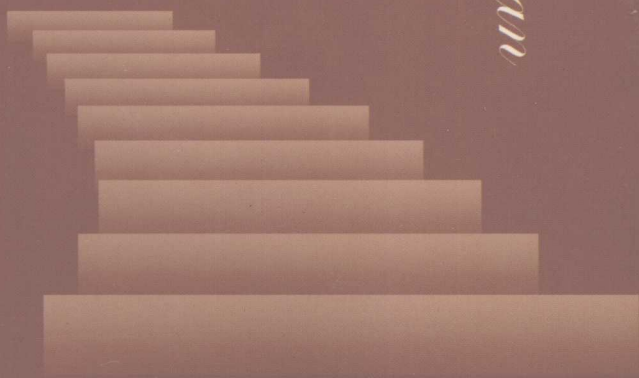


21
世纪
高职
高专
规划
教材

计算机应用系列

Jisuanji Wangluoguanli Yu Anquan



赵立群 主编

车亚军 车东升 副主编

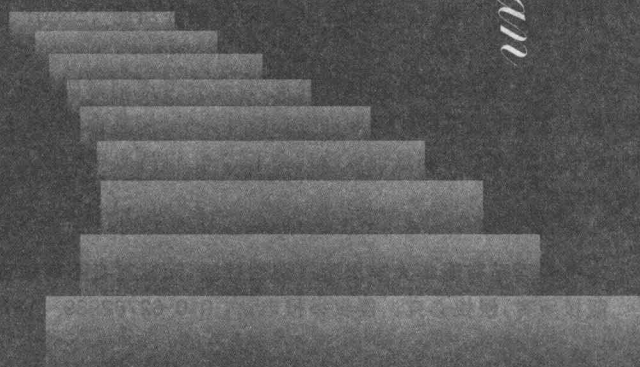
计算机网络管理 与安全

清华大学出版社



21世纪高职高专规划教材
计算机应用系列

Jisuanji Wangluoguanli Yu Anquan



赵立群 主编

车亚军 车东升 副主编

计算机网络管理 与安全



清华大学出版社
北京

内 容 简 介

计算机网络安全既是推进信息化的基础保障,也是信息系统正常运行的关键环节。本书针对高职高专的教学特点,坚持实用技术和实际案例相结合的原则,注重操作能力和实践技能的培养,以管理与安全为主线,介绍当前计算机网络管理与安全的主要技术与工具。内容包括:基于 Windows 2003 的活动目录管理方法、Windows 2003 网络服务功能、SNMP 协议,以及加强计算机网络安全管理等技术应用。

本书的实用性和操作性并重,且充分考虑到高职学生的特点和社会需求,注重学生实践能力的培养。本书不仅适用于高职高专院校计算机、信息管理、电子商务、物流管理等各专业的教学;也可作为企业从业人员在职培训以及社会 IT 人士提高应用技能与技术的教材;对于广大自学者也是一本有益的读物。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。侵权举报电话:010-62782989 13701121933

图书在版编目(CIP)数据

计算机网络管理与安全/赵立群主编. —北京:清华大学出版社,2008.10

21 世纪高职高专规划教材. 计算机应用系列

ISBN 978-7-302-17691-6

I. 计… II. 赵… III. ①计算机网络—管理—高等学校:技术学校—教材 ②计算机网络—安全技术—高等学校:技术学校—教材 IV. TP393

中国版本图书馆 CIP 数据核字(2008)第 074141 号

责任编辑:田 梅

责任校对:袁 芳

责任印制:李红英

出版发行:清华大学出版社

地 址:北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编:100084

社 总 机:010-62770175

邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 装 者:北京嘉实印刷有限公司

经 销:全国新华书店

开 本:185×260 印 张:16.5 字 数:379 千字

版 次:2008 年 10 月第 1 版 印 次:2008 年 10 月第 1 次印刷

印 数:1~4000

定 价:25.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770177 转 3103 产品编号:023714-01

