某局点无线1x认证客户端地址变化后不回复计费报文

802.1X AAA 郭文浩 2021-09-26 发表

组网及说明

客户AC型号WX3520h 版本R5433P03，对接第三方服务器做了1x认证

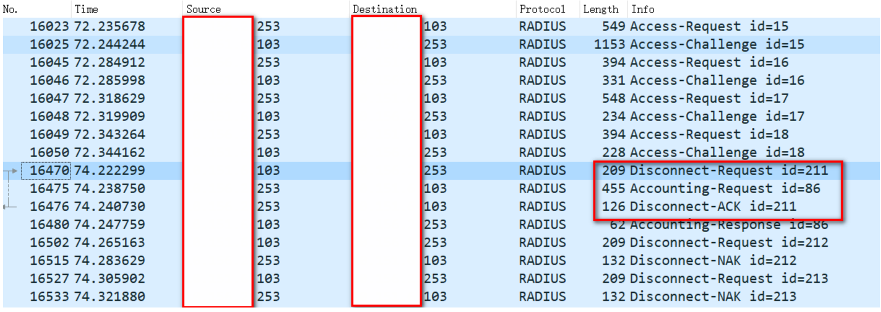
问题描述

客户第三方服务器有安全合规检测，终端正常认证（合规检查通过）拿x.71地址，合规不通过拿y.7地址，x.71是vlan103，y.7是vlan112

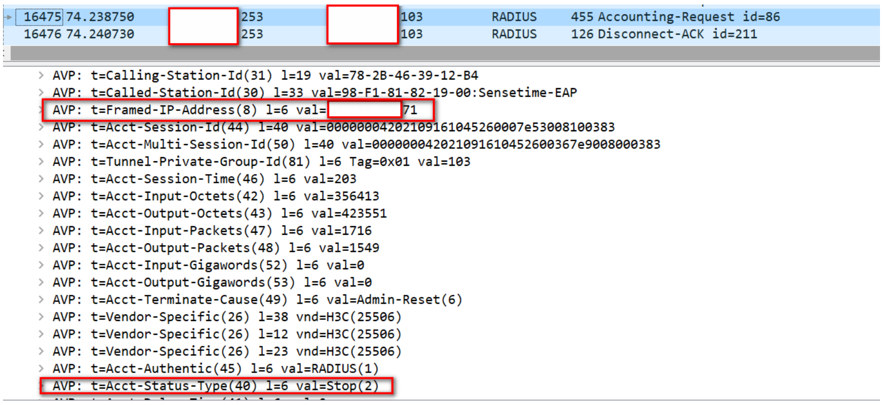
当手动删除合规软件时，服务器踢终端下线重新拿地址后不再回复计费报文，导致安装好合规软件后无法拿正常的x.71地址

过程分析

查看抓包信息



```
No.     Time        Source            Destination        Protocol  Length  Info
16023 72.235678  [redacted]253   [redacted]103   RADIUS   549 Access-Request id=15
16025 72.244244  [redacted]103   [redacted]253   RADIUS  1153 Access-Challenge id=15
16045 72.284912  [redacted]253   [redacted]103   RADIUS   394 Access-Request id=16
16046 72.285998  [redacted]103   [redacted]253   RADIUS   331 Access-Challenge id=16
16047 72.318629  [redacted]253   [redacted]103   RADIUS   548 Access-Request id=17
16048 72.319909  [redacted]103   [redacted]253   RADIUS   234 Access-Challenge id=17
16049 72.343264  [redacted]253   [redacted]103   RADIUS   394 Access-Request id=18
16050 72.344162  [redacted]103   [redacted]253   RADIUS   228 Access-Challenge id=18
16470 74.222299  [redacted]103   [redacted]253   RADIUS   209 Disconnect-Request id=211
16475 74.238750  [redacted]253   [redacted]103   RADIUS   455 Accounting-Request id=86
16476 74.240730  [redacted]253   [redacted]103   RADIUS   126 Disconnect-ACK id=211
16480 74.247759  [redacted]103   [redacted]253   RADIUS    62 Accounting-Response id=86
16502 74.265163  [redacted]103   [redacted]253   RADIUS   209 Disconnect-Request id=212
16515 74.283629  [redacted]253   [redacted]103   RADIUS   132 Disconnect-NAK id=212
16527 74.305902  [redacted]103   [redacted]253   RADIUS   209 Disconnect-Request id=213
16533 74.321880  [redacted]253   [redacted]103   RADIUS   132 Disconnect-NAK id=213
```

