

交换机接口配置MAC认证导致接入桥接瘦AP的胖AP获取不到IP地址

wlan接入 谭奇伟 2024-04-02 发表

组网及说明

AC旁挂，AC --- 核心交换机 --- 汇聚交换机 --- PoE交换机 (V5) --- FIT AP, 桥接FAT AP, 其中FIT AP使用集中转发服务模板，业务vlan 93，FAT AP上设置同名SSID的服务模板，同样使用业务vlan 93。

告警信息

无

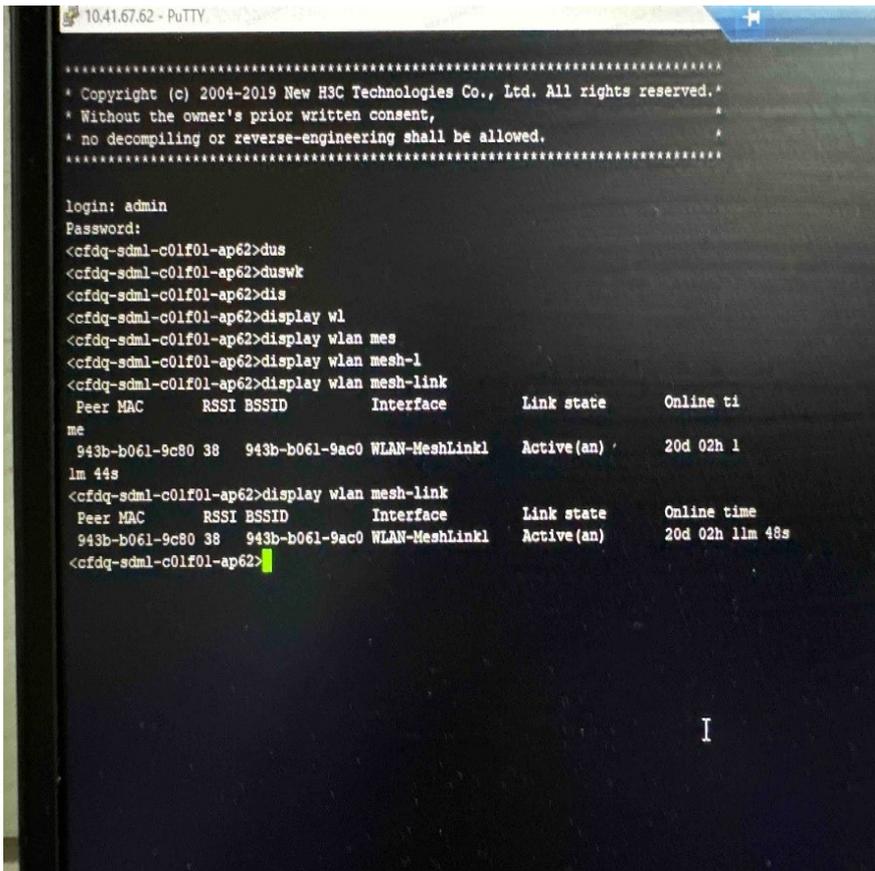
问题描述

某工厂的无线叉车（类似AGV小车）运动到一块区域后发现无线上网，但是连接该区域周围的AP可以正常上网。现场工程师排查发现，该区域AP全部使用FAT模式，与周围的FIT AP使用桥接模式进行连接，因此无线叉车连接这部分FAT AP后，无法获取IP地址，且无法访问网关，但连接周围区域的FIT AP可以正常接入和获取地址，并正常上网。另外该区域的无线网络最近几天才出现故障，之前的使用过程中均无问题，近期无线设备未做任何配置变更。

过程分析

1. 首先检查FAT AP的配置，FAT AP上添加了和该厂区使用的AC --- FIT AP所释放的同名SSID的服务模板（AC的模板是集中转发），且均使用业务vlan 93，并绑定在FAT AP的interface-Wlan Radio 1/0/1和1/0/2口上，而FAT AP的interface-Wlan Radio1/0/1接口也用于和FIT AP的mesh。进一步地，分别检查了FAT AP和AC上相关FIT AP视图下的mesh配置和mesh-interface的配置，发现配置均未问题，且mesh-interface口也放通了vlan 93。

