因特网将忠实地将该分组转发到目的地。想象某接收到这样一个分组的不可信的接收方（比如说一台因特网路由器），将该（虚假的）源地址作为真实的，进而执行某些嵌入在该分组内容中的命令（比如说修改它的转发表）。将具有虚假源地址的分组注入因特网的能力被称为 **IP 哄骗**（IP spoofing），而它只是一个用户能够冒充另一个用户的许多方式中的一种。

为了解决这个问题，我们需要采用*端点鉴别*，即一种使我们能够确信一个报文源自我们认为它应当来自的地方的机制。当你继续学习本书各章时，再次建议你思考怎样为网络应用程序和协议做这件事。我们将在第 8 章研究端点鉴别机制。

在本节结束时，值得思考一下因特网是如何从一开始就落入这样一种不安全的境地的。大体上讲，答案是：因特网最初就是基于“一群相互信任的用户连接到一个透明的网络上”这样的模型［Blumenthal 2001］进行设计的，在这样的模型中，安全性没有必要。初始的因特网体系结构的许多方面都深刻地反映了这种相互信任的观念。例如，一个用户向任何其他用户发送分组的能力是默认的，而不是一种请求/准予的能力，还有用户身份取自所宣称的表面价值，而不是默认地需要鉴别。

但是今天的因特网无疑并不涉及“相互信任的用户”。无论如何，今天的用户并不是必须相互信任的，他们仍然需要通信，也许希望匿名通信，也许间接地通过第三方通信（例如我们将在第 2 章中学习的 Web 高速缓存，我们将在第 6 章学习的移动性协助代理），也许不信任他们通信时使用的硬件、软件甚至空气。随着我们进一步学习本书，会面临许多安全性相关的挑战：我们应当寻求对嗅探、端点假冒、中间人攻击、DDoS 攻击、恶意软件等的防护办法。我们应当记住：在相互信任的用户之间的通信是一种例外而不是规则。欢迎您到现代计算机网络世界来！

1.7 计算机网络和因特网的历史

1.1 节到 1.6 节概述了计算机网络和因特网的技术。你现在应当有足够的知识来给家人和朋友留下深刻印象了。然而，如果你真的想在下次鸡尾酒会上一鸣惊人，你应当在你的演讲中点缀上一些有关因特网引人入胜的历史轶闻［Segaller 1998］。

1.7.1 分组交换的发展：1961～1972

计算机网络和今天因特网领域的开端可以回溯到 20 世纪 60 年代的早期，那时电话网是世界上占统治地位的通信网络。1.3 节讲过，电话网使用电路交换将信息从发送方传输到接收方，这种适当的选择使得语音以一种恒定的速率在发送方和接收方之间传输。随着 20 世纪 60 年代早期计算机的重要性越来越大，以及分时计算机的出现，考虑如何将计算机连接在一起，并使它们能够被地理上分布的用户所共享的问题，也许就成了一件自然的事。这些用户所产生的流量很可能具有“*突发性*”，即活动的间断性，例如向远程计算机发送一个命令，接着由于在等待应答或在对接收到的响应进行思考而有静止的时间段。

全世界有 3 个研究组首先发明了分组交换，以作为电路交换的一种有效的、健壮的替代技术。这 3 个研究组互不知道其他人的工作［Leiner 1998］。有关分组交换技术的首次公开发表出自 Leonard Kleinrock［Kleinrock 1961，Kleinrock 1964］，那时他是麻省理工学