21世纪高等院校计算机教材系列

计算机网络构建与安全技术

●俞承杭　主编

购书可获得增值回报
提供教学用电子教案

机械工业出版社
CHINA MACHINE PRESS

21 世纪高等院校计算机教材系列

计算机网络构建与安全技术

俞承杭　主　编
梁冲海　赵志刚　等编著

机 械 工 业 出 版 社

本书首先介绍必要的计算机网络基础知识，再从组建局域网（LAN）开始，通过硬件连接、软件安装配置、各种服务器架设等步骤完成整个网络的组建工作。书中介绍了网站制作技术；通过互联网接入技术，完成LAN与外界网络的互联与服务器发布。在网络与信息安全技术方面，主要从系统保护的角度，介绍了信息内容安全、网络系统安全和管理安全所涉及的技术。

本书适合作为信息管理专业、电子类专业和自动化类专业应用型本、专科相关课程的教材，并适合作为公共计算机网络和信息安全课程的教材。

图书在版编目（CIP）数据

计算机网络构建与安全技术/俞承杭主编．—北京：机械工业出版社，2008.1
（21世纪高等院校计算机教材系列）
ISBN 978-7-111-22903-2

Ⅰ.计… Ⅱ.俞… Ⅲ.①计算机网络－高等学校－教材 ②计算机网络－安全技术－高等学校－教材 Ⅳ.TP393

中国版本图书馆CIP数据核字（2007）第182402号

机械工业出版社（北京市百万庄大街22号 邮政编码 100037）
责任编辑：董 欣
责任印制：洪汉军

中国农业出版社印刷厂印刷

2008年1月第1版·第1次印刷
184mm×260mm·20.75印张·513千字
0001—5000册
标准书号：ISBN 978-7-111-22903-2
定价：33.00元

凡购本书，如有缺页，倒页，脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639 88379641 88379643
编辑热线电话：（010）88379739
封面无防伪标均为盗版

出 版 说 明

信息技术是当今世界发展最快、渗透性最强、应用最广的关键技术，是推动经济增长和知识传播的重要引擎。在我国，随着国家信息化发展战略的贯彻实施，信息化建设已进入了全方位、多层次推进应用的新阶段。现在，掌握计算机技术已成为21世纪人才应具备的基本素质之一。

为了进一步推动计算机技术的发展，满足计算机学科教育的需求，机械工业出版社聘请了全国多所高等院校的一线教师，进行了充分的调研和讨论，针对计算机相关课程的特点，总结教学中的实践经验，组织出版了这套“21世纪高等院校计算机教材系列”。

本套教材具有以下特点：

(1) 反映计算机技术领域的新发展和新应用。

(2) 注重立体化教材的建设，多数教材配有电子教案、习题与上机指导或多媒体光盘等。

(3) 针对多数学生的学习特点，采用通俗易懂的方法讲解知识，逻辑性强、层次分明、叙述准确而精炼、图文并茂，使学生可以快速掌握，学以致用。

(4) 符合高等院校各专业人才的培养目标及课程体系的设置，注重培养学生的应用能力，强调知识、能力与素质的综合训练。

(5) 适合各类高等院校、高等职业学校及相关院校的教学，也可作为各类培训班和自学用书。

机械工业出版社

前　言

在计算机应用网络化的时代里，互联网的海量信息、日常事务的网络化处理等特征，使得具备一定的网络知识、网络组建技能、网络管理和维护技术，掌握防病毒、防攻击、信息保密等信息安全技术，有效保证身边的网络或计算机稳定、安全地运行等技能，已经不再是网络管理员所专有，而是对使用网络的人员提出的普遍要求。本教材课题组调研了若干所高校非计算机专业的网络相关课程的教学大纲、专业应用需求特点，经过多个轮次的实际教学，形成了目前的教学体系结构。本书适用于公共计算机网络教学，也适用于要求较高的电子、信息、管理等专业的网络课程教学。

全书内容分为四个部分。

第一部分由第 1 章和第 2 章构成，介绍计算机网络的一般知识和利用 Windows 2003 软件组建局域网的体系特点。

第二部分由第 3 章至第 8 章构成，介绍了 Windows 2003 网络的具体构建过程。从服务器软件安装开始，介绍了 TCP/IP 设置，WWW、FTP、Email、流媒体等应用服务器的架设，最后介绍了如何将建设好的局域网接入到互联网中，使内部网络融入互联网应用中。本部分还介绍了网站开发工具及其应用。

