JI SUAN JI AN QUAN YONG HU ZHI NAN

计算机安全用户指南

主 编 宣 力 罗忠海 罗忠雁

电子科技大学出版社

内 容 提 要

本书主要讨论了网络安全的理论基础，研究了网络安全的原理及其实现方法，同时深入研究了分组过滤型防火墙核心的实现，及介绍了实际计算机网络系统安全的操作和实践。

本书内容安排由浅入深，由大及细，由理论到实践，非常适合学习网络安全的初学者。

图书在版编目（CIP）数据

计算机安全用户指南 / 宣力，罗忠海，罗忠雁主编.
成都：电子科技大学出版社，2000.6
ISBN 7-81065-421-7

Ⅰ.计… Ⅱ.①宣…②罗…③罗… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2000)第 24907 号

计算机安全用户指南

主 编 宣 力 罗忠海 罗忠雁

出 版：电子科技大学出版社 （成都建设北路二段四号 邮政编码：610054）
责任编辑：谢应成
发 行：新华书店经销
印 刷：四川导向印务有限公司
开 本：787×1092 1/16 印张 17.5 字数 400 千字
版 次：2000 年 6 月第一版
印 次：2000 年 6 月第一次印刷
书 号：ISBN 7—81065—421—7/TP・281
印 数：1—3000 册
定 价：21.00 元

前　言

随着 Internet 与 Intranet 的普及和广泛应用，网络安全问题越来越得到广泛的重视。本书以我国特殊的国情为背景，讲述了 Internet 安全和防火墙的基本原理，并试图设计一种较为简单的防火墙类型。

本书首先对计算机网络安全体系结构中的各要素与组成部分，包括安全性、安全威胁因素、安全服务与安全机制等作了探讨，接着分析了 TCP/IP 协议的一些细节和网络安全技术的一些关键技术，特别是作为保障内部网络安全的防火墙技术，从原理、分类、体系结构和优缺点等各方面均作了大量细致的分析，并在此基础上，介绍了如何设计分组过滤型防火墙的核心。为追踪国际先进技术，同时在分组过滤型防火墙的核心中探讨了网络地址转换（NAT）功能，使得防火墙的功能更为完善，安全性更高。本书还探讨了在实践中遇到的一些问题，如 Unix、NT 系统安全等。本书的出版无疑对一个网络安全的初学者具有较大的参考价值。

尽管国外防火墙技术已经较为成熟，但国内市场上却没有真正的国产防火墙产品，并且连参考资料都非常稀少，这使本书的写作遇到了不少困难。由于各方面的原因本书依然存在许多不足和错误，在此希望有关专家和读者能够指正。

参加本书编写的还有：张克起、杨丽、马竹天、刘玲、邓小勤、唐冰、姜海鹏、丁香荣、罗松、赵夏阳和唐寅峰等。

编　者

目 录

第一章　计算机网络概论

第一节　计算机网络的发展和现状

20 世纪末期，人类社会在经历了工业化大发展的时期以后，正进入一个以信息收集、处理和分发等为中心的信息化时代。传统的地理位置上的分割正随着信息化的发展而逐步减小，全球正越来越连成一个紧密的整体。所有这一切，都源于两个主要技术的大发展，这就是计算机技术和通信技术，而这两种技术的紧密结合则形成了计算机网络。

从概念上讲，计算机网络是指通过数据通信系统把地理上分散的自主计算机系统连接起来，以达到数据通信和资源共享的目的的一种计算机系统。所谓自主计算机，是指具有独立处理能力的计算机。计算机网络是在计算机技术和通信技术高度发展的基础上，两者相互结合的产物。一方面，通信系统为计算机之间的数据传送，提供最重要的支持；另一方面，计算机技术渗透到通信领域中，又极大地提高了通信网络的性能。