编委会

主 任：牟惟仲

副主任：	王纪平	吴江江	冀俊杰	赵志远	郝建忠	鲁瑞清
	张昌连	冯仁华	李 弘	周 平	仲万生	林 亚
	王茹琴	张建国	王 松	米淑兰	宁雪娟	李大军
编 委：	宋承敏	孟震彪	刘长鑫	付绪昌	侯 杰	沈 煜
	马爱杰	李贵保	白文祥	栾茂茹	卫停战	孟乃奇
	王伟光	李书胜	李敬锁	阚晓芒	高光敏	王 玲
	王 凯	赵 茜	盛定宇	孟繁昌	赵立群	车东升
	赵宝生	侯貽波	刘 健	金 颖	徐 爽	李 多
	董 铁	王 谨	都日娜	贾 晖	万 纓	李 昊
	关 忠	赵春利	马 涛	田 颖	李春艳	闫秋冬

总 编：李大军

副总编：武信奎 车亚军 延 静 梁 露 吴 霞

序言

针对我国高职教育“计算机应用”等信息技术应用专业知识老化、教材陈旧、重理论轻实践、缺乏实际操作技能训练等问题,为了适应我国国民经济信息化发展对计算机应用人才的需要,为了全面

IV 贯彻教育部关于“加强职业教育”的精神和“强化实践实训、突出技能培养”的要求，根据企业用人与就业岗位的真实需要，结合高职高专院校“计算机应用”和“网络安全”等专业的教学计划及课程设置与调整的实际情况，我们组织北京联合大学、北方工业大学、北京财贸职业学院、首钢工学院、北方工业技术学院、北京石景山社区学院、北京城市学院、北京西城经济科学大学、北京朝阳社区学院、北京宣武社区学院、黑龙江工商大学等全国 30 多所高校及高职院校多年在一线从事计算机教学的主讲教师和具有丰富实践经验的企业人士共同撰写了这套教材。

本套教材包括：《计算机基础实例教程》、《微机组装（DIY）与维护》、《多媒体案例教程》、《办公自动化应用技术》、《Visual Basic.NET 基础教程》、《SQL Server 数据库案例教程》、《网页设计与制作实用教程》、《中小企业网站建设与管理》、《计算机网络管理与安全》、《管理信息系统》、《电子商务案例》11 本书。在编写过程中，所有作者都自觉地以科学发展观为指导思想，严守统一的创新型格式化设计，采取任务制或项目制写法，贴近行业企业岗位实际，注重实用性技术与能力的训练培养，注重实践技能应用与工作背景紧密结合，同时也注重计算机、网络、通信、多媒体等现代化信息技术的新发展，使教材具有集成性、系统性、针对性、实用性、形式新颖和易于实施教学等特点。

本套教材不仅适合高职高专“计算机应用”和“网络安全”等专业及经济管理、税务、财会、金融类各专业学生的学历教育，同时也可作为广大工商流通企事业单位从业人员的职业教育和在职培训，对于其他自学者也是一本有益的读物。

系列教材编委会

2007 年 7 月

前言

随着计算机技术与网络通信技术的飞速发展, 计算机网络应用已经渗透到社会经济领域的各个方面。 计算机网络技术是现代信息科学与技术的重要组成部分, 也是计算机管理信息系统的核心; 计算机网络管理与安全既是信息化推进的基础保障, 也是信息系统正常运行的关键环节, 因而备受世界各国高度关注。

本教材针对计算机网络管理与安全等方面存在的管理及技术问题, 按照教育部关于“加强职业教育、强化实践教学、突出技能和能力培养”教育教学改革精神, 根据计算机网络管理与安全课程教学规律和特点, 对原有的计算机网络管理、网络安全等内容进行了深度综合与提炼, 并注意打通相关知识联系, 采取了集成式写法。 本书内容包括: 基于 Windows 操作系统的活动目录管理方法、网络操作系统、网络管理、对因特网工作环境的支持、网络安全技术与应用、SNMP 协议管理等基本知识, 以及加强计算机网络安全管理等技术应用。

