重点大学计算机专业系列教材

网络协议与网络安全

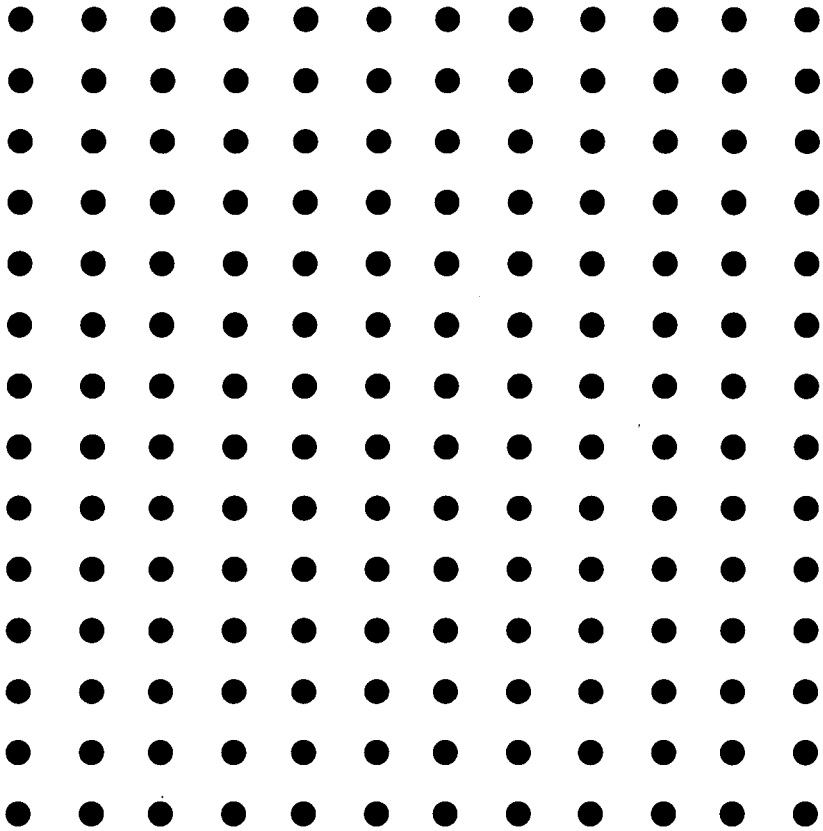
凌 力 编著

清华大学出版社

重点大学计算机专业系列教材

网络协议与网络安全

凌 力 编著



清华大学出版社
北京

内 容 简 介

本书由相互关联的三部分内容组成：第一部分主要从共享网络入手，探讨协议的本质、作用和方法，由此过渡到互联网协议、宽带网络和无线网络等基础技术；第二部分则以安全性设计为目标，着重阐述密码学原理、网络安全威胁与安全防范对策；第三部分内容着眼于互联网领域，部析各类应用系统的技术内涵和实现框架，并总结了网络与安全技术的发展趋势。

本书没有遵循“按部就班”的常规模式，而是把大量的“经典”或“创新”技术进行了融合，编排成不同的“知识板块”，便于比较和把握各种技术的关联性、继承性、差异性和独特性。

本书既适合作为高等院校计算专业的教材，也可供自学及工程技术人员参考。

图书在版编目(CIP)数据

网络协议与网络安全/凌力编著. —北京：清华大学出版社，2007.11
(重点大学计算机专业教材系列)
ISBN 978-7-302-15756-4

Ⅰ. 网… Ⅱ. 凌… Ⅲ. ①计算机网络－通信协议－高等学校－教材 ②计算机网络－安全技术－高等学校－教材 Ⅳ. TN915.04 TP393.08

中国版本图书馆 CIP 数据核字(2007)第 112889 号

责任编辑：丁　岭　徐跃进
责任校对：梁　毅
责任印制：李红英
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
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京国马印刷厂
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：17.75　**字　数**：405 千字
版　　次：2007 年 11 月第 1 版　　**印　次**：2007 年 11 月第1 次印刷
印　　数：1～3000
定　　价：28.00 元

