全国高职高专教育“十一五”规划教材

网络安全运行与维护

第一册 操作系统安全管理与维护

龚小勇 张选波 主 编
安淑梅 唐继勇 副主编

高等教育出版社
HIGHER EDUCATION PRESS

全国高职高专教育“十一五”规划教材
国家精品课程配套教材

网络安全运行与维护

Wangluo Anquan Yunxing yu Weihu

第一册　操作系统安全管理与维护

Di Yi Ce　Caozuo Xitong Anquan Guanli yu Weihu

龚小勇　张选波　主　编
安淑梅　唐继勇　副主编

高等教育出版社·北京
HIGHER EDUCATION PRESS　BEIJING

内容提要

本书是全国高职高专教育“十一五”规划教材，是国家精品课程“网络安全运行与维护”的配套教材。

本书主要从应用的角度出发，全面介绍 Windows、Linux 桌面系统及服务器系统的安全运行与维护，不仅介绍有关 Windows、Linux 操作系统本身的安全问题，还包含一般用户在使用 Windows、Linux 操作系统完成日常工作的过程中可能遇到的各种安全风险，提出解决和预防的办法。

全书通过 4 个模块，由浅入深、循序渐进地介绍 Windows 桌面系统安全管理与维护、Windows 服务器系统安全管理与维护、Linux 桌面系统安全管理与维护、Linux 服务器系统安全管理与维护。内容包括：Windows 或 Linux 桌面系统用户和文件系统管理，加强 Windows 或 Linux 操作系统主机安全访问权限的管理，使用防火墙规则、文件系统加密、本地安全策略、安全审计等保护操作系统安全，Windows 或 Linux 服务器系统中 DHCP、DNS、IIS 等服务的安全配置以及保护这些日常服务的安全技术等。

本书通过任务驱动方式对以上列举的技术内容进行讲解，让读者不仅能够了解如何提高计算机的整体安全性，还可以深入学习技术细节和原理。本书可以作为面向应用的高等院校、高等职业院校计算机及相关专业学生学习 Windows 或 Linux 系统安全基础课程的教材，也可作为希望了解 Windows 系统安全的管理人员、系统安全及审计方面的专业人员的自学教材。

图书在版编目（CIP）数据

网络安全运行与维护. 第 1 册，操作系统安全管理与维护 / 龚小勇，张选波主编. —北京：高等教育出版社，2010. 12

ISBN 978 - 7 - 04 - 030323 - 0

Ⅰ. ①网… Ⅱ. ①龚… ②张… Ⅲ. ①计算机网络 - 安全技术 - 高等学校：技术学校 - 教材②操作系统 - 安全技术 - 高等学校：技术学校 - 教材 Ⅳ. ①TP393. 08 ②TP316

中国版本图书馆 CIP 数据核字（2010）第 190227 号

策划编辑 许兴瑜　**责任编辑** 萧　潇　**封面设计** 于　涛　**责任绘图** 尹　莉
版式设计 王艳红　**责任校对** 刘　莉　**责任印制** 毛斯璐

出版发行	高等教育出版社	**购书热线**	010 - 58581118
社　　址	北京市西城区德外大街 4 号	**咨询电话**	400 - 810 - 0598
邮政编码	100120	**网　　址**	http://www. hep. edu. cn http://www. hep. com. cn
		网上订购	http://www. landraco. com http://www. landraco. com. cn
经　　销	蓝色畅想图书发行有限公司	**畅想教育**	http://www. widedu. com
印　　刷	国防工业出版社印刷厂		
开　　本	787 × 1092　1/16	**版　　次**	2010 年 12 月第 1 版
印　　张	12. 75	**印　　次**	2010 年 12 月第 1 次印刷
字　　数	310 000	**定　　价**	20. 50 元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　30323 - 00

前　言

在日新月异的信息时代，新知识、新标准层出不穷，技术的更新不断挑战传统专业课程的教学，致使大中专院校计算机学科专业课程的更新落后于技术的换代，教学内容和社会应用的脱节、实践教学能力的严重不足都给当前计算机学科专业技术人才培养提出极大挑战。基于此，由高校的专家联合来自厂商的信息安全工程师，开发了网络安全运行与维护课程，希望着重培养高等职业院校学生在网络安全领域实施和防范的能力。

为全面培养学生网络安全运行与维护岗位工作技能，本书按照从新手到专家的成长过程，循序渐进地组织相关的安全知识内容，希望学生通过学习能够胜任企事业单位信息安全系统的配置、管理和维护工作，完成包括本地桌面系统的安全维护、服务器系统的安全维护、网络传输系统的安全维护、信息系统安全加固方案设计与实施、信息安全产品的安装与配置、网络安全与设备故障排除等工作任务，具备其对应工作岗位的职业技能。

1. 关于模块化课程规划

本课程的规划遵循教育部高职高专电子信息类教学指导委员会（以下简称“教指委”）开发的“工作过程—支撑平台系统化课程”思想，课程规划前期在教指委的协调下与锐捷网络成立课程组，依托锐捷网络分布在全国的网络平台，针对“网络安全运行与维护”职业岗位能力展开了大量的市场调研工作。

