“十五”国家重点电子出版物规划项目·计算机知识普及和软件开发系列

编程新概念丛书 3

VB网络与远程控制编程实例教程

北京希望电子出版社 总策划
崔彦锋 许小荣 编 写

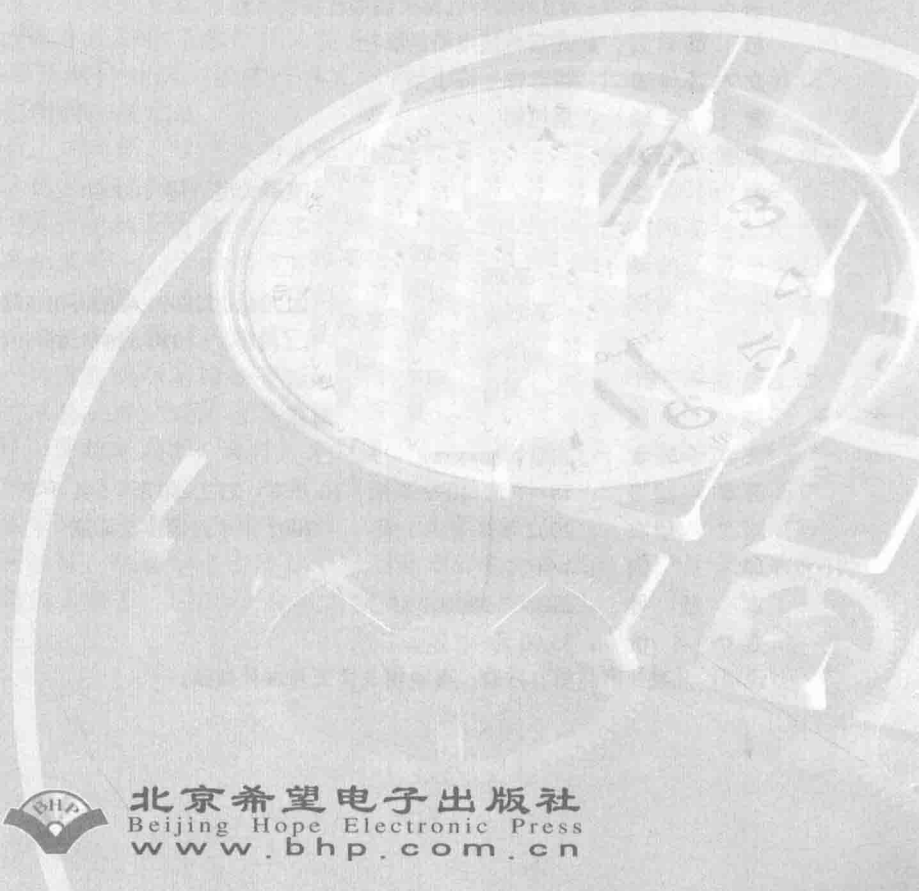
北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

“十五”国家重点电子出版物规划项目·计算机知识

编程新概念丛书 3

VB网络与远程控制编程实例教程

北京希望电子出版社 总策划
崔彦锋 许小荣 编 写



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本版是关于使用 VB 进行网络编程和远程控制方面的书。

本书着重介绍 VB 网络编程的功能，并与远程控制编程相结合，以木马程序的编写为载体，较为详细的介绍了进行网络通信与远程控制的原理和方法。本书为上下两篇，按照使用网络协议层次从高到低和木马程序的两种类别分篇。其中上篇主要介绍了网络基础、WNSOCK 使用、高级控件、系统与网络 API、文件处理等知识。并给出了一个综合应用上述知识的客户/服务器型木马程序的例子。下篇主要介绍了 HTTP、FTP、TELNET、POP3、SMTP 等网络应用层协议的内容和使用方法，并给出了无客户端木马的原理，最后本书附录 1 给出了常用的 Windows Socket 错误代码，附录 2 给出了有关 HTML 语言的基础知识，这些在网络程序的编写过程中经常遇到。

本书内容系统而丰富，例程众多，是对从事用 VB 进行网络编程及远程控制的广大编程人员重要的指导和参考书，同时也可作为高等院校相关专业师生教学、自学读物。

本书实例源代码请到www.b-xr.com下载。

有关该书的技术咨询，请与作者（sqq_books@263.net）联系。

系 列 书 名 ：“十五”国家重点电子出版物规划项目 计算机知识普及和软件开发系列
编程新概念丛书（3）

书　　名 ：VB网络与远程控制编程实例教程

总 策 划 ：北京希望电子出版社

文本著作者 ：崔彦锋　许小荣

责 任 编 辑 ：周凤明

出版、发行者 ：北京希望电子出版社

地　　址 ：北京市海淀区知春路63号卫星大厦三层 100080
网址: www.bhp.com.cn
E-mail: lwm@bhp.com.cn
电 话： 010-62520290,62521724,62528991,62630301,62524940,62521921,82610344
（发行） 010-82675588-202（门市） 010-82675588-501,82675588-201（编辑部）