INTRODUCTION

出版说明

随着国家信息化步伐的加快和高等教育规模的扩大，社会对计算机专业人才的需求不仅体现在数量的增加上，而且体现在质量要求的提高上，培养具有研究和实践能力的高层次的计算机专业人才已成为许多重点大学计算机专业教育的主要目标。目前，我国共有16个国家重点学科、20个博士点一级学科、28个博士点二级学科集中在教育部部属重点大学，这些高校在计算机教学和科研方面具有一定优势，并且大多以国际著名大学计算机教育为参照系，具有系统完善的教学课程体系、教学实验体系、教学质量保证体系和人才培养评估体系等综合体系，形成了培养一流人才的教学和科研环境。

重点大学计算机学科的教学与科研氛围是培养一流计算机人才的基础，其中专业教材的使用和建设则是这种氛围的重要组成部分，一批具有学科方向特色优势的计算机专业教材作为各重点大学的重点建设项目成果得到肯定。为了展示和发扬各重点大学在计算机专业教育上的优势，特别是专业教材建设上的优势，同时配合各重点大学的计算机学科建设和专业课程教学需要，在教育部相关教学指导委员会专家的建议和各重点大学的大力支持下，清华大学出版社规划并出版本系列教材。本系列教材的建设旨在“汇聚学科精英、引领学科建设、培育专业英才”，同时以教材示范各重点大学的优秀教学理念、教学方法、教学手段和教学内容等。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

1. 面向学科发展的前沿，适应当前社会对计算机专业高级人才的培养需求。教材内容以基本理论为基础，反映基本理论和原理的综合应用，重视实践和应用环节。

2. 反映教学需要，促进教学发展。教材要能适应多样化的教学需要，正确把握教学内容和课程体系的改革方向。在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养，为学生知识、能力、素质协调发展创造条件。

3. 实施精品战略，突出重点，保证质量。规划教材建设的重点依然是专业基础课和专业主干课；特别注意选择并安排了一部分原来基础比较好的优秀教材或讲义修订再版，逐步形成精品教材；提倡并鼓励编写体现重点大学计算机专业教学内容和课程体系改革成果的教材。

4. 主张一纲多本，合理配套。专业基础课和专业主干课教材要配套，同一门课程可以有多本具有不同内容特点的教材。处理好教材统一性与多样化的关系；基本教材与辅助教材以及教学参考书的关系；文字教材与软件教材的关系，实现教材系列资源配套。

5. 依靠专家，择优落实。在制订教材规划时要依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时，要引入竞争机制，通过申报、评审确定主编。书稿完成后要认真实行审稿程序，确保出书质量。

繁荣教材出版事业，提高教材质量的关键是教师。建立一支高水平的以老带新的教材编写队伍才能保证教材的编写质量，希望有志于教材建设的教师能够加入到我们的编写队伍中来。

教材编委会

FOREWORD

前言

■ 关于观点

我们不要惧怕亮出自己的观点来——即使有失偏颇也可供大家评判、批评、争论、思考、品味。客观的数据是必要的、枯燥的理论是难免的，但最终还是要有观点和结论，这关系到立场问题。

在本书中可以找到许多观点，谦虚地说，它们不一定都是正确的！影响正确性判断的原因有三：一是认识有偏颇；二是事物在发展，丑小鸭长啊长，说不定是只白天鹅呢！三是有更多更好的事物在孕育中、诞生中。这正是计算机网络领域的特点：朝气蓬勃，欣欣向荣，这也是研究计算机网络的乐趣所在：推陈出新，创意无限，不过这也是置身计算机网络行业的辛苦所在：三日不见，形同陌路！

