•全国网管技能水平考试唯一指定教材 •全国网管师职业评定指定考试教材

金牌网管师

中级

王 达 阚京茂◎等编著

网络工程方案规划与设计

国内唯一全局视角的企业网络系统设计图书
典型企业综合网络系统设计全面体现
深入、专业分析三大子系统设计技术和方法
专业理论和实战配置完美结合尽显专家本色

◎以企业网络构建流程为主线的网络通信子系统设计
从用户调查、拓扑结构设计，到综合布线系统设计
从设备选型、体系架构规划，到网络系统方案选择

◎以OSI/RM七层架构为主线的网络安全子系统设计
全局剖析各层隐含的主要安全隐患及防范策略
详尽介绍各层主流网络安全管理技术和方案配置

国内著名网络专家
王达
亲自主笔

中国水利水电出版社
www.waterpub.com.cn

全国网管技能水平考试唯一指定教材

全国网管师职业评定指定考试教材

金牌网管师（中级）

网络工程方案规划与设计

王　达　阚京茂　等编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书是“全国网管技能水平考试”（NMSE，“网管师”认证）中级考试和认证中，面向专业、综合的网络系统设计的指定教材。全书共三篇，16章，前两篇（共14章）侧重于介绍企业网络中通信子系统、网络安全子系统的规划与设计，最后一篇介绍了在大型企业网络中才可能需要的网络存储子系统设计的基础知识。在通信子系统和安全子系统的规划与设计中，从最初的用户需求调查、拓扑结构设计等，一直到综合的网络系统方案设计与配置都进行了较为详细的介绍。

本书是目前国内IT图书市场中唯一一本全面、系统、深入地介绍3个主要网络子系统规划与设计的图书，不仅可作为网络工程设计人员的自学教材，还是高校网络系统设计专业的最佳教材选择。

图书在版编目（CIP）数据

金牌网管师（中级）网络工程方案规划与设计 / 王达等编著. -- 北京 : 中国水利水电出版社, 2010.2
全国网管技能水平考试唯一指定教材. 全国网管师职业评定指定考试教材
ISBN 978-7-5084-7164-8

Ⅰ. ①金… Ⅱ. ①王… Ⅲ. ①计算机网络－水平考试－教材 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2010)第012285号

策划编辑：周春元　　责任编辑：张玉玲　　封面设计：李　佳

书　名	全国网管技能水平考试唯一指定教材 全国网管师职业评定指定考试教材 **金牌网管师（中级）网络工程方案规划与设计**
作　者	王　达　阚京茂　等编著
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路1号D座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京蓝空印刷厂
规　格	210mm×285mm　16开本　35印张　1000千字
版　次	2010年4月第1版　2010年4月第1次印刷
印　数	0001—5000册
定　价	68.00元

编委会

序

21 世纪被称为信息时代，信息资源对社会发展的重大意义人所共知，有着全球最大网络用户的中国随着网络产业的不断发展，具备实际操作能力的网络管理人才的大量短缺逐渐成为制约我国信息化发展的“瓶颈”之一。计算机网络业在中国发展不过十几年时间，计算机网络管理职业到2002 年才被正式承认。在中国还未有一个针对我国网络管理人员制定的科学培训体系推出，大学里也没有专门为网管人员设置的专业培训课程。

党中央、国务院高度重视网络建设和管理，为此制定了一系列大政方针，出台了一系列政策法规。2007 年 1 月 23 日，国家主席胡锦涛在中央政治局第 38 次集体学习会议上发表“以创新的精神加强网络文化建设和管理”的重要讲话。胡锦涛指出，各级党委和政府要从加强规划、完善制度、规范管理、充实队伍等方面采取措施，加强信息产业发展与网络文化发展的统筹协调，切实把一手抓发展、一手抓管理的要求贯彻到网络技术、产业、内容、安全等各个方面。要加快网络文化队伍建设，形成与网络文化建设和管理相适应的管理队伍、舆论引导队伍、技术研发队伍，培养一批政治素质高、业务能力强的干部。各级领导干部要重视学习互联网知识，提高领导水平和驾驭能力，努力开创网络文化建设的新局面。

为了提升我国计算机网络管理的核心竞争实力，为了贯彻胡锦涛同志关于“加强网络文化建设和管理”的讲话精神，落实《2006-2020 年国家信息化发展战略》关于人才保障的规划，结合社会对网络管理人才的实际需求和网络管理专业人员职业发展的切身需要，特别是为用人单位提供科学规范的网管技能考评体系，国家工业和信息化部直属中国电子信息产业发展研究院培训中心（原国家信息产业部电子信息中心职业技能培训中心）在 2008 年推出了全国网管技能水平考试（Network Management Skills Examination，简称 NMSE）科学评定体系。本套科学评定体系整合了国家相关教育资源，结合国际技术认证标准，面向就业市场推出网络管理人员技能水平考试。NMSE 按当前网络管理行业实际情况科学划分为四个等级：助理级网管（网吧网管）、初级网管师、中级网管师、高级网管师。

“十一五”期间，我们将按照科学发展观、全面建设小康社会进程，构建社会主义和谐社会，加快实现社会主义现代化的重要战略机遇期的要求，在国家相关部门的监管要求下，不断完善和推广全国网管技能水平考试，为我国信息化建设特别是计算机网络管理行业发展培养出一支适应全球化竞争的高层次、复合式、应用型的中国特色网络管理技术人才队伍。

全国网管技能水平考试管理办公室

阚京茂

前　言

一直以来不断有网友问我，网管到底能不能拿高薪，如何才能拿高薪，或者问到底什么样才算专业，……。对于这类提问，我一般都是反问对方，如果让你自己一人设计一个企业网络，能胜任吗？作为中级网管师，我们不仅要强调具备大中型企业的网络系统管理能力，更重要的是要具备设计出一个大中型企业网络系统的能力。

