计算机专业人员书库

远程控制编程技术

张友生 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

计算机专业人员书库

远程控制编程技术

张友生　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

远程控制是管理人员在异地通过计算机网络,异地拨号或双方都接入 Internet 等手段,连接目标计算机,并通过本地计算机对远程计算机进行管理和维护的行为。远程控制既可以作为黑客攻击手段之一,也可以作为远程维护,在家办公等应用领域的支持工具。

本书在源代码级上系统而全面地介绍了远程控制的技术和方法。全书共分 5 章。第 1 章介绍网络应用协议、常用设备和服务,并对 TCP/IP 协议进行重点分析。第 2 章讲述远程控制的基本概念、功能和发展前景。第 3 章讲述远程控制软件的实现基础,重点阐述 Socket 编程的基本原理及 Windows 的消息系统。第 4 章详细讲解远程控制软件各种功能的具体实现方法。第 5 章讲解一个远程控制的综合实例,其内容主要包括控制端程序、被控制端程序、Windows 帮助的加入和制作安装程序。

通过本书学习,读者会对远程控制软件有系统、深入的理解,能够独立完成远程软件的分析和编程工作,熟练地编写互联网络程序。

本书可供网络工程师、网络管理维护人员及网络爱好者学习与使用。

图书在版编目(CIP)数据

远程控制编程技术/张友生编著 .—北京:电子工业出版社,2002.1
(计算机专业人员书库)
ISBN 7-5053-7382-X

Ⅰ.远… Ⅱ.张… Ⅲ.网络控制程序—程序设计 Ⅳ.TP311.1

中国版本图书馆 CIP 数据核字(2001)第 093151 号

丛 书 名:计算机专业人员书库
书 名:**远程控制编程技术**
编 著 者:张友生
责任编辑:黄志瑜
排版制作:电子工业出版社计算机排版室
印 刷 者:北京天宇星印刷厂
装 订 者:三河市万和装订厂
出版发行:电子工业出版社 http://www.phei.com.cn
北京市海淀区万寿路 173 信箱 邮编 100036
经 销:各地新华书店
开 本:787×1 092 1/16 印张:19.5 字数:499 千字
版 次:2002 年 1 月第 1 版 2002 年 1 月第 1 次印刷
书 号:ISBN 7-5053-7382-X / TP·4255
印 数:5 000 册 定价:30.00 元

前　言

对于广大网民来说，远程控制软件不算陌生。它因简便、易行及有效而深受广大黑客青睐。你的计算机一旦运行远程控制软件，它就变成了一台傀儡机，对方可以在你的计算机上下载与上传文件，任意执行程序，控制你的屏幕和鼠标，偷窥你的私人信息，窃取你的各种密码及口令。它还可秘密共享你的硬盘，为其他人访问你的计算机打开后门，受控制的你的一切秘密都将暴露在别人面前，隐私已不复存在！

什么是远程控制

在系统安全的分析中对于远程控制软件的定义有很多种。笔者认为，远程控制是管理人员在异地通过计算机网络(WAN)和异地拨号或双方都接入 Internet 等手段，连接目标计算机，通过本地计算机对远程计算机进行管理和维护的行为。

远程控制软件实际上是一种客户机/服务器程序，服务器程序安放在被控制的计算机端，客户机程序安装在控制端。在客户端和服务器端都安装成功之后，客户端在网络上一搜寻到已经安装了服务器的远程计算机，就发出获得服务器端的连接指令，两台 PC 建立起连接，然后就可以通过网络的互联协议 TCP/IP 进行远程控制。

远程控制的原理很简单：本机直接启动运行的程序拥有与使用者(客户端)相同的权限。因此，如果能够启动服务器端的服务器程序，就可以使用相应的客户端程序直接控制主机了。也就是说，客户端就好比一个超级用户，可以直接控制计算机。

远程控制的发展

起初，使用远程控制软件，是为了让 PC 用户在离开办公室时能访问其台式 PC 硬盘中的信息，甚至可以通过其台式 PC 访问企业网络资源。今天，许多企业和增值分销商正在把远程控制能力作为有效的技术支持工具。很多网络管理员都采用这类软件对局域网进行管理，或者在家中更新自己网站的内容。这类软件对于出差在外的商务人员用处非常大，因为他们可以随时提取自己家里计算机中的数据和资料。远程控制软件在计算机远程教学和培训中也发挥了不少的作用，使身处异地的学生能够与老师进行实时交流，犹如坐在同一教室一般。