理解是观点的起步，观点是理解的体现。理解了，有观点了，往往就成功了一半。

■ 关于情感

为什么大数学家说在天书般的方程式堆中漫游是妙不可言、富有乐趣的？那就是情感。固然他们到达了某种常人无法企及的境界，但不可否认，任何事物都是可以有情感的，不管这种情感是其自身所具备的，还是感怀的人所赋予的。

所以我们可以大胆地说，技术文献是有情感的，论文讲义是有情感的，计算机网络也是有情感的。

计算机网络本来就是很拟人化的东西，人类还逐渐地在互联网上构筑起一个虚拟世界。这是一个多么富有想象力的全人类共同参与的大工程！所以，本书读者们在阅读到那些看上去和计算机网络术语、技术无关的文字时，请不要忽略，相信我，它们是属于计算机网络领域的。

■ 关于角度

但凡足球运动员用大家认为不可思议的角度射入一个球时，都会得到

暴风雨般的喝彩，因为这个球与众不同，因为把自己从昏昏欲睡的比赛过程中弄醒了。没有统计过，不知道有多少人在阅读技术文章时处于半清醒状态，我想应该不在少数，因为不客气地说，大部分的教科书都很教科书，有千篇一律的公式和行文，有从基础到深入的严密逻辑。

然而我不认为这有什么可取的，或者说不认为一定非得这样。花开两朵还各有不同呢！本书抓的一个个的点并不全落在“网”的“纲”上，但希望抓起这些点能有一些“目”能够张开，由点及面，窥一斑知全豹，也是一个了解“全网”的不容易睡着的方法。

本书的每一个章节都试图去了解一个或大或小的问题，并扩展到周围的问题。我们比较多地采用“比较性分析”的办法，通过对比来加深概念和技术方法的理解。不过是否能达到预期效果——还得靠读者自己琢磨！

■ 关于细节

有人说“细节决定成败”，那大概是在说装配钟表吧。回想童年，你还记得多少细节？——无非是和谁闹别扭了，后来又要好了等等，至于为什么事情吵架多半已经不记得了。不要慌张，不是健忘，那是人脑的优秀性能之一：忘记不必要的东西。那样你才没有崩溃。

计算机网络中也有很多细节，它们是由许许多多数字、字母构成的，足够把人弄疯。所以，我们最好要学会什么时候要关注细节（当少尉排长），什么时候要看重全局（当五星将军）。

普天下阐述技术细节的书已经够多了，所以本书不打算凑这个热闹。而当我们把一些所谓的细节屏蔽掉之后，我们往往会发现技术的核心思想显露出来了。至于细节，很简单，我们可以检索有关资料来获取。

■ 关于本教材

- 本教材可作为本科生、研究生课程教学用书或参考书。
- 虽然涉及“网络协议”，但并非以单纯的网络协议原理为首要内容，而是从较为宏观的网络与通信技术的角度来体现较为微观的协议技术，旨在从网络理解协议、从协议透视网络。
- 每章为一个大的知识点，阐述一个网络及其安全技术的“板块”；每个板块由若干小的知识点构成。各板块间的内容略有交叉重叠，反映出网络通信领域各项关键技术的关联性，因此，既要对各个“分支”进行深入钻研，又要有全局的、整体的观念。
- 每章学习约需一两个“单元时间”（每单元时间为两三课时）。
- 由于涉及的概念、术语较多，这个“基础”打得不会很轻松，但会从知识面拓展上有所获益。
- 希望在学习过程中不要仅仅局限于书本内容，而应该主动去学习更多的相关知识，对感兴趣的问题予以纵深挖掘。这里包含两层意思：第一，鼓励借助计算机、互联网进行学习，而不要停留在书本涵盖的有限知识上；第二，把对理论的理性认识应用于实践中，获得感性认识，达到融会贯通的目的。

- 勤于思考，不迷信“权威”。对“可疑”观点应勇敢地提出质疑和自己的见解。同时也要善于发现问题、提出问题，并提高分析问题、解决问题的能力。
- 因为网络技术的发展速度很快，本教材也将不断更新，力争与本领域的新进展同步。

