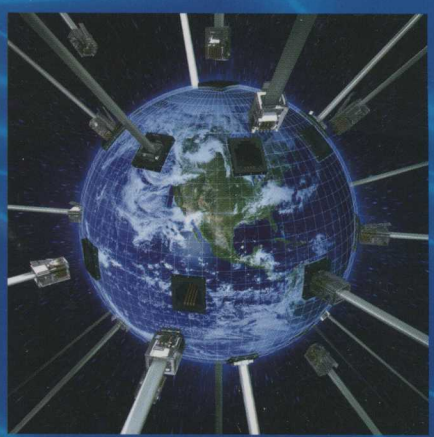
TCP/IP

WANGLUO BIANCHENG
JISHU YU SHILI

TCP/IP 网络编程技术与实例



孙飞显 主编

国防工业出版社
National Defense Industry Press

TCP/IP 网络编程技术与实例

主　编　孙飞显
副主编　靳晓婷　张俊宝　王海龙

国防工业出版社
·北京·

内容简介

本书是在作者总结多年的TCP/IP协议原理与应用课程教案的基础上，结合从事网络安全技术研究与实践教学的经历，按照Internet网络体系结构的从低到高顺序讲述各层的协议及相关的编程技术，并给出了“近似实战”的应用实例的设计方法和实现步骤。本书共10章，其中，第1章在概述TCP/IP协议原理的基础上，讲述了基于TCP/IP的网络通信过程；第2～3章讲解了套接口编程的基础知识，并重点讲述了Winsock编程技术；第4～9章分别讲述了网络接口层、网络层、传输层和应用层的协议原理及相关的编程技术，并给出了“近似实战”的应用实例的设计方法和实现步骤；第10章通过实例，剖析了当前较热的P2P编程技术。

本书可以作为大学本科、大专及高职院校网络工程、计算机科学与技术、软件工程、信息安全等计算机类专业学生的教材，也可作为网络研发人员的参考书。

图书在版编目(CIP)数据

TCP/IP网络编程技术与实例/孙飞显主编. —北京：国防工业出版社，2014.1

ISBN 978-7-118-09095-6

Ⅰ.①T... Ⅱ.①孙... Ⅲ.①计算机网络-通信协议 ②计算机网络-网络编程 Ⅳ.①TN915.04②TP393.09

中国版本图书馆CIP数据核字(2013)第248150号

※

国防工业出版社出版发行

（北京市海淀区紫竹院南路23号 邮政编码100048）

北京奥鑫印刷厂印刷

新华书店经售

*

开本 787×1092 1/16 **印张** 21 **字数** 485千字

2014年1月第1版第1次印刷 **印数** 1—4000册 **定价** 45.00元

（本书如有印装错误，我社负责调换）

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

前　言

随着QQ以及迅雷、网际快车、电驴等网络应用软件的日益普及，社会对计算机网络技术人才的需求越来越强烈。但真正懂得计算机网络技术、会编写网络应用程序、能够深入理解TCP/IP协议并进行高层次的网络应用系统设计和网络软件编程的人才极为匮乏。作者的课程教学改革、课程建设、学生课外科技活动指导等经验表明：仅通过课堂理论教学和课程实验的途径，无法使学生真正掌握TCP/IP协议原理及相关的网络编程技术，学生对TCP/IP协议原理及网络编程知识的理解和实际动手能力的提高是在学习相关理论知识的基础上，通过参加各级别的科技竞赛、科研工作及完成相关开发任务的过程中逐渐锻炼出来的。

在近10年的本科毕业设计指导过程中，作者发现网络工程、计算机科学与技术、软件工程等计算机类专业学生的编程能力不强，甚至基本没有编程能力，特别是缺乏网络编程能力。计算机类毕业生在求职及用人单位在招聘过程中的“毕业生找不到工作，用人单位招不到人”的现象进一步反映了计算机类学生的动手能力差。这充分说明了在计算机网络编程、协议分析、TCP/IP协议原理与应用等课程教学中存在教材不合适、学生软件编程训练不足的问题。