课程组从反馈表中收集到近200项岗位能力，筛选出企业认同前50位的职业能力，形成本课程的能力单元。最后邀请来自锐捷网络、天融信、北京绿盟、趋势科技等多家企业的从事信息安全的专家参与，把企业认同前50位的职业能力按照任务相近度归类组合，形成17项能力模块，整合出表1的课程能力模块，规划每一项能力知识、能力和态度，形成本课程开发指导文件——“网络安全运行与维护”能力标准。关于课程能力标准文件，可访问课程网络平台：http://www.wlaqyx.com/res/。

表1　能力单元整合成能力模块

编　号	能 力 单 元	能 力 模 块
NS-001	Windows 桌面系统安装与配置能力	M1:Windows 桌面系统安装与配置能力
NS-002	Windows 桌面系统用户与文件系统管理能力	
NS-003	加强 Windows 主机安全访问权限的管理能力	M2:Windows 桌面系统安全管理与维护能力
NS-004	使用防火墙规则加强 Windows 桌面系统的防御能力	
NS-005	使用文件系统加密加强 Windows 文件系统的安全能力	
NS-006	使用本地安全策略加强 Windows 主机的整体防御能力	
NS-007	使用安全审计加强 Windows 主机的安全维护能力	
NS-008	Windows 系统活动目录安装与配置能力	M3:Windows 服务器系统安装与配置能力

续表

编　号	能 力 单 元	能 力 模 块
NS-009	Windows 系统 DHCP 服务安装与配置能力	M3:Windows 服务器系统安装与配置能力
NS-010	Windows 系统 DNS 服务安装与配置能力	
NS-011	Windows 系统 IIS 服务安装与配置能力	
NS-012	提高 Windows 系统活动目录服务安全访问能力	M4:Windows 服务器系统安全管理与维护能力
NS-013	加强 Windows 系统的 DHCP 服务的安全防御能力	
NS-014	加强 Windows 系统的 IIS 服务的安全防御能力	
NS-015	加强 Windows 系统的 DNS 服务的安全防御能力	
NS-016	Linux 桌面系统安装与配置能力	M5:Linux 桌面系统安装与配置能力
NS-017	Linux 桌面系统用户与文件系统管理能力	
NS-018	通过系统口令加强 Linux 系统安全防护能力	M6:Linux 桌面系统安全管理与维护能力
NS-019	加强 Linux 用户网络访问权限的安全控制能力	
NS-020	加强 Linux 文件系统安全访问的能力	
NS-021	使用安全审计加强 Linux 主机的安全维护能力	
NS-022	Linux 系统 Web 服务安装与配置能力	M7:Linux 服务器系统安装与配置能力
NS-023	Linux 系统 DHCP 服务安装与配置能力	
NS-024	Linux 系统 DNS 服务安装与配置能力	
NS-025	Linux 系统 FTP 服务安装与配置能力	
NS-026	Linux 系统防火墙安装与配置能力	
NS-027	加强 Linux 系统的 DNS 服务的安全防御能力	M8:Linux 服务器系统安全管理与维护能力
NS-028	加强 Linux 系统的 DHCP 服务的安全防御能力	
NS-029	提升 Linux 系统的 Web 服务的安全防御能力	
NS-030	加强 Linux 系统的 FTP 服务的安全访问及安全防御能力	
NS-031	使用 Linux 防火墙模块加强服务器的安全防御能力	
NS-032	安装与配置路由器的能力	M9:网络基础设备的基本配置能力
NS-033	安装与配置交换机的能力	
NS-034	配置和维护路由协议的能力	
NS-035	安全管理路由器与交换机的能力	M10:网络基础设备的安全配置能力
NS-036	配置访问控制的能力	
NS-037	实施接入层安全的能力	
NS-038	配置安全路由协议的能力	
NS-039	实施身份验证与网络接入控制能力	
NS-040	安装与配置硬件防火墙的能力	M11:网络安全设备配置能力
NS-041	安装与配置入侵检测系统的能力	
NS-042	使用 Windows 系统服务器实现 VPN 服务的能力	M12:实施和配置数据传输安全的能力
NS-043	使用 Linux 系统服务器实现 VPN 服务的能力	
NS-044	使用路由器实现 VPN 功能的能力	
NS-045	使用 VPN 网关实现 VPN 功能的能力	

续表

编　号	能 力 单 元	能 力 模 块
NS-046	提高园区网络互连系统的安全运行与管理维护能力	M13:网络互连系统安全运行与维护能力
NS-047	提高企业网络互连系统的安全运行与管理维护能力	
NS-048	提高园区网网络行为的控制和防御能力	M14:网络行为控制与防御能力
NS-049	提高企业网网络行为的控制和防御能力	
NS-050	提高网络安全故障与设备故障排除的能力	M15:网络安全技术与设备故障排除流程、技巧能力
NS-051	就业能力	M16:就业能力
NS-052	创业能力	M17:创业能力

2. 关于本课程的能力培养

本书是“网络安全运行与维护”核心课程体系第一册，主要从应用角度全面介绍 Windows、Linux 桌面系统及服务器系统的安全运行和维护，全书不仅介绍有关 Windows、Linux 操作系统本身的安全问题，还描述用户在使用 Windows、Linux 操作系统完成日常工作的过程中可能遇到的各种安全风险，提出解决和预防的办法。