全书共 8 章, 采取新颖统一的格式化设计, 突出案例教学, 在案例的选择上具有实用性, 以学习者应用能力培养与提高为主线, 依照学习计算机网络管理与安全的基本过程和规律, 以任务剖析的方式, 结合知识要点循序渐进地进行讲解。 本书在引导读者对知识和技术理解与掌握的基础上, 通过多动手、多练习的方式, 提高实践应用技能, 注重动手能力的培养, 以达到学以致用目的。

目前, 世界正处于科学技术的高速发展期, 我国也正处在经济发展最活跃的时期, 面对激烈的市场竞争, 面对科技进步, 所有企事业单位都在科学发展观的统领下加快信息化进程, 加速信息技术应用, 特别关注和加强计算机网络管理与安全的监控。 当前面临企业拼发展, 面临社会就业上岗的巨大压力, 无论是企业员工、即将毕业的各类学生, 还是下岗转岗的待业人员, 努力学习和掌握计算机网络管理与安全的软件工具及技术应用, 不断提高业务技术素质, 对于今后的

FOREWORD

VI 发展都具有特殊意义。

本教材由李大军进行总体方案策划并具体组织，赵立群主编并统编全稿，车亚军和车东升为副主编，本书由具有丰富专业教学和企业实践经验的杜春涛教授审定。参加编写的人员有：车亚军（第1章），李多（第2章），王海珊（第3章），杨春（第4章），赵立群（第5章），孙钢凝（第6章），关忠（第7章），车东升（第8章）。

本书在编写过程中，广泛征集了各高等职业院校计算机网络管理与安全课程的主讲老师和有关企事业单位计算中心负责人对本书的修改意见与建议，得到了我国有关计算机行业协会的支持与帮助，得到了长期从事计算机教育教学有关专家教授的指导；在此，对参与本书出版论证与写作指导的牟惟仲、王纪平、张昌连、冀俊杰、吴明、林亚、储祥银、丁建忠、侯杰、沈煜、赵茜等同志一并表示衷心地感谢。由于时间紧，在编写过程中难免存在不足和疏漏，恳请各位专家及读者给予批评指正。

编 者

2007年7月

目录

第1章 基于操作系统的管理	1
1.1 网络操作系统的主要功能和工作模式	1
1.2 对等网模式下的管理	3
1.2.1 用户和组的管理	3
1.2.2 共享资源的管理	4
1.3 综合实训	5
1.4 活动目录的基本概念	15
1.4.1 域的概念	15
1.4.2 组织单元的概念	17
1.4.3 组的概念	18
1.4.4 用户的概念	19
1.5 活动目录的安装与卸载	20
1.5.1 活动目录的安装	20
1.5.2 活动目录的卸载	27
1.6 本章小结	32
1.7 本章习题	32
第2章 Windows Server 2003 域模式下管理	33
2.1 设置和管理用户与组	33
2.1.1 域模式下用户的设置与管理	35
2.1.2 域模式下组的设置与管理	43
2.1.3 域模式下对分区文件夹文件的管理	49
2.2 设置组织单位与配置客户端	52
2.2.1 管理组织单位	52
2.2.2 配置客户端	53
2.3 组策略	58
2.3.1 组策略的概念	58
2.3.2 组策略的内容	61

VIII	2.4 利用组策略进行管理	62
	2.4.1 创建和链接组策略对象	62
	2.4.2 利用组策略管理用户环境实例	65
	2.5 综合实训	71
	2.6 本章小结	75
	2.7 本章习题	76
	第3章 Windows 2003 服务器的架设	77
	3.1 DNS 服务器的架设	77
	3.1.1 DNS 原理	77
	3.1.2 DNS 的服务器安装	79
	3.1.3 在 DNS 服务器中创建搜索区域	80
	3.1.4 DNS 测试	90
	3.2 DHCP 服务器的架设	91
	3.2.1 DHCP 的运行方式	91
	3.2.2 DHCP 的工作原理	91
	3.2.3 DHCP 服务器的安装与设置	92
	3.3 IIS 的使用	98
	3.3.1 IIS 的介绍	98
	3.3.2 Web 站点的建立与管理	100
	3.3.3 FTP 站点的建立与管理	108
	3.4 综合实训	111
	3.5 本章小结	121
	3.6 本章习题	121
	第4章 信息安全	122
	4.1 网络安全概论	122
	4.2 加密技术	126
	4.2.1 数据加密基本概念	126
	4.2.2 对称数据加密技术	127
	4.2.3 非对称数据加密技术	132
	4.3 数字签名和报文鉴别	137
	4.3.1 数字签名	137
	4.3.2 报文鉴别和 MD5 算法	138
	4.4 信息安全技术在电子商务中的应用	139
	4.4.1 电子商务的安全概述	140
	4.4.2 电子商务中使用的安全协议	143
	4.5 实训: 数字证书的申请与应用	146
	4.6 本章小结	153
	4.7 本章习题	153



