HZ BOOKS
华章教育

高等院校信息安全专业规划教材

Windows网络编程

Windows Network Programming

刘琰 王清贤 刘龙 陈熹 ◎ 编著

机械工业出版社
China Machine Press

高等院校信息安全专业规划教材

Windows网络编程

Windows Network Programming

刘琰 王清贤 刘龙 陈熹 ◎ 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Windows 网络编程 / 刘琰等编著. —北京：机械工业出版社，2013.10
（高等院校信息安全专业规划教材）

ISBN 978-7-111-44196-0

I. W… II. 刘… III. Windows 操作系统—网络软件—程序设计—高等学校—教材 IV. TP316.86

中国版本图书馆 CIP 数据核字（2013）第 231608 号

本书全面和系统地介绍了网络编程的基本原理，剖析了网络应用程序实现与套接字实现和协议实现之间的关联，重点阐述了 Windows Sockets 编程和 WinPcap 编程的主要思想、程序设计方法以及开发技巧和可能的陷阱，分析了不同编程方法的适用性和优缺点。

本书系统性较强，内容丰富、结构清晰、论述严谨，既突出基本原理和技术思想，也强调工程实践，适合作为网络工程、信息安全、计算机应用、计算机软件、通信工程等专业的本科生教材，也可供从事网络工程、网络应用开发和网络安全等工作的技术人员参考。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：刘立卿
北京瑞德印刷有限公司印刷
2014 年 1 月第 1 版第 1 次印刷
185mm × 260mm • 17.75 印张
标准书号：ISBN 978-7-111-44196-0
定 价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

编委会

丛书序

经过数年的筹划与努力，信息安全系列丛书终于和广大读者见面了。

众所周知，进入21世纪以来，信息化对社会发展的影响日益深刻。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。

人们在享受信息化所带来的便利的同时，也不得不面对各种信息安全问题。信息安全是信息化的关键，各种天灾（如地震、洪水、飓风）和“人祸”（如网络故障、黑客入侵、病毒等）都会影响信息化进程。因此，在发展信息化的同时要重视信息安全，要在安全中发展，在发展中确保安全。

目前，世界各国都将信息安全视为国家安全的重要组成部分。党的十六届四中全会在《中共中央关于加强党的执政能力建设的决定》中明确提出：“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。党中央把信息安全和政治安全、经济安全、文化安全并列，作为我们国家四大安全内容之一，可见信息安全之重要，绝不能掉以轻心。近年来，我国在信息安全保障方面的工作逐步加强，制定并实施了国家信息安全战略，建立了信息安全管理体制和工作机制。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

信息安全问题的解决，既要依靠技术的发展，更要重视人的作用。随着科技的进步，信息安全的概念和内涵不断发生变化，今天我们所说的信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等领域的交叉学科，各种保障信息安全的技术也不断推陈出新。我们应大力培养信息安全的专业人才，对从业人员进行技术、职业道德、法律等全方位的教育。同时，要普及信息安全教育，增强国民的信息安全意识，提高全民的信息化知识水平和防范意识。

面对社会对信息安全人才的迫切需求，国内已有几十所高校设立了信息安全专业，还有众多高校开设了信息安全相关的必修与选修课。为了有力地支持信息安全相关课程的教学，促进信息安全的科学研究，在机械工业出版社华章分社的精心策划与组织下，国内高校从事信息安全领域研究、教学的专家和教师共同编写了这套“高等院校信息安全专业规划教材”。这套丛书是各位作者多年教学、科研成果的结晶，其特点是理论与实践紧密结合、深入浅出、实例丰富，既包括基础知识，也反映最新科研成果与发展趋势。我深信，丛书的出版必将对信息安全知识的普及和推广、信息安全人才的培养、教学与科研产生积极影响并作出重要的贡献。

最后，作为本丛书的编委会主任，我对各位编委的努力工作、各位作者的辛勤劳动、机械工业出版社华章分社的大力支持表示衷心的感谢。

丛书编委会主任　卿斯汉

2009年6月

前言

在信息化高度发展的今天，网络应用层出不穷，技术日新月异。越来越多的应用运行在网络环境下，这就要求程序员能够在最普及的 Windows 操作系统上开发网络应用程序。目前，国内大批专门从事网络技术开发与技术服务的研究机构和高科技企业需要网络基础扎实、编程技术精湛的专业技术人才。作为计算机网络课程体系的重要组成部分，网络编程相关课程已在国内各大高校开设。