全书通过 4 个模块，由浅入深、循序渐进地介绍 Windows、Linux 桌面系统及服务器系统的安全运行和维护，着重培养计算机操作系统的安全管理和维护能力、操作系统的安全实施和防范能力。全书通过任务分配、任务分析、任务讲解到任务实施、验证测试这一过程，让学生不仅能够了解如何提高计算机操作系统的整体安全，还可以深入学习其中的技术细节。

3. 关于模块化课程的实施思想

“网络安全运行与维护”是信息安全专业的核心课程，由于网络安全运行与维护职业岗位涉及的知识体系较为复杂，为培养学生具备核心职业技能，根据网络安全运行与维护职业的成长规律，本书将介绍 Windows 系统安全和 Linux 系统安全两方面内容。

考虑本课程的使用阶段以及高等职业院校学生现有的安全知识水平，本书选择了 Windows 操作系统安全和 Linux 操作系统安全的部分模块。如需全面介绍操作系统的安全知识，还需配合其他课程模块（课程模块网站：http://www.wlaqyx.com/res/），以完成网络安全运行与维护职业岗位上从新手到专家的全部工作任务学习。

此外，通过抽离出本课程中部分模块，与其他课程模块进行组合，还可以服务于其他领域培训课程，满足不同人群对网络安全运维能力的需求。适用的培训课程包括：农民工安全培训课程，政府官员安全培训课程，IT 行业网络安全管理人员、非 IT 行业网络安全管理人员、IT 行业网络安全工程师、非信息安全专业高职学生培训课程。适用的课程模块如表 2 所示。

表 2　不同人群对网络安全运行与维护培训课程的需求

培 训 课 程	适用的课程模块
信息安全专业高职学生培训课程	M2+M4+M6+M8+M13+M14+M15+M16+M17
农民工安全培训课程	M1+M2+M3+M9+M16+M17
政府官员安全培训课程	M1+M2+M3+M9
IT 行业网络安全管理人员培训课程	M2+M3+M4+M5+M6++M7+M8+M9+M11+M12+M15++M16+M17

续表

培 训 课 程	适用的课程模块
非 IT 行业网络安全管理人员培训课程	M1+M2+M3+M4+M5+M9+M16+M17
IT 行业网络安全工程师培训课程	M3+M4+M7+M8+M9+M10+M11+M12+M13+M14+M15+M16+M17
非信息安全专业高职学生培训课程	M2+M3+M4+M5+M6+M7+M8+M9+M10+M11+M16+M17

4. 关于模块化课程的实施环境

为顺利实施本教程，学习者除需要具有学习热情之外，还需要为课程的有效实施提供可以再现企业网络安全工作的环境，包括：一个可以容纳 40 人左右的网络实验室、至少 4 组工作台、20 台 PC（2 人共用一台）、相关的网络互连设备（如交换机、路由器设备等），以及相应的 Windows、Linux 操作系统及服务器系统配套软件，或者可以架构在 Windows 系统上的虚拟机软件 VMware 等。

虽然本书选择的任务都来自厂商案例，但课程在规划中力求技术的诠释具有通用性。全书有关的接口标准、技术诠释、协议细节、命令语法解释、命令格式、操作规程和拓扑图绘制都使用业内标准，遵循行业通用技术规范和行业规则。

5. 关于课程实践的教学资源

为保证课程有效实施，课程组投入巨大的人力和物力，为本课程建设了专门的教学资源平台，包括电子课件、电子教案、教学指导、学习指导、视频录像、单元自测等，以方便选择不同模块课程的教师使用。详细内容可访问课程实施配套资源网站：http://www.wlaqyx.com/ res/。此外，为支持课程资源的更新、疑难问题的解决、课程实施讨论等一系列服务工作，课程组还为本课程建设了课程拓展资源网站http://www.labclub.com.cn，读者从中可以获得更多资源支持。

6. 关于策划、编撰和致谢

不同于传统的课程教材规划模式，本书由出版社、厂商和院校教师联合开发，希望能吸收各方面的经验，集众所长，保证课程规划的科学性、实用性和针对性。

本书主编龚小勇有多年从事网络安全实践教学的经验，主要研究方向为计算机网络信息系统安全集成实践教学研究。其所带领的网络信息安全创新教学团队，依托本课程实施的“面向西部，实施全程工学结合、四环相扣教学模式改革”的教学改革成果，获得教育部第六届高等教育国家级教学成果奖一等奖。

张选波、安淑梅（CCIE 认证编号 11720）均来自星网锐捷网络有限公司，都有多年在一线从事售前服务工作的工作背景，主攻整网安全实施和防范，熟悉不同厂商的安全设备，能够根据应用实施网络安全防范。他们积累了多年来自工程一线的项目实施经验，为本书选择了具有典型性、真实性、专业性并且方便在学校进行教学、实施的工作任务。

