高等学校计算机网络工程专业规划教材

Windows 网络程序设计

夏靖波　杜华桦　王晓东　段弢　编著

西安电子科技大学出版社
http:// www.xduph. com

高等学校计算机网络工程专业规划教材

Windows 网络程序设计

夏靖波　杜华桦
王晓东　段　弢　编著

西安电子科技大学出版社

2006

内 容 简 介

随着网络的日趋复杂和规模的日趋庞大，网络编程技术已成为计算机网络技术的重要分支之一。本书简洁而系统地介绍了网络编程的基本概念、基本知识和编程技术，主要内容包括TCP/IP网络基础知识、基于NetBIOS的网络编程、WinSock基础、基于WinSock的一些网络应用、直接网络编程和高级网络编程等。本书采用理论与实际相结合的方法进行编写，在介绍各种理论知识的基础上及时引入相对应的应用程序，以加深读者对理论知识的理解。各章均附有适量习题，供读者练习和思考。另外，本书给出的附录包括NetBIOS命令和命令返回值、WinSock 1.1和WinSock 2函数、WinSock错误代码表和Tracert程序示例等，方便读者进行查询和进一步研究。

本书可作为高校计算机网络工程专业及相关专业研究生或本科生的教材，也可作为计算机网络和数据通信领域工程技术人员的参考书。

★本书配有电子教案，需要者可与出版社联系，免费提供。

图书在版编目（CIP）数据

Windows网络程序设计 / 夏靖波等编著. —西安：西安电子科技大学出版社，2006.2

高等学校计算机网络工程专业规划教材

ISBN 7-5606-1621-6

Ⅰ.W… Ⅱ.夏… Ⅲ.窗口软件，Windows—程序设计—高等学校—教材 Ⅳ.TP316.7

中国版本图书馆CIP数据核字（2005）第155186号

策　　划　云立实　臧延新

责任编辑　雷鸿俊　云立实

出版发行　西安电子科技大学出版社(西安市太白南路2号)

电　　话　(029)88242885　88201467　　邮　编　710071

http://www.xduph.com　　E-mail: xdupfxb@pub.xaonline.com

经　　销　新华书店

印刷单位　西安文化彩印厂

版　　次　2006年2月第1版　2006年2月第1次印刷

开　　本　787毫米×1092毫米　1/16　印张　23

字　　数　541千字

印　　数　1～4000册

定　　价　26.00元

ISBN 7-5606-1621-6/TP・0929

XDUP 1913001-1

出 版 说 明

计算机技术和通信技术的结合形成的全球互联网络已经把人类社会带入了以互联网为中心的信息化时代。目前网络技术日新月异，网络已成为承载信息经济运转的高效平台，但是我国的网络工程专业人才还很缺乏，与IT产业的飞速发展很不适应，不能满足社会各行各业对网络专业人才的需求，因此培养具有计算机技术和网络技术方面的理论基础，具备系统工程和综合能力，能够从事网络规划、网络工程设计、网络维护和管理、网络安全防护等工作的专业技术人才成为当务之急。许多高校看到了这一趋势，纷纷开设了网络工程专业，但是缺乏能够满足当前教学要求的系列教材。为此，西安电子科技大学出版社聘请了西安交通大学、华南理工大学、西安电子科技大学、西安理工大学、山东科技大学、空军工程大学、杭州电子科技大学、西安邮电学院、成都信息工程学院等九所高校长期在教学科研第一线的专家教授，组成了高等院校计算机网络工程专业教材编审专家委员会，对网络工程专业的教学计划和课程大纲进行了反复研究、充分讨论，通过招标方式筛选并确定了系列书的主编院校及作者，争取在一年的时间里出版并推出整套教材。