第三部分由第 9 章至第 11 章构成，针对当前严峻的信息安全问题，从网络安全技术、信息内容安全技术、网络管理与维护技术等几个方面，介绍了维持网络稳定运行、保证用户的信息安全的方法。为确保万无一失，还介绍了数据备份与恢复技术。

第四部分是我们精心组织的实验，针对教学内容，通过工具软件，特别是网上共享的工具软件，加深学生对教学内容的理解和掌握。这部分中还介绍了功能强大的虚拟计算机软件 VMWare。使用该软件可使学生在一台计算机中完成网络实验。

本课程建议授课学时为 51 学时，其中实验不少于 20 学时，并可根据专业需求适当调整。本书中所介绍的实例或实验都在 Windows 2003 环境下调试通过。按教材的组织步骤完成实验，即可成功搭建好一个稳定安全、功能齐全的网络应用环境。

本书由俞承杭任主编。具体分工为：第 1 章和第 2 章由李慧编写，第 3 章和第 7 章由梁冲海编写，第 4 章至第 6 章由赵志刚编写，第 8 章至第 11 章由俞承杭编写；第 12 章由俞承杭和朱根良编写。全书由俞承杭统稿。

本书提供完整的电子课件，读者可到机械工业出版社网站 www.cmpedu.com 下载。此外，本书作者还收集了完整的实验素材，并制作了各实验的课件，需要这些资料的读者请与作者联系（net05info@163.com）。

由于时间仓促，书中难免存在不妥之处，请读者原谅，并提出宝贵意见。

作　者

目　录

第 1 章　计算机网络概论

本章介绍计算机网络、数据通信、网络拓扑结构、网络体系结构、网络硬件以及网络操作系统等基础理论知识，这是学习本书后续内容的必要准备。

1.1　概述

1.1.1　计算机网络的发展

计算机网络是计算机技术和通信技术相结合的产物。计算机网络从问世以来，经历了从简单到复杂、从初级到高级的发展过程，并已深入到人们工作、学习和生活的方方面面。纵观计算机网络的形成与发展，大致可以分为四个阶段。

第一阶段为计算机网络的初级阶段。以形成具有通信功能的“终端—通信线路—计算机”系统为主要形式，实现了计算机技术与通信技术的结合，以及对数据通信技术与计算机通信网络的研究，为计算机网络的产生奠定了理论基础。美国于 20 世纪 50 年代建立的半自动化地面防空系统 SAGE 就属于这一类网络，它把远程雷达及其他设备测量到的数据信息通过通信线路送到一台计算机上进行处理和控制，首次实现了计算机技术与通信技术的结合，是计算机通信发展史上的里程碑。

第二阶段为计算机网络的形成阶段。计算机网络的通信方式由终端与计算机之间的通信，发展到计算机与计算机之间的直接通信。美国于 20 世纪 60 年代建成的 ARPAnet 就是这一阶段的代表，它首先实现了以资源共享为目的的不同计算机互联的网络，标志着计算机网络的发展进入了第二代，奠定了计算机网络技术的基础，成为今天因特网的前身。

第三阶段为标准化的计算机网络阶段。随着计算机网络的迅速发展，产生了网络体系结构与网络协议的国际标准化问题。为了使不同体系结构的网络都能互联，国际标准化组织(ISO)于 1977 年成立了专门机构研究并制定网络通信标准，以实现网络体系结构的标准化。1984 年，国际标准化组织(ISO)颁布了开放系统互联基本参考模型(OSI/RM)，它的提出引导着计算机网络走向开放的标准化的道路，标志着计算机网络的发展进入了成熟的阶段，同时对网络理论体系的形成与网络技术的发展起到了重要的作用。

第四阶段为高速、智能的计算机网络阶段。从 20 世纪 80 年代末开始，计算机技术、通信技术及建立在互联网络技术基础上的计算机网络技术得到迅猛发展，特别是 90 年代后，随着光纤通信技术的应用和多媒体技术的迅速发展，计算机网络正朝着综合化和高速化方向发展，从而进入了一个新的发展阶段。在网络高速化发展的同时，用户对网络的可靠性、安全性和可用性提出了新的要求。为了向用户提供更高的网络服务质量，网络管理也逐渐进入了智能化阶段。

1.1.2 计算机网络的组成

我们从计算机网络的发展过程中可以看到，计算机网络是计算机技术和通信技术发展的产物，它充分体现了信息传输与分配手段和信息处理手段的有机联系，信息传输和资源共享是计算机网络最初的两个重要目的。那么，什么是计算机网络呢？

