计 算 机 科 学 丛 书

PEARSON

原书第7版

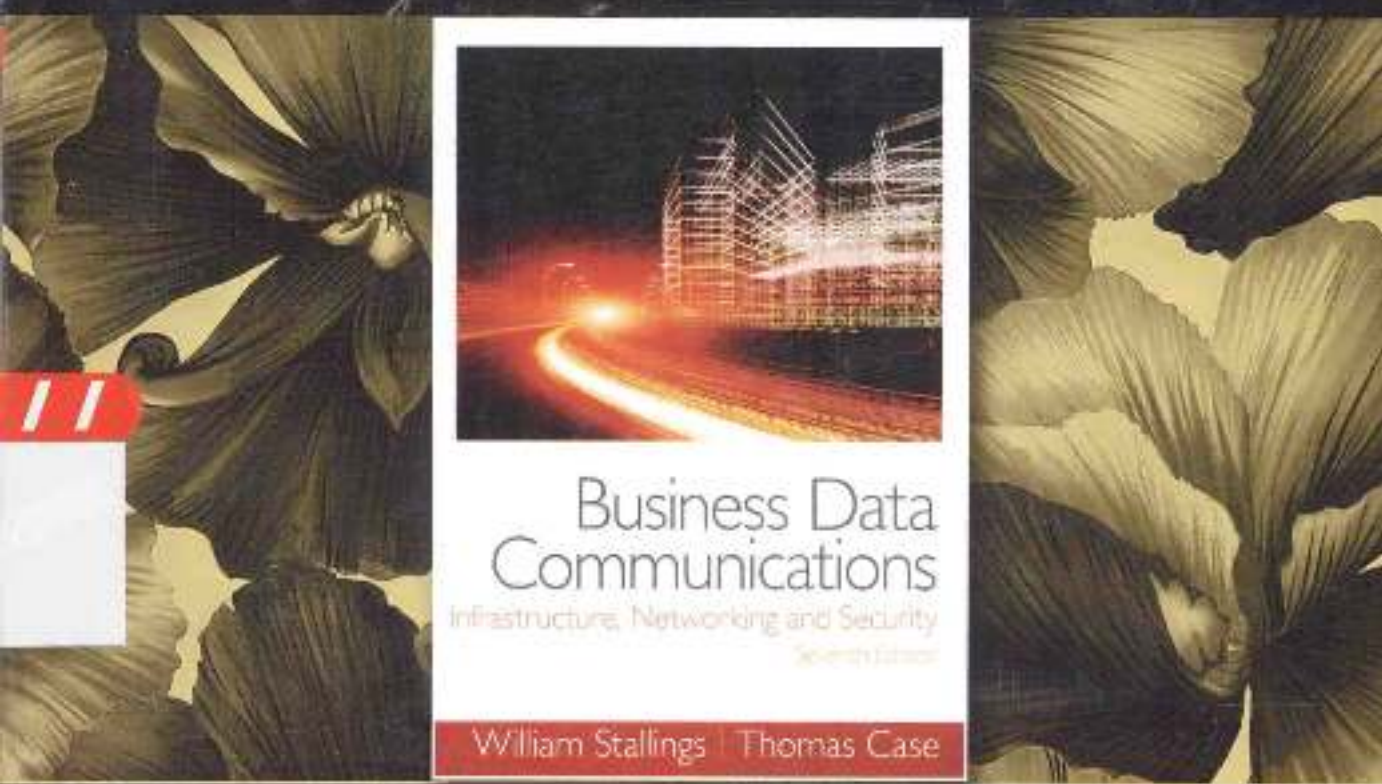
数据通信

基础设施、联网和安全

（美）William Stallings Thomas Case 著 陈秀真 等译

Business Data Communications

Infrastructure, Networking and Security Seventh Edition



机械工业出版社
China Machine Press

数据通信 基础设施、联网和安全 原书第7版

Business Data Communications Infrastructure, Networking and Security Seventh Edition

传播技术的演进不断推动着信息传播方式的革新。20世纪50年代，随着计算机技术的广泛普及与通信技术的发展，数据通信应运而生。数据通信是计算机技术和通信技术二者相结合产生的一种新的通信方式，它实现了计算机与计算机之间、计算机与终端之间的信息传递。数据通信技术不断影响和改变人类的生活，而对于企业运作而言，网络和数据通信更是起着至关重要的作用。本书从实际业务角度出发，采用案例教学方法，详细介绍了应用于事务领域的数据通信和计算机网络的基本知识、规律、应用的技术和发展的方向。本书可作为高等院校信息通信相关专业本科生和研究生的教材，也可供IT专业人士参考。

本书从六个部分详细讲解了业务领域的数据通信，分别是需求、数据通信、因特网及分布式应用、局域网、广域网和管理问题。从第6版出版以来，数据通信领域在不断发展，本书致力于捕捉这些变化，并保持内容覆盖的广泛全面。许多旧材料被修订，并添加了新的内容。每章都收录了关键术语、复习题、练习题、进一步阅读的建议以及重要网站列表供读者参考。另外，书中还包括大量的专业术语、常用缩略词列表和参考文献列表，并为教师提供了一个测试题库。

作者简介



William Stallings 拥有美国麻省理工学院计算机科学博士学位，现任教于澳大利亚新南威尔士大学国防学院（塔培拉）信息技术与电子工程系。William博士在计算机网络和计算机体系结构方面成就卓著。他6次荣获由美国教材与大学作者协会颁发的“年度最佳计算机科学与工程教材”奖。作品包括《操作系统——精髓与设计原理》、《计算机组成与体系结构》、《数据与计算机通信》和《密码学与网络安全：原理与实践》等。



Thomas Case 是佐治亚南方大学的信息系统系教授和主任。1981年，他在佐治亚大学完成博士学业后加入佐治亚南方学院。Thomas博士曾在专业协会担任多个领导职务，他是南部协会信息系统（SAIS）的创始人之一。他撰写了3本计算机网络和管理信息系统的教科书并发表30余篇期刊文章，在他的职业生涯中获得无数殊荣。

PEARSON

PEARSON

www.pearson.com

投稿热线：(010) 88379604
客服热线：(010) 88378991 88361066
购书热线：(010) 68326294 88379649 68995259

华章网站：www.hzbook.com
网上书店：www.china-pub.com
数字阅读：www.hzmedia.com.cn

上架指导：计算机网络

ISBN 978-7-111-45379-6

9 787111 453796 >

定价：99.00元

计 算 机 科 学 丛

原书第7版

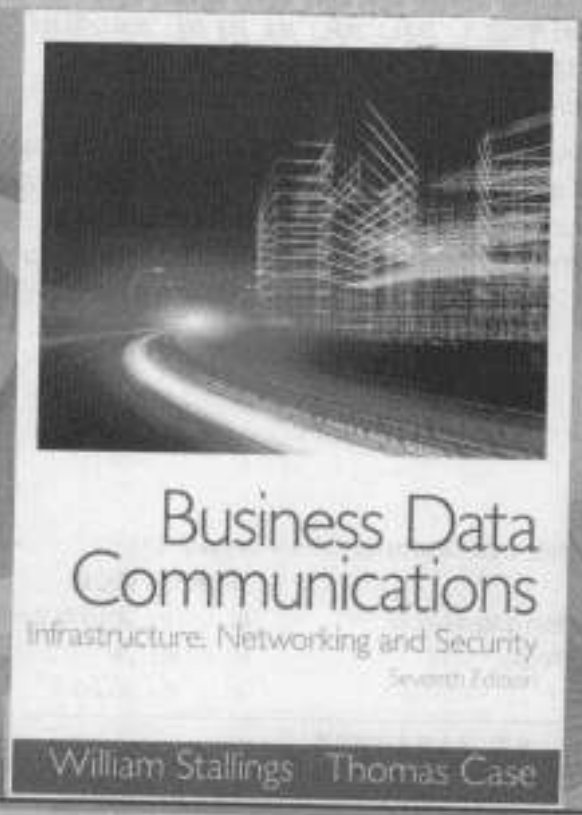
数据通信

基础设施、联网和安全

（美）William Stallings Thomas Case 著 陈秀真 等译

Business Data Communications

Infrastructure, Networking and Security Seventh Edition



机械工业出版社

图书在版编目（CIP）数据

数据通信：基础设施、联网和安全（原书第7版）/（美）斯托林斯（Stallings, W.），（美）凯斯（Case, T.）著；陈秀真等译．—北京：机械工业出版社，2015.2
（计算机科学丛书）
书名原文：Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

ISBN 978-7-111-45379-6

I. 数… II. ①斯… ②凯… ③陈… III. 数据通信 IV. TN919

中国版本图书馆CIP数据核字（2014）第276920号

本书版权登记号：图字：01-2013-0210

Authorized translation from the English language edition, entitled *Business Data Communications : Infrastructure, Networking and Security, Seventh Edition*, 9780133023893 by William Stallings, Thomas Case, published by Pearson Education, Inc., Copyright © 2013, 2009, 2005.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

Chinese Simplified language edition published by Pearson Education Asia Ltd., and China Machine Press Copyright © 2015.

本书中文简体字版由Pearson Education（培生教育出版集团）授权机械工业出版社在中华人民共和国境内（不包括中国台湾地区和中国香港、澳门特别行政区）独家出版发行。未经出版者书面许可，不得以任何方式抄袭、复制或节录本书中的任何部分。

本书封底贴有Pearson Education（培生教育出版集团）激光防伪标签，无标签者不得销售。

本书是著名计算机专业作家William Stallings的经典著作之一。分六个部分介绍了数据通信的相关知识。其中：第一部分定义商业环境中的信息通信需求。第二部分涉及信息通信的基本技术。第三部分概述因特网及其基本协议。第四部分探讨短距离网络的技术和架构。第五部分考察长距离网络上支持语音、数据和多媒体通信的内部机制和用户网络接口。第六部分涉及网络安全和网络管理两个关键领域。

本书可供通信或计算机、信息技术专业的本科生或研究生使用，同时也可供广大通信或计算机领域相关人员参考。

出版发行：机械工业出版社（北京市西城区百万庄大街22号　邮政编码：100037）
责任编辑：姚　蕾　　责任校对：董纪丽
印　　刷：北京市荣盛彩色印刷有限公司　　版　　次：2015年2月第1版第1次印刷
开　　本：185mm×260mm　1/16　　印　　张：28
书　　号：ISBN 978-7-111-45379-6　　定　　价：99.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

版权所有·侵权必究
封底无防伪标均为盗版
本书法律顾问：北京大成律师事务所　韩光/邹晓东

文艺复兴以来，源远流长的科学精神和逐步形成的学术规范，使西方国家在自然科学的各个领域取得了垄断性的优势；也正是这样的优势，使美国在信息技术发展的六十多年间名家辈出、独领风骚。在商业化的进程中，美国的产业界与教育界越来越紧密地结合，计算机学科中的许多泰山北斗同时身处科研和教学的最前线，由此而产生的经典科学著作，不仅擘划了研究的范畴，还揭示了学术的源变，既遵循学术规范，又自有学者个性，其价值并不会因年月的流逝而减退。

近年，在全球信息化大潮的推动下，我国的计算机产业发展迅猛，对专业人才的需求日益迫切。这对计算机教育界和出版界都既是机遇，也是挑战；而专业教材的建设在教育战略上显得举足轻重。在我国信息技术发展时间较短的现状下，美国等发达国家在其计算机科学发展的几十年间积淀和发展的经典教材仍有许多值得借鉴之处。因此，引进一批国外优秀计算机教材将对我国计算机教育事业的发展起到积极的推动作用，也是与世界接轨、建设真正的世界一流大学的必由之路。

机械工业出版社华章公司较早意识到“出版要为教育服务”。自 1998 年开始，我们就将工作重点放在了遴选、移译国外优秀教材上。经过多年的不懈努力，我们与 Pearson，McGraw-Hill，Elsevier，MIT，John Wiley & Sons，Cengage 等世界著名出版公司建立了良好的合作关系，从他们现有的数百种教材中甄选出 Andrew S. Tanenbaum，Bjarne Stroustrup，Brain W. Kernighan，Dennis Ritchie，Jim Gray，Afred V. Aho，John E.Hopcroft，Jeffrey D. Ullman，Abraham Silberschatz，William Stallings，Donald E. Knuth，John L. Hennessy，Larry L.Peterson 等大师名家的一批经典作品，以“计算机科学丛书”为总称出版，供读者学习、研究及珍藏。大理石纹理的封面，也正体现了这套丛书的品位和格调。

“计算机科学丛书”的出版工作得到了国内外学者的鼎力相助，国内的专家不仅提供了中肯的选题指导，还不辞劳苦地担任了翻译和审校的工作；而原书的作者也相当关注其作品在中国的传播，有的还专门为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近两百个品种，这些书籍在读者中树立了良好的口碑，并被许多高校采用为正式教材和参考书籍。其影印版“经典原版书库”作为姊妹篇也被越来越多实施双语教学的学校所采用。

权威的作者、经典的教材、一流的译者、严格的审校、精细的编辑，这些因素使我们的图书有了质量的保证。随着计算机科学与技术专业学科建设的不断完善和教材改革的逐渐深化，教育界对国外计算机教材的需求和应用都将步入一个新的阶段，我们的目标是尽善尽美，而反馈的意见正是我们达到这一终极目标的重要帮助。华章公司欢迎老师和读者对我们的工作提出建议或给予指正，我们的联系方法如下：

华章网站：www.hzbook.com
电子邮件：hzjsj@hzbook.com
联系电话：（010）88379604
联系地址：北京市西城区百万庄南街 1 号
邮政编码：100037



华章教育
华章科技图书出版中心

译者序

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

数据通信是以“数据”为业务的通信系统，是计算机和通信相结合的产物，它实现了计算机与计算机之间、计算机与终端之间的信息传递。由于业务需求的变化及通信技术的发展，数据通信经过了不同的发展历程，数据通信网交换技术历经了电路方式、分组方式、帧方式、信元方式等阶段。

本教材经过多次修订，最新的第 7 版吸纳了许多讲授这门课程的教授和工作在这个领域的专业人士的建议，涵盖了这个领域的改革与创新，包括云计算、大数据、第 4 代（4G）移动网络、VoIP 等。本教材紧密结合企业需求，涉及的数据类型有语音、数据、图像和视频，并提供了大量在线学习资源和案例。

高质量地完成一本技术著作的翻译工作具有很大的挑战性。对于一本书而言，译者的翻译可以称得上是书籍的第二次生命，“信”乃其骨，“达”乃其肉，“雅”则为其貌。作为一名专业研究人员，我很荣幸能够翻译 William Stallings 的这本著作。同时，在我的诚邀之下，姚立红老师和邱洋女士的“加盟”无疑又为本书的翻译添加了成功的砝码。姚立红老师具有丰富的计算机通信网络课程讲授经验，并长期从事该领域的科学研究工作。

本书的第 4 ~ 6 章及第 12 ~ 14 章由姚立红老师翻译，第 7 ~ 11 章及术语部分由邱洋女士翻译，我负责翻译除这些章之外的其余章以及附录、前言，并负责全书的技术审校。由于译者技术水平有限，疏漏在所难免，敬请广大读者指正。

感谢我的合作者姚立红老师和邱洋女士，你们的加入无异于雪中送炭。否则，我一个人无法在如此短的时间内翻译完这本厚达 600 页的巨著。

感谢机械工业出版社引进这本关于数据通信技术的杰作，它必然会在数据通信领域的众多书籍中占据重要的地位，并为推动国内的通信技术发展做出卓越贡献。

陈秀真

2013 年 11 月 15 日于上海

第 7 版新增内容

自从这本书的第 6 版出版以来，4 年内这个领域一直在不断地创新和改进。在这个新版本里，我们试图捕捉到这些变化，同时保持广泛而全面地覆盖整个领域。为了启动这本书的修订过程，许多讲授这门课程的教授和工作在这个领域的专业人士对本书的第 6 版本进行了全面的审查。因此，在许多地方，叙述已经很清晰并且贴切，插图也已经改进。值得注意的是，对本版中的章节顺序进行了调整，详情请参阅第 0 章的论述。

除了教学方法以及用户易懂性方面的进一步改进之外，全书整体上有了实质性的变化。修订了许多旧的材料，并添加一些新的材料。最值得注意的变化如下：

- **云计算**：在企业 IT 环境中，云计算已经成为一个重要且必不可少的工具。云计算的概念在整本书的许多章中都会涉及。
- **大数据**：新增一节来考察非常大的数据集（以 TB、PB 或 EB 计）的创建、操纵和管理以及这些数据集的存储设施。
- **第 4 代（4G）移动网络**：4G 网络继续在全球范围内扩展，新增了覆盖这一最新技术的小节。
- **动态主机配置协议（DHCP）**：DHCP 是一种广泛使用的协议，其使能动态 IP 地址分配。新增一节讨论了这个协议。
- **MPLS**：这个新版本包含一节专门讲述多协议标签交换（Multiprotocol Label Switching，MPLS），它在因特网以及其他基于 IP 的网络和电信网络上变得越来越重要。
- **以太网演进**：本书涵盖了以太网技术及其应用的新发展，包括有源以太网（PoE）和广域以太网（WAE）。
- **虚拟局域网（VLAN）**：VLAN 技术以及 IEEE 802.1Q 标准涵盖在本书里。
- **电子邮箱**：在第 10 章中的电子邮箱部分已经扩展到包括对标准因特网邮件架构的讨论。
- **多媒体应用**：第 10 章讨论这个新话题。
- **可接受的使用策略**：第 10 章添加了电子邮箱、Web 和因特网应用的可接受的使用策略。
- **因特网寻址**：因特网寻址部分已更新并扩展为包括 CIDR 和 IPv6 地址。
- **多播**：多播在商业环境中越来越重要，它也作为一个新的部分被添加到本书中。
- **VoIP**：IP 语音电话（VoIP）正日益取代传统的语音服务。第 15 章新增一节讨论了这个技术和服务。
- **存在信息和服务**：当前可用的存在服务支撑即时消息和 VoIP，以及协作服务的增加使用。在第 15 章中新增一节探讨存在信息和服务。

对于每一个新版本，既要保持一个合理的页面数量，同时也要增加新的材料，这是一个搏斗。在某种程度上，淘汰过时的材料和简练叙述可以实现这个目标。对于这个版本，普遍被很少关心的章节和附录都放在网上作为单独的 PDF 文件。这使得内容得以扩展，而书的尺寸和价格却没有相应地增加。

最后，本书作者的数量增加了一倍！我们的背景知识和经验在许多方面是互补的，我们有信心，合作出版的这本书比前的版本对企业学生更加有用。

背景

技术的发展和标准的广泛接受正在改变用信息来支持企业功能的方法。除了语音和数据（即文本和数字数据）的传统通信要求外，现在我们还需要处理形象化的图像和视频信息。在当今竞争激烈的国际环境下，这 4 种类型的信息（语音、数据、图像和视频），对任何企业的生存都是至关重要的。企业数据通信方面的书籍需要的不只是**数据通信**的处理，也需要业务环境中**信息通信**的处理。

对当今企业的功能运作而言，信息通信和计算机网络已经或多或少地起着至关重要的作用。而且，它们已成为机构的一个占很大比重并不断增长的成本。管理层及全体员工需要对信息通信有透彻的了解，以便能够评估需求；规划产品引进、服务和系统；管理系统和运维系统的技术人员。这种理解必须包括以下内容：

- **技术**：信息通信设施、网络系统和通信软件的基本技术。
- **架构**：为计算机和终端提供互连的硬件、软件和服务的组织方式。
- **应用**：信息通信和网络系统满足当今企业需求的方式。

方法

部分内容的目的是通过与企业环境以及企业管理人员和员工关注的具体问题直接联系的方式来展示信息通信的概念。为此，本书基于需求、组成部分和应用 3 个方面来进行诠释：

- **需求**：提供服务使企业能够利用信息的需求是数据和信息通信技术发展背后的动力。本书概述了该技术旨在解决的具体需求。需求和技术之间的这种联系对于推动内在的主题是必不可少的。
- **组成部分**：信息通信技术包括硬件、软件和支持分布式系统的通信服务。为使管理者在众多的替代品中做出明智的选择，了解这项技术是必不可少的。
- **应用**：管理人员和员工必须了解的不仅是技术，还有该技术被用来满足企业需求的应用方式。

这 3 个概念构成了这部分内容，它们提供了一种方法使学生了解在文中任何地方所讨论问题的来龙去脉，并且推动这些内容。因此，学生将真正理解企业信息通信。

贯穿全书的一个重要主题是标准的实质性作用。个人计算机和其他计算机系统的广泛应用意味着管理者将不可避免地面临整合不同供应商设备的需要。有效管理这一需求的唯一方法是通过标准。事实上，越来越多的供应商提供符合国际标准的产品和服务。本书讨论了一些关键的分组标准，这些标准用于塑造市场和定义决策者可用的选择。

目标读者

本书是面向现在有或预期会有信息技术管理责任的学生和专业人士。有些读者可能已经或计划负责管理公司的电信功能，并以此为他们的全职工作。但是，几乎所有的管理者和工作人员都需要对公司信息通信有一个基本的了解，以便有效地执行他们的任务。

新版本应该对寻求满足 ACM/AIS IS 2010 课程模式的大学特别有吸引力。本教材涵盖了 IS 2010.5 IT 基础设施推荐的所有主题，它是课程模式的核心课程之一。本书还涉及 IS 2010.3 企业架构课程推荐的多个主题，包括虚拟化、业务连续性、软件即服务（SaaS）、企业数据模

型、网络管理和新兴技术。

本书可以作为企业和信息管理专业学生的信息通信入门课程。本书不介绍任何数据通信的背景知识，但是介绍了数据处理的基本知识。通过重点介绍驱动网络基础设施演变的商业因素和用来度量网络性能的指标，本书内容将特别适合 MIS 和商科专业。学生将会更好地理解为什么企业投资于通信技术以及他们所期望的从这些投资中所获得的效益。

本书既适用于自学，也适合那些已经参与了企业信息通信的人作为教程和参考用书。

本书安排

全书共分六部分，在第 0 章分别进行描述：

- **需求**
- **数据通信**
- **因特网和分布式应用**
- **局域网**
- **广域网**
- **管理问题**

本书包括教师使用的许多功能，如使用了动画和众多的数字和表格，使问题讨论更加清晰。每章包括关键术语、复习题、练习题、进一步阅读的建议，以及建议的网站列表，书中还包括大量的专业术语、常用缩略词列表和参考文献列表。此外，还给教师提供了一个测试题库。

教师辅助材料

这部分内容的主要目标是使该书尽可能成为一个有效的教学工具，帮助学习这个令人兴奋且不断变化的课题。这个目标反映在书的结构和辅助支撑材料上。该书包括对教师有所帮助的以下补充材料：

- **答案手册**：所有章节后的复习题和练习题的答案。
- **项目手册**：下面列出的所有项目类别的任务建议。
- **PowerPoint 幻灯片**：涵盖所有章节的幻灯片集合，它们适用于讲学。
- **PDF 文件**：书中所有的图和表格的复制品。
- **题库**：每一章的练习题和针对这些练习题的答案文件。

所有这些辅助材料都可在本书的**教师资源中心**（IRC）得到，可以通过出版商的网站（www.pearsonhighered.com/stallings）或通过单击本书的配套网站（www.WilliamStallings.com/BusinessDataComm/）中的标记链接——提供给老师的 Pearson 资源（Pearson Resources for Instructors）。为了访问 IRC，请通过 pearsonhighered.com/educator/replocator/requestSalesRep.page 联系当地的 Pearson 销售代表或致电 Pearson 学院的服务电话 1-800-526-0485[㊀]。

配套网站 www.WilliamStallings.com/BusinessDataComm/（单击 Instructor Resources（讲师资源）链接），包括以下内容：

- 使用本书教授的其他课程的网站链接。
- 因特网邮件列表的注册信息，便于使用本书的教师能够相互之间或与作者交换信息、建议和问题。

㊀ 这里的地址为英文版教材的服务地址。中文版的相关辅助资料，请联系：service.cn@pearson.com; www.pearsonhighered.com/educator。——编辑注

在线案例研究

本书还包括许多案例研究。这些都不是“虚构的”或“玩具”案例，而是文献中报道的实际案例。通过每个案例，可以加强或拓展对本书中介绍的一些概念的理解。本书中，不仅创建了一些新的研究案例，而且还对以前版本的几个案例进行了更新。表 P-1 显示每个案例研究在本书的章节。

这些案例研究可在 www.pearsonhighered.com/stallings 中找到。

表 P-1 案例研究

案例	参考章节	案例中涉及的主要概念	其他相关章节
波音公司的统一通信	第 1 章	统一通信；融合的 IP 网络	第 17 章
核心信贷联盟	第 2 章	语音和数据网络；虚拟专用网（VPN）；云服务	第 3 章、第 9 章、第 10 章、第 12 章、第 13 章、第 19 章
万事达卡	第 3 章	数据仓库；大规模存储系统；“大数据”	第 2 章、第 19 章、第 21 章
宽带接入	第 6 章	宽带因特网接入选项；“有线社区”和国家；数字鸿沟	第 7 章、第 8 章、第 10 章、第 17 章
网络中立性	第 7 章	因特网流量增长；因特网的业务使用	第 9 章、第 10 章、第 11 章、第 17 章
雪佛龙公司	第 9 章	云计算；Web 服务	第 3 章、第 10 章、第 17 章、第 21 章
美国守护者人寿保险公司	第 10 章	电子商务、数字商务；门户网站	第 10 章、第 17 章、第 19 章
卡尔森公司	第 12 章	大规模存储系统；存储区域网络；后端网	第 3 章、第 13 章
St.Luke 保健系统	第 14 章	无线局域网；移动应用	第 17 章、第 19 章、第 21 章
纽伊斯酒店	第 17 章	卫星通信；无线广域网	第 2 章、第 3 章、第 21 章
云计算安全	第 19 章	云计算；网络安全；网络设计	第 3 章、第 9 章、第 10 章、第 17 章、第 21 章

项目和其他学生练习

对于许多教师，企业数据通信这门课程的一个重要组成部分就是项目或项目组，学生可以从中得到实践经验，以便加强对本书概念的理解。本书为这门课收录项目提供了空前的支持。教师资源中心不仅包括如何分配和构建项目，而且还包括为各种项目类型提供一套使用手册来附加各种特定任务，这些都特别写在本书中。教师可以在以下几个方面分配工作：

- **动画任务**：在下面的章节进行描述。
- **实际练习**：使用网络命令，使学生获得网络连接的经验。
- **Wireshark 项目**：Wireshark，以前称为 Ethereal，是一款协议分析软件，使学生能够学习协议的行为。
- **研究项目**：一系列研究任务指导学生研究特定的与因特网相关的课题并撰写报告。
- **安全案例研究**：一组现实世界中与安全相关的案例研究，包括学习目标、案例说明以及一系列案例讨论问题。
- **阅读 / 报告分配**：一系列的论文需要阅读并撰写阅读报告，当然需要在阅读清单上给出一些阅读建议。
- **写作任务**：一系列的书面作业需要完成，以促进对这些内容的学习。

这种多样化的项目和学生练习，让教师将本书作为丰富多样的学习过程的一个组成部分，这个量身定制的课程计划，可以满足教师和学生的具体需求。本书的详细信息请参阅附录 A。

动画

本书采用大量的动画，这些动画建立在以前版本提供的动画的基础上。动画为了解网络协议的复杂机制提供了一个强大的工具。共有 17 个基于 Web 的动画用来说明协议的行为。附录 A 提供了一个关键字动画映射，通过它可以在本书中找到所说明概念的适当位置。每个动画允许用户通过选择下一步的协议交换节点逐步查看协议的操作步骤。随着交换的继续，整个协议交换可以通过动画图表来说明。动画可以采用两种方式。在**被动模式**下，学生可以随机单击动画的任意节点的下一步来观看，这样给定的概念或原理可以很好地加以说明。在**主动模式**下，用户可以给定一组特定的步骤来调用和观看动画，或者被赋予一个特定的端点，并需要设计一个步骤序列来获得所需的结果。因此，动画可以作为学生作业的基础。教师补充说明对每个动画的一组分配及建议的解决方案，便于教师评估学生的工作。

可以在本书的配套网站单击旋转的地球获取动画。

学生资源

对于这个新的版本，学生可以大量从两个网站（原出版商网站和配套网站）上获得原始的辅助材料。**配套网站** http://www.WilliamStallings.com/BusinessDataComm/（单击 Student Resources（学生资源）链接）包括一个推荐阅读清单、按章节组织的相关链接列表和本书的勘误表。

致谢

这个新的版本得益于许多人的审查，他们慷慨地付出了他们的时间和专业知识。下面的人审阅了手稿：Khaled Kamel（Texas Southern University）、Barbara Holt（Northern Virginia Community College）、Kenny Jih（Middle Tennessee State University）、Asim Roy（Arizona State University）、Michael Chilton（Kansas State University）、Dave Croasdell（University of Nevada）、Brad Prince（University of West Georgia）、Bin Wang（Wright State University）、Zehai Zhou（University of Houston）、Glen Sagers（Illinois State University）、Manoel Oliveira（Florida International University）,Annette Kerwin（College of Dupage）,Angela Clark（University of South Alabama）、Mark Harris（University of South Carolina）、Randall Boyle（University of Utah）、Kuan Chen（Purdue University）、Jeffrey Kane（Nova Southeastern University）、Robert Folden（Texas A& M University）和 Brian West（University of Louisiana）。

还要感谢提供了一个或多个章节的详细技术审查人，他们是：Nikhil Bhargava（Hughes Systique，India）、John South（University of Dallas）、Paul Pot、Vance Shipley、Jennifer Jabbusch 和 Peter Tregunno。

在苏格兰斯特灵大学（University of Stirling）的 Larry Tan 开发了动画分配。美国印第安纳大学的 Michael Harris 首先开发了 Wireshark 的练习和用户指南。Dave Bremer，新西兰的奥塔哥理工学院的首席讲师，为近期发布的 Wireshark 更新了材料；他还开发了一个使用 Wireshark 的在线视频教程。

最后，我们感谢负责本书出版工作的很多人，所有人都一如既往很好地完成了工作。

这包括普伦蒂斯·霍尔出版社的员工，尤其是我们的编辑 Tracy Johnson、她的助手 Carole Snyder、产品主管 Kayla Smith-Tarbox、产品项目经理 Pat Brown。我们还感谢 Shiny Rajesh 公司的 Shiny Rajesh 和生产人员优秀、快速的工作。还感谢 Pearson 出版社的市场营销和销售人员，没有他们的努力，本书也不会在你的手中。

在线资源

网　站	位　置	描　述
相关 Web 网址	www.WilliamStallings.com/BusinessDataComm/	学生资源链接，提供给学生的有用链接和文档 教师资源链接，提供给教师的有用链接和文档
教师资源中心（Instructor Resource，IRC）	点击相关网址的教师链接 Pearson resources 或者点击 pearsonhighered.com/stallings 教师资源链接	解决方案手册、项目手册、幻灯片和其他有用文档
计算机科学学生资源网站	www.ComputerScienceStudent.com	为计算机科学学生提供的有用链接和文档

William Stallings 博士出版了 17 种超过 40 本有关计算机安全、计算机网络、计算机体系结构方面的书籍，（包括修订的版本）。他的作品已经出现在许多 ACM 和 IEEE 刊版物上，包括《Proceedings of the IEEE》和《ACM Computing Reviews》。他先后 10 次获得教材和著作家协会颁发的最佳计算机科学教材奖。

他在该领域超过 30 年，一直作为一些高科技公司的技术贡献者、技术管理者和执行者。他曾设计并实施了各种计算机和操作系统的基于 TCP/IP 和基于 OSI 协议栈，包括微机和大型机。作为一名顾问，他曾为政府机构、计算机和软件供应商以及主要用户给出网络软件和产品的设计、选择和使用方面的建议。

在 WilliamStallings.com/StudentSupport.html，他创建并维护 Computer Science Student Resource Site（计算机科学学生资源网站）。这个网站为计算机科学专业的学生和专业人士提供大量相关课题的文件和链接。他是《Cryptologia》的编委成员，Cryptologia 是一本致力于密码学各个方面的学术期刊。

Stallings 博士拥有麻省理工学院计算机科学博士学位和圣母大学电气工程学士学位。

Thomas Case 博士是佐治亚南方大学信息系统系教授和主任，他教本科生和研究生企业数据通信、网络设计、数字商务、企业资源规划（ERP）系统、人力资源信息系统（HRIS）、IT 管理、IT 战略等课程。1981 年，他在佐治亚大学完成博士学业后，加入佐治亚南方大学。

20 世纪 80 年代初，Case 博士教管理课程。20 世纪 80 年代中期，随着企业数据通信重要性的日益增加，他转向网络和信息系统教学。这样的背景帮助他的学生从企业的角度体会计算机网络的发展。

Case 博士曾在专业协会担任多个领导职务，他是信息系统南部协会（SAIS）的创始人之一。他是《Communications of the AIS》的副主编，并担任多个 IS 期刊的编委。在写作本书之前，他撰写了 3 本计算机网络和管理信息系统的教科书。他已发表 30 余篇期刊论文，并赢得了众多专业会议的最佳论文奖。

他在教育机构、金融机构、技术协会的咨询委员会任职，并积极参加 SAP 大学联盟和美洲多个 SAP 用户组分会。在他的职业生涯中，他已经获得了无数的荣誉，包括他所在大学的贡献卓越教学奖和卓越服务奖。

目 录

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

出版者的话
译者序
前 言
作者简介

第 0 章 读者和教师指南 …… 1
0.1 本书提纲 …… 1
0.2 主题顺序 …… 1
0.3 网络资源 …… 2
0.3.1 本书网站 …… 2
0.3.2 计算机科学专业学生资源网站 …… 2
0.3.3 其他网站 …… 2
0.4 有用的刊物 …… 2
第 1 章 引言 …… 4
1.1 信息和通信 …… 4
1.2 当今企业的数据通信和网络 …… 5
1.2.1 趋势 …… 5
1.2.2 企业驱动力 …… 7
1.3 融合和统一通信 …… 8
1.3.1 融合 …… 8
1.3.2 统一通信 …… 9
1.4 企业信息需求的本质 …… 13
1.5 信息传输 …… 14
1.5.1 传输和传输介质 …… 15
1.5.2 通信技术 …… 15
1.6 分布式数据处理 …… 15
1.7 因特网及分布式应用 …… 15
1.7.1 因特网 …… 16
1.7.2 TCP/IP 协议 …… 16
1.7.3 客户机 / 服务器架构、内部网、外部网和 SOA …… 16
1.7.4 分布式应用程序 …… 17
1.8 网络 …… 17
1.8.1 广域网 …… 18
1.8.2 局域网 …… 19
1.8.3 无线网络 …… 20
1.8.4 城域网 …… 20
1.8.5 配置示例 …… 20
1.9 管理问题 …… 21
1.9.1 网络安全 …… 21
1.9.2 网络管理 …… 22
1.10 标准 …… 23
1.11 关键术语、复习题和练习题 …… 24
附录 1A 数值单位的前缀 …… 25

第一部分 需求

第 2 章 业务信息 …… 28
2.1 音频 …… 29
2.2 数据 …… 31
2.3 图像 …… 33
2.3.1 图像表示 …… 34
2.3.2 图像和文档格式 …… 35
2.3.3 网络化含义 …… 35
2.4 视频 …… 36
2.4.1 数字视频 …… 37
2.4.2 网络化含义 …… 38
2.5 性能度量 …… 39
2.5.1 响应时间 …… 39
2.5.2 体验度量 …… 42
2.5.3 吞吐量 …… 43
2.6 总结 …… 45
2.7 关键术语、复习题和练习题 …… 45
第 3 章 分布式数据处理 …… 48
3.1 集中式与分布式数据处理 …… 49
3.1.1 集中式与分布式组织 …… 49
3.1.2 分布式数据处理的技术趋势 …… 52
3.1.3 管理与组织的考虑 …… 52
3.1.4 数据中心的发展 …… 55
3.1.5 客户机 / 服务器架构 …… 57
3.1.6 内部网与外部网 …… 58
3.1.7 Web 服务与云计算 …… 58
3.2 分布式数据处理的形式 …… 59

3.2.1 分布式应用 …… 60
3.2.2 其他形式的 DDP …… 61
3.3 分布式数据 …… 61
3.3.1 数据库管理系统 …… 62
3.3.2 集中式与分布式数据库 …… 63
3.3.3 复制型数据库 …… 63
3.3.4 分区数据库 …… 64
3.4 DDP 的网络含义 …… 66
3.5 大数据基础设施的考虑 …… 67
3.6 总结 …… 69
3.7 关键术语、复习题和练习题 …… 70

第二部分 数据通信

第 4 章 数据传输 …… 74
4.1 传递信息的信号 …… 74
4.1.1 电磁信号 …… 74
4.1.2 模拟信号 …… 80
4.1.3 数字信号 …… 82
4.2 传输损伤和信道容量 …… 82
4.2.1 有导向的传输介质 …… 83
4.2.2 无导向的传输介质 …… 86
4.2.3 信道容量 …… 87
4.3 总结 …… 89
4.4 关键术语、复习题和练习题 …… 89
第 5 章 数据通信基础 …… 91
5.1 模拟数据通信和数字数据通信 …… 91
5.2 数据编码技术 …… 95
5.2.1 数字信息的模拟编码 …… 95
5.2.2 模拟信息的数字编码 …… 100
5.2.3 数字数据的数字编码 …… 101
5.2.4 模拟信息的模拟编码 …… 103
5.3 异步传输和同步传输 …… 104
5.3.1 异步传输 …… 104
5.3.2 同步传输 …… 106
5.4 差错检测 …… 106
5.4.1 差错控制的必要性 …… 106
5.4.2 奇偶校验 …… 107
5.4.3 循环冗余校验 …… 107
5.5 总结 …… 109
5.6 关键术语、复习题和练习题 …… 110
第 6 章 数据链路控制及复用 …… 113
6.1 流控制和差错控制 …… 114
6.1.1 流控制 …… 114
6.1.2 差错控制 …… 115
6.2 链路复用的动机 …… 115
6.3 频分复用 …… 116
6.3.1 波分复用 …… 118
6.3.2 ADSL …… 119
6.4 同步时分复用 …… 121
6.4.1 TDM 机制 …… 121
6.4.2 数字传输系统 …… 122
6.4.3 T-1 设施 …… 124
6.4.4 Sonet/SDH …… 124
6.4.5 蜂窝和无绳电话系统 …… 126
6.5 总结 …… 128
6.6 关键术语、复习题和练习题 …… 128
附录 6A 高级数据链路控制协议 …… 130

第三部分 因特网和分布式应用

第 7 章 因特网 …… 136
7.1 因特网结构 …… 136
7.1.1 商业和因特网 …… 136
7.1.2 因特网起源 …… 136
7.1.3 分组交换的使用 …… 137
7.1.4 关键要素 …… 138
7.1.5 万维网 …… 139
7.1.6 因特网架构 …… 140
7.2 域 …… 142
7.2.1 因特网的名称和地址 …… 142
7.2.2 域名系统 …… 144
7.3 动态主机配置协议 …… 147
7.4 总结 …… 150
7.5 关键术语、复习题和练习题 …… 150
第 8 章 TCP/IP …… 153
8.1 一个简单的协议结构 …… 153
8.1.1 对协议结构的需求 …… 153
8.1.2 一种三层协议结构模型 …… 155
8.1.3 标准化协议结构 …… 158
8.2 TCP/IP 协议体系 …… 158
8.2.1 TCP/IP 层 …… 159

8.2.2 TCP/IP 操作 …… 159
8.2.3 TCP 和 UDP …… 161
8.2.4 IP 和 IPv6 …… 161
8.2.5 TCP/IP 应用 …… 162
8.2.6 协议接口 …… 163
8.3 网络互联 …… 163
8.3.1 路由器 …… 164
8.3.2 网络互联的示例 …… 165
8.4 虚拟专网和 IP 安全 …… 167
8.4.1 IPSec …… 168
8.4.2 IPSec 的应用 …… 168
8.4.3 IPSec 的益处 …… 169
8.4.4 IPSec 的功能 …… 169
8.5 总结 …… 171
8.6 关键术语、复习题和练习题 …… 171
附录 8A TCP、UDP 和 IP 详细内容 …… 174
附录 8B 简单文件传输协议 …… 177
第 9 章 客户 / 服务器、内部网及云计算 …… 181
9.1 客户 / 服务器计算的增长 …… 181
9.2 客户 / 服务器应用 …… 183
9.2.1 数据库应用 …… 184
9.2.2 客户 / 服务器应用的类别 …… 185
9.2.3 三层客户 / 服务器结构 …… 186
9.3 中间件 …… 187
9.3.1 中间件结构 …… 187
9.3.2 消息传递 …… 188
9.3.3 远程过程调用 …… 190
9.3.4 面向对象机制 …… 191
9.4 内部网 …… 192
9.4.1 Web 内容 …… 192
9.4.2 Web/ 数据库应用 …… 193
9.4.3 内部 Web 和传统的客户 / 服务器 …… 194
9.5 外部网 …… 194
9.6 面向服务架构 …… 195
9.7 云计算 …… 198
9.7.1 云计算元素 …… 198
9.7.2 云计算参考结构 …… 200
9.8 总结 …… 202
9.9 关键术语、复习题和练习题 …… 203
第 10 章 基于因特网的应用 …… 206
10.1 电子邮件 …… 206
10.1.1 互联网邮件架构 …… 207
10.1.2 简单邮件传输协议 …… 209
10.1.3 多用途因特网邮件扩展 …… 211
10.1.4 POP 和 IMAP …… 213
10.2 网页访问和 HTTP …… 213
10.2.1 HTTP 概述 …… 214
10.2.2 消息 …… 216
10.3 网络安全 …… 217
10.3.1 网络通信安全防护 …… 218
10.3.2 安全套接层 …… 218
10.3.3 HTTPS …… 219
10.4 多媒体应用 …… 219
10.4.1 媒体类型 …… 219
10.4.2 多媒体应用 …… 220
10.4.3 多媒体技术 …… 221
10.5 可接受使用策略 …… 221
10.5.1 动机 …… 221
10.5.2 策略 …… 222
10.5.3 策略制定指南 …… 222
10.6 总结 …… 224
10.7 关键术语、复习题和练习题 …… 225
第 11 章 因特网操作 …… 227
11.1 因特网寻址 …… 227
11.1.1 IPv4 地址 …… 227
11.1.2 IPv6 地址 …… 230
11.2 因特网路由协议 …… 231
11.2.1 自治系统 …… 231
11.2.2 边界网关协议 …… 232
11.2.3 开放最短路径优先协议 …… 233
11.3 IP 多播 …… 234
11.3.1 多播传送 …… 234
11.3.2 多播路由协议 …… 236
11.4 服务质量 …… 236
11.4.1 高速 LAN 的出现 …… 237
11.4.2 企业广域网的需求 …… 237
11.4.3 因特网流量 …… 238
11.5 差异化服务 …… 239
11.5.1 服务 …… 239

11.5.2 DS 域 …… 240
11.5.3 差异化服务的配置与运行 …… 241
11.6 服务等级协议 …… 242
11.7 IP 性能度量 …… 243
11.8 总结 …… 246
11.9 关键术语、复习题和练习题 …… 247

第四部分 局域网

第 12 章 局域网体系结构和基础设施 … 250
12.1 背景 …… 250
12.1.1 个人计算机 LAN …… 250
12.1.2 后端网络和存储区域网络 …… 251
12.1.3 高速办公网络 …… 253
12.1.4 骨干 LAN …… 253
12.1.5 工厂 LAN …… 253
12.2 LAN 配置 …… 254
12.2.1 分层 LAN …… 254
12.2.2 演进场景 …… 255
12.3 有导向传输介质 …… 255
12.3.1 双绞线 …… 257
12.3.2 同轴电缆 …… 260
12.3.3 光纤 …… 260
12.3.4 结构化布线 …… 261
12.4 LAN 协议结构 …… 263
12.4.1 IEEE 802 参考模型 …… 263
12.4.2 逻辑链路控制 …… 264
12.4.3 介质接入控制 …… 265
12.5 总结 …… 267
12.6 关键术语、复习题和练习题 …… 268
附录 12A 分贝和信号强度 …… 270
第 13 章 以太网、交换机和虚拟 LAN …… 272
13.1 传统以太网 …… 272
13.1.1 总线型拓扑 LAN …… 273
13.1.2 介质接入控制 …… 273
13.1.3 MAC 帧 …… 275
13.1.4 IEEE 802.3 10Mbps 介质选择 …… 276
13.2 网桥、集线器和交换机 …… 276
13.2.1 网桥 …… 276
13.2.2 集线器 …… 278
13.2.3 第二层交换机 …… 280
13.2.4 第三层交换机 …… 281
13.3 高速以太网 …… 282
13.3.1 快速以太网 …… 282
13.3.2 千兆以太网 …… 283
13.3.3 10Gbps 以太网 …… 284
13.3.4 100Gbps 以太网 …… 286
13.4 虚拟局域网 …… 287
13.4.1 虚拟局域网的使用 …… 288
13.4.2 表明 VLAN 成员身份 …… 290
13.4.3 IEEE 802.1Q VLAN 标准 …… 290
13.5 以太网供电 …… 290
13.6 总结 …… 292
13.7 关键术语、复习题和练习题 …… 293
第 14 章 无线局域网 …… 295
14.1 概述 …… 295
14.1.1 无线 LAN 应用 …… 295
14.1.2 无线 LAN 需求 …… 297
14.1.3 无线 LAN 技术 …… 297
14.2 Wi-Fi 体系结构和服务 …… 298
14.2.1 IEEE 802.11 体系结构 …… 298
14.2.2 IEEE 802.11 服务 …… 300
14.3 IEEE 802.11 MAC 层和物理层标准 — 301
14.3.1 IEEE 802.11 介质接入控制 …… 301
14.3.2 IEEE 802.11 物理层 …… 302
14.4 千兆 WLAN …… 305
14.4.1 千兆 Wi-Fi …… 305
14.4.2 Li-Fi …… 306
14.5 IEEE 802.11 安全考虑 …… 306
14.5.1 访问和私密性服务 …… 306
14.5.2 无线 LAN 安全标准 …… 307
14.6 总结 …… 308
14.7 关键术语、复习题和练习题 …… 309

第五部分 广域网

第 15 章 广域网技术和协议 …… 312
15.1 交换技术 …… 312
15.2 电路交换网络 …… 313
15.2.1 基本操作 …… 313
15.2.2 控制信令 …… 315

15.3 分组交换网络 …… 316
15.3.1 基本操作 …… 317
15.3.2 交换技术 …… 318
15.4 传统广域网实例 …… 319
15.4.1 语音广域网 …… 320
15.4.2 数据广域网 …… 321
15.5 IP 语音 …… 323
15.5.1 VoIP 信令 …… 323
15.5.2 VoIP 处理 …… 324
15.5.3 VoIP 上下文 …… 325
15.6 存在 …… 326
15.6.1 存在服务结构 …… 326
15.6.2 存在信息 …… 327
15.7 总结 …… 327
15.8 关键术语、复习题和练习题 …… 328
第 16 章 广域网服务 …… 330
16.1 广域联网方案 …… 330
16.1.1 WAN 服务 …… 330
16.1.2 WAN 结构的演化 …… 332
16.2 帧中继 …… 334
16.2.1 背景 …… 334
16.2.2 帧中继协议结构 …… 335
16.2.3 用户数据传输 …… 336
16.2.4 帧中继呼叫控制 …… 337
16.2.5 拥塞控制 …… 338
16.3 异步传输模式 …… 339
16.3.1 虚通道和虚路径 …… 339
16.3.2 ATM 信元 …… 341
16.3.3 ATM 服务种类 …… 342
16.4 多协议标签交换 …… 344
16.4.1 MPLS 操作 …… 344
16.4.2 MPLS VPN …… 346
16.5 广域以太网 …… 347
16.6 总结 …… 349
16.7 关键术语、复习题和练习题 …… 349
第 17 章 无线广域网 …… 352
17.1 蜂窝无线网络 …… 352
17.1.1 蜂窝网络组织 …… 353
17.1.2 蜂窝系统运行 …… 356
17.2 多址接入 …… 358
17.2.1 码分多址（CDMA） …… 358
17.2.2 使用哪种接入方法 …… 359
17.3 第 3 代无线通信 …… 360
17.3.1 无线应用协议 …… 361
17.3.2 WAP 编程模型 …… 362
17.3.3 无线标记语言 …… 362
17.3.4 微浏览器 …… 362
17.3.5 无线电话应用 …… 363
17.3.6 配置样例 …… 363
17.4 第 4 代无线通信 …… 363
17.4.1 第 4 代网络需求 …… 363
17.4.2 正交频分多址（OFDMA） …… 365
17.4.3 4G 网络演化 …… 365
17.5 卫星通信 …… 365
17.5.1 卫星轨道 …… 365
17.5.2 卫星网络配置 …… 368
17.5.3 应用 …… 368
17.6 总结 …… 370
17.7 关键术语、复习题和练习题 …… 371

第六部分 管理问题

第 18 章 计算机和网络安全威胁 …… 374
18.1 计算机安全概念 …… 374
18.2 威胁、攻击和资产 …… 375
18.2.1 威胁和攻击 …… 375
18.2.2 威胁和资产 …… 377
18.3 入侵者 …… 379
18.3.1 入侵者的行为模式 …… 380
18.3.2 入侵技术 …… 382
18.4 恶意软件概述 …… 382
18.4.1 后门 …… 383
18.4.2 逻辑炸弹 …… 383
18.4.3 木马 …… 383
18.4.4 移动代码 …… 384
18.4.5 多重威胁的恶意软件 …… 384
18.5 病毒、蠕虫、僵尸程序和垃圾邮件 …… 385
18.5.1 病毒 …… 385
18.5.2 蠕虫 …… 389

18.5.3 僵尸程序 …… 390
18.5.4 垃圾（大量不请自来的）邮件 … 392
18.6 键盘记录器、钓鱼和间谍软件 …… 392
18.6.1 凭据盗窃、键盘记录器和间谍软件 …… 392
18.6.2 钓鱼和身份盗窃 …… 393
18.6.3 侦查和间谍活动 …… 393
18.7 计算机安全趋势 …… 394
18.8 总结 …… 395
18.9 关键术语、复习题和练习题 …… 396
第 19 章 计算机和网络安全技术 …… 399
19.1 虚拟专用网和 IPSec …… 399
19.1.1 IPSec 的功能 …… 399
19.1.2 传输模式和隧道模式 …… 399
19.1.3 密钥管理 …… 400
19.1.4 IPSec 和 VPN …… 401
19.2 SSL 和 TLS …… 401
19.2.1 SSL 架构 …… 401
19.2.2 SSL 记录协议 …… 402
19.2.3 握手协议 …… 402
19.3 Wi-Fi 网络安全接入 …… 403
19.4 入侵检测 …… 404
19.4.1 基本原理 …… 405
19.4.2 基于主机的入侵检测技术 …… 406
19.5 防火墙 …… 406
19.5.1 防火墙特性 …… 407
19.5.2 防火墙类型 …… 408
19.6 恶意软件防御 …… 410
19.6.1 防御病毒的方法 …… 410
19.6.2 蠕虫防御 …… 412
19.6.3 Bot 防御 …… 412
19.7 总结 …… 413
19.8 关键术语、复习题和练习题 …… 414
附录 A 企业业务数据通信教学项目 —— 417
术语表 …… 420
参考文献 …… 425

读者和教师指南

本书及其配套网站涵盖了大量的内容。在本章中，我们对本书进行概述。

0.1 本书提纲

在引导性的章节之后，本书分为6部分：

第一部分需求：定义商业环境中的信息通信需求。讨论各种信息的使用方式、互联的需求以及网络设施。对分布式数据处理的性质和作用进行考察是这部分的重点。

第二部分数据通信：涉及信息通信的基本技术。重点是数字通信技术，因为所有这些与信息通信相关的产品和服务迅速取代了模拟技术。主要议题包括传输介质、数据链路控制协议和多路复用。

第三部分因特网和分布式应用：概述因特网及其基本协议，其中基本协议是因特网的基础，也是解决服务质量（QoS）这一关键问题的基础。本部分还涉及需要信息通信设施和网络的特定企业应用。本部分介绍关键的应用程序，如电子邮件和万维网，还包含对客户机/服务器和内部网的讨论。

第四部分局域网：探讨短距离网络的技术和架构。传输介质、拓扑和介质访问控制协议是一个局域网（LAN）设计的主要组成部分，我们对其进行了探索，同时，对具体标准化的LAN系统进行了考察。

第五部分广域网：考察在长距离网络上支持语音、数据和多媒体通信的内部机制和用户网络接口。对传统的分组交换和电路交换技术，以及最近的多协议标签交换（MPLS）和无线广域网（WAN）进行了考察。

第六部分管理问题：涉及网络安全和网络管理两个关键领域。

本书配套网站的许多在线附录涵盖与本书相关的其他主题。

0.2 主题顺序

本书从第6版开始重新组合，更加紧密地与学生的需求相匹配。企业/信息系统/信息技术（business/IS/IT）的学生希望看到企业需求背景下的技术材料，以及通信和网络技术支持期望的业务功能方式。因此，本书从定义信息通信企业的要求开始。首先，检查信息的类型和它们的效用，然后考察基本的通信技术。这两部分为讨论能够满足这些需求的应用程序以及支持这些应用程序的因特网作用做好准备。然后，我们考察形成分布式应用和网络基础设施的通信网络，包括局域网和广域网。最后，对网络安全和网络管理方面的问题进行讨论。希望这种安排可以使本书的内容更容易理解，同时提供一个结构使得企业方向的读者觉得更加自然。

有些读者和教师更喜欢自底向上的方法。通过这种方法，每个部件建立在前面部分内容的基础上，因此读者总是可以清晰地了解下层如何支撑某一给定的功能层。因此，本书是采

用模块化的组织方式。读完第一部分后，其他部分可以有许多不同的阅读次序。

0.3　网络资源

网络上有许多支持本书的资源，并帮助读者跟上这一领域的发展。

0.3.1　本书网站

我们维护本书的**配套网站**：http://williamstallings.com/BusinessDataComm。对于学生来说，这个网站包含相关链接列表、章节组织和本书的勘误表。对于老师，本网站提供本书的教授课程网页的链接。

还有一个受控访问的**优质内容网址**，它提供丰富的辅助材料，包括额外的网络章节、额外的在线附录、一组课后问题与解决方案、这一领域的一些重要论文的副本，以及一些其他证明文件。查看本书前面的卡片可以获得访问信息。

最后，教师的附加材料，包括解决方案手册和项目手册，在本书的**教师资源中心**（IRC）可以获得。访问信息详见前言。

0.3.2　计算机科学专业学生资源网站

Bill Stallings 也维护**计算机科学学生资源网站**：ComputerScienceStudent.com。这个网站的目的是为计算机科学专业的学生和专业人士提供文件、信息和相关链接。链接和文件分为6大类：

- **数学**：包括基本的数学复习、排队分析入门教程、一些系统的初级教程，以及众多数学网站的链接。
- **操作方法**：为解决作业问题、撰写技术报告和准备技术演示提供建议和指导。
- **研究资源**：具有收藏价值的重要论文、技术报告和书目的链接。
- **杂项**：多种其他有用的文件和链接。
- **计算机科学事业**：对那些考虑在计算机科学方面工作的人有用的链接和文件。
- **幽默和其他娱乐活动**：偶尔将你的注意力从你的工作转移。

0.3.3　其他网站

许多网站提供与本书主题相关的信息。配套网站提供到这些网站的链接，并且这些网址按章节进行组织。

0.4　有用的刊物

本书作为学习企业数据通信领域的教程，也可以作为某个特定课题的参考。然而，这一领域快速变化，没有一本书可以单独适用很长时间。如果你真正对这个领域感兴趣，你可能需要花费一些时间，跟上新的发展，而做到这一点的最好办法是通过阅读一些相关的期刊。可以推荐的出版物清单非常多，这里包括的是一个小的、可供选择的刊物列表，它们一定不会辜负你所花的时间。所有这些出版物都有网址（见表0-1）。