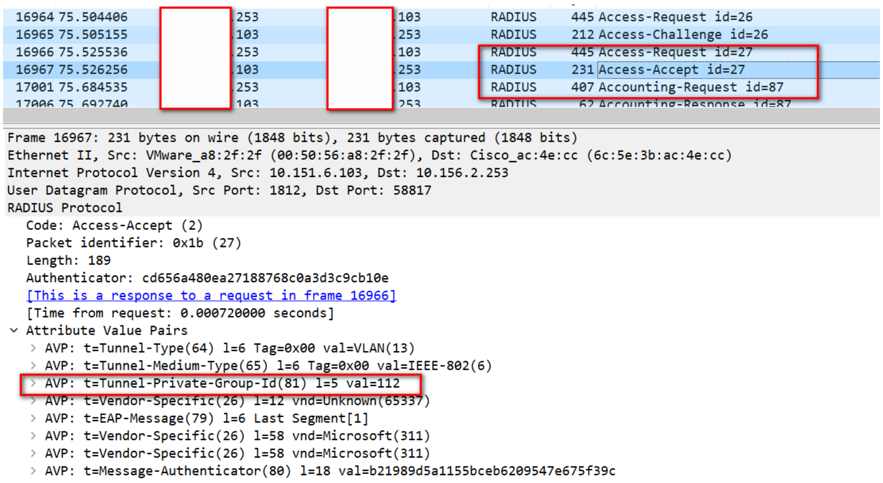


```
16475 74.238750  [redacted]253   [redacted]103   RADIUS   455 Accounting-Request id=86
16476 74.240730  [redacted]253   [redacted]103   RADIUS   126 Disconnect-ACK id=211

    > AVP: t=Calling-Station-Id(31) l=19 val=78-2B-46-39-12-B4
    > AVP: t=Called-Station-Id(30) l=33 val=98-F1-81-82-19-00:Sensetime-EAP
    > AVP: t=Framed-IP-Address(8) l=6 val=[redacted]71
    > AVP: t=Acct-Session-Id(44) l=40 val=00000004202109161045260007e53008100383
    > AVP: t=Acct-Multi-Session-Id(50) l=40 val=000000042021091610452600367e9008000383
    > AVP: t=Tunnel-Private-Group-Id(81) l=6 Tag=0x01 val=103
    > AVP: t=Acct-Session-Time(46) l=6 val=203
    > AVP: t=Acct-Input-Octets(42) l=6 val=356413
    > AVP: t=Acct-Output-Octets(43) l=6 val=423551
    > AVP: t=Acct-Input-Packets(47) l=6 val=1716
    > AVP: t=Acct-Output-Packets(48) l=6 val=1549
    > AVP: t=Acct-Input-Gigawords(52) l=6 val=0
    > AVP: t=Acct-Output-Gigawords(53) l=6 val=0
    > AVP: t=Acct-Terminate-Cause(49) l=6 val=Admin-Reset(6)
    > AVP: t=Vendor-Specific(26) l=38 vnd=H3C(25506)
    > AVP: t=Vendor-Specific(26) l=12 vnd=H3C(25506)
    > AVP: t=Vendor-Specific(26) l=23 vnd=H3C(25506)
    > AVP: t=Acct-Authentic(45) l=6 val=RADIUS(1)
    > AVP: t=Acct-Status-Type(40) l=6 val=Stop(2)
```

