SUNDRAY

NAC 3.10.0 用户手册

SUNDRAY 信锐技术

目录

声明

Copyright © 2022 深圳市信锐网科技术有限公司及其许可者版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

SUNDRAY 为深圳市信锐网科技术有限公司的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系深圳市信锐网科技术有限公司客户服务部。

前言

本手册各章节内容如下：

第 1 部分 SUNDRAY NAC 产品安装指南。该部分主要介绍 NAC 设备的外观特点及功能特性和性能参数，以及连接前的准备和注意事项。

第 2 部分 SUNDRAY NAC 控制台的使用，如何登陆控制台等。

第 3 部分 SUNDRAY NAC 功能说明及使用。

第 4 部分 案例集。讲解各功能模块在常见环境下的配置案例。

本手册以 NAC-6200 为例进行配置。由于各型号产品硬件和软件规格存在一定差异，所有涉及产品规格的问题需要和深圳市信锐网科技术有限公司联系确认。

本书约定

图形界面格式约定

文字描述	代替符号	举例
按钮	边框+阴影+底纹	“确定”按钮可简化为确定
菜单项	『 』or 【 】	菜单项“系统设置”可简化为『系统设置』或【 】
连续选择菜单项及子菜单项	→	选择【系统设置】→【接口配置】
下拉框、单选框、复选框选项	[ ]	复选框选项“启用用户”可简化为[启用用户]
窗口名	【 】	如点击弹出【新增用户】窗口
提示信息	“ ”	提示框中显示“保存配置成功，配置已修改，需要重启 DLAN 服务才能生效，是否立即重启该服务？”

各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

小心、注意：提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。

警告：该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。

说明、提示、窍门：对操作内容的描述进行必要的补充和说明。

技术支持

用户支持邮箱： support@sundray.com.cn

技术支持热线电话： 400-878-3389（手机、固话均可拨打）

公司网址： www.sundray.com.cn

致谢

感谢您使用我们的产品及用户手册，如果您对我们的产品或用户手册有什么意见和建议，您可以通过电话、论坛或电子邮件反馈给我们，我们将不胜感谢。

安装指南

本部分主要介绍了 SUNDRAY NAC 系列产品的构成与硬件安装。硬件安装正确之后，您可以进行配置和调试。

1.1. 环境要求

SUNDRAY NAC 设备可在如下的环境下使用。

- 输入电压：110V~230V
- 温度：0～45℃
- 湿度：5～90%

为保证系统能长期稳定的运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

1.2. 电源

SUNDRAY　NAC 系列产品使用交流 110V 到 230V 电源。在您接通电源之前，请保证您的电源有良好的接地措施。

1.3. 产品外观

图 1 SUNDRAY　NAC6200 外观图

图 2 SUNDRAY　NAC6200 前面板图

图 2：SUNDRAY　NAC6200 前面板（以 NAC-6200 为例）

1.CONSOLE(控制)口　2.USB 口　3.MANAGE(ETH0)　4.ETH1

5.ETH2　6.ETH3　7.ETH4　8.ETH5

告警灯在设备启动期间是红灯长亮的。一般一两分钟后红灯熄灭，说明正常启动。如

红灯长时间不熄灭，请关闭设备等待 5 分钟后重新开机。如果还是长亮，请联系客服部门确认是否设备损坏。正常启动后，有时红灯会闪烁，这是正常现象，红灯闪烁表示设备正在写系统日志。

控制口仅供开发和测试调试使用。最终用户需通过控制台网口接入设备。

1.4. 配置与管理

在配置设备之前，您需要配备一台电脑，配置之前请确定该电脑的网页浏览器能正常使用（如 Internet Explorer），然后把电脑与 NAC 设备连接在同一个局域网内，通过网络对设备进行配置。

NAC 设备的管理口为 MANAGE(ETH0)口，管理口默认出厂 IP 为 10.252.252.252/24。初次登陆设备，请用网线连接 MANAGE(ETH0)口到局域网或直接连接电脑。

1.5. 设备接线方式

在背板上连接电源线，打开电源开关，此时前面板的 Power 灯（绿色，电源指示灯）和 Alarm 灯（红色，告警灯）会点亮。大约 1-2 分钟后 Alarm 灯熄灭，说明网关正常工作。

请用标准的 RJ-45 以太网线将 MANAGE(ETH0)口与内部局域网连接，对 NAC 设备进行配置。

登录控制台后根据网络环境和部署要求配置『网络配置』和接线。（详情参见章节 3.2）

设备正常工作时 POWER 灯常亮，接线的数据接口 LINK 灯长亮，ACT 灯在有数据流量时会不停闪烁。ALARM 红色指示灯只在设备启动时因系统加载会长亮（约一分钟），正常工作时熄灭。如果在安装时此红灯长亮，请将设备断电重启，重启之后若红灯一直长亮不熄

灭，请与我们联系。

网口直接连接 MODEM 和交换机应使用直连线、连接路由器和电脑网口应使用交叉线。当指示灯显示正常，但不能正常连接的时候，请检查连接线是否使用错误。直连网线与交叉网线的区别在于网线两端的线序不同，如下图：

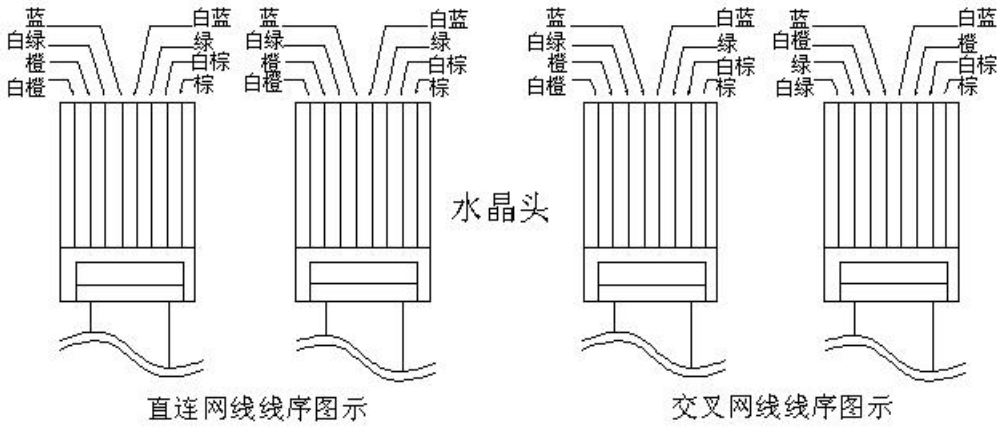


图 1　直连线、交叉线 线序

第 2 章 NAC 控制台的使用

2.1. 登录 WebUI 配置界面

NAC 支持安全的 HTTPS 登录，使用的是 HTTPS 协议的标准端口登录。如果初始登录从管理口(MANAGE)登录，那么登录的 URL 为：https://10.252.252.252

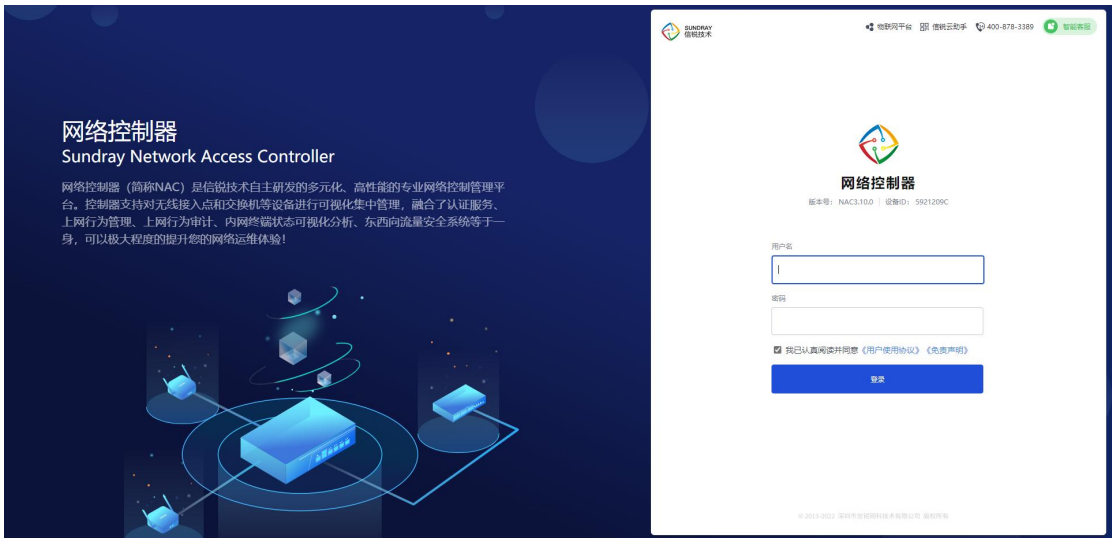
HTTPS 登录 WEBUI 管理 NAC 可以防止配置过程在传输过程中被截获而产生的安全隐患。

如何登录 NAC 设备控制台页面?

按照前面所示方法接好线后，通过 WEB 界面来配置 SUNDRAY NAC 设备。方法如下：

首先为登陆控制台的电脑配置一个 10.252.252.X 网段的 IP（如配置 10.252.252.100），然后在 IE 浏览器中输入管理口的默认登陆 IP 及端口 https://10.252.252.252，出现一个如下图的安全提示：

点击继续浏览此网站（不推荐）后出现以下的登录界面：

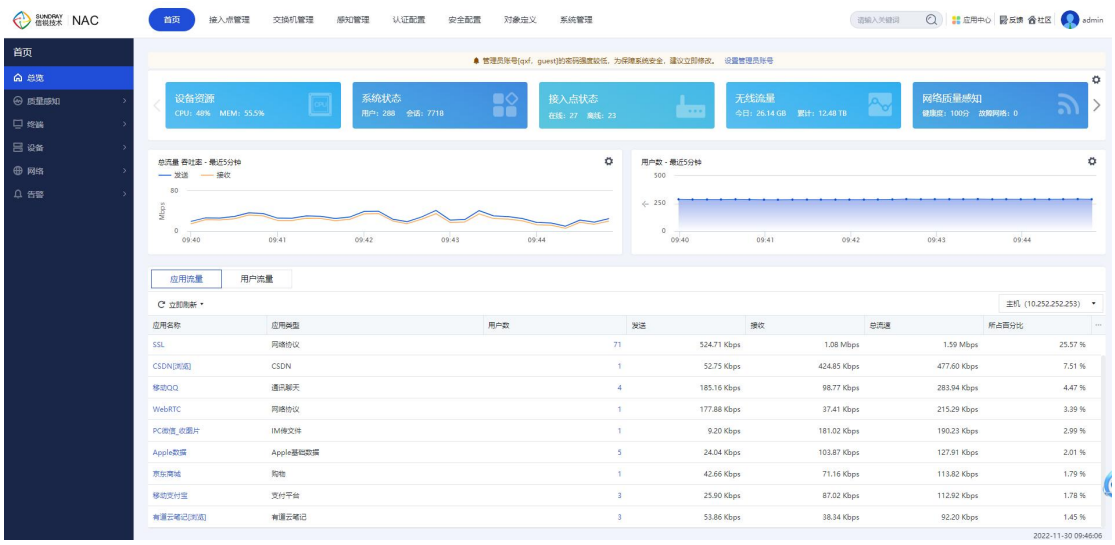


在登陆框输入『账号』和『密码』，点击登录按钮即可登录 NAC 设备进行配置，出厂情况下的用户名和密码为 admin/admin。

如果需要查看当 NAC 设备的版本号，点击版本信息，即显示当前设备的版本信息。

2.2. 配置和使用

登录 WebUI 配置界面后，可以看到以下配置模块：包括『首页』、『接入点管理』、『交换机管理』、『感知管理』、『认证配置』、『安全配置』、『对象定义』、『系统管理』。



所有配置界面中的图标，当鼠标放到此图标上时，可以显示当前配置项的简要帮助说明。后面的文档不再赘述。

第 3 章 NAC 功能说明

3.1. 帮助文档

对于 NAC，每个菜单页面的配置页面右上角，设备页面都自带有帮助文档，该配置文档详细的介绍了 NAC 各种功能的使用方法以及原理介绍。

3.2. 首页

『首页』主要用于查看设备的基本状态信息，包括【总览】、【质量感知】、【终端】、【设备】、【网络】、【告警】。

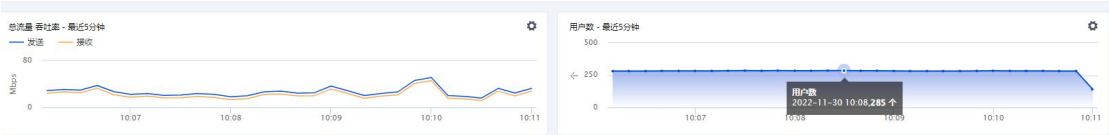
3.2.1. 总览

『总览』可以查看设备运行的基本信息，包括 CPU/内存利用率、在线用户、当前会话数、接口信息、接入点状态、无线流量、接口吞吐率、应用流量、用户流量等信息。

3.2.1.1. CPU 和内存使用率

在【运行状态】界面上面可以直接看到 CPU 和内存的使用率以及接口的状态等信息。

在【运行状态】界面下面可以直接看到无线吞吐率的趋势图，以及在线用户的趋势图，还有当前的应用流量与用户流量。

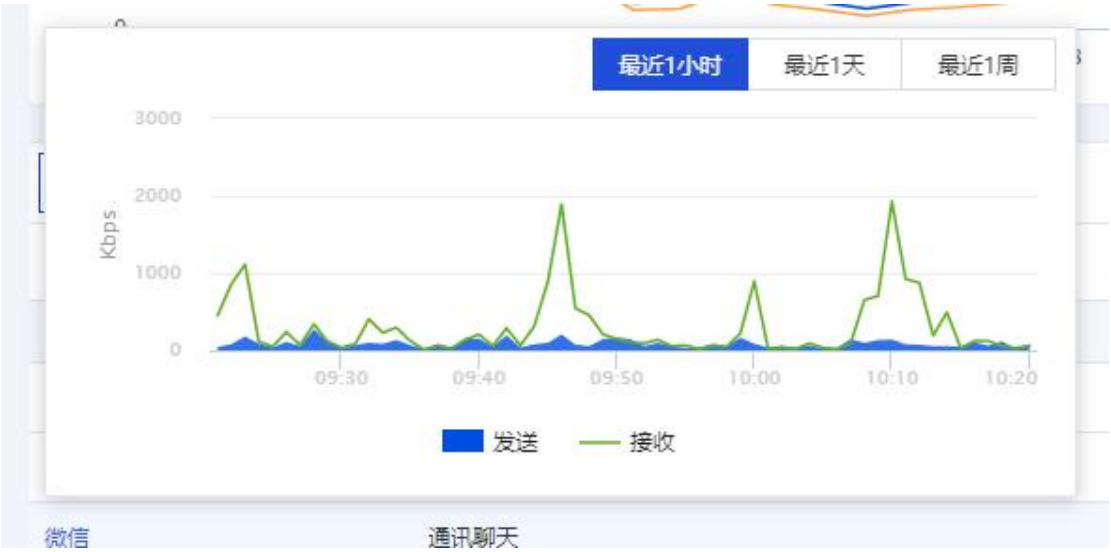


3.2.1.2. 应用流量

在【运行状态】界面下方，详细的查看无线用户的详细应用流量和用户流量

应用名称	应用类型	用户数	发送	接收	总流量	所占百分比
SSL	网络协议	73	419.70 Kbps	6.50 Mbps	6.90 Mbps	64.47 %
App_Store	下载工具	1	54.88 Kbps	998.72 Kbps	1.03 Mbps	9.61 %
Microsoft更新	软件更新	1	30.37 Kbps	342.23 Kbps	372.60 Kbps	3.40 %
Apple数据	Apple基础数据	5	33.27 Kbps	327.61 Kbps	360.88 Kbps	3.29 %
Microsoft数据	Microsoft基础数据	10	71.70 Kbps	225.37 Kbps	297.06 Kbps	2.71 %
WebRTC	网络协议	1	214.49 Kbps	34.09 Kbps	248.59 Kbps	2.27 %
字节跳动基础服务	字节跳动基础数据	12	131.70 Kbps	98.73 Kbps	230.43 Kbps	2.10 %
微信_基础服务	微信	3	16.00 Kbps	211.68 Kbps	227.68 Kbps	2.08 %
微信	通讯聊天	14	133.98 Kbps	92.14 Kbps	226.12 Kbps	2.06 %

点击应用流量下面的应用名称，还可以查看该应用流量的趋势图，可以选择 5 分钟，1 小时，最近 1 天，最近一周的该流量趋势图，便于掌握流量趋势情况，规划流控策略使用。选择方法如下图所示：



点击用户数，还可以看到当前应用流量的用户组成情况，如下图：

用户名	所属组	IP地址	发送	接收	总速率↓
D8-12-65-6C-E5-...	/PSK认证组/	172.16.193.196	341.32 Kbps	16.02 Kbps	357.34 Kbps
junge	/MOA/	172.16.199.19	8.58 Kbps	27.85 Kbps	36.43 Kbps
32933	/MOA/MOA/信...	172.16.198.228	10.68 Kbps	14.35 Kbps	25.03 Kbps
13144	/MOA/MOA/信...	172.16.196.79	5.14 Kbps	11.88 Kbps	17.02 Kbps
24934	/MOA/	172.16.198.69	12.63 Kbps	1.53 Kbps	14.16 Kbps
16675156617	/MOA/	172.16.196.203	2.59 Kbps	1.30 Kbps	3.89 Kbps
11627	/MOA/	172.16.198.133	640 bps	1.41 Kbps	2.04 Kbps
71944	/MOA/MOA/信...	172.16.196.133	504 bps	816 bps	1.29 Kbps
50-2B-73-D5-57-...	/PSK认证组/	172.16.195.140	368 bps	464 bps	832 bps
18483	/MOA/	172.16.199.47	272 bps	464 bps	736 bps

3.2.1.3. 用户流量

在【运行状态】页面底下还可以看到用户流量状况，当前哪些用户占用流量较多，默认依次按流量百分比从上到下进行排列，界面如下图：

用户名	所属组	转发模式	应用	IP地址	发送	接收	总流量	所占百分比
90260	/MOA/	集中转发	App_Store	172.16.196.169	468.79 Kbps	7.21 Mbps	7.67 Mbps	41.07 %
16671	/MOA/	集中转发	PC微信_收文件,微信PC版,SSL,飞书,360doc[浏览]	172.16.197.100	158.52 Kbps	3.87 Mbps	4.02 Mbps	21.53 %
62015	/MOA/MOA/信锐公司/信锐软件研发...	集中转发	飞书,字节跳动基础服务,今日头条,SSL,飞书_传文件,D...	172.16.199.136	1.27 Mbps	838.84 Kbps	2.09 Mbps	11.19 %
42663	/MOA/	集中转发	新浪微博[浏览],SSL,DNS协议,新浪基础服务	172.16.197.226	85.37 Kbps	1.26 Mbps	1.34 Mbps	7.18 %
42842	/MOA/	集中转发	网易云音乐,网易灵犀办公,HTTP_POST,SSL	172.16.198.142	55.84 Kbps	978.23 Kbps	1.01 Mbps	5.41 %
97410	/MOA/	集中转发	移动微信_收图片,QUIC,微信	172.16.197.78	56.23 Kbps	583.96 Kbps	640.19 Kbps	3.35 %
50580	/MOA/	集中转发	移动支付宝,SSL,DNS协议	172.16.196.115	54.38 Kbps	136.88 Kbps	191.26 Kbps	1.00 %
EE-6C-A1-53-64-24	/PSK认证组/	集中转发	华为运动健康,iCloud_Drive[浏览]	172.16.192.99	61.34 Kbps	67.70 Kbps	129.03 Kbps	0.67 %
cwj	/MOA/	集中转发	SSL,口袋助理	172.16.197.21	10.16 Kbps	117.69 Kbps	127.84 Kbps	0.67 %

2022-11-30 10:23:06

3.2.2. 质量感知

质量感知包含了【质量感知向导】、【认证质量感知】、【无线环境质量】、【网络质量感知】、【业务质量感知】。

3.2.2.1. 质量感知向导

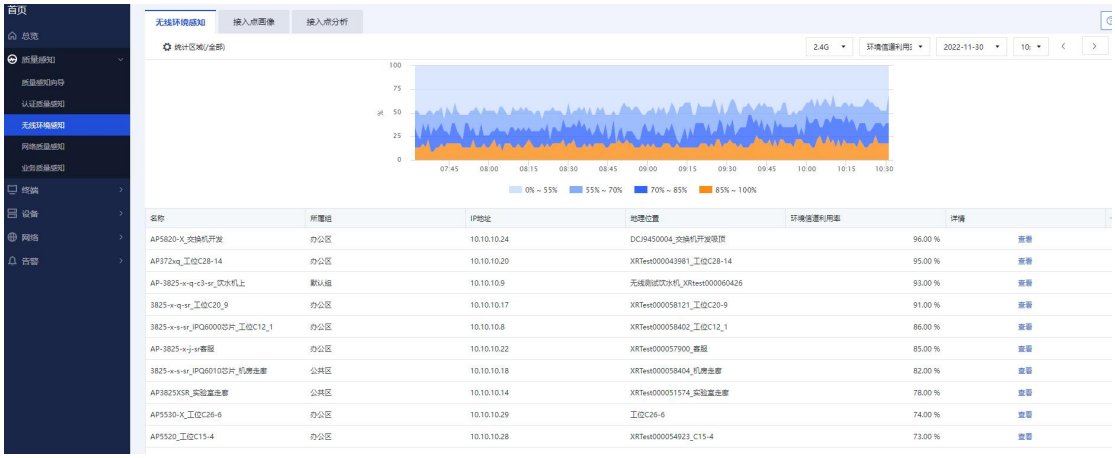
如下图显示，质量感知功能的向导页面，点击页面上的对应按钮可以跳转到无线环境感知、认证质量感知、网络质量感知、业务质量感知的配置和展示页面。

3.2.2.2. 认证质量感知

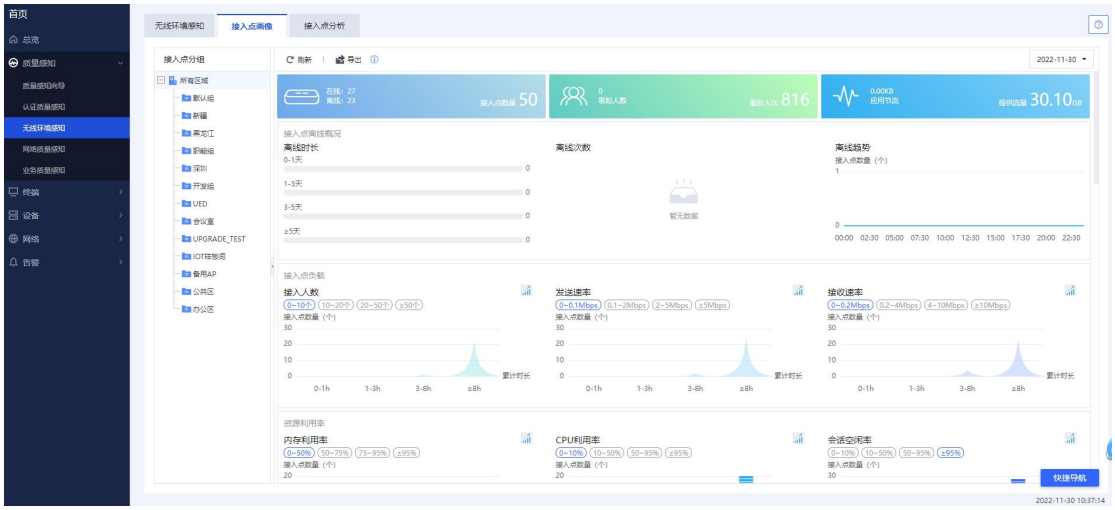
认证质量感知通过卡片形式呈现各个认证策略的整体认证情况，方便用户一目了然地查看当前所有认证策略的运行质量。支持导出认证质量汇总页面。

3.2.2.3. 无线环境质量

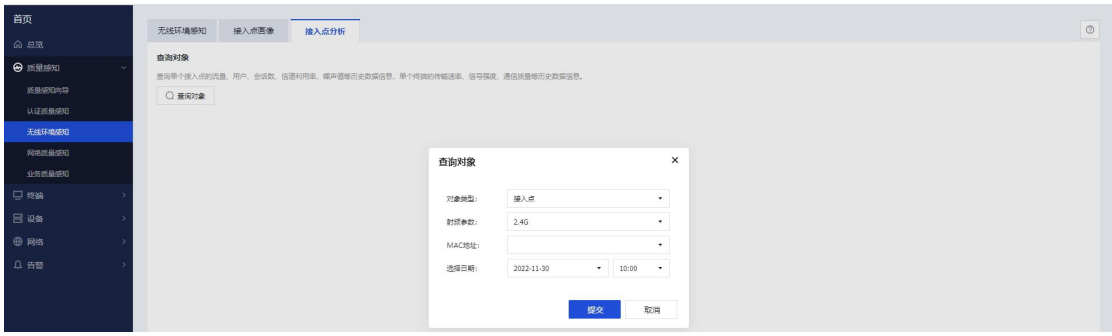
无线环境感知中，根据环境信道利用率、自身信道利用率、重传率、误码率、噪声值、同频干扰等参数划定的区间，将无线接入点划入指定的区间。管理员通过分析接入点在各个区间的分布情况，排查接入点的问题，并通过增加接入点、调整接入点位置等方式，提高无线网络的整体服务质量。



接入点画像中，汇总展示无线环境的质量信息，包括接入点离线概况、接入点负载、资源利用率、流量状态、射频接入人数、信道利用率、噪声值等信息。进一步的详细数据可以到接入点状态页面查看。

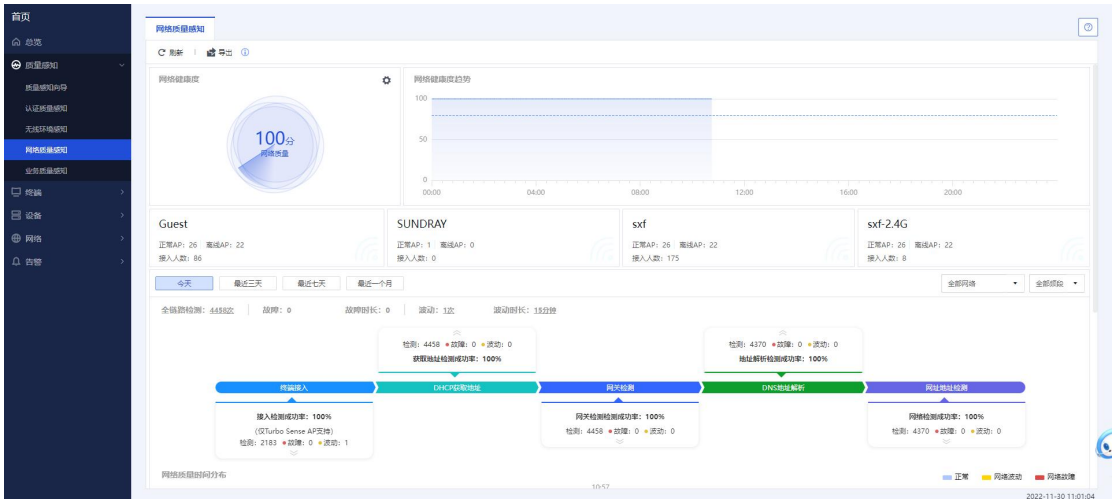


接入点分析中，可以查询单个接入点的流量、用户、会话数、信道利用率、噪声值等历史数据信息，单个终端的传输速率、信号强度、通信质量等历史数据信息。



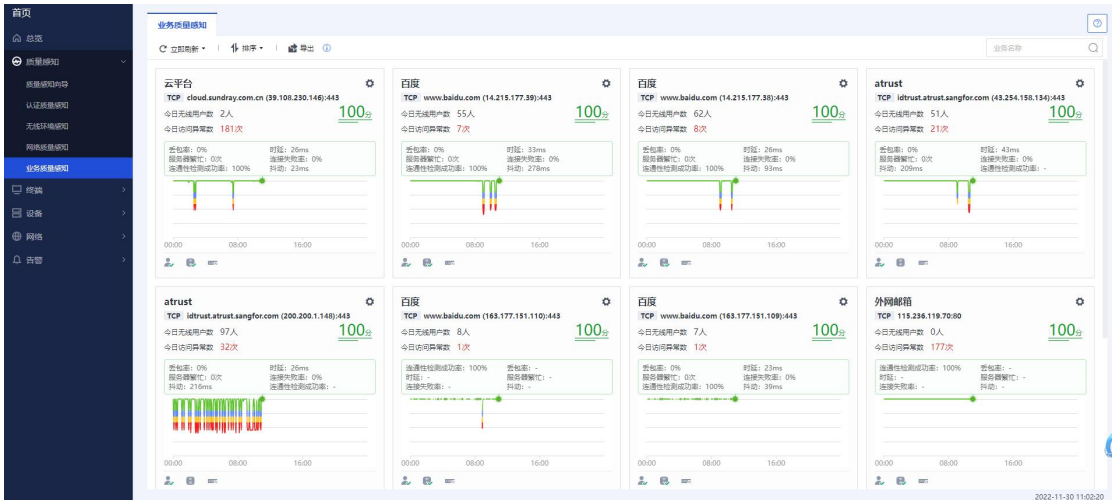
3.2.2.4. 网络质量感知

网络质量感知是 Turbo Sense AP 独有的功能，无线网络开启网络质量感知之后会启用自身的 AI 射频接入自己的无线网络，进行终端接入、DHCP 获取地址、网关检测、DNS 地址解析、网络地址检测五个阶段的检测，并通过设置的阈值得出该射频当次的检测结果。



3.2.2.5. 业务质量感知

业务质量感知通过用户体验监测、AI 模拟探测来监控用户业务，将对应业务的网络质量的情况通过图形和打分的形式直观展示。可通过业务卡片快速修改、勾选对应 SLA 指标对分值进行重新运算，快速按照新阈值生成标准的新图表。



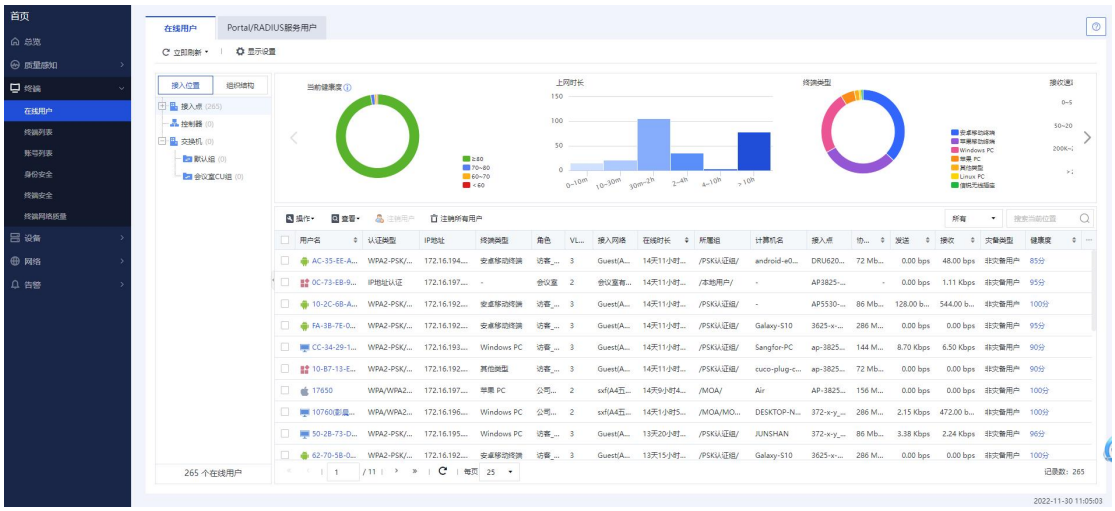
3.2.3. 终端

3.2.3.1. 在线用户

在线用户，可以看到当前接入网络的无线用户信息，显示无线网络的用户，以及用户的终端，

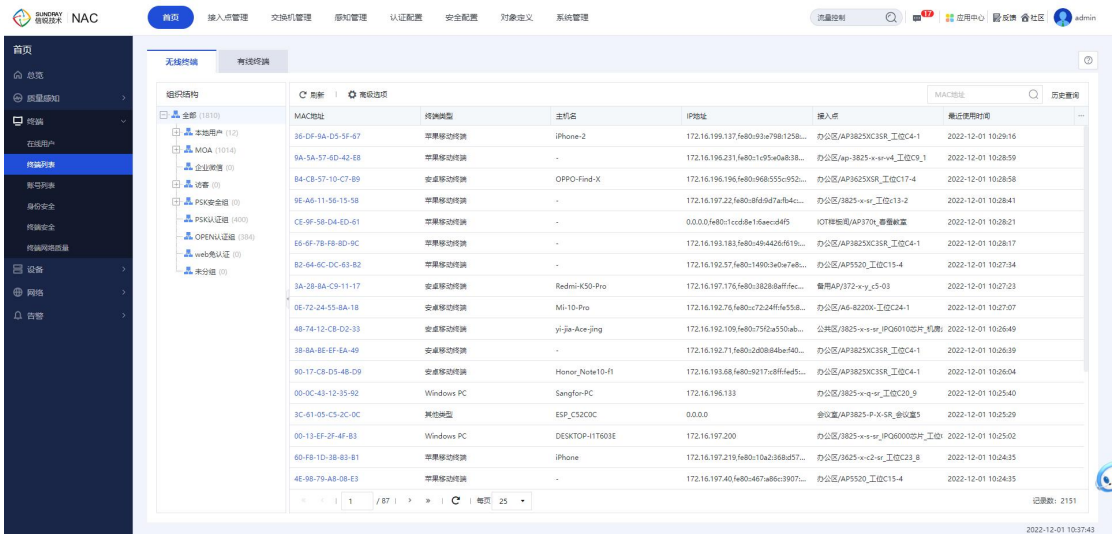
权限，流速等信息。

无线用户除了以组织结构查看外，还支持以接入点分组的方式查看无线用户信息，如下图：



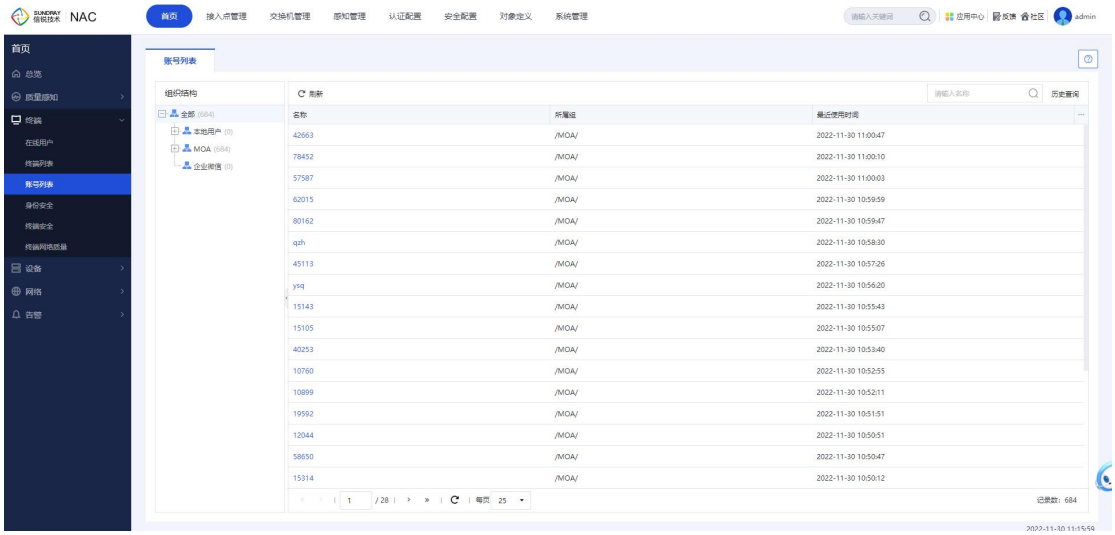
3.2.3.2. 终端列表

终端列表展示单个终端的详细运维信息。包括终端活跃状态等。



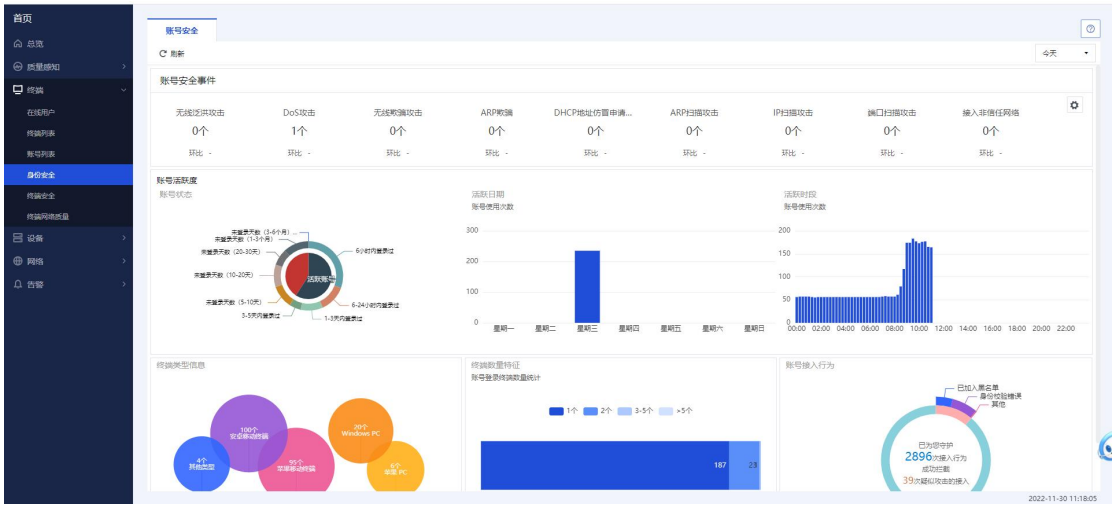
3.2.3.3. 账号列表

展示单个账号的详细运维信息。包括账号活跃状态、接入非信任网络、安全事件、流量协商速率、DHCP 质量、流量趋势、DNS 质量、网关质量、信号强度、通信质量、空口状态等。



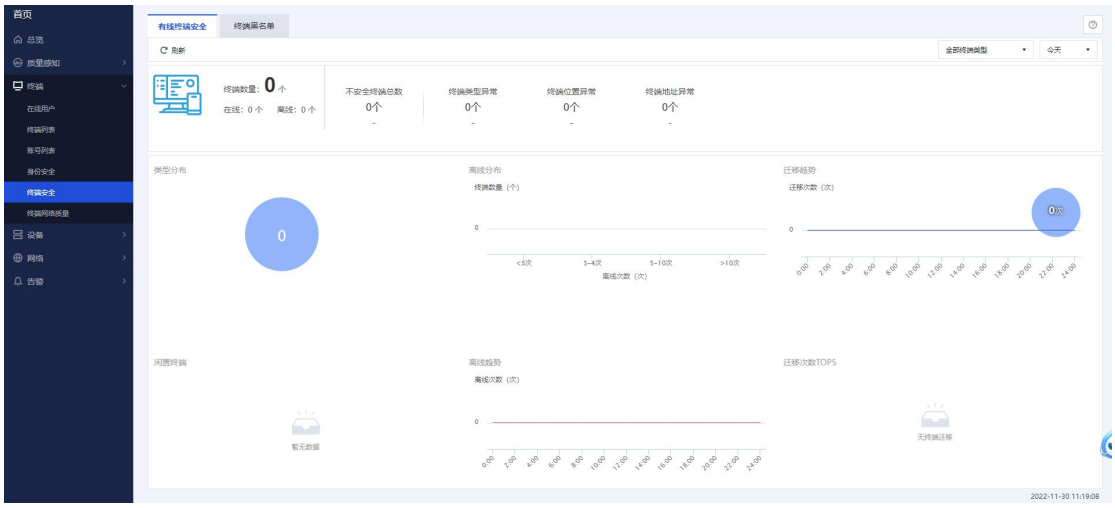
3.2.3.4. 身份安全

展示账号安全时间、账号状态、活跃日志、活跃时段、终端类型信息、终端数量特征、账号接入行为等信息。



3.2.3.5. 终端安全

有线终端安全中，显示终端状态，可查看终端数量（在线和离线终端）、终端类型分布、闲置终端、终端离线分布、终端离线趋势及终端迁移和安全事件的行为、次数。可以通过类型分布的饼状图，查看不同类型具体的占比，同时可以通过趋势图，查看一段时间内终端的变化情况，包括离线趋势、迁移情况等。另外，还可点击相应的表项查看相对应的模块具体的数据信息，如：点击“闲置终端”中离线时间大于 10 天的设备，可看到该设备的 mac 地址、主机名和最近登陆时间。

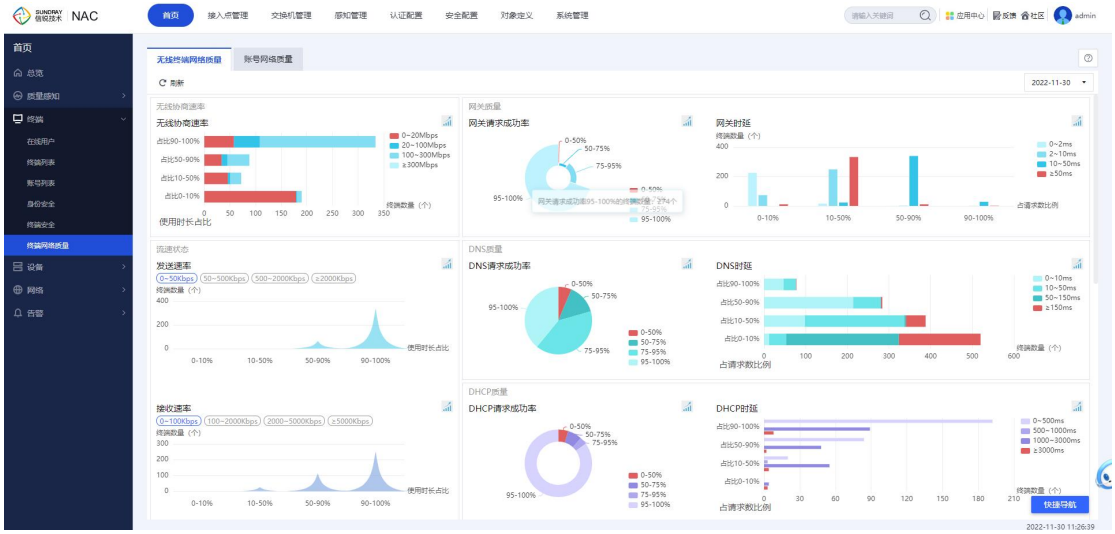


终端黑名单，管理员可以手动添加黑名单，以阻止指定的 MAC 地址终端连接有线和无线

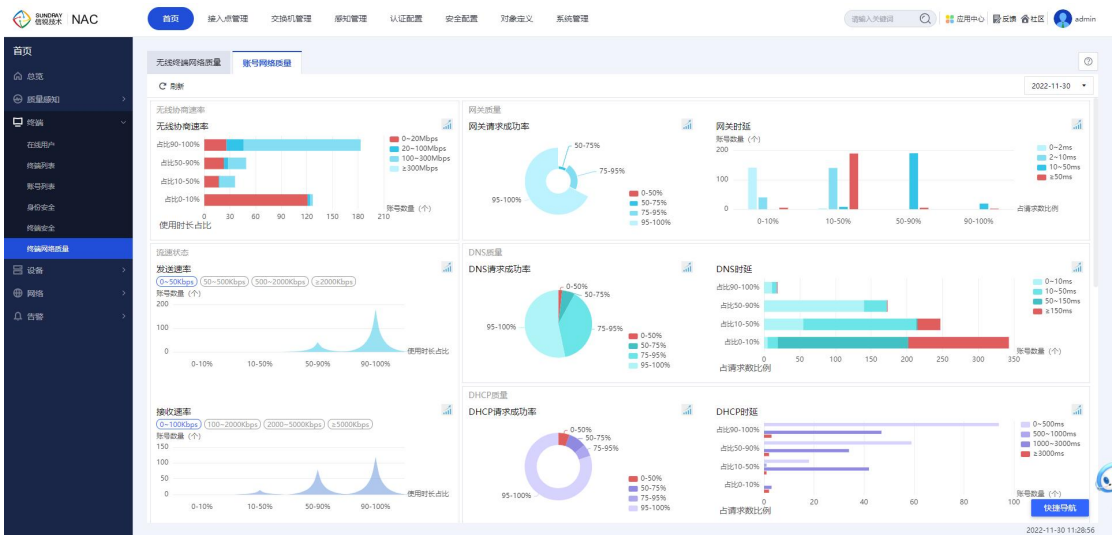
网络。

3.2.3.6. 终端网络质量

无线终端网络质量汇总展示终端画像信息，包括流量协商速率、网关质量、流速状态、DNS 质量、DHCP 质量、信号强度、通信质量、空口状态等。



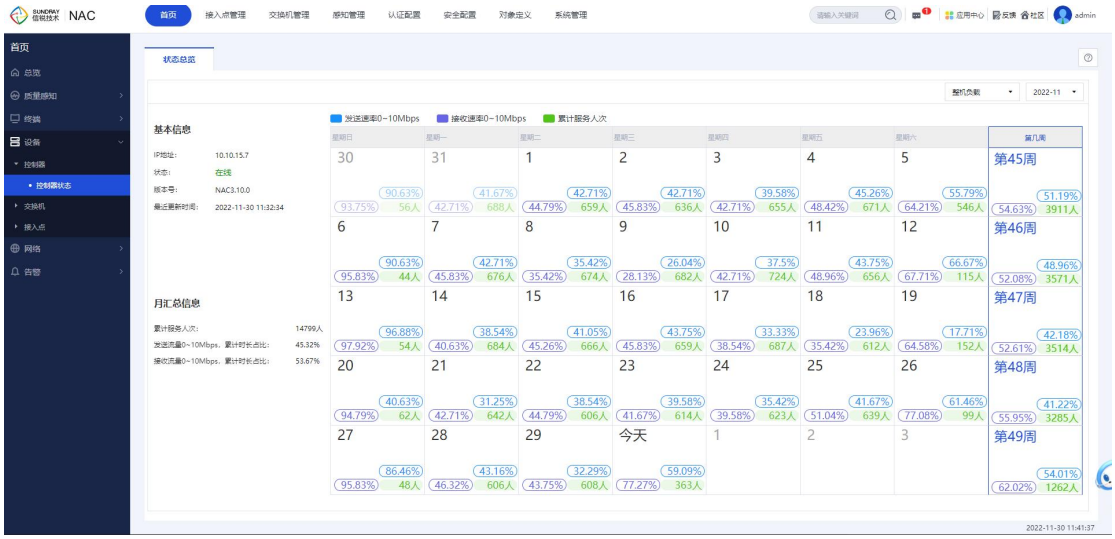
账号网络质量汇总展示账号画像信息，包括流量协商速率、网关质量、流速状态、DNS 质量、DHCP 质量、信号强度、通信质量、空口状态等。



3.2.4. 设备

3.2.4.1. 控制器

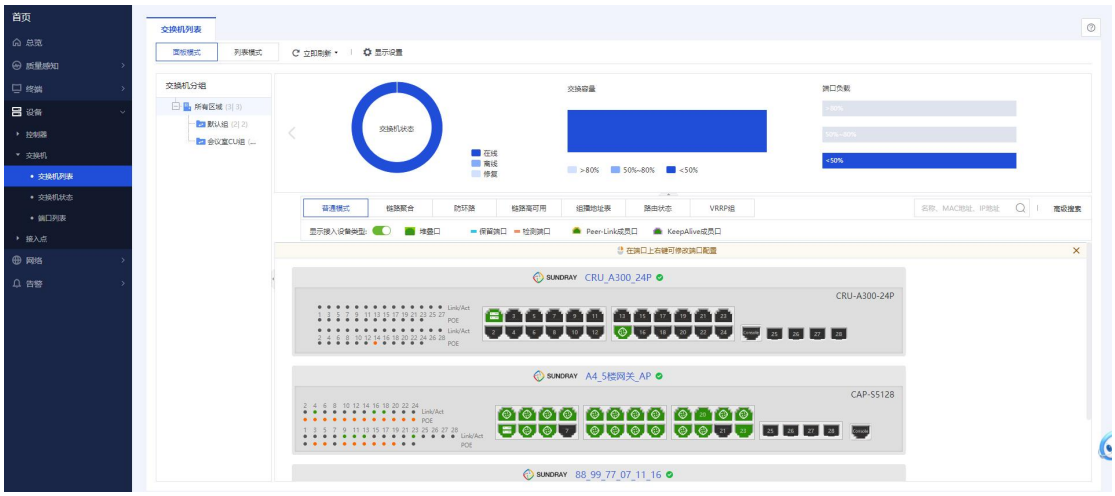
状态总览中，监控分支设备的状态信息，提供各分支状态图形信息。



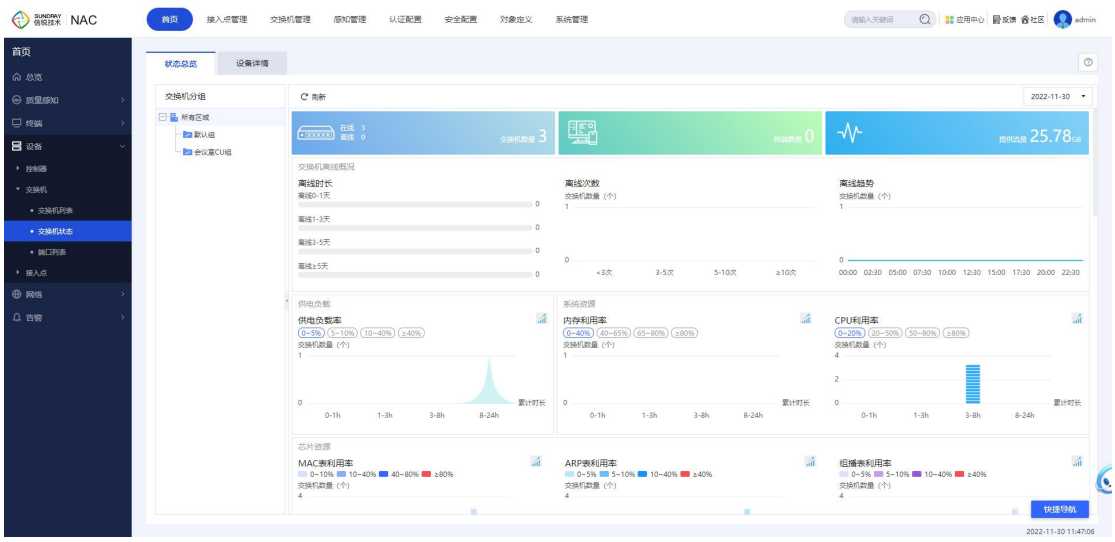
3.2.4.2. 交换机

显示交换机的运行状态，可查看交换机的在线状态、负载以及端口状态。可以通过交换机面板图看出来，交换机每个口的 Link/Act。点击具体的某个口，可以看到端口的详情，包括 VLAN

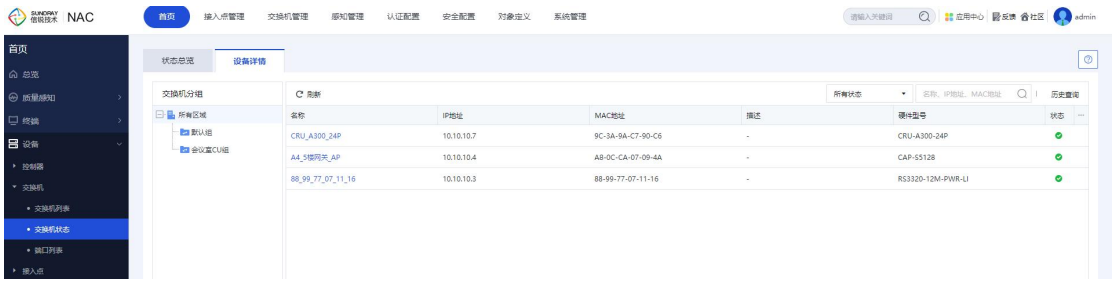
和 POE 配置信息、供电状态，以及流量趋势，端口收发包情况；点击具体的某个光口，可以看到光口的光功率上报详情，包括光发送/接收功率及其阈值。



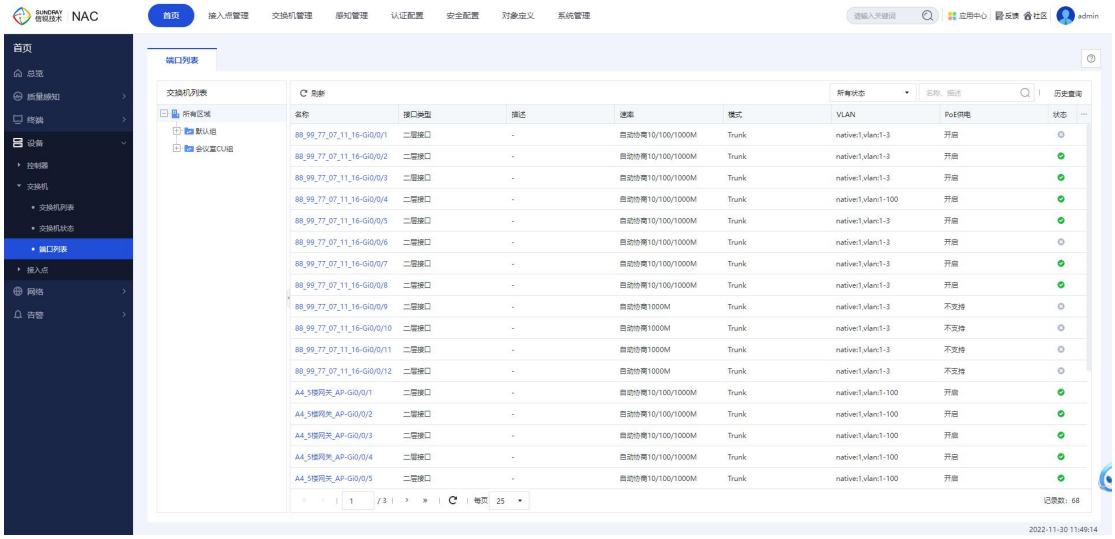
交换机状态总览，显示有线网络的整体运行，能够直接通过该页面查看有线网络下所有交换机和端口的总体运行情况。交换机画像页面由主要包括交换机离线概况、供电负载、系统资源、芯片资源、网络质量、流量负载、帧类型分析、报文分析和网络协议报文接收速率等。



设备详情显示单个交换机的运行情况，主要包括活跃状态、系统资源、供电负载率、芯片资源等。

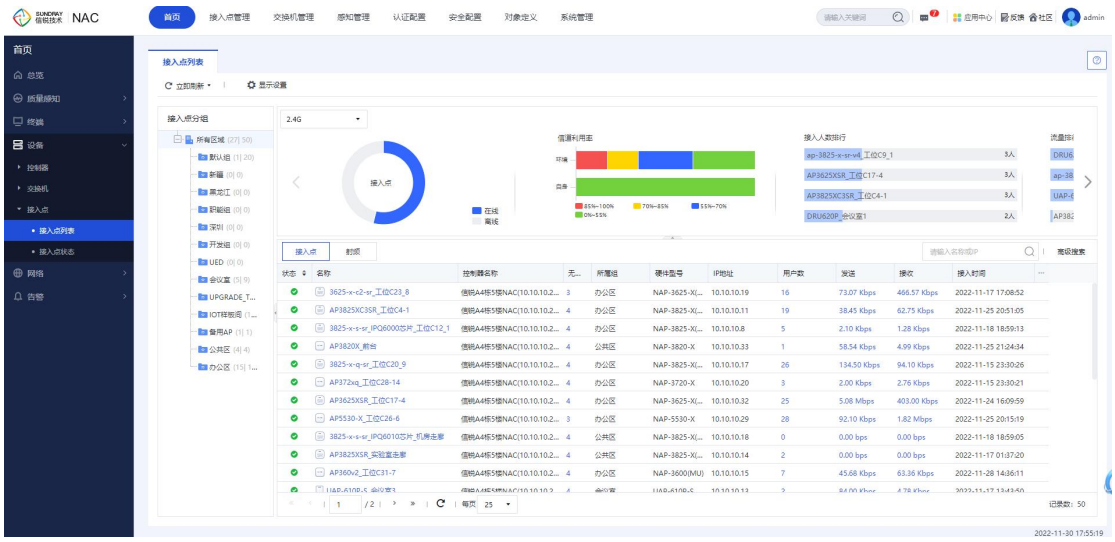


端口列表显示单个端口的运行情况，主要包括活跃状态、网络质量、流量空闲率、帧类型分析、泛洪报文分析、报文数量分析等。

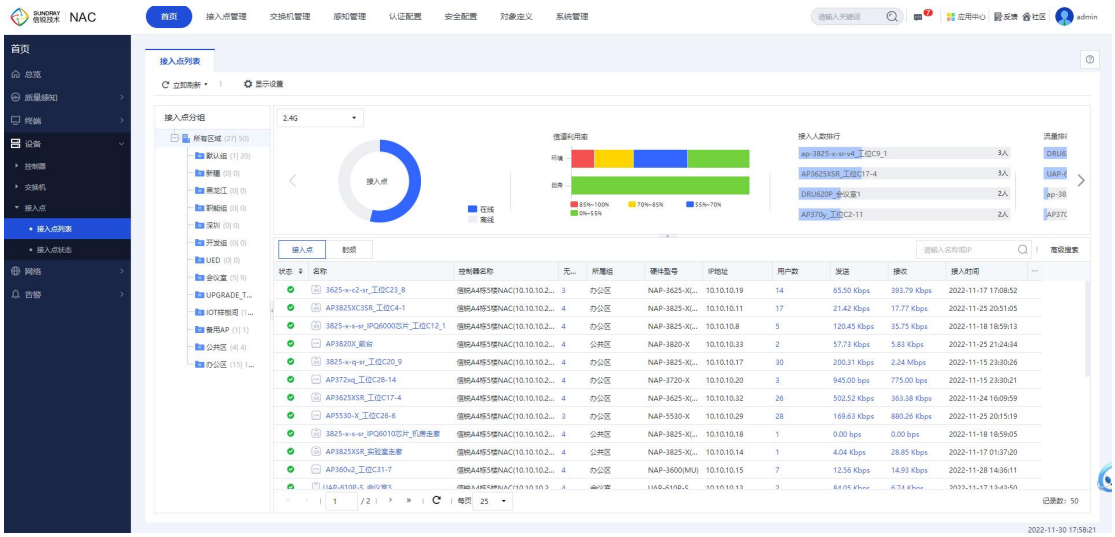


3.2.4.3. 接入点

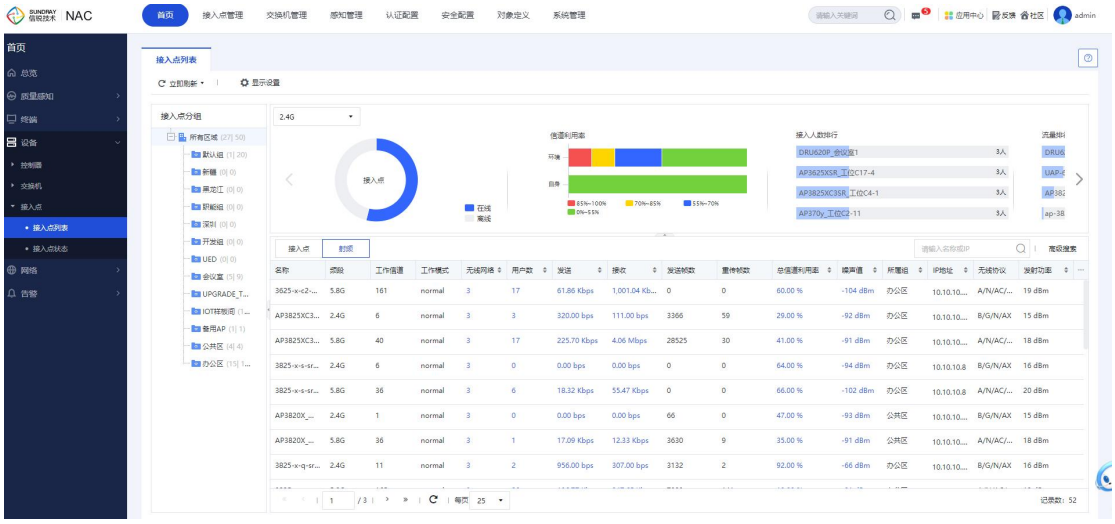
在【接入点列表】显示无线接入点运行状态，可查看接入点的在线状态、负载及射频质量。



【接入点状态】的接入点列表中，汇总展示接入点业务感知信息，包括接入点离线概况、接入点负载、资源利用率、网关质量、DNS 质量、DHCP 质量、TCP 质量、隧道状态、流量状态、射频接入人数、信道利用率、噪声值等信息。



点击【射频】还可以看到每个 AP 的工作频段、工作信道、AP 承载的无线网络数量、信道利用率、噪声值、无线协议、重传率、误码率等信息。



点击【发送】或【接收】下面的数据，可以看到当前 AP 详细的上下行流量，还可以选择【最近 5 分钟】、【最近 1 小时】、【最近一天】、【最近一周】的流量图。

信道利用率：信道利用率数值代表信道的繁忙程度，信道利用率越低体验越稳定。

噪声值：指无线网络频率范围内的辐射电磁干扰。噪声问题容易引发无线数据帧的丢包及误码，如果一个接入点所处的位置噪声值比较高，严重影响数据传输，应考虑更换部署地点或清除干扰源。

无线协议：无线接入点的无线网络协议，例如无线网络协议，2.4G 支持 802.11b/g/n，5.8G 支持 802.11a/n/ac。

重传率：重传率越高，代表无线网络数据的丢包越严重。

误码率：误码率（BER：bit error ratio）是衡量数据在规定时间内数据传输精确性的指标。在无线数据通信中，如果发送的信号是"1"，而接收到的信号却是"0"，这就是"误码"，也就是发生了一个差错。在一定时间内收到的数字信号中发生差错的比特数与同一时间所收到的数字信号的总比特数之比,就叫做"误码率"。噪声、交流电或闪电造成的脉冲、传输设备故障及其他因素都会导致误码。

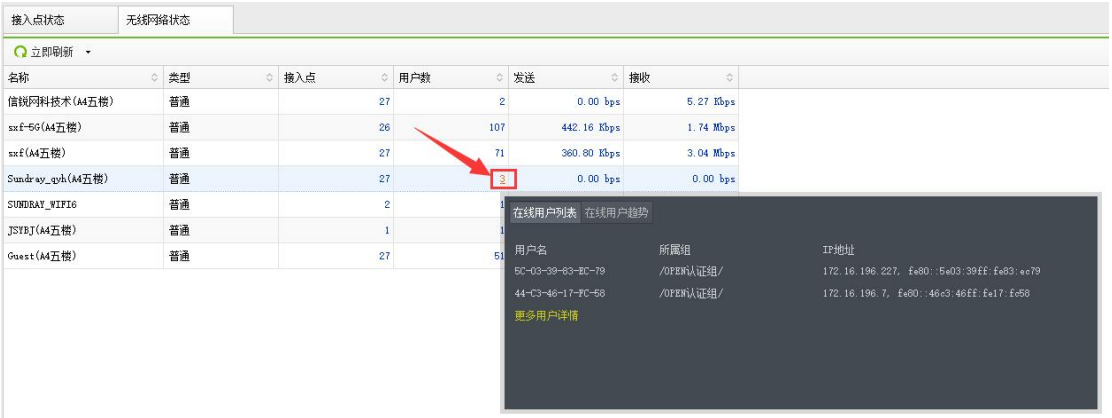
3.2.4.4. 无线网络状态

在【无线网络状态】中可以看到所有的无线网络情况，包括每个网络包含的接入点 AP 数量，当前网络的接入用户数，当前网络的发送和接收流量统计。

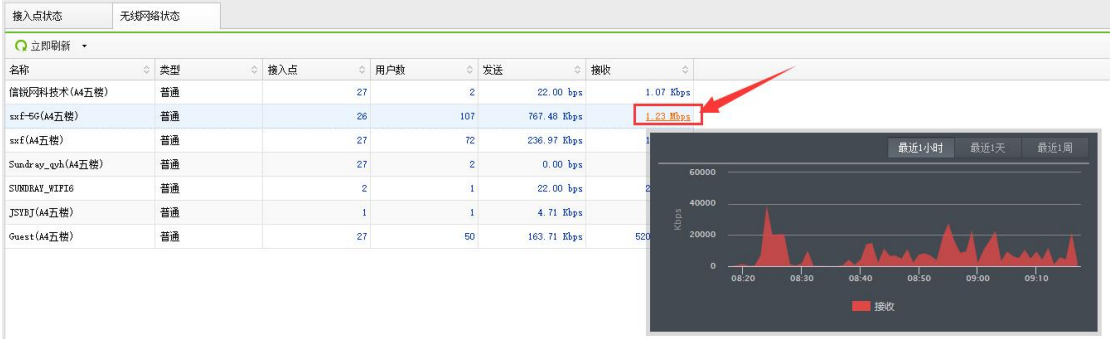
名称	类型	接入点	用户数	发送	接收
信锐网科技术(A4五楼)	普通	27	2	4.81 Kbps	8.46 Kbps
sxf-5G(A4五楼)	普通	26	106	674.90 Kbps	2.52 Mbps
sxf(A4五楼)	普通	27	71	517.83 Kbps	6.03 Mbps
Sundray_qyh(A4五楼)	普通	27	2	0.00 bps	0.00 bps
SUNDRAY_WIFI6	普通	2	1	345.00 bps	345.00 bps
JSYBJ(A4五楼)	普通	1	1	1.87 Kbps	0.00 bps
Guest(A4五楼)	普通	27	49	337.32 Kbps	1.01 Mbps

点击接入点，用户数，以及发送或接收可以看到相应的数据，比如点击接入点，就可以跳入到该网络所有接入点列表。

点击【用户数】时，就可以看到当前接入的用户的用户名，所属组，IP 地址信息。



点击【接收】或【发送】就可以看到当前网络【最近 5 分钟】、【最近 1 小时】、【最近 1 天】、【最近 1 周】的流量情况：



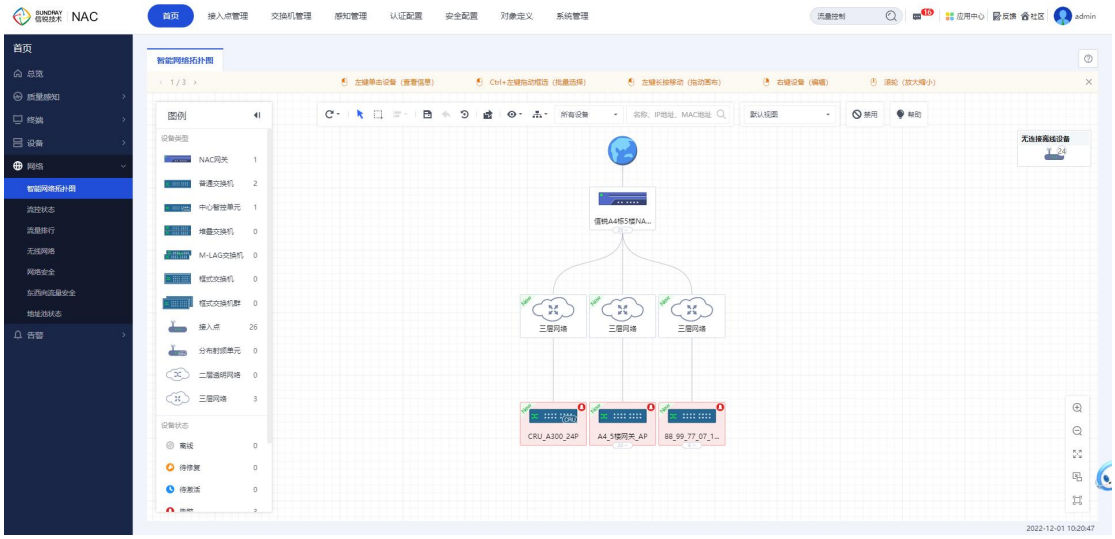
3.2.5. 网络

3.2.5.1. 智能网络拓扑图

【智能网络拓扑图】显示信锐设备(交换机和 ap)的运行状态，可查看信锐设备的在线状态、负载以及端口状态。可以通过交换机面板图看出来，交换机每个口的 Link/Act。点击具体的某个口，可以看到端口的详情，包括 VLAN 和 POE 配置信息、供电状态，以及流量趋势，端口收发包情况。通过 AP 面板图看出来 AP 和交换机以及 AP 和 AP 连接状态。点击 AP 之间或 AP 和交换机之间的连线，可以看到端口连接情况。

- 主拓扑：与控制器同二层的信锐设备通常显示在主拓扑中。
- 分支拓扑：与控制器跨三层的信锐设备通常显示在分支拓扑中。
- 无连接离线设备：信锐设备离线以后，且与智能网络拓扑图中的其他设备无连接数据，成为无组织离线设备。
- 无连接待激活设备：跨三层可发现、未激活的设备，与智能网络拓扑图中的其他设备无连接数据，称为无连接待激活设备。

- 二层透明网络：我司框式交换机/我司胖模式交换机/我司低版本交换机/我司低版本 AP/我司胖 AP/非我司设备等在拓扑中均显示为二层透明网络。可根据实际拓扑，将二层透明网络替换成我司设备，进行后续管理。
- 三层网络：分支拓扑与控制器之间经过三层网络相连。



3.2.5.2. 流控状态

【通道状态】显示流量控制通道的实时信息。

- 通道名称：通道名称。
- 线路：该通道属于哪条线路。

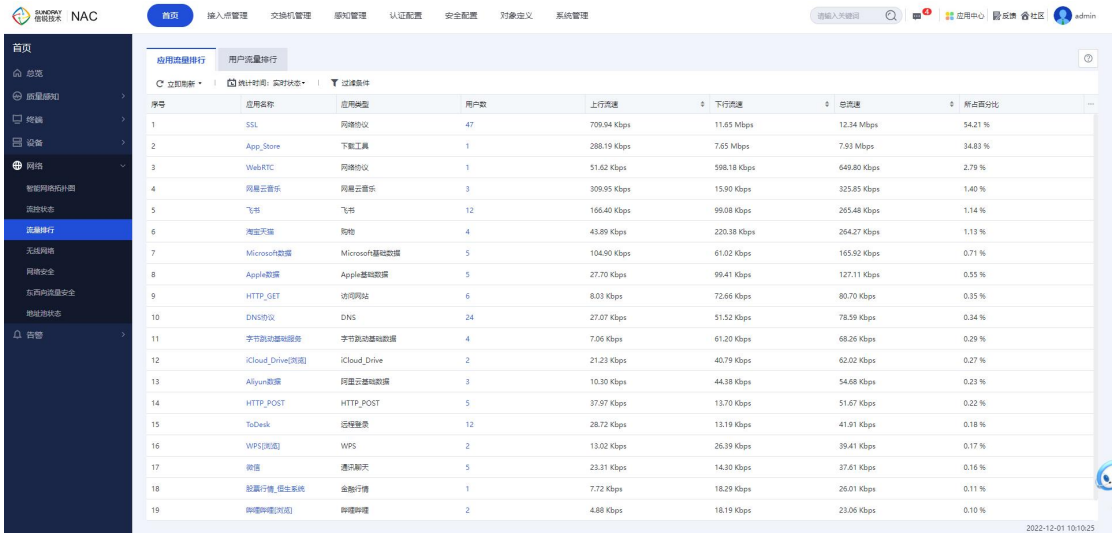
- 瞬时速度：通道的实时速率（上 1 秒的流量）。
- 占用比例：通道实时带宽占用率。
- 用户数：通道中的基于 IP 统计的用户数（上一秒的统计值）。
- 保证带宽：通道配置的保证带宽值，如果是限制通道，则保证带宽值为 0。
- 最大带宽：通道配置的最大带宽值。
- 优先级：通道中配置的优先级。
- 突破限制：限制通道中开启了空闲带宽突破功能后，该通道的突破状态：
- 绿色箭头：则表示该通道已经突破自身最大带宽，并且实际速率超过最大带宽。
- 灰色箭头：则表示该通道已经突破自身最大带宽，但是实际速率并没有超过最大带宽。
- -：表示该通道没有开启带宽突破功能。

【线路状态】显示当前线路的总的瞬时速率。

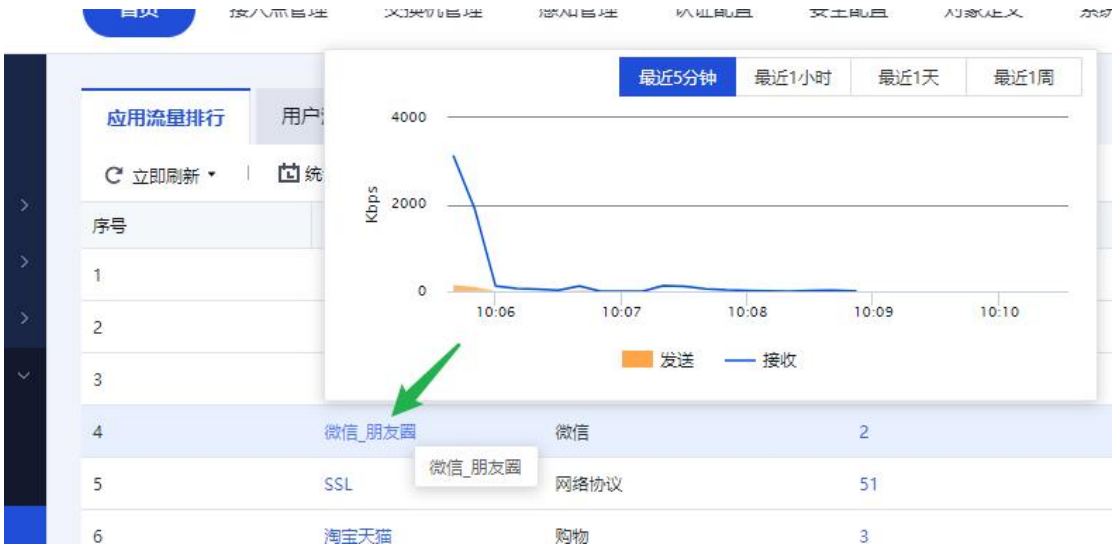
【排除策略】显示被排除策略排除的流量统计，会统计每条线路每条策略排除的流量。

3.2.5.3. 流量排行

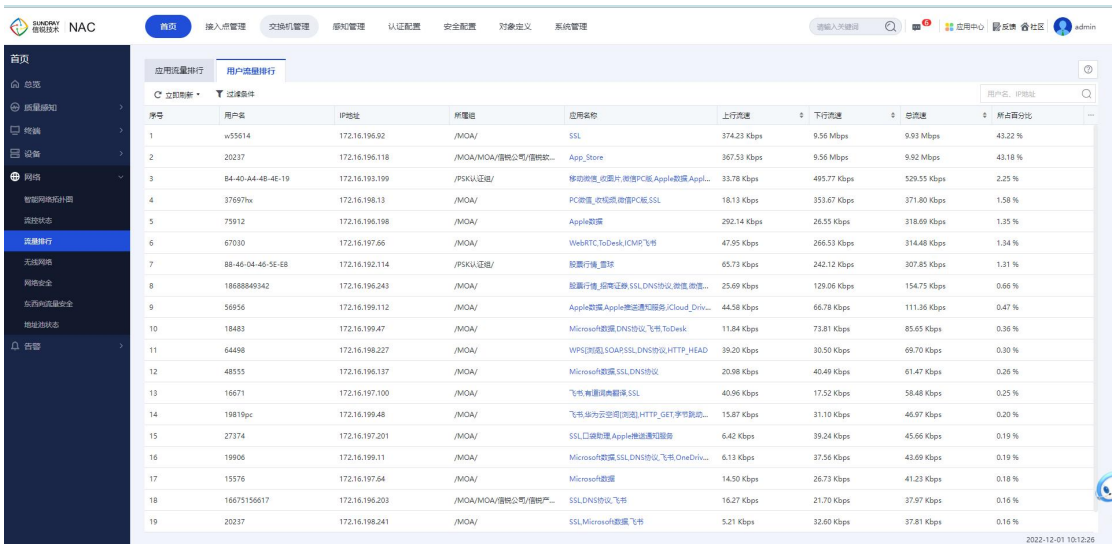
【应用流量排行】可以查看所有用户的应用流量情况，依次按百分比从大到下排行，并显示该应用的用户数，与上下行流速，情况如下图，此功能的分析可以用于优化【流量控制】中的流量控制策略。



点击应用流量下面的应用名称，还可以查看该应用流量的趋势图，可以选择 5 分钟，1 小时，最近 1 天，最近一周的该流量趋势图，便于掌握流量趋势情况，规划流控策略使用。选择方法如下图所示：



【用户流量排行】可以看到用户流量状况，当前哪些用户占用流量较多，默认依次按流量百分比从上到下进行排列，界面如下图。



3.2.5.4. 无线网络

【无线网络】显示无线网络的实时状态，包括生效的接入点，上线用户线，发送速率和接收速率。

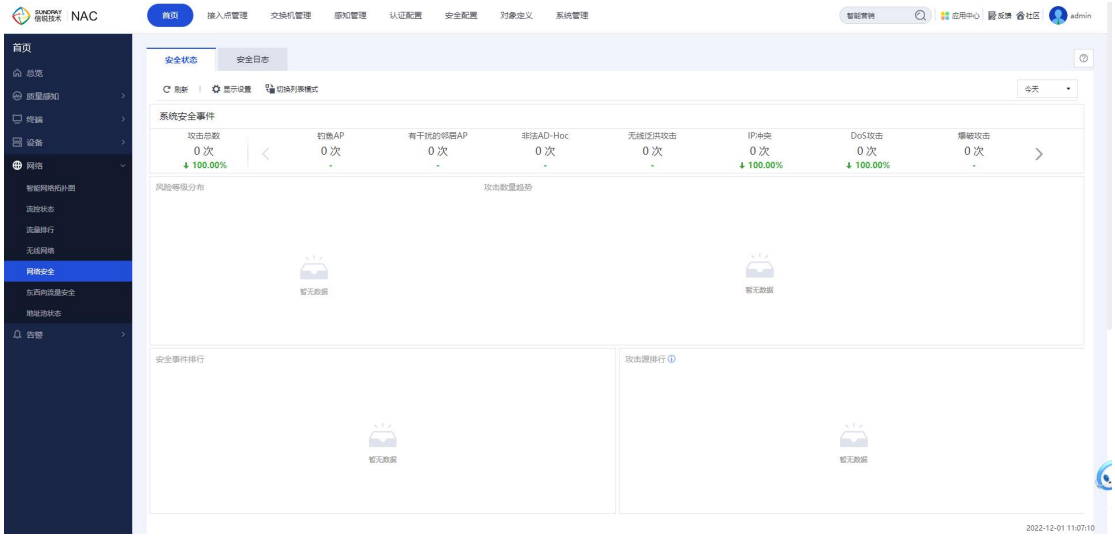
3.2.5.5. 网络安全

【安全状态】显示当前无线网络环境下，网络控制器、接入点的安全状态。安全状态检测的

事件类型包括：钓鱼 AP，有干扰的邻居 AP，非法 AD-Hoc，无线泛洪攻击，DoS 攻击，爆破攻击，BSSID 冲突检测，私设 ip，无线欺骗攻击，ip 冲突，ARP 欺骗，DHCP 泛洪攻击，ARP 扫描攻击，ip 扫描攻击，端口扫描攻击。

安全状态可以查看时间段分别为今天、某一天、最近 7 天和最近 30 天发生的各种安全事件的简要信息。

- 趋势图 ：攻击者个数的趋势信息。
- 饼图 ：各种安全事件的比例。
- 详情 ：此攻击者出现的时间段。



烟感告警显示当前烟感探测器探测到浓烟时，发生告警的事件。烟感告警查看时间段分别为今天，某一天，最近 7 天和最近 30 天

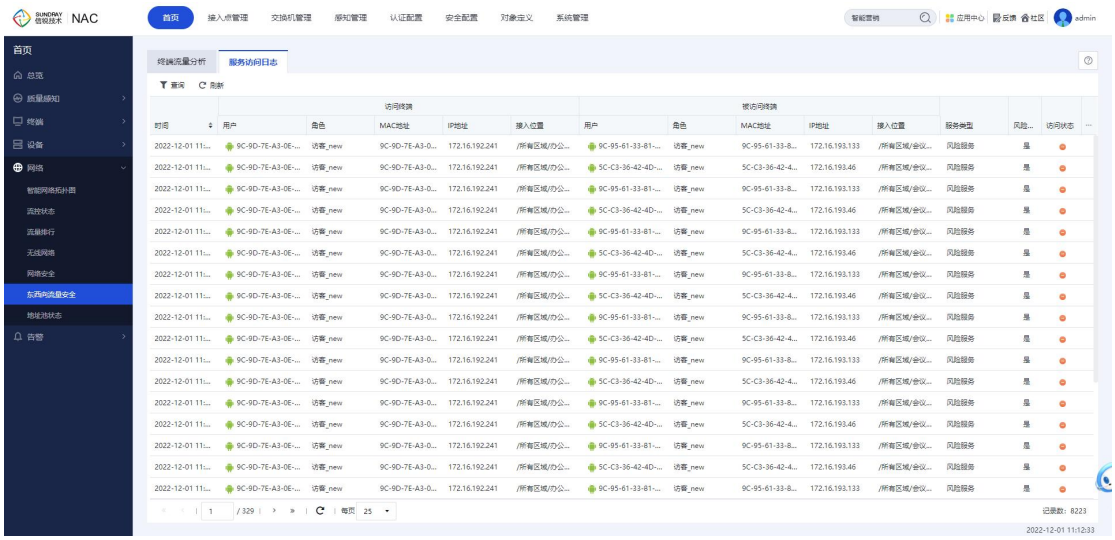
- 柱状图：显示烟感告警的次数
- 详情：烟感告警发生的时间段

【安全日志】记录所有的检测到的无线网络安全事件，并记录检测到的结果。

3.2.5.6. 东西向流量安全

【终端流量分析】展示终端流量统计分析状况，包括区域概况、实时守护终端、终端类型分布、区域守护状态、安全/风险服务访问状态、出站/入站服务访问趋势、出站/入站访问拦截、攻击服务分、攻击访问趋势情况等。

【服务访问日志】显示观察区域/保护区域/观察角色/保护角色内的终端的详细访问记录，包括时间、访问终端、被访问终端、服务类型、访问状态、访问次数等。还支持按服务类型或访问状态等多种条件进行过滤，按终端信息进行查询。



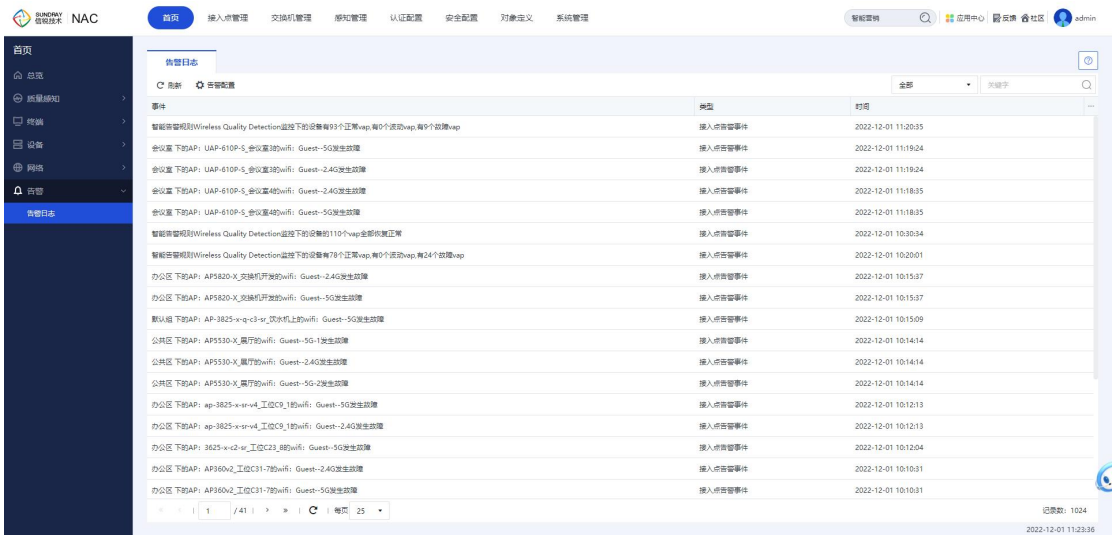
3.2.5.7. 地址池状态

【地址池状态】展示控制器和交换机 DHCP 地址池的 IP 分配情况，通过 发生冲突的 IP、获取 IP 失败的终端、地址池利用率等信息，管理员可以直观快速地发现解决网络问题。

3.2.6. 告警日志

【告警事件】系统运行过程中，如果检测到较严重的事件，并且需要管理员注意或确认时，将产生告警事件。例如：接口掉线，接口故障检测失败，VRRP 备份组发生主备状态切换。管

