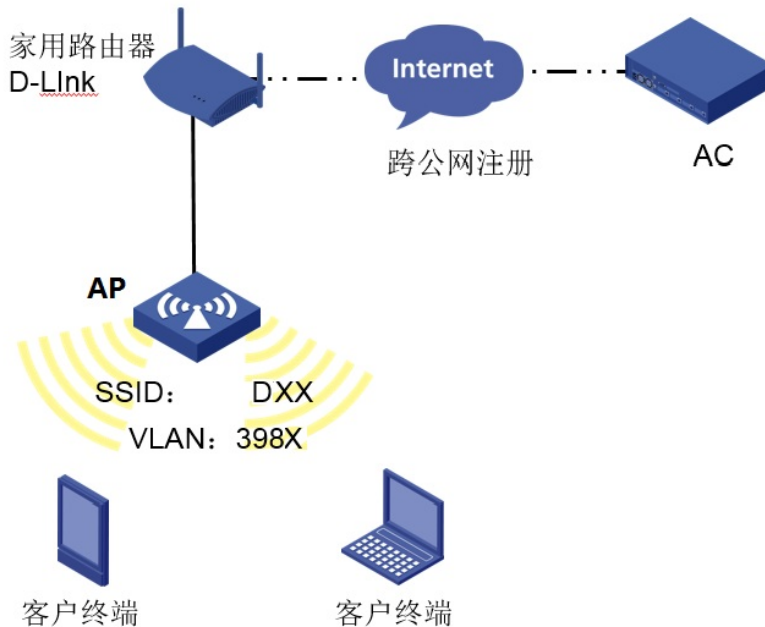


知 AP连接家用路由器进行跨公网注册后，终端无法上线的问题排查

AP管理 wlan接入 徐猛 2018-03-18 发表

某局点采用AP跨公网注册的方式进行无线环境组网，大致组网环境如下，AC处于公网中，连接在电信的运行商网络下。现该局点有部分学校需要进行无线网络的覆盖安装。这些学校均使用的是电信的网络接入学校，采用D-Link品牌家用路由器接入电信的ONU中，实现和公网的互联。在完成一系列AP的注册以及AC上的配置后，进行网络测试，结果发现，使用终端进行连接时，终端始终无法获取地址，无法正常的上线。（为保护隐私，本案例中使用D**代替现场使用的SSID名，同时部分可能包含隐私的部分均使用*号进行了替换）



使用终端测试时，终端的联网状态情况为：

1. 安卓手机连接测试时，一直显示正在连接并无法连接成功：
3. 苹果手机连接测试时，直接提示无法加入网络D**：

由如上测试可以看出终端始终无法获取地址并关联到AP上，且可以确定该问题与终端的系统平台无关。

1. 先检查使用该组网方式的AP是否能够正常的获取IP地址，在AC上的注册状态是否为R/M(即注册成功状态)，结果发现AP均能正常注册：

```
<HE-HD-H3C-1.MAN.AC>display wlan ap all
```

```
Total number of APs: 111
```

```
Total number of connected APs: 80
```

```
Total number of connected manual APs: 80
```

```
Total number of connected auto APs: 0
```

```
Total number of connected common APs: 80
```

```
Total number of connected WTUs: 0
```

```
Total number of inside APs: 0
```

```
Maximum supported APs: 3072
```

```
Remaining APs: 2992
```

```
Total AP licenses: 512
```

```
Remaining AP licenses: 432
```

```
AP information
```

```
State : I = Idle, J = Join, JA = JoinAck, IL = ImageLoad
```

```
C = Config, DC = DataCheck, R = Run, M = Master, B = Backup
```

AP name	APID	State	Model	Serial ID
D**-1	58	R/M	WA4320	219801A0UE8175E039**
D**-2	59	R/M	WA4320	219801A0UE8175E013**

D**3	60	R/M	WA4320	219801A0UE8175E016**
D**4	61	R/M	WA4320	219801A0UE8175E152**
D**5	62	R/M	WA4320	219801A0UE8175E022**
D**6	63	R/M	WA4320	219801A0UE8175E034**

