2.4 在路由网络环境中进行嗅探

所有在交换式网络中用来监听网络线路的技术在路由网络环境中都同
适用。面对路由网络环境时，唯一需要重点考虑的问题是，当你调试一个
及多个网络分段的故障时，如何安装你的嗅探器？正如你所学到的，一个
备的广播域一直延伸，直到到达一个路由器，在这个点上，网络流量将会
转发给上游路由器。

在网络数据必须经过多个路由器的情况下，在各个路由器上分析网络
量是非常重要的。举例来说，考虑你很可能会遇到的一个场景，在网络中
几个路由器将几个网络分段连接在一起。在这个网络中，每个网段与上游
段进行通信，来获取和存储数据。

如图 2-14 所示，我们要解决的一个故障问题：一个下游子网 D，无
与网络 A 中的任何设备进行通信。

如果在存在故障问题的网络 D 中嗅探流量，你可以清楚地看到数据包
传输到了其他网段，但你可能看不到回来的数据包所说的「一会儿回来」。
如果你重新考虑你的嗅探器部署位置，在网络 D 的直接上游网段（网络 B
中开始嗅探，那么你将会有一个关于故障更清晰的视图。

此时，你可能会发现，来自网络 D 的流量被丢弃了，或是被网络 B 的
路由器错误地路由了。

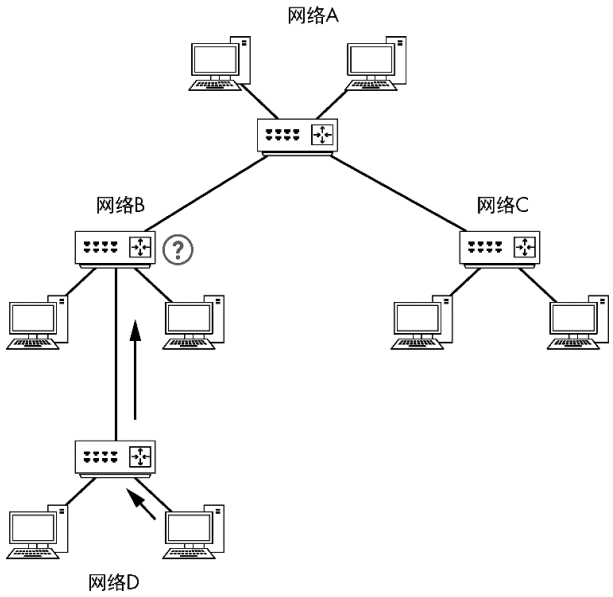

图 2-14　网络 D 中的计算机不能与网络 A 中的计算机进行通信

最终，这会导致路由器配置问题，如果得到纠正，那么便会解决掉你大麻烦。虽然这个场景有点宽泛，但其中的精髓是，在处理涉及多个网段路由器的问题时，可能需要将你的嗅探器移动到不同的位置上，才能获得个完整的网络画面。

这是一个很好的例子，它说明了为什么往往需要在不同的网段中对多设备流量进行嗅探，才能很快地诊断出故障的根本原因。

「网络地图」

在关于网络布局的讨论中，我们已经研究了好几种不同的「网络地图」。「网络地图」，或称网络拓扑图，是一个显示了网络中所有技术资源以及它们之间连接关系的图形表示。

在决定你的数据包嗅探器安置位置时，没有比拿着一张「网络地图」来进行分析更好的办法了。如果你有一张「网络地图」，请把它保留在手边，它在故障排除和分析过程中，都会是一份贵的资产。建议对你自己的网络画出一份详细的「网络地图」。请记住在大多数时候，排除故障半以上的工作，都集中在收集正确的网络数据上。