



“十二五”普通高等教育本科国家级规划教材

计算机网络经典教材系列

微课版（教学视频 教学课件PPT）

计算机网络

（第8版）

谢希仁 编著



中国工信出版集团



电子工业出版社
http://www.phei.com.cn



“十二五”普通高等教育本科国家级规划教材

计算机网络经典教材系列

微课版（教学视频 教学课件PPT）

计算机网络

（第8版）

谢希仁 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书自 1989 年首次出版以来，曾多次修订。在 2006 年本书通过了教育部的评审，被纳入普通高等教育“十一五”国家级规划教材；2008 年出版的第 5 版获得了教育部 2009 年精品教材称号。2013 年出版的第 6 版是“十二五”普通高等教育本科国家级规划教材。现在的第 8 版又在原有的基础上进行了一些修订。

全书分为 9 章，比较全面系统地介绍了计算机网络的发展和原理体系结构、物理层、数据链路层（包括局域网）、网络层、运输层、应用层、网络安全、互联网上的音频/视频服务，以及无线网络和移动网络等内容。各章均附有习题（附录 A 给出了部分习题的答案和提示）。全书课件放在电子工业出版社华信教育资源网（www.hxedu.com.cn），供读者下载参考。

本书的特点是概念准确、论述严谨、内容新颖、图文并茂，突出基本原理和基本概念的阐述，同时力图反映计算机网络的一些最新发展。本书可供电气信息类和计算机类专业的大学本科生和研究生使用，对从事计算机网络工作的工程技术人员也有参考价值。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

计算机网络 / 谢希仁编著. —8 版. —北京：电子工业出版社，2021.6
ISBN 978-7-121-41174-8

I. ①计... II. ①谢... III. ①计算机网络—高等学校—教材 IV. ①TP393

中国版本图书馆 CIP 数据核字（2021）第 090476 号

责任编辑：郝志恒 牛晓丽

印 刷：保定市中画美凯印刷有限公司

装 订：保定市中画美凯印刷有限公司

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱

邮编：100036

开 本：787×1092 1/16 印张：30.25 字数：774 千字

版 次：1989 年 11 月第 1 版

2021 年 6 月第 8 版

印 次：2021 年 6 月第 1 次印刷

印 数：1~150000 册

定 价：59.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlbs@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：QQ 1098545482。

目 录

第 1 章 概述.....	1
1.1 计算机网络在信息时代中的作用.....	1
1.2 互联网概述.....	3
1.2.1 网络的网络.....	3
1.2.2 互联网基础结构发展的三个阶段.....	5
1.2.3 互联网的标准化工作.....	8
1.3 互联网的组成.....	9
1.3.1 互联网的边缘部分.....	10
1.3.2 互联网的核心部分.....	12
1.4 计算机网络在我国的发展.....	17
1.5 计算机网络的类别.....	19
1.5.1 计算机网络的定义.....	19
1.5.2 几种不同类别的计算机网络.....	19
1.6 计算机网络的性能.....	21
1.6.1 计算机网络的性能指标.....	21
1.6.2 计算机网络的非性能特征.....	26
1.7 计算机网络体系结构.....	27
1.7.1 计算机网络体系结构的形成.....	27
1.7.2 协议与划分层次.....	29
1.7.3 具有五层协议的体系结构.....	31
1.7.4 实体、协议、服务和访问点.....	34
1.7.5 TCP/IP 的体系结构.....	36
本章的重要概念.....	38
习题.....	39
第 2 章 物理层.....	42
2.1 物理层的基本概念.....	42
2.2 数据通信的基础知识.....	43
2.2.1 数据通信系统的模型.....	43
2.2.2 有关信道的几个基本概念.....	44
2.2.3 信道的极限容量.....	46
2.3 物理层下面的传输媒体.....	48
2.3.1 导引型传输媒体.....	48
2.3.2 非导引型传输媒体.....	52
2.4 信道复用技术.....	56
2.4.1 频分复用、时分复用和统计时分复用.....	56
2.4.2 波分复用.....	59
2.4.3 码分复用.....	60