理员通常需要确认是否确实存在异常，并尝试排除异常。



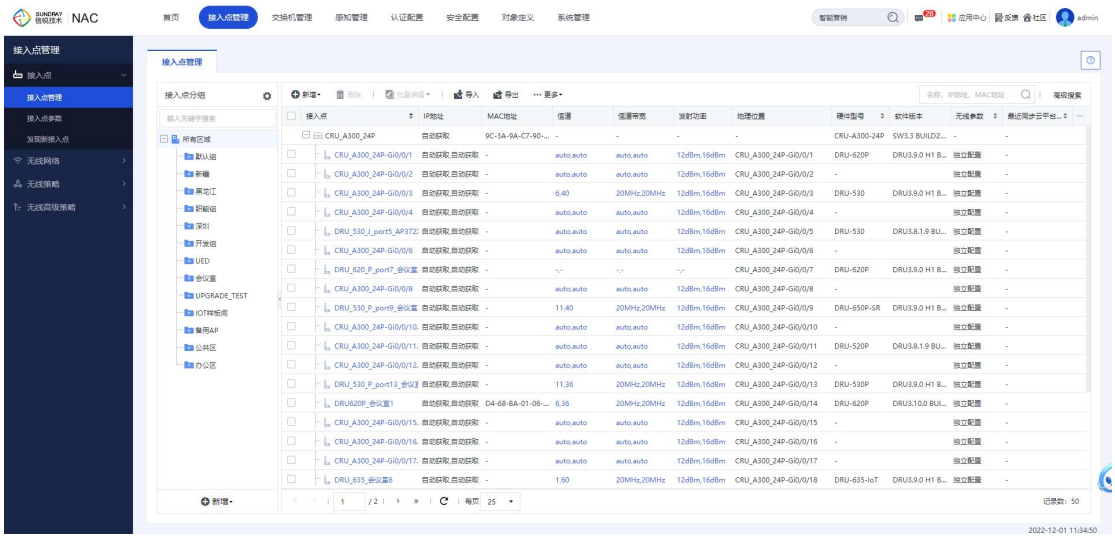
3.3. 接入点管理

『接入点管理』包括【接入点】、【无线网络】、【无线策略】、【无线高级策略】。

3.3.1. 接入点

3.3.1.1. 接入点管理

对所有无线接入点进行全部集中分组和管理，包括配置无线信号，工作模式，射频工作范围，隧道参数等。如果有大批量的 AP 需要集中配置，也可以下载采用下面接入点管理文件的示列文件进行批量的编辑和导入。接入点分组用于大规模部署中，可以把无线接入点，按地理位置，用途等方式划分到接入点分组中。以易于无线网络的部署及维护。



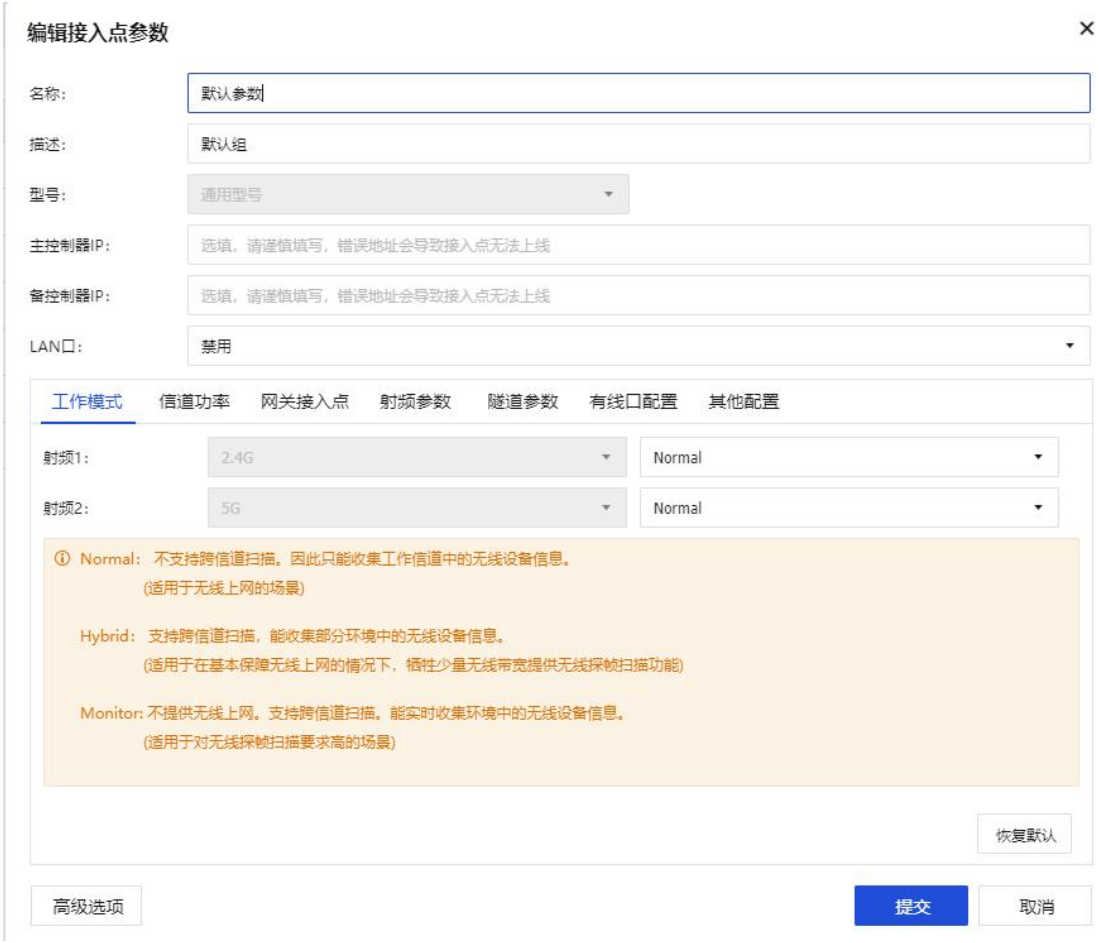
3.3.1.2. 接入点参数

无线网络的很多参数都可以在接入点参数中配置，接入点分组引用某一接入点参数后，则该分组的接入点默认情况下将使用该分组引用的接入点参数配置，如果某个接入点需要使用不同的配置，有以下方式选择：

- 把此接入点移动到一个新的接入点分组中，对新的接入点分组进行配置。
- 编辑接入点属性中的无线参数，选择使用独立的配置，然后修改接入点的无线参数。

工作模式

可以分为三种，分别是：Normal，Hybrid 和 Monitor 模式，如下图：



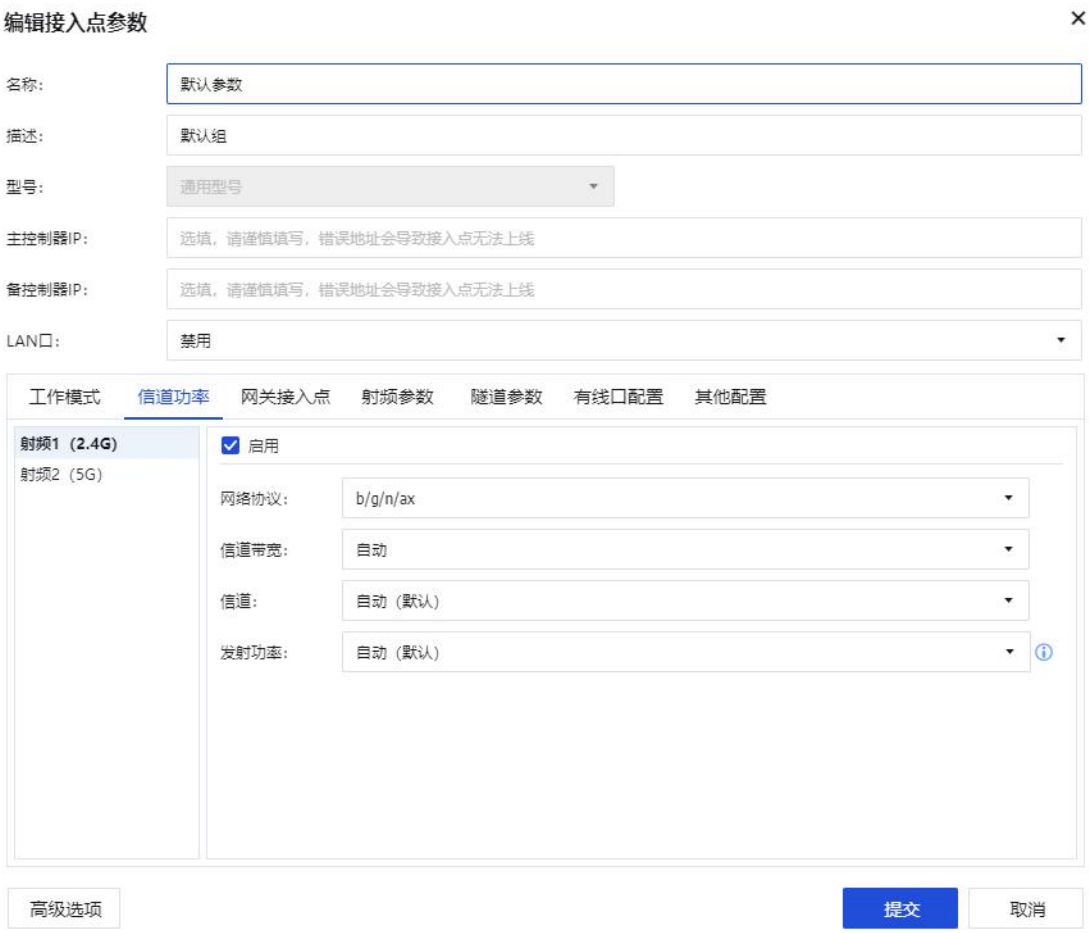
Normal 模式：表示是正常工作模式，AP 在该模式下，AP 可以固定工作信道，如果选择为 auto，射频和信道参数只会在 AP 每次加电时自动调整一次，后续都会稳定在该频率范围和信道上工作，不会变化，除非手动去【射频管理】菜单下手动点击调整。

Hybrid 模式：混合模式，默认选择该模式，AP 在该模式下，射频和信道参数会默认每个 10 分钟检测一次，如果发现当前信道通讯质量没有其他信道通讯质量好，会自动切换到质量更好的信道进行通讯。Hybrid 模式 AP 也可以用于钓鱼 AP 反制，但是反制效果不及 Monitor 模式 AP 效果好。

Monitor 模式：监控模式，在该模式下，无线网络不能正常使用，主要用于钓鱼 AP 反制。

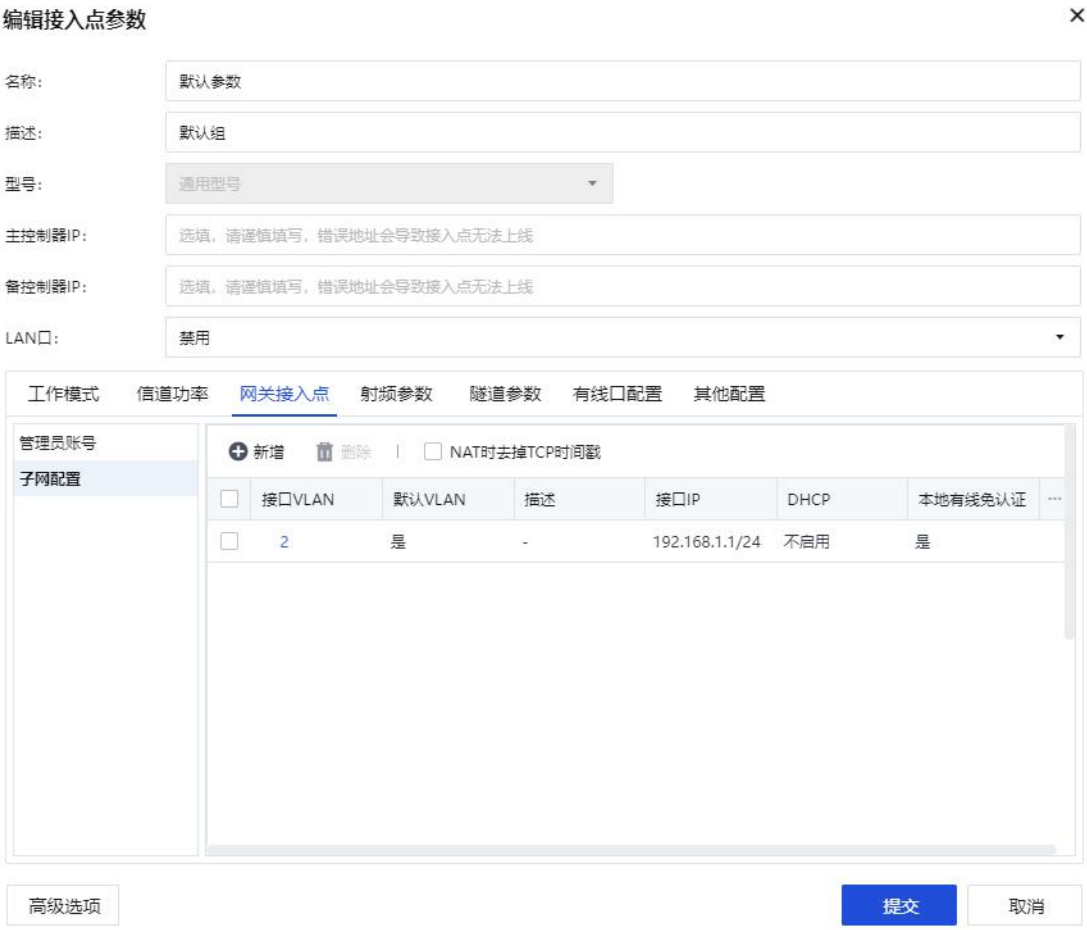
信道功率

可以在此对每个 AP 的功率和信道进行手动调整，在网络优化时，才需要手动配置此项功能。不同类型 AP 支持最大功率不一样，需要正确选择 AP 可工作的功率范围，配置界面如下：



网关接入点

在 AP 为网关模式本地转发时，在这里配置用于给 AP 下的终端分配地址的地址池。



射频参数

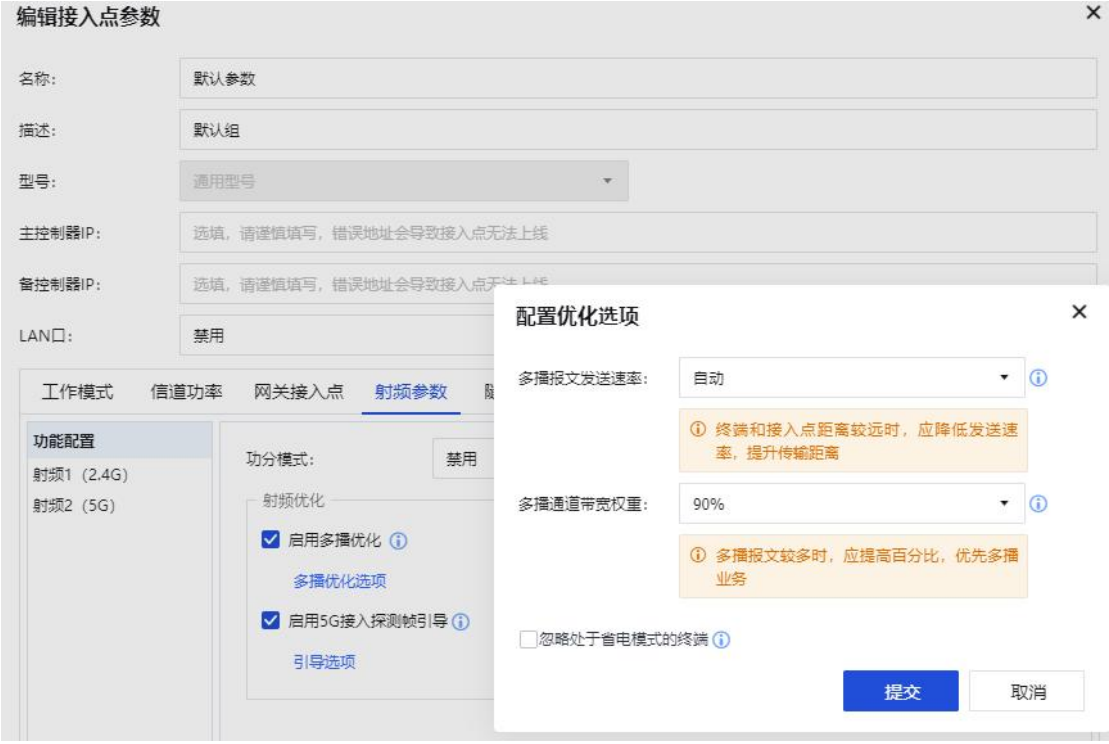
射频参数主要用于选择 AP 是工作在 2.4G 频段还是 5.8G 频段，以及选择网络协议 b/g/n 和 a/g/n 的选择，是否启用功分方案、调整信道、功率、等射频相关的功能。

1、5G 接入探测帧引导

在无线网络环境中，无论终端是否接入到无线网络，都会定期在每一个信道发送广播 probe request（探测帧请求）。当在无线用户比较多的网络环境中时，会产生大量以低速率发送的 probe reponse（探测帧响应）报文，影响接入点整体的吞吐量。启用高密优化选项后，接入点将不会响应终端广播的 probe request（探测请求），降低了由于低速率发送 probe response（探测帧响应）消耗的性能空间，提升高密度场景用户的无线上网体验。

2、多播优化

一般当单接入点覆盖范围内超过 40 个终端时，建议开启此功能。



无线接入点默认以 1Mbps 速率来发送多播报文，在多播报文较多的情况下会严重降低无线网络的总体吞吐率。目前可通过如下方式来提高无线网络的整体总体吞吐率。

（1）多播报文发送速率：

自动：系统将持续评估当前的无线网络环境， 自动选择一个更优，且不显著影响广播报文可靠性的速率来发送广播报文，提高了无线网络的总体吞吐率。

固定速率：无线接入点若以固定速率发送多播报文，可防止低速终端拉低多播报文整体吞吐率。适用于终端与无线热点距离在 10 米以内非干扰的多播应用场景。

（2）多播通道带宽权重：

在开启用户间平均分配带宽或者流量通道间动态分配带宽时，默认多播通道占用权重比例为 90%。若当前环境处于多播应用场景，可根据实际情况调整多播通道占用的权重比例。比如电子书包场景，建议将多播通道占用权重设置为 90%。

（3）忽略省电模式的终端：

按照 802.11 协议规定，如果接入点上有一个无线终端处于省电模式，则系统需要将所有的多播进行缓存，等到 beacon 帧发送后才能进行发送。这样在实时的多播应用场景下，如果存在睡眠的无线终端，将会导致多播报文无法快速及时发送，影响用户体验。

启用该功能后，接入点发送多播报文时将会忽略处于省电模式的无线终端，直接将报文发送出去。由于该功能实际上打破了 802.11 协议的定义，会造成处于省电模式的无线客户端无法接收到多播报文，所以仅对特殊场景应用（例如电子书包）可以考虑启用。

3、终端速率限制

该功能是信锐技术产品自研的优势功能，对于距离远的低速终端，拒绝其接入，可以提高其他正常信号范围内用户的上网体验。

通常情况下，离无线接入点越远的地方，终端接入进来的速率会越低。通过限制终端接入的速率，可以限制边缘区域的低速终端接入，这样可以提高无线接入点的吞吐效率，也能防止非目标用户的接入。限制的速率越大，有效的接入范围越小；限制的速率越小，有效的接入范围越大；不限制时，有效接入范围为最大。如果部署无线接入点的密度较大时，接入点的信号覆盖范围会较小，边缘接入的终端速率也相对较大些，如果想限制边缘终端用户接入，可以将限制的速率调大。如果部署无线接入点的密度较小时，接入点的信号覆盖范围会较大，边缘接入的终端速率也相对较小些，如果想限制边缘终端用户接入，可以将限制的速率调小。

4、数据传输速率下限

通常情况下，离无线接入点越远的地方，数据传输速率会越低。通过限制数据传输速率，可以限制边缘区域的低速终端接入，这样可以提高无线接入点的吞吐效率，也能防止非目标用户的接入。

5、限制 beacon 帧发送速率

Beacon 帧发送速率低时，对应睡眠周期拉长，节能省电，但是新连进来的设备就要很久才能显示出来这个 wifi 热点；Beacon 帧发送速率高时，发送 beacon 较为频繁，适合漫游之类的环境，可以高速切换到功率高，性能好的 AP 身上，但是会占用信道传输正常数据。

6、天线 MIMO

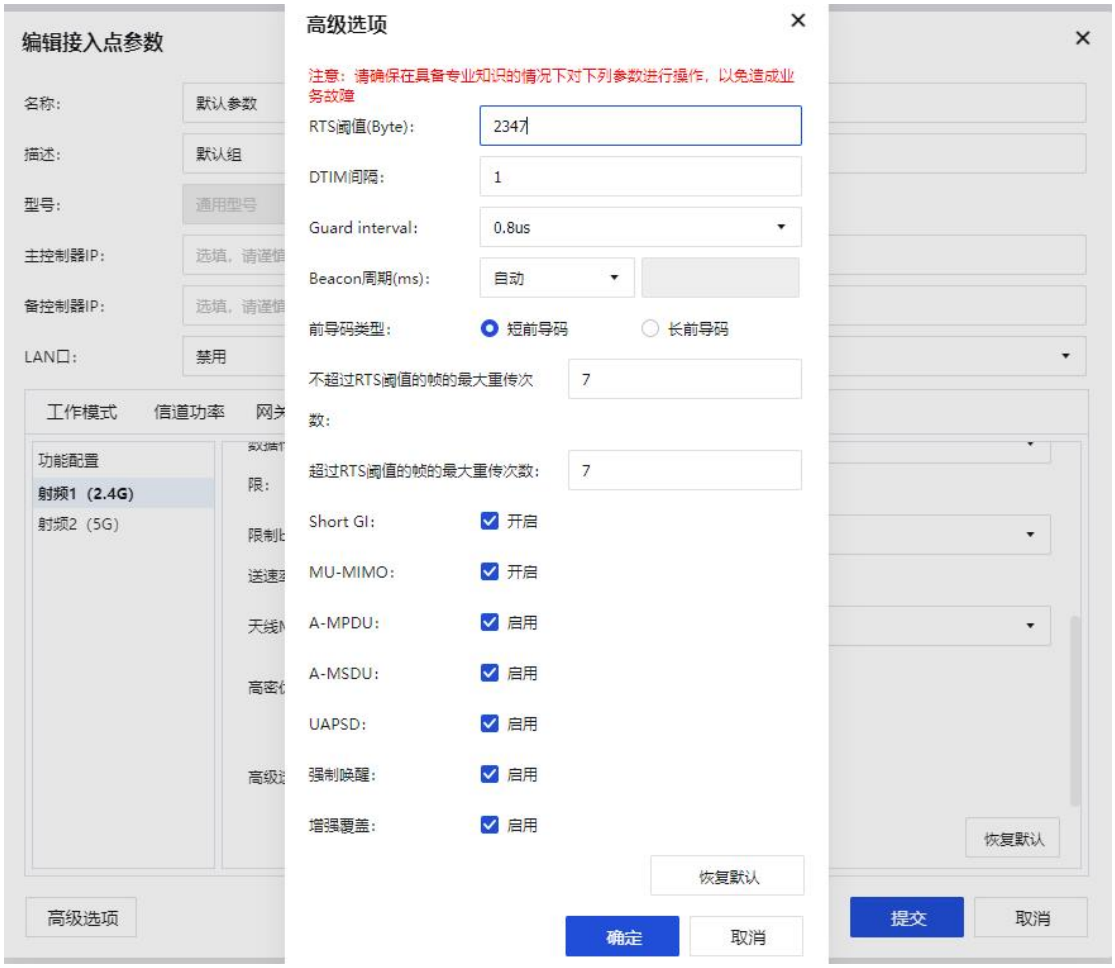
在做室外网桥/中继，或者部署一个狭长区域的时候，往往需要使用抛物面定向天线，但目前很多定向天线，只有 1 个天线接头，很少有支持 2X2 的，即使支持，很多体积和价格都过高，因此为了节约用户成本，需要将接入点上不用的天线关闭掉。

7、高密优化

在无线网络环境中，无论终端是否接入到无线网络，都会定期在每一个信道发送广播 probe request（探测帧请求）。当在无线用户比较多的网络环境中时，会产生大量以低速率发送的 probe reponse（探测帧响应）报文，影响接入点整体的吞吐量。启用高密优化选项后，接入点将不会响应终端广播的 probe request（探测请求），降低了由于低速率发送 probe response（探测帧响应）消耗的性能空间，提升高密度场景用户的无线上网体验。

8、高级选项

涉及到无线数据的传输效率问题，默认不建议也不推荐修改。

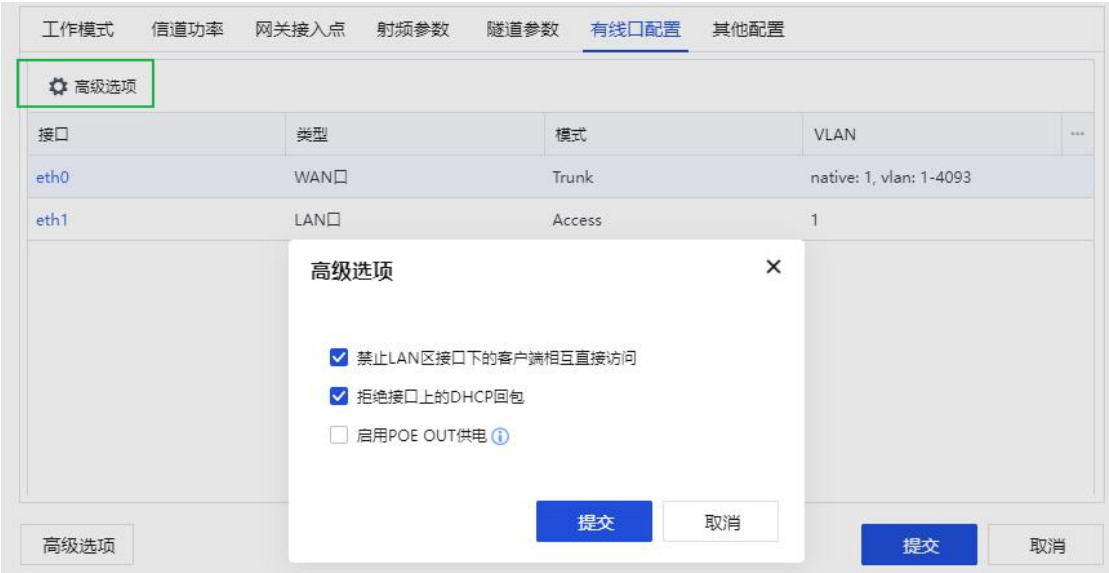


隧道参数

隧道参数：可以设置 AP 到 NAC 之间的数据隧道是否启用加密。用于设置 AP 与 NAC 之间的控制隧道保活时间，在较差的网络环境中，放大隧道保活时间，可避免因网络抖动造成的 AP 频繁断线。

有线口配置

有线口配置是指 AP 上的物理二层口，可以配置成 Trunk 口和 Access 口。当 VLAN 属性为 Trunk 时，允许 VLAN 是可以放通 vlan 范围，Native VLAN 是判断是否添加或剥离 vlan 头。



中继网桥

单个 AP 的参数配置里，还包含“中继网桥”的配置。中继网桥即无线中继与无线网桥，也就是 WDS（Wiresless Distribution System,无线分布系统），通过桥接方式，无线连接不同的局域网以及扩展无线局域网的覆盖范围。

一般用于有线部署不方便或者虽然有有线网络，但是网络拓扑配置不方便的场景。

传统的 wds 实现方式存在如下问题：

（1）client ap 仅仅充当无线天线的功能，所有业务都集中在 root ap 上处理，从无线覆盖的角度来看，root ap 和 client ap 的业务负载是对等的，导致 root ap 和 client ap 上的数据处理负载不均衡，即 client ap 过于空闲，root ap 过于繁忙。另外 root ap 可能会连接多个 client ap，更加重了这种不平衡，使得 root ap 成为了系统局部的一个业务瓶颈。

（2）AP 一旦作为 client ap 的角色，都是不支持企业级认证的，仅仅支持到 wep 和 wpa

psk。

（3）配置 client ap 时，必须手动配置指定 root ap，一旦网络拓扑发生变化，需要让 client ap 连接到别的 root ap 时，需要通过无线连接告知 root ap，在操作上比较复杂

而本功能完美地解决了上述存在的不足和缺陷，即：

（1）通过对 client ap 上的业务数据使用不同于传统 wds 机制的处理和转发方式，client ap 可以支持现有 7 种认证方式，即 WPA/WAP2（企业）、开放式、WPA-PSK/WPA2-PSK（个人）、WPA、WPA2、WPA-PSK/WPA2-PSK（个人）+ Web 认证、开放式+Web 认证。

（2）在本功能的实现中，root ap 仅仅只充当交换机的角色，即 root ap 仅负责转发数据，client ap 上的业务有 client ap 自己处理。

（3）client ap 通过自动发现机制发现和连接 root ap，实现了 root ap 的动态主备冗余，当一台 root ap 出现故障的时候，client ap 会自动连接到其他的 root ap 上，避免了 root ap 的单点故障。client AP 动态选路连接 root ap 存在限制条件：client ap 和 root ap 必须属于同一个 AP 分组。

（4）client ap 无法支持控制器灾备。

（5）root ap 上提供给 client ap 建立 WDS 连接的 SSID 和接入密钥以及连接频段可配置。client ap 上支持配置要连接的 root ap 的连接 SSID 以及接入密钥。

注：1)组建 WDS 网络之间的接入点所选择的无线频段必须是相同的。

2）Root 网关模式和 client 普通模式：client 的 wan 口 IP 不可以配成与 Root 的 wan 口 IP 相同网段；client 的 wan 口 IP 要从 Root 的子网上获取， Root 为网关模式时，桥接口为 trunk， native vlan 是子网的默认 vlan。因为 client 的桥接口是 trunk native1， wan 口 vlan 需要默认与 eth0 相同是 vlan1；client 上的用户如果是本地转发，那么策略 vlan 只能

配成 Root 上的子网的 vlan， 在 Root 上的子网内转发。因为 Root 是网关模式， eth0 口是 access1，client 通过桥接发上来的本地转发的带 vlan 的用户报文不能从 Root 的 eth0 转发出去；client 上的用户如果是集中转发，那么策略 vlan 可以随意配。

3）Root 普通模式和 client 普通模式：client 的 wan 口 IP 应该与 Root 的 wan 口 IP 相同网段；client 上的用户本地转发/集中转发都可以

4）慢速移动桥接：慢速移动桥接主要解决传统无线网卡单链路漫游效果差的问题，提供双链路（client）保证慢速移动过程中的网络连通性，仅支持 NAP3620/AP362 和 NAP3620（R3）/AP 533(R3)。

其他配置

3.3.1.3. 发现新接入点

为防止未授权的接入点连接到 NAC，并获取无线网络配置的风险。无线接入点（AP）连接到 NAC 后，并未进入工作状态，需要管理员在"发现新接入点"列表中，确认接入点的合法性，并手动执行激活操作，接入点才能正常工作。

当 AP 接入网络中，AP 会自动发现 NAC，当 AP 第一次发现 NAC 时，会在 NAC 上看

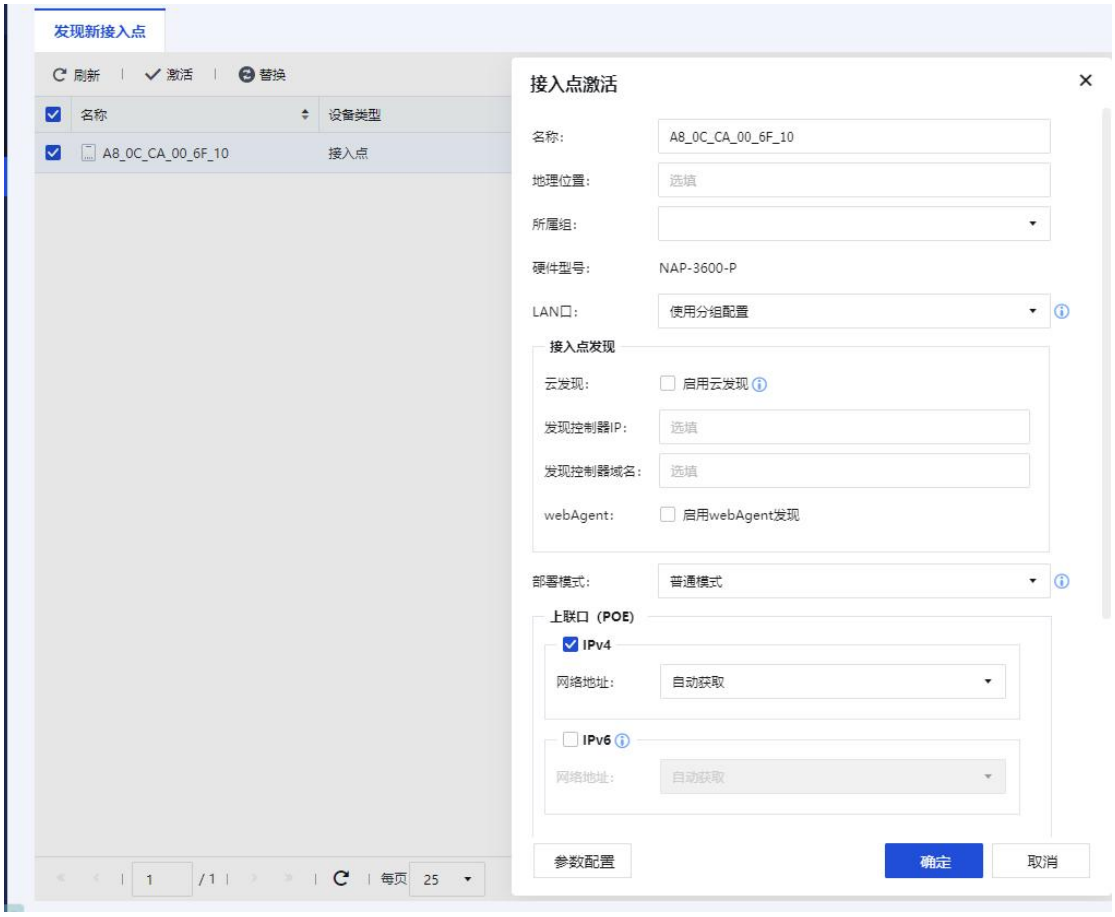
到新的接入点，需要进行激活后，才能正常使用无线 AP，并下发配置。

提示：在 NAC 控制台的右上角，当有出现图标  时，表示还有未激活的接入点，需要到该页面激活。

激活 AP

当 NAC 上发现 AP 时，需要激活，激活按钮可用

点击激活后，配置界面如下：



可以编辑 AP 的名称，地理位置，便于后续 AP 的识别分组和管理，默认 AP 以其 MAC 地址为名称

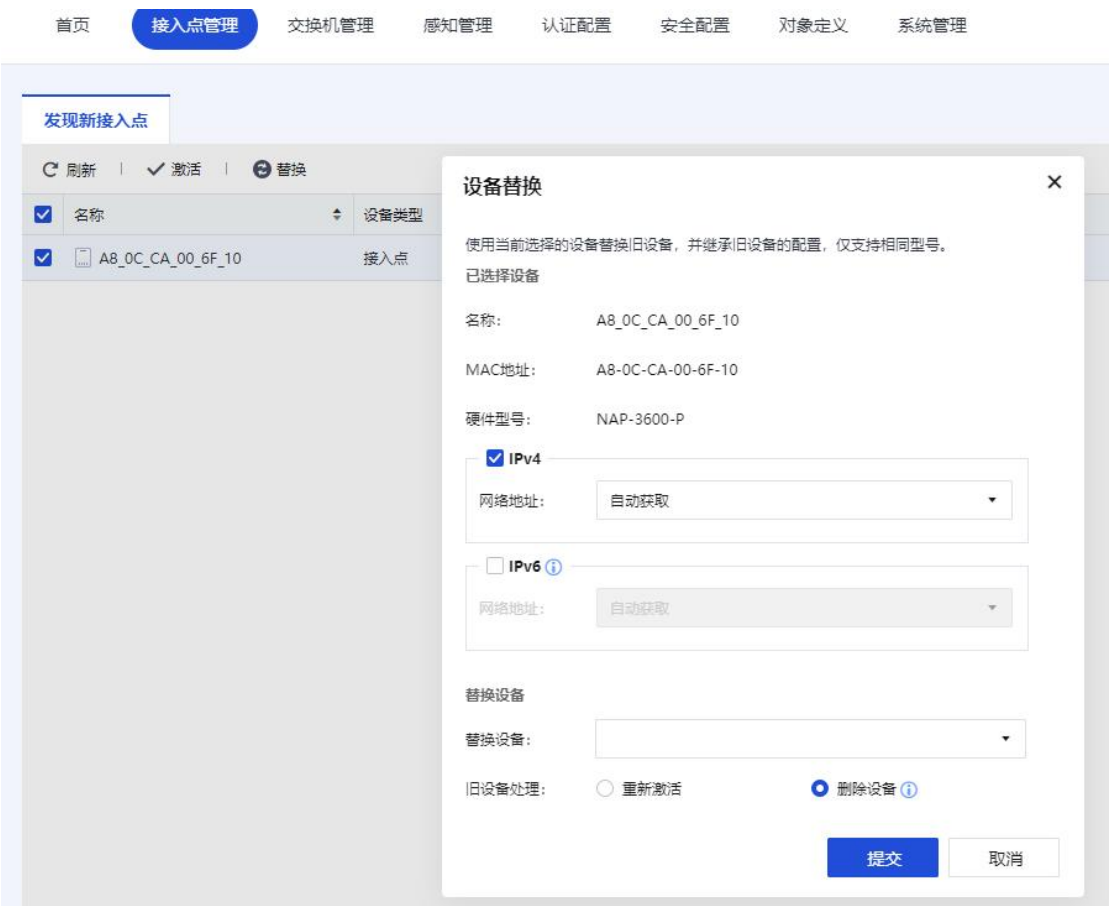
- 所属组：配置 AP 所属于的管理组，便于对 AP 进行集中管理和配置。
- 发现控制器 IP：填写 AP 用于连接的 NAC 的 IP 地址，如果给 AP 填写了 NAC 的地址，AP 下次重启后，会自动以该配置 IP 连接 NAC 并建立隧道
- 发现控制器域名：用于 AP 自动发现 NAC 用，当 AP 解析到该域名时，AP 会自动向 NAC 请求连接。NAC 发现该 AP 后，就可以对该 AP 进行策略下发配置了
- 网络地址：可以设置自动获取，也可以设置固定 IP 地址

替换

接入点和交换机均支持设备替换功能，设备替换分为两种操作：

交换机激活的时候，设备类型分为两种：

- 发现新设备时，可以将要激活的设备替换为已经激活过的设备。替换时，可以选择将旧设备删除或是重新激活。
- 接入点管理或交换机管理页面，可以选择将两个设备的配置互相替换。



3.3.2. 无线网络

『无线网络』：可以【新增】、【删除】、【启用】、【禁用】一个无线网络。新增无线网络需要设置无线终端接入的无线信号 SSID，认证方式，设置无线接入点范围，数据转发模式等，下面将一一详细讲解。下面的无线网络的配置截图：

无线网络号 SSID 可以设置为“汉语”，对汉语的支持比较好无线终端可以正常显示，多数 PC 无法正常显示，一般建议设置为英文类型的 SSID。

新增一个【无线网络】，包含【基本配置】、【认证类型】、【终端验证】、【帐号认证】、【访客认证】、【多因子认证】【vlan 设置】、【权限设定】、【应用节流】、【高级选项】，如下图：

3.3.2.1. 基本配置

【基本配置】需要设置无线网络名称（SSID），并设置无线网络在哪些接入点 AP 上启用，

以及该无线网络在 AP 上的数据转发模式，并设置工作频段。

数据转发模式分为集中转发，和本地转发模式，集中转发模式表示无线终端 STA 所有的上网业务数据到达 AP 后，由 AP 进行数据分装，由 AP 集中转发给 NAC，在由 NAC 集中转发出去上网。本地转发模式表示无线终端 STA 所有的上网业务数据到达 AP 后，由 AP 根据本地路由网关直接转发数据出去，不对数据包进行分装。

设置的频段分为 2.4G 和 5G 共 2 个频段，可以分别设置启用，也可以设置 2 个频段同时启用。其中高级选项中，可以针对该 SSID，每个 AP 接入人数做限制，隐藏 SSID 表示该无线网络不主动广播其信号，无线终端不能自动发现该网络，必须在无线终端 STA 上手动填写 SSID，并设置才能接入该无线网络。营销广告推送设置，如果需要使用控制器营销推送功能，需要勾选以下 2 个设置。

3.3.2.2. 认证类型

认证类型有以下几种类型可以选择：

- [WPA/WPA2(企业)]：选择 WPA 或 WPA2 加密方式的企业认证方式
- [WPA（企业）]：仅选择 WPA 加密方式的企业认证方式
- [WPA2（企业）]：仅选择 WPA2 加密方式的企业认证方式
- [WPA-PSK（个人）]：选择 WPA 加密方式与预共享密钥的个人认证方式
- [WPA2-PSK（个人）]：选择 WPA2 加密方式与预共享密钥的个人认证方式
- [WPA/WPA2-PSK(个人)]：选择 WPA 或 WPA2 加密方式与预共享密钥的个人认证方式
- [开放式]：选择开放式的无线接入方式认证
- [开放式+WEB 认证]：选择开放式的无线接入方式与 WEB 方式认证组合
- [WPA-PSK/WPA2-PSK+WEB 认证]：选择 WPA 或 WPA2 加密方式与预共享密钥认证方式接入无线网络，再结合 WEB 方式认证的组合。

下面我们对这些认证类型做一个简单的分类，以便进行功能区分，所以该分类依据是以功能

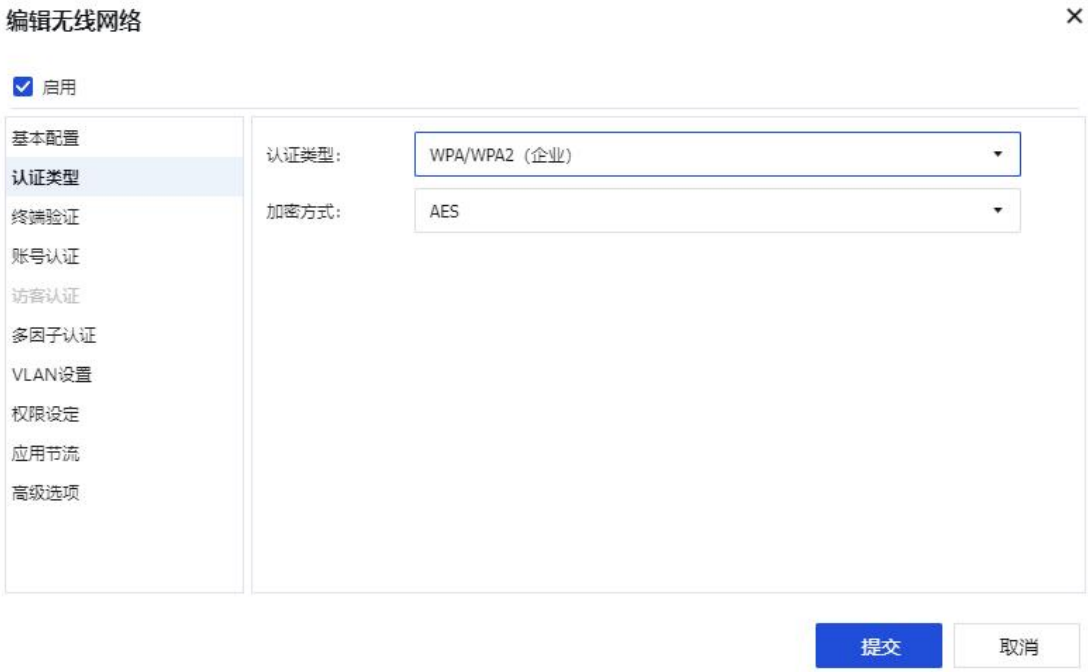
性差别进行的划分，他们之间有重合的可能，比如开放式认证和 WEB 认证就可以结合一起使用，划分为如下四类：

企业方式认证

选择采用“企业”方式的认证还包括 WPA（企业）、WPA2(企业)、WAPI(企业)

加密方式：自动选择，包括 AES 和 TKIP，企业类型的认证，在终端验证和用户认证出现的界面与 WEB 方式认证是有所差别的，这些差别就决定了“企业方式认证”和“WEB 方式认证”与“个人方式认证”的差别。

企业方式认证是采用 802.1X 架构的认证方式，无线终端也需要采用配置 802.1X 方式认证。

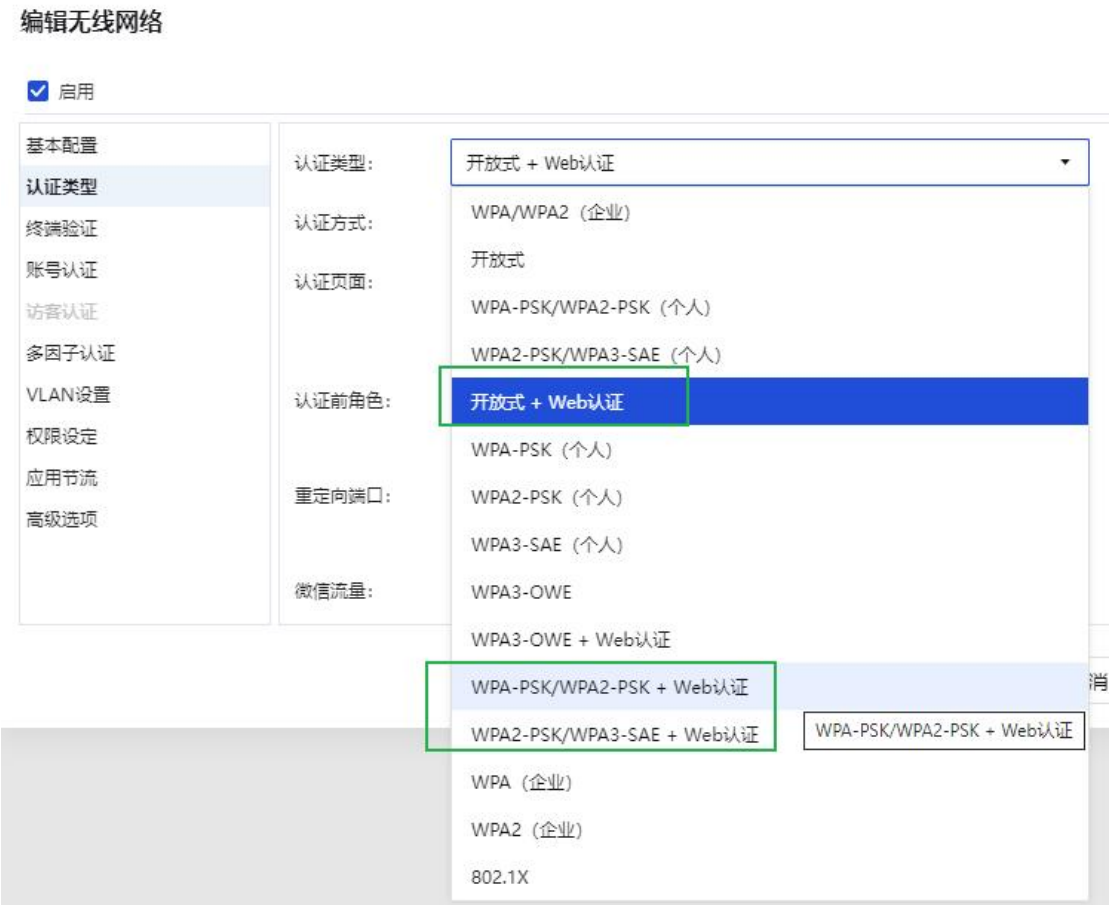


WEB 方式认证

web 认证是指无线终端接入无线网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。

web 认证通常与开放式无线网络一起使用，也就是用户连接无线网络时，不需要任何认证。由于无线网络的流量未加密，因此 web 认证的无线网络，通常只用于非关键性的网络中，例如仅用于访客访问互联网，无法访问企业内部网络。

WEB 方式认证包括：WPA-PSK/WPA2-PSK+WEB 认证、开放式+WEB 认证；



认证方式:

1、【帐号认证】、【访客认证】、【账号认证+访客认证】

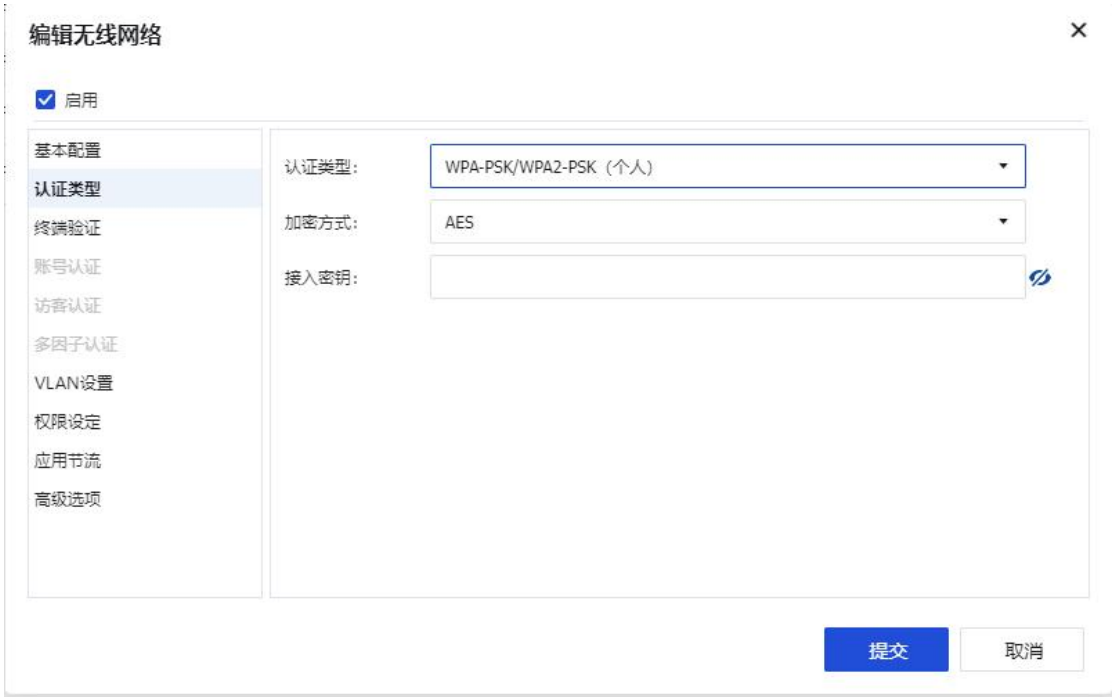
2、【使用外部 Portal 服务器认证】可以对接外部 Portal 服务器实现外部 portal 认证。

认证页面是我们在【认证授权】-【认证页面】设置的自定义页面或者采用系统默认的页面。采用第三方 Portal 认证时，Portal 服务器选择【认证授权】-【认证服务器】中添加的 portal 服务

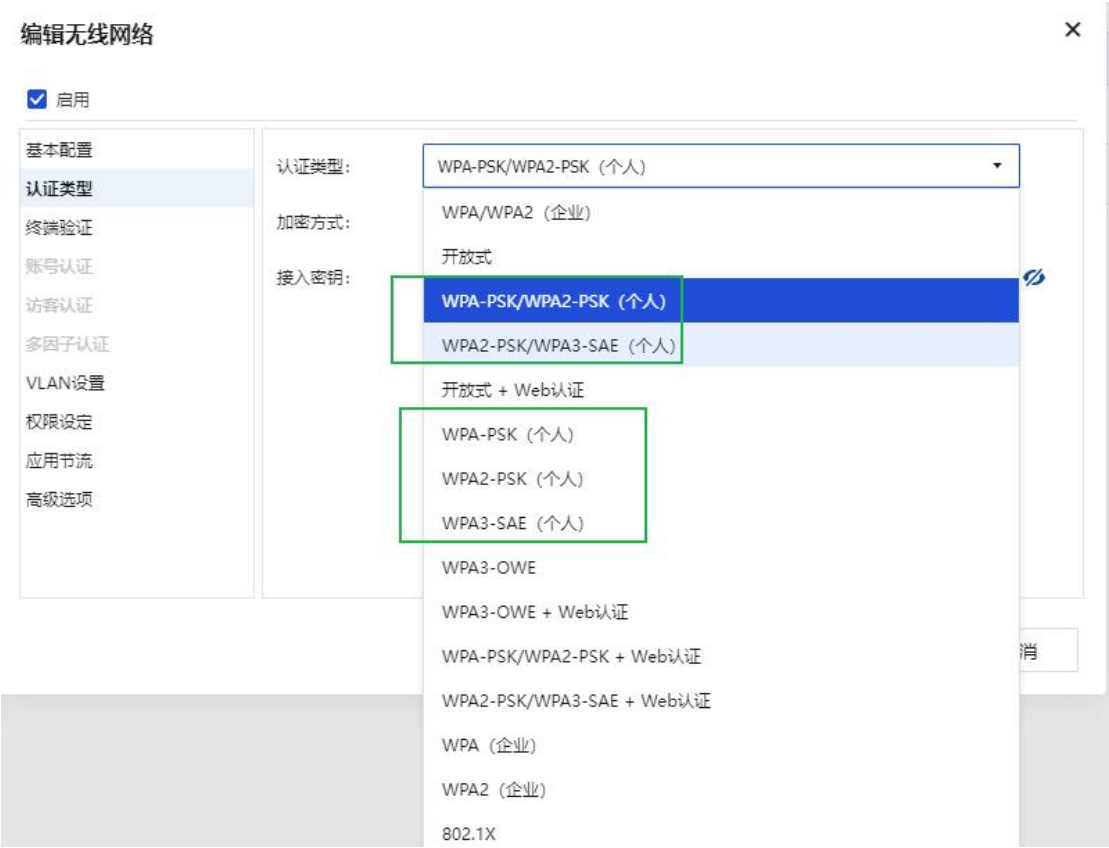
器。认证前角色是指进行 WEB 认证成功前，默认可以使用的网络权限对应的角色，重定向端口是指无线终端 STA 有该端口的数据时，进行认证页面的重定向。

个人方式认证

选择“个人”方式的认证



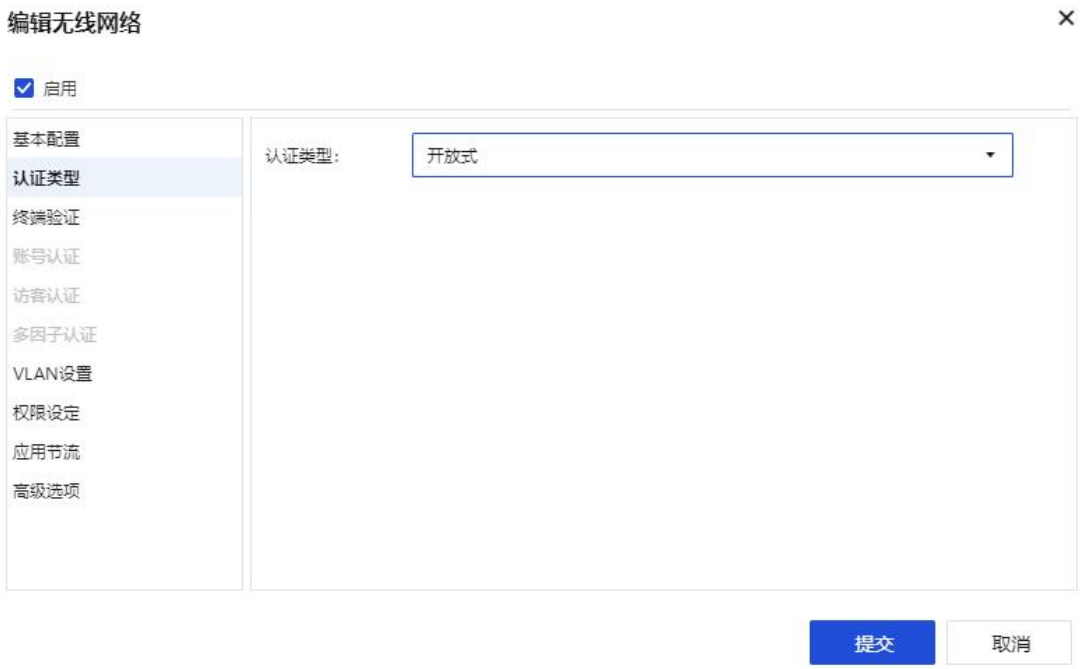
个人方式认证包括：WPA2-PSK（个人）、WPA-PSK（个人）、WPA/WPA2-PSK(个人)以及 WAPI-PSK（个人）。



加密方式：自动选择，包括 AES 和 TKIP 方式，接入密钥是只设置接入无线网络的预共享密钥。

开放式认证

开放式认证是指无线终端用户接入无线网络时不需要进行验证即可正常接入无线。



3.3.2.3. 终端验证

终端验证可以显示的内容是由已经选择的认证类型来决定的，选择不同的“认证方式”，会显示不同的页面，也就会有不同的功能性差异。

当选择了包含“开放式认证“和“个人认证”方式时，可以对无线终端的终端类型和 MAC 地址的合法性进行校验，其中 MAC 地址校验是通过启用“检测终端 MAC 黑白名单”来进行的。MAC 白名单是在【认证授权】-【MAC 白名单】预先设置好的合法 MAC 地址。

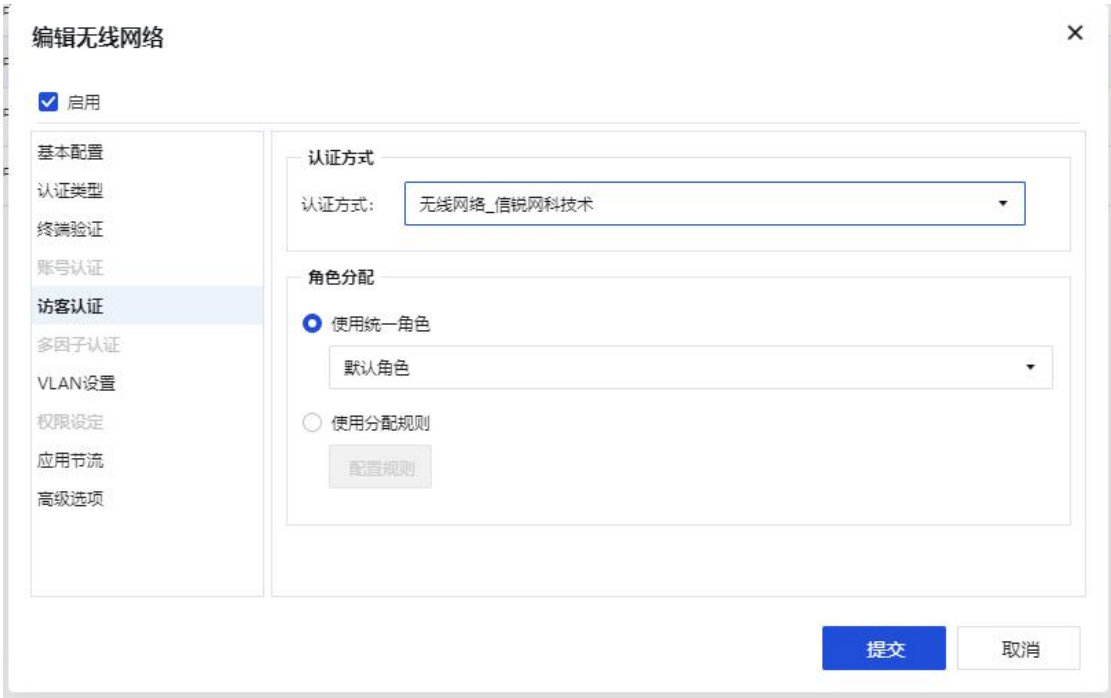
开放式+web 认证时，终端验证的配置如下：

“终端验证失败后”表示即使 MAC 与终端类型验证失败后，也继续让该用户进行后续的 WEB 方式认证。如果不勾选该功能，只要无线终端的 MAC 验证不在【对象定义】中的【MAC 白名单】中，就完全拒绝该用户的进行进一步认证，直接拒绝其上网。

选择“企业”方式认证后，终端验证也可以启用检查终端 MAC 白名单。可以设置允许终端验证失败（或未加入域）时，继续进行用户认证，并设置认证通过后的角色。认证通过后的 vlan。为通过域计算机验证的客户端分配权限以登录到域，需要设置可以使用的角色让 PC 能正常登录到域，并设置对应的 vlan。

3.3.2.4. 访客认证

在部署用于访客使用的无线网络时，为了简化用户体验，通常设置为开放式的无线网络。但单纯的开放式的无线网络，存在无法验证访客身份的问题，因此通常需要设置认证方式。此方式主要部署在公众访问的无线网络中，例如部署在机场，交通枢纽，医院，酒店，商场，学校等地方。



3.3.2.5. 帐号认证

Web 方式认证

当选择【开放式认证】和【个人认证】时不能选择配置【帐号认证】，只有选择【WEB 方式】或【企业】方式时才可以配置

如下是当选择企业或 WEB 方式认证时，可以配置的用户认证配置：

当选择 WEB 方式认证时，帐号配置页面如下

企业方式

企业方式有以下下几种认证类型：EAP 终结与 EAP 中继 2 种方式。并可以设置服务器认证配置冗余，以及设置自动绑定最初认证用户名与 MAC 地址，并可以指定对某一类型的终端进行 MAC 地址绑定关系检查，比如 windows 终端。

1、EAP 中继

EAP 中继是指无线接入点把无线客户端的 EAP 报文直接转发到 RADIUS 服务器，由 RADIUS 服务器来完成认证过程。因此认证方法由 RADIUS 服务器中配置，与 NAC 无关。

在 WPA/WPA2-企业 无线网络中，通常使用的认证方式为 EAP-TLS 或者 PEAP-MSCHAPv2，因此需要确认 RADIUS 服务器支持所需的认证方式。常见的 RADIUS 认证服务器为微软 Windows Server 系列中提供的 IAS/NPS 服务。

2、EAP 终结

“EAP 终结：EAP-TLS” 是指由 NAC 来完成 EAP-TLS 认证过程。EAP-TLS 协议是在 EAP 协议框架上，使用 TLS 协议来完成身份认证，密钥交换功能。TLS 协议也是 HTTPS 协议的核心。因此 EAP-TLS 可以视为与 HTTPS 协议具备同等的安全性。

EAP-TLS 协议使用双向证书认证，要求服务器及客户端都使用证书，向对方证明身份。并使用非对称加密方式，在无线客户端及认证服务器间安全地协商数据加密密钥，保证无线数据传输的机密性及完整性。

由于使用了基于证书的身份验证方法，避免了基于密码认证方法所存在的由于密码泄漏，密码强度低等原因导致的密码被猜测或暴力破解的风险。因此 EAP-TLS 提供了目前无线认证中，最安全的认证方法。缺点是所有客户端都需要安装个人证书，部署比较复杂。

3、**服务器证书（向无线用户证明身份）**

在 EAP-TLS 身份验证过程中，服务器使用此证书创建 TLS 连接，并向客户端计算机证明身份。客户端可以选择验证此证书的颁发者及主题名称，来保证连接到正确的企业无线网络中，避免连接到由攻击者伪造的同名恶意网络导致的安全风险。

由于系统自带的服务器证书未被客户端信任，在 Windows 系统客户端中，如果无线网络配置选择了"验证服务器证书"，将导致客户端无法连接无线网络。因此需要了解关于服务器证书的要求，如果有必要，需要考虑向商业证书颁发机构购买证书。

4、CA 证书

用于检查客户端合法性的 CA 证书。客户端提交的证书将要求由此 CA 颁发，并通过此 CA 配置的有效性检查选项。

5、EAP 终结：PEAP-MSCHAPv2

“EAP 终结：PEAP-MSCHAPv2” 是指由 NAC 来完成 PEAP-MSCHAPv2 认证过程。

EAP-MSCHAPv2 是基于密码的认证方法，最初是由微软设计用于为拨号及 VPN 连接提供更安全的认证方法。虽然 EAP-MSCHAPv2 提供了更安全的认证方法，但存在的安全弱点是，如果攻击者能监听 EAP 报文，则可以通过离线的字典攻击，分析用户的密码。

把 EAP-MSCHAPv2 跟 PEAP 结合一起使用，得益于 PEAP 内部创建的 TLS 隧道所提供的健壮安全性，EAP-MSCHAPv2 的交互过程可以得到加密保护，从而防止了攻击者通过离线字典攻击方式来分析用户密码的安全弱点。

PEAP-MSCHAPv2 协议，由 2 个阶段组成：

阶段 1，PEAP。首先协商 PEAP 协议，创建一个只使用服务器证书的 TLS 隧道。在这个阶段中，客户端可以选择验证服务器证书，并检查服务器端证书的主题、颁发者等证书信息，完成对服务器证书的认证，避免连接到一个由攻击者创建的，名称相同的无线网络中导致的安全风险。

阶段 2，EAP-MSCHAPv2。在 PEAP 协议的 TLS 隧道内部，协商另外一个 EAP 方法，这里为：EAP-MSCHAPv2。在这一步中，客户端需要提供用户名及密码凭据，以完成

对客户端的身份验证。验证完成后，RADIUS 服务器，会为每个客户端生成不同的会话密钥，以对接入点与无线客户端之间传输的无线数据包进行加密。

6、服务器证书（向无线用户证明身份）

在 PEAP-MSCHAPv2 协议阶段 1 中，服务器使用此证书创建 TLS 连接，并向客户端计算机证明身份。客户端可以选择验证此证书的颁发者及主题名称，来保证连接到正确的企业无线网络中，避免连接到由攻击者伪造的同名恶意网络导致的安全风险。

由于系统自带的服务器证书未被客户端信任，在 Windows 系统客户端中，如果无线网络配置选择了"验证服务器证书"，将导致客户端无法连接无线网络。因此需要了解关于服务器证书的要求，如果有必要，需要考虑向商业证书颁发机构购买证书。

7、允许登录用户

选择允许连接无线网络的组，默认选择根组，也就是所有本地用户都允许通过认证，并连接此无线网络。

8、RADIUS 服务器冗余

使用 RADIUS 中继模式下，允许配置多个 RADIUS 服务器，实现认证服务器的故障冗余备份。

3.3.2.6. VLAN 设置

VLAN 配置是为了更好的实现无线终端的控制和管理，进行无线 VLAN 的划分；无线 VLAN 划分与有线网络 VLAN 的划分是有一些差别的，无线 VLAN 的划分以及 VLAN 之间的数据处理，是由 AP 和 NAC 针对无线网络用户进行管控和路由的，而 AP 和 NAC 之间是由隧道封装的。所以当采用集中转发时，无线 VLAN 的标签是在 AP 与 NAC 中间的隧道内。当本地转发数据时，配置 VLAN，无线数据标签由 AP 打上标签转发出去。

用户认证成功后，系统将提取出用户此次认证过程的所有属性，主要包括：用户名，所属组，接入的 AP，RADIUS 服务器返回的属性值，用户的 LDAP 属性值，证书中的属性值等。然后从上往下，按优先级方式查找角色以及 VLAN 分配规则表，如果用户的属性匹配上规则的条件，则根据规则中的设定值，为用户分配角色或 VLAN。

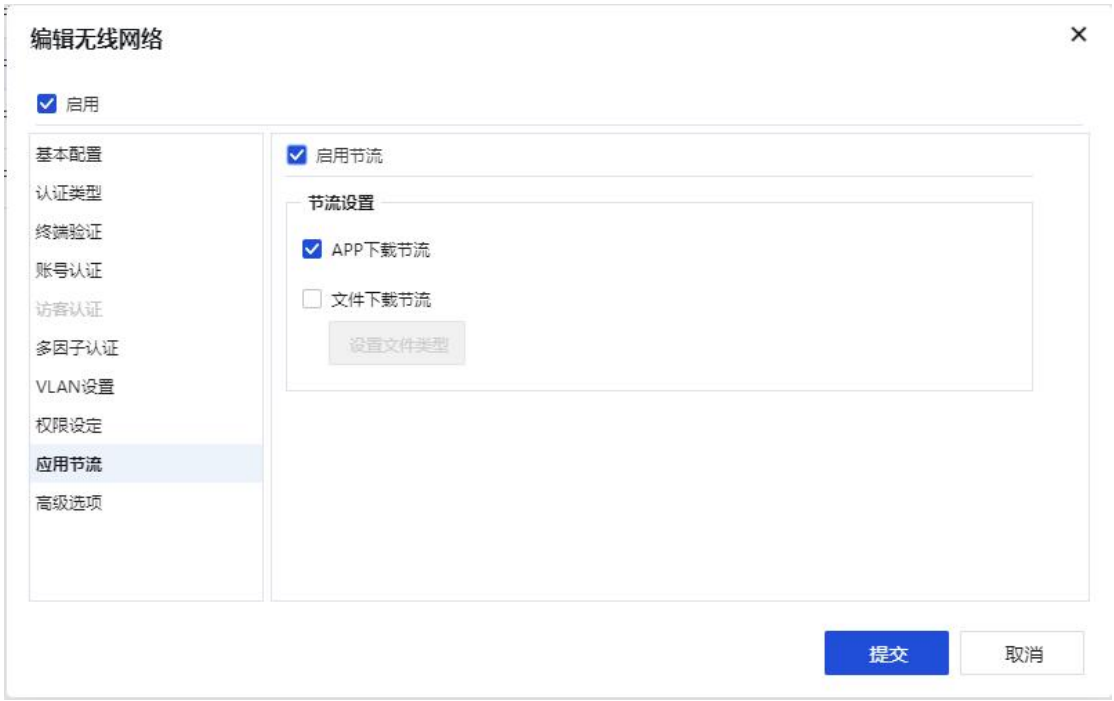
每一条规则中可以包含 1 个或多个条件，如果包含多个条件，则要求同时满足，才视为匹配此规则。如果用户未匹配规则表中的任何规则，则使用设定的 "默认角色" 和 "默认 VLAN"。

3.3.2.7. 权限设定

【权限设定】主要用于设定终端通过认证后，具有访问网络资源的权限，角色包括访问控制策略、审计策略、流速限制策略、流量与时长控制策略，可以根据 AP 组，无线终端用户组等信息详细的配置角色策略，可以根据 SSID 设置一个默认的角色，配置如下：

3.3.2.8. 应用节流

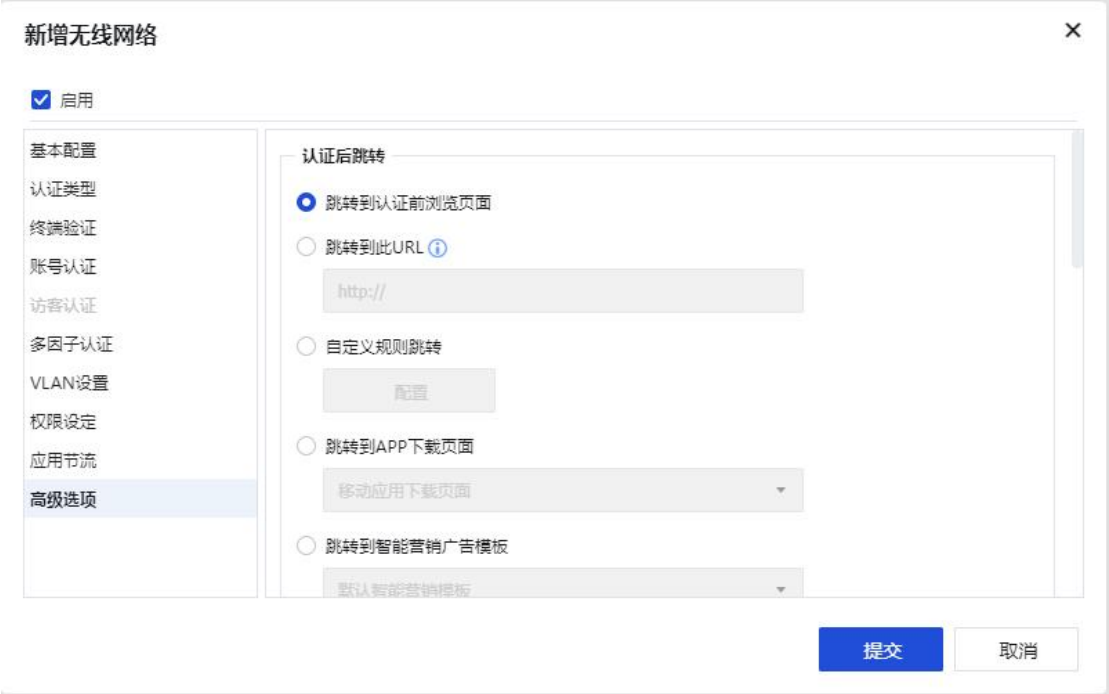
有利于节省您的网络带宽资源，提升终端浏览/下载体验。如果您使用了 APP 推广，推荐开启 APP 下载加速。



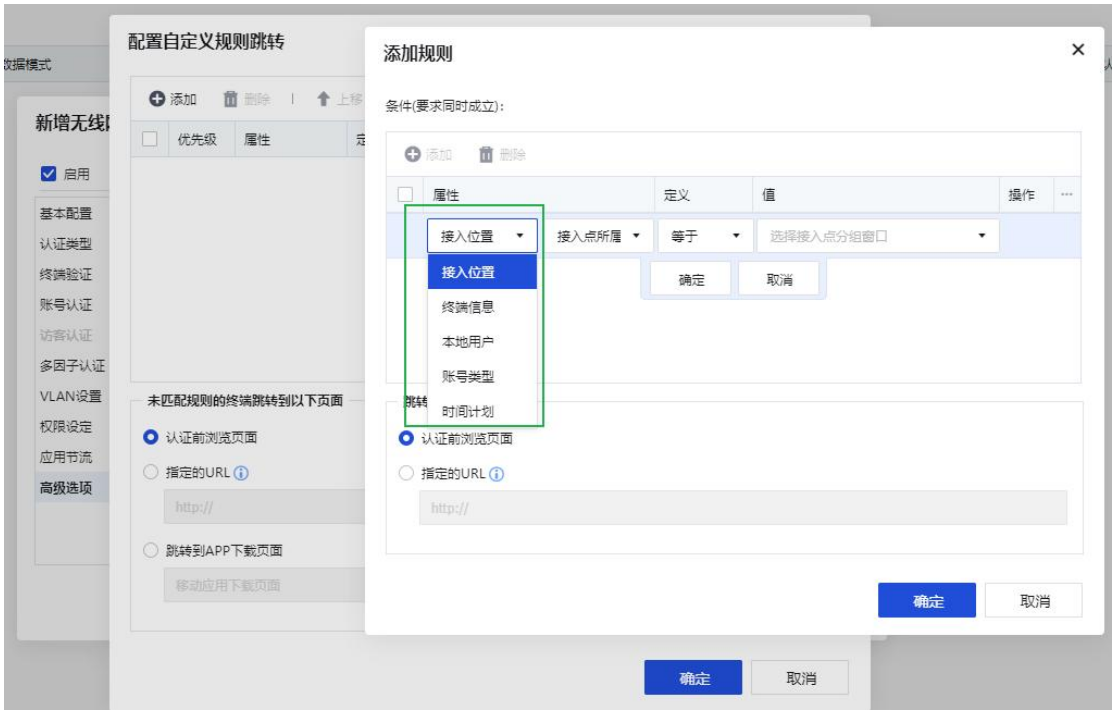
3.3.2.9. 高级选项

认证后跳转

认证后跳转功能是指启用 WEB 认证后，帐号认证用户与访客认证用户通过认证后调整的页面，默认跳转到认证前浏览的页面，可以设置固定的 URL，配置如下：

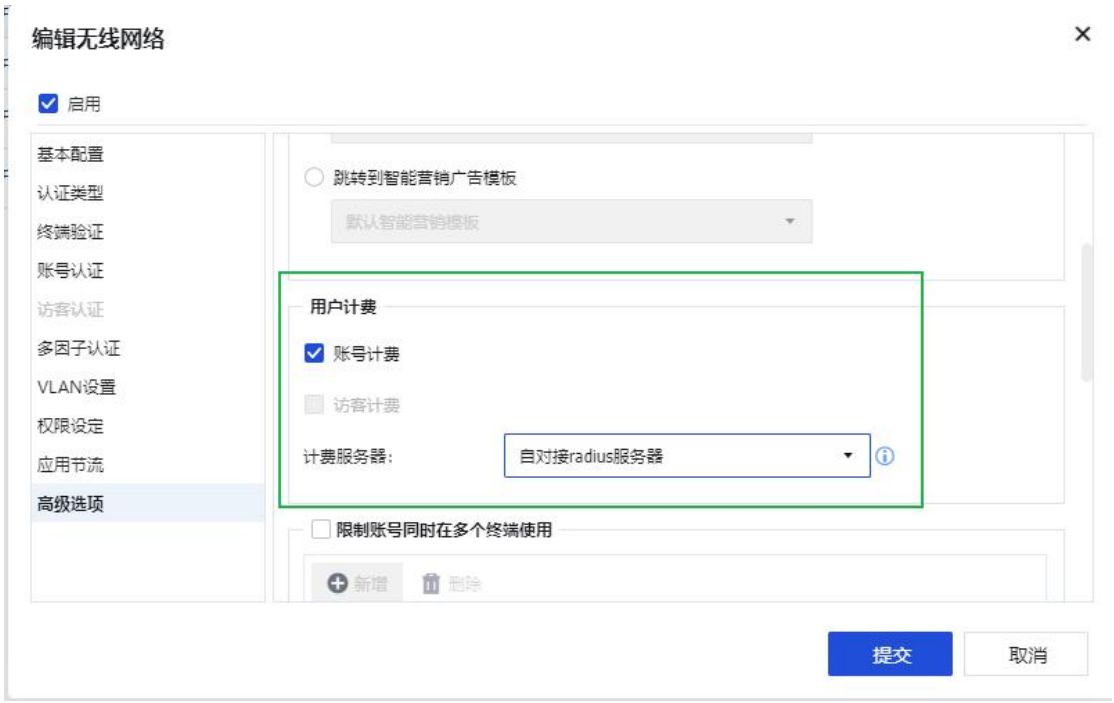


还可以根据不同用户所在 AP 组的位置，以及用户组的方式指定认证跳转的页面，配置如下：



用户计费

可针对 WEB 认证账号认证和访客认证的用户添加计费服务器进行计费。



限制账号在多个终端同时登录

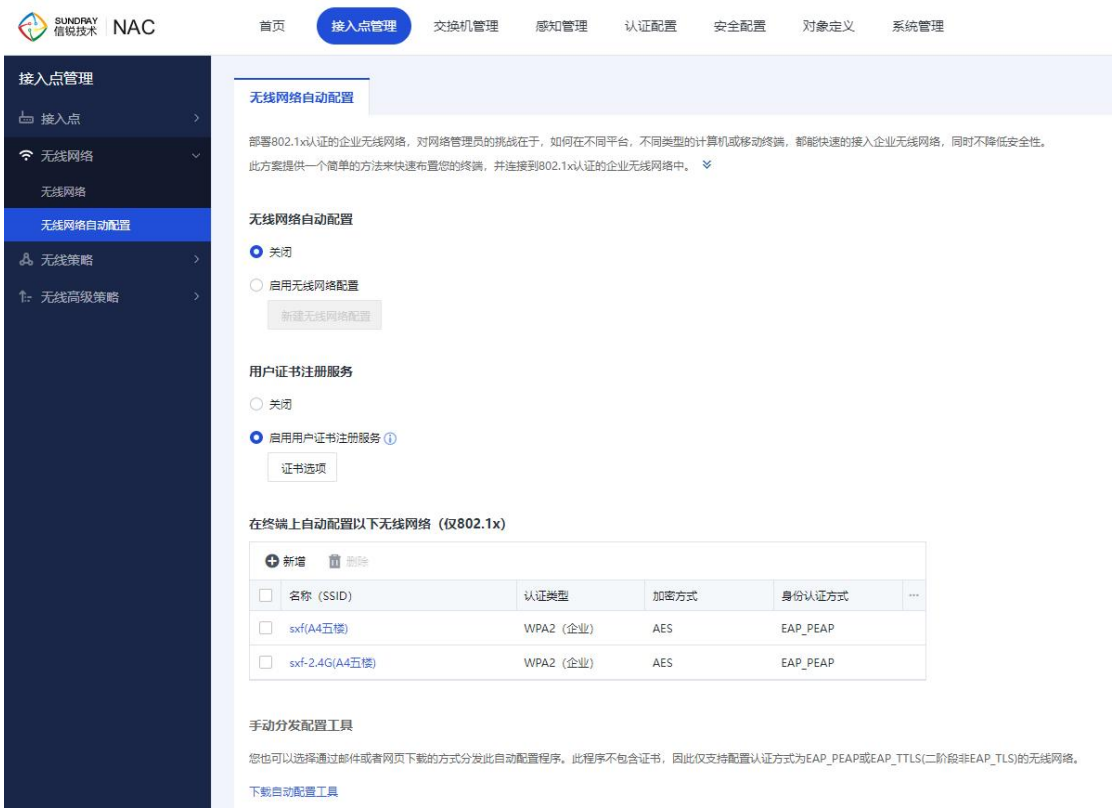
限制帐号同时登录的终端数，比如只允许帐号在一台终端上登录，不允许在多台终端上登录，就类似私有帐号与公有帐号的区别。

WEB 接入 MAC 免认证

Web 接入 MAC 免认证针对 WEB 认证的账号认证及访客认证有效，在该列表中排除的终端，连接无线后将不需要进行 WEB 认证直接分配对应角色。

3.3.2.10. 无线网络自动配置

无线网络自动配置，为了快速便捷的部署无线网络，便于管理员维护，可以在此配置无线网络自动配置，具体配置页面如下：

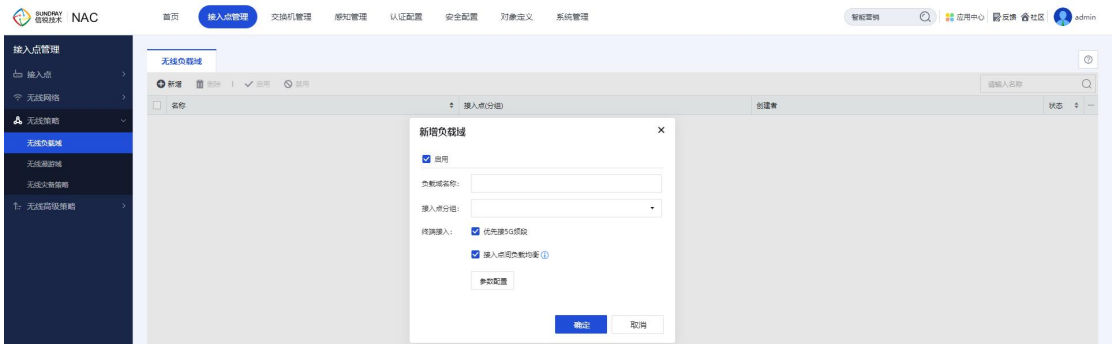


用户证书注册服务：“证书注册服务” 是无线网络自动配置方案的一部分。在部署基于证书认证，且使用内置 CA 颁发用户证书的无线网络时，需要启用 “证书注册服务”，使得 “自动配置工具” 能为用户自动申请并安装个人证书，才能完成无线网络的自动配置。

3.3.3. 无线策略

3.3.3.1. 无线负载域

按接入点分组划分出一个区域，控制该区域的终端接入时是否优先接入 5.8g 频段、是否开启接入点间负载均衡和动态负载引导，也可以控制该区域的射频是否需要射频信号覆盖补偿。



优先接入 5.8G 频段

用来引导双频无线客户端优先接入无线环境中的 5.8G 网络，勾选后，可以提高 5.8G 网络的利用率。

接入点间负载均衡

客户端连接无线网络时，如果同时探测到多个接入点的信号，通常会选择连接信号强度最高的接入点。这可能会导致相邻的几个接入点间，负载不平衡，例如某个接入点服务了大量的用户，但临近的另外一个接入点仍然比较空闲。

启用接入点间负载均衡功能后， 在用户接入网络时，如果已连接用户数超过指定值时， 将会执行负载均衡(当无线客户端连接到某个繁忙的接入点后， 此接入点将拒绝该客户端接入， 迫使无线客户端漫游到一个附近较空闲的接入点。 如果拒绝失败，则会使用漫游引导报文， 引导无线客户端漫游到人数较少， 信道利用率较低的接入点)，以平衡接入点的负载。 负载均衡操作只会在物理上邻近，且处于相同分组的接入点间进行。

符合较空闲的接入点必须满足两个条件：

- 检测到无线客户端信号强度大于等于页面上配置的信号强度阈值；
- 邻居接入点上的接入人数减去该接入点上接入人数的差值大于页面上配置的接入人数差值。

比如： 邻居接入点上的接入人数为 10，页面上配置的接入人数差值为 3，则此时该接入点

上的接入人数应该小于等于 10-3=7。

动态负载引导(防终端粘滞)

