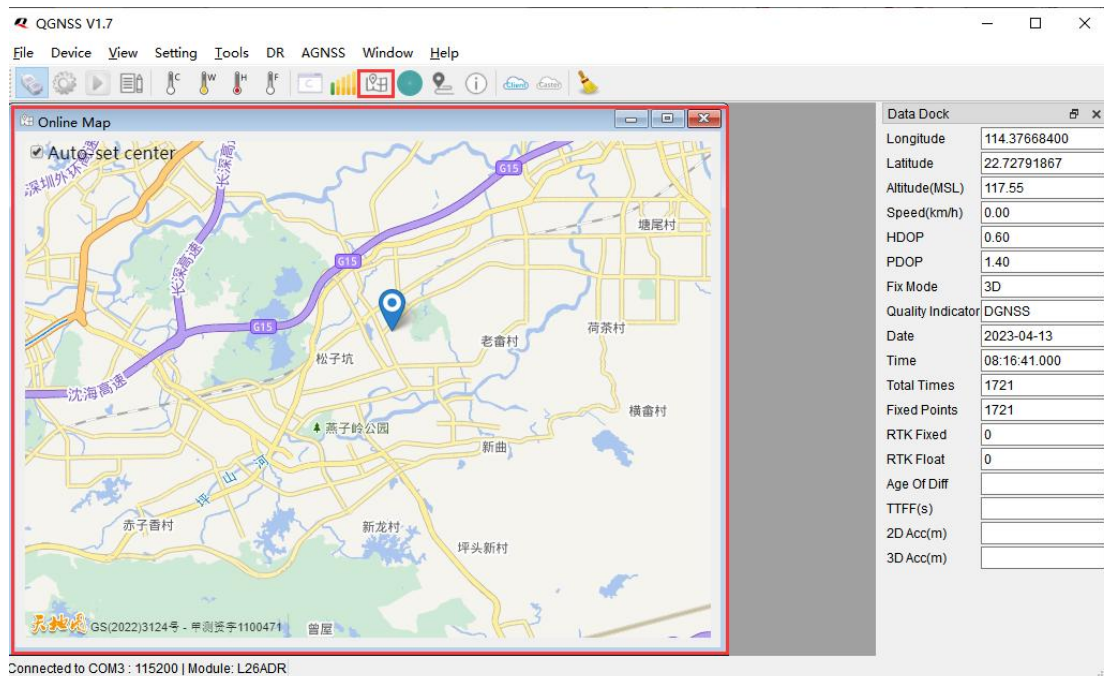
3.1.4 卫星观察

点击按钮后，将打开“卫星视图”，显示目前固定的卫星的方位角和仰角。



3.1.5 电子地图

点击电子地图  按钮,将显示设备所在地区地图及其位置, 地区地图可放大缩小查看其准确位置。



3.4 数据格式

GPS 数据还可以通过连接 4002 端口用 TCP、UDP 通信协议获取。数据自动上报到 4002 端口。

① \$GPRMC,<1>,<2>,<3>,<4>,<5>,<6>,<7>,<8>,<9>,<10>,<11>,<12>*hh

例:\$GPRMC,081027.000,A,3149.33388,N,11706.94688,E,0.0,0.0,140222,,D*66

<1> 标准定位时间(UTC time)格式: 时时分分秒秒。秒秒秒(hhmmss.sss)。

<2> 定位状态, A=数据可用, V=数据不可用。

<3> 纬度, 格式:度度分分.分分分分(ddmm.mmmm)。

<4> 纬度区分:北半球(N)或南半球(S)。

<5> 经度, 格式:度度分分.分分分分(ddmm.mmmm)。

<6> 经度区分:东半球(E)或西半球(W)。

<7> 相对位移速度, 0.0 至 1851.8knots

<8> 相对位移方向, 000.0 至 359.9 度。

<9> 日期, 格式: 日日月月年年(ddmmyy)。

<10> 磁极变化:不支持

<11> 磁极变化方向:不支持

<12> 模式指示(仅 NMEA0183 3.00 版本输出, A=自主定位, D=差分, E=估算, N=数据无效)*后 hh 为\$到*所有字符的异或和。

②\$GPGGA,<1>,<2>,<3>,<4>,<5>,<6>,<7>,<8>,<9>,<10>,<11>,<12>*hh

例:\$GPGGA,082233.000,3149.33371,N,11706.94684,E,2,16,0.8,054.42,M,-0.3,M,,*7D

- <1> 标准定位时间(UTC time)格式: 时时分分秒秒。秒秒秒(hhmmss.sss)。
- <2> 纬度, 格式: 度度分分.分分分分(ddmm.mmmm)。
- <3> 纬度区分: 北半球(N)或南半球(S)。
- <4> 经度, 格式: 度度分分.分分分分(ddmm.mmmm)。
- <5> 经度区分: 东半球(E)或西半球(W)。
- <6> GPS 状态: 0=未定位, 1=非差分定位, 2=差分定位, 6=正在估算
- <7> 正在使用解算位置的卫星数量 (00~12) (前面的 0 也将被传输)。
- <8> HDOP 水平精度因子 (0.5~99.9)。
- <9> 海拔高度 (-9999.9~99999.9)。
- <10> 地球椭球面相对大地水准面的高度
- <11> 差分时间: 不支持
- <12> 模式指示(仅 NMEA0183 3.00 版本输出, 差分站 ID 不支持) *后 hh 为\$到*所有字符的异或和。

③\$GPVTG,<1>,T,<2>,M,<3>,N,<4>,K,<5>*hh

例:\$GPVTG,0.0,T,,M,0.1,N,0.2,K,A*0E

- <1>以真北为参考基准的地面航向 (000~359 度, 前面的 0 也将被传输)
- <2>以磁北为参考基准的地面航向: 不支持
- <3>地面速率 (000.0~999.9 节, 前面的 0 也将被传输)
- <4>地面速度 (0000.0~1851.8 公里/小时, 前面的 0 也将被传输)
- <5>模式指示 (仅 NMEA0183 3.00 版本输出, A =自主定位, D =差分, E =投放, N =数据无效) *后 hh 为\$到*所有字符的异或和。

④\$GPGSA, <1>, <2>, <3>, <4>, <5>, <6>, <7>, <8>, <9>, <10>, <11>, <12>, <13>, <14>, <15>, <16>, <17>, <18>

例:\$GNGSA,A,3,08,07,01,30,27,14,17,,,,,1.1,0.7,0.9*29

- <1> 模式: M =手动, A =自动。
- <2> 定位型式 1 =未定位, 2 =二维定位, 3 =三维定位。
- <3> 到<14> PRN 数字: 01 至 32 表天空使用中的卫星编号, 最多可接收 12 颗卫星信息
- <15> HDOP 水平精度因子 (0.5~99.9)
- <16> VDOP 垂直精度因子 (0.5~99.9)
- <17> 模式指示 (仅 NMEA0183 3.00 版本输出, GNSS 系统 ID) *后 hh 为\$到*所有字符的异或和。

⑤\$GPGSV, <1>, <2>, <3>, <4>, <5>, <6>, <7>, <8>, <9>, <10>, <11>, <12>, <13>, <14>, <15>, <16>, <17>, <18>

例:\$GPGSV,3,1,12,20,66,289,38,11,59,348,37,02,57,343,36,06,46,063,36*70

\$GPGSV,3,2,12,05,40,250,38,19,37,142,28,12,29,256,34,09,23,049,29*77

\$GPGSV,3,3,12,17,18,143,31,25,15,298,30,13,11,184,,50,51,161,31*78

\$GLGSV,2,1,06,68,71,186,34,82,54,074,38,67,51,035,33,83,48,352,23*62

\$GLGSV,2,2,06,69,19,203,20,81,16,115,,,,,,*6C

- <1> GSV 语句的总数, 范围 1-8。
- <2> 本句 GSV 的编号
- <3> 可见卫星的总数, 00 至 12。
- <4> 卫星编号, 01 至 32。
- <5> 卫星仰角, 00 至 90 度。
- <6> 卫星方位角, 000 至 359 度。实际值。

<7> 讯号噪声比 (C / No) , 00 至 99 dB; 无表未接收到讯号。

<8> 模式指示(仅 NMEA0183 3.00 版本输出, GNSS 信号 ID)*后 hh 为\$到*所有字符的异或和。

第<4>, <5>, <6>, <7>项单独的卫星会重复出现, 每行最多有四颗卫星。其余卫星信息会于次一行出现, 若未使用, 这些相邻会空白。

⑥\$GPGLL,<1>,<2>,<3>,<4>,<5>,<6>hh

例:\$GPGLL,3149.33233,N,11706.94768,E,083358.000,A,A*54

<1>纬度 ddmm.mmmm, 度分格式(前导位数不足则补 0)。

<2>纬度 N(北纬)或 S(南纬)。

<3>经度 dddmm.mmmm, 度分格式(前导位数不足则补 0)。

<4>经度 E(东经)或 W(西经)。

<5>UTC 时间, hhmmss.sss 格式。

<6>状态, A=定位, V=未定位。

<7>模式指示(仅 NMEA0183 3.00 版本输出, A=自主定位, D=差分, E=估算, N=数据无效)*后 hh 为\$到*所有字符的异或和。

⑦\$PSTMDRSENMSG,<1>,<2>,<3><4>*hh

例:\$PSTMDRSENMSG,24,17186159,-787,1*2B

<1> MsgID=24。

<2> 自模块通电以来的 CPU 滴答计数。

<3> 实际温度: 摄氏度= $\frac{\text{<3>}}{256}+25.0$

<4> 模式指示 (0=温度无效, 1=温度有效) *后 hh 为\$到*所有字符的异或和

例:\$PSTMDRSENMSG,30,17370342,-2442,2272,16295*34

<1>MsgID=30;

<2>传感器帧中的原始带符号 16 位整数 X 轴加速度数据。

<3>传感器帧中的原始带符号 16 位整数 Y 轴加速度数据。

<4>传感器帧中的原始带符号 16 位整数 Z 轴加速度数据。

例:\$PSTMDRSENMSG,31,17370342,44,-5,-53*17

<1>MsgID=31;

<2>传感器帧中的原始带符号 16 位整数 Z 轴角速率数据。

<3>传感器帧中的原始带符号 16 位整数 Z 轴角速率数据。

<4>传感器帧中的原始带符号 16 位整数 Z 轴角速率数据。

⑧\$PSTMANTENNASTATUS,<1>,<2>,<3><4>*hh

例:\$PSTMANTENNASTATUS,0,0,0,0*51

<1> 当前天线状态: -1:当前天线未初始化; 0=正常;1=打开;2=短路

<2> 操作模式: 0=自动-天线由软件逻辑自动管理

1=手动-天线的开/关状态或射频开关由命令控制

<3>当前射频路径:0=外部天线,1=内部天线

<4>天线电源状态。0=开启, 1=关闭。

第四章 防火墙及应用

4.1 防火墙开启与关闭

防火墙默认是开启的，在做 DMZ 和端口映射的时候需要将防火墙禁用，防火墙禁用步骤，导航栏“路由设置”——“防火墙”，防火墙选择禁用，然后点击“保存&应用”。



4.2 DMZ 设置

DMZ 功能可以把 WAN 口地址映射成 LAN 端的某一台主机；所有到 WAN 地址的包都会被转到指定的 LAN 端主机，以实现双向通信。实际上就是把内网中的一台主机完全暴露给互联网，开放所有端口，等同于全部端口映射。等于直接使用公网 IP。

