安视交换机瘦模式

用户使用手册

V3.8.1.0

SUNDRAY 信锐技术

目录

第 1 章 NAC 控制台的使用与激活

1.1. 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后出现以下的登录界面：

在登陆框输入『账号』和『密码』，应用选择“交换机管理中心”，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。

1.2. 配置和使用

登录 WebUI 配置界面后，可以看到以下关于安视交换机配置模块：包括『系统状态』、『对象定义』、『认证授权』、『交换机管理』、『以太网管理』、『路由管理』、『组播管理』、『流控与安全』、『高可用性』、『系统管理』、『系统维护』以及边缘安全相关模块功能。

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。

设备登陆控制器方式：

1、电脑连接 M 口，电脑 IP 地址改为 10.252.252.56/24，其他默认即可。

2、打开浏览器输出 https://10.252.252.252　　admin　　sundray123

3、控制器的有线配置，接口配置，网络配置，VLAN 配置在首页的有线配置栏里。

4、鼠标移到右上角应用中心，点击交换机管理中心，即可对交换机进行配置。

5、鼠标移到右上角应用中心，点击边缘安全，即可对交换机，控制器等进行安全配置。

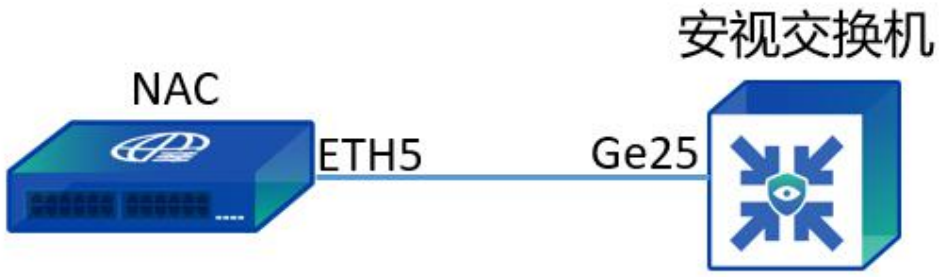
1.3. 交换机产品简介

信锐 RS3300&5300&6300&6500 系列产品是信锐自主研发的下一代安视交换机。下一代安视交换机采用全新的系统架构设计，可以同瘦 AP 模式一样在无线 AC 上零配置上线管理，实现安视交换机的即插即用。信锐下一代安视交换机可以通过多种方式自动发现无线 AC，通过无线 AC 即可对交换机进行配置管理，包括端口信息、VLAN、端口开启关闭等；可以通过无线 AC 进行可视化状态查看，包括交换机负载、端口转发负载、交换机在线离线状态、端口开启关闭状态等；还具备比传统交换机更安全的特性，同时可以与无线网络、安全设备进行联动实现更安全的网络终端安全管控。

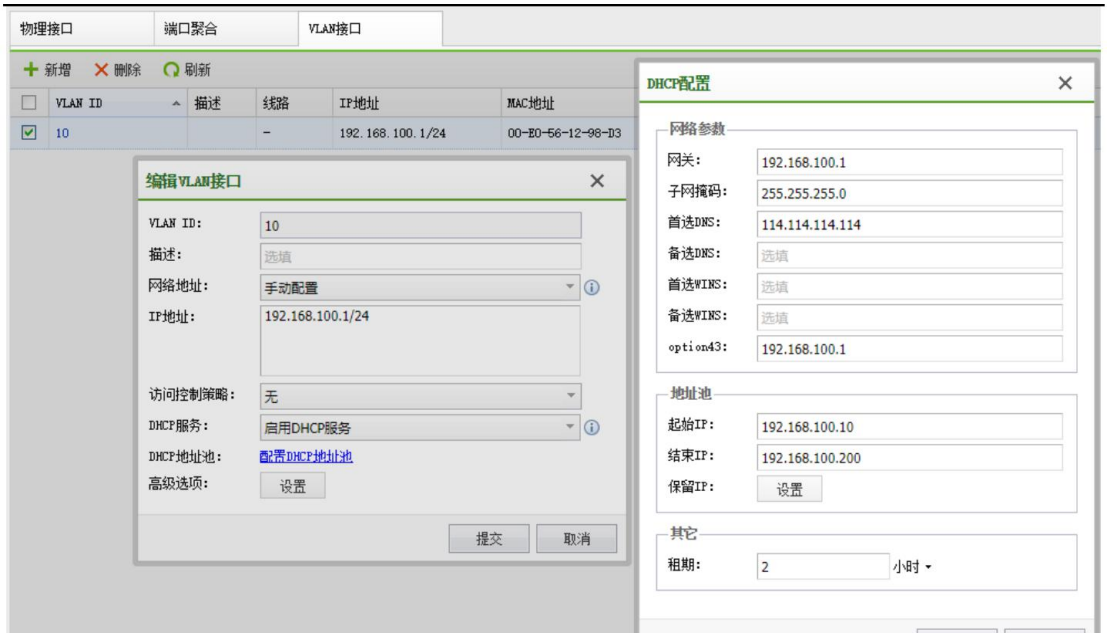
信锐下一代安视交换机 RS3300&5300&6300&6500 提供了丰富的千兆电/光、万兆光接口。RS3300&5300&6300&6500 系列交换机在同类产品中处于领先地位，能够满足大型网络的组网需求，并具备丰富的安视和安全特性，特别适合于作为大型校园网、企业网、IP 城域网的网络设备。

1.4. 交换机的激活方式

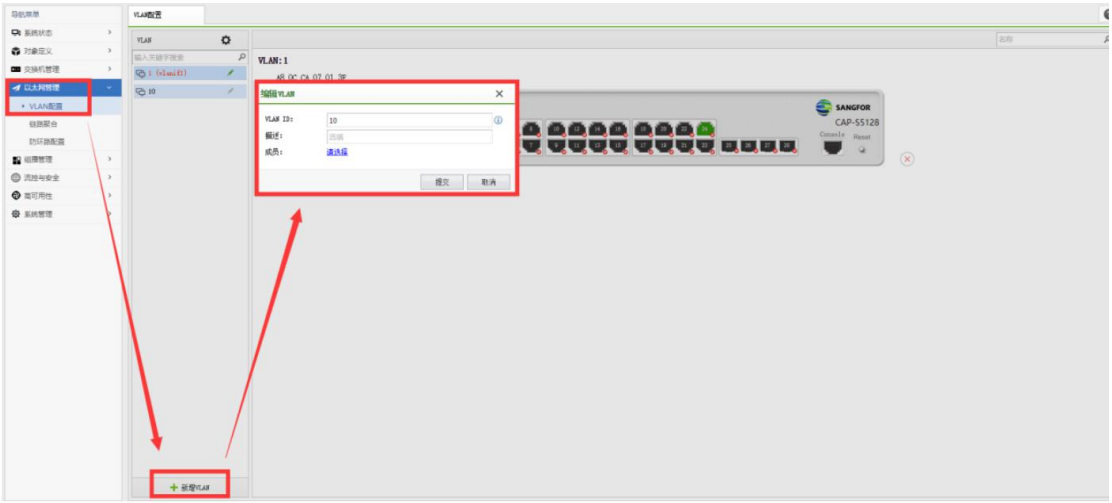
拓扑环境：



1、首先将控制器的接口 ETH5 配置为 Trunk native vlan10，并开启 vlan10 接口，配置 DHCP。



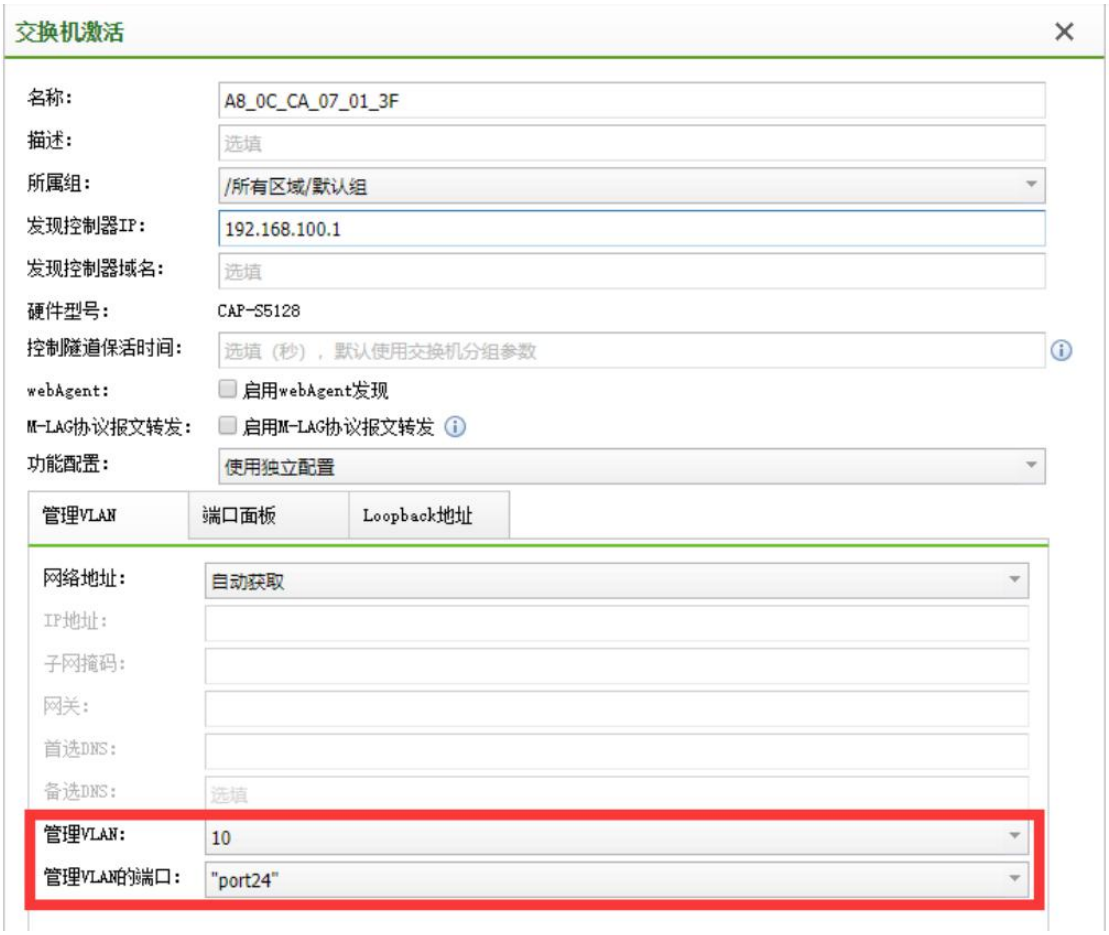
2、还需要提前在交换机的配置页面新增一个 VLAN10，因为在后面激活交换机选择管理 VLAN 时需要这边先进行添加。



3、激活交换机

大致流程为修改交换机管理 vlan，并把相应端口进行修改后，点击提交，如下所示：

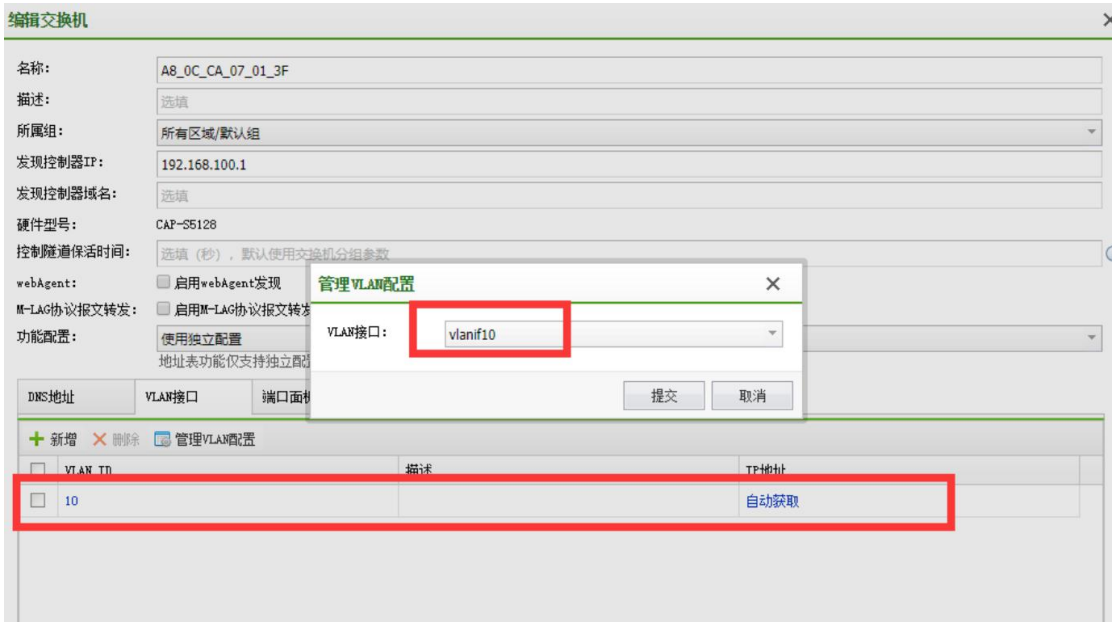
（1）我们将交换机的管理 VLAN 改为 10，选择对应的物理接口。



（2）端口面板配置

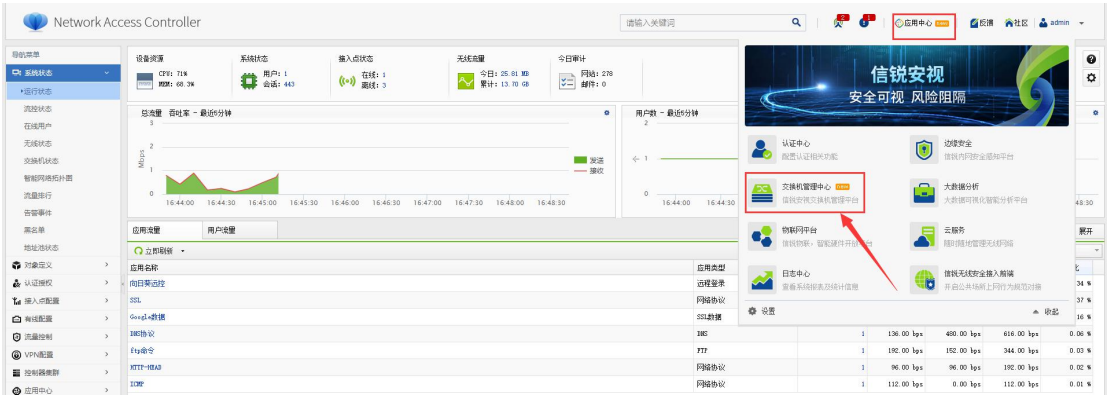
打开端口面板，点击交换机上对应的上联端口，修改该接口的 VLAN 属性，修改为 trunk PVID 为 10，允许所有。配置完成之后点击提交。

（3）提交后之后就可以看到设备上线了， 同时交换机的配置里面管理 VLAN 为 10，VLAN 接口里面也只有 VLAN 10。



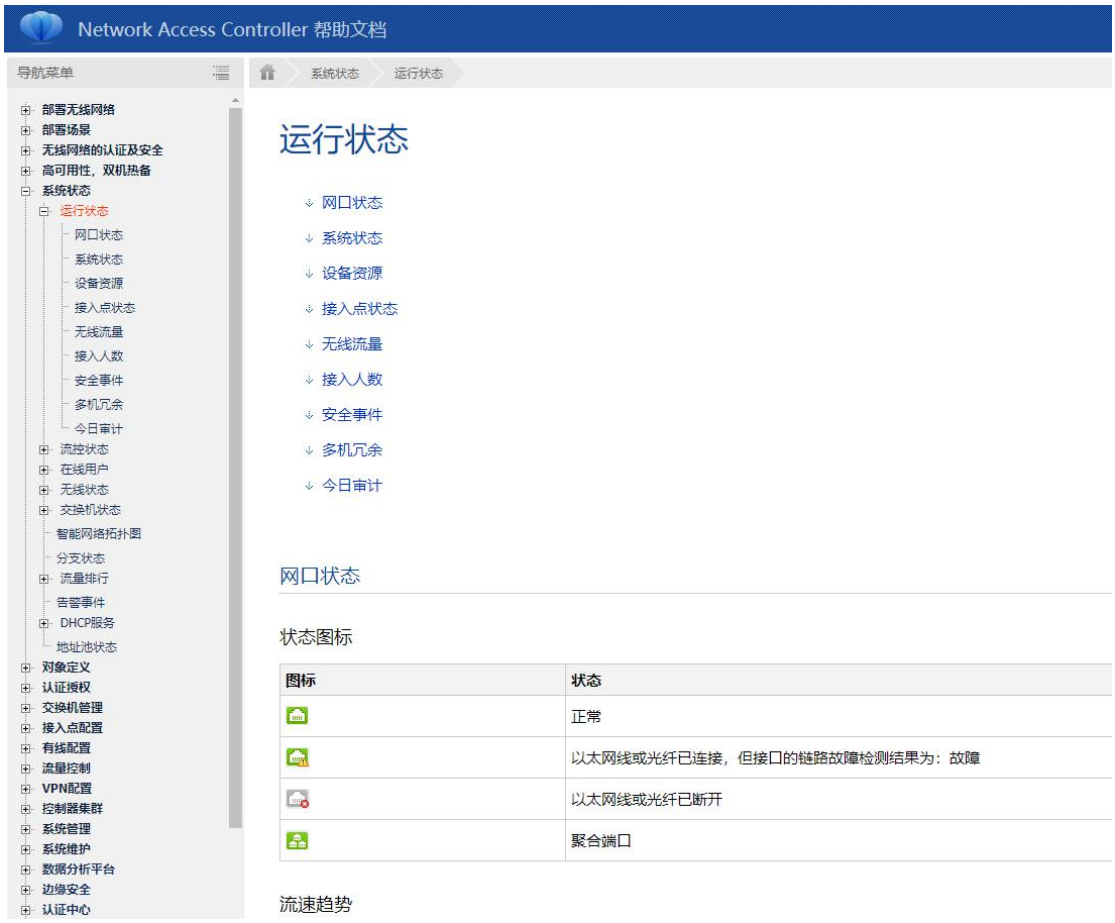
第 2 章 交换机管理中心

通过点击应用中心->交换机管理中心进入交换机管理中心页面。



2.1. 安视交换机帮助文档

对于 NAC 控制器平台，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。



2.2. 系统状态

『系统状态』主要用于查看设备的基本状态信息，包括【交换机状态】、【智能网络拓扑图】、【交换机地址池状态】、【在线用户】。

2.2.1. 交换机状态

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，PoE 供电状态。点击具体的某个口，可以看到端口的详情，包括 VLAN 和 PoE 的配置信息，以及流量趋势，端口收发包情况。

单独点击交换机名称可以查看交换机配置信息。

【普通模式】可以查看交换机的所属组、MAC 地址、管理 IP、描述、控制器、序列号、射频天线数、软件版本、硬件版本、管理 VLAN、交换机日志、整机吞吐。

【链路聚合】可以查看当前配置的链路聚合组状态。

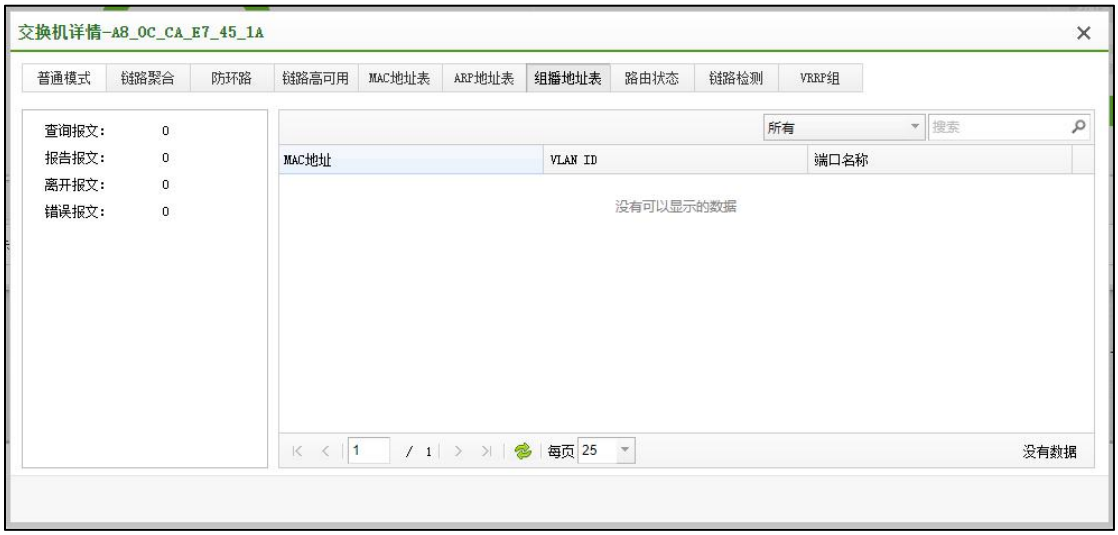
【防环路】可以查看当前配置的生成树以及环路检测信息。

【链路高可用】可以查看当前配置的备份链路以及上行链路监控的状态。

【MAC 地址表】可以查看当前交换机的 MAC 地址表信息。

【ARP 地址表】可以查看当前交换机的 ARP 地址表信息。

【组播地址表】可以查看当前交换机的组播地址表信息。



【路由状态】可以查看当前交换机的路由表信息。

【链路检测】可以查看当前交换机配置的链路检测信息。

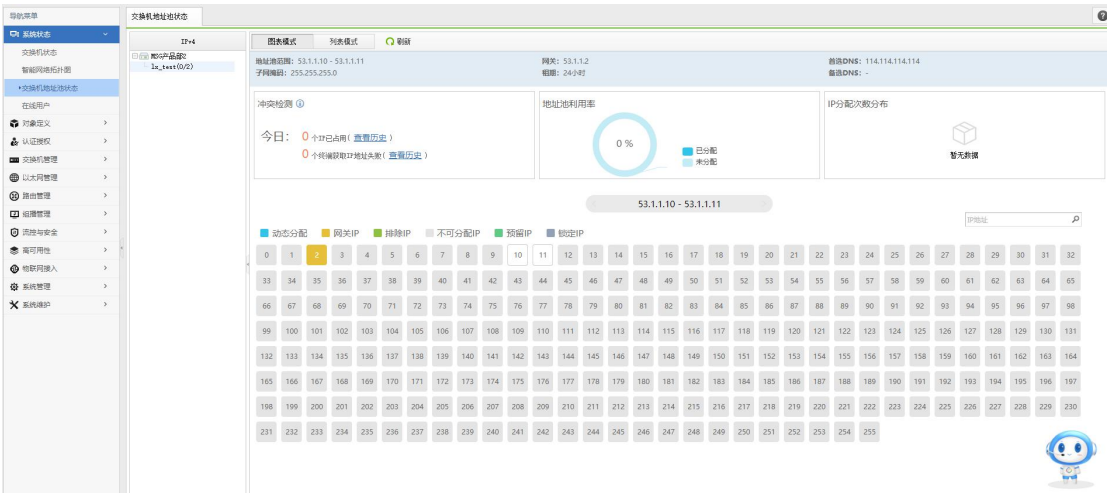
【链路检测】可以查看当前交换机配置的 VRRP 组状态。

2.2.2. 智能网络拓扑图

瘦交换机接入到网络当中，会自动生成拓扑，便于管理员清晰的了解整网拓扑情况，并通过智能拓扑图可以清晰的看出交换机在线情况。

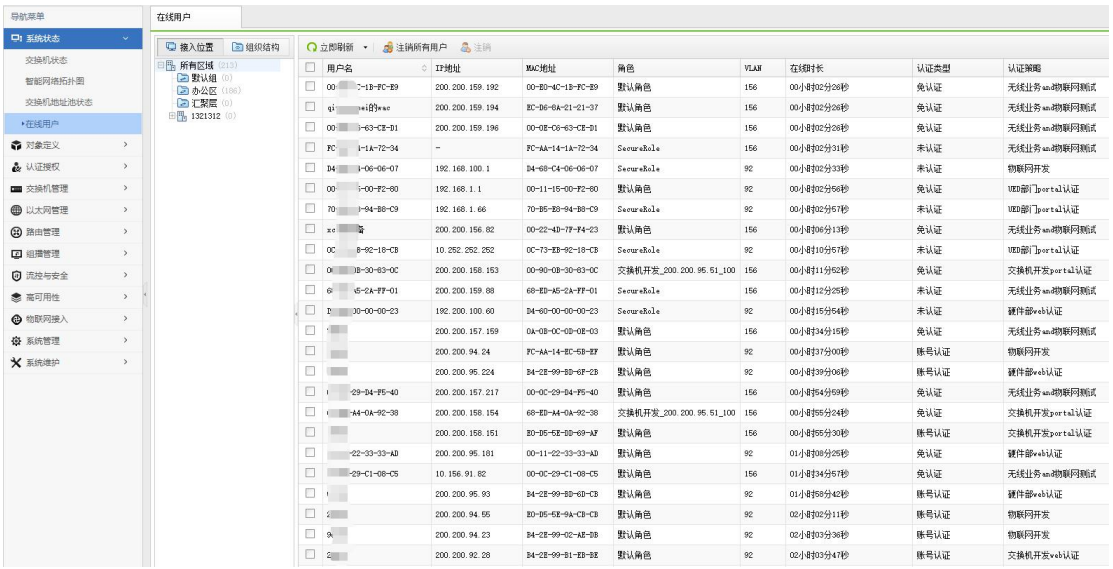
2.2.3. 交换机地址池状态

展示交换机 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。



2.2.4. 在线用户

显示交换机上以有线方式上线的用户，以及用户的终端，权限，接入端口，交换机分组等信息。



2.3. 对象定义

『对象定义』用于配置【IP 组】、【MAC 地址库】、【时间计划】、【DHCP 服务】。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。

2.3.1. IP 组

将一个、多个 IP 地址或 IP 段划分为一个 IP 组，以便在系统的其它功能中调用，例如角色中的访问控制策略。

支持输入多个 IP 地址、IP 范围、网段，例如：

IP 地址：192.168.1.1

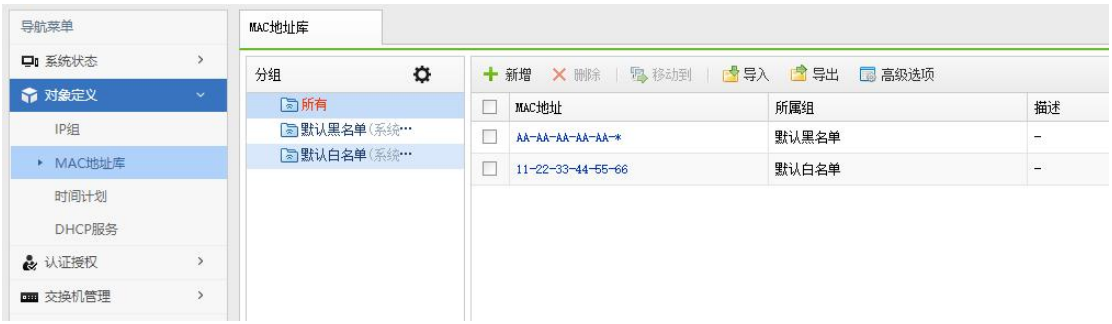
IP 范围：192.168.1.10-192.168.1.100

网段：192.168.1.0/24

网段：192.168.1.0/255.255.255.0

2.3.2. 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。



2.3.3. 时间计划

在配置网络安全策略（即 ACL）时，如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，时间计划分为【单次时间计划】和【循环时间计划】。

2.3.4. DHCP 服务

2.3.4.1. 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。

2.3.4.2. 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。

2.4. 认证授权

『认证授权』包含【角色授权】、【本地用户】、【访客帐号】、【证书管理】、【Web 认证】、【用户终端绑定】、【外部服务器】、【微信认证选项】、【单点登录】、【portal 服务】、【认证漫游域】、【Radius 服务】、【认证高级选项】。

2.4.1. 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，功能包括【角色授权】、【有线访问控制策略】。

2.4.1.1. 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访问控制策略。

2.4.1.2. 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。

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

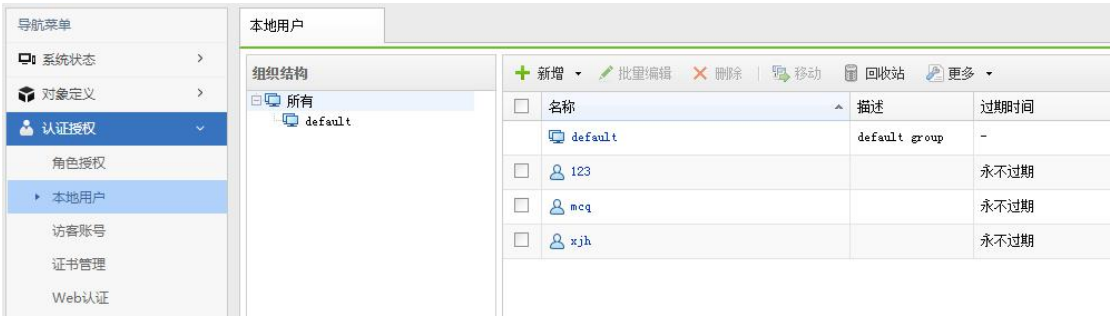
支持使用二层/三层网络协议来定义 ACL 规则，包括 ARP、RARP、ICMP、TCP、UDP、IGMP、IP、OSPF 等协议。

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。

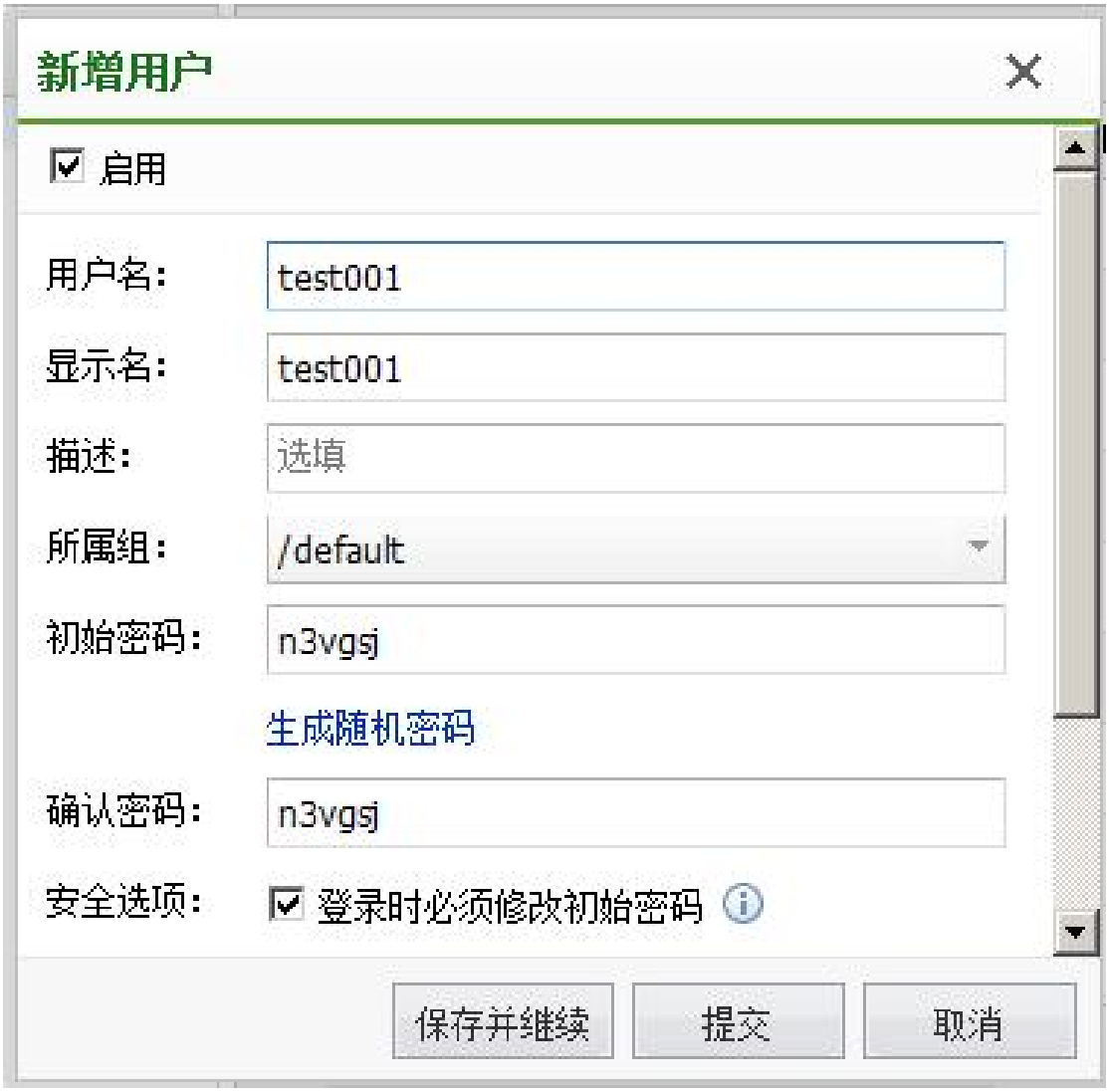
2.4.2. 本地用户

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



2.4.2.1. 新增用户

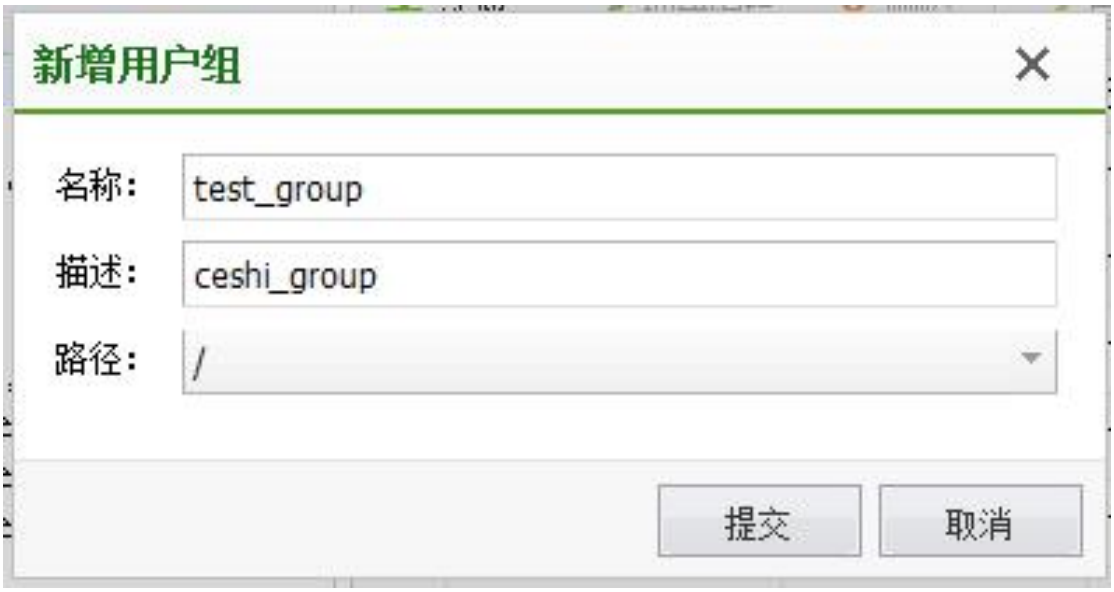
新增用户：新增一个用户，包括用户名，所属组，设置初始密码，并且可以设置登录时必须修改初始密码。



