某局点通过Radius DM消息报文下发离线失败问题

Portal AAA **朱恺** 2023-04-18 发表

组网及说明

产品： WX3540X （用新款V9 AC替换之前的V5 AC）

现象： portal认证，radius服务器踢用户需要通过DAE下发DM消息给AC，在V5环境可以稳定可用，但是在V9 AC环境下发现无法踢用户。

问题描述

现象：portal认证，radius服务器踢用户需要通过DAE下发DM消息给AC，在V5环境可以稳定可用，但是在V9 AC环境下发现无法踢用户。

过程分析

对交互的radius报文进行抓包分析。按照acct-session-id进行检索区分

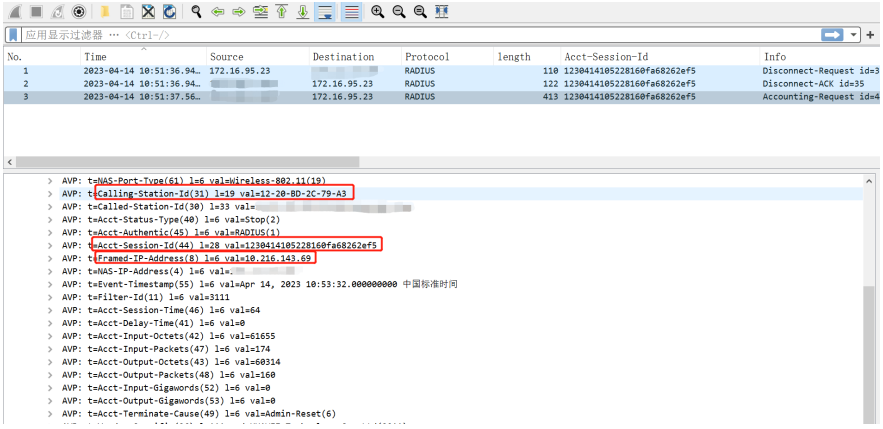
先看V5正常的报文内容：

1、V5环境的历史在线报文。

显示Acct-seesion-id为 1230414105228160fa68262ef5

Calling-station-id为12-20-BD-2C-79-A3

Framed-IP-Address为10.216.143.69

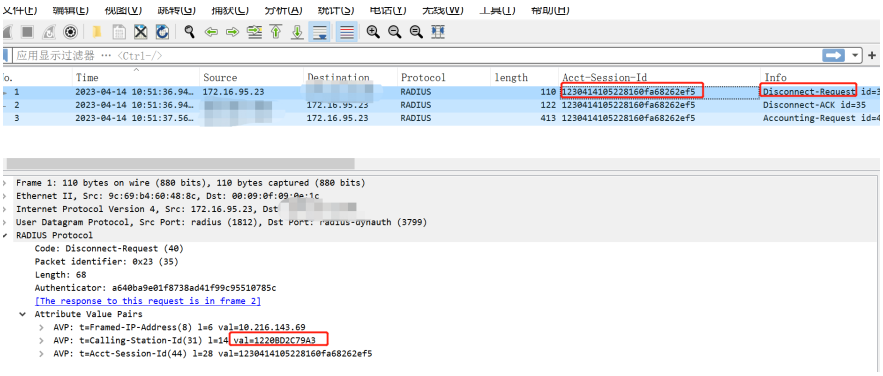


2、V5环境下AAA下发的DM请求消息内容

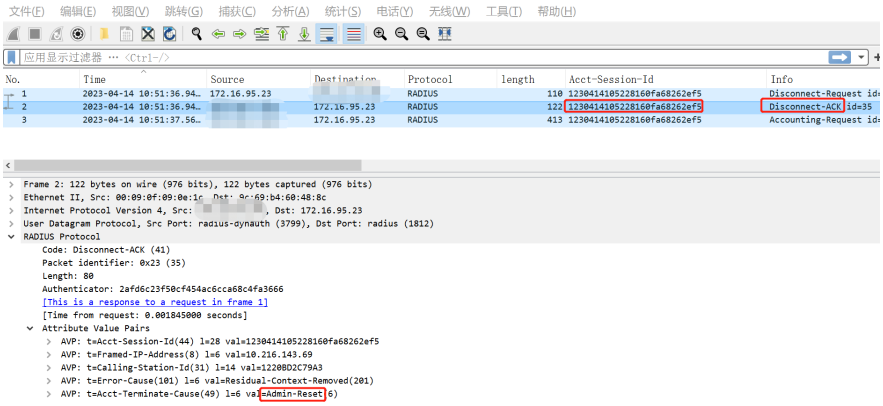
显示Acct-seesion-id为 1230414105228160fa68262ef5