2.5	数字传输系统	61
2.6	宽带接入技术	63
2.6.1	ADSL 技术	63
2.6.2	光纤同轴混合网 (HFC 网)	66
2.6.3	FTTx 技术	67
	本章的重要概念	69
	习题	70
第 3 章	数据链路层	71
3.1	数据链路层的几个共同问题	72
3.1.1	数据链路和帧	72
3.1.2	三个基本问题	73
3.2	点对点协议 PPP	78
3.2.1	PPP 协议的特点	78
3.2.2	PPP 协议的帧格式	80
3.2.3	PPP 协议的工作状态	82
3.3	使用广播信道的数据链路层	84
3.3.1	局域网的数据链路层	84
3.3.2	CSMA/CD 协议	87
3.3.3	使用集线器的星形拓扑	92
3.3.4	以太网的信道利用率	94
3.3.5	以太网的 MAC 层	95
3.4	扩展的以太网	99
3.4.1	在物理层扩展以太网	99
3.4.2	在数据链路层扩展以太网	101
3.4.3	虚拟局域网	104
3.5	高速以太网	106
3.5.1	100BASE-T 以太网	106
3.5.2	吉比特以太网	107
3.5.3	10 吉比特以太网(10GbE)和更快的以太网	108
3.5.4	使用以太网进行宽带接入	110
	本章的重要概念	111
	习题	112
第 4 章	网络层	115
4.1	网络层的几个重要概念	115
4.1.1	网络层提供的两种服务	115
4.1.2	网络层的两个层面	117
4.2	网际协议 IP	119
4.2.1	虚拟互连网络	119
4.2.2	IP 地址	122
4.2.3	IP 地址与 MAC 地址	130
4.2.4	地址解析协议 ARP	133

4.2.5 IP 数据报的格式.....	136
4.3 IP 层转发分组的过程.....	140
4.3.1 基于终点的转发.....	140
4.3.2 最长前缀匹配.....	142
4.3.3 使用二叉线索查找转发表.....	144
4.4 网际控制报文协议 ICMP.....	146
4.4.1 ICMP 报文的种类.....	146
4.4.2 ICMP 的应用举例.....	148
4.5 IPv6.....	149
4.5.1 IPv6 的基本首部.....	150
4.5.2 IPv6 的地址.....	152
4.5.3 从 IPv4 向 IPv6 过渡.....	155
4.5.4 ICMPv6.....	156
4.6 互联网的路由选择协议.....	157
4.6.1 有关路由选择协议的几个基本概念.....	157
4.6.2 内部网关协议 RIP.....	159
4.6.3 内部网关协议 OSPF.....	164
4.6.4 外部网关协议 BGP.....	168
4.6.5 路由器的构成.....	175
4.7 IP 多播.....	179
4.7.1 IP 多播的基本概念.....	179
4.7.2 在局域网上进行硬件多播.....	180
4.7.3 网际组管理协议 IGMP 和多播路由选择协议.....	181
4.8 虚拟专用网 VPN 和网络地址转换 NAT.....	185
4.8.1 虚拟专用网 VPN.....	185
4.8.2 网络地址转换.....	188
4.9 多协议标签交换 MPLS.....	189
4.9.1 MPLS 的工作原理.....	190
4.9.2 MPLS 首部的位置与格式.....	193
4.9.3 新一代的 MPLS.....	193
4.10 软件定义网络 SDN 简介.....	194
本章的重要概念.....	200
习题.....	202
第 5 章 运输层.....	211
5.1 运输层协议概述.....	211
5.1.1 进程之间的通信.....	211
5.1.2 运输层的两个主要协议.....	213
5.1.3 运输层的端口.....	214
5.2 用户数据报协议 UDP.....	215
5.2.1 UDP 概述.....	215
5.2.2 UDP 的首部格式.....	217
5.3 传输控制协议 TCP 概述.....	219
5.3.1 TCP 最主要的特点.....	219