经　　销 ：各地新华书店、软件连锁店

排　　版 ：希望图书输出中心　杜海燕

文本印刷者 ：北京媛明印刷厂

开本 / 规格 ：787 毫米×1092 毫米　16 开本　23.25 印张　546 千字

版次 / 印次 ：2002 年 8 月第 1 版　　2002 年 8 月第 1 次印刷

印　　数 ：1-4000 册

本 版 号 ：ISBN 7-900101-85-3

定　　价 ：35.00 元

前 言

近年来，随着 PC 的广泛应用和网络的不断发展，网络技术已经成为计算机领域内一个最为热门的发展方向。同时，随着网络技术一起发展的则是黑客技术和与之对应的网络安全技术。黑客技术虽然会对网络安全构成威胁，但它的不断发展从另一个方面讲则不断地促进了网络技术的发展和完善。

木马技术是最近几年来黑客技术中十分引人注目的一个方面，以国外的 BO.NETBUS 到国内的冰河木马，它吸引着无数的人去使用、探讨和研究。

Visual Basic 语言是目前世界上应用最为广泛地编程语言之一，它的简单易学、功能强大的特点使它在世界上拥有几百万的使用者。可以说，利用 VB 可以编制几乎所有的应用程序。在网络编程和远程控制方面，VB 同样有着诸多的优点，无论从控件出发还是从 API 出发，都可以轻松地写出强大的应用程序。

将网络编程与远程控制编程相结合，产生的正是木马程序。本书正是通过讲述木马程序的编写，一步步的为读者介绍网络与远程控制编程的方法。

需要说明的是，本书的编写目的，绝不是讲述如何编写木马程序，而是通过对木马程序编写的分析，讨论使用 VB 进行网络编程和远程控制的一般方法，木马仅是一个载体，一个可以引起读者更多兴趣的载体，所以本书并没有深入讨论黑客技术，只是介绍了木马原理和一个木马程序范例，没有直接给出可能引起严重后果的控制技术。

本书在编写过程中，避开了在网络编程和远程控制方面的繁琐细节和底层知识，直接用例程来讲述编程方法，使读者能够用最短的时间和最少的精力掌握这些方法，独立的编写此类软件。并且本书的例程都有着简单、典型的特点。需要说明的是，为了满足读者进一步深入学习的需要，本书还给出了几个较为复杂的例程，请读者阅读时注意。

本书并没有完全抛开理论知识，读者一样可以系统的学习到关于网络方面的编程知识，并掌握进行远程控制的一般方法。

本书在结构上分为上下两篇，这基于两方面的考虑：从编程所依靠的网络协议上讲，从上篇到下篇是一个从低层协议到高层协议的过程，从木马编程上讲，上篇讨论的是普通 C/S 型木马的编写。下篇讨论的是最新的无客户端木马的编写。这种结构的安排，对于读者的阅读和学习有许多的益处。一方面读者可以系统的学习网络编程的知识；另一方面，也为读者提供了多种阅读的方法，读者可以选择自己不熟悉的内容进行阅读，也可以系统的从第一章开始阅读，都将获得较好的效果。

本书的对象是有一定 VB 编程基础并有一定网络使用经验的读者，对使用非 VB 语言的读者和对远程控制技术感兴趣的读者也具有参考作用。

本书由崔彦锋、许小荣执笔编写，此外，朱双平、张蒙恩、谢海多、鲁逸凡、唐益梅、姚典、孔亮、魏勇、萧玉、丁桦、李林、朱莉、肖育新、李星雨、张刚、张诚华、高征、刘鹤年和李华羽等对本书的编写都作了很多工作，在此一并致谢。

由于本书编写时间仓促，编者水平有限，书中难免有错误和疏漏之处。读者如果有什么建议和意见，欢迎与编者联系。EMAIL 地址为：cuiyanfeng@x263.net。

编 者

2002.4

目　录

上　篇

下 篇

第1章　网络与协议基础

所谓的计算机网络，就是采用通信手段，将地理位置分散的、各自具备自主功能的若干台计算机有机的连接起来组成的一个复合系统，这个复合系统可以用来实现通信交往、资源共享和协同工作等目标。

现代计算机几乎是无法离开网络的，正如当年个人电脑以惊人的速度和规模进入人类的各个科研领域和日常生活中，如今网络技术和网络的飞速发展给人类的生存和生活又带来了一次巨大的冲击。认识网络，了解网络，使用网络已经成为人们的普遍愿望。在本章中，将重点讨论网络的应用知识，并会关注与编程有关的网络知识。

