13.1.1 一次嗅探一个信道

当从无线局域网（Wireless Local Area Network，WLAN）捕获流量时，最特殊的莫过于无线频谱是共享介质。不像有线网络的每个客户端都有它自己的网线连接到交换机，无线通信的介质是客户端共享的空域。单个 WLAN 只占用 802.11 频谱的一部分。这允许同一个物理空间的多个系统在频谱不同的部分进行操作。

> 注意
>
> 无线网络的基础是美国电子和电气工程师协会（Institute of Electrical and Electronics Engineers，IEEE）开发的 802.11 标准。整章涉及的「无线网络」「WLAN」等术语均指 802.11 标准中的网络。

空间上的分离是通过将频谱划分为不同信道实现的。一个信道只是 802.11 无线频谱的一部分。在美国，有 11 个信道可用（有些国家允许使用更多的信道）。这是很重要的，因为 WLAN 同时只能操作一个信道，就意味着我们只能同时嗅探一个信道，如图 13-1 所示。所以，如果你要处理信道 6 的 WLAN，就必须将系统配置成捕获信道 6 的流量。

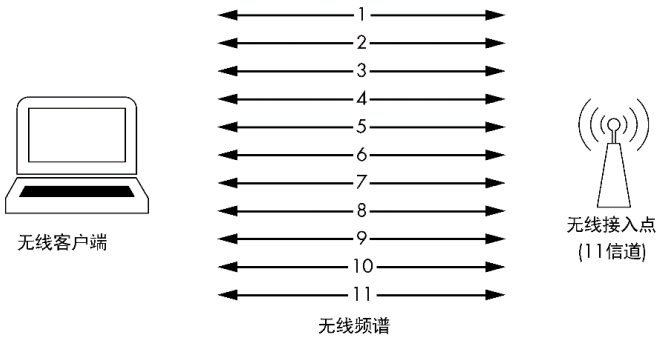

图 13-1　嗅探无线网络很麻烦，因为同一时间只能处理一个信道

> 注意
>
> 传统的无线嗅探只能同时处理一个信道，但有一个例外：某些无线扫描应用程序使用「跳频」技术，可以迅速改变监听信道以收集更多数据。其中一个很流行的工具是 Kismet 可以每秒跳跃 10 个信道，从而高效地嗅探多个信道。