ACG1000-AK230 创建用户绑定mac后，上线后该用户被归类为匿名用户

ACG1000 陈启敏 2021-10-31 发表

组网及说明

设备型号和版本：SecPath ACG1000-AK230 6611p06

组网：acg部署在防火墙和华为交换机之间，二层透传，另外又接了个线连华为交换机和acg，配置ip地址

问题描述

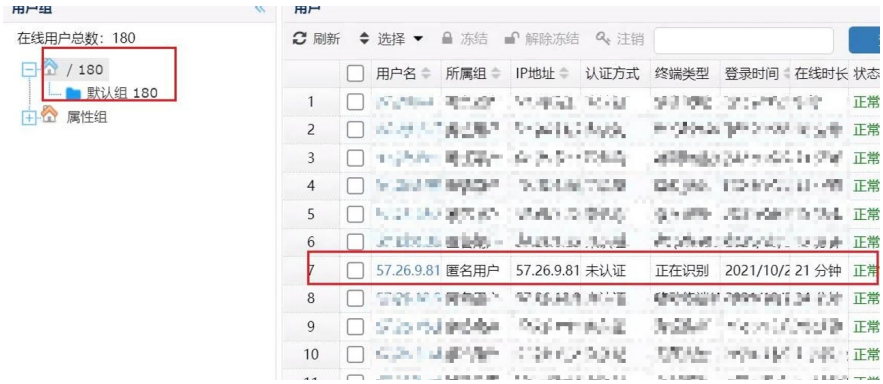
故障现象:现场创建了多个用户组，其中的用户均只绑定了mac地址，但是该mac地址的设备上线后的用户还是属于匿名用户，认证方式为未认证

以下面用户为例，9.81为该用户获取的ip地址后两位

```
4c:34:88:9e:44:04    9.81
```

用户创建时绑定的mac

在线用户的状态



过程分析

分析

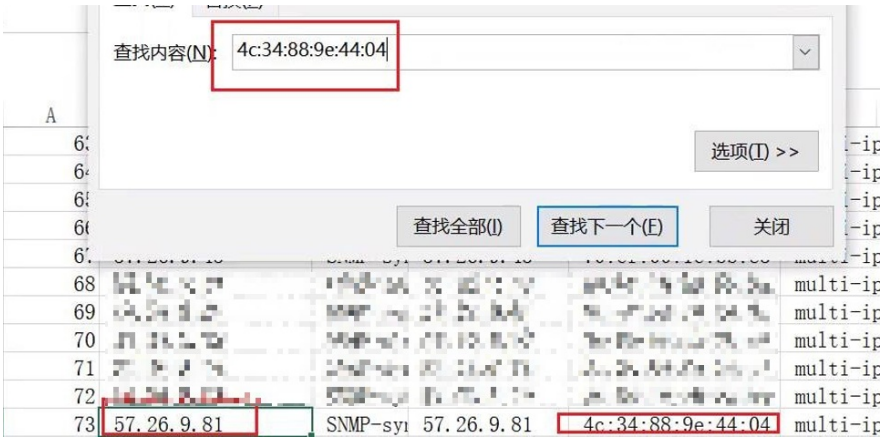
1、正常来说，当未进行认证的用户上到acg的时候会归类为匿名用户，如果是创建的用户，绑定了ip或者mac地址的用户，上来到acg后会匹配ip地址与mac地址，然后归类为静态绑定用户

2、根据故障现象来看：用户均只绑定了mac地址，但是该mac地址的设备上线后的用户还是属于匿名用户，认证方式为未认证。可能的原因是现场该用户的报文到acg上转发时，属于三层转发，而acg只识别到核心接口的mac，而没有识别到该用户的真实mac导致，mac未匹配上，因此归类为匿名用户

3、向现场确认是否是三层转发，现场表示acg是在防火墙和华为交换机之间做透传，部署透明模式，但是业务报文上到acg的时候是跨三层上来的

4、如果三层转发的话，acg要识别真实的用户的mac地址的话，必须在acg上配置snmp跨三层mac学习，检查现场配置，发现现场也是有做跨三层mac学习，是在acg与华为交换机单独连线的接口上配置的，检查snmp同步的表项如下，也没有问题，能成功同步到