2.通过display dhcp server free-ip 命令查看地址池资源,发现地址池资源充足,不存在地址池用完的情况

3.检查AC及链路上的相关配置,地址池以及服务模板均配置正确,服务模板与AP模板的绑定等配置也均无问题

4.引导现场工程师收集相关debug capwap all以及debug wlan client verbose信息进行分析(测试认证终端MAC为:****-2e45-253f)

```
*Dec 4 16:26:10:700 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/FSM: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49e0] Received authentication request in the Unauth state.
```

```
*Dec 4 16:26:10:701 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Event: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49e0] Processed authentication request successfully, and sent authentication response.
```

//处理认证请求成功,并且发送认证响应。

```
*Dec 4 16:26:10:701 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Timer: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49e0] Created state timer.
```

```
*Dec 4 16:26:10:701 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/FSM: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49e0] Changed the client's state from Unauth to Auth. //记录认证成功终端的表项
```

```
*Dec 4 16:26:11:761 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/FSM: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49e0] Received authentication request in the Auth state. //再次受到已认证终端的认证请求
```

对该debug wlan client 过程进行分析发现,AC端已经对终端认证成功并发出了认证成功的响应报文,但终端可能未收到认证成功的响应报文,从而认为自己还未认证成功,进而继续发送认证请求报文,AC继续进行认证及回应,整个过程形成一个死循环,使终端使用无法成功上线。

5.后来猜测问题可能出在AP与AC之间的中间链路设备上,于是引导现场工程师进行家用路由器的替换测试,将D-LINK品牌家用路由器替换为飞鱼星品牌仍然不行,后又建议工程师替换为TP-LINK品牌家用路由器后,终端此时能够正常获取IP地址和上线,以下为现场收集的替换为TP-LINK家用路由器后的debug wlan client信息,可以看到终端做了认证后,由认证状态转变为上线状态。

..... (认证过程,参考步骤4中内容,此处不再赘述)

```
*Dec 4 15:51:23:855 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/FSM: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Received association request in the Auth state.
```

```
*Dec 4 15:51:23:855 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/FSM: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Client state: Auth.
```

```
*Dec 4 15:51:23:855 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Event: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Checking (re)association load of the device.
```

```
*Dec 4 15:51:23:856 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Event: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Processing fields and IE in the (re)association request.
```

```
*Dec 4 15:51:23:856 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Event: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Processed (re)association request successfully when the client was in Auth state.
```

```
*Dec 4 15:51:23:856 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Event: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Processed (re)association request successfully, and sent (re)association response.
```

.....

```
%Dec 4 15:51:23:885 2017 HE-HD-H3C-1.MAN.AC STAMGR/6/STAMGR_CLIENT_ONLINE: Client ****-2e45-253f went online from BSS ****-8362-49f1 with SSID D** on AP ceshi11. State changed to Run.
```

//终端成功关联AP并转变为上线状态

```
*Dec 4 15:51:23:888 2017 HE-HD-H3C-1.MAN.AC STAMGR/7/Timer: [APID: 114] [MAC: ****-2e45-253f, BSSID: ****-8362-49f1] Created idle timer.
```

```
%Dec 4 15:51:24:336 2017 HE-HD-H3C-1.MAN.AC STAMGR/6/STAMGR_CLIENT_SNOOPING: Detected client IP change:Client MAC: ****-2e45-253f, IP: 27.188.4.185 -NA-, -NA-, -NA-, Username: -NA-, AP name: ceshi11, Radio ID: 2, Channel number: 11, SSID: D**, BSSID: ****-8362-49f1. //终端成功获取IP地址
```

6.根据整个分析过程,我们得出结论,问题应该是出在了中间的家用户路由器设备上。

根据AP和AC通信过程中报文的封装及转发流程,我们发现应该是D-LINK品牌和飞鱼星品牌的家用路由器对我司CAPWAP隧道封装使用的UDP端口做了拦截。

下面对我司无线组网中的端口做一个说明:V7中的CAPWAP隧道使用5246端口做控制端口进行控制隧道封装,5247端口作为数据端口进行通信数据报文封装,V5中的LWAPP隧道中AC使用12223端口进行控制隧道封装,使用12222端口进行数据隧道封装。

现场咨询了飞鱼星以及D-LINK厂家后进行了确认，该品牌家用路由器在开启快速模式时，会对一些端口的报文做丢弃动作，其中就包含我司的无线隧道通信数据报文封装端口。关闭该功能后，问题解决。

当无线组网环境下，AP采用公网进行注册时，中间途径的设备环境比较多，组网也比较复杂，一定要先确保中间设备对我司无线报文转发过程中使用协议端口号是放通的，否则会导致终端上线失败的情况产生。