某局点 WX2540H 无线终端经常掉线问题排查

wlan安全 WIPS wlan优化 **zhiliao_tnNTSE** 2021-01-31 发表

组网及说明

不涉及

问题描述

现场终端连接无线后使用过程中，频繁出现无线连接中断4-5s（终端上对应无线wifi图标消失），然后又重新连上的问题；大部分终端均有问题，现场主要终端类型是苹果电脑。现场表示终端连接小的家用路由器测试无问题。

过程分析

依据现场所有的SSID都会导致大部分终端掉线的情况，结合debug wlan client mac xxxx 和抓包分析，认为两种可能性：

1、 极大可能是现场有其他的设备反制了无线SSID；

分析如下：

因为从AP的debug来看是,终端的掉线原因都是AC收到了终端主动发送的去关联和去认证报文：

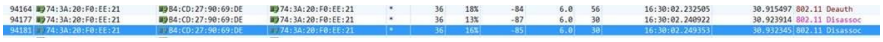
Line 7337: %Dec 29 16:30:21:438 2020 WLC2540H STAMGR/6/STAMGR_CLIENT_OFFLINE: Client b4cd-2790-69de went offline from BSS 743a-20f0-ee22 with SSID my-test on AP fzee20 Radio ID 1. State changed to Unauth. Reason: Received disassociation frame in Run state: reason code=2

Line 9922: %Dec 29 16:30:39:605 2020 WLC2540H STAMGR/6/STAMGR_CLIENT_OFFLINE: Client b4cd-2790-69de went offline from BSS 743a-20f0-ee22 with SSID my-test on AP fzee20 Radio ID 1. State changed to Unauth. Reason: Received disassociation frame in Run state: reason code=2

Line 22490: %Dec 29 16:32:22:693 2020 WLC2540H STAMGR/6/STAMGR_CLIENT_OFFLINE: Client b4cd-2790-69de went offline from BSS 743a-20f0-ee22 with SSID my-test on AP fzee20 Radio ID 1. State changed to Unauth. Reason: Received deauthentication frame in Run state: reason code=3

而从空口抓包来看，看到的都是BSSID为743a-20f0-ee22的设备主动发送的disassociation报文；并且抓包的苹果电脑是没有移动的，但是它收到的743a-20f0-ee22的AP的发出报文的信号强度有-87和-53，两个差别这么大，怀疑是非法AP和正常AP发出的：

还有一点怀疑点是这个终端b4cd-2790-69de实际连接的只有这个BSSID的信号743a-20f0-ee22，但是空口抓包里面却有BSSID是743a-20f0-ee21的设备一直给这个终端发送disassociation或者deauth报文。



因此，综合以上分析，怀疑是有其他设备仿冒我们的AP给终端不停的发Deauth或者Disassoc报文。

2、 还有一种可能性是：

终端上线过程中，可能存在延时，导致终端已经发数据报文时，ac还没有把终端信息下到ap上，这种情况下，每个数据报文都会触发AP主动发一个reason6的deauth报文。

这种可能性可以在服务模板配置以下命令，这个命令会改为收到报文不发deauth，仅丢弃报文：

[WX5510E-wlan-st-1]unknown-client drop

如果配置了这个命令还是不行，基本上就可以确认现场是被反制了。如果是被反制了，就要人工一点一点去找反制源头。知了有相关排查案例，可以参考一下，不是完全一样https://zhiliao.h3c.com/Theme/details/5591。

解决方法

现场存在反制源，排查之后发现确实存在。