每一层，一个分组具有两种类型的字段：首部字段和**有效载荷字段**（payload field）。有效载荷通常是来自上一层的分组。

这里一个有用的类比是经过公共邮政服务在某公司分支办公室之间发送一封备忘录。假定位于一个分支办公室的 Alice 要向位于另一个分支办公室的 Bob 发送一封备忘录。该备忘录类比于应用层报文。Alice 将备忘录放入办公室之间的公函信封中，并在公函信封上方写上了 Bob 的名字和部门编号。该办公室之间的公函信封类比于运输层报文段，即它包括了首部信息（Bob 的名字和部门编码）并封装了应用层报文（备忘录）。当发送方分支办公室的收发室拿到该办公室之间的备忘录，将其放入适合在公共邮政服务发送的信封中，并在邮政信封上写上发送和接收分支办公室的邮政地址。此处，邮政信封类比于数据报，它封装了运输层的报文段（办公室之间信封），该报文段封装了初始报文（备忘录）。邮政服务将该邮政信封交付给接收方分支办公室的收发室。在此处开始了拆封过程。该收发室抽取了办公室间的备忘录并转发给 Bob。最后，Bob 打开封套并拿走了备忘录。

封装的过程能够比前面描述的更为复杂。例如，一个大报文可能被划分为多个运输层的报文段（这些报文段每个可能被划分为多个网络层数据报）。在接收端，则必须从其连续的数据报中重构这样一个报文段。

## 1.6 面对攻击的网络

对于今天的许多机构（包括大大小小的公司、大学和政府机关）而言，因特网已经成为与其使命密切相关的一部分了。许多个人也依赖因特网进行许多职业、社会和个人活动。但是在所有这一切背后，存在着一个阴暗面，其中的“坏家伙”试图对我们的日常生活中进行破坏，如损坏我们与因特网相连的计算机，侵犯我们的隐私以及使我们依赖的因特网服务无法运行。

网络安全领域主要探讨以下问题：坏家伙如何攻击计算机网络，以及我们（即将成为计算机网络的专家）如何防御以免受他们的攻击，或者更好的是设计能够事先免除这样的攻击的新型体系结构。面对经常发生的各种各样的现有攻击以及新型和更具摧毁性的未来攻击的威胁，网络安全已经成为近年来计算机网络领域的中心主题。本书的特色之一是将网络安全问题放在中心位置。

因为我们在计算机网络和因特网协议方面还没有专业知识，所以这里我们将开始审视某些今天最为流行的与安全性相关的问题。这将刺激我们的胃口，以便我们在后续章节中进行更为充实的讨论。我们在这里以提出问题开始：什么东西会出现问题？计算机网络是怎样易于受到攻击的？今天某些最为流行的攻击类型是什么？

### 1. 坏家伙能够经因特网将有害程序放入你的计算机中

因为我们要从/向因特网接收/发送数据，所以我们将设备与因特网相连。这包括各种好东西，例如 Web 页面、电子邮件报文、MP3、电话、视频实况、搜索引擎结果等。但是，不幸的是伴随好的东西而来的还有恶意的东西（这些恶意的东西可统称为**恶意软件**（malware）），它们能够进入并影响我们的设备。一旦恶意软件感染我们的设备，就能够做各种不正当的事情，包括删除我们的文件，安装间谍软件来收集我们的隐私信息，如社会保险号、口令和击键，然后将这些（当然经因特网）发送给坏家伙。我们的受害主机也可能成为数以千计的类似受害设备网络中的一员，它们被统称为**僵尸网络**（botnet），坏家伙