SLK-R620 系列

工业级 5G 路由器

使用说明书

产品介绍

简介：

SLK-R620-5G 是基于 5G NR/LTE-FDD/LTE-TDD/HSPA+蜂窝调制解调器的高速 5G 终端，集成双核 880MHz CPU，提供 2 个 10/100/1000m 网络端口，1 个 SIM 卡插槽和插入 LAN 端口，接收 5G 高速网络。小尺寸的设计，以及采用铝制外壳，使其拥有很好的散热。同时产品进行了宽温度、宽电压输入和电磁兼容 EMC 测试。

已广泛应用于物联网产业链 M2M 的行业,如自助服务终端、智能电网、智能交通、智能家居、金融、移动 POS 终端、供应链自动化、工业自动化、智能建筑、消防、公安、环保、气象、数字医疗、遥测、军事、太空探索、农业、林业、水、煤炭、石化等领域。

特征：

- ✓ MTK 双核 880MHz CPU
- ✓ 2 x 10/100/1000M 以太网 LAN/WAN 接口
- ✓ 5G NR/LTE-FDD/LTE-TDD/HSPA+网络
- ✓ 极小尺寸
- ✓ 支持 DC6-30V 输入电压

目录

第一章 参数配置.....4
1.1 路由器配置前准备.....4
1.1.1 自动获取 ip 地址（推荐使用）.....4
1.1.2 设置静态 ip 地址.....4
1.2 登录配置页面.....4
1.3 网络配置.....5
1.3.1 修改静态登录页面地址.....5
1.3.2 SIM 卡 2/3/4/5G 方式上网.....6
1.4 APN 设置表.....9
1.4.1 国内物联网卡 APN 参数.....9
1.4.2 普通流量 4G 卡 APN，一般无需任何设置都可以正常上网：.....10
1.4.2 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）.....10
1.5 DHCP 服务器.....10
1.6 WAN 口设置.....11
1.6.1 DHCP 客户端.....11
1.6.2 PPOE 拨号.....12
1.6.3 静态地址.....12
1.6.4 关联 Lan（将 WAN 口转化为 LAN 口）.....13
第二章 防火墙.....14
2.1 防火墙开启与关闭.....14
2.2 DMZ 设置.....14
2.3 端口转发.....16
2.3 内网穿透（frp）.....18
2.3.1 添加 TCP 代理协议.....23
2.3.2 添加 STCP 代理协议.....25
2.3.3 添加 UDP 代理协议.....32
2.3.4 添加 HTTP 代理协议.....34
第三章 VPN（虚拟专用网）.....36
3.1 PPTP VPN.....36
3.2 L2TP VPN.....37
3.3 OPENVPN.....38
第四章 基本管理（设备管理）.....41
4.1 诊断.....41
4.2 日期和时间.....42
4.3 语言设置.....43
4.4 升级固件.....43
4.5 恢复出厂设置.....44
4.6 设备重启.....45
4.7 页面退出.....45

第一章 参数配置

1.1 路由器配置前准备

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。

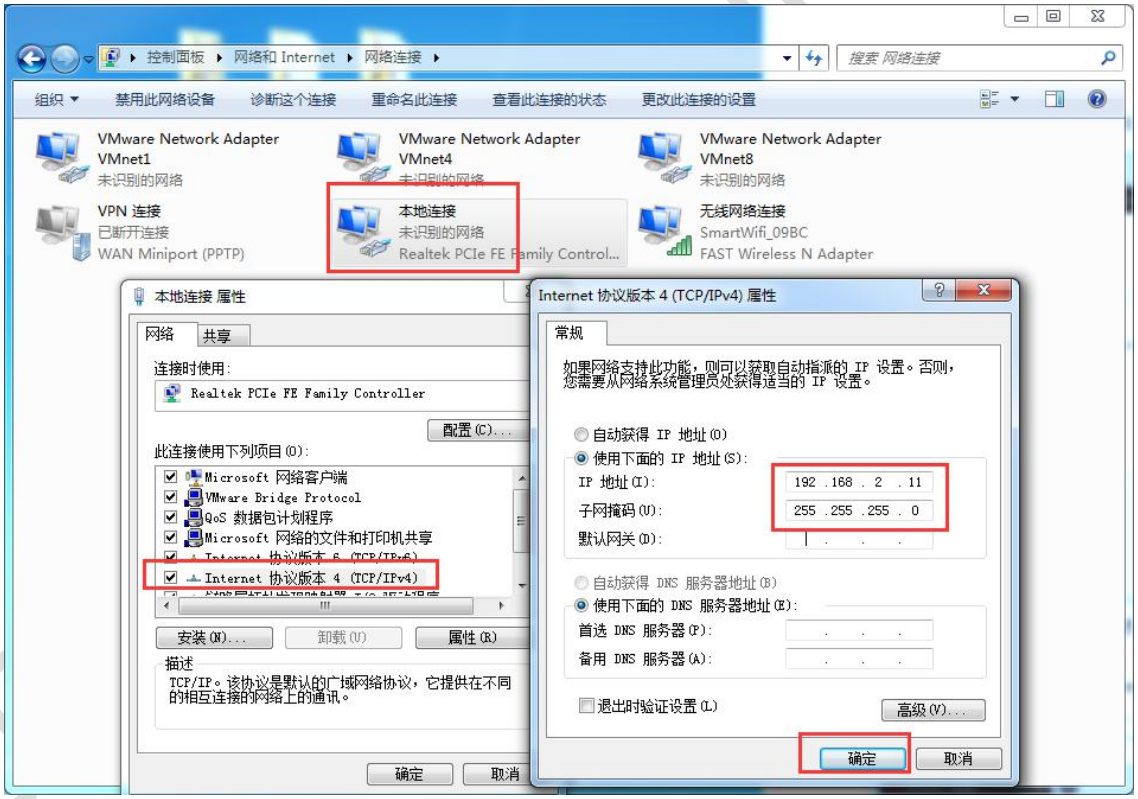
1.1.1 自动获取 ip 地址（推荐使用）

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。

1.1.2 设置静态 ip 地址

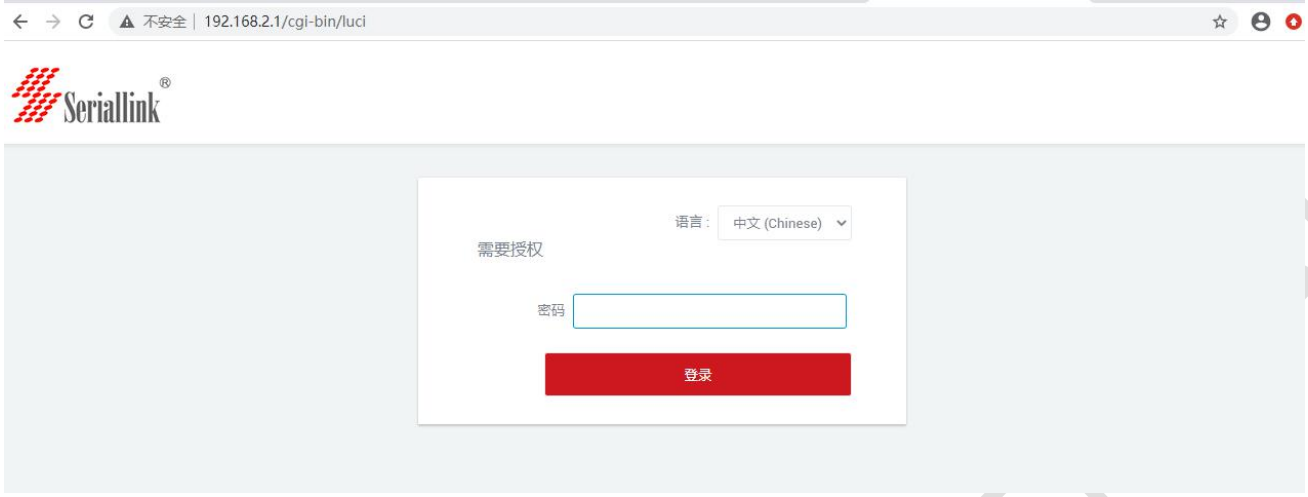
请将管理 PC 的 IP 地址（例如设置为：192.168.2.11）与设备的 LAN 口 IP 地址设置在同一网段内（设备 LAN 口初始 IP 地址为：192.168.2.1，子网掩码均为 255.255.255.0）。

打开“控制面板”——“网络和 Internet”——“网络连接”——“本地连接”修改如下：

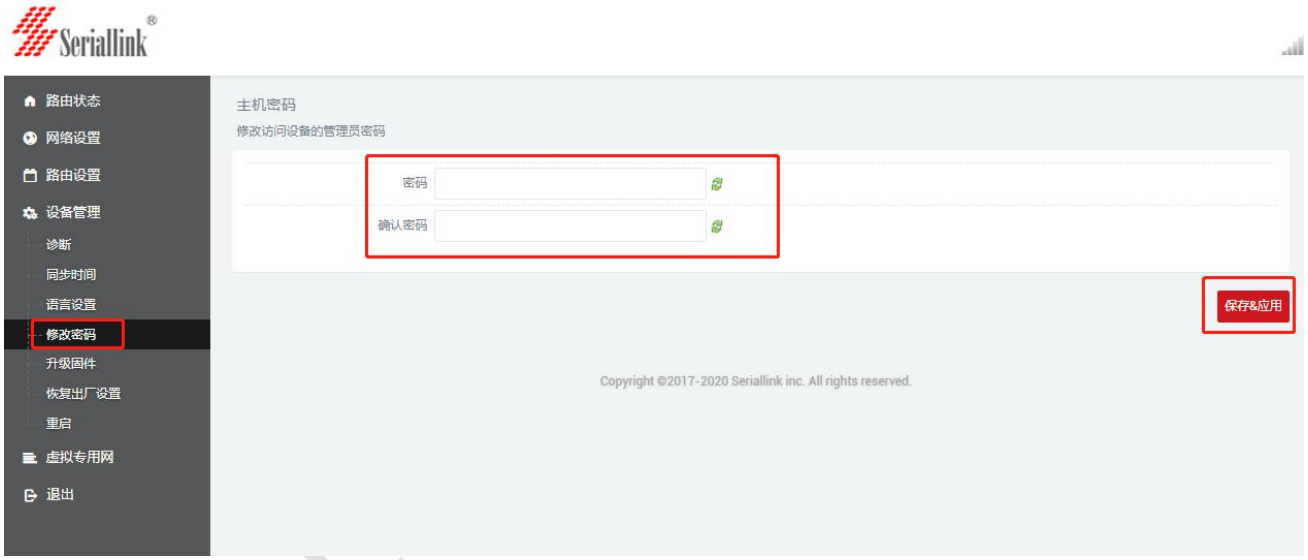


1.2 登录配置页面

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（密码的出厂默认设置为 admin）。



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“设备管理器”——“修改密码”，然后填入将要修改的密码，然后保存&应用，如下



1.3 网络配置

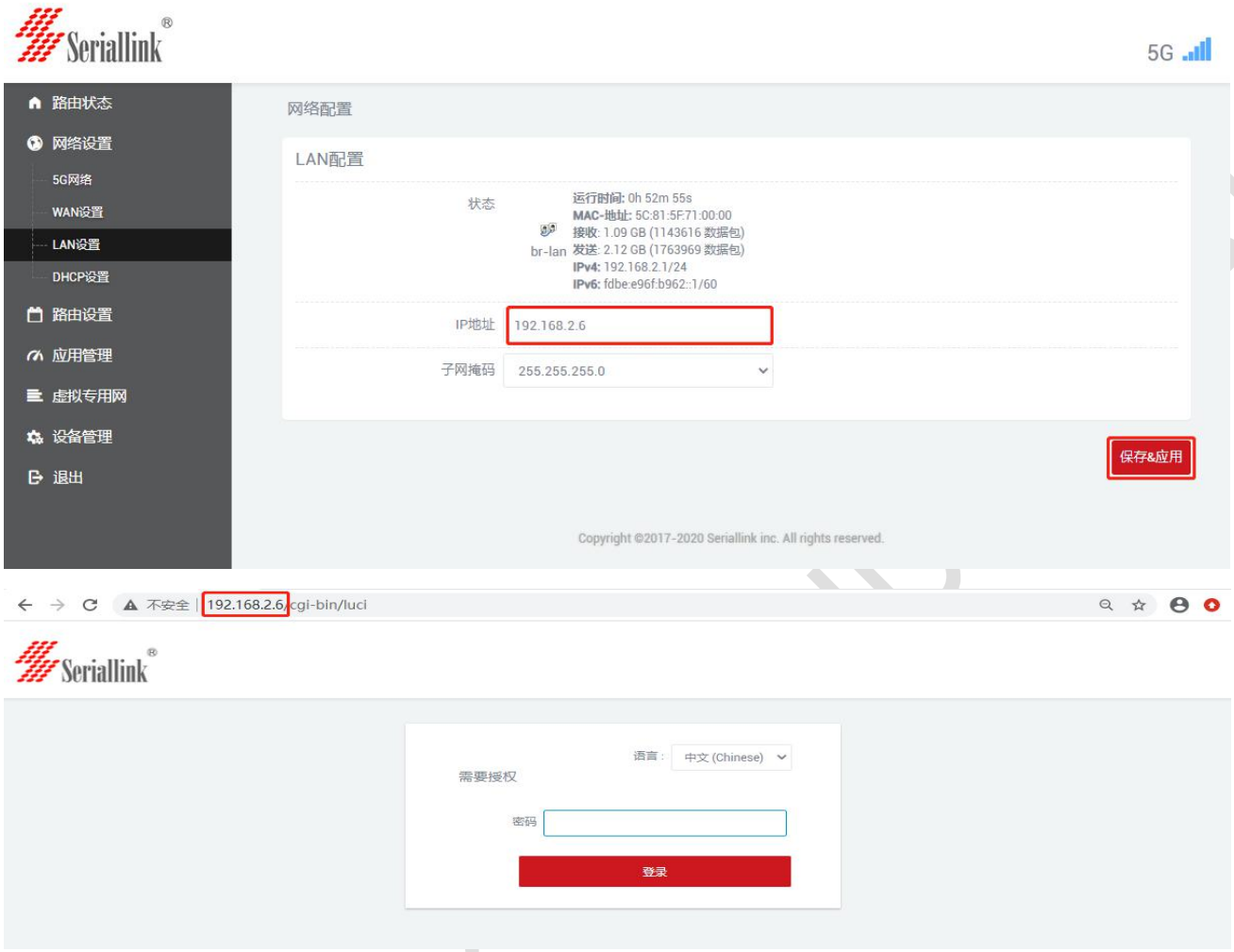
1.3.1 修改静态登录页面地址

路由器默认静态地址为 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）

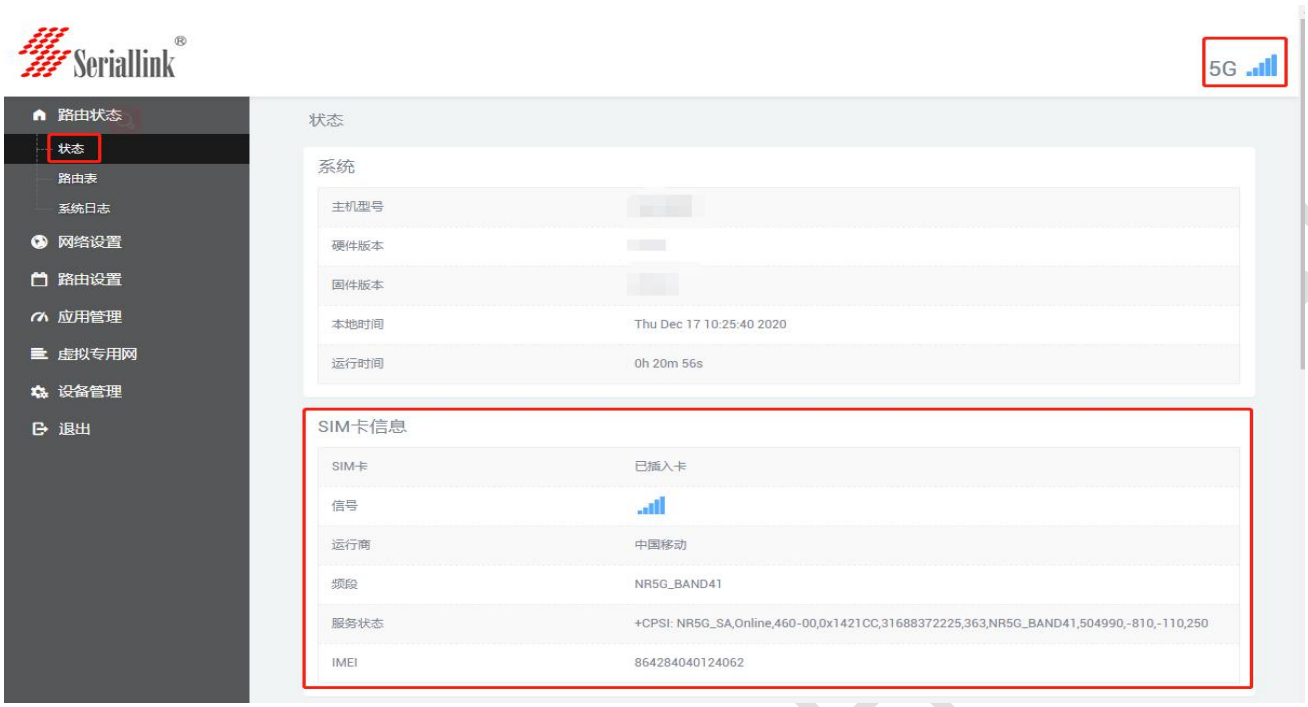
子网掩码：一般是 255.255.255.0，可以根据需要进行修改。

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。

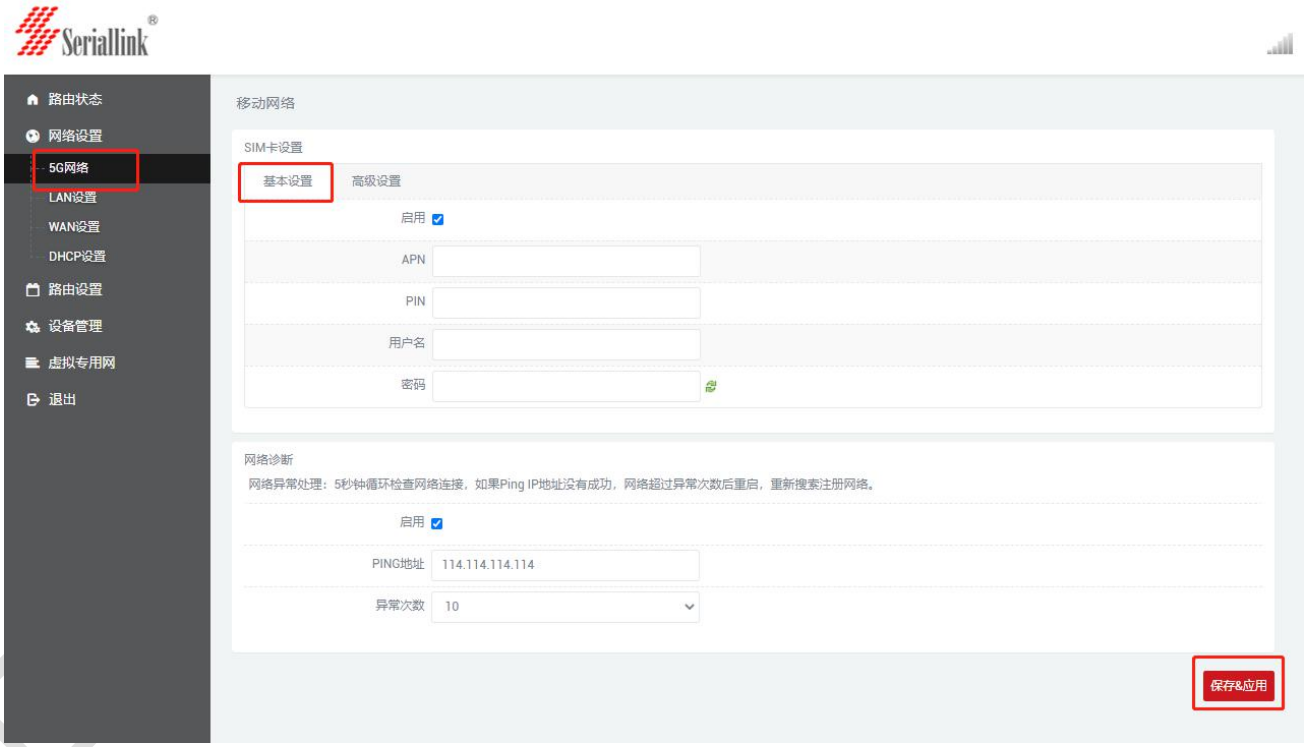


1.3.2 SIM 卡 2/3/4/5G 方式上网

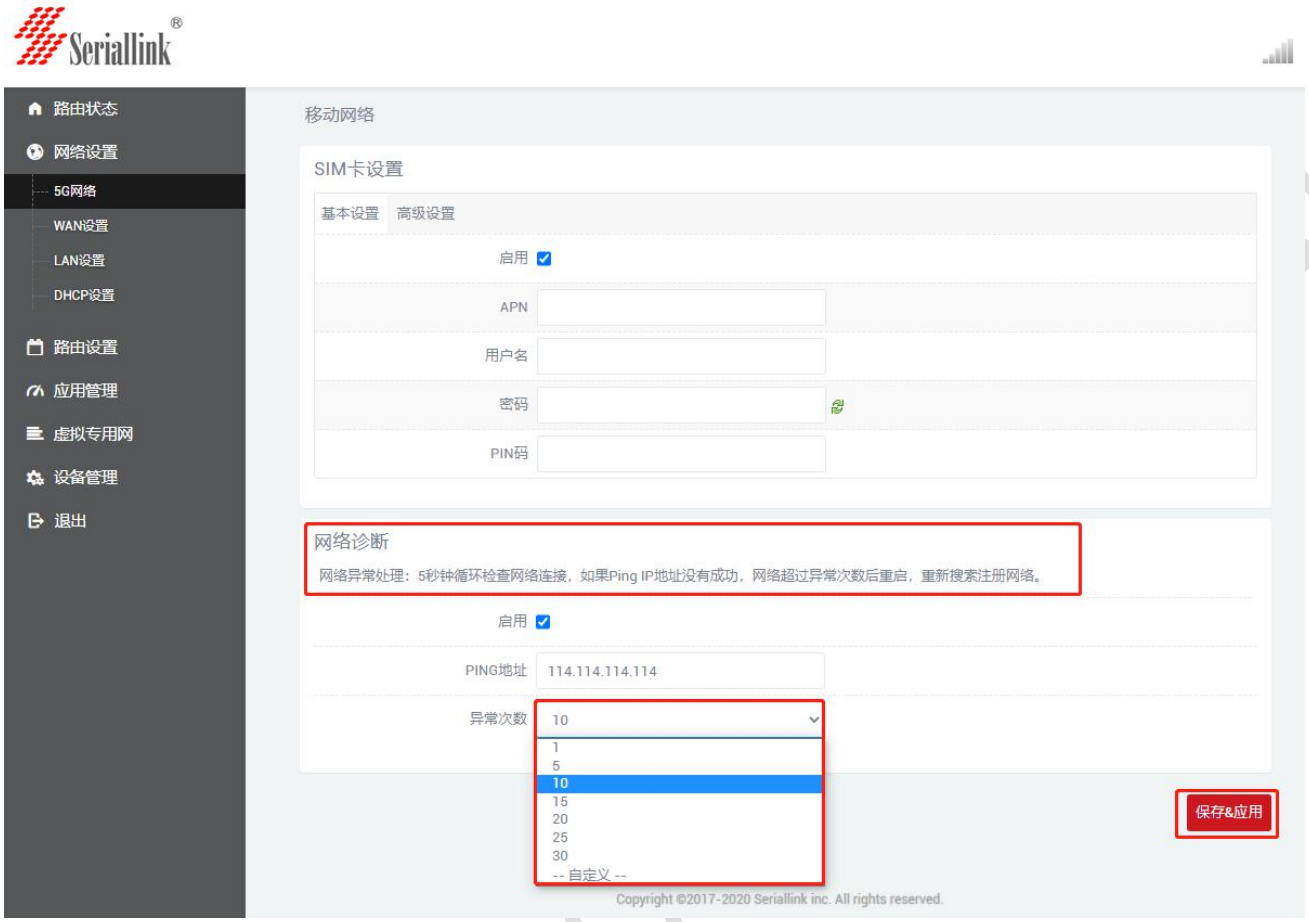
路由器默认是使用 SIM 卡 2/3/4/5G 上网，在导航栏“路由状态”——“状态”可以看到 SIM 卡的信息，右上角可以查看网络是 2/3/4/5G 以及手机卡信号。