在此背景下，作者总结多年的TCP/IP协议原理与应用课程教案的基础上，借鉴从事网络安全技术研究、理论与实践环节教学、指导大学生课外科技竞赛、毕业设计指导等经验，按照Internet网络体系结构的从低到高顺序讲述TCP/IP协议原理及相关的编程技术，并给出了“近似实战”的应用实例的设计方法和实现步骤。本书共10章，其中，第1章在概述TCP/IP协议原理的基础上，讲述了基于TCP/IP的网络通信过程；第2章在概述网络编程、网络程序的概念后，介绍了常见的网络编程技术，并给出了当今流行的客户机/服务器、浏览器/服务器、P2P等网络程序的体系结构；第3章在讲解套接字含义、分类的基础上，通过实例讲解了流式和用户数据报套接字编程流程，阐述了套接字的两种I/O模型，并详细、重点讲述了Winsock的6种编程模型，为学生学习真实的网络应用系统设计和实现奠定了基础；第4~9章分别讲述了网络接口层、网络层、传输层和应用层的协议原理及相关的编程技术，并给出了“近似实战”的应用实例的设计方法和实现步骤；第10章通过实例，剖析了当前较热的P2P编程技术。

为了方便读者学习本书内容并进行网络编程实战演练，本书的实例在组织结构上都包括设计要求、设计原理和实现步骤三个环节，读者可在实例指定的编程环境下，按照操作步骤逐步模仿练习，并在此基础上学会举一反三。本书提供的PPT课件、程序源代码

等资源，读者可以登录国防工业出版社网站（http://www.ndip.cn）进行免费下载。

感谢路林生、胡战士、郭强、王继轩对本书撰写工作的大力协助，感谢国防工业出版社李宝东编辑在书稿编辑过程中的协助，其敬业精神给我们留下了深刻的印象。

限于编写水平有限，本书错漏之处还望各位专家和读者批评指正。

编著者

2013年8月

目　录

第1章 概 述

1.1 TCP/IP 概述

1.1.1 TCP/IP 简介

传输控制协议/网际协议(Transmission Control Protocol/Internet Protocol，TCP/IP)是目前流行的网络通信协议，它规范了网络上所有通信设备(包括计算机、交换机、路由器、网络打印机，等)之间数据往来的格式以及传送方式，得到了桌面操作系统、服务器操作系统和嵌入式操作系统的全面支持。

TCP/IP 是普遍使用的网络互连标准协议，它使得不同的网络环境、不同操作系统的节点之间的互连互通成为可能，也是接入 Internet 的所有计算机进行信息交换和传输所必须采用的协议，是 Internet 的基础协议。

TCP/IP 协议有别于 TCP/IP 协议族(Protocol Suite)。一般说来，TCP/IP 协议仅包括传输控制协议 TCP 和网际协议 IP，而 TCP/IP 协议族是不同层次上的多个协议的组合，除了包含传输控制协议(TCP)和网际协议(IP)之外，还包括：用户数据报协议(User Datagram Protocol，UDP)、超文本传输协议(Hyper Text Transfer Protocol，HTTP)、远程文件传输协议(File Transfer Protocol，FTP)、远程登录标准协议 Telnet、简单邮件传输协议(Simple Message Transfer Protocol，SMTP)等。

需要说明的是，现在人们经常提到的 TCP/IP 并非一定是指 TCP 和 IP 这两个具体协议，而往往指的是 Internet 的体系结构或者是指整个的 TCP/IP 协议族。

1.1.2 TCP/IP 起源历史

世界上有各种不同类型的计算机，也有不同的操作系统。要想让这些装有不同操作系统、不同类型计算机彼此之间能够互相通信，就必须有统一的标准——TCP/IP，TCP/IP 的起源历史概述如下。

早期的计算机并不像现在的 PC 那样小，它们大都是以中央处理器(CPU)为中心，并用一定线路将终端系统(输入/输出设备)与中央处理器链接在一起的集中式运算系统。这种以中央处理器为核心的集中式计算机模式就是早期的集中式计算机网络，它们各自拥有自己独立的一套规则或约定，彼此之间通信困难。

网络互连促成了 TCP/IP 协议的产生。1969 年，美国政府机构试图建立一套机制，用来链接各个离散的网络系统，以应付战争危机的需求。这个计划就是由美国国防部委托 Advanced Research Project Agency 研发的 ARPAnet 网络系统，其目的就是研究当部分计算机遭受攻击而瘫痪后，网络还能够透过其他未瘫痪的线路来传送资料。ARPAnet 的构想和原理，除了研发出一套可靠的资料通信技术外，还同时要兼顾跨平

台作业能力。ARPAnet 的成功实验，奠定了目前的互连网络模式，它包括了一组计算机通信细节的网络标准，以及一组用来链接网络和选择网络交通路径的协定，这就是目前的 TCP/IP 协议。

