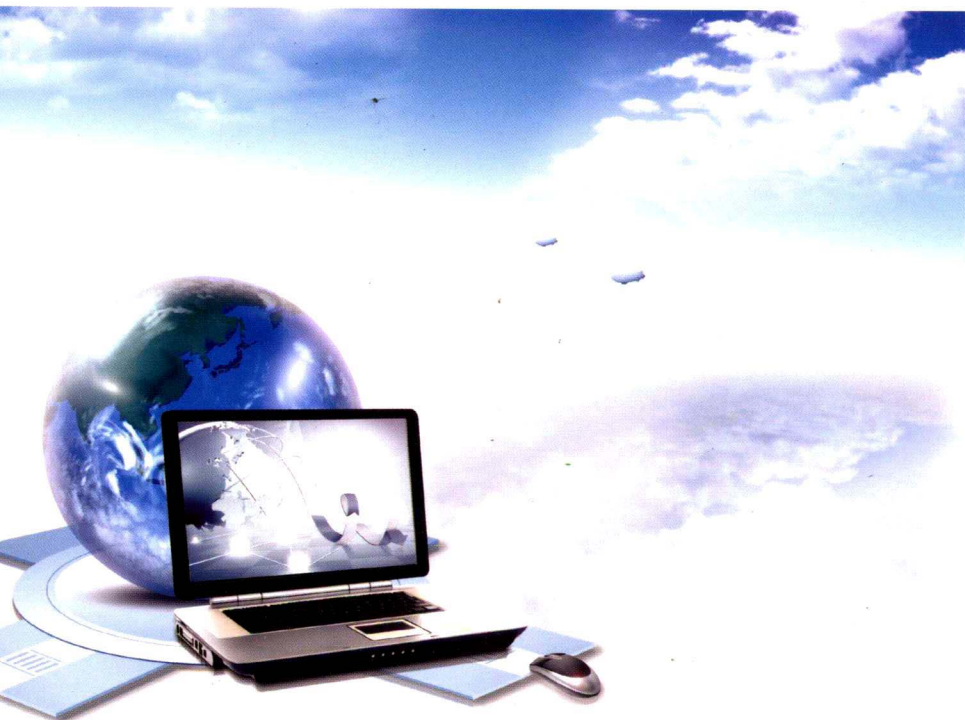




TEACHING MATERIALS
FOR COLLEGE STUDENTS
高等学校教材



TCP/IP 协议分析

■ 主 编 刘素芹 曹绍华

中国石油大学出版社

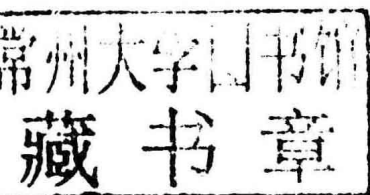


TEACHING MATERIALS
FOR COLLEGE STUDENTS
高等学校教材

TCP/IP 协议分析

TCP/IP Protocol Analysis

刘素芹 曹绍华 主编



中国石油大学出版社

图书在版编目(CIP)数据

TCP/IP 协议分析/刘素芹,曹绍华主编. —东营:

中国石油大学出版社,2012.3

ISBN 978-7-5636-3632-7

I. ①T… II. ①刘…②曹… III. ①计算机网络—通信协议—研究 IV. ①TN915.04

中国版本图书馆 CIP 数据核字(2012)第 039073 号

中国石油大学(华东)规划教材

书 名: TCP/IP 协议分析

作 者: 刘素芹 曹绍华

责任编辑: 高 颖(电话 0532—86981531)

封面设计: 青岛友一广告传媒有限公司

出 版 者: 中国石油大学出版社(山东 东营 邮编 257061)

网 址: <http://www.uppbook.com.cn>

电子信箱: shiyoujiaoyu@126.com

印 刷 者: 青岛星球印刷有限公司

发 行 者: 中国石油大学出版社(电话 0532—86981532,0546—8392563)

