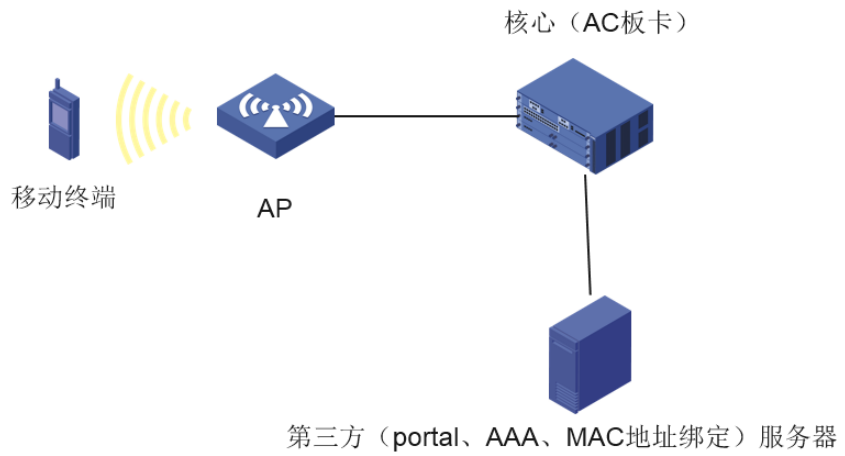
某局点V7 AC板卡portal无感知异常的经验案例

wlan接入 Portal MAC地址认证 **张腾** 2019-08-23 发表

组网及说明



组网：二层注册、本地转发、第三方服务器

问题描述

现场测试终端首次portal认证成功后，能够正常上网；后续再连接无线无需认证即可上网1-2分钟，然后通信中断，如此循环；

过程分析

1、开始能够正常上网1-2分钟，检查配置发现配置了 free-traffic threshold 1024000免认证流量阈值，即流量在未达到1024000字节时是可以正常上网的； 通信中断时，在AC上通过display portal user查看在线用户，发现测试终端不在线，说明流量达到阈值后用户被踢下线了，从现场故障现象看，怀疑无感知未成功；

2、检查现场配置正确，在AC上采集故障终端的debugging portal all和debugging radius all信息；

在看dbeug前，先看一下portal无感知认证的基本流程：

（1） 用户收发的流量达到设定的阈值之前，用户无需进行认证，接入设备将用户的MAC地址及接入端口信息保存为MAC-trigger表项；

（2） 当用户收发的流量达到设定的阈值时，AC 会向MAC Server发送Portal Type：48（0x30）的查询报文,查询MAC-trigger表项里测试终端的MAC是否存在；

（3）如果MAC Server中未查到终端的MAC（即此终端第一次关联无线），MAC Server向AC回应Portal Type：49（0x31）的应答报文，**ErrCode为1**表示MAC未绑定。AC就会将终端重定向到认证页面输入用户名密码，进行正常的portal认证流程；

（4）如果过MAC Server中查到终端的MAC, MAC Server向AC回应Portal Type：49（0x31）的应答报文，**ErrCode为0表示MAC已绑定，**会进行无感知认证。Portal Server/MAC Server向AC发起Portal认证，**用于认证的用户名\密码为MAC Server从AAA同步过来的账号信息**；

（5）AC向Radius服务器发起AAA认证

（6）认证通过后用户能访问网络；

3、查看现场debug信息

测试终端地址：192.168.2.179　测试终端MAC:fc18-3c36-0f71

*Aug 23 10:25:15:306 2019 AC PORTAL/7/MAC-trigger Event: Set MAC-trigger rule status 0.

*Aug 23 10:25:15:306 2019 AC PORTAL/7/MAC-trigger:

MAC-trigger rule:

InterfaceL3 = WLAN-BSS1/0/9292

InterfaceL2 = WLAN-BSS1/0/9292

VLAN = 10

SrcMAC = fc18-3c36-0f71

SrcIP = 192.168.2.179

Operation = 0

*Aug 23 10:25:15:306 2019 AC PORTAL/7/MAC-trigger Event: Received MAC overflow event, MAC=fc18-3c36-0f71.

*Aug 23 10:25:15:306 2019 AC PORTAL/7/EVENT: Success to get ssid by user mac, ssid:ceshi, user MAC:FC-18-3C-36-0F-71.