由于网络工程专业是各高校新开办的专业，各高校的课程设置和教学要求不尽相同，因此这套教材尽可能系统地覆盖了网络工程专业的主要课程和相关知识，反映网络技术的最新进展和研究成果，在介绍基本理论和基本方法的基础上，特别突出工程实践的重要性和内容的新颖性，重点培养学生从事实际工程的研发能力。在写作风格上，本套教材力求逻辑严谨，语言明快，形式活泼，可读性强。本套教材的作者都是长期从事网络教学的骨干教师，他们较高的学术水平和丰富的教材编写经验是这套丛书顺利出版的保障，在此向他们表示衷心的感谢。

这套经过精心策划和组织的系列教材的出版，不仅是对网络工程专业教学改革的有益探索，而且也积极推动了该专业的教材建设，我们将听取来自各方面的建议，通过不断的改进，使这套教材能够得到各院校的认可并更趋完善。

系列教材编委会

2005年2月

高等学校计算机网络工程专业
教材编审专家委员会

前　言

近年来，由于网络日趋复杂，规模日趋庞大，网络编程技术的需求日趋强烈，本书正是顺应这种需求而编写的。本书内容翔实、实例丰富，并遵循理论与实践相结合的原则，在系统介绍理论的前提下，结合实际工作经验，给出了适量的编程实例，以飨读者。

本书第 1 章是网络基础，主要包括 TCP/IP 的基础知识和网络编程应考虑的问题，介绍网络基础知识，指出网络编程与单机程序设计的不同之处，给读者建立起网络编程的宏观概念。第 2 章是基于 NetBIOS 的网络编程。网络基本输入/输出系统(NetBIOS)是一个应用程序接口(API)，用于数据源与目的地之间的数据交换，为程序提供请求低级网络服务的统一命令集，从而给局域网(LAN)提供网络以及其他特殊功能。在介绍 NetBIOS 的基本概念和编程基础上，设计了基于 NetBIOS 的数据报通信程序和会话通信程序。第 3 章是 WinSock 基础，主要介绍 WinSock 的基本概念、编程原理、I/O 模型，WinSock 2 的扩展特性，套接字选项和 I/O 控制命令。第 4 章是基本网络应用，主要介绍使用较广泛的各种网络应用，如获取主机的名字、域名和 IP 地址，获取子网掩码、网卡的 MAC 地址，获取网络协议信息，模拟 FTP 功能，TCP 实现客户机/服务器聊天功能和 UDP 实现点到点会话功能等。第 5 章是直接网络编程，介绍几种不同的直接网络编程方法，以帮助读者了解网络低层协议的运行状况，并可以通过直接网络编程方法来构造自己的网络高级应用程序。第 6 章是高级网络编程，重点介绍基于微软基本类库(Microsoft Foundation Class Library，MFC)的 WinSock 网络编程和多线程技术，这些技术能够为程序员开发功能更为强大的网络程序提供有力支持。

本书给出的附录包括 NetBIOS 命令和命令返回值、WinSock 1.1 和 WinSock 2 函数、WinSock 错误代码表和 Tracert 程序示例等，以方便读者进行查询和进一步研究。

由于作者的水平有限，书中疏漏之处在所难免，欢迎读者批评指正，并提出宝贵意见和建议，以便不断改进。

编　者

2005 年 11 月

目　录

第1章 网络基础

计算机网络程序设计就是利用网络应用编程接口编写网络应用程序，实现网络应用进程间的信息交互功能。本书主要讨论的是基于 TCP/IP 协议栈的网络编程，即网络应用程序访问 IPv4 协议提供的服务，以实现不同系统上进程间的通信。

网络通信基于网络协议，网络编程接口访问网络协议提供的服务。不同的网络协议提供不同的服务访问接口，同一网络应用编程接口可提供访问不同网络协议的接口。

随着计算机网络的飞速发展和日益普及，网络应用越来越多。业界对计算机网络程序设计的需求也相应增多。因此，计算机网络程序设计作为一种重要的知识技能开始受到人们的重视。要学好网络编程，对于操作系统、网络协议、网络编程模式和方法应有较好的理解。

