

164

TN 915.04-43
L98

TCP/IP 权威教程

(第七版)

Adolfo Rodriguez

等著

John Gatrell

杨铁男 李增民 译



A1004264

清华大学出版社

(京) 新登字 158 号

北京市版权局著作权合同登记号: 01-2002-3186

内 容 简 介

TCP/IP 协议簇已经成为当今网络通信的标准之一。我们不仅在娱乐和信息方面用到了 TCP/IP 协议和 Internet, 而且通过执行事务、买卖产品和向顾客传送服务来实施商务工作。我们还在继续扩展使用 TCP/IP 的应用集, 从而引导读者深入学习基础性支持技术。

本书分为三部分, 深入讨论了 TCP/IP 协议簇。第一部分介绍 TCP/IP, 让读者对协议的重要基础性概念有基本的了解。第二部分继续讨论当今最流行的一些 TCP/IP 应用协议, 包括刚刚浮出水面的无线协议和多媒体应用协议。第三部分讲述了一些高级的概念和网络的最新发展趋势, 包括: IPv6、安全性、服务质量、IP 移动性和 MPLS。还提出了 TCP/IP 当前面临的挑战, 以及有望取代 TCP/IP 的技术。

本书适合于 TCP/IP 的初学者, 对希望全面了解 TCP/IP 的网络开发人员也有很好的参考价值。

Simplified Chinese edition copyright © 2002 by Pearson Education NORTH ASIA LIMITED and Tsinghua University Press.

TCP/IP Tutorial and Technical Overview: Adolfo Rodriguez John Gatrell, Copyright © 2002.

All Rights Reserved.

Published by arrangement with Pearson Education, Inc., publishing as PH PTR.

This edition is authorized for sale only in the People's Republic of China (excluding the Special Administrative Region of Hong Kong and Macau).

本书中文简体字版由清华大学出版社和美国 Pearson Education 出版集团合作出版。未经出版者书面许可, 不得以任何方式复制或抄袭本书内容。

版权所有, 翻印必究。

本书封面贴有 Pearson Education 出版集团激光防伪标签, 无标签者不得销售。

图书在版编目(CIP)数据

TCP/IP 权威教程(第七版)/(美)阿道夫·罗德格斯等著; 杨铁男, 李增民译.—北京: 清华大学出版社, 2002

书名原文: TCP/IP Tutorial and Technical Overview

ISBN 7-302-05594-7

I. T... II. ①罗...②杨...③李... III. 计算机网络—通信协议 IV. TN915.04

中国版本图书馆 CIP 数据核字(2002)第 041124 号

出 版 者: 清华大学出版社(北京清华大学学研大厦, 邮编 100084)

<http://www.tup.tsinghua.edu.cn>

责任编辑: 夏兆彦

封面设计: 康博

版式设计: 康博

印 刷 者: 北京密云胶印厂

发 行 者: 新华书店总店北京发行所

开 本: 787×1092 1/16 印张: 40 字数: 1023 千字

版 次: 2002 年 7 月第 1 版 2002 年 7 月第 1 次印刷

书 号: ISBN 7-302-05594-7/TP·3303

印 数: 0001~4000

定 价: 75.00 元

前 言

在当今的互联网络世界中，TCP/IP 协议簇已经成为计算机通信的事实标准。特定网络标准的普遍实施，使人们难以置信地依赖于它所支持的应用程序。现在，我们不仅把 TCP/IP 协议和 Internet 用于娱乐和信息，而且还用它们来指导我们的商业行为，诸如执行交易、购买和销售产品以及为顾客提供服务等。我们持续不断地拓展利用 TCP/IP 的应用系列，从而促进了对更多的基础结构支持的需求。

在本书中，我们深入地讨论了 TCP/IP 协议簇。在第一部分中，我们介绍了 TCP/IP 协议，基本上介绍了核心协议中出现的基本概念。在第二部分中，我们讨论了当今最流行的 TCP/IP 应用协议，包括新兴的无线应用和多媒体应用。在第三部分中，我们讨论了网络中的高级概念和网络基础结构的最新发展趋势，包括 IPv6、安全性、服务质量、IP 移动和 MPLS。我们还介绍了当前 TCP/IP 面临的挑战以及正在研究中的用来克服它们的技术。