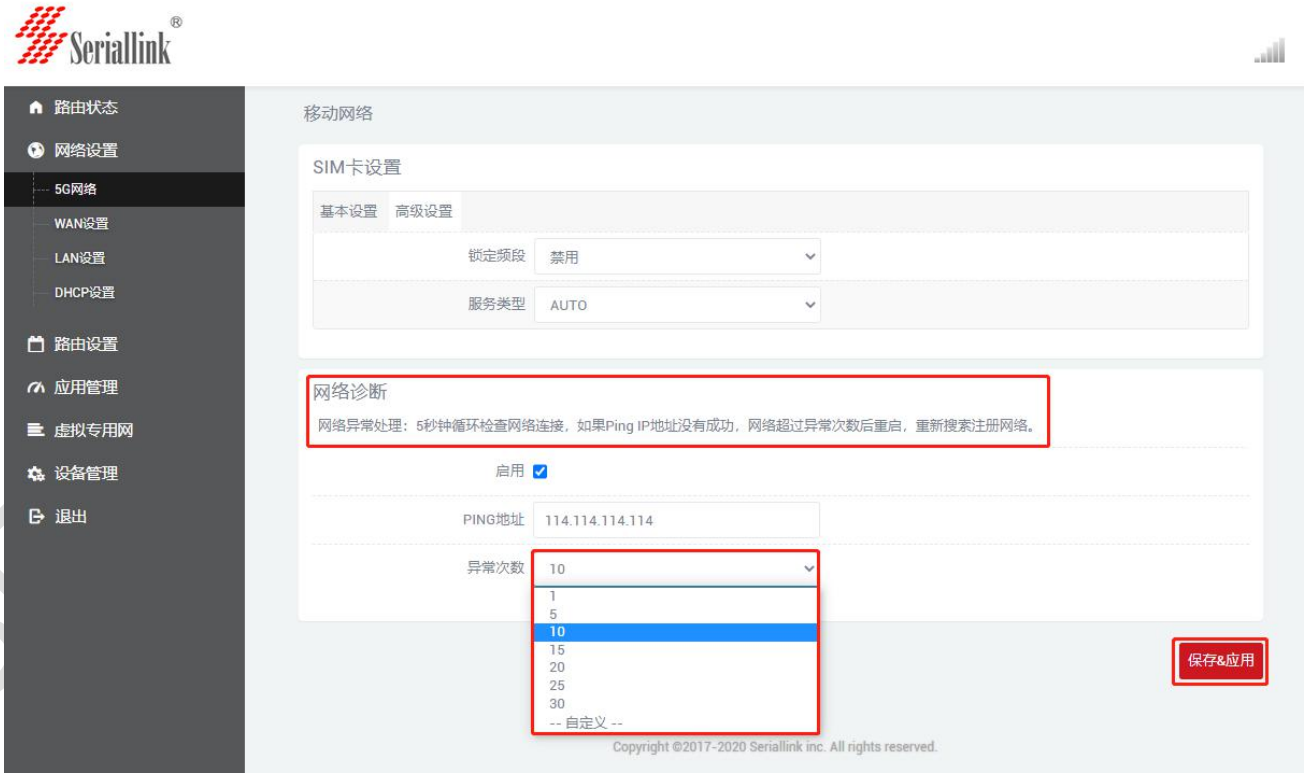


如果使用普通手机流量卡， APN 设置的位置可以不用关心，默认为空即可。 如果您使用了 APN 卡，需要在“网络设置”——“5G 网络”——“基本设置”设置 APN，自行填写用户名跟密码。

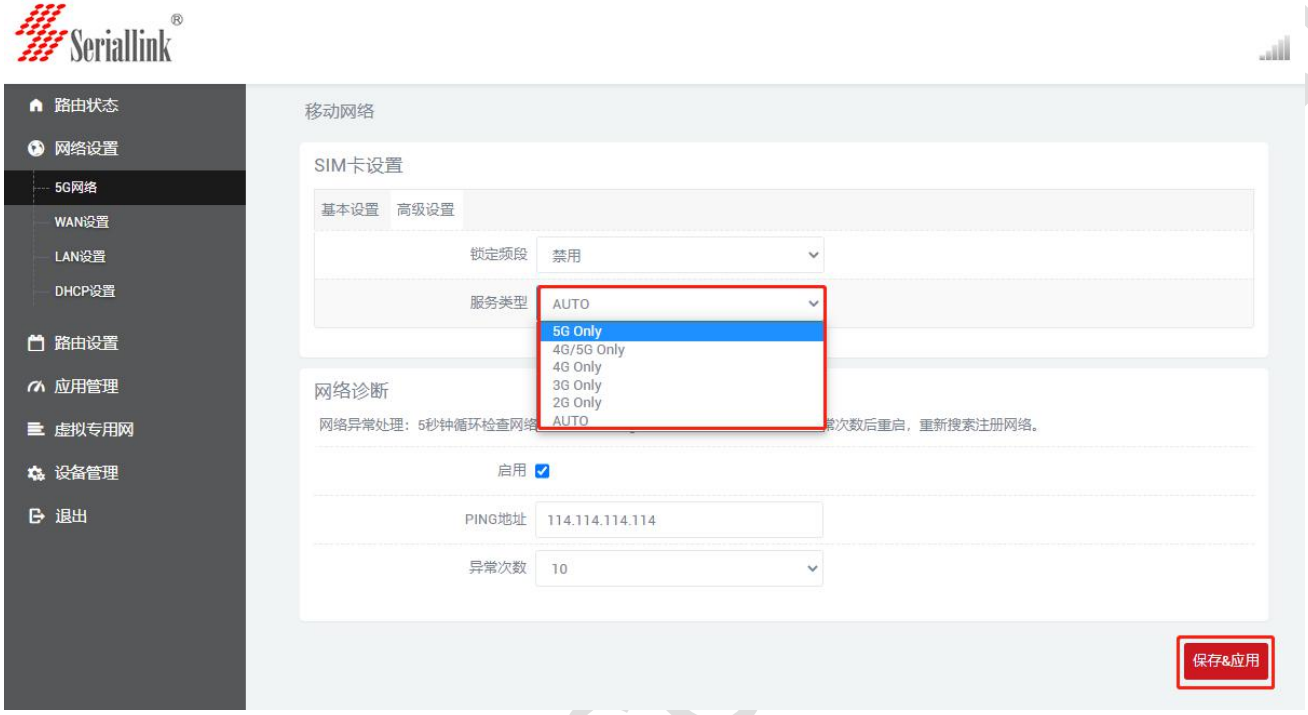


网络诊断：是对网络异常进行处理，每 5s ping 一次设置的 ip 地址，ping 完异常的次数后还是不能 ping 通，将重新注册网络。在“基本设置”和“高级设置”都可以设置网络诊断，也可以不启用网络诊断，将启用不勾选即可。


路由状态
网络设置
5G网络
WAN设置
LAN设置
DHCP设置
路由设置
应用管理
虚拟专用网
设备管理
退出
移动网络
SIM卡设置
基本设置
高级设置
启用
APN
用户名
密码
PIN码
网络诊断
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
异常次数
10
1
5
10
15
20
25
30
-- 自定义 --
保存&应用
Copyright ©2017-2020 Seriallink inc. All rights reserved.


路由状态
网络设置
5G网络
WAN设置
LAN设置
DHCP设置
路由设置
应用管理
虚拟专用网
设备管理
退出
移动网络
SIM卡设置
基本设置
高级设置
锁定频段
禁用
服务类型
AUTO
网络诊断
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
异常次数
10
1
5
10
15
20
25
30
-- 自定义 --
保存&应用
Copyright ©2017-2020 Seriallink inc. All rights reserved.

“网络设置”——“5G 网络”——“高级设置”可以对 2/3/4/5G 进行绑定，如果服务类型选择了 5G Only，代表只用 5G 的网，不是 5G 会自动没有网络。默认是 2/3/4/5G 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”。



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（如有请参考 APN 设置表章节）或请咨询运当地营商。

1.4 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:

1.4.1 国内物联网卡 APN 参数

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

1.4.2 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#

1.4.2 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

1.5 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（一般为默认）：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

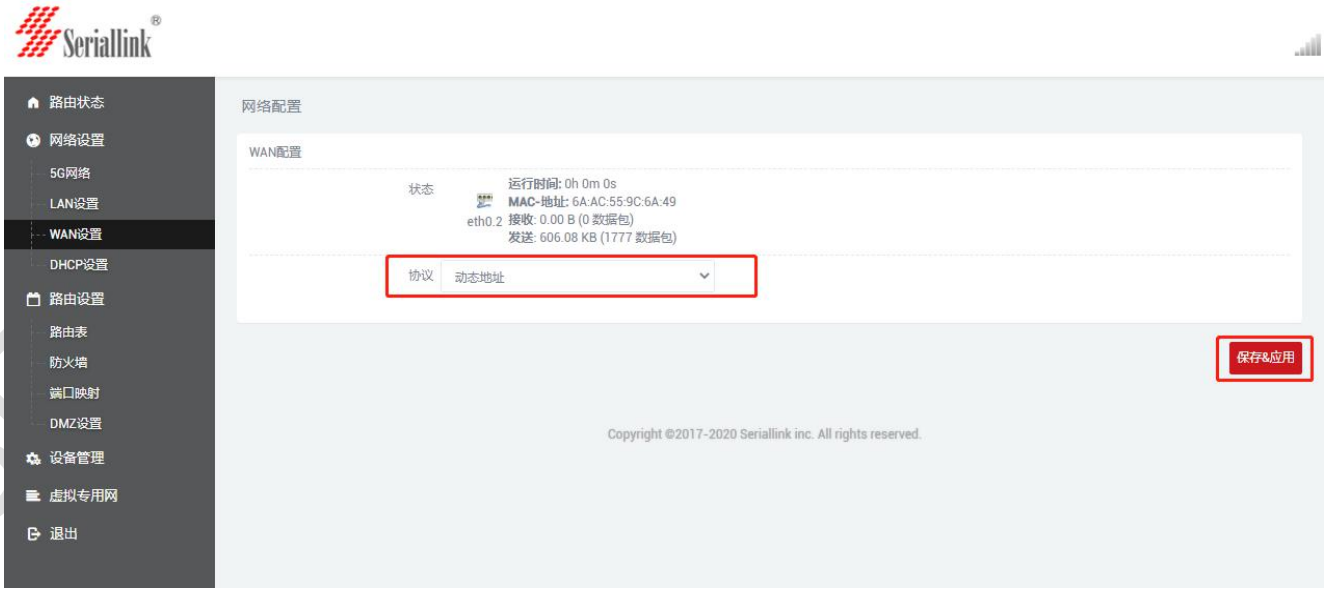
客户数：分配的 ip 个数。

租用时间：分配的 IP 的时间长短。

1.6 WAN 口设置

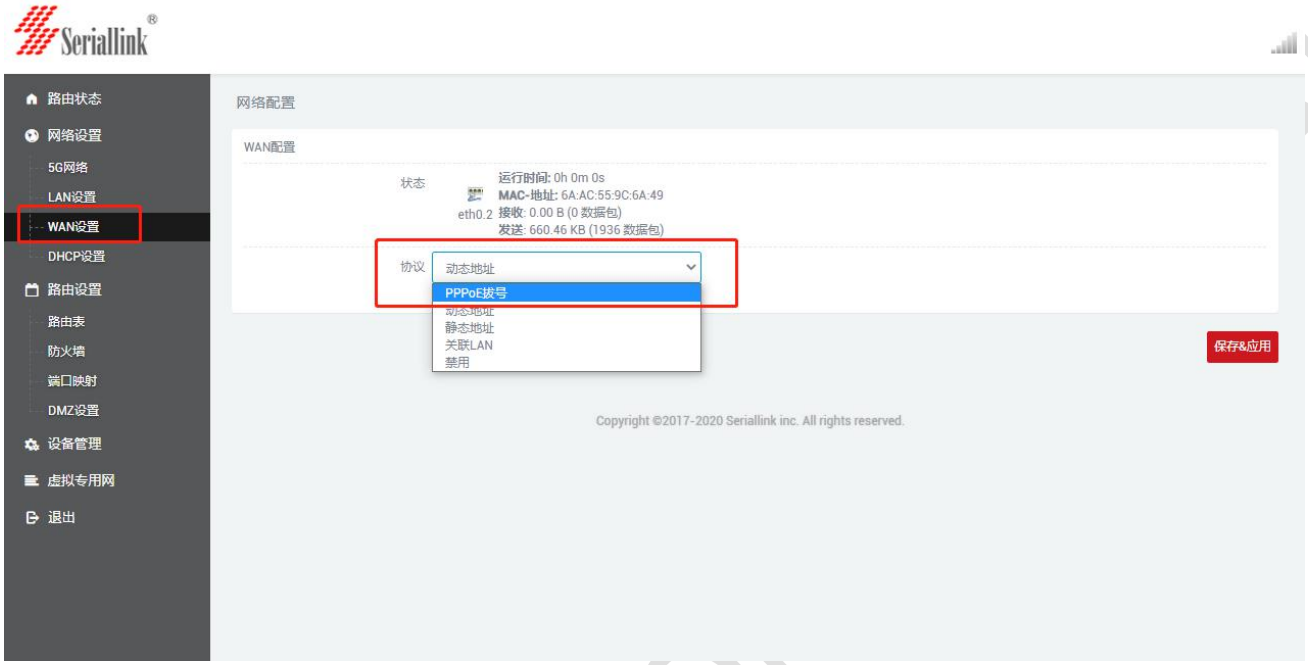
1.6.1 DHCP 客户端

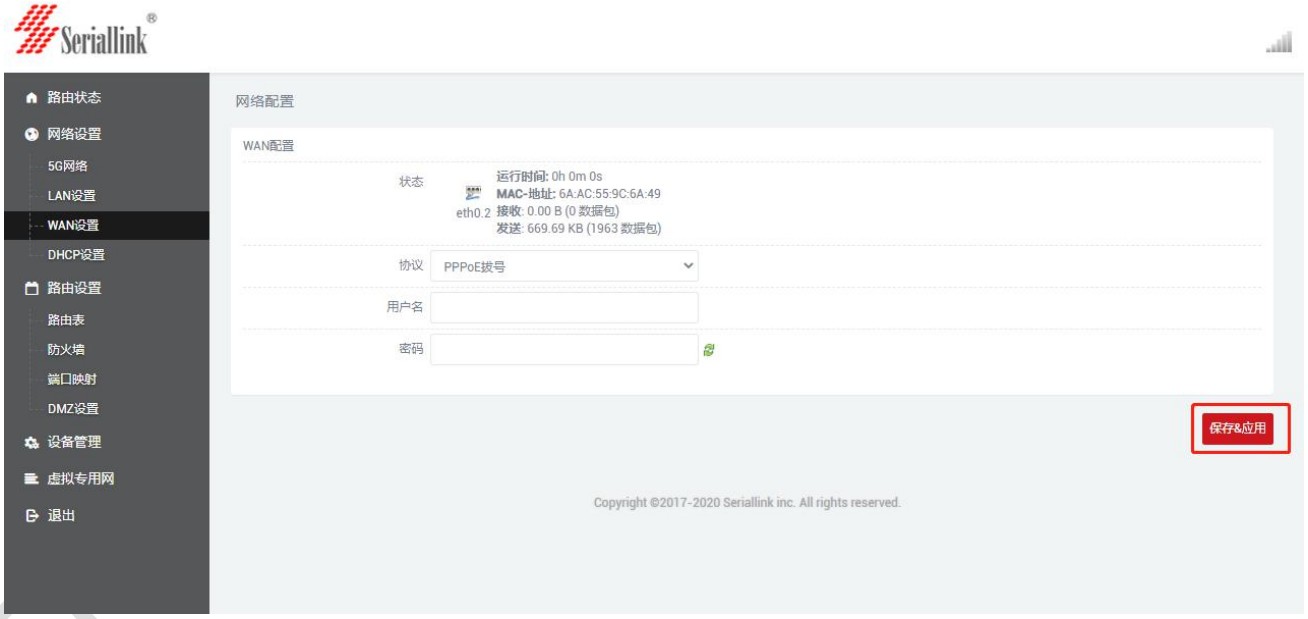
导航栏“网络设置”——“wan 设置”，WAN 口默认协议是动态地址（即 DHCP 客户端），需要上级设备能够为 wan 口分配 ip。



1.6.2 PPOE 拨号

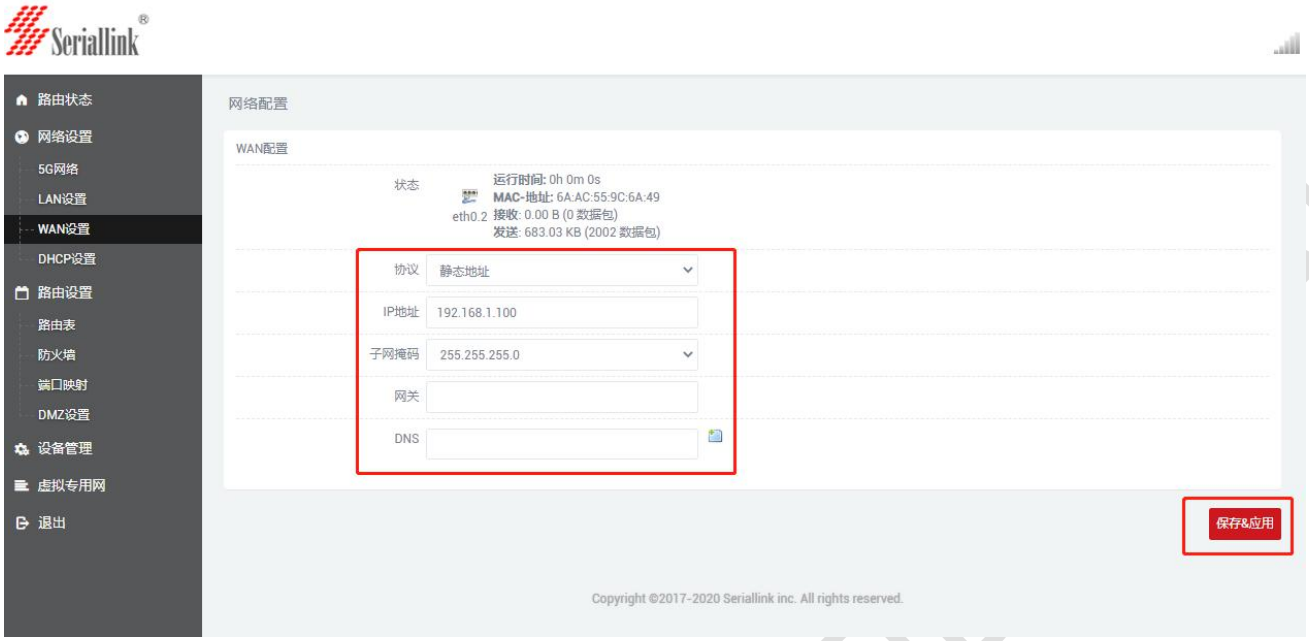
如果 wan 口需要拨号才能上网的，需要选择 ppoe 拨号，根据实际情况填写用户名和密码。