作　者

2007 年 6 月于复旦大学

CONTENTS

目录

第 1 章　网络技术概要 …… 1

1.1　按拓扑结构分类 …… 1
1.2　按覆盖范围分类 …… 4
1.3　按通信方式分类 …… 5
1.4　计算机网络协议 …… 6
1.5　计算机网络的数字化本质 …… 8
1.6　思考与讨论 …… 9

第 2 章　共享网络协议原理 …… 10

2.1　方案一：时钟同步方案 …… 11
2.2　方案二：异步轮流方案 …… 12
2.3　方案三：主从轮询方案 …… 12
2.4　方案四：令牌传递方案 …… 14
2.5　方案五：自由竞争方案 …… 15
2.6　方案六：带外信令方案 …… 16
2.7　协议机设计和实现方法 …… 18
2.8　思考与讨论 …… 20

第 3 章　以太网技术变迁 …… 21

3.1　以太网与 Internet 的关系 …… 21
3.2　以不变应万变，万变不离其宗 …… 22
3.3　变化中的以太网 …… 24
3.3.1　第一阶段：同轴电缆 …… 24
3.3.2　第二阶段：集线器 …… 25
3.3.3　第三阶段：二层交换机 …… 26
3.3.4　第四阶段：三层交换机 …… 27

3.4 以太网技术部分术语和相关知识 …… 28
3.5 思考与讨论 …… 29

第 4 章 Internet 技术 …… 30

4.1 Internet 概述 …… 30
4.2 TCP/IP 协议 …… 31
4.2.1 IP 协议概要 …… 31
4.2.2 TCP/UDP 协议概要 …… 34
4.2.3 路由协议概要 …… 39
4.2.4 TCP/IP 协议簇其他协议 …… 42
4.3 VLAN …… 44
4.3.1 VLAN 原理 …… 44
4.3.2 VLAN 类型 …… 45
4.4 DNS 与 URL …… 45
4.4.1 DNS …… 46
4.4.2 URL …… 46
4.5 Internet 典型应用 …… 47
4.5.1 E-mail …… 47
4.5.2 FTP …… 50
4.5.3 Telnet …… 51
4.5.4 Web …… 52
4.6 intranet 与 extranet …… 53
4.6.1 intranet …… 53
4.6.2 extranet …… 54
4.7 思考与讨论 …… 55

第 5 章 宽带网络与接入技术 …… 56

5.1 网络设备类型 …… 56
5.1.1 终端设备 …… 56
5.1.2 中继设备 …… 57
5.1.3 通信设备 …… 58
5.2 宽带网络 …… 59
5.2.1 宽带网络层次结构 …… 59
5.2.2 宽带网络技术分布 …… 60
5.3 宽带网络接入 …… 66
5.3.1 接入服务 …… 66
5.3.2 最后一公里 …… 68
5.3.3 最后一百米 …… 70

5.3.4 宽带接入的未来 …… 71
5.4 思考与讨论 …… 73

第6章 无线网络接入技术 …… 74

6.1 无线网络接入技术概要 …… 74
6.1.1 无线接入网系统结构 …… 74
6.1.2 无线接入与有线接入的比较 …… 74
6.1.3 无线接入网技术的作用和影响 …… 75
6.2 无线接入网典型技术 …… 76
6.2.1 无线局域网 …… 76
6.2.2 蓝牙 …… 77
6.2.3 本地多点分配业务 …… 78
6.2.4 微波多点分配系统 …… 79
6.2.5 无线异步传输模式 …… 79
6.2.6 蜂窝式数字分组数据 …… 80
6.2.7 第二代移动通信系统 …… 80
6.2.8 第三代移动通信系统 …… 81
6.2.9 无线本地环路 …… 82
6.2.10 无绳电话系统 …… 82
6.2.11 卫星接入系统 …… 82
6.2.12 家庭无线频率 …… 83
6.2.13 红外线传输 …… 83
6.2.14 无线应用协议 …… 84
6.3 无线接入网技术比较 …… 84
6.4 无线接入网技术应用和发展 …… 85
6.5 思考与讨论 …… 87