1983 年，美国国防部下令用于链接长距离的网络的电话都必须适应 TCP/IP，同时 Defense Communication Agency(DCA)将 ARPAnet 分成两个独立的网络，一个用于研究用途，依然叫 ARPAnet；另一个用于军事通信，则称为 MILNET(Military Network)。ARPA 后来发展出一个便宜版本，以鼓励大学和研究人员来采用它的协定，其时正适逢大部分大学计算机学系的 UNIX 系统需要链接它们的区域网络。由于 UNIX 系统上面研究出来的许多抽象概念与 TCP/IP 的特性有非常高度的吻合，再加上设计上的公开性，而导致其他组织也纷纷使用 TCP/IP 协议。从 1985 年开始，TCP/IP 网络迅速扩展至美国、欧洲好几百个大学、政府机构、研究实验室。它的发展大大超过了人们的预期，而且每年以超过 15%的速度递增，到 1994 年，使用 TCP/IP 协议的计算机已经超过 300 万台之多。其后数年，由于 Internet 的爆炸性成长，TCP/IP 协议已成为无人不知、无人不用的互联网了。

1.2 TCP/IP 协议族的体系结构

网络的体系结构是指计算机网络的层次结构划分和每层所使用协议的集合，为网络中不同计算机之间的互连和互操作提供了相应的规范和标准。与开放系统互联参考模型 OSI/RM 相似，TCP/IP 的体系结构如图 1-1 所示。

图 1-1 TCP/IP 的体系结构

1. 网络接口层

网络接口层是 TCP/IP 体系结构的最低层，对应于 OSI 模型的物理层和数据链路层。网络接口层的功能包括两个方面，一方面是从物理网络上接收数据帧，抽出 IP 数据报并交给网际层 IP；另一方面是将 IP 数据报封装成数据帧，并以比特流的方式发送到网络传输介质上。

网络接口层包括物理和数据链路两个子层，该层的功能由网卡及其驱动程序共同实现，它定义了如何使用实际网络(如 Ethernet、Serial Line 等)来传送数据，处理与电缆(或其他网络传输介质)的物理接口细节，实现对实际网络媒体的管理。

2. 网际层

网际层也叫网络层或 IP 层，是 TCP/IP 体系结构中最重要的一层，它定义了能够标识网络中所有结点的逻辑地址(IP 地址)、路由实现和学习方式；同时，为适应最大传输单元长度小于 IP 数据报长度的传输介质，网际层还规定了 IP 数据报的分片和重组方法。

网际层负责 Internet 节点之间的通信，为数据在结点之间传输创建逻辑链路，并通过路由选择算法为 IP 数据报通过通信子网选择最适当的路径。此外，网际层还能实现流量控制、拥塞控制等功能。

在 TCP/IP 协议族中，网际层协议主要包括 IP 协议、Internet 控制报文协议 ICMP、

Internet 组管理协议 IGMP 等。

3. 运输层

运输层的基本任务是为两台主机上的应用程序提供端到端的通信。运输层管理信息流，提供可靠的传送服务，以确保数据无差错的、按序地到达。它包括面向链接的传输控制协议(TCP)和无链接的用户数据报协议(UDP)。

传输控制协议(TCP)为应用程序提供可靠的通信链接，适用于大批量数据传输并要求得到响应的应用程序。

用户数据报协议(UDP)提供了无链接通信，且不对传送包进行可靠的保证，适用于小量数据传输，可靠性由应用层来负责。

4. 应用层

应用层是 TCP/IP 体系结构的最高层，负责处理特定的应用程序。TCP/IP 协议族中常用的应用层协议包括：超文本传输协议(HTTP)、远程文件传输协议(FTP)、远程登录标准协议(Telnet)、简单邮件传输协议(SMTP)、简单网络管理协议(SNMP)等。

说明：尽管四层结构的 TCP/IP 体系结构模型不像国际标准 ISO 那样得到了法律上的认可，但 TCP/IP 占领了大部分的市场份额，通常被认为是事实上的国际标准。

1.3 基于 TCP/IP 的网络通信过程

互联网上源主机与目标主机的通信是一个非常复杂的过程，从 TCP/IP 体系结构看，源、目主机应用层实体间的对话是通过下层提供的服务实现的。为说明网络程序的基本工作原理，本节在介绍 TCP/IP 通信模型的基础上，通过具体实例阐述基于 TCP/IP 的网络通信过程。