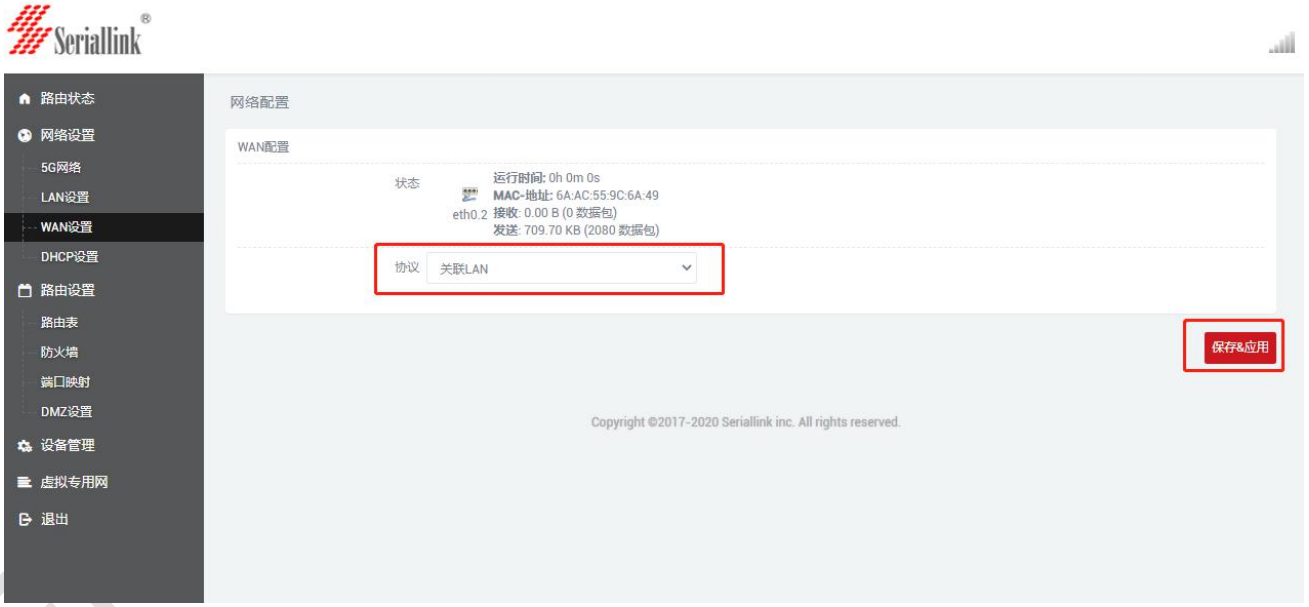
1.6.3 静态地址

wan 口也可以选择自己手动设置 ip 地址。



1.6.4 关联 Lan（将 WAN 口转化为 LAN 口）

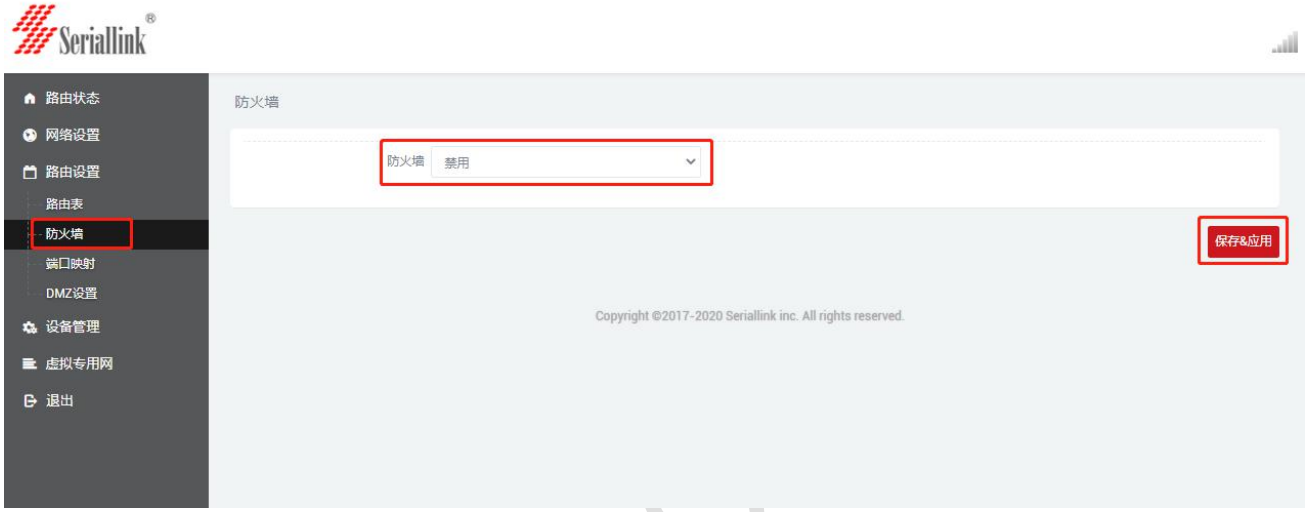
如果要将 WAN 口转化为 LAN 口，将 wan 设置的协议改为“关联 LAN”，点击“保存&应用”，就可以将 wan 口转化为 lan 口。



第二章 防火墙

2.1 防火墙开启与关闭

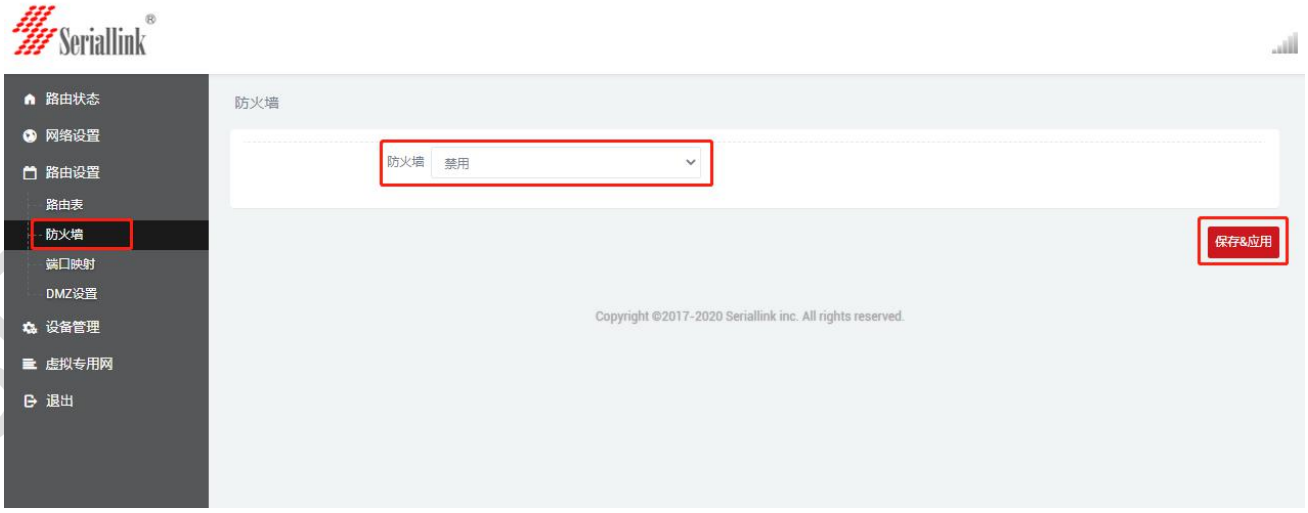
防火墙默认是开启的，在做 DMZ 和端口映射的时候需要将防火墙禁用，防火墙禁用步骤，导航栏“路由设置”——“防火墙”，防火墙选择禁用，然后点击“保存&应用”。



2.2 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。

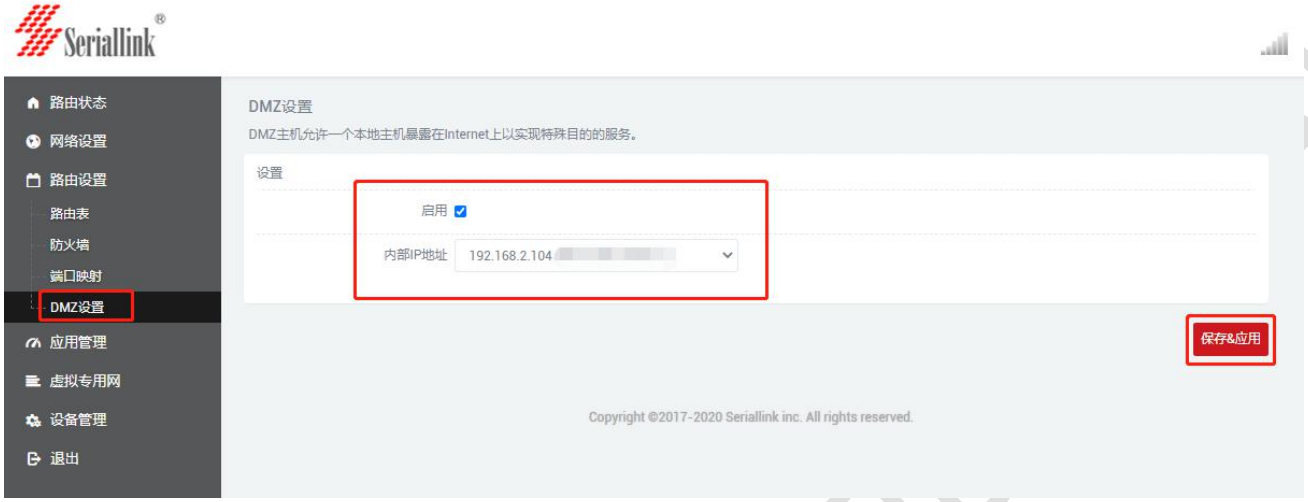


导航栏中“路由设置”——“DMZ 设置”，点击启用，设置 lan 口给下接设备分配的 ip 地址，将下接设备所有的端口转发出来，通过 wan 口的 ip 地址可以直接访问。

启用：将启用勾选

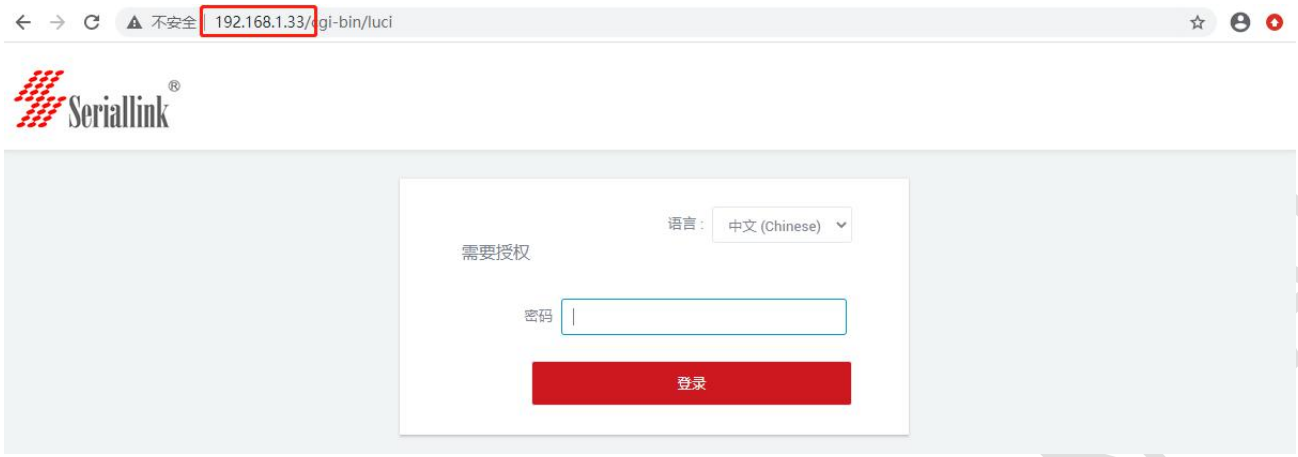
内部 IP 地址：本机设备的 ip 或 lan 口为下接设备分配的 ip

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。

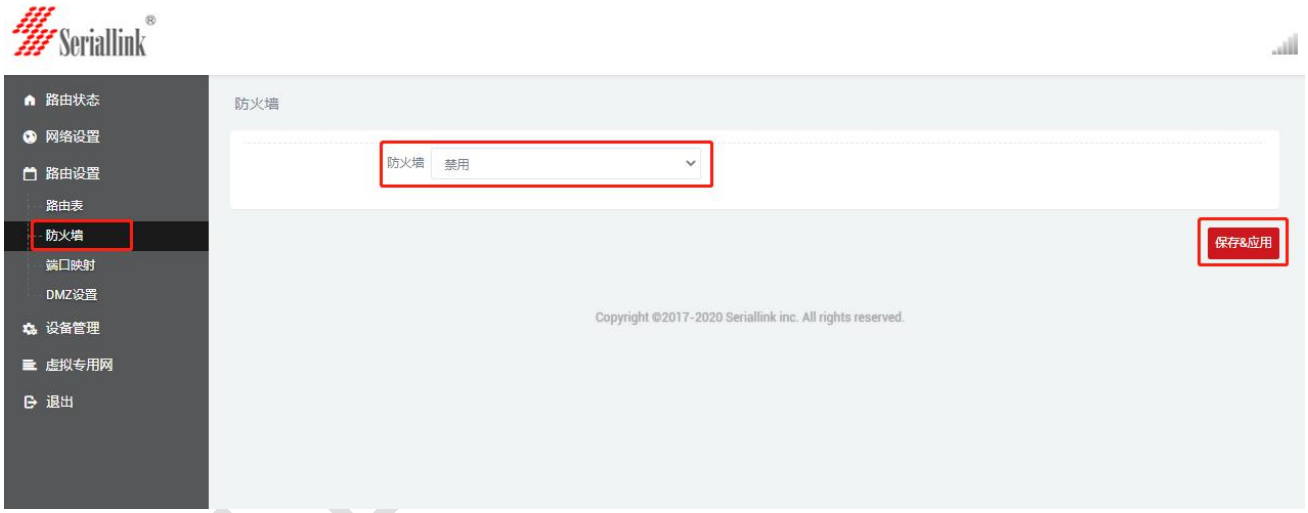
直接通过 wan 口的 ip 就可以访问下接设备了。（注意：电脑需要与 wan 口的 ip 在同一个局域网内才可以访问）



2.3 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。

首先需要先禁用防火墙。



导航栏中“路由设置”——“端口映射”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。

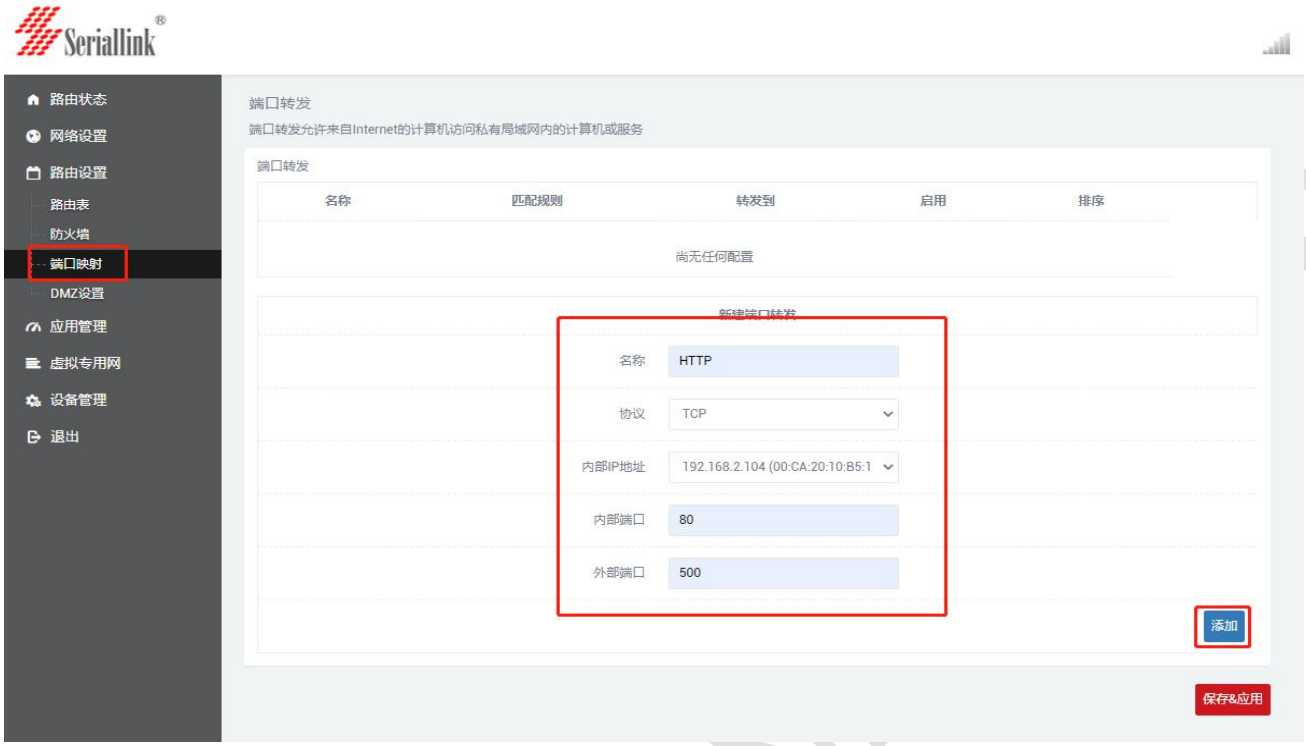
协议：指定要转发的协议，可以是 TCP，UDP，或者 TCP/UDP。

内部 IP 地址：选择需要转发到外网的 IP 地址。

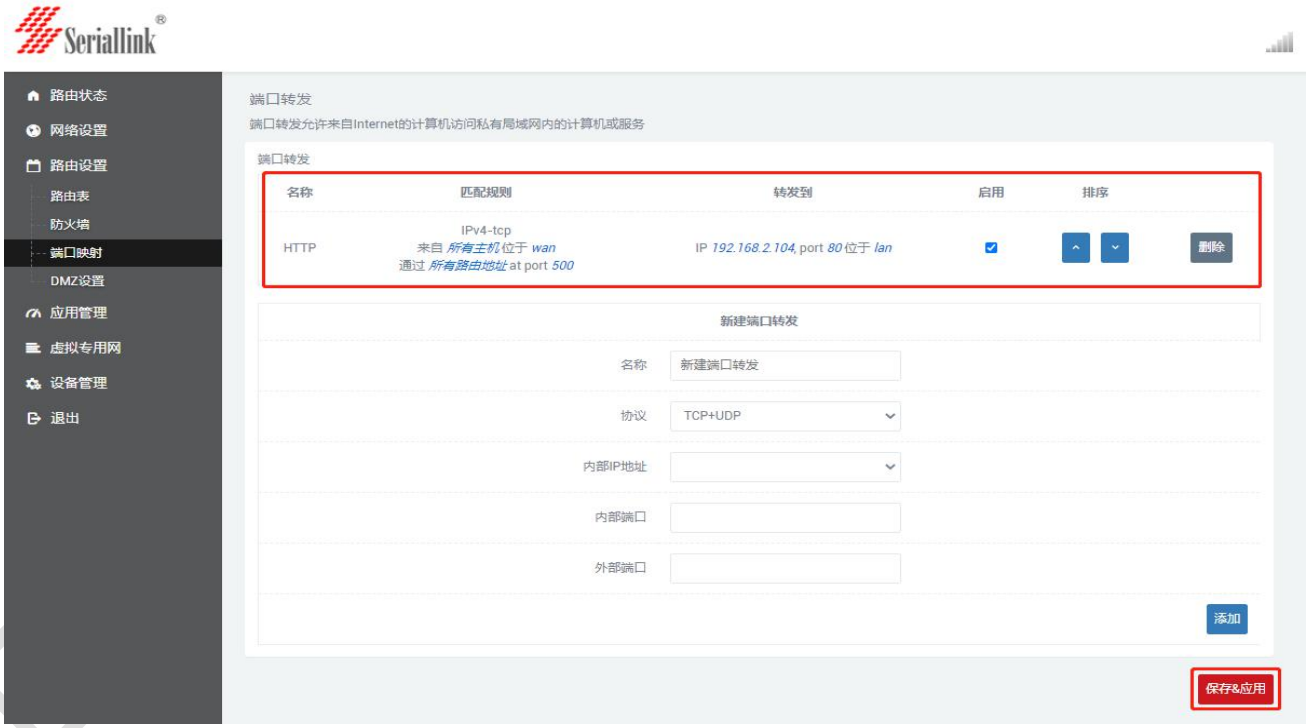
内部端口：下接设备或本机要转发出来的端口。

外部端口：通过 wan 口 ip 加这个外部端口即可访问下接设备。

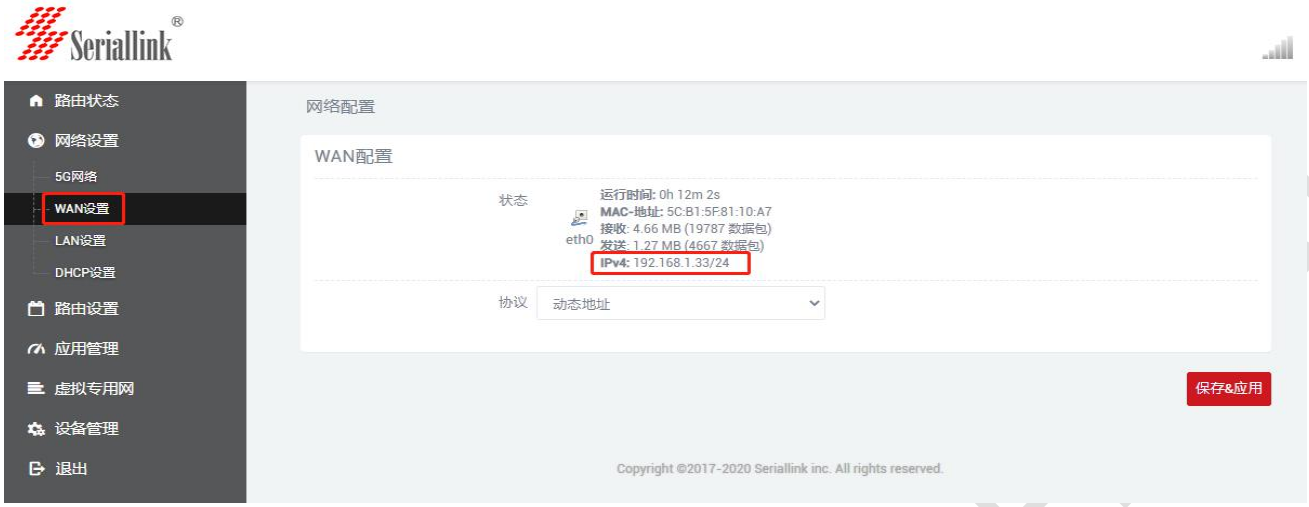
配置完后，点击“添加”按钮，新增一条转发规则。点击“保存&应用”按钮，使规则生效。



