高等学校计算机专业教材精选·网络与通信技术

计算机网络
信息安全与应用

贺思德 编著

清华大学出版社

高等学校计算机专业教材精选·网络与通信技术

计算机网络信息安全与应用

贺思德 编著

清华大学出版社
北京

内 容 简 介

本书介绍了计算机网络远程连接的规划设计、运行管理、网络信息安全的保障与监测、网络用户上网行为监管等实际应用中的基础知识。书中按照互联网参考模型的分层结构，从下层至上层，即按照网络数据包封装的逐层解剖顺序，深入浅出地讨论每一层的主流协议原理与实用技术，以及各层出现的现实安全威胁问题，图文并茂地列举了网络信息安全监管中的大量案例分析。采用开源的网络数据捕获与分析软件作为教学实验工具，每章附有习题与实践课题，让读者在自己的网络计算机上理论联系实际、由浅入深地边学习边实践，掌握与提高分析解决网络信息安全系统规划、运维监管中的实际问题的能力。

本书可作为通信与计算机网络、信息安全、电子商务等相关专业的本科生、研究生的教材，也可作为计算机网络和信息安全运维管理的工程技术人员的参考书。

图书在版编目（CIP）数据

计算机网络信息安全与应用/贺思德编著. --北京：清华大学出版社，2012.2
（高等学校计算机专业教材精选·网络与通信技术）
ISBN 978-7-302-27296-0

Ⅰ. ①计… Ⅱ. ①贺… Ⅲ. ①计算机网络－安全技术－高等学校－教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 233236 号

责任编辑：白立军
封面设计：傅瑞学
责任校对：李建庄
责任印制：王秀菊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：28　　**字　　数**：700 千字
版　　次：2012 年 2 月第 1 版　　**印　　次**：2012 年 2 月第1 次印刷
印　　数：1～3000
定　　价：45.00 元

产品编号：040032-1

出版说明

我国高等学校计算机教育近年来迅猛发展，应用所学计算机知识解决实际问题，已经成为当代大学生的必备能力。

时代的进步与社会的发展对高等学校计算机教育的质量提出了更高、更新的要求。现在，很多高等学校都在积极探索符合自身特点的教学模式，涌现出一大批非常优秀的精品课程。

为了适应社会的需求，满足计算机教育的发展需要，清华大学出版社在进行大量调查研究的基础上，组织编写了《高等学校计算机专业教材精选》。本套教材从全国各高校的优秀计算机教材中精挑细选了一批很有代表性且特色鲜明的计算机精品教材，把作者们对各自所授计算机课程的独特理解和先进经验推荐给全国师生。

本系列教材特点如下。

(1) 编写目的明确。本套教材主要面向广大高校的计算机专业学生，使学生通过本套教材，学习计算机科学与技术方面的基本理论和基本知识，接受应用计算机解决实际问题的基本训练。

(2) 注重编写理念。本套教材作者群为各高校相应课程的主讲，有一定经验积累，且编写思路清晰，有独特的教学思路和指导思想，其教学经验具有推广价值。本套教材中不乏各类精品课配套教材，并努力把不同学校的教学特点反映到每本教材中。

(3) 理论知识与实践相结合。本套教材贯彻从实践中来到实践中去的原则，书中的许多必须掌握的理论都将结合实例来讲，同时注重培养学生分析问题、解决问题的能力，满足社会用人要求。

(4) 易教易用，合理适当。本套教材编写时注意结合教学实际的课时数，把握教材的篇幅。同时，对一些知识点按教育部教学指导委员会的最新精神进行合理取舍与难易控制。

(5) 注重教材的立体化配套。大多数教材都将配套教师用课件、习题及其解答，学生上机实验指导、教学网站等辅助教学资源，方便教学。

随着本套教材陆续出版，我们相信它能够得到广大读者的认可和支持，为我国计算机教材建设及计算机教学水平的提高，为计算机教育事业的发展做出应有的贡献。

清华大学出版社

目　录

第 1 章　互联网及其应用概述 …… 1
1.1　网络应用与分层结构 …… 1
1.1.1　协议、服务和分层结构的例子 …… 2
1.1.2　开放系统互连 OSI 模型及规范化描述 …… 9
1.2　TCP/IP 网络模型与协议构架 …… 16
1.2.1　TCP/IP 网络协议的结构 …… 16
1.2.2　TCP/IP 网络模型与 OSI 模型之间的关系 …… 19
1.2.3　异类网络之间如何互联通信 …… 19
1.3　利用 Wireshark 捕获分析网络数据及其安全性 …… 24
1.4　计算机网络知识中的若干基本概念 …… 27
1.5　本章小结 …… 30
习题与实践 …… 31

