某局点 WX3540H V7无线网络中部分终端MAC+PSK密码认证失败问题排查

MAC地址认证 wlan安全 **徐猛** 2018-03-18 发表

现场使用我司的V7无线控制器WX3540H替换网络中的原有的WX3510E设备，原有网络中终端上线使用的认证方式为MAC+PSK认证，终端先经过网络中的一个radius服务器进行MAC认证后再进行PSK的认证。在指导现场工程师将V5无线控制器的命令转为V7的命令后，发现部分终端能够上网，部分终端不能上网，出现该问题后，我们立即投入了问题分析当中。（为避免纠纷，本案例中部分信息使用*进行隐匿）

终端连接入相应的SSID后始终获取不到地址。考虑到mac认证为二层认证，只有基于mac的认证成功后，终端才能正常的获取地址，怀疑是现场mac认证阶段未成功。

1.首先检查了现场V7无线控制器的配置：

```
#
radius scheme mac_authen
 primary authentication 80.52.*.*
 primary accounting 80.52.*.*
 secondary authentication 81.52.*.*
 secondary accounting 81.52.*.*
 key authentication cipher $c$3$m7ZSPvpxsD/CPR97Yhzb1fk3lnPW3L8g
 key accounting cipher $c$3$fOo7ulkFW/ZB8QJh/1Ae22ZY5xdmOG0j
 user-name-format without-domain
 nas-ip 84.32.*.*
#
domain mac_authen
 authentication lan-access radius-scheme mac_authen none
 authorization lan-access radius-scheme mac_authen none
 accounting lan-access radius-scheme mac_authen none
#
wlan service-template 1
 ssid C**
 vlan 1400
 beacon ssid-hide
 client forwarding-location ap
 akm mode psk
 preshared-key pass-phrase cipher $c$3$sCYBbRfLfr+n3G5W9GC98SIDNx0GOTTeCyxUQw==
 cipher-suite ccmp
 security-ie rsn
 client-security authentication-mode mac
 mac-authentication domain mac_authen
 service-template enable
#
```

检查配置未发现问题

2.让现场收集下面两条debug信息并分析：

debugging mac-authentication all

debugging radius all

内容如下：

```
*Jan 30 00:42:23:508 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Found request context, dstIP: 80.52.*.*; dstPort: 1812; VPN instance: --(public); socketfd: 353; pktID:
94.
*Jan 30 00:42:23:509 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Retransmitting request packet, currentTries: 3, maxTries: 3.
*Jan 30 00:42:24:258 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
*Jan 30 00:42:24:258 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
PAM_RADIUS: Sent authentication request successfully.
*Jan 30 00:42:24:258 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Processing AAA request data.
*Jan 30 00:42:24:258 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Got request data successfully, primitive: authentication.
```