表 0-1 有用期刊

书 名	网 站
Network World	这是本列表最好的网站。它包含组织好的论文目录存档，还包含当前的最新消息、各种论文涵盖的技术课题和供应商信息的网站链接
Network Computing	来自可用杂志的文章，以及指向广告商的指针。该网站还包含为终端用户网络设计提供实用技巧的超文本网络设计手册
Performance Edge Journal	所有期刊的存档
Telecommunications	过去期刊的文章和产品信息，以及工业贸易的国际列表。该产品列表包含产品的简要描述和从供应商获得的产品信息。利用关键字，可以有效地搜索文章和产品列表
IT Professional	包含关于信息技术的专业资源和链接
ACM Networker	包含杂志文章的在线副本

《Network Word》，是获取信息通信产品和服务的工业与市场的一个极好信息源。它的覆盖范围很彻底，并包括对产品和服务的买家指南。每星期，它有一篇或多篇有深度的文章，触及某个单一的领域，如网络管理。它关注的是管理，而不是技术方向，它还提供产品的比较。《Network Computing》，不只专注于网络产品，也有一些技术文章。这本杂志提供了一个很好的跟踪新产品的发布、获取产品种类比较分析的途径。

《Performance Edge Journal》，专注于网络性能管理问题，这是一个免费的在线杂志。《Telecommunications》，是月刊，包含行业相关技术的文章。该杂志着重远距离网络的课题，如电话、电信和监管问题。

《IT Professional》，由 IEEE（电气和电子工程师协会）出版，目标用户是企业信息系统的开发者和管理者。该杂志很好地阐述技术方面的问题，以帮助建立和管理今天的信息系统，并提供在未来几年内企业发展的趋势预告。ACM（美国计算机协会）发布的《Networker》，是另一个很好的企业信息系统开发者和管理者的信息来源，但是相比较而言它更注重网络和数据通信。

第 1 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

引　言

学习目标

通过本章的学习，读者应该能够：

- 确定企业网络的演变和企业驱动的主要力量。
- 书中讨论的主要议题的大体框架。
- 阐述企业规划中因特网和无线通信的重要性。
- 了解数据通信和网络中标准的核心作用。

本章首先简要介绍数据通信和网络在企业中的作用，然后简单讨论本书的各个部分。

1.1　信息和通信

计算机和通信技术编织成企业架构，并将继续成为全球市场的关键竞争力。信息的产生、存储和移动是管理企业业务处理的核心，也是确保长期的盈利能力和竞争力的核心。因此，企业必须时刻提高警觉，确保使用信息和通信技术（ICT）最好地满足信息管理需求。

毫无疑问，我们依赖计算机、通信设备以及连接它们的服务。世界各地的员工所使用的计算机、终端和移动设备数以 10 亿计，连通性、完整性和信息的易于获取对员工和企业合作伙伴之间的有效沟通是必不可少的。许多企业都吸收了社交媒体（例如，Twitter 和 Facebook），以提高通信和业务处理能力。所以，信息通信技术对企业的成功起着根本性作用，它正在成为新的商业模式和战略基础。最明显的是，企业已经采用云计算来提供有竞争力的产品，如基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。

随着企业不断面临全球竞争、兼并、收购的挑战，传统的部门壁垒和头重脚轻的管理金字塔的组织结构正在让位给新的扁平化、更精简、更敏捷、适应创新的企业结构。企业和其合作伙伴（供应商、客户、服务供应商等）之间的传统界限由于紧密联系在一起的伙伴关系正在变得模糊，使得很难确定一个组织过程的结束和另一个过程的开始。与此同时，网络技术促进商业伙伴之间协调活动所需的信息流，使得跨组织的企业流程更加透明。今天，网络技术确实不仅仅支持一个企业的内部运营，它也服务于供应链管理（SCM）、客户关系管理（CRM）以及使企业网络发生转变的其他企业范围的应用程序。

通信技术在许多方面为企业提供帮助。例如，良好的网络可以更容易地管理地理上分散的运营点，还有助于企业向员工及时传递信息，包括在必要时随时随地访问移动设备。也许最重要的是，良好的网络提高企业内部及相互之间的沟通和信息管理，也使企业合作伙伴在提高效率、客户服务、灵活性和创新等方面更加紧密联系在一起。当我们考察本书中的技术和应用时，我们将看到很多信息通信技术促使企业成功的方法。

1.2 当今企业的数据通信和网络

有效、高效的数据通信和网络设施对任何企业都是至关重要的。在本节中，我们首先看看在规划和管理这些设施方面，企业管理者所面临的不断增加的挑战。接下来，我们介绍企业驱动力的概念，它引导企业发展一个整体的数据通信和网络计划。

1.2.1 趋势

3种不同的力量一直推动着数据通信和网络设施的架构及其进化：流量的增长、新服务的发展和技术的进步。

几十年来，无论是本地（建筑物或企业的校园内）和长途的通信**流量**都一直稳定高速增长。网络流量不再局限于语音和数据，也日益包括图像和视频。越来越重视网络服务、远程访问、网上交易和社交网络，而且这种趋势很可能会继续。因此，企业管理者不断受到压力，要以符合成本效益的方式增加通信容量。

随着企业越来越依赖于信息技术，企业用户希望享受的**服务**范围正在扩大。例如，由于企业用户的智能手机和平板电脑推动移动网络数据量的增长，所以移动宽带流量也呈现爆炸式增长。此外，移动用户越来越要求高品质的服务，以支持他们的高分辨率摄像头手机、喜欢的视频流和高端音频。为了跟上消费者和企业用户所产生的迅速增长的流量需求，移动运营商必须对大容量的网络和传输设施持续投资。反过来，高速网络的增长提供了更具竞争力的价格，促进移动应用和服务的扩大。因此，服务和流量容量的增长齐头并进。图1-1给出了一些基于信息的服务和支持它们所需的数据传输速率的例子[ELSA02]。

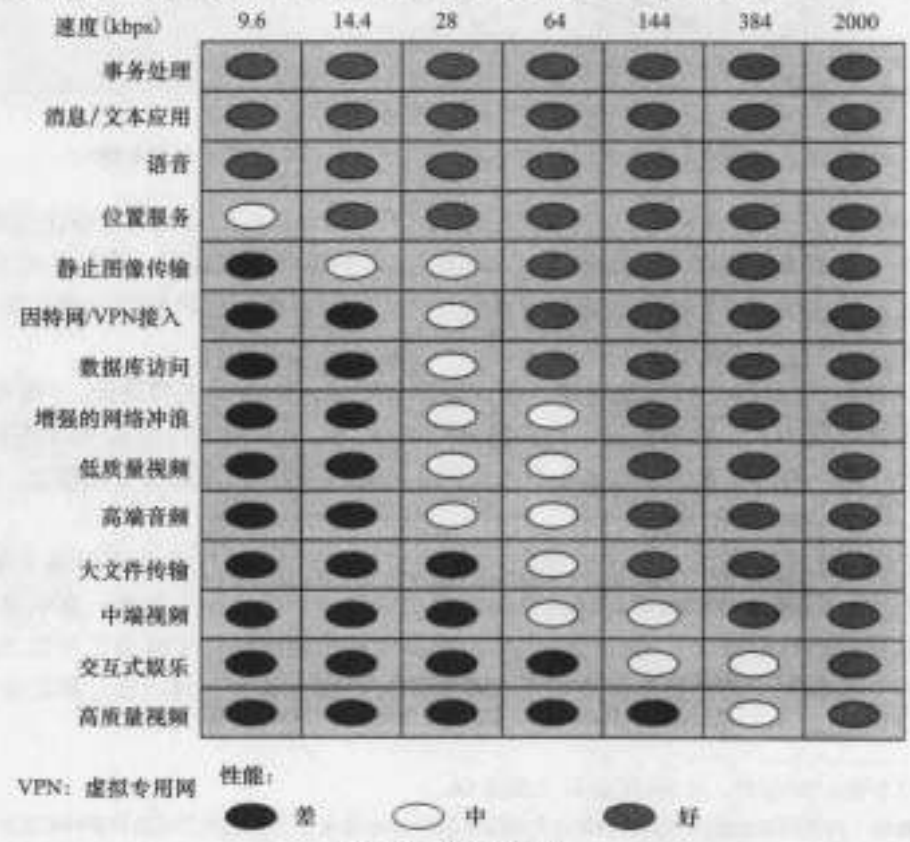


图1-1 服务与吞吐率

最后，技术的发展趋势使得因特网能够支持不断增长的流量容量，并提供更广泛的服务支持。4大技术趋势尤为显著，企业信息技术管理者需要理解。4个技术发展趋势如下：

1）在计算和通信方面更快、更便宜的服务趋势在持续。在计算方面，这意味着更强大的计算机和集群能够支持更多的应用，如多媒体应用。在通信方面，越来越多地使用光纤和高速无线传输促使价格下降和容量增加。例如，对于长途电信和数据网络链接，密集波分复用（DWDM）技术使通信流量以每秒数兆兆位的速率通过光纤电缆。对于局域网（LAN），许多企业现在有千兆以太网或10Gbps以太骨干网[⊖]。此外，对下一代100Gpbs以太网的需求日益迫切。40Gbps和100Gbps以太网产品已经开始投放市场，并且一些权威人士预测到2015年以太网速度将达到兆兆位。图1-2显示了以太网的需求趋势。

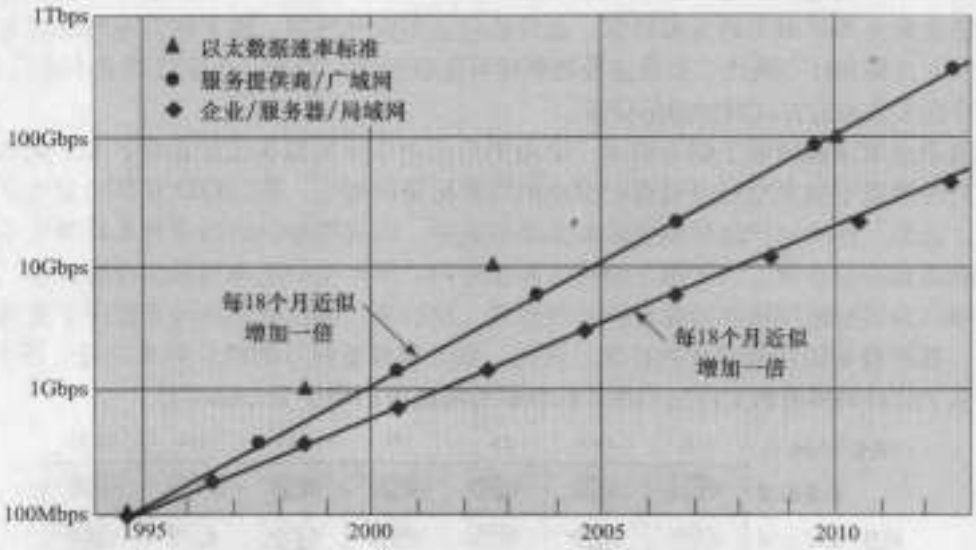


图1-2　相比于当前以太网数据速率标准，以太网带宽过去和预期增长

2）今天的网络比以往任何时候都更“智能”，其中两个方面的智能是值得注意的。首先，今天的网络可以提供不同级别的服务质量（QoS），其中包括最大延迟、最低吞吐量等规格，以确保高品质的应用程序和服务的支持。其次，今天的网络提供各种网络管理和安全等领域的定制服务。

3）因特网、Web以及相关的应用已经成为企业和个人网络的主要特征。“所有基于IP”的转移在继续，这为ICT经理创造了许多机遇和挑战。除了利用因特网和Web连接到客户、供应商和合作伙伴外，企业已实施了企业内部网和外部网[⊜]的形式来隔离专用信息，阻止不必要的访问。

4）对ICT管理者来说，移动性是最前沿的技术。流行的消费电子设备（如iPhone、Droid和iPad），已成为企业网络的演进及其使用的驱动力。虽然几十年来一直朝移动性的趋势发展，然而移动性的爆炸式增长已经发生，它从实体企业的框框中将员工解放出来。终端和办公台式计算机上支持的传统企业应用现在经常在移动设备上交付。云计算正在被所有主

⊖ 对于数值前缀的解释，如tera和giga，见附录1A。

⊜ 简略地，内部网在企业内部隔离的设施使用因特网和Web技术；外部网把公司的内部网拓展到因特网，有选择地允许客户、供应商和移动工作人员访问公司的专有数据和应用，具体讨论见第6章。

要企业的软件销售商接受，包括 SAP、甲骨文和微软，这确保了移动性进一步创新将迅速到来。业内专家预测，到 2015 年移动设备将成为占主导地位的企业计算平台，增强随时随地使用企业信息资源和服务的能力将是未来十年的主要趋势。

1.2.2 企业驱动力

前一小节中所讨论的趋势，促进了企业网络和通信基础设施的发展，这与基于信息的企业运营紧密相关。企业网络管理和运行依赖于组织特定的关键信息，如名称、网络地址、安全功能、终端用户分组、优先级指定、邮箱和应用程序属性等。随着企业网络容量和功能的增加，这些信息可以统一放在企业信息库中，以确保所有企业应用的信息是正确的、一致的和可用的。

企业网络和通信基础设施的性质取决于所支持的企业流程的应用程序。[MIL004] 列出了 4 个主要应用领域，它们持续推动当今企业网络的设计和构成。这些都在图 1-3 中进行说明。橙色商业服务（Orange Business Services）[ORAN12] 确定了 5 个额外的应用领域，它们将形成未来企业网络的设计和基础设施。这些应用领域及其企业驱动因素、典型用途的例子在表 1-1 中进行了总结。



IP=因特网协议
电子商务=基于企业网络移动、全局访问的企业活动

图 1-3 应用驱动型企业网络

表 1-1 新兴的企业网络应用

应 用	典型应用 / 例子	企业理念
远程监控	视频会议	减少旅行费用 减少能源成本 减少碳消耗 增加经营生产力 增加销售成功率 增加销售周期时间
视频广播和在线学习	销售 训练 监督	更好地通知用户 增加员工能力 部署公司 YouTube 频道 减少训练相关的旅行开支

（续）

应 用	典型应用 / 例子	企业理念
丰富的视频合作	视频聊天 统一通信 公司间合作	更好的管理虚拟团队 改善企业流程的执行 增加个人生产率 加强团队交流 增加公司对社交媒体的使用
智能对象	机器对机器通信 物联网 车辆追踪	成熟的 RFID 应用 降低传感器、驱动器和调制解调器的成本 更好的监视和解决纷争设备 向 IPv6 迁移
云计算	随时随地接入应用、服务器和存储器 软件即服务（SaaS） 平台即服务（PaaS）	计算按需扩展 第三方数据中心 增加各种基于云的服务和按需解决方案 减小内部部署网络的开销 增强移动性的支持 增加灵活性和可变性

1.3 融合和统一通信

本节介绍了两个相关的概念：融合和统一通信，它们是企业数据通信和网络设施需求的重要决定因素。

1.3.1 融合

融合是指以前不同的电话和信息技术以及市场的合并。我们从企业通信三层模型的角度来看融合：

- **应用**：这是一个企业的最终用户看到的东西。融合是将通信应用（如语音通话、语音邮件、电子邮件和即时消息）与企业应用（如工作组协作、客户关系管理和后台功能）相结合。通过融合，应用提供丰富的特征，包括以无缝、有组织、增值的方式提供语音、数据和视频。其中一个例子是多媒体信息，使用户能够采用单一的界面访问各种来源的消息（如办公室语音邮件、电子邮件、短信和移动语音信箱）。
- **企业服务**：在这个层面上，管理者从服务的角度处理信息网络，以确保用户可以充分利用他们所使用的应用程序。例如，网络管理员需要确保合适的隐私保护机制和认证服务是到位的，以支持基于融合的应用。它们也能够跟踪用户的位置，为移动工作者提供远程打印服务和网络存储设备。企业网络管理服务也包括为不同用户、组群和应用程序以及 QoS 条款建立协作环境。
- **基础设施**：网络和通信基础设施由通信链路、局域网、广域网和企业可用的因特网连接而成。越来越多的企业网络基础设施还承载包括私人或公共的云连接，用以连接到承载大容量数据存储和网络服务的数据中心。在这个层次上融合的一个关键方面是用过最初设计来承载数据流量的网络具有传输语音、图像和视频的能力。基础设施融合也发生在设计为承载语音流量的网络。例如，视频、图像、文本和数据通过手机网络将数据定期传送给智能手机用户。

图 1-4 显示了企业通信三层模型的主要属性。简单来说，融合涉及将企业的语音、视频

和图像流量移动到一个单一的网络基础设施。这往往涉及将不同的语音和数据网络集成到一个单一的网络基础设施，并扩大基础设施以支持移动用户。这种融合的基础是使用因特网协议（IP）的基于分组的传输机制。使用IP数据包来传送各种通信流量，有时也称为“一切基于IP”，使底层的基础设施能够给企业用户提供广泛的有用应用。

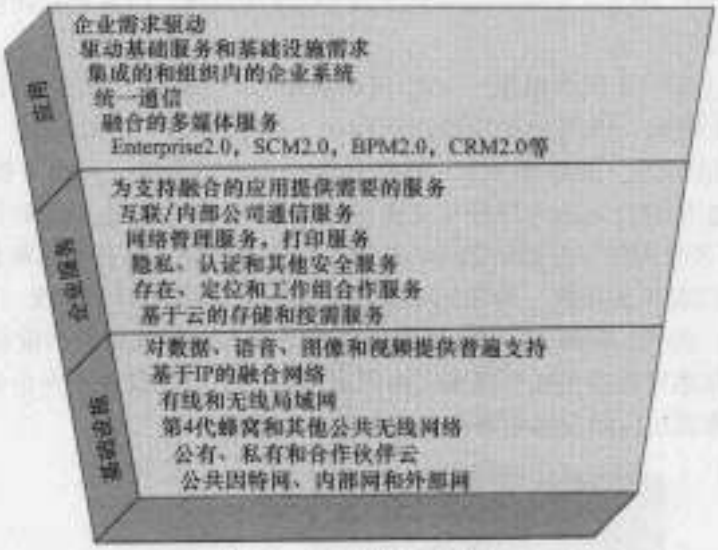


图1-4 业务驱动的融合

融合带来很多好处，包括简化网络管理，提高效率，提高应用层面的灵活性。例如，一个融合的网络基础设施提供了一个可预测的平台，在这个平台上构建结合视频、数据和语音的新应用。这使得它更容易为开发人员创造新的混搭（mashup）以及其他增值业务应用和服务。IP网络融合的3个关键好处概述如下：

- **节省成本**：融合网络可以使网络管理、维护和运营成本显著减少。传统网络融合到一个单一的IP网络能够更好地利用现有资源，实现集中的容量规划、资产管理和策略管理。
- **有效性**：在融合的环境中，不论用户身在何处，都有可能为他们提供极大的灵活性。IP融合允许企业创造更具移动性的劳动力。移动工作人员可以使用虚拟专用网络（VPN）远程访问公司网络上的企业应用和通信服务。通过分离企业流量和其他因特网流量，VPN有助于维护企业网络的安全性。
- **转型**：因为融合的IP网络是可修改的、互操作的，所以在无需安装新的基础设施的前提下，通过技术改进就可以很容易地使融合的IP网络适应新的功能和特性。融合还使企业广泛采用全球标准和最佳实践，从而提供更好的数据、增强的实时决策、改进的企业关键流程和操作的执行。最终增强了灵活性和响应能力，它们是企业创新的关键成分。

这些引人注目的商业利益正激励企业投资于融合网络基础设施。然而，企业敏锐地意识到融合的缺点：一个单一的网络意味着单点故障。鉴于它们对信息和通信技术的依赖，今天的融合企业网络基础设施通常包括冗余组件和备份系统，以提高网络的灵活性并减少网络中断带来的严重损失。

1.3.2 统一通信

与网络融合有关的概念是统一通信（UC）。鉴于企业网络融合的重点是将传统的不同的

语音、视频和数据通信网络融合到一个共同的基础设施上，UC 专注于整合实时通信服务来优化企业流程。与融合企业网络一样，因特网协议是 UC 系统的基石。UC 的关键要素包括：

1）UC 系统通常提供一个统一的用户界面和跨多个设备和媒体的一致的用户体验。

2）UC 将非实时服务和企业流程应用融入实时通信服务中。

基于 [LAZA07]，图 1-5 显示了一个典型的 UC 架构组件，以及它们如何彼此连接。这种架构的关键要素如下：

- **实时通信（RTC）的仪表板**：RTC 仪表板是 UC 架构的一个关键组成部分。这是给 UC 用户提供统一的用户接口的通信设备。理想情况下，无论用户目前正在使用的是什么通信装置，他都有一个一致的界面，无论是手机、无线平板电脑、台式机系统，还是连接到公司的专用分支交换机（PBX）的办公室电话。在图 1-5 中，可以看到 RTC 仪表板提供实时通信服务的访问，如即时消息、语音和视频会议以及交互式白板。RTC 仪表板还在统一的视图中提供非实时业务的访问，如统一消息（电子邮件、语音邮件、传真、SMS）。RTC 仪表板包括同事和合作伙伴的当前信息，使用户可以知道哪些同事可以通信或可以加入协同通信会话。RTC 仪表板在企业中已经成为必需品，它需要高层次的沟通和协作，以支持企业流程。

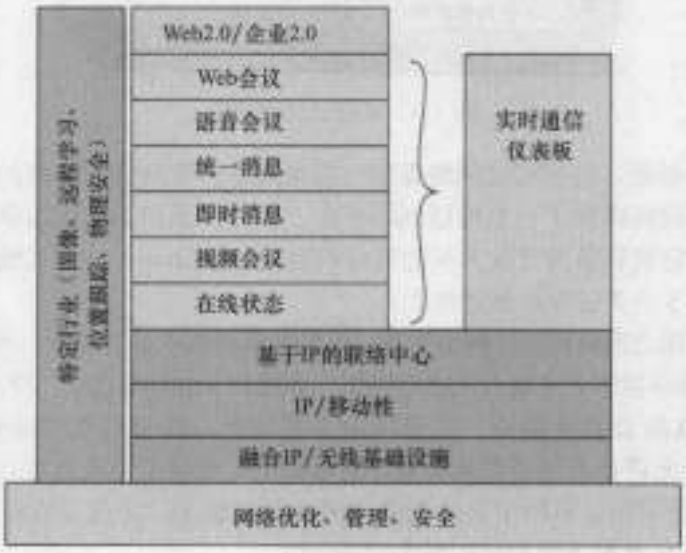


图 1-5　统一通信架构的要素

- **Web 会议**：指实时会议或演讲，参加者通过移动设备或 Web，也可以通过因特网或公司内部网参加会议或演讲。网络会议通常包括通过网络连接的交互式白板（IWB）进行数据共享。
- **音频会议**：也称为电话会议，音频会议是指参与者连接在一起，进行实时音频传输和接收的会议。参与者可利用固定电话、移动电话，或配备麦克风和扬声器的计算机中的“软件电话”。
- **统一消息**：统一消息系统为来自多个源的消息提供共同的资料库。它允许用户从一台计算机、电话或移动设备上取回保存的电子邮件、语音邮件和传真消息。计算机用户可以从他们的统一消息收件箱中选择并播放语音信箱的录音。电话用户既可以获取语音邮件，也可以听到将电子邮件文本翻译出来的语音消息。它可以保存、答复、归

档、分类或转发任何类型的消息。统一的信息系统减轻企业用户对多个语音信箱的监控，确保公室电话和手机接收到的语音邮件消息被保存到同一个邮箱中。由于 UC，用户可以使用任何设备在任何时间内从统一消息邮箱取回电子邮件或语音邮件。

- **即时消息（IM）**：两个或两个以上的参与者之间实时的文本消息传递。IM 类似于网上聊天，因为它是基于文本的实时双向交换。IM 不同于聊天的地方在于，IM 客户端使用联系人（或好友）列表，以方便相识用户之间的连接，而网上聊天可以包括匿名用户之间的文本信息的交流。
- **视频会议（VTC）**：视频会议允许用户在两个或两个以上的位置，同时通过双向视频和音频交互传输。UC 系统使用户能够通过台式计算机、智能手机和移动设备参与视频会议。
- **在线状态**：能够实时确定某人所处的位置、他喜欢的联系方式，甚至他目前正在做什么的能力。即时消息可以在同事试图联系之前显示他的状态。它一度被认为只是即时通信（如“在线”或“忙碌”）的一种底层技术，但现在已扩大到包括显示是否在办公室、是否在移动通话中、是否登录到计算机、是否进行视频通话或会议、离开办公室用餐或度假等状态。由于许多商业原因（如快速响应客户的紧急情况），同事的地理位置正越来越普遍地的成为当前状态信息的重要元素。企业已经接受了当前状态信息，因为它有利于更高效、有效的沟通。它有助于消除“电话标签”或撰写和发送电子邮件确认的效率低下的问题，这些问题可以通过电话或简短的会议更迅速解决。
- **基于 IP 的联络中心**：是指使用基于 IP 的统一通信，以提高客户联络中心的功能和性能。统一通信基础设施利用上线提醒技术，使客户和企业内部员工可以快速连接到所需的专家或技术支持人员。此外，该技术支持移动性，使呼叫中心的工作人员不必在一个特定的办公室或待在一个特定的地方。最后，统一通信基础设施使呼叫中心员工可以快速访问其他员工和信息资源，包括数据、视频、图像和音频资源。
- **IP/ 移动性**：指通过 IP 网络基础设施，向经常使用手机的企业人员传递信息或收集信息。在典型的企业中，多达 30% 的员工每周在他们的工作中使用某种形式的远程访问技术。行业研究员指出，移动员工和远程办公的人数不断增加，到 2016 年美国的员工将超过 60 万。来自 [SENS02] 的图 1-6 显示了移动员工典型的使用模型。



在办公桌旁	在现场某处	移动中
90%	10%	
70%	30%	
100%（家）		
10%	10%	80%
30%		70%
25%	25%	50%

图 1-6 移动员工的 3 个主要模型

- **融合 IP/ 无线基础设施**：统一网络和通信基站使用 IP 数据包支持语音、数据和视频传输，并可以扩展到局域网和广域无线通信领域。使用 UC 的移动设备能够在通信会话

中切换 Wi-Fi 和蜂窝系统。例如，UC 用户可以通过连接到家用 Wi-Fi 的智能手机接收同事的呼叫，同时在驾驶时通过蜂窝网络连接时继续交谈，最后在办公室利用企业的 Wi-Fi 网络中断呼叫连接。两个切换（hand-off）（家庭 Wi-Fi 到蜂窝、蜂窝到办公室的 Wi-Fi）将无缝、透明地发生，而且电话不会被挂断。

统一通信的重要性不仅体现在集成了通信信道，同时它还提供了一种集成通信功能和企业应用的方法。表 1-2 总结了统一通信的主要优点。通常企业使用 UC 可以实现的三大类好处为：

表 1-2　统一通信的企业利益

层　次	企业利益
个人工作者	增强与同事间的交流 增加对客户和伙伴的响应能力 改善生产率 远程 / 移动访问统一通信系统 改善对所有信息形式的访问（语音邮件、电子邮件和文本信息）
工作团队	增进团队成员之间的合作 实时的观点交换和问题解决 方便安排团队会议日程 提升将 IM 会话传递给会议通话的能力 更好地管理 / 协调工作组活动 改善项目管理 改善事件管理
公司	通过通信驱动的业务流程（CEBP）改善业务执行流程 改善企业流程的连续性 提供到 ERP、CMP、SCM 和其他企业系统的统一通信接口的能力 削减电话开销 增强用户服务 增加客户保有度 减少销售周期时间 由于更快的销售周期导致收入增加

- **个人生产率的提高**：在线状态信息帮助员工找到对方，并选择最有效的实时通信方式。更少的时间浪费在呼叫多个号码找到同事或检查多个与工作相关的语音信箱上。贵宾联系人的电话可以同时路由到 UC 用户的所有电话设备（办公电话、软件电话、智能手机、家庭电话），以确保更快地响应客户、合作伙伴和同事。利用移动的在线状态信息功能，可以派遣地理上最接近的员工解决问题。
- **工作组的性能提升**：UC 系统支持团队成员之间的实时协作，这有利于提高工作组的性能。例如，工作团队需要解决一个问题时，使用在线状态信息来加快识别拥有合适技能的可用的人。利用桌面视频会议（VTC）和交互式白板增强会议性能、自动化的路由或升级通信功能的企业规则也有助于提高工作组的性能。
- **企业级的过程改进**：IP 融合使 UC 集成到企业范围和部门级应用、企业流程和工作流中。与客户、供应商和企业合作伙伴之间的 UC 使能的增强通信正在重新定义客户关系管理（CRM）、供应链管理（SCM）以及其他企业级应用的最佳实践，正在改变企业网络成员之间的关系。通信支持的企业流程（CEBP）正在推动多个行业的竞争，包括金融服务行业、医疗保健业和零售业。

越来越多的企业正在迁移到统一通信，业内专家估计，到 2015 年，多达 50 万的美国员

工将成为UC用户。这种增长有点儿令人惊讶，因为目前没有任何国际公认的标准，用于确保正在由Avaya、Cisco、ShoreTel、Siemens和其他主要UC厂商出售的系统之间的互操作性。基于IP的会话发起协议（SIP）的演变引发的新UC功能似乎是克服传统企业规避的专用解决方案，至少在现在是这样的。企业从实现统一通信和融合网络基础设施获得的利益推动企业通信模型三个层次的变革（如图1-4所示），似乎注定在可预见的将来需要这样做。

1.4 企业信息需求的本质

企业的生存和发展靠信息：企业内部信息；与供应商、客户和监管机构交换的信息。而且，信息要求是一致的、可访问的和能交付到正确的位置。在第一部分的第2章和第3章中，我们考虑企业网络传输的四个主要类型的信息（语音、数据、图像和视频）和支持分布式数据存储和处理所需的基础设施。

在本书中，术语**语音通信**主要是指与电话相关的通信。在企业和其他组织的通信中，电话交谈仍然是最常见的形式。几十年来，电话一直是一个基本的企业工具，对于某些组织它将仍然是主要的通信技术。各种以计算机为基础的服务（包括语音邮件和程控电话交换系统），使得电话通信得到增强。语音信箱提供发送、转发和非同步语音留言回复的能力，它部署在各种规模的企业中。程控电话交换系统（包括内部数字私有分支交换以及当地电话公司所提供的中央交换机系统），也取得了进展。这些新系统提供了广泛的功能，包括来电显示、呼叫转移、占线呼叫等待、最低成本长途电话路由以及各种计费和审计功能。最近，基于VoIP协议的因特网技术和语音的合并已经导致内部部署和提供充分的因特网支持的托管式IP-PBX产品。

术语**数据通信**被频繁用来指除语音之外的任何形式的信息传递。有时将这个术语限制为以文本（如报告、备忘录和其他文件）和数字数据（如审计文件）形式的信息。科技的快速发展已经给想要有效地利用数据通信的企业管理者带来了新的挑战。在这一章的后面部分，我们简要地描述传输技术、网络和通信软件的重大变化，它们带来新的和更加强大的企业工具，也使管理者选择这些可以相互替代的产品更具挑战性。

图像通信是在办公环境下一个越来越重要的组成部分。这项技术最有名的例子是传真（fax）。传真机仍然是不同地方之间发送文件最常用的方法，尤其是在长距离情况下。利用传真，任何内容（包括文本、图形、签名和照片）的文件可在几秒内通过电话网络传送到目的地。传真功能往往和联网的办公复印机及与小型办公室/家庭办公室（SOHO）网络中常见的多功能打印机捆绑在一起。在较大的组织中，复印机通常连接到以太网或IP网络，使传真图像通过因特网发送到其他地方。此外，图像常附着或嵌入在电子邮件消息中。因此，各种图像，包括工程和设计规范、混合文档（文本、图形、签名等）、演示材料等，正在被企业用户在办公室内部和不同办公室之间快速地传送。图像通信也影响移动通信。今天的智能手机经常使用户能够拍摄并通过移动网络发送高清数字图像。企业用户产生的图像给企业捕获、传输和存储带来挑战，这将产生一个高容量网络的需求，它是新的网络技术发展的驱动力之一。

视频通信在办公环境中也变得越来越重要。传统上，这种技术已用来作为娱乐节目的单向传送系统。现在，大容量传输链路和网络的可用性使得视频会议和视频电话会议已经成为一个重要的商业应用程序。视频会议在提高效率和生产力方面是一个强大的工具，它有助于

我们节省在旅游、食品和住宿上的时间和金钱。视频会议的发展（包括高分辨率的网真系统的出现），使地理上分散的用户可以进行实时的规划会议、合同谈判和项目审查，就像他们出现在同一个房间里一样。而且，正如前面提到的，统一通信系统支持视频会议，使企业用户使用台式计算机和智能手机参与会议。基于IP的视频（和基于IP的电视（-TVoIP））也被企业用于提供高清晰度的直播和按需员工培训计划、视频标识系统、安全和监控以及客户的销售演示。它也被更广泛地用于远程病人监测和诊断等医疗保健。因特网协议电视（IP Protocol Television，IPTV）正被越来越多地用于教育和餐饮业，并有望成为一种非常流行的在消费者家中为数字娱乐系统提供电视内容的方式。

所有这些信息通信形式在今天的企业中都发挥了关键作用。第2章更主要介绍这4种类型信息的商业使用以及必须满足的通信要求，确保企业网络有足够的传输速率。

1.5　信息传输

任何企业网络基础设施的基本构建模块都是传输线。关于信息是如何编码和传输的大部分技术细节，企业管理者并不感兴趣。相反，企业管理者更关心网络是否具有所需要的处理语音、数据、图像和视频流量的能力，关心网络是否具有可接受的可靠性和低廉的价格。不过，企业管理者必须明白传输技术的某些方面，并提出正确的问题，继而做出明智的决定。

企业网络用户的基本选择之一是传输介质。对于内部网络，这种选择一般完全由企业决定。对于连接地域分散的企业地点，选择一般由可用的因特网服务提供商（ISP）或长途电话运营商决定。在其他情况下，传输媒体的演变正在改变企业网络介质的组合。例如，光纤传输和无线传输介质正在驱动数据通信传输的演变。

光纤通信电路日益增长的可用性使得信道容量几乎成为免费的资源。自20世纪80年代初，光纤传输系统市场的增长是史无前例的。在过去的10年中，光纤传输的成本已经下降了不止一个数量级，而系统的容量几乎以相同的速度迅速增长。在美国境内几乎所有的长途电话通信主干网和高速因特网链路几乎都由光纤电缆组成。由于其高容量和安全的特征（光纤难以被窃听），它正在越来越多地用于办公楼和局域网，传输不断增长的企业负载。光缆的广泛使用也带动了通信交换技术和网络管理架构的进步。

第二种使用量日益增多的介质——无线传输，是由于通用个人通信和通信接入普及的发展趋势造成的。通用个人通信是指一个人可以随时随地，最理想的是在全球范围的，以单独账户使用任何通信系统的能力。通用接入通信是指在各种环境中使用某人喜欢的计算设备连接信息服务的能力（例如，有一台笔记本电脑、智能手机或平板电脑，在大街、飞机、公共汽车或火车上将与其在办公室的工作能力同样出色）。今天，这两个概念都由于企业的推动来支持移动性。无线LAN已成为企业网络和SOHO网络的常见组成部分，具有无线功能的智能手机和平板电脑正迅速成为主流商务用户的通信设备。正如我们前面UC的讨论中提到的，移动性有潜力在所有企业层面发挥更高的性能，不管是个人、工作组，还是企业范围，这为无线技术的进一步商业投资提供了令人信服的理由。

尽管容量的增长和传输介质成本的下降，但在企业网中传输语音、数据、图像和视频流量依旧继续占据了大多数企业通信预算的主要部分。为了节省企业开支，企业管理者需要了解如何最有效地使用企业网络基础设施中的传输介质。更有效地利用通信电路的两种主要方法是多路复用和压缩。多路复用是指许多设备共享一条传输线路的能力。共享安排使得传输

链路的费用分摊给许多用户，并有助于确保用于传输链路的总容量。正如其名称所示，压缩涉及将数据转换成更小的形式，这样小容量的、更便宜的传输线路可以用于计算设备之间的传输。这两种技术（多路复用和压缩）可以单独或组合使用，确保企业网络内传输介质的有效使用，并且许多类型的通信设备都支持这两种技术。知道什么时候以及在哪里使用这些技术可以帮助企业最大限度地减少其数据通信费用。

在第二部分的第5章和第6章讨论与信息传输相关的关键问题和技术。第6章描述今天所使用的主要的多路复用类型：频分复用、时分复用和波分复用，以及使用这些技术的电路类型。

1.5.1 传输和传输介质

信息可以通过将其转换成电磁信号并通过一定的介质传输，如双绞线电缆。最常用的传输介质是双绞线电缆、同轴电缆、光纤电缆、地面和卫星微波。可以达到的数据传输速率和传输误码率依赖于信号性质和媒介类型。第4章讨论电磁信号的重要特性。第12、14和17章讨论当今企业网络中使用的各种传输介质。

1.5.2 通信技术

通过传输介质传输信息，不是简单地将信号插入传输介质中，而是必须确定信息编码转换成电磁信号的技术。有多种方法可以实现编码，不同的选择会影响它的性能和可靠性。此外，成功发送信息需要发送者和接收者之间的高度合作。必须使用一些手段来控制信息流，并恢复它在传输过程中丢失或损坏的数据。这些功能可以通过数据链路控制协议实现。这些重要的数据传输问题将在第5章和第6章进行讨论。

1.6 分布式数据处理

多年来，数据处理设备的成本稳步下降，而这类设备的能力不断增强，导致中小型规模的计算机在企业内不断增加。桌面系统是商务办公的标准装备，这些都与通信机柜里的数据通信设备、服务器、存储技术、服务器机房或数据中心相互连接，这里数据中心依赖于组织规模和企业网络的复杂性。局域网是任何企业网络的基本构建模块，这些模块都支持分布式数据处理的配置，控制着今天的组织计算蓝图。由于无线局域网的实施，分布式数据处理能力已扩展到许多企业内部。支持移动工作者的动力也使得分布式数据处理更为常见。

在企业网络的早期，数据处理功能集中在一台大型机上。然而，今天更为常见的是，通过网络将计算机和终端连接在一起的分布式数据处理配置。但这并不意味着中央数据处理配置不再存在。虚拟化、数据中心整合、共享服务中心、第三方数据中心和云计算正在使许多观察者认为集中式数据处理有抬头的势头。第3章探讨围绕集中式和分布式数据处理的企业问题，并讨论每种类型的配置可能采取的各种形式。

1.7 因特网及分布式应用

企业需要关注计算机通信软件的两个方面：通过企业网络给企业用户计算设备提供的应用软件；让这些计算设备一起协同工作的底层互联（网络）软件。

企业用户间大量的计算设备需要协同工作。例如，当一个组织中大多数员工访问一台个人计算机（PC）或智能手机时，组织内通信的最有效手段之一是电子邮件。当员工需要与同事沟通时，通过电子邮件发送的消息比随意地通过电话联系更有效。电子邮件的详细信息可以留在收件人的电子邮箱中，当收件人方便时可以阅读和回复这些邮件。企业用户之间计算设备的增多，引起了网络环境广泛的应用需求，包括合作、文档和数据共享以及工作流应用。

这些应用程序成功合作的关键是，所有计算设备使用相同的语言“说话”，这是底层互联软件的作用。此软件必须确保所有设备与它们想要通信的设备以它们可以理解的方式传输消息。在企业网络的初期，保证计算设备之间通信的唯一方法就是利用专门的网络解决方案，如 IBM 的系统网络架构（SNA）。SNA 是在 20 世纪 70 年代引入的，并且只能用于 IBM 设备。其他厂商跟随 IBM 的引导，将自己专用的通信架构与他们的设备连接。虽然使用单一厂商的架构和设备可以创建一个企业级的网络，但实现使用不同通信架构的地方和组织之间的互联几乎是不可能的。令人高兴的是，这种情况已经发生了根本性变化，通过采用互联软件标准，使来自多个厂商的设备可以用在同一个网络中。通过了解这些标准的范围和现状，今天的企业管理者能够帮助企业基于多厂商的设备建立健壮的网络基础设施。

现代数据通信和微电子技术正在从根本上改变现代信息系统的架构。大多数企业软件应用程序不再需要大型的通用主机运行，集中式计算架构已经让位给分布式计算，因为它可以与用户的计算设备共享处理负载。商业用户的设备由特定服务器支持功能执行，如打印、存储文件或支持数据库活动，用户设备通常通过高速局域网连接到服务器。这种方法称为客户机/服务器架构，需要先进、可靠、安全的数据通信，但其固有的灵活性和响应能力使其在今天的企业网络中成为一个常见部分。

本书的第三部分仔细分析与用于支持分布式应用程序的基础设施相关的许多主题。

1.7.1 因特网

各种规模的企业竞相利用因特网和 Web。Web 为企业与客户沟通和销售产品与服务提供了多种方法，它已成为一个重要的销售渠道，电子商务交易量不断增加。搜索引擎和社交媒体营销占据企业广告预算的比例不断提高，往往牺牲纸质广告（杂志和报纸）的消费。因特网技术以内部网和外部网的形式，使企业与客户、供应商和合作伙伴之间可以实现安全通信。在第三部分的第 7 章提供了因特网的重要背景，并指出它已经成为大多数企业网络重要方面的原因。

1.7.2 TCP/IP 协议

历来抑制灵活的企业网络发展的最大困难之一是，源于不同的数据通信设备供应商所开发的专用架构。因特网的出现及其使用的标准化的通信协议，促进企业将来自不同供应商的不同设备整合到自己的网络基础设施中。第 8 章的重点是 TCP/IP 协议套件，即现在广泛应用在跨越多厂商设备之间的通信软件，是因特网运行的基础。

1.7.3 客户机/服务器架构、内部网、外部网和 SOA

第 9 章讨论客户机/服务器架构的特点以及这种架构为什么演变为当今企业网络的主导架构。在当今企业网络的客户机/服务器模型中，单独的计算机（服务器）在许多用户（客户）共享的基础上提供专门的服务，如数据库函数、文件存储、打印和其他功能。这些服务

器可以通过局域网（LAN）和其他通信网络访问，通过专业化技术提高性能，降低成本。

内部网在企业组织内部也获得了广泛的支持。它提供与因特网、万维网相同的应用程序和接口。不同的是，内部网被限制在该组织内的授权用户使用，外部用户无法访问。内部网以一种灵活的、易于使用的且易于实施的方法支持多种企业应用。例如，包括用于人力资源管理目的（如培训和发展、工作时间和出勤、申请/审批休假和福利管理）而设计的员工自助服务（ESS）和管理自助服务门户（MSS）。

除了考察客户机/服务器模式和内部网外，第9章还讨论了外部网和面向服务的架构（SOA）。与内部网一样，外部网依赖于TCP/IP协议和应用。外部网使外部客户和企业合作伙伴能够访问公司的计算资源，并且它还是用于支持组织内业务处理的主要方法，如供应链管理（SCM）和适时反应战略（JIT）生产。SOA是另一种类型的客户机/服务器架构，已被企业系统软件供应商广泛应用，使客户在所属网站能够获得他们的商业软件产品。由于SOA，中小型企业（MSE）可以使用ERP、CRM以及其他企业系统软件来运行业务，而无需提前安装。增加关于SOA的理解是理解Web服务、SaaS（软件即服务）、PaaS（平台即服务）和其他今天企业正在越来越多使用的基于云计算服务的基础。

1.7.4 分布式应用程序

对于几乎所有的企业来说，分布式信息处理是必要的。公司内部和公司间信息交换的应用程序正在被分布式计算设备越来越多地使用，这些应用程序包括SMTP、HTTP和其他广泛使用的以TCP/IP为基础的应用程序。第10章考察了企业网络中使用的一些主要应用程序，还考察了推动企业采用统一通信协议的会话发起协议（SIP）。

1.8 网络

全球使用的计算机数量达到数以10亿计，而且所有类型计算设备（包括智能手机）的存储和处理能力的提升，意味着很多员工可以为各种与工作相关的应用和功能使用他们喜欢的设备。因此，用户使用自己喜欢的计算设备访问个人和企业应用的压力是不可抗拒的，它正在改变所有通信设备供应商的思考方式和所有通信基础设施产品和服务的销售方式。这种连接性的需求表现为以下两个方面：通信软件的需求和能够支持语音、数据、图像和视频流量的高性能网络的需要，其中通信软件的需求在下一节中简要介绍。

局域网（LAN）已经成为非常常见的网络类型。事实上，几乎在所有的大中型办公楼中都能看到局域网。局域网，尤其是Wi-Fi局域网，也越来越多地被用于小型办公室和家庭网络。随着计算设备的数量和处理能力的不断增长，企业局域网的数量和容量也随之提升。局域网的国际公认标准的发展也促进它们在企业中广泛应用。虽然以太网已成为占主导地位的局域网架构，但企业管理者仍然可以选择企业内部网络的传输速率（例如，百兆、千兆与万兆以太网），以及有线和无线局域网的结合程度。在今天企业网络中，多种局域网和计算设备的互联给网络专业人员带来持续的挑战。

企业对能够支持语音、数据、图像和视频通信的强大网络的需求，并不局限于一个单一的办公楼或局域网。今天，它是一个企业范围的通信需求。局域网交换机和其他数据通信技术的进步，大大提高了局域网的传输能力和集成概念的出现。集成意味着通信设备和网络能够同时处理语音、数据、图像甚至视频，伴随着一个备忘录或一份报告的是配音解说、图形

展示，有可能甚至是短小的视频介绍、展示和总结。虽然图像和视频在局域网中能够提供很好的性能，但给广域网传输提出高要求，且成本昂贵。而且，随着局域网的普及以及LAN传输速率的增加，增加了企业实现不同地理位置区域互联的要求，这反过来促使企业增加WAN传输和交换能力。幸运的是，光纤和无线传输服务能力的日益增长，为满足这些企业的数据通信需求提供了足够的资源。然而，能够应对日益增加的传输链路容量和企业通信流量要求的交换系统的发展是现在面临的一个还未克服的挑战。

企业使用网络作为一竞争工具，网络成为提高生产率、削减成本的手段，机遇是巨大的。当企业管理者理解这些技术后，他们可以有效地周旋于数据通信设备供应商和服务提供商之间，提高企业的竞争位置。

在本节的其余部分，简要概述企业网络架构中各种类型的网络。第四部分和第五部分更详细地介绍了这些主题。

1.8.1 广域网

广域网一般覆盖一个大的地理区域。它们往往需要通过公共线路，通常至少在一定程度上依靠一个或多个公共载体提供的电路。这里公共载体指的是给公众提供通信服务的通信公司。通常情况下，一个广域网由若干相互连接的交换节点组成。从任何连接网络的设备发出的信息都是通过这些节点路由到指定的目标设备。这些节点不关心数据的内容，相反，他们的目的是提供一个交换设备，将数据从一个节点发送到另一个节点，直到它们到达目的地。

传统上，已实施的广域网一般使用两种技术：电路交换和分组交换。最近，帧中继和信元中继网络已经承担了重要的角色。第16章介绍帧中继和ATM（异步传输模式），即广泛使用的中继技术。这章还考察了多协议标签交换（MPLS）和广域以太网（WAE）。

1. 电路交换

在电路交换网络中，通过网络的交换节点在发送者和接收者之间建立一个专用的通信路径。这条路径是节点之间的物理链路序列。在每一个链路中，逻辑通道是专门用于发送者和接受者之间的一个连接。由发送装置所产生的数据通过这个专门的路径尽可能快地传输。在每个交换节点，输入数据无延迟地路由或交换到合适的输出通道。电话网络是最经典的电路交换的例子。当你打电话给某人并接听时，一个稳定的数据流通道通过电路连接建立起来。为了连接你呼叫的人，无论需要多少个交换节点，该电路的运作方式都是相同的。只要你需要使用该电路，它就是你的，直到你挂断。

2. 分组交换

在分组交换网络中，使用另一种方法。在这种情况下，没有必要独占一条网络路径的传输容量。相反，数据通过一系列的数据包（叫做分组）传输。每个数据包沿着由源地址到目的地址的路径，通过网络从一个交换节点传输到另一个交换节点。在每个交换节点，接收整个数据包，可能进行简单的存储，然后将数据包发送到下一个节点。传统上，分组交换网络最常用于终端到计算机和计算机到计算机的数据通信。现在，它们也可用于进行即时性的语音和视频通信。分组交换和电路交换在第15章中进行更详细的介绍。

3. 帧中继

当长距离数字传输设备比今天使用的设备有相对高的错误率时，分组交换技术就出现了。因此，在分组交换方案中有相当数量的额外开销，用以补偿误差。这些开销包括加到每

个分组的附加位，以便在目的设备进行错误检查和额外处理，或者在中间交换节点检测和恢复错误。

对于现代高速通信系统，这方面的开销是不必要的，且会适得其反。现在，错误率已经大大降低，而那些仍然存在的少量错误可以很容易地被目标设备发现和解决。这意味着，它不再需要在交换节点进行错误检查活动。取消节点到节点的错误检查和错误恢复，意味着电路容量可以更高效地用来传输数据，而不是差错控制信息。

帧中继开发利用更高的数据速率和更低的误码率，它们可用来实现广域网。鉴于原来的分组交换网络支持每个用户约 64Kbps 的数据传输速率，设计帧中继网络在用户数据速率 2Mbps 以上的前提下有效运行。实现这些高数据传输率的关键是使用不易出错的电路，并去除大部分参与差错控制的开销。

4. ATM

异步传输模式（ATM），通常也称为信元中继，它是电路交换和分组交换发展的顶峰。然而，ATM 被广泛视为帧中继技术的进化。帧中继和 ATM 之间最明显的区别是，帧中继使用可变长度的称为帧的数据包，而 ATM 采用固定长度的称为信元的数据包。与帧中继相比，ATM 提供了很少的用于差错控制的开销，它依靠传输系统固有的可靠性，并使用目的设备捕获和改正错误。与帧中继相比，使用一个固定长度的数据包，可以进一步降低 ATM 网络之间数据传输的处理开销。因此，ATM 的数据速率为 100Mbps，在 Gbps 范围内。

ATM 也可以看作电路交换的演变结果。与电路交换相比，它的发送设备和接收设备使用唯一的固定数据速率的电路。ATM 允许发送者和接收者建立多个不同数据速率的虚拟通道，而且数据速率是创建每个虚拟信道时动态定义的。每个通道可以传输不同类型的数据（如语音、数据、图像或视频），ATM 可以很好地支持视频会议和其他即时性的多媒体应用。即使 ATM 采用分组交换技术，但通过使用小的、固定大小的信元，ATM 可以有效地提供逻辑的、专用恒定数据速率的通道。因此，ATM 扩展了电路交换，允许在每个通道上根据需求动态设置具有不同数据速率的多个通道。第 16 章对 ATM 和帧中继技术进行了更充分的研究。

1.8.2 局域网

与广域网相比，局域网是一个连接各种设备的通信网络，它为这些设备之间的信息交换提供了一种手段。局域网和广域网之间有几个关键的区别：

1）局域网的地理范围比较小，通常是一个单一的建筑物或建筑群。正如我们将看到的，在地理范围上的这种差异会导致不同的技术解决方案。

2）通常情况下，用于实现局域网的交换机和通信设备都属于同一个企业，该企业拥有与 LAN 相连的计算设备。而广域网，除了较少的情况下，广域网的电路和交换节点的全部或至少主要部分不属于这个公司。这有两个含义：首先，公司管理者选择局域网时必须小心，因为这个选择会转化为将大量资金投入网络设备采购和持续的网络维护。其次，局域网的网络管理责任仅落在拥有者身上。

3）局域网内部的数据传输速率通常远远大于广域网的数据传输速率，它可以花费较小代价建立 100Mbps 或超过 1Gbps 的网络，而在连接局域网的广域网中相当的数据传输速率的代价是高昂的。

局域网可以有多种不同的配置。最常见的是交换局域网和无线局域网。最常见的交换局

域网是交换以太网局域网；无线局域网最常见的类型是 Wi-Fi 无线局域网。

本书的第四部分涵盖了局域网的介绍。第 12 章涵盖企业中常见的各种类型的局域网，包括存储区域网络（SAN）、骨干网、分层局域网和介质、结构化电缆基础设施以及实现局域网的介质访问控制架构。第 13 章重点介绍以太局域网。第 14 章更详细地考察 Wi-Fi 网络。

1.8.3 无线网络

正如刚才提到的，无线局域网在公司网络中是常见的，且成为标准的特征。企业移动性的推动力意味着企业网络通常包括无线技术来支持广域语音和数据网络。第 17 章的重点是无线广域网，包括：蜂窝网络、第三代（3G）和第四代（4G）无线服务以及基于卫星的通信。

1.8.4 城域网

正如它的名字所暗示的，城域网（MAN）占据了局域网和广域网之间的中间地带。人们已经越来越认识到传统的在广域网中使用的点到点和交换网络技术可能不足以满足企业网络通信流量增加的需要，这促使公司对城域网产生兴趣。虽然继续使用帧中继和 ATM 可以满足大范围的高速传输的需求，但对于低成本覆盖大城域的大容量私有和公共网络的需求不断扩大。有很多种方法已得到实现，包括无线网络（如 WiMax 和 Wi-Fi 无线云）、城域网扩展到城域以太网。

城域网的主要市场是都市区具有高容量需求的企业客户。城域网主要是用来提供比从本地电话公司或因特网服务提供商获得同等服务的成本更低、效率更高的需求容量。

1.8.5 配置示例

为了帮助读者理解第三至五部分涉及的内容，用图 1-7 来说明一些目前使用的典型通信和网络元素。在图的左上部分，我们看到了个人住宅用户通过某种用户连接连接到因特网服务提供商。数字用户线（DSL）就是这种连接一个常见的例子，它需要特殊的 DSL 调制解调器，通过电话线或光纤电缆提供高速链路，或者利用一个电缆调制解调器连接到有线电视服务提供商。每一种情况下，信号编码、差错控制和用户连接到网络的内部结构都是不同的问题。

通常情况下，一个 ISP 网络包括多个相互连接的服务器（虽然如图 1-7 所示只有一个服务器），它们通过高速链路连接到因特网。同步光纤网络（Synchronous Optical Netork，SONFT）是这种链接的一个例子，它在第 6 章中进行描述。因特网包含相当数量的覆盖全球的互联路由器，这些路由器通过因特网转发从源地址到目的地址的数据包。

图 1-7 的下部分显示了一个使用单一以太网交换机实现的局域网。在小型公司和其他小企业中这是一种常见的配置。局域网通过防火墙连接到因特网，这里通过防火墙提供安全服务。在这个例子中，防火墙通过一个 ATM 网络连接到因特网。还有一个局域网路由器挂接到一个专用广域网，这可能是一个专用 ATM 或帧中继网络。

各种设计问题，如信号编码和差错控制，都与相邻部件之间的链接相关，例如因特网上路由器之间的链路、ATM 网络中的交换机之间，以及住宅用户或企业用户与 ISP 之间的链接。各种网络（电话、ATM、以太网）的内部结构产生了额外的问题。图 1-7 建议的设计特征在第三到第五部分进行讨论。