管理员可以为用户设置初次随机密码，然后勾选“登录时必须修改初始密码”，便于用户的认证管理。

2.4.2.2. 新增用户组

新增用户组为了便于给无线用户分组管理，可以新增用户组，并选择路径，默认是跟组路径/。



2.4.2.3. 批量编辑用户

批量编辑用户：用于批量编辑用户的启用/禁用状态，所属组，有效期和密码修改，便于多用户管理和维护。

2.4.3. 访客帐号

【访客账号】存储所有的访客认证信息，包括短信验证的访客、二维码审核的访客、临时帐号访客、微信验证的访客等。

2.4.3.1. 短信认证

短信认证是指访问网络时，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。

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。

4、短信认证的有效期为：永久生效。

短信认证服务

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：

1、通过连接到 NAC 串口的短信猫发送

2、通过连接到外部服务器的短信猫发送

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

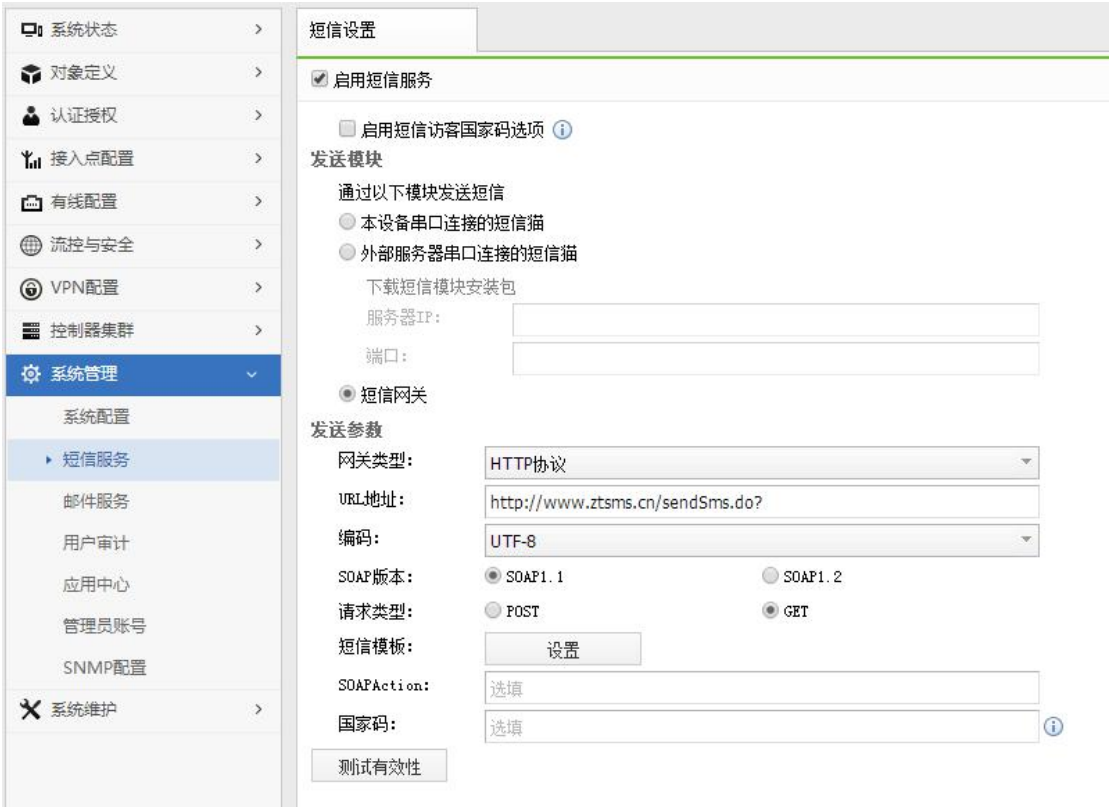
短信猫连接到一台服务器，并把服务器部署到此机房以外，且信号良好的环境中，由此服务器来代理发送短信。

部署步骤如下：

1、在短信认证选项界面中，下载“信锐短信发送服务程序”，并安装在运行 Windows XP，Windows 7，Windows Server 2003，Windows Server 2008，32 位系统的计算机中。

2、把短信猫连接到此计算机的串口/USB 口（取决于短信猫型号）。

3、确保 NAC 可以访问此计算机。并在 NAC 中，配置正确的短信发送参数。



还可以通过 WebServices 方式发送短信，通过 HTTP 方式的短信网关，此方法较为常用。

2.4.3.2. 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。在 Web 认证中，可以指定审核人，在二维码审核时分配被审核人的角色和上网时长，并且记录访客信息。

2.4.3.3. 临时帐号认证

此方式通常用于企业、酒店的访客网络认证，可以在访客登记后，接待人员创建一个临时账号，并设置账号的有效期。访客使用此账号完成认证。

临时账号管理员

访客账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，系统提供了临时账号管理员，以区别于 NAC 的管理员。临时账号管理员只允许管理访客账号，无法修改 NAC 的其它设置。

临时账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

2.4.3.4. 社交应用

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。

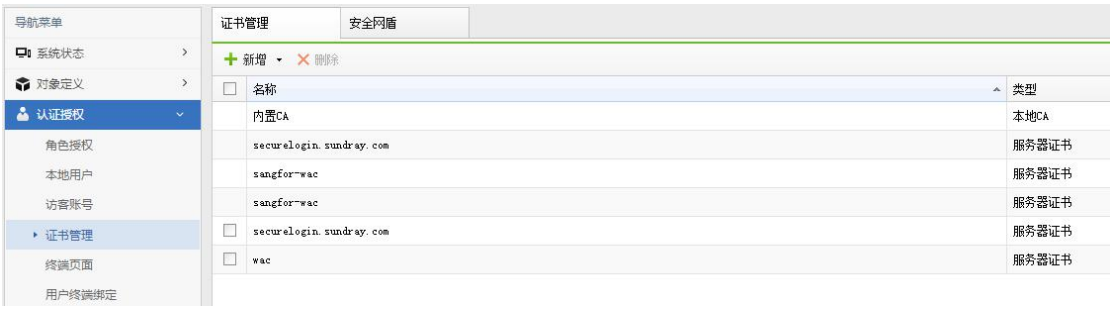
配置社交应用认证时，认证前需要放通对应流量，推荐使用内置角色进行认证。

2.4.4. 证书管理

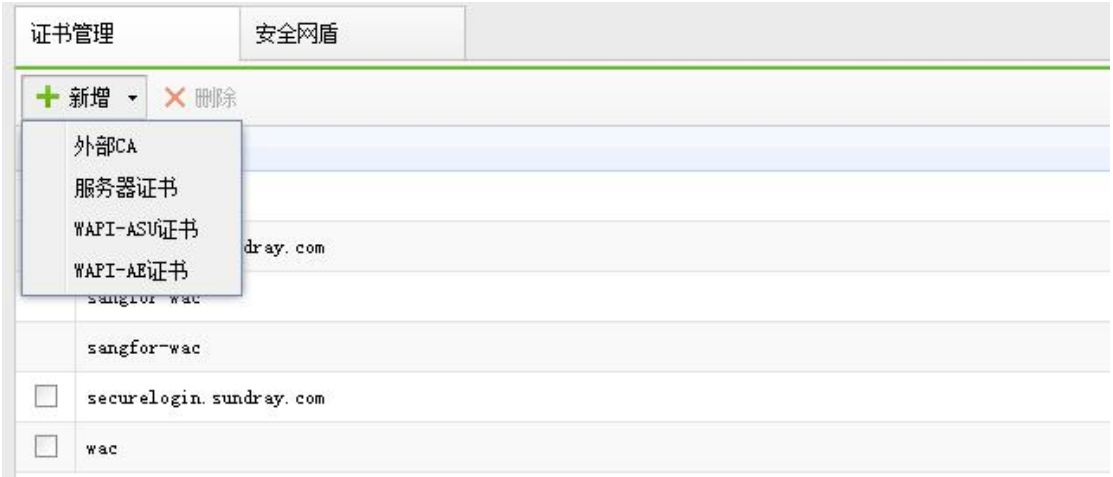
包含【证书管理】和【安全网盾】两个模块。

2.4.4.1. 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，大大加强了企业用户终端的安全接入。



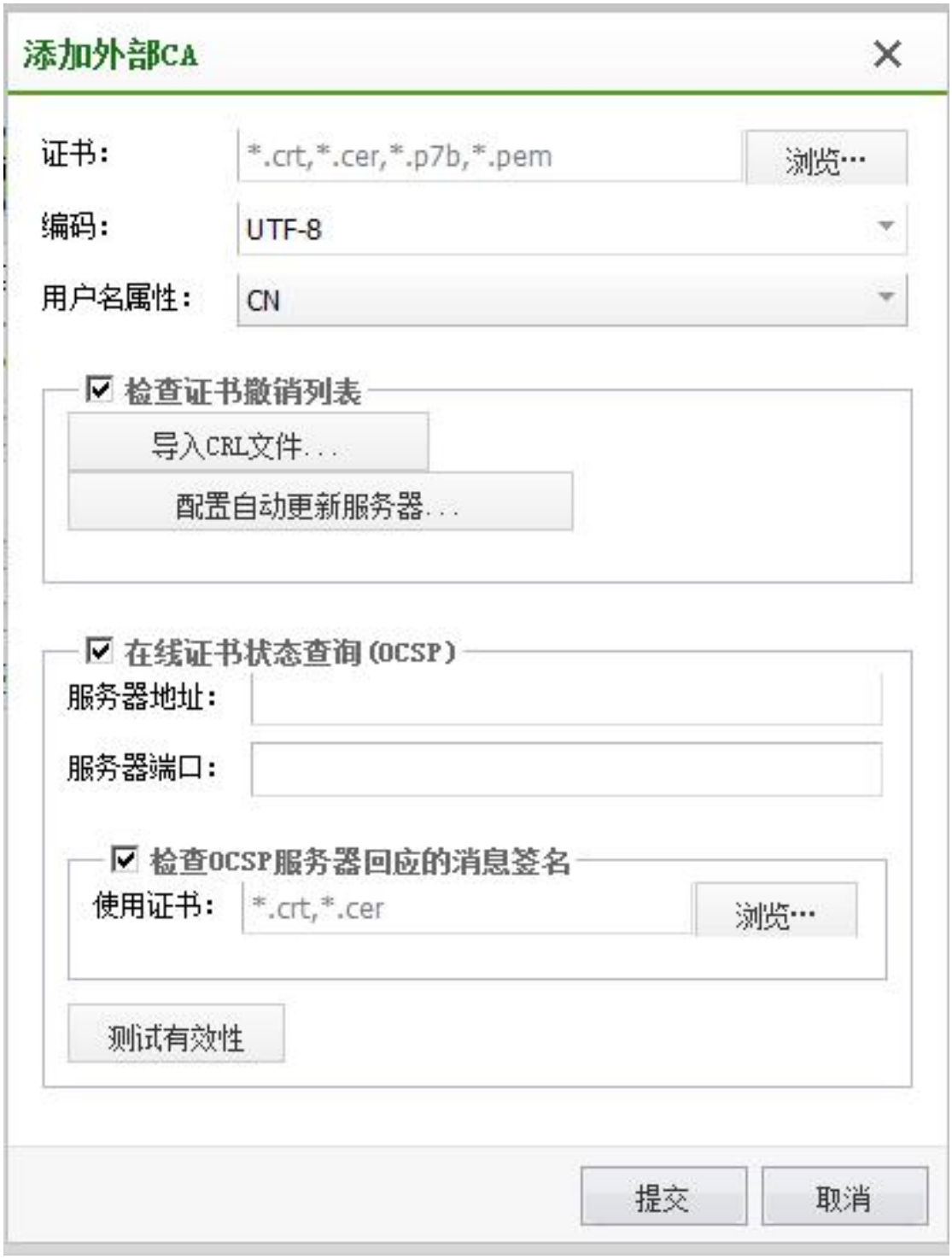
证书可以新增【外部 CA】、【服务器证书】、【WAPI-ASU 证书】和【WAPI-AE 证书】



2.4.4.1.1. 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。

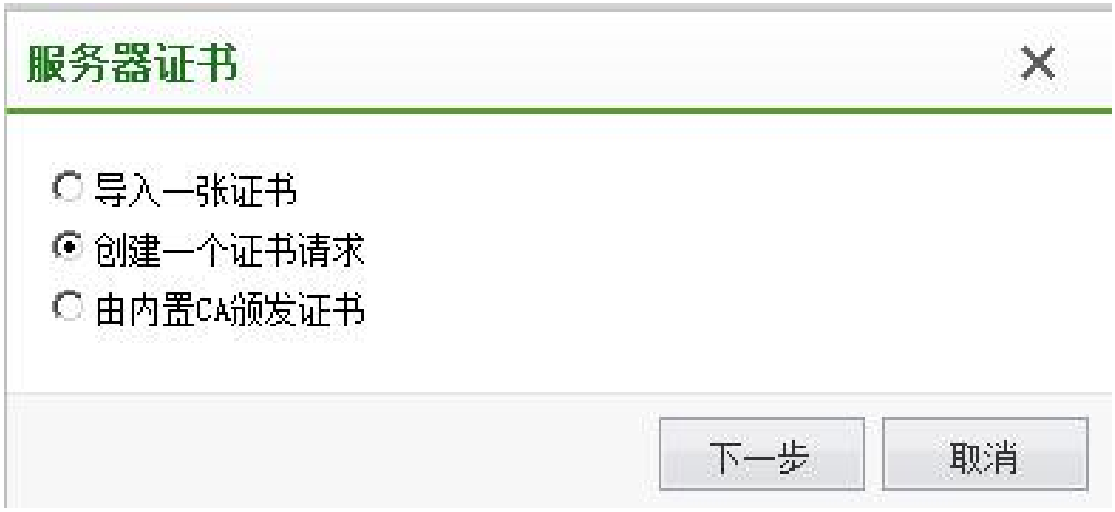
【导入 CRL 文件】：CRL 文件可以简单的理解为一个记录了用户证书序列号的文件，该文件由 CA 签发发布，记录了的证书序列号表示该证书已经失效。也就是 CRL 里面记录的证书序列号表示由这个 CA 签发的证书并且序列号在 CRL 文件里面的都已经是无效了的证书。

【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

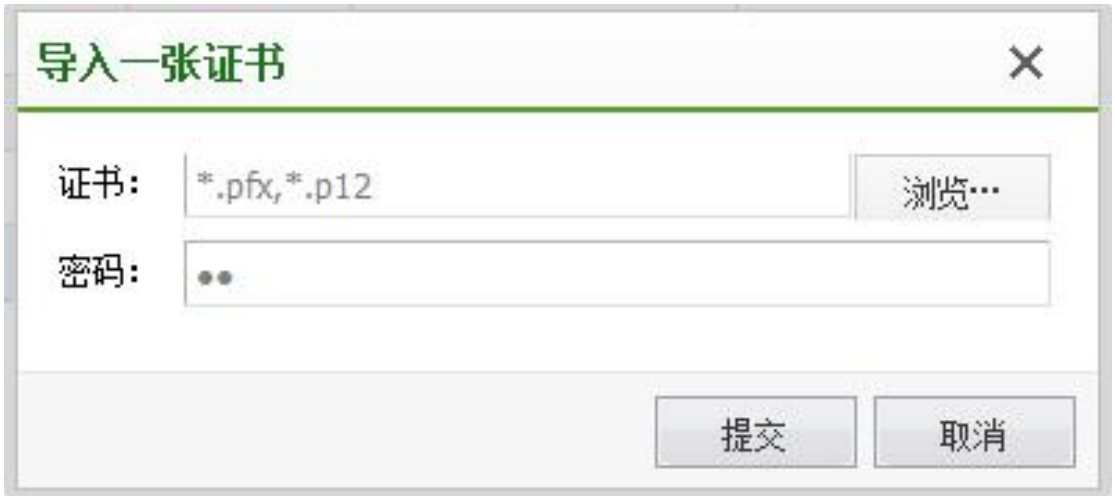
【检查 OCSP 服务器回应的消息签名】导入 OCSP 服务端签名证书的公钥，主要检测 OSCP 数据在传输过程中是否被篡改。

2.4.4.1.2. 服务器证书

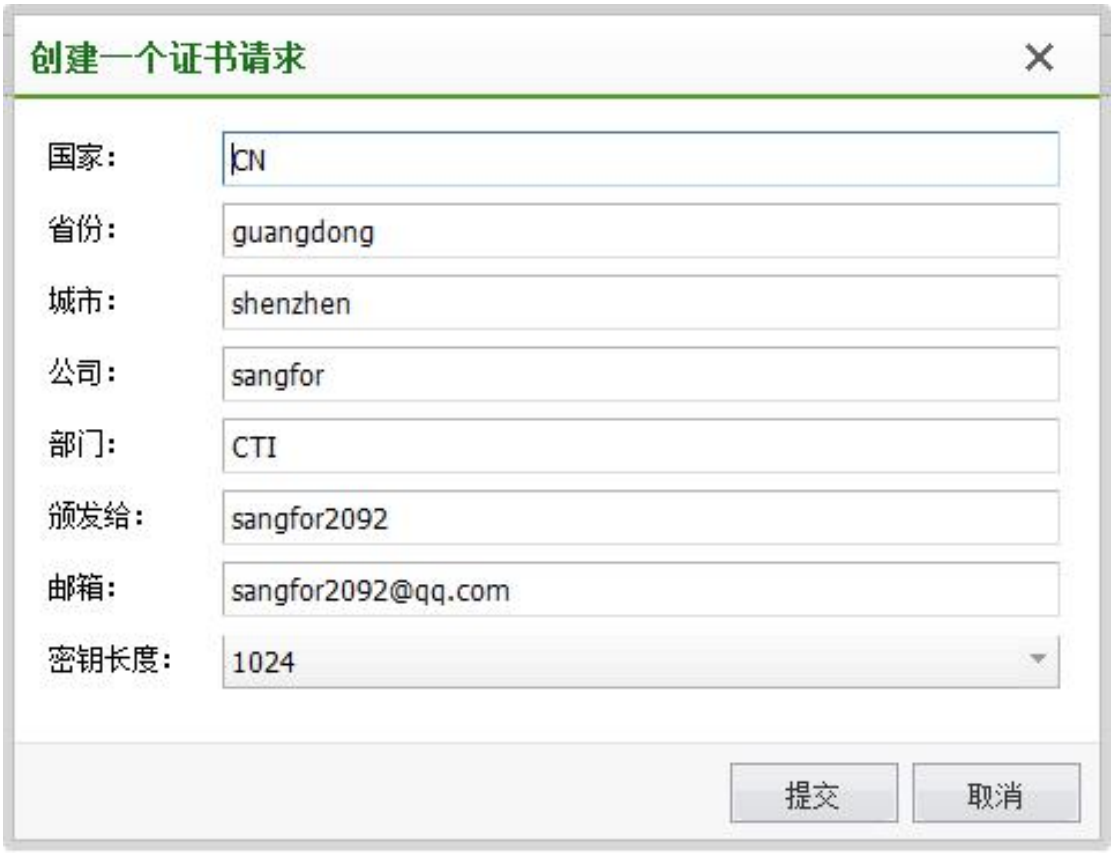
配置服务器证书，是为了让无线终端用户反向认证服务器是否合法，可以配置服务器证书，服务器证书可以通过 2 种方式生成。【导入一张证书】和【创建一个证书请求】，如下图：

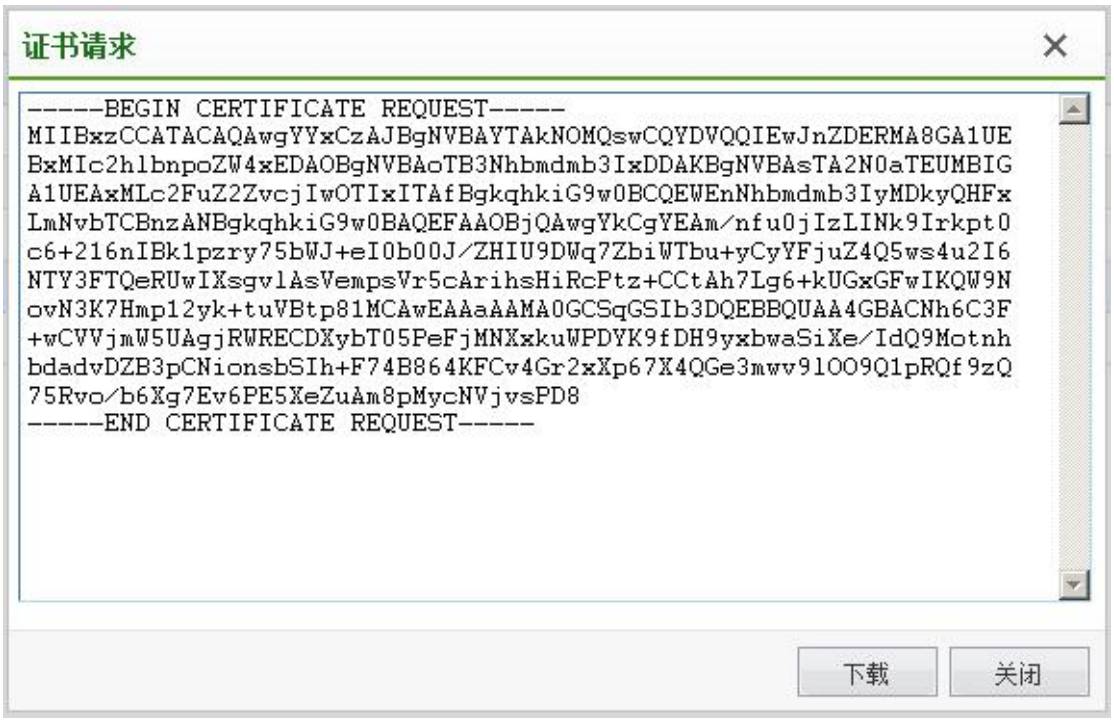


【导入一张证书】直接将已有的服务器证书的公钥私钥一起导入到设备里面。如果证书采用了密码，需要使用密码后，才可以正常导入。



【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

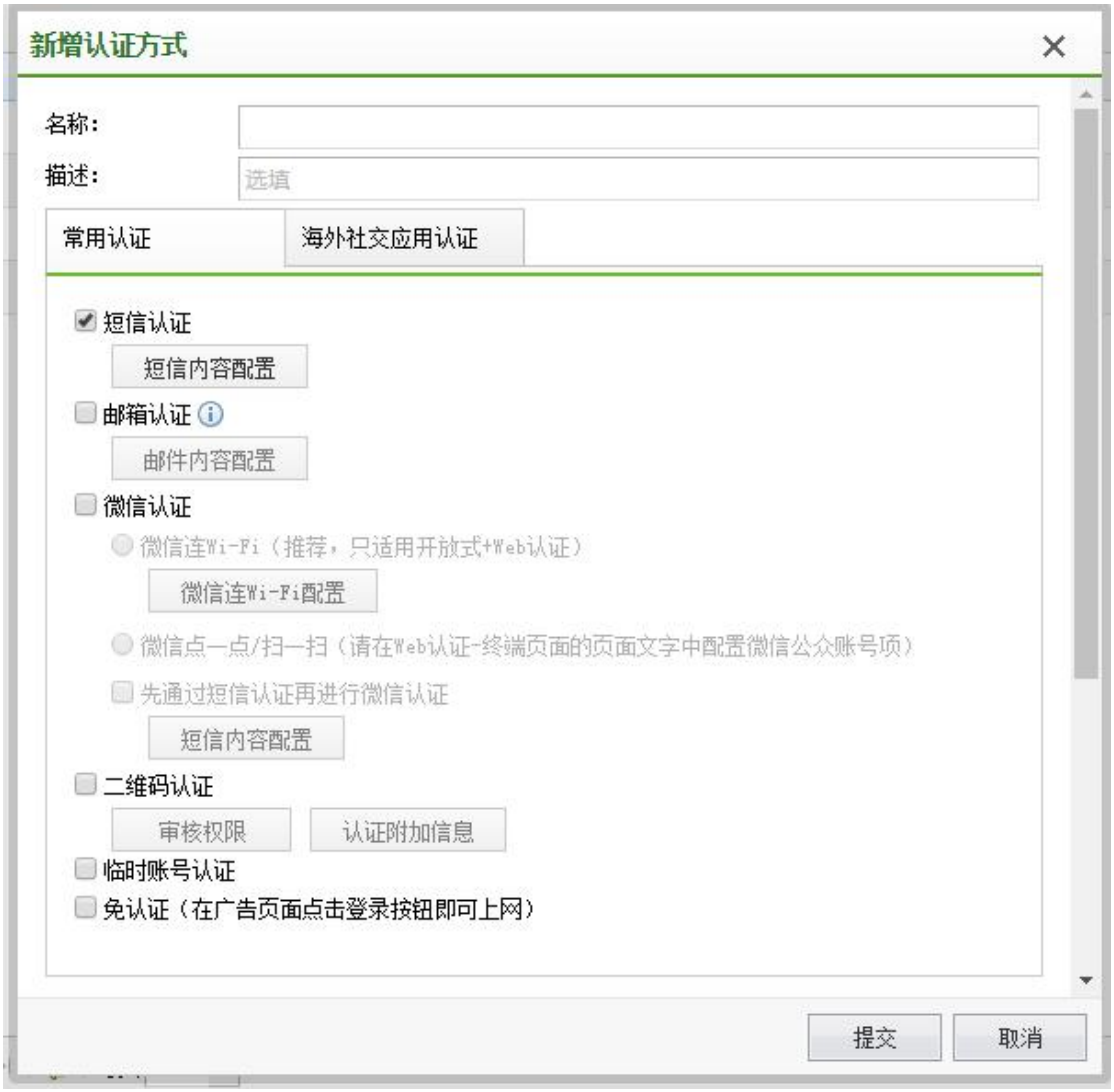
内置 CA 颁发证书：由内置颁发证书，填写用户信息，包括国家、省份、城市、公司、部门、颁发给、邮箱，可以设置由 NAC 内置 CA 中心颁发的服务器证书。对于不同的 SSID 认证，可以设置不同的服务器证书。初次使用内置 CA 颁发证书前，需要对内置 CA 进行初始化。

2.4.5. 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】五个模块

2.4.5.1. 访客认证

在部署用于访客使用的网络时，为了简化用户体验，通常设置为开放式的网络。但单纯的开放式的网络，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。



2.4.5.1.1. 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，才能访问网络，此方式获取了访客用户的手机号码作为身份信息。

2.4.5.1.2. 邮箱认证

邮箱认证是指访问网络时，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，才能访问网络，此方式获取了访客用户的邮箱地址作为身份信息。

2.4.5.1.3. 二维码认证

此方式通常用于企业的访客网络认证，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，访客可以访问网络的时长。

2.4.5.1.4. 临时访客认证

此方式通常用于企业、酒店的访客网络认证，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网络认证。

2.4.5.1.5. 免用户认证

免用户认证是指访问网络时，访客无需认证，在广告页面点击登录按钮即可上网。

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。

2.4.5.1.6. 社交应用认证

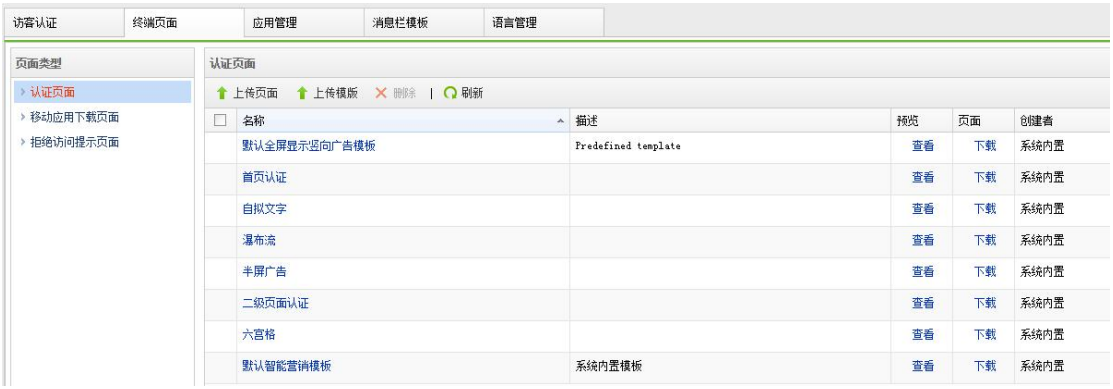
此方式通常用于海外或港澳台等地区，终端用户可以使用 Facebook，Twitter，Line，Live，Instagram 账号进行授权，授权后关注商家账号即可通过认证。

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。

2.4.5.2. 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”。



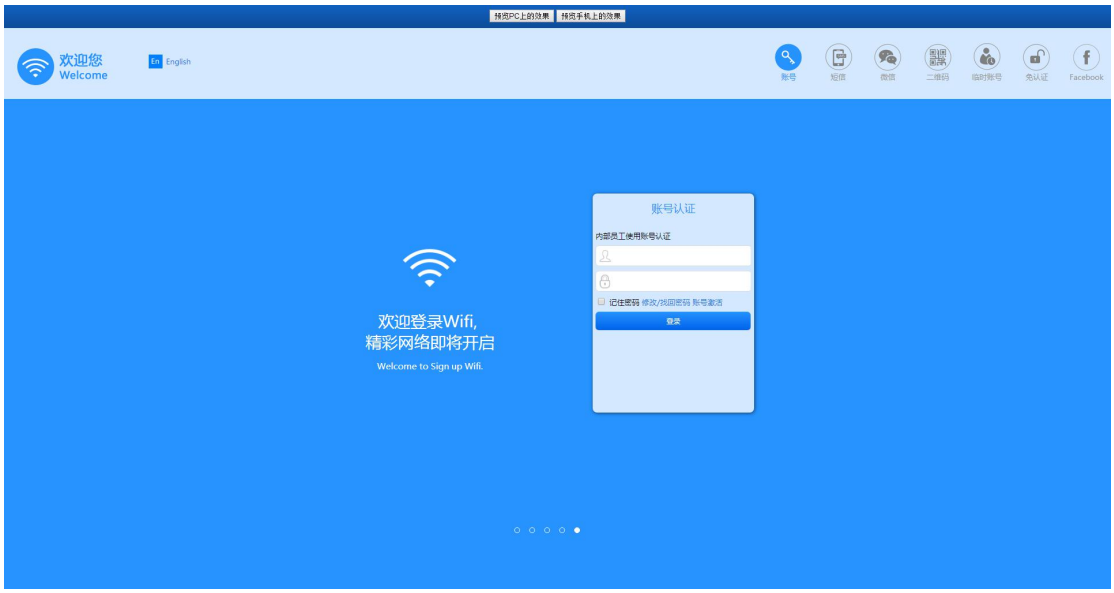
2.4.5.2.1. 认证页面

“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


编辑
名称:
默认全屏显示竖向广告模板
描述:
Predefined template
页面标题:
认证页面
营销管理员权限:
选填
页面显示效果
LOGO:
欢迎您
Welcome
上传
默认
支持格式有png，jpeg，jpg，gif，推荐尺寸230*82
二维码内部图标:
文件上传(*.jpg,*.png,*
浏览…
清空
认证区透明度:
80
%
页面文字:
编辑
免责声明:
编辑
默认语言:
中文
广告展示效果
广告来源:
播放广告图片
外部网页
添加
删除
上移
下移
序号
图片描述
链接地址
编辑

预览电脑认证效果图：



预览手机认证效果图：

2、自拟文字


编辑
名称:
自拟文字
描述:
选填
浏览器页面标题:
选填
营销管理员权限:
选填
页面显示效果
LOGO:
欢迎您
Welcome
上传
默认
背景颜色:
#CCFFFF
选择
默认语言:
中文
页面文字:
编辑
自拟文字:
编辑
二维码内部图标:
文件上传(*.jpg,*.png,*.gif)..
浏览...
清空
提交
取消

预览电脑认证效果图：

预览手机认证效果图：

3、瀑布流


编辑
名称:
瀑布流
描述:
选填
浏览器页面标题:
选填
营销管理员权限:
选填
页面显示效果
默认语言:
中文
页面文字:
编辑
免责声明:
编辑
二维码内部图标:
文件上传(*.jpg,*.png,*.gif)..
浏览...
清空
广告展示效果
图片轮播
瀑布流
Wi-Fi
基于网络
行为推广
提交
取消

预览电脑认证效果图：

预览手机认证效果图：

4、半屏广告


编辑
名称:
半屏广告
描述:
选填
浏览器页面标题:
选填
营销管理员权限:
选填
页面显示效果
默认语言:
中文
页面文字:
编辑
免责声明:
编辑
二维码内部图标:
文件上传(*.jpg,*.png,*.gif)..
浏览...
清空
广告展示效果
图片轮播
广告来源:
本地图片（多图时轮播）
广告图片:
添加
删除
上移
下移
序号
图片名称
链接地址
编辑
1
-
提交
取消

预览电脑认证效果图：

预览手机认证效果图：

5、二级页面认证


编辑
名称:
二级页面认证
描述:
选填
浏览器页面标题:
选填
营销管理员权限:
选填
页面显示效果
默认语言:
中文
页面文字:
编辑
免责声明:
编辑
二维码内部图标:
文件上传(*.jpg,*.png,*.gif)..
浏览...
清空
广告展示效果
图片轮播
广告来源:
本地图片（多图时轮播）
广告图片:
添加
删除
上移
下移
序号
图片名称
链接地址
编辑
1
-
提交
取消

预览电脑认证效果图：

预览手机认证效果图：

6、六宫格


编辑
二维码内部图标：
文件上传(*.jpg,*.png,*.gif)..
浏览…
清空
广告展示效果
图片轮播
六宫格
无线防钓鱼
营销推广
防终端拖滞
基于行为推广
终端类型识别
统一认证平台
提交
取消

预览电脑认证效果图：

预览手机认证效果图：

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。

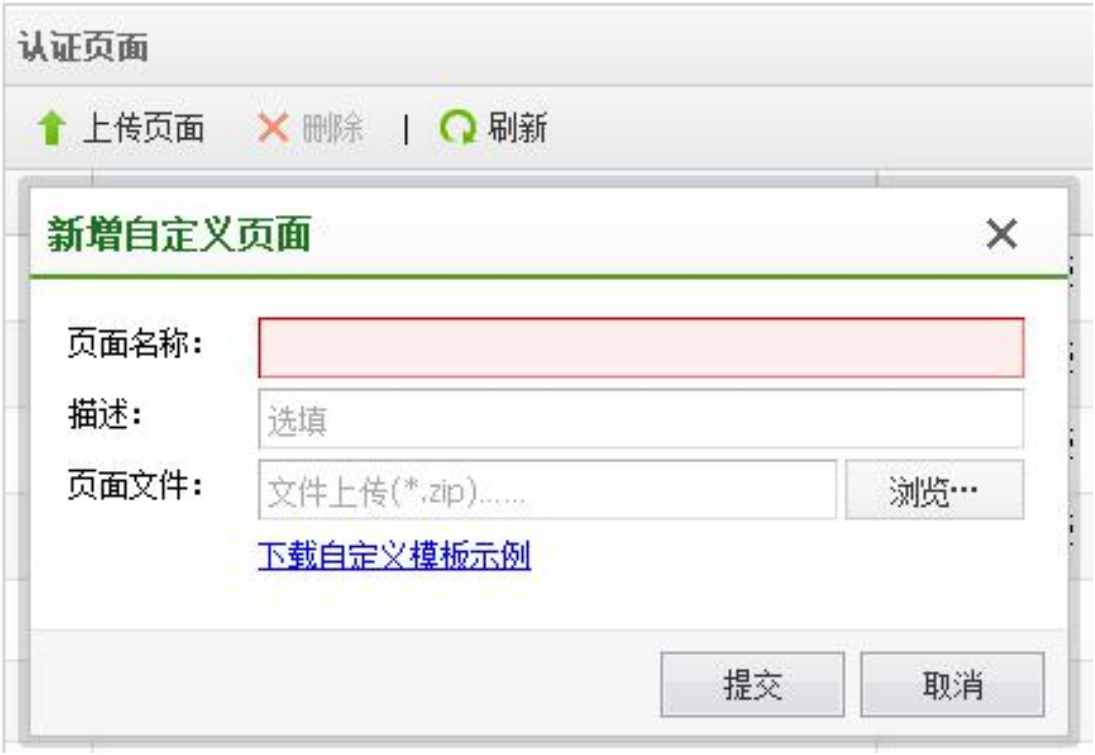
统一配置：在总部、多个门店场景下，可以启用统一配置，用于在指定生效时间内强制展示总部设定的广告内容，若部分门店不展示总部统一广告可以进行排除。