第 2 章　广域网接入与身份认证技术 …… 33
2.1　电信系统的互联网接入服务 …… 33
2.1.1　电路交换的概念 …… 33
2.1.2　电话系统的信令和数据传输系统 …… 34
2.1.3　电信系统提供的互联网接入服务 …… 35
2.1.4　拨号调制解调器 …… 36
2.1.5　数字用户线路 xDSL …… 39
2.1.6　点对点的数据通信协议 PPP …… 42
2.2　身份认证协议 PAP 和 CHAP …… 45
2.2.1　口令认证协议(PAP) …… 46
2.2.2　挑战握手身份认证协议(CHAP) …… 46
2.3　AAA 与 RADIUS 协议原理与应用 …… 47
2.3.1　对用户的 AAA 认证、授权与计费管理 …… 47
2.3.2　RADIUS 协议原理与应用 …… 48
2.4　基于 SDH 的多业务传输平台 MSTP 在互联网中的应用 …… 50
2.4.1　SDH 同步数据通信网简介 …… 50
2.4.2　基于 SDH 的多业务传输平台 MSTP 的广域网接口技术 …… 53
2.4.3　千兆广域以太网在多业务传输平台 MSTP 上的实现 …… 58
2.5　本章要点 …… 59

习题与实践 …… 60

第 3 章　以太网家族及其安全应用 …… 62
3.1　以太网与 IEEE 802.3 …… 62
3.1.1　IEEE 802 局域网标准 …… 62
3.1.2　IEEE 802.3 与标准以太网 …… 63
3.1.3　以太网的物理层 …… 67
3.1.4　IEEE 802.3u 快速以太网 …… 71
3.1.5　IEEE 802.3z 千兆以太网 …… 72
3.1.6　IEEE 802.3ae 十千兆以太网 …… 73
3.2　动态主机配置协议 DHCP 及其安全 …… 74
3.2.1　DHCP 协议的工作过程 …… 75
3.2.2　DHCP 协议的安全问题 …… 76
3.3　地址解析协议 ARP 及其安全问题 …… 76
3.3.1　静态 ARP 地址映射 …… 77
3.3.2　动态 ARP 地址查询 …… 78
3.3.3　ARP 诱骗的原理与防御 …… 80
3.4　基于无源光纤网的千兆以太网 EPON …… 82
3.4.1　EPON 的网络结构 …… 83
3.4.2　EPON 的工作原理 …… 84
3.4.3　EPON 在城域网的三网融合中的应用 …… 86
3.4.4　EPON 的信息安全问题 …… 87
3.5　IEEE 802.11 无线局域网 …… 87
3.5.1　IEEE 802.11 无线局域网的结构 …… 87
3.5.2　IEEE 802.11 无线局域网的 MAC 子层 …… 89
3.5.3　IEEE 802.11 无线局域网的物理层 …… 95
3.5.4　IEEE 802.11 无线局域网的安全性 …… 97
3.6　本章小结 …… 99
习题与实践 …… 100

第 4 章　IPv4 和 IPv6 协议及其安全 …… 102
4.1　互联网 IP 地址 …… 102
4.1.1　IPv4 地址及其分类 …… 102
4.1.2　无类 IP 地址分配 …… 105
4.1.3　网络地址转换(NAT) …… 109
4.1.4　IPv6 地址 …… 112
4.2　互联网层协议 …… 115
4.2.1　网络互联需解决的问题 …… 115
4.2.2　IPv4 互联网协议 …… 116