1.1 TCP/IP 简介

TCP/IP(Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议)是一系列协议，或者说是一个协议族，它定义了数据传输如何通过因特网进行交换。TCP/IP 起源于 20 世纪 60 年代末美国政府资助的一个分组交换网络研究项目，到 20 世纪 90 年代发展成为计算机之间最常应用的组网协议。它允许分布在各地的装着完全不同系统的计算机互相通信，是一个真正的开放系统。TCP/IP 是根据两个最常用的协议命名的，已经实际应用了许多年，并已在世界范围内证明了它的有效性。随着 PC 的普及，TCP/IP 以其开放性的特点，成为了 Internet(因特网)的基础。

1.1.1 OSI 模型与 TCP/IP 结构

OSI/RM(Open System Interconnection/Reference Model，开放系统互连参考模型)将计算机网络通信定义为一个七层框架模型，如图 1.1 所示。

图 1.1 OSI 模型与通信流程

OSI 模型把计算机网络通信的组织与实现按功能划分为七个层次，即从一个计算机系统发出通信请求起，到信息经过实际物理线路传送到另一个目标计算机系统为止，把通信功能从高到低划分为应用层、表示层、会话层、传输层、网络层、数据链路层和物理层，各层的具体功能如表 1.1 所示。每一层协议建立在它的下层协议的基础上，并为其上层提供服务。对于它的上层协议来说，该层是透明的。一台计算机的某指定层同另一台计算机的相应层对话，对话的全部规则和约定就构成该层的协议。当然，信息(数据和控制信息)并不是从某一计算机系统的第 N 层直接传到另一计算机系统的第 N 层，而是从这台计算机的某一层直接传送至下层，最后经过物理介质到达另一台计算机，然后再由底层逐层向上传送，如图 1.1 所示。

表 1.1　OSI 模型中各个层的功能

名称	层次	功　能
物理层	1	实现计算机系统与网络间的物理连接
数据链路层	2	进行数据打包与解包，形成信息帧
网络层	3	提供数据通过的路由
传输层	4	提供传输顺序与相应信息
会话层	5	建立和中止连接
表示层	6	数据转换，确认数据格式
应用层	7	提供用户程序接口

当然，OSI 模型只是一个框架，它的每一层并不执行某种功能，功能的具体实现还需通信协议，主要通过软件来进行。当数据在层间向下传播时(源主机部分)，每一层都会为传输中的数据增加一个包头(header)，用于标识包的来源与目的。到了目标主机时，每一层都从数据中读取相应包头，执行请求的任务，并负责向上传输数据包。每一种具体的协议一般都定义了 OSI 模型中的各个层次具体实现的技术要求。