动态负载引导功能是指终端距离接入点较远时，接入点主动使终端发生漫游，提高终端上网体验。即接入点检测到的终端的信号强度小于信号强度阈值，并且该终端的无线流量小于阈值流量时，接入点会使终端发生漫游。 仅使用 1 台 AP 时不建议启用该功能。

1、负载参数：只有负载参数同时满足时，优先接入 5.8G 频段和接入点间负载均衡才会被触发。

2、人数阈值：接入点上达到的在线用户数，建议取值为 10。

3、人数差值：用来决策可接入的邻居接入点，建议取值范围[1,5]。AP 部署密度较大时，取值越大体验越好；AP 部署密度较小时，取值越小体验越好。

4、信号强度阈值：用来决策参与负载均衡的邻居接入点， 建议取值范围[-90, -70]。AP 部署密度较大时，取较大值效果较好；AP 部署密度较小时，取较小值效果较好。

5、总信道利用率：用来决策参与负载均衡的接入点，建议取值范围为[60,90]，其中：总信道利用率=环境中的信道利用率+自身信道利用率。

6、弱终端参数：只有弱终端参数同时满足时，动态负载引导才会被触发。

7、智能射频：射频信号覆盖补偿，接入点异常/离线时，由邻居接入点自动放大功率进行信号覆盖

3.3.3.2. 无线漫游域

功能概述

1、主要解决的客户问题

（1）终端跨 VLAN 漫游时，偶尔会出现终端没有重新获取 IP 地址的情况，导致无法上网；

（2）终端跨设备跨 VLAN 漫游时，偶尔会出现终端没有重新获取 IP 地址的情况，导致无法上网。

2、给客户带来的价值

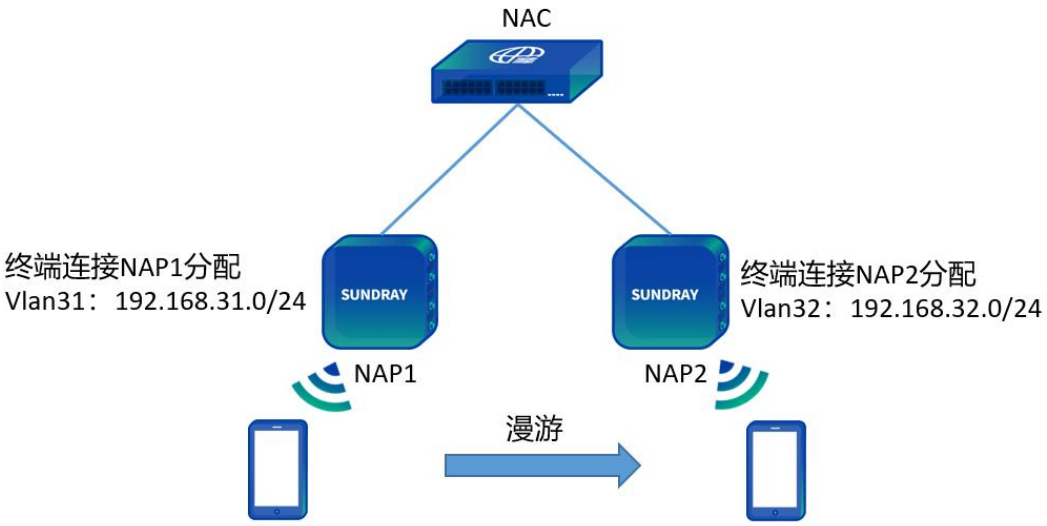
终端在跨 VLAN 漫游和跨设备漫游时，可以继续上网。

配置方法

控制器漫游域对集中转发生效。漫游域针对组网需要跨 VLAN 漫游的情况，如组网不涉及跨 VLAN 漫游，则无需使用控制器漫游域。

1、同控制器漫游：终端在同一台控制器上漫游

（1）存在如下集中转发的组网，为解决终端从接入点 1 漫游到接入点 2 能继续上网，漫游域配置如下。



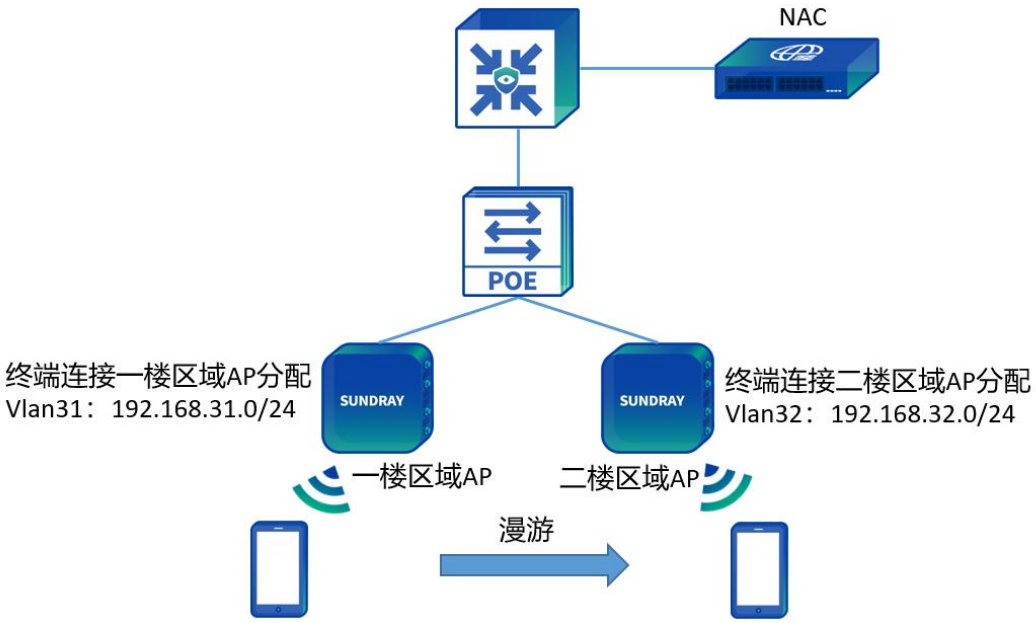
（2）控制器漫游域的 HA 网络是给终端分配的 VLAN 和 IP，将需要漫游的 IP 和 VLAN 写到一个漫游域中，终端连接无线网络 VLAN31 对应的地址段 192.168.31.0，VLAN32 对应的地址段为 192.168.32.0，归属则选择本控制器。

接入点漫游域配置方法

接入点漫游域对本地转发生效。漫游域针对组网需要跨 VLAN 漫游的情况，如组网不涉及跨 VLAN 漫游，则无需使用漫游域。

同控制器漫游

1.存在如下本地转发的组网，为解决终端从接入点 1 漫游到接入点 2 能继续上网，漫游域配置如下：

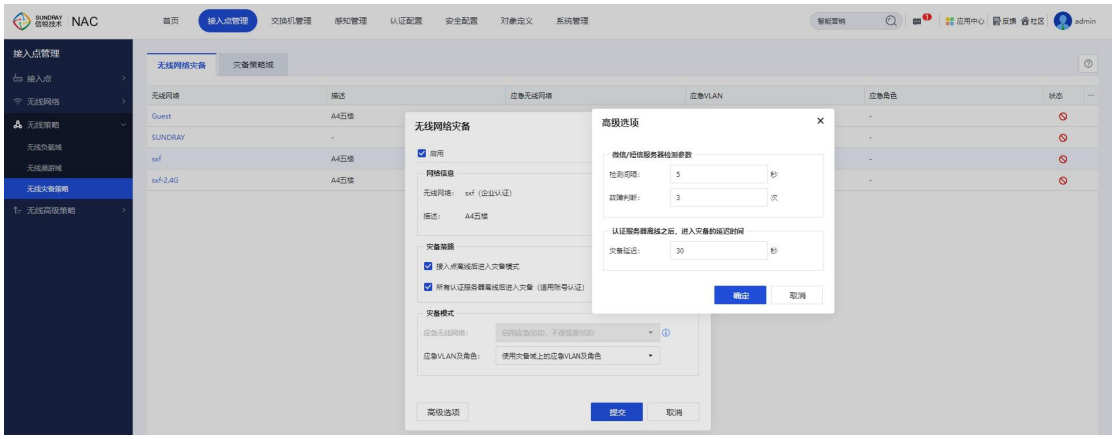


2.根据 VLAN 分配的地址配置接入点漫游域，将需要漫游的 IP 和 VLAN 配置在同一个漫游域中。终端连接一楼区域接入点分配 VLAN31 的地址段 192.168.31.0/24，终端连接二楼接入点分配 VLAN32 的地址 192.168.32.0/24。

3.3.3.3. 灾备策略

无线网络灾备

用于配置无线网络在接入点在无法连接 NAC、用户认证服务器、短信服务器或微信服务器进入灾备模式的时候，这个无线网络使用哪个应急无线网络、应急 VLAN 和角色。



高级选项

- 灾备延迟：是指认证服务器与控制器断开连接后，延迟多长时间生效灾备。
- 检测间隔：检测微信\短信服务器的间隔时间。
- 故障判断：检测到服务器连续故障多少次，才认为需要生效灾备。

灾备策略域

用于将无线接入点划分为不同的区域，配置这个区域下接入点进入灾备的条件和进入灾备后使用的应急 VLAN 和应急角色。

注意:

- 应急 VLAN 环境下必须存在 DHCP 服务器，否则终端无法获取到 IP 地址。
- 无线网络根据不同用户信息匹配不同用户 vlan，灾备模式下都会使用同一个灾备 VLAN。

3.3.4. 无线高级策略

3.3.4.1. 射频高级配置

当选择不同的国家码时，AP 可以工作的频率范围是不一样的，可以根据当地法律选择不同的国家码。

射频控制策略，可以选择 AP 信号发射信号时间，比如下班时间自动关闭 WIFI 射频信号，一定程度上可以提升安全性以及省电。

整网调优会根据算法优化 AP 的信道，通过错开相邻 AP 之间的信道，减小 AP 之间的干扰，从而优化用户的上网体验。

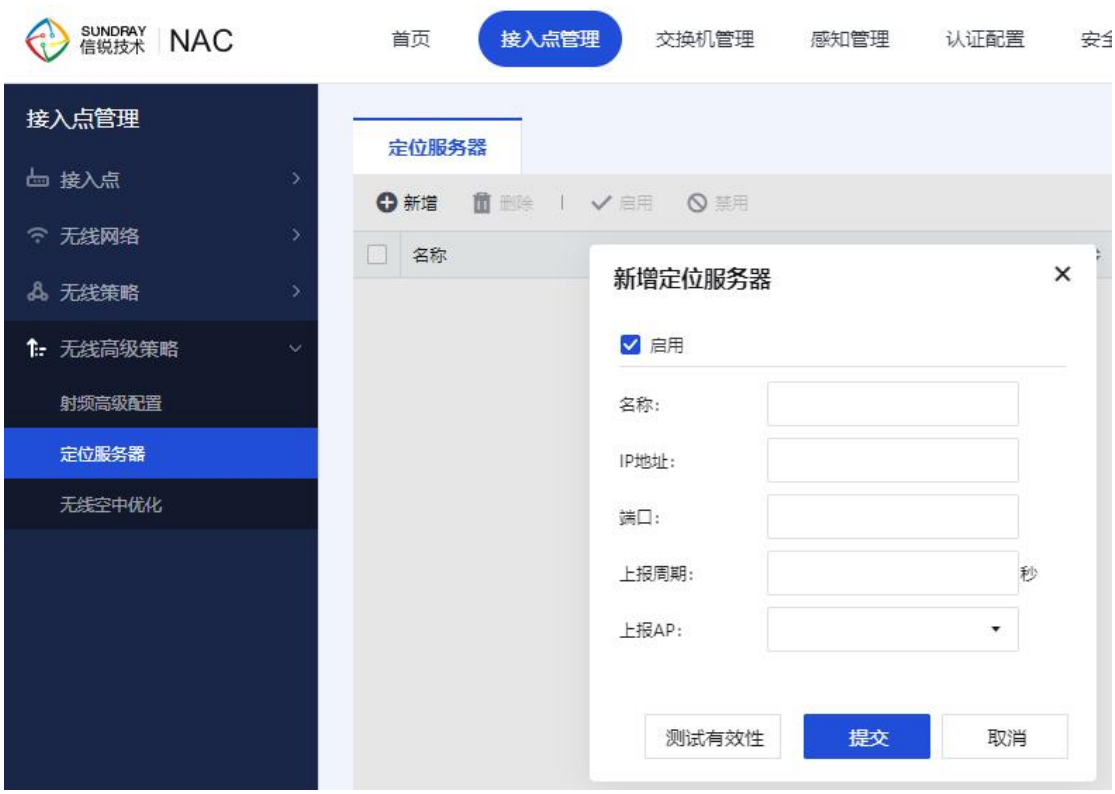
整网调优之后，2.4G 会调优至 1、6、11 信道上，5G 会调优至对应带宽所在的信道，调优之后 AP 的带宽保持不变。调优方法分为两种，分别是定时调优和立即调优。

定时调优可选择对应区域和生效对象，调优方式可分为两种：每天定时调优和每周定时调优。

立即调优可选择对应区域和生效对象，调优效果同定时调优。

3.3.4.2. 定位服务器

开放接口包括定位服务器，目前 NAC 做定位需要结合第三方定位厂商一起做定位，我们的无线仅提供底层信息数据支持。



针对自己拥有定位算法的客户，我们提供了定位所需的数据。

配置定位服务器，可以获取的信息：AP 的 MAC 地址、STA 的 MAC 地址、射频类型、无线信道、终端类型、是否关联上 AP、关联 AP 的 MAC 地址、信号强度 RSSI、底噪 noise floor 等。开启此功能需要开启定位服务器序列号。

3.3.4.3. 无线空中优化

射频提速功能可以减少无用的广播包转发至无线终端，增加无线的传输的稳定性，并有效的提高无线终端的数据传输效率。包含广播优化，电子书包优化功能。

启用用户间平均分配带宽:同一无线接入点上同一频段的所有无线终端用户之间带宽分配权重相同，当无线接入点传输带宽不足时，每个终端占用的无线时间保持基本一致；带宽足够时，用户带宽将不受此限制。建议关闭掉。

ARP 转单播：从有线测到无线终端的 ARP 广播包，在 NAC 和 AP 有记录的 ARP 对应表会转为单播，而不再采用广播数据，提高数据的传送效率

禁止 DHCP 请求发往无线终端：对于无线测的终端，默认是以上网类的 PC、平板、智能手机等终端，默认不包括 DHCP 服务器的，所以启用该功能可以有效抑制 DHCP 请求包发往无线终端测，提高传输效率。

禁止 ipv6 报文发往无线终端：目前绝大多数情况不使用 ipv6 协议，开启此开关可以减少空中的 ipv6 报文，优化无线网络环境。

禁止 mdns 发往无线终端：mdns 报文用于在没有传统 dns 服务器的情况下广播发现局域网内的主机。目前苹果系统的产品支持较多，如果要使用类似 Bonjour 这样的软件，请在使用的 vlan 不开启禁止功能。

禁止 nbns 发往无线终端：windows 系统的名称解析协议的数据包，在局域网内一般会大量存在，严重时会影响用户的上网数据传输。

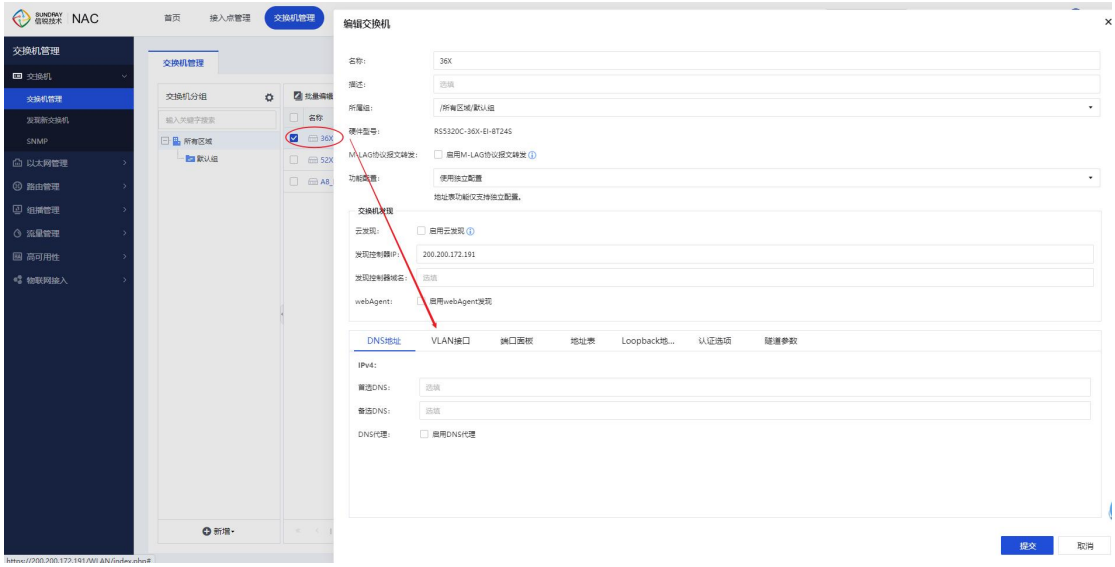
电子书包多播优化功能：对于默认的 802.11 协议中，对于广播数据是有一定速率限制的，为了适应新环境下的网络需求，有效且合理的提升了广播包的发送速率，增加了无线终端发送速率。

3.4. 交换机管理

3.4.1. 交换机

3.4.1.1. 交换机管理

对所有交换机进行全部集中分组和管理，包括配置所属组、发现网关 IP、发现网关域名、webAgent、DNS 地址、VLAN 接口、端口面板、地址表、Loopback 地址、认证选项、隧道参数。



所属组：配置交换机所属于的管理组，便于对交换机进行集中管理和配置。

网关 IP：填写交换机用于连接的 网关 IP 地址，如果给交换机填写了网关的地址，交换机下次重启后，会自动以该配置 IP 连接 NAC 并建立隧道。

发现网关域名：用于交换机自动发现网关用，当交换机解析到该域名时，交换机会自动向网关请求连接。网关发现该交换机后，就可以对该交换机进行策略下发配置了。

DNS 地址：如果启用了 DNS 代理，客户端的 DNS 服务器可以指向交换机。交换机接收到 DNS 请求后，会转发到这里设置的外部 DNS 服务器解析。

VLAN（Virtual Local Area Network）即虚拟局域网，是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信，而 VLAN 间不能直接互通，从而将广播报文限制在一个 VLAN 内。

通过配置 VLANIF 接口、子接口方式可以实现 VLAN 间的通信。

管理 VLAN 是指要通过 SSH、TELNET 访问交换机，需要将使用的交换机端口添加到管理 VLAN。

端口面板是以图形化的方式显示交换机的所有的端口，可以在这设置端口的端口属性。

VLAN 端口属性：

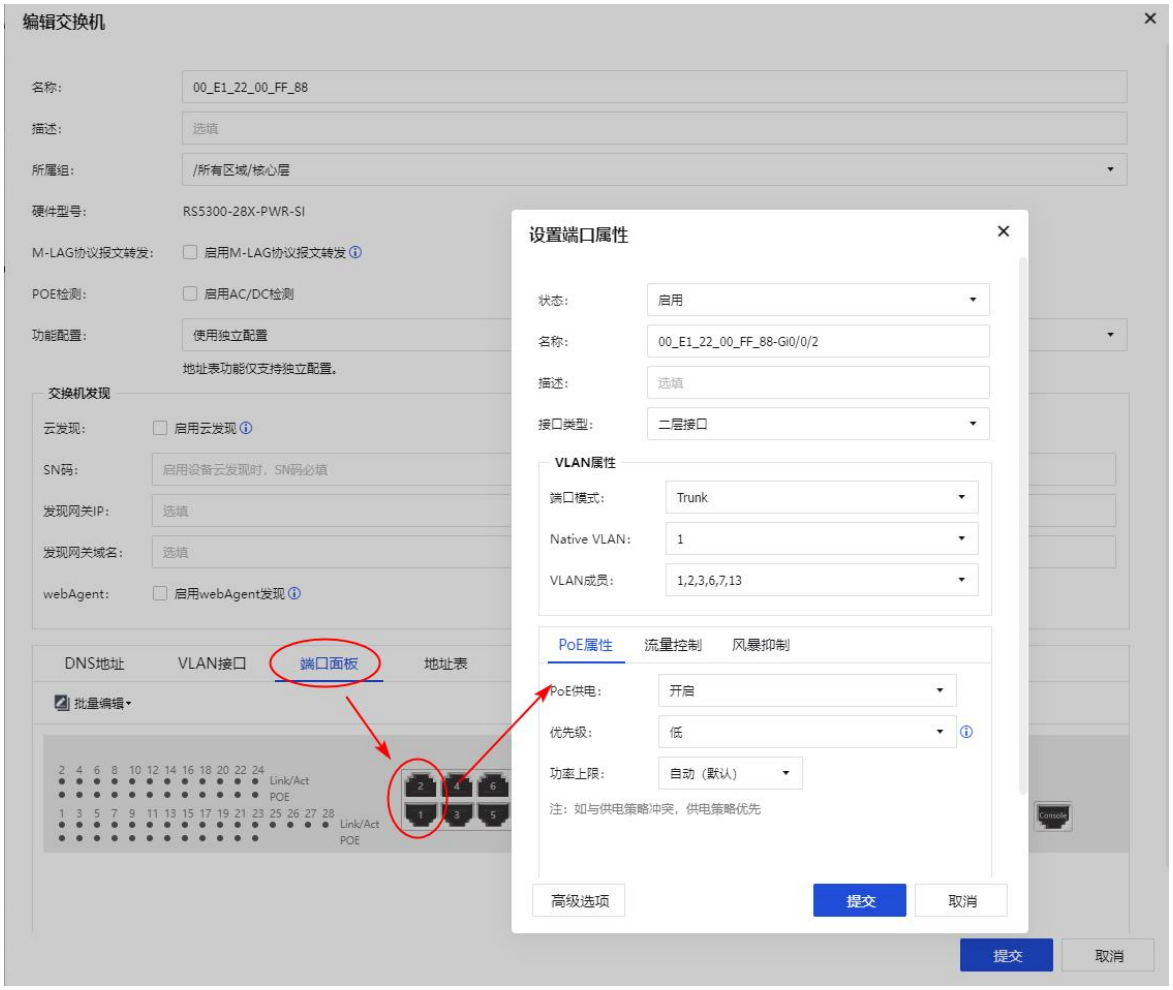
Access 只属于一个 VLAN，一般用于连接计算机端口。

Trunk 可以允许多个 vlan 通过，可以接收和发送多个 vlan 的报文，一般用于交换机之间的端口。

hybrid 接口：可以允许多个 vlan 通过，可以接收和发送多个 vlan 报文，一般用于交换机之间的端口，比 Trunk 属性多了 untaggedvlan 和 taggedvlan。

风暴抑制：风暴控制特性会不断地监控端口的入站流量，最高的频率为每秒进行一次监控，然后再把所获得的数据与配置在设备上的风暴抑制级别进行对比。风暴控制防止交换机的端口被局域网中的广播、多播或者一个物理端口上的单播风暴所破坏。

流量控制：如果发送者发送数据过快，接收者来不及接收，那么就会有分组丢失。为了避免分组丢失，控制发送者的发送速度，使得接收者来得及接收，这就是流量控制。流量控制根本目的是防止分组丢失，它是构成 TCP 可靠性的一方面。



配置静态 MAC 地址

设备通过源 MAC 地址学习自动建立 MAC 地址表时，无法区分合法用户和非法用户的报文，带来了安全隐患。为了提高安全性，网络管理员可手工在 MAC 地址表中加入特定 MAC 地址表项，将用户设备与接口绑定，从而防止非法用户骗取数据。

为了避免 MAC 地址表项爆炸式增长，可以手工配置动态 MAC 表项的老化时间。老化时间越短，路由器对周边的网络变化越敏感，适合在网络拓扑变化比较频繁的环境；老化时间越长，路由器对周边的网络变化越不敏感，适合在网络拓扑比较稳定的环境。

当需要配置的静态 MAC 表项较多，并且静态 MAC 表项中 MAC 地址与端口在同一二层环境时，可以采用自动扫描与绑定方式批量配置。

配置静态 ARP 地址

静态 ARP 表项不会被老化，不会被动态 ARP 表项覆盖，因此配置静态 ARP 表项可以增加通信的安全性。

当老化时间超时后，设备会清除动态 ARP 表项。此时如果设备转发 IP 报文匹配不到对应的 ARP 表项，则会重新生成动态 ARP 表项，如此循环重复。

用户可以通过手工方式或者自动扫描与绑定的方式配置静态 ARP 表项：当需要配置的静态 ARP 表项较少时，可以采用手工方式新增或删除；当需要配置的静态 ARP 表项较多，并且静态 ARP 表项中 IP 地址与 VLANIF 接口的 IP 地址在同一网段时，可以采用自动扫描与绑定方式批量配置。

Loopback 接口创建后除非手工关闭该接口，否则 Loopback 接口物理层状态和链路层协议永远处于 UP 状态，用户可通过配置 Loopback 接口达到提高网络可靠性的目的。

交换机支持认证功能，启用认证信息转发，即可通过深信服单点登录协议，实现网关与深信服上网行为管理等其他设备之间的单点登录，无需进行重复认证。交换机可限制认证用户上限

数，超出上限以后，新接入的终端会被加入黑名单，无法进行认证也无法上网。

交换机可通过二层隧道或三层隧道在网关激活上线，三层隧道在线的交换机功能正常，二层隧道在线的交换机只支持配置下发，不支持状态上报。

3.4.1.2. 发现新交换机

为了让控制器统一管理交换机，当交换机接入内网时，并未进入工作状态，需要管理员 在"发现新交换机"列表中，手动执行激活操作，交换机才能正常工作。

当交换机接入网络中，交换机会自动发现网关，当交换机第一次发现网关时，会在网关上看到新的交换机，需要进行激活后，才能正常使用交换机，并下发配置。

在 NAC 控制台的右上角，当有出现图标 时，表示还有未激活的交换机，需要到该页面激活。

当 NAC 上发现交换机时，需要激活，激活按钮可用。

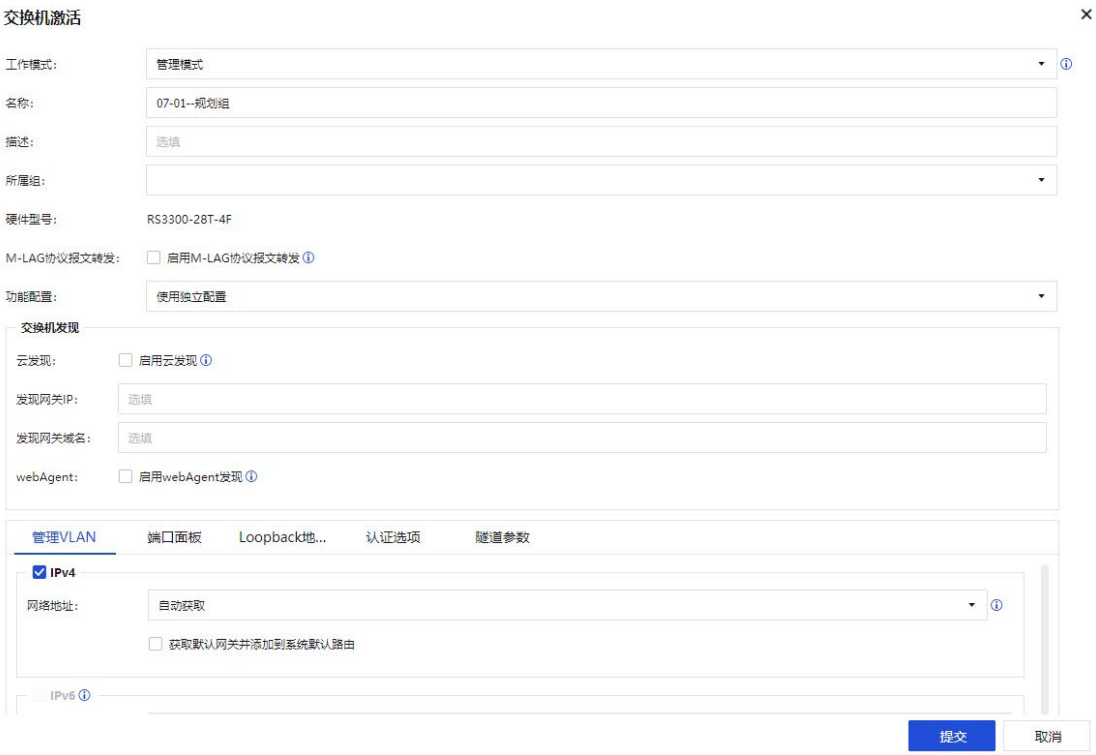
激活的时候，交换机只支持配置为普通模式，不支持网关模式。 交换机激活的时候，设备类型分为两种：

1. 射频交换机

射频交换机：激活的时候，交换机端口会默认添加射频交换机，射频交换机插到交换机端口上时，可以即插即用。

2. 普通交换机

普通交换机（除射频交换机外）：激活的时候，序列号字段为选填，但只有填写了序列号，才能在无线接入点页面添加射频交换机配置，这样射频交换机才能正常工作。点击激活后，配置界面如下：



可以编辑交换机的名称，地理位置，便于后续交换机的识别分组和管理，默认交换机以 其 MAC 地址为名称。

名称：编辑交换机名称，便于识别交换机。

描述：对交换机进行描述便于是被交换机。

所属组：配置交换机所属于的管理组，便于对交换机进行集中管理和配置。

发现网关 IP：填写交换机用于连接网关的 IP 地址，如果给交换机填写了网关的地址，交换机下次重启后，会自动以该配置 IP 连接网关并建立隧道。

发现网关域名：用于交换机自动发现网关用，当交换机解析到该域名时，交换机会自动向网关请求连接。网关发现该交换机后，就可以对该交换机进行策略下发配置了。

硬件型号：交换机的型号。

射频序列号:交换机序列号分为普通交换机序列号和射频交换机序列号。普通交换机序列号。

要添加射频交换机，需要给指定交换机开启序列号；射频交换机序列号给射频交换机专用，激活射频交换机没有超过序列号时，都会为射频交换机自动添加射频交换机，以达到即插即用的目的。

控制隧道保活时间：填写控制隧道保活时间，默认 12 秒，如果网络环境较差，可修改控制器隧道时间，降低交换机频繁上下线次数。

Webagent：发现控制器的一种方式，webagent 地址可联系 400-878-3389 进行申请开通。

网络地址：可以设置自动获取，也可以设置固定 IP 地址。如果设置的固定 IP 地址，与当前交换机获取到的 IP 地址不一致，配置生效下发后，有可能会导致交换机不能在当前网络上网，并使交换机与网关失去联系，所以一般设置交换机的 IP 地址为自动获取。

管理 VLAN 和管理端口：配置交换机的上联口以及管理 VLAN。管理 VLAN 是指要通过 SSH、TELNET 访问交换机，需要将使用的交换机端口添加到管理 VLAN。

3.4.1.3. SNMP 配置

SNMP 配置

SNMP(Simple Network Management Protocol,简单网络管理协议)，用于管理网络中上众多的软硬件平台。开启后可以通过 snmp 协议查询本设备系统信息，如设备型号，内存使用率，硬盘使用率，CPU 消耗等。

SNMP v1/v2：SNMP 的第一版本和第二版本。它们都是基于团体名进行报文认证。

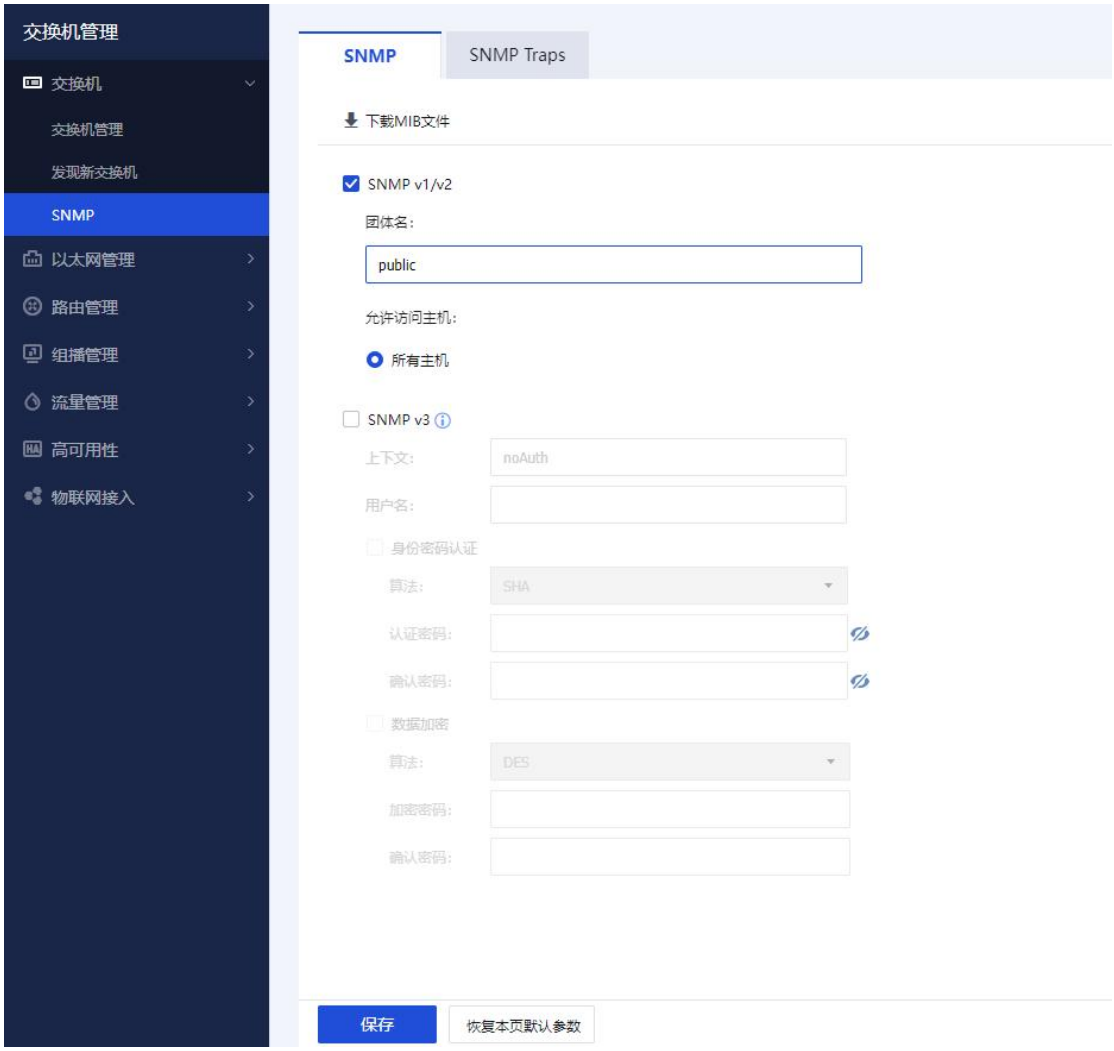
SNMP v3：SNMP 的第三版本。

此版本提供重要的安全性功能，其中就包括了认证和加密两项。

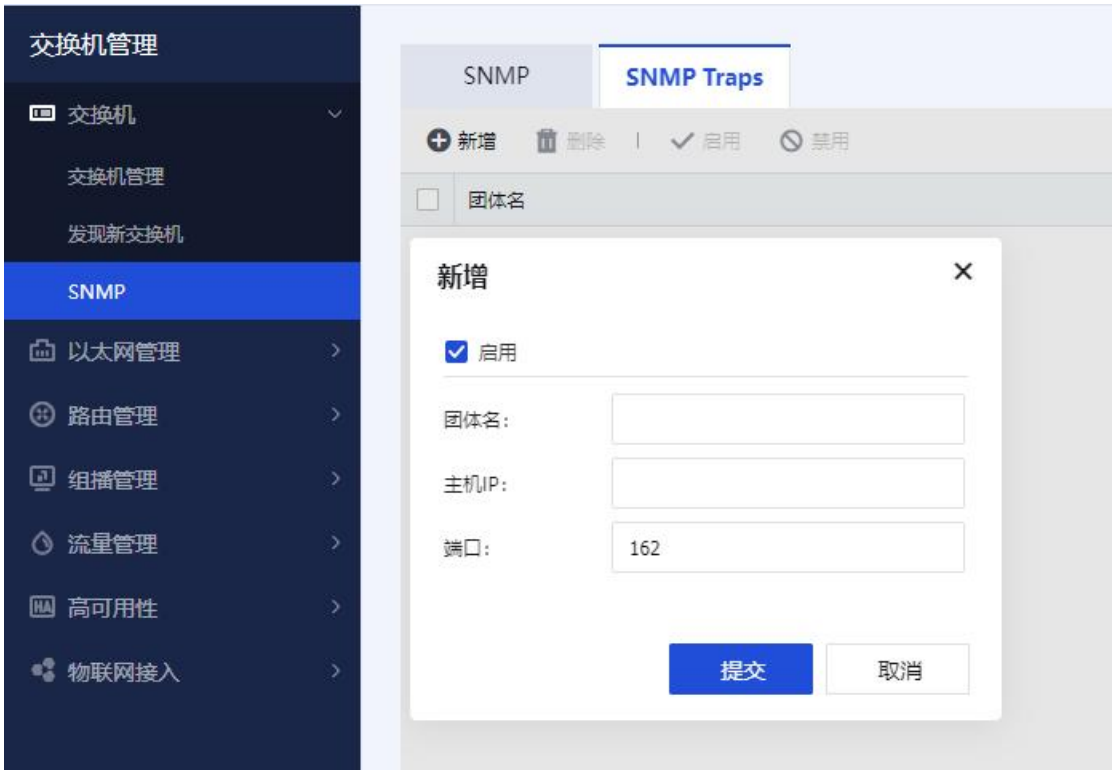
认证需要提供认证方式（MD5，SHA）和认证密码。

加密需要提供加密方式（DES）和加密密钥。

MIB（Management Information Base，管理信息库），是由网络管理协议访问的管理对象数据库，也可理解为是所有可管理对象的集合。下载本设备 MIB 后，再导入到相应的管理端后，可以管理或查询的本设备的一些基本信息，如设备型号，内存使用率，硬盘使用率，CPU 消耗等。



SNMP Trap 又称 SNMP 陷阱，启用后可以让本设备主动发送信息到管理端，而不需要等到管理端轮询后再发送。需要配置管理端的 IP 地址和端口，以及团体名。支持向多个管理端发送信息。



3.4.2. 以太网管理

包含【证书管理】和【安全网盾】两个模块。

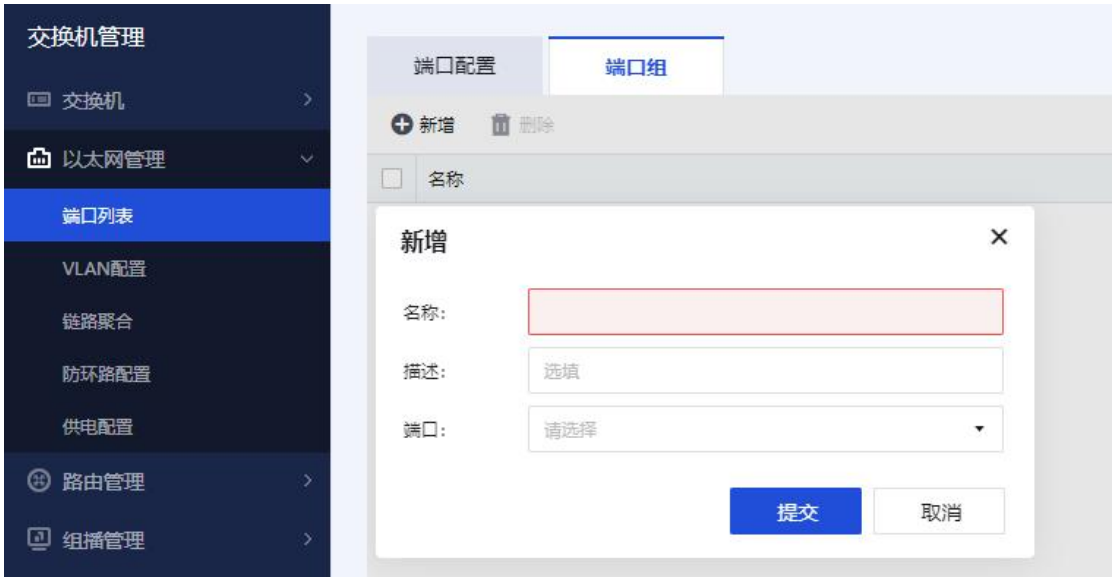
3.4.2.1. 端口列表

激活在当前网关（包括集中管理的分支）的交换机的所有端口列表，在此页面可以批量编辑所选端口的基本信息、PoE 属性、VLAN 属性，以达到方便管理操作的目的。

条件过滤：高级搜索可以过滤出指定的交换机或交换机分组，也可以根据端口模式、VLAN ID 来过滤端口。

PoE 供电重启：重启 PoE 芯片，使指定的端口停止 PoE 供电，然后重新供电。非受电设备不受影响。

端口组：端口组实现为多个接口批量配置命令的功能，减少单独配置的输入错误，同时节省人力。

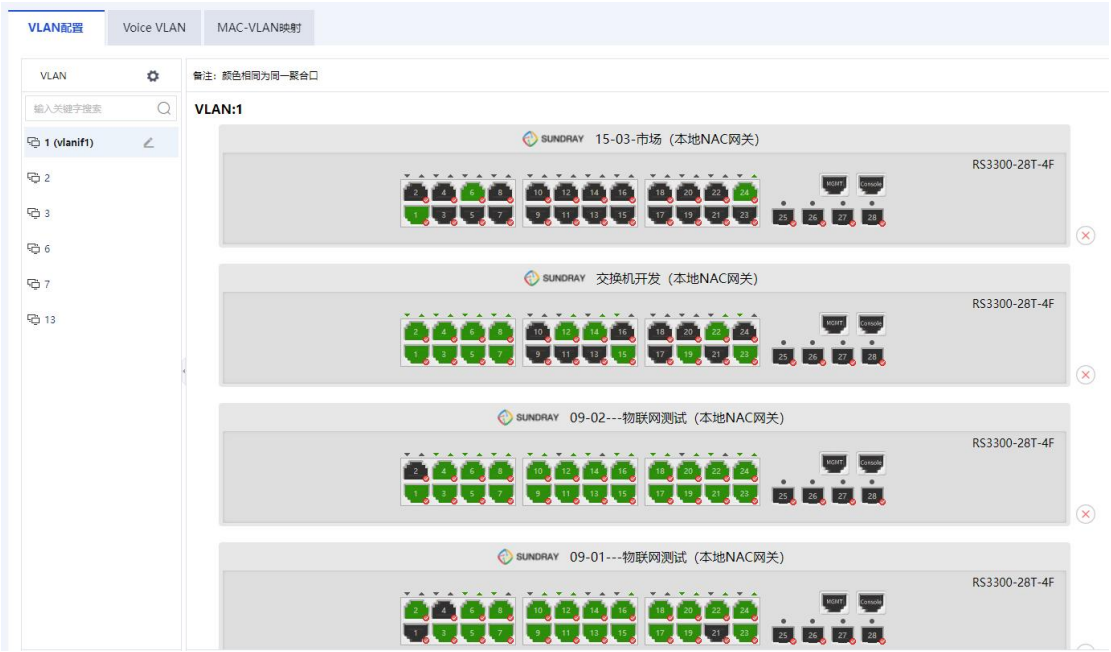


3.4.2.2. VLAN 配置

以全局、统一的视图来管理交换机和网关的 VLAN 配置。每个 VLAN 的视图中包括当前网

关以及分支的 VLAN-设备-端口三者的关系。功能适用于网络开局部署，统一规划 VLAN 配置，也适用于网络维护时，需要批量修改多台设备之间的 VLAN。

初始情况下，设备会默认添加 VLAN 1，交换机激活时，所有端口默认为 Access VLAN 1。

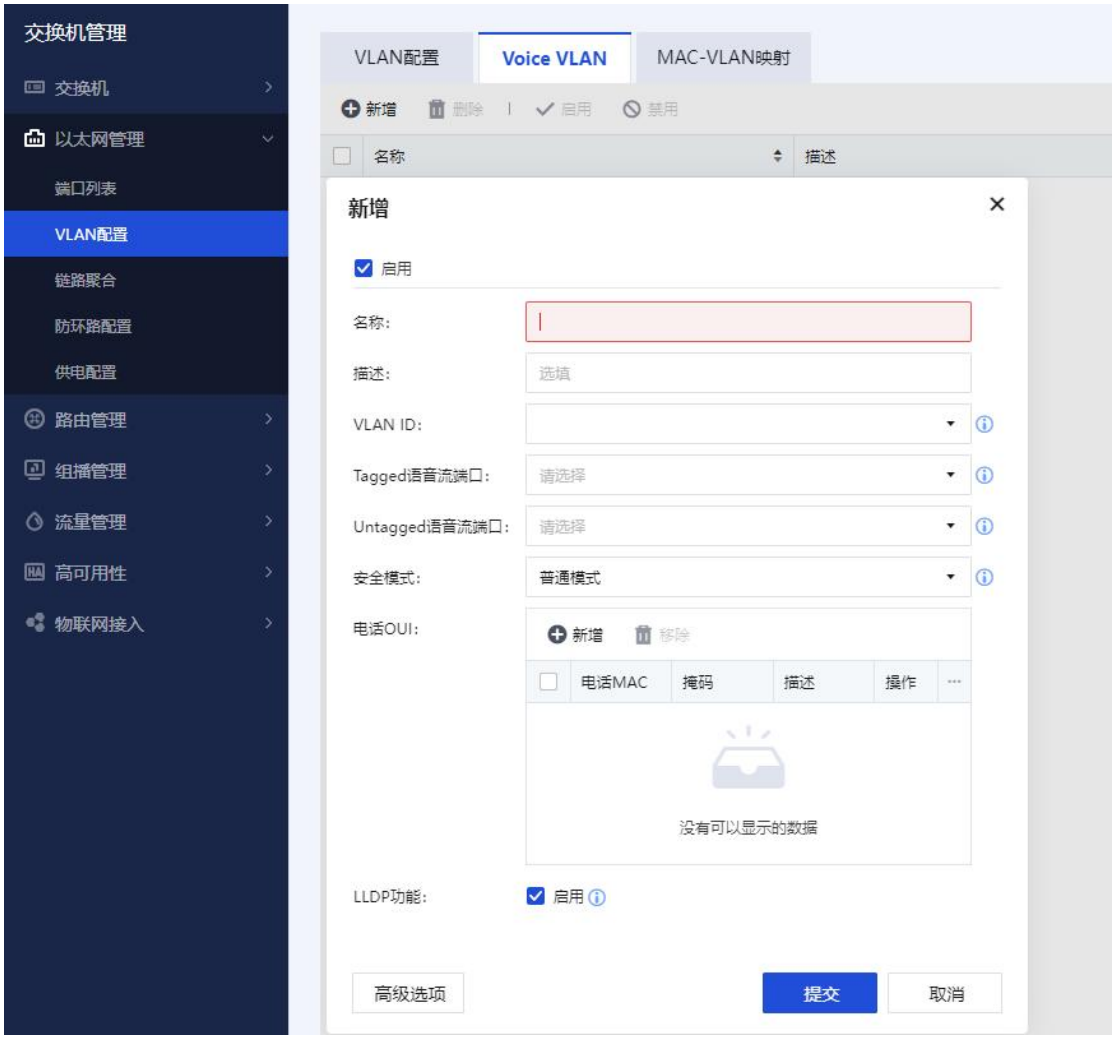


Voice VLAN

网络中经常有数据、语音、视频等多种流量同时传输。因为丢包和时延对通话质量的影响很大，用户对语音的质量比数据或者视频的质量更为敏感，因此在带宽有限的情况下就需要优先保证通话质量。

通过配置 Voice VLAN，交换机可识别语音流，对其进行有针对性的 QoS 保障，当网络发生拥塞时可以优先保证语音流的传输。

在电话通过 DHCP 获取 IP 的情况下，当电话开启 LLDP 功能接入时可以感知端口上 voice-vlan 变化，能够在 voice-vlan 发生变化时同步发起 DHCP 请求，获取新的 IP 地址；当电话不开启 LLDP 功能接入时无法感知端口上 voice-vlan 变化，需要等待 IP 地址租期到期时才会发送续租请求，进而获取新的 IP 地址。



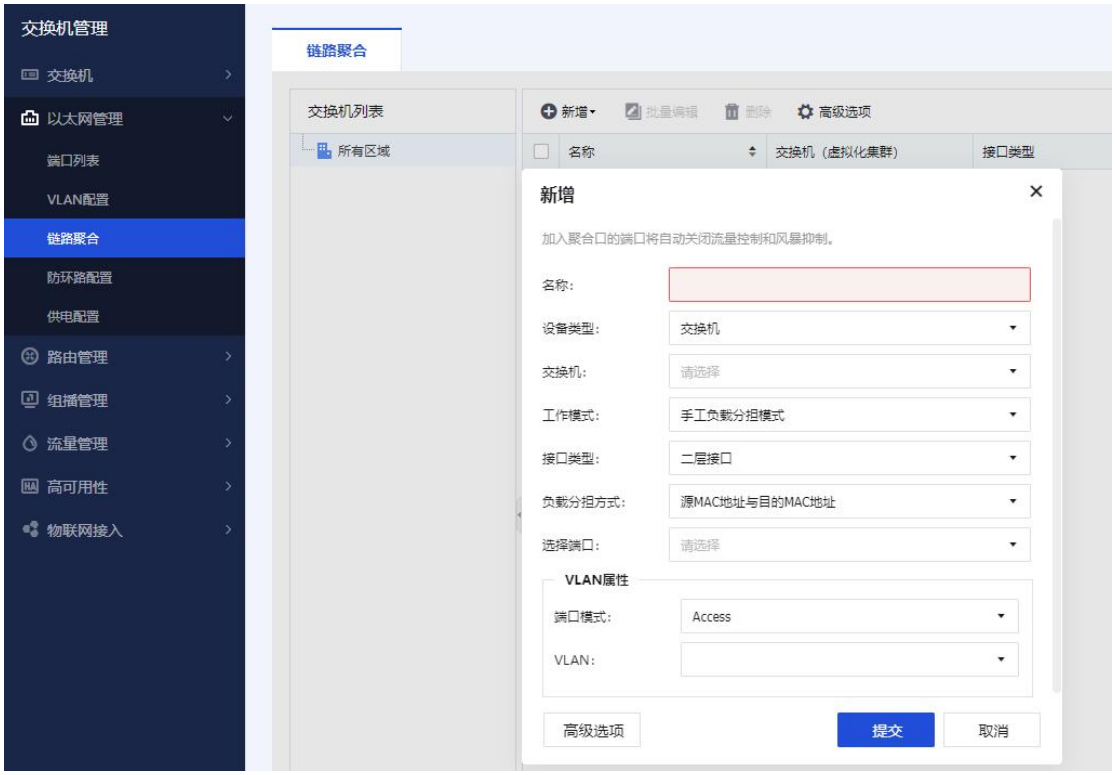
MAC-VLAN 映射

基于 MAC 地址划分 VLAN 不需要关注终端用户的物理位置，提高了终端用户的安全性和接入的灵活性。

MAC-VLAN 映射，其主要的功能是将用户报文中的私网 VLAN Tag 替换为公网的 VLAN Tag，使其按照公网的网络规划进行传输。在报文被发送到对端用户私网时，再按照同样的规则将 VLAN Tag 恢复为原有的用户私网 VLAN Tag，使报文正确到达目的地。

3.4.2.3. 链路聚合

链路聚合（Link Aggregation）是将多条物理链路捆绑在一起成为一条逻辑链路，从而实现增加带宽、提高可靠性、负载分担的目的。



设备类型

根据设备类型确定链路聚合的应用场景。设备类型选择为交换机时，指的是单个交换机上的普通链路聚合；设备类型选择为 M-LAG 组时，指的是部署 M-LAG 的两台设备与用户侧或者是网络侧设备之间的链路聚合。

工作模式

根据是否启用链路聚合控制协议 LACP，链路聚合分为手工负载分担模式和 LACP 模式。

手工负载分担模式下，Eth-Trunk 的建立、成员端口的加入由手工配置，没有链路聚合控制协议的参与。该模式下所有活动链路都参与数据的转发，平均分担流量，因此称为手工负载分担模式。

为了提高 Eth-Trunk 的容错性，并且能提供备份功能，保证成员链路的高可靠性，出现了链路聚合控制协议 LACP（Link Aggregation Control Protocol），LACP 模式就是采用

LACP 的一种链路聚合模式。

LACP 为交换数据的设备提供一种标准的协商方式，以供设备根据自身配置自动形成聚合链路并启动聚合链路收发数据。聚合链路形成以后，LACP 负责维护链路状态，在聚合条件发生变化时，自动调整或解散链路聚合。

接口类型

支持根据需要聚合的以太网接口类型来配置相应类型的聚合组：当需要聚合的是二层以太网接口时，需选择接口类型为二层接口；当需要聚合的是三层以太网接口时，需选择接口类型为三层接口。聚合链路的两端应配置相同的接口类型。

负载分担方式

二层链路聚合支持的负载分担方式有根据目的 MAC 地址、源 MAC 地址、源 MAC 与目的 MAC 地址、目的 IP 地址、源 IP 地址，源 IP 地址与目的 IP 地址六种方式。

三层链路聚合支持的负载分担方式有根据目的 IP 地址、源 IP 地址和源 IP 与目的 IP 地址三种方式。

系统 LACP 优先级

系统 LACP 优先级是为了区分两端设备优先级的高低而配置的参数。LACP 模式下，两端设备所选择的活动端口必须保持一致，否则链路聚合组就无法建立。此时可以使其中一端具有更高的优先级，另一端根据高优先级的一端来选择活动端口即可。系统 LACP 优先级值越小优先级越高。

端口 LACP 优先级

端口 LACP 优先级是为了区别同一个 Eth-Trunk 中不同接口被选为活动端口的优先程度，优先级高的接口将优先被选为活动接口。接口 LACP 优先级值越小，优先级越高。

LACP 报文工作模式

主动模式

聚合组处于主动模式，能够发送和接收 LACP 协议报文，用于协商聚合组状态。

被动模式

聚合组处于被动模式，只能接收 LACP 协议报文。

超时时间

超过超时时间，没有收到 LACP 协议报文，聚合组就无法建立。

缺省情况下，端口的 LACP 超时时间为长超时（即 30 秒），可配置端口的 LACP 超时时间为短超时（即 1 秒）。

3.4.2.4. 防环路配置

以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及 MAC 地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议 STP（Spanning Tree Protocol）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 IEEE 802.1D 中定义的 STP 到 IEEE 802.1W 中定义的快速生成树协议 RSTP（Rapid Spanning Tree Protocol），再到最新的 IEEE 802.1S 中定义的多生成树协议 MSTP（Multiple Spanning Tree Protocol）。

在生成树协议中，MSTP 兼容 RSTP、STP，RSTP 兼容 STP。

简单模式与高级模式

简单模式下，支持一键启用所有交换机的防环路功能，如有部分设备不需要开启防环路，可在排除列表中设置。

高级模式下，可以在策略列表中添加需要开启防环路功能的交换机，更多防环路参数请在策略中配置。

STP/RSTP 简介

STP 是一个用于局域网中消除环路的协议。运行该协议的设备通过彼此交互信息而发现网络中的环路，并适当对某些端口进行阻塞以消除环路。由于局域网规模的不断增长，生成树协议已经成为了当前最重要的局域网协议之一。

IEEE 于 2001 年发布的 802.1w 标准定义了快速生成树协议 RSTP（Rapid Spanning Tree Protocol），该协议基于 STP 协议，对原有的 STP 协议进行了更加细致的修改和补充。

MSTP 基本原理

MSTP 协议在计算生成树时使用的算法和原理与 STP/RSTP 大同小异，只是因为在 MSTP 中引入了域和内部路径开销等参数，故 MSTP 中的优先级向量是 7 维，而 STP/RSTP 是 5 维。STP/RSTP 中的优先级向量是{根桥标识符,根路径开销,桥标识符，发送 BPDU 报文端口标识符，接收 BPDU 报文端口标识符},MSTP 中的优先级向量是{CIST 根桥标识符,CIST 外部根路径开销，CIST 域根标识符,CIST 内部根路径开销，CIST 指定桥标识符，CIST 指定

端口标识符，CIST 接收端口标识符}，其中 STP/RSTP 中的桥标识符实际上是发送 BPDU 的设备的标识符，与 MSTP 中的 CIST 指定桥标识符对应。MSTP 中的 CIST 域根标识符有两种情况，一种是总根所在域内，BPDU 报文中该字段是参考总根的标识符，另一种情况是不包含总根的域中，BPDU 报文该字段是参考主设备的标识符。运行 MSTP 的实体初始化时认为自己是总根、域根，通过交互配置消息，按照上面介绍的 7 维向量计算 CIST 生成树和 MSTI。

MST 域

MST 域即多生成树域，是由交换网络中的多台交换设备以及它们之间的网段所构成。这些交换设备启动 MSTP 后，具有相同域名、相同 VLAN 到生成树映射配置和相同 MSTP 修订级别配置，并且物理上直接相连。一个交换网络可以存在多个 MST 域，用户可以通过 MSTP 配置命令把多台交换设备划分在同一个 MST 域内。

端口参数

边缘端口：用户如果将某个端口指定为边缘端口，那么当该端口由 Block 状态向 Forward 状态迁移时，这个端口可以实现快速迁移，而无需等待延迟时间。

BPDU 过滤：通过使用 BPDU 过滤功能，将能够防止交换机在启用了边缘端口特性的接口上发送 BPDU。对于配置了边缘端口特性的端口，它通常连接到主机 设备，因为主机不需要参与 STP，所以它将丢弃所接收到的 BPDU。通过使用 BPDU 过滤功能，将能够防止向主机设备发送不必要的 BPDU。

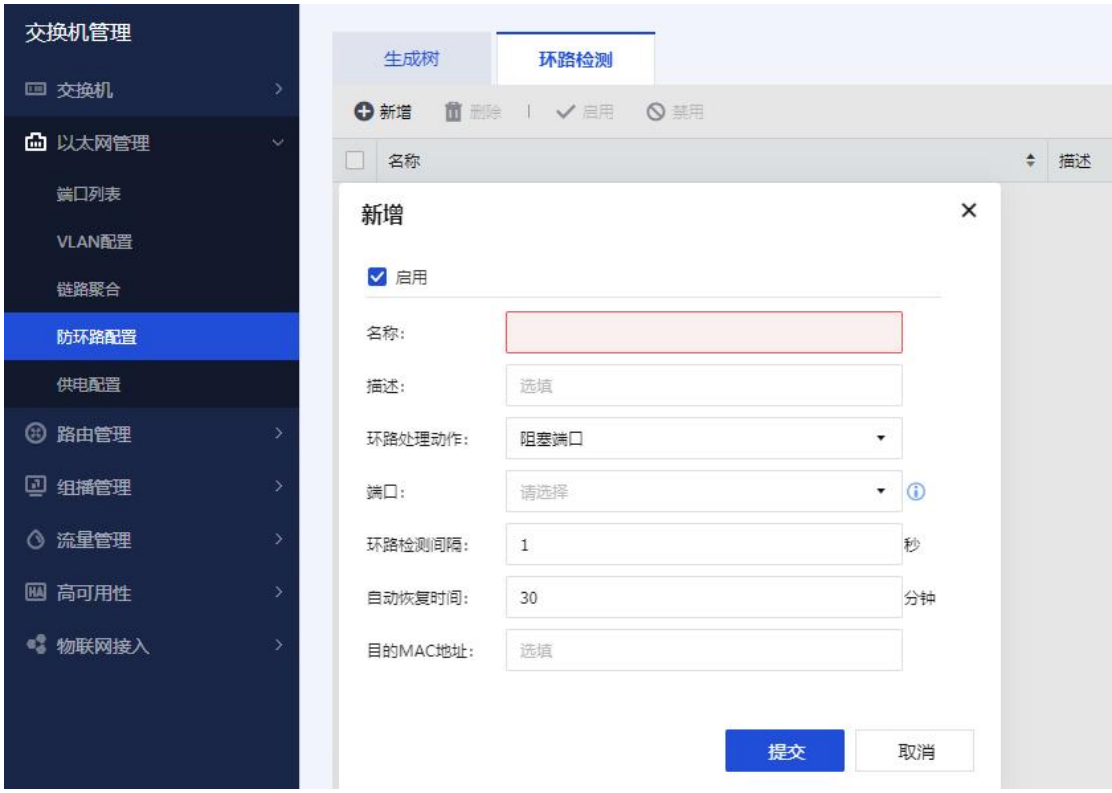
BPDU 保护：与用户设备直接相连边缘端口，收到恶意攻击 BPDU 报文时，边缘端口属性丢失变为非边缘端口，引起整网拓扑重新计算，导致网络振荡。

根保护：避免协议报文恶意攻击导致网络中合法根设备收到优先级更高的 BPDU 报文，使合法根设备失去根设备地位，从而引起网络拓扑结构的错误变动。

环路保护：在启动了环路保护功能后，如果根端口或 Alternate 端口长时间收不到来自上

游的 RST BPDU，则向网管发出通知信息（如果是根端口则进入 Discarding 状态）。而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。直到根端口收到 RST BPDU，端口状态才恢复正常到 Forwarding 状态。

环路检测机制可发现某个端口下的环路，并通知用户检查网络连接和配置情况，以避免对整个网络造成严重影响。



环路处理动作：环路处理动作是指发现二层网络中的环路以后所采取的处理方式，常用方式包括阻塞端口、关闭端口、退出环路 vlan。

环路检测间隔：环路检测间隔是环路检测报文的发送时间间隔，通过环路检测报文来确定各端口是否出现环路、以及存在环路的端口上是否已消除环路等。

自动恢复时间：当设备检测到某端口出现环路后，若在一定环路检测时间间隔内仍未收到环路检测报文，就认为该端口上的环路已消除，自动将该端口恢复为正常转发状态。

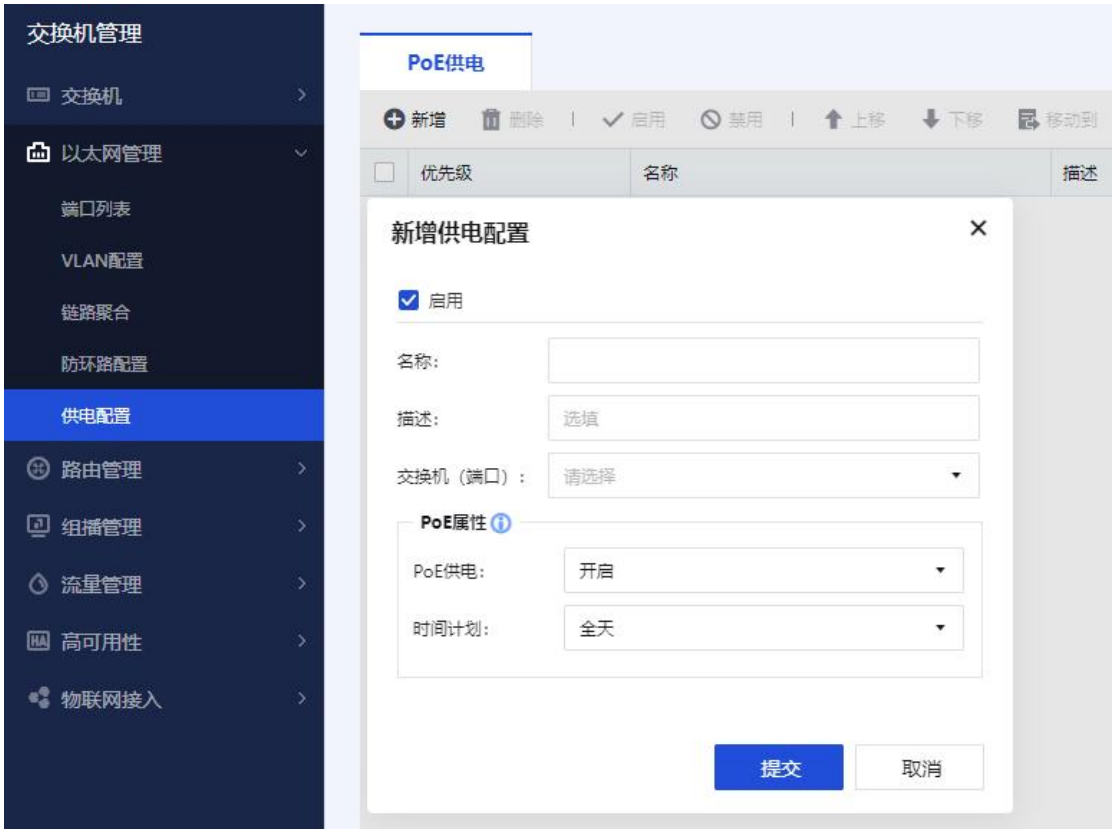
目的 MAC 地址：环路检测报文的目的 MAC 地址默认为广播地址，用户可根据实际需要进行配置。

3.4.2.5. 供电配置

供电配置管理功能可以配置 PoE 交换机的供电属性，也可以配置时间计划给交换机的端口，以实现统一管理、科学省电的需求。

交换机和网关断开一定时间之后（5 分钟），所有端口会保持供电状态。

未激活的 PoE 交换机，所有端口会保持供电状态。



3.4.3. 路由管理

3.4.3.1. 静态路由

静态路由是一种需要管理员手工配置的特殊路由。

当网络结构比较简单时，只需配置静态路由就可以使网络正常工作；在复杂网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽。

IPv4 静态路由

在创建静态路由时，可以同时指定目标地址和下一跳地址。

支持创建静态路由时，启用链路检测，包括 BFD 检测与 PING 检查，配置链路检测可见高可用性-链路检测。

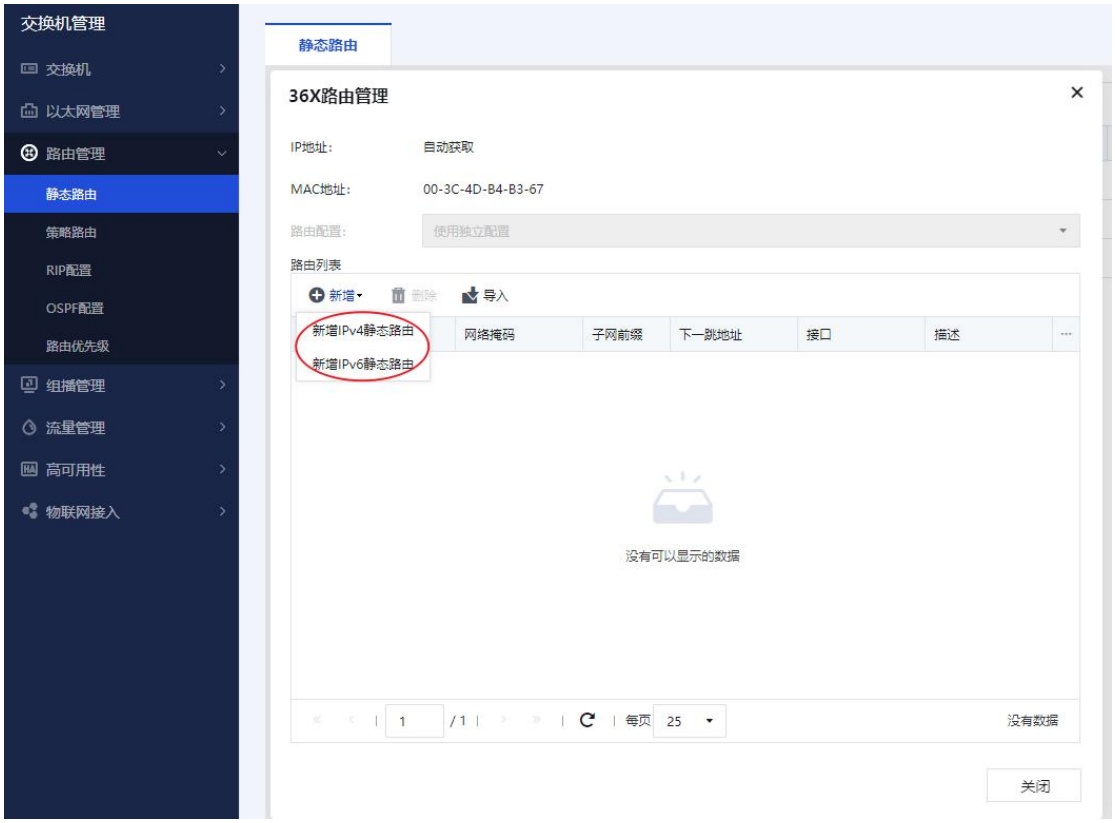
在创建相同目的地址的多条静态路由时，支持创建静态路由时，启用链路检测并备份配置备份链路，实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。

IPv6 静态路由

在创建 IPv6 静态路由时，可以同时指定目的地址和下一跳地址。

在创建 IPv6 静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv6 静态缺省路由。缺省情况下，没有创建 IPv6 静态缺省路由。



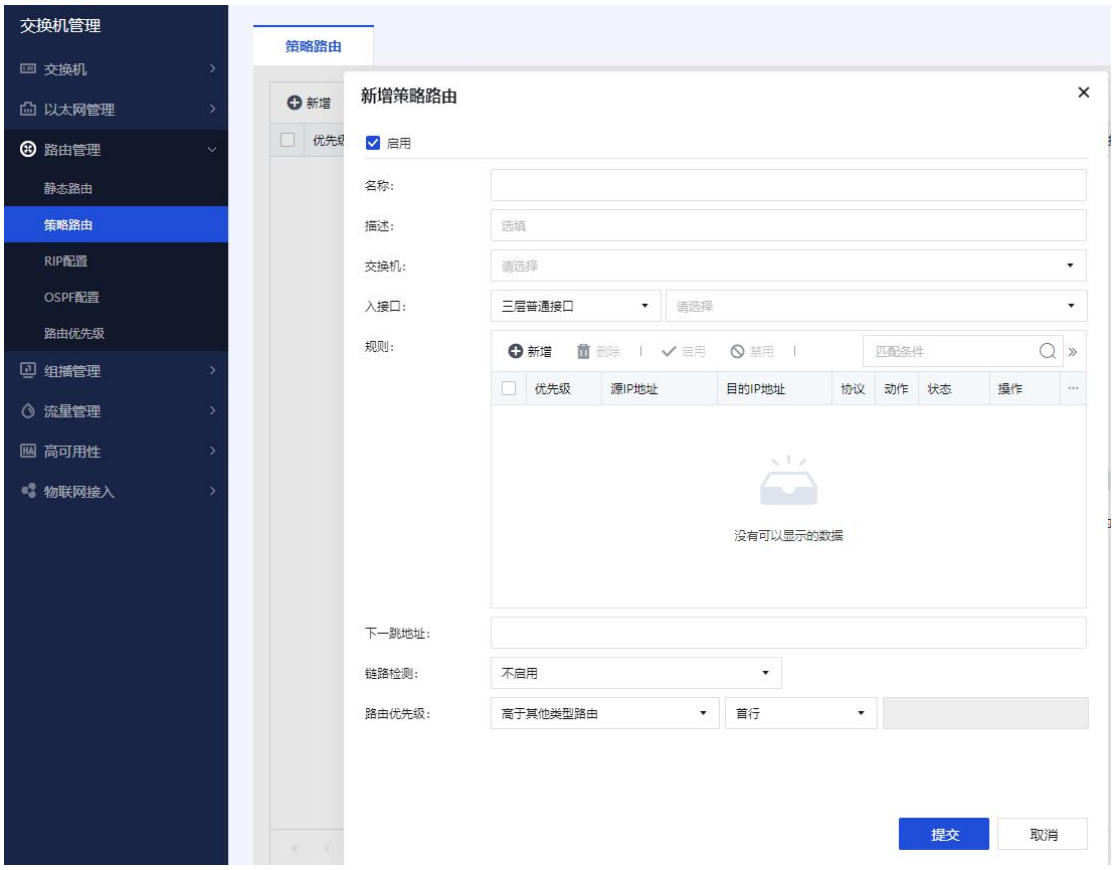
3.4.3.2. 策略路由

策略路由是一种依据用户制定的策略进行路由选择的机制。设备配置策略路由后，若接收的报文（包括二层报文）匹配策略路由的规则，则按照规则转发；若匹配失败，则根据目的地址按照正常转发流程转发。

支持使用 ACL 作为策略路由的分类规则，配置相应的 ACL 实现可以使不同的数据流通过不同的链路进行发送，提高链路的利用效率。

通过配置策略路由与链路检测联动可以为策略路由提供检测机制，配置完以后，当重定向下一跳对应的链路发生故障的时候，重定向下一跳会因为链路检测失败而立即失效，而不需要等待 ARP 表项老化。这样就可以达到缩短通信中断时间，提高服务质量的目的。

支持通过配置策略路由的优先级实现路由选择的优先顺序。



3.4.3.3. RIP 配置

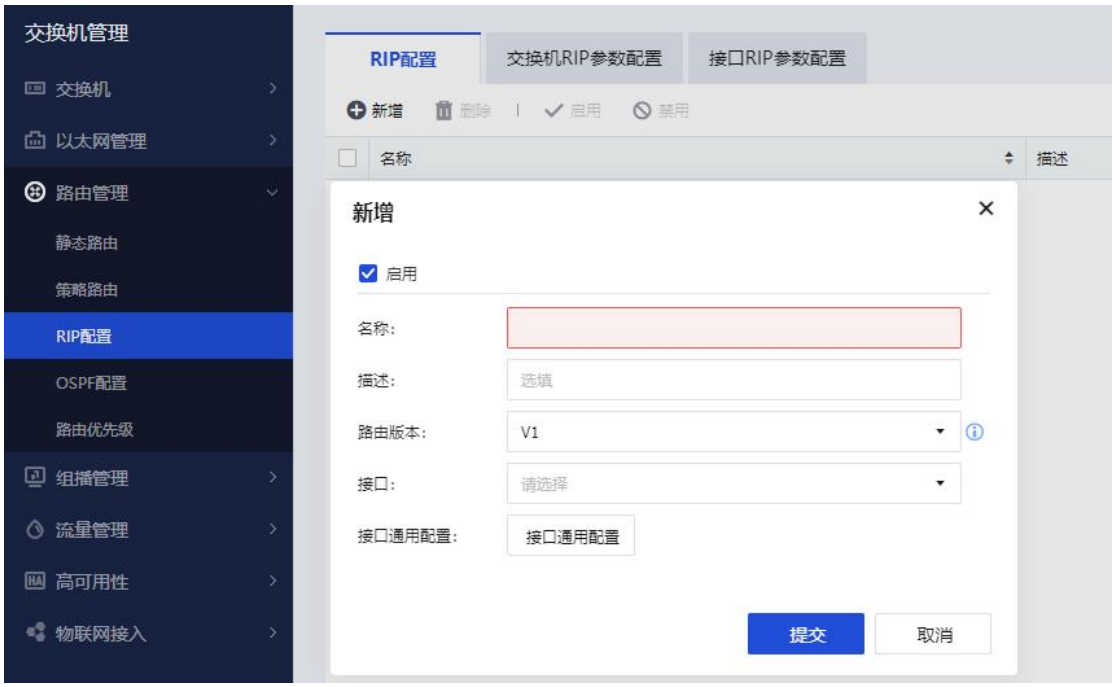
RIP 配置

RIP 路由 V1 版本是有类别路由协议，它只支持以广播方式发布协议报文，且协议报文中没有携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 无法支持路由聚合，也不支持不连续子网。

RIP 路由 V2 版本是一种无分类路由协议，支持外部路由标记，可以在路由策略中根据 Tag 对路由进行灵活的控制。支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

在创建相同目的地址的多条静态路由时，支持创建静态路由时，启用链路检测并备份配置备份链路，实现路由备份。

在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。



交换机 RIP 参数配置

在规模比较大的网络中，可能会结合区域设备的特点，配置不同的路由协议。为了实现 RIP 区域与其他路由区域之间的同心，需要在设备上配置引入非本协议的路由信息，包括默认路由，直连路由，静态路由，OSPF 路由。

接口 RIP 参数配置

认证方式：RIP 路由 V2 版本提供了报文认证机制来满足网络安全性的要求。支持的认证方式，包含明文认证与 MD5 认证。明文认证：将配置的密码直接加入报文中，这种加密方式安全性较其他两种方式低。MD5 认证：通过将配置的密码进行 MD5 算法之后再加入报文中，这样提高了密码的安全性。

防止路由环路：支持启用水平分割或毒性反转。水平分割 RIP 从某个接口学到的路由，不

会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由环路。毒性逆转 RIP 从某个接口学到路由后，将该路由的开销设置为 16（即指明该路由不可达），并从原接口发回邻居路由器。利用这种方式，可以清除对方路由表中的无用路由。

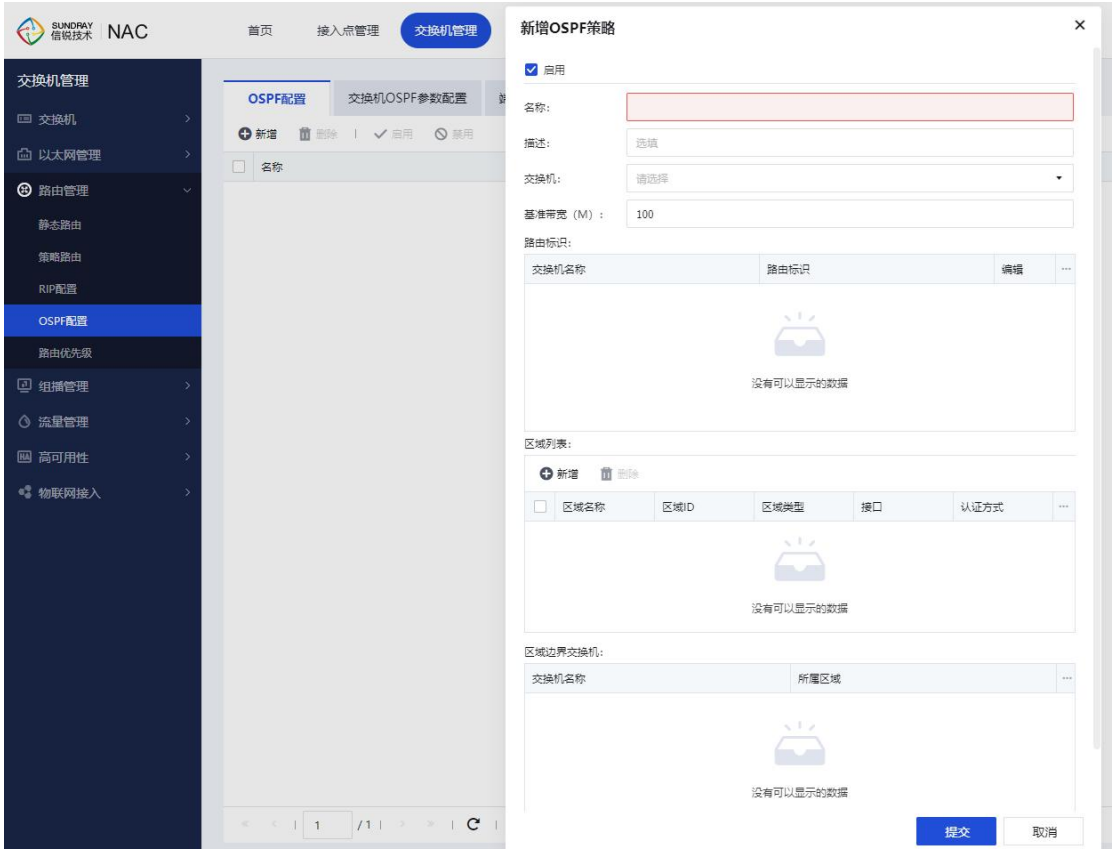
RIP 更新报文：勾选允许发送 RIP 更新报文后，当路由信息发生变化时，立即向邻居路由器发送触发更新报文，通知变化的路由信息。触发更新可以缩短网络收敛时间，在路由表项变化时立即向其他路由器广播该信息，而不必等待定时更新。

BFD 检测：接口 RIP 的 BFD 检测可以快速感知链路故障，实现 RIP 网络的快速收敛，用来提高 RIP 网络的可靠性,用于对可靠性要求较高的网络。

附加度量值：附加路由度量值是在 RIP 路由原来度量值的基础上所增加的度量值（跳数）。

3.4.3.4. OSPF 配置

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF（Internet Engineering Task Force，互联网工程任务组）组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2。



OSPF 配置

区域列表：

可编辑区域名称，配置区域 ID，区域类型，添加接口及配置认证方式；区域有骨干区域、普通区域、Stub 区域、Talloy Stub 区域、NSSA 区域和 Totally NSSA 区域，其中骨干区域区域 ID 只能为 0，其它区域为非 0。

虚连接：

虚连接是指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。它的两端必须是 ABR，而且必须在两端同时配置方可生效。

认证：

建立邻居关系时，在发送的报文中会携带配置好的口令，接收报文时进行密码验证。如果区域验证和接口验证都进行了配置，以接口验证的配置为准。认证方式有两种，分别为明文密码认证以及 MD5 认证，一个区域中所有交换机的验证模式和验证密码或者邻居交换机两端接口必须一致，否则无法认证。

边界交换机：

多区域连接时，区域与区域间的边界交换机会在此处显示 ；可对边界交换机配置路由白名单，用户可根据自身情况设置入、出方向的域间路由设置过滤条件；路由聚合是指 ABR 将具有相同前缀的域间路由信息聚合，只发布一条路由到其它区域。

交换机 OSPF 参数配置：

可对已加入 OSPF 中的交换机进行配置，实现路由引入。

用户可配置所引入路由的类型，度量值和标签，同时也可以配置引入规则，实现对引入路由的过滤。

缺省路由度量值：

针对特殊区域的 ABR 产生的默认路由配置度量值。

端口 OSPF 参数配置：

可配置已加入 OSPF 的接口参数，如 DR 选举优先级，接口开销，认证方式。

接口开销：

OSPF 基于接口带宽计算开销，计算公式为：接口开销=带宽参考值÷带宽。带宽参考值可配置，缺省为 100Mbit/s。因此，一个百兆接口的开销为 1，一个千兆接口的开销为 0.1，取整为 1。

BFD（Bidirectional Forwarding Detection，双向转发检测）：

为 OSPF 邻居之间的链路提供快速检测功能。当邻居之间的链路出现故障时，加快 OSPF 协议的收敛速度。

高级选项：

可开启 DD 报文检测及 OSPF 报文抑制；定时器可配置 OSPF 的时间参数，接口定时器 Hello 和失效间隔需与对端一致，否则邻居关系将无法建立。

报文抑制：

接口开启报文抑制，则抑制接口发送 OSPF 报文，则会导致邻居建立失败，可避免伪冒设备接入 OSPF 域中。

Hello 间隔：

接口向邻居发送 Hello 报文的时间间隔，OSPF 邻居之间的 Hello 定时器的值要保持一致。

失效间隔：

在邻居失效时间内，如果接口还没有收到邻居发送的 Hello 报文，路由器就会宣告该邻居无效。

重传间隔：

交换机向它的邻居通告一条 LSA 后，需要对方进行确认。若在重传间隔时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。

传输时延：

LSA 在本设备的链路状态数据库（LSDB）中会随时间老化（每秒钟加 1），但在网络的传输过程中却不会，所以有必要在发送之前在 LSA 的老化时间上增加本命令所设置的一段时间。此配置对低速率的网络尤其重要。

