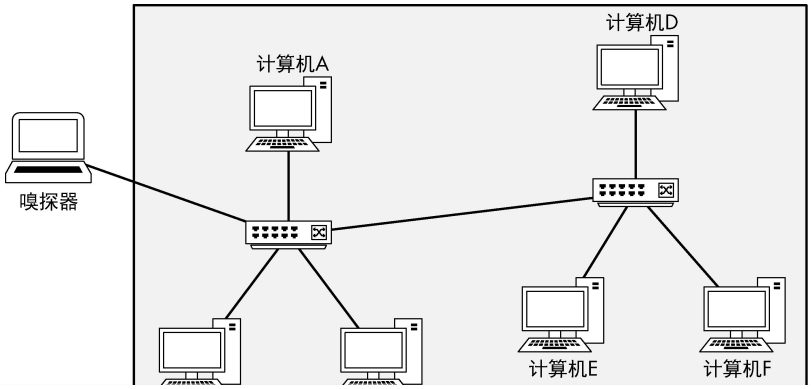
## 2.2 在集线器连接网络中嗅探

在使用集线器连接的网络中进行嗅探，对于任何数据包分析师来说，是一个梦想。正如你在第 1 章中了解到的那样，流经集线器的所有网络数包都会被发送到每一个集线器连接的端口。因此，要想分析一台连接到集器上的计算机的网络通信，你所需要做的所有事情就是将数据包嗅探器连到集线器的任意一个空闲端口上。这样你就能看到所有从那台计算机流入出的网络通信，以及其他接入集线器的所有计算机之间的通信。

如图 2-2 所示，当你的嗅探器连接到一个集线器网络时，你对本地网的可视范围是不受限制的。

> 注意
>
> 可视范围，这个术语将在整本书的很多图示中显示，表示你在数据包嗅探器中能够看到通信流量的主机范围。

然而对我们来说不幸的消息是，集线器网络已经是非常罕见的了，因它们曾经给网络管理员们带来了很大的困扰，而且已经被基本淘汰了。因在集线器网络中，在任意时刻里，只有一个设备可以通信。因此，通过集线器连接的设备必须与其他设备进行竞争，才能取得带宽来进行通信，当个或多个设备同时通信时，数据包就会产生冲突碰撞，如图 2-3 所示。结可能是丢包，然后通信设备需要承受重新传输数据包所带来的性能损失，这又增加了网络拥塞和碰撞。当通信流量水平和碰撞概率增加时，设备需传输每个数据包 3 次甚至 4 次，这大大降低了网络性能。因此很容易理解什么现在各种规模的网络都已经转而使用交换机了。虽然在现代网络中你难再碰到集线器了，但在一些支持老旧或特殊设备的网络里，比如工业控系统（ICS）网络中，你仍有可能遇到它们。



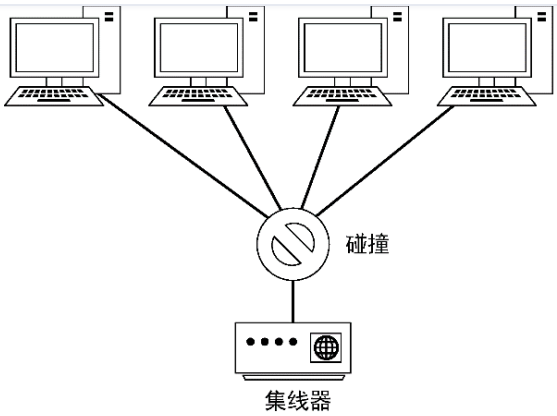




图 2-3　当集线器网络上两个设备在同一时间通信时产生的碰撞

要辨别一个网络中是否有集线器，一个简单的方法就是去机房观察网
机柜。当你认不出来的时候，只需在服务器机框最黑暗的角落寻找网络硬
件，并且上面有一些积灰。