本红皮书的编写团队

本红皮书由在国际技术支持组织 Raleigh 中心（International Technical Support Organization Raleigh Center）工作的来自世界各地的专家组共同编写。

Adolfo Rodriguez 是国际技术支持组织 Raleigh 中心的 I/T 顾问专家。他编写了大量关于 TCP/IP 的著作，并在世界各地讲授 IBM 关于 TCP/IP 的各个领域的课程。在加入 ITSO 之前，Adolfo 参与了 RTP、NC 中 IBM Communications Server for OS/390 的设计和开发。他在美国北卡罗来纳州的达勒姆城市的杜克大学获得了数学 B.A. 学位和计算机科学的 B.S. 和 M.S. 学位。现在他正在杜克大学攻读计算机科学博士学位，专业方向为网络系统。

John Gatrell 效力于 IBM 的英国分公司。他在通信顾客支持方面已有 15 年的经历，还有 7 年的编程史。他在牛津大学获得了物理学的 B.A. Honours 学位。他的专业领域包括 UNIX 和通信。

John Karas 是位于美国的 IBM 全球服务（IBM Global Service）公司的网络设计师。他已经在数据网络领域工作了 14 年。他取得了佩斯大学的通信方面的理学学士学位。他的专业领域包括 IP 路由算法、复杂网络设计、容量规划以及应用性能测试。他写了大量关于支持 OSPF 和 BGP 网络方面的文章，也写了大量关于 SAP 环境中性能监视方面的文章。

Roland Peschke 是一个高级 IT 网络专家，从事 IBM 的 OS/390 TCP/IP 和 SNA 环境的顾客请求咨询和教育服务。他在这些领域的丰富经验源于在 IBM 德国公司和 ITSO Raleigh 的 30 多年的工作经历。他完成了几本 SNA 红皮书和 TCP/IP 红皮书的编写工作。

感谢下列人员在本书编写过程中给予的大力支持：

国际技术支持组织，Raleigh 中心

Gail Christensen、Margaret Ticknor、Jeanne Tucker、David Watts、Juan Rodriguez、Byron Braswell、Thomas Barlen、Linda Robinson

国际技术支持组织，Austin 中心



Wade Wallace 和 Matthew Parente

IBM Communication Server for OS/390 Development

Jeff Hagggar、Bebe Isrel、Dinakaran Joseph

Cisco Systems 公司

Rick Williams 和 Edward Mazurek

BOPS 公司

Richardo Rodriguez

美国北卡罗来纳州大学

Karina Rodriguez

第一版作者

Peter Frick、Gerard Bourbigot、Frank Vandewiele

第二版作者

Peter Frick、Lesia Cox、Ricardo Haragutchi

第三版作者

Philippe Beaupied 和 Frederic Debulois

第四版作者

Philippe Beaupied 和 Francis Li

第五版作者

Eamon Murphy、Matthias Enders、Steve Hayes

第六版作者

Martin Murhammer、Ocun Atakan、Stefan Bretz、Larry Pugh、Kazunari Suzuki、David Wood

欢迎大家对本书提出宝贵意见

您的意见对我们非常重要！

我们希望使该红皮书尽善尽美。请通过如下方式反馈关于本红皮书和其他红皮书的宝贵意见：

- 通过“IBM 红皮书评论（IBM Redbooks review）”表单上给出的传真号传真该评估表单。
- 使用 ibm.com/redbooks 上的联机评估表单。
- 把您的意见通过 Internet 短信发送到 redbook@us.ibm.com。