1.1　计算机网络的发展

一、远程信息处理系统

计算机技术和通信技术的密切结合，首先形成了远程信息处理系统，又称为联机系统。它是由一台主机和若干个终端，通过电话连接而成。这种系统的缺点是：

1. 通信线路利用率低
2. 主机负担过重

二、计算机通信网络

自 20 世纪 60 年代中期以来，计算机获得日益广泛的应用。在不少大型公司、事业单位和军事部门中，往往拥有若干个分散的、面向终端的计算机网络。为了将这些分散于各地的终端网连接起来，使它们彼此能进行数据交换和进行业务处理，科学家们研究的结果是形成了一个以传输信息为主要目的的计算机网络，即计算机通信网络。该网络的主要任务是在各个计算机系统之间进行通信，如在各研究机构的各个分支机构或各研究人员之间交换数据等。

三、以资源共享为主要目的的计算机网络

在人们从计算机通信网络中获得好处的同时，又对计算机网络提出了一系列新的要求，其中最重要的两条是：

1. 实现网络资源共享

使设置在一个计算机系统中的某种硬件资源和丰富的软件资源可以被联网的其它计

算机系统所共享。

60 年代末期，美国国防部高级研究计算局开发的 ARPA 网络，便是世界上第一个以资源共享为主要目标的计算机网络。该网络基于这样一种主导思想：即网络必须能够经受住故障的考验而维持正常的工作。一旦发生战争，当网络的某一部分因遭受攻击而失去工作能力时，网络的其它部分应能维持正常通信。最初，ARPA 网络主要用于军事研究，它有五大特点：

(1)支持资源共享。

(2)采用分布式控制技术。

(3)采用分组交换技术。

(4)使用通信控制处理机。

(5)采用分层的网络通信协议。

1972 年，ARPA 网络在首届计算机后台通信国际会议上首次与公众见面，立即引起轰动。由此，ARPA 成为现代计算机网络诞生的标志。

2. 负荷均衡

使计算任务较繁重的计算机系统，能把部分任务转移到任务不重的系统中去处理，以均衡各系统的负荷。

1.2 计算机网络的现状

经过 60 年代、70 年代的理论准备和研究，到 80 年代，计算机网络技术日渐成熟，特别是局域网技术，已在 80 年代走入市场，如 Novell 网络等。到 90 年代，广域网技术亦趋于成熟，使 Internet(国际互联网络)等广域网技术在全球迅速普及和使用，极大地促进了社会生产和生活的发展。

计算机网络的发展是社会化大生产的必然趋势和要求，是人类由工业化走向信息化社会的必然之路。而计算机网络的发展反过来又进一步促进了社会生产和生活的发展，这两者之间是相辅相成，共同发展的。

简单说来，当今的计算机网络主要有以下几个大类：

一、专用计算机网络

主要存在一些需要保密或重要性很强的部门。比如一些公司的实时工业控制计算机网络，我国银行、气象等部门的专用计算机网络等。这些网络只用于公司或部门内部的数据交换，不允许他人共享。

二、局域网(LAN——Local Area Network)

自 70 年代以来，由于大规模集成电路的迅速发展，使计算机硬件成本急剧下降，从而出现在一个单位甚至一栋楼中，便拥有多台微机。为实现微机之间的资源共享，可将它们连接起来而形成局域网。引入局域网的好处是：

(1) 用户之间可直接进行文件传输和交换电子函件。

(2) 能方便地共享网络中的各种硬件和软件资源，如硬盘共享、打印机共享、文件和数据共享等。用户也可以登录到具有高级处理能力的大型机或工作站上去工作，以节省硬件成本。

(3) 提高了整个系统的处理能力，可用局域网(LAN)来实现原来需要中、小型机才能实现的功能。

(4) 增加了系统的可靠性和可服务性。

(5) 增强了用户之间的相互协作，使用户之间能够更好地共同完成一定任务。

LAN 的主要特点是：

(1) 地理范围限于 100m～10km 之间；

(2) 通信介质有双绞线、同轴电缆和光纤等；

(3) 通信速率较高，可达 100M～1000Mbps，可实现电视会议等多种多样的计算机网络高级功能。

(4) 网上运行的既可能是运行 Unix 操作系统的小型机，也可以是运行 Windows 和 DOS 等操作系统的微形机，从而实现硬、软件资源的共享和数据通信。

三、广域网(WAN——Wide Area Network)

