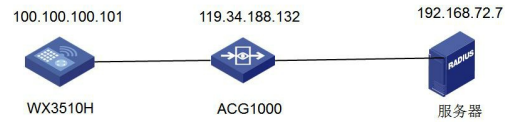
某局点WX3510H配合第三方服务器强制用户下线不生效

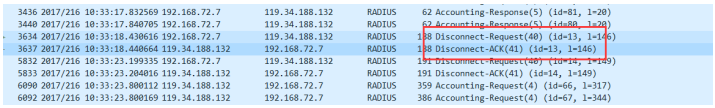
Portal AAA 陈孙潇 2017-09-14 发表

某局点使用我司WX3510H无线控制器和第三方厂商对接portal认证，测试发现portal认证等基本功能都正常，但是从服务器上踢用户下线不生效。服务器侧工程师抓包反馈服务器已经正常发出下线报文，AC侧也正常回应了，但是用户就是无法下线，因此现场怀疑AC端存在问题。收到信息后，我们立即投入力量进行分析。
现场大致组网拓扑：



其中ACG上作了NAT映射，将公网口地址119.34.188.132映射到AC上的nas-ip地址100.100.100.101。

1、服务器上抓包结果如下：



可以看到服务器上发起了下线请求（Disconnect-Request）,设备上也回包同意了服务器的请求（Disconnect-Ack），正常情况下终端应该下线，但是通过dis portal user查看仍然看到对应的终端在线，且该终端也能正常访问网络。因此怀疑AC端存在问题。

2、查看AC配置：

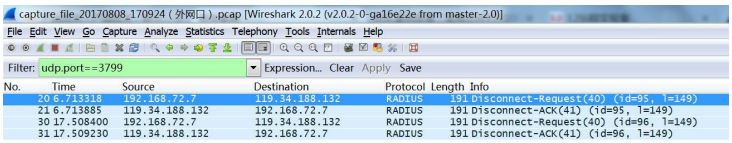
```
interface Vlan-interface3900
 ip address 10.50.255.254 255.255.0.0
 ip address 10.50.255.252 255.255.0.0 sub
 portal enable method direct
 portal domain weixin_neiwang
 portal bas-ip 100.100.100.101
 portal apply web-server zjzy
portal web-server zjzy
 url http://192.168.72.7:8080/am/portal/serviceId/SN7279365752/ac/H3C/ssid/FYBJY
 server-type cmcc
 url-parameter ap-mac ap-mac
 url-parameter source-address source-address
 url-parameter source-mac source-mac
 url-parameter ssid ssid
radius session-control enable
 radius scheme weixin
 primary authentication 116.199.5.7
 primary accounting 116.199.5.7
 accounting-on enable
 accounting-on extended
 key authentication cipher $c$3$WwrvWRvLNT/GXFj1FYtZg64SPuYHkskEVfQW
 key accounting cipher $c$3$LMegr5OiT62LxKeFiWfuUXcHtRvKBqM1ir8A
 timer realtime-accounting 5
 user-name-format without-domain
 nas-ip 100.100.100.101
```

查看设备基本portal和radius配置，没有问题。但是发现设备上没有配置dae server，于是联系现场配置dae server。

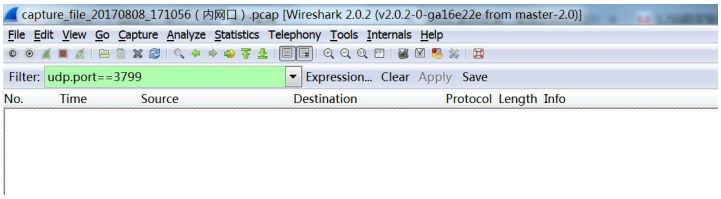
```
radius dynamic-author server
    client ip 192.168.72.7
```

但是现场修改完配置后测试发现依旧不生效，服务器端的抓包结果依旧与之前相同。

3、在排除AC端配置问题后，于是便收集AC的debug portal all和debug radius all信息以确认报文交互过程是否有异常。但是查看debug却没有看到任何下线相关的报文信息。这就比较奇怪了，既然设备回应了disconnect-ack报文，正常来说设备上是能够看到相应的debug信息的。因此怀疑是否上行的ACG上出现了问题。于是便在ACG的内外网口同时抓包确认。
外网口抓包结果：



内网口抓包结果：



可以看到外网口正常抓到了源目地址为ACG和服务器的下线报文，但是内网口却抓不到对应的报文，怀疑ACG没有将报文正常透传到内网。也刚好证实了为何debug信息里看不到下线报文。

4、查询ACG上相关配置，发现设备在配置nat server时，将下线报文的3799端口号配置成了源端口，而正确的配置应该是配置为目的端口，因为AC设备处于ACG后的内网。

		名称	内容(协议:端口开始-端口结束)	引用	描述	操作
1		shld2000	UDP目的端口:2000-2000源端口:0-65535	1		
2		shld3799	UDP目的端口:0-65535源端口:3799-3799	1		
3		shld50100	UDP目的端口:50100-50100源端口:0-65535	1		
4		udp1812	UDP目的端口:1812-1812源端口:0-65535	0		
5		udp1813	UDP目的端口:1813-1813源端口:0-65535	0		

在现场将ACG上的nat server修改完毕后，此时再在服务器上点击强制下线时，终端正常下线了。

修改ACG设备的nat映射配置后解决。