某局点ACG100使用IMC联动Portal认证上网出现用户无法登录问题

ACG1000　孔凡安　2024-04-08 发表

组网及说明

不涉及

告警信息

不涉及

问题描述

某局点使用IMC联动Portal认证功能，配置完成后发现用户无法登录。

经IMC侧分析为ACG发送的Radius报文中没有携带正确的用户MAC。

Radius报文中对应用户mac的 字段为Calling-station-id ，如下所示，和IMC上记录到的用户mac不符导致登录失败。

```
<2024-03-22 14:32:44>   User-Name = "\025\002\021\310\303\~"
        NAS-Identifier = "58-B3-8F-37-50-3"
        User-Password = "Yyb3891963"
        Calling-Station-Id = "C4-07-78-2A-E0-01"
        Called-Station-Id = "58-B3-8F-37-50-3:bvi3"
        NAS-Port-Id = "trunk bvi3"
        Acct-Session-Id = "    791574:C4-07-78-2A-E0-01"
        NAS-IP-Address = 10.3.255.2
        Framed-IP-Address = 10.3.20.6
        NAS-Port = 1812
        NAS-Port-Type = Ethernet
        Cleartext-Password = "Yyb3891963"

<2024-03-22 14:32:44>
<2024-03-22 14:32:44> radius_read 1456 thread_cancel
<2024-03-22 14:32:44> Received Access-Reject(3) Id 249 from 10.3.1.51:1812 to 0.0.0.0:1812 length 66

<2024-03-22 14:32:44>   Reply-Message = "E63025: Failed to check MAC address binding."
```

过程分析

经过前面的分析，怀疑ACG到终端用户之间有其他三层设备，导致ACG携带的mac为和ACG直连的三层设备的mac。查看ACG的ARP表项，确实如此：

```
ShengH-ACG1000(DEBUG)# dsip arp
% Unknown command..[dsip arp]
ShengH-ACG1000(DEBUG)# disp arp
Codes:  V - neighbor's HW address is valid       S - static neighbor

-------------------------------------------------------------------------------
IP address         HW address          Device     Flags       State
-------------------------------------------------------------------------------
10.3.255.1         04:a9:59:3f:c3:f5   bvi3       V           REACHABLE
10.3.1.52          34:dc:99:7f:42:70   mgt0       V           STALE
10.3.255.3         c4:07:78:2a:e0:01   bvi3       V           REACHABLE
10.3.1.51          34:dc:99:7f:3b:60   mgt0       V           STALE
```

看了下现场的跨三层mac学习，发现存在问题。从终端到ACG之间有多个三层设备。下面说一下正确的配置方法：

下面说一下SNMP跨三层MAC学习的原理：

> SNMP跨三层mac地址学习数据包经过三层设备时，源目MAC地址会重新封装，当AC

> G部署在三层设备上游时无法直接从数据包中获取到终端的MAC信息。此时在在线用户中用户MAC地址显示为三层设备接口的MAC。若获取终端真实MAC，需要借助snmp协议，此时三层设备上开启该服务，ACG设备上配置交换机信息后。ACG会定时调用snmpwalk进程向三层交换机mib库at组节点中ip/mac对应关系信息获取到终端真实的MAC地址。由于脚本定期执行，因此终端MAC地址学习有一定延迟性。

某些情况下还需要开启mac敏感功能：

> user mac-sensitive 命令用来配置用户识别是否对MAC变化保持敏感。

【命令】

user mac-sensitive {enable | disable}

【视图】

(config)#视图

【参数】

enable：开启用户MAC敏感，用户MAC发生变化后会被踢下线重新识别。

disable：关闭用户MAC敏感。

【使用指导】

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。

【举例】

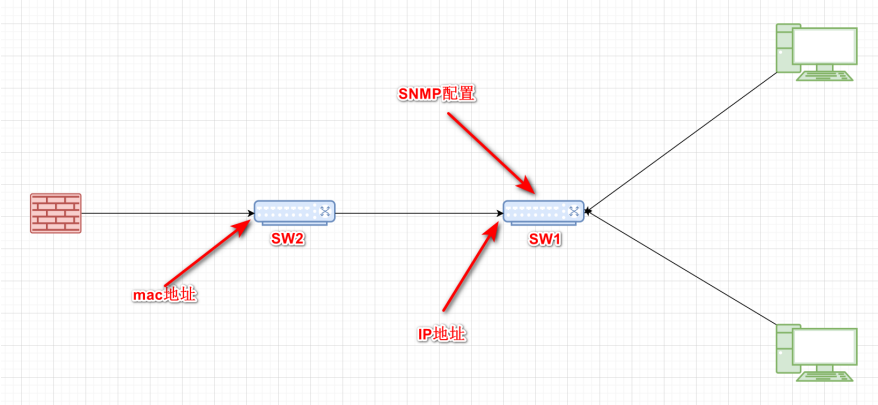
配置用户MAC敏感

Host(config)# user mac-sensitive enable 开启用户MAC敏感

Host (config)# user mac-sensitive disable 关闭用户MAC敏感

解决方法

方案如上，如下图示说明：



注：如上图示交换机均为三层交换机，要求ACG到填写IP地址的交换机SW1三层路由可达，即snmp读取的是该交换机上的ARP表项信息。