目 录

第 I 部分 TCP/IP 核心协议

第 1 章 TCP/IP 体系结构、历史现状、标准和发展趋势	1
1.1 TCP/IP 体系结构模型	1
1.1.1 网络互联	1
1.1.2 TCP/IP 协议层	3
1.1.3 TCP/IP 应用	4
1.1.4 网桥、路由器和网关	6
1.2 Internet 起源	7
1.2.1 ARPANET	8
1.2.2 NSFNET	8
1.2.3 Internet 在商业上的应用	10
1.2.4 Internet2	11
1.2.5 开放式系统互联(OSI)参考模型	12
1.3 TCP/IP 标准	13
1.3.1 请求注解(RFC)	14
1.3.2 Internet 标准	15
1.4 Internet 的未来	16
1.4.1 多媒体应用	16
1.4.2 在商业上的运用	17
1.4.3 无线 Internet	17
第 2 章 网络接口	18
2.1 以太网和 IEEE 802.x 局域网	18
2.2 光纤分布式数据接口(FDDI)	20
2.3 串行线路接口协议(SLIP)	21
2.4 点到点协议(PPP)	22
2.5 综合业务数字网(ISDN)	23
2.6 X.25	24
2.7 帧中继	26
2.7.1 帧格式	26
2.7.2 互联问题	27
2.7.3 数据链路层参数协商	27
2.7.4 帧中继上的 IP	28
2.8 SONET 和 SDH 回路上的 PPP	28



2.9 多路径信道+(MPC+)	29
2.10 异步传输模式(ATM)	29
2.10.1 地址解析(ATMARP 和 InATMARP)	30
2.10.2 ATM 上的经典 IP	32
2.10.3 ATM LAN 仿真	36
2.10.4 ATM 上的经典 IP 与 LAN 仿真	38
2.11 ATM 上的多协议(MPOA)	39
2.11.1 MPOA 的好处	39
2.11.2 MPOA 逻辑部件	39
2.11.3 MPOA 功能性部件	40
2.11.4 MPOA 操作	42
2.12 参考文献	42
第 3 章 网络互联协议	44
3.1 网际协议(IP)	44
3.1.1 IP 编址	44
3.1.2 IP 子网	47
3.1.3 IP 路由	50
3.1.4 发送方法——单播、广播、组播和任意播	54
3.1.5 IP 地址耗尽问题	56
3.1.6 Intranet——专用 IP 地址	58
3.1.7 无类域间路由(CIDR)	59
3.1.8 IP 数据报	61
3.2 网际控制消息协议(ICMP)	69
3.2.1 ICMP 消息	70
3.2.2 ICMP 应用	76
3.3 网际组管理协议(IGMP)	77
3.4 地址解析协议(ARP)	78
3.4.1 ARP 综述	78
3.4.2 ARP 详细概念	78
3.4.3 ARP 和子网	80
3.4.4 代理 ARP 或者透明的子网划分	80
3.5 反向地址解析协议(RARP)	82
3.6 引导程序协议(BOOTP)	82
3.6.1 BOOTP 转发	85
3.6.2 BOOTP 考虑	86
3.7 动态主机配置协议(DHCP)	86
3.7.1 DHCP 消息格式	87

3.7.2	DHCP 消息类型	88
3.7.3	分配一个新的网络地址	89
3.7.4	DHCP 续租过程	90
3.7.5	重新使用以前分配的网络地址	91
3.7.6	配置参数存储库	92
3.7.7	DHCP 考虑	92
3.7.8	BOOTP 和 DHCP 的互操作性	92
第 4 章	路由协议	94
4.1	自治系统	95
4.2	IP 路由类型与 IP 路由算法	96
4.2.1	静态路由	96
4.2.2	距离向量路由	97
4.2.3	链路状态路由	97
4.2.4	混合路由	98
4.3	路由信息协议(RIP)	99
4.3.1	RIP 报文类型	99
4.3.2	RIP 报文格式	99
4.3.3	RIP 操作模式	100
4.3.4	计算距离向量	100
4.3.5	收敛与无穷计数	101
4.3.6	RIP 局限性	104
4.4	路由信息协议版本 2(RIP-2)	104
4.4.1	RIP-2 报文格式	105
4.4.2	RIP-2 局限性	106
4.5	RIPng for IPv6	106
4.5.1	RIPng 与 RIP-2 间的不同	106
4.5.2	RIPng 报文格式	106
4.6	开放式最短路径优先(OSPF)	108
4.6.1	OSPF 术语	109
4.6.2	OSPF 报文类型	113
4.6.3	邻居通信	113
4.6.4	OSPF 邻居状态机	115
4.6.5	OSPF 虚链路和传输区域	115
4.6.6	OSPF 路由重分发	116
4.6.7	OSPF stub 区域	117
4.6.8	OSPF 路由汇总	117
4.7	增强内部网关路由协议(EIGRP)	118