第5章 系统安全	154
5.1 Windows 2003 操作系统的安全性	154
5.1.1 Kerberos 身份认证	154
5.1.2 访问控制	157
5.2 防火墙技术	160
5.2.1 什么是防火墙	160
5.2.2 防火墙的基本技术	162
5.2.3 防火墙的体系结构	164
5.3 计算机病毒	166
5.3.1 计算机病毒的特点及分类	166
5.3.2 计算机病毒的工作过程	168
5.3.3 计算机防病毒技术	170
5.3.4 计算机病毒举例	172
5.4 黑客的攻击技术简介	173
5.4.1 黑客的进攻过程	173
5.4.2 黑客常用的攻击方法	175
5.4.3 黑客的常用工具	177
5.5 本章小结	180
5.6 本章习题	181
第6章 网络安全工具的使用	182
6.1 防火墙软件的使用案例	182
6.1.1 Windows Server 2003 防火墙	182
6.1.2 天网防火墙	185
6.2 防病毒软件的使用案例及经验	187
6.2.1 诺顿杀毒软件的使用方法	187
6.2.2 使用卡巴斯基的命令行方式对服务器进行杀毒	190
6.2.3 杀毒软件的选择	191
6.3 黑客攻防案例	192
6.3.1 入侵案例	192
6.3.2 防御案例	195
6.4 设置相对安全的 Windows Server 2003 系统	198
6.5 本章小结	203
6.6 本章习题	203
第7章 基于 SNMP 协议的管理	204
7.1 网络管理的概念	204
7.1.1 网络管理的内容	204
7.1.2 网络管理的体系结构	206
7.2 管理信息库	208



X	7.2.1 管理信息结构	208
	7.2.2 MIB-2 功能组	214
	7.3 SNMP 通信模型	216
	7.3.1 SNMP 协议数据单元	216
	7.3.2 SNMP 的安全机制	219
	7.3.3 SNMP 的操作	220
	7.3.4 SNMP 通信示例	222
	7.4 远程网络监视	228
	7.4.1 RMON 的基本概念	228
	7.4.2 RMON 的信息管理库	230
	7.4.3 RMON2 信息管理库	230
	7.5 本章小结	231
	7.6 本章习题	231
	第 8 章 网络管理软件	232
	8.1 网路岗软件的安装与验证	232
	8.1.1 软件的安装	232
	8.1.2 验证安装是否正确	235
	8.2 网路岗各种监控模式的介绍	235
	8.2.1 基于网卡监控	235
	8.2.2 基于 IP 监控	237
	8.2.3 基于账户监控	238
	8.3 NAT 功能和常见配置	241
	8.3.1 NAT 功能	241
	8.3.2 常见系统配置	243
	8.4 上网规则	245
	8.5 日志查阅、日志报表及远程控制中心	250
	8.5.1 日志查阅和日志报表	250
	8.5.2 远程控制中心	250
	8.6 本章小结	252
	8.7 本章习题	252



第 1 章

基于操作系统的管理

【本章内容】

本章主要介绍网络操作系统的概念和工作模式,同时介绍在对等网模式下 Windows 2003 的组网过程,讲解 Windows 2003 提供的域模式与对等网模式各自的特点,使读者对基于操作系统的管理有一个初步认识。

【本章重点】

- ① 了解 Windows 2003 操作系统提供的网络工作模式。
- ② 掌握用 Windows 2003 在对等网模式下组网的方法。
- ③ 理解域模式中的基本概念和网络设计规划应注意的主要问题,掌握活动目录安装、卸载操作;理解网络操作系统的功能。
- ④ 了解网络操作系统在共享资源管理上的基本特点。

