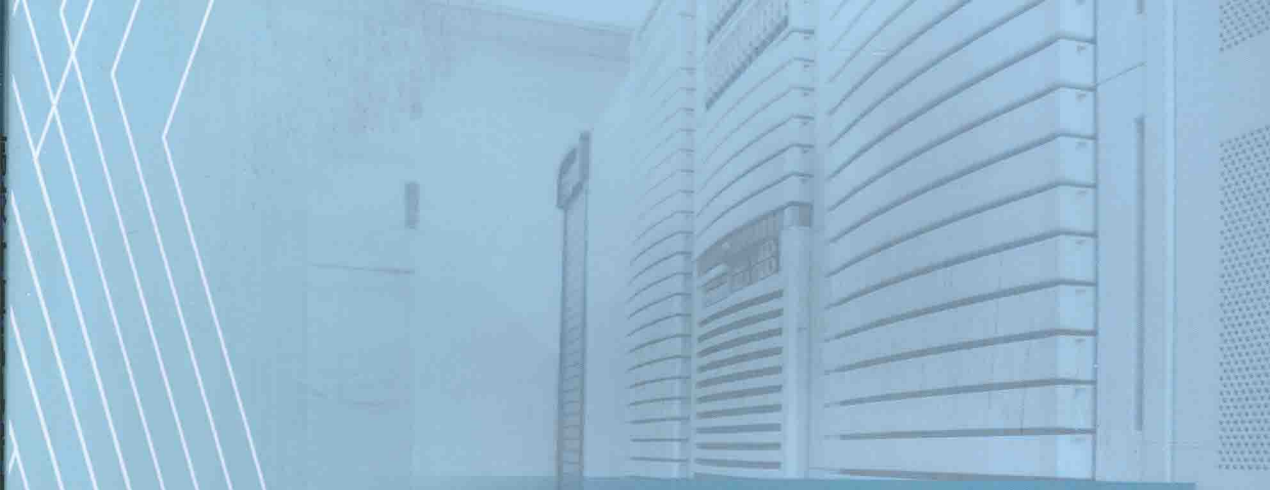

高校计算机机房的运行管理与技术控制

GAOXIAO JISUANJI JIFANG DE
YUNXING GUANLI YU JISHU KONGZHI

张 蕾◇著

北京交通大学出版社
http://www.bjtup.com.cn

高校计算机机房的运行管理与技术控制

张 蕾 著

北京交通大学出版社

·北京·

内 容 简 介

本书从高校计算机机房的运行管理和技术控制等方面出发，以应用、实用、技能为主线，从网络系统管控、数据管控、环境管控、服务管控、安全设计管控五个方面进行讲解，系统地介绍了计算机机房的管理及维护的各个方面。

本书是一本技术性较强的学术读物，力求内容深入浅出、图文并茂，适合各类高等院校、职业院校、培训机构等相关专业人士阅读，也适合各类计算机技术人员作为参考用书。

图书在版编目（CIP）数据

高校计算机机房的运行管理与技术控制 / 张蕾著. — 北京：北京交通大学出版社，2015.8

ISBN 978-7-5121-2392-2

Ⅰ. ① 高… Ⅱ. ① 张… Ⅲ. ① 高等学校-电子计算机-机房管理 Ⅳ. ① TP308

中国版本图书馆 CIP 数据核字（2015）第 207351 号

策划编辑：田秀青
责任编辑：田秀青
出版发行：北京交通大学出版社　　电话：010-51686414
　　北京市海淀区高梁桥斜街 44 号　邮编：100044
印 刷 者：北京泽宇印刷有限公司
经　　销：全国新华书店
开　　本：170×235　印张：11.5　字数：141 千字
版　　次：2015 年 8 月第 1 版　2015 年 8 月第 1 次印刷
书　　号：ISBN 978-7-5121-2392-2/TP · 820
定　　价：39.00 元

本书如有质量问题，请向北京交通大学出版社质监组反映。对您的意见和批评，我们表示欢迎和感谢。
投诉电话：010-51686043，51686008；传真：010-62225406；E-mail：press@bjtu.edu.cn。