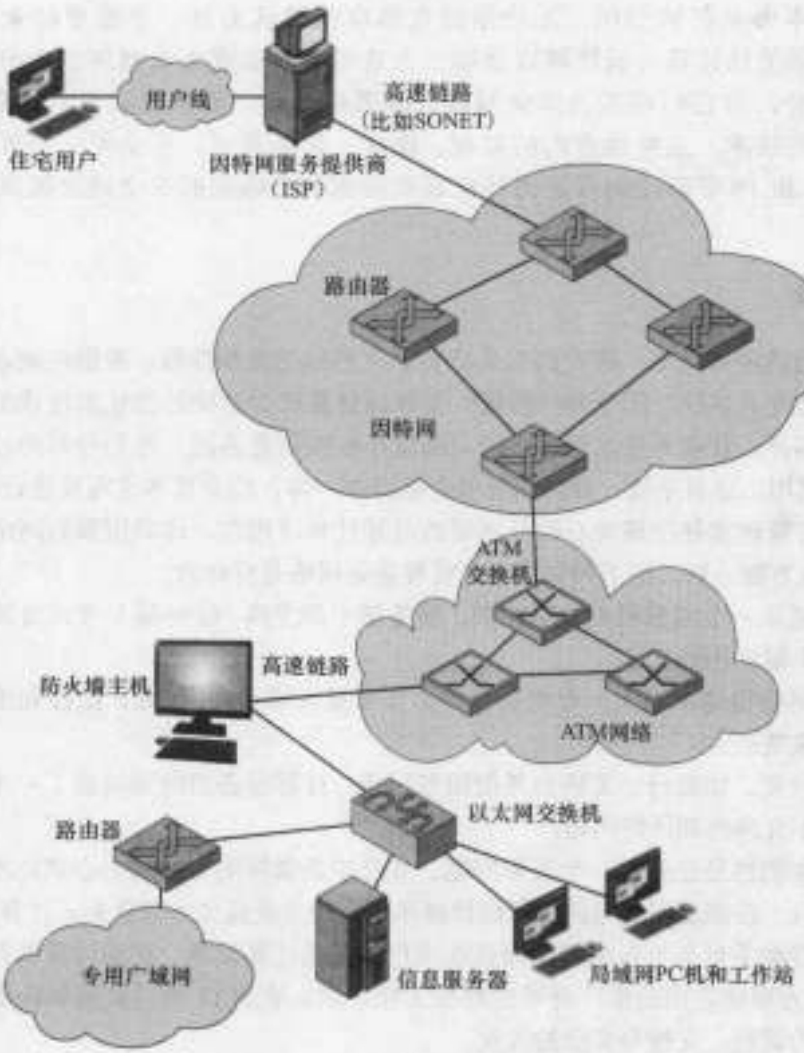


图 1-7 网络配置示例

1.9 管理问题

第六部分通过考察与企业数据通信相关的密钥管理问题对本书进行总结。

1.9.1 网络安全

随着企业越来越依赖于网络，通过因特网的外部访问和其他链接不断增加，棘手的安全问题变得越来越重要。公司处于机密信息泄露和企业数据非授权改变的风险中。在第 18 和 19 章中，我们讨论实现网络安全的基本工具和如何调整这些工具以满足公司的需要。

由于网络安全不能、也不应该与本书中其他数据通信和网络概念相孤立，所以它的讨论并没有仅仅局限在第 18 和 19 章。相反，这两章考察了前面章节里涉及的与重要概念相关联的安全概念，而当时还无法详细探讨。例如，在本章中介绍的内部网、外部网和虚拟专用网，它们典型地包含了安全机制，如访问控制、邮件加密、防火墙和与其相关的安全控制，以及企业使用它们的原因。

安全在整本书里都被引用，无论何时它都应该被认为是一个重要的业务考虑。例如，随着移动和无线计算、云计算以及第三方数据中心变成企业网络基础设施的越来越重要的组成部分，与它们相关的安全问题也越来越重要。如果我们没有提到安全问题，而仅仅讨论这些技术，这将是我们的失职。因此，你将看到，安全是一个贯穿全书的重要主题，第 18 和 19 章陈述的课题将补充或对前面章节确定的安全概念提供一个更深入的了解。

1.9.2 网络管理

在数据通信的最初几年，研究的重点是关于技术的功能和性能。关键问题是，这种技术可以做什么？速度有多快？用于哪些传输？随着以计算机为基础的信息系统成为许多企业的基本结构的一部分，管理人员发现他们公司的运作依赖信息系统，他们公司的经济绩效取决于技术的有效利用。也就是说，像任何其他企业资源一样，信息技术也需要进行管理。例如，今天，数据通信管理者往往最关心的是网络的可靠性和可用性，许多所需的网络管理功能对企业管理的其他方面一样，但下列要求对于管理企业网络是特殊的：

- 网络已经从一个容易控制的客户机 / 服务器（即主机 / 哑终端）方式发展到高度分布式系统中端到端的互连。
- 对等网络变得越来越大（有些有成千上万个接入设备），管理、监控和维护它们已经变得非常复杂。
- 在很多行业，如银行、零售和其他服务行业，计算设备的网络构成了一个关键的战略资源，不允许出现任何问题。
- 通信成本仍然是企业的一个重要问题，并且缺乏指挥网络控制中心和处理网络管理的技术人员。控制通信费用的愿望促使越来越多的企业接受虚拟化和云计算。
- 伴随着智能手机和平板电脑成为企业用户的首选计算设备，移动计算因此而流行。基于 Web 的移动应用的推广有可能转变工作方式。企业 IT 部门必须解决随着移动计算而带来的管理、支持与安全的挑战。

在大型企业中，网络管理必须提供全球可见的企业信息流。先进的网络管理系统需要提供远程监控、快速故障通知和自动调用恢复措施。为了使用不同周期的业务活动，需要即时分析设备的网络性能并动态调整网络参数。今天，网络管理是一门复杂的学科，特别是在多设备供应商的环境中。企业管理者必须了解网络管理的要求，以及计划和有效实施相应网络管理策略的可用工具和技术。

第 20 和 21 章重点关注网络管理，但正如本节前面所述，有些网络管理的主题很难局限于数据通信课本的特定章节，尤其是与企业网络基础设施演化相关的主题。大多数的企业管理者认识到他们的组织高度依赖于网络来进行企业的运作和竞争，这也提升了有效管理网络资源的重要性。许多业内专家认为，云计算和移动性将给企业网络基础设施带来新的变化，这可以与从集中的、大型机为中心的网络到客户机 / 服务器架构的变化相提并论。如果移动性和云计算推动企业网络架构发生里程碑式的变化，那么企业的各方面都将受到影响。

与安全性一样，网络基础设施是贯穿全书并在许多地方进行强调的主题，在第三～六部分尤其明显。第三部分讨论因特网、客户机 / 服务器架构、内部网、外部网、面向服务的架构（SOA），以及因特网应用，让人们了解企业网络中公共因特网和基于 IP 的应用是

如何使用的。第四部分讨论有线和无线局域网，这些是本地网络的核心部分。第五部分讨论如何使用广域网连接地域分散的企业单位。第六部分讨论如何使用网络管理系统监控企业的通信流量和向网络管理者提供问题告警，以便最大限度地提高企业网络的可用性和性能；它还讨论了如何设计网络，以确保关键业务应用的性能。网络基础设施也是第一部分分布式数据处理的一个主题。第3章讨论“为什么存储区域网（SAN）已经成为许多企业网络中的重要组成部分”、“为什么‘大数据’有望成为企业竞争、企业增长和创新的重要基础”。

1.10 标准

标准是数据通信领域的一个非常重要的部分，几乎所有数据通信产品和服务供应商都致力于支持国际标准。本书描述了正在使用的最重要的标准，以及为数据通信和网络各个方面而正在开发的协议。许多组织已经参与这些标准的开发或推广。几个最重要的标准制定组织是：

- **因特网协会**：ISOC领导解决未来的因特网的问题，同时，它也是负责因特网基础设施标准的组织，包括因特网工程任务组（IETF）和因特网架构委员会（IAB）。这些组织负责制定因特网标准和相关规范，所有这一切都作为RFC（请求评议）发布。
- **ITU-T**：国际电信联盟（ITU）是联合国系统内的国际组织，政府和私营部门通过它协调全球电信网络和服务。国际电信联盟的电信标准化部门（ITU-T）是国际电联的3个部门之一。ITU-T的使命是制定涵盖所有通信领域的标准。ITU-T标准也称为建议书。ITU-T标准通常以大写字母后跟一个句点（.）和数字表示，例子包括H.263（视频编码）、V.90（拨号调制解调器）和X.25（分组交换）。
- **ISO**：国际标准化组织（ISO）[⊖]是一个来自140多个国家的全球性组织。ISO是一个非政府组织，为了促进标准化的发展、方便商品和服务的国际交换，以及在智力、科学、技术和经济活动领域的合作发展。ISO的工作导致国际约定，并作为国际标准发布。
- **IEEE 802**：IEEE（电气和电子工程师协会）802LAN/MAN标准委员会负责制定局域网标准和城域网标准。最广泛使用的标准是以太网系列（802.3）、无线LAN（802.11）和虚拟局域网（802.1q）。每个工作组专注于一个领域的标准。
- **国家标准和技术**：国家标准和技术（NIST）是美国联邦机构，它处理涉及美国政府使用的并促进美国私营部门创新的测量科学、标准和技术。尽管是国家范围的，但NIST联邦信息处理标准（FIPS）和特别出版物（SP）有全球性的影响。

这些组织在附录B中进行更详细的讨论。

案例研究I：波音公司的统一通信

这个案例研究中包含的主要概念包括统一通信和融合的IP网络。**该案例研究以及更多可用信息可在www.pearsonhighered.com/stallings查看。**

⊖ ISO不是一个首字母缩略词（如果使用缩略词，那么是IOS），而是一个来自希腊语的单词，意味着相等。

1.11 关键术语、复习题和练习题

关键术语

Asynchronous Transfer Mode（ATM，异步传输模式）
circuit switching（电路交换）
client/server（客户机/服务器）
convergence（融合）
data communication（数据通信）
distributed application（分布式应用程序）
frame relay（帧中继）
image communication（图像通信）
Internet（因特网）
Local Area Network（LAN，局域网）
Metropolitan Area Network（MAN，城域网）
packet switching（分组交换）
unified communication（统一通信）
video communication（视频通信）
voice communication（语音通信）
wide area network（WAN，广域网）
wireless network（无线网络）

复习题

1.1 至少从3个方面确定并简要说明网络有助于企业的成功。
1.2 简要描述企业网络的流量、服务和硬件的趋势。
1.3 简要定义融合，并描述融合带给企业的主要利益。
1.4 简要描述统一通信（UC）的特征，同时描述UC如何促进个人、工作组和企业范围的性能提升。
1.5 识别并简要介绍企业网络传输的4种类型的通信流量。
1.6 为什么光纤布线已经成为企业网络常见的基础设施？
1.7 为什么企业越来越广泛地使用无线传输？
1.8 为什么分布式处理在企业网络中变得常见？
1.9 对比网络互连软件与应用软件的功能。
1.10 对比广域网、局域网和城域网的主要特征。

练习题

1.1 针对软件即服务（SaaS）、平台即服务（PaaS）和基础设施即服务（IaaS）的特点展开在线研究。写一篇简短的文章，描述这些服务的不同，并识别每种类型服务的一些主要供应商。
1.2 关于统一通信，搜索并查看多个YouTube视频。确定3个你认为能很好说明UC系统的特征和功能的网址。选择一个你认为是最好的，并简要说明你的选择。
1.3 做一些网上研究，找到几家从统一通信中受益的企业信息。写一篇简短的文章描述他们如何以及为何使用统一通信，统一通信已经给企业带来什么好处。
1.4 做一些网上研究，找到几家已实施IPTV的企业的信息。写一个简短的论文，描述他们如何以及为何使用IPTV，IPTV已经给企业带来什么好处。
1.5 对城域网和城域以太网做网上调查。写一篇简短的论文，对比城域以太网和其他可供企业选择使用的城域网。
1.6 使用Skype、雅虎即时通信，或结合了实时语音、视频（网络摄像头）、聊天的类似工具，与朋友或家庭成员建立通信会话。使用一个或多个屏幕捕捉器为通信会话记录语音、视频和聊天，然后对它们进行文字处理，并以导师可以打开的文档格式（如rtf或

docx）保存。你的屏幕捕捉器应包括你自己和你的朋友或家庭成员的网络摄像头窗口，以及说明你正在实时聊天的一个窗口。

附录 1A 数值单位的前缀

位（b，也称为比特）是离散信息的基本单位，它代表一个选择结果：1 或 0、是或否、开启或关闭。一位代表两种可能的结果。因此，举例来说，1 位可以代表一个开关的开 / 关状态。2 位可以代表 4 种结果：00、01、10、11。3 位代表 8 种结果：000、001、010、011、100、101、110、111。每添加 1 位，可能表示的结果数就翻倍（见表 1-3）。一个**字节**（或 **8 位组**，通常简称为 B）代表 8 位（例如，8b=1B）。一个字节代表潜在结果的数量是 $2\times2\times2\times2\times2\times2\times2\times2=2^8=256$ 个。字节通常用于表示在计算机中的存储量。位通常用来描述通信速率。

表 1-3 位数和对应的结果数

位数（x）	结果数（2^x）	典型应用
1	2	信息基本单元
4	16	十六进制数字
7	128	没有奇偶校验位的 IRA（国际参考字母表）字符
8	256	字节；有奇偶校验位的字符
10	1024	以 kB 存储的字节数
13	8192	以 kB 存储的位数
16	65 536	老式计算机的地址空间
20	1 048 576	以 MB 存储的字节数
23	8 388 608	以 MB 存储的位数
32	4.3×10^9	通常的内存地址空间
64	1.84×10^{19}	较新计算机的内存地址空间

在计算机科学文献中，前缀 kilo、mega 等经常用于数值的单位。这有两种不同的解释（见表 1-4）：

- **数据传输**：对于数据传输，使用的前缀是为国际单位制（SI）定义的，是国际标准。在这个方案中，前缀用来作为表达 10 的幂的一种速记方法。例如，1 千位每秒（1Kbps）=10^3bps=1000bps。
- **计算机存储**：在计算机存储器、文件或消息传输的数据量通常以字节为单位。因为存储器是用二进制地址表示的，所以存储器的大小表示为以 2 为底的幂。它使用前缀的方式与 SI 方案相似。例如，1 千字节（1kB）=2^{10} 字节 =1024 字节。

表 1-4 数字前缀

前缀名	前缀符号	因子	
		国际标准（SI）	计算机存储
tera	T	10^{12}	2^{40}
giga	G	10^9	2^{30}=1 073 741 824
mega	M	10^6	2^{20}=1 048 576
kilo	k	10^3	2^{10}=1024
milli	m	10^{-3}	
micro	μ	10^{-6}	
nano	n	10^{-9}	

第一部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

需　求

第 2 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

业务信息

学习目标

通过本章的学习，读者应能够：

- 区分数字信息源和模拟信息源。
- 把业务信息类型分成 4 个类别：音频、数据、图像和视频。
- 定量评估这 4 类信息源所需的通信资源。
- 能够解释为什么系统响应时间是度量用户工作效率的关键因素。

如今业务网上传输的信息量一直处于增长的趋势，这在某种程度上是由于不断增长的业务越来越依赖于网络来实施和操作，同时也是由于企业网所承载的信息类别的革新所导致的结果。视频和图像信息通信量的增长，促使行业急需建起更为健壮的企业网络基础设施。

理解信息通信与业务需求的相关性是很重要的。理解的第一步是在基本层面检查不同类型的业务信息。业务应用有很多种，而且每种都有各自的信息特征。然而为了能更好地分析和设计企业网络，与业务应用相关的信息流量通常被分为 4 种基本信息源：**音频、数据、图像**和**视频**。

本章介绍以下主题：

- 如何度量信息源对通信系统的影响。
- 4 种基本类型的业务信息（音频、数据、图像、视频）的本质。
- 每种信息源的主要业务用途。
- 从充分支持业务通信需求的角度，概括性地认识这些业务用途的网络基础设施的意义。

业务信息可以以**数字**或**模拟**两种形式来传输。数字系统利用一串离散的、不连续的数值或符号来表示信息。离散信息有一个有限的“字母表”。例子包括字母、数字、符号和二进制数字（用来代表两种状态，如“开”或“关”、“是”或“否”等）。在数字系统中，信息传输速率和数字信道的容量都是由每秒传输的位数来度量的。

非数字的模拟系统用一个连续范围内的数值来代表信息。模拟信息源包括声音、音乐和视频。人们主要是通过模拟方式来感知这个世界的，这在听觉和视觉上尤其明显。例如，我们通过对形状和颜色的渐变来感知世界，通过一个大范围内的音拍、音调、音量变化来欣赏一段管弦乐交响曲。相似地，我们通过从寒冷、较冷、微温、温暖、炎热这一连串连续的变化来感知温度，而不是离散的“热”和“冷”两个值。

模拟通信系统是用连续信号来代表连续信息源或离散信息源。电压可以被使用，正是因为其可以用一段连续的数值来表示信息。例如模拟麦克风，当有人对着它讲话时生成模拟电信号。这种情况下，这些模拟电信号代表人向麦克风讲话而形成声音在空气气压的连续变化。对于模拟通信系统，信息传输速率和信道容量是由带宽的赫兹（Hz）来度量（1 赫兹 =1 秒内的周期数）。事实上，不管是离散的还是模拟的信号源，都可以用一串不同频率的纯粹振动组

合来表达。在模拟系统中，带宽是用来度量代表信息的频率的限度（或范围）。该频率所能达到的范围越大，带宽就越大，并且一个复杂信息源也越能被精确地表现出来。

这里需理解的很重要的一点是，不管是模拟信息系统还是离散信息系统，都可以通过数字传输系统或模拟传输系统来传输。例如，如今我们通常“数字化”一些模拟信息源，如将声音和视频转换为数字音频或数字视频，从而使其可以通过数字传输系统来传送。当然也可以将离散数据用连续信号来表示，并且通过模拟传输系统来传送。因为企业并不局限于只用数字传输系统来传送离散信息源，或只用模拟传输系统来传输模拟信息源，所以管理者需要理解何种传输系统可以满足他们的信息传送需求。

2.1 音频

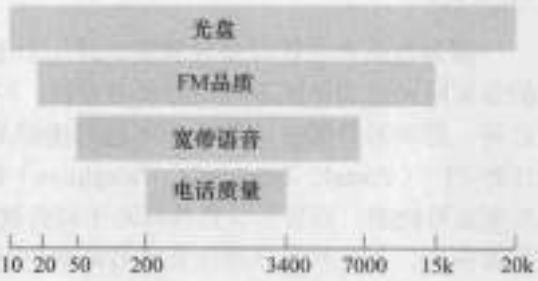


图 2-1 信号频率和带宽（Hz）

音频通信服务支持基于声音的应用，尤其是人的声音。传统上，电话（电话通信）已成为声音服务的主要业务应用，其他应用包括电话销售、语音信箱、音频会议、交互式语音应答（IVR）系统、呼叫中心、播客和商业广播等。与这些声音应用相关的声音质量主要是由可利用带宽来度量（见图 2-1）。在传统的模拟电路中，电话中能传输的声音仅局限于约 3400Hz 的带宽，这只能提供一定层面的质量保证。对于电话会议，则需要约 7000Hz 的带宽。对于高保真声音的质量要求，则需要 15 000Hz（大约在人类听力的范围之内）的带宽。对于光盘，一个立体声的每个声道都需要 20 000Hz 的带宽容量。

音频信息也可用数字形式来表示。关于模拟信号转换成数字信号的过程（数字化）将在第 4 章中更详细地讲解，这里先做一个简略的讲述。为了能以数字形式较好地表示声音，我们需要以至少模拟信号的最大频率值的两倍速率来取其振幅的样本。对于要求电话品质的声音，我们通常需要每秒采集 8000 个样本，这也是人们演讲频率（4000Hz）均值的两倍。对于高质量光盘的声音，每个声道需要每秒 44 100 个样本。在采样之后，需将信号振幅转成数字形式，这个过程称为**量化**。对于电话声音通常需要每个样本 8 位，对于光盘立体声的每个信道则需要每个样本 16 位。在第一个例子中，可以区分 256 个强度的振幅，在第二个例子中可以区分 65 536 个强度的振幅。因此，如果没有压缩，数字声音需要 8（位 / 样本）× 8000（样本 / 秒）=64 000（位 / 秒）。在 CD 音乐的例子中，将前面提到参数进行简单的乘法（16 × 44 100 × 2）可知，两个信道共需要 1.41Mbps（位 / 秒）。一张容量为 600MB 的 CD 唱片可以维持 1 小时左右的立体声播放。

传统电话交谈的平均长度在 1 ~ 5 分钟。对于寻常的语音电话通信，任何方向上的信息传输在少于一半的时间内传输，不然将会导致通话双方同时讲话。

采用音频压缩算法来降低通过通信线路传输的数字音频流的宽带要求，该算法也可用来降低音频文件的存储空间。目前存在有损耗的和无损耗的 2 种音频压缩算法，并且它们都应用于数字传输系统中的音频编码器和解码器以及计算机软件中。与无损耗压缩算法相比，有损耗压缩算法可提供更高的压缩比，因此用于更多的用户音频设备中。

有损耗的和无损耗的压缩算法有很大的不同。若使用**无损耗压缩算法**，通过解压缩接收

到的文件，接收者可以精确地还原出与发送者传输的原始声音流完全一致的数字信号。若使用**有损耗压缩算法**，当接收者解压文件时，会发现破坏原始声音流质量的不可逆转的源文件损伤已造成。在某些情况下，人们不一定能听得出来声音质量的损耗，但是在更高压缩比的压缩情况下声音损耗就显得很明显了。

有损耗算法可以将音频文件压缩至原来大小的 20% 以下，同时会造成原始文件平均减小 5% ~ 20%。有损耗算法的例子是 MP3 和 Vorbis 格式。无损耗算法可以将音频文件压缩至原来大小的 50% ~ 60%。无损耗压缩算法的例子有 FLAC（Free Lossless Audio Codec）、Apple Lossless、MPEG-4ALS（MPEG-4 Audio Lossless Coding）和 WMA（Windows Media Audio）Lossless。

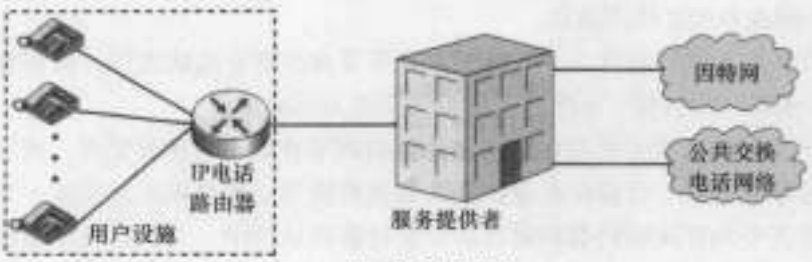
网络化含义

因为电话产业依旧是音频服务的一个主要业务应用，所以在如今的企业网络中电话服务的强大而灵活的访问方式是必须考虑的。户外服务可以由公共电话网来提供，包括当地电话公司、提供语音服务的竞争性本地转接服务（CLEC）、远距离传输工具（如 AT&T）和全国性的 PTT（Postal，Telegraph，Telephone）权威组织。另外，多种专用网络设施、租用线路安排都是可能的，而且云计算选择对于以音频业务为中心的应用来说也是越来越具有可行性了。无需多言，业务推动移动性意味着蜂窝电话服务提供商在企业网络蓝图中所占比重越来越大了。传统的电话选项将在第 15 章中讨论。蜂窝网络将在第 17 章中论述。

传统业务认为保证某个特殊场所声音质量最有效的方法是把所有的电话都绑定到单个系统中。对此有两种主要选择：专用分支交换（Private Branch Exchange，PBX）和托管式服务（如中央交换机）。**专用分支交换**是指某个组织拥有或租用的电话交换机将本地电话机在内部连起来，并向公共电话系统或声音服务提供外部接口（见图 2-2a）。通常，专用分支交换（PBX）和托管式服务使得在一个办公地点的电话用户可以通过拨打三四个数字号码来连接到另一个在线的工作合作者；或者得到一个外接线路，用户可以通过拨打一个数字号码（通常是 8 或 9）和呼叫接收者电话号码的其他数字来完成连接。



a）专用分支交换



b）托管式IP-PBX

图 2-2　企业电话配置

在 PBX 的演化过程中，最新的发展是承担电话呼叫功能的因特网协议（IP）的使用。支持 IP 声音协议的 PBX 称为 VoIP PBX 或 IP-PBX。托管式 IP-PBX 不仅可以提供与 PBX 服务相同的类型，还可以提供通过 IP 通信可获得的额外功能，包括可以将用户访问功能扩充到通过 Web 端口语音邮件或 E-mail.WAV 文件等的统一信息服务。托管式 IP-PBX 物理上搭建在供应商设施的基础上，并且在用户站点的唯一设备是可以通过 IP 电话与 PBX 通信的 IP 手持机（见图 2-2b）。托管式 IP-PBX 已经大量取代由电话公司提供的中央交换机（Centrex），并且某些 CLEC 可提供与 PBX 相同的服务，但 PBX 在电话公司的中央办公室的设备中完成交换功能。

如今的 PBX 和托管式 IP-PBX 服务可以支持多种与语音相关的服务，包括语音信箱和音频会议呼叫等。为了保持企业通信服务的可实现性，PBX 和托管式 IP-PBX 服务正在慢慢适应支持基础设施和移动业务用户之间的合作，以使得统一通信系统实现的可行性更高。支持统一通信的托管、基于云和基于设施的 PBX 越来越成为企业网络基础设施中的常见因素。

在商业网络上传送音频的数字传输的使用日益增加，这需要网络管理者监控传输给用户的音频的质量。为了增加音频传输的高效性，必须在各种音频压缩算法中做出明智的选择。无需多言，企业不愿意将音频文件压缩得过小，以至于用户、客户或者合作者的声音体验受到大程度损减。

对于企业网络管理者而言，另一个重要的音频传输问题是电话需要与企业系统应用（如 CRM（用户关系管理））相结合。为了实现商业潜能，CRM 系统必须记录每个用户和公司的联系日志，无论是经由 E-mail、Web、短信息、办公电话、家庭电话或者移动电话。记录日志的行为使得企业用户可以及时访问一位客户与公司的联系史，从而获知这位客户的疑问是否被解答了或者问题是否被解决了。通常情况下，CRM 系统也要与其他企业系统（如 ERP（企业资源规划））相结合，并且有超过那些在呼叫中心广泛应用结合了计算机电话应用的能力。

2.2 数据

数据包括能用一些有限字符来表示的信息，字符可以是 0 ~ 9 的数字或计算机键盘上的可用字符。数据的通常例子包括文本信息和数字信息。在计算机或者在传输过程中，符号通常用 8 位的组合来表示。

数字数据最熟悉的例子是文本或字符串。虽然文本数据很方便人们用来与他人交流，但是数据处理和传输系统不容易以字符形式来存储或传输它们。人们已经设计出用于存储和传输二进制数据的系统，即 0 和 1 两种取值。同时，已经设计出许多文本到二进制的转换编码器，用以把文本字符来用二进制数字（位）序列来表示，也许最早常使用的例子是摩斯电码。历史上，运用最广泛的文本编码称为**国际参考字母数字**（International Reference Alphabet，IRA）[⊖]。在这个编码体系中，每个字符用唯一的 7 位形式来表示，因此可以表示 128 种不同的字符。要表示计算机键盘上的所有字符需要一个很大的数字，而且有些位形式是不可见的，如不可输出的控制字符。IRA 编码的字符几乎总是以每字符 8 位来存储和传输，第 8 位是用来检错的奇偶校验位。该校验位的设置保证每个 8 位的字节中 1 的总数总是**奇数**（奇校验）或**偶数**（偶校验）。因此，如果在传输过程中错了 1 个位或奇数个位，都能被检测出来。

在文本到二进制转换完成后，每个字符或符号都用一个位串（0 或 1）来表示，这些位可

⊖ IRA 是在 ITU-T 建议书 T5.0 定义的，以前称为国际 5 号电码（International Alphabet Number 5，IA5）。IRA 在美国的国家版被称为**美国信息交换标准编码**（ASCII）。附录 D 给出 IRA 编码的描述及表格。

以通过模拟系统或数字系统来传输。

ACSII（IRA）字符集是英文文本文件最常用的格式。文本文件（以 .txt 形式保存的文件）只支持很少的格式，如不能支持粗体、斜体和下划线等格式。这是因为以 .txt 形式保存的文件可以被任何文本读取程序打开和读取，它们是独立于平台的。

另一个重要的文本到二进制的编码体系是 UTF-8（通用字符集转换格式 -8）。由于 8 位编码制 UTF-8 可以向后兼容 IRA，所以也许你会认为 UTF-8 局限于代表 256 个字符或符号。然而，因为 UTF-8 支持可变长度编码，可以用多个字节来表示字母表或字符集里的字符，所以 UTF-8 能够表示全世界所有语言中的符号或字符。UTF-8 允许字符或符号用 1 ~ 4 字节来表示，因此可以表示超过 100 万的不同字符或符号。2007 年，使用 UTF-8 的 Web 页面的总数超过了 50%，因此 UTF-8 成为了万维网中具有统治地位的字符编码体系。

Unicode 是另一种重要的字符编码体系，很多种编程语言都支持这个编码体系，包括 Java、微软 .NET 框架、XML 等。它同样被大多数计算机和通信设备上使用的操作系统支持。Unicode 是 16 位编码机制，可以向后兼容 IRA/ASCII。实质上，UTF-8 是 Unicode 的 8 位版本。与 UTF-8 一样，Unicode 的最新版本（包括 Unicode 6.0）可使得一些语言中的符号用多于一个字节来表示，从而使它可以用来表示世界上使用的大多数写字系统。

企业通常会把文本、数字和其他形式的数据，包括图像和视频，组织在一个或多个数据库中。行业专家估计每天有 15PB（15 000GB）的新电子数据产生，其中大部分是由视频、图像、音频和社交媒体数据的大幅增长而生成的。不断增长的创建、收集和存储数据的欲望对于企业业务来说是一个越来越严峻的挑战，而且有重要的通信和网络基础设施含义。与商务数据库的部署和使用相关的网络意蕴将在第 3 章中探索。

为了对本节中讨论的文本到二进制转换概念的通信含义有更好的理解，让我们来估计传输一个简单的打字页面大约需要多少位。通常，字母表中的一个字母或一个印刷字符是用一个字节，即 8 位来表示。对于使用 ASCII-8 或 UTF-8 编码的书面英语绝对是这种情况。假设一张 8.5 × 11 英寸的页面，每边有 1 英寸的空白，这意味着有 6.5 × 9 英寸的空间可以保存计算机键入的字符。一张双倍行距的页面通常是 1 英寸 3 行，或者一页有 27 行。一个通用的字体格式是每英寸 10 个字符，或者每行 65 个字符。如果空白内所有空间都被充分利用，那么总共有 8 × 27 × 65=14 040 位。这当然夸大了每页纸上的字符总数，因为实际上不可能每行都包含相同的字符数，特别是在一个段落的开头和结尾处。而且，并非一个文本的所有页都是满的。因此，若取整数，比较公正的估计应该是每页 10 000 位（每页 1250 个字符）。如果使用 Unicode 编码取代 ASCII-8 或 UTF-8，则每页 20 000 位是合理的估计。

对于通过电话线使用拨号连接的住宅用户，他们使用的是速度相对较慢的调制解调器，其传统的信道容量是 56 000bps。因此，它将占用大约 0.18 秒的时间来传输用 ASCII-8 或 UTF-8 编码的页；占用大约 0.36 秒的时间来传输用 Unicode 编码的页。如果居民有一个平均传输速率可达 400K 比特每秒的 DSL 连接的话，只需占用 0.025 秒的时间来传输一个 ASCII-8 编码的页面，只需 0.05 秒的时间来传输一个 Unicode 编码的页面。当住宅用户有一个平均传输速率可达 750Kbps 的线缆调制解调器时，只需 0.013 秒来传输 ASCII 编码的页，只需 0.026 秒的时间来传输 Unicode 编码的页。可以看出，用通信线路来传输一个固定大小的数据文件所需要的时间是由文本到二进制的转换体系和连接传输速率两者决定的。企业必须能够估计在一段特定时间内（如每秒、每分钟、每小时等）所需传输的数据量总和，从而获知对通信线路的容量需求。

这些绝对不是整个故事。例如，利用数据压缩技术可以使得只需比数据原有格式更少的位数来传输这些数据。在数据压缩中使用无损耗压缩算法，因为它可使终端设备接收到发送

者发送的字符和符号的精确副本。Lempel-Ziv 编码算法是在数据存储和数据网络通信中应用最广泛的无损耗数据压缩体系。例如，在 Lempel-Ziv 算法使用中，被压缩的文件以 .zip 为后缀名并可以作为邮件附件进行传输。数据压缩算法可被大部分类型的调制解调器支持，包括拨号器。例如，V.44 是数据压缩的一种 ISO 标准，它使用 Lempel-Ziv 编码来压缩通过通信线路传输的数据流。表示原始数据所需的“被压缩”位的数目取决于所传输数据的内容，但是当 V.44 使用时缩减率平均可达 6 : 1。

使用数据压缩算法可以帮助业务高效地利用通信线路。然而，对于面向数据的许多信息源，应该考虑的另一个重要因素是所需要的反应时间。在某些例子中，业务能够对数据改变做出快速反应是很关键的。当需要快速反应时，数据传输和接收过程中漫长的延迟就不能允许了，企业网络基础设施必须提供足够的容量和传输速率来确保充分的响应时间。反应时间和与其相关的数据传输问题在本章后续部分将有更深入的讨论。

网络化含义

为了支持以数据为中心的业务应用，所需要的网络和基础设施的需求将根据生成、传输和存储的数据种类和容量的不同而有很大变化。我们将在第 3 章中开始考虑这些需求。在许多例子中，确保这些数据能够被安全地传输和存储也是很重要的。当传输数据时，广泛采用加密技术来保护数据，而且重要的业务文件经常以加密形式来存储。加密技术将在附录 J 中讨论。

2.3 图像

图像服务可以支持个人的图片、图表和图样的通信。业务中使用的基于图像的应用包括传真、计算机辅助设计、电子打印（e-publishing）、在线（Web）打印和医学成像等。许多信息工作者和用户都有配备相机功能的智能手机，可以使用短信服务或者电子邮件的附件功能来保存或传输图像。用手机拍摄的图片可以上传到社交媒体网站（例如 Facebook）上。当企业网络越来越需要来处理大量的图像信息时，必须做出明智的选择，以便确保有充分的基础设施来高效地处理这些类型的文件。

把布置成像系统所需的要求作为一个例子，我们来考虑医学成像传输需求。表 2-1 总结了不同医学图像类型的传输影响 [DWYE92]。另外，根据每个图像所占的位数和每次测试中的图像数，该表给出了 3 种标准数字传输速率下每次测试所需的传输时间：DS-0=56Kbps、DS-1=1.544Kbps，以及 DS-3=44.736Mbps。

表 2-1 数字放射学图像的传输时间

图像类型	每个图像的兆字节数	每次测试的图像数	DS-0 时间 / 测试（秒）	DS-1 时间 / 测试（秒）	DS-3 时间 / 测试（秒）
计算机合成 X 线断层摄影术（CT）	0.52	30	2247	81	3
核磁共振成像（MRI）	0.13	50	928	34	1
数字血管造影法	1	20	2857	104	4
数字 X 光间接摄影法	1	15	2142	78	3
超声波	0.26	36	1337	48	2
原子核药物	0.016	26	59	2	0.1
计算机合成 X 射线照相术	8	4	4571	166	6
数字电影	8	4	4571	166	6

注：DS-0=56Kbps; DS-1=1.544Mbps; DS-3=44.736Mbps

再一次使用压缩技术。如果我们允许一些很难被感觉到的信息损失，我们可以使用有损耗压缩技术，该种技术可以以大致 10∶1 ～ 20∶1 的比例来压缩数据。另一方面，医学成像中有损失耗压缩往往是不被接受的。使用无损耗压缩技术，这些应用的压缩比例只能达到 5∶1 以下。PNG（可移植网络图像格式）和 GIF（图像交换格式）是只使用无损耗图像压缩算法的图像文件格式的例子。TIFF（标签图像文件格式）和 MNG（多图像网络成像格式）可支持有损耗和无损耗的图像压缩技术。

2.3.1　图像表示

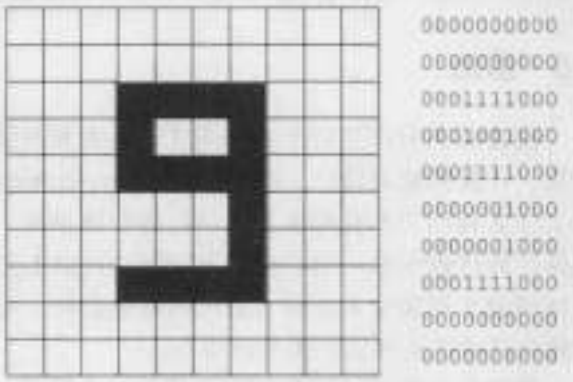
现在有很多种技术可以用来表示图像信息，可以分为两大类：向量图形和光栅图形。

向量图形：图像表示为直线和曲线元素的组合。简单对象（例如，矩形和椭圆），以及更复杂的对象可以定义为线段的组合。

光栅图形：图像表示为一个称为像素[⊖]的二维点阵。这里，像素是组成数字图像的最小的单个元素，最简单的形式中每一个像素点为黑点或白点。该种方法不仅应用于计算机图像处理技术，也可应用于传真技术。

本书中的所有图片均由运用向量图形的图形包（Adobe Illustrator）来生成，向量图形涉及使用二进制代码来表现物体的种类、大小和方向。在所有这些情况中，图像都是以二进制数值集合来表示和存储，而且可以用数字信号来传输。

图 2-3 给出一个使用向量光栅成像的 10×10 的简单图像，这个图像可能由传真生成或者由具有光栅扫描功能的计算机生成。这个图像的 10×10 的表现方式很容易被转换为 100 位的编码。在该例子中，每个像素由一个显示黑点或白点的单个位来表示。如果每个像素用多个位来表示，即代表灰度级别，则一个灰度图像就可生成。图 2-4 显示使用 3 位灰度产生 8 个灰度级别，范围从白色到黑色。灰度也可用于向量图形中，以便定义线段或者封闭物体内部（例如矩形）的灰度。



a）图像　　b）二进制代码

图 2-3　100 像素的图像及其二进制代码



图 2-4　8 级灰度

图像也可以用颜色来定义，针对该目标可用的方案有很多。一个例子是 RGB（红－绿－蓝）方法，其中每个像素或图像区域用 3 个值来定义，每个值可以代表一种颜色。这个 RGB 方法利用了一个事实，即很大比例的可见色谱都可用红色、绿色、蓝色以不同比例或程度的混合表现。3 种颜色中每种颜色的相对大小决定了实际合成的颜色。

彩色图像是如今企业网中传输的最常见的图像类型，并且一个图像文件中可表示的不同颜色的数目是由代表每个像素的位数决定的，或者称为位数每像素（bpp）。使用单个位来

⊖ 像素或图像元素是能够分配灰度级别的数字图像的最小元素。同样，像素是图像的点矩阵表示中单个点。

表示一个像素的图像称为 1bpp 图像，其局限于代表黑色或白色的两种颜色。一个 2bpp 图像可以表现 4 种颜色，3bpp 图像可以支持 8 种颜色，8bpp 图像可以支持 256 种不同的颜色，24bpp 图像可以支持 1680 百万种颜色。

传输图像的分辨率也与用来表现图像的像素数目相关。今天，包括安装在智能手机上的数码相机，都可以拍照由百万像素生成的图片。1 兆像素（MP）等于 100 万像素，并且许多相机拥有 3.1MP 甚至以上的分辨率。3.1MP 等于 2048 × 1536 的像素阵列，如果用 3 字节（24 位）来代表一个像素，则需要超过 1830 万位来对 3.1MP 彩色图像或照片图像进行数字化。

2.3.2 图像和文档格式

对于光栅扫描的图像，最广泛使用的格式是 JPEG。联合图像专家组（JPEG）是 ISO 和 ITU-T 之间的合作标准。JPEG 已经针对光栅扫描图像的压缩开发了一套标准，包括 8 位灰度和 24 位颜色。JPEG 标准是针对通用目的而设计的，它满足很多领域的需求，例如桌面打印、图像艺术、报纸电报照片传输和医学成像。JPEG 适合于高质量图像，包括相片，而且它被广泛应用于照片图像的编码。另一种在 Web 上经常见到的格式是图像交换格式（GIF），这是一种可以最多表现 256 种颜色的 8 位颜色格式，而且对具有相对狭小的颜色范围的非相片图像很有用（例如，公司徽标（logo））。表 2-2 比较了这些格式和其他比较受欢迎的格式。

表 2-2 常见图像文件格式的比较

类 型	文件扩展名	压缩算法	主要应用 / 用途	公司或机构
图像交换格式	.gif	LZW 算法	单调颜色图像、动画	CompuServe
联合图像专家组	.jpg	多种有损耗算法	照片图像	联合图像专家组
可移植网络图像格式	.png	无损耗算法	GIF 的替换	万维网联盟
原始底片	多种格式	没有	高端数码相机	个人设备制造商
标签图像文件格式	.tif	多种或没有	文件成像、扫描	Adobe 系统有限公司
Windows 位图	.bmp	没有	屏幕显示	微软公司

TIFF（.TIF）文件被商业印刷和出版机构广泛使用。这是存储 / 存档重要文件的一种可选格式，并且当其无损耗压缩选项被启用时，该格式对于高分辨率图像和高质量图像、LOGO、艺术线条和文件都是非常出色的。它可以支持 24 或 48 位颜色以及 8 或 16 位灰度。与其他图像格式相比，TIFF 文件非常大，因此在 Web 页面中必然不会被采用，因为 TIFF 文件可能会降低下载速度。

PNG（可移植网络图像格式）可以支持与 TIFF 相同的颜色和灰度范围。它使用无损耗 ZIP 压缩技术，并且类似于 TIFF，它可以用来存储或存档照片的高质量图像、LOGO、图片、文档和数据的主要备份。PNG 文件平均比 TIF 文件小 25%，比 GIF 文件小 10% – 30%。

有两种比较常用的文件格式适合于包括文本和图像在内的文件。便携文件格式（PDF）在 Web 上被广泛使用，实际上所有操作系统均有可用的 PDF 阅读软件。Postscript 是一种页面描述语言，可以嵌入许多桌面打印机和所有高档打印系统中。

2.3.3 网络化含义

图像信息所使用和通信的各种配置与文本和数字数据所使用的配置基本上没有什么不同，主要的不同之处在于数据的容量。正如之前提到过的，一页文本包含大约 10 000 位的 8 位字母数据，一个高质量的个人计算机屏幕的位图需要超过 200 万位（例如，对于

640 × 480 × 256 视频模式）。对于简单的黑白图像，一个每英寸 200 点分辨率（足够大的分辨率但未必是高分辨率）的传真页面针将生成 400 万位，对于灰度或彩色图像则需要多得多的位数。因此，对于图像信息，在计算机上呈现需要巨大数目的位数。

呈现一个图像所需的位数可以通过图像压缩技术来减少。在典型文档中，不管它包含文本还是图片信息，图像的黑白区域都是趋向于集中的。这个性质可以用来以一种更简明的方式来描述黑白模式，而不是简单地提供一列黑色和白色的值，每一个值代表图中每一个点。压缩比（未压缩图片大小与压缩图片大小的比值）从 8 ~ 16 都是可以达到的。

即便使用了压缩技术，图像信息中需要传输的位数还是很大的，特别对于彩色图片。与往常一样，有两点需要考虑：响应时间和吞吐量。在某些情况下，例如 CAD/CAM（计算机辅助设计 / 计算机辅助制造）应用，用户可以通过通信线路实时操作图像。如果用户的计算设备地理上是与 CAD/CAM 服务器分开的，那么 WAN 链路必须有足够的容量来保证充分的响应时间。对于其他业务应用，例如传真，几秒甚至几分钟的延迟通常是没有关系的。然而，商业通信设施仍然需要足够大的容量来跟上传真传输的平均速率。不然的话，当积压越来越多时，设备的延迟会随着时间增长。

对于某些类型的图像传输而言，安全性是一个重要问题。例如，在美国，医学图像的传输必须遵从 HIPPA（健康保险携带和责任法案）的要求。这通常意味着设备之间图像传输必须发生在安全链路上，通常要求在传输之前加密图像。在发送端和接收端处加密和解密文件是额外增加的处理步骤，且其对响应时间会产生负面影响。许多金融的交易也要求加密，包括一些在银行 ATM（自动柜员机）终端上的交易。有些 ATM 机器支持支票存款，因此在这些机器上存储和传输支票图像必须根据银行法律和规定来加密。

2.4 视频

视频应用要求能及时承载图片序列。本质上，视频使用光栅扫描图像的序列。这里，若从观众（终端）的电视或计算机显示监控器角度将数据进行特征分类，比从视频摄像机所记录的原始现场（来源）角度，简单很多。

视频可以用模拟或数字视频录像机来拍摄，这些拍摄的视频可以用连续的（模拟）或离散的（数字）信号来传输，可以被模拟或数字设备接收，可以以模拟或数字格式存储。不用说，有关视频拍摄、传输、显示和存储的所有可能性是令人困惑的。例如，认为 HDTV（高清晰度电视）系统是数字系统的消费者也许会因得知日本 HDTV 使用模拟信号进行广播这一事实而感到惊讶。

最初的电视和计算机监视器采用阴极射线管（CRT）技术，现在仍然有很多 CRT 显示设备在使用中，并且在未来的一段时间内仍会使用。CRT 监视器实际上是使用一个电子枪在屏幕上“画”图的模拟设备。电子枪发射电子束，从左到右和从上到下扫描屏幕表面。对于黑白电视，任一点产生的照度（从黑到白的级别）与经过该点时电子束的密度成正比。因此，任何时刻根据密度的模拟值电子束在屏幕上的那点产生预想的亮度。进一步，当电子束扫描时，模拟值发生变化。因此视频图像可以当作随时间变化的模拟信号。

图 2-5 描绘了扫描过程。在每根扫描线的末端，电子束很快扫描回左边（水平折回）。当电子束到达底端时，很快扫描回底端（垂直折回）。在回扫间隔内，电子束是关闭的（空白的）。

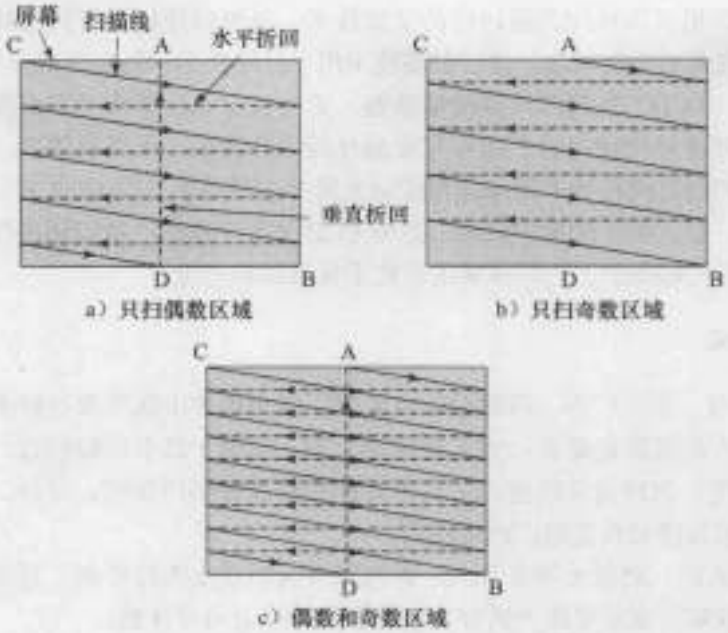


图 2-5 视频交错扫描

为了达到足够的分辨率，电子束在每秒 30 次屏幕完全扫描的速率下总共产生 483 条水平线。测试表明，这个速率会产生一种闪烁的感觉而不是平滑的运动。为了在不增加带宽需求的前提下提供不闪烁的画面，一种称为**交错**（interlacing）的技术投入使用。如图 2-5 所示，奇数扫描线和偶数扫描线分开扫描，奇数区域和偶数区域在连续的扫描下交替变换。奇数区域是从 A 到 B 扫描，偶数区域是从 C 到 D 扫描。在扫描 241.5 条线之后，电子束到达屏幕最低线的中间。在这点上，电子束被快速重定位在屏幕顶端，然后在屏幕最高可见线的中间重新开始，并产生与原有集合交错的额外的 241.5 条线。因此，屏幕每秒刷新 60 次而不是 30 次，且不会发生闪烁现象。

虽然对于黑白 CRT 电视和显示器只需要一个电子枪，但彩色 CRT 需要 3 个电子枪。第一个负责在屏幕上打出红色的荧光点，第二个打出绿色的荧光点，第三个打蓝色的荧光点。这些电子枪实质上都使用上面描述的相同的扫描过程。在计算机监视器中，彩色图像分辨率可以通过控制电子束的位置和它们开启或关闭的速度来改变，这使得 CRT 可以产生大小可变的像素。计算机使用视频卡，将计算机的数字信号转换为能被 CRT 电子枪使用并生成图像的模拟信号。

2.4.1 数字视频

数字视频这个术语是指以数字形式来捕获、处理和存储视频。如果模拟视频摄像机信号被数字化后以数字形式传输或存储，它也可认为是数字视频。然而，这个词现在主要应用于视频内容，指最初用数字视频设备捕获的视频内容。

数字视频摄像机可以数字化地捕获移动的图像。实质上，这可以通过以每秒至少 30 帧的速度拍摄一系列数字照片来实现。典型地，其分辨率是远远小于数字照相机的分辨率，与传统的个人计算机屏幕的分辨率一致。数字视频摄像机的低端是网络摄像机（Webcam），它们的低分辨率可以调整以便匹配网播（Webcasting）和视频消息的需要。

数字视频摄像机可以使用之前讨论的交错技术，也可以使用逐行扫描技术。在逐行扫描中，每帧的所有线都被顺次画出。逐行扫描技术用于计算机显示器和大部分 HDTV 机制中。

液晶显示器（LCD）电视和计算机显示器，更为人所知的平板和平板屏幕监视器，都是数字设备。这些屏幕使用很薄的中间夹有液晶材料的玻璃夹层来显示图像，电流使得液晶材料的分子改变它们的直线行列来阻塞或者传输光线并生成图像。在 LCD 显示屏上，每个像素是由红色、绿色、蓝色的子像素组成的。因为 LCD 是数字设备，所以通过帮助保证无信号丢失或损坏地捕获和传输图像，它们非常适合数字视频源和传输。

2.4.2　网络化含义

随着在线学习、在线广告、视频会议、监控、社交媒体市场以及各种多媒体应用的广泛使用，业务网络上的视频流量正以惊人的速度扩展。如第 1 章中所提到的，通过统一传输和其他实时协作系统，视频会议的能力正在扩展到移动业务用户领域。另外，远程手术和其他远程应用也正在被保健机构更加广泛地使用。

正如之前提到的，图像文件非常大，而视频可以看成是图像序列。这说明除非采用压缩技术，否则实时视频流量需要庞大的带宽来确保足够好的用户体验。

例如，用于视频会议的黑白电视信号可能有每 1/30 秒 360 × 280 像素的帧分辨率，并且有从黑色到灰色到白色的强度变换，色度由 8 位表示。这与没有经过压缩的大约 250Mbps 的原始数据速率相一致。为了增加颜色，比特率（bit rate，也称为位速率）可能会增长 50% 甚至更多。表 2-3 给出了 3 种常见的视频类型的采样速率，表中仅给出了亮度的速率，因为颜色用 3 种格式来区分处理。极端情况下，没有经过压缩的高清晰彩色电视需要大于每秒 1 吉位的速率来传输。

表 2-3　数字电视格式

格式	时空分辨率	采样率（MHz）
CIF	360 × 288 × 30	3
CCIR	720 × 576 × 30	12
HDTV	1280 × 720 × 60	60
HDTV RGB	1920 × 1080 × 60	60

在图像中，可以使用有损耗压缩技术。而且，可以加以利用如下事实：邻近帧的视频场景通常是非常相似的。在基本层面，有损耗视频压缩算法分析视频流，并丢弃那些不被观察者察觉到的信息。使用从 20 : 1 ~ 100 : 1 的压缩比可以达到合理的质量。

离散余弦变换（DCT）是存在于 JPEG、MPEG 和 H.263 视频文件格式中的视频压缩算法，它以有规律的间隔进行图像采样，分析该图像的频率组成并丢弃不会影响人类眼睛感知图像方式的频率。因为 JPEG 在图像文件中也可以使用，所以在前面章节中已有介绍。动态图像专家组（MPEG）是一个致力于制订数字音频和视频格式标准的 ISO/IEC 工作组，有些 MPEG 标准已被广泛使用，这些标准包括：MPEG-1（针对移动图片和音频）、MPEG-2（针对数字电视机顶盒和 DVD 压缩）和 MPEG-4（针对多媒体和 Web 压缩）。H.263 是针对双向视频通信（视频会议）的 ITU 标准，其是否为最重要的 VTC 标准还存在争议，但它在统一通信系统中得到广泛支持。

使用基于 IP 协议的网络（包括因特网和专用内部网）进行视频传输，对于企业来说越来

越重要。这种传输类型被认为是视频流或者 TVoIP（基于 IP 的电视）。TVoIP 对企业网络施加了重担，但同时也带来了很大的好处。作为一项免费的或订阅的基于云计算的电视服务，它对 IPTV（付费电视）提供了一个可选项，可以促使像 AT&T 这样的提供商对基础设施的更新进行投资。IPTV 和 TVoIP 都表明，在 IP 网络上的路由视频流量是未来的发展方向。因此，企业网络面临的主要挑战是如何升级 IP 网络以便有效支持视频传输，并给其他业务传输需求提供足够的服务质量。

2.5 性能度量

2011 年由 ABI 研究所开展的调查报告显示，2012 – 2016 年数据流量每年将以 50% 的速率增长，其中视频流量的增长是导致其增长的因素之一 [NG11]。预计每年的总容量在 2016 年将超过 6000PB，而且视频和电视流量将超过其他（如万维网和因特网）形式的流量。预计移动连接的无线流量在此期间将以接近的年度速率增长。企业将继续面临挑战，需要容纳其网络上不断增长的流量并满足工作者、用户和业务伙伴的需求。本节将考虑企业网络上与业务性能相关的 3 个主要因素：响应时间、体验质量和吞吐量。

2.5.1 响应时间

用户有效利用业务应用的能力经常受到应用与用户之间交互的速度的控制。如今的业务用户越来越需要多任务和在多个任务中同时工作。例如，一个知识工作者可以在接电话的同时撰写邮件并检索数据库记录。如果计算机应用的反应很慢，那么多任务业务用户将会把注意力集中在另一个应用上而不是那个响应慢的应用。有更多的证据表示，用户对于反应慢的计算机应用的耐心度在逐渐降低。用户越来越希望人机交互的应用能够提供即刻响应，而不能忍受那些不能提供即刻响应应用。要满足这样的用户要求，对于企业网络管理者而言是一个持续的挑战。

响应时间是指系统对给定输入做出反应所需要的时间。在人机交互事务中，响应时间定义为用户最后一次键盘敲击和计算机给出显示结果的开始时刻的时间差。对于某些类型的业务应用，需要有稍微不同的定义。总的说来，响应时间是指系统对用户要求完成某个特定任务做出反应所需的时间。

理想地，一个人总是希望任何应用的响应时间都尽可能地短。然而，有个恒久不变的规律：越短的响应时间伴随着越高昂的成本。这个成本主要来自于两方面：

- **计算机处理能力**：计算机速度越快，响应时间越短。当然，增长的处理能力总是意味着增长的成本。
- **竞争需要**：对某些应用提供快速的响应时间可能会使其他应用处于不利地位。

因此，对于某个应用，达到给定的响应时间标准的商业价值应通过为达到这样的响应时间而需付出的成本代价来评估。

在客户机 / 服务器网络架构中，计算处理能力是服务器和客户机计算设备之间的网络连接两端的问题。服务器和客户机都趋向于更快的处理能力发展，而且随着服务器和客户机设备变得越来越快，更需要网络能力来处理多应用功能所施加的要求，这一需求是决定假定业务应用响应时间的主要因素。

基于 [MART88]，表 2-4 列出了响应时间的 6 种大致范围。当要求响应时间小于 1 秒时，

可能会引起网络设计的困难。要让企业提供的网络设施能够满足所有的应用都有小于1秒的响应时间，这是不太可行的。要做到这些的代价是被禁止的。因此，业务网络设计者经常会根据重要性将应用进行优先级排序，并将企业网络设计成保证关键任务的应用具有快速的响应时间，即便这意味着牺牲了一些不太重要应用的响应时间。服务质量（QoS）机制经常用来支持重要业务应用的适当性能，特别是实时视频和声音应用。