谈到网络系统设计，许多人并不真正了解，甚至错误地认为那很简单，无非是一些软/硬件产品的组合。其实这是极端错误的。有时我问一些网友是否可以设计出一套网络系统时，有的回答得很干脆，说没问题。可是当我再具体地问一下，某个方面的设计思路和方法，或者所涉及的一些具体技术时，可以说没有一个人能有个全局的概念，最多就是知道把几个相关的技术简单地拼凑起来，至于为什么要这么组合，根本说不出理由。

要真正设计出一套高水平，满足用户应用、安全、存储和管理需求的网络系统，并不是一件容易的事，也不是可以轻松达到的。首先要对相应领域系统设计的基础知识、产品、技术和方案有一个比较深入的了解；然后还需要对相应领域的这些知识、产品、技术和方案有一个全局统领、管理的能力；再就是要有一个如何组织、应用这些技术、产品和方案的清晰的思路与方法。这就是笔者在与读者交流过程中一直强调的系统、全局观念；一定得先经过系统、全面、深入地学习，而不是只孤立地学习某一个方面；一定得有相应领域丰富的管理经验才能胜任专业的网络系统设计工作的原因。因为任何一个网络系统设计都可能要面对整个网络领域的方方面面，正如我们在书中说到的那样，在一个比较完整的网络系统设计中，就可能要面对像通信子系统、安全子系统、存储子系统、应用子系统、办公子系统这 5 个基本模块。如果你只注重某一方面的学习，就不可能全面胜任这样一个复杂的网络系统设计工作，当然也就不可能拿到相应级别的工资待遇。

设计一套网络系统要掌握什么，具体还真说不清，太多、太广了。但任何事情都有一个主流，我们在学习过程中不可能把所有技术、应用和方案都精通掌握，但可以尽可能地掌握当前主流的，这就是本书中所讲的内容。本书介绍了上面所说的五大基本设计模块中的三个主要子系统：通信子系统、安全子系统和存储子系统的规划与设计。对于绝大多数大中型企业来说，通信子系统和安全子系统又更为普遍，所以书中侧重介绍这两个子系统的规划与设计，对于存储子系统，因为目前来说通常只有大型企业网络才需要设计专门的存储子系统，所以在本书中只介绍了基础的网络存储知识和技术。

第 1 章先从宏观角度介绍网络系统设计的基本要素、原则和思路，第 2 章集中介绍在网络系统设计过程中用户需求调查的内容和方法。

在通信子系统的规划与设计篇中，本书按照通信子系统规划与设计的基本步骤，用 5 章内容进行了详细介绍：

第 3 章：网络系统拓扑结构规划与设计，介绍企业局域网和广域网拓扑结构的规划与设计思路和方法。

第 4 章：综合布线系统规划与设计，介绍企业网络中双绞线和光纤综合布线系统的规划与设计思路和方法。

第 5 章：网络设备的选型，介绍企业网络通信子系统中的主要网络设备（如网卡、服务器、交换机、AP、路由器和 UPS 等）的选型考虑和选型方法。

第 6 章：网络体系架构规划与设计，介绍网络系统体系架构的规划与设计的考虑和方法，如网络管理模式的选择、服务器与客户端操作系统的选择、域控制器/DNS/DHCP 服务器的规划与设计、域信任关系的设计考虑等。

第 7 章：企业网络通信子系统结构方案，介绍 Cisco、H3C 等主流网络设备品牌针对各种规模企业网络提供的局域网和广域网系统结构方案，并且对各个方案的方案配置方法和特点进行了详细介绍。

在网络安全子系统的规划与设计篇中，本书按照 OSI/RM 参考模型用 7 章内容对各层主流可用

的网络安全技术、方案以及配置方法进行了详细介绍。

第 8 章：网络安全系统设计综述，从宏观角度介绍网络安全子系统规划与设计的基本思路和方法，以及 OSI/RM 各层中主要流可用的安全技术和方案。

第 9 章：物理层安全方案，介绍 OSI/RM 中物理层可用的主要安全方案，如线路屏蔽、机房屏蔽、物理隔离、线路和设备冗余等。

第 10 章：数据链路层安全方案及应用配置，介绍 OSI/RM 中数据链路层可用的主要安全方案及相关的配置方法，如数据链路加密、WLAN 网络中的各种链路加密方法，以及 MAC 地址与 IP 地址绑定方法等。

第 11 章：网络层 Kerberos 和 IPSec 安全方案及应用配置，介绍 OSI/RM 中网络层的两种主要身份认证技术：Kerberos 和 IPSec 的身份认证原理、体系架构及应用方案配置。

第 12 章：网络层证书服务和 PKI 安全方案及应用配置，介绍 OSI/RM 中网络层的另一种主要身份认证技术——证书服务，以及利用证书服务及其他相关技术的 PKI 安全系统方案设计方法。

第 13 章：传输层安全方案及应用配置，介绍 OSI/RM 中网络层可用的主要安全方案及相关的配置方法，如 TLS、SSL、WTLS、SSH、SOCKS 的技术原理及综合应用配置方法。

第 14 章：Web 服务器安全系统设计与配置，以 Web 服务器为代表介绍应用层 Web 服务器的综合安全系统设计考虑以及相关的配置方法。

在网络存储子系统的规划与设计篇中，由于篇幅原因仅用了两章内容（第 15 和 16 章）介绍与网络存储密切相关的主要技术，如服务器磁盘接口技术、磁盘阵列技术、各种 FC-SAN 和 IP-SAN 存储技术等。

最后，我要衷心感谢许许多多一直关心我、信任我、支持我的读者朋友和各界老师、朋友，是您们的信任与支持，才使我有决心和恒心为国内广大网管、网工朋友编写一部又一部著作，也才使我宁愿牺牲所有的节假日和休息时间，把我毕生的经验积累奉献给大家。当然，无论我再怎么努力，由于时间和精力的原因，书中仍可能存在一些疏漏甚至错误，恳请大家原谅的同时，还望能及时联系我或者出版社，我们将尽快修正。