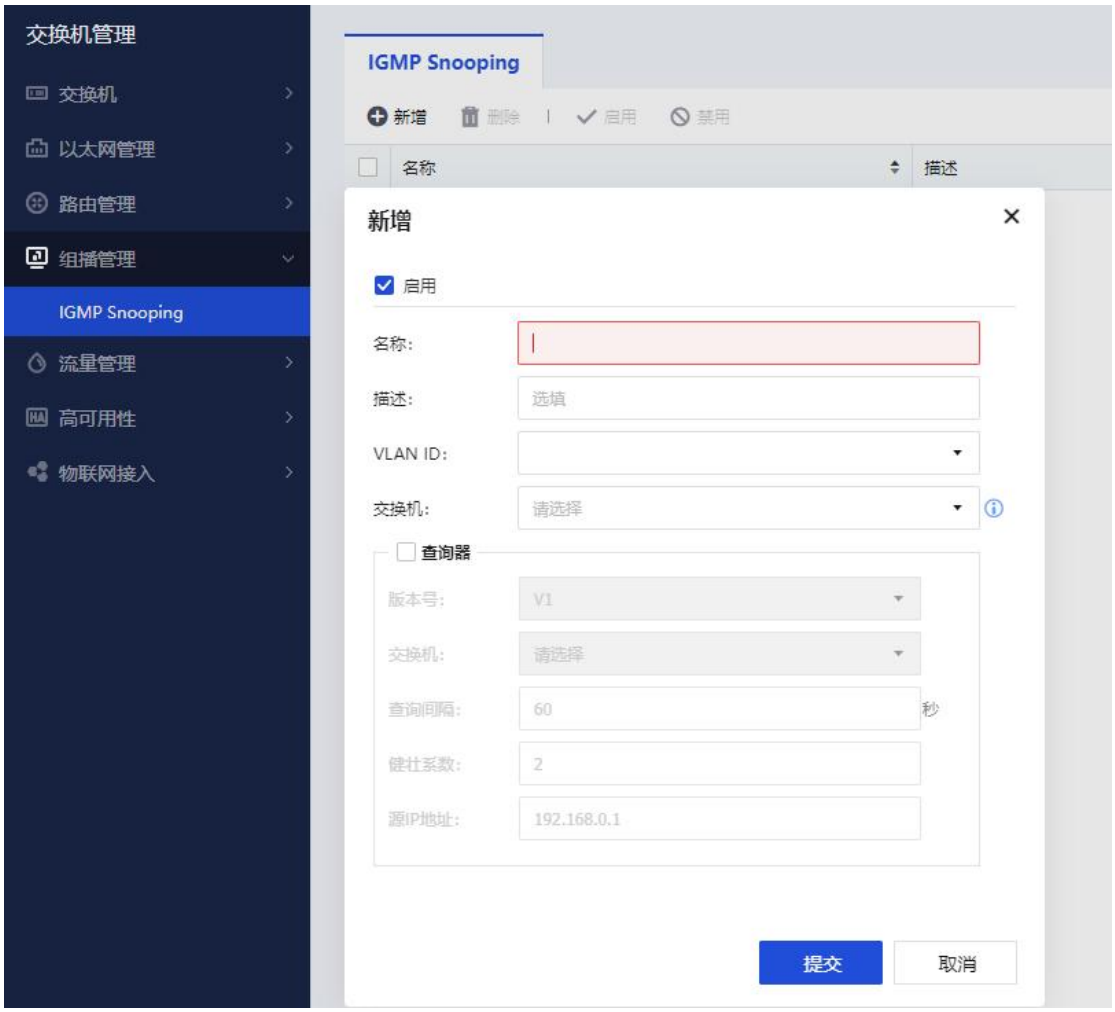
3.4.3.5. 路由优先级

对于相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但这些路由并不都是最优的。事实上，在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。为了判断最优路由，各路由协议（包括静态路由）都被赋予了一个优先级，当存在多个路由信息源时，具有较高优先级（取值较小）的路由协议发现的路由将成为最优路由，并将最优路由放入本地路由表中。

支持手工为各路由协议配置的优先级包含静态路由优先级，RIP 协议优先级和 OSPF 协议优先级。

3.4.4. 组播管理

IGMP Snooping 即组播侦听功能，可以实现组播数据在数据链路层的转发和控制。当主机和上游三层设备之间传递的 IGMP 协议报文通过二层组播设备时，IGMP Snooping 分析报文携带的信息，根据这些信息建立和维护二层组播转发表，从而指导组播数据在数据链路层按需转发，减少二层网络中的广播报文，节约网络带宽，增强组播信息的安全性。



版本号:

IGMPv1 主要基于查询和响应机制来完成对组播组成员的管理。与 IGMPv1 相比，IGMPv2 增加了查询器选举机制和离开组机制。IGMPv3 在兼容和继承 IGMPv1 和 IGMPv2 的基础上，进一步增强了主机的控制能力，并增强了查询和报告报文的功能。

查询间隔:

查询间隔是指查询者发送普遍组查询报文之间的时间间隔。普遍组查询报文用于向与其连接的所有子网进行轮询来发现是否有组员存在。

健壮系数：

查询器的健壮系数是为了弥补可能发生的网络丢包而设置的报文重传次数。

源 IP 地址：

用户可根据实际需要配置查询器的源 IP 地址，从而建立数据链路层组播转发表项，进行组播数据转发。

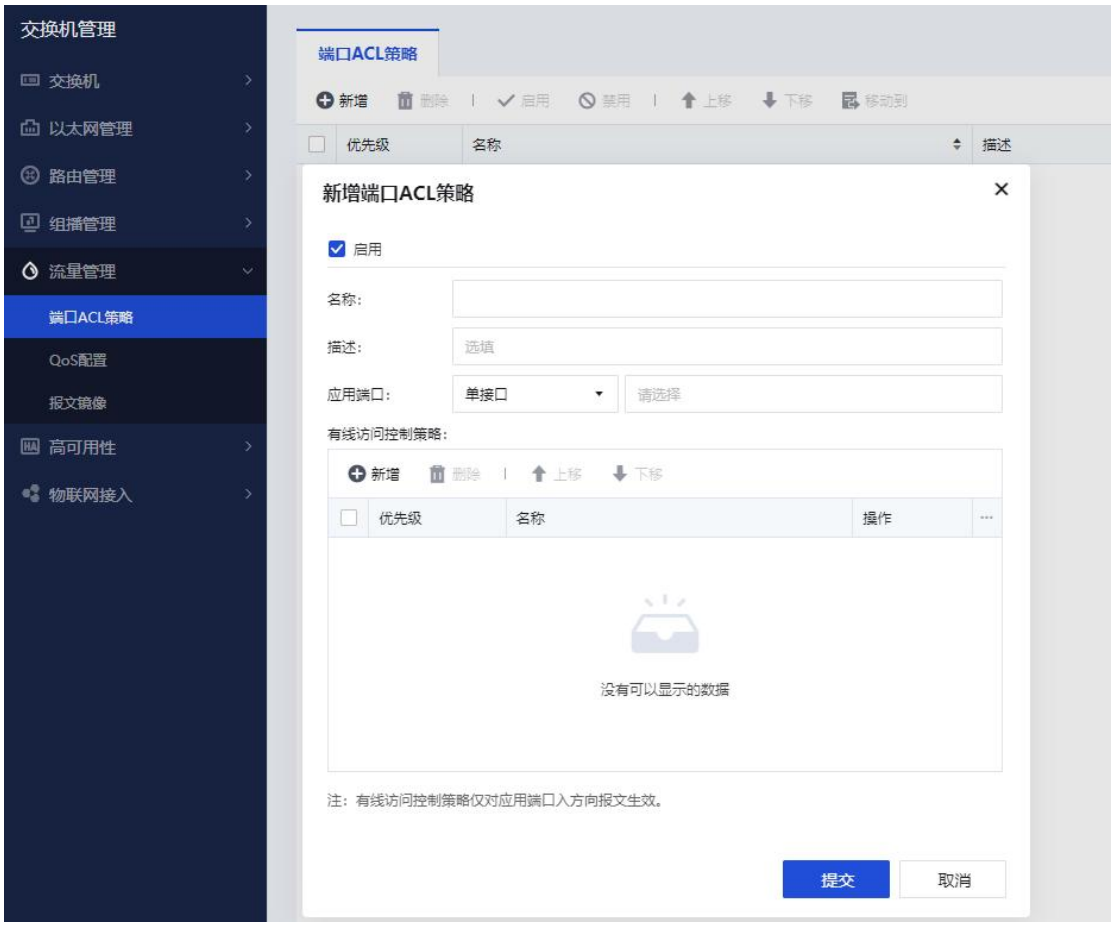
3.4.5. 流量管理

3.4.5.1. 端口策略

端口策略能够对网络访问行为进行控制，例如企业网中内、外网的通信，用户访问特定网络资源的控制，特定时间段内允许对网络的访问。限制网络流量和提高网络性能，例如限定网络上行、下行流量的带宽，对用户申请的带宽进行收费，保证高带宽网络资源的充分利用。

支持配置应用到单接口或者聚合口的有线访问控制策略。

有线访问控制策略在 “认证授权->角色授权” 中定义。



3.4.5.2. QoS 配置

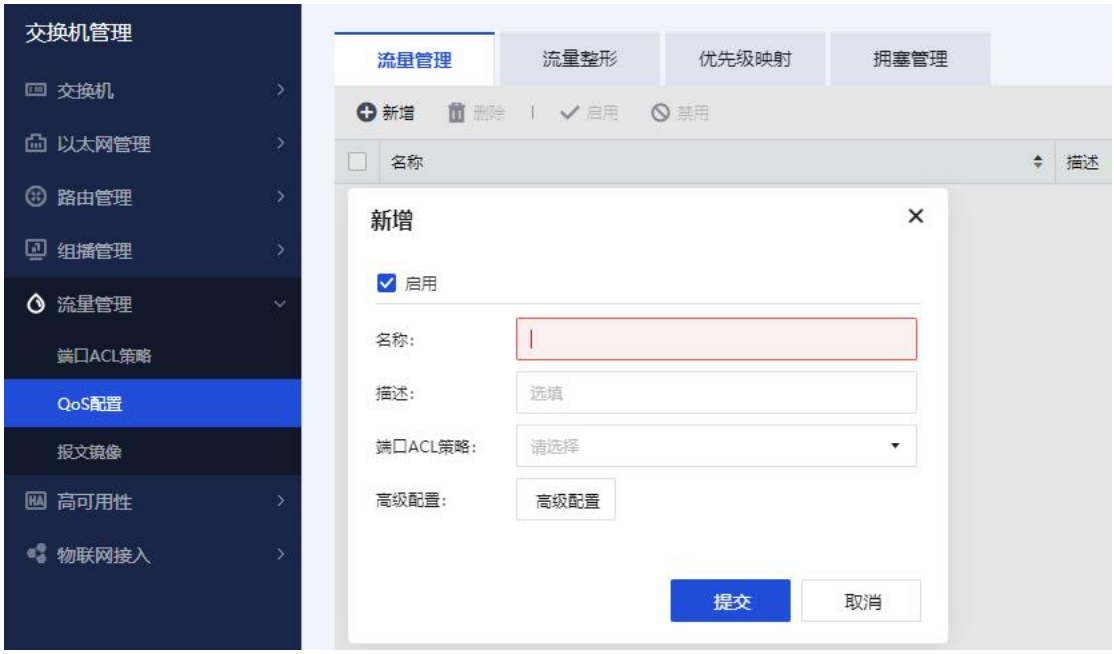
QoS（Quality of Service）即服务质量，是指网络通信过程中，允许用户业务在丢包率、延迟、抖动和带宽等方面获得可预期的服务水平。

流量管理功能包括重标记、流量监管、重定向等。

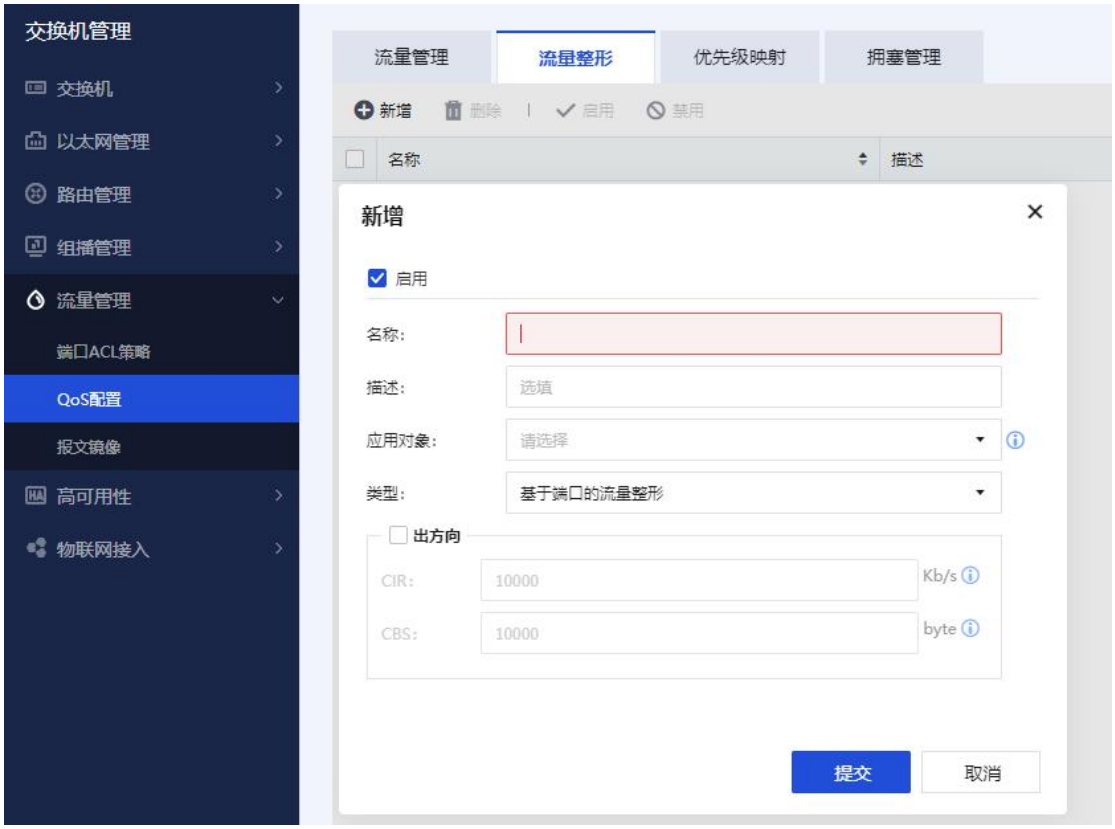
重标记：通过设置报文的优先级或标志位，重新定义报文的优先级。

流量监管：通过监控进入网络的流量速率，将输入流量限制在一个合理范围内。当一台设备存在多个芯片时，进入网络的流量速率以每个芯片为单位进行统计，不同芯片之间的流量速率互不影响。

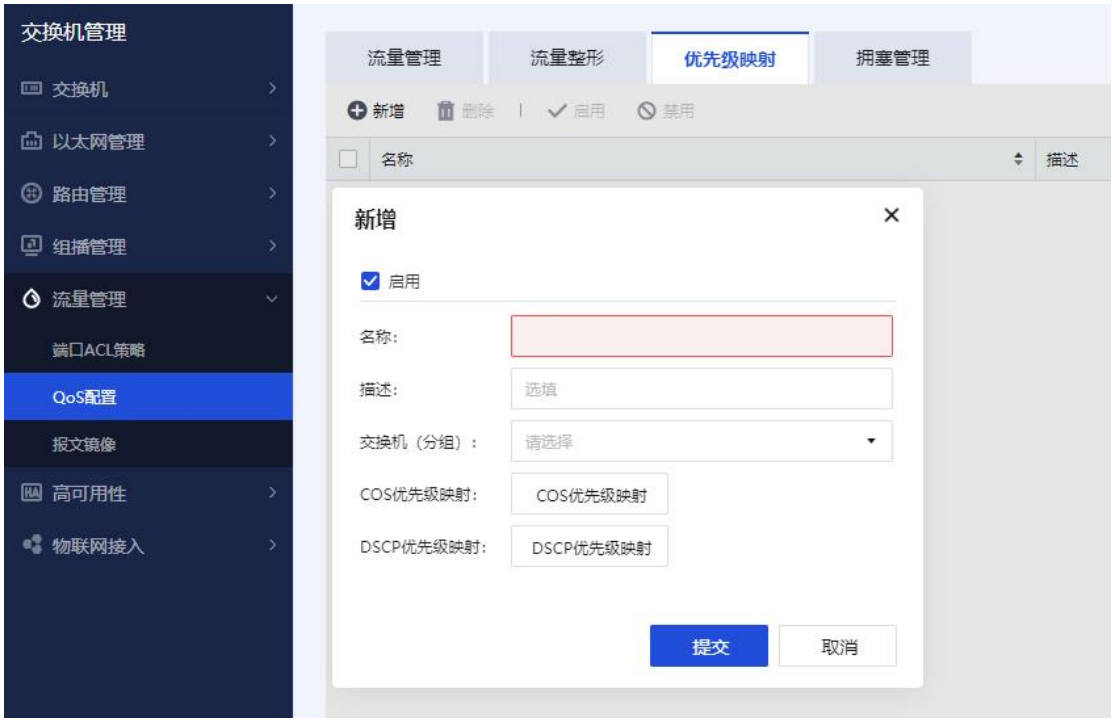
重定向：将符合流分类的报文流重定向到其他端口进行处理。



流量整形是一种主动调整流量输出速率的措施，对上游输入的不规整流量进行缓冲，使流量输出趋于平稳，从而解决下游设备的拥塞问题。



优先级映射实现从 COS 优先级到 DSCP 优先级之间的映射，设备可根据优先级提供有差别的 QoS 服务。

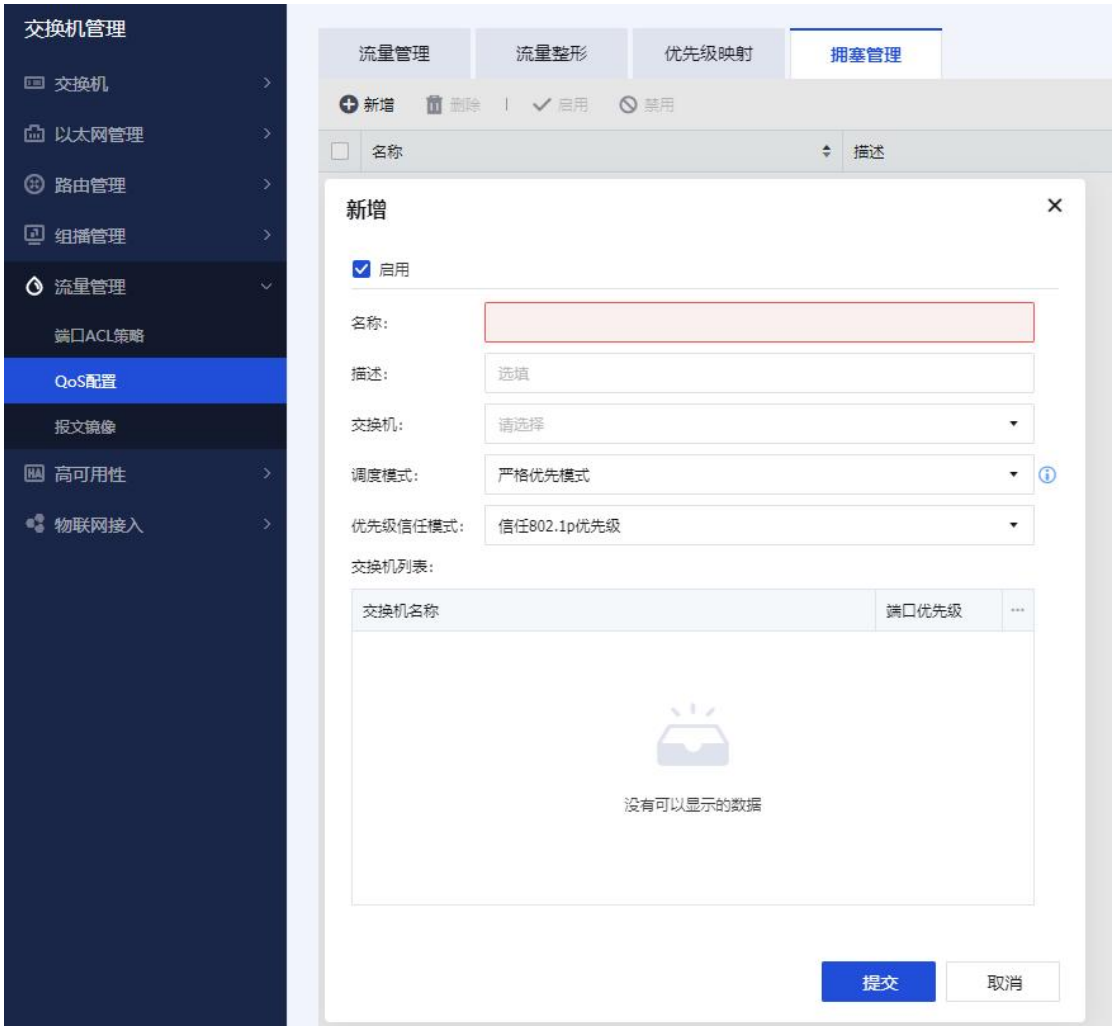


当时延敏感业务要求得到比非时延敏感业务更高质量的 QoS 服务，且网络中间歇性的出现拥塞，此时需要进行拥塞管理。拥塞管理一般采用排队技术，使用不同的调度算法来发送队列中的报文流。常用调度模式包括严格优先模式、轮询模式、加权轮询模式、严格优先+加权轮询模式和差分加权轮询模式。

常用优先级信任模式包括信任 dscp 优先级和信任 802.1p 优先级。信任 dscp 优先级是指直接根据报文携带的 dscp 优先级来转发数据，信任 802.1p 优先级分两种情况：

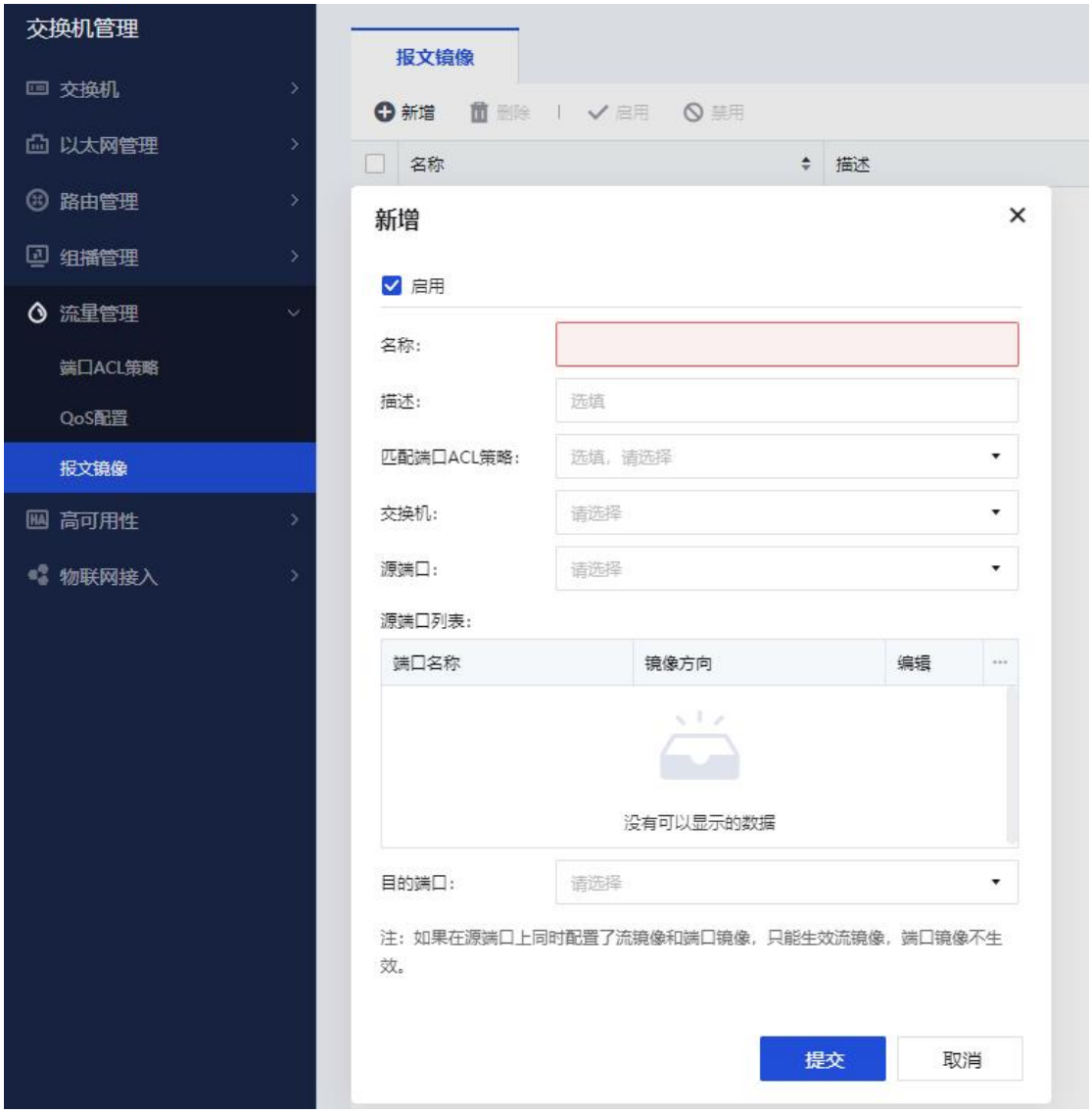
1.当入口报文不带 802.1p 优先级，设备将使用端口优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

2.当入口报文携带 802.1p 优先级，此时按报文携带的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。



3.4.5.3. 报文镜像

网络运行过程中，经常需要对网络设备的端口状况进行监控和分析。如果直接对转发端口进行监控和分析，可能会影响端口的转发效率。用户可以通过配置镜像功能，将网络中某个接口（镜像端口）接收或发送的报文，复制一份到指定接口（观测端口），然后发送到和观测端口直连的报文分析设备上。用户通过分析镜像报文，可进行网络监控和故障排查。



端口镜像：指将镜像端口接收或发送的报文完整地复制输出到指定的观测端口。

匹配 ACL 的流镜像：匹配 ACL 的流镜像：指将镜像与匹配 ACL 相结合，只复制满足特定条件的报文，过滤报文分析设备不关心的报文，为报文分析提供更精细的控制，提高报文分析设备的工作效率。

源端口：源端口是镜像端口，即报文流经的端口。

目的端口：目的端口是观察端口，即报文重新发送至的指定端口。

镜像规则数量统计说明

1.源端口包含普通端口时，若镜像方向为单方向，则端口所在板卡镜像规则数量加 1；若镜像方向为双方向，则端口所在板卡镜像规则数量加 2。

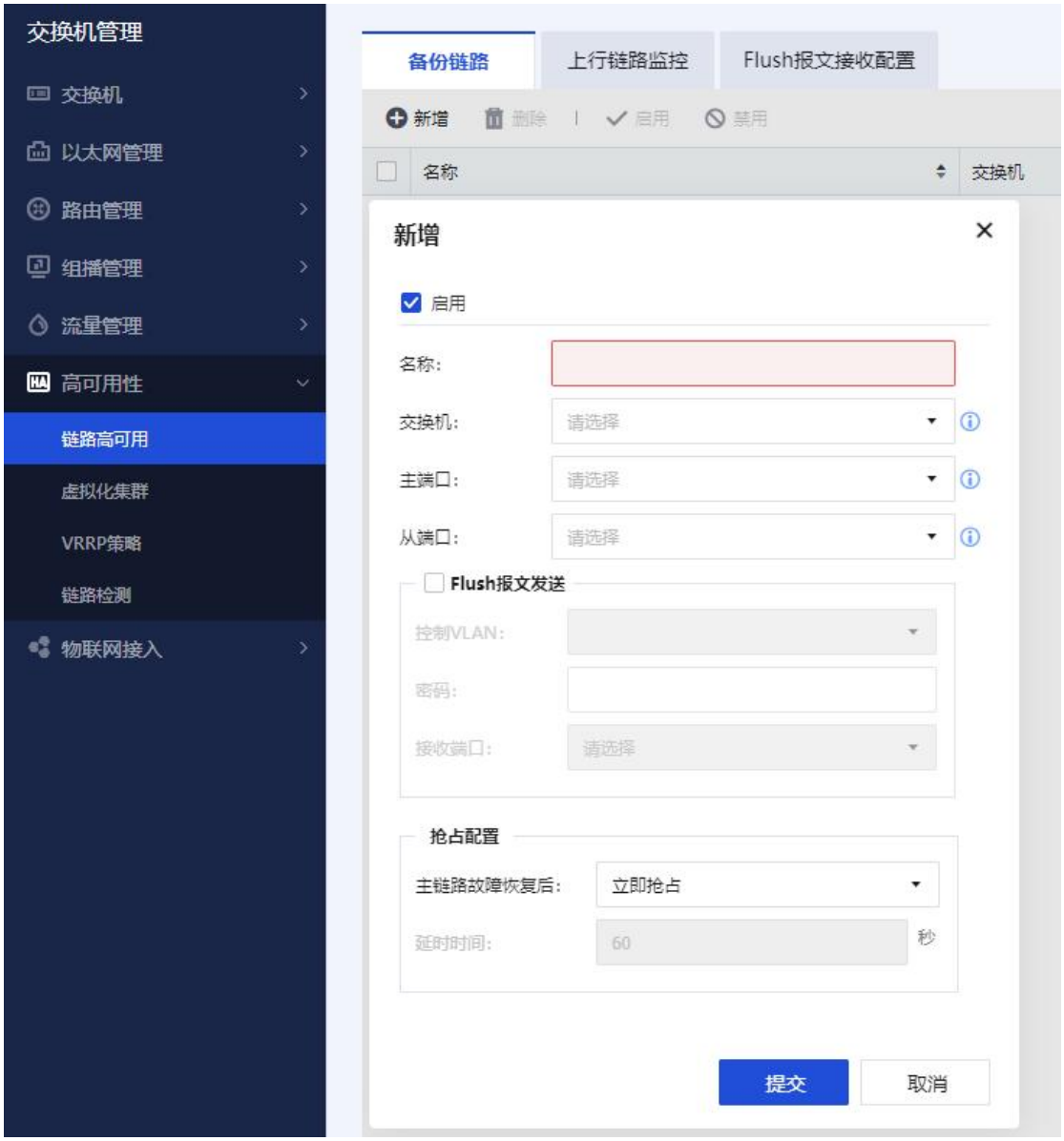
2.源端口包含聚合口时，若镜像方向为单方向，则所有板卡镜像规则数量加 1；若镜像方向为双方向，则所有板卡镜像规则数量加 2。

3.板卡镜像规则数量不累加。源端口同时包含普通端口与聚合口时，板卡镜像规则数量以聚合口计算为准。

3.4.6. 高可用性

3.4.6.1. 链路高可用

备份链路，又叫做灵活链路。一个备份链路由两个端口组成，其中一个端口作为另一个的备份。备份链路常用于双上行组网，提供可靠高效的备份和快速的切换机制。



主用链路和备用链路：

备份链路组中处于转发状态的链路称为主用链路，处于阻塞状态的链路称为备用链路。

主端口和从端口：

备份链路组的主用和备用链路在特定的设备上体现为端口或者聚合组端口，此处统称为端口。为了区分备份链路组中的两个端口，将两个端口分别命名为主端口和从端口。备份链路组中的从

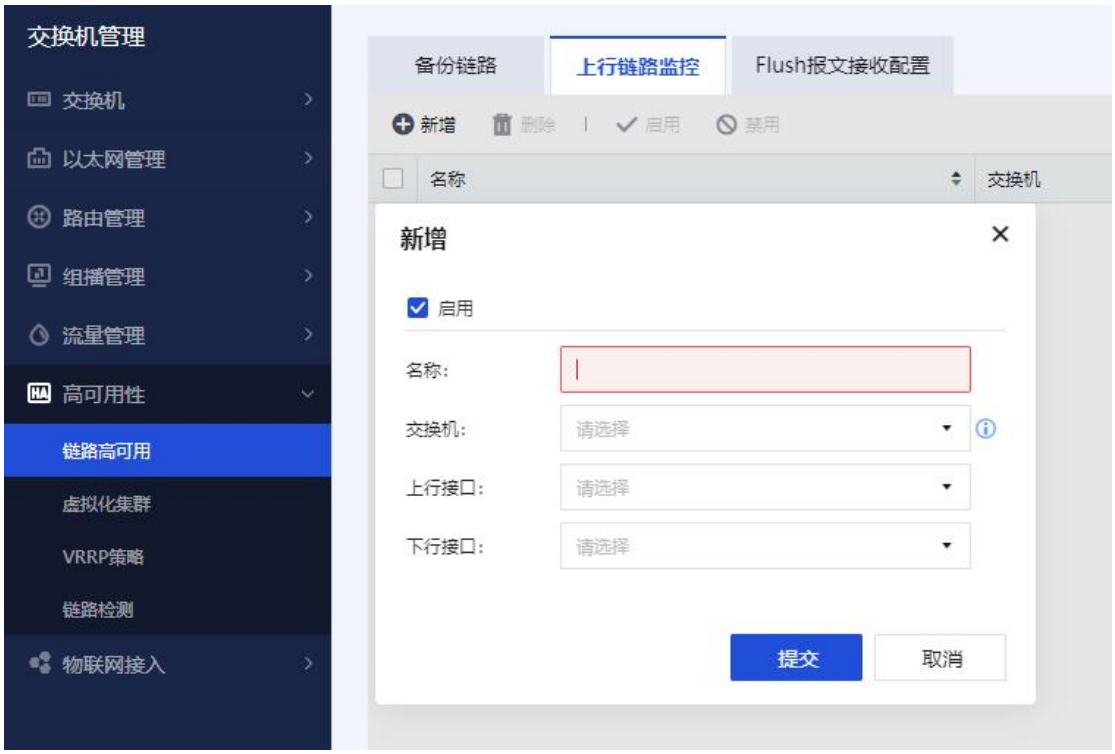
接口在备份链路组启动后会被阻塞。

FLUSH 报文：

端口切换之后，备份链路通过发送 FLUSH 报文通知其他设备进行地址刷新，且相关设备必须使能 Flush 报文接收功能。但是，由于该技术为私有技术，目前只限于我司的交换机、华为、华三的设备能够识别该报文。对于不识别 FLUSH 报文的设备，只能通过流量触发 MAC 地址的更新。

抢占配置：

抢占配置方式选择立即抢占，即备份链路组中主链路出现故障并倒换到从链路后，当原主链路故障恢复后，立刻进行备份链路倒换。抢占配置选择延时抢占，即等待延时时间到达后，根据备份链路组的接口最后获得的 Up/Down 状态处理备份链路组的状态。抢占配置方式选择不抢占，即为了保持流量稳定，原有的主用链路将维持在阻塞状态，不进行抢占。



上行链路监控是一种端口联动方案，它能通过监控设备的上行端口，根据其 UP/DOWN 状

态的变化来触发下行端口 UP/DOWN 状态的变化，从而触发下游设备上的拓扑协议进行链路的切换。

上行接口：

上行接口是上行链路监控组中的被监控的端口，上行链路监控组的上行接口可以是以太网端口（电口或光口）、聚合口或备份链路组。

下行接口：

下行接口是上行链路监控组中的监控端口，上行链路监控组的下行接口可以是以太网端口（电口或光口）或聚合口。

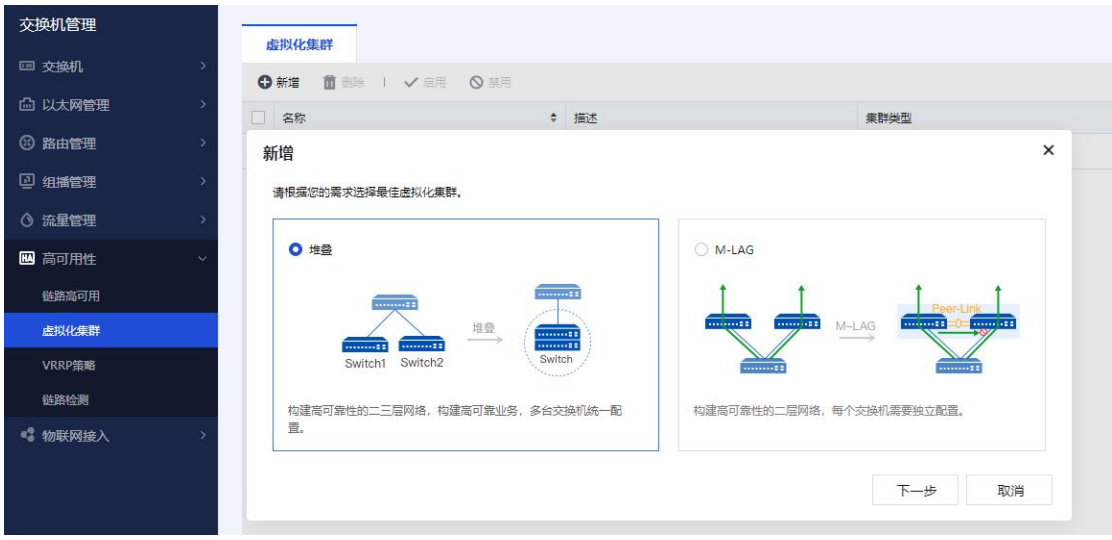
支持独立配置 Flush 报文接收功能，并配置接口接收 Flush 报文的加密方式、接收控制 VLAN ID 和密码。当上游设备收到 Flush 报文时，判断该 Flush 报文的发送控制 VLAN 是否在收到报文的接口配置的接收控制 VLAN 列表中。如果不在接收控制 VLAN 列表中，设备对该 Flush 报文不做处理，直接转发；如果在接收控制 VLAN 列表中，设备会处理收到 Flush 报文，

进而执行 MAC 地址转发表项和 ARP 表项的刷新操作。

3.4.6.2. 虚拟化集群

堆叠就是将多台设备通过专用的堆叠口或业务口连接起来，形成一台虚拟的逻辑设备。用户对这台虚拟设备进行管理，来实现对堆叠中所有成员设备的管理。堆叠系统具有高可靠性及易管理等优点。

M-LAG（Multichassis Link Aggregation Group）即跨设备链路聚合组，是一种实现跨设备链路聚合的机制，将一台设备与另外两台设备进行跨设备链路聚合，从而把链路可靠性从单板级提高到了设备级，组成双活系统。



堆叠成员：

组建堆叠的成员需要同样的软件版本，硬件型号满足组堆叠。最多支持两台交换机组堆叠。

堆叠口：

堆叠系统通信链路两端的接口为堆叠口，仅支持光口作为堆叠口。堆叠口的连接可以由多条堆叠物理链路自动聚合而成，多条聚合链路之间可以对流量进行负载分担，有效地提高了带宽及

堆叠可靠性。堆叠成员端口必须为统一类型端口，例如 10GE 与 40GE 端口不可以组成堆叠聚合链路。普通口切换为堆叠口后，将不再支持切换速率与单双工，GE 口速率配置为 1000M 全双工，10GE 口速率配置为 10G 全双工，40GE 口速率配置为 40G 全双工，堆叠口再切换为普通口后，又会恢复原来的配置。

本地流量优先转发：

由于堆叠链路带宽有限，为了提高转发效率，减少跨堆叠成员的流量转发，支持 TRUNK 口的本地流量优先转发功能。即从本设备进入的流量，优先从本设备上相应的 TRUNK 成员口转发出去；如果本设备相应的接口故障或流量已经达到了接口线速，那么就从对端堆叠成员设备的接口转发出去。

Hello 报文超时时间：

堆叠系统中备机超时时间内，未收到主机发送的保活报文，会自动升级为主机。

多主检测：

为了减少堆叠分裂对业务的影响，建议用户在堆叠组建完成后进行双主检测的配置。堆叠链路断开或堆叠心跳超时出现多主时，MAD 检测机制会检测到网络中存在多个处于主机状态的堆叠系统。MAD 冲突检测机制会保持原主机继续工作，将其他的堆叠系统转入 recovery 状态，并且在 recovery 状态的堆叠系统的所有成员上，关闭除保留端口以外的其他所有物理端口，以保证该堆叠系统不再转发业务报文。堆叠多主检测支持不检测，直连检测与代理检测，且默认检测方式为直连检测。直连检测选择的检测端口需要覆盖所有的堆叠成员，每个成员只能选择一个端口。代理检测仅支持信锐的交换机的聚合口做代理检测。

Peer-Link 口：

Peer-Link 链路两端直连的接口均为 Peer-Link 接口，支持配置光口，电口，聚合口。

链路故障配置：

Peer-Link 链路是一条直连链路，用于交换协商报文及传输部分流量，保证 M-LAG 的正常工作。

Peer-Link 故障但心跳状态正常会导致备设备上除管理网口、Peer-Link 接口以及自定义的排除端口以外的物理接口处于 DOWN 状态，此时双归场景变为单归场景。一旦配置 Peer-Link 链路故障恢复，处于 DOWN 状态的物理接口默认将在 120 秒时间自动恢复为 Up 状态。

LACP 协商配置：

部署 M-LAG 的两台设备与用户侧设备之间的链路已经分别配置为聚合链路。为了提高可靠性，建议将链路聚合模式配置为 LACP 模式。用户需确定协商 MAC 地址和 LACP 优先级以方便进行 LACP 协商配置，用来适用于 LACP 模式的 Eth-Trunk 组成的 M-LAG。

KeepAlive 口：

KeepAlive 链路是一条三层互通链路，用于 M-LAG 主备设备间发送双主检测报文。

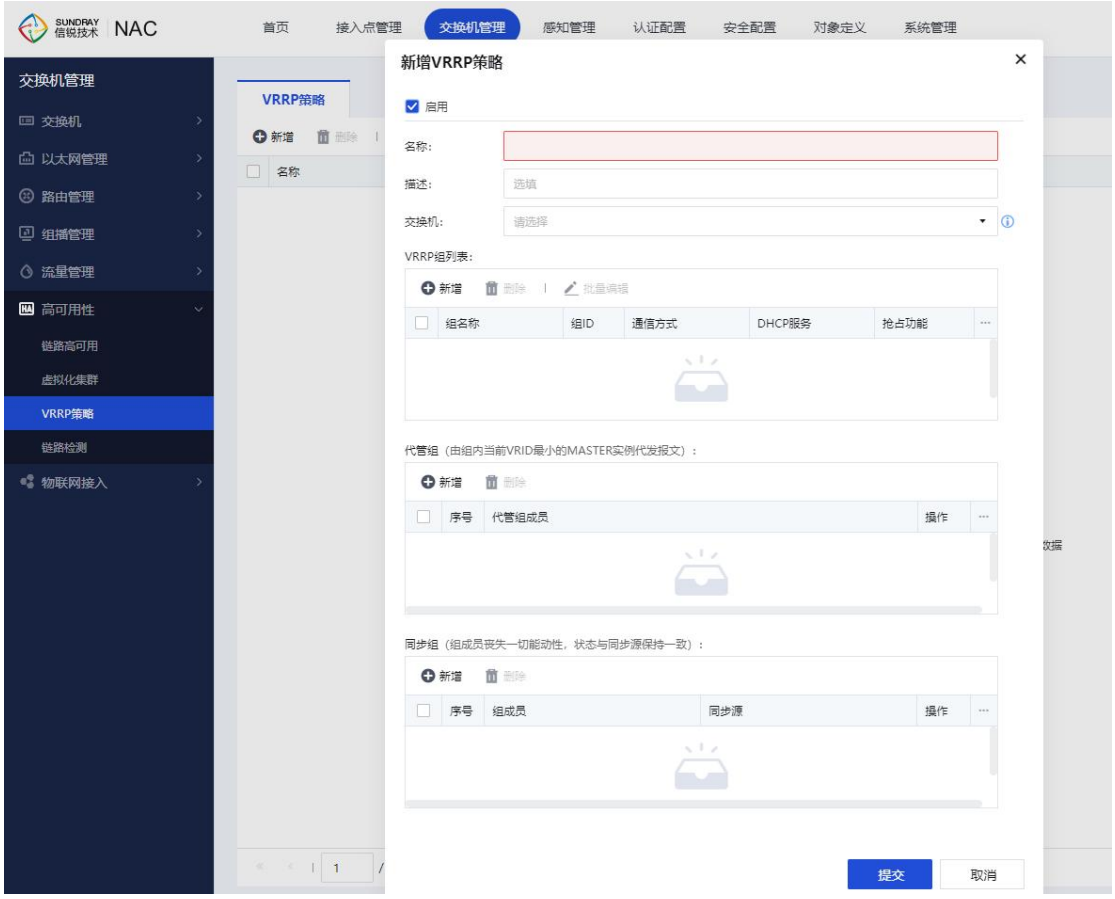
正常情况下，双主检测链路不会参与 M-LAG 的任何转发行为，只在故障场景下，用于检查是否出现双主的情况。用于检测对端的选举状态是否正常。

M-LAG 口：

M-LAG 口是 M-LAG 主备设备上连接上下行设备的 Eth-Trunk 接口。加入同一 M-LAG 口的接口，对外表现为同一个聚合接口。

3.4.6.3. VRRP 策略

VRRP（Virtual Router Redundancy Protocol）即虚拟冗余备份组协议,通过把几台路由设备联合组成一台虚拟的路由设备，使用一定的机制保证当主机的下一跳路由器发生故障时，及时地将业务切换至备份路由器，从而保证业务的连续性和可靠性。



组 ID：

虚拟路由器 ID，VRRP 备份组标识，同一个实例的 VRID 值必须一致才可以正常工作。

虚拟 IP 地址：

VRRP 备份组的 IP 地址，一个虚拟路由器可以有一个或多个 IP 地址。

虚拟 MAC 地址：

VRRP 备份组根据虚拟路由器 ID 自动生成的 MAC 地址。

通信方式：

默认使用组播的通信方式，支持单播的通信方式。

优先级：

VRRP 备份组中的设备优先级，备份组根据优先级选举出 Master 和 Backup 设备。

VRRP 绑定接口：

VRRP 备份组中，虚拟 IP 地址所在的接口。

超时时间：

VRRP 备份组中 Backup 设备因未收到 Master 设备报文，自动切换为 Master 所等待的时间。

接口监视：

VRRP 备份组中，设备监控上联口或上联链路，当上联口或上联链路故障时，降低设备优先级，触发主备切换。

状态恢复延时时间：

VRRP 备份组中，设备因故障进入 fault 状态后，在故障恢复正常时，设备从错误状态切换至 Backup 状态等待的时间。

DHCP 服务：

VRRP 备份组支持提供 DHCP 服务，且 DHCP 服务仅对 Master 设备生效。

抢占功能：

开启抢占功能后，Backup 设备的优先级高于 Master 设备优先级时，自动切换为 Master 设备。

VRRP 版本：

默认采用 VRRPv2 版本，支持 VRRPv3 版本。

通告间隔：

VRRP 备份组中，Master 设备主动发送保活报文的时间间隔。

免费 ARP 间隔：

备份组虚拟 IP 地址不断发送免费 ARP 的时间间隔。

VRRP 报文认证方式：

VRRP 备份组中，VRRPv2 版本支持不认证，简单认证和 MD5 认证方式，VRRPv3 版本不支持认证。

代管组：

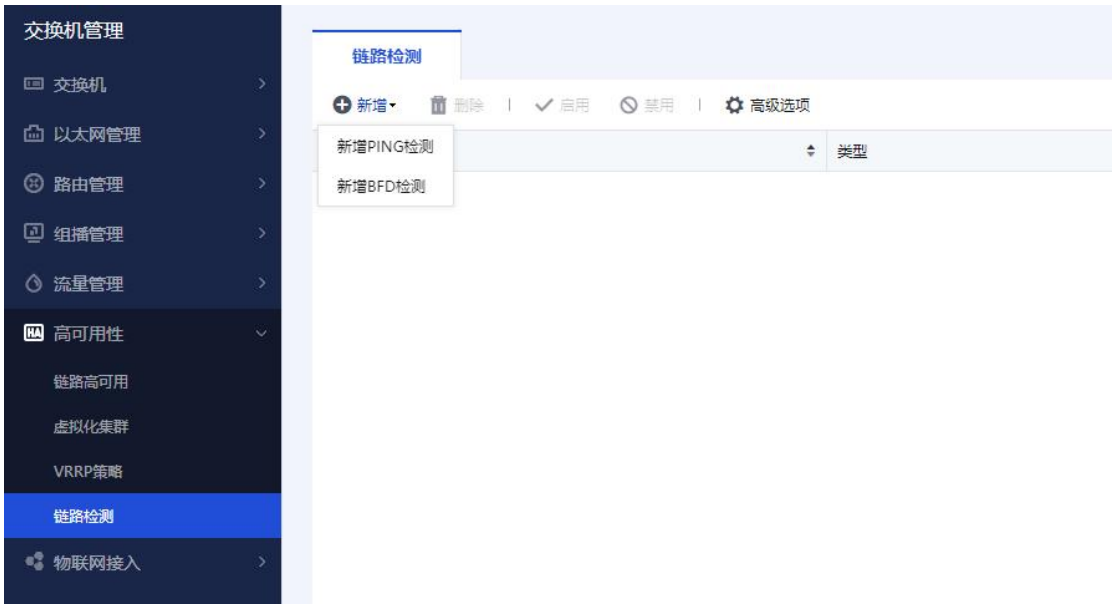
多个 VRRP 备份组实例加入同一个代管组中时，由备份组中当时 VRID 最小的 Master 设备代为发送 VRRP 报文，减少 VRRP 报文发送数量。

同步组:

由同步源负责 VRRP 保活，成员设备不发送保活报文，实例状态与同步源状态保持一致，减少 VRRP 报文发送数量。

3.4.6.4. 链路检测

链路检测含 ping 检测及 BFD 检测。



PING 检测

当设备出现故障时，可以使用 PING 检测测试网络连接是否正常工作。

PING 检测主要用于检查网络连接及主机是否可达。源主机向目的主机发送 ICMP 请求报文，目的主机向源主机发送 ICMP 回应报文。

BFD 检测

BFD 检测用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

BFD 提供了一个与介质和协议无关的快速故障检测机制。是网络设备间任意类型的双向转发路径提供快速、轻负荷的故障检测。

支持的检测类型有私有二/三层链路检测，外部二/三层链路检测和单臂回声功能。

私有二/三层链路检测:

私有二/三层链路检测可以当前网关内的交换机实现通过二层接口或三层接口连通的设备间链路故障的快速检测。

外部二/三层链路检测:

外部二/三层链路检测可以实现与第三方或者其它网关的交换机通过二层接口或三层接口连通的设备间链路故障的快速检测。

单臂回声功能:

在两台直接相连的设备中，其中一台设备支持 BFD 功能，另一台设备不支持 BFD 功能。为了能够快速的检测这两台设备之间的故障，可以在支持 BFD 功能的设备上创建单臂回声功能的 BFD 会话。支持 BFD 功能的设备主动发起回声请求功能，不支持 BFD 功能的设备接收到该报文后直接将其环回，从而实现转发链路的连通性检测功能。

标识符:

静态建立 BFD 会话是指通过命令行手动配置 BFD 会话参数，包括配置本地标识符和远端标识符等，然后手工下发 BFD 会话建立请求。

如果对端设备采用动态 BFD，而本端设备既要与之互通，又要能够实现 BFD 检测静态路由，必须配置静态标识符自协商 BFD。

高级选项:

报文优先级：支持将 BFD 报文设置为高优先级报文后，优先保证 BFD 报文的转发

BFD 会话的检测时间由 BFD 会话的本端检测倍数、本端 BFD 报文的接收间隔、发送间隔决定，检测时间 = 检测倍数 × max（接收间隔，发送间隔）

发送间隔（毫秒）：缺省情况下，BFD 报文的发送间隔是 1000 毫秒。

接收间隔（毫秒）：缺省情况下，BFD 报文的接收间隔是 1000 毫秒。

检测倍数：缺省情况下，本地检测倍数为 3。

报文生存时间：为使得使用不同版本的设备能够互通，并考虑后续版本升级以及和其他厂商的设备互通，此时可以配置报文生存时间。

DOWN 状态发包间隔（毫秒）：链路协议 Down 状态，在该状态下只可以处理 BFD 报文，支持配置 DOWN 状态发包间隔，从使是该接口也可以快速感知链路故障。

WTR 等待恢复时间（分钟）：如果 BFD 会话发生振荡，则与之关联的应用将会在主备之间频繁切换。为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间 WTR。当 BFD 会话从状态 Down 变为状态 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用。如果使用 WTR，用户需要手工在两端配置相同的 WTR。否则，当一端会话状态变化时，两端应用程序感知到的 BFD 会话状态将不一致。

3.4.7. 物联网接入

3.4.7.1. 智能设备接入

接入服务：

智能设备接入是专门为物联网 DTU 设备提供的一类端口，DTU 设备可以通过交换机快速的和物联网平台建立连接。

端口 vlan:

将已选择的所有接入端口划分为同一 vlan，可以根据需求设置 vlan 标签，注意设置 vlan 标签时不要和交换机其他功能已设置的 vlan 标签重复，同样的其他功能将要设置的 vlan 标签也不要和智能设备接入的端口 vlan 重复。

端口 DHCP 地址池:

交换机为接入的 DTU 设备分配 IP 的地址池，默认 3.3.3.0/24。

物联网平台地址:

物联网平台的 IP 地址，可以通过有效性检测检查该地址是否有效。

端口信息:

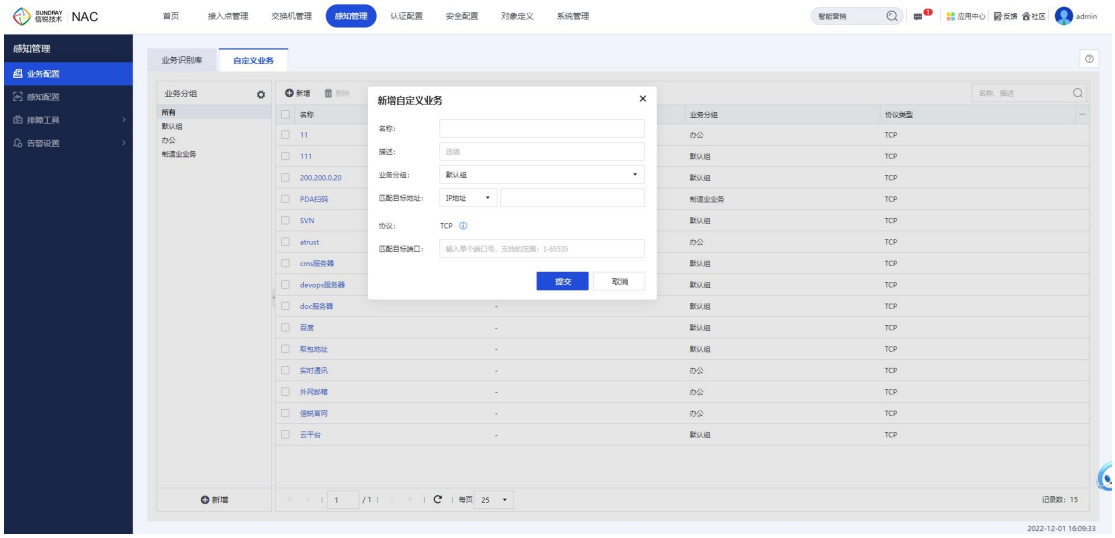
显示交换机端口下接的 DTU 设备信息，方便当 DTU 设备出现故障之后根据端口信息简单判断是什么问题。

3.5. 感知管理

3.5.1. 业务配置

【业务识别库】是系统内置业务，包括有线和无线的业务。支持后续通过上传包的形式拓展业务识别库。

【自定义业务】允许用户配置自定义，自定义业务支持 tcp 协议，可以指定业务服务器的地址和端口来添加业务，地址支持 ip 和域名两种形式。



3.5.2. 感知配置

3.5.2.1. 用户体验检测

【用户体验监测】通过分析无线用户的上网行为，了解其认证、网络、业务访问质量。实时监测真实用户的流量，统计各类网络指标数据和业务指标数据、并判断用户的网络体验和业务体验如何。在该页面可以开启/关闭用户流量监测。

- **网络质量：**默认开启，统计用户的无线终端的网络体验质量。
- **业务质量：**支持开启/关闭业务质量检测，监测业务中可以选择要监测的用户业务，并通过业务健康全局指标配置设定各个业务质量指标的评分标准。

AI 模拟探测

通过无线 AP、交换机智能模拟终端自主持续探测业务，通过 SLA 指标阈值计算以业务卡片的形式直观展示健康度分值、等级。当网络出现异常时会在对应业务卡片生成异常访问事件（详见业务质量感知页面）。该页面支持对模拟探测策略进行配置，并设置统一的模拟检测间隔。

3.5.2.2. AI 模拟探测

【AI 模拟探测】分为无线探测策略和有线探测策略。

无线探测策略

➢ 探测内容

默认开启，统计用户的无线终端的网络体验质量。

➢ 网络质量探测

检测配置的网络地址的连通性。最多支持配置 3 个网络地址。

➢ 业务连通性

模拟终端接入被测网络，向引用的业务服务器发起连通性检测。检测对应的地址和端口是否能够正常访问。

➢ 业务健康指标全局配置

支持编辑对应 SLA 指标的阈值，根据对应的业务特性配置对应指标阈值。

➢ 探测无线网络

支持探测开放式、开放式+web、psk 认证、企业认证等认证方式的无线网络，配置页面一样。企业认证的无线网络，则还需配置认证账号跟认证密码。

➢ 探测接入点

选择被检测网络下的接入点，注意：部分接入点不支持模拟检测功能，详情请联系信锐技服。

➢ 探测时间

管理员可以根据业务的特性来自由配置进行 AI 探测的时间段。

➢ 探测间隔

全局的 AI 模拟探测策略中的无线 AP、交换机智能模拟终端访问业务的间隔，范围是 15 分钟-24 小时。注意：模拟终端过多的情况下，探测间隔周期到了也会继续执行剩余的探测策略，即优先保证所有的模拟终端探测完成再进行下一轮探测。

有线探测策略

➢ 探测内容

仅支持业务连通性，有效的 SLA 指标包含时延、抖动、丢包率、业务连通性检测成功率。

➢ 探测业务

模拟终端向引用的业务服务器发起连通性检测。注意：

1. 探测有线内置业务，需要在探测交换机上的探测 VLAN 属性的端口对服务端进行重连才能识别到服务器的 IP，否则服务器的业务卡片数据一直为空。

2. 如果连续两轮探测有线内置业务连通性均为失败，则需要重新断开重连服务、重新识别服务器的 IP，否则模拟终端不会再进行探测，业务质量卡片不会产生新数据。

3. 当一台交换机同时探测监控、SANGFOR aDesk 业务时，需将摄像头与监控服务器通讯涉及的上下联口配置为对应 VLAN 允许 tagged 通过的端口属性，否则监控服务器的 IP 无法被识别，业务质量卡片数据会一直为空。

➢ 业务健康指标全局配置

支持编辑对应 SLA 指标的阈值，根据对应的业务特性配置对应指标阈值。

➢ 探测 VLAN

配置选择交换机生成对应网络配置的智能模拟终端。注意：

1. 模拟终端配置的网关、DNS 不能为该探测交换机的接口地址。

2. 模拟终端的 DHCP 服务器不能配置在该探测交换机上。

3. 探测自定义业务的 IP 不能为该探测交换机的接口 IP。

否则会导致创建模拟终端失败，业务质量卡片无数据或者连通性检测一直为失败状态。

➢ 探测时间

管理员可以根据业务的特性来自由配置进行 AI 探测的时间段。

➢ 探测间隔

全局的 AI 模拟探测策略中的无线 AP、交换机智能模拟终端访问业务的间隔，范围是 15 分钟-24 小时。注意：模拟终端过多的情况下，探测间隔周期到了也会继续执行剩余的探测策略，即优先保证所有的模拟终端探测完成再进行下一轮探测。

3.5.3. 排障工具

3.5.3.1. 路径监测

功能说明

在用户访问网络服务出现故障时，可以通过路径监测功能绘制出用户终端访问网络经过的网络设备，并可以通过路径绘制的结果定位到是哪一个网络设备出现故障，帮助网络管理人员快速定位问题。路径监测功能可支持用户无线接入和有线接入时进行绘制。路径监测为辅助排障功能，可单独配置使用也可以组合其他业务感知类功能一起使用。

使用说明

1. 通过配置路径监测任务持续绘制路径。

在路径监测页面新增任务，允许用户自定义需要匹配的终端的 IP 或 MAC 地址，服务器的协议类型、端口号、地址信息进行路径绘制。可配置监测时长，在监测时长内设备会持续通过用户的流量查找绘制路径。

路径监测任务允许用户手动停止、重新开启监测，允许修改监测配置。并支持用户通过每个任务的历史记录查看历史的绘制结果。

清理监测结果配置会自动清理超过保存时间的路径绘制结果。

注：

1. 在使用该任务进行路径绘制时，需要用户在持续访问网络才可绘制出结果。

2. 路径监测任务最大允许创建 100 条，同时最多只有 16 个路径监测任务可同时绘制，其他任务需排队等待。

2. 通过配置路径监测任务模拟用户进行网络访问绘制路径。

路径监测页面新增的任务需要持续有用户流量才可绘制路径，当用户没有进行网络访问时可以通过接入点与交换机模拟无线和有线用户进行网络访问进行路径绘制。在路径监测任务的结果中可开启模拟流量进行路径绘制，模拟流量绘制仅会绘制一次路径结果，可暂停、重复发起模拟绘制。

模拟无线流量检测，用户需要选择想要探测的无线网络和接入点。

模拟有线流量检测，用户需要选择想要探测的 VLAN 和交换机，并配置探测设备的地址。

3. 通过网络检测功能进行绘制路径。

无线网络检测、有线网络检测功能在进行探测时可搭配路径绘制一起使用进行网络排障。

在使用网络检测的单终端模拟（适用于排障）时，在进行检测的同时会自动绘制出模拟检测的流量路径辅助排障。

在使用网络检测的多终端模拟（适用于开局）时，在进行检测过程中若出现了检测失败的结果，可手动进行当前失败结果的路径绘制辅助排障。

4. 通过业务质量感知用户体验监测功能进行绘制路径。

业务质量感知开启了用户体验监测时，若接入用户出现了访问异常事件时会自动开启路径绘制，绘制当前用户流量经过的设备辅助排障。该路径绘制仅绘制一次会存在用户停止网络访问后无路径结果的情况。

在用户无流量访问时可通过开启模拟流量检测，使用当前用户接入的设备发起模拟探测绘制访问对应业务服务器的路径帮助进行排障。

可通过接入终端详情快速创建一个路径监测任务持续跟踪绘制该终端访问网络的路径结果。

注：

1. 仅无线终端接入支持上述种方式绘制路径。

2. 仅真实终端连接失败 的访问异常事件支持绘制路径。

使用限制

1. 路径监测需要设备开启智能拓扑功能才能使用。

2. 路径监测的流量经过 NAT 设备后，不能绘制出 NAT 后的路径。

3. 路径监测仅在网络部署均为信锐设备且都在智能拓扑中才绘制准确。

3.5.3.2. 网络监测

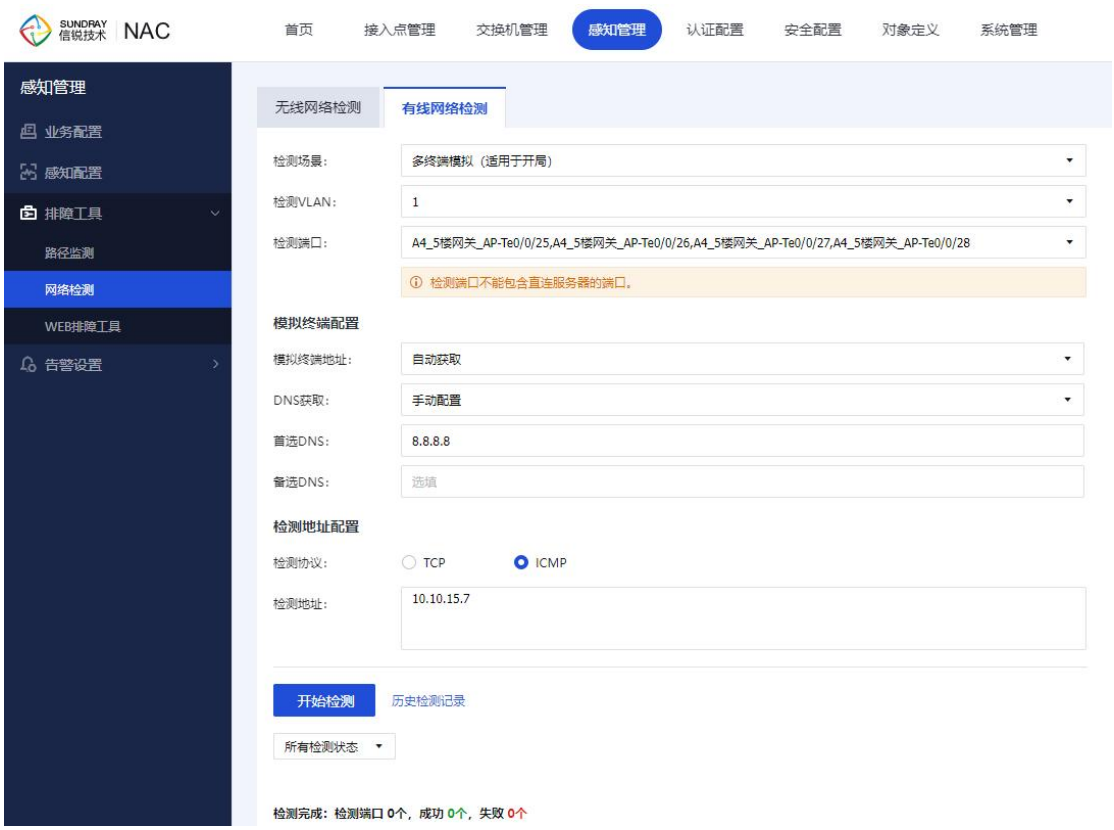
无线网络检测

【无线网络检测】支持单终端模拟和多终端模拟探测，单终端模拟和多终端模拟分别适用于管理员进行排查网络问题以及改造/新建网络时验证网络连通性。

- 单终端模拟：模拟单个终端对单一网络地址进行连通性检测、路径绘制。
- 多终端模拟：模拟多个终端至多同时对 3 个网络地址进行连通性检测，当连通性检测失败时，可以在查看详情中进行模拟流量绘制路径，排查网络故障点。
- 历史检测记录：管理员使用无线网络探测的记录，默认保留 3 天。

有线网络检测

【有线网络检测】支持单终端模拟和多终端模拟探测，单终端模拟和多终端模拟分别适用于管理员进行排查网络问题以及改造/新建网络时验证网络连通性。，一般用于接入层交换机。



- 单终端模拟：模拟单个终端进行 1 个网络地址进行连通性检测、路径绘制。
- 多终端模拟：模拟多个终端并至多同时对 3 个网络地址进行连通性检测，当连通性检测失败时，可以在最近检测记录中进行绘制路径排查网络故障点。
- 历史检测记录：管理员使用有线网络探测的记录，默认保留 3 天。

注意事项

1. 检测端口只能选择 access 属性的端口。
2. DHCP 服务不能在选择端口所在的交换机上开启。
3. 无法检测选择端口所在交换机上的接口地址。
4. 模拟终端的网关不能在配置在选择端口所在的交换机上。
5. DNS 无法通过选择端口所在交换机代理转发。
6. 历史记录不支持绘制路径。

3.5.3.3. Web 排障工具

【Ping 检测】在网络出现故障时，通过 ping 检测可以检测出交换机与目的地址之间连通性和时延。

即时 Ping 检测

【即时 Ping 检测】交换机通过发送固定数量包到目的地址，统计丢包率与时延。

- 目的地址：支持 IP 地址和域名。
- 源 IP 地址：支持自动选择和手动选择。
- Ping 包大小：发送 ping 包的包长。
- 历史检测记录：最多保存 10 条最近的记录，支持自动清理最大超过 30 天结果记录(默认 3 天)。

持续 Ping 检测

【持续 Ping 检测】可同时配置多条 Ping 检测任务，使交换机发送固定时长 ping 包到目的地址，持续统计丢包计数。测试结果支持下载。

- ping 时长：发送 ping 包检测的时长。
- 自动清理配置：支持自动清理最大超过 30 天的检测记录(默认 7 天)。
- 历史检测记录：最多保存 10 条最近的记录，测试记录可下载。

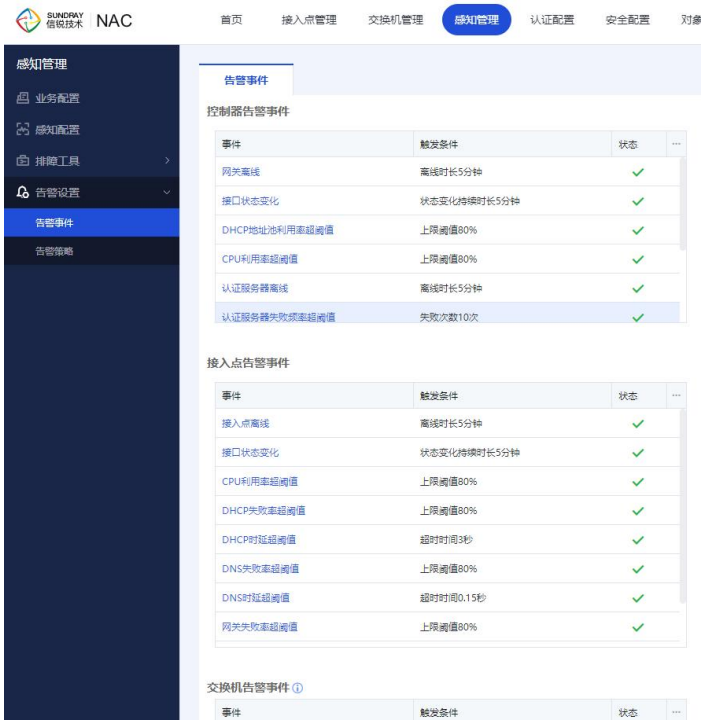
- 备注：持续 ping 检测累计失败 300 次后，将自动停止任务。

3.5.4. 告警设置

3.5.4.1. 告警事件

根据用户实际需要配置控制器告警事件、接入点告警事件和交换机告警事件的触发条件。

例如：MAC 地址表利用率超阈值告警事件的触发条件分为同时满足 80%（上限阈值）和满足 5 次（触发次数）。



3.5.4.2. 告警策略

概述

根据用户的实际需要配置智能告警的应用对象。

注意事项

1、同一设备的同一事件支持配置多条告警规则，告警规则可以上下移动，位于上方规则优先级高，位于下方的规则优先级低下，一旦匹配中优先级高的规则便不再匹配优先级低的规则；

2、全局选项中可以配置单设备单事件单日最大推送个数，数值范围为 1-1440；

3、告警规则支持配置 通知内容，发送间隔，发送时间；

名词解释

- 告警设备：选择控制器、接入点和交换机中需要监控的具体设备。
- 告警接口：选择需要监控设备的端口。
- 告警方式：选择通过短信/APP 消息的方式将告警消息发送给用户。

3.6. 认证配置

3.6.1. 证书管理

『证书管理』是用于管理【外部 CA】和管理【服务器证书】。配置证书管理后，可以在【接

入点配置】-【无线网络】中选择认证方式属于“企业”方式认证的时候，启用证书方式认证。证书方式认证，大大加强了企业无线用户终端的安全接入。

证书可以新增【外部 CA】、【服务器证书】

3.6.1.1. 外部 CA 证书

【添加外部 CA】主要是通过在线方式去检测证书的有效性，不需要把用户认证证书导入到 NAC 设备上，当无线终端采用证书方式认证的，NAC 主动去与服务器进行交互认证。验证证书用户的有效性。

【证书】:导入外部 CA 的根证书。

【编码】包括：UTF-8、UCS-2、GBK、GB2312、BIG5，指明该 CA 所颁发用户证书的编码格式，让 NAC 能正确提取用户证书的信息，如选择了 BIG5，但选择的证书是 UTF8，则会显示不正确。

【用户名属性】CN、Email 前缀、OID，用户认证成功后用指定的属性值显示为登录用户名。

【检查证书撤销列表】通过 CRL 文件或在线查询被吊销的证书。

【导入 CRL 文件】：CRL 文件可以简单的理解为一个记录了用户证书序列号的文件，该文件由 CA 签发发布，记录了的证书序列号表示该证书已经失效。也就是 CRL 里面记录的证书序列号表示由这个 CA 签发的证书并且序列号在 CRL 文件里面的都已经是无效了的证书。

【在线证书状态查询】一般 CRL 文件并不是每天都发布，而是周期性的发布，而在这个周期内有可能其他证书被吊销了，所以可以配置在线证书状态实时去查询证书的有效性

【检查 OCSP 服务器回应的消息签名】导入 OCSP 服务端签名证书的公钥，主要检测 OSCP 数据在传输过程中是否被篡改。

3.6.1.2. 服务器证书

配置服务器证书，是为了让无线终端用户反向认证服务器是否合法，可以配置服务器证书，服务器证书可以通过 2 种方式生成。【导入一张证书】和【创建一个证书请求】，如下图：

【导入一张证书】直接将已有的服务器证书的公钥私钥一起导入到设备里面。如果证书采用了密码，需要使用密码后，才可以正常导入。

【创建证书请求】：填写用户信息，包括国家、省份、城市、公司、部门、颁发给、邮箱、并设置密码长度，就可以创建一张证书请求文件：

证书请求文件需要让 CA 签名，附上签名数据，有效期后，点击【处理未决的证书请求】再把证书导入到设备中，就可以在设备生成一张完整的服务器证书了。

类型	证书	操作
服务器证书	查看	
服务器证书	查看	处理未决的证书请求
服务器证书	查看	处理未决的证书请求
服务器证书	查看	处理未决的证书请求
外部CA	查看	设置CA选项

内置 CA 颁发证书：由内置颁发证书，填写用户信息，包括国家、省份、城市、公司、部门、颁发给、邮箱，可以设置由 NAC 内置 CA 中心颁发的服务器证书。对于不同的 SSID 认证，可以设置不同的服务器证书。初次使用内置 CA 颁发证书前，需要对内置 CA 进行初始化。

3.6.2. 有线认证

3.6.2.1. 控制器有线认证

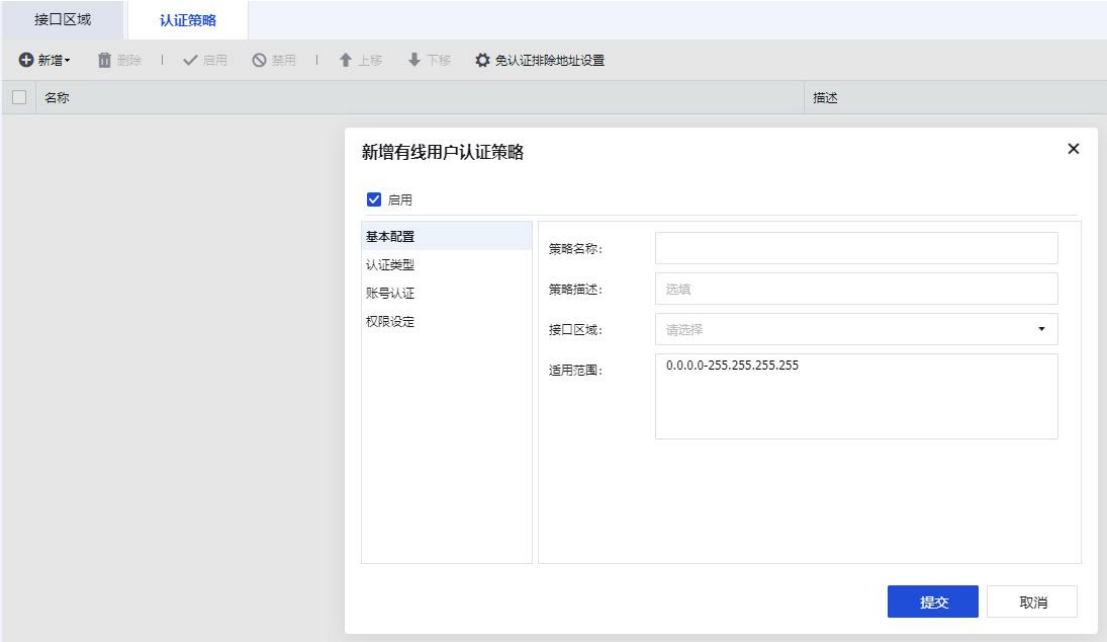
经过 NAC 控制器的有线用户，可以选择对有线用户进行认证。

接口区域

控制器认证配置，可以对认证做出一些特殊配置，比如通过定义非信任接口直接拒绝掉某个接口的所有流量，不再采取认证。

认证策略

认证策略的名称，只在选择数据通过时需要认证的接口。支持物理接口、聚合接口和 VLAN 接口，选择 TRUNK 模式的接口时可指定需要认证的 VLAN。只在选择需要认证的用户范围，支持 IP 地址及 MAC 地址



认证类型

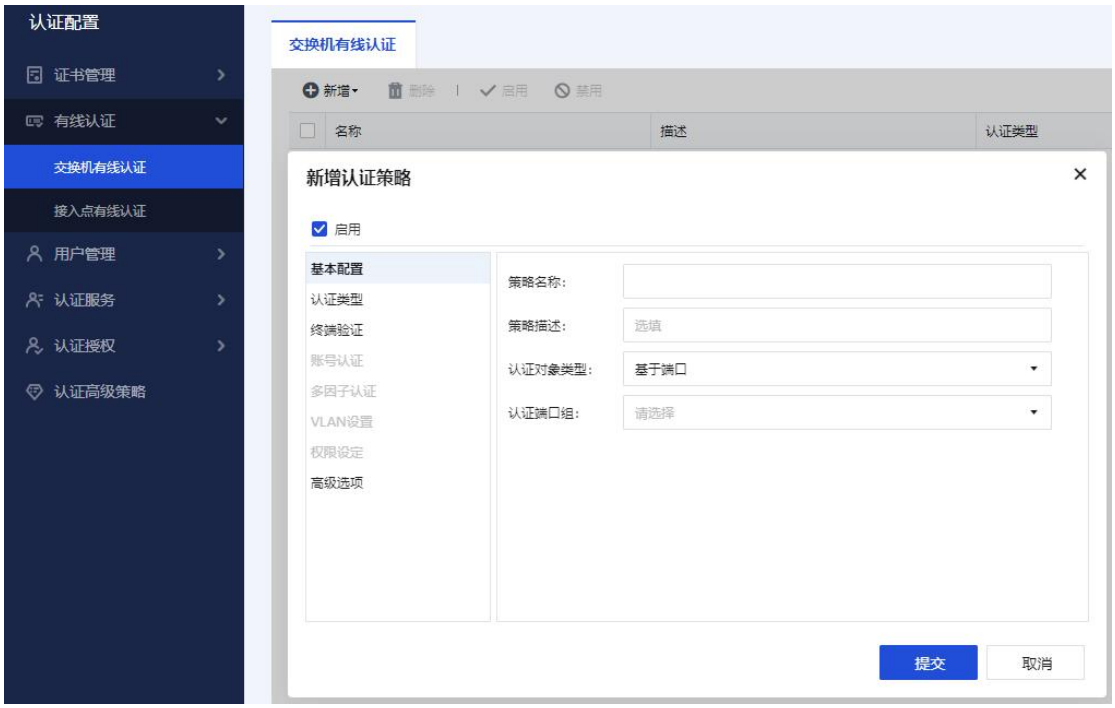
IP 地址认证，web 认证。IP 地址认证，无须认证即可连接到网络。web 认证：web 认证是指终端接入网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。

Web 认证支持在本控制器上进行 Portal 认证，此时选择【认证授权】-【portal 服务】-【web 认证策略】中添加的认证策略。也支持对接外部 portal 服务器进行 portal 认证。

3.6.2.2. 交换机有线认证

交换机有线认证

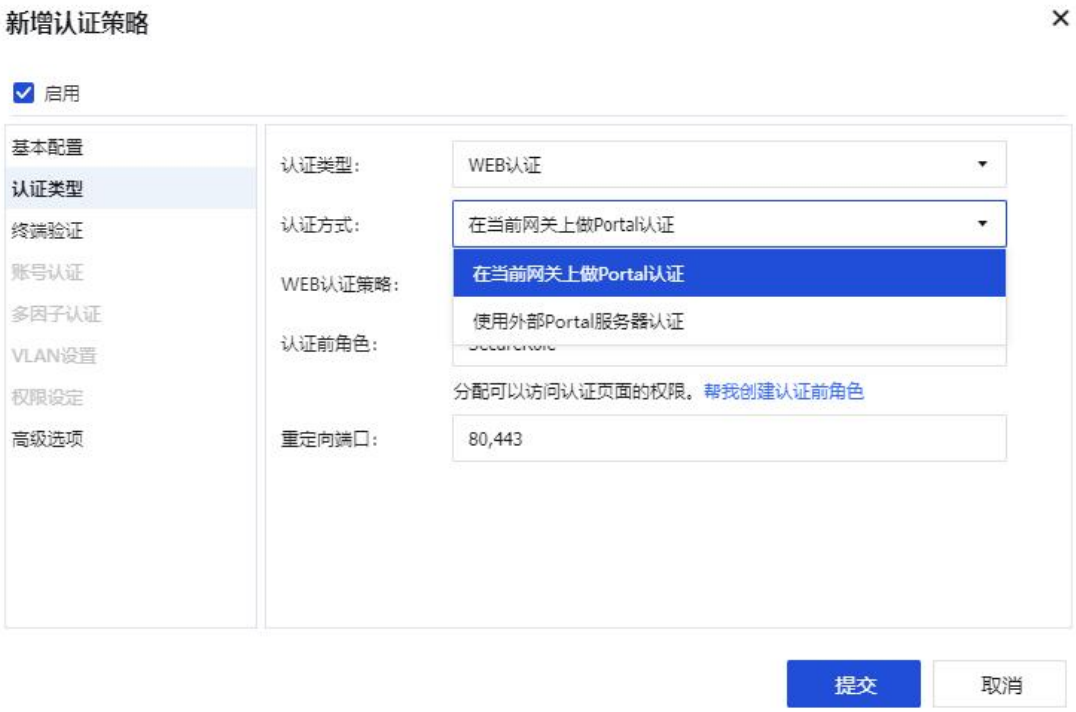
- 选择认证对象类型：支持基于端口与基于 VLAN 提供网络接入服务。
- 认证端口组：只在选择的认证端口组上提供网络接入服务。
- 认证类型：WEB 认证、802.1X 认证



WEB 认证

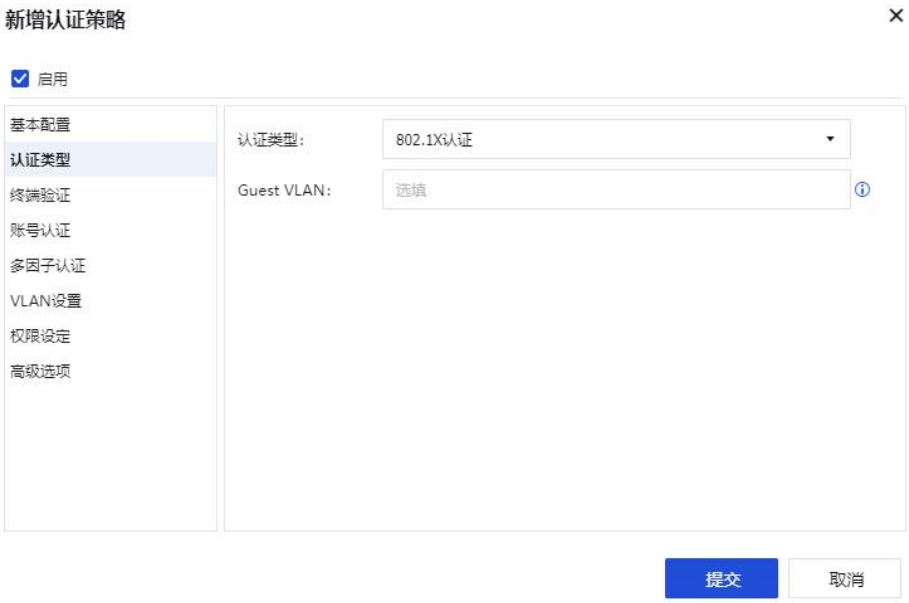
WEB 认证是指终端接入网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。

认证方式：提供在当前网关上做 Portal 认证和对接第三方 Portal 服务器认证的功能，这两种认证方式均需要用户先登录认证页面，输入用户名和密码进行认证，认证成功后才可以访问网络资源。



802.1X 认证

支持 802.1x 协议作为局域网端口的接入控制机制以解决以太网内认证和安全方面的问题。



在局域网接入设备的端口或者 VLAN 这一级，对所接入的用户设备进行认证和控制。连接

的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

终端验证：检查终端 MAC 黑名单、检查终端 MAC 白名单、免认证终端

MAC 黑名单对象定义了不允许连接网络的终端 MAC 地址列表。配置认证策略时，可设置为不允许 MAC 黑名单的终端连接网络。

检查终端 MAC 白名单：MAC 白名单对象定义了允许连接网络的终端 MAC 地址列表。配置网络时，可设置为允许 MAC 白名单的终端无需认证，直接接入网络。

免认证终端:配置不需要进行认证的终端 MAC，也可以配置不需要进行有线认证的交换机，并可分配免认证的角色。

两者的区别在于：

在当前网关上做 Portal 认证采用网关内置的 Web 服务器，采用内部 Portal 认证推送页面，用户通过账号和静态密码方式进行认证，部署简单，适合小型无线环境。

对接第三方 Portal 服务器认证认证采用外部 WEB 服务器，自定义 Portal 认证推送页面和认证成功跳转页面，搭配外部认证服务器、短信服务器，可以实现静态密码、短信动态密码等多种认证方式，并可实现广告推送等业务。

角色及 VLAN 设置：角色中定义了用户的网络访问权限，VLAN 定义了用户的子网。不同用户连接到网络后，可以设置不同的角色及 VLAN，从而实现子网划分，以及对网络权限的灵活控制。

系统将为每一个接入网络的用户分配唯一的角色及 VLAN。

角色分配及 VLAN 分配规则：用户认证成功后，系统将提取出用户此次认证过程的所有属性，主要包括：用户名，所属组，接入位置，RADIUS 服务器返回的属性值等；按照规则优先

级从上往下，为用户分配角色或 VLAN。

每一条规则中可以包含 1 个或多个条件，如果包含多个条件，则要求同时满足，才视为匹配此规则。如果用户未匹配规则表中的任何规则，则使用设定的 "默认角色" 和 "默认 VLAN"。

规则设定说明：

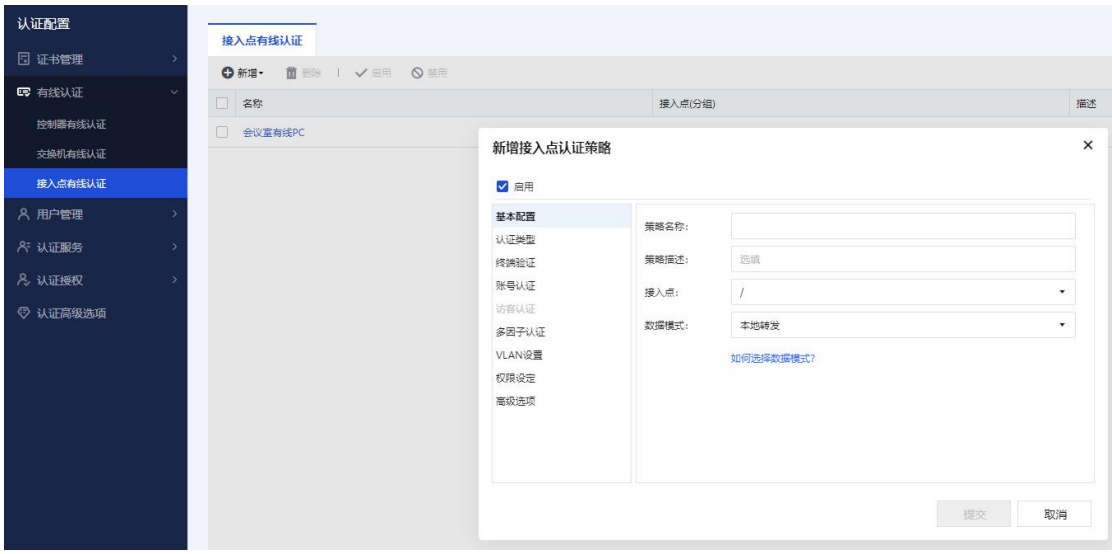
每一条规则中可以包含 1 个或多个条件，如果包含多个条件，则要求同时满足，才视为匹配此规则。

规则的值中，可以输入或者选择多个值，多个值间以英文逗号隔开。只用满足这些值中的一个，即视为满足此条件。

规则中的条件，可以选择"赋值给"。也就是把用户的属性值中保存了用户的角色及 VLAN。例如 RADIUS 的 Tunnel-Pvt-Group-ID 中，可能保存了用户的 VLAN。

3.6.2.3. 接入点有线认证

接入点有线认证，主要指接在 AP 上的有线用户的认证方式，不包括在 NAC 上进行有线认证的用户。



基本配置

基本配置，可以配置认证策略的名称，选择接入点（分组），只在选择的接入点（或分组）上提供网络接入服务。

数据转发模式： 集中转发模式中，接入点（AP）与 NAC 之间建立 2 层的数据隧道，用户的所有网络流量，通过此隧道传输到 NAC，NAC 再把流量转发到有线网络中。最简单的方法，可以把此模式理解为：相当于用户直接连接到 NAC。

本地转发是指用户的网络流量，由接入点（AP）直接转发到有线网络（不经过 NAC）。最简单的方法，可以把此模式理解为：接入点的无线用户直接连接到了接入点（AP）上联网卡所连接的有线网络。

认证类型

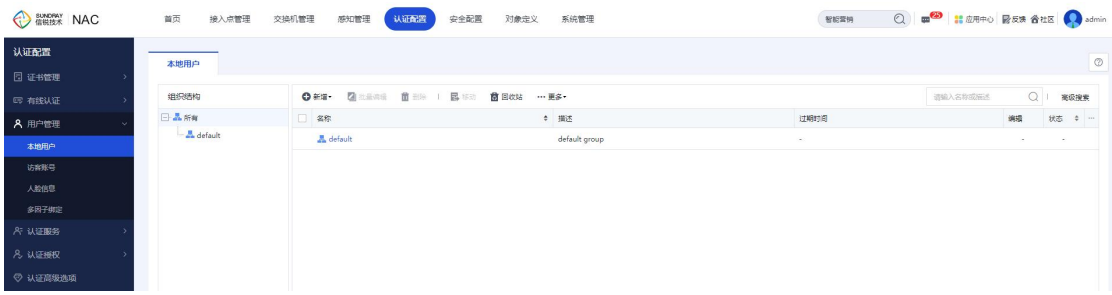
认证类型包括【IP 地址认证】和【web 认证】。IP 地址认证，无须认证即可连接到网络。

Web 认证，web 认证是指终端接入网络后，浏览器访问任意网址，都会被重定向到登录页面，用户在网页上输入用户名、密码等方式通过认证后才能访问网络资源。 有线认证配置类似于无线网络配置，可参考 3.3.2 节。

3.6.3. 用户管理

3.6.3.1. 本地用户

在未部署集中的账号数据库或认证服务器的环境中，无线网络的身份验证方法可以设置为本地用户认证。



用户组

本地用户数据库支持多级的组织结构树，可按照企业实际组织结构划分组，并进行分级管理。

用户名

用户名是账号的唯一标识，不同用户间不允许重名。用户身份验证过程中，需要输入此名称。

显示名

用户名由于要求唯一性，因此在部分部署环境中，用户名被设置为诸如员工工号等可读性较低的名称。这种情况下，可以把显示名设置为员工的姓名。系统将在“在线用户列表”等显示用户名的地方，同时显示账号的用户名及显示名，以更直观的对账号进行管理。显示名可以留空，不同用户的显示名允许重名。

描述

对账号的描述，选填。

过期时间

指定账号的过期时间点，过期后将无法通过身份验证。

登录时必须修改初始密码

本地账号是由管理员创建的，为了简化管理，不同账号的初始密码可能相同，这带来了严重的安全问题。选择此选项将要求账号在首次登录时，修改初始密码。

手机账号用户

适用于终端使用手机号码自助激活账号的场景。由用户在终端认证页面选择自助激活，管理员无需配置账号密码，用户在激活时自己设置密码。手机账号用户同时也支持短信二次认证。

邮箱绑定用户

适用于在用户忘记密码时，在终端认证页面上选择找回密码，系统将发送该用户的密码到绑定的邮箱。如果管理员在创建账号的时候未设置绑定邮箱，则由用户在首次登录的时候自己设置一个邮箱地址。

批量导入导出

csv 为通用表格文件格式，几乎所有的电子表格软件都支持此格式，例如 Microsoft Excel。在大量用户的情况下，通过 csv 表格文件管理，并导入到设备中，可以简化用户管理操作。

导入的表格文件列顺序及格式等，参考导入界面中的示例文件。

3.6.3.2. 访客账号

在部署用于访客使用的无线网络时，为了简化用户体验，通常设置为开放式的无线网络。但单纯的开放式的无线网络，存在无法验证访客身份的问题，因此通常需要设置认证方式。此方式主要部署在公众访问的无线网络中，例如部署在机场，交通枢纽，医院，酒店，商场，学校等地方。

通过访客认证的终端信息护记录在访客账号里。

3.6.3.3. 人脸信息

用于新增人脸账号并绑定底片。用户名必须在认证服务器中存在。

3.6.3.4. 多因子绑定

设置用户与终端绑定信息，相关的验证设置请在认证选项/策略中开启。支持终端绑定功能的有无线网络认证、有线认证和 Portal 服务认证策略。

3.6.4. 认证服务

3.6.4.1. Portal 服务

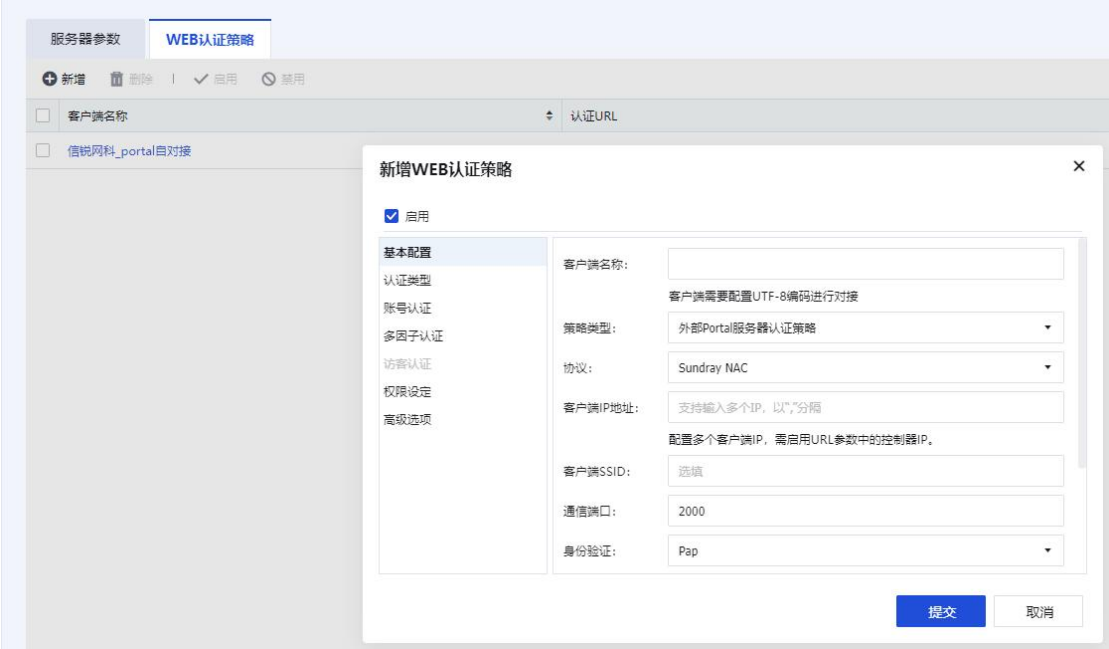
控制器可作为 Portal 服务器为第三方设备提供 Portal 认证服务。

服务器参数

- NAC 内置 Portal 服务器，Portal 服务器运行的必要参数。
- 协议端口：Portal 服务器监听的协议端口。
- 服务器通信 IP：当前控制器的通信 IP，双机部署时建议配置为 VRRP 中的虚拟 IP。
- 认证页面端口：默认是 80，配置为非 80 端口时，客户端配置 Portal 服务器的 URL 时需要带上端口号。
- 在线用户同步时间（分钟）：Portal 服务器主动向客户端同步用户的时间，针对 Aruba 和 Cisco 设备。
- 在线用户保留时间（小时）：超过保留时间，注销所有的在线用户。
- Portal 页面超时重定向地址：Portal 页面超时（在 URL 参数中设置时间戳参数）后系统自动重定向的地址.