本书由汪双顶负责统稿。本书规划、编写的过程历经两年多的时间，经过多轮修订，牵涉到很多人力，其改革力度之大远远超过策划者前期的估计，书中疏漏之处敬请广大读者及时指正（training@ruijie.com.cn）。

编　者

2010 年 9 月

目　录

模块 1

Windows 桌面系统安全管理与维护

南天信息集成有限公司（以下简称“南天公司”）的办公网中有 300 台办公计算机，每台计算机都使用 Windows 操作系统。为方便日常工作，公司中的计算机互相连接形成小型的办公网，网络中的计算机利用组建的网络实现共享。

为保护办公网络安全，公司的信息中心希望通过文件权限的分配措施保护公司文件服务器的安全，保证网络中每个用户都有不同的权限级别，享受不同等级的文件共享资源。为了使系统能健康运行，信息中心在每台计算机中都启用了防火墙，设定了桌面系统运行的策略，并针对每个文件及文件夹都采取了加密措施。这些措施保证了在企业办公网中，各类人员都有自己的权限，运行在不同的策略级别上，可以访问不同级别的加密文件。

为了实现以上目标，信息中心需要设置以下策略。

- 加强 Windows 主机网络安全访问权限的管理
- 使用防火墙规则加强 Windows 桌面系统的防御
- 使用文件系统加密加强 Windows 文件系统的安全
- 使用本地安全策略加强 Windows 主机的整体防御
- 使用安全审计加强 Windows 主机的安全维护

能力单元 1　加强 Windows 主机安全访问权限的管理

【任务描述】

在南天公司的办公网中，没有设置任何网络安全防范措施，日常网络的应用存在很大风险，公司中经常有保密文件泄密的事情发生，因此公司希望加强办公网中计算机的安全行为管理。实现 Windows 主机安全访问权限的管理，要从以下几个方面入手：在计算机操作系统中，保护用户账户的安全是最基本的安全；其次是加强文件系统的安全；再次是实现文件夹共享的安全。

为加强办公网中 Windows 主机访问权限安全的管理，本能力单元主要实施以下几项任务。

① 保护用户账号安全。

② 保护文件系统安全。

③ 实现文件共享安全。

【任务分析】

在网络应用环境中，为了保证网络终端的安全，防止企业内的用户或者黑客恶意访问敏感数据信息，首先需要考虑的安全是加固网络中用户的账户安全。为了保证桌面系统的安全，防止敏感信息的泄露，使用户可以安全地访问与共享信息，必须从用户账号、文件系统安全、共享安全 3 方面着手来加强桌面系统安全。

1．用户账户安全

每台计算机使用者都可建立自己的用户账户，用户的访问权限决定了用户对计算机、对网络的控制能力与范围。对于计算机中存放的一些重要管理资料，往往要求计算机的用户拥有特殊的权限才可以访问，如果非法用户获得该用户的权限或密码，也就相当于获取了这些资料。因此，保护好用户账户是保障计算机网络安全的重要措施。

在本任务中需要为 300 台计算机分别设定用户账户策略，具体如下。

① 为每一个用户配置 Administrator 默认管理员账户并设置权限。

② 建立多个新的 Windows 用户账户。

③ 建立多个新的 Windows 组。

④ 将不同用户加入不同的用户组中。

2．文件系统安全

文件服务系统既可以为局域网用户提供数据存储服务，同时也可作为网站服务器的远程共享文件夹，实现数据的集中安全存储。由于网络往往采用集中式远程存储，几乎所有重要且敏感的数据都被存储在各种文件服务器中，而这些文件和数据是网络内、外部恶意用户所觊觎的真正目标，这是导致各种网络攻击频繁发生的真正原因，因此确保网络中文件服务系统的访问安全才是保证网络安全的根本所在。

借助于文件服务器中设置的访问控制列表（Access Control List，ACL），不仅可以最大限度地保障重要数据存储安全，保证数据不会由于计算机的硬件故障而丢失，而且还可以通过严格的权限设置，有效地保证数据的访问安全。

在本任务中需要为网络中的计算机文件及文件夹设定 NTFS 权限，具体如下。

① 针对各用户设定文件夹的 NTFS 权限。

② 针对各用户设定文件的 NTFS 权限。

3．文件共享安全

由于网络用户对文件资源的访问都是通过网络共享实现的，所以除了设置 NTFS 权限外，还需要设置共享文件夹权限，但在设置共享文件夹权限之前，根据安全的需要，应启动/关闭默认共享。

默认共享是为了方便管理员远程管理而默认开启的共享（当然可以关闭它），即对所有的逻辑磁盘（C$，D$，E$…）和系统目录 Windows NT 或 Windows（Admin$），都可以通过 IPC$ 连接实现其默认共享的访问。