首先需要将防火墙禁用，导航栏中“路由设置”——“DMZ 设置”，点击启用，设置 lan 口给下接设备分配的 ip 地址，将下接设备所有的端口转发出来，通过 wan 口的 ip 地址可以直接访问。

启用：将启用勾选。

内部 IP 地址：本机设备的 ip 或 lan 口为下接设备分配的 ip。

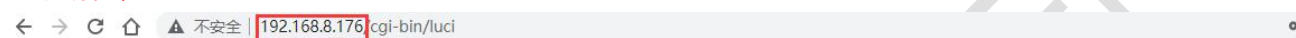
DMZ 实际上是将设备的所有端口转发出来，配置完成后点击“保存&应用”使其生效。



查看 wan 口 ip, 通过 wan 口的 ip 可以直接访问下接设备了, 如果访问不了可能原因是下接设备开了防火墙, 需要将下接设备的防火墙关闭。



直接通过 wan 口的 ip 就可以访问下接设备了。(注意: 电脑需要与 wan 口的 ip 在同一个局域网内才可以访问)



4.3 端口转发

相比 DMZ, 端口转发是更精细化控制, 可以把发往某一端口的数据包转发到 LAN 端的某一台主机, 可以实现把不同的端口转到不同的主机。

首先需要禁用防火墙。

导航栏中“路由设置”——“端口转发”设置菜单, 进入“端口转发”界面即可进行配置。

名字: 指定这条规则的名字, 可以起一个有意义的名字。

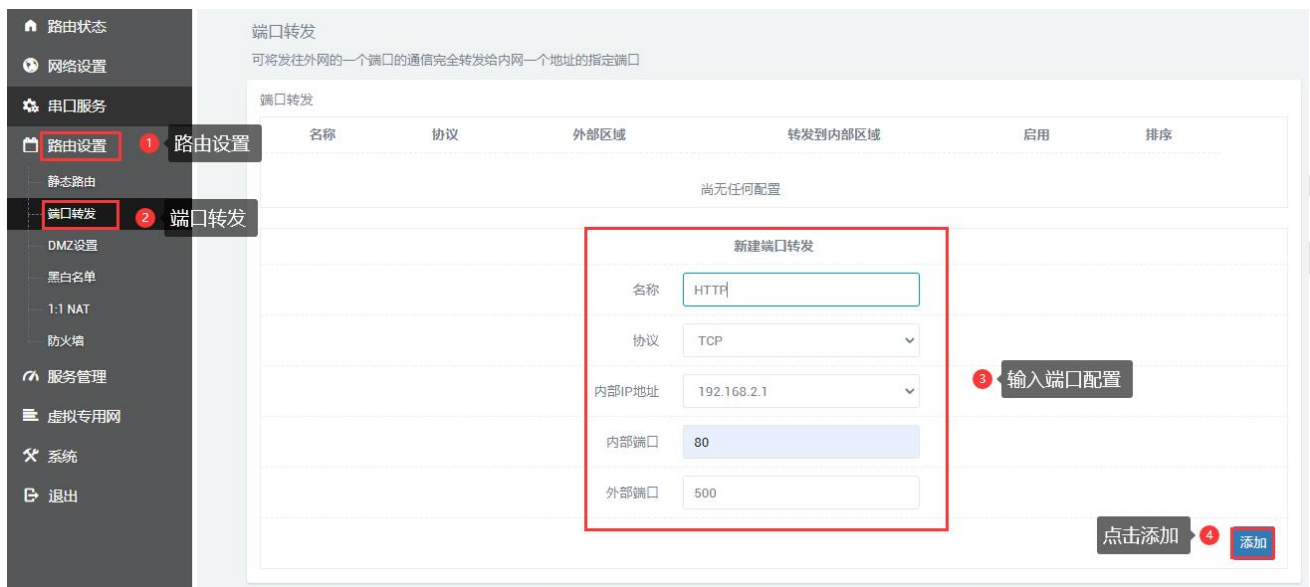
协议: 指定要转发的协议, 可以是 TCP, UDP, 或者 TCP/UDP。

内部 IP 地址: 选择需要转发到外网的 IP 地址。

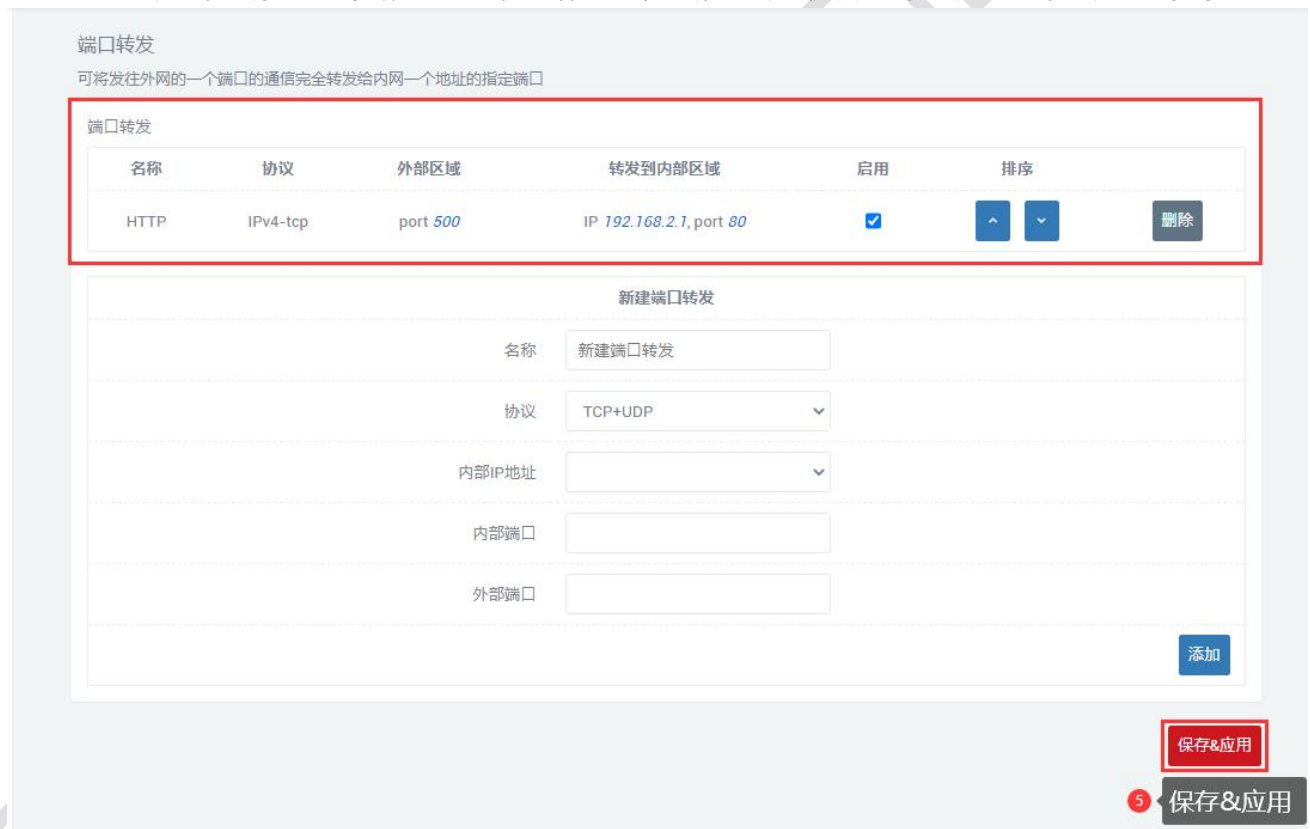
内部端口: 下接设备或本机要转发出来的端口。

外部端口: 通过 wan 口 ip 加这个外部端口即可访问下接设备。

配置完后, 点击“添加”按钮, 新增一条转发规则。点击“保存&应用”按钮, 使规则生效。



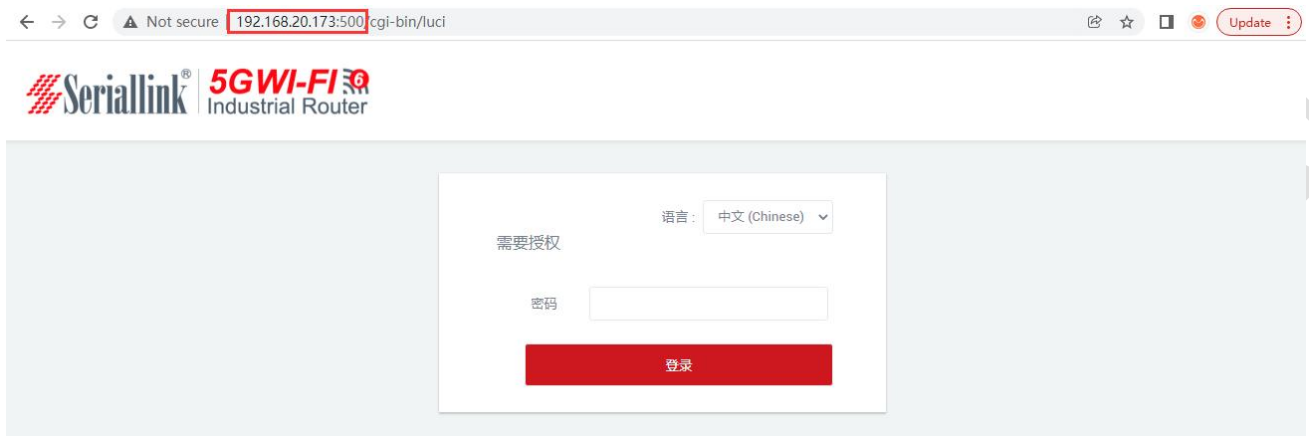
添加成功后，会多出一条端口转发的规则，点击“保存&应用”使该规则生效。规则可以添加多条。



查看 wan 口 ip，通过 wan 口 ip 与外部端口号即可访问下接设备或本机设备的内部端口。



通过 192.168.20.173:500 访问下接设备的内部端口。（注意：电脑需要与 wan 口的 ip 在同一个局域网内才可以访问）



4.4 黑白名单

4.4.1 白名单

限制所有非白名单的主机通过本机设备访问外部网络，例如禁止所有设备不能访问 Internet，只允许某一台电脑可以，则可以将这台电脑添加进白名单。

名称：自定义。

协议：默认选择所有协议，根据需要选择。

匹配 ICMP 类型：默认选择所有类型，根据需要选择。

本地 IP 地址：添加进白名单的设备 IP 地址，人为或其他原因导致的 IP 地址变动，会使能够访问 Internet 的设备发生变化。

本地 MAC 地址：添加进白名单的设备 MAC 地址，更换设备 IP 地址也不会失效。

目标地址：不选则表示所有网络，也可以输入 IP 地址，例如公网服务器 IP。

动作：白名单模式选择允许。



列表

名称	协议	本地	目标地址	动作	启用	排序
尚无任何配置						

新建名单

名称: 2.59

协议: 所有

匹配ICMP类型: 所有

本地IP地址: 192.168.2.59 (40:8d:5c:7a:f3:f7)

本地MAC地址:

目标IP地址: 106.55.4.1

动作: 允许

名称自定义, 本地IP地址和本地MAC地址选择其中一个, 这里目标地址选择的是服务器公网地址, 动作选择允许

添加

6 点击添加

保存&应用

点击添加后, 页面列表中会自动刷新出一条规则, 点击“保存&应用”即可。

列表

名称	协议	本地	目标地址	动作	启用	排序
2.59	所有	IP 192.168.2.59	IP 106.55.4.1	允许	☒	删除

新建名单

添加

7 保存&应用

保存&应用

添加白名单后, 只能访问服务器公网地址, 不能访问 Internet 了, 同时其他电脑既不能访问公网地址, 也不能访问 Internet 了。

```
C:\Users\Administrator>ping 106.55.4.1
正在 Ping 106.55.4.1: 具有 32 字节的数据:
来自 106.55.4.1 的回复: 字节=32 时间=10ms TTL=51
来自 106.55.4.1 的回复: 字节=32 时间=10ms TTL=51
来自 106.55.4.1 的回复: 字节=32 时间=10ms TTL=51
来自 106.55.4.1 的回复: 字节=32 时间=10ms TTL=51

106.55.4.1 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 = 10ms, 最长 = 10ms, 平均 = 10ms

C:\Users\Administrator>ping www.baidu.com
正在 Ping www.a.shifen.com [14.215.177.38] 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

14.215.177.38 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

如果目标地址为空, 则表示白名单内设备能够访问所有网络, 其他设备不行, 如果要关闭黑白名单功能, 只要取消启用的勾选, “保存&应用”即可。

4.4.2 黑名单

限制黑名单的主机通过本机设备访问外部网络，例如禁止某台电脑不能访问 Internet，则可以将这台电脑添加进黑名单。

名称：自定义。

协议：默认选择所有协议，根据需要选择。

匹配 ICMP 类型：默认选择所有类型，根据需要选择。

本地 IP 地址：添加进黑名单的设备 IP 地址，人为或其他原因导致的 IP 地址变动，会使拒绝访问 Internet 的设备发生变化。

本地 MAC 地址：添加进黑名单的设备 MAC 地址，更换设备 IP 地址也不会失效。

目标地址：不选则表示所有网络，也可以输入 IP 地址，例如公网服务器 IP。

动作：黑名单模式选择禁止。

点击添加后，页面列表中会自动刷新出一条规则，点击“保存&应用”即可。

添加黑名单后，就不能访问服务器公网地址，只能访问 Internet 了，其他设备不受限制。

```
C:\Users\Administrator>ping www.baidu.com

正在 Ping www.a.shifen.com [14.215.177.39] 具有 32 字节的数据:
来自 14.215.177.39 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.39 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.39 的回复: 字节=32 时间=9ms TTL=54
来自 14.215.177.39 的回复: 字节=32 时间=9ms TTL=54

14.215.177.39 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 = 9ms, 最长 = 9ms, 平均 = 9ms

C:\Users\Administrator>ping 106.55.

正在 Ping 106.55.    ■具有 32 字节的数据:
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。
来自 192.168.2.1 的回复: 无法连接到端口。

