

医用PDA异常下线后无法再重新关联原有的AP 问题处理

一、组网说明:

XX医院采用我司AC+瘦AP的组网模式，SSID使用明文方式，终端动态获取IP地址。

二、问题描述:

XX医院使用的PDA异常下线后，无法再重新关联原有的AP，手动重启PDA后同样无法再重新关联原有的AP。

三、问题分析:

1. 正常情况下，PDA第一次关联AP成功的过程

158	Ethernet Broadcast	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.155054	802.11 Beacon
159	Ethernet Broadcast	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.257454	802.11 Beacon
160	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	15.323626	802.11 Probe Req
161	Ethernet Broadcast	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.359789	802.11 Beacon
162	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	15.417448	802.11 Probe Req
163	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.418923	802.11 Probe Req
164	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.419199	802.11 Ack
165	Ethernet Broadcast	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.462182	802.11 Beacon
166	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	34	15.554192	802.11 Auth
167	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.554567	802.11 Ack
168	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	34	15.559433	802.11 Auth
169	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.559753	802.11 Ack
170	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	77	15.560948	802.11 Assoc Req
171	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.561221	802.11 Ack
172	Ethernet Broadcast	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	134	15.564638	802.11 Beacon
173	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	50	15.570364	802.11 Assoc Req
174	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.570879	802.11 Ack
175	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	1.0	135	15.590174	EAPOL-Key
176	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	1.0	14	15.590553	802.11 Ack
177	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	5.5	161	15.596345	EAPOL-Key
178	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	5.5	14	15.596490	802.11 Ack
179	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	2.0	161	15.599912	EAPOL-Key
180	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	2.0	14	15.600051	802.11 Ack
181	00:23:89:4b:2c:f0	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	5.5	135	15.602536	EAPOL-Key
182	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	00:23:89:4b:2c:f0	FF	1	0x	5.5	14	15.602565	802.11 Ack
183	Ethernet Broadcast	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	5.5	84	15.605888	802.11 TXOP Data
184	Ethernet Broadcast	Sychip:2C:CB:B7	00:23:89:4b:2c:f0	FF	1	0x	5.5	84	15.607099	802.11 TXOP Data

第162号报文是一个probe request，展开如下所示：

802.11 MAC Header	
Version:	0
Type:	%00 Management
Subtype:	%0100 Probe Request
Frame Control Flags:	%00010000
0... .. Non-strict order	
.0.. .. Non-Protected Frame	
..0..... No More Data	
...1.... Power Management - power save mode	
.... 0... This is not a Re-Transmission	
.... .0.. Last or Unfragmented Frame	
.... ..0. Not an Exit from the Distribution System	
.... ..0 Not to the Distribution System	
Duration:	0 Microseconds
Destination:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Source:	00:0B:6C:2C:CB:B7 Sychip:2C:CB:B7
BSSID:	FF:FF:FF:FF:FF:FF Ethernet Broadcast
Seq Number:	5
Frag Number:	0
802.11 Management - Probe Request	
SSID	
Element ID:	0 SSID
Length:	4
SSID:	mzsy

PS:

- 简单的说，PDA关联AP的过程就是从162号报文(probe request)开始。从目前看来，目前市场上主流的无线网卡是会在probe request中携带休眠标记的(图中红框所示)。
 - 当PDA第一次关联一个新的AP时，因为AP上这个客户端并不存在，所以对于probe request报文中的休眠标记不予理会，直接回复probe response(第163号报文)。PDA收到后，继续发送auth(166号报文)继续接下来的关联过程，直至完成。
2. 如果PDA出现掉线后，PDA无法重新关联AP

193	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	32.738355	802.11 Probe Req
194	Ethernet Broadcast	00:23:89:36:68:90	00:23:89:36:68:90	FF	1	0x	1.0	134	32.765495	802.11 Beacon
195	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	32.818274	802.11 Probe Req
196	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	32.832653	802.11 Probe Req
197	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	32.918271	802.11 Probe Req
198	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	32.935589	802.11 Probe Req
199	Ethernet Broadcast	00:23:89:36:68:90	00:23:89:36:68:90	FF	1	0x	1.0	134	32.970514	802.11 Beacon
200	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	33.025002	802.11 Probe Req
201	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	33.041788	802.11 Probe Req
202	Ethernet Broadcast	00:23:89:36:68:90	00:23:89:36:68:90	FF	1	0x	1.0	134	33.072636	802.11 Beacon
203	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	33.141471	802.11 Probe Req
204	Ethernet Broadcast	00:0F:2E:11:14:6D	00:23:89:36:68:90	FF	1	0x	1.0	102	33.689172	802.11 TXOP Data
205	Ethernet Broadcast	00:23:89:36:68:90	00:23:89:36:68:90	FF	1	0x	1.0	134	33.994297	802.11 Beacon
206	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	34.245838	802.11 Probe Req
207	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	34.263138	802.11 Probe Req
208	Ethernet Broadcast	Sychip:2C:CB:B7	Ethernet Broadcast	*	1	0x	1.0	40	34.401758	802.11 Probe Req
209	Ethernet Broadcast	00:23:89:36:68:90	00:23:89:36:68:90	FF	1	0x	1.0	134	34.813481	802.11 Beacon