操作系统是用户与计算机之间的接口,是计算机系统资源的管理者,用户可以通过操作系统方便地使用计算机系统。本书第 1 章到第 3 章主要从应用层面上介绍以操作系统为工具对网络中的资源及用户进行管理的基本方法。

1.1 网络操作系统的主要功能和工作模式

网络操作系统(Network Operating System, NOS)是使网络上各计算机方便而有效地管理本地及网络资源,为网络用户提供所需的各种服务的系统软件。网络操作系统除了应具有操作系统的功能之外,还应提供高效、可靠的网络通信能力以及多种网络服务功能。

单机操作系统必须具备以下两个方面的功能:

- (1) 为用户提供各种简便有效的访问本级资源的手段。
- (2) 合理地组织系统工作流程,有效地管理系统。

为了实现以上两个基本功能,需要在操作系统中建立各种进程,编写不同的功能模块,并按层次结构的思想将功能模块组织起来,以完成处理器管理、存储管理、设备管理、



2 文件管理和作业管理等任务。

随着计算机网络技术的发展,各种规模的局域网纷纷被建立起来。传统的单机操作系统只能为本地用户使用本机资源提供服务,不能满足开放的网络环境的要求,对于联网的计算机系统,其资源既是本地资源,又是网络资源;既要为本地用户提供资源共享服务,又要为网络中的远程用户提供服务。网络操作系统的基本任务就是屏蔽本地资源与共享资源的差异,为用户提供各种基本的网络服务功能,完成网络共享系统的资源管理并提供网络系统的安全服务。

因此网络操作系统除了具有单机操作系统的功能外,还应具有以下功能:

(1) 网络通信管理负责实现网络中计算机之间的通信。

(2) 对网络中软硬件资源实施有效的管理,以保证用户方便、正确地使用这些资源,提高资源的利用率。

(3) 提供网络访问的安全措施,保证系统中共享资源的安全性。

(4) 提供网络服务,包括文件传输服务、打印服务、电子邮件服务等。

网络操作系统是网络的心脏和灵魂,是计算机网络不可缺少的系统软件,一个网络操作系统是一个复杂的计算机程序集合,它提供网络操作过程的协议或行为准则,没有网络操作系统,计算机网络就无法工作。一台计算机通过网络操作系统能访问同一网络的所有共享资源。

计算机网络在操作系统的干预下,有 3 种工作模式:对等网模式、工作站/服务器模式、客户机/服务器模式。

(1) 对等网模式

网络中每台计算机的地位是平等的,既可以给其他计算机提供服务充当服务器,也可以向其他计算机索取服务充当客户机,网络中不存在明确的服务器和客户机。对等网模式如图 1-1 所示。

(2) 工作站/服务器模式

网络以服务器为中心,严格地定义了每一个实体的工作角色,即网络上工作站无法在彼此之间进行文件传输,要通过服务器作为媒介,所有文件的读取、消息传送等是在服务器掌握之中。工作站/服务器模式如图 1-2 所示。

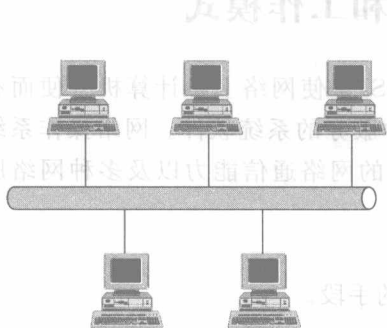


图 1-1 对等网模式

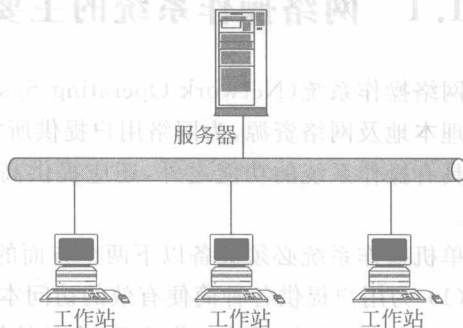


图 1-2 工作站/服务器模式

(3) 客户机/服务器模式(主从模式)