本书由 NSME 专家团队共同策划并编写，由王达主笔并统稿。参加编写、校验和排版的人员有：马亮、阚京茂、赵增祥、宋希岭、刘中洲、潘朝阳、刘伟、何艳辉、王珂、沈芝兰、马平、何江林、周建辉、周志雄、洪武、高平复、尚宝宏、姚学军、李翔等，在此一并表示由衷的感谢。

若读者有什么问题或建议可以在笔者博客（http://winda.blog.51cto.com、http://blog.zdnet.com.cn/html/84/447184-type-index.html、http://blog.csdn.net/lycb_gz）、学生大本营（http://student.csdn.net/space.php?uid=2334）、以下 13 个分地区的读者服务 QQ 群（每人只能加入对应地区的一个群，另有一个 VIP 读者群）中提出，我们都将尽量及时地为大家解答。

群 1（17201450）：北京、天津、河北
群 2（21566766）：广东、广西、海南
群 3（32354930）：湖北、安徽、河南
群 4（5208368）：宁夏、青海、甘肃、浙江
群 5（13836245）：山东、山西、陕西、上海
群 6（4789821）：云南、贵州、四川、重庆
群 7（73417650）：新疆、西藏、内蒙古、广东
群 8（57828783）：湖南、江西、福建
群 9（17838740）：上海、江苏、浙江
群 10（21576699）：辽宁、吉林、黑龙江、江苏
群 11（74496579）：北京、上海、广东
群 12（69537591）：上海、江苏、浙江、新疆、内蒙古
群 13（19129079）：湖南、湖北、江西、福建、四川