5.3.2 TCP 的连接	220
5.4 可靠传输的工作原理	221
5.4.1 停止等待协议	221
5.4.2 连续 ARQ 协议	224
5.5 TCP 报文段的首部格式	225
5.6 TCP 可靠传输的实现	229
5.6.1 以字节为单位的滑动窗口	229
5.6.2 超时重传时间的选择	233
5.6.3 选择确认 SACK	235
5.7 TCP 的流量控制	236
5.7.1 利用滑动窗口实现流量控制	236
5.7.2 TCP 的传输效率	237
5.8 TCP 的拥塞控制	238
5.8.1 拥塞控制的一般原理	238
5.8.2 TCP 的拥塞控制方法	241
5.8.3 主动队列管理 AQM	245
5.9 TCP 的运输连接管理	246
5.9.1 TCP 的连接建立	247
5.9.2 TCP 的连接释放	248
5.9.3 TCP 的有限状态机	250
本章的重要概念	251
习题	253
第 6 章 应用层	260
6.1 域名系统 DNS	261
6.1.1 域名系统概述	261
6.1.2 互联网的域名结构	262
6.1.3 域名服务器	264
6.2 文件传送协议	269
6.2.1 FTP 概述	269
6.2.2 FTP 的基本工作原理	269
6.2.3 简单文件传送协议 TFTP	271
6.3 远程终端协议 TELNET	271
6.4 万维网 WWW	272
6.4.1 万维网概述	272
6.4.2 统一资源定位符 URL	274
6.4.3 超文本传送协议 HTTP	276
6.4.4 万维网的文档	283
6.4.5 万维网的信息检索系统	288
6.4.6 博客和微博	290
6.4.7 社交网站	292
6.5 电子邮件	293
6.5.1 电子邮件概述	293
6.5.2 简单邮件传送协议 SMTP	296

6.5.3	电子邮件的信息格式	298
6.5.4	邮件读取协议 POP3 和 IMAP	298
6.5.5	基于万维网的电子邮件	300
6.5.6	通用互联网邮件扩充 MIME	300
6.6	动态主机配置协议 DHCP	304
6.7	简单网络管理协议 SNMP	306
6.7.1	网络管理的基本概念	306
6.7.2	管理信息结构 SMI	308
6.7.3	管理信息库 MIB	311
6.7.4	SNMP 的协议数据单元和报文	313
6.8	应用进程跨越网络的通信	316
6.8.1	系统调用和应用编程接口	316
6.8.2	几种常用的系统调用	318
6.9	P2P 应用	320
6.9.1	具有集中目录服务器的 P2P 工作方式	320
6.9.2	具有全分布式结构的 P2P 文件共享程序	322
6.9.3	P2P 文件分发的分析	324
6.9.4	在 P2P 对等方中搜索对象	325
	本章的重要概念	328
	习题	330
第 7 章	网络安全	334
7.1	网络安全问题概述	334
7.1.1	计算机网络面临的安全性威胁	334
7.1.2	安全的计算机网络	336
7.1.3	数据加密模型	337
7.2	两类密码体制	338
7.2.1	对称密钥密码体制	338
7.2.2	公钥密码体制	339
7.3	鉴别	341
7.3.1	报文鉴别	341
7.3.2	实体鉴别	346
7.4	密钥分配	348
7.4.1	对称密钥的分配	348
7.4.2	公钥的分配	350
7.5	互联网使用的安全协议	352
7.5.1	网络层安全协议	353
7.5.2	运输层安全协议	357
7.5.3	应用层安全协议	362
7.6	系统安全: 防火墙与入侵检测	364
7.6.1	防火墙	364
7.6.2	入侵检测系统	365
7.7	一些未来的发展方向	366
	本章的重要概念	366

习题	368
第 8 章 互联网上的音频/视频服务	370
8.1 概述	370
8.2 流式存储音频/视频	374
8.2.1 具有元文件的万维网服务器	375
8.2.2 媒体服务器	375
8.2.3 实时流式协议 RTSP	378
8.3 交互式音频/视频	379
8.3.1 IP 电话概述	379
8.3.2 IP 电话所需要的几种应用协议	383
8.3.3 实时传输协议 RTP	384
8.3.4 实时传输控制协议 RTCP	386
8.3.5 H.323	387
8.3.6 会话发起协议 SIP	388
8.4 改进“尽最大努力交付”的服务	390
8.4.1 使互联网提供服务质量	390
8.4.2 调度和管制机制	392
8.4.3 综合服务 IntServ 与资源预留协议 RSVP	395
8.4.4 区分服务 DiffServ	398
本章的重要概念	400
习题	401
第 9 章 无线网络和移动网络	405
9.1 无线局域网 WLAN	405
9.1.1 无线局域网的组成	406
9.1.2 802.11 局域网的物理层	411
9.1.3 802.11 局域网的 MAC 层协议	412
9.1.4 802.11 局域网的 MAC 帧	418
9.2 无线个人区域网 WPAN	422
9.3 蜂窝移动通信网	425
9.3.1 蜂窝无线通信技术的发展简介	425
9.3.2 LTE 网络与互联网的连接	432
9.4 移动 IP	436
9.4.1 移动 IP 的基本概念	436
9.4.2 移动网络对高层协议的影响	440
9.5 移动通信的展望	440
本章的重要概念	441
习题	443
附录 A 部分习题的解答	445
附录 B 英文缩写词	461
附录 C 参考文献与网址	472