近年来，黑客技术不断成熟起来，对网络安全造成了极大的威胁。黑客的主要攻击手段之一，就是使用远程控制技术，渗透到对方的主机系统里，从而实现远程操作目标主机。其破坏力之大，是绝不容忽视的。

远程控制的前景

随着网络技术的进一步发展，网络速度越来越快，家庭办公将成为未来的时尚，远程技术支持将逐渐占据技术支持的主流。远程教学和培训也将快速发展，企业规模将迅速扩大。所有这些发展都为远程控制软件提供了一个广阔的天地。根据 IDC 预计，远程控制软件市场将从 1998 年的 6.77 亿美元发展到 2002 年的 19 亿美元，年增长率达 31.5%，是软件技术支持消

费中第3个增长最快的领域。

本书的内容

常言道:“知己知彼,百战百胜”。本书将对远程控制所涉及的技术和方法进行源代码级的详细讲解,使读者对远程控制软件有系统和深入的理解,能够独立完成远程控制软件的分析和编程工作,能够熟练地编写互联网络程序。

本书正文共分5章。第1章简单地介绍网络应用协议、常用设备和服务,对TCP/IP协议进行重点分析。第2章讲述远程控制的基本概念、功能和发展前景,对远程控制软件、木马、病毒与黑客程序进行了对比分析,最后介绍了远程唤醒的基本原理和一个常见远程控制软件的使用方法。第3章讲述远程控制软件的实现基础,重点阐述Socket编程的基本原理及Windows的消息系统。第4章通过Visual C++ 6.0,详细讲解远程控制软件各种功能的具体实现方法。这些功能包括远程屏幕抓取的实现,远程关机或重新启动,网络邻居及IP地址的获取,程序的自动启动与隐藏,键盘与鼠标的控制,网络聊天功能的实现,远程文件管理的实现,系统信息的获取与修改,拨号功能的实现及执行和关闭外部应用程序等。第5章讲解一个远程控制的综合实例,包括控制端程序、被控制端程序、Windows帮助的加入及制作安装程序。

技术支持

本书没有配备光盘,但所有程序源代码及最终的控制软件都可以在软件工程专家网(http://www.21cmm.com)上下载。

致谢

在本书出版之际,我要衷心感谢在研究和写作过程中曾给我大力支持的陈祖福、刘顺保、肖东辉等同志,感谢陈松乔教授给予我的指导。特别要感谢何玉云和张啸杰同志,在本书的成稿过程中,他们几乎承担了所有程序的调试工作和文稿的打印工作。另外,在本书编写过程中,也参考了一些Internet上的文章,在此,对这些文章的作者一并表示感谢。

由于时间仓促,作者水平有限,书中难免有不妥和错误之处,恳请读者批评指正。

张友生

2001年12月

目　录

第 1 章　网络及应用协议

进行远程控制的一个前提条件是有一个控制环境，这个环境就是计算机网络。因此，在讲述远程控制的具体技术之前，先学习一些网络的基本知识。这些知识对于编写远程控制软件是不可或缺的，特别是 TCP/IP 协议，因为 TCP/IP 是整个计算机网络的灵魂。

在这一章里，先简单地介绍一些网络的基本概念，然后讲一讲网络的应用和常用协议，最后对 TCP/IP 协议进行剖析。

1.1　计算机网络的基本概念

1.1.1　计算机网络的定义

对于计算机网络（Computer Network），在不同的阶段或从不同的角度看有着不同的定义，有的把它定义为“以相互共享（硬件、软件和数据）资源的方式而连接起来，且各自具有独立功能的计算机系统的集合”。这个定义着重于应用目的而没有指出计算机网络的结构。有的则从结构上来看待计算机网络，而把它定义为“在网络协议控制下，由两台以上计算机和若干台终端，或数据传输设备连接而成且相互间能进行通信的计算机复合系统”。还有的把计算机网络定义为“利用各种通信手段，如电报、电话和微波通信等，把地理位置上分散的计算机有机地连接在一起，达到相互通信而且共享软件、硬件和数据等资源的系统”。

1.1.2　计算机网络的基本功能

1．数据通信

计算机联网之后，便可以互相传递数据和进行通信。现在随着 Internet 在世界各地的风行，传统的传媒已经受到了很大的冲击，特别对于邮电、报纸、新闻及电视等行业的影响更深刻。随着宽带网的出现，这些行业通过计算机网络将会提供速度更快，质量更优和价格更低廉的服务。