4.2.3 IPv6 互联网协议 …… 125
4.2.4 从 IPv4 网络到 IPv6 网络的过渡技术方案 …… 130
4.3 本章要点 …… 131
习题与实践 …… 132

第 5 章 传输层协议及其攻击案例 …… 134
5.1 进程对进程的传输 …… 134
5.2 用户数据报协议 …… 137
5.2.1 UDP 协议使用的公认端口号 …… 137
5.2.2 UDP 的数据报结构 …… 138
5.2.3 UDP 数据报的传输 …… 139
5.2.4 UDP 协议的应用领域 …… 139
5.3 传输控制协议 …… 140
5.3.1 TCP 提供的服务 …… 140
5.3.2 TCP 的特性 …… 143
5.3.3 TCP 数据段 …… 144
5.3.4 建立 TCP 连接的过程 …… 145
5.3.5 TCP 数据段的传输过程 …… 147
5.3.6 终止 TCP 的连接 …… 149
5.3.7 TCP 的流量控制 …… 150
5.3.8 TCP 的差错控制 …… 151
5.4 数据流控制传输协议简介 …… 154
5.5 传输层的网络攻击案例 …… 156
5.5.1 利用 TCP 对目标主机的开放端口扫描 …… 156
5.5.2 利用 TCP 对目标主机的半开放端口扫描 …… 158
5.5.3 利用 TCP 对目标主机的 Xmas 扫描 …… 158
5.5.4 无效包扫描 …… 159
5.6 本章小结 …… 160
习题与实践 …… 161

第 6 章 应用层协议及其安全 …… 163
6.1 万维网的基本构架 …… 163
6.2 域名系统及其安全 …… 166
6.2.1 域名系统概述 …… 166
6.2.2 DNS 报文格式 …… 169
6.2.3 DNS 域名/IP 地址解析的工作流程 …… 171
6.2.4 DNS 报文的封装实例 …… 172
6.2.5 域名系统的安全隐患 …… 174
6.3 超文本传输协议 …… 176

6.4 Cookie 及其安全应用 …… 181
6.5 文件传输协议及其安全 …… 184
6.5.1 FTP 工作过程举例 …… 186
6.5.2 FTP 的安全问题 …… 188
6.6 电子邮件及其信息安全 …… 189
6.6.1 电子邮件的传输过程 …… 189
6.6.2 邮件传输代理和邮件访问代理 …… 190
6.6.3 多功能互联网邮件扩展与安全邮件 …… 193
6.6.4 垃圾电子邮件及其防范 …… 197
6.7 本章要点 …… 201
习题与实践 …… 202

第 7 章 网络故障诊断与信息安全分析工具 …… 204
7.1 网络测试常用命令 …… 204
7.1.1 PING 在线连通性测试命令 …… 205
7.1.2 路由跟踪探测命令 Traceroute …… 209
7.1.3 本机联网状态检测命令 Netstat …… 210
7.1.4 地址解析协议命令 Arp …… 214
7.1.5 IPconfig 本机网络配置状态命令 …… 215
7.1.6 net 命令 …… 217
7.2 网络数据捕获与信息安全诊断 …… 217
7.2.1 网络数据捕获工具的分类 …… 218
7.2.2 网络数据流的监测点选择 …… 218
7.2.3 捕获网络数据流的方法 …… 220
7.2.4 网络协议分析软件 Wireshark …… 221
7.3 本章小结 …… 248
习题与实践 …… 249

第 8 章 恶意软件及其监测防护 …… 252
8.1 恶意软件 …… 252
8.1.1 恶意软件及其威胁 …… 252
8.1.2 病毒的本质 …… 254
8.1.3 蠕虫 …… 258
8.2 病毒对抗措施 …… 260
8.2.1 对抗病毒的方法 …… 260
8.2.2 高级反病毒技术 …… 261
8.3 木马的工作原理与检测防范 …… 264
8.3.1 木马程序的工作原理 …… 264
8.3.2 木马的种类 …… 265

8.3.3 被木马入侵后出现的症状 …… 267
8.3.4 木马常用的启动方式及检测 …… 267
8.3.5 木马的隐藏与检测方法 …… 270
8.4 特洛伊木马入侵后的网络数据分析案例 …… 272
8.4.1 木马 SubSeven Legend …… 273
8.4.2 后门木马 NetBus …… 273
8.4.3 木马 RST.b …… 275
8.5 蠕虫的网络数据捕获分析案例 …… 276
8.5.1 SQL Slammer(监狱)蠕虫 …… 276
8.5.2 Code Red Worm(红色代码蠕虫) …… 277
8.5.3 Ramen 蠕虫 …… 278
8.6 本章小结 …… 282
习题与实践 …… 283