随着 LAN 技术的不断成熟，人们看到了计算机网络带给社会生产和生活的种种好处，更加远程的联网就自然而然地提上了日程。而在这一时期通信技术，尤其是光纤和无线电通信技术都得到了很大的发展，这为广域网技术的发展提供了可能。

广域网技术主要包括 X.25、ISDN(综合业务数字)以及 Internet(国际互联网络)等。它的主要特征是：

(1) 地理距离在 10km 以上。

(2) 不限于某个单位或部门所有，可以是多个单位和部门，甚至是整个世界所有。

(3) 通信信道主要为光纤和卫星。

(4) 传输时间相对较慢。

(5) 连接的主要为异种机和异种操作系统，即可以是 IBM 大型机、中、小型机，也可以是 Intel 系列的微机，甚至可以为一般的兼容机。操作系统既可以为 Unix，也可以为 DOS 和 Windows 等。

(6) 网上传输的信息多元化，既可以是文字，也可以是声音、图像等。

在我国范围内最大的几个广域网有：中国教育科研网(CERNET)，主要连接高校和研究所，提供科研和教育服务；邮电部公用计算机网（CHINANET），主要为公众提供 Internet 服务；以及整个连接中科院的网络等。

第二节 计算机网络的功能和可提供的服务

2.1 计算机网络的功能

一般而言，计算机网络主要提供以下几个方面的功能：

一、资源共享

一般计算机中的资源可分成三大类，即硬件资源、数据资源和软件资源，因此资源共享也可分为以下三类：

1. 硬件共享

为发挥巨型机和特殊外围设备的作用，满足用户要求，计算机网络应具有硬件资源共享的功能。例如，某计算机系统 A 由于没有某特殊外围设备而无法处理某些较复杂的问题时，它可将处理该问题的数据连同有关软件一起送到拥有这种特殊外围设备的系统 B 中去，由系统 B 对该数据进行处理，处理完后再把有关软件及其结果返回给计算机系统 A。

2. 数据共享

随着信息时代的到来，数据资源的重要性也越来越大。各发达国家都已经建立了成千上万个拥有各类资源的大型甚至巨型数据库，供全国乃至全世界的各类不同的用户查询。如产品供求信息数据库、人才库、气象信息库等等。事实上，现代计算机网络中是否设置了大型数据库，设置了哪些类型的大型数据库，往往是衡量一个国家计算机网络先进水平的重要标志，尤其是当今发展势头正劲的分布式数据库处理系统，它把计算机网络技术和数据库技术有机地结合起来，使用户能够方便存取几千里之外的数据，使全球越来越连成一个整体，极大地推动了信息社会的发展。我国亦建立了几百个大型的数据库，供全国人民查询使用。另外，随着 Internet(国际互联网络)在我国的广泛应用，各种各样的在线信息亦在网上发布，用户可上网查询。

计算机网络中有两种方式实现数据共享：

(1) 当计算机系统甲需要系统乙中的数据时，可将请求信息送至计算机系统乙中，由乙对请求信息进行处理，最后将请求结果通过计算机网络返回计算机系统甲中，这就是当今最为流行的客户/服务器模式（Client/Server）。这种模式的主要思想是：由客户发出请求，服务器进行处理并只将处理结果返回给客户，这样就大大节约了在网络上传输的信息量，从而大大提高了整个计算机网络的效率。

(2) 与(1)相反，当计算机系统甲需要计算机系统乙中的数据时，由乙根据甲的请求信息将整个状态下有关的数据内容送至甲，由甲自行处理。这种方式的缺点是占用网络通信量大，要求计算机系统甲应有足够的处理能力，这种方式已趋于淘汰。

3. 软件共享

计算机网络可提供共享的软件包括各种语言处理程序和各式各样的应用程序，实现软件共享的方法也有两种：

(1) 当计算机甲需要计算机乙中的软件 A 时，甲将数据 D 送至乙，由乙利用 A 对 D 进行处理后，再将结果送回甲。

(2) 计算机甲请求乙把软件 A 送至甲，由甲自己处理。

二、数据传输

该功能用于实现计算机与终端，计算机与计算机之间的数据传输，这是计算机网络最基本的功能，也是实现其它几个功能的基础。为实现数据传输，数据通信功能应包含下述几个内容：