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”。

2.4.5.2.2. 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



2.4.5.2.3. 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。

2.4.5.2.4. 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。

2.4.5.3. 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。

2.4.5.4. 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。

2.4.5.5. 语言模版

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。

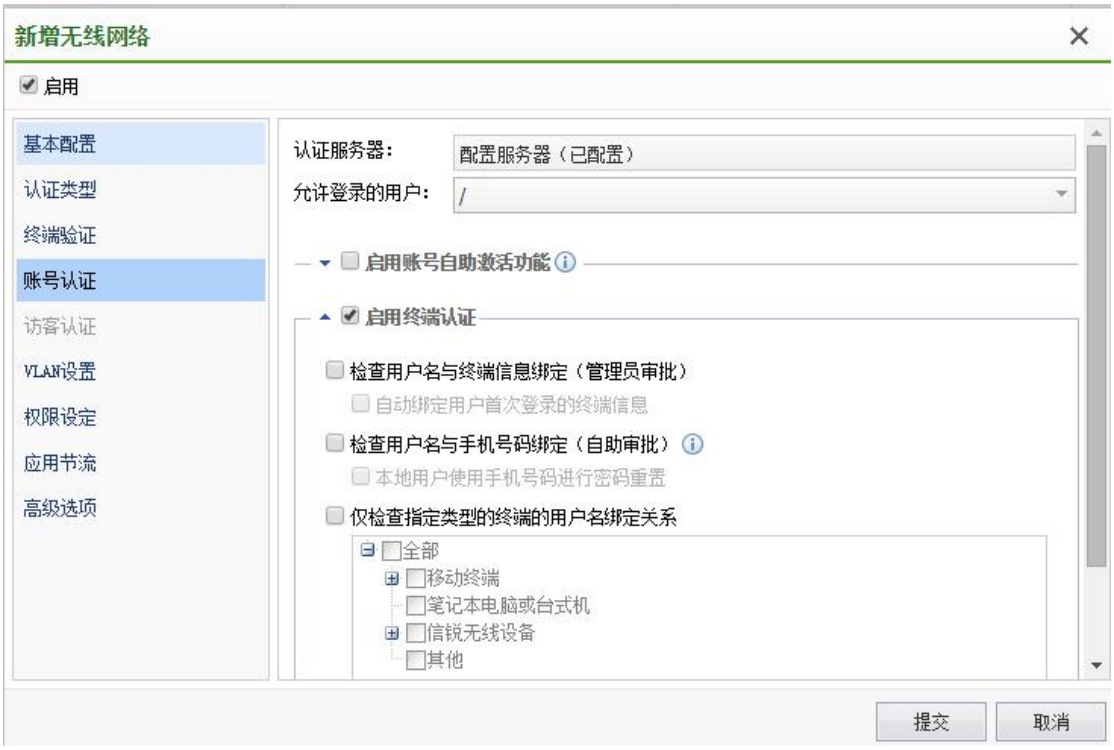
在添加其他国家或者区域的语言前，需要先下载英文模板，然后在英文模板的 json 中，将对应的英文内容修改为需要展示的语言内容。

2.4.6. 用户终端绑定

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。支持“终端绑定”、“手机号码绑定”、“手机号码绑定、终端绑定”。

此页面中仅定义了用户终端的绑定关系，要启用绑定关系检查功能，还需要在【接入点配置】-【无线网络】-【编辑无线网络】-【账号认证】中勾选【启用终端认证】并且勾选【检查用户名与终端信息绑定】或【检查用户名与手机号码绑定】。

一个用户，最多支持绑定在 5 个 MAC 地址上，一个 MAC 可以绑定的用户名个数不受限制。用户名和 MAC 地址绑定都是双向绑定的关系。



用户终端绑定关系，可以通过以下几种方式创建：

1、手动添加：管理员通过手动添加或者 csv 表格文件导入方式，提供用户名与 终端信息的绑定关系。在有大量终端需要管理的环境中，这种方式的缺点是较大的管理工作量。

2、自动添加：无线网络中，可以设置为：用户第一次登录时，自动绑定登录的终端。此方式以牺牲少量的安全性作为代价，减少了管理工作量。

3、管理员审批：对于未授权终端上的登录请求，系统会拒绝此用户连接，并且把终端的信息加入到待审批列表中，网络管理员以人工审批的方式，来决定是否允许此未终端接入。

2.4.7. 外部服务器

『外部服务器』包括【认证服务器】、【虚拟服务器】

2.4.7.1. 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。

2.4.7.1.1. 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：

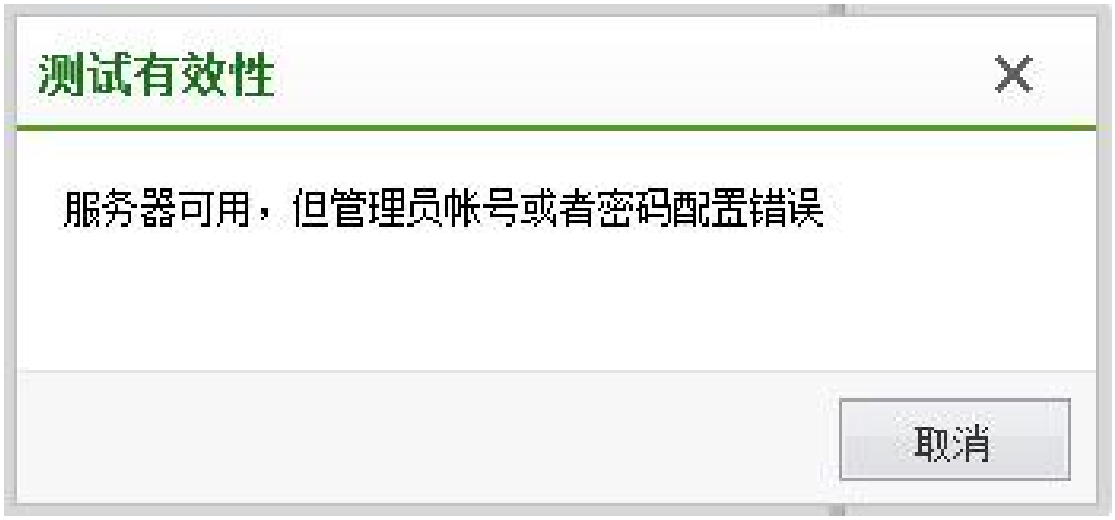
设置 Radius 服务器的时候可以另外设置获“取用户属性”，企业级认证时，NAC 会去用户数据库中去获取用户的组织结构，来作为无线终端的用户名和组织结构。这里可以选择与 radius 服务器对应的 LDAP 服务器。

2.4.7.1.2. 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：



2.4.7.1.3. 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

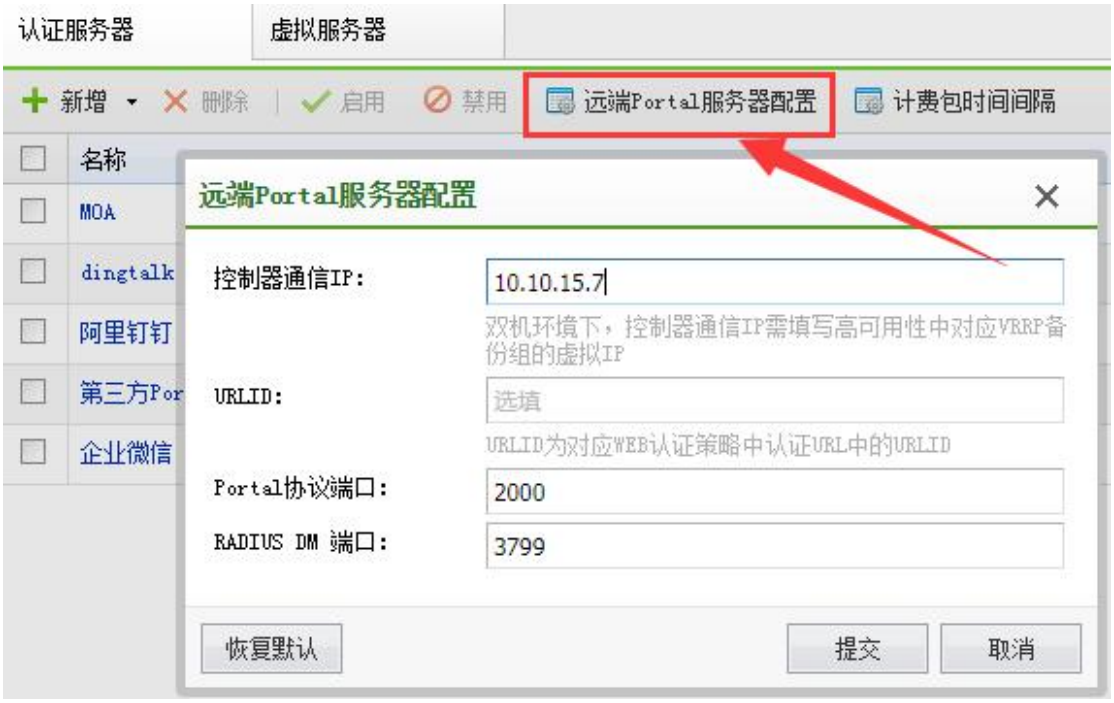
协议：

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。

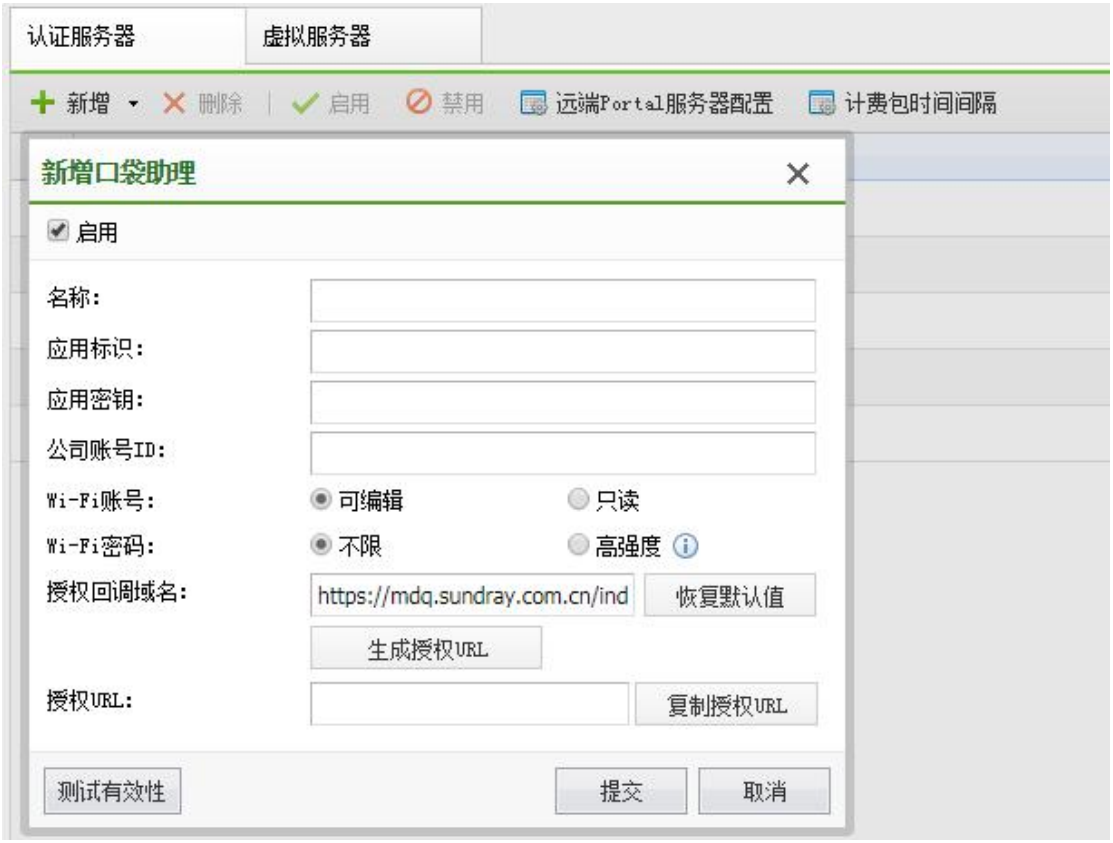
Portal 协议端口：客户端监听的 Portal 服务端口。

RADIUS DM 端口：RADIUS 服务器主动下线一个用户时，使用的端口。

2.4.7.1.4. 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。

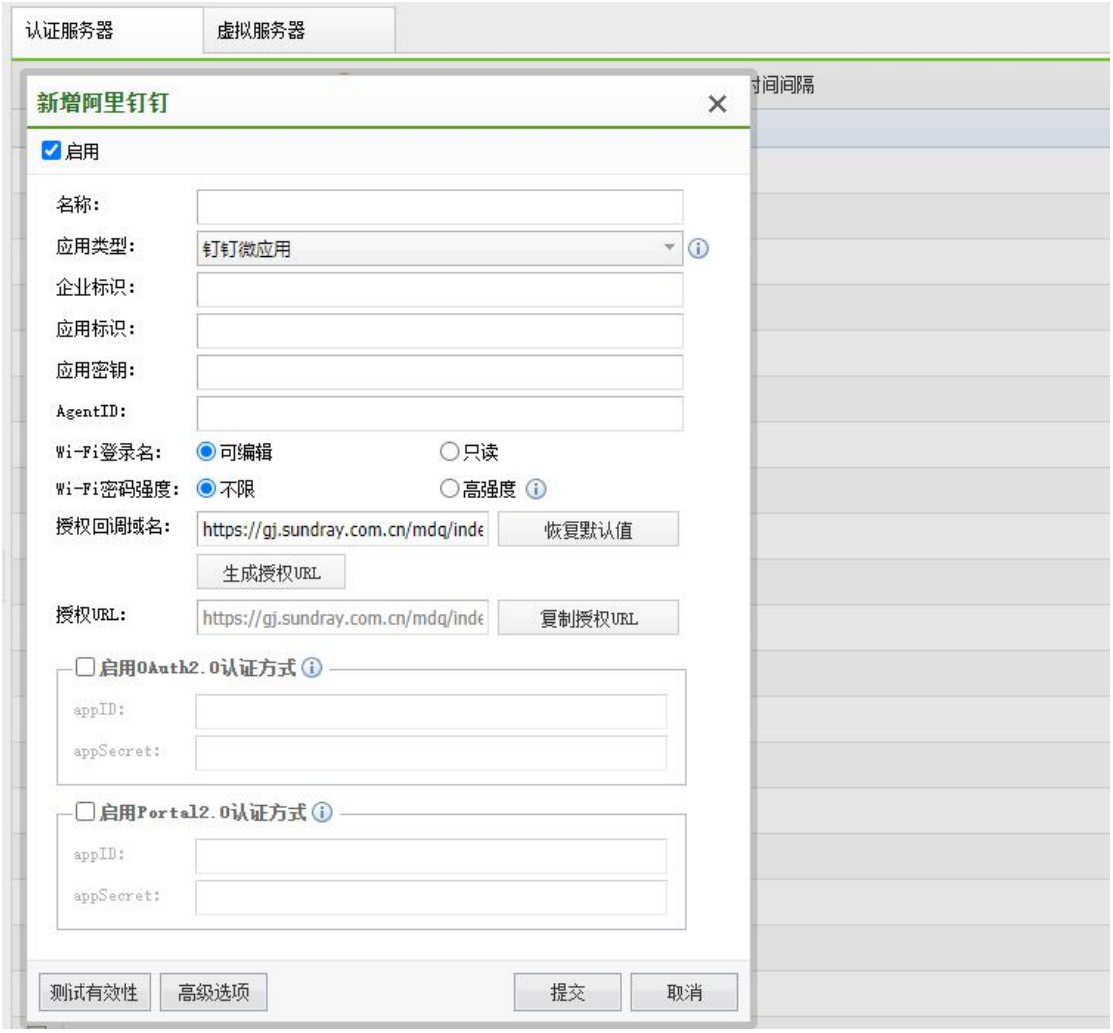
适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



2.4.7.1.5. 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。

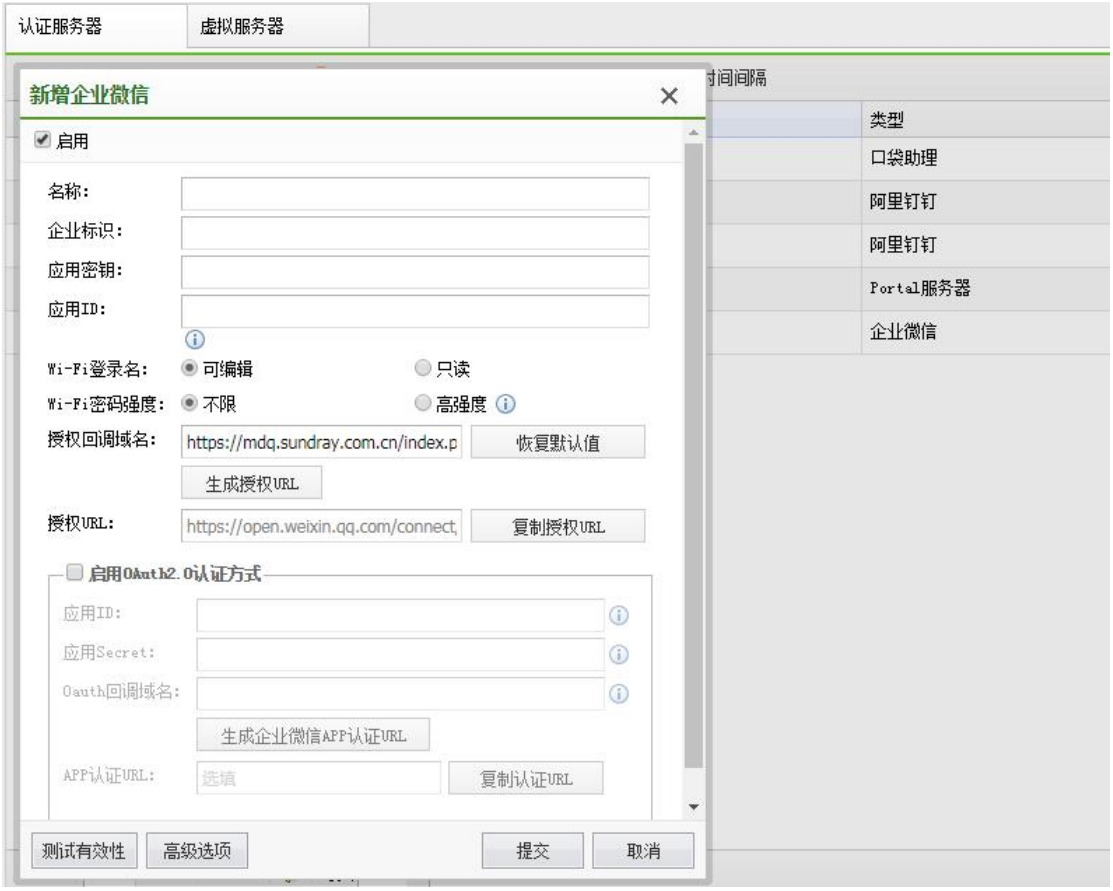
适用认证方式：1）WPA/WPA2 企业认证； 2）WEB 认证 - 账号认证



2.4.7.1.6. 微信企业号

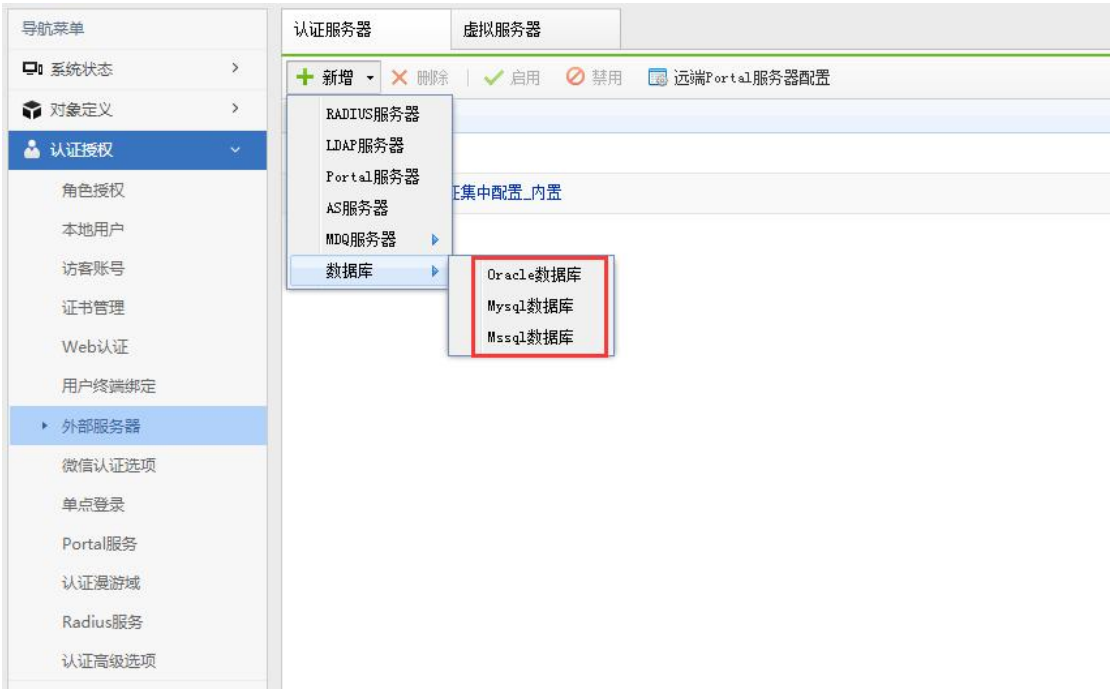
微信企业号认证是指将微信企业号移动办公平台作为认证服务器，用户通过使用微信企业号上创建的上网账号完成认证，实现无线上网账号与微信企业号的对接，便于使用微信企业号办公的用户对无线上网账号进行实时管理。

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



2.4.7.1.7. 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。

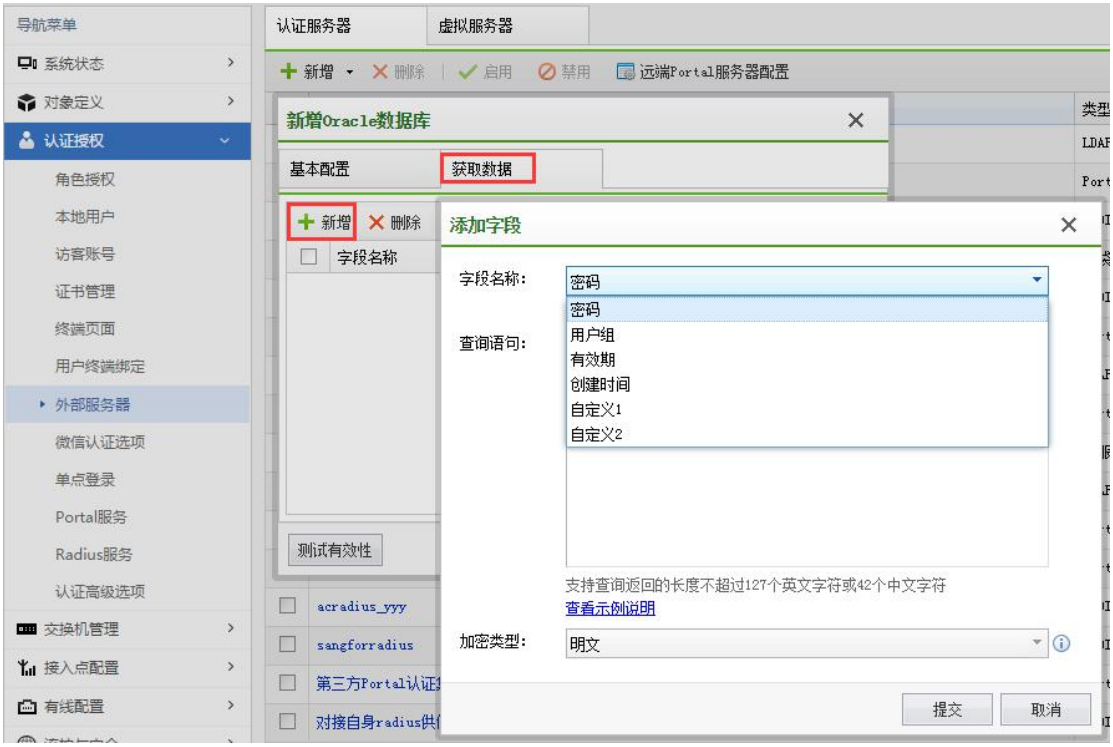
（6）管理员帐号：登录数据库的账号，该账号需要有查询“数据库名”指定的数据库的权限。

（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：

a、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：

a、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

),

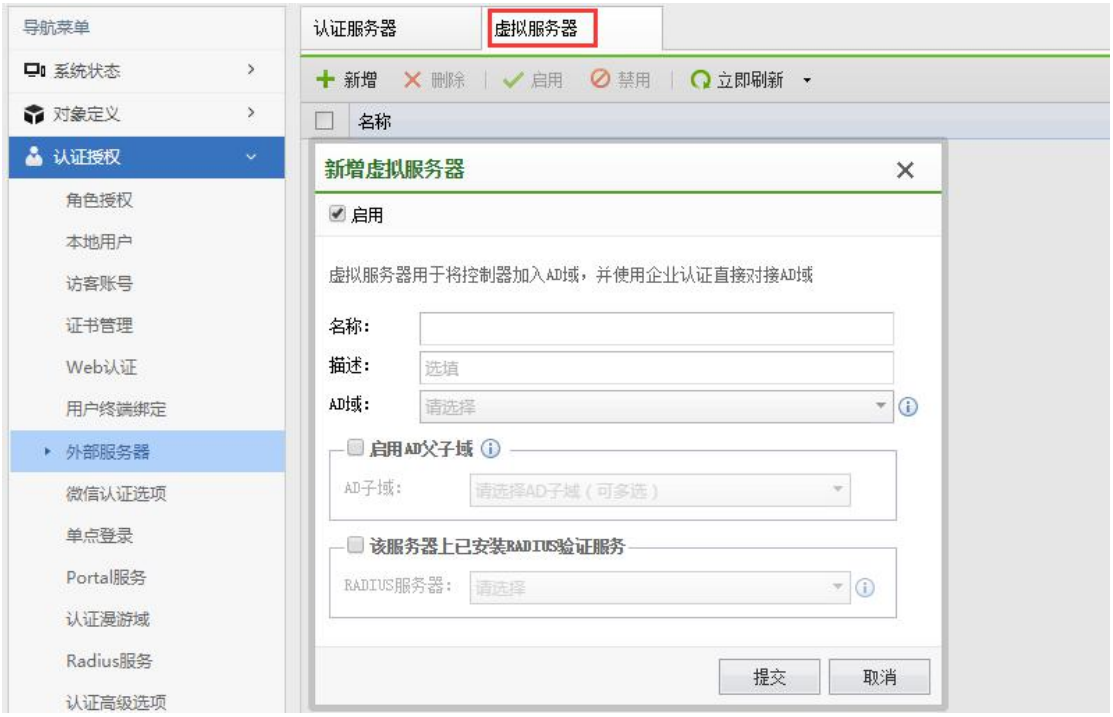
)LEN(用户名字段名)

) = $$USERNAME$$

2.4.7.2. 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。



2.4.7.2.1. 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

2.4.7.2.2. 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

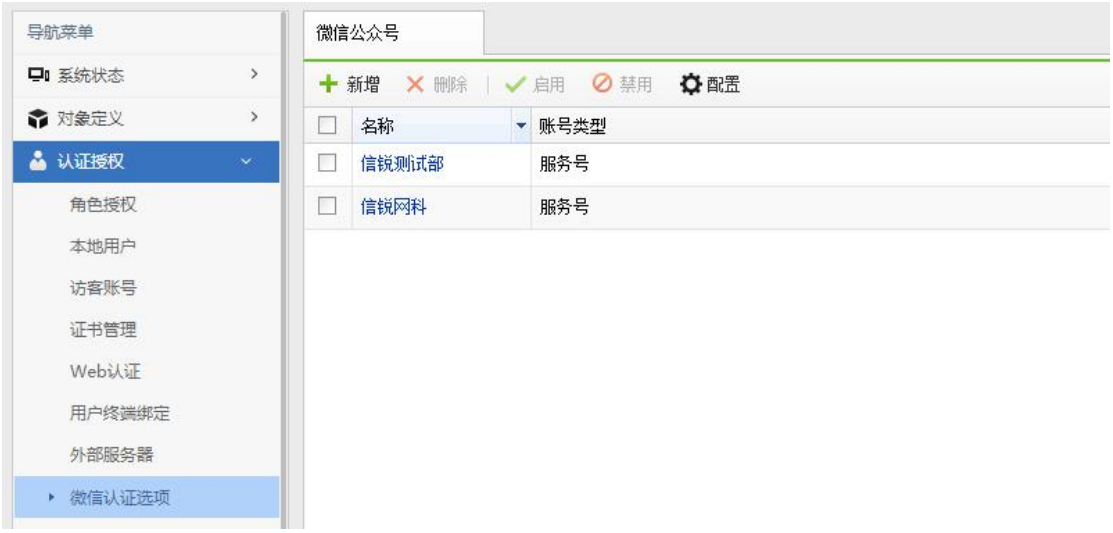
AD 域：选择 AD 域服务器配置(可为父域或独立域)

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

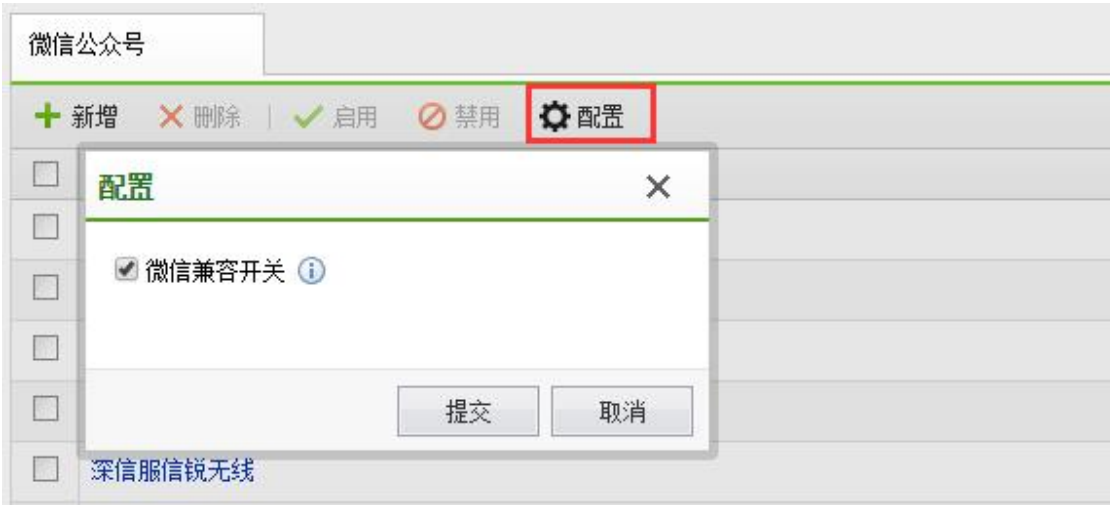
RADIUS 服务器：选择已在配置的 AD 域中注册 RADIUS 服务器

2.4.8. 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。

2.4.8.1. 微信推广功能

推广功能需要微信公众账号类型为服务号，且账号处于开发者模式。推广功能使用注意事项：

A、微信公众平台默认仅对保持关注且 48 小时内与公众平台有任何主动联系业务的用户才提供主动推广消息业务，超过这个限制用户将无法接收该消息；

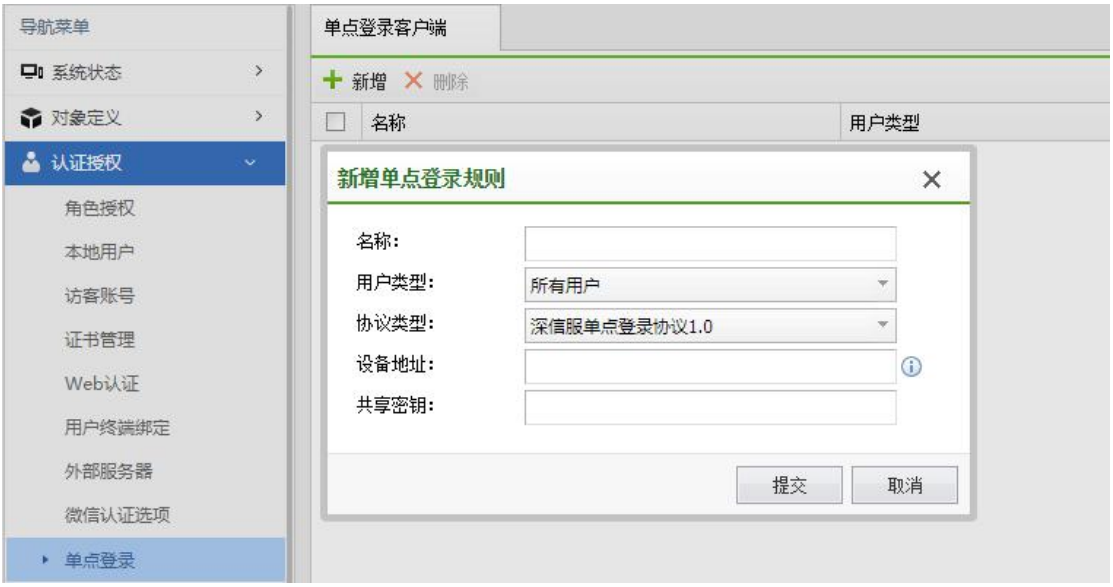
B、使用本功能请确认使用的第三方公众平台不会使用高级接口 access token,或者对应的第三方公众平台可以提供 access token 获取功能，否则将造成 access token 快速耗尽，导致本功能或者第三方公众平台异常（比如：微盟、微购等）。

2.4.9. 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。



2.4.9.1. 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。

2.4.9.2. 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：

2.4.10. 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。

2.4.10.1. 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。

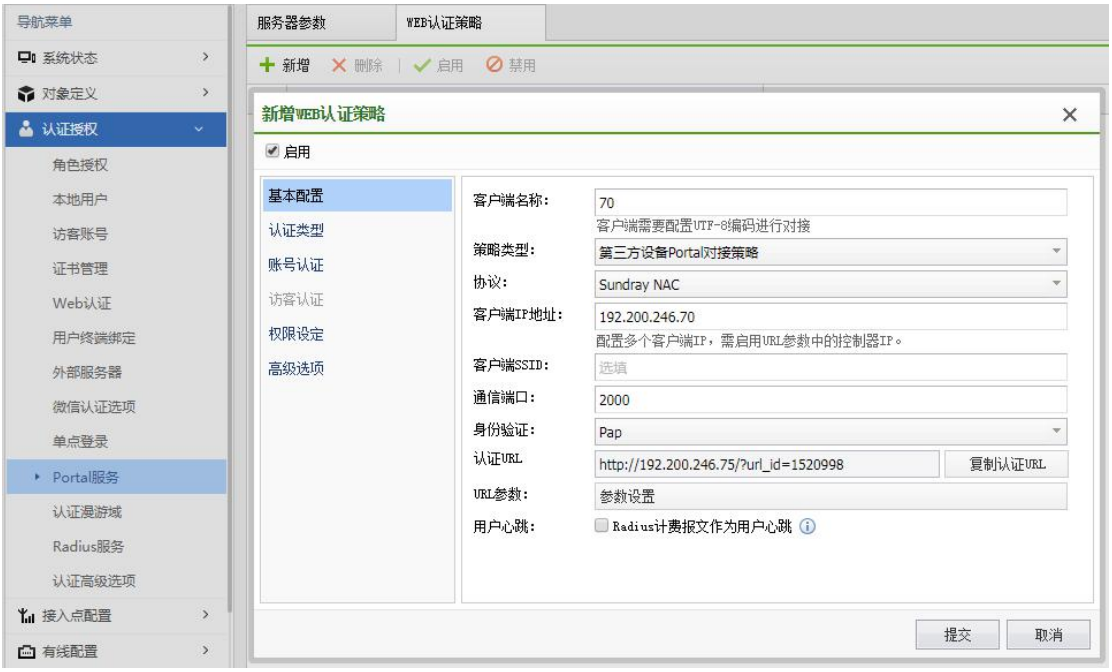
在线用户保留时间（小时）：超过保留时间，注销所有的在线用户。

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.

