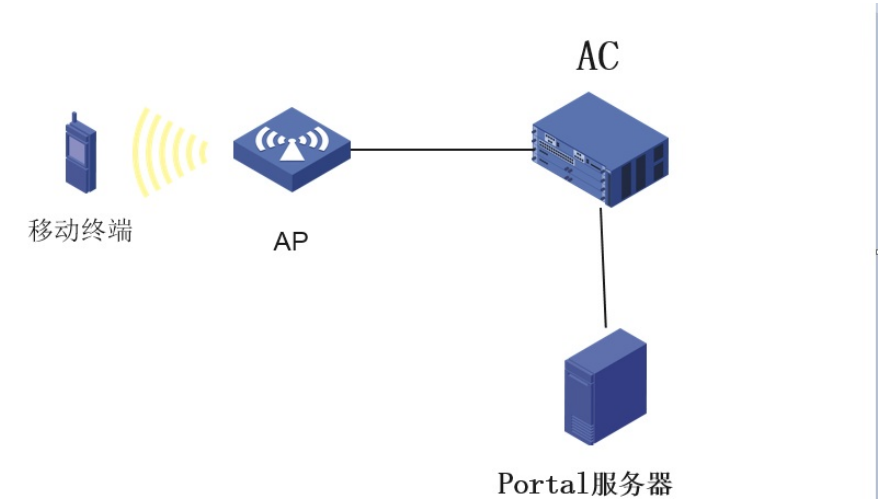
某局点V7无线控制器portal认证失败的经验案例

AAA Portal 张腾 2019-10-27 发表

组网及说明



组网：二层注册、本地转发

问题描述

终端关联无线后，能够正常跳转到portal认证页面，但输入账号密码点击登录后页面会一直转圈，无法正常上网；

过程分析

一、能够正常重定向到认证页面，说明portal web服务器本身的http页面没问题，设备重定向功能也没问题。

二、AC能够ping通portal服务器，并且在输入用户名密码后，登陆页面一直在转圈，没有提示“设备向服务器发送请求超时”，初步判断设备与服务器通信没问题，是portal或者Radius报文交互出现问题；

三、采集设备侧的debug信息：

*Sep 27 17:07:34:312 2019 AC-WX2560H PORTAL/7/PACKET:

Portal received 34 bytes of packet: **Type=req_auth(3)**, ErrCode=0, IP=10.11.60.162 **//设备收到portal服务器发来的req_auth报文，获取用户输入的用户名密码信息**

*Sep 27 17:07:34:312 2019 AC-WX2560H PORTAL/7/PACKET:

[1 USERNAME] [6] [test]

[2 PASSWORD] [12] [******]

*Sep 27 17:07:34:312 2019 AC-WX2560H PORTAL/7/PACKET:

01 03 01 00 00 12 00 00 0a 0b 3c a2 00 00 00 02

01 06 74 65 73 74 02 0c 48 75 61 77 65 69 40 31

32 33

*Sep 27 17:07:34:313 2019 AC-WX2560H PORTAL/7/ERROR: **Failed to obtain user physical information when create user.UserIP=10.11.60.162 //设备提示获取用户信息失败**

*Sep 27 17:07:34:313 2019 AC-WX2560H PORTAL/7/ERROR: **Portal is disabled on the interface.**

*Sep 27 17:07:34:314 2019 AC-WX2560H PORTAL/7/PACKET:

Portal sent 23 bytes of packet: **Type=ack_auth(4)**, **ErrCode=1**, IP=10.11.60.162 **//正常情况下，设备获取用户信息后会向radius服务发起认证，认证成功后回给portal服务器errcode=0的ack_auth报文，这里设备回了已errcode=1的报文，即AAA认证失败；**

*Sep 27 17:07:34:314 2019 AC-WX2560H PORTAL/7/PACKET:

[5 TEXTINFO] [7] [AC999]

*Sep 27 17:07:34:315 2019 AC-WX2560H PORTAL/7/PACKET:

01 04 01 00 00 12 00 00 0a 0b 3c a2 00 00 01 01

05 07 41 43 39 39 39

*Sep 27 17:07:34:318 2019 AC-WX2560H PORTAL/7/PACKET:

Portal received 22 bytes of packet: **Type=req_logout(5)**, ErrCode=254, IP=10.11.60.162 **//AAA认证失败，后续portal服务器就把用户踢下线了**

*Sep 27 17:07:34:318 2019 AC-WX2560H PORTAL/7/PACKET:
01 05 00 00 00 13 00 00 0a 0b 3c a2 00 00 fe 01
0c 06 00 00 00 00