(1) 连接的建立和拆除。

(2) 数据传输控制。

(3) 差错检测。

(4) 流量控制。

(5) 路由选择。

(6) 多路复用(即将一条物理链路虚拟为多条虚电路，使一条物理链路能为多个用户对同时提供信息传输功能。

三、负荷均衡和分布处理

(1)负荷均衡。这是指网络中的工作负荷被均匀地分配给网络中的计算机系统。当某系统的负荷过重时，网络能自动将该系统中的一部分负荷移至负荷较轻的系统中去处理。为此，网络必须具有把本地作业传送至其它计算机系统中的批处理系统，待远程计算机系统处理完后又把结果返回该系统的功能。

(2)分布处理。即将一个大型任务分散到网上的多台机器中去进行。

2.2 计算机网络提供的服务

为了方便用户，计算机网络在其基本功能的基础上，又提供了许多非常有效的服务。不论是广域网还是局域网，通常都提供下述几种网络服务：

(1)电子函件服务。

(2)文件传送服务。

(3)远程登录服务等。

一、电子函件服务 E-mail

1. 电子函件的引入

所谓电子函件是指利用通信系统传送的邮件。电子函件服务最早出现在电话系中，后来又引入到计算机网络中。引入电子函件服务可带来以下好处：

(1) 加快了邮件的传送速度。通常的邮件，即使是航空信件一般也要几天时间；而电子函件，快则几分钟，慢也只需要几小时便可被传送到千里之外的指定目标。

(2) 提供了非实时业务。打电话虽快，但电话是一种实时业务，它要求通话双方必须同时在电话机旁。据国外统计，大约有 70%的业务电话，其第一次呼叫是失败的。然而电子函件是一种非实时业务，当用户甲要把电子函件传送给用户乙时，无论乙是否在场，邮件都能自动和安全地保存在乙的信箱中。

(3) 提高了通信系统的利用率。由于电子函件属于非实时业务，因此电子函件可以利用信道的空闲时间传送。

2. 电子函件的类型。

随着电子函件服务应用领域的日益拓宽，多种多样类型的电子函件便应运而生，目前主要有三种：

(1)文字类型电子函件。这是最常见的一种电子函件形式。文字型电子函件与通常的邮件一样，也是两部分组成：即信头和信体。

(2)图像型电子函件。对于诸如照片、工程制图和手写书信等这类信息，显然不能用文字型电子函件服务来进行传送，必须利用传输数率更高的图像型电子函件服务。以前常用传真机传送图像，在高速网络出现后，便可利用高速网络来传送图像型电子函件。

(3)语音类电子函件。这是将录有声音的邮件通过网络传送到目标站。这类服务与

电话的主要区别是具有“非实时”性且可以存档。

二、文件传送协议(FTP——File Transmission Protocol)

文件传送协议 FTP 可用于将文件从一台计算机传送到另一台远程计算机上，并允许用户进行与文件传送有关的操作，比如列文件目录、传送指定文件、设置文件传送参数和改变当前工作目录等。所传送的文件可以是多种多样的，如文本文件、二进制可执行文件、语音文件和图像文件等。FTP 实际上是一个软件流通渠道，用户可利用它获得多种多样的软件。

由于文件传输和电子函件同属于用户通信，两者有些相似之处，但也有明显的区别，主要表现在：

(1) 电子函件服务是一种非时实业务，而文件传送服务是实时联机服务。在进行工作时，用户要先到目标站的计算机上登录，然后再进行文件传送。

(2) 电子函件在传送时，仅涉及到对方的电子信箱，而文件传送则往往要涉及到对方的文件系统。

(3) 电子函件服务有自身的一套特有功能，比如，将一份电子函件同时传送给多个目标站的多目标传送功能及转发功能，后者是指一用户收到电子函件后，再将该邮件转发给多个用户；而文件传送也有特有的功能，如列文件目录和实现文件共享等。

三、其它类型的服务

1. 远程登录服务(Telnet)