2.4.10.2. 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：分为第三方设备 Portal 对接策略和控制器有线认证策略。第三方设备 Portal 对接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。

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。

2.4.11. 认证漫游域

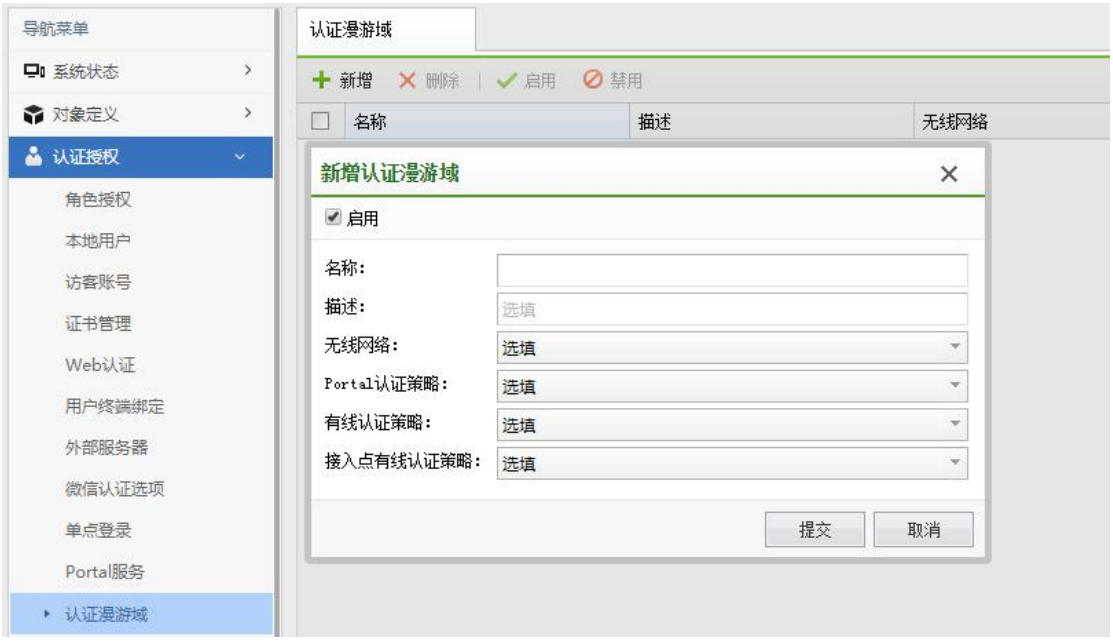
认证漫游域主要解决如下问题：

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。

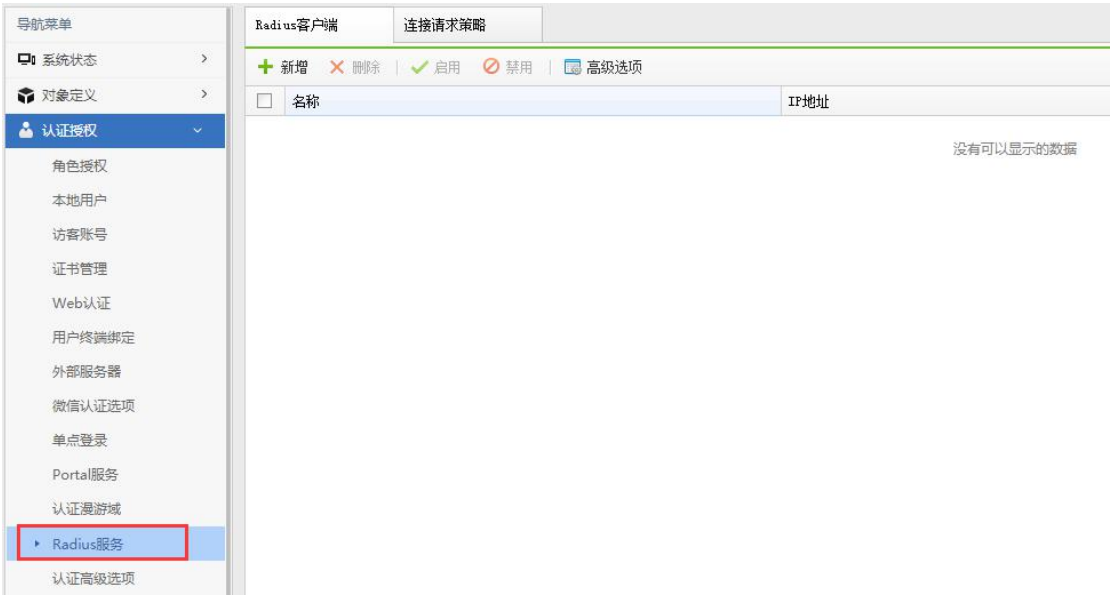
配置认证漫游域后，支持终端在不同类型的 portal 服务器上漫游；支持不同类型认证方式之间的漫游。

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。



2.4.12. Radius 服务

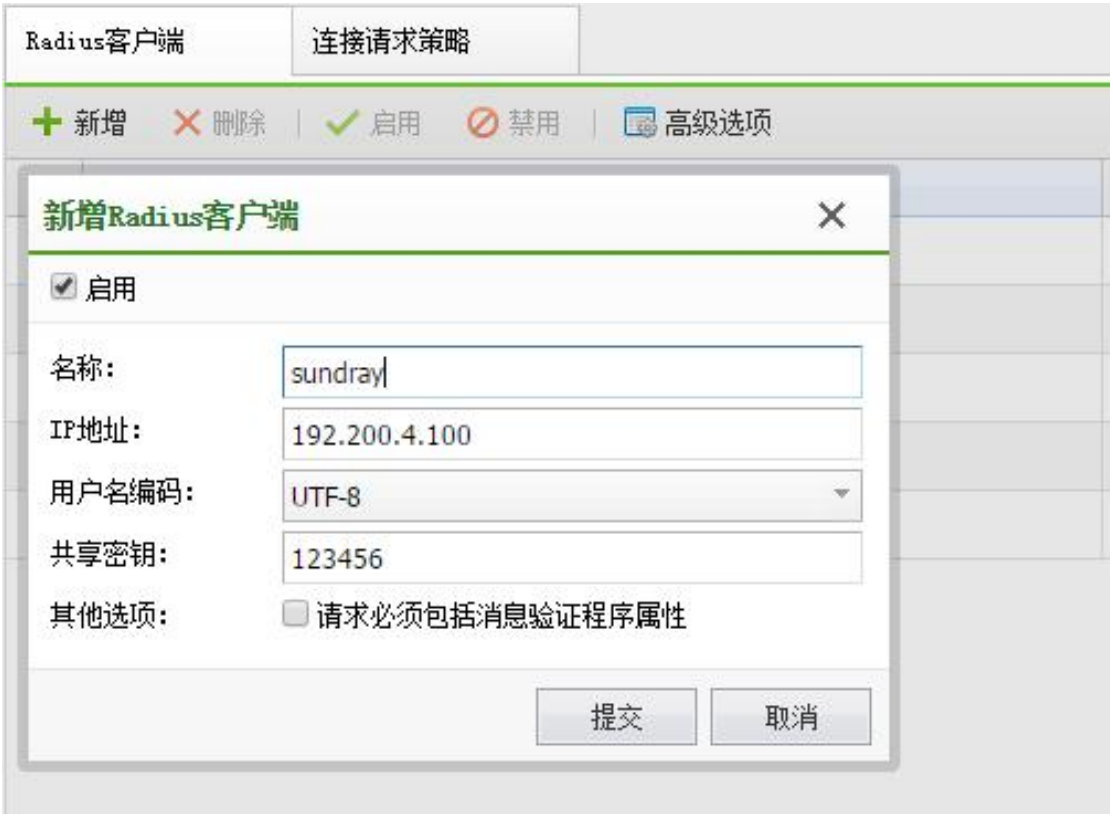
Radius 服务器负责接收客户端的连接请求、认证用户，然后返回客户端所有必要的配置和认证信息。



2.4.12.1. 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

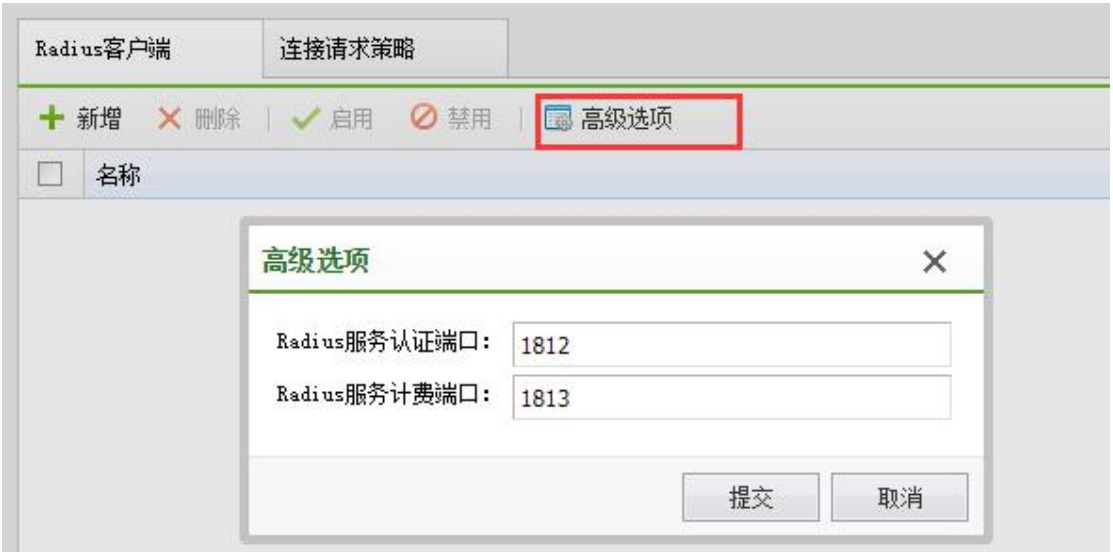
客户端和服务通过该共享密钥建立信任，两端密钥一致才可以建立信任。

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。

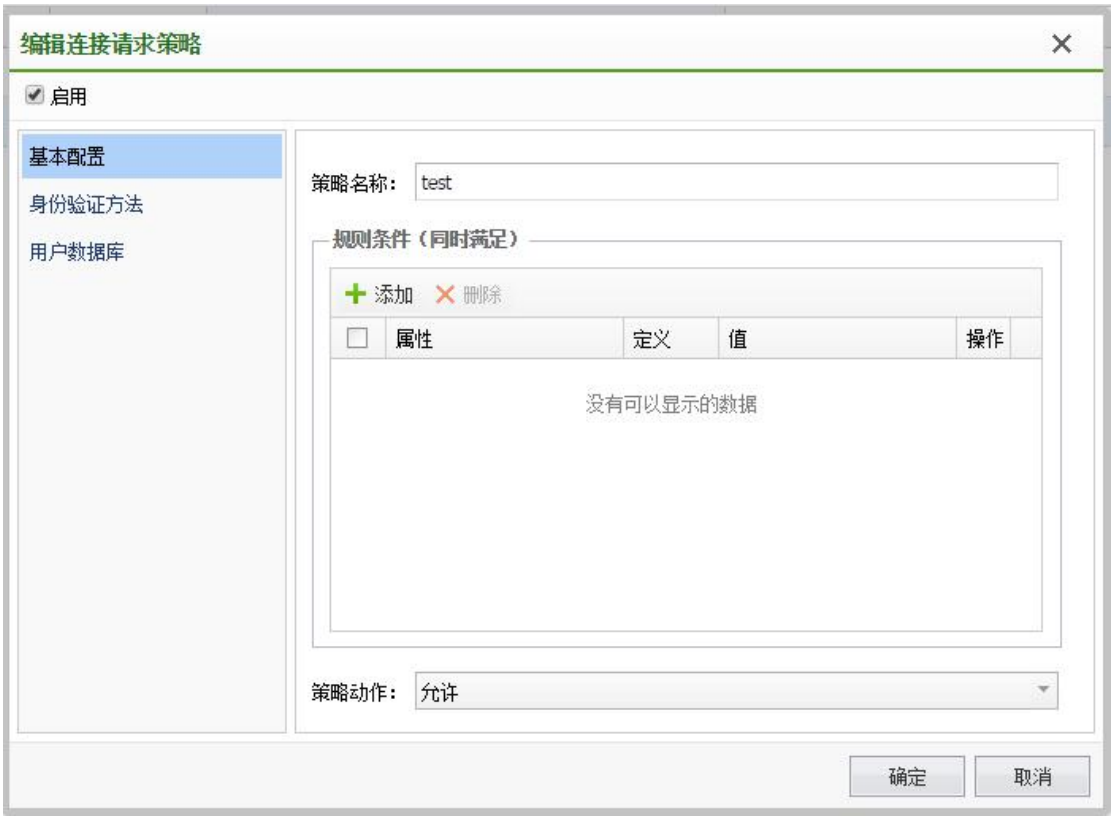
6、高级选项

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。



2.4.12.2. 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。

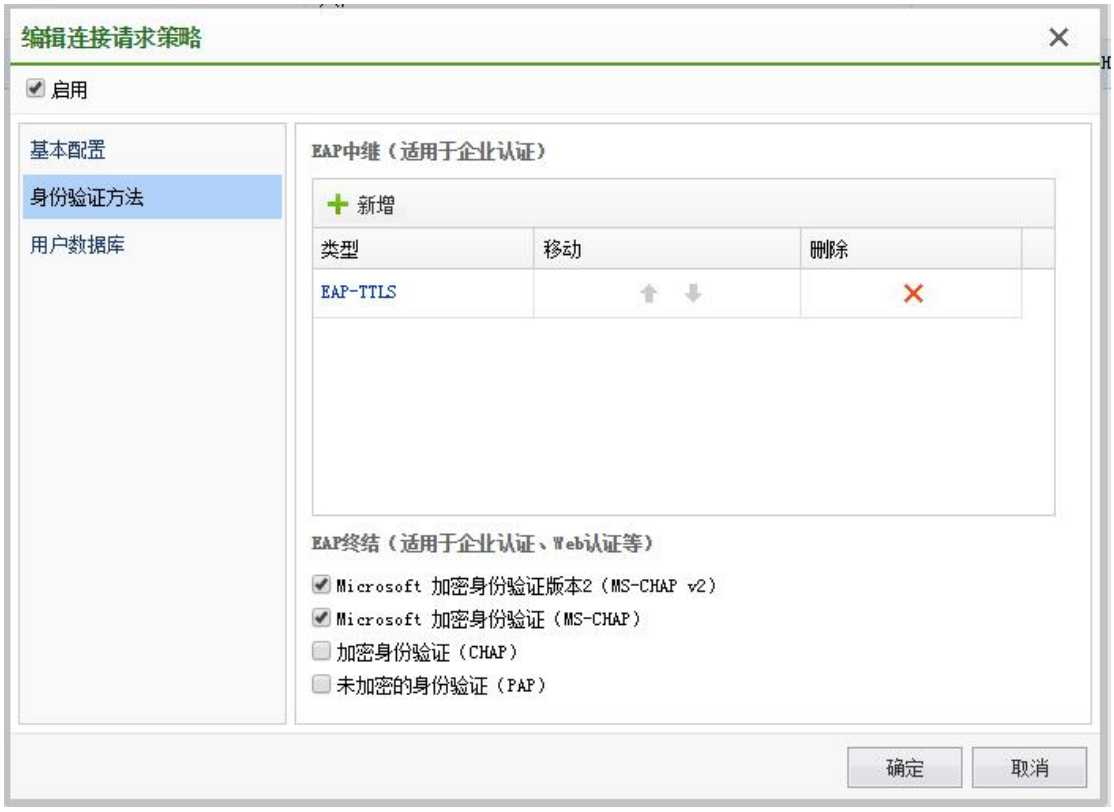


1、规则条件

通过传输 Radius 属性的值进行匹配。

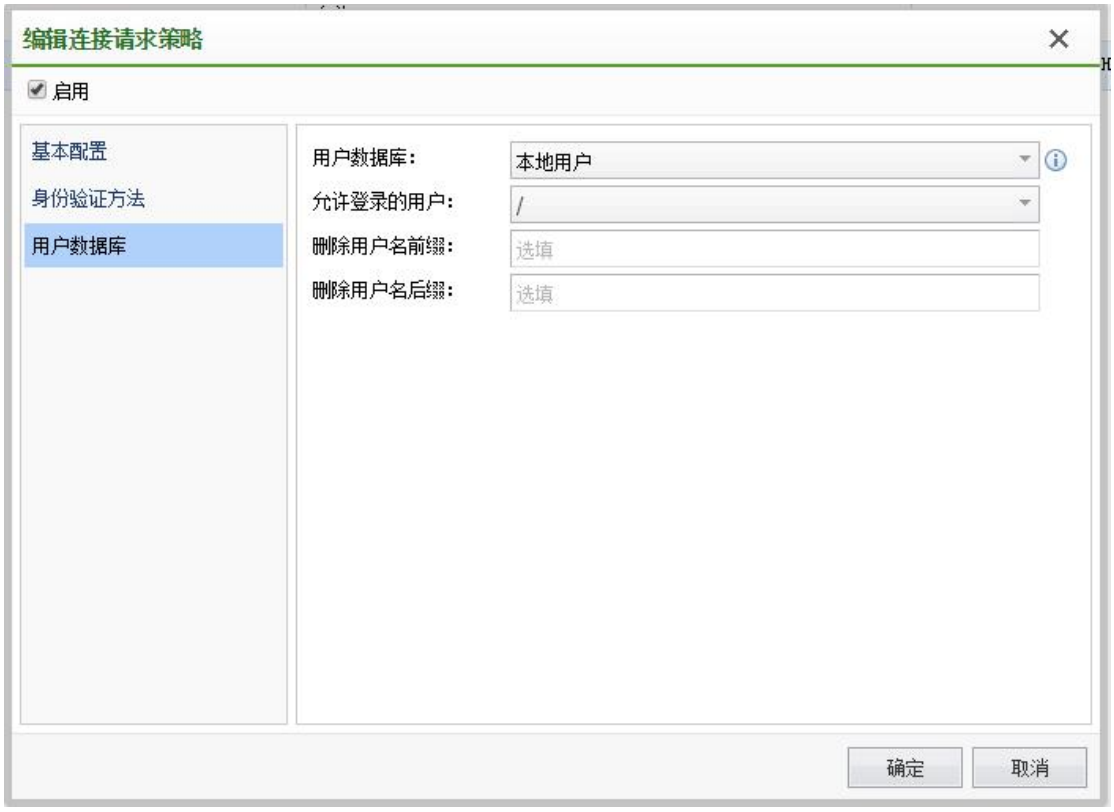
2、策略动作

允许或者拒绝匹配该策略的用户通过认证。



1、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。



1、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）。

2、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。

2.4.13. 认证高级选项

2.4.13.1. WEB 认证通用配置

1、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。

2、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。

3、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。

4、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：

5.1 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；

5.2 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。

5、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。

6、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。

7、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

8、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

9、认证前角色：

10.1 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；

10.2 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。

2.4.13.2. 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。

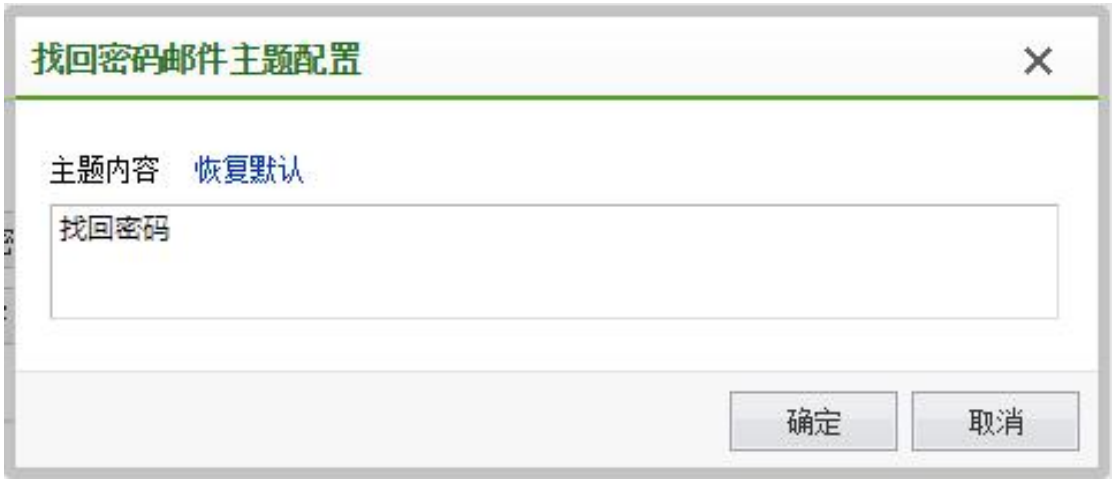
2.4.13.3. 生物识别认证选项

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。

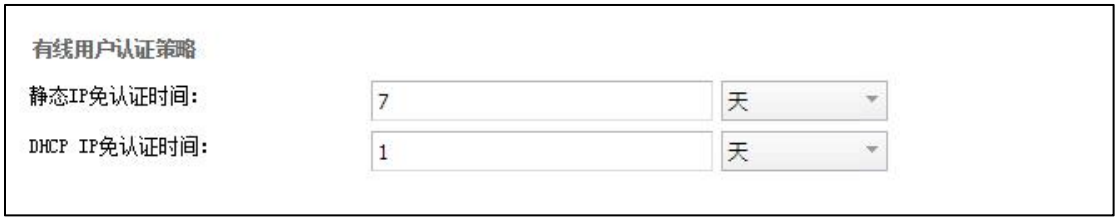
2.4.13.4. 模板内容配置

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。



2.4.13.5. 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。

2.4.13.6. 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。

2.5. 交换机管理

『交换机管理』包括【交换机】、【端口列表】、【供电配置】、【有线认证】这 4 个菜单选项；

交换机的发现和激活和无线接入点方式类似，具体方法请参照 无线接入点。

控制器管理交换机，目前支持的交换机型号有：CAP-5128、RS3300-28T-4F、RS3300-52T-4F 、 RS3320-12M-LI 、 RS3320-12M-PWR-LI 、 RS3320-28M-PWR-LI 、RS3320-28M-4MT-PWR-LI 、 RS5300-28T-4F 、 RS5300-52T-4F 、 RS5300-28X-PWR-SI 、RS5300-52X-PWR-SI、RS5300-28X-SI-24S、RS5300-28X-EI-24S、RS-6300-26Q-EI-24X、RS-6300-50Q-EI-24X、RS6300-24X-LI-12X、RS6300-24X-LI-15X、RS6500-54Q-EI-48X，激活交换机还需要控制器有对应交换机管理序列号。

2.5.1. 交换机

『交换机』包括了【发现新交换机】和【交换机管理】。

2.5.1.1. 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 NAC，当交换机第一次发现 NAC 时，会在 NAC 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：

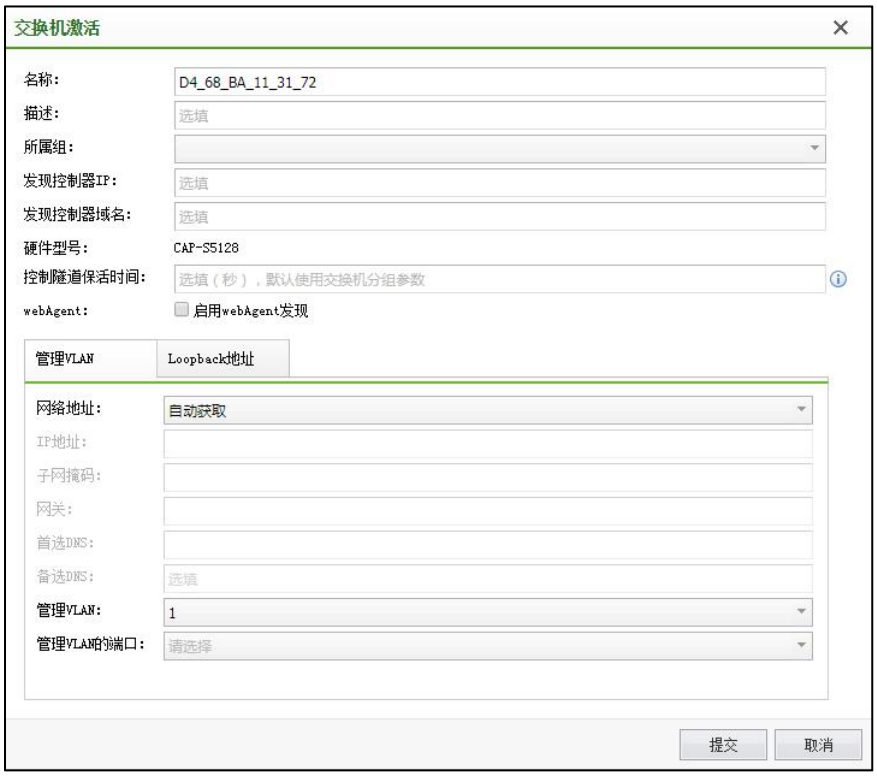
1.射频交换机

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。

发现控制器 IP：填写交换机用于连接的 NAC 的 IP 地址，如果给交换机填写了 NAC 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

发现控制器域名：用于交换机自动发现 NAC 用，当交换机解析到该域名时，交换机会自动向 NAC 请求连接。NAC 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 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 NAC 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。

2.5.1.2. 设备替换

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：

1．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。

2．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。

射频序列号：填写对应设备的射频序列号。

网络地址：填写新设备的 IP 地址。

替换设备：选择要替换的交换机。

旧设备处理：选择重新激活/删除设备。

2.5.1.3. 交换机

对所有交换机进行全部集中分组和管理，包括配置所属组、发现控制器 IP、发现控制器域名、隧道参数、webagent、管理 vlan 和管理 vlan 端口、管理地址。


交换机管理
发现新交换机
交换机分组
输入关键字搜索
所有区域
默认组
批量编辑
删除
导入
导出
替换
重启
名称、IP地址、MAC地址
名称
IP地址
MAC地址
描述
硬件型号
软件版本号
序列号
已选中所有页全部 1 项，取消勾选
A8_0C_CA_1F_04_14
自动获取
A8-0C-CA-1F-04-14
RS3300-28T-4F
SW1.2 BUILD2017120…
3C9577E8

批量修改如下图：


批量编辑交换机
所属组：
发现控制器IP：
发现控制器域名：
控制隧道保活时间：
12
webAgent：
启用webAgent发现
禁用webAgent发现
管理VLAN：
请选择管理VLAN
请选择管理VLAN的端口
管理地址：
手动配置
管理口
起始IP：
结束IP：
掩码：
网关：
首选DNS：
备选DNS：
选填
提交
取消

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。

发现控制器 IP：填写交换机用于连接的 NAC 的 IP 地址，如果给交换机填写了 NAC 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

发现控制器域名：用于交换机自动发现 NAC 用，当交换机解析到该域名时，交换机会自动向 NAC 请求连接。NAC 发现该交换机后，就可以对该交换机进行策略下发配置了。

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 进行申请开通。

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。

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 NAC 失去联系，所以一般设置交换机的 IP 地址为自动获取。

单独点击交换机，可以对单台交换机进行管理。

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。

发现控制器 IP：填写交换机用于连接的 NAC 的 IP 地址，如果给交换机填写了 NAC 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

发现控制器域名：用于交换机自动发现 NAC 用，当交换机解析到该域名时，交换机会自动向 NAC 请求连接。NAC 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 进行申请开通。

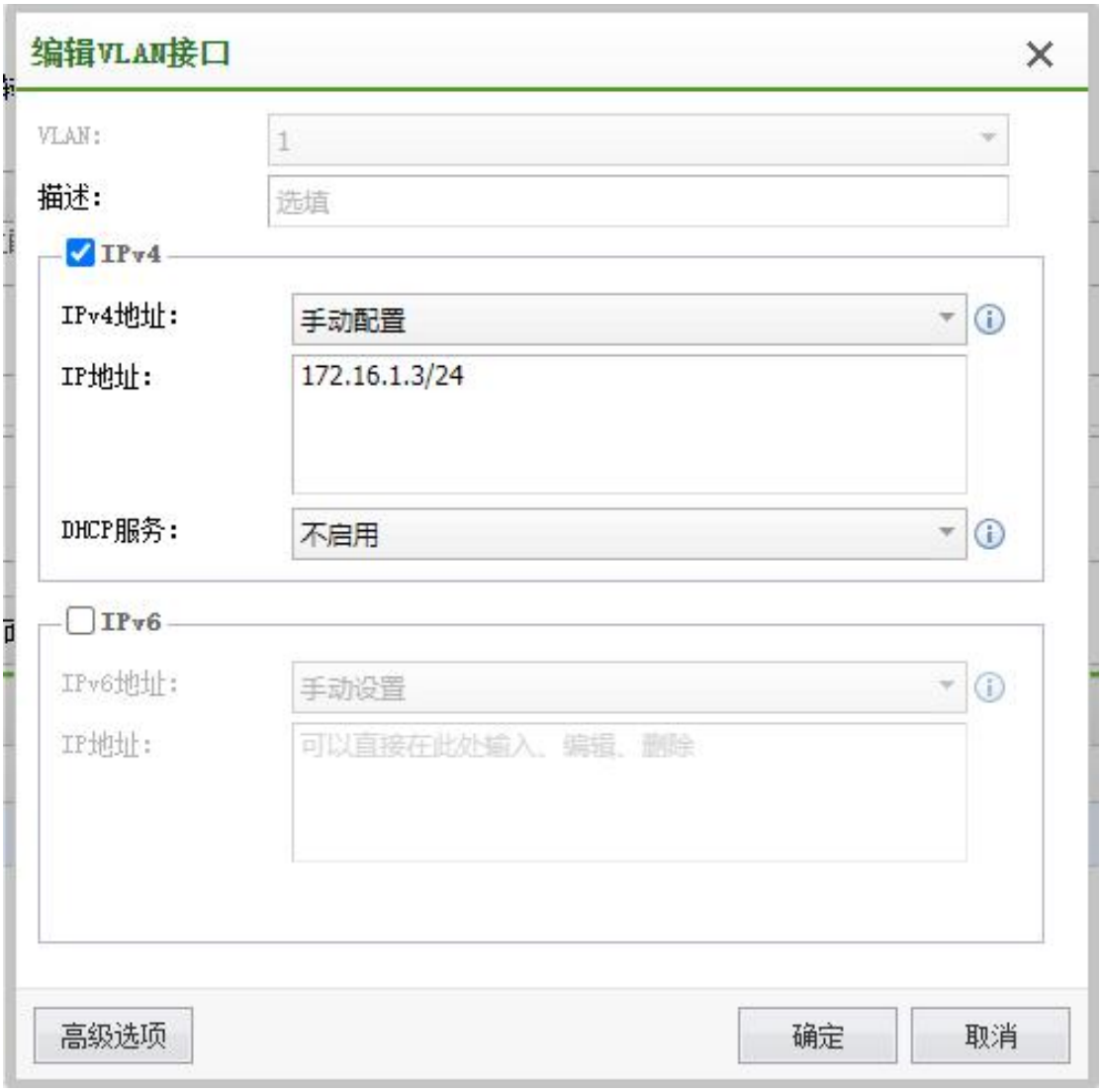
2.5.1.3.1. VLAN 接口

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。

点击**新增**，添加 VLAN 接口。



VLAN：选择新增的 VLAN 接口。

描述：对 VLAN 接口的描述。

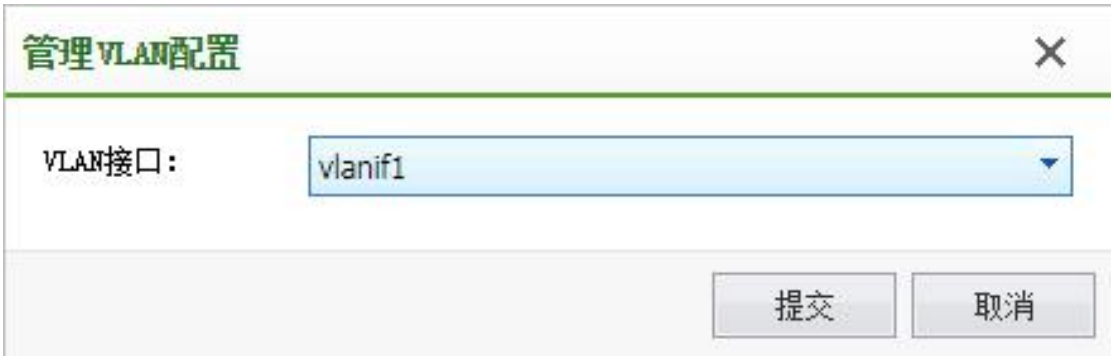
网络地址：可以选择自动获取或者手动配置。

IP 地址：在选择手动配置时填写的 IP 地址。

DHCP 服务：在静态 IP 时，VLAN 接口下可以开启 DHCP 服务功能。

MTU：默认 1500，支持范围 576~9174。

点击**管理 VLAN 配置**，修改交换机的管理 vlan

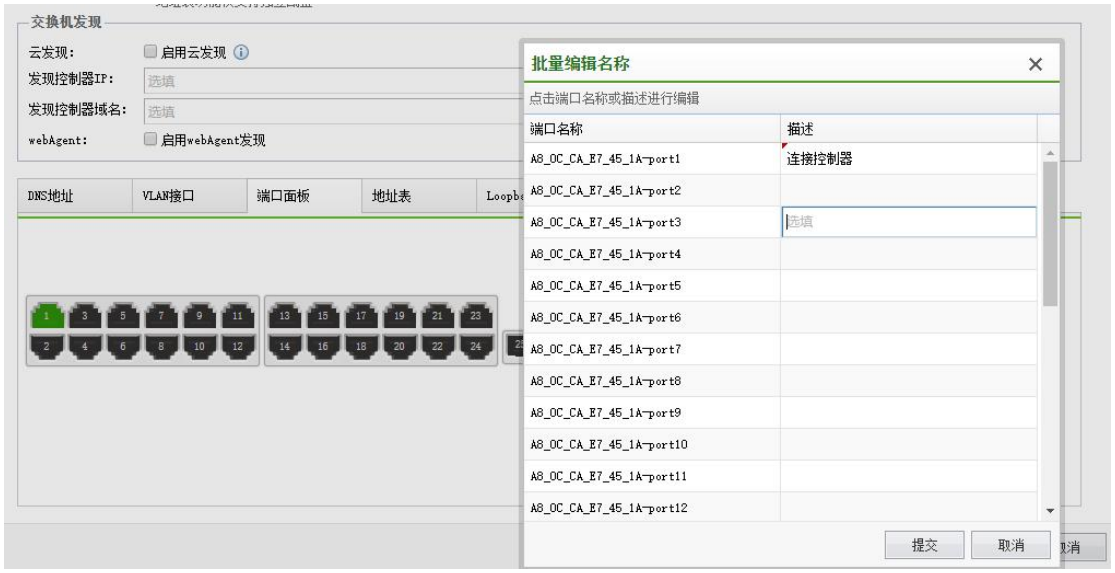


在 VLAN 接口中存在的 VLAN 才可以被选择成管理 vlan。

2.5.1.3.2. 端口面板

在这里可以单独点击接口进行修改该接口的名称、描述、速率、告警日志、MTU 和 VLAN 属性。

选择批量编辑名称，是针对端口名称做修改



选择批量编辑名称，是针对选择好的端口进行修改接口状态、速率、告警日志、MTU 和 VLAN 属性。

网口状态：批量启用/禁用端口。

速率：批量修改端口的协商速率。

告警日志：批量启用/禁用告警日志。

MTU:批量修改端口 MTU。

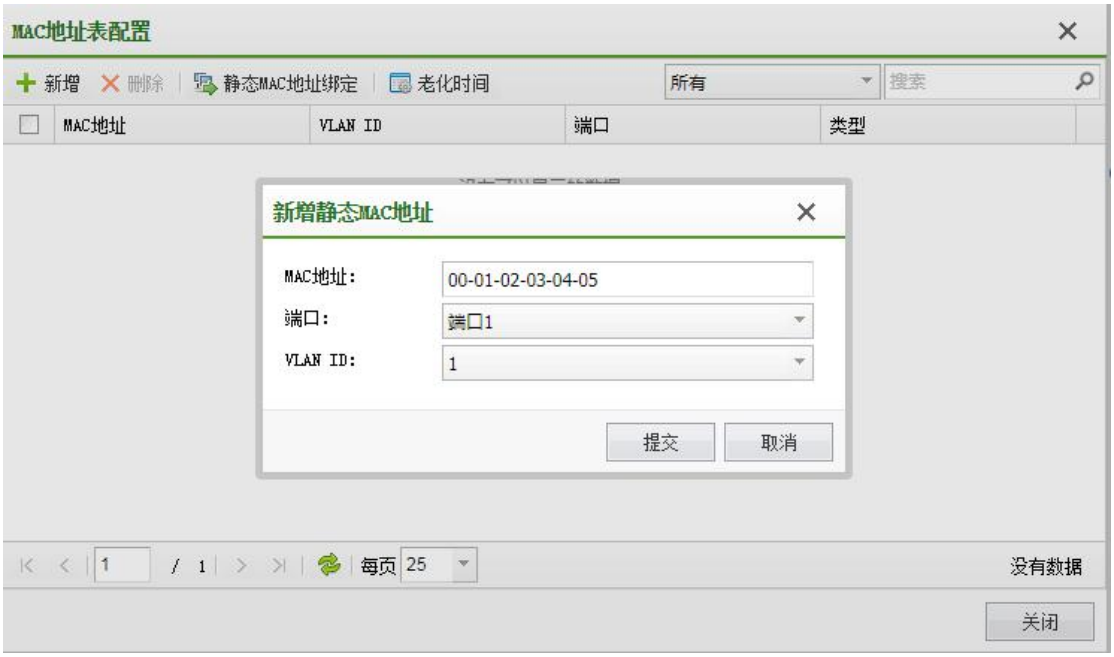
VLAN 属性：批量修改端口 VLAN 属性。

2.5.1.3.3. 地址表

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。

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。

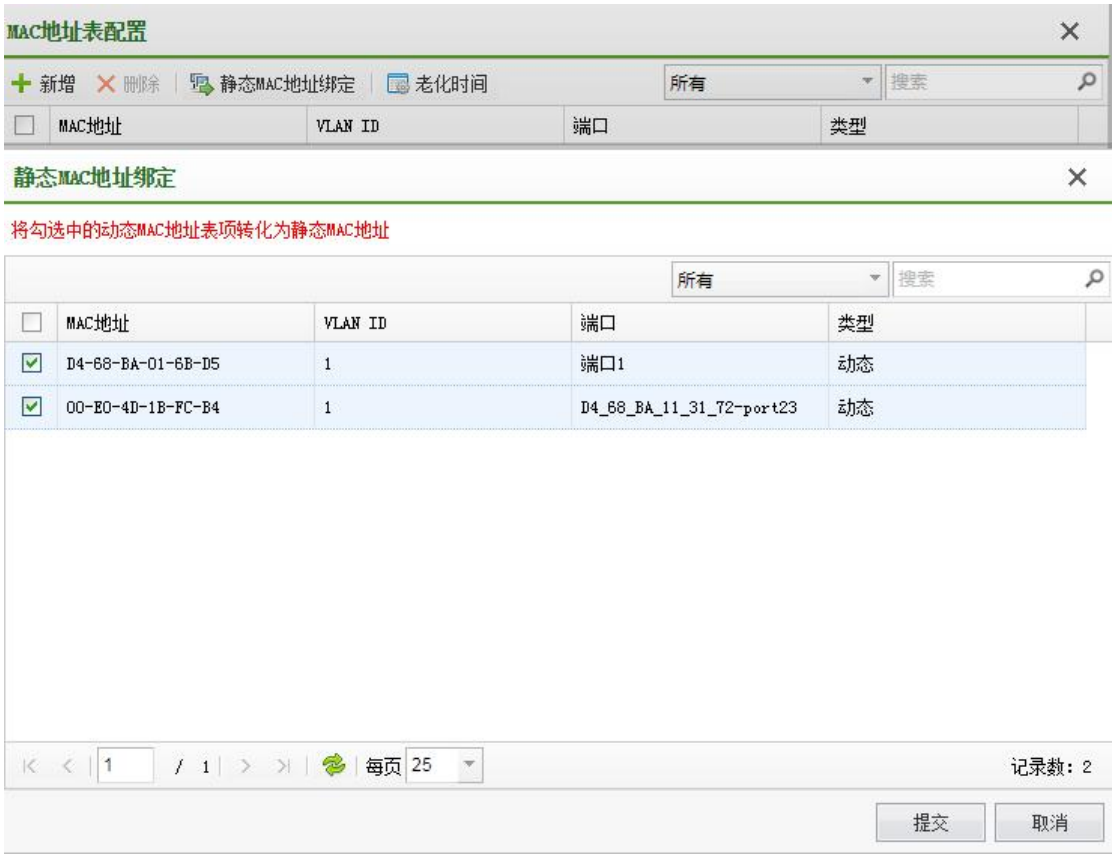


MAC 地址：配置指定的 MAC 地址。

端口：选择添加静态的 MAC 地址是从哪个端口连接到交换机。

Vlan ID：选择添加静态的 MAC 地址是从哪个 VLAN 中接入。

通过点击静态 MAC 地址绑定，可以批量将动态 MAC 地址转换成为静态 MAC 地址。



在静态 MAC 地址绑定中，选中要转换成静态的 MAC 地址，点击提交即可批量将动态 MAC 地址转换成为静态 MAC 地址。

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。交换机动态 MAC 地址老化时间默认为 300 秒，可以根据实际 情况进行调整，调整范围为：60 秒-1000000 秒之间。