本书详细地介绍了网络编程的基本原理，剖析了网络应用程序实现与套接字实现和协议实现之间的关联，重点阐述了 Windows Sockets 编程和 WinPcap 编程的主要思想和程序设计方法，分析了不同编程方法的适用性和优缺点。通过本书内容的学习，读者可以熟悉 Windows 系统中网络编程的基本方法，系统掌握网络数据处理的原理和技术，提高网络实践能力，为将来从事网络技术研究、网络应用程序开发和网络管理等工作打下坚实的基础。

本书着眼于基本技能的训练和强化，以问题为牵引，由浅入深，辅以前后贯穿的范例实验，力求将编程方法的适用场合分析透彻，将网络编程的原理解释清楚，将网络通信中遇到的瓶颈问题优化改进。本书共分 9 章和 1 个附录。第 1 ~ 3 章阐述网络编程所涉及的相关基础知识，包括分布式网络应用程序的结构、TCP/IP 协议基础、网络程序通信模型和网络数据的内容与形态等；第 4 ~ 7 章重点介绍 Windows Sockets 编程的基本方法，包括协议软件接口、套接字的基本概念，Windows Sockets 中流式套接字、数据报套接字和原始套接字三种基本套接字的适用场合、通信功能、处理细节和优化策略等；第 8 章比较详尽地讲解了 Windows 系统中常用的 7 种 I/O 模型的基本概念、相关函数、编程框架和应用场合；第 9 章重点阐述了基于 WinPcap 的网络数据构造、捕获、过滤和分析技术；附录部分给出了 Windows Sockets 错误码和错误原因。

为了方便读者阅读和学习，编者根据本书内容另外提供了课后习题和解答、PPT 课件、使用 Visual Studio 2008 开发的 Visual C++ 应用程序源代码等辅助教学资源。读者可以登录机械工业出版社华章公司网站（http://www.hzbook.com/）免费下载。

本书由解放军信息工程大学网络空间安全学院组织编写，刘琰完成了本书全部章节的撰写和示例代码编码，王清贤教授参与部分章节的编写并审校全书，刘龙和陈熹完成了本书习题和教学资源的制作和整理。

本书是编者根据多年开发网络应用程序和研究相关课程教学的经验，并在多次编写的内部交流讲义的基础上修改而成的。由于网络技术的快速发展，加之作者水平有限，疏漏和错误之处在所难免，恳请读者和有关专家不吝赐教。

编者

2013 年 6 月

教学和阅读建议

本课程的先修课程为“程序设计”、“计算机网络”、“网络协议分析”。本课程强调技能训练，在授课内容上注重知识的实用性和连贯性，建议授课学时为 40 学时（22 学时授课，18 学时实践），各章的教学内容可做如下安排。

第 1 章　网络应用程序设计基础（课堂教学 2 学时）

教学内容：

- 协议层次和服务模型。
- 网络程序寻址方式。
- 分布式网络应用程序的特点及分类。
- 常用网络编程方法。

考核要求：

通过课堂讲解，学生应能比较全面地巩固网络程序设计中所涉及的计算机网络方面的基础知识，包括各种网络术语、网络协议、网络程序寻址方式等，了解基于计算机网络开发的分布式网络应用程序的特点，从层次化的角度了解网络应用程序设计的基本方法。

第 2 章　网络程序通信模型（课堂教学 2 学时，上机实践 2 学时）

教学内容：

- 网络应用程序与网络通信之间的关系。
- 客户 / 服务器模型。
- 浏览器 / 服务器模型。
- P2P 模型。

考核要求：

通过课堂讲解，学生应能理解各种网络程序通信模型产生的原因，掌握客户 / 服务器模型的基本原理，了解浏览器 / 服务器模型和 P2P 模型的基本概念，能够根据实际问题需求选择合适的通信模型，搭建合理的程序架构。