2．资源共享

这是计算机网络的主要用途。计算机在广大的地域范围内联网后，网络中各计算机的资源原则上都可以共享，可以突破地域范围的限制。共享的资源主要有：硬件、软件、数据及各种类型的信息。

3．提高系统可靠性

计算机网络一般都采用分布式控制方式，如果有单个部件或少数计算机失效，但由于相同的资源可分布在不同地点的计算机上，所以可以通过不同的网络路由来访问这些资源，从而不影响用户对同类资源的访问。

4．促进分布式数据处理和分布式数据库的发展

分布式结构使得在获得数据和需要进行数据处理的地方都可以设置计算机，把数据处理的功能分散到各个计算机上。因此利用网络环境可实现分布处理和建立性能优良，可靠性高的分布式数据库系统。

1.1.3　计算机网络体系结构

对于计算机终端或其他数据处理设备间的数据交换，必须考虑完成下列任务：

1）信源系统要激活直接数据通道或通知通信网络所期望的信宿系统的地址；

2）信源系统必须确认信宿系统已准备好接收数据；

3）在文件传输过程中必须确认信宿系统的文件管理程序已准备接收并存储这个文件；

4）如果两台机器的文件格式不兼容，其中的某台机器必须进行格式转换工作。

这表明，在两个计算机系统之间，必须存在更高级别的合作。在计算机之间进行以协作为目的的数据交换一般称之为“计算机网络通信”。同样，当两台以上计算机经由通信网络互相连接，这个计算机工作站的集合也称之为“计算机网络”。由于对终端用户或计算机用户来说两者都具有相同的协作层次，因而这些通信的实体往往被称之为终端。

协议是为了在不同系统中的实体间进行通信而使用的。这里，实体和系统两词都是泛指的。实体的例子可以是用户应用程序、文件传输信息包、数据库管理系统、电子邮件系统及终端等；系统的例子有计算机、终端及远程传感器。一般来说，实体能够发送或接收信息，而系统可以包容一个或多个实体，而且在物理上是实际存在的物件。

为了两个实体能够实现通信，它们须使用“相同的语言”。交流什么信息，如何交换，何时通信，这在参与通信的实体间必须达成互相都能接受的安排。这些安排就是规程或协议。协议往往被制订成一系列规则，用来管制两个实体间的数据交换。协议中的关键因素包括：

1）语法，包括数据格式和信号电平等；

2）语义，包括协调用的控制信息和差错管理；

3）规则，包括时序控制，速率匹配和定时。

在介绍了协议之后，再引入协议体系结构的概念。我们已经知道，在计算机之间通信，需要更高层次的协作。如果不再把它从逻辑上看成一件事（任务），而是将其划分成几件事来做（也叫子任务），则可以把文件传输这样的任务分成 3 件事（或模块）来做。通信模块要保证激活和使参与通信的两个计算机系统处于准备好状态，并跟踪数据的交换且保证送达。这些任务被剥离出来，放到了另一个分立的网络访问模块中。这样，倘若使用网络更替时，所影响的只是网络访问模块。不用一个模块来完成通信任务，而用一个构造好的模块集合来完成不同的通信功能，这就是协议体系结构的思想。本节提供的是一个简化的协议体系结构的例子，为将来引入现实世界中使用的更为复杂的 TCP/IP 和 OSI 体系结构作铺垫。

1.1.4　OSI 体系结构

开放式系统互联模型（OSI）是作为计算机通信体系结构的模型由国际标准化组织（ISO）制订并构架的开发协议标准。

OIS 模型由应用层、表示层、会话层、传输层、网络层、数据链路层和物理层 7 个层次构成，其意图是每层次上的功能都由若干个协议实现。OIS 的设计者试图用这个模型并在这个模型的框架内开发协议以最终代替类似 TCP/IP 的协议及模型，并取得计算机通信方面的

