5.1 端点和网络会话

要想让网络通信正常进行，你必须至少拥有两台设备进行数据流的交互。端点（endpoint）就是指网络上能够发送或者接收数据的一台设备。两个端点之间的通信被称之为会话（conversation）。Wireshark 根据交互的特性来标识端点会话，特别是在多种协议之间所使用的地址。

端点在 OSI 的不同层级上使用多种不同类型的地址。例如在数据链路层，通信使用物理网卡的 MAC 地址。每个设备的 MAC 地址独一无二（虽然也有办法修改，但这可能会削弱它的唯一性）。然而在网络层，端点使用 IP 地址。IP 地址可以在任何时间修改。我们将在接下来的章节里讨论这些地址类型是怎么使用的。

图 5-1 展示了地址是如何标识端点的两个例子。图中会话 A 阐释了数据链路（MAC）层的两个端点之间的通信。端点 A 的 MAC 地址是 00:ff:ac:ce:0b:de，端点 B 的 MAC 地址是 00:ff:ac:e0:dc:0f。会话 B 阐释了工作在网络（IP）层的两个设备之间的通信。端点 A 的 IP 地址是 192.168.1.25。端点 B 的 IP 地址是 192.168.1.30。

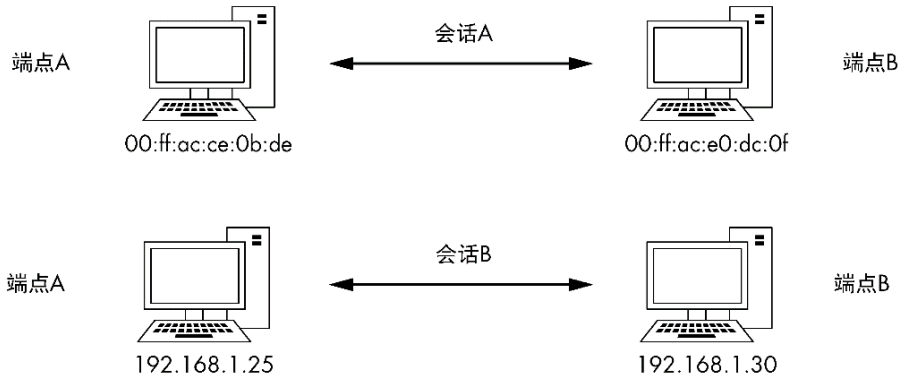

图 5-1　网络上的端点和会话

现在让我们来看一看 Wireshark 如何在端点层面或会话层面上提供网络通信的相关信息。