普通高等教育“十一五”国家级规划教材

21世纪高等学校计算机规划教材

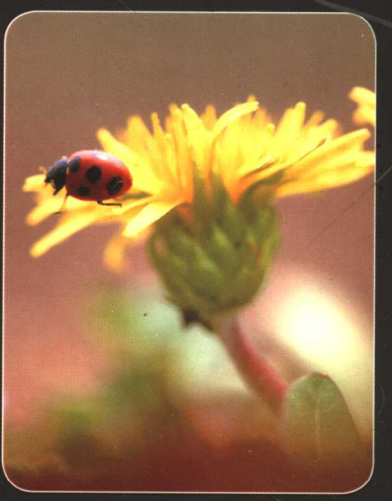
21st Century University Planned Textbooks of Computer Science

计算机网络安全基础（第三版）

The Basis of Computer Network Security (3rd Edition)

袁津生 齐建东 曹佳 编

- 讲解网络安全实例丰富
- 反映先进成果启发学生创新思维
- 配套实战教程《计算机网络与实用编程》



精品系列

人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

21世纪高等学校计算机规划教材

21st Century University Planned Textbooks of Computer Science

TP393.08/236

2008

计算机网络安全基础（第三版）

The Basis of Computer Network Security (3rd Edition)

袁津生 齐建东 曹佳 编

精品系列

人民邮电出版社

北京

图书在版编目（CIP）数据

计算机网络安全基础 / 袁津生，齐建东，曹佳编. —3 版.
北京：人民邮电出版社，2008.3
21 世纪高等学校计算机规划教材. 普通高等教育“十一五”国家级规划教材
ISBN 978-7-115-16915-0

Ⅰ. 计… Ⅱ. ①袁…②齐…③曹… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 150260 号

内 容 提 要

本教材共有 11 章，内容包括：网络的基础知识与因特网提供的主要服务、网络常用的操作系统、网络安全的基本知识、计算机系统安全与访问控制、数据安全、数据库系统安全、数据加密与认证技术、计算机病毒的防治、网络安全技术、网络站点的安全等内容。重点介绍如何保护自己的网络以及网络系统中的数据不被破坏和丢失，如何保证数据在传输过程中的安全，如何避免数据被篡改以及维护数据的真实性等。其中第 1～10 章各章的后面均附有小结和习题，第 11 章为实验及综合练习题，以帮助学生提高实际动手能力。

本书可作为高等院校计算机专业教材，也可作为计算机网络的系统管理人员、安全技术人员的相关培训教材或参考书。

普通高等教育“十一五”国家级规划教材

21 世纪高等学校计算机规划教材

计算机网络安全基础（第三版）

◆ 编　　袁津生　齐建东　曹　佳
责任编辑　滑　玉

◆ 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
北京隆昌伟业印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：22
字数：529 千字　　2008 年 3 月第 3 版
印数：79 001－82 000 册　　2008 年 3 月北京第 1 次印刷

ISBN 978-7-115-16915-0/TP

定价：35.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223
反盗版热线：(010)67171154

出版者的话

计算机应用能力已经成为社会各行业最重要的工作要求之一，而计算机教材质量的好坏会直接影响人才素质的培养。目前，计算机教材出版市场百花争艳，品种急剧增多，要从林林总总的教材中挑选一本适合课程设置要求、满足教学实际需要的教材，难度越来越大。

人民邮电出版社作为一家以计算机、通信、电子信息类图书与教材出版为主的科技教育类出版社，在计算机教材领域已经出版了多套计算机系列教材。在各套系列教材中涌现出了一批被广大一线授课教师选用、深受广大师生好评的优秀教材。老师们希望我社能有更多的优秀教材集中地呈现在老师和读者面前，为此我社组织了这套“21 世纪高等学校计算机规划教材-精品系列”。

“21 世纪高等学校计算机规划教材-精品系列”具有下列特点。

（1）前期调研充分，适合实际教学需要。本套教材主要面向普通本科院校的学生编写，在内容深度、系统结构、案例选择、编写方法等方面进行了深入细致的调研，目的是在教材编写之前充分了解实际教学的需要。

（2）编写目标明确，读者对象针对性强。每一本教材在编写之前都明确了该教材的读者对象和适用范围，即明确面向的读者是计算机专业、非计算机理工类专业还是文科类专业的学生，尽量符合目前普通高等教学计算机课程的教学计划、教学大纲以及发展趋势。

