

安视交换机用户使用手册



目录

第 1 章 NAC 控制台的使用与激活	11
1.1. 登录 WebUI 配置界面	11
1.2. 配置和使用	12
1.3. 交换机的激活方式	14
第 2 章 WLAN 控制器&NAC 安视交换机基础配置功能	18
2.1. 安视交换机帮助文档	18
2.2. 系统状态	19
2.2.1. 运行状态	19
2.2.1.1. CPU 和内存使用率	20
2.2.2. 流控状态	20
2.2.3. 在线用户	22
2.2.4. 交换机状态	24
2.2.5. 流量排行	25
2.2.6. 黑名单	26
2.2.7. DHCP 服务	28
2.3. 交换机产品简介	29
2.4. 交换机管理	29

2.4.1. 交换机.....	30
2.4.1.1. 发现新交换机.....	30
2.4.1.2. 设备替换.....	32
2.4.1.3. 交换机.....	33
2.4.2. VLAN 配置	61
2.4.3. 链路聚合.....	65
2.4.4. 防环路配置.....	66
2.4.5. 链路高可用.....	68
2.4.6. 端口列表.....	70
2.4.7. 组播管理.....	73
2.4.8. ACL 策略.....	73
2.4.9. 服务质量 Qos.....	75
2.4.10. DHCP Snooping.....	75
2.4.11. 报文镜像.....	76
2.4.12. 跨设备链路聚合.....	77
2.4.13. 供电配置.....	78
2.5. 控制器有线配置.....	80
2.5.1. 接口管理.....	80

2.5.1.1. 物理接口.....	80
2.5.1.2. 端口聚合.....	83
2.5.1.3. VLAN 接口.....	84
2.5.2. 网络配置.....	85
2.5.2.1. 静态路由.....	86
2.5.2.2. 网络 IP 组.....	87
2.5.2.3. 策略路由.....	87
2.5.2.4. SNAT 地址池.....	88
2.5.2.5. 地址转换.....	88
2.5.2.6. DNS.....	90
2.5.3. 线路带宽.....	90
2.5.4. 有线认证（基于控制器）.....	91
2.5.4.1. 接口区域.....	92
2.5.4.2. 认证策略.....	92
2.5.4.3. 认证类型.....	93
2.5.5. 有线认证应用场景及其优势介绍.....	94
2.5.5.1. 交换机支持有线认证.....	94
2.5.5.2. 支持无线网络异构.....	94

2.5.5.3. 有线无线一体化.....	95
2.5.5.4. 实例一.有线 web 认证(二维码审核).....	95
2.5.5.5. 实例二. 802.1X 认证.....	102
2.6. 边缘安全配置.....	109
2.6.1. 场景一.准确识别终端和网络资产统计.....	112
2.6.2. 场景二.终端防替换与防冒接入(终端地址绑定).....	113
2.6.3. 场景三. 终端防替换与防冒接入(终端位置绑定).....	115
2.6.4. 场景四.禁止共享网络与终端类型校验.....	116
2.7. DHCP 功能改进.....	118
2.7.1. 解决手动配置设备网络过于繁琐的问题.....	118
2.7.1.1. 场景 1: 和设备同二层的终端需要支持即插即用.....	118
2.7.1.2. 场景 2: 和设备跨三层的终端需要支持即插即用.....	121
2.7.1.3. 场景 3: 利用客户已有 DHCP 服务器, 节约成本.....	124
2.7.2. 解决接口无法分配不同网段 IP 地址的问题.....	126
2.7.2.1. 场景 1: 不同设备获取不同网段的 IP.....	126
2.7.2.2. 场景 2: 根据 option82 自动携带的用户属性精细化分配 IP.....	128
2.7.3. 解决管理员网络运维复杂的问题.....	131
2.7.3.1. 场景 1: 管理员定期检视网络状态.....	131

2.7.3.2. 场景 2: 管理员定位网络问题.....	131
2.7.4. 解决用户接入无法上网的问题.....	132
2.7.4.1. 场景 1: 地址池无可分配 IP 地址时清除租约	132
2.7.4.2. 场景 2: 避免终端发生 IP 冲突	133
第 3 章 设备支持 IPv6	134
3.1. 无线设备支持 IPv6.....	134
3.1.1. 用户网络升级 IPv6, 无线网络支持 IPv6 部署.....	134
3.1.1.1. 场景 1 无线设备二层部署, AP 使用 IPv6 地址上线终端集中转发 无线用户获取 IPv6 地址.....	134
3.1.1.2. 场景 2 无线设备跨三层部署, AP 使用 IPv6 地址上线到控制器	139
3.1.1.3. 场景 3 控制器作为中继, 终端用户通过控制器获取上级 DHCPv6 服务器分配的地址.....	142
3.1.2. 用户部署控制器为网关接入运营商 IPv6 网络.....	145
3.1.2.1. 场景 1 控制器上行出口自动获取 IPv6 地址, 下接交换机、接入 点及终端用户使用 IPv6 地址通信.....	145
3.2. 交换机支持 IPv6.....	149
3.2.1. 用户 IPv6 网络部署三层交换机.....	149
3.2.1.1. 场景 1 用户在 IPv6 网络中使用控制器统一管理交换机设备...149	
3.2.1.2. 场景 2 部署交换机作为网关设备, 转发 IPv6 数据.....	154

3.2.1.3. 场景 3 客户端接入交换机从外置的 DHCPv6 服务器获取网络配置	157
3.2.1.4. 场景 4 胖模式交换机接入 IPv6 网络转发数据	161
第 4 章 交换机支持 VRRP	166
4.1.1. 场景 1: 对三层核心交换机进行冗余备份, 提高网络可靠性	166
4.1.2. 场景 2: 对核心交换机冗余备份, 通过生成树协议进行链路冗余, 提高网络可靠性	171
4.1.3. 场景 3: 对核心交换机冗余备份, 通过 MLAG 进行设备和链路冗余提高网络可靠性	178
4.1.4. 场景 4: 部署交换机冗余备份组, 使用同步组功能较少交换机 CPU 消耗	184
4.1.5. 场景 5: 部署交换机冗余备份组, 使用代管组功能较少交换机 CPU 消耗	185
第 5 章 OSPF 配置	189
5.1. 企业快速配置 OSPF 网络实现设备间网络互通	189
5.2. 企业 OSPF 网络引入外部路由(路由引入)	191
5.3. 企业 OSPF 网络区域 1 不接收区域 2 的路由(路由白名单)	194
5.4. 企业网络中存在多条前缀有重叠的路由(路由聚合)	196
5.5. 企业 OSPF 网络中配置虚连接	200
5.6. 企业 OSPF 网络中配置特殊区域	202

5.7. 企业部署 OSPF 网络与 BFD 联动	204
5.8. 企业部署 OSPF 网络，并配置认证方式	207
5.9. 企业部署 OSPF 网络，其他高级选项功能配置	211
5.10. 企业部署 OSPF 与 RIP 网络，更改管理距离而更改选路	214
5.11. 企业部署 OSPF 网络，网络故障进行故障诊断	215
第 6 章 静态路由	218
6.1. 企业配置静态路由，进行链路检测	218
6.2. 企业对三层核心交换机进行路由备份，提高网络可靠性	219
第 7 章 策略路由	222
7.1. 企业希望通过策略路由为不同的部门划分不同的服务器	222
7.2. 企业部署策略路由，并希望主链路配置故障后切换到备份链路	223
7.3. 网络管理员部署策略路由根据不同用户控制可访问的网站	225
7.4. 用户策略路由链路故障切换到静态路由，链路恢复后切回策略路由	226
7.5. 用户希望将不同优先级的流量送往不同的服务器	228
第 8 章 链路检测	230
8.1. 用户希望检测交换机到某一 IP 间的多跳三层链路是否正常，且对检测实时性 要求不高	230
8.2. 管理员希望检测两台交换机间的二层链路是否正常	232

8.3. 用户希望检测两台交换机间的三层链路，且对实时性要求较高.....	233
8.4. 管理员希望检测交换机与不支持 BFD 协议设备间的直连三层链路，且对实时性要求较高.....	235
8.5. 用户希望通过链路检测来检查链路间的网络动荡.....	237
第 9 章 RIP 配置	240
9.1. 企业快速配置 RIP 网络实现设备间网络互通	240
9.2. 企业 RIP 网络引入外部路由(路由引入).....	242
9.3. 企业 RIP 网络不接收某些路由(路由白名单).....	244
9.4. 企业部署 RIP 网络与 BFD 联动	247
9.5. 企业部署 RIP 网络，并配置认证方式	249
9.6. 企业部署 RIP 网络，其他高级选项功能配置	253
9.7. 企业部署 RIP 网络，网络故障进行故障诊断	256
9.8. 控制器系统维护.....	258
9.8.1. 序列号.....	259
9.8.2. 系统更新.....	259
9.8.2.1. 自动更新.....	259
9.8.2.2. 设备升级.....	260
9.8.3. 日志查看.....	261

9.8.3.1. 系统日志.....	261
9.8.3.2. 管理日志.....	262
9.8.3.3. 安全日志.....	263
9.8.3.4. 用户认证日志.....	263
9.8.4. 故障排除.....	264
9.8.5. 重启及格式化.....	265
9.8.6. 命令控制台.....	265
第 10 章 附录.....	268
10.1. SUNDRAY 设备升级系统的使用.....	268

第1章 NAC 控制台的使用与激活

1.1. 登录 WebUI 配置界面

WLAN-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>，出现一个如下图所示的安全提示：



点击[继续浏览此网站](#)后出现以下的登录界面：

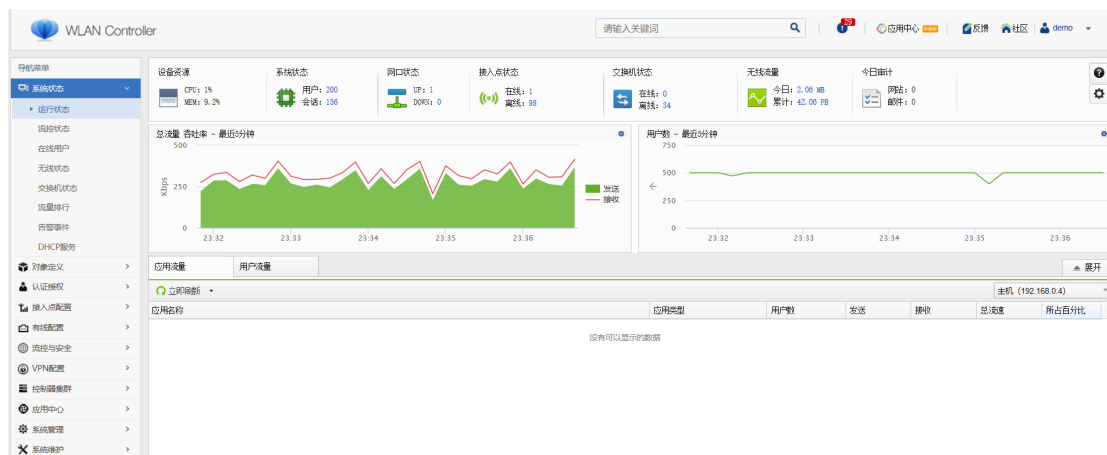


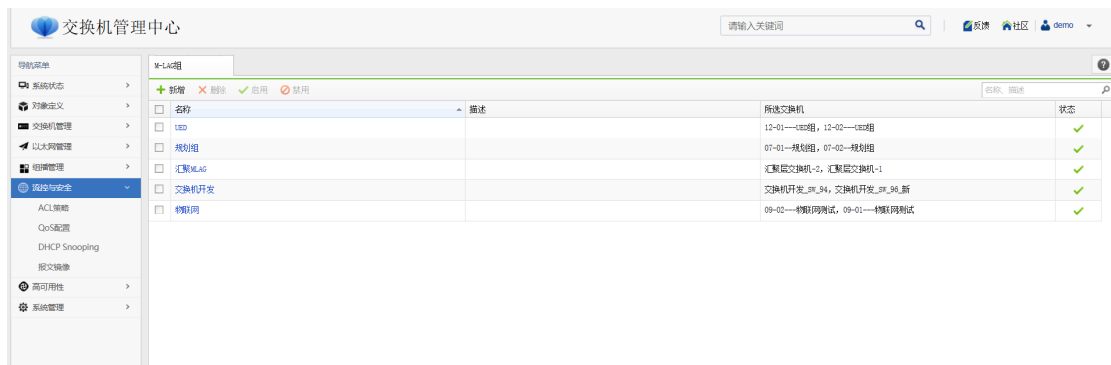
在登陆框输入『账号』和『密码』，点击**登录**按钮即可登录 WLAN 设备进行配置，出厂情况下的用户名和密码为 admin/admin。

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』、『认证授权』、『交换机管理』、『有线配置』、『流控与安全』、『高可用性』、『组播管理』、『系统管理』、『边缘可视』、『交换机安全』、『系统维护』。





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。

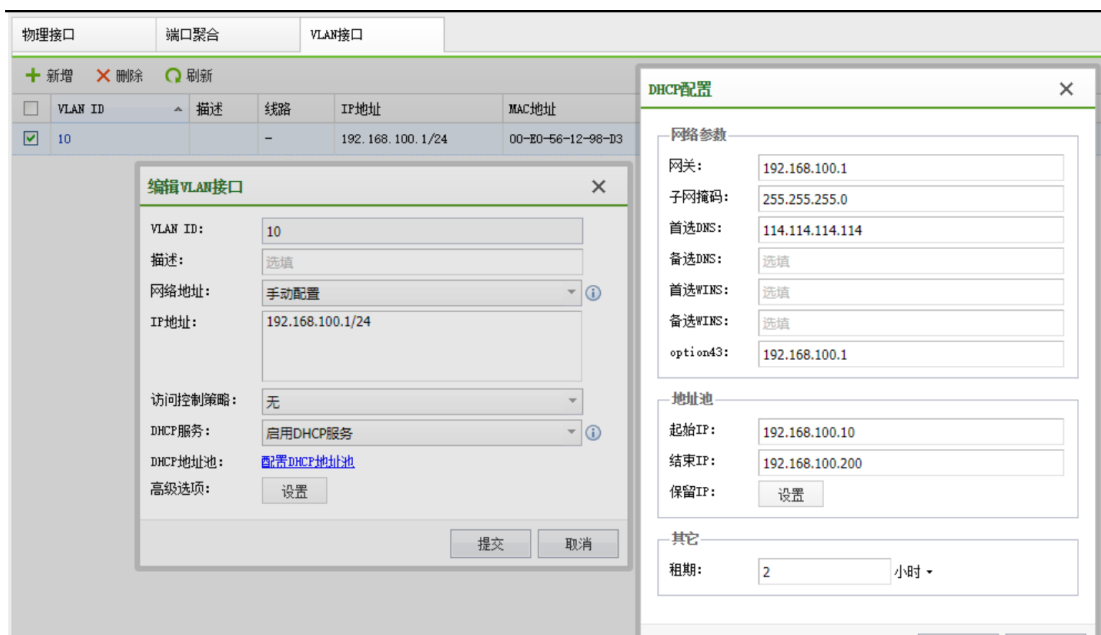
1.3. 交换机的激活方式

拓扑环境：

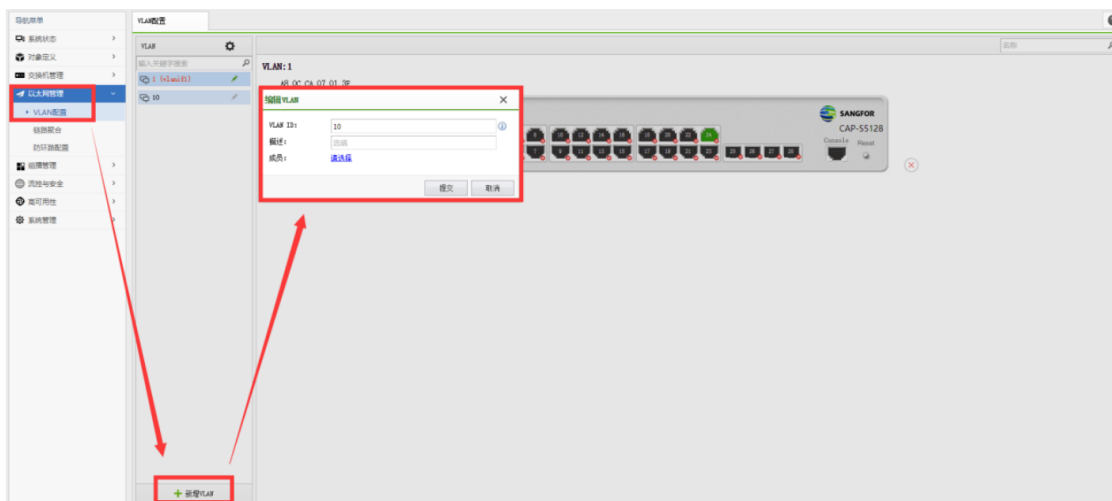


- 1、首先将控制器的接口 EHT1 配置为 trunk，Native VLAN 为 10。并开启 VLAN10 接口，配置 DHCP。

物理接口	端口聚合	VLAN接口							
<input type="checkbox"/> 刷新 <input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用									
网口	IP地址	类型	模式	VLAN	MAC地址	速率	MTU	状态	
<input type="checkbox"/> eth0(管理口)	10.252.252.252/24	三层接口	-		00-E0-4C-12-98-D3	-	1500		
<input type="checkbox"/> eth1	-	二层接口	Trunk	native:10,vlan:1-4094	00-E0-4C-12-98-D2	自动协商 - 1000M full-duplex	1500	<input checked="" type="checkbox"/>	
<input type="checkbox"/> eth2	192.200.254.131/23	三层接口	-		00-E0-4C-12-98-D1	自动协商 - 100M full-duplex	1500	<input checked="" type="checkbox"/>	
<input type="checkbox"/> eth3	-	二层接口	Trunk	native:10,vlan:1-4094	00-E0-4C-12-98-D0	自动协商 - 1000M full-duplex	1500	<input checked="" type="checkbox"/>	
<input type="checkbox"/> eth4	-/-	三层接口	-		00-E0-4C-12-98-CF	-	1500	<input checked="" type="checkbox"/>	
<input type="checkbox"/> eth5	-/-	三层接口	-		00-E0-4C-12-98-CE	-	1500	<input checked="" type="checkbox"/>	



- 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

- (1) 如下图我们将交换机的

的管理 VLAN 改为 10，选择对应的物理接口。

交换机激活
✕

名称:	<input type="text" value="A8_OC_CA_07_01_3F"/>
描述:	<input type="text" value="选填"/>
所属组:	<input type="text" value="/所有区域/默认组"/>
发现控制器IP:	<input type="text" value="192.168.100.1"/>
发现控制器域名:	<input type="text" value="选填"/>
硬件型号:	CAP-S5128
控制隧道保活时间:	<input type="text" value="选填 (秒), 默认使用交换机分组参数"/> ⓘ
webAgent:	<input type="checkbox"/> 启用webAgent发现
M-LAG协议报文转发:	<input type="checkbox"/> 启用M-LAG协议报文转发 ⓘ
功能配置:	<input type="text" value="使用独立配置"/>

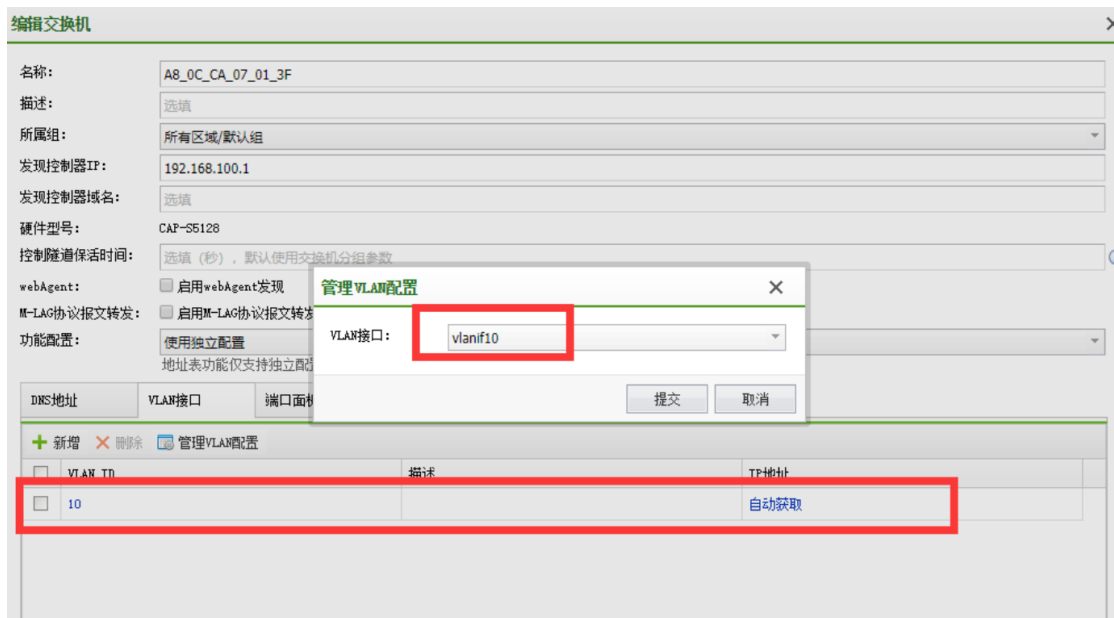
管理VLAN	端口面板	Loopback地址
网络地址:	<input type="text" value="自动获取"/>	
IP地址:	<input type="text"/>	
子网掩码:	<input type="text"/>	
网关:	<input type="text"/>	
首选DNS:	<input type="text"/>	
备选DNS:	<input type="text" value="选填"/>	
管理VLAN:	<input type="text" value="10"/>	
管理VLAN的端口:	<input type="text" value="port24"/>	

(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。



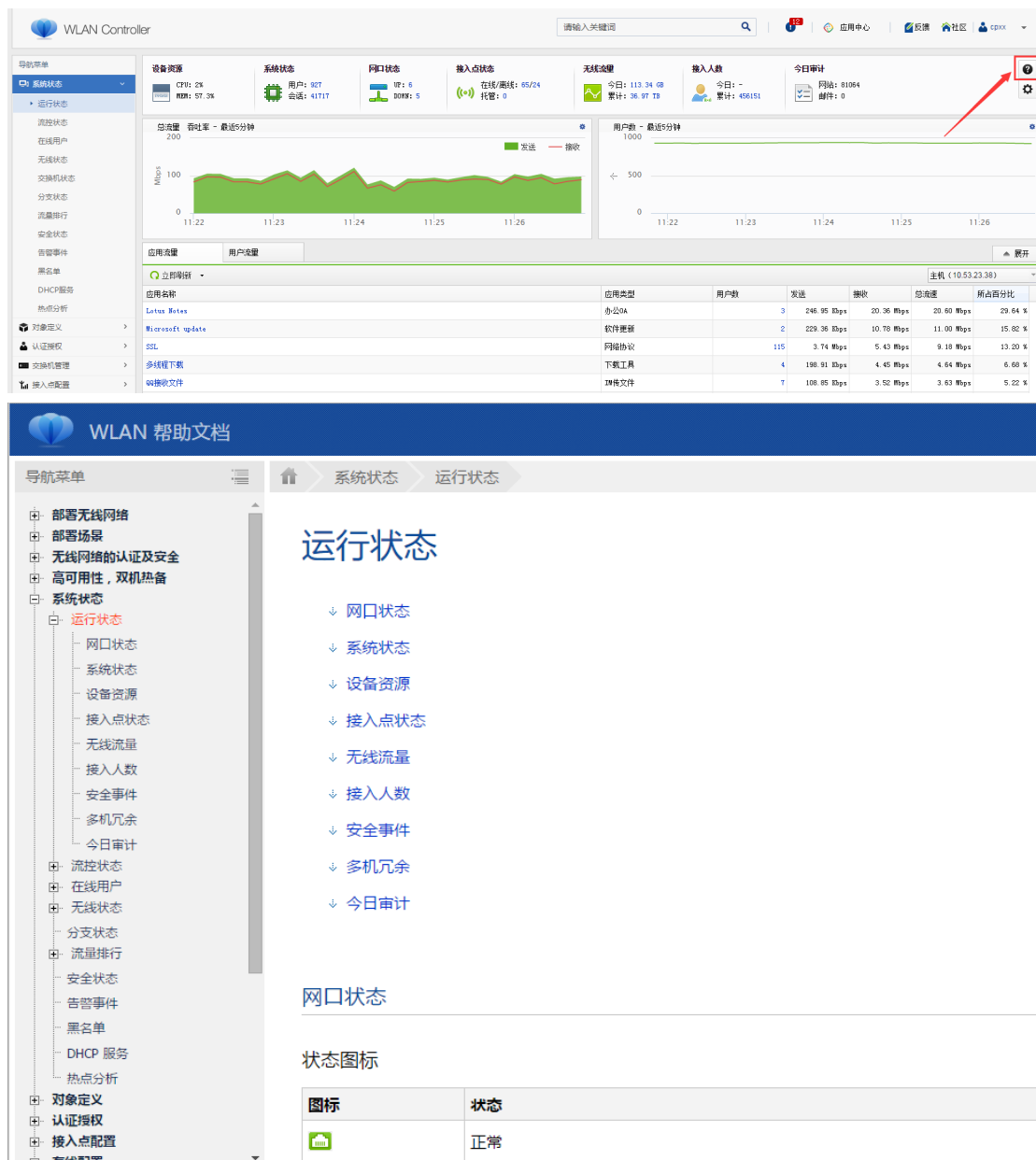
(3) 提交后之后就可以看到设备上线了，同时交换机的配置里面管理 VLAN 为 10，VLAN 接口里面也只有 VLAN 10。



第2章 WLAN 控制器&NAC 安视交换机基础配置功能

2.1. 安视交换机帮助文档

对于 WLAN 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无线 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【运行状态】、【流控状态】、【在线用户】、【交换机状态】、【分支状态】、【流量排行】、【安全状态】、【告警事件】、【黑名单】、【DHCP 服务】、【热点分析】。



2.2.1. 运行状态

『运行状态』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、接口吞吐量、应用流量、用户流量等信息。



2.2.1.1. 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。



2.2.2. 流控状态

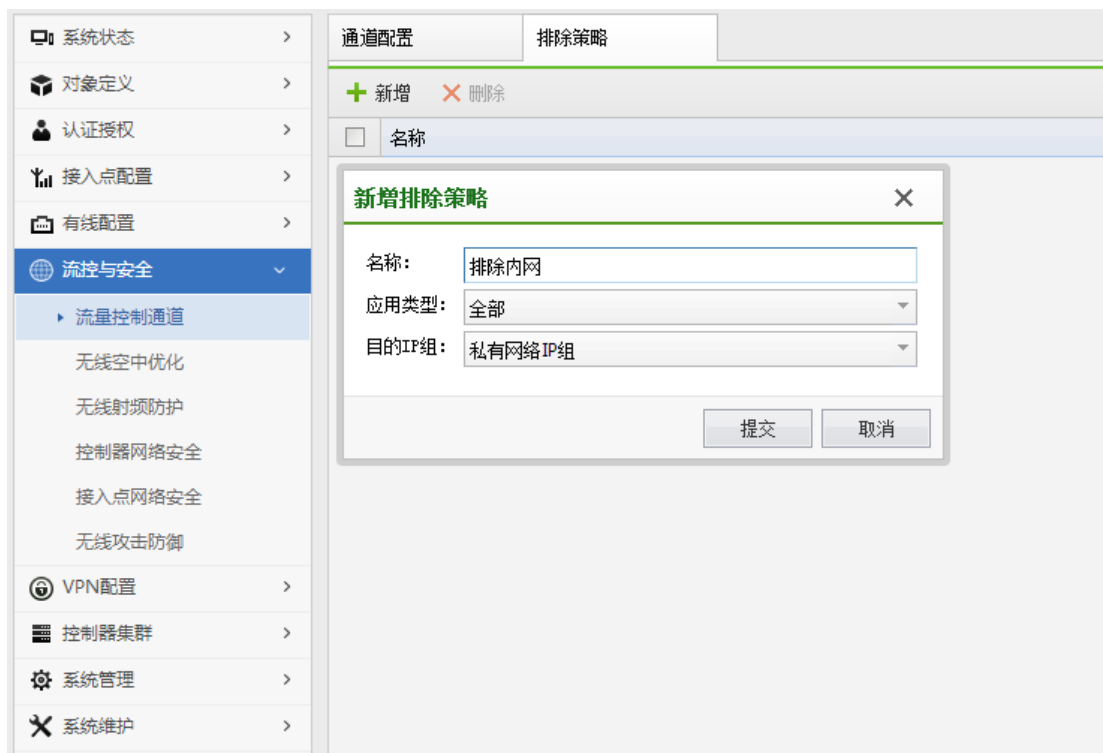
流控状态包含了【通道状态】、【线路状态】、【排除策略】，如下图显示，其中通道状态显示了流控通道配置后，每条通道的实时运行状态与当前配置。

通道状态	线路状态	排除策略						
立即刷新		所有线路						
通道名称	线路	瞬时速率	占用比例	用…	保证带宽	最大带宽	优…	
1楼	wac_0_38…	↑403.96… ↓5.19 M…	↑0.0 % ↓0.5 %	18	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
2楼	wac_0_38…	↑119.79… ↓325.75…	↑0.0 % ↓0.0 %	10	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
3楼	wac_0_38…	↑755.43… ↓844.93…	↑0.1 % ↓0.1 %	11	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
4楼	wac_0_38…	↑330.87… ↓4.55 M…	↑0.0 % ↓0.4 %	13	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
5楼	wac_0_38…	↑61.77 … ↓50.94 …	↑0.0 % ↓0.0 %	8	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	高	
6楼	wac_0_38…	↑31.93 … ↓26.23 …	↑0.0 % ↓0.0 %	3	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
7楼	wac_0_38…	↑2.26 M… ↓22.04 …	↑0.2 % ↓2.2 %	18	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
8楼	wac_0_38…	↑81.52 … ↓266.44…	↑0.0 % ↓0.0 %	9	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
楼顶	wac_0_38…	↑0.00 bps ↓0.00 bps	↑0.0 % ↓0.0 %	0	↑113.78 M… ↓113.78 M…	↑1.00 Gbps ↓1.00 Gbps	中	
默认通道	wac_0_38…	↑62.00 … ↓493.13…	↑0.0 % ↓0.0 %	10	↑0.00 Kbps ↓0.00 Kbps	↑1.00 Gbps ↓1.00 Gbps	低	
默认通道	wac_10_3…	↑0.00 bps ↓0.00 bps	↑0.0 % ↓0.0 %	0	↑0.00 Kbps ↓0.00 Kbps	↑1.00 Gbps ↓1.00 Gbps	低	

线路状态显示了每条线路的当前流量瞬时速率、线路占用比率，和线路带宽。线路状态是需要先在【有线配置】-【线路带宽】根据实际线路情况提前配置并调用，才能在此处正常显示。

通道状态	线路状态	排除策略				
立即刷新						
线路名称	瞬时速率	占用比例	线路带宽			
wac_0_38_接收	↑4.28 Mbps ↓39.32 Mbps	↑0.4 % ↓3.8 %	↑1.00 Gbps	↓1.00 Gbps		
wac_10_38_发送	↑0.00 bps ↓0.00 bps	↑0.0 % ↓0.0 %	↑1.00 Gbps	↓1.00 Gbps		

排除策略显示了在流控功能中，不受流控策略限制的流量状态，需要在【流控与安全】-【流量控制通道】中添加排除策略，才可在此查看到。



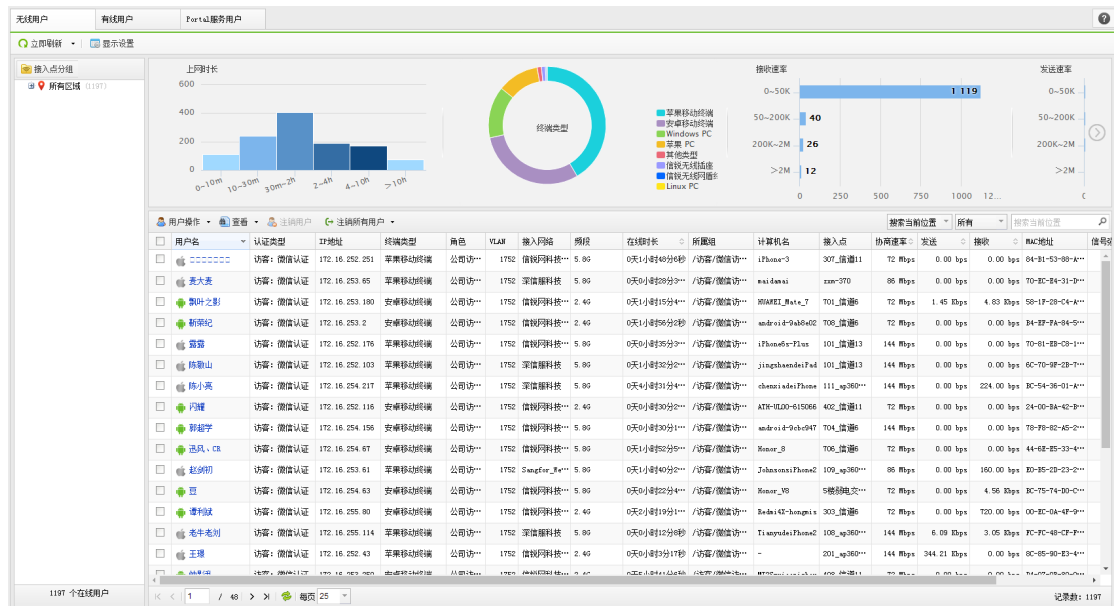
2.2.3. 在线用户

在线用户，可以看到当前接入网络的无线用户信息、有线用户信息以及 portal 服务用户信息。无线用户可以查看到用户名、所属组、认证方式、计算机名、IP 地址、角色、VLAN、

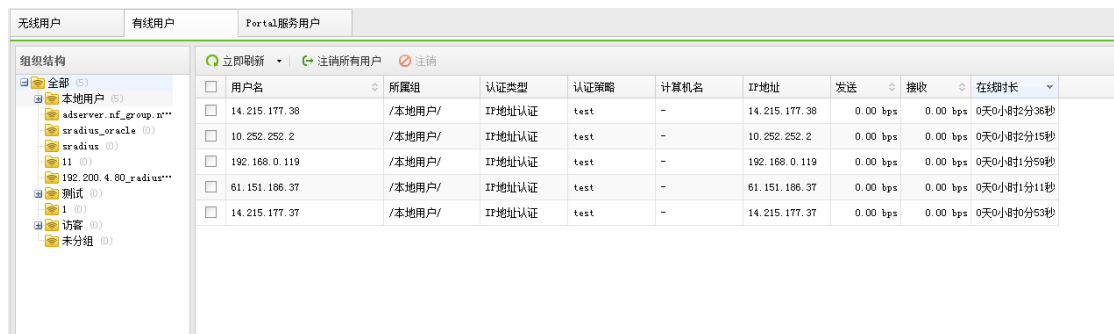
接入网络、协商速率、发送、接收、在线时长、MAC 地址、无线协议、信道号、误码率、重传率、信号强度等各种详细信息。

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



有线用户基本信息，可以查看到有线状态下的用户基本信息。包括用户名、IP 地址，收发流量，在线时长等信息。

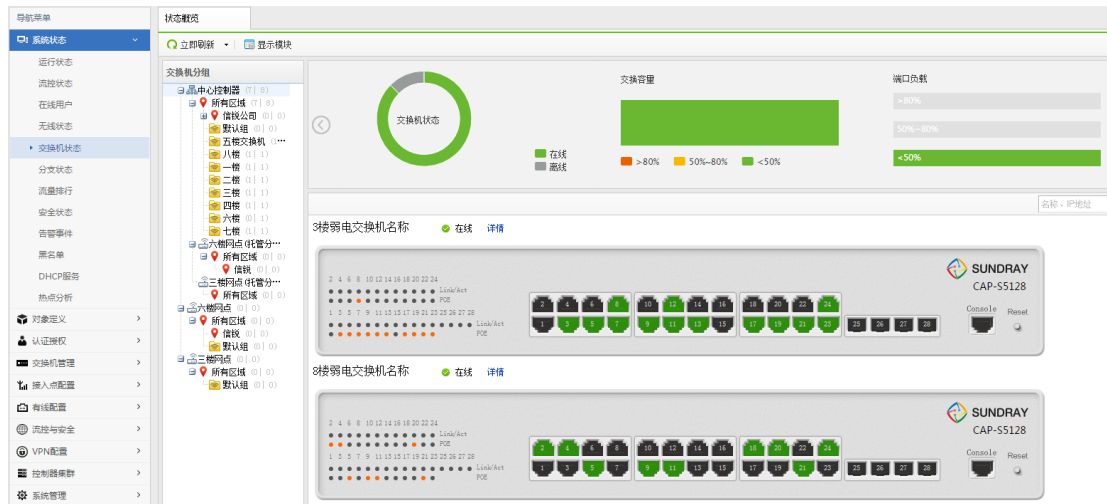


portal 服务用户信息，控制器做为 Portal 服务器，显示在 Portal 服务器上完成认证的用户。

用户名	认证类型	终端IP	终端MAC	接入号码	接入点	接入点分组	认证策略	认证策略	接入时间
1510095977	访客; 匿名验证	172.16.0.113	44-04-44-A9-5A-1B			默认组室外AP			2017-04-28 11:13:49
18976118982	访客; 匿名验证	172.16.3.177	14-1F-79-5A-0B-66			默认组室外AP			2017-04-28 11:09:26
15619947544	访客; 匿名验证	172.16.3.166	30-AF-2D-4D-53-89			默认组室外AP			2017-04-28 10:52:47
18769975153	访客; 匿名验证	172.16.3.131	44-04-44-23-99-33			默认组室外AP			2017-04-28 10:39:57
13876274951	访客; 匿名验证	172.1.5.167	FF-FF-00-01-33-A7						2017-04-28 10:39:57
13307522285	访客; 匿名验证	172.16.3.125	D4-M-4D-FF-3F-70			默认组室外AP			2017-04-28 10:36:34
18886990986	访客; 匿名验证	172.16.3.73	7D-14-A0-8A-F2-C3			默认组室外AP			2017-04-28 10:04:32
15103821516	访客; 匿名验证	172.16.1.6	E4-47-9D-C3-8C-AB			默认组室外AP			2017-04-28 09:28:26
18886900356	访客; 匿名验证	172.16.1.155	8C-01-2E-79-F6-75			默认组室外AP			2017-04-28 09:28:21
13667548410	访客; 匿名验证	172.16.1.41	5C-FF-C3-FA-E2-88			默认组室外AP			2017-04-28 09:09:12
13976762267	访客; 匿名验证	172.16.2.159	64-CC-2E-8D-39-2A			默认组室外AP			2017-04-28 09:07:32
13976919467	访客; 匿名验证	172.16.0.234	00-23-82-5E-01-AE			默认组室外AP			2017-04-28 09:05:20
13667522636	访客; 匿名验证	172.16.1.71	0C-2B-83-37-13-C9			默认组室外AP			2017-04-28 07:28:44
15348813446	访客; 匿名验证	172.16.0.132	00-23-82-5C-5D-8D			默认组室外AP			2017-04-28 02:57:24
15100963933	访客; 匿名验证	172.16.0.103	34-69-07-C3-00-98			默认组室外AP			2017-04-28 21:37:40

2.2.4. 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。



2.2.5. 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【流控与安全】中的流量控制策略。

序号	应用名称	应用类型	用户数	上行流速	下行流速	总流速	所占百分比
1	HTTP_GET	访问网站	20	358.70 Kbps	4.07 Mbps	4.42 Mbps	44.34 %
2	亚马逊	购物支付	2	1.31 Mbps	62.27 Kbps	1.37 Mbps	13.80 %
3	多线程下载	下载工具	4	23.27 Kbps	930.44 Kbps	953.71 Kbps	9.35 %
4	360网盘[上传]	360网盘	1	847.59 Kbps	22.90 Kbps	870.48 Kbps	8.53 %
5	腾讯视频	Web流媒体	1	16.42 Kbps	627.96 Kbps	644.38 Kbps	6.32 %
6	SSL	网络协议	16	399.30 Kbps	94.88 Kbps	494.18 Kbps	4.84 %
7	中国网络电视	P2P流媒体	1	336.30 Kbps	62.10 Kbps	398.40 Kbps	3.91 %
8	PFSream	P2P流媒体	1	239.32 Kbps	17.38 Kbps	256.70 Kbps	2.52 %
9	iCloud	网络存储	3	157.77 Kbps	56.21 Kbps	213.98 Kbps	2.10 %
10	HTTP_POST	HTTP_POST	10	53.82 Kbps	27.49 Kbps	81.31 Kbps	0.80 %
11	有道云笔记	网络存储	2	14.82 Kbps	33.63 Kbps	48.45 Kbps	0.47 %
12	DNS协议	DNS	44	18.82 Kbps	24.96 Kbps	43.78 Kbps	0.43 %
13	Microsoft w...	软件更新	1	1.82 Kbps	29.22 Kbps	31.04 Kbps	0.30 %
14	QQ	IM	17	6.57 Kbps	23.02 Kbps	29.59 Kbps	0.29 %

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，此功能的分析可以用于优化【流控与安全】中的流量控制策略。

序号	用户名	IP地址	所属组	应用名称	上行流速	下行流速	总流速	所占百分比
1	31438	10.10.28.122	/sangferradius/	多线程下载, 豆瓣网[...	117.27 Kbps	2.13 Mbps	2.25 Mbps	22.74 %
2	18873	10.10.26.158	/sangferradius/	中国网络电视, QQ, HTTP...	104.75 Kbps	1.38 Mbps	1.48 Mbps	14.97 %
3	35094	10.10.20.133	/sangferradius/	360网盘[上传], HTTP...	953.73 Kbps	28.93 Kbps	982.66 Kbps	9.70 %
4	90957	10.10.17.67	/sangferradius/	多线程下载, HTTP_GET...	40.35 Kbps	717.11 Kbps	757.46 Kbps	7.48 %
5	45928	10.10.22.138	/sangferradius/	亚马逊	707.41 Kbps	18.69 Kbps	726.10 Kbps	7.17 %
6	C0-18-85-50-94...	10.10.16.24	/PSK认证组/	腾讯视频, HTTP_GET, QQ	19.70 Kbps	683.61 Kbps	703.30 Kbps	6.94 %
7	00-87-46-0F-61...	10.10.20.11	/PSK认证组/	HTTP_GET, HTTP_POST, ...	43.17 Kbps	407.74 Kbps	450.91 Kbps	4.45 %
8	10207	10.10.30.203	/sangferradius/	HTTP_GET, 微信传文件...	38.37 Kbps	329.46 Kbps	367.83 Kbps	3.63 %
9	18-59-36-89-25...	10.10.30.15	/PSK认证组/	淘宝天猫, HTTP_GET, D...	29.29 Kbps	306.20 Kbps	335.49 Kbps	3.31 %
10	86840	10.10.18.13	/sangferradius/	移动QQ, Apple数据, SS...	50.91 Kbps	204.78 Kbps	255.69 Kbps	2.52 %
11	38584	10.10.20.33	/sangferradius/	iCloud, SSL, DNS协议	129.74 Kbps	102.09 Kbps	231.84 Kbps	2.29 %
12	B8-EE-85-20-31...	10.10.31.20	/PSK认证组/	PPStream	214.92 Kbps	15.45 Kbps	230.38 Kbps	2.27 %
13	D4-F4-6F-64-39...	10.10.18.168	/PSK认证组/	SSL	219.58 Kbps	8.33 Kbps	227.91 Kbps	2.25 %
14	B8-78-2E-BD-0E...	10.10.24.84	/PSK认证组/	亚马逊, 微信, DNS协议	178.66 Kbps	22.65 Kbps	201.30 Kbps	1.99 %

2.2.6. 黑名单

【黑名单】可以手动添加，也可以由设备自动添加，设备的【入侵检测】和【DOS 攻击检测功能】启用时，检测到不合法的无线用户接入的时候，会自动把该 MAC 添加到黑名单，冻结该 MAC 地址的接入，冻结时间超过后，再自动放开，默认 30 分钟，可以在相应的模块更改或关闭。手动添加的 MAC 为永久冻结。

<input type="checkbox"/>	MAC地址	冻结原因	剩余冻结时间(秒)	加入时间
<input type="checkbox"/>	00-11-22-33-44-55	手动添加	永不	2013-07-03 16:20:15

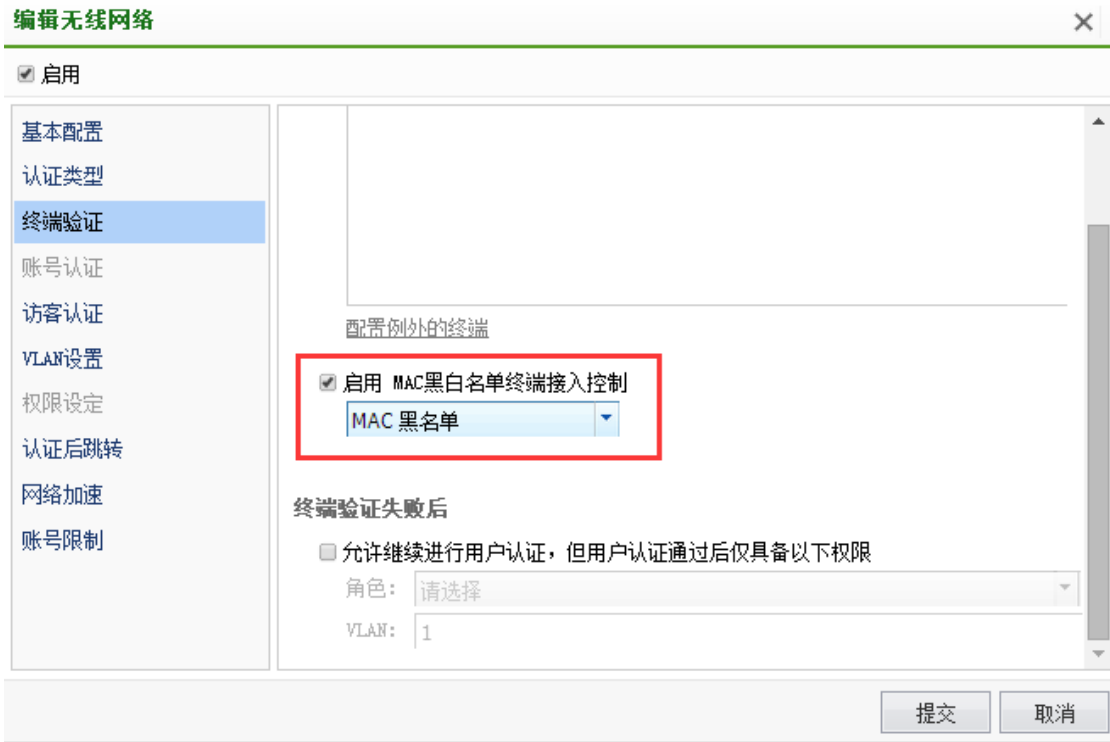
点击【新增】菜单，添加 MAC 地址：

新增

MAC地址: 00-12-12-12-12-12

提交 取消

需要黑名单生效，需要在编辑无线网络中，终端验证下面，启用 MAC 黑名单功能，MAC 黑名单才能正常生效。



2.2.7. DHCP 服务

该页面可以观察到 NAC 作为 DHCP 服务器时，对外分配 IP 地址的分配情况：包括了 IP 地址、计算机名、MAC 地址、获取租约时间，租约过期时间：

DHCP 服务		MAC地址、IP地址			
接口列表	当前分配: 15	未分配: 83			
	IP地址	计算机名	MAC地址	分配时间	租
> vlani f10	10.10.10.6	android-bb869460fed	B4-52-7D-BF-3A-5F	2014-07-13 20:14	:
> vlani f12	10.10.10.3	android-13fc8471915	40-F3-08-24-BF-5A	2014-07-13 20:37	:
> vlani f20	10.10.10.4	android_fc88e9a36ce	24-DB-AC-DF-98-D9	2014-07-13 22:57	:
> vlani f100	10.10.10.7	android-2a6108437dd	2C-28-2D-2D-78-1D	2014-07-14 00:08	:
	10.10.10.8	android-53c8a70d8d9	00-16-6D-FA-A0-37	2014-07-14 08:08	:
	10.10.10.9	tuares-pc	74-E5-0B-F1-96-2C	2014-07-14 08:24	:
	10.10.10.10	4LX5J1NCSWSFMIJ	7C-E9-D3-F2-89-31	2014-07-14 08:30	:
	10.10.10.12	android-d4e8c70b19e	AC-F7-F3-2D-AC-18	2014-07-14 08:41	:
	10.10.10.13	android-b205bcb542b	88-30-8A-E2-12-FC	2014-07-14 09:00	:
	10.10.10.16	android-b07bd350a14	24-69-A5-3E-FE-59	2014-07-14 10:01	:
	10.10.10.15	LanProductionS	54-E4-3A-71-D0-D7	2014-07-14 10:07	:

每页 25 记录数: 15

2.3. 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。

2.4. 交换机管理

『交换机管理』包括【交换机】、【VLAN 配置】、【链路聚合】、【防环路配置】、【链路高可用】、【端口列表】、【供电配置】这 7 个菜单选项；【交换机】用于管理接入 NAC 的交换机，给交换机进行分组和独立配置。

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、RS3320-28M-PWR-LI、RS5300-28T-4F、RS5300-52T-4F、RS5300-28X-PWR-SI、RS5300-52X-PWR-SI、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。

2.4.1. 交换机

『交换机』包括了【发现新交换机】和【交换机管理】。

2.4.1.1. 发现新交换机

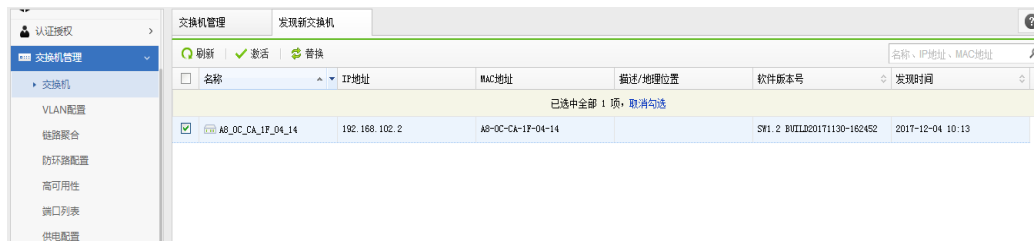
为了让控制器统一管理交换机，当交换机接入内网时，并未进入工作状态，需要管理员在“发现新交换机”列表中，手动执行激活操作，交换机才能正常工作。

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：

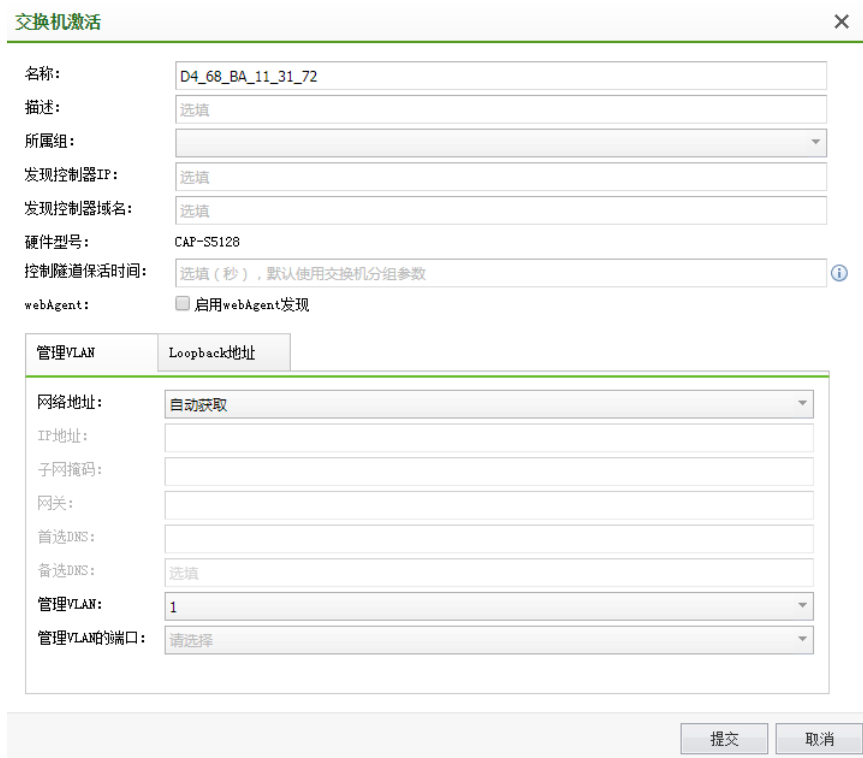
1. 射频交换机

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：



交换机激活配置界面截图，包含以下字段：

- 名称: D4_68_BA_11_31_72
- 描述: 选填
- 所属组: [下拉菜单]
- 发现控制器IP: 选填
- 发现控制器域名: 选填
- 硬件型号: CAP-SS128
- 控制隧道保活时间: 选填 (秒), 默认使用交换机分组参数
- webAgent: 启用webAgent发现

管理VLAN配置部分：

管理VLAN	Loopback地址
网络地址: 自动获取	
IP地址:	
子网掩码:	
网关:	
首选DNS:	
备选DNS: 选填	
管理VLAN: 1	
管理VLAN的端口: 请选择	

底部按钮: 提交, 取消

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。

2.4.1.2. 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。

设备替换✕

使用当前选择的设备替换旧设备，并继承旧设备的配置，仅支持相同型号。

已选择设备

名称: D4_68_BA_11_31_72
MAC地址: D4-68-BA-11-31-72
硬件型号: CAP-S5128
网络地址:

替换设备

替换设备:

旧设备处理: 重新激活 删除设备 i

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。

2.4.1.3. 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。



批量修改如下图：



批量编辑交换机 [X]

所属组: [下拉菜单]

发现控制器IP: [输入框]

发现控制器域名: [输入框]

控制隧道保活时间: [12] [i]

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: [输入框]

结束IP: [输入框]

掩码: [输入框]

网关: [输入框]

首选DNS: [输入框]

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。

编辑交换机 ✕

名称:	<input type="text" value="D4_68_BA_11_31_72"/>
描述:	<input type="text" value="选填"/>
所属组:	<input type="text" value="所有区域/默认组"/>
发现控制器IP:	<input type="text" value="选填"/>
发现控制器域名:	<input type="text" value="选填"/>
硬件型号:	CAP-S5128
控制隧道保活时间:	<input type="text" value="选填 (秒), 默认使用交换机分组参数"/> ⓘ
webAgent:	<input type="checkbox"/> 启用webAgent发现
DNS地址:	<input type="button" value="配置"/>

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。

2.4.1.3.1. 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。

VLAN接口	端口面板	静态路由	地址表	链路高可用	防环路配置	安全功能	Loopback地址	
+ 新增 ✕ 删除 📄 管理VLAN配置								
<input type="checkbox"/>	VLAN ID	描述						IP地址
<input type="checkbox"/>	1							自动获取
< < 1 / 1 > > 🔄 每页 25 记录数: 1								
							提交	取消

点击**新增**，添加 VLAN 接口。

添加VLAN接口 ✕

VLAN:	<input type="text" value="2"/>
描述:	<input type="text" value="选填"/>
网络地址:	<input type="text" value="手动配置"/> ⓘ
IP地址:	<input type="text" value="10.10.10.1/24"/>
DHCP服务:	<input type="text" value="不启用"/> ⓘ
MTU:	<input type="text" value="1500"/>

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

管理VLAN配置 ✕

VLAN接口:	<input type="text" value="vlanif1"/>
---------	--------------------------------------



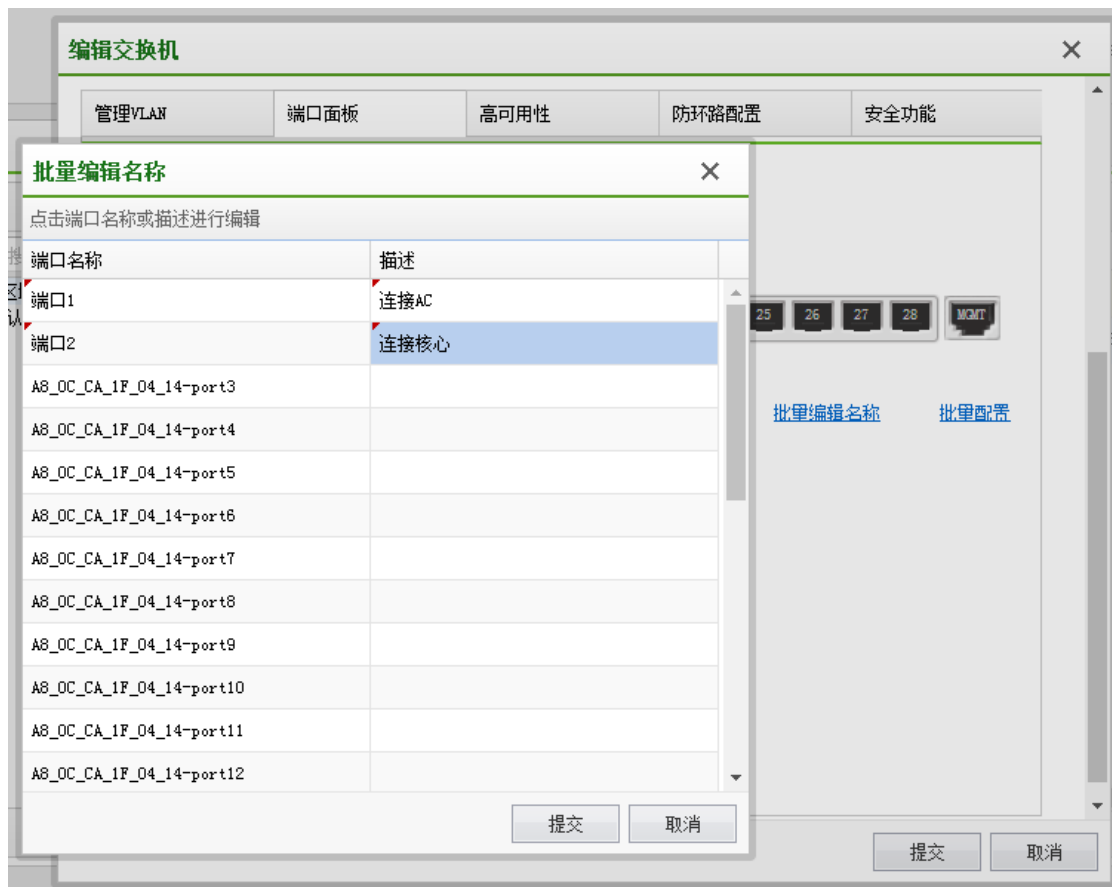
在 VLAN 接口中存在的 VLAN 才可以被选择成管理 vlan。

2.4.1.3.2. 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。

2.4.1.3.3. 高可用性

备份链路组

备份链路，又叫做灵活链路或备份链路。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。Smart Link 组中的从接口在 Smart Link 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。

组名称：编辑备份链路策略名称。

主端口：选择主端口，主端口承载业务，端口类型选择端口/聚合口。

从端口：选择从端口，备份端口，当主端口断开后备端口激活，端口类型选择端口/聚合口。

Flush 报文发送：配置要发送 Flush 报文的 VLAN 及密码。

抢占配置：当主链路故障恢复后可以选择立即抢占、延迟抢占或不抢占。

上行链路监控组

上行链路监控是一种端口联动方案，它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。



组名称：编辑上行链路监控策略名称。

上行接口：监控交换机的链路，一般用于监控交换机的上联口，端口可以监控备份链路组/聚合口/端口。

下行接口：当上行链路故障后，需要断开的下行接口，可以选择端口和聚合口。

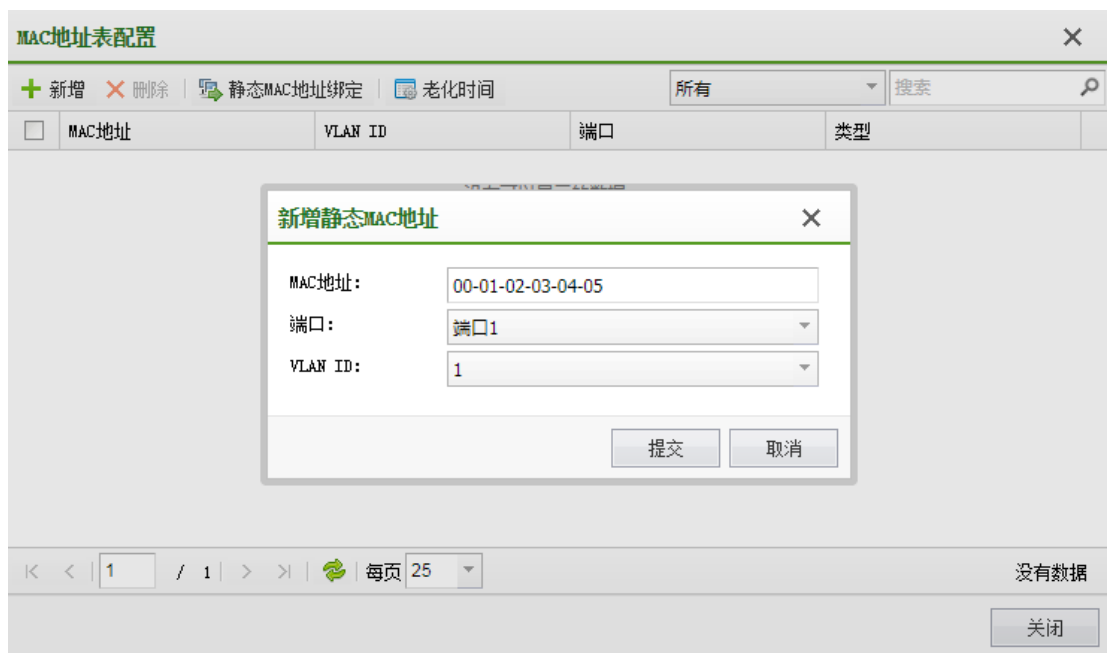
2.4.1.3.4. 地址表



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 地址转换为静态 MAC 地址。

MAC地址表配置
✕

+ 新增 ✕ 删除 🔄 静态MAC地址绑定 🕒 老化时间

 所有 搜索 🔍

<input type="checkbox"/>	MAC地址	VLAN ID	端口	类型
<input checked="" type="checkbox"/>	D4-68-BA-01-6B-D5	1	端口1	动态
<input checked="" type="checkbox"/>	00-E0-4D-1B-FC-B4	1	D4_68_BA_11_31_72-port23	动态

静态MAC地址绑定
✕


将勾选中的动态MAC地址表项转化为静态MAC地址
所有 搜索 🔍

<input type="checkbox"/>	MAC地址	VLAN ID	端口	类型
<input checked="" type="checkbox"/>	D4-68-BA-01-6B-D5	1	端口1	动态
<input checked="" type="checkbox"/>	00-E0-4D-1B-FC-B4	1	D4_68_BA_11_31_72-port23	动态

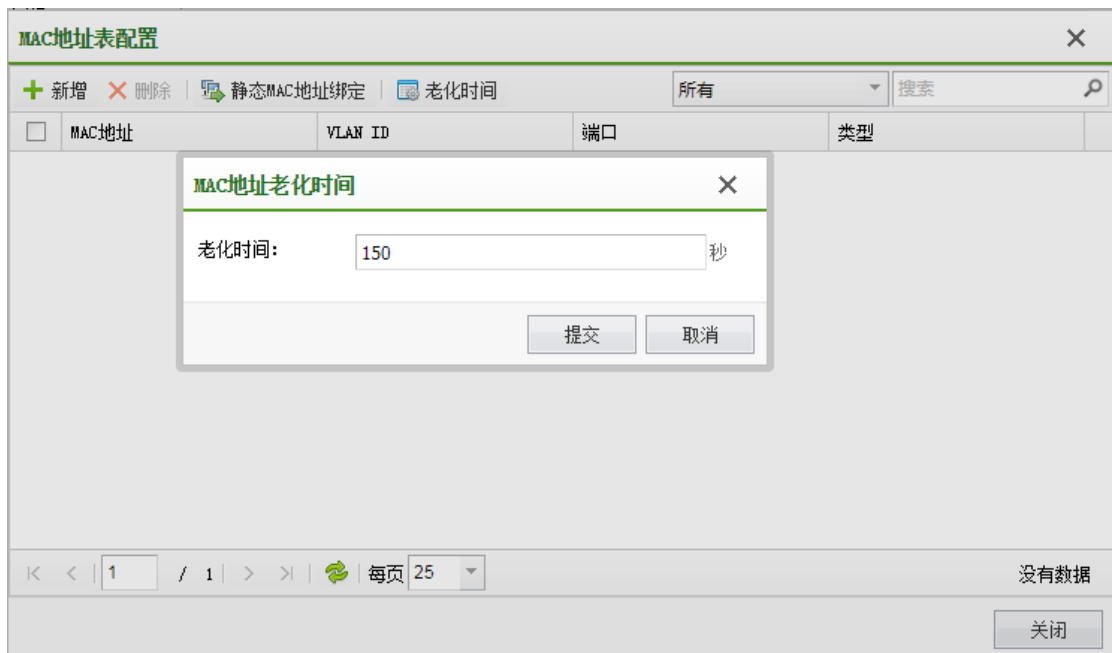
< < 1 / 1 > > 🔄 每页 25

记录数: 2

提交
取消

 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 150 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。

ARP地址表配置

+ 新增 X 删除 静态ARP地址绑定 老化时间 所有 搜索

<input type="checkbox"/>	IP地址	MAC地址	接口	类型
没有可以显示的数据				

新增静态ARP地址

IP地址:

MAC地址:

提交 取消

< < | 1 / 1 | > > | 刷新 | 每页 25 没有数据

关闭

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 地址转换为静态 ARP 地址。

静态ARP地址绑定


将勾选中的动态ARP地址表项转化为静态ARP地址

所有 搜索

<input type="checkbox"/>	IP地址	MAC地址	接口	类型
<input checked="" type="checkbox"/>	10.10.10.3	D4-68-BA-01-6B-D5	vlan1 f1	动态
<input checked="" type="checkbox"/>	10.10.10.1	00-E0-4D-1B-FC-B4	vlan1 f1	动态

< < | 1 / 1 | > > | 刷新 | 每页 25 记录数: 2

提交 取消

 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。



2.4.1.3.5. 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。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。

手工负载分担模式链路聚合

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，因此称为负载分担模式。



The screenshot shows a web-based configuration interface for a network switch. A '新增' (New) dialog box is open, allowing the user to configure a link aggregation strategy. The dialog contains the following fields and options:

- 名称:** 聚合 (Name: Aggregation)
- 工作模式:** 手工负载分担模式 (Work Mode: Manual Load Sharing Mode)
- 接口类型:** 二层接口 (Interface Type: Layer 2 Interface)
- 负载分担方式:** 源MAC地址与目的MAC地址 (Load Balancing Method: Source MAC Address and Destination MAC Address)
- 选择端口:** 端口1, 端口2 (Select Ports: Port 1, Port 2)
- JumboFrame:** 1518
- VLAN属性:**
 - 端口模式:** Access (Port Mode: Access)
 - VLAN:** 1

Buttons for '确定' (OK) and '取消' (Cancel) are located at the bottom of the dialog. The background interface shows a navigation menu with '链路聚合' (Link Aggregation) selected.