TCP/IP 是一个四层的协议模型，它的结构及与 OSI 模型之间的关系如图 1.2 所示。

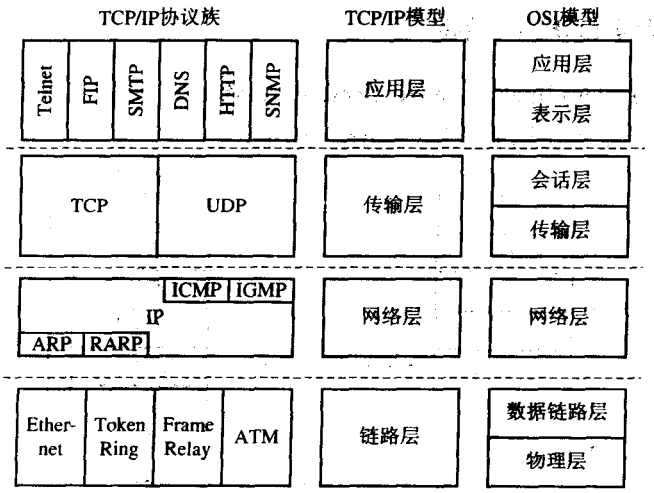

图 1.2　TCP/IP 族的体系结构

每一层负责的功能如下：

- 链路层：有时被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。
- 网络层：有时也被称为互联网层，负责分组在网络中的活动，包括 IP(网际协议)、ICMP(Internet 控制报文协议)以及 IGMP(Internet 组管理协议)。
- 传输层：该层主要为两台主机上的应用程序提供端到端的数据通信，它分为两个不同的协议——TCP(传输控制协议)和 UDP(用户数据报协议)。TCP 提供端到端的质量保证的数据传输，该层负责数据的分组、质量控制和超时重发等，对于应用层来说，就可以忽略这些工作。UDP 则只负责简单地把数据报从一端发送到另一端，至于数据是否到达或按时到达、数据是否损坏都必须由应用层来做。这两种协议各有用途，前者可用于面向连接的应用，而后者则在及时性服务中有着重要的用途，如网络多媒体通信等。
- 应用层：该层负责处理实际的应用程序细节，包括 Telnet、HTTP、SMTP、FTP、DNS 和 SNMP 等协议和应用。

图 1.3 是 TCP/IP 的四层结构的一个具体示例。

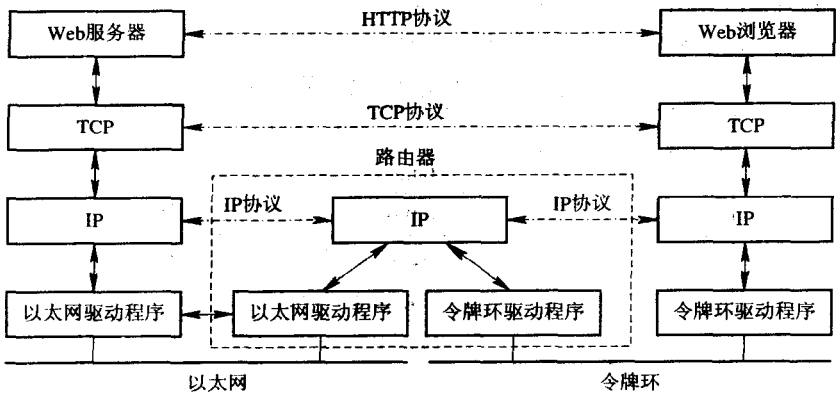

图 1.3　通过 TCP/IP 和路由器连接的两台主机

在图 1.3 所示的系统中，两台主机通过路由器互相连接。路由器可以把以太网、令牌点对点链接和 FDDI(光纤分布式数据接口)等不同的网络连接在一起。协议中的各层对上一层是透明的，也就是说，应用层只负责应用程序之间的通信规则，不必了解数据如何在网络中传输，也不必了解怎样接入网络。而链路层只需要负责传输，而不需要知道正在传送的是什么数据。

1.1.2　TCP/IP 基本概念

作为一个整体的结构体系，TCP/IP 必然要涉及到一系列基本但非常重要的概念，本节主要简要介绍 IP 地址、地址解析及端口号等基本概念。

1. IP 地址与子网掩码

网络互联的目的是提供一个无缝的通信系统。为此，必须用互联网协议屏蔽物理网络的具体细节，并提供一个虚拟网络的功能。在 TCP/IP 栈中，编址由 IP 协议规定，IP 标准

分配给每台主机一个 32 位的二进制数作为该主机的 IP 地址。在最新出台的 IPv6 中 IP 地址升至 128 位，这样 IP 资源就变得更加丰富了。

每个 IP 地址被分割成前缀和后缀两部分。前缀用于确定计算机从属的物理网络，后缀则用于确定网络上一台单独的计算机。互联网中每一个物理网络都有一个唯一的值作为网络号(Network Number)。IP 地址的层次性保证了以下两个重要性质：

- 每台计算机分配一个唯一的地址。
- 网络号的分配全球统一，但后缀可本地分配，无须全球统一。

IP 地址共分五类：A 类、B 类、C 类、D 类和 E 类。其中 A 类、B 类和 C 类为基本类；D 类用于多播传送；E 类属于保留类，现在不用。它们的格式如下(其中*代表网络号位数)：

A 类：0 ******* ×××××××× ×××××××× ××××××××
B 类：10 ****** ******** ×××××××× ××××××××
C 类：110 ***** ******** ******** ××××××××
D 类：1110 ×××× ×××××××× ×××××××× ××××××××
E 类：1111 ×××× ×××××××× ×××××××× ××××××××