106.55. 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
```

如果目标地址为空，则表示黑名单内设备不能访问所有外部网络，如果要关闭黑白名单功能，只要取消启用的勾选，“保存&应用”即可。

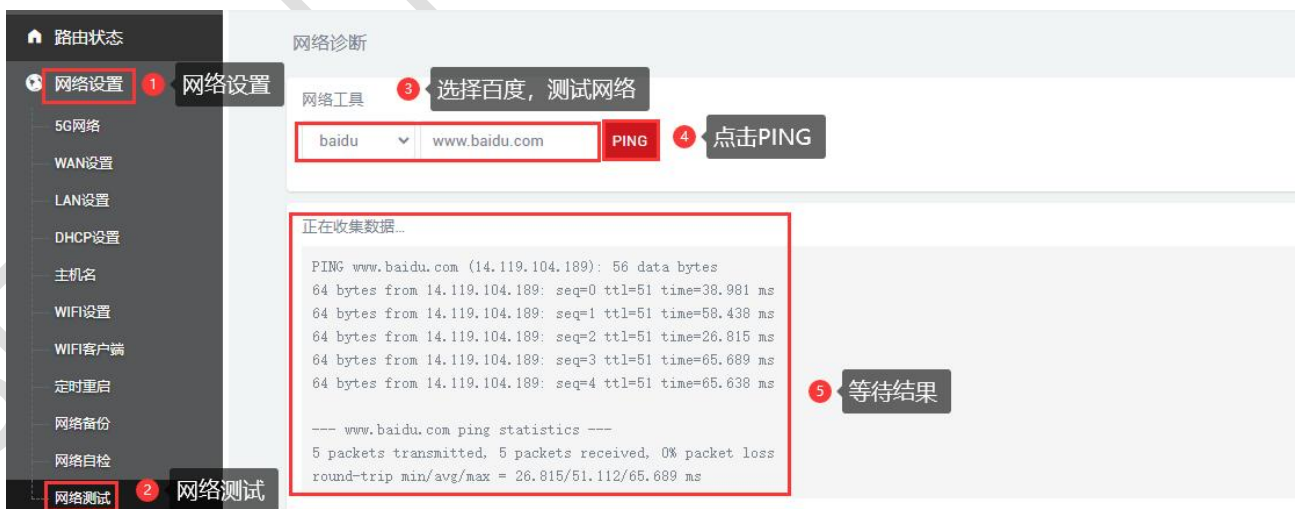
4.5 内网穿透 (frp)

Frp 是利用处于内网或防火墙后的机器，多外网环境提供 http 或 https 服务，对于 http，https 服务支持基于域名的虚拟主机，支持自定义域名绑定，使多个域名共用一个 80 端口；利用处于内网或防火墙后的机器，对外网环境提供 tcp 和 udp 服务，例如家里通过 ssh 访问处于公司内网环境内的主机。

Frp 主要实现的功能：外网通过 ssh 访问内网机器；外网通过公网地址加端口号访问内网机器通过 frp 转发出来的端口；自定义绑定域名访问内网 web 服务。

配置内网穿透的前提是要保证路由器能够上网，如果路由器不能上网，则做不了内网穿透。导航栏“网络设置”——“网络测试”；并且将防火墙禁用，导航栏“路由设置”——“防火墙”。

能 ping 通百度，说明设备能够上网。



将防火墙禁用，防火墙选择禁用后点击“保存&应用”。

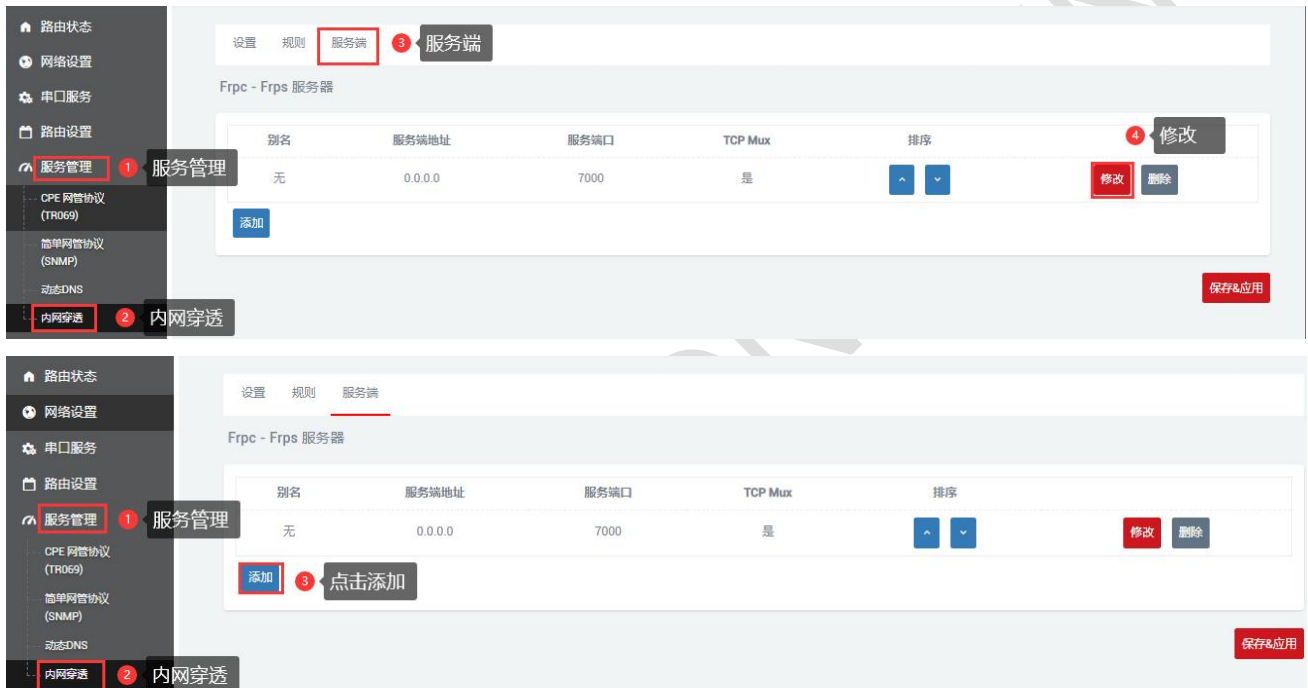
4.5.1 连接服务器

配置前准备：

- (1) 公网服务器 1 台。
- (2) 路由器 1 台（支持 frp 的路由器，即内网服务器 1 台）。
- (3) 公网服务器绑定域名 1 个。

frp 客户端配置如下：

(1) 客户端需要先添加服务端的配置来连接上服务端，导航栏“DDNS/FRP”——“内网穿透”，选择服务端，默认有一个空的服务端，可以直接点击修改，也可以直接删除自己添加一个。



(2) 点击“添加”或“修改”后会弹出一个编辑 frps 服务器的页面，根据服务端的设置进行配置，配置完成后点击“保存&应用”。

别名：自定义一个服务端的名字，可以定义一个有意义的名字。

服务端地址：服务端的地址（一般为公网 ip 地址）。

服务端端口：服务端端口。

令牌：服务端设置的密码。

TCP mux：与服务端一致，服务端设置了这里就要勾选，没有就不用勾选。

设置完成后点击“保存&应用”。

设置 规则 服务端

Frpc - 编辑 Frps 服务器

别名 frpc

服务端地址 106

服务端端口 5443

令牌 *****

TCP mux ☒

5 根据服务端配置端口、令牌、和TCP mux

返回至概况

保存&应用

6 保存&应用

(3) 添加成功后这里会多出一条 frpc 的服务器，点击“保存&应用”让服务端启动。

设置 规则 服务端

Frpc - Frps 服务器

别名	服务端地址	服务端端口	TCP Mux	排序	
frpc	106.55...	5443	是	↑ ↓	修改 删除

添加

(4) 接下来进入“内网穿透”的“设置”页面，启动 frpc 客户端，按照下图进行配置，配置完成后，点击“保存&应用”，配置完成后“设置”页面会出现“服务正在运行”，证明 frp 客户端已经启动了。

已启用：将已启用勾选上。

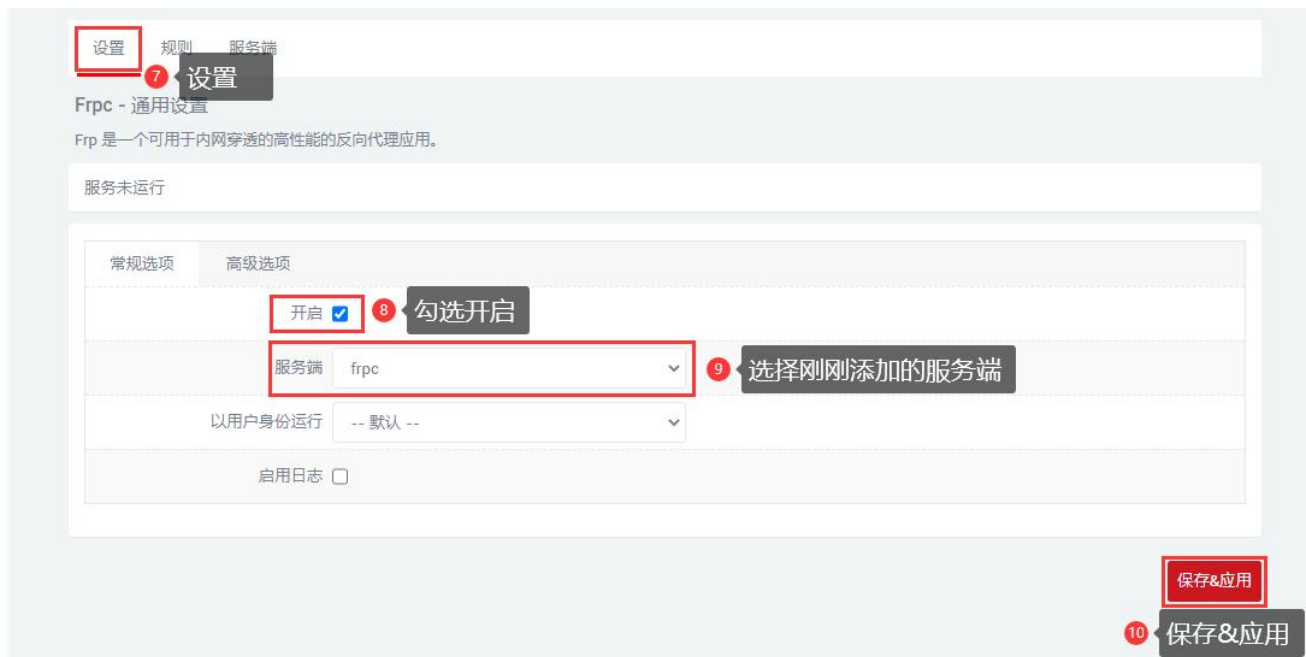
客户端文件：不需要修改，系统自动匹配的，默认就可以了。

服务端：刚刚自定义的服务端别名。

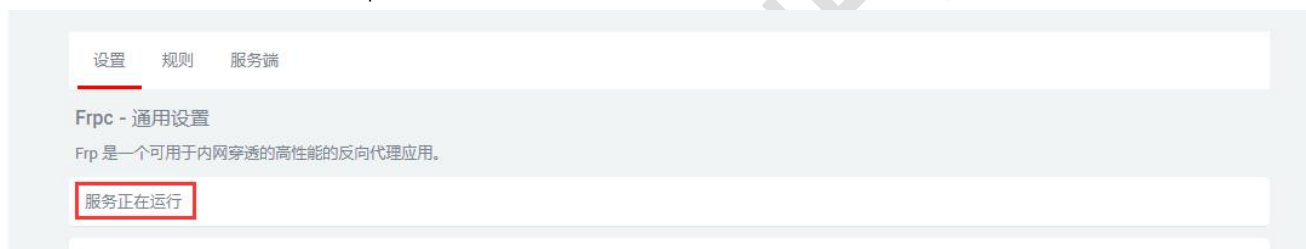
以用户身份运行：一般选择默认，可以根据需要自行修改。

启用日志：根据需要勾选。

配置完成后点击“保存&应用”。



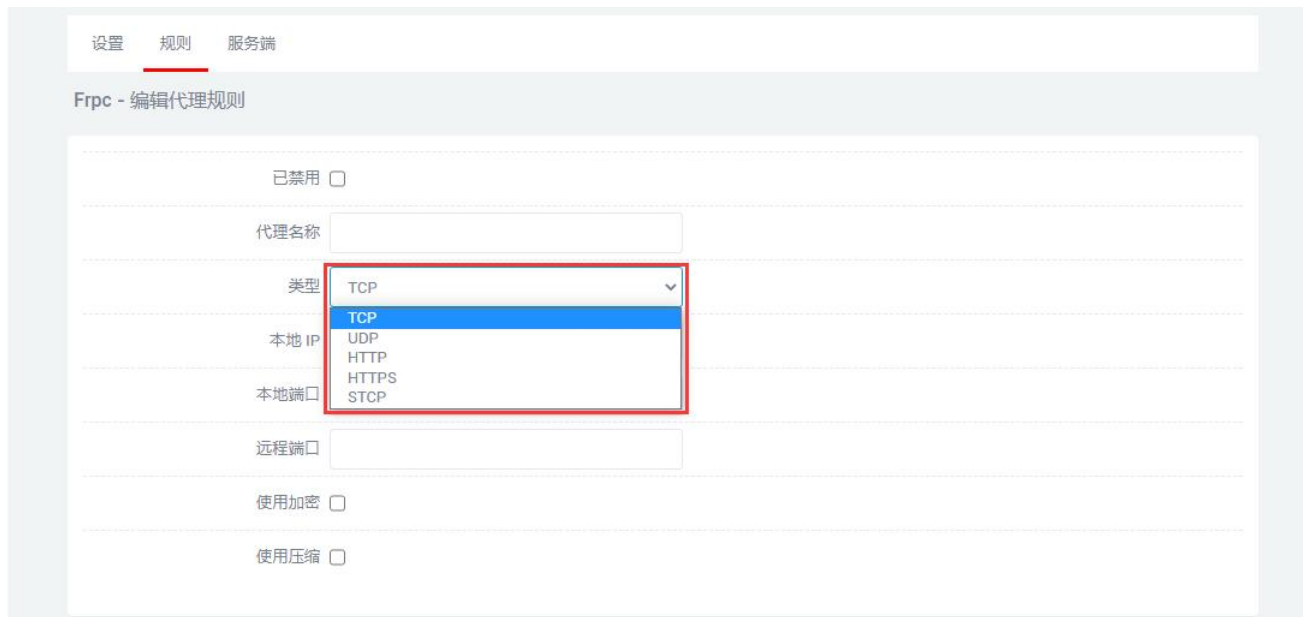
显示服务正在运行说明 frp 客户端启动成功。



(5) 接下来进入“内网穿透”的“规则”页面，点击“添加”，默认有一条规则，如果不需要这个规则可以删除这个规则，需要的话就保留，直接添加新的规则。



(6) 添加后会弹出一个“编辑代理规则”的页面，会有不同的协议类型，不同的协议类型实现的功能是不一样的。



4.5.2 添加 TCP 代理协议

TCP 协议支持 ssh 连接，也支持将页面端口（一般都是 80 端口）转发出来，通过公网:远程端口即可访问本地设备的页面。

在“编辑代理规则”页面根据需求按下图方式进行配置，配置完成后，点击“保存&应用”，会回到“代理规则”的页面，页面上会多出一条规则，再次点击“保存&应用”，使得规则生效，最后通过公网 ip:端口号（格式：106.107.108.109:3333 其中 106.107.108.109 是公网地址）即可访问本地设备所开放的本地端口。可以添加多个 tcp 规则，只需要保证远程端口不要一样即可，远程端口如果和前面设置过得一样，最新的将会覆盖之前的，之前的规则将不生效。

已禁用：如果勾选代表禁用这条规则。

代理名称：自定义一个代理名称，代理名称不可重复，否则会因为冲突而不生效。

类型：选择 TCP 协议。

本地 ip：填写本机的 ip 或者本机 lan 口为下接设备分配的 ip。（需要通过公网访问的设备的 ip 地址）。

本地端口：该设备需要转发到公网的端口。

远程端口：公网地址加这个远程端口即可访问对应的本地设备开放的本地端口，这个端口号不要和其他规则一样，并且不要使用已经被占用的端口，否则这条规则将不生效。

使用加密，使用压缩：这两个根据需要进行勾选。

规则可以添加多条，远程端口号不要冲突就可以了。

配置完成后点击“保存&应用”。

设置 规则 服务端

Frpc - 编辑代理规则

已禁用 ☐

代理名称 HTTP

类型 TCP

本地 IP 127.0.0.1

本地端口 80

远程端口 3333

使用加密 ☐

使用压缩 ☐

1 配置转发规则，这里是把此设备的80端口也就是网页转发出去，就能通过服务器IP加端口号访问

返回至概况

保存&应用

2 保存&应用

生成了一条新的规则后，需要点击“保存&应用”使规则生效。

设置 规则 服务端

Frpc - 代理规则

已禁用	名称	类型	本地 IP	本地端口	远程端口	排序	
☐	ssh	TCP	127.0.0.1	22	6000	^ v	修改 删除
☐	HTTP	TCP	127.0.0.1	80	3333		修改 删除

添加

保存&应用

3 保存&应用

通过公网 ip 和端口号访问本地设备的本地端口, 106.107.108.109:3333 访问 192.168.2.1 (默认 80 端口)。

← → ↻ Not secure 106.107.108.109:3333/cgi-bin/luci ☆ ⓘ Update

需要授权

语言: 中文 (Chinese)

密码

登录

可以添加多个 tcp 规则，需要保证远程端口号还有代理别称与之前设置的不要重复，如果重复了，可能导致该规则即使存在但是不会生效。

4.5.3 添加 STCP 代理协议

(1) STCP 需要配置客户端和访问端，其中 192.168.2.227 (lan 口下接设备) 作为客户端，PC 作为访问端，访问端可通过绑定本地 IP 和端口访问客户端。

已禁用：这里勾选的话会禁用这条规则。

代理名称：自定义一个代理名称，不能和其他规则一样，否则会因为冲突而不生效。

类型：选择 STCP 协议。

本地 IP：本机设备或 lan 口为下接设备分配的 IP 地址。

本地端口：该设备要开放到公网的端口。

SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

使用加密，使用压缩：根据需要进行配置。

角色，服务端名称，绑定地址，绑定端口：这四个作为客户端不需要设置。

设置 规则 服务端

Frcp - 编辑代理规则

已禁用 ☐

代理名称 stcp1

类型 STCP

本地 IP 192.168.2.104

本地端口 4001

使用加密 ☐

使用压缩 ☐

角色

服务端名称

SK

绑定地址

绑定端口

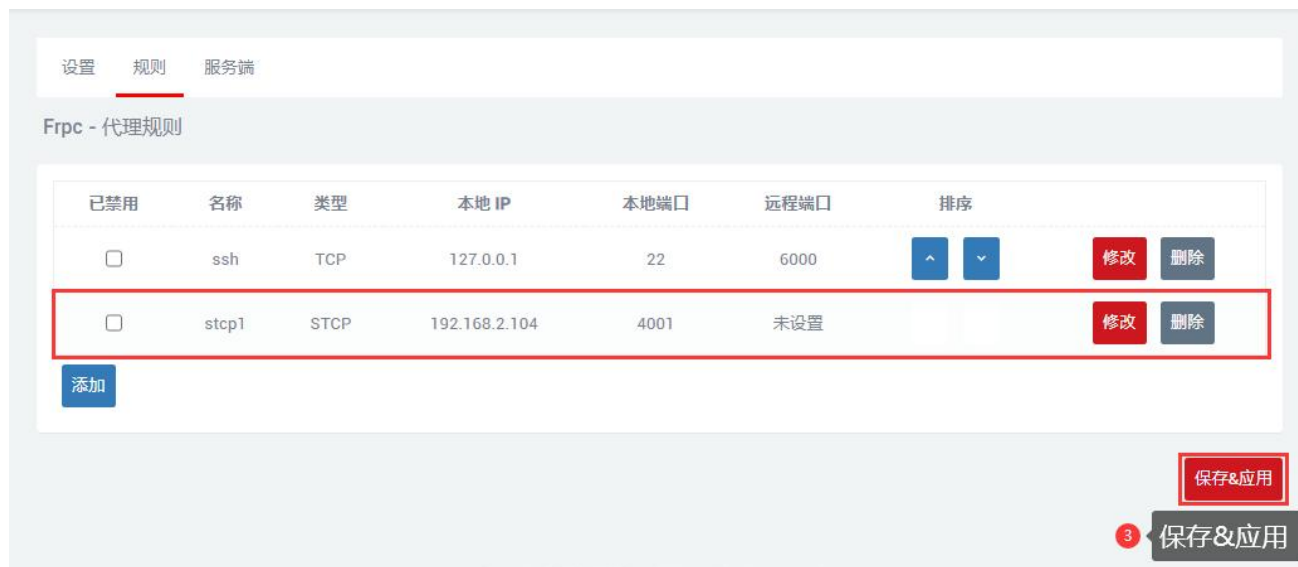
1 这里192.168.2.104,4001是指转发的同一网络内的一个串口服务器的4001端口，空白处不需要填写

2 保存&应用

保存&应用

返回至概况

生成了新的规则后，需要点击“保存&应用”使该规则生效。



PC 要想作为访问端访问路由器的下接设备，需要做一个 frp 的客户端，并且也是 stcp 协议，但是要设定 visitor 角色和绑定本地地址和端口。Windows 的 frp 文件可到公司官网下载。下载后打开 frpc_602.ini 配置文件进行配置。



frpc_602.ini - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
#服务端公网IP地址
server_addr=
#服务端端口
server_port=5443
#服务端提供用于验证的令牌
token=slk100200
#通过tcp协议连接服务端
protocol=tcp
#和服务端配置保持一致
tcp_mux=true
#防止一次连接失败即退出
login_fail_exit=false
```