名称：编辑链路聚合策略名称。

工作模式：配置链路聚合的工作模式，链路聚合模式支持手工负载分担/LACP 静态模式。


接口类型：默认为二层接口，链路聚合支持二层接口聚合和三层接口聚合。

负载分担方式：选择负载分担方式。支持源 MAC 地址与目的 MAC 地址、源 MAC 地址、目的 MAC 地址。默认为源 MAC 地址与目的 MAC 地址。

选择端口：选择要做链路聚合的端口。

JumboFrame：默认为 1518，支持 1518~9192。

VLAN 属性：配置聚合口的 Access 模式或 Trunk 模式。

 三层聚合口也可以配置 DHCP 服务，配置方法与三层物理口和 VLAN 接口配置方法一样，均需要将接口配置成静态 IP 地址才可以开启 DHCP 服务或配置 DHCP 中继。

LACP 模式链路聚合

作为链路聚合技术，手工负载分担模式 Eth-Trunk 可以完成多个物理端口聚合成一个 Eth-Trunk 口来提高带宽，同时能够检测到同一聚合组内的成员链路有断路等有限故障，但是无法检测到链路层故障、链路错连等故障。

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）。

新增
×

名称:

工作模式:

LACP报文:

接口类型:

负载分担方式:

选择端口:

超时时间:

JumboFrame:

端口优先级:

端口名称	端口LACP优先级	编辑	
端口1	32768		
端口2	32768		

VLAN属性

端口模式:

VLAN:

名称：编辑链路聚合策略名称。

工作模式：配置链路聚合的工作模式，链路聚合模式支持手工负载分担/LACP 静态模式。

LACP 报文：选择 LACP 报文支持的工作模式为：主动协商、被动协商。默认为主动协商。

接口类型：默认为二层接口，链路聚合支持二层接口聚合和三层接口聚合

负载分担方式：选择负载分担方式。支持源 MAC 地址与目的 MAC 地址、源 MAC 地址、目的 MAC 地址。默认为源 MAC 地址与目的 MAC 地址。


选择端口：选择要做链路聚合的端口。

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，默认 90 秒。

JumboFrame：默认为 1518，支持 1518~9192。

端口优先级：设置端口 LACP 优先级，默认为 32768。

VLAN 属性：配置聚合口的 Access 模式或 Trunk 模式。

 三层聚合口也可以配置 DHCP 服务，配置方法与三层物理口和 VLAN 接口配置方法一样，均需要将接口配置成静态 IP 地址才可以开启 DHCP 服务或配置 DHCP 中继。

2.4.1.3.6. 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，所有交换机默认开启防环路功能，如有部分设备不需要开启防环路，请在排除列表中设置。

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 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。

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。

VLAN接口	端口面板	静态路由	地址表	链路高可用	防环路配置	安全功能	Loopback地址
配置方式:	使用独立配置						
防环路功能:	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用						
工作模式:	MSTP						
MST:	<input checked="" type="radio"/> 使用独立域 <input type="radio"/> 加入统一域						
	<input type="button" value="配置MST域"/>						
优先级:	32768						
路径开销标准:	IEEE 802.1t标准 ?						
端口参数:	<input type="button" value="参数配置"/>						

配置方式：选择独立配置或使用统一的组配置。

防环路功能：启用/禁用防环路功能。

MST：选择使用独立域/加入统一域。

优先级：配置交换机的优先级，越小越优先，默认为 32768。

路径开销标准：配置交换机的路径开销协议。

端口参数：设置交换机的边缘端口、BPDU 过滤、BPDU 保护、根保护、环路保护功能，端口优先级和路径开销，端口优先级默认为 128，聚合口默认优先级为 64。路径开销默认为自动。

端口参数												
批量编辑												
<input type="checkbox"/>	名称	类型	所选端口	防环路状态	端口优先级	路径开销	边缘端口	BPDU过滤	BPDU保护	根保护	环路保护	
<input checked="" type="checkbox"/>	端口3	普通端口	-	🚫	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port7	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port8	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port9	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port10	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port11	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port12	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port13	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port14	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port15	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port16	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port17	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port18	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫
<input type="checkbox"/>	A8_OC_CA_1F_04_14-port19	普通端口	-	✅	128	自动选择	🚫	🚫	🚫	🚫	🚫	🚫

点击接口名称进行选择启用或禁用边缘端口、BPDU 过滤、BPDU 保护、根保护、环路保护功能。

端口配置

启用

端口优先级:

路径开销:

边缘端口:

BPDU过滤:

根保护:

环路保护:

BPDU保护:

延时时间: 秒

启用：勾选即启用防环路功能。

端口优先级：配置端口优先级。

路径开销：配置端口的路径开销。

边缘端口：启用/禁用边缘端口。

BPDU 过滤：启用/禁用 BPDU 过滤。

根保护：启用/禁用根保护。

环路保护：启用/禁用环路保护。

BPDU 保护：启用/禁用 BPDU 保护。

延时时间：启用 BPDU 保护后的延时时间。

高级选项：调整生成树的网络直径、最大跳数、生成树的定时器。

高级选项 ✕

网络直径：

最大跳数：

定时器

老化时间： 秒

握手时间： 秒

转发延迟： 秒

网络直径：交换网络中任意两台终端设备间的最大设备数。网络直径越大，说明网络的规模越大。默认情况下，交换机的网络直径为 7。

最大跳数：从 MST 域内的生成树的根桥开始，域内的配置消息（即 BPDU）每经过一台设备的转发，跳数就被减 1；设备将丢弃跳数为 0 的配置消息，以使处于最大跳数外的设备无法参与生成树的计算，从而限制了 MST 域的规模。数值范围为 1-40，默认 20 跳。

老化时间：老化时间，数值范围为 6-40 秒。如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。默认 20 秒。

握手时间：握手时间，数值范围为 2-10 秒，是指根桥向其它所有交换机发出 BPDU 数据包的时间间隔，用于交换机检测链路是否存在故障。默认 2 秒。

转发延迟：转发延迟，数值范围为 4-30 秒，是指交换机的端口状态迁移所用的时间。默认 15 秒。

2.4.1.3.7. 安全功能

DHCP Snooping 技术是 DHCP 安全特性，通过建立和维护 DHCP Snooping 绑定表过滤不可信任的 DHCP 信息，这些信息是指来自不信任区域的 DHCP 信息。DHCP Snooping 绑定表包含不信任区域的用户 MAC 地址、IP 地址、租用期、VLAN-ID 接口等信息。

当交换机开启了 DHCP-Snooping 后，会对 DHCP 报文进行侦听，并可以从接收到的 DHCP Request 或 DHCP Ack 报文中提取并记录 IP 地址和 MAC 地址信息。另外，DHCP-Snooping 允许将某个物理端口设置为信任端口或不信任端口。信任端口可以正常接收并转发 DHCP Offer 报文，而不信任端口会将接收到的 DHCP Offer 报文丢弃。这样，可以完成交换机对假冒 DHCP Server 的屏蔽作用，确保客户端从合法的 DHCP Server 获取 IP 地址

VLAN接口	端口面板	静态路由	地址表	链路高可用	防环路配置	安全功能	Loopback地址
--------	------	------	-----	-------	-------	------	------------

DHCP Snooping

启用DHCP Snooping功能

高级配置

提交 取消

启用 DHCP Snooping 功能：勾选即启用 DHCP Snooping 功能


高级配置：添加信任端口和信任 IP、MAC

高级配置

信任端口：

信任地址：

+ 新增 ✕ 删除

<input type="checkbox"/>	IP地址	MAC地址	编辑
<input type="checkbox"/>	192.168.1.1	00-00-00-00-01-11	

信任端口：添加 DHCP 信任端口。

信任地址：添加信任 DHCP 服务器地址和 MAC。

2.4.1.3.8. 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。

VLAN接口	端口面板	静态路由	地址表	链路高可用	防环路配置	安全功能	Loopback地址
<input checked="" type="checkbox"/> 启用							
IP地址:		<input type="text" value="1.1.1"/>					
子网掩码:		<input type="text" value="255.255.255.255"/>					
MTU:		<input type="text" value="1500"/>					

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。

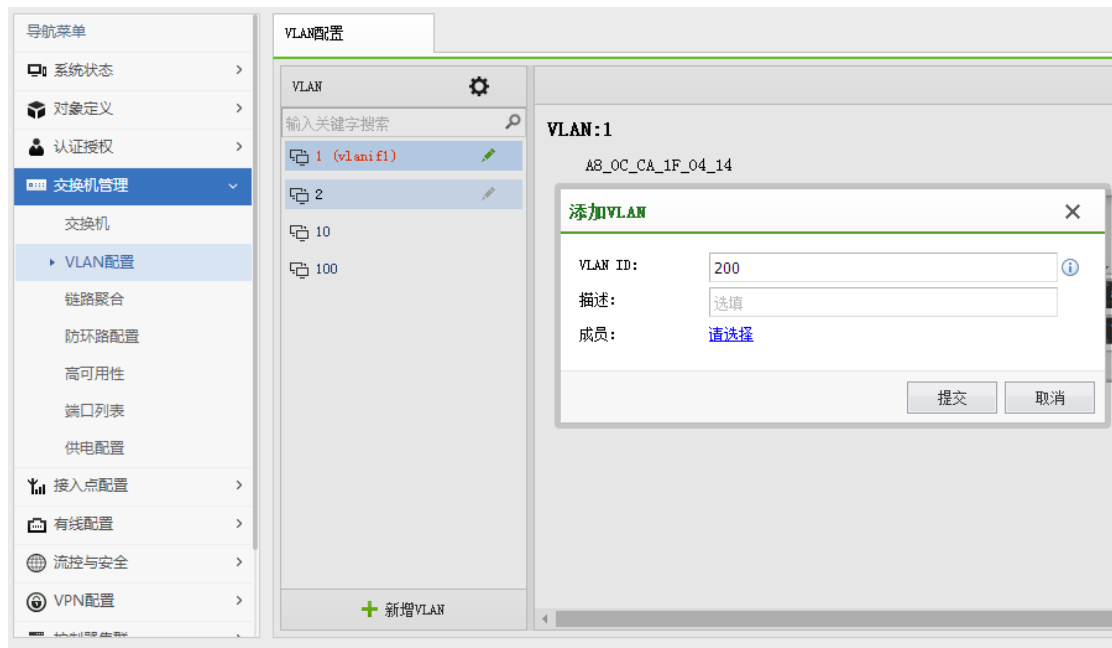


启用 loopback 地址尽量不要使用内网中存在的网段地址。


2.4.2. 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。

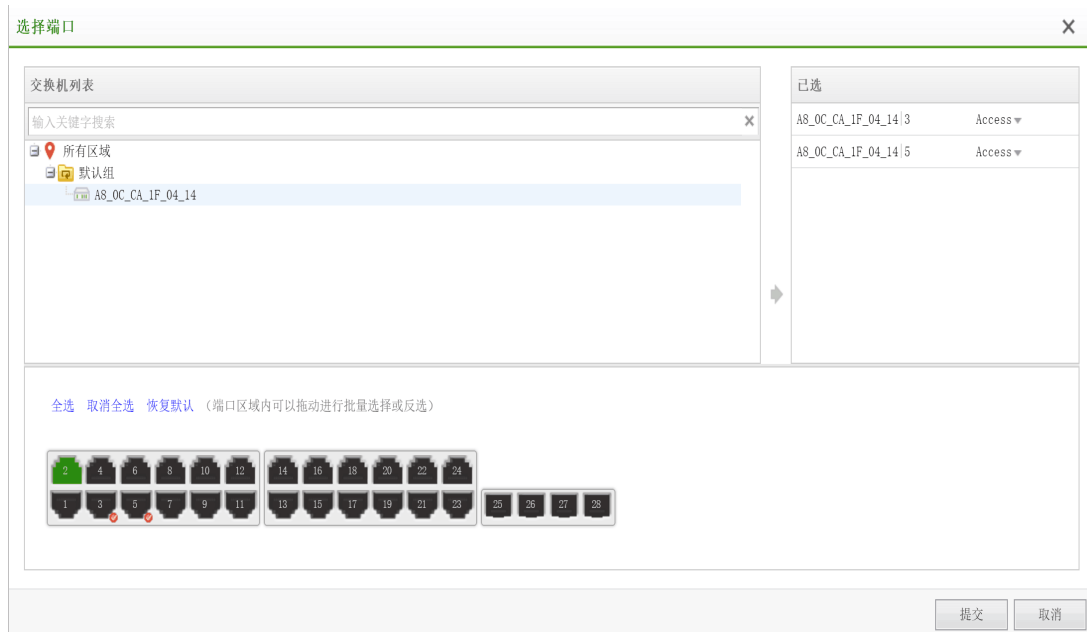


VLAN ID:填写对接的 VLAN 编号

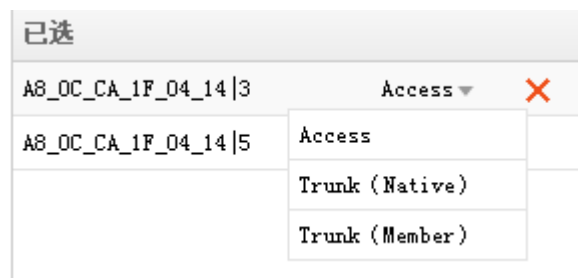
 注意：此处的 VLAN ID 只针对交换机创建，和有线配置里面的 VLAN 不能互相调用

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。

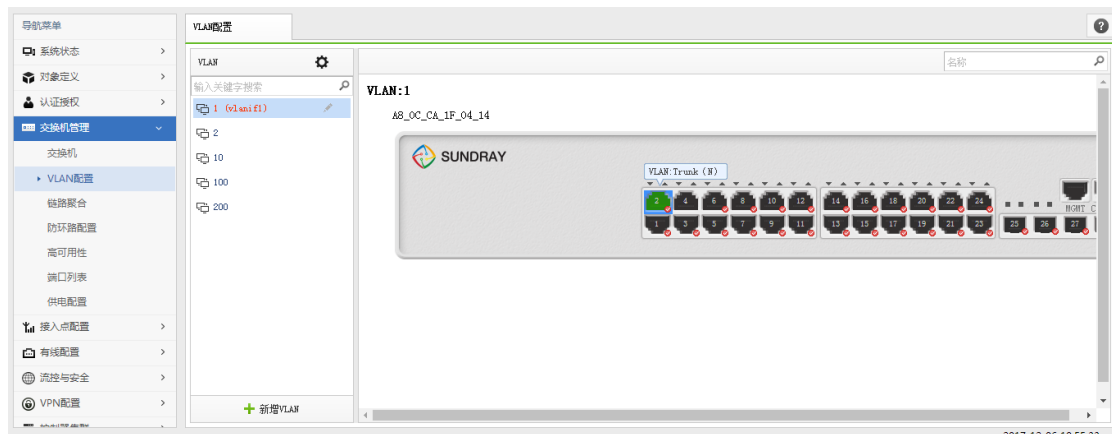


在已选接口中可以修改接口的模式：

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。

设置端口属性 ✕

启用

名称:

描述:

速率:

告警日志: ⓘ

MTU:

VLAN属性

端口模式:

VLAN:

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。

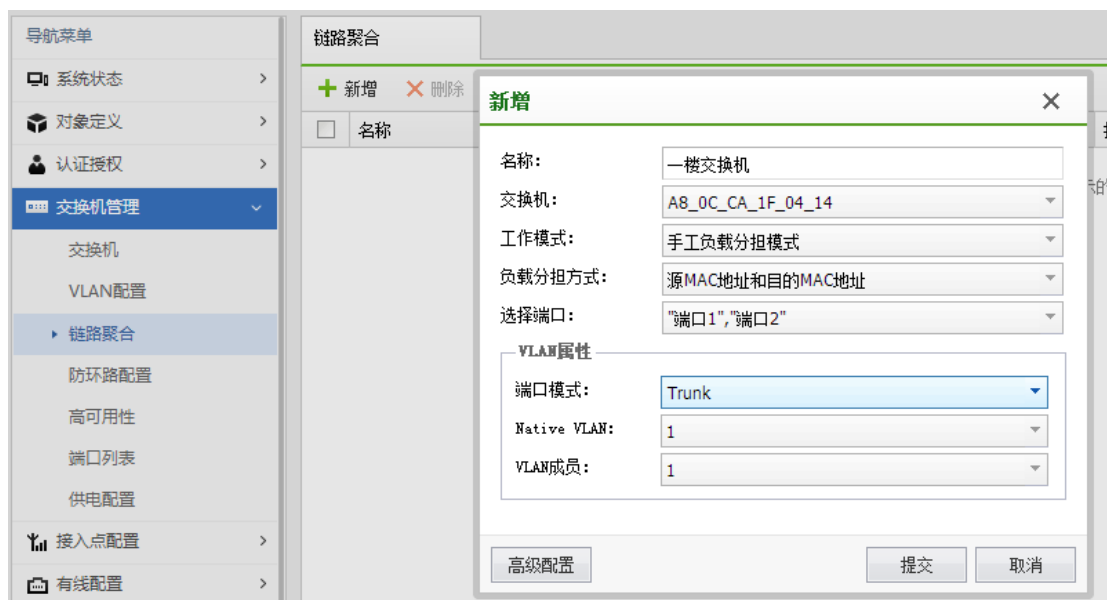
告警日志：启用/禁用告警日志。

MTU:配置端口的 MTU。

VLAN 属性：配置端口的 VLAN 属性。

2.4.3. 链路聚合

此处的链路聚合是针对交换机进行批量编辑，链路聚合详细内容可以查看交换机的链路聚合章节。



名称：对链路聚合组的命名。

交换机：选择对应交换机。

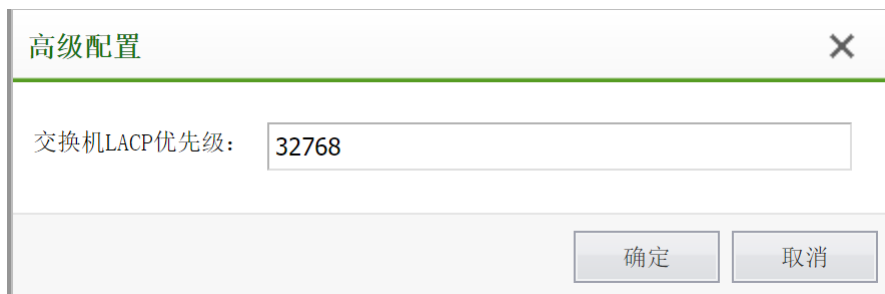
工作模式：选择手工负载分担模式或选择 LACP 静态模式。

负载分担方式：默认使用源 MAC 地址和目的 MAC 地址，还可以选择成源 MAC 地址或目的 MAC 地址。

选择端口：选择要做链路聚合的端口。

VLAN 属性：端口模式修改链路聚合接口模式，可以使用 Access 或使用 Trunk。

高级配置：配置交换机 LACP 的优先级,默认优先级为：32768。



高级配置

交换机LACP优先级:

确定 取消

2.4.4. 防环路配置

该选项是针对交换机的防环路功能进行批量编辑，防环路详细内容可以查看交换机的防环路章节。



选择开启防环路模式：

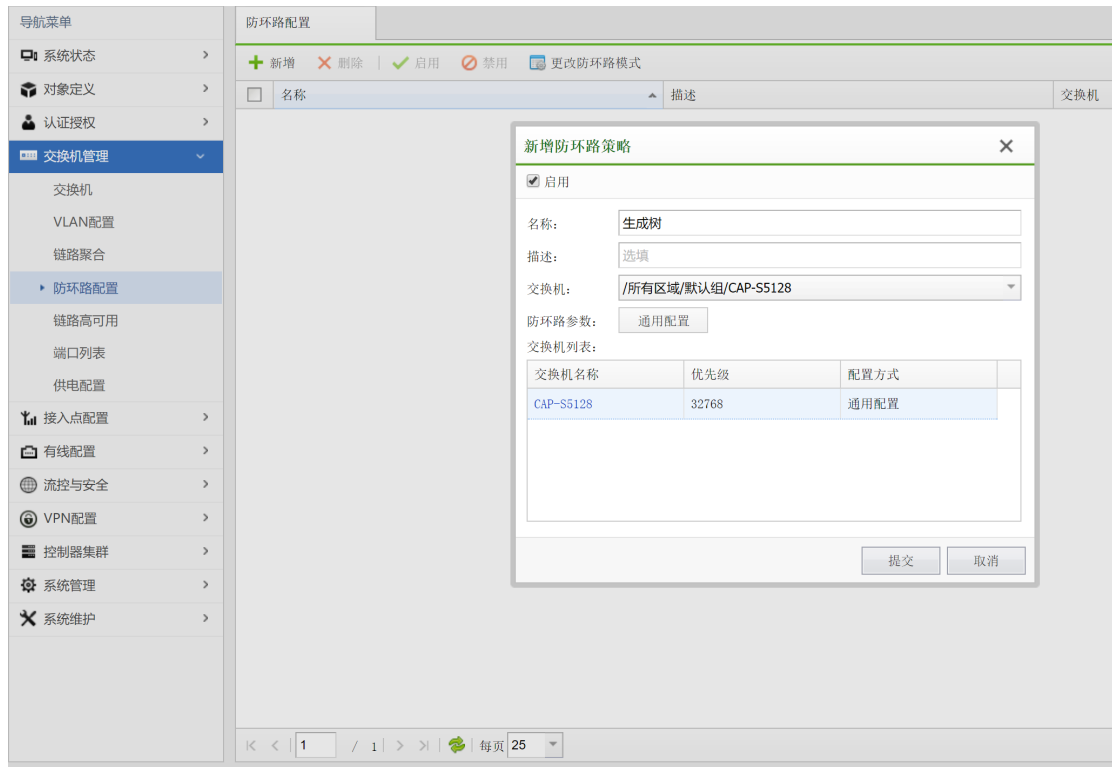
简单模式：一键开启防环路

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。



名称：编辑策略名称

描述：对策略做描述

交换机：选择要使用该策略交换机

防环路参数：修改交换机的生成树工作模式及 MSI 域配置

交换机列表：此策略选中的交换机

2.4.5. 链路高可用

该选项是批量编辑交换机的高可用性，包含了备份链路、上行链路监控和 Flush 报文接收配置，备份链路、上行链路监控、Flush 报文详细内容可参考之前介绍备份链路、上行链路监控内容。

备份链路配置如下图：

名称：编辑策略名称

交换机：选择要使用该策略交换机

主端口：使用备份链路的主端口

从端口：使用备份链路的从端口

Flush 报文发送：选择控制器 VLAN、密码和接口端口

抢占设置：当主链路故障恢复后可以选择立即抢占、延迟抢占和从不抢占

延时时间：配合抢占设置中的延迟抢占

上行链路监控配置如下图：

编辑
✕

启用

名称:

交换机:

上行接口:

下行接口:

名称：编辑策略名称

交换机：选择要使用该策略交换机

上行接口：可以配合备份链路策略做联动

下行接口：选择对应接口

2.4.6. 端口列表

显示当前控制器上管理的交换机所有接口的基本信息

端口	端口位置	描述	速率	模式	VLAN	PoE供电	MTU	状态	
共 28 条记录，选择所有页中的记录									
<input type="checkbox"/>	端口1	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	端口2	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Trunk	native:1,vlan_全部	-	1518	✓
<input type="checkbox"/>	端口3	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Trunk	native:1,vlan_1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	2	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Trunk	native:1,vlan_1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Trunk	native:1,vlan_1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓
<input type="checkbox"/>	A8_OC_CA_1F_04_14-po...	A8_OC_CA_1F_04_14-po...	-	自动协商10/100/1000M	Access	1	-	1518	✓

在该界面下可以批量编辑接口状态：

批量编辑端口 ✕

网口状态:

速率:

告警日志: ⓘ

MTU:

VLAN属性

端口模式:

VLAN:

网口状态：批量启用/禁用端口

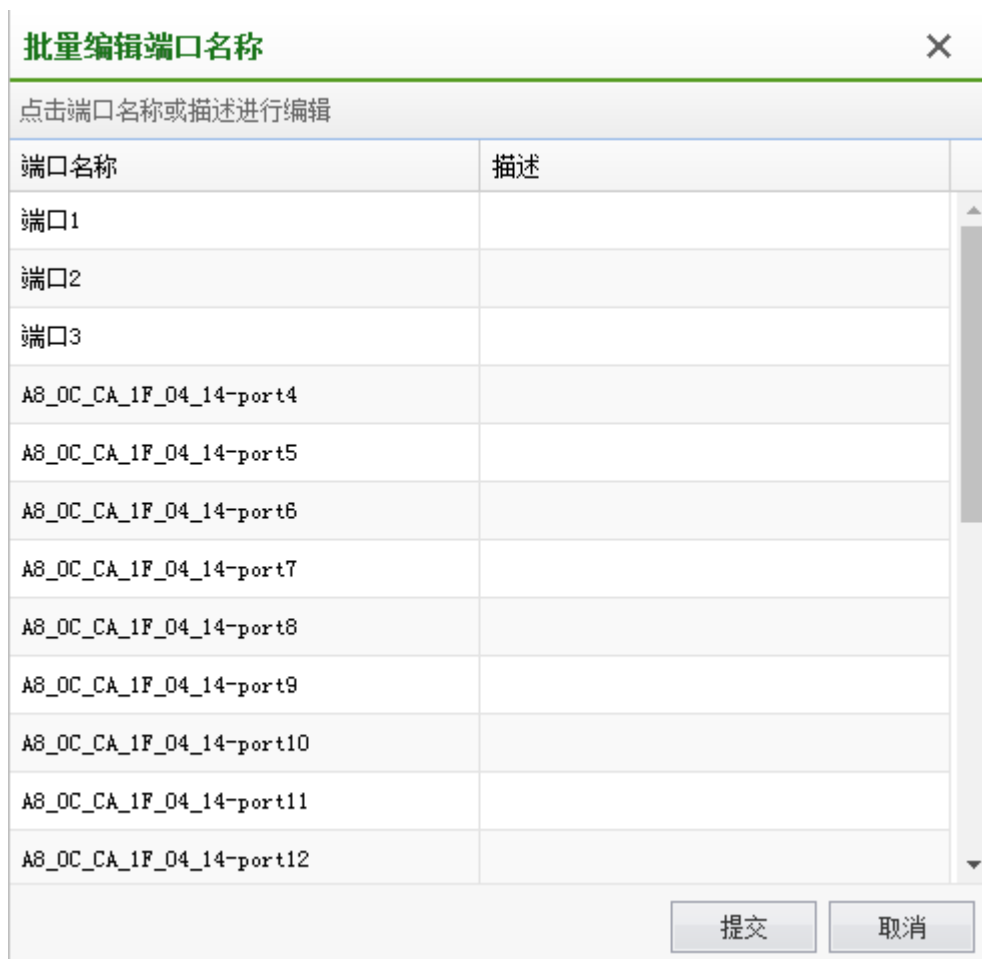
速率：批量配置端口的速率

告警日志：批量启用/禁用告警日志

MTU：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

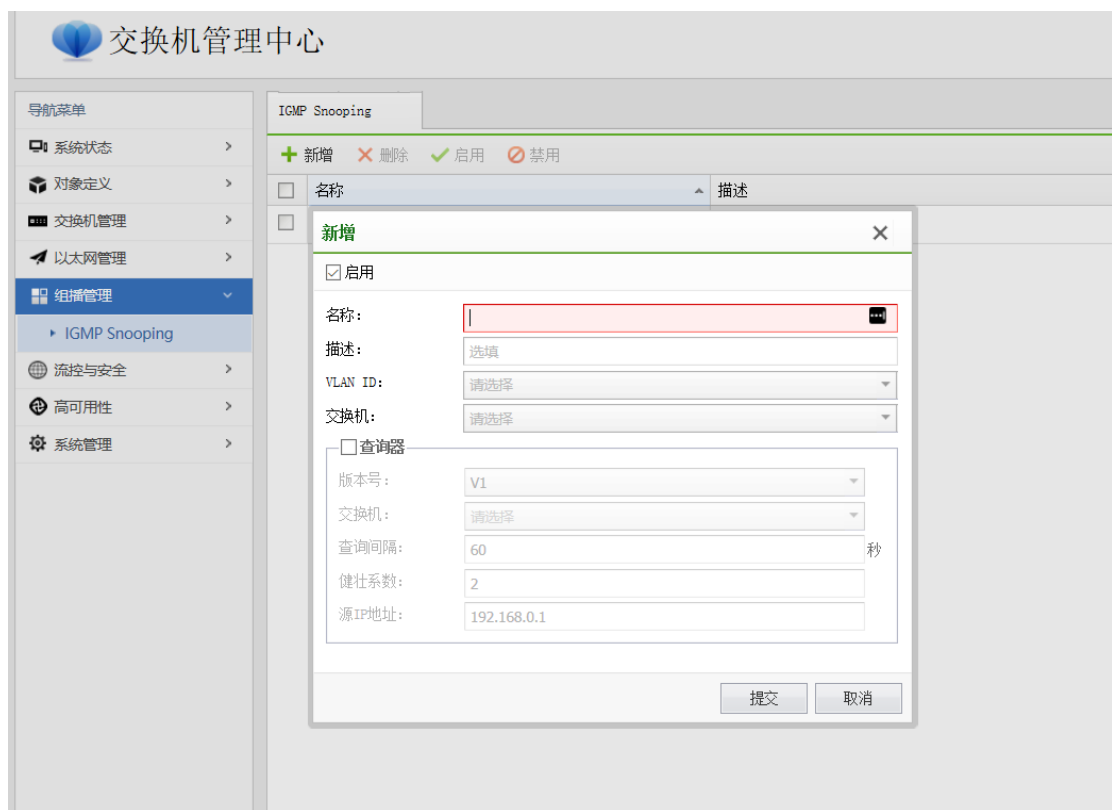
端口模式：端口的 VLAN 属性

VLAN：根据 VLAN 过滤端口

2.4.7. 组播管理

配置交换机的 IGMP Snooping

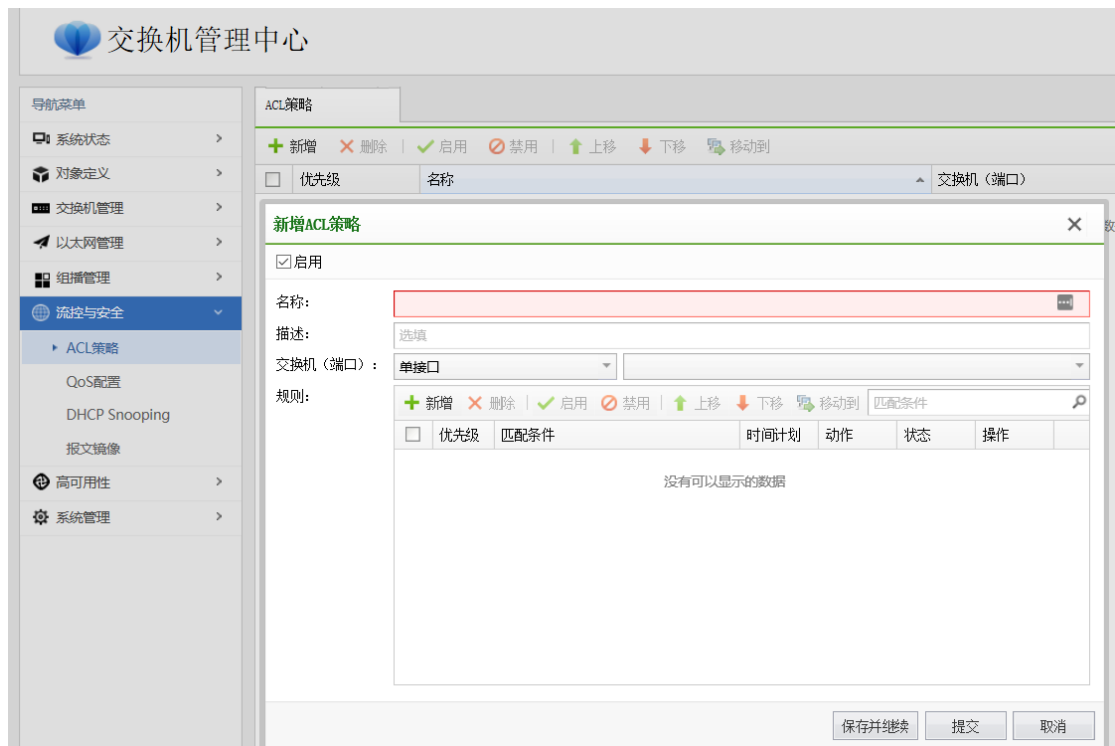
该选项是针对批量选择安视交换机开始组播功能



2.4.8. ACL 策略

配置安视交换机的 ACL 策略

针对安视交换机的单端口或聚合口进行 ACL 策略匹配



IP 地址：基于源目 IP 地址进行匹配

MAC 地址：源目 MAC 地址进行匹配

协议：基于 TCP、UDP、IP、OSPF 等协议进行匹配

时间：自定义时间接入策略

2.4.9. 服务质量 Qos

配置安视交换机的服务质量



流量管理：基于匹配 ACL 策略，同时对于流量重标记、重定向

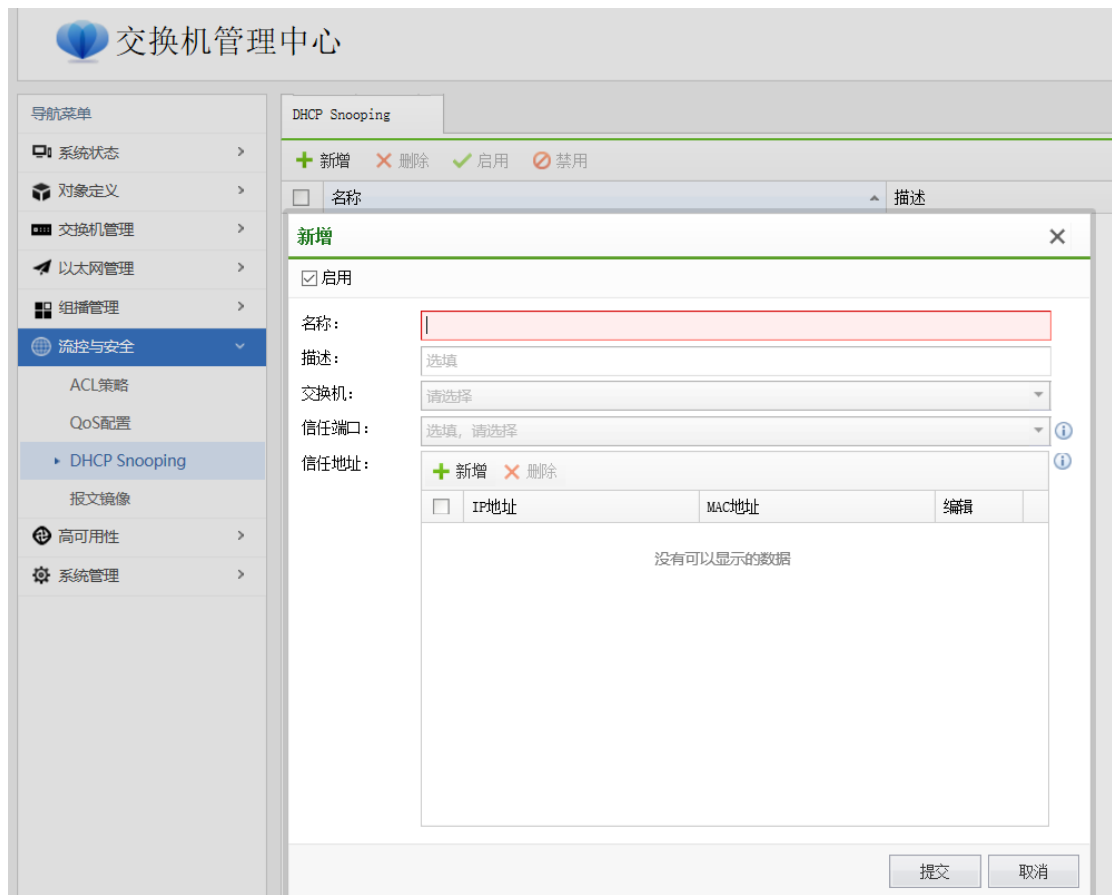
流量整形：批量应用于安视交换机基于端口、队列进行流量整形，自定义入方向、出方向文件传输速率

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

2.4.10. DHCP Snooping

配置安视交换机的 DHCP 安全功能



交换机/信任端口：批量选择安视交换机对端口进行信任授权

信任地址：对于非信任端口也可以配置白名单地址放通

2.4.11. 报文镜像

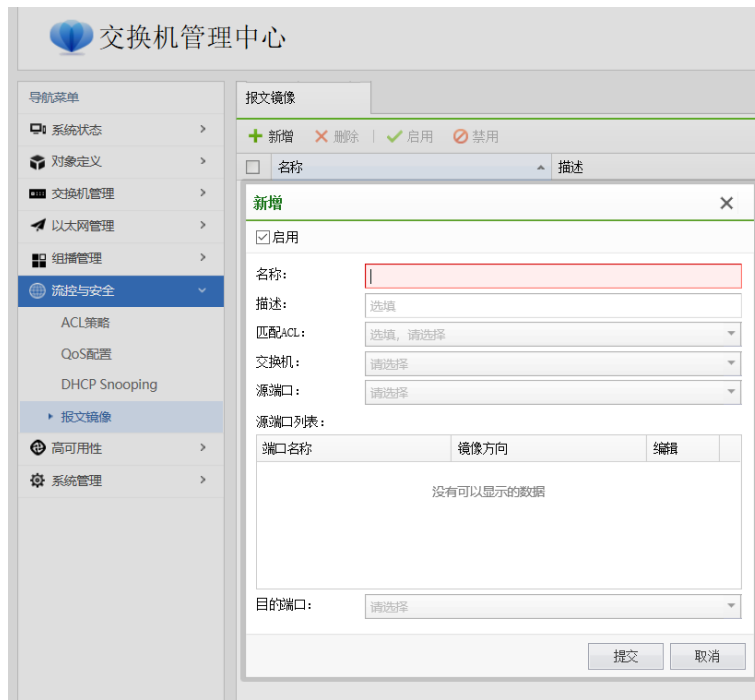
配置安视交换机的端口镜像功能

匹配 ACL：基于 ACL 进行匹配

交换机：批量选择安视交换机

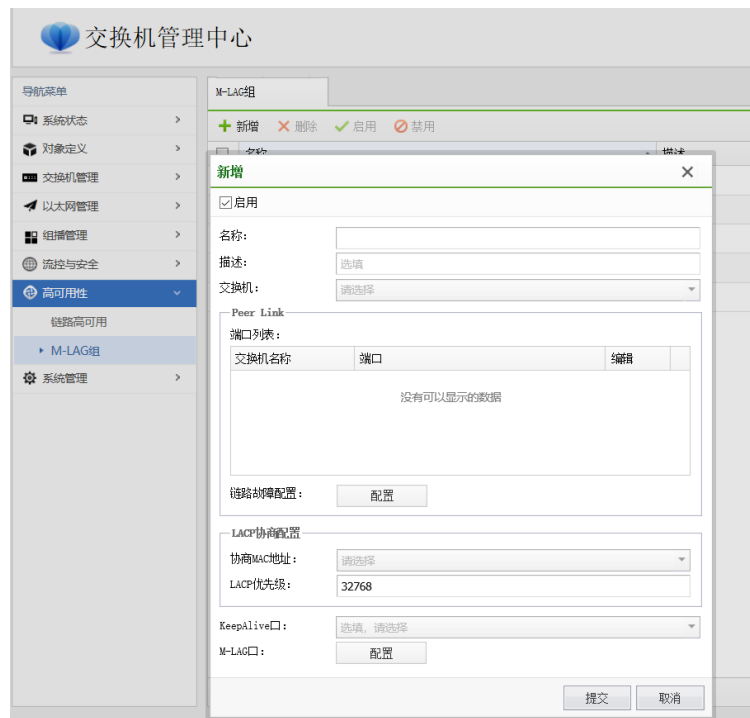
源端口：选择安视交换机需要被镜像流量的端口

目的端口：把流量镜像到该端口



2.4.12. 跨设备链路聚合

配置安视交换机的跨设备链路聚合

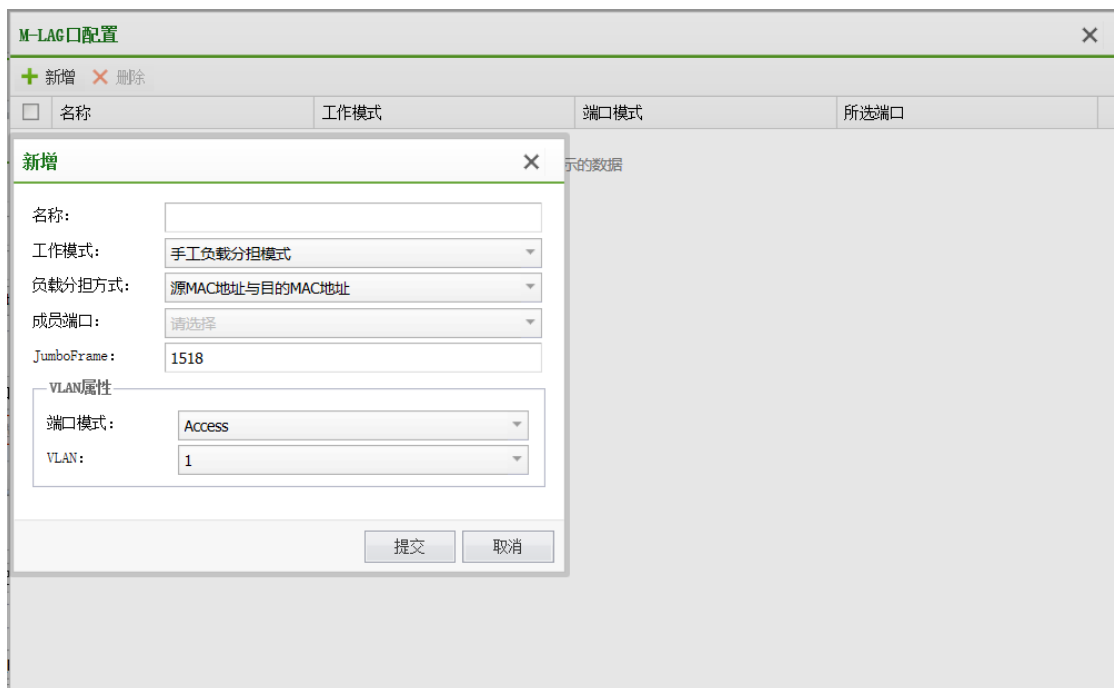


交换机：选择需要建立虚拟化系统的两台安视交换机

端口列表：选择安视交换机对应的端口作为 Peer-link 先连接口

KeepAlive 口：保障协商报文可靠性

M-LAG 口：确定业务端口的负载封单方式



The screenshot shows the 'M-LAG口配置' (M-LAG Port Configuration) window. A '新增' (Add) dialog box is open, allowing configuration of a new M-LAG link. The dialog includes the following fields:

- 名称 (Name): [Empty text box]
- 工作模式 (Work Mode): 手工负载均衡模式 (Manual Load Balancing Mode)
- 负载均衡方式 (Load Balancing Method): 源MAC地址与目的MAC地址 (Source MAC Address and Destination MAC Address)
- 成员端口 (Member Port): 请选择 (Please select)
- JumboFrame: 1518
- VLAN属性 (VLAN Attributes):
 - 端口模式 (Port Mode): Access
 - VLAN: 1

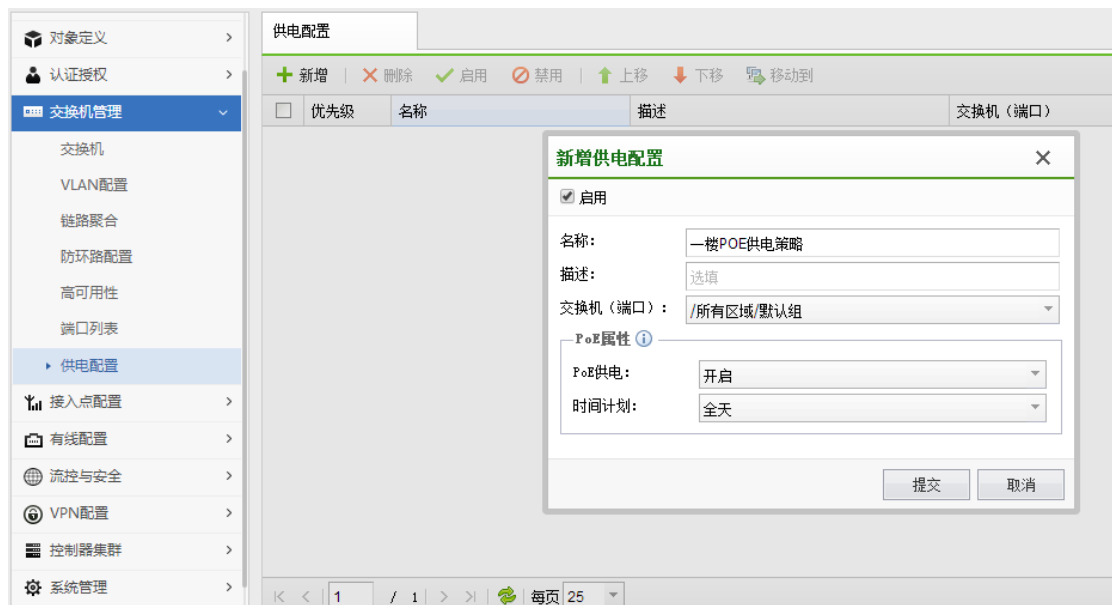
Buttons for '提交' (Submit) and '取消' (Cancel) are located at the bottom of the dialog.

