1.2.5 网络硬件

现在是时候来看一看网络硬件了，至此脏活累活都已经完成，接下来内容都很简单了。我们将专注于几个较为常见的网络硬件：集线器、交换和路由器。

1．集线器

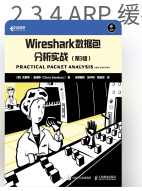
集线器一般是提供了多个 RJ-45 端口的机盒，图 1-4 所示为一个 NETGEAR 集线器。集线器从非常小的 4 端口的设备，到企业环境中安装架设计的 48 端口机盒设备，变化很大。

图 1-4　一个典型的 4 端口以太网集线器

因为集线器产生很多不必要的网络流量，并仅在半双工模式下运行（能在同一时间发送和接收数据），所以你通常不会在现代或高密度的网络中再看到它们的身影了（用交换机来代替）。然而，你应该知道集线器的工作机制，因为它们对于数据包分析技术非常重要，特别是在实施我们将于第章介绍的「枢纽」技术时。

一个集线器无非就是工作在 OSI 参考模型物理层上的转发设备。它从个端口接收到数据包，然后将数据包传输（中继）到设备的每个端口上。例如，如果一台计算机连接到一个 4 端口集线器的 1 号端口上，需要发送据到连接在 2 号端口的计算机，那么集线器将会把数据发送给端口 2、3、4。连接到 3 号端口与 4 号端口上的客户端计算机通过检查以太网帧头字段中的目标媒体访问控制（MAC）地址，判断出这些数据包并不是给它们的便丢弃这些数据包。

图 1-5 是一个从计算机 A 发送数据到计算机 B 的例子，当计算机 A 发出数据时，所有连接到集线器的计算机都将接收到数据，但只有计算机 B 实际将数据接收下来，而其他计算机则将丢弃它。



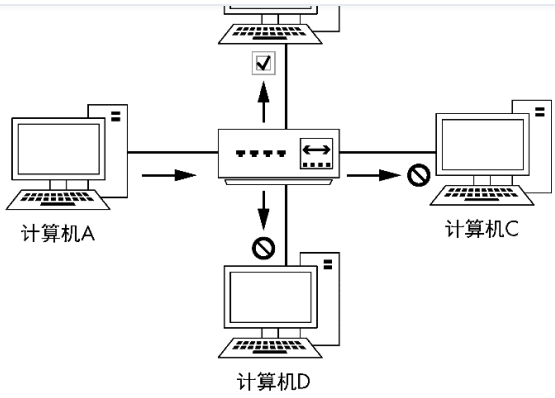


图 1-5　计算机 A 通过集线器传输数据到计算机 B 的通信流

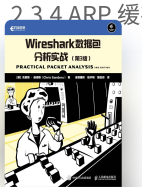
作一个比喻，假设你发送一封主题为「所有的营销人员请注意」的电邮件给贵公司所有雇员，而不是只有那些在营销部门工作的人。市场营销门的员工会知道这封邮件是给他们的，他们很可能会打开它；而其他员工到这封邮件并不是给他们的，则很可能会选择丢弃。可以看出这会导致很不必要的通信和时间浪费，然而这正是集线器的工作原理。在高密度的实网络中，集线器最好的替代产品是交换机，它们是支持全双工的设备，可同步地发送和接收数据。

2．交换机

与集线器相同，交换机也是用来转发数据包的。但与集线器不同的是交换机并不是将数据广播到每一个端口，而是将数据发送到目的计算机所接的端口上。如同你在如图 1-6 中看到的那样，交换机的外表与集线器十相似。

市场上几个大牌公司的交换机，比如思科品牌的交换机，能够通过专化的供应商特定软件或 Web 接口进行远程管理。这些交换机通常被称为管理型交换机。管理型交换机提供了多种在网络管理中非常有用的功能特性包括启用或禁用特定端口、查看端口细节参数、远程修改配置、远程重启等。

图 1-6　一个机架式 48 端口以太网交换机



交换机将每个连接设备的 2 层地址都存储在一个 CAM（Content Addressable Memory：内容寻址寄存器）表中，CAM 表充当着一种类似交通警察的角色。当一个数据包被传输时，交换机读取数据包中的第 2 层议头部信息，并使用 CAM 表作为参考，决定往哪个或哪些端口发送数据交换机仅仅将数据包发送到特定端口上，从而大大降低了网络流量。

图 1-7 说明了流量经过交换机进行传输的过程。在这个图示中，计算 A 发送数据到唯一的目标：计算机 B，虽然同一时间里网络上可能有很多话，但信息将会直接通过交换机和目标接收者进行传输，而不会被传递到换机和所有连接计算机之间。