指某台用户计算机通过该网络服务，暂时成为另一台远程主机的仿真终端。用户要使用远程服务时，应先在指定的远程主机上进行登录，以成为该主机的合法用户。登录成功后，用户便可以在自己的仿真终端上实时使用远程主机上对外开放的全部资源，比如访问该主机数据库中的数据等。

2. 共享硬盘服务

在 LAN 中广泛提供共享硬盘服务。该服务允许连接在 LAN 上的多个工作站共享服务器上的硬盘，既将指定文件或数据部分或全部地储存在服务器的硬盘上，这样，工作站上便可不配置硬盘和软盘而形成无盘工作站；或者将另一部分可供全网用户使用的文件和数据存储在服务器的硬盘上，以便实现文件和数据共享。

3. 共享打印机服务

在 LAN 中，通常以共享硬盘为基础，又提供了共享打印机服务。该服务允许网上各工作站共享连接在服务器上的打印机，亦即当工作站需要打印数据时，可将要打印的数据送服务器，由服务器上的共享打印机进行(排队)打印。LAN 提供了该服务后，便不需要在所有的工作站上配置打印机，节省了硬件设备。

第三节 计算机网络的拓扑结构

所谓拓扑结构，是指构成计算机网络的一种连接方式，即计算机网络的硬件实体是按何种方式连成一个整体的。总的来说，计算机网络的拓扑结构可分为以下几类：

3.1 总线型网络

由一条高速公用总线连接若干个节点所形成的网络，其中一个节点是网络服务器，由它提供网络通信及资源共享服务，其它节点是网络工作站(即用户计算机)。总线型网络采用广播通信方式，即由一个节点发出的信息可被网络上的多个节点所接收。由于多个节点连接到一条公用总线上，因此必须采取某种介质访问控制规程来分配信道，以保证在一段时间内只允许一个节点传送信息。目前最常用的且已列入国际标准的规程有：

- CSMA/CD 访问控制规程；
- 总线令牌传送访问控制规程等。

总线型网络的特点为：

(1) 传输速率高。可利用高速信道来连接多个节点，其传输速率可达 1～100Mbps，1000Mbps 的快速以太网速率可达 1000Mbps。

(2) 信道利用率高。由于多个节点共用一条传输信道，故信道的利用率较低。

(3) 地理覆盖范围小。公用线的长度受到一定的限制，通常小于几千米，节点至总线的连接线也较短，故总线的地理范围一般局限于某个单位。

(4) 网络建造容易，成本低。由于网络的物理结构简单，将节点连接到总线上也容易；相应地，传输控制结构也简单，故这是一种较易实现的计算机网络。

(5) 可靠性差。一旦总线的某段出了毛病，则网络将陷入瘫痪状态。

3.2 星型网络

每一个远程节点都通过一条单独的通信线路，直接与中心点连接，即中心节点与每一个远程节点之间，都采用点到点的连接方式，中心节点是其它节点的惟一中继节点，前述的联机系统便属于星型网络。

该网络的特点是：

(1) 可靠性好。这种网络的可靠性比总线型要好得多，一旦一个从中心节点(如 HUB)到终端的线路出现故障不会影响到其它节点。

(2) 功能高度集中。整个网络的处理和控制功能高度地集中于中心节点。

(3) 响应时间与终端数目有关。当终端数目较少时，终端的请求能获得及时的响应，但随着终端数目的增多，响应时间也随之加长。

(4) 单信息流通路径。每个终端通常只有一条信息流通路径到达中心节点，反之亦然，因此不存在路径选择问题，这无疑又是影响网络可靠性的一个因素。

(5) 线路利用率低。每条线路只连接一个终端，使该线路利用不充分。

3.3. 环型网络

在环型网络中，每台入网的计算机都先连接到一个转发器上，再将所有的转发器通过高速点——点式信道，连成一个环型，网络中的信息是单向流动的，从任一源转发器所送出的信息，经环路传送一周后，又都返回到源转发器。为了控制各个联网计算机对环路的访问，在环型网络中，也同样可有多种介质访问控制规程。现已列入国际标准的规程，有如令牌环介质访问控制规程。