在本任务中需要为网络中的计算机文件及文件夹设定文件共享权限，具体如下。

① 关闭不需要的默认共享，提高桌面系统安全性。

② 创建需共享的多个文件夹。

③ 为不同的文件夹分配不同的共享权限。

4．验证测试

在完成以上网络用户账户安全、文件系统安全以及默认的文件共享安全设置后，可以通过以下方法，测试网络安全性。

① 不同的用户通过网络访问共享文件夹。

② 查看其访问的内容。

③ 了解 NTFS 权限与共享权限的应用。

【相关知识】

1．用户账户安全

（1）用户账户的分类

在现实世界中，人人都有一个身份，每个人的身份决定了其工作与职权范围。同样，在网络中每台计算机和计算机的使用者也都有其各自不同的身份，拥有不同的访问管理权限。

对于大中型网络而言，为每个单独的用户赋予权限是一件费时费力又非常容易出错的工作。虽然用户权限可以应用于单个的账户，但最好是在组账户上管理。将用户添加至不同的组，并且为组指定权限，确保作为组成员登录的账户自动继承该组的相关权利，这样通过对组而不是对单个用户指派用户权利，可以简化账户管理的任务。具体的组类型如下。

① Administrators 组：管理员组，可以被授权的权利包括更改系统事件、创建页面文件、装载和卸载设备驱动程序、在本地登录、管理审核安全日志、配置单一进程、配置系统性能、关闭系统、取得文件或者对象的所有权。

② Backup Operators 组：备份操作员组，可以被授权的权利包括备份文件和目录、在本地登录、还原文件和目录。

③ Everyone 组：每台计算机及网络账户所在的组。

④ Power Users 组：高级用户组，Power Users 可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务。分配给 Power Users 组的默认权限允许 Power Users 组的成员修改整个计算机的设置。但 Power Users 不具有将自己添加到 Administrators 组的权限。在权限设置中，这个组的权限是仅次于 Administrators 的。

⑤ Users 组：普通用户组，新建的用户在默认情况下都属于这个组。这个组的成员用户可以运行经过验证的应用程序。分配给 Users 组的默认权限不允许成员修改操作系统的设置或用户资料。Users 组提供了一个最安全的程序运行环境。在经过 NTFS 格式化的卷上，默认安全设置旨在禁止该组的成员破坏操作系统和已安装程序的完整性。用户不能修改系统注册表设置、操作系统文件或程序文件。Users 可以创建本地组，但只能修改自己创建的本地组。Users 可以关闭工作站，但不能关闭服务器。

⑥ System 组：这个组拥有和 Administrators 一样甚至更高的权限，在查看用户组的时候它不会被显示出来，也不允许任何用户的加入。这个组主要是为了保证系统服务的正常运行，赋予系统及系统服务的权限。

⑦ Guest 组：来宾组，来宾组跟 Users 组的成员有同等访问权，但来宾账户的限制更多。

（2）用户账户的密码

在 Windows 桌面系统中，用户账户的密码是保证用户系统安全的重要手段之一。用户的密码长度不受限制（即允许密码为空），但在 Windows 服务器系统中，规定用户账户的密码最少为 7 位。

2．文件系统安全

（1）NTFS 权限概述

NTFS 是从 Windows NT 开始引入的文件系统。借助于 NTFS，不仅可以为文件夹授权，而且还可以为单个的文件授权，对用户访问权限的控制变得更加细致。NTFS 还支持数据压缩和磁盘配额，从而可以进一步高效率地使用硬盘空间。

一旦用户磁盘格式化成 NTFS 格式，那么用户就可以对 NTFS 磁盘内的文件夹与数据设定访问权限，具有访问权限的用户才可以访问这些资源。

（2）NTFS 权限分类

① NTFS 文件权限。

- 读取（read）：可以读取文件内容、查看文件属性与权限等。文件属性指的是只读、隐藏等。
- 写入（write）：可以修改文件内容、在文件后面添加数据或修改文件属性等。
- 读取和执行（read&execute）：除了拥有读取的权限外，还具备运行应用程序的权限。
- 修改（modify）：除了拥有读取、写入与读取和执行的权限外，还可以删除文件。
- 完全控制（full control）：拥有所有的 NTFS 文件权限，也就是除了拥有上述所有权限之外，还拥有更改权限与取得所有权的特殊权限。

② NTFS 文件夹权限。

- 读取（read）：查看该文件夹中的文件和子文件夹，查看文件夹的所有者、权限和属性。
- 写入（write）：可以在文件夹内新建文件与子文件夹、修改文件夹属性等。
- 列出文件夹目录（list folder contents）：查看该文件夹中的文件和子文件夹的名称。
- 读取和执行（read&execute）：拥有与列出文件夹目录几乎完全相同的权限。
- 修改（modify）：除了拥有前面的所有权限外，还可以删除此文件夹。
- 完全控制（full control）：拥有所有的 NTFS 文件夹权限，还拥有更改权限与取得所有权的特殊权限。

③ NTFS 权限属性。

- NTFS 权限具有可继承的属性：当父文件夹的权限设置完毕后，父文件夹的 NTFS 权限自动被子文件夹继承。
- NTFS 权限具有累加的属性：如果某一个用户属于多个用户组，而这个用户及用户所在的组对某个文件或者文件夹拥有不同的 NTFS 权限，那么这个用户的最后 NTFS 权限为多个组 NTFS 权限的集合。例如 A 用户同时属于销售组与经理组，销售组对某文件夹的权限是读取，经理组的权限是读取+执行，那么 A 用户的权限是读取+执行。
- 拒绝的 NTFS 权限比允许的权限级别高：上面提到 NTFS 的权限是累加的，但有一种特殊情况，就是只要其中一个权限是拒绝的权限，则用户就不再拥有此权限。比如上面