与公网服务器配置一致即可

#连接客户端1-192.168.2.6

[stcp1_visitor]

#选择STCP协议

type =stcp

#以访问者的角色

role=visitor

访问端角色要设置visitor

#客户端1的代理名称

server_name=stcp1

要与要访问的客户端的代理名称一致

#与客户端1的SK一致

sk=slk100200

#绑定本地地址和端口用于访问客户端1

bind_addr=127.0.0.1

bind_port=6005

一般设置为本地的ip地址 (127.0.0.1) , 端口号要本地没有使用的

利用快捷键“win+R”，快速打开 cmd 命令行。

运行



Windows 将根据你所输入的名称，为你打开相应的程序、文件夹、文档或 Internet 资源。

打开(O):

cmd

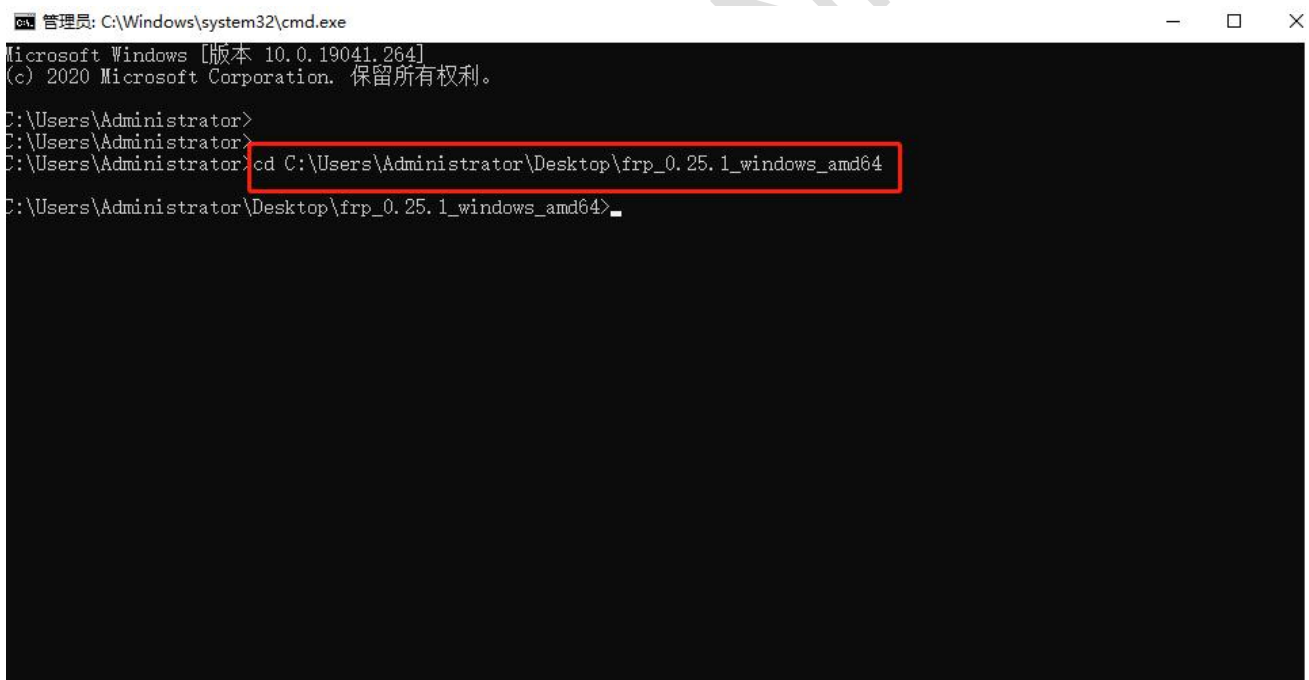
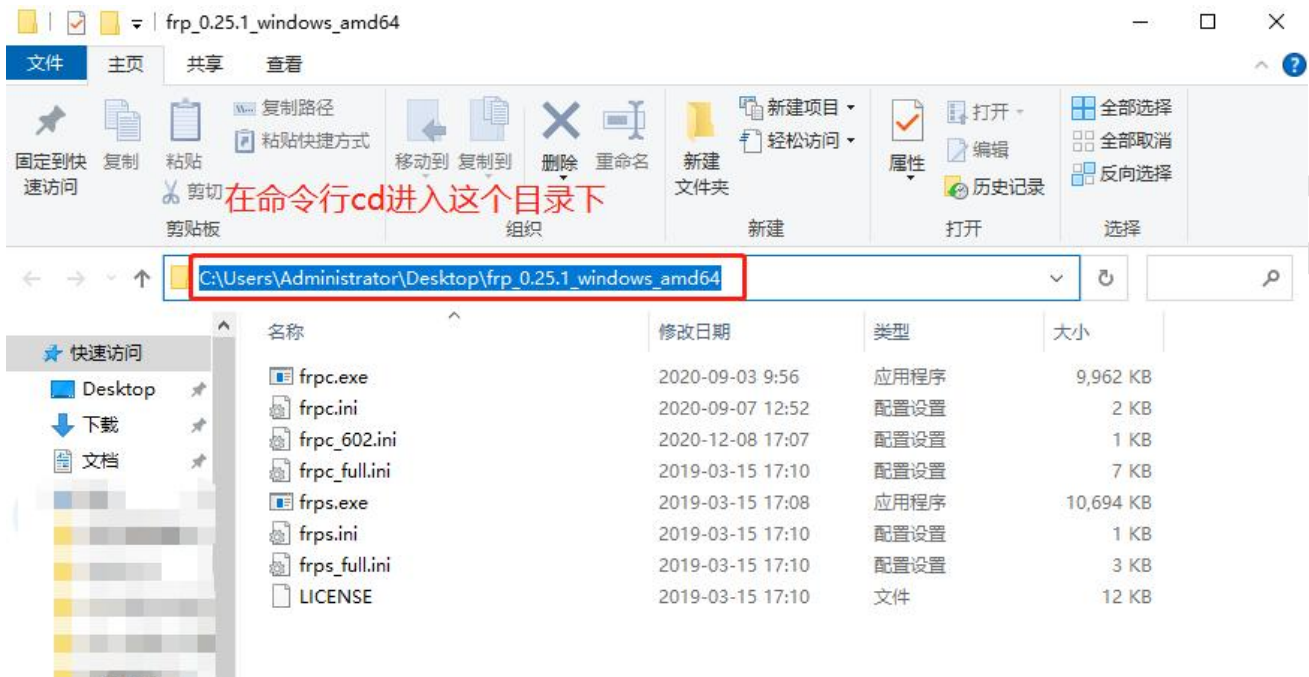


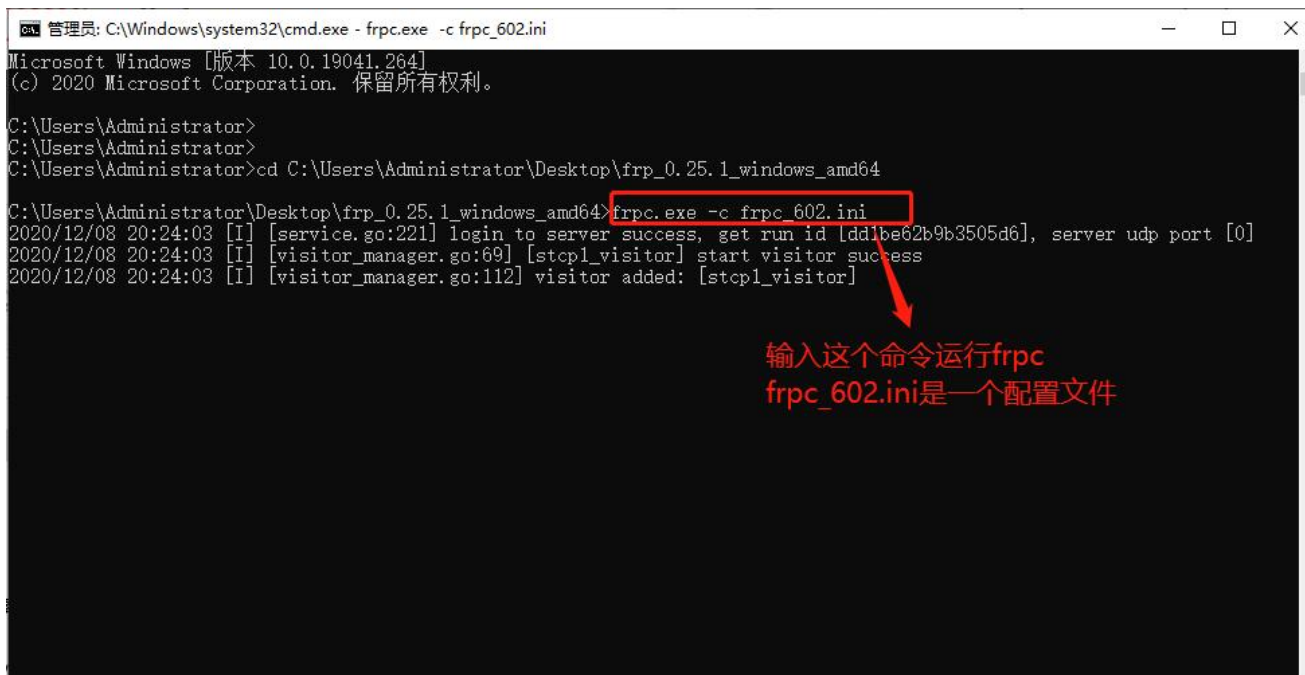
使用管理权限创建此任务。

确定

取消

浏览(B)...



