某局点BYOD认证不成功

MAC地址认证 **孙建刚** 2023-06-30 发表

组网及说明

无线集中转发组网，结合IMC做byod认证

问题描述

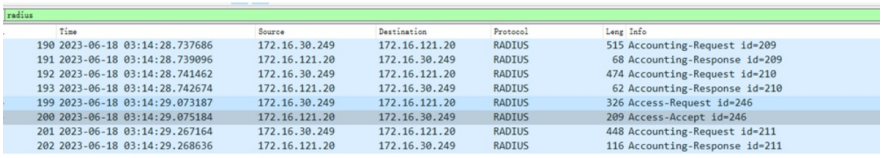
现场遇到问题有：

1、无法弹出认证页面；

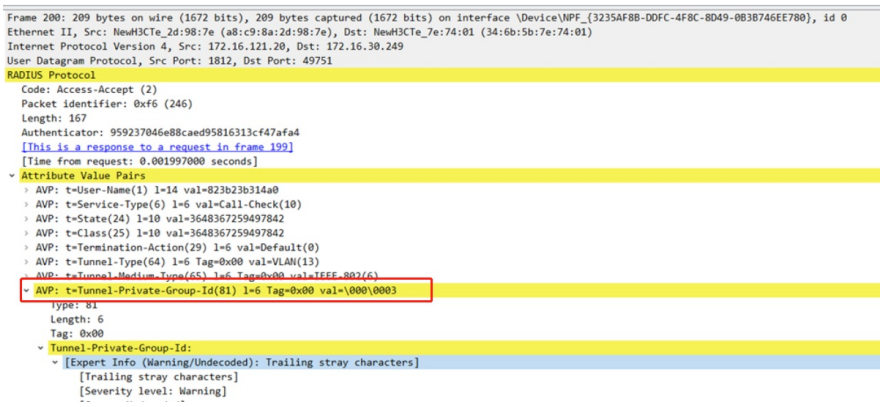
2、弹出认证页面后输入账号密码认证失败

过程分析

对于问题1，BYOD认证实际为MAC认证方式下EIA给匿名用户引用的接入规则下发启用portal认证的VLAN，利用portal的页面重定向功能将终端重定向到byod页面，并非真正的portal认证。所以第一步先检查是否完成MAC认证，并下通过radius报文下发正确VLAN，通过抓包分析：



No.	Time	Source	Destination	Protocol	Leng	Info
190	2023-06-18 03:14:28.737686	172.16.30.249	172.16.121.20	RADIUS	515	Accounting-Request id=209
191	2023-06-18 03:14:28.739096	172.16.121.20	172.16.30.249	RADIUS	68	Accounting-Response id=209
192	2023-06-18 03:14:28.741462	172.16.30.249	172.16.121.20	RADIUS	474	Accounting-Request id=210
193	2023-06-18 03:14:28.742674	172.16.121.20	172.16.30.249	RADIUS	62	Accounting-Response id=210
199	2023-06-18 03:14:29.073187	172.16.30.249	172.16.121.20	RADIUS	326	Access-Request id=246
200	2023-06-18 03:14:29.075184	172.16.121.20	172.16.30.249	RADIUS	209	Access-Accept id=246
201	2023-06-18 03:14:29.267164	172.16.30.249	172.16.121.20	RADIUS	448	Accounting-Request id=211
202	2023-06-18 03:14:29.268636	172.16.121.20	172.16.30.249	RADIUS	116	Accounting-Response id=211



```
Frame 200: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits) on interface \Device\NPF_{3235AF8B-DDFC-4F8C-8D49-0B3B746EE780}, id 0
Ethernet II, Src: NewH3CTe_2d:98:7e (a8:c9:8a:2d:98:7e), Dst: NewH3CTe_7e:74:01 (34:6b:5b:7e:74:01)
Internet Protocol Version 4, Src: 172.16.121.20, Dst: 172.16.30.249
User Datagram Protocol, Src Port: 1812, Dst Port: 49751
RADIUS Protocol
   Code: Access-Accept (2)
   Packet identifier: 0xf6 (246)
   Length: 167
   Authenticator: 959237046e88caed95816313cf47afa4
   [This is a response to a request in frame 199]
   [Time from request: 0.001997000 seconds]
Attribute Value Pairs
   AVP: t=User-Name(1) l=14 val=823b23b314a0
   AVP: t=Service-Type(6) l=6 val=Call-Check(10)
   AVP: t=State(24) l=10 val=3648367259497842
   AVP: t=Class(25) l=10 val=3648367259497842
   AVP: t=Termination-Action(29) l=6 val=Default(0)
   AVP: t=Tunnel-Type(64) l=6 Tag=0x00 val=VLAN(13)
   AVP: t=Tunnel-Medium-Type(65) l=6 Tag=0x00 val=IEEE-802(6)
   AVP: t=Tunnel-Private-Group-Id(81) l=6 Tag=0x00 val=\000\003
      Type: 81
      Length: 6
      Tag: 0x00
      Tunnel-Private-Group-Id:
         [Expert Info (Warning/Undecoded): Trailing stray characters]
            [Trailing stray characters]
            [Severity level: Warning]
```