前　言

随着计算机技术的飞速发展，在我国各高校的教学信息化过程中，计算机应用越来越频繁，许多高校建立了计算机机房。此外，随着我国高等教育的快速发展及大学招生规模的不断扩大，高校计算机机房的数量与规模也随之不断地扩大，这给机房管理等工作带来了机遇和挑战。计算机机房是提高学生理论知识和实际操作能力，进行科学研究的重要基地。计算机机房管理是一门综合性的技术管理，它涉及计算机系统、网络系统、多媒体设备及供电系统、安防系统、照明空调等多种学科和技术。要想真正把计算机机房管理好，不仅要掌握这些学科和技术的理论知识、技能、工作原理、技术要求等，还要协调好它们之间的关系。计算机机房管理工作的实质就是这些综合技术在计算机机房中的实际应用。这些技术的应用和管理发挥得好，计算机机房就能长期为用户创造一个良好的上机环境，从而最大限度地发挥计算机机房的作用。此外，计算机机房的管理工作还涉及科学的管理方法，包括人、物及部门之间制度的制定、落实等诸多方面。总而言之，计算机机房管理是一项系统工程，它需要各个环节的共同优化。

对于从事计算机机房管理的工作人员，基本的岗位职责如下：

（1）负责计算机机房设备的日常管理，做好日常巡检工作，包括配电、空调、消防等设施及网络、服务器、存储等设备的检查工作；

（2）计算机机房及部门所属各种资产的管理，做好设备清点、分类、统计、标识等工作；

（3）负责安排机房硬件设备的维修工作，协调相关设备维修人员进行维修，安排好相关维修工作；

（4）复杂计算机机房软件的安装与维护工作；

（5）对计算机机房各类设备上所运行的系统、服务进行管理和配置，满足办公部门的 IT 服务需求。

相关技术能力要求如下：

（1）熟悉 Windows Sever、Linux 等操作系统的硬件维护、网络和服务配置；

（2）熟悉网络安全技术和虚拟化技术；

（3）熟悉数据库技术和数据安全技术；

（4）熟悉存储技术；

（5）熟悉交换机设备及接入网络设备的基本配置和命令。

以上技术能力和经验并不要求某一机房管理员全部具备或精通，每个人的技术能力各有侧重，互补配合进行计算机机房管理。

针对以上技能要求，本书从 5 个方面展开论述。全书共分 5 章内容：第 1 章介绍了如何加强和提高对机房设备、网络安全的管理并制定相关的安全制度；第 2 章从机房数据的管理角度出发，重点分析了计算机机房用电保护、数据备份和消冗、硬盘数据维护及数据安全等；第 3 章从计算机机房设计角度出发，对机房环境、电气安全作了详细介绍；第 4 章就如何树立以人为本的良好计算机机房形象，从计算机机房门禁系统、网络行为监控系统、计算机机房人员管理等方面进行阐述；第 5 章针对计算机是否

能安全、稳定、标准地运行，从计算机机房如何防雷、防水及其他干扰源（电磁、鼠虫害等）方面进行了详细分析。

本书作者既具有在教学一线工作的丰富经验，又有从事计算机机房管理工作的实践经验。本书以实战为线、以理论为面，注重二者结合。读者通过本书的学习，能熟练运用本书讲到的机房管理技巧、维护方法，能架设一个趋向于零维护的计算机机房网络，建立一套现代化、技术化、创新化、人性化的管理模式，管理好计算机机房。

本书的编写过程中，作者参考了大量的专业书籍，也走访了许多高校及培训机构的计算机机房及企事业单位的计算机机房，并得到了许多同行的真诚帮助，在此一并向他们表示衷心的感谢。

由于作者水平有限，疏漏与不足之处在所难免，敬请广大读者和专家批评指正，期望在今后的工作中不断完善和改进。

作　者

2015 年 6 月

目　录

随着计算机信息技术的发展，计算机知识的掌握和应用已成为当代学生知识结构和能力素质的重要组成部分，计算机教学在高等学校教育中的地位越来越重要，而计算机实验教学又是计算机教学的一个重要组成部分。计算机实验室是学生掌握计算机应用能力的主要场所，所以许多高校建立了计算机机房。目前，由于计算机的普及，高校计算机机房的规模也逐渐扩大，规模的扩大给计算机机房管理工作带来了机遇和挑战。只有对计算机机房进行科学管理，才能保证计算机实验教学的顺利进行。