放是每一次面向连接的通信中必不可少的过程。因此，运输连接就有三个阶段，即：**连接建立、数据传送和连接释放**。运输连接的管理就是使运输连接的建立和释放都能正常地进行。

在 TCP 连接建立过程中要解决以下三个问题：

- (1) 要使每一方能够确知对方的存在。
- (2) 要允许双方协商一些参数（如最大窗口值、是否使用窗口扩大选项和时间戳选项以及服务质量等）。
- (3) 能够对运输实体资源（如缓存大小、连接表中的项目等）进行分配。

TCP 连接的建立采用客户服务器方式。主动发起连接建立的应用进程叫作**客户(client)**，而被动等待连接建立的应用进程叫作**服务器(server)**。

5.9.1 TCP 的连接建立

TCP 建立连接的过程叫作**握手**，握手需要在客户和服务器之间交换三个 TCP 报文段。图 5-28 画出了三报文握手^①建立 TCP 连接的过程。

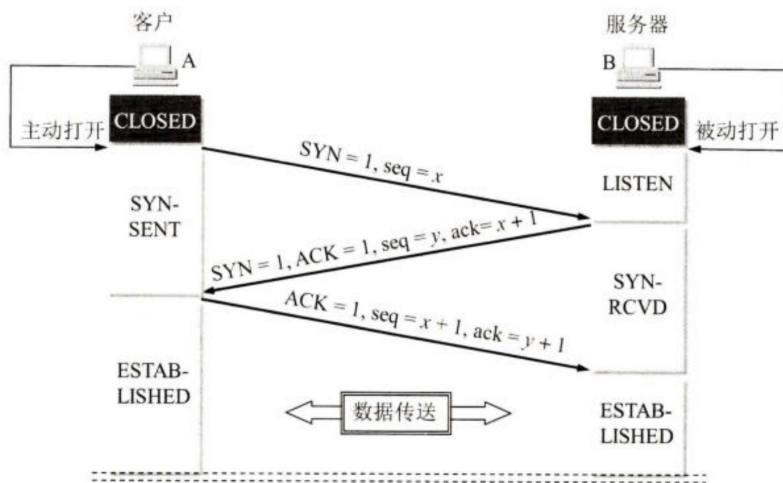


图 5-28 用三报文握手建立 TCP 连接

假定主机 A 运行的是 TCP 客户程序，而 B 运行 TCP 服务器程序。最初两端的 TCP 进程都处于 CLOSED（关闭）状态。图中在主机下面的方框分别是 TCP 进程所处的状态。请注意，在本例中，A 主动打开连接，而 B 被动打开连接。

一开始，B 的 TCP 服务器进程先创建**传输控制块 TCB**^②，准备接受客户进程的连接请求。然后服务器进程就处于 LISTEN（收听）状态，等待客户的连接请求。如有，即做出响应。

① 注：三报文握手是本教材首次采用的译名。在 RFC 793（TCP 标准的文档）中使用的名称是 three way handshake，但这个名称很难译为准确的中文。例如，以前本教材曾采用“三次握手”这个广为流行的译名。其实这是在一次握手过程中交换了三个报文，而并不是进行了三次握手（这有点像两个人见面进行一次握手时，他们的手上下摇晃了三次，但这并非进行了三次握手）。最近再次重新阅读了 RFC 793 文档，发现有这样的表述：“three way (three message) handshake”。可见采用“三报文握手”这样的译名，在意思的表达上应当是比较准确的。请注意，handshake 使用的是单数而不是复数，表明只是一次握手。

