13.5 802.11 数据包结构

无线数据包与有线数据包的主要不同在于额外的 802.11 头部。这是一个第 2 层的头部，包含与数据包和传输介质有关的额外信息。802.11 分组有 3 种类型。

管理：这些分组用于在主机之间建立 2 层连接。管理分组还有一些重要的子类型，包括认证（authentication）、关联（association）和信号（beacon）分组。

控制：控制分组允许管理分组和数据分组的发送，并与拥塞管理有关。常见的子类型包括请求发送（request-to-send）和准予发送（clear-to-send）分组。

数据：这些分组含有真正的数据，也是唯一可以从无线网络转发到有线网络的数据包。

一个无线数据包的类型和子类型决定了它的结构，因此各种数据包结构可能不计其数。我们将考察其中一种结构，请看 80211beacon.pcap 文件里的单个数据包。这个文件包含一种叫 beacon 的管理数据包的例子，如图 13-9 所示。

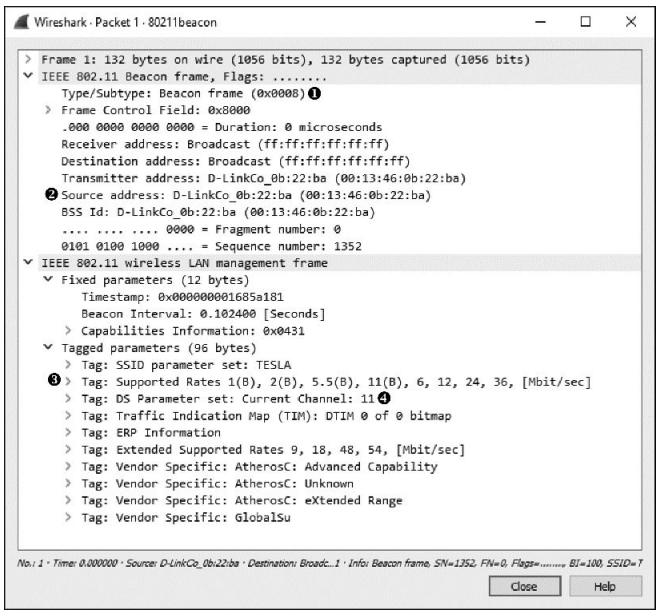

图 13-9　这是一个 802.11 beacon 数据包

beacon 是你能找到的最有信息量的无线数据包之一。它作为一个广播数据包由 WAP 发送，穿过无线信道通知所有无线客户端存在这个可用的

WAP，并定义了连接它必须设置的一些参数。在我们的示例文件中，你可以看到这个数据包在 802.11 头部的 Type/Subtype 域被定义为 beacon❶。

在 802.11 管理帧头部发现了其他信息，包括以下几点。

Timestamp：发送数据包的时间戳。

Beacon Interval：beacon 数据包重传间隔。

Capability Information：WAP 的硬件容量信息。

SSID Parameter Set：WAP 广播的 SSID（网络名称）。

Supported Rates：WAP 支持的数据传输率。

DS Parameter：WAP 广播使用的信道。

这个头部也包含了来源和目的地址以及厂商信息。

在这些知识的基础上，我们可以了解到示例文件中发送 beacon 的 WAP 的很多信息。显然这是一台 D-Link 设备 ❷，使用 802.11b 标准（B）❸，在信道 11 上工作 ❹。

虽然 802.11 管理数据包的具体内容和用途不一样，但总体结构跟这个例子相差不大。