（3）精选作者，保证质量。本套教材的作者，既有来自院校的一线授课老师，也有来自 IT 企业、科研机构等单位的资深技术人员。通过他们的合作使老师丰富的实际教学经验与技术人员丰富的实践工程经验相融合，为广大师生编写出适合目前教学实际需求、满足学校新时期人才培养模式的高质量教材。

（4）一纲多本，适应面宽。在本套教材中，我们根据目前教学的实际情况，做到“一纲多本”，即根据院校已学课程和后续课程的不同开设情况，为同一科目提供不同类型的教材。

（5）突出能力培养，适应人才市场要求。本套教材贴近市场对于计算机人才的能力要求，注重理论技术与实际应用的结合，注重实际操作和实践动手能力的培养，为学生快速适应企业实际需求做好准备。

（6）配套服务完善，共促提高。对于每一本教材，我们在教材出版的同时，都将提供完备的 PPT 课件，并根据需要提供书中的源程序代码、习题答案、教学大纲等内容，部分教材还将在作者的配合下，提供疑难解答、教学交流等服务。

在本套教材的策划组织过程中，我们获得了来自清华大学、北京大学、人民大学、浙江大学、吉林大学、武汉大学、哈尔滨工业大学、东南大学、四川大学、上海交通大学、西安交通大学、电子科技大学、西安电子科技大学、北京邮电大学、中国林业大学等院校老师的大力支持和帮助，同时获得了来自信息产业部电信研究院、联想、华为、中兴、同方、爱立信、摩托罗拉等企业和科研单位的领导和技术人员的积极配合。在此，人民邮电出版社向他们表示衷心的感谢。

我们相信，“21 世纪高等学校计算机规划教材-精品系列”一定能够为我国高等院校计算机课程教学做出应有的贡献。同时，对于工作欠缺和不妥之处，欢迎老师和读者提出宝贵的意见和建议。

人民邮电出版社

第三版前言

计算机网络技术无疑是当今世界最为激动人心的高新技术之一。它的出现和快速的发展，尤其是因特网的迅速成长正在把一个世界连接成一个整体，同时也正在改变人们的传统生活方式，使人们的工作、学习以及娱乐方式发生了深刻变化。

但是，在科学技术进步的同时，计算机网络安全也越来越引起世界各国的关注。随着计算机在人类生活各个领域中的广泛应用，计算机病毒也不断的产生和传播，计算机遭到非法入侵，重要资料被破坏或丢失，由此造成网络系统的瘫痪给各个国家以及众多公司造成巨大的经济损失，甚至危及到国家和地区的公共安全。可见计算机系统的安全问题是一件关系到人类生活与生存的大事情，必须给予充分的重视并设法解决。

编写本书的目的是帮助网络系统管理员在这个千变万化的网络世界中保护自己的网络以及网络系统中的数据，也就是说如何保护“数据”不被毁坏和丢失。同时本书还着重介绍了计算机安全的一些基础知识，如安全级别、访问控制、病毒和加密等。

目前大多数高等院校陆续开设了计算机网络安全方面的课程。为了使本教材跟上时代的步伐和更好地适应教师的教学工作和学生的学习，经过 5 年多的实践和教学循环，作者对第一版和修订版的部分内容再次进行了修订，修正了原书中的错误，增加了一些近几年计算机网络安全领域发展的最新技术，并加强了理论知识，希望对读者学习网络安全的相关知识有所帮助。具体调整如下：