开 本: 180 mm×235 mm 印张:17 字数:343 千字

版 次: 2012 年 5 月第 1 版第 1 次印刷

定 价: 26.00 元

前言

PREFACE

随着计算机网络尤其是因特网应用的日益普及,人们越来越依赖于网络,网络新技术层出不穷,而支撑这些新技术的基础就是 TCP/IP 协议。众所周知,TCP/IP 协议已经成为计算机网络实际上的标准,只有深入了解 TCP/IP 协议,才能更深刻地理解计算机网络的工作原理,为进行网络方面的应用和研究打下坚实的基础,因此,“TCP/IP 协议分析”成为计算机专业本科生的一门专业基础课。

本书是作者根据多年的授课教案、实验资料,并参考一些新的资料整理而成的,具有以下特点:

- (1) 在介绍协议原理时,穿插了一些实验,能够激发读者的兴趣。
- (2) 在分析原理时,对相应的程序进行了分析,能够使读者的编程能力得到相应的提高。
- (3) 介绍了协议分析工具 Sniffer 的原理及使用方法,便于理论和实践的相互促进。

本书共分 12 章,第 1~6 章、第 8 章、第 9 章由刘素芹编写,第 7 章、第 10~12 章及附录由曹绍华编写。第 1 章介绍了 TCP/IP 协议的产生和发展,以及标准化流程等常识性的内容;第 2 章介绍了 TCP/IP 协议的基本原理、工作方法等基础知识;第 3~11 章详细介绍了 TCP/IP 协议中主要协议的原理、包格式及详细工作流程;第 12 章介绍了在 Windows 和 Unix/Linux 环境下 TCP/IP 协议的实现方式;附录介绍了 MPLS 协议的原理、应用情况及协议分析工具 Sniffer 的原理与使用方法。

在当今的网络社会,围绕着计算机和网络的技术日新月异,但“万变不离其宗”,计算机和网络的基础知识是不会变的。通过对本书的学习,希望读者掌握 TCP/IP 协议的核心技术,为以后的学习和工作打下良好的基础。

本书面向的主要对象是计算机学科各个专业的学生及从事计算机、通信、自动化等相关专业的工程技术人员,本书也可作为非计算机专业的学生及成人、网络教育学

生的教材,亦可供非计算机专业的工程技术人员参考。

在本书的编写过程中,参考了部分国内外有关教材和资料,获益匪浅,在此对这些文献的作者表示感谢。参考的主要资料有 Stevens(美国)编写的《TCP/IP》详解卷1 和村山公保(日本)等编写的 TCP/IP 系列丛书。硕士研究生李柏丹、邵红李、冯雪丽、李兴盛、孟令芬、硕珺、王婧、刘会会、焦芳、安仲奇在查阅资料、验证实验、文字录入和绘图方面做了大量工作,在此一并表示衷心的感谢。

由于书中涉及的内容是正在飞速发展的新技术,不当之处在所难免,敬请读者批评指正。

编 者
2011 年 12 月

目 录

CONTENTS

第 1 章 概 述	1
1.1 TCP/IP 协议的产生和发展	1
1.1.1 TCP/IP 协议的产生	1
1.1.2 TCP/IP 协议的发展	2
1.2 TCP/IP 协议的标准化	3
1.2.1 TCP/IP 协议的结构	3
1.2.2 TCP/IP 协议的标准化思想	4
1.2.3 TCP/IP 协议的标准化流程	4
1.2.4 TCP/IP 协议的请求评论文档 RFC	6
1.2.5 获得 RFC 的方法	8
1.3 TCP/IP 协议的特征	8
习 题	9
第 2 章 TCP/IP 协议基础知识	10
2.1 TCP/IP 计算机网络的构成	10
2.1.1 TCP/IP 计算机网络的结构	10
2.1.2 硬件和软件	10
2.1.3 控制通信的三个软件	12
2.2 TCP/IP 的工作原理	12
2.2.1 分层次模型和包交换	12
2.2.2 包的发送和接收	13
2.2.3 协议报头及其处理	16
2.3 TCP/IP 协议栈的实现方法	17
2.3.1 地址变换	17
2.3.2 协议栈的内部处理	20