第7章 多媒体通信 …… 88

7.1 多媒体信息编码技术 …… 88
7.1.1 文字编码 …… 89
7.1.2 格式化文本编码 …… 90
7.1.3 音频编码 …… 90
7.1.4 静态图像编码 …… 91
7.1.5 动态视频编码 …… 92
7.2 流媒体传输技术 …… 94
7.2.1 流媒体系统特性 …… 94
7.2.2 典型的流媒体播放系统 …… 95
7.3 多媒体应用系统 …… 96

7.3.1 多媒体应用系统体系结构 …… 96
7.3.2 典型的多媒体应用系统 …… 97
7.4 思考与讨论 …… 102

第 8 章 个人即时通信 …… 103

8.1 个人即时通信概述 …… 103
8.2 个人即时通信系统体系结构 …… 104
8.3 个人即时通信地址编码 …… 105
8.4 典型的个人即时通信系统 …… 107
8.4.1 IM …… 107
8.4.2 VoIP …… 109
8.4.3 NGN …… 111
8.4.4 视频电话 …… 114
8.4.5 网络会议 …… 115
8.5 思考与讨论 …… 116

第 9 章 网络测试、管理与诊断 …… 117

9.1 网络基本测试方法 …… 117
9.1.1 协议测试原理 …… 117
9.1.2 协议测试分类 …… 118
9.1.3 协议测试方法 …… 119
9.1.4 协议一致性测试 …… 120
9.2 网络管理与系统管理 …… 121
9.2.1 网络管理基本原理 …… 122
9.2.2 网络管理功能域 …… 123
9.2.3 网络管理系统结构 …… 124
9.2.4 网络管理协议 …… 125
9.3 网络故障诊断 …… 127
9.4 思考与讨论 …… 128

第 10 章 密码学基础 …… 130

10.1 信息加密原理 …… 130
10.2 古典加密技术 …… 132
10.2.1 Caesar 密码 …… 132
10.2.2 标准字头密码 …… 132
10.2.3 Playfair 密码 …… 133
10.2.4 Vigenere 密码 …… 134
10.2.5 Vernam 密码 …… 134

10.2.6 Hill 密码 …… 135
10.2.7 其他古典加密方法 …… 136
10.3 对称密钥加密 …… 138
10.3.1 DES …… 139
10.3.2 IDEA …… 142
10.3.3 AES …… 143
10.4 非对称密钥加密 …… 144
10.4.1 公开密钥体制 …… 144
10.4.2 背包加密 …… 145
10.4.3 RSA …… 145
10.4.4 ElGamal …… 147
10.4.5 ECC …… 148
10.5 数字签名 …… 149
10.5.1 单向函数概述 …… 149
10.5.2 MD5 …… 150
10.5.3 数字签名原理 …… 153
10.5.4 数字证书 …… 156
10.6 密钥管理 …… 158
10.6.1 Diffie-Hellman 算法 …… 158
10.6.2 Kerberos …… 158
10.6.3 PKI …… 159
10.6.4 CA …… 161
10.7 思考与讨论 …… 164

第 11 章 网络安全威胁 …… 166

11.1 网络安全认识 …… 166
11.2 网络攻击原理 …… 167
11.3 网络安全攻击基本手段 …… 169
11.3.1 口令破解 …… 169
11.3.2 通信监听 …… 172
11.3.3 漏洞扫描 …… 173
11.3.4 拒绝服务 …… 174
11.3.5 溢出攻击 …… 179
11.3.6 特洛伊木马 …… 183
11.3.7 病毒与蠕虫 …… 186
11.3.8 网络欺诈 …… 189
11.3.9 垃圾信息 …… 190
11.4 思考与讨论 …… 192

