Windows

Windows网络与通信程序设计

王艳平　张　越　编著

- 讲述Windows网络程序设计的入门教程，展示了各种Windows I/O方法，详细说明了高性能可伸缩性服务器的开发过程，并给出详尽的实现代码。
- 将编程方法、网络协议和应用实例有机结合起来，详细介绍了Internet广播和IP多播、原始套接字、SPI、LAN和WAN上的扫描和侦测技术、网络数据的窃取和保护、ARP欺骗、IP欺骗等。
- 详细演示了协议驱动的开发过程，介绍了NDIS编程接口。
- 在编程实践中学习P2P程序设计，讨论了穿透防火墙、NAT等直接建立UDP和TCP连接的各种方案。
- 包含了Windows个人防火墙的完整实例代码，防火墙采用应用层（SPI）/核心层（IMD驱动）双重过滤机制，能够有效地抵挡网络入侵和攻击。
- 提供了大量完整的实例，许多例子稍做修改即可应用到实际项目中。

人民邮电出版社
POSTS & TELECOM PRESS

Windows

Windows网络与通信程序设计

王艳平　张　越　编著

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目（CIP）数据

Windows 网络与通信程序设计 / 王艳平，张越编著. —北京：人民邮电出版社，2006.1
ISBN 7-115-14150-9

Ⅰ. W… Ⅱ. ①王…②张… Ⅲ. 窗口软件，Windows—程序设计 Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字（2005）第 132938 号

内 容 提 要

本书将编程方法、网络协议和应用实例有机结合起来，详细阐明 Windows 网络编程的各方面内容。本书首先介绍 Windows 平台上进行网络编程的基础知识，包括网络硬件、术语、协议、Winsock 编程接口和各种 I/O 方法等。然后通过具体实例详细讲述当前流行的高性能可伸缩服务器设计、IP 多播和 Internet 广播、P2P 程序设计、原始套接字、SPI、协议驱动的开发和原始以太数据的发送、ARP 欺骗技术、LAN 和 WAN 上的扫描和侦测技术、个人防火墙与网络封包截获技术等。最后讲述 IP 帮助函数。

本书结构紧凑，内容由浅入深，是学习 Windows 网络与通信程序设计的理想书籍。

Windows 网络与通信程序设计

◆ 编　　著　王艳平　张　越
责任编辑　刘　浩

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：27.75
字数：677 千字　　2006 年 1 月第 1 版
印数：1 – 5 000 册　　2006 年 1 月北京第 1 次印刷

ISBN 7-115-14150-9/TP • 5062

定价：52.00 元（附光盘）

读者服务热线：(010)67132692　印装质量热线：(010)67129223

前　言

随着计算机和网络的普及，单独工作、不需要与其他用户交互的应用程序越来越少了。打开电脑，打开浏览器，打开各种各样的聊天和通信工具，我们接触到的是网络。展望未来的IT产业，网络将成为核心。高性能的服务器设计，用户程序的分布管理，高效率的数据传输，数据安全等无不是网络程序设计者要考虑的问题。

网络编程复杂，一方面是因为网络协议本身复杂多样，许多编程者又对具体使用的下层协议了解不够，另一方面是因为Windows系统提供的编程接口多种多样，且都工作在不同的层次。虽然现在介绍网络编程的书很多，但大都没有将概念解释清楚，如完成端口、分层服务提供者、NDIS等，有些书对重要的概念、机制和协议等避而不谈。

Internet的迅速发展给现代人的生产和生活都带来了前所未有的飞跃，但是也给人们带来了一个日益严峻的问题——网络安全。各种各样的“黑客”技术如路由跟踪技术、封包嗅探技术、TCP半开扫描技术、IP欺骗及ARP欺骗技术等在网上也被炒得沸沸扬扬，但是这些技术都是以原理的形式出现，很少有人提及具体的实现方法。要想维护网络的安全，彻底弄清楚这些技术是非常必要的。

作为一项新兴技术，P2P以其无与伦比的可伸缩性和对资源的利用率吸引了开发者、投资者、IT经理人和大众的注意。常见的BT、eMule、Kuro、OICQ等网络软件都是基于P2P模型的，其基本思想是不经过固定的服务器，Internet上的任意两台电脑就可以直接通信。现在市场上这方面的书籍大多是注重理论，没有讲解如何使用C/C++进行P2P程序设计的。

在网络安全越发显得重要的今天，防火墙在网络软件中扮演的角色越来越不容忽视了。然而，Windows防火墙的开发涉及到太多的系统底层知识，网上虽然有一些出售防火墙源程序代码的站点，但是撇开不菲的价格不说，其过于简单的文档说明令没有相关编程经验的人很难看懂。这使得许多想从事防火墙开发的读者不知如何下手。