通过上机实践，学生应能熟悉常用的网络编程辅助工具，掌握网络应用程序的调试和分析技能。

第 3 章　网络数据的内容与形态（课堂教学 2 学时）

教学内容：

- 整数的长度与符号。

- 字节顺序。
- 结构的对齐与填充。
- 网络数据传输形态。
- 字符编码。
- 数据校验。

考核要求：

通过课堂讲解，学生应能掌握网络数据在存储、传输过程中的基本概念，掌握正确的整数符号处理、字节顺序转换、结构对齐、字符编码转换和数据校验计算等方法。

第 4 章　协议软件接口（课堂教学 2 学时，上机实践 2 学时）

教学内容：

- TCP/IP 协议软件接口的位置和功能。
- 网络通信的基本方法。
- 套接字的基本概念和通信过程。
- Windows 套接字的基本概念和编程接口。

考核要求：

通过课堂讲解，学生应能了解套接字的起源和设计初衷，掌握套接字的基本概念，掌握 Windows 套接字的组成和特点，熟悉 Windows 套接字的基本函数功能，掌握套接字的初始化和释放、套接字控制以及地址的描述与转换等方法。

通过上机实践，学生应能掌握使用 Windows 套接字进行网络应用程序开发的基本方法，包括开发环境配置方法、常用数据结构和程序开发流程等。

第 5 章　流式套接字编程（课堂教学 4 学时，上机实践 4 学时）

教学内容：

- 流式套接字的适用场合、通信过程和交互模型。
- 流式套接字编程相关函数的使用方法。
- TCP 的流传输控制。
- 面向连接程序的可靠性保护和传输效率分析。

考核要求：

通过课堂讲解，学生应能明确流式套接字的应用场合，掌握流式套接字编程的基本模型、函数使用细节和开发流程，掌握 TCP 流的传输控制方法，了解使用 TCP 协议传输的应用程序可能出现的失败模式，掌握面向连接程序的可靠性保护和传输效率改进的基本方法。

通过上机实践，学生应能掌握流式套接字编程的基本方法，熟练使用辅助工具观察程序运行过程中的状态和通信细节，排除常见的套接字编程中的异常问题。

第 6 章　数据报套接字编程（课堂教学 2 学时，上机实践 2 学时）

教学内容：

- 数据报套接字的适用场合、通信过程和交互模型。
- 数据报套接字编程相关函数的使用方法。
- 无连接程序的可靠性维护方法。

- 无连接服务器的并发处理方法。

考核要求：

通过课堂讲解，学生应能明确数据报套接字的应用场合，掌握数据报套接字编程的基本模型、函数使用细节和开发流程，了解使用 UDP 协议传输的应用程序可能出现的不可靠性问题和维护方法，了解无连接服务器并发处理的基本思路。

通过上机实践，学生应能掌握数据报套接字编程的基本方法，熟练使用辅助工具观察程序运行过程中的状态和通信细节，排除常见的套接字编程中的异常问题。

第 7 章　原始套接字编程（课堂教学 2 学时，上机实践 2 学时）

教学内容：

- 原始套接字的功能、适用场合、通信过程和交互模型。
- 原始套接字的创建、数据发送和数据接收方法。

考核要求：

通过课堂讲解，学生应能明确原始套接字的功能和应用场合，掌握原始套接字编程的基本模型和开发流程，掌握原始套接字的创建、控制、发送和接收处理方法，了解 Windows 对原始套接字的限制。

通过上机实践，学生应能掌握原始套接字编程的基本方法，排除常见的套接字编程中的异常问题，提高对协议数据的操控能力。

第 8 章　网络通信中的 I/O 操作（课堂教学 4 学时，上机实践 4 学时）

教学内容：

- 套接字的 I/O 模式。
- 阻塞 I/O 模型。
- 非阻塞 I/O 模型。
- I/O 复用模型。
- 基于消息的 WSAAsyncSelect 模型。
- 基于事件的 WSAEventSelect 模型。
- 重叠 I/O 模型。
- 完成端口模型。

