

某局点WX3510E 短信认证结合迈普服务器对接失败问题处理经验案例

wlan接入 Portal SSID 刘文峰 2018-12-13 发表

组网及说明

无

问题描述

某局点采用WX3540E 无线控制器做短信认证结合迈普服务器对接，但是发现对接失败，portal 界面已正常弹出，也能正常收到短信息，但是输入验证码之后，提示失败，现场还有V7的无线控制器也是和迈普对接，能正常使用。

过程分析

在设备侧收集debug portal 和抓包分析，打开抓包软件，过滤portal 报文，有两个报文，看到portal server 向AC发送了REQ_AUTH，AC回复了ACK_AUTH里边讲error_code 置1。并没有发送radius 报文。推测REQ_AUTH 报文包含错误原因，打开该报文发现CMCC标准中没有标注的未知的ca属性。但是客户那边使用V7设备的局点，采用相同的方式，能够通过认证，从收集的V7 设备抓包来看，确认未解读ca属性，跳过未知属性的障碍，并正常接收到portal server 发送的AFF_ACK_AUTH。推荐软件可以规避未知属性，拿到必须的属性后进入下一步流程。

172.31.1.9	172.31.1.9	PORTAL	115 Portal type REQ_AUTH
172.31.1.9	172.31.1.9	PORTAL	60 Portal type ACK_AUTH
172.31.1.9	172.31.1.9	PORTAL	62 Portal type AFF_ACK_AUTH

进入了radius 报文流程

172.31.1.9	172.31.1.9	PORTAL	60 Portal type ACK_AUTH
172.31.1.9	172.31.1.9	RADIUS	213 Accounting-Request(4) (Id=65, I=171)
172.31.1.9	172.31.1.9	PORTAL	62 Portal type AFF_ACK_AUTH

V7确实跳过解读ca

```
Type: REQ_AUTH (0x03)
Pap/Chap: 0x01
Reserve: 0
Serial Number: 16
Request ID: 0
User IP: 192.168.100.93 (192.168.100.93)
User Port: 0
Error Code: 0x00
Attribute Number: 0x04
+ Attribute: UserName
+ Attribute: Password
0000 00 01 7a 7c 4d 96 28 51 32 10 18 7d 08 00 45 00 ..z|M.(Q 2..}..E.
0010 00 65 00 00 40 00 40 11 11 67 0a f8 71 01 ac 1f .e..@.@. .g..q...
0020 01 09 07 d0 07 d0 00 51 29 84 01 03 01 00 00 10 .....Q ).....
0030 00 00 c0 a8 64 5d 00 00 00 04 01 0d 31 35 39 36 .....d].. ....1596
0040 33 32 39 39 37 38 39 02 17 64 65 66 61 75 6c 74 3299789. .default
0050 6d 61 69 70 75 40 2a 26 31 32 33 38 36 35 ca 0d maipu@*& 123865..
0060 61 75 74 68 5f 74 79 70 65 3a 31 c9 08 9c e3 3f auth_typ e:1....?
0070 b2 89 e3 ...
```

请求进一步收集DEBUG信息。通过以下命令：

Debug portal packet

debug portal error,

debug portal server ,

debug portal connection,

dis portal server statistics interface Vlan-interface X /测试认证的时候多敲几次，看看统计报文是够有增长

收集到的debug中比起第一次收集的debug，包含了疑似portal认证失败的原因：

PORTAL_DEBUG: No ARP or invalid interface for IP:0xa0701b4

在终端和portal server完成重定向之后，portal server和AC对终端的信息如req_auth中的用户名和密码属性进行交互，同时AC会反查终端合法性，发现AC的ARP表里，终端ARP表项找不到，AC会认为终端已掉线，遂停止正常认证流程

解决方法

针对AC未学到终端ARP表项：

V5平台：

1.在集中转发情况下分为两种情况通过display wlan client看到接入终端IP地址:

a.终端通过portal认证之后, 通过portal表项可以获取终端IP地址;

b.AC上开启arp-snooping enable之后上线的终端, 可以通过arp-snooping表项采集到终端IP地址;

2、本地转发情况下, 在AC上开启wlan client learn-ipaddr enable后, 终端通过DHCP或者静态设备IP地址将在wlan client表项中显示;

V7平台:

在V7平台下, AC默认开启wlan client learn-ip addr enable功能, 本地转发或者集中转发模式下都能采集到终端IP地址。因此, 终端接入并获取地址之后可以在wlan client表项中看到IP地址。

5、远程AC全局加入arp-snooping enable, 终端认证通过。

本次认证通过收集的Debug:

Portal send to x.x.x.xpacket length:16

Portal packet head:

Type:4 SN:39654 ReqId:0 AttrNum:0 ErrCode:0 UserIP:10.7.3.5

属性: Ack_Auth 0x04 BAS-->server BAS对服务器请求认证报文的响应报文

Portal receive from x.x.x.x packet length:20

Portal check packet OK

Portal packet head:

Type:7 SN:39654 ReqId:0 AttrNum:1 ErrCode:0 UserIP:10.7.3.5

属性: Aff_Ack_Auth 0x07 server-->BAS 服务器收到认证成功响应报文后向BAS发送的确认报文