2.3.3 套接字.....	22
2.3.4 系统调用及内部处理.....	24
2.3.5 原始 IP 和数据链路访问	25
2.3.6 多任务处理.....	25
习 题	29
第 3 章 数据链路层协议	30
3.1 数据链路层的定义.....	30
3.2 以太网 Ethernet	30
3.2.1 以太网的帧格式.....	31
3.2.2 CSMA/CD 共享介质访问.....	33
3.2.3 以太网的类型.....	34
3.3 串行链路 IP——SLIP	36
3.4 点对点协议 PPP	38
3.5 PPPoE	40
3.5.1 PPPoE 的特点	40
3.5.2 PPPoE 的优点	41
3.5.3 PPPoE 的帧格式	41
3.5.4 PPPoE 的实现过程	41
3.6 最大传输单元 MTU	42
习 题	43
第 4 章 ARP 和 RARP	44
4.1 ARP 的工作原理	44
4.2 ARP 高速缓存	46
4.3 ARP 的包格式	47
4.4 ARP 攻击	48
4.4.1 ARP 广播	48
4.4.2 ARP 欺骗	49
4.5 ARP 攻击的防御	49
4.5.1 对 ARP 广播的防御及根治	49
4.5.2 对 ARP 欺骗的防御	50
4.6 免费 ARP	50
4.7 RARP	51
习 题	52
第 5 章 网际互联协议 IP	53
5.1 IP 地址	53

5.1.1 IP 地址的分类	53
5.1.2 特殊 IP 地址	54
5.1.3 保留 IP 地址	55
5.1.4 子网掩码	55
5.2 IP 报文格式	55
5.3 IP 路由	60
5.4 IP 选路	61
5.4.1 选路的原理	62
5.4.2 ICMP 重定向	66
5.4.3 ICMP 路由器发现报文	68
5.5 动态路由协议	69
5.5.1 引言	69
5.5.2 动态选路	70
5.5.3 路由信息协议(RIP)	73
5.5.4 开放最短路径优先协议(OSPF)	76
5.5.5 边界网关协议(BGP)	83
5.6 IP 广播与多播	84
5.7 IP 分片与重组	85
5.7.1 IP 数据报的分片和处理	85
5.7.2 分片处理存在的问题	88
5.7.3 路径 MTU 探索	88
5.8 计算机内部的 IP 处理	91
5.8.1 主机的处理	91
5.8.2 路由器的处理	92
5.9 IP 的未来	93
5.9.1 IP 存在的问题	93
5.9.2 IPv6	94
习 题	95
第 6 章 因特网控制报文协议 ICMP	96
6.1 ICMP 报文的格式	96
6.2 ICMP 报文的类型	97
6.3 ICMP 的主要功能	100
6.4 Ping	100
6.4.1 Ping 命令的用法	101
6.4.2 使用 Ping 的顺序	102

6.5	Tracert	103
6.5.1	Tracert 的工作原理	103
6.5.2	Tracert 命令	104
6.6	利用 ICMP 进行主机探测	105
6.6.1	ICMP Echo	105
6.6.2	ICMP Sweep	106
6.6.3	Broadcast ICMP	106
6.6.4	Non-Echo ICMP	106
6.7	ICMP 的安全性分析	107
6.7.1	基于 ICMP 的 DoS 攻击	108
6.7.2	基于重定向的路由器欺骗	108
6.7.3	针对安全问题的应对策略	109
	习 题	110
第 7 章	IP 多播与 IGMP	111
7.1	广播与多播概述	111
7.2	广播	112
7.2.1	受限的广播	112
7.2.2	指向网络的广播	112
7.3	多播	113
7.3.1	多播组地址	113
7.3.2	多播组地址到以太网地址的转换	113
7.4	因特网组管理协议 IGMP	115
7.4.1	引言	115
7.4.2	IGMP 报文	115
7.4.3	IGMP 协议	115
	习 题	118
第 8 章	用户数据报协议 UDP	119
8.1	UDP 和 TCP 的比较	119
8.1.1	可靠性	119
8.1.2	数据流型与数据报型	120
8.1.3	数据报分发的实时性	121
8.1.4	通信对方的数量	122
8.1.5	流控制	122
8.1.6	拥塞控制	123
8.2	UDP 首部	125