鉴于以上几点，我们编写了《Windows网络与通信程序设计》一书，希望本书的读者不但能够学会网络编程，更能从此喜欢它，既愿意又有能力为中国的网络发展贡献一份力量。

—— 内容安排

全书共分13章，具体内容安排如下：

第1章～第3章讲解计算机网络基础、Windows网络编程接口、Windows套接字I/O模型，讲述Windows平台上进行网络编程的基础知识，包括网络硬件、网络协议和Winsock接口等知识。目的是让初学者熟悉常见网络结构和网络协议，学会使用Winsock编程接口，懂得各种I/O模型的优缺点，能够熟练使用它们进行程序设计。能够解决网络编程中的一般性问题，如文件传输、错误处理等。

第4章讲解IOCP与可伸缩网络程序设计。现今，无论是Web服务器，还是各种游戏服务器，每时每刻都要处理成千上万的客户连接，因此，服务器的性能和可伸缩性变的越来越重要了。本章将讨论设计高性能的服务器程序要注意的问题，并详细讲述广泛应用于各种类型商业服务器（如Apache等）的IOCP技术，给出一些函数和类供读者在开发中直接使用。

第 5 章讲解 Internet 广播和 IP 多播。广播和多播在实际中有许多重要的应用，如视频点播、远程教学、网络电视等。本章详细讲述广播和多播协议编程，并给出一个基于 IP 多播的组讨论会实例。

第 6 章～第 9 章讲解原始套接字、Winsock 服务提供者接口（SPI）、Windows 网络驱动接口标准（NDIS）和协议驱动的开发、网络扫描与诊测技术，将讨论 Windows 网络程序设计的各种高级特性，如原始套接字的使用，协议驱动的开发，路由跟踪，LAN 和 WAN 扫描，ARP 欺骗技术、封包嗅探、网络数据的窃取和保护等，这些知识点都有完整的实例相对应。

第 10 章讲解点对点（P2P）网络通信技术，将提出各种解决方案并给出具体的实现代码，以使 Internet 上的任何电脑之间都可以直接建立 UDP 或 TCP 连接。

第 11 章～第 12 章讲解核心层网络封包截获技术、Windows 网络防火墙开发技术，将讨论各种流行的网络封包截获技术，详细讲述开发 Windows 个人防火墙（采用应用层/核心层双重过滤机制）。

第 13 章讲解 IP 帮助函数，做为参考资料，介绍了常用的 IP 帮助函数以及未公开的 IP 帮助扩展函数。

—— 读者对象

- 想使用 Winsock 函数编写网络客户程序和服务器程序的读者。
- 想学习如何开发 Windows 网络驱动程序的读者。
- 想了解各种标准的网络协议在 Windows 平台下是如何实现的读者。
- 对互联网和局域网网络安全和防火墙开发感兴趣的读者。
- 需要用到网络封包截获技术的读者。
- 欲进行 P2P 对等网络程序设计的读者。

—— 在阅读本书之前，读者应该具有的基础知识

- 读者应该熟知 C 编程语言，懂得 C++语言的基础知识。
- 读者应该有基本的 Windows API 编程经验。

—— 关于附书光盘和读者反馈

本书的例子源代码都可以在附书光盘中找到，代码全部使用 Visual C++ 6.0 和 7.0 编译通过。虽然本书中的所有例子都已经在 Windows 2000、Windows XP 和 Windows 2003 下测试通过，但由于许多工程比较复杂，加之作者理论水平有限，书中难免出现差错和遗漏，如果发现书中的任何问题，请发电子函件至：book_better@sina.com，以便在下一版中改进。

—— 致谢

感谢深圳万兴软件公司的杨长元先生，提供并调试了本书的许多实例代码。

感谢高晓玉、王冰女士以及刘雪东、赵涛、魏新明、王俊波、吴俊峰先生，他们为本书的编写提出了很多宝贵的意见和建议。

编者

2006 年 1 月

目 录

第 1 章　计算机网络基础

本章详细讲述网络程序设计中要用到的计算机网络方面的基础知识，包括各种网络术语、网络硬件设备、网络拓扑结构、网络协议等。

1.1　网络的概念和网络的组成

网络是各种连在一起的可以相互通信的设备的集合。本书讲述的网络是最常见的，将数亿计算机连接到一起的 Internet。下面通过讲述组成 Internet 的基本硬件和软件来进一步明确计算机网络的概念。

Internet 是世界范围内的计算机网络，它不仅连接了个人 PC、存储和传输信息的服务器，还连接了 PDA、电视、移动 PC 等。所有的这些设备称为**主机**（host）或**终端系统**（end system）。

