关注安全性

TCP 安全

无论 TCP 还是 UDP 都没有提供任何加密机制，这就是说发送进程传进其套接字的数据，与经网络传送到目的进程的数据相同。因此，举例来说如果某发送进程以明文方式（即没有加密）发送了一个口令进入它的套接字，该明文口令将经过发送方与接收方之间的所有链路传送，这就可能在任何中间链路被嗅探和发现。因为隐私和其他安全问题对许多应用而言已经成为至关重要的问题，所以因特网界已经研制了 TCP 的加强版本，称为**安全套接字层**（Secure Sockets Layer，SSL）。用 SSL 加强后的 TCP 不仅能够做传统的 TCP 所能做的一切，而且提供了关键的进程到进程的安全性服务，包括加密、数据完整性和端点鉴别。我们强调 SSL 不是与 TCP 和 UDP 在相同层次上的第三种因特网运输协议，而是一种对 TCP 的加强，这种强化是在应用层上实现的。特别是，如果一个应用程序要使用 SSL 的服务，它需要在该应用程序的客户端和服务器端包括 SSL 代码（利用现有的、高度优化的库和类）。SSL 有它自己的套接字 API，这类似于传统的 TCP 套接字 API。当一个应用使用 SSL 时，发送进程向 SSL 套接字传递明文数据；在发送主机中的 SSL 则加密该数据并将加密的数据传递给 TCP 套接字。加密的数据经因特网传送到接收进程中的 TCP 套接字。该接收套接字将加密数据传递给 SSL，由其进行解密。最后，SSL 通过它的 SSL 套接字将明文数据传递给接收进程。我们将在第 8 章中更为详细地讨论 SSL。

2. UDP 服务

UDP 是一种不提供不必要服务的轻量级运输协议，它仅提供最小服务。UDP 是无连接的，因此在两个进程通信前没有握手过程。UDP 协议提供一种不可靠数据传送服务，也就是说，当进程将一个报文发送进 UDP 套接字时，UDP 协议并不保证该报文将到达接收进程。不仅如此，到达接收进程的报文也可能是乱序到达的。

UDP 没有包括拥塞控制机制，所以 UDP 的发送端可以用它选定的任何速率向其下层（网络层）注入数据。（然而，值得注意的是实际端到端吞吐量可能小于这种速率，这可能是因为中间链路的带宽受限或因为拥塞而造成的。）

3. 因特网运输协议所不提供的服务

我们已经从 4 个方面组织了运输协议服务：可靠数据传输、吞吐量、定时和安全性。TCP 和 UDP 提供了这些服务中的哪些呢？我们已经注意到 TCP 提供了可靠的端到端数据传送。并且我们也知道 TCP 在应用层可以很容易地用 SSL 来加强以提供安全服务。但在我们对 TCP 和 UDP 的简要描述中，明显地缺少了对吞吐量或定时保证的讨论，即这些服务目前的因特网运输协议并没有提供。这是否意味着诸如因特网电话这样的时间敏感应用不能运行在今天的因特网上呢？答案显然是否定的，因为在因特网上运行时间敏感应用已经有多年了。这些应用经常工作得相当好，因为它们已经被设计成尽最大可能对付这种保证的缺乏。我们将在第 7 章中研究几种设计技巧。无论如何，在时延过大或端到端吞吐量受限时，好的设计也是有限制的。总之，今天的因特网通常能够为时间敏感应用提供满意的服务，但它不能提供任何定时或带宽保证。