第 9 章 防火墙、IPS 入侵保护与安全访问控制 …… 285
9.1 防火墙的设计目标 …… 285
9.1.1 防火墙的控制功能 …… 285
9.1.2 防火墙功能的局限性 …… 286
9.1.3 防火墙的日志记录 …… 286
9.2 防火墙的类型与参数配置 …… 286
9.2.1 网络层的包过滤防火墙 …… 286
9.2.2 网络层的全状态检测防火墙 …… 290
9.2.3 应用层防火墙 …… 291
9.2.4 堡垒主机 …… 292
9.2.5 代理服务器 …… 293
9.3 网络防火墙的配置案例 …… 296
9.3.1 防火墙与 NAT 功能的组合配置 …… 296
9.3.2 防火墙的路由模式配置案例 …… 297
9.4 入侵检测与入侵保护系统 …… 298
9.4.1 入侵检测系统 …… 298
9.4.2 入侵保护系统 …… 300
9.4.3 分布式 NIPS 入侵保护系统配置案例 …… 301
9.5 主机安全访问控制系统 …… 302
9.5.1 安全访问控制的基本概念 …… 302
9.5.2 可信任系统的概念 …… 304
9.5.3 一种盗号木马的工作原理与防护 …… 305
9.5.4 Windows XP 操作系统的安全访问控制 …… 307
9.6 本章小结 …… 308
习题与实践 …… 309

第 10 章　信息加密与安全验证的基本技术 …… 311
10.1　对称密钥通信系统 …… 312
10.1.1　传统的对字符加密的方法 …… 312
10.1.2　数据加密的基本技术 …… 314
10.1.3　数据加密标准 DES 和 AES …… 316
10.2　非对称密钥通信系统 …… 320
10.2.1　RSA 加密算法 …… 320
10.2.2　Differ-Hellman 对称密钥交换算法 …… 322
10.3　信息安全技术提供的服务 …… 324
10.3.1　网络信息的保密通信 …… 325
10.3.2　报文的完整性验证 …… 326
10.3.3　对报文的数字签名 …… 330
10.3.4　网络实体的身份认证 …… 330
10.3.5　对称密钥系统的密钥分配 …… 333
10.3.6　非对称密钥系统的公钥发布方式 …… 337
10.3.7　CA 数字证书应用实例 …… 340
10.4　本章要点 …… 344
习题与实践 …… 345

第 11 章　互联网安全协议与电子商务应用 …… 347
11.1　网络层安全协议 IPSec 与 VPN …… 351
11.1.1　IPSec 的传输模式 …… 351
11.1.2　IPSec 的隧道模式 …… 351
11.1.3　IPSec 的两个安全协议 AH 和 ESP …… 352
11.1.4　实现虚拟私有网络的各类技术 …… 356
11.2　传输层安全协议 …… 360
11.2.1　SSL/TLS 中 4 个子协议的功能 …… 361
11.2.2　传输层安全协议 TLS 与 SSL 和 HTTPS 的关系 …… 364
11.2.3　基于单方认证的 TLS 安全电子邮件案例分析 …… 366
11.3　PGP 安全协议及其应用 …… 369
11.3.1　PGP 安全电子邮件 …… 370
11.3.2　PGP 采用的加密与验证算法 …… 372
11.4　安全电子交易 SET 系统 …… 374
11.4.1　安全电子交易 SET 系统概况 …… 374
11.4.2　SET 系统的组成部分 …… 375
11.4.3　SET 系统的工作流程 …… 376
11.4.4　对订货单与支付信息进行双重签名 …… 376
11.4.5　SET 的业务类型 …… 377
11.4.6　SET 的购货请求 …… 378

11.4.7 安全电子交易 SET 货款的授权与支付 …… 380
11.4.8 互联网电子商务中使用 SSL/TLS 与 SET 的比较 …… 381
11.4.9 Visa 公司的“3D 安全交易”(3-D Secure)协议简介 …… 382
11.5 本章要点 …… 382
习题与实践 …… 383