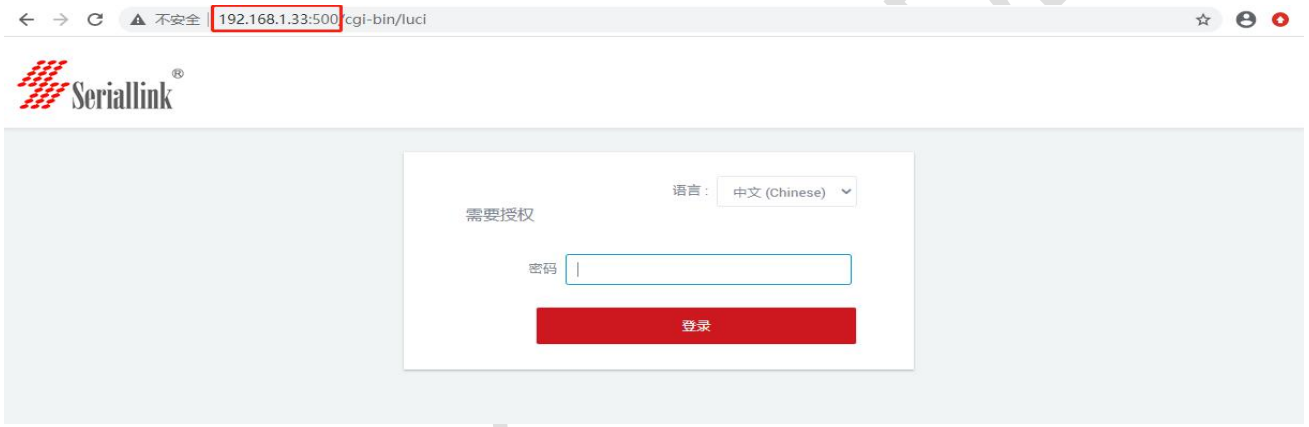
添加成功后，会多出一条端口转发的规则，点击“保存&应用”使该规则生效。规则可以添加多条。



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 192.168.1.33:500 访问下接设备的内部端口。



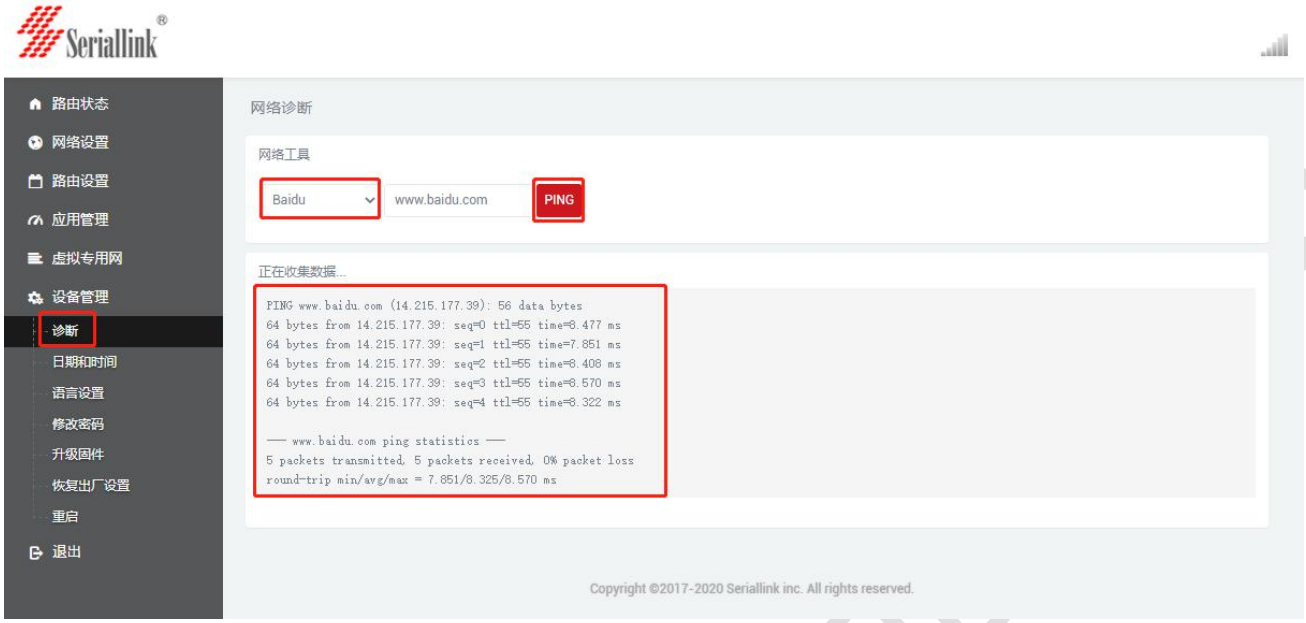
2.3 内网穿透（frp）

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。

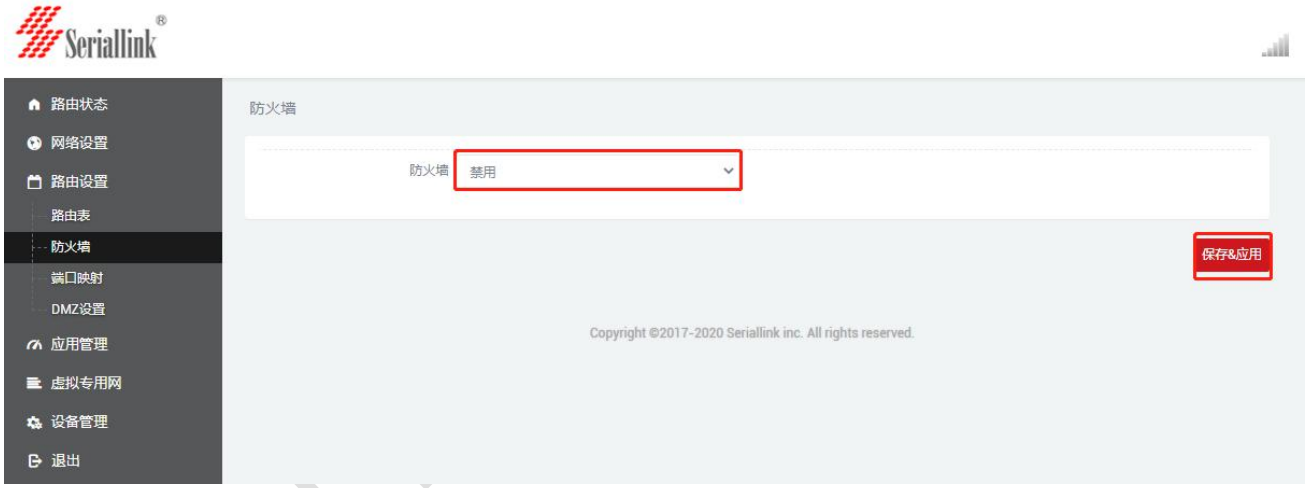
Frp 主要实现的功能：外网通过 ssh 访问内网机器；外网通过公网地址加端口号访问内网机器通过 frp 转发出来的端口；自定义绑定域名访问内网 web 服务。

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“设备管理”——“诊断”；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”。



配置前准备：

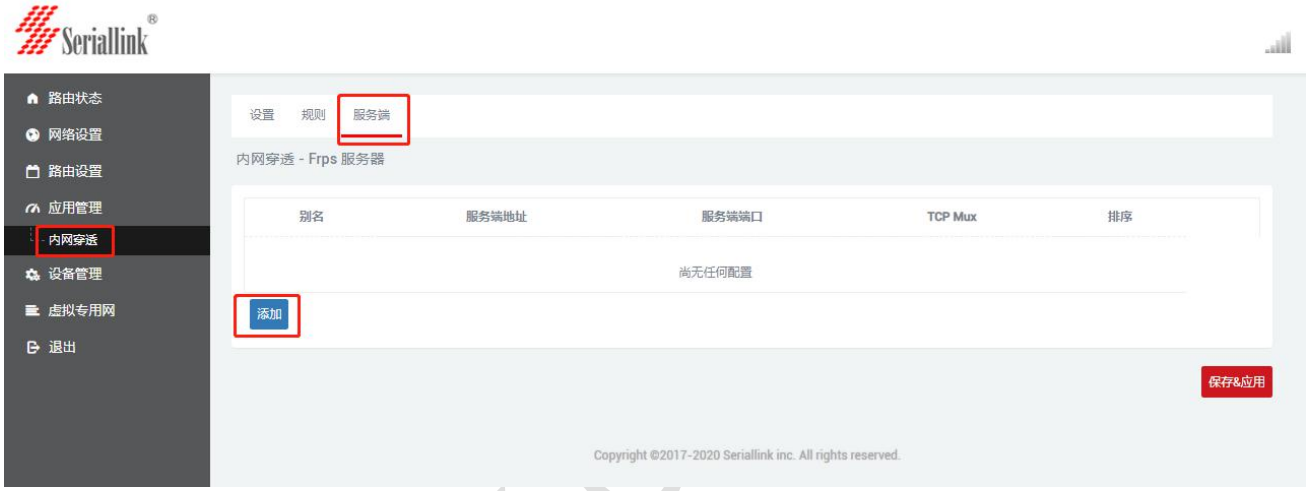
（1）公网服务器 1 台。

（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“应用管理”——“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。

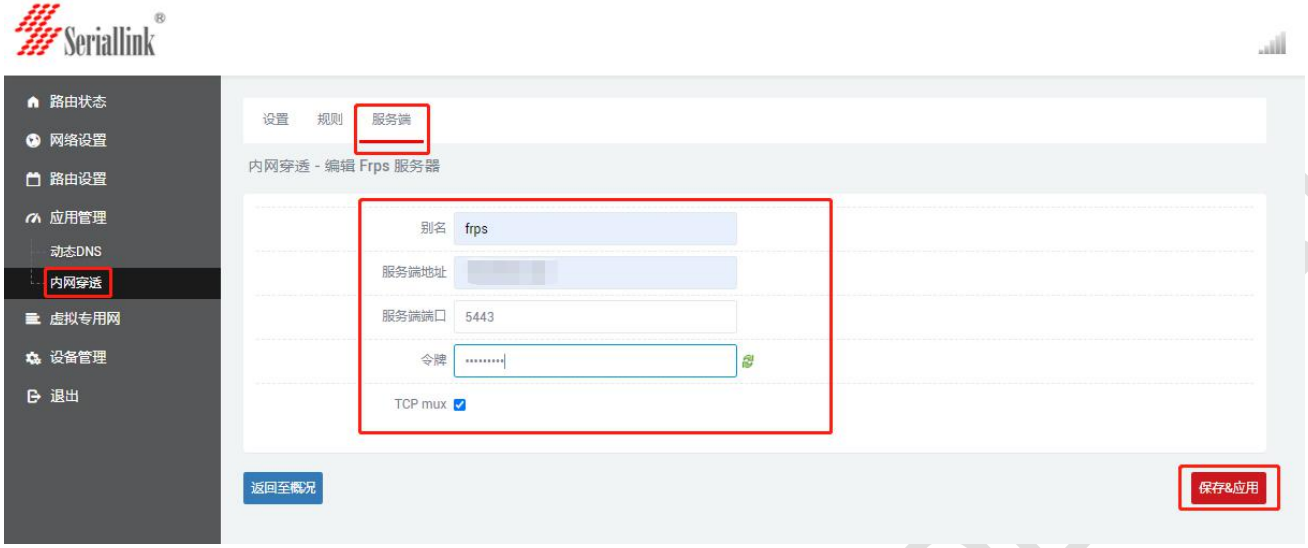
服务端地址：服务端的地址。（一般为公网 ip 地址）

服务端端口：服务端端口

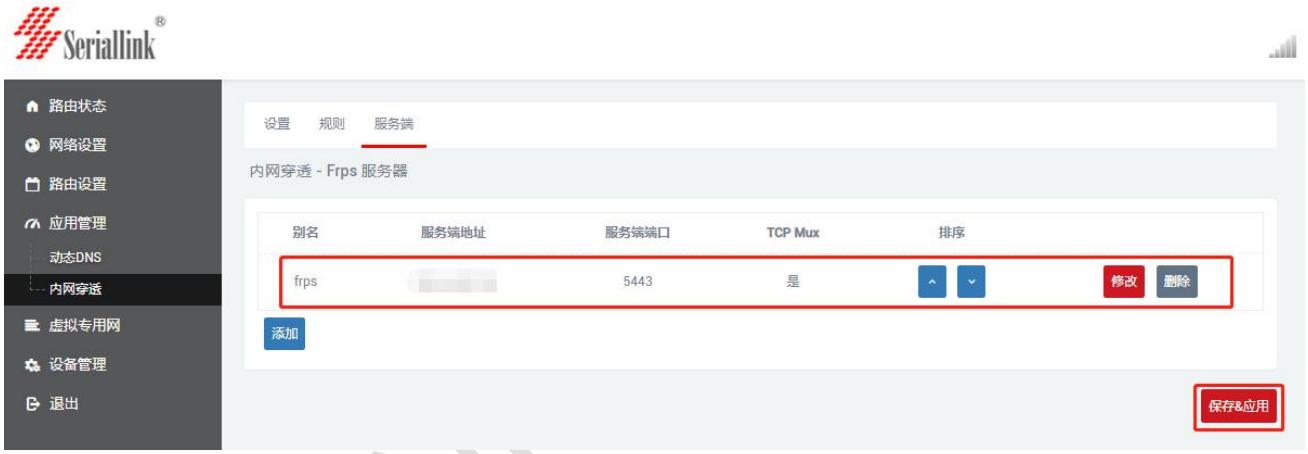
令牌：服务端设置的密码

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”。



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



（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。

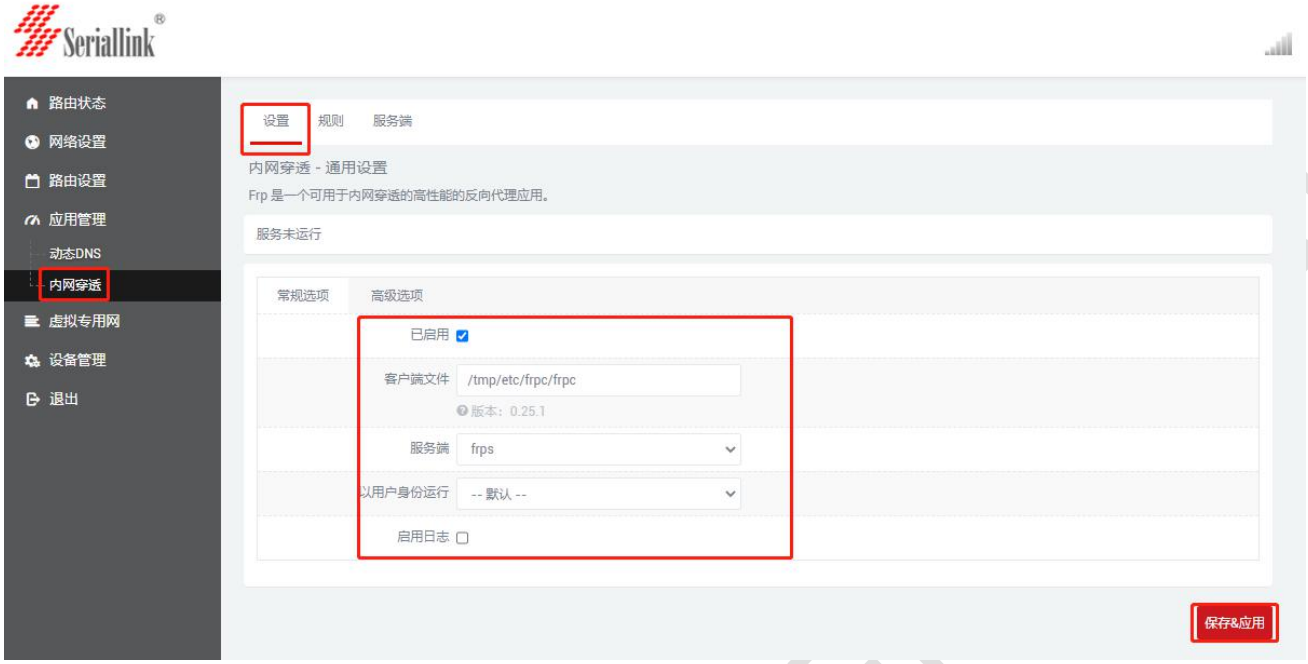
客户端文件：不需要修改，系统自动匹配的，默认就可以了。

服务端：刚刚自定义的服务端别名。

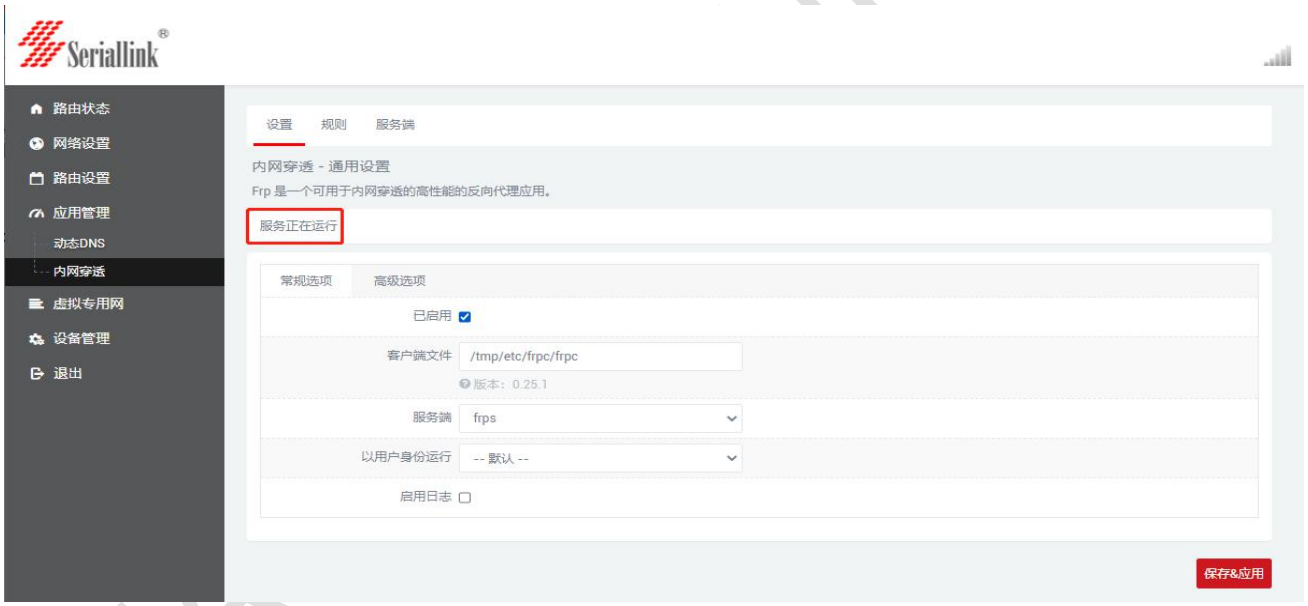
以用户身份运行：一般选择默认，可以根据需要自行修改。

启用日志：根据需要勾选。

配置完成后点击“保存&应用”。

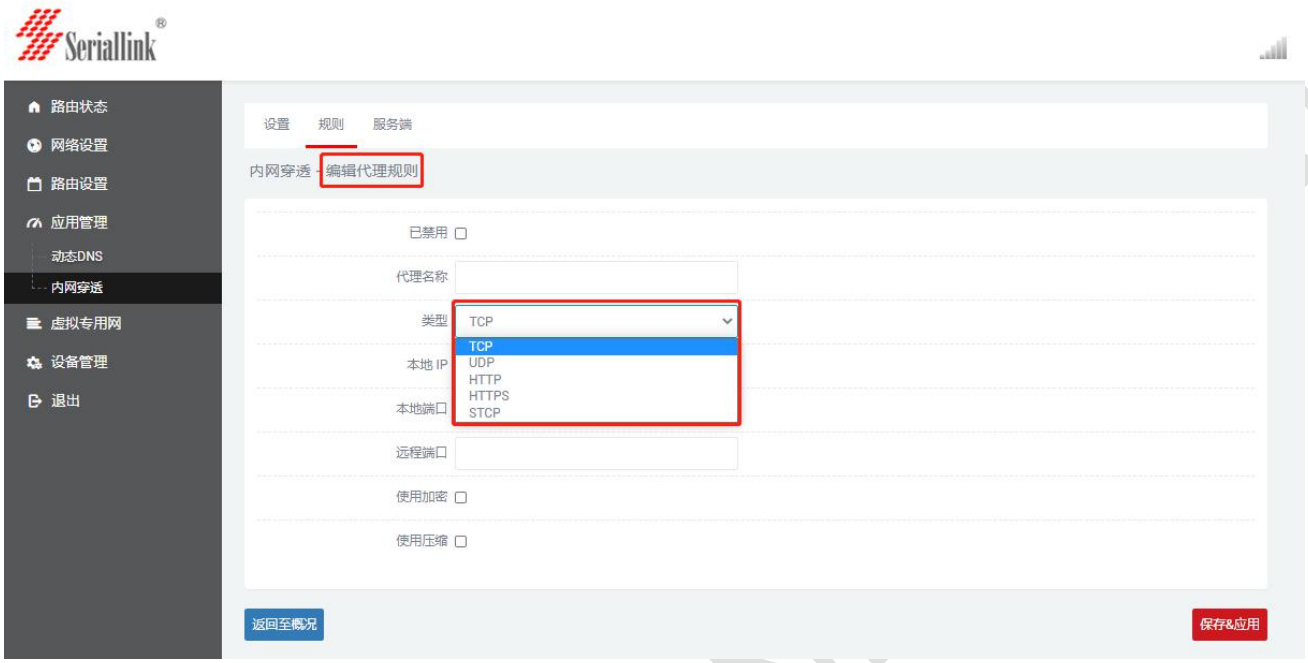


显示服务正在影响说明 frp 客户端启动成功。



（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。



2.3.1 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：111.111.111.111:600 其中 111.111.111.111 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）