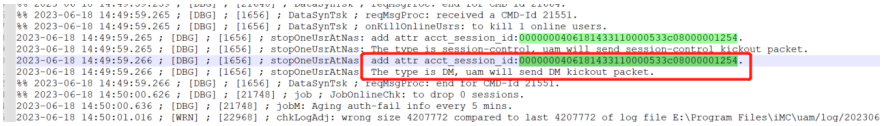
查看抓包服务器侧已经通过type81属性下发vlan，具体值（val=\000\003），终端也能拿到对应网段地址，但是依旧无任何portal页面，进一步查看配置，发现在该下发的vlan接口下未启用portal的配置，因此不会有重定向页面，补充相关配置即可：

```
#
interface Vlan-interface81
 ip address [redacted] 255.255.255.0
 portal enable method direct
 portal apply web-server macbyod
#
```

此时debugging portal redirect分析看设别可完成重定向动作，终端弹出BYOD认证页面：

*Jun 18 11:55:48:409 2023 AC1_E_172.16.xx.xx PORTAL/7/REDIRECT-EVENT: The user ip is 172.16.xx.xx; the redirect url is http://172.16.xx.xx:8080/byod?ssid=ycm%2Dwifi1&usermac=DE-8E-xx-xx-xx-xx&userip=172.16.xx.xx.

但是紧接着终端完成认证无法切到最终业务vlan。在新增接入用户时，可设置该用户为缺省BYOD用户（系统中尚不存在缺省BYOD用户时，该选项才可见）。缺省BYOD用户的帐号名固定为“byodanonymous”，且帐号密码不用再设置。MAC认证方式下，如果相应MAC地址没有和任何帐号名绑定，则使用缺省BYOD用户上线。用户上线后可以访问iMC注册页面注册一个访客帐号或者使用一个已知帐号与MAC地址绑定。MAC地址与帐号绑定成功后，系统会强制用户下线，重新认证时就会使用该MAC地址新绑定的帐号名。 此时在服务器侧可以看到有DM报文下发：



```
%% 2023-06-18 14:49:59.265 ; [DBG] ; [1656] ; DataSynTsk ; reqMsgProc: received a CMD-Id 21551.
%% 2023-06-18 14:49:59.265 ; [DBG] ; [1656] ; DataSynTsk ; onKillOnlineUsrs: to kill 1 online users.
2023-06-18 14:49:59.265 ; [DBG] ; [1656] ; stopOneUsrAtNas: add attr acct_session_id:00000004061814331100005330800001254.
2023-06-18 14:49:59.265 ; [DBG] ; [1656] ; stopOneUsrAtNas: The type is session-control, uam will send session-control kickout packet.
2023-06-18 14:49:59.266 ; [DBG] ; [1656] ; stopOneUsrAtNas: add attr acct_session_id:00000004061814331100005330800001254.
2023-06-18 14:49:59.266 ; [DBG] ; [1656] ; stopOneUsrAtNas: The type is DM, uam will send DM kickout packet.
%% 2023-06-18 14:49:59.266 ; [DBG] ; [1656] ; DataSynTsk ; reqMsgProc: end for CMD-Id 21551.
%% 2023-06-18 14:50:00.626 ; [DBG] ; [21748] ; job ; JobOnlineChk: to drop 0 sessions.
2023-06-18 14:50:00.636 ; [DBG] ; [21748] ; jobM: Aging auth-fail info every 5 mins.
2023-06-18 14:50:01.016 ; [WRN] ; [22968] ; chkLogAdj: wrong size 4207772 compared to last 4207772 of log file E:\Program Files\iMC\uam/log/202306
```

但是用户并没有下线，检查设备配置发现缺少RADIUS服务器使用session control报文向设备发送授权信息的动态修改请求以及断开连接请求。开启RADIUS session control功能后，设备会打开知名UDP端口1812来监听并接收RADIUS服务器发送的session control报文。

所以增加radius session-control enable配置即可解决。

解决方法

1、分配的业务vlan下需要起portal认证；

2、增加radius session-control enable控制功能