第194号报文是一个beacon，展开如下所示：



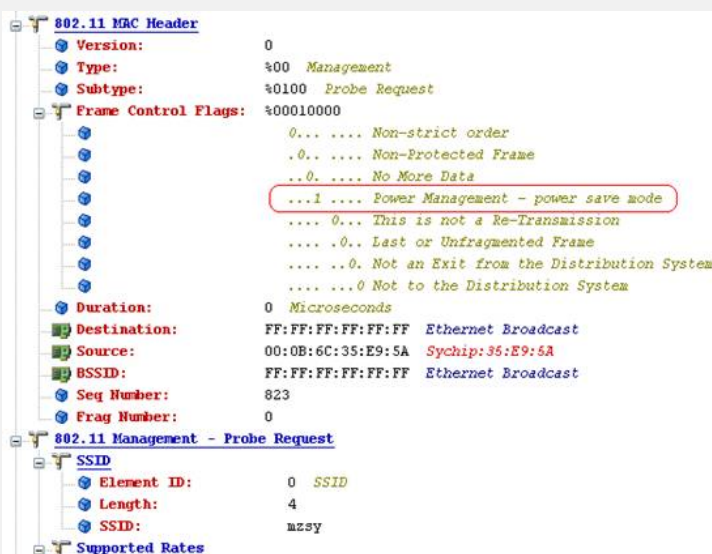
PS:

- 1) PDA掉线后，由于PDA没有向AP发送de-authentication断开连接报文，所以AP继续认为此PDA在线，并且保留有客户端的信息。
 - 2) 根据协议，收到客户端的报文中携带休眠标记时则认为客户端处于休眠状态，不能把发送给客户端的报文直接发送出去，而是把报文缓存起来，并且通过beacon携带信息（上图红框所示）来通知客户端；当客户端苏醒后需要主动发送报文获取“AP上为客户端缓存的报文”。
 - 3) 通过上面抓包，掉线后的PDA在不断的发送probe request，但是由于probe request表明了PDA要睡眠（睡眠标志为1），所以AP所有发送的probe response被缓存起来，并且通过beacon来通知PDA“AP有数据需要发送”。但是PDA始终没有苏醒过来，也不会主动向AP获取报文（苏醒过来的话会发送一个null报文携带苏醒标记），从而造成PDA无法获取probe response，而在此种情况下，PDA就不进行后续的关联过程，最终导致PDA无法注册成功。
3. PDA连接成功后，休眠苏醒过程的处理介绍

2406	Ethernet Broadcast	Sychip:35:E9:5A	Ethernet Broadcast	*	1	0x	1.0	40	0:02:43:118194	802.11 Probe Req
2407	Ethernet Broadcast	00:23:89:40:2C:FD	00:23:89:40:2C:FD	*/	1	0x	1.0	134	0:02:43:163924	802.11 Beacon
2408	00:23:89:40:2C:FD	Sychip:35:E9:5A	00:23:89:40:2C:FD	*/	1	0x	2.0	29	0:02:43:163163	802.11 Null Data
2409	Sychip:35:E9:5A	00:23:89:40:2C:FD	00:23:89:40:2C:FD	*/	1	0x	2.0	14	0:02:43:165427	802.11 Ack
2410	Sychip:35:E9:5A	00:23:89:40:2C:FD	00:23:89:40:2C:FD	*/	1	0x	1.0	128	0:02:43:166729	802.11 Probe Req
2411	00:23:89:40:2C:FD	Sychip:35:E9:5A	00:23:89:40:2C:FD	*/	1	0x	1.0	14	0:02:43:167107	802.11 Ack
2412	Sychip:35:E9:5A	00:23:89:40:2C:FD	00:23:89:40:2C:FD	*/	1	0x	1.0	128	0:02:43:168476	802.11 Probe Req

第2406

号报文是一个probe request，展开如下所示：



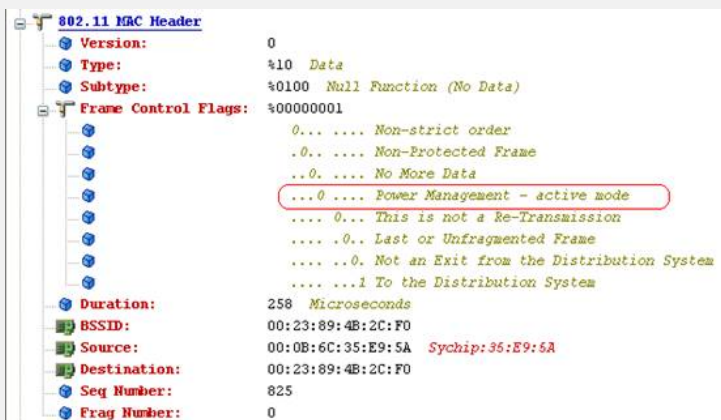
第2407

号报文是一个beacon，展开如下所示：



第240

8号报文是一个null，展开如下所示：



PDA正常在线的时候，会定期发送probe request来探测网络。这种情况下，因为probe request（2406号报文）中携带了休眠标记，AP缓存probe response，并且通过beacon（2407号报文）试图唤醒PDA。PDA收到beacon后回复了一个null（2408号报文），里面没有携带休眠标记，也就是在声明自己苏醒过来了。AP收到这个null报文后才认为PDA已经苏醒，从而把缓存的probe response发送出去。

四、解决方法：

1. PDA可以处理AP直接回复的probe response报文，说明PDA实际上并没有休眠，也就是PDA对于休眠的处理有问题（参见分析1）。
2. 在关联过程中和关联成功以后对于休眠的处理表现不一致（参见分析3和分析2）。
3. 总之，PDA的每一个probe request报文都携带休眠标志，不但与协议不符，而且与实际情况不符合，最终导致该现象的出现。
4. 由于是PDA没有遵循规范操作，建议PDA厂商修改驱动解决该问题。