



21 世纪大学本科
计算机专业系列教材

吴功宜 吴英 编著

计算机网络教师用书

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

- 根据教育部高教司主持评审的《中国计算机科学与技术学科教程 2002》组织编写
- 与美国 ACM 和 IEEE/CS *Computing Curricula 2001* 同步

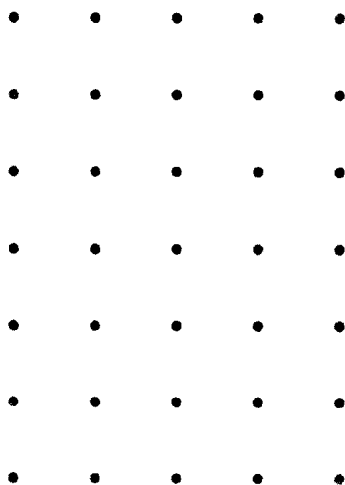


清华大学出版社

21世纪大学本科计算机专业系列教材

计算机网络教师用书

吴功宜 吴英 编著



清华大学出版社
北京

内 容 简 介

本书是《计算机网络》(吴功宜著,清华大学出版社2003年出版)的配套教材。全书的内容分为两个部分。第0章主要对网络课程的知识点结构和教学方法进行了讨论。第1~9章针对《计算机网络》教材的具体章节中的一些重点与难点问题进行了讨论,同时还提供一些对于理解某一项技术比较重要的背景资料。本书在有关章节中提供了一些有用的网站地址或RFC文档。

本书可以作为担任计算机网络、数据通信技术及相关课程教学的教师的教学参考书,也可以作为计算机专业的本科生以及电子信息类专业本科、研究生与工程技术人员的学习参考书。

版权所有,翻印必究。举报电话:010-62782989 13901104297 13801310933

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

计算机网络教师用书/吴功宜,吴英编著. —北京:清华大学出版社,2004.8

(21世纪大学本科计算机专业系列教材)

ISBN 7-302-08956-6

I. 计… II. ①吴… ②吴… III. 计算机网络—高等学校—教学参考资料 IV. TP393

中国版本图书馆CIP数据核字(2004)第063271号

出 版 者: 清华大学出版社 地 址: 北京清华大学学研大厦

<http://www.tup.com.cn> 邮 编: 100084

社 总 机: 010-62770175 客 户 服 务: 010-62776969

组稿编辑: 张瑞庆

文稿编辑: 咏 鹏

封面设计: 孟繁聪

印 刷 者: 清华大学印刷厂

装 订 者: 三河市李旗庄少明装订厂

发 行 者: 新华书店总店北京发行所

开 本: 185×230 印 张: 22.5 字 数: 463 千字

版 次: 2004年8月第1版 2004年8月第1次印刷

书 号: ISBN 7-302-08956-6/TP·6336

印 数: 1~2000

定 价: 29.80 元

本书如存在文字不清、漏印以及缺页、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)62770175-3103 或 (010)62795704

21 世纪大学本科计算机专业系列教材编委会

名誉主任：陈火旺

主 任：李晓明

副 主 任：钱德沛 焦金生

委 员：（按姓氏笔画为序）

马殿富	王志英	王晓东	宁 洪	刘 辰
孙茂松	李大友	李仲麟	吴朝晖	何炎祥
宋方敏	张大方	张长海	周兴社	侯文永
袁开榜	钱乐秋	黄国兴	蒋宗礼	曾 明
廖明宏	樊孝忠			

秘 书：张瑞庆

本书责任编辑：钱德沛

PREFACE

21 世纪是知识经济的时代,是人才竞争的时代。随着 21 世纪的到来,人类已步入信息社会,信息产业正成为全球经济的主导产业。计算机科学与技术的信息产业中占据了最重要的地位,这就对培养 21 世纪高素质创新型计算机专业人才提出了迫切的要求。

为了培养高素质创新型人才,必须建立高水平的教学计划和课程体系。在 20 多年跟踪分析 ACM 和 IEEE 计算机课程体系的基础上,紧跟计算机科学与技术的发展潮流,及时制定并修正教学计划和课程体系是尤其重要的。计算机科学与技术的发展对高水平人才的要求,需要我们从总体上优化课程结构,精炼教学内容,拓宽专业基础,加强教学实践,特别注重综合素质的培养,形成“基础课程精深,专业课程宽新”的格局。