3.6.4.1.1.WEB 认证策略

WEB 认证策略给当前控制器的有线认证，第三方的 Portal 客户端（包括信锐控制器）对接时，配置认证页面、认证方式、权限设定方面的信息。



策略类型：分为外部 Portal 服务器认证策略、控制器有线认证策略和交换机有线认证策略。外部 Portal 服务器认证策略是指给当前设备的无线网络对接第三方(包括信锐控制器)的 Portal 客户端对接。控制器有线认证策略是指给当前控制器的有线策略提供对接。交换机有线认证策略是指给安视交换机的有线策略提供对接。

协议：当前 Portal 服务器支持对接的设备厂商类型和协议版本。不在列表里面的请选择 Portal2.0 标准协议。

身份验证：身份验证方法，包括 PAP 和 CHAP，这里的配置需要和客户端配置的 RADIUS 服务器的身份验证方法保持一致才能认证成功。

认证 URL：需要将这个 URL 拷贝到 Portal 客户端的认证 URL 里面去，客户端配置的和这里的不一致时，将会认证失败。

参数设置：Portal 客户端的认证 URL 里面携带的参数的名称。

开启本地认证（在控制器进行用户认证）：Portal2.0 协议里面，Portal 服务器和认证服务器可以分开配置。当 Portal 服务器启用了访客认证时，客户端的 RADIUS 服务器需要配置

为当前控制器。

权限匹配：Portal 服务器对接有线认证时，权限匹配的结果就是有线认证的角色。提供给第三方设备 Portal 对接时，匹配到的角色将会通过 RADIUS 报文中的 Class 字段，以字符串的形式返回给 RADIUS 客户端。

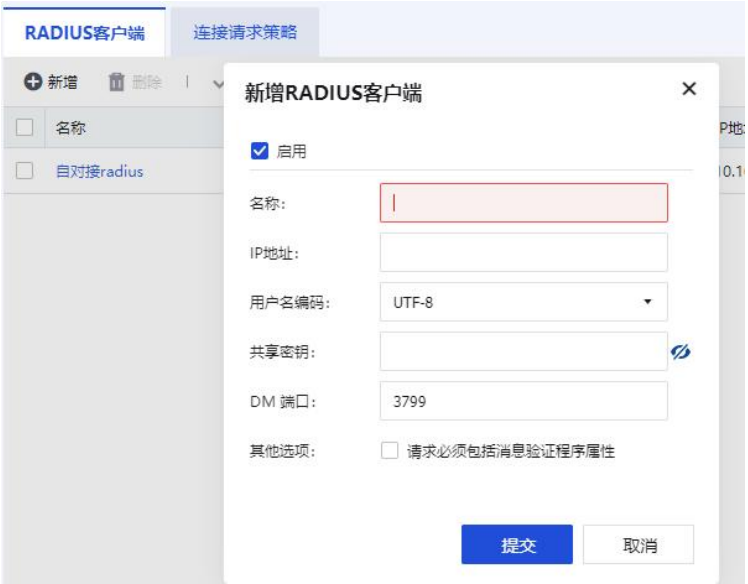
3.6.4.2. Radius 服务

Radius 服务器负责接收客户端的连接请求、认证用户，然后返回客户端所有必要的配置和认证信息。

Radius 客户端

NAC 作为 Radius 服务对客户端进行认证和计费时，需要配置信任的客户端；

NAC 作为 Radius 客户端需要配置认证的服务器时请在外部服务器进行配置。



1、Radius 客户端—名称

Radius 客户端的名称，用于区分不同的 Radius 客户端。

2、Radius 客户端—IP 地址

客户端的 IP 地址，双机部署时建议配置为 VRRP 中的虚拟 IP。

3、Radius 客户端—用户名编码

服务器和客户端之前数据传输的编码类型，两端的编码一致才能保证验证的有效性。

4、Radius 客户端—共享秘钥

客户端和服务通过该共享密钥建立信任，两端密钥一致才可以建立信任。

5、Radius 客户端—其他选项

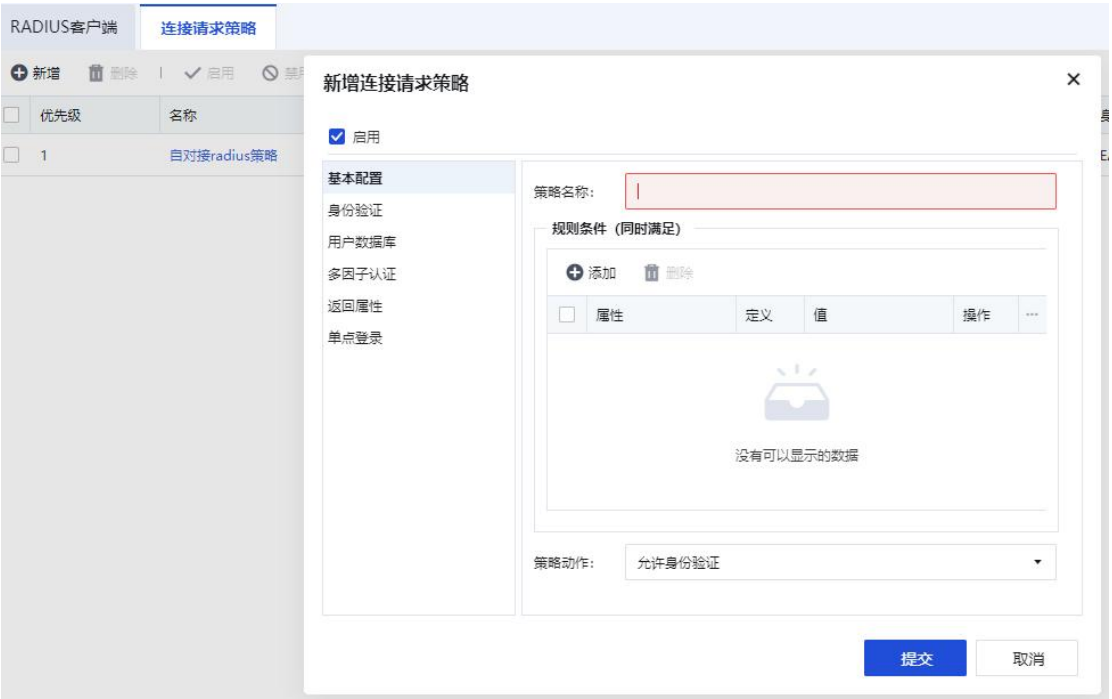
当勾选了“请求必须包括消息验证程序属性”表示请求的消息必须包含 Message-Authenticator 属性。

6、高级选项

配置 Radius 服务器的认证和计费端口，必须与客户端配置的端口一致。

连接请求策略

认证的的策略配置，连接请求策略有优先级，当优先级高的策略为允许策略时，配置失败则不通过验证，当优先级高的策略为拒绝策略时，配置失败时则跳转至下一策略进行验证。



➢ 策略动作

允许或者拒绝匹配该策略的用户通过认证。

➢ 规则条件

通过传输 RADIUS 属性的值进行匹配。

➢ 用户数据库

选择认证数据的数据库（数据库需在在外部数据库进行配置）。

➢ 删除用户名前后缀

可以定义用户名的前、后缀，验证的用户名会删除定义的前、后缀再进行验证。

➢ 身份验证方法

认证的协议的选择，为了保证认证的有效性，请确保选择的身份验证方法包含了需要处理的认证协议类型。

➢ 多因子认证

- 可以启用、禁用新终端需要 TrustSpeed 审批。启用[新终端需要 TrustSpeed 审批]功能后用户接入网络需要在 TrustSpeed 内进行二次生物识别授权验证，以增加账号的安全性。授权方式分为：[直接授权]、[人脸识别]、[faceID/touchID/手势识别]、[人脸识别、faceID/touchID/手势识别]。
- 直接授权：APP 内点击无线网络、审核消息、扫描二维码，无需生物识别验证而直接通过授权。
- 人脸识别：APP 内点击无线网络、审核消息、扫描二维码，需校验人脸识别验证授权。

- faceID/touchID/手势识别：APP 内点击无线网络、审核消息、扫描二维码，需校验 faceID、touchID、手势识别中的 1 种方式验证授权。
- 人脸识别、faceID/touchID/手势识别：APP 内点击无线网络、审核消息、扫描二维码，需先人脸识别，如果人脸失败则校验 faceID、touchID、手势识别中的 1 种方式验证授权。

➢ 返回属性

RADIUS 服务器端[返回属性]功能是用于让 RADIUS 客户端可以根据返回的属性值，做一些角色匹配、VLAN 分配等等附加功能。

支持按规则配置返回属性和默认返回属性两种方式。

例如：客户端希望用户[张三]在服务端认证完成后以 RADIUS 属性 Filter-Id 返回一个角色[role1]，用于分配该用户的上网权限为[role1]。

按规则返回属性中添加如下条件：

属性:RADIUS User Name 定义:等于 值:字符串[张三]

满足条件后返回属性：

属性:Filter-Id 值:字符串[Role1]

属性标识：

用于定义 RADIUS 客户端返回的哪种属性值用于给 RADIUS

3.6.4.3. TrustSpeed 服务

用于配置人脸识别认证相关功能。

3.6.4.4. 认证漫游域

认证漫游域主要解决如下问题：

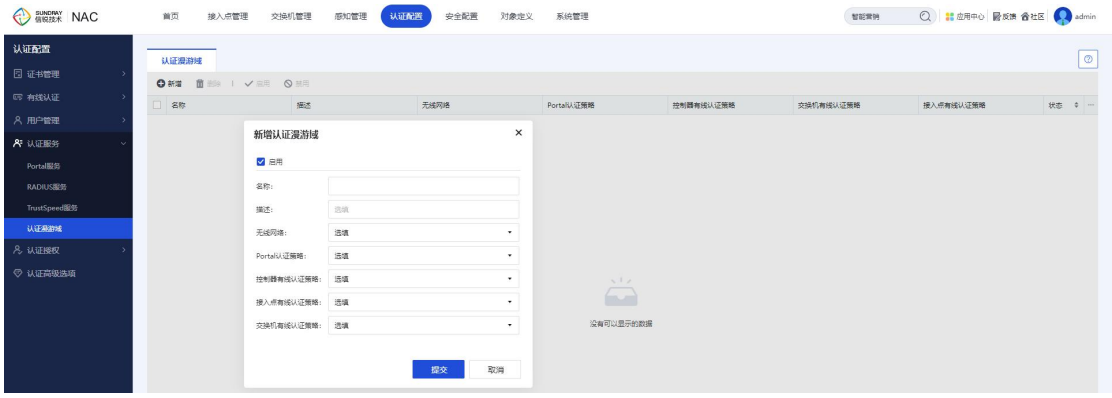
1、客户有多台不同厂商的 portal 客户端，终端在客户端 A 上认证成功后，漫游到控制器 B 后需要重新认证；

2、客户的第三方设备级联到控制器的接口做有线认证后，漫游到控制器的其他 ssid 上后需要重新认证。

配置认证漫游域后，支持终端在不同类型的 portal 服务器上漫游；支持不同类型认证方式之间的漫游。

注意：只有相同的认证服务器的认证策略才能添加到一起，并且只支持账号认证，访客认证

本身就支持漫游。



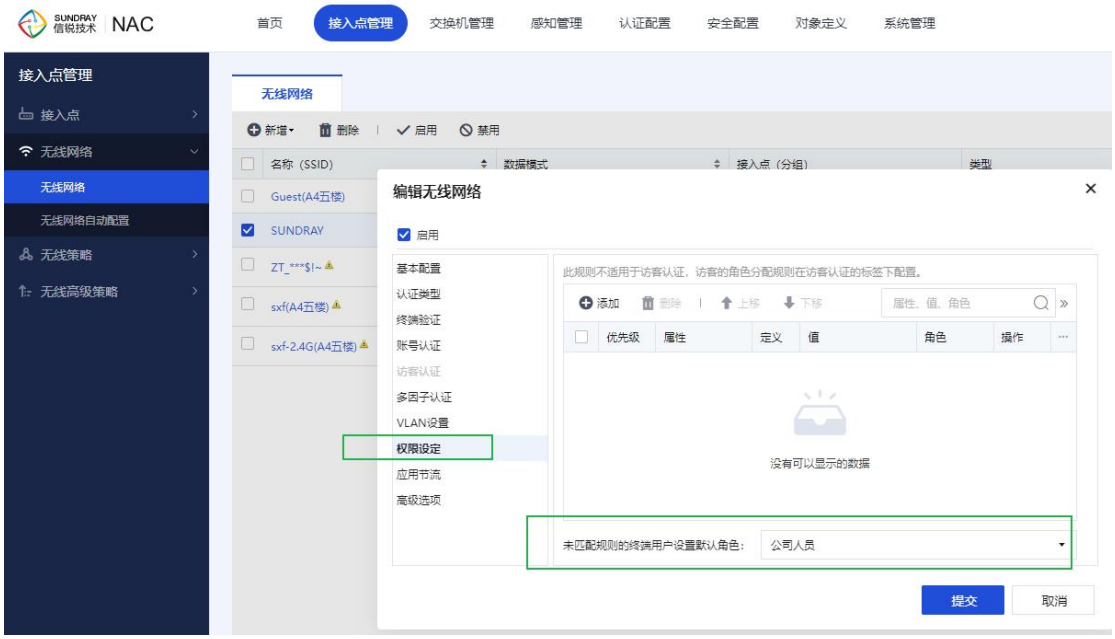
3.6.5. 认证授权

『认证授权』包含【角色授权】、【Web 认证】、【微信认证选项】、【外部服务器】、【单点登录】、【本地转发应用策略】。

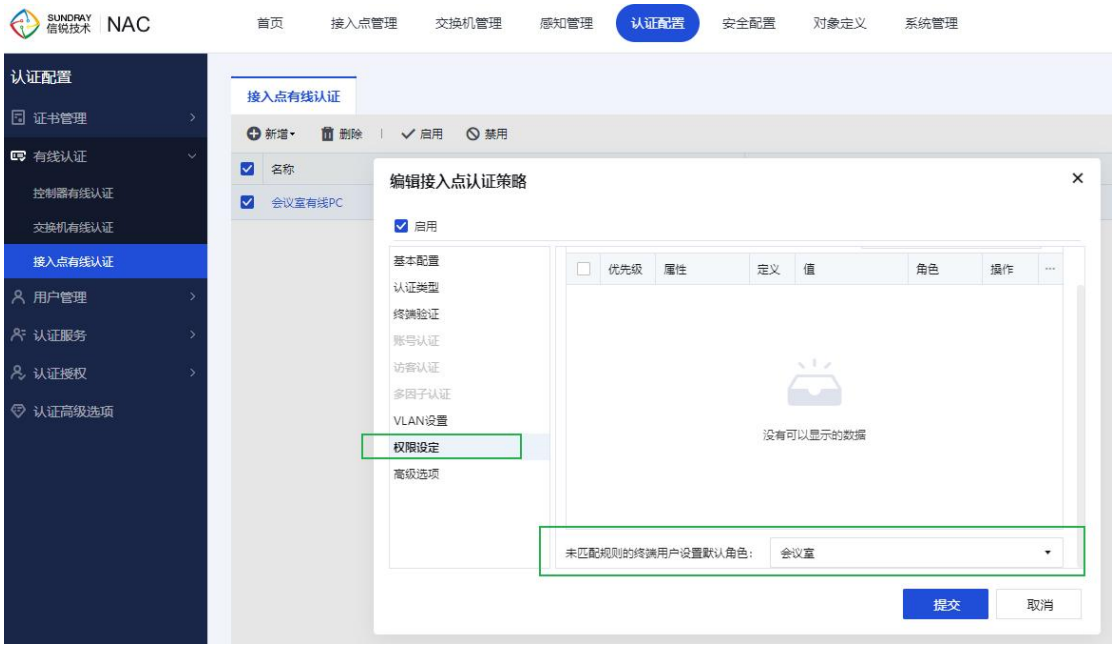
3.6.5.1. 角色授权

『角色授权』定义了用户可以访问网络的各种权限设定，包括【角色授权】、【有线访问控制策略】、【无线访问控制策略】、【用户审计策略】、【流速限制策略】、【流量/时长配额策略】。

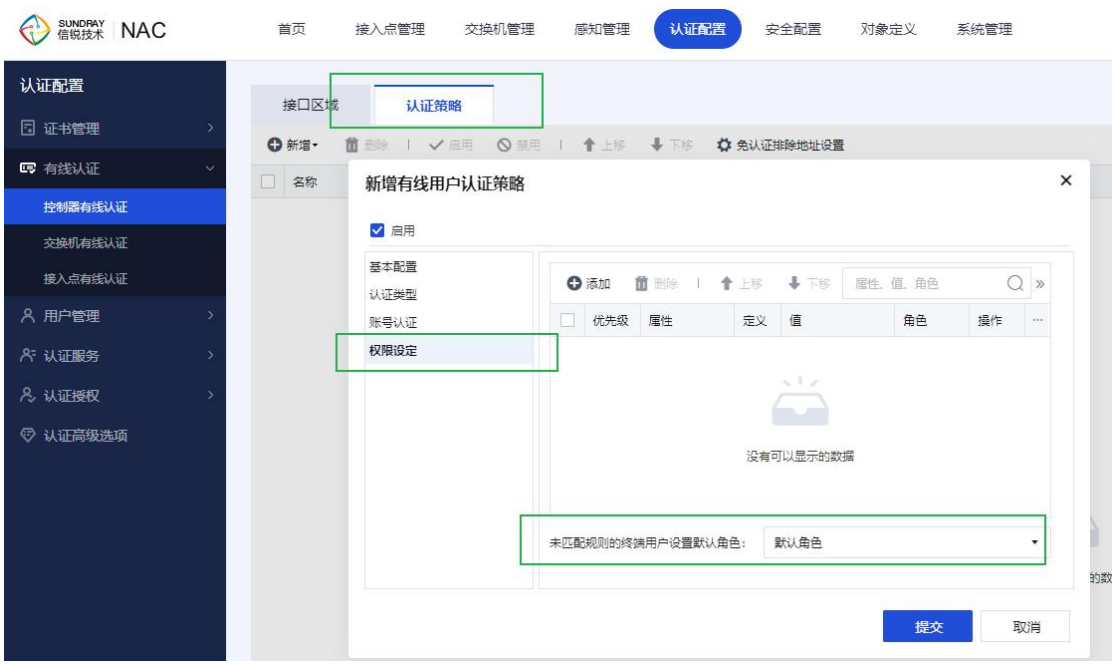
角色授权设置好后，并没有立刻被使用生效，需要在【接入点管理】-【无线网络】-【编辑无线网络】-【权限设定】中调用角色，匹配给无线用户。



另外【认证配置】-【有线认证】-【接入点有线认证】-【编辑接入点认证策略】-【权限设定】可以定义了经过 AP 的有线用户的角色，如下图：



在【认证配置】-【有线认证】-【控制器有线认证】-【认证策略】定义了直接经过 NAC 的有线用户的角色，如下图：



角色授权

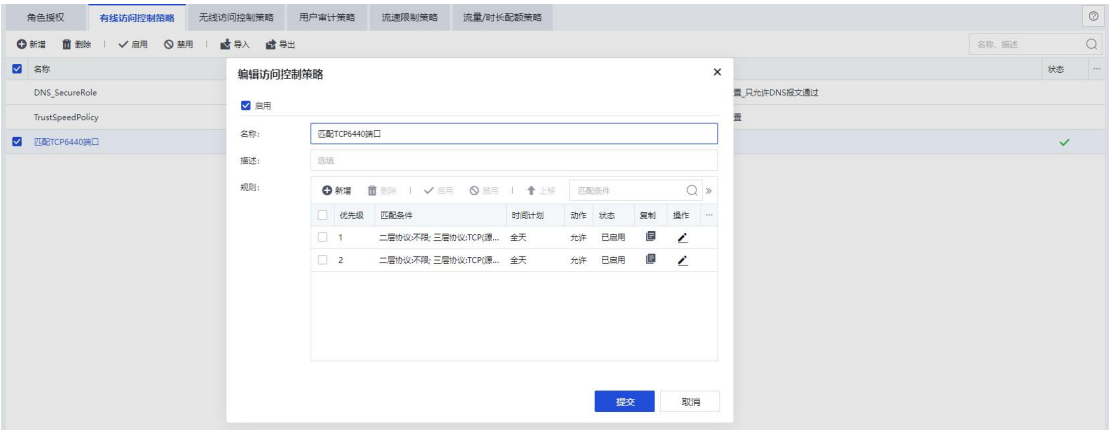
角色授权可以新增角色，然后调用左侧已经建立成功的有线、无线访问控制策略、用户审计策略、和流速限制策略、以及流量/时长配额策略，也可以在角色授权中调用新增其他策略。

有线访问控制策略

有线访问控制策略中，包含一条或多条网络访问权限规则，是一个有序的规则的集合，通过匹配报文中信息与规则中参数来对数据包进行分类，并执行规则对应的动作。未匹配任何有线访问控制规则的流量，动作为放行。

参数包含源/目的 IP 地址、源/目的 MAC 地址、VLAN ID、二层/三层协议、时间计划。

- 源/目的 IP 地址：支持使用以太网帧的源 IP 地址（地址段）或目的 IP 地址（地址段）来定义 ACL 规则。
- 源/目的 MAC 地址：支持使用以太网帧的源 MAC 地址或目的 MAC 地址来定义 ACL 规则。
- VLAN ID：支持使用以太网帧的 VLAN ID 来定义 ACL 规则。
- 二层/三层协议：支持使用二层/三层网络协议来定义 ACL 规则，包括 ARP、RARP、ICMP、TCP、UDP、IGMP、IP、OSPF 等协议。
- 时间计划：时间计划是指 ACL 规则生效的时间段，表示仅在指定时间段内按该规则过滤。

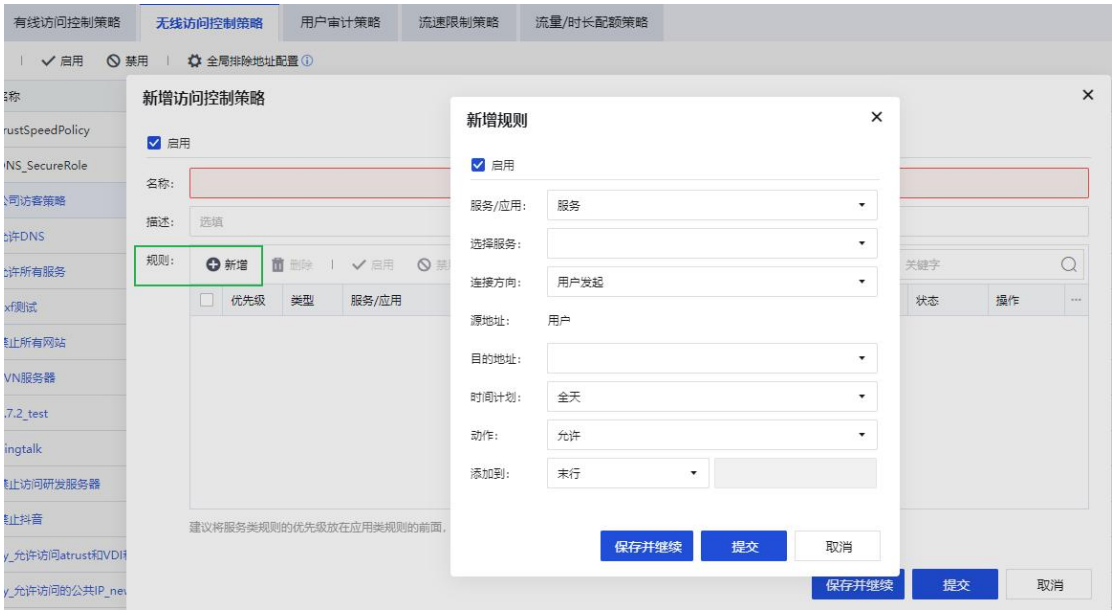


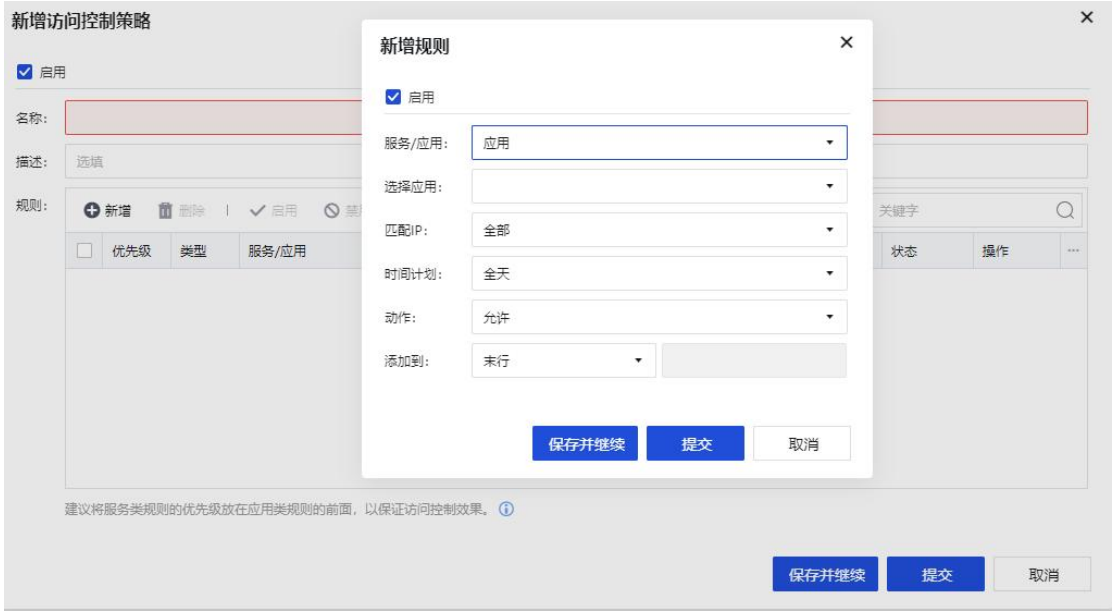
无线访问控制策略

访问控制策略主要是用来限制无线终端用户可以访问的网络权限，一般网络设备设置网络权限会有 LAN 区域和 WAN 区域的划分，WLAN 不设置 LAN 区域和 WAN 区域的划分，只需要设置【用户发起】和【用户接收】2 个方向即可，配置策略还需要调用到对象定义中的【服务】、【应用】、【IP 组】以及【时间计划】。

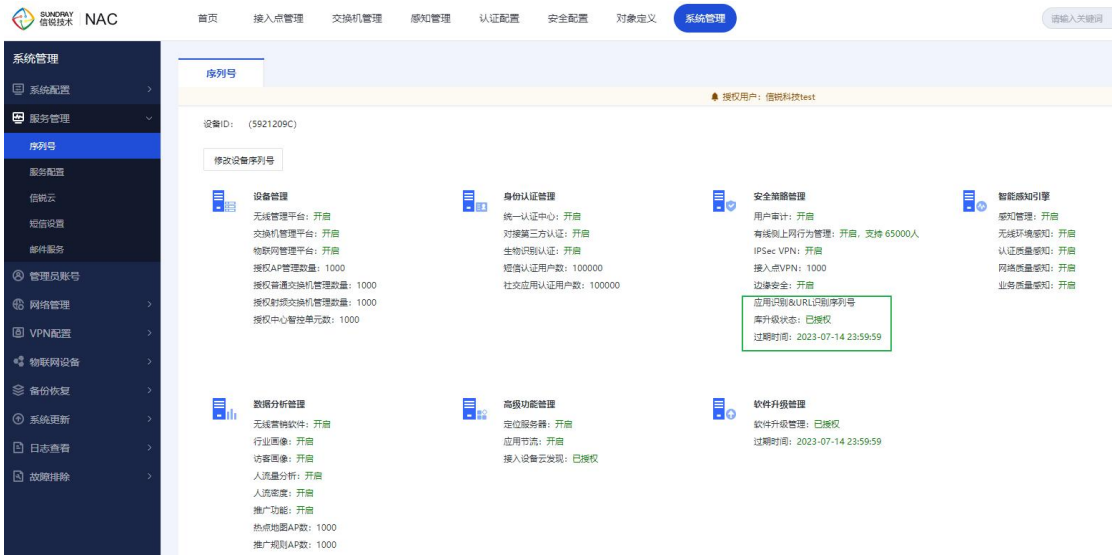
[编辑访问控制策略]：可以新增多条访问控制策略，并且可以设置不同的优先级，策略会依次从上往下匹配。

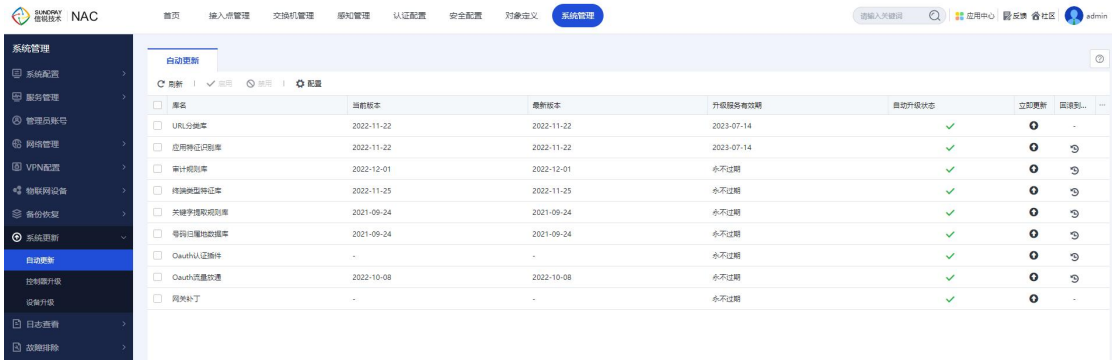
新增规则





选择服务时，会调用【对象定义】中的服务，选择应用时，会调用【对象定义】中的应用。需要调用【应用】前，需要确保设备已经开启应用识别序列号，并且应用识别规则库与 URL 规则库需要处于最新状态。

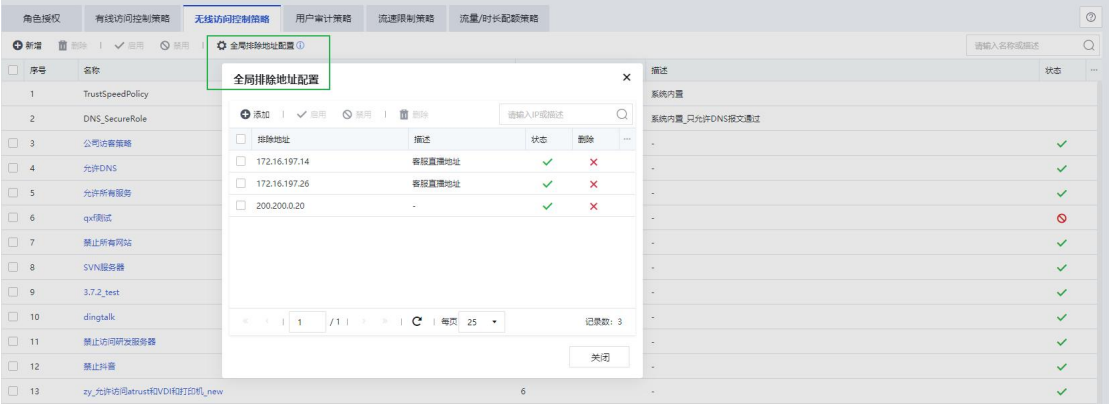




URL 规则库如果未处于最新状态，会影响基于应用的访问控制策略的正常生效，需要点击立即更新更新到最新版本。

全局排除地址

添加到全局排查地址的 IP 或域名不受访客控制策略的限制



用户审计策略

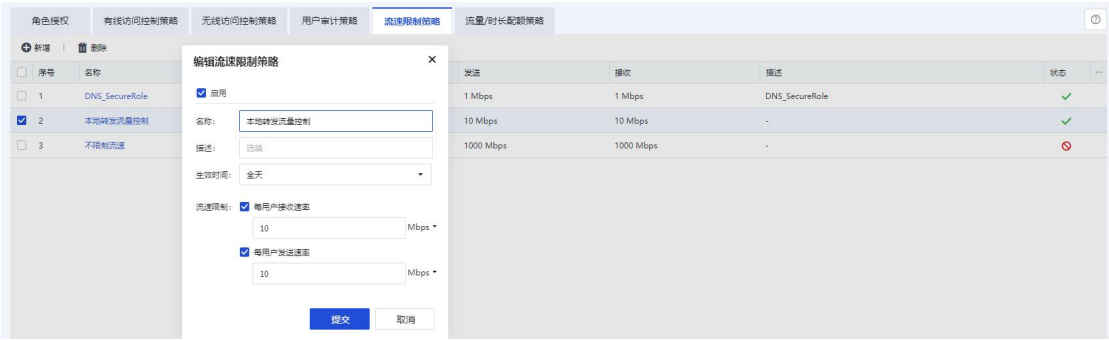
用户审计策略支持审计 HTTP 外发内容、访问网站/下载、邮件、FTP、telnet、网络应用、流量与上网时长。

HTTP 外发内容，包括 WebBBS 发帖、外发的 WebMail 邮件、通过网页上传的附件，通过网页上传的文本，微博等方式。HTTP 外发内容审计，不包括 HTTPS 方式的内容审计。

访问网站/下载，包括了 URL 规则库中所有类型的站点。邮件包括了标准的 SMTP/POP3 以及 IMAP 方式的邮件。FTP 包括 FTP 上传文件，也可以被审计，超过 50M 的文件，只会截取前 50M 文件大小。对于采用 SSL 加密的内容无法审计，比如 https 与 SMTPS/POP3S 等内容。

流速限制策略

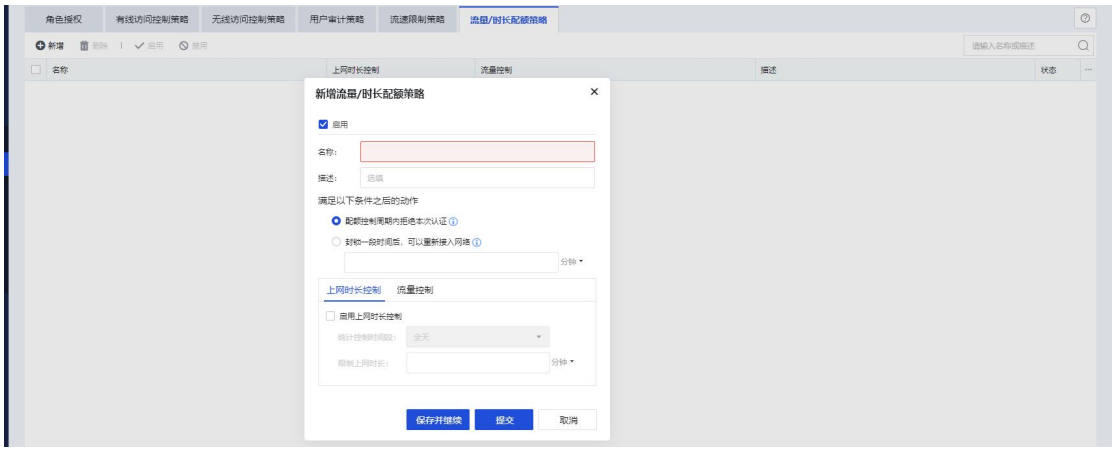
流速限制策略可以针对所有终端用户生效，包括有线与无线用户，但此功能只能限制用户的整体上行和下行的速率，无法根据应用进行流控，应用流控需要到【流控与安全】菜单下配置。该功能策略如下图：



流速限制策略可以对每一个终端进行流速限制，以避免部分终端的流速过大，影响整体无线用户体验。例如设定为发送最大限制为 512KB/s，则对使用此策略的每一个终端最大发送流速都将被限制为 512KB/s 秒。

流量/时长配额策略

流量/时长配额策略可以限制用户的上网时长和总流量大小，可以设置一个上网时长或者流量的阈值(上网的最大时长或者能使用的最大流量)，可以设置当用户上网达到这个阈值后在配额控制周期内不能再次进行认证或者只封锁一段时间后可以重新接入网络。

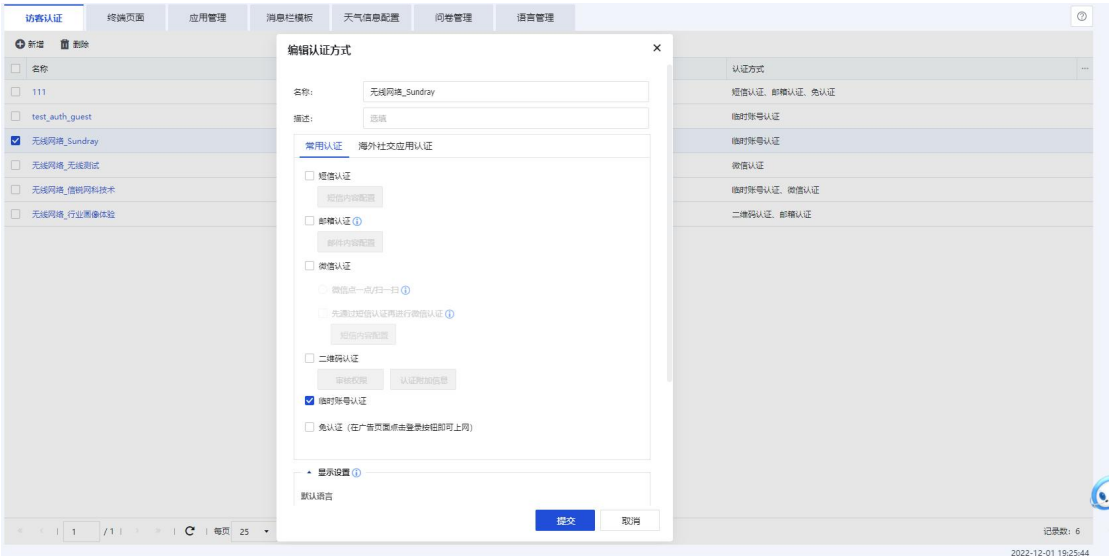


3.6.5.2. Web 认证

『Web 认证』包括【访客认证】、【终端页面】、【应用管理】、【消息栏模版】、【语言管理】、【问卷题库】、【问卷分析】七个模块

访客认证

在部署用于访客使用的无线网络时，为了简化用户体验，通常设置为开放式的无线网络。但单纯的开放式的无线网络，存在无法验证访客身份的问题，因此通常需要设置认证方式。此方式主要部署在公众访问的无线网络中，例如部署在机场，交通枢纽，医院，酒店，商场，学校等地方。



➢ 短信认证

启用短信认证时，需要到【系统管理】-【短信服务】页面配置短信设备，包括采用短信猫，外置短信服务器或外置短信网关。

短信认证是指访问无线网络时，系统需要发送短信验证码到用户的手机上，用户输入验证码后，才能访问无线网络，此方式获取了访客用户的手机号码作为身份信息。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。
2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。
3、认证页面中，输入用户的手机号码，系统将把验证码发送到此手机。
4、认证页面中，输入短信中获取的验证码，通过认证。

短信认证方式的优点：

1、认证页面中，可以设置企业的广告等展示信息，提高企业形象。
2、可以获取访客的手机号码用于后续的短信营销。
3、简化了访客连接无线网络的体验。

➢ 邮箱认证

邮箱认证是指访问无线网络时，系统需要发送验证码及授权 url 发送到用户的邮箱上，用户输入验证码或者点击授权 url 后，才能访问无线网络，此方式获取了访客用户的邮箱地址作为身份信息。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。
2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。
3、认证页面中，输入用户的邮箱地址，系统将把验证码和授权 url 发送到此邮箱。
4、认证页面中，输入邮箱中获取的验证码或者点击授权 url，通过认证。

邮箱认证方式的优点：

1、迎合了国外使用邮箱较多的习惯，提升用户体验。

2、认证页面中，可以设置企业的广告等展示信息，提高企业形象。

3、可以获取访客的邮箱地址用于后续的邮件营销。

4、提供点击链接认证上网的方式，简化了访客连接无线网络的体验。

➢ 微信认证

此方式通常用于商场、超市的无线网络认证，可以确保只有关注过指定微信公众账号的访客用户才具备无线网络访问权限。认证选项中，可以设置关注微信后，每次申请上网的有效期。

访客连接无线网络的过程如下：

1. 连接到开放式的访客无线网络，例如无线网络名称为：Example-WeChat。
2. 打开浏览器，访问任意网站，系统将把用户的浏览器重定向到指定的认证页面，点击认证页面上的微信连 WiFi 按钮跳转到微信完成微信认证。

PS：微信连 WiFi 相关参数需从微信公众平台后台获取后填入控制器。

➢ 二维码认证

此方式通常用于企业的访客无线网络认证，可以确保只有经过二维码审核的访客用户才具备无线网络访问权限。认证选项中，可以设置审核通过后，访客可以访问无线网络的时长。

访客连接无线网络的过程如下：

1、连接到开放式的访客无线网络，例如无线网络名称为：Example-Guest。

2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。

3、认证页面中，显示一个二维码。

4、访客的接待人员，也就是企业的内部员工，使用手机连接到企业无线网络中，并具备审批权限。审批权限由无线网络配置中指定，可以设置哪些角色的用户具备访客审批权限。

5、接待人员，打开手机中的二维码应用，扫描访客的二维码，访客即通过审核。需要说明的是，目前很多流行的互联网应用都提供了二维码扫描功能，例如腾讯微信(用此软件的时候需要审核人角色必须能正常访问互联网，因为此软件二维码扫描的时候要访问互联网才能正常使用)和我查查。

➢ 临时访客认证

此方式通常用于企业、酒店的访客无线网络认证，可以在访客登记后，接待人员创建一个临时帐号，并设置帐号的有效期。访客使用此帐号完成无线网络认证。

以酒店的部署场景为例，顾客连接无线网络的过程如下：

1、顾客在酒店前台登记入住。
2、酒店的前台工作人员，在访客管理系统中，为此顾客添加一个临时帐号，以手机号或者身份证号码作为帐号的用户名，密码为手机号码或身份证号码的后 6 位。帐号的有效时间设置为顾客的离店时间。
3、顾客连接到酒店部署的，开放式的无线网络，例如无线网络名称为：Example-Guest。
4、打开浏览器，访问任意网站，系统将把浏览器重定向到认证页面。
5、在认证页面中，输入此临时帐号及密码，完成无线网络认证。
6、顾客离开酒店后，帐号自动失效。

访客帐号通常并非由网络管理员管理，而是由负责访客接待的人员管理。因此，系统提供了临时帐号管理员，以区别于 NAC 的管理员。临时帐号管理员只允管理访客帐号，无法修改 NAC 的其它设置。

临时帐号管理员的登录地址与 NAC 管理员不同，登录地址为： https://设备地址/guest.php，例如：https://192.168.0.1/guest.php

➢ 免用户认证

免用户认证是指访问无线网络时，访客无需认证，在广告页面点击登录按钮即可上网。

访客连接无线网络的过程如下：

1、连接到访客无线网络，例如无线网络名称为：Example-Guest。
2、打开浏览器，访问任意网站，系统将把用户的浏览器重定向到认证页面。
3、认证页面中，用户点击登陆，直接上网。

免用户认证方式的优点：

1、认证页面中，可以设置企业的广告等展示信息，提高企业形象。
2、简化了访客连接无线网络的体验。

➢ 社交应用认证

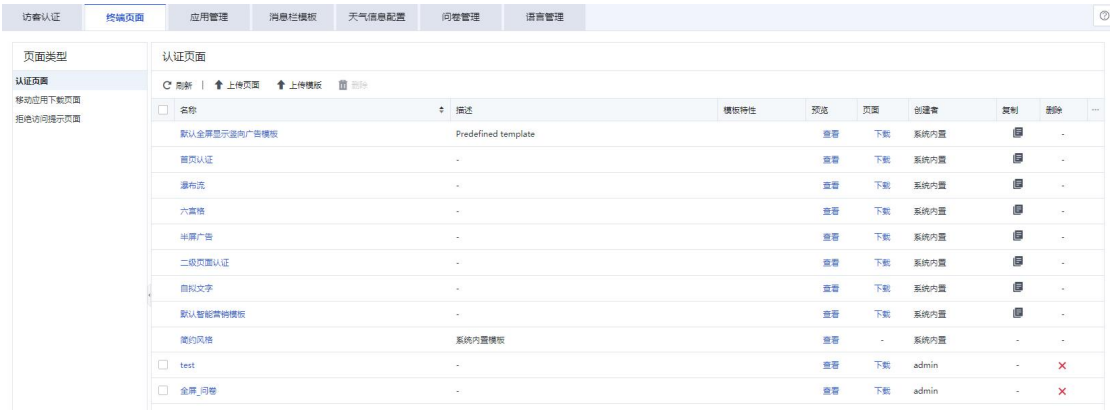
此方式通常用于海外或港澳台等地区，终端用户可以使用 Facebook，Twitter，Line，Live，Instagram 账号进行授权，授权后关注商家账号即可通过认证。

通常，通过认证的用户，控制器可以获取到用户的用户 ID、用户名、终端 MAC 地址、邮箱地址、性别、年龄段等。但上述字段在用户没有配置的时候，是获取不到的。

配置社交应用认证时，认证前需要放通对应流量，推荐使用内置角色进行认证。

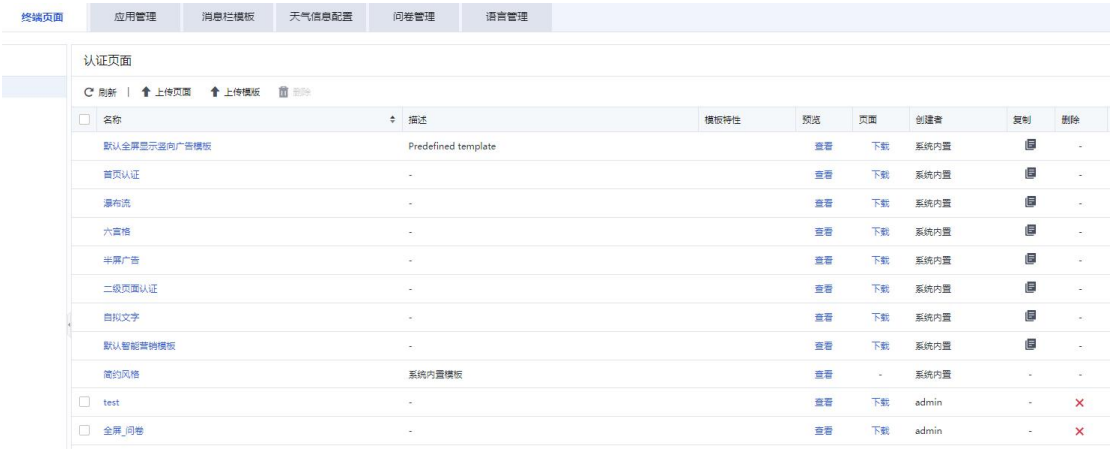
终端页面

【终端页面】分为“认证页面”、“移动应用下载页面”、“拒绝访问提示页面”。



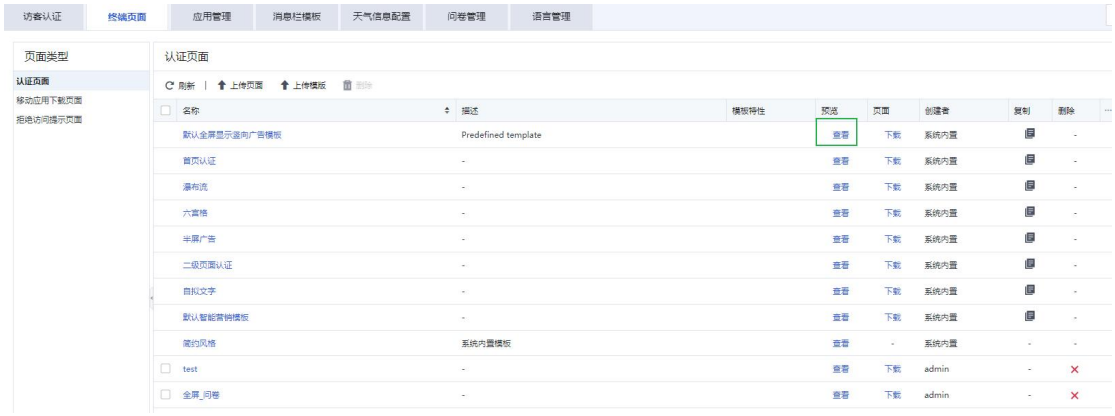
➢ 认证页面

“认证页面”用于设置无线用户接入无线网络后，设置 WEB 认证跳转的页面，系统内置了 Web 认证页面的模板，系统允许您在默认模版的基础上，自定义认证页面的标题，背景，LOGO 等。如果您熟悉 Web 开发，可以上传自定义的页面。

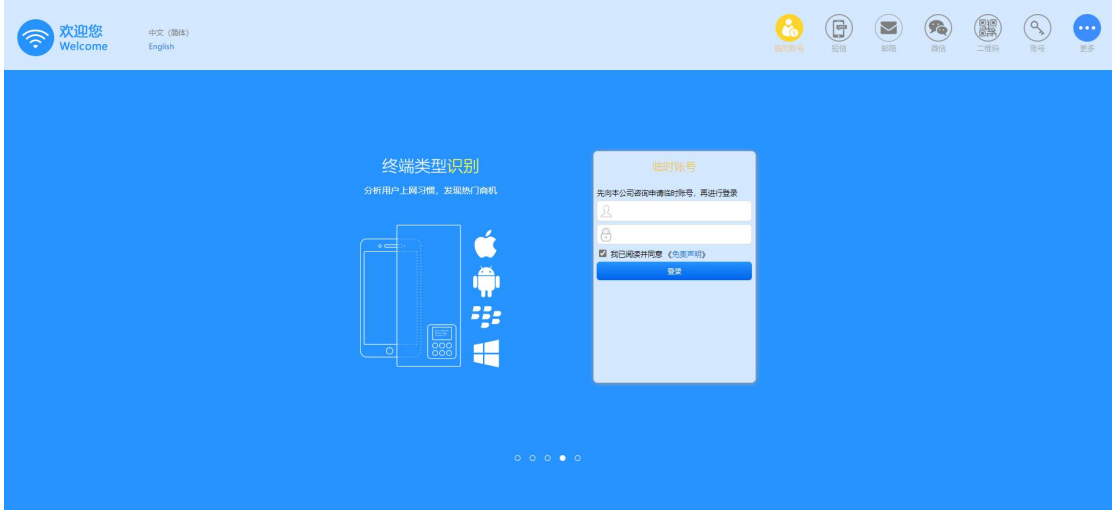


1、默认全屏显示竖向广告模板

点击查看可查看 PC 端和手机端预览图，以下几种模板查看方式同理。



预览电脑认证效果图：



预览手机认证效果图：

2、自拟文字

3、瀑布流

4、半屏广告

5、二级页面认证

6、六宫格

7、默认智能营销模版

智能营销模板支持更加丰富的区域显示规则，帮助营销人员结合天气环境情况，推送与顾客直观感受相吻合的广告内容，能让每个顾客看到与自己相关的"专属"信息，做到千人千面的展示效果。

支持一套模板多个门店使用，且不同门店展示不同广告内容。每个门店(单条显示规则）均支持引用接入点分组并配置多张广告图片，每张广告图片可以设定不同环境属性、用户属性、所在位置、推送时间进行智能展示。

支持每个显示规则引用不同的消息栏，以个性化的展示消息栏信息。消息栏信息可以在消息栏模板页面进行配置。

统一配置：在总部、多个门店场景下，可以启用统一配置，用于在指定生效时间内强制展示总部设定的广告内容，若部分门店不展示总部统一广告可以进行排除。

注：统一配置禁用或生效时间外，各门店恢复显示门店设定的独立广告内容。

页面效果图，参考“默认全屏显示竖向广告”。

➢ 上传自定义页面

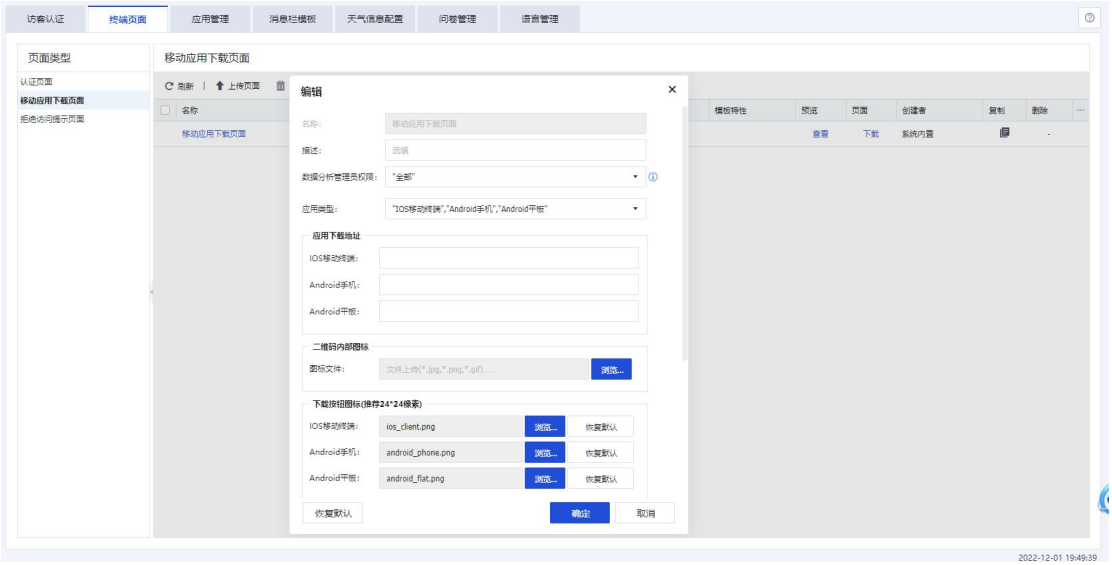
如果系统默认的认证页面还不能满足需求，还可以自定义页面，自定义页面需要下载“自定义模版示例”，按照示例标准进行上传页面

➢ 访问拒绝页面

当用户被访问控制策略拒绝时，可以启用页面返回，提示用户访问被拒绝，也可以自定义编辑。

➢ 移动应用下载页面

当您需要做手机应用推广时，需要先创建一个移动应用下载页面。在无线网络设置认证后跳转页面，勾选 APP 推广，再选择此处创建的页面。如果您使用了 APP 推广，别忘了在无线网络设置中开启应用缓存加速，这将大大节省您的网络带宽资源，提升终端下载体验。当前适配 IOS 和 Android 移动终端，移动终端访问时可直接下载，PC 端访问时将显示一个二维码图片，提示用户使用移动终端扫码下载。



应用管理

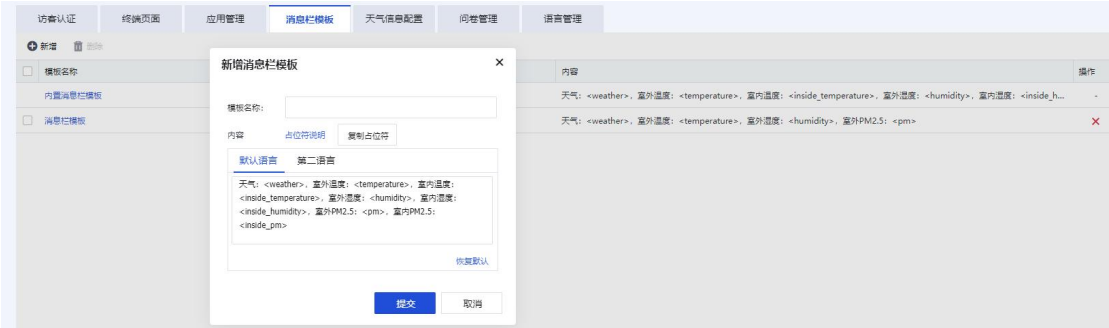
应用管理用于配置各种社交软件做认证时所要对接的应用，以让不同社交软件的用户使用自己的社交账号接入 wifi。同时支持 like 功能，实现商超客户的品牌推广，目前支持 like 的社交软件有 Facebook，Twitter 和 Line。

消息栏模版

消息栏的展示文字在终端页面的顶部，可以根据识别出的终端用户的系统语言，对应展示其相符合的语言文字。消息栏内容支持展示天气、室内外温度、湿度、PM2.5，使终端用户能直观在认证页面看到当前所处场所的环境信息。

通过修改内置消息栏模板文字，或者新增消息栏模板，可以由客户定义想要给终端用户展示的内容。

注意，此处的模板内容和语言管理中的语言模板内容相互独立，以便客户快速编辑。



天气信息配置

➢ 区域环境参数

根据不同的区域，配置不同的环境数据。在此页面可以统一管理全区域的关联数据的频率和采样时间。

- 采样时间：关联区域环境数据采集的时间范围。
- 室外环境数据来源：支持第三方天气预报或传感器获取。其中天气仅支持第三方预报。
- 室内环境数据来源：支持传感器获取，分别为温度、湿度、PM2.5。

注：采样频率设置对所有配置生效。

➢ 信息服务器配置

信息服务器配置可以配置第三方天气数据和本地传感器数据，给其他模块提供环境数据。

启用第三方预报采集数据，要求先上传一份.wa 格式的插件。配置参数的格式为：key=秘钥，如果天气插件的秘钥是 aaaaaa，配置参数则填写 key=aaaaaa。配置成功后可以获取到第三方预报数据。

注：若需获取第三方预报采集数据插件模板请访问信锐官网或咨询信锐技术服务电话。

启用本地传感器采集数据，要求使用本机或者其它信锐物联网平台。使用非本机的信锐物联网平台，请准确填写服务器的 IP 地址、API Token。其中 API Token 可在信锐物联网平台获取。配置成功后可以获取到本地传感器的数据。

问卷管理

➢ 问卷题库

问卷推送前需要准备进行问卷的题目，支持一次性把题目导入一个题库的功能、一次性把题目复制到多个题库的功能、一次性导出一个题库所有题目的功能，支持数据清理功能，删除题库或题目可以清理对应题库或题目的统计数据，支持更新数据功能，修改题目可以仅更新对应题目的统计数据而不清理数据。

➢ 问卷分析

题目分析针对当前题库每道题目的用户答题情况进行分析，包括选项分布，终端类型，耗时分布。

- 选项分布：选择当前题目的各个选项的人数分布。多选题情况下，一个用户选了多个选项，被选的选项人数分布都会加 1
- 终端类型:作答当前题目的用户终端类型
- 耗时分布：作答当前题目的用户耗费的时间

运营分析展示单个题库的详细运营信息，包括推送结果分析、终端类型、题目推送次数排行、推送趋势、完成时长分布、对比分析等信息。

- 推送结果分析：
  - 浏览量：当前问卷被浏览的数量
  - 问卷提交率：问卷提交数/浏览量
  - 问卷有效率：有效问卷份数/问卷提交数
  - 平均完成时长：所有推送的问卷完成总时长/有效问卷份数
- 终端类型：作答当前题库推送的所有问卷的用户使用的终端类型
- 题目推送次数排行：当前题库组成的问卷中推送次数最多的题目排行
- 推送趋势：指定查询时间范围内，当前题库每天浏览量增减趋势
- 完成时长分布：当前题库推送的问卷中所有题目的完成耗时分布
- 对比分析：以 ap 分组为单位，以浏览量，问卷提交率，问卷有效率，平均完成时长为维度作对比

调查对象，在当前题库推送的问卷中作答的用户列表

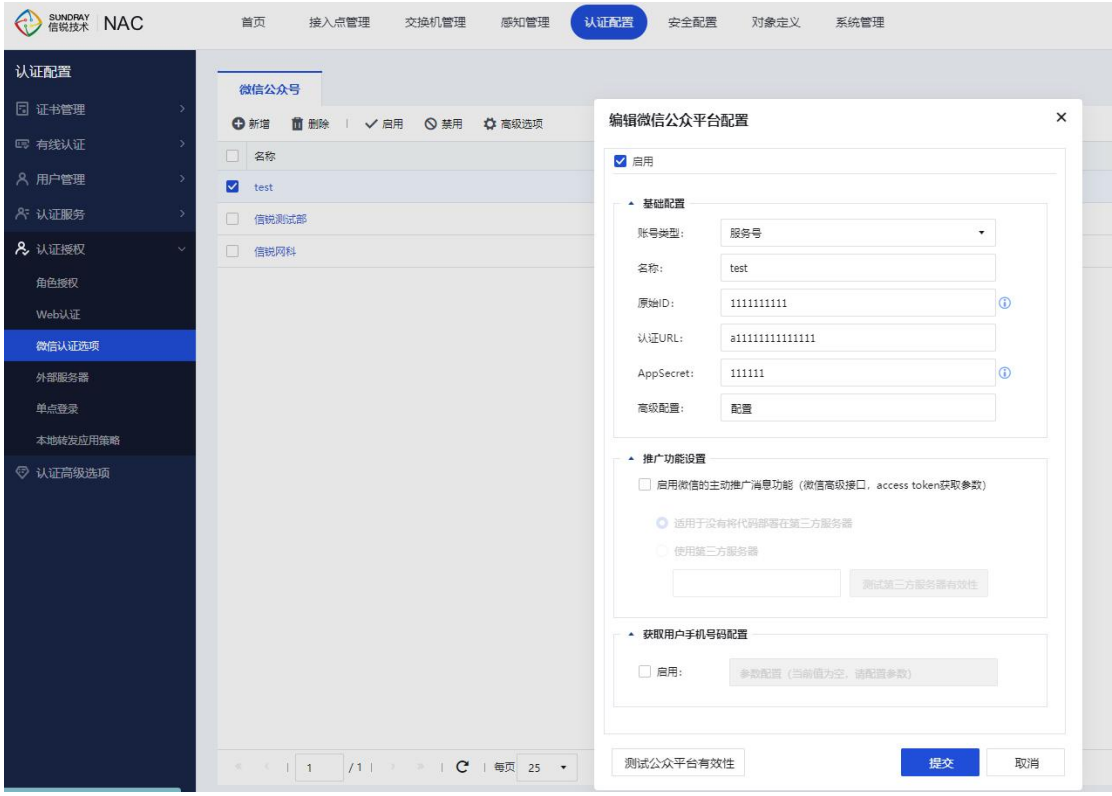
语言管理

有中文（简体）和英文两个默认模板，客户可以根据应用场景，添加语言模板，使终端认证页面显示出更多的语言。

在添加其他国家或者区域的语言前，需要先下载英文模板，然后在英文模板的 json 中，将对应的英文内容修改为需要展示的语言内容。

3.6.5.3. 微信认证选项

配置微信认证、微信推广功能，需要先配置好微信公众平台。



微信兼容性开关

第三方公众平台如果没有升级到 2.0 及其以上版本，需要开启此开关（默认为启用状态），否则微信认证方式将不能正常使用。

3.6.5.4. 外部服务器

『外部服务器』包括【认证服务器】、【虚拟服务器】

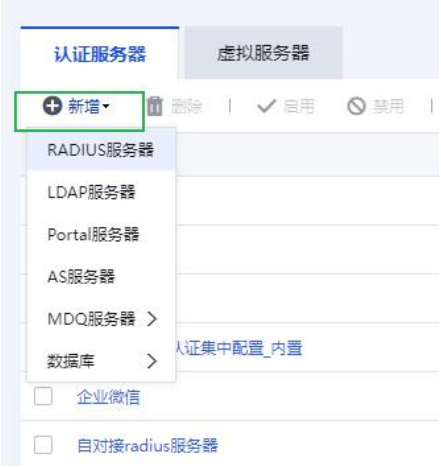
认证服务器

如果企业已部署集中的用户数据库，或者认证服务器，无线网络可选择使用外部服务器来完成用户身份验证。

使用 WAPI 企业认证的无线网络，需要在 AS 服务器上面进行用户身份的验证。

802.1x 认证的企业无线网络，支持使用 RADIUS 中继的方式，把认证请求中继到外部的 RADIUS 服务器，完成用户验证。web 认证的无线网络，支持通过外部的 RADIUS 服务器或 LDAP 服务器，完成用户身份验证。第三方 PORTAL 认证的无线网络，对接外部的 PORTAL 服

务器完成认证。



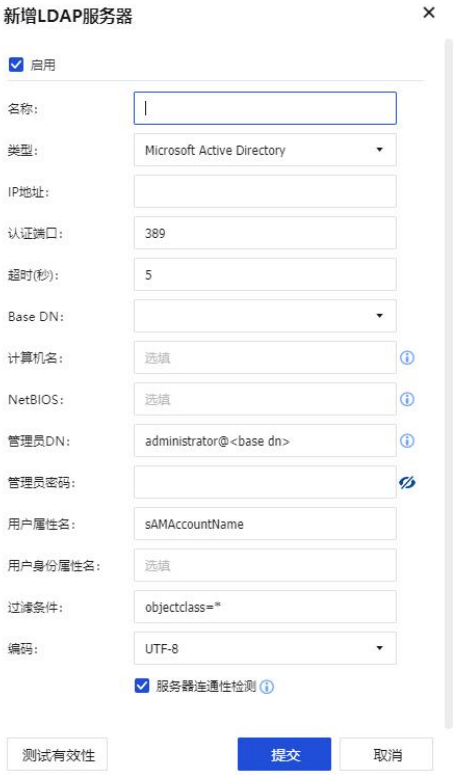
➢ Radius 服务器

『新增 Radius 服务器』需要设置“名称”、“IP 地址”、“认证端口”、“计费端口”、“超时”、“共享密钥”、“采用协议”、“编码”，可选配置“NAS_ID”、“NAS_IP”、“用户身份属性 ID”，如下图:

设置 Radius 服务器的时候可以另外设置获“取用户属性”，企业级认证时，NAC 会去用户数据库中去获取用户的组织结构，来作为无线终端的用户名和组织结构。这里可以选择与 radius 服务器对应的 LDAP 服务器。

➢ LDAP 服务器

『新增 LDAP 服务器』：设置 LDAP 服务器需要设置“名称”、“类型”、“IP 地址”、“认证端口”、“超时（秒）”、“Base DN”、“管理员 DN”、“管理员密码”，可选填“计算机名”、“NetBIOS”，“用户属性名”、“用户身份属性名”、“过滤条件”和编码，如无特殊需求，保持默认即可。



配置完成后，可以点击测试有效性，测试 LDAP 服务器是否配置正确，如果服务器 IP 配置以及用户名和密码都配置正确，会提示服务器可用，如下图：

如果服务器 IP 配置都正确，用户名和密码配置格式不对或用户名和密码错误，会提示“服务器可用，但管理员账号或密码配置错误”。如下图：

➢ Portal 服务器

添加外部 Portal 服务器，可以实现无线用户通过外部 Portal 服务认证上网。设置 Portal 服务器需要设置“名称”、“认证 URL”、“协议”、“URL 参数”、“通信端口”、“身份验证”、“加密密钥”、“报文编码”。

认证 URL：

PORTAL 服务器的 url 为终端接入无线网络时，被重定向到的地址。其中 urlid 可以使用占位符来扩展，占位符为：，占位符的值可以在认证服务器->Portal 服务器设置中配置。

认证 URL 支持配置为 IP 的形式和域名的形式。

认证 IP：

Portal 服务器的通信 IP，会自动从认证 URL 中提取

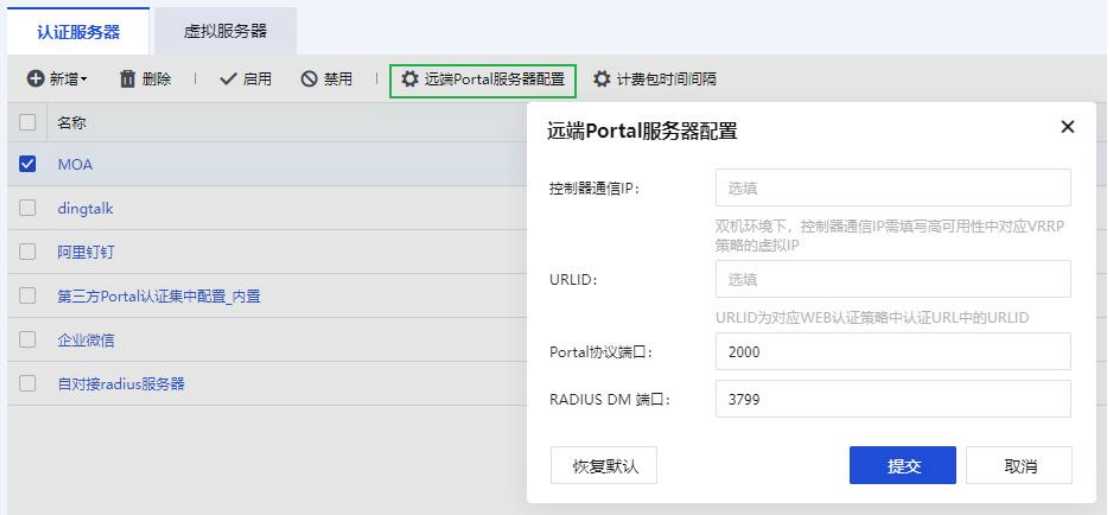
协议：

对接的 Portal 服务器类型，类型不在里面的，请选择 Portal 2.0 协议

URL 参数：

勾选某个参数类型，参数类型后面的输入框为自定义的参数名称。如勾选 SSID，自定义名称为 wlanssid，终端接入认证时，认证 URL 将会是：http://1.1.1.1:8080/portal/?wlanssid=xxx，‘xxx”为终端接入的 SSID 名称。

远端 Portal 服务器配置:

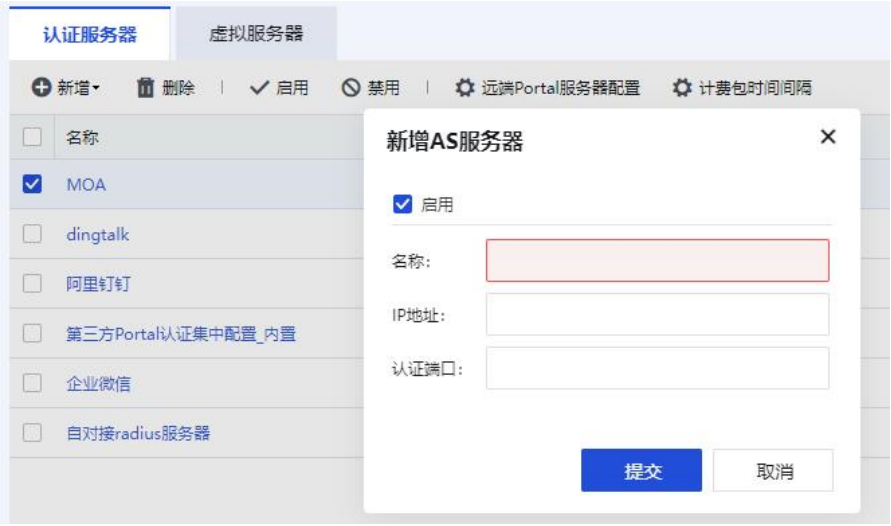


- 控制器通信 IP：对接 Portal 服务器时，当前控制器作为 Portal 客户端，服务器会主动和当前控制器通信。通信 IP 是服务器主动访问客户端使用的 IP。

  双机环境下，建议配置为高可用性中对应 VRRP 备份组的虚拟 IP。
- URLID：URLID 为对应 WEB 认证策略中认证 URL 中的 URLID。
- Portal 协议端口：客户端监听的 Portal 服务端口。
- RADIUS DM 端口：RADIUS 服务器主动下线一个用户时，使用的端口。

➢ AS 服务器

AS 服务器适用于 WAPI 企业认证的无线网络中，作为外部认证服务器。

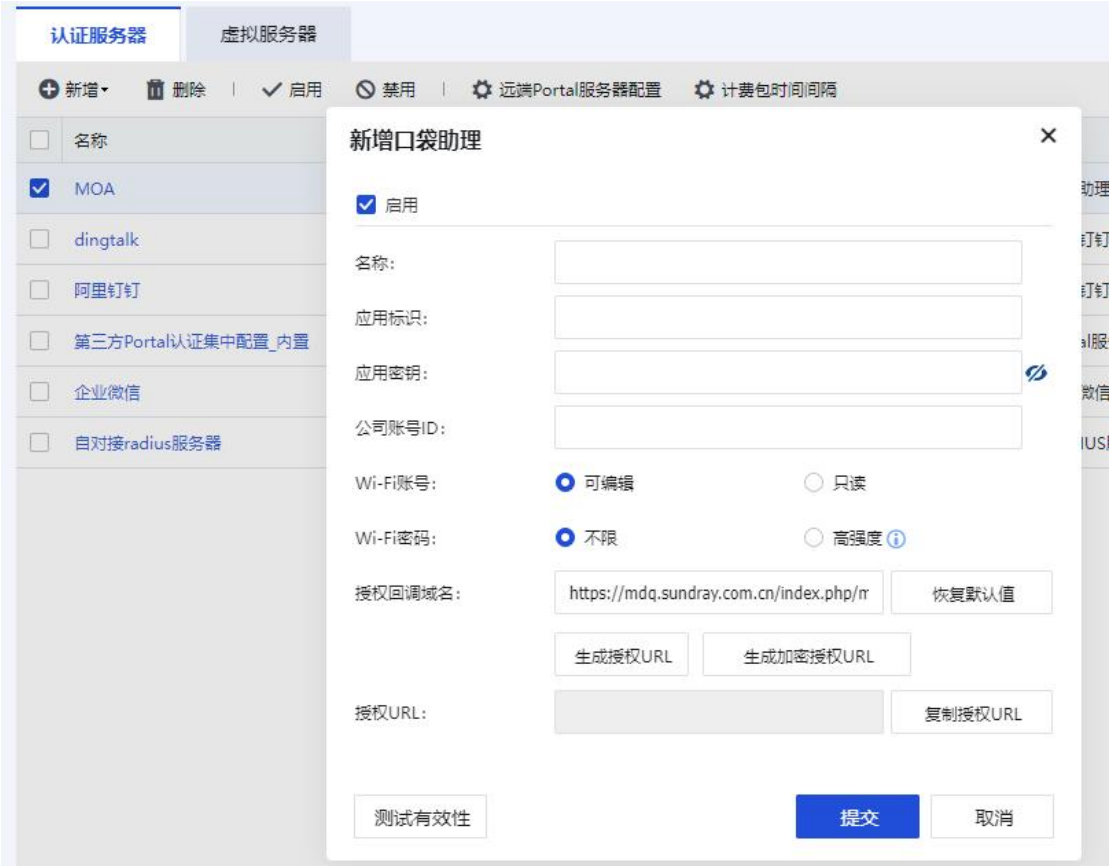


- 名称：AS 服务器的名称
- IP 地址：AS 服务器的 IP 地址
- 认证端口：服务器的认证端口，一般默认为 3810

➢ 口袋助理

口袋助理认证是指将口袋助理移动办公平台作为认证服务器，用户通过使用口袋助理上创建的上网账号完成认证，实现无线上网账号与口袋助理的对接，便于用户对无线上网账号进行实时管理。