配置静态 ARP 地址

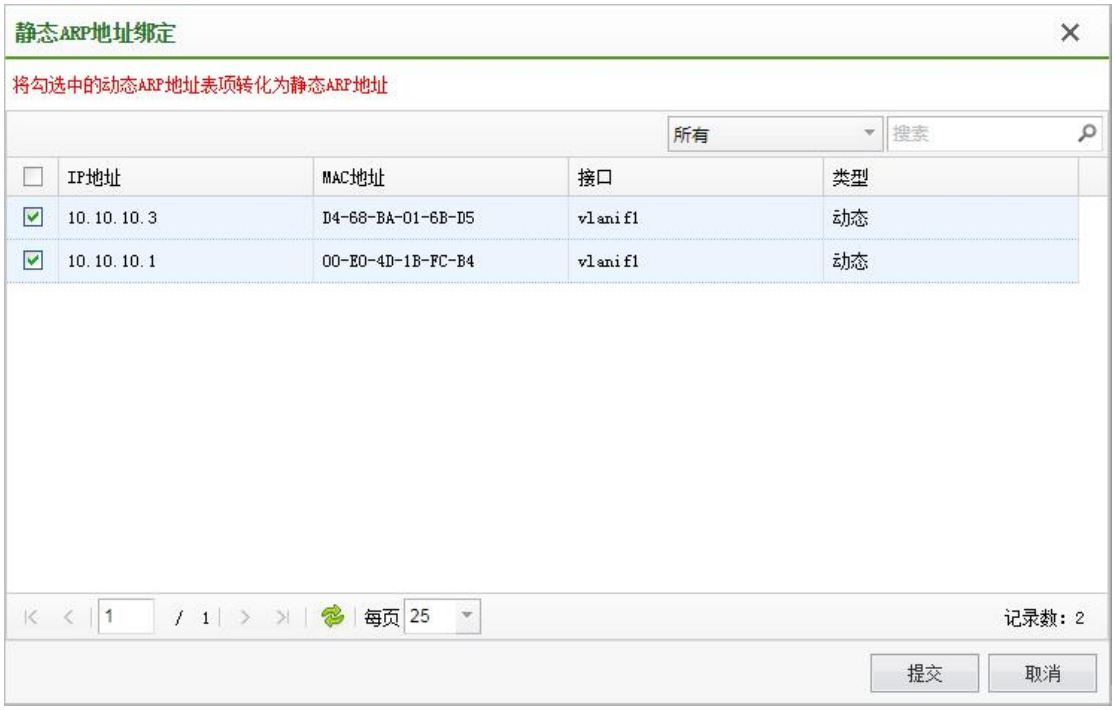
静态 ARP 表项不会被老化，不会被动态 ARP 表项覆盖，因此配置静态 ARP 表项可以增加通信的安全性。

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。

IP 地址：配置静态 ARP 地址。

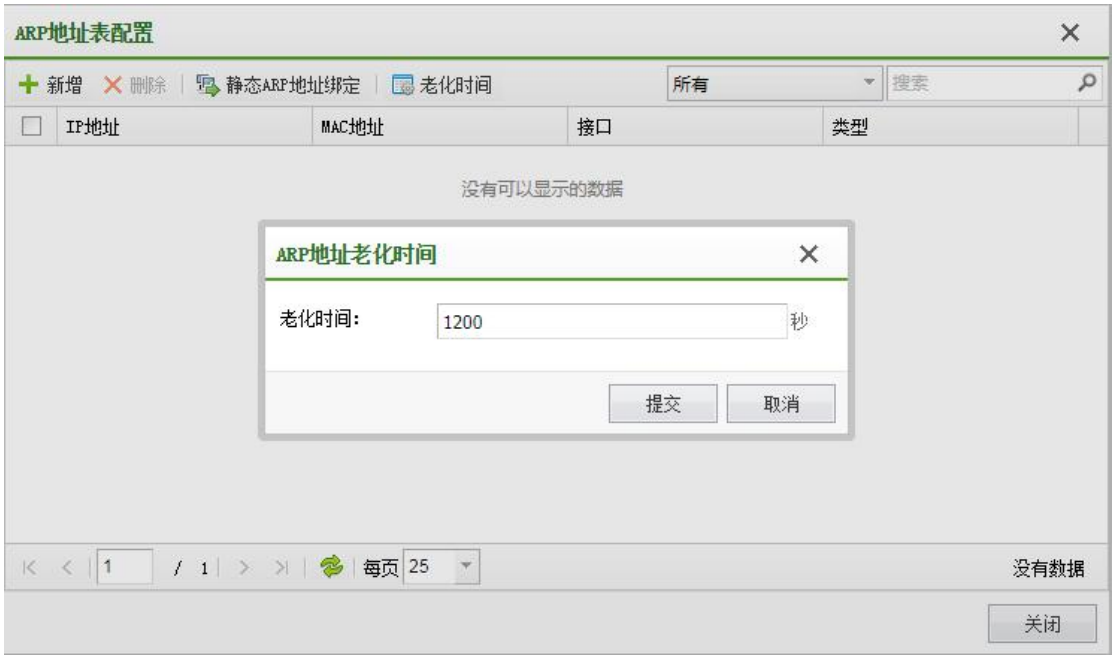
MAC 地址：配置指定的 MAC 地址。

通过点击静态 ARP 地址绑定，可以批量将动态 ARP 地址转换成为静态 ARP 地址。



在静态 ARP 地址绑定中，选中要转换成静态的 ARP 地址，点击提交即可批量将动态 ARP 地址转换成为静态 ARP 地址。

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。交换机动态 ARP 地址老化时间默认为 1200 秒，可以根据实际 情况进行调整，调整范围为：60 秒-3600 秒之间。



2.5.1.3.4. Loopback 地址

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。

IP 地址：配置 Loopback 地址。

子网掩码：配置 Loopback 地址的子网掩码。

MTU：默认 1500，支持范围 576~9174。

启用 loopback 地址尽量不要使用内网中存在的网段地址。

2.5.1.3.5. 认证选项

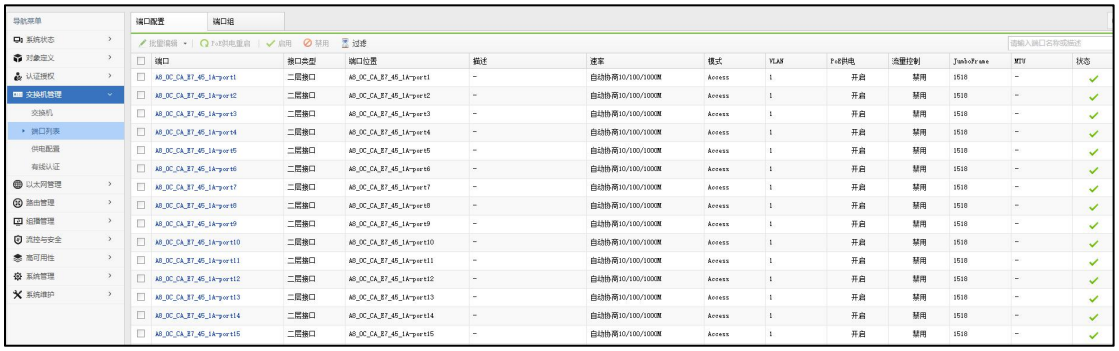
认证选项用于配置认证信息转发以及交换机有线认证单台交换机支持的认证终端个数。

2.5.1.3.6. 隧道参数

交换机可通过二层隧道或三层隧道在控制器激活上线，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。

2.5.2. 端口列表

激活在当前控制器（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。



在该界面下可以批量编辑接口状态：

网口状态：批量启用/禁用端口

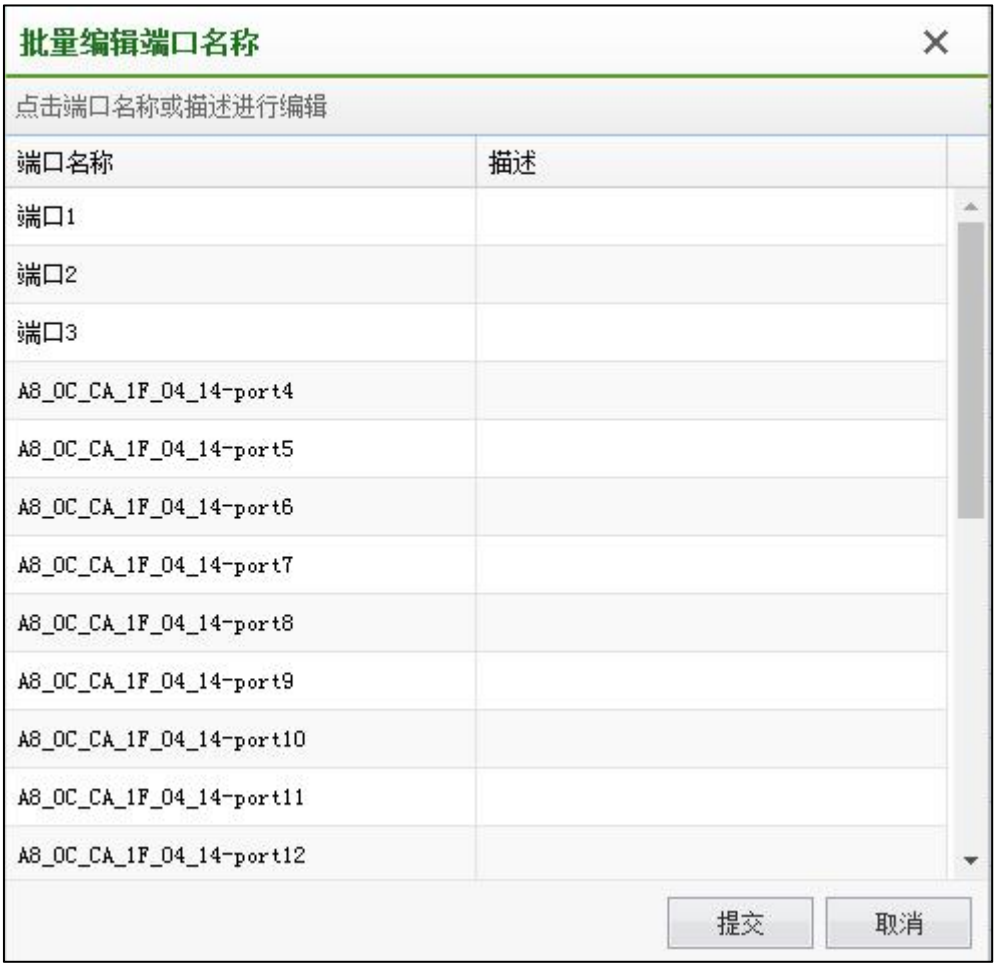
速率：批量配置端口的速率

告警日志：批量启用/禁用告警日志

JumboFrame：批量调整端口的 MTU

VLAN 属性：批量修改端口的 VLAN 属性

批量编辑接口名称和描述：



通过过滤可以查看某台交换机的配置，也可以根据 VLAN 属性过滤端口

交换机：选择想要查看的交换机

POE 供电：仅支持查看 POE 交换机

端口模式：端口的 VLAN 属性

VLAN：根据 VLAN 过滤端口

2.5.3. 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。

交换机和控制器断开一定时间之后（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。

注意：供电配置仅对支持 POE 功能的交换机生效

2.5.4. 有线认证

用于配置交换机有线认证，详细配置可看交换机有线认证配置手册。

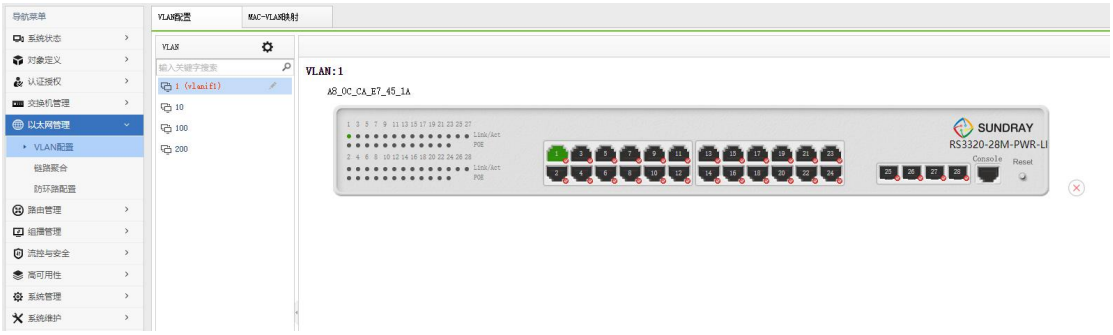
2.6. 以太网管理

『以太网管理』包括【VLAN 配置】、【链路聚合】、【防环路配置】这 3 个菜单选项。

2.6.1. VLAN 配置

VLAN（Virtual Local Area Network）即虚拟局域网，这项技术可以根据功能、应用或者管理的需要将局域网内部的设备逻辑地划分为一个个网段，从而形成一个个虚拟的工作组，并且不需要考虑设备的实际物理位置。IEEE 颁布了 IEEE802.1Q 协议以规定标准化 VLAN 的实现方案，交换机的 VLAN 功能即按照 802.1Q 的标准实现。

VLAN 技术的特点在于可以根据需要动态的将一个大的局域网划分成许多不同的广播域。



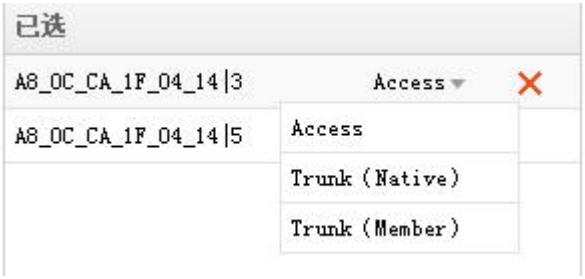
VLAN ID:填写对接的 VLAN 编号

注意：此处的 VLAN ID 只针对交换机创建，和有线配置里面的 VLAN 不能互相调用

描述：对 VLAN 进行描述

成员：选择交换机的对应接口进行划分 VLAN

在 VLAN ID 中选择交换机接口时，接口默认使用 access 方式。

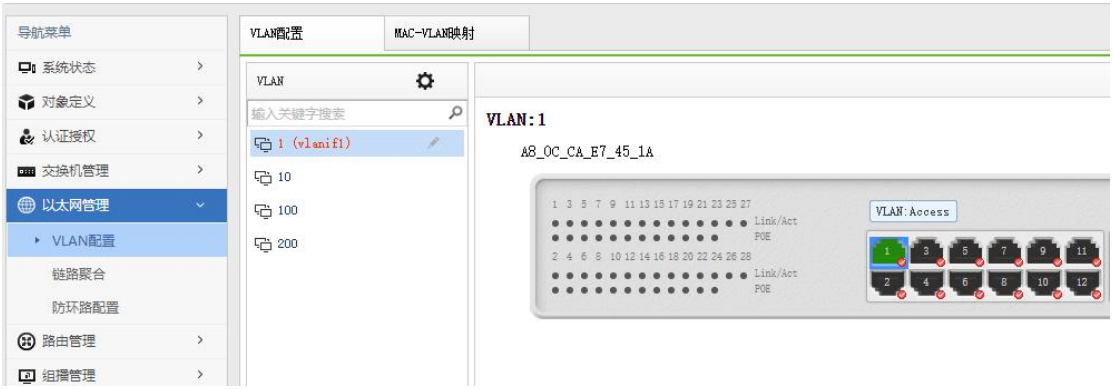


在已选接口中可以修改接口的模式：

Access：接口只允许一个 VLAN 通过

Trunk（Native）：接口改为 trunk，该 VLAN 为本征 VLAN

Trunk（Member）：接口改为 trunk，接口允许该 VLAN 通过



点击左边对应的 VLAN ID，在右边交换机上即可显示出该 VLAN 可以在哪些接口上存在，将鼠标放到右边交换机的接口上即可显示出该接口的接口模式；在右边交换机接口上使用右键可以对该接口的名称、描述、速率、告警日志、MTU 和 VLAN 属性进行编辑。

启用：勾选即启用端口。

描述：对端口进行描述。

速率：配置端口速率。

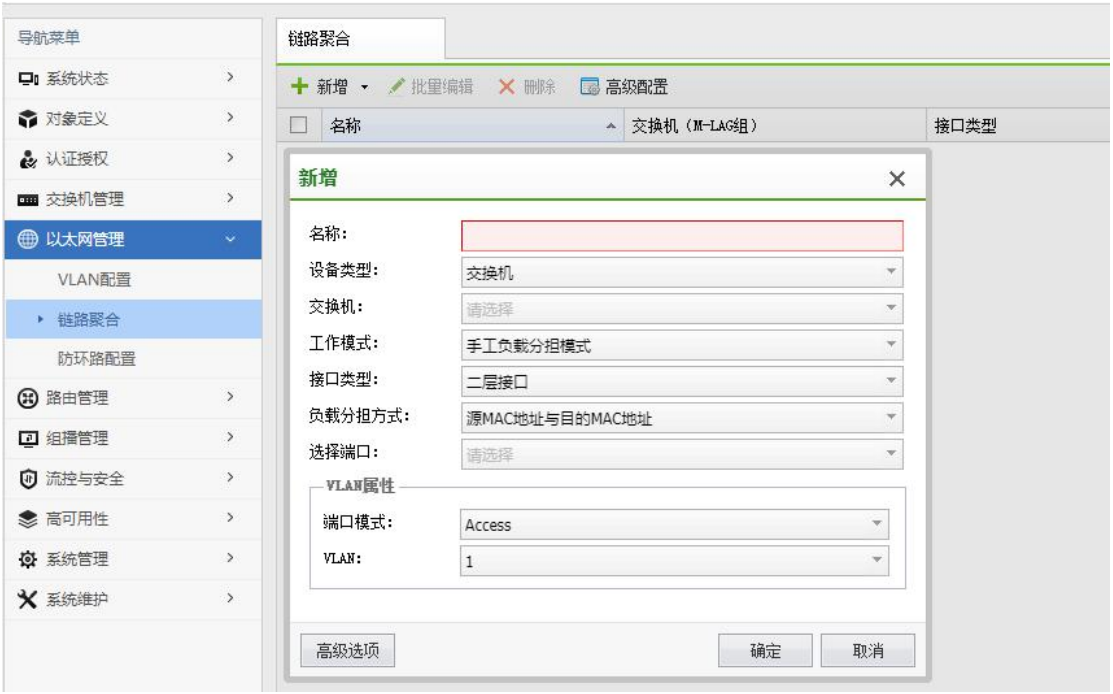
告警日志：启用/禁用告警日志。

MTU:配置端口的 MTU。

VLAN 属性：配置端口的 VLAN 属性。

2.6.2. 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

（1）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。

（2）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）。

2.6.3. 防环路配置

2.6.3.1. 生成树

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）。

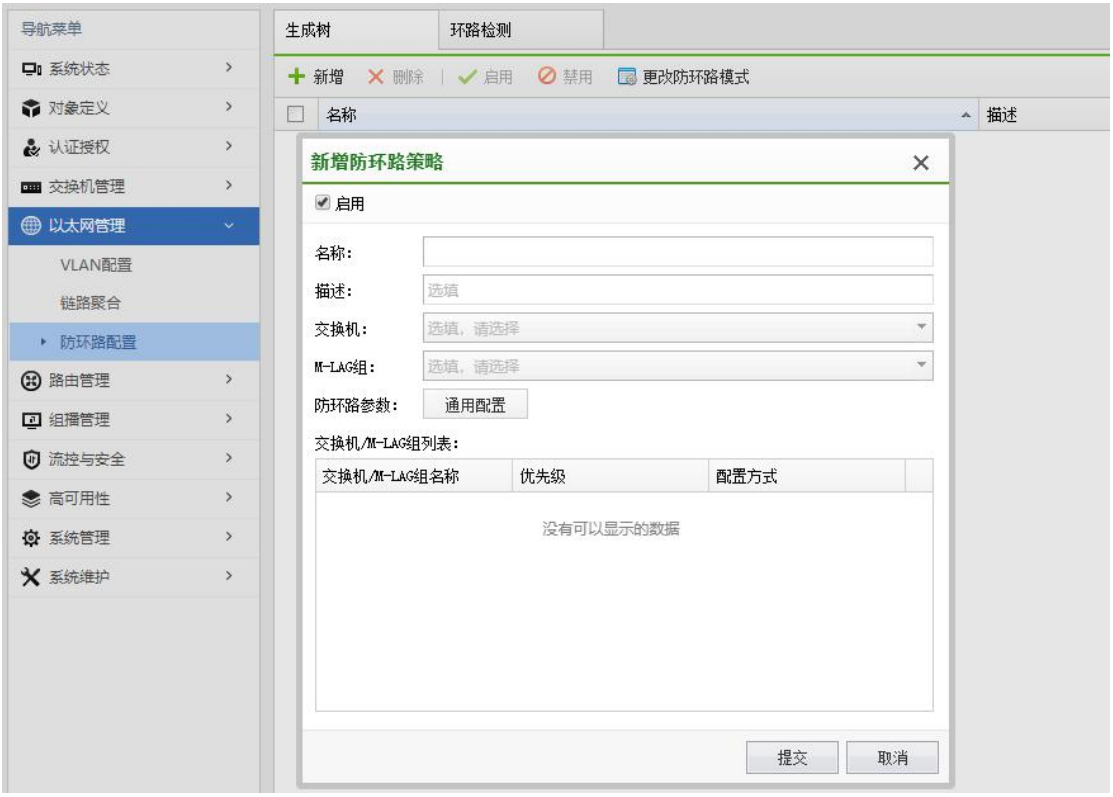
选择开启防环路模式：

简单模式：一键开启防环路

高级模式：调整生成树的更多功能

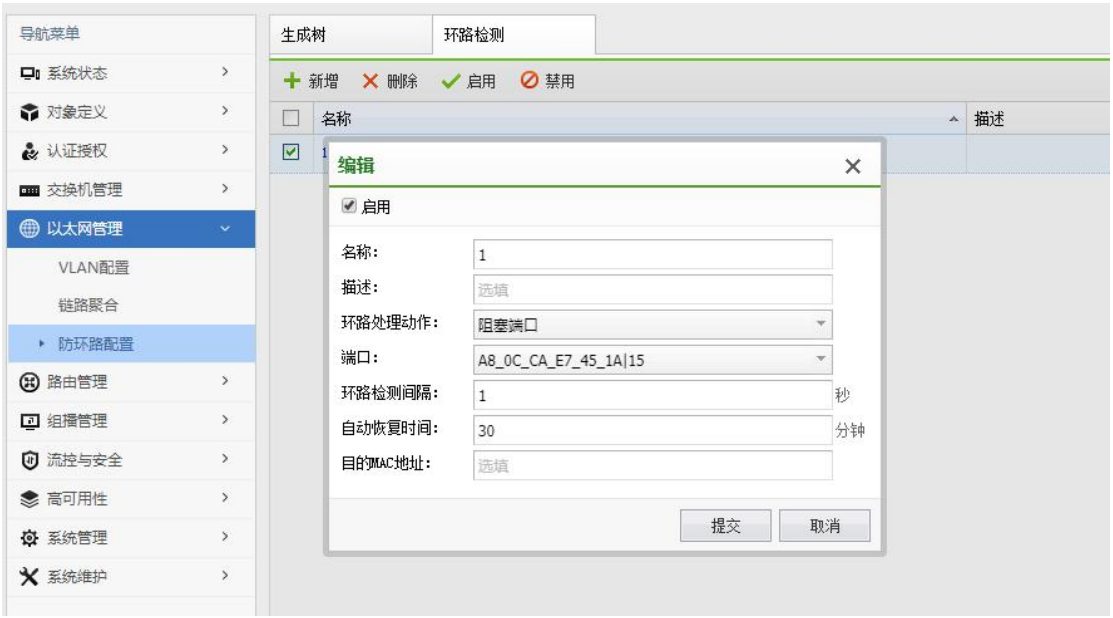
一键开启生成树，某些交换机不需要开启生成树，可以通过排除交换机进行排除，排除交换机可以精确到交换机的端口。

通过点击更改防环路模式，将简单模式修改成高级模式，对生成树做更多的调整。



2.6.3.2. 环路检测

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。

2.7. 路由管理

『路由管理』包括【静态路由】、【策略路由】、【RIP 配置】、【OSPF 配置】、【路由优先级】这 5 个菜单选项。

2.7.1. 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。

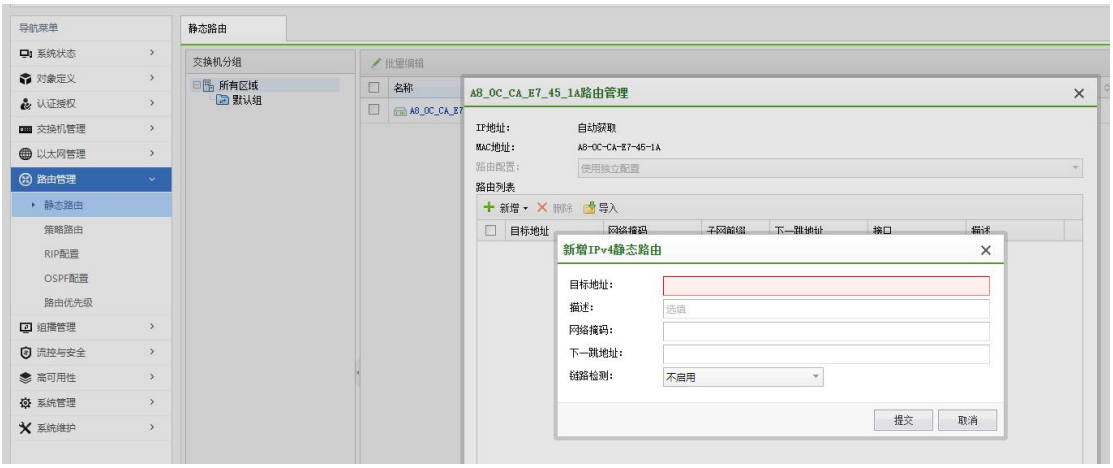
2.7.1.1. IPV4 静态路由

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。

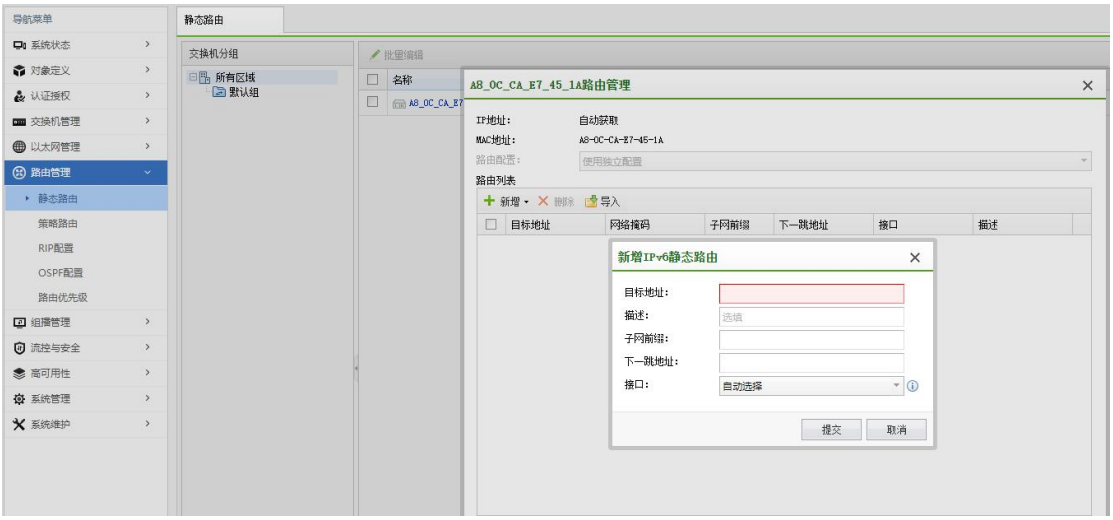
在创建静态路由时，如果将目的地址与掩码配置为全零，则表示配置的是 IPv4 静态缺省路由。缺省情况下，没有创建 IPv4 静态缺省路由。



2.7.1.2. 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。



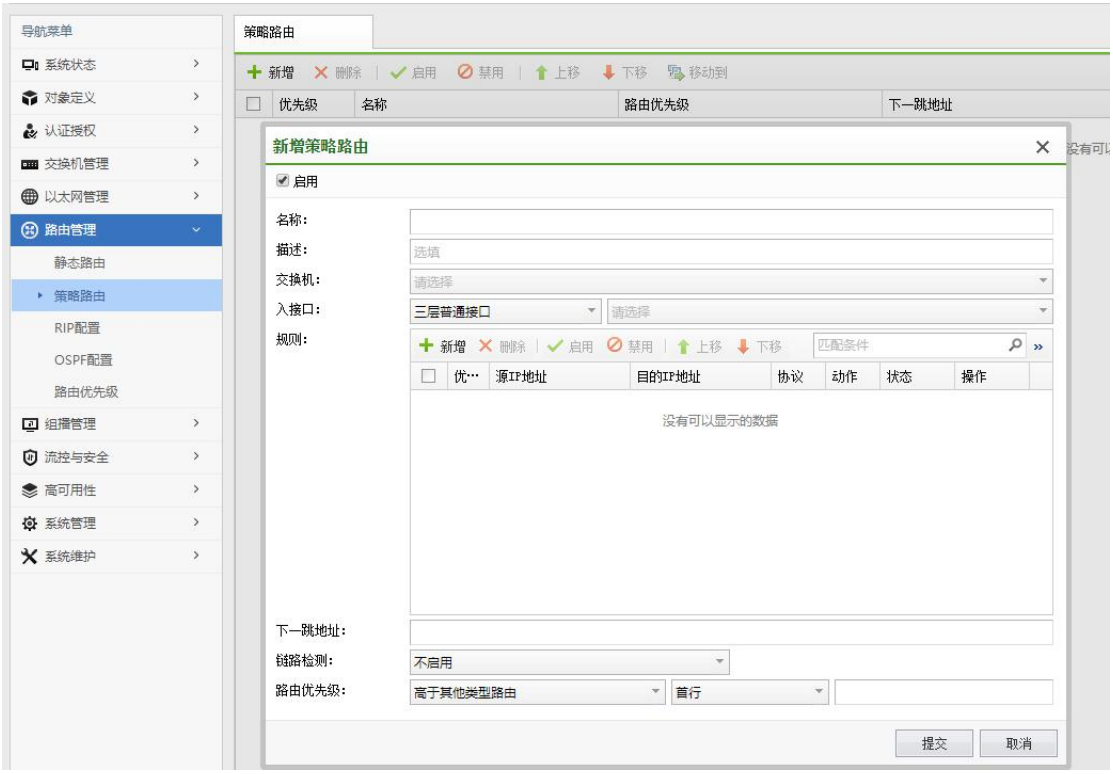
2.7.2. 策略路由

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。

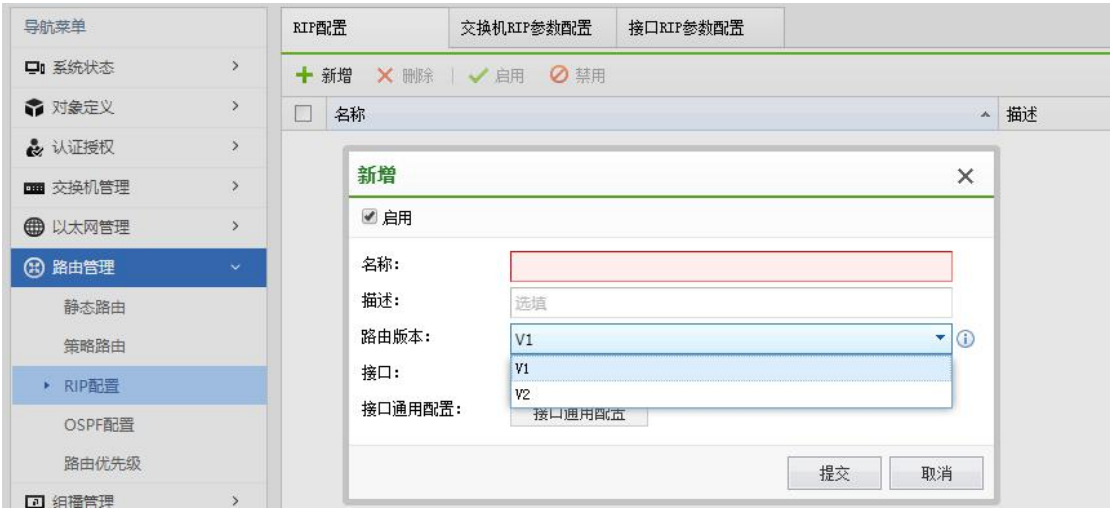


2.7.3. RIP 配置

2.7.3.1. 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。

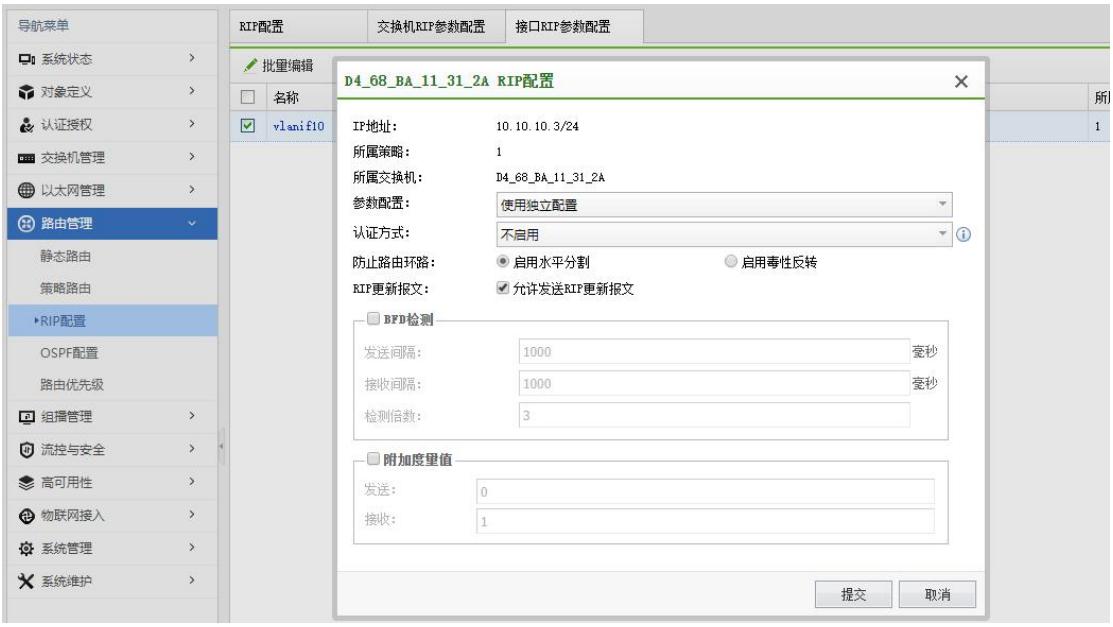
RIP 路由 V2 版本是一种无分类路由协议，支持外部路由标记，可以在路由策略中根据 Tag 对路由进行灵活的控制。支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。