2.4.13. 供电配置

配置交换机的供电选项



注意：供电配置仅对支持 POE 功能的交换机生效




名称：编辑策略名称

描述：对策略做描述

交换机（端口）：选择 POE 交换机的端口

POE 属性：关闭或开启 POE 供电，或根据时间计划来让 POE 交换机进行供电

 如果一台 POE 交换机被多个策略引用时，供电策略是由上往下依次匹配只有第一条策略会生效

2.5. 控制器有线配置

物理接口	端口聚合	VLAN接口	
刷新 启用 禁用			
网口	IP地址	线路	
<input type="checkbox"/> eth0 (管理口)	10.53.23.36/16	-	
<input type="checkbox"/> eth1	-	线路2	
<input type="checkbox"/> eth2	-	-	
<input type="checkbox"/> eth3	-	-	
<input type="checkbox"/> eth4	PPPoE (拨号已断开)	线路4	
<input type="checkbox"/> eth5	PPPoE (拨号已断开)	线路5	
<input type="checkbox"/> eth6	PPPoE (拨号已断开)	线路6	

2.5.1. 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。

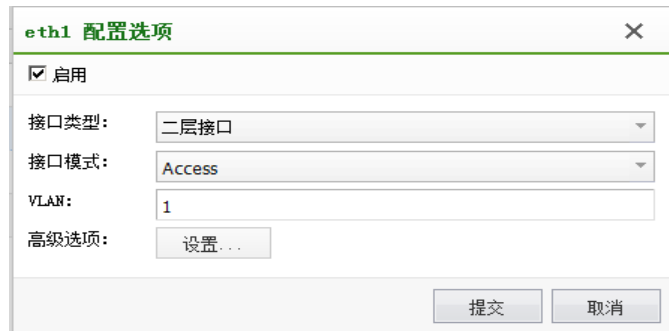
2.5.1.1. 物理接口

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。



2.5.1.1.1 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：



2.5.1.1.2 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，配置 DHCP 方法与地址池如下：

NAC 的 DHCP 配置比常规的 DHCP 服务器多了一个 option43 的选项，该选项的 IP 一般建议填写 NAC 的 IP。

保留 IP 地址可以将保留下来的地址分配给某个固定的终端。

保留 IP 设置
✕

+ 新增 ✕ 删除

<input type="checkbox"/>	名称	IP地址	MAC地址	编辑
	选择	单个IP地址或IP段	单个IP地址时可选	

确定 取消

确定 取消

2.5.1.2. 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 lACP 如下图：

物理接口	端口聚合	VLAN接口									
<div style="display: flex; justify-content: space-between; align-items: center;"> + 新增 ✕ 删除 🔄 刷新 </div> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 5%;"><input type="checkbox"/></th> <th style="width: 30%;">名称</th> <th style="width: 40%;">聚合网口</th> <th style="width: 25%;">工作模式</th> </tr> </thead> <tbody> <tr> <td></td> <td>channel1</td> <td>eth2, eth3</td> <td>负载均衡</td> </tr> </tbody> </table>				<input type="checkbox"/>	名称	聚合网口	工作模式		channel1	eth2, eth3	负载均衡
<input type="checkbox"/>	名称	聚合网口	工作模式								
	channel1	eth2, eth3	负载均衡								

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：

2.5.1.3. 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：

物理接口		端口聚合		VLAN接口	
+ 新增		X 删除		刷新	
VLAN ID		IP地址		MAC地址	
<input checked="" type="checkbox"/>	1	100.100.10.1/24		28-51-33-04-7B-CE	

每页 25 记录数: 1

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：

2.5.2. 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。

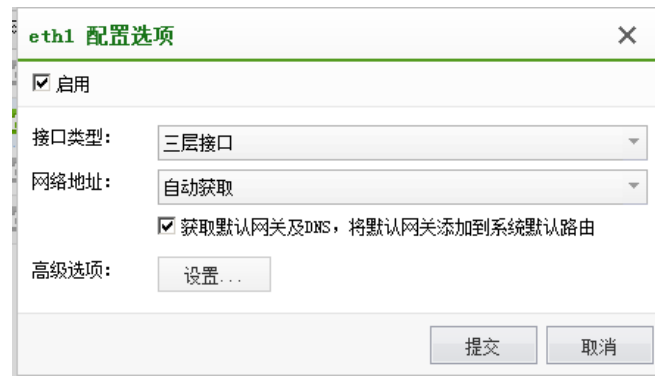
导航菜单	静态路由	网络IP组	策略路由	SNAT地址池	地址转换	DNS
系统状态	+ 新增 × 删除 📁 导入					
对象定义	<input type="checkbox"/> 目标地址	网络掩码	下一跳地址			
认证授权	<input type="checkbox"/> 114.114.115.115	255.255.255.255	172.222.222.42			
交换机管理	<input type="checkbox"/> 33.33.33.0	255.255.255.0	200.200.10.251			
接入点配置	<input type="checkbox"/> 172.16.100.0	255.255.255.0	200.200.10.251			
有线配置	<input type="checkbox"/> 172.16.205.0	255.255.255.0	200.200.10.251			
接口管理	<input type="checkbox"/> 172.16.227.0	255.255.255.0	200.200.10.251			
网络配置	<input type="checkbox"/> 192.100.100.0	255.255.255.0	200.200.10.251			
线路带宽	<input type="checkbox"/> 199.201.0.0	255.255.252.0	200.200.10.251			
有线认证	<input type="checkbox"/> 10.0.0.0	255.255.0.0	200.200.10.251			
流控与安全	<input type="checkbox"/> 10.53.0.0	255.255.0.0	10.19.0.254			
VPN配置	<input type="checkbox"/> 172.16.0.0	255.255.0.0	200.200.10.251			
控制器集群	<input type="checkbox"/> 192.200.0.0	255.255.0.0	200.200.10.251			
系统管理	<input type="checkbox"/> 199.200.0.0	255.255.0.0	200.200.10.251			
系统维护	<input type="checkbox"/> 200.200.0.0	255.255.0.0	200.200.10.251			
	<input type="checkbox"/> 201.200.0.0	255.255.0.0	200.200.10.251			
	<input type="checkbox"/> 10.0.0.0	255.0.0.0	200.200.10.251			
	<input type="checkbox"/> 0.0.0.0	0.0.0.0	200.200.10.200			

2.5.2.1. 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。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：



2.5.2.2. 网络 IP 组

静态路由	网络IP组	策略路由	SNAT地址池	地址转换	DNS	
+ 新增 × 删除 <input type="text" value="请输入名称或IP"/>						
<input type="checkbox"/>	名称	描述	IP地址		操作	
<input type="checkbox"/>	全部	所有IP地址	0.0.0.0-255.255.255.255		-	
<input type="checkbox"/>	Private IP	All private IP	172.16.0.0-172.31.255.255,192.168.0.0-192.168.255.255		-	
<input type="checkbox"/>	IP Selection		10.10.4.5-10.10.4.25,10.10.2.25-10.10.2.50		✗	
<input type="checkbox"/>	Not for Lupko		192.168.31.2		✗	
<input type="text" value="1"/> / <input type="text" value="1"/> > > 每页 25 记录数: 4						

2.5.2.3. 策略路由

静态路由	网络IP组	策略路由	SNAT地址池	地址转换	DNS			
+ 新增 × 删除 ✓ 启用 ✗ 禁用 ↑ 上移 ↓ 下移 移动到 <input type="text" value="名称、IP地址或协议"/>								
<input type="checkbox"/>	优先级	名称	源IP组	目的IP组	协议	接口/下一跳地址	描述	状态
<input type="checkbox"/>	1	内网_0.254	全部	流控用_访问内网的...	all	200.200.0.254		✓
<input type="checkbox"/>	2	访客外网_eth6	路由用_访客_172网段	全部	all	eth2	eth2	✓
<input type="checkbox"/>	3	员工外网_路线1	路由用_员工_分组1	全部	all	eth1	eth1	✓
<input type="checkbox"/>	4	员工外网_路线2	路由用_员工_分组2	全部	all	eth4	eth4	✓
<input type="checkbox"/>	5	员工外网_路线3	路由用_员工_分组3	全部	all	eth5	eth5	✓
<input type="checkbox"/>	6	线路备份4	全部	全部	all	eth5	eth5	✓
<input type="checkbox"/>	7	线路备份1	全部	全部	all	eth1	eth1	✓
<input type="checkbox"/>	8	线路备份2	全部	全部	all	eth2	eth2	✓
<input type="checkbox"/>	9	线路备份3	全部	全部	all	eth4	eth4	✓
<input type="text" value="1"/> / <input type="text" value="1"/> > > 每页 25 记录数: 9								

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：

新增源地址策略路由 ✕

启用

名称:

描述:

源IP组:

目的IP组:

协议:

接口/下一跳: 接口

下一跳

添加到:

2.5.2.4. SNAT 地址池

静态路由	网络IP组	策略路由	SNAT地址池	地址转换	DNS	
+ 新增		✕ 删除		请输入名称或IP地址		
名称	IP地址(范围)	描述	操作			
<input type="checkbox"/> 200.200.0.38	200.200.0.38-200.200.0.38		被引用			
<input type="checkbox"/> 无线SNAT	172.16.0.1-172.16.254.253		✕			

记录数: 2

2.5.2.5. 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

静态路由		网络IP组		策略路由		SNAT地址池		地址转换		DNS			
+ 新建 × 删除 ✓ 启用 ✗ 禁用 ↑ 上移 ↓ 下移 📁 移动到 📄 导入 📄 导出													
□	优先级	名称	类型	原始数据包				转换后数据包					
				源地址	目的地址	协议	入接口	出接口	源地址	目的地址	目的端口	状态	
□	1	11APnat	源地...	AP	全部	所有	vlanif11	eth3, et...	出接口地址	-	-		✓
□	2	无线用户NAT	源地...	全部	流控用_...	所有	eth0, et...	eth3	200.200....	-	-		✓
□	3	公网线路NAT	源地...	全部	全部	所有	vlanif21...	eth1, et...	出接口地址	-	-		✓

< < | 1 | > > | 📄 每页 25 | 记录数: 3

2.5.2.5.1. 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。

添加源地址转换

启用

名称:

转换条件

源地址:

入接口:

出接口:

转换后数据包

源地址转换为:

添加到:

2.5.2.5.2. 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。

2.5.2.6. 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。

2.5.3. 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 vlanid，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。

2.5.4. 有线认证（基于控制器）

经过 NAC 控制器的有线用户，可以选择对有线用户进行认证，认证策略在【有线配置】-【有线认证】下配置策略。

<ul style="list-style-type: none"> 系统状态 > 对象定义 > 认证授权 > 接入点配置 > 有线配置 > <ul style="list-style-type: none"> 接口管理 网络配置 线路带宽 有线认证 流控与安全 > VPN配置 > 控制器集群 > 系统管理 > 系统维护 > 	接口区域	认证策略		
	<input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用 在非信任接口区域内的接口，会拒绝未能匹配中该接口上所配认证策略的报文通过			
	<input type="checkbox"/>	区域名称	接口	共启用3条，总共64条 全部显示
	<input type="checkbox"/>	非受信任区域	eth0	
	<input type="checkbox"/>	区域1	eth0, v1ani f200	
	<input type="checkbox"/>	区域2	eth1	
	<input type="checkbox"/>	区域3		
	<input type="checkbox"/>	区域4		
	<input type="checkbox"/>	区域5		
	<input type="checkbox"/>	区域6		

2.5.4.1. 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。

接口区域	认证策略	
<input checked="" type="checkbox"/> 启用 <input type="checkbox"/> 禁用 在非信任接口区域内的接口，会拒绝未能匹配中该接口上所配认证策略的报文通过		
<input type="checkbox"/>	区域名称	接口
共启用3条，总共64条 全部显示		
<input type="checkbox"/>	非受信任区域	eth0
<input type="checkbox"/>	区域1	eth0, v1ani f200
<input type="checkbox"/>	区域2	eth1
<input type="checkbox"/>	区域3	
<input type="checkbox"/>	区域4	
<input type="checkbox"/>	区域5	
<input type="checkbox"/>	区域6	
<input type="checkbox"/>	区域7	
<input type="checkbox"/>	区域8	
<input type="checkbox"/>	区域9	

2.5.4.2. 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

新增有线用户认证策略
✕

启用

- 基本配置
- 认证类型
- 账号认证
- 权限设定

策略名称:	<input type="text" value="vlan1认证"/>
策略描述:	<input type="text" value="选填"/>
接口区域:	<input type="text" value="区域2"/>
适用范围:	<input type="text" value="0.0.0.0-255.255.255.255"/>

2.5.4.3. 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。

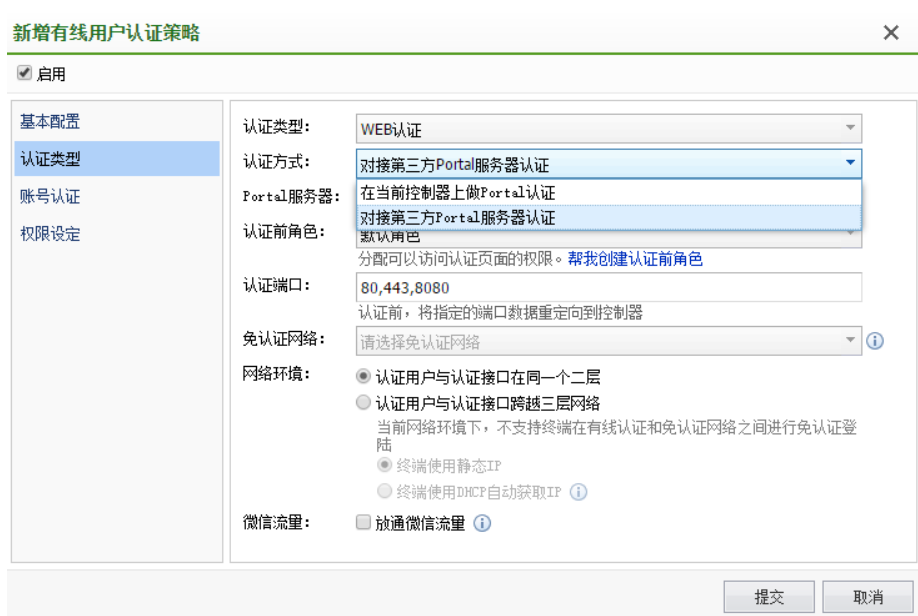
新增有线用户认证策略
✕

启用

- 基本配置
- 认证类型
- 账号认证
- 权限设定

认证类型:	<input type="text" value="IP地址认证"/>
以此组上线:	<input type="text" value="WEB认证"/> <input type="text" value="IP地址认证"/> <input type="text" value="单点登录用户(免二次认证)"/>

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。



2.5.5. 有线认证应用场景及其优势介绍

2.5.5.1. 交换机支持有线认证

【优势体现】

- 1 支持 portal 和 802.1x 认证，满足用户边缘接入安全需求；
- 2 针对不同人员上网需求，提供多类的准入方案，如：账号认证、访客认证、证书认证；
- 3 针对不同类型的终端的特性，提供多类的准入方案，如：办公 PC 等可以采用账号认证、证书认证；打印机、摄像头等哑终端可以采用免认证的方式接入网络

2.5.5.2. 支持无线网络异构

【优势体现】

- 1 支持不同厂商的 AP 部署相同的 portal 认证（我司和友商 AP 混用，不同友商混用），方便已有网络加点和改造；
- 2 支持对接客户已有的认证服务器和账号数据库，无需更换认证账号系统，降低网络改

造成本

2.5.5.3. 有线无线一体化

【优势体现】

1 统一认证,业务随行,不管终端在什么位置接入,无论通过交换机有线还是无线网络,接入认证后都有相同的上网权限

2 终端免认证,无线有线整网通用

目前我们的交换机支持的有线认证可以**基于端口**和 **VLAN**,简单来说这二者的区别如下

1.如果目前客户那边的仅想让某些 **vlan** 的用户认证上网,所以我们可以选择基于 **VLAN**(基于 **vlan** 的话还需要选择端口,其作用为在那些端口下的所选 **VLAN** 需要认证)

2.如果客户想让交换机的某些端口都要做认证的话就选择基于端口

注意事项:3.7.6 版本的交换机支持有线认证,**胖模式不支持认证**

2.5.5.4. 实例一.有线 web 认证(二维码审核)

场景一:

客户场景: 由于客户的公司时而有访客来参观走访,故需要接入有线电脑使用。如果使用 802.1x 认证的话,每次访客来访的话都需要创建账号(需要定期更换,不然会导致账号泄漏造成不安全),对用户数据库做修改,这样对网络管理员来说的运维成别较大。

解决方案: 使用有线认证的二维码审核解决,每次访客接入交换机的终端需要通过网络管理员的许可以后,分配访客权限然后入网

优势: 减低运维成本,可支持远程审核方便网络管理员管理,审核后可以根据需求分配访客权限

2.5.5.4.1 认证流程

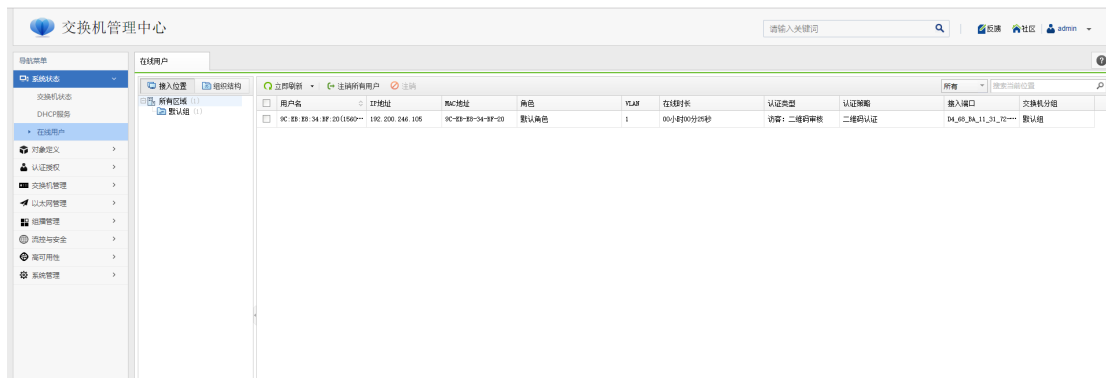
1.电脑接入网口以后，分配到地址自动弹出页面，填写姓名点击下一步



2.登入云助手 APP，这时候打开二维码审核可以使用扫码审核和远程审核(可以并用)。一般推荐远程审核，打开远程审核就可以审核用户，给用户分配对应角色和上网时长



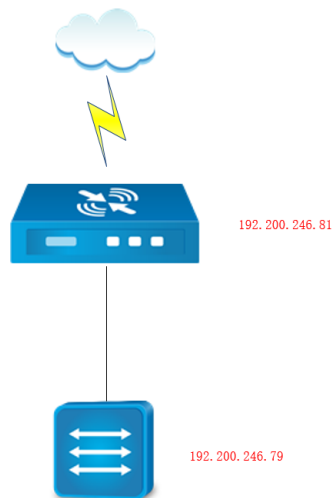
3.通过审核以后可以在【系统状态】-【在线用户】中看到用户信息



2.5.5.4.2 有线认证配置

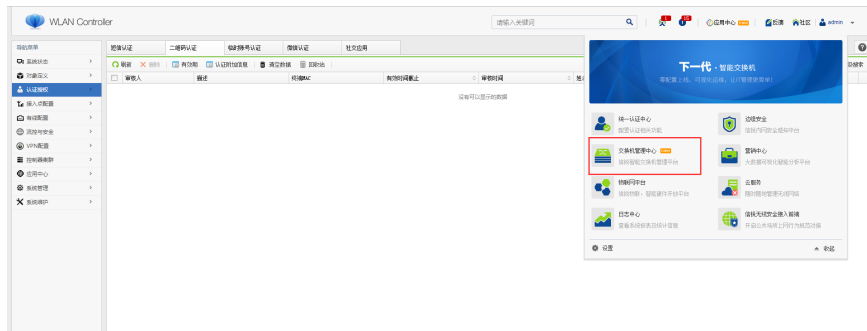
需要注意:有线认证的二维码审核,控制器需要登入云管家,使用云助手 APP 来审核

拓扑如下:

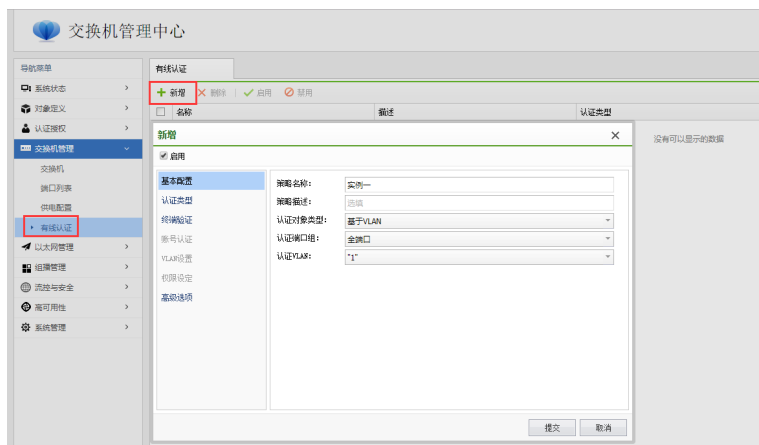


根据以上需求我们得知是需要根据匹配 VLAN 来实现有线认证的

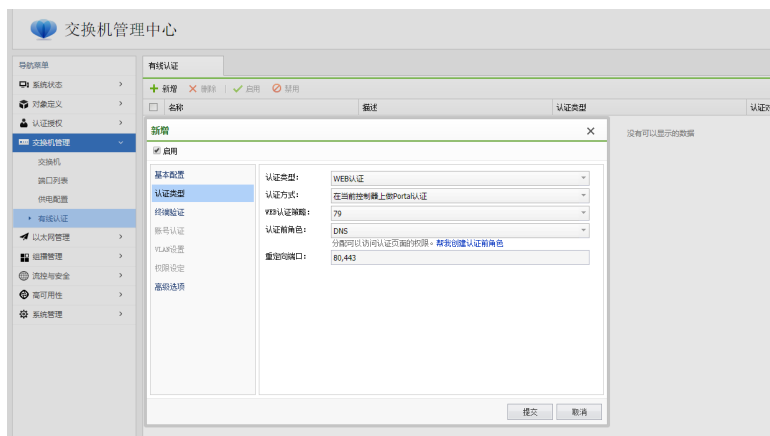
1.打开交换机管理中心,【应用中心】-【交换机管理中心】



2. 点击【有线认证】新增一个策略，策略名称自拟，认证对象类型选择基于 VLAN，认证端口组选择交换机上需要认证的端口(可以在【交换机管理】-【端口列表】-【端口组】里面定义和添加)，认证 VLAN 选择对应的需要认证的 VLAN



3. 认证类型选择 WEB 认证

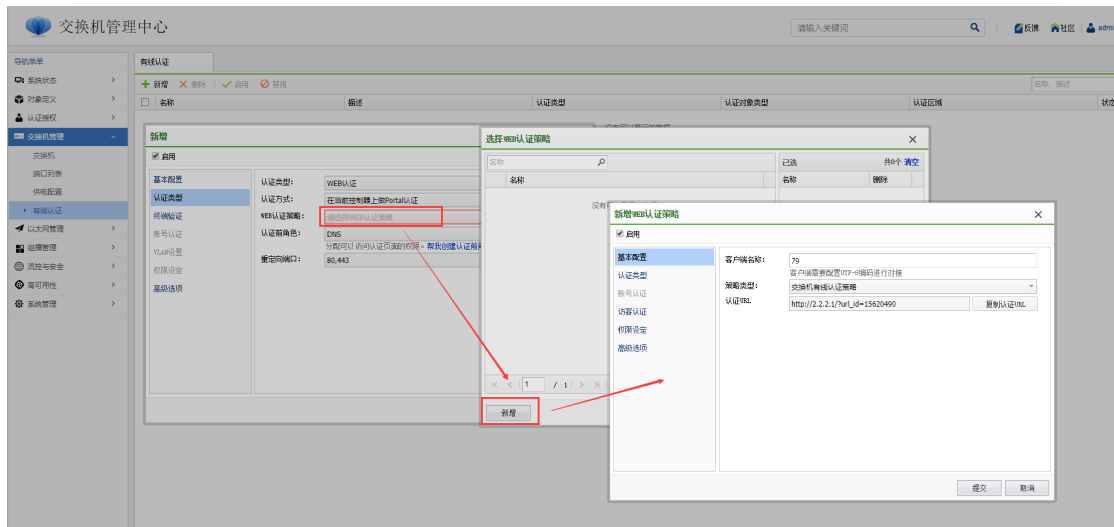


认证方式选择在本地控制器上对 portal 认证

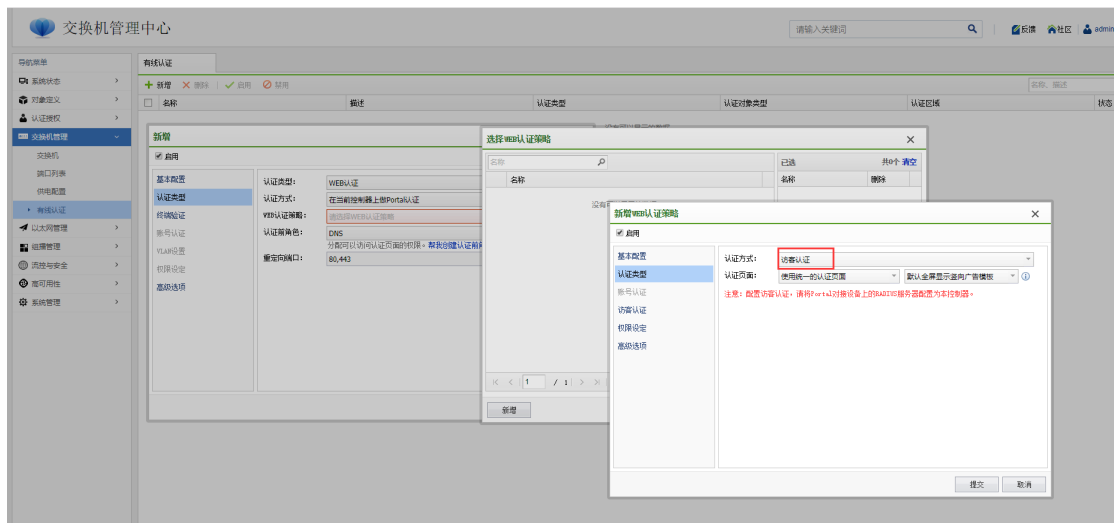
认证前角色：配置一个仅放通 DNS 的角色即可(可以点击“帮我创建认证前角色”)

重定向端口 80, 443

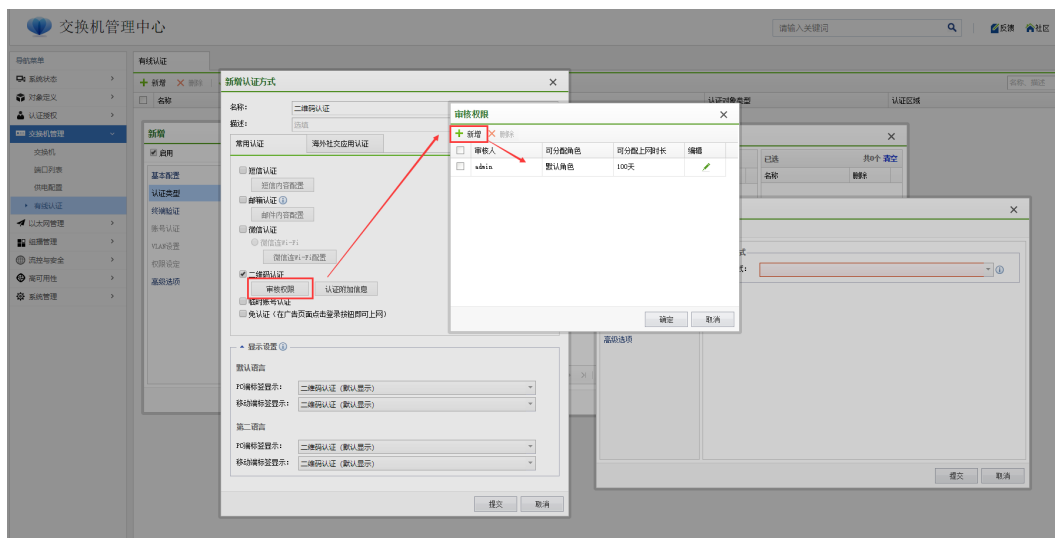
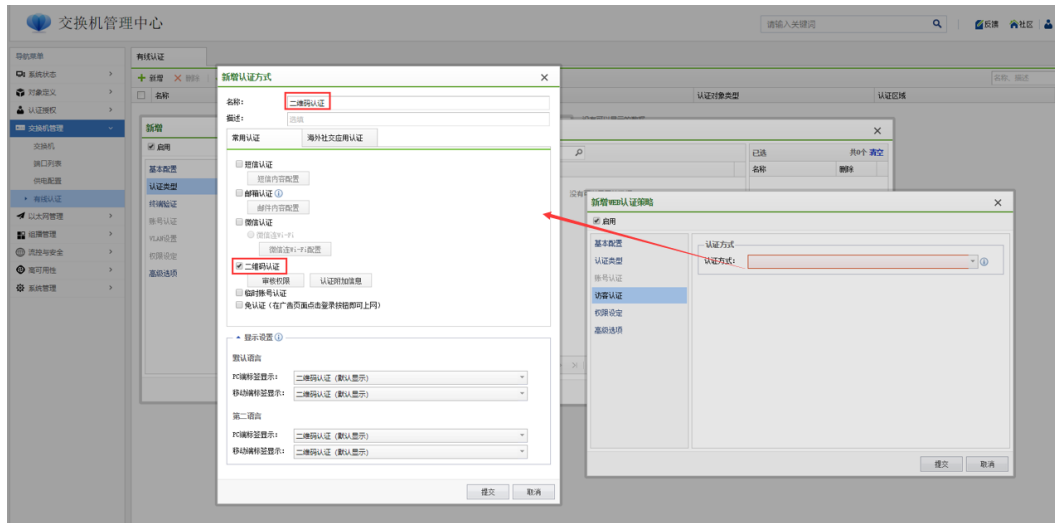
4.对应的 WEB 认证策略在【认证授权】-【Portal 服务】-【WEB 认证策略】中配置，也可以在配置页面直接添加。**注意策略类型需要选择交换机有线认证策略**



5.然后在 WEB 认证策略这边的认证类型选择访客认证



6.访客认证中的认证方式在【认证授权】-【WEB 页面】-【访客认证】中配置和修改，也可以直接在这边的页面配置

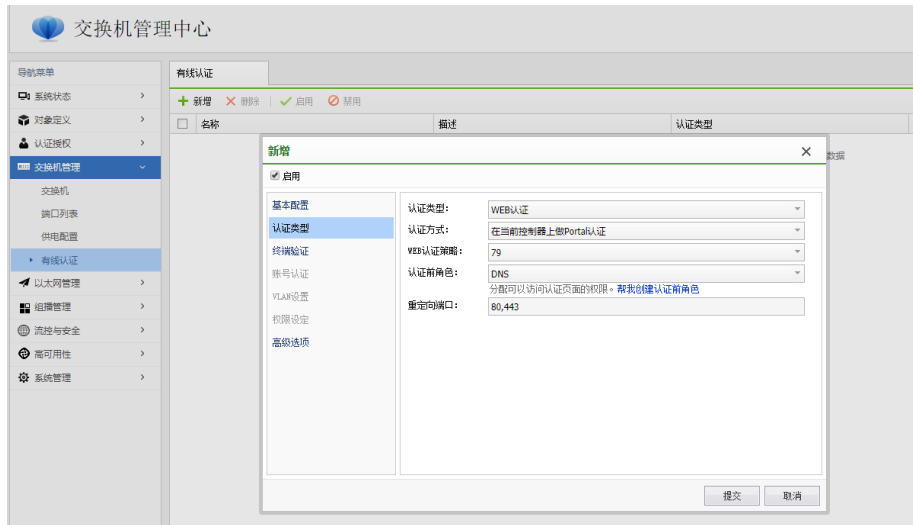


需要注意的是:这边的审核人需要勾选管理员账号 admin

可分配角色选择对应权限的角色即可, 这边分配默认角色

上网时长默认是 10 分钟, 1 小时和 1 天。这个时长可以自行拟定, 路径在【认证授权】-【访客认证】-【二维码审核】-【有效期】, 最长可以设置为 1000 天。

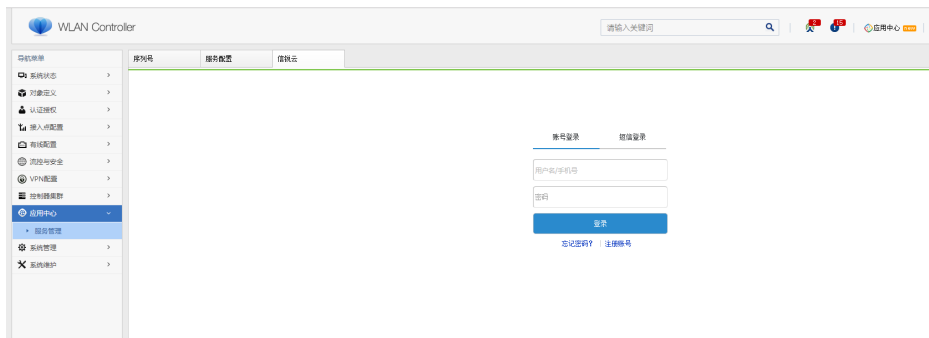
按以上方式设置以后可以点击提交然后调用该认证策略,就完成认证类型的配置



如果想要开启终端校验和免认证终端就在终端验证这边开启即可，若无就完成有线认证配置。

2.5.5.4.3 登入云管家

在控制器的【应用中心】-【服务管理】-【信锐云】，登入云管家



看到用户在线即可



手机上需要下载一个信锐云助手的 APP，然后也登入 APP。在 APP 的管理中可以切换控制器，然后在应用的二维码审核中可以审批二维码

2.5.5.5. 实例二. 802.1X 认证

场景二：

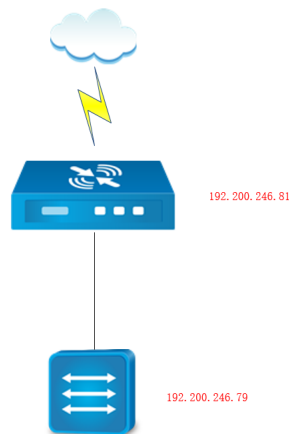
客户场景：客户是学校场所，想实时看到用户信息，且接入有线校园网的时候需要按时间来计费，且不想让无线共享设备接入有线网络。

解决方案：采用信锐安视交换机来做 802.1x 认证，且在端口上开启终端类型绑定(仅允许笔记本接入)、

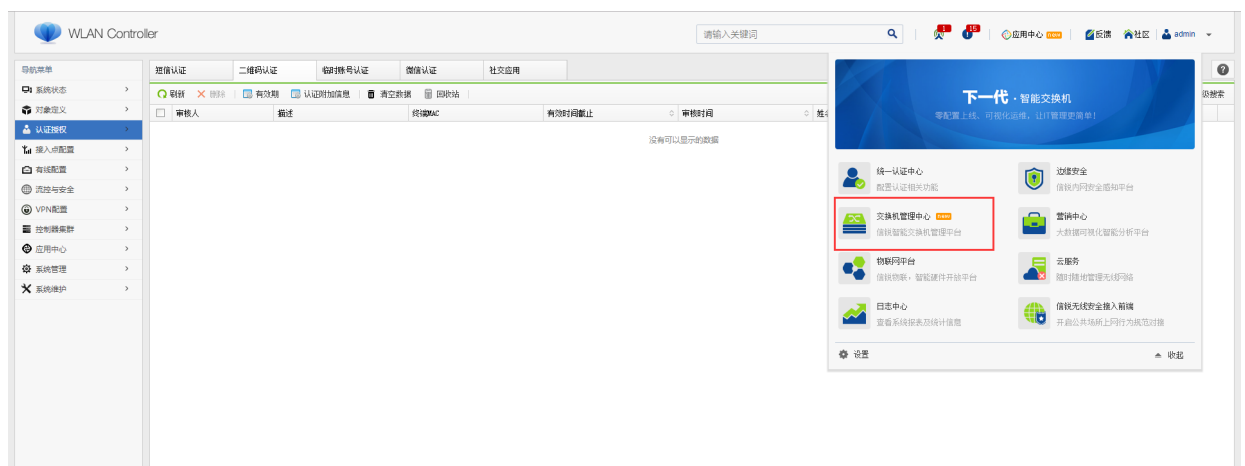
优势：用户数据直观(可以在 web 页面直接看到用户信息)，禁止网络被共享，图形化配置简单

2.5.5.5.1 有线认证配置

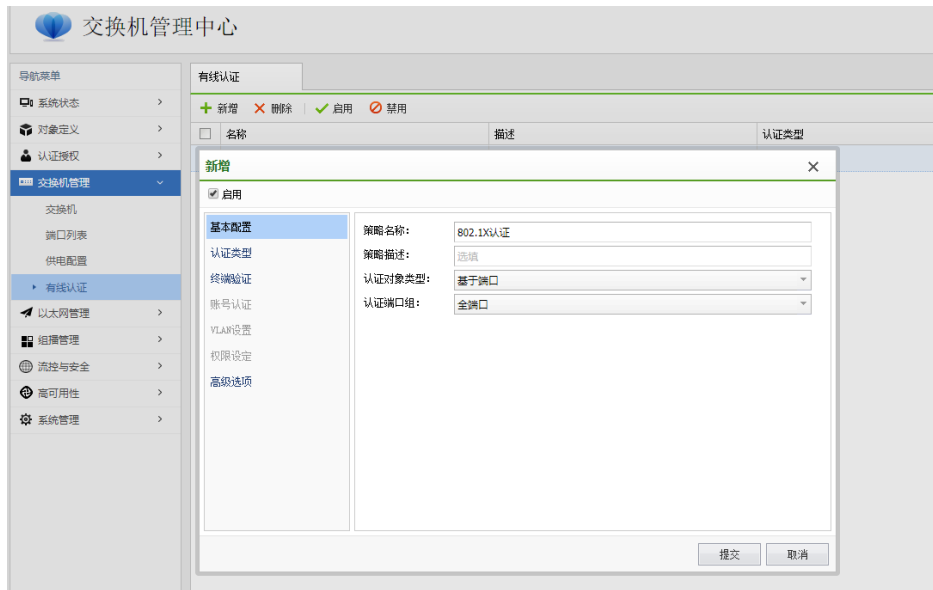
拓扑图如下：



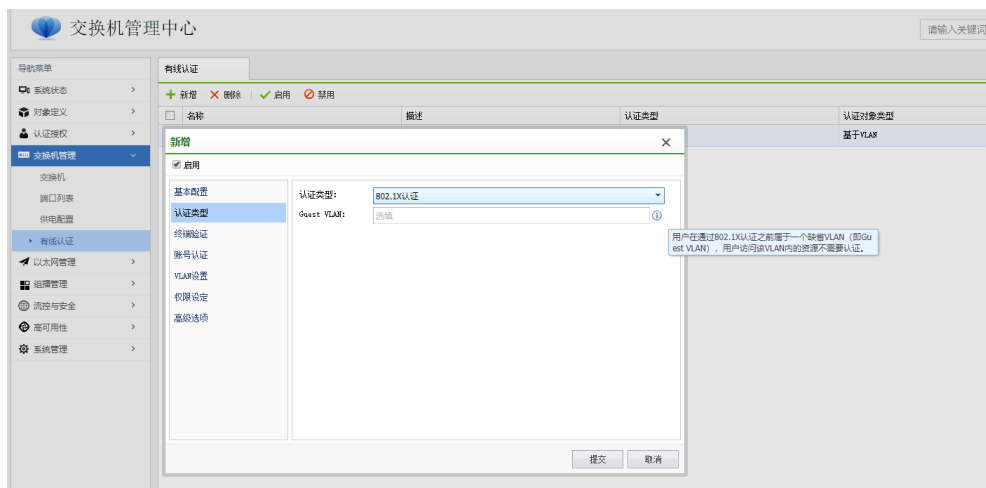
1.打开交换机管理中心，【应用中心】-【交换机管理中心】



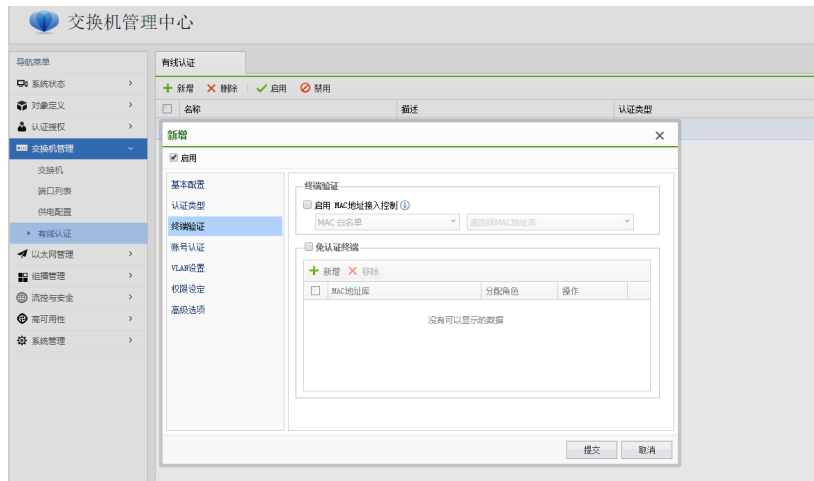
2.点击【有线认证】新增一个策略，策略名称自拟，认证对象类型选择基于端口，认证端口组选择交换机上需要认证的端口(可以在【交换机管理】-【端口列表】-【端口组】里面定义和添加)



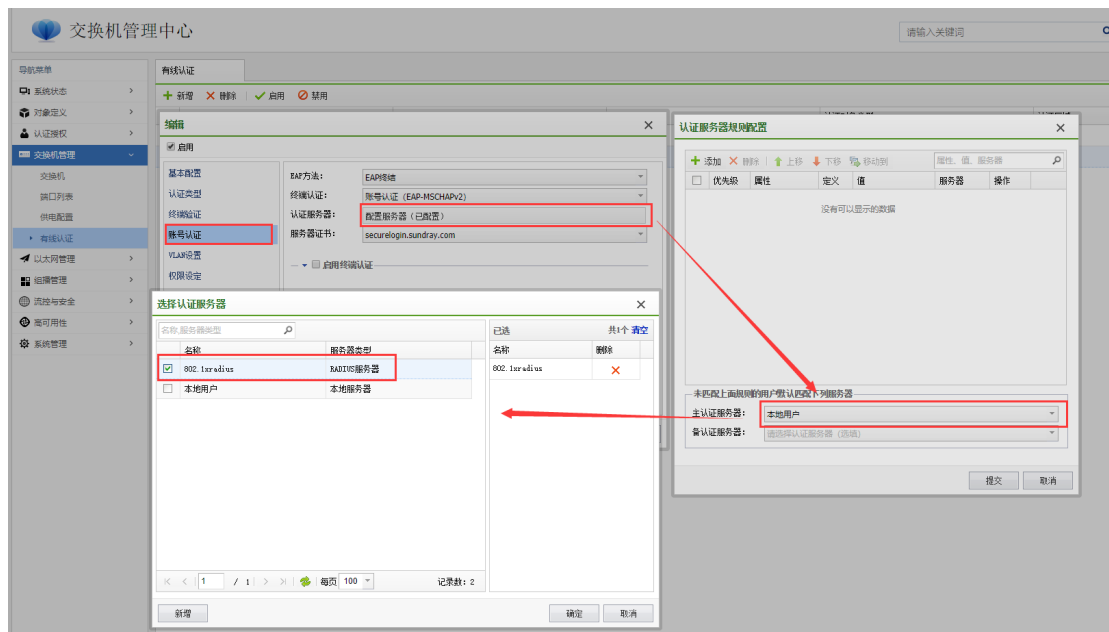
3. 认证类型中选择 802.1x 认证，guest vlan 可以不填写



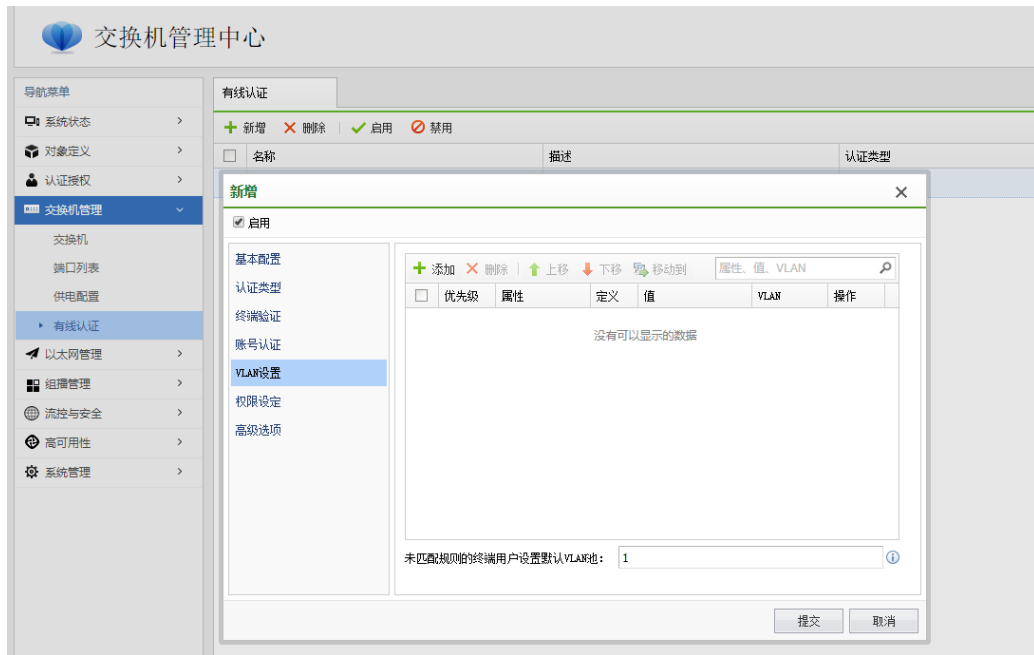
4. 在终端认证中可以开启 MAC 地址接入控制器和免认证终端，这个选项根据需求开启即可，这边不做配置



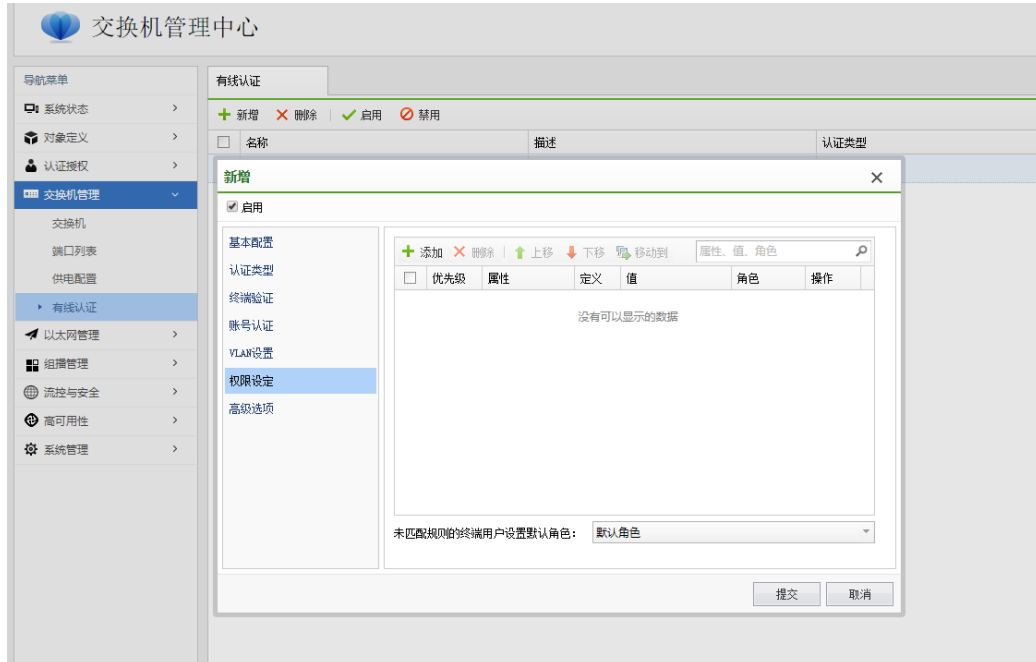
5.在账号认证这边选择对应认证服务器即可(可以在【认证授权】-【外部服务器】中添加), 这边使用的是本地服务器



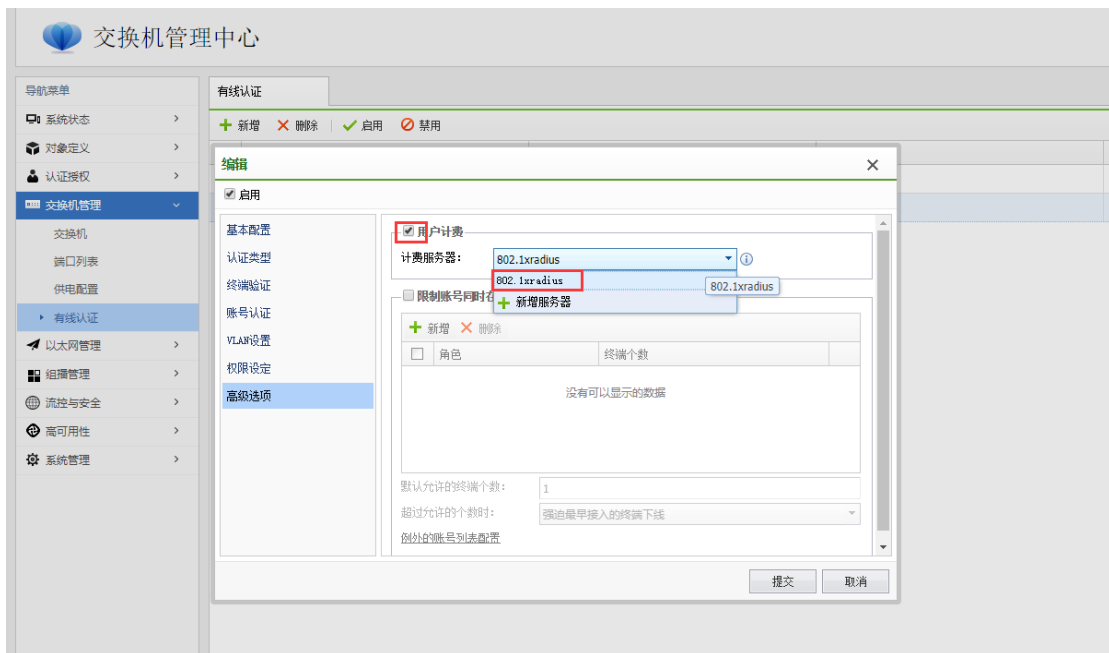
6.认证后 VLAN 可以根据权限设定在添加里面设置, 这边使用的是缺省 vlan 1



7.在权限设定这边设置认证后的角色，这边使用默认角色，具体角色需要根据情况来设置



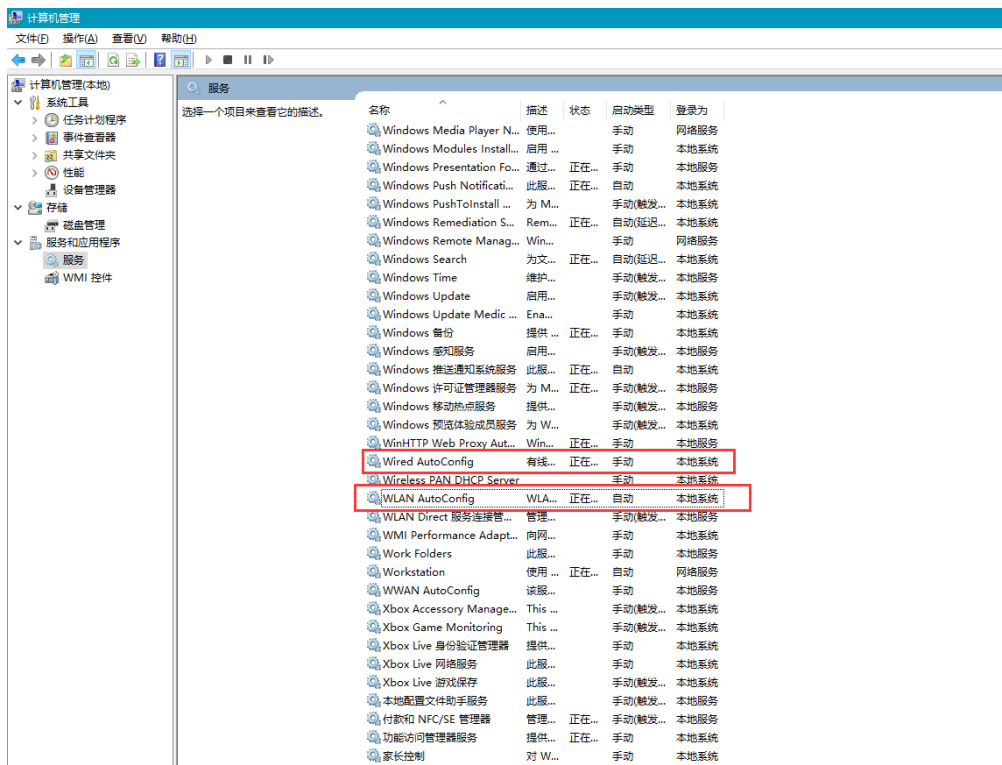
8.高级选项中可以开启计费功能，前提是对接的第三方 radius 服务器支持计费。



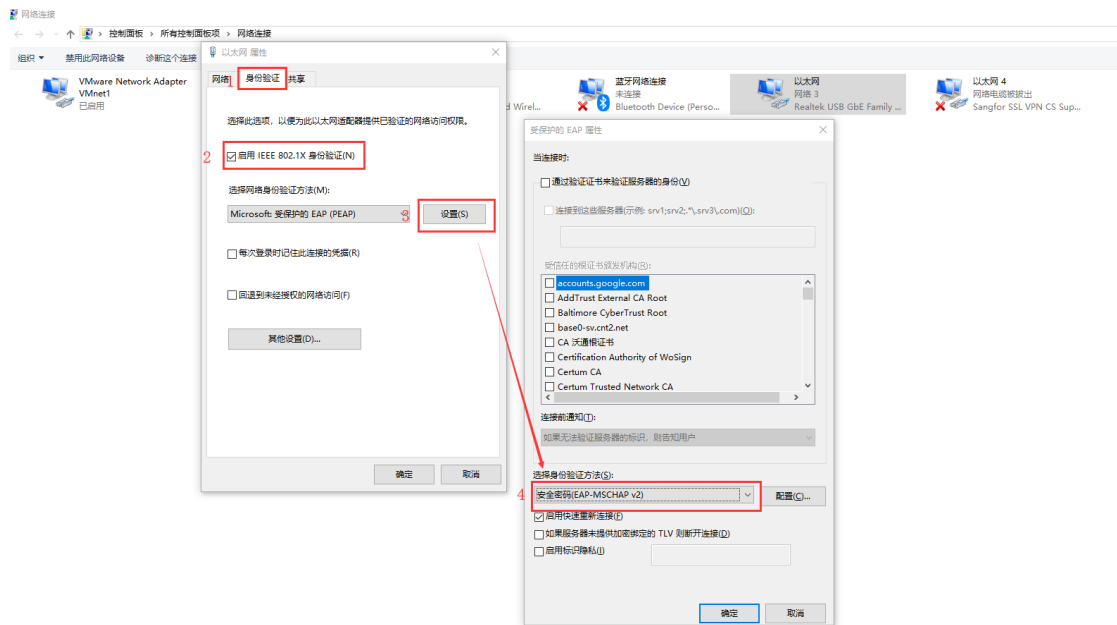
这样设置以后点击提交，就完成配置

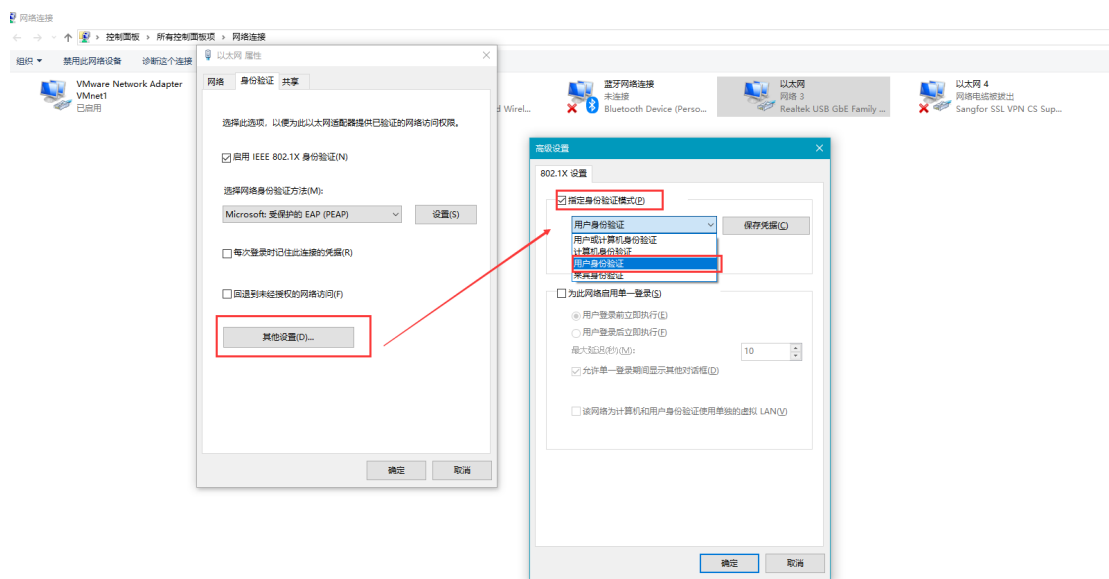
2.5.5.5.2 认证流程

1.右键我的电脑打开管理，点击服务。启动 Wired Autoconfig 和 WLAN AutoConfig 这两个服务



2.打开网卡适配器页面，选中所使用的网卡右键属性，然后如图操作





按照以上配置以后，电脑接上开启 802.1x 认证的端口就可以自动弹出认证框，输入正确的用户名密码即可上网



2.6. 边缘可视

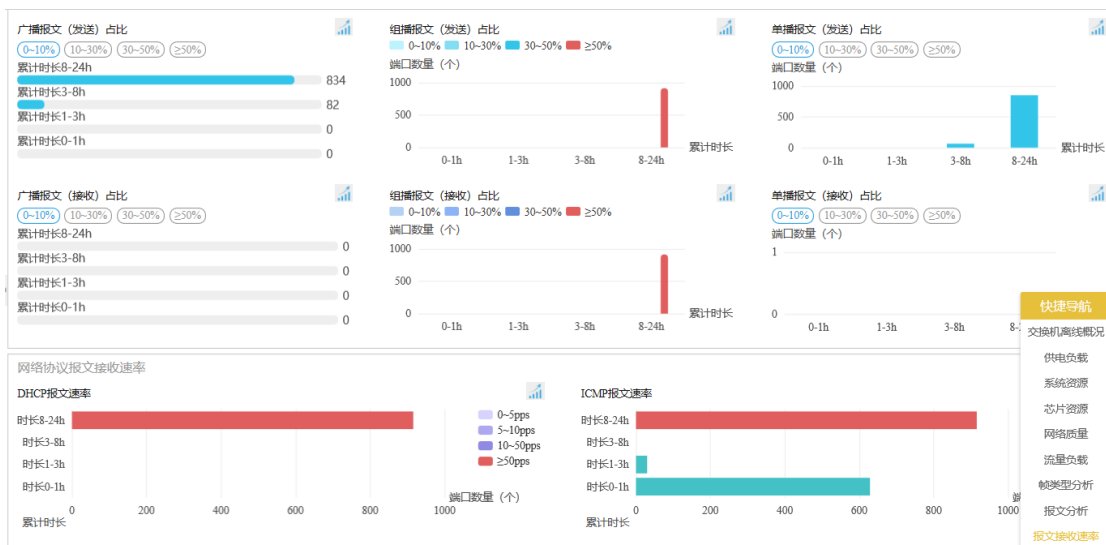
『边缘安全』主要包括【终端状态】、【业务感知】

【终端状态】当终端接入网络，通常我们都非常关注这些终端在网络里的状态，为了满足客户的需求，我们在边界终端管理上从多个角度去分析了当前终端的安全状态：

- 1) 终端在网络中发生的安全事件（终端类型/位置/地址异常）
- 2) 终端端口迁移记录及次数
- 3) 网络中终端接入类型分布



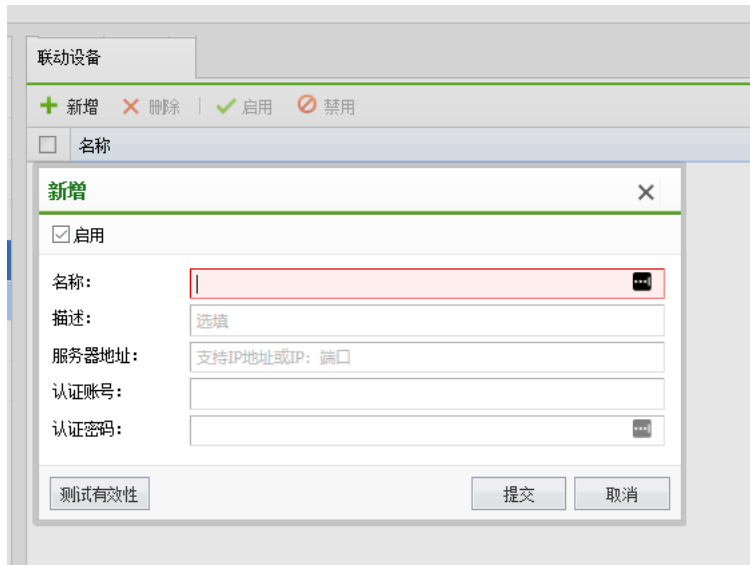
【业务感知】在边缘可视里面点击业务感知，再点击交换机即可



2.7. 边缘监控

『边缘监控』主要包括【安全联动】、【智能告警】

在控制器页面的【边缘监控】点击【安全联动】进入配置页面



在控制器页面的【边缘监控】点击【智能告警】进入配置页面

交换机告警事件

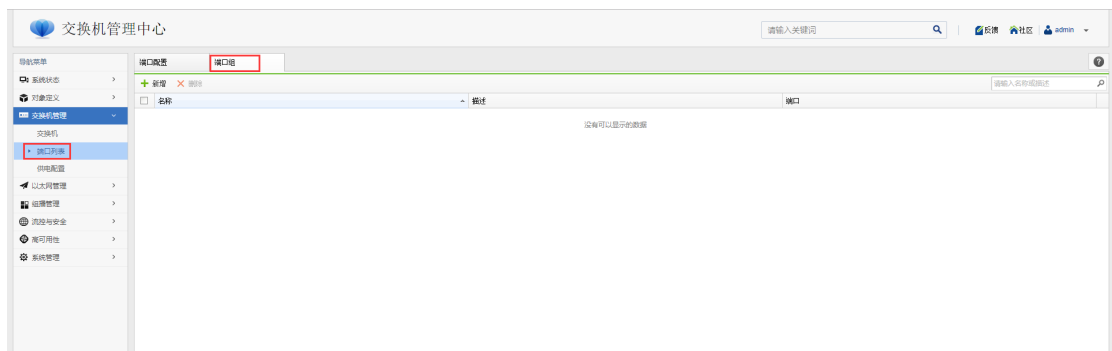
事件	触发条件	状态
交换机离线	离线时长5分钟	✓
MAC地址表利用率超阈值	上限阈值80%	✓
ARP表利用率超阈值	上限阈值80%	✓
单网口环路	-	✓
接口状态变化	状态变化持续时长5分钟	✓
接口协商速率下降	-	✓
接口错报报文速率超阈值	上限阈值200pps	✓
接口泛洪报文超阈值	占比上限阈值80%:速率上限阈值200pps	✓

2.8. 边缘安全配置

在控制器页面的【应用中心】点击【边缘安全】进入配置页面



其中端口组的配置在【交换机配置中心】-【交换机管理】-【端口列表】-【端口组】中配置



2.8.1. 场景一.准确识别终端和网络资产统计

终端状态跟踪即用于跟踪连接交换机端口的终端状态，包括在线、离线、终端类型等具体信息并显示在状态页面。可以满足客户以下几个使用场景：

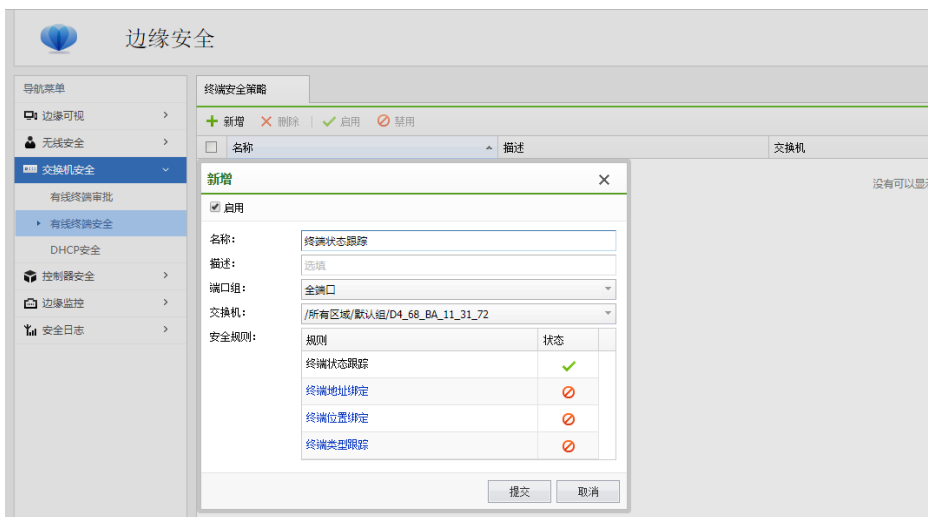
- 1、客户需要知道接入交换机上的接口都接了什么类型的设备，需要能直观的看出；
- 2、某些接口上接着服务器或者重要的终端设备，需要能够实时的观察到这些终端的状态，包括但不限于终端离线次数、终端在线时间等。