适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



➢ 阿里钉钉

阿里钉钉认证是指将阿里钉钉移动办公平台作为认证服务器，用户通过使用钉钉上创建的上网账号完成认证，实现无线上网账号与阿里钉钉的对接，便于用户对无线上网账号进行实时管理。

适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证

➢ 微信企业号

微信企业号认证是指将微信企业号移动办公平台作为认证服务器，用户通过使用微信企业号上创建的上网账号完成认证，实现无线上网账号与微信企业号的对接，便于使用微信企业号办公的用户对无线上网账号进行实时管理。

适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证

➢ 数据库

目前 NAC 直接对接 Oracle 数据库、Mysql 数据库以及 Mssql 数据库，实现帐号认证和企业级认证

1、基本配置

基本配置是用于连接数据库的信息。

（1）名称：数据库认证服务器的名称。

（2）IP 地址：数据库的服务器地址。

（3）端口：数据库服务器使用（监听）的端口。

（4）超时（秒）：向数据库服务器查询用户信息时的查询超时时间。

（5）数据库名/SID：数据库中保存用户信息的数据库（数据库实例）的名称。

（6）管理员帐号：登录数据库的账号，该账号需要有查询“数据库名”指定的数据库的权限。

（7）管理员密码：登录数据库的账号对应的密码。

2、获取数据

用于配置获取数据库信息的 SQL 语句，支持 6 个字段信息的获取；SQL 语句中使用$$USERNAME$$代表用户登录名。

（1）密码（必填）：用于查询用户的密码，作密码校验。portal 认证支持明文、MD4、MD5、SHA1、NT-Password 加密类型。企业认证支持明文、NT-Password。

（2）有效期和创建时间（可选）：用于校验用户是否有效。如果只配置有效期字段，具体使用方法见[外部数据库获取创建时间和有效期]。

（3）用户组（可选）：用于获取用户组做 vlan 匹配、权限匹配（无线网络配置）。支持中文编码，具体见[外部数据库对中文编码的支持]。

3、外部数据库对中文编码的支持

（1）用户名支持设置中文编码。

（2）用户组、自定义 1、自定义 2 这三个查询字段支持使用中文编码。

（3）支持的中文编码格式如下（UTF-8 是最为通用的格式；GBK 是常用的简体中文编码格式，BIG5 是常用的繁体中文编码格式）：

- ORACLE:支持 UTF-8、GBK、BIG5
- MYSQL:支持 UTF-8、GBK、BIG5、GB2312
- SQLSERVER:支持 UTF-8、UCS-2、简体中文、繁体中文

4、外部数据库获取创建时间和有效期

WAC 支持%Y、%m、%d、%H、%M、%S 几个通配符，使用通配符在自定义格式中填写与数据库中内容同样的格式，WAC 就能够识别，其意义分别为：

%Y 年、%m 月、%d 日、%H 时、%M 分、%S 秒

根据数据库中的内容是字符串和内置格式，分别有不同的处理方式（根本目的都是转化为字符串形式）

情况 1:字符串格式

数据库中的时间格式的类型是字符串，则使用匹配符按照本地的字符串的样式得到对应的格式；

例如数据库的时间内容是 2017-10-20 10:30:50，则自定义格式填%Y-%m-%d %H:%M:%S；

例如数据库的时间内容是 10:30:50,2017,10,20，则自定义格式填%H:%M:%S,%Y,%m,%d。

情况 2:内置时间格式

数据库中的时间类型是数据库内置的时间格式，则需要将内置时间格式转为指定的字符串格式。不同数据库有不同的转换处理函数；

a、对于 oracle，时间字段使用的是时间格式（包括 date、timestamp），使用 TO_CHAR 进行转换；

SELECT TO_CHAR(时间字段名, 'yyyy-mm-dd hh24:mi:ss') FROM EXTDB_USER_TB WHERE USERNAME = $$USERNAME$$；

格式中填写:%Y-%m-%d %H:%M:%S。

b、对于 mysql，时间字段使用的是时间格式（包括 date、datetime、timestamp），直接按照情况 1 处理即可 oracle 的 timestamp；

因为 mysql 查询到的内容直接就是 2019-10-20 10:30:50 或者 2019-10-20 形式的字符串。

c、对于 sqlserver，时间格式是 datetime，则使用 CONVERT 将 datetime 格式转为字符串（2017-01-01 12:00:00）的格式；

SQL 语句:SELECT CONVERT(nvarchar(24), 时间字段名, 20) FROM 表名 WHERE 用户名字段名 = $$USERNAME$$；

格式中填写:%Y-%m-%d %H:%M:%S。

d、对于 sqlserver，时间格式是 datetime 之外的格式，则使用 CAST 将其强制转换为 datetime，再使用 CONVERT 进行转换；

SQL 语句:SELECT CONVERT(nvarchar(24), CAST(时间字段名 AS DATETIME) FROM 表名 WHERE 用户名字段名 = $$USERNAME$$；

格式中填写:%Y-%m-%d %H:%M:%S。

5、外部数据库其它复杂 SQL 语句示例（SQLSERVER）

（1）联表查询

用户名和需要查询的内容（例如用户组）在不同的表中，需要使用外键进行关联查询

示例：

用户表 usertb 的内容如下，

id	username	grp_fk
1	test1	2

b、用户组表 grptb 的内容如下，

id	groupname
2	sundray

c、SQL 语句：

SELECT grptb.groupname FROM usertb,grptb WHERE usertb.username = $$USERNAME$$ and usertb.grp_fk = grptb.id;

（2）内容以键值对的形式保存（例如一些 radius 服务器），利用 max case 做“行转列”处理

示例：

用户表 usertb 的内容如下，我们需要提取其中的 attribute 列中，内容为"password"的行所对应的 value 作为密码

username	attribute	value
test1	password	pwd
test2	group	sundray

b、SQL 语句：

SELECT MAX(CASE WHEN attribute='password' THEN value ELSE ' ' END) AS MY_PASSWORD FROM usertb WHERE username = $$USERNAME$$

（3）截断用户名

因为 WAC 支持的用户名长度不能超过 95，如果数据库中的用户名长度超过 95，就需要将过长的用户名作截断。这种情况下可以使用 SUBSTRING 处理。

示例：

SELECT 密码字段名 FROM 表名 WHERE SUBSTRING(用户名字段名, 1, 95) = $$USERNAME$$

（4）去掉用户名前后缀

数据库中的用户名有一些前后缀，例如 XXX@sundray.com、sundray_XXX，我们想要用户使用 XXX 登陆。这种情况下可以使用 SUBSTRING 处理。

示例 1：

a、用户表 usertb 中的用户名都是 XXX@sundray.com 的形式，我们想要用户使用 XXX 登陆

b、SQL 语句 1：

```
SELECT 密码字段名 FROM 表名 WHERE

SUBSTRING(用户名字段名,

1,

(

CASE WHEN CHARINDEX('@sundray.com', USERNAME)=0 THEN

LEN(用户名字段名)

ELSE

CHARINDEX('@sundray.com', USERNAME )-1

END

)

) = $$USERNAME$$
```

示例 2：

用户表 usertb 中的用户名都是 XXX@sundray.com 的形式，我们想要用户使用 XXX 登陆

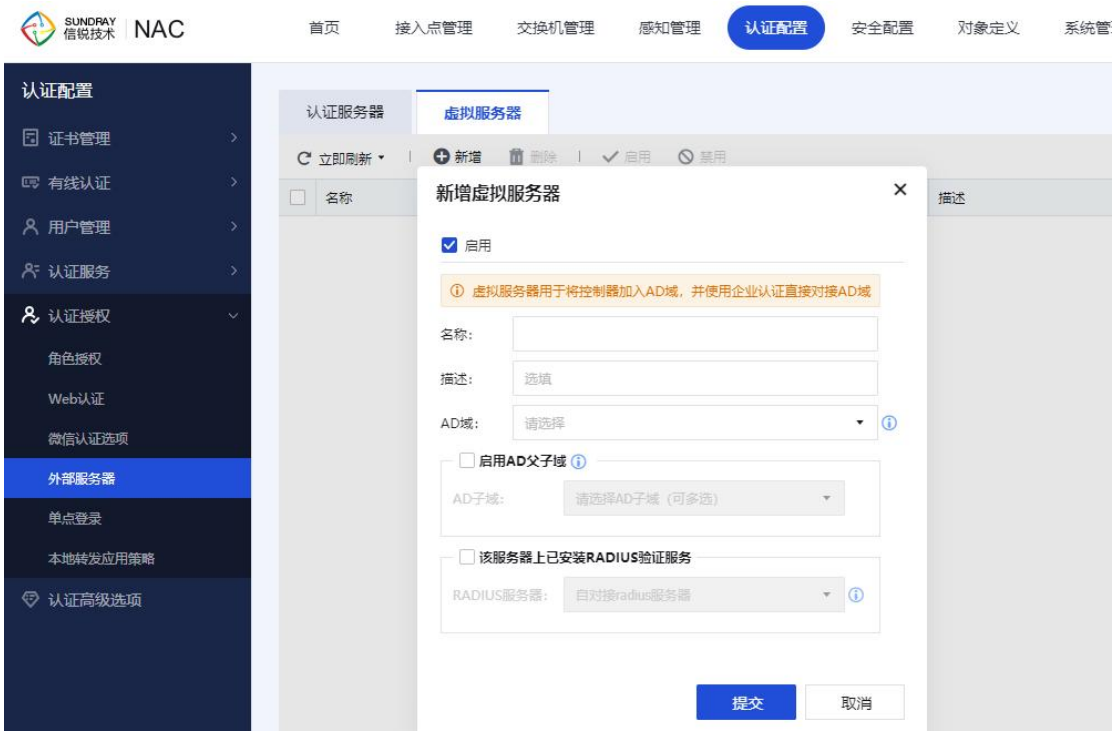
SQL 语句 1：

```
SELECT 密码字段名 FROM 表名 WHERE
SUBSTRING(用户名字段名,
(
CASE WHEN CHARINDEX(REVERSE('sundray_'), REVERSE(用户名字段名))=0 then
1
ELSE
2+len(用户名字段名)-CHARINDEX(REVERSE('sundray_'), REVERSE(用户名字段名))
END
),
)LEN(用户名字段名)
) = $$USERNAME$$
```

虚拟服务器

如果企业已部署多台微软 AD 域控制器且互相之间存在父子域关系，无线网络可选择使用虚拟服务器来完成用户身份验证。

虚拟服务器支持 TTLS-PAP 认证以及 EAP-MSCHAPv2 认证。



➢ 未安装 RADIUS 验证服务虚拟服务器

适用于 WPA/WPA2 企业认证及 802.1X 无线网络的终结认证，需要用户启用 netbios 服务以支持对接 AD 域。

- 名称：虚拟服务器名称
- AD 域：选择 AD 域服务器配置(可为父域或独立域)
- AD 子域：选择与已添加 AD 域存在子域关系的 AD 域服务器配置

➢ 已安装 RADIUS 验证服务的虚拟服务器

若用户不愿启用 netbios 服务且已安装 RADIUS 验证服务，用户可选择启用“该服务器上已安装 RADIUS 验证服务”对接 AD 域。

- 名称：虚拟服务器名称
- AD 域：选择 AD 域服务器配置(可为父域或独立域)

- AD 子域：选择与已添加 AD 域存在子域关系的 AD 域服务器配置
- RADIUS 服务器：选择已在配置的 AD 域中注册 RADIUS 服务器

单点登录

单点登录，将用户的认证信息发送到深信服上网行为管理设备，避免终端通过控制器认证后，还需要再次认证。

1、本地转发，请在接入点（编辑->参数配置->其他配置）或者接入点分组（编辑->其他配置）中 ，配置认证信息转发。

2、集中转发和有线认证，由控制器转发认证信息，需要在该页进行配置。

➢ 用户类型

- 无线用户：无线用户，包括本地转发和集中转发的用户
- 控制器有线用户：在控制器上完成有线认证的用户
- 接入点有线用户：完成接入有线认证的用户

- 交换机有线用户：完成交换机有线认证的用户
- 所有用户：包括无线用户、控制器有线用户、接入点有线用户以及交换机有线用户。

➢ **协议类型**

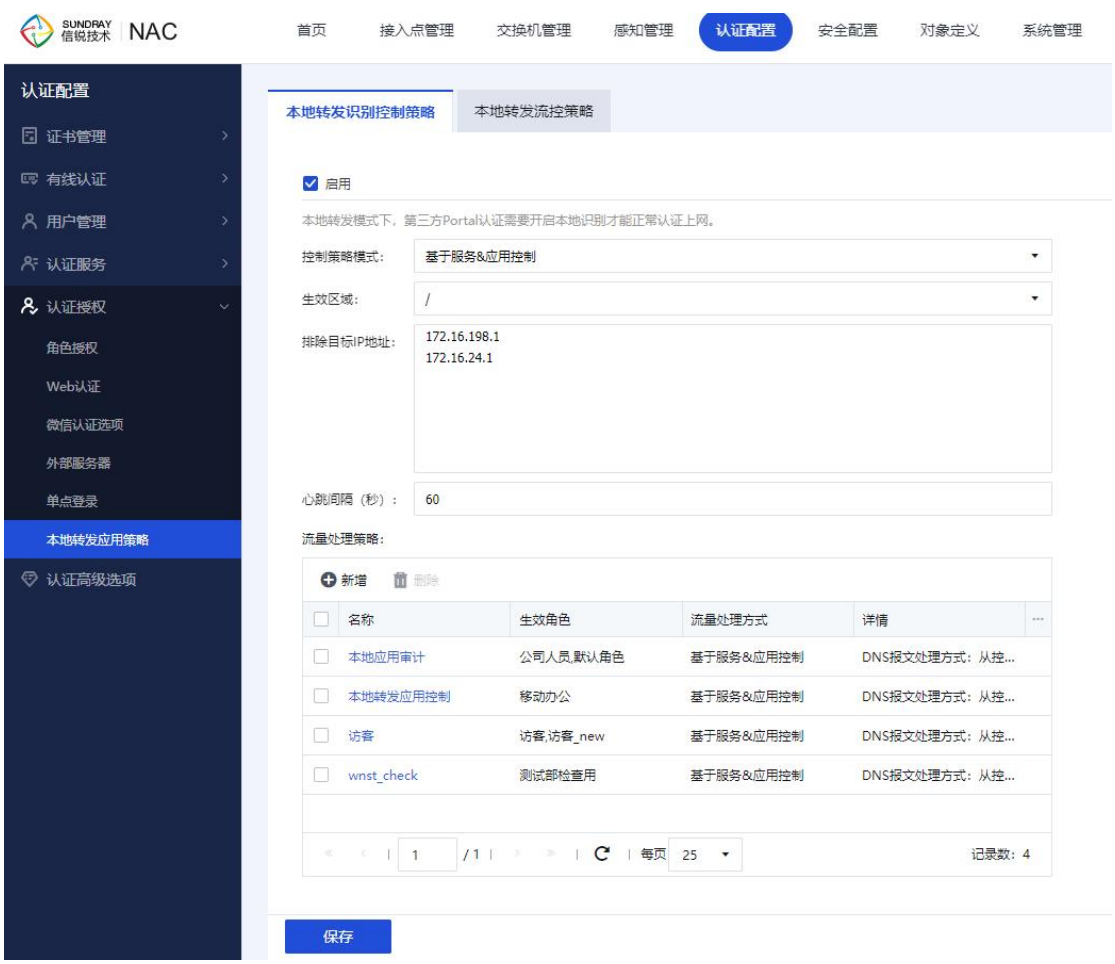
深信服单点登陆协议 0.1：深信服上网行为管理设备使用的单点登陆协议（AC11.0 之前版本支持），协议默认使用 1773 端口。

深信服单点登陆协议 1.0: 深信服上网行为管理设备使用的单点登陆协议（AC11.0 及后续版本支持），协议同时兼容 0.1 版本。协议默认使用 1775 端口。

深信服上网行为管理的配置菜单如下：

3.6.5.5. 本地转发应用控制

该功能可实现本地转发下基于应用的访问控制策略以及基于应用的流控，需确保有应用识别序列号。



本地转发识别控制策略

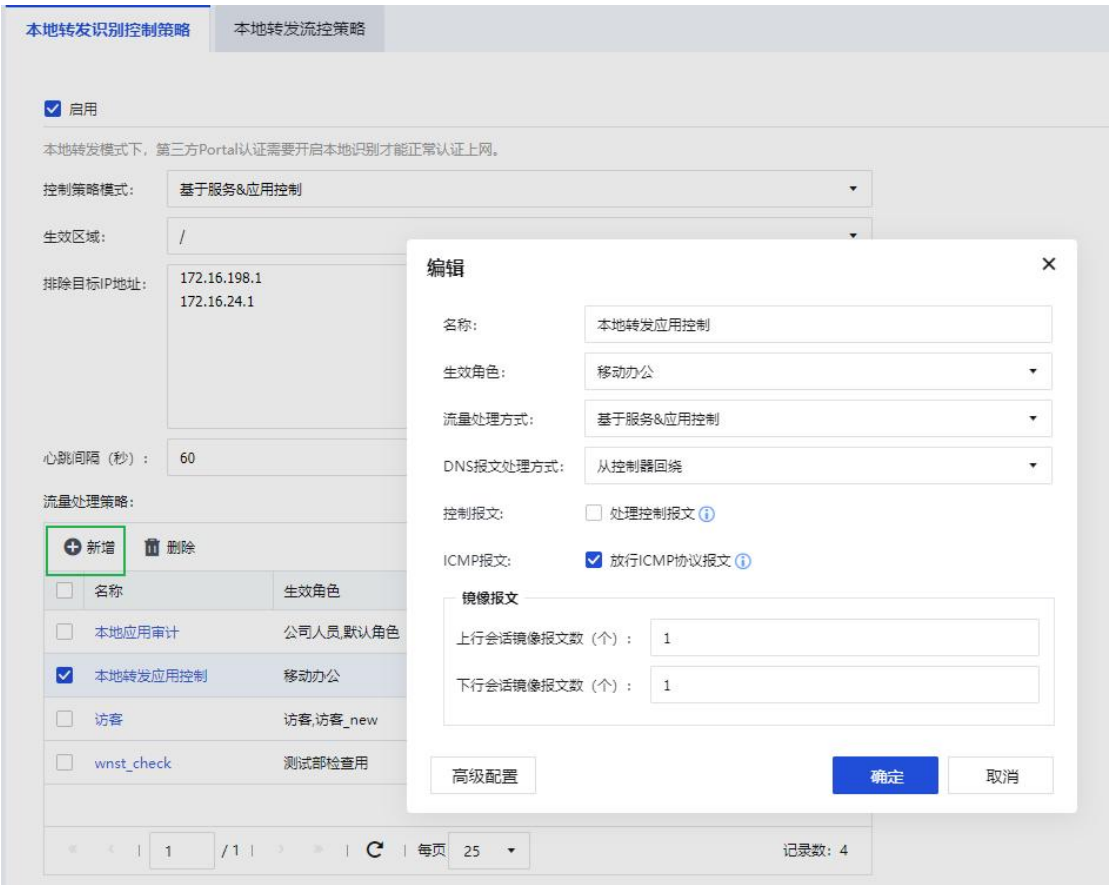
控制策略模式：可选择基于服务控制或基于应用控制，选择基于应用控制，能识别具体应用进行相应的访问控制或是流量控制；

生效区域：选择需要进行本地转发应用控制的 接入点或是接入点分组；

排除目标 IP 地址：应用于本地内网环境中的服务器及终端这类需要额外直通访问的设备，访问这类设备的流量不会被识别和控制。

流量处理策略：关联需要生效的角色，流量处理方式选择应用控制，其他配置保持默认。此处需要注意的是，镜像报文的配置；镜像报文数量配置越大（配置范围为 2-15 个），应用识别

效果会更好，识别率会更高。但是相应的，镜像报文过多时会降低终端访问网络时的响应速度，建议保持默认配置。



本地转发流控策略

本地转发的流控策略类似于控制器流控功能，可以实现在总的流速限制条件下再对应用流控子通道进行带宽限制，只能做限制通道，不能做保障通道。

通道匹配的顺序取决于通道所处的位置，是从上往下逐个通道匹配的。

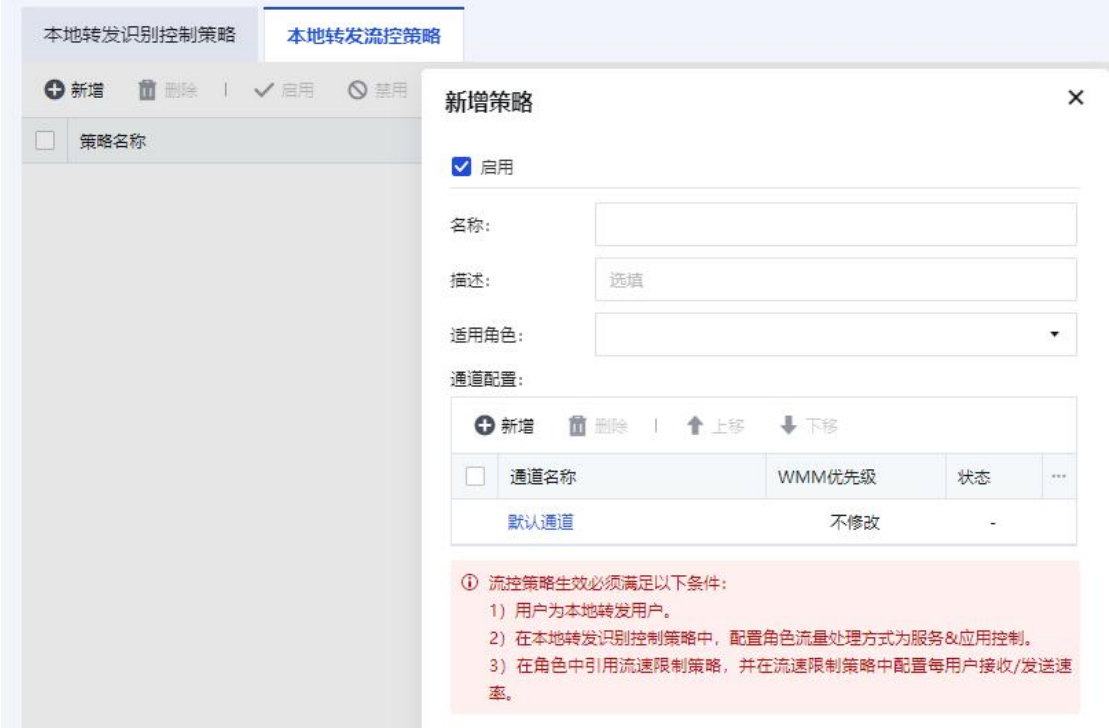
通道属性中的“优先级”，是指带宽分配以及数据包发送的优先级。

流控策略生效必须满足以下条件：

1）用户为本地转发用户。

2）在本地转发识别控制策略中，配置角色流量处理方式为应用控制。

3）在角色中引用流速限制策略，并在流速限制策略中配置每用户接收/发送速率。



3.6.6. 认证高级选项

3.6.6.1. WEB 认证通用配置

- 认证域名：认证域名默认配置为：auth.wifi.com。Web 认证时，会跳转到该域名上来。

  注：域名配置为公网上已经存在的域名时，Web 认证的用户访问该公网域名也会跳转到认证或注销页面。
- 认证域名解析的 IP：修改认证域名解析的 IP 地址之前，请确保要修改的 IP 地址不会冲突，否则将会出现终端进行 web 认证时无法打开认证页面。
- 手机号绑定验证：账号二次认证时，绑定手机号码之后，同一个终端在有效期之内无需再次绑定。
- 注销无流量用户：完成有线认证、接入点有线认证之后，终端在阈值内无流量产生，控制器会主动注销这个用户。
- 访客认证免弹 Portal 页面有效期，该选项值仅对只配置了访客认证的无线网络生效。同时配置访客认证和账号认证，终端用户接入无线网络时，每次都会重定向至认证页面：
  - 弹出 Web 认证页面：短信认证、二维码认证、微信认证的用户，非首次接入无线网络，跳转到认证页面，不需要输入账号信息，只需要点击登录即可；

- 不弹出 Web 认证页面：短信认证、二维码认证、微信认证的用户，非首次接入无线网络，不跳转到认证页面，用户只需接入网络，无需认证即可上网。

- 账号认证免弹 Portal 页面有效期：账号认证非首次认证，断开无线网络后，再次登录的时间间隔在阈值范围内时，不重定向至认证页面，超出阈值时间，终端用户将会重定向至认证页面。
- 账号+访客认证，启用访客认证免弹 Portal 页面有效期：账号认证+访客认证的网络，访客认证的老用户在免弹 portal 页面有效期内接入，可以直接上网不显示认证页面。
- 无线 portal 用户认证超时时间：配置多长时间停留认证页面没做认证，需要重新触发 portal 页面的时间
- 账号自动登录：勾选“每次都到服务器上验证账号密码”，即终端每次连接 WiFi 时都需要到认证服务器校验用户名和密码
- 认证前角色：
  - 使用上次的用户角色，账号自动登录时先使用上一次的角色，认证通过后置为新角色，认证不通过置为认证前角色；
  - 重新匹配角色规则，将默认使用认证前角色，再根据认证结果重置角色。

3.6.6.2. 访客认证选项

1、微信认证直通：微信认证唤起微信应用的时候，需要在认证过程中放通微信流量，以及和腾讯的微信服务器进行交互。唤起微信应用失败的时候，可以选择对终端进行免认证处理。

2、手机号登录有效期：手机号登录的认证有效期，通过短信认证之后可以访问无线网络的时长。超过该时间之后，需要重新获取验证认证上网。

3、微信登录有效期：微信认证有效期，通过微信认证之后可以访问无线网络的时长。超过该时间之后，需要重新在微信公众账号菜单中，申请上网。

4、二维码审核有效期：只通过二维码方式，二维码审核后，访客可以访问无线网络的时长。超过设置时间后，如果仍然需要访问无线网络，需要再次审核。

5、短信验证码有效期：短信认证获取到的验证码，使用的有效次数，可选单次有效或多次有效。

6、短信验证码有效时长：短信认证获取到的验证码使用的有效期，在有效期内验证码可重复使用。

7、海外社交应用认证有效期：通过海外社交应用之后可以访问无线网络的时长。有效期内终端无需再次输入登录信息等，只需在页面上点击“我要上网”即可。

8、邮箱登录有效期：通过邮箱认证之后可以访问无线网络的时长。有效期内终端无需再次输入登录信息等，只需在页面上点击“我要上网”即可。

9、邮箱验证码有效期：邮箱认证获取到的验证码，使用的有效次数，可选单次有效或多次有效。

10、邮箱验证码有效时长：邮箱认证获取到的验证码使用的有效期，在有效期内验证码可重复使用。

11、自动登陆优先级：在同一个无线网络中配置多种认证方式的时候，如果一个终端使用过多种认证方式，再次认证时免登陆的优先级。

3.6.6.3. 生物识别认证选项

生物识别认证有效期：终端非首次认证，断开无线网络后，再次连接的时间间隔在阈值范围内时，不需要 TrustSpeed 内生物识别授权，超出阈值时间，终端连接需要在 TrustSpeed 内再次生物识别授权。

3.6.6.4. 模板内容配置

短信服务内容（二次认证)：二次认证时发送短信的模板。

邮箱找回密码：本地用户使用邮箱找回密码时，邮件主题和邮件内容模板。

3.6.6.5. 有线用户认证策略

1、静态 IP 免认证有效期：有线认证，当网络环境为认证用户和认证接口跨三层网络，给终端配置使用静态 IP 部署时，终端用户 WEB 认证二次认证免认证的有效期。

2、DHCP IP 免认证时间：有线认证，当网络环境为认证用户和认证接口跨三层网络，给终端配置使用 DHCP 分配 IP 部署时，终端用户 WEB 认证二次认证免认证的有效期。

3.6.6.6. 其他配置

1、终端绑定管理员免审批有效期：启用此功能时，终端绑定管理员免审批为选定日期的 23:59。

2、第三方 portal 用户免认证：适用于 portal 对接场景，若第三方 portal 服务器不支持 MAC 免认证功能，启用此功能，终端用户认证通过后，在时长配额范围内不需要再次认证。

3、终端类型识别：开启精准终端类型识别，将会识别终端的操作系统。

4、剔除获取 IP 失败的终端：DHCP 获取失败，大部分无线终端 IP 地址会显示为 169.254.x.x。

（1）开关开启，超过超时时间，终端还未获取到 IP 地址，将会被踢下线让终端重新认证，重新获取 IP 地址。

（2）开关关闭，适用于内网使用 169.254.x.x 网段的客户，避免获取到这个网段的无线终端，被控制器误判为未获取到 IP 用户而踢掉。

5、云管家灾备选项：控制器与云服务器断开连接时，终端审批消息无法下发，认证用户不需要经过审批即可上网.

6、单点登录发送终端下线消息：控制器结合深信服 AC 做单点登录时，可选择是否将终端的下线报文单点登录发给深信服 AC。

7、用户名区分大小写：控制器默认会将账号认证的用户名转换成小写，勾选之后将不进行转换。

3.7. 安全配置

3.7.1. 终端安全

3.7.1.1. 有线终端审批

待审批

终端策略中的终端地址绑定功能与终端位置绑定功能可触发终端进入待审批列表，并阻塞流量；管理员可手动进行审批操作，以放通流量。

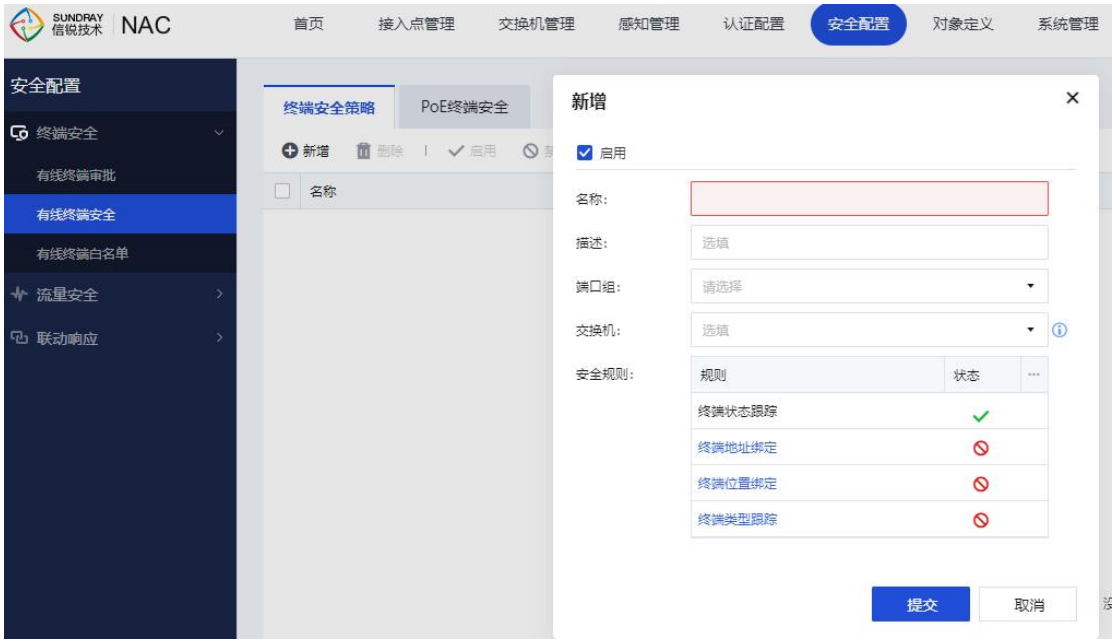
已审批

已审批的终端对应关系进入已审批列表，并放通流量。默认老化时间为永不老化，支持配置自定义老化时间。

3.7.1.2. 有线终端安全

终端安全策略

终端安全策略，是帮助用户管理、识别和跟踪其网络环境下的终端而建立的人性化功能，解决用户对网络安全的需求并为其提供了快捷有效的实现方法。



终端状态跟踪

用于跟踪连接交换机端口的终端状态，包括在线、离线、类型等具体的信息并显示在状态页面。

终端地址绑定

用于绑定终端和 ip 地址，实现 IT 管理员对其网络环境下的 ip 地址的监管；可启用自动审批并设置审批数量来实现批量操作的自动化，也可手动审批；其中，自动审批的个数是包含已审批列表的终端对应关系个数。另有免审批和强制审批功能，免审批地址在更换 IP 地址时无需审批，强制审批地址在自动审批阶段仍需审批。

终端位置绑定

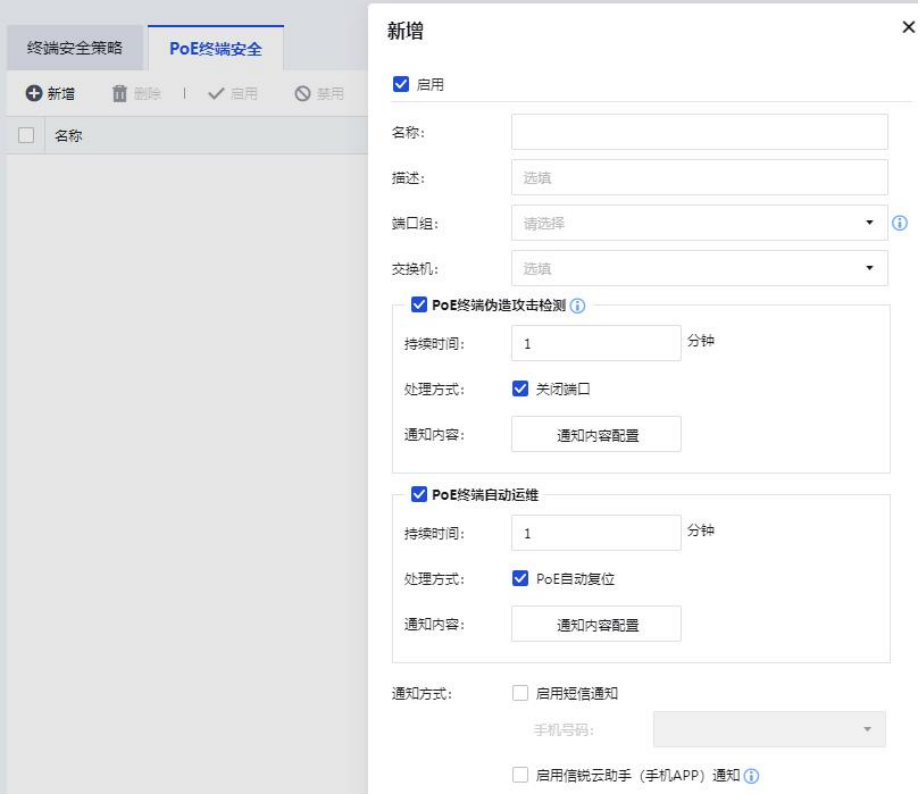
用于绑定终端和端口，实现监管端口下联设备的功能；可启用自动审批并设置审批数量来实现批量操作的自动化，也可手动审批。

终端类型跟踪

用于跟踪下联终端的类型状态，帮助用户实时获取下联终端的各种信息；可限制接入的设备类型并通知用户。

PoE 终端安全

针对 PoE 交换机，检测到 PoE 终端伪造攻击/PoE 终端无法通信的情况时，交换机会自动进行处理，并将相应告警通过短信/APP 消息发送给用户，帮助用户监控 PoE 终端。



- PoE 终端伪造攻击检测：通过检测设备的供电特征，以排查仿冒设备接入并执行相应安全措施。
- PoE 终端自动运维：通过检测设备通信情况，自动复位 PoE 端口，帮助用户解决无法正常通信的情况。

有线终端白名单

管理员可以手动添加有线终端白名单，以保护可信的重要设备不被交换机安全业务误判拉黑。有线终端白名单只对交换机安全业务生效，管理员手动添加的黑名单优先级高于白名单。

3.7.2. 流量安全

3.7.2.1. 用户隔离

通常情况下，同一 VLAN 的用户间是可以相互通信的，但在无线接入的环境下，移动终端间相互通信，存在较大安全隐患。例如部署用于公公众上网的无线网络中，多个无线用户之间没有直接通信的需求，在此环境下，启用此选项可以减少无线终端间的报文，提高了无线网络性能，同时提高了安全性。还有避免某些感染了病毒的终端传播病毒的风险。

禁止同一 VLAN 内的用户之间相互通信后，只要是通过同一无线接入点接入的，所有 VLAN 相同的无线用户间将不能相互通信。这样不仅可以降低了安全风险，还可以减少移动终端间的广播报文。不同 VLAN 间是否能相互通信，由第三方路由设备控制，本设备暂不支持。通常不同 VLAN 间默认是不能通信的。

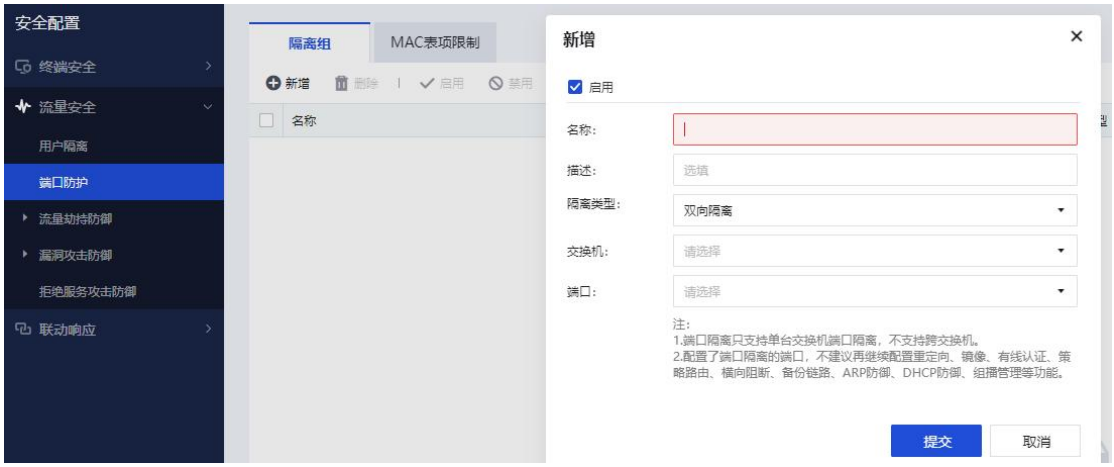
3.7.2.2. 端口防护

隔离组

采用端口隔离特性，可以实现报文之间的二、三层隔离，用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间的隔离，为用户提供了更安全、更灵活的组网方案。

单向隔离是指从“源端口”发送的报文不能到达“目的端口”，但从“目的端口”发送的报文可以到达“源端口”。

双向隔离是指隔离组内的任一端口发送的报文不能到达隔离组内的其他端口，但可以到达隔离组外的其他端口。



MAC 表项限制

一些安全性较差的网络容易受到黑客的 MAC 地址攻击，由于 MAC 地址表的容量是有限的，当黑客伪造大量源 MAC 地址不同的报文并发送给交换机后，交换机的 MAC 表项资源就可能被耗尽。当 MAC 表被填满后，即使它再收到正常的报文，也无法学习到报文中的源 MAC 地址。配置限制 MAC 地址学习数，当超过限制数时不再学习 MAC 地址，同时可以配置当 MAC 地址数达到限制后对报文采取的动作，从而防止 MAC 地址表资源耗尽，提高网络安全性。

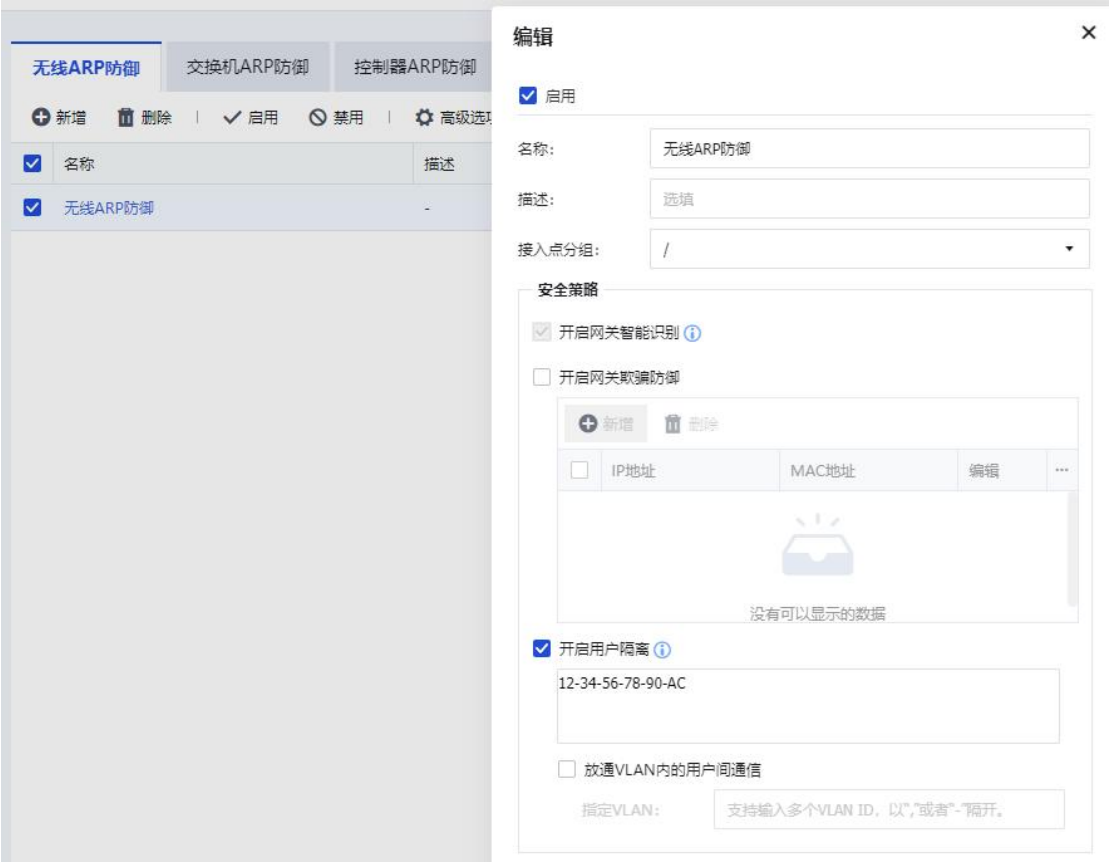
处理动作为丢弃数据包时，如果端口上的 MAC 地址数量超过限制，交换机不再学习新的 MAC 地址并且不再转发处理新 MAC 的数据包；处理动作为转发数据报文时，如果端口上的 MAC 地址数量超过限制，交换机不再学习新的 MAC 地址，但还会转发处理新 MAC 的数据包。

3.7.2.3. 流量劫持防御

ARP 防御

1、无线 ARP 防御

支持网关 ARP 防御功能，以及无线用户隔离，确保网络安全。网关智能识别：智能识别网关，如果所有终端都是静态 IP，此功能不生效。 开启 ARP 欺骗防御：开启此功能后，手动配置和智能识别的网关会被默认保护起来。开启无线用户隔离：禁止无线终端之前互相通信。



2、交换机 ARP 防御

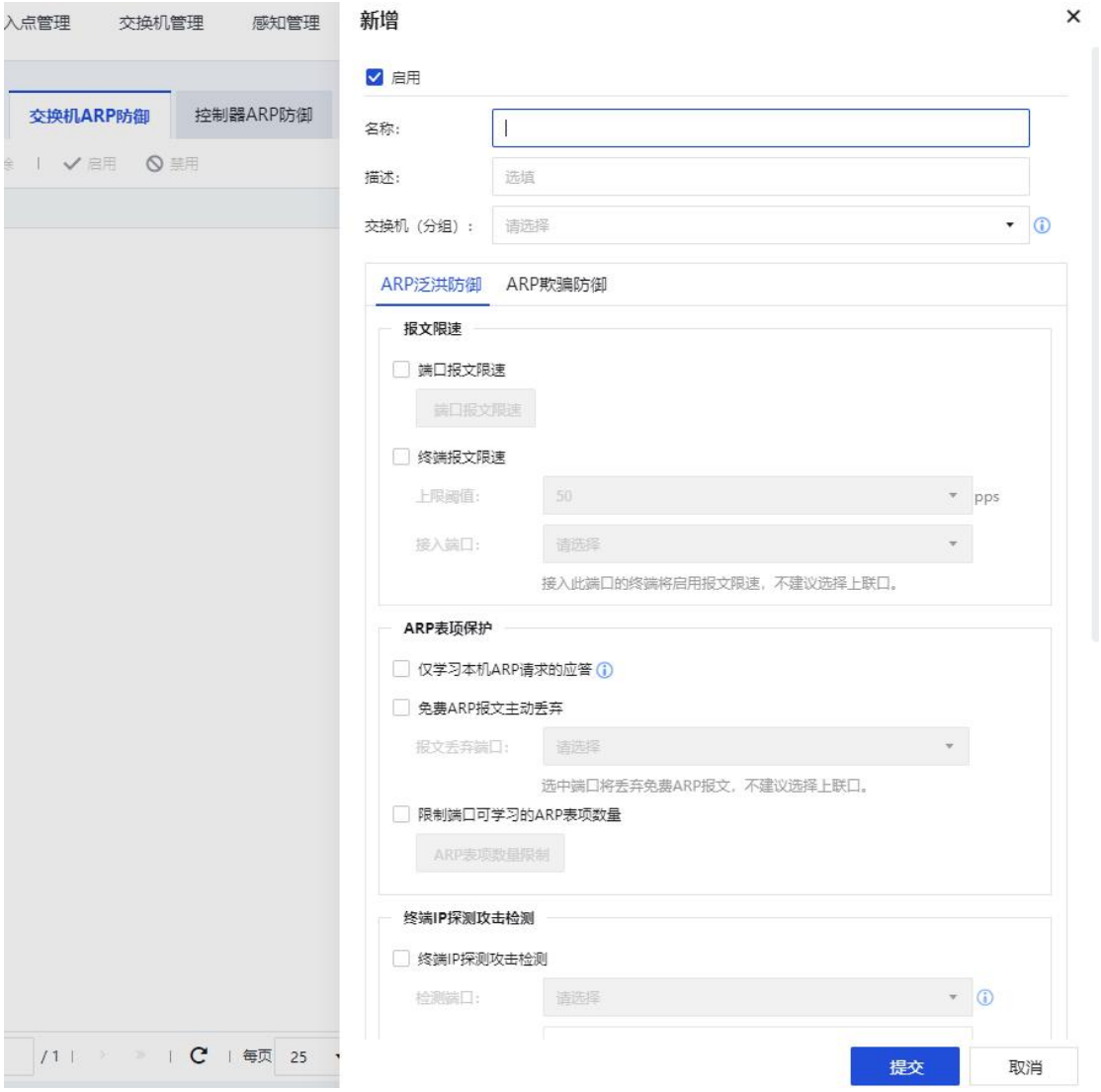
ARP 安全是针对 ARP 攻击的一种安全特性，它通过一系列对 ARP 表项学习和 ARP 报文处理的限制、检查等措施来保证网络设备的安全性。ARP 安全特性不仅能够防范针对 ARP 协议的攻击，还可以防范网段扫描攻击等基于 ARP 协议的攻击。

（1）ARP 泛洪防御

ARP 泛洪攻击也叫拒绝服务攻击 DoS（Denial of Service），主要存在这样两种场景：

1）设备处理 ARP 报文和维护 ARP 表项都需要消耗系统资源，同时为了满足 ARP 表项查询效率的要求，一般设备都会对 ARP 表项规模有规格限制。攻击者就利用这一点，通过伪造大量源 IP 地址变化的 ARP 报文，使得设备 ARP 表资源被无效的 ARP 条目耗尽，合法用户的 ARP 报文不能继续生成 ARP 条目，导致正常通信中断。

2）攻击者利用工具扫描本网段主机或者进行跨网段扫描时，会向设备发送大量目标 IP 地址不能解析的 IP 报文，导致设备触发大量 ARP Miss 消息，生成并下发大量临时 ARP 表项，并广播大量 ARP 请求报文以对目标 IP 地址进行解析，从而造成 CPU（Central Processing Unit）负荷过重。



报文限速

通过 ARP 报文限速功能，可以防止设备因处理大量 ARP 报文，导致 CPU 负荷过重而无法处理其他业务，分为基于单个交换机端口报文限速和基于源 MAC 地址报文限速。

仅学习本机的 ARP 请求应答

只有本设备主动发送的 ARP 请求报文的应答报文才能触发本设备学习 ARP，其他设备主动向本设备发送的 ARP 报文不能触发本设备学习 ARP。这可以防止设备收到大量 ARP 攻击报文时，ARP 表被无效的 ARP 条目占满。

免费 ARP 报文主动丢弃

设备直接丢弃免费 ARP 报文，可以防止设备因处理大量免费 ARP 报文，导致 CPU 负荷过重而无法处理其他业务。

限制端口可学习的 ARP 表项数量

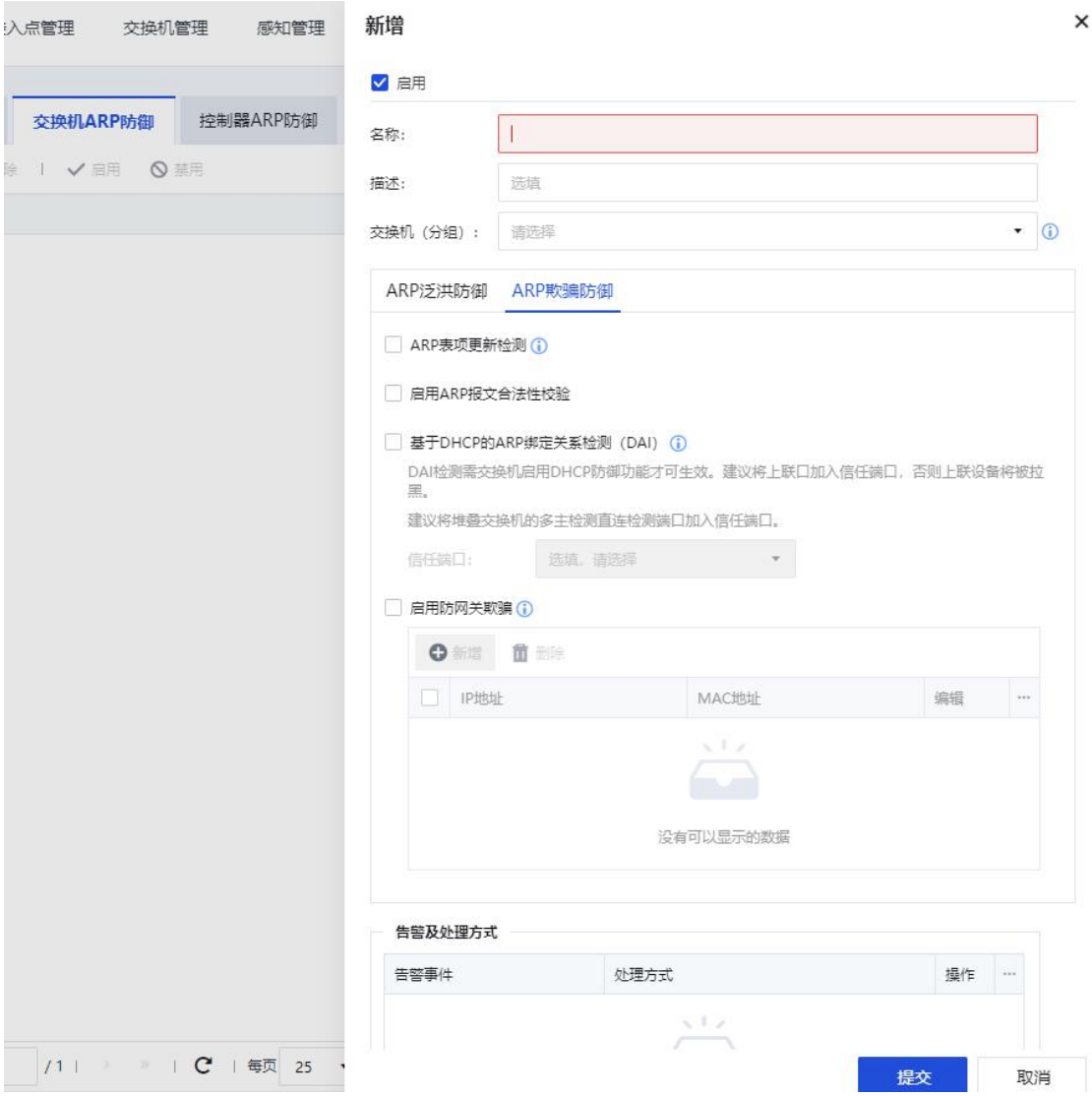
设备接口只能学习到设定的最大动态 ARP 表项数目。这可以防止当一个接口所接入的某一台用户主机发起 ARP 攻击时整个设备的 ARP 表资源都被耗尽。

（2）ARP 欺骗防御

ARP 欺骗攻击是指攻击者通过发送伪造的 ARP 报文，恶意修改设备或网络内其他用户主机的 ARP 表项，造成用户或网络的报文通信异常。ARP 攻击行为存在以下危害：

1）会造成网络连接不稳定，引发用户通信中断。

2）利用 ARP 欺骗截取用户报文，进而非法获取游戏、网银、文件服务等系统的账号和口令，造成被攻击者重大利益损失。



ARP 表项更新检查

ARP 表项更新检查：设备在第一次学习到 ARP 之后，用户更新此 ARP 表项时通过发送 ARP 请求报文的方式进行确认，以防止攻击者伪造 ARP 报文修改正常用户的 ARP 表项内容。

ARP 报文合法性校验

通过检查报文中的 IP 地址、MAC 地址，直接丢弃非法的 ARP 报文，避免非法用户伪造 ARP 报文，刻意的进行 ARP 攻击。

基于 DHCP 的 ARP 绑定关系检测（DAI）

当设备收到 ARP 报文时，将此 ARP 报文的源 IP、源 MAC（Media Access Control）、收到 ARP 报文的接口及 VLAN（Virtual Local Area Network）信息和绑定表的信息进行比较，如果信息匹配，则认为是合法用户，允许此用户的 ARP 报文通过，否则认为是攻击，丢弃该 ARP 报文。本功能仅适用于 DHCP Snooping（Dynamic Host Configuration Protocol Snooping）场景。

网关防欺骗

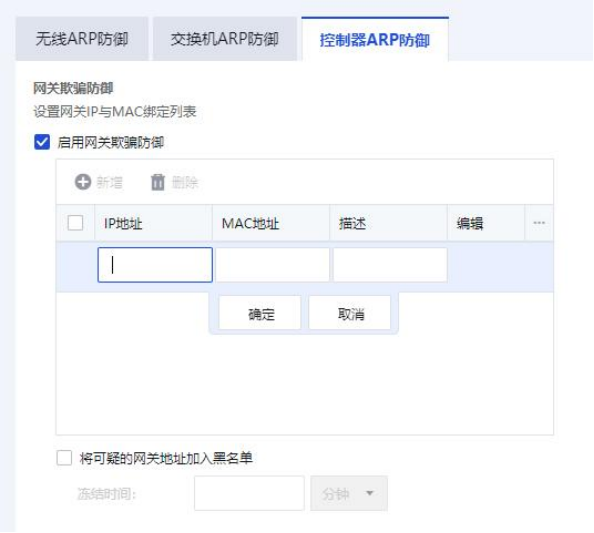
丢弃源 IP 地址为网关设备 IP 地址的 ARP 报文，防止攻击者仿冒网关，建议在网关设备上开启。

3、控制器 ARP 防御

网关欺骗防御

攻击者通过伪造 ARP 报文，截获原本发向网关的报文，对网络安全构成威胁。网关防御欺骗防御支持将配置网关 mac 和 ip 的绑定关系，可以有效遏制这种攻击。适用于集中转发环境。

注意：IP、MAC 中其中一个出现在配置中，并不满足对应关系，将被识别为网关欺骗攻击。



DHCP 防御

1、无线 DHCP 防御

系统将持续监听无线客户端的 DHCP 分配过程数据包，并从 DHCP 报文中，获取无线客户端的 MAC 地址以及分配的 IP 地址，据依据此信息构建有效的 IP，MAC 对应关系数据库。

检测无线客户端发出的 ARP 数据包，检查 IP 与 MAC 地址对应关系的合法性，丢弃不合法的 ARP 包。

2、交换机 DHCP 防御

DHCP 防御用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系，防止网络上针对 DHCP 攻击。

（1）DHCP 泛洪防御

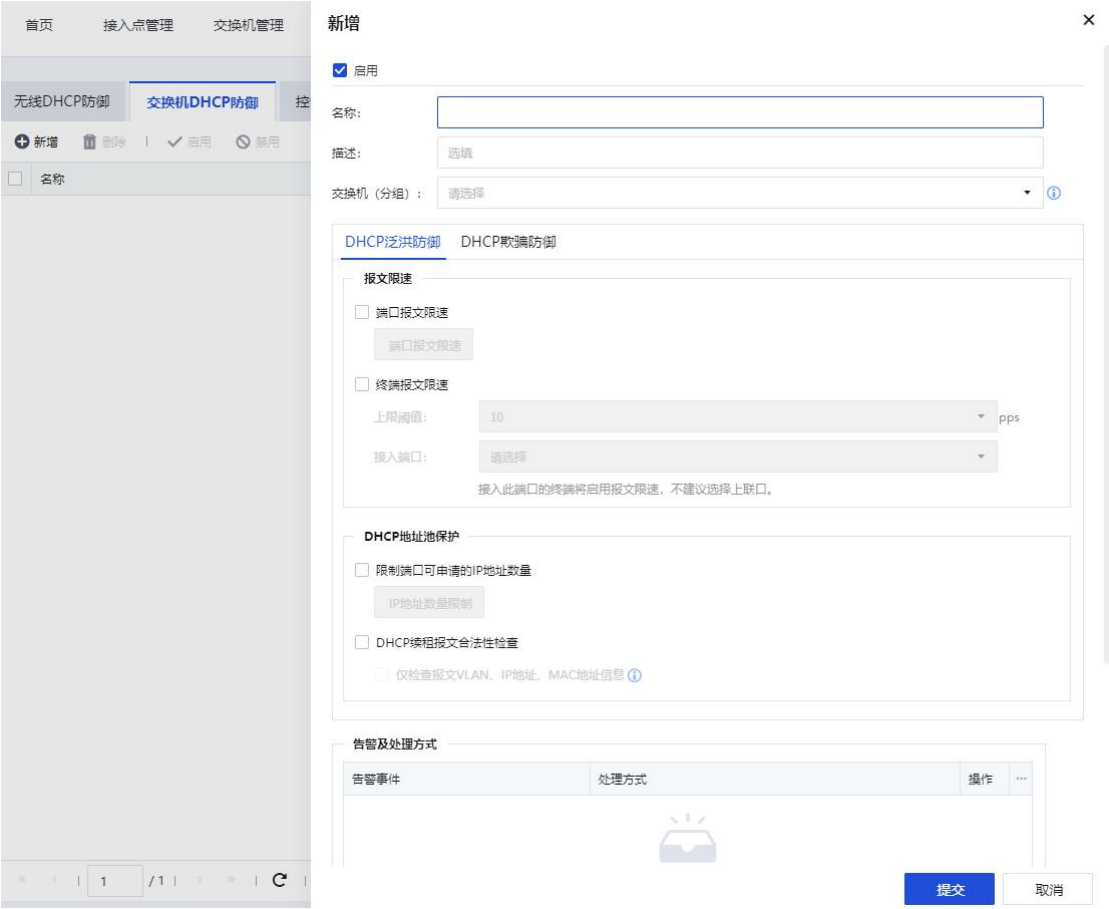
DHCP 泛洪攻击也叫拒绝服务攻击 DoS（Denial of Service），主要存在以下几种场景：

1）非法用户在短时间内发送大量 DHCP 报文，使 DHCP Server 无法正常处理报文，从而无法为客户端分配 IP 地址。

2）非法用户通过恶意申请 IP 地址，使 DHCP 服务器中的 IP 地址快速耗尽， 无法为合法用户再分配 IP 地址。

3）已获取到 IP 地址的合法用户通过向服务器发送 DHCP Request 报文用以续租 IP 地址。非法用户冒充合法用户不断向 DHCP Server 发送 DHCP Request 报文来续租 IP 地址，导致到期的 IP 地址无法正常回收，新的合法用户不能再获得 IP 地址。

4）已获取到 IP 地址的合法用户通过向服务器发送 DHCP Release 报文用以释放 IP 地址。非法用户仿冒合法用户向 DHCP Server 发送 DHCP Release 报文，使合法用户异常下线。



报文限速

通过 DHCP 报文限速功能，可以防止设备因处理大量 DHCP 报文，导致 CPU 负荷过重

而无法处理其他业务，分为基于单个交换机端口报文限速和基于源 MAC 地址报文限速。

限制端口可申请的 IP 地址数量

限制用户接入数。当用户数达到指定值时，任何用户将无法通过此接口申请到 IP 地址。

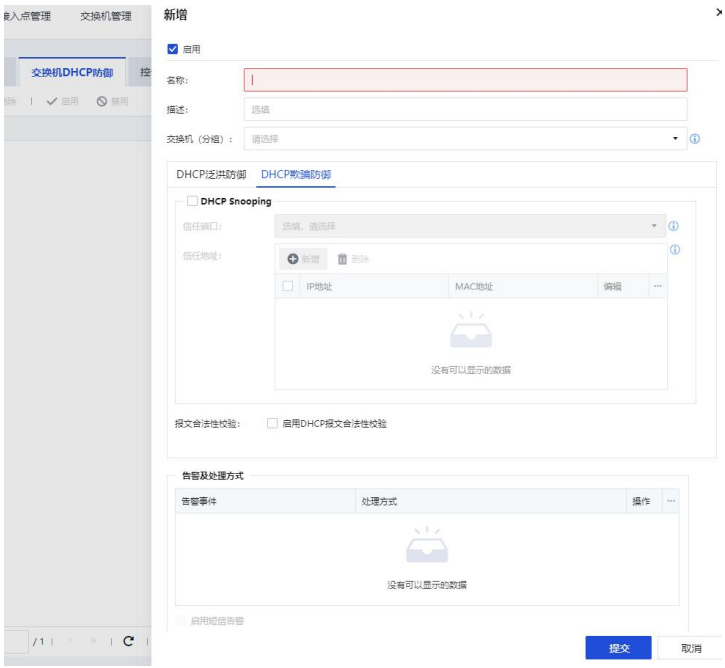
DHCP 续租报文合法性检查

在 DHCP Server 为客户端分配 IP 地址过程中，根据 DHCP 报文生成 DHCP Snooping 绑定表，该绑定表记录 MAC 地址、 IP 地址、租约时间、 VLAN ID、接口等信息，然后通过 DHCP 报文与绑定表的合法性检查，丢弃非法报文， 防止 DHCP 报文仿冒攻击。

（2）DCHP 欺骗防御

网络中如果存在私自架设的 DHCP Server 仿冒者，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。

DHCP Snooping 信任功能可以控制 DHCP 服务器应答报文的来源，以防止网络中可能存在的 DHCP Server 仿冒者为 DHCP 客户端分配 IP 地址及其他配置信息。



报文合法性校验

设备具有防御网络上 DHCP 攻击的能力，增强了设备的可靠性，保障通信网络的正常运行。为用户提供更安全的网络环境，更稳定的网络服务。

DHCP Snooping

DHCP Snooping 是 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，防止网络上针对 DHCP 攻击。

信任端口正常转发接收到的 DHCP 应答报文，非信任端口在接收到 DHCP 服务器响应的 DHCP Ack、DHCP Nak、DHCP Offer 和 DHCP Decline 报文后，丢弃该报文。

信任 IP 地址是指当 DHCP 响应报文的源 IP 地址与配置项相匹配时，允许报文通过。

信任 MAC 地址是指当 DHCP 响应报文的源 MAC 地址与配置项相匹配时，允许报文通过。

信任 IP+MAC 地址是指当 DHCP 响应报文的源 MAC 地址和源 IP 地址与配置项完全匹配时，允许报文通过。

3、控制器 DHCP 防御

（1）启用控制器受信任的 DHCP 服务器

在绝大部分的无线网络部署中，无线客户端都使用 DHCP 方式获取 IP 地址、网关、DNS 等。因此 DHCP 服务也被视为无线网络正常运行的基础。DHCP 服务基于广播方式运作，如果同一个子网内运行了多个 DHCP 服务器，则客户端发起 DHCP 请求后，会收到多个回应，客户端会选择回应最快消息中指定的 IP 地址。因此如果子网内存在非法的 DHCP 服务器，则会干扰正常的 DHCP 过程，客户端可能获取到错误的 IP 地址，导致无法访问网络。

启用“控制器受信任的 DHCP 服务器”选项，并配置合法的 DHCP 服务器 IP 地址，NAC 及接入点将只转发来自受信任 DHCP 服务器的 DHCP 报文，来自其它 IP 地址的

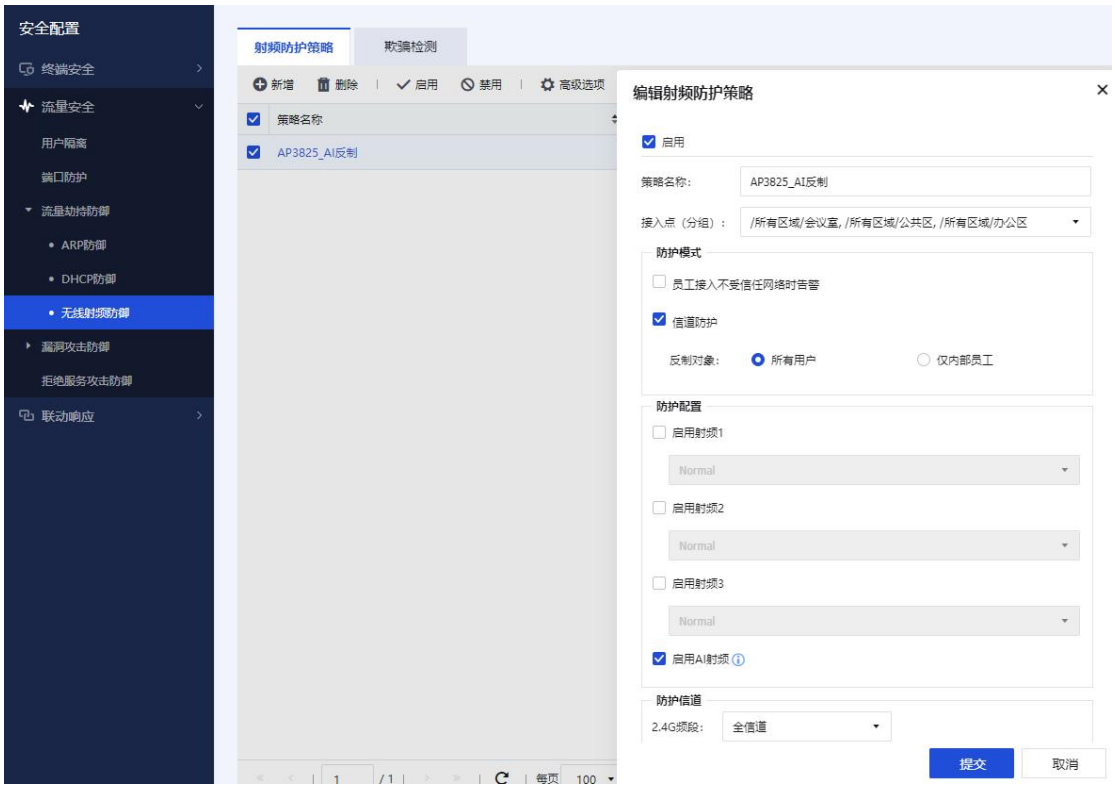
DHCP 服务报文将被丢弃，从而保证 DHCP 服务能正常运行，不受干扰。

（2）DHCP 地址仿冒申请防御

默认开启，防御 DHCP 泛洪攻击行为，防止 DHCP 地址池被耗尽。

无线射频防御

1、射频防护策略



配置信道保护/信道压制/自定义可以按一个或多个接入点分组划分出一个区域保护这个区域内的射频信号不被其他 ap 的射频信号干扰。

当防护模式为信道保护时，如果射频是 Normal 模式，则只反制工作信道；如果射频是 Hybrid 模式，则可以反制工作信道，以及工作信道±1/±2 信道。

- 内部员工：接入高级选项配置的认证类型的无线网络的员工即为受监控的内部员工。
- 非信任无线网络：非本控制器无线网络并且不在受信任 SSID 列表的无线网络。
- 检测内部员工接入非信任网络行为：监控内部员工接入非法无线网络的行为并产生告警日志。
- 信道保护/信道压制/自定义+内部员工：只有内部员工受反制影响，无法连接非法无线网络，内部员工连接非法无线网络会产生接入非法无线网络的告警日志。
- 信道保护/信道压制/自定义+所有用户：所有用户都会受反制影响，无法连接非法无线网络。

2、欺骗检测

（1）无线欺骗攻击

无线欺骗攻击是指攻击者假冒其他设备/终端的名义发送报文。例如：假冒无线接入点的身份，向无线客户端发送解除认证的报文，导致无线终端断开无线连接。启用欺骗攻击检测可以识别此类攻击，将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

（2）BSSID 冲突检测

BSSID 冲突检测是指检测到环境中 BSSID 地址冲突，可能会造成无线终端接入到有冲突的 BSSID 的 AP，会造成网络掉线，丢包等不可预知的情况。

3.7.2.4. 漏洞攻击防御

扫描防御

该功能可以防御网络中 ARP、IP、端口扫描攻击。

防御选项：防御 ARP 扫描，IP 扫描，端口扫描攻击，超过设置阈值的用户行为将被识别为扫描攻击。

防御动作：可以将攻击者加入黑名单，并支持设置冻结的时间。

漏洞利用防御

1、东西向流量防御

（1）观察区域/保护区域

可以将指定交换机端口或认证策略配置为观察区域/保护区域，观察区域默认放通所有入站访问流量，保护区域默认拦截所有入站访问流量。若同时配置交换机端口组和交换机，则满足两

者的交换机端口才生效；若同时配置无线网络/接入点有线认证策略和接入点，也是只有满足两者的认证策略才生效。

（2）观察角色/保护角色

可以将指定角色配置为观察角色/保护角色，观察角色默认放通所有入站访问流量，保护角色默认拦截所有入站访问流量。若同时满足观察角色/保护角色和观察区域/保护区域，则满足角色策略优先。

（2）访问黑名单

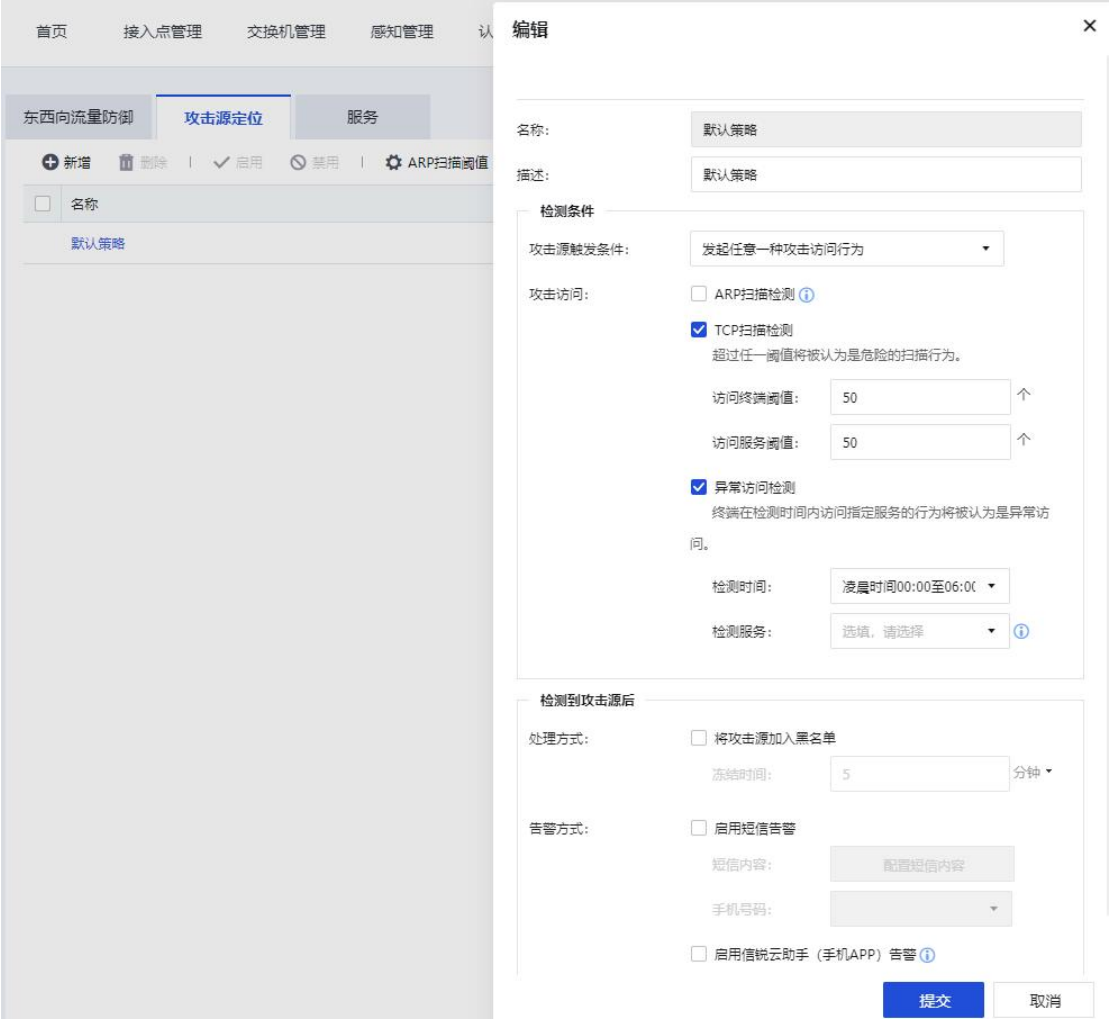
可设置黑名单，拒绝源访问区域的终端访问信任区域的指定服务，源访问区域可以是所有区域，也可以是指定区域。

（3）访问白名单

可设置白名单，允许源访问区域的终端访问保护区域的指定服务，源访问区域可以是所有区域，也可以是指定区域。

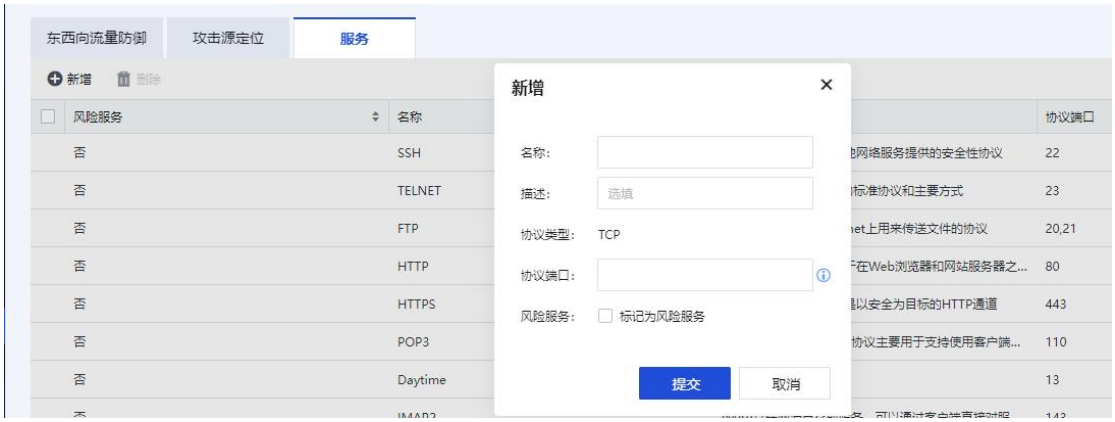
2、攻击源定位

通过对终端的访问行为判断是否是攻击终端。触发的条件有：发起任意一种攻击访问行为和检测间隔内发起多种攻击访问行为；检测的攻击访问类型有：ARP 扫描检测、TCP 扫描、异常访问检测；检测到攻击后的处理方式有：将攻击源加入黑名单、启用短信告警、启用信锐云助手告警。可通过添加攻击源白名单来排除攻击终端。



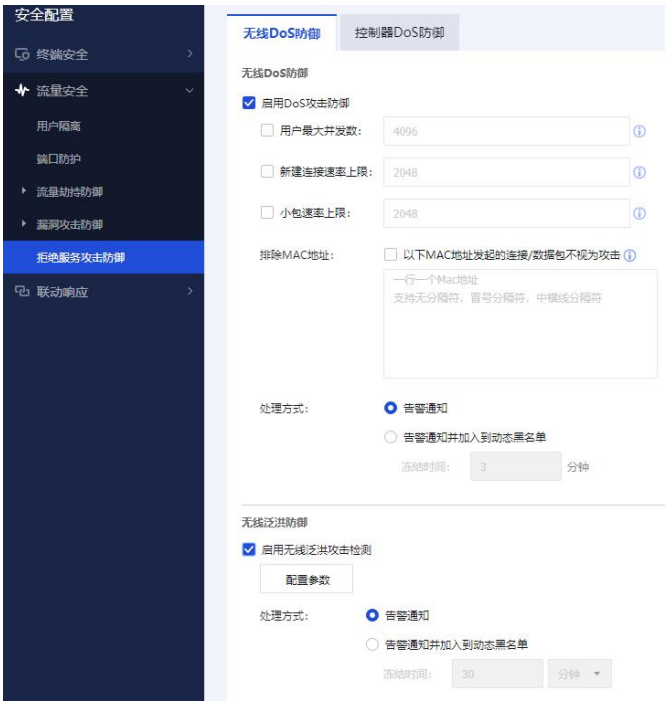
3、服务

可设置白名单，允许源访问区域的终端访问保护区域的指定服务，源访问区域可以是所有区域，也可以是指定区域。



3.7.2.5. 拒绝服务攻击防御

无线 DDOS 防御



DDoS 防御

DDoS 攻击在众多网络攻击技术中，是一种简单有效并且具有很大危害性的攻击方法。它通过各种手段消耗网络带宽和系统资源，使网络陷于瘫痪状态。在无线网络中，大部分 DDoS 攻

击行为并不是由用户故意发起的，而是由于计算机感染了病毒或恶意软件造成的。

DDoS 攻击防御模块通过统计无线客户端的数据包速率，连接数等信息，有效识别并阻挡无线客户端发起的 DDoS 攻击行为，降低对无线网络的影响。

无线泛洪攻击（Flooding 攻击）

NAC 在短时间内接收大量同种类型的报文，将导致系统资源被大量占用，可能无法处理无线用户的数据报文。启用泛洪攻击检测可以识别此类攻击，并自动将发起攻击的终端 MAC 地址添加到黑名单，一段时间内禁止接入无线网络。

控制器 DDOS 防御

DHCP 报文泛洪攻击是指：恶意用户利用工具伪造大量 DHCP 报文发送到服务器，恶意耗尽了 IP 资源，使得合法用户无法获得 IP 资源。

启用 DHCP 泛洪攻击检测

用户启用 DHCP 泛洪攻击检测后，当控制器每秒收到的 DHCP 报文数大于阈值时，系统将提供告警信息，帮助管理员及时处理风险问题。

3.7.3. 联动响应

3.7.3.1. 安全联动

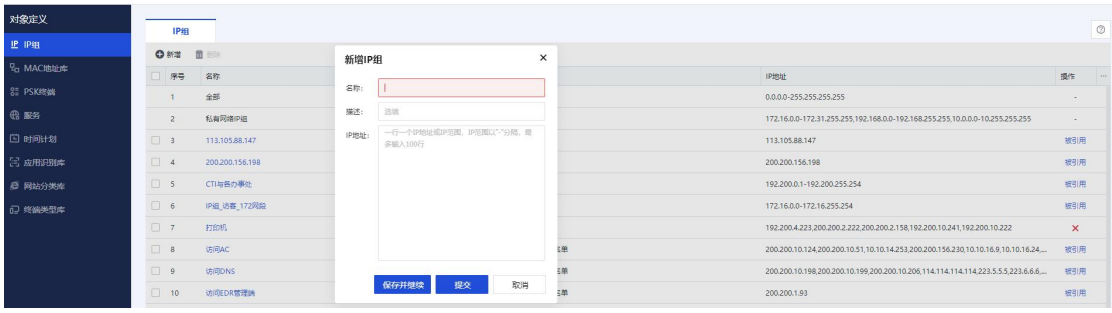
支持联动深信服安全设备进行用户安全可视化和内网边缘安全管理。

3.8. 对象定义

『对象定义』用于配置【IP 组】、【MAC 地址库】、【服务】、【应用识别库】、【时间计划】、【PSK 终端】、【网站分类库】、【终端类型库】。这里定义的对象，在后续的模块中会使用到，比如 IP 组和服务会应用到访问控制策略中，MAC 地址库将在使用 MAC 地址认证时黑白名单调用。

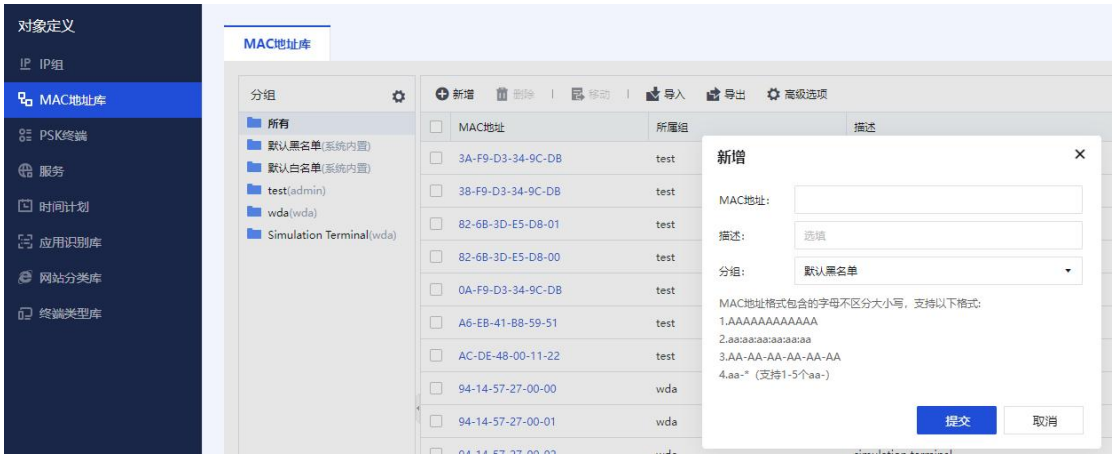
3.8.1. IP 组

此页面可查看和新增 IP 组，IP 组用于后续【角色授权】中的【访问控制策略】，以及后续的【网络配置】中的【地址转换】。



3.8.2. MAC 地址库

将一个、多个 MAC 地址划分为一个 MAC 组，以便在系统的其它功能中调用，例如 web 免认证。默认有默认黑名单和默认白名单两个分组，用户可以自定义分组。



3.8.3. PSK 终端

1、适用范围：

智能 PSK 终端页面配置的终端只针对智能 PSK 无线网络有效。

2、使用场景：

为防止 PSK 密钥泄漏，杜绝 PSK 密钥分享带来的网络安全隐患，可通过设置私有密钥实现一人一机一密码，保障网络安全。

3、问题排查：

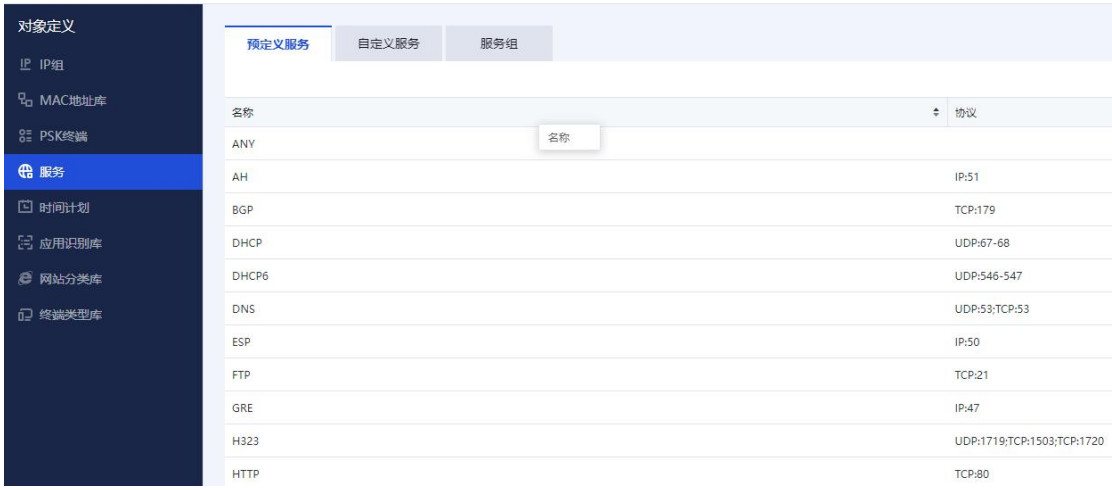
信锐智能终端如果连接过其他 NAC，请删除该终端的记录，重新添加。

3.8.4. 服务

『服务』分为【预定义服务】、【自定义服务】和【服务组】，【服务组】是【预定义服务】或【自定义服务】或 2 者的组合。用于后续【角色授权】中的【访问控制策略】。

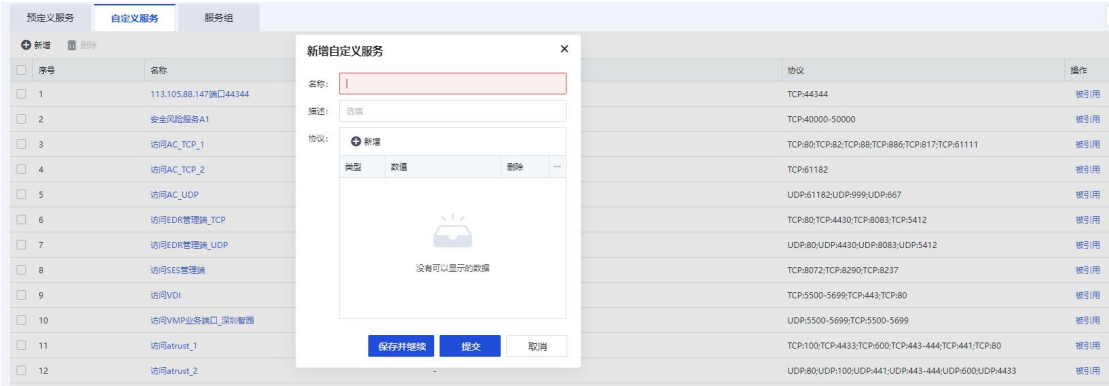
3.8.4.1. 预定定义服务

【预定义服务】包括了 TCP，UDP 协议中各种常用端口号包含的应用协议，比如 BGP，DHCP、DNS、HTTP、FTP、SNMP、SSH 等。



3.8.4.2. 自定义服务

【自定义服务】可以让客户自定义所有需的不在预定义范围内的服务，比如客户自己的一些 C/S 架构的 OA 系统所使用的特殊端口号，都可以在这里自定义配置，配置界面如下：