第 12 章 P2P 对等网络应用与上网行为管理 …… 385
12.1 P2P 对等网络应用系统的结构 …… 386
12.1.1 非结构化的 P2P 网络 …… 386
12.1.2 结构化的 P2P 网络系统 …… 389
12.2 P2P 对等网络应用系统 …… 392
12.2.1 P2P 应用系统的优缺点 …… 392
12.2.2 常见的 P2P 应用系统 …… 393
12.2.3 某校园网数据流分类统计案例 …… 394
12.3 网络用户的上网行为管理 …… 395
12.3.1 上网行为管理系统及其功能 …… 395
12.3.2 P2P 上网行为的监测与控制 …… 396
12.4 P2P 网络数据流的识别方法 …… 397
12.4.1 P2P 网络数据流识别方法的分类 …… 397
12.4.2 基于特征码的 P2P 网络数据识别技术 …… 399
12.5 P2P 应用系统及其特征码分析案例 …… 401
12.5.1 案例分析 Bit Torrent 原理及其特征码 …… 401
12.5.2 PPlive 的工作过程 …… 407
12.5.3 P2P 应用系统的特征码提取方法总结 …… 410
习题与实践 …… 411

附录 A 传输层常用的端口号 …… 413

附录 B 校验和的计算 …… 418
B.1 部分和的计算 …… 418
B.2 和的计算 …… 419
B.3 校验和的计算 …… 419

附录 C 各种进制的数值换算与 IPv4 地址 …… 420
C.1 十进制数 …… 420
C.2 二进制数与十进制数的转换 …… 420
C.3 十六进制数与十进制数的转换 …… 421
C.4 256 进制数与十进制数的转换 …… 421
C.5 计算举例：IPv4 地址的 4 种数值表达方式 …… 422

附录 D　CRC 循环冗余校验码的计算 …… 423
D.1　数组的运算可以转换为多项式的运算 …… 423
D.2　数据通信系统中 CRC 码的使用方法 …… 423

附录 E　素数与模运算的基本概念 …… 426
E.1　素数与互素数 …… 426
E.2　模运算的几个规则 …… 427

附录 F　ASCII 编码表 …… 429

参考文献 …… 434

第 1 章　互联网及其应用概述

本章先介绍互联网最常用的 Web 浏览、域名查询和电子邮件等的工作原理，让读者了解互联网络的总体概念，这是学习和研究网络安全的基础。以常见的网络应用为例简要说明：什么是网络协议，计算机网络通信的各方如何进行数据包的交换，各种协议数据包中所包含的信息，如何利用网络协议分析软件对网络传输的数据进行实时捕获与分析，具体包含以下内容。

计算机网络系统的业务与分层结构：一个十分复杂的网络通信系统可以分解成由一系列功能较为单一的模块或层(layer)来组成。利用大家熟悉的互联网最常用业务——Web 浏览、域名查询和电子邮件的工作过程，来说明通信双方的系统中各对等层协议之间是如何协调工作的，以及该层如何利用下层协议所提供的服务。例子包括 HTTP 网页浏览、DNS 域名查询和 SMTP 电子邮件、传输层 TCP 和 UDP 的服务、对等网络的文件共享、OSI 开放系统互连参考模型、单一路由进程的包交换网络、异构网络的互联模型、TCP/IP 网络的数据包构成。

TCP/IP 网络协议及分析工具：①TCP/IP 的网络模型；②TCP/IP 各层之间是如何工作的，分析一个简单的互联网络的实例来说明网络设备的 IP 地址和物理地址的作用，网络通信的双方如何发送和接收 IP 数据包，路由选择的过程；③物理层、互联网层、传输层和应用层之间是如何协调工作的；④如何使用网络协议分析工具 Wireshark 来捕获与分析网络传输的数据，由此可以直观地理解基于 TCP/IP 协议的客户机/服务器之间的通信工作过程。

本书强调必须理论联系实际进行学习，书中介绍的所有网络安全知识都需要学员在自己的网络计算机上进行同样的网络数据捕获与分析实验，以加深理解。因此对于具有初步网络基础知识的读者，建议首先学习掌握第 7 章介绍的网络数据分析工具和 Wireshark(下载网址 http://www.wireshark.org/download.html)，然后再利用这些工具从第 1 章开始边读书边实践。

1.1　网络应用与分层结构

网络通信可提供广泛的服务。人们通常使用网络与别人对话、发送电子邮件、传送文件、获取信息。在电子商务和工业控制领域使用网络执行重要的功能，例如：资金的转账，银行交易的自动处理，查询和更新数据库的信息，各种传感器和控制数据的传输。互联网越来越多地被用来提供传统的由无线电和电视系统所提供的“广播”服务。计算机网络在设计的时候应该考虑到其灵活性和可扩展性，既要能够提供和支持当前的业务，也要能适应未来的业务发展。为了达到这样的灵活性，必须要对网络有总体的构架和规划。