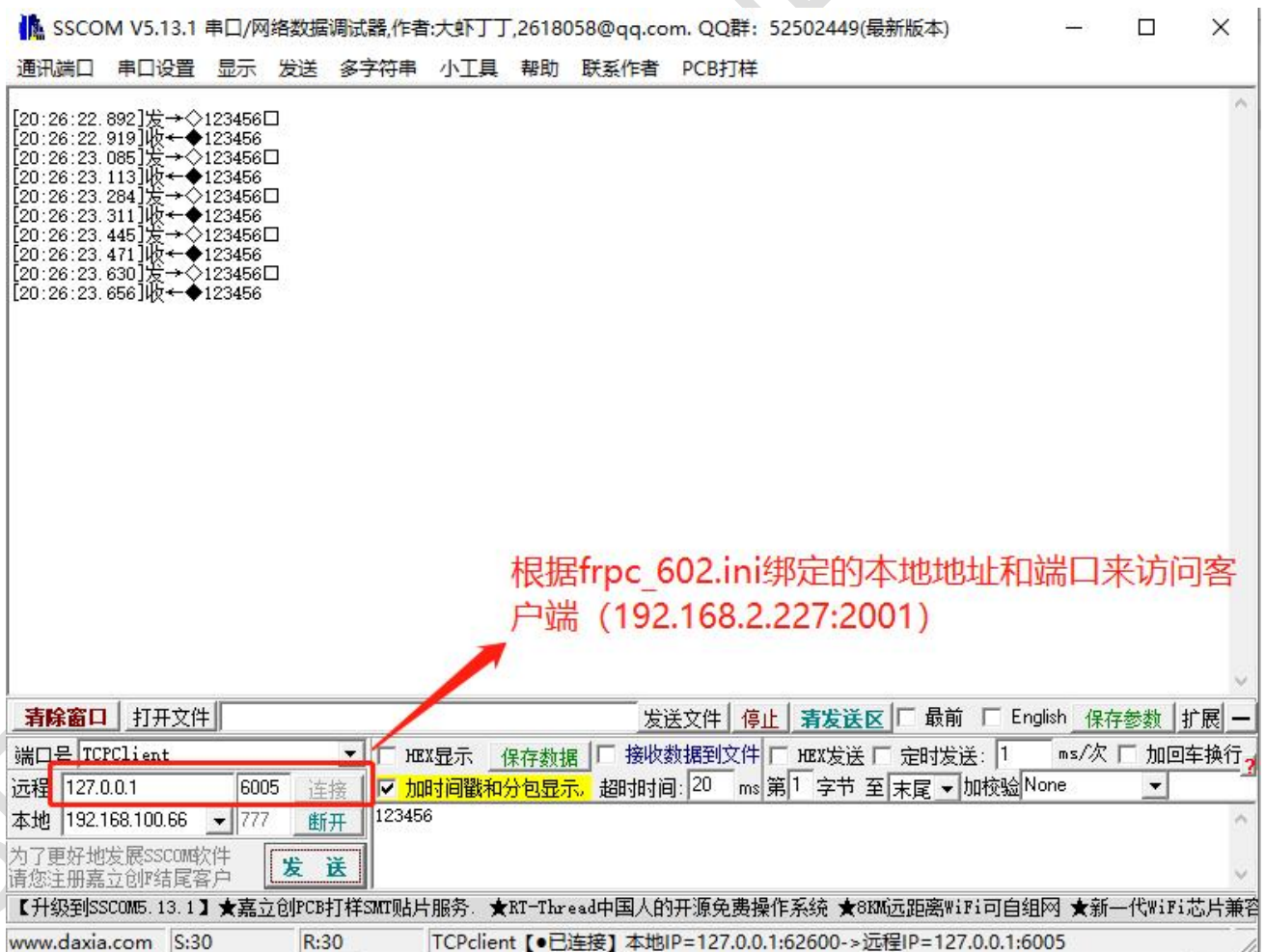


```

管理员: C:\Windows\system32\cmd.exe - frpc.exe -c frpc_602.ini
Microsoft Windows [版本 10.0.19041.264]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>
C:\Users\Administrator>
C:\Users\Administrator>cd C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64>frpc.exe -c frpc_602.ini
2020/12/08 20:24:03 [I] [service.go:221] login to server success, get run id [dd1be62b9b3505d6], server udp port [0]
2020/12/08 20:24:03 [I] [visitor_manager.go:69] [stcp1_visitor] start visitor success
2020/12/08 20:24:03 [I] [visitor_manager.go:112] visitor added: [stcp1_visitor]
  
```

输入这个命令运行frpc
frpc_602.ini是一个配置文件



(2) 如果有两台路由器，有一台路由器要远程访问另一台路由器或另一台路由器的下接设备，则一台做 stcp 访问端，另一台做 stcp 客户端。

配置如下：

① 配置客户端（第一台路由器）

添加新的规则，配置完成后点击“保存&应用”。

已禁用：这里勾选的话会禁用这条规则。

代理名称：自定义一个代理名称，不能和其他规则一样，否则会因为冲突而不生效。

类型：选择 STCP 协议。

本地 IP：本机设备或 lan 口为下接设备分配的 IP 地址。

本地端口：该设备要开放到公网的端口。

SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

使用加密，使用压缩：根据需要进行配置。

角色，服务端名称，绑定地址，绑定端口：这四个作为客户端不需要设置。

设置 规则 服务端

Frpc - 编辑代理规则

已禁用 ☐

代理名称	stcp1
类型	STCP
本地 IP	192.168.2.104
本地端口	4001
使用加密	☐
使用压缩	☐
角色	
服务端名称	
SK	*****
绑定地址	
绑定端口	

1 这里192.168.2.104,4001是指转发的同一网络内的一个串口服务器的4001端口，空白处不需要填写

返回至概况

保存&应用

2 保存&应用

生成了新的规则后，需要点击“保存&应用”使该规则生效。

Frpc - 代理规则

已禁用	名称	类型	本地 IP	本地端口	远程端口	排序	
☐	ssh	TCP	127.0.0.1	22	6000	^ v	修改 删除
☐	stcp1	STCP	192.168.2.104	4001	未设置		修改 删除

添加

保存&应用

3 保存&应用

② 配置访问端（另一台路由器 SLK-R680）

添加新的规则，配置完成后点击“保存&应用”。

已禁用：这里勾选的话会禁用这条规则。

代理名称：自定义一个代理名称，不能和其他规则一样，否则会因为冲突而不生效。

类型：选择 STCP 协议。

本地 IP，本地端口：这两个访问端可以不用填写。

SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

使用加密，使用压缩：根据需要进行配置。

角色：访问端要填写 visitor。

服务端名称：刚刚客户端设置的 stcp 代理名称。

绑定地址，绑定端口：通过绑定地址和端口可以访问客户端，地址和端口是本机或者本机的下接设备。

设置 规则 服务端

Frpc - 编辑代理规则

已禁用 ☐

代理名称 stcp1_visitor

类型 STCP

本地 IP

本地端口

使用加密 ☐

使用压缩 ☐

角色 visitor

服务端名称 stcp1

SK

绑定地址 192.168.2.123

绑定端口 6000

1 输入配置

2 保存&应用

返回至概况

保存&应用

生成了新的规则后，需要点击“保存&应用”使该规则生效。

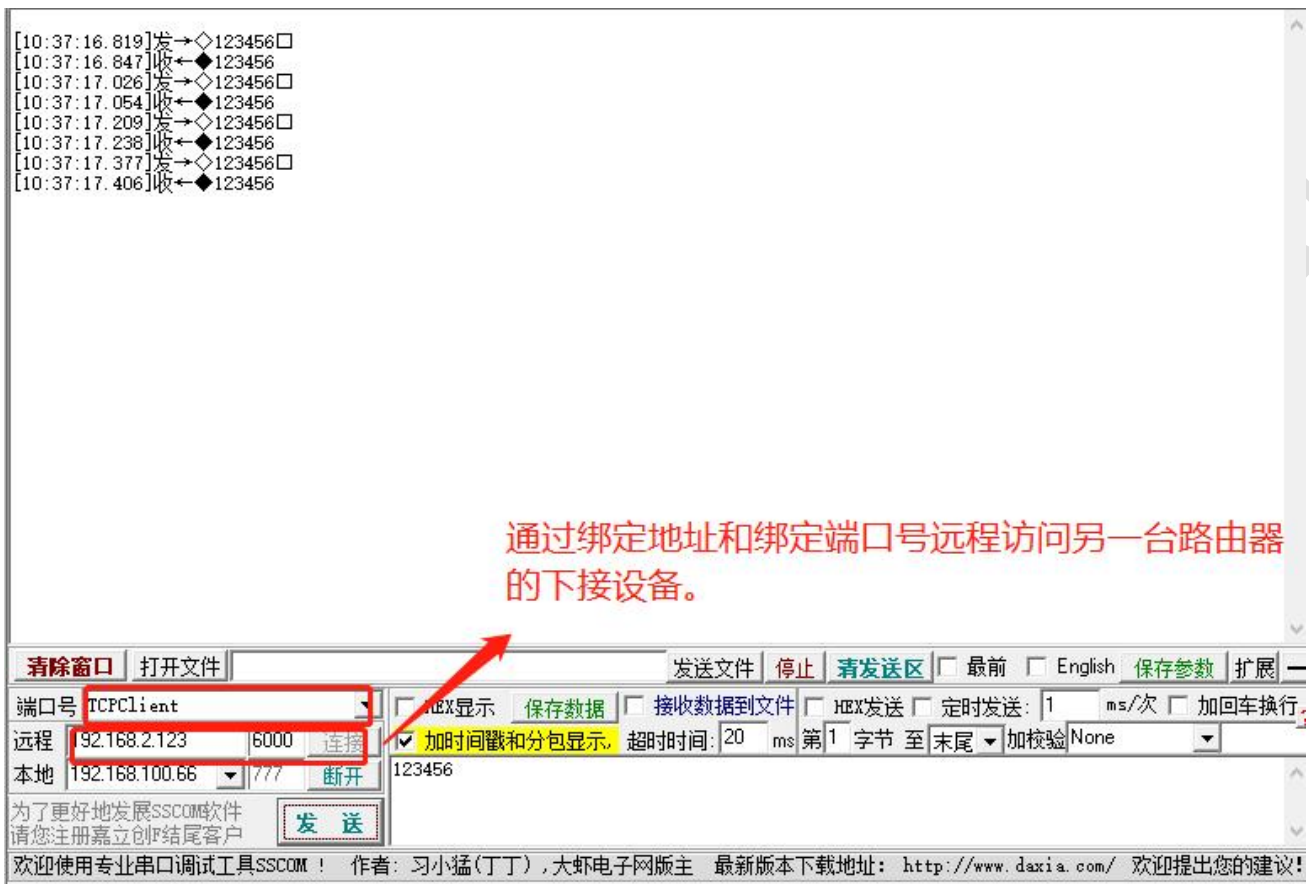
Frpc - 代理规则

已禁用	名称	类型	本地 IP	本地端口	远程端口	排序		
☐	ssh	TCP	127.0.0.1	22	6000		修改	删除
☐	stcp1_visitor	STCP	?	?	未设置		修改	删除