在FAT AP上通过：display wlan mesh-link命令查看于FIT AP的mesh连接，发现mesh邻居关系是正常建立的且RSSI的数值也符合要求。

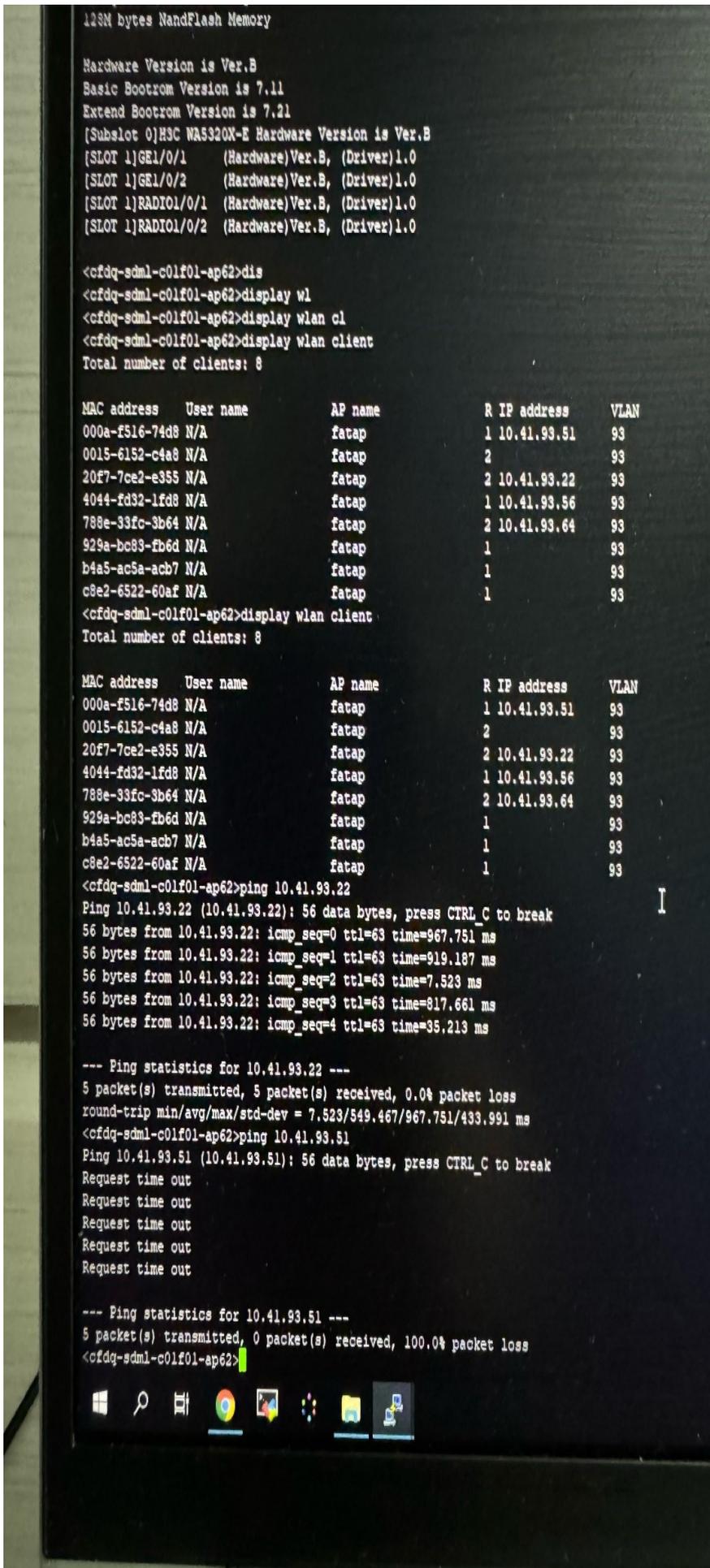


```
10.41.67.62 - PuTTY
*****
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

login: admin
Password:
<cfdq-sdml-c01f01-ap62>dus
<cfdq-sdml-c01f01-ap62>duswk
<cfdq-sdml-c01f01-ap62>dis
<cfdq-sdml-c01f01-ap62>display wl
<cfdq-sdml-c01f01-ap62>display wlan mes
<cfdq-sdml-c01f01-ap62>display wlan mesh-1
<cfdq-sdml-c01f01-ap62>display wlan mesh-link
Peer MAC      RSSI  BSSID      Interface      Link state      Online ti
me
943b-b061-9c80 38    943b-b061-9ac0 WLAN-MeshLink1 Active(an)      20d 02h 1
1m 44s
<cfdq-sdml-c01f01-ap62>display wlan mesh-link
Peer MAC      RSSI  BSSID      Interface      Link state      Online time
943b-b061-9c80 38    943b-b061-9ac0 WLAN-MeshLink1 Active(an)      20d 02h 11m 48s
<cfdq-sdml-c01f01-ap62>
```