4.7.1	EIGRP 特征	118
4.7.2	术语	119
4.7.3	邻居发现和恢复	120
4.7.4	DUAL 算法	120
4.7.5	EIGRP 报文类型	122
4.8	外部网关协议(EGP)	122
4.9	边界网关协议(BGP)	123
4.9.1	BGP 概念和术语	123
4.9.2	IBGP 与 EBGP 通信	124
4.9.3	协议描述	126
4.9.4	路径选择	128
4.9.5	BGP 同步	130
4.9.6	BGP 聚集	131
4.9.7	BGP 联邦(Confederation)	132
4.9.8	BGP 路由反射器	133
4.10	路由协议选择	134
4.11	路由器执行的新增功能	134
4.12	基于 UNIX 系统的路由进程	135
第 5 章	传输层协议	136
5.1	端口和套接字	136
5.1.1	端口	136
5.1.2	套接字	137
5.2	用户数据报协议(UDP)	138
5.2.1	UDP 数据报格式	139
5.2.2	UDP 应用程序编程接口	139
5.3	传输控制协议(TCP)	140
5.3.1	TCP 概念	140
5.3.2	TCP 应用编程接口	149
5.3.3	TCP 拥塞控制算法	150
第 6 章	IP 组播	154
6.1	组播编址	154
6.1.1	单个物理网络上的组播技术	155
6.1.2	网络段之间的组播技术	155
6.2	网际组管理协议(IGMP)	156
6.2.1	IGMP 消息	156
6.2.2	IGMP 操作	157
6.3	组播传送树	158

6.4 组播转发算法	159
6.4.1 反向路径转发算法	159
6.4.2 基于中心的树算法	160
6.4.3 组播路由协议	160
6.5 距离向量组播路由协议(DVMRP)	160
6.5.1 协议综述	161
6.5.2 建立和维护组播传送树	162
6.5.3 DVMRP 隧道	163
6.6 组播 OSPF(MOSPF)	163
6.6.1 MOSPF 协议综述	164
6.6.2 MOSPF 和多个 OSPF 区域	164
6.6.3 MOSPF 和多个自治系统	165
6.6.4 MOSPF 互操作性	165
6.7 独立协议组播(PIM)	165
6.7.1 PIM 密集模式	166
6.7.2 PIM 稀疏模式	167
6.8 互联组播域	169
6.8.1 组播源发现协议(MSDP)	169
6.8.2 边界网关组播协议	171
6.9 组播主干网	171
6.9.1 MBONE 路由	171
6.9.2 组播应用	173

第 II 部分 TCP/IP 应用协议

第 7 章 应用结构和编程接口	174
7.1 应用特征	174
7.2 应用编程接口(API)	175
7.2.1 套接字 API	175
7.2.2 远程过程调用(RPC)	178
7.2.3 Windows 套接字版本 2	181
7.2.4 SNMP 分布式编程接口(SNMP DPI)	182
7.2.5 FTP API	184
7.2.6 CICS 套接字接口	184
7.2.7 IMS 套接字接口	185
7.2.8 扩展套接字	185
7.2.9 REXX 套接字	185