IP 地址一般采用点分十进制的表示方法，例如：

10000001 00110100 00000110 00000000→129.52.6.0

采用点分十进制表示方法后的地址分类如表 1.2 所示。

表 1.2 各类 IP 地址的范围

类 型	范 围
A 类	0.0.0.0～127.255.255.255
B 类	128.0.0.0～191.255.255.255
C 类	192.0.0.0～223.255.255.255
D 类	224.0.0.0～239.255.255.255
E 类	240.0.0.0～247.255.255.255

此外，需要特别注意以下几个特殊的 IP 地址：

- 网络地址：IP 中主机地址为 0 的地址表示网络地址，如 128.211.0.0。
- 广播地址：网络号后跟一个所有位全是 1 的后缀，就是直接广播地址。
- 回送地址：127.0.0.1 用于测试。

除了给每台主机分配一个 IP 地址外，IP 协议规定也应给路由器分配一个 IP 地址。事实上，每个路由器被分配了两个或更多的 IP 地址。一个路由器连接到多个物理网络，每一个 IP 地址包含一个特定物理网络的网络号。一个 IP 地址并不标识一台特定的计算机，而是标识一台计算机和一个网络间的连接。

现在所有的主机都要求支持子网编址(RFC950，J.Mogul and J.Postel，1985)，该功能要求不仅把 IP 地址看成由单纯的一个网络号和一个主机号组成，而且要把主机号再分成一个子网号和一个主机号。这样做的原因是因为 A 类和 B 类地址为主机号分配了太多的空间，可分别容纳的主机数为 $2^{24}-2$ 和 $2^{16}-2$。但是，事实上在一个网络中并不会有这么多的主机，因此在 InterNIC 获得某个 IP 网络号后，就由系统管理员来进行分配，由他来决定是否建立子网，以及分配多少位给子网号和主机号。例如，这里有一个 B 类网络地址

(140.252.0.0)，在剩下的 16 位中，8 位用于子网号，8 位用于主机号，其格式如图 1.4 所示。这样就允许有 254 个子网，每个子网可以有 254 台主机。

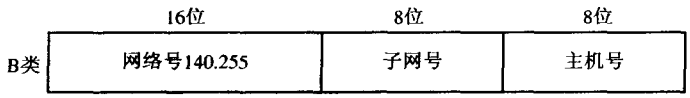

图 1.4　B 类地址的子网编址举例

除了地址以外，主机还需要知道有多少位用于子网号及多少位用于主机号。这是在引导过程中通过子网掩码来确定的。这个掩码是一个 32 位的值，其中值为 1 的位留给网络号和子网号，为 0 的位留给主机号。在上面的例子中，子网掩码就是 255.255.255.0。

2. 地址解析

地址解析(Address Resolution)就是将计算机中的协议地址翻译成物理地址(或称 MAC 地址，即媒体映射地址)。地址解析只能在本地网内进行。

地址解析技术可分为如下三种：

(1) 表查询(Table-Lookup)。该方法适用于广域网(WAN)，通过建立映射数组(协议地址↔物理地址)的方法解决。用户可通过查询找到物理地址。

(2) 相近形式计算(Close Form-Computation)。该方法适用于可以自行配置的网络，IP 地址和物理地址相互对应，例如：

220.123.5.1→ XXX1

220.123.5.2→ XXX2

可通过这种算法得到物理地址：物理地址＝协议地址&0xFF。

(3) 信息交换(Message-Exchange)。该方式适用于 LAN，是基于分布式的处理方式，即主机发送一个解析请求，以广播的形式发出，并等待网络内各个主机的响应。

3. 域名系统

一个系统的全域名由主机名、域名和扩展名三部分组成，各部分间使用“.”分隔，例如 www.sina.com。在 TCP/IP 应用中，域名系统(DNS)是一个分布的数据库，由它来提供 IP 地址和主机名之间的映射信息，可以通过在程序中调用标准库函数来编程实现域名与 IP 地址之间的相互转换。通过从域名地址到 IP 地址的映射，使得在日常的网络应用中可以使用域名这种便于记忆的网络地址表示形式。