主导地位。尽管在 OIS 的框架内开发了很多有用的协议，但全面的 7 层模型并没有真正流行起来，而 TCP/IP 体系结构在现实的网络世界中仍占据着支配地位。

OIS 模型各层次的功能如下所述。

物理层：保证无特定结构的位流在物理介质上的传输；规范物理介质访问的机械、电气、功能和过程特性。

数据链路：为穿越物理链路的信息提供可靠的传输手段，为数据（帧）块发送提供必要的同步、差错控制和流量控制。

网络层：为更高层次提供独立于数据传输和交换技术的系统连接，并负责建立、维持和结束连接。

传输层：提供可靠和透明的端点间的数据传输，并提供端点间的错误校正和流量控制。

会话层：为应用程序间和通信提供控制结构，包括建立、管理及终止连接（任务）。

表示层：提供应用进程在数据表示（语法）差异上的独立性。

应用层：提供给用户对 OSI 环境的访问和分布式信息服务。

1.2　网络设备及工作原理

在这一节里，将从网络工程应用的角度，介绍常用的网络设备及工作原理。

1.2.1　网络适配器

网络适配器（Network Interface Card，NIC）简称为网卡，是插在计算机总线插槽内或某个外部接口上的扩展卡。它与网络程序（网络操作系统）配合工作，控制网络上信息的发送与接收。网卡上一般有一个或多个网络接口，用来连接网络传输介质。根据网络介质访问方法，网卡可以分以太（Ethernet）、令牌环（Token Ring）、光纤分布式接口（FDDI）和异步传输方式（ATM）等几种。目前国内应用最广泛的是以太网卡，而其他几种网卡只在特殊场合使用。

以太网卡主要包括以下几个部分：

发送和接收部件、载波检测部件、发送和接收控制部件、曼彻斯特编码/译码器、LAN 管理部件及微处理器。但有些网卡没有微处理器。

每块网卡在出厂时都赋予了一个世界范围内的惟一的地址，称为网卡的网络地址（MAC 地址）。所有网卡制造商对网卡地址范围达成协议，每个制造商只能使用许可范围内的地址，这样可保证生产出来的网卡不使用重复的地址。网卡地址是一串 16 进制数，被固化在网卡硬件中。所有可用的网卡地址总数约为 70 亿个。

网卡具有一组配置选项以保证网卡能与计算机中的其他部件协同工作。这些选项主要包括 IRQ（中断请求）、I/O 地址和存储器基地址。

IRQ 是这些参数中最重要的一个参数。其缺省配置一般为 IRQ3、IRQ11 或 IRQ12，在大多数情况下这个值无须改变。

I/O 端口地址用于访问网卡上包含的状态寄存器和控制寄存器，以便使网络终端了解网卡的工作状态和对网卡实施控制。在终端上，除了具有网卡外还有其他外设，因此，在选择 I/O 端口地址时，要避免冲突。一般网卡上都有多个 I/O 端口地址可以供选择使用。当终端需要远程引导启动时，需要在网卡上插一片远程引导 ROM 芯片，这个芯片必须映射到终端

640KB 到 1MB 之间的存储区上。为了实现映射，一要允许网卡进行远程引导，二要规定基地址。这个基地址就是网卡的 ROM 芯片要映射到的存储区的起点地址。

1.2.2 网络集线器

集线器（HUB）是局域网中常用的设备之一。从基本工作原理来看，集线器实质上是一个多端口的中继器，也就是说它工作在 OSI 参考模型的第一层（物理层）。典型的集线器有多个用户端口，用于连接工作站和服务器之类的网络站点。每一个端口支持一个来自网络站点的连接。数据帧从一个站点发送到集线器的某个端口上，然后它就被中继到集线器的其他所有端口上。尽管每一个站点是用它自己专用的电缆线连接到集线器的，但基于集线器的网络仍然属于共享介质的局域网络。通俗地说，集线器就是一个将共享介质干线（总线）折叠到铁盒子中的集中连接设备。

按集线器的结构不同，有以下 3 种形式的集线器。

1. 独立型集线器（Standalone HUB）

独立型集线器是带有许多接线端口的单盒子式的产品。这类集线器非常便宜，适用于小型独立的工作小组、部门或办公室，一般可连接 8～24 个工作站。还可以用级联方法串接多个集线器来扩充连接端口数量。

2. 堆叠式集线器（Stackable HUB）

这一类集线器可通过一条高速链路叠加起来使用。这个高速链路实际上用一根特殊电缆将两台集线器的内部总线相连接，因此这种连接在速度上要高于集线器级联方式的连接。在一个堆叠中最多可有 4～10 个集线器，提供上百个连接端口，但它们在逻辑上只相当于单个集线器单元。