编　者

2009 年 10 月

目　　录

序

前言

第 1 章　网络工程设计综述 …… 1

1.1　网络工程设计基础 …… 2

1.1.1　网络系统集成概述 …… 2

1.1.2　网络工程设计综述 …… 3

1.2　网络工程设计的考虑 …… 4

1.2.1　网络通信标准和协议的选择考虑 …… 4

1.2.2　网络规模和网络拓扑结构考虑 …… 5

1.2.3　网络功能和应用需求考虑 …… 7

1.2.4　可扩展性和可升级性考虑 …… 7

1.2.5　其他方面的考虑 …… 8

1.3　网络工程集成设计的步骤和原则 …… 10

1.3.1　网络工程集成设计的一般步骤 …… 10

1.3.2　网络工程集成设计的基本原则 …… 13

1.3.3　局域网系统设计的主要内容 …… 16

1.3.4　广域网系统设计的主要内容 …… 18

第 2 章　用户需求调查与分析 …… 19

2.1　用户调查内容 …… 20

2.1.1　一般企业状况调查 …… 20

2.1.2　应用需求调查 …… 22

2.1.3　功能需求调查 …… 23

2.1.4　性能需求调查 …… 25

2.1.5　管理需求调查 …… 28

2.2　用户性能需求分析 …… 29

2.2.1　接入速率需求分析 …… 29

2.2.2　吞吐性能需求分析 …… 32

2.2.3　可用性能需求分析 …… 34

2.2.4　并发用户数需求分析 …… 36

2.2.5　可扩展性需求分析 …… 37

第一篇　网络通信子系统设计篇

第 3 章　网络拓扑结构规划与设计 …… 42

3.1　网络拓扑结构 …… 43

3.1.1　局域网拓扑结构 …… 43

3.1.2　广域网拓扑结构 …… 43

3.2　网络拓扑结构绘制 …… 46

3.2.1　简单网络拓扑结构图元的获取 …… 47

3.2.2　拓扑结构绘制 …… 49

3.3　网络拓扑结构设计 …… 57

3.3.1　小型星型网络结构设计示例 …… 57

3.3.2　中型扩展星型网络结构设计示例 …… 59

3.3.3　大型混合型网络结构设计示例 …… 62

3.3.4　园区网络结构设计示例 …… 65

3.3.5　无线局域网结构设计示例 …… 69

3.4　广域网网络拓扑结构设计 …… 70

3.4.1　小型企业互联网接入拓扑结构设计 … 71

3.4.2　X.25 广域网接入拓扑结构设计 …… 72

3.4.3　FR 广域网接入拓扑结构设计 …… 74

3.4.4　ATM 广域网接入拓扑结构设计 …… 76

3.4.5　光纤接入广域网拓扑结构设计 …… 78

第 4 章　综合布线系统规划与设计 …… 82

4.1　综合布线系统概述 …… 83

4.1.1　综合布线系统的由来 …… 83

4.1.2　综合布线系统的组成 …… 83

4.1.3　综合布线系统的特点 …… 85

4.2　综合布线标准 …… 86

4.2.1　综合布线标准的发展历程 …… 86

4.2.2　我国等效采用的综合布线标准 …… 87

4.3　综合布线系统中的传输介质标准 …… 88

4.3.1　双绞线综合布线标准 …… 88

4.3.2　双绞线布线标准中的参数测试规范 … 90

4.3.3　光缆布线装置 …… 93

4.3.4　光缆布线标准 …… 97

4.4　综合布线系统设计 …… 99

4.4.1　综合布线系统设计的基本步骤 …… 99

4.4.2　3 个综合布线系统设计等级 …… 99

4.4.3　综合布线系统的设计要领 …… 101

4.5　综合布线系统设计要点 …… 102

4.5.1　工作区子系统设计要点 …… 102

4.5.2 水平子系统设计要点……103
4.5.3 垂直干线子系统设计要点……104
4.5.4 设备间子系统设计要点……106
4.5.5 管理子系统设计要点……107
4.5.6 建筑群子系统设计考虑……109
第5章 网络设备的选型……111
5.1 网卡的选型……112
5.1.1 有线以太网卡的选型……112
5.1.2 无线局域网网卡的选型……117
5.1.3 网卡的综合选型考虑……118
5.2 服务器的选型……120
5.2.1 服务器处理器架构的选型……120
5.2.2 服务器的综合选型考虑……122
5.3 交换机和无线 AP 的选型……124
5.3.1 交换机的综合选型考虑……124
5.3.2 无线 AP 的综合选型考虑……129
5.4 路由器的选型……130
5.4.1 边界和中间节点路由器的选型……131
5.4.2 宽带路由器的选型……132
5.4.3 企业级路由器的综合选型考虑……134
5.5 防火墙的选型……136
5.5.1 防火墙的选型……137
5.5.2 防火墙的综合选型考虑……138
5.6 UPS 的选型与选购……142
5.6.1 UPS 的主要作用和分类……142
5.6.2 主要 UPS 技术……143
5.6.3 UPS 的综合选型考虑……145
第6章 网络体系架构规划与设计……147
6.1 两种网络架构模型……148
6.1.1 P2P 网络架构模型……149
6.1.2 C/S 网络架构模型……150
6.2 P2P 工作组局域网架构设计考虑……151
6.3 域网络架构设计的基本考虑……153
6.3.1 域网络操作系统选择的考虑……154
6.3.2 林和域的规划基础……156
6.3.3 新建林、子域和域树的考虑……157
6.3.4 域命名空间规划考虑……159
6.3.5 域和林信任关系的设计考虑……163
6.3.6 多域环境下的访问控制策略规划与设计……166
6.3.7 域控制器和成员服务器的规划与设计……170
6.3.8 DNS 服务器的规划考虑……172
6.3.9 DHCP 服务器的规划考虑……174
第7章 企业网络通信子系统结构方案……180
7.1 小型 SOHO 办公室网络系统结构方案……181
7.1.1 小型 SOHO 办公室网络方案的特点与要求……181
7.1.2 Cisco 小型 SOHO 办公室有线局域网方案……182
7.1.3 H3C 小型 SOHO 办公室有线局域网方案……185
7.1.4 小型 SOHO 办公室的 WLAN 方案……189
7.1.5 小型 SOHO 办公室局域网的互联网连接……192
7.2 中小型企业网络系统结构方案……193
7.2.1 中小型企业局域网方案的特点与要求……193
7.2.2 Cisco 中小型企业有线局域网方案……194
7.2.3 H3C 中小型企业有线局域网方案……200
7.2.4 Cisco 1800 的中小型企业广域网连接方案……204
7.2.5 H3C 中小型企业广域网连接方案……207
7.3 中型企业网络系统结构方案……210
7.3.1 中型企业网络方案的主要特点与要求……210
7.3.2 Cisco 中型企业局域网方案……211
7.3.3 H3C 中型局域网方案……215
7.3.4 Cisco 中型企业网络的广域网连接方案……218
7.3.5 H3C 中型企业网络的广域网连接方案……222
7.4 大中型企业网络结构方案……226
7.4.1 大中型网络方案的特点与要求……226
7.4.2 Cisco 大中型局域网方案……227
7.4.3 H3C 大中型局域网方案……232
7.4.4 Cisco 大中型网络广域网连接方案……237

第二篇 网络安全子系统规划与设计

第8章 网络安全系统设计综述……242
8.1 网络安全系统设计基础……243

8.1.1 网络安全系统的发展……243
8.1.2 网络安全威胁综述……244
8.1.3 企业网络的主要安全隐患……246
8.1.4 常用网络安全防护策略……247
8.1.5 网络安全系统设计基本原则……248
8.2 OSI/RM 各层的安全保护概述……250
8.2.1 物理层的安全保护……251
8.2.2 数据链路层的安全保护……252
8.2.3 网络层的安全保护……253
8.2.4 传输层的安全保护……254
8.2.5 会话层和表示层的安全保护……255
8.2.6 应用层的安全保护……255
8.3 网络安全系统设计的基本思路……255
8.3.1 安全隐患分析和基本系统结构信息的收集……256
8.3.2 调查和分析当前网络的安全需求……259
8.3.3 现有网络安全策略评估……259
8.3.4 设计细化的新网络安全策略初稿……260
8.3.5 方案的测试、评估和修改……265
8.3.6 方案定稿和应用……266
第 9 章 物理层安全方案……267
9.1 物理层的线路窃听技术分析……268
9.2 计算机网络通信线路屏蔽……269
9.2.1 选择屏蔽性能好的传输介质和适配器……269
9.2.2 屏蔽机房和机柜的选择……272
9.2.3 WLAN 无线网络的物理层安全保护……273
9.3 物理线路隔离……273
9.3.1 主要的物理隔离产品……273
9.3.2 物理隔离网闸隔离的原理……276
9.4 设备和线路冗余……279
9.4.1 网络设备部件冗余……279
9.4.2 网络设备整机冗余……281
9.4.3 网络线路冗余……282
9.5 机房和账户安全管理……283
9.5.1 机房安全管理……283
9.5.2 账户安全管理……284
9.6 物理层安全管理工具……284
9.6.1 泛达综合布线实时管理系统……284
9.6.2 Molex 综合布线实时管理系统……287
第 10 章 数据链路层安全方案及应用配置……289
10.1 典型的数据加密算法……290
10.1.1 基于“消息摘要”的算法……290
10.1.2 “对称/非对称密钥”加密算法……292
10.2 数据加密……294
10.2.1 数据加密技术……294
10.2.2 链路加密机……297
10.2.3 网卡集成式链路加密原理……299
10.3 WLAN 数据链路层保护方案……301
10.3.1 WLAN SSID 安全技术及配置方法……301
10.3.2 WLAN MAC 地址过滤及配置……303
10.3.3 WLAN WEP 加密……304
10.3.4 WLAN WPA/WPA2 加密认证……306
10.4 无线 AP/路由器的 WPA 和 WPA2 设置……309
10.4.1 个人用户无线 AP/路由器的 WPA-PSK 或 WPA2-PSK 设置……309
10.4.2 企业级无线 AP/路由器的 WPA 或 WPA2 设置……310
10.4.3 WLAN 客户端第三方软件的 WPA 和 WPA2 设置……311
10.4.4 Windows XP 无线客户端 WPA/WPA2 配置……314
10.5 MAC 地址欺骗防护……316
10.5.1 ARP 和 RARP 协议工作原理……316
10.5.2 MAC 地址欺骗原理……317
10.5.3 MAC 地址欺骗源的查找和预防……318
10.6 Cisco 设备基于端口的 MAC 地址绑定……320
10.6.1 基于端口的单一 MAC 地址绑定的基本配置步骤……321
10.6.2 基于端口的单一 MAC 地址绑定配置示例……322
10.6.3 基于端口的多 MAC 地址绑定配置思路……322
10.7 Cisco 设备基于 IP 地址的 MAC 地址绑定……323
10.7.1 一对一的 MAC 地址与 IP 地址绑定……323
10.7.2 一对多或者多对多的 MAC 地址与 IP 地址绑定示例……324
第 11 章 网络层 Kerberos 和 IPSec安全方案及应用配置……325
11.1 身份认证概述……326
11.1.1 主要的身份认证方式……326