2.7.3.2. 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。

2.7.3.3. 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）。

2.7.4. 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。

2.7.4.1. 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。

2.7.4.2. 交换机 OSPF 参数配置

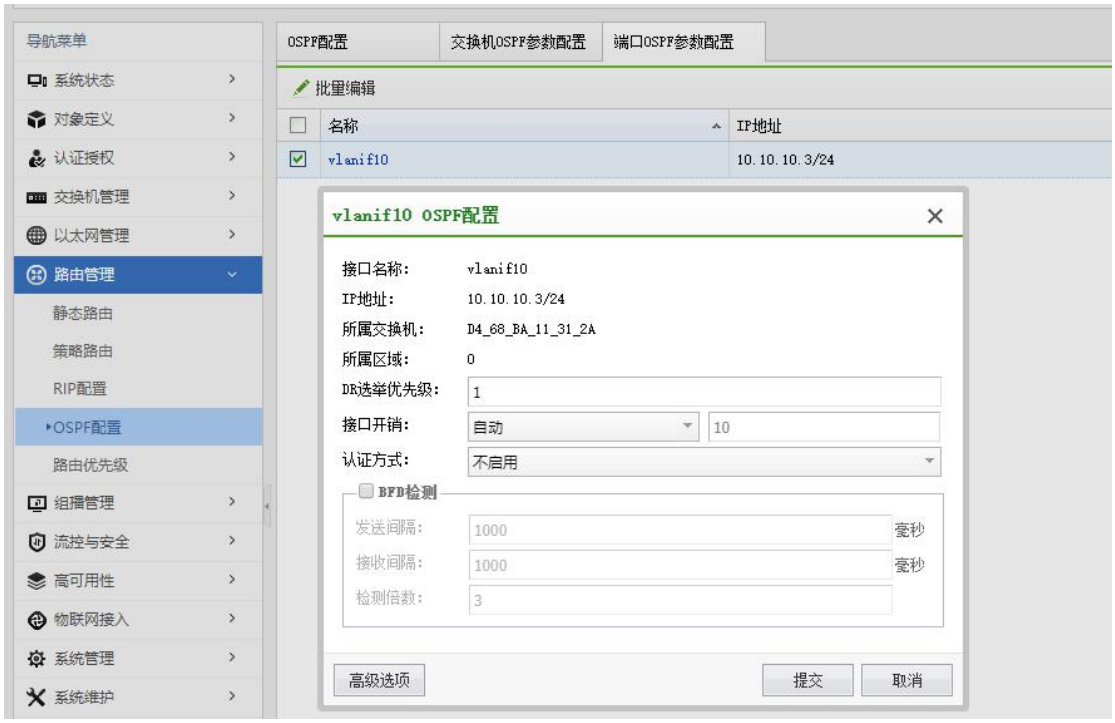
可对已加入 OSPF 中的交换机进行配置，实现路由引入。

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。

2.7.4.3. 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。

2.7.5. 路由优先级

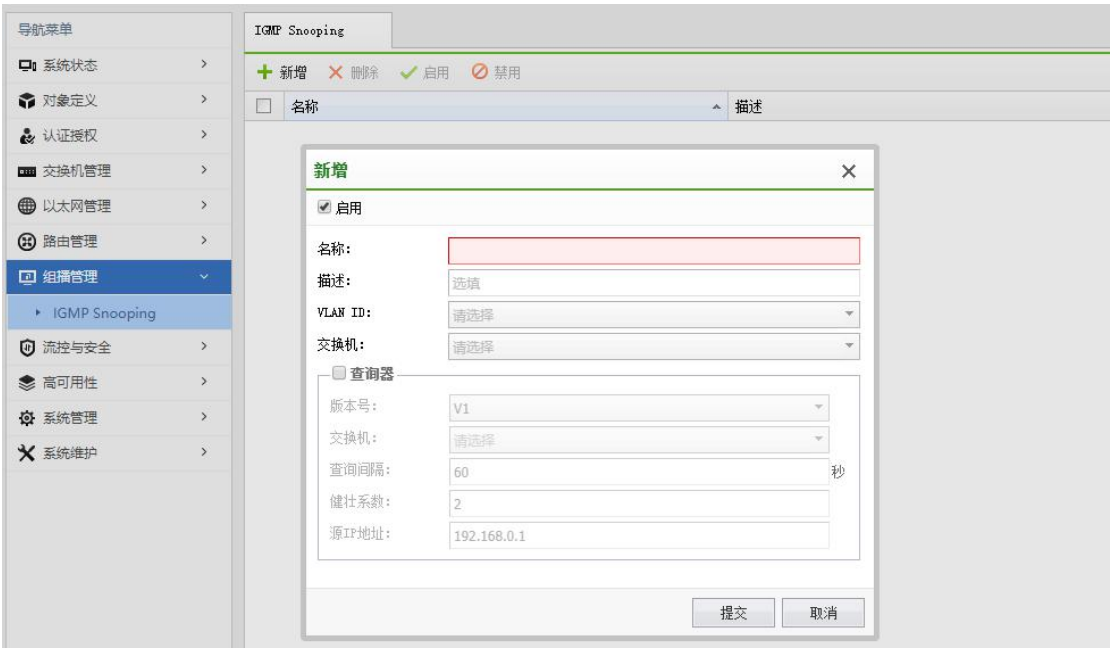
对于相同的目的地，不同的路由协议（包括静态路由）可能会发现不同的路由，但这些路由并不都是最优的。事实上，在某一时刻，到某一目的地的当前路由仅能由唯一的路由协议来决定。为了判断最优路由，各路由协议（包括静态路由）都被赋予了一个优先级，当存在多个路由信息源时，具有较高优先级（取值较小）的路由协议发现的路由将成为最优路由，并将最优路由放入本地路由表中。

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。

2.8. 组播管理

2.8.1. IGMP Snooping

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。

2.9. 流控与安全

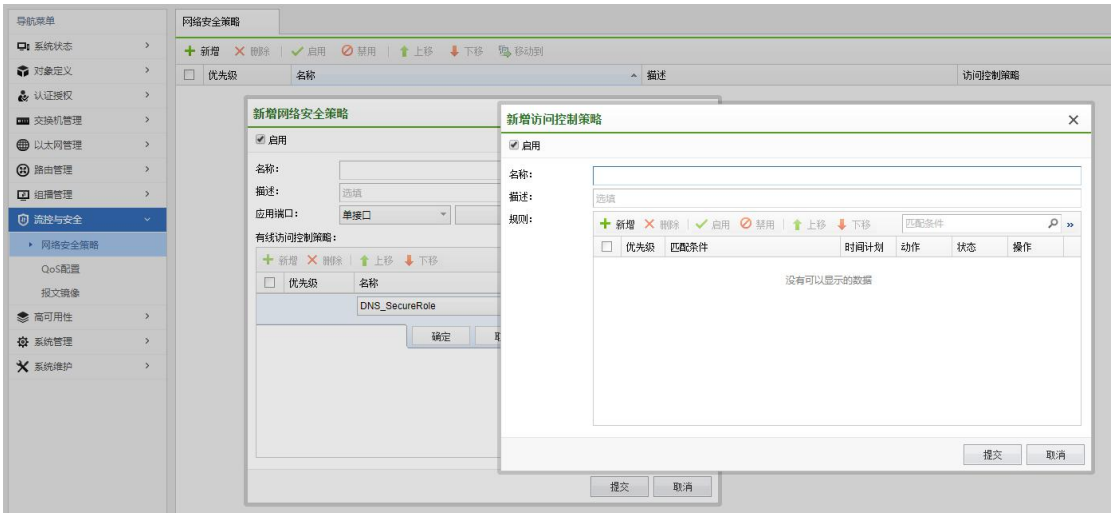
『流控与安全』包括【网络安全策略】、【QoS 配置】、【报文镜像】这 3 个菜单选项。

2.9.1. 网络安全策略

网络安全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。



2.9.2. 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：基于匹配 ACL 策略，同时对于流量重标记、重定向

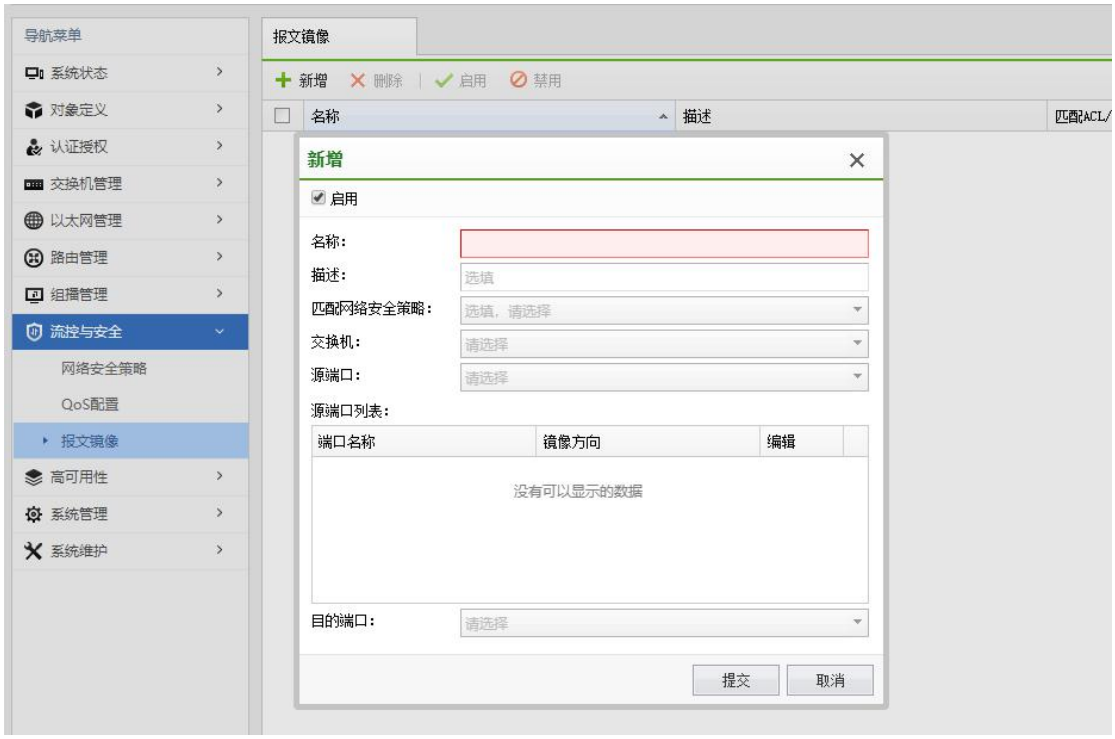
流量整形：批量应用于安视交换机基于端口、队列进行流量整形，自定义入方向、出方向文件传输速率

优先级映射：基于交换机对流量进行 COS、DSCP 优先级设置

拥塞管理：通过严格优先模式、轮询模式、加权轮询模式、差分加权轮询模式等调度模式对交换机端口流量进行管理

2.9.3. 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。

2.10. 高可用性

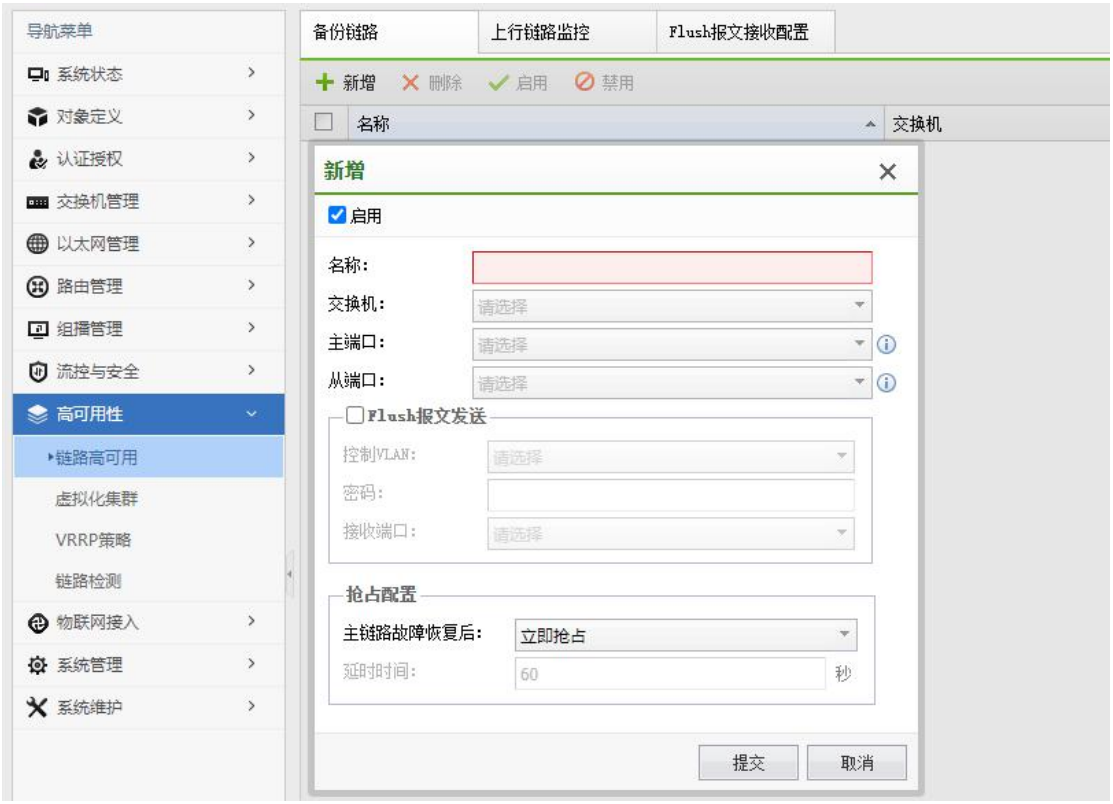
『高可用性』包括【链路高可用】、【虚拟化集群】、【VRRP 策略】、【链路检测】

这 4 个菜单选项。

2.10.1. 链路高可用

2.10.1.1. 备份链路

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

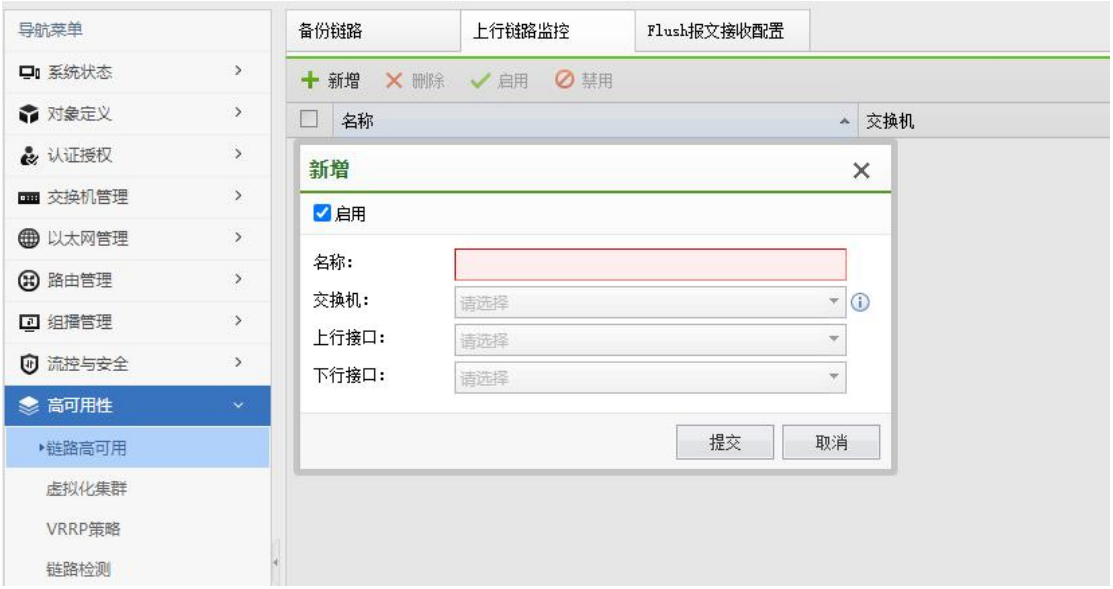
端口切换之后，备份链路通过发送 FLUSH 报文通知其他设备进行地址刷新，且相关设备必须使能 Flush 报文接收功能。但是，由于该技术为私有技术，目前只限于我司的交换机、华为、华三的设备能够识别该报文。对于不识别 FLUSH 报文的设备，只能通过流量触发 MAC 地址的更新。

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。

2.10.1.2. 上行链路监控

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

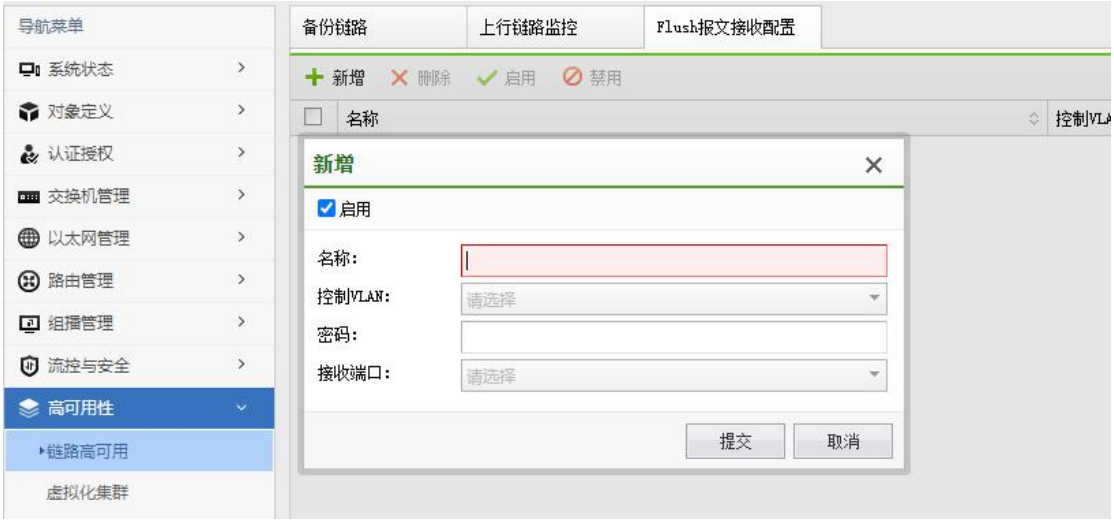
上行接口是上行链路监控组中的被监控的端口，上行链路监控组的上行接口可以是以太网端口（电口或光口）、聚合口或备份链路组。

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。

2.10.1.3. Flush 报文接收配置

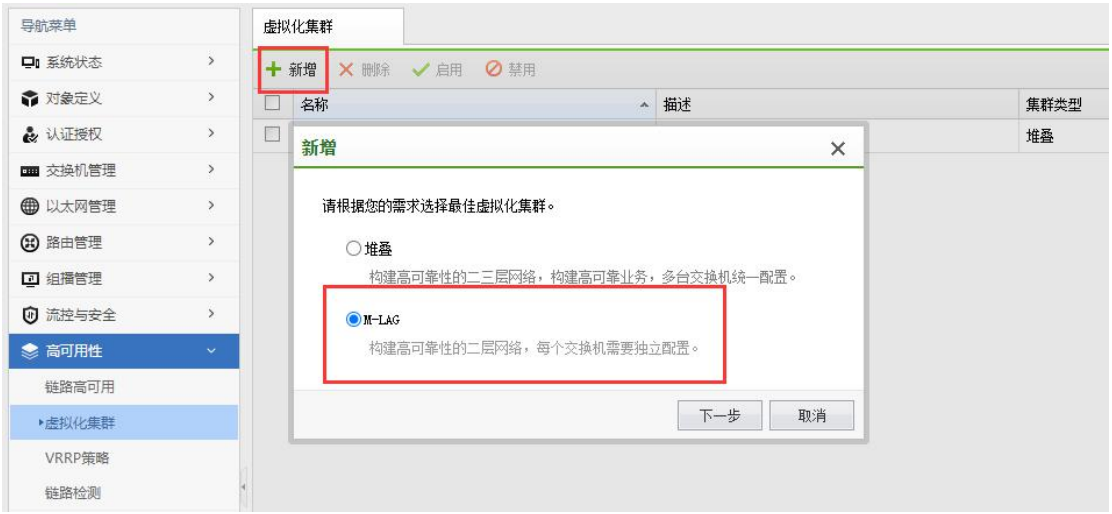
支持独立配置 Flush 报文接收功能，并配置接口接收 Flush 报文的加密方式、接收控制 VLAN ID 和密码。当上游设备收到 Flush 报文时，判断该 Flush 报文的发送控制 VLAN 是否在收到报文的接口配置的接收控制 VLAN 列表中。如果不在接收控制 VLAN 列表中，设备对该 Flush 报文不做处理，直接转发；如果在接收控制 VLAN 列表中，设备会处理收到 Flush 报文，进而执行 MAC 地址转发表项和 ARP 表项的刷新操作。

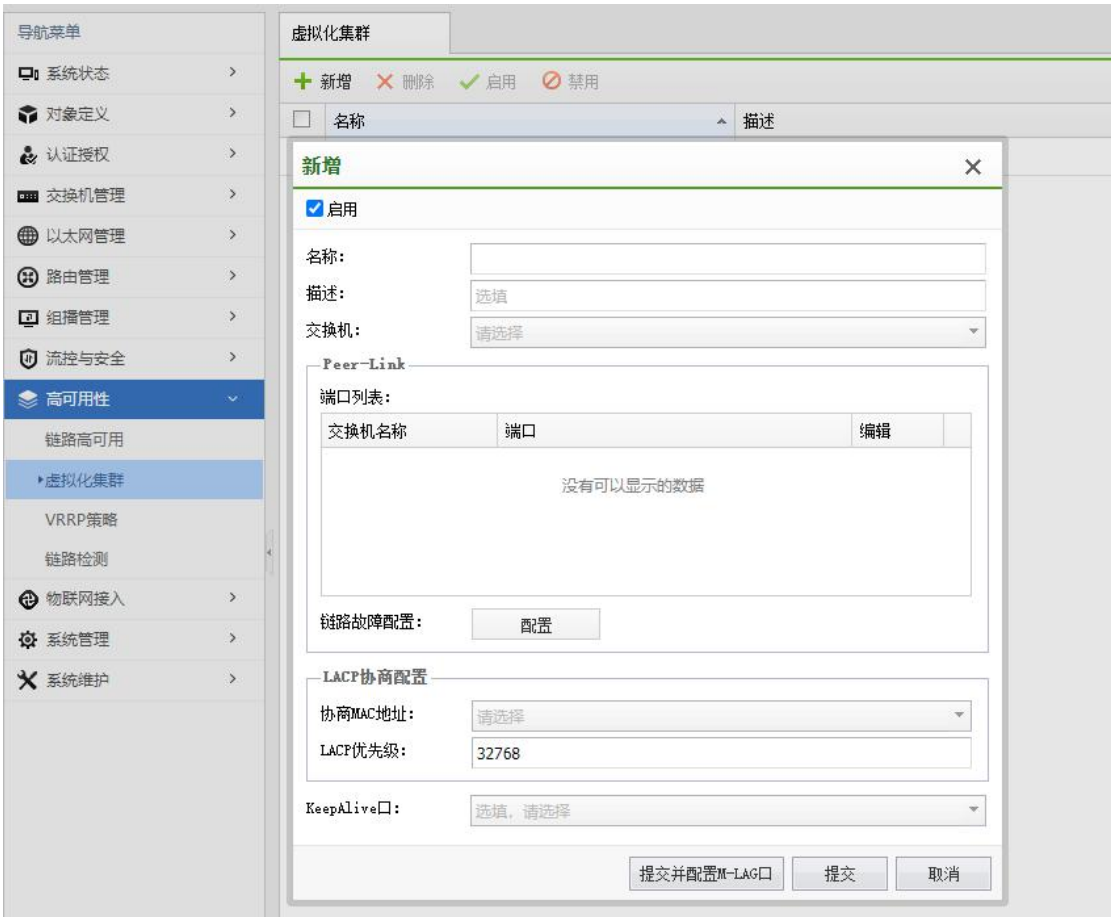


2.10.2. 虚拟化集群

2.10.2.1. M-LAG

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。





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。

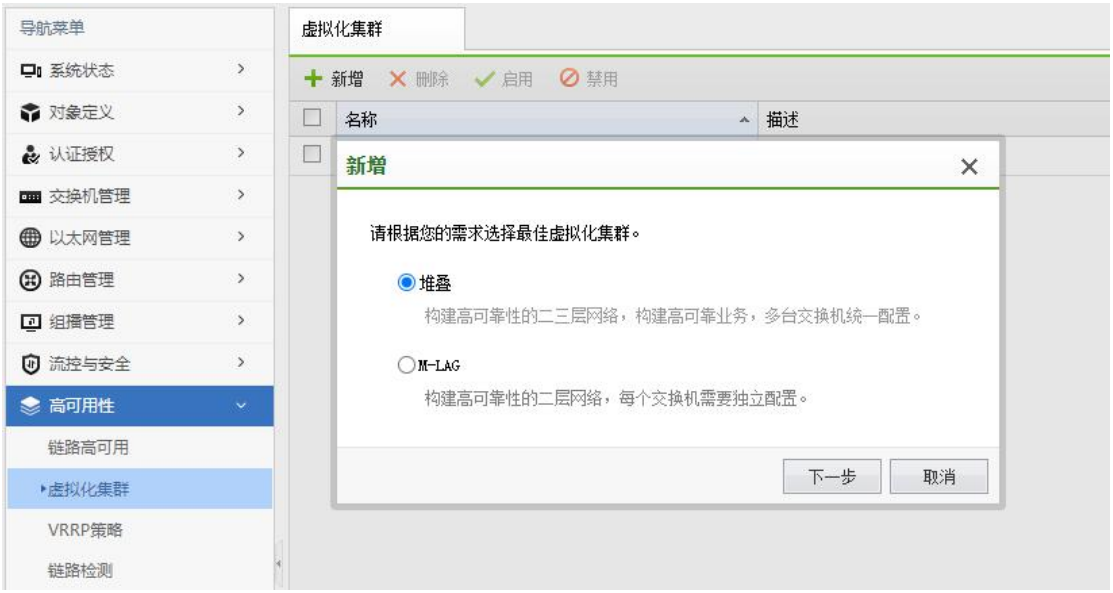
正常情况下，双主检测链路不会参与 M-LAG 的任何转发行为，只在故障场景下，用于检查是否出现双主的情况。用于检测对端的选举状态是否正常。

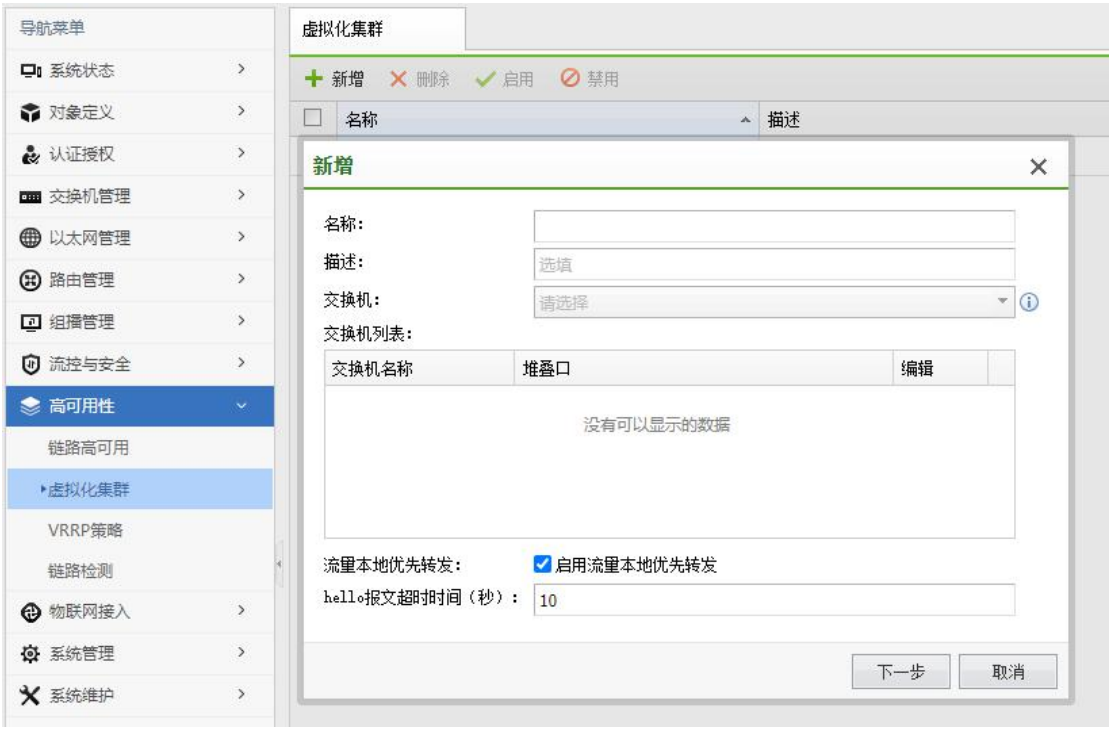
M-LAG 口

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。

2.10.2.2. 堆叠

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。





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，仅支持光口做为堆叠口。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

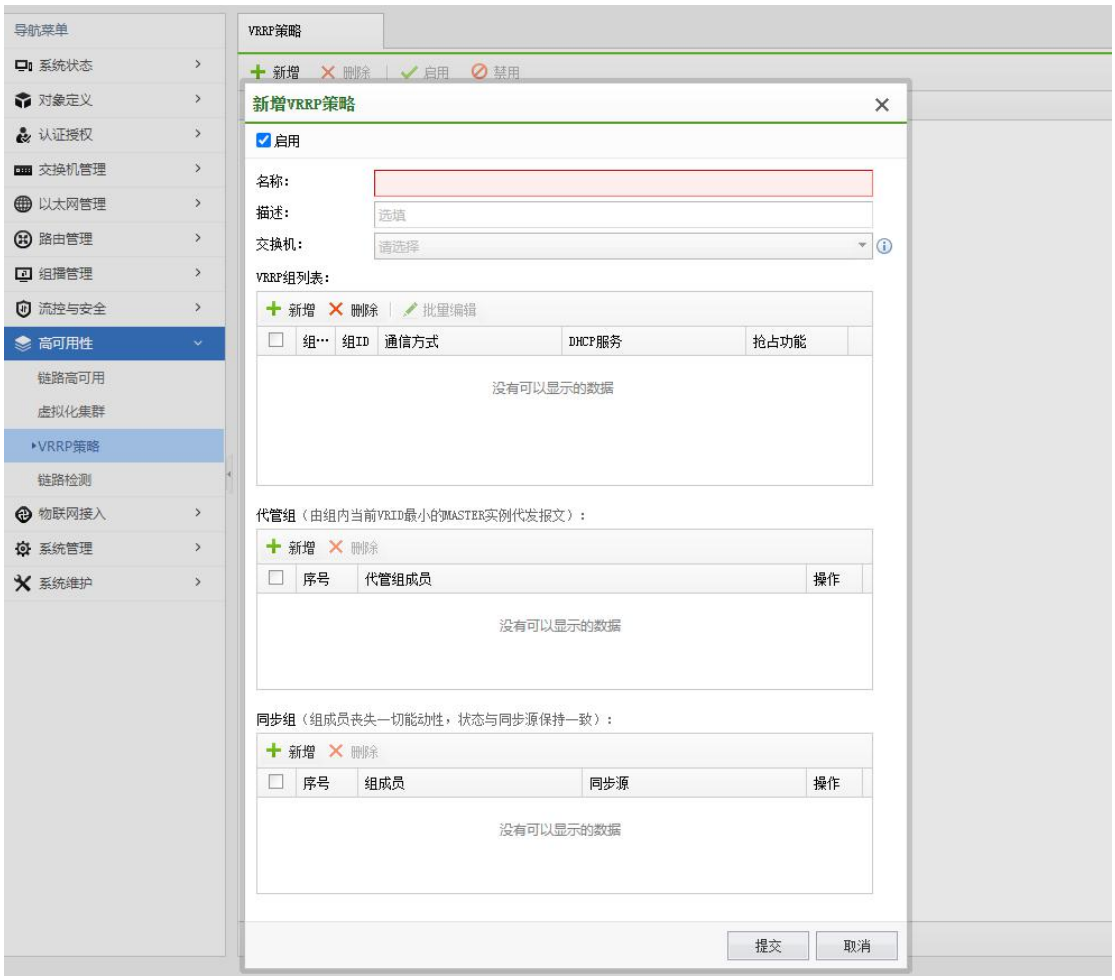
堆叠系统中备机超时时间内，未收到主机发送的保活报文，会自动升级为主机。

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。

2.10.3. 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。

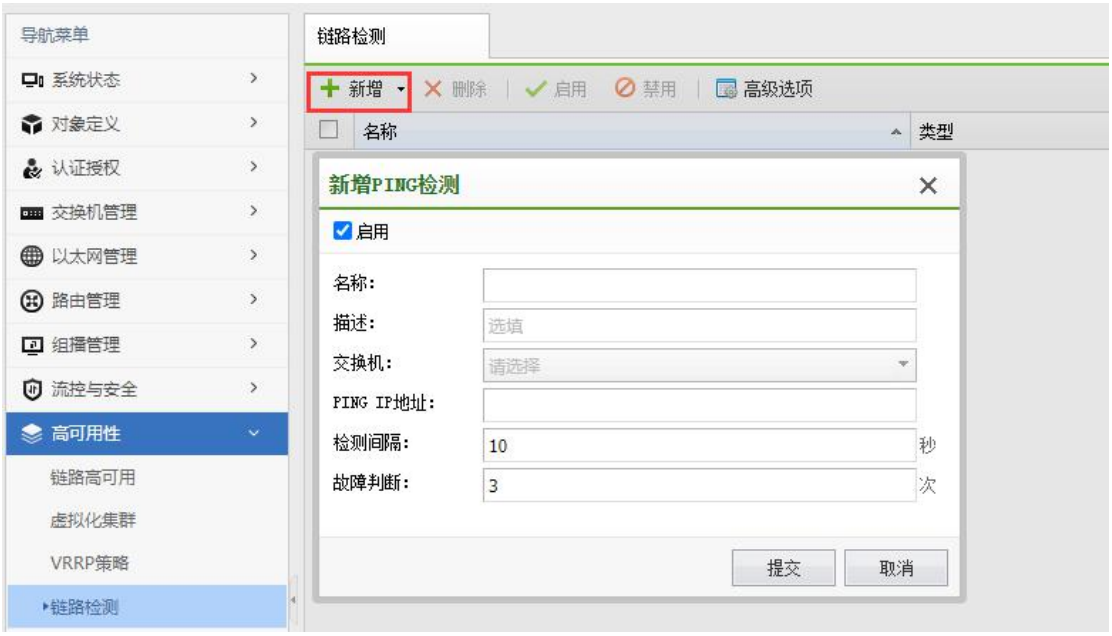
2.10.4. 链路检测

包含 PING 检测和 BFD 检测。

2.10.4.1. 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。

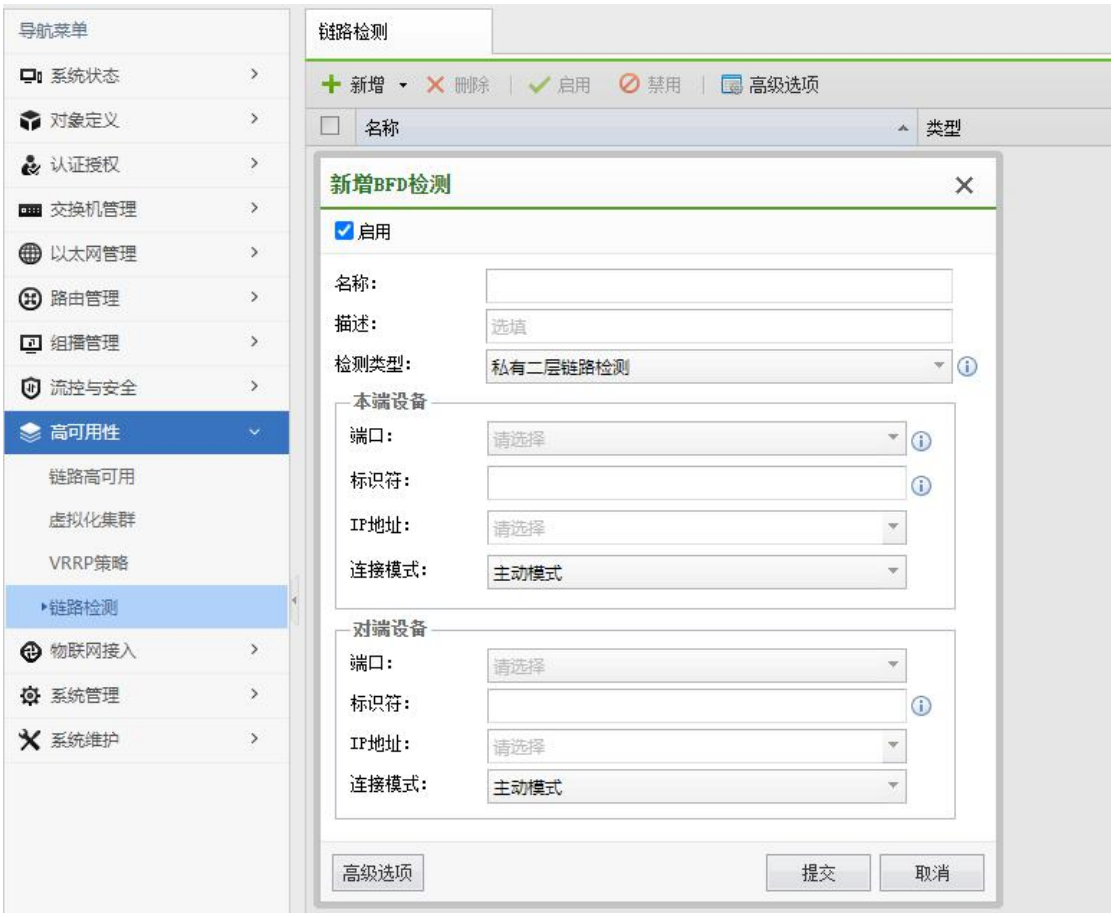


2.10.4.2. **BFD 检测**

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控制器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控制器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。