第一次COA（使用授权更改）和account-stop

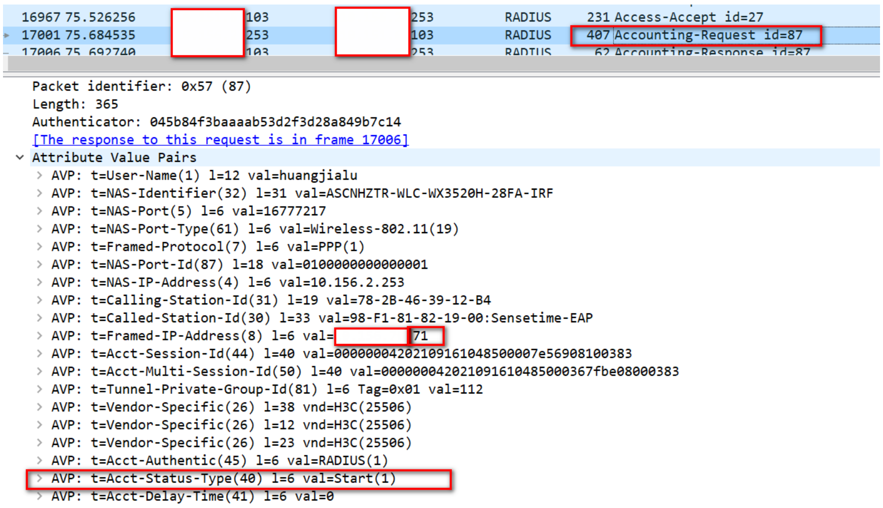
终端地址是x.71



```
16964 75.504406  [redacted].253   [redacted].103   RADIUS   445 Access-Request id=26
16965 75.505155  [redacted].103   [redacted].253   RADIUS   212 Access-Challenge id=26
16966 75.525536  [redacted].253   [redacted].103   RADIUS   445 Access-Request id=27
16967 75.526256  [redacted].103   [redacted].253   RADIUS   231 Access-Accept id=27
17001 75.684535  [redacted].253   [redacted].103   RADIUS   407 Accounting-Request id=87
17006 75.692740  [redacted].103   [redacted].253   RADIUS    62 Accounting-Response id=87

Frame 16967: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits)
Ethernet II, Src: VMware_a8:2f:2f (00:50:56:a8:2f:2f), Dst: Cisco_ac:4e:cc (6c:5e:3b:ac:4e:cc)
Internet Protocol Version 4, Src: 10.151.6.103, Dst: 10.156.2.253
User Datagram Protocol, Src Port: 1812, Dst Port: 58817
RADIUS Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x1b (27)
  Length: 189
  Authenticator: cd656a480ea27188768c0a3d3c9cb10e
  [This is a response to a request in frame 16966]
  [Time from request: 0.000720000 seconds]
v Attribute Value Pairs
   > 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=5 val=112
   > AVP: t=Vendor-Specific(26) l=12 vnd=Unknown(65337)
   > AVP: t=EAP-Message(79) l=6 Last Segment[1]
   > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
   > AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
   > AVP: t=Message-Authenticator(80) l=18 val=b21989d5a1155bceb6209547e675f39c
```

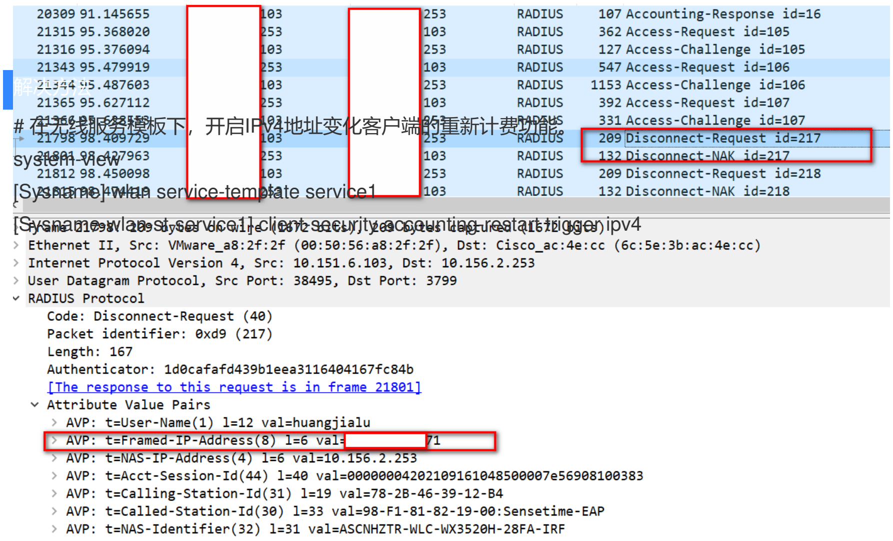
用户下线后，重新认证，获取vlan12



```
16967 75.526256  [redacted]103   [redacted]253   RADIUS   231 Access-Accept id=27
17001 75.684535  [redacted]253   [redacted]103   RADIUS   407 Accounting-Request id=87
17006 75.692740  [redacted]103   [redacted]253   RADIUS    62 Accounting-Response id=87

   Packet identifier: 0x57 (87)
   Length: 365
   Authenticator: 045b84f3baaaab53d2f3d28a849b7c14
   [The response to this request is in frame 17006]
 v Attribute Value Pairs
    > AVP: t=User-Name(1) l=12 val=huangjialu
    > AVP: t=NAS-Identifier(32) l=31 val=ASCNHZTR-WLC-WX3520H-28FA-IRF
    > AVP: t=NAS-Port(5) l=6 val=16777217
    > AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    > AVP: t=Framed-Protocol(7) l=6 val=PPP(1)
    > AVP: t=NAS-Port-Id(87) l=18 val=0100000000000001
    > AVP: t=NAS-IP-Address(4) l=6 val=10.156.2.253
    > AVP: t=Calling-Station-Id(31) l=19 val=78-2B-46-39-12-B4
    > AVP: t=Called-Station-Id(30) l=33 val=98-F1-81-82-19-00:Sensetime-EAP
    > AVP: t=Framed-IP-Address(8) l=6 val=[redacted]71
    > AVP: t=Acct-Session-Id(44) l=40 val=00000004202109161048500007e56908100383
    > AVP: t=Acct-Multi-Session-Id(50) l=40 val=000000042021091610485000367fbe08000383
    > AVP: t=Tunnel-Private-Group-Id(81) l=6 Tag=0x01 val=112
    > AVP: t=Vendor-Specific(26) l=38 vnd=H3C(25506)
    > AVP: t=Vendor-Specific(26) l=12 vnd=H3C(25506)
    > AVP: t=Vendor-Specific(26) l=23 vnd=H3C(25506)
    > AVP: t=Acct-Authentic(45) l=6 val=RADIUS(1)
    > AVP: t=Acct-Status-Type(40) l=6 val=Start(1)
    > AVP: t=Acct-Delay-Time(41) l=6 val=0
```