8.3	UDP 的内部处理	126
8.4	套接字基础知识	126
8.4.1	套接字概述	127
8.4.2	基本套接字	129
8.4.3	典型过程图	131
8.5	利用套接字的 UDP 的控制	133
8.6	使用 UDP 协议进行通信	134
8.7	UDP 端口扫描	135
	习 题	136
第 9 章	传输控制协议 TCP	137
9.1	TCP 首部	137
9.2	TCP 的连接管理	140
9.2.1	建立连接	141
9.2.2	释放连接	141
9.2.3	其他	142
9.3	TCP 的数据传输	144
9.3.1	TCP 的交互数据流	144
9.3.2	TCP 的成块数据流	145
9.4	TCP 的定时器管理	146
9.4.1	TCP 的坚持定时器	146
9.4.2	TCP 的保活定时器	146
9.5	TCP 的超时与重传	146
9.5.1	往返时间测量	147
9.5.2	拥塞避免算法	147
9.5.3	快速重传和快速恢复算法	147
9.5.4	ICMP 差错	148
9.5.5	重新分组	148
9.6	使用 TCP 的应用程序设计	148
9.6.1	利用套接字进行 TCP 的控制	148
9.6.2	抽样程序与工作环境	150
9.6.3	TCP 服务端程序设计基础	150
9.6.4	TCP 客户端程序的基础	152
9.7	使用 TCP 协议进行通信	154
9.7.1	利用套接字进行 TCP 协议通信	154
9.7.2	TCP 程序实例的基本情况和使用方法	156

9.7.3	程序的执行实例	157
9.7.4	处理流程	157
9.8	TCP 端口扫描	160
9.8.1	TCP 扫描的类型	160
9.8.2	TCP 端口扫描程序 scanport_tcp	162
习 题		164
第 10 章	应用层协议	165
10.1	域名系统 DNS	165
10.1.1	DNS 概述	165
10.1.2	DNS 的工作原理	165
10.1.3	DNS 的报文格式	166
10.2	超文本传输协议 HTTP	168
10.2.1	HTTP 协议简介	168
10.2.2	HTTP 协议的几个重要概念	169
10.2.3	HTTP 协议的运作方式	169
10.3	SMTP 和 POP3	172
10.3.1	引言	172
10.3.2	SMTP 协议	172
10.3.3	POP3	173
10.4	Telnet	174
10.4.1	引言	174
10.4.2	Telnet 协议	175
10.5	文件传输协议 FTP	178
10.5.1	FTP 命令	179
10.5.2	FTP 应答	179
10.5.3	连接管理	180
10.6	网络文件系统 NFS	182
习 题		184
第 11 章	网络管理标准 SNMP	185
11.1	引言	185
11.1.1	网络管理要求	185
11.1.2	SNMP 参考模型	186
11.2	SNMP 发展历史	187
11.3	管理信息库 MIB	188
11.3.1	管理对象注册树	188