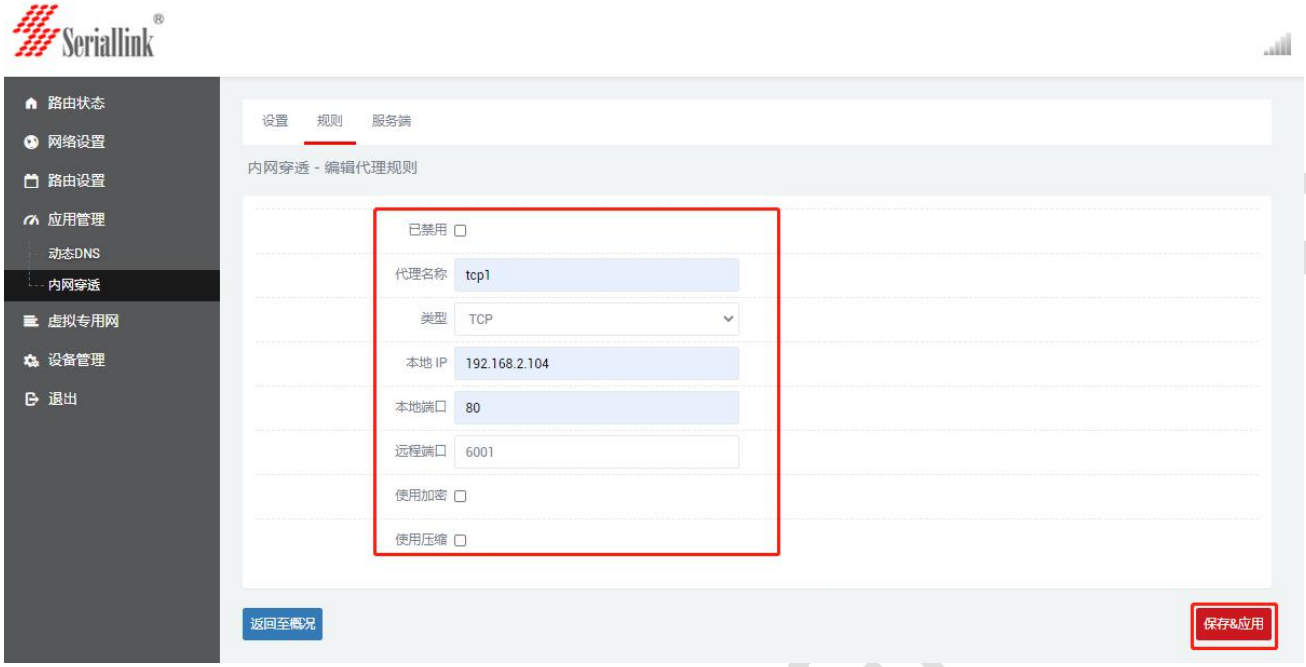
本地端口：该设备需要转发到公网的端口

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。

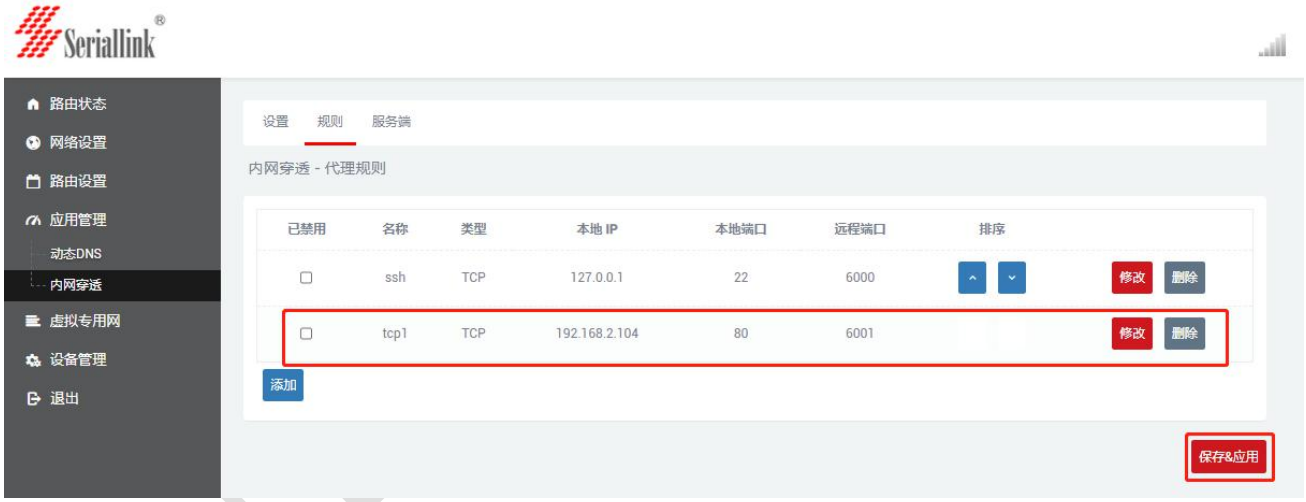
使用加密，使用压缩：这两个根据需要进行勾选

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”。



生成了一条新的规则后，需要点击“保存&应用”使规则生效。



通过公网 ip 和端口号访问本地设备的本地端口，111.111.111.111:6001 访问 192.168.2.104:80。

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。

2.3.2 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。

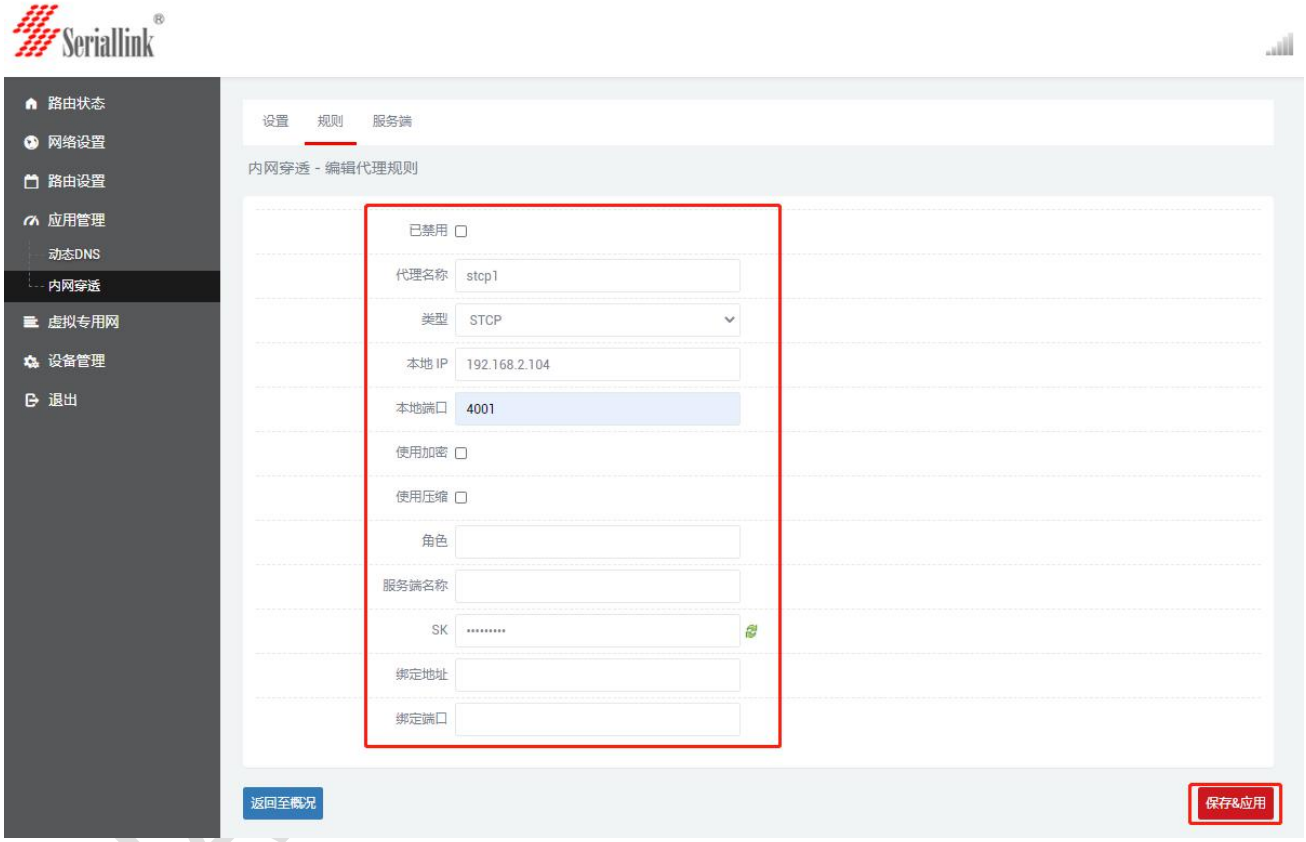
本地 IP：本机设备或 lan 口为下接设备分配的 IP 地址。

本地端口：该设备要开放到公网的端口。

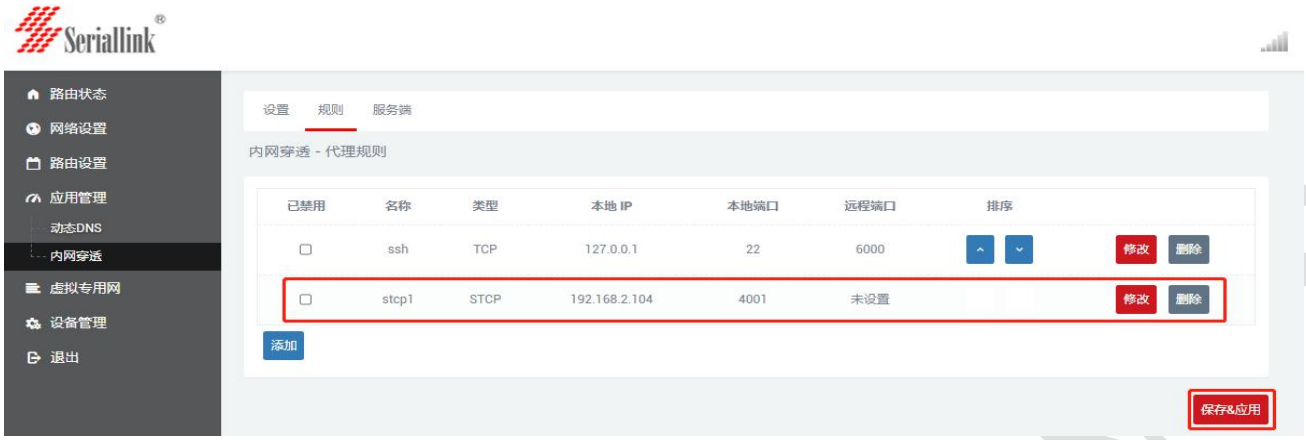
SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