计算机网络是指将不同地理位置且功能相对独立的多个计算机系统通过通信线路相互连接在一起、由专门的网络操作系统进行管理，以实现资源共享的系统。

无论是哪一种计算机网络，从资源构成的角度来看，计算机网络是由硬件和软件组成的。但是，从计算机网络的数据通信和数据处理的功能角度来看，计算机网络可划分为两层：内层通信子网和外层资源子网，如图 1-1 所示。

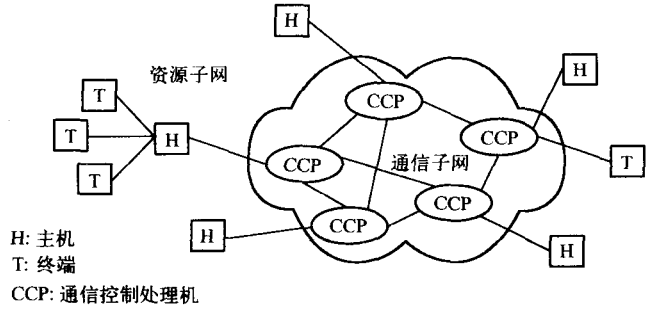

图 1-1　计算机网络的基本组成

1. 通信子网

通信子网主要由通信控制处理机、通信链路以及其他设备如调制解调器等组成，提供网络通信功能，完成主机之间的数据传输、交换和控制等通信任务。通信控制处理机(CCP)是一种具有通信控制功能的专用计算机，按照它的功能和用途，可以分为存储转发处理机、网络协议变换器和报文分组组装/拆卸设备等。通信链路是用于传输信息的物理信道以及为达到有效、可靠的传输质量所必需的信道设备的总称。一般来说，通信子网中的链路属于高速线路。调制解调器是一种能将数字信号调制成模拟信号，又能将模拟信号解调为数字信号的装置。不同类型的网络，其通信子网的物理组成各不相同。

局域网的通信子网较为简单，由传输介质和网卡组成。而在广域网中，通信子网除了包括传输介质和网卡之外，还包括一组转发部件，它主要起到通信控制与转发作用。

2. 资源子网

资源子网主要由主机、终端以及相应的 I/O 设备和各种软件资源构成，负责全网的数据处理业务，并向网络用户提供各种网络资源和网络服务。主机和终端是资源子网的主体设备。主机(Host)可以是大型机、中型机、小型机、工作站或微型机，它利用高速通信线路或 I/O 接口与通信控制处理机相连接。主机系统拥有各种终端用户要访问的资源，负责网络中的数据处理和网络控制等任务。终端(Terminal)是用户进行网络操作时所使用的末端设备，它的主要作用是将用户输入的信息转变为适合传送的数据格式送到网络上，或将网络上其他节点输出的经过通信线路的数据转变为用户所能识别的信息。终端的种类繁多，而且可以直接或通过通信控制处理机和主机相连。

通信子网和资源子网的划分，完全符合国际标准化组织（ISO）所制定的开放式系统互联参考模型（OSI）的思想。其中通信子网对应于 OSI 中的底三层（物理层、数据链路层、网络层），而资源子网对应于 OSI 中的高三层（会话层、表示层、应用层）。这种划分将通信子网的任务从主机中抽取出来，由通信子网中的设备专门解决数据传输和通信控制问题，而资源子网中的计算机可集中精力处理数据，从而提高主机效率和网络的整体性能。

1.1.3 计算机网络的分类

用于对计算机网络进行分类的标准很多。例如，按所使用的通信介质可分为有线网络和无线网络；按使用网络的对象分为公众网络和专用网络；按网络拓扑结构可分为总线网、星形网、环形网、树形网、网状网等。但是，这些分类标准都只能给出网络某一方面的特征。

在计算机网络中，一般来说传输距离影响着传输速率，距离越短，传输速率也就越高，而传输速率又极大地影响着计算机网络硬件技术的各个方面。为了反映网络技术的本质特性，人们通常按照网络覆盖范围的不同进行分类，把计算机网络大致分为局域网、城域网和广域网三大类。

1. **局域网**（Local Area Network，LAN）

局域网是指传输距离有限，传输速度较高，以共享网络资源为目的的网络系统。由于局域网投资规模较小，网络实现简单，故新技术易于推广。局域网具有如下特点：

- 网络所覆盖的地理范围比较小，一般在几千米以内（不超过 10 千米），甚至只在一幢建筑或一个房间内。
- 数据的传输速率比较高，从最初的 1 Mbit/s 到后来的 10 Mbit/s、100 Mbit/s，近年来已达到 1000 Mbit/s、10000 Mbit/s。
- 具有较低的延迟和误码率，其误码率一般为 10^{-8}～10^{-11}。
- 局域网络的经营权和管理权属于某个单位所有。
- 便于安装、维护和扩充，建网成本低、周期短。