添加

3 保存&应用

保存&应用



4.5.4 添加 UDP 代理协议

UDP 协议是用于传输大量数据的，需要下接设备的端口支持 udp 协议，将支持 udp 协议的端口开放到公网上，即可通过公网加远程端口号进行数据传输。可配置多条 udp 协议规则。

添加新的规则，配置完成后点击“保存&应用”。

已禁用：这里勾选代表禁用这条规则。

代理名称：自定义一个代理名称，代理名称不可重复，否则会因为冲突而导致规则不生效。

类型：选择 UDP 协议。

本地 ip：填写本机的 ip 或者本机 lan 口为下接设备分配的 ip。（需要通过公网访问的设备的 ip 地址）

本地端口：该设备需要转发到公网的端口，必须是使用 UDP 协议的端口。

远程端口：公网地址加这个远程端口即可访问对应的本地设备开放的本地端口，这个端口号不要和其他规则一样，并且不要使用已经被占用的端口，否则这条规则将不生效。

使用加密，使用压缩：这两个根据需要进行勾选。

规则可以添加多条，远程端口和代理名称不要冲突就可以了。

配置完成后点击“保存&应用”。

设置

规则

服务端

Frpc - 编辑代理规则

已禁用 ☐

代理名称

类型

本地 IP

本地端口

远程端口

使用加密 ☐

使用压缩 ☐

1 选择UDP，输入配置

2 保存&应用

返回至概况

保存&应用

生成了新的规则后，需要点击“保存&应用”使该规则生效。

设置

规则

服务端

Frpc - 代理规则

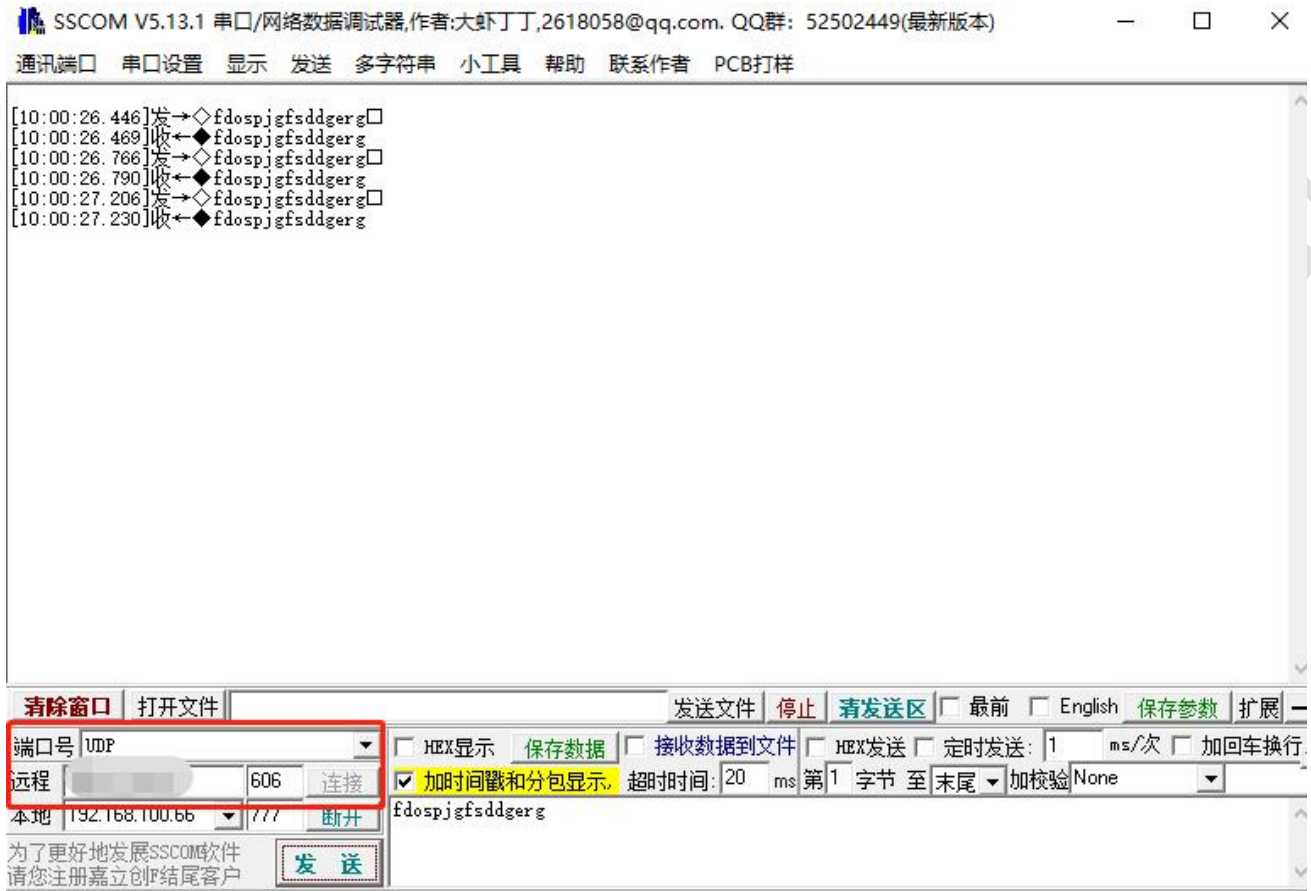
已禁用	名称	类型	本地 IP	本地端口	远程端口	排序	
☐	ssh	TCP	127.0.0.1	22	6000	^ v	修改 删除
☐	udp1	UDP	192.168.2.106	4001	606		修改 删除

添加

3 保存&应用

保存&应用

通过 UDP 协议，采用公网地址和远程端口号访问转发到公网的设备（111.111.111.111:606 访问 192.168.2.105:4001）。



4.5.5 添加 HTTP 代理协议

对于 http, https 服务支持基于域名的虚拟主机, 支持自定义域名绑定, 使多个域名共用一个 80 端口, 通过自定义域名访问内网 web 页面。可以配置多条 http 规则, 通过自定义域名可以直接访问。配置完成后通过自定义域名加服务端提供的 http 穿透端口 (即 vhost_http_port) 就可以访问对应的 web 页面了。

添加新的规则, 配置完成后点击“保存&应用”。

已禁用: 这里勾选代表禁用这条规则。

代理名称: 自定义一个代理名称, 代理名称不可重复, 否则会因为冲突而导致规则不生效。

类型: 选择 HTTP 协议。

本地 ip: 填写本机的 ip 或者本机 lan 口为下接设备分配的 ip (需要通过公网访问的设备的 ip 地址)。

本地端口: 该设备需要转发到公网的端口, 这个端口要是内部页面的端口号。

使用加密, 使用压缩, HTTP 用户, HTTP 密码: 这四个根据需要进行勾选。

子域名: 有就写, 没有可以不写。

自定义域名: xxx.公网绑定的域名, xxx 自己定义, 但是后面一定是公网绑定的域名。

设置

规则

服务端

Frpc - 编辑代理规则

已禁用 ☐

代理名称

类型

本地 IP

本地端口

使用加密 ☒

使用压缩 ☒

HTTP 用户

HTTP 密码

子域名

自定义域名

1 输入配置

返回至概况

保存&应用

2 保存&应用

生成了新的规则后，需要点击“保存&应用”使该规则生效。

设置

规则

服务端

Frpc - 代理规则

已禁用	名称	类型	本地 IP	本地端口	远程端口	排序	
☐	ssh	TCP	127.0.0.1	22	6000	^ v	修改 删除
☐	http1	HTTP	192.168.2.105	80	未设置		修改 删除

添加

保存&应用

3 保存&应用

浏览器登录 openwrt1.frp1.sifangtx.com:8080 可进入客户端路由管理页面，其中 8080 端口是服务器提供的内网穿透端口（即 vhost_http_port），openwrt1.frp1.sifangtx.com 是自定义域名。