*Aug 23 10:25:15:306 2019 AC PORTAL/7/PACKET:

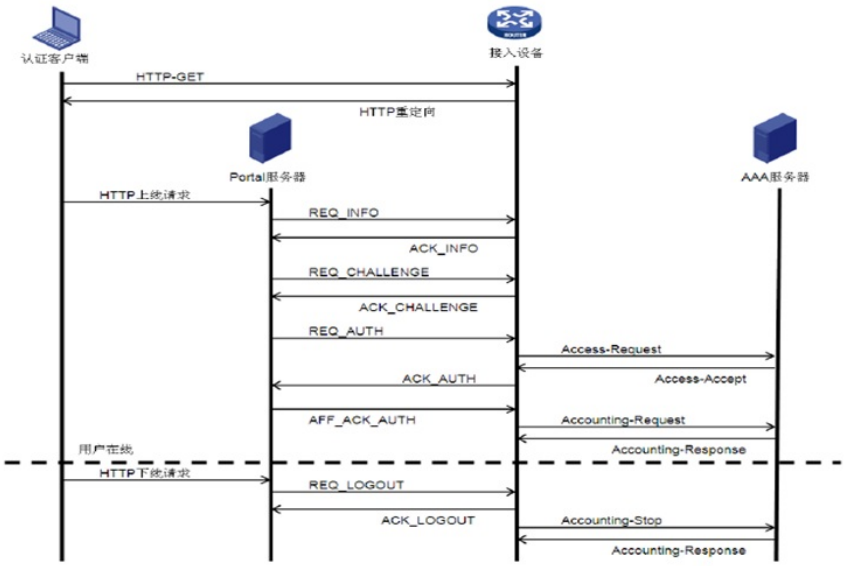
Portal sent 41 bytes of packet: Type=req_macbind_info(48), ErrCode=0, IP=192.168.2.179 //AC向MAC Server发送48号查询报文

*Aug 23 10:25:15:306 2019 AC PORTAL/7/PACKET:
[11 SESSIONID] [8] [fc18-3c36-0f71]
[10 BASIP] [6] [10.0.0.5]
[48 NASID] [4] [AC]
[30 SSID] [7] [ceshi]

*Aug 23 10:25:15:307 2019 AC PORTAL/7/PACKET:
01 30 00 00 70 7d 00 00 c0 a8 02 b3 00 00 00 04
0b 08 fc 18 3c 36 0f 71 0a 06 0a 00 00 05 30 04
41 43 1e 07 63 65 73 68 69

*Aug 23 10:25:15:307 2019 AC PORTAL/7/MAC-trigger Event: MAC entry(fc18-3c36-0f71) state changed from DEFAULT to WAIT, user IP = 192.168.2.179.
*Aug 23 10:25:15:307 2019 AC PORTAL/7/EVENT: Success to get info from wlan snooping, vlan:10. mac:fc18-3c36-0f71,userip:192.168.2.179
*Aug 23 10:25:15:307 2019 AC PORTAL/7/EVENT: Success to get ifindex(128) and vlan(10) from IP CIM, user IP=192.168.2.179,MAC=fc18-3c36-0f71
*Aug 23 10:25:15:308 2019 AC PORTAL/7/PACKET:
Portal received 16 bytes of packet: Type=ack_macbind_info(49), ErrCode=0, IP=192.168.2.179 //AC收到MAC服务器 49号回应报文并且 ErrCode=0 证明MAC地址存在，接下来进行无感知portal认证
*Aug 23 10:25:15:308 2019 AC PORTAL/7/PACKET:
01 31 00 00 70 7d 00 00 c0 a8 02 b3 00 00 00 00