1.3.1 TCP/IP 通信模型

在互联网上，源主机的协议层与目的主机的同层协议通过下层提供的服务实现对话。源主机到目的主机对等实体(Peer Entities)间的对话实际上是在源主机上从上到下然后穿越网络到达目的主机后再从下到上到达相应层。基于 TCP/IP 协议的网络通信模型如图 1-2 所示。

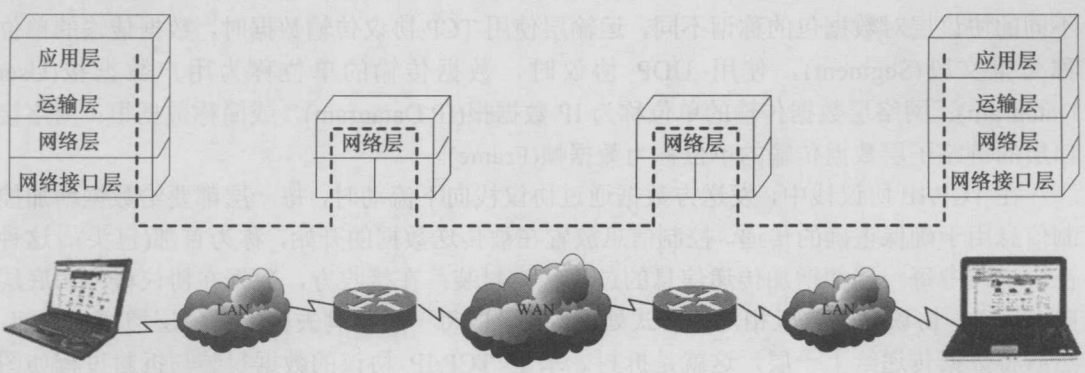


图 1-2 TCP/IP 通信模型

为说明基于 TCP/IP 协议的网络通信的基本原理，现以面向链接的数据发送和接收过程为例，具体实现过程见表 1-1 所列。

表 1-1　面向链接的数据发送和接收过程

序号	源主机		目的主机	
	任务	实现层次	任务	实现层次
(1)	将数据流送给运输层	应用层		
(2)	将数据流截成分组，加上 TCP 报头形成 TCP 段，然后送交网络层	运输层		
(3)	给 TCP 段加上 IP 报头，生成 IP 数据报，并将 IP 数据报送交链路层	网络层		
(4)	给 IP 数据报包加上帧头，形成数据帧，并依据目的 MAC 将数据帧以比特流形式发往目的主机或 IP 路由器	网络接口层		
(5)			将收到的比特流还原成数据帧，去掉帧头，将 IP 数据包送交网络层	网络接口层
(6)			计算校验和，若计算结果与报头校验和一致，则去掉 IP 报头后将 TCP 段送交运输层，否则丢弃该 IP 数据包	网络层
(7)			检查 TCP 报头，若 TCP 分组正确，则向源主机进行确认；否则要求源主机重发	运输层
(8)			去掉 TCP 报头，将排好序的分组形成应用数据流送给应用程序	应用层

1.3.2　数据的封装与拆封

在 Internet 中，数据是以“包”的形式在网络上进行传输。在 TCP/IP 体系结构中，不同的协议层对数据包的称谓不同，运输层使用 TCP 协议传输数据时，数据传输的单位称为报文段(Segment)，使用 UDP 协议时，数据传输的单位称为用户数据报(User Datagram)；网络层数据传输的单位称为 IP 数据报(IP Datagram)，或简称数据报；网络接口层的链路子层数据传输的单位称为数据帧(Frame)。

在 TCP/IP 协议栈中，发送方数据通过协议栈向下流动时，每一层都要给数据增加控制信息用于确保正确的传递。控制信息放置在被传送数据的开始，称为首部(包头)，这种在协议栈中每一层都增加传递信息的过程称为封装；在接收方，数据在协议栈中由底层向上流动，协议软件就以相反的方式处理数据，即每一层都剥去栈中对应层增加的首部，然后将数据传递给上一层，这就是拆封。基于 TCP/IP 协议的数据封装与拆封过程如图 1-3 所示。