为了适应计算机科学与技术学科发展和计算机教学计划的需要,要采取多种措施鼓励长期从事计算机教学和科技前沿研究的专家教授积极参与计算机专业教材的编著和更新,在教材中及时反映学科前沿的研究成果与发展趋势,以高水平的科研促进教材建设。同时适当引进国外先进的原版教材。

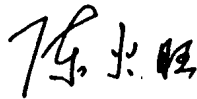
为了提高教学质量,需要不断改革教学方法与手段,倡导因材施教,强调知识的总结、梳理、推演和挖掘,通过加快教案的不断更新,使学生掌握教材中未及时反映的学科发展新动向,进一步拓广视野。教学与科研相结合是培养学生实践能力的有效途径。高水平的科研可以为教学提供最先进的高新技术平台和创造性的工作环境,使学生得以接触最先进的计算机理论、技术和环境。高水平的科研还可以为高水平人才的素质教育提供良好的物质基础。学生在课题研究中不但能了解科学研究的艰辛和科研工作者的奉献精神,而且能熏陶和培养良好的科研作风,锻炼和培养攻关能力和协作精神。

进入 21 世纪,我国高等教育进入了前所未有的大发展时期,时代的进步与发展对高等教育质量提出了更高、更新的要求。2001 年 8 月,教育部颁发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》。文件指出,本科教育是高等教育的主体和基础,抓好本科教学是提高整个高等教育质量的重点和关键。随着高等教育的普及和高等学校的扩招,在校大学本科计算机专业学生的人数将大量上升,对适合 21 世纪大学本科计算机科学与技术学科课程体系要求的,并且适合中国学生学习的计算机专业教材的需求量

也将急剧增加。为此,中国计算机学会和清华大学出版社共同规划了面向全国高等院校计算机专业本科生的“21 世纪大学本科计算机专业系列教材”。本系列教材借鉴美国 ACM 和 IEEE/CS 最新制定的 *Computing Curricula* 2001(简称 CC2001)课程体系,反映当代计算机科学与技术学科水平和计算机科学技术的新发展、新技术,并且结合中国计算机教育改革成果和中国国情。

中国计算机学会教育专业委员会和全国高等学校计算机教育研究会,在清华大学出版社的大力支持下,跟踪分析 CC2001,并结合中国计算机科学与技术学科的发展现状和计算机教育的改革成果,研究出了《中国计算机科学与技术学科教程 2002》(*China Computing Curricula* 2002,简称 CCC2002),该项研究成果对中国高等学校计算机科学与技术学科教育的改革和发展具有重要的参考价值和积极的推动作用。

“21 世纪大学本科计算机专业系列教材”正是借鉴美国 ACM 和 IEEE/CS CC2001 课程体系,依据 CCC2002 基本要求组织编写的计算机专业教材。相信通过这套教材的编写和出版,能够在内容和形式上显著地提高我国计算机专业教材的整体水平,继而提高我国大学本科计算机专业的教学质量,培养出符合时代发展要求的具有较强国际竞争力的高素质创新型计算机人才。



中国工程院院士

国防科学技术大学教授

21 世纪大学本科计算机专业系列教材编委会名誉主任

2002 年 7 月

前言

FOREWORD

我国信息技术与产业的发展,需要大量从事计算机应用的系统设计工程师、网络系统集成工程师、软件工程师、电信技术工程师,以及信息服务、信息系统管理、网络管理与维护的专业技术人员,他们都需要掌握计算机网络的知识与技术。

《计算机网络》教程是中国计算机学会组织编写的“21 世纪大学本科计算机专业系列教材”之一,与它配套的有《计算机网络教师用书》、《计算机网络习题指导书》、《计算机网络实验指导书》和《计算机网络电子教案》,它们构成了一个立体的教材体系。

在本书的写作中,我们希望能参考国内外类似的书籍,但是除了可以在个别的教学网站上看到个别类似的内容讨论之外,没有见到系统讨论网络课程教学的教师用书。我们深知,写一本教师用书,其实要比写一本教材的工作量与难度还要大。作者经过多年的教学实践,一直希望能够对教学的心得与体会做一个总结和提高,和国内的同行们有一个交流的机会。尽管在教师用书的写作上花的时间可能比较多,风险比较大,但是还是下决心动手做这件事。因为作为教师来说,没有比提高自身的教学水平与教学质量更重要的。尽管一个人的知识和阅历是有限的,但如果通过教学经验的总结,能够引起同行的讨论,进而促进课程教学质量的提高,那么即使书有很多不足之处,也会对课程的建设有益。