② 注：传输控制块 TCB (Transmission Control Block) 存储了每一个连接中的一些重要信息，如：TCP 连接表、指向发送和接收缓存的指针、指向重传队列的指针、当前的发送和接收序号，等等。

A 的 TCP 客户进程也是首先创建**传输控制块 TCB**。然后，在打算建立 TCP 连接时，向 B 发出连接请求报文段，这时首部中的同步位 $SYN = 1$ ，同时选择一个初始序号 $seq = x$ 。TCP 规定，SYN 报文段（即 $SYN = 1$ 的报文段）不能携带数据，但要**消耗掉一个序号**。这时，TCP 客户进程进入 SYN-SENT（同步已发送）状态。

B 收到连接请求报文段后，如同意建立连接，则向 A 发送确认。在确认报文段中应把 SYN 位和 ACK 位都置 1，确认号是 $ack = x + 1$ ，同时也为自己选择一个初始序号 $seq = y$ 。请注意，这个报文段也不能携带数据，但同样**要消耗掉一个序号**。这时 TCP 服务器进程进入 SYN-RCVD（同步收到）状态。

TCP 客户进程收到 B 的确认后，还要向 B 给出确认。确认报文段的 ACK 置 1，确认号 $ack = y + 1$ ，而自己的序号 $seq = x + 1$ 。TCP 的标准规定，ACK 报文段可以携带数据。但**如果不携带数据则不消耗序号**，在这种情况下，下一个数据报文段的序号仍是 $seq = x + 1$ 。这时，TCP 连接已经建立，A 进入 ESTABLISHED（已建立连接）状态。

当 B 收到 A 的确认后，也进入 ESTABLISHED 状态。

上面给出的连接建立过程叫作**三报文握手**。请注意，在图 5-28 中 B 发送给 A 的报文段，也可拆成两个报文段。可以先发送一个确认报文段（ $ACK = 1, ack = x + 1$ ），然后再发送一个同步报文段（ $SYN = 1, seq = y$ ）。这样的过程就变成了**四报文握手**，但效果是一样的。

为什么 A 最后还要发送一次确认呢？这主要是为了防止已失效的连接请求报文段突然又传送到了 B，因而产生错误。

所谓“已失效的连接请求报文段”是这样产生的。考虑一种正常情况，A 发出连接请求，但因连接请求报文丢失而未收到确认。于是 A 再重传一次连接请求。后来收到了确认，建立了连接。数据传输完毕后，就释放了连接。A 共发送了两个连接请求报文段，其中第一个丢失，第二个到达了 B，没有“已失效的连接请求报文段”。

现假定出现一种异常情况，即 A 发出的第一个连接请求报文段并没有丢失，而是在某些网络节点长时间滞留了，以致延误到连接释放以后的某个时间才到达 B。本来这是一个早已失效的报文段。但 B 收到此失效的连接请求报文段后，就误认为是 A 又发出一次新的连接请求。于是就向 A 发出确认报文段，同意建立连接。假定不采用报文握手，那么只要 B 发出确认，新的连接就建立了。

由于现在 A 并没有发出建立连接的请求，因此不会理睬 B 的确认，也不会向 B 发送数据。但 B 却以为新的运输连接已经建立了，并一直等待 A 发来数据。B 的许多资源就这样白白浪费了。

采用三报文握手的办法，可以防止上述现象的发生。例如在刚才的异常情况下，A 不会向 B 的确认发出确认。B 由于收不到确认，就知道 A 并没有要求建立连接。

5.9.2 TCP 的连接释放

TCP 连接释放过程比较复杂，我们仍结合双方状态的改变来阐明连接释放的过程。

数据传输结束后，通信的双方都可释放连接。现在 A 和 B 都处于 ESTABLISHED 状态（如图 5-29 所示）。A 的应用进程先向其 TCP 发出连接释放报文段，并停止再发送数据，主动关闭 TCP 连接。A 把连接释放报文段首部的终止

扫一扫



视频讲解

控制位 FIN 置 1，其序号 $seq = u$ ，它等于前面已传送过的数据的最后一个字节的序号加 1。这时 A 进入 FIN-WAIT-1（终止等待 1）状态，等待 B 的确认。请注意，TCP 规定，FIN 报文段即使不携带数据，它也消耗掉一个序号。