3. 模块化集线器（Module HUB）

模块化集线器是以前在大型网络中经常用到的设备，因为它们扩充方便且备有管理模块选件。模块化集线器配有机架或卡箱，带多个插槽，每个插槽可插入一块通信卡（模块），每个通信卡的作用就相当于一个独立型集线器。当通信卡插入机架内卡槽中时，它们就被连接到机架的背板总线上。这样，背板上的两个通信卡口间就可以方便地进行通信。模块化集线器的规格可以为 4～14 个插槽，故网络的规模可以方便地进行扩充。例如，当插入 10 个通信卡（每卡能支持 12 个工作站）时，一个集线器就可以支持 120 个工作站的连接。此外，模块化集线器中也可插入交换机模块、路由器模块、冗余电源模块和管理模块等，使其应用范围更加广泛。传统集线器的速率一般为 10 Mb/s（10 Base-T）。随着 IEEE 802.3u 标准的颁布，速率为 100 Mb/s 的快速以太网技术得到了迅速发展，支持 100 Mb/s 的集线器流行起来了。

1.2.3 交换机

交换机是一种存储转发设备，它和网桥一样都是根据其发送帧中的目标 MAC 地址进行信息帧转发的。但和网桥相比，其转发的传输延时比网桥少很多，几乎和单一局域网的情况相差无几，接近于线速的水平。交换机转发信息有如下所述的 3 种方法。

1．直通方式（Cut-Through）

交换机以直通方式转发信息时，不需要接收整个转发的帧，只需要收到该转发帧最前面的源地址和目的地址部分即可。根据目的地址找到相应的交换机端口，然后直接把该帧引导至该端口。直通方式有两个优点：一是转发速度非常快，比存储转发方式快得多；二是延时一致性很好，无论长帧还是短帧都具有相同的传输延时。直通方式的缺点是在转发信息帧时不进行错误校验，这样，当某些帧已被破坏或有错误时，仍然会无条件地把这些错误帧转发出去。这些无意义的坏帧自然要浪费掉一部分带宽，部分抵消了采用交换机带来的好处。在出错率较高的网络上，不适合采用直通工作方式。另外，直通方式也不能对不同速率的端口进行转发，如从速率为 100 Mb/s 的高速端口向 10 Mb/s 的低速端口转发信息时，就必须对帧进行缓冲存储，否则低速端口将来不及处理从高速端口送来的信息，造成缓冲溢出错误。

2．无碎片直通方式（Fragment-free Cut Through）

根据以太网帧的结构可知，一个正常的帧其长度至少是 64 个字节，小于 64 个字节的帧（称为碎片）肯定是错误的帧。为了既拥有直通方式快速的优点，又使小于 64 字节的错误帧不再转发，可以让交换机在转发数据前，不仅接收 MAC 地址，还必须满足收到帧的前 64 个字节后判断该帧是否满足最小帧长度的要求。这种转发方式称为无碎片直通方式。无碎片直通方式可以在不显著增加延迟时间的前提下降低错误帧转发的概率，这在某些场合下是有一定实用价值的。

3．存储转发方式（Store-and-Forward）

存储转发方式与以上两种转发方式相反，它首先要把整个信息帧全部读入到内部缓冲区中，并对信息帧进行错误校验，一旦发现错误，就立即通知源发送站重新发送上述信息帧。因此，错误信息帧可立即被发现，并且一旦发现就立即纠正，而不必等目的站点收到该信息帧后再纠正这些错误信息帧。利用存储转发机制，网络管理员还可以定义一些过滤算法来控制通过该交换机的通信流量，这是存储转发方式的另一个优点。另外，存储转发方式允许在不同速率的端口之间进行转发操作，如对于同时拥有 10 Mb/s 端口和 100 Mb/s 端口的交换机。

存储转发方式的缺点在于它的传输延迟较大，并且随转发帧的长短而有所不同；此外由于交换机内的缓冲存储器的大小是有限的，所以当负载较重时，由于缓冲存储器很快会被到达的帧塞满，使后到达的帧不得不扔掉，造成数据帧的丢失。也就是说当负载较重时，其性能会下降。不过现在有的交换机为了解决这个问题，采用了一种称为“背压”（Back Pressure）的控制技术。当交换机内的缓冲存储器快满时，它会自动地向有信息到达的端口发出拥塞信号，造成冲突的假象，使发送站停止发送，从而避免了由于来不及处理而造成的数据包丢失现象。