此时终端地址已经是y.7，但是account-start报文里的ip还是x.71



```
20309 91.145655 [redacted]103 [redacted]253 RADIUS  107 Accounting-Response id=16
21315 95.368020 [redacted]253 [redacted]103 RADIUS  362 Access-Request id=105
21316 95.376094 [redacted]103 [redacted]253 RADIUS  127 Access-Challenge id=105
21343 95.479919 [redacted]253 [redacted]103 RADIUS  547 Access-Request id=106
21344 95.487603 [redacted]103 [redacted]253 RADIUS 1153 Access-Challenge id=106
21365 95.627112 [redacted]253 [redacted]103 RADIUS  392 Access-Request id=107
21366 95.628553 [redacted]103 [redacted]253 RADIUS  331 Access-Challenge id=107
21798 98.409729 [redacted]103 [redacted]253 RADIUS  209 Disconnect-Request id=217
21801 98.427963 [redacted]253 [redacted]103 RADIUS  132 Disconnect-NAK id=217
21812 98.450098 [redacted]103 [redacted]253 RADIUS  209 Disconnect-Request id=218
21815 98.474419 [redacted]253 [redacted]103 RADIUS  132 Disconnect-NAK id=218

> Frame 21798: 209 bytes on wire (1672 bits), 209 bytes captured (1672 bits)
> Ethernet II, Src: VMware_a8:2f:2f (00:50:56:a8:2f:2f), Dst: Cisco_ac:4e:cc (6c:5e:3b:ac:4e:cc)
> Internet Protocol Version 4, Src: 10.151.6.103, Dst: 10.156.2.253
> User Datagram Protocol, Src Port: 38495, Dst Port: 3799
v RADIUS Protocol
    Code: Disconnect-Request (40)
    Packet identifier: 0xd9 (217)
    Length: 167
    Authenticator: 1d0cafafd439b1eea3116404167fc84b
    [The response to this request is in frame 21801]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=12 val=huangjialu
    > AVP: t=Framed-IP-Address(8) l=6 val=[redacted]71
    > AVP: t=NAS-IP-Address(4) l=6 val=10.156.2.253
    > AVP: t=Acct-Session-Id(44) l=40 val=00000004202109161048500007e56908100383
    > AVP: t=Calling-Station-Id(31) l=19 val=78-2B-46-39-12-B4
    > AVP: t=Called-Station-Id(30) l=33 val=98-F1-81-82-19-00:Sensetime-EAP
    > AVP: t=NAS-Identifier(32) l=31 val=ASCNHZTR-WLC-WX3520H-28FA-IRF
```

解决方法

# 在无线服务模板下，开启IPv4地址变化客户端的重新计费功能。

```
system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security accounting-restart trigger ipv4
```

所以第二次COA时，请求的地址还是70.71，ac回复没有此会话