## 2.3.1 端口镜像

端口镜像也许是在交换式网络中捕获一个目标设备所有网络通信最简的方法了。为了使用端口镜像，你必须能够通过命令行或 Web 管理界面访问目标设备所连接的交换机。此外，这个交换机还必须支持端口镜像的能，并且有一个空闲的端口，让你可以插入你的嗅探器。

要启用端口镜像，你需要发出一个命令，来强制交换机将一个端口上所有通信都镜像到另一端口上。例如，为了捕获交换机 3 号端口连接的一设备发出的所有流量，你只需要简单地将你的嗅探分析器接入 4 号端口，后将 3 号端口镜像复制到 4 号端口，这就可以让你看到目标设备所传输与收的所有网络流量了。图 2-5 显示了端口镜像的原理。

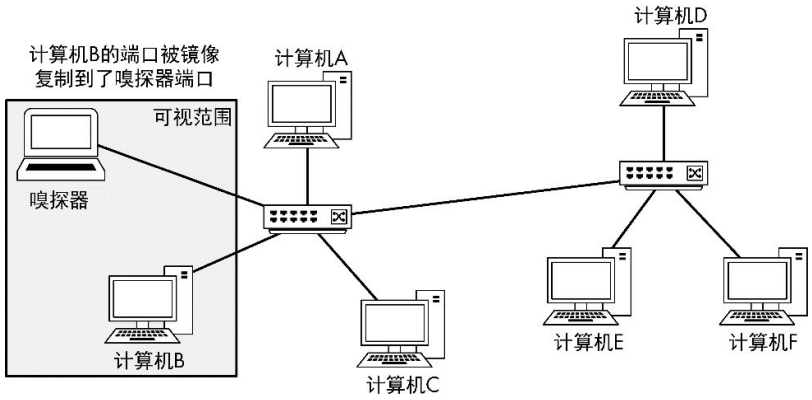


图 2-5　端口镜像可以让你在交换式网络上扩大可视范围

设置端口镜像的具体方法取决于不同的交换机制造商。对于大多数的换机，你需要登录到命令行界面，然后输入端口镜像命令。你可以在表 2中找到一些通用的端口镜像命令。

**表 2-1 用于启用端口镜像的命令**

| 制造商 | 命令 |
| --- | --- |
| 思科 | set span <source port> <destination port> |

| 造商 | |
|---|---|
| 凯创 | set port mirroring create <source port> <destination port> |
| 北电 | port-mirroring mode mirror-port <source port> monitor-port <destination port> |

注意

某些交换机提供基于 Web 的图形用户管理界面，并提供端口镜像作为一个选项，但这种配方式不像命令行那么普遍和标准。但是，如果你的交换机提供了一种图形化界面，可以高效配置端口镜像的方法，那么你也可以使用。除此之外，越来越多的小型办公和家庭办公（SOHO）交换机开始提供端口镜像功能，并且这些功能通常可以在图形化界面里设置。

在进行端口镜像时，需要留意被镜像端口的流量负载。有些交换机厂允许你将多个端口的流量镜像到一个单独端口上，这在分析一个交换机上个或多个设备的网络通信时，可能是非常有用的。然而，这是我们使用一简单的算术来考虑会发生什么事情。比如你有一个 24 端口交换机，你将个全双工的 100Mbit/s 端口流量都镜像到一个端口上，那么在这个端口上能会有 4600Mbit/s 的流量。由于这将会远远超出一个单独端口的物理承能力，因此在网络流量达到一定级别后，将可能会导致数据包丢失，甚至络速度变慢。在这种情况下，交换机会丢弃所有多余的数据包，或者甚至「暂停」内部交换电路，从而造成通信中断的情况。当你开始执行你的数包捕获时，请务必小心，不要让这种情况在你的网络中发生。

在企业网络或有持续网络流量安全监控需求的场景里，端口镜像功能起来是一个吸引人的、低成本的解决方案。但是，该方案对于一些应用并不靠谱。特别是在高吞吐量级别的环境下，端口镜像可能会产生不稳定结果，并且造成无法追踪的数据丢失。对于这种情况，我建议你使用分流器，详见 2.3.3 小节。