所有的网络应用程序理论上都应该具有内嵌的域名解析机制。

4. 数据包的封装和分用

当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐个通过每一层，直到被当作一串比特流送入网络。其中每一层对收到的数据都要增加一些首部信息(有时还要增加尾部信息)，该过程如图 1.5 所示。TCP 传给 IP 的数据单元称作 TCP 报文段或简称 TCP 段。IP 传给网络接口层的数据单元称作 IP 数据报(IP Datagram)。通过以太网传输的比特流称作帧(Frame)。图 1.5 中帧头和帧尾下面所标注的数字是典型以太网帧首部的字节长度。以太网数据帧的长度必须在 46～1518 字节之间。

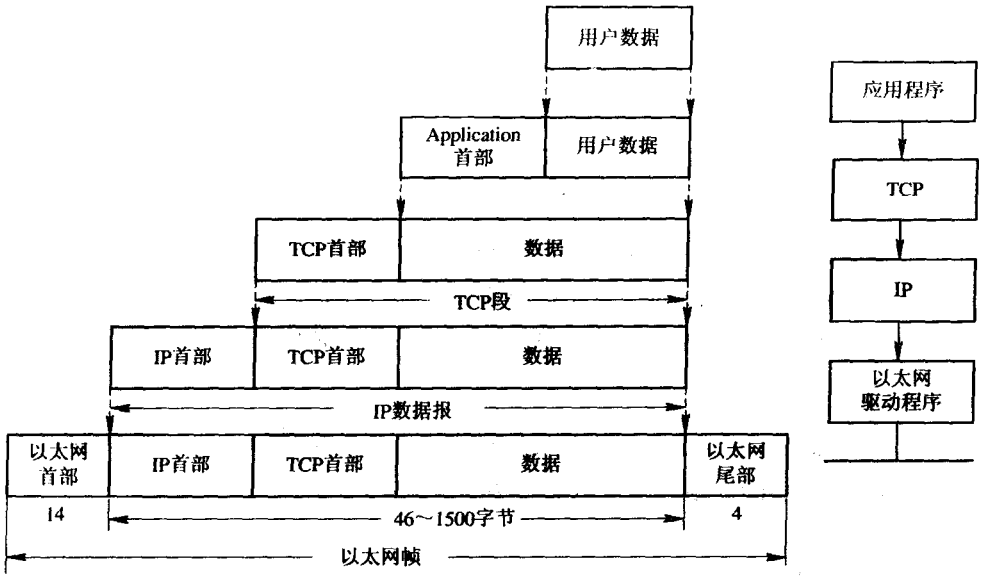

图 1.5　数据包的封装过程示意图

由于 IP 数据报通常是分组传输的，因此更准确地说，图 1.5 中 IP 和网络接口层之间传送的数据单元应该是分组(Packet)。分组既可以是一个完整的 IP 数据报，也可以是 IP 数据报的一个片(Fragment)。关于分组的细节算法不在本书的讨论范围之内。

UDP 数据与 TCP 数据基本一致。唯一不同的是，UDP 传给 IP 的信息单元称作 UDP 数据报(UDP Datagram)，而且 UDP 的首部长为 8 字节。由于 TCP、UDP、ICMP 和 IGMP 都要向 IP 传送数据，因此 IP 必须在生成的 IP 首部中加入某种标识，以表明数据属于哪一层。为此，IP 在首部中存入一个长度为 8 bit 的数据，称作协议域。1 表示 ICMP，2 表示 IGMP，6 表示 TCP，17 表示 UDP。

同样，许多应用程序都可以使用 TCP 或 UDP 来传送数据。传输层协议在生成报文首部时要存入一个应用程序的标识符。TCP 和 UDP 都用一个 16 位的端口号来表示不同的应用程序。TCP 和 UDP 把源端口号和目的端口号分别存入报文首部中。