第 8 章 目录和命名协议	186
8.1 域名系统(DNS)	186
8.1.1 层次名称空间	186
8.1.2 正式域名(FQDN)	187
8.1.3 通用域名	187
8.1.4 国家域	188
8.1.5 映射域名到 IP 地址	188
8.1.6 映射 IP 地址到域名——指针查询	189
8.1.7 分布式名称空间	189
8.1.8 域名解析	190
8.1.9 域名系统资源记录	192
8.1.10 域名系统消息	194
8.1.11 一种简单的方案	197
8.1.12 扩展方案	199
8.1.13 传输	199
8.1.14 DNS 应用	200
8.1.15 参考文献	200
8.2 动态域名系统	201
8.2.1 UPDATE DNS 消息格式	202
8.2.2 IBM 的 DDNS 实现	203
8.2.3 代理 A 记录更新	209
8.3 网络信息系统(NIS)	211
8.4 轻量目录访问协议(LDAP)	211
8.4.1 LDAP——X.500 的轻量访问	212
8.4.2 LDAP 目录服务器	213
8.4.3 LDAP 体系结构综述	214
8.4.4 LDAP 模型	215
8.4.5 LDAP 安全性	219
8.4.6 LDAP URL	221
8.4.7 LDAP 与 DCE	222
8.4.8 支持目录的网络首创技术规范(DEN)	223
8.4.9 基于 Web 的企业管理(WBEM)	224
8.4.10 参考文献	224
第 9 章 远程执行与分布式计算	226
9.1 TELNET	226
9.1.1 TELNET 操作	226
9.1.2 终端仿真(TELNET 3270)	231

9.1.3	TN3270 增强(TN3270E).....	232
9.1.4	参考文献.....	234
9.2	远程执行命令协议(REXEC 与 RSH).....	234
9.3	分布式计算环境(DCE)简介	235
9.3.1	DCE 目录服务	236
9.3.2	DCE 安全服务	238
9.3.3	DCE 线程	241
9.3.4	DCE 远程过程调用	241
9.3.5	分布式时间服务.....	242
9.3.6	分布式文件服务(DFS).....	243
9.3.7	参考文献.....	245
第 10 章	文件相关的协议.....	246
10.1	文件传输协议(FTP)	246
10.1.1	FTP 综述	246
10.1.2	FTP 操作	247
10.1.3	应答码	249
10.1.4	FTP 演示方案	249
10.1.5	FTP 会话示例	250
10.1.6	匿名 FTP	251
10.1.7	使用 FTP 的远程作业项.....	251
10.2	普通文件传输协议(TFTP).....	251
10.2.1	TFTP 用法	251
10.2.2	协议描述	252
10.2.3	TFTP 组播选项	253
10.2.4	安全问题	254
10.3	网络文件系统(NFS).....	254
10.3.1	NFS 概念.....	254
10.3.2	NFS 版本 4	258
10.3.3	WebNFS	258
10.3.4	参考文献	259
10.4	Andrew 文件系统(AFS)	259
第 11 章	邮件应用	261
11.1	简单邮件传输协议(SMTP).....	261
11.1.1	SMTP 工作机制	262
11.1.2	SMTP 与域名系统.....	267
11.1.3	参考文献	269
11.2	多用途 Internet 邮件扩充协议(MIME).....	269



11.2.1	MIME 工作机制	271
11.2.2	内容类型字段	272
11.2.3	Content-Transfer-Encoding 字段	276
11.2.4	在消息报文头中使用非 ASCII 字符	280
11.2.5	参考文献	281
11.3	邮局协议(POP)	282
11.3.1	POP3 命令和响应	282
11.3.2	参考文献	283
11.4	Internet 消息访问协议版本 4(IMAP4)	283
11.4.1	IMAP4 基本电子邮件模型	284
11.4.2	IMAP4 命令和响应	284
11.4.3	消息号	285
11.4.4	IMAP4 状态	285
11.4.5	客户命令	286
11.4.6	参考文献	288
第 12 章	WWW	289
12.1	Web 浏览器	289
12.2	Web 服务器	290
12.3	超文本传输协议(HTTP)	291
12.3.1	HTTP 综述	291
12.3.2	HTTP 操作	292
12.4	内容	298
12.4.1	静态内容	299
12.4.2	客户端动态内容	299
12.4.3	服务器端的动态内容	300
12.4.4	对象	301
12.4.5	用 IBM Web 应用程序服务器开发内容	303
12.5	参考文献	303
第 13 章	多媒体协议	305
13.1	实时协议: RTP 和 RTCP	305
13.1.1	实时传输协议(RTP)	305
13.1.2	实时控制协议	309
13.1.3	RTCP 报文格式	311
13.1.4	RTP 转换器和混合器	312
13.1.5	实时应用	314
13.2	IP 电话	314
13.2.1	简介	315