*Aug 23 10:25:15:308 2019 AC PORTAL/7/MAC-trigger Event: MAC entry(fc18-3c36-0f71) state changed from WAIT to BIND. user IP=192.168.2.179.
*Aug 23 10:25:15:308 2019 AC PORTAL/7/MAC-trigger Event: Set MAC-trigger rule status 3.
*Aug 23 10:25:15:308 2019 AC PORTAL/7/MAC-trigger:
MAC-trigger rule:
InterfaceL3 = WLAN-BSS1/0/9292
InterfaceL2 = WLAN-BSS1/0/9292
VLAN = 10
SrcMAC = fc18-3c36-0f71
SrcIP = 192.168.2.179
Mac status = 3
*Aug 23 10:25:15:309 2019 AC PORTAL/7/EVENT: Success to get info from wlan snooping, vlan:10. mac:fc18-3c36-0f71,userip:192.168.2.179
*Aug 23 10:25:15:309 2019 AC PORTAL/7/EVENT: Success to get ifindex(128) and vlan(10) from IP CIM, user IP=192.168.2.179,MAC=fc18-3c36-0f71
*Aug 23 10:25:15:309 2019 AC PORTAL/7/EVENT: Success to get ifindex(128) and vlan(10) from IP CIM, user IP=192.168.2.179,MAC=fc18-3c36-0f71
*Aug 23 10:25:15:309 2019 AC PORTAL/7/PACKET:
Portal received 69 bytes of packet: Type=req_auth(3), ErrCode=0, IP=192.168.2.179 //AC直接收到portal服务器发起的req_auth报文；
这里有人可能会有疑问，从下图看，正常的portal认证流程，应该是portal服务器先发起req_info报文交互用户信息，第三方portal服务器是不是有问题？当portal认证采用了CMCC2.0的协议时,省略了req_info、req_challenge阶段，直接收到req_auth是正常的，AC能够正常识别；和第三方服务器厂商确认，他们最开始发的确实是req_auth报文；



***Aug 23 10:25:15:309 2019 AC PORTAL/7/PACKET:　　//req_auth报文把用户名密码信息同步给了AC**
[1 USERNAME　　] [19] [fc:18:3c:36:0f:71] //注意这里的用户名是MAC地址，正常应该是时测试终端输入的账号
[2 PASSWORD　　] [18] [******]

*Aug 23 10:25:15:310 2019 AC PORTAL/7/PACKET:
02 03 01 00 34 44 00 00 c0 a8 02 b3 00 00 00 02
98 f1 93 7f 98 50 31 b4 b1 93 66 63 42 92 28 a1
01 13 66 63 3a 31 38 3a 33 63 3a 33 36 3a 30 66
3a 37 31 02 12 32 38 65 38 66 61 64 30 32 64 39
39 39 33 33 66

*Aug 23 10:25:15:310 2019 AC PORTAL/7/EVENT:
Auth-SM [192.168.2.179]: Don't Started auth_sm timer for user from local web server or NOC.
*Aug 23 10:25:15:311 2019 AC PORTAL/7/EVENT: Success to get option info from IPCIM, user IP=1
92.168.2.179, user MAC=FC-18-3C-36-0F-71.
*Aug 23 10:25:15:311 2019 AC PORTAL/7/EVENT: Success to get option55 from DHCP
option55:1,121,3,6,15,119,252,len:7, user IP-192.168.2.179, user MAC=FC-18-3C-36-0F-71
*Aug 23 10:25:15:312 2019 AC PORTAL/7/EVENT: Success to get ssid by user mac, ssid:ceshi, use
r MAC:FC-18-3C-36-0F-71.
*Aug 23 10:25:15:312 2019 AC PORTAL/7/EVENT: Success to get ap mac by user mac, ap mac: 3C
-8C-40-45-0B-60, user MAC: FC-18-3C-36-0F-71.
*Aug 23 10:25:15:312 2019 AC PORTAL/7/EVENT: User-SM[192.168.2.179]: Notified Auth-SM to pr
ocess the REQ_AUTH packet.
*Aug 23 10:25:15:312 2019 AC PORTAL/7/FSM: Auth-SM: Started to run.
***Aug 23 10:25:15:312 2019 AC PORTAL/7/FSM: Auth-SM [192.168.2.179]: Entered state Authent
icating. //进入RADIUS认证阶段，RADIUS报文中，code=1是认证请求报文，code=2是认证成功报文，code=3是认证失败报文，这三种报文只在用户上线时产生；code4、code5是认证成功后计费用的；**
*Aug 23 10:25:15:312 2019 AC PORTAL/7/MAC-trigger:
　MAC-trigger rule:
　InterfaceL3　= WLAN-BSS1/0/9292
　InterfaceL2　= WLAN-BSS1/0/9292
　VLAN　　= 10
　SrcMAC　　= fc18-3c36-0f71
　SrcIP　　= 192.168.2.179
　Operation　= 1
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:
Processing AAA request data.
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:
Got request data successfully, primitive: authentication.
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:

Getting RADIUS server info.
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:
Got RADIUS server info successfully.
*Aug 23 10:25:15:313 2019 AC RADIUS/7/EVENT:
Created request context successfully.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Created request packet successfully, dstIP: 10.0.0.3, dstPort: 1812, VPN instance: --(public), socketF
d: 84, pktID: 69.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Added packet socketfd to epoll successfully, socketFd: 84.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Mapped PAM item to RADIUS attribute successfully.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Got RADIUS username format successfully, format: 2.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Added attribute user-name successfully, user-name: fc:18:3c:36:0f:71.
*Aug 23 10:25:15:314 2019 AC RADIUS/7/EVENT:
Filled RADIUS attributes in packet successfully.
*Aug 23 10:25:15:315 2019 AC RADIUS/7/EVENT:
Composed request packet successfully.
*Aug 23 10:25:15:315 2019 AC RADIUS/7/EVENT:
Created response timeout timer successfully.
*Aug 23 10:25:15:315 2019 AC RADIUS/7/EVENT:
PAM_RADIUS: **Sent authentication request successfully.**
*Aug 23 10:25:15:315 2019 AC RADIUS/7/PACKET:
User-Name="fc:18:3c:36:0f:71" **//可以看到radius报文的用户密码封装的还是MAC地址**
User-Password=****
Service-Type=Framed-User
Framed-Protocol=255
NAS-Identifier="AC"
NAS-Port=16777226
NAS-Port-Type=Wireless-802.11
NAS-Port-
Calling-Station-
Called-Station-
Acct-Session-
H3c-User-Vlan-Id=10
Framed-IP-Address=192.168.2.179
H3c-Ip-Host-Addr="192.168.2.179 fc:18:3c:36:0f:71"
H3c_DHCP_OPTION55=0x017903060f77fc
NAS-IP-Address=10.0.0.5
H3c-Product-
H3c-Nas-Startup-Timestamp=1565282790
*Aug 23 10:25:15:315 2019 AC PORTAL/7/EVENT: User-SM[192.168.2.179]: AAA processed authen
tication request and returned processing.
*Aug 23 10:25:15:315 2019 AC PORTAL/7/FSM: User-SM[192.168.2.179]: Begin to run.
*Aug 23 10:25:15:316 2019 AC RADIUS/7/EVENT:
Sent request packet successfully. **//发送RADIUS认证请求报文**
*Aug 23 10:25:15:316 2019 AC PORTAL/7/FSM: User-SM [192.168.2.179]: State changed from
Initial to Authenticating.
*Aug 23 10:25:15:316 2019 AC RADIUS/7/PACKET:
01 45 01 2d 49 aa b8 b9 e0 61 2b ed c6 31 35 5b **//第一个字节01表示code=1，是radius的认证请求报文**
73 0c fd bf 01 13 66 63 3a 31 38 3a 33 63 3a 33
36 3a 30 66 3a 37 31 02 12 bc 2f 4b 9d e1 1f f9
f2 56 07 28 f2 b3 4d fa e6 06 06 00 00 00 02 07
06 00 00 00 ff 20 04 41 43 05 06 01 00 00 0a 3d
06 00 00 00 13 57 12 30 31 30 30 30 30 30 30 30
30 30 30 30 30 31 30 1f 13 46 43 2d 31 38 2d 33
43 2d 33 36 2d 30 46 2d 37 31 1e 19 33 43 2d 38
43 2d 34 30 2d 34 35 2d 30 42 2d 36 30 3a 63 65
73 68 69 2c 28 30 30 30 30 30 30 30 37 32 30 31
39 30 38 32 33 31 30 32 35 31 35 30 30 30 30 33
34 61 65 30 38 31 30 39 39 33 36 1a 0c 00 00 63

