网络工程师
实用培训教程系列

丛书主编　刘晓辉　张运凯　李福亮

计算机网络安全

○ 王文斌　王黎玲　等编著

清华大学出版社

网络工程师
实用培训教程系列

丛书主编　刘晓辉　张运凯　李福亮

计算机网络安全

清华大学出版社
北京

内容简介

本书主要以现有企业网络为模型，分别介绍服务器系统安全、网络应用服务安全、网络设备安全、网络安全设备管理、局域网接入安全、Internet 接入安全和远程访问安全等内容，全面涵盖了当前主要网络中可能遇到的信息安全问题，并详细介绍了不同的网络安全方案。本书紧密依托选定项目，对企业网络安全中常用的技术进行了深入浅出的讲解，可以帮助读者快速掌握最基本的计算机网络安全技术，打造安全、可靠的企业网络环境。

本书既可作为培养 21 世纪计算机网络安全工程师的学习教材，同时也是从事计算机网络安全的规划、设计、管理和应用集成的专业技术人员的必备工具书。

图书在版编目(CIP)数据

计算机网络安全/王文斌，王黎玲等编著. —北京：清华大学出版社，2010.6
(网络工程师实用培训教程系列)
ISBN 978-7-302-22550-8

Ⅰ. ①计…　Ⅱ. ①王… ②王…　Ⅲ. ①计算机网络－安全技术－技术培训－教材
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 069736 号

责任编辑：孟毅新
责任校对：袁　芳
责任印制：孟凡玉
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：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×260　**印　张**：30.25　**字　数**：729 千字
版　　次：2010 年 6 月第 1 版　　**印　　次**：2010 年 6 月第1 次印刷
印　　数：1～3000
定　　价：48.00 元

产品编号：034323-01

PREFACE 丛书序

近年来，计算机网络在我国已经得到了较快的发展。许多企业、事业单位、行政机关、司法机构和金融系统构建了高速的办公专用网。各种类型的计算机网络高达数十万个，计算机网络已经深入到我们工作、生活和学习的方方面面。

毫无疑问，大量的网络必然需要大量的网络管理人才。初步估计，到目前为止，仅我国每年需要的网络管理人才就达十余万人。随着网络应用的日益深入以及网络所承载的业务量和数据量的不断增长，网络的重要性和安全性也将与日俱增，对网络管理人员的需求也将随之不断地增长。由此可见，网络管理是一个稳定且前途远大的职业。

综观现有的网络技术培养教材，大多将网络技术进行条块分割，按章节、分模块独立讲授，人为地将紧密联系在一起的各种理论和技术分裂开来。这样所带来的问题就是，学生必须将所学的知识和理论全部融会贯通之后，才能初步掌握作为一个网络技术人员所必须具备的一些基本技能，显然这不符合学生的学习规律，也不符合现实的网络管理实际，同时，也是导致许多网络爱好者望而却步的重要原因。

本丛书具有以下特点。

(1) 案例贯穿。本丛书从最常见、最典型的网络应用情境和需求入手，围绕统一的网络环境、统一的网络规划、统一的网络拓扑、统一的资源分配、统一的网络用户和统一的网络需求，提供全面的网络解决方案，以及实用、够用的网络技术，为网络工程师提供宝典级别的现场技术手册。

(2) 项目驱动。本丛书由情境导入需求，以项目进行教学，再由实训实现强化，进而达到培养技能的目的，最终使学生顺利就业。按照网络构建的工作过程系统化课程开发，以真实的网络管理过程为导向规划课程内容，使读者能够真正掌握网络构建与管理的知识和技能，独立完成相关的网络技术项目。

(3) 贴近实战。本丛书突出“先做后学，边做边学”的主旨，通过“练中求学、学中求练、练学结合、边练边学”的教学内容安排，实现“学得会，用得上”的最终目的。由于全书围绕统一的典型网络工程展开，因此，读者能够非常方便地将教学案例移植到真实的网络项目中，学为所用，学以致用。

(4) 内容全面。本丛书涵盖了作为初、中级网络管理员必须掌握的所有理论和技术，以网络管理的实际需求为导向，以培养基本技能为目的，将枯燥的理论融于实际操作中，从而使学生学得会、记得住、用得上。