3.8.4.3. 服务组

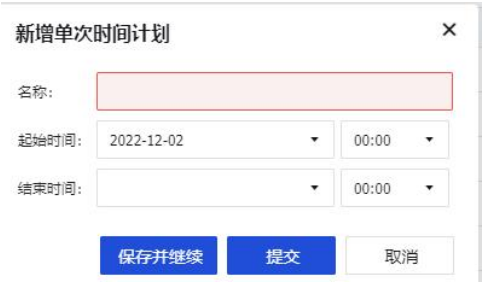
【服务组】就是【预定义服务】和【自定义服务】的组合，便于做复杂的控制策略时方便调用。而且可以节省原本需要多条控制策略的条数。

3.8.5. 时间计划

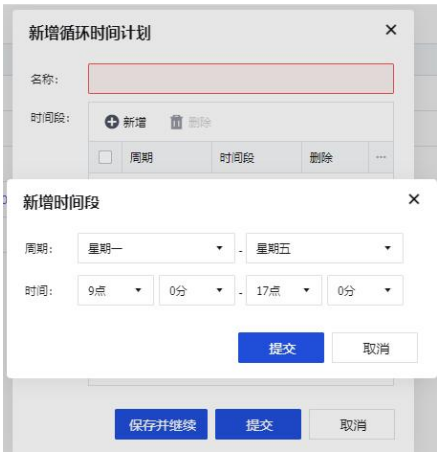
对于不同的无线或有线用户，我们需要在不同的时间段设置不同的访问控制策略以及流控策略，比如上班时间或下班时间，就需要配置时间计划，为了便于后续设置【认证授权】-【角色授权】-【访问控制策略】的生效时间，需要提前设置时间计划，『时间计划』分为【单次时间计划】和【循环时间计划】。

新增单次时间计划和循环时间计划:

设置循环时间时，大多数客户可以按照上班时间和下班时间，以及节假日方式设置循环时间，便与管理。



点击新增循环时间计划:

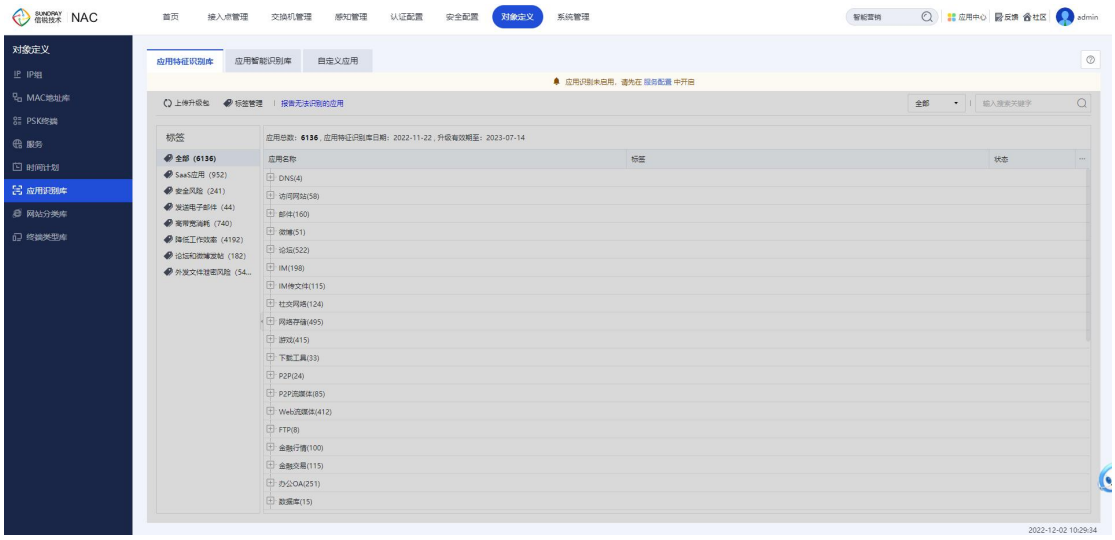


3.8.6. 应用识别库

『应用识别库』包括:【应用特征识别库】、【应用智能识别库】、【自定义应用】三类,网络应用流经 NAC 时,可通过特征,识别其应用类型,识别后,即可对连接进行基于应用策略控制、资源调度及流量审计。

3.8.6.1. 应用特征识别库

【应用特征识别库】中记录着应用的字节流特征,通过持续不断的收集及更新,保证应用识别的正确性,应用特征识别库升级需要序列号授权,过期后无法更新。



3.8.6.2. 应用智能识别库

某些类型的网络应用没有固定的字节流特征，需要通过智能的方式识别流量间的关联性等来识别出其类型，应用智能识别库目前只支持 P2P 行为，支持灵敏度、排除端口的设置。

3.8.6.3. 自定义应用

内网应用往往由于其私有性，应用特征识别库无法收集其网络流特征，可以将数据包方向、协议类型、IP 地址、端口号及域名作为应用的规则特征，自定义某种类型的应用，自定义应用同样适用于外网应用。

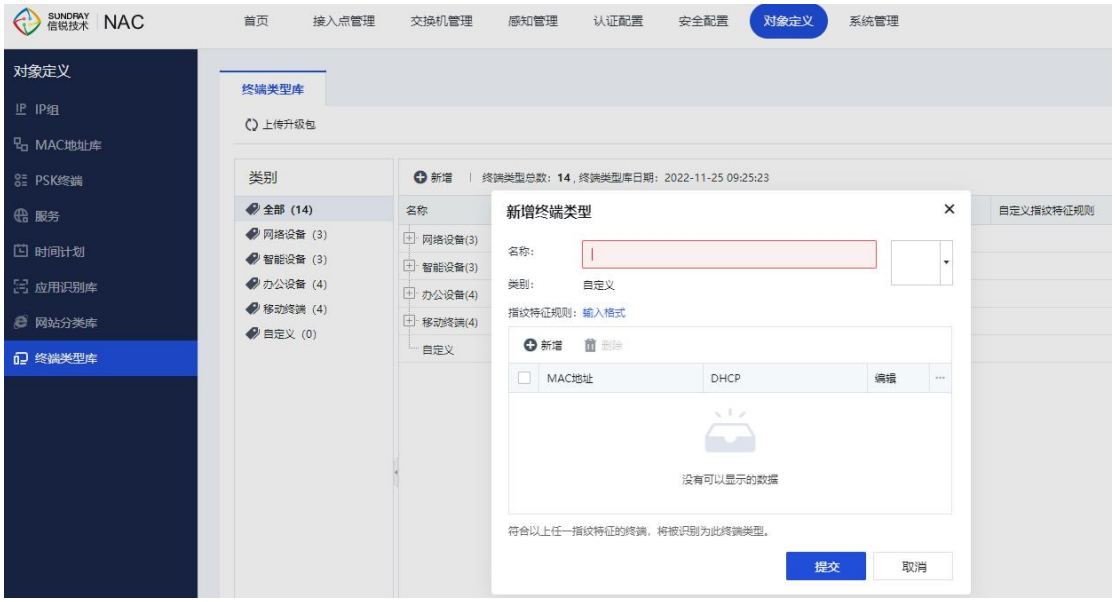
3.8.7. URL 分类库

『URL 分类库』中是由信锐技术自主研发并收集的全国最大、最全、最专业的 URL 分类库。关于 URL 规则库的使用，需要在【认证授权】-【角色授权】-【访问控制策略】中新增规则，选择应用的方式来调用。另外对于少部分，客户内网自由的域名系统，如果无法识别到，用户还自定义 URL 类别，可将 URL 设置为内置的 URL 类别或自定义 URL 类别，也可以设置域名关键字，模糊匹配为某种类别。并设置自定义的 URL 类别优先级最高来优先调用。

URL 分类库的升级需要序列号授权，过期后无法更新。

3.8.8. 终端类型库

终端类型库中记录着终端的指纹特征，通过持续不断的收集及更新，保证终端类型识别的正确性，终端类型特征库支持手动和联网时自动更新。



3.9. 系统管理

3.9.1. 系统配置

3.9.1.1. 系统选项

系统选项可以配置关于设备的基本信息，包括设备的中英版本切换，可以在此选择切换。

1、设备信息

- 设备名称：填写设备的名称
- 默认编码：选择你所在国家/地区的本地编码，例如简体中文选择 GBK，繁体中文选择 BIG5。设备的部分功能需要依赖于正确地选择此编码。例如在 Windows 无线客户端中，PEAP-MSCHAPv2 认证过程中发送的用户名使用本地编码格式，而本地用户数据库中用户

名为 utf-8 编码。如果需要支持中文用户名，则系统在认证过程中需要知道原始编码，并转换为 utf-8 编码。

- HTTPS 端口：控制台登录界面端口
- 设备证书：给 NAC 设备设置证书，用于安全登录 NAC 设备。
- 控制隧道端口：默认控制隧道端口号 7070，手动指定端口号范围：1024-65535。
- 数据隧道端口：默认数据隧道端口号 7077，手动指定端口号范围：1024-65535。
- 发现控制器端口：发现控制器端口号默认 7777。
- 发现控制器备用端口：手动指定备用端口号范围：1024-65535。修改备用端口号后，默认的端口 7777 还可以发现控制器。
- 集中管理端口：默认集中管理端口号 5000，手动指定端口号范围：1024-65535。

2、系统安全选项

控制台超时：管理员登录控制台后，如果在设定的超时时间内，未进行任何操作，则系统会注销此次登录。

3、webAgent

webAgent 功能用于解决接入点跨广域网/公网远程部署时，由于控制器没有固定 IP 地址，导致接入点无法与控制器无法进行通信的问题。使用该功能时，请联系客服或技术支持获取 webAgent 服务。

注：开启 webagent 功能时，需要开放 7777（udp 协议）、7070（tcp 协议）、7077（udp 协议）、800（tcp 协议）端口号。

3.9.1.2. 日期时间

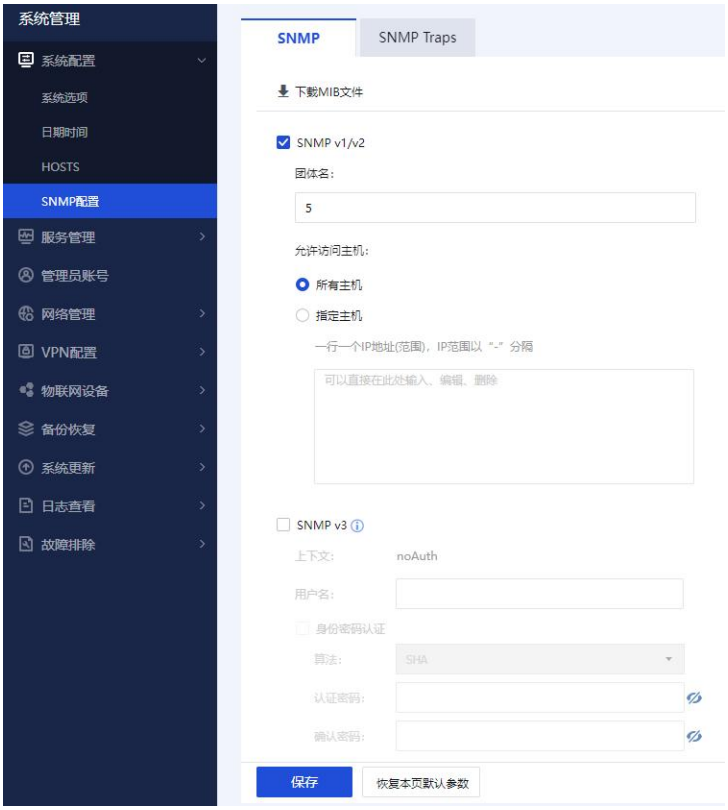
设置系统时间，可以通过获取本地 PC 或通过同步 NTP 服务器的方式同步时间，如下图，并可以设置设备工作所在的时区。

3.9.1.3. HOSTS

当指定我们设备作为域名解析服务器时，可以通过设置 HOSTS 对外解析域名已经设置好的域名，而且后续还可以设置 DNS 代理，真正实现以我们设备的 IP 地址作为服务器解析所有的域名。当网络中设置以 NAC 的 IP 为 DNS 服务器时，并设置了 HOSTS 中对于域名 wwww.adminwlan.com 的 IP 时，AP 会以该域名对应的 IP 去自动发现 NAC，实现 NAC 对 AP 的管控。

3.9.1.4. SNMP 配置

SNMP(Simple Network Management Protocol,简单网络管理协议)，用于管理网络中上众多的软硬件平台。开启后可以通过 snmp 协议查询本设备系统信息，如设备型号，内存使用，硬盘使用率，cpu 消耗等。



SNMP V1/V2

SNMP 的第一版本和第二版本。它们都是基于团体名进行报文认证。

SNMP V3

SNMP 的第三版本此版本提供重要的安全性功能，其中就包括了认证和加密两项。认证需要提供认证方式（MD5，SHA）和认证密码。加密需要提供加密方式（DES）和加密密钥。

MIB

MIB（Management Information Base，管理信息库），是由网络管理协议访问的管理对象数据库，也可理解为是所有可管理对象的集合。下载本设备 MIB 后，再导入到相应的管理端后，可以管理或查询的本设备的一些基本信息，如设备信号，内存使用，硬盘使用，CPU 消耗等。

SNMP Traps

SNMP trap 又称 SNMP 陷阱，启用后可以让本设备主动发送信息到管理端，而不需要等到的管理端轮询后再发送。需要配置管理端的 IP 地址和端口，以及团体名。支持向多个管理端发送信息。

3.9.2. 服务管理

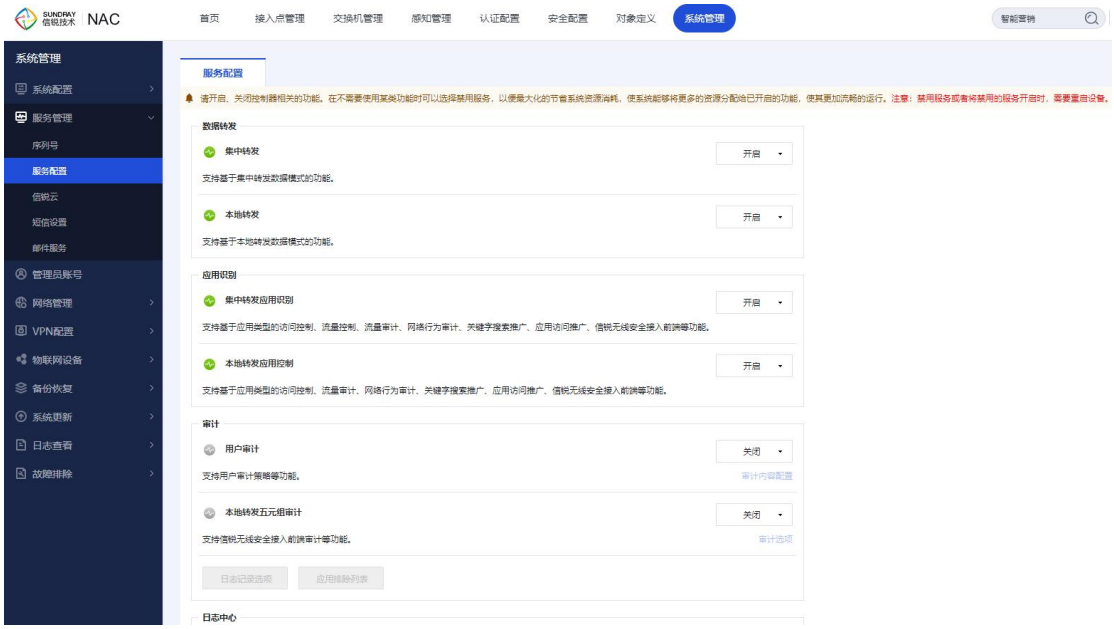
『应用中心』包含【序列号】、【服务配置】、【信锐云】、【短信设置】、【邮件服务】五个功能模块。

3.9.2.1. 序列号

使用 NAC 前，必须向设备供应商购买有效的产品或功能序列号。NAC 的版本序列号包括设备序列号和软件升级序列号，设备序列号决定了一个 NAC 最多可以管理 AP 的个数。软件升级序列有效，NAC 才可以正常升级软件版本，配置界面如下：

3.9.2.2. 服务配置

本页面可以配置控制器需要开启、关闭哪些功能，在不需要使用某类功能时可以选择禁用服务，以便最大化的节省系统资源消耗，使系统能够将更多的资源分配给已开启的功能，使其更加流畅的运行。



数据转发

集中转发：适用于所有接入点都使用集中转发模式。禁用服务可以释放大量资源，需要重启设备。该服务禁用状态时“集中转发应用识别”服务和集中转发无线网络也将被禁用。

本地转发：适用于所有接入点都使用本地转发模式。禁用服务可以释放大量资源，需要重启设备。该服务禁用状态时“本地转发应用识别”服务和本地转发无线网络也将被禁用。

应用识别

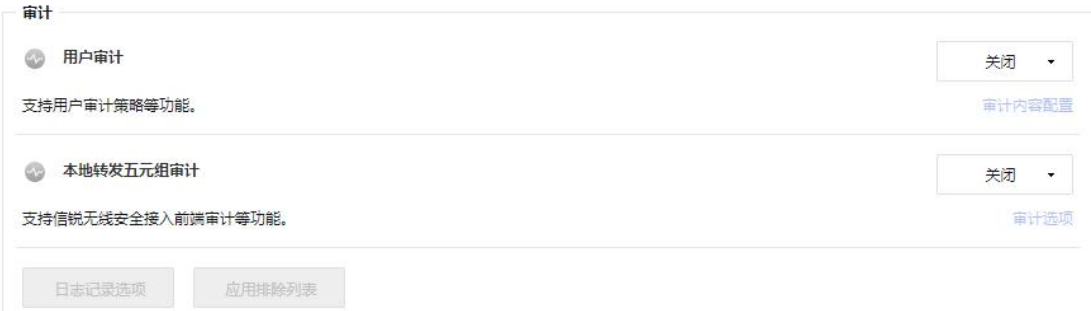
集中转发应用识别：功能开启之后，将会识别集中转发用户的应用。关闭后可以释放部分资源，无需重启设备。禁用服务可以释放大量资源，需要重启设备。

开启本地转发应用识别：功能开启之后，将会识别本地转发用户的应用。启用功能之后，需要在本地转发应用识别选项中选择，需要开启识别的本地转发的无线网络或是接入点有线认证策略，默认不勾选。功能开启之后，将会消耗接入点 2%-5%的上行带宽。

审计

用户审计：开启功能，需要启用内置日志中心或是配置一个外置的日志中心。

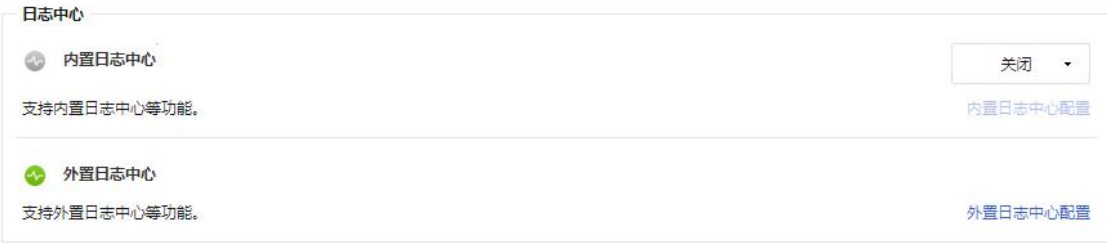
本地转发五元组审计：开启功能，可以审计本地转发用户的五元组信息。



日志中心

内置日志中心：开启和关闭内置日志中心，配置磁盘预警和自动删除数据选项。

外置日志中心：开启和关闭内置日志中心，管理外置日志中心的同步账号。



特色服务

信锐无线安全接入前端：开启、关闭信锐无线安全接入前端服务。服务开启时将采集的终端信息、上网行为信息等上报给第三方设备。

物联网服务：开启、关闭物联网功能。服务开启时才能进行物联网设备的部署和管理

VPN 服务：开启、关闭 VPN 服务。服务开启时才能在 VPN 配置页面进行配置。

数据分析平台：开启、关闭数据分析平台服务。服务开启时才允许进行数据分析平台配置项配置。

3.9.2.3. 信锐云

云服务主要是为了帮助企业 IT 管理员更好的服务企业员工，增加紧急事件远程处理的能力，

方便 IT 管理员管理企业无线，在有无线故障时 IT 能够及时知晓并作出响应。

要加入云管家，首先需向云服务器注册企业账号，信锐云服务现在支持账号登录和短信登录两种方式。

企业账号注册成功后用该企业账号登录，控制器即可加入到云管家。

如果显示“在线”，表示成功加入云管家，如果显示“离线”，表示控制器与云管家的连接断开。

成功加入云管家之后，用手机扫描页面上的二维码，下载信锐云管家 APP，并用注册的账号登录，就可以进入到 app 管理页面，方便的管理控制器了。

3.9.2.4. 短信设置

在部署短信认证的无线网络时，需要先启用短信认证服务，并正确配置短信发送参数。

系统支持的短信发送方式：通过连接到 NAC 串口的短信猫发送、通过连接到外部服务器的短信猫发送、通过短信网关发送。

说明：如果 NAC 部署的机房中，手机网络信号差，导致无法发送短信。则可以选择把短信猫连接到一台服务器，并把服务器部署到此机房以外，且信号良好的环境中，由此服务器来代理发送短信。

3.9.2.5. 邮件服务

本地用户数据库中邮箱绑定类型的账号绑定邮箱后，可以通过邮件找回密码，管理员也可以将用户名密码发送到用户绑定的邮箱中。使用之前需要启用并正确配置邮件服务。

- 发件人邮箱地址：邮件发件人账号，需要在 smtp 服务器上注册。
- SMTP 服务器器：邮件发送服务器，可以填写域名或者服务器 ip 地址，默认端口 25。
- 用户名：邮件服务器校验使用的用户名，建议与发件人邮箱地址保存一致。
- 密码：邮件服务器校验密码，即用户名对应的密码。

3.9.3. 管理员账号

默认系统内置了 admin 超级管理员，用于登录设备。

超级管理员账号：默认 admin/admin 是 webui 的超级管理员，只能修改自身密码，可以新增和删除和修改其他用户的用户名和密码。

新建分为新建普通管理员和新建数据分析管理员。

3.9.3.1. 普通管理员

可以查看控制台页面和营销中心页面，支持按页面配置权限，按分支或接入点分组配置权限，按本地用户组织结构配置权限，热点地图权限，并且可以关联云管家账号。

支持创建公有配置，查看或修改其他管理员的配置。

3.9.3.2. 数据分析管理员

只允许登陆营销中心页面，支持针对接入点和热点地图分权。

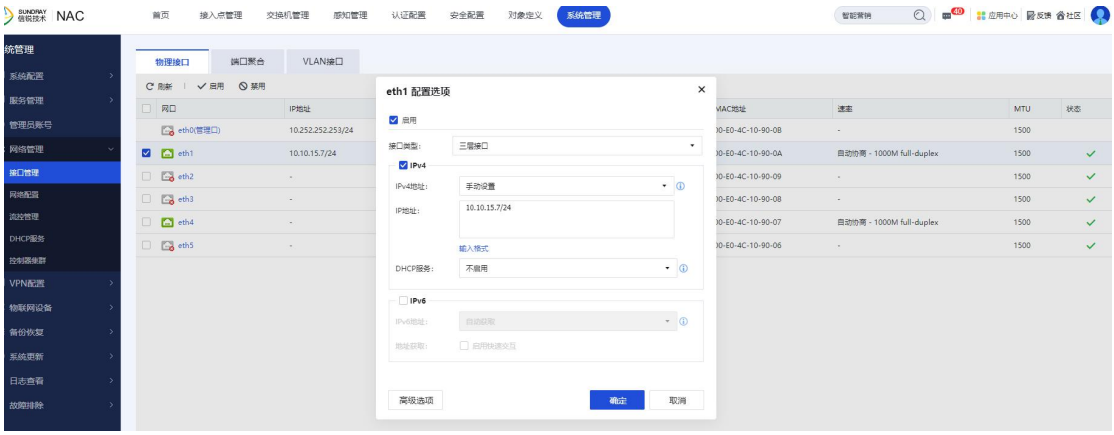
3.9.4. 网络管理

3.9.4.1. 接口管理

接口管理主要用于设置接口的 IP 地址以及工作模式，接口的工作模式是由部署需求决定的，需要根据网络环境设置合理的接口地址与工作模式，NAC 才能正常工作。

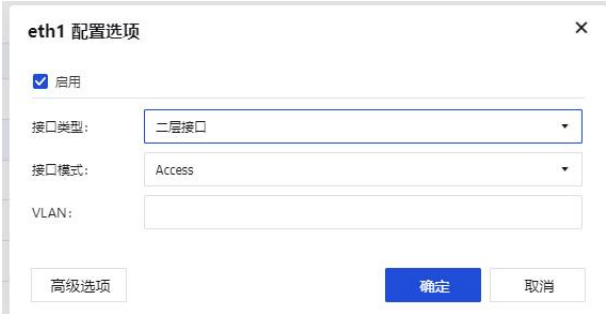
物理接口

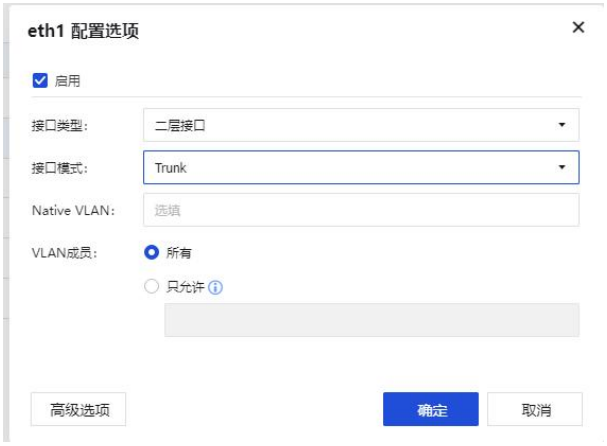
物理接口中，eth0 默认是管理口，属性是 3 层路由口，默认 IP 地址是 10.252.252.252，掩码：255.255.255.0。



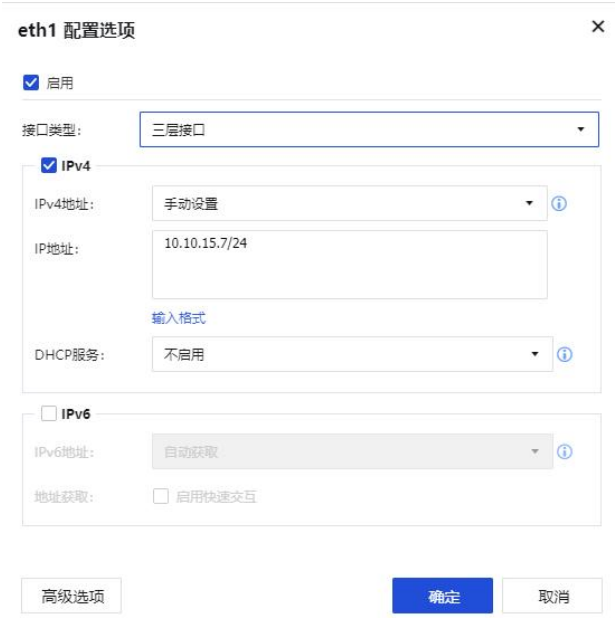
➢ 二层接口

接口可以设置为 2 层接口，2 层接口包括 access 模式和 trunk 模式两种，截图如下：





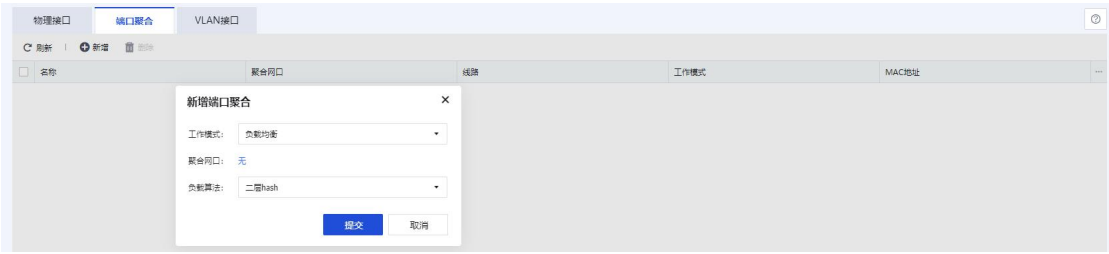
➢ **三层接口**



三层接口支持自动获取 IP，配置固定 IP、PPPOE 拨号，当配置固定 IP 时，可以启用配置 DHCP 服务器。

端口聚合

当有需要使用多个网口聚合的环境时，可以配置端口聚合功能，控制器使用的聚合协议为手动聚合模式。

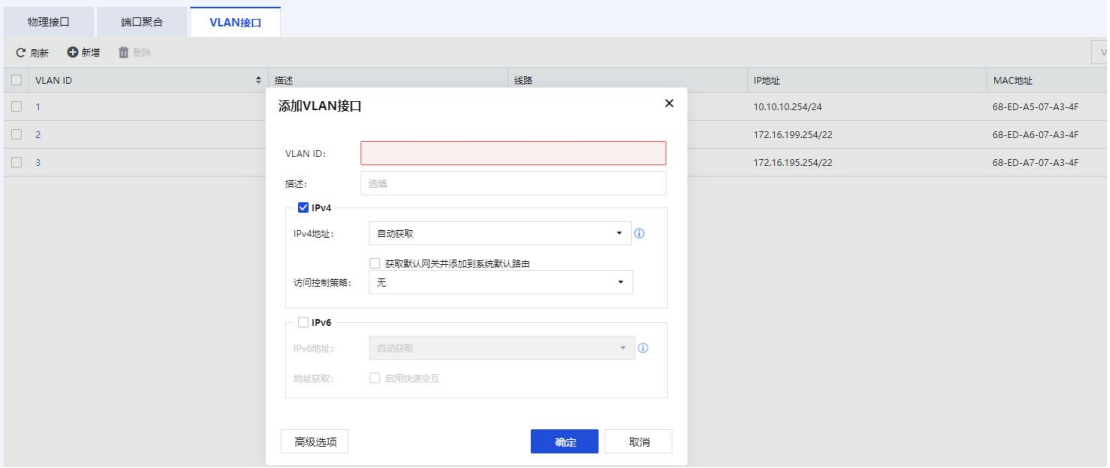


聚合接口包括主备模式的，主接口先跑流量，当主接口故障时，备份网口启用，如果启用抢占模式，当主接口从故障中恢复过来时，会抢占优先跑数据。

聚合接口还可以有负载均衡的方式，负载均衡时，可以选择多个网口，以 3 层 Hash 方式或 2 层 Hash 方式进行负载，如下图：

VLAN 接口

VLAN 接口在需要配置 3 层虚拟接口的时候可以配置，配置界面如下：



编辑 VLAN 接口界面如下，也可以启用 DHCP 服务，方法与界面同物理接口的 3 层口配置：

3.9.4.2. 网络配置

网络配置主要包括以下模块：【静态路由】、【网络 IP 组】、【策略路由】、【SNAT 地址池】、【地址转换】、【DNS】六个部分。

静态路由

静态路由：静态路由，填写目的地址，网络掩码，下一跳，并选择自动选择接口，并设置度

量值即可。静态路由配置支持 IPv4 与 IPv6。一般为了保障 NAC 能正常上网，需要配置 8 个 0 的默认静态路由，尤其是在【接口管理】处，配置的 3 层接口都是手动配置时。

当 3 层接口配置了 DHCP 时，可以勾选设置默认网关自动添加系统路由，也会后台自动添加 8 个 0 的默认静态路由，保障 NAC 可以正常上网，如下图：

网络 IP 组

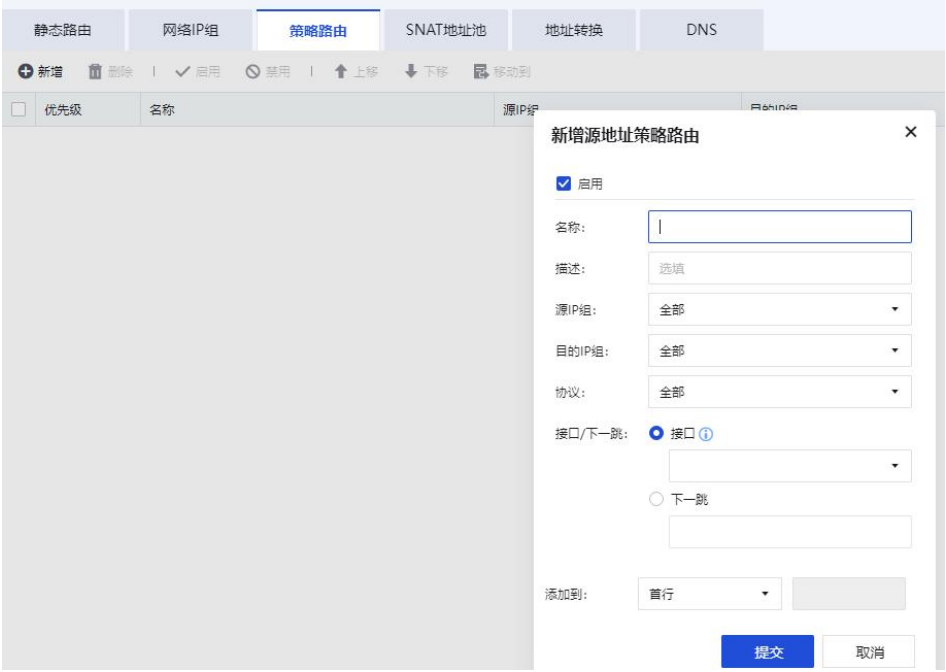
将一个、多个 IP 地址或 IP 段划分为一个 IP 组，以便在网络配置中调用

支持输入多个 IP 地址、IP 范围、网段，例如：

- IP 地址：192.168.1.1
- IP 范围：192.168.1.10-192.168.1.100
- 网段：192.168.1.0/24
- 网段：192.168.1.0/255.255.255.0

策略路由

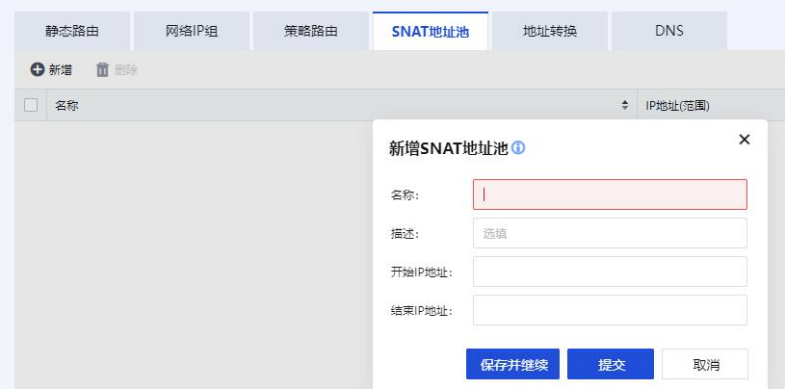
策略路由可以根据不同的源 IP 和目的 IP，以及协议，自动选择下一跳进行数据包发送选路，更好的适应的复杂网络环境的适应能力，如下图：



SNAT 地址池

SNAT 指的是源地址转换，SNAT 地址池是指源 IP 转换后的地址范围。通常 SNAT 地址池中的 IP 比较多，不方便配置在接口中。引用 SNAT 地址池后，将自动启用 ARP 代理，以保证

SNAT 地址池中的 IP 能正常使用。



地址转换

地址转换包括【源地址转换】、【目的地址转换】、【双向地址转换】三种类型，下面将一一介绍

➢ 源地址转换

源地址转换也称为 SNAT，主要用与给无线终端设置代理上网规则的，当无线终端采用集中转发模式，并给无线终端分配了私有 IP 地址时，一般都需要在 NAC 上配置源地址转换的代理上网规则。

➢ 目的地址转换

目的地址转换也叫做 DNAT，常用于内网有服务器需要发布，NAC 以网关模式部署时，对内网进行端口映射，配置方法如上图。该功能针对无线终端用户用得很少。

DNS

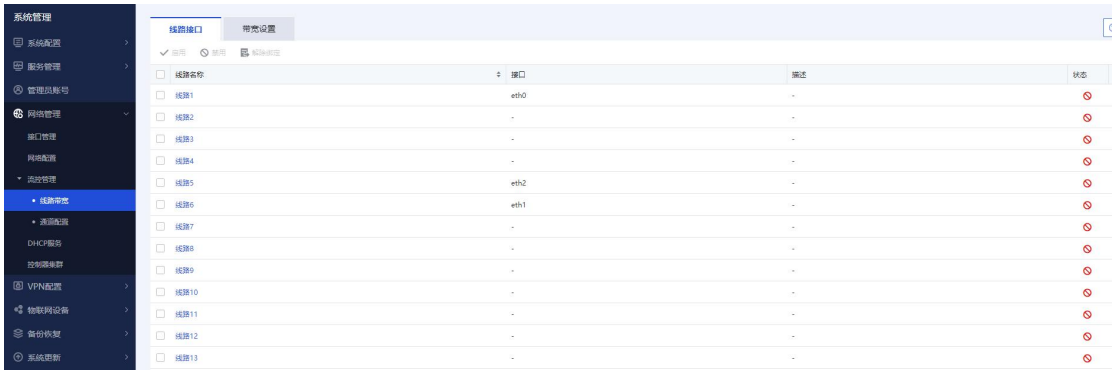
配置 NAC 设备的自身上网的 DNS 服务器，用于 NAC 自身的上网，NTP 服务同步，系统更新以及针对内网启用 DNS 代理功能。

当启用 DNS 代理功能时，内网的 PC 和无线终端，可以设置设备的接口作为 DNS 服务器解析服务器来配置，可以保证这些用户能正常解析域名上网。

3.9.4.3. 流控管理

线路带宽

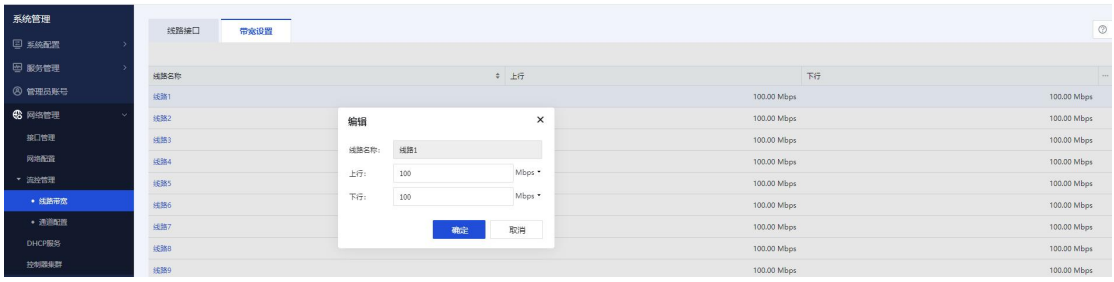
线路带宽配置是为了，在流控与安全中，调用时使用。线路带宽基于接口配置，且 NAC 没有明显区分外网口与内网口，从某个接口进，则这条流对于这个接口属于下行，从某个接口出，则这条流对这个接口属于上行。有需要时，可以针对内网和外网设置不同接口对应线路来进行流控。



设备在正常转发数据的时候，数据会从一个接口进，从另外一个接口出，在这个接口上配置

了线路，经过这个线路的数据才能被流控，最多支持 16 条线路(设备型号不同支持最大线路数不同)。 在配置线路的时候，接口类型可以有多种选择：物理口、三层 vlanif 口、二层聚合口，可以根据不同的组网需要选择不同类型的接口。在选择接口的实时候需要遵循以下几个原则：

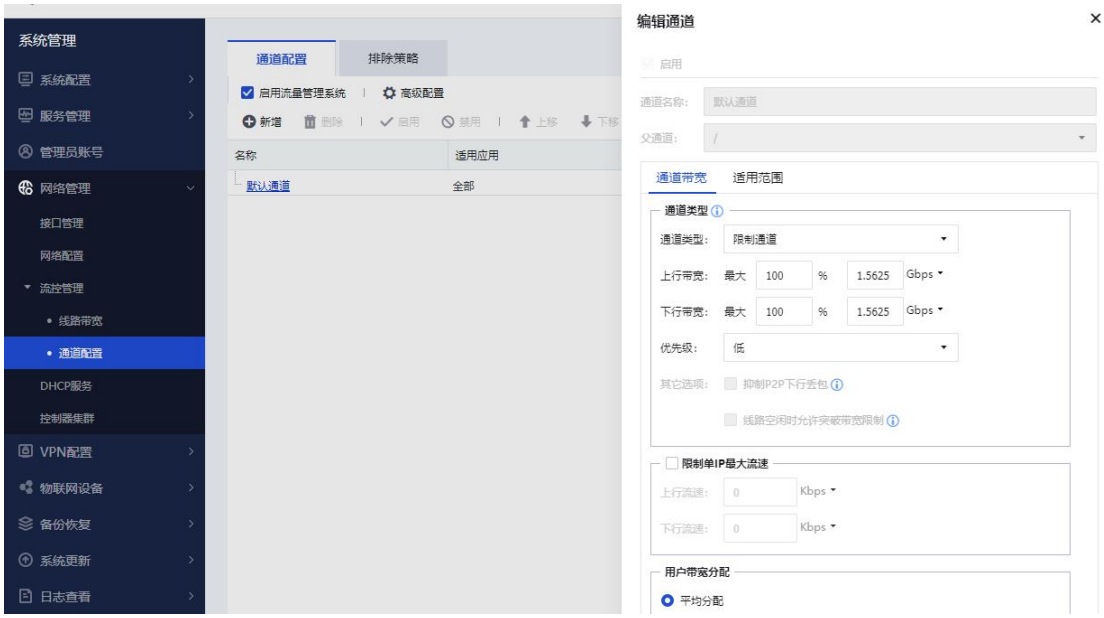
第一：如果已经配置了一条 vlanif 口，同时某个二层口在这个 vlan 内（access 的 vlanid 为该 vlanifid，或者 trunk vlan 列表中有该 vlan），那么这个二层口就不允许再配置成一条新的线路。第二：如果一个二层口和一个 vlanif 接口都配置成线路，修改这个二层接口的 vlan 属性时，不能修改为线路中 vlanif 接口的 vlan 值。 第三：配置线路时，不能选择聚合口下面的物理接口。



通道配置

➢ 通道配置

流量管理系统可以对不同用户及应用的网络流量进行管理，划分。提供了带宽保证和带宽限制功能，通过带宽保证功能可以保证重要应用的带宽，带宽限制功能可以做到根据本地用户、服务器认证用户、用户接入方式、用户角色、源 IP、位置、终端类型限制上下行总带宽、各种应用的带宽等。



流量管理系统同时提供流量子通道的功能，可以根据需求建立流量子通道，对通道流量做更为细化的分配。

通过流量管理，可以实现的主要功能有：

- 动态保证重要网络应用的带宽
- 通道内，不同 IP 间，带宽平均分配
- 限制网络应用的带宽
- 控制每 IP 的最大带宽

➢ 排除策略

流量管理系统的排除策略是指配置后，符合排除策略的流量完全不受流量管理系统的管理，直接进行转发。

而流量管理系统具备带宽保证的功能，也就是在线路上，能为特定的通道保证一定的带宽，因为这个保证带宽是动态的，因此需要实时地统计线路当前的流量情况，也就是要清楚地知道线路目前的状况，流量分布等。否则，无法达到保证带宽的效果。因此，流量管理系统需要知道以下信息：

- 线路的物理带宽
- 线路实时的流量情况

经过流量管理系统的网络数据，会进入其中一个带宽通道，通道的最大带宽最大不会超过设定的线路带宽，因此只要经过流量管理系统，转发流量的速率就不会超过线路的带宽。

在某些网络环境下，设备转发的流量并不是全部都会真正转发到线路上，对于这种情况，为了避免这部分应用的带宽受到线路的限制，避免错误地统计线路实时流量情况，进而影响流量管理的正常功能，因此需要配置排除策略。

因此，排除策略配置的应该是：经过设备转发（LAN<->WAN 方向），但并没有实际消耗线路带宽的流量。

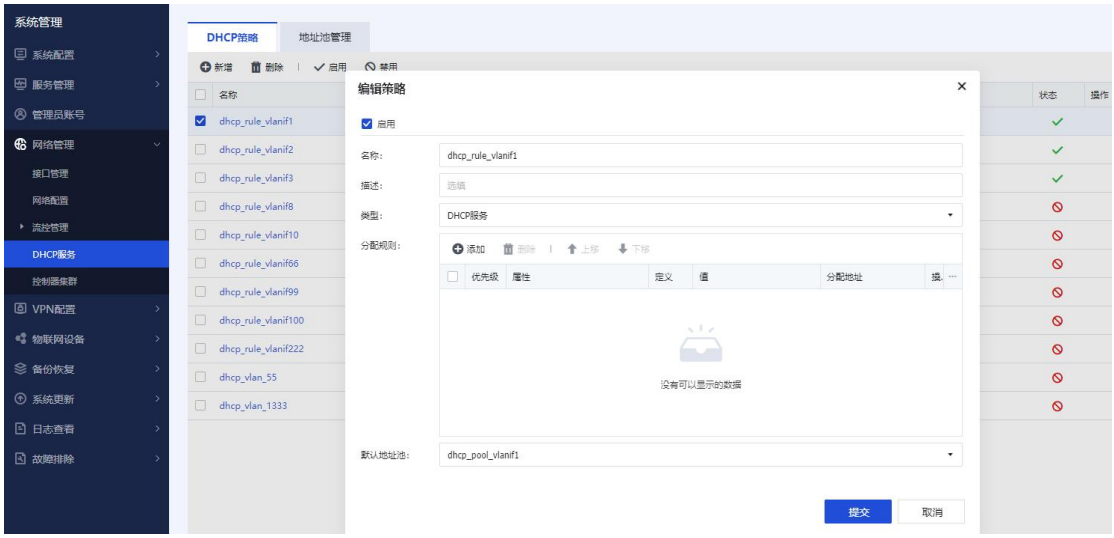
例如：

- 设备以网桥模式，部署在出口防火墙及核心交换之间，内网用户访问防火墙 DMZ 区域的服务器流量。这种环境下，需要配置排除策略（或者配置全局排除地址）。
- 内网用户通过代理服务器上网，因此经过设备的流量可能没有真正消耗公网带宽，此种情况下，需要配置排除策略。

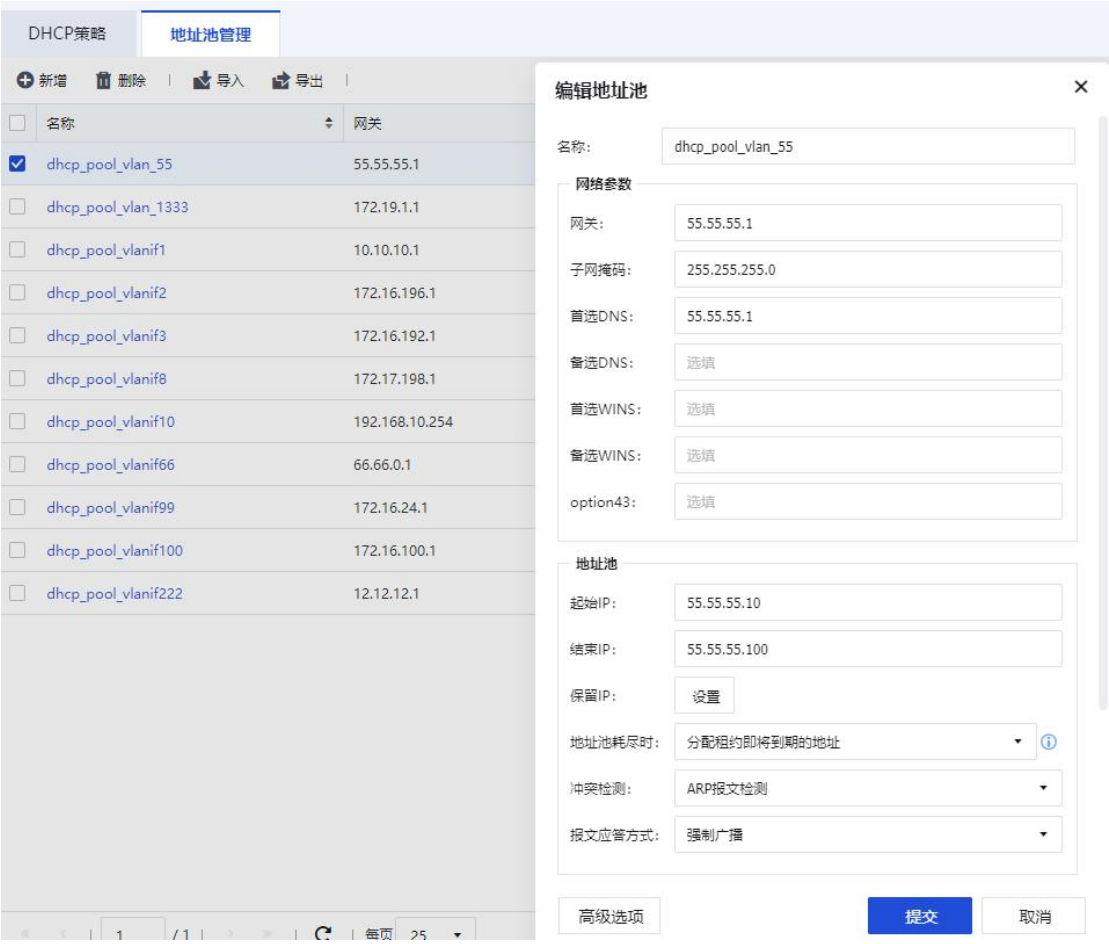
3.9.4.4. DHCP 服务

DHCP 服务可以为自动获取 IP 地址的终端分配 IP 地址，支持所有三层接口（物理口、聚合口、vlan 接口、vrrp 接口）且支持在一个接口上分配不同网段 IP。三层接口通过引用 DHCP 策略可以生效 DHCP 服务。

DHCP 策略，配置如何为终端分配 IP 地址的策略，支持根据 DHCP 终端的信息、用户属性、Option82 等为其分配不同网段的 IP，或将其 DHCP 请求转发至外部不同的 DHCP 服务器。



地址池管理，配置 DHCP 地址池，多个地址池可以被同一个策略引用。



3.9.5. 控制器集群

3.9.5.1. 接入中心端

集中管理中 NAC 控制器分三种角色：独立控制器，分支控制器，中心控制器。

独立控制器

未开启集中管理功能。

分支控制器

分支分三种状态（管理，监控，维护）。

1、管理状态：需要中心控制器和分支版本一致，由中心控制器集中配置下发无线网络等集中管理的配置。

认证方式

管理模式状态的分支，终端接入时有两种认证方式：集中认证和分布式认证。

集中认证

终端的认证在中心控制器上完成，分支控制器转发用户的数据。终端完成认证之后，用户信

息存储在中心控制器。

中心控制器和分支控制器断开时，访客认证会进入灾备模式，终端在灾备模式下完成认证，会以灾备角色在分支上线。

灾备角色在控制器集群->集中管理->分支控制器->灾备选项里面配置。

中心控制器恢复之后，在分支以灾备角色上线的用户是否下线，控制开关在接入点配置->灾备策略->灾备策略域->全局选项中配置。

分布式认证

终端认证在各自的分支控制器上进行，用户信息会存储在分支控制器上。

分布式认证的无线网络，要利用本地用户的组织结构来分配权限的时候，需要手动填写本地用户组的组名。

2、监控状态：分支自己管理配置。

3、维护状态：当中心控制器和分支版本不一致时自动切换，或由中心控制器管理员主动切换，维护状态下暂时不下发配置，分支也不可以修改集中管理的配置。

中心控制器

1. 增加、删除、编辑分支账号。
2. 批量切换分支的状态（管理，监控，维护）。
3. 导入导出分支账号。
4. 生成分支的解控密码。
5. 远程登录到分支的控制器。

- **本地配置**

集中管理一大亮点，在中心控制器统一修改管理状态的分支的配置，分支只需配置线路、区域与网口的对应关系以及少量的基础配置即可。

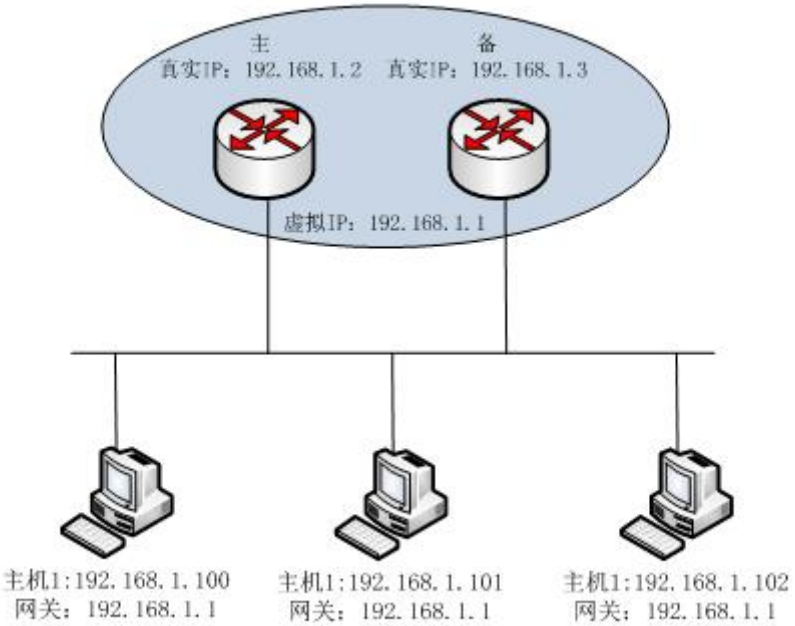
- **立即同步**

为了节约流量，某些配置（如：本地用户）默认为定时一段时间同步一次，若期望马上同步时，可以使用立即同步功能。

3.9.5.2. VRRP 组

VRRP（Virtual Router Redundancy Protocol）协议，提供了虚拟 IP 的机制来解决网关 IP 在多个路由器间迁移的问题。在 3 层部署的环境中，无线客户端的默认网关指向 NAC 的 VLAN 接口地址，因此在双机部署中，当某台设备故障时，VLAN 接口的 IP 地址需要使用 VRRP 协议迁移到备份设备上，从而保证无线用户仍然能够正常访问网络。

VRRP 的虚拟 IP 迁移通过备份组机制实现，基本原理如下：

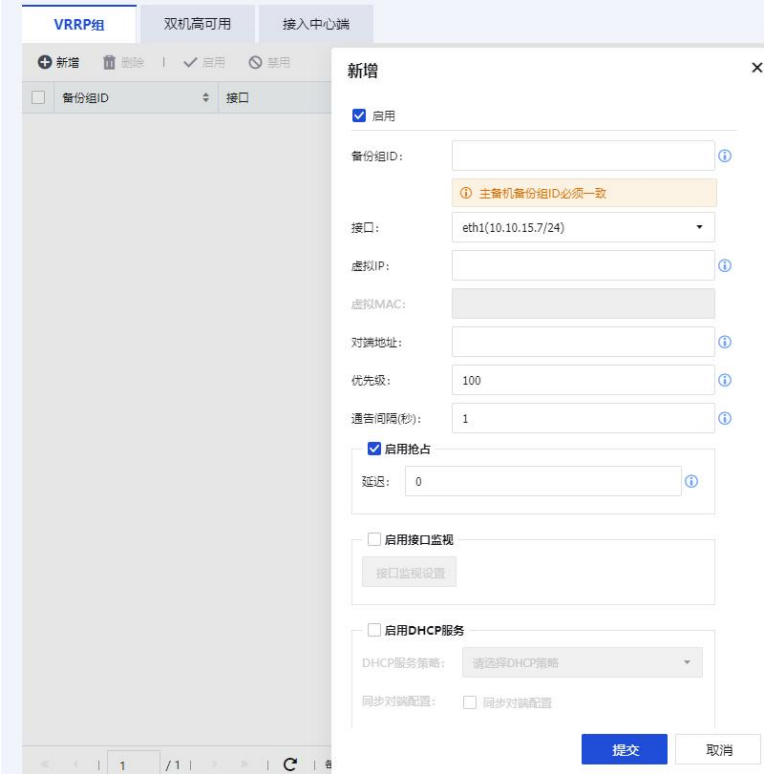


把两个路由器划分为一个 VRRP 备份组，备份组设置一个虚拟 IP。

备份组内的路由器，使用基于优先级的选举机制，优先级较高的为 Master 路由器，其余为 Backup 路由器。

只有 Master 路由器，才真正持有备份组的虚拟 IP，也就是对于其它主机询问此虚拟 IP 的 ARP 请求，PING 请求等，只有 Master 路由器会回应。

Master 路由器定期发送 VRRP 通告报文，通知备份组内的其他路由器自己工作正常。Backup 路由器则监听通告报文的到来，如果在一定时间内没有收到 Master 路由器的通告报文，则优先级最高的 Backup 路由器将转化为 Master 路由器。



3.9.5.3. 双机高可用

1、通信网口

双机热备情况下，两台 NAC 之间，需要同步内部状态信息，例如心跳信号，在线用户信息，漫游信息，无线射频调整决策信息等。因此在控制器上，通常需要分别使用一个专用的网口来完成双机状态同步。此选项选择用于状态同步的物理接口。

2、对端地址

对端控制器的 IP 地址，系统使用所选择的物理接口及对端地址来完成双机状态同步。因此对端地址是指双机心跳线所连接的对端接口 IP 地址。

3、管理 VRRP

选择一个 VRRP 备份组作为管理 VRRP 组，在此备份组中，Master 状态的设备将作为“主管理设备”。只有登录到“主管理设备”，才允许修改系统配置。

4、主备配置

主机选择允许编辑配置，备机选择同步对端配置，双机热备才会搭建成功。

3.9.6. VPN 配置

NAC 集成了 SangforVPN，标准 IpsecVPN，接入点 VPN 三种 VPN。

『VPN 配置』包含了【DLAN 运行状态】、【基本配置】、【用户管理】、【连接管理】、【第三方对接】、【接入点 VPN】、【高级设置】。

3.9.6.1. DLAN 运行状态

此页面可以查看当前的 VPN 连接和网络流量信息。页面如下

点击开启可开启 VPN 服务。

点击停止可暂时停止 VPN 服务。

点击刷新，则显示实时的 vpn 连接信息以及流量信息。

在【输入用户名】输入框中输入用户名，可以快速找到当前用户的连接情况。可以进行模糊搜索。

注意：需要开启 VPN 服务，VPN 配置才会生效。

3.9.6.2. 基本设置

【基本设置】用于配置 Sangfor VPN 的服务端。页面如下

主、备 WebAgent：指动态 IP 寻址文件在 WEB 服务器中的地址，包括主 WebAgent 和备份 WebAgent 地址。

如果是“动态寻址（总部非固定 IP）”请填写“WebAgnet 网页地址”（一般为.php 结尾的网页地址），填写完 Webagent 后可以点击测试按钮查看是否能够连通，如果总部是“固定 IP”，请按照“IP 地址:端口”的格式填写，如 202.96.134.133:4009。点击修改密码可以设置 Webagent 密码，以防止非法用户盗用 Webagent 更新虚假 IP 地址，只对网页地址有效。点击加密密钥可以设置共享密钥，防止非法设备接入。

注意：如果设置了【WebAgent 密码】，一旦遗失该密码则无法恢复，只能联系深信服科技客户服务中心重新生成一个不包含 Webagent 密码的文件并替换原有文件。如果设置了【共享密钥】，则所有 VPN 网点都必须设置相同的【共享密钥】才能相互连接通信。如果是多线路且都是固定 IP 的情况下，可以采用“IP1#IP2:port”的方式来填写

Webagent。

- MTU 值：用于设置 VPN 数据的最大 MTU 值，默认为 1500。
- 最小压缩值：用于设置对 VPN 数据启用压缩的最小数据包大小，默认为 99。
- VPN 监听端口：用于设置 VPN 服务的监听端口，缺省为 4009，可根据需要设置。
- 修改 MSS：用于设置 UDP 传输模式下 VPN 数据的最大分片。

注意：MTU 值、最小压缩值、修改 MSS 一般情况下请保留默认值，如需设置，请在深信服技术支持工程师的指导下修改。

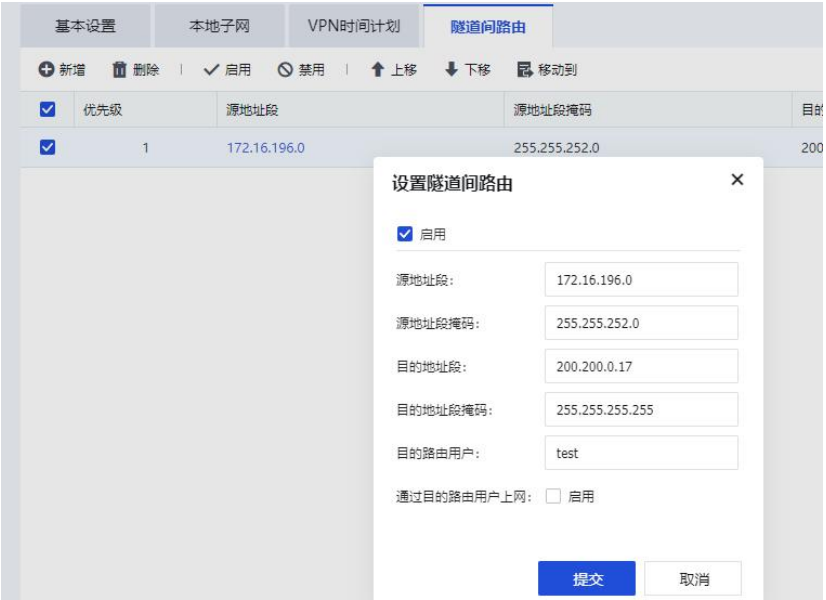
直连、非直连：用于设置网关与 Internet 的连接方式，如果能直接获得 Internet IP 或者能通过端口映射等方式让 Internet 用户可以访问到网关设备的 VPN 端口，则可设置为“直连”，不能获得 Internet IP 的连接方式则需设置为“非直连”。

点击高级设置可以进行 VPN 性能设置，线程数设置，如下图所示：

本地子网：配置走 Sangfor VPN 的网段，此网段会同步给其他建立 sangfor VPN 连接的设备。

VPN 时间计划：配置 VPN 独立的时间计划。

隧道间路由：通过配置源网络号和源子网掩码，以及目的网络号和目的子网掩码以及建立 VPN 连接的目的路由用户，实现隧道间路由的目的。



为实现隧道间路由，需完成以下两个步骤：

1、在 VPN 客户端的基本设置->本地子网处，创建本地子网的相关配置（子网网段与子网掩码）；

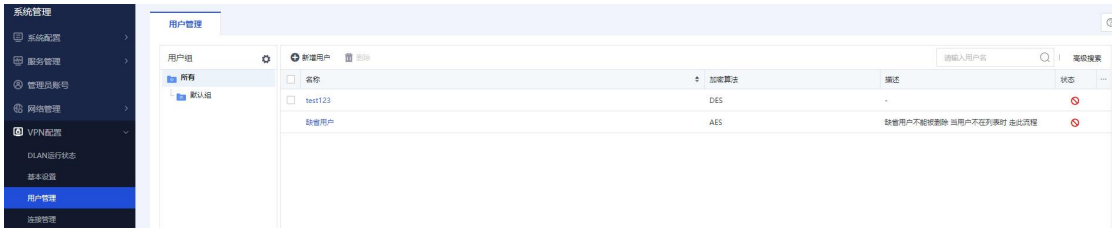
2、在 VPN 客户端的基本设置->隧道间路由处，新增隧道间路由配置。源网络号与子网掩码与本地子网配置一致。目的网络号和目的子网掩码的配置则随着用户的需要有所不同：

（1）设置成 VPN 服务端的本地子网配置，则允许访问 VPN 服务端内网资源；

（2）勾选“启用”通过目的路由用户上网，则目的网络号和目的子网掩码都自动填充为 0.0.0.0 和 0.0.0.0 代表所有流量均通过隧道间路由进行访问。

3.9.6.3. 用户管理

【用户管理】用于管理 VPN 接入账号信息，设置允许接入 VPN 的用户名、初始密码，设置账号使用的加密算法、账号有效时间。页面如下：



【新增用户】：可依次设置接入账号的用户名、初始密码、确认密码、算法、描述、等信息，如下图：

使用组属性：用于对用户进行分组，如勾选使用组属性，则可激活选择用户组设置，选择将该用户加入到某一个用户组并应用这个组的公共属性。

设置【使用组属性】前请先新增用户组。用户加入用户组后，该用户的加密算法、权限设置、高级将无法再单独设置。

有效时间和启用过期时间：用于设置“接入账号”的有效时间及过期时间。

启用压缩：用于设置对网关设备与该用户之间传输的数据使用压缩算法进行压缩。

该设置是 SANGFOR VPN 的独特技术，在低带宽的环境下能有效利用有限带宽，加速数据传输，但并不适用于所有网络环境，实际应用中可根据情况进行设置。

启用多用户登录：用于设置是否允许多个用户同时共用该账号登录 VPN。

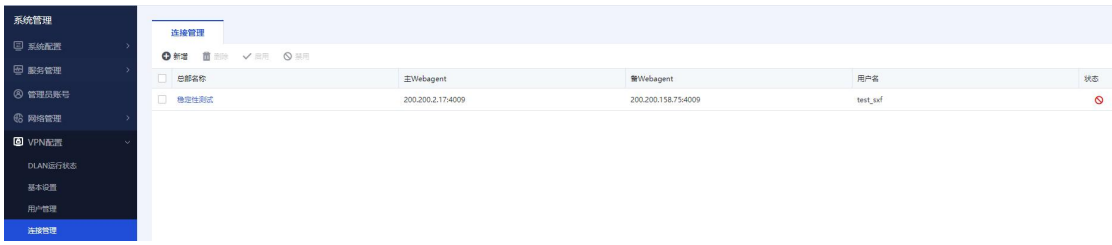
点击高级页面，可以设置【VPN 隧道超时时间】，页面如下

点击删除 确认删除可对勾选的用户进行删除操作。页面如下

3.9.6.4. 连接管理

为了实现多个网络节点的互联（组成“网状”网络），VPN 硬件网关提供了对网络节点互联的自主管理和设置功能。可在【连接管理】中进行相关的设置。页面如下：

注意：连接管理只有此设备当分支使用需要连接其他 Sangfor VPN 设备时才需要启用，否则本端是 VPN 总部设备的不需要启用连接管理。



新增：可以添加到一个到其他 VPN 总部的连接。页面如下：

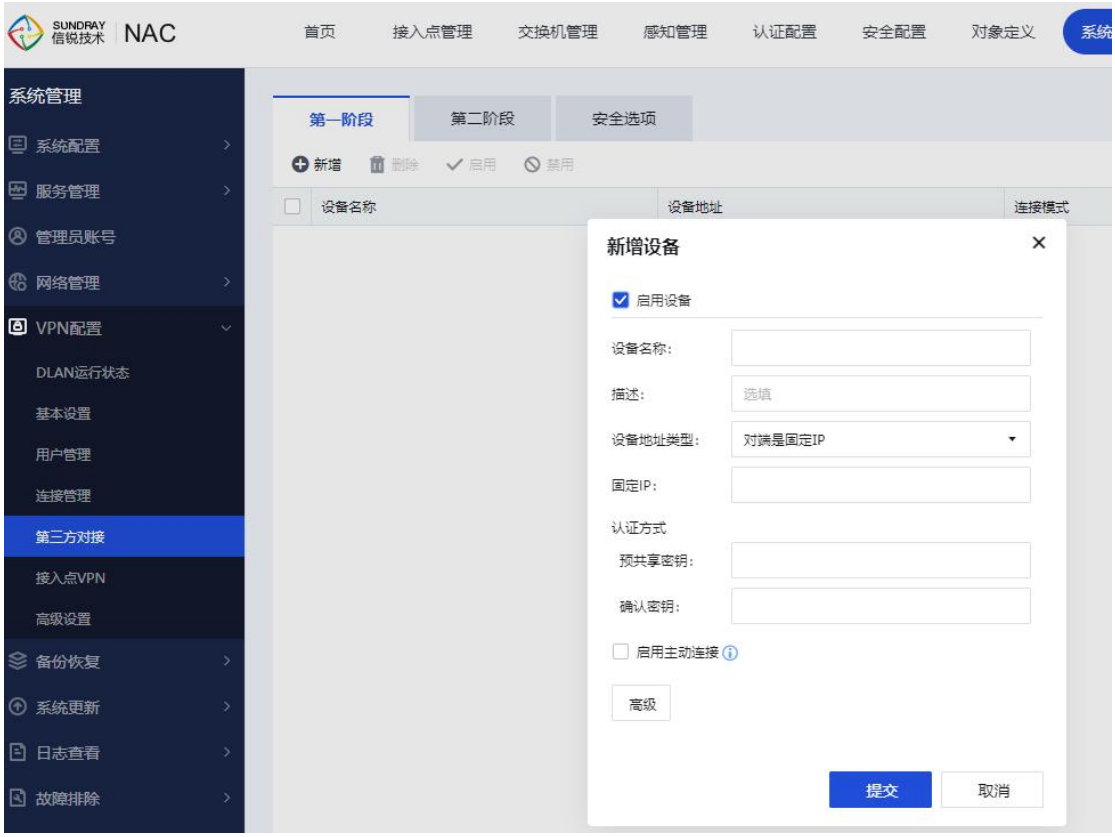
- 总部名称：用于标记连接名称，可以任意填写。
- 描述：可自行定义描述信息。
- 主/备份 Webagent：用于填写需要连接的总部的对应 Webagent，点测试按钮可以测试 Webagent 是否工作正常。
- 传输类型：可选“TCP”或“UDP”，用于决定传输 VPN 数据包的类型，默认为 UDP 模式。
- 用户名和密码：请根据总部提供的接入账号信息来填写。
- 跨运营商：适用于总部分支采用了不同运营商线路互联且经常丢包的情况下。可以选择“低丢包率”、“高丢包率”和“手动设置”。

注意：跨运营商功能需要额外激活，否则该功能无效。只要总部激活跨运营商功能，则所有连接到该总部的移动用户均可启用跨运营商功能。如果是设备和设备之间互连，则需要双方都开启跨运营商序列号，否则该功能无效。

3.9.6.5. 第三方对接

SUNDRAY IPSEC VPN 系列硬件设备提供了与第三方 IPSEC VPN 设备互联的功能，能与第三方的 IPSEC VPN 设备建立标准 IPSec VPN 连接。

【第一阶段】用于设置需要与 SUNDRAY IPSEC VPN 硬件网关建立标准 IPSec 连接的对端 IPSEC VPN 设备的相关信息，也就是标准 IPSec 协议协商的第一阶段。页面如下：



- 设备名称：可自行定义。

- 描述：可自行定义。
- 设备地址类型：包括对端是固定 IP、对端是动态 IP、对端是固定域名三种。请根据实际情况选择。选择固定 IP，就填写上对端的 IP 地址；选择动态域名，就填写上对端外网绑定的域名。

注意：标准 IPSEC 不允许连接的双方都是动态 IP，只能允许其中一方为动态 IP。

预共享密钥及确认密钥：填入正确的预共享密钥，并确保连接双方采用的都是相同的预共享密钥。

点击高级，显示【高级选项】对话框，可进行其它高级设置，如下图：

ISAKMP 存活时间：标准 IPSEC 协商的第一阶段存活时间，只支持按秒计时方式。

重试次数：当 VPN 故障断开后，重试连接的次数，超过次数还未能连上，则不再主动发起连接，除非有 VPN 流量触发才能再次主动发起连接。

协商模式：包括主模式和野蛮模式两种类型。主模式适用于双方均为固定 IP 或者一方固定 IP 一方动态域名方式，并且不支持 NAT 穿透；野蛮模式适用于其中一方为拨号的情

况，并且支持 NAT 穿透。

DH 群：设置 Diffie-Hellman 密钥交换的群类型，包括 1、2、5 三种，请与对端设备配置保持一致。

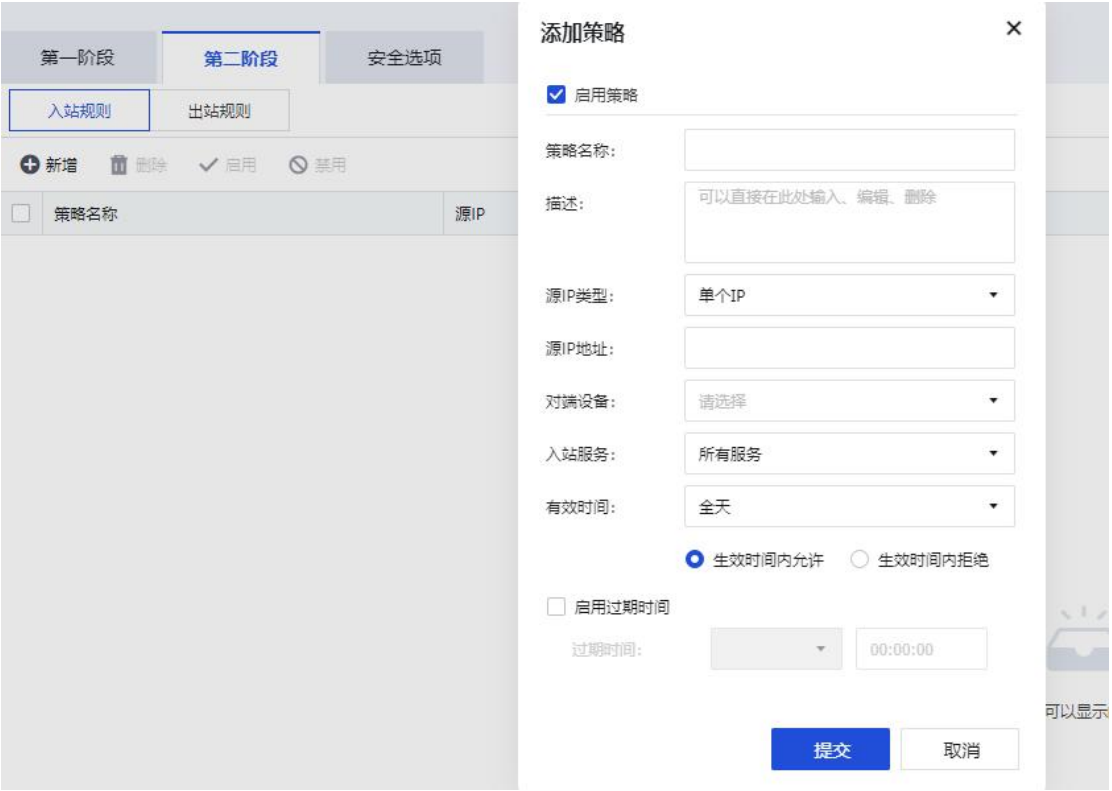
认证算法：选择数据认证的 Hash 算法，包括 MD5。

加密算法：选择数据加密的算法，包括 DES、3DES、AES。

野蛮模式的身份 ID 有 3 种表达方式，一种为 IP 地址；一种为域名字符串（FQDN）格式，可以为任意的网址或者一串字符串；另一种为用户字符串（USER_FQDN），需要是“xxx@xxx.xxx”这种格式。

第二阶段：

【入站策略】用于设置由对端发到本端的数据包规则，策略较多时自动分页显示。可以在右上角搜索策略名称、源 IP、对端设备名称等；其中对于源 IP 是“子网+掩码”的策略，仅搜索的是子网，不搜索掩码。



- 策略名称及描述：可自行定义。
- 源 IP 类型：包括单个 IP、子网+掩码两种类型。分别指定对端 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入对端 VPN 数据的源地址。
- 对端设备：该出站策略跟对端哪个设备相关联。
- 入站服务：定义对端哪些类型的服务允许进入 VPN 隧道传输至本端内网。
- 有效时间及过期时间：在什么时间范围内，该入站策略有效。其中有【效时间】可选【生效时间内允许】，【生效时间内拒绝】。

出站策略：用于设置从本端发往对端的数据包规则，点击新增，显示【策略设置】对话框，页面如下：

- 策略名称及描述：可自行定义。
- 源 IP 类型：包括单个 IP、子网+掩码两种类型。分别指定 VPN 数据的源 IP 是单个 IP 还是整个网段，并正确填入 VPN 数据的源地址。
- 对端设备：该出站策略跟对端哪个设备相关联。
- 安全选项：该出站策略跟哪个安全选项相关联。
- SA 生存时间：标准 IPSEC 第二阶段协商的存活时间，同样只支持按秒计时。
- 出站服务：定义哪些类型的服务允许进入 VPN 隧道传输至对端内网。
- 有效时间及过期时间：在什么时间范围内，该出站策略有效。其中有【效时间】可选【生效时间内允许】，【生效时间内拒绝】。

注意：【有效时间】模块，只在连接双方都是 SUNDRAY 设备情况下生效，与其他厂商设备互联时无效。

启用密钥完美向前保护：根据对端设备情况而定，如果对端启用了 PFS，则本端也需要勾上此选项，否则不用勾选。

注意：【出站规则】和【入站规则】中的【出站服务】、【入站服务】和【有效时间】均为 SUNDRAY 扩展的规则，此类规则仅在本端设备生效，在与第三方设备建立 VPN 连接的过程中不会协商此类规则。【出站策略】和【入站策略】中策略所对应的源 IP 地址是指【源 IP 类型】和【本/对端服务】中所设置的源 IP 的交集。

【安全选项】用于与对端建立标准 IPSec 连接时所使用的参数，页面如下：

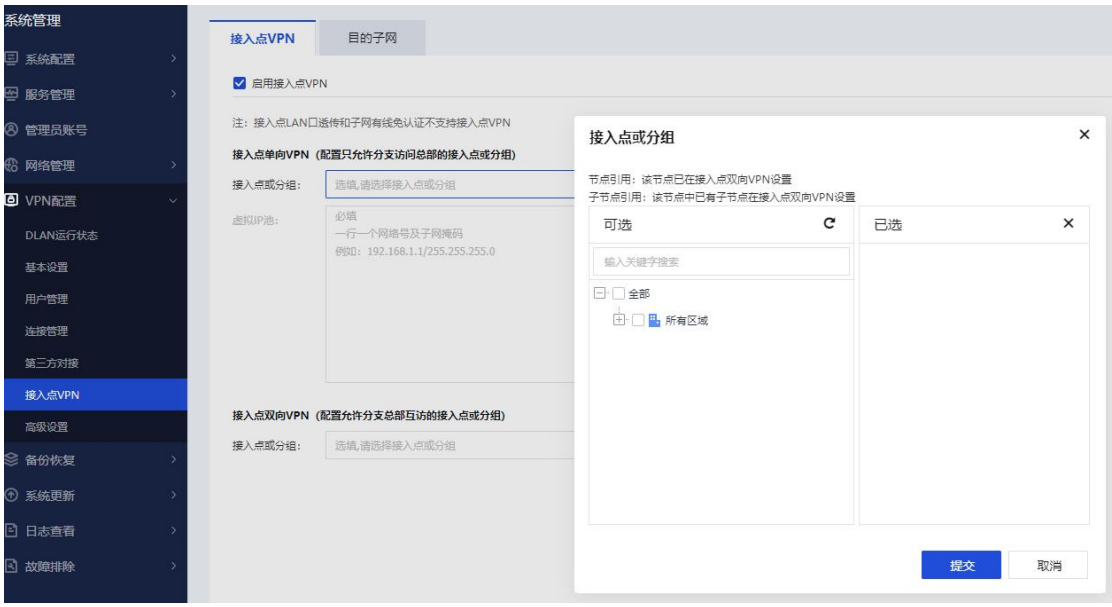
在建立与第三方设备的 IPSec 连接前，请先确定对端设备采用何种连接策略，包括：使用的【协议】（AH 或 ESP）、【认证算法】（MD5 或 SHA-1）、【加密算法】（DES、3DES、AES）。点击新增，添加新的选项，页面如下：

SUNSRAY IPSEC VPN 系列硬件设备会使用设置好的连接策略与对端协商建立 IPSec 连接。

【安全选项】中的【加密算法】用于设置标准 IPSec 连接的第二阶段所使用的数据加密算法，如果要与多个采用不同连接策略的设备互联，需要分别将各个设备使用的连接策略添加到【安全选项】中。

3.9.6.6. 接入点 VPN

接入点 VPN 主要用于远程部署场景，分部要通过分部的 VPN 访问总部资源、或者总部分部互访。由 AP 和控制器之间建立 VPN 隧道，传输总分部之间的流量。



虚拟 IP 池：由接入点 VPN 系列硬件设备指定设备内网中空闲的一段 IP 作为移动用户接入时的虚拟 IP。当移动用户接入后，分配一个虚拟 IP 给移动用户，移动用户对总部的任何操作都是以分配的 IP 作为源 IP、就完全和在总部局域网内一样。例如使用虚拟 IP 的移动接入后，无论总部局域网的计算机是否把网关指向总部接入点 VPN 系列硬件设备，移动用户均可以访问，还可以为接入的移动用户指定 DNS 等网络属性。

