13.9.4 失败的 WPA 认证

与 WEP 一样，用户输入 WPA 密码后，无线客户端程序报告无法连接到无线网络，但没有指出问题在哪里，我们来看一看发生了什么。捕获的结果保存在 80211-WPAauthfail.pcap 文件中。

像刚才成功的 WPA 认证那样，捕获文件以同样的方式开始。这包括探测、认证和关联请求。WPA 握手从数据包 8 开始，但在这个例子中，我们看到了 8 个握手数据包，而不是之前在成功认证环节中看到的 4 个。

数据包 8 和 9 表示 WPA 握手的前两个数据包。然而在这个例子中，客户端发送回 WAP 的质询文本有误。结果，这个序列在数据包 10 和 11、12 和 13、14 和 15 中多次重复，如图 13-19 所示。使用 Replay Counter 可以配对每个请求和响应。

No.	Time	Source	Destination	Protocol	Length	Channel	Signal strength (dBm)	Data rate	Info
8	0.073773	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	157	1	-18	24	Key (Message 1 of 4)
9	0.076510	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	183	1	-30	1	Key (Message 2 of 4)
10	1.074290	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	157	1	-19	24	Key (Message 1 of 4)
11	1.076573	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	183	1	-32	1	Key (Message 2 of 4)
12	2.075292	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	157	1	-18	36	Key (Message 1 of 4)
13	2.077610	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	183	1	-29	1	Key (Message 2 of 4)
14	3.077211	Netgear_ab:96:16	Apple_78:6c:9c	EAPOL	157	1	-18	48	Key (Message 1 of 4)
15	3.079537	Apple_78:6c:9c	Netgear_ab:96:16	EAPOL	183	1	-32	1	Key (Message 2 of 4)

图 13-19　这里的额外 EAPOL 数据包表明 WPA 认证失败了

握手过程重试 4 次后，通信中止了。如图 13-20 所示，数据包 16 表明无线客户端没有通过认证 ❶。

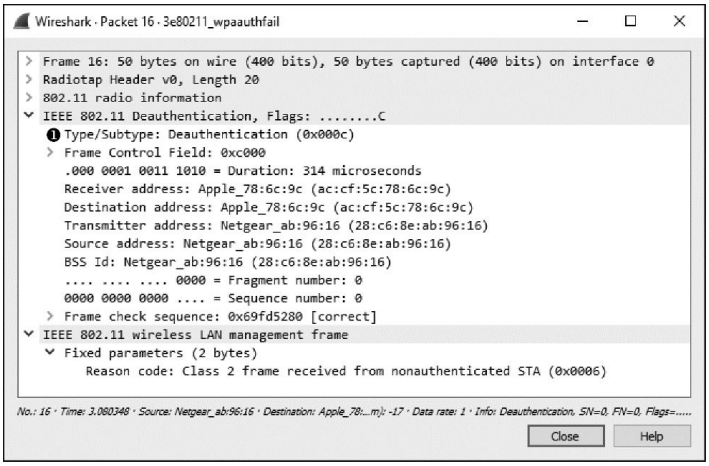

图 13-20　WPA 握手失败后，客户端认证失败