1.2.4　路由器

路由器是一种多个网络或网段的网络连接设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方的数据，从而构成一个更大的网络。

路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、背板转发以及输出链路调度等，一般由特定的硬件来完成；控制功能一般用软件来实现，实现包括与相邻路由器之间的信息交换、系统配置及系统管理等功能。

路由器是一种典型的网络层设备。它完成两个局域网之间的数据传输。在 OSI/RM 之中它被称之为中介系统，完成网络层中继或第 3 层中继的任务。路由器负责在两个局域网的网络层之间的传输数据，转发帧时需要改变帧中的地址。路由器（Router）用于连接多个逻辑上分开的网络。逻辑网络代表一个单独的网络或者一个子网。当数据从一个子网传输到另一个子网时，可通过路由器来完成。因此，路由器具有判断网络地址和选择路径的功能。它能在多网络互联环境中，建立灵活的连接；可用完全不同的数据分组和介质访问方法连接各种子网。路由器只接受源站或其他路由器的信息，是属网络层的一种互联设备。它不关心各子网使用的硬件设备，但要求运行与网络层协议相一致的软件。路由器分本地路由器和远程路由器。本地路由器是用来连接网络传输介质的，如光缆、同轴电缆和双绞线；远程路由器用来连接远程传输介质，并要求相应的设备，如电话线应配置调制解调器，对于无线通信要具备无线接收机和发射机。

一般来说，异种网络互联与多个子网互联都应采用路由器来完成。

路由器的主要工作就是为经过路由器的每个数据帧寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路径表（Routing Table），供路由选择时使用。路径表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路径表可以是由系统管理员固定设置好的，也可以由系统动态修改，可以由路由器自动调整，也可以由主机控制。下面对此再做一些说明。

1．静态路径表

由系统管理员事先设置好的固定路径表称之为静态路径表。它一般是在系统安装时就根据网络的配置情况预先设定的，不会随未来网络结构的改变而改变。

2．动态路径表

动态路径表是路由器根据网络系统的运行情况而自动调整的路径表。路由器根据路由选择协议提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

1.2.5　拨号设备

拨号设备主要有如下一些，并对它们分别加以介绍。

1．调制解调器（MODEM）

在计算机的远程通信中，一般都利用现有的庞大而成熟的公用电话网。目前的电话入户信号基本上都是模拟信号，而计算机所处理和传输的信息都是数字化的，因此计算机入网通信时必须有能将数字信号转换为模拟信号及把模拟信号转换成数字信号的转换装置。前者完成调制功能，后者完成解调功能，把两种功能做在同一台设备上，该设备就叫调制解调器，即 MODEM。

MODEM 在核心结构上主要由处理器和“数据泵”组成。处理器负责 MODEM 的指令控制，“数据泵”负责 MODEM 的底层算法。如果 MODEM 的处理器和“数据泵”全部在卡上实现，这种 MODEM 卡便是通常所说的“硬猫”。它最主要的特点是不使用计算机主机的资源，可以在 DOS 下使用。

在传统 MODEM 的内部，有两个独立的功能模块。一个是负责模拟/数字信号处理的信

号处理模块，而另一块是用于数据流控制的控制模块。MODEM 的控制模块负责提供 MODEM 必需的通信协议、差错控制、维持连接以及数据压缩等功能。在硬 MODEM 中，这些功能被固化到 MODEM 的控制芯片中。

软 MODEM 利用电脑 CPU 强大的运算能力，用软件来代替硬 MODEM 控制模块的功能。这么做的首要目的是省掉 MODEM 的控制芯片及相关电路，从而降低制造成本；另一个目的是可更高效地利用系统资源。由于减少了 MODEM 卡上的电子元件，所以软 MODEM 还能节约能源和减少发热量（这一点对便携式电脑来说意义很大）。当然 MODEM 本身的信号处理模块是无法用软件代替的。

另外一种 MODEM 是介于以上两者之间的一种半软半硬的 MODEM。这种 MODEM 没有处理器，却具有硬的“数据泵”，复杂数据算法在卡上实现，简单的控制命令交给计算机处理。这样既可少占用主机资源，又可节省硬件成本，是一种折衷方案。软 MODEM 必须借助 CPU 来完成对通信数据流的控制，因此，它会占用 CPU。至于软 MODEM 的数据传输速率，一般都略低于硬 MODEM，但差距并不太明显。

