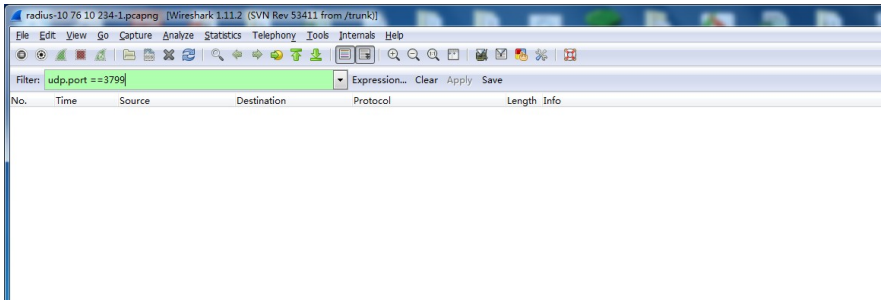
WX系列无线AC与国创对接Radius DM下线不成功处理案例

Portal AAA 赵杰 2016-08-11 发表

客户使用我司AC部署无线网络，用户接入网络之后需要portal认证才能访问内部资源以及公网，Portal服务器以及Radius服务器使用第三方国创设备，目前对接认证计费正常，无线用户portal认证成功正常，现测试在Radius服务器上使用DM报文让终端下线失败，Radius服务器上点击下线按钮之后用户依旧可以上网，在设备上查看认证表项依旧存在。
以下为AC Portal相关配置

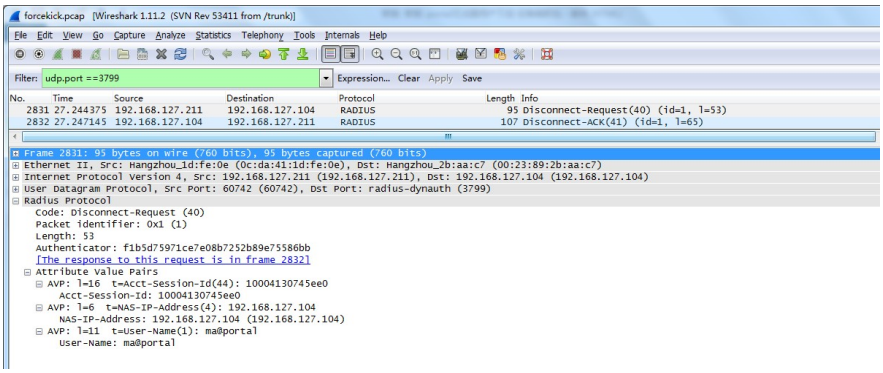
```
#
 portal server shijiazhuang ip 1.1.1.1 key cipher $c$3$VbFbQNOjHqLk6MkzbHSTYmDDP+EG0lrJROlDjxWPcy9dM3w= url http://1.1.1.1:8081 server-type cmcc
 portal url-param include nas-id param-name nasid
 portal url-param include user-mac param-name srcmac
 portal url-param include nas-ip param-name acip
 portal url-param include ap-mac param-name apmac
 portal url-param include user-ip param-name srcip
 portal url-param include ac-name param-name sysname
 portal url-param include ssid
 portal url-param include nas-port-id param-name nasportid
#
domain shijiazhuang
 authentication portal radius-scheme shijiazhuang
 authorization portal radius-scheme shijiazhuang
 accounting portal radius-scheme shijiazhuang
 access-limit disable
 state active
 idle-cut enable 15 1
 self-service-url disable
#
 radius scheme shijiazhuang
  primary authentication 1.1.1.1 key cipher $c$3$Bz8CGEjitkvrlvG8RijB9XOiXZBSyo+CHA==
  primary accounting 1.1.1.1 key cipher $c$3$xvTIb/a4O38ejsvdOpi2bPdbwF41VtoMHA==
  secondary authentication 1.1.1.1 key cipher $c$3$9//QjhwPuXcYXbY+B68WEqwlE21LRqELTA==
  secondary accounting 1.1.1.1 key cipher $c$3$dgk5FeR0pfj5QviHQ2zkwHYfs68YQ08a3g==
  user-name-format without-domain
  nas-ip 1.1.1.2
#
 interface Vlan-interface221
  ip address 2.2.2.2 255.255.255.0
  dhcp select relay
  dhcp relay server-select 1
  portal server shijiazhuang method direct
  portal domain shijiazhuang
  portal nas-ip 1.1.1.2
 #
```