环型网络的特点是：

(1) 网络建造容易。由于网络中的每个转发器都只与相邻的两个转发器相连接，这使网络结构简单，且介质访问控制也不复杂，故使网络的建造比较容易。

(2) 传输时延的确定性。从某源点发出的信息，能在确定的时间内到达目标节点。基于这一特点，可构成实时性要求较高的网络，如工业控制网络等。

(3) 可靠性差。当环路上任何一个转发器或者两个转发器之间的连接发生故障时，都将导致整个网络瘫痪，因此，环型网络是不可靠的。

(4) 灵活性差。无论在增或减网络节点时，都需断开原有环路，并对介质访问进行调整。

3.4 树型网络

在实际建造一个较大型网络时，往往采用多级星型网络，将多级星型网络按层次方式排列即形成树型网络。网络的最高层是中央处理机，最低层是终端，而其它各层可以是多路转换器，集中器或部门用计算机。采用树型结构的原因可归结为：

- 使为数众多的终端能共享一条通信线路，以提高线路利用率。
- 增强网络的分布处理能力，以改善星型网络的可靠性和可扩充性。例如，可将若干个终端连接到一多路转换器上，再把若干个多路转换器连接到部门计算机上，最后再把各个部门计算机连接到企业(单位)的中央处理机上。

3.5 网状网络

其中的接口信息处理机 IMP(Interface Message Processor)专门用于实现数据通信，将多个 IMP 通过点——点式信道连接成的不规则网状网，被称为数据通信网或简称为通信子网。凡是需要入网的计算机(HOST)都应连接在 IMP 上，而各 HOST 之间必须通过通信子网方能进行通信。通常把通信子网以外的计算机和终端设备等一起称为数据处理子网或通称为资源子网。网状网络是广域网中最常采用的一种网络形式。

网状网络的特点是：

(1) 网络可靠性高。通常通信子网中的任意两个 IMP 之间，都存在着两条或两条以上的通信路径，这样，当一条通信路径发生故障时，还可以通过另一条路径把信息传送到目标 IMP。

(2) 可扩充性好。该网络无论是要增加新的功能，还是要将另一新的计算机入网，

以形成更大的或更新的计算机网络时，都很方便。

(3)灵活性好。网络可组建成各种形状、采用多种通信通道、多种传输方式及传输速率的网络。

(4)两级网络形式。网状网络在逻辑上可以分为通信子网和资源子网两部分，前者专门用于实现网络通信；后者主要用于数据处理。这种两级网络形式的最大好处是便于将各种类型的计算机连接成异构型计算机网络。

具体使用哪种网络拓扑结构，要视所在单位的具体要求和情况而定，若对实时性要求较高则宜采用环型网络；若对可靠性要求较高则宜采用星型网络、网状网络而不宜采用总线型网络；若各种要求均不高，则可以简单地采用总线型网络即可。另外还要考虑到网络建设成本、未来的扩充方式等。总之，要视具体情况综合加以考虑后决定。

第四节 计算机网络体系结构

现代计算机网络的设计是按高度结构化方式进行的。在下一节中，我们将比较详细地探讨这种结构化技术。

一、协议分层

为了减少协议设计的复杂性，大多数网络都按层或级的方式来组织，每一层都建立在它的下层之上。不同的网络，其层的数量、各层的名字、内容和功能都不尽相同。然而，在所有的网络中，每一层的目的都是向它的上一层提供一定的服务，而把如何实现这一服务的细节对上层加以屏蔽。

一台机器上的第 n 层与另一台机器上的第 n 层进行通话，通话的规则就是第 n 层协议，说明了一个 ISO/OSI(国际标准化组织/开放系统互联参考模型)7 层协议的网络。不同机器内包含相应协议层的实体称为对等进程，换言之，正是对等进程利用这些协议进行通信。

实际上，数据不是从一台机器上的第 n 层直接传送到另一台机器上的第 n 层，而是每一层都把数据和控制信息传给它的下一层，直到最下面一层。第一层之下是物理介质(Physical medium)，物理介质进行实际的通信。