第 12 章　网络安全防范 …… 193

12.1　网络安全防范技术基本原理 …… 193
12.2　嵌入式安全防范 …… 194
12.2.1　VPN …… 194
12.2.2　NAT …… 197
12.2.3　FireWall …… 199
12.2.4　Proxy …… 203
12.3　主动式安全防范 …… 204
12.3.1　Password …… 204
12.3.2　SubNetwork …… 208
12.3.3　SimAttack …… 208
12.3.4　SoftwarePack …… 209
12.4　被动式安全防范 …… 210
12.4.1　log …… 210
12.4.2　IDS …… 211
12.4.3　SAS …… 213
12.5　网络安全防范体系 …… 213
12.6　思考与讨论 …… 217

第 13 章　冗余技术 …… 218

13.1　冗余技术概要 …… 218
13.2　路径冗余 …… 219
13.2.1　线路冗余 …… 219
13.2.2　路由冗余 …… 221
13.3　协议冗余 …… 223
13.4　设备冗余 …… 223
13.5　数据冗余 …… 224
13.6　思考与讨论 …… 225

第 14 章　Internet 应用 …… 226

14.1　网络应用系统架构 …… 226
14.1.1　应用系统架构的演变 …… 226
14.1.2　C/S 与 B/S …… 226
14.1.3　中间件技术 …… 228
14.2　用户认证 …… 229
14.2.1　用户登录及其认证 …… 229
14.2.2　统一认证与单点登录 …… 229

14.2.3 用户身份标识 …… 230
14.3 搜索引擎 …… 231
14.4 Internet 应用系统分类 …… 233
14.4.1 X2Y …… 233
14.4.2 E-Applications …… 234
14.5 思考与讨论 …… 235

第 15 章 网络与安全技术大趋势 …… 236

15.1 IPv6 …… 236
15.1.1 IPv6 技术概要 …… 236
15.1.2 IPv6-IPv4 互联 …… 238
15.2 Web 2.0 …… 240
15.3 GGG …… 243
15.4 Private Personalized Portal …… 244
15.5 WSN …… 245
15.6 Pervasive Computing …… 246
15.7 Cyberspace …… 247
15.8 Internet 现象 …… 248
15.9 思考与讨论 …… 249

附录 A 计算机病毒简史 …… 250

附录 B 根域名服务器及其面临的安全威胁 …… 252

术语索引 …… 254

参考文献 …… 263

CHAPTER 1

第1章 网络技术概要

计算机网络(computer network),这是一个广义的概念,如今却很容易被等同于Internet(互联网、国际互联网、因特网),当然也有另一个极端,把电话网络也称为是计算机网络。那么:究竟什么是计算机网络?

也许本章结束后就可以对计算机网络的本质基本理解了,也许本书结束后还懵懵懂懂的。不用太在意,形式化的定义不是关键。重要的是人们已经惊觉并惊呼计算机网络就在我们身边、在每一个角落;重要的是人们不再认为计算机网络是神秘的、难以琢磨和把握的;重要的是人们正在有意、无意地使用计算机网络——在生活、学习和工作中。

和传统行业相比,计算机网络简直就是一个婴儿。虽然她在摇头晃脑、咿呀作声中显露出聪明、出息的意思,但离成熟还差得很远。今天我们能举樽赏月,品葡萄美酒,那是酿酒业千百年积淀的窖香飘溢的结果,与此相比,计算机网络还是在"家乡土制烧酒"的时代。

但千万不能因此小看了计算机网络的发展速度,我们完全可以用日新月异来形容。著名的"摩尔定律"认为:用于构造计算机的半导体集成电路的单位面积晶体管数量,以每十八个月翻一番的速度增长。事实已经验证了这一论断。Internet发展初期,IP地址的分配出手阔绰,奢侈到一个大学拿一个A类地址群,直到有一天突然发现IP地址资源竟然已经捉襟见肘了。我们还经常听到有IT领域人士感慨,光是那些层出不穷的新概念、新名词就够受的,要想跟上网络发展的节奏都很费劲啊(言下之意,要创新谈何容易啊)!——这些都是计算机和计算机网络飞速发展的印记。