本章是全书的理论基础。通过本章的学习，读者应该重点掌握以下内容：

- 了解关于网络的基础知识
- 了解两种网络模型
- 了解 TCP/IP 协议
- 了解客户/服务器模式的原理

1.1　计算机网络

1.1.1　网络的概念与功能

在本章开始，我们已经给出了网络的一般定义。但在计算机网络发展过程的不同阶段中，人们对计算机网络提出了不同的定义，这些定义可分为三类：广义的观点、资源共享的观点与用户透明性观点。由目前计算机网络的特点看来，资源共享观点的定义能比较准确的描述计算机网络的基本特征。所以，简单看来，以资源共享为目的，把多台独立计算机在硬件上连接，并在软件上对这些连接加以规范，就形成了计算机网络。

我们可以通过对计算机网络与分布式系统区别认识来进一步的理解网络。分布式系统存在一个以全局方式管理系统资源的操作系统，可以动态的给系统拥有的所有通用的物理和逻辑资源分配任务，系统中的各台计算机既共同工作又自我管理，并通过计算机网络实现相互之间的信息交换，系统的内部结构对用户是完全透明的。当用户在当前计算机上键入命令时，是不必知道系统是如何运作的，整个系统就像是一个虚拟的单一处理器一样，任务的分配、文件的调用、传输等都是自动完成的。这正是分布式系统与计算机网络的最大不同点。在计算机网络中，当用户需要使用网络的共享资源时，是必须事先知道资源在网络中的位置的，而如前所述，在分布式系统中，这些是由系统自动完成的。

因此，我们知道分布式系统是建立在网络基础上的一种系统，它具有高度的整体性。相反，网络中的独立计算机是没有进行统一管理的。可见，利用软件在网络之上建立一个可以保证系统高度的一致性和整体性的系统，即是分布式系统。分布式系统是计算机网络技术发展的高级阶段。

概括说来，计算机网络可以实现以下三个基本功能：

- 计算机之间或计算机用户之间进行相互通信和交往。
- 共享资源，包括硬件资源、软件资源和数据与信息资源。
- 计算机之间或计算机用户之间的协同工作。

也就是，通信、共享、协同是计算机网络的三大基本功能。但它具体可以带给我们什么呢？

（1）计算机网络可以产生一个性价比更高的系统

在某些需要一个大型主机加上多台终端的使用中，可以考虑把多台 PC 机连成一个网络协同工作来代替大型机系统，这样，不仅维护运行简单，对人员要求低，并且在价格上会更加的便宜，在功能上完全可以替代大型机系统。

（2）计算机网络可以提供更好的可用性和可靠性的应用环境

独立的计算机一旦出现问题，整个系统所有应用将不能运行，而利用网络，不仅可以利用其他计算机继续进行工作，而且如果文件损坏，还可以在其他计算机上找到副本以代替，甚至某些连接线路出现问题，也可以以其他线路来代替传递信息，进而保证系统继续运转。这样整体系统的可用性和可靠性就会大大提高。

（3）在网络内对任务的调度可以使工作负荷均衡分配

在网络中依靠软件调度，可以把某段时间中工作负担特别重的计算机中的部分任务重新分配给其他空闲计算机来运行，也可以依靠事先的调度策略来平衡计算机间的工作量，从而可以节约时间，节省运行成本等。

（4）计算机网络可以增强系统的可扩展性

随着企业机关规模的扩大，信息系统的规模也不断的扩大，主要表现在用户的增多和共享信息量的增大，这时，相应可以通过增加客户机和服务器的个数来满足以上增长的需要，从而提供很好的可扩展性。

（5）计算机网络为用户提供了功能更加强大的通信工具

随着网络的发展，其通信特性越来越被人们发现和利用，网络用户可以互相传递文件，可以通过 EMAIL 方便的传递信息，甚至可以利用软件进行即时聊天通信，越来越多的人利用网络形成全新的工作方式和交往方式。

总之，网络的种种功能，不仅日益方便了人们的工作，在人们的生活中也将发挥越来越大的作用。

1.1.2 网络分类

网络因分类方式的不同而分成不同的种类，最常用的分类方式是如下两种：

- 按地理区域范围分类网络
- 按信息传输技术分类网络

1. 按地理区域范围分类网络

由于地理区域范围的不同，计算机网络中采用的技术也不相同，从而形成了不同的网络技术特点和网络服务功能。按范围大小的不同，网络可分为三类：局域网 LAN、城域网 MAN、广域网 WAN。

（1）局域网 LAN 及其特点

局域网典型的应用场合为：

- 同一房间内的所有主机，覆盖范围在 10 米以内。
- 同一楼宇内的所有主机，覆盖范围在 100 米以内。
- 同一校园内、厂区内的所有主机，覆盖范围在 1000 米以内。

局域网的基本特征是：

- 整个 LAN 内的所有物理设备分布在半径不超过几公里的有限地理范围内。
- 整个 LAN 为同一组织或机构所拥有。
- 在 LAN 中可实现极高的数据传输速率，一般在 1Mbps～100Mbps 之间，此处 bps 是指每秒传递的二进位数。
- LAN 的连接非常规范，有严格的标准可遵循。