在边缘安全中【交换机安全】-【有线终端安全】新增一个终端安全策略，默认勾选终端状态跟踪。

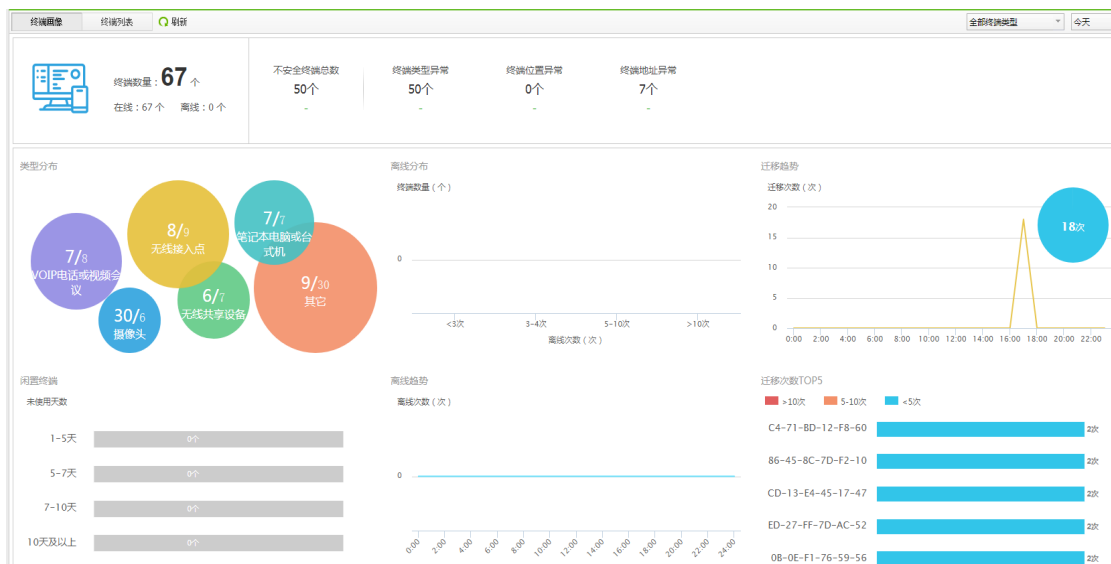
配置步骤：

第一步：添加端口组

第二步：选择交换机



其实现效果如下图：



2.8.2. 场景二.终端防替换与防冒接入(终端地址绑定)

终端地址绑定主要运用场景为：防止终端设备被恶意替换

若将摄像头替换为仿冒设备（例如笔记本或台式机），则可以通过终端地址校验(终端的 IP 发生变化)感知。



状态	MAC地址	终端类型	主机名	IP地址
●	B5-2B-B9-E6-6B-06	笔记本电脑或台式机	lhj_b5:2b:b9:e6:6b:06	121.46.242.111
●	终端地址绑定校验不通过	摄像头	lhj_cf:73:a6:8e:f8:20	121.46.194.132
●	65-43-35-2C-87-4A	苹果移动终端	lhj_65:43:35:2c:87:4a	121.46.31.48
●	17-28-45-25-48-71	投影仪	lhj_17:28:45:25:48:71	121.46.75.149
●	26-0C-C8-1C-C3-7F	WINDOWS移动终端	lhj_26:0c:c8:1c:c3:7f	121.46.132.148
●	86-45-8C-7D-F2-10	VOIP电话或视频会议	lhj_86:45:8c:7d:f2:10	121.46.96.200
●	5E-42-1F-6F-4A-33	路由器	lhj_5e:42:1f:6f:4a:33	121.46.35.172
●	2B-79-4D-5F-A8-0F	安卓移动终端	lhj_2b:79:4d:5f:a8:0f	121.46.110.65
●	12-38-61-91-75-23	打印机或扫描仪	lhj_12:38:61:91:75:23	121.46.178.18
●	95-4A-E4-DB-2E-39	投影仪	lhj_95:4a:e4:db:2e:39	121.46.29.188

终端地址绑定即 IP/MAC 绑定，用于绑定有线终端的 IP 和 mac

可以配置启用自动审批，最大可配置自动审批 10000 个（如配置自动审批 10 个，即前 10 个接入进来的有线终端可以自动审批，第 11 个终端就需要手动审批）；

支持配置免审批地址，终端以该地址上线即可上网(相当于这个 IP 不做 IP/MAC 绑定)；

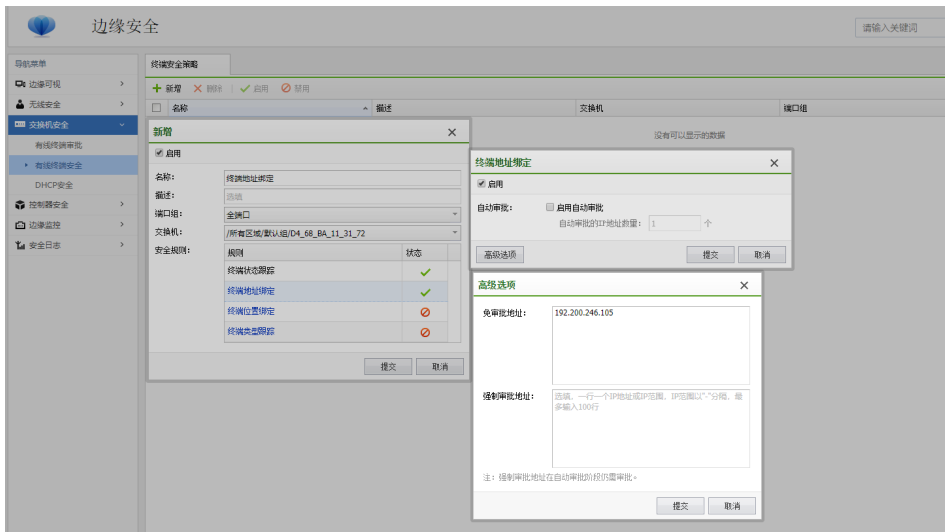
支持配置强制审批地址，即使自动审批的终端个数还没用完，以该地址上线的终端也需要手动审批

配置步骤：

第一步：添加端口组

第二步：选择交换机

第三步：打开终端地址绑定，可以添加免审批地址和启用自动审批



可在【交换机安全】->【有线终端审批】->【待审批】里看到需要审批的终端，勾选审批即会出现在已审批列表里



2.8.3. 场景三. 终端防替换与防冒接入(终端位置绑定)

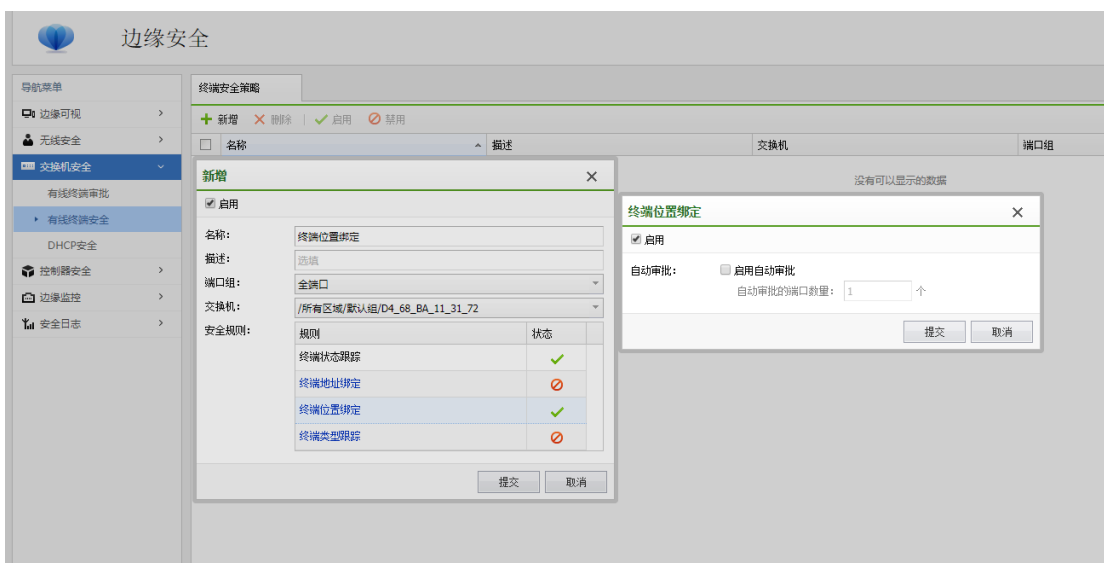
终端位置绑定主要运用场景：防止终端设备位置被替换

终端位置绑定即端口/MAC 绑定，用于绑定有线终端接入交换机的端口和 mac

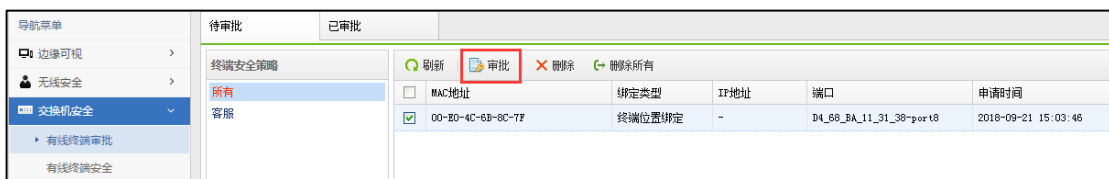
配置过程：

第一步：选择端口与交换机

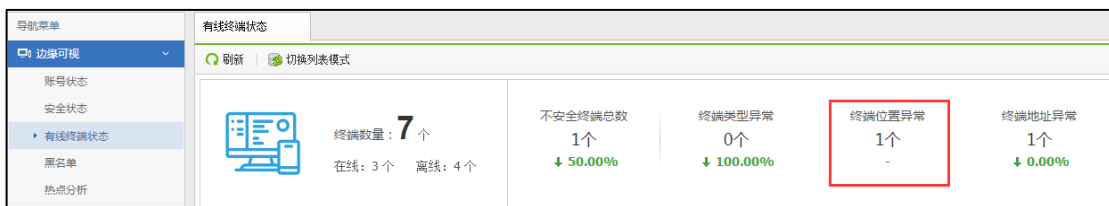
第二步：打开终端位置绑定(可以开启自动审批)



可在【交换机安全】->【有线终端审批】->【待审批】里看到需要审批的终端，勾选审批即会出现在已审批列表里



如已审批的终端换了端口接入，会在【边缘可视】->【有线终端状态】看到终端位置异常信息



2.8.4. 场景四.禁止共享网络与终端类型校验

可以在【交换机安全】->【有线终端安全】进行配置，如下配置：

在允许接入终端类型中选择摄像头和笔记本

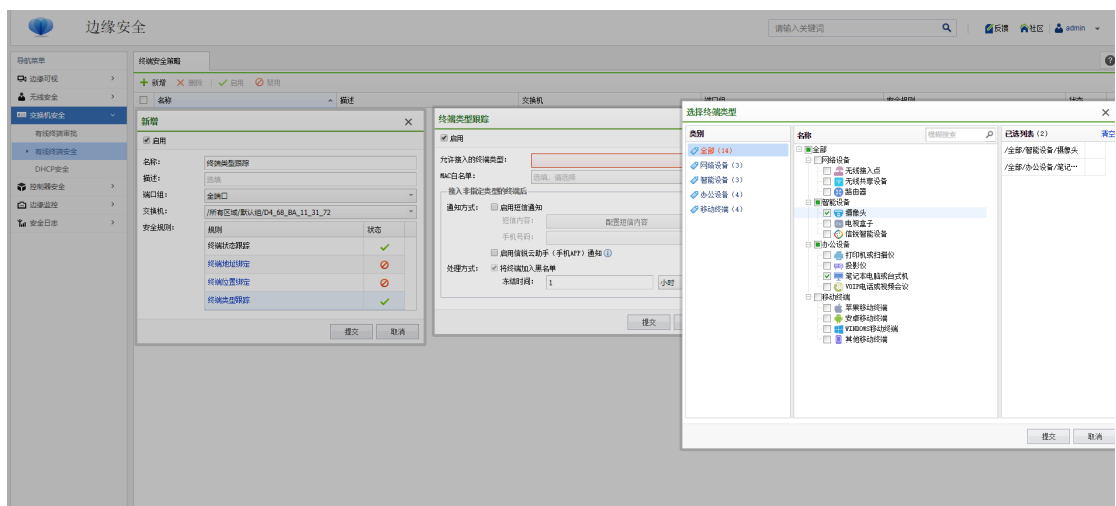
检查到有非指定类型终端接入后,将该有线终端加入黑名单 1 小时(最多冻结 24 小时,最少冻结 1 分钟)

配置步骤:

第一步:勾选端口组和交换机

第二步:打开终端类型跟踪

第三步:点击允许接入的终端类型,勾选允许通过的终端



配置终端类型绑定安全策略,其中接入的终端类型只选择了摄像头、笔记本电脑或台式机,则对于接入的路由器等其它类型的设备不会让其校验通过

✓	B5-2B-B9-E6-6B-06	笔记本电脑或台式机	1hj_b5:2b:b9:e6:6b:06
✓	CF-73-A6-8E-F8-20	摄像头	1hj_cf:73:a6:8e:f8:20
✗	65-43-35-2C-87-4A	苹果移动终端	1hj_65:43:35:2c:87:4a
✗	17-28-45-25-48-71	投影仪	1hj_17:28:45:25:48:71
✗	26-0C-C8-1C-C3-7F	WINDOWS移动终端	1hj_26:0c:c8:1c:c3:7f
✗	86-45-8C-7D-F2-10	VOIP电话或视频会议	1hj_86:45:8c:7d:f2:10
✗	终端类型校验不通过 3E-4E-1F-0F-4A-33	路由器	1hj_3e:4e:1f:0f:4a:33
✗	2B-79-4D-5F-A8-0F	安卓移动终端	1hj_2b:79:4d:5f:a8:0f
✗	95-4A-E4-DB-2E-39	投影仪	1hj_95:4a:e4:db:2e:39
✗	9D-63-86-97-1F-50	苹果移动终端	1hj_9d:63:86:97:1f:50

2.9. DHCP 功能改进

2.9.1. 解决手动配置设备网络过于繁琐的问题

2.9.1.1. 场景 1: 和设备同二层的终端需要支持即插即用

用

场景描述:

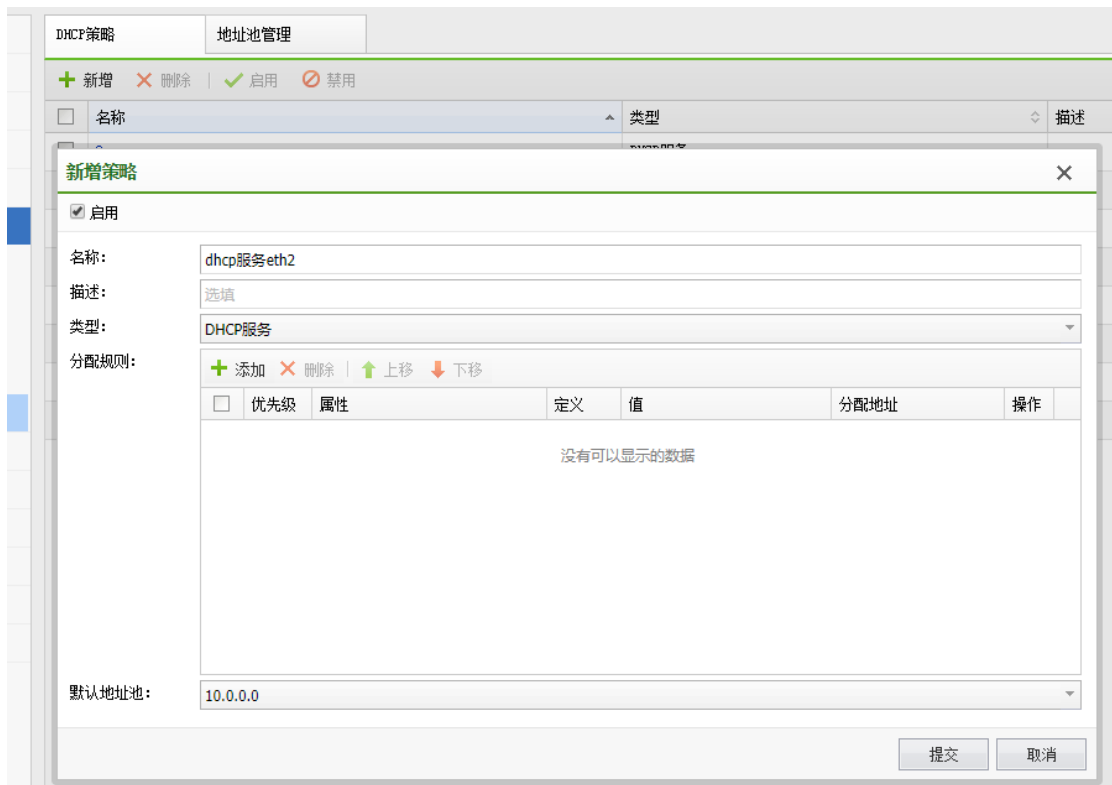


- (1) 环境准备
- (2) 策略配置

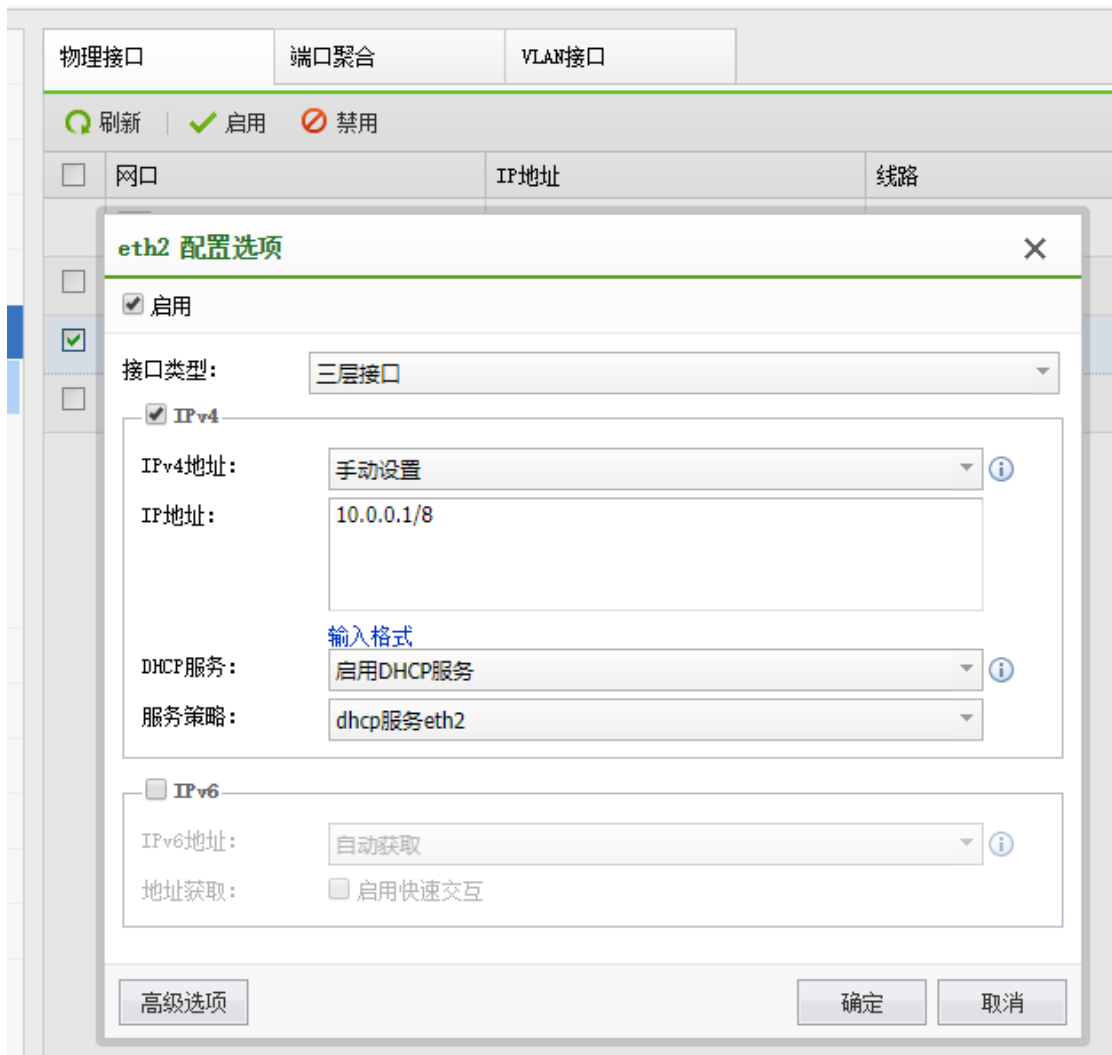
(1) 新 增 dhcp 地 址 池



(2) 新增 dhcp 策略，类型为 dhcp 服务，默认地址池选择 10.0.0.0



(3) 控制器 eth2 接口启用 dhcp 服务，dhcp 策略选择上步新增的策略

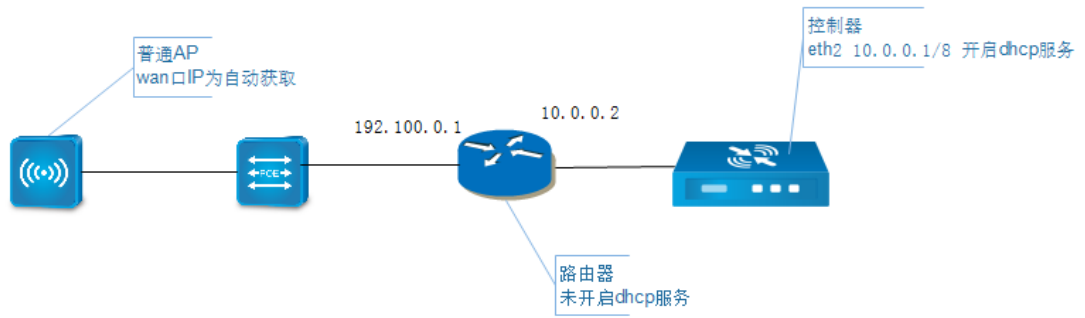


(3) 功能验证

AP 接入到 POE 交换机后可以自动获取到 IP 并上线

2.9.1.2. 场景 2: 和设备跨三层的终端需要支持即插即用

场景描述:



1.环境准备

2.策略配置

(1) 控制器新增地址池，网关 192.100.0.1

DHCP策略 地址池管理

+ 新增 × 删除 导入 导出

编辑地址池

名称: 192.100.0.0

网络参数

网关: 192.100.0.1

子网掩码: 255.255.0.0

首选DNS: 8.8.8.8

备选DNS: 选填

首选WINS: 选填

备选WINS: 选填

option43: 选填

地址池

起始IP: 192.100.0.10

结束IP: 192.100.0.100

保留IP: 设置

地址池耗尽时: 分配租约即将到期的地址 ⓘ

冲突检测: ICMP报文检测

其它

租期: 24 小时 ▾

1、接口地址和地址池同网段建议用arp检测。
2、接口地址和地址池不同网段，或者配合DHCP中继服务器使用时，建议用icmp检测。
3、选择在线用户检测时，仅查询集中转发的无线用户。交换机不支持在线用户检测。

提交 取消

1.控制器 eth2 开启 dhcp 服务，分配默认地址池 192.100.0.0

编辑策略

启用

名称: dhcp服务eth2

描述: 选项

类型: DHCP服务

分配规则:

+ 添加 × 删除 | ↑ 上移 ↓ 下移

<input type="checkbox"/>	优先级	属性	定义	值	分配地址	操作
没有可以显示的数据						

默认地址池: 192.100.0.0

提交 取消

2.添加静态路由：目的子网为 192.100.0.0 的报文发送到 10.0.0.2

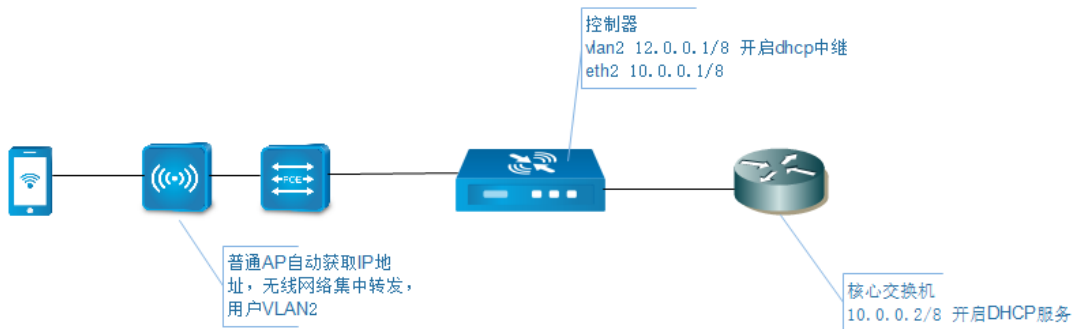
3.路由器开启 dhcp 中继，将 192.100.0.1 接口的 dhcp 报文中继到 10.0.0.1

3.功能验证

AP 接入 POE 后可以获取到控制器分配的 IP 并在控制器上线

2.9.1.3. 场景 3：利用客户已有 DHCP 服务器，节约成本

场景描述：



3.环境准备

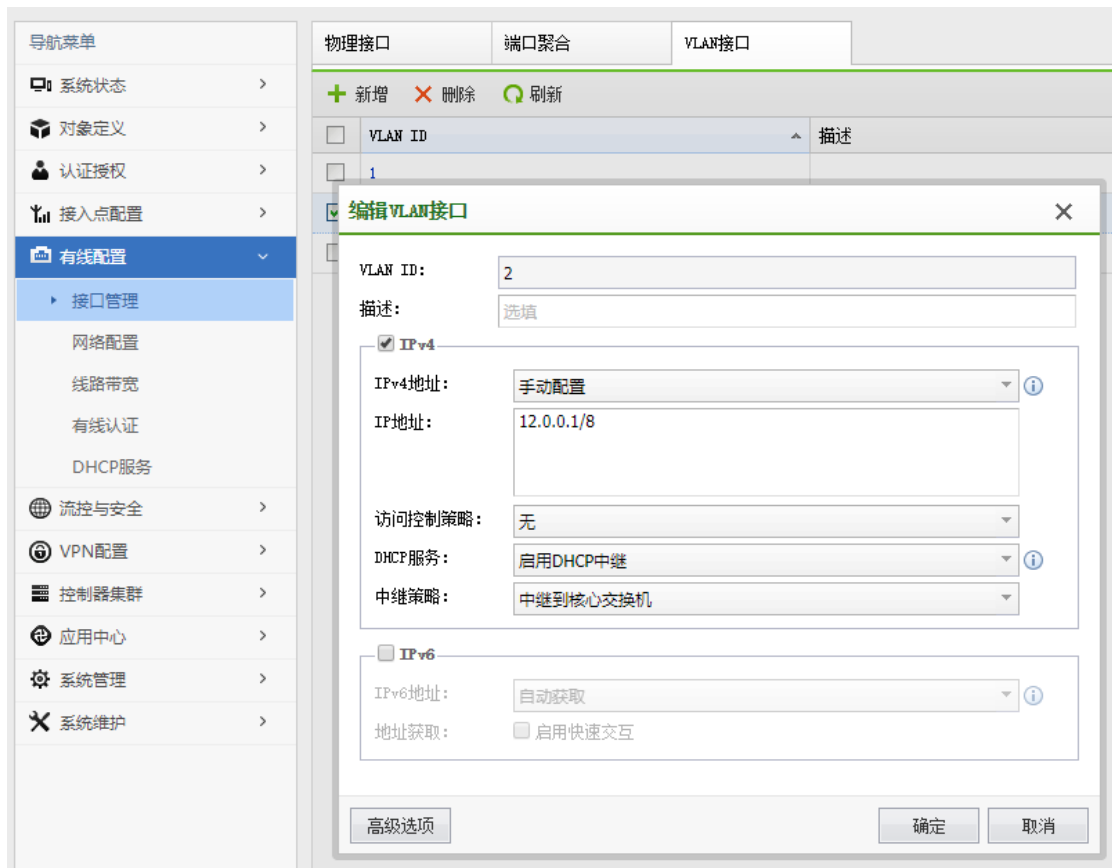
WAC、外部 DHCP 服务器

4.策略配置

(1) 新建 DHCP 中继策略，默认服务器填写核心交换机的 IP



(2) 编辑 vlan2，启用 DHCP 中继，选择上步配置的中继策略，保存



(3) 核心交换机添加静态路由：目的子网为 12.0.0.0 的报文发送到 10.0.0.1

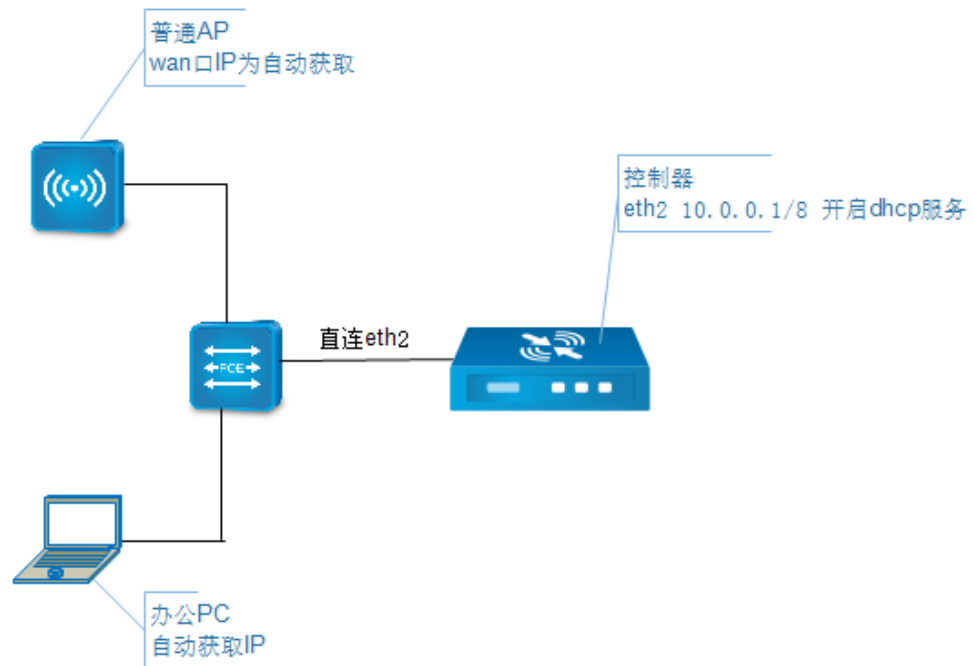
5. 功能验证

无线终端连接无线网络后可以获取到核心交换机分配的 IP 地址

2.9.2. 解决接口无法分配不同网段 IP 地址的问题

2.9.2.1. 场景 1：不同设备获取不同网段的 IP

场景描述：



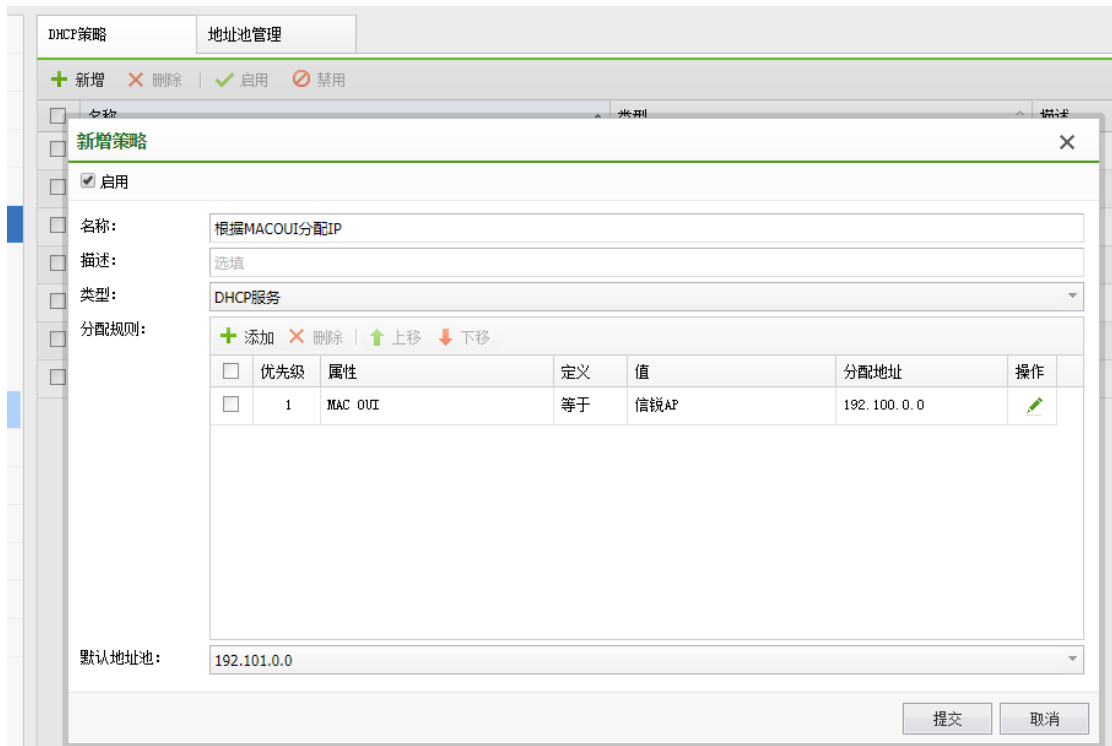
1.环境准备

2.策略配置

(1)将信锐 AP 的 macoui 添加到 mac 分组



(2) 新建 DHCP 服务策略，默认分配 192.101.0.0 网段，当 dhcp client 的 mac 地址符合信锐 AP 时则分配 192.100.0.0 网段



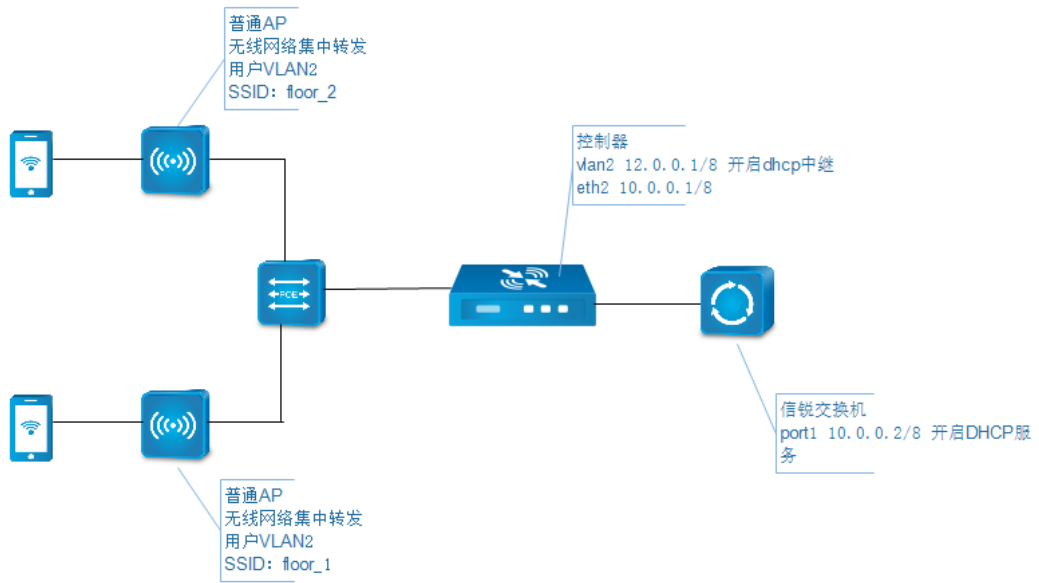
(3) 控制器 eth2 启用 dhcp 服务，策略选择上步新建的策略

2.功能验证

信锐 AP 自动获取到 192.100.0.0 网段的 IP，办公 PC 获取到 192.101.0.0 网段的 IP

2.9.2.2. 场景 2：根据 option82 自动携带的用户属性 精细化分配 IP

场景描述



3.环境准备

4.策略配置

(1) 新建 dhcp 中继策略，中继到信锐交换机 10.0.0.2，并配置子选项 0x01 为 ASCII 格式的 SSID



(2) 控制器 vlan2 启用 dhcp 中继，中继策略选择上步新建的策略

(3) 新建 dhcp 服务策略，默认地址池分配 10.61.0.0 网段，添加分配规则：如果中继代理信息 0x01 等于 ASCII 格式的 floor_1 则分配 192.100.0.0 网段，等于 floor_2 则分配 192.101.0.0 网段



(4) 信锐交换机端口 port1 启用 dhcp 服务，策略选择上步新建的策略

(5) 信锐交换机添加静态路由：目的子网为 12.0.0.0 的报文发送到 10.0.0.1

5. 功能验证

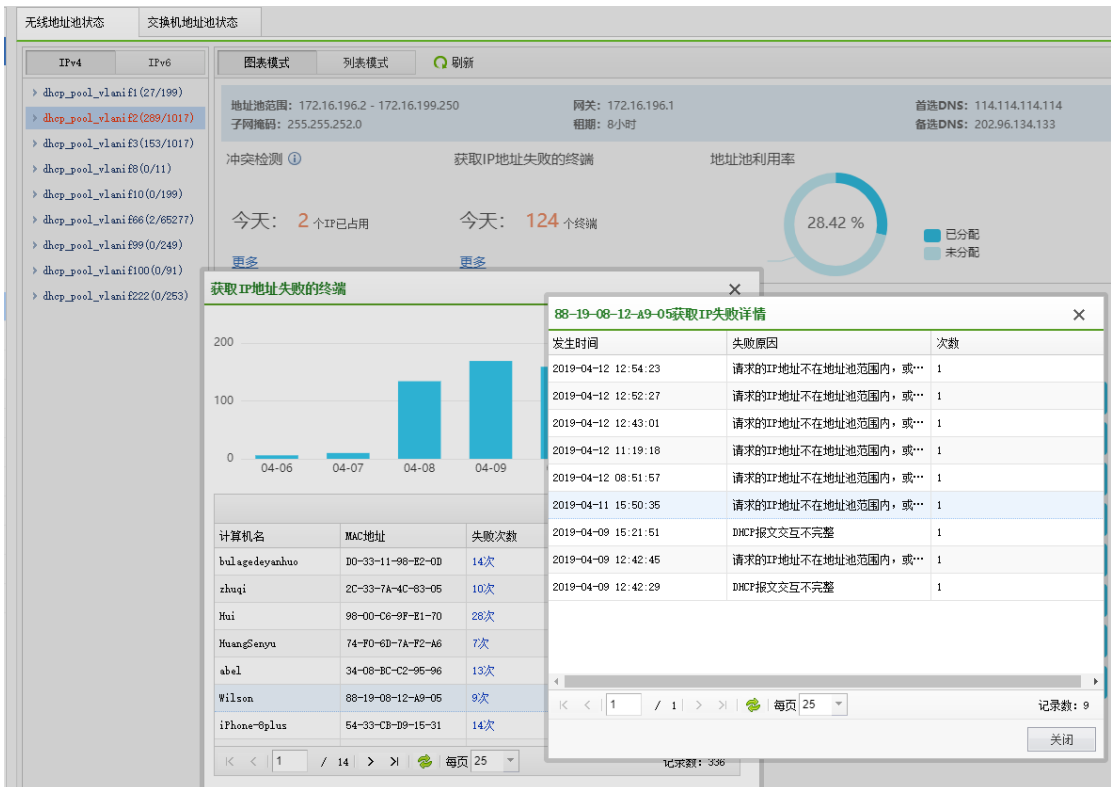
无线终端连接无线网络 floor_1 获取到 192.100.0.0 网段的 IP，连接 floor_2 则获取到 192.101.0.0 网段的 IP

2.9.3. 解决管理员网络运维复杂的问题

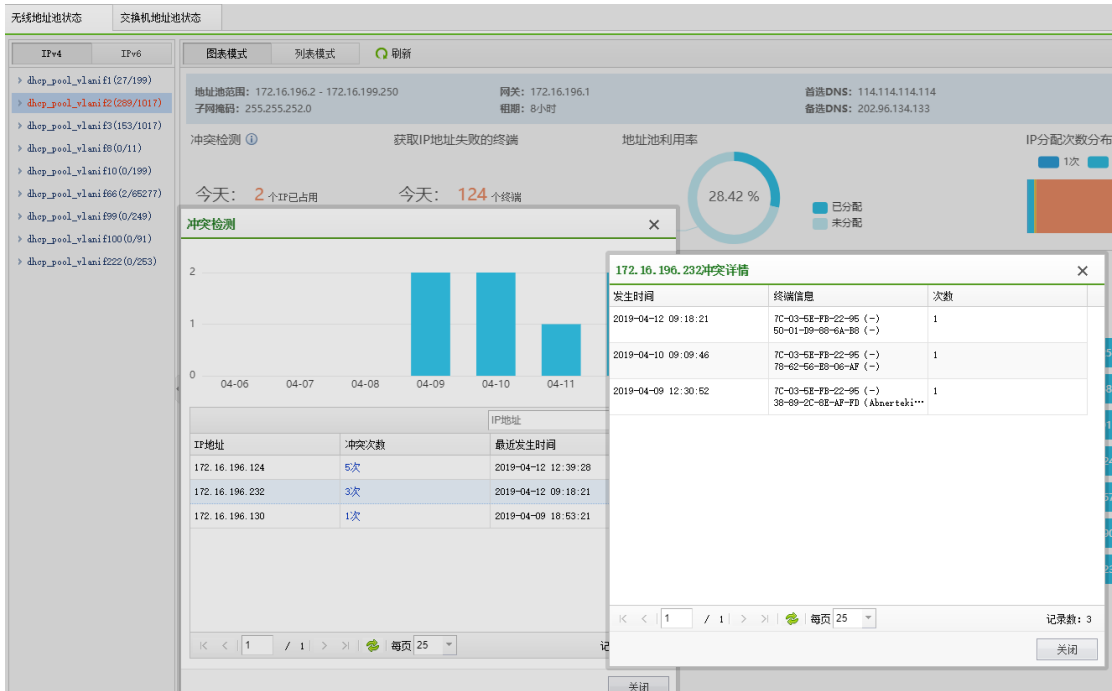
2.9.3.1. 场景 1：管理员定期检视网络状态



2.9.3.2. 场景 2：管理员定位网络问题



2.9.4. 解决用户接入无法上网的问题



2.9.4.1. 场景 1：地址池无可分配 IP 地址时清除租约



2.9.4.2. 场景 2：避免终端发生 IP 冲突

DHCP策略 地址池管理

+ 新增 X 删除 导入 导出

名称
10.61.0.0
<input checked="" type="checkbox"/> 192.100.0.0
192.101.0.0
192.102.0.1
192.168.188.1

编辑地址池

名称: 192.100.0.0

网络参数

网关: 192.100.0.1

子网掩码: 255.255.0.0

首选DNS: 8.8.8.8

备选DNS: 选填

首选WINS: 选填

备选WINS: 选填

option43: 选填

地址池

起始IP: 192.100.0.10

结束IP: 192.100.0.100

保留IP: 设置

地址池耗尽时: 分配租约即将到期的地址

冲突检测: ICMP报文检测

其它

租期: ICMP报文检测

在线用户检测

提交 取消

1、接口地址和地址池同网段建议用arp检测。

2、接口地址和地址池不同网段，或者配合DHCP中继服务器使用时，建议用icmp检测。

3、选择在线用户检测时，仅查询集中转发的无线用户。交换机不支持在线用户检测。

第3章 设备支持 IPv6

3.1. 无线设备支持 IPv6

3.1.1. 用户网络升级 IPv6，无线网络支持 IPv6 部署

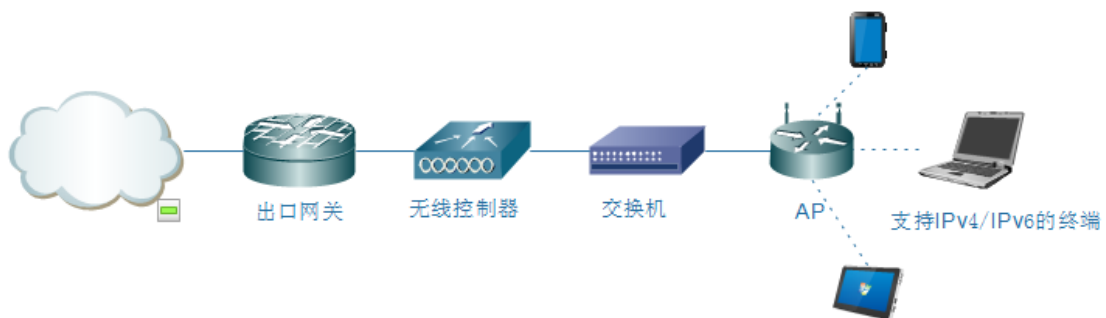
3.1.1.1. 场景 1 无线设备二层部署，AP 使用 IPv6 地址上线终端集中转发无线用户获取 IPv6 地址

1. 场景描述

用户网络支持 IPv6，确保控制器与 AP 可以通过 IPv6 地址进行管理；控制器上联出口接入支持 IPv6 的网关，集中转发的无线用户可以使用 IPv6 地址与外网进行通信。

使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到控制器与交换机。

2. 网络拓扑

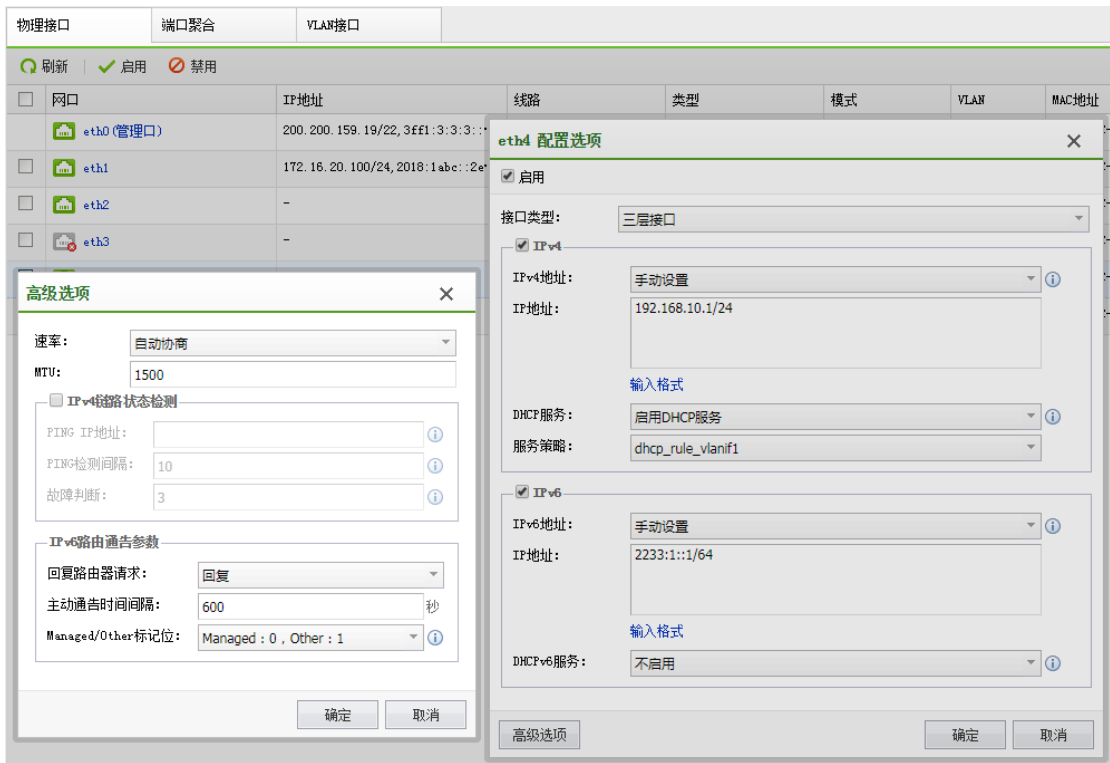


3. 配置步骤

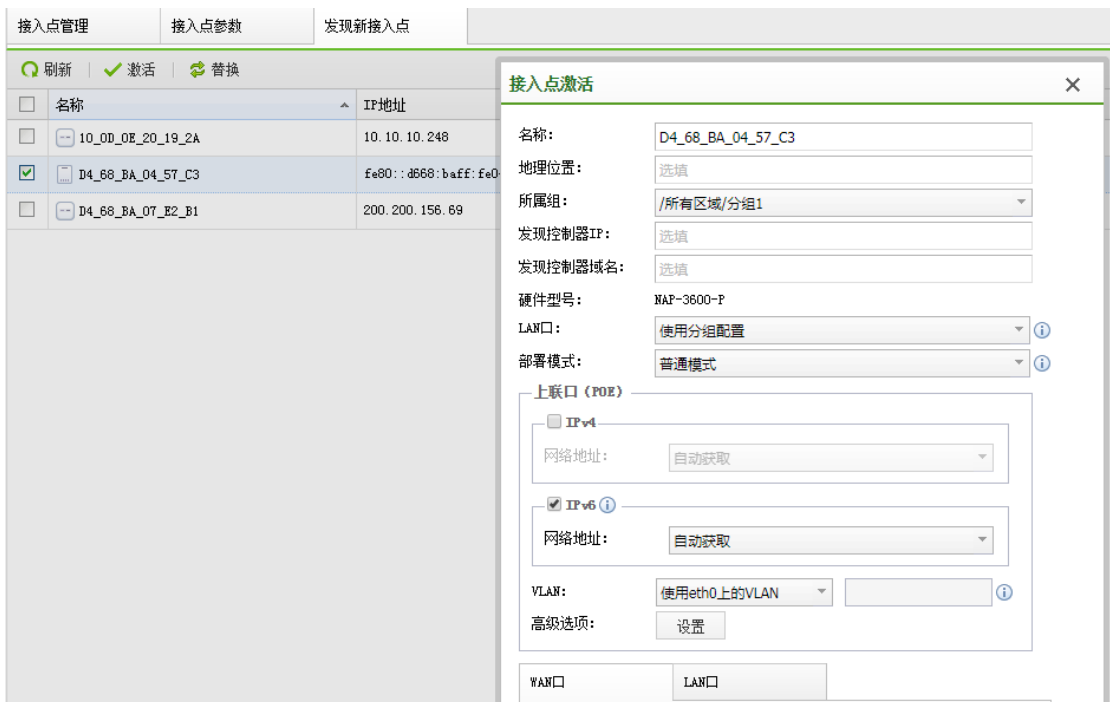
(1). 控制器配置 eth1 为上联出接口，无状态自动配置获取 IPv6 地址，自动获取 IPv6 默认网关。



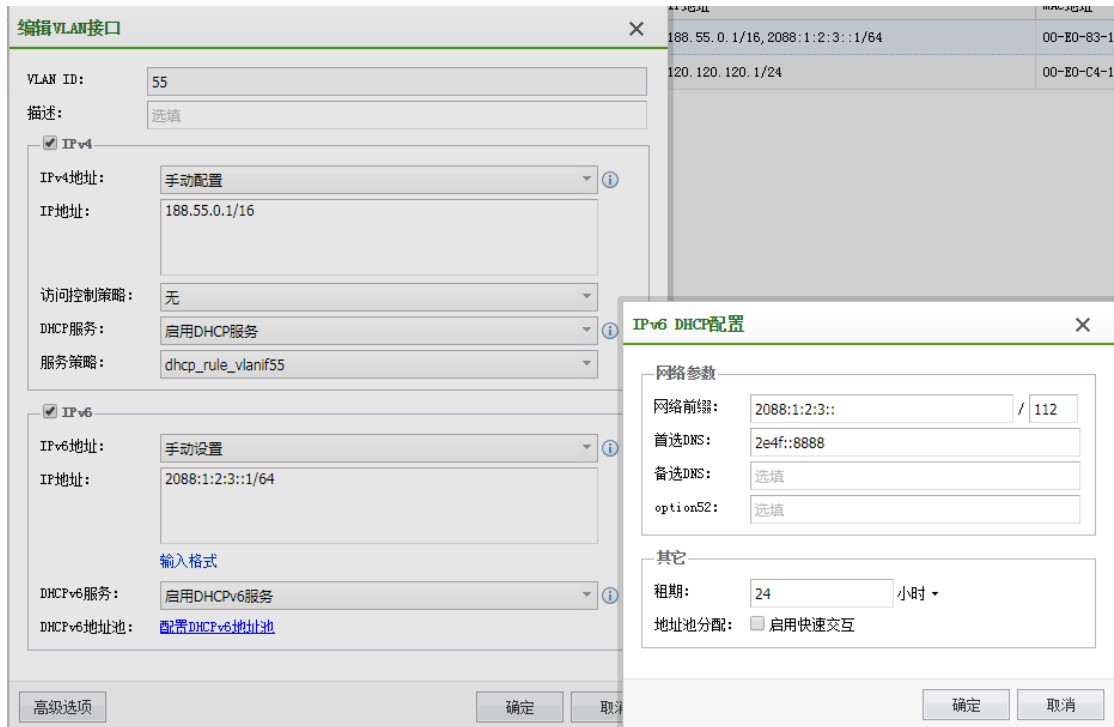
(2). 控制器接口与 AP 接入同二层网络，接口启用静态 IPv6，下发路由通告分配 IPv6 地址前缀，高级设置中路由请求设置为回复，M/O 标记位配置为 0/1。



(3) 发现激活 AP，配置 AP 上联口为单栈的 IPv6 地址，自动获取。



(4).控制器创建 vlan 55 接口，配置 IPv6 静态地址，启用 DHCPv6 服务并配置地址池，接口高级设置中路由通告配置为回复，M/O 标记位为 1/1。



(5).控制器创建 PSK 认证的集中转发无线网络分配该 vlan 中地址，使用支持 IPv4 与 IPv6 的客户端连接无线网络。

4. 效果验证

(1).控制器上联出口可以生成 IPv6 地址,接口管理页面可以看到接口生成的 IPv6 地址,控制器路由表中生成出接口为 eth1 的默认路由。

物理接口	端口聚合	VLAN接口	
刷新 启用 禁用			
<input type="checkbox"/>	网口	IP地址	
<input checked="" type="checkbox"/>	eth0 (管理口)	200.200.159.19/22, 3ff1:3:3:3::199/64	
<input type="checkbox"/>	eth1	172.16.20.100/24, 2018:1abc::2e0:4cff:fe12:9572/64	

(2).配置生效,接口管理页面可以到配置的接口 IPv6 地址。

<input type="checkbox"/>	eth4	192.168.10.1/24, 2233:1::1/64
--------------------------	------	-------------------------------

(3).AP 激活上线到控制器成功,无线状态页面可以看到 AP 使用 IPv6 地址上线。

状态	名称	控制器名称	无线网络	所属组	硬件型号	IP地址
<input checked="" type="checkbox"/>	D4_68_BA_04_57_C3	WAC_A693F9FE (fe80::2e0:4cff:fe12:956f)	3	分组1	NAP-3600-F	fe80::8568:baff:fe04:57c3
<input checked="" type="checkbox"/>	D4_66_BA_03_AF_36	WAC_A693F9FE (192.168.10.1)	6	分组2	NAP-3600-F	192.168.10.2

(4).配置生效,vlan 接口显示配置的静态 IPv6 地址。

物理接口	端口聚合	VLAN接口	
+ 新增 × 删除 刷新			
<input type="checkbox"/>	VLAN ID	描述	IP地址
<input type="checkbox"/>	55	-	188.55.0.1/16, 2088:1:2:3::1/64

(5).无线终端获取到 IPv6 地址,可以使用 IPv6 地址与出口网关及外网通信。

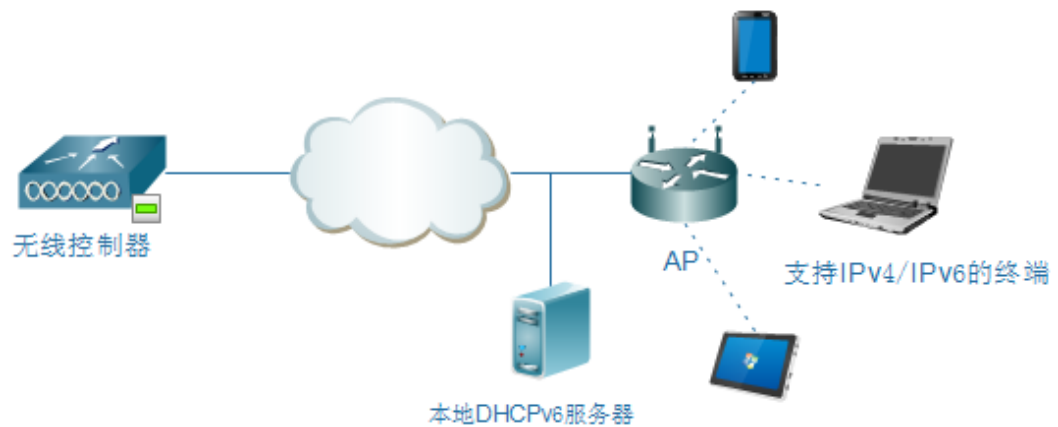
3.1.1.2. 场景 2 无线设备跨三层部署，AP 使用 IPv6 地址 上线到控制器

1.场景描述

无线控制器与 AP 跨公网环境部署,网络在原 IPv4 部署基础上增加支持 IPv6 数据转发。控制器有 AP 的通信链路需要切换到 IPv6 网络,可以通过 IPv6 地址上线到控制器。支持 IPv6 的终端可以通过本地转发获取到 IPv6 地址。

使用 IPv6 地址与网关及外网通信,需要保证配置的 IPv6 地址在外部存在路由回到控制器与交换机。

2.网络拓扑



3.配置步骤

(1).AP 已使用 IPv4 地址跨公网上线到控制器，无线控制器上联出口启用配置静态 IPv6 地址接入公网环境，可以在公网中使用 IPv6 地址通信。

(2).接入点管理中启用 IPv6 地址；根据网络环境配置为自动获取 IPv6 地址或静态 IPv6 地址。发现控制器 IP 指定为控制器出口的 IPv6 地址。

编辑

名称: D4_66_BA_03_AF_36

地理位置: 选填

所属组: 所有区域/分组2

发现控制器IP: 2015::1

发现控制器域名: 选填

硬件型号: NAP-3600-P

LAN口: 使用分组配置

网络配置: 使用接入点上报的配置

部署模式: 普通模式

上联口 (POE)

IPv4

网络地址: 自动获取

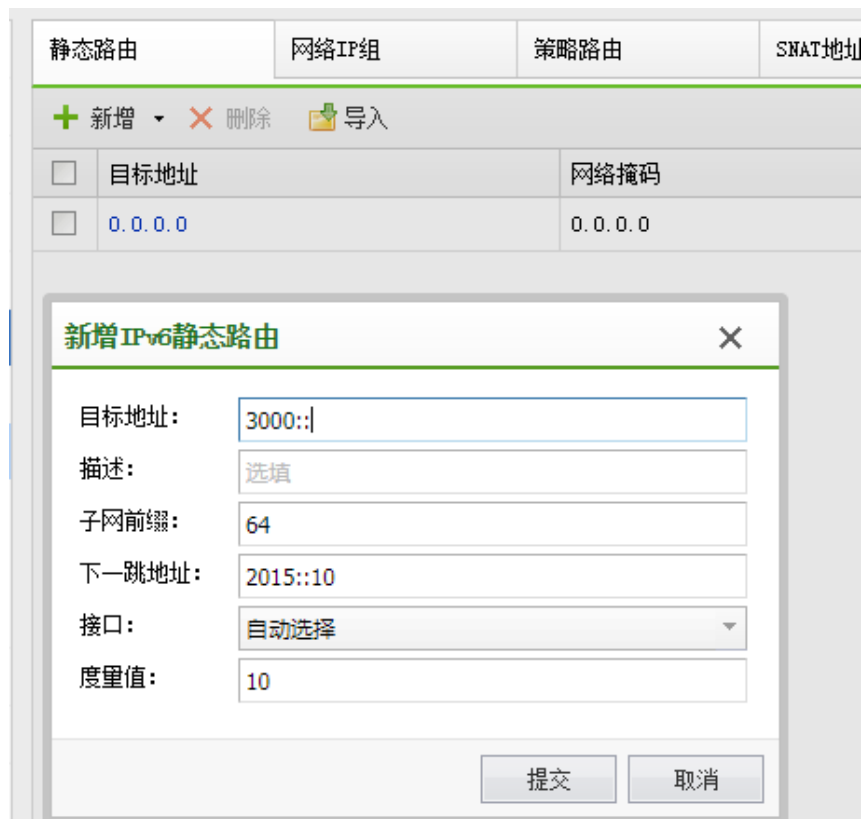
IPv6

网络地址: 自动获取

VLAN: 使用eth0上的VLAN

高级选项: 设置

(3).控制器添加指向 AP IPv6 地址的静态路由。这里已 AP IPv6 地址为 3000::/64 前缀，控制器出接口下一跳地址为 2015::10 为例