Calling-station-id为1220BD2C79A3 //与AC记录的12-20-BD-2C-79-A3格式不太一样

Framed-IP-Address为10.216.143.69



3、V5环境下AC发的DM ACK内容



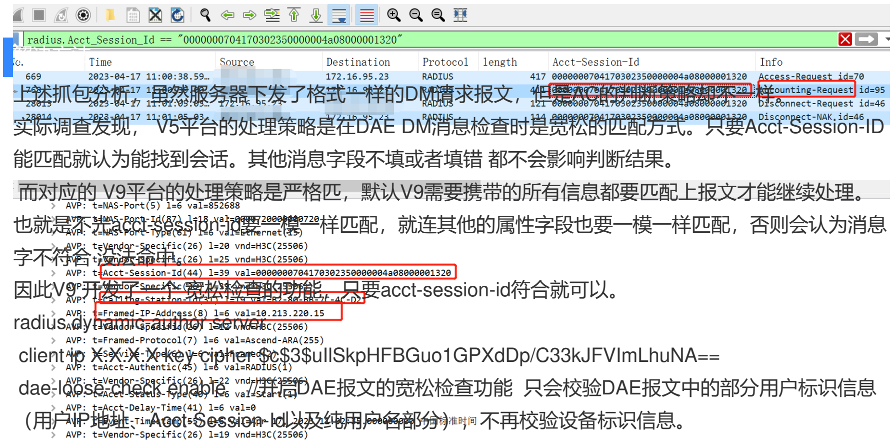
再看V9异常的报文内容：

1、V9环境的历史在线报文。

显示Acct-seesion-id为 00000007041703023500000004a08000001320

Calling-station-id为B2-80-BB-7C-4C-D2

Framed-IP-Address为10.213.220.15



上述抓包分析，虽然服务器下发了格式一样的DM请求报文，但是AC的判断策略不一样。
实际调查发现， V5平台的处理策略是在DAE DM消息检查时是宽松的匹配方式。只要Acct-Session-ID能匹配就认为能找到会话。其他消息字段不填或者填错 都不会影响判断结果。

而对应的 V9平台的处理策略是严格匹，默认V9需要携带的所有信息都要匹配上报文才能继续处理。
也就是不光acct-session-id要一模一样匹配，就连其他的属性字段也要一模一样匹配，否则会认为消息字不符合 没法命中。

因此V9开发了一个宽松检查的功能，只要acct-session-id符合就可以。

radius dynamic-author server

client ip X.X.X.X key cipher c3$ulISkpHFBGuo1GPXdDp/C33kJFVImLhuNA==

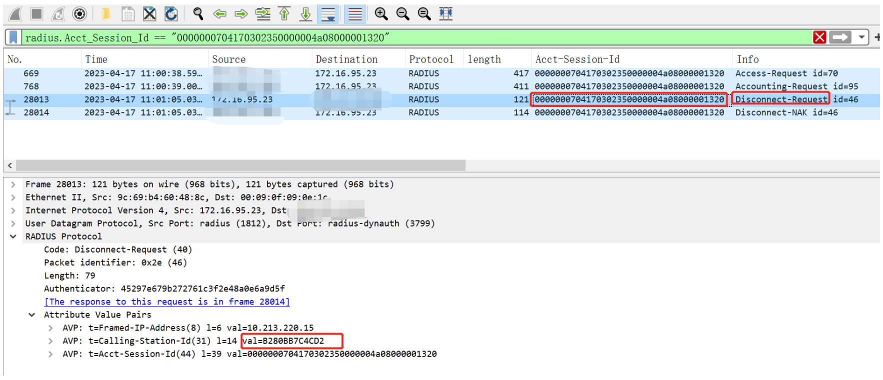
dae-loose-check enable //开启DAE报文的宽松检查功能 只会校验DAE报文中的部分用户标识信息（用户IP地址、Acct-Session-Id以及纯用户名部分），不再校验设备标识信息。

2、V9环境AAA下发的DM请求消息。

显示Acct-seesion-id为 000000070417030235000000 4a08000001320

Calling-station-id为B280BB7C4CD2 //格式风格不一样 没有携带"-"字符

Framed-IP-Address为10.213.220.15



3、V9环境AC回应的DM NAK消息。

显示没法发现这个会话信息