考核要求：

通过课堂讲解，学生应能掌握网络 I/O 操作的基本思想，掌握在 Windows 系统中常用的 7 种 I/O 模型的基本概念、相关函数、编程框架和应用场合。

通过上机实践，学生应能掌握基本网络 I/O 模型的编程方法，结合现实需求，选择合适的网络 I/O 模型，对网络应用程序的通信性能进行改进。

第 9 章　WinPcap 编程（课堂教学 2 学时，上机实践 2 学时）

教学内容：

- WinPcap 的起源与功能。
- WinPcap 的体系结构和编程接口。

- WinPcap 编程环境配置。
- wpcap.dll 的常用数据结构和编程方法。
- Packet.dll 的常用数据结构和编程方法。

考核要求：

通过课堂讲解，学生应能掌握 WinPcap 的功能、体系结构和编程接口，掌握利用 wpcap.dll 进行底层网络程序开发的基本方法，掌握利用 Packet.dll 进行底层网络程序开发的基本方法。

通过上机实践，学生应能掌握 WinPcap 编程环境的配置方法，掌握使用 WinPcap 进行底层网络通信程序开发的基本流程，排除常见的 WinPcap 编程中的异常问题，提高对底层协议数据的操控能力。

目录

Chapter 1

第1章 网络应用程序设计基础

网络编程的基础是计算机网络，本章简要讲述网络程序设计中涉及的计算机网络方面的基础知识，包括各种网络术语、网络拓扑结构、网络协议等。基于计算机网络开发的分布式网络应用程序种类多样，设计需求也千差万别，本章对常用的网络程序设计方法进行归纳，由高层至底层分别介绍了面向应用的网络编程方法、基于TCP/IP协议栈的网络编程方法和面向原始帧的网络编程方法。

1.1 计算机网络基础

1.1.1 协议层次和服务模型

计算机网络，是指将地理位置不同且具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。总的来说，计算机网络的组成基本上包括计算机、网络操作系统、传输媒体以及相应的应用软件四部分。

计算机网络是一个极为复杂的系统，网络中有许多部分：大量的应用程序和协议、各种类型的端系统，以及各种类型的链路级媒体。面对这种复杂的系统，如何简化管理是非常重要的。为了降低设计难度，网络设计者以分层的方式组织协议以及实现这些协议的网络硬件和软件。协议分层具有概念化和结构化的优点，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服务实现的细节。

一个机器上的第 n 层与另一个机器的第 n 层交流，所使用的规则和协定合起来被称为第 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，每个协议属于某个层次。特定系统所使用的一组协议被称为协议栈（protocol stack）。

1. OSI 参考模型

在OSI出现之前，计算机网络中存在多种体系结

构，其中以 IBM 公司的系统网络体系结构（System Network Architecture，SNA）和 DEC 公司的数字网络体系结构（Digital Network Architecture，DNA）最为著名。为了解决不同体系结构的网络互连问题，国际标准化组织 ISO 于 1981 年制定了开放系统互连参考模型（Open System Interconnection Reference Model，OSI/RM）。这个模型把网络通信的工作分为 7 层，它们由低到高分别是物理层（physical layer）、数据链路层（data link layer）、网络层（network layer）、传输层（transport layer）、会话层（session layer）、表示层（presentation layer）和应用层（application layer），如图 1-1a 所示。

OSI参考模型	
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

a）

TCP/IP 参考模型	
5	应用层
4	传输层
3	网络层
2	数据链路层
1	物理层

b）

图 1-1　OSI 参考模型与 TCP/IP 参考模型

第 1 层到第 3 层属于 OSI 参考模型的低三层，负责创建网络通信连接的链路；第 4 层到第 7 层为 OSI 参考模型的高四层，具体负责端到端的数据通信。每层完成一定的功能，每层都直接为其上层提供服务，并且所有层次都互相支持，而网络通信则可以自上而下（在发送端）或者自下而上（在接收端）双向进行。当然并不是每一通信都需要经过 OSI 的全部七层，有的甚至只需要双方对应的某一层即可。物理接口之间的转接，以及中继器与中继器之间的连接就只需在物理层中进行；而路由器与路由器之间的连接则只需经过网络层以下的三层。总的来说，双方的通信是在对等层次上进行的，不能在不对等层次上进行。