的案例，A 用户所在销售组的权限是允许读取，而在经理组的权限为拒绝读取，那么 A 用户的权限就为拒绝读取。

3．文件共享安全

将文件夹设置为共享资源时，除了必须为文件和文件夹指定 NTFS 权限外，还应当为共享文件夹指定相应的访问权限。共享文件夹权限类似于 NTFS 权限，但 NTFS 权限的优先级要高于共享文件夹权限。因此，共享文件夹的权限可以粗略设置，而 NTFS 权限则必须详细划分。

（1）共享文件夹权限的特点

共享文件夹权限只适用于文件夹，而不适用于单个文件，并且只能为整个共享文件夹设置共享权限。

（2）共享文件夹权限的种类

- 读取：显示文件夹名称、文件名称、文件数据和属性，运行应用程序文件。
- 修改：创建文件夹，向文件夹中添加文件，修改文件中的数据，向文件中追加数据，修改文件属性，删除文件夹中的文件，以及执行“读取”权限所允许的操作。
- 完全控制：修改文件，获得文件的所有权。

【任务实施】

1．拓扑结构

本任务的网络拓扑结构如图 1-1 所示，通过一台二层交换机组建一个简单的办公网，模拟南天公司办公网的场景，其中交换机不需要做任何配置。

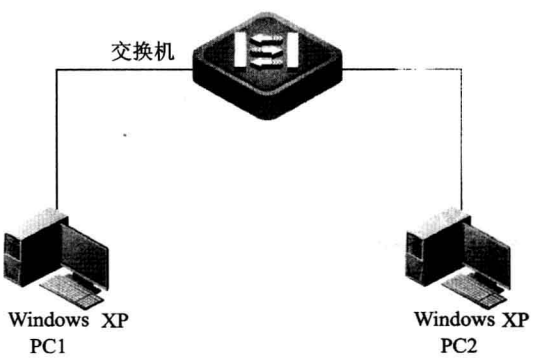

图 1-1　拓扑结构

2．项目设备

计算机（2 台）、二层交换机（1 台）、网线（若干根）。

注意：按图 1-1 所示拓扑结构进行网络连接，两台计算机使用 Windows XP 操作系统，其中用 PC1 来存储数据，用 PC2 来进行网络测试。其网络地址规划分别为：PC1 的 IP 地址为 10.1.1.1，255.255.255.0，默认网关为 10.1.1.2；PC2 的 IP 地址为 10.1.1.2，255.255.255.0，默认网关为 10.1.1.1。

3．操作步骤

〖步骤 1〗 配置本地连接

分别启动 PC1、PC2 计算机，选择“开始”→“控制面板”→“网络连接”→“本地连接”选项，打开“本地连接”对话框，单击“属性”按钮，在打开的对话框中双击“Internet 协议（TCP/IP）”选项。在打开的对话框中选中“使用下面的 IP 地址”单选按钮，输入规划的网络地址，完成本地连接的 IP 地址配置。

〖步骤 2〗 创建用户账户

第一步：创建多个 Windows 用户账户并进行密码安全设置

在 PC1 上，选择“开始”→“控制面板”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，展开“本地用户和组”节点，右击“用户”节点，在弹出的快捷菜单中选择“新用户”选项，打开“新用户”对话框，依次创建 bob、Mary、Tim 3 个账户。

在创建 3 个用户的时候，建议将其密码设置为 7 位以上并包含数字、符号等元素以保证用户密码安全。在本例中，根据密码规则输入密码，出于安全考虑，密码自定义。创建 3 个用户的过程如图 1-2、图 1-3、图 1-4 所示。

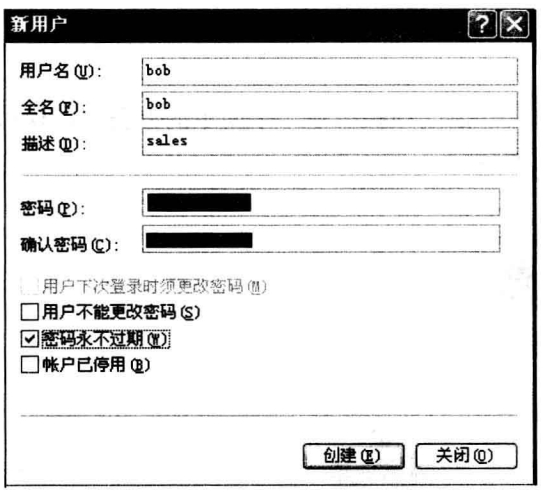

图 1-2 新建 bob 用户

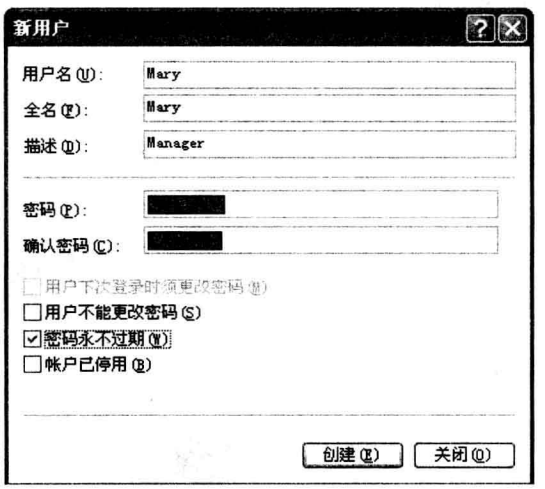

图 1-3 新建 Mary 用户

第二步：创建 Windows 用户组

打开 PC1，选择“开始”→“控制面板”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，展开“本地用户和组”节点，右击“组”节点，在弹出的快捷菜单中选择“新建组”选项，打开“新建组”对话框。输入组名，单击“创建”按钮完成组的创建。