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。



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

#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
#客户端1的代理名称
server_name=stcp1
#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
```

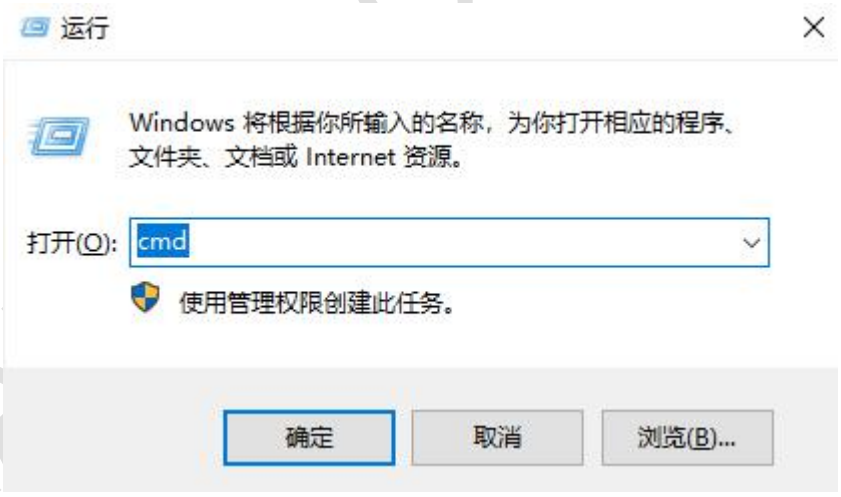
与公网服务器配置一致即可

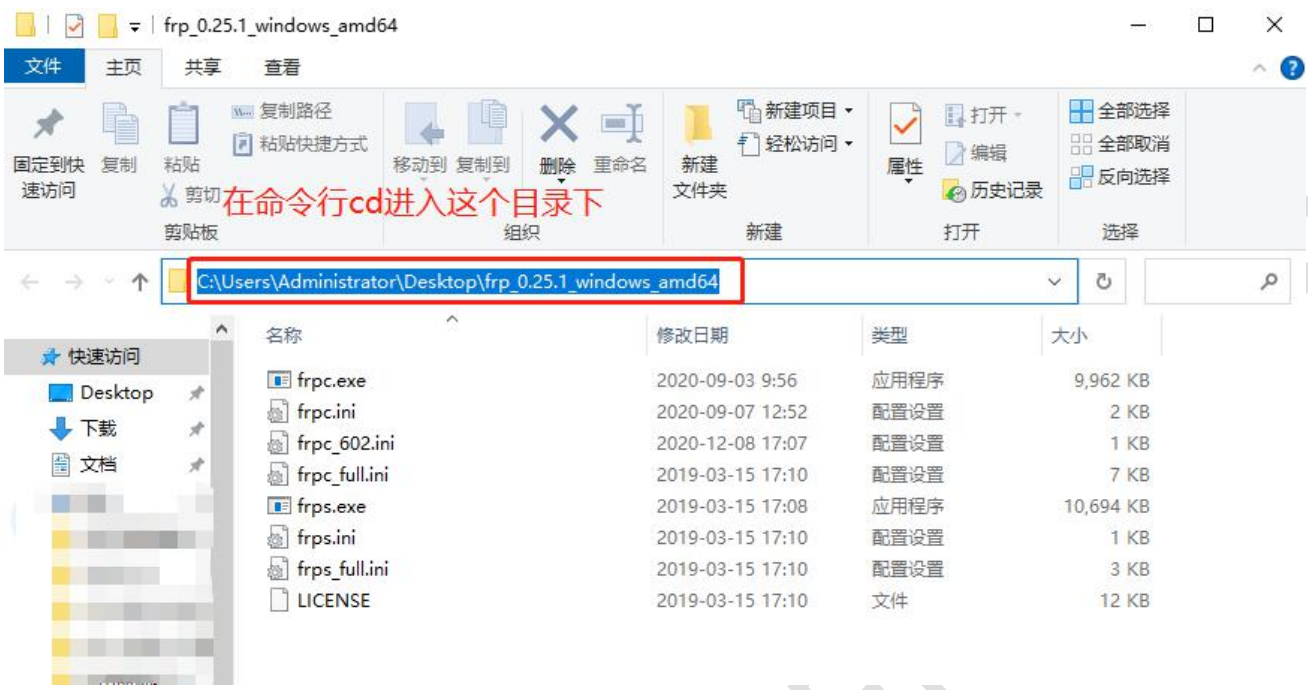
访问端角色要设置visitor

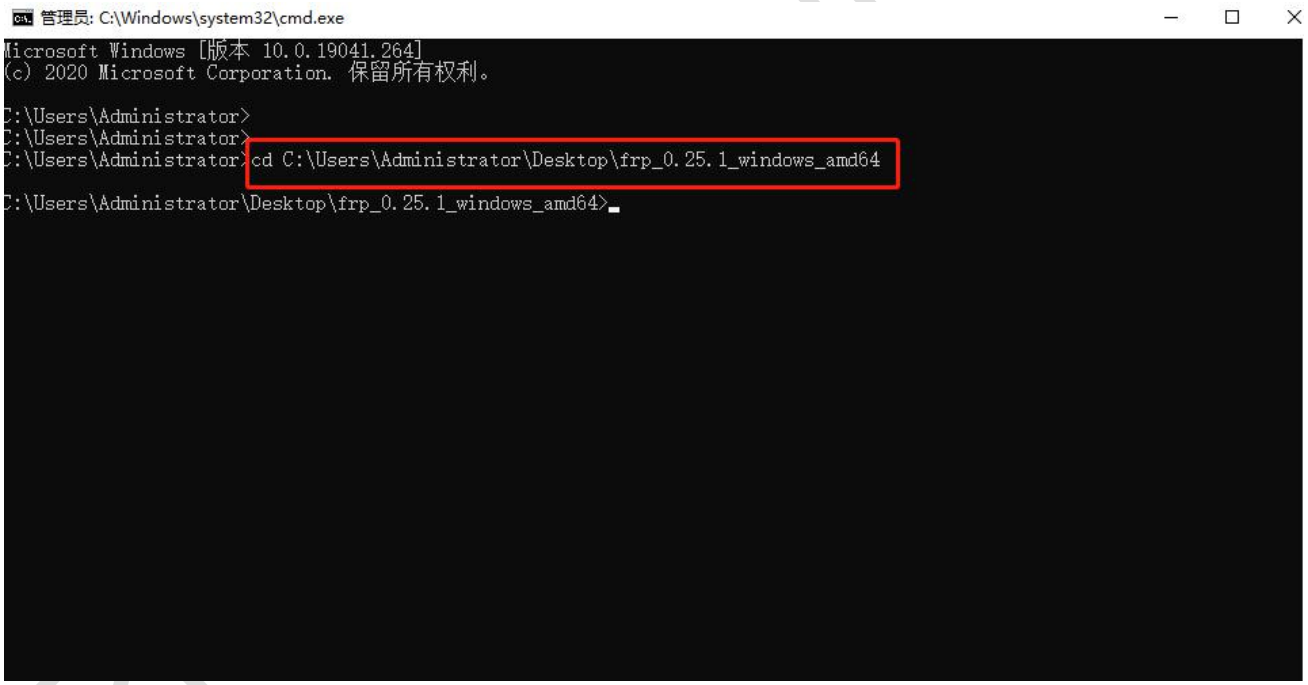
要与要访问的客户端的代理名称一致

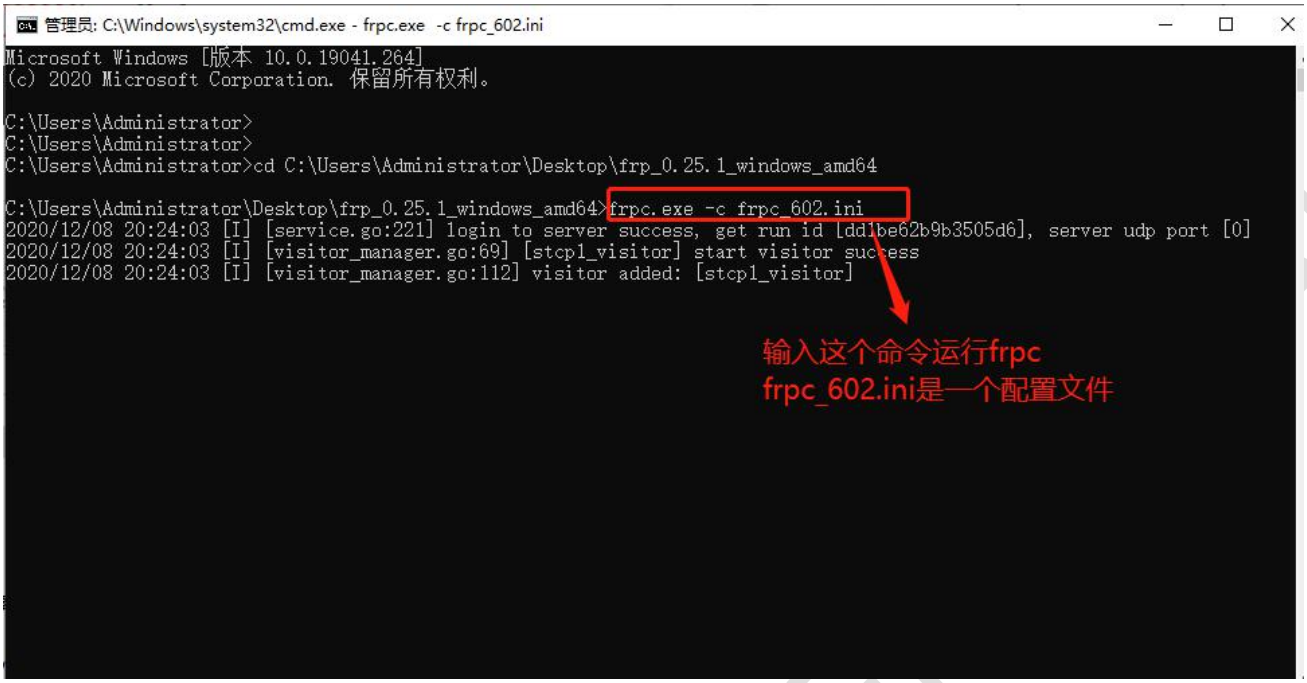
一般设置为本地的ip地址（127.0.0.1），端口号要本地没有使用的

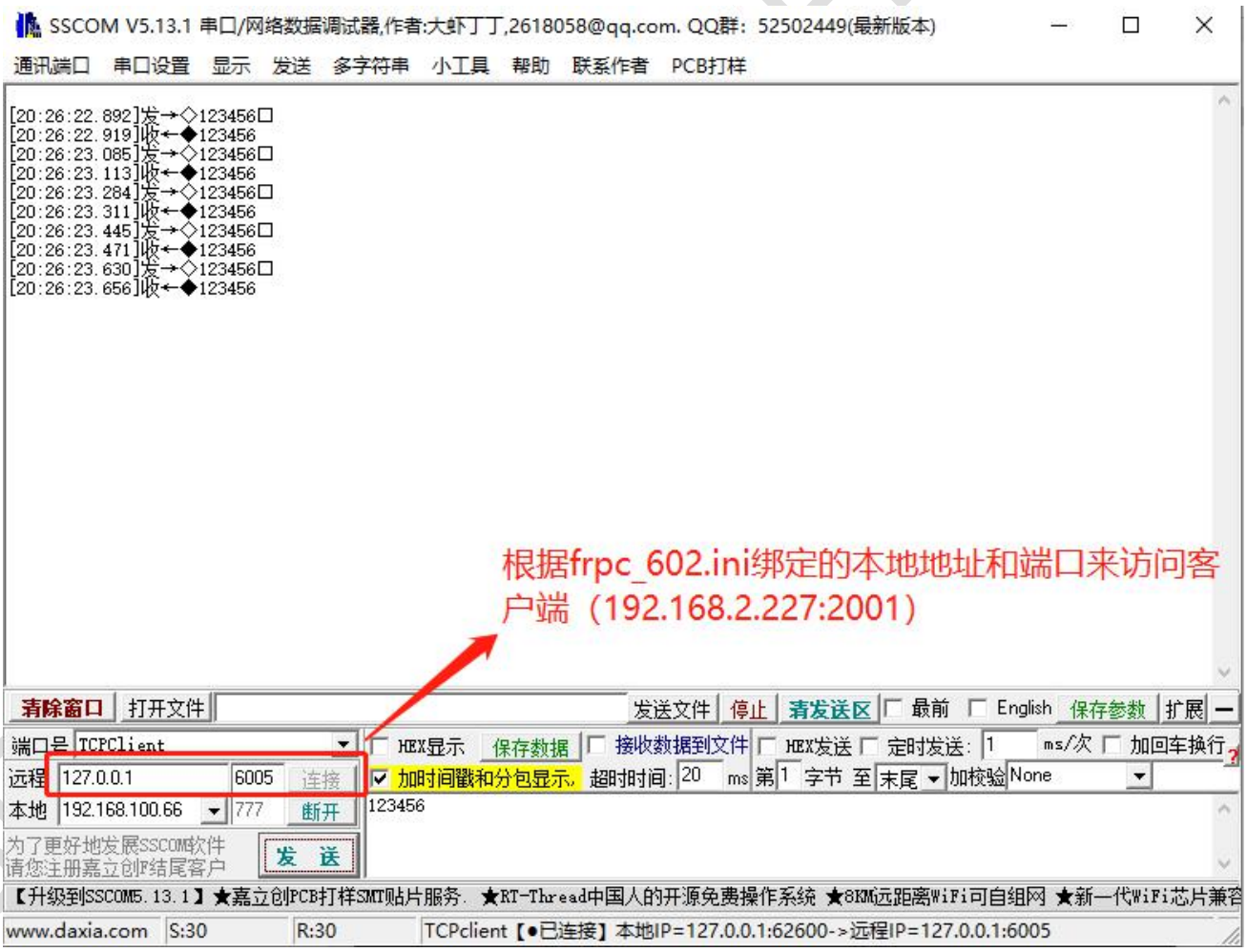
利用快捷键“win+R”，快速打开 cmd 命令行




frp_0.25.1_windows_amd64
文件
主页
共享
查看
固定到快速访问
复制
粘贴
复制路径
粘贴快捷方式
剪切
在命令行cd进入这个目录下
剪贴板
移动到
复制到
删除
重命名
组织
新建文件夹
新建项目
轻松访问
新建
属性
打开
编辑
历史记录
打开
全部选择
全部取消
反向选择
选择
C:\Users\Administrator\Desktop\frp_0.25.1_windows_amd64
快速访问
Desktop
下载
文档
名称
修改日期
类型
大小
frpc.exe 2020-09-03 9:56 应用程序 9,962 KB
frpc.ini 2020-09-07 12:52 配置设置 2 KB
frpc_602.ini 2020-12-08 17:07 配置设置 1 KB
frpc_full.ini 2019-03-15 17:10 配置设置 7 KB
frps.exe 2019-03-15 17:08 应用程序 10,694 KB
frps.ini 2019-03-15 17:10 配置设置 1 KB
frps_full.ini 2019-03-15 17:10 配置设置 3 KB
LICENSE 2019-03-15 17:10 文件 12 KB


管理员: C:\Windows\system32\cmd.exe
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>





（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

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。

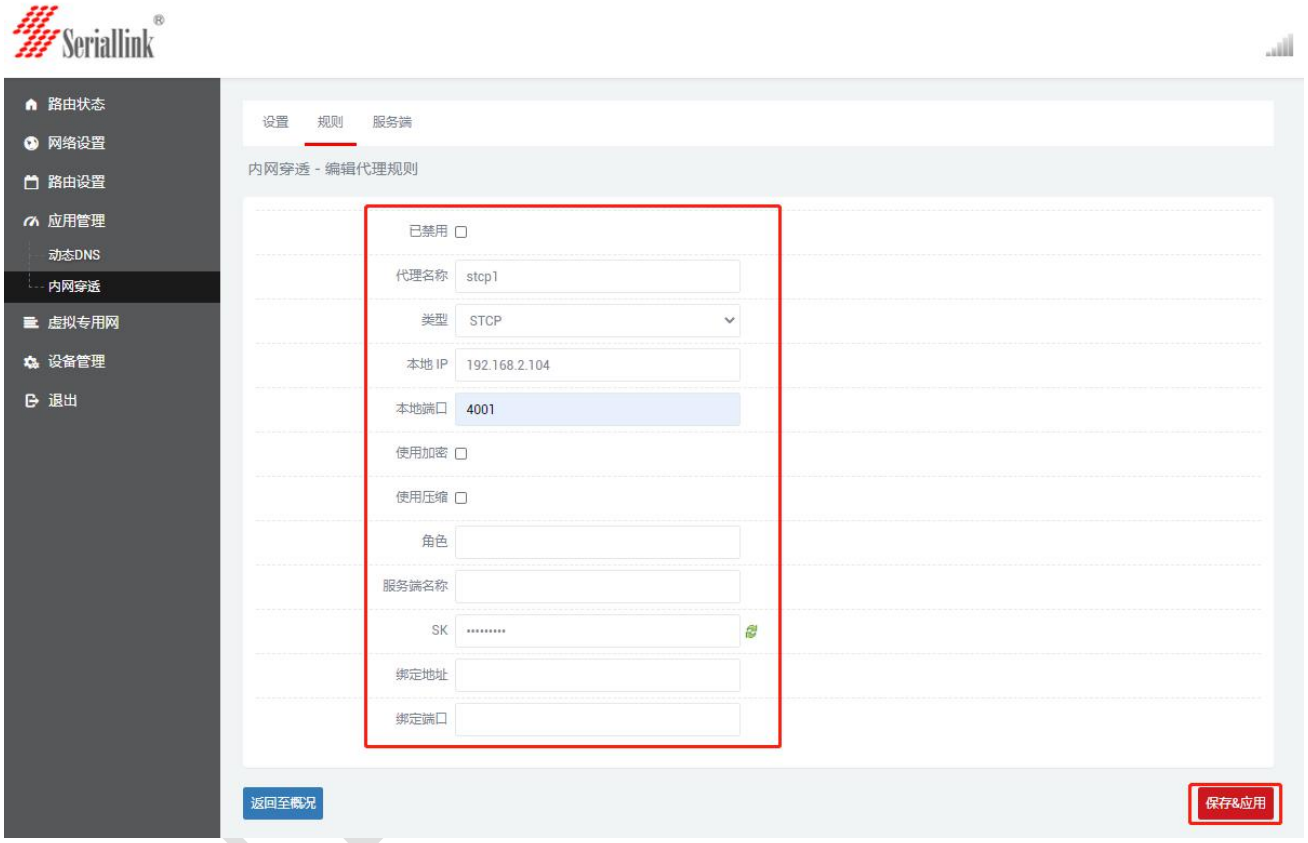
本地 IP：本机设备或 lan 口为下接设备分配的 IP 地址。

本地端口：该设备要开放到公网的端口。

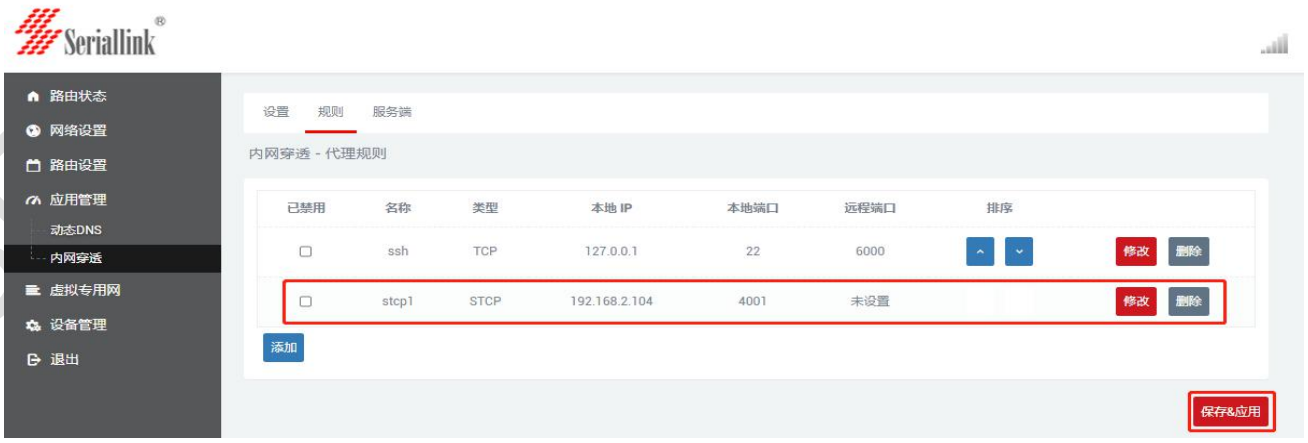
SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

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。



生成了新的规则后，需要点击“保存&应用”使该规则生效。



② 配置访问端（另一台路由器）

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。

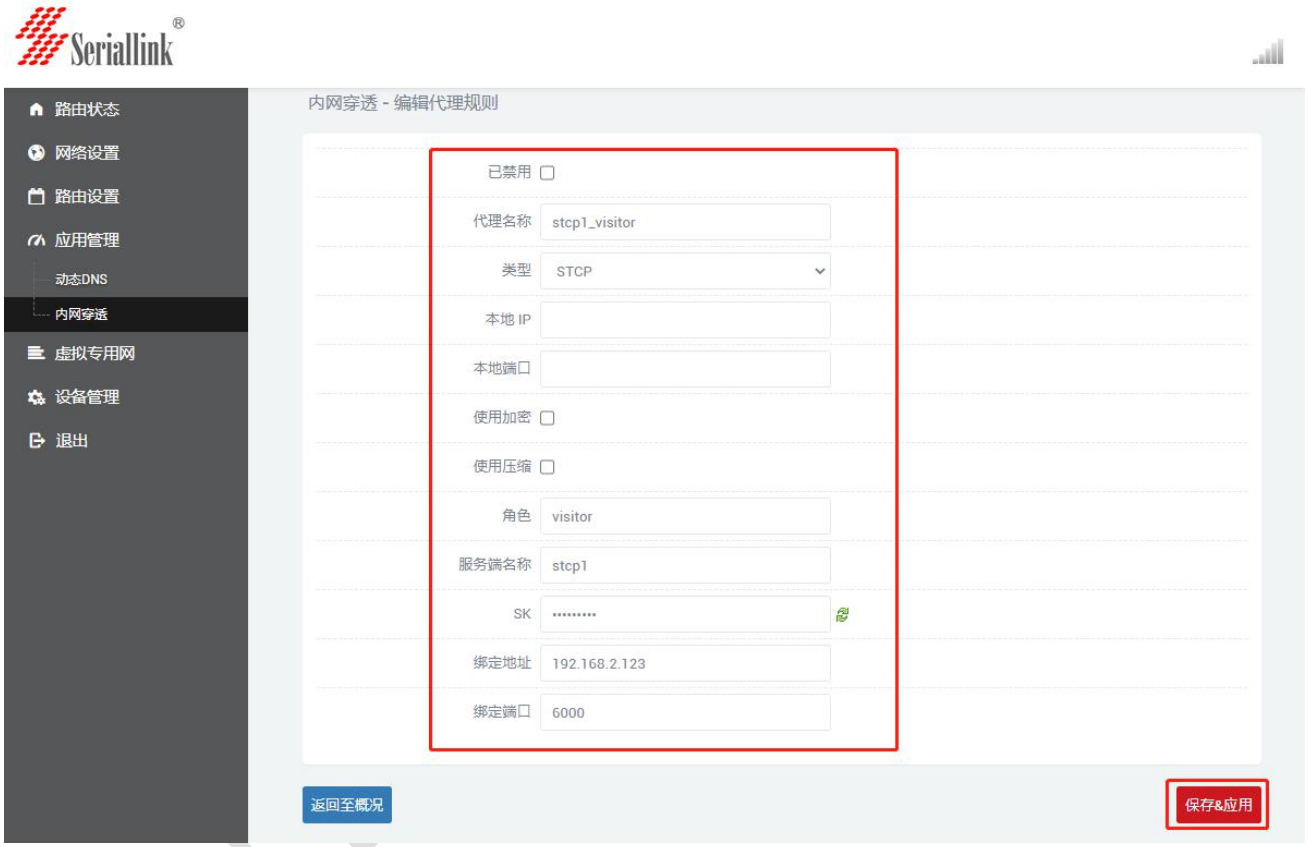
SK：设置一个密码，访问端访问这个设备的时候需要输入这里设置的 SK。

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。



生成了新的规则后，需要点击“保存&应用”使该规则生效。

2.3.3 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）

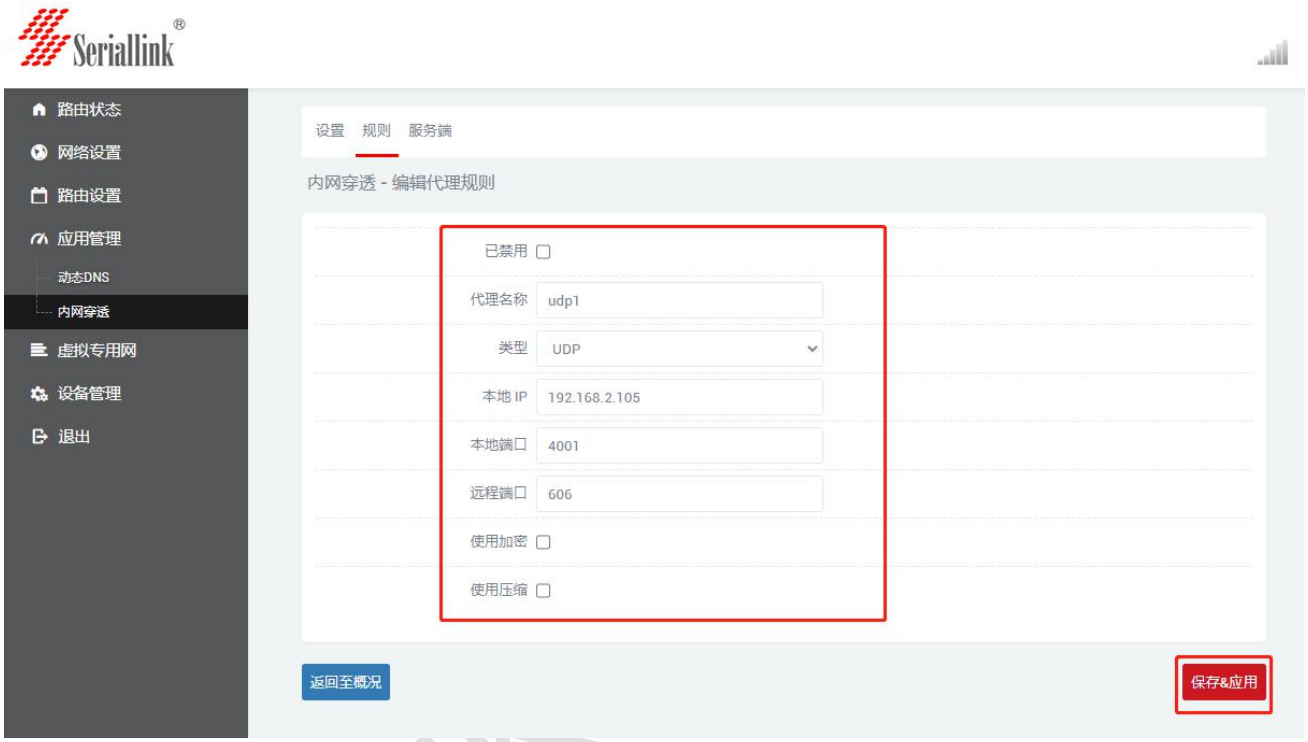
本地端口：该设备需要转发到公网的端口，必须是使用 UDP 协议的端口。

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。

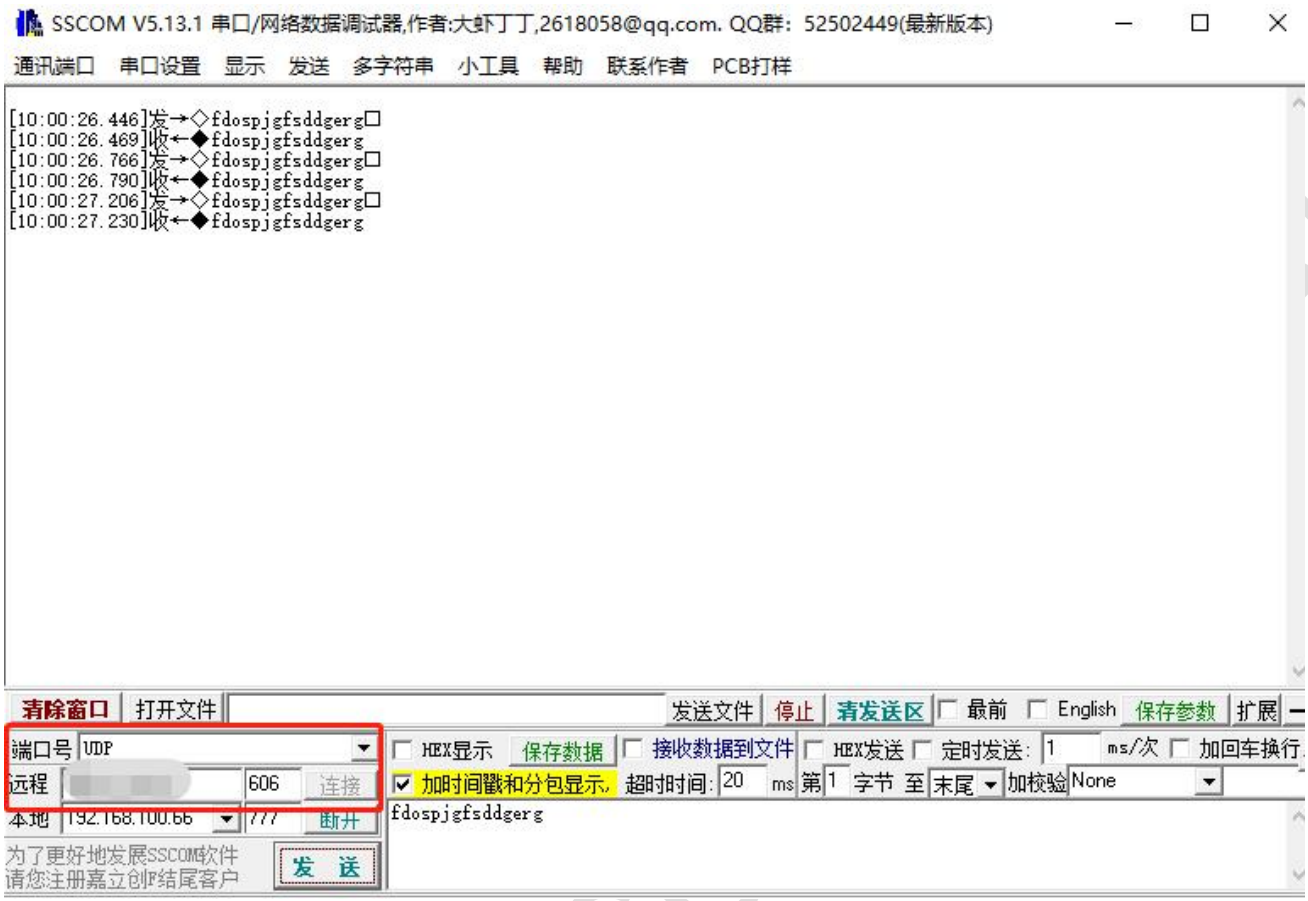
规则可以添加多条，远程端口和代理名称不要冲突就可以了。

配置完成后点击“保存&应用”。



生成了新的规则后，需要点击“保存&应用”使该规则生效。

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）



2.3.4 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。

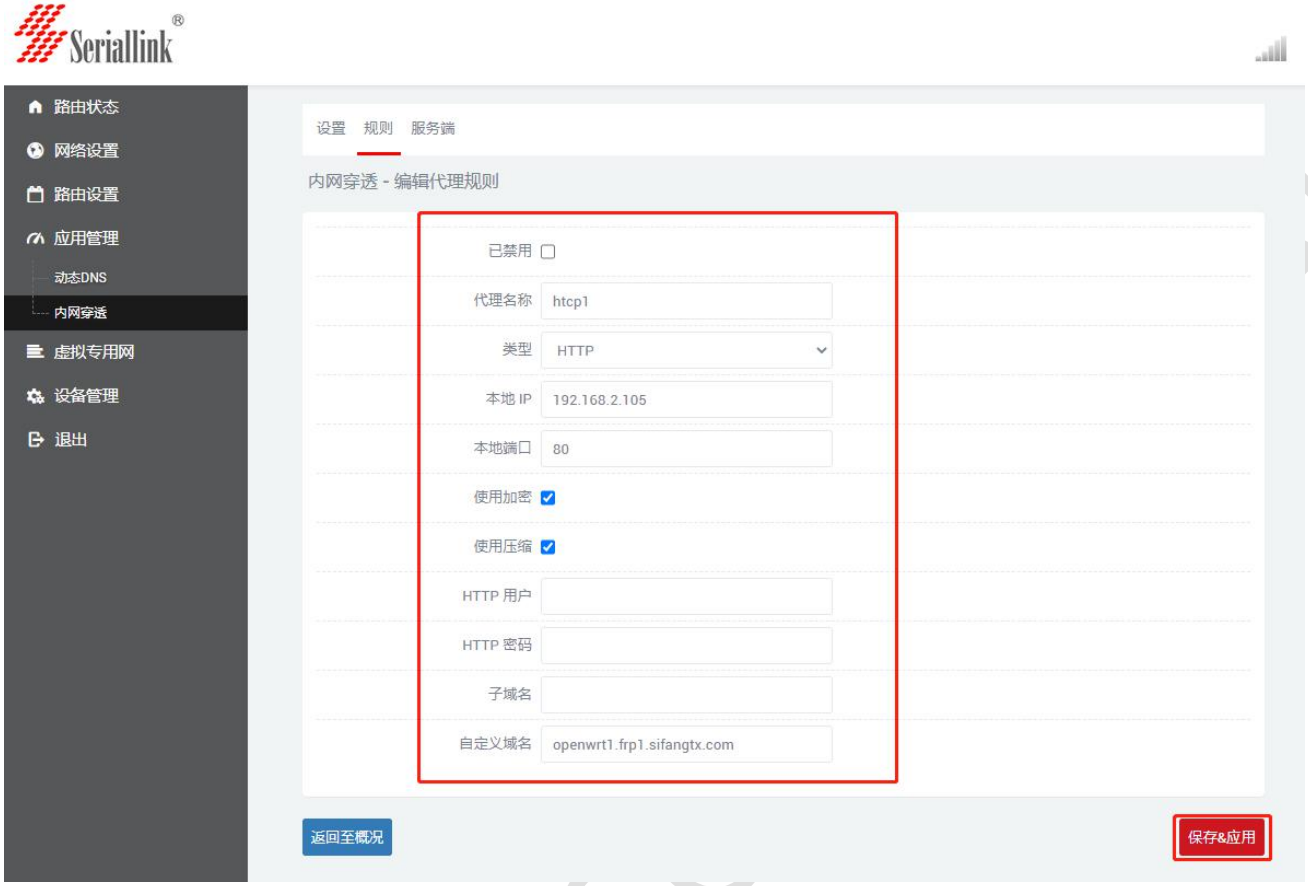
本地 ip：填写本机的 ip 或者本机 lan 口为下接设备分配的 ip。（需要通过公网访问的设备的 ip 地址）。

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。



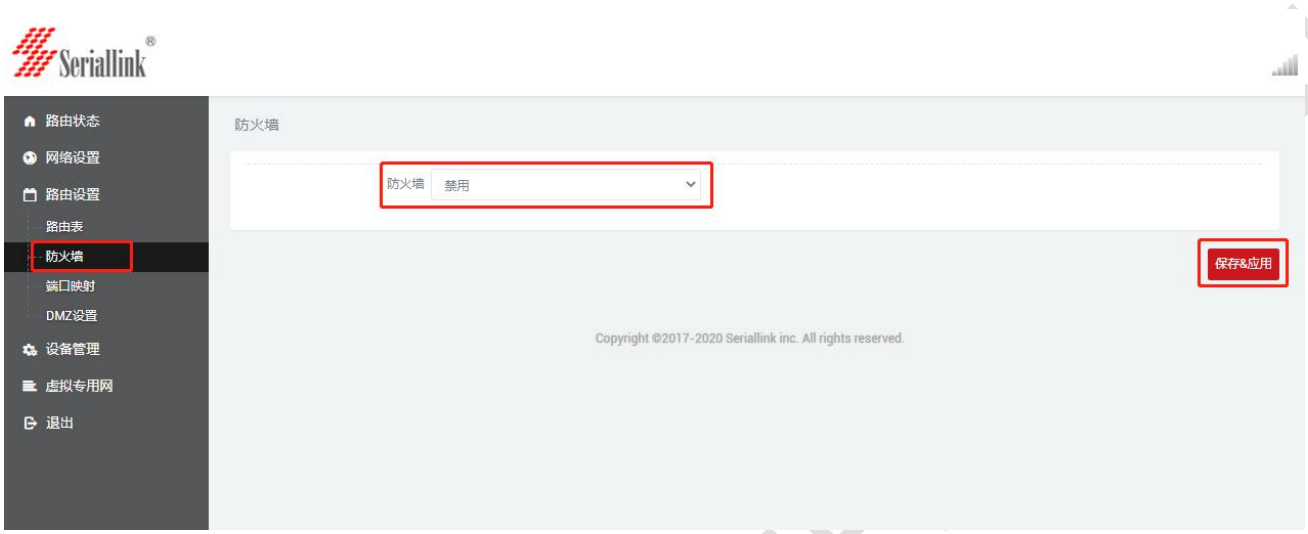
生成了新的规则后，需要点击“保存&应用”使该规则生效。

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。

第三章 VPN（虚拟专用网）

配置 VPN 的时候需要先将防火墙禁用，不管用哪个 VPN，都需要先将防火墙禁用。



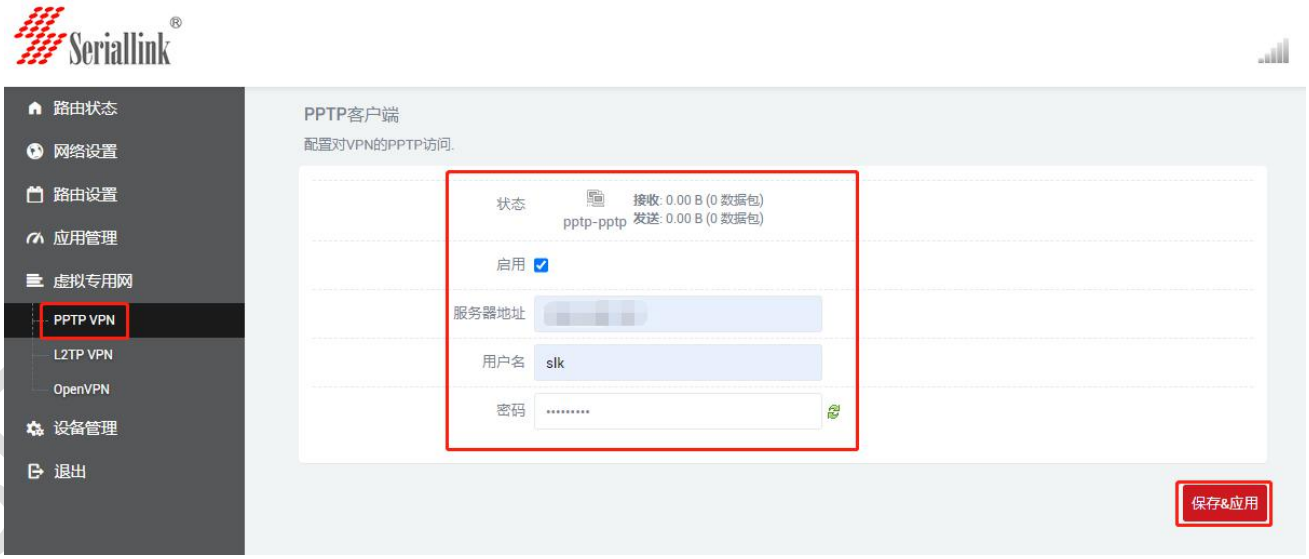
3.1 PPTP VPN

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，将启用不勾选后点击“保存&应用”即可。

3.2 L2TP VPN

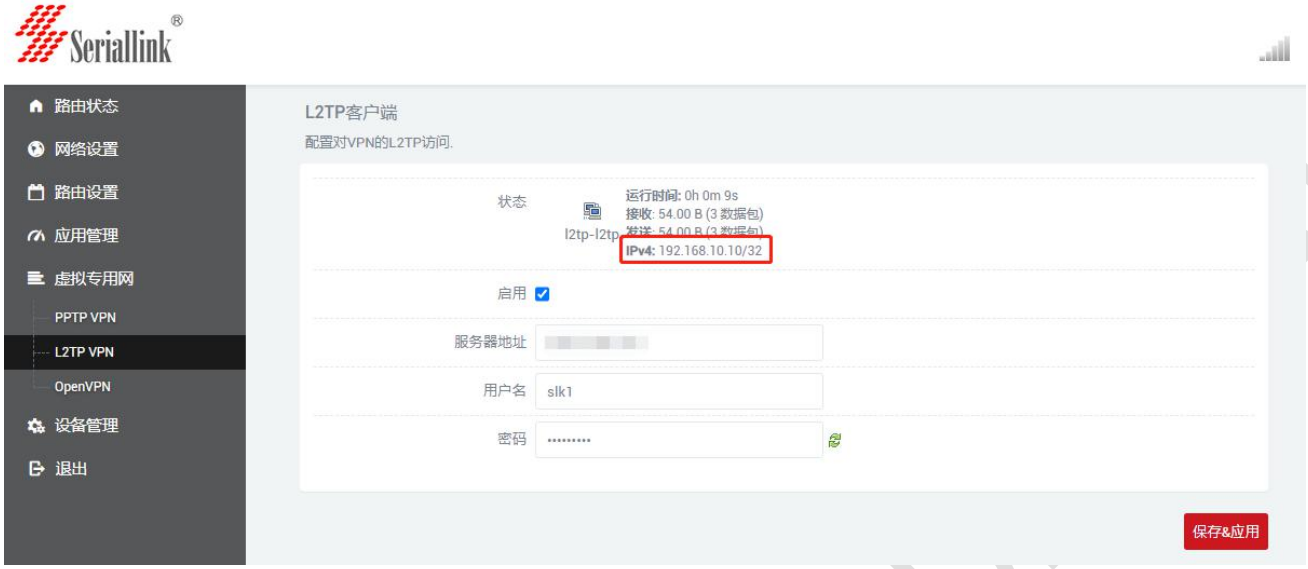
导航栏“虚拟专用网”——“L2TP VPN”,选择启用，根据服务器的设置填写用户名和密码，点击“保存&应用”。

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。

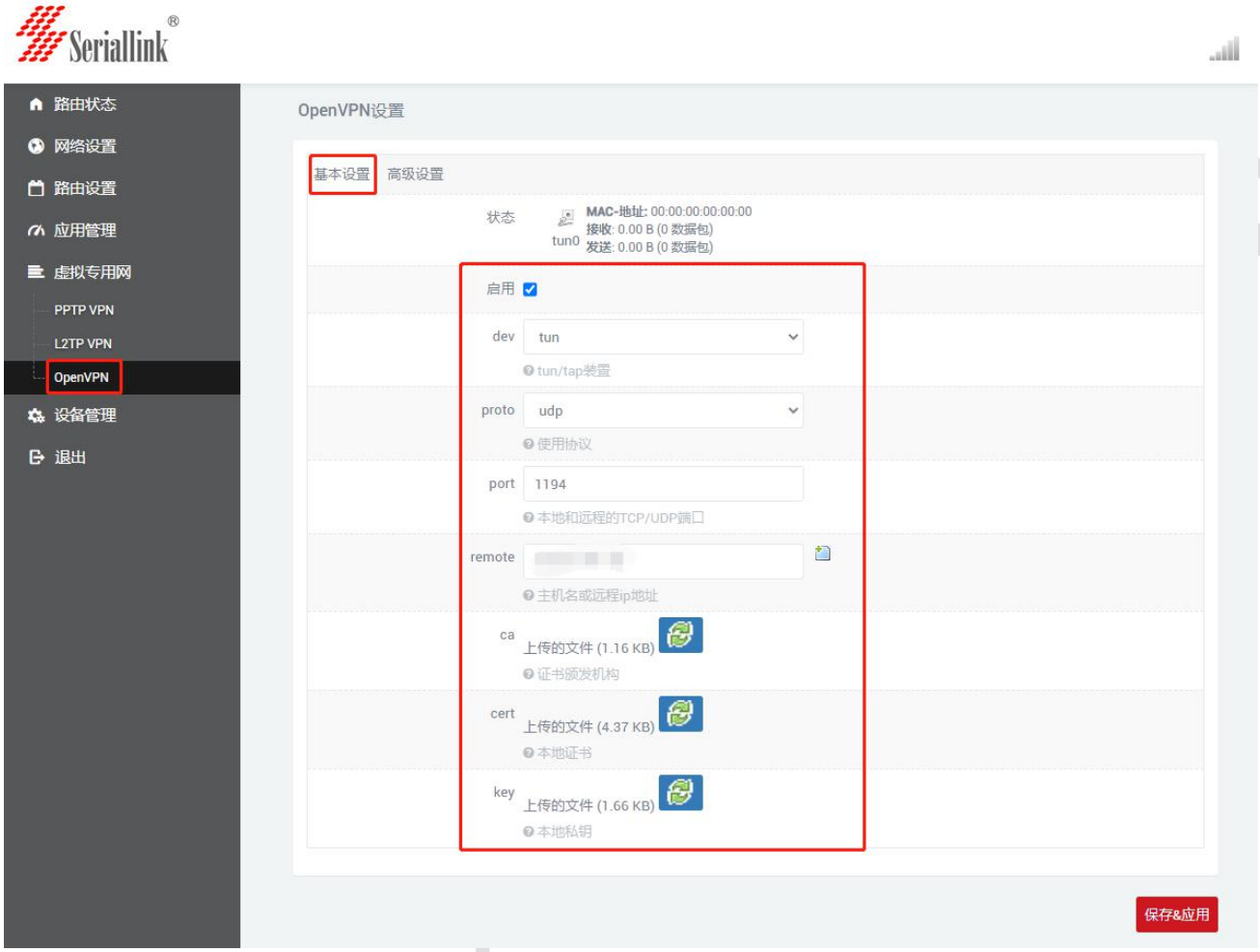