11.3.2	管理对象命名	189
11.3.3	管理对象访问约束	189
11.3.4	mib-2 子树	190
11.4	SNMP 通信协议	193
11.4.1	访问控制机制	194
11.4.2	报文格式	195
11.4.3	请求报文的处理过程	198
11.4.4	读取表格对象值的方法	199
11.4.5	端口的使用	201
11.5	管理信息结构 SMI	201
11.5.1	抽象标记语法 1	202
11.5.2	MIB 对象定义格式	203
11.5.3	基本编码规则 BER	204
11.5.4	用 BER 对 SNMP 报文进行编码	207
11.6	SNMP 的应用	209
	习 题	210
第 12 章	常见操作系统的 TCP/IP 协议实现	211
12.1	Windows 的 TCP/IP 协议实现	211
12.1.1	物理链路层	212
12.1.2	IP 层	214
12.1.3	传输层	217
12.1.4	TCP/IP 开发接口	221
12.2	UNIX/Linux 的 TCP/IP 协议实现	222
12.2.1	Linux 网络协议栈	222
12.2.2	Linux 网络数据处理流程	222
12.2.3	Linux 的 IP 路由	225
	习 题	225
附录 A	多协议标签交换 MPLS	226
A.1	MPLS 技术背景	226
A.2	MPLS 基本原理	227
A.2.1	术语	227
A.2.2	MPLS 数据结构	228
A.3	MPLS 数据转发原理	229
A.3.1	传统 IP 分组转发	230
A.3.2	MPLS 分组转发	230

A.4 标签分发协议	232
A.4.1 LDP 的消息类型	232
A.4.2 LDP 会话的建立过程	233
A.4.3 标签的分配和管理	233
A.4.4 倒数第二跳弹出	236
A.4.5 流合并	237
A.5 MPLS 体系发展	237
附录 B Sniffer 技术介绍	239
B.1 Sniffer 软件简介	239
B.1.1 概述	239
B.1.2 功能简介	239
B.2 报文捕获解析	240
B.2.1 捕获面板	240
B.2.2 捕获过程报文统计	241
B.2.3 捕获报文查看	241
B.2.4 设置捕获条件	243
B.3 报文放送	245
B.3.1 编辑报文发送	245
B.3.2 捕获编辑报文发送	246
B.4 网络监视功能	246
B.4.1 Dashboard	246
B.4.2 Application Response Time(ART)	247
B.5 数据报文解码详解	247
B.5.1 数据报文分层	248
B.5.2 以太报文结构	248
B.5.3 IP 协议	249
B.5.4 ARP 协议	251
B.5.5 PPPOE 协议	253
B.5.6 Radius 协议	256
参考文献	260

第 1 章 概 述

1.1 TCP/IP 协议的产生和发展

目前,在计算机网络领域,TCP/IP 协议是使用最广泛的协议,已经成为事实上的标准。那么,为什么 TCP/IP 协议如此普及呢?一方面是因为个人计算机的操作系统如 Windows 和 Mac OS 等都支持 TCP/IP 协议标准;另一方面是因为各计算机公司的操作系统中都使用了 TCP/IP 协议的通信功能,再加上计算机工业界的全体都支持 TCP/IP 协议这股不可抗拒的潮流,两者综合起来就形成了今天的 TCP/IP 协议普及的势头。目前,在市场上几乎看不到不支持 TCP/IP 协议的操作系统。

为什么计算机制造商都大力支持 TCP/IP 协议呢?下面首先从 Internet 的发展历史来考虑这个问题。

1.1.1 TCP/IP 协议的产生

1) TCP/IP 协议起源于军事应用

20 世纪 60 年代后期,以美国国防部 DoD(the Department of Defense)组织为中心,人们开展了通信技术研究试验,认为通信在军事上是非常重要的,而且还指出了使用包通信的必要性。

在通信的过程中,人们期望能够获得这样的计算机网络:即使计算机网络的一部分遭到敌人的攻击,可能会发生一定的故障,但是整个通信线路也可以发送数据,通信不会停止。另外,如果使用包通信技术,多个用户还可以共享一条线路,具有提高线路利用率的优点,因此包交换技术和包通信技术受到了人们的青睐。

2) ARPANET 的诞生

1969 年,为了检验包交换技术的实用性,美国构建了一个计算机网络。最初,这个计算机网络以美国国防部为中心,将美国西海岸的大学和研究机构的 4 个节点(node)连接起来,之后随着技术的迅速发展,一般的用户也开始加入进来,其规模在当时是非常大的,后来又迅速发展壮大。