表 2-4 响应时间范围

大于 15 秒 这几乎宣布谈话类交互应用不可能完成。对于某些类型的应用，某些类型的用户可以容忍坐在终端前等待回复一个简单的询问超过 15 秒。然而，对于一个比较繁忙的人，超过 15 秒的束缚是不可忍受的。如果发生这样的延迟现象，系统应设计成用户可以转向其他活动并在晚些时候再请求响应
大于 4 秒 对于要求用户在短时间记忆（用户的记忆，不是计算机内存）中保留信息的谈话，这个响应显得有点长。这些延迟将会很大地妨碍问题解决过程以及组码数据输入行为。然而，在完成一段漫长的输入之后，4 – 15 秒的延迟也就可以接受了
2 – 4 秒 超过 2 秒的延迟会阻碍用户完成一个需要高集中度的任务。当用户全神贯注于或投入大量情感于他所做的事时，2 – 4 秒的等待时间也会变得惊人地漫长。需要再次说明的是，该范围内的延迟对某些交互行为是可接受的
小于 2 秒 当用户需要通过某些响应来记忆信息时，响应时间必须很短。需要记忆的信息越是细节化，越是需要响应时间绝不能超过 2 秒。对于复杂的交互行为，2 秒代表重要事件的响应上限
亚秒响应时间 某些思考密集型工作，特别是图像应用，需要非常短的响应时间来保持用户长时间的兴趣和注意力
1/10 秒响应时间 按一个键并观察该字符在屏幕上的显示或者用鼠标单击一个屏幕目标的响应时间必须是非常及时的——在行为发生后小于 0.1 秒。如果设计者要避免应用中的一些陌生语法组合（命令、记忆、标点符号等），则与鼠标之间的交互行为需要极为快速的交互

很多研究已证明，快速的响应时间是保证使用人机交互应用的工作者生产效率的关键[THAD81；SHNE84；SEVC03]。这些研究表明，当计算机和工作者以一个可以保证任一方都无需等待另一方的步调进行交互时，生产率会显著提高，而且表现出来的工作质量也会提高。生产率和效率获得增长意味着在计算机上完成工作的所有业务开销得到了减少。

对于大部分人机交互应用，过去被广泛接受的一个相对比较慢的响应时间，上限是 2 秒，因为人们在思考下一个任务。然而，现在看来似乎随着响应时间的缩短，生产效率得到了增长。通常，一个业务应用的响应时间应该越快越好。然而，确保系统不至于反应过快使得用户无法跟上也是很重要的。例如，如果对一个用户行为的响应没有被展现得足以使用户可以读取或者做出反应，那么由快速的响应时间而获得的潜在生产效率是不可实现的。

如今，如果应用在 0.1 秒甚至更短的时间内做出响应，则用户认为该系统可以做出及时的响应。用户可以意识到 1 秒的延迟，但还不至于打断他们的思考过程。因此，0.1 – 1 秒的响应时间比较适合交互式的业务应用。当延迟超过 10 秒时，工作者开始失去注意力，并且在等待系统完成时经常会希望能做其他任务。在这些例子中，在应用中加入一个完成百分比或者进度指示器来告诉用户还需要等多久（且使得等待过程不那么痛苦）是很明智的做法。

响应时间是度量执行在线事务的工作者生产效率的重要决定因素。一个事务包括来自于

计算设备的用户命令和系统的回复，它是在线系统用户的基本工作单元。响应时间可以分为两个时间序列：

- **用户响应时间**：用户收到一个命令的完整响应和输入下一个命令之间的时间间隔，通常称为思考时间（thinktime）。
- **系统响应时间**：用户输入命令和一个完整响应显示在计算设备上的时间间隔。

作为减少的系统响应时间影响工作者生产效率的例子，图 2-6 给出一项使用 CAD 图像程序来设计集成电路芯片和电路板的工程师所执行的研究结果 [SMIT88]。每个事务包括工程师使用某种方式改变屏幕上显示图像的命令。结果表明一旦系统响应时间降到 1 秒以下，工程师执行事务的次数会急剧增加。正在发生的事情是，如果系统响应时间缩短，则用户响应时间也会缩短。这与短期记忆和人注意力持续期的影响是相关的。

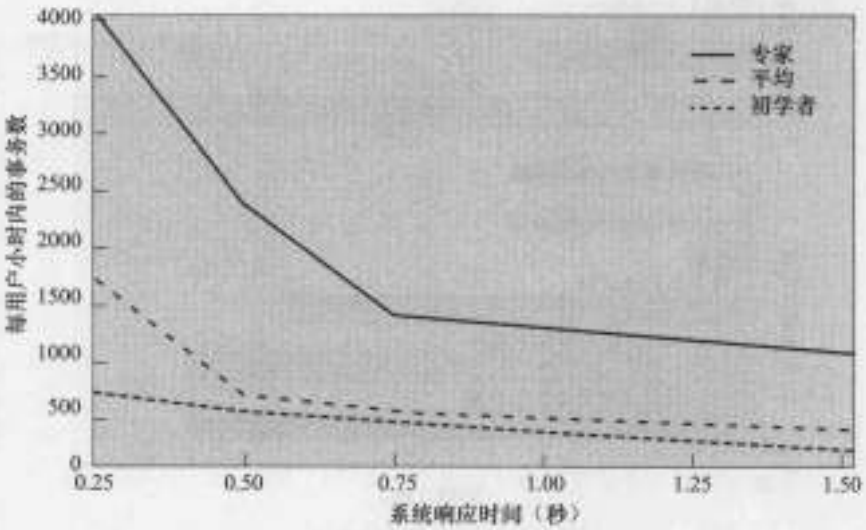


图 2-6 高性能图形的响应时间结果

快速的响应时间对于某些类型的业务信息系统是更重要的，尤其是对于交互处理系统而言是很关键的。管理信息系统和决策支持系统的输出通常是报告或模型训练的结果。在这些情况下，快速的周转时间是可取的，但不是必需的。

今天，企业资源管理（ERP）系统对于大型企业而言是最核心的事务处理系统，它们在中小型企业中也越来越流行。ERP 用户需要快速的事务响应时间，不管与他们交互的系统就在现场还是在云端。不管他们是在自己办公室的计算机桌面上还是在移动终端设备上与 ERP 系统进行交互，快速的响应时间都是需要的。对于任何集成的企业系统，包括用户关系管理（CRM）系统和供应链管理（SCM）系统，业务用户都期望有快速的响应时间。

虽然业务用户对电子邮件和视频会议等应用能够有更多的耐心，但大致趋势是大部分业务应用（不是所有的），拥有越来越快的响应时间。这个趋势的业务网络暗示是很清楚的：如果一个网络将交互用户的计算设备连接到应用服务器且该应用需要很短的响应时间，那么该网络必须以与该响应时间相兼容的方式来设计。因此，如果一个事务处理应用需要 1 秒的响应时间，并且应用服务器对用户询问生成回复的平均时间为 0.75 秒，那么该网络必须设置成可以确保用户请求和服务器回复的传送总时间不超过 0.25 秒。

响应时间非常重要的另一个领域是通过 IP 网络（包括因特网、外部网或企业内部网）给

业务用户发布应用[⊖]。下载并在用户屏幕上呈现一个 Web 页面所需要的时间是变化很大的。与其他业务应用一样，用户与交互式的基于 Web 的应用之间的交互受到响应时间的影响。特别地，有很快响应速度的基于 Web 的应用可以控制用户越来越多的注意力。

如图 2-7 所示，拥有 3 秒级别或者更高级别响应时间的 Web 系统可以保持用户很高的注意力 [SEVC96]。如果响应时间为 3 ~ 10 秒，那么某些用户的注意力就会丧失，而 10 秒以上的响应时间会使用户很沮丧，甚至直接中止这个会话。对于一个需要维护因特网网站的机构，大部分响应时间是由该机构控制之外的因素决定的，例如因特网吞吐量、因特网拥塞和终端用户的访问速率。在这些例子中，机构可以考虑保持页面上图片内容尽可能少，而重点通过文本来缩短响应时间。

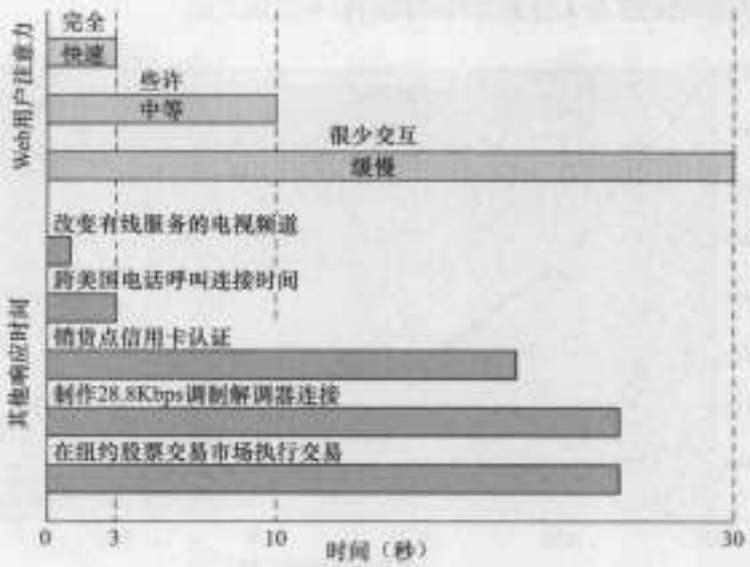


图 2-7　响应时间要求

2.5.2　体验质量

响应时间是用户对网络应用和服务的总体感受，是**体验质量**（QoE）的一项重要影响因素。QoE 是用户对网络应用或服务的整体感知的主观度量。QoE 和 QoS 不一样，但是它会因为 QoS 用于提高性能和用户参与应用或服务的程度而受到影响。QoE 是在终端用户计算设备上度量的，而且有很多网络元素可以降低服务质量，因为它是由终端用户（包括编码过程、广域网基础设施组件、企业局域网、家庭网络和用户计算设备等）来感受的。对于特殊网络应用或服务的用户而言，那些可以完善灵活性、安全性、成本、移动性和个性化的网络元素可能对 QoE 起到积极作用。

传输所有类型流量（音频、数据、图像和视频）的集中式 IP 网络不断增长的使用，使得 QoE 和用户对于网络应用和服务体验的其他度量的重要性越来越大。良好的 QoE 对于实时应用（如音频和视频）尤其重要。用户尤其对紧张的、模糊的、扭歪的音频和视频特别敏感，因为它们会降低用户对于应用或服务的体验。随着视频、音频和多媒体内容的不断增长，并且很

⊖ 内部网（intranet）是一个术语，用于指在公司组织范围内因特网技术的实现，而不是全球因特网的外部连接。在第 9 章中探讨这个主题。

快就能超越其他所有种类的网络流量，QoE 将成为业务网络设计的一个越来越重要的因素。

2.5.3 吞吐量

追求越来越高的传输速率的趋势使得对于不同服务（如宽带多媒体服务）的增长支持变得可能，这些服务曾经对于数字通信而言是很费力的。为了能有效利用这些新能力，企业必须能感知每项服务所施加于集中式企业网络的存储和通信的需求。与你在本章中看到的一样，网络应用和服务可以分为数据、音频、图像和视频，而不同种类的信息对于承载网络的需求也是各不相同的。图 2-8 给出了提供可接受的性能和用户 QoE 所需要的数据速率的指示[TEGE95]。

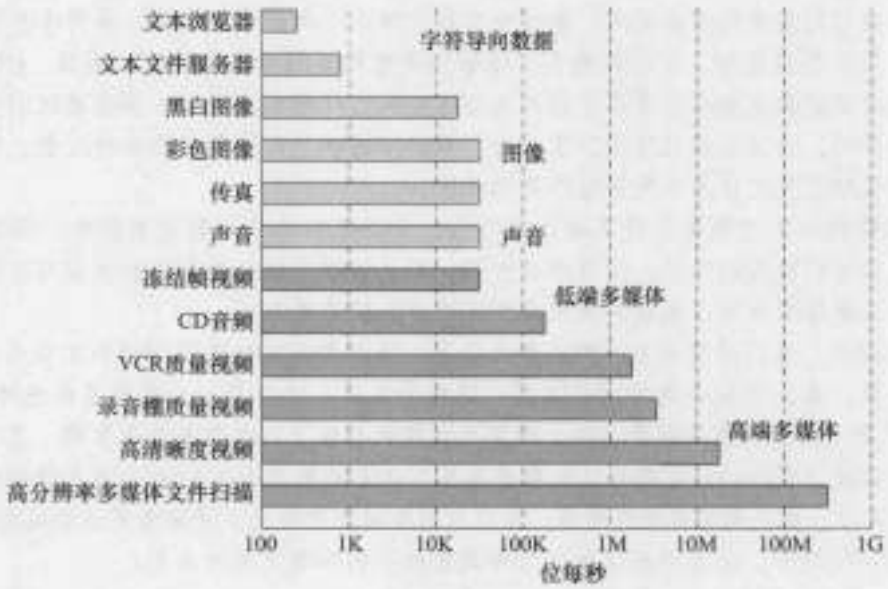


图 2-8 不同信息种类所需的数据速率

吞吐量在业务环境下有很多意义，包括指定时间段内的机器、进程、系统或过程的生产效率。在商业网络中，吞吐量是指通过单个通信信道或整个网络传输信息的平均速率。它可以认为是一个通信信道或网络的总体带宽容量，并且可以通过很多方式来度量，包括位每秒、字节每秒或数据包数每秒。在本书接下来的章节中，你将会了解到吞吐量会受到许多因素的影响，包括通信介质、介质访问控制协议、交换机和路由器能力、安全机制、网络拥塞、终端设备的配置和 QoS 机制的合理使用。

对集中式网络承载所有种类的业务应用（音频、数据、图像和视频）的依赖不断增大，已经使吞吐量成为企业网络设计中一个越来越重要的因素。对高吞吐量、改进的 QoS 和可觉察的 QoS（或 QoE）的需求驱动网络基本设施的投资和商业软件更新，增长的吞吐量可以帮助缩短响应时间和提高工作者的生产效率。因此，有很多原因可以解释为什么企业管理者关心如何确保企业网络提供足够的吞吐量来支持现有的和计划的应用及服务。

不断增加的对视频、图像和其他带宽占用应用的使用，使得公司投资基础设施更新来足够快地满足他们用户的期望越来越困难。在这些例子中，有一点很重要，就是企业需要做到能够区分网络流量需求的优先次序，以保证能给关键任务的应用及服务提供充分的带宽，在足够好的层面上运行。使用 QoS 机制来识别和标注那些高优先级的流量，从而使其可以在网

络中快速地传送，即便这会导致那些不重要的应用及服务的延迟。对音频、数据、图像、视频压缩算法和文件格式的合理使用可帮助达到足够好的网络服务和应用的性能。

吞吐量、响应时间和 QoE 都是与网络应用及服务的端到端传输有关的重要因素。这些是所有企业管理者都应该熟悉的概念，因为它们可以帮助提高工作者的生产效率和业务进程的效率。

应用注解

文件大小

图像文件大小是基于页面和颜色内容的信息量大小。高分辨率的彩色图片可以占据很大一块存储空间，声音和视频文件可能占用的存储空间更大。虽然音频文件不包含数据或颜色，但它们随着时间会变大。能改变音频文件大小的因素有长度、采样率和每个样本的位数。声音质量越好，文件就越大，传输该声音所需的带宽也越大。例如，CD 质量的声音比同样音乐的基本录音需要大得多的存储空间。视频本质上是一些随着时间变化的彩色图片的序列，所以这些文件是非常大的。帧速率描述了图像每秒传送的次数，而且这个值可以大幅地改变文件大小和传输所需的带宽。

数码相机的流行程度已经呈爆炸性态势，尤其是自它成为智能手机的一项常用功能之后。因为它们既可以照相，又可以录视频，所以稍微理解文件大小和类型可以帮助用户理解为什么数字照片可以迅速充满硬盘和可移动介质存储空间。

在开始时，我们必须决定所需达到的质量。高质量会减少我们对减小文件大小的可选项。下一步，我们选择合适的文件类型。依赖于应用，这将是一个很重要的选择。例如，在 Web 页面上使用很高的质量、很大的图片和视频会对下载速度有负面影响，尤其是通过较低速率的通信线路。这也是为什么要考虑那么多来最优化企业 Web 页面上的内容。通过调节图像大小、颜色内容或文件类型，可以大幅地减小文件大小并降低页面加载的时间。

作为一个例子，下表列出了基于信息类型的不同图像文件的大小。

信 息	文件类型	大 小
640 × 480 像素图像	24 位位图	900KB
640 × 480 像素图像	256 色（8 位）位图	300KB
640 × 480 像素图像	16 色（4 位）位图	150KB
640 × 480 像素图像	GIF	58KB
640 × 480 像素图像	JPEG	45KB

你可以看到，改变使用的文件类型和颜色内容对文件大小有很大的影响。这也难怪拍摄高分辨率的相片会导致很快就用完内存。使用有损耗压缩算法来修改图像或流来减小文件大小的缺点通常是需要牺牲一些质量。一旦质量受到了损害，如果没有原始文件那么是无法逆转的。对于某些应用，如电子制表软件和文字处理器，压缩算法是不能选择使用的，因为需要精确的副本来传输或存储。幸运的是，这种类型文件，仅仅只有文本，不会占太多空间。

网络通常是转换为数字图像和视频流的接收端。当更多的信息通过网络传输时，链路会过度利用，响应会变慢。IP 语音、流媒体、视频会议都会对性能问题有所影响。这也是为什么企业需要重新设计和升级他们的网络，以便适应这些变化，并对网络管理者适当施压，使其能够提供充分的网络存储空间和带宽。然而，一旦开始传输后，网络管理者也不能做很多来改变信息。在数据传输之前，通过采用合适的压缩算法和文件格式，某些网络利用和存储问题可以在它们开始之前就得以减轻。

2.6 总结

今天的企业网络承载许多类型的信息，这些信息可以方便地归类为音频、数据、图像和视频。集中式网络的广泛流行意味着这些类型的网络流量将一起享用通信线路和网络资源，即便是需要不同层次的带宽、吞吐量和响应时间来保证用户充分的体验质量。可以通过设置应用和服务的优先级，来确保那些对于业务而言比较重要的应用和服务有足够好的性能级别。视频和多媒体流量不断增长的容量使得企业需要重新设计他们的网络并投资更新基础设施。对压缩算法、文件格式和服务质量机制的合理使用，对于保证业务应用具有可接受的性能级别变得越来越重要，尤其对于基于 Web 的交互式应用。

案例研究 II：核心信贷联盟

这个案例研究涉及的主要概念有声音和数据网络：虚拟专用网（VPN）和云服务。有关该案例研究的更多细节，请参考 www.pearsonhighered.com/stallings。

2.7 关键术语、复习题和练习题

关键术语

analog（模拟）
ASCII（美国信息交换标准码）
audio（音频）
Centrex（中央交换机）
data（数据）
digital（数字）
image（图像）
interlacing（交错）
Lempel-Ziv（压缩算法）
lossless compression（无损耗压缩算法）
lossy compression（有损耗压缩算法）
Private Branch Exchange（PBX，专用分支交换）
Quality of Experience（QoE，感受质量）
quantization（量化）
raster graphics（光栅图像）
response time（响应时间）
throughput（吞吐量）
Unicode（统一字符编码）
vector graphics（向量图像）
video（视频）
voice（声音）

复习题

2.1 数字通信系统和模拟通信系统之间的区别是什么？
2.2 离散信息源和连续信息源之间的区别是什么？请分别举例说明。
2.3 简单描述为了通过数字传输系统来传输音频而需的“数字化”音频的过程。
2.4 对比无损耗压缩算法和有损耗压缩算法。
2.5 PBX 和托管式 IP-PBX 之间的区别是什么？
2.6 简单描述以下几个编码的特征：IRA、UTF-8、Unicode。
2.7 简单解释为什么无损耗压缩技术用于压缩数据（符号、数字、字符），实现数据的存储或传输。
2.8 什么是 Lempel-Ziv？什么是 V.44？
2.9 解释向量图像和光栅图像的基本原理。

2.10 简单解释 JPEG、GIF、TIFF、PNG 图像格式之间的区别。
2.11 对比 PDF 和 Postscript 文件格式。
2.12 描述交错技术和它在视频屏幕上防止闪烁起到的作用。
2.13 对比 CRT 和 LCD 显示器。
2.14 什么是数字视频?
2.15 什么是 DCT?
2.16 简单描述 MPEG 并识别几个广泛使用的 MPEG 标准。
2.17 什么是 H.263?
2.18 定义响应时间。
2.19 响应时间如何与工作者生产效率相关?
2.20 对于交互式应用,认为是一个可接受的系统响应时间是什么?
2.21 列出并简单描述影响响应时间的几个因素。
2.22 什么是 QoE?列出影响 QoE 的几个因素。
2.23 在业务网络环境中,吞吐量意味着什么?
2.24 对于企业网络而言,解释为什么吞吐量是一个越来越重要的问题。

练习题

2.1 做一些有关组织机构如何使用交互式语音应答系统(IVR)来提高业务过程的在线研究。写一篇小论文来讲述业务使用的 IVR 模式、实现 IVR 的商业原因,以及部署 IVR 所实现的益处。请包含一些案例。
2.2 做一些有关 IP-PBX 系统能力的在线研究。写一篇小论文来解释业务是如何从现有的 IP-PBX 系统的能力中获益,以及将来可能会增加的新能力。
2.3 公司的电话交互系统(PBX 或托管式 IP-PBX)数字化 8000 smp/s 的电话信道,使用 8 位来量化。电话交互系统通过相同的通信线路同时在 24 个电话信道上传输。
a. 所需要的每个信道的数据速率是多少?
b. 通信链路上 24 个信道的联合数据速率是多少?
c. 为了提供语音邮件服务,电话交互系统可以存储 3 分钟的音频信息,使用电话信道的相同数字化过程。为存储 3 分钟的语音邮件信息,需要多少 MB 的数据存储空间呢?
2.4 为了表示下述符号、字符或状态,需要多少个量化级别?
a. 大写字母表 A,B,…,Z
b. 数字 0,1,…,9
c. 256 种不同的颜色
d. 10 000 个汉字
e. 40 亿台计算设备
2.5 检查附录 D 中的 IRA 编码(mercury.Webster.edu/aleshunas/COSC%205130/Q-IRA.pdf)。
a. 给出字母 B、D、C、7 和 e 的 7 位编码。
b. 仍为问题 a 中的要求,但这次需给出包括一个奇偶校验位的 8 位编码。
2.6 《Encyclopedia Britannica》(不列颠百科全书)大约有 440 万单词。每个单词的平均字长是 6.3 个字符(包括单词中的字母和单词之间的空白和间隔)。
a. 百科全书里大概有多少字符?

b. 通过 1.544Mbps 速率的 T-1 线路来传输百科全书需要多长时间？如果是 51.84Mpbs 速率的光纤线路呢？如果是 40Gbps 速率的以太网线路呢？

2.7 一张 8.5×11 英寸纸上的图片被以每英寸 300 点的扫描器进行数字化。

a. 最终成像的可见分辨率是多少（每维的点数）？

b. 如果 8 位用于量化每个像素点，需要多少数据存储空间以不压缩的形式存储该图像？

2.8 当检查 X 射线时，放射线学者通常同时处理 4 ~ 6 个图像。对于一张 X 射线照片的可信数字表示，2048×2048 的像素矩阵经常使用每个像素 12 位的灰度密度。正如你所希望的，放射线学者不希望使用降低质量的压缩技术。

a. 12 位可以表示多少个级别的灰度？

b. 需要多少位可以表示一个简单的 X 射线照片？

c. 假设要将 5 条 X 射线通过一条 1.544Mbps 速率的 T-1 线路传送到另一边，不考虑经费开销需要多久可以传送到？

d. 假设我们希望根据要求，建立可以提供问题 c 的 5 条 X 射线的通信系统，也就是说，从这些 X 射线开始，我们希望可以在 2 秒内获得。满足该需求的最低信道速率是多少？

e. X 射线的下一代显示技术计划是 4096×4096 像素，12 位的灰度。当使用这样的分辨率时，问题 d 的答案是多少？

2.9 通常，医学数字放射性超声波研究由 25 个从全动态超声波实验中提取出来的图像组成，每个图像包括 512×512 个像素，每个像素是 8 位的强度信息。

a. 这 25 张图像共有多少位？

b. 然而，理想情况下，医生使用 512×512×8 位的帧，速率为 30fps（帧每秒）。忽略可能的压缩和开销因素，为保持这个全动态超声波需要的最小信道容量是多少？

c. 假设每个全动态研究包括 25 秒的帧，以不压缩的形式存储一个单一的研究需要多少字节的存储空间？

2.10 一个 24 位颜色深度的 800×600 图像需要存储在磁盘上。即使该图像可能包含 2^{24} 种不同的颜色，但只有 256 种颜色可以实际表现出来。这个图像可以用 256 个 24 位元素表的方式来编码，对于每个像素，其 RGB 值的索引在表中。该种形式的编码通常称为颜色查找表（CLUT）编码。

a. 以原始信息方式存储该图像需要多少字节？

b. 以 CLUT 编码方式存储该图像需要多少字节？

c. 使用这种简单的编码方式可以获得的压缩比是多少？

2.11 一个数字视频摄像机提供未经压缩的输出视频流，分辨率为 320×240 像素，帧速率为 30 帧每秒，用 8 位来量化每个像素。

a. 传输这些未经压缩的视频流需要多少带宽？

b. 存储 2 分钟的视频流需要多少数据存储空间？

2.12 做一些关于企业如何使用 TVoIP 来支持他们业务的在线研究。写一篇小论文来总结 TVoIP 的业务使用模式和用于保证可接受性能要求的网络基础设施的特征。请包含一些案例。

第 3 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

分布式数据处理

学习目标

通过本章的学习，读者应该能够：

- 描述与大数据相关的通信与基础设施问题。
- 描述集中式与分布式数据处理的区别，讨论每一种方式的优点与缺点。
- 定义和描述数据中心的特征以及形成数据中心发展的技术。
- 定义和描述客户机 / 服务器架构的特征。
- 描述应用服务提供商的角色与企业网络中的云计算。
- 描述不同形式的分布式应用与应用处理。
- 描述不同形式的分布式数据库。
- 讨论分布式数据处理的网络与通信含义。

在第 2 章中，我们探讨了一个机构对于信息的总体要求，并了解了有 4 种信息对于任何商业的竞争力至关重要：数据、声音、图像和视频。如今的机构正在获取、传送、存储和挖掘这 4 种类型中的有用信息。

在数据通信的历史中，正是数据（如第 2 章中定义的那样）决定了一个企业的策略。声音在过去被作为一个完全独立的要求来处理，而如今在很多机构中，它仍然以这样的方式被处理着。向数字传输的转移、网络设备和存储的使用以及灵活的传输协议（如 IP）等的应用，使得企业可以将声音、数据、图像和视频这 4 种信息整合到一起，从而提供性价比高的网络解决方案。

正如在第 2 章中讨论的那样，声音、图像和视频给企业网络带来了存储和传输上的挑战。如今，任何一种信息都可以在同一个融合网络上存储与传输。对于业务数据的定义也由传统的字母数字字符和符号拓展到了音频（声音）、图像和视频。最近，“大数据”这个新名词也开始流行于 IT、商业人士和软件销售的交谈中。

简单来说，**大数据**（big data）指的是所有一切可以让机构创造、操纵和管理超大数据集（以太字节、拍字节、艾字节等度量）的东西以及存储这些数据的设备。分布式数据中心、数据仓库以及云存储已成为如今企业网络中的常见方面。众多因素导致“大数据”和企业网络的融合，如持续下降的存储成本、成熟的数据挖掘和商务智能（Business Intelligence，BI）工具、政府政策以及法庭案件。其中法庭案件也使得机构开始存储大量的结构化与非结构化数据，如文档、电子邮件、语音邮件、短信信息以及社交网络数据等。其他被企业获取、传送和存储的数据源包括 Web 日志、因特网文档、因特网搜索目录、电话记录、科研数据和结果、军事监测、医疗报告、影像档案以及电子商务交易等。

随着遥感传感器、移动设备、照相机、麦克风、射频识别技术（Radio Frequency Identification，RFID）和相关技术的发展，越来越多的数据被收集起来，数据集变得越来越庞大。一些专家预测，每天有超过 25 000 亿亿字节的数据产生，而且大部分行业的专家认为数据

的种类、容量和速率将持续增长 [DOOL11]。

如今，融合网络和大数据正在渐渐改变着业务，进一步了解业务可能使用的各种数据处理系统可以帮助理解为什么会有这些改变以及改变是如何发生的。我们首先看看计算功能的组织中的两个极端：集中式与分布式数据处理。在大部分企业中，计算功能通常处在这两个极端中间的某处。通过研究这个范围区间，如分布式数据处理的优点以及数据中心的技术发展等，我们可以更清楚地知道如今业务所要求的通信及网络。我们思考企业网络怎样分配应用处理和数据，以及客户机 / 服务器架构怎样让云计算服务成为业务网络的常用组件。大数据和数据处理与通信技术的发展继续在企业网络中改变着集中式与分布式数据处理的平衡。

3.1 集中式与分布式数据处理

3.1.1 集中式与分布式组织

在企业网络中，数据中心是很重要的构件。**数据中心**是包含计算机系统和相关组件的设施，相关组件包括存储和通信系统。一个数据中心可以占有一幢大楼里的一个单独的房间，一个或多个楼层，甚至是整幢大楼。数据中心的大部分设备由堆在机柜上的服务器组成，一排一排的服务器形成一条条走道，可以通往每个机柜的头部和尾部。由于大型计算机和存储设备的大小可以与机柜相当，所以它们沿着架子安放。为了确保服务器和计算设备的正常运行，数据中心通常使用空调设备来控制湿度与温度。

如今的数据中心是由早期的大型计算机机房、计算机中心衍生而来的。由于早期计算系统的使用和维护很复杂，而且需要受控的环境来运行，所以它们通常安置在严格控制进出的计算机机房里，并且计算机机房里的工作人员和管理者也都受过特定的训练。直到计算机的体积越来越小且越来越容易使用和联网时，计算机才渐渐从数据中心走出，进入办公室和其他建筑中。如今，一系列因素共同将集中式数据中心再次带回人们的视野，这让我们回想起早期的计算中心和它们的集中式数据处理架构。

在**集中式数据处理**架构中，数据处理是由一个或一群计算机共同完成的，它们通常安置在设备服务中心中，有很大的体积和强大的功能。有些商业处理任务（如工资单的更新等）可以从头到尾地由中央数据中心的人员全部完成。其他的一些任务可能需要由不同数据处理中心的人员进行交互式访问来完成，比如说，一个数据输入功能（如库存更新等）需要由机构的各个站点的人员完成之后再将数据传送到数据中心，数据中心的计算机随后再将实际数据库进行更新。因此，在集中式的架构中，一个应用的数据处理并不在用户的计算设备上进行，而是由用户将数据传输到集中式数据处理设备上，再由那里的计算机上运行应用进行处理。

一个完全集中式的数据处理设备包含多项“集中”，主要包括：

- **集中式计算机**：一个设备中心中通常含有一台或多台计算机。历史上，大的机构通常有一个或多个大型计算机，而这些大型机的运行经常需要有空调、抬高的地面等特殊设施。较小的机构经常使用高性能服务器或中端系统来作为中央计算机。IBM 的 Power Systems 服务器产品线就含有中端系统。
- **集中式处理**：所有的应用程序都由位于中央数据处理设备的计算机来运行。这包括给全公司各部门使用的程序，例如工资单等，也包括支持特定业务部门特殊用户需求的一些应用，例如产品设计部门的用户需要与在设备服务中心服务器运行的计算机辅助

设计（Computer Aided Design，CAD）图像应用进行交互。

- **集中式数据**：大多数数据存储在设备中心的文件和数据库里，这包括机构中各业务部门共同使用的数据，如库存数据等，也包括特定业务部门独立使用的数据，例如市场部在数据中心可能有一个存储客户调查结果的数据库。
- **集中式控制**：数据处理或者信息系统主管负责管理设备中心。基于设备服务中心的规模和重要性，数据中心主管可以是中层管理者或者高层管理者。数据中心主管常常需要向由副总裁（例如，IT 服务部门的副总裁）或者首席信息官（Chief Information Officer，CIO）这些有董事会权力的人员汇报。某些情况下，数据中心主管可以直接向首席安全官（Chief Security Officer，CSO）或首席技术官（Chief Technology Officer，CTO）汇报，这些 CSO 或 CTO 职位在企业并购、信息使用与保护上有更大的权力。
- **集中式支持人员**：每个设备数据处理中心都有一名技术支持人员来运行和维护数据中心的硬件。此外，用来支持各部门共享和特定部门应用的编程与应用开发服务也与设备服务中心相关联。

集中式数据处理架构有一些吸引人的优势。在设备和软件的购买和运行上，可能由于规模的扩大而节约成本。另外，拥有集中式 IT 服务的机构一般更能吸引和留住高薪酬的编程人才来支持全公司的系统和战略型部门的特殊需求。数据中心主管可以掌控数据中心的硬件采购、推行数据质量的标准、设计和实施合理的安全政策。

图 3-1 概要介绍了美国德州达拉斯县采用的集中式数据处理设施 [CLAR03]。这个县的信息技术（Information Technology，IT）基础设施是与它类似规模的政府机构中很典型的一个案例，这个州的大部分应用程序和数据库都存储在数据中心中，并且数据中心由多台大型机和许多高端服务器构成。大型机用来运行司法体系特定的应用程序，而服务器用来支持县里公务员工作所需的各种数据库应用。

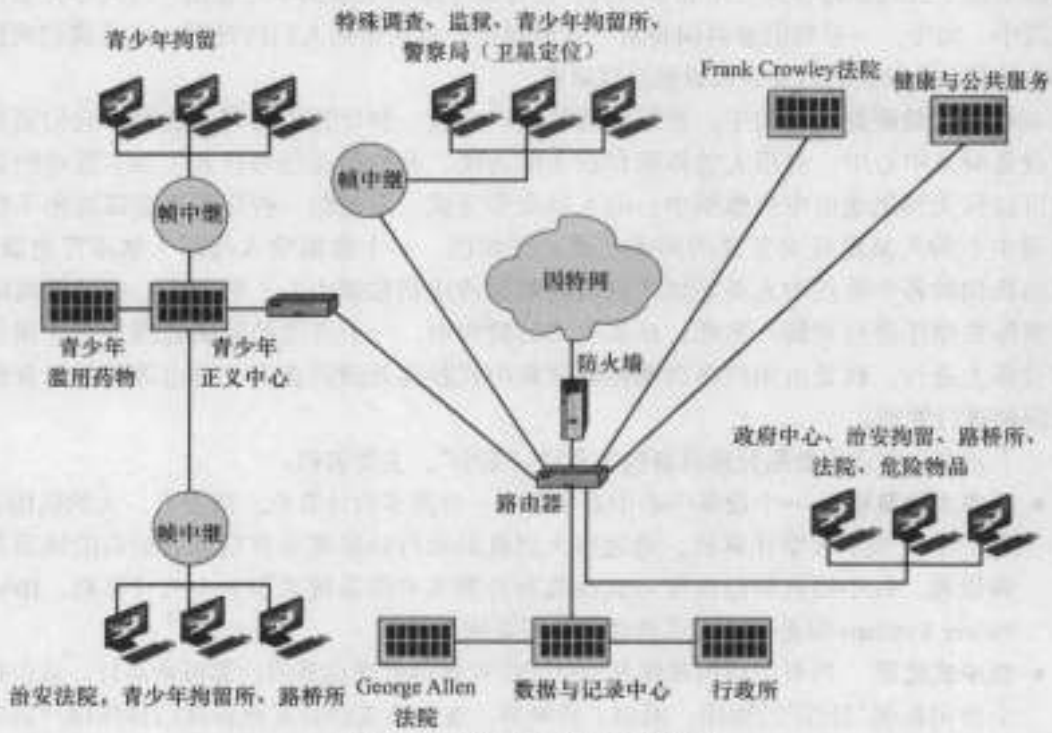


图 3-1　达拉斯县的信息系统架构

网络架构是星形（hub-and-spoke）配置的一个例子。在此结构中，有些点租用高速直通线路与数据中心的基准路由器相连，而其他站点使用专用帧中继广域网服务连接，这样的安排使得各点之间的通信传输成本和网络设备数量最小化。除此之外，数据中心还提供受防火墙保护的因特网连接服务。

这个集中式配置满足达拉斯县的众多目标。为了满足安全与隐私要求，达拉斯县发现，相比于将各种资源分配到不同的地理位置来说，这种集中式的数据中心与应用程序更容易受到保护。此外，县里的公务员需要对他们工作所需要的数据和应用程序拥有访问权限，这样的架构将所有的资源连接在一起，大大简化了网络管理。

数据处理设备采用**分布式数据处理**（Distributed Data Processing，DDP）策略，与集中式数据处理机构有不同程度的改变。当采用分布式数据处理策略时，将计算机（通常是小型计算机）分配到企业的各个部门，这种分配的目的是希望使得信息可以得到最有效的处理，不论是基于运营、经济还是地理因素的考虑。分布式数据处理设备一般包含一个中央数据中心和卫星数据中心，或者更类似于一个对等计算设备组成的团体。不论上述哪一种情况，都需要特定形式的互连，也就是说，系统中的不同计算机必须要互相连接在一起。正如所期望的，鉴于我们所提供的集中式数据处理的特性，DDP 设备也涉及计算机的分布、处理和数据。

分布式数据处理架构的一个简单例子是在佛罗里达州的 Carnival 游轮产品 Carnival Valor 豪华游轮上实现的系统 [KNAU05]。船上所用的网络（见图 3-2）是无线局域网（Wireless Local Area Network，WLAN），支持数据流和 IP 语音（VoIP，Voice over IP）。这个无线局域网通过卫星链路与因特网相连，与 Carnival 的专用广域网（Wide Area Network，WAN）相连，并与美国的公用交换电话网络（Public Switched Telephone Network，PSTN）相连接。

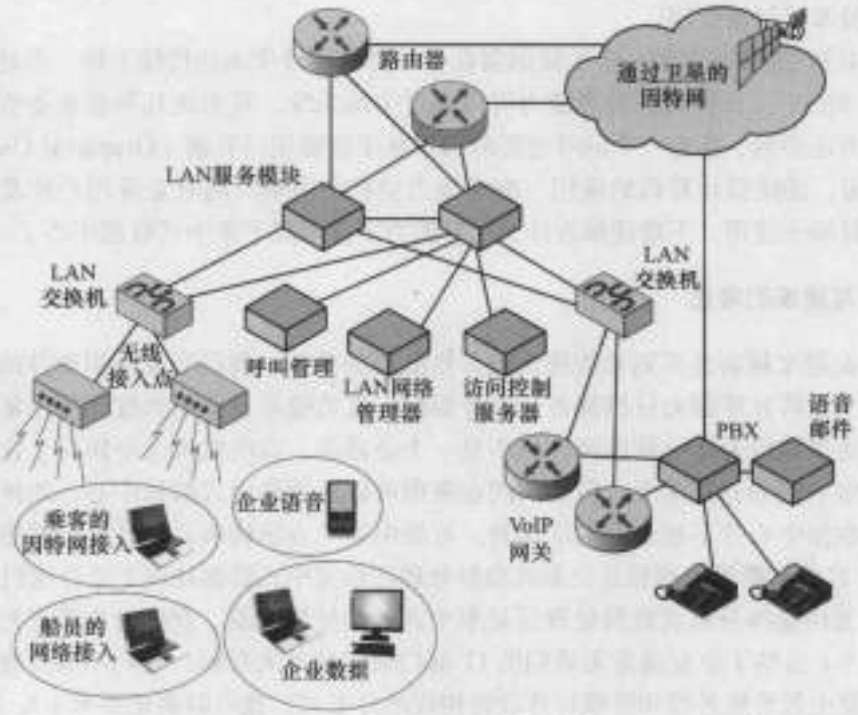


图 3-2 Carnival Valor 无线局域网

船上的专用分支机（Private Branche Xchange，PBX）支持许多与它相连的业务电话机并支持船上雇员的语音邮件设备，乘客和船员也可以使用移动电话通过无线接入点（wireless access point，WAP）与 WLAN 相连。通过使用 VoIP 协议，WAP 设备可以将移动电话流量通过 WLAN 路由到 PBX。充当 VoIP 网关的路由器将信号在 VoIP 流量与声音信号之间转换，从而连接到 PBX。

在数据方面，WLAN 支持基于应用的分布式数据处理配置。不同的服务器分别处理呼叫管理、网络管理以及接入控制 / 安全应用，这些服务器都直接连接到实现有线 LAN 和 WAP 互连的交换机。一系列与船的运营相关的程序由企业的数据服务器直接管理，并且数据服务器可以通过 WAP 与 WLAN 进行无线连接，船上的乘客与船员也都可以通过 WAP 使用笔记本电脑无线上网。最后，LAN 服务模块既充当 LAN 的交换机，也充当网络管理的控制点。

这种分布式架构提供了极大的灵活性。各种与船相关的应用程序（如娱乐的安排、餐点服务和工程维护等）都由不同的服务器维护，这样使程序升级大大简化。服务器在物理位置上也不必放在一个集中式的计算机房里，它们可以放在任何方便的地方。由于所有的通信和网络服务（如声音、网络接入、船上的应用程序等）都与一个单一的 LAN 相连，所以易于实现网络管理和网络安全。

3.1.2　分布式数据处理的技术趋势

直到 20 世纪 70 年代初期，集中式数据处理一直都在各行各业中广泛使用。但在那之后，分布式处理发生了稳定的变革。我们可以从方式和动机这两方面来讨论这个趋势。首先，我们来看看使得公司可以选择分布式处理的数据处理行业的变化；其次，我们再来分析为什么大家会偏好分布式数据处理。

使得企业被 DDP 吸引的一个关键因素在于计算机硬件成本的持续下跌，而处理能力却逐渐增加。如今的个人计算机的处理能力可以超过中端系统，甚至比几年前企业所使用的大型机的处理能力还要强。还有一个同等重要的因素在于图像用户界面（Graphical User Interface，GUI）的崛起，这使得计算机的使用与响应能力空前的简单。随着企业用户涉及的计算装置越来越强大且易于使用，不难理解为什么计算能力不再局限于集中式数据中心了。

3.1.3　管理与组织的考虑

由于企业越来越容易买到功能强大但价格低廉的系统，所以商业应用软件的种类也越来越多，企业开始将计算能力分摊到各个业务部门。虽然很多企业仍然继续使用集中式数据中心，但这也更多地成为了一种选择，而不是一个必需品。有些机构已经倾向于选择分布式数据中心来处理它们的计算需求，但他们的业务仍可以选择集中式数据中心，即使在某些情况下，集中式数据中心并不是企业内部部署，可能由第三方机构运营。计算与网络技术的不断发展使得 IT 高管不断思考到底是分布式数据处理还是集中式数据处理更适合他们的企业。

在考虑怎样选择分布式数据处理还是集中式数据处理之前，我们首先需要思考企业计算的要求。表 3-1 总结了企业通常为他们的 IT 部门设定的 9 大目标，我们不难发现令人信服的情况，只需要由低价服务器和终端计算设备构成的分布式，就可以满足要求 1）、3）、7）、8）、9）。例如，在各个部门之间分发低价但功能合适的计算系统可以提供个性化服务，用户可以在他们的工作中有更多的独立性，部门的绩效也会大大提升。

表 3-1 企业计算功能的需求

1）为所有有需求的组织单位提供计算能力
2）将企业内与计算服务供给相关联的资本与运营成本计算到企业总账中来
3）帮助满足用户部门特殊的计算需求
4）为各个基于计算的部门提供平衡的支持（也就是说，避免对各部门之间有不同程度的支持）
5）确保经理可以得到管理业务部门与整个企业所需要的信息
6）提供可信的、专业的并且有技术竞争力的计算服务
7）给予各部门充足的自由度来使用技术，达到优化它们的创新能力与部门绩效
8）以保留业务部门自主性的方式布置计算服务，同时增加这些操作对大企业的重要性与影响
9）确保员工可以愉快并有效地使用技术支持

两个方面的用户需求（对新应用的需求和对短响应时间的需求），证明了前述声明的真实性。我们首先来看看对新应用的需求，为了使企业有足够强的竞争力，各部门必须持续地提升产能和效率，而使用 IT 来优化业务过程是最好的解决方案。然而，即使是在管理最好的公司里，用户对于新应用的需求也常常大于 IT 部门可以满足的，这就积压了众多不同的程序需求。而且，在很多企业中，这种需求不断增多。采用分布式数据处理策略，可以使业务部门自主地控制计算目标，从而帮助缓解 IT 部门处理积压的应用需求的压力。允许各业务部门自己提升雇员的技术水准，或者采用提高产能的现成的应用可以使业务部门对于 IT 部门的依赖性大大减弱。公司也可以让业务部门使用合同工形式的程序员来开发自己部门的程序，从而缓解 IT 部门积压程序任务。

用户对短响应时间的需求也使得分布式数据处理架构的优势凸显出来。如同第 2 章中所提到的，对于很多业务应用来说，响应时间直接决定了工人的生产力水平，而将合适的应用服务器放在离业务部门较近的地方是缩短响应时间的一种方式，这也是为什么新的办公和学术楼房通常有通信机柜和服务器机房的原因。

我们可以发现，当分布式小型系统在物理位置上靠近用户并专门针对用户特定的应用时，用户的生产力和部门的效率会大大增加。然而，当今的 IT 经理不应该太快地转移到分布式战略中，尤其当这种转移会造成潜在的集中控制丢失时。不同的部门可能会采用不兼容的系统，这会使得部门之间的协调和集成非常困难，而且大家也可能在没有系统地考虑需求和成本的预测及软件、硬件和通信设备的标准前进行采购。这样会使表 3-1 中的目标 4）与 6）受到影响，也会限制企业达成目标 5）的能力。

表 3-2 和表 3-3 概括了分布式数据处理的其他潜在好处和弊端。

表 3-2 分布式数据处理的潜在好处

响应性 分布式计算设备的使用通常是为了更直接地满足局部业务部门的需求，而集中式计算设备则更偏向于企业全局的需求
可用性 在多个系统互连的架构中，任何单个系统的损坏对整体业务的运营产生的影响最小。关键系统和构件（例如，运行关键程序的服务器，存储关键数据的存储技术等）应当有备份，这样即使出现问题也不影响运行
与企业结构的一致性 很多企业采用使用与相应政策和运营步骤相一致的分散式的管理组织结构。由于分散的业务部门的数据和程序需求不同，所以分布式系统更容易满足各不同的要求
资源共享 分布式系统可以让多个用户共享昂贵的硬件，例如宽体彩色绘图仪等。数据文件可以集中管理和维护，但不同的部门都可以使用这些资源。为整个企业支持开发的服务、应用和数据库都可以分散到各个不同的设备中

（续）

增量增长

在集中式数据中心，增加的工作量和新功能的需求通常需要购买大型设备和更新重要软件，而这些更新很可能干扰企业正常运行。在分布式系统中，可以逐渐在最需要的地方替换系统和软件。这样的更新相比集中式数据中心全有或全无的整体更新来说，对企业整体运行的干扰会更小，成本也会更低

更多的用户参与与控制

当计算设备离用户更近时，用户有更多的机会影响系统的设计、运行以及使用

分散运营和集中控制

分散式的程序和设备可以更好地适应企业不同部门的需求，而服务与数据库的集中控制则可以增强这些分散的程序与设备

终端用户的生产力

分布式系统可以减少用户与程序交互的响应时间，而且程序与用户界面也更容易满足每个管理部门的需求。各部门经理也更容易分析分布式系统的有效性，并做最好的局部调整

距离和位置的独立性

分布式系统可以让用户使用企业级的软件、数据以及服务。一旦成功配置，用户很难分辨内部系统与分布式系统的区别

隐私和安全

在分布式系统中，我们更容易将数据和其他资源完整性和安全性的任务分配给这些资源的用户和拥有者

对供货商的独立性

只要安装恰当，分布式系统可以使用不同供货商的产品和软件，这使得买方有更多选择权和谈价的机会，机构就不会太依赖于一个具有风险的单一供货商

灵活性

用户可以灵活地调节他们的应用软件来适应不断变化的情况。在不影响其他位置使用的系统的前提下，用户就能改变他们系统的配置

表 3-3 分布式数据处理的潜在缺点

更具挑战性的故障诊断

当分布式系统各元素之间交互很多时，很难确定故障和性能退化的真正原因

更加依赖于通信技术

分布式系统的效率与通信和网络技术息息相关，所以企业的日常运行很大程度依赖于通信和网络技术

设备间的不兼容性

各个不同供应商的设备可能很难相互连接与通信。为了最大化的减小这个问题，业务部门通常只购买有标准的计算资源

数据的不兼容性

在分布式环境中，尤其是那些分散式的组织架构中，一个地点的程序产生的数据可能不能在另一个地点的应用使用。使用企业级的数据字典和数据库标准，例如开放式数据库连接性（Open Data Connectivity，ODBC）等，可以帮助减小数据的不兼容性

网络管理和控制

由于设备被分散在不同的地方且属于不同的供货商，并且由不同的管理部门进行维护和控制，所以我们很难有效地管理和控制整个网络。如果软件和数据的标准没有被各个业务部门很好地遵守或实施，那么数据处理设备和服务会向一个不受控制的方向发展

企业数据资源的难于控制

在分布式结构中，数据被分散到各处，或者数据至少被不同地方的人使用。一旦分布式用户可以对功能进行更新（在很多程序中很有必要），那么要控制企业级数据的完整性和安全性就很具有挑战性。在有些情况下，管理部门要从分散的、不相似的数据库中收集信息也很难

次优化

由于计算机设备分散，并且很容易逐渐增加新程序与设备，所以经理更愿意为他们的业务部门购买新的计算资源。尽管每项购买对于单个部门来说是合适的，但整个企业的总购买量还是可能会超出总需求

重复工作

分布式系统和数据中心需要有经验的支持人员。如果没有恰当的监管和协调能力，分布式系统可能会产生不必要的重复工作

（续）

数据完整性

分散数据的分布式访问很难保证重复的请求不会使数据库瘫痪。如果为了提供更有效的使用而备份数据文件，那么就更难满足数据完整性了

安全性

在分布式系统中，实施安全策略和用户验证变得更复杂

3.1.4 数据中心的发展

我们需要意识到，要达到表 3-1 中总结的企业的计算目标，我们并不一定要使用 DDP 策略，怎样达到目标应该与企业采用集中式还是分布式的策略无关。尽管有些观点偏向于使用 DDP，数据通信技术、数据中心技术和数据中心本身的发展使得集中式设备的优势更加凸显。这使得一些业务联合了它们的分布式数据处理设备，而在某些情况中，最终的结果是回到了原来的集中式数据处理设备。在本节中，我们分析了一些重新使用集中式设备的主要驱动力。

1. 数据中心

与之前提到的一样，数据中心是一个设有计算机系统和存储与通信系统中相关组件的设施。冗余 / 备用电源、环境控制（例如，供暖、空调和灭火等）和数据通信连接在当今的数据中心中都很常见。数据中心也常含有备用计算系统（例如，镜像或双重服务器）、存储系统，以及用来保护数据和设备的复杂的安全机制。这些备用设备都是为了最小化业务系统停止的概率，一旦数据中心的系统无法使用，业务运作会受到极大的损失。因此，对于数据中心备用设备的投资是很值得的。

我们可以从表 3-4 中看到，数据中心层主要由数据中心备份的程度而决定的。第一层中的数据中心大多比较基本，很少有备份构件。而在第四层的数据中心中，大部分的主要构件都有备份，即使是 HVAC 设备也有两个电力系统来减少断电的机会。电力和通信的中断是数据中心运营中最大的威胁，尤其当公司只有单个集中式设备时尤为明显。

表 3-4 数据中心层的主要特点

层 次	特 征
第一层	服务器、存储系统、网络设备和因特网与其他网络的通信连接都没有备份保证 电力和制冷线路都是单通道，没有冗余部件 可用性：99.671%
第二层	符合或超出第一层的需求 与因特网和其他网络的通信连接是单一线路，没有冗余 有多余的容量组件（服务器、存储系统、网络设备） 有提升地板，不间断电源（Uninterruptible Power Supply，UPS）和驻场发电机 可用性：99.741%
第三层	符合或超出第二层的要求 对所有 IT 设备都有两路电源 IT 设备与网关之间有多路段独立的连接 为因特网或其他网络提供多条（冗余）链路 当一条线路维护时，有足够的能力可以承载负荷 可用性：99.882%
第四层	符合或超出第三层的要求 所有构件都有冗余备份来确保它们的容错率，包括存储系统、供暖、通风及空调（Heating, Ventilation, and Air Conditioning，HVAC）系统、服务器等 含有驻场电源存储及供应设备 使用生物识别技术控制划分的安全区域 可用性：99.995%

为了保证业务连续性，很多有中央数据中心的公司都与第三方公司签署协议，保证冗余数据和处理设备在数据中心发生灾难性事件后异地可用。第三方公司的数据中心存储签约公司可使用的服务器和备用数据库，以防止签约公司的数据中心出现故障。

第三方数据中心的可用性已经使得一些公司将他们大部分的数据和计算移出了他们自己公司的数据中心，这种转移使得这些公司原有的数据中心的处理活动大大减少，甚至关闭了自己本地的数据中心。因此，使用第三方数据中心来满足业务上数据处理的需求可以大大降低成本，而这样的第三方数据中心在吸引客户方面的竞争正在逐渐加剧，很多第三方公司正逐渐投资于第三层或者第四层数据中心来吸引较大公司的注意力。

2. 数据中心计算和存储技术

集中式数据中心在某种程度上仍然存活的原因是因为大型机的再生。与其他类型的计算机一样，数据中心功能强大的大型机的价格也在逐渐降低，而功能越来越强大。由于大型机可能对安全性、可用性和易管理性有很好的提升，所以它们的销售势头仍然很好，且更多地被公司用做企业基础设施的中心。与我们对虚拟化的讨论中指出的一样，大型机可以运行多个操作系统，也就意味着它们可以运行所有大型商业软件包。

另一个与集中式数据中心兴起相关的重要技术发展是**内存计算**。内存处理器包含可存储大数据集的太字节以上的 RAM。可以将数据直接存储在处理器中，大数据集的运行比用传统服务器处理快得多，不必再因为受限的 RAM 而将数据在存储设备之间调出调进。内存计算有颠覆人工智能（Business Intelligence，BI）的潜能，因为它能将数据仓库带入内存，从而实现实时的数据挖掘和业务分析。SAP 的内存计算系统称为高性能分析应用设备（High Performance Analytic Appliance，HANA），它的外表像可以装入普通大小的数据中心服务器机柜的高端服务器，却有着 Intel 内存处理器 [HARD12]。HANA 盒的价格很高，但由于它所带来的收益也很高，所以很多使用 SAP 的公司都迅速采用这种新技术，SAP 也调节它的 ERP 和商业系列软件来适应 HANA。

内存处理的日渐流行使得使用分布式数据中心的公司开始重新考虑他们的 DDP 战略，并开始将他们的高性能计算资源整合到集中式数据处理中心。曾经放弃使用大型机计算和集中式数据处理设备的公司现在也被迫回归中央数据中心。这使得数据中心技术的投入又越来越多，也加强了数据中心在公司网络基础设施组件中的重要性。

数据存储硬件也在发展，并继续将数据存储的成本降到前所未有的底线上。2000 年，平均存储一个千兆字节的成本大约是 10 美元；到了 2004 年，成本降到了 1 美元；而到了 2010 年，这个成本更是跌到了 0.1 美元 [BUSH11]。这个价格的下滑与企业对各种类型数据（如声音和视频等）的存储需求正好相弥补，因此企业继续在各种存储技术，如存储区域网（Storage Area Network，SAN）和网络附加存储（Network-Attached Storage，NAS）等，上面进行大量投资。如果考虑所有支出（包括备用存储设备、支持人员、服务器设施、电力系统、制冷系统等），一个企业实际存储每千兆字节的费用每月接近 25 美元 [VERT09]。