用户名，密码：填写服务端设置的用户名和密码。

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。

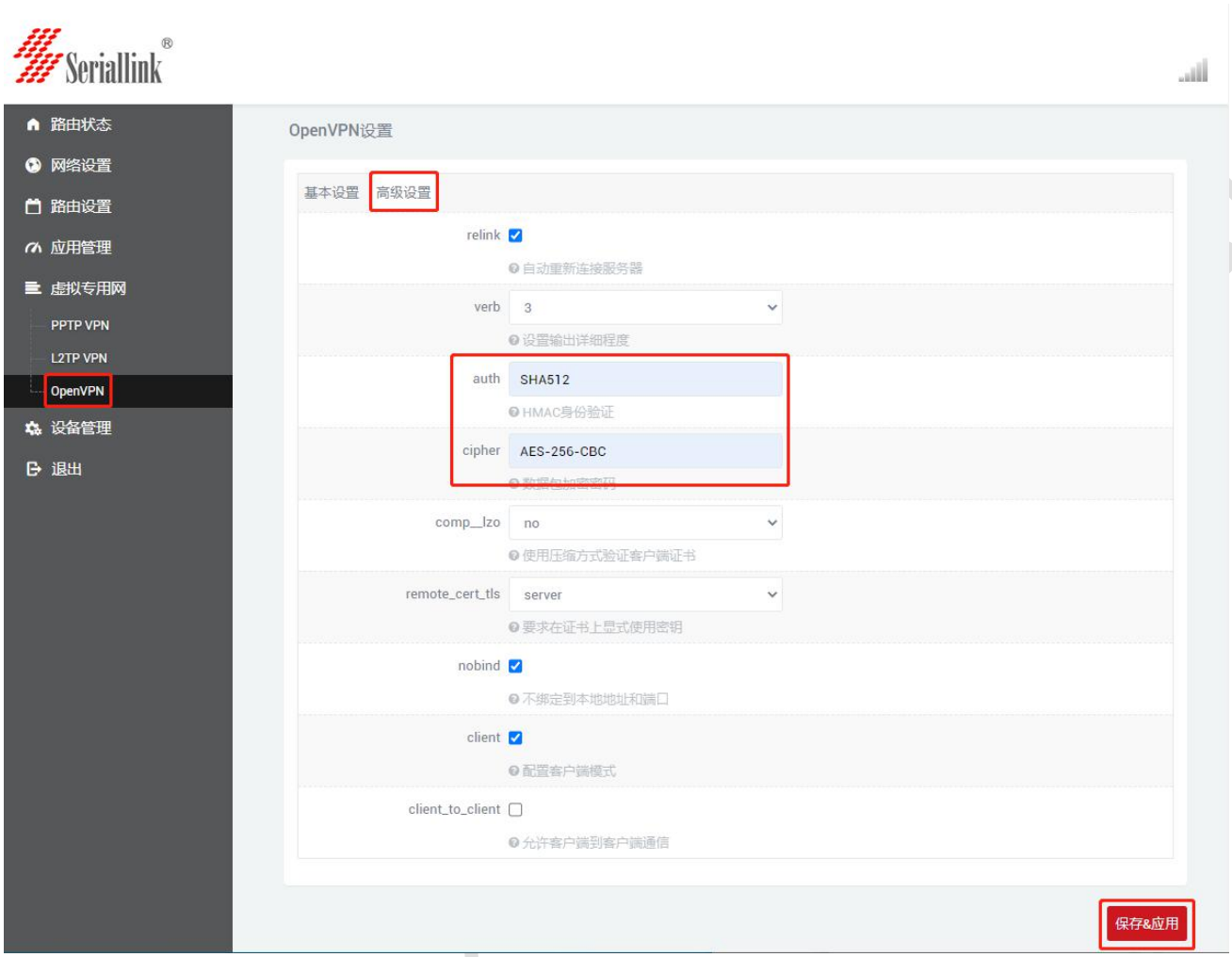


3.3 OPENVPN

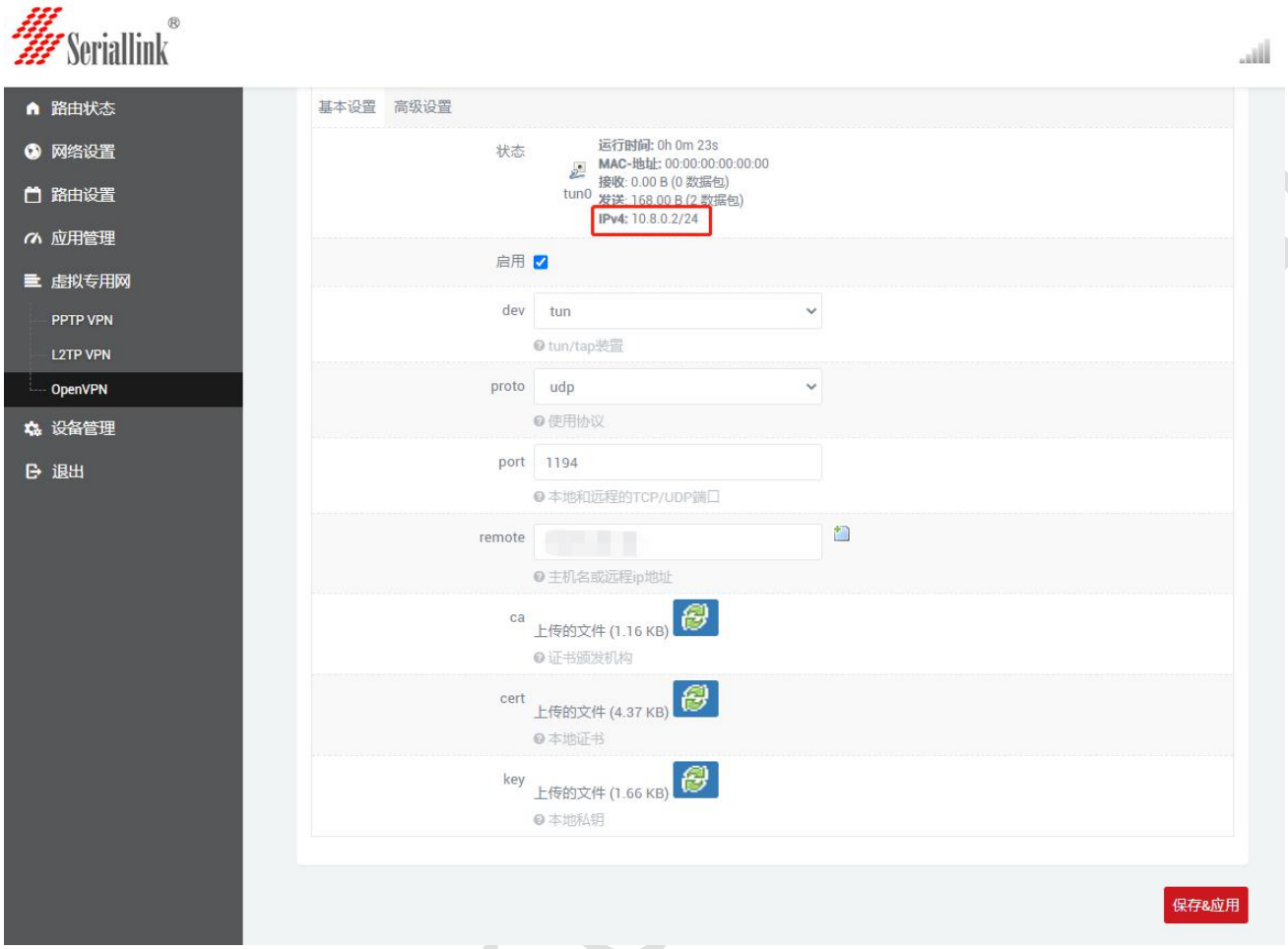
导航栏“虚拟专用网”——“openvpn”，所有配置与服务器一致后点击“保存&应用”，三个证书由服务端提供。



auth,cipher 这两个也要与服务端一致，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出现服务器给它分配的地址，如果不用 openvpn 的话，将启用不勾选后点击“保存&应用”即可。



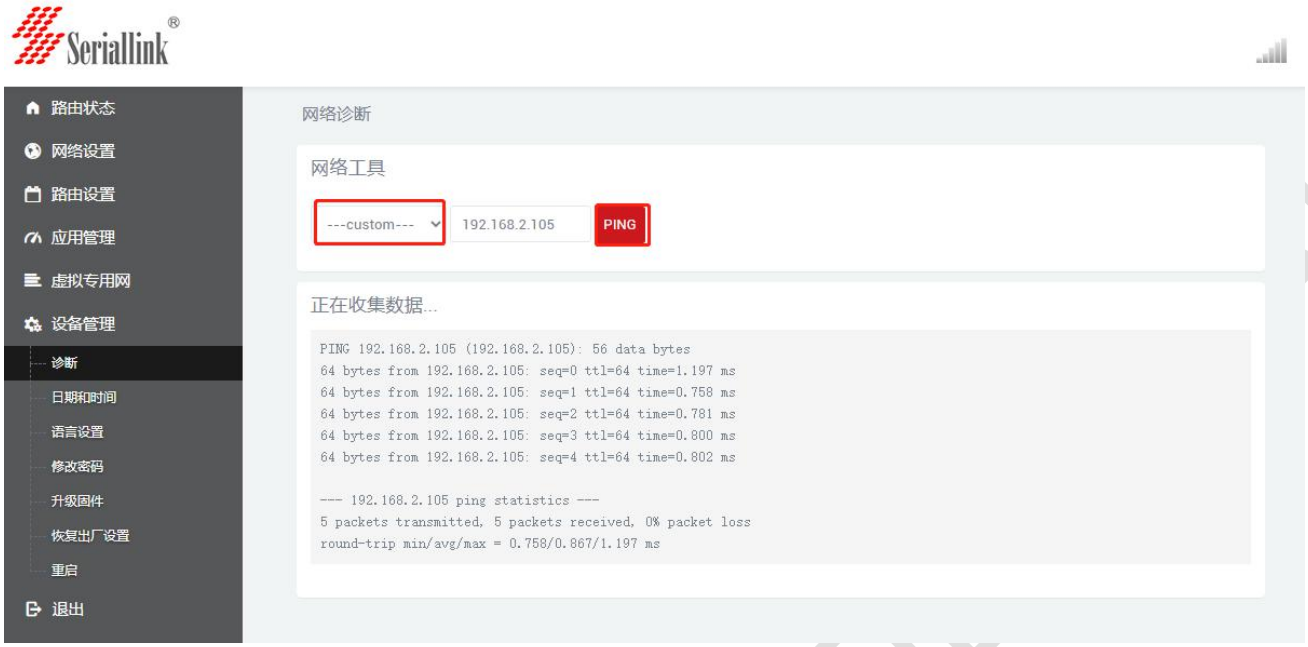
第四章 基本管理（设备管理）

4.1 诊断

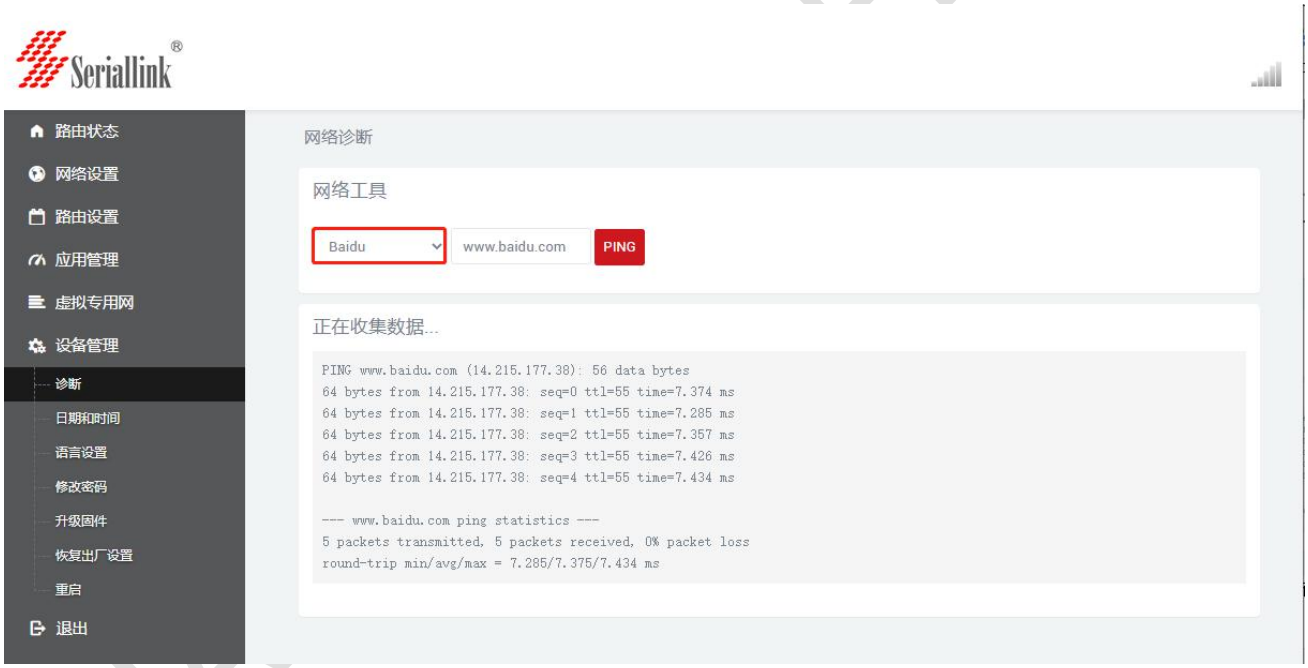
通过诊断可以判断路由器与下接设备之间是否能够通信，设备是否能够上网，设备连接 VPN 是否成功。还可以用来测试别的方面，根据自己的需求进行测试即可。

导航栏“设备管理”——“诊断”。

custom：自定义，一般用来测试能否 ping 通下接设备，填写 ip 地址。

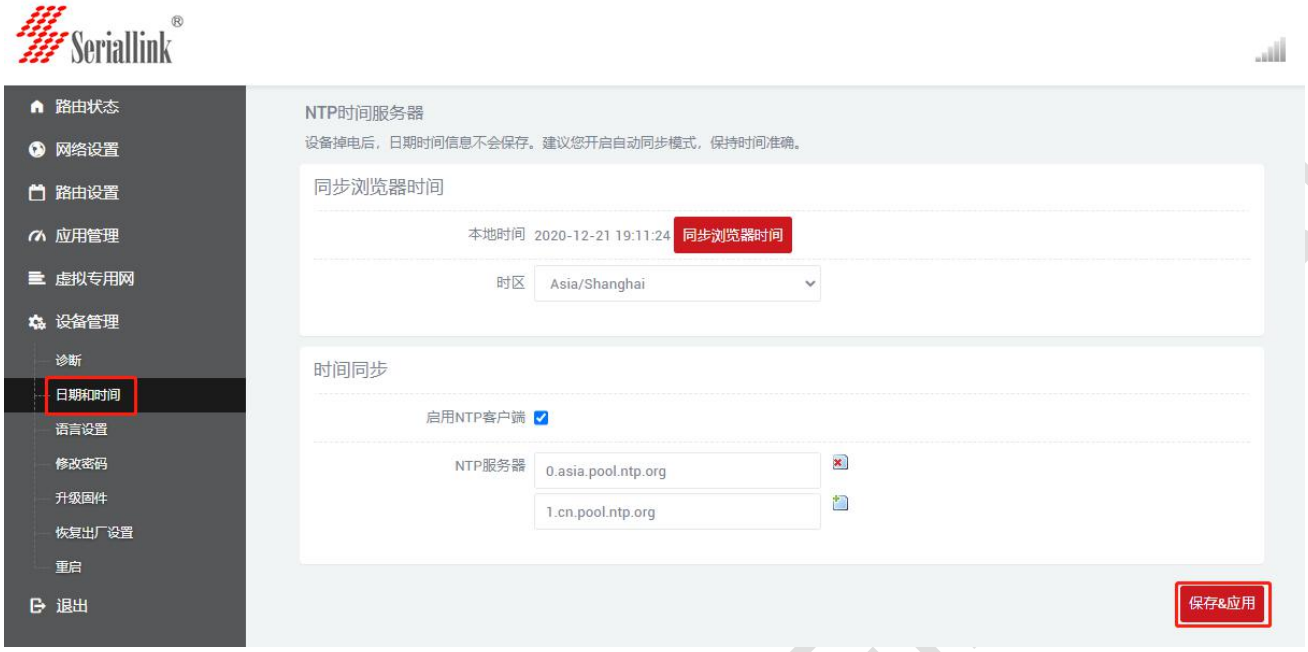


Baidu：ping 百度，能 ping 通说明设备能够上网，不能 ping 通说明设备不能上网。



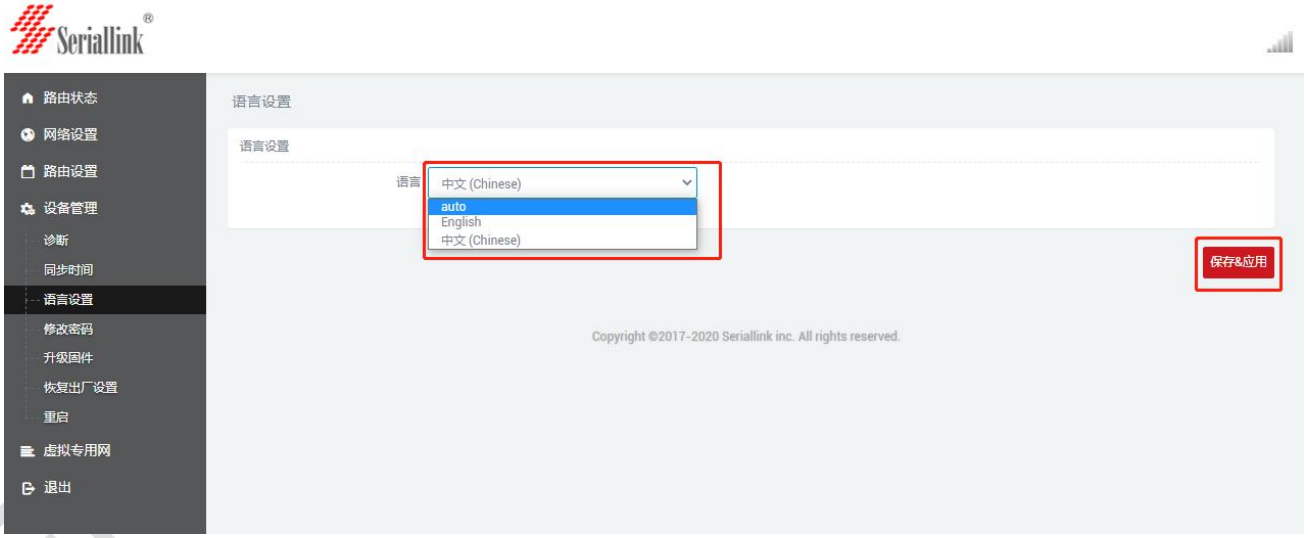
4.2 日期和时间

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“设备管理”——“日期和时间”，设置完成后点击“保存&应用”。



4.3 语言设置

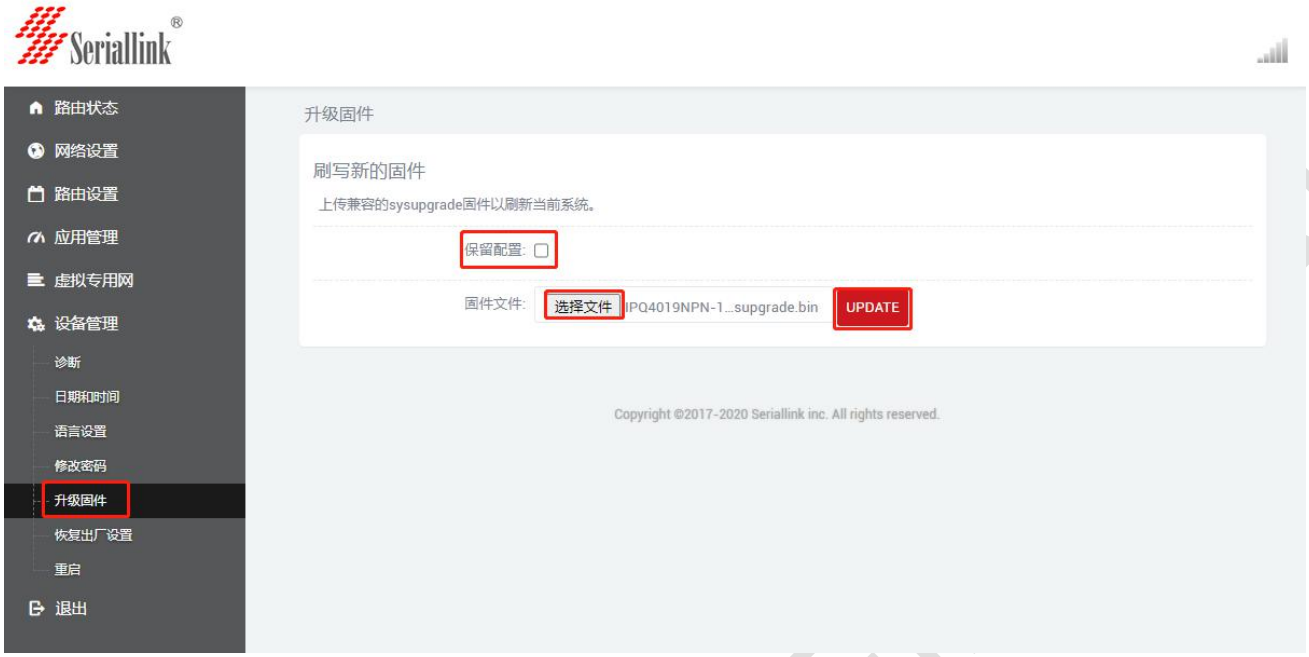
根据自己需要更改页面显示的语言，可以选择英文或者中文，在导航栏“设备管理”——“语言设置”进行更改。

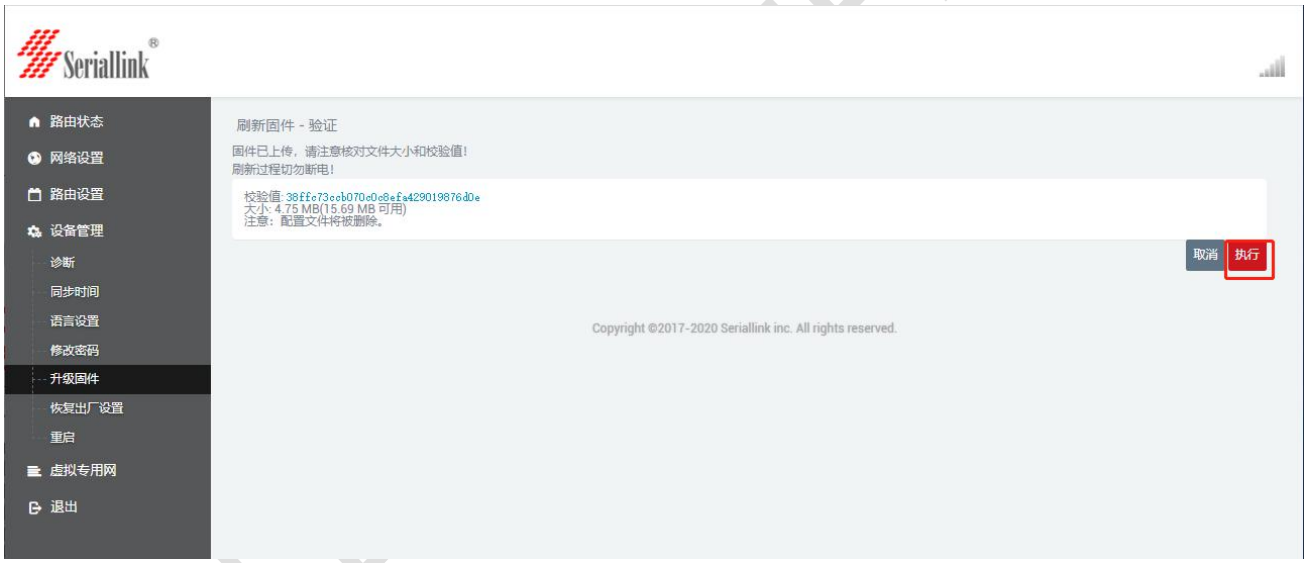


4.4 升级固件

导航栏“设备管理”——“升级固件”，选择文件后点击“UPDATE”，上传完毕后会出现 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。

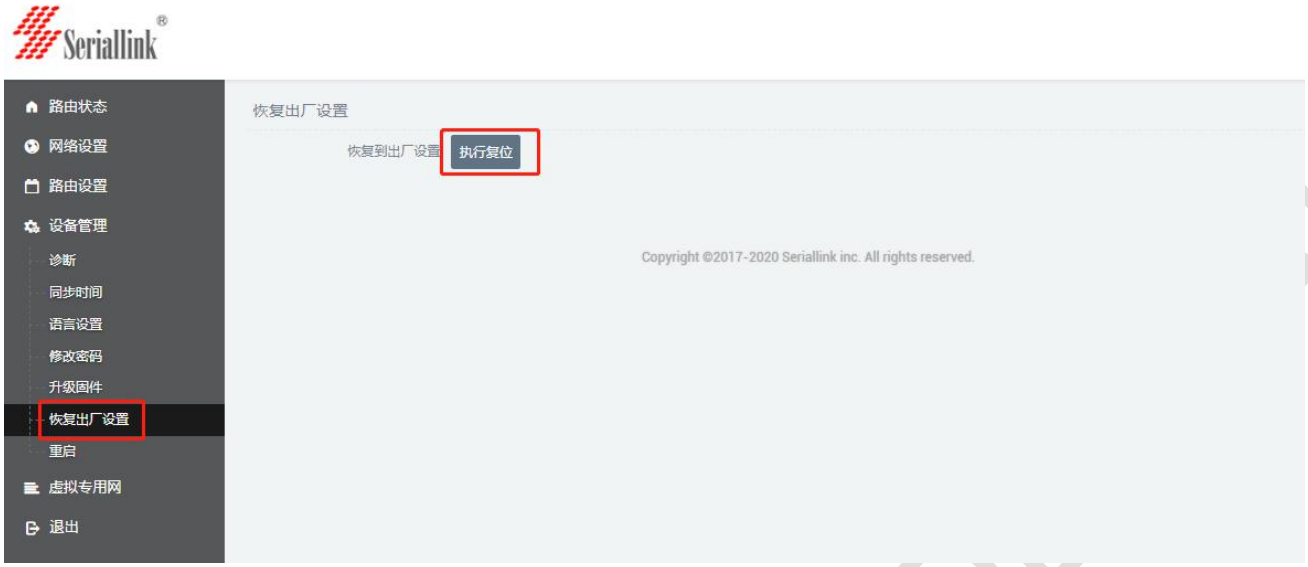
升级固件时需要将“保留配置”选项不勾选。





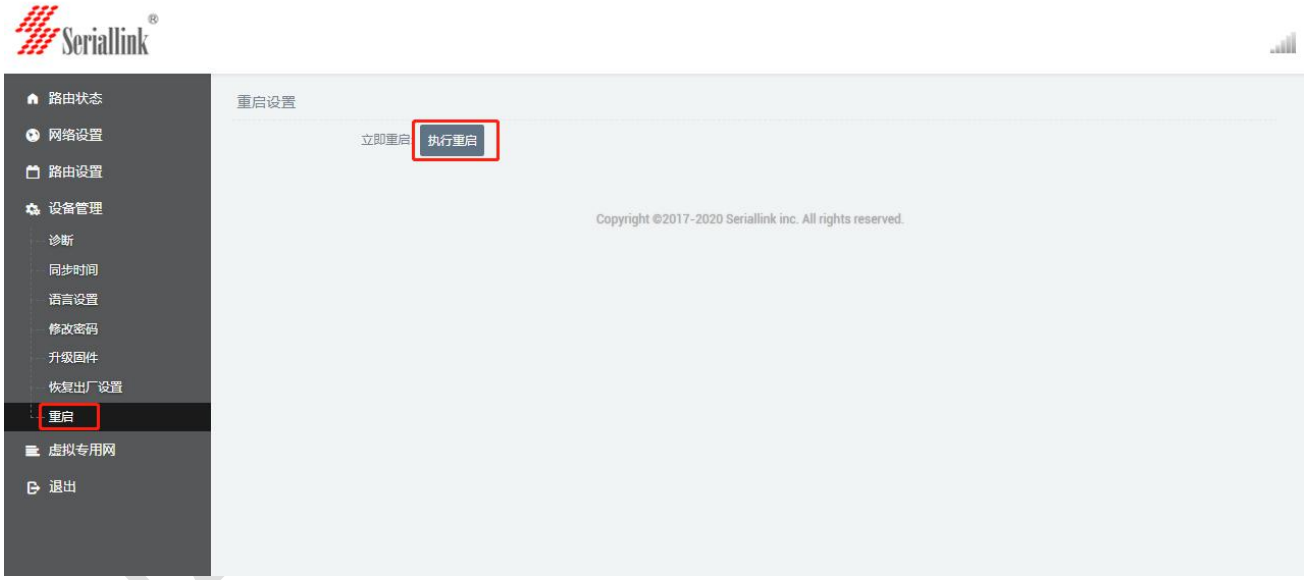
4.5 恢复出厂设置

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‘设备管理’——‘恢复出厂设置’，点击‘执行复位’，即可将设备恢复出厂值。



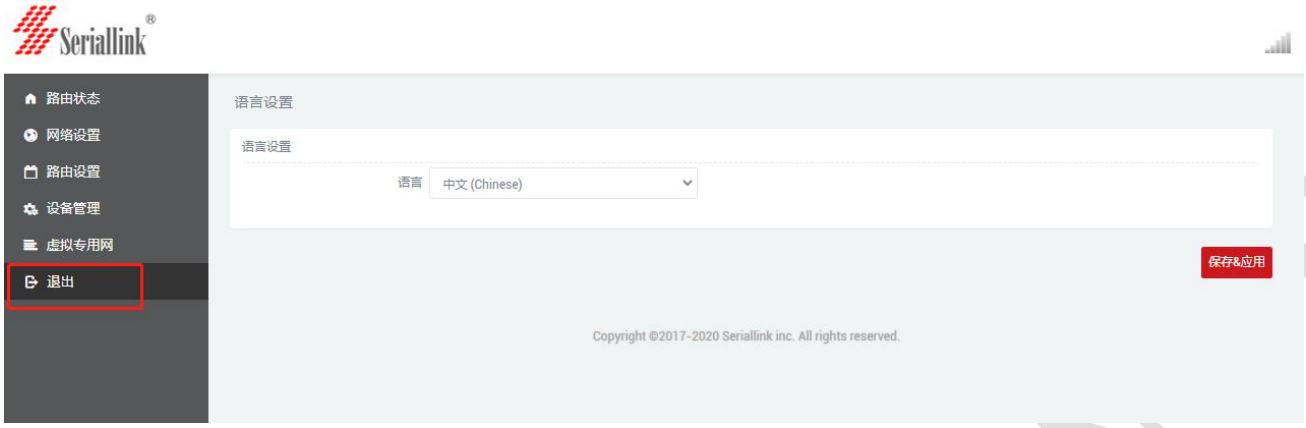
4.6 设备重启

设备可以通过页面进行重启，导航栏“设备管理”——“重启”，点击“执行重启”，即可重启设备。



4.7 页面退出

点击‘退出’既可以退出页面。



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**