*Sep 27 17:07:34:318 2019 AC-WX2560H PORTAL/7/PACKET:
Portal sent 16 bytes of packet: Type=ack_logout(6), ErrCode=2, IP=10.11.60.162
*Sep 27 17:07:34:318 2019 AC-WX2560H PORTAL/7/PACKET:
01 06 00 00 00 13 00 00 0a 0b 3c a2 00 00 02 00

四、设备为什么会出现如下报错：
Failed to obtain user physical information when create user.UserIP=10.11.60.162
AC作为protal设备时，有一个客户端合法性检查的机制，即检查此客户端是否合法，如果不合法就会出现以上报错。客户端是否合法的判断依据是什么呢？在缺省情况下，设备仅根据ARP表项对无线Portal客户端进行合法性检查，即AC上如果有此终端的ARP表项，就认为此客户端是合法的。
但在实际环境中可能会有以下组网：
1、AC旁挂核心交换机，本地转发，终端的网关在核心交换机上；这种组网用户流量不经过AC，AC上肯学不到终端的ARP表项，就会出现上面的报错；
2、AC旁挂核心交换机，集中转发，终端的网关在核心交换机上；这种组网用户流量虽然经过AC，但AC实际上相当于一个二层设备，还是由核心交换机（网关）去响应终端的arp请求，所以AC还是学不到终端的ARP，也会出现上面报错；
总结一下就是：AC学不到终端的ARP就会出现上面的报错；

五、那么如何规避？
设备侧开启无线Portal客户端合法性检查功能
portal host-check enable
功能开启后，当设备收到未认证Portal用户的认证报文后，将使用WLAN Snooping表、DHCP Snooping表和ARP表对其进行合法性检查。如果在这三个表中查询到该Portal客户端信息，则认为其合法并允许进行Portal认证。 这样即使设备侧没有终端的ARP表项也可通过其他表项检查客户端合法性；而WLAN Snooping表，终端关联后就会生成，所以不用担心其他表项也没有此终端，也不用特意去配置dhcp snooping。

六、现场配置**portal host-check enable** 命令后发现还是认证失败
再次收集debug信息，发现经过上述优化，这次报文交互已经到了radius认证阶段：
*Sep 29 15:06:02:014 2019 AC-WX2560H RADIUS/7/EVENT:
Composed request packet successfully.
*Sep 29 15:06:02:014 2019 AC-WX2560H RADIUS/7/EVENT:
Created response timeout timer successfully.
*Sep 29 15:06:02:015 2019 AC-WX2560H RADIUS/7/PACKET:
User-Name="song"
User-Password=******
Service-Type=Framed-User
Framed-Protocol=255
NAS-Identifier="AC-WX2560H"
NAS-Port=16778376
NAS-Port-Type=Wireless-802.11
NAS-Port-
Calling-Station-
Called-Station-
Acct-Session-
H3c-User-Vlan-Id=1160
Framed-IP-Address=10.11.60.83
H3c-Ip-Host-Addr="10.11.60.83 9c:4e:36:8e:94:cc"
H3c_DHCP_OPTION55=0x010f03062c2e2f1f2179f9fc2b
NAS-IP-Address=10.11.3.2
H3c-Product-
H3c-Nas-Startup-Timestamp=1569586143
*Sep 29 15:06:02:015 2019 AC-WX2560H RADIUS/7/EVENT:
Sent request packet successfully.
*Sep 29 15:06:02:016 2019 AC-WX2560H RADIUS/7/PACKET:
01 33 01 2f 14 d8 37 3b 33 f7 aa 92 9f a2 94 0c //**设备发送code=1的认证报文**
4a eb 05 e0 01 06 73 6f 6e 67 02 12 58 9f db ab
f1 dd fc 86 5a 8d 61 8b e5 bd d7 3f 06 06 00 00
00 02 07 06 00 00 00 ff 20 0c 41 43 2d 57 58 32