（1）修正了图表的错误，调整了部分章节不规范的内容；

（2）在第 7 章中新增加了 RC5 算法、安全 Hash 函数和数字信封技术；

（3）在第 8 章中删除了堡垒主机、包过滤和代理服务等内容，新增加了网络安全协议、网络加密技术、入侵检测技术和虚拟专用网技术；

（4）在第 9 章中增加了网络攻击类型的内容；

（5）重新设计了课后的习题，并给出相应的参考答案。

经过修订后，书中的内容更加完善、结构更加合理，更便于学生自学。

全书分为 10 章。第 1 章对网络参考模型、网络互连设备、协议以及基本的局域网和广域网技术作一般性的介绍，同时还介绍 TCP/IP 及因特网提供的主要服务。第 2 章探讨与计算机操作系统及其网络有关的安全问题和网络的配置。第 3 章讲述网络安全基础知识、威胁网络安全的因素、网络安全分类以及网络安全解决方案。第 4 章介绍什么是计算机安全、安全级别、系统访问控制、选择性访问控制和强制性访问控制等基本概念。第 5 章重点讨论数据库的安全、数据库安全的威胁、数据库的数据保护和数据库备份与恢复等有关问题。第 6 章讲述病毒的分类、机理、传播、破坏和预防及清除，着重介绍网络病毒和宏病毒的清理。第 7 章讲述数据加密的历史，现在流行的数据加密算法，如 DES、RAS 和 PGP 等。第 8 章主要介绍网络安全协议、网络加密技术、防火墙技术、入侵检测技术和虚拟专用网技术。第 9 章主要内容有因特网的安全、Web 站点安全、黑客、口令安全、网络监听、扫描器、E-mail 的安全和 IP 电子欺骗等。第 10 章讲述数据的完整性、容错与网络冗余和网络备份系统等基本

此为试读，需要完整PDF请访问：www.ertongbook.com

概念。第 11 章给出学习本书所必须做的实验和综合练习题。

本书是作者在多年教学实践的基础上编写的。在教材的编写过程中，对基本概念、基础知识的介绍力求作到简明扼要；各章相互配合，又自成体系并附有小结和习题。为配合教学，本书同时还配有电子课件，需要的教师可从人民邮电出版社网站下载。建议本课程为 50 学时，其中讲课 40 学时，上机和课堂讨论 10 学时。学生应具备系统导论、操作系统、计算机网络和 C 语言的预备知识。

本书由袁津生、齐建东、曹佳编写，最后由袁津生统稿。在本书的修订过程中得到了众多老师的指导和帮助，在此特别感谢北京林业大学教务处韩处长和张戎老师，正是由于他们的帮助，本书才得以正常出版。

由于编写时间仓促，编者水平有限，书中难免有错误和不当之处，请读者批评指正。

袁津生

2007 年 8 月

目　　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　网络基础知识与因特网

计算机网络技术（Computer Network Technology）是当今世界最为激动人心的高新技术之一，它涉及计算机、通信、电子学、自动化、光电子和多媒体等诸多学科。它的出现和快速发展，特别是因特网的迅猛发展正在使世界成为一个整体。

网络是建设信息高速公路和实现现代化信息社会的物质及技术基础，它的迅速发展使世界更加绚丽多彩。

本章将要介绍网络参考模型、网络互连设备、局域网技术、广域网技术、TCP/IP 基础以及因特网提供的主要服务等。

1.1　网络参考模型

在各种类型计算机之间进行信息传递是一件比较困难和麻烦的工作。20 世纪 80 年代初期，国际标准化组织（ISO）认识到，需要一个网络模式来帮助厂商实现网络间的相互操作，于是在 1984 年发表了著名的开放系统互连（OSI）参考模型。这种模式是学习网络技术的最好的工具。

1.1.1　分层通信

在 OSI 参考模型中，将整个通信功能划分为七个层次。每一层的目的是向相邻的上一层提供服务，并且屏蔽服务实现的细节。模型设计成多层，像是在与另一台计算机对等层通信。实际上，通信是在同一计算机的相邻层之间进行的。七个层次自上而下分布，并具有不同的功能。每一层都按照一组协议来实现某些网络功能。七个层次之间的问题相对独立，而且易于分开解决，也无需过多地依赖于外部信息。

（1）应用层。应用层是 OSI 参考模型的最高层。它是应用进程访问网络服务的窗口。这一层直接为网络用户或应用程序提供各种各样的网络服务，它是计算机网络与最终用户间的界面。应用层提供的网络服务包括文件服务、打印服务、报文服务、目录服务、网络管理以及数据库服务等。

（2）表示层。表示层保证了通信设备之间的互操作性。该层的功能使得两台内部数据表示结构都不同的计算机（例如，一个设备使用某种编码，而另一个设备却使用另一种编码）能实现通信。它提供了一种对不同控制码、字符集和图形字符等的解释，而这种解释是使两台设备都能以相同方式理解相同的传输内容所必需的。表示层还负责为安全性引入的数据提供加密与解密，以及为提高传输效率提供必需的数据压缩及解压等功能。

（3）会话层。会话层是网络对话控制器，它建立、维护和同步通信设备之间的交互操作，保证每次会话都正常关闭而不会突然断开，使用户被挂起在一旁。会话层建立和验证用户之间的连接，包括口令和登录确认；它也控制数据的交换，决定以何种顺序将对话单元传送到传输层，以及在传输过程的哪一点需要接收端的确认。

