某局点V7 AC PSK加密后终端获取不到地址经验案例

wlan接入 wlan安全 陈孙潇 2017-06-22 发表

现场使用我司WX3510H作为无线控制器，AP为WA4320-ACN-C，使用PSK加密的方式上网。现场测试发现使用PSK加密后，终端获取不到地址。当把PSK加密去除，使用无加密的方式直接上网测试正常，可以获取到DHCP地址。

1、首先检查AC上PSK加密相关配置，发现配置上并没有任何问题。查看现场PSK的加密套件使用的是ccmp+rsn的方式，怀疑是和终端的加密算法有兼容适配性问题，因此便把tkip+wpa的加密套件也配置上。但是配置上后测试发现终端依然获取不到地址。

```
wlan service-template 3
 ssid Guest
 vlan 16
 akm mode psk
 preshared-key pass-phrase cipher $c$3$TEZbLXBkUkVGRpj9YDECOIDktqe8QuRwr7Cw
 cipher-suite ccmp
 cipher-suite tkip
 security-ie rsn
 security-ie wpa
 service-template enable
```

2、排除加密算法兼容问题后，便按照DHCP获取不到地址的的排查思路，通过debugging dhcp server all信息查看终端和DHCP服务器的报文交互是否有什么问题。现场AC旁挂在我司S5560交换机上，并且DHCP Server起在该交换机上，因此便在S5560上开启debug信息查看。但是在设备上开启terminal debug和terminal monitor后发现并没有任何关于测试终端的信息。

3、交换机上收集不到debug dhcp的信息，因此便在AC上收集下debug mac all信息查看该终端的相关信息，发现依旧没有任何信息输出。

4、收集不到任何信息，怀疑是否有可能版本问题，查看AC版本为R5205P02，已经是目前官网最新版本。查看AP上版本，发现却是ESS2109这一版本，跟AC上的版本不匹配。为什么AP和AC版本会不匹配呢？这时候再检查AC上的配置，发现AP组里面开启了firmware-upgrade disable，该命令是用来关闭AP升级功能的。于是让现场工程师将该命令去掉，让AP升级到和AC相同的版本后再进行测试，发现可以正常获取到地址了。

```
wlan ap-group default-group
 firmware-upgrade disable
 broadcast-probe reply disable
 vlan 1
  ap-model WA4320-ACN-C
```

目前V5和V7都存在AC和AP版本跨度太大导致加密认证异常的情况，需要开启firmware-upgrade enable，保持AP版本和AC版本统一。

AP版本默认情况下就是跟随AC升级的，建议在没有特殊需求的情况下，不要使用firmware-upgrade enable命令关闭AP升级功能。