11.1.2 单点登录身份认证执行方式……327
11.2 Kerberos 身份认证……328
11.2.1 Kerberos v5 身份认证机制……328
11.2.2 Kerberos v5 身份认证的优点与缺点……331
11.3 Kerberos 应用原理与配置示例……332
11.3.1 利用 kerberos 进行本地登录的原理……332
11.3.2 利用 Kerberos 进行域登录的原理和示例……333
11.3.3 Kerberos v5 身份认证的策略配置……337
11.4 IPSec 协议……338
11.4.1 IPSec 的两种使用模式……339
11.4.2 IPSec 的 AH 协议……340
11.4.3 IPSec 的 ESP 协议……343
11.5 IPSec 协议应用方案设计与配置思路……346
11.5.1 IPSec 策略规则……346
11.5.2 IPSec 安全通信方案的主要应用……350
11.5.3 不推荐使用 IPSec 协议保护的应用方案……354
11.5.4 配置 IPSec 应用方案前的准备……355
11.5.5 配置 IPSec 安全应用方案的基本步骤……355
11.6 IPSec 在 Web 服务器访问限制中的应用配置示例……356
11.6.1 创建两个筛选器操作……356
11.6.2 创建 IP 筛选器列表……359
11.6.3 创建和指派 IPSec 策略……363
11.7 IPSec 的其他应用方案示例……367
11.7.1 IPSec 在数据库服务器访问限制中的应用配置示例……367
11.7.2 IPSec 在阻止 NetBIOS 攻击中的应用配置示例……367
11.7.3 IPSec 在保护远程访问通信中的应用配置示例……369
第 12 章 网络层证书服务和 PKI安全方案及应用配置……373
12.1 证书和证书服务基础……374
12.1.1 证书概述……374
12.1.2 证书的主要功能……375
12.1.3 证书的主要应用……376
12.2 Windows Server 2003 系统 PKI 体系……380
12.2.1 Windows Server 2003 系统 PKI 体系基础功能设施……380
12.2.2 Windows Server 2003 系统 PKI 体系规划和部署的基本流程……381
12.3 定义证书需求……382
12.3.1 确定安全应用需求……382
12.3.2 确定证书需求……386
12.3.3 文档化证书策略和证书实施声明……387
12.3.4 定义证书应用需求步骤示例……388
12.4 证书颁发机构层次结构设计……389
12.4.1 规划核心 CA 选项……389
12.4.2 选择信任模式……398
12.4.3 CA 层次结构设计中的其他步骤……401
12.4.4 CA 层次结构设计示例……402
12.5 扩展证书颁发机构结构……403
12.5.1 评估影响扩展信任的因素……404
12.5.2 选择扩展 CA 结构配置……406
12.5.3 限制计划外的信任……408
12.6 定义证书配置文件……409
12.6.1 选择证书模板……410
12.6.2 选择证书安全选项……410
12.6.3 使用合格的从属来限制证书……413
12.6.4 配置证书示例……417
12.7 创建证书管理规划……418
12.7.1 选择注册和续订方法……418
12.7.2 将证书映射到用户账户……419
12.7.3 创建证书吊销策略……423
12.7.4 密钥和数据恢复……426
12.7.5 创建证书管理规划示例……427
第 13 章 传输层安全方案及应用配置……428
13.1 TLS/SSL 基础……429
13.1.1 TLS/SSL 简介……429
13.1.2 TLS 与 SSL 的区别……430
13.1.3 常见的 TLS/SSL 应用……430
13.2 Windows Server 2003 TLS/SSL 体系架构……432
13.2.1 安全通道 SSPI 体系架构……432
13.2.2 TLS/SSL 体系架构……433
13.3 TLS/SSL 在 IIS Web 服务器中的应用……434
13.3.1 安装 CA……435
13.3.2 生成证书申请……436
13.3.3 提交证书申请……438
13.3.4 证书的颁发和导出……441
13.3.5 在 Web 服务器上安装证书……444