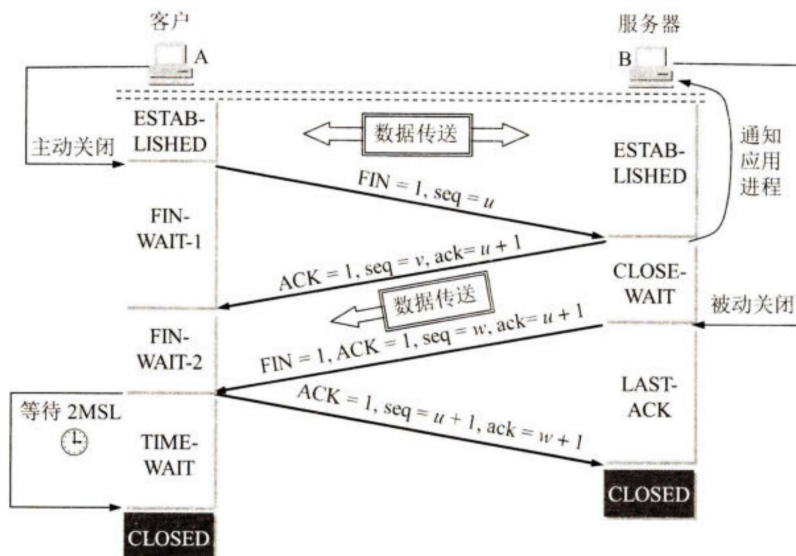


图 5-29 TCP 连接释放的过程

B 收到连接释放报文段后即发出确认，确认号是 $ack = u + 1$ ，而这个报文段自己的序号是 v ，等于 B 前面已传送过的数据的最后一个字节的序号加 1。然后 B 就进入 CLOSE-WAIT（关闭等待）状态。TCP 服务器进程这时应通知高层应用进程，因而从 A 到 B 这个方向的连接就释放了，这时的 TCP 连接处于半关闭(half-close)状态，即 A 已经没有数据要发送了，但 B 若发送数据，A 仍要接收。也就是说，从 B 到 A 这个方向的连接并未关闭，这个状态可能会持续一段时间。

A 收到来自 B 的确认后，就进入 FIN-WAIT-2（终止等待 2）状态，等待 B 发出的连接释放报文段。

若 B 已经没有要向 A 发送的数据，其应用进程就通知 TCP 释放连接。这时 B 发出的连接释放报文段必须使 $FIN = 1$ 。现假定 B 的序号为 w （在半关闭状态 B 可能又发送了一些数据）。B 还必须重复上次已发送过的确认号 $ack = u + 1$ 。这时 B 就进入 LAST-ACK（最后确认）状态，等待 A 的确认。

A 在收到 B 的连接释放报文段后，必须对此发出确认。在确认报文段中把 ACK 置 1，确认号 $ack = w + 1$ ，而自己的序号是 $seq = u + 1$ （根据 TCP 标准，前面发送过的 FIN 报文段要消耗一个序号）。然后进入到 TIME-WAIT（时间等待）状态。请注意，现在 TCP 连接还没有释放掉。必须经过时间等待计时器(TIME-WAIT timer)设置的时间 2MSL 后，A 才进入到 CLOSED 状态。时间 MSL 叫作最长报文段寿命(Maximum Segment Lifetime)，RFC 793 建议设为 2 分钟。但这完全是从工程上来考虑的，对于现在的网络， $MSL = 2$ 分钟可能太长了一些。因此 TCP 允许不同的实现可根据具体情况使用更小的 MSL 值。因此，从 A 进入到 TIME-WAIT 状态后，要经过 4 分钟才能进入到 CLOSED 状态，才能开始建立下一个新