13.2.2	IP 电话协议栈	315
13.2.3	ITU-T 建议 H.323	316
13.2.4	会话启动协议(SIP)	319
13.2.5	介质网关控制协议(MGCP)	321
13.2.6	介质网关控制器(Megaco)	321
13.2.7	信令协议功能比较	322
13.2.8	语音编码和压缩	323
第 14 章	无线应用协议(WAP)	324
14.1	WAP 环境	324
14.2	WAP 规范的关键要素	325
14.2.1	WAP 编程模型综述	325
14.2.2	WAP 网络配置	327
14.3	无线标记语言(WML)与 WMLScript	329
14.3.1	WML	329
14.3.2	WMLScript	331
14.4	推体系结构	331
14.4.1	推技术的框架	331
14.4.2	推代理网关(PPG)	332
14.4.3	推访问控制协议(PAP)	333
14.4.4	服务指示	334
14.4.5	推 OTA 协议	334
14.4.6	客户端基础结构	334
14.4.7	安全性	334
14.5	WAP 协议栈综述	335
14.5.1	无线应用环境(WAE)	336
14.5.2	无线电话应用	337
14.5.3	无线会话协议(WSP)	337
14.5.4	无线事务协议(WTP)	345
14.5.5	无线传输层安全(WTLS)	347
14.5.6	无线数据报协议(WDP)	350
14.6	协议总结	352
第 15 章	网络管理	354
15.1	简单网络管理协议和 MIB 综述	354
15.2	管理信息结构和管理信息标识(SMI)	355
15.3	管理信息库(MIB)	356
15.4	简单网络管理协议(SNMP)	359
15.5	简单网络管理协议版本 2(SNMPv2)	361



15.5.1	SNMPv2 实体	362
15.5.2	SNMPv2 团体	362
15.5.3	GetBulkRequest	363
15.5.4	InformRequest	364
15.6	SNMPv2 的 MIB	364
15.7	新的管理模型	365
15.8	简单网络管理协议版本 3(SNMPv3)	366
15.9	参考文献	368
第 16 章	实用程序	370
16.1	远程打印(LPR 和 LPD)	370
16.2	X Window 系统	370
16.2.1	功能概念	371
16.2.2	协议	374
16.3	网络新闻传输协议(NNTP)	374
16.4	Finger 协议	375
16.5	Netstat	375

第Ⅲ部分 高级概念和新技术

第 17 章	IPv6	376
17.1	IPv6 综述	377
17.2	IPv6 报文头格式	377
17.2.1	报文大小	379
17.2.2	扩展报文头	379
17.2.3	IPv6 编址	384
17.2.4	流量类型	389
17.2.5	流标志	389
17.3	网际控制消息协议版本 6(ICMPv6)	389
17.3.1	邻居发现	390
17.3.2	无态地址自动配置	397
17.3.3	组播侦听器发现	398
17.4	IPv6 中的 DNS	400
17.5	IPv6 中的 DHCP	402
17.5.1	DHCPv6 与 DHCPv4 间的不同	403
17.5.2	DHCPv6 消息	403
17.6	IPv6 的移动支持	404
17.7	Interent 迁移——从 IPv4 迁移到 IPv6	404