(5) 兴趣教学。本丛书设计的教学内容按照“案例情景→需求分析→解决方案→技术操作→理论背景”的结构进行组织，有实际案例、有动手操作、有理论分

析，可以激发读者的学习兴趣和学习的主动性，培养读者解决实际问题的能力，提高读者的综合实战水平。

（6）注重动手。本丛书加大了动手操作的比重，减弱了理论知识的介绍，以适应特定的读者群，体现“做中学”的宗旨。借助大量的网络实验，可以使读者迅速提高技术和技能。

（7）涵盖认证。本丛书充分考虑到了网络管理员的职业需求及职业资格认证要求，在内容安排和习题设置上与相关认证紧密结合，基本涵盖了国内认证（网络管理员、网络工程师）和国际认证（MCSE、CCNA）所涉及的理论和知识技能，以帮助学生获取“双证书”——学历证书和职业资格证书，增强学生的就业竞争力。

（8）资深作者。本丛书作者全部来源于网络教学、网络管理和网络工程第一线，具有非常丰富的网络设计、施工和管理经验，既掌握理论技术，又通晓实际操作。作者们做了大量的技术需求和人才需求调研，多次修改提纲以使其更加符合网络搭建和管理实际。

（9）深度支持。本丛书不仅提供优秀的纸质教材，还为教师提供了电子课件和全方位的技术支持，同时设置有 QQ 群在线答疑、E-mail 离线交流和 BBS 论坛互动平台，并为读者提供网络构建方案和配置技术咨询，形成一个让师生更加方便、更加自主学习的教学环境，有效地提升了教师授课和学生学习的能力。

本丛书删繁就简，围绕一个典型的网络工程展开理论和技术讲解，囊括了网络布线、网络搭建、网络管理、网络服务、网络安全、数据存储等各种组网、管网和用网技术。因此，读者学完本套丛书后，可以直接将其应用至自己的工作实践。即使是初学者，只要熟悉 Windows 的一般操作，就能非常容易地上手，迅速成长为一名合格的网络管理员。

刘晓辉

2010 年 6 月

FOREWORD 前言

随着信息化进程的推进，几乎所有的企事业单位都有自己的网络，而由此产生的网络管理人才的需求缺口正在逐年扩大。据相关部门统计，2009 年网络管理人才缺口达到 13.5 万人，许多企业不惜重金，招募一名出色的网络管理人员。随着网络应用的不断拓展，企业发展对计算机网络的依赖性将越来越强，而掌握大量精尖网络技术的人才也会变得越来越受欢迎。为什么在如此光明的就业形势下，却经常听到网络管理员的工资只有几百元呢？原因很简单，企业真正需要的网络管理员是能够独当一面的专业人员。向网络工程师晋升，是摆在网络管理员面前的唯一出路。

本套丛书作为网络工程师培训教材，以实际的公司网络为案例，以打造实用的网络工程为目标，以实用和技能为主，摒弃了复杂的原理，以简明的操作为引导，通俗易懂，上手容易。读者只需按照书中的操作来学习，就能掌握相应的技能，学完全套书之后，即可掌握大部分的网络知识。

计算机网络技术的应用虽然加速了企业发展的步伐，但随之而来的安全问题，也时刻威胁着企业的根本利益。近年来，企业网站遭到篡改，病毒泛滥成灾，商业机密失窃，企业网络瘫痪，各种高科技信息犯罪活动正在严重危害着社会的发展和企业的生存。本书以中小型企业的计算机网络安全为例，全面、系统地介绍了企业网络的安全建设，旨在帮助企业打造安全、可靠、高效、便捷的计算机网络。

全书内容共分为 13 章，技术操作与需求目标紧密结合，并对应用到的新技术以“知识链接”的方式加以剖析。第 1 章网络安全规划，从整个网络的安全管理任务出发，对整个网络项目的安全需求进行全面分析和规划。第 2 章 Windows 系统安全，以 Windows Server 2008 为例介绍服务器系统安全，包括常规安全配置、系统漏洞安全、管理员账户安全等。第 3 章网络服务安全，介绍常用网络服务的安全，包括活动目录服务、WWW 服务、FTP 服务等的安全配置与管理。第 4 章文件权限管理，介绍 AD RMS、IRM 文件权限保护技术在企业网络中的应用和配置。第 5 章网络病毒防御，以 Symantec 网络防病毒系统为例，介绍局域网防病毒系统的部署与应用。第 6 章系统补丁更新，介绍如何通过 WSUS 服务器实现企业网络中计算机的系统补丁管理。第 7 章 Cisco IOS 安全，介绍常用 Cisco 网络设备基于 IOS 的安全，包括交换机、路由器、无线 AP 的安全配置。第 8 章局域网接入安全认证，介绍如何通过“Cisco ACS + Active Directory”模式实现网络设备接入的 802.1x 身份验证。第 9 章 Internet 接入安全，介绍如何通过 Forefront TMG 实现局域网共享接入、安全防护以及内网服务器的发布。第 10 章远程接入安全，介绍远程接入 VPN 技术在企业网络中的应用，包括 IPSec VPN、SSL VPN 的部署与测