既然如此,有必要用一种新的视角来剖析计算机网络,用发展的眼光来跟随计算机网络的步伐。先从简单的分类做起,再深入挖掘一下计算机网络的内涵和本质。

1.1 按拓扑结构分类

计算机网络就是把计算机设备通过传输媒介相互连接而构成的系统。这可以看作是计算机网络的形式化定义。其中包含三个要素:

(1) 计算机设备。包括个人计算机(personal computer,PC)、工作站(workstation)、服务

器(server)、主机(host)、网络终端(network terminal)、联网设备(networking equipment)。

(2) 传输媒介。包括各种有形、无形的传输信道,有光、电、电磁波等。

(3) 连接方式及其相互关系。这是隐含的要素,即系统的拓扑结构。

思考:终端(terminal,这里特指"主机的终端"、"傻终端")是否属于计算机网络范畴?

思考:生活中有哪些设备可以称为网络终端?

网络的拓扑结构不仅仅是连接方式上的区别。不同的网络拓扑结构对计算机网络的影响很大,关系到网络的性能、可靠性、安全性等;反之亦然,不同的通信技术、应用需求也会"形成"相应的网络拓扑结构。所以,网络拓扑结构的设计是规划计算机网络系统的重要工作之一。

如图 1.1 所示,网络的拓扑结构有线状(总线状、串联状)、环状、星状、树状和网状等形式。值得注意的是,网状的拓扑结构不一定是"全连通"的,而且其他拓扑结构可以从网状结构"蜕变"而成。

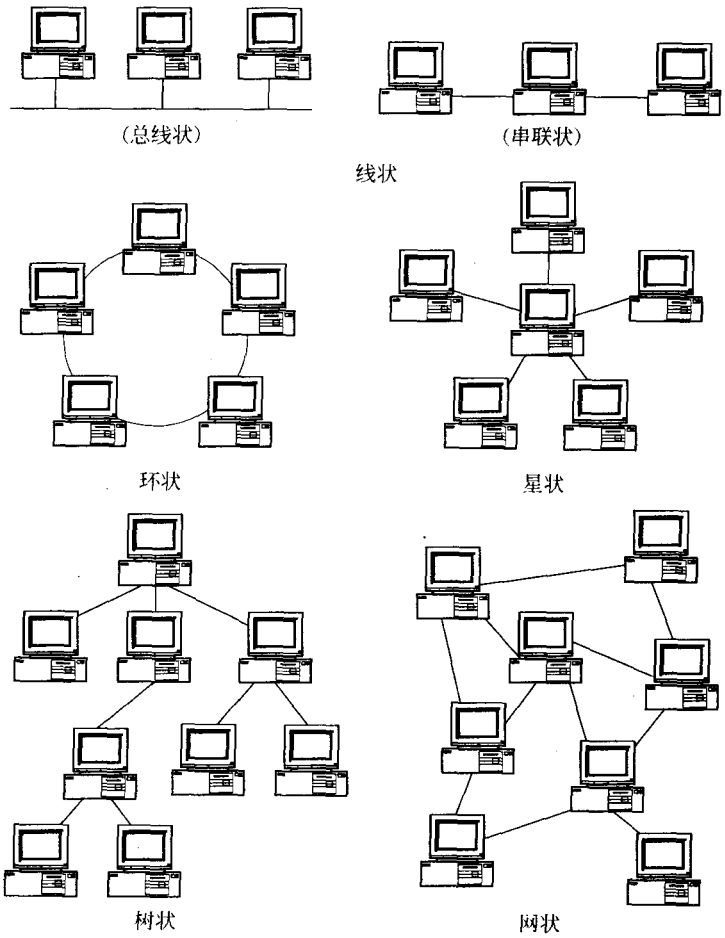


图 1.1 网络拓扑结构分类图示