3. 值得注意的是，由于AC --- FIT AP上同名模板使用集中转发，终端接入时候可以正常获取地址，而同这些FIT AP建立mesh连接的FAT AP上终端接入时无法获取地址，在排除FIT AP的上行有线口和FIT AP与FAT AP之间mesh-interface口没有放通业务vlan 93的情况下，就要按照网络拓扑检查从PoE---汇聚---核心交换机（DHCP服务器）之间是否放通了业务vlan 93了。这时因为AC --- FIT AP之间使用了集中转发，终端接入FIT AP后DHCP请求和应答报文也是先通过CAPWAP隧道走到AC后再由AC传递给核心交换机的，但FAT AP下终端的DHCP请求和应答报文则是先通过无线mesh到大FIT AP，再由FIT AP的有线口经PoE交换机、汇聚交换机后到达核心交换机，流量路径和本地转发是相似的，因此中间必须放通vlan 93。检查之后发现果然是中间交换机近期做了变更，关闭了vlan 93的放通，于是进行了相应的放通，放通后发现部分终端可以获取IP地址，但部分无法获取，但获取IP地址的终端也无法ping通网

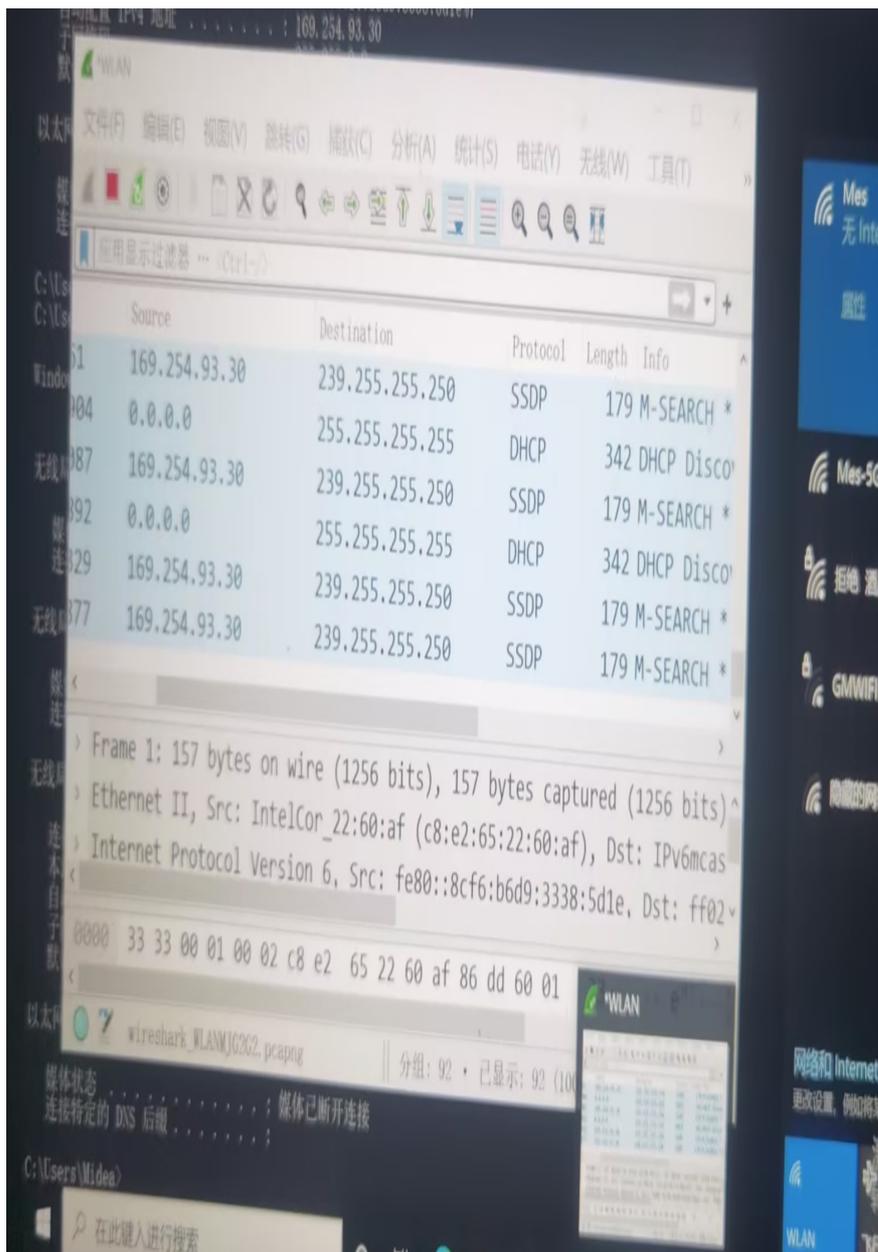
关，但是FAT AP却可以ping通这些终端。



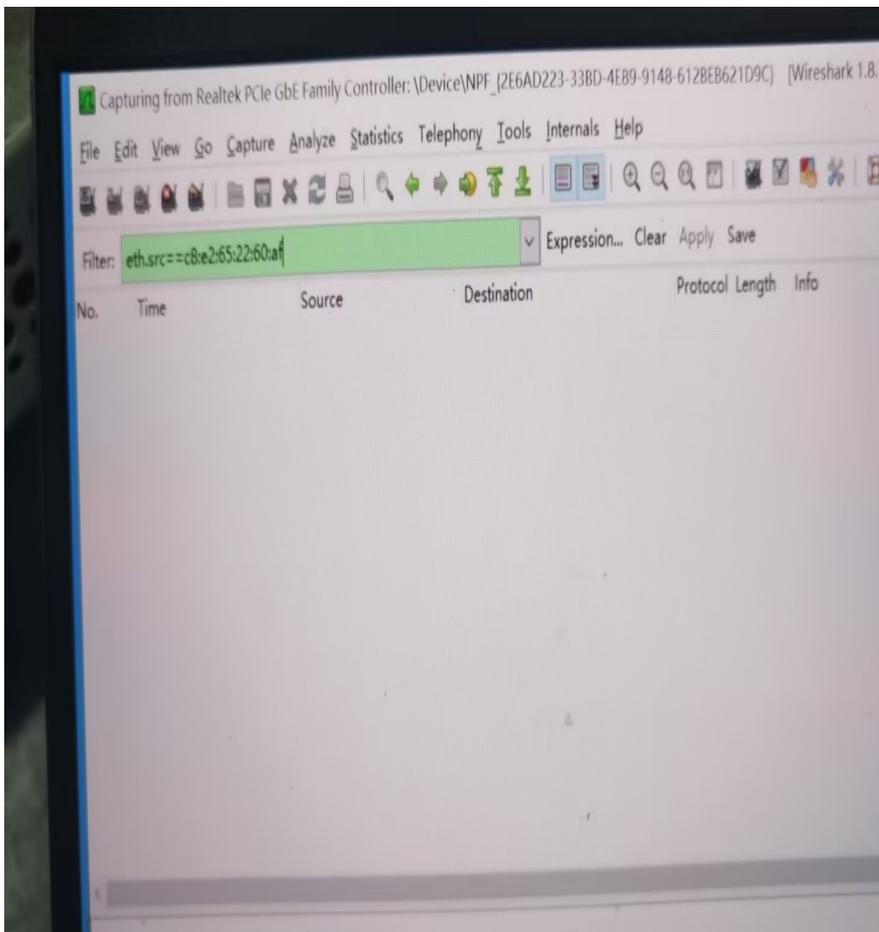
4. 终端无法ping通网关，或者部分连接FAT AP的终端无法获取IP地址，针对这两个问题，就只能在沿途进行抓包或者流统来分析了，可能的丢包路径包括：① 终端和FAT AP空口；② FAT AP