可以通过这种方式配置多个 http 规则，自定义域名不要一样即可。

第五章 VPN（虚拟专用网）

5.1 PPTP VPN

导航栏“虚拟专用网”——“PPTP VPN”,选择启用,填写服务器地址,根据服务器的设置填写用户名和密码,点击“保存&应用”。

启用:要使用 PPTP VPN 需要将其勾选,不使用的时候直接不勾选就可以了。

服务端地址:服务端 ip 地址,一般是公网 ip。

用户名,密码:填写服务端设置的用户名和密码。



连接成功后状态栏会出现服务器给它分配的地址,如果不用 pptp 的话,将启用取消勾选后点击“保存&应用”即可。



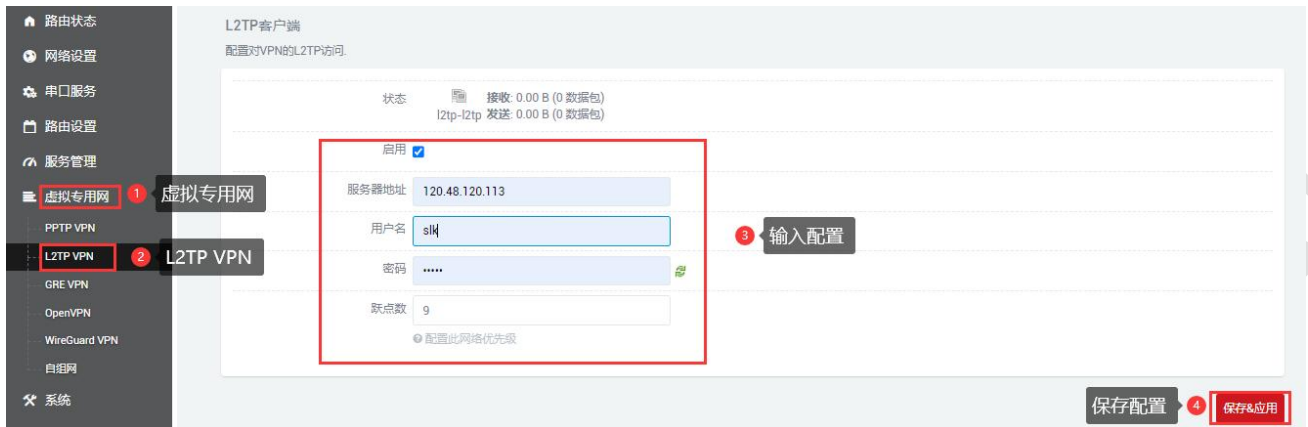
5.2 L2TP VPN

导航栏“虚拟专用网”——“L2TP VPN”,选择启用,根据服务器的设置填写用户名和密码,点击“保存&应用”。

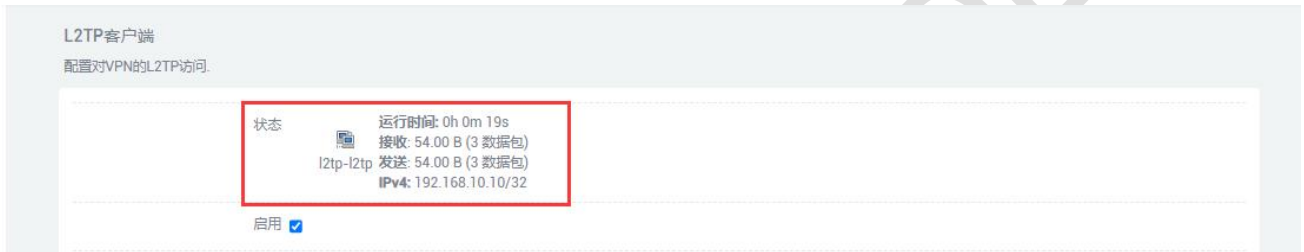
启用:要使用 L2TP VPN 需要将其勾选,不使用的时候直接不勾选就可以了。

服务端地址:服务端 ip 地址,一般是公网 ip。

用户名,密码:填写服务端设置的用户名和密码。

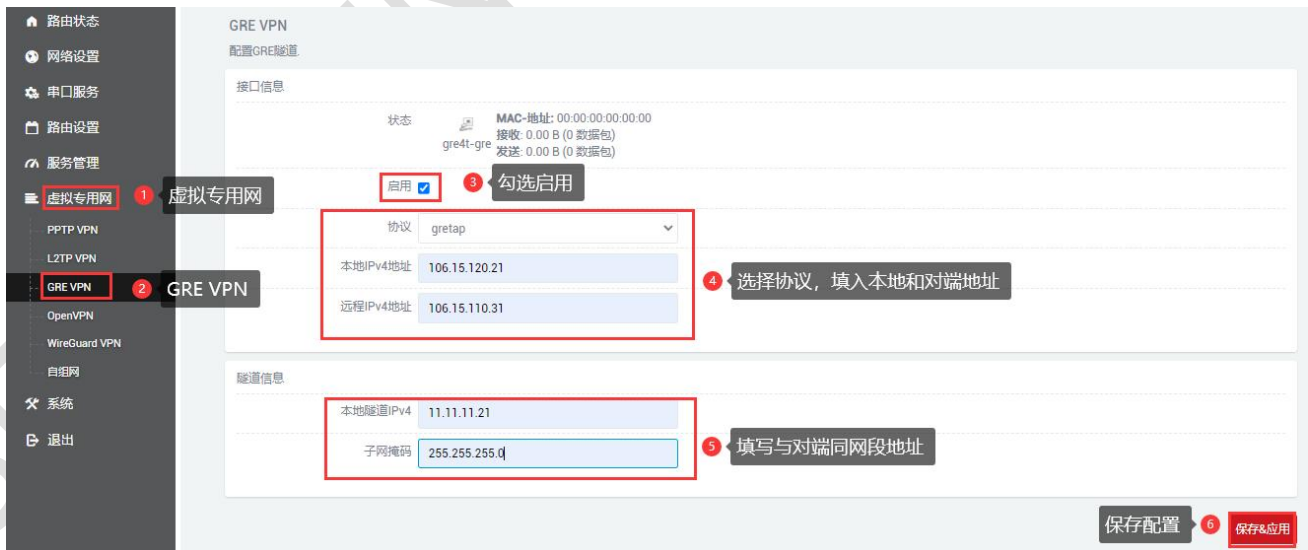


连接成功后状态栏会出现服务器给它分配的地址，如果不用 l2tp 的话，将启用不勾选后点击“保存&应用”即可。



5.3 GRE VPN

导航栏“虚拟专用网”——“GRE VPN”,选择启用，根据对端协议选择 gretap 或 gre（保持两端协议相同），本地 IPv4 地址和远程 IPv4 地址根据本地 wan 口（公网）地址和对端 wan 口（公网）地址填入，本地隧道地址填入与对端同网段 IP 地址及子网掩码。



“保存&应用”后刷新状态信息。

GRE VPN

配置GRE隧道。

接口信息

状态 运行时间: 0h 0m 8s
MAC-地址: BA:E6:09:22:26:68
gre-gre 接收: 0.00 B (0 数据包)
发送: 0.00 B (0 数据包)
IPv4: 11.11.11.21/24

启用 ☒

然后添加路由表规则，就可以成功访问对端 Lan 口设备了。

路由状态
网络设置
串口服务
路由设置 1 路由设置
静态路由 2 静态路由
接口转发
DMZ设置
黑白名单
1:1 NAT

静态路由
路由表描述了数据包的可达路径。

静态IPv4路由

接口	对象	IPv4-子网掩码	IPv4-网关	跃点数	MTU
	主机IP或网络	如果对象是一个网络			
尚无任何配置					

添加 3 点击添加

静态路由
路由表描述了数据包的可达路径。

静态IPv4路由

接口	对象	IPv4-子网掩码	IPv4-网关	跃点数	MTU
	主机IP或网络	如果对象是一个网络			
gre_static	192.168.2.0	255.255.255.0	11.11.11.31	0	1500

10 接口选择 gre_static 11 对象为对端Lan口 12 对端Lan口子网掩码 13 对端隧道IP

静态IPv6路由

接口	对象	IPv6-网关	跃点数	MTU
	IPv6-地址或超网() (CIDR)			
尚无任何配置				

添加

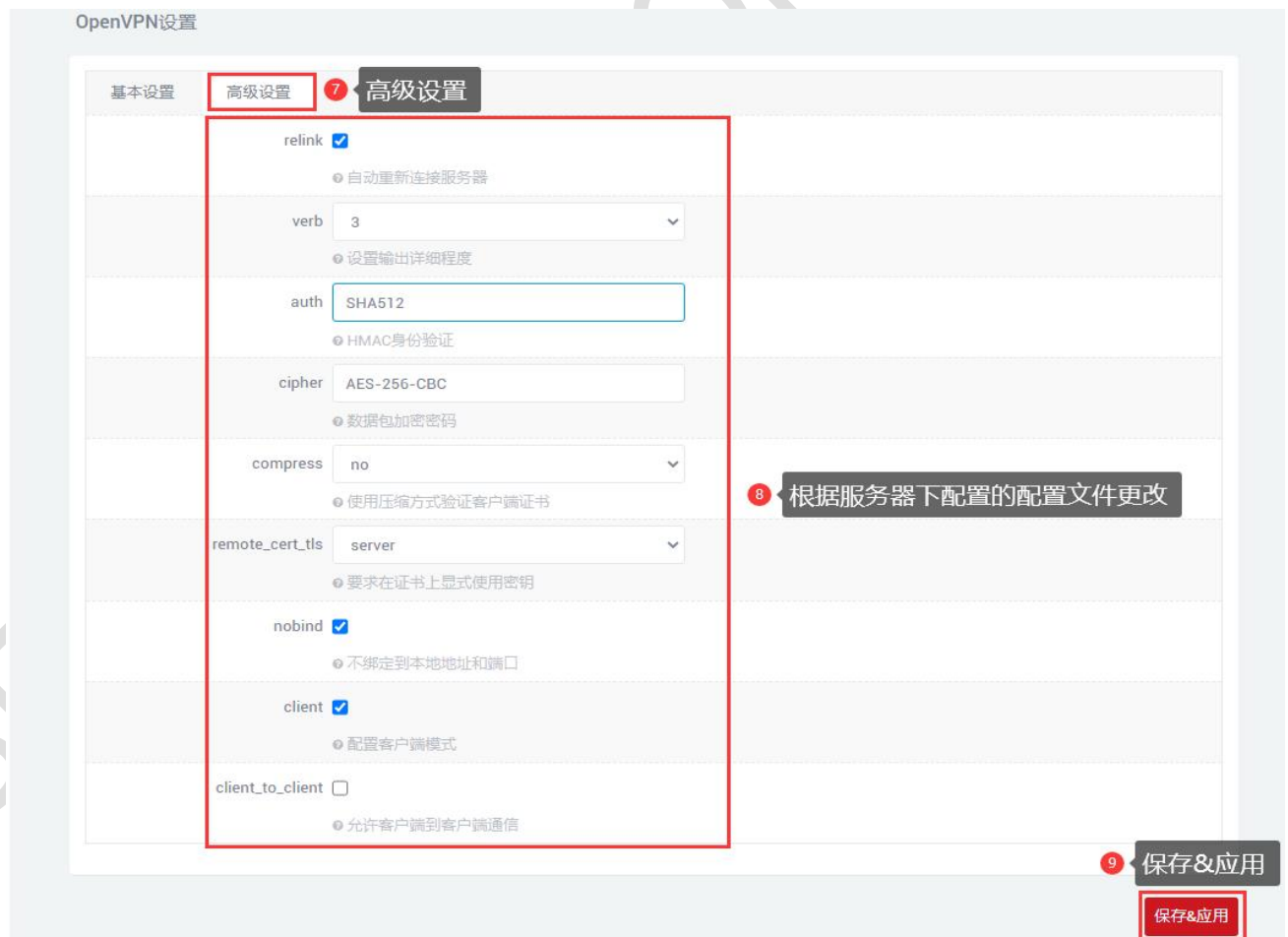
保存&应用 14 保存&应用

5.4 OpenVPN

导航栏“虚拟专用网”——“OpenVPN”，所有配置与服务器一致后点击“保存&应用”，三个证书由服务端提供。



高级设置页面根据服务端修改，relink 勾选的话代表 openvpn 可以自动重连，需要自动重连将其勾选即可，不需要就不勾选，所有配置完成后点击“保存&应用”。



连接成功后状态栏会刷新地址，如果不用 openvpn 的话，将启用取消勾选后点击“保存&应用”即可。

第六章 系统（设备管理）

6.1 日期和时间

默认时间同步是开启的，有需求的话可以根据需要更改 NTP 服务器来同步服务器的时间。

导航栏“系统”——“日期和时间”，设置完成后点击“保存&应用”。



6.2 语言设置

根据自己需要更改页面显示的语言，可以选择英文或者中文，在导航栏“系统”——“语言设置”进行更改，也可以在登录界面更改语言。



6.3 修改密码

登陆默认密码都为 admin。若是用户需要保护配置界面，避免被他人修改，可以修改登录密码，依次点击“系统”——“修改密码”，然后填入将要修改的密码，然后保存&应用，如下。



6.4 升级固件



导航栏“系统”——“升级固件”，选择文件后点击“UPDATE”，上传完毕后会显示 MD5 校验码的页面，点击“执行”即可升级，升级需要一定的时间，大概 1~2 分钟，升级完成后通过“192.168.2.1”重新登录页面。

升级固件时需要将“保留配置”选项取消勾选。



6.5 备份/恢复

备份功能可以用于生成设备的配置文件，并下载到本地。



下载的配置文件如下。



恢复功能通过本地配置文件去恢复设备配置，恢复过程中，设备会重启。



6.6 恢复出厂设置

恢复出厂设置一般是在设备出现问题后，无法进入设备页面，或者功能设置比较多，想要重新设置的时候，可以进行恢复出厂值设置，导航栏“系统”——“恢复出厂设置”，点击“执行复位”，即可将设备恢复出厂值。



6.7 设备重启

立即重启：设备可以通过页面进行重启，导航栏“系统”——“重启”，点击“执行重启”，即可重启设备。



6.8 页面退出



点击“退出”即可以退出至登录界面。

感谢您对赛诺联克产品的支持

若您有任何问题，请联系：info@seriallink.net or www.seriallink.net