该计算机网络被人们称为 ARPANET,它是 Internet 的鼻祖。在短短的三年内,它就从几个节点发展到了几十个节点。该试验取得了很大的成功,充分证明了使

用包进行数据通信的方法是实用的。

3) TCP/IP 协议的诞生

在试验过程中,不仅单纯地进行了大学和研究机构之间通信干线的包交换试验,还在通信双方的计算机之间进行了具有高可靠性的通信方法的综合通信协议试验。ARPANET 内部的研究小组于 1975 年开发了 TCP/IP 协议,并且在 1982 年制定了 TCP/IP 协议的标准。

1.1.2 TCP/IP 协议的发展

1) UNIX 的普及和 Internet 的壮大

在 TCP/IP 协议的发展历程中,ARPANET 发挥了重要作用。TCP/IP 协议之所以能在计算机网络领域迅速普及,与 BSD 的 UNIX 有着很大的关系。

当时,在大学和企业的研究机构中,作为计算机的操作系统,BSD 的 UNIX 已被广泛使用,它的内部实际上已经安装了 TCP/IP 协议。1983 年,UNIX 作为 ARPANET 的正式连接手续,采用了 TCP/IP 协议。在同一年里,Sun Microsystems 公司开始将安装有 TCP/IP 协议的产品提供给一般用户。

20 世纪 80 年代,随着 LAN 的迅速发展,UNIX 工作站开始迅速普及,采用 TCP/IP 协议构筑的计算机网络也盛行起来。伴随着这股潮流,大学和研究机构也慢慢地与 Internet 连接起来。

Internet 使得 UNIX 机器的互联迅速普及,因此,可以说作为计算机网络的主流协议,TCP/IP 协议与 UNIX 有着不解之缘,两者都在迅速地发展和普及。

另外,从 20 世纪 80 年代后期开始,以企业为主的用户更多地使用计算机,计算机制造商们也开始将自己的协议与 TCP/IP 协议相对应。

2) 商用 Internet 服务的开始

Internet 最初是作为试验和研究用的。到了 20 世纪 90 年代,企业和一般家庭开始使用 Internet 连接,Internet 服务开始被广泛利用,同时利用 Internet 的商业服务也随之普及。通常把提供这样服务的公司称为 ISP,即因特网服务提供者(互联网服务提供商)。

当时,在微型计算机的通信中,人与人之间利用计算机进行通信的需求开始激增,但是由于微型计算机通信只能在有限的会员之间进行,所以当多个微型计算机加入通信时,由于不同的微型计算机通信的操作方法各异,存在着许多不便之处。

随后,Internet 将企业和一般家庭相连接,同时也提供商业服务。作为研究用的计算机网络,由于已经过很长一段时间的使用,所以 TCP/IP 协议在服务中不断成熟起来,并成为广泛使用的协议。因此,现在的 Internet 不再是作为研究用的计算机网络,而是作为有偿的商业服务,并且迅速地普及和壮大。

如果使用 Internet,那么利用 WWW(万维网)就可以在世界范围内收集信息,还

可以利用电子邮件进行通信,向世界的各个角落随心所欲地发送消息。Internet 本身并不存在什么会员,它是一个在世界范围内连接、能够被广大用户所使用、开放的计算机网络。它不但能够提供丰富多彩的服务,而且用户自己也能够开辟新的服务。自由自在、开放的 Internet,正在迅速地被企业和人们所使用。

TCP/IP 协议的发展历程见表 1-1。

表 1-1 TCP/IP 协议发展历程

时 间	内 容
1960 年后期	由 DoD 研究和开发了与通信技术有关的问题
1969 年	ARPANET 诞生,开发包交换技术
1972 年	ARPANET 获得成功,节点扩大到 50 个以上
1975 年	TCP/IP 协议诞生
1982 年	制定了 TCP/IP 协议的标准,开始提供 UNIX,并在 UNIX 系统中实际安装了 TCP/IP 协议
1983 年	由 ARPANET 的正式手续确定了 TCP/IP 协议
1989 年左右	在 LAN 上,TCP/IP 协议的应用迅速普及
1990 年左右	无论是 WAN 还是 LAN,都向着 TCP/IP 协议的方向发展
1995 年左右	随着 Internet 的商业化,成立了许多因特网服务提供者
1996 年	制定了下一代 IPv6 标准,该标准登录进了 RFC(1998 年对其进行了修改)