终端系统由**通信链接**（communication links）连在一起。常见的通信链接有双绞线、同轴电缆、光纤等，它们负责传递原始的比特流。

终端系统通常并不通过单一的通信链接相互连在一起，而是通过中介交换设备间接相连。这些中介交换设备称为**包交换器**（packet switch）。包交换器在通信链路上接收到达的信息块，并向其他的通信链路上推进这个信息块。这些信息块称为**包**（packet）。包交换器有多种形状和特色，当今 Internet 上最基本的两种包交换器是**路由器**（router）和**链路层交换器**（link-layer switch）。两种类型的交换器都推动包向它们的目的地址前进，后面还要详细讨论它们。

从发送终端系统到接收终端系统，包所经过的通信链接和包交换器称为**路线**（route）或**路径**（path）。

每个终端系统通过 ISP（Internet Service Provider，Internet **服务提供商**）连接 Internet。ISP 拥有由许多通信链接和包交换器组成的网络，它提供的网络访问类型多种多样，有 56kbit/s 的拨号 Modem 访问、高速 LAN 访问、无线访问等。

终端系统、包交换器和 Internet 的其他部分，都运行**协议**（protocol）来控制数据的发送和接收，协议是计算机用来与其他计算机通信的语言。TCP（Transfer Control Protocol, **传输控制协议**）和 IP（Internet Protocol, **网际协议**）是两个最重要的协议。IP 指定了在路由器和终端系统中传输的封包的格式。Internet 中所有重要的协议共同称为 TCP/IP。本书还会详细介绍它们。

除了 Internet，还有许多专用网络，如许多公司和政府的网络。这些专用网络通常称为**企业内部互联网**（Intranet），它们使用的主机、路由器、链接和协议与 Internet 相同。

1.2 计算机网络参考模型

了解网络的相关概念之后，本节将讨论计算机网络中主机之间是如何进行通信的，以及各种通信协议之间的关系等。

1.2.1 协议层次

为了降低设计难度，大部分网络都以**层**（layer 或 level）的形式组织在一起，每一层都建立在它的下层之上，使用它的下层提供的服务，下层对它的上层隐藏了服务实现的细节。这种方法几乎应用于整个计算机科学领域，也可以称为信息隐藏、数据类型抽象、数据封装、面向对象编程等。

一个机器上的第 n 层和另一个机器的第 n 层交流，所使用的规则和协定合起来称为第 n 层协议。这里的**协议**，是指通信双方关于如何进行通信的一种约定。各层和各层协议的集合称为**网络体系**（network architecture）。特定系统所使用的一组协议称为**协议堆栈**（protocol stack）。下面介绍 Inernet 网络分层情况和它的协议堆栈。

1.2.2 TCP/IP 参考模型

为了帮助不同的厂商标准化和一体化它们的网络软件，1974 年，国际标准化组织（ISO，International Organization for Standardization）为在机器之间传送数据定义了一个软件模型，就是著名的 OSI 模型（Open Systems Interconnection，开放式系统互联模型）。这个模型共有 7 层，如图 1.1 所示。

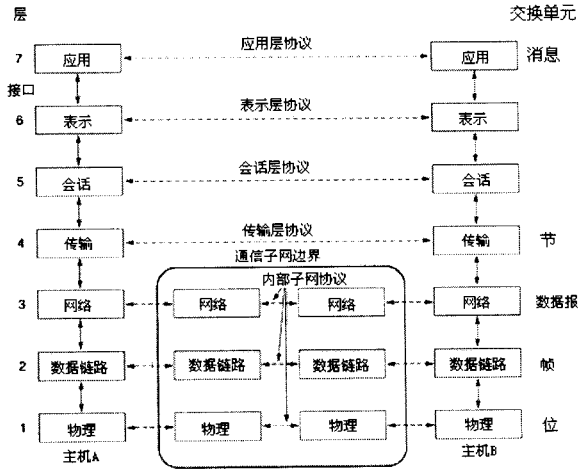

图 1.1 OSI 参考模型

OSI 参考模型仅是一个理想方案，几乎没有什么系统能够完全实现它，它存在的作用是给人们一个设计网络体系的框架。机器上的每一层都假设它正在直接与另一机器的同一层“交谈”，它们“说”相同的语言，或者协议，各层的目的是向更高的层提供服务，抽象低层的实

现细节。TCP/IP 实现了 OSI 参考模型中的 5 层，如图 1.2 所示，各层使用的协议连在一起便是互联网协议堆栈。

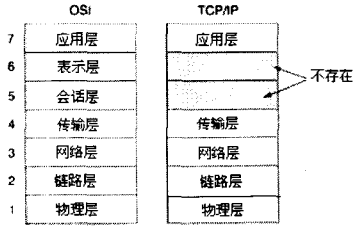

图 1.2　TCP/IP 与 OSI 参考模型

1.2.3　应用层（Application Layer）

应用层是网络应用程序和它们的应用层协议存在的地方。Internet 应用层包含许多协议，如 HTTP（它提供 Web 文档的请求和传输）、SMTP（它提供 e-mail 消息的传输）和 FTP（它提供两个终端系统间的文件传输）。一些特定的网络功能，如映射主机名到它们的网络地址的 DNS（Domain Name System，域名服务器）也在此层完成。