(4).创建 PSK 认证的本地转发无线网络，支持 IPv6 的终端接入无线网络。

4.效果验证

AP 使用 IPv6 地址重新上线到控制器，无线状态页面可以看到 AP 使用 IPv6 地址上线成功。无线客户端连接无线网络获取 IPv6 地址成功，可以使用 IPv6 进行通信。

3.1.1.3. 场景 3 控制器作为中继，终端用户通过控制器获取上级 DHCPv6 服务器分配的地址

1. 场景描述

IPv6 网络中个设备的 IPv6 地址由独立的 DHCPv6 服务器统一分配，控制器作为 DHCPv6

中继向客户端转发上级服务器分配的 IPv6 地址。

使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到控制器。

2. 网络拓扑

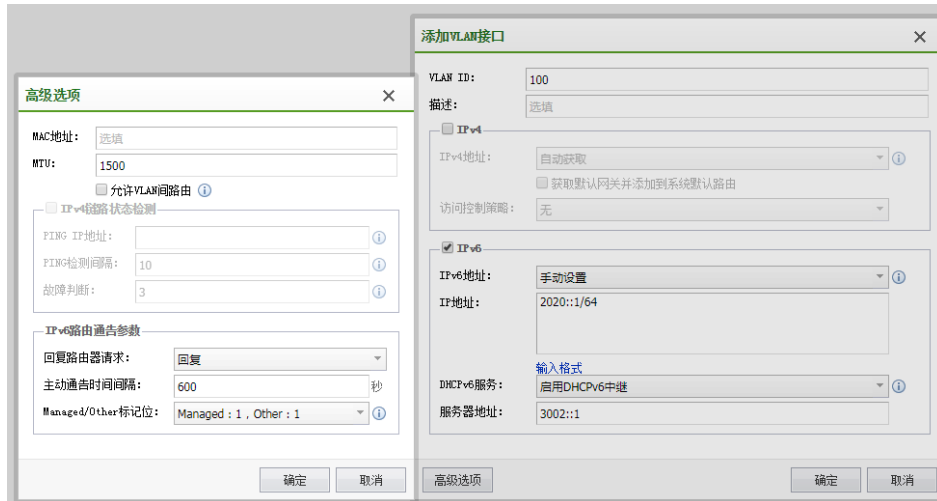


3. 配置步骤

(1). 控制器上联出口启用 IPv6 地址，配置静态 IPv6 地址。控制器创建 IPv6 静态路由或默认路由，可以与 DHCPv6 服务器地址 3002::1 通信。



(2). 无线控制器创建 vlan 接口，启用 IPv6 静态地址，启用 DHCPv6 中继，中继服务器地址填写 DHCPv6 服务器地址；接口高级选项中配置路由通告为回复，M/O 标记位为 1/1。控制器 eth2 接口配置为二层接口 Access vlan 100。



(3). AP 上线到控制器，配置 PSK 认证的集中转发的无线网络，引用 VLAN 100。

(4). 支持 IPv6 的有线终端接入 eth2 接口自动获取地址，无线终端连接无线网络自动获取地址。

4. 效果验证

控制器接口启用 DHCPv6 中继成功，有线终端与无线终端获取上线 DHCPv6 服务器分配的 IPv6 成功，可以使用 IPv6 访问外网。

3.1.2. 用户部署控制器为网关接入运营商 IPv6 网络

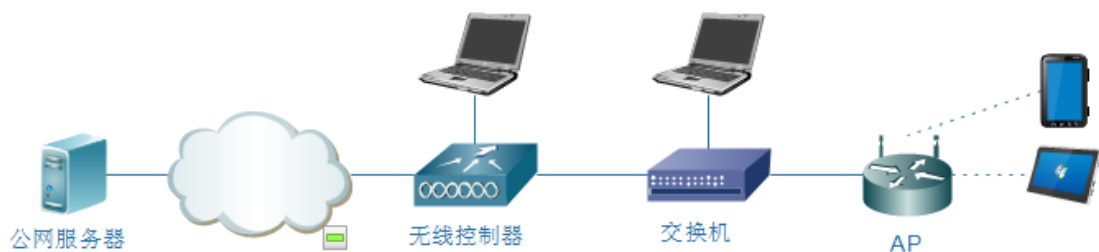
3.1.2.1. 场景 1 控制器上行出口自动获取 IPv6 地址，下接交换机、接入点及终端用户使用 IPv6 地址通信

1. 场景描述

运营商网络支持 IPv6 部署，控制器作为出口网关获取 IPv6 地址。控制器下连管理的交换机与接入点支持使用 IPv6 地址进行通信，接入的终端用户可以使用 IPv6 地址访问外网。

使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到控制器与交换机。

2. 网络拓扑



3. 配置步骤

(1). 控制器作为出口网关，配置上联出口启用 IPv6 地址自动获取。创建一条 IPv6 默认路由，下一跳地址指定为上联出口下一跳设备的本地链路地址。

eth1 配置选项 ✕

启用

接口类型: 三层接口

IPv4

IPv4地址: 自动获取 ⓘ

获取默认网关并添加到系统默认路由

IPv6

IPv6地址: 自动获取 ⓘ

地址获取: 启用快速交互

高级选项
确定
取消

静态路由	网络IP组	策略路由	SNAT地址
+ 新增 ✕ 删除 📁 导入			
<input type="checkbox"/>	目标地址	网络掩码	
<input type="checkbox"/>	0.0.0.0	0.0.0.0	

新增 IPv6 静态路由 ✕

目标地址:

描述:

子网前缀:

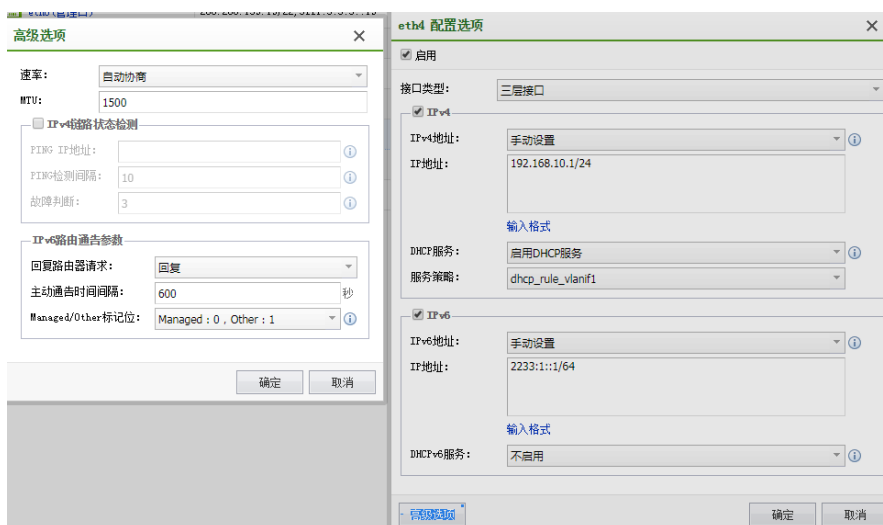
下一跳地址:

接口: eth1

度量值:

提交
取消

(2). 控制器内网 eth4 接口配置 IPv6 静态地址，接口高级选项启用路由通告为回复，M/O 标记位为 0/1。



(3). 交换机管理 vlan 1 接口启用 IPv6 地址，配置静态 IPv6 地址与控制器接口 IPv6 地址同前缀。接入点管理配置 AP 上联口启用 IPv6 地址自动获取。



编辑

名称: D4_66_BA_03_AF_36

地理位置: 选填

所属组: 所有区域/分组2

发现控制器IP: 选填

发现控制器域名: 选填

硬件型号: NAF-3600-P

LAN口: 使用分组配置

网络配置: 使用接入点上报的配置

部署模式: 普通模式

上联口 (POE)

IPv4

网络地址: 自动获取

IPv6

网络地址: 自动获取

VLAN: 使用eth0上的VLAN

高级选项: 设置

(4). 控制器创建 vlan 55 接口配置 IPv6 静态地址，启用 DHCPv6 服务配置地址池。控制器内网接口 eth3 配置为二层口 Access vlan 55，创建 PSK 认证的集中转发无线网络，引用 vlan 55。

eth3 配置选项

启用

接口类型: 二层接口

接口模式: Access

VLAN: 55

高级选项

确定 取消

(5). 支持 IPv6 的有线终端接入控制器 eth3 接口自动获取地址，有线终端接入交换机自动获取的，无线终端接入无线网络自动获取地址。

4. 效果验证

- (2). 控制器可以使用 IPv6 地址与公网服务器通信。
- (3). 交换机与接入点配置 IPv6 地址成功，可以使用 IPv6 地址与控制器通信。
- (5). 有线终端和无线终端获取生成 IPv6 地址成功，可以与公网服务器通信。

3.2. 交换机支持 IPv6

3.2.1. 用户 IPv6 网络部署三层交换机

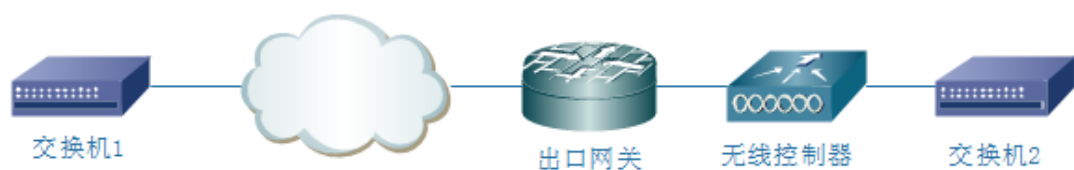
3.2.1.1. 场景 1 用户在 IPv6 网络中使用控制器统一管理交换机设备

1. 场景描述

交换机与控制器同二层或跨三层部署，已部署的交换机需要支持控制器使用 IPv6 地址管理。

使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到控制器与交换机。

2. 网络拓扑

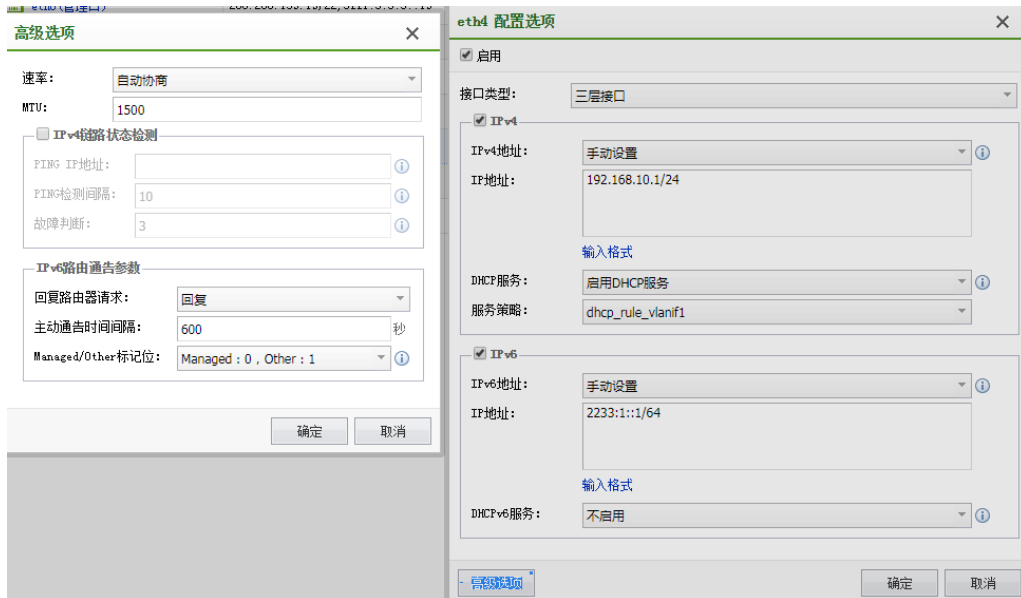


3.配置步骤

(1).交换机 1 与交换机 2 已使用 IPv4 地址上线到控制器，无线控制器上联出口启用配置静态 IPv6 地址接入公网环境，这里接口地址以 2015::1 为例。可以在公网中使用 IPv6 地址通信。控制器添加 IPv6 默认路由。

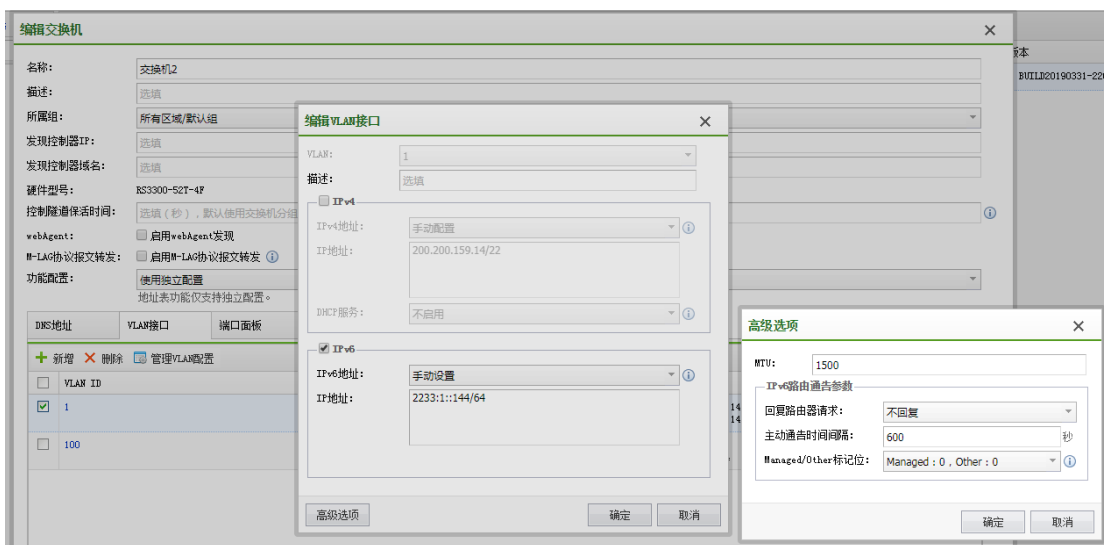


(2).控制器内网 eth4 接口配置 IPv6 静态地址，接口高级选项启用路由通告为回复，M/O 标记位为 0/1。

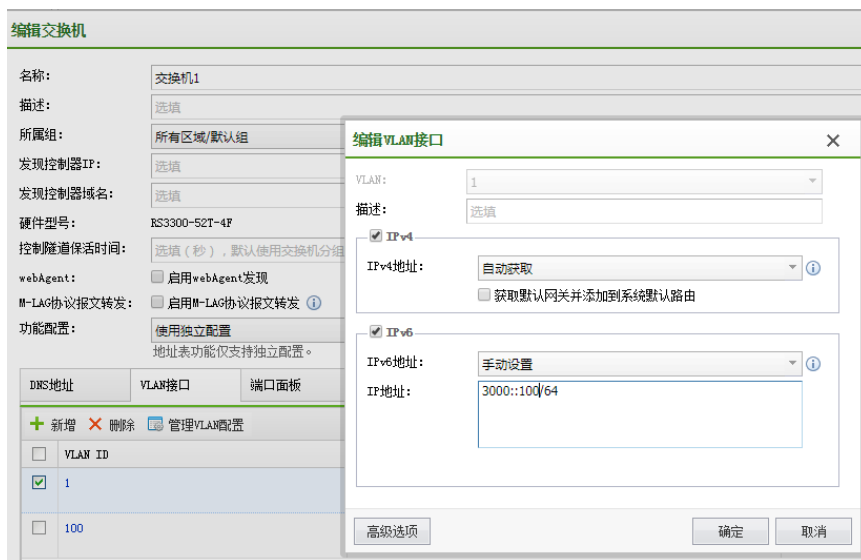


(3).交换机管理中配置交换机 2 管理 vlan 1 接口启用 IPv6 地址，配置静态 IPv6 地址与控制器 eth4 接口 IPv6 地址同前缀，禁用接口 IPv4 地址，高级选项中路由通告选择不回

复。



(4).交换机管理中配置交换机 1 管理 vlan1 接口启用 IPv6 地址，配置静态 IPv6 地址与公网部署环境同前缀，这里交换机地址以 3000::10 为例。发现控制器 IP 添加控制器 IPv6 地址。



编辑交换机

名称:	交换机1
描述:	选填
所属组:	所有区域/默认组
发现控制器IP:	2015::1
发现控制器域名:	选填

(5) 交换机路由管理添加交换机的 IPv6 默认路由

The screenshot shows the '静态路由' (Static Routing) configuration page for '交换机001'. The '路由列表' (Route List) table is as follows:

目标地址	网络掩码	子网前缀	下一跳地址	接口
0.0.0.0	0.0.0.0	-	200.200.159.254	-

The '新增IPv6静态路由' (Add New IPv6 Static Route) dialog box contains the following fields:

- 目标地址: ::1
- 描述: 选填
- 子网前缀: 0
- 下一跳地址: 3000::1
- 接口: 自动选择

4. 效果验证

禁用交换机 1 与交换机 2 的管理 vlan IPv4 地址，交换机可以使用 IPv6 地址重新上线到控制器。控制器-交换机状态页面可以看到交换机上线使用的 IPv6 地址。

状态	名称	MAC地址	IP地址	控制器	硬件型号
●	交换机1	E0-D5-5E-77-77-77	3fe1:3:3:3::144	MAC_A693F9FE (3:3:3:3:3:3)	RS3300-S2T-4F

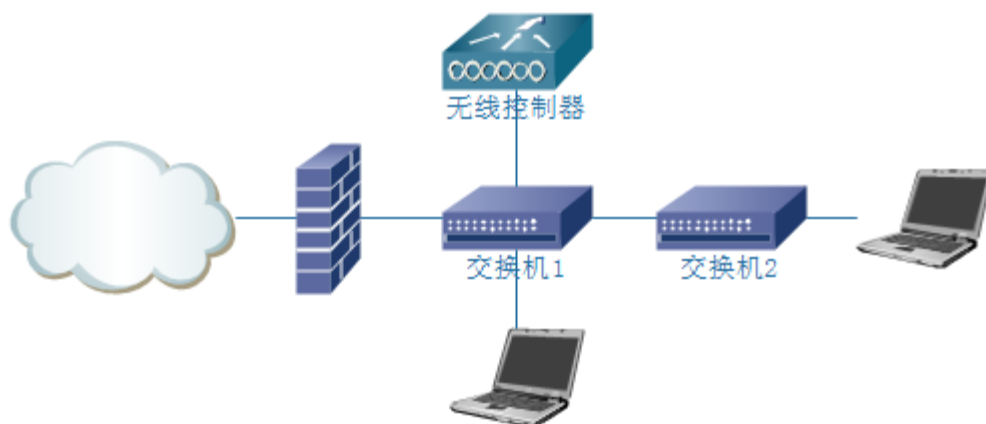
3.2.1.2. 场景 2 部署交换机作为网关设备, 转发 IPv6 数据

1. 场景描述

网络部署支持 IPv4 与 IPv6 双栈，交换机作为出口设备在原有 IPv4 基础增加对 IPv6 地址的支持。交换机给下连有线设备下发 IPv6 地址前缀与默认路由配置；转发网络中的 IPv6 数据。

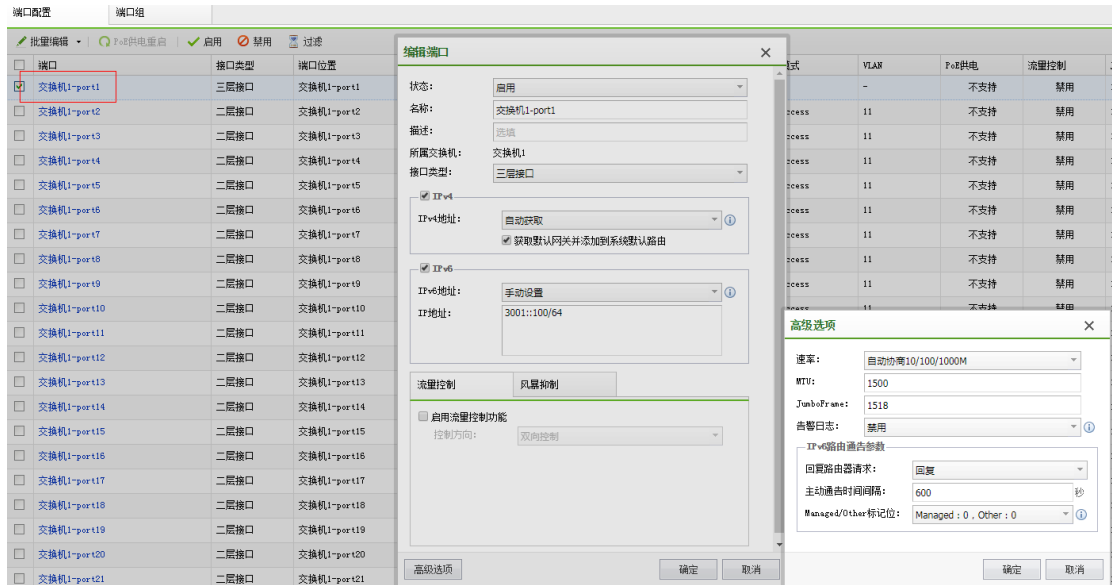
使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到交换机

2. 网络拓扑



3.配置步骤

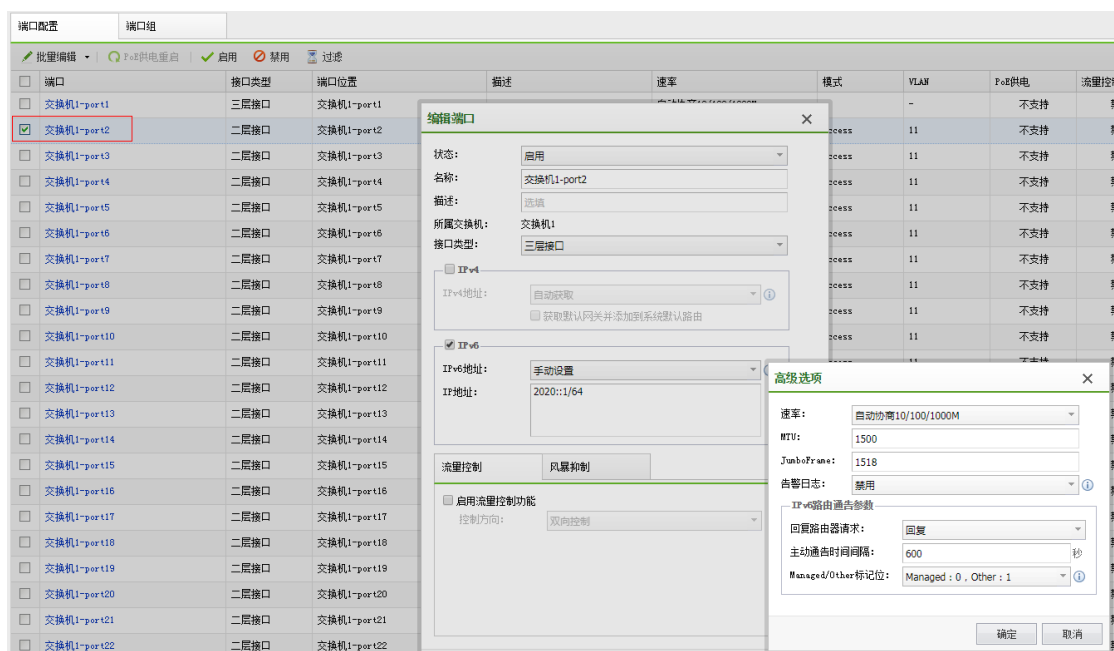
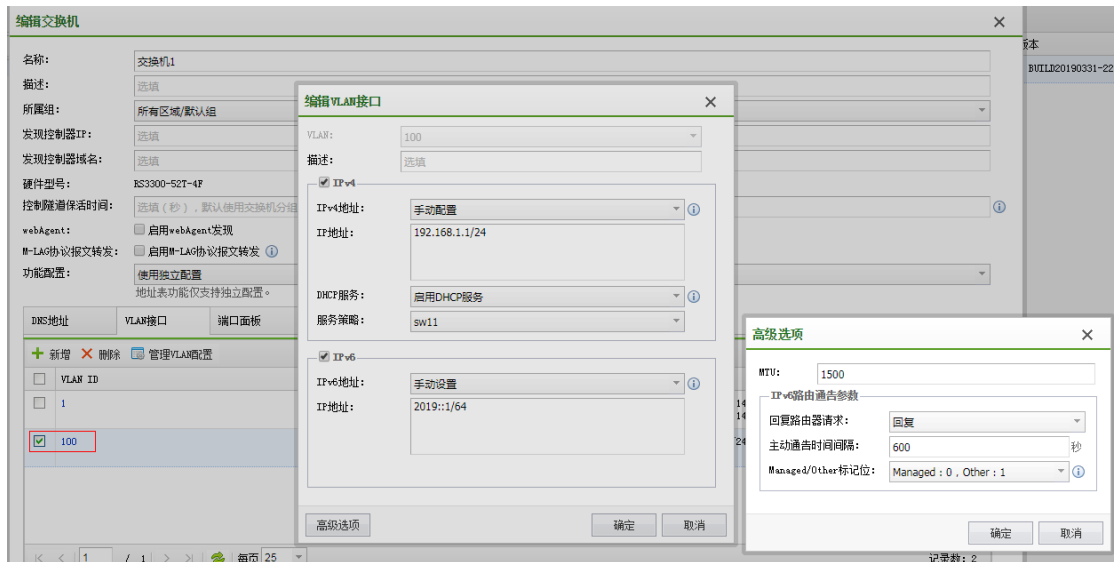
(1).无线控制器管理交换机,交换机 1 启用一个三层物理口作为网络出口,接入公网 IPv6 网络环境中。交换机 1 三层接口配置 IPv6 静态地址,端口高级选项中配置路由通告为不回复,这里以 1 号端口为例。



(2).交换机 1 静态路由中添加一条 IPv6 的默认路由,出接口为端口 1。



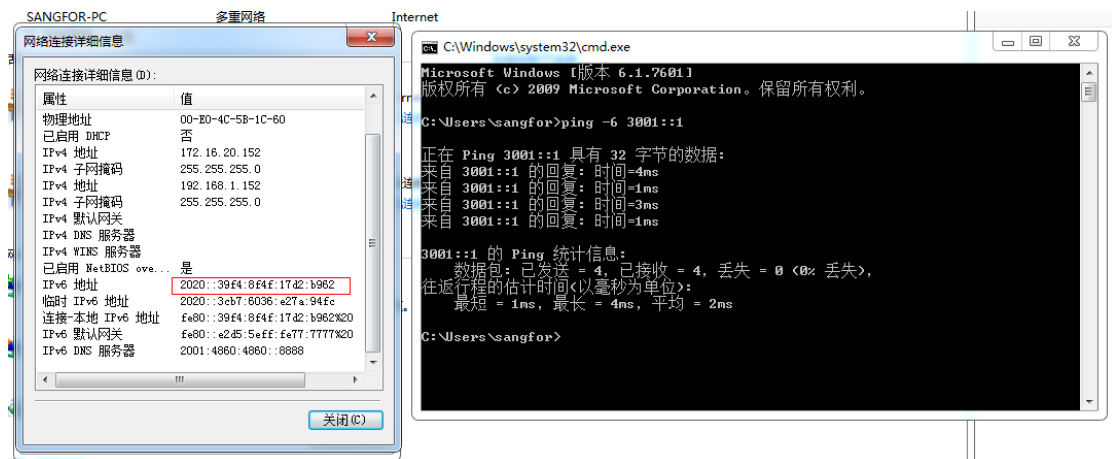
(3).交换机划分 vlan 100 接入有线客户端，vlan100 端口启用静态 IPv6 地址，高级选项路由通告配置为回复，M/O 标记位配置为 0/1。启用端口 2 为三层口下接二层交换机 2，接口启用静态 IPv6 地址，高级选项路由通告配置为回复，M/O 标记位配置为 0/1。



(4).支持 IPv6 的有线设备接入交换机，自动获取 IPv6 地址，指定静态的 IPv6 DNS 服务器。

4. 效果验证

交换机接口 IPv6 地址配置生效，有线终端接入交换机端口，可以使用交换机接口前缀生成 IPv6 地址，可以使用 IPv6 地址访问外网 IPv6 服务。这里以 PC 接入，ping 交换机上联出口网关为例。



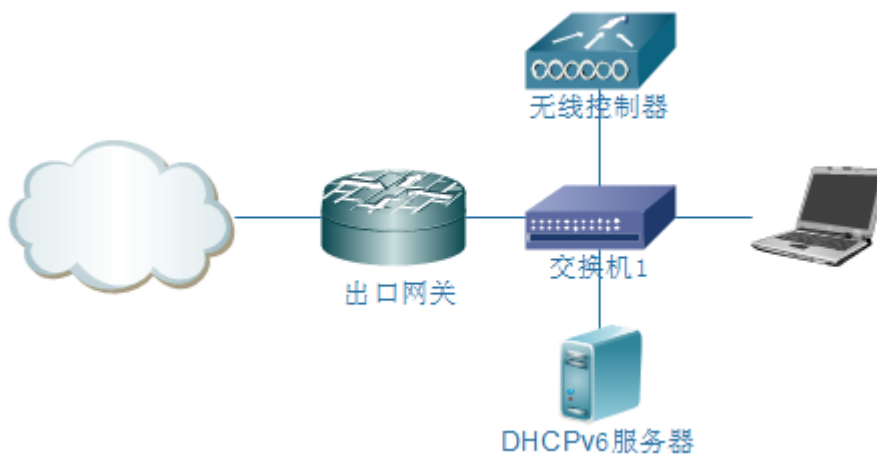
3.2.1.3. 场景 3 客户端接入交换机从外置的 DHCPv6 服务器获取网络配置

1. 场景描述

用户网络出口网关支持 IPv6 数据转发，下接交换机使用无线控制器管理，部署外置 DHCPv6 服务器接入交换机，有线用户接入交换机自动获取 IPv6 地址，交换机转发用户 IPv6 数据到出口网关。

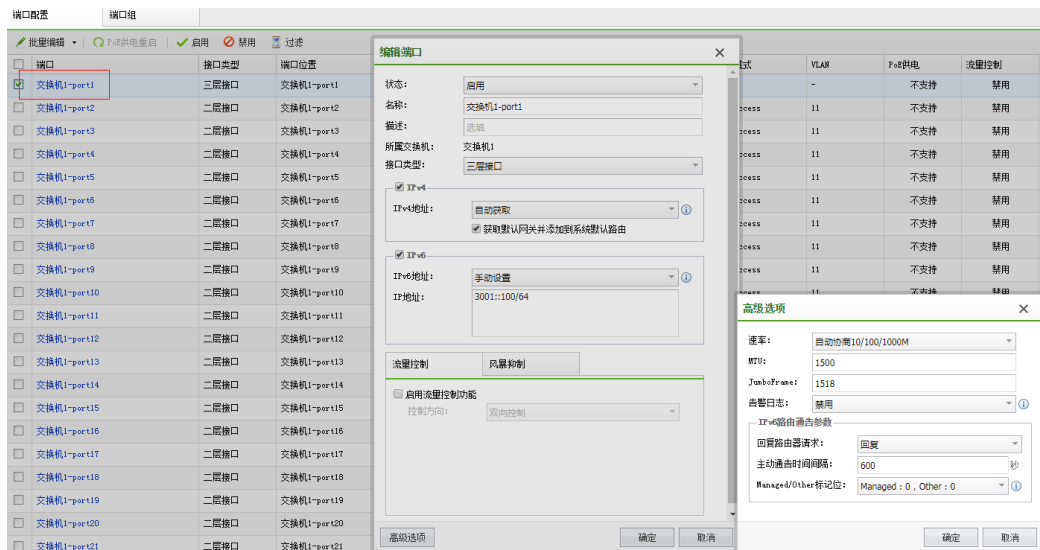
使用 IPv6 地址与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到交换机。

2.网络拓扑

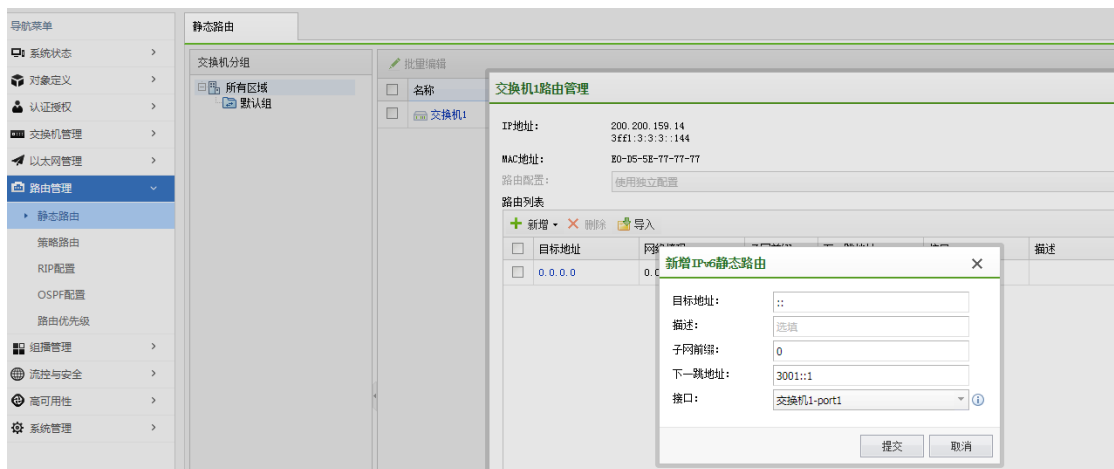


3.配置步骤

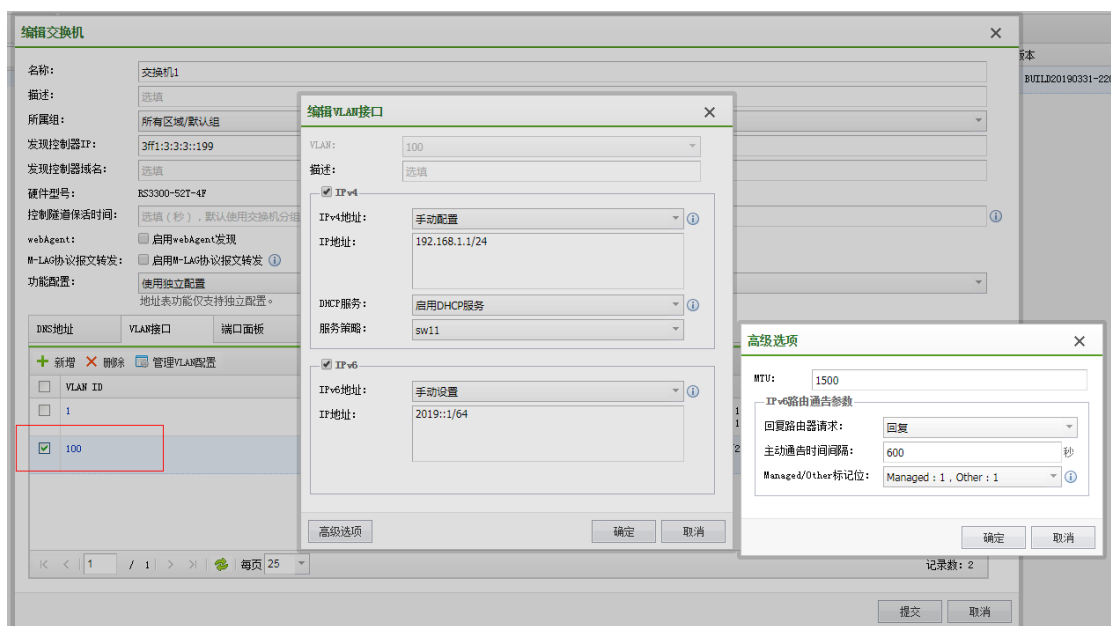
(1)交换机 1 启用一个三层物理口作为上联出口，接入出口网关。交换机 1 三层接口配置 IPv6 静态地址，端口高级选项中配置路由通告为不回复，配置接口地址与出口网关子网 IPv6 地址同前缀，这里以 1 号端口，网关子网 IPv6 地址为 3001::1/64 为例。



(2). 交换机 1 静态路由中添加一条 IPv6 的默认路由，出接口为端口 1。



(3).交换机划分 vlan 100 接入有线客户端，vlan100 端口启用静态 IPv6 地址，高级选项路由通告配置为回复，M/0 标记位配置为 1/1。



4.效果验证

交换机 vlan100 中接入外部 DHCPv6 服务器分配 IPv6 地址及 DNS 信息，有线终端接入交换机的 vlan100 接口中自动获取 IPv6 地址与 DNS 地址。可以获取成功，终端设备可以与出口网关及外网 IPv6 通信。

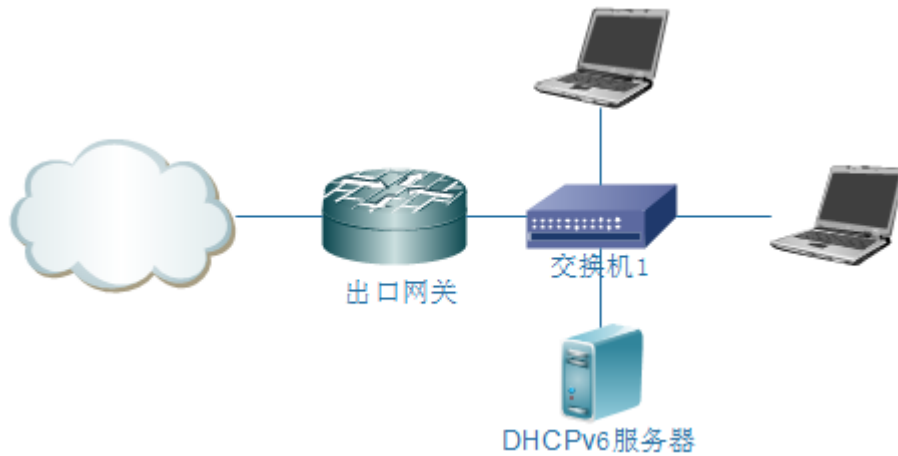
3.2.1.4. 场景 4 胖模式交换机接入 IPv6 网络转发数据

1.场景描述

用户网络出口网关支持 IPv6 数据转发，下接胖交换机管理划分子网 vlan，部署外置 DHCPv6 服务器接入交换机，有线用户接入交换机自动获取 IPv6 地址，交换机转发用户 IPv6 数据到出口网关。

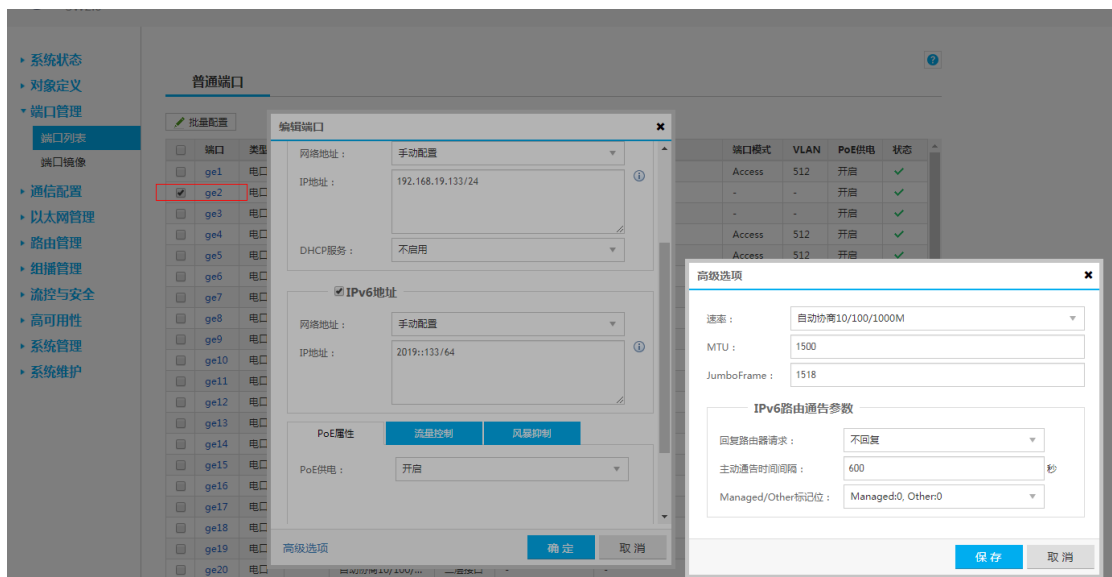
使用 IPv6 与网关及外网通信，需要保证配置的 IPv6 地址在外部存在路由回到交换机。

2.网络拓扑



3.配置步骤

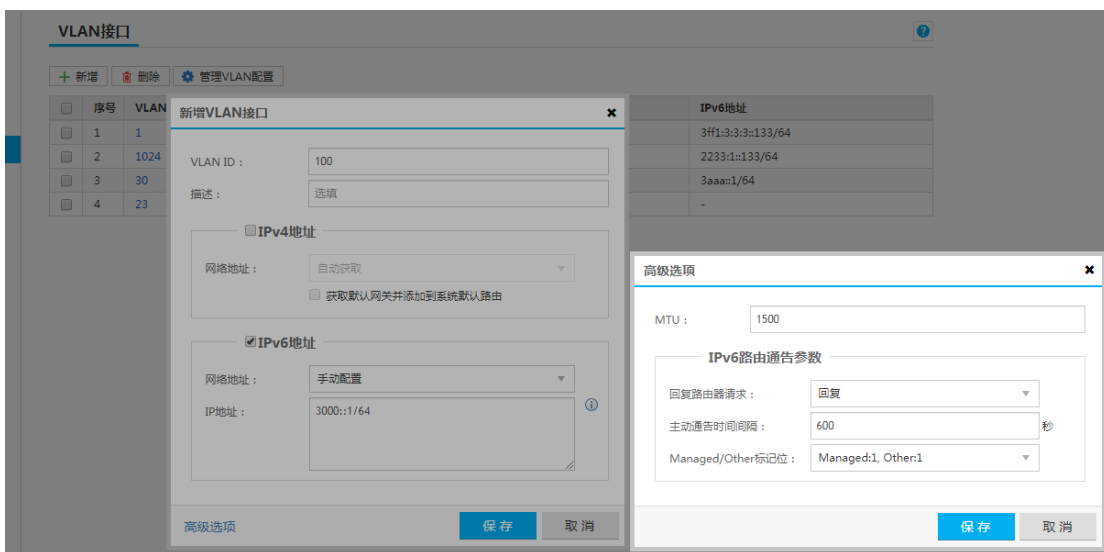
(1).胖模式交换机 1，启用端口 2 启用为三层口与出口网关对接，接口启用 IPv6 静态地址与出口网关子网 IPv6 地址同前缀。这里以网关子网为 2019::1/64 为例。



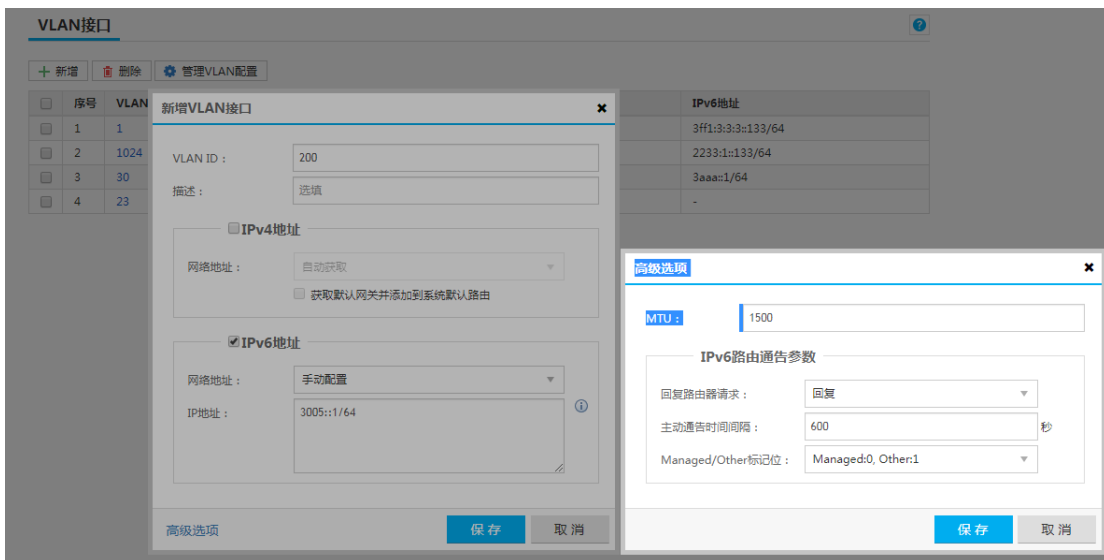
(2).静态路由创建一条 IPv6 默认路由，配置下一跳为出口网关子网 IPv6 地址，接口选择端口 2



(3).交换机划分两个 vlan 100、vlan200，vlan 100 启用静态 IPv6 地址，启用路由通告为回复，M/O 标记位为 1/1，外置 DHCPv6 服务器接入 vlan100。有线终端接入 vlan 100 自动获取 IPv6 地址与 DNS。



(4).vlan 200 启用静态 IPv6 地址，启用路由通告为回复，M/O 标记位为 0/1。有线终端接入 vlan 200 自动获取 IPv6 地址，配置静态 DNS 地址。



4.效果验证

(3). 终端获取到外置 DHCPv6 服务器分配的 IPv6 的与 DNS, 可以与出口网关及外网 IPv6

服务通信。

(4). 终端获取 vlan 200 接口 IPv6 地址前缀生成 IPv6 地址，可以与出口网关及外网 IPv6 服务通信。

第4章 交换机支持 VRRP

4.1.1. 场景 1：对三层核心交换机进行冗余备份，提高网络可靠性

场景描述：

- (1) 小型网络汇聚交换机做网关，并提供 DHCP 服务器；
- (2) 保证网关可靠性，汇聚(2)为备份设备，默认不转发流量，当主汇聚设备故障后，

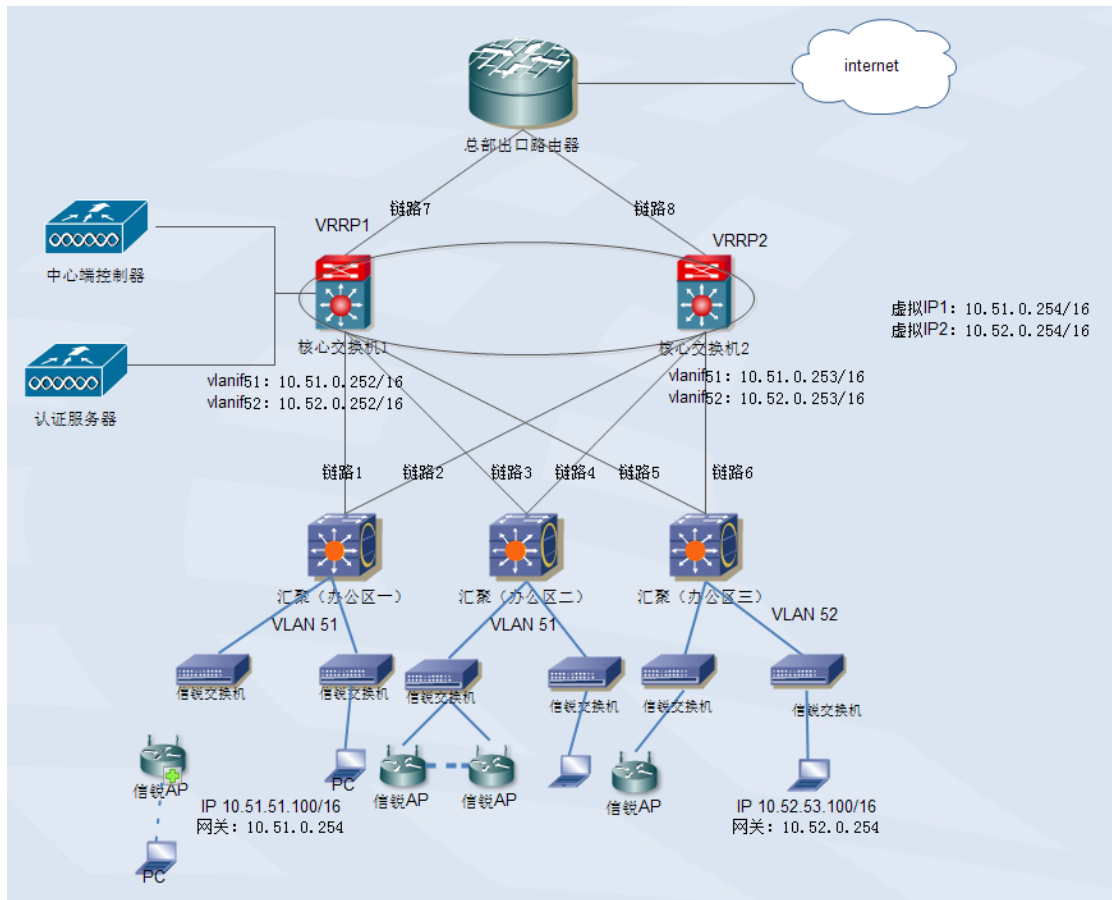
备份设备开始转发数据；

- (3) 任意链路断开，不会导致业务中断；
- (4) 网关升级维护时，业务不会中断；

3.1.1 环境准备

控制器，交换机，PC

网络拓扑：



3.1.2 策略配置:

6. 创建 VRRP 组 1，选择两个核心交换机，核心交换机 1 的优先级为 200，核心交换机 2 的优先级为 100，选择接口 vlanif51，虚拟 IP 地址为 10.51.0.254；

新增VRRP组 ✕

组名称:

组ID:

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	200	vlanif51 (10.51.0.4)	
智邦3	100	vlanif51 (10.51.0.3)	

DHCP服务: 启用DHCP服务 ?

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒):

7. 创建 VRRP 组 2，选择两个核心交换机，核心交换机 1 的优先级为 100，核心交换机 2 的优先级为 200，选择接口 vlanif52，虚拟 IP 地址为 10.52.0.254；

新增VRRP组



组名称:

组ID: i

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	100	vlanif52 (10.52.0.4)	
智邦3	200	vlanif52 (10.52.0.3)	

DHCP服务: 启用DHCP服务 i

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒): i

智邦4配置

优先级:

VRRP绑定接口: i

超时时间(秒):

接口监视: 启用接口监视

状态延迟恢复时间(秒): i

接口监视设置

监视链路断开或者端口异常时, 会独立升降其优先级

监视对象	故障时处理方式	操作
监视端口: 智邦4-port52	降级: 200	

3.1.3 终端验证:

1. 在实例 51 中交换机 1 为主机, 交换机 2 为备机, 在实例 52 中交换机 1 为备机, 交换机 2 为主机;

```
Sundray-SW ~ #tail -f /wns/log/openswitch/wns-vrrpd.log
[2019-4-1 20:47:2] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:3] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:4] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:5] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:6] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:7] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:8] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:10] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:11] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:12] [vrrp_in_chk:595](VI_10) invalid version. 7 and expect 3

[2019-4-1 20:49:14] [s_config_update_cb:56]Receive config change message
[2019-4-1 20:49:14] [reload_vrrp_thread:347]Reloading
[2019-4-1 20:49:14] [unreg_ipc_callback:145]Unregister ipc callback
[2019-4-1 20:49:14] [uninit_ovsdb_callback:728]Unregister ovsdb callback
[2019-4-1 20:49:14] [reset_ovsdb:757]Reset ovsdb related vars
[2019-4-1 20:49:14] [read_conf_file:423]Opening file '/var/wns/config/ap/keepalived.conf'
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_10) Found matching interface vrrp.10
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_11) Found matching interface vrrp.11
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_12) Found matching interface vrrp.12
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_13) Found matching interface vrrp.13
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_14) Found matching interface vrrp.14
[2019-4-1 20:49:14] [vrrp_complete_instance:2591](VI_15) Found matching interface vrrp.15
[2019-4-1 20:49:15] [vrrp_init_state:215](VI_10) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215](VI_11) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215](VI_13) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215](VI_15) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [init_ovsdb_callback:723]Register ovsdb callback
[2019-4-1 20:49:15] [reg_ipc_callback:116]Register ipc callback
[2019-4-1 20:49:15] [wns_cl_ev_init_thread:88]Init ipc thread
[2019-4-1 20:49:15] [wns_cl_ev_init_thread:96]Init telnet thread
[2019-4-1 20:49:15] [vrrp_register_workers:436]Init health checker thread
[2019-4-1 20:49:15] [vrrp_register_workers:449]Init heartbeat thread
[2019-4-1 20:49:15] [vrrp_register_workers:454]Init garp sending thread
[2019-4-1 20:49:15] [vrrp_state_backup:1592](VI_10) peer ip change to 10.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592](VI_13) peer ip change to 13.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592](VI_11) peer ip change to 11.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592](VI_15) peer ip change to 10.1.1.7
```

```
Sundray-SW ~ #telnet 127.0.0.1 20100
VRRP_DBG_CMD > s1

time now: Mon Apr 1 20:52:25 2019

NO  VRID  NAME  STATUS  PRIO_SET  PRIO_TOTAL  PRIO_NOW  FD_IN  FD_OUT  LAST_MASTER_ADDR  LAST_MASTER_PRIO  LAST_TRANS_TIME
1   10    VI_10 backup  50       50         50        17    18     10.1.1.8         100                Mon Apr 1 20:52:17 2019
2   11    VI_11 master  200      200        200        19    20     0.0.0.0          0                  Mon Apr 1 20:52:17 2019
```

2. vlan51 网段的业务流量默认走核心交换机 1 至路由出口, vlan52 的流量默认走核心交换机 2 至路由出口;

3. 核心交换机 1 故障, 在 VRRP 组 1 中, 核心交换机 2 自动切换为主机, 所有 vlan 的流量走核心交换机 2 至路由出口;

1. 上行链路 7-8，任意一条链路断开，均会触发主备切换，所有流量走另一条链路至路由器出口；

2. 下行链路 1-6 任意一条链路断开，均会触发主备切换，所有流量走一台核心交换机至路由器出口；

4.1.2. 场景 2：对核心交换机冗余备份，通过生成树协议进行链路冗余，提高网络可靠性

场景描述：

3. 小型网络汇聚交换机做网关，并提供 DHCP 服务器；

4. 保证网关可靠性，汇聚（2）为备份设备，默认不转发流量，当主汇聚设备故障后，备份设备开始转发数据；

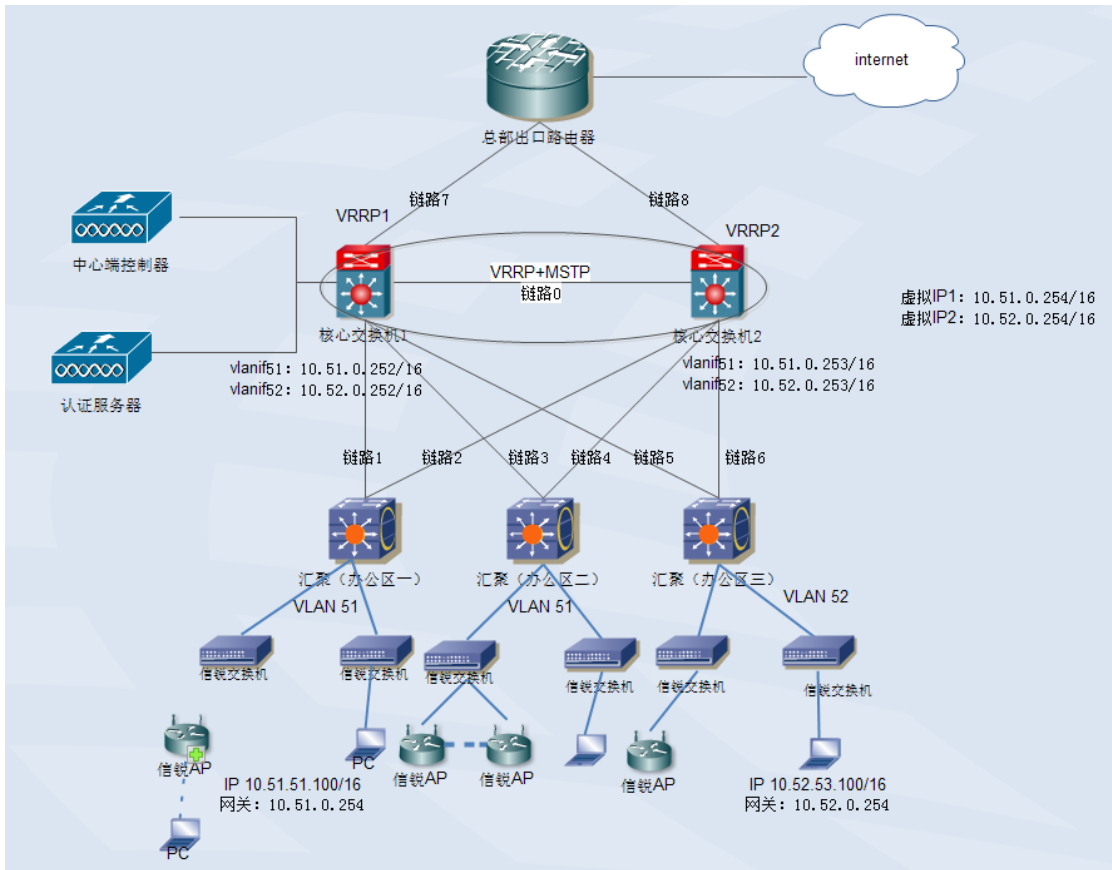
5. 任意链路断开，不会导致业务中断；

6. 网关升级维护时，业务不会中断；

3.2.1 环境准备

控制器，交换机，PC

网络拓扑：



3.2.2 策略配置

1. 创建 VRRP 组 1，选择两个核心交换机，核心交换机 1 的优先级为 200，核心交换机 2 的优先级为 100，选择接口 vlanif51，虚拟 IP 地址为 10.51.0.254；

新增VRRP组 ✕

组名称:

组ID:

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	200	vlanif51 (10.51.0.4)	
智邦3	100	vlanif51 (10.51.0.3)	

DHCP服务: 启用DHCP服务 i

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒):

2. 创建 VRRP 组 2，选择两个核心交换机，核心交换机 1 的优先级为 100，核心交换机 2 的优先级为 200，选择接口 vlanif52，虚拟 IP 地址为 10.52.0.254；

新增VRRP组



组名称:

组ID: i

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	100	vlanif52 (10.52.0.4)	
智邦3	200	vlanif52 (10.52.0.3)	

DHCP服务: 启用DHCP服务 i

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒): i

智邦4配置

优先级:

VRRP绑定接口:

超时时间(秒):

接口监视: 启用接口监视

状态延迟恢复时间(秒):

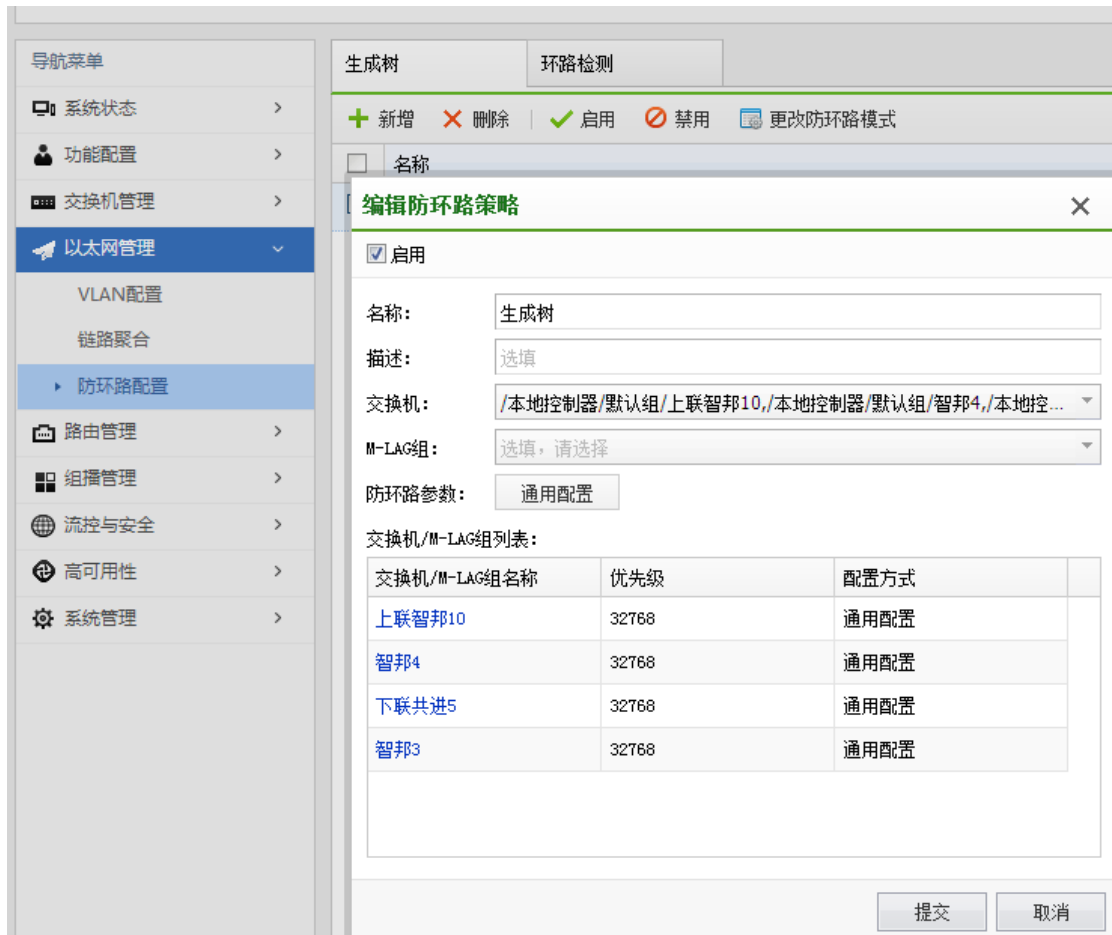
[接口监视设置](#)