3. 虚拟化

虚拟化是另一个促进数据中心发展和它们在企业网络作用壮大的计算机硬件发展趋势。**虚拟化**是指创造某东西的虚拟版（而不是真实的），在计算中它指的是创造一个操作系统、服务器、存储设备和网络的虚拟版本。划分一个硬盘创建两个不同的硬盘是虚拟化的另一个例子。在现实中，第二个硬盘并不存在，但它在计算机目录里显示出的信息与真的安装了第二

个硬盘一样。

我们这里只讨论4类虚拟化：操作系统虚拟化、服务器虚拟化、存储虚拟化和网络虚拟化。接下来我们分别简单介绍这4类虚拟化。

当使用操作系统虚拟化时，软件将允许计算机硬件同时运行多个操作系统。这在几十年前曾被使用在大型机上，为了避免浪费昂贵的处理资源。

从服务器用户的角度来看，服务器虚拟化将实际使用的服务器信息掩饰起来，使得用户只看到一台服务器，而不是一系列物理服务器、处理器和与之交互的操作系统等信息。

存储虚拟化在SAN中广泛使用，它将众多存储器的存储能力融合到一起，看起来像一个单一的存储器，使得中央控制台的管理更便捷。

网络虚拟化将背后复杂的通信网掩盖起来，它可以将网络带宽分为一个个独立的通道，让不同的服务器和硬件使用。

虚拟化促进了企业所青睐的“按需计算”和“效用计算”。在虚拟化环境下，用户通常认为企业的计算资源无限大。当需要更多的带宽来支持网络应用时，就会有通道被安排出来；当需要更多的服务器来支持用户需求时，无需改变用户目录就可以在数据中心设施中增加更多的服务器；如果需要更多的存储设备来支持企业不断加剧的数据要求，也在不改变用户界面的情况下获得这些资源。虚拟化让大家似乎看到一个无限可扩展的网络。计算设备和数据存储都与用户位置相距甚远，如何中央监管和控制一个虚拟化计算环境成为了企业关注的问题，这也是云计算渐渐获得关注的原因。

3.1.5 客户机/服务器架构

广泛使用的客户机/服务器（Client/Server，C/S）架构创建的目的是为了体现分布式和集中式计算的最佳之处。在这个架构中，用户使用的个人计算机、笔记本、平板电脑和移动设备统一称为客户机，这些客户机都由特定的服务器支持。服务器是指为客户机提供数据库服务、打印服务和通信服务的专业计算机。C/S架构中服务器的命名遵循为客户机提供的功能，提供数据库服务的通常称为数据库服务器，其他广泛应用的服务器有打印服务器、传真服务器、通信服务器和应用服务器等。随着高速LAN、WAN/LAN整合技术和提供和机器之间处理的复杂系统软件等的发展，C/S架构逐渐开始被广泛接受。

客户机/服务器架构被企业青睐有众多原因。首先，这种架构的性价比很高，并可以通过特殊功能的集中化实现规模化经济。文件服务器和数据库服务器方便了授权用户通用存取数据，方便维护文件和数据的安全性和一致性。服务器的物理架构也可以为用户个性化制定，最好地支持为用户提供的服务。

另一个让客户机/服务器架构越来越流行的原因是它的灵活性。这是由于服务器提供的功能服务并非与实体计算机一一对应。例如，文件服务和打印服务不用再使用不同的服务器分别提供，而可以由同一台服务器来提供。而一个反面的极端是，数据库服务可能由分散在各地的不同机器来提供。在较小的企业中，所有服务可以使用同一台服务器中的处理器提供。在大型企业中，服务可由多台服务器的多个处理器一起提供，提升可用性、容量和响应能力。在第9章中，我们会更详细地讨论这种方法。

在20世纪90年代，随着客户机/服务器架构被企业软件供应商（如SAP等）逐渐使

用，企业对于这种架构的关注度逐渐提升。这些商业软件供应商开发了与图 3-3 相类似的三层版本的产品。通过将用户界面（客户机）与应用（例如，ERP 系统等）和企业系统数据库分离，企业高层开始相信计算资源可以分配到不同的位置。用户再也不用离应用服务器很近，而且应用服务器也不用再与企业数据存储系统位于同一个地方，这种实现使得 DDP 受到很多企业的关注。

客户机 / 服务器架构在商业应用的一个例子是 MasterCard 国际。我们在线上案例研究中有详细说明。



图 3-3　三层企业系统架构

3.1.6　内部网与外部网

内部网和外部网在企业分布式数据处理的发展中也起到了重要的作用，很多专家把因特网、内部网与外部网称为客户机 / 服务器模型的例子或者延伸。本质上，内部网给客户机用户提供因特网相关的应用，但是应用仅限于企业内部。内部网的主要特征有：

- 使用基于因特网的标准，如超文本标记语言（Hypertext Markup Language，HTML）和简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）。
- 使用 TCP/IP 协议组的应用和服务。
- 包含有外界用户不能通过公共因特网访问的自有内容。即使企业有网络连接并使用 Web 服务器，这样的内容也限制为只能被已授权的内部网用户使用。

内部网方法的优势在于实现和使用都很简单，第 9 章将仔细分析内部网的细节。

与内部网相似，外部网使用 TCP/IP 协议与应用，尤其是 Web。外部网的一个明显特征是它能给授权的外部用户（如企业的供应商和客户等）提供访问企业资源的途径，这可以通过公司与因特网的连接或使用其他数据通信网络来提供。外部网不仅仅提供访问企业公共 Web 网站的途径，还能使外部授权用户有足够的权限访问公司丰富的资源。与内部网一样，外部网的经典操作模型也是客户机 / 服务器模型。外部网的具体内容也在第 9 章中给予解释。

3.1.7　Web 服务与云计算

很多企业将它们的企业网络扩展到托管服务和应用，通过网络给业务用户提供基于计算机的服务的企业称为**应用服务提供商**（Application Service Provider，ASP）。如今，ASP 提供的软件通常称为按需软件或软件即服务（Software as a Service，SaaS）。一个简单的 ASP 例子是，企业使用标准 TCP/IP 协议（如 HTTP），通过因特网提供对特定应用程序（如时间和考勤电子时间表服务）的访问。

ASP 的流行起源于中小型企业，他们的竞争能力依赖于支持他们业务流程对个性化软件的需求。很多时候，这些企业需要的个性化软件的费用大大高于中小型企业的预算，而且企业没有专业人员来支持软件的复杂性。ASP 的到来大大减少了个性化软件的费用和复杂度，使得中小型企业可以买得起个性化软件。应用服务提供商（ASP）负责软件的更新，并提供全天候的技术支持，协助处理物理和电子安全问题，保证业务用户的可持续性。

ASP 客户所使用的应用软件位于供应商的系统上，用户通过 Web 浏览器或者供应商提供的专用客户软件来访问。ASP 是这些应用软件的拥有者，它们运行并维护这些软件和相关服务器。ASP 客户通常基于软件的使用时间，以月费和年费的形式来支付，ASP 则提供一个服务级别协议，保证可用性等的服务级别。

对于客户而言，个性化 ASP 软件的灵活性很小，很多时候它们需要接受这些应用原本的样子。如果 ASP 软件用来处理关键的业务功能，那么客户对于这种功能的控制力就很局限，如果这个 ASP 遇到一个重大的故障，那么这个业务功能就会处于危险之中。

尽管 ASP 服务有很多局限性，但它们仍以多种形式存在，并未来仍会继续存在。ASP 业务包含很多类型：

- 功能化 / 专业化的 ASP 提供单一应用，例如信用卡处理或工资单处理。
- 垂直型市场的 ASP 为特定类型的用户（如医生等）提供解决方案包。
- 企业 ASP 为企业系统提供许多不同的解决方案。

与之前提到的一样，ASP 服务传统上针对的是中小型企业。如今，软件仅仅是客户通过“云计算”使用的服务之一。从最广泛的意义来说，**云计算**包含任意通过因特网实时拓展企业已有 IT 能力的基于订阅或基于使用时间来进行付费的服务。云计算服务供应商使企业可以增强 IT 能力，而不用投入新的设施、购买新的软件或培训新的专业人员。如 [KNOR12] 中提到的那样，云计算持续发展并产生了各种形式：

- **软件即服务**（Software as a Service，SaaS）：使用多租户架构，通过浏览器为客户提供单一的应用。
- **基础设施即服务**（Infrastructure as a Service，IaaS）：为客户提供存储和虚拟服务器（虚拟数据中心）。
- **平台即服务**（Platform as a Service，PaaS）：为客户提供开发环境，在供应商的基础设施上开发应用软件，并且这些软件可以使用供应商的服务器通过因特网提供给开发者的客户。
- **管理服务提供商**（Managed Service Providers，MSP）：为客户提供个性化的服务，提升客户已有的 IT 服务，如电子邮件病毒扫描、应用监控、反垃圾邮件服务、桌面管理服务和安全管理服务等。

云计算服务通常与设备无关，因为它们可以交付给任意的终端用户计算设备，如个人计算机、便携式计算机、平板电脑或智能手机等，它们对移动用户的支持也是云计算在企业中越来越流行的另一个原因。

在第 9 章中，我们将更详细地讨论云计算，但在这里提到也很合适，因为它在很多企业的 DDP 架构中已经成为一个重要的构件。

3.2 分布式数据处理的形式

我们之前已经定义 DDP 系统为计算架构，并且在这个架构中互连的计算机分布在企业的不同地方。DDP 系统在企业中以各种形式实施，每种形式都与这个定义相符合。用来鉴别这种多样性的一种方法是考虑以下几个功能或对象是怎样在网络中分布的：

- 应用
- 设备
- 网络管理
- 数据

通常情况下，在一个 DPP 系统里会同时存在两个或两个以上的功能或对象。为此，这里我们一个个来分析以便了解 DPP 的实施配置。本节讨论前 3 种，最后一种我们将在下一节中讨论。

3.2.1 分布式应用

我们可以从两个维度来描述应用的分布，首先来看看应用功能在网络中的分配：

- 一个应用可以分为多个构件，这些构件被分散部署到多台计算机中。
- 一个应用可以在不同的计算机上复制。
- 不同的应用可以在分散到不同的计算机中。

分布式应用处理也根据它们是垂直分布还是水平分布来区分。一般情况下，垂直分区指的是一个应用被分隔多个构件，分散在多台机器上；而水平分区指的是一个应用被复制到多台机器上，或者多个不同的应用被分配到多台机器上。

在**垂直分区**中，数据处理按层次分布，这种分布可以反映一个企业的架构，对于应用来说这也可能是最合适。以下有多个例子：

- **保险**：在保险公司中，数据处理分布通常分为两层。在典型的系统中，每个分部有一个计算机系统来准备新的合同和处理索赔。大多数情况下，这种类型的事务可以直接由本地办公室来办理。信息汇总之后再传给总公司。总公司使用合同和索赔信息来进行风险分析和实际的计算。基于公司的财政现状和现行风险承担，总公司可以调节客户群和个体客户的利率，并将这些调整传达到各个分部。
- **零售链**：典型的零售店包括含销售点的终端以及销售和办公室人员使用的计算机。通常，一个单独的服务器用来存储整个店的信息。销售点（Point-Of-Sale，POS）应用的本质也屈从这样的安排。销售点的终端使用服务器上的价格信息，当产品销售时，销售事务记录为库存和应收账款的变化。销售人员和办公人员可以使用客户机设备来显示销售信息的总结、库存情况、应收账款和客户事务总结。商店的管理层可以看到整体销售业绩、产品老化等其他报告。商店层面上的数据和信息也可以通过销售链传送到总部。
- **过程控制**：一个工厂的过程控制功能非常适应于垂直分区的 DDP 系统。每一个主操作区域都由一个控制台或工作站来控制。控制台或工作站的信息由分布式过程控制微处理器来提供，这些微处理器负责传感器和机器人的自动控制或工作场所其他的受动器装置。操作控制工作站扫描传感器的读数、寻找异常或者分析趋势，也控制部分工序使得生产率和产品结构更多样化。这些分布式工作站保证了工作流程层次对于变化环境的快速反应，所有的工作站都与一个强大的服务器或大型机相连。在这些服务器和大型机上运行着众多管理层的应用，如过程规划、最优化、商业分析以及企业数据处理等。
- **Web 糅合**：基于 Web 的糅合已经广泛流行起来。它们通常整合不同渠道的数据来创造一个新的应用，通过掩盖数据源的具体信息，用户可以在新的应用中获得一个无缝体验。大型网络服务公司（如谷歌、eBay、亚马逊）针对他们的很多服务等提供免费或者低价的应用程序界面（Application Programming Interface，API），让开发者可以很容易创造新的 Web 糅合。Web 糅合所使用的 API 是分层的，通过组合不同层次的 API 形成。Web 糅合中所使用的与 Web 服务相关的数据源通常存储在分布式数据中心。实际上，很多 Web 糅合是用户可以实时体验的垂直分区 DDP 的例子。在第 9 章中，我们将更仔细地探讨 Web 服务。

由这些例子可以看出，一个垂直分区的 DDP 系统通常由一个中央计算机系统（服务器或者大型机）和一层或多层卫星系统构成。划分的本质反映了机构的架构或者处理任务的架构，

目的是将一个应用的处理任务加载到性价比最高的分层中。这样的安排既结合了集中式和分布式数据处理中最好的特点，也符合了客户机/服务器架构。

在**水平分区**的结构中，将数据处理分配到多个具有对等关系的计算机中。也就是说，没有了客户机/服务器分离的概念。在水平配置中，各个计算机通常独立运作，虽然有些情况下，这样的配置是为了平衡负载，但在很多情况下，水平分区反映了一个组织的非集中化。我们举两个例子：

- **小型办公/家庭办公**（Small Office/Home Office，SOHO）**对等网络**：在小型办公或家庭办公网络中，用户可能共同连接到对等局域网中。在对等 MSWindows 网络中，SOHO 计算设备属于同一“工作组”，每个设备都可以与工作组中的其他设备共享文档、打印机和其他服务。在这种安排中，每个计算设备都可同时充当客户机与服务器，没有一台计算机拥有特殊的网络操作系统来为其他设备提供服务器端的应用（如目录服务等）。在对等局域网中，对共享资源的访问权限通过在独立机器上设定共享允许来管理。例如，如果某用户有一个其他用户想访问的打印机，那么此用户必须要将他的机器设定为允许（共享）权限。同样，如果一个用户想访问另一个用户机器上的文件或文件夹，另一用户需要在他的计算机上共享此文档。在对等网络中安全选项受限制，但是我们可以通过设定密码等措施来控制共享文档和打印机等资源的访问权限。
- **空中交通控制系统**：空中交通控制的每一个区域中心都独立于其他中心的运行，但它们使用同一系列的应用。在每个区域中心，使用多台计算机处理雷达和无线电数据，并以可视化的形式将空中交通状态传送到控制器。

  更多的情况是，一个机构的计算功能既包含水平分区的业务应用，也包含垂直分区的应用。公司总部可能有一个集中式数据中心，大型机的应用程序提供基本的企业管理信息系统和决策支持系统。其他集中式功能，如公共关系、策略规划、企业财会和会计等也由它支持。在分公司提供从属的计算设施构成垂直分区，而在每个分公司内部，自动化支持又是由水平分区来完成的。

3.2.2 其他形式的 DDP

DDP 环境也包含分布式设备控制和分布式网络管理。接下来，我们简要分析各种可能性。

1. 分布式设备

在企业网络里，DDP 的一个基本应用是支持自动取款机等分散的业务设备集。另一个常用的应用是工厂自动化。一个工厂通常有多个传感器、可编程控制器以及用来自动化流水线的机器人，这样的系统包含对工作中心不同位置的流水线分配计算技术。

2. 网络管理

任何分布式系统都要求一定形式的管理和控制，包括对分布式系统内不同构件状态的监控、构件之间通信网络的管理等，这样才能确保可用性与响应性。很多情况下，我们需要某些类型的中央网络管理系统，但这样的系统需要随时获取分布式系统中各个设备的状态信息，并需要给设备发送指令来避免干扰。因此，在分布式系统中，至少有一部分计算机会装有管理和控制逻辑，能够与中央网络管理系统交互。在第 20 章中，我们将更仔细地探讨这些问题。

3.3 分布式数据

在开始探讨分布式数据之前，我们需要了解计算机系统中数据组织的本质。我们首先简

要回顾数据库和数据管理系统的基本概念，然后介绍企业选择分布数据的不同方式。

3.3.1　数据库管理系统

有些情况下，只需要一些简单的文件集合就可以使一个业务运行起来。每个文件包含文本（如备忘录和报告的副本）或数字数据（如电子数据表），有些更复杂的文件将事务记录包含进来。尽管小型公司通过文件和电子数据表就可以将业务运行起来，但大型公司通常需要更复杂的数据结构，这种数据结构通常称为数据库。**数据库**是为一个或多个应用的使用所存储的结构化数据集。除了数据之外，数据库也包含数据间和数据组间的关系。为了区分数据文件和数据库，我们来看看以下的例子。一个简单的人事文件中包含每个雇员的一条记录，每条记录提供雇员的姓名、地址、出生日期、职位、工资和其他人事部门需要的信息。而一个人事数据库不仅包含上述的人事文件，还包含一个记录每位雇员每周工作的时间与出勤率的文件。工资计算程序通过数据库这样的结构，将这两个文件关联到一起，通过结合每个员工的实际工作时间和薪资标准，可以简单地获得每位员工的工资单。

与数据库相伴的是**数据库管理系统**（Database Management System，DBMS），这是用于构建和维持数据库并为多个用户和应用提供查询功能的一系列程序。**查询语言**为用户和应用程序访问数据库提供了统一的界面。

图 3-4 介绍了 DBMS 架构的简化图解。开发者利用数据定义语言（Data Definition Language，DDL）来定义数据库的逻辑架构和程序属性，并通过数据库描述表来呈现。数据操作语言（Data Manipulation Language，DML）也为程序开发者提供了一系列强大的工具。查询语言是终端用户在数据库中访问特定数据子集的说明性语言。数据库管理系统使用数据库描述表来管理物理数据库。文件管理器和事务管理器模块为数据库提供接口。除了数据库描述表之外，还有两个表（授权表和并发访问表）支持 DBMS。DBMS 使用授权表来确保用户有权对数据库执行查询语言命令，而并访问表预防当多个数据库用户同时执行相矛盾的命令时产生冲突。



图 3-4　DBMS 架构

数据库系统为大数据提供了有效的访问，对很多机构的运行极为重要。从图 3-3 中我们可以看到，数据库在企业系统中起到了关键的作用，充当企业系统整合业务流程中所有数据的中央存储库。

分布式数据库由分布在多台计算机中的不同数据库构成，它看上去与每个用户使用单个数据库一样。计算机可以位于集中式数据中心，也可以分布在相距甚远的不同地理位置。DBMS 控制对分布式数据库的访问，也使得用户可以像处理单个数据库一样地处理分布式数据库。DBMS 包含可以识别数据库中任意元素物理位置的目录，这些元素可以在同一数据中心的不同机器上，也可以在不同数据中心的机器上。

总的来说，我们可以将企业数据分为 3 类：集中的、复制的和分区的。

3.3.2　集中式与分布式数据库

集中式数据库位于中央计算机设备中。然而，依赖于数据库的用户和应用程序可以分布在较远的地理位置，仍然可以对集中式数据库进行访问。集中式数据库通常采用垂直分区的 DDP 结构。对它而言，数据的安全性和完整性是最重要的，因为中央数据中心通常比分散的数据和计算技术更容易控制。另一方面，分布式数据组织受关注还有一系列原因，其中包括：

1）分布式设计反映了一个企业的功能结构，使得数据结构的设计和数据的使用更易于理解，也更容易实施和维护。

2）数据可以存储在本地，并在局部控制之下。局部存储可以大大减少响应时间和通信成本，同时提高数据可用性。

3）将数据分配到多个独立的位置，可将计算机故障的影响限制在发生点，其余非故障计算机仍然可以被访问并进行数据处理。

4）整个数据量的大小和用户数不会受单台计算机的大小和处理能力的限制。

3.3.3　复制型数据库

在分布数据时，我们会采用两个整体策略中的一种：复制型或分区型。在**复制型数据库**中，数据库的整体或部分被复制到了两台或多台计算机上。在看这个重要策略的基本原理之前，我们先来看来自 [CONN99] 的两个例子。

第一个例子是金门金融集团。这个集团每月都创造将近 10 亿美金的交易额，这些交易记录存储在旧金山的系统中。在每条交易发生时，在圣何塞的远距离公司也会进行记录。金门集团每月都使用专线传送 66 亿字节的数据来进行复制。当旧金山遇到整日的断电时，这个公司收回了它们在复制软件和专用传输线上的投资。雇员到圣何塞建立店面，并利用当前复制的数据来完成工作，这使得这个金融公司的交易仅仅中断了半个小时。

美林集团采用的则是另一种策略，他们每天将 20 亿字节的关键金融信息分配到 3 个远程办公室以供员工使用。过去，信息系统（Information System，IS）工作人员每周人工将整个数据库复制到远程的办公室。如今，数据每天都会更新到各个远程点两次。由于只有当变化的数据达到 200MB 时，变化的数据才会被传送，所以时间和带宽得以大大缩短。如今用户可以在本地访问最新的数据，不再需要使用长途连接。

数据复制已经变得越来越流行。众多供应商为 Windows 和 UNIX 平台提供数据复制技术来备份主框架的基础数据。在银行业中，使用数据复制来保护用户的账户已经成为了不成文

的要求。数据复制的一个重要优势在于它为网络和服务器故障同时提供了备份和恢复。

在数据复制中，有3个变体被广泛使用：实时、近实时和延迟，见表3-5（基于[GOLI99]）。**实时复制**通常在事务性系统中使用，例如ERP系统中的订单填写系统，所有数据的副本必须立刻同步。更新通常使用称为两阶段提交的算法，该算法通过为每个更新增加确认步骤来避免两个数据库（原始和备份）之间的非一致性。这项操作减少了数据库更新的总反响时间，不过并非总是成功。

表3-5　复制型策略的变种

	实　时	近 实 时	延　迟
设计架构	两阶段提交	级联或广播分布	信息和队列
优点	紧数据 同步 分布式事务 数据普及性	数据合并 数据分布 改进的响应时间 较小的广域网负载	异构数据库更新 在任意网络中有保证地传输 多网络协议支持
缺点	更长的响应时间 难以实施 两阶段提交并不是总能实现	缺少数据普及性 单供应商解决方案	更新有时间延迟 需要更多的编程工作

近实时复制也是一种选择。在这种情况下，备份成批量地出现，同时伴随着少量的时延（例如，10 – 30分钟），但这对很多商业应用已经足够了。

延迟复制指的是以比近实时复制更长时间段，批量传输大量的变化，例如每天一次或两次。这种传输可以是大量数据的批量文件传输。这种方法最小化了对同步复制的网络资源的需求，但它不能保证像实时和近实时复制那样的一致性程度。

3.3.4　分区数据库

在分区数据库中，数据库是分散在不同计算机系统中独特、非重叠的部分。通常情况下，分区数据库的各部分之间没有数据复制，也就是说，每个分区存储总数据库的一个非重叠子集。这种策略不是使用水平DDP，就是使用垂直DDP。

这种方法的一个主要优点在于它分散了数据存储与负载更新，同时避免了单点故障。但是，如果典型的数据库请求包含多个分区的数据，则这种方法可能会失效。

表3-6简单比较了3种数据库的组织类型。在实践中，将多种策略混合起来使用很常见。在表3-7中，我们更详细地分析了数据库组织的策略（基于[HOFF02]）。对于复制型数据库，我们可以有两种策略。第一种策略，需要维护中央数据库，各地远程提取部分数据库的副本进行使用。典型的情况下，如果远程计算机有权限更新数据库中的部分数据，那么这种系统会在更新时把这部分数据锁起来，远程计算机在交易完成后将更新传回中央数据库。另一种策略使用一种更复杂的同步技术，复制型数据库的副本自动在DDP系统中传播来更新所有副本。在企业网络中，这种策略需要更多的处理和通信负载，但它也能让业务有更强的灵活性。

表3-6　各数据库分配方法的优点与缺点

分配类型	优　点	缺　点
在不同位置的用户访问同一个数据库（**集中式**）	没有数据复制，重组很少	多用户同时访问同一个数据时发生竞争，如果数据库很大，响应时间会很长。在存储系统发生故障时，所有用户都无法访问数据

（续）

分配类型	优 点	缺 点
每个用户处储有中央数据库的副本（复制型）	减少了多个用户访问数据发生的竞争，响应时间缩短。在发生故障时，可以从其他位置获得新的副本	对数据的大量复制产生高存储要求和高成本。数据库任意副本更新之后都必须统一到其他副本上
每个用户存储独立的数据库（分区型）	不在每个用户部里都复制整个数据库，可以减少总数据存储成本。每个本地数据库的大小都由本地使用来决定，并逐渐增加。响应时间短	从不同分散位置的数据库获取数据，开发企业级报表和管理报告比较有挑战

表 3-7 数据库组织的策略

策 略	可 靠 性	可扩展性	通信开销	可管理性	数据一致性或完整性
集中式					
集中式数据库 数据库位于某个固定位置；数据可以分布到地理位置不同的用户用于本地处理	**有好有坏** 高度依赖于中央数据中心的冗余程度	**有好有坏** 虚拟化可以克服约束传统系统性能的内存限制	**很高** 大通信量通往一个固定位置；使用连接数据中心的冗余连接处理较高的流量负载	**很好** 只需协调一个单一的站点设备	**优异** 所有用户永远都有相同的数据
复制型					
分布式快照数据库 为方便远程使用，抽取中心数据库部分数据建立副本	**好** 有冗余和可容忍的延时	**很好** 额外副本的成本小于线性	**低到中等** 各站点间交互的周期性快照会导致网络通信量的爆发	**很好** 所有的副本都一致	**中等** 只要延时可以满足业务需求就可以
复制型分布式数据库 数据在多个站点复制并同步	**优异** 有冗余和最小延时	**很好** 多余副本的成本很低	**中等** 信息是恒定的，不过需要容忍部分延时	**中等** 同步为管理增加了一定的复杂度	**中等到很好** 接近精确的一致性
分区型					
分布式非集成数据库 应用访问的独立数据库在远程计算机上	**好** 取决于本地数据库的可用性	**好** 新的站点独立于已有的站点	**低** 很少，只有需要在网络中传递数据和请求查询时才会有	**很好** 对每个站点来说都很便捷，只有当各个站点之间需要共享数据时才需要管理	**低** 不保证一致性
分布式集成数据库 数据跨越多台计算机和软件	**很好** 有效地使用分区	**很好** 新的节点只得到它们所需的数据，而不用改变整个数据库的设计	**低到中等** 大多数查询是本地的，但当需要多个站点的数据时会导致暂时性的负载增量	**很难** 当查询请求需要分散表中的数据时尤其困难，更新必须实时进行协调	**很低** 需要大量的工作，且不能容忍非一致性

最简单的分区策略含有多个独立运行的数据库，每个数据库都允许远程访问。实际上，我们有一系列集中式数据库，而不止一个中心。在更加复杂的系统中，数据库分区被整合，用户通过一条查询命令可以访问任意分区。在复杂系统中，这种访问用户是看不到的，因此用户不需要详细说明所需的数据存储在哪里，也不用使用不同的指令来访问分布式数据库中不同分区的数据。

因此，我们可以使用各种策略。在设计分布式数据库时，两类目标是最重要的：数据库目标和通信目标。数据库目标包含数据可用性、安全与隐私性以及数据完整性。通信目标是

最小化通信负载和用户访问存储在其他位置数据的响应时间。

3.4　DDP 的网络含义

我们可以将使用分布式数据处理产生的网络与通信要求描述为以下 3 个关键领域：连通性、可用性和性能。

分布式系统的**连通性**指的是系统中构件交换数据的能力。在垂直分区的 DDP 系统中，系统中的构件通常只需要与它们分级结构中上层或者下层的构件相连接。因此，通常使用简单的直接链路就能满足这个需求。在水平分区系统中，我们需要任意两个系统之间都能交换数据。例如，在 SOHO 对等网络中，如果用户能与工作组中的任意用户共享文件是很占优势的。

在一个要求高度连通性的系统中，某些类型的网络会比大量的直接链路更有优势。为了理解这点，我们看看图 3-5。如果我们有一个要求完全连通的分布式系统，并在任意两个系统或位置之间使用直接链路，那么链路的数量和通信接口将随着系统和位置数量急剧增长。4 台计算机需要 6 条链路，5 台计算机需要 10 条链路。然而，假设我们使用一个中央交换机创建网络，将所有计算机连接到交换机上。由图 3-6 可以看到，4 台计算机需要 4 条链路，5 台计算机只需要 5 条链路。

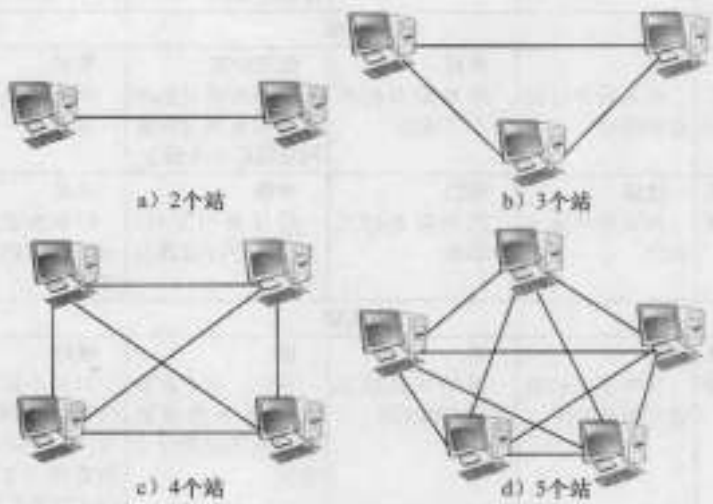


图 3-5　使用直接链路的全连通

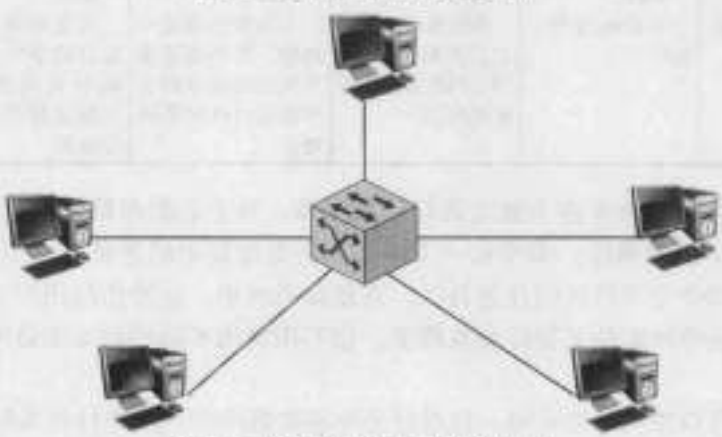


图 3-6　使用中央交换机的全连通

如果一个分布式系统中的构件分散在不同地方，连通性就需要有远距离传输数据的方法。这个需求引入了 ISP 和公共因特网的使用、通信载体上的广域网服务 / 连接或者投资专用基础设施。正如 3.1 节提到的，第三方数据中心越来越被企业网络所使用。第三方数据中心的业务使用从备份和恢复存储数据库备份的站点，延伸到企业多集中数据中心处理站点。如今，很多第三方数据中心为他们的客户提供众多“云计算”服务。在第 9 章中，我们将更全面地讨论云计算。

可用性指的是用户可以使用特定功能和应用的时间百分比。根据应用的不同，可用性或许不重要，也可能很重要。例如，在空中交通控制系统中，支撑空中交通控制的计算机系统的可用性十分关键。高可用性的需求意味着在设计分布式系统时，单台计算机或网络中设备的故障不会导致整个应用的访问瘫痪。例如，所有提供关键应用或服务的服务器要有一台备用服务器，当主服务器出现故障时，备用服务器可以随时加载并进行处理。高可用性也意味着通信链路和设备也需要有很高的可用性。因此，也需要一定形式的链路和通信设备冗余与备份。

最后，我们还需要考虑连接 DDP 系统各个应用的通信网络的**性能**。对于高度交互的应用，如数据输入系统或图形设计程序等，响应时间是至关重要的。这不仅需要运行程序的计算机处理器很快，还要求网络连接也很迅速，网络也需要有足够的能力和灵活性来提供需求的响应时间。另一方面，如果应用程序在时间不紧迫的情况下需要移动很多数据，主要的网络性能问题就在于吞吐量。在这种情况下，设计网络时就需要让它能够处理大容量的数据。

一旦我们考虑企业网络中能够使用的数据通信技术和设备的细节，我们会再次考虑通信和网络规划的策略，包括那些最满足 DDP 的策略。

3.5　大数据基础设施的考虑

本章，我们开始注意如今的企业正在存储越来越多种类和容量的数据，数据日益增长的需求使得集中式数据中心的虚拟存储系统越来越流行，这样的系统也常称为“私有云”。使用公共云的存储服务拓展存储能力在商业界也广受关注。

传统企业数据存储和管理技术包含关系数据库管理系统（Relational Database Management System，RDBMS）、网络附加存储（Network Attached Storage，NAS）、存储区域网络（Storage Area Network，SAN）、数据仓库（Data Warehouses，DW）和商务智能（Business Intelligence，BI）分析。这些技术的特性总结在表 3-8 中。

表 3-8　传统的数据存储 / 管理技术

数据存储 / 管理技术	主要特点
关系数据库管理系统（RDBMS）	这是基于关系模型的数据库管理系统（Database Management System，DBMS）。在 RDBMS 中，数据以表格的形式存储，数据之间的关系也存储在表格中。这使得我们可以以不同方式访问或重新组装存储的数据，而不用改变数据表 在 RDBMS 中，用户使用查询语言结构化查询语言（Structured Query Language，SQL）来访问和处理数据 大部分当今流行的数据库都是基于关系数据库模型
网络附加存储（NAS）	网络附加存储系统是可以与多台异种计算机共享一个或多个硬盘的网络设备，它们在网络中的专门任务是存储和提供文件 NAS 磁盘驱动器主要支持嵌入式数据保护机制，比如冗余存储箱或独立磁盘冗余阵列（Redundant Arrays of Independent Disk，RAID）等 NAS 将文件服务的任务从网络中其他服务器独立出来，并提供比传统文件服务器更快的数据访问

（续）

数据存储 / 管理技术	主要特点
存储区域网络（SAN）	SAN 是用来访问各类存储设备（如磁带库、光盘库和磁盘阵列等）的专用网络 对于网络中的服务器和其他设备，SAN 存储设备看起来与本地附加设备一样 由于专门为存储通信而设计，所以光纤通道用于 SAN 内部通信 根据不同的计算需求，SAN 在企业网络中可以是集中式也可以是分布式的
数据仓库（DW）	DW 是用于报告和分析的数据库，而且 DW 中的数据是从其他操作系统中上传的，元数据，也就是数据的数据，也存储在 DW 中 数据仓库可以细分为存储 DW 中数据子集的数据集市，这里数据集市与传统数据库的分区比较类似 DW 数据是经过清理、转化、分类的数据，可以被经理和其他商务专家用来进行决策支持、市场调研、数据挖掘、在线分析处理（OLAP）和其他形式的商务智能
商务智能（BI）	BI 技术为业务操作提供当前、预测性和历史性的观点。由于 BI 旨在提升商务决策制定，所以 BI 系统通常归类到决策支持系统（Decision Support System，DDS）中 定义为 BI 技术的通常有标杆管理、商务分析、商务性能管理、数据挖掘、事件处理、预测分析和文本挖掘等技术

传统数据仓库和 BI 分析系统倾向于高度集中在企业基础设施中，这包含使用 RDBMS 的中央数据存储、高性能存储和分析软件，如用来挖掘和虚拟化数据的在线分析处理（Online Analytical Processing，OLAP）工具。

大数据通常包含这些技术，但也需要一些其他技术。要在可容忍的时间内处理大量的数据，需要用到分布式文件系统、分布式数据库、云计算平台、网络存储以及其他可扩展的存储技术。数据集的大小使得我们很难仅依赖于关系数据库和 NAS 等共享数据存储系统，对于大数据应用来说，SAN 速度太慢。用于大数据分析的桌面统计软件和数据虚拟化软件正在开发大数据并行处理的新形式，这将使得搜索、共享、分析和虚拟化更加快速。实时或近实时的信息传递是大数据分析的一大目标，通过将大量数据集在内存中处理而达到实时分析的内存内处理系统的需求如今正日益增长。

大数据应用正成为商业竞争优势的重要渠道，尤其对于那些想通过捕获和存储巨型数据而提供数据产品和服务的企业来说更为关键。众多迹象显示，在未来几年，数据挖掘对企业将会越来越重要，更多企业会从大数据应用中获益。

应用注解

分布式计算支持

我们很难想象在没有大量台式计算机的情况下可以将一个业务运行起来，而如今，笔记本电脑和手提设备也成了必备品。为了支持如此大量的高性能设备以及部分移动设备，给企业带来了前所未有的挑战。使用合适的战略会带来很大的不同，比如店铺可以很有效地运行或者以更高的成本和更低的效率运行。

这些挑战中很重要的一个就是早已超负荷工作的支持人员面对的维修请求。唯一一种可以让企业省钱又省时地处理计算机和数据网络问题的方式是将一系列应用、计算系统和网络硬件标准化。然而，也常有例外发生，此时选择就很少了。通过为台式计算机和笔记电脑本选择单一的应用，企业可以减少授权费用。因为单独对每台机器进行授权的费用很高，但按点来授权的性价比就高得多了。此外，对技术人员来说，软件的维护也简单很

多，因为更新和故障分析的变化相对少了很多。

对于硬件来说也一样。使用单一制造商可以减少手头上的备件，技术人员对设备更为熟悉，且销售商也更熟悉且会尽量使客户满意。如果从一台装有 Windows 的机器硬转到苹果电脑或使用 LINUX 系统的机器会是一个很麻烦的过程。

对于网络和系统管理员，安全是最大的挑战，尤其当面对众多机器时。除了补丁、间谍软件、广告软件和病毒之外，还需要对抗外界来的常规攻击。很多情况下，攻击不仅仅是一个初始问题，很可能是一连串问题。例如，当一个病毒下载下来之后，通常会通过共享深入到其他用户。大部分病毒是通过邮件下载下来的，但如今，USB 成为了独立机器之间病毒传播的重要途径。在一个全分布式环境中，防治它的最好方式是预防。一个好的防病毒软件对于机器和服务器来说都是至关重要的。

一旦网络或机器被病毒感染，必须立即启动杀毒程序。标准的扫描对清除病毒可能还不够，有时需要使用可移动介质的扫描和接种步骤来移除病毒。更坏的情况是，中毒的机器可能备份到了网络中，使得服务器瘫痪和潜在的企业数据的大规模丢失，当这种情况发生时，数据很可能不能被恢复，在感染时使用任何可移动介质也会成为潜在风险。

要了解所有保护现代通信网络安全的措施是一个很难的过程，需要一名全职人员负责。如果我们加入可移动和手提设备，那么安全任务就更复杂了。因此，随着环境的不断变化，对管理员和终端用户的持续培训很重要。

如果工作人员技术完善且配备很好的支持结构，那么很多类似的问题都可以很快很容易解决。通常，IT 部门不被认为是核心业务部门，所以在预算、人员和设备上都不被优先考虑。很多案例中，计算机部门受到很少的支持，发生问题时却遭受所有的指责。由于个人计算机相比大型机而言价格低廉且复杂度低，所以企业一般会配备同等技能的人员，尽管这看起来性价比很高，但长期而言这是不合适的。

通常，我们会低估帮助台和故障呼叫中心，殊不知这个特定区域的人员和可靠性都很重要。对于大企业，故障呼叫的电话数量很大，不够有效和人员匮乏的呼叫台会减缓主业务功能的运行，也会因为过多的工时和故障时间大大地影响底线。此外，支持这样一个系统的软件必须要简单易用，且有趋势分析、调研、分类和各种报告能力。

分散系统或分布式系统会带来集中式系统没有遇到过的特殊问题。面对大量的独立节点，对问题的良好了解、适当的培训和合适的资源可以减少故障带来的经济影响，也可以减少通信系统的故障时间。

3.6 总结

随着个人计算机和移动设备的价格越来越低、功能越来越强大，分布式数据处理（DDP）的趋势越来越明显。在 DDP 中，处理器、数据和企业数据处理系统的其他方面被分散，这需要给企业提供能响应用户需求、响应时间更短且性价比更高的通信网络。DDP 系统包含水平分区或垂直分区的计算功能，也可能有分布式数据库、设备控制和交互（网络）控制。这种趋势已经促成客户机 / 服务器架构的推出和云计算的出现。

至此，我们还不准备将 DDP 的特征转换成数据通信和网络设备的需求。概括起来，我们可以说 DDP 系统涉及连通性、可用性和性能领域的业务需求，这些需求反过来指出对于给定 DDP 系统的合适的数据通信类型或网络方法。

案例研究III：管理万事达卡国际组织的大型数据仓库

这个案例研究中的主要概念包含数据仓库、大型存储系统和“大数据”。可以从 www.pearsonhighered.com/stallings 获得这个案例研究和更多知识。

3.7 关键术语、复习题和练习题

关键术语

Application Service Provider（ASP，应用服务器提供商）
availability（可用性）
big data（大数据）
centralized data processing（集中式数据处理）
client/server architecture（客户机/服务器架构）
connectivity（连接性）
database（数据库）
data center（数据中心）
Distributed Data Processing（DDP，分布式数据处理）
extranet（外部网）
horizontal partitioning（水平分区）
intranet（内部网）
partitioned database（分区数据库）
performance（性能）
peer-to-peer network（对等网络）
replicated database（复制型数据库）
vertical partitioning（垂直分区）

复习题

3.1 什么是“大数据”？
3.2 识别导致大数据在业务网络中出现的因素。
3.3 概要描述数据中心的主要特征。
3.4 什么是集中式数据处理架构？
3.5 哪些是集中式数据处理设备的主要特征？
3.6 集中式数据处理设备的优势是什么？
3.7 分布式数据处理策略是什么？
3.8 阐述在分布式环境中应用分配的 3 种方式。
3.9 描述与 DDP 相关的主要管理与 IT 组织问题。
3.10 为什么企业实现分布式数据处理系统的互连？
3.11 识别如今数据中心的主要设备类别和通信冗余。
3.12 第一层、第二层、第三层和第四层数据中心的差异是什么？
3.13 为什么企业与第三方数据中心合作？
3.14 什么是内存计算？
3.15 什么是 HANA？
3.16 简要描述操作系统虚拟化、服务器虚拟化、存储虚拟化和网络虚拟化的区别。
3.17 简要描述存储区域网络（SAN）和网络附加存储（NAS）系统的区别。
3.18 什么是“按需计算”？
3.19 客户机/服务器架构的特征是什么？
3.20 什么是应用服务提供商（ASP）？为什么企业与 ASP 合作？

3.21 识别和简要描述吸引业务客户的云计算服务的主要类别。
3.22 识别应用的水平分区和垂直分区，各给出几个例子。
3.23 什么是数据库？什么是数据库管理系统（DBMS）？
3.24 企业为什么需要分布式数据库？
3.25 说出复制型和分区数据库的区别，识别两者的主要优点和缺点。
3.26 识别并简要描述以下每个 DDP 网络含义：连通性、可用性和性能。
3.27 识别几种大数据的基础设施含义。

练习题

3.1 上网搜索大数据的最佳实践，寻找一些有关企业管理日益增长的数据量和使用数据作为竞争优势的好的信息资源。写一篇 500 ~ 1000 字的论文或 8 ~ 12 页的 PPT 来总结。

3.2 你刚接受 Holiday Inn 公司（见图 3-7）CIO 的职务，作为你的第一个官方动作，CEO 让你分析公司的计算机运作现状并给出你的意见：维持现有架构（如图 3-1 所示的集中式 IS 架构）还是转向分布式架构，或者使用两个架构给出一个综合解决方案，也可以将 ASP 和云计算服务包含进来。准备一篇 8 ~ 12 页的 PPT 在下一次员工会议上展示。

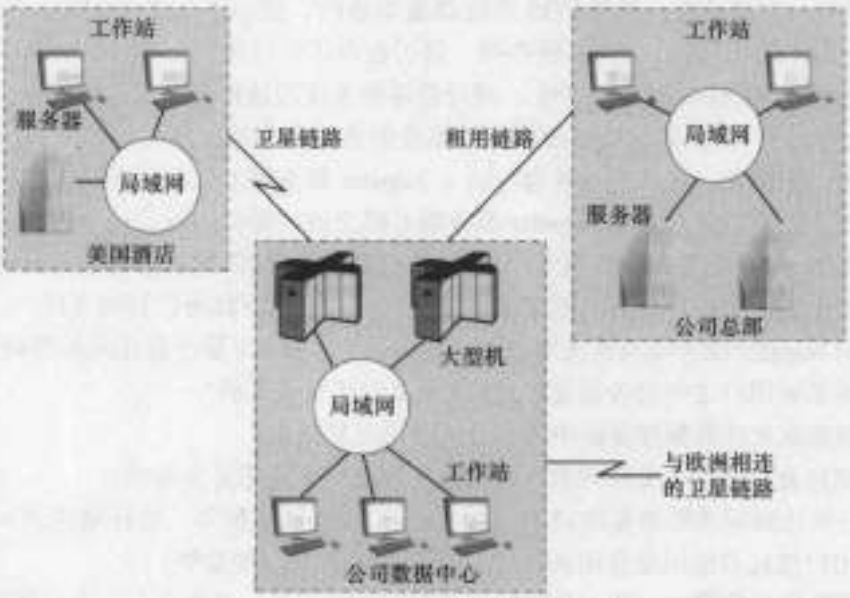


图 3-7 Holiday Inn 的信息系统架构

3.3 从全局客户机 / 服务器的角度来看，因特网由 Web 服务器、相关的数据库、服务器端的其他数据库、各种 Web 浏览器的应用程序和客户机端的相关插件构成。这种系统应该描述成垂直分布式应用处理、水平分布式应用处理还是两者的结合？

3.4 上网搜索关于内存计算系统的知识，以及它们为什么开始被企业使用。写一篇 500 ~ 1000 字的文章（或 8 ~ 12 页的 PPT），总结企业投资内存计算系统的原因以及企业如何使用这些内存计算系统。

3.5 上网搜索有关虚拟化的信息，以及驱动虚拟化技术演化发展的主要供应商。写一篇 500 ~ 1000 字的文章（或 8 ~ 12 页的 PPT），总结企业开始关注虚拟化的原因，列出为企业提供虚拟化技术和服务的主要供应商。

3.6 上网搜索有关应用服务供应商的信息，以及哪些服务是商业用户最多使用的，同时也寻找哪些 ASP 在吸引用户上做得最好。写一篇 500 ~ 1000 字的文章（或 8 ~ 12 页的 PPT），总结企业通过 ASP 访问的最流行的应用程序，并举几个在吸引用户上做得最好的 ASP 的例子。

3.7 上网搜索有关第三方数据中心的信息，以及企业网络中如何使用第三方数据中心。写一篇 500 ~ 1000 字的文章（或 8 ~ 12 页的 PPT），总结企业与第三方数据中心合作的主要原因，以及企业网络使用第三方数据中心的主要方式。

3.8 两个用于零售信贷授权的数据中心位于两个不同的主要人员密集中心，并且这两个中心被一个大的人员稀疏的区域隔开。每个数据中心都覆盖一个特定的地理区域，存储此区域内持卡者的账户状态。只有当一个区域的持卡用户到另一个区域购物时，这两个数据中心才会有交互。

a. 分辨这两个数据中心的关系是客户机 / 服务器还是对等的？

b. 分辨零售信贷系统的数据库是分区型还是复制型？

c. 这两个数据中心是否应该合并成一个集中式基于云的设备？阐述理由。

3.9 零售业是第一个采取分布式数据处理的行业，与集中型 POS 系统不同，零售商使用分布式数据库，也就是说，所有 POS 系统都是本地的，但与中央系统相连。所有销售商的价格都是固定的，并由中央系统存储。每天在商店开门前，相关价格会从中央系统复制并下载到每个店铺的 POS 系统上。请分析零售业使用这种分布式系统的经济优势。

3.10 Napster 曾是一个著名的提供很多增值服务的音乐共享系统，但由于侵权问题，它被法院裁定停止营业。系统是这样运行的：Napster 服务器上保存包含所有用户音乐文件的数据库，用户需要登录到 Napster 服务器并提交他们提供的音乐清单，接着每个用户就可以向 Napster 服务器发送搜索请求，以获得与请求相匹配的用户清单。请求者可以选择列表上的一个用户，并与他建立直接联系，并请求下载所需要的文件。

a. 辨别 Napster 服务器与系统用户之间的关系是客户机 / 服务器还是对等的？

b. 辨别系统用户之间的关系是客户机 / 服务器还是对等的？

c. 辨别音乐文件数据库是集中式、分区型还是复制型？

d. 辨别包含可用音乐文件列表所在的数据库是集中式还是分布式？

3.11 一个公司计划采用赊销系统对 10 个大型人口中心提供服务。它计划使用一个数据库来存储用户信息和信用交易记录，IT 部门正考虑以下两种选择：

a. 使用集中式数据库，在一个数据中心存储数据副本，供各个人口中心使用。

b. 使用复制型数据库，在多个数据中心（每个人口中心各一个）存储副本，并同步所有副本。

准备一篇 8 ~ 12 页的 PPT，总结每种选择的优势和劣势并给出建议，在下一次 IT 员工会议上展示。

3.12 上网搜索有关固态存储技术的信息以及它在数据中心和大数据环境下逐渐流行的原因，寻找几个广泛使用的高性能固态存储设备的图像。准备一篇 8 ~ 12 页的 PPT 来展示这些例子，并阐述固态存储与大数据管理的联系。

第二部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

数据通信

第 4 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

数据传输

学习目标

通过本章的学习，读者应该能够：

- 理解将音频、数据、图像和视频表示成电磁信号的多种方法。
- 描述模拟波形和数字波形的特征。
- 描述多种形式的传输质量损耗，该损耗能影响信号质量和通信介质上的信息传递。
- 识别影响信道容量的因素。

数据和信号构成任何计算机网络的两大基石。在前面两章中，我们涉及了企业网络中数据获取、存储和传输的主要类型。在本章中，我们给出与信号相关的一些基本概念。

为了在已连接到计算机网络中的两个设备之间传递数据，这些数据必须要转换成合适的信号。在本章中，我们主要关注用来传递数据的一种特殊信号：电磁波（electromagnetic wave）。我们可用电磁信号来表示所描述的各种信息形式（音频、数据、图像和视频），并在合适的传输介质上传递它们。

我们首先看一看能用来传输信息的电磁信号的类型以及它们的基本特征。为此，我们给出表示这四种信息类型的最直接的方法。然后，我们讨论用电磁信号传输数据时的传输质量损伤，该损伤能引入传输错误并降低传输效率。在本章的最后一节中，我们讨论信道容量是怎样与信号特征以及信号损伤相关的。

通过掌握本章所介绍的概念，对计算机网络中的商务方面感兴趣的读者能从多个方面获益。最重要的是，掌握了计算机网络的基本原理，为理解后继章节中更深层次的计算机网络专题打好了基础。本章介绍了许多术语，这些术语能帮助你与计算机网络专家熟练地进行交流。它也能帮助你理解通信信道中数据传输容量的限制因素，并且让你明白为什么所有的通信形式（音频、数据、图像和视频）都要从模拟传输系统迁移到数字传输系统。

4.1 传递信息的信号

4.1.1 电磁信号

几乎所有用于通信的信号都是电磁波谱的一部分。电磁能量通过波的形式从源点向外发散传递。在计算机网络中，源点通常称为传送者，传送者产生的电磁能量以电磁波的形式在传输媒介上进行传递。电磁能量传播的典型例子包括电能在电缆上传输，以及无线电信号的广播。可见光是电磁能量传播的另一种例子。

如第 2 章描述的那样，数据可以模拟或数字的形式存在。模拟数据表示为连续波形，即在任意给定的时间点，在一个最大值和最小值之间存在无数个点。音乐和视频，在它们的自然状态，是模拟数据的例子。人的声音也是一样。当人对着传统电话的话筒说话时，话筒中

的接收器将空气中的语音波形转换成模拟电磁波，并且该电磁波有最大电压值和最小电压值。

电磁信号有许多基本特征，这些特征对于理解计算机网络中的数据传递非常重要。首先，时间和时间间隔是定义大多数电磁信号的基本概念的重要组成部分。当用数学方式表示时，电磁信号是时间的函数。然而，电磁信号也可表示成频率的函数，即传递的信号由不同的频率部分组成。实际上，大多数的信号是由倍频组成的，包括声音、视频和音频信号。正是因为倍频的存在，我们才能将一个乐器与另一个乐器区分开，或者将一个人的声音与另一个人的声音区别开。我们可从时域或频域来理解电磁信号。实际上，要了解数据传输，用频域的观点解释信号比用时域的观点解释信号更为重要。这其中的原因在我们讨论信号的损伤（如噪声），以及怎样使得在计算机网络中的影响最小化时，会看得很清楚。

下面分别介绍电磁信号的时域和频域。

1. 时域的概念

从时间角度来看，电磁信号可以是模拟的也可是数字的。**模拟信号**（analog signal）是指信号强度随着时间平滑地变化。也就是说，信号中间没有断点或不连续。**数字信号**（digital signal）是指信号强度在一段时间内保持在一个固定值，随后变到另一个固定值。图4-1给出了两类信号的例子。模拟信号可用来表示语音、音乐或视频，数字信号可用来表示二进制1和0。

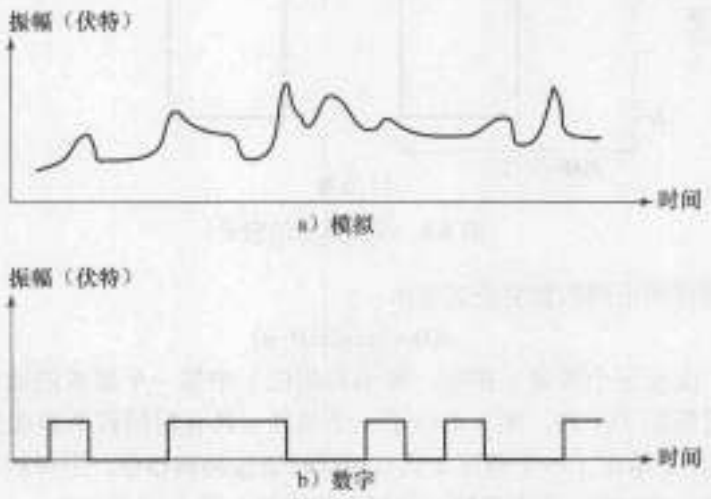


图4-1 模拟和数字波形

最简单的一类信号是**周期信号**（periodic signal），其中相同的信号模式随时间重复出现。图4-2展示了一个周期模拟信号（正弦波）和一个周期数字信号（方波）。正弦波是一种基本的模拟信号。一个常规的正弦波能用三个基本要素表示：峰值振幅（A）、频率（f）和相位（φ）。**峰值振幅**（peak amplitude）指的是在一个参考点上下的波形最高值。它代表了信号随时间变化的强度。该值典型的是用伏特来衡量。有些时候，振幅能表示以瓦来衡量的信号的功率电平，或者以安培来衡量的信号的电流电平。它更通常地代表的是信号的电压电平。

频率是指在一个给定的时间帧内信号完成一个完整周期所需的时间。每秒钟内完整的信号重复次数通常是用每秒钟内的循环次数或用赫兹（Hz）来表示的。一个循环的长度或时间间隔称作信号的**周期**（T）。该周期可用频率（f）的倒数计算得到，就是说，周期等于1/频率