第 1 章

网络系统管控

互联网的迅猛发展和普及，已经成为推动人类进步的巨大动力。其中浩如烟海的信息成为人们日常生活、工作和学习必不可少的帮手，极大地丰富了人类的生活。作为继报纸、广播、电视之后的第四大媒体，互联网逐渐融入人们生活，使用互联网已成为当代人类的一种生活方式，对人的

心理和行为产生了重要的影响。高校计算机机房不单提供日常教学服务，也是在校师生、科研人员工作的基地。此外，现有的计算机机房不单是一台服务器和几台 PC 机的组合，而是由多台专业服务器、小型机、专业高级网络设备、存储设备及电源 UPS 设备等众多的专业高级设备组成。所以加强和提高对计算机设备、操作系统、网络安全的管理是非常迫切的。

1.1 网 络 防 护

1.1.1 网络安全概述

通常，系统的安全与性能/功能是相互矛盾的关系。如果某个系统不向外界提供任何服务（断开/脱机），外界是不可能对其构成安全威胁的。由于计算机机房网络安全事件频发，管理难度越来越大，特别是在网络上运行关键业务时，网络安全是首先要解决的问题。

国际标准化组织（ISO）将计算机网络系统的安全定义为："为数据处理系统建立所采取的技术和管理的安全保护，保护计算机网络系统的硬件、软件和数据不因偶然和恶意的原因而遭到破坏、更改和泄露。"随着 Internet（互联网）的发展，网络安全与计算机安全是不可分割的。计算机安全的工作主要是阻止及检测计算机系统用户的未经授权的行为，从保密性、完整性和可用性等方面考虑计算机安全；而网络安全则是保证计算机在互联网网络上的正常运行。

1. 网络安全的技术隐患

1）网络的威胁

自然灾害等意外事故，硬件故障、软件漏洞等人为失误，黑客攻击等计算机网络犯罪，信息丢失、电子谍报，信息站、网络协议中的缺陷等都是来自网络的威胁。

2）资源共享带来的漏洞及技术的开放标准所带来的不安全因素

这主要包括：操作人员设置不当、系统安全配置不规范，用户安全意识不强、选择用户口令不慎，将自己的账号随意转告他人、人为的恶意攻击等。

3）个人计算机的安全问题

个人计算机开放性的设计模式，导致使用者可以了解其内部结构和工作原理，极易发生系统漏洞。

2. 网络的不安全因素

1）操作系统的安全性

目前流行的许多操作系统（UNIX 操作、Windows NT/2000/2003 操作系统及 Windows XP、操作系统桌面 PC 等）均存在网络安全漏洞。

2）网络协议的安全性

由于大型网络系统内运行多种网络协议，如 TCP/IP、IPX/SPX、NETBEUA 等，而这些网络协议并非专为安全通信设计的，部分协议本身也缺乏安全性。

3）防火墙的安全性

防火墙本身的安全性不一定能得到很好的保障。

4）内部网用户的安全性

网络的管理制度不健全、缺少管理者的日常维护、数据备份管理、用户权限管理及应用软件的维护等都存在安全风险。

5）缺乏有效的手段

这主要是指网络认证环节薄弱，监视、评估网络系统的安全性跟不上网络技术的发展。

6）应用服务的安全性

许多应用服务系统在访问控制及安全通信方面考虑不周而造成安全风险。

7）忽视黑客、病毒和计算机犯罪所造成的严重后果

舍不得投入必要的人力、财力和物力来加强网络的安全性，人们的安

全意识不强会造成严重后果。

1.1.2　网络安全技术

1. 认证技术

认证技术是实现计算机网络安全的关键技术之一。认证主要是指对某个实体的身份加以鉴别、确认，从而证实是否名副其实或者是否有效的过程。认证的基本思想是验证某一实体的一个或多个参数的真实性和有效性。