和FIT AP的mesh空口；③ FIT AP和PoE之间；④ PoE交换机内部；⑤ PoE和汇聚之间；⑥ 汇聚和核心交换机之间。

于是，现场工程师首先在连接FAT AP的PC上抓取其自身无线网络卡的报文，发现PC发出了DHCP Discover报文，但却没有收到应答报文；



随后在汇聚交换机上和PoE之间的端口做镜像抓包，发现终端发送的DHCP Discover请求报文并未上送到汇聚交换机，这说明丢包位置在：① 终端和FAT AP空口；② FAT AP和FIT AP的mesh空口；③ FIT AP和PoE之间；④ PoE交换机内部，这四个位置之一。



5. 由于PoE交换机和AP部署在工厂房顶，现场并无高空作业人员，因此无法在PoE交换机和FIT AP之间抓包用于排查上述③的可能，而由于PoE交换机的是Comware V5的无法配置流统，因此④也暂使无法排查，只能先行排查①和②的可能性。

6. 于是使用AP的ar5drv驱动debug，Wlan-forward debug和MAC forward debug的方式捕获终端接入后DHCP的报文，并使用相关分析工具进行报文的解析：

<https://zhiliao.h3c.com/Tool/details/5249>。

注意：终端接入FAT AP后获取IP地址的DHCP报文路径是：

STA → FAT AP射频口Rx → FAT AP射频口Tx (mesh) → FIT AP射频口Rx → PoE → 汇聚交换机 → 核心交换机 (DHCP服务器)

(1) 首先让终端接入FAT AP，然后在FAT AP上进行ar5drv驱动debug，目的在于收集AP的射频驱动是否收到了终端的DHCP discover报文，以及是否通过射频驱动通过mesh把报文发送给了FIT AP，结果发现FAT AP收到了终端的DHCP Discover报文并通过mesh发送给了FIT AP。

下图中ID为43号的报文是FAT AP的射频口Rx收到终端的DHCP discover报文，ID为45号的对应FAT AP的射频口Tx通过mesh发送给FIT AP的报文（注意：这里工具的当前版本R2.2.9由于暂未合入针对mesh报文源目mac的解析，因此45号报文填写的源目mac地址不具备参考价值，但是解析出来的如报文类型等其它内容是准确无误的，通过分析报文的原始hex字符串也进一步确认了，工具后续版本会新增合入对mesh报文的解析）。