（2）城域网 WAN 及其特点

城市地区网络常简称城域网。城域网是介于广域网与局域网之间的一种高速网络。它的覆盖范围是几十公里范围内的大量企业机关公司的多个局域网，能适应大量用户之间的数据、语音、图形和视频等多种信息的传输。

（3）广域网 WAN 及其基本特征

所有主机与工作站点分布的地理范围能覆盖 1000 公里以上的数量级，比如同一个大城市，同一个国家，同一洲甚至几个洲等。

它的基本特征是：

- 在 WAN 中信息传递的传输距离相对很长，可达几公里以上，甚至几千公里以上，涉及到对远程计算机的访问。
- WAN 通常为多个部门所共有。
- WAN 中长距离通信的传输速率相对较低，一般在几十 Kbps 到 2Mbps 之间。
- WAN 的互联结构一般并不规整，有相当大的随意性。

2. 按信息传输技术分类网络

网络所采用的传输技术决定了网络的主要技术特点，因此根据网络所采用的传输技术对网络进行分类是一种很重要的方法。据此大致可以将网络分为两类：

- 广播式网络：在网络中只有单一的一个通信信道，由这个网络中所有的主机所共享。当从一个广播式网络中任何一台主机发送出一个短的报文（分组）时，在网上所有的主机都可以接受到，通过报文内的“地址字段”来决定是发送到哪台主机。
- 点到点网络：当在一个网络中成对的主机之间存在着若干对的相互连接关系时，便组成了一个点到点的网络。在每一对主机之间进行通信时，一台主机作为信息的源，另一台主机作为信息的宿。允许一台主机与多台主机建立点点通信关系。

1.1.3　局域网

1. 局域网的组成

任何网络都是由计算机硬件、软件、通信设备和通信线路（通信介质）所组成。具体

来看，一个LAN大体上由以下三部分组成：

- 网络硬件：包括作为LAN站点的各台计算机及其配置的各种外围设备，如网卡等。其它还有诸如集线器、交换机、重发器和网桥等。
- 网络软件：通常是指实现LAN功能用的“服务器软件”和“客户机工作站软件”。一般来说网络操作系统可以满足要求。
- 网络信息资源与网络应用程序：在网络上的数据与信息资源有可能涉及到相当广泛的内容，包括广义的数据，也包括应用程序，系统程序以及各类工具软件或其他软件。

如果把一个LAN看成由“资源子网”和“通信子网”组成，通信子网由传输介质，计算机内的网卡和可选的网络连接设备等组成。资源子网则由LAN中的各台计算机及其外部设备组成。网络上硬件资源、软件资源与信息资源等都驻留在相应的各台计算机内，客户机面向最终用户工作使用，服务器作为资源的主要存放点和服务点。

2. 网络拓扑结构

计算机网络设计中，首要问题就是要在给定的位置及保证网络流量的和可靠性的前提下，选择合适的线路和连接方式，在局域网中，这一点尤为明显。

常见的网络拓扑结构有以下5种。

（1）星型　星形拓扑结构是由通过点到点链路接到中央结点的各站点组成的。星型网络中有一个唯一的转发结点（中央结点），每个计算机都通过单独的通信线路连接到中央结点。星型拓扑的优点是：利用中央结点可方便地提供服务和重新配置网络；单个连接点的故障只影响一个设备，不会影响全网，容易检测和隔离故障，便于维护；任何一个连接只涉及到中央结点和一个站点，因此控制介质访问的方法很简单，从而访问协议也十分简单。星型拓扑的缺点是：每个站点直接与中央结点相连，需要大量电缆,因此费用较高；如果中央结点产生故障，则全网不能工作，所以对中央结点的可靠性和冗余度要求很高。Windows 95对等网常采用星形拓扑。

（2）环型　环形拓扑结构由连接成封闭回路的网络结点组成，每一结点与它左右相邻的结点连接。环形网络常使用令牌环来决定哪个结点可以访问通信系统。在环形网络中，信息流只能是单方向的，每个收到信息包的站点都向它的下游站点转发该信息包。信息包在环网中“旅行”一圈，最后由发送站进行回收。当信息包经过目标站时，目标站根据信息包中的目标地址判断出自己是接收站，并把该信息拷贝到自己的接收缓冲区中。为了决定环上的哪个站可以发送信息，平时在环上流通着一个叫令牌的特殊信息包，只有得到令牌的站才可以发送信息，当一个站发送完信息后就把令牌向下传送，以便下游的站点可以得到发送信息的机会。环形拓扑的优点是它能高速运行，而且为了避免冲突其结构相当简单。