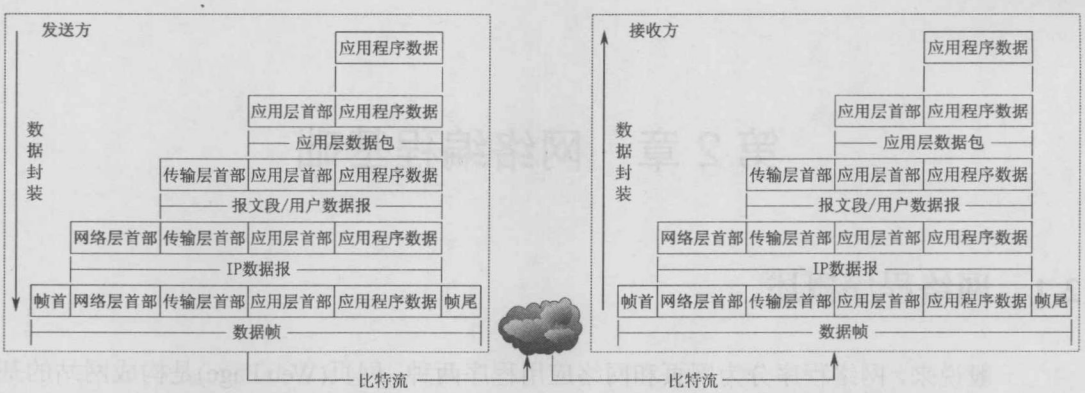


图 1-3　数据的封装与拆封过程

发送方数据的封装过程描述如下。

发送方应用程序首先收集待发送的用户数据，依据既定的应用层协议，加上应用层首部后形成应用层数据包，并发送到运输层。

运输层依据应用程序事先确立的运输层协议类型(TCP 或 UDP)，加上 TCP 头形成 TCP 报文段(或加上 UDP 头形成用户数据报)后发送到网络层。

为屏蔽下层各种物理网络的差异，网络层将 TCP 报文段和用户数据报添加上发送方 IP、接收方 IP 等网络层首部信息，形成 IP 数据报后投递给网络接口层的数据链路子层。

依据物理网络(以太网、令牌环网、X.25 网等)的不同，网络接口层将 IP 数据报封装成实际物理网络需要的数据帧。例如，对 Ethernet 来说，链路层将 IP 数据报封装成以太网帧；对于令牌环网，链路层将 IP 数据报封装成令牌环帧；而对于通过 Modem 接入 Internet 的网来说，链路层将 IP 数据报封装成 SLIP 帧或 PPP 帧格式。数据封装成帧后，发到网络传输介质上。

与此相反，当接收方接收数据时，TCP/IP 协议栈要做和封装相反的工作——拆封。拆封首先是将各种格式的数据帧转换成 IP 数据报，再根据协议号转换成 TCP 报文段或用户数据报，最后通过端口号到达正确的进程，还原成原始数据。

针对上述数据封装和拆封过程，需要说明如下。

(1) 传输层选用的具体协议由应用程序确定，应用程序负责对通信数据含义进行解释，数据从发送方到接收方的选路问题由路由器负责。

(2) 在网络层和数据链路层之间，通常要进行数据包的分割与重组。分割是将单个数据包分成两个或多个小数据包的过程。当应用程序传送的数据包大于网络的 MTV(网络最大传输单元)时，或所经过的路由器其 MTU 小于本地网络发送方的 MTU 时，网络软件自动将数据包分成小块，并当成多个数据包进行传输；重组是在接收方将已分割的数据按正确的顺序合并在一起，重组比分割复杂，它有时间要求，不能无限制的等待。如果在规定的时间内主机未收到全部分块，它就会放弃已收到的分块，并停止处理这个数据包。分块的小数据包重组完成后传送到网络层，此时网络层处理数据包就好像网络从未分割它一样。

第 2 章　网络编程基础

2.1　网络程序概述

一般说来，网络程序分为网页和网络应用程序两种。网页(Web Page)是构成网站的基本元素，是承载各种网站应用的平台，以文件格式(扩展名为.html、.htm、.asp、.aspx、.php、.jsp，等)存放在计算机(多为服务器)，并通过浏览器来阅读。通俗地说，网站就是由网页组成的。网页经由网址、(URL)来识别与存取，当我们在浏览器输入网址后，网页文件会被传送到自己的计算机，然后再通过浏览器解释网页的内容，再展示到自己眼前。ASP、PHP 和 JSP 动态网页可以看成是一个程序或系统，因为里面也包含了复杂的业务逻辑和数据处理和传递，例如，表单形式的注册网页就是将用户填好的注册信息提交服务器进行验证、存储等处理。网络应用程序与网页不同，一般是指带网络接连或需要网络接连才能使用的新型智能程序，例如腾讯 QQ、迅雷等。