过滤器: dhcp

源文件: C:\Users\25850\Desktop\2024-01-05 美的集团 fit-ap_2.txt

WLANFW

导出 不加载

ID	Direction	Time	Error	Interface	src-addr	dst-addr	src-ip	dst-ip	BSSID	Protocol	SubType	Prompt
1	40	Jan 5 22:05:29:697	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
2	172	Jan 5 22:05:34:682	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
3	188	Jan 5 22:05:38:624	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
4	214	Jan 5 22:05:49:658	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
5	324	Jan 5 22:05:53:320	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
6	356	Jan 5 22:05:57:190	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
7	368	Jan 5 22:06:05:807	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
8	370	Jan 5 22:06:21:617	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
9	388	Jan 5 22:06:22:507	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
10	442	Jan 5 22:06:26:378	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
11	446	Jan 5 22:06:29:614	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
12	448	Jan 5 22:06:36:996	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
13	464	Jan 5 22:06:51:338	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
14	564	Jan 5 22:06:56:002	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
15	586	Jan 5 22:06:59:939	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.
16	594	Jan 5 22:07:08:689	-	WLAN-Radio1 0/1	943B-B061-9AC0	Broadcast	0.0.0.0	255.255.255.255	----	IPv4	DHCP Discover request	Received a frame from a radio.

Link Type: 1, Length: 22;
 Ver: 0, Type: 2, SubType: 8, Duration: 15360, ProtoType: 0x3100;
 TCDS: 1, FromDS: 1, MoreFrag: 0, Retry: 0, PrvMgt: 0, MoreData: 0, Wep: 1, Order: 0;
 FragNum: 0, SeqNum: 4061, Tid: 4, Flag: 0x0;
 PllRcvTime: 168, CcaChannel: 149, RcvRate: 60, RadioBssi: 35, SNR: 35, NF: 100.

*Jan 5 22:05:29:697 2024 cfdq-sdml-c01f01-ap61 WLANFW/7/PACKETE
 interface = WLAN-Radio1 0/1 payload =
 FF FF FF FF FF FF 94 3B B0 61 9A C0 01 66 02 FF
 53 AD 00 00 FF FF FF FF FF FF 2C DB 07 86 B2 1C
 AA AA 03 00 00 00 81 00 00 5D 08 00 45 00 01 48
 70 15 00 00 40 11 09 91 00 00 00 00 00 00 FF FF FF
 00 44 00 43 01 34 4F 44 01 01 06 00 3A FC TE 0E
 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 2C DB 07 86 B2 1C 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 prompt: Received a frame from a radio.

Received a frame from a radio.
 Transaction: jid: 0x3AFC7E0E
 packet length = 308
 bootpflag = Broadcast

将hex字符串粘贴在这里，按照ASCII码转换后在下方对话框中显示

但是由于工具R2.2.9报文暂未合并对MACFW报文的解析，从工具的开发（就是本人啦）了解到相关功能暂未更新。
 因此只能参考其精心撰写的报文解析原理：
<https://zhiliao.h3c.com/theme/details/202461>
<https://zhiliao.h3c.com/theme/details/216257>

针对报文的hex字符串进行解析，发现FIT AP通过interface G1/0/1口将DHCP Discover报文中送到了PoE的有线口，那么FAT AP和FIT AP完成了终端发送DHCP Discover报文的传递到达有线侧，后续需要做的就是排查有线设备PoE交换机了。

```
*Jan 5 22:05:49:658 2024 cfdq-sdml-c01f01-ap61 MACFW/7/MACFW_PACKET:
Sending, vlan = 93, interface = GigabitEthernet1/0/1, payload =
FF FF FF FF FF FF 2C DB 07 86 B2 1C 81 00 00 5D
08 00 45 00 01 48 70 18 00 00 40 11 09 8E 00 00
00 00 FF FF FF FF 00 44 00 43 01 34 4A BD 01 01
06 00 DC AA E0 E6 00 00 80 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 2C DB 07 86 B2 1C
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Sending an Ethernet frame.
```

7. 现场工程师找来了交换机管理人员，发现原来是近期在PoE交换机上新增配置了有线MAC认证，这才导致终端的DHCP Discover报文被丢弃，导致终端无法获取到IP地址。

解决方法

1. 放通AP到核心交换机之间端口的业务vlan 93，并去掉PoE交换机上的MAC认证配置；
2. 后续建议将现场该区域所有FAT AP改为FIT AP，通过瘦瘦桥接由AC统一纳管，然后走CAPWAP隧道转发，这样AP和核心交换机中间的交换机端口就可以不必放通业务vlan 93了。