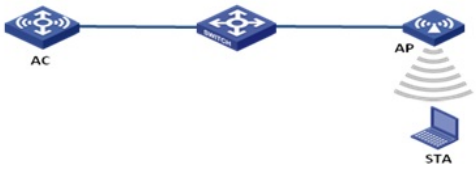
某局点安卓无线终端随机掉线的经验案例

DNS NAT 余晨 2014-10-22 发表

某局点安卓无线终端随机掉线的经验案例

一、 组网：



二、 问题描述：

该局点AC WX5540E , WA2620i-AGN Fit AP组网，出现部分终端（小米3，三星等安卓类型）随机出现掉线，PC、IOS终端使用正常情况。且问题发生前后没有组网变动。

三、 过程分析：

通过debug 调试信息，发现出现如下报错：

WMAC/7/ERROR : Failed to parse group management cipher suite, invalid suite 加密组件解析失败

。

通过空口抓包，从出现rsn ie加密字段时，观察客户端发出的报文可以看出rsn information中携带了18字节未知数据，查看这18字节数据，发现其与签名PMKID字段内容完全一致，但其格式存在问题。

```
RSN Information
    Element ID:             48  RSN Information
    Length:                 56
    Version:                1
    Group Cipher OUI:       00-0F-AC
    Group Cipher Type:      4  CCMP - default in an RSN
    Pairwise Cipher Count:1
    PairwiseKey Cipher List
        Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN
    AuthKey Mngmnt Count: 1
    AuthKey Mngmnt Suite List
        AKMP Suite OUI:       00-0F-AC-01  802.1X Authentication
    RSN Capabilities:       %0000000000000000
                              xxxxxxxx x....... Reserved
                              ........ ..00.... GTKSA Replay Ctr: 0 - 1 replay counter
                              ........ ....00.. PTKSA Replay Ctr: 0 - 1 replay counter
                              ........ ......0. Does not Support No Pairwise
                              ........ .......0 Does Not Support Pre-Authentication
    PMKID Count:            1
    PMKID:                  0xC41AD5F46F25BA4681E2D435D1D2164B
    Remaining Data:         (18 bytes)
```

根据802.11协议的规定，RSN IE的标准结构应该是：

8.4.2.27 RSNE

8.4.2.27.1 General

The RSNE contains authentication and pairwise cipher suite selectors, a single group data cipher suite selector, an RSN Capabilities field, the PMK identifier (PMKID) count, a PMKID list, and a single group management cipher suite selector. See Figure 8-186. The size of the RSNE is limited by the size of an element, which is 255 octets. Therefore, the number of pairwise cipher suites, AKM suites, and PMKIDs is limited.

	Element ID	Length	Version	Group Data Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List
Octets:	1	1	2	4	2	4 × *m*

	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKIDCount	PMKID List	Group Management Cipher Suite
Octets:	2	4 × *n*	2	2	16 × *s*	4

Figure 8-186—RSNE format

PMKID后边，只有可选的Group Mangement字段了。而如果要携带多个PMKID，只需要在PMKID的头两个字节，标示自己的count就行了。

所以问题就明确了，安卓或者某些客户端，在运行一段时间之后，准备快速漫游的时候，内部程序会

出错，导致它会把自己准备携带的最后一个字段复制两次，出现了错误的Group Management字段，就导致了上线失败。 之所以肯定，不是它想携带两个PMKID，而是它程序出错，是因为看报文内容，第二次的18个字节明显和前面18个一模一样，如果要携带两个PMKID，格式应该是 2 +16 + 16的格式，头两个字节标示自己带了几个就可以了，这是协议的标准规定。所以综上，现网就是由于安卓等无线终端快速漫游发出的RSN IE异常引起的。

四、 解决方法：

这种错误，我们没办法给出标准的兼容方法，毕竟它的原因是客户端实现错误，属于标准协议规定之外的情况，只能终端升级安卓版本才能根本解决。