网络接口分别要发送和接收 IP、ARP 和 RARP 数据，因此也必须在以太网的帧首部中加入某种形式的标识，以指明生成数据的网络层协议。为此，以太网的帧首部也有一个 16 bit 的帧类型域。

当目的主机收到一个以太网数据帧时，数据就开始从协议栈中由底向上升，同时去掉各层协议加上的报文首部。每层协议盒都要去检查报文首部中的协议标识，以确定接收数据的上层协议。这个过程称作分用(Demultiplexing)，图 1.6 显示了该过程。

图 1.6 中把 ARP 和 RARP 放在 IP 层是因为它们都有以太网头部和尾部，而在前面的论述中把它们作为链路层的协议，这并不矛盾，因为 TCP/IP 栈的层次划分本来就不是非常清晰。

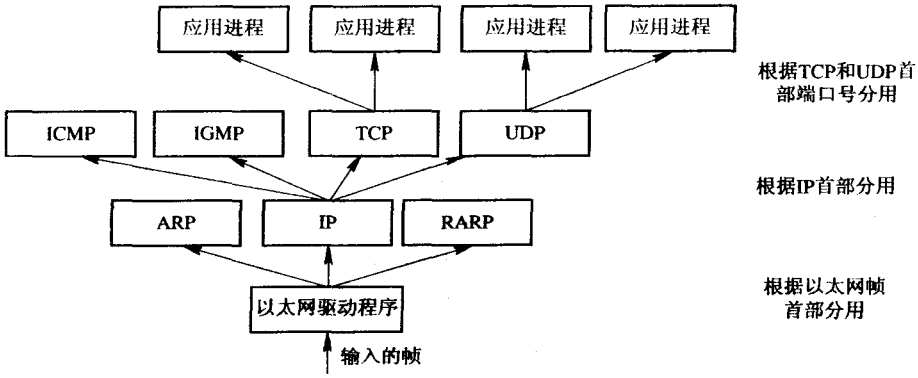

图 1.6　数据分用过程

5. 端口号

TCP 和 UDP 采用端口号来识别应用程序。例如，服务器提供的服务一般都是通过通用端口号来识别的，对于 TCP/IP 实现来说，FTP 服务器的 TCP 端口号都是 21，Telnet 服务器的 TCP 端口号都是 23，TFTP(简单文件传送协议)服务器的 UDP 端口号都是 69。任何 TCP/IP 实现所提供的服务都使用通用端口号 1～1023。这些通用端口号由 Internet 号分配机构(Internet Assigned Numbers Authority, IANA)来管理。

客户端通常对它所使用的端口号并不关心，只需保证该端口号在本机上是唯一的就可以了。客户端口号又称作临时端口号(即存在时间很短暂)，这是因为它通常只是在用户运行该客户程序时才存在，而服务器则只要主机是开着的，其服务就运行。

大多数 TCP/IP 实现给临时端口分配 1024～5000 之间的端口号。大于 5000 的端口号是为其他服务(Internet 上并不常用的服务)预留的。

1.1.3　常用协议

下面对一些常用协议进行简要的介绍。

1. 以太网数据链路层帧结构

IEEE 802.3 定义了一种具有七个字段的帧(MAC)：前导符、起始帧分界符、目标地址、源地址、PDU 的长度/类型、数据以及 CRC。以太网不提供任何对收到的帧进行确认的机制，确认在高层完成，这表明它是一种不可靠的介质。CSMA/CD 中 MAC 帧的格式如图 1.7 所示。

前导符	起始帧分界符	目标地址	源地址	长度/类型	数据	CRC
7字节	1字节	6字节	6字节	2字节	46～1500字节	4字节

图 1.7　IEEE 802.3 MAC 帧结构

- 前导符(Preamble)：该字段长 7 个字节(56 位)，其中 1 和 0 交替出现，警告接收系统即将有数据帧到来，同时同步系统时序。
- 起始帧分界符(SFD)：该字段长 1 字节，为 10101011，标志帧的开始。SFD 通知接