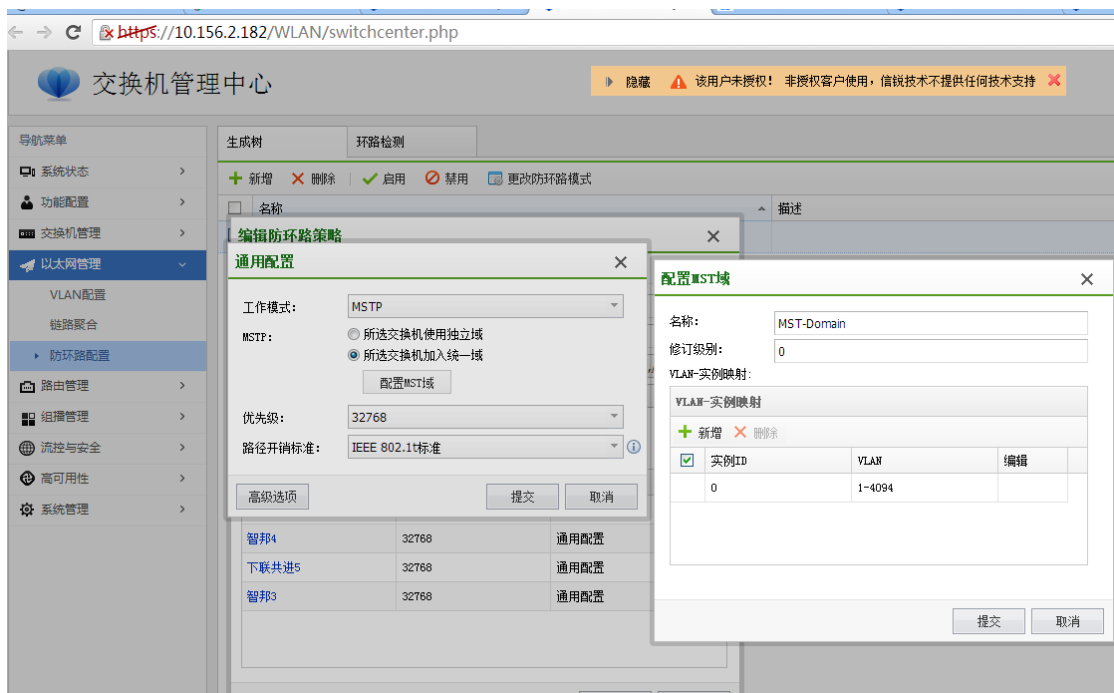
接口监视设置

监视链路断开或者端口异常时, 会独立升降其优先级

监视对象	故障时处理方式	操作
监视端口: 智邦4-port52	降级: 200	

3. 核心交换机与汇聚交换机启用 MSTP 功能，配置阻塞端口为直连链路端口（阻塞端口需要人工调整）；





3.2.3 终端验证

4. vlan51 网段的业务流量默认走核心交换机 1 至路由出口，vlan52 的流量默认走核心交换机 2 至路由出口；


```

Sundray-SW ~ #tail -f /wms/log/openswitch/wms-vrrpd.log
[2019-4-1 20:47:2] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:3] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:4] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:5] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:6] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:7] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:8] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:10] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:11] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:12] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3

[2019-4-1 20:49:14] [s_config_update_cb:56]Receive config change message
[2019-4-1 20:49:14] [reload_vrrp_thread:347]Reloading
[2019-4-1 20:49:14] [unreg_ipc_callback:145]Unregister ipc callback
[2019-4-1 20:49:14] [uninit_ovsdb_callback:728]Unregister ovsdb callback
[2019-4-1 20:49:14] [reset_ovsdb:757]Reset ovsdb related vars
[2019-4-1 20:49:14] [read_conf_file:423]Opening file '/var/wms/config/ap/keepalived.conf'.
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_10) Found matching interface vrrp.10
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_11) Found matching interface vrrp.11
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_12) Found matching interface vrrp.12
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_13) Found matching interface vrrp.13
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_14) Found matching interface vrrp.14
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_15) Found matching interface vrrp.15
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_10) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_11) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_13) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_15) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [init_ovsdb_callback:723]Register ovsdb callback
[2019-4-1 20:49:15] [reg_ipc_callback:116]Register ipc callback
[2019-4-1 20:49:15] [wms_cl_ev_init_thread:88]Init ipc thread
[2019-4-1 20:49:15] [wms_cl_ev_init_thread:96]Init telnet thread
[2019-4-1 20:49:15] [vrrp_register_workers:436]Init health checker thread
[2019-4-1 20:49:15] [vrrp_register_workers:449]Init heartbeat thread
[2019-4-1 20:49:15] [vrrp_register_workers:454]Init garp sending thread
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_10) peer ip change to 10.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_13) peer ip change to 13.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_11) peer ip change to 11.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_15) peer ip change to 10.1.1.7
    
```

```

Sundray-SW ~ #telnet 127.0.0.1 20100
VRRP_DBG_CMD > #1
time now: Mon Apr 1 20:52:25 2019

```

NO	VRID	NAME	STATUS	PRIO_SET	PRIO_TOTAL	PRIO_NOW	FD_IN	FD_OUT	LAST_MASTER_ADDR	LAST_MASTER_PRIO	LAST_TRANS_TIME
1	10	VI_10	backup	50	50	50	17	18	10.1.1.8	100	Mon Apr 1 20:52:17 2019
2	11	VI_11	master	200	200	200	19	20	0.0.0.0	0	Mon Apr 1 20:52:17 2019

5. 核心交换机 1 故障，在 VRRP 组 1 中，核心交换机 2 自动切换为主机，所有 vlan 的流量走核心交换机 2 至路由出口；

6. 上行链路 7-8，任意一条链路断开，均会触发主备切换，所有流量走另一条上行链路至路由器出口；

7. 下行链路 1-6 任意一条链路断开，MSTP 重新收敛，不会触发主备切换；

5. 直连线路 0 断开，MSTP 重新收敛，不会触发主备切换；

4.1.3. 场景 3：对核心交换机冗余备份，通过 MLAG 进行设备和链路冗余提高网络可靠性

场景描述：

(1) 小型网络汇聚交换机做网关，并提供 DHCP 服务器；

(2) 保证网关可靠性，汇聚 (2) 为备份设备，默认不转发流量，当主汇聚设备故障后，备份设备开始转发数据；

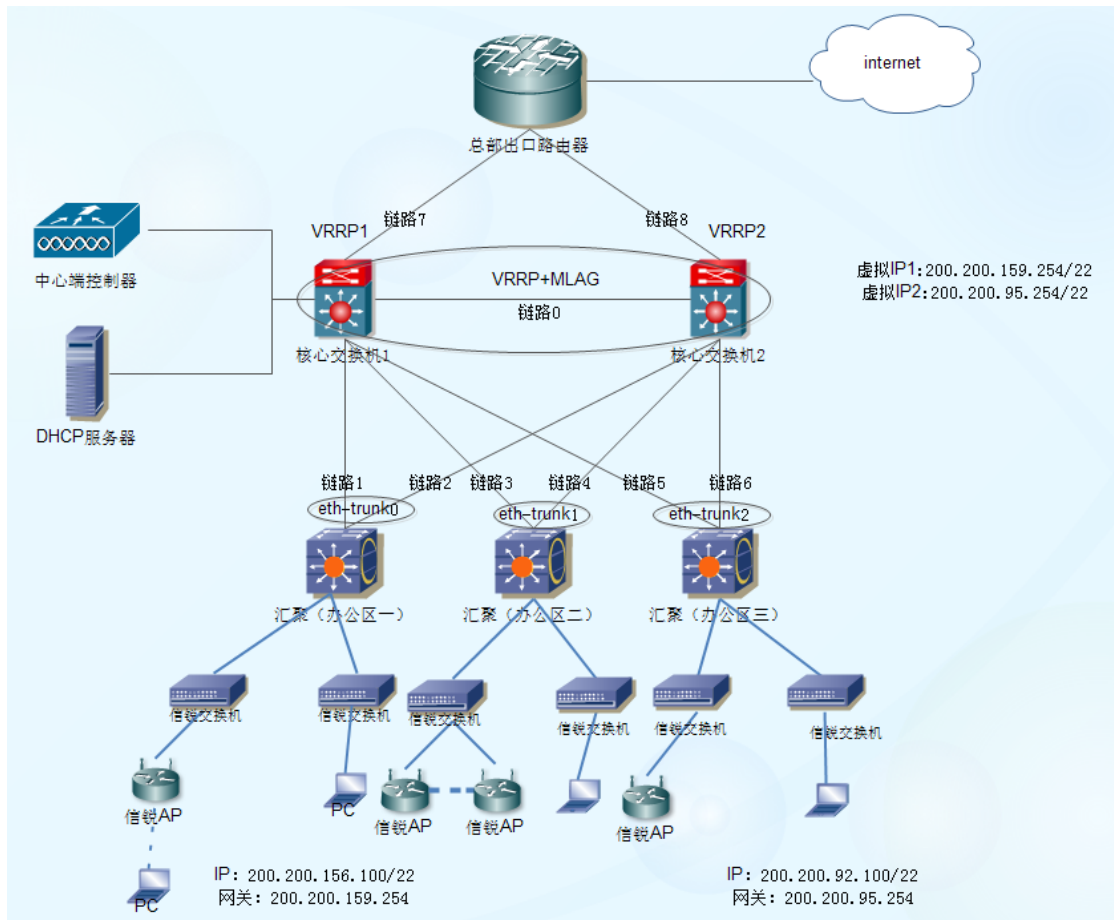
(3) 任意链路断开，不会导致业务中断；

(4) 网关升级维护时，业务不会中断；

3.3.1 环境准备

控制器，交换机，PC

网络拓扑：



3.3.2 策略配置

1. 创建 VRRP 组 1，选择两个核心交换机，核心交换机 1 的优先级为 200，核心交换机 2 的优先级为 100，选择接口 vlanif51，虚拟 IP 地址为 10.51.0.254；

新增VRRP组 ✕

组名称:

组ID:

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	200	vlanif51 (10.51.0.4)	
智邦3	100	vlanif51 (10.51.0.3)	

DHCP服务: 启用DHCP服务 ?

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒):

2. 创建 VRRP 组 2，选择两个核心交换机，核心交换机 1 的优先级为 100，核心交换机 2 的优先级为 200，选择接口 vlanif52，虚拟 IP 地址为 10.52.0.254；

新增VRRP组



组名称:

组ID: i

虚拟IP地址:

虚拟MAC: 启用虚拟MAC

通信方式:

交换机配置:

交换机名称	优先级	接口	编辑
智邦4	100	vlanif52 (10.52.0.4)	
智邦3	200	vlanif52 (10.52.0.3)	

DHCP服务: 启用DHCP服务 i

DHCP服务策略:

抢占功能: 启用抢占功能

延时抢占时间(秒): i

智邦4配置

优先级:

VRRP绑定接口: i

超时时间(秒):

接口监视: 启用接口监视

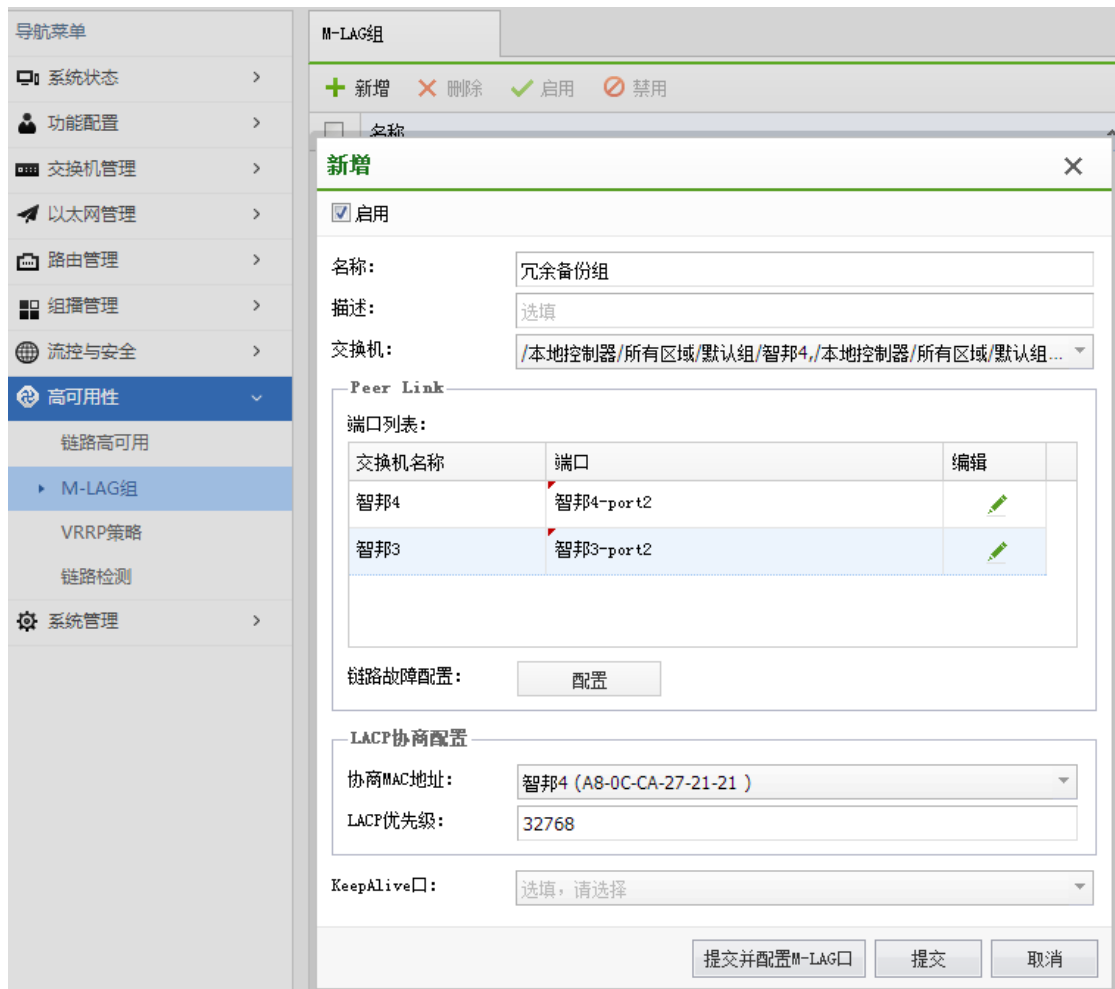
状态延迟恢复时间(秒): i

接口监视设置

监视链路断开或者端口异常时, 会独立升降其优先级

监视对象	故障时处理方式	操作
智邦4-port52	降级: 200	

3. 创建 MLAG 组，选择两台核心交换机；



3.3.3 终端验证

(1) vlan51 网段的业务流量默认走核心交换机 1 至路由出口，vlan52 的流量默认走核心交换机 2 至路由出口；

```

Sundray-SW ~ #tail -f /wms/log/openswitch/wms-vrrpd.log
[2019-4-1 20:47:2] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:3] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:4] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:5] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:6] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:7] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:8] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:10] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:11] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3
[2019-4-1 20:47:12] [vrrp_in_chk:595] (VI_10) invalid version. 7 and expect 3

[2019-4-1 20:49:14] [s_config_update_cb:56]Receive config change message
[2019-4-1 20:49:14] [reload_vrrp_thread:347]Reloading
[2019-4-1 20:49:14] [unreg_ipc_callback:145]Unregister ipc callback
[2019-4-1 20:49:14] [uninit_ovsdb_callback:728]Unregister ovsdb callback
[2019-4-1 20:49:14] [reset_ovsdb:757]Reset ovsdb related vars
[2019-4-1 20:49:14] [read_conf_file:423]Opening file '/var/wms/config/ap/keepalived.conf'.
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_10) Found matching interface vrrp.10
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_11) Found matching interface vrrp.11
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_12) Found matching interface vrrp.12
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_13) Found matching interface vrrp.13
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_14) Found matching interface vrrp.14
[2019-4-1 20:49:14] [vrrp_complete_instance:2591] (VI_15) Found matching interface vrrp.15
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_10) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_11) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_13) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [vrrp_init_state:215] (VI_15) Entering BACKUP STATE (init)
[2019-4-1 20:49:15] [init_ovsdb_callback:723]Register ovsdb callback
[2019-4-1 20:49:15] [reg_ipc_callback:116]Register ipc callback
[2019-4-1 20:49:15] [wms_cl_ev_init_thread:88]Init ipc thread
[2019-4-1 20:49:15] [wms_cl_ev_init_thread:96]Init telnet thread
[2019-4-1 20:49:15] [vrrp_register_workers:436]Init health checker thread
[2019-4-1 20:49:15] [vrrp_register_workers:449]Init heartbeat thread
[2019-4-1 20:49:15] [vrrp_register_workers:454]Init garp sending thread
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_10) peer ip change to 10.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_13) peer ip change to 13.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_11) peer ip change to 11.1.1.7
[2019-4-1 20:49:15] [vrrp_state_backup:1592] (VI_15) peer ip change to 10.1.1.7
    
```

```

Sundray-SW ~ #telnet 127.0.0.1 20100
VRRP_DBG_CMD > #1
time now: Mon Apr 1 20:52:25 2019
NO  VRID  NAME  STATUS  PRIO_SET  PRIO_TOTAL  PRIO_NOW  FD_IN  FD_OUT  LAST_MASTER_ADDR  LAST_MASTER_PRIO  LAST_TRANS_TIME
1   10    VI_10 backup  50       50          50         17     18     10.1.1.8         100                Mon Apr 1 20:52:17 2019
2   11    VI_11 master  200      200         200         19     20     0.0.0.0          0                  Mon Apr 1 20:52:17 2019
    
```

(2) 核心交换机 1 故障，在 VRRP 组 1 中，核心交换机 2 自动切换为主机，所有 vlan 的流量走核心交换机 2 至路由出口；

(3) 上行链路 7-8，任意一条链路断开，均会触发主备切换，所有流量走另一条上行链路至路由器出口；

(4) 下行链路 1-6 任意一条链路断开，MLAG 及 VRRP 正常工作，不会触发主备切换；

5. peerlink 链路 0 故障，MLAG 备机会 down 端口，此时 VRRP 触发主备切换，所有流量走一台设备至路由出口；

4.1.4. 场景 4：部署交换机冗余备份组，使用同步组功能较少交换机 CPU 消耗

3.4.1 环境准备

控制器，交换机，PC

3.4.2 策略配置

(1) 创建 vrrp 冗余备份组，选择两个交换机，新增 5 个实例；

(2) 在冗余备份组中，新增同步组，选择所配置的 5 个实例，并选择实例 10 为同步源；

VRRP组列表：

+ 新增 × 删除 ✎ 批量编辑					
<input type="checkbox"/>	组名称	组ID	通信方式	DHCP服务	抢占功能
<input type="checkbox"/>	实例10	10	组播通信	禁用	启用
<input type="checkbox"/>	实例...	110	组播通信	禁用	启用
<input type="checkbox"/>	实例12	12	组播通信	禁用	启用
<input type="checkbox"/>	实例13	13	组播通信	禁用	启用

代管组（由组内当前VRID最小的MASTER实例代发报文）：

+ 新增 × 删除			
<input type="checkbox"/>	序号	代管组成员	操作
没有可以显示的数据			

同步组（组成员丧失一切能动性，状态与同步源保持一致）：

+ 新增 × 删除				
<input type="checkbox"/>	序号	组成员	同步源	操作
<input type="checkbox"/>	1	实例10, 实例12, 实例13, 实例15, ...	实例10	✎

3.4.3 终端验证

1. 加入同步组后，以上配置的所有 5 个实例中，同步源中的主机发送 VRRP 报文，其他实例均不发送报文，且 VRRP 主备状态与同步源保持一致；

2. 加入同步组的所有实例主备机状态均一致，也就是说在一台交换机上所有实例的状态都是主机或者都是备机状态（此处与代管组不同），无法进行流量的负载分担。

4.1.5. 场景 5：部署交换机冗余备份组，使用代管组功能较少交换机 CPU 消耗

3.5.1 环境准备

控制器，交换机，PC

3.5.2 策略配置

1. 创建 vrrp 冗余备份组，选择两个交换机，新增 5 个实例；
2. 在冗余备份组中，新增代管组，选择所配置的 5 个实例；

VRRP组列表：

+ 新增 × 删除 批里编辑					
<input type="checkbox"/>	组名称	组ID	通信方式	DHCP服务	抢占功能
<input type="checkbox"/>	实例10	10	组播通信	禁用	启用
<input type="checkbox"/>	实例...	110	组播通信	禁用	启用
<input type="checkbox"/>	实例12	12	组播通信	禁用	启用
<input type="checkbox"/>	实例13	13	组播通信	禁用	启用

代管组（由组内当前VRID最小的MASTER实例代发报文）：

+ 新增 × 删除			
<input type="checkbox"/>	序号	代管组成员	操作
<input type="checkbox"/>	1	实例10, 实例12, 实例13, 实例15, 实例110	

3.5.3 终端验证

3. 加入代管组后，以上配置的所有 5 个实例中，由实例 ID 值最小的主机负责发送 VRRP 报文，其他实例的信息均包含在该主机发送的 VRRP 报文中；

4. 加入代管组的所有实例均具有自己的主备机状态，也就是说一台交换机上所有实例的状态可以不一致（此处与同步组不同），可以进行流量的负载分担。

WNS3.7.9 版本产品白皮书



修订记录

修订版 本号	作 者	日期	简要说明

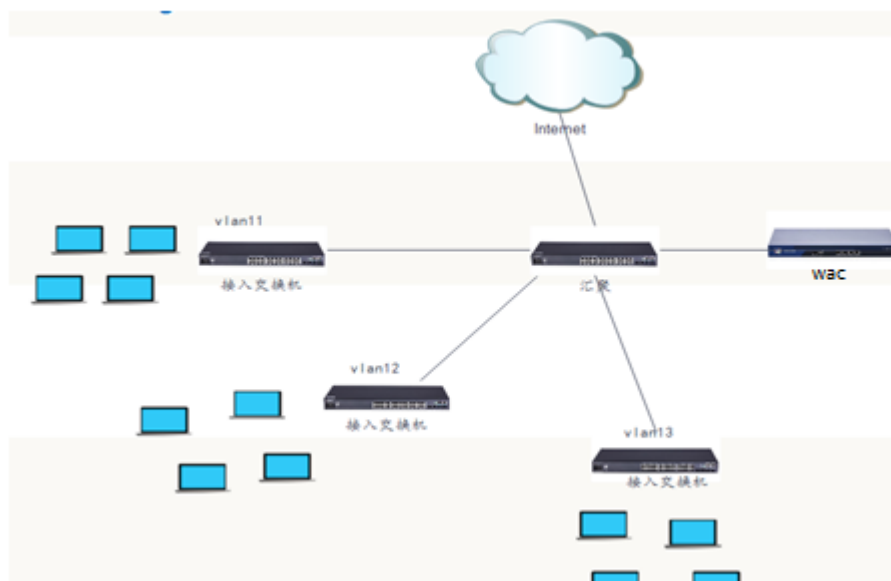
第5章 OSPF 配置

5.1. 企业快速配置 OSPF 网络实现设备间网络互通

场景描述:

某企业存在研发、财务和客服三个部门，每个部门分属不同的 vlan，各 vlan 间不能互相访问，将各个 vlan 接口加入 OSPF 策略区域中，即可实现，研发、财务和客服部门之间可以跨三层互相访问。

网络拓扑:



拓扑说明:

研发、财务和客服分别属于 vlan 11、vlan 12 和 vlan 13。

演示步骤:

1.环境准备:

WAC: 1 台

信锐交换机: 3 台

2.策略配置

(1) 新增 OSPF 策略，并选择对应的 vlan 接口和邻接关系协商口通告到区域中；

OSPF配置 | 交换机OSPF参数配置 | 端口OSPF参数配置

+ 新增 × 删除 | ✓ 启用 ⊘ 禁用

名称: OSPF

描述: 选填

交换机: /所有区域/默认组/第一台sw1,/所有区域/默认组/第四台sw4,/所有区... 路由标识

基准带宽 (M): 100

区域列表:

区域名称	区域ID	区域类型	接口	认证方式
area 0	0	骨干区域	Loopback (第一...	不启用

6.功能验证

第一台sw1-OSPF路由详情

路由标识符: 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
22.22.22.22/32	111.111.111.2	vlan11	2	110	正常	
112.112.112.0/24	111.111.111.2	vlan11	1	110	正常	
111.111.111.0/24	-	vlan11	1	110	已失效	
44.44.44.44/32	111.111.111.2	vlan11	1	110	正常	
11.11.11.11/32	-	loopback1	1	110	已失效	

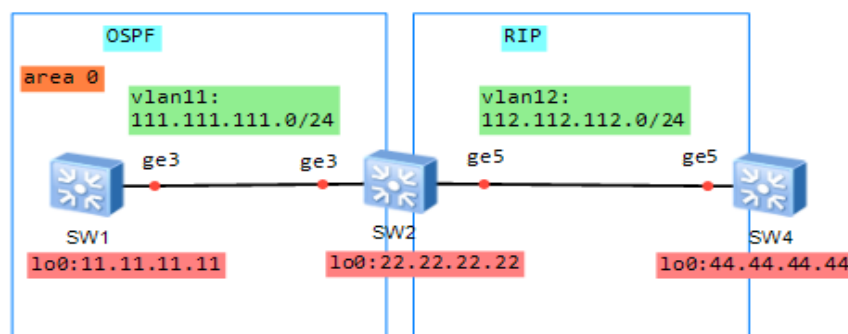
OSPF 区域内的 vlan11、vlan12、vlan13 的设备之间可以互相访问。

5.2. 企业 OSPF 网络引入外部路由(路由引入)

场景描述:

某企业网络中使用了 RIPv2 和 OSPF 协议。企业希望实现 RIP 区域设备与 OSPF 区域设备之间的互通,可以在交换机 OSPF 参数配置 RIP 路由引入,RIP 配置中也引入 OSPF 路由,从而实现 RIP 区域与 OSPF 区域设备之间的互通。路由引入包括直连路由、RIP 路由、静态路由、默认路由。

网络拓扑:



演示步骤:

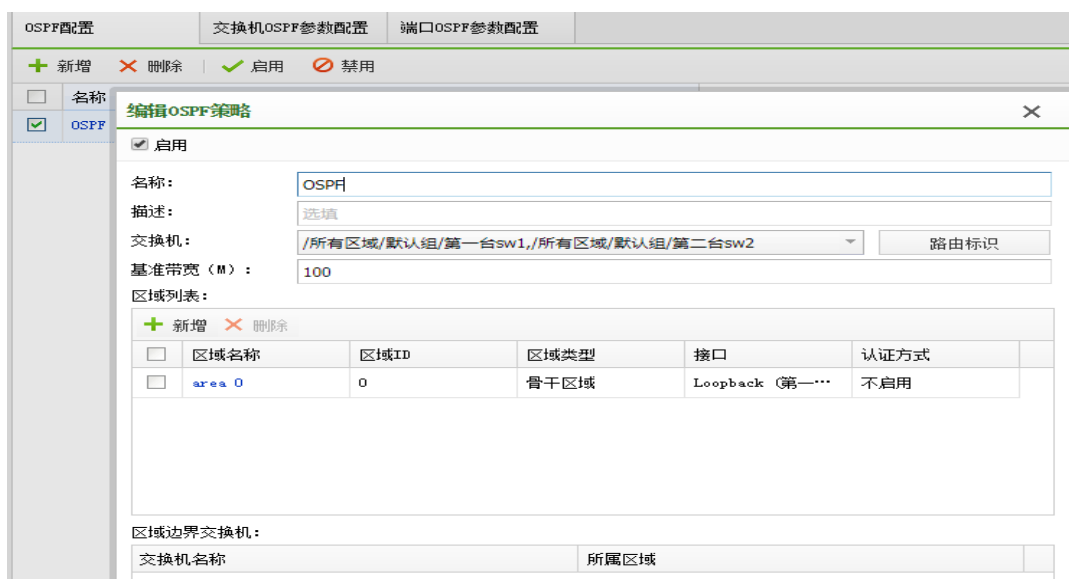
1.环境准备:

WAC: 1 台

信锐交换机: 三台

2.策略配置:

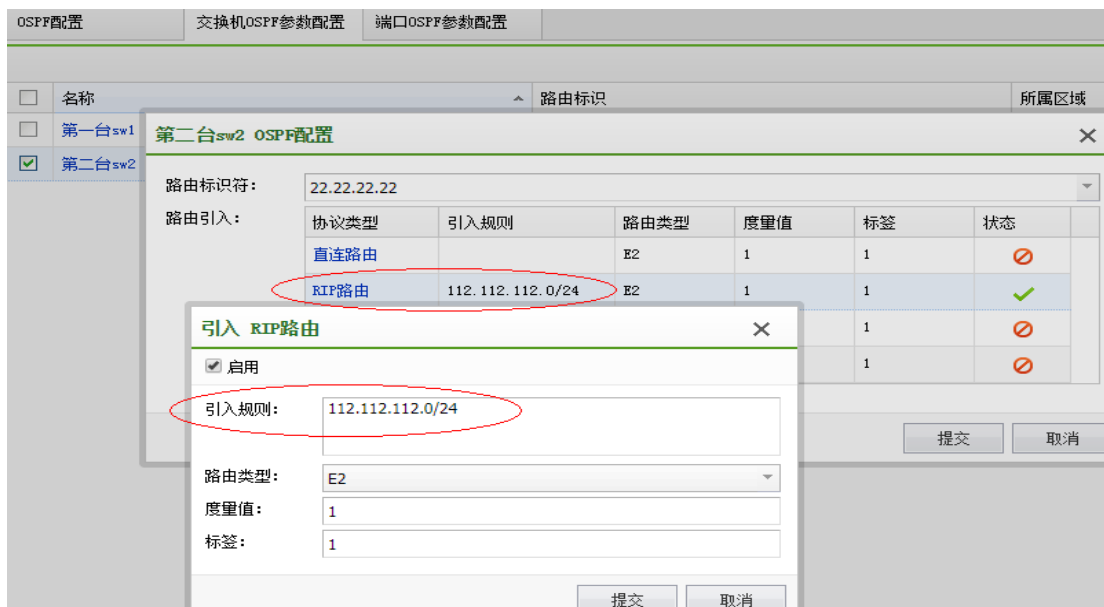
(1) 新增 OSPF 策略, 选择对应需要加入 OSPF 区域的接口以及对应的邻接关系协商口;



(2) 在交换机 OSPF 参数配置页面, 在加入了 RIP 区域的设备上配置 RIP 路由引入;



引入 RIP 路由也可增加引入规则配置，符合规则的路由则会被引入到 OSPF 区域中，从而实现 OSPF 区域内的设备能够访问 RIP 区域的部分设备，默认是引入全部 RIP 路由。



8.功能验证

未配置引入规则：

第一台sw1-OSPF路由详情

路由标识符： 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
22.22.22.22/32	111.111.111.2	vlan11	2	110	正常	
112.112.112.0/24	111.111.111.2	vlan11	1	110	正常	
111.111.111.0/24	-	vlan11	1	110	已失效	
44.44.44.44/32	111.111.111.2	vlan11	1	110	正常	
11.11.11.11/32	-	loopback1	1	110	已失效	

OSPF 区域内的设备已经存在去往 RIP 区域内的设备的路由，不同路由协议类型之间的设备可以互访。

配置了引入规则：

第一台sw1-OSPF路由详情

路由标识符: 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
22.22.22.22/32	111.111.111.2	vlan11	2	110	正常	
112.112.112.0/24	111.111.111.2	vlan11	1	110	正常	
111.111.111.0/24	-	vlan11	1	110	已失效	
11.11.11.11/32	-	loopback1	1	110	已失效	

OSPF 区域内的设备已经存在符合引入规则前缀的去往 RIP 区域内设备的路由，从而实现 OSPF 区域内设备只能访问 RIP 区域中客服部（vlan12）的设备。

直连路由、静态路由和默认路由的引入与 RIP 路由的引入类似，只是引入的路由类型不同。

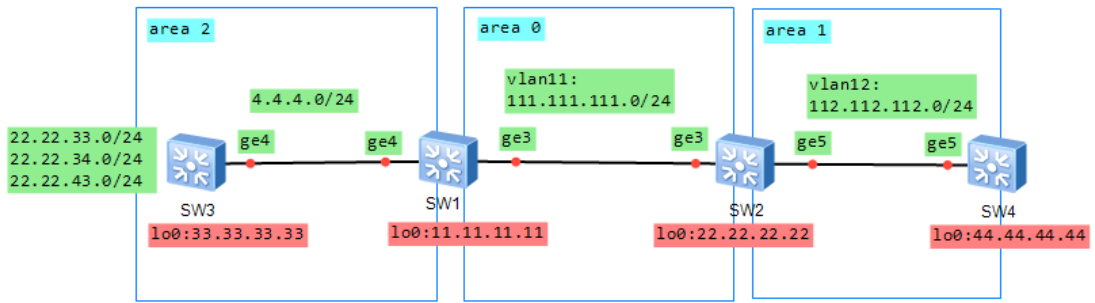
5.3. 企业 OSPF 网络区域 1 不接收区域 2 的路由 (路由白名单)

场景描述:

企业网络中，区域 1（研发部）的设备不能访问区域 2（财务部）的部分设备，此时通过配置区域 1 中 ABR 设备的入方向的路由白名单，或者区域 2 中 ABR 设备的出方向的路由白名单，可以实现区域 1 内设备只能访问区域 2 的部分设备。

用户网络存在性能设备较差，不支持学习大量路由，可以通过配置路由白名单，只保留需要学习到的路由信息。

网络拓扑:



演示步骤:

1.环境准备:

WAC: 1台

信锐交换机: 4台

2.策略配置:

(1) 在交换机 OSPF 参数配置页面区域 1 配置 ABR 设备启用入方向的路由白名单



(2) 在交换机 OSPF 参数配置页面区域 2 配置 ABR 设备启用出方向的路由白名单

OSPF配置 | 交换机OSPF参数配置 | 端口OSPF参数配置

第一台sw1 OSPF配置

名称: 第一台sw1 第三台sw3 第二台sw2 第四台sw4

路由标识符: 11.11.11.11

路由引入:

协议类型	引入规则	路由类型	度量值	标签	状态
直连路由		E2	1	1	
RIP路由		E2	1	1	
静态路由		E2	1	1	
默认路由		E2	1	1	

区域配置

区域名称: area 0, area 2

缺省路由度量值: 1

路由白名单

对区域内出/入方向的域间路由设置过滤条件，只有通过路由白名单的信息才能被发布/接收。

入方向
目标地址前缀: 一行一个IP地址/掩码，例如192.168.1.1/24或192.168.1.1/255.255.255.0

出方向
目标地址前缀: 22.22.30.0/24

3.功能验证

第四台sw4-OSPF路由详情

路由标识符: 44.44.44.44

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
22.22.33.0/24	112.112.112.2	vlan12	4	110	正常	
22.22.34.0/24	112.112.112.2	vlan12	4	110	正常	
44.44.44.44/32	-	loopback1	1	110	已失效	
112.112.112.0/24	-	vlan12	1	110	已失效	

区域 1 中的设备只有去往区域 2 的部分设备的路由。

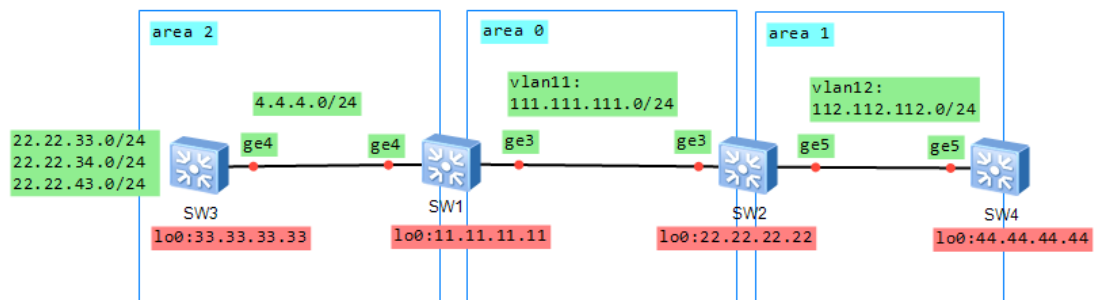
路由白名单只对 3 类 LSA 生效。

5.4. 企业网络中存在多条前缀有重叠的路由（路由聚合）

场景描述:

当企业 OSPF 网络规模较大时，配置路由聚合，可以有效减少路由表中的条目，减小对系统资源的占用，不影响系统的性能。此外，如果被聚合的 IP 地址范围内的某条链路频繁 Up 和 Down，该变化并不会通告到被聚合的 IP 地址范围外的设备。因此，可以避免网络中的路由震荡，在一定程度上提高了网络的稳定性。

网络拓扑：



演示步骤：

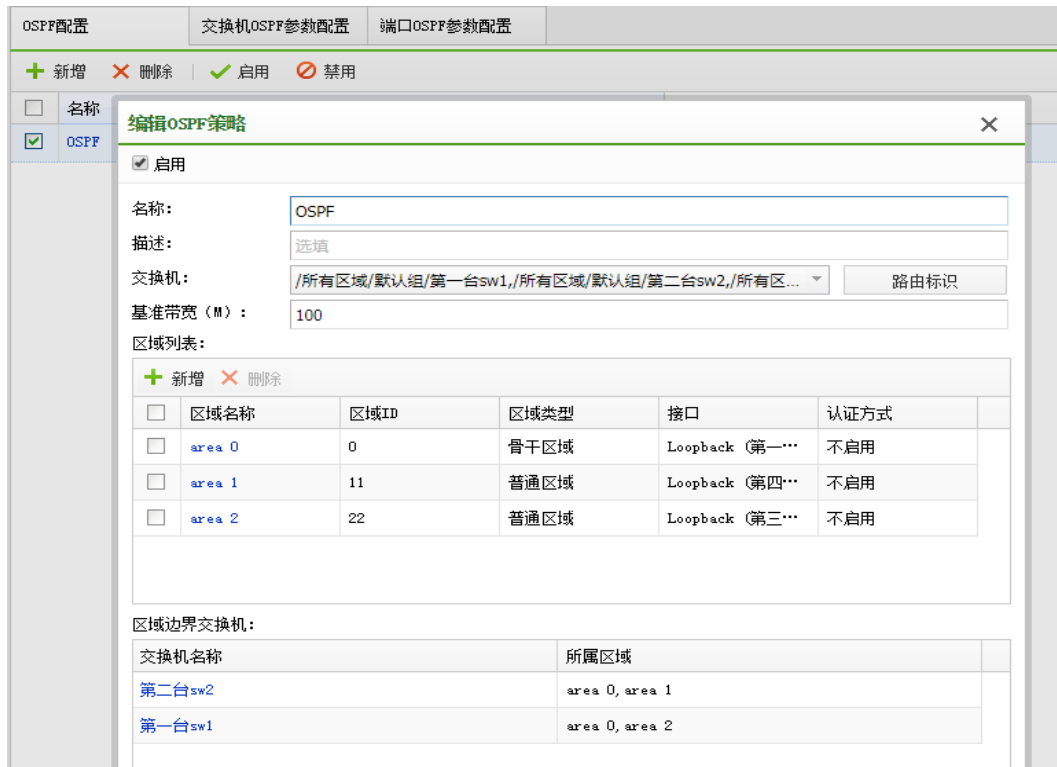
1.环境准备：

WAC: 1 台

信锐交换机: 3 台

2.策略配置：

(1) 新增 OSPF 策略；



(2) 交换机 OSPF 参数配置页面，选择区域 2 中的 ABR 设备（区域边界设备）配置路由聚合，这样在区域 0 中的设备即可学习到聚合后的对应路由信息；

OSPF配置 交换机OSPF参数配置 端口OSPF参数配置

第一台sw1 OSPF配置

路由标识符: 11.11.11.11

路由引入:

协议类型	引入规则	路由类型	度量值	标签	状态
直连路由		E2	1	1	<input checked="" type="checkbox"/>
RIP路由		E2	1	1	<input checked="" type="checkbox"/>
静态路由		E2	1	1	<input checked="" type="checkbox"/>
默认路由		E2	1	1	<input checked="" type="checkbox"/>

区域配置

区域名称

- area 0
- area 2**

缺省路由度量值: 1

路由白名单

对区域内出/入方向的域间路由设置过滤条件，只有通过路由白名单的信息才能被发布/接收。

入方向
目标地址前缀: 一行一个IP地址/掩码，例如192.168.1.1/24或192.168.1.1/255.255.255.0

出方向
目标地址前缀: 22.22.32.0/22

路由聚合:

+ 新增 - 删除

IP地址	网络掩码	度量值	路由发布	编辑
<input type="checkbox"/>				
<input checked="" type="checkbox"/>	22.22.0.0	255.255.0.0	自动设置	是

3.功能验证

第二台sw2-OSPF路由详情

路由标识符: 22.22.22.22

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
112.112.112.0/24	-	vlan12	1	110	已失效	
33.33.33.33/32	111.111.111.1	vlan11	3	110	正常	
4.4.4.0/24	111.111.111.1	vlan11	2	110	正常	
22.22.0.0/16	111.111.111.1	vlan11	3	110	正常	
11.11.11.11/32	111.111.111.1	vlan11	2	110	正常	
22.22.22.22/32	-	loopback1	1	110	已失效	
111.111.111.0/24	-	vlan11	1	110	已失效	
44.44.44.44/32	112.112.112.4	vlan12	2	110	正常	

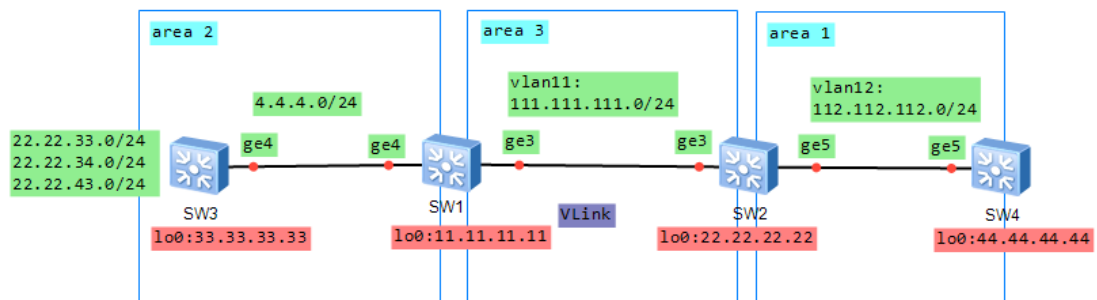
区域 0 中的设备学习到了聚合之后的路由条目，减少了路由表中的条目，减小对系统资源的占用。路由聚合只对 3 类 LSA 有效。

5.5. 企业 OSPF 网络中配置虚连接

场景描述:

在划分 OSPF 区域后，非骨干区域之间的 OSPF 路由更新是通过骨干区域来交换完成的。因此，OSPF 要求所有非骨干区域必须与骨干区域保持连通，并且骨干区域之间也要保持连通。但在实际应用中，因为各方面条件的限制，可能无法满足这个要求，这时可以通过配置 OSPF 虚连接解决。

网络拓扑:



演示步骤:

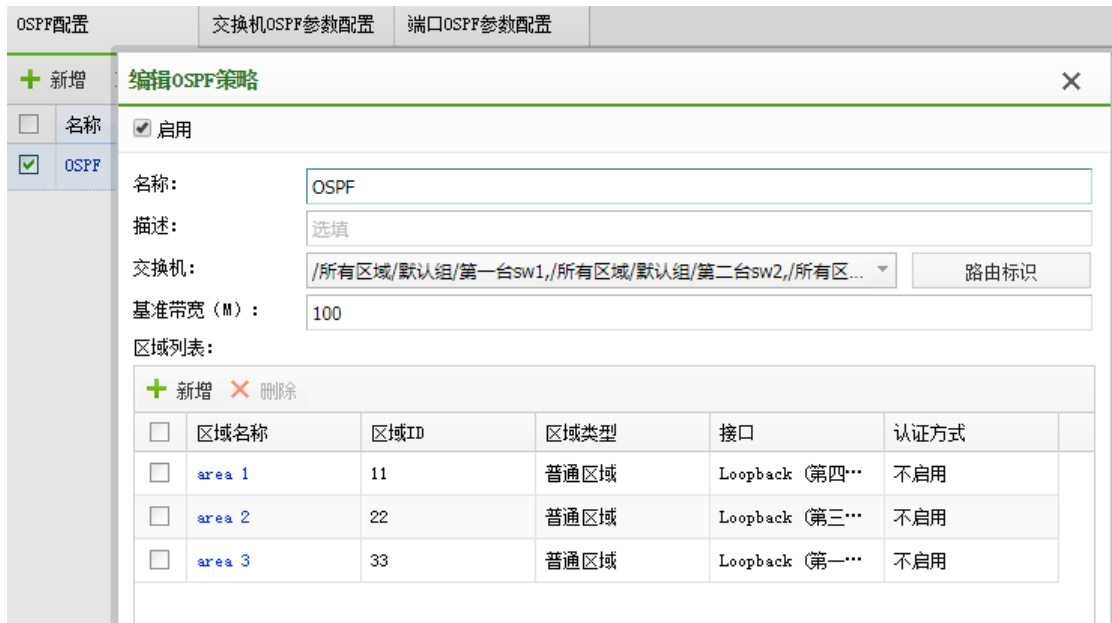
1.环境准备

WAC : 1 台

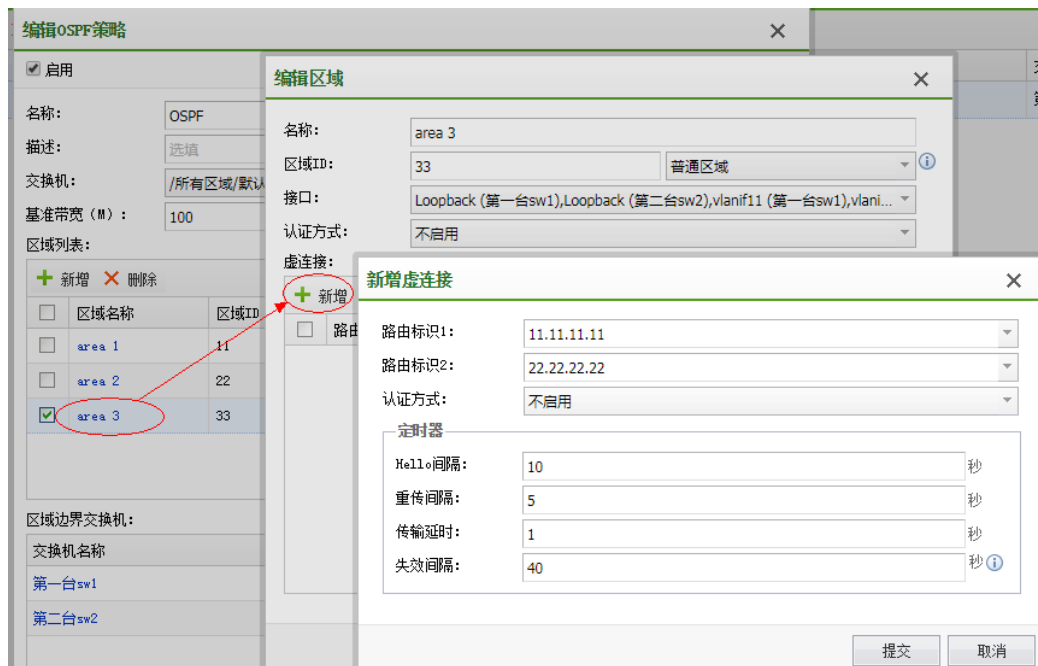
信锐交换机: 4 台

2.策略配置

- (1) 新增 OSPF 策略，策略中有两个相邻区域，且都为非骨干区域；



(2) 在区域 3 配置一条虚连接;



8. 功能验证

第一台sw1-OSPF路由详情

路由标识符: 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息						
接口名称	IP地址	区域	网络类型	度量值	DR选举优先级	邻居状态改...	DR设备	认证方式	状态
VLINK0	-	-	P2P	1	1	1次	-	不启用	Point-to-Po...
loopback1	11.11.11.11...	area 3	Broadcast	1	1	1次	-	不启用	Loopback
vlan11	111.111.111...	area 3	Broadcast	1	1	2次	111.111.111.2	不启用	Backup DR
ge4	4.4.4.1/24	area 2	Broadcast	1	1	2次	4.4.4.3	不启用	Backup DR

第四台sw4-OSPF路由详情

路由标识符: 44.44.44.44

OSPF状态	邻接关系	接口信息	路由信息		
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态
22.22.0.0/16	112.112.112.2	vlan12	4	110	正常
33.33.33.33/32	112.112.112.2	vlan12	4	110	正常
4.4.4.0/24	112.112.112.2	vlan12	3	110	正常
111.111.111.0/24	112.112.112.2	vlan12	2	110	正常
11.11.11.11/32	112.112.112.2	vlan12	3	110	正常
22.22.22.22/32	112.112.112.2	vlan12	2	110	正常
44.44.44.44/32	-	loopback1	1	110	已失效
112.112.112.0/24	-	vlan12	1	110	已失效

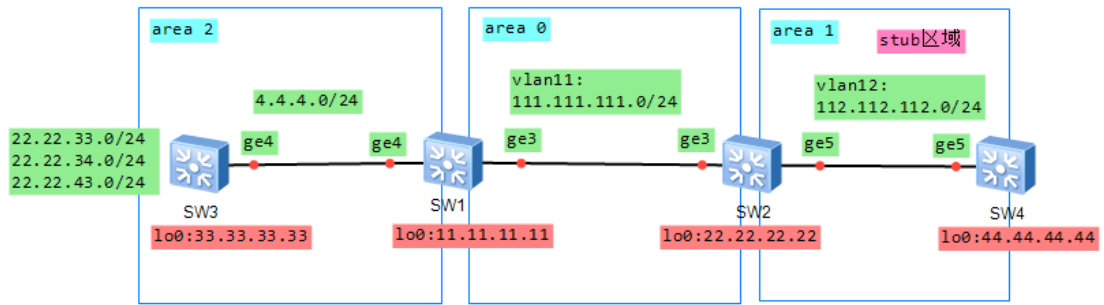
区域 2 能够学习到来自区域 1 中的设备的路由信息，从而实现区域 2 的设备能够与区域 1 的设备互通。（注：1、虚连接不可创建在骨干区域与特殊区域之上。）

5.6. 企业 OSPF 网络中配置特殊区域

场景描述:

企业部署了 OSPF 网络，位于自治系统边缘的非骨干区域的设备性能较差，不能接受大量的 LSA，为了减少负载，过滤掉五类 LSA。可以通过配置特殊区域缩减其路由表规模，减少需要传递的路由信息数量。

网络拓扑:



演示步骤:

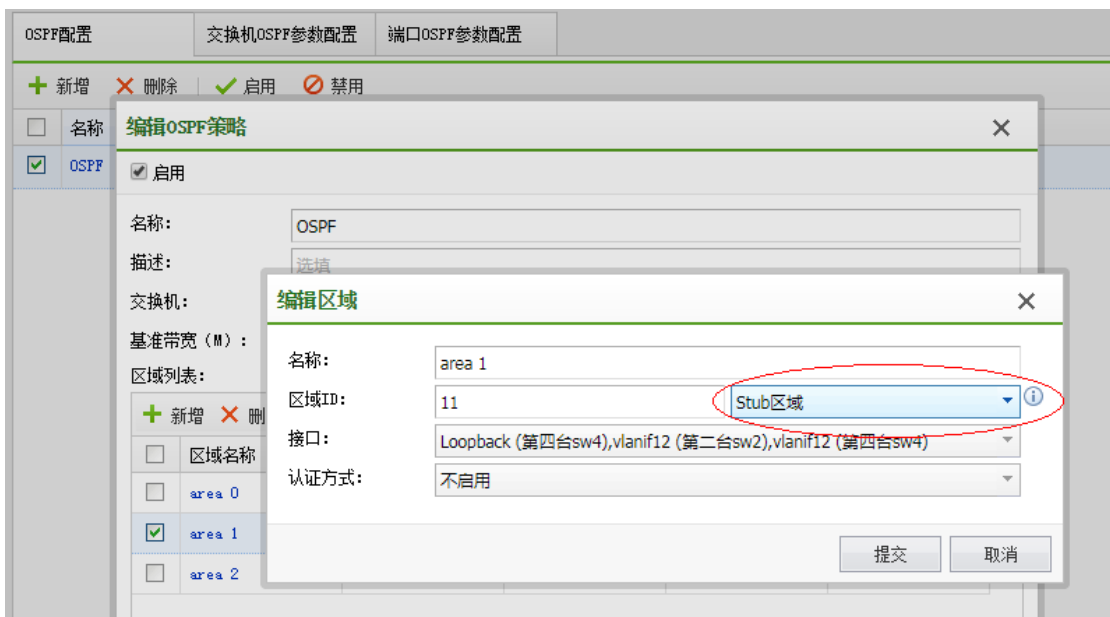
1.环境准备

WAC : 1 台

信锐交换机: 4 台

2.策略配置

(1) 新增 OSPF 策略，配置特殊区域: stub 区域



3.功能验证

第四台sw4-OSPF路由详情 ×

路由标识符: 44.44.44.44

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
22.22.34.0/24	112.112.112.2	vlan12	4	110	正常	
111.111.111.0/24	112.112.112.2	vlan12	2	110	正常	
33.33.33.33/32	112.112.112.2	vlan12	4	110	正常	
0.0.0.0/0	112.112.112.2	vlan12	2	110	正常	
4.4.4.0/24	112.112.112.2	vlan12	3	110	正常	
22.22.22.22/32	112.112.112.2	vlan12	2	110	正常	
11.11.11.11/32	112.112.112.2	vlan12	3	110	正常	
44.44.44.44/32	-	loopback1	1	110	已失效	
22.22.43.0/24	112.112.112.2	vlan12	4	110	正常	
22.22.22.0/24	112.112.112.2	vlan12	4	110	正常	

OSPF历史日志

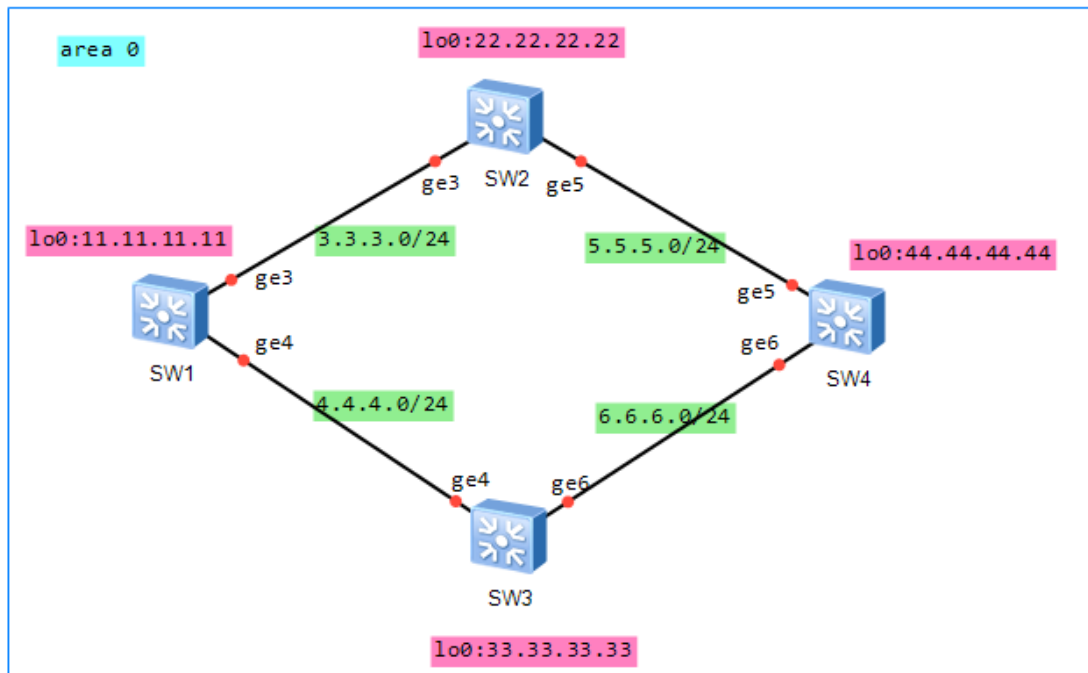
Stub 区域的设备不接受外部五类和四类 LSA，在路由表中会增加一条默认路由以到达外部路由。

5.7. 企业部署 OSPF 网络与 BFD 联动

场景描述:

企业 OSPF 网络动态感知链路变化，快速来进行链路切换。

网络拓扑:



演示步骤:

1.环境准备

WAC : 1 台

信锐交换机: 4 台

2.策略配置

(1) 新增 OSPF 策略;



(2) 在端口 OSPF 参数配置页面, 启用 bfd 检测, SW1 与 SW2 的 ge3 口和 SW2 与 SW3 的 ge5 口配置 BFD;



3. 功 能 验 证

第一台sw1-OSPF路由详情 ×

路由标识符: 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息			
目标地址/掩码	下一跳地址	下一跳接口	度量值	优先级	状态	
3.3.3.0/24	-	ge3	1	110	已失效	
33.33.33.33/32	4.4.4.3	ge4	2	110	正常	
4.4.4.0/24	-	ge4	1	110	已失效	
113.113.113.0/24	4.4.4.3	ge4	2	110	正常	
22.22.22.22/32	3.3.3.2	ge3	2	110	正常	
5.5.5.0/24	3.3.3.2	ge3	2	110	正常	
44.44.44.44/32	4.4.4.3	ge4	3	110	正常	
11.11.11.11/32	-	loopback1	1	110	已失效	
22.22.33.0/24	4.4.4.3	ge4	2	110	正常	

OSPF历史日志

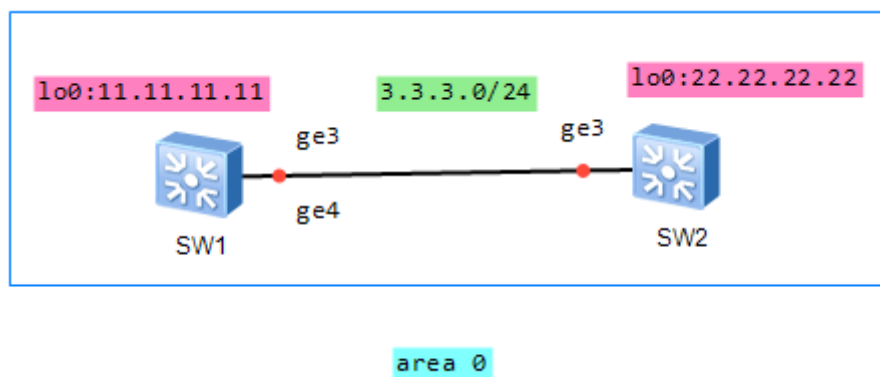
将 SW1 与 SW2 之间的链路断开 SW1 ping SW3 时的链路在快速收敛，切换到 SW4 的链路，SW1 能够正常访问 SW3。