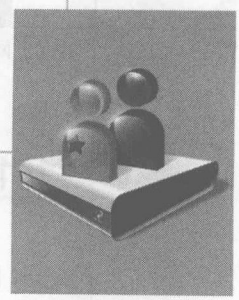
13.3.6 在 Web 服务器上启用 SSL ····· 445
13.4 WLAN 网络中的传输层安全协议 WTLS ····· 446
13.4.1 WAP 的主要特点和体系架构 ····· 447
13.4.2 WAP 架构与 WWW 架构的比较 ···· 450
13.4.3 WAP 安全机制 ····· 451
13.4.4 WTLS 体系架构 ····· 453
13.4.5 WTLS 的安全功能 ····· 454
13.4.6 WTLS 与 TLS 的区别 ····· 455
13.5 SSH 和 SOCKS 协议 ····· 456
13.5.1 SSH 协议 ····· 456
13.5.2 SOCKS 协议 ····· 458
第 14 章 Web 服务器安全系统设计与配置 ····· 460
14.1 Web 服务器的安全威胁与对策分析 ····· 461
14.1.1 主机枚举攻击及防御策略 ····· 461
14.1.2 拒绝服务攻击及防御策略 ····· 464
14.1.3 其他攻击及预防策略 ····· 466
14.2 安全 Web 服务器检查表 ····· 467
14.2.1 程序修补和更新 ····· 467
14.2.2 安装 IISLockdown ····· 469
14.2.3 禁用不需要的服务 ····· 469
14.2.4 禁用不需要的协议 ····· 474
14.2.5 禁用或正确使用账户 ····· 474
14.2.6 正确配置文件和目录访问权限 ····· 476
14.2.7 删除不必要的共享和正确使用共享 477
14.2.8 限制端口 ····· 478
14.2.9 正确配置注册表 ····· 479
14.2.10 正确配置和使用审核与日志记录 ····· 479
14.2.11 正确配置站点和虚拟目录 ····· 481
14.2.12 正确配置脚本映射和 ISAPI 过滤器 ····· 482
14.2.13 正确配置 IIS 元数据库和服务器证书 ····· 483
14.2.14 代码访问安全性 ····· 484
14.2.15 IIS Web 服务器的整体安全检查表 ····· 485

第三篇 网络存储子系统设计篇

第 15 章 网络存储基础 ····· 488
15.1 3 种主流的数据存储方式 ····· 489
15.1.1 DAS 数据存储方式 ····· 489
15.1.2 NAS 数据存储方式 ····· 490
15.1.3 SAN 数据存储方式 ····· 491
15.2 SCSI 接口 ····· 493
15.2.1 SCSI 接口简介 ····· 493
15.2.2 SCSI 设备连接 ····· 494
15.3 SATA 接口 ····· 496
15.3.1 SATA 简介 ····· 496
15.3.2 SATA 的技术特性 ····· 497
15.3.3 SATA II 标准 ····· 499
15.3.4 eSATA 规范 ····· 501
15.4 SAS 接口 ····· 502
15.4.1 SAS 接口简介 ····· 503
15.4.2 SAS 接口结构 ····· 504
15.4.3 SAS 接口的设备连接 ····· 505
15.5 磁盘阵列（RAID） ····· 507
15.5.1 主要 RAID 模式 ····· 508
15.5.2 主要 RAID 模式比较 ····· 514
第 16 章 SAN 网络存储 ····· 516
16.1 SAN 基础 ····· 517
16.1.1 SAN 的基本特性 ····· 517
16.1.2 光纤通道（FC）基础 ····· 518
16.2 FC 体系结构和标准 ····· 520
16.2.1 FC 体系结构 ····· 520
16.2.2 FC 标准 ····· 521
16.3 FC 的 3 种主要拓扑架构 ····· 522
16.3.1 点对点架构 ····· 522
16.3.2 光纤通道仲裁环架构 ····· 523
16.3.3 交换式架构 ····· 525
16.4 光纤通道设备 ····· 526
16.4.1 光纤通道端口类型 ····· 527
16.4.2 FC-SAN 的主要设备 ····· 527
16.4.3 光纤集线器和交换机 ····· 528
16.5 IP SAN 存储基础 ····· 530
16.5.1 IP 存储概述 ····· 530
16.5.2 IP 存储的优势和面临的挑战 ····· 531
16.6 iSCSI-SAN ····· 532
16.6.1 iSCSI 协议基础 ····· 533
16.6.2 iSCSI 协议栈和数据包封装 ····· 534
16.6.3 iSCSI-SAN 应用方案体系架构 ····· 535

16.6.4 iSCSI-SAN 的优缺点 …… 537
16.7 FCIP-SAN …… 538
16.7.1 FCIP 协议基础 …… 538
16.7.2 FCIP 协议栈和数据封装 …… 540
16.7.3 FCIP-SAN 存储 …… 541
16.8 iFCP-SAN …… 542
16.8.1 iFCP 协议基础 …… 542
16.8.2 iFCP-SAN 存储 …… 543
16.9 3 种主要 IP 存储协议的比较 …… 544
16.10 FCoE 技术 …… 546
16.10.1 FCoE 协议概述 …… 546
16.10.2 FCoE-SAN 所带来的好处 …… 547

第 1 章



网络工程设计综述

网络工程设计是网络系统集成工程的前期工作，也是网络系统集成最重要的工作。网络工程设计的最终结果就是工程设计报告和施工规范，用于指导后期的网络工程施工、维护和管理。工程设计报告又是网络系统集成工程竞标的最主要文件，所以网络工程设计的好坏直接关系着工程竞标的成败，非常关键。即使是不用参加竞标的工程，网络系统设计的好坏也是非常重要的，因为它直接决定了最终构建的网络系统是否符合用户要求，也就相当于决定了工程的最终成败。

目前，对于中型以上的企业网络来说，整个网络工程设计主要包括：网络通信子系统、网络安全子系统和网络存储子系统这 3 个主要子系统（还可能有像网络应用子系统、自动办公子系统等）的设计。本章首先从宏观角度介绍这 3 个子系统的设计，然后再各单独用一篇来介绍这 3 个子系统的设计和主要方案。但要注意的是，本章所介绍的基本流程是按大中型网络工程的设计流程来展开的，并不要求所有网络工程的设计都要严格遵守这个设计流程，因为有些小型网络工程设计中有些步骤是无须进行的，如小型办公室网络就不需要综合布线考虑，只需要考虑网络布线部分；也可能对网络安全没有那么高要求，无须专门设计网络安全子系统。

