机减小其发送速率。我们在第 3 章已看到，TCP 有自己在运输层操作的拥塞控制机制，不需要利用网络层中的反馈信息（如 ICMP 源抑制报文）。

在第 1 章中我们介绍了 Traceroute 程序，该程序允许我们跟踪从一台主机到世界上任意一台其他主机之间的路由。有趣的是 Traceroute 是用 ICMP 报文来实现的。为了判断源和目的地之间所有路由器的名字和地址，源主机中的 Traceroute 向目的主机发送一系列普通的 IP 数据报。这些数据报的每个携带了具有一个不可达 UDP 端口号的 UDP 报文段。第一个数据报的TTL为 1，第二个的TTL为 2，第三个的TTL为 3，依次类推。该源主机也为每个数据报启动定时器。当第 n 个数据报到达第 n 台路由器时，第 n 台路由器观察到这个数据报的TTL正好过期。根据 IP 协议规则，路由器丢弃该数据报并发送一个 ICMP 告警报文给源主机（类型 11 编码 0）。该告警报文包含了路由器的名字与它的 IP 地址。当该 ICMP 报文返回源主机时，源主机从定时器得到往返时延，从 ICMP 报文中得到第 n 台路由器的名字与 IP 地址。

Traceroute 源主机是怎样知道何时停止发送 UDP 报文段的呢？前面讲过源主机为它发送的每个报文段的TTL字段加 1。因此，这些数据报之一将最终沿着这条路到达目的主机。因为该数据报包含了一个具有不可达端口号的 UDP 报文端，该目的主机将向源发送一个端口不可达的 ICMP 报文。当源主机收到这个特别的 ICMP 报文时，知道它不需要再发送另外的探测分组。（标准的 Traceroute 程序实际上用相同的TTL发送 3 个一组的分组；因此 Traceroute 输出对每个TTL提供了 3 个结果。）

以这种方式，源主机知道了位于它与目的主机之间的路由器数量和标识，以及两台主机之间的往返时延。注意 Traceroute 客户程序必须能够指令操作系统产生具有特定TTL值的 UDP 数据报，当 ICMP 报文到达时，也必须能够由它的操作系统进行通知。既然你已明白了 Traceroute 的工作原理，你也许想回去更多地使用它。

关注安全性

检查数据报：防火墙和入侵检测系统

假定你被赋予了管理家庭网络、部门网络、大学网络或公司网络的任务。知道你网络 IP 地址范围的攻击者，能够方便地在此范围中发送 IP 数据报进行寻址。这些数据报能够做各种不正当的事情，包括用 ping 搜索和端口扫描形成你的网络图，用恶意分组使易受攻击的主机崩溃，用纷至沓来的 ICMP 分组洪泛服务器，并且通过在分组中带有恶意软件感染主机。作为网络管理员，你准备做些什么来将这些能够在你的网络中发送恶意分组的坏家伙拒之门外呢？对抗恶意分组攻击的两种流行的防御措施是防火墙和入侵检测系统（IDS）。

作为一名网络管理员，你可能首先尝试在你的网络和因特网之间安装一台防火墙。（今天大多数接入路由器具有防火墙能力。）防火墙检查数据报和报文段首部字段，拒绝可疑的数据报进入内部网络。例如，一台防火墙可以被配置为阻挡所有的 ICMP 回显请求分组，从而防止了攻击者横跨你的 IP 地址范围进行传统的 ping 搜索。防火墙也能基于源和目的 IP 地址和端口号阻挡分组。此外，防火墙能够配置为跟踪 TCP 连接，仅许可属于批准连接的数据报进入。