由客户机、服务器上的各种服务程序构成的一种网络计算机环境,把应用程序要完成的任务分派到客户机和服务器上共同完成,其中的客户机和服务器并没有一定的严格界限,而取决于运行的软件。在客户机/服务器模式中,服务器所提供的不仅是文件、数据库功能,还有计算、通信等能力。工作时,由客户机和服务器各自负担部分计算或通信功能。客户机/服务器模式如图 1-3 所示。

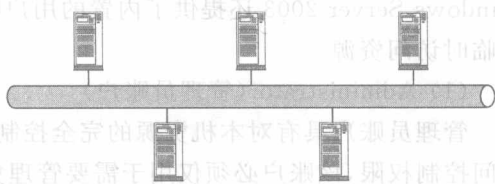


图 1-3 客户机/服务器模式

3 种模式各自的优缺点,如表 1-1 所示。

表 1-1 3 种模式的比较

工作模式	优点	缺点
对等网	结构简单,资源直接共享,任何两台计算机可以直接通信	每台计算机以双重身份工作,负担重
	不需专用服务器	数据保密性差 管理分散
工作站/服务器	可以按照不同的需要给予使用者相应的权限	多个使用者使用同一文件时,效率会降低
	文件安全管理较好	工作站资源不能直接共享 一旦服务器有问题,将影响全网
客户机/服务器	任务由服务器、客户机分担,执行速度快。发生故障时,网络不会崩溃	管理较为复杂
	扩大系统时,容易加挂服务器或客户机 安全性好	开发环境较为困难

目前,网络操作系统并非只有一种,而是存在着多种操作系统。常见的有 Windows、Netware、UNIX 等。在这里只讲 Windows 2003,它的工作模式只有对等网和主从网两种。

1.2 对等网模式下的管理

Windows 2003 的对等网工作模式是以工作组方式来实现的,采用工作组组织方式的对等网具有以下特点:

- 工作组中的所有计算机之间是一种平等的关系;
- 工作组模式下资源和账户的管理是分散的;
- 每台计算机上有一套本地安全数据库,用来验证在本机登录的用户。

1.2.1 用户和组的管理

1. 用户的管理

在对等网模式中,采用本地用户账号的方式对用户进行管理。如果想使用某台计算机上的资源,就必须要在该计算机上有相应的账号,并且该账号对资源有一定的访问权

4 限。权限是与对象(通常是文件、文件夹或打印机)相关联的一种规则,它规定哪些用户可以访问该对象以及以何种方式访问。用户账户包含了用户唯一的身份标识。在对等网模式下,可以创建本地用户账号。Windows Server 2003 还提供了内置的用户账户,用于协助用户进行日常的管理任务,或者临时访问资源。

(1) Administrator(管理员账户)

管理员账户具有对本机资源的完全控制权限,可以根据需要创建用户并指派相应的访问控制权限,该账户必须仅用于需要管理凭据的任务。由于大多数人都知道管理员这个账户,为了安全起见,可以将此账户设置为使用强密码或者重命名后赋予其最低的权限来进行保护。

(2) Guest(访客账户)

Guest 账户由在这台计算机上没有实际账户的用户使用。Guest 账户不需要密码。默认情况下,Guest 账户是禁用的,但也可以启用它。

可以设置 Guest 账户的权利和权限,设置方式与其他用户一样。默认情况下,Guest 账户是默认的 Guest 组的成员。默认情况下将禁用 Guest 账户,并且建议将其保持禁用状态。

2. 组的管理

如果多个用户对同一个资源有相同的访问权限时,逐个设置显然是非常愚蠢的事情,这时可以引入组的概念。组是用户账号的集合,可以将对网络资源中拥有相同的控制和访问权限的用户组织在一起,集中授权,统一管理。在对等网模式下,可以创建本地组。本地组是一种安全组,只被赋予了对创建该组的计算机上的资源进行访问的权利和权限。