要使两个设备在网络上实现有效通信的整个过程是很复杂的，必须具备很多要素。早期的网络设计人员就意识到需要建立一个统一规范的通信网络的体系结构，将各种功能分类组织成一个相互关联的形式。于是在20世纪70年代各计算机公司开发了各自知识产权的不同的网络结构规范。所有这些结构的一个共同特点是将通信的功能分组归类为一组相关的和可以管理的“层”。通信系统的功能可按以下的任务进行分层：

(1) 从一台网络计算机的一个进程与另一台网络计算机的一个对等进程间的数据传输，即将网络的应用功能分为一层。

(2) 在相互连接的网络里通过多个不同的网段对数据包进行路由和转发，即将网络互联的传输系统类型分为一层。

(3) 在同一个网络内，将数据帧从一台计算机的物理接口传送到另一台计算机的物理接口，即在同一个网段内按信道的物理参数进行分层。

将执行这些功能的实体按层的模型相互叠加起来，一个层工作于另一个层之上来实现通信，并用“网络的分层结构”来表示一组协议，它们定义了每一层应当具有的功能。

将整个通信过程分解为一叠含若干层的结构是简化整个网络设计的第一步。还要准确定义各层之间的相互关系，确定每一层对上一层所提供的服务，以及各层之间的接口，上层通过这些接口对下层提出服务的要求，而下层通过接口向上层传递服务的结果。一个清晰定义的服务和层间接口可以让上层直接调用下层的服务，而不必去考虑下面的各层如何实现这样的服务。一旦下层向上层提交并完成了所要求的服务，下层的工作就结束了。同样，在任何时候都可以在已经具有的某一层之上再引入和建立新的服务，在此上层又可以开发新的服务。这样就对网络未来的功能扩展提供了很大的灵活性。反之，如果将网络设计为一个单一的整体，由一个很复杂的硬件和软件来实现对网络的所有功能要求，这样的网络很快就会过时淘汰，因为要对它进行功能扩展和改进是特别困难和昂贵的。网络分层构建的方案可以满足和适应当前及未来对网络应用越来越多样化的发展需要。

每个开发商按照网络各层定义的功能和层间接口来开发自己的硬件和软件产品，那么不同开发商的产品就可以相互组合起来构成一个完整的网络系统。如果对网络提出了新的功能需求，那么就只涉及某些层的功能扩展和更新，而对网络其他层无影响。

1.1.1 协议、服务和分层结构的例子

协议(Protocol)是一组规范，它规定了两个或多个通信实体之间的交互过程。在学习网络时会遇到各种协议，如HTTP、FTP和TCP等。协议的目的是提供某种类型的通信服务，例如，HTTP协议可实现网页的浏览，TCP协议可实现计算机之间的字节流的可靠传输。本章将看到整个通信过程可以被分组成一个协议的堆叠，每层使用它自己的协议执行一组特定的通信功能，并且每层都建立在它的下层所提供的服务之上。

这里使用大家熟悉的电子邮件和网页浏览为例来说明什么是协议，以及两个相邻层之间是如何互动的。先简单地讨论，详细分析见后面的章节。

1. 超文本传输协议HTTP、域名服务DNS和简单邮件协议SMTP

当前互联网的大多数应用都是基于客户端/服务器(Client/Server)关系结构。服务器

的进程通过监听某“端口”来等待外来的请求。端口是一个地址，标识了网络计算机上运行的一个特定进程。端口号范围是0～65 535，其中0～1023是公认端口号(Well Known Port Number)，1024～49 151为注册端口号，49 152～65 535为动态的和私有端口号，详细介绍见附录A。互联网广泛使用的应用服务都有固定的公认端口号，因此在网络计算机上的客户进程一旦有了需要就可以马上向服务器的众所周知的端口发出访问请求。服务器对这些请求提供响应服务。服务器软件通常运行在后台，被称为后台守护程序(Daemon)，例如，httpd就指的是超文本传输协议HTTP的服务器后台守护程序。