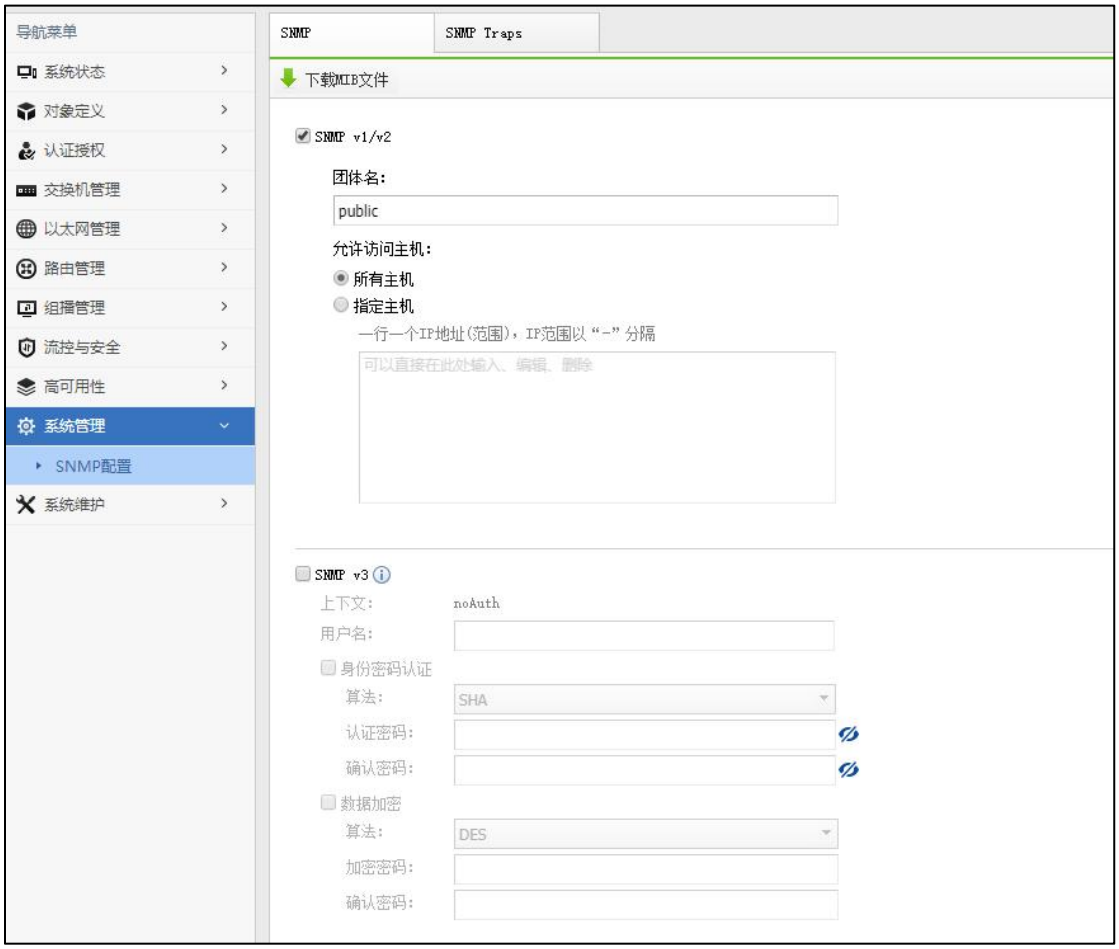
WTR 等待恢复时间（分钟）：如果 BFD 会话发生振荡，则与之关联的应用将会在主备之间频繁切换。为避免这种情况的发生，可以配置 BFD 会话的等待恢复时间 WTR。当 BFD 会话从状态 Down 变为状态 Up 时，BFD 等待 WTR 超时后才将这个变化通知给上层应用。如果使用 WTR，用户需要手工在两端配置相同的 WTR。否则，当一端会话状态变化时，两端应用程序感知到的 BFD 会话状态将不一致。

2.11. 系统管理

2.11.1. 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。

2.11.1.1. SNMP



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。

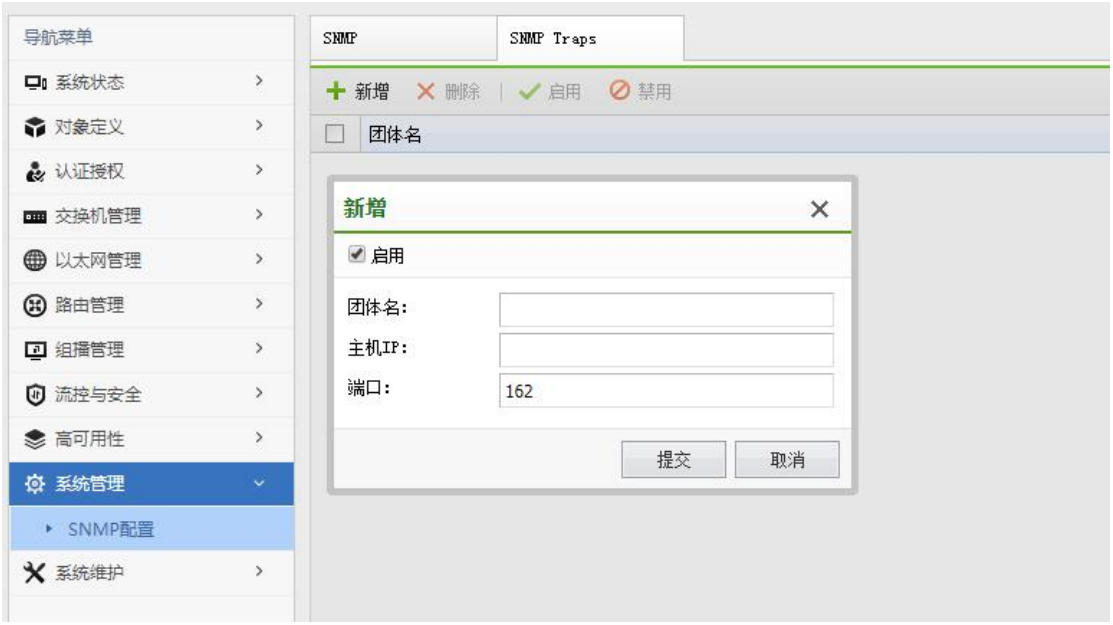
加密需要提供加密方式（DES）和加密密钥。

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。

2.11.1.2. 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。



2.12. 系统维护

2.12.1. 日志查看

2.12.1.1. 设备日志

查看设备产生的日志，协助发现及排除故障。

2.12.1.2. 设备日志

查看系统运行过程中产生的日志，协助发现及排除故障。

2.12.1.3. 设备日志

管理日志中，记录了管理员登录、注销、修改配置的日志。

2.12.1.4. 用户认证日志

用户认证日志中，记录了所有终端的认证日志。

第 3 章 边缘安全

通过点击应用中心->边缘安全进入边缘安全页面。

边缘安全里与交换机相关的功能如下：

1、『安全可视』中的【终端安全】、【东西向流量安全】
2、『业务感知』中的【交换机业务感知】
3、『终端安全』
4、『流量安全』中的【流量劫持防御】、【漏洞攻击防御】
5、『联动响应』
6、『智能告警』

3.1. 安全可视

3.1.1. 终端安全

3.1.1.1. 有线终端安全

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。

3.1.1.2. 终端黑名单

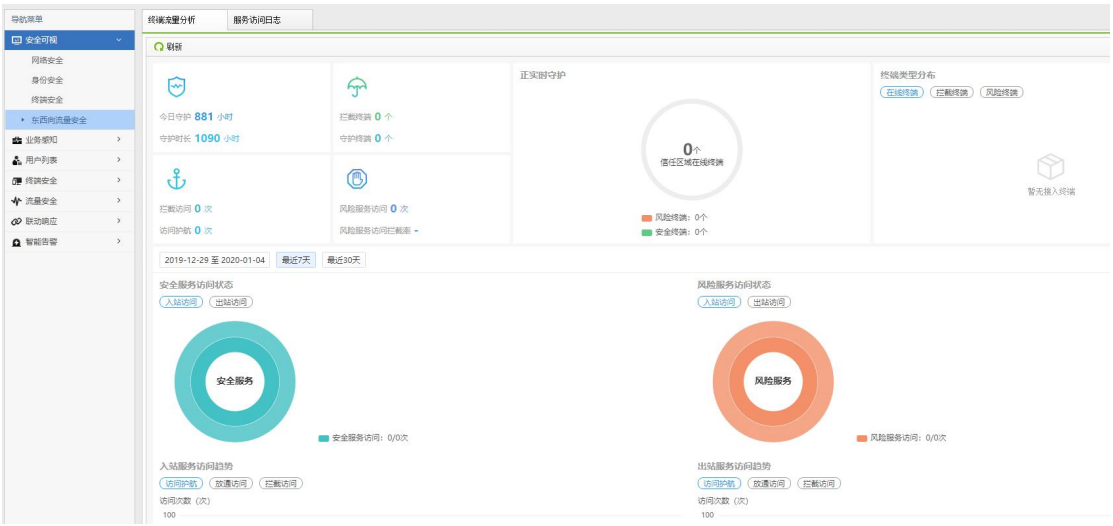
管理员可以手动添加黑名单，以阻止指定的 MAC 地址终端连接有线和无线网络。

当终端进行暴破登录或者其它恶意攻击行为时，系统会将此终端的 MAC 地址加入黑名单，拒绝一段时间内该终端的连接请求。由终端类型绑定策略触发的非指定类型终端接入，系统也会将此终端 MAC 地址加入黑名单并拒绝该终端的连接请求，限制时间随策略而定。

3.1.2. 东西向流量安全

3.1.2.1. 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/入站访问拦截情况等。



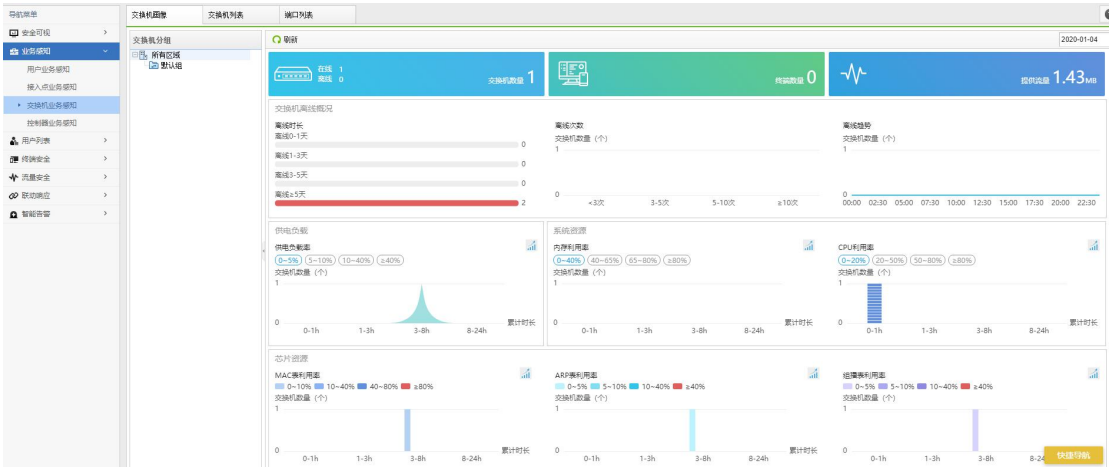
3.1.2.2. 服务访问日志

显示信任区域/保护区域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. 业务感知

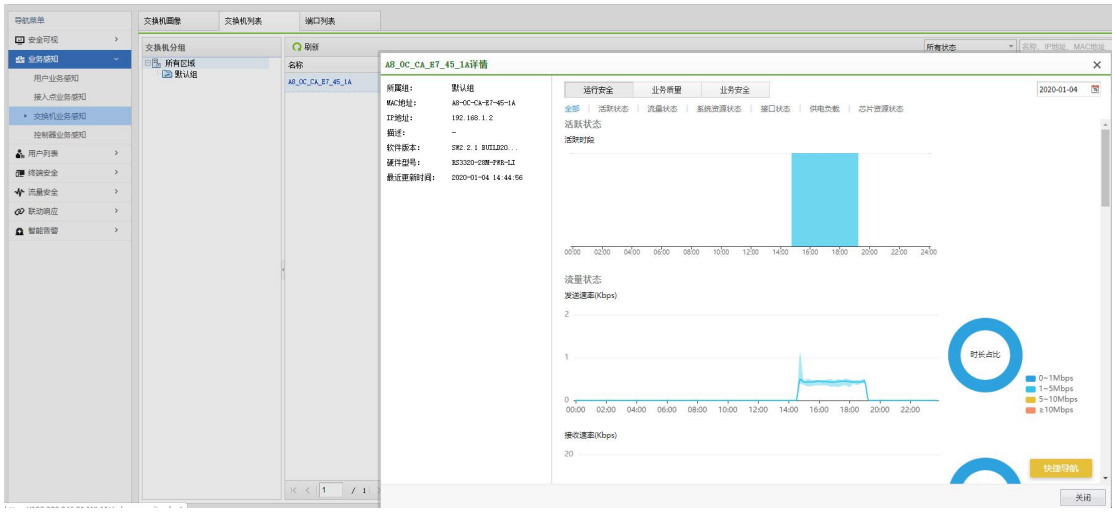
3.2.1. 交换机画像

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。



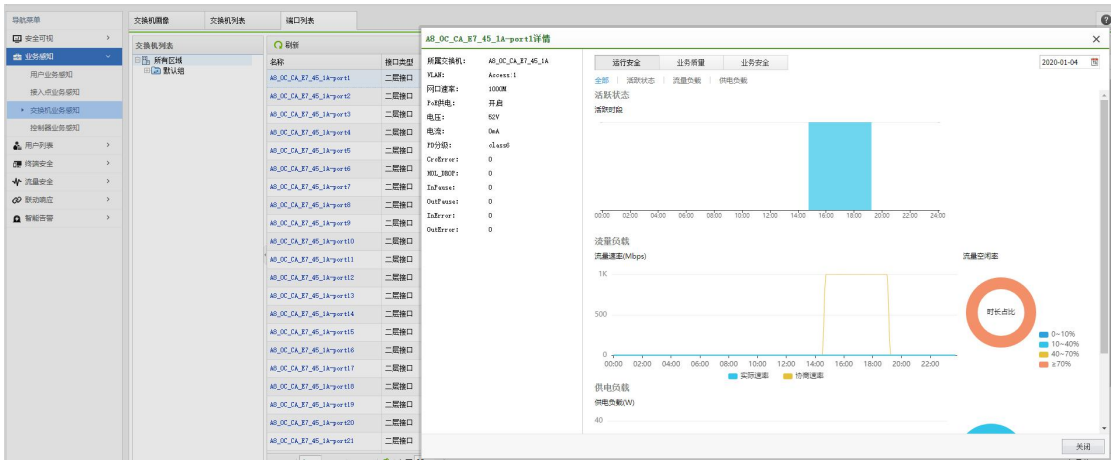
3.2.2. 交换机列表

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。



3.2.3. 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。

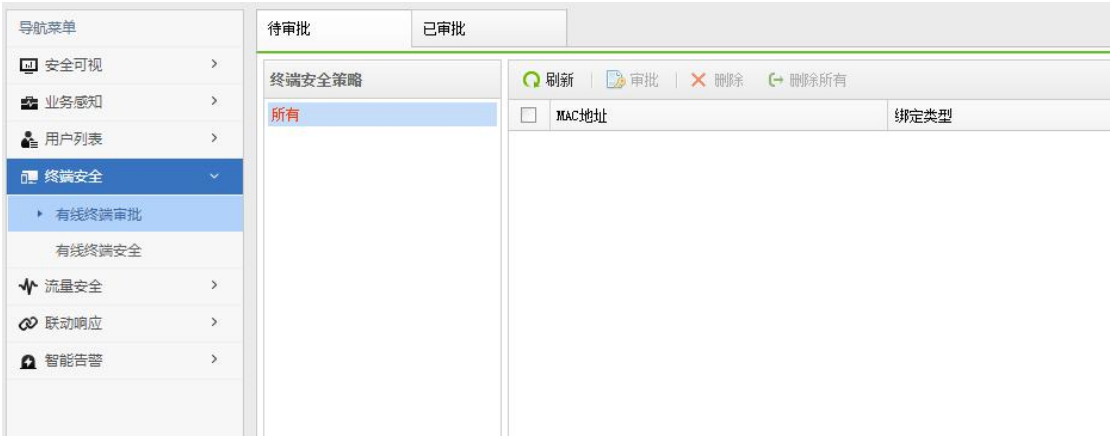


3.3. 终端安全

3.3.1. 有线终端审批

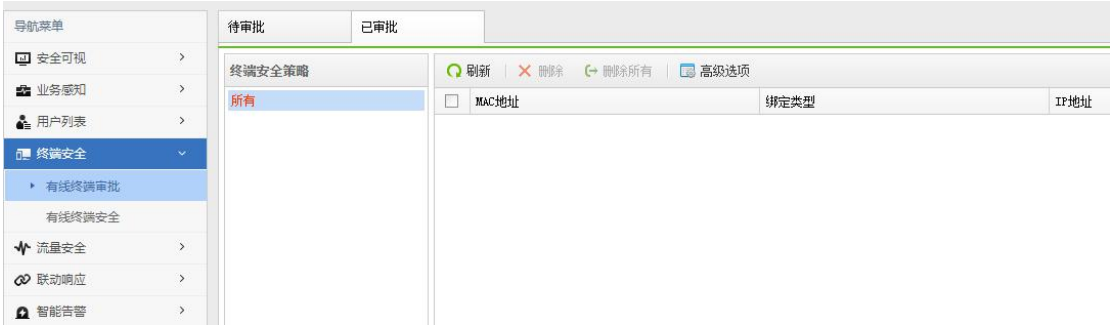
3.3.1.1. 待审批

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。



3.3.1.2. 已审批

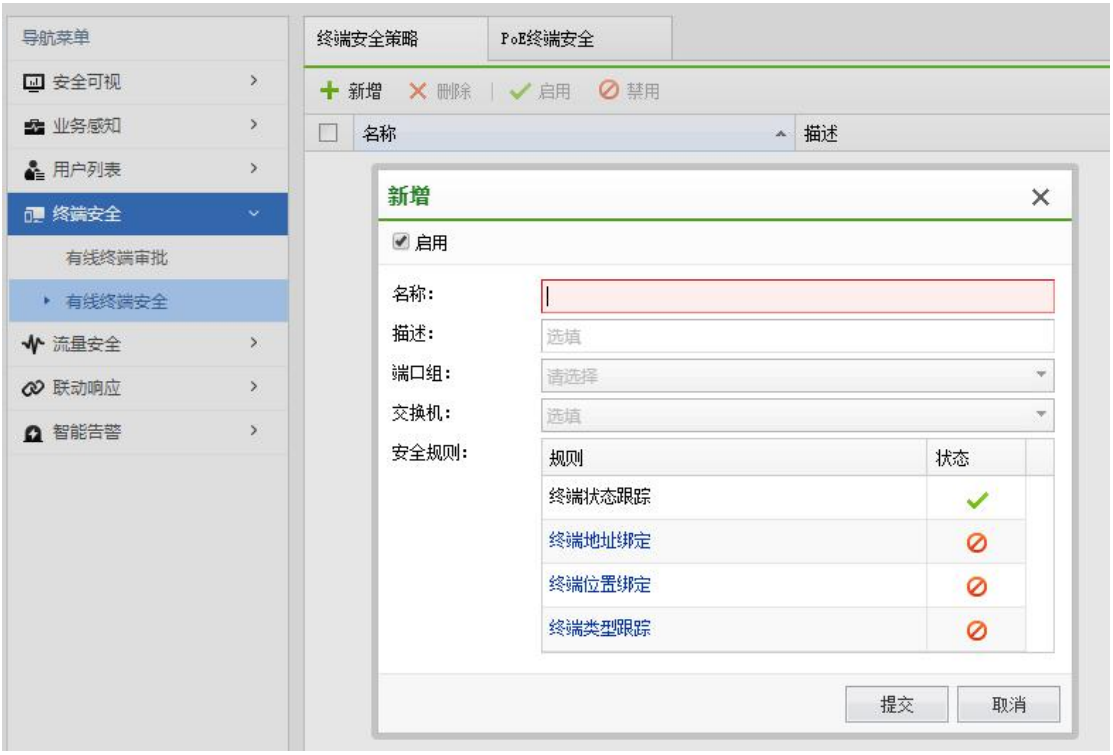
已审批的终端对应关系进入已审批列表，并放通流量。默认老化时间为永不老化，支持配置自定义老化时间。



3.3.2. 有线终端安全

3.3.2.1. 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

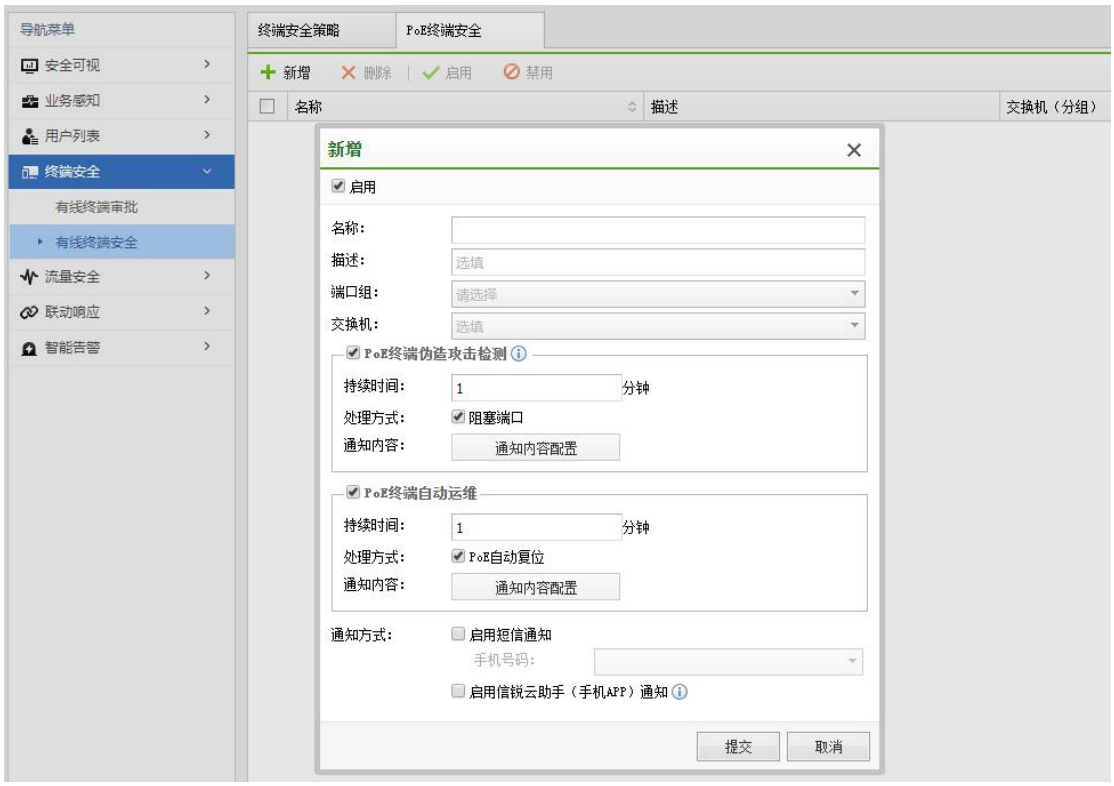
用于绑定终端和端口，实现监管端口下联设备的功能；可启用自动审批并设置审批数量来实现批量操作的自动化，也可手动审批。

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。

3.3.2.2. 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。

3.4. 流量安全

3.4.1. 流量劫持防御

3.4.1.1. 交换机 ARP 防御

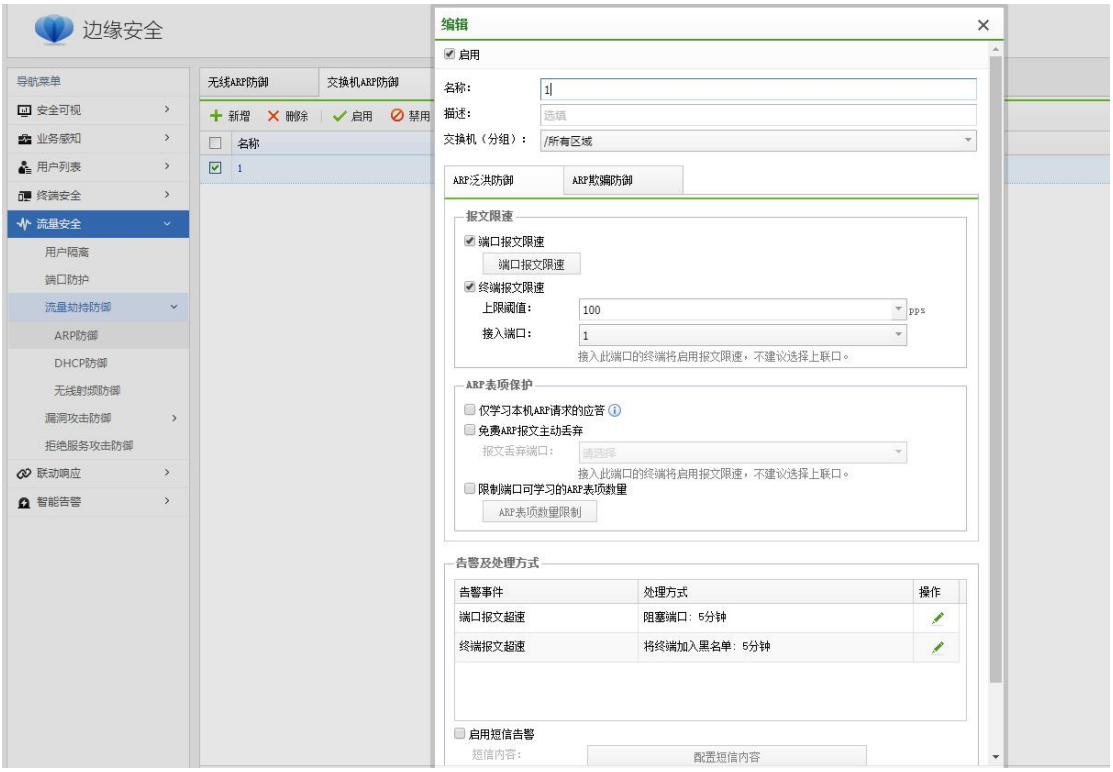
ARP 安全是针对 ARP 攻击的一种安全特性，它通过一系列对 ARP 表项学习和 ARP 报文处理的限制、检查等措施来保证网络设备的安全性。ARP 安全特性不仅能够防范针对 ARP 协议的攻击，还可以防范网段扫描攻击等基于 ARP 协议的攻击。

3.4.1.1.1. 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

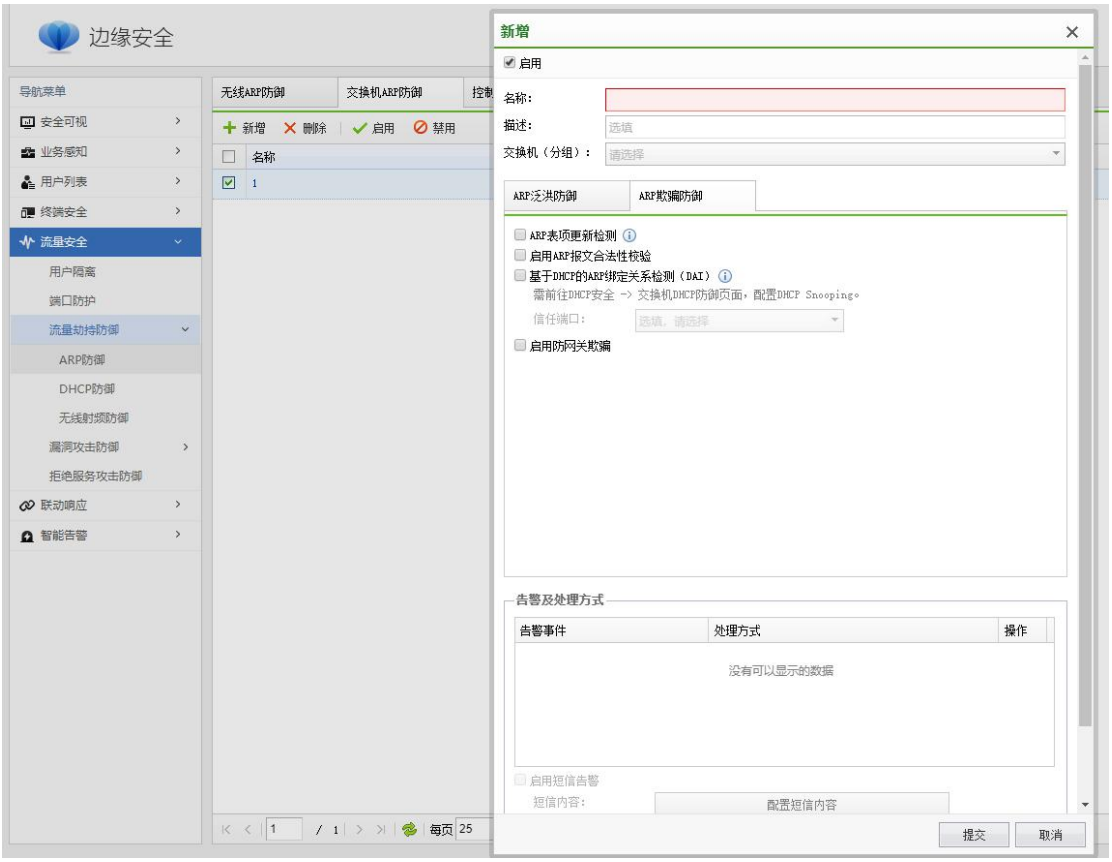
设备接口只能学习到设定的最大动态 ARP 表项数目。这可以防止当一个接口所接入的某一台用户主机发起 ARP 攻击时整个设备的 ARP 表资源都被耗尽。

3.4.1.1.2. 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。

3.4.1.2. 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。

3.4.1.2.1. DHCP 泛洪防御

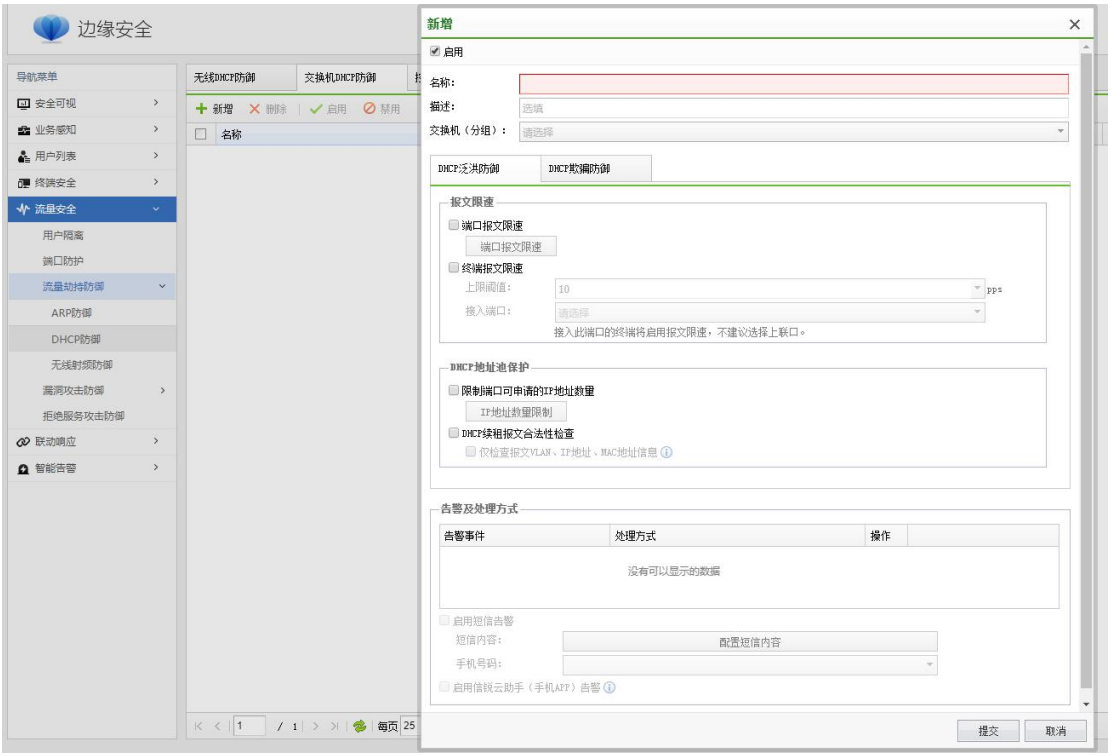
DHCP 泛洪攻击也叫拒绝服务攻击 DoS（Denial of Service），主要存在以下几种场景：