现场AC是V5软件版本，在V5软件版本上，配置radius scheme之后设备默认支持DM下线，使用的端口为UDP 3799，即AC上不需要配置任何命令就支持DM下线。Radius服务器上通过点击用户下线触发DM下线报文，现服务器上点击下线之后设备认证表项依旧存在问题，初步怀疑设备未收到DM下线报文或者收到的DM下线报文格式错误，为定位现场问题，在AC侧镜像抓包分析。
第一次测试：无线用户连接网络并通过portal认证，在radius服务器WEB页面上点击用户下线，触发Radius服务器发送DM下线报文，在AC侧镜像抓包中使用udp.port == 3799 过滤报文，检查是否有DM报文以及报文格式是否正确：

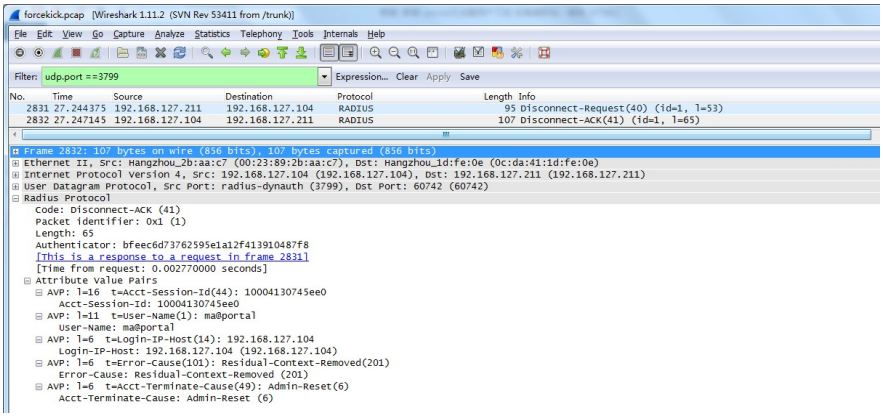


在抓取的报文中过滤发现没有DM下线报文，联系radius服务器检查确认，服务器侧检查之后发现WEB页面点击下线之后调用DM下线程序失败，所以服务器侧没有发送下线报文，服务器侧希望我司提供标准的下线报文，于是在实验室IMC认证环境中抓取了一个标准的DM下线交互报文：