a2 85 06 00 00 00 0a 08 06 c0 a8 02 b3 1a 27 00
00 63 a2 3c 21 31 39 32 2e 31 36 38 2e 32 2e 31
37 39 20 66 63 3a 31 38 3a 33 63 3a 33 36 3a 30
*Aug 23 10:25:15:317 2019 AC RADIUS/7/PACKET:
66 3a 37 31 1a 0f 00 00 63 a2 d0 09 01 79 03 06
0f 77 fc 04 06 0a 00 00 05 1a 18 00 00 63 a2 ff
12 48 33 43 20 45 57 50 58 4d 32 57 43 4d 44 30
46 1a 0c 00 00 63 a2 3b 06 5d 4c 51 e6
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Sent request packet and create request context successfully. //RADIUS请求报文发送成功
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Added request context to global table successfully.
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Processing AAA request data.
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Reply SocketFd recieved EPOLLIN event.
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Received reply packet succuessfully. //收到RADIUS服务器的回复报文
*Aug 23 10:25:15:317 2019 AC RADIUS/7/EVENT:
Found request context, dstIP: 10.0.0.3, dstPort: 1812, VPN instance: --(public), socketFd: 84, pktID: 6
9.
*Aug 23 10:25:15:318 2019 AC RADIUS/7/EVENT:
The reply packet is valid.
*Aug 23 10:25:15:318 2019 AC RADIUS/7/EVENT:
Decoded reply packet successfully. //解析RADIUS回复报文
***Aug 23 10:25:15:318 2019 AC RADIUS/7/PACKET:**
User-Name="fc:18:3c:36:0f:71" //用户名错误
Reply-Message="authen reject" //认证请求被拒绝
*Aug 23 10:25:15:318 2019 AC RADIUS/7/PACKET:
03 45 00 36 2a d8 b4 9e de 7e 22 18 39 55 68 0e **//第一个字节03表示code=3，是radius的认证失败报文**
24 c8 1d be 01 13 66 63 3a 31 38 3a 33 63 3a 33
36 3a 30 66 3a 37 31 12 0f 61 75 74 68 65 6e 20
72 65 6a 65 63 74
*Aug 23 10:25:15:318 2019 AC RADIUS/7/EVENT:
Sent reply message successfully.
*Aug 23 10:25:15:318 2019 AC RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
*Aug 23 10:25:15:319 2019 AC RADIUS/7/EVENT:
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 1
*Aug 23 10:25:15:319 2019 AC PORTAL/7/EVENT: User-SM[192.168.2.179]: Received authenticatio
n response, RespCode=26.
*Aug 23 10:25:15:319 2019 AC PORTAL/7/FSM: Auth-SM: Started to run.
*Aug 23 10:25:15:320 2019 AC PORTAL/7/PACKET:
Portal sent 62 bytes of packet: Type=ack_auth(4), ErrCode=1, IP=192.168.2.179
*Aug 23 10:25:15:320 2019 AC PORTAL/7/PACKET:
[11 SESSIONID] [8] [fc18-3c36-0f71]
[5 TEXTINFO] [16] [authen reject]
[10 BASIP] [6] [10.0.0.5]

*Aug 23 10:25:15:321 2019 AC PORTAL/7/PACKET:
02 04 01 00 34 44 00 00 c0 a8 02 b3 00 00 01 03
0e 17 07 c4 50 7a a5 02 1f 24 e7 69 58 6d 75 38
0b 08 fc 18 3c 36 0f 71 05 10 61 75 74 68 65 6e
20 72 65 6a 65 63 74 00 0a 06 0a 00 00 05

*Aug 23 10:25:15:321 2019 AC PORTAL/7/EVENT: User-SM[192.168.2.179]: Auth-SM logged out th
e user and notified User-SM to process.
*Aug 23 10:25:15:321 2019 AC PORTAL/7/FSM: User-SM[192.168.2.179]: Begin to run.
***Aug 23 10:25:15:321 2019 AC PORTAL/7/FSM: User-SM [192.168.2.179]: State changed from A
uthenticating to Done. //用户认证失败状态变为DOWN**
***Aug 23 10:25:15:321 2019 AC PORTAL/7/FSM: User-SM[192.168.2.179]: User was destroyed.**
*Aug 23 10:25:15:323 2019 AC PORTAL/7/EVENT: User-SM[192.168.2.179]: Notified User-Detect-S
M to stop detection.

4、从debug过程可以看到，portal无感知在radius认证阶段失败，由于认证的用户名错误，而用户名密码是第三方服务器通过req_auth报文同步给我们的，协调第三方服务器排查修改服务器侧配置后认证成功；

解决方法

第三方服务器问题，修改服务器侧配置解决；

总结：

1、MAC Server回应Portal Type：49（0x31）的应答报文，ErrCode为0表示MAC已绑定，ErrCode为1表示MAC未绑定；

2、 当portal认证采用了CMCC2.0的协议时,省略了req_info、req_challenge阶段；

3、Radius报文中，code = 1是认证请求报文，code = 2和code = 3分别是认证通过和认证失败报文，这三种报文只在用户上线时产生。在用户上网的漫长过程中，是依靠code = 4报文来维系计费和用户在线信息。