1.2 TCP/IP 协议的标准化

虽然 ISO(国际标准化组织)组织制定了称为 OSI 的国际标准化协议,但 OSI 并不是一个能够真正使用的协议,它只是一个网络体系结构蓝本。在这个蓝本的基础上制定的网络通信协议才能够互相通信,而 TCP/IP 协议正是符合 OSI 要求的通信协议。本节将介绍 TCP/IP 协议的标准化。

1.2.1 TCP/IP 协议的结构

TCP/IP 协议的结构如图 1-1 所示。

仅就 TCP/IP 协议整个术语来讲,读者可能会认为它就是两个协议。实际上,TCP/IP 协议这个术语不仅表示 TCP 和 IP 这两个协议,还包括使用 IP 通信时所需要的其他协议,是一个协议簇。具体地讲,它还包括与 TCP 和 IP 关系密切的协议,例如 ARP,RARP,ICMP,IGMP,UDP 及很多应用层协议。另外,有时也把 TCP/IP 协议称为 Internet 协议簇,其含义是构筑 Internet 所需的协议的集合。

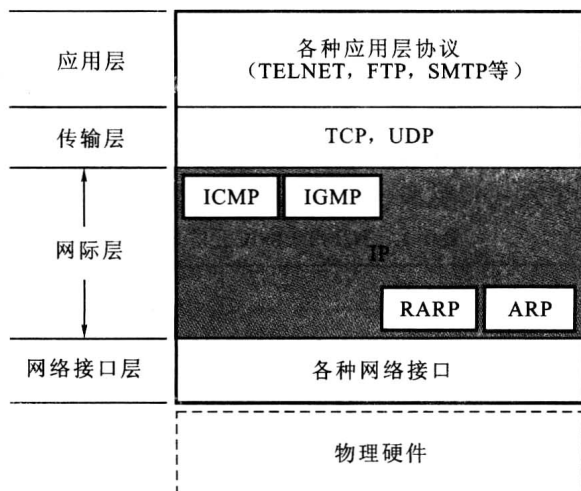


图 1-1 TCP/IP 协议的结构

1.2.2 TCP/IP 协议的标准化思想

TCP/IP 协议的标准化具有两个明显的特点,即开放性和实用性。

首先,TCP/IP 协议是对所有人开放的,是经过 IETF (Internet Engineering Task Force,互联网工程任务组)的多阶段讨论后才确定的。通常,这种讨论是通过电子邮件列表进行的。对电子邮件列表来说,无论谁都能参加。

其次,在重视协议性能指标的同时,还追求相互之间能够通信的技术。人们常说,与设计 TCP/IP 协议的性能指标相比,TCP/IP 协议更重视程序的开发,这也就是说以重视开发的形式来确定协议。一般地,在编译程序后才书写性能规格说明书。但是,在确定协议的性能指标时,必须一边考虑实际安装一边进行作业。在仔细斟酌协议的详细性能指标时,已经具有了安装该协议的设备,它们必须在限定的条件下能够进行实际的运行。所以,在 TCP/IP 协议中,当大体上确定了协议的性能指标后,再根据多个实际安装的情况进行相互连接试验。如果发生了问题,就进行讨论,然后进行程序、协议的标准化工作。由于 TCP/IP 协议是试验实际运行情况后才确定性能指标的,所以它是一个实用性很高的协议。

1.2.3 TCP/IP 协议的标准化流程

协议的标准化工作是通过 IETF 的讨论进行的。通常,IETF 每年召开三次会议,这些会议是按照邮件列表使用电子邮件进行讨论的。在这些邮件列表中,无论谁都可以自由地参加。

TCP/IP 协议的标准化流程如图 1-2 所示。