教学（自学）课时安排

课时安排	本章老师共需安排 2 个授课课时。	
授课课时	主要内容	重点
1	①网络系统集成主要内容 ②网络通信协议的选择考虑 ③网络规模和网络结构考虑 ④网络功能和应用需求考虑 ⑤可扩展性和可升级性考虑	①网络通信协议的选择考虑 ②网络规模和网络结构考虑 ③网络功能和应用需求考虑 ④可扩展性和可升级性考虑
2	①网络工程设计的一般步骤 ②网络工程设计的基本原则 ③局域网系统设计的主要内容 ④广域网系统设计的主要内容	①网络工程设计的一般步骤 ②网络工程设计的基本原则 ③局域网系统设计的主要内容

1.1 网络工程设计基础

网络工程设计所做的工作就是整个网络系统（包括网络的各方面，如网络通信子系统、网络安全子系统、网络存储子系统、网络应用子系统、网络办公子系统等）的设计，是工程施工的依据和后期维护、管理的重要参考。具体要设计哪些子系统模块，要因不同网络规模和应用需求来区别对待。如在绝大多数中小型企业网络中，通常只有网络通信子系统的设计模块，没有专门的网络安全和网络存储两个子系统模块，只是把这两个子系统模块附属在网络通信子系统的设计过程中来考虑。本书将以典型的大中型企业网络系统设计为例介绍上述这 3 个子系统设计过程中的主要方法和案例。

1.1.1 网络系统集成概述

网络工程设计是整个网络系统集成（System Integration，SI）工程的前期工作，是通过结构化的综合布线系统和计算机网络技术将各个分离的设备（如用户计算机、打印机、网络设备等）、功能和信息等集成到相互关联的、统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理。系统集成应采用功能集成、网络集成、软件界面集成等多种集成技术。系统集成实现的关键在于解决系统之间的互连和互操作性问题，它是一个多厂商、多协议和面向各种应用的体系结构。这需要解决各类设备、子系统间的接口、协议、系统平台、应用软件等与子系统、建筑环境、施工配合、组织管理和人员配备相关的一切面向集成的问题。

总体来说，系统集成主要还是包括硬件集成和软件集成两个方面，硬件集成就是网络设备系统集成，而软件集成可以看成是应用系统集成。

1．设备系统集成

设备系统集成，通常也直接称为系统集成，或者称为弱电系统集成，以区分于机电设备安装类的强电集成。它是指以构建组织机构内的信息化管理平台为目的，利用综合布线技术、楼宇自控技术、计算机网络通信技术、网络设备互联技术、多媒体应用技术、网络安全防护技术等将相关设备、软件进行集成设计、安装调试、界面定制开发和应用支持。

设备系统集成也可分为智能建筑系统集成、计算机网络系统集成、安防系统集成 3 个方面。

- 智能建筑系统集成

智能建筑系统集成（Intelligent Building System Integration，IBSI）是将建筑物内各弱电子系统集成在一个计算机网络平台上，从而实现子系统间信息、资源和任务的共享，为物业管理者提供高效、便利、可靠的管理手段，给物业使用者提供全面、优质、安全、舒适的综合服务。

- 计算机网络系统集成

计算机网络系统集成（Computer Network System Integration，CNSI）是指通过结构化的综合布线系统和计算机网络技术，将各个分离的设备（如个人计算机）、功能和信息等集成到相互关联的、统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理。计算机网络系统集成包括功能集成、网络集成、软件界面集成等多种集成技术。其实现的关键在于解决系统之间的互连和互操作性问题，因为它是一个多厂商、多协议和面向各种应用的综合体系结构，需要解决各类设备、子系统间的接口、协议、系统平台、应用软件等与子系统、建筑环境、施工配合、组织管理和人员配备相关的一切面向集成的问题。

- 安防系统集成

安防系统集成（Security System Integration，SSI）是指以构建组织机构内的安全防范管理平

台为目的，利用综合布线技术、计算机网络通信技术、网络设备互联技术、多媒体应用技术、安全防范技术、网络安全技术等将相关设备、软件进行集成设计、安装调试、界面定制开发和应用支持。安防系统集成实施的子系统包括门禁系统、楼宇对讲系统、监控系统、防盗报警、一卡通、停车管理、消防系统、多媒体显示系统、远程会议系统。安防系统集成既可作为一个独立的系统集成项目，也可作为一个子系统包含在智能建筑系统集成中。

2．应用系统集成

应用系统集成（Application System Integration，ASI）是以全局、系统的高度为客户量身设计一整套计算机网络应用解决方案，是系统集成的高级阶段，也是建立在系统集成基础之上的，独立的应用软件供应商将成为核心。应用系统集成已经深入到用户的具体业务和应用层面。在大多数场合，应用系统集成又称为行业信息化解决方案集成。

1.1.2 网络工程设计综述

“网络工程设计”是“网络系统集成”中的先期工作，是针对具体用户所需网络中的所有软硬件系统方案设计的，从最基础网络拓扑结构、综合布线系统，到 Office 办公系统、文件打印系统，再到当前主流的 MIS 管理系统和 ERP、B2C 电子商务应用系统，最后到互联网应用和外网的互联，这一切无不都是网络工程设计需要解决的内容。

因为网络工程设计所需设计的项目非常多，涉及面非常广，这就涉及了各具体项目之间的关联（也就通常所说的“接口”问题）和综合考虑。在网络工程设计中，不仅要考虑到当前系统的应用，还要考虑到与之关联的其他系统的应用与互联；不仅要考虑到网络应用需求，还要考虑到网络安全需求；不仅要考虑到当前的应用需求，还要考虑到在未来一段时间内的应用需求发展；不仅要考虑到关键应用的性能需求，还要尽可能平衡各用户节点的性能；不仅要考虑到高性能，还要追求高的性价比，……，是一项综合的系统工程。正因为如此，在进行网络工程设计时一定要有全局观念、系统观念，当然这也要求工程设计人员具有全面、系统、专业的工程设计水平。