（3）树型　树形拓扑结构可以看成是星型拓扑的扩展，在此结构中，结点按层次进行连接，信号主要在上下两层间传输，相邻结点及同层结点之间一般不进行数据交换。

（4）网状型　在网状拓扑结构中，结点之间的连接是任意的没有规律，其主要优点是系统可靠性高。但是这种结构过于复杂，不方便管理和应用。

（5）总线型　总线拓扑结构采用单根传输线作为传输介质，所有的站点都通过相应的

硬件接口直接连接到传输介质或称总线上。任何一个站点发送的信号都可以沿着介质传播，而且能被其他所有站点接收。总线拓扑的优点是：电缆长度短，易于布线和维护；结构简单，传输介质又是无源元件的，从硬件的角度看，十分可靠。总线拓扑的缺点是：因为总线拓扑的网不是集中控制的，所以故障检测需要在网上的各个站点上进行；在扩展总线的干线长度时，需重新配置中继器、剪裁电缆、调整终端器等；总线上的站点需要介质访问控制功能,这就增加了站点的硬件和软件费用。以太网等常采用总线结构。

1.1.4 Internet 介绍

Internet是全球性的互联网络，它是由计算机和网络互相连接组成的庞大集合，任何一台Internet中的计算机都能够和其它网中交换信息。

Internet的产生可以追溯到20世纪60年代末期，由为美国军方服务的ARPA网经过三十多年而发展形成的。

联入 Internet 通常有以下几种方式：

- 普通用户可以通过电话线拨号联入校园网或企业网，或者联入 Internet 服务提供商
- 通过局域网联入校园网或企业网
- ISDN 接入
- ADSL 接入
- cable modem 接入
- 低轨道卫星网接入

用户可以根据对速度等的需要选择自己的接入方式。

我国现有四个较大的互联网，分别是：CHINANET(中国公用计算机互联网，由邮电部门的相关公司负责)，CHINAGBNET(中国金桥互联网，以信息产业部下属公司为主负责)，CERNET(教育科研网)和 CSTNET(中国科学技术互联网)。1997 年开始发展了多媒体网(169)和其他一些互联网。我国的广大用户可以通过接入 ISP 申请加入因特网获得其服务。

Internet目前提供的较为流行的服务有：

- 全球范围的超媒体信息浏览服务（WWW）
- 远程登录（telnet）
- 文件传输（FTP）
- 电子邮件（E-mail）

其中，WWW 服务是目前广泛在因特网上使用的高级浏览服务，把存放于全球范围内的众多计算机上的信息以超媒体的方式链接在一起，构成了一个世界范围的网，称为 WWW（world wide web）。它制定了一套标准化且易懂的超文本描述语言 HTML、超文本传输协议 HTTP 协议和统一的资源定位格式 URL。URL 规定了一个文档在 WWW 中存放地点的统一格式及地址。如：http://www.seu.edu.cn 就是一个 URL 地址，其中第一部分 http 表示所遵循的协议，第二部分就是信息资源所在的计算机名，它的后面还可以有目录名和文件名，如果省略，就表示主页。在进行 WWW 浏览时，通过浏览器看到的即是一个 HTML 格式的文件，它可以引导访问者进一步访问其他的信息和资源。

到目前为止，Internet 还在不断的发展和扩大中，它提供的服务也在不断的增长中。

1.2　两种网络模型

计算机网络结点之间的信息和数据交换是在不断进行着的，要做到有条不紊的交换数据，每个结点都必须遵守一些事先约定好的规则，这些规则对交换时数据的格式、交换的顺序、流量的控制等进行了一系列的规定。这些规定就成为网络协议。对复杂的计算机网络协议最好的组织方式是层次结构，我们将计算机网络层次结构模型和各层协议的集合称为计算机网络体系结构，实行层次结构，灵活性高，易于实现和维护，各层可以采用最合理的技术来实现，并且有利用促进标准化的发展，所有的这种网络体系结构发展很快，至今，影响最大的是 ISO/OSI 参考模型和 TCP/IP 参考模型。

1.2.1　ISO/OSI 模型

ISO/OSI 参考模型（即开放系统互联参考模型，Open System Inter connection Reference Model）是由国际标准化组织（ISO）发布的，它定义了网络的七层框架，并在这一框架下进一步详细规定了每一层的功能，以实现开放系统环境中的互联性、互操作性和应用的可移植性。在这个模型中，将通信会话需要的各种进程划分成 7 个相对独立的功能层次，这些层次的组织是以在一个通信会话中事件发生的自然顺序为基础的。

表 1-1 描述了 OSI 模型，其中 1~3 层提供了网络访问，4~7 层用于支持端端通信。

表 1-1　OSI 模型层次参考

OSI 层次号	OSI 参考模型层次描述
7	应用层
6	表示层
5	会话层
4	传输层
3	网络层
2	数据链路层
1	物理层

1. 物理层

最底层称为物理层(Physical Layer)，这一层负责传送比特流，它从第二层数据链路层(DLL)接收数据帧，并将帧的结构和内容串行发送，即每次发送一个比特，然后这些数据流被传输给 DLL 重新组合成数据帧。从字面上看，物理层只能看见 0 和 1 ，它没有一种机制用于确定自己所传输和发送比特流的含义，而只与电信号技术和光信号技术的物理特征相关。这些特征包括用于传输信号电流的电压、介质类型以及阻抗特征，甚至包括用于终止介质的连接器的物理形状。

