某局点macbook终端被反制导致频繁上下线

wlan接入 wlan安全 **周睿** 2021-02-08 发表

组网及说明

不涉及

问题描述

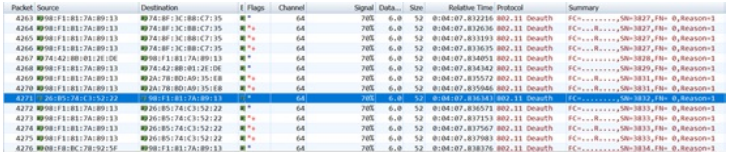
某局点出现macbook连接SSID频繁掉线的情况，故障现象偶发复现，没有发生漫游，终端在同一个AP下反复掉线重连，如下所示。

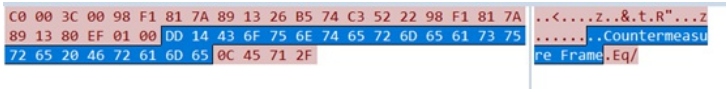
BSSID	Created at	Online time	AC IP address	RID	AP name
88df-9e8d-d1e3	2021-02-01 14:53:31	00h 04m 13s	127.0.0.1	2	l3-5-11-s
88df-9e8d-d1e3	2021-02-01 14:53:29	00h 00m 02s	127.0.0.1	2	l3-5-11-s
88df-9e8d-d1e3	2021-02-01 14:53:27	00h 00m 01s	127.0.0.1	2	l3-5-11-s
88df-9e8d-d1e3	2021-02-01 14:53:23	00h 00m 02s	127.0.0.1	2	l3-5-11-s
88df-9e8d-d1e3	2021-02-01 14:52:57	00h 00m 24s	127.0.0.1	2	l3-5-11-s
88df-9e8d-d1e3	2021-02-01 14:52:53	00h 00m 02s	127.0.0.1	2	l3-5-11-s

过程分析

检查配置，AP空口正常，radio口下配置了max-count 30，怀疑和客户端限制数有关，当AP在线终端数达到限制后，在beacon帧会隐藏ssid，部分终端感知到beacon帧不携带ssid后，会认为该无线网络异常，出现掉线重连的情况，将客户端数量限制删除后，故障依旧复现。

初步怀疑该无线网络信号遭到wips反制攻击，于是空口抓包分析。空口抓包报文发现有大量的deauthentication帧，并且deauth报文的SN都是连续的。而且这些deauthentication帧发现为Countermeasure Frame帧。





查看反制记录，确实有大量反制记录。

[wips_AC]display wips virtual-security-domain vsd_sina countermeasure record

MAC address	Type	Reason	Countermeasure AP	Radio ID	Time
80e4-55dc-21a5	AP	Class	l6-1-08	1	2021-02-02/15:05:42
80e4-55dc-2270	AP	Class	l3-1-05	1	2021-02-02/15:06:25
80e4-55dc-2270	AP	Class	l3-2-08-n	1	2021-02-02/15:06:25
80e4-55dc-2271	AP	Class	l3-1-05	1	2021-02-02/15:06:25
80e4-55dc-2271	AP	Class	l3-2-08-n	1	2021-02-02/15:06:25
80e4-55dc-2272	AP	Class	l3-1-05	1	2021-02-02/15:06:25
80e4-55dc-2272	AP	Class	l3-2-08-n	1	2021-02-02/15:06:25
80e4-55dc-2273	AP	Class	l3-1-05	1	2021-02-02/15:06:25
80e4-55dc-2273	AP	Class	l3-2-08-n	1	2021-02-02/15:06:25
80e4-55dc-2274	AP	Class	l3-1-05	1	2021-02-02/15:06:25
80e4-55dc-2274	AP	Class	l3-2-08-n	1	2021-02-02/15:06:25
80e4-55dc-2bc0	AP	Class	l3-5-10	1	2021-02-02/15:05:57
80e4-55dc-2bc0	AP	Class	l3-5-10	1	2021-02-02/15:07:59

原因是该局点开启了wips反制功能，由于新加了一批AP，没有在wips的AP分配策略里添加trust oui。

解决方法

在wips的AP分配策略里添加新AP的trust oui，业务恢复正常。