5.8. 企业部署 OSPF 网络，并配置认证方式

场景描述:

对网络安全性要求较高的网络中，企业可以通过配置认证的方式来提高网络拓扑的安全性；提高 OSPF 网络的安全性，防止误接入导致网络震荡。

网络拓扑:



演示步骤:

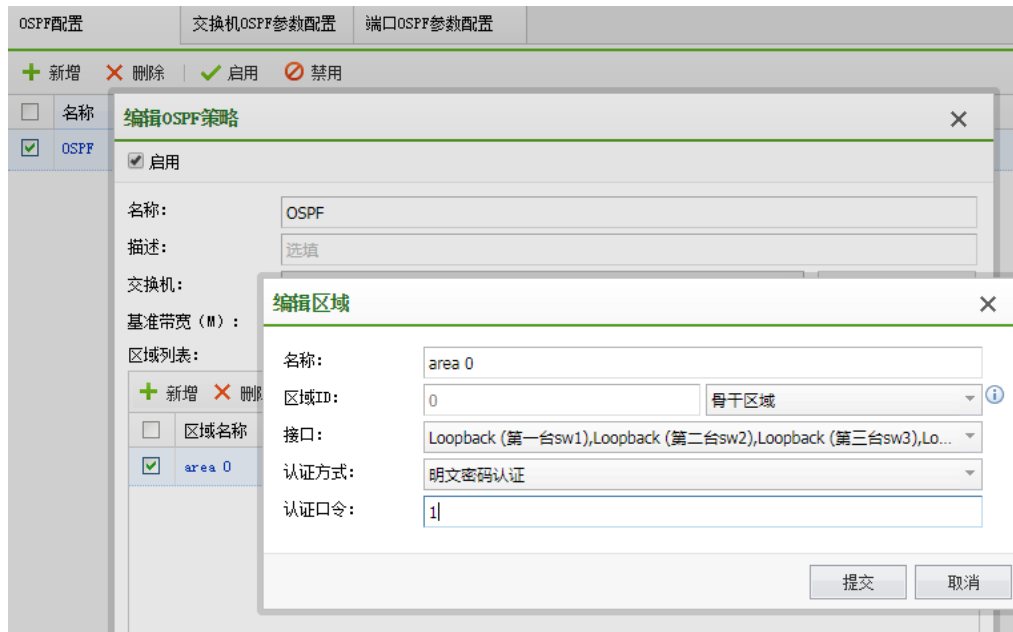
1.环境准备

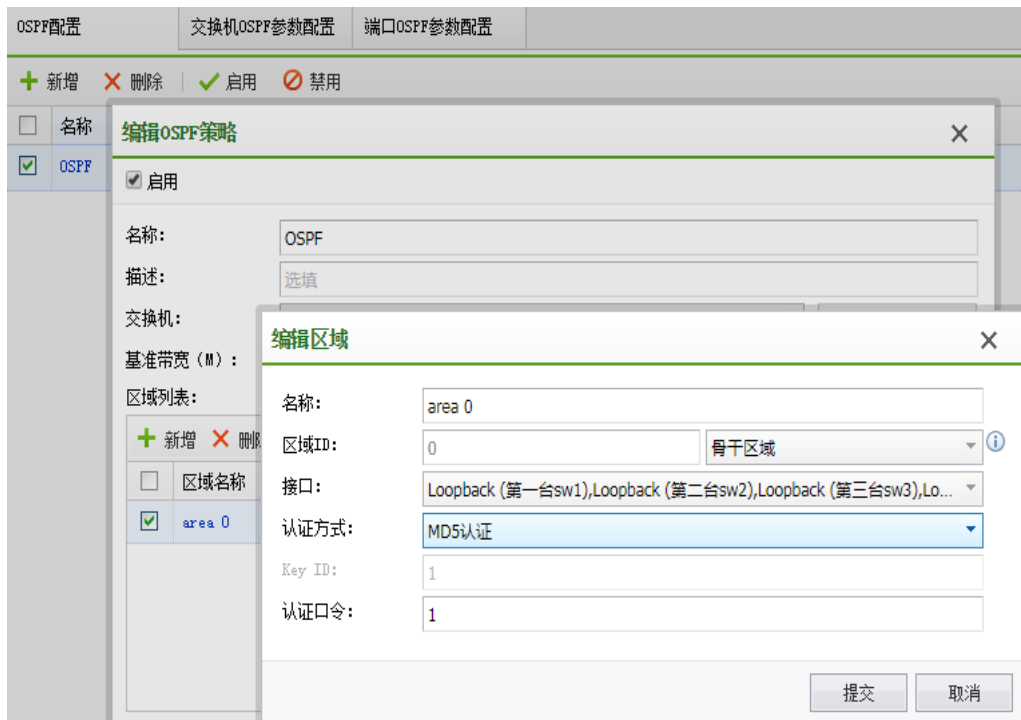
WAC : 1 台

信锐交换机: 2 台

2.策略配置

(1) 新增 OSPF 策略，并配置区域认证方式为明文密码认证或 MD5 认证;





(2) 在端口 OSPF 参数配置页面，配置接口认证方式为明文密码认证或 MD5 认证；



OSPF配置 交换机OSPF参数配置 **端口OSPF参数配置**

批量编辑

<input type="checkbox"/>	名称
<input type="checkbox"/>	Loopback
<input type="checkbox"/>	Loopback
<input type="checkbox"/>	Loopback
<input type="checkbox"/>	Loopback
<input type="checkbox"/>	Loopback
<input type="checkbox"/>	vlanif13
<input type="checkbox"/>	vlanif13
<input checked="" type="checkbox"/>	第二台sw2-port3
<input type="checkbox"/>	第二台sw2-port5
<input type="checkbox"/>	第三台sw3-port4
<input type="checkbox"/>	第三台sw3-port22
<input type="checkbox"/>	第四台sw4-port5
<input checked="" type="checkbox"/>	第一台sw1-port3
<input type="checkbox"/>	第一台sw1-port4

批量编辑

DR选举优先级: 1

接口开销: 自动 10

DD报文检查: 启用DD报文检查MTU值

OSPF报文抑制: 启用OSPF报文抑制

认证方式

认证方式: MD5认证

认证口令: 1

BFD检测

BFD检测: 禁用

定时器

Hello间隔: 10 秒

重传间隔: 5 秒

传输延时: 1 秒

3.功能验证

第一台sw1-OSPF路由详情

路由标识符: 11.11.11.11

OSPF状态	邻接关系	接口信息	路由信息						
接口名称	IP地址	区域	网络类型	度量值	DR选举优先级	邻居状态政...	DR设备	认证方式	状态
loopback1	11.11.11.11...	area 0	Broadcast	1	1	1次	-	不启用	Loopback
ge3	3.3.3.1/24	area 0	Broadcast	1	1	3次	3.3.3.2	明文密码认证	Backup DR
ge4	4.4.4.1/24	area 0	Broadcast	1	1	3次	4.4.4.3	明文密码认证	Backup DR

第一台sw1-OSPF路由详情

X

路由标识符: 11.11.11.11

OSPF状态		邻接关系		接口信息		路由信息			
接口名称	IP地址	区域	网络类型	度量值	DR选举优先级	邻居状态改...	DR设备	认证方式	状态
loopback1	11.11.11.11...	area 0	Broadcast	1	1	1次	-	不启用	Loopback
ge3	3.3.3.1/24	area 0	Broadcast	1	1	3次	3.3.3.2	MDS认证	Backup DR
ge4	4.4.4.1/24	area 0	Broadcast	1	1	3次	4.4.4.3	明文密码认证	Backup DR

区域认证：是将整个区域中运行 OSPF 协议的端口都开启认证，相当于区域认证把所有运行 OSPF 协议接口都开启接口认证，认证方式明文认证及密文认证，明文认证在抓取数据包时可以看到认证字段及明文密码，密文认证在抓取数据包时可以看到认证字段及密文密码。

接口认证：是将开启 OSPF 协议并与设备建立邻居的接口开启认证，是以交换机接口为单位，认证方式同上。

注：

- 1、一台设备既可以开启区域认证与接口认证
- 2、接口认证优先级优于区域认证

5.9. 企业部署 OSPF 网络，其他高级选项功能配置

场景描述：

1.企业 OSPF 网络中可以根据需求，需要将两台邻接设备解除邻接关系，启用 OSPF 报文抑制功能；2.DD 报文检查 MTU 值默认不启用，启用时检测到对端接口发送过来的报文

信息中 MTU 值大于该端口的 MTU 值则建立邻居关系失败；3.当端口报文泛洪时，可以修改 Hello 报文间隔时间，调整端口发送 hello 报文的时间间隔。4.为了加快企业 OSPF 网络的收敛，可以将失效时间间隔调小。

演示步骤：

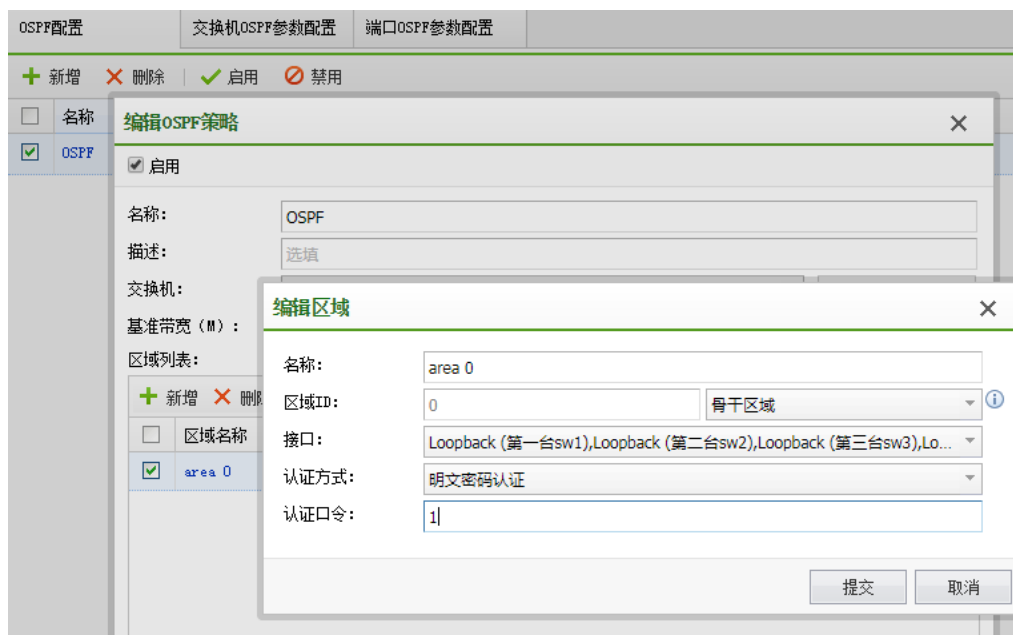
1.环境准备

WAC : 1 台

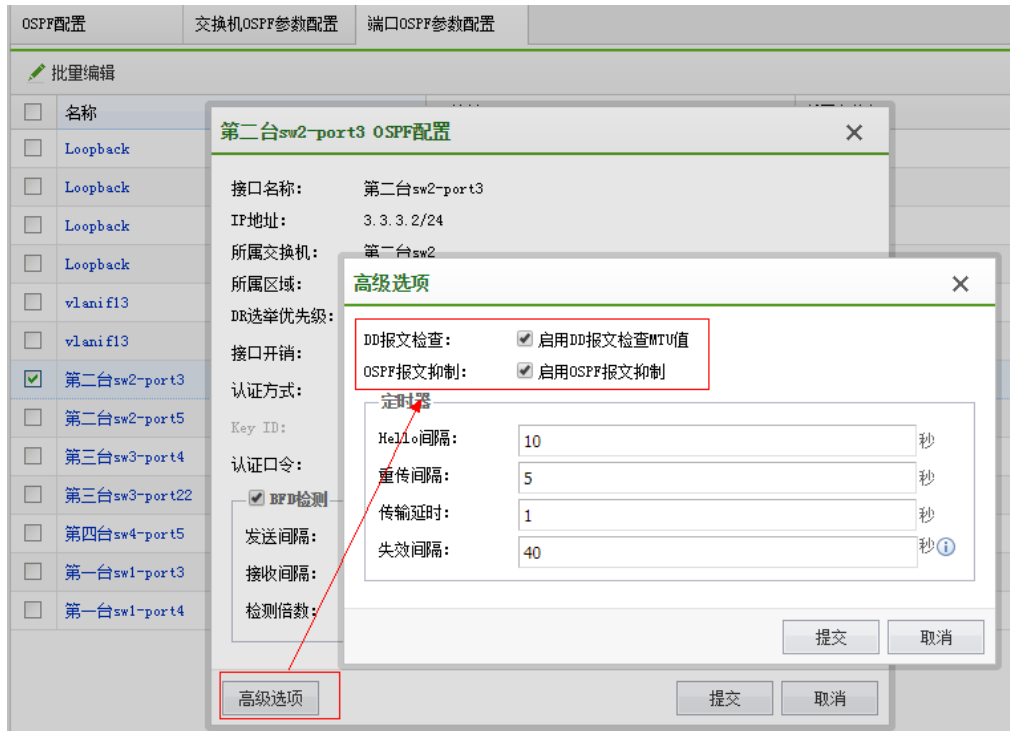
信锐交换机：2 台

2.策略配置

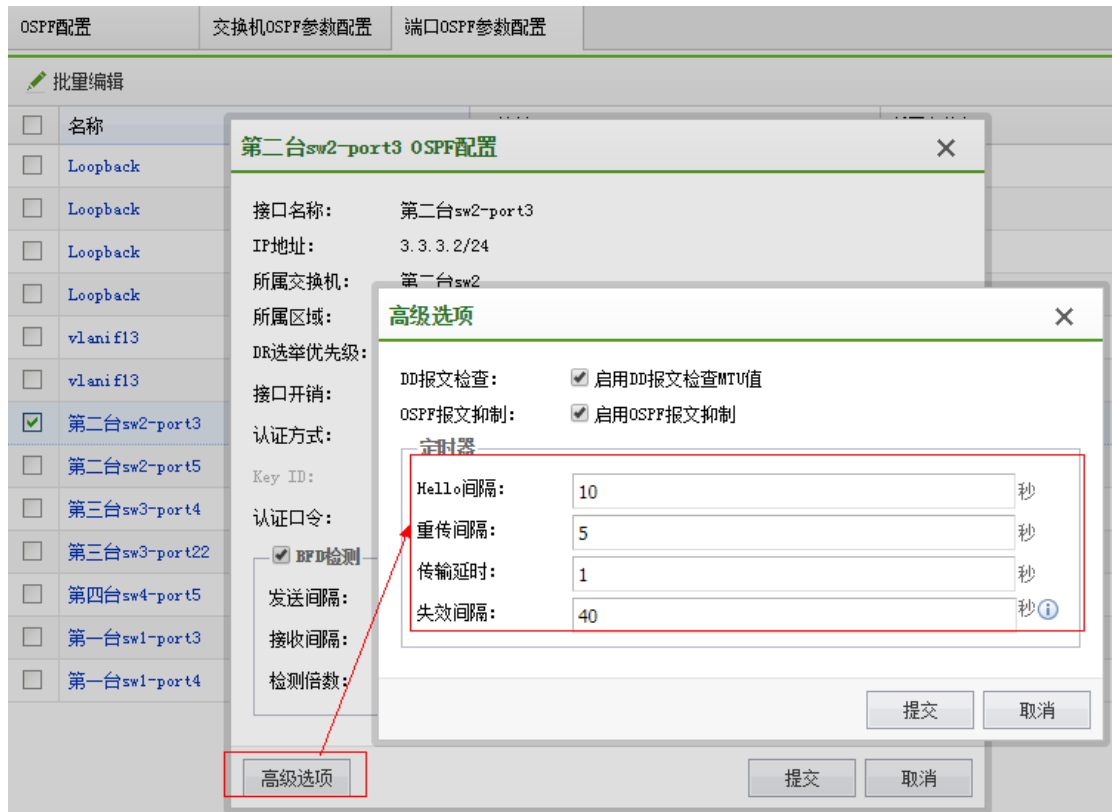
(1) 新增 OSPF 策略：



(2)在端口 OSPF 参数配置页面，接口参数中的高级选项中配置启用 DD 报文检查 MTU 值或启用 OSPF 报文抑制；



(3) 在端口 OSPF 参数配置页面，接口参数中的高级选项中修改定时器的时间；



5.10. 企业部署 OSPF 与 RIP 网络，更改管理距离而更改选路

场景描述：

企业网络中，部署多个协议，且各协议内有相同网段，需要通过更改管理距离而更改选路。

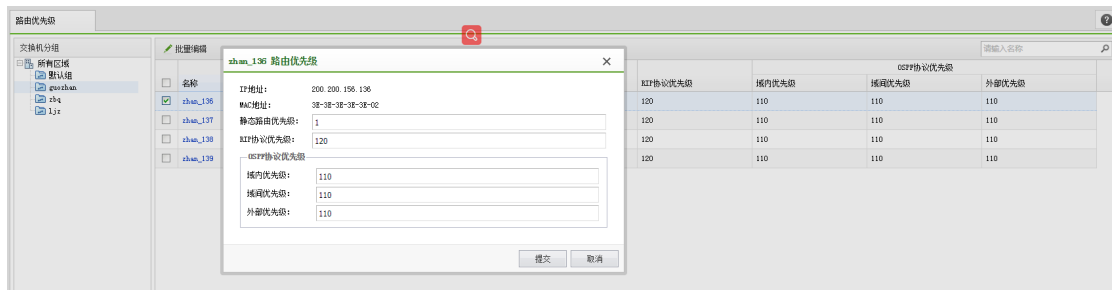
演示步骤：

1.环境准备

WAC : 1 台

信锐交换机: 3 台

2.策略配置



根据需求配置管理距离，管理距离值越小，优先级越高

5.11. 企业部署 OSPF 网络，网络故障进行故障诊断

场景描述：

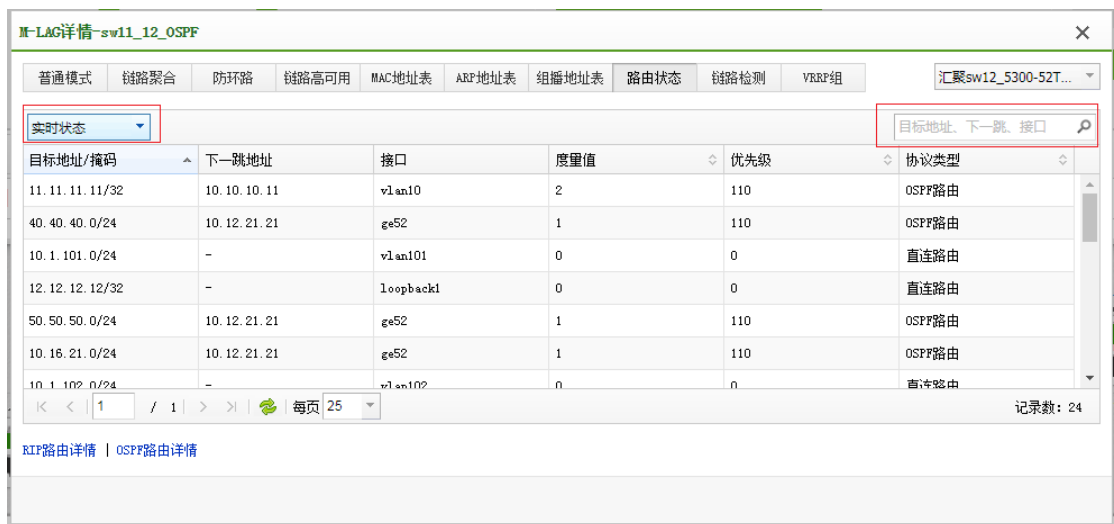
企业 OSPF 网络出现的网络故障，需要进行性故障诊断

功能：

(4) 历史回溯：支持查看某一时刻路由表的学习情况，进而进行诊断当时路由的变化情况



(5) 实时路由表：可查看此时的路由表情况，支持搜索功能



(6) OSPF 路由详情：分为 OSPF 状态、邻接关系、接口信息、路由信息、历史日志。

可查看 OSPF 的相关配置，及历史信息

汇聚sw12_5300-52T_ABR-OSPF路由详情

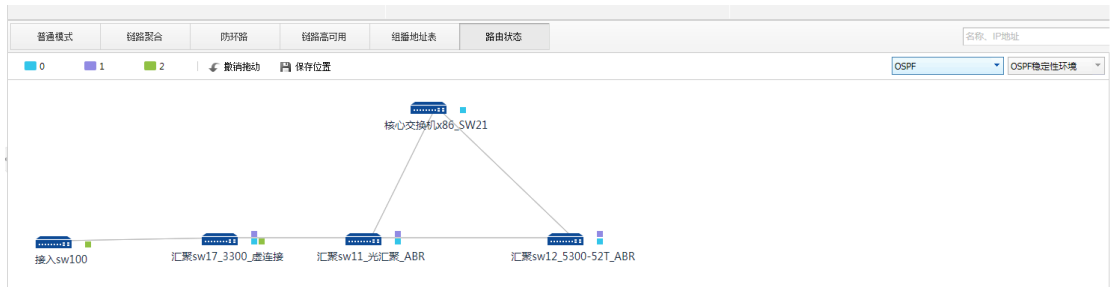
路由标识符: 12.12.12.12

OSPF状态 邻接关系 接口信息 路由信息

区域名称	SPF计算次数:	116次
0	区域边界路由器:	3个
1	自治系统边界路由器:	1个
	Full状态区域边界路由器:	1个

OSPF历史日志

(7) 实时路由拓扑：可查看此时路由拓扑，点击设备可查看相关信息



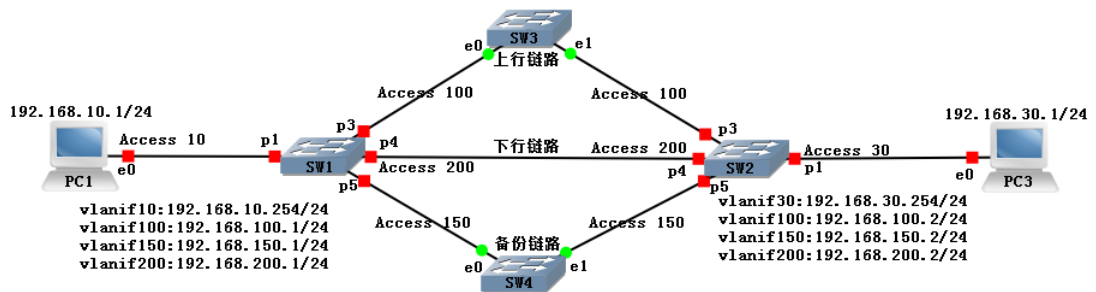
第6章 静态路由

6.1. 企业配置静态路由，进行链路检测

场景描述:

企业配置某条静态路由，检测到链路故障时，会将故障上报系统，促使该路由失效。

网络拓扑:



配置步骤:

- (1) 配置各接口所属 VLAN
- (2) 配置各 VLANIF 接口的 IP 地址
- (3) SW1 上配置默认路由 0.0.0.0/0->192.168.200.2，SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1
- (4) 在上行链路上新建系统三层 BFD 链路检测 LinkDetect1
- (5) SW1 新建静态路由 192.168.30.0/24->192.168.100.2，启用链路检测，引用 LinkDetect1;



功能验证:

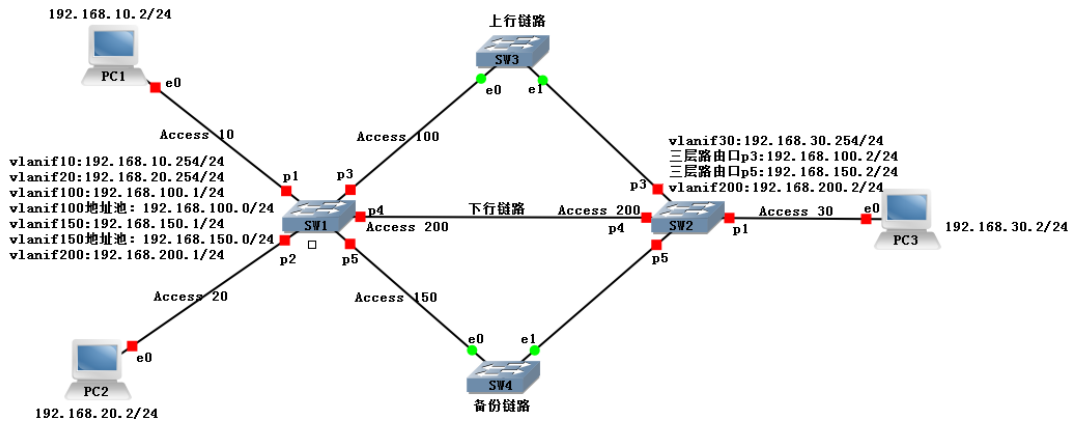
- (1) 在 SW2 上的 p3 可以抓到源 ip 为 192.168.10.1 的数据流;
- (2) SW1 的 BFD 状态为 up、SW1 的 BFD 状态为 up, 且 SW2 的 p3 可以抓到源 ip 为 192.168.10.1 的数据流及来自 PC2 的回复报文。

6.2. 企业对三层核心交换机进行路由备份，提高网络可靠性

场景描述:

某企业存在多个部门，每个部门分别从不同的交换机接入网络，希望通过配置两条不等价的静态路由可以实现主备份，当主用链路故障的时候流量切换到备用链路上。

网络拓扑:



拓扑说明:

PC1 和 PC3 通过 4 台 Switch 相连, 从拓扑图中可以看出, 数据从 PC1 到 PC3 有两条路径可以到达, 分别是 PC1-SW1-SW3-SW2-PC2 和 PC1-SW1-SW4-SW2-PC2, 用户希望要求从 PC1 到 PC2 的数据流实现主备备份, 即优先走经过 SW3 的这条路径, 当这条路径故障的时候流量自动切换到经过 SW2 的这条路径。

操作步骤:

5.配置各接口所属 VLAN

6.配置各 VLANIF 接口的 IP 地址

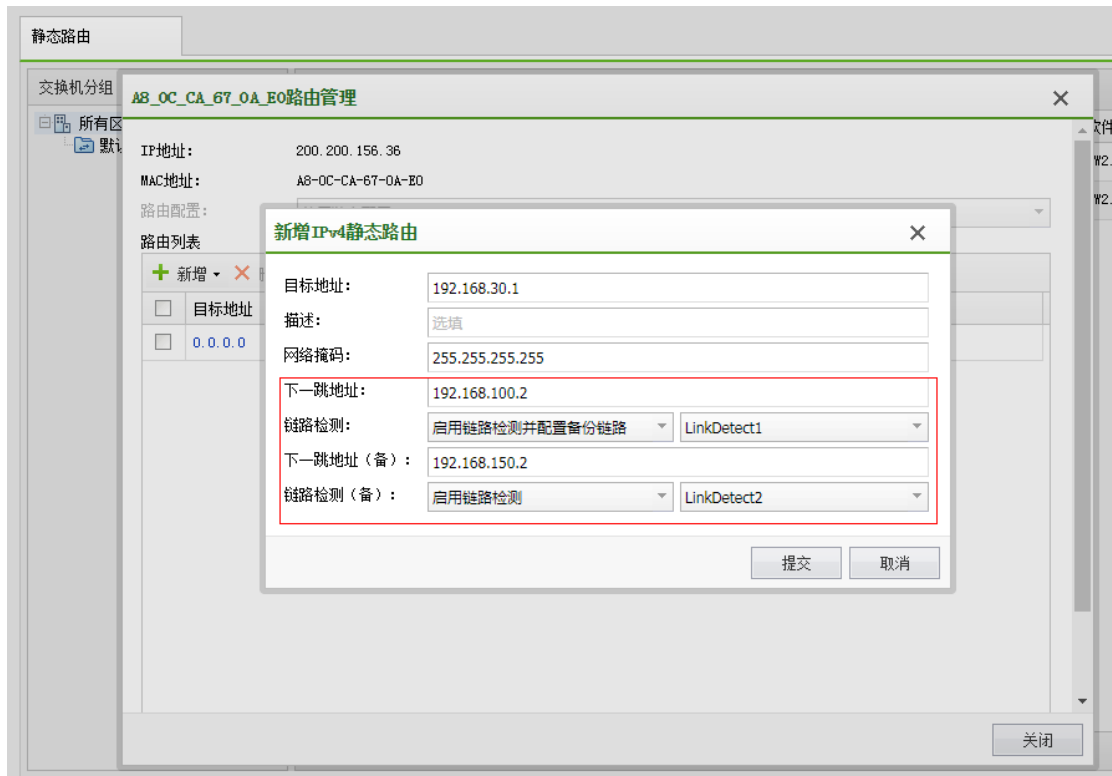
7.新建 BFD 链路检测 LinkDetect1,

SW1->p3, 192.168.100.1, SW2->p3, 192.168.100.2;

新建 BFD 链路检测 LinkDetect2,

SW1->p5, 192.168.150.1, SW2->p5, 192.168.150.2;

8.配置 PC1 - PC2 的去程的静态路由 192.168.30.1/255.255.255.255，下一跳地址为 192.168.100.2，启用链路检测并配置备份链路，引用 LinkDetect1，下一跳地址（备）为 192.168.150.2，启用链路检测，引用 LinkDetect2；



功能验证：

- (1) p3 的 BFD 会话断开，PC1 能 ping 通 PC3，p5 上能抓到 PC1 的 ICMP 包；
- (2) PC1 不能 ping 通 PC3，p4 上抓不到 PC1 的 ICMP 包；
- (3) PC1 能 ping 通 PC3，p5 上能抓到 PC1 的 ICMP 包；
- (4) p3 的 BFD 会话恢复，PC1 能 ping 通 PC3，p3 上能抓到 PC1 的 ICMP 包；

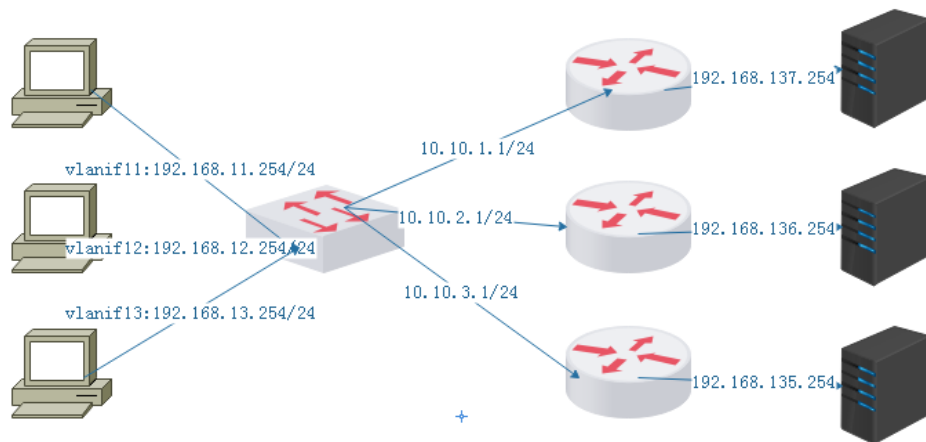
第7章 策略路由

7.1. 企业希望通过策略路由为不同的部门划分不同的服务器

场景描述:

企业有两个出口线路，需要通过策略路由实现内网部分电脑固定从某一个出口线路上网，另外一部分电脑固定从另外一个出口线路上网，此时可以在路由器上启用策略路由功能。

网络拓扑:



拓扑说明:

PC1 与 PC2 访问 PC3,分别通过上行链路和下行链路不同链路访问外网。

操作步骤:

- (1) 配置各接口所属 VLAN
- (2) 配置各 VLANIF 接口的 IP 地址

(3) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2, SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1 和 192.168.20.0/24->192.168.200.1

优先级	名称	高于/低于静态路由	下一跳地址	描述
<input checked="" type="checkbox"/>	1	部门13	高于静态路由	10.10.3.1
<input type="checkbox"/>	2	部门12	高于静态路由	10.10.2.1
<input checked="" type="checkbox"/>	3	部门11	高于静态路由	10.10.1.1

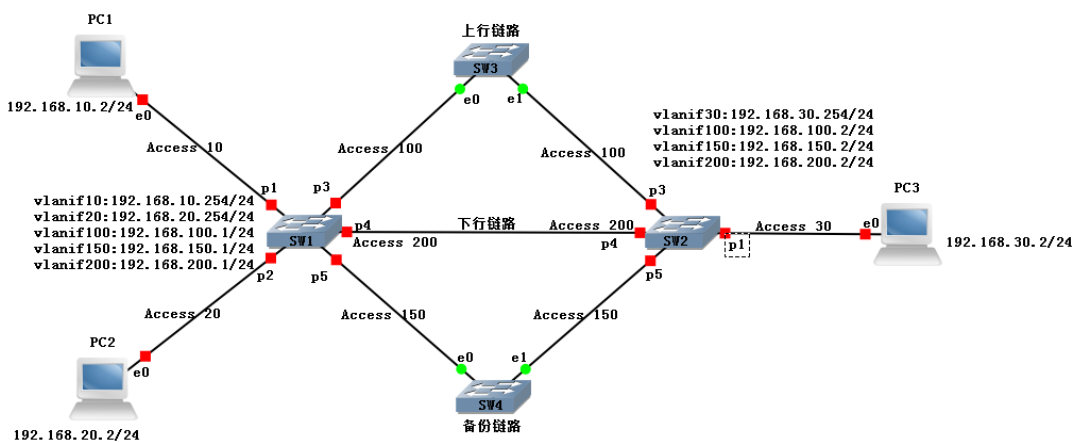
(4) SW1 新建策略路由，入接口类型为三层路由口，引用三层路由口 p1，源 IP 为 192.168.10.1/255.255.255.255，下一跳为 192.168.100.2，协议为 ICMP，不启用链路检测；

7.2. 企业部署策略路由，并希望主链路配置故障后切换到备份链路

场景描述：

企业希望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。

网络拓扑：



配置步骤：

- (1) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见附件
- (2) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2，SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1 和 192.168.20.0/24 ->192.168.200.1
- (3) 新建 BFD 链路检测 LinkDetect1，选择 SW1 的 p3、地址 192.168.100.1 和 SW2 的 p3、地址 192.168.100.2
- (4) SW1 新建策略路由，入接口类型为 vlanif 口，引用 vlanif 口 p1，源 IP 为 192.168.10.1/255.255.255.255，协议为 ICMP，主下一跳为 192.168.100.2，备下一跳为 192.168.150.2，启用链路检测（主），引用 LinkDetect1，不启用链路检测（备）；

策略路由

+ 新增 × 删除 | ✓ 启用 ⊘ 禁用 | ↑ 上移 ↓ 下移 ↔ 移动到

优先级
 1

新增策略路由
×

启用

名称:
 描述:
 交换机:
 入接口:
 规则:

+ 新增 × 删除 | ✓ 启用 ⊘ 禁用 | ↑ 上移 ↓ 下移

匹配条件

🔍 >>

	优...	源IP地址	目的IP地址	协议	动作	状态	操作
<input type="checkbox"/>	1	192.168.10.1/255.2...		ICMP	路由	✓	✎

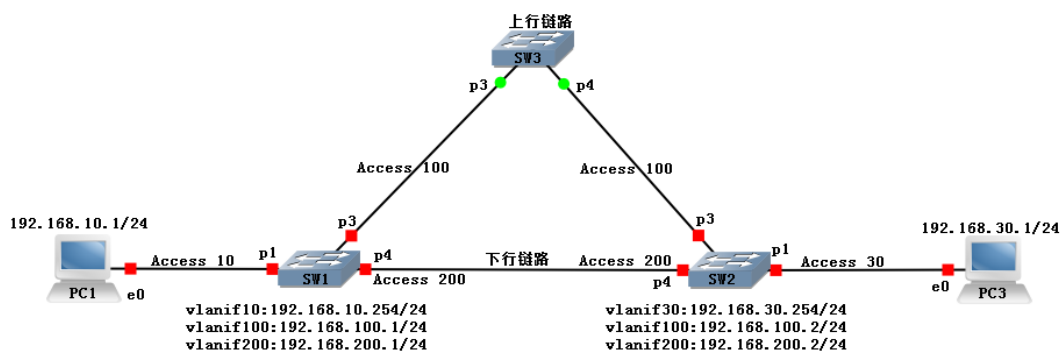
下一跳地址:
 链路检测:
 下一跳地址(备):
 链路检测(备):
 路由优先级:

7.3. 网络管理员部署策略路由根据不同用户控制可访问的网站

场景描述:

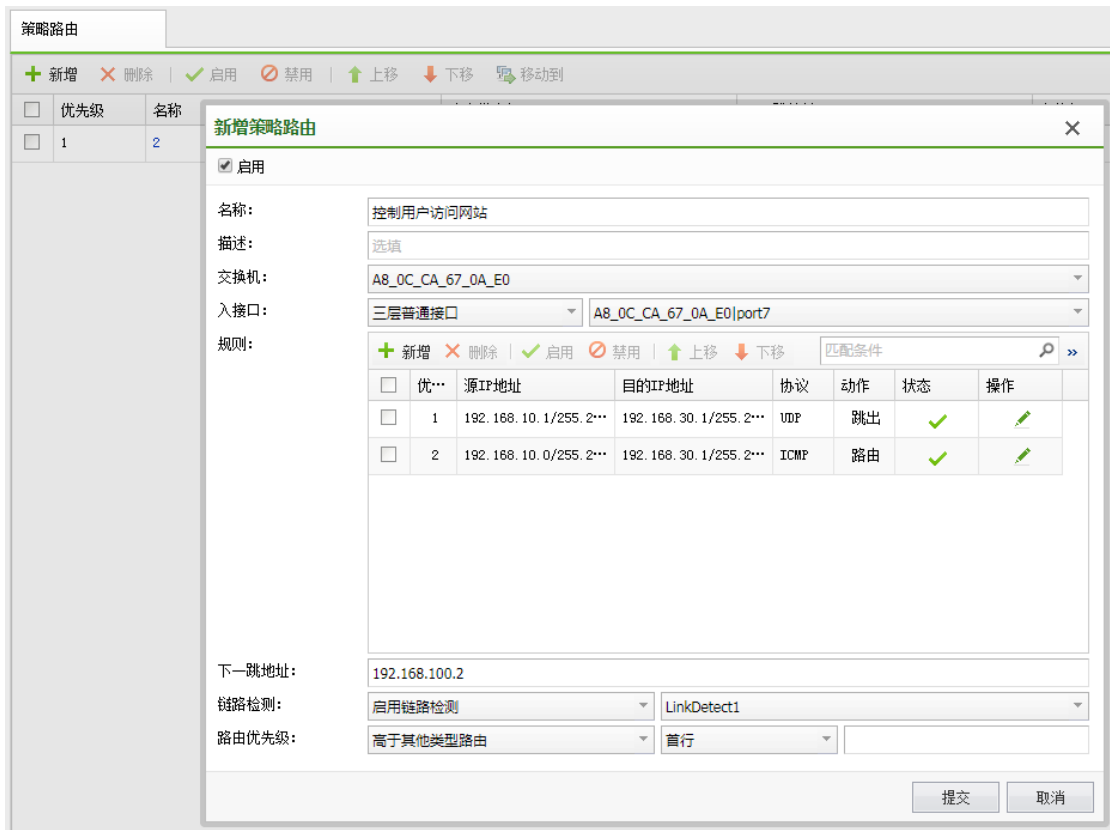
网络管理员希望能够通过部署策略路由根据不同用户控制可访问的网站;

网 络 拓 扑 :



配置步骤:

- (1) SW1,2 根据拓扑图划分 vlan, 所有设备的 IP 地址配置见拓扑图;
 - (2) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2,
SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1;
 - (3)新建 BFD 链路检测 LinkDetect1, SW1->p3、192.168.100.1, SW2->p3、192.168.100.2;
 - (4) SW1 新建策略路由 1, 入接口类型为 vlanif 口, 引用 vlanif10, 源 IP192.168.10.1/255.255.255.255,目的 IP192.168.30.1/255.255.255.255,协议 UDP,动作跳出;
源 IP192.168.10.0/255.255.255.0, 目的 IP192.168.30.1/255.255.255.255, 协议 ICMP, 动作路由;
- 下一跳为 192.168.100.2, 启用链路检测, 引用 LinkDetect1;

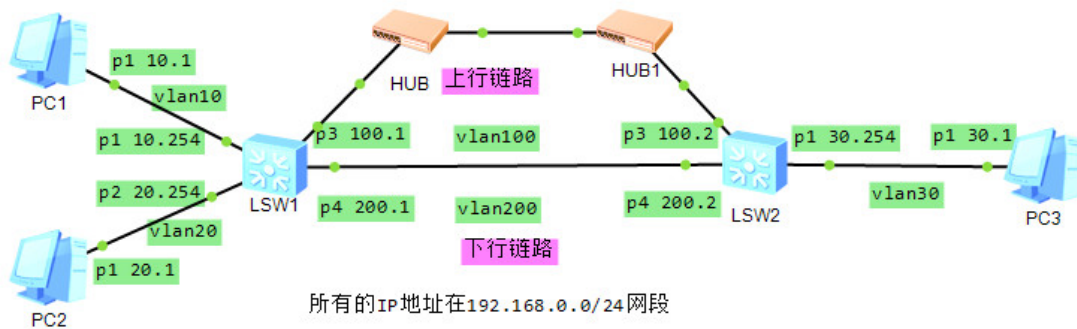


7.4. 用户策略路由链路故障切换到静态路由，链路恢复后切回策略路由

场景描述:

用户策略路由链路故障切换到静态路由，链路恢复后切回策略路由

网络拓扑:



配置步骤:

- 1.SW1,2 根据拓扑图划分 vlan, 所有设备的 IP 地址配置见拓扑图;
- 2.SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2, SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1 和 192.168.20.0/24 ->192.168.200.1;
- 3.新建 BFD 链路检测 LinkDetect1, 选择 SW1 的 p3、地址 192.168.100.1 和 SW2 的 p3、地址 192.168.100.2;
- 4.SW1 新建策略路由, 入接口类型为 vlanif 口, 引用 vlanif 口 p1, 源 IP 为 192.168.10.1/255.255.255.255, 下一跳为 192.168.100.2, 协议为 ICMP, 启用链路检测, 引用 LinkDetect1;

编辑策略路由 ✕

启用

名称:

描述:

交换机:

入接口:

规则:

+ 新增 ✕ 删除 | ✓ 启用 ⊘ 禁用 | ↑ 上移 ↓ 下移

<input type="checkbox"/>	优...	源IP地址	目的IP地址	协议	动作	状态	操作
<input type="checkbox"/>	1		192.168.135.254/25...	不限	路由	✓	✎

下一跳地址:

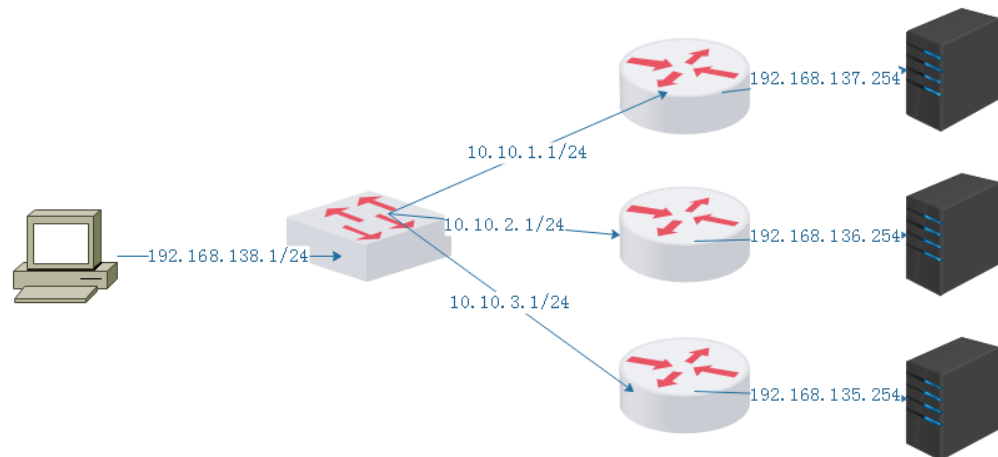
链路检测:

7.5. 用户希望将不同优先级的流量送往不同的服务器

场景描述:

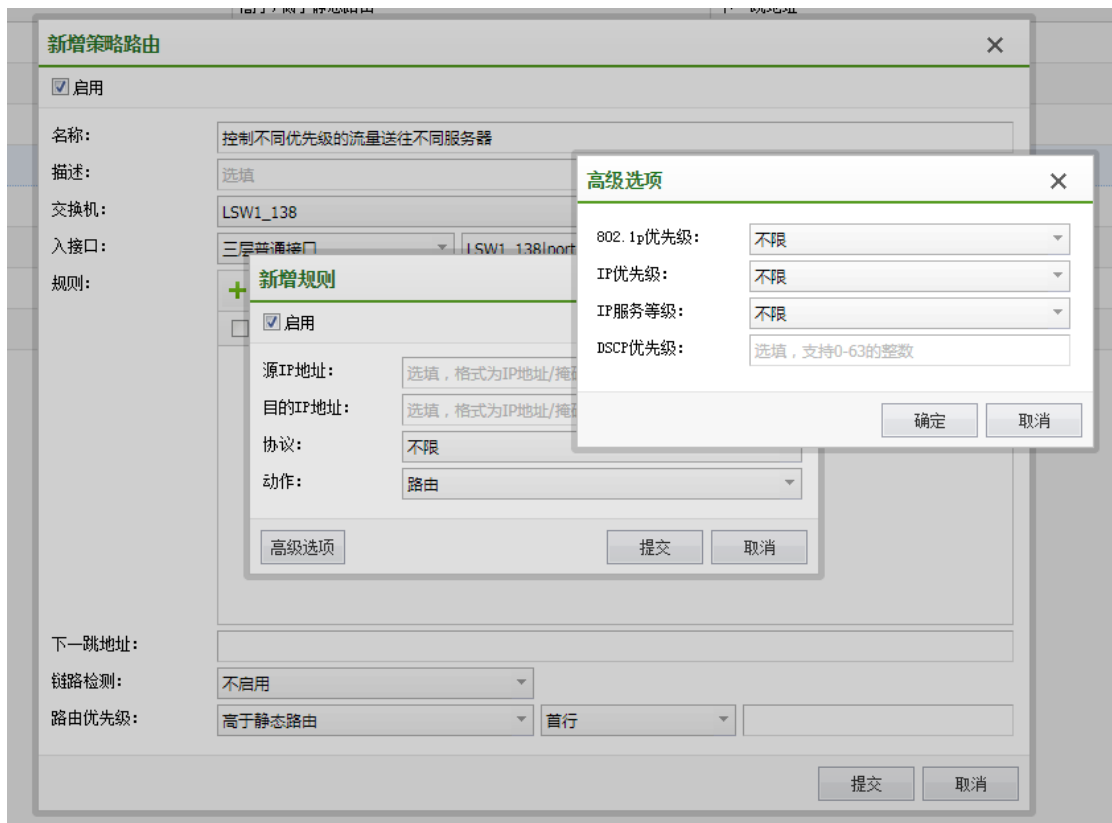
在某些需要指定特定的数据流走特定的下一跳的场景下可以使用策略路由实现,例如使不同的数据流通过不同的链路进行发送,提高链路的利用效率。

网络拓扑:



配置步骤:

- (1) 配置各接口所属 VLAN;
- (2) 配置各 VLANIF 接口的 IP 地址, 静态路由;
- (3) 进入策略路由页面, 配置 ACL 规则并配置高级选项以匹配不同优先级流量, 配置相应的下一跳地址。

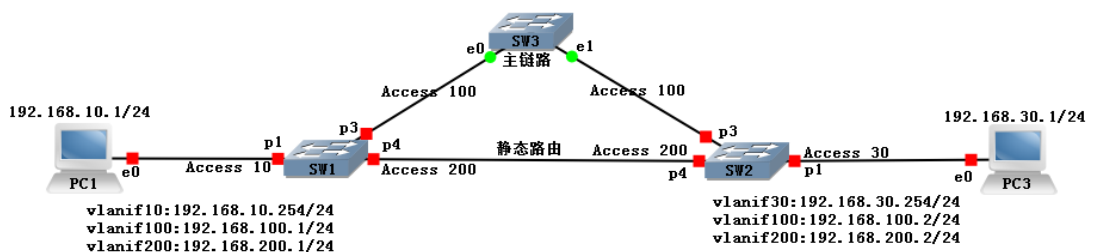


第8章 链路检测

8.1. 用户希望检测交换机到某一 IP 间的多跳三层链路是否正常，且对检测实时性要求不高

场景描述：

网络拓扑：



配置步骤：

(1) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见附件

(2) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2;

SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1;

(3) 新增 PING 链路检测 LinkDetect1，PING IP 地址为 192.168.100.2，提交保存；

新增PING检测

启用

名称: LinkDetect1

描述: 选填

交换机: /所有区域/默认组/A8_0C_CA_67_0A_E0

PING IP地址: 192.168.100.2

检测间隔: 10 秒

故障判断: 3 次

提交 取消

(4) SW1 新建策略路由 EmerRoute，入接口类型为 vlanif 口，引用 vlanif10，源 IP 为 192.168.10.1/32，下一跳为 192.168.100.2，协议为 ICMP，启用链路检测，引用 LinkDetect1；

功能验证：

- (1) 配置下发成功，PC1 能 ping 通 PC3，p4 上能抓到 PC1 的 ICMP 请求包；
- (2) 配置下发成功，PC1 能 ping 通 PC3，p3 上能抓到 PC1 的 ICMP 请求包；
- (3) 断开 SW3 和 SW2 之间的链路之后，21-30s 后 p4 上才能抓到 PC1 的 ICMP 请求包；恢复之后，1-10s 后 p3 上才能抓到 PC1 的 ICMP 请求包；

新增策略路由

启用

名称: EmerRoute

描述: 选填

交换机: A8_OC_CA_67_0A_E0

入接口: vlanif10(192.168.10.1)

规则:

+ 新增 × 删除 | ✓ 启用 ⚡ 禁用 | ↑ 上移 ↓ 下移 匹配条件 🔍 >>

<input type="checkbox"/>	优...	源IP地址	目的IP地址	协议	动作	状态	操作
<input type="checkbox"/>	1	192.168.10.1/255.255.255		ICMP	路由	✓	✎

下一跳地址: 192.168.100.2

链路检测: 启用链路检测 LinkDetect1

路由优先级: 高于其他类型路由 首行

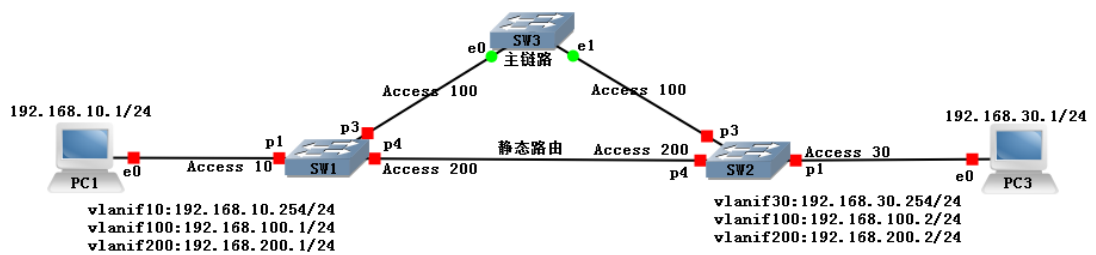
提交 取消

8.2. 管理员希望检测两台交换机间的二层链路是否正常

场景描述:

用户希望配置二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。

网络拓扑:



配置步骤:

- (1) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见附件
- (2) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2;
- SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1
- (3) 新增 BFD 链路检测 LinkDetect1，检测类型为系统二层检测，选择 SW1->p3 和 SW2->p3，提交保存;
- (4) SW1 新建策略路由 EmerRoute，入接口类型为 vlanif 口，引用 vlanif10，源 IP 为 192.168.10.1/32，协议为 ICMP，下一跳为 192.168.100.2，启用链路检测，引用 LinkDetect1;

功能验证:

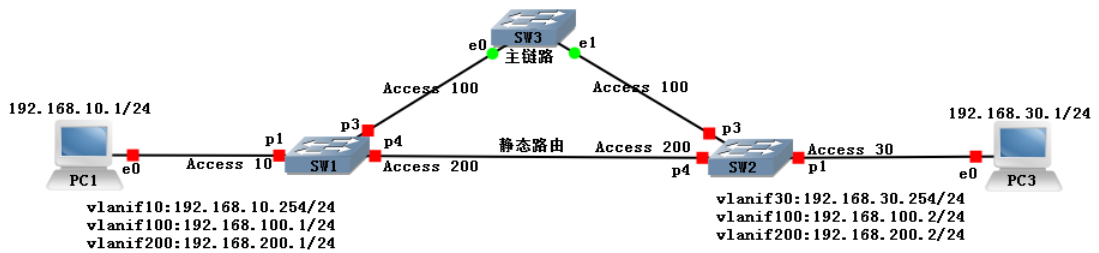
- (1) 端口 p3 已建立 BFD 会话，p3 上能抓到 BFD 控制报文;
- (2) PC1 能 ping 通 PC3，p3 上能抓到 PC1 的 ICMP 请求包;
- (3) BFD 会话断开，p4 上能抓到 PC1 的 ICMP 请求包，p3 上抓不到 BFD 控制报文;

8.3. 用户希望检测两台交换机间的三层链路，且对实时性要求较高

场景描述:

用户希望检测两台交换机间的三层链路，且对实时性要求较高。

网络拓扑:



配置步骤:

(1) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见拓扑图；

(2) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2；

SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1；

(3) 新增系统三层链路检测 LinkDetect1，手动指定标识符，主动协商，

交换机 1 选择 SW1，标识符=111，IP=192.168.100.1，

交换机 2 选择 SW2，标识符=222，IP=192.168.100.2；

(4) SW1 新建策略路由 EmerRoute，入接口类型为 vlanif 口，引用 vlanif10，源 IP 为 192.168.10.1/32，协议为 ICMP，下一跳为 192.168.100.2，启用链路检测，引用 LinkDetect1；

功能验证:

- (1) 端口 p3 建立 BFD 会话，p3 上能抓到 BFD 控制报文；
- (2) PC1 能 ping 通 PC3，p3 上能抓到 PC1 的 ICMP 请求包；
- (3) BFD 会话断开，p4 上能抓到 PC1 的 ICMP 请求包，p3 上抓不到 BFD 控制报文；

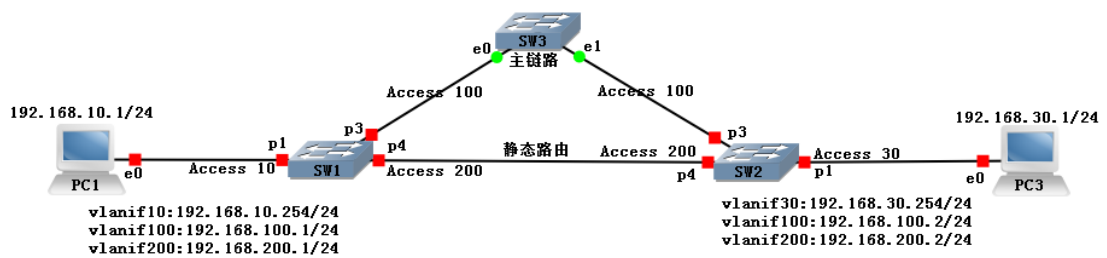
8.4. 管理员希望检测交换机与不支持 BFD 协议设备间的直连三层链路，且对实时性要求较高

场景描述:

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，只支持基本的网络层转发。为了能够快速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。

网络拓扑:



配置步骤:

(5) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见拓扑图；

(6) SW1 上配置静态路由 192.168.30.0/24 ->192.168.200.2；

SW2 上配置静态路由 192.168.10.0/24 ->192.168.200.1；

(7) 新增 BFD 检测，检测类型为单臂回声检测，本端设备选择 SW1,IP 地址选择 192.168.10.1/32，对端 IP 地址 192.168.100.2，提交保存；



(8) SW1 新建策略路由 EmerRoute，入接口类型为 vlanif 口，引用 vlanif10，源 IP 为 192.168.10.1/32，下一跳为 192.168.100.2，协议为 ICMP，启用链路检测，引用 LinkDetect1；

功能验证：

3.端口 p3 的 BFD 会话状态为 Down，p3 上能抓到 BFD 控制报文；

4.配置下发成功，BFD 会话状态为 Up，PC1 能 ping 通 PC3，p3 上能抓到 PC1 的 ICMP 请求包和 BFD 回显报文

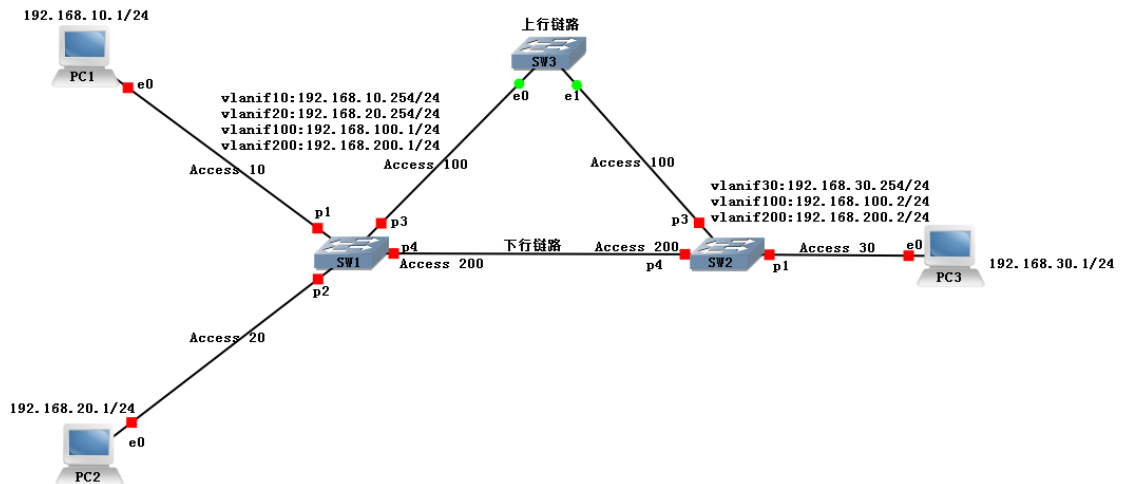
8.5. 用户希望通过链路检测来检查链路间的网络动荡

场景描述：

用户可以根据网络的实际状况增大或者降低设备的本端检测倍数、最短接收间隔或最短发送间隔，以调整 BFD 检测时间。对于不太稳定的链路，如果 BFD 检测时间较小，则 BFD 会话可能会发生震荡，这时可以选择调大 BFD 检测时间。通常情况下，建议使用缺省值，