目前最主要的认证方法有口令认证、数字签名和认证中心 3 种。

1）口令认证

口令是一种鉴别用户是否有权使用计算机及软件的一种比较脆弱的手段。由于实现起来比较简单，因此得到了广泛应用。口令认证的基本思想是每一个用户都有一个标识（或口令），当用户进入某系统时，必须先提供其标识（或口令），然后系统验证用户的合法性。

口令认证具有价格低廉、容易实现且用户界面友好等特点，但其安全性较低，如可用套口令的方式破译（如某些人经常喜欢用自己的生日、姓名、家里的电话等作为口令）。

2）数字签名

数字签名是通信双方在网上交换信息时，用公钥密码方式防止伪造

和欺骗的一种身份签证。它以加密技术为基础，其核心是采用加密技术的加密、解密算法来实现对报文的数字签名。因此，通过数字签名，接收方能够证实发送方的真实身份，发送方事后不能否认所发送过的报文。接收方或非发送方不能伪造、篡改报文。

实现数字签名的方法较多，常用的数字签名技术有两种：私人密钥的数字签名和公用密钥的数字签名。

（1）私人密钥法（又称对称密钥法，DES），是指发送方和接收方依照事先约定的密钥对明文进行加密和解密的算法，它的加密密钥和解密密钥为同一密钥，只有发送方和接收方才知道这一密钥。

（2）公用密钥法（又称非对称密钥法，RAR），是加密密钥与解密密钥不同的加密算法体制，且能找到一个陷门单向函数，从加密密钥根本无法推算出解密密钥。

3）认证中心

认证中心就是一个负责发放和管理数字证书的权威机构。对于一个大型的应用环境，认证中心往往采用一种多层次的分级结构，各级的认证中心类似于各级行政机关，上级认证中心负责签发和管理下级认证中心的证书，最下一级的认证中心直接面向最终用户。

2. 防火墙技术

防火墙是建立在内外网络边界上（通常是路由器或计算机之间）的过滤封锁机制，对内连接局域网，对外连接 Internet，通过隔离、过滤、封锁等技术，阻止信息资源的非法访问。

防火墙是设置在被保护网络和外部网络之间的一道屏障，以防止发生不可预测的、潜在破坏性的侵入，如黑客袭击、病毒破坏、资源被盗用或文件被篡改等。它可以过滤一个信息包，转发其他认为安全的部分分组，即通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。防火墙结构如图 1–1 所示。

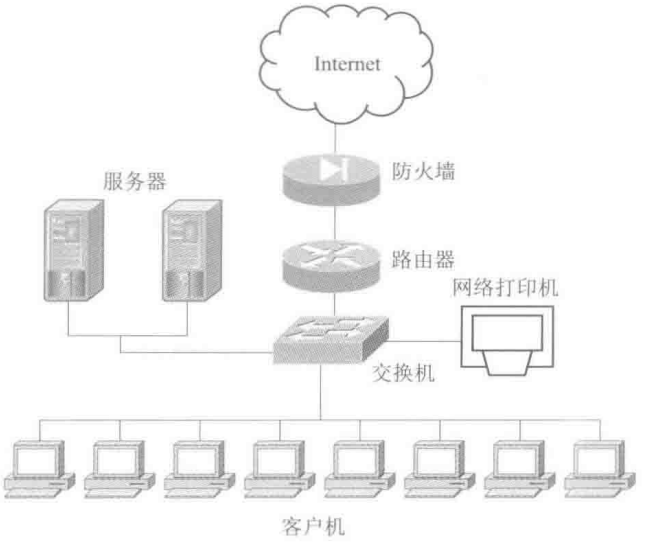

图 1–1　防火墙结构

防火墙是一种安全有效的防范技术，是访问控制机制、安全策略和防入侵措施。通常分为分组过滤防火墙和基于代理的防火墙两种。

（1）分组过滤防火墙是根据网络层和传输层的头部信息来转发或阻止分组，使用过滤表来确定不转发哪些分组的路由表。对于需要基于报文（应用层）中可利用的信息进行过滤，分组过滤防火墙显得无能