分别在 PC1 上新建 Sales、Manager、Engineer 3 个用户组，如图 1-5、图 1-6、图 1-7 所示。

第三步：将不同的用户加入到不同的用户组中

用户组创建完成后，将用户 bob、Mary、Tim 分别加入 Sales、Manager、Engineer 这 3 个用户组中。

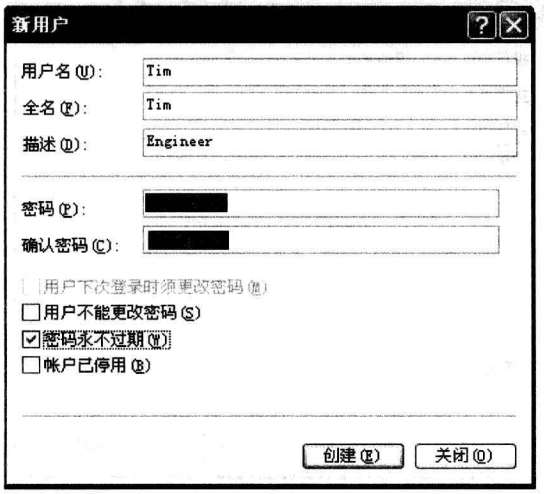

图 1-4　新建 Tim 用户

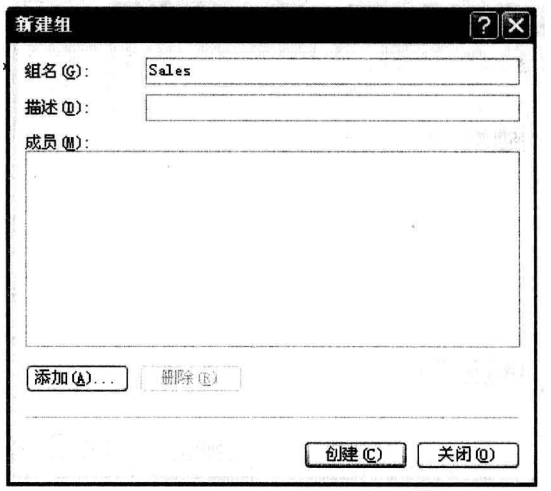

图 1-5　新建 Sales 组

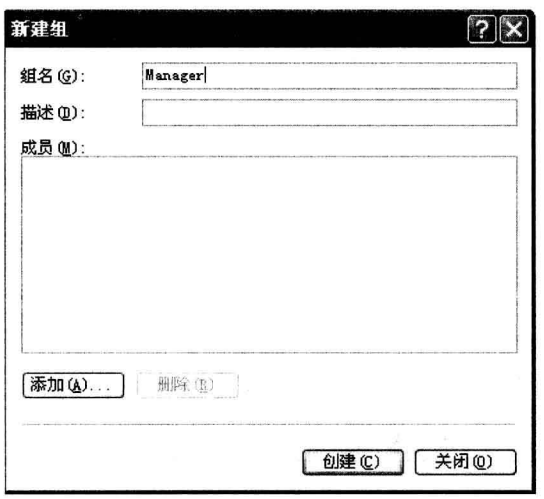

图 1-6　新建 Manager 组

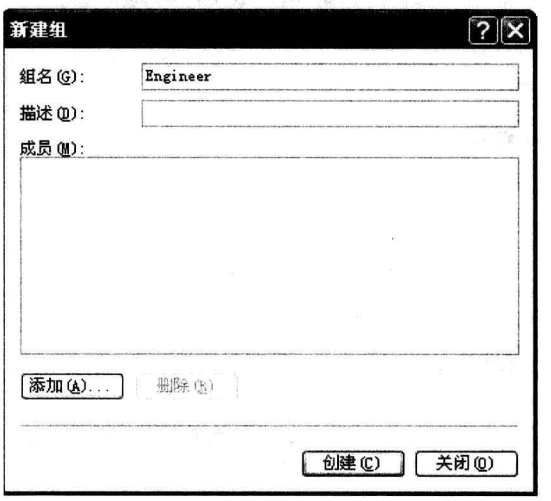

图 1-7　新建 Engineer 组

在 PC1 上，选择“开始”→“控制面板”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，展开“本地用户和组”节点，选择“组”选项，在其对应的右边列表框中找到相应的组，双击组名，依次在打开的对话框中单击“添加”→“高级”→“立即查找”按钮，找到相应的用户名，将用户加入组中。将用户 bob、Mary、Tim 分别加入 Sales、Manager、Engineer 这 3 个用户组中的过程如图 1-8、图 1-9、图 1-10 所示。