尽管局域网地理覆盖范围小，但这并不意味着它们必定是小型的或简单的网络，局域网可以扩展得相当大或者非常复杂。一般来说，局域网的主要功能是为了实现资源共享，其次是为了更好地实现数据通信与交换以及数据的分布处理，而决定局域网特性的主要技术要素是网络拓扑结构、传输介质与介质访问控制方法。

局域网上的传输介质都是各工作站的共享资源，各工作站对于传输介质的使用权利是相同的。如果在某一时刻，同时有两个或多个站点发送信包，这些信包必将在传输介质上产生碰撞和叠加，导致接收站不能正确接收数据。为了避免这种“冲突”的产生，就要对传输介质的访问进行控制，也就是如何合理使用信道、合理分配信道。所以，传输介质的访问控制方式的功能，就是合理解决信道的分配。局域网的拓扑结构对网络的介质访问控制方法有较大的影响，因此，按网络拓扑结构的不同，我们主要介绍局域网标准中最常用的三种介质访问控制方法。

（1）带有冲突检测的载波侦听多路访问（CSMA/CD）控制方式

CSMA/CD 是一种采用争用的方法来决定对媒体访问权的协议，这种争用协议只适用于逻辑上属于总线拓扑结构的网络。在总线网络中，当某个节点要发送数据时，首先要侦听信道上有没有数据正在传送，即检测信道是否空闲。如果信道处于空闲状态则立即抢占信道发送数据；反之，如果信道正忙，则计算机会等待一段时间后再检测信道的状态，直到空闲再传送数

据。但如果同时有多个节点侦听到信道空闲并发送数据，就可能发生冲突。CSMA/CD 采取了一种巧妙的解决方法，就是在发送数据的同时进行冲突检测，一旦发现冲突，便立即停止发送，并等待冲突平息后，再进行 CSMA/CD，重新去抢占信道，直至将数据成功地发送出去为止。为了便于理解和记忆，CSMA/CD 的工作原理可概括成四句话，即先听后发、边发边听、冲突停止、随机延迟后重发。

(2) 令牌环(Token Ring)访问控制方式

Token Ring 是令牌传递环(Token Passing Ring)的简写，只有一条环路，信息沿环单向流动，不存在路径选择问题。

在令牌环网中，有一个特殊格式的帧在物理环中沿固定方向逐站传送，这个特殊帧称为令牌。令牌是用来控制各个节点介质访问权限的控制帧。当一个节点需要发送数据，必须获得空闲令牌，并修改令牌帧中的标志，使其变为“忙”的状态，然后去掉令牌的尾部，加上数据，成为数据帧，发送到下一个节点。数据帧每经过一个节点，该节点就比较数据帧中的目的地址，如果不属于本节点，则转发出去；如果属于本节点，则复制到本节点的计算机中，同时在帧中设置已经复制的标志，然后向下一个节点转发。当数据帧通过闭环重新传到发送节点时，发送节点不再转发，而是检查发送是否成功。如果发现数据帧没有被复制(传输失败)，则重发该数据帧；如果发现传输成功，则清除该数据帧，并产生一个新的空闲令牌发送到环上。归纳起来，令牌环的工作原理可概括成三句话，即截获令牌并发送数据帧，接收与转发数据，取消数据帧并重发令牌。

(3) 令牌总线(Token Bus)访问控制方式

令牌总线访问控制方式是在综合了 CSMA/CD 访问控制方式和令牌环访问控制方式的优点基础上形成的一种介质访问控制方式。令牌总线控制方式主要用于总线型网络结构中，该方式是在物理总线上建立一个逻辑环，如图 1-2 所示，一个总线结构网络，如果指定每一个节点在逻辑上相互连接的前后地址，就可构成一个逻辑环，如图中 A→B→D→E→A(C 节点没有接入)。任何一个节点只有取得令牌才能发送帧，而令牌在逻辑环上依次循环传递。