为了反映出与《计算机网络》教材的配套关系,本书的内容按两个部分来组织。第一部分为第 0 章,主要涉及教学方法、知识点设计与组织的讨论,不涉及具体课程内容。第二部分包括第 1~9 章,针对《计算机网络》具体的章节内容进行了讨论。除了讨论一些重点与难点问题之外,我们将根据个人的理解、认识与掌握的资料,对一些教材中没有展开写的、重要的背景资料进行讨论。本书在每一章中都提供了一些有用的网站地址或 RFC 文档,作为教师和学生使用时参考。当然,读者还可以通过 Internet 找到更好的网站和更多的内容。

我们认为,教师一辈子最主要的任务是尽自己最大的努力,把承担的每一门课程教好,不能误人子弟。作为一名好的教师,他在教授这门课程时最重要的是“知道学生在哪些知识的学习时,可能有哪些知识点不容易掌握,以及为什么不容易掌握”。教师最大的贡献是教出一批好学生。要达到这个目的,教师需要对自己所教的课程开展教学研究。

我们将本书作为教学研究成果之一奉献给同行,希望引起讨论,并从讨论中获取更多宝贵的教学经验,也希望同学参与到探讨网络课程教学方法之中,提出宝贵的意见与建议,共同提高我国计算机网络课程的教学水平。《计算机网络教师用书》只能起到一个“抛砖引玉”的作用。

本书的第0~7章由吴功宜编写,第8、9章由吴英编写。在本书的编写过程中得到刘瑞挺教授、徐敬东教授、张建忠副教授、韩毅刚副教授的帮助。网络实验室的陶智华博士、刘涛博士提出了不少建议和帮助,在此一并表示感谢。

作 者

2004年3月12日

于南开大学信息技术科学学院

吴功宜 wgy@nankai.edu.cn

吴英 wuy.netlab@eyou.com

目 录

CONTENTS

第 0 章 计算机网络课程知识点设计与组织的总体说明	1
0.1 计算机网络课程知识点设计	1
0.1.1 计算机网络课程教学的特点	1
0.1.2 计算机网络课程知识点组织的基本思路	2
0.2 计算机网络课程知识点设计与章节结构	3
0.2.1 计算机网络课程教学单元的划分	3
0.2.2 关于广域网与局域网、城域网的物理层、 数据链路层的内容安排	4
0.2.3 全书的知识点结构	5
0.2.4 《计算机网络》教材体系	6
0.2.5 《计算机网络教师用书》编写的指导思想	6
0.2.6 教学方法的讨论	8
第 1 章 计算机网络概论	12
1.0 学习目的、要求与知识点结构	12
1.0.1 学习目的与要求	12
1.0.2 知识点的组织结构	13
1.1 对计算机网络的形成与发展要点的理解	13
1.2 对计算机网络定义与分类的理解	14
1.2.1 计算机网络定义的基本要点	14
1.2.2 对计算机网络的分类方法的理解	16
1.3 对计算机网络的组成与结构要点的理解	17
1.3.1 资源子网和通信子网划分的意义与局限性	17
1.3.2 组网方式的变化与现代网络系统的结构特点	18
1.4 对计算机网络的拓扑构型要点的理解	18

1.4.1	网络拓扑构型的要点	18
1.4.2	对计算机网络拓扑的分类方法的理解	19
1.5	典型计算机网络	20
1.6	对网络计算研究与应用的发展的了解	22

第2章 网络体系结构与网络协议 24

2.0	学习目的、要求与知识点结构	24
2.0.1	学习目的与要求	24
2.0.2	知识点的组织结构	24
2.1	网络体系结构的基本概念	26
2.1.1	对网络通信协议的理解	26
2.1.2	对网络协议、协议族基本概念的理解	27
2.1.3	对协议、层次、接口与体系结构概念的理解	27
2.1.4	对面向连接服务与无连接服务的理解	28
2.1.5	对确认和重传机制的理解	29
2.2	对 OSI 参考模型发展过程及评价的理解	30
2.3	对 TCP/IP 参考模型发展过程及评价的理解	31
2.4	网络与 Internet 协议标准组织与管理机构	31
2.4.1	网络协议标准组织	31
2.4.2	RFC 文档	32
2.4.3	Internet 管理机构	33
2.4.4	Internet 管理和研究机构网址	34
2.5	对建议的参考模型的理解	35