每一相邻层之间有一接口，该接口定义下层向上层提供的原语操作和服务。当网络设计者决定一个网络应当包括多少层，每一层应当做什么的时候，其一个很重要的考虑就是要在相邻层间定义一个清晰的接口。为达此目的，又要求每一层完成一组特定的有明确含义的功能。除了要尽可能地减少必须在相邻层间传递的信息的数量外，一个清晰的接口可以使同一层能够轻易地用一种实现来替换另一种完全不同的实现(如用卫星信道来代替所有的电话线)，只要新的实现能向上层提供旧的实现所提供的同样一组服务就行了。

层和协议的集合叫做网络体系结构。体系结构的描述必须包含足够的信息，使实现者可以用来为每一层编写程序和进行硬件设计，并使之符合有关协议。协议实现的细节

和接口的描述都不是体系结构的内容，因为它们都隐藏在机器内部，对外部说来是不可见的。只要机器能够正确地使用全部协议，其接口完全不必相同。网络体系结构和协议并非是本书的主题和重点，只是它们都是一个需要了解的网络和安全的理论基础。

用一个比喻也许会有助于理解多层通信的实质。假如有两位国家领导人希望进行对话，一位讲英语，另一位讲德语。因为没有共同的语言，他们每人都带了一位翻译(第二层的对等进程)，每一位翻译又进一步同一位领导人保持联系(第一层的对等进程)。这样，两个领导人便可以进行对话了。

现在来考虑一个更有技术特点的例子：如何向 7 层网络的最上层提供通信。在第 7 层进行的某进程产生了信息 M，该信息按 6/7 接口的定义从第 7 层传送给第 6 层。在本例中，第 6 层以某种特定的方式转换信息(如文本压缩)，然后跨过 5/6 接口把新的信息 M 交到第 5 层。本例的第 5 层并不修改信息，只调节(信息)流的方向(也就是说，在第 6 层忙于向第 5 层递交输出信息序列时，第 5 层避免将它的输入信息传送给第 6 层)。

在很多网络中，第 4 层对所接收的信息长度没有限制，但第 3 层却存在一个限度。因此，第 4 层必须把上层来的信息分成较小的单元，每个单元先加上一个报头。报头包括控制信息，如序号，以便在下层不能保持信息顺序时，目标机器上的第 4 层能把错序的信息按原序组装好。在很多层中，报头还包括长度，时间和其它控制字段。

第 3 层决定使用哪一条输出线路，再加上自己的报头，把数据传送给第 2 层。第 2 层不仅给每段信息加上头部信息，而且还加上尾部信息，然后把合成报文传送给第 1 层进行实际传送。在收方，报文向上传送 1 层，该层的报头就被剥掉，绝不会出现把带有 N 层以下的报头的报文交给 N 层的情况。

要理解这个概念，关键是要理解虚拟通信和实际通信之间的关系，以及协议与接口之间的区别。比如，第 4 层中的对等进程，在概念上认为他们的通信是水平方向地应用第 4 层协议，每一方都好像有一个叫做“发送到另一方去”和一个叫做“从另一方接收”的过程，尽管实际是跨过 3/4 接口与下层通信而不是直接同另一方通信。

抽象出对等进程这一概念，对网络设计是至关重要的。如果没有这种抽象技术，要想把完整的网络设计这一复杂的问题，划分为几个较小的、易于处理的问题(即各层的设计)，即使可能，也是十分困难的。

二、各层的设计问题

计算机网络的某些问题在好几层的设计中都会出现。下面， 我们将简略地提出其中比较重要的问题。

每一层都必须有一个建立连接的机制。因为网络中通常有许多计算机，有的机器又有多个进程。因此，要想建立连接的进程需要某种手段说明它想与哪一个进程建立连接。因为具有多个目标，要指明某个特定的目标需要某种寻址手段。

与在网上建立密切相关的一个机制是一旦不再需要连接时能够终止连接。正如我们将在下面看到的一样，这些看起来微不足道，实际上却很有技巧。

另一组设计决策与数据传输的规则有关。在某些系统中，数据仅在一个方向上传输(单工通信)。在另一些系统中，数据能在任意方向上传输，但不能同时传(半双工通信)。还有一些系统，数据能同时双向传输(全双工通信)。协议还需确定每条连接将对应多少