2.3 在交换式网络中进行嗅探

正如第 1 章中所讨论的，交换机是现在网络环境中一种常见的连接设
类型。它们为通过广播、单播与组播方式传输数据提供了高效的方法。另
外，一些交换机还允许全双工通信，也就是说，设备可以同时发送和接收
据。

而这对数据包分析师来说是不幸的，交换机给数据包嗅探带来了一些
杂因素。当将嗅探器连接到交换机上的一个端口时，你将只能看到广播数
包，及由你自己电脑传输与接收的数据包，如图 2-4 所示。

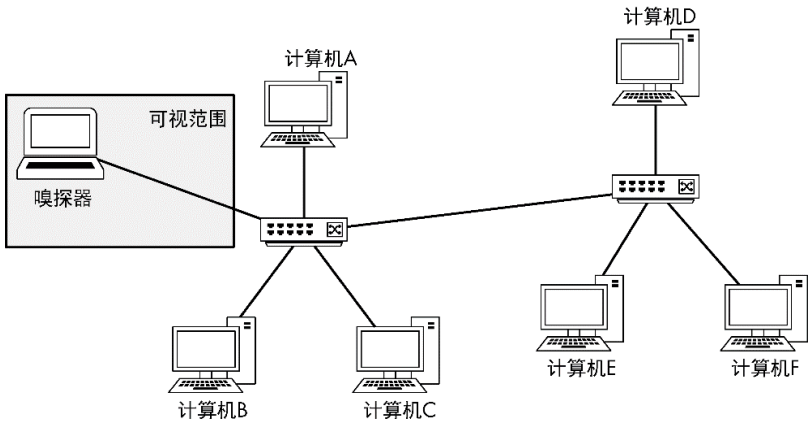

图 2-4 交换式网络上的可视范围仅限于你所接入的端口

在一个交换式网络中从一个目标设备捕获网络流量的基本方法有如下
种：端口镜像、集线器接出（hubbing out）、使用网络分流器和 ARP 缓
污染攻击。