2. TCP/IP 参考模型

ISO 制定的 OSI 参考模型过于庞大、复杂，招致了许多批评。与此对照，由技术人员自己开发的 TCP/IP 协议栈获得了更为广泛的应用。

TCP/IP 协议栈是美国国防部高级研究规划局计算机网（Advanced Research Projects Agency Network，ARPANET）和其后继因特网使用的参考模型。TCP/IP 参考模型分为五个层次：应用层、传输层、网络层、链路层和物理层，如图 1-1b 所示。

在 TCP/IP 参考模型中，去掉了 OSI 参考模型中的会话层和表示层（这两层的功能被合并到应用层实现）。以下分别介绍各层的主要功能。

（1）应用层

应用层是网络应用程序及其应用层协议存留的层次。TCP/IP 协议簇的应用层协议包括 Finger（用户信息协议）、文件传输协议（File Transfer Protocol，FTP）、超文本传输协议（Hypertext Transfer Protocol，HTTP）、Telent（远程终端协议）、简单邮件传输协议（Simple

Mail Transfer Protocol，SMTP）、因特网中继聊天（Internet Relay Chat，IRC）、网络新闻传输协议（Network News Transfer Protocol，NNTP）等。

应用层之间交换的数据单位为消息流或报文（message）。

（2）传输层

在 TCP/IP 模型中，传输层的功能是使源端主机和目标端主机上的对等实体可以进行会话。在传输层定义了两种服务质量不同的协议，即传输控制协议（Transmission Control Protocol，TCP）和用户数据报协议（User Datagram Protocol，UDP）。

TCP 协议是一个面向连接的、可靠的协议，为应用程序提供了面向连接的服务。这种服务将一台主机发出的消息流无差错地发往互联网上的其他主机。在发送端，它负责把上层传送下来的消息流分成数据段并传递给下层；在接收端，它负责把收到的数据包进行重组后递交给上层。另外，TCP 协议还要处理网络拥塞控制，在网络拥塞时帮助发送源抑制其传输速度；提供端到端的流量控制，避免缓慢接收的接收方没有足够的缓冲区接收发送方发送的大量数据。TCP 的协议数据传输单元为 TCP 数据段（TCP segment）。

UDP 协议是一个不可靠的、无连接的协议，为应用程序提供无连接的服务。这种服务主要适用于广播数据发送和不需要对报文进行排序和流量控制的场合。UDP 的协议数据传输单元为 UDP 数据报（UDP datagram）。

（3）网络层

网络层是整个 TCP/IP 协议栈的核心。网络层的功能是通过路径选择把分组发往目标网络或主机，进行网络拥塞控制以及差错控制。

网际协议（Internet Protocol，IP）是网络层的重要协议，该协议定义了数据包中的各个字段以及端系统和路由器如何作用于这些字段。

网络层中的另一个协议 Internet 控制报文协议（Internet Control Message Protocol，ICMP）用于在 IP 主机、路由器之间传递控制消息。控制消息包括网络是否畅通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

另外网络层也包括决定路由的选路协议（如 RIP、OSPF 等），数据包根据选定的路由从源传输到目的地。

网络层的协议数据传输单元为数据包（packet），或称为分组。

（4）数据链路层

数据链路层负责物理层和网络层之间的通信，将网络层接收到的数据分割成特定的、可被物理层传输的帧，并交付物理层进行实际的数据传送。

数据链路层提供的服务取决于应用于该链路层的协议，常用的协议包括以太网的 802.3 协议、Wi-Fi 的 802.11 协议和点对点协议（PPP）等。因为数据包从源到目的地传送通常需要经过几条链路，所以它可能被沿途不同链路上的不同链路层协议处理。

数据链路层的协议数据传输单元为帧（frame）。

（5）物理层

链路层的任务是将整个帧从一个网络元素移动到邻近的网络元素，而物理层的任务是将该帧中的一个一个比特从一个节点移动到下一个节点。该层中的协议仍然是链路相关的，并且进一步与链路（如双绞线、单模光纤）的实际传输媒体相关。对应于不同的传输媒体，跨越这些链路移动一个比特的方式也不同。