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。

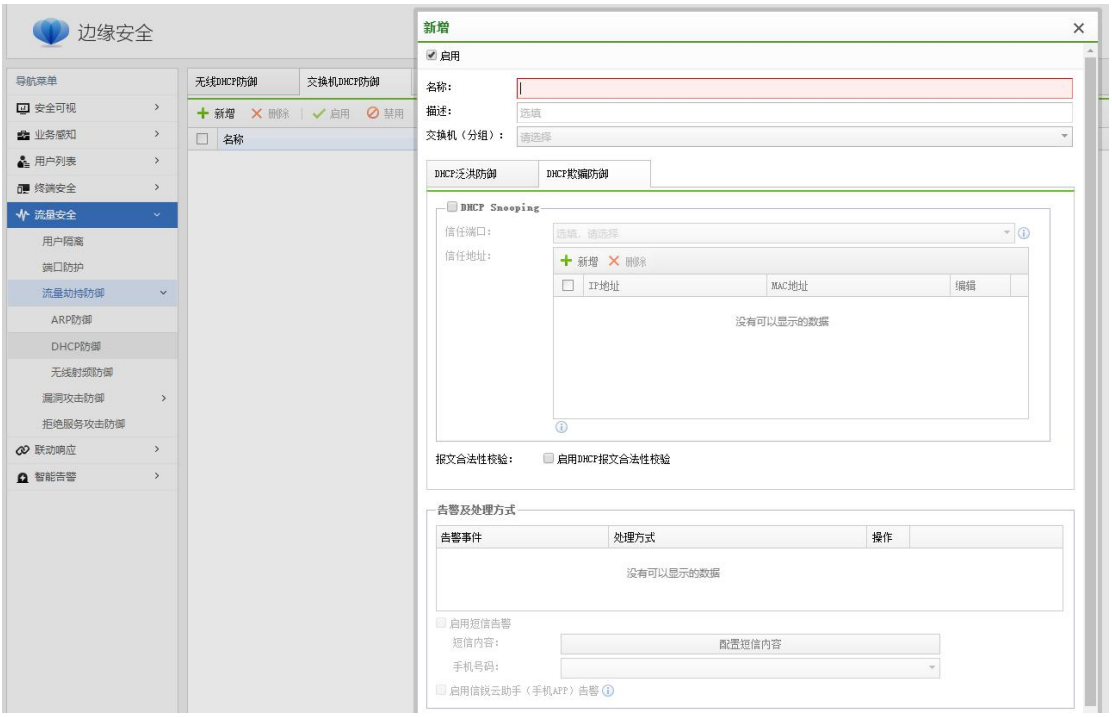
DHCP 续租报文合法性检查

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。

3.4.1.2.2. 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。

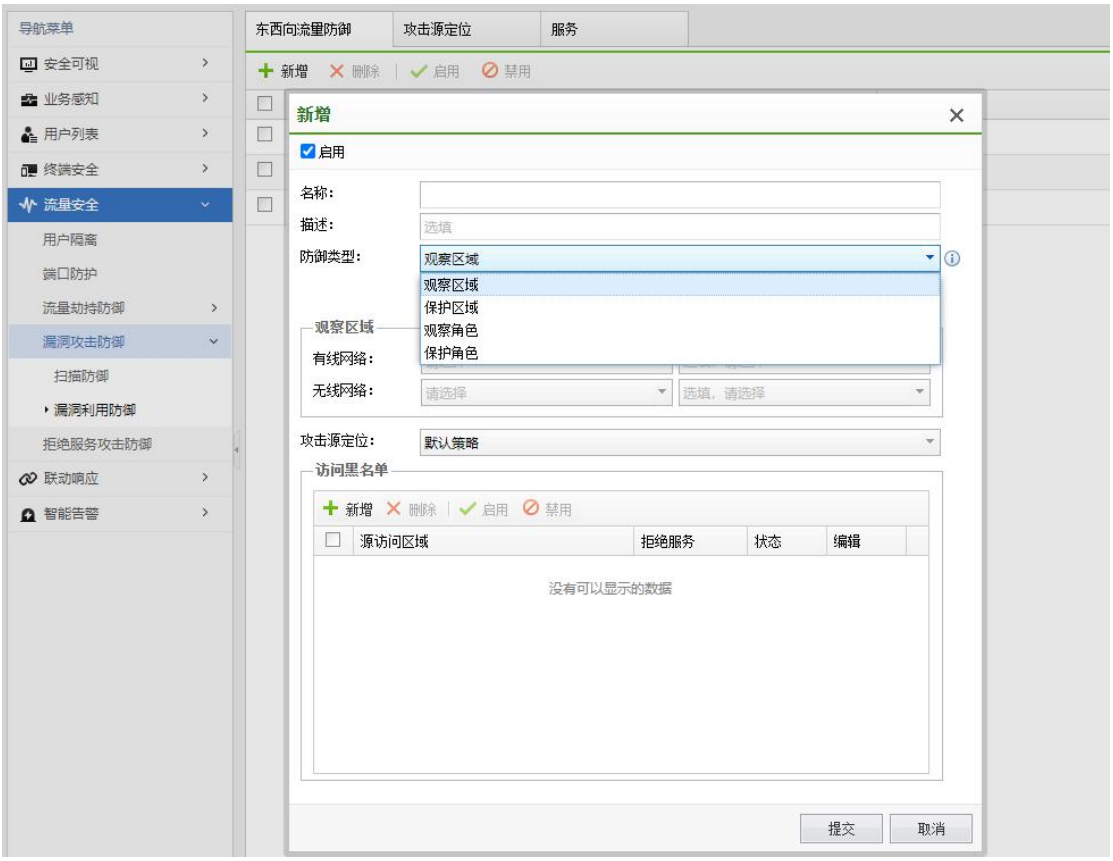
信任 MAC 地址是指当 DHCP 响应报文的源 MAC 地址与配置项相匹配时，允许报文通过。

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。

3.4.2. 漏洞攻击防御

3.4.2.1. 漏洞利用防御

3.4.2.1.1. 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

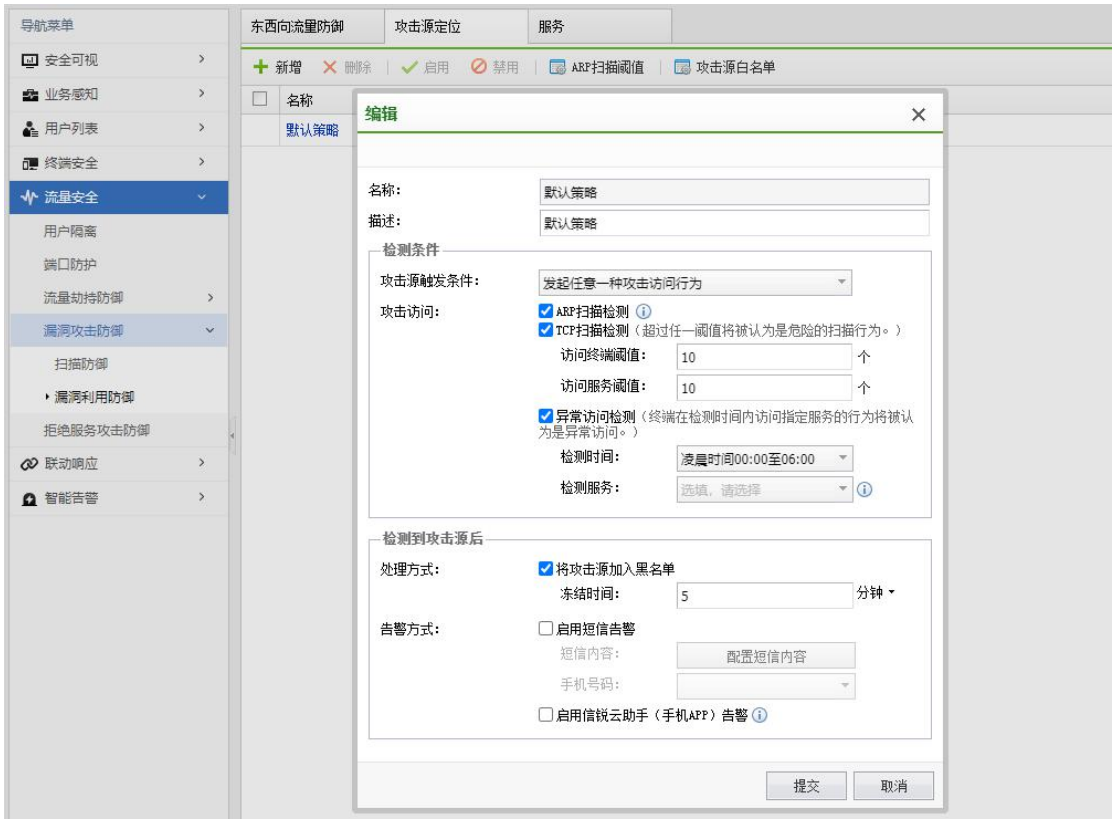
可设置黑名单，拒绝源访问区域的终端访问信任区域的指定服务，源访问区域可以是所有区域，也可以是指定区域。

（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。

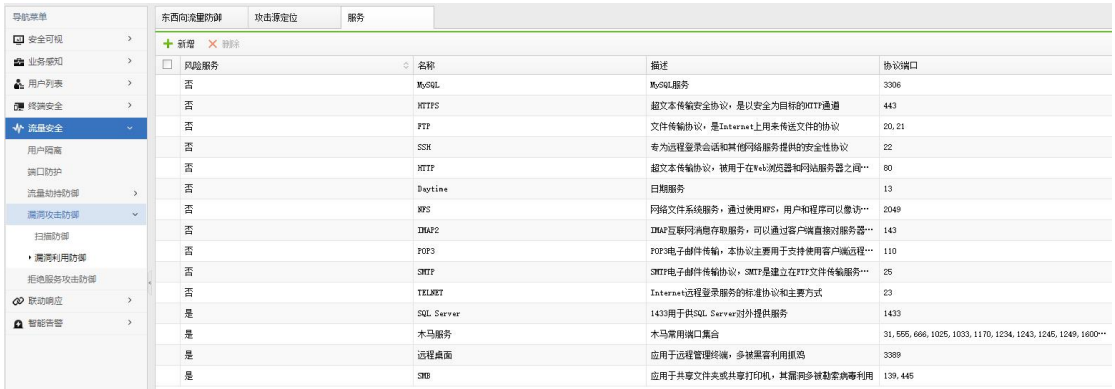
3.4.2.1.2. 攻击源定位

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。



3.4.2.1.3. 服务

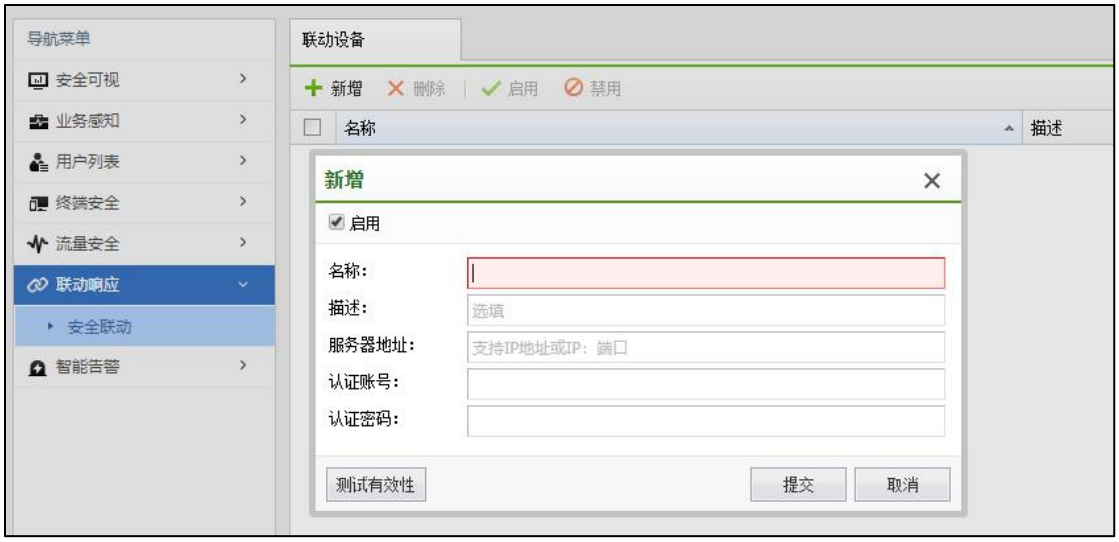
可设置白名单，允许源访问区域的终端访问保护区域的指定服务，源访问区域可以是所有区域，也可以是指定区域。



3.5. 联动响应

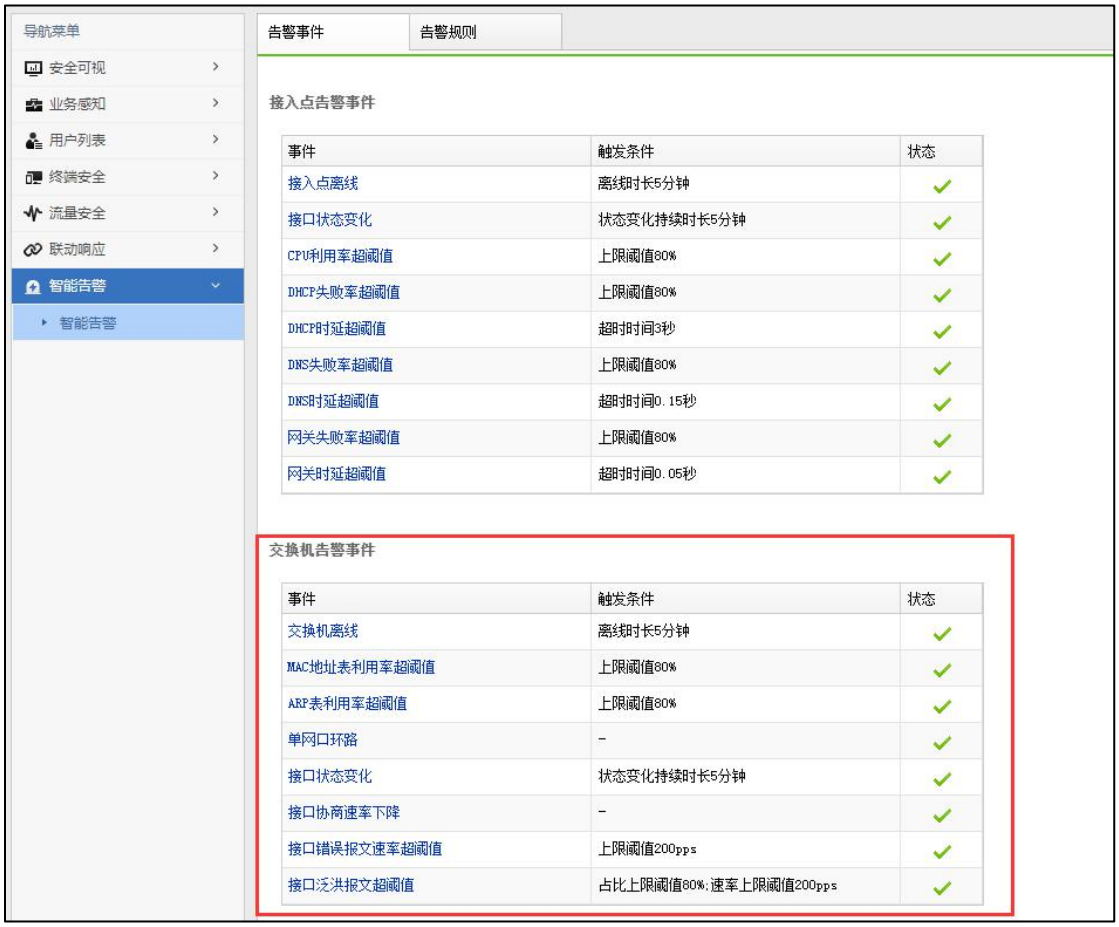
3.5.1. 安全联动

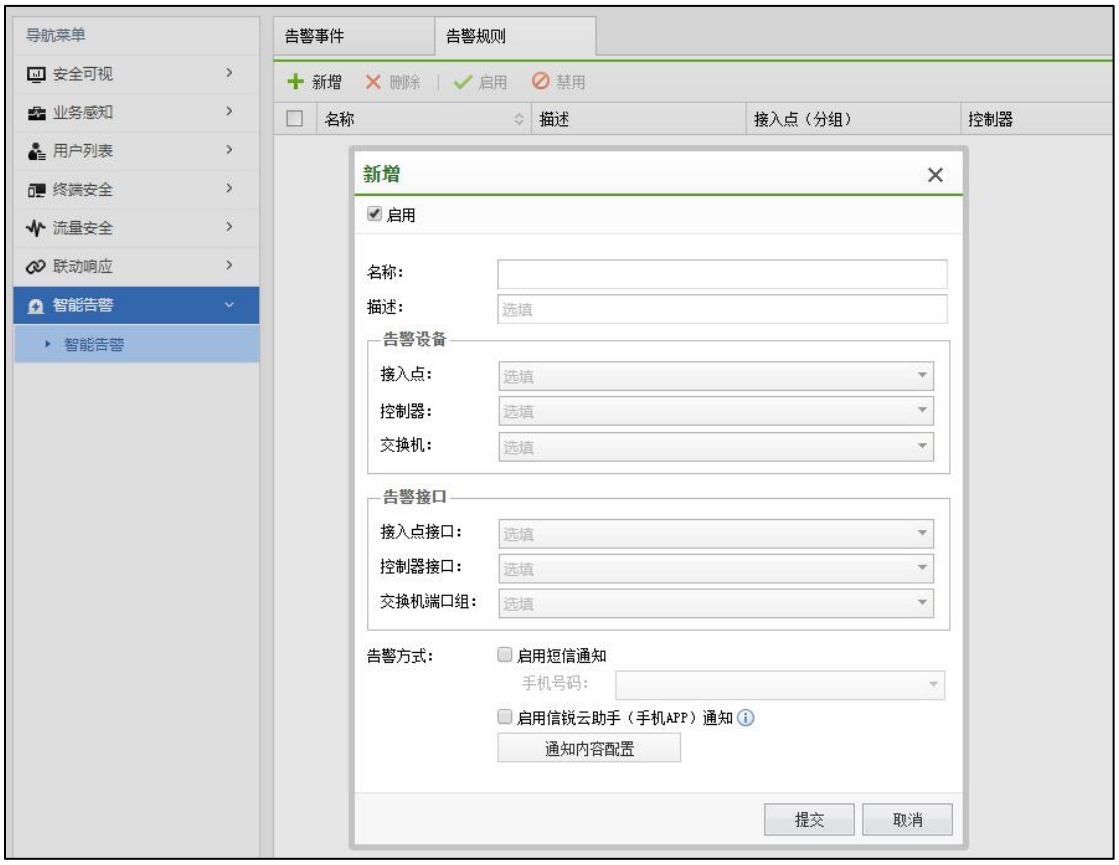
支持联动深信服安全设备进行用户安全可视化和内网边缘安全管理。



3.6. 智能告警

可通过配置相关告警规则，当安视交换机触发配置的事件时，进行短信或云助手 APP 通知管理员。


导航菜单
安全可视
业务感知
用户列表
终端安全
流量安全
联动响应
智能告警
智能告警
告警事件
告警规则
接入点告警事件
事件 触发条件 状态
接入点离线 离线时长5分钟
接口状态变化 状态变化持续时长5分钟
CPU利用率超阈值 上限阈值80%
DHCP失败率超阈值 上限阈值80%
DHCP时延超阈值 超时时间3秒
DNS失败率超阈值 上限阈值80%
DNS时延超阈值 超时时间0.15秒
网关失败率超阈值 上限阈值80%
网关时延超阈值 超时时间0.05秒
交换机告警事件
事件 触发条件 状态
交换机离线 离线时长5分钟
MAC地址表利用率超阈值 上限阈值80%
ARP表利用率超阈值 上限阈值80%
单网口环路 -
接口状态变化 状态变化持续时长5分钟
接口协商速率下降 -
接口错误报文速率超阈值 上限阈值200pps
接口泛洪报文超阈值 占比上限阈值80%;速率上限阈值200pps


导航菜单
安全可视
业务感知
用户列表
终端安全
流量安全
联动响应
智能告警
智能告警
告警事件
告警规则
新增
删除
启用
禁用
名称
描述
接入点（分组）
控制器
新增
启用
名称:
描述:
选填
告警设备
接入点:
选填
控制器:
选填
交换机:
选填
告警接口
接入点接口:
选填
控制器接口:
选填
交换机端口组:
选填
告警方式:
启用短信通知
手机号码:
启用信锐云助手（手机APP）通知
通知内容配置
提交
取消

第 4 章 附录

4.1. 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：

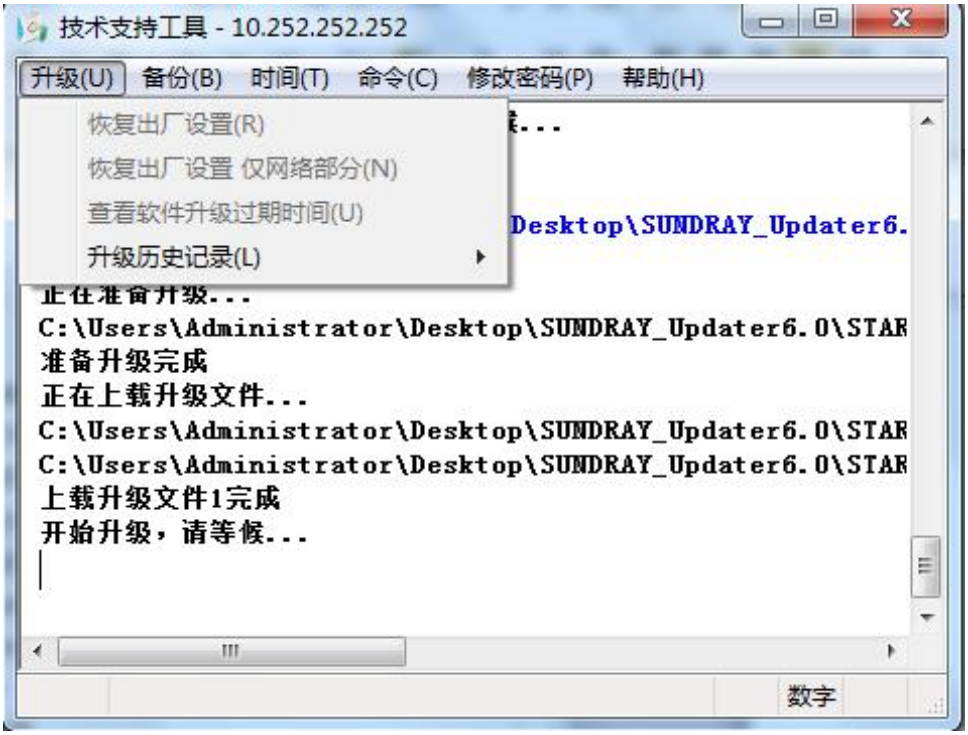
选择从本地加载升级包，点击浏览，选择下载到本地的相应升级包，然后点击下一步，显示当前升级包的基本信息，确认无误后，点击开始升级进行升级操作，界面如下：

升级完成后，设备升级状态里会显示“升级成功”，界面如下：

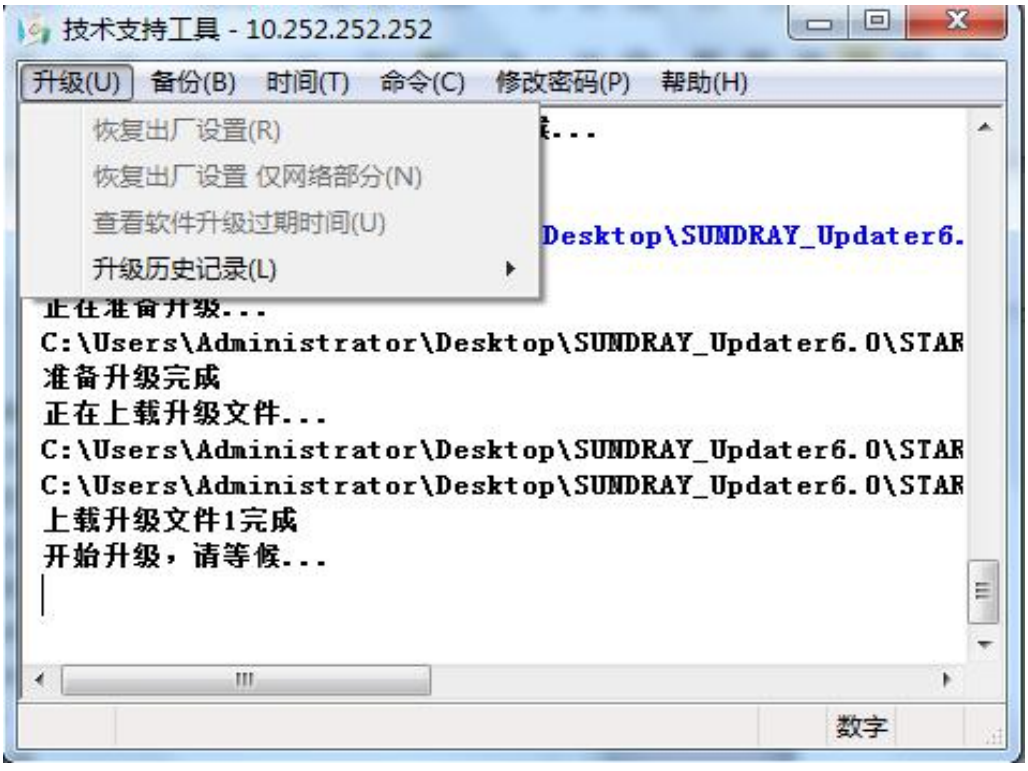
1．升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如需升级请联系信锐技术客户服务部。

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：



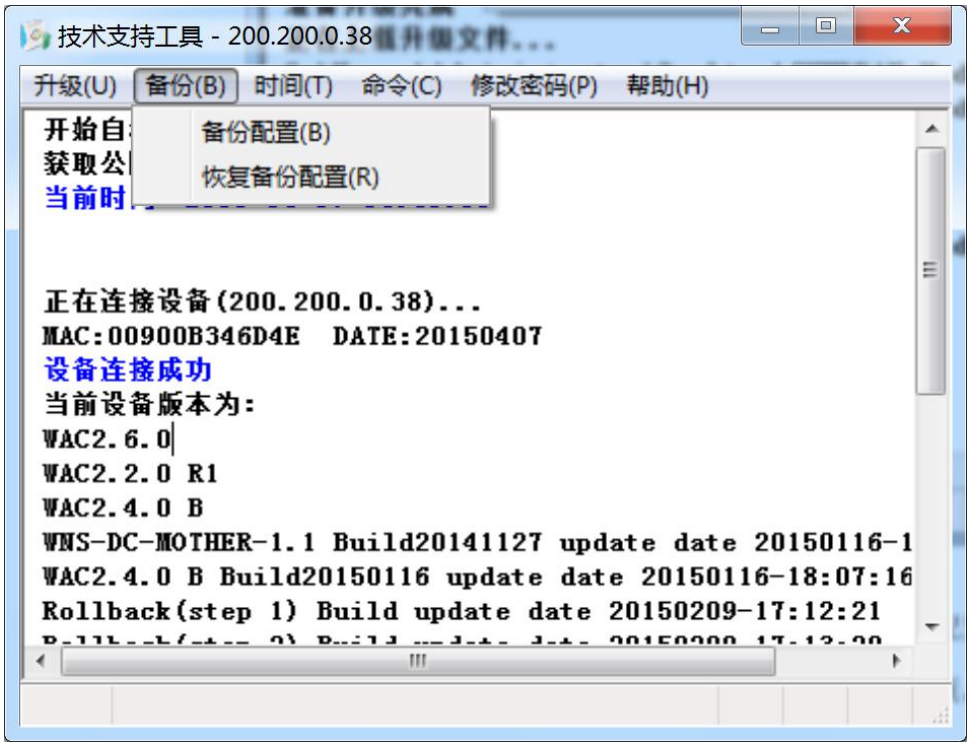
[恢复出厂设置]：用于将 SUNDRAY 硬件设备恢复到默认配置，需要通过加载升级包将设备恢复出厂设置。

[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。

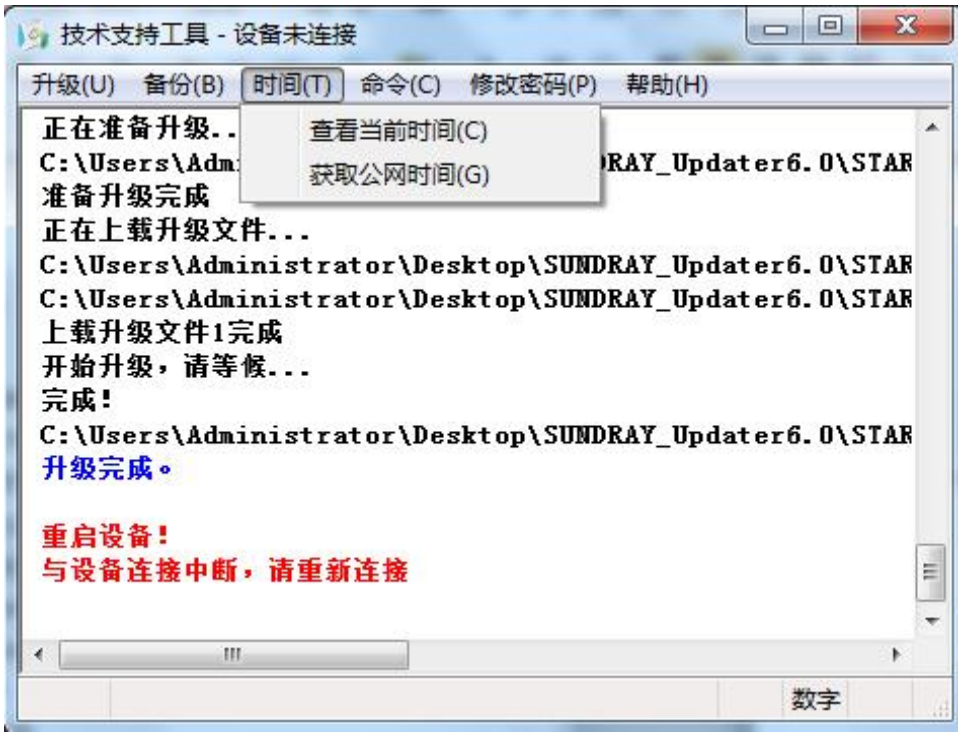
『备份』：包括备份配置、恢复备份配置选项，如下图：



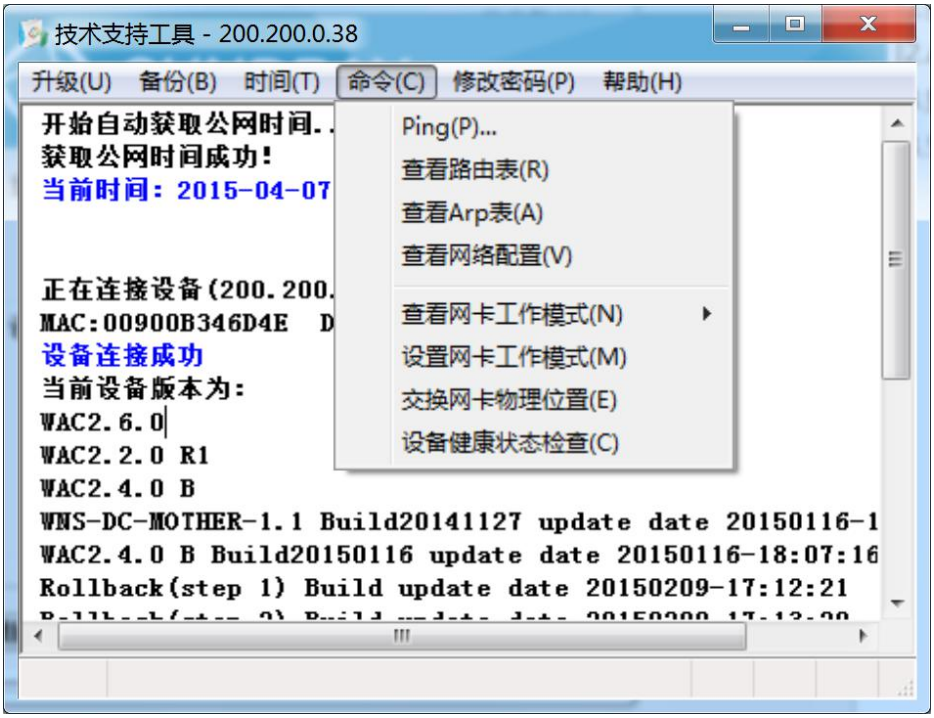
[备份配置]：将设备现有的配置信息进行备份。

[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。

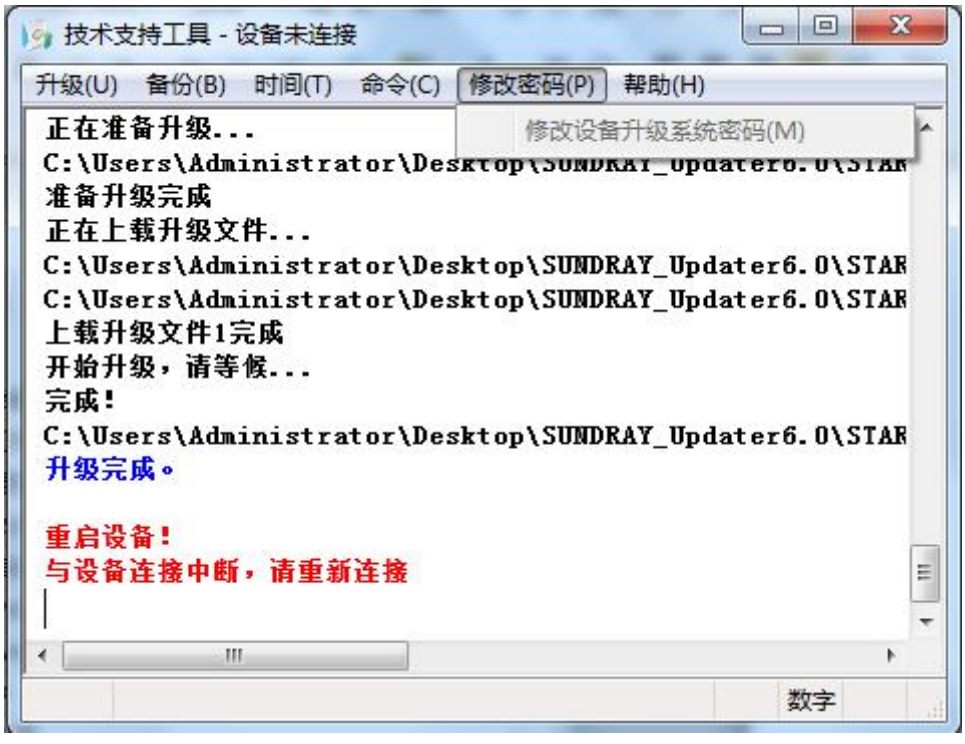
[查看网卡工作模式]：查看设备各网卡的工作模式。

[设置网卡工作模式]：NAC 产品线该功能不可用。

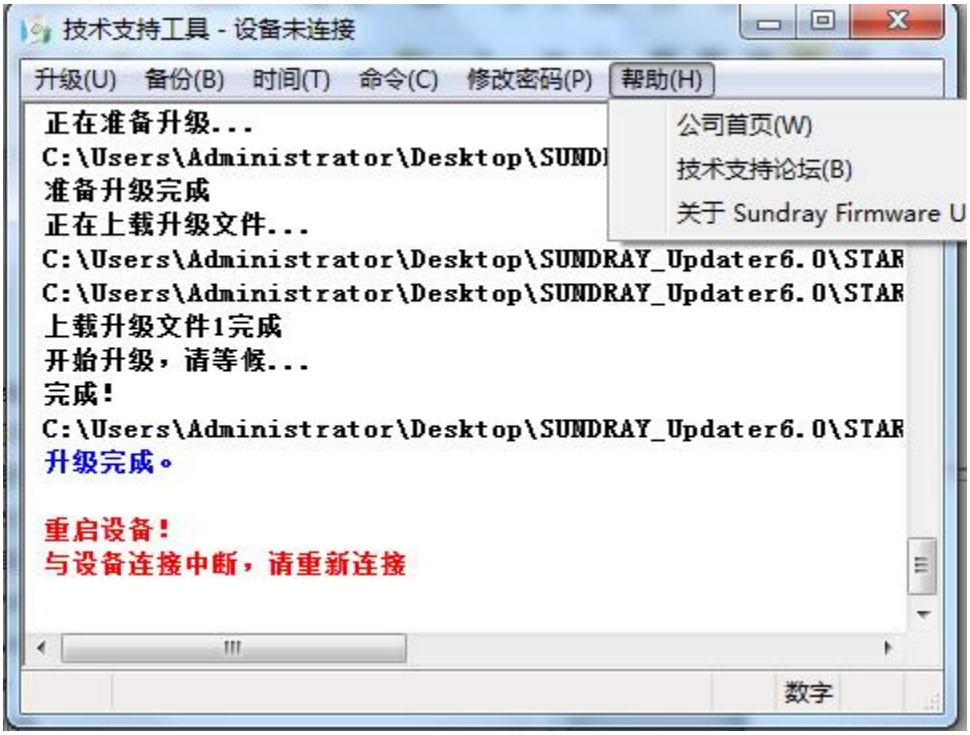
[交换网卡物理位置]：NAC 产品线，该功能不可用。

[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\SUNDI
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