*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Getting RADIUS server info.
*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Got RADIUS server info successfully.
*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Created request context successfully.
*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Created request packet successfully, dstIP: 80.52.*.*, **dstPort: 1812,** VPN instance: --(public), socket Fd: 353, pktID: 97. //**构造向radius认证端口发送的认证请求报文**
*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Added packet socketfd to epoll successfully, socketFd: 353.
*Jan 30 00:42:24:259 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Mapped PAM item to RADIUS attribute successfully.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Got RADIUS username format successfully, format: 2.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Added attribute user-name successfully, user-name: f431c33b****.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Filled RADIUS attributes in packet successfully.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Composed request packet successfully.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Created response timeout timer successfully.
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/PACKET:
User-Name="f431c33b**"** //**mac认证的用户名信息**
User-Password=****** //**mac认证的用户密码信息**
Service-Type=Call-Check
Framed-Protocol=PPP
NAS-Identifier="JR35AC0A-A4-3F****"
NAS-Port=600
NAS-Port-Type=Wireless-802.11
NAS-Port-Id="VLANID=600;"
Calling-Station-Id="F4-31-C3-3B-36-AB"
Called-Station-Id="AC-74-09-73-79-60:Cinda Mobile"
Acct-Session-Id="00000004201801291642240001 21c308100470"
H3c-User-Vlan-Id=600
H3c-Ip-Host-Addr="0.0.0.0 f4:31:c3:3b:36:ab"
NAS-IP-Address=84.32.*.* //**nas的ip地址为84.32.*.***
H3c-Product-Id="H3C WX3540H"
H3c-Nas-Startup-Timestamp=1516550284
*Jan 30 00:42:24:260 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:
Sent request packet successfully.
*Jan 30 00:42:24:261 2018 JR35AC0A-A4-3FDC05 RADIUS/7/PACKET:
01 61 01 1a 60 f4 ec 24 ac 27 a3 5b 1b 1d 38 07 //**radius的code为01，代表由client设备向服务器设备发送认证求情报文**
b1 9c 81 e2 01 0e 66 34 33 31 63 33 33 62 33 36
61 62 02 12 8b 44 c5 b0 74 8f d6 7c 32 51 fe 95
a8 2e 3a 19 06 06 00 00 00 0a 07 06 00 00 00 01
20 14 4a 52 33 35 41 43 30 41 2d 41 34 2d 33 46
44 43 30 35 05 06 00 00 02 58 3d 06 00 00 00 13
57 0d 56 4c 41 4e 49 44 3d 36 30 30 3b 1f 13 46
34 2d 33 31 2d 43 33 2d 33 42 2d 33 36 2d 41 42
1e 20 41 43 2d 37 34 2d 30 39 2d 37 33 2d 37 39
2d 36 30 3a 43 69 6e 64 61 20 4d 6f 62 69 6c 65
2c 28 30 30 30 30 30 30 30 34 32 30 31 38 30 31
32 39 31 36 34 32 32 34 30 30 30 31 32 31 63 33
30 38 31 30 30 34 37 30 1a 0c 00 00 63 a2 85 06
00 00 02 58 1a 21 00 00 63 a2 3c 1b 30 2e 30 2e
30 2e 30 20 66 34 3a 33 31 3a 63 33 3a 33 62 3a
*Jan 30 00:42:24:261 2018 JR35AC0A-A4-3FDC05 RADIUS/7/PACKET:
33 36 3a 61 62 04 06 54 20 cf 22 1a 13 00 00 63
a2 ff 0d 48 33 43 20 57 58 33 35 34 30 48 1a 0c
00 00 63 a2 3b 06 5a 64 b8 8c
*Jan 30 00:42:24:261 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:

Sent request packet and create request context successfully. /构造请求报文并发送请求报文成功

*Jan 30 00:42:24:261 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:

Added request context to global table successfully.

*Jan 30 00:42:24:261 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:

Processing AAA request data.

*Jan 30 00:42:24:507 2018 JR35AC0A-A4-3FDC05 RADIUS/7/EVENT:

Response timed out. /响应超时

至此我们发现我们的AC设备已经正常的将radius的认证请求报文发出，但是并未收到服务器侧的回应，引导现场工程师协调radius服务器工程师进行服务器侧配置以及响应的排查后，发现认证使用的服务器侧地址对端口等做了限制导致回包异常，修改服务器侧配置后解决。

根据debug过程分析发现服务器侧未响应，现场排查服务器侧问题后解决。

1.今后遇到AAA认证类的问题时，可以先检查配置，如果配置暂时未发现问题，可以通过debug的方式进行查看协议报文的交换过程来定位问题。

2.同时radius认证使用的是1812端口来做认证/授权,使用1813端口来做计费，需要确保这两个端口可用。尤其类似这种涉及三方配合类的问题时，需要通过debug等手段定位问题所在。

3.对于AAA认证类的问题，可以通过查看radius报文的code值来看认证进行到了那个阶段，radius的code值说明如下：

Code	报文类型	报文说明
1	Access-Request认证请求包	方向Client->Server，Client将用户信息传输到Server，请求Server对用户身份进行验证。该报文中必须包含User-Name属性，可选包含NAS-IP-Address、User-Password、NAS-Port等属性
2	Access-Accept认证接受包	方向Server->Client，如果Access-Request报文中的所有Attribute值都可以接受（即认证通过），则传输该类型报文
3	Access-Reject认证拒绝包	方向Server->Client，如果Access-Request报文中存在任何无法被接受的Attribute值（即认证失败），则传输该类型报文
4	Accounting-Request计费请求包	方向Client->Server，Client将用户信息传输到Server，请求Server开始/停止计费。该报文中的Acct-Status-Type属性用于区分计费开始请求和计费结束请求
5	Accounting-Response计费响应包	方向Server->Client，Server通知Client已经收到Accounting-Request报文，并且已经正确记录计费信息