a.imc发给设备的DM下线请求报文：

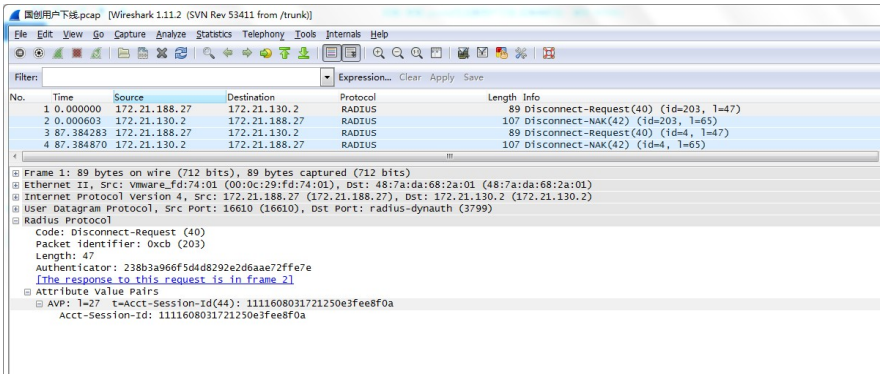


b.设备回应给imc的DM下线ACK报文



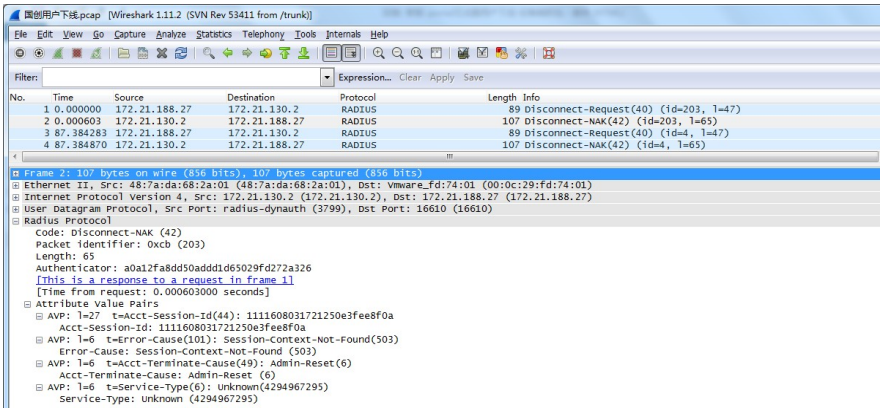
第二次测试：服务器上使用命令触发DM下线，AC侧抓包过滤udp.port == 3799，过滤发现存在DM下线报文，但是设备识别存在问题，导致用户下线失败：

a.Radius服务器发送给设备的DM下线请求报文：



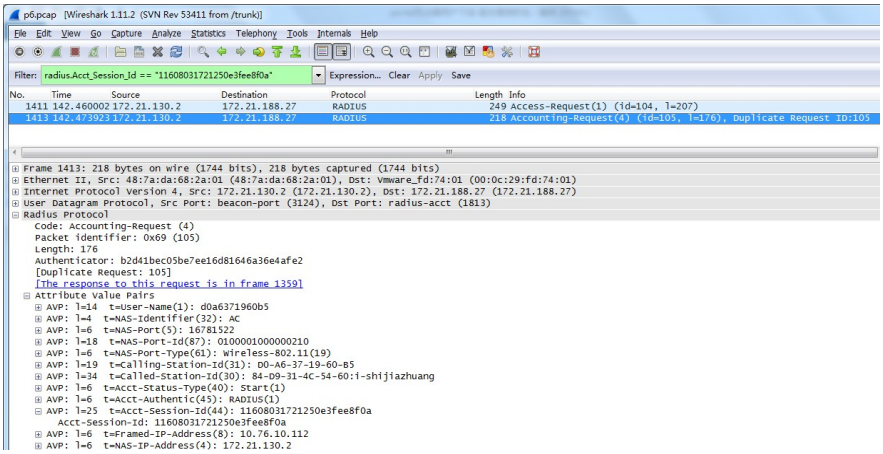
对比IMC发送的下线请求报文，国创发送的DM下线请求报文缺少1号属性和4号属性

b.设备回复的DM下线报文



抓包中设备回应了NAK报文，说明AC接收DM下线报文处理用户下线失败，查看101号属性Error-Cause提示未找到对应会话（context-not-found），AC处理用户下线不成功。联系国创反馈触发DM下线的命令：[root@Portal_Server_01 ~]# echo Acct-Session-Id=11608031721250e3fee8f0a | /opt/freeradius-server/bin/radclient 172.21.130.2:3799 disconnect "secret"

通过国创提供的命令中session-id查询认证报文，可以找到对应的计费请求报文：



通过对比国创下线命令 、计费报文以及国创下线报文中的Acct-Session-Id，发现国创下线命令和上线计费报文中的Acct-Session-Id相同均为11608031721250e3fee8f0a，而DM下线报文中的Acct-Session-Id为11116080031721250e3fee8f0a，相比计费报文左侧多了两个数字1。也就是国创Radius服务器命令下线Acct-Session-Id=11608031721250e3fee8f0a，服务器实际发出的Acct-Session-Id=11116080031721250e3fee8f0a，将相关分析数据发给国创分析更改。

服务器更改软件之后重新测试，客户端DM下线成功，设备上删除认证表项，现场DM下线问题解决。