【经验之谈】在这里，要特别注意的一点是，现在许多人认为，从事网络工程设计只要具备网络设备连接、配置和调试方面的能力就行了，其实这是非常错误的。网络工程系统的设计不仅是网络拓扑结构的设计，更是网络应用系统、网络管理系统、网络安全系统、网络存储系统等的设计。没有专业的网络系统管理经验，是不可能设计出真正符合用户需求，符合网络应用、管理、安全和存储需求的系统的。所以笔者一直奉劝那些一毕业就想进网络集成公司，成为专业的网络工程师的大学毕业生，最好不要这样规划自己的职业人生，因为这是不科学的职业规划，也不符合网络职业发展规律，也必将严重影响自己将来的网络职业发展之路。万丈高楼平地起，网管是网工的基础，必须先做好一个专业的网管才可能成为一名专业的网络工程师。

有些小型个体企业，为了节省投资，通常是从二手市场中购买一些淘汰的设备，如 10Mb/s 的集线器或交换机，结果尽管网络规模相当小，但仍可能导致当前的一些基本网络应用都无法顺利进行。同时这也是一种对原有投资不负责任的态度，因为这些早已淘汰的设备在未来的网络应用中根本无法使用，这是对当前或未来一段时间内主流网络应用需求考虑不周所导致的。还有些用户的网络虽然能正常连通，一般的文件和资源共享应用也没什么问题，但却在网络安全上考虑得不够，给网络中的服务器甚至客户机带来极大的安全风险。也有些网络没有充分考虑到网络用户的发展需求，在经过了小规模的扩展后，因核心层交换机端口带宽的不足导致整个网络连接性能的大幅下降。还有些工程师在网络工程设计时没有充分考虑网络系统的升级与扩展，在需要升级时便发现有许多设备根本无法通过现有组件、模块或者固件升级而实现，需要重新购买，浪费了大量的软硬件投资。

另外，如今的网络应用不再仅局限于单一局域网中，许多关键性的应用通常涉及多个局域网的互联（如通过 VPN 互联而实现的不同局域网系统数据库、ERP 系统互联等），或者与其他外部网络（如互联网）的连接，如电子商务。在这样一个彼此关联的网络系统中，网络应用所需的带宽和安全需求就成了重中之重。因为像网络连接性能和安全性能严格遵循木桶原理，最终的性能不是取决于网络中最好的那部分，而是取决于最差的那部分。

通常的局域网系统设计包括：机房规划、基本网络拓扑结构、综合布线结构、IP 地址规划、域系统结构、各种网络服务器（如 DNS 服务器、DHCP 服务器、WINS 服务器等）部署、服务器选型（包括服务器档次、服务器架构、所支持的磁盘阵列级别等）、服务器操作系统、客户端操作系统、OA 办公系统、打印系统、数据库系统、MIS 系统、ERP 系统、电子商务、数据存储系统、数据备份与容灾系统、防火墙系统（包括 DMZ 区域部署）、病毒防护系统、入侵检测系统等。当然以上各方面并不要求在设计之初就全部到位，有些应用（如网络打印、ERP、电子商务和入侵检测系统等）可能暂时没有部署的必要，也不是要求所有网络系统都需要设计以上各部分，特别是网络功能和应用系统部分，但在网络系统设计时最好兼顾考虑，这样就可以为日后的应用扩展打下很好的基础。

如果是广域网系统设计，则要充分考虑的是：网络接入方式、网络中继传输方式和数据交换方式。当然在这些网络选型中一定要结合所支持的业务类型和成本综合考虑。另外，选择合适的 ISP（因特网服务提供商）或 NSP（网络服务提供商）也是非常重要的。

以上这些局域网系统设计和广域网系统设计项目在具体实施前都需要建立在全面、详细的用户调查之上。这虽然是前期工作，但对于整个系统设计却关系重大，稍不谨慎就可能导致最终付出了高昂代价的系统不能满足用户的需求，甚至产生与用户之间的矛盾。

1.2 网络工程设计的考虑

本章前面就已经说到，网络工程设计需要考虑的内容非常多，涉及网络系统中所有软硬件系统的方方面面。首先需要从宏观上确定一些主要方面，然后再根据这些主要方面逐步展开、细化，最终形成一个完整的工程设计方案。

1.2.1 网络通信标准和协议的选择考虑

现在的企业计算机网络一般不是单独的局域网应用那么简单了，所以现在设计一个网络工程系统都需要从局域网和广域网两个方面来考虑。在网络通信协议上，也需要考虑局域网通信协议和广域网通信协议两个方面。当然这只是一个最粗放的划分方式，在局域网和广域网通信协议中又要根据实际的网络通信、应用需求选择具体的通信协议。通信协议的选择一定要根据具体的网络类型、网络应用和网络管理等方面的需求来考虑。

- 局域网通信标准和规范的选择考虑

在网络类型方面，现在的局域网基本上都是基于 TCP/IP 协议的以太网络。在以太网中，又有许多不同的以太网标准和规范，现在主流的有 10/100Mb/s 快速以太网、1000Mb/s 千兆位以太网、10Gb/s 万兆以太网。10/100Mb/s 快速以太网最多只应用于接入层，1000Mb/s 是目前最主流应用的以太网标准，10Gb/s 主要是在一些大型的局域网核心层中应用。

而在这些不同的以太网标准中又有许多具体的以太网规范，如快速以太网的 100Base-TX、100Base-T、100Base-FX 规范，千兆位以太网的 1000Base-LX、1000Base-SX、1000Base-LH、1000Base-ZX、1000Base-LX10 和 1000Base-BX10 等；在万兆以太网标准中，应用于局域网的基于双绞线（6 类以上）的万兆以太网规范有 10GBase-CX4、10GBase-KX4、10GBase-KR 和