第3章 物理层 36

3.0	学习目的、要求与知识点结构	36
3.0.1	学习目的与要求	36
3.0.2	知识点的组织结构	36
3.1	对物理层与物理层协议基本概念的理解	38
3.2	对数据通信基本概念的理解	39
3.2.1	对信息、数据和信号概念的理解	39
3.2.2	数据通信研究的主要问题	40
3.2.3	传输介质的主要类型	42
3.3	对数据编码技术要点的理解	49

3.3.1	数据编码类型	49
3.3.2	对多相调制方法的理解	49
3.3.3	脉冲编码调制方法	51
3.4	对基带信号的频谱特性的理解	52
3.4.1	观察与分析电信号的时域方法与频域方法	52
3.4.2	傅里叶分析的基本方法	53
3.4.3	周期性矩形脉冲信号的频谱分析	53
3.4.4	数字信号的频谱特点	55
3.4.5	对通信信道带宽影响基带传输的理解	56
3.4.6	对奈奎斯特准则与香农定律的理解	58
3.5	对广域网技术发展的理解	61
3.5.1	对广域网技术发展的理解	61
3.5.2	交换多兆位数据服务的要点	62
3.5.3	X.25 网技术要点	63
3.5.4	帧中继技术要点	63
3.5.5	B-ISDN 技术要点	64
3.5.6	异步传输模式 ATM 技术要点	66
3.6	对同步数字体系的理解	68
3.6.1	SDH 发展的背景	68
3.6.2	SDH 的发展过程	68
3.6.3	几种速率标准的制定	68
3.6.4	SDH 速率体系的技术要点	69
第 4 章	数据链路层	70
4.0	学习目的、要求与知识点结构	70
4.0.1	学习目的与要求	70
4.0.2	知识点的组织结构	70
4.1	对差错产生与差错控制方法的理解	71
4.1.1	为什么要设计数据链路层	71
4.1.2	对差错产生的原因和差错类型的理解	72
4.1.3	理解误码率定义的要点	73
4.1.4	对检错码与纠错码的理解	73
4.1.5	对循环冗余编码工作原理的理解	73
4.1.6	对差错控制机制要点的理解	74

4.2	对数据链路层的基本概念的理解	75
4.2.1	物理线路与数据链路	75
4.2.2	对数据链路控制原理的理解	76
4.2.3	数据链路层向网络层提供的服务	76
4.3	面向字符型数据链路层协议实例	78
4.3.1	数据链路层协议的分类	78
4.3.2	面向字符型协议实例——BSC	78
4.4	面向比特型数据链路层协议实例——HDLC	79
4.4.1	HDLC 的发展过程	79
4.4.2	对数据链路的配置方式和数据传送方式要点的理解	79
4.4.3	HDLC 的帧结构	80
4.5	Internet 中的数据链路层	81
4.5.1	Internet 数据链路层协议	81
4.5.2	对 SLIP 协议技术要点的理解	81
4.5.3	对 CSLIP 协议技术要点的理解	82
4.5.4	对 PPP 协议技术要点的理解	82
第 5 章	介质访问控制子层	84
5.0	学习目的、要求与知识点结构	84
5.0.1	学习目的与要求	84
5.0.2	知识点的组织结构	84
5.1	局域网与城域网的基本概念	85
5.1.1	局域网的主要技术特点	85
5.1.2	局域网拓扑、传输介质与介质访问控制方法的分类	86
5.1.3	对 IEEE 802 组织与 802.3 协议结构的理解	88
5.2	对 Ethernet 技术要点的理解	90
5.2.1	Ethernet 技术的产生与发展的过程	90
5.2.2	对 Ethernet 网核心技术理论研究发展的理解	93
5.2.3	对 Ethernet 物理地址的理解	97
5.3	对 CSMA/CD、Token Bus 与 Token Ring 三种基本介质 访问控制方法的理解	98
5.3.1	CSMA/CD、Token Bus 与 Token Ring 的共同之处	98
5.3.2	CSMA/CD、Token Bus 与 Token Ring 的不同之处	99
5.3.3	CSMA/CD、Token Bus 与 Token Ring 的性能分析与比较	99