（或者 $T=1/f$）。相位是指在信号周期内的某时间点上波形的位置测量。本章的后面再详细地介绍相位。

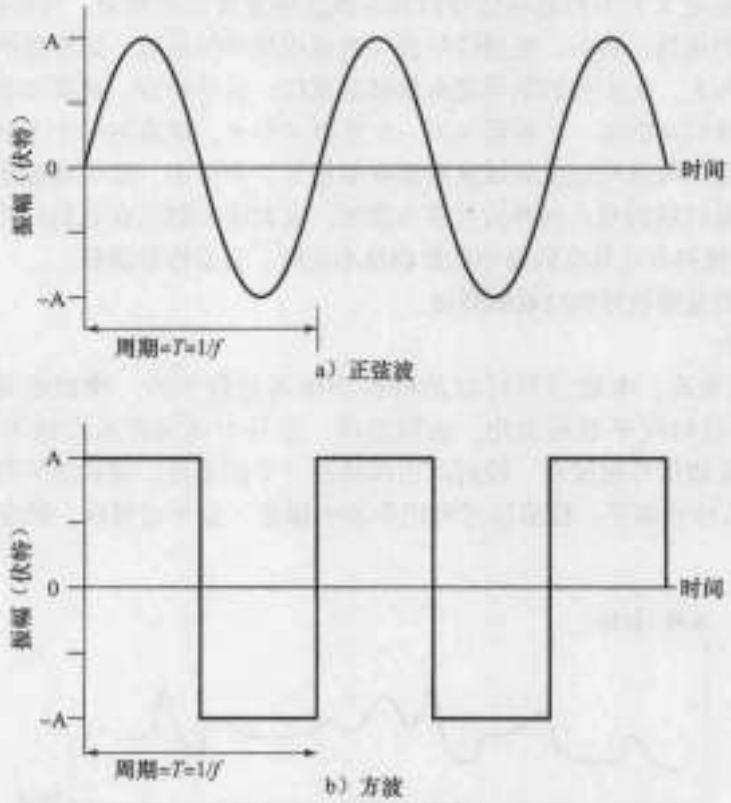


图 4-2　周期信号的例子

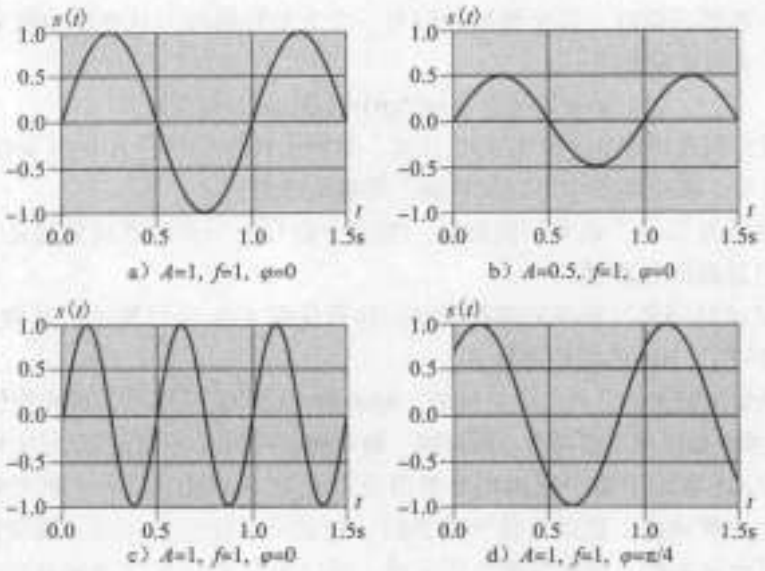
常规的正弦波可用下列的数学公式表示：

$$s(t)=A\sin(2\pi ft+\varphi)$$

图 4-3 给出了改变三个要素（振幅、频率和相位）中每一个要素的效果。在图 a 中，频率是 1Hz，因此周期是 $T=1$ 秒。图 b 给出了一个与图 a 具有相同频率和相位，但峰值振幅只有 0.5 的正弦波。图 c 给出了一个与图 a 具有相同峰值振幅和相位，但每秒频率是 2($f=2$) 的正弦波，这意味着图 c 中的波形周期是图 a 中波形周期的一半，即 $T=1/2$。

图 4-3d 展示了将图 4-3a 中正弦波进行 45 度相位偏移后的正弦波形。在图 4-3a 中，波形以一个重复的模式上下震荡，从不突然改变。相位移动（改变）则引起一个给定时间点上波形的前跳（或后退）。前跳半个信号周期表示 180 度的相位改变，前跳四分之一个信号周期则产生了 90 度的相位改变。在图 4-3d 中，相位移动是 45 度，相当于波形前跳了八分之一个信号周期（45 度的相位移动可用数学方法表示为 $\pi/4$ 弧度，一个完整的波形周期可用数学方法表示为 2π 弧度 =360°=1 周期。）45 度、135 度、225 度和 315 度的相位移动在模拟传输系统中是非常普遍的。

图 4-3 中的水平轴是时间，图形展示了空间某点对应的信号值是时间的函数。这些只在比例上有区别的相同图形，可用来表示某时间点上的信号值是距离的函数。例如，对于一个正弦传递（如电磁无线电从无线电接收天线传播一段距离，或声音从扩音器传播一段距离），在一特定的时间段内，信号的强度以离源点距离的函数形式发生正弦变化。换句话说，就是信号离源点越远，其强度越弱。

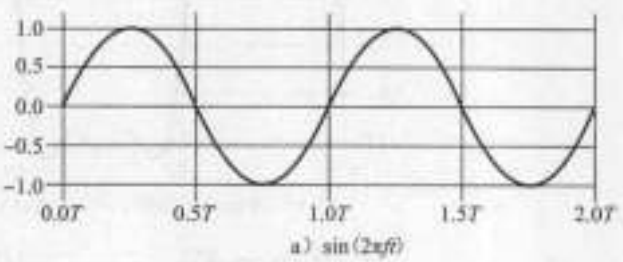


a) A=1, f=1, φ=0　b) A=0.5, f=1, φ=0

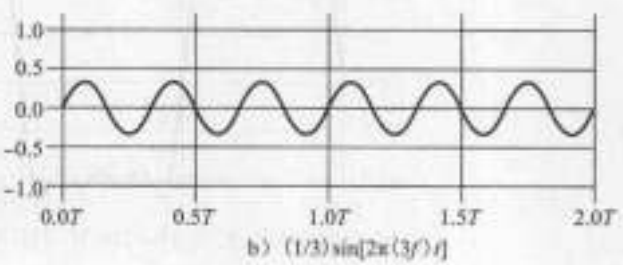
c) A=1, f=1, φ=0　d) A=1, f=1, φ=π/4

图 4-3　$s(t)=A\sin(2\pi ft+\varphi)$

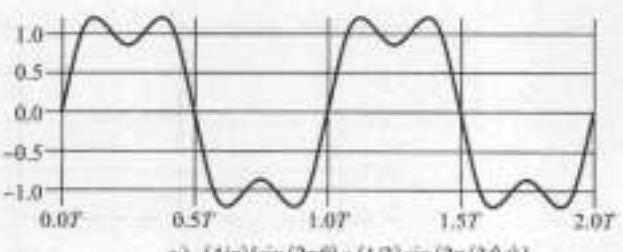
波长的概念能帮助我们理解为什么相同的正弦形式能用时间或空间的函数表示。信号的波长（λ）定义成一个周期内信号传播的距离，换句话说，即两个连续周期对应的相位点之间的距离，如最大振幅处或者波形跨越 0 处。波长通用以米来衡量。波长能用来简单地理解为什么两个不同频率的正弦波能由同一源点传递，并且能以相同的速率（v）传播。每个波的波长与它的周期相关：$\lambda=vT$（波长 = 速率 × 空间周期）。从数学角度来看，这就意味着 $\lambda f=v$（波长 × 频率 = 速率）。对于以相同速率传递的两个波形，频率低的波形具有较长的波长。



a) $\sin(2\pi ft)$



b) $(1/3)\sin[2\pi(3f)t]$



c) $(4/\pi)[\sin(2\pi ft)+(1/3)\sin(2\pi(3f)t)]$

图 4-4　频率成分的叠加（$T=1/f$）

如第 6 章所示，理解如何做到在同一通信介质上以同样速率传递两个或多个频率，对于理解一些类型的多路复用如何工作很重要。同样地，理解多个信号怎样在自由空间（如卫星通信）共享传输信道也很重要。在该自由空间中，$v=c$，即自由空间中的光速，近似为 3×10^8m/s。

2. 频域的概念

至此，我们用的是简单的、周期性的正弦波传递方式作为例子，来解释电磁波的基本组成和特征。实际生活中我们很难发现简单的、周期性的正弦波传递方式，最有可能碰到的是由多种波形组合而成的复合信号。例如，图 4-4c 展示了如何从图 4-4a 和图 4-4b 所描述的波

形组合形成一个新的正弦波，该正弦波近似为一个方形数据波。从数学角度来看，图 4-4c 中正弦波的数学公式可表示如下：

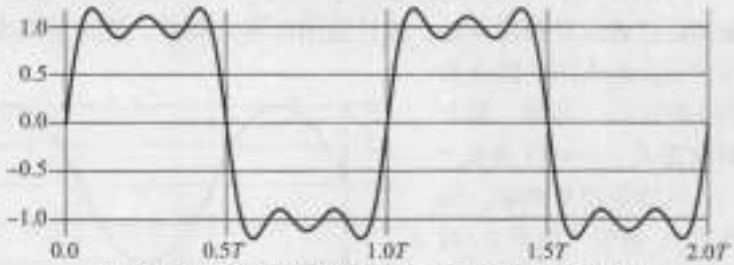
$$s(t)=(4/\pi)\times\{\sin(2\pi ft)+(1/3)\sin[2\pi(3f)t]\}$$

该信号的组成成分就是频率为 f 和 $3f$ 的正弦波，这两个频率分别包含在图 4-4a 和图 4-4b 正弦波所对应的公式中。从这张图中可以发现两个有趣的现象：

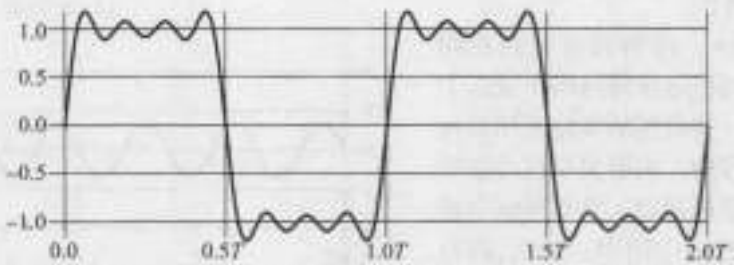
- 第二个频率是第一个频率的整数倍。当一个信号的所有频率成分都是某个频率的整数倍时，后者就称为**基频**。
- 整个正弦波的周期与基频的周期相等。这可从图 4-4c 中可看出，其中成分 $\sin(2\pi ft)$ 的周期是 $T=1/f$，$S(t)$ 的周期也是 T。

通过同时添加足够多的、具有合适振幅、频率和相位的正弦信号，可构建任意的电磁信号。换句话说，任意的电磁信号可由具有不同振幅、频率和相位的周期性模拟信号（如正弦波）组成。

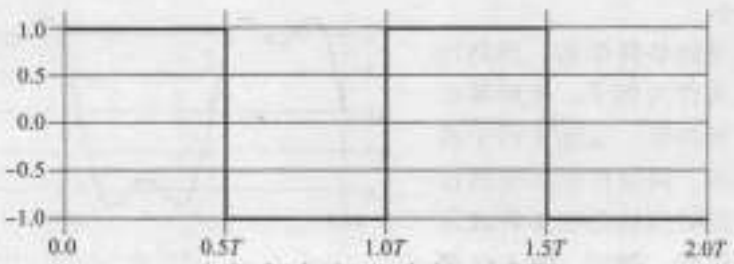
图 4-4 和图 4-5 展示了多个模拟信号能组合产生出一个数字信号。该处理过程可用一个数学分支很好地解释清楚，那就是傅里叶分析，它表明了任何复杂的、周期性的波形（包括数字信号）都可由简单的、周期性的波形组成。通过向图 4-4c 所描述的复合波形中添加更多的波形（波形的频率为基频的整数倍），所得到的波形就更像图 4-4c 所描述的方形数字信号。这个组合信号在形状和行为上也更像数字信号。虽然数字信号通常被描述成与模拟信号没有任何共同点，实际上它们都是从正弦波形组合而成的。



a）$(4/\pi)[\sin(2\pi ft)+(1/3)\sin[2\pi(3f)t]+(1/5)\sin[2\pi(5f)t]]$



b）$(4/\pi)[\sin(2\pi ft)+(1/3)\sin[2\pi(3f)t]+(1/5)\sin[2\pi(5f)t]+(1/7)\sin[2\pi(7f)t]]$



c）$(4/\pi)\sum(1/k)\sin[2\pi(kf)t]$，$k$为奇数

图 4-5　方波的频率成分（$T=1/f$）

从频率角度而不是从时间角度来看一个信号，其重要性在我们继续讨论信号原理时会体现得更清楚。

我们还需要知道一些其他有关频率的概念，包括频谱（spectrum）和带宽（bandwidth）。信号的**频谱**指的是信号所包含的频率的范围。对于图 4-4c 中的组合信号，它的频谱从 f（图 4-4a 所示）延伸到 $3f$（图 4-4b 中波形的频率）。信号的**绝对带宽**（absolutebandwidth）是指它的频谱宽度。在图 4-4c 的例子中，带宽是 $3f-2f=f$。对多数信号而言，其带宽是无限的。但是，一个信号的绝大部分能量集中在相当窄的频率带宽内，这个频带被称为**有效带宽**（effective bandwidth），或者就称为**带宽**（bandwidth）。正如我们即将看到的，一个传递人类语音的电话信道，其有效带宽比它的绝对带宽要小得多。

一个信号的信息承载能力与它的带宽有着直接的关系：带宽越大，则信息承载能力越强。举个简单例子，我们来看一下图 4-2b 中的方波。假设我们让正脉冲（振幅为 A）代表二进制 0，负脉冲（振幅为 $-A$）代表二进制 1，则该波形代表了二进制数字流 0101…。每个脉冲的持续期（即时间间隔）是半个信号周期（[1/2]T 或 1/[2f]），那就是说数据率是每周期 T 两个脉冲或者每秒 $2f$ 比特（bps）。

图 4-2b 中的信号有哪些频率成分呢？要回答这个问题，我们再来考虑一下图 4-4。通过将频率 f 和 $3f$ 的正弦波叠加在一起，我们可以得到一个与原方波相似的波形。让我们继续这个过程，再叠加一个频率为 $5f$ 的正弦波（如图 4-5a 所示），我们再加上一个频率为 $7f$ 的正弦波（如图 4-5b 所示）。当我们叠加更多 f 的奇数倍的正弦波，并按比例对这些正弦波进行调整，所形成的波形就越来越接近方波[⊖]。

如果我们将带宽限制在最前面的 3 个频率成分会发生什么呢？我们已经在图 4-5a 中看到了答案。正如我们所看到的，所得到波形的形状已经相当接近原方波了。

我们可用图 4-4 和图 4-5 来说明数据率与带宽之间的关系。假定我们正在使用一个数字传输系统，该系统能够传递带宽为 4MHz 的信号。让我们试着以图 4-5c 中方波形式传递一组 0、1 交替的序列，能获得什么样的数据率呢？我们考虑如下 3 种情况。

1）**情况 1**。假设我们的方波近似于图 4-5a 中的波形。虽然这是个“失真”的方波，但它与方波足够相似，接收器应该能够区分出二进制 0 和 1[⊜]。在这种情况下，如果带宽为 4MHz，则能获得 2Mbps 的数据率。

2）**情况 2**。现在我们假定带宽为 8MHz，让我们再看看图 4-5a，这次 f=2MHz。在这种

⊖ 实际上，振幅为 A 和 $-A$ 的方波，其频率成分可表示为：

$$s(t)=A\times\frac{4}{\pi}\times\sum_{k\text{为奇数}=1}^{\infty}\frac{\sin(2\pi kft)}{\pi}$$

这样，这个波形就有无限多的频率成分以及无限大的带宽。然而，第 k 个频率成分（即 kf）的峰值振幅为 $1/k$。因此这个波形的大部分能力集中在最前面的几个频率成分中。

⊜ 如果令 $f=10^6$ 循环 / 秒 =1MHz，那么信号

$$s(t)=\frac{4}{\pi}\times\left\{\sin[(2\pi\times10^6)t]+\frac{1}{3}\sin[(2\pi\times3\times10^6)t]+\frac{1}{5}\sin[(2\pi\times5\times10^6)t]\right\}$$

的带宽就是 $(5\times10^6)-10^6=4$MHz。请注意，由于 f=1MHz，那么基频的周期就是 $T=\frac{1}{10^6}=10^{-6}=1\mu s$。如果我们将这个波形看成是 0 和 1 的比特序列，那么每 0.5μs 就传递 1 比特数据，因此数据率就是 $2\times10^6=2$Mbps。

情况下，有效的数据率为 4Mbps。[⊖]因此，假如其他项保持不变，如果带宽加倍，则数据率也加倍。

3）**情况 3**。现在假设图 4-5c 中的波形接近方波，那就是说，图 4-4c 中正、负脉冲之间的差别足够大，这样波形才能成功地用来表示 0 和 1 的比特序列。在这种情况下，带宽和数据率都为 4Mbps[⊖]。

以上情况总结如下：

- **情况 1**　带宽 =4MHz，数据率 =2Mbps；
- **情况 2**　带宽 =8MHz，数据率 =4Mbps；
- **情况 3**　带宽 =4MHz，数据率 =2Mbps。

因此，在存在噪声和其他损伤的情况下，依据接收器区分 0 和 1 之间差别的能力，给定的带宽可以支持不同的数据率。

我们来总结一下前面所讨论的关键点。第一，数字信号是一种由多个模拟正弦波组成的电磁信号。它所包含的成分越多，就越接近如图 4-2b 所示的理想的方波。第二，任何理想的方波有无限大的带宽。这就意味着，数字信号理论上拥有无限大的信息运载能力。例如，通过减少代表二进制 0 和 1 的脉冲的宽度，我们就能在给定的时间段内传递更多的信息。这就导出了第三个关键点：当数字信号在通信介质上传递时，是所使用的传输系统限制了能够传输的信息总量。对于任意给定的介质，越大的带宽常伴随着越多的数据丢失。如果一个业务提供商想通过相同的介质传递更多的数据量，他就必须在传输系统中投入更多。这就导致业务提供商为在带宽和通信代价之间追求可接受的平衡，往传输介质上发送尽可能多的数据，即使这意味着采用的不是理想的波形来承载数据。因此，如果让他们在情况 2 和情况 3 中做选择，他们可能会选择情况 3，特别是当在情况 2 下要取得多点的带宽而需要付出更大的代价时。

如我们将在 4.2 节介绍，限制带宽使得信号损伤产生失真的可能性增大，从而使接收端更难正确解析所接收到的信号。带宽限制得越多，则失真得越厉害，接收端越容易解析出错。

4.1.2　模拟信号

1. 音频信号

就像模拟信号的值是连续变化的一样，模拟信息也是具有连续值的信息。模拟信号已在第 2 章介绍过了。

我们最熟悉模拟信息的例子是音频（或声音）信息，它是一种声波，能直接被人类察觉到。声音信息的一种形式是人类的话音，它由频率范围在 20Hz ~ 20kHz（20 000Hz）的频率成分组成。人类话音和其他声音信息能比较容易地转换成电磁信号，以便于传输（见图 4-6）。具体的转换过程是将声音频率（其振幅用音量衡量）转换成电磁频率（其振幅用瓦特衡量）。传统的模拟电话话筒中包含一个简单的装置，即声音传感器，来实现该转换过程。

因此在一个模拟电话系统中，语音声波是用电磁信号来表示和传递的。为了能够传递人

⊖ 与前面的推理方法相同，信号的带宽为 $(5\times2\times10^6)-(2\times10^6)=8$MHz。在这种情况下，$T=1/f=0.5\mu s$。结果是，对于 4Mbps 的数据率，每 0.25μs 传递 1 比特数据。

⊖ 如在情况 2 中那样假设 $f=2$MHz 和 $T=1/f=0.5\mu s$，其结果是在 4Mbps 数据率下，每 0.25μs 传递 1 比特数据。利用图 4-4c 中的波形，信号的带宽是 $(3\times2\times10^6)-(2\times10^6)=4$MHz。

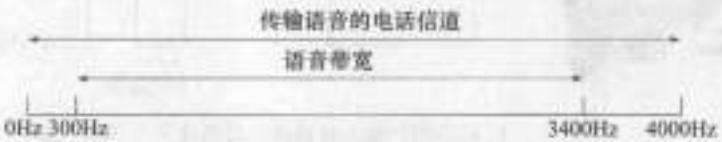
类话音中所有的频率范围，电话电路必须具有 20kHz 的带宽。然而，在实际的传统电话网中，其模拟语音信道的带宽比 20kHz 要小很多。



在这个包含典型模拟信号的图形中，振幅和频率的变化反映了话音或音乐中音量和音调的渐变过程。类似的信号用来传递电视画面，但会采用高得多的频率。

图 4-6 声音输入到模拟信号的转换

通常声音的保真度（精度）都经过特意的折中考虑。采用较小的带宽能使语音的传输代价较为合理，随着带宽的增大，所需的传输代价也在增加。另外，即使人类语音的频谱是 20Hz 到 20kHz，测试表明一个窄得多的带宽（范围为 300 – 3400Hz）也能生成可接受的再生语音。也就是说，当除去人类话音中超出该范围的频率成分时，剩下的听起来也很自然。因此，电话网络中能使用一些将声音限制在那个窄带宽中进行传输的通信设备（见图 4-7）。



人类的语音能产生具有多个频率的声波，但是自然发音能限制在300 – 3400Hz频率范围（或频带）内。电话设备能允许的声音带宽为4000Hz，其中包含了在每个频率范围末尾的防护频带，以在多个语音信道复用时，防止相邻语音之间的干扰

图 4-7 语音频带

如图 4-7 所见，用于语音传输的电话信道，其实际的频带宽度是 4kHz，而不是 3.1kHz。额外的带宽是用来隔离在语音信道中传输的信号，免得与相邻语音信号的信号产生干扰[⊖]。当传输的时候，电话听筒中的声音传感器将接收到的语音声波转换成模拟电磁信号（频率范围为 300 – 3400Hz），该信号然后通过电话网络传递到对方的电话接收器，电话接收器根据接收到的电磁信号再生出声波。

2. 视频信号

就像电话听筒的功能一样，电视的摄像头生成视频信号并将其传递到接收电视中。摄像头中有一个感光板，能对景色进行光学聚焦。电子束在感光板上从左到右、从上到下地进行扫动，采用了与图 2-5 中相同的方法（描绘了模拟视频信号接收器中的视频扫描过程）。

在电子束扫动过程中，产生出与特定点上景色亮度成比例的模拟电子信号。扫描时，采用的是每秒 30 次完整扫描的速率，共扫描 483 行[⊜]。

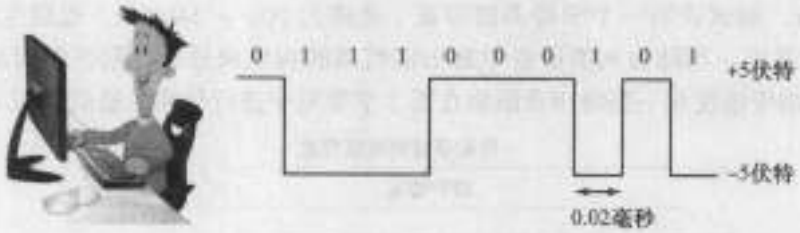
⊖ 如第 6 章所示，不同的信号能通过占用频谱中不同的频率范围，从而在相同的传输介质进行传输，该过程称为复用。这需要额外的带宽或防护频带来防止相邻信号之间形成干扰。

⊜ 这是一个近似值，其中考虑了因垂直的折返间隔而损失的时间。实际上美国标准是 525 行，其中的 42 行在垂直折返中丢失。因此，水平扫描频率是 525 行 × 30 扫描 / 秒 =15 750 行每秒，或者 63.5μs/ 行。在这 63.5μs 中，大约 11μs 可用于水平折返，剩下的 52.5μs 用于每个视频行。

为了以合理的速率传递模拟视频信息，通常需要 4MHz 的带宽。与在电话网络中传递语音一样，在用有线电视或广播传递视频信号时，也需要额外带宽或防护频带来隔离视频信号。在有防护频带情况下，彩色视频信号的标准带宽为 6MHz。

4.1.3　数字信号

数字信号的概念通常是指表示二进制数字 1 和 0 的电磁脉冲的传输。例如，用一个恒定的正电压脉冲表示二进制 0，一个恒定的负电压脉冲常量表示二进制 1。另一种方法的是，用一个恒定的电压脉冲表示一个二进制数字，而没有电压脉冲表示另一个二进制数字。不管采用上述哪种方法，表示的都是二进制信息。二进制信息一般由计算机、终端和其他的数据处理设备产生，在传输时需要转换成数字电压脉冲，如图 4-8 所示。就像第 2 章提及的那样，数（number）[⊖]或文本（text）通常需要依据一定的编码方案（ASCII 或 UTF-8）转换成二进制串。在转换为二进制格式后，信息就能转换成数字信号。



PC机的用户输入转换成二进制数字（1和0）串。这是典型的数字信号的图片，其中-5伏特表示二进制1，+5伏特表示二进制0。在每秒50 000比特的数据率（即50Kbps）下，每位信号的持续时间是0.02毫秒

图 4-8　PC 机输入转换成数字信号

第 2 章也提到，任何类型的数据都能表示成数字信号。将模拟数据（如音乐、视频和语音）转换成二进制格式，则需要采样和量化。模拟信息的数字编码将在第 5 章讨论。

4.2　传输损伤和信道容量

在任何通信系统中，由于存在各种各样的传输损伤，接收到的信号通常与发送的信号有差别。这些损伤通常称为噪声（noise）。噪声是能降低信号质量的电磁或电能。噪声存在于各种类型的数据传输系统中，它的影响范围包括从背景中不易觉察的“嘶嘶”声到完全的信号

⊖ 对人类而言，数通常是用十进制格式表示的。在十进制系统中，通常采用 10 个不同的数字来表示数。数中每个数字的不同位置决定了它的值。因此，十进制数 83 就是 8 个十乘以 3；83=(8×10+3)，数 4728 就是 4728=(4×1000)+(7×100)+(2×10)+8。

十进制系统有一个基数 10。这就意味着，数中的每个数字都乘以 10 的指数，该指数值与该数字的位置相对应。因此，$83=(8\times10^1)+3$，$4728=(4\times10^3)+(7\times10^2)+(2\times10^1)+8$。

在二进制系统中，只有两个数字 1 和 0。因此，二进制系统中的数表示成基数 2。就像十进制表示法一样，二进制数中的每个数字的值依赖于它在数中的位置。例如，10=(1×2)+0= 十进制 2，11=(1×2)+1= 十进制 3，$100=(1\times2^2)+(0\times2)+0$= 十进制 4。

二进制表示法经扩展后也能表示分数和负数，具体的细节不在本书的讨论范围。

丢失。对于模拟信号，噪声能引入各种各样的随机修改，从而降低信号的质量。对于数字信号，噪声能导致位错误：表示位1的信号发生失真，形成的信号被接收端解析为位0，反之亦然。

模拟信息和模拟信号最大的不足就是，很难将噪声从原始信号中分离出来。因为噪声本身也是模拟波形，当噪声产生时，它将叠加到原始的模拟信号上，生成使传输波形发生失真的复合信号。因为噪声能降低信号的质量，大多数的数据传输系统都尽可能地减少噪声。

在这节中，我们考察数据传输系统产生噪声的主要原因，以及这些噪声是如何损害信号质量和通信链路的信息承载能力的。第5章将探寻弥补这些损伤的方法。

对于导向传输介质（如双绞线、同轴电缆和光纤），最重要的信号质量损伤源如下：

- 衰减和衰减失真。
- 延迟失真。
- 噪声。

在无线传输中，信号损伤最有可能由如下的原因导致：

- 自由空间损耗。
- 大气层吸收。
- 多径衰减。
- 折射。
- 热噪声。

4.2.1 有导向的传输介质

1. 衰减

当电磁信号沿着任何传输介质传递时，随着距离的加大，其强度逐渐变弱，这通常称为衰减。衰减导致了如下需考虑的三种情况，网络专家们不能忽视这些：

1）接收的信号必须有足够的能量，使得接收器中的电子线路能正确检测和解析信号。

2）为保证信号能被无误地接收，信号必须保持比噪声高得多的电平。

3）频率越高，则衰减越大，从而导致了失真。

针对第一种和第二种情况，可用留意信号强度以及使用放大器或中继器来解决。在计算机网络中，数据传输发生在发送端和接收端之间，在传输介质上进行传输。在一个简单网络中，发送端和传输者之间可能存在一条直接的链路。如果发送端和传输者之间的链路距离很短，就不需要采取措施来弥补衰减。如果发送端和接收端之间的距离比较大，衰减会比较严重，需要在两者之间添置一个或一些中间设备来弥补衰减。在模拟信号情况下，中间设备使用的是放大器，来增强信号的振幅或能量。理想情况下，放大器不改变信号的信息内容。但是实际上，放大器通常会给信号引入失真。如果发送端和传输者之间的传输路径上采用了多个放大器，则这些失真会累积起来。在数字信号情况下，用来弥补衰减的中间设备是中继器。中继器从它的一边接收输入信号，恢复出原始的二进制波形，然后在它的另一边发送一个新的数字信号（见图4-9）。中继器不累积失真。但是，如果中继器在从输入信号恢复出二进制波形的过程中出错，则该错误将一直在传输线路上存在，最终到达接收端。

第三个需要考虑的，也就是衰减失真，对于模拟信号需要特别注意。由于不同的频率其衰减不同，并且大部分的模拟信号都是由不同频率成分组成的合成信号，接收到的信号不仅在能量上会减弱，而且还会有失真。为了应对这个问题，可采用一些技术来使得整个频带的

衰减均衡。在电话线中通常使用加感线圈来改变电话线的电路特性，从而平滑衰减的影响。用来使电子信号中的频率成分均衡的设备称为均衡器。

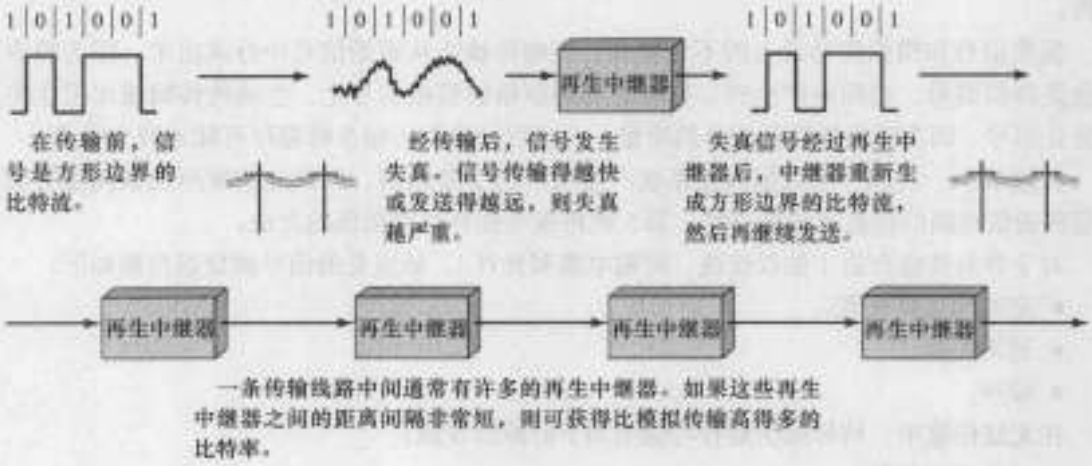


图 4-9　再生中继器

如前面所述，数字信号通常也是由多个频率组成的。然而，数字信号的大部分能量通常集中在一个较窄的频带内，因此其衰减失真问题就没有模拟信号严重。

2. 延迟失真

延迟失真是发生在传输电缆（如双绞线、同轴电缆和光缆）上的一种现象，而当信号通过天线在空间传播时，延迟失真就不会发生。延迟失真是由于信号的不同频率成分在电缆上的传播速率不一样所导致的。对于给定带宽的信号，接近信号中心频率的频率成分，其传播速率最大，而越往频带边界则传播速率越小。因此，信号的不同频率成分到达接收端的时间各不相同。

这种影响之所以称为延迟失真，是由于信号的不同频率成分引起了延迟的变化，从而导致了接收信号的失真。延迟失真对于数字数据特别关键。由于延迟失真的存在，对应一个比特位置的信号能量会溢出到对应另一个比特位置，从而导致接收端解析信号错误。这严重限制了数字数据的数据率。

3. 噪声

当信息以电磁信号的形式传输时，所接收的信号中包含了所传递的经过衰减的信号，以及由传输系统引入的各种失真，再加上在发送端和接收端之间某些地方所引入的不需要的电磁能量。对于后者，由于它不是所期望的信号，因此将其称之为噪声。噪声是影响通信系统性能的主要限制因素。

噪声可分为 4 类：

- 热噪声。
- 互调噪声。
- 串扰。
- 脉冲噪声。

热噪声是由导体中的电子热运动引起的。在数据通信介质上或多或少地会存在热噪声，其程度取决于介质的温度。当温度升高时，介质中的电子运动加剧，从而增加了介质中的噪声电平。热噪声在整个频谱范围内是均匀分布的，因此通常称为白噪声。这种噪声是一种连续的噪声，就像我们在收音机调台时所听到的静电干扰一样。将信号通过过滤器的过滤，可

降低热噪声，但是该噪声是不能完全消除的，因此它就限定了通信系统的性能上界。

当具有不同频率成分的多个信号共享同一个传输介质时，可能会导致互调噪声。[⊖]互调噪声能产生一种信号，该信号的频率是两个原始频率的和或差值，或者是这些频率的倍数。例如有两个信号，一个信号的频率为4000Hz，另一个信号的频率为8000Hz，它们使用相同的传输介质，可能产生出12 000Hz的信号能量。互调信号就会干扰频率为12 000Hz的第三个信号。

串扰每个人都可能经历过，如在打电话时可能会听到其他人的电话对话，它是信号线路之间不希望的耦合。它能由相距较近的电缆（如电话线中的两组双绞线）之间的电子耦合或通过天线传输的信号之间的重叠产生。典型地，串扰不会降低信号质量。它对数据传输的影响等于或小于热噪声对数据传输的影响。

到目前为止所讨论的各种类型的噪声，其对信号失真的影响一定程度上是可预测的和持续的。因此可以设计传输系统来处理它们。但是脉冲噪声是非持续的，它由短时间内的一些不规则脉冲或噪声尖刺组成，并且振幅相对比较高。典型的脉冲噪声是干扰模拟信号传输的能量模拟突发。有多种原因导致脉冲噪声，包括外部的电磁干扰，如闪电以及通信系统中的缺陷和瑕疵等。

对模拟数据来说，脉冲噪声通常只会产生非常小的影响，例如语音传输中会产生一些嚼啪声或咯哒声，但不会损失语音的完整性。然而在数字数据通信中，脉冲噪声是主要的错误源。例如，0.01s持续时间的能量尖刺不会损坏任何的语音信息，但在56Kbps传输速率下能丢失大约500比特的数据。图4-10是脉冲噪声对数字信息造成影响的例子。

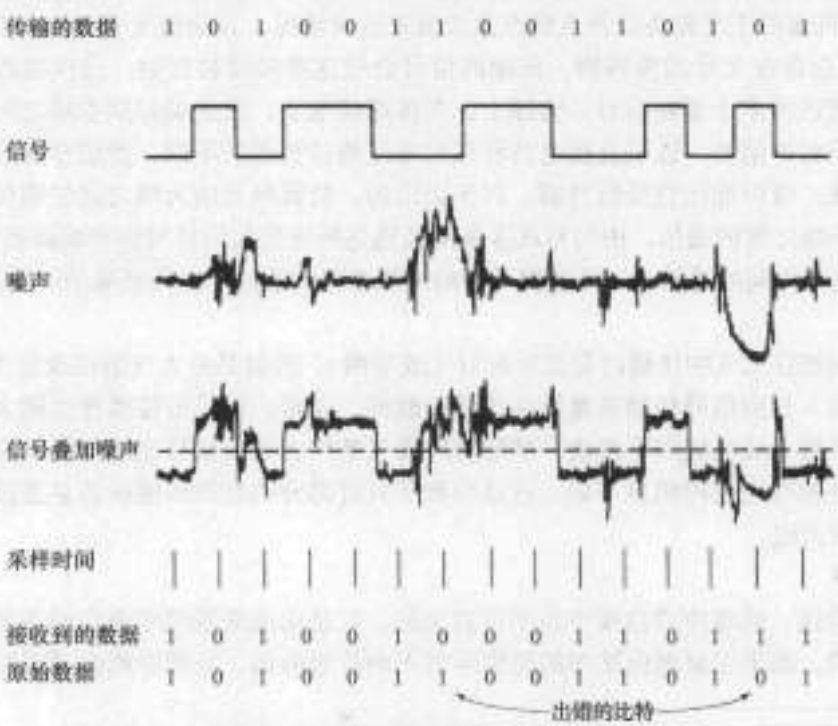


图4-10 噪声对数字信号的影响

⊖ 当发送端、接收端或者中间的传输系统具有一些非线性特性时，就会产生互调噪声。通常，这些设备是以线性系统方式工作的，即输入乘以一个常量就等于输出。在非线性系统中，输出是输入的一个较为复杂的函数。这种非线性通常是由设备故障或使用了过大的信号能量所导致的。在这些情况下，就会产生和与差的条件。

这里的噪声由相对适中程度的热噪声加上偶尔的脉冲噪声尖刺组成。从接收到的电波中，通过每比特时间一次的采样获得信号，进而恢复出数字数据。就像所看到的，偶尔的噪声就能将比特 1 变成比特 0 或将比特 0 变成比特 1，这样就导致了数字电波恢复过程中的错误。

4.2.2　无导向的传输介质

1. 自由空间丢失

对任意类型的无线通信，信号会随着距离散播。因此，距离发射天线越远的固定区域内的接收天线，其接收到的信号能量越弱。对卫星通信而言，这是信号丢失的基本模型[⊖]。

2. 大气吸收

导致发射天线和接收天线之间信号丢失的另一个原因是大气吸收。信号的衰减主要是由大气中的水蒸汽和氧气造成的。由水蒸汽导致的信号衰减，其峰值出现在 22GHz 频率附近，当频率低于 15GHz 时，信号衰减就比较小。对于氧气造成的信息衰减，在 60GHz 频率附近出现衰减峰值，低于 30GHz 频率时衰减就很小。雨和雾（即悬浮的水滴）能造成无线电波的散射，从而导致信号衰减，这是导致信号丢失的一个重要因素。因此，在降雨量比较多的地区，应该让信号的发送端和接收端之间保持较短的距离，或者采用低频率的频带。

3. 多径衰减

对于无线设备，其天线放置位置的选择相对比较自由。在某些场合下，天线之间可放置在附近没有干扰障碍物的场所，这样发送端和接收端之间就是一条直线传播路径（line-of-sight path）。许多的卫星设备以及点到点微波就是这种情况。其他情况下，如移动电话（蜂窝电话系统），会存在大量的障碍物。传输的信号会被这些障碍物反射，这样接收端就会接收到具有不同延迟的多个复制信号。实际上，在极端情况下，发送端和接收端之间没有直接的信号，只有反射的信号。依据直接电波和反射电波路径长度的不同，所组合成的信号有可能比直接信号强，也可能比直接信号弱。对于固定的、放置得当的天线之间的通信，以及卫星和固定地面基站之间的通信，由信号从多条路径到达所导致的信号增强和减弱是可以控制的。但对于移动电话之间的通信，以及放置不当的天线之间的通信，多径衰减是主要需要考虑的。

4. 折射

当无线电波在大气中传播时会发生折射（或弯曲）。折射是由大气条件改变（如高度或其他的空间改变）导致信号传播速度发生改变引起的。通常，信号的传播速度随大气高度的增加而加快，导致无线电波向下弯曲。然而有时天气条件会导致信号速度与大气高度之间的变化规律与典型的变化规律明显不同。这就导致了只有部分的直线传播电波甚至没有直线传播电波到达接收天线。

5. 热噪声

如前面所述，热噪声或白噪声是不可避免的。它是由通信系统中通信设备和传输介质的热活性导致的。如果卫星地面站中的热噪声得不到控制的话，该噪声就会覆盖掉从卫星接收

⊖ 在理想情况下，天线接收到的能量 P_r 与发射的能量 P_t 之间的比率关系是由下式给出的：

$$\frac{P_r}{P_t}=\frac{A_r A_t f^2}{(cd)^2}$$

其中 A_r 是接收天线的区域，A_t 是发射天线的区域，d 是两个天线之间的距离，f 是载波频率，$\lambda=c/f$ 是波长，c≈300 000km/s 是电磁波的速率。因此，对于相同的天线尺寸和间距，载波频率 f 越高，则自由空间路径损耗越低。

到的信号。

4.2.3 信道容量

我们已经看到，有多种的损伤能够使信号出现失真或损坏。对数字数据来说，出现的问题是这些损伤能多大程度地限制数据传输速率。在给定的条件下，数据在给定的通信线路或信道上传输的最大速率称为**信道容量**（channel capacity）。

决定信道容量的四个重要相关概念如下：

- **数据率**：是指数据能够进行通信的速率，用比特每秒（bps）表示。
- **带宽**：是指传输信号的带宽，它受限于发送端以及传输介质的性质，通常用每秒周期数（或赫兹）来表示。
- **噪声**：即通信线路上的平均噪声电平。
- **出错率**：即差错发生率，该里的差错为发送的是0而接收的是1，或者发送的是1而接收的是0。

我们需要注意的问题是：通信系统是昂贵的，通常来说，计算机网络所需的带宽越大，则费用就越高。并且，企业网络要提供的几乎所有传输信道其带宽都是有限制的。减少噪声、阻止干扰以及其他的一些差错限制措施都会造成数据传输的代价。相应地，企业网络需要尽可能地有效利用有限带宽信道。对于数字数据而言，这就意味着对于给定带宽，我们需在可接受的差错率范围下获得尽可能高的数据率。而噪声是限制我们达到所希望的高效率的主要因素。

我们已在图4-4中表明了带宽和数据率之间的关系。如果其他条件相同，带宽加倍则数据率加倍。现在我们来考虑数据率、噪声和差错率之间的关系。这可再次通过图4-10直观地加以说明。噪声的存在能损坏1个比特或多个比特的数据。如果数据率提高了，则每比特就变“短”了，那么给定模式的噪声影响到的比特数就越多，不论其持续时间多长。因此，在一个给定噪声电平下，数据率越高，则差错率越高。

所有这些概念可通过数学家香农的公式简洁地联系在一起。如我们前面所述，数据率越高，则噪声造成的损害越大。对于给定的噪声电平，我们能期望的是信号强度越强，在噪声下正确接收到数据的可能性越大。这个推理中的关键参数是信噪比（Signal-to-Noise Ratio，SNR或者S/N），即在某传输点上信号能量与噪声能量的比值。典型地，这个比值在发送端测定，因为通常是在发送端采取措施来处理信号和降低噪声。在数字数据传输中，信噪比非常重要，因为它限定了所能获得数据率的上限值。香农的结论是：最大信道容量（bps）满足等式

$$C=B\log_2(1+\mathrm{SNR})$$

其中C是信道容量（bps），B是信道带宽（Hz）。香农等式给出了信道容量的理论最大值。然而，实际上能够达到的数据率要低得多。原因之一是香农等式中假定了噪声为白噪声（热噪声），而忽略了脉冲噪声，也没有考虑衰减失真和延迟失真。

关于香农公式，我们可得出一些注意点。数字传输的效率可用C/B的比值测量，即所获得的每赫兹比特数。对于给定的噪声电平，通过提高信号强度或带宽，就能提高数据率。然而，随着信号强度的增加，系统中的非线性特性也在增加，从而导致了互调噪声的增加。需要注意的是，由于噪声是假定为白噪声的，带宽越宽，则系统中引入的噪声越多。因此，当B增加，SNR就会降低。

应用注解

模拟信号

我们身边充满了来自各种信号源的信号。理解这些信号有助于我们解决通信设备中的基本问题。例如，移动电话用户经常站在窗口以提高他们的接收效果。当我们负责通信系统时，了解我们周围的信号能使得我们明白可靠连接和不可靠连接之间的区别。

了解数字信号和模拟信号之间的区别会很有趣。基于正弦波调制的模拟通信已存在很长时间。随着20世纪70年代和80年代的数字革命，人们认识到模拟系统的不足。现在随着蜂窝技术和其他通信系统的发展，我们都需要数字通信了。有意思的是，实际上所有的通信仍然是模拟的。术语数字蜂窝通信（digital cellular communication）和数字用户线（digital subscriber lines）的真正含义是我们转换数字信息，以便在模拟网络上传输。

许多系统中的通信，尤其是通过空气传播的通信需要模拟载体。即使在光纤上的高速通信，使用的也是基于模拟的信号。数字蜂窝电话仍旧在使用模拟载体，将数字编码的信息从一地传递到另一地。即使数字局域网信号也能分解成各个模拟成分。

基于这个原因，理解模拟信号、环境影响和基础设施类型对企业网络组织特别有好处。对这些问题的评估能使我们在设计阶段做出更好的选择，并且在系统安装后出现问题时，方便进行问题的追踪。

对于有导向的传输介质，错误容易定位并且消除。如我们在第4章中所讨论的，在使用有导向传输介质的系统中，应对通信问题最好的方法是固定安装。这不仅对基于铜缆的系统（如利用非屏蔽双绞线UTP的以太网）是正确的，对于基于光缆的系统也是正确的。对于无线系统，即使是质量最好的系统，也可能因为不可控制的外力使得系统无法工作。这些外力不必需要是像飓风这样大的重要事件，即使环境中很小的变化都可能导致问题。蜂窝电话运营商是深刻知道这点的，因为他们体验过一棵树因其是否潮湿也能造成通话质量的不同。当地的建筑（如新大楼或喷泉）能产生反射，甚至阻止了发送端和接收端之间的视线。

除了像摩天大楼等看得见的问题外，剩下的就是一些看不见的障碍物，如其他的电磁辐射源。蜂窝塔、无线电基站、警用和消防通道、天狼星XM无线电（Sirius XM radio）以及许多其他的设施都能单个地或一起对局域无线系统造成问题。在无线光通信情况下，无线电干扰不会带来问题，而视线和天气条件确定会导致问题。就天气而言，会引起最坏情况的是薄雾或雾，而其他的问题如无线电收发器平台的热胀冷缩、风、灰尘甚至大货车能导致信号偏移问题或降低性能。

天狼星XM无线电引起的是一种比较有趣的无线电干扰情况。天狼星XM无线电是一种基于卫星的服务，利用卫星频率提供音乐和新闻频道。它所使用的频率恰好与WiFi或无线局域网使用的频率相近。无线“热点”（hot spots）现在安装得越来越多，这些热点就与天狼星XM无线电接收器产生了干扰。天狼星XM无线电运营商是付费使用这段频谱的，因此给人的感觉是他们的信号被来自无许可的信号源干扰了。不幸的是，随着无线网络设备的快速增长，这个问题越来越难得到解决。

有线和无线模拟系统中的问题数量多并且多样。即使人们需要的是数字信息，实际上我们仍旧很依赖模拟传输。理解模拟信号是怎样传输的、它们的相互作用以及本地条件的影响能极大地提高我们通信成功的机会。有意思的是，我们要学习的有关模拟有线和无线通信、业余无线电操作的知识，其实我们已知晓很多年了。

4.3 总结

本书讨论的所有信息形式（如音频、数据、图像和视频）都可用电磁信号表示，并能在合适的传输介质上传递。依据传输介质和通信环境，可采用模拟信号或数字信号来传递信息。任何电磁信号都由一系列的频率成分组成，无论其是模拟信号还是数字信号。描述信号的一个关键参数是带宽，即组成信号的频率范围的宽度。通常来讲，信号随着带宽的增大，其承载信息的容量也越大。

通信设备设计中的一个主要问题是传输损伤。最主要的传输损伤是衰减、衰减失真、延迟失真和各种类型的噪声。各种形式的噪声包括热噪声、互调噪声、串扰和脉冲噪声。对模拟信号而言，传输损伤在信号中引入了随机的更改，从而降低了所接收信息的质量，并且可能影响其可理解性。对数字信号而言，传输损伤可能造成比特错误。

通信设备的设计者需要处理四个因素：信号带宽、用于传输数字信息的数据率、噪声和其他损伤的总量、可接受的错误率。带宽通常受限于传输介质以及避免与相邻信号干扰的措施。由于带宽是稀缺资源，在给定的带宽下，我们需要使数据率最大化。数据率通常受限于带宽、存在的损伤以及可接受的错误率。我们一般用数据率（单位为 bps）与带宽（单位为 Hz）的比值来衡量一个传输系统的效率。效率在 1 ~ 5bps/Hz 之间通常认为是好的。

4.4 关键术语、复习题和练习题

关键术语

amplitude（振幅）
analog signal（模拟信号）
attenuation（衰减）
bandwidth（带宽）
channel capacity（信道容量）
delay distortion（延迟失真）
digital signal（数字信号）
frequency（频率）
fundamental frequency（基频）
Hertz（赫兹）
noise（噪声）
peak amplitude（峰值振幅）
period（周期）
periodic signal（周期信号）
phase（相位）
radian（弧度）
sine wave（正弦波）
spectrum（频谱）
square wave（方波）
wavelength（波长）
white noise（白噪声）

复习题

4.1 模拟电磁信号和数字电磁信号之间的区别是什么？
4.2 什么是周期信号？
4.3 指出并简单描述所有电磁信号的三种组成成分。
4.4 什么是信号的周期？它是怎样测量的？
4.5 什么是信号的波长？它是怎样测量的？
4.6 正弦波中的波长和频率之间的关系是什么？
4.7 什么是信号的频谱？

4.8 信号的带宽是什么?
4.9 信号的频谱与其带宽之间的关系是什么?
4.10 为什么电话网络中音频信道的带宽比人声音中的频谱窄得多?
4.11 什么是衰减?
4.12 为什么延迟失真限制了数字数据的数据率?
4.13 什么是噪声?
4.14 什么是白噪声以及它是如何影响信号的?
4.15 什么是脉冲噪声以及它是如何损害数据通信的?
4.16 什么是互调噪声?
4.17 什么是串扰以及它是如何影响信号的?
4.18 简单描述无线信号中的主要损害类型。
4.19 定义信道容量。
4.20 影响信道容量的关键因素有哪些?

练习题

4.1 一个信号的基频是 1000Hz，该信号的周期是什么?
4.2 由从 50Hz 到 5000Hz 频率组成的信号，其带宽是多少?
4.3 寻找并观看一些介绍正弦波基本特征（振幅、频率、波长、周期）的 YouTube 视频。提供你认为这些概念介绍得最好的三个 URL。如果你只能向其他人推荐一个视频，你会选择哪一个? 为什么?
4.4 解释为什么数据传输的代价会随着带宽的增加而加大?
4.5 数字信号中哪种噪声最难消除? 为什么?
4.6 模拟信号中哪种噪声最难消除? 为什么?
4.7 哪些类型的信号更易受互调失真的影响?
4.8 在因特网上做一些香农理论的研究。给出一些你认为在解释等式中各部分之间关系方面做得比较好的参考文献。总结香农理论在网络设计方面的指导作用。
4.9 解释为什么计算机网络中减少噪声的代价比较大?