关于对等网模式中用户和组的管理操作,将在 1.3 节的综合实训中作详细介绍。

1.2.2 共享资源的管理

在对等网中是通过共享文件夹的设定来实现资源的共享。共享文件夹的设定方法非常简单,具体操作如下:

(1) 右击需要共享的文件夹,在出现的快捷菜单中选择“共享”命令,如图 1-4 所示。

(2) 在弹出的文件夹属性对话框中,选择“共享该文件夹”单选按钮,然后在“共享名”文本框中输入该共享文件夹的共享名称,如图 1-5 所示。

(3) 默认情况下,系统对设置共享的文件夹都给 everyone 用户组完全控制的权限,当然这样做从安全角度考虑是非常不保险的,所以建议管理员根据情况适当改变权限。可通过单击“权限”按钮进行修改。

(4) 设置共享后,文件夹将会变成带有蓝色手形标志的共享文件夹图标。

不过要注意的是,在 Windows 2000/2003 系统中,有一种共享文件夹是在网上看不到的,那就是系统本身用于管理的共享文件夹,这类共享文件夹的共享名后面都带有一个“\$”,如图 1-6 所示。

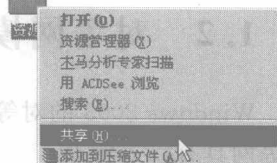


图 1-4 资源共享

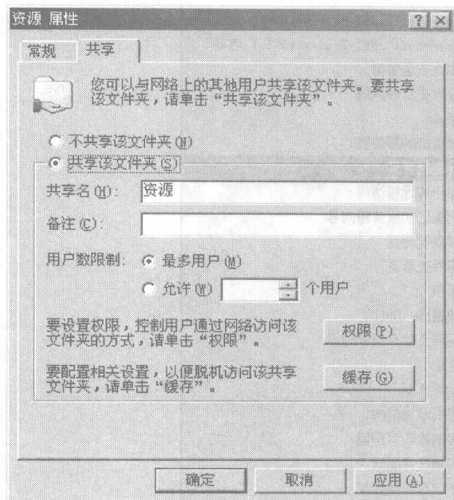


图 1-5 设置共享

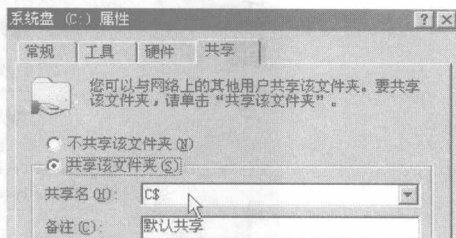


图 1-6 隐藏共享

这类共享文件夹通常是逻辑磁盘,这主要是出于安全和管理方面考虑的。用户虽然在“网上邻居”中看不到这类共享文件夹,但实际上该共享文件夹是存在的,用户输入“\计算机名\共享名\$”即可进入相应文件夹。

通过以上各步的配置,其他用户现在就可以通过“网上邻居”查看其他计算机上的共享资源了。在“网上邻居”中双击“选择邻近的计算机”选项即可显示对等网中所有计算机。要查看某计算机的共享资源,只需双击相应计算机名称即可。

1.3 综合实训

实训目的:

- (1) 通过本实训理解工作组模式的特点。
- (2) 通过本实训学会在工作组环境下进行资源的共享访问。

实训案例:

计算机 A 上 C 盘根目录有一个“教务处”文件夹,里面存储有一些供其他用户访问的文件。现要建立一个用户组“教务处组”,使得该组中的用户可以对“教务处”文件夹完全控制。计算机 B 的 C 盘上有“管理系”文件夹,要求建立一个“管理系组”的用户组,使得该组可以对“管理系”文件夹有完全控制权限。计算机 C 中建立一个用户名为 user3,密码为 abc123,要求用户 user3 可以通过计算机 C 访问计算机 A 上共享文件夹“教务处”及计算机 B 上共享文件夹“管理系”。

假设:计算机 A、B 的操作系统为 Windows Server 2003,计算机 C 的操作系统为 Windows XP 专业版。

1. 计算机 A、B、C 的共享资源设置

- (1) 在计算机 A 上选择“开始”→“所有程序”→“管理工具”→“计算机管理”命令,如图 1-7 所示。