对 OSI 第一层，人们常常有这样的误解：就是认为 OSI 第一层应该包括所有产生或发送通信数据信号的机制。其实并非如此，OSI 第一层只是一个功能模型，物理层只是一种

处理过程和机制，这种过程和机制用于将信号放到传输介质上以及从介质上收到信号。它较低层的边界是连向传输介质的物理连接器，但并不包含传输介质。

传输介质包含真正用于传输由OSI第一层机制所产生信号的任何方法。一些传输介质是同轴电缆、光纤、双绞线等。人们之所以感到迷惑，主要是因为物理层对介质的性能没有提出任何规范。介质的性能特征对于物理层定义的过程和机制是需要并假定存在的。

因此，传输介质处于物理层之外，有时被称为OSI参考模型的第0层。

2. 数据链路层

OSI参考模型的第二层称为数据链路层(DLL)。与所有其他层一样，它肩负两个责任：发送和接收。它还要提供数据有效传输的端端(端到端)连接。在发送方，DLL需负责将指令、数据等包装到帧中，帧(frame)是DLL层生成的结构，它包含足够的信息，确保数据可以安全地通过本地局域网到达目的地。成功发送意味着数据帧要完整无缺地到达目的地。也就是说，帧中必须包含一种机制用于保证在传送过程中内容的完整性。

为确保数据传送完整安全到达，必须要做到两点：

- 在每个帧完整无缺地被目标节点收到时，源节点必须收到一个响应。
- 在目标节点发出收到帧的响应之前，必须验证帧内容的完整性。

有很多情况可以导致帧的发送不能到达目标或者在传输过程中被破坏或不能使用。DLL有责任检测并修正所有这些错误。

DLL的另一个职责是重新组织从物理层收到的数据比特流。不过，如果帧的结构和内容都被发出，DLL并不重建一个帧。相反，它缓存到达的比特流直到这些比特流构成一个完整的帧。不论哪种类型的通信都要求有第一层和第二层的参与，不管是局域网(LAN)还是广域网(WAN)都是如此。

3. 网络层

网络层负责在源机器和目标机器之间建立它们所使用的路由。这一层本身没有任何错误检测和修正机制，因此，网络层必须依赖于端端之间的由DLL提供的可靠传输服务。

网络层用于本地LAN网段之上的计算机系统建立通信，它之所以可以这样做，是因为它有自己的路由地址结构，这种结构与第二层机器地址是分开的、独立的。这种协议称为路由或可路由协议。路由协议包括IP、Novell公司的IPX以及AppleTalk协议。本书将着重讲述IP协议以及与其相关的协议和应用。

网络层是可选的，它只用于当两个计算机系统处于不同的由路由器分割开的网段这种情况，或者当通信应用要求某种网络层或传输层提供的服务、特性或者能力时。例如，当两台主机处于同一个LAN网段的直接相连这种情况，它们之间的通信只使用LAN的通信机制就可以了(即OSI参考模型的一二层)。

4. 传输层

传输层提供类似于DLL所提供的服务，传输层的职责也是保证数据在端端之间完整传输，不过与DLL不同，传输层的功能是在本地LAN网段之上提供这种功能，它可以检测到路由器丢弃的包，然后自动产生一个重新传输请求。传输层的另一项重要功能就是将乱

序收到的数据包重新排序，数据包乱序有很多原因。例如，这些包可能通过网络的路径不同，或者有些在传输过程中被破坏。不管是什么情况，传输层应该可以识别出最初的包顺序，并且在将这些包的内容传递给会话层之前要将它们恢复成发送时的顺序。

5. 会话层

OSI 的第五层是会话层，相对而言，这一层没有太大用处，很多协议都将这一层的功能与传输层捆绑在一起。OSI 会话层的功能主要是用于管理两个计算机系统连接间的通信流。通信流称为会话，它决定了通信是单工还是双工。它也保证了接受一个新请求一定在另一请求完成之后。

但是，我们有必要解释传输层与会话层之间的不同侧重点。运输层为会话层提供两个节点间的连接。而会话层提供用户间的连接。举个例子可能利于这个问题的理解。

王经理想要和李经理通个电话，这里面可能包括两个过程，首先他对他的秘书说："请给李经理打个电话！"然后，他的秘书就会拿起电话机，开始拨李经理的电话号码。接着，李经理就收到了电话，得知是李经理要和他通话，最后，王经理的秘书去通知王经理，王李二经理开始通话。

过程一是请求一次会话层连接，这时，王经理并不需要知道李经理的电话号码，也不需要自己来拨这个电话；过程二是一个请求传输层连接，拨号和初始化连接的过程与电话公司的交换电路传送电话的实际方式无关。传输层也不必关心这些具体技术细节。过程三则是建立了传输层连接；过程四是最终建立了会话层的连接。通过这个例子中的四个过程，读者应该可以清楚传输层和会话层之间的不同了。