的连接。当 A 撤销相应的传输控制块 TCB 后，就结束了这次的 TCP 连接。

为什么 A 在 TIME-WAIT 状态必须等待 2MSL 的时间呢？这两个理由。

第一，为了保证 A 发送的最后一个 ACK 报文段能够到达 B。这个 ACK 报文段有可能丢失，因而使处在 LAST-ACK 状态的 B 收不到对已发送的 FIN + ACK 报文段的确认。B 会超时重传这个 FIN + ACK 报文段，而 A 就能在 2MSL 时间内收到这个重传的 FIN + ACK 报文段。接着 A 重传一次确认，重新启动 2MSL 计时器。最后，A 和 B 都正常进入到 CLOSED 状态。如果 A 在 TIME-WAIT 状态不等待一段时间，而是在发送完 ACK 报文段后立即释放连接，那么就无法收到 B 重传的 FIN + ACK 报文段，因而也不会再发送一次确认报文段。这样，B 就无法按照正常步骤进入 CLOSED 状态。

第二，防止上一节提到的“已失效的连接请求报文段”出现在本连接中。A 在发送完最后一个 ACK 报文段后，再经过时间 2MSL，就可以使本连接持续的时间内所产生的所有报文段都从网络中消失。这样就可以使下一个新的连接中不会出现这种旧的连接请求报文段。

B 只要收到了 A 发出的确认，就进入 CLOSED 状态。同样，B 在撤销相应的传输控制块 TCB 后，就结束了这次的 TCP 连接。我们注意到，B 结束 TCP 连接的时间要比 A 早一些。

上述的 TCP 连接释放过程是四报文握手。

除时间等待计时器外，TCP 还设有一个保活计时器(keepalive timer)。设想有这样的情况：客户已主动与服务器建立了 TCP 连接。但后来客户端的主机突然出故障。显然，服务器以后就不能再收到客户发来的数据。因此，应当有措施使服务器不要再白白等待下去。这就是使用保活计时器。服务器每收到一次客户的数据，就重新设置保活计时器，时间的设置通常是两小时。若两小时没有收到客户的数据，服务器就发送一个探测报文段，以后则每隔 75 秒钟发送一次。若一连发送 10 个探测报文段后仍无客户的响应，服务器就认为客户端出了故障，接着就关闭这个连接。

5.9.3 TCP 的有限状态机

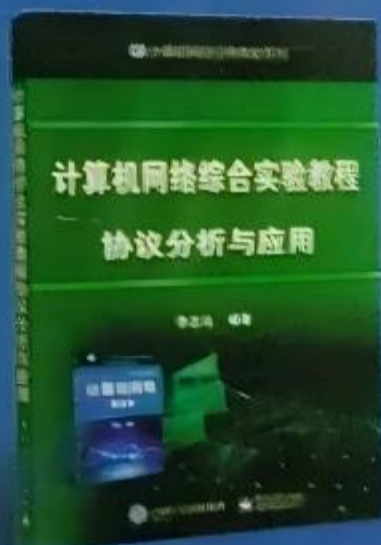
为了更清晰地看出 TCP 连接的各种状态之间的关系，图 5-30 给出了 TCP 的有限状态机。图中每一个方框是 TCP 可能具有的状态。每个方框中的大写英文字符串是 TCP 标准所使用的 TCP 连接状态名。状态之间的箭头表示可能发生的状态变迁。箭头旁边的字，表明引起这种变迁的原因，或表明发生状态变迁后又出现什么动作。请注意图中有三种不同的箭头。粗实线箭头表示对客户进程的正常变迁。粗虚线箭头表示对服务器进程的正常变迁。另一种细线箭头表示异常变迁。

我们可以把图 5-30 和前面的图 5-28、图 5-29 对照起来看。在图 5-28 和图 5-29 中左边客户进程从上到下的状态变迁，就是图 5-30 中粗实线箭头所指的状态变迁。而在图 5-28 和 5-29 右边服务器进程从上到下的状态变迁，就是图 5-30 中粗虚线箭头所指的状态变迁。

还有一些状态变迁，例如连接建立过程中的从 LISTEN 到 SYN-SENT 和从 SYN-SENT 到 SYN-RCVD。读者可分析在什么情况下会出现这样的变迁（见习题 5-43）。



计算机网络经典教材系列



陆续出版中……



第7版视频讲解
微信扫码，即可观看



计算机网络**教师**沟通群 (QQ)
教师交流，资源共享，与作者和编辑互动



责任编辑：郝志恒 牛晓丽
责任美编：秦 靖
交流投稿请联系QQ：9616328 1098545482



定价：59.80元