数据通信基础

学习目标

- 通过本章的学习，读者应该能够：
- 解释模拟传输与数字传输的不同。
- 描述怎样用调制解调器来编码数字数据以便在模拟电话线上传输。
- 描述怎样用编解码器来编码模拟数据以便在数字设备上传递。
- 解释异步传输和同步传输之间的区别以及各自使用的场景。
- 描述差错检测的过程。

企业网络中，在传输介质上传递数据涉及的不只是将信号插入到传输介质中，传输介质两端的设备也需要适当的合作。这章和下章讨论的都是一些基本机制，用于在传输介质两端设备之间成功地传输数据。首先，我们讨论模拟传输和数字传输之间的区别。然后，我们讨论信号的编码方案以便进行有效和高效的通信。其次，我们看一下同步问题：为了对所接收到的信号正确解码，接收端必需知道到达的起始位和结束位，以便能与发送端保持步调一致。我们介绍了一些保持发送端和接收端同步的通用技术。在本章的最后，我们介绍差错检测的概念。

5.1 模拟数据通信和数字数据通信

电磁信号能在多种的传输介质上传播，因此能用来传输数据。为了传递数据，需将这些信号进行编码，而编码方法直接决定了传输的有效性和可靠性。这节主要介绍一些基本概念，这些概念对理解数据如何在传输介质上从发送端传递到接收端非常重要。

术语模拟（analog）和数字（digital）大致分别与连续（continuous）和离散（discrete）相对应。当数据通信涉及数据、发信号和传输三方面内容时，会经常用到这两个术语。

信号和数据是计算机网络中的基本成分，理解它们之间的不同非常重要。信号用来表示在计算机网络中传递的数据。为了接收端能正确解析，发送端在传递数据时需要将其转换成合适的信号。

这些术语在不同场景中的使用导致了许多文章和书的混乱。在这节中，我们要明确这两个术语的不同用法。简而言之，我们将**数据**（data）定义为传达某种意思或信息的实体。**信号**（signal）则是数据的电气或电磁表示。**发信号**（signaling）是信号沿着通信介质的物理传播。**传输**（transmission）则是数据通过传播和信号处理过程在计算机网络中的通信过程。

在企业网络中，获取、传递和存储的数据有多种不同的类型。正如我们在前面几章所看到的，与文本和数字混合在一起的音频、视频和图像是业务数据的重要类型。我们还注意到，一些形式的数据是模拟的，而其他的是数字的。

模拟数据（analog data）在一段时间内具有连续的值。例如，声音和视频是连续变化的

强度模式。传感器收集到的大部分数据（如温度和气压）都具有连续的值。**数字数据**（digital data）具有离散的值，例如文本、十进制整数和二进制数据。通过无线介质或有线介质，将任何类型的数据从一点传递到另一点，这些数据必需转换成信号。因此，用信号来编码和传递数据。依据网络中待传递数据的类型（模拟的或数字的）以及传输设备的类型（模拟的或数字的），采用不同类型的设备将数据转换成信号，反之亦然。

由第 4 章可知，在企业网络或其他的通信系统中，电磁信号是数据传输的基础。**模拟信号**（analog signal）是连续变化的电磁波，它在有导向介质和无导向介质上都可传递。模拟波形（正弦波）中的组成成分，即幅值、频率和相位，可用来传递数据。**数字信号**（digital signal）是电压脉冲序列，可在有线介质上传递，如一个正电压常量表示二进制 0，一个负电压常量表示二进制 1。数字信号传输的优点是比模拟信号传输便宜，并且不容易受噪声的干扰。数字信号传输的不足是比模拟信号的衰减严重。注意，数字信号只能在铜线介质上传输，而不能用在光缆或无线介质上。

模拟数据和数字数据都可以表示成模拟信号或数字信号，如图 5-1 所示。目前的趋势只要能采用数字传输就选择数字传输。用于传输计算机数据的局域网（Local Area Network，LAN）通常支持数字信号。LAN 中用数字信号来传输业务中常见的各种大小的模拟数据和数字数据。然而存在一些通信设备，这些设备只能以模拟信号来传递数据，因此对模拟和数字数据传输的基本了解仍然是很重要的。

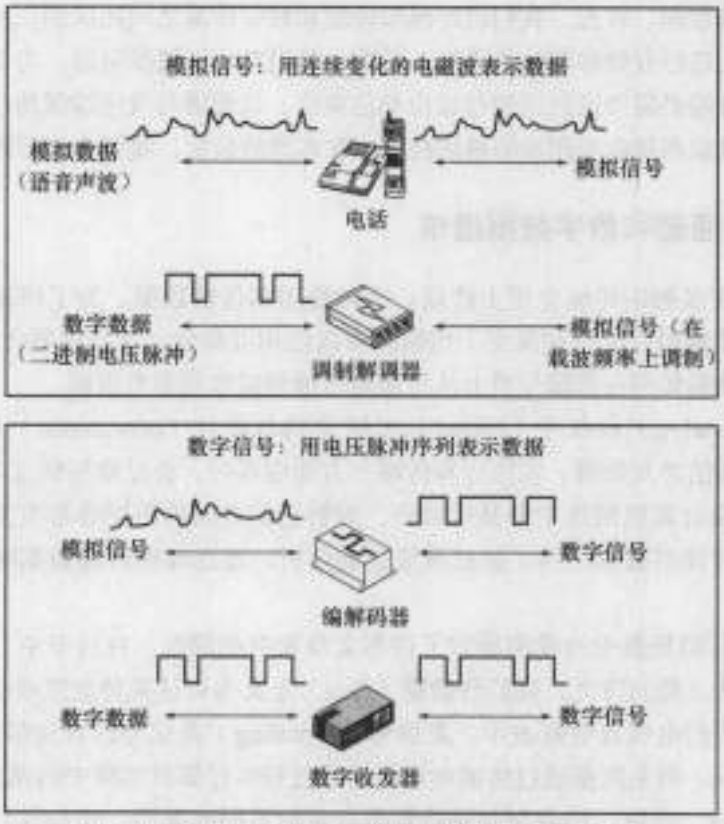


图 5-1　模拟数据和数字数据的模拟信号和数字信号

将模拟数据转换成模拟信号是很普通的。在传统电话、广播电视、有线模拟电视以及 AM 和 FM 无线电中，发送端采用的方法是：利用调制技术，将声音和 / 或视频波形转化成能

在电线或电视上传输的电磁波形。在某些情况下，所传输的电磁波形与原始模拟波形所对应的波形近似相同，传输频率范围（即频谱）也可能相同，并且这些所传输的电磁波形与原始模拟波形在许多方面是电磁等价的。当模拟电话听筒的传感器将语音声音转换成电磁正弦波，以便在电话网络上传递时，这样的情况就发生了。在其他情况下，模拟数据被转换成模拟信号，该模拟信号的频率范围是与原始数据的频率不同的。这样的一个实例是 FM 无线电广播在有线模拟电视信道上传输。

将数字数据转换成模拟信号需要用到**调制解调器**（modem）。调制解调器通过调制载波频率（carrier frequency），将输入的二进制电平脉冲（代表二进制 0 和二进制 1）序列转换成模拟信号。调制成的信号占用的频谱范围以载波频率为中心。最普遍的调制解调器（即拨号调制解调器）表示了语音频谱范围内的数字数据，因此数字数据能够在普通的语音级电话线上传播。在电话线的另一端，调制解调器解调所接收到的信号，从中恢复出原始的数据。本节后面将讨论调制解调器所用的主要调制技术。

经过与调制解调器相似的操作，模拟数据能表示成数字信号。完成这个功能的设备是**编解码器**（codec）。从本质上来讲，编码器得到直接表示语音、音频或视频数据的模拟信号，并用比特流来近似该信号。在传输线路的另一端，编解码器利用这个比特流重构出模拟数据。编解码器中进行这种转换的基本流程将在 5.2 节介绍。

最后，数字数据可以直接通过两个电压电平以二进制形式表示，一个电压电平表示二进制 1，另一个电压电平表示二进制 0。然而，为了提高发送端和接收端之间的传播特性以及同步，二进制数据可能编码成这样的数字信号，其中利用电压电平转换而不是电压电平常量来表示二进制数据。5.2 节将具体介绍数字数据的编码类型。

刚介绍的 4 种组合应用得都比较广泛。业务提供商在为任一通信任务选择一个特定组合时，其选择理由是多种多样的。其中具有代表性的理由包括：

- **数字数据，数字信号**：通常而言，与将数字数据编码成模拟信号的设备相比，将数字数据编码成数字信号的设备不那么复杂且不昂贵。
- **模拟数据，数字信号**：将模拟数据转换成数字形式时，允许使用现代数字传输和交换设备。
- **数字数据，模拟信号**：一些传输介质，如光纤和卫星，只能传输模拟信号。
- **模拟数据，模拟信号**：模拟数据很容易转换成模拟信号。

我们还需要最终区分一下。模拟信号和数字信号都可在合适的传输介质上传递。处理这些信号的方法是传输系统的功能。表 5-1 概括了数据传输的方法。**模拟传输**是一种不考虑信号内容的信号传输方法，这些信号可能表示模拟数据（如语音）或者数字数据（如经过了调制解调器的数据）。不论在哪种情况下，模拟信号都要遭受衰减，而这限制了传输线路的长度。为了进行远距离的传输，模拟传输系统中采用了放大器来增强信号的能量。遗憾的是，放大器同时也增强了信号中的噪声成分。在通过放大器的级联以获得更远的传输距离时，信号的失真会变得越来越严重。对模拟数据而言，如语音，即使失真比较多还是可以忍受的，其数据（说的单词）仍是可理解的。但是对于以模拟信号传输的数字数据，级联的放大器会导致传输错误的增加。

表 5-1　模拟传输和数字传输

a）数据和信号

	模拟信号	数字信号
模拟数据	两种选择： 1）信号占用与模拟数据相同的频谱 2）模拟数据经过编码占用不同的频谱段	模拟数据经过编解码器编码产生数字比特流
数字数据	数字数据经过调制解调器编码产生模拟信号	两种选择： 1）信号由两种电压电平组成，以表示两个二进制值 2）数字数据经编码生成具有所要求属性的数字信号

b）信号的处理

	模拟传输	数字传输
模拟信号	经放大器传播，不论信号表示的是模拟数据还是数字数据，处理方式相同	假设模拟信号表示的是数字数据。信号经过中继器传播。在每个中继器上，从输入的信号恢复出数字数据，并用它生成新的模拟输出信号
数字信号	不用	数字信号表示的是 1、0 的比特流，该比特流表示的是数字数据，或者是经过编码的模拟数据。信号经过中继器传播。在每个中继器上，从输入的信号恢复出 1、0 比特流，并用它生成新的数字输出信号

与之相反，**数字传输**则需要考虑信号的内容。通常，在衰减威胁到信号所表示数据的完整性之前，数字信号只能传递有限的距离。为了获得较远的传输距离，我们要使用中继器。中继器接收数字信号，从中恢复出 1 和 0 的模式，再重新传输一个新的信号，这样就克服了衰减。

如果一模拟信号承载的是数字数据，同样的技术也可用在该模拟信号。在传输系统中适当的地方加入一些转发设备（而不是放大器），这些转发设备从模拟信号中恢复出数字数据，并且生成新的干净的模拟数据，因此噪声就不会累积。图 4-9 中给出了这个过程。

这样问题就来了，对于业务数据来说，哪一个才是更好的传输方法呢。电信通信界和它的业务客户提供的答案是数字传输，尽管上世纪在模拟通信设施上做了巨额的投资。如今，超长距离传输网络和建筑物间网络都在向数字传输转换，并且在可能的地方采用数据信号传输技术。导致这些的最主要原因在表 5-2 中进行了概括。

表 5-2　数字传输的优点

代价

数字电路的发展使得数字电路的价格持续降低，尺寸持续变小，而模拟设备则没有相应的下降，并且数字电路的维护代价也比模拟电路的维护代价小得多

更少出错；传输数据的高完整性

由于传输的是二进制数据，更容易检测和纠正错误。利用中继器而不是模拟放大器，噪声和其他信号衰减的影响不会累积。因此，数据能进行更长距离的传输，并且错误更少，这样就保持了所传输数据的完整性

传输效率高和信道容量利用率高

利用数字电路能传递更多的数据。构建高带宽的传输线路变得很经济，如光纤和卫星信道。为了更好地利用信道容量，通常需要采用信道复用技术，而这用数字技术（如时分）比用模拟技术（如频分）更容易实现，并且更便宜（见第 6 章）

安全性和私密性

加密技术能轻而易举地应用于数字数据中，以及用于经过数字化的模拟数据中

语音、数据和视频的简单集成

如果用数字化的方法来处理模拟信息和数字信息，所有信号就具有相同的形式，并且能进行相似的处理。这样它们在同一条电路上就能容易地组合在一起。这样语音、视频、图像和数据流量的规模经济、方便性和收敛性就能实现

现在我们来仔细看一下信号编码的每种主要形式。我们将考虑数字数据的模拟编码、模拟数据的数字编码、数字数据的数字编码和模拟数据的模拟编码。

5.2　数据编码技术

如我们指出的，不论是模拟的还是数字的数据，必须转换成信号后才能传输。

对于数字数据，不同的信号元素分别代表二进制的 1 和 0。从二进制数字到信号元素的映射就是传输的**编码方案**。编码方案的设计目标是使得判定位开始和结束的错误最小化，并且使确定某位是 1 还是 0 时的错误最小化。

对于模拟数据，编码方案的设计目标是增加传输的质量或保真度，即我们希望接收到的模拟数据是发送数据的精确和准确再现。

5.2.1　数字信息的模拟编码

模拟编码的基础是一个连续的、频率恒定的信号，该信号称为**载波信号**。数字信息的编码采用的是**调制解调器**，对载波的三个特征（振幅、频率或相位）之一或这三个特征的组合进行调制。图 5-2 展示了将数字数据调制成模拟信号的三种基本形式：

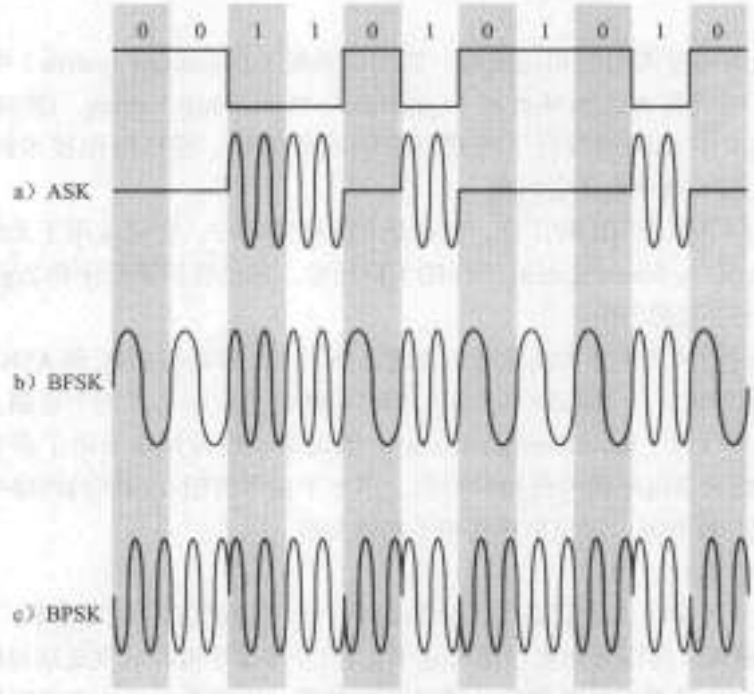


图 5-2　数字数据的模拟信号调制

- 幅移键控（Amplitude-Shift Keying，ASK）。
- 频移键控（Frequency-Shift Keying，FSK）。
- 相移键控（Phase-Shift Keying，PSK）。

在上面的所有情况中，调制成的信号所包含的频率范围以载波频率为中心。该频率范围就是传输信号的带宽。

在**幅移键控**（ASK）中，数字数据用载波的不同振幅的变化来表示。最简单的形式是用

载波存在来表示一个二进制数（典型的是 1），不存在载波来表示另一个二进制数（典型的是 0），如图 5-2a 所示。在其他情况下，一个幅移表示二进制 1，两个幅移表示二进制 0。ASK 易受突然的增益改变的影响，如噪声、失真以及其他的信号衰减，这就使得该调制技术不是很有效。然而，ASK 的调制和解调技术比较便宜，这就增加了将其用于业务网络的吸引力。

ASK 技术也通常用于在光纤上传输数字数据。当发送器为发光二极管（LED）时，用一个短光脉冲来表示二进制 1，没有光表示二进制 0。激光发送器通常有一个固定的“偏流（bias）”，它可使设备发射出弱光，该弱光表示二进制 0，而振幅高的光波表示二进制 1。

在**频移键控**（FSK）中，数字信息通过载波的离散频率改变来传递。最简单的 FSK 形式称为二项频移键控（Binary FSK，BFSK），用载波频率附近的两个不同频率来表示两个二进制值，如图 5-2b 所示。FSK 受噪声和其他错误源影响的程度比 ASK 小，因此在 FSK 中更容易解码，并且信噪比也比 ASK 中的高。FSK 是多数调制解调器中的可选支持项，通常用于高频率（4 – 30MHz）的无线电传输。

在**相移键控**（PSK）中，通过载波信号相位的偏移对数据进行编码。图 5-2c 给出的是一个两相位系统的例子。在该系统中，通过发送与前一个信号突发（signal burst）相同相位的信号突发来表示二进制 0，而发送与前一信号突发相反相位的信号突发来表示二进制 1。图 5-2c 给出了二项相移键控（Binary Phase-Shift Keying，BPSK），其中两个相位偏移间的间隔是 180°。

相移键控能用超过两个的相位偏移。四相位系统（four-phase system）中每个信号突发编码两位，该系统就是正交相移键控（Quadrature Phase-Shift Keying，QPSK）的特例。与 BFSK 相比，QFSK 在相同的带宽下能获得双倍的数据率。相移键控技术的抗噪声能力比 ASK 和 FSK 强，传输效率也比它们高。

PSK 在业务网络中应用比较广泛，特别是在无线网络中。它通常用于无线局域网和射频识别（Radio Frequency Identification，RFID）应用中。它也应用于蓝牙和 ZigBee 系统中，就如调制解调器用于卫星通信中。

最后，前面讨论的几种基本技术可组合起来使用。通常是将 PSK 和 ASK 组合起来使用，在该组合的编码技术中，一些或所有的相位偏移可能发生在一个或两个振幅上。这些技术通常称为多电平信号传输（multilevel signaling），因为每个信号元素表示了多个二进制位。注意四相位相移键控是多电平信号传输的特例。多电平信号传输在目前的网络中应用很广，如 56Kbps 的拨号调制解调器、数字用户线和千兆以太网。

1. 数据率和信号率

在多电平信号传输中，我们必须区分数据率（即二进制位传输的速率，单位为 bps）与调制率或信号传输率（即信号元素传输的速率）。信号传输率可看成发送端每秒钟发送不同信号脉冲的次数，它也可看成每秒钟所传递的不同振幅、频率或相位的改变次数。该传输率用波特率（baud）或者信号元素 / 秒来表示。

四相位 PSK 有助于说明信号的数据率 R（单位为 bps）和调制率 D（单位为波特）之间的区别。我们假定该编码用于每一比特用一常量电平脉冲表示的数字输入中，其中一种电平用于表示二进制 1，另一种电平用于二进制 0。我们还假定所使用的四相位 PSK 中，通过振幅与相位的组合，形成 16 种不同的组合形式，即 16 种不同的信号元素。利用这 16 种信号元素，每一传递的信号代表了 4 比特数据（L=4）。因此，如果调制器的波特率为 2400（即每秒传递 2400 个信号元素），那么它的数据率为 9600bps（$R=D\times L$）。这个例子表明了在语音级线

路上，通过采用越复杂的调制技术，就能获得越高的比特率[⊖]。

2. 调制解调器

虽然公共电信设备和私有电信设备都逐渐变为数字式的，模拟传输的使用范围仍然比较广。因此，调制解调器仍然是应用最为广泛的通信装置之一。调制解调器是对模拟载波进行调制以编码数字信息的基础设备，它也解调所接收的信号，从中解码出传递的信息。

调制解调器有多种不同形式，以用于不同的应用中。如独立的调制解调器（standalone modem），内置了内部供电装置，可用于单个的信息设备中。在有许多电路集中在一起的地方，如因特网服务提供商的计算机系统接口处，通常使用的是机架式调制解调器，共享系统的供电设备和包装。调制解调器也可封装在其他系统（如个人计算机）的内部。这种集成的调制解调器降低了系统的总体成本，但加大了计算设备的复杂度以及设计成本。集成调制解调器通常是可选的配置，因为如果将某一产品的调制解调器标准化为某一特定类型，就限制了该产品的使用范围。

调制解调器在今天的计算机网络中非常普遍。例如、直接卫星广播、Wi-Fi 和移动电话都使用调制解调器来通信。WiMax 系统以及其他一些家庭网络系统中也用到调制解调器。在这节中，我们将简要介绍 3 种应用广泛的调制解调器类型：语音级（voice-grade）调制解调器、电缆（cable）调制解调器和 ADSL 调制解调器。

语音级调制解调器设计用来在普通的电话线路上传递数字数据。因此，该调制解调器采用与语音信号同样的 4kHz 带宽。因为调制解调器是用于成对的通信，并且是在公共电话网上使用，为便于不同的语音级调制解调器能成对工作，必须形成相应的标准。表 5-3 列出了最常使用的语音级调制解调器的类型，这些类型由 ITU-T 定义并指定[⊜]。

表 5-3　调制解调器规范

ITU-T 建议	数据率（bps）	拨号	半双工	全双工
V.29	9600		X	X
V.32	9600	X		X
V.32bis	14 400	X		X
V.33	14 400			X
V.34	33 600	X	X	X
V.90	33 600（发送） 56 000（接收）	X	X	X
V.92	48 000（发送） 56 000（接收）	X	X	X

电缆调制解调器使得我们能通过有线电视网络访问因特网。有线电视业是提供家庭用户访问高速因特网的早期领导者。图 5-3 给出了有线电视传输的典型布局图。在有线电视中心

⊖ 通常，

$$D\frac{R}{L}=\frac{R}{\log_2 M}$$

其中，

D= 调制率，波特

R= 数据率，bps

M= 不同信号元素的个数 $=2^L$

L= 每个信号元素的比特数

⊜ 这本书对应网页上的支持文档中有关于 ITU-T 以及其他标准的具体描述。

局或通过高速线路连接的是因特网服务提供商（Internet Service Provider，ISP）。通常有线电视公司就是一个 ISP，它也可提供线路与其他 ISP 相连。从有线电视中心局开始，有线电视公司就在地面上或地下布置出由光纤和同轴电缆组成的线路网络，通过该网络到达其辖区范围内所有家庭和办公室。通常这个系统用来单向传输电视频道，每个频道为 6MHz。同样的有线布局，如果在两端都采用相应的电子器件，就可为用户传输数字信道，或者提供从用户到中心局的反向信道。利用第 6 章中描述的时分复用线路共享技术，许多用户可共享用于用户数据传输的上传信道或下传信道。在用户的家里或办公室，采用分用器（splitter）来将传统的电视信号输出至电视机，将数据信道输出至电缆调制解调器，该调制解调器可服务于单个 PC 机或由多个 PC 机组成的网络。电缆调制解调器能使数据和电视信号在同一个电缆上传输，因此电缆调制解调器是一种宽带调制解调器。

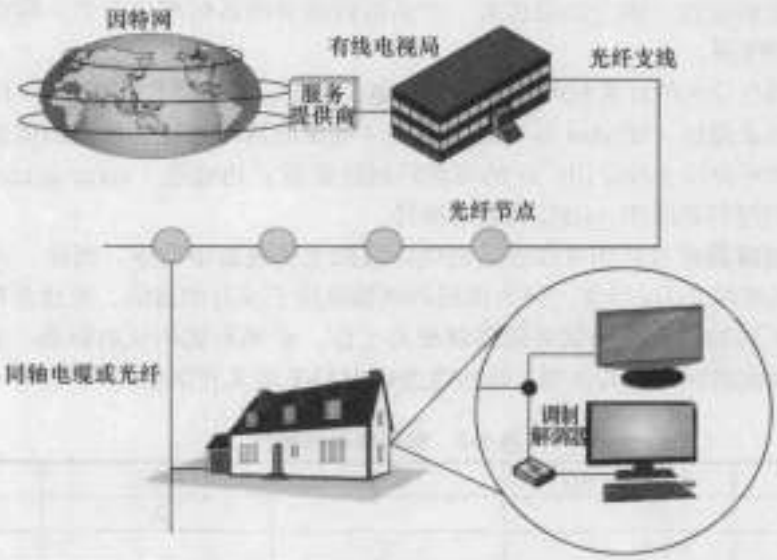


图 5-3　电缆调制解调器的应用

一些有线电视公司提供 VoIP 电话业务，如果有线电视客户选择了这个业务，就可不必连接公共电话网络了。通过将话音、电视盒因特网服务捆绑，通常能取得有竞争性的价格优势，这对一些客户和小的商家很有吸引力。

在高速广域公共数字网络的应用和开发中，最有挑战性的是用户和网络的连接部分。目前世界范围内有数以十万计的潜在终端，若每有一个新客户就要安装新的电缆则令人望而生畏。实际情况是，网络设计者一直在寻求方法来利用现已安装的双绞线，这些双绞线将所有的家庭客户和商业客户虚拟地连接到电话网络中。这些链路用来传递 0 ~ 4kHz 带宽的语音级信号。然而，这些电路也能传输更宽频谱的信号，如 1MHz 或更高。**非对称数字用户线**（Asymmetric Digital Subscriber Line，ADSL）是家庭采用最广的一种调制解调技术，用来在普通的电话线上提供高速的数字数据传输。美国的大部分传输公司都提供 ADSL 服务，并且全球大部分国家的 ISP 都支持 ADSL。

图 5-4 描绘了利用 ADSL 访问因特网时的配置情况。电话中心局能为多个 ISP 提供支持，每个 ISP 都要支持 ADSL 的调制解调技术。在中心局，ISP 的数据信号和来自普通电话语音交换机的语音信号混合在一起。然后，组合的信号通过用户线传递到或传回至本地用户。在用户端，双绞线分开并分别路由到 PC 机和电话机。在 PC 上，ADSL 调制解调器将数据信号解调后给 PC 机。在电话机上，微型滤波器过滤出 4kHz 的语音信号。数据信号和语音信号通

过频分复用技术（在第 6 章描述）组合在一起，然后在双绞线上传输。ADSL 调制解调器能将语音和数据同时在相同的线路上进行传递，因此它是一种宽带调制解调器。

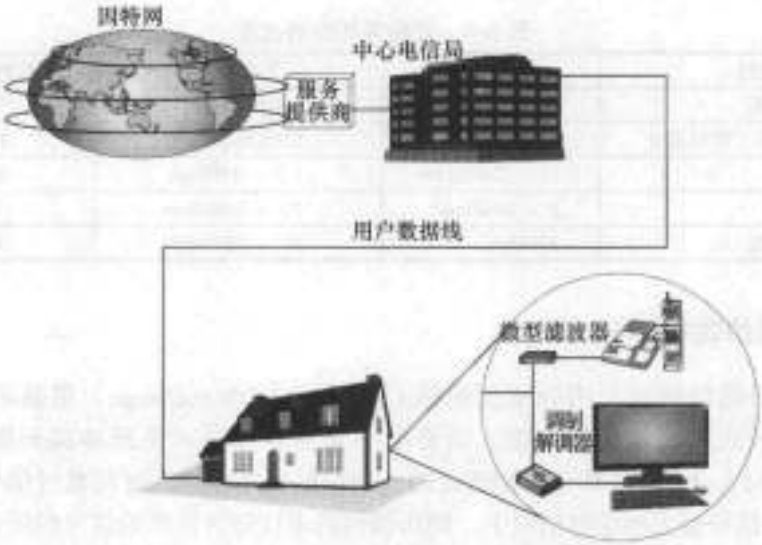


图 5-4　ADSL 调制解调器的应用

目前，在公司到家庭或商业建筑之间直接采用光纤能取得最好的传输效率，通常称为光纤到屋（Fiber To The Home，FTTH）或光纤到户（Fiber To The Premises，FTTP）。对于家庭用户和小型商业客户来说，FTTH/FTTP 是除电缆和 DSL 技术之外可行的选择。图 5-5 给出了家庭用户服务的典型配置。从中心局和住户小区之间布置了一条光缆，该光缆的带宽是由 32 个端用户共享，即在小区端点分用信号实现共享。中心局为电视和视频点播服务提供一个频带上的广播服务。其他的频带则单独地分配给用于双向因特网访问的用户以及传统公用电话网络上的双向语音服务。因此不像电缆通信，通过 FTTH，每个用户都有专用的信道用于数据和语音传输。在端用户处，调制解调器将光信号转变成电信号，以便设备访问，如计算机、电话和电视。

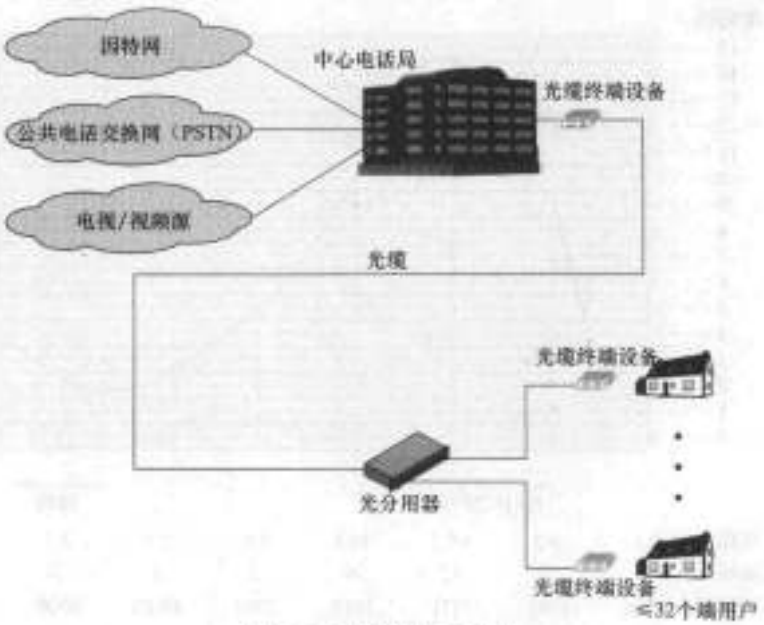


图 5-5　光纤到屋的配置

表 5-4 对比了我们所讨论的各种调制解调器的性能，以及通过综合业务数字网（采用数字信号传输技术）访问的性能。

表 5-4　因特网访问的速度

访问方法	上传速度	下载速度	下载时间（10M 文件）
拨号调制解调器	48Kbps	56Kbps	3min
ISDN 基准速率（双信道）	128Kbps	128Kbps	1.3min
ADSL	16 – 740Kbps	1.5 – 11Mbps	0.9 – 6.7s
FTTH	2 – 60Mbps	10 – 147Mbps	0.07 – 1s
电缆调制解调器	20Mbps	30 – 100Mbps	0.1 – 0.3s

5.2.2　模拟信息的数字编码

将公共电话通信网和专用分支交换机（private branch exchange）更新到数字传输和交换需要用数字形式来表示语音数据。语音数字化的最好技术是**脉冲编码调制**（pulse code modulation，PCM）。PCM 是基于采样理论的，即如果每隔一固定时间就对信号采样一次，并且采样频率高出信号最大频率两倍以上，则所得到的采样包含该原始信号的所有信息。

如果语音数据的频率被限制在 4000Hz 以下，就像模拟电话网络中一样，那么每秒钟 8000 次的采样就能完整地描述语音信号的特征。然而需要注意的是，所得到的是模拟采样，要将这些转换成数字的，需要为每个模拟采样都指定一个二进制代码。图 5-6 中给出了一个脉冲编码调制的例子，其中假设原始信号被限制在值为 B 的带宽内。模拟采样的频率是 $2B$，或每隔 $T_s=1/2B$ 秒就采样一次。每一个模拟采样近似量化为 16 个等级中的一个等级。这样，每个采样就可用 4 比特来表示，从 0000（表示等级 0）到 1111（表示等级 15）。由于量化的值是近似的，因此不能从其精确恢复出原始信号。如果利用 8 比特采样（有 256 个等级），恢复出的信号就能达到与模拟传输相近的效果。这就意味着，为将语音数据表示为数字信号，所需要的数据率为 64Kbps，即 8000 次每秒的采样 × 每个采样 8 比特 =64Kbps。

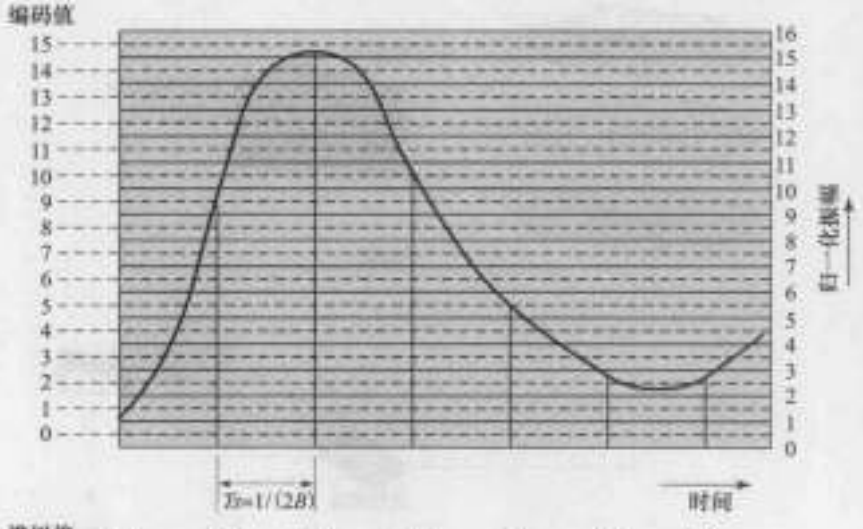


图 5-6　脉冲调制编码的例子

当然，除语音信号外，PCM 还可用于其他的应用中。例如，彩色电视信号的有效带宽为 4.6MHz。依据采样理论，为了与原始信号相似，它的模拟波形应该每秒采样 9200 万次。利用这样的采样频率，并且采样值用 10 比特（代表 1024 个量化值）表示，所得到的数据率为 92Mbps。

近年来，通常采用一些 PCM 技术以及其他编码技术的变种，以减少承载语音所需要的数字数据率。例如采用第 2 章所述的压缩技术，就可以 8Kbps 这样的低数据率获得质量较好的语音传输。在视频中，可利用帧与帧之间大部分的图片元素不发生变化这个优势。帧间编码技术（interframe coding technique）可将视频的数据率需求降低至 15Mbps 左右，对于较少改变的场景，如视频电话画面，甚至可低至 1.5Mbps 或更低。实际上，随着现代技术的进步，商用视频会议产品的数据率已低至 64Kbps 了。

5.2.3　数字数据的数字编码

传输数字信号最通常、最简单的方法是运用两个不同电压电平来表示两个二进制数字。典型地，用一个负电压表示二进制 1，用一个正电压表示二进制 0（如图 5-7a 所示）。这种编码方式称为**电平不归零制**（Nonreturn-to-Zero-Level，NRZ-L），即信号从不返回至零电压，并且在信号脉冲持续期内，用一个常量的电压电平来表示二进制数字。为表示一个二进制值，一个数字信号维持在某一特定电压电平的总时间称为比特周期（bit interval）或比特时间（bit time）。NRZ-L 通常用于超短距离通信，如个人电脑与外置调制解调器之间的通信或一个终端与邻近的主机之间的通信。

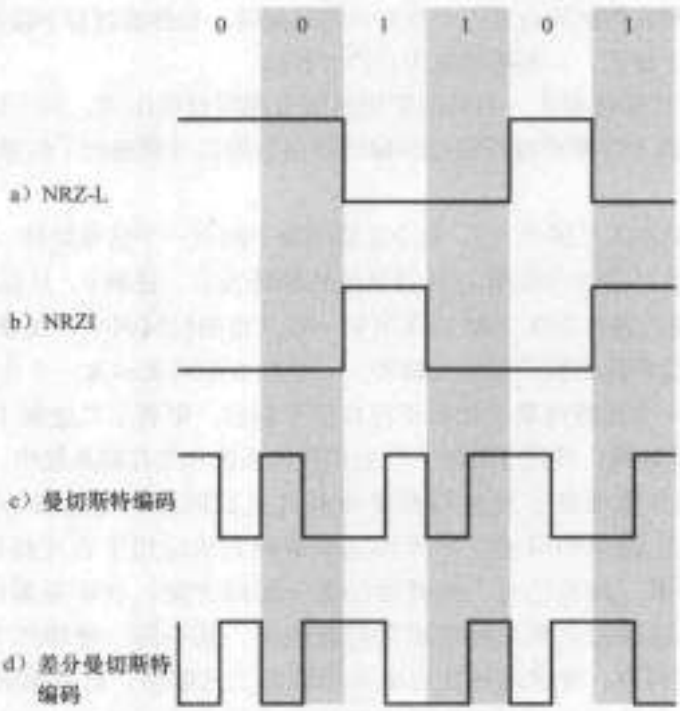


图 5-7　数字信号编码方案示例

NRZ 的一个变种是**翻转不归零制**（NRZ, Invert on Ones, NRZI）。与 NRZ-L 一样，NRZI

在一个比特周期中也维持一个常量的电压脉冲。用在一个比特周期开始处是否发生信号翻转来编码数据。在比特周期开始处，如果发生信号翻转（从低电压电到高电压电平，或从高电压电平到低电压电平）则表示该比特时间内传递的是二进制 1，如没发生信号翻转则表示传递的是二进制 0，见图 5-7b。NRZI 通常用于 100Mbps 的以太网中。

NRZI 是一种差分编码（differential encoding）。在差分编码中，信号的解码通过比较相邻信号元素的极性实现，而不是直接确定信号元素的绝对值。这种方案的一个优点是：在存在噪声情况下，检测信号的翻转比检测某值是否超出一阈值更为可靠。该方案的另一个优点是：在复杂的布线环境下，信号更容易失去其极性。例如，信号在从设备发往双绞线时发生了意外的翻转，这样 NRZ-L 中所有的 0 和 1 就发生了反转。这种情况在差分编码下不会发生。

利用 NRZ 传输的一个很大的不足是难以判定一个比特结束、另一个比特开始的位置。为了描绘这个问题，我们考虑一个运用 NRZ-L 编码的、全由 0 或全由 1 组成的长二进制串，则输出为一个长时间段内的常量电压。在这种情况下，发送端和接收端之间任意的时间漂移都能导致两者之间失去同步。

目前有许多可选的编码技术来解决这类问题，这些编码技术统称为二相（biphase）。其中用得最多的两类技术是曼切斯特编码和差分曼切斯特编码。所有的二相技术要求在每比特时间内至少有一次信号翻转，有可能是两次信号翻转。因此，这类编码的最大调制率是 NRZ 的两倍，这也意味着需要更大的带宽。由于这类编码中是用两个电压电平之间的翻转来表示一比特数据，要传输与 NRZ 相同的比特数，与 NRZ 相比就需要两倍的电压脉冲。然而，二相编码方案有如下的两个重要优点：

- **同步**：由于每比特时间内有一个预知的信号翻转，在传输过程中接收方就能进行同步。正是由于这个原因，二相码也称为自带时钟码。
- **差错检测**：传输过程中，如果所期望的信号翻转没有出现，则可以依此检测到出错。如果传输线路上的噪声将所期望的翻转处前后的信号都进行了转置，则该错误就没法检测出来。

在**曼切斯特**编码中（见图 5-7c），每个比特间隔中间有一个信号翻转。比特位中间的翻转可作为一种时钟方案，也表示数据：从高到低的翻转表示二进制 0，从低到高的翻转表示二进制 1。曼切斯特编码通常用在 10M 以太网和一些其他的局域网中。在**差分曼切斯特**编码中（见图 5-7d），比特位中间的翻转仅提供时钟。二进制 0 编码表示为一个比特周期开始处存在一个信号翻转，而一个比特周期开始处不存在信号翻转，则表示二进制 1。差分曼切斯特编码通常用于令牌环局域网，并用于其他一些电磁存储系统和光存储系统中。

曼切斯特编码方案保证了发送端和接收端之间的同步，但这种方案的效率比较低，因为它的波特率是比特率的两倍。如果将这种编码方案应用于吉比特以太局域网中，则需要二百万的波特率。目前已有一些其他的数字编码方案，在不需要两倍于数据率的波特率情况下，还能保持发送端和接收端之间的同步。其中的一种编码方案是 4B/5B 编码方案。在 4B/5B 编码中，发送端每次取出 4 比特的二进制串，将其编码为 5 比特的序列，以保证其间有多次的信号翻转（为了发送端和接收端之间的同步），见表 5-5。4B/5B 中用的是 NRZI 信号。在接收端，每接收到 5 比特的编码，就将其转变为所表示的原始 4 比特数据。

表 5-5　4B/5B 数字编码

4 比特数据串（原始的）	5 比特编码（变换后的）	未使用的 5 比特编码
0000	11110	00001
0001	01001	00010
0010	10100	00011
0011	10101	01000
0100	01010	10000
0101	01011	
0110	01110	
0111	01111	
1000	10010	
1001	10011	
1010	10110	
1011	10111	
1100	11010	
1101	11011	
1110	11100	
1111	11101	

在满容量运行的 100Mbps 以太局域网中，每传输 10 亿比特就传递了 8 亿比特的数据，其他的 2 亿比特是 4B/5B 编码中为了保证同步而添加的。因此 4B/5B 编码方案的编码效率为 80%。在速度更高的以太网中，其编码方案采用与 4B/5B 编码相似的操作方法。例如千兆以太网中采用的是 8B/10B 编码。该编码也用于火线（firewire，IEEE 1394）、光纤通道、InfiniBand 和 USB3.0 中。

5.2.4　模拟信息的模拟编码

在一些情况下，模拟信息能直接转换成占有相同带宽的模拟信号。这种情况的最好例子是语音。语音产生的 300 – 3400Hz 声波能用具有相同频率成分的电磁信号表示。该信号能直接在语音级电话线上传输。

在传输模拟信息时，也可用模拟信号调制载波来生成新的信号，该新信号传递相同的信息，但是占用的是不同的频带范围。这样做的基本原因有如下两个：

- 有时为了实现高效的传输需要高的频率。无导向传输介质上通常不能传递低频信号，所需的天线一般要覆盖直径几公里的范围。有导向传输介质也有频率范围的限制。例如光纤所需的频率近似于 10^{14}Hz。
- 模拟到模拟的调制允许使用频分复用，第 6 章给出了这类重要技术。

与数字到模拟的调制相比，模拟到模拟的调制涉及一个信号源，用来对载波信号的三个基本特征之一进行调制：振幅、频率或相位。

图 5-8 给出了 3 种调制例子。在振幅调制

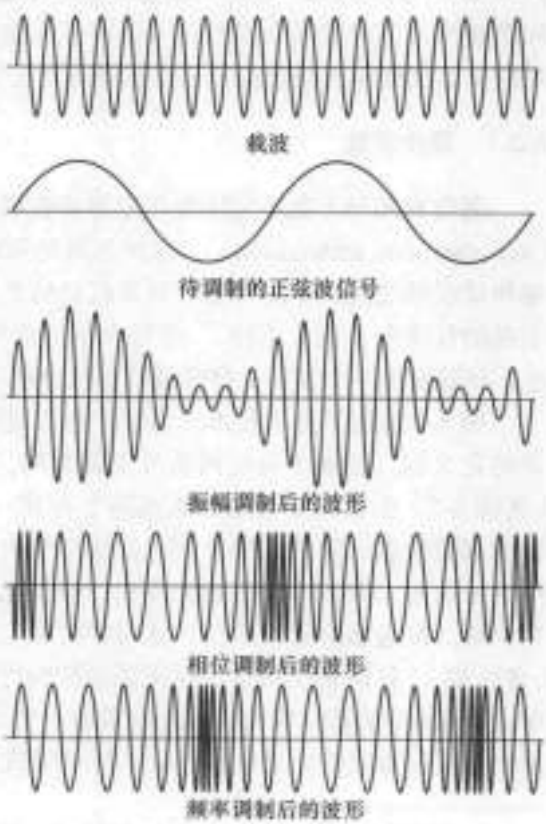


图 5-8　利用正弦波信号对正弦波载波的振幅、相位和频率进行调制

（Amplitude Modulation，AM）中，载波的振幅随着调制信号模式的改变而变化。相似地，频率调制（Frequency Modulation，FM）和相位调制（Phase Modulation，PM）分别对载波的频率和相位进行调制。

5.3　异步传输和同步传输

由图 4-10 可回想到，数字数据的接收需要对输入的信号每比特时间采样一次，以决定所传输的二进制值。这个过程中遇到的困难之一是传输中的各种损伤会破坏信号，从而导致偶尔的错误发生。这类问题还混合着时间问题：为了接收端能对输入的比特正确采样，必须知道所接收比特对应信号的开始时间和信号持续时间。

假定发送端简单地发送一数据比特串。发送端维护一时钟来指导比特的传输时间。例如，如果以 1Mbps 的速率发送数据，则每 $1/10^6$=1 微秒（μs）发送一个比特数据，该时间由发送端时钟测量得到。典型地，接收端会尝试着在每比特时间的中心时间点对介质采样。接收端每隔一比特时间就采样一次。在我们的例子中，每 1μs 采样一次。如果接收端依据自己的时钟确定采样时间，这样在发送端和接收端的时钟没有达到精确对齐时就会出现问题。如果两者的时间偏差是 1%（即接收端比发送端快或慢 1%），那么第一次采样的时间点就与比特时间中心点（比特时间中心点分别距离比特开始时间点和结束时间点各 0.5μs）有 0.01 比特时间（即 0.01μs）的距离。在经过 50 次或以上的采样后，接收端就有可能因为在错误的比特时间内（50×0.01=0.5μs）采样而出错。如果发送端和接收端的时钟偏差小一些，则错误的发生时间会晚些，但只要发送端发送了足够长的比特串，并且期间不采取措施来使得发送端和接收端同步，最终接收端会跟不上发送端的发送节奏。

5.3.1　异步传输

通常有两种方案来实现发送端和接收端的同步。一种方案，说来也奇怪，称为**异步传输**（asynchronous transmission）。这种方案的策略是不发送长的、连续的比特串，从而避免发送端和接收端之间的定时问题。取而代之的是，数据以每次发送一个字符的方式来传递，每个字符的长度是 5 到 8 比特[⊖]。在每个字符的发送期间内保持发送端和接收端之间的定时或同步，每新发送一个字符，接收端就有机会在字符开始处实现与发送端的再同步。

图 5-9 描述了这个技术。当无字符发送时，发送端和接收端之间的线路为空闲状态。空闲的定义与二进制 1 对应的信号元素相同。因此，对异步传输中常用到的 NRZ-L 信号发送（见图 5-7）而言，空闲意味着线路上存在一个负电压。字符以一起始位（其值为二进制 0）作为起始标志，随后紧跟着发送组成字符的 5 到 8 比特数据。字符所对应比特的发送以最重要的位结束。例如，对于 IRA 字符，数据比特发送后紧跟着奇偶校验位，因此是最重要的比特位置。发送端设置校验位，使得字符中 1 的数目（包括校验位）为偶数（偶校验）或奇数（奇校验），具体是使用偶校验还是奇校验可依据使用惯例决定。该位是发送端要来检测错误的，如 5.4 节所述。校验位后还有最后一个元素，称为停止元素，它是二进制 1。停止元素的最小长度是指定的，通常是普通比特时间的 1 倍、1.5 倍或 2 倍，而其最大长度不指定。由于

⊖ 组成字符的比特数目由使用的编码决定。我们已看到的一个常用例子是 IRA 编码，其中每个字符 7 比特（见第 2 章）。另一个常用例子是扩增二进式十进交换码（EBCDIC 码），其中每个字符为 8 比特，该编码通常用于 IBM 大型机系统和中型机系统中。

停止元素和空闲状态是一样的，发送端可在其准备好发送下一个字符前一直发送停止元素。

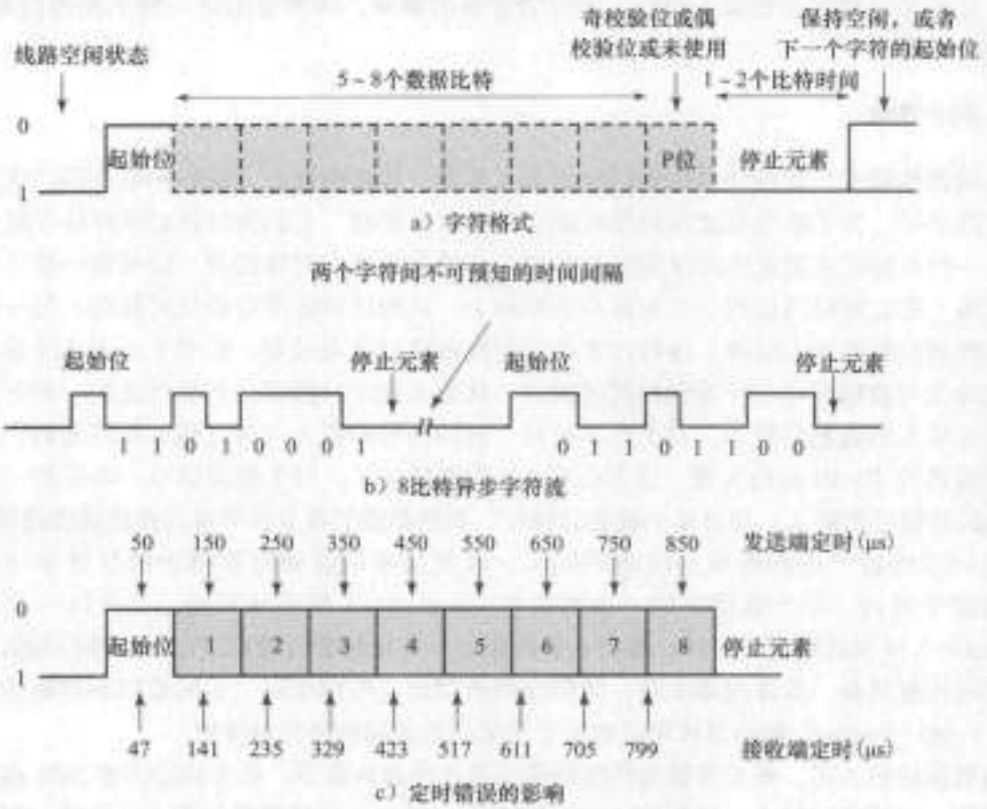


图 5-9 异步传输

如果发送的是平稳的字符流，那么两个字符之间的间隔是统一的，并且与停止元素相等。例如，停止元素一个比特时间，并且发送的是 IRA 字符 A、B、C（用的是偶校验），那么发送的模式是 0100000101001000010101100001111…111[⊖]。起始位（0）开始了其后 9 个元素的时序，这 9 个元素分别是 7 比特的 IRA 码、奇偶校验位和停止元素。在空闲状态时，接收端查找从 1 到 0 的转变，作为下一个字符开始的标志，然后对输入的信号每一个比特时间间隔就采样一次，一共采样 7 次。其后再查找下一个 1 到 0 的转变，这个转变的出现不会早于一个比特时间。

这种传输方案的定时需求程度为中等。例如，IRA 字符典型的是发送 8 比特单元，其中包含一个奇偶校验位。如果接收端比发送端快或慢 5%，第八个字符比特的采样时间偏差了 45%，但仍然可以正确采样。图 5-9c 展示了定时错误的影响严重到导致接收出错的情况。在这个例子中，我们假定数据率是每秒 10 000 比特（10Kbps），因此每一比特的信号持续时间为 0.1ms 或 100μs。假定接收端是快了 6%，或者每比特时间快了 6μs，因此接收端每 94μs（依据接收端的时钟）就对输入的字符进行采样。可以看到，最后一次采样是错误的。

异步传输简单并且便宜，但其为每字符引入了 2 到 3 比特的额外开销。例如，对于不带奇偶校验位的 8 比特字符，其中使用了一个比特长度的停止元素，这样每 10 个比特中就有 2 比特是仅用来同步而不传输信息的，这样额外开销就是 20%。当然，可通过在起始位和停止

⊖ 在文中，传输的数据是从左（第一个传输的比特）到右（最后传输的比特）显示的。

元素之间传递更大的比特块，来降低额外开销所占百分比。然而，就如图 5-9c 所示，比特块越大，定时错误越容易积累。因此，为得到更高的效率，通常采用另一种不同的同步形式，称为同步传输。

5.3.2　同步传输

在**同步传输**中，比特块以稳定的流的形式传递，传输中没有开始码和结束码。该比特块可为一段字符。为了避免发送端和接收端之间的定时漂移，它们的时钟必须保持一定程度的同步。一种可能的方案是在发送端和接收端之间提供单独的时钟线路。信号的一端（发送端或接收端）每比特时间加载一个短脉冲到线路上，从而使得线路有规则地脉动。另一端则可用这些规则的脉冲作为时钟。这种技术在短距离传输时效果较好，但对于远距离传输，这些时钟脉冲会与数据信号一样受到相同的损伤，从而出现定时错误。其他可选的一种方案是将时钟信息嵌入到数据信号中。对于数字信号，时钟信号的嵌入可通过曼切斯特编码、差分曼切斯特编码或 4B/5B 编码实现，这些已在 5.2 节解释过了。对于模拟信号，可采用一些技术来实现时钟信号的嵌入，如可基于载波的相位，利用载波的自身频率来与接收端保持同步。

在同步传输中还需要另一层面的同步，以使接收端能确定数据块的开始和结束。为了达到这个目的，每个数据块以一个前同步（preamble）位模式开始，并且以一个后同步（postamble）位模式结束。另外，数据块还需添加一些比特来传递控制信号，该控制信号用于数据链路控制规程，具体见第 6 章。所传递的数据加上前同步码、后同步码和控制信号，就构成了一**帧**（frame）。帧的具体格式取决于所采用的数据链路控制规程。

当数据块较大时，同步传输的传输效率比异步传输高得多。异步传输需要 20% 或以上的额外开销。在同步传输中，控制信号和前同步码、后同步码通常都少于 100 比特。例如，在一种比较通用的方案，即 HDLC 中，控制信号和前同步码、后同步码共 48 比特。因此，对于由 1000 个字符组成的一个数据块而言，每帧包含 48 比特的额外开销和 10008=8000 比特的数据，因此额外开销的比例仅为 $48/8048 \times 100\%=0.6\%$。

对于在低速的终端或个人电脑上的应用来说，可采用异步传输。这种传输技术成本低，并且在大部分的交互式应用中，这种技术的效率低也不会成为问题，因为这些应用中大部分时间是用来看屏幕和思考，而不是传输。然而对于通信比较多的应用，异步传输中的额外开销则会花费很多的代价。

对于大型系统和计算机网络，则需要同步传输的效率，即使同步传输带来了发送端和接收端之间时钟同步的技术问题。

除了传输效率的需求外，大量数据的传输也引入了差错检测的需求。在一些交互式应用中，用户检查自己的输入和输出来检测错误，这可通过查看包含错误的重新按键内容和屏幕显示内容来实现。而这个差错检测过程在长文件传输中是明显不可行的，因为该传输过程非常快，并且通常没有操作者在场。如我们即将看到的，同步传输中使用了数据链路控制规程，该规程可自动检测传输错误，并且重传出错的帧。

5.4　差错检测

5.4.1　差错控制的必要性

如第 4 章所述，噪声和其他损伤能造成数据通信错误。在计算机网络中，错误检测和错

误恢复的能力是其很重要的一个方面，并且随着时间的推移变得愈为重要。究其原因，部分是因为业务操作中数据的完整性越来越重要。没有业务会使用在数据获取、传输和存储方面质量较差的网络。在数据存储或使用于数据库更新之前，检测出该数据在传输过程中发生错误非常重要。一些数据是不能出错的，例如，试想一下电子基金数据传输中一个未检测到的数据错误可能造成的影响。由于带宽增加和数据量的增大，在通信和大型存储系统中的业务对错误越来越难以容忍。通常，在任何处理大量数据的系统中，未纠正和未检测到的错误能降低系统的性能和延长系统的响应时间。

差错控制（error control）涉及两个概念：

- **差错检测**（error detection）：为了检测到错误的出现，将冗余（redundancy）引入到数据流中。
- **差错纠正**（error correction）：一旦接收端检测到错误，接收端和发送端就协作实现错误所在帧的重传。

在本节中，我们探讨错误检测的过程，有关错误纠正将在第6章描述。

5.4.2 奇偶校验

一种最简单的错误检测方法是在数据块的末尾添加一个奇偶校验位。典型例子是IRA字符的异步传输，每个7比特的字符后都附加一个奇偶校验位。通过该校验位值的选取，使得字符有偶数个二进制1（偶校验）或奇数个二进制1（奇校验）。因此，例如，如果传输者传递字符G（1110001）并且使用奇校验，那么他将在末尾添加一个二进制1，实际传递的是11100011。接收端检查所接收到的字符，如果二进制1的总个数是奇数，则认定没发生错误。如果其中的一个比特（或奇数个比特）在传输过程中发生了错误的反转（例如11000011），那么接收端就会检测到错误发生。然而需注意的是，如果两个比特（或偶数个比特）因为出错发生了反转，则错误将不会被检测到。因此，利用奇偶校验位的方法不是一个万无一失的数据错误检测方法。

实际上，噪声脉冲的持续时间通常比较长，从而导致多个比特出错，特别是在数据率比较高的情况下。脉冲噪声除了损坏数据比特外，也会损坏奇偶校验位。因此，奇偶校验的错误检测能力依赖于噪声脉冲损坏的比特总数（是奇数还是偶数）以及使用的奇偶校验惯例（奇校验还是偶校验）。典型地，同步传输中使用的是偶校验，异步传输中使用的是奇校验。

5.4.3 循环冗余校验

当使用同步传输时，可采用比简单的奇偶校验更有效（具有较低的额外开销比例）并且检测能力更强（能检测到更多的错误）的一种错误检测技术。这种技术需要在每一个同步帧后添加**帧校验序列**（Frame Check Sequence，FCS）或**错误检测码**（error-detecting code）。图5-10展示了FCS的使用，该FCS使用了这节中所介绍的循环冗余校验码。在发送端，将待传递帧中的比特进行计算，所得结果作为一个添加字段插入到帧中。在接收端，对所接收到的比特进行与发送端相同的计算，计算得到的结果与输入帧中存储的值比较。如果两者不相符，则接收端认定出现了错误。

循环冗余校验（Cyclic Redundancy Check，CRC）是一种最常用并且检测能力最强的错误检测码。在这种技术中，所传递的消息作为一个长的二进制数字进行处理。将该数字除以一个唯一的二进制质数（即该数只能被其自身或1整除），所得余数附加在待传递帧后。当接

收端接收到一帧后，利用相同的除数，经过相同的除法过程，将所得的余数与附加在帧后的余数进行比较。除数用得最多的是17比特的除数（产生16比特的余数）和33比特的除数（产生32比特的余数）。它们分别称为CRC-16和CRC-32，其中数字16和32代表添加在待传递帧后的FCS的长度（单位为比特）。