6. 表示层

表示层负责管理数据编码方式，不是所有的计算机系统都使用相同的数据编码方式，表示层的职责就是在可能不兼容的数据编码方式，例如在 ASCII 和 EBCDIC 之间，提供翻译。表示层可以用在浮点格式间的调整转换，并提供加密解密服务。

我们必须区分信息与数据之间的区别，因为这很重要。当我们说数据时，浮现在脑海中的是大批存储的数字，一大堆十六进制数，或是一长串字母和特殊符号。简单地说，计算机存储的不是信息，而是数据。信息是人为地赋予数据的含义。从最根本上说，数据是比特位、字节和其他无法表达的东西的分类。信息则是一种人为的解释。现在的问题是不同的计算机表示相同信息的方式各不相同。所以，仅仅定义有效的数据通信是不够的，还必须定义有效的信息通信。而这正是表示层的任务。

比如有一个在两台计算机间传输数据的网络，其中一台计算机使用 ASCII 编码存储信息，另一台使用 EBCDIC 编码，它们代表了存储数据的两种不同方式（第二章将进一步介绍 ASCII 和 EBCDIC 编码）。当基于 ASCII 的计算机说"HELLO"时，网络将其 ASCII 编码传送出去。基于 EBCDIC 的计算机接收并存储这些数据。但不幸的是，由于对接收到的比特位有不同的解释，人们看到的信息将是"<<!"。

表示层在数据传输过程的加密也是被广泛利用的，有兴趣的读者可以参看其它书籍。

7. 应用层

OSI 模型中的最高层就是应用层，它负责与用户和应用程序进行通信。之所以称它为应用层，是因为它包含网络应用。网络应用不同于用户的各种应用，例如工资册或会计程序、图像设计工具包、语言翻译工具或数据库程序等。典型的网络应用包括万维网应用、电子邮件、文件传输、虚拟终端协议和分布式系统等。

以上我们较为详细的介绍了 OSI 模型的七层结构，读者只需要理解它们，在我们的编程过程中，将不会遇到这些具体的问题，但是，这些知识对我们更好的理解程序是有很大益处的。

1.2.2 TCP/IP 参考模型

TCP/IP 起源于 60 年代末美国政府资助的一个分组交换网络研究项目，到 90 年代已发展成为计算机之间最常应用的组网形式，它是 Internet 的基础。鉴于此模型的广泛使用和支持，我们将会详细的讨论和介绍这个模型及其使用。

TCP/IP 通常被认为是一个四层协议系统，可以参看表 1-2。

表 1-2 TCP/IP 模型结构

TCP/IP 模型各层序号	各层名称
4	应用层
3	传输层
2	网络层
1	链路层

与 OSI 模型类似，每一层负责的功能如下：

1. 链路层

有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

2. 网络层

有时也称作互联网层，处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（网际协议），ICMP 协议（Internet 互联网控制报文协议）以及 IGMP 协议（Internet 组管理协议）。

3. 运输层

主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。由于运输层提供了高可靠性的端到端的通信，因此应用层可以忽略所有这些细节。而另一方面，UDP 则为应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端。任何必需的可靠性必须由应用层来提供。这两种

运输层协议分别在不同的应用程序中有不同的用途。

以上两种协议将会在我们在以后章节中讨论的 WINSOCK 控件得到广泛的应用。

4. *应用层*

负责处理特定的应用程序细节。几乎各种不同的 TCP/IP 实现都会提供下面这些通用的应用程序：

- Telnet 远程登录
- FTP 文件传输协议
- SMTP 简单邮件传送协议
- SNMP 简单网络管理协议

它们的具体应用我们在本书中会详细的讨论。

以上四层结构和其所包含的网络协议及其互相依赖关系可以参看图 1-1。

ARP（地址解析协议）和 RARP（逆地址解析协议）是某些网络接口使用的特殊协议，用来转换 IP 层和网络接口层使用的地址。IGMP 是 Internet 组管理协议。它用来把一个 UDP 数据报多播到多个主机。ICMP 是 IP 协议的附属协议。IP 层用它来与其他主机或路由器交换错误报文和其他重要信息。IP 是网络层上的主要协议，同时被 TCP 和 UDP 使用。TCP 和 UDP 的每组数据都通过端系统和每个中间路由器中的 IP 层在互联网中进行传输。TCP 协议和 UDP 协议是最有用的传输层协议，它们都是基于网络层的 IP 协议，虽然 TCP 使用不可靠的 IP 服务，但它却提供一种可靠的运输层服务。UDP 为应用程序发送和接收数据报。一个数据报是指从发送方传输到接收方的一个信息单元（例如，发送方指定的一定字节数的信息）。但是与 TCP 不同的是，UDP 是不可靠的，它不能保证数据报能安全无误地到达最终目的。