（4）传输层。传输层负责整个消息从信源到信宿（端到端）的传递过程，同时保证整个消息无差错、按顺序地到达目的地，并在信源和信宿的层次上进行差错控制和流量控制。

（5）网络层。网络层负责数据包经过多条链路，由信源到信宿的传递过程，并保证每个数据包能够成功和有效率地从出发点到达目的地。为实现端到端的传递，网络层提供了两种服务：线路交换和路由选择。线路交换是在物理链路之间建立临时的连接，每个数据包都通过这个临时链路进行传输；路由选择是选择数据包传输的最佳路径。在这种情况下，每个数据包都可以通过不同的路由到达目的地，然后再在目的地重新按照原始顺序组装起来。

（6）数据链路层。数据链路层从网络层接收数据，并加上有意义的比特位形成报文头和尾部（用来携带地址和其他控制信息）。这些附加信息的数据单元称为帧。数据链路层负责将数据帧无差错地从一个站点送到下一个相邻站点，即通过数据链路层协议在物理链路上实现可靠的数据的传输。

（7）物理层。物理层是OSI参考模型的最低层，它建立在物理通信介质的基础上，作为系统和通信介质的接口，用来实现数据链路实体间透明的比特（bit）流传输。为建立、维持和拆除物理连接，物理层规定了传输介质的机械特性、电气特性、功能特性和过程特性。

在上述七层中，上五层一般由软件实现，而下面的两层是由硬件和软件实现的。

1.1.2 信息格式

信息在各层间的格式变化如图1-1所示。

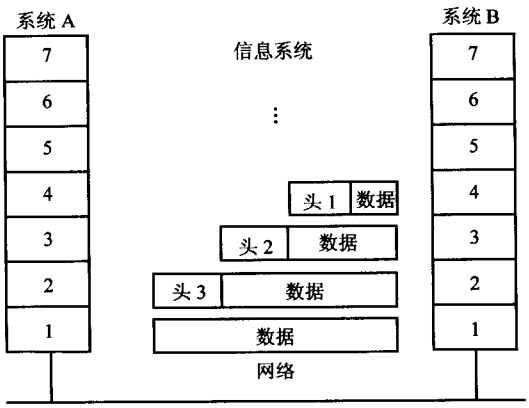


图1-1 信息在各层之间的传递

图1-1中，系统B的第n层（n<7）是如何知道系统A的第n层所做的处理呢？第n层将其请求作为控制信息，放在传送信息前面、被称为“头”的里面，当对方的第n层读到该头时，便可还原信息。

1.2　网络互连设备

网络互连设备是实现网络互连的关键，它们有 4 种主要的类型：中继器、网桥、路由器以及网关，这些设备在实现局域网（LAN）与 LAN 的连接中相对于 OSI 参考模型的不同层。中继器在 OSI 参考模型的第 1 层建立 LAN 对 LAN 的连接，网桥在第 2 层，路由器在第 3 层，网关则在第 4 至第 7 层。每种 Internet 设备提供的功能与 OSI 参考模型规定的相应层的功能一致，但它们都可以使用所有低层提供的功能。