5.4	高速局域网、交换式局域网与虚拟局域网	101
5.4.1	高速局域网的研究方法	101
5.4.2	对 Fast Ethernet 技术要点的理解	101
5.4.3	对 Gigabit Ethernet 技术要点的理解	102
5.4.4	对 10Gb/s Ethernet 技术要点的理解	102
5.4.5	对交换式局域网技术要点的理解	103
5.4.6	对虚拟局域网技术要点的理解	105
5.5	IEEE 802.3 物理层标准与组网方法	106
5.5.1	IEEE 802.3 物理层协议标准的结构	106
5.5.2	几种典型的物理层协议	106
5.5.3	局域网组网的基本方法	108
5.5.4	对局域网结构化布线基本概念的理解	110
5.6	无线局域网	112
5.6.1	无线局域网的应用	112
5.6.2	红外无线局域网的技术要点	112
5.6.3	扩频无线局域网的技术要点	114
5.6.4	窄带微波无线局域网的技术要点	115
5.6.5	无线局域网标准 IEEE 802.11	116
5.6.6	几种主要无线局域网技术的比较	119
5.7	对局域网互联概念与中继器、集线器、网桥、交换机的理解	120
5.7.1	中继器的基本工作原理与特点	120
5.7.2	集线器的基本工作原理与特点	122
5.7.3	局域网桥的基本工作原理与特点	123
5.7.4	局域网交换机的基本工作原理与特点	126
5.7.5	对第二层交换的基本概念的理解	128
第 6 章	网络层	129
6.0	学习目的、要求与知识点结构	129
6.0.1	学习目的与要求	129
6.0.2	知识点的组织结构	129
6.1	对网络层作用与 IP 协议要点的理解	131
6.1.1	网络互联的需求是推动网络层和 IP 协议研究的原动力	131
6.1.2	网络层协议必须独立于互联网络通信子网所采用的技术	131
6.1.3	IP 协议设计遵循的基本原则	132

6.1.4	网络层协议所要包括的基本内容	132
6.2	对 IP 地址概念的理解	132
6.2.1	IP 地址类型	132
6.2.2	确定一个 IP 地址的类	137
6.2.3	特殊地址形式	138
6.2.4	IP 地址的申请与管理	139
6.3	对子网与超网基本概念的理解	140
6.3.1	为什么要划分子网与超网	140
6.3.2	对子网掩码与子网地址空间划分办法的理解	140
6.3.3	子网规划与地址空间划分举例	141
6.3.4	可变长度子网掩码的技术要点	148
6.3.5	无类域间路由的技术要点	149
6.4	对 IP 分组交付和路由选择技术要点的理解	152
6.4.1	IP 分组交付	152
6.4.2	对路由选择算法的基本概念的理解	153
6.4.3	提高路由表查询效率的基本方法	155
6.5	Internet 的路由选择协议	155
6.5.1	自治系统与路由选择协议	155
6.5.2	对于内部网关协议要点的理解	156
6.5.3	对于开放最短路径优先协议要点的理解	157
6.5.4	对于外部网关协议要点的理解	159
6.6	对 IP 协议技术要点的理解	160
6.6.1	IP 协议的特点	160
6.6.2	IP 数据报的格式	161
6.6.3	对 IP 数据报的分片与组装技术要点的理解	165
6.6.4	对 IP 数据报选项技术要点的理解	166
6.7	对地址解析技术要点的理解	175
6.7.1	IP 地址与物理地址的映射	175
6.7.2	对地址解析协议技术要点的理解	176
6.7.3	反向地址解析协议	178
6.7.4	网络层基本工作原理小结	179
6.8	对路由器与第 3 层交换技术要点的理解	183
6.8.1	路由器的基本功能	183
6.8.2	对路由器的结构与工作原理的理解	184

6.8.3	路由器技术的演变与发展	185
6.8.4	对路由器与第三层交换机异同点与应用范围的理解	189
6.9	对 Internet 控制报文协议要点的理解	190
6.9.1	控制报文协议 ICMP 的作用与特点	190
6.9.2	ICMP 数据报格式与类型	191
6.9.3	对 ICMP 差错报告数据报技术要点的理解	192
6.9.4	对 ICMP 查询报文技术要点的理解	197
6.10	对 IP 多播与 Internet 组管理协议的理解	201
6.10.1	IP 多播的基本概念	201
6.10.2	Internet 组管理协议	202
6.10.3	多播路由器与 IP 多播中的隧道技术	203
6.11	对 IPv6、IP Sec 与 ICMPv6 协议要点的理解	204
6.11.1	对 IPv6 协议要点的理解	204
6.11.2	ICMPv6 与 IPv6 的网络层协议结构	209
6.11.3	从 IPv4 向 IPv6 的过渡方法	210
6.11.4	对 IP 安全协议技术要点的理解	211
第 7 章	传输层	213
7.0	学习目的、要求与知识点结构	213
7.0.1	学习目的与要求	213
7.0.2	知识点的组织结构	213
7.1	对网络环境中分布式进程通信概念的理解	214
7.1.1	单机系统中的进程通信方法	214
7.1.2	网络环境中分布式进程通信的特点	215
7.1.3	对进程间相互作用模式 client/server 的理解	217
7.1.4	进程通信中 client/server 模式实现方法	218
7.2	对传输层的基本功能的理解	223
7.2.1	传输层的端到端通信	223
7.2.2	传输层协议的基本功能	223
7.2.3	网络服务与服务质量	225
7.3	对用户报文协议 UDP 要点的理解	227
7.3.1	UDP 协议的主要 RFC 文档与特点	227
7.3.2	UDP 的基本工作过程	228
7.3.3	UDP 端口号	230