同时由图 1-1 知道，用户的程序只可以直接工作在 TCP、UDP 以及 ICMP 和 IP 协议之上，其中 TCP 和 UDP 协议使用的较为广泛，也是我们重点讨论的对象；依赖 ICMP 协议的程序有常用的 PING 命令等；依赖 IP 协议的程序已经不太多见。我们的程序是工作在应用层的，即为某一个用户进程，它们直接依靠的就是 TCP 和 UDP 协议。同时在应用层也存在者多种协议，它们是为了某种专门的应用而引入的，这点我们将在本书的后半部分加以讨论。

我们使用 Internet 服务程序大都工作在应用层，使用的协议主要是 FTP、HTTP、TELNET、SMTP 等。其中 HTTP 协议（Hypertext Transfer Protocol，超文本传输协议）是 Web 操作的基础，它是一个使信息能通过 Web 交换的客户/服务器协议。HTTP 定义了浏览器能提出的请求的类型以及服务器返回的响应的类型。通过 HTTP，用户可以从远程服务器中获取网页，或如果他有权限，就可以将网页存储在服务器中。HTTP 还提供向网页上添加新信息或全部删除它们的能力。FTP（File Transfer Protocol，文件传输协议）是进行多种格式文件访问的最常用协议，同 HTTP 协议一样，在互联网上有许多的 FTP 服务器，使用 FTP 协议进行工作，大多用来传递文件和发布文件等。Telnet 是网络虚拟终端协议的一个例子，目前的普通应用就是各个著名大学的 BBS 系统。SMTP 支持着网络的最普遍用途之一——电子邮件——将报文或文件传送给本地或远程站点。这些协议在 VB 中的应用将会在后面的章节中进行讨论。

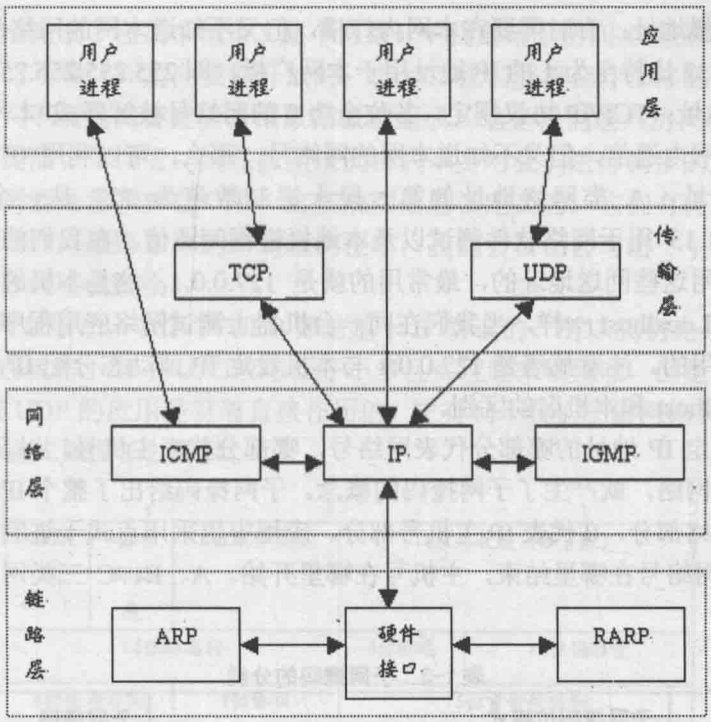


图 1-1　TCP/IP 层次模型作用的相互作用

1.3　通信协议

我们将要进行的内容都是基于传输层协议的，在 TCP/IP 模型中，最常用的传输层协议是 UDP 和 TCP 协议，所以在下面的章节中我们将要学习这两种最常用的协议。

在此之前我们先来看看 TCP/IP 协议组中的三个参数，它们分别是：IP 地址、子网掩码和网关地址，这是在 TCP/IP 网络环境中确定某一台计算机的基础。

IP 地址实际上是采用 IP 网间网层通过上层软件完成“统一”网络物理地址的方法,这种方法使用统一的地址格式，在统一管理下分配给主机。Internet 网上不同的主机有不同的 IP 地址，每个主机的 IP 地址都是由 32 比特，即 4 个字节组成的。为了便于用户阅读和理解，通常采用“点分十进制表示方法”表示，每个字节为一部分，中间用点号分隔开来。如 202.119.0.22 就是东南大学的某台计算机。每个 IP 地址又可分为两部分。网络号表示网络规模的大小，主机号表示网络中主机的地址编号。按照网络规模的大小，IP 地址可以分为 A、B、C、D、E 五类，其中 A、B、C 类是三种主要的类型地址，D 类专供多目传送用的多目地址，E 类用于扩展备用地址。

在 IP 地址中，有几种特殊含义的地址：

- 广播地址：TCP/IP 协议规定，主机号部分各位全为 1 的 IP 地址用于广播。所谓广播地址指同时向网上所有的主机发送报文，也就是说，不管物理网络特性如何，Internet 网支持广播传输。如 136.78.255.255 就是 B 类地址中的一个广播地址，你将信息送到此地址，就是将信息送给网络号为 136.78 的所有主机。