第 2 章　监听网络线路

进行高效的数据包分析的一个关键决策是在哪里放置数据包嗅探器，恰当地捕捉网络数据。数据包分析师通常把这个过程称为监听网络线路。而言之，这是将数据包嗅探器安置在网络上恰当物理位置的过程。

然而不幸的是，嗅探数据包并不像是将一台笔记本电脑连入网络那么单。事实上，有些时候，在网络布线系统上放置一个数据包嗅探器，要比实际分析数据包更难一些。

安置嗅探器的挑战是要考虑到种类繁多的用来连接网络的硬件设备。2-1 显示了一种典型的情况。由于网络上主要的 3 种设备（集线器、交换机、路由器）对网络流量的处理方式都不相同，因此你必须非常清楚你所析网络使用的是哪些硬件设备。

本章的目标是帮助你理解如何在各种不同网络拓扑结构中安置数据包探器。首先，让我们来看一看，我们实际上是如何捕获网络线路上所有传的数据包的。

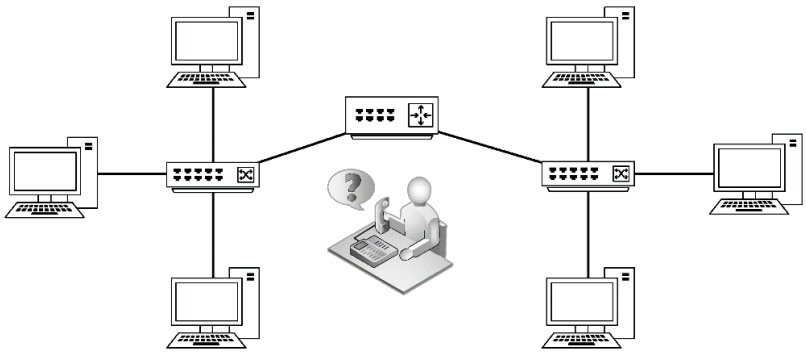

图 2-1　将嗅探器安置在你的网络上，有时是你面对的最大挑战