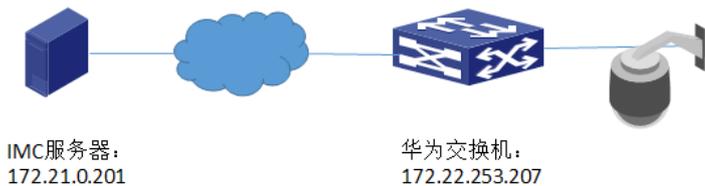


组网需求:

客户有大量监控设备,摄像头都安装在室外,经常有终端可能被私自替换或者非法终端接入监控网络,为了防止其它终端接入,使用MAC认证,本案例使用的交换机为华为的S5700。使用iMC做MAC认证。MAC认证并不是最安全,私接终端可以更改跟摄像头一样的MAC地址。如果需要完全防止私接,可以配合H3C EPS组件,通过分析摄像头协议栈指纹来识别不同的终端,用来防止仿冒MAC地址终端接入,本案例只是摄像头认证前部分。

组网如下,iMC连接在监控网中的服务器端,摄像头连接在华为交换机的G0/0/3的接口。iMC服务器IP地址与华为交换机的NAS-IP网络可达,或者华为交换机连接iMC服务器的最近的IP地址网络可达。



颜美花 2017-08-21 发表

颜美花 2017-08-21 发表

1, 华为交换机S5700创建vlan及管理ip地址

```
[Switch]vlan batch 508 521
[Switch] interface vlanif 521
[Switch-Vlanif10]ip address 172.22.253.207 255.255.255.0
```

2, 配置华为交换机RADIUS认证

配置RADIUS服务器模板, 实现交换机与iMC采用RADIUS方式通信

```
[Switch]radius-server template rd1
[Switch-radius-rd1] radius-server shared-key simple 123456
[Switch-radius-rd1] radius-server authentication 172.21.0.201 1812
[Switch-radius-rd1] radius-server accounting 172.21.0.201 1813
[Switch-radius-rd1] undo radius-server user-name domain-included
[Switch-radius-rd1] radius-attribute nas-ip 172.22.253.20
# 配置AAA认证方案, 指定认证方式为RADIUS
[Switch] aaa
[Switch-aaa] authentication-scheme abc
[Switch-aaa-authen-sch1] authentication-mode radius
```

配置AAA计费方案, 指定计费方式为RADIUS

```
[Switch-aaa] accounting-scheme ac1
[Switch-aaa-accounting-account1] accounting-mode radius
# 在domain域下引用AAA认证方案和RADIUS服务器模板。
[Switch-aaa] domain mac
[Switch-aaa-domain-mac] radius-server rd1
[Switch-aaa-domain-mac] authentication-scheme abc
[Switch-aaa-domain-mac] accounting-scheme ac1
#在全局使能mac认证, 并指定缺省域和mac quiet-period时间。在连接
哑终端的物理接口开启MAC地址认证。
[Switch] mac-authen
[Switch]mac-authen domain mac
[Switch]mac-authen timer quiet-period 10
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 508
[Switch-GigabitEthernet0/0/3] mac-authe
```

3, 配置iMC服务器

a, 单击“用户>接入策略管理>接入设备管理>接入设备配置”菜单, 点击“增加”,如下图所示。注意密钥要与设备端匹配, 并且设备接入类型选择“HUAWEI (general) ”

接入配置

认证端口 * 1812 计费端口 * 1813

业务类型 * 不限 强制下线方式 * 断开用户连接

接入设备类型 * **HUAWEI (General)** 接入位置分组 * 无

共享密钥 * ***** 确认共享密钥 * *****

设备列表

设备名称	设备IP地址	设备型号	备注
	172.22.253.207		

b, 单击“用户>接入策略管理>接入策略管理”菜单, 点击“增加”如下图所示, 如果无限制, 保存缺省配置。

用户 > 接入策略管理 > 接入策略管理 > 修改接入策略

基本信息

接入策略名称 * mac

业务分组 * 未分组

描述

接收信息

接入时段 * 无 分配IP地址 * 否

下行速率(Kbps) 上行速率(Kbps)

优先级 下发用户组

首选EAP类型 * EAP-MD5 单次最大在线时长(分钟)

EAP自协商 * 启用 下发VLAN

下发地址池 下发VSI名称

下发User Profile

c, 单击“用户>接入策略管理>接入服务管理”菜单, 点击“增加”, 如下图所示, 绑定创建好的接入策略。如果交换机携带域名后缀, 则在接入服务管理中的服务后缀输入与交换机一样的domain, 比如本案例的domain是mac。

用户 > 接入策略管理 > 接入服务管理 > 修改接入服务

基本信息

服务名称 * mac 服务后缀 * mac

业务分组 * 未分组 缺省接入策略 * mac

缺省私有属性下发策略 * 不使用

缺省单号最大递增间隔 * 0 缺省单号在线数量限制 * 0

单日累计在线最长时时间(分钟) * 0

服务描述

可申诉 无感知认证

接入场景列表

名称	接入策略	私有属性下发策略	优先级	修改	删除

d, 单击“用户>哑终端用户配置”菜单, 点击“增加”如下图所示, 绑定接入服务, 及哑终端mac地址起始和终止范围以及描述。添加成功后, 并点击“立即审计”

配置名称 * 哑终端 用户名前缀 * monitor

业务分组 * 未分组 用户分组 * 未分组

失效日期 * 生效日期 * 控制类型 * 允许接入 优先级 * 0

描述

MAC地址段

增加 批量导入 全部删除

起始MAC地址	终止MAC地址	描述	修改	删除
44:19:86:19:3F:CC	44:19:86:19:3F:CC	G0/0/3		

共有1条记录。

接入服务

服务名称	服务描述	服务后缀	状态
mac			可申诉

配置结果验证

交换机上执行命令display access-user显示认证通过结果

```
<HF-LY-AQL-S5700>dis access-user domain mac
-----
UserID Username                IP address                MAC
-----
228 4419b6193fcc@mac           172.22.79.246            4419-b619-3fcc
-----
Total 1,1 printed
```

iMC服务器显示认证通过结果



The screenshot shows the '在线用户' (Online Users) page in the iMC management console. It includes search filters for '帐号名' (Account Name) and '用户分组' (User Group). Below the filters are buttons for '下线' (Offline), '强制下线' (Force Offline), '清除在线信息' (Clear Online Info), '重认证' (Re-authenticate), '忘記密碼' (Forgot Password), and '批量导出' (Batch Export). A table lists the online users with columns for selection, account name, login name, service name, login time, login duration, device IP, user IP, and security status.

<input type="checkbox"/>	帐号名	登录名	用户姓名	服务名	接入时间	接入时长	设备IP地址	用户IP地址	安全状态
<input type="checkbox"/>	44-19-b6-19-3fcc	4419b6193fcc	monitor-44-19-b6-19-3fcc	mac	2017-08-18 14:20:04	0秒	172.22.253.207	172.22.79.246	无需安全认证

配置注意事项

第一：确保iMC配置的密钥和设备端保持一致，并且NAS-IP 网络可达，设备接入类型选择对应的HUAWEI厂家。

第二：确保交换机与服务器端的服务名是否有后缀，否则认证日志会提示“用户不存在或者没有申请该服务”。