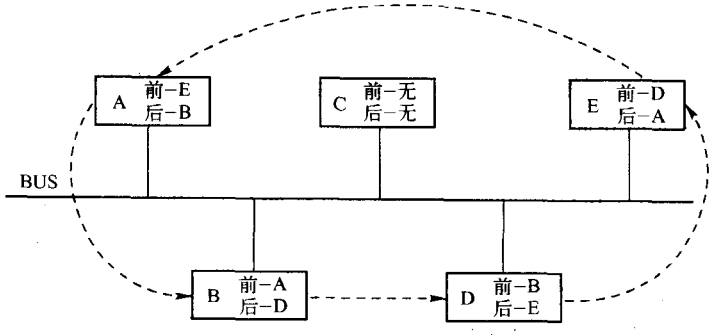

图 1-2　令牌总线访问控制方式

局域网发展到今天，在实际应用中已相当普及，最常见最普及的局域网技术包括以太网、令牌网和 FDDI 等。

(1) 以太网

目前，局域网几乎成了以太网(Ethernet)的代名词，人们通常所说的局域网大多指以太

网。以太网是当今世界上应用范围最广的一种网络技术，最早起源于美国的夏威夷大学，经过不断发展完善后，其相关技术已经十分成熟。

以太网组建和维护较为容易，各个设备之间的兼容性好，目前主流操作系统 Windows、NetWare 和 Linux 都支持以太网。如无特别说明，一般提到的局域网都是指以太网。以太网按照其带宽标准，可分为标准以太网、百兆位以太网、千兆位以太网和万兆位以太网。

1）标准以太网。通常情况下，人们将以太网的第一个工业标准 IEEE802.3 定义的以太网称为标准以太网，它以直径为 1 cm 的同轴电缆为通信介质，电缆电阻为 50 Ω，最大传输距离为 200 m，每段电缆最多可连接 100 个节点，数据传输速率为 10 Mbit/s。标准以太网采用总线型拓扑结构，通常称为 10Base2 网络。IEEE 通常使用一种简易的命名方法表示各类以太网，例如 10Base2 各部分的意义如下：

- 10 表示网络带宽为 10 Mbit/s。
- Base 表示信号类型为“基带”，基带网络以数字信号传递数据，宽带网络以模拟信号传递数据。
- 2 表示通信介质的最大传输距离为 200 m。
- 此外，以太网支持的介质不同，介质代码也不同，例如 T 代表非屏蔽双绞线，F 代表光纤。

2）百兆位以太网。提高以太网传输速率最直接的方法就是增加其带宽。1995 年，IEEE 正式通过 802.3u 工业标准，即 100BaseT 快速以太网的标准，百兆位以太网由此诞生。百兆位以太网是目前市场的主流，共有 4 种不同的类型：

- 100BaseTX：问世于 1993 年，采用 5 类 UTP（非屏蔽双绞线）为通信介质，完全兼容 10BaseT 以太网。
- 100BaseT4：使用内含四对双绞线的 3 类以上 UTP 为通信介质。
- 100BaseFX：使用内含两束光纤的电缆为通信介质。
- 100BaseT2：1997 年，IEEE 推出了百兆位以太网的第 4 种规格 IEEE 802.3y，采用内含两对 3 类以上的 UTP 为通信介质。

上述几种百兆位以太网的主要区别在于所采用的通信介质类型不同，由于目前 5 类以上 UTP 是双绞线的主流产品，因此最常用的百兆位以太网属 100BaseTX。

3）千兆位以太网。1998 年通过的 IEEE 802.3z 工业标准，定义了超高速以太网的规格。超高速以太网必须拥有 1000 Mbit/s 的数据传输速率，因此通常称为千兆位以太网。IEEE 802.3z 定义了以下 3 种规格的千兆位以太网：

- 1000BaseSX：短波长激光光纤以太网，可使用 62.5 μm 或 50 μm 的多模光纤。
- 1000BaseLX：长波长激光光纤以太网，可使用 62.5 μm，50 μm 和 10 μm 的单、多模光纤。
- 1000BaseCX：采用两对 150 Ω 屏蔽双绞线（STP）为主要通信介质。

此外，IEEE 802.3z 标准附带了一个 1000BaseT 的条款，讨论有关利用 5 类以上的 UTP 构建千兆位以太网的规则。当前市场上可见的产品仍以 1000BaseSX 和 1000BaseLX 为主，价格偏高，集中应用在大型网络的骨干线上。

4）万兆位以太网。1999 年 IEEE 成立相关工作小组负责万兆位以太网标准的制定工作。这种以太网仍然采用 IEEE 802.3 以太网介质访问控制（MAC）协议、帧格式和帧长度，保持了高度的兼容性。