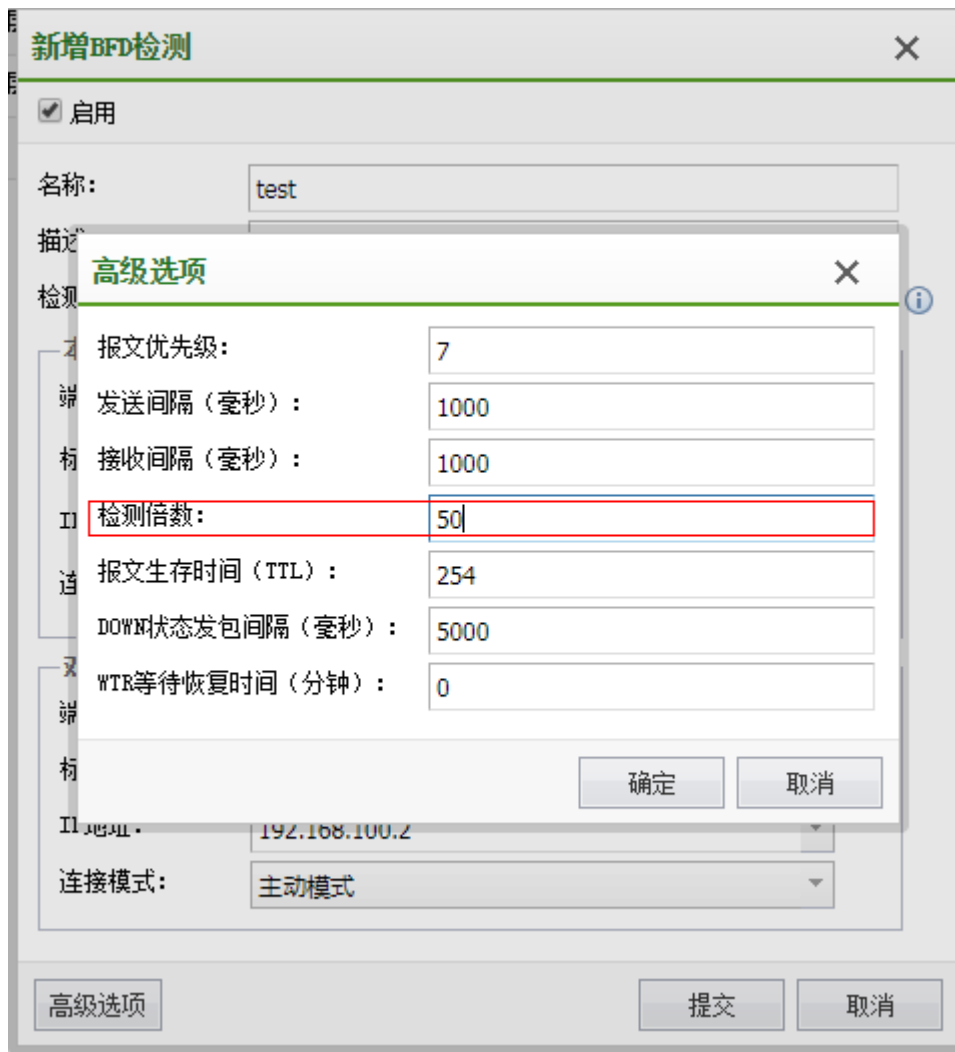
不随意修改本端检测倍数、最短接收间隔和最短发送间隔。

网络拓扑:



配置步骤:

- (1) SW1,2 根据拓扑图划分 vlan，所有设备的 IP 地址配置见附件
- (2) 新增 BFD 链路检测 LinkDetect1，检测类型为系统二层检测，选择 SW1 的 p3 和 SW2 的 p3，异步模式，提交保存；
- (3) 编辑链路检测 LinkDetect1，在高级选项中将检测倍数改为 50，提交保存；



功能验证:

- (1) LinkDetect1 检测到链路 Up, 断开链路 30ms 后, LinkDetect1 检测到链路 Down;
- (2) LinkDetect1 检测到链路 Up, 断开链路 500ms 后, LinkDetect1 检测到链路 Down;

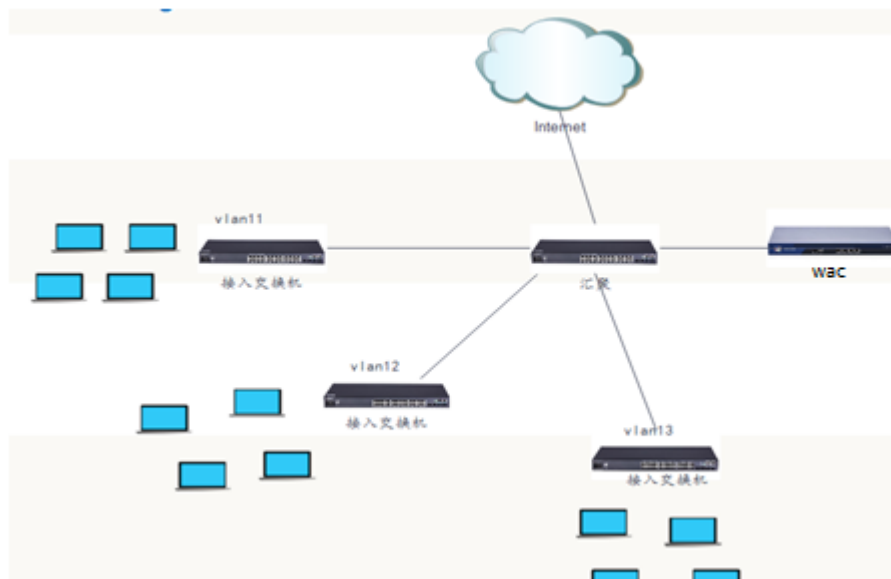
第9章 RIP 配置

9.1. 企业快速配置 RIP 网络实现设备间网络互通

场景描述:

某企业存在研发、财务和客服三个部门，每个部门分属不同的 vlan，各 vlan 间不能互相访问，将各个 vlan 接口加入 RIP 策略区域中，即可实现，研发、财务和客服部门之间可以跨三层互相访问。

网络拓扑:



拓扑说明:

研发、财务和客服分别属于 vlan 11、vlan 12 和 vlan 13。

演示步骤:

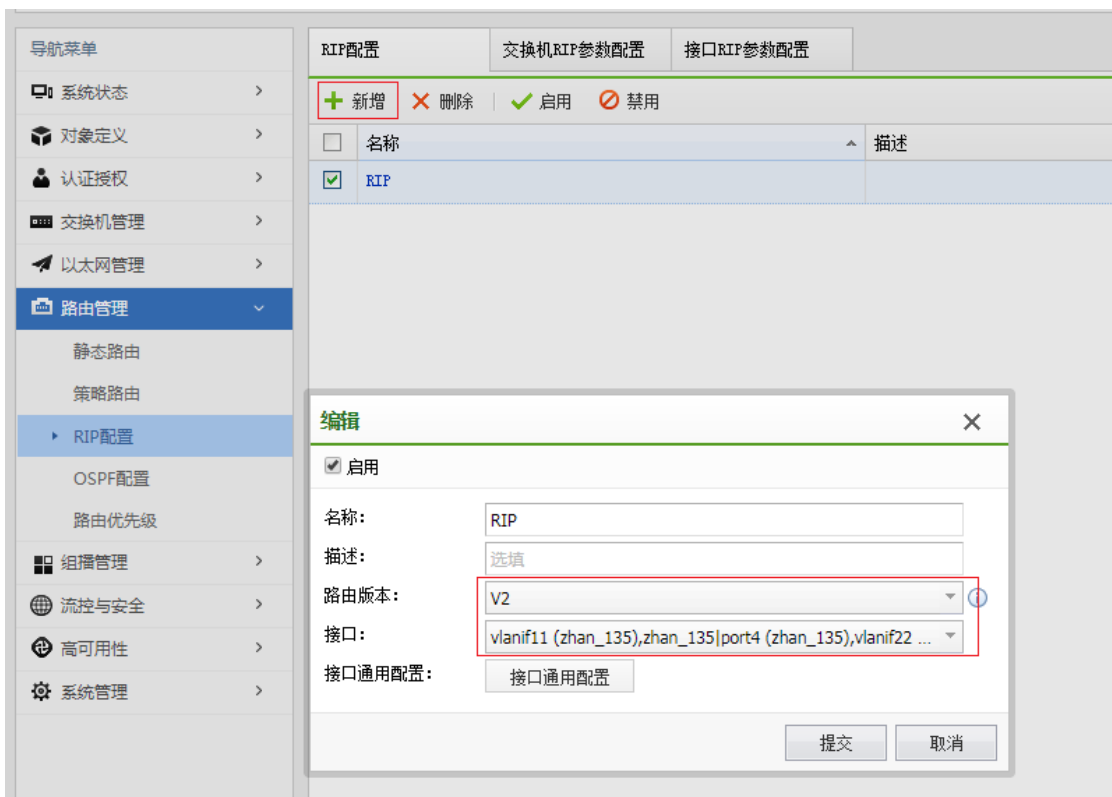
1.环境准备:

WAC: 1 台

信锐交换机: 3 台

2.策略配置

(1) 新增 RIP 策略，选择 v2，并选择对应的 vlan 接口和邻接关系协商口通告到 RIP 中；（v2 是 v1 加强版，无特殊需要，建议使用 v2）



3.功能验证

交换机详情 - zhan_137

普通模式 链路聚合 防环路 链路高可用 MAC地址表 ARP地址表 组播地址表 路由状态 链路检测 VRRP组

实时状态 目标地址、下一跳、接口

目标地址/掩码	下一跳地址	接口	度量值	优先级	协议类型
33.33.33.0/24	-	vlan33	0	0	直连路由
22.22.22.0/24	10.1.23.2	ge24	2	120	RIP路由
11.11.11.0/24	10.1.23.2	ge24	3	120	RIP路由
200.200.156.0/22	-	vlan1	0	0	直连路由
10.1.23.0/24	-	ge24	0	0	直连路由
0.0.0.0/0	200.200.159.254	-	0	1	静态路由
10.1.12.0/24	10.1.23.2	ge24	2	120	RIP路由

每页 25 记录数: 7

[RIP路由详情](#) | [OSPF路由详情](#)

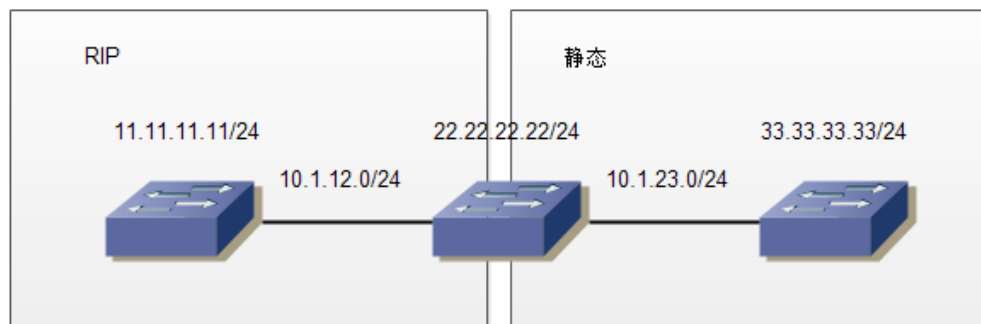
设备的不同 vlan 之间可以查看到路由信息，并且能够互访

9.2. 企业 RIP 网络引入外部路由(路由引入)

场景描述:

某企业网络中使用了 RIPv2 和静态路由协议。企业希望实现 RIP 区域设备与静态路由设备之间的互通，可以在交换机 RIP 配置中也引入静态路由，从而实现 RIP 区域与静态路由设备之间的互通。路由引入包括直连路由、OSPF 路由、静态路由、默认路由。

网络拓扑:



演示步骤:

1.环境准备:

WAC: 1 台

信锐交换机: 三台

2.策略配置:

(1) 在交换机 RIP 参数配置页面，在配置了静态路由的设备上配置静态路由引入；



3.功能验证:

4.未引入之前的现象:

交换机详情-zhan_135

普通模式 链路聚合 防环路 链路高可用 MAC地址表 ARP地址表 组播地址表 路由状态 链路检测 VRRP组

实时状态 目标地址、下一跳、接口

目标地址/掩码	下一跳地址	接口	度量值	优先级	协议类型
10.1.12.0/24	-	ge4	0	0	直连路由
200.200.156.0/22	-	vlan1	0	0	直连路由
11.11.11.0/24	-	vlan11	0	0	直连路由
22.22.22.0/24	10.1.12.2	ge4	2	120	RIP路由
0.0.0.0/0	200.200.159.254	-	0	1	静态路由
10.1.23.0/24	10.1.12.2	ge4	2	120	RIP路由

1 / 1 每页 25 记录数: 6

[RIP路由详情](#) | [OSPF路由详情](#)

(2) 引入之后的现象:

交换机详情-zhan_135

普通模式 链路聚合 防环路 链路高可用 MAC地址表 ARP地址表 组播地址表 路由状态 链路检测 VRRP组

实时状态 目标地址、下一跳、接口

目标地址/掩码	下一跳地址	接口	度量值	优先级	协议类型
10.1.12.0/24	-	ge4	0	0	直连路由
200.200.156.0/22	-	vlan1	0	0	直连路由
11.11.11.0/24	-	vlan11	0	0	直连路由
22.22.22.0/24	10.1.12.2	ge4	2	120	RIP路由
33.33.33.0/24	10.1.12.2	ge4	2	120	RIP路由
0.0.0.0/0	200.200.159.254	-	0	1	静态路由
10.1.23.0/24	10.1.12.2	ge4	2	120	RIP路由

1 / 1 每页 25 记录数: 7

[RIP路由详情](#) | [OSPF路由详情](#)

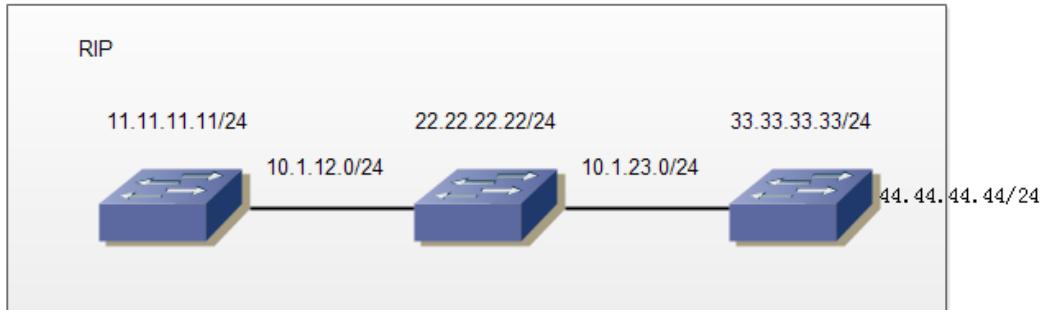
同时,可根据具体需要配置相应的引入规则与度量值,也可将直连路由与 OSPF 作为引入。

9.3. 企业 RIP 网络不接收某些路由(路由白名单)

场景描述:

用户网络存在性能设备较差,不支持学习大量路由,可以通过配置路由白名单,只保留需要学习到的路由信息。

网络拓扑:



演示步骤:

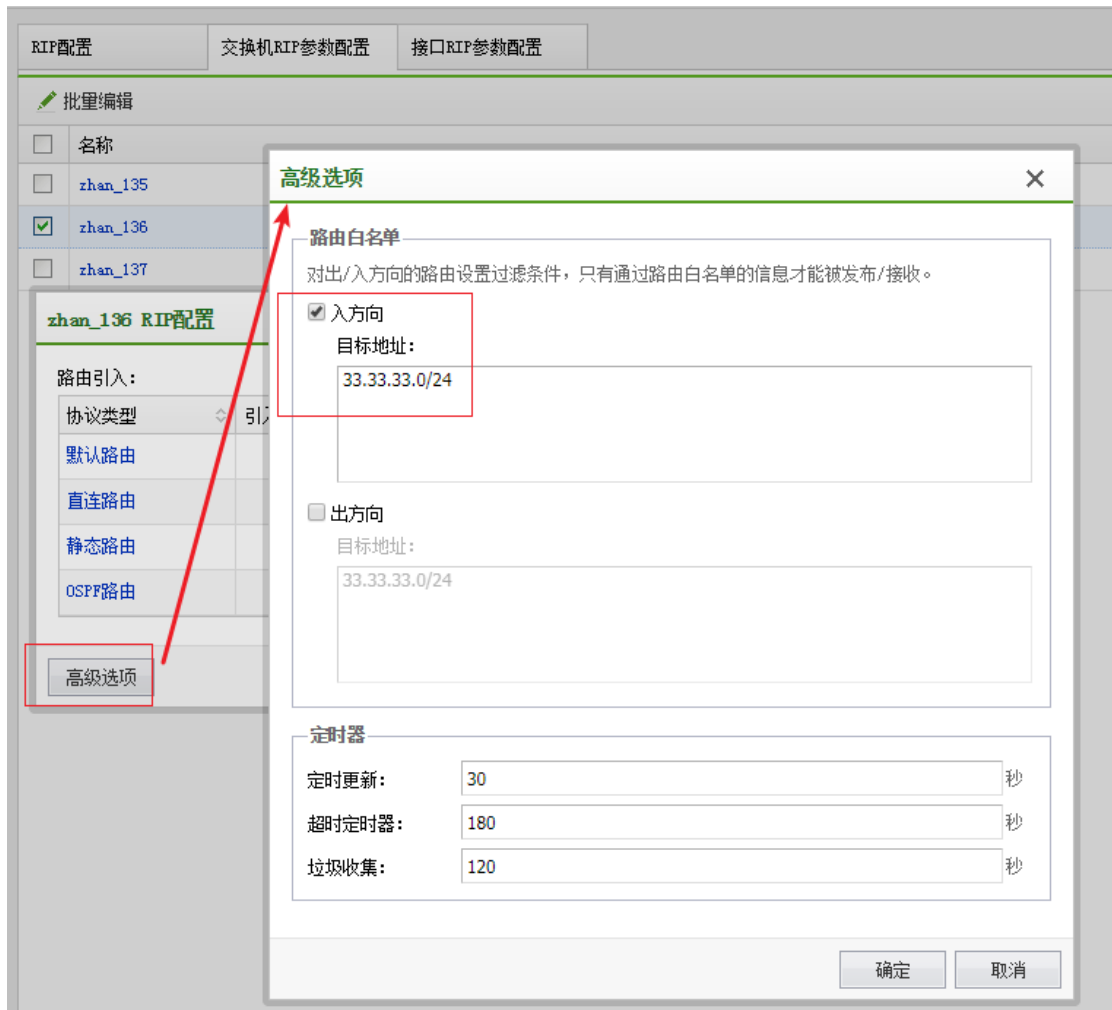
1.环境准备:

WAC: 1 台

信锐交换机: 三台

2.策略配置:

(1) 在交换机 RIP 参数配置页面, 配置路由白名单将 44.44.44.44 的路由信息过滤; 可配置入方向或出方向的路由白名单。



3.功能验证:

(1) 未开启路由白名单时:

交换机详情-zhan_135

普通模式 链路聚合 防环路 链路高可用 MAC地址表 ARP地址表 组播地址表 路由状态 链路检测 VRRP组

实时状态

目标地址/掩码	下一跳地址	接口	度量值	优先级	协议类型
33.33.33.0/24	10.1.12.2	ge4	3	120	RIP路由
44.44.44.0/24	10.1.12.2	ge4	3	120	RIP路由
10.1.12.0/24	-	ge4	0	0	直连路由
200.200.156.0/22	-	vlan1	0	0	直连路由
11.11.11.0/24	-	vlan11	0	0	直连路由
22.22.22.0/24	10.1.12.2	ge4	2	120	RIP路由
0.0.0.0/0	200.200.159.254	-	0	1	静态路由

记录数: 8

RIP路由详情 | OSPF路由详情

(2) 开启路由白名单时:

交换机详情-zhan_135

普通模式 链路聚合 防环路 链路高可用 MAC地址表 ARP地址表 组播地址表 路由状态 链路检测 VRRP组

实时状态

目标地址/掩码	下一跳地址	接口	度量值	优先级	协议类型
33.33.33.0/24	10.1.12.2	ge4	3	120	RIP路由
10.1.12.0/24	-	ge4	0	0	直连路由
200.200.156.0/22	-	vlan1	0	0	直连路由
11.11.11.0/24	-	vlan11	0	0	直连路由
22.22.22.0/24	10.1.12.2	ge4	2	120	RIP路由
0.0.0.0/0	200.200.159.254	-	0	1	静态路由
10.1.23.0/24	10.1.12.2	ge4	2	120	RIP路由

记录数: 7

RIP路由详情 | OSPF路由详情

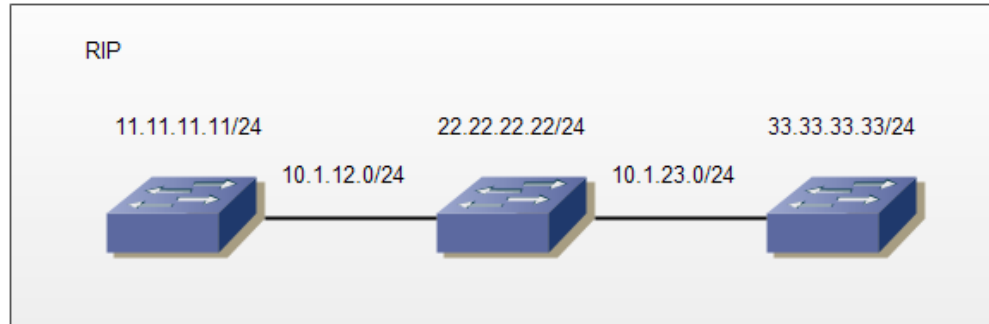
出入方向的区别在于：出方向是发送路由信息时进行过滤，入方向是接收路由信息是进行过滤。

9.4. 企业部署 RIP 网络与 BFD 联动

场景描述:

企业 RIP 网络动态感知链路变化，快速来进行链路切换。

网络拓扑:



演示步骤:

1.环境准备

WAC : 1 台

信锐交换机: 3 台

2.策略配置

(1) 在端口 RIP 参数配置页面, 启用 bfd 检测;



(5) 功能验证



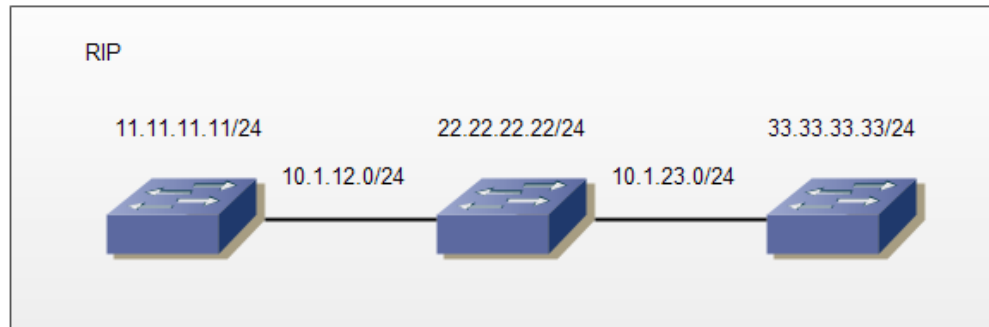
当链路出现故障时，可马上进行路由切换，不用等待老化时间。

9.5. 企业部署 RIP 网络，并配置认证方式

场景描述：

对网络安全性要求较高的网络中,企业可以通过配置认证的方式来提高网络拓扑的安全性;提高 RIP 网络的安全性,防止误接入导致网络震荡。

网络拓扑:



演示步骤:

1.环境准备

WAC : 1 台

信锐交换机: 3 台

2.策略配置

(1) 新增 RIP 策略,并配置接口认证方式为明文密码认证或 MD5 认证;

RIP配置 交换机RIP参数配置 接口RIP参数配置

批量编辑

<input type="checkbox"/>	名称
<input type="checkbox"/>	vlanif11
<input checked="" type="checkbox"/>	zhan_135 port4
<input type="checkbox"/>	vlanif22
<input type="checkbox"/>	zhan_136 port10
<input type="checkbox"/>	zhan_136 port4
<input type="checkbox"/>	vlanif33
<input type="checkbox"/>	zhan_137 port24

zhan_135 RIP配置

IP地址: 10.1.12.1/24
所属策略: RIP
所属交换机: zhan_135
参数配置: 使用独立配置

认证方式: 明文密码认证 ?
认证口令: 123456

防止路由环路: 启用水平分割 启用毒性反转

RIP更新报文: 允许发送RIP更新报文

BFD检测

发送间隔: 1000 壹秒
接收间隔: 1000 壹秒
检测倍数: 3

附加度量值

发送: 0
接收: 1

提交 取消



3.功能验证



接口认证：是将开启 RIP 协议并与设备相邻的接口开启认证，是以交换机接口为单位，认证方式明文认证及密文认证，明文认证在抓取数据包时可以看到认证字段及明文密码，密

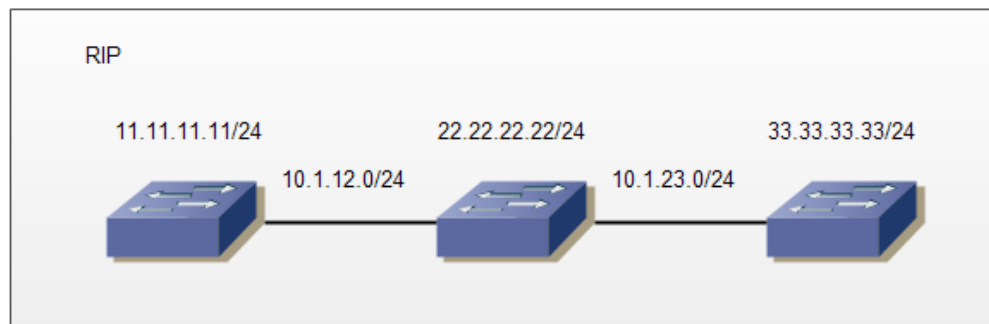
文认证在抓取数据包时可以看到认证字段及密文密码。

9.6. 企业部署 RIP 网络，其他高级选项功能配置

场景描述：

- 1.企业 RIP 网络中某设备存在大量路由，可通过关闭更新报文发送，抑制路由同步；
- 2.RIP 网络中收敛较慢，通过更改定时器加快收敛；
- 3.RIP 网络中容易出现路由环路，开启防止路由环路功能（必开）；
- 4.更改路由选路可通过更改度量值来改变选路。

网络拓扑：



演示步骤：

1.环境准备

WAC : 1 台

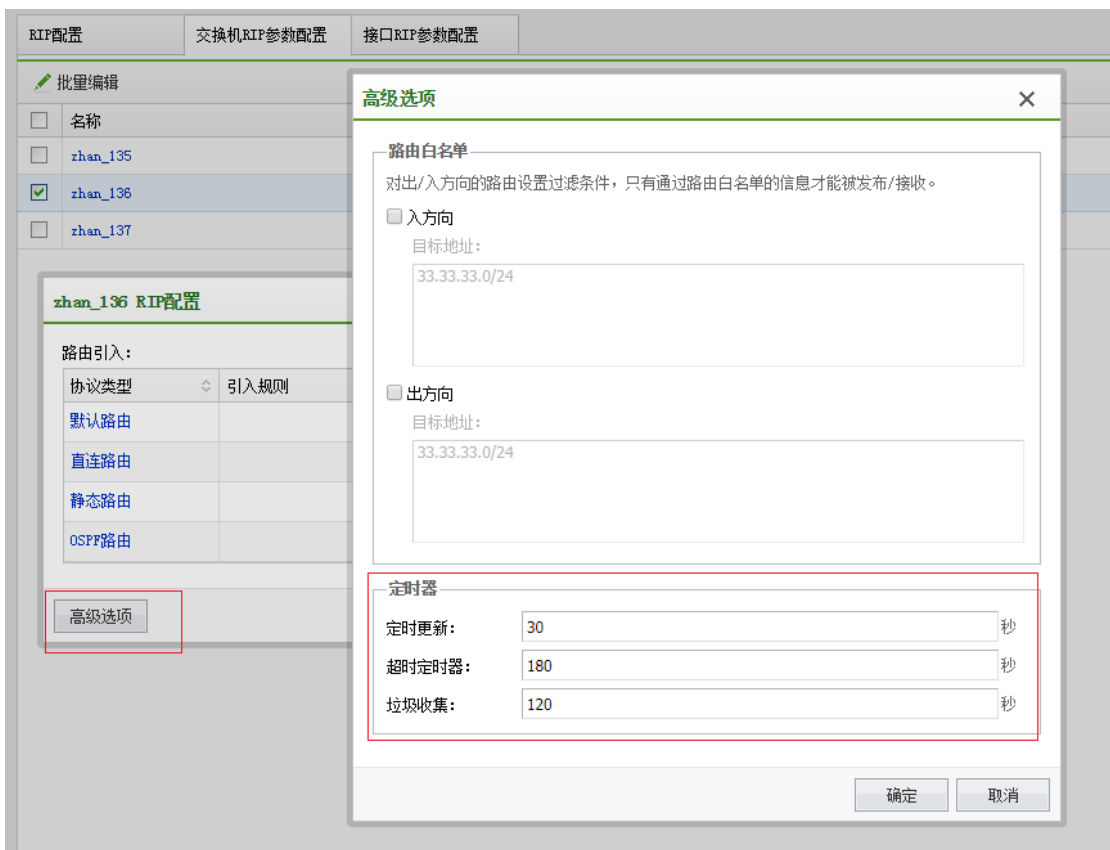
信锐交换机：3 台

2.策略配置

- (1) 在端口 RIP 参数配置页面，接口参数中不勾选允许发送 RIP 更新报文



(2) 在交换机 RIP 参数配置页面，高级选项中配置定时器时间；



(3) 在端口 RIP 参数配置页面，接口参数中配置防环路机制；

The screenshot shows the 'zhan_135 RIP配置' dialog box with the following configuration details:

- IP地址: 10.1.12.1/24
- 所属策略: RIP
- 所属交换机: zhan_135
- 参数配置: 使用独立配置
- 认证方式: 明文密码认证
- 认证口令: 123456
- 防止路由环路: 启用水平分割 启用毒性反转
- RIP更新报文: 允许发送RIP更新报文
- BFD检测
 - 发送间隔: 1000 毫秒
 - 接收间隔: 1000 毫秒
 - 检测倍数: 3
- 附加度量值
 - 发送: 0
 - 接收: 1

Buttons at the bottom: 提交 (Submit), 取消 (Cancel)

(4) 在端口 RIP 参数配置页面，接口参数中配置附加度量值；

zhan_135 RIP配置

IP地址: 10.1.12.1/24
所属策略: RIP
所属交换机: zhan_135
参数配置: 使用独立配置
认证方式: 明文密码认证
认证口令: 123456
防止路由环路: 启用水平分割 启用毒性反转
RIP更新报文: 允许发送RIP更新报文

BFD检测

发送间隔: 1000 毫秒
接收间隔: 1000 毫秒
检测倍数: 3

附加度量值

发送: 0
接收: 1

提交 取消

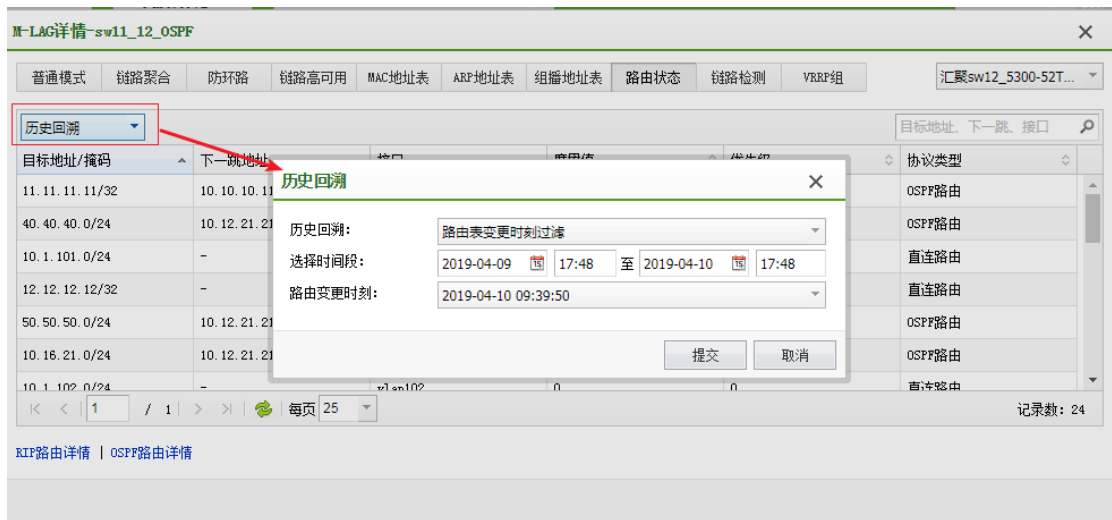
9.7. 企业部署 RIP 网络，网络故障进行故障诊断

场景描述:

企业 RIP 网络出现的网络故障，需要进行性故障诊断

功能:

- (1) 历史回溯: 支持查看某一时刻路由表的学习情况，进而进行诊断当时路由的变化情况



(2) 实时路由表：可查看此时的路由表情况，支持搜索功能



(3) RIP 路由详情：分为 RIP 状态、邻接关系、接口信息、路由信息、历史日志。可查看 RIP 的相关配置，及历史信息



(4) 实时路由拓扑：可查看此时路由拓扑，点击设备可查看相关信息



9.8. 控制器系统维护

『系统维护』包括如下几个功能模块【序列号】、【系统更新】、【日志查看】、【备份恢复】、【故障排除】、【调试选项】、【重启及格式化】、【命令行控制台】、【导出系统记录】、【设备授权更新】；下面将一一讲解

9.8.1. 序列号

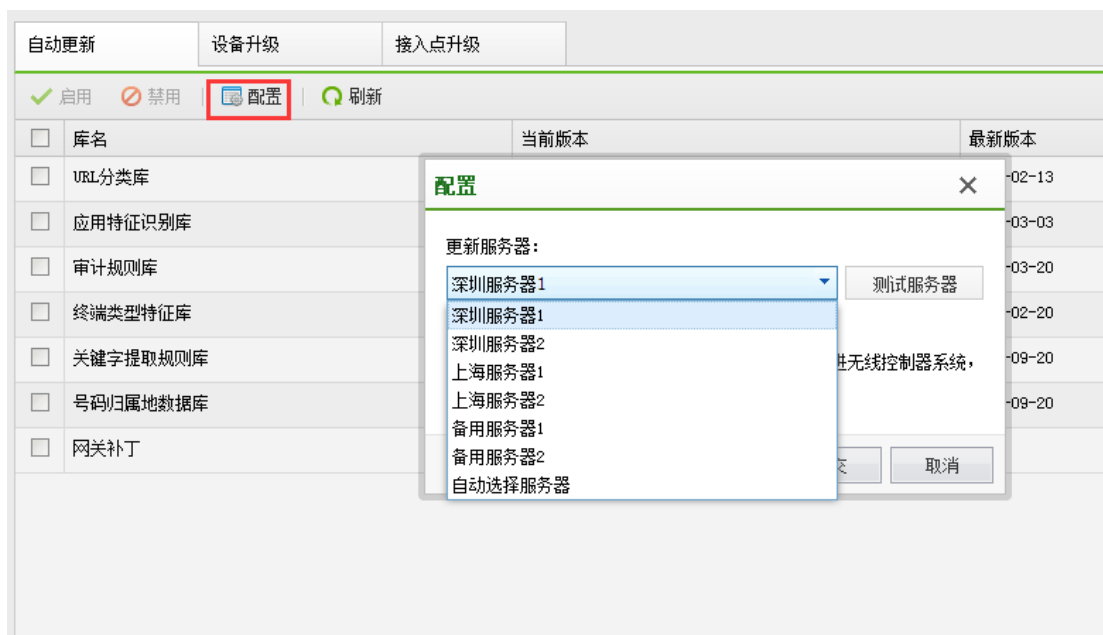
使用无线控制器前，必须向设备供应商购买有效的产品或功能序列号。NAC 的版本序列号包括设备序列号和软件升级序列号，设备序列号决定了一个 NAC 最多可以管理安视交换机的个数。软件升级序列有效，NAC 才可以正常升级软件版本，配置界面如下：



9.8.2. 系统更新

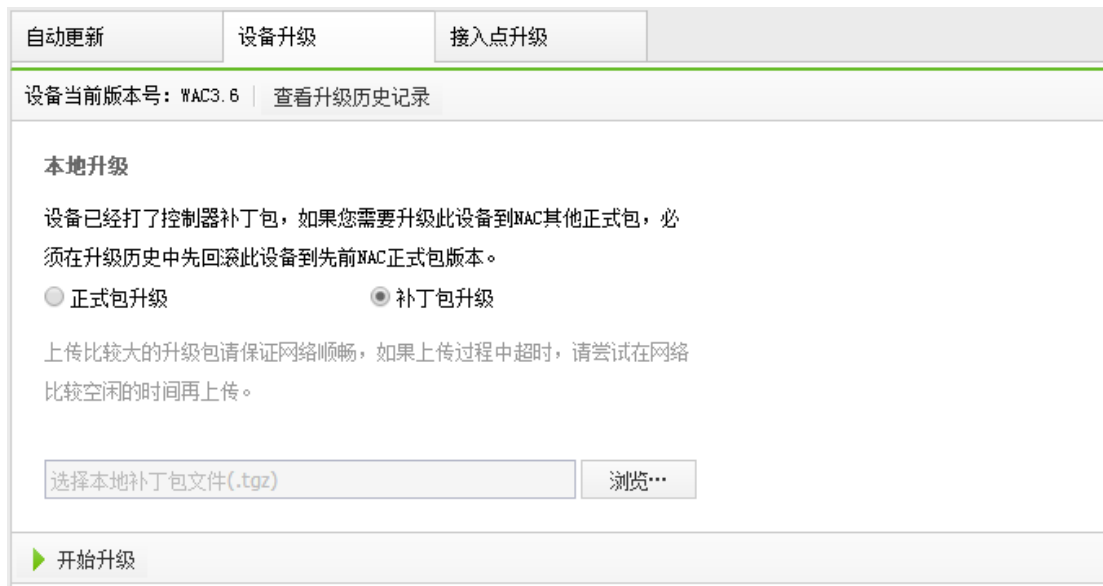
9.8.2.1. 自动更新

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，帮助我们改进无线控制器系统，该报告不会涉及您组织的任何信息。

9.8.2.2. 设备升级



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，详细方法参考第六章。

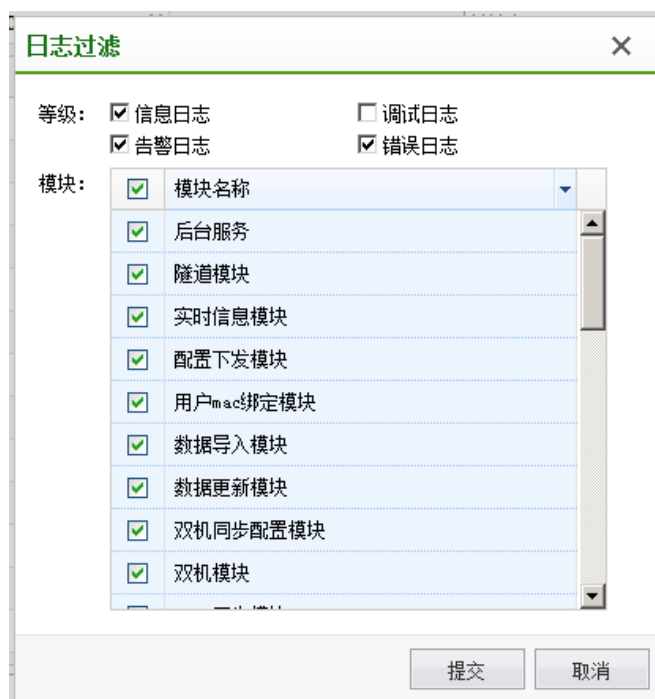
9.8.3. 日志查看

9.8.3.1. 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

接入点日志	系统日志	管理日志	安全日志	用户认证日志	
日期: 2014-07-14   日志过滤  刷新 <input type="text" value="关键字"/> 					
时间	日志	模块	等级		
2014-07-14 20:00:18	客户端解除关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 20:00:17	新客户端关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 20:00:17	终端[AC-CF-5C-E6-F8-53]允许接入ap[100D0E2000CB000...	ap负载模块	信息		
2014-07-14 20:00:15	ap:10:0D:0E:20:00:CE sta:AC:CF:5C:E6:F8:53 接收到...	在线用户模块	信息		
2014-07-14 20:00:15	新客户端关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 20:00:15	终端[AC-CF-5C-E6-F8-53]允许接入ap[100D0E2000CB000...	ap负载模块	信息		
2014-07-14 19:58:29	客户端解除关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 19:57:27	ap:10:0D:0E:20:00:CE sta:AC:CF:5C:E6:F8:53 接收到...	在线用户模块	信息		
2014-07-14 19:57:27	新客户端关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 19:57:27	终端[AC-CF-5C-E6-F8-53]允许接入ap[100D0E2000CB000...	ap负载模块	信息		
2014-07-14 19:57:10	客户端解除关联, MAC地址 [ac:cf:5c:e6:e8:53]	二层认证模块	信息		
2014-07-14 19:56:16	客户端解除关联, MAC地址 [84:38:38:4e:83:38]	二层认证模块	信息		
< < 1 / 79 > >  每页 25 记录数: 1958					

日志过滤选项界面如下：



9.8.3.2. 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

接入点日志	系统日志	管理日志	安全日志	用户认证日志	
日期: 2014-07-14					关键字
时间	日志	操作对象	结果	管理员	IP地址
2014-07-14 19:52:04	添加建筑物 test 的楼...	系统管理	成功	admin	192.200.200.57
2014-07-14 19:48:56	部署楼层	系统管理	成功	admin	192.200.200.57
2014-07-14 19:21:36	添加建筑物 test 的楼...	系统管理	成功	admin	192.200.200.57
2014-07-14 18:49:46	登录系统	系统管理	成功	admin	192.200.200.57
2014-07-14 18:49:32	登录系统	系统管理	成功	admin	192.200.200.57
2014-07-14 18:48:15	登录系统	系统管理	成功	admin	192.200.200.57
2014-07-14 18:46:19	登录系统	系统管理	成功	admin	192.200.200.57
2014-07-14 15:59:05	删除建筑物 zb	系统管理	成功	admin	192.200.200.121
2014-07-14 15:59:03	登录系统	系统管理	成功	admin	192.200.200.57
2014-07-14 15:53:05	添加建筑物 zb	系统管理	成功	admin	192.200.200.121
2014-07-14 10:13:47	登录系统	系统管理	成功	tzm	192.200.60.119
2014-07-14 10:10:10	登录系统	系统管理	成功	tzm	192.200.60.119

日志过滤配置界面如下图：



9.8.3.3. 安全日志

记录所有的检测到的无线网络安全事件，并将检测到后进行的操作记录。



9.8.3.4. 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：

接入点日志	系统日志	管理日志	安全日志	用户认证日志					
<input type="text"/> 查询 <input type="button" value="刷新"/> <input type="button" value="导出"/>									
时间	事件类型	攻击者MAC	攻击者设备类型	发现后动作	描述	接入点	接入点分组	攻击者IP	攻击者计算机名
2017-05-02 15:15:54	IP扫描攻击	68-3E-34-ED-FC-B7	终端	告警	终端(68-3e-34-e4-fc-b7)IP扫描攻击	303_信通9	三楼	-	-
2017-05-02 15:15:05	IP扫描攻击	C8-F2-30-66-5C-85	终端	告警	终端(c8-f2-30-66-5c-85)IP扫描攻击	111_43360信通6	一楼	-	-
2017-05-02 15:13:11	ARP扫描攻击	90-48-9A-40-94-A1	终端	告警	终端(90-48-9a-40-94-a1)ARP扫描攻击	202_43360信通11	二楼	-	-
2017-05-02 14:53:38	IP扫描攻击	40-C8-2A-48-F9-87	终端	告警	终端(40-c8-2a-48-f9-87)IP扫描攻击	301_信通13	三楼	-	-
2017-05-02 14:51:53	端口扫描攻击	0C-A9-02-3C-4F-E8	终端	告警	终端(0c-a9-02-3c-4f-e8)端口扫描攻击	406_信通1	四楼	-	-
2017-05-02 14:48:15	IP扫描攻击	3C-91-57-9D-A1-03	终端	告警	终端(3c-91-57-9d-a1-03)IP扫描攻击	308_信通1	三楼	-	-
2017-05-02 14:32:34	IP扫描攻击	84-73-03-5C-EE-8C	终端	告警	终端(84-73-03-5c-ee-8c)IP扫描攻击	407_信通9	四楼	-	-
2017-05-02 14:30:48	IP扫描攻击	98-7A-E3-39-3F-87	终端	告警	终端(98-7a-e3-39-3f-87)IP扫描攻击	701_信通5	七楼	-	-
2017-05-02 14:22:07	IP扫描攻击	FC-3B-83-79-88-A9	终端	告警	终端(fc-3b-83-79-88-a9)IP扫描攻击	-2F便利店	公共区域	-	-
2017-05-02 14:17:14	IP扫描攻击	8C-3A-EA-09-6B-95	终端	告警	终端(8c-3a-ea-09-6b-95)IP扫描攻击	503_信通11	五楼	-	-
2017-05-02 14:12:38	IP扫描攻击	88-1F-A1-1A-65-5A	终端	告警	终端(88-1f-a1-1a-65-5a)IP扫描攻击	211_43360信通11	二楼	-	-
2017-05-02 13:31:20	IP扫描攻击	84-73-03-5C-EE-8C	终端	告警	终端(84-73-03-5c-ee-8c)IP扫描攻击	407_信通9	四楼	-	-
2017-05-02 13:28:55	IP扫描攻击	98-7A-E3-39-3F-87	终端	告警	终端(98-7a-e3-39-3f-87)IP扫描攻击	701_信通5	七楼	-	-
2017-05-02 13:24:17	IP扫描攻击	C8-F2-30-66-5C-85	终端	告警	终端(c8-f2-30-66-5c-85)IP扫描攻击	111_43360信通6	一楼	-	-
2017-05-02 13:14:45	IP扫描攻击	80-45-09-E2-54-95	终端	告警	终端(80-45-09-e2-54-95)IP扫描攻击	111_43360信通6	一楼	-	-

9.8.4. 故障排除

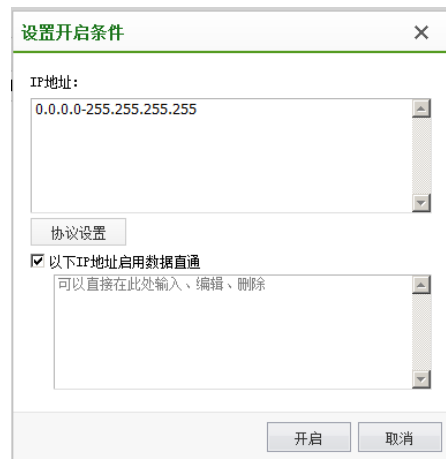
故障排除，主要用于网络故障时，用于排查问题原因，当无线终端可能由于配置问题导致用户无法正常上网时，进行故障排除和数据直通，使用方法与深信服 AC 设备类似，先是开启故障日志，也可以同时开启数据直通。提供了以下功能：

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。

时间	源	目的	协议	规则类型	规则名称	大小(Byte)	丢包原因
2017-12-19 11:52:39	10.1.1.32	101.226.211.105	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49821	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49820	101.226.211.44:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32:49819	101.226.211.44:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:38	10.1.1.32	10.1.1.1	ICMP	服务	-	122	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49818	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49817	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49816	14.116.140.36:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32	180.163.25.150	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49815	114.80.10.31:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:37	10.1.1.32:49814	114.80.10.31:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49813	101.227.169.159:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49812	101.227.162.149:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32	10.1.1.1	ICMP	服务	-	122	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32	180.163.25.150	ICMP	服务	-	98	经角色引用的访问控制策略(允许DNS)判断为拒绝
2017-12-19 11:52:36	10.1.1.32:49810	183.57.85.133:80	TCP	服务	-	78	经角色引用的访问控制策略(允许DNS)判断为拒绝

设置开启条件界面如下图：



9.8.5. 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



9.8.6. 命令控制台

提供可直接操作 nac 设备的调试命令，用于排除问题。

```
命令行控制台

控制台支持的命令：
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
dhcpoolbind           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
dhcpool              查看地址池信息
interface             查看网口信息

> Type and execute commands here, type 'help' for help
```

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
dhcpoolbind	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
dhcpool	查看地址池信息
interface	查看网口信息

第10章 附录

10.1. 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』：WLAN 设备的默认密码为 dlanrecover 或者是与 WLAN 设备的控制台密码保持一致，与所连接的 WLAN 设备的版本有关。

『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。

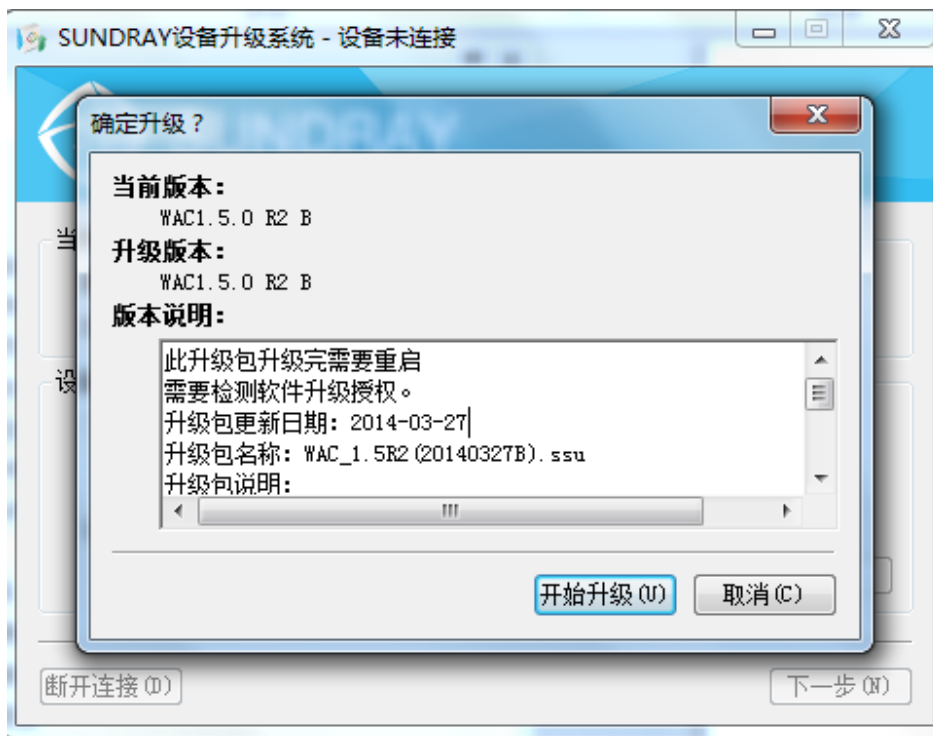


1.使用 SUNDRAY 设备升级系统进行在线升级时，要求所连接的 SUNDRAY 设备能够正常上网，否则将不能进行在线升级。

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：



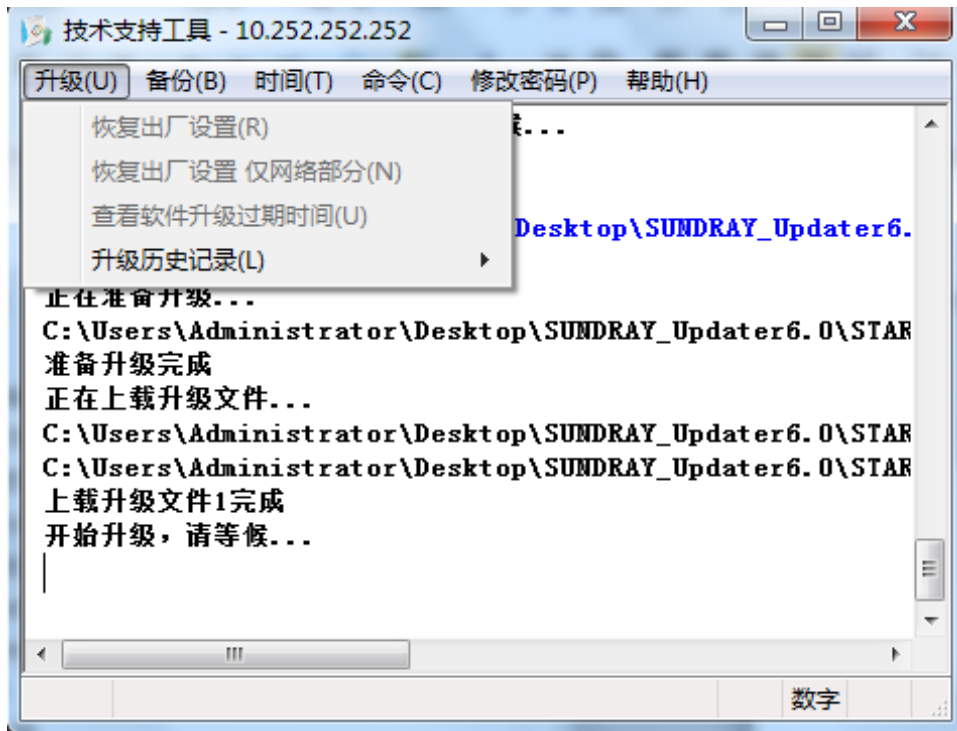
升级完成后，设备升级状态里会显示“升级成功”，界面如下：



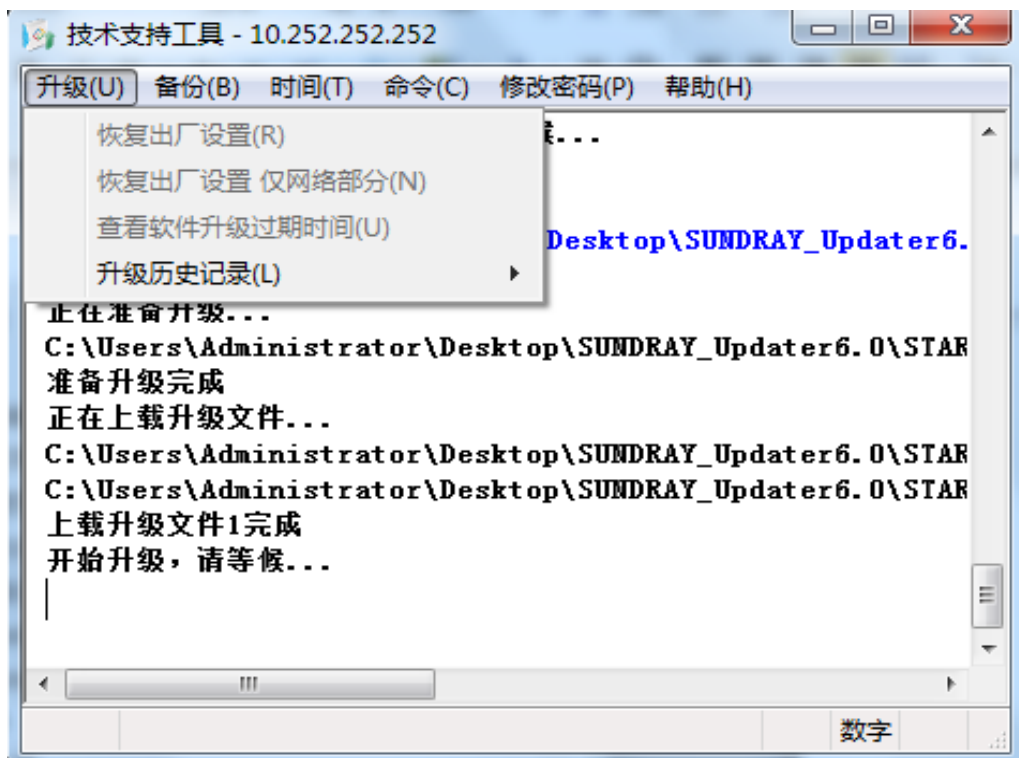
1. 升级具有一定的风险，如升级不当会导致设备损坏。请勿自行升级。如需升级请联系信锐技术客户服务部。

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：



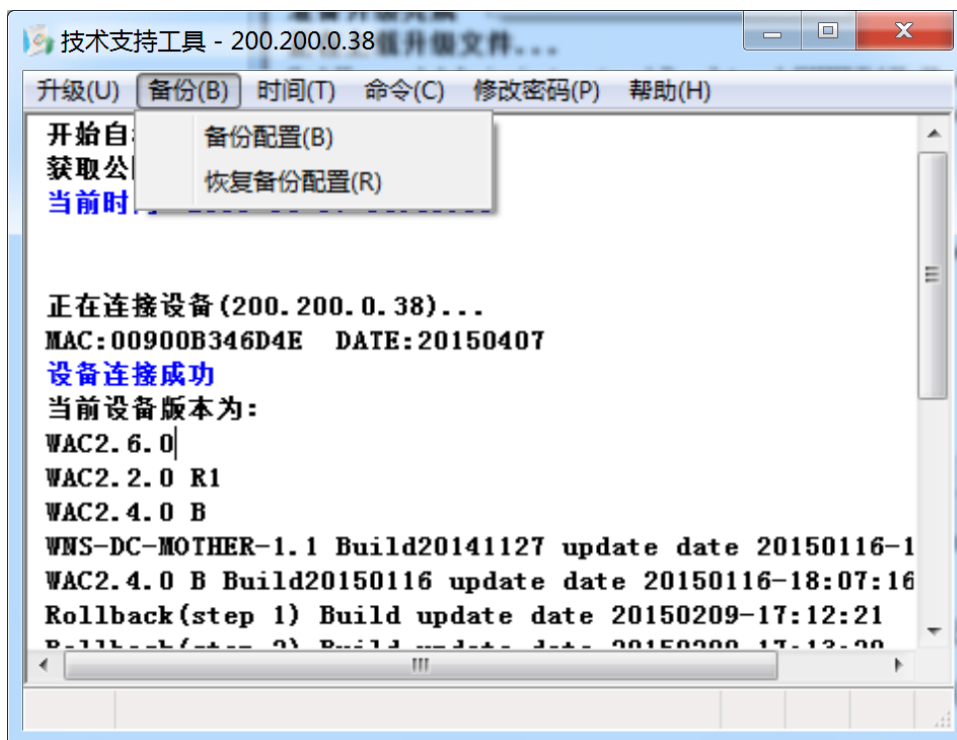
[恢复出厂设置]: 用于将 SUNDRAY 硬件设备恢复到默认配置, 需要通过加载升级包将设备恢复出厂设置。

[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。

[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。

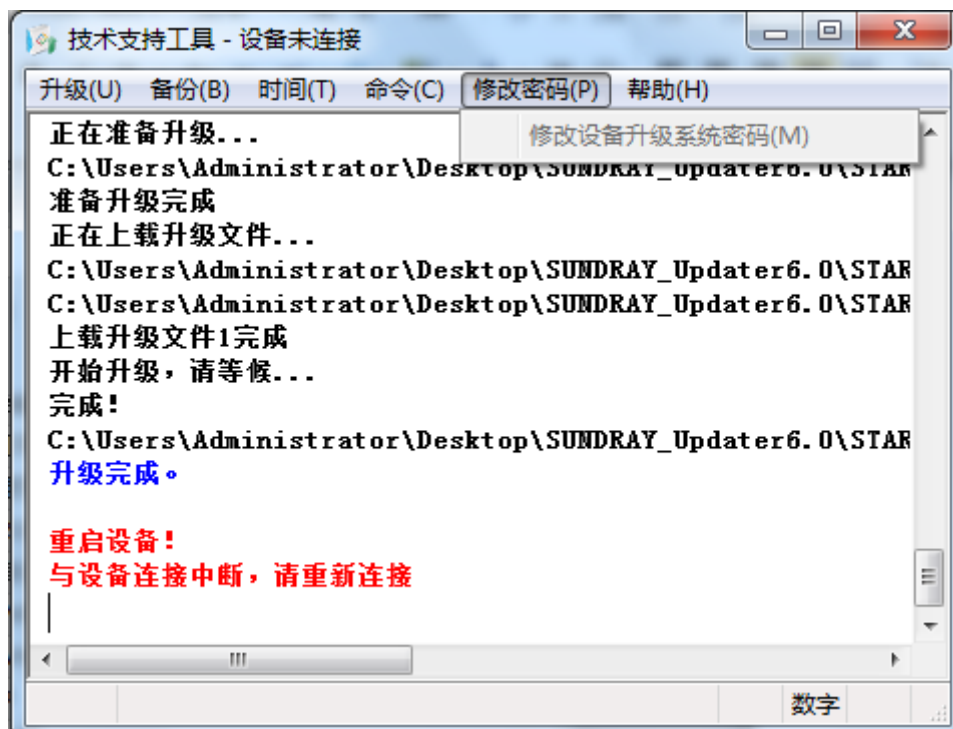
[查看网卡工作模式]: 查看设备各网卡的工作模式。

[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。