各种网络互连设备在 OSI 参考模型 7 层中的位置如图 1-2 所示，其作用见表 1.1。

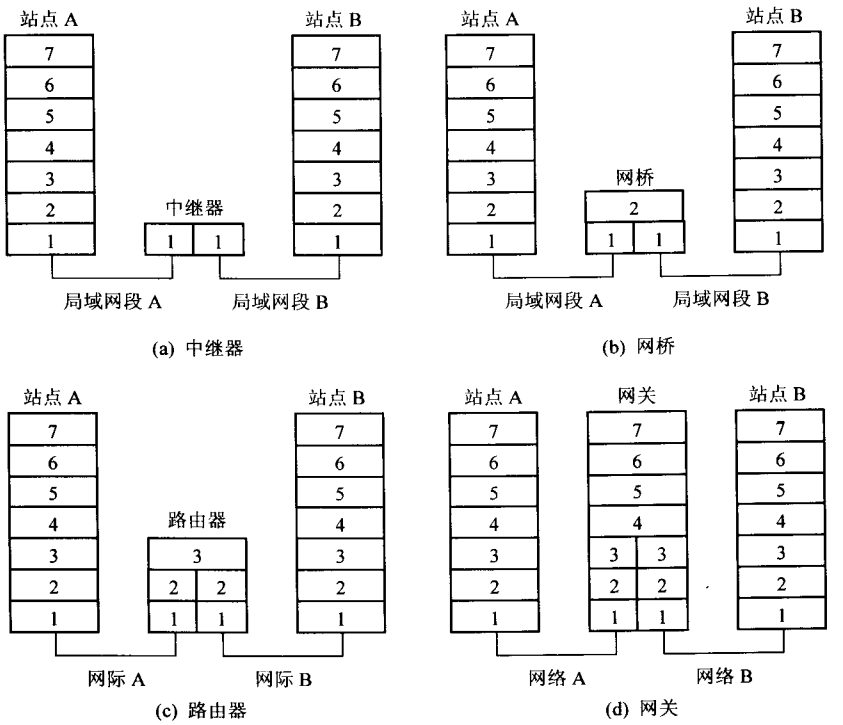


图 1-2　网络互连设备的功能层次

表 1.1　　**网络互连设备的作用**

OSI 层次	互 连 设 备	作　用	寻 址 功 能
物理层	中继器	在电缆段间复制比特	无地址
数据链路层	网桥	在 LAN 之间存储转发帧	MAC 地址
网络层	路由器	在不同的网络间存储转发分组	网络地址
传输层及以上	网关	提供不同体系间互连接口	

下面分别介绍 4 种主要类型的网络互连设备。

1.2.1 中继器和集线器

因特网中最简单的设备是中继器（Repeater），它的作用是放大电信号，提供电流以驱动长距离电缆。它工作在 OSI 参考模型的最低层（物理层），因此只能用来连接具有相同物理层协议的 LAN。对于数据链路层以上的协议来讲，用中继器互连起来的若干段电缆与单根电缆之间并没有差别（除了有一定的时间延迟）。中继器主要用于扩充 LAN 电缆段（Segment）的距离限制。如粗线以太网，由于收发器只能提供 500m 的驱动能力，而 MAC（介质访问控制）协议的定时特性允许粗以太网电缆最长为 2.5km。这样在每隔 500m 的网段之间就要利用中继器来连接。值得注意的是，中继器不具备检查错误和纠正错误的功能，因此错误的数据经中继器后仍被复制到另一电缆段。另外，中继器还会引入时延。使用中继器时应注意以下两点。

（1）用中继器连接的以太网不能形成环路。

（2）必须遵守 MAC 协议定时特性，即不能用中继器将电缆段无限连起来。例如，一个以太网上最多有 4 个中继器，连接 5 个电缆段。

灵活利用中继器，可以让总线型以太网适用多种布线结构变化。如一幢办公大楼分成多层，如果用逐层电缆绕线，不但浪费电缆，而且出故障时查找也不方便。如果用一根垂直的电缆穿过大楼，每层用中继器引入一水平电缆连起来则十分方便，这种配置一般垂直电缆用粗线，水平电缆用细电缆。

集线器（Hub）的工作原理与中继器类似，只是它能对更多的设备进行中继。注意，绝大多数集线器只能以双绞线介质连接，而中继器主要用同轴电缆进行连接。有些集线器只是集中连接的简单硬件设备（称作被动集线器）；有些则是复杂的电子部件，它们对到达各个物理位置的信息流进行监视和控制（称作主动集线器）。

1.2.2 网桥

网桥（bridge）是一种在数据链路层实现互连的存储转发设备，它独立于高层设备，或者说与高层协议无关。它在两个局域网段之间对链路层帧进行接收、存储与转发，它把两个物理网络（段）连接成一个逻辑网络，使这个逻辑网络的行为看起来就像一个单独的物理网络一样。网桥通过数据链路层的逻辑链路控制子层（LLC）来选择子网路径。它接受完整的链路层帧，并对帧进行校验，然后查看介质存取控制层（MAC）的源地址和目的地址以决定该帧的去向。网桥在转发一帧前可以对其作一些修改，如在帧头加入或删除一些字段。由于网桥与高层协议无关，原则上网桥可以互连，如 DEC 网、TCP/IP 网或 XNS 网络。不过在实际应用中，网桥只有连接协议一致才能使用，如两个 802.X 网络，只有当它们都采用相同的网络操作系统才有价值；如果高层协议不一样，既便用网桥连接起来，应用程序也不能交换信息。

与上面介绍的中继器相比，网桥具有以下特点。

（1）可以实现不同类型的 LAN 互连，而中继器只能实现以太网段间的相连。例如，用网桥可以把以太网和令牌环网（token ring）连起来。

（2）利用网桥可以实现大范围局域网的互连。由于中继器受 MAC 定时特性的限制，一般只能将 5 段以太网连接起来，且不能超过一定的距离。但网桥工作在数据的链路层，不受

此为试读，需要完整PDF请访问：www.ertongbook.com