试等。第11章网络访问保护，介绍NAP技术的部署及应用，包括IPSec强制技术、802.1x强制技术、VPN强制技术以及DHCP强制技术的实施。第12章安全设备规划与配置，介绍企业网络中常用安全设备的规划与部署，包括Cisco ASA、IPS、IDS等。第13章配置网络可靠性，介绍通过故障转移群集和网络负载均衡技术，以及网络设备的链路冗余技术提高企业网络的可靠性。

为了让读者更深入地了解所学的知识，在每章的最后还配备了习题和实验，从而可以起到复习和测验的作用，能使读者尽快迈向网络工程师的行列。

本书可作为大中专院校计算机网络专业的教材，也可作为中小型网络管理员、网络工程技术人员和网络爱好者的参考书。

本丛书由刘晓辉、张运凯、李福亮主编。本书由王文斌、王黎玲等编著。具体分工如下：王文斌编写了第1～4章，王黎玲编写了第5～8章，李文俊编写了第9～10章，王同明编写了第11章，石长征编写了第12章，郭腾编写了第13章。编者长期从事系统维护和网络管理工作，具有较高的理论水平和丰富的实践经验，本书作为对一段工作的总结与回顾，希望能对大家的系统维护和网络管理工作有所帮助。

由于编者水平有限，书中难免有不足之处，恳请广大读者批评指正。

编　者

2010年4月

目录

CONTENTS

第 1 章 chapter 1

网络安全规划

随着计算机应用的日益普及，网络已经成为大多数企业的重要组成部分，许多常规办公应用已经开始转向网络，例如企业办公、视频会议、合作伙伴沟通等。随之而来的网络安全问题，也就成为制约企业生存与发展的命脉。网络安全建设的总体思路是：以信息资产为核心，以安全战略为指导，根据安全需求逐步完善安全基础设施，为网络应用提供安全能力支持。

1.1 项目背景

某高新产品研发企业拥有员工 2000 余人，公司总部坐落在省会城市高新技术开发区，包括 4 个生产车间和两栋职工宿舍楼，产品展示、技术开发与企业办公均在智能大厦中进行。该企业在外地另开设有两家分公司，由总公司进行统一管理和部署。目前，该企业网络的拓扑结构如图 1-1 所示，基本情况如下。

(1) 公司局域网已经基本覆盖整个厂区，中心机房位于智能大厦的第 3 层(共 15 层)，职工宿舍楼和生产车间均有网络覆盖。

(2) 网络拓扑结构为“星型＋树型”，接入层交换机为 Cisco Catalyst 2960，汇聚层交换机为 Cisco Catalyst 3750，核心层交换机为 Cisco Catalyst 6509。

(3) 现有接入用户数量为 500 个，客户端均使用私有 IP 地址，通过防火墙或代理服务器接入 Internet。部分服务器 IP 地址为共有 IP 地址。

(4) Internet 接入区的防火墙主要提供 VPN 接入功能，用于为远程移动用户或子公司网络提供远程安全访问。

(5) 会议室、产品展示大厅等公共场所部署无线接入点，实现随时随地无线漫游接入。

(6) 服务器操作系统平台多为 Windows Server 2003 和 Windows Server 2008 系统。客户端系统为 Windows XP Professional 和 Windows Vista。

(7) 网络中部署有 Web 服务器，为企业网站提供运行平台。

(8) 企业网络办公平台为 WSS，文件服务器可以为智能大厦的办公用户提供文件共享、存储与访问。

(9) E-mail 用于员工之间的彼此交流，以及企业与外界的通信联络。

(10) 打印服务和传真服务主要满足智能大厦用户网络办公的应用。

(11) 企业分支结构通过 VPN 方式远程接入总部局域网，并且可以访问网络中的共享资源。