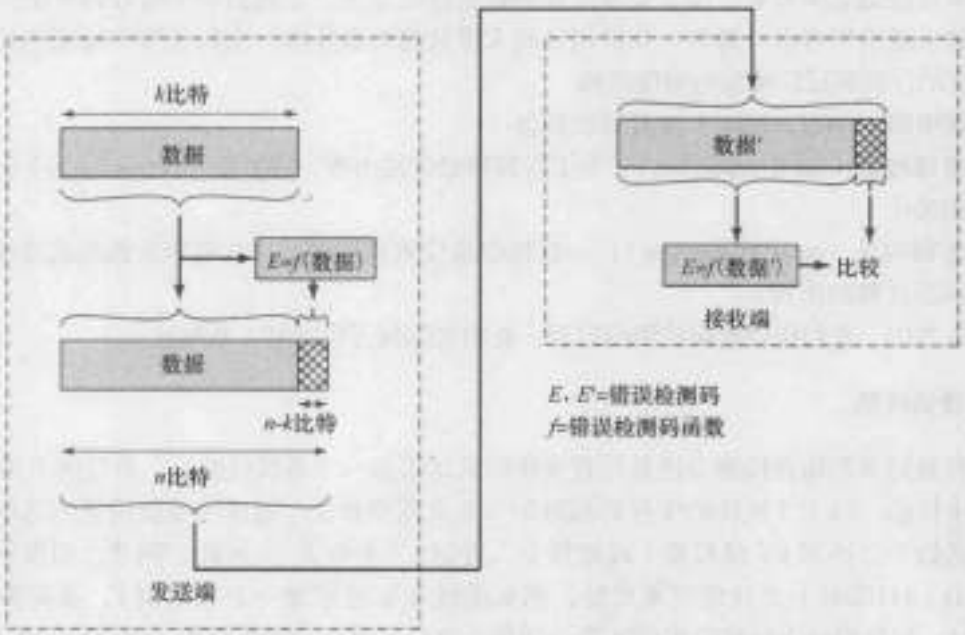


图5-10　错误检测过程

一个错误检测码评价的检测效率通常用它所能检测到的错误百分比来表示。对于长度为N的CRC，未检测到错误的比率大约为2^{-N}（详见[STAL04]）。这就意味着CRC-16能检测到99.998%的通信错误，而CRC-32能检测到近99.9999998%。总的来说，CRC是一种检错能力非常强的方法，并且需要的额外开销非常小。例如，如果将16比特的CRC用于1000比特的帧中，所带来的额外开销仅为1.6%。对于32比特的CRC，额外开销为3.2%。

应用注解

设备、编码、通信参数和协议

编码方案、协议和传输错误通常不是我们每天网络体验中的一部分。从终端用户角度来看，我们所知道的只是网络（或计算机）是否工作。即使我们直接与各种通信系统有交互，我们通常都不会深层次地考虑这些事情。然而，如果在网络安装、维护和错误追踪过程中，对其中所涉及的数据通信设备和标准有较深的了解，那就大不同了。

今天的计算机可用很多方法实现与其他机器的通信。USB、EIA232（又名COM或串口）、防火墙、网卡、视频以及鼠标和键盘接口分别代表着一种数据传输形式。容易使人困惑的是一些机构通常利用不同的计算平台连接在一起。结果是一个设备所使用的协议和编码方案可能与另一个设备截然不同。例如，一个公司拥有一些Macintosh计算机和一些运行Windows系统的计算机。因此，就需要为防火墙和USB分别购买对应的外围设备，如打印机。此外，它们所运行的网络协议也可能不同或需要额外的支持。

终端模拟程序可能也会带来困难。串行连接在一起的计算机必需配置成“讲同一种语言”，包括确定链路的速度、所使用的数据比特数目和奇偶校验方法。这需要在链路两端人工进行配置。这些程序的最典型应用是通过一个控制端口配置路由器和访问点。然而，网络协议，如连接到 WAN 的协议，可能需要一些额外的一连串的配置。如果其中的一项配置出错，则通信就无法进行。

操作系统和设备驱动由于将设置暴露给用户进行修改，从而会产生一些问题。这样的例子可在以太网速度配置中看到。网络设备上的端口和网络接口卡可配置为特定的速率和全双工或半双工工作模式。这些信息的配置通常可由“自动感知”网络自动实现，手工改变配置则可能限制甚至阻断了网络连接。在这种情况下，不同的设置使得通信两端的速率不同，甚至完全改变了编码方案，因此通信的两端不能相互理解对方。另一个例子是你将连接到的无线网络的类型。从 802.11 标准到其他标准的简单转换能让你无法连接到网络。

每一个成功的传输都离不开错误控制。错误控制的意思是错误检测或者错误检测与纠正。现在的网络出错率非常低，每传输十亿比特数据出现一比特错误就已经非常多了。现在最常用的错误检测形式是单个奇偶校验位、循环冗余校验和校验和（checksum）。这些技术通常应用在底层协议和文件系统中。一些底层协议中内置了一些错误检测和测试功能。一些协议，如点到点协议（Point-to-Point Protocol，PPP），还提供了一些额外的错误控制工具，虽然这些工具现在已不常使用了。这些机制的补充机制通常应用于高层协议，如 TCP 协议中的序列号和重传机制。

随着无线网络的出现，网络传输的错误率就增加了，并且出现了一些额外的问题，如连接丢失等。通常而言，无线局域网的吞吐量比有线网络小得多。这是因为无线网络是共享传输介质的，每个节点必须和其他节点竞争带宽。无线网络的这种接入方式与以太网相似，但接入时间更长。最后，无线局域网中的每帧都需要确认（acknowledge，ACK），这进一步减缓了网络的速率。虽然可通过一些新的快速无线标准减少这些延迟，传输介质仍然是共享的，并且还是需要 ACK 的。由于这些原因，有必要通过修改一些通信参数（如前同步码长度、负载均衡、信道）来保证无线传输的成功。

终端用户和网络管理员都不能修改所有的通信系统参数。例如，没人能修改用于 100baseT 以太网中的 4B/5B 编码。然而，理解编码方案、配置和协议操作之间的相互关系能有助于提高效率、加快解决问题和为设计过程提供支持，以避免许多问题。明智的管理员应该了解哪些设置是终端用户能修改并且要修改的。在许多情况下，回归本原是解决一个通信问题的唯一办法。

5.5 总结

模拟信号和数字信号都可编码成模拟信号或者数字信号。编码方案的选取要依赖于所要满足的需求，以及可用的传输介质和通信设施。例如，在模拟电话线路上传输数字信息时，需要用一个调制解调器将数字数据转换成模拟形式。相似地，目前数字设施用得越来越广泛，语音信息需要编码成数字形式后，才能在这些数字设施上传递。现今网络中所用的数据和信号的多种组合总结在表 5-6 中。

表 5-6 数据和信号的组合

数据	信号	编码方案	转换设备	实例
数字	模拟	幅移键控（ASK） 频移键控（FSK） 相移键控（PSK）	调制解调器	电缆调制解调器 DSL 调制解调器 拨号调制解调器
模拟	数字	脉冲编码调制（PCM）	编解码器	数字电话
数字	数字	4B/5B 差分曼切斯特编码 曼切斯特编码 NRZI NRZ-L	数字收发器	局域网 ISDN PC 到外置调制解调器
模拟	模拟	振幅调制（AM） 频率调制（FM） 相位调制（PM）	变换器	电话 有线电视 AM 和 FM 无线电

在将比特流从一个设备经由传输链路传至另一个设备时，需要两边的大量合作和协定。其中最基本的需求是同步。接收端必须知道所接收比特的速率，这样才能定期对线路取样，以此决定所接收到比特的值。通常采取两种技术达到这个目的。在异步传输中，数据的每个字符单独处理。每个字符以一起始位作为开始，来提醒接收端一个字符正在到达。接收端对字符中每比特取样，然后寻找下一个字符的开始处。这种技术对于长的数据块效果不好，因为接收端的时钟可能会偏移到最终与发送端的时钟失去同步。然而，以大数据块的形式发送数据比每次只发送一个字符效率要高。对于大数据块的传输，通常采用同步传输技术。每个数据块格式化成一帧，其中包含起始标志和结束标志。一些同步形式，如曼切斯特编码，可用来保持同步。

错误检测技术是数据传输中的一个重要部分。使用得最为广泛的错误检测算法是循环冗余校验。

5.6 关键术语、复习题和练习题

关键术语

Amplitude-Shift Keying（ASK，幅移键控）
analog data（模拟数据）
analog signal（模拟信号）
analog transmission（模拟传输）
asynchronous transmission（异步传输）
codec（编解码器）
Cyclic Redundancy Check（CRC，循环冗余检验）
digital data（数字数据）
digital signal（数字信号）
digital transmission（数字传输）
error-detecting code（错误检测码）
error detection（错误检测）
Frequency-Shift Keying（FSK，频移键控）
modem（调制解调器）
Phase-Shift Keying（PSK，相移键控）
Pulse Code Modulation（PCM，脉冲编码调制）
synchronous transmission（同步传输）

复习题

5.1 数据和信号之间有什么不同？
5.2 区分模拟数据、模拟信号和模拟传输。

5.3　区分数字数据、数字信号和数字传输。
5.4　调制解调器的功能是什么？
5.5　编解码器的功能是什么？
5.6　请说明在业务网络中数字传输比模拟传输好的主要原因。
5.7　简要描述将数字数据编码成模拟信号的三种基本方法。
5.8　波特率的意思是什么？
5.9　对比信号率和数据率。
5.10　描述下列调制解调器类型之间的区别：语音级、电缆、ADSL。
5.11　什么是脉冲编码调制？它是怎样工作的？
5.12　什么是 NRZ-L 编码？它与 NRZI 编码有什么区别？
5.13　什么是 4B/5B 编码？它是怎样工作的？
5.14　将设备或系统与正确的信号和数据进行匹配。

设备 / 系统	数据 / 信号
调制解调器传输	A：数字数据 / 数字编码
以太网	B：数字数据 / 模拟编码
AM/FM 无线电	C：模拟数据 / 数字编码
PCM	D：模拟数据 / 模拟编码

5.15　同步传输和异步传输之间最基本的不同点是什么？
5.16　在异步传输中，每个字符要额外添加哪些比特？简单解释每比特的添加理由。
5.17　为什么同步传输比异步传输更有效？
5.18　数据传输中为什么要使用错误控制？
5.19　错误控制中两大主要组成部分是什么？
5.20　奇偶校验是怎样工作的？
5.21　奇偶校验检测不到什么类型的错误？
5.22　循环冗余校验是怎么工作的？

练习题

5.1　给定比特串 01100，分别用 ASK、BFSK 和 BPSK 对该数据进行编码。
5.2　利用曼切斯特编码对比特串 01001110 进行编码。
5.3　一个数字信号采用的是差分曼切斯特编码，并且数据传输率是 4Mbps，该信号的波特率是多少？
5.4　下面的每个 4 比特数据串采用什么样的 4B/5B 码：1011，0011，1101，1001？
5.5　给定字符 1010010，为了实现偶校验，需要添加的比特是什么？
5.6　两个通信设备采用单比特的偶校验来进行错误检测。发送端发送字节 10101010，由于信道噪声，接收端接收到的字节是 10011010。接收端能检测到错误吗？为什么？
5.7　从 YouTube 查找并观看一些介绍数字传输优点的视频。推荐 3 个 URL 给其他业务数据通信的学生观看。如果仅能推荐一个，你会推荐哪一个？为什么？
5.8　利用因特网研究拨号调制解调器、电缆调制解调器和 DSL 调制解调器的演变过程。利用 8 – 12 页的 ppt 报告，总结这些类型的调制解调器在调制能力和传递速度方面是怎样增

长的，以及这些增长背后的主要原因。并总结这些技术的未来发展。

5.9　在网上做一些研究，查找一些图片，其中比较好地完成了使用脉冲调制来数字化模拟波形这方面的任务。并且查找 PCM 应用的一些通用实例。将你找到的图片放到 8 到 12 页的 ppt 报告中，该报告主要调查 PCM 的基本过程以及它的广泛应用。

5.10　假定一个经脉冲调制编码的信号导致了接收端不能很好地解码出原始数据。简要描述能改进所调制信号的准确性的两种方法。

5.11　在脉冲调制编码中，每秒对模拟数据采样 8000 次，每个样本转换成 8 比特的值，那么这种信号编码的数据率是多少？

5.12　假设你需要下载一个大小为 400 000 字节的文件。假定下载中所需的控制字符使得共需要下载的数据增加 10%（共 440 000 字节）。计算使用如下类型的调制解调器时，下载该文件各需要的时间（秒）：

a. 56Kbps 拨号调制解调器

b. 1.5Mbps ADSL 调制解调器

c. 10Mbps 电缆调制解调器

数据链路控制及复用

学习目标

通过本章的学习，读者应该能够：

- 了解流量控制和差错控制的需求。
- 了解传输效率的需求，并列出获取效率的两种主要方法。
- 详述视频分发和音频网络中的频分复用技术的使用。
- 描述数字载波系统中复用技术的使用。
- 详述 T-1 服务，并描述它的重要性以及可能使用该服务的应用。
- 详述 SONET 标准及其在广域网组网中的重要性。

本章讨论了两种重要的数据通信概念：数据链路控制和复用技术。

数据链路控制协议包括通信链路上数据流的整形技术，以及传输错误的弥补措施。所有类型的商务计算机网络（如以太 LAN、Wi-Fi 网络以及专用 WAN）中都有数据链路空盒子协议。我们首先考察流控制和差错控制的概念，然后关注复用技术以及通常使用复用技术的链路类型。本章末的附录展示了数据链路控制协议 HDLC 中的流控制和差错控制。

本章探查为什么复用技术能在公共数据通信网络以及私有数据通信网络中得到广泛应用。任何企业分布式数据处理（Distributed Data Processing，DDP）环境中主要的花费是传输费用。企业要想使其物理上分散的操作场所相互通信就必须购买或租用线路，通信线路的每种使用方案都与一定的费用相关联。

在早期的企业计算机网络中，通信线路基本由电话公司提供。企业数据通常使用调制解调器来转换成模拟载波信号，在语音信道上进行传递。在这种场合下，数据沿着已存在的电话线路，从企业工作场所传递到电话公司的中心局交换机，数据再从那里沿着电话公司的电路交换网络传输，直至传递到企业其他的工作场所。一些企业如果不愿通过公共电话交换网（PSTN）来传递他们的数据，就可租用线路，在工作场所之间提供点到点的连接。

如今，电话公司需要与竞争性的本地接入运营商（competitive local access carriers）以及其他一些因特网服务提供商（Internet Service Provider，ISP），如有线电视公司，来竞争为企业订购者和消费者提供通信线路。在本地市场中竞争的多个生产商能提供拨号连接、租用线路以及各种宽带服务。这样的本地竞争能帮助企业控制住在数据通信方面的开销，但需要他们来监督定价与服务供应，以保证他们能从通信方面的投资中获得最大的经济效益。

为了能从数据通信方面的投资中获得最大的回报，企业需要利用传输线路传递最大化的信息量。这就意味着最大限度地利用他们网络中的链路容量。如果企业还未充分利用已有的链路容量，就没有必要投资额外的链路容量，更不必投资不需要的额外通信容量。当你能租用一个廉价的 56Kbps 线路，为什么要租用 1.5Mbps 的通信线路呢？对于企业的计算机网络管理者而言，如何在通信开销与数据传输需求之间获得较好的平衡点，是一个持续性的挑战。

广而言之，企业的决策关乎着数据的传输效率。显然，企业希望以尽可能高的成本效率来传递企业数据。企业使用的传输设施必须有能力来处理需要通信的数据流量。然而，企业如果将资金花费在超出他们需求的通信线路上，则他们就牺牲了效率。因此本章的大部分内容都在讨论获得高传输效率的主要方案：复用技术。

6.1　流控制和差错控制

物理层接口标准提供了在传输介质上以同步或异步方式传输数据流的方法。然而，这些接口没有包括数据通信需要的所有功能。这些所缺的功能中，最重要的是流控制和差错控制。

为了提供这些必需的功能，需要使用链路控制协议。这些协议通常仅用于同步传输。基本的方案如下。应用待传递的数据首先传递至数据链路模块，由该模块将数据封装成一系列帧。每帧中添加了控制位，允许通信两端合作以可靠地传递数据。控制位由帧的发送者添加。在帧到达后，由接收者检查控制位，如果数据正确到达，就剥离掉控制位，然后将纯数据传递到系统中指定的目的点。图 6-1 描述了这个处理过程。通过控制位的使用，能实施一些功能，包括流控制和差错控制。

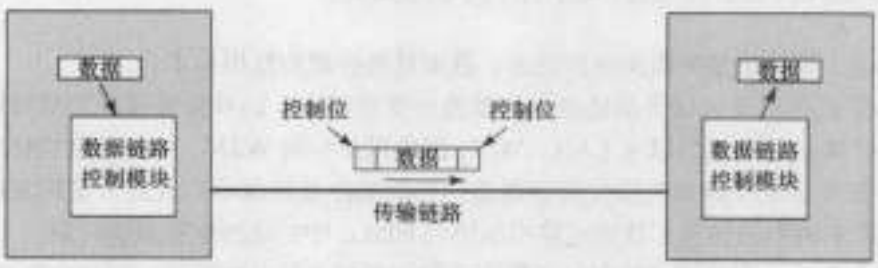


图 6-1　数据链路控制模块的操作

6.1.1　流控制

设想我们希望编写一个程序，称为打印机驱动程序，将数据从计算机传输到打印机。我们将用一个合适的电缆将打印机与计算机的通信端口连接起来。通信端口可通过编程来与外围设备相匹配。在这种情况下，我们设定打印机传输的是 IRA（ASCII）7 位字符、奇校验、1 位停止位，并且数据传输速率是 9600bps。我们用这些参数对通信端口进行编程，并且试着发送一页的文本到打印机。结果是，在文本最初几行之后，就出现了大量的字符丢失，实际上是丢失的字符比打印出的字符还多。

问题出自哪里？首先，我们来计算字符的传输速率。每个字符有 7 位，另外 1 位用于起始位，1 位用于奇偶校验，1 位用于停止位，因此每个字符共有 10 位。因为计算机的传输速率是 9600bps，字符速率是每秒 960 个字符。通过检查打印机的说明书，我们发现打印机的最大打印速率是每秒 80 个字符。这意味着我们以打印机能接受速率的 12 倍速率发送数据，难怪数据会丢失。

打印机的数据接收能力比它的打印能力要高，这看起来很奇怪，其实很普通。打印机有一个小的缓冲区（可能是 200 字符），因此能接收突发速率的字符，并打印这些字符，然后再接收下一个突发。这样允许打印机运用在一个高速运行的共享线路中，该线路为多台打印机和计算机提供服务。例如，一条 9600bps 的线路能容易地容纳 5 台或 10 台打印机。然而由于

数据传输速率是高于打印速率的，前面所描述的过载条件也会发生。

流控制（flowcontrol）是一种使发送实体不会用数据淹没接收实体的技术。与企业网络相连的许多设备（如打印机或磁盘驱动器）都有固定大小的缓冲区来接收数据。当数据传递到一台计算机时，典型情况下，这些数据是指定给某个应用或系统程序的。接收数据的计算机为该应用或系统程序分配具有某最大长度的缓冲区。当接收到数据后，计算机必须对该数据进行一定的处理，然后再将其传送给上层软件。如果没有流控制，接收端在处理前面接收到的数据时，缓冲区会被填满和溢出。

流控制是网络通信的开放系统互连（Open System Interconnection，OSI）参考模型中数据链路层（即第二层）的基本功能之一。数据链路层直接工作在物理层之上，在物理层上传输的是用来运载数据的信号。数据链路层的任务是在网络中的物理链路（如电信线路）上提供可靠的数据传输。除流控制外，数据链路层的基本功能还包括定义帧，以及这些帧的错误检测和控制。

对数据链路控制协议而言，流控制可通过对帧顺序标号（如 0，1，2，…）来实现。接收端初始分配一个协商好大小的缓冲区。当帧到达并处理后，接收端向发送端发回一个确认，用来表明帧已被接收，并暗示发送端可发送更多的帧。

许多的数据链路控制协议都支持滑动窗口流控制。这在附录 6A 所讨论的 HDLC 流控制中进行了说明。有关该机制的详细讨论在网上附录 K 中。

6.1.2　差错控制

在第 5 章中，我们讨论了一些技术，使得接收端能检测到传输和接收处理过程中出现的错误。为了能纠正这些错误，数据链路控制协议提供机制使得通信两端合作，重传那些检测到错误的帧。这些机制扩展了前面讨论的流控制技术。这里，数据仍然以顺序标号帧的形式发送。此外，我们还需考虑两种类型的错误：

- **帧丢失**：即帧没到达通信的另一边。在网络错误类型中，网络可能仅是简单地传递帧失败。在直接的点到点数据链路情况下，突发噪声可能损坏一帧达到一定程度，使得接收端根本不知道发送端已发送了一帧。
- **帧损坏**：一个可被识别的帧到达了，但是帧中的一些比特出错（在传输过程中被修改）。

最通用的差错控制技术通常基于下述一些或全部要素实现：

- **差错检测**：目的端利用差错检测技术（如第 5 章描述的 CRC）检测帧是否出错，并且丢弃这些错误帧。
- **肯定应答**：在正确接收到没有错误的帧后，目的端返回给源端一个肯定应答。
- **超时重传**：如在预定的时间内源端没收到来自目的端对已发送帧的应答，则重传该帧。
- **否定应答和重传**：当检测到帧出错时，目的端返回一个否定应答，源端则重发该帧。

这些机制总体上称为**自动请求重传**（Automatic Repeat Request，ARQ）。ARQ 的功能是使得不可靠的数据链路变为可靠链路。ARQ 的过程在附录 6A 中作为 HDLC 一部分进行描述。

6.2　链路复用的动机

通常两个通信站点不能完全利用连接它们的链路的容量。为了通信效率和提高容量利用

率，需要与其他通信设备共享链路的容量。这种共享的常用术语是复用（multiplexing）。

复用通常应用在长距离通信。长距离网络的干线通常是一些高容量的光纤、同轴电缆或者微波链路。通过复用，这些链路能同时承载大量的语音和数据传输。

图 6-2 中描述了一种最简单的复用功能，其中的复用器（multiplexer）有 n 个输入。复用器通过一单根数据链路与分用器（demultiplexer）连接在一起。该链路能传递 n 个独立的数据信道。复用器将 n 条低速输入线路上的数据组合（即复用）起来，并将其发送到高容量的数据链路上。分用器接收到经复用的数据流，依据信道将这些数据独立出来（即分用），并将它们发送到对应的输出线路上。



图 6-2　复用

数据通信中广泛应用的复用技术可解释如下：

- 数据率越高，则数据设备的成本效益越高。就是说，对于给定的应用和给定的传输距离，随着传输设备的数据率的增加，其每 Mbps 的成本是下降的。同样，发送设备和接收设备的每 Mbps 成本也是随数据率的增加而下降的。
- 大部分的单个数据通信设备仅需要适中的数据率支持。例如，对于许多个人计算机和移动设备应用，如果不涉及 Web 访问或集中的图片浏览，数据率在 9600bps – 64Kbps 之间通常就能满足需要了。

前面描述的是数据通信中的情况，这在语音通信中也是相似的。就是说，一个传输设备（就语音信道而言）的容量越大，则单个语音信道的成本就越低。

本章余下部分将集中讨论两种类型的复用技术。一种是频分复用（Frequency-Division Multiplexing，FDM），这个技术用得最多，任何用过无线电或电视机的人都比较熟悉这个技术。第二种是时分复用技术（Time-Division Multiplexing，TDM）的一个特例，即同步 TDM，这种技术通常用于数字化语音流和数据流的复用。

6.3　频分复用

频分复用（FDM）是一种大家熟悉的、应用广泛的复用技术。频分复用的一个简单使用例子是有线电视系统，用一条电缆承载多路的视频信道。当传输介质的带宽超出信号传输所需的带宽时，就可以用 FDM 了。如果一些信号中的每个信号调制到不同的载波频率上，并且每个载波频率之间是充分隔离开的，使得各信号的频带不相互重叠，那么这些信号就可同时传递。图 6-3a 给出了 FDM 的一个常用例子。六个信号源将信号输入到复用器，该复用器将每个信号调制到一个不同的频率（f_1，…，f_6）上。每个经调制的信号需要某个以它的载波频率为中心的带宽，称为一个信道（channel）。为了避免相互干扰，这些信道用保护带隔离开，这些频带是频谱中未被使用的部分。

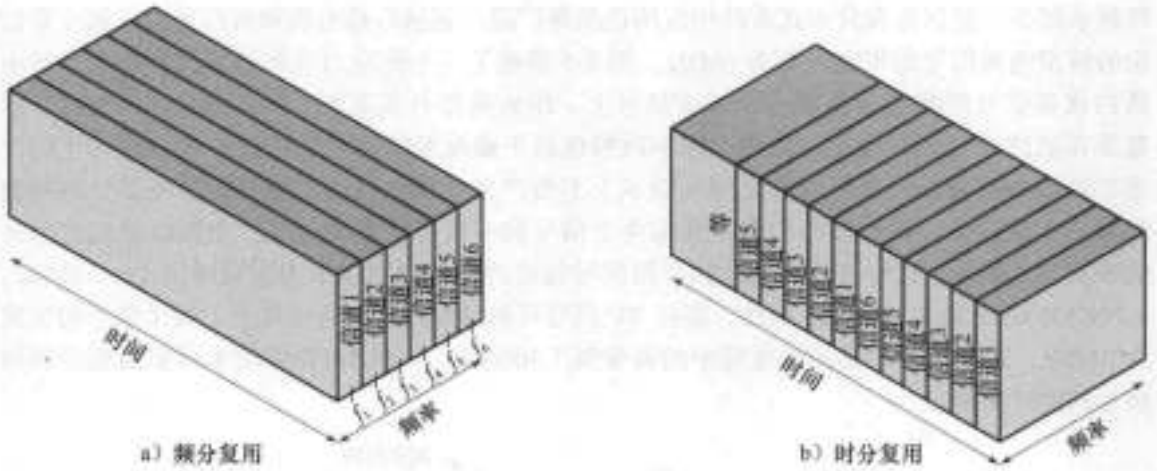


图 6-3　FDM 和 TDM

在介质上传输的组合信号是模拟的。但要注意的是，输入信号可以是数字的，也可是模拟的。在数字输入的情况下，输入信号必须经过一个调制解调器转换成模拟信号。在任一情形下，每个模拟输入信号都需经调制转移到合适的频带中。

图 6-4 给出了一个 FDM 的简单例子，图中展示了三个语音信号同时在一个传输介质上传递的情形。如前面所述，语音信号的带宽通常为 4kHz，其有效频谱是 300 – 3400Hz（见图 6-4a）。如果用这样的信号来幅值调制一个 64kHz 的载波，那么就得到图 6-4b 所示的频谱。经调制后的信号其带宽为 8kHz，从 60kHz 延伸到 68kHz。为了充分利用带宽，我们选择传输该频谱的下半部分，称为下边带。相似地，其他两个语音信号可分别调制到 64 – 68kHz 和 68 – 72kHz 范围内。这些信号然后经过复用器的组合，产生出 60 – 72kHz 范围内的一个信号。在接收端，分用器将所接收到的信号拆分成三个频带，然后将每个信号解调回原始的语音频带（0 – 4kHz）。注意，经复用的信号之间仅有很少一部分的频率重叠。由于每个信号的有效带宽（算上有效频带上下两边的保护带）实际上都少于 4kHz，实际上不会产生显著的干扰。

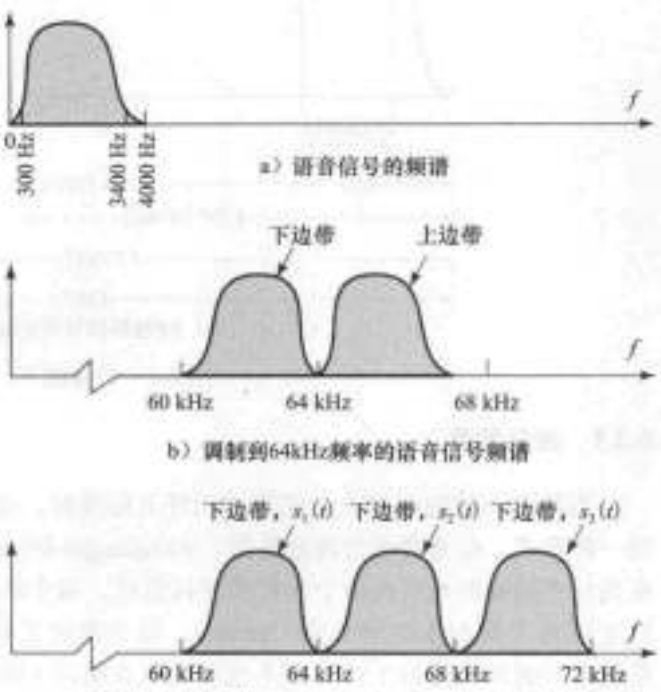


图 6-4　三个语音频带信号的频分复用

FDM 多年来曾经一直是电话传输中的支撑技术。就带宽而言，FDM 在电话传输中比在数字系统中更有效。但在 FDM 中，噪声是随语音信号一起放大的。由于这个原因，再加上数字电子器件价格的急剧下降，电话网络中 TDM 系统大范围地取代了 FDM 系统。

虽然 FDM 在语音传输中使用

得越来越少，但在电视分布式系统中应用仍然很广泛，包括广播电视和有线电视。第 2 章讨论的模拟电视信号的带宽正好为 6MHz。图 6-5 描述了一个传递的视频信号及其带宽，其中黑白视频信号经幅值调制到一个载波信号上。得到的信号带宽大约为 5MHz，其大部分带宽是在载波信号带宽之上。另外，用单独的色彩子载波来传递色彩信息。该载波与主载波在空间上相隔很远，这样两者之间从根本上不会产生干扰。最后，信号的音频部分则调制到第三个载波上，该载波的带宽在其他两个信号的有效带宽范围之外。所形成的组合信号的带宽为 6MHz，其中视频、色彩和音频信号载波的频率分别在下边缘频带之上 1.25MHz、4.799 545MHz 和 5.75MHz。因此，多路 TV 信号可频分复用到一条电缆上，每个信号的带宽为 6MHz。如果提供的是同轴电缆中的高带宽（500MHz），则用 FDM 技术可实现很多视频信号的同时传输。

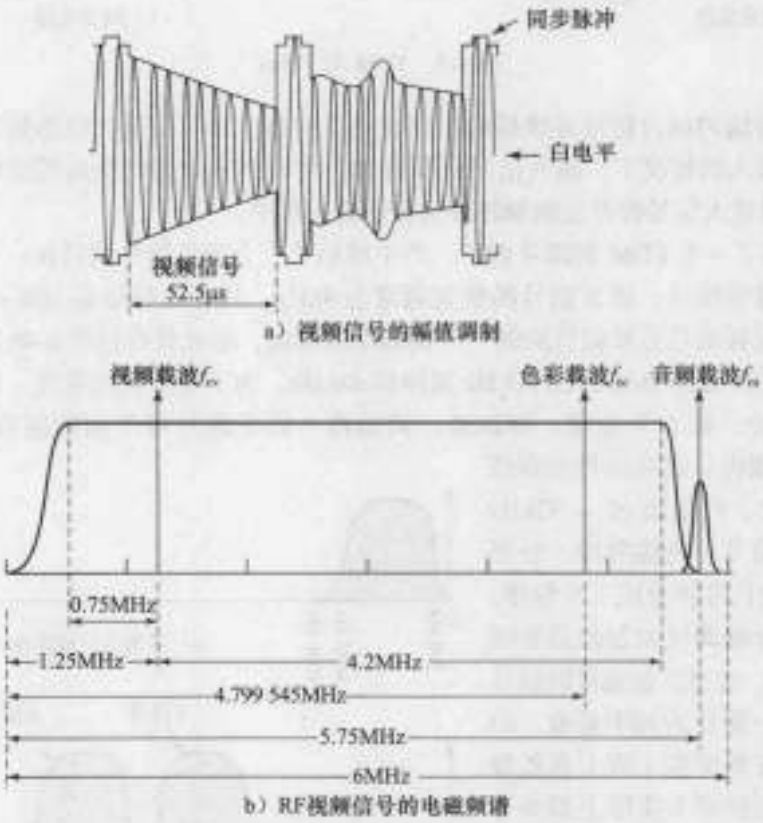


图 6-5　传输的 TV 信号

6.3.1　波分复用

当频率不同的多束光在相同的光纤上传递时，光纤的潜能就发掘出来了。这是频分复用的一种形式，但通常称为**波分复用**（Wavelength-Division Multiplexing，WDM）。利用 WDM，在光纤中传递的光可由多个色彩或波长组成，每个承载一个单独的数据信道。1997 年 Bell 实验室证实了具有 100 个光束（beam）、每个光束工作在 10Gbps 的 WDM 系统的可用性，该系统的数据率是每秒 1 百万兆（也可表示为每秒 1 兆兆位，或 1Tbps）。现在的商用系统能有 160 个信道，每个信道的数据率是 10Gbps。在实验室环境中，阿尔卡特的系统能有 256 个信道，每个信道的数据率是 39.8Gbps，总的数据率是 10.1Tbps，并能传递 100km 的距离。正在

进行着的研究和开发表明，单个信道的数据率超出 100Gps 是可能的。

一个典型的 WDM 系统与其他 FDM 系统具有相同的通用架构。一些信号源产生具有不同波长的激光束。这些光传到复用器，由复用器将它们组合起来在单个的光纤线路上传递。通常由相距几公里的一些光放大器将这些波长同时放大。最后，该组合信号到达一个分用器，在那里组合的信道被分离出来，并发送到位于目的地的接收端。

绝大多数的 WDM 系统的波长范围是 1550nm 之内。在早期的系统中，每个信道分配 200GHz 的波段区间（spacing），但是现在大部分的 WDM 系统用的是 50GHz。表 6-1 给出了由 ITU-TG.692 定义的信道区间，该定义能容纳 80 个 50GHz 信道。

表 6-1　ITU WDM 信道区间

频率（THz）	真空中的波长（nm）	50GHz	100GHz	200GHz
196.10	1528.77	X	X	X
196.05	1529.16	X		
196.00	1529.55	X	X	
195.95	1529.94	X		
195.90	1530.33	X	X	X
195.85	1530.72	X		
195.80	1531.12	X	X	
195.75	1531.51	X		
195.70	1531.90	X	X	X
195.65	1532.29	X		
195.60	1532.68	X	X	
…	…			
192.10	1560.61	X	X	X

文献中经常看到术语**密集波分复用**（Dense Wavelength-Division Multiplexing，DWDM）。这个术语没有官方的或标准的定义。该术语暗示着可以比普通的 WDM 用更多的信道，这些信道在区间上更加接近。通常认为，一个区间为 200GHz 左右的信道就是密集的。

WDM 也用于光纤到户（Fiber-To-The-Home，FTTH）系统中，这些系统已在第 5 章介绍，并在图 5-5 中进行了展示。许多服务供应商通过他们的 FTTH 与用户之间建立连接，并用该连接传送有线电视服务。在 FTTH 有线电视网络（能提供如每次观看付费的交互式服务）中，分别为上行信号和下行信号使用不同的波长。

6.3.2　ADSL

非对称数字用户线（Asymmetric Digital Subscriber Line，ADSL）提供了使用 FDM 的一个有趣例子。ADSL 在第 5 章介绍并在图 5-4 中进行了展示。在这节中，我们简要回顾一下这种方法。

1. ADSL 设计

使用术语非对称是因为 ADSL 中下行信道（从网络运营商的中心局到用户端）的容量比上行信道（从用户到网络运营商）的容量大。ADSL 最初的应用目标是视频点播（Video On

Demand，VOD）以及相关服务。自从 ADSL 引入后，运行于 ADSL 之上的 VOD 并没有取消高速因特网的接入需求。典型地，因特网用户对下行传输的容量需求比上行传输的容量需求大。绝大多数用户的传输形式是：先是上传键盘输入或短的电子邮件消息，随后的输入流量（特别是 Web 下载）能产生包括图像甚至视频的大量数据。因此，ADSL 很适合用户来进行因特网访问。

ADSL 通过一种新的方法使用频分复用（FDM），从而充分利用双绞线电话线的 1MHz 容量。ADSL 的部署策略包含三个要素（见图 6-6）：

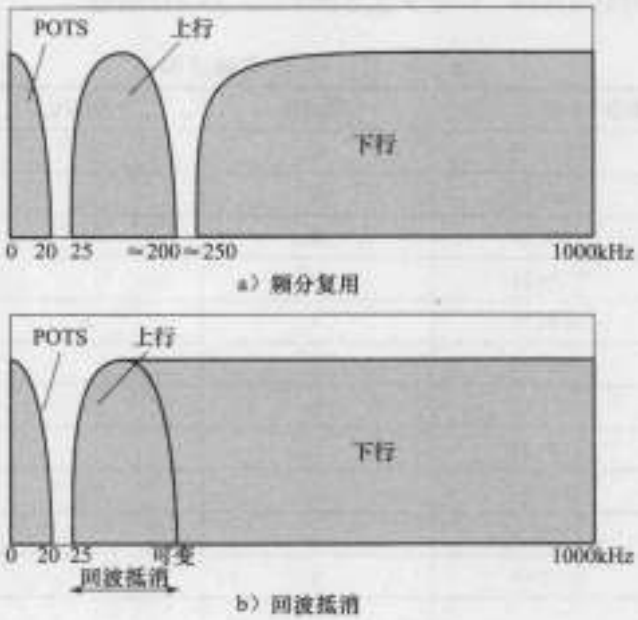


图 6-6　ADSL 信道配置

- 将容量中最低的 25kHz 部分预留给语音，称为简易老式电话服务（Plain Old Telephone Service，POTS）。语音只能承载在 0 到 4kHz 频带中。额外的带宽能防止语音信道和数据信道之间的串扰。
- 使用回波抵消[⊖]或者 FDM 来分配两个频带：一个小的上行频带，一个大的下行频带。
- 在上行和下行频带内使用 FDM。这种情况下，单个的位流划分成多个并行的位流，每一部分承载到一个单独的频带上。一种常用的技术称为离散多音调（Discrete Multi Tone，DMT），这种技术将在后面解释。

当使用回波抵消时，上行信道的整个频带都与下行信道的频带低端部分相重叠。与上行信道和下行信道分别使用不同频带的方法相比，这种方法具有两个优势。

- 频率越高，衰减越大。利用回波抵消技术，下行带宽中更多的部分位于频谱中好的区域。
- 回波抵消设计能更灵活地改变上行信道的容量。上行信道能在不进入下行频带的情况下向上扩大自己的频带（如当需要上传大文件时），随之而来的是重叠的区域也扩大了。

⊖ 回波抵消是一种信号处理技术，允许在一条传输线路上同时以相同的频带进行双向的信号传输。实际上就是，传输者必须从输入信号中减去自己所传输的回波，以恢复出从另一端发送的信号。

使用回波抵消的不足是线路两端都需要回波抵消逻辑。

依据线缆的直径和质量，ADSL 方案能提供近 5.5km 的传输范围。这能覆盖 95% 的美国用户，在其他国家也能提供具有竞争性的覆盖率。

2. 离散多音调

离散多音调利用工作在不同频率的多路载体信号，在每条信道上发送一些数据比特。可用的传输频带（上传频带或下传频带）划分为多个 4kHz 的子信道。初始时，DMT 调制解调器先在每条子信道上发送一些测试信号，获得每条信道上的信噪比。然后，调制解调器在信号传输质量好的信道上多发送一些比特，而在信号传输质量差的信道上少发送一些比特。图 6-7 表明了这个过程。每个子信道承载的数据率是从 0 ~ 60Kbps。图中展示了一个典型的场景，其中随着频率的增加，信号的衰减逐渐增大，因此信噪比也随着下降。因此，子信道的频率越高，则该信道能承载的负荷越少。

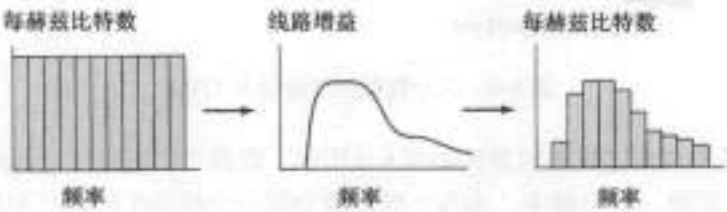


图 6-7　每个信道的 DMT 比特数分配

目前的 ADSL/DMT 设计采用 256 个下行子信道。从理论上来说，每个 4kHz 子信道承载 60Kbps，因此能获得的数据率为 15.36Mbps。由于传输损伤的存在，这个数据率实际上是无法获得的。依据传输线路的距离和质量，目前所实现的系统通常工作在 1.5Mbps 到 9Mbps。

6.4　同步时分复用

6.4.1　TDM 机制

复用的另一种主要形式是**时分复用**（Time-Division Multiplexing，TDM）。在这节中，我们将考察**同步 TDM**（synchronous TDM）。

当传输介质的数据率超出信号传输所需的数据率时，就可使用时分复用技术。利用该技术，通过将每个信号的一部分在时间上交错插入，可实现多个数字信号或模拟信号同时传输。图 6-3b 给出了 TDM 的一个常用例子。在该图中，6 个信号源输入到复用器中，该复用器以循环的方式交错插入每个信号的位，从而实现每个信号位的轮流传输。例如，在图 6-3 中的复用器有六个输入，每个输入比如说是 9.6Kbps，这样单条线路的容量至少为 57.6Kpbs 时才能容纳这六个信号源。

图 6-8 展示 TDM 的一个简单例子，其中三个数据信号在传输介质上同时传递。在该例中，每个信号源工作在 64Kbps。每个信号源的输出利用缓冲区进行缓存。每个缓冲区的长度典型地为 1 比特或 1 字符。循环扫描这些缓存器，形成组合的数字数据流。这些扫描的操作非常快，这样在下个数据到达前就能清空缓冲区。经扫描的数据由复用器组合形成一个混合数据流。因此，复用器的数据传输率至少要等于这三个输入的数据率之和（3 × 64=192Kbps）。由复用器产生的数字信号可用数字方式传递，或者经由调制解调器转换

成模拟信号后进行传递。不论采用上述哪种传输方式，一般都是同步传输（相对于异步传输）。在接收端，分用器需要将输入的数据分布到三个目的地缓冲区中。

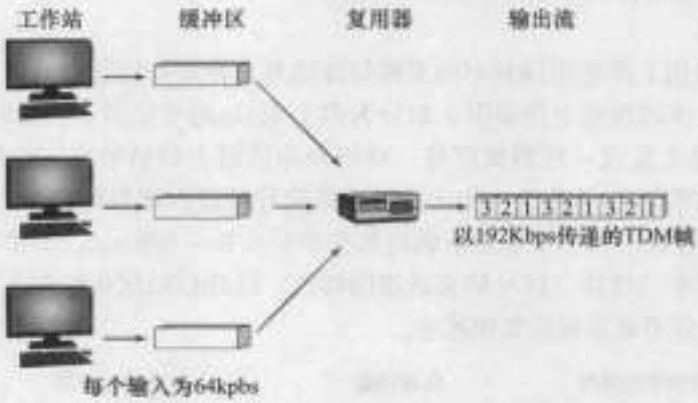


图 6-8　三个数据信道的同步 TDM

同步 TDM 系统所传递数据的形式如图 6-9 所示。数据组织成帧（frame），每帧包含一个时隙（time slot）周期。在每帧中，为每个数据源分配一个或多个时隙。因此在同步 TDM 系统中，数据传输就是帧序列的传递。在每帧中为某数据源分配的时隙组成的集合就称为信道（channel），注意这术语与 FDM 中使用的术语相同，术语“信道”的两种用法逻辑上是等价的。在这两种情况下，为每个信号源的信号分配一部分传输容量，每个信号源见到的是一个具有常量数据率或常量带宽的信道，用于传输数据。

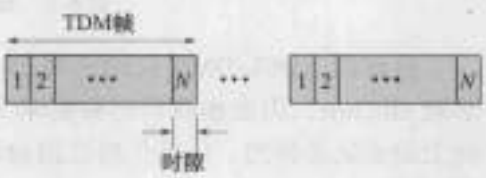


图 6-9　TDM 帧结构

时隙长度通常等于发送缓冲区的长度，典型的值为 1 位或 1 字节（字符）。字节交错技术可用于同步信号源和异步信号源。这时每个时隙包含一个字节的数据。对于异步传输，在传输前通常先要除去每个字符的起始位和结束位，然后由接收端再插入起始位和结束位，这样可提高传输效率。位交错技术通常用于同步信号源中。

同步 TDM 之所以称为同步并不是因为采用了同步传输，而是因为预先为每个数据源分配时隙，并且时隙保持固定。对于一个给定的数据源，不论其是否有数据需要发送，都会传递为其分配的时隙。这个当然与 FDM 相同；不论数据源在某时间内是否有数据发送，频带都会分配给该数据源。在这两种情况下，为了实现的简单都浪费了容量。即使采用固定分配时隙的形式，一个 TDM 设备也能处理具有不同数据率的数据源。例如，在每帧中为低速输入设备分配 1 个时隙，而为高速设备分配多个时隙。

6.4.2　数字传输系统

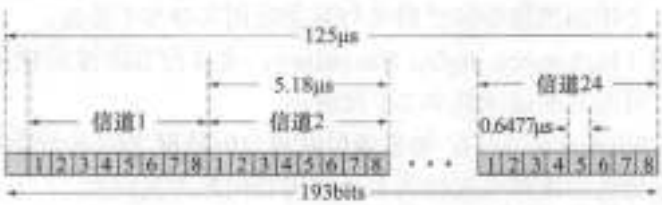
美国以及整个全球提供的长距离传输系统最初用来在高容量传输线路（如光纤、同轴电缆和微波）上传递语音信号。由于这些电话通信网络向数字技术的迈进，这些网络中已采用同步 TDM 传输结构。在美国，AT&T 公司开发了具有多重容量的层次式 TDM 结构，

这种结构也在加拿大和日本使用。相似的但不完全相同的层次式结构在 ITU-T 的推动下已在全球采用，在欧洲，也广泛使用这种结构并称为 E 载波层次，其中的 E 代表欧洲，见表 6-2。

表 6-2　北美和国际 TDM 载波标准

北　美			国际（ITU-T）		
名称	语音信道数	数据率（Mbps）	级别	语音信道数	数据率（Mbps）
DS-1	24	1.544	1	30	2.048
DS-1C	48	3.152	2	120	8.448
DS-2	96	6.312	3	480	34.368
DS-3	672	44.736	4	1920	139.264
DS-4	4032	274.176	5	7680	565.148

在北美和日本，TDM 层次的基础是 DS-1 传输格式（见图 6-10），共 24 个信道。每帧中包含每个信道的 8 位数据，共 24 个信道，再加上 1 个组帧位。因此，每帧是 193 位（24 信道 × 每信道 8 位 +1 组帧位）。语音传输遵循如下的规则。每帧中每个信道包含 1 字节（8 位）经数字化后的语音数据。原始的模拟语音信号的数字化通过脉冲编码调制（PCM）进行，采样速率为每秒采样 8000 次。因此每个信道时隙和每帧必须每秒钟重复 8000 次。如果帧的长度为 193 位，那么数据率就为每秒 8000 帧 × 每帧 193 位 =1.544Mbps。每 6 帧中的前 5 帧使用的是 8 位 PCM 采样。对于第 6 帧，每个信道包含 7 位 PCM 字节再加上一个信令位（signaling bit）。这些信令位为每个信道形成了一个控制流，其中包含一些网络控制信息和路由信息。例如，控制信号用来为电话建立连接或断开电话。



注：

1. 第 1 位为组帧位，用于同步
2. 语音信道
   - 每 6 帧中的 5 帧采用 8 位 PCM
   - 每个第 6 帧采用 7 位 PCM，每个信道的第 8 位为信令位
3. 数据信道
   - 某些方案中的第 24 信道用于信令
   - 位 1 ～ 7 用于 56Kbps 服务
   - 位 2 ～ 7 用于 9.6Kbps、4.8Kbps 和 2.4Kbps 服务

图 6-10　DS-1 传输格式

相同的 DS-1 格式用于提供数字数据服务。为了与语音数据兼容，采用与语音数据相同的 1.544Mbps 数据率。在这种情况下，提供 23 个信道的数据。第 24 信道保留给特殊的同步字节，可用于在帧出错后快速、可靠地重构帧。在每个信道中，每帧中的 7 位用于数据，第 8 位为该帧指明这个信道包含的是用户数据还是系统控制数据。由于每个信道是 7 位，并且每秒钟每帧要重复 8000 次，因此每个信道的数据率是 56Kbps。利用一种称为低率复用

（subrate multiplexing）[⊖]的技术来提供低的数据率。

最后，DS-1 格式可用来混合承载语音信道和数据信道。这种情况下要使用全部的 24 个信道，不提供同步字节。

基于 1.544Mbps 这个基本的数据率，可通过将 DS-1 输入进行位交错实现更高层次的复用。例如在 DS-2 传输系统中，将四个 DS-1 的输入组合起来形成一个 6.312Mbps 的数据流。将这四个数据源输入的数据每次交错 12 比特位。注意 1.544 × 4=6.176Mbps，余下的容量用于组帧位和控制位。

DS-1、DS-1C 等名称依据传递信息的复用方案来确定。AT&T 和其他电信公司提供传输设施来支持这些经复用的信号，这些设施称为电信系统（carrier system）。这些系统用“T”标签表示。因此，T-1 系统提供 1.544Mpbs 的数据率，能支持 DS-1 复用格式，并能支持更高的数据率。

6.4.3　T-1 设施

T-1 设施被公司广泛应用，以提供网络功能以及控制成本。T-1 设施最通常的外部应用是给客户提供租用通信。这些设施能允许客户建立专用网络以便在机构内传递流量。这些专用网络的应用举例如下：

- **专用语音网络**（private voicene network）：当通信站点之间有大量的语音流量时，租用拨号设施之上的专用网络能节省很大的开销。
- **专用数据网络**（private data network）：相似地，两个或多个通信站点之间大量的数据传输可用 T-1 线路支持。
- **视频电话会议**（video teleconferencing）：允许传递高质量的视频数据。由于视频所需带宽的下降，专用的视频会议线路可与其他应用共享 T-1 设施。
- **高速数据传真**（high-speed digital facsimile）：允许传真图像的快速传输，并且依据传真负载情况，可与其他应用共享 T-1 设施。
- **因特网接入**（Internet access）：如果通信站点与因特网之间有大量的流量，那么就需要有一根高容量的访问线路来连接到本地的因特网服务提供商。

当用户需要传递大量的数据时，使用专用 T-1 网络有两个优势。一是 T-1 的配置比使用其他低速混合设备（如多路专用的 56Kbps 线路）的配置简单，二是 T-1 传输服务比较便宜。

T-1 的另一个广泛应用是提供从客户房屋到电话网络的高速访问。在该应用下，在客户房屋内的局域网或 PBX 为产生大量区域外流量的一些设备提供 T-1 线路，以便该设备访问公共网络。

6.4.4　Sonet/SDH

同步光纤网（Synchronous Optical Network，SONET）是一种光传输接口，它最初是为公用电话网络设计的，并在 20 世纪 80 年代开始实施，到现在仍在广泛应用着。它由 ANSI 进

⊖ 在这种技术中，从每个信道夺取 1 个额外位，用于指明是否采用了低率复用。这样每个信道的总容量为 6 × 8000=48Kpbs。该容量可用于复用 5 个 9.6Kpbs 的信道、10 个 4.8Kpbs 的信道或者 20 个 2.4Kpbs 的信道。例如，如果第 2 个信道用于提供 9.6Kpbs 的服务，那么最多有 5 个数据子信道可分享该信道。每个子信道的数据显示为第 2 个信道中每第 5 帧中的 6 位。

行标准化，以便用于语音、长途数据和 / 或视频通信应用。与之类似的版本，称为同步数字系列（Synchronous Digital Hierarchy，SDH），是由 ITU-T 在建议书 G.707、G.708 和 G.709 中提出的[⊖]。

SONET 的目标是提供规范来利用光纤的高速数据传输能力。与以太网相似，SONET 提供物理层（对应 OSI 模型的第一层）接口技术，其上能运行多个高层应用协议。例如，可将 IP 数据包配置成在 SONET 电路上传递。

1. 信号等级

SONET 规范定义了经标准化的数字数据速率的等级，见表 6-3。最低级是 51.84Mbps，该级称为 STS-1（Synchronous Transport Signal Level1）或者 OC-1（optical carrier level 1）[⊜]。这速率能用来传递单个的 DS-3 信号或者一组低速信号，如 DS1、DS2、加上 ITU-T 数据率（例如 2.048Mbps）。

多路 STS-1 信号能组合形成 STS-N 信号，通过将来自于互同步的 N 路 STS-1 信号的字节进行交错得到该信号。对于 ITU-T 的同步数字系列，其最低数据率为 155.52Mbps，称为 STM-1，它对应于 SONETSTS-3。

SONET 上最通用的数据传输速度是在 155Mbps 和 2.5Gbps 范围之内。为了创建这样的数据流，SONET 将低速信号（带宽为 64Kpbs）复用成 STS 帧。

2. 帧格式

SONET 的基本单元为 STS-1 帧，该帧由 810 个八位字节组成，每隔 125μs 发送一帧，总的数据率为 51.84Mbps（见图 6-11a）。每帧逻辑上可看成一个矩阵，该矩阵为 9 行，每行 90 个八位字节，按照从左向右、从上到下的顺序每次传递一行。

帧的前三列（3 个八位字节 ×9 行 =27 个八位字节）是开销八位字节，称为段开销（section overhead）和线路开销（line overhead），它们与描述 SONET 传输的详细程度相关联。这些 8 位字节不仅传递同步信息，还传递网络管理信息。

表 6-3　SONET/SDH 信号等级

SONET 名称	ITU-T 名称	数据率	负载率（Mbps）
STS-1/OC-1	STM-0	51.84 Mbps	50.112 Mbps
STS-3/OC-3	STM-1	155.52 Mbps	150.336 Mbps
STS-9/OC-9		466.56 Mbps	451.008 Mbps
STS-12/OC-12	STM-4	622.08 Mbps	601.344 Mbps
STS-18/OC-18		933.12 Mbps	902.016 Mbps
STS-24/OC-24		1.244 16 Gbps	1.202 688 Gbps
STS-36/OC-36		1.866 24 Gbps	1.804 032 Gbps
STS-48/OC-48	STM-16	2.488 32 Gbps	2.405 376 Gbps
STS-96/OC-96		4.876 64 Gbps	4.810 752 Gbps
STS-192/OC-192	STM-64	9.953 28 Gbps	9.621 504 Gbps
STS-768	STM-256	39.813 12 Gbps	38.486 016 Gbps
STS-3072		159.252 48 Gbps	1.539 440 64 Gbps

⊖ 在本文后面，我们用术语 SONET 来表示这两种标准，当存在不同时会在文中标明。

⊜ OC-N 速率是 STS-N 电子信号的光等效速率。为了在光纤中传输，当终端用户发送电子信号时，这些信号必须转换成光信号，当终端用户接收时，必须从光信号转换为电子信号。

帧中的其他部分是有效载荷，它由 SONET 的逻辑层提供，该逻辑层称为路径层。有效载荷中包含一列路径开销，它不是必须在第一列的位置。线路开销中有个指针用来指明路径开销的起始位置。

图 6-11b 给出了高速帧的通用格式，其中采用的是 ITU-T 名称。

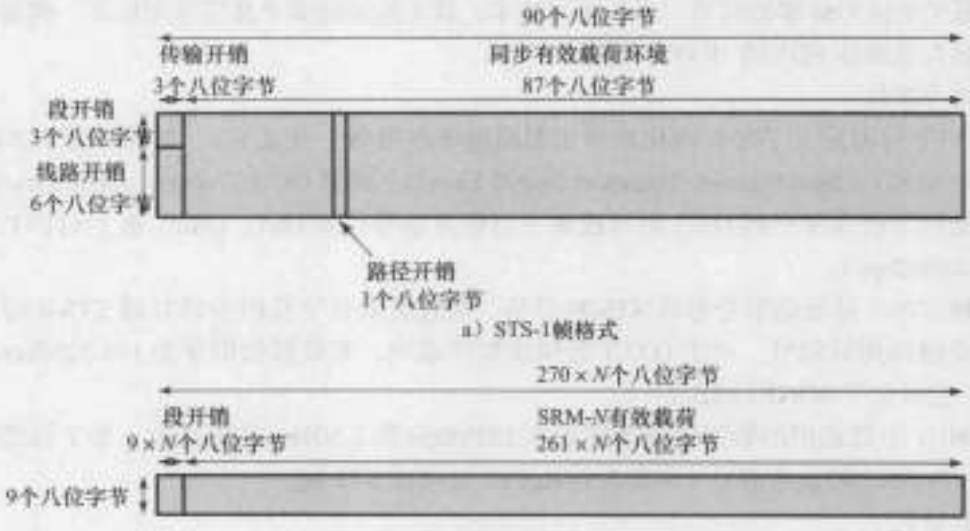


图 6-11　SONET/SDH 帧格式

6.4.5　蜂窝和无绳电话系统