网页和网络应用程序的区别：网页是一个个的 Web 页面拼凑起来的，而网络应用程序则是用的窗体和控件来实现数据的采集、传递和处理的。两者的区别还在于网页采用的是 B/S 结构，即需要浏览器和服务器的支持，而网络应用程序大多是 C/S 结构，需要客户端和服务器的支持。二者的相同点是都需要服务器和网络链接，就像大多数的网络游戏一样，须下载客户端并联网后才能够正常工作。

2.2.1　网络编程术语

1. 端口

计算机网络领域所谓的“端口(Port)”大致包含两层含义：一是物理意义上的端口，例如，ADSL Modem、集线器、交换机、路由器等网络设备用于链接其他网络设备的接口，如 RJ-45 端口；二是逻辑意义上的端口，一般是指 TCP/IP 协议中的端口，本书中提及的端口指的是后者。

TCP/IP 协议中的端口是一种抽象的软件结构，包括一些数据结构和 I/O 缓冲区，用于标识通信的进程，并用“IP+Port”的方式来区分不同的服务。网络程序对应的进程通过系统调用的办法与某端口建立链接(Binding)后，传输层传给该端口的数据都被相应的进程所接收，相应进程发给传输层的数据都从该端口输出。在 TCP/IP 协议的实现中，端口操作类似于一般的 I/O 操作，进程获取一个端口，相当于获取本地唯一的 I/O 文件，可以用一般的读写原语访问。

每个端口都拥有一个称为端口号的整数描述符，用于区别不同的端口。由于 TCP/IP 传输层的两个协议 TCP 和 UDP 是两个完全独立的软件模块。因此，TCP 和 UDP 协议的端口号也相互独立。如 TCP 有一个 255 号端口，UDP 也可以有一个 255 号端口，两者并

不冲突。那么，端口号是如何分配的呢？

一般地，计算机网络中的端口号有两种分配方式：全局分配和本地分配。全局分配是集中分配的方式，由公认的中央机构(Internet Assigned Numbers Authority, IANA)统一分配，并将结果公布于众。Windows 操作系统使用且由 IANA 定义的端口信息，详见 Windows 安装文件夹中的 Services 文件(例如，C:\WINDOWS\system32\drivers\etc\services，可用记事本或写字板打开)。端口的本地分配(又称动态链接)是当进程访问传输层服务时，向本地操作系统提出申请，操作系统返回本地唯一的端口号，进程再通过合适的系统调用，将自己和该端口链接起来。

服务器一般都是通过知名端口号来识别的，即任何由 TCP/IP 协议实现并提供的服务都用知名的 1～1023 之间的端口来标识。例如，对于每个 TCP/IP 实现来说，Web 服务器的 TCP 端口号大都是 80，FTP 服务器的 TCP 端口号都是 21，每个 Telnet 服务器的 TCP 端口号都是 23，每个 TFTP(简单文件传送协议)服务器的 UDP 端口号都是 69。

然而，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，因为只是在用户运行该客户程序时端口号才存在。在 TCP/IP 协议中，给临时端口分配的端口号大都在 1024～5000，例如 QQ 客户端使用的端口号为 4000(UDP 端口)。

需要说明的如下：

(1) 大于 5000 的端口号是为其他服务器预留的，例如 QQ 服务器端使用的端口号为 8000(UDP 端口)。

(2) 在 TCP/IP 中，常用的端口、服务及其详细说明，可查阅附录 1。

2. 地址

在计算机网络领域，相互通信的两个进程可以在同一网络主机中，也可分别在两台不同的网络主机上。不难理解，互联网中的两台主机可能位于相距甚远的不同网络内(通过网际互连设备相连)。那么，如何标识通信双方的地址呢？

网络通信双方的地址需要以下三级寻址得到：

某一主机与多个网络相连，必须指定一特定网络地址；

网络上每一台主机应有其唯一的地址(IP 地址)；

每一主机上的每一进程应有在该主机上的唯一标识(端口号)。

网络编程过程中用到的地址结构及其用法详见 3.2.2 节。

3. 字节顺序

计算机网络领域的字节顺序包括两种：主机字节顺序和网络字节顺序。

主机字节顺序是指占内存多于一个字节类型的数据在内存中的存放顺序，通常有小端、大端两种字节顺序。小端字节序(Little Endian，LE)指低字节数据存放在内存低地址处，高字节数据存放在内存高地址处；大端字节序(Big Endian, BE)是高字节数据存放在低地址处，低字节数据存放在高地址处。

例如，在内存中双字 0x01020304(DWORD)的存储方式见表 2-1 所列。