〖步骤 3〗 创建共享文件夹

第一步：创建多个文件夹

在 PC1 的 D 盘上创建 File 文件夹，如图 1-11 所示。

图 1-8　将 bob 加入 Sales 组中

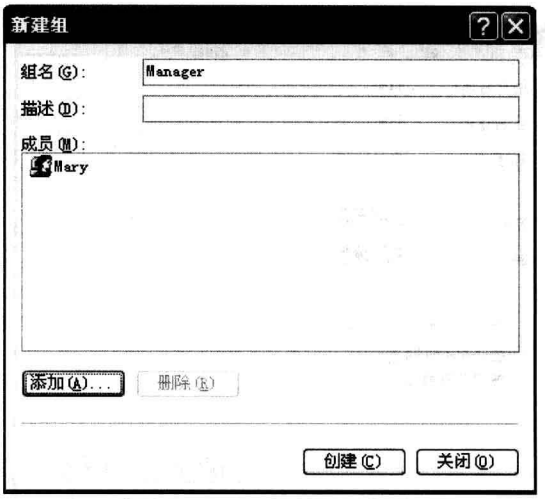

图 1-9　将 Mary 加入 Manager 组中

图 1-10　将 Tim 加入 Engineer 组中

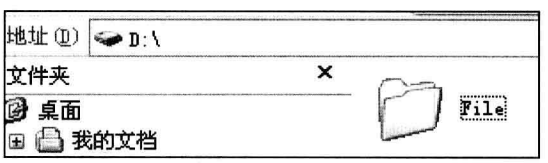

图 1-11　创建 File 文件夹

在 File 文件夹中创建 3 个子文件夹，分别以 Sales、Manager、Engineer 命名。建立完成的子文件夹 Sales、Manager、Engineer 如图 1-12 所示。

图 1-12　新建子文件夹

选中 Sales 文件夹并右击，在弹出的快捷菜单中选择“新建”→“BMP 图像”选项，创建一个文件名为 Sales.bmp 的图像文件。

第二步：为文件夹配置共享权限

在 PC1 上打开“我的电脑”窗口，选中需要共享的 File 文件夹并右击，选择快捷菜单中的

“共享和安全”选项，在打开的对话框中选中“共享此文件夹”单选按钮，如图 1-13 所示，单击“确定”按钮，完成配置。

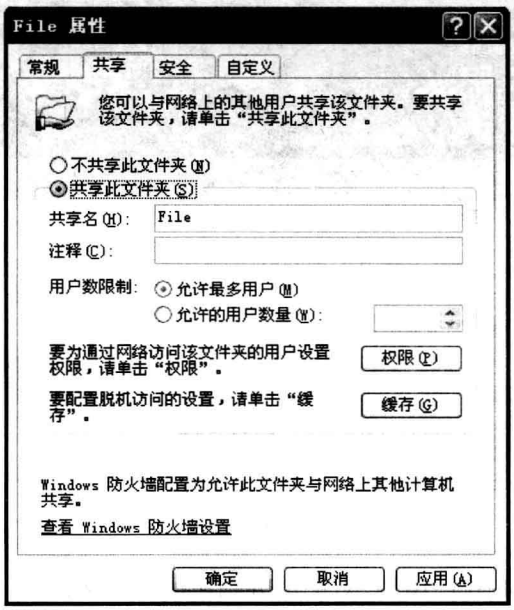

图 1-13　共享文件夹

第三步：测试文件夹共享结果

（1）访问共享文件夹

在 PC2 上，选择“开始”→“运行”选项，在打开的对话框中输入命令“cmd”，单击“确定”按钮，打开如图 1-14 所示的 DOS 命令行操作窗口。在命令行操作窗口中输入“ipconfig”命令，查看 PC2 本机 IP 地址信息。

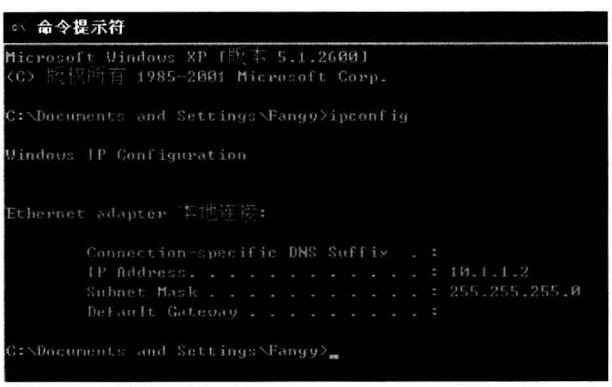

图 1-14　查看 IP 地址

接下来返回 PC2 的桌面，分别使用不同的用户名（bob、Mary、Tim）登录到 PC2 上。

在 PC2 的操作系统中，选择“开始”→“运行”选项，在打开的“运行”对话框中输入“\\10.1.1.1”，单击“确定”按钮，这样就可以在 PC2 中查看到在 PC1 上发布的共享文件夹 File