现在还有一种带 AMR 接口的 MODEM，AMR（Audio/MODEM Riser，音频/调制解调器插卡）采用开放工业标准，它定义的扩展卡可同时支持音频和 MODEM 功能。采用这种设计，可有效地降低成本，同时解决主板集成声音与 MODEM 子系统在功能上的一些限制，并通过附加的解码器可以实现软件音频功能和软件调制解调器功能。由于存在电磁干扰以及另一些不利的因素，MODEM 最重要的模拟 I/O 电路（编码器/译码器和 DAA）暂时还不能直接做到主板上。Intel 公司之所以制订这套 AMR 规则，很重要的一个目的就是为解决这个问题，即将模拟 I/O 电路转移到单独的插卡中，其他部件则留在主板上。

2. ISDN

CCITT 对 ISDN 是这样定义的：ISDN 是以综合数字电话网（IDN）为基础发展演变而成的多种电信业务，用户能够通过有限的一组标准化的多用途用户-网络接口接入网内。

ISDN 是在 IDN 基础上发展而成的。采用数字交换和数字传输（PCM）技术的电信网，简称为 IDN。在 IDN 中，以数字信号形式和时分复用方式进行通信。数据等数字信号可以直接在数字网中传输，而话音和图像等模拟信号则必须在发送端进行模拟/数字变换之后进行传输，在接收端要进行数字/模拟的反变换后才能完成通信。脉冲编码调制（ PCM）系统和程控交换设备的广泛应用为 ISDN 的发展打下了基础。综合数字网的通路的传输速率是基于 64 Kb/s 的，而 ISDN 正是使用 64 Kb/s 的传输速率，为用户提供端到端的数字连接。

ISDN 与其他网络的最大不同在于它能够提供端到端的数字连接。所谓端到端的数字连接，指从一个用户终端到另一个用户终端之间的传输全部是数字化的，包括用户线部分。但传统的电话网中，从用户终端到交换机之间的传输是采用模拟方式的，当用户进行数字通信时必须利用调制解调器（MODEM）进行数字/模拟变换后才能在用户线上传送；同时在对方一端还需要通过 MODEM 进行信号的反变换。ISDN 改变了传统的电信网模拟环路的状态，使全网数字化变为现实，从而使用户可以获得数字化的优异性能。

ISDN 支持范围广泛的各类业务，不仅可以提供话音业务而且还提供数据、图像和传真等的各种非话音业务。还可以在用户需要通信时提供即时连接，而且能提供专线连接。

ISDN 能够提供标准的用户-网络接口，这是 ISDN 能获得发展的技术关键所在。它可以通过标准接口，将各类不同的终端纳入到 ISDN 网络中，使一对普遍的用户线最多连接 8 个

终端，并为多个终端提供多种通信的综合服务。

ISDN 具有综合通信业务，提供呼叫速度快，传输质量高，使用灵活方便和费用适宜等优良服务。

3. ADSL

ADSL 的全称是 Asymmetric Digital Subscriber Line，中文意思是“非对称数字用户线路”。它是 DSL（Digital Subscriber Line，即数字用户线路，是以铜质电话线为传输介质的传输技术组合）技术的一种。它以现有普通电话线为传输介质，能够在普通电话线，即铜双绞线上提供高达 8 Mb/s 的高速下行速率，远高于 ISDN 速率；而且上行速率为 1 Mb/s，传输距离则达到 3000 m ~ 5000 m。因此只要在线路两端加装 ADSL 设备即可使用 ADSL 提供的高带宽服务。通过一条电话线，便可以比使用普通 MODEM 快 100 倍的速度浏览因特网。通过网络可进行学习、娱乐、购物，更可享受到网上视频会议、视频点播、网上音乐、网上电视及网上 MTV 的乐趣，还可以很高的速率下载文件。

ADSL 的另外一个优点在于它可以与普通电话共存于一条电话线上，在一条普通电话线上接听或拨打电话的同时进行 ADSL 传输而又互不影响。用户通过 ADSL 接入宽带多媒体信息网与因特网，可以同时收看影视节目，举行一个视频会议，还可以很高的速率下载数据文件。而且，安装 ADSL 也极其方便快捷，可以在同一条电话线上使用电话而又不影响以上所说的其他活动。安装 ADSL 也极其方便快捷，在现有的电话线上安装 ADSL，除了在用户端安装 ADSL 通信终端外，不用对现有线路做任何改动。