应用层程序设计在现实生活中应用最广泛，因为它是直接面向用户的。本书在后面要讨论的客户端和服务器端程序、P2P 通信程序等都属于此层。本书使用应用层消息来表示应用层的数据传输单元。

1.2.4　传输层（Transport Layer）

Internet 的传输层在应用程序的客户和服务器之间传递应用层消息，在这里定义了两个点对点的传输协议——TCP（Transmission Control Protocol，传输控制协议）和 UDP（User Datagram Protocol，用户数据报协议）。

TCP 是一个可靠的面向连接的协议，它允许源于一个机器的字节流被无错误地传输到 Internet 上的任何其他机器。TCP 将上层传递的字节流分成封包，再接着传递到它的下层——网络层。在接收方，TCP 重新集合接收到的封包，将其转化成为输出流。TCP 也处理流控制，以确保一个快的发送者不会发送太多的封包而淹没接收者。

UDP 是一个不可靠的无连接的协议，它是为那些不需要 TCP 的序列号管理和流控制，而想自己提供这些功能的应用程序设计的。

Windows 为传输层的编程接口提供了 Socket 函数，即通常所说的 Winsock。网络程序设计者可以非常方便地使用 Winsock 开发基于 TCP 或者 UDP 的应用程序。本章后面要详细讨论这些编程接口。

本书使用节（segment）来表示传输层封包。

1.2.5　网络层（Network Layer）

Internet 的网络层负责将网络层封包从一个主机移动到其他主机，这里的网络封包称为数据报（datagram）。在源主机，Internet 传输层协议（TCP 或 UDP）向网络层传递一个传输层节和一个目的地址，就如同你给邮递员一个带有地址的信。然后，网络层提供将这个节邮递到目的主机传输层的服务。

Internet 的网络层有两个基本组件。一个是 IP 协议，它定义了数据报中各域以及终端系统和路由器如何在这些域上进行操作。仅有一个 IP（Internet Protocol）协议，所有有网络层的 Internet 组件都必须运行这个协议。另一个是路由协议，它们用来决定数据报所走的路径。网络层的路由协议很多，因为 Internet 含有多种不同类型的网络，各个网络使用的路由协议有可能不同。即便是这样，网络层还是经常被人们简单地称为 IP 层，反映了 IP 是将 Internet 绑在一起的胶带。

网络层包含了子网的操作，是懂得网络拓扑结构（网络中机器的物理配置、带宽的限制等）的最高层，也是内网通信的最高层。它的责任是确定数据的物理路径。

1.2.6 链路层（Link Layer）

Internet 的网络层通过一系列的路由器在源地址和目的地址之间传输数据报。为了将封包从路径上的一个节点移动到下一个节点，网络层依赖于链路层的服务。在每个节点，网络层传递数据报到下面的链路层，让它将之发送到路径上的下一个节点。在下一个节点，链路层再把这个数据报传递给网络层。

链路层间的通信方式有两种，一种是将数据发给它所有相邻的节点，这便是广泛用于 LAN（Local Area Network，局域网）的广播通信；另一种是应用于 WAN 中的点对点通信，例如，两个路由器之间或者住宅的拨号调制解调器（Modem）和 ISP 路由之间的通信。对应这两种通信方式的常用协议有 Ethernet 和 Point-to-Point（PPP）。

对一个给定的连接来说，链路层协议主要实现在适配器中，即我们平常所说的 NIC（Network Interface Card，网卡），它有一个主机总线接口和一个连接接口。传输节点的网络层把网络层数据报传递到适配器，由适配器将此数据报封装到链路层的帧中，然后把这个帧传输到物理层通信链路。在另一方，接收适配器接收到整个帧，从中萃取出网络层数据报，将它传给网络层。

本书将使用帧（frame）来表示链路层封包。

1.2.7 物理层（Physical Layer）

链路层的工作是从一个网络节点向其临近的网络节点传送整个帧，其下面的物理层的工作是将帧中的原始比特流从一个节点传送到下一个节点。应用于此层的协议在 TCP/IP 参考模型中并没有定义，它们与连接有关，更依赖于传输介质。例如，以太网有许多物理层协议，有针对双绞线的，有针对同轴电缆的，有针对光纤的，等等。它们都以不同的方式在链接中传送数据位。

1.3 网络程序寻址方式

编写网络程序，必须要有一种机制来标识通信的双方。本节详细讨论 Internet 中各层的寻址方式，以及相关的寻址协议。

1.3.1 MAC 地址

网络通信的最边缘便是 LAN 了，我们先来看看在 LAN 中是如何寻址的。