35 36 30 48 05 06 01 00 04 88 3d 06 00 00 00 13
57 12 30 31 30 30 30 30 30 30 30 30 30 30 31 31
36 30 1f 13 39 43 2d 34 45 2d 33 36 2d 38 45 2d
39 34 2d 43 43 1e 21 37 38 2d 32 43 2d 32 39 2d
30 44 2d 46 42 2d 41 30 3a 53 68 63 6f 6f 70 2d
70 75 62 6c 69 63 2c 28 30 30 30 30 30 30 30 37
32 30 31 39 30 39 32 39 31 35 30 36 30 32 30 30
30 30 30 30 31 62 30 38 31 30 31 31 35 33 1a 0c
00 00 63 a2 85 06 00 00 04 88 08 06 0a 0b 3c 53
1a 25 00 00 63 a2 3c 1f 31 30 2e 31 31 2e 36 30
2e 38 33 20 39 63 3a 34 65 3a 33 36 3a 38 65 3a
*Sep 29 15:06:02:016 2019 AC-WX2560H RADIUS/7/PACKET:
39 34 3a 63 63 1a 15 00 00 63 a2 d0 0f 01 0f 03
06 2c 2e 2f 1f 21 79 f9 fc 2b 04 06 0a 0b 03 02
1a 13 00 00 63 a2 ff 0d 48 33 43 20 57 58 32 35
36 30 48 1a 0c 00 00 63 a2 3b 06 5d 8d fb df
*Sep 29 15:06:02:016 2019 AC-WX2560H RADIUS/7/EVENT:
Sent request packet and create request context successfully.
*Sep 29 15:06:02:016 2019 AC-WX2560H RADIUS/7/EVENT:
Added request context to global table successfully.
*Sep 29 15:06:02:017 2019 AC-WX2560H RADIUS/7/EVENT:
Processing AAA request data.
*Sep 29 15:06:02:019 2019 AC-WX2560H RADIUS/7/EVENT:
Reply SocketFd recieved EPOLLIN event.
*Sep 29 15:06:02:019 2019 AC-WX2560H RADIUS/7/EVENT:
Received reply packet succuessfully.
*Sep 29 15:06:02:019 2019 AC-WX2560H RADIUS/7/EVENT:
Found request context, dstIP: 10.11.10.99, dstPort: 1812, VPN instance: --(public), socketFd: 84, pktID: 51.
*Sep 29 15:06:02:019 2019 AC-WX2560H RADIUS/7/EVENT:
The reply packet is valid.
*Sep 29 15:06:02:019 2019 AC-WX2560H RADIUS/7/EVENT:
Decoded reply packet successfully.
*Sep 29 15:06:02:020 2019 AC-WX2560H RADIUS/7/PACKET: //
收到code=2的认证成功报文
02 33 00 14 3a 74 4f 1e 4b 26 de 2b a7 6e e4 97
e9 d7 ca 0e
*Sep 29 15:06:02:020 2019 AC-WX2560H RADIUS/7/EVENT:
Sent reply message successfully.
*Sep 29 15:06:02:020 2019 AC-WX2560H RADIUS/7/EVENT:
PAM_RADIUS: Processing RADIUS authentication.
*Sep 29 15:06:02:020 2019 AC-WX2560H RADIUS/7/EVENT:
PAM_RADIUS: Fetched authentication reply-data successfully, resultCode: 0
*Sep 29 15:06:02:020 2019 AC-WX2560H PORTAL/7/EVENT: User-SM[10.11.60.83]: Received authentication response, RespCode=0.
*Sep 29 15:06:02:021 2019 AC-WX2560H PORTAL/7/FSM: Auth-SM: Started to run.
*Sep 29 15:06:02:021 2019 AC-WX2560H PORTAL/7/FSM: Auth-SM [10.11.60.83]: Entered state Authenticated.
*Sep 29 15:06:02:021 2019 AC-WX2560H PORTAL/7/FSM: User-SM[10.11.60.83]: Begin to run.
*Sep 29 15:06:02:022 2019 AC-WX2560H PORTAL/7/FSM: User-SM [10.11.60.83]: State changed from Authenticating to Waiting_Author.
***Sep 29 15:06:02:023 2019 AC-WX2560H PORTAL/7/EVENT: User-SM[10.11.60.83]: AAA processed authorization request and returned fail.** **//正常下一步应该是设备发送ACK_AUTH报文给portal服务器，但AAA认证阶段虽然认证成功，但授权失败了，所以设备不发ack——auth报文**

再次核对现场配置，发现设备侧缺少授权的配置
domain portal
authentication portal radius-scheme ac
accounting portal radius-scheme ac

七、现场增加授权配置后，认证成功。

解决方法

设备侧开启portal host-check enable 命令，并且规范portal基础配置；

总结：

1、AC作为protal设备时，有一个客户端合法性检查的机制，即检查此客户端是否合法，如果不合法就会出现以上报错。

2、portal host-check enable 功能开启后，当设备收到未认证Portal用户的认证报文后，将使用WLAN Snooping表、DHCP Snooping表和ARP表对其进行合法性检查。如果在这三个表中查询到该Portal客户端信息，则认为其合法并允许进行Portal认证。

3、掌握portal认报文交互的具体过程，方便portal问题排查；