创建移动虚拟 IP 池。虚拟 IP 池中的 IP 相当于是直连在总部控制器网关设备的网段。

在【虚拟 IP 池】对话框，设置“IP 池”的起止 IP 即可。页面如下：

分支网络部分走本地转发，部分走集中转发。

满足分支远程 AP 本地转发下的用户即想访问公网，又想访问总部资源的需求。

分两种场景：

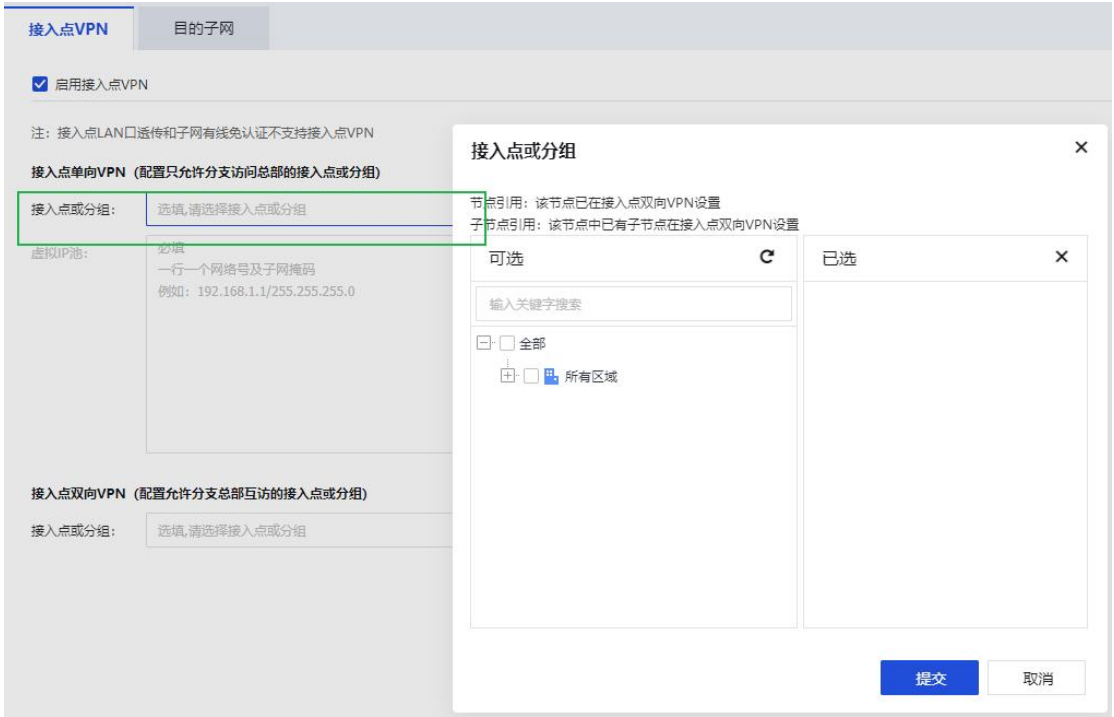
场景 1：只允许分支访问总部。

配置方法：在虚拟 IP 池中设置足够多的虚拟 IP。将总部资源的 IP 填写到目的子网中，即可。

场景 2：允许分支总部互访。

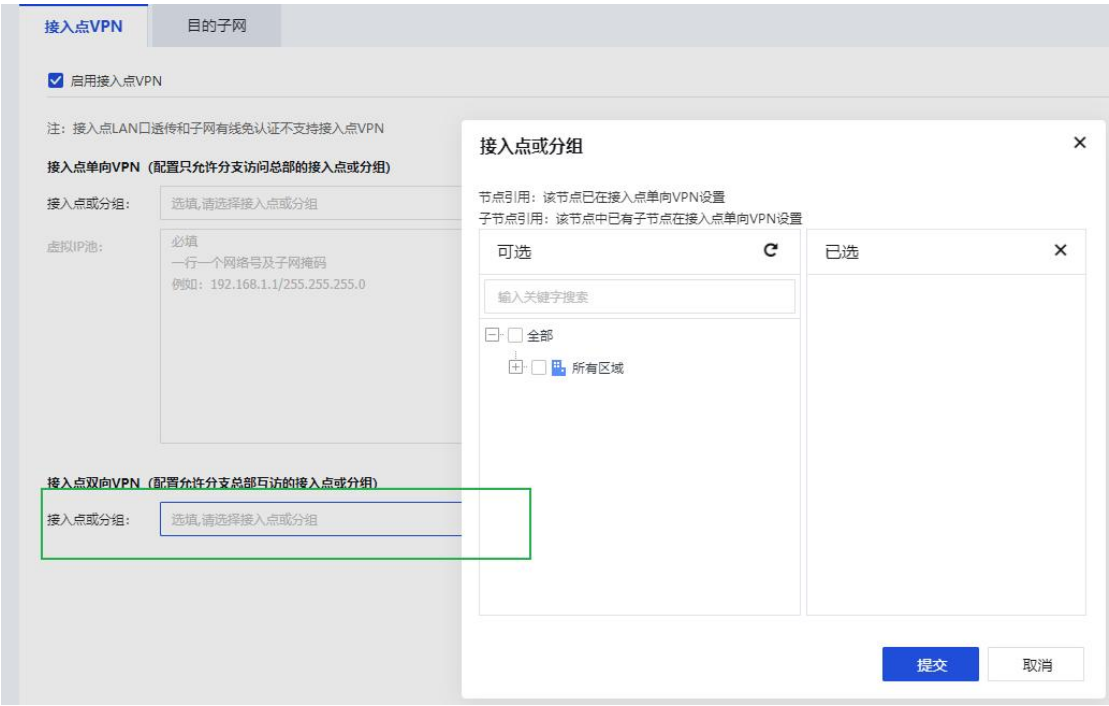
配置方法：需要划分每个 AP 的子网网段，保证子网网段不冲突。将总部资源的 IP 填写到目的子网中。

接入点单向 VPN，只允许分支访问总部：

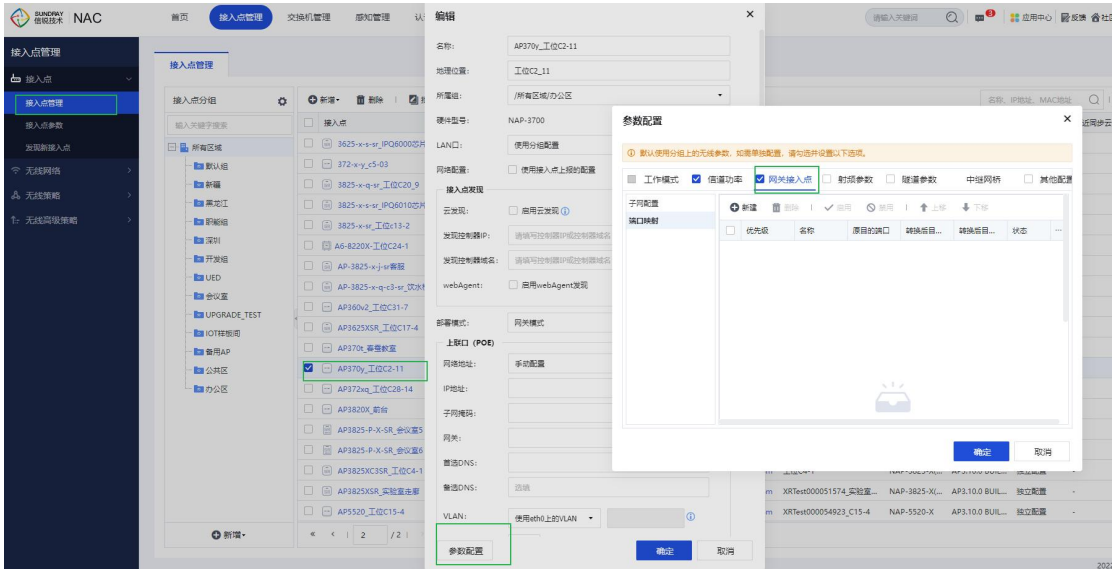


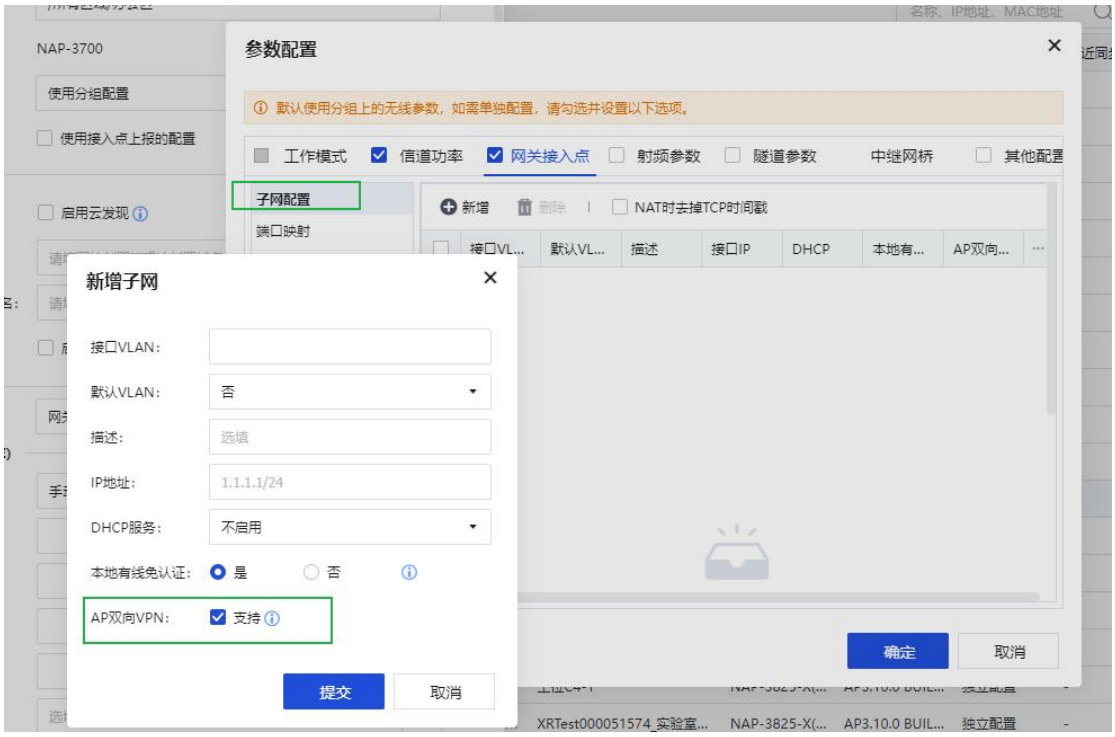
接入点双向 VPN：允许总分部互访。

在接入点双向 VPN（配置允许分支总部互访的接入点或分组）选项下，接入点或分组里选择需要双向互访的 AP 或者 AP 组。



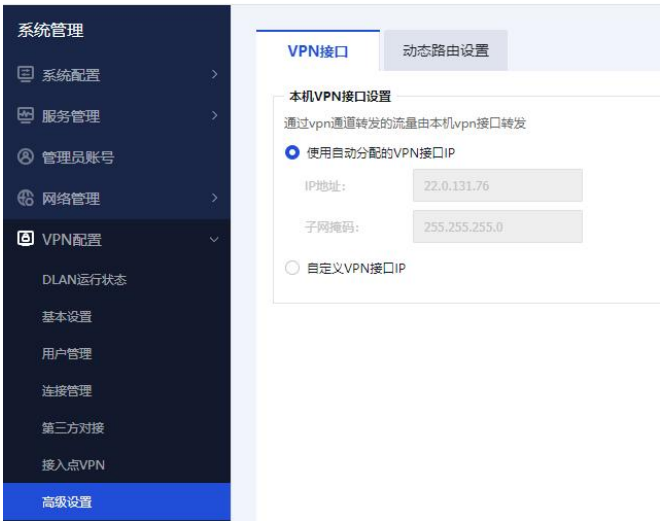
在 AP 端，需要开启【AP 双向 VPN】的支持，具体在【接入点管理】，点开对应的接入点，AP 选择网关模式，点参数配置，选中【网关接入点】，点添加，勾选【双向 VPN 支持】。





【目的子网】配置分支走集中转发的网段。配置远程 AP 下的用户访问哪些 IP 时走集中转发。

3.9.6.7. 高级设置



VPN 接口：

支持自动分配和手动配置，可在此接口上做地址转换。

动态路由设置：

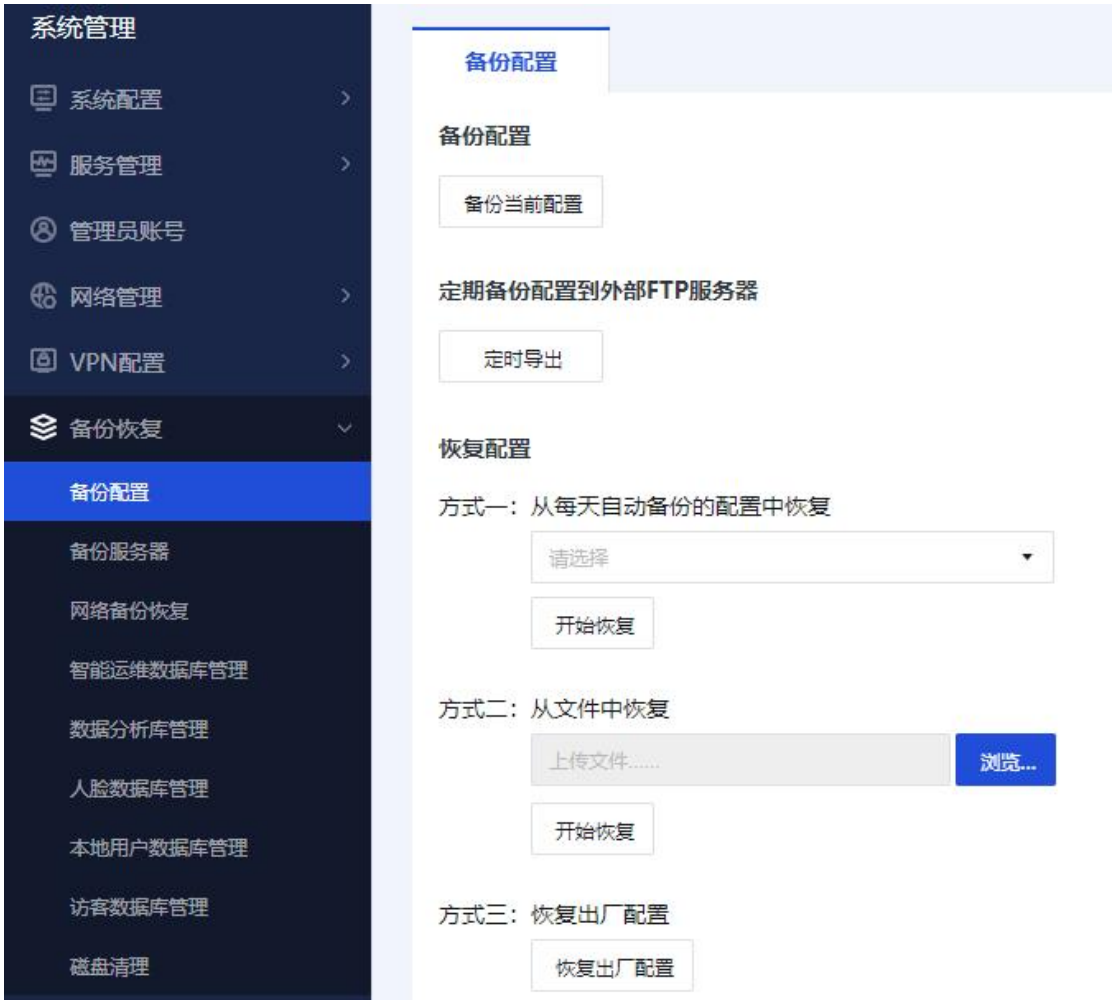
动态将 VPN 的路由表通告给接在控制器内网的路由器。

允许通告接入点 VPN 的 IP 地址：将 AP VPN 目的子网路由下发给内网路由器。

3.9.7. 备份恢复

3.9.7.1. 备份配置

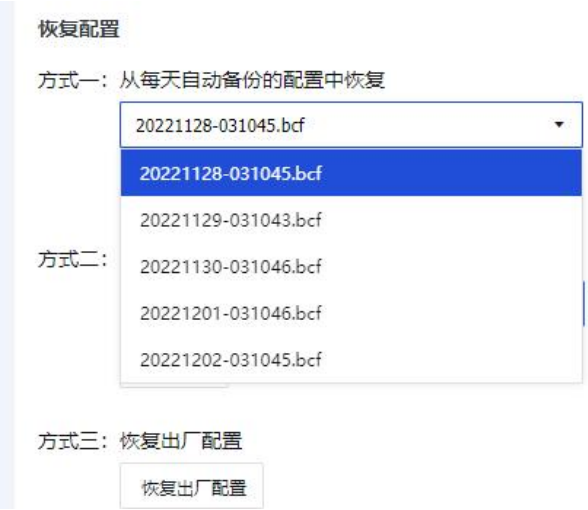
点击备份配置时，可以从 NAC 上下载当前系统配置，并可以保存到在 PC 上，用户可以自行保存。也可以采用方式二：从文件中恢复的方法还原下载的配置，点击备份配置时，可以下载的配置文件如下，是 bcf 格式的文件。



还可以采用备份自动备份到 FTP 服务器的方法备份

恢复配置

方式一：从每天自动备份的配置中恢复，默认系统会自动备份最近一周的配置



方式二：从之前备份的配置进行恢复

方式三：直接点击“恢复出厂配置”。

3.9.7.2. 备份服务器

配置还可以采用备份自动备份到 FTP 服务器的方法备份。备份服务器用于备份系统配置和人流量分析的数据。

3.9.7.3. 网络备份恢复

系统中保存了大量网络配置信息，因此定期对设备网络配置执行备份操作是一个良好的管理习惯。

在以下情况下，可以考虑从最近备份的数据中恢复网络配置，以尽快恢复您的网络，并减少损失：

1、设备损坏或丢失，需要更换全新的硬件设备

2、设备误配置，例如误删除了大量的网络配置

3、分支设备性能不够，需要升级新设备

网络备份恢复，只有一种形式：手动备份

管理员从控制台网络备份恢复页面中，下载当前的网络配置备份文件，并保存在管理员的本地计算机中。手动备份的网络配置备份文件由于保存在设备之外，将具备更高的可靠性，即使设备损坏或丢失，分支替换新设备，购买新的设备后，仍然可以从备份文件中恢复，因此建议定期执行手动备份操作。

3.9.7.4. 智能运维数据库管理

智能运维数据库管理

清空数据：清空智能网络拓扑图 中离线交换机数据、自定义成员设备地址以及所有设备的位置信息，重新生成拓扑。

网络质量感知数据

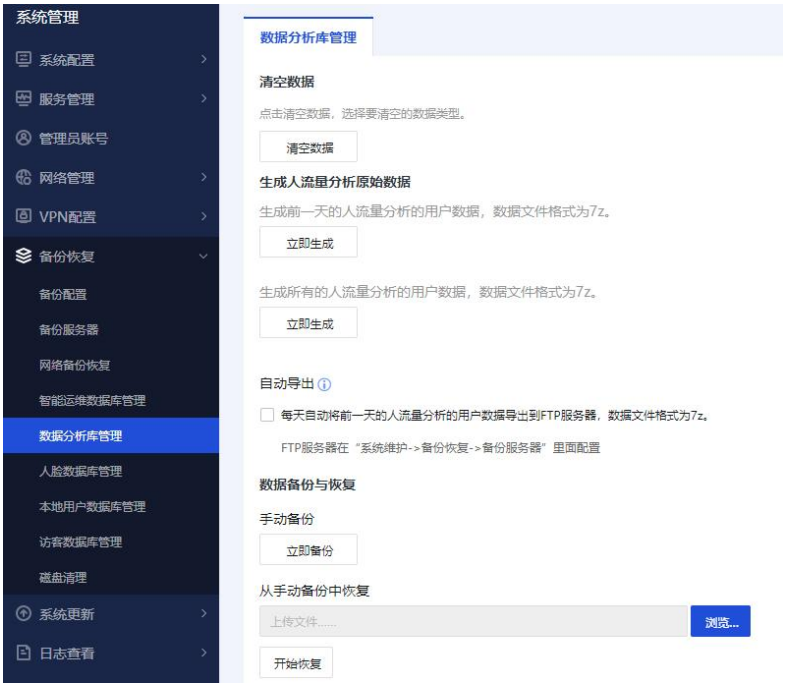
清空数据：清除首页->网络->网络质量感知 页面数据。

业务画像数据库管理

清空数据：清除首页->终端->终端网络质量、首页->设备->各设备状态 页面数据。

3.9.7.5. 数据分析管理

- 清空数据：点击该选系，就会清空客流分析和热点地图的客流数据，还会清空推广统计的数据。注：清空后无法恢复。
- 生成客流原始数据：可以生成前一天的客流分析用户数据，也可以生成所有的客流分析的用户数据。
- 自动导出：如果配置了 FTP 服务器，可以每天自动将前一天的客流分析的用户数据导出到 FTP 服务器上。
- 数据备份与恢复：手工备份客流分析和推广统计数据。
- 手动备份:手动备份客流与推广数据，导出备份数据文件。注：可能需要较长时间，请耐心等待。
- 从手动备份恢复：使用手动备份的数据进行数据恢复。

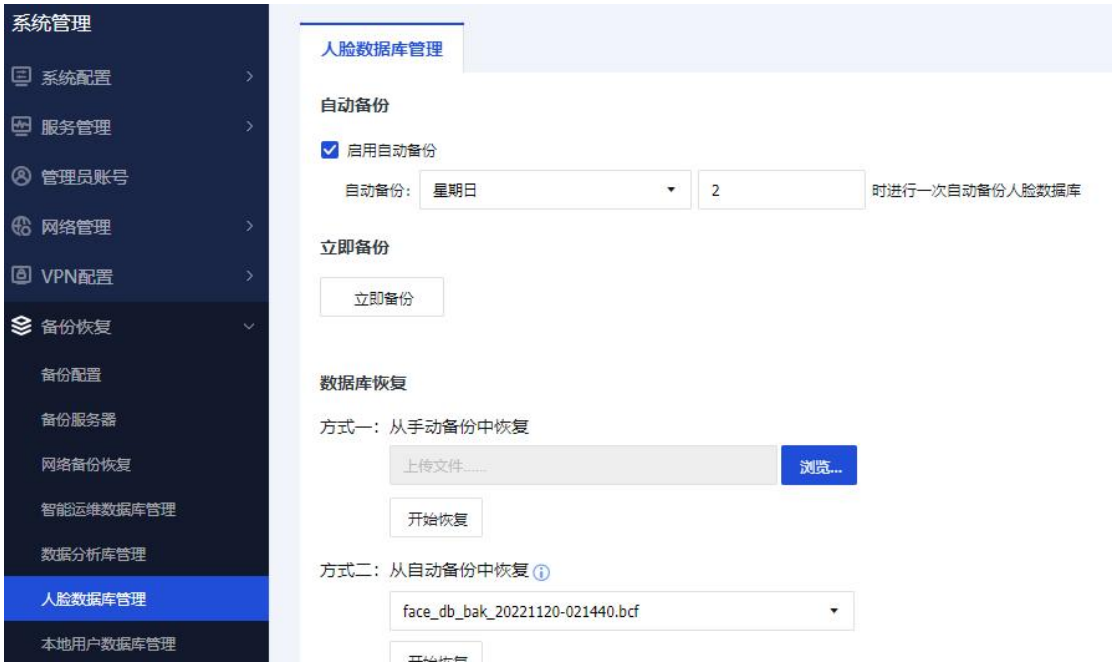


3.9.7.6. 人脸数据库管理

提供两种方式恢复数据库：

1、使用立即备份导出的数据库进行数据库恢复。

2、使用每周自动备份的数据库进行数据库恢复。



自动备份

指定每周何时进行人脸数据备份。建议设置为设备空闲时间。

立即备份

立即将当前的人脸数据库导出，用于数据库恢复。用户量较多时，导出时间可能也会相应较长，也可能占用设备较多资源，建议在空闲时段进行操作。

3.9.7.7. 本地用户数据库管理

系统中保存了大量用户账号信息，因此定期对设备本地用户数据执行备份操作是一个良好的管理习惯。

在以下情况下，可以考虑从最近备份的数据中恢复系统，以尽快恢复您的数据，并减少损失：

1. 设备损坏或丢失，需要更换全新的硬件设备
2. 设备误配置，例如误删除了大量的用户账号信息

本地用户数据库备份，有以下几种形式：

- 自动备份

系统每天会自动执行一次本地用户数据库备份操作，并保存在设备内置磁盘中，只保留 3 天的备份文件。

- 手动备份

管理员从控制台本地用户数据库管理页面中，下载当前的本地用户数据库备份文件，并保存在管理员的本地计算机中。手动备份的本地用户数据库备份文件由于保存在设备之外，将具备更高的可靠性，即使设备损坏或丢失，购买新的设备后，仍然可以从备份文件中恢复，因此建议定期执行手动备份操作。

- 定期备份本地用户数据库到外部 FTP 服务器

系统每天凌晨 03:10 开始，会自动将设备的本地用户数据库上传到外部 ftp 服务器。可以避免因本设备故障而导致本地用户数据丢失的问题。

3.9.7.8. 访客数据库管理

自动清理

提供选项，当访客数据库达到上限时，可以删除超过多少天未接入 Wi-Fi 的短信和微信访客。

立即备份

立即将当前的访客数据库导出，用于数据库恢复。

提供三种方式恢复数据库

1、使用立即备份导出的数据库进行数据库恢复。

2、使用每日 2 点-3 点自动备份的数据库进行数据库恢复。

3、将数据库恢复至被全量同步覆盖之前的还原点，只用于搭建过双机的设备。

3.9.7.9. 磁盘清理

磁盘清理

系统中长时间运行，会产生较多无用数据，比如：网监临时数据，以及过期的运维、安全数据等，需要及时清理删除，为保证系统保持最佳状态稳定运行，建议保持开启状态。

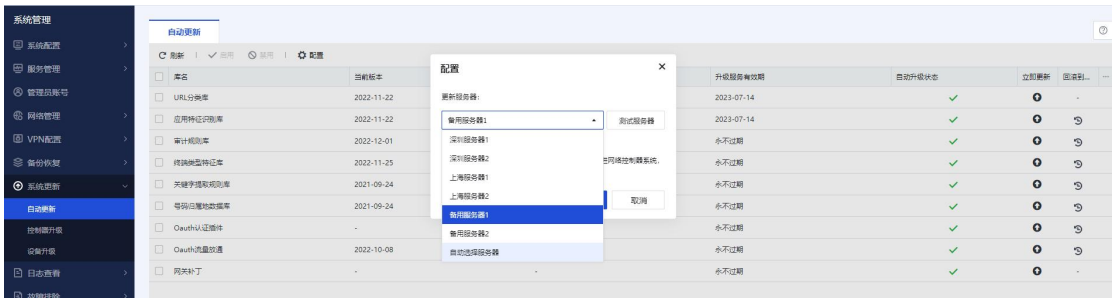
磁盘利用率阈值

开启磁盘清理时，当磁盘利用率超过配置的阀值，自动清理无用、过期数据，如清理过后仍然超过阀值，则在系统日志中进行告警。

3.9.8. 系统更新

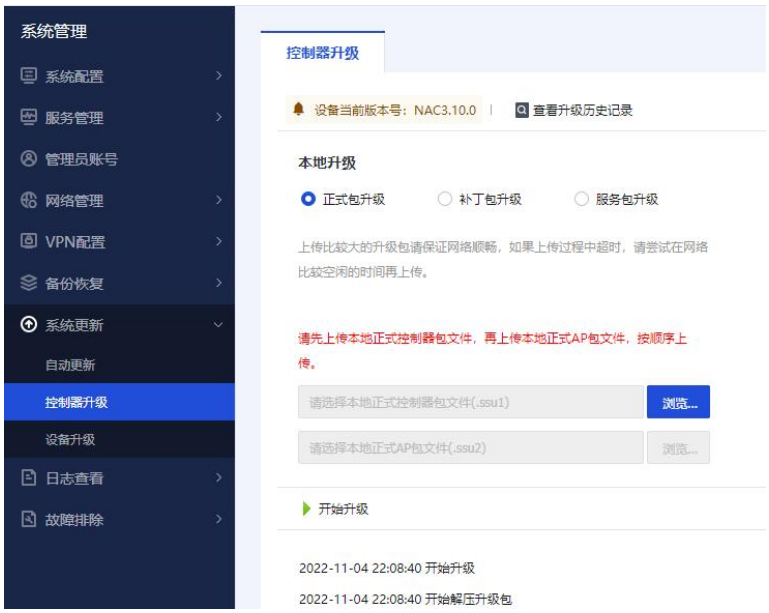
3.9.8.1. 自动更新

启用自动更新：NAC 可以自动更新系统补丁，实现 NAC 功能的优化。更新服务器可以选择“自动更新服务器”，也可以手动选择“深圳服务器”、“上海服务器”或“备用”服务器。



当勾选“加入用户体验改善计划”时，表示允许发送系统质量报告给信锐技术，帮助我们改进 NAC 系统，该报告不会涉及您组织的任何信息。

3.9.8.2. 控制器升级

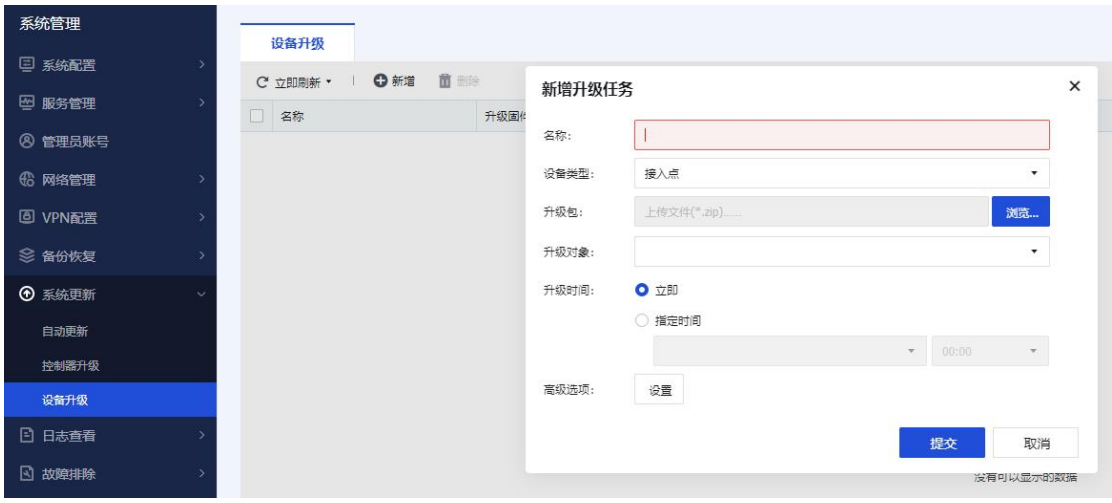


设备升级包括正式包升级与补丁包升级，设备升级功能可以替代原有信锐系列升级客户端给设备升级的方法，并且可以支持升级补丁包与补丁包回滚操作。

提示：为了保障升级顺畅、稳定，建议正式包升级时，采用专业的客户端升级，详细方法参考第五章 5.1。

3.9.8.3. 设备升级

接入点/交换机为零配置设备，通常并不需要关心设备的软件版本。接入点或交换机连接到 NAC 后，会自动从 NAC 中下载并安装系统。如果要升级到最新版本，只需要升级 NAC，不需要单独升级无线接入点或交换机。该页面的升级功能，主要提供给设备供应商的技术支持人员使用。



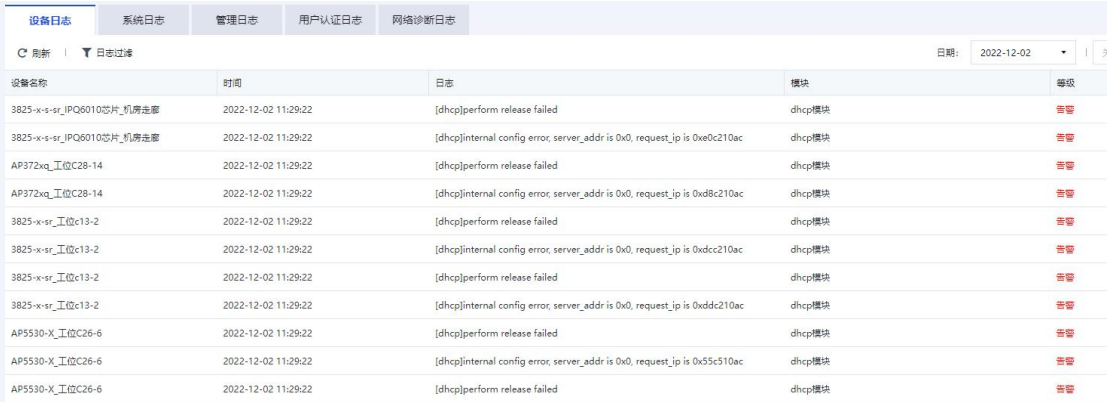
新增升级任务还可以设置高级选项：设置最长升级等待时间，当 AP 并没有立刻接入 NAC 时，可以设置比较长的升级等待时间，当 AP 接入 NAC 时，NAC 就会自动给 AP 升级，设置界面如下图：

提示：当 AP 接入 NAC 控制器时，AP 版本与 NAC 版本不匹配，AP 会自动升降到与 NAC 相同版本，只有当 AP 不能顺利升级到 NAC 版本时，或者 AP 版本是比 NAC 版本低但兼容的 β 版本时，才需要在控制台上主动加载包给 AP 升级。

3.9.9. 日志查看

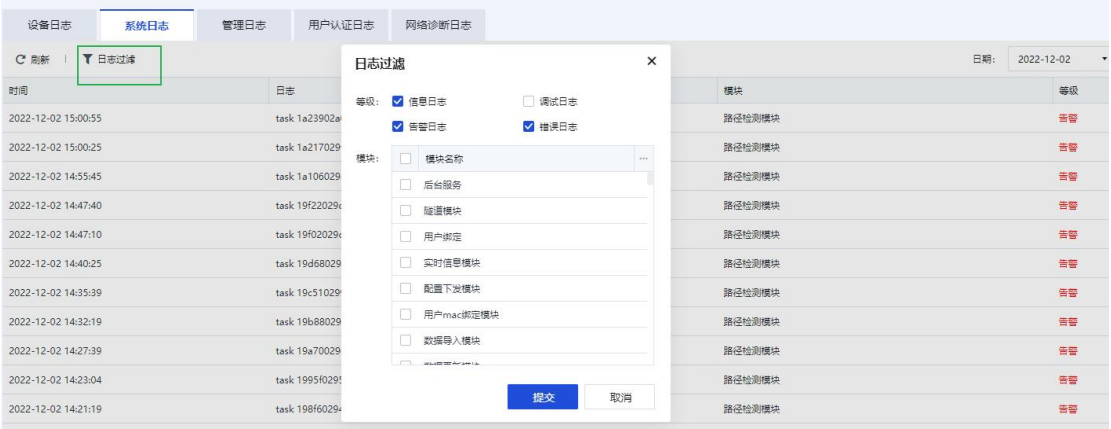
3.9.9.1. 设备日志

查看接入点日志产生的日志，协助发现及排除故障。



3.9.9.2. 系统日志

系统日志主要用于分析设备是否工作异常，系统日志有【信息日志】，【告警日志】、【调试日志】、和【错误日志】四种类型，并且可以根据需要选择某一个功能模块，专门查看该功能模块的日志，便于分析 NAC 是否有故障和异常，日志过滤选项界面如下



3.9.9.3. 管理日志

管理日志主要用于记录管理员登陆系统，注销系统，和修改系统配置的记录，便于进管理员操作的记录和审计。且日志可以通过记录“成功”和“失败”的方式进行记录和过滤，还可以进行操作对象的过滤，配置界面如下图

日志过滤配置界面如下图:

3.9.9.4. 用户认证日志

用户认证日志主要用于记录用户接入无线和退出无线的认证日志，用户分析用户认证情况，可以在设置的时间范围内，根据在 IP 地址，和用户名查询：

3.9.9.5. 网络诊断日志

网络诊断日志收集了 TrustSpeed 中进行网络检测后发送的检测报告，用于辅助排查用户在使用 TrustSpeed 过程中遇到的网络问题。

3.9.10. 故障排障

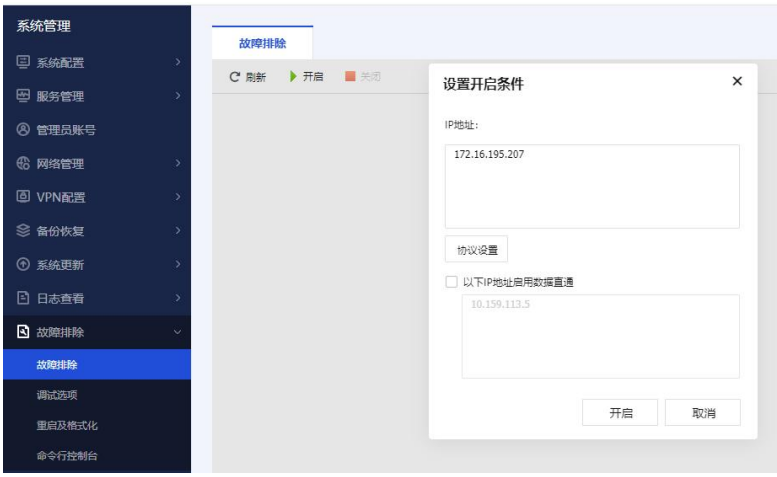
3.9.10.1. 故障排除

故障排除，主要用于网络故障时，用于排查问题原因，当无线终端可能由于配置问题导致用户无法正常上网时，进行故障排除和数据直通，使用方法与深信服 AC 设备类似，先是开启故障日志，也可以同时开启数据直通。提供了以下功能：

显示被系统拦截的数据包日志，以及拦截原因。当用户无法访问网络时，可以开启数据包拦截日志，并输入 IP 地址过滤，以查看数据包被拦截的原因。

开启直通，数据包将完全不受策略的控制，直接转发。此功能在遇到策略配置错误所导致的网络访问故障时，能快速地恢复网络。直通开启后，为了方便定位原因，系统将仍然输出数据包拦截日志，但实际上并未拦截数据包。

设置开启条件界面如下图：



3.9.10.2. 调试选项

调试选项

允许用户通过 sshd，telentd 方式连接到本设备上进行调试。允许用户通过开启历史日志信息和系统实时状态信息开关，采集设备的相关日志信息（不包含任何用户配置信息）。

设备故障分析

当设备工作不正常时，可以使用该功能修改查看设备状态，定位故障原因，使设备正常工作。工作不正常是指设备已经连入网络，但是无法连接上 wac 甚至无法发现，这时可以用该故障分析功能进行调试。主要功能为修改网络配置，查询 CLI 命令，恢复默认配置。如果设备工作正常，无需使用此功能。注意，如果操作不当可能适得其反。

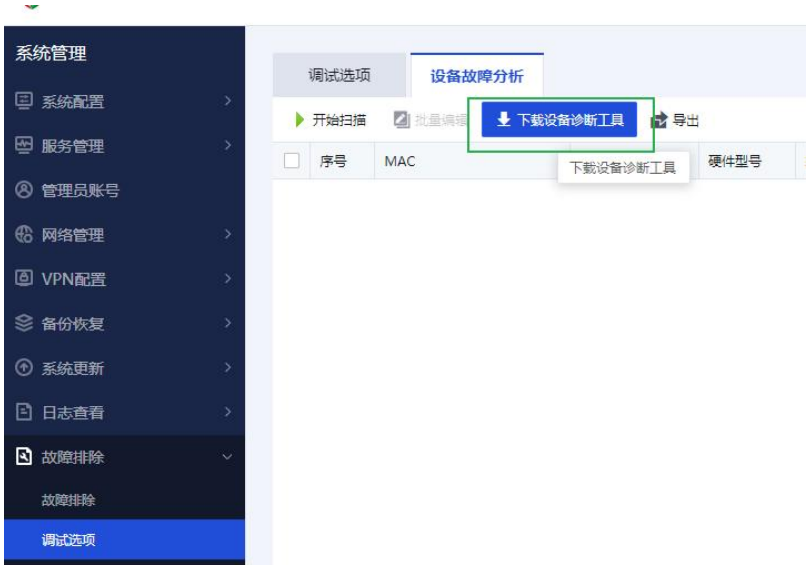
网页版工具只能扫描到与 NAC 二层相连的 AP 和安视交换机；如果 AP、安视交换机与

NAC 三层连接，则需要在 AP 和安视交换机的二层网络中接入一台 PC，下载设备诊断工具，在这台 PC 上运行工具调试 AP 和安视交换机。网页版工具默认使用 NAC 的登陆密码去操作 AP 和安视交换机，如果密码输入不正确会提示用户重新输入密码。

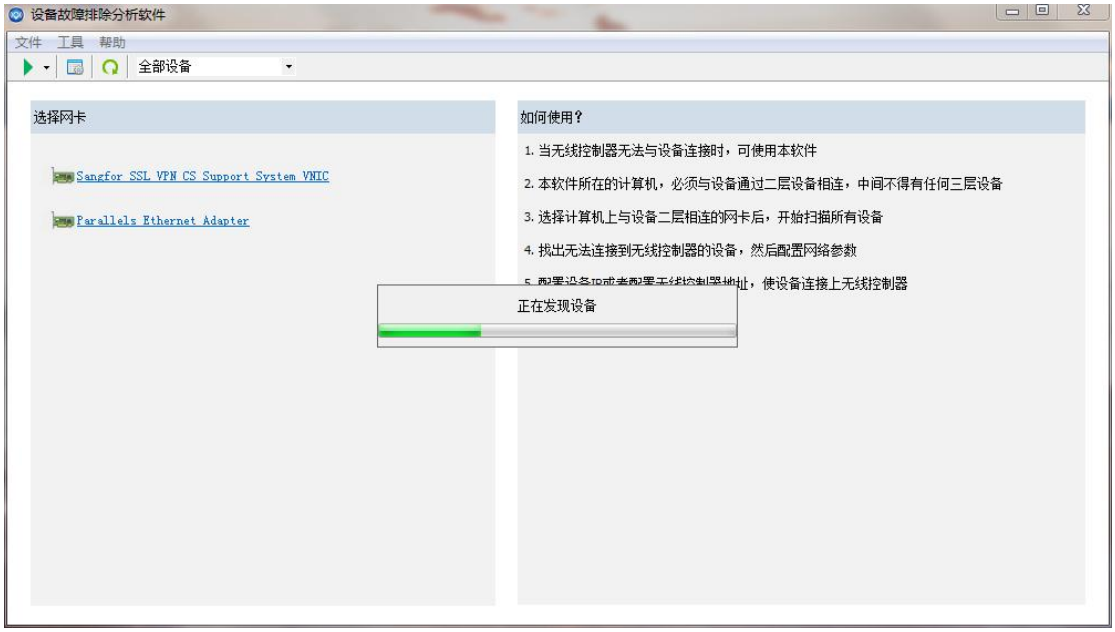
如果 AP 和安视交换机网络配置有误，例如 IP、网关、掩码不正确 导致不能和 NAC 通讯，点击开始配置通过设置正确的数据即可解决。

设备诊断工具

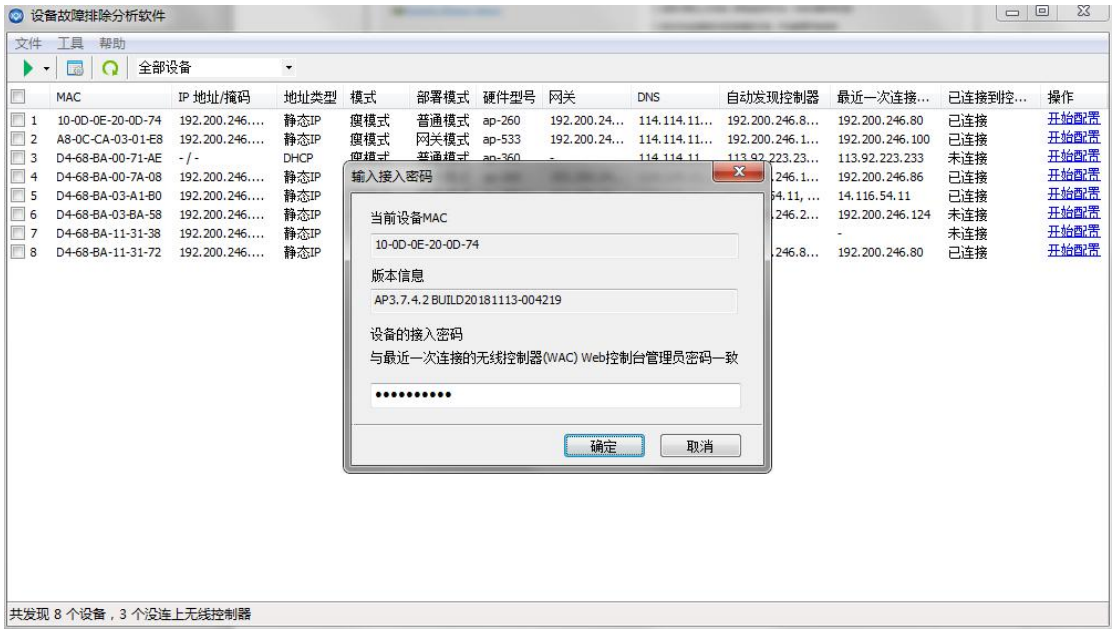
设备诊断工具客户端版本可以下载到 Windows 系统上运行，并且需要在 PC 上安装 winpcap 后才能可以使用。常用于 AP 和安视交换机无法自动发现 NAC 的场景，比如无 DHCP 环境，远程 AP、安视交换机配置，AP 和安视交换机掉线故障排查，拨号 AP 配置 Webagent 等环境。目前该工具配置功能只能临时保存在 AP 和安视交换机上，如果 AP、安视交换机重启会失效，需要 AP、安视交换机在 NAC 上线后，从 NAC 上下发配置保存到 AP、安视交换机上，AP、安视交换机重启配置才不会失效。



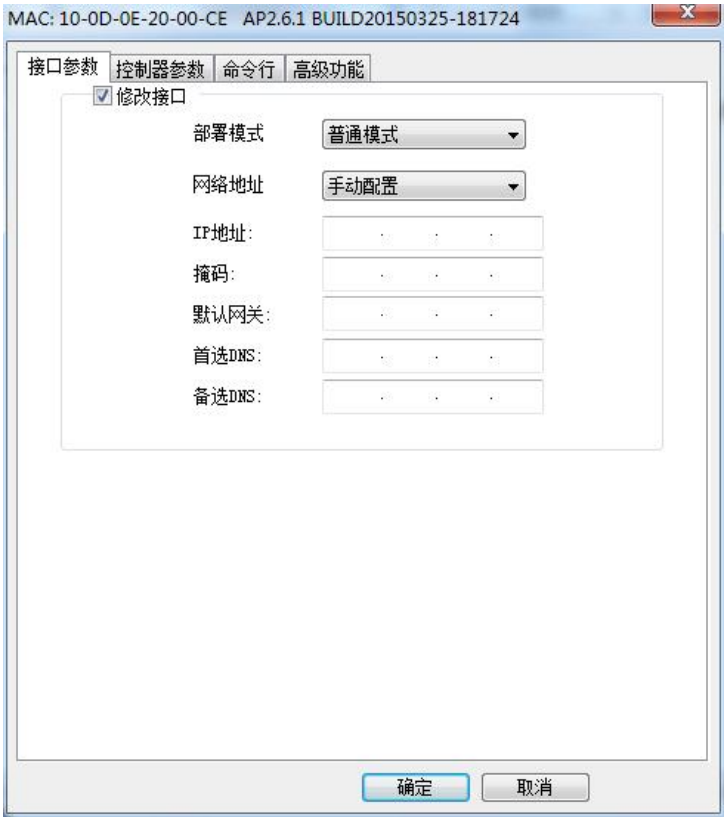
选择本地网卡后扫描 AP、安视交换机，页面如下：



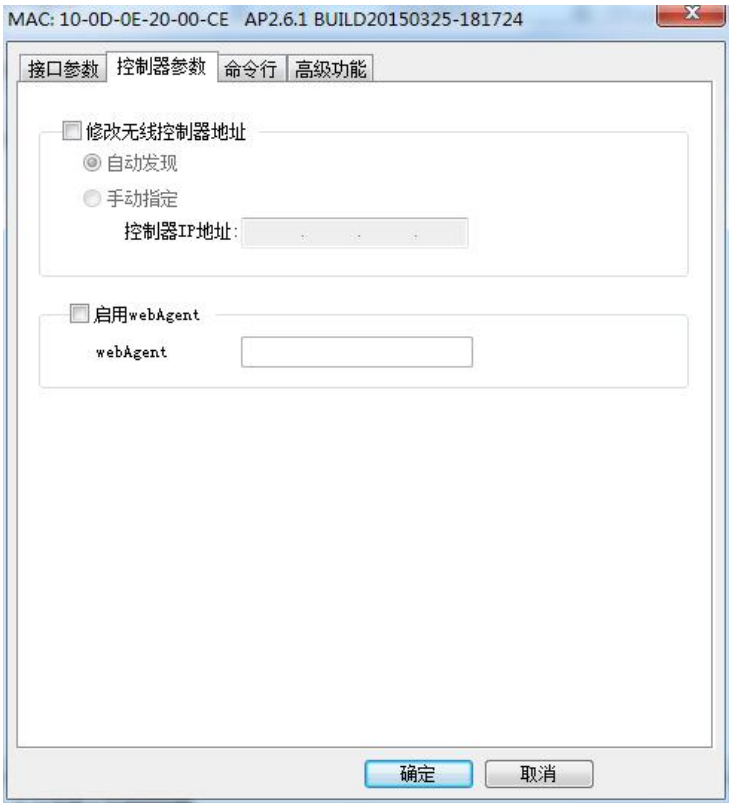
登录 AP 或安视交换机。



配置 AP 和安视交换机接口参数：修改 AP 的部署模式，IP 地址 ，网关信息等。



控制器参数：修改 NACIP 地址，webagent 地址。



命令行：在命令行下可以执行一些简单的调试命令

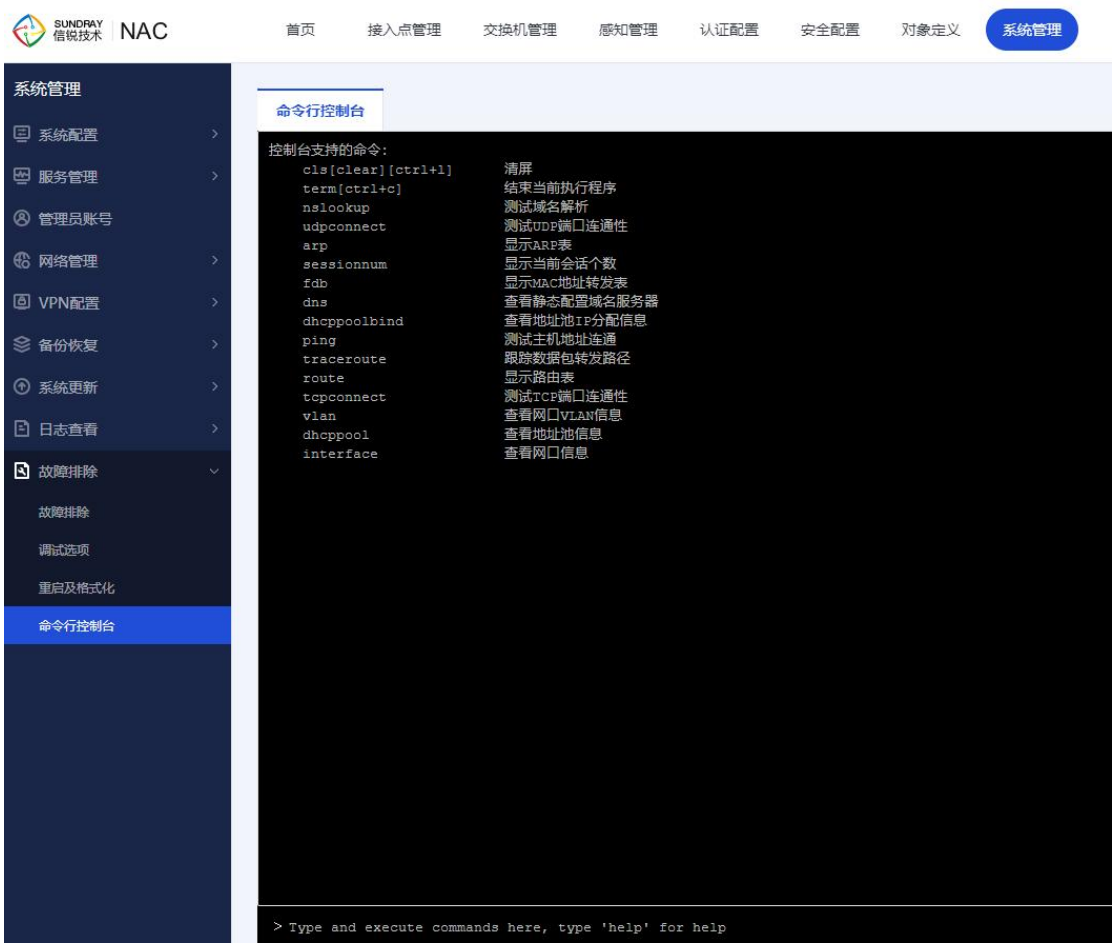
高级配置：恢复 AP 和安视交换机的默认配置，重启 AP 和安视交换机。

3.9.10.3. 重启及格式化

在 WEB 页面上重启数据中心、重启服务、重启设备、格式化缓存空间

3.9.10.4. 命令行控制台

提供可直接操作 nac 设备的调试命令，用于排除问题。



支持命令：

cls[clear][ctrl+l]	清屏
term[ctrl+c]	结束当前执行程序
vrrp	显示 VRRP 表
udpconnect	测试 UDP 端口连通性
arp	显示 ARP 表
sessionnum	显示当前会话个数
fdb	显示 MAC 地址转发表
dns	查看域名服务器
dhcppoolbind	查看地址池 IP 分配信息
ping	测试主机地址连通

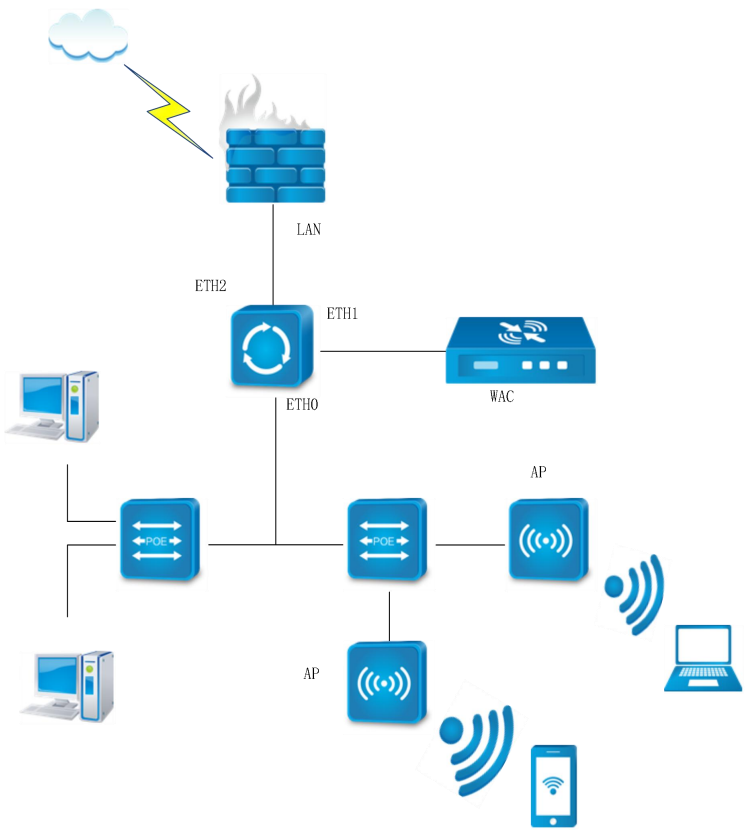
traceroute	跟踪数据包转发路径
route	显示路由表
tcpconnect	测试 TCP 端口连通性
vlan	查看网口 VLAN 信息
dhcppool	查看地址池信息
interface	查看网口信息

第 4 章 案例集

4.1. 设备部署配置案例

4.1.1. 部署案例

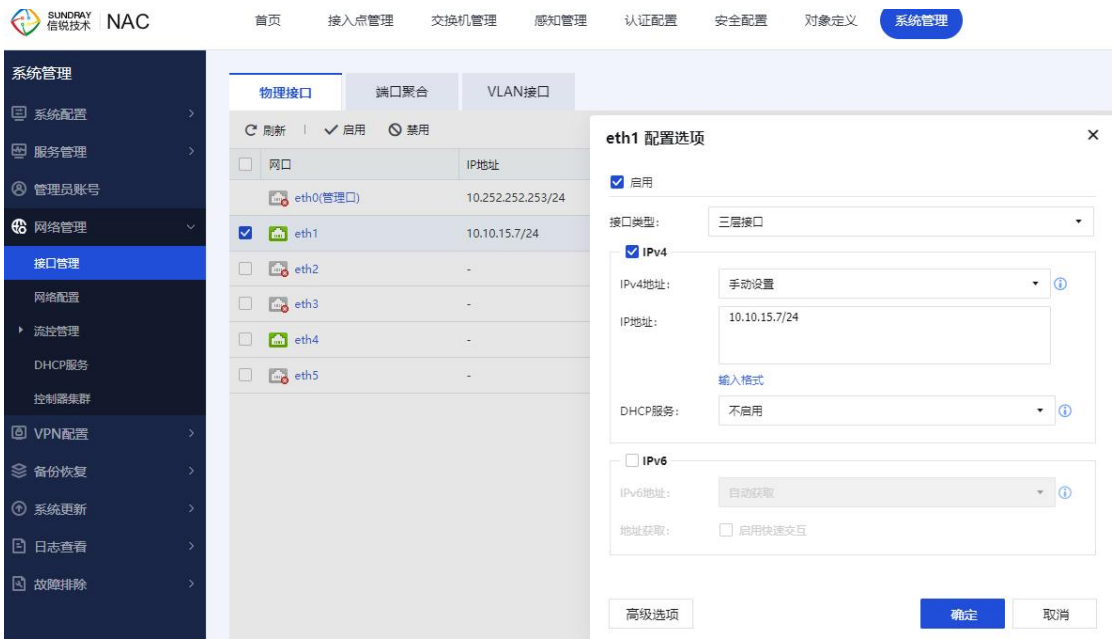
用户网络是复杂跨三层的网络环境，购买 NAC 设备以单臂部署在 3 层交换机上，实现对内网的所有无线 AP 进行集中管控和认证，通常部署 WLAN 时，部署的 AP 个数会非常多，下面部署案例中，都只以 2-3 个 AP 作为范例表示。图中，NAC 以单臂模式部署在客户网络 3 层交换机上，3 层交换机是内网 PC 的网关，如下图所示：



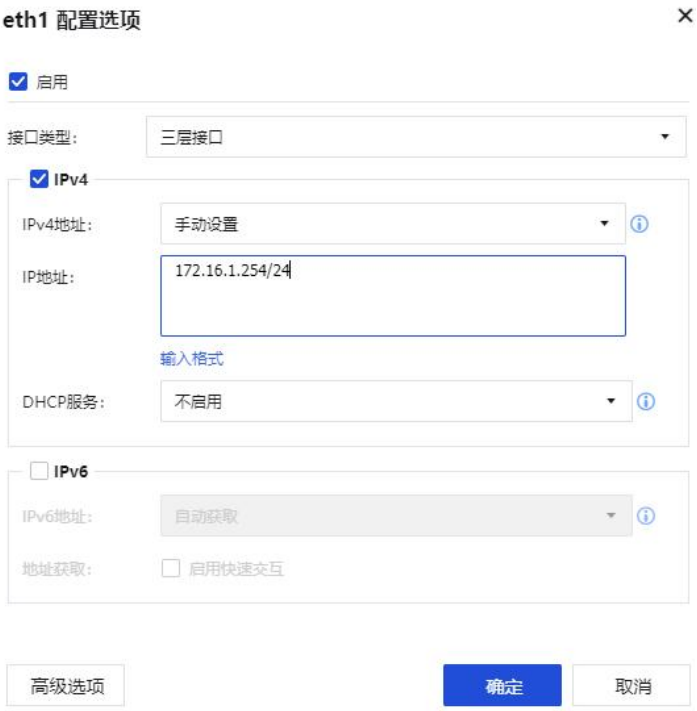
网络环境：三层交换机 eth0 口：192.168.1.1/24,eth1 口：172.16.1.1/24，eth2:10.0.0.1/24，FW：lan 口 10.0.0.2/24，NAC：172.16.1.254/24

第一步:通过管理口(ETH0)的默认 IP 登录设备。管理口的默认 IP 是 10.252.252.252/24，在电脑上配置一个相同网段的 IP 地址，通过 https://10.252.252.252 登录设备。

第二步：配置 NAC 可以上网，通过『网络管理』→『接口管理』，点击需要设置成外网接口的接口，如 eth1，出现以下页面：



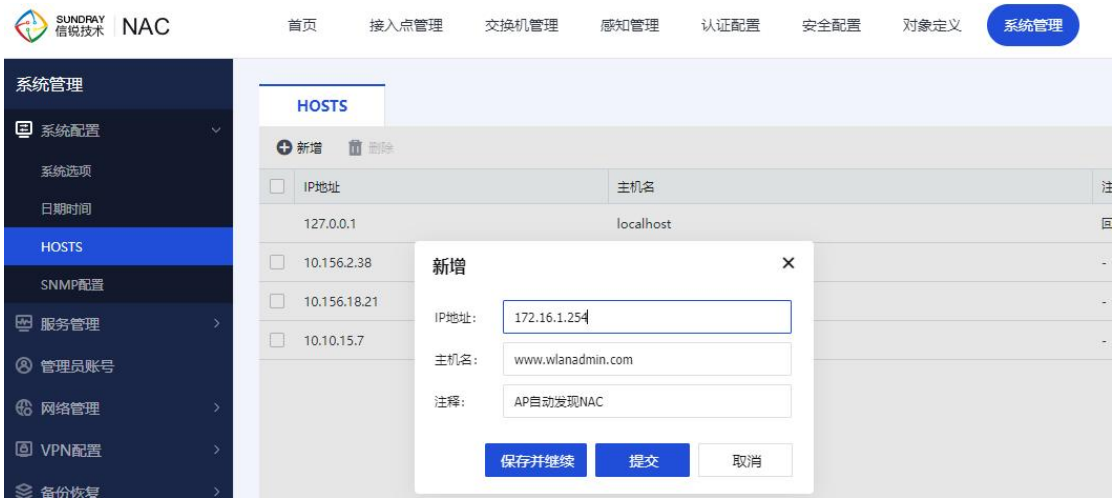
配置 eth1 接口 IP 地址为：172.16.1.254/24



第三步：配置 NAC，让 NAC 可以正常上网，到【网络管理】-【网络配置】处添加 8 个 0 的静态路由

第四步：在 NAC 上配置 HOSTS，并启用 DNS 代理，当 AP 获取解析到的默认域名 www.wlanadmin.com 为 NAC 的 IP 地址时，AP 会自动发现 NAC。在【系统管理】-【系统配置】-【HOSTS】这里配置 NAC 的 IP 地址 172.16.1.254 的主机名为：

www.wlanadmin.com。并在【网络管理】-【网络配置】-【DNS】配置 DNS 地址，并且启用 DNS 代理。



需要在 3 层交换机启用 DHCP，并且对配置分发的 DNS 服务器为 NAC 的 LAN 口 IP 地址：172.16.1.254。

第五步：激活 AP，当 AP 第一次部署在网络中时，默认会通过 DHCP 请求获取 IP 地址，会生成默认网关，并且获取到 DNS。这是 AP 会默认请求域名 www.wlanadmin.com，会向解析到的 IP 发起连接协议，这里 NAC 上就可以在【接入点管理】-【接入点】-【发现新接入

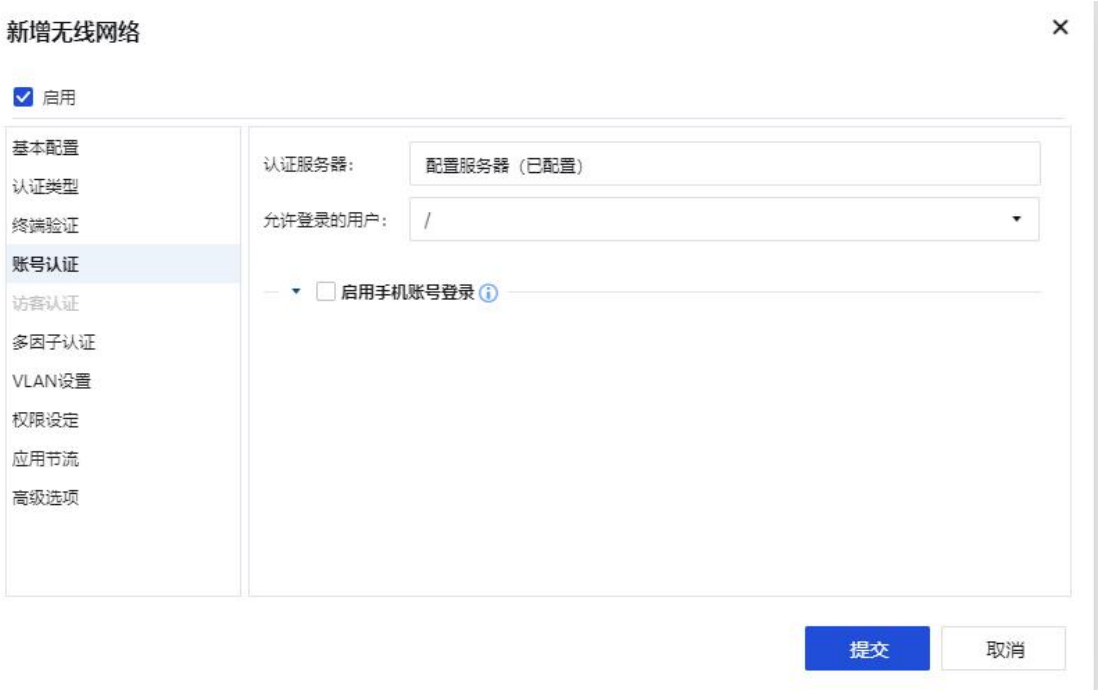
点】处激活 AP。（因环境原因，截图中的 IP 地址应该为 192.168.199.104/24 网段的 IP 地址）

激活 AP 时，选择 AP 的所属于组为“默认组”，网络地址配置为：自动获取，填写发现控制器 IP。

第六步：新增无线网络“sundray_test”并选择该网络匹配的 AP 组为默认组，以及设置该无线网络的认证方式。数据转发模式选择为“本地转发模式”。设置频段选择“所有”。

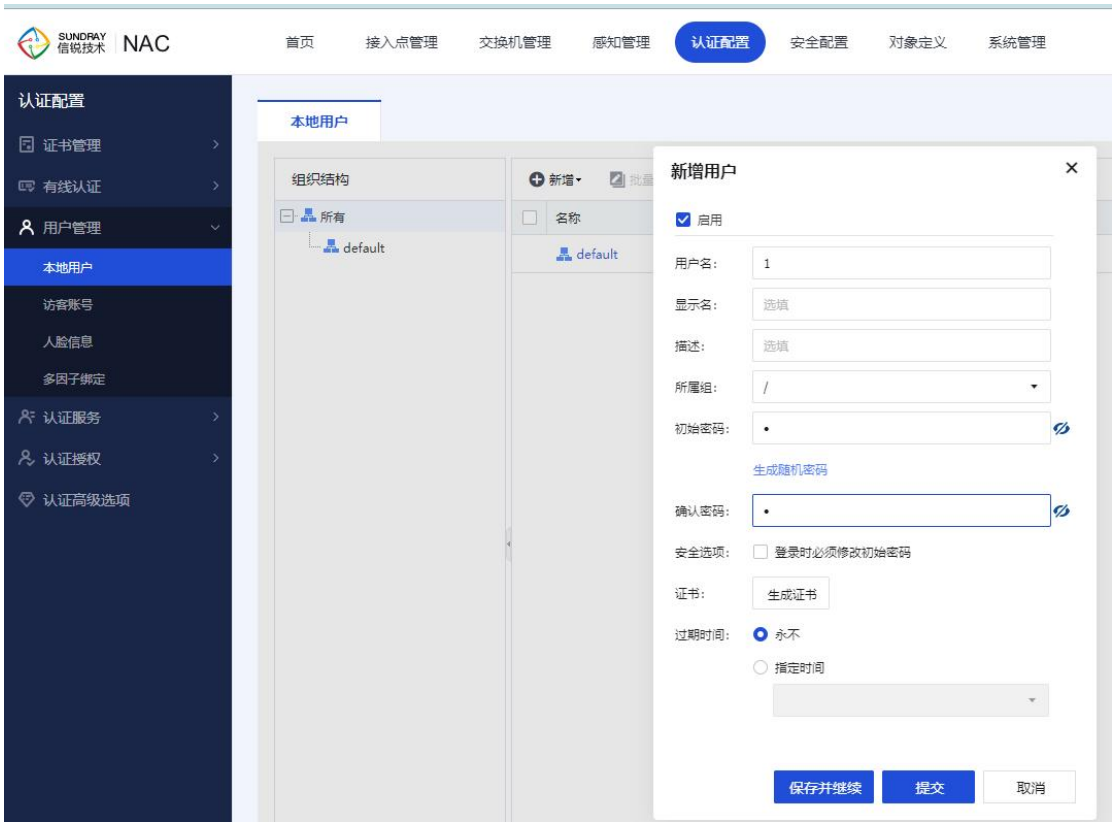
认证类型选择为：“WPA-PSK/WPA2-PSK+ Web 认证”，并设置接入密钥为“support1”。

终端验证不启用，设置用户认证为“本地用户”方式，允许登录的用户组为所有。



VLAN 配置和角色分配这个案例默认就可以了，暂时不需要配置。

第八步：新增本地用户，当无线终端接入 WEB 认证时，需要输入本地用户名和密码才可以正常上网。


SUNDRAY 信锐技术 NAC
首页
接入点管理
交换机管理
感知管理
认证配置
安全配置
对象定义
系统管理
认证配置
证书管理
有线认证
用户管理
本地用户
访客账号
人脸信息
多因子绑定
认证服务
认证授权
认证高级选项
本地用户
组织结构
所有
default
新增
名称
default
新增用户
启用
用户名:
1
显示名:
选填
描述:
选填
所属组:
/
初始密码:
生成随机密码
确认密码:
安全选项:
登录时必须修改初始密码
证书:
生成证书
过期时间:
永不
指定时间
保存并继续
提交
取消

第 5 章 附录

5.1. SUNDRAY 设备升级系统的使用

SUNDRAY 设备升级系统可用于对设备进行内核版本升级和备份恢复设备配置。在设备出现致命错误时，也可通过 SUNDRAY 设备升级系统把设备恢复到出厂状态。同时，SUNDRAY 设备升级系统还可以启动技术支持工具来检查系统网口工作状态，路由等配置信息以及更改网口工作模式等。

SUNDRAY 设备升级系统为绿色版软件，解压后即可使用，解压文件里包含一个文件夹和一个主程序，界面如下：

双击打开主程序的主界面，界面如下：

『设备 IP 地址』：连接的 SUNDRAY 设备的 IP 地址，格式为 IP：端口，也可以直接输入 IP 地址进行访问，则默认连接的是该 IP 地址的 51111 端口。

『管理员密码』：NAC 的默认密码为 dlanrecover 或者是与 NAC 的控制台密码保持一致，与所连接的 NAC 的版本有关。

『查找设备』：通过点击查找设备来搜索局域网内部的 SUNDRAY 设备。

输入 SUNDRAY 设备的 IP 地址以及管理员密码后，点击连接即可连接到设备进行系统升级、恢复默认配置等操作，界面如下：

『当前设备信息』：用于显示连接的 SUNDRAY 设备的版本信息以及连接的 IP 地址。

『设备升级』：对当前连接的 SUNDRAY 设备进行升级操作，包括在线升级和从本地加载升级包进行升级。

在线升级：

选择在线升级，点击选择版本，SUNDRAY 设备升级系统会自动判定设备当前版本支持升级到哪个版本，并自动列出可以支持升级的版本信息，选择期望升级到的版本，点击确定后，系统会自动从服务器上下载升级包进行升级操作。

1.使用 SUNDRAY 设备升级系统进行在线升级时，要求所连接的 SUNDRAY 设备能够正常上网，否则将不能进行在线升级。

2.SUNDRAY 设备的某些版本不支持在线升级功能，具体请联系信锐技术客户服务中心确认。

从本地加载升级包：

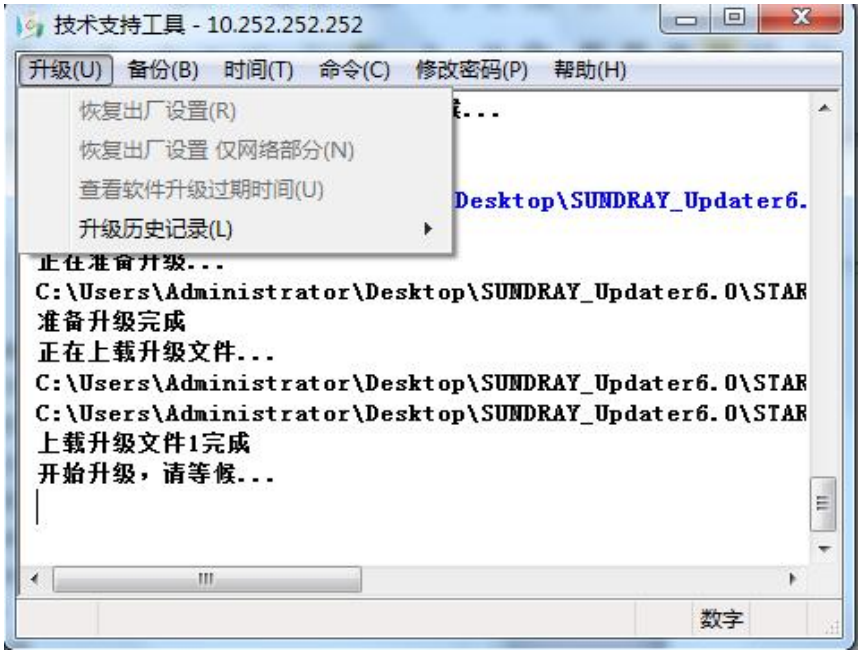
选择从本地加载升级包，点击浏览，选择下载到本地的相应升级包，然后点击下一步，显示当前升级包的基本信息，确认无误后，点击开始升级进行升级操作，界面如下：

升级完成后，设备升级状态里会显示“升级成功”，界面如下：

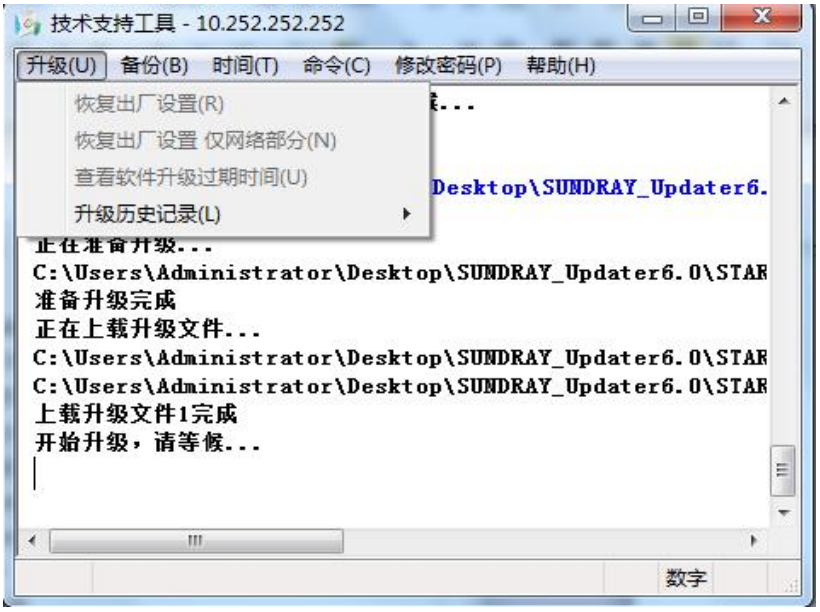
1. 升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如需升级请联系信锐技术客户服务部。

启动技术支持工具:

SUNDRAY 设备升级系统连接到 SUNDRAY 设备后，可以按 F10 或 Ctrl+Shift+F10 启动技术支持工具。技术支持工具有『升级』、『备份』、『时间』、『命令』、『修改密码』和『帮助』几个菜单，下面分别介绍它们的功能。



『升级』：包括恢复出厂设置，恢复出厂设置仅网络部分，查看软件升级过期时间和升级历史记录。如下图：



[恢复出厂设置]：用于将 SUNDRAY 硬件设备恢复到默认配置，需要通过加载升级包将设备恢复出厂设置。

[恢复出厂设置仅网络部分]：只能在没有连接到设备时才能使用。会将设备的网络配置恢复到默认出厂配置，此操作是通过广播包发送命令进行操作的，会对局域网内的所有 SUNDRAY 硬件网关生效，有一定危险性，请勿擅自点击操作。

[查看软件升级过期时间]：检测当前网关是否处于升级服务有效期内。若不在升级服务有效期内，则不能升级，需要购买相应授权才能升级。

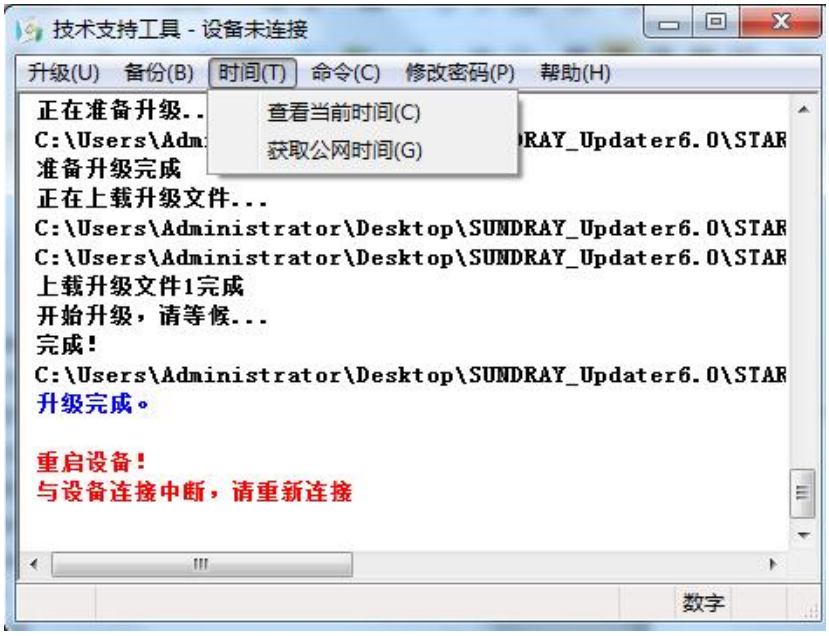
[升级历史记录]：用于查看当前设备的以往升级历史，或者查看或清除本地的历史升级记录。

『备份』：包括备份配置、恢复备份配置选项，如下图：

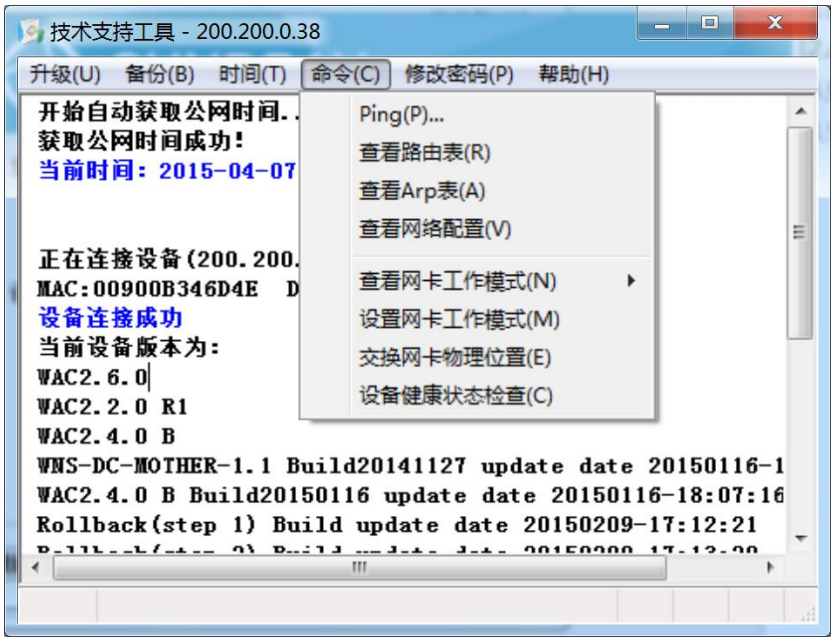
[备份配置]：将设备现有的配置信息进行备份。

[恢复备份配置]：将以前备份过的配置信息恢复到设备中。

『时间』用来查看当前时间和同步公网时间，来效验设备升级授权是否过期。如下图：



『命令』：包括 Ping、查看路由表、查看 Arp 表、查看网络配置、查看网卡工作模式、设置网卡工作模式、交换网卡物理位置以及设备健康状态检查选项。如下图：



[Ping]：登录设备后，从设备往外网 ping，以验证设备是否和外网连通。

[查看路由表]：查看设备本机的路由表。

[查看 ARP 表]：查看设备本机的 ARP 表，因为 NAC 属于特殊无线网络设备，通过升级客户端方式查看的 ARP 不代表其内部真实的 ARP 表，所以该返回值不具备参考性。

[查看网络配置]：查看设备本机的网络配置，包括接口 IP 配置等。

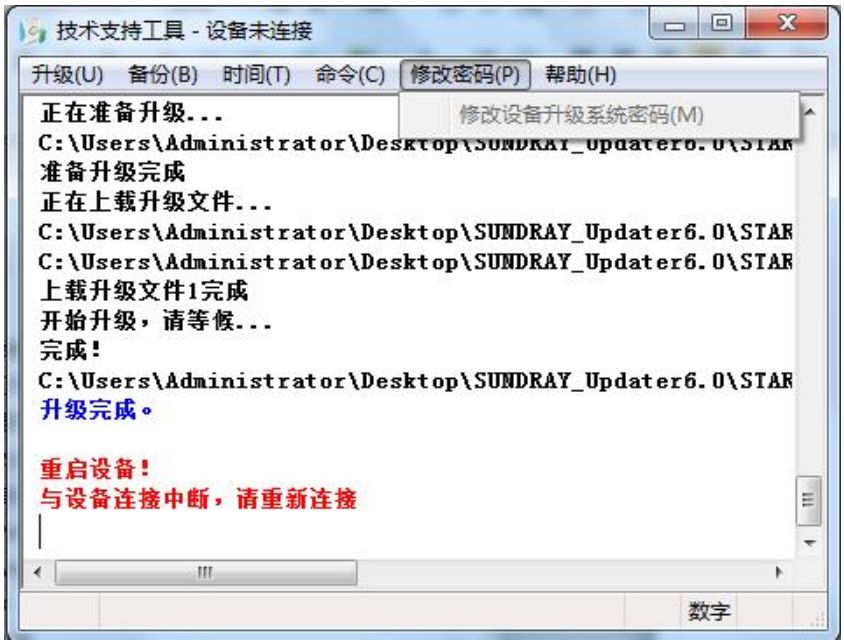
[查看网卡工作模式]：查看设备各网卡的工作模式。

[设置网卡工作模式]：NAC 产品线该功能不可用。

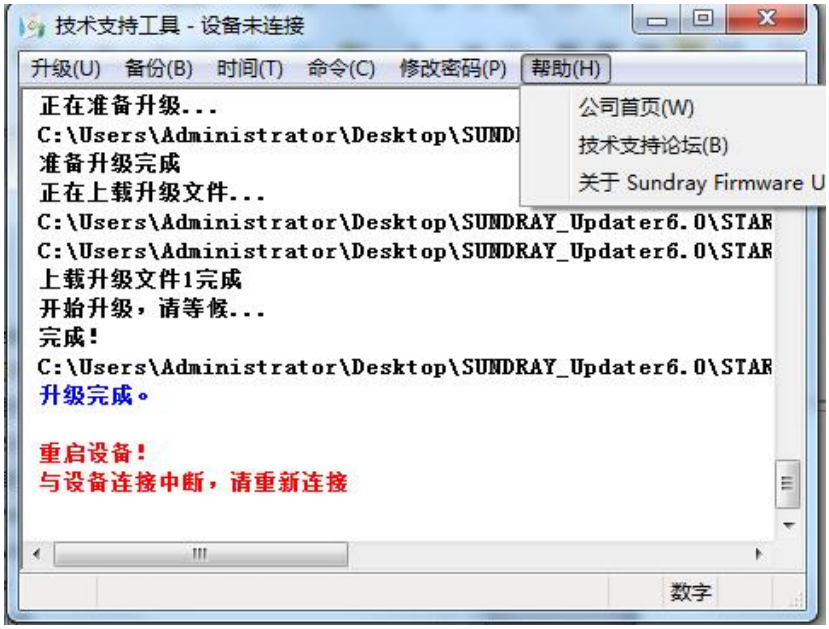
[交换网卡物理位置]：NAC 产品线，该功能不可用。

[设备健康状态检查]：通过在线检测或者是上传脚本来检测设备的硬件状态。

『修改密码』：用于修改 SUNDRAY 设备升级系统密码，如下图：



『帮助』包括公网首页的链接，技术支持论坛的链接和查看当前 Updater 的版本信息。


技术支持工具 - 设备未连接
升级(U) 备份(B) 时间(T) 命令(C) 修改密码(P) 帮助(H)
公司首页(W)
技术支持论坛(B)
关于 Sundray Firmware U
正在准备升级...
C:\Users\Administrator\Desktop\SUND
准备升级完成
正在上载升级文件...
C:\Users\Administrator\Desktop\SUNDRAY_Updater6.0\STAR
C:\Users\Administrator\Desktop\SUNDRAY_Updater6.0\STAR
上载升级文件1完成
开始升级，请等候...
完成！
C:\Users\Administrator\Desktop\SUNDRAY_Updater6.0\STAR
升级完成。
重启设备！
与设备连接中断，请重新连接
数字