7.3.4	UDP 数据报格式	231
7.3.5	UDP 检验和的基本概念与计算示例	232
7.4	对传输控制协议 TCP 要点的理解	234
7.4.1	关于 TCP 协议的主要 RFC 文档与标准	234
7.4.2	TCP 协议的主要特点	236
7.4.3	TCP 的端口号分配和 socket 地址	237
7.4.4	TCP 报文段格式	238
7.4.5	对 TCP 流量控制技术要点的理解	241
7.4.6	对 TCP 差错控制技术要点的理解	244
7.4.7	TCP 传输连接建立、维护与释放	247
7.4.8	对 TCP 状态转换图的理解	249
第 8 章	应用层	253
8.0	学习目的、要求与知识点结构	253
8.0.1	学习目的与要求	253
8.0.2	知识点的组织结构	253
8.1	对应用层作用与应用层协议的理解	254
8.2	对域名系统技术要点的理解	255
8.2.1	学习域名系统的目的	255
8.2.2	关于域名系统的主要 RFC 文档、标准草案与 Internet 标准	255
8.2.3	域名解析与地址解析的区别	255
8.2.4	域名系统研究的背景与设计目标	256
8.2.5	域名系统的解决方案	258
8.2.6	域名数据库	259
8.2.7	域名系统技术发展与安全问题的	262
8.3	对电子邮件系统技术要点的理解	264
8.3.1	关于电子邮件协议的主要 RFC 文档、 标准草案与 Internet 标准	264
8.3.2	Internet 电子邮件系统设计的基本思路	264
8.3.3	对电子邮件体系结构与基本工作原理的理解	265
8.3.4	邮件报文交付的三个阶段	268
8.3.5	SMTP 协议要点	269
8.3.6	通用协议 Internet 邮件扩展 MIME 协议要点	273
8.3.7	POP3 与 IMAP4 协议	274

8.4	对 FTP 技术要点的理解	276
8.4.1	关于 FTP 协议的主要 RFC 文档、标准草案与 Internet 标准	276
8.4.2	FTP 协议的主要特点	276
8.4.3	RFC 959 定义的 FTP 主要命令	276
8.4.4	简易文件传输协议 TFTP 要点	277
8.5	对 WWW 技术要点的理解	278
8.5.1	关于 WWW 服务的主要 RFC 文档、 标准草案与 Internet 标准	278
8.5.2	对 WWW 服务方法的理解	279
8.5.3	超文本传输协议 HTTP 的要点	279
8.5.4	对 WWW 客户、服务器连接与协商方法的理解	288
8.5.5	超文本标记语言 HTML 的要点	290
第 9 章	网络安全与网络管理	294
9.0	学习目的、要求与知识点结构	294
9.0.1	学习目的与要求	294
9.0.2	知识点的组织结构	294
9.1	对网络安全的重要性与研究的主要问题的理解	295
9.1.1	网络安全的重要性	295
9.1.2	网络安全技术研究的主要问题	296
9.1.3	网络安全服务与安全标准	298
9.1.4	网络安全策略的设计	301
9.1.5	网络安全策略制定的方法与基本内容	303
9.1.6	网络安全问题的鉴别与受到威胁时的行动方案	307
9.2	对加密与认证技术要点的理解	311
9.2.1	密码算法与密码体制的基本概念	312
9.2.2	对称密钥密码体系的技术要点	312
9.2.3	对称密钥密码体系实现方法举例	313
9.2.4	非对称密钥密码体系技术要点	316
9.2.5	公钥加密实现方法的举例	317
9.2.6	对密钥的管理与 CA 认证中心概念的理解	319
9.2.7	对数字信封技术要点的理解	320
9.2.8	对数字签名技术要点的理解	321
9.2.9	了解身份认证技术的发展	323