例1-1 HTTP和Web网页浏览。

首先以万维网(World Wide Web，WWW)为例。WWW的构架可以让用户访问放置于互联网上的计算机内的网页文件，这些文件采用超文本标记语言HTML等编写，文件由文本、图表和其他媒体构成，并通过嵌入在文档中的标记互相连接。万维网通过浏览器进行访问，它将HTML文件翻译显示为易懂的图形化界面，并允许用鼠标点击界面上的连接来访问其他网页文档。每个连接向浏览器提供一个“统一资源定位符URL”，它标识了存放这些文件的计算机名称、所需文档的存放路径和文件名，详见第6章。

超文本传输协议(Hyper Text Transfer Protocol，HTTP)定义了一组规则，客户机遵循这些规则与服务器沟通来获取文件。这些规则也定义了请求与响应的句法结构。此协议的实施中假设客户机与服务器之间是能直接交换信息的。通常，客户机的软件在发出请求之前，首先要与服务器建立起一个双向的TCP连接，详见第5章。

图1.1和表1.1所示为客户机向服务器获取一个文件所产生的进程顺序。在第1步中，一个用户通过点击一个链接来选择一个文件。例如，浏览器要获取有关此统一资源定位符URL的首页链接：http://www.sina.com.cn/index.shtml。

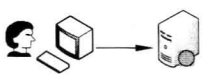
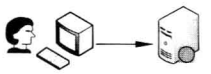
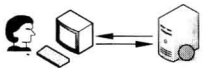
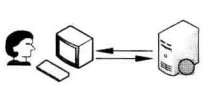
1		DNS查询：用户点击浏览器上文档的URL链接，浏览器向本地域名服务器发送请求，获取存放该文档的计算机的IP网络地址
2		获得了Web服务器的IP地址后，浏览器主动与服务器进程建立连接，一般是TCP连接。为了连接成功，服务器必须时刻等待着
3		浏览器运行的是HTTP客户版，它发出的请求中申明要获取的文件名以及可处理的文件格式等信息
4～6		存放所需文档的计算机运行HTTP服务器版软件。通过发送HTTP回答来响应客户机的HTTP请求，该应答包含了客户机所需格式的文档等信息
7～8		这时客户机就可以观看文档了。服务器等待一定时间后，若客户机无后续请求，它就关闭TCP连接

图1.1 客户机从Web服务器上获取一个网页文档的过程

表 1.1　在浏览 Web 网站的一个文档时客户机与服务器的 HTTP 信息交换

步　骤	事　　件	语 句 内 容
1	用户浏览器选定 Web 服务器的文档	
2	客户端通过 DNS 查询找到 Web 服务器 IP 地址，并建立一个 TCP 双向连接	
3	HTTP 客户端发送请求，要求获取文档。说明自己使用的协议和版本号	GET /news/2006118.html HTTP/1.1
4	HTTP 服务器后台守护程序监听 TCP 的 80 端口，等待接收客户的请求	
5	HTTP 服务器守护程序将查询结果回复客户，告诉客户将要收到的信息的描述，文件长度和文件类型等。大多数服务器使用的是格林尼治国际标准时间 GMT	HTTP /1.1 200 OK\r\n Date: Thu,09 Nov 2006 09:32:44 GMT\r\n Server: Microsoft IIS/5.0\r\n Last Modified: Wed,08 Nov 2006 02:58:36 GMT \r\n Content-Length: 8218\r\n Content-Type: text/html\r\n <html>
6	HTTP 服务器守护程序从内存读取所需文件，并将它通过 TCP 端口发给客户	<head><title></title>… 今日新闻
7	客户机收到 HTML 格式的网页文件后，显示在浏览器上	
8	HTTP 服务器守护程序等待一段时间空闲后，断开与客户机的连接	

通常客户机软件必须向域名服务器(DNS)进行查询，以获得域名 www.sina.com.cn 的主机的 IP 地址，DNS 查询结果为 211.95.77.17，在下一个例子中将讨论 DNS 是如何工作的。然后，客户端软件使用一个临时端口号与这个 IP 地址的 Web 服务器的默认端口 80 建立 TCP 连接(第 2 步)。客户端的临时端口号用于标识它自己的本次进程，此临时端口号仅用于本次连接。TCP 协议提供的是可靠的字节流传输服务。

当 TCP 连接建立后，客户端使用 HTTP 来请求获得一个文件(第 3 步)，这请求语句定义了获取的方法和指令、文件名和路径(/news/2006118.html)，以及浏览器使用的协议版本(HTTP/1.1)。服务器守护程序识别出这语句中的 3 个要素，并在存储器中找到这个文件的位置(第 4 步)。