Snmp 同步结果的表格：



5、向现场确认是否有配置用户mac敏感 ： user mac-sensitive enable 现场表示没有开启，该命令作用如下，开启也也没有成功归类为静态用户

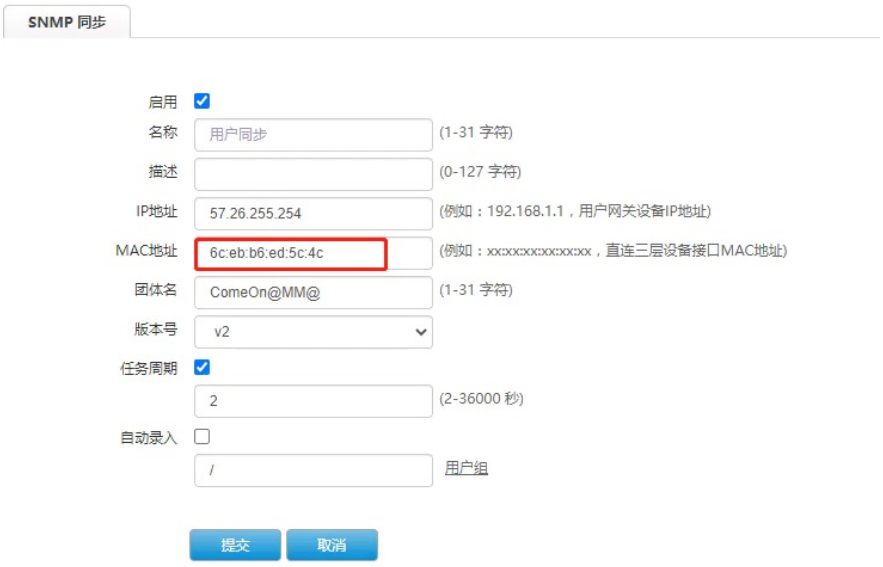
用户MAC敏感命令是配合SNMP跨三层学习MAC功能一起使用的，默认情况下为disable状态，即用户MAC发生变化后用户不会被踢下线；在跨三层环境下由于通过SNMP获取到真实MAC后在线用户的MAC会发生变化，开启MAC敏感以将用户踢下线，重新进行识别，以便重新关联用户。 说明：跨三层环境下，用户上线时MAC识别为匿名用户，MAC 地址为下联三层设备的接口MAC1,用户静态绑定条目为（user2 MAC2），当开启跨三层学习后，正常获取到用户的真实MAC2,如果用户MAC敏感为关闭状态，用户不会重新识别会导致无法关联上静态绑定用户，在线用户仍然会显示匿名用户，就会导致所有引用了账号user2的策略均不生效

6、怀疑是否判定的mac地址不正确，于是让重新创建用户，绑定mac地址的各项，进行空格、带-，不带-等修改，然后用户踢下线，重新上来依旧无法正确归类

解决方法

问题定位：

最后排查发现是配置snmp的时候时候，配置mac地址是核心交换机上的mac地址，但是不是互联的接口mac地址，两者相差最后一位，一个是4c，一个是4d ，如下图：



ACG1000的“跨三层MAC学习”功能配置参数要求：其中IP地址为网关地址，MAC地址为网关设备与ACG互联三层接口的MAC地址（若网关设备与ACG设备之间还有多跳，则为距ACG最近一跳设备的转发三层出接口MAC，亦即ACG指向绑定网段路由下一跳IP的MAC），团体名为SNMP只读团体名即可

修改为正确的接口mac地址之后，用户归类正确

用户名	终端Mac	所属组	IP地址	认证方式
tianlibin		应用一组		静态绑定
tianlibin		应用一组		静态绑定
liyuebing		应用一组		静态绑定
zhangchen		应用一组		静态绑定
qianxueyu		应用三组		静态绑定
qianxueyu		应用三组		静态绑定
mashiguang		应用三组		静态绑定
mashiguang		应用三组		静态绑定
shilei		应用三组		静态绑定
shilei		应用三组		静态绑定
zhouyongwei		应用二组		静态绑定
litang		应用二组		静态绑定
zhouhailong		应用二组		静态绑定
qixingfu		应用二组		静态绑定
qixingfu		应用二组		静态绑定
liujunliang		应用二组		静态绑定

总结： 配置snmp跨三层mac学习是，要配置互联接口的mac。只要mac 是核心的都能 同步过来，但是如果不是直连接口的mac ， 用户mac是无法更新的。