13.9.3 成功的 WPA 认证

WPA 使用了与 WEP 完全不同的认证机制，但它仍然依赖于用户在无线客户端输入的密码来连接到网络。80211-WPAauth.pcap 文件中有一个成功的 WPA 认证的例子。

该文件的第 1 个数据包是 WAP 发送的 beacon 广播。我们展开这个数据包的 802.11 头部，沿着 tagged parameters 往下看，展开 Vendor Specific 标题，如图 13-16 所示，能看到无线接入点的 WPA❶ 属性部分。这让我们了解到 WAP 支持的 WPA 版本与实现（如果有的话）。

无线客户端（00:0f:b5:88:ac:82）收到这个 beacon 广播后，就向无线接入点（00:14:6c:7e:40:80）发送一个探测请求，并得到了响应。无线客户端和无线接入点在数据包 4 到 7 之间的交互，是认证与关联的请求及响应。

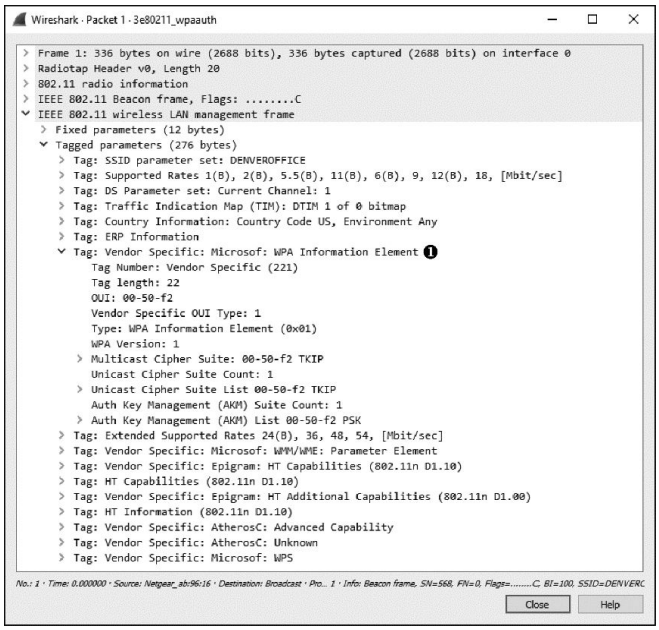

图 13-16　这个 beacon 让我们知道无线接入点支持 WPA 认证

现在把目光转移到数据包 8 上。这是 WPA 开始握手的地方，一直持续到数据包 11。这个握手过程就是 WPA 质询响应的过程，如图 13-17 所示。

No.	Time	Source	Destination	Protocol	Length	Channel	Signal strength (dBm)	Data rate	Info
8	0.…	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	157	1	-18	24	Key (Message 1 of 4)
9	0.…	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	183	1	-42	1	Key (Message 2 of 4)
10	0.…	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	181	1	-18	36	Key (Message 3 of 4)
11	0.…	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	157	1	-42	1	Key (Message 4 of 4)

图 13-17　这些数据包是 WPA 握手的一部分

这里有两个质询与响应。每个数据包都可在基于 802.1x Authentication 头部下的 Replay Counter 域找到匹配对象，如图 13-18 所示。注意到前两个握手数据包的 Replay Counter 值是 1❶，而后两个握手数据包的值是 2❷。

WPA 握手完成并认证成功后，数据就开始在无线客户端和 WAP 之间传输了。

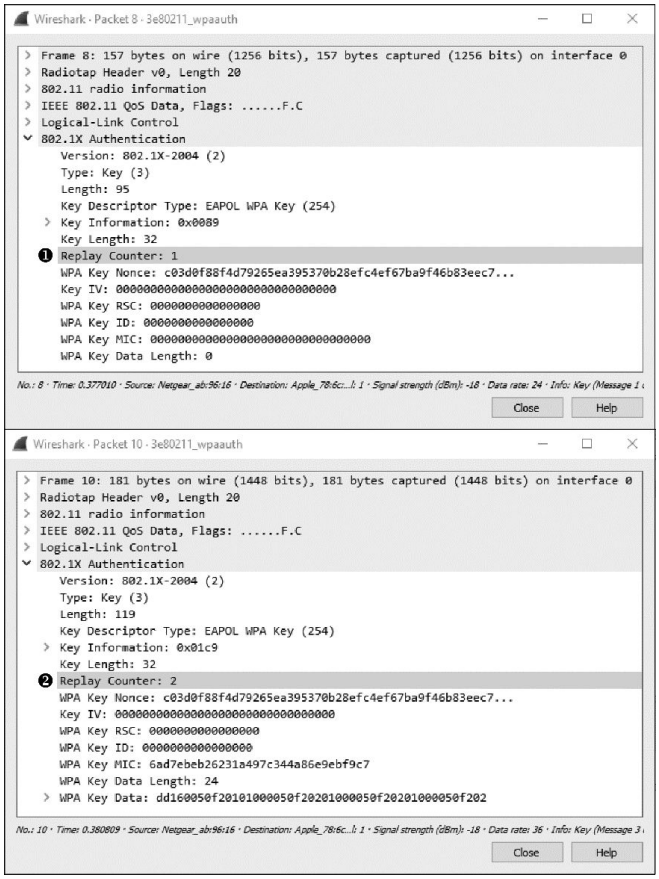

图 13-18　Replay Counter 域帮助我们匹配质询和响应