在第 5 步中，守护程序发送一条状态语句(STATUS)，对将要发送的信息进行描述。应答码“200”表示客户端的请求成功接受，且所需文件附在后面。这些语句还包括服务器端的软件信息、文件长度(8218 字节)、文档类型(text/html)。如果是获取一幅图片，文档类型可以为 image/gif。如果请求失败，不被服务器接受，服务器会发送一个不同的响应代码来标识查询的失败，如“404”代表所需文件未找到。

在第 6 步中，HTTP 守护程序通过 TCP 连接发送文件，客户端接收并显示文件(第 7 步)。服务器保持此 TCP 连接以便接收该客户端的后续请求。当此 TCP 连接空闲了一段时限后，服务器将其断开。

从这个 HTTP 的例子可清楚地看出，一个协议只是处理在客户机和服务器之间的两个

对等进程间的互动。协议假定两个对等进程之间是直接交换信息的(忽略中转过程),如图 1.2 所示。

由于应用协议的客户端和服务器端通常不会直接连接在一起,在它们之间必须先建立一个连接。在此 HTTP 例子中,需要建立一个双向的、能按照正确顺序、无差错地传输信息的连接,TCP 协议提供了这样的可靠的连接服务。服务器端的 HTTP 进程把要发送的网页信息放入缓存中,TCP 实体将缓存中的网页数据分为数据段(segment)发送到客户端的 TCP 进程,如图 1.3 所示。在数据段头部中含有源端口地址和目的端口地址。HTTP 通信使用了由下一层的 TCP 所提供的服务,因此,在 HTTP 客户端和服务器端的网页文件传输实际上是通过虚拟通道传输的,通过 TCP 等下层实体透明地转发。图中的虚线箭头表示间接通信,实线箭头表示直接互连。在后面,将会看到 TCP 又依次使用了它下层的 IP 层提供的服务。

图 1.2 HTTP 客户端发出请求和服务器返回响应

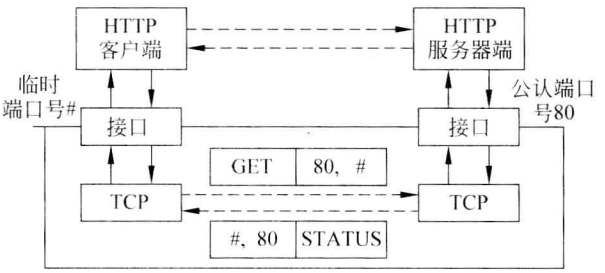


图 1.3 TCP 在 HTTP 客户端和服务器端之间提供了一个传输管道

应当注意 HTTP 应用协议如何调用 TCP 所提供的服务。当 HTTP 客户需要建立 TCP 连接时,客户端就调用"套接地址 socket address"系统。这种调用类似于功能函数调用,只是当套接地址的连接完成后,控制权被移交给操作系统内核处理。套接地址调用定义了一个确定的行动步骤,其中包括一些参数,例如:TCP 或 UDP,以及 IP 地址和端口地址信息。因此,HTTP 层与 TCP 层之间的交互是通过这些套接地址系统调用来实现的,详见后面介绍。

例 1-2 DNS 域名查询。

在 HTTP 的例子里提到客户端首先需要进行域名查询(DNS)以获得要访问的主机域名的 IP 地址。如图 1.4 所示,这个过程需要客户端向域名服务器 DNS 发送一个查询消息。DNS 是设置于互联网上很多主机中的一个分布式数据库,它用来进行域名和 IP 地址的转换查询,并提供电子邮件的路由信息。每一台 DNS 服务器持有和维护它自己的数据库并供其他计算机进行查询。需要查询的计算机首选访问本地域名服务器,本地 DNS 服务器可能放在某大学的网管部门或者互联网服务提供商 ISP 那里。这些本地域名服务器可保存近期经常被查询的域名/IP 地址。当遇到不可解析的域名查询时,本地域名服务器将查询请求转送给根域名服务器,目前全球分布有 13 台根域名服务器。当根域名服务器也解析不了时,就将其送到"域名授权服务器"。因为 Internet 上的每台 Web 服务器都要求至少在两台授权域名服务器注册。如果一台指定的域名服务器不能解析此域名,它就查询另一台域名服务器,如此继续直到找到能够解析此域名的 DNS 服务器。