1.3 网络应用协议简介

网络中不同的工作站与服务器之间能传输数据，源于协议的存在。随着网络的发展，不同的开发商开发了不同的通信方式。为了使通信成功可靠，网络中的所有主机都必须使用同一“语言”，不能带有“方言”。因而必须开发严格的标准，定义主机之间的每个数据包中的每个字的每一位。目前，局域网中最常见的 3 个协议是 Microsoft 的 NETBEUI、Novell 的 IPX/SPX 和交叉平台 TCP/IP。

1. NETBEUI

NETBEUI 是为 IBM 开发的非路由协议，用于携带 NETBIOS 通信。NETBEUI 缺乏路由和网络层寻址功能，这既是其最大的缺点，也是其最大的优点。因为它不需要附加网络地址和网络层头尾，所以它可以很快并很有效地适用于只有单个网络或整个环境都桥接起来的小工作组环境。

因为不支持路由，所以 NETBEUI 永远不会成为企业网络的主要协议。NETBEUI 帧中惟一的地址是数据链路层媒体访问控制（MAC）地址，该地址标识了网卡但没有标识网络。路由器靠网络地址将帧转发到最终目的地，而 NETBEUI 帧完全缺乏该信息。

网桥负责按照数据链路层地址在网络之间转发通信，但这种方法有很多缺点。因为所有的广播通信都必须转发到每个网络中，所以网桥的扩展性不好。NETBEUI 特别包括了广播通信的计数并依赖它解决命名冲突。一般而言，桥接 NETBEUI 网络中的主机很少有超过 100 台的。

近年来依赖于第二层交换器的网络变得更为普遍。完全的转换环境降低了网络的利用率，尽管广播仍然转发到网络中的每台主机。事实上，联合使用 100-BASE-T 的以太网，允许转换 NETBIOS 网络扩展到 350 台主机时，才能避免广播通信成为严重的问题。

2．IPX/SPX

IPX/SPX 是 Novell 公司用于 NetWare 客户机/服务器的协议群组，避免了 NETBEUI 的弱点。但是，带来了新的弱点。

IPX/SPX 具有完全的路由能力，可用于大型企业网。它包括 32 位网络地址，在单个环境中允许有许多路由网络。

IPX/SPX 的可扩展性受到其高层广播通信和高开销的限制。服务广告协议（Service Advertising Protocol，SAP）将路由网络中的主机数限制为几千台。尽管 SAP 的局限性已经被智能路由器和服务器配置所克服，但是，大规模 IPX 网络的管理员的工作仍是非常困难的。

3．TCP/IP

每种网络协议都有自己的优点，但是只有 TCP/IP 允许与 Internet 完全的连接。TCP/IP 是在 20 世纪 60 年代由麻省理工学院和一些商业组织为美国国防部开发的。即便遭到核攻击而破坏了大部分网络，TCP/IP 仍然能够维持有效的通信。ARPANET 就是基于 TCP/IP 协议开发的，并发展成为作为科学家和工程师交流的媒体——因特网。

TCP/IP 同时满足了可扩展性和可靠性的需求。遗憾的是，它牺牲了速度和效率（可是，TCP/IP 的开发受到了政府的资助）。

因特网公用化以后，人们开始发现全球网的强大功能。因特网的普遍性是 TCP/IP 至今仍然使用的原因。常常在没有意识到的情况下，用户就在自己的 PC 上安装了 TCP/IP 栈，从而使该网络协议在全球广泛应用。

TCP/IP 的 32 位寻址功能方案不足以支持即将加入因特网的主机和网络数，因而又出现了可能代替当前标准的协议——IPv6。

1.4　TCP/IP 协议分析

TCP/IP 起源于 20 世纪 60 年代末，是美国政府资助的一个分组交换网络研究项目，现在已发展成为计算机之间最常用的网络协议。它是一个真正的开放系统，因为协议组件的定义及其多种实现可以不用花钱或花很少的钱就可以公开地得到。它已成为被称做“全球互联网”或“因特网”（Internet）的基础。

本节主要对 TCP/IP 协议组件进行概述，其目的是为本书其余章节提供充分的背景知识。

1.4.1　分层

网络协议通常分不同层次进行开发，每一层分别负责不同的通信功能。一个协议组件，比如 TCP/IP，是一组不同层次上的多个协议的组合。TCP/IP 通常被认为是一个 4 层协议系统，每一层负责不同的功能。