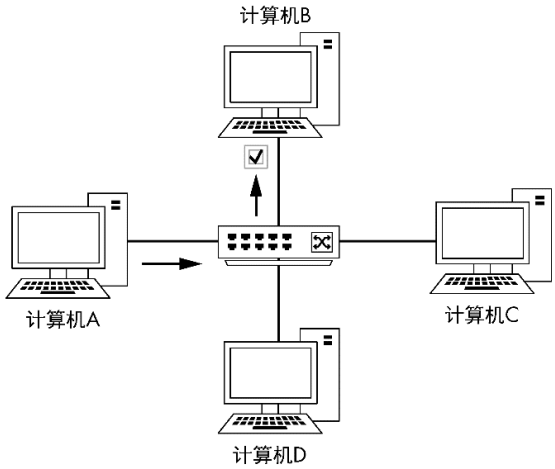


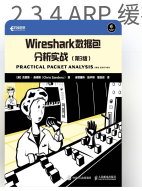
图 1-7　当计算机 A 通过交换机传输数据到计算机 B 时的通信流图示

3．路由器

路由器是一种比交换机或集线器具有更高层次功能的先进网络设备。个路由器可以有许多种不同的形状和外形，但大多数路由器在正前方的面上会有几个 LED 指示灯，在背板上会有一些网络端口，个数则取决于网络的大小。图 1-8 显示了一款路由器的外形。

图 1-8　一款低端的 Enterasys 路由器，适合在一个中小型网络使用

路由器工作在 OSI 参考模型的第 3 层，它们负责在两个或多个网络之



为了更清楚地解释路由的概念，我们以一个拥有几条街道的街区进行比。假设有一些房子，它们都有着自己的地址，就像网络上的计算机一样而每条街道就如同网段，如图 1-9 所示。从你所在街道上的某个房子，你以很容易地与同一街道中居住的邻居进行沟通交流，这类似于交换机的操作，能够允许在同一网段中的所有计算机进行相互通信。

然而，与其他街道上居住的邻居进行沟通交流，就像是与不同网段中计算机进行通信。参照图 1-9，假设你住在藤街 503 号，需要到山茱萸巷 202 号。如果想要过去，你必须先到橡树街，然后再到山茱萸巷。现在请应到跨越网段的场景中，如果在 192.168.0.3 地址的设备需要和 192.168.0.54 地址的设备进行通信，它必须经由路由器到 10.100.1.1 网络上，然后再经过连接目的网段的路由器，才可以到达目标网段。

网络上的路由器的数量与大小通常取决于网络的规模与功能。个人和庭办公网络可能只需要一个放置在网络中心的小型路由器。而大型企业网则可能有几个路由器分布在不同的部门，它们都连接到一个大型的中央路器或三层交换机上（具有内置功能，可以充当一台路由器的先进型交换机

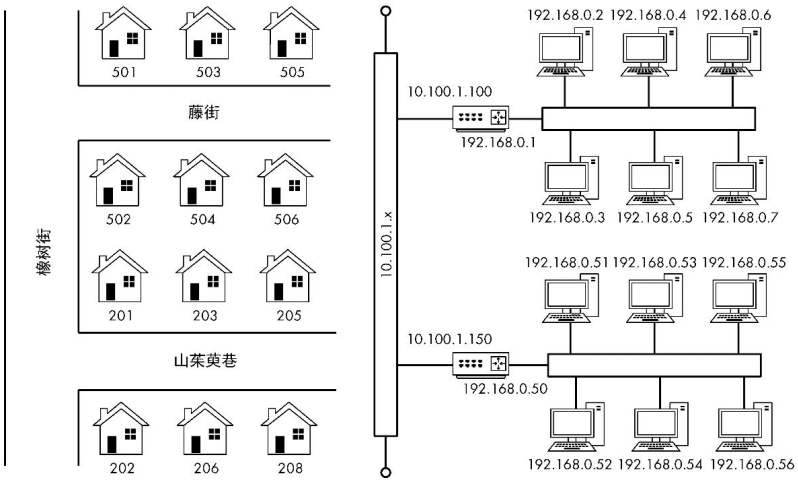
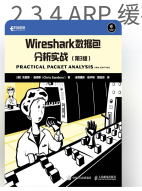


图 1-9　一个路由网络与街区的类比

当你开始查看越来越多的网络图时，就会更加了解网络数据流是如何经这些不同类型的网络设备节点的，图 1-10 显示了路由网络中的一个很常见的布局形式。在这个例子中，两个单独的网络通过一个路由器进行连接如果网络 A 上的计算机希望与网络 B 上计算机进行通信，则传输数据将必通过路由器。



Wireshark 数据包分析实战（第 3 版）
作者：[美]克里斯·桑德斯（Chris Sander…

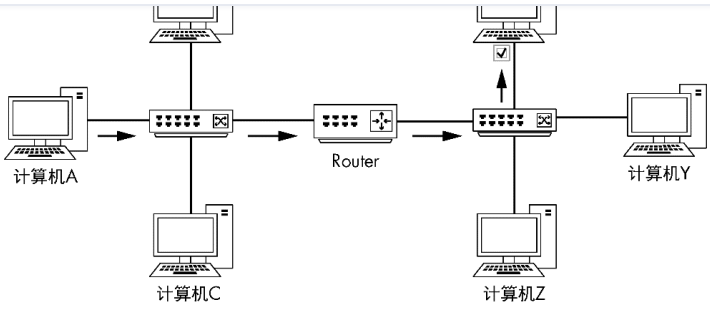


图 1-10　计算机 A 通过路由器将数据传送到计算机 X 的通信流图示