17.7.1 双重 IP 栈实现——IPv6/IPv4 结点	405
17.7.2 隧道技术	406
17.7.3 报文头转换	410
17.7.4 互操作性总结	410
17.8 朝 IPv6 方向发展	411
17.9 参考文献	411
第 18 章 多协议标志交换(MPLS)	413
18.1 MPLS 概述	413
18.1.1 传统的路由模型	413
18.1.2 MPLS 转发模型	413
18.1.3 附带的好处	413
18.2 MPLS 网络的组成部分	415
18.2.1 同等转发类(FEC)	415
18.2.2 标志切换	417
18.2.3 标志交换路径(LSP)	418
18.2.4 标志栈和标志层次	418
18.2.5 BGP 环境中的 MPLS 栈	419
18.3 标志分发协议	420
18.3.1 标志分发协议的类型	421
18.3.2 标志分发方法	421
18.4 流合并	421
18.4.1 在基于帧的环境中合并	422
18.4.2 在 ATM 环境中合并	422
18.5 多协议 λ 交换	422
第 19 章 移动 IP	424
19.1 移动 IP 概述	424
19.2 移动 IP 的操作	425
19.3 移动代理公告扩展	426
19.4 移动 IP 注册过程	427
19.5 隧道	429
19.6 广播数据报	429
19.7 移动检测	430
19.8 ARP 的考虑	430
19.9 移动 IP 的安全考虑	431
第 20 章 TCP/IP 与其他协议的集成	432
20.1 企业扩展器	432



20.2	数据链路交换	433
20.2.1	概述	433
20.2.2	功能描述	433
20.3	多协议传输网络(MPTN)	435
20.3.1	混合多协议网络的需求	435
20.3.2	MPTN 体系结构	435
20.3.3	MPTN 方法	435
20.3.4	MPTN 的主要部件	436
20.4	TCP/IP 之上的 NetBIOS	438
第 21 章	TCP/IP 安全	441
21.1	安全漏洞及其解决方案	441
21.1.1	破坏安全的常用攻击手段	441
21.1.2	网络安全问题的解决方案	441
21.1.3	实现安全解决方案	442
21.1.4	网络安全策略	444
21.2	密码学概述	444
21.2.1	术语	445
21.2.2	对称加密和密钥算法	446
21.2.3	不对称的或公钥算法	447
21.2.4	散列函数	450
21.2.5	数字证书和证书权威机构	454
21.2.6	随机数产生器	455
21.2.7	加密的出口/进口限制	456
21.3	防火墙	457
21.3.1	防火墙的概念	457
21.3.2	防火墙的组成部件	458
21.3.3	报文过滤路由器	458
21.3.4	应用级网关	460
21.3.5	电路级网关	463
21.3.6	防火墙的类型	464
21.4	网络地址转换(NAT)	467
21.4.1	NAT 的概念	468
21.4.2	转换机制	469
21.4.3	NAT 的局限性	470
21.5	IP 安全体系结构(IPsec)	471
21.5.1	概念	471
21.5.2	认证报文头(AH)	473

21.5.3	封装安全净荷(ESP).....	477
21.5.4	结合使用 IPsec 的两个协议.....	481
21.5.5	Internet 密钥交换协议(IKE)	486
21.6	SOCKS	497
21.7	安全 Shell(l).....	503
21.8	安全套接层(SSL)	503
21.8.1	SSL 概述	503
21.8.2	SSL 协议	505
21.9	传输层安全(TLS)	508
21.10	安全的多用途网际邮件扩充协议	509
21.11	虚拟专用网络(VPN)概述	509
21.12	Kerberos 认证和授权系统	510
21.12.1	假定	511
21.12.2	命名	511
21.12.3	Kerberos 认证过程	512
21.12.4	Kerberos 数据库管理	515
21.12.5	Kerberos 授权模型	515
21.12.6	Kerberos 版本 5 增强	515
21.13	远程访问认证协议	516
21.14	第二层隧道协议(L2TP)	517
21.14.1	术语	518
21.14.2	协议概述	519
21.14.3	L2TP 安全问题	520
21.15	安全电子事务(SET)	521
21.15.1	SET 角色	521
21.15.2	SET 事务	522
21.15.3	SET 证书方案	523
21.16	参考文献	524
第 22 章	服务质量	526
22.1	为什么需要 QoS	526
22.2	综合服务	527
22.2.1	服务类	529
22.2.2	资源预约协议(RSVP)	532
22.2.3	综合服务展望	541
22.3	差分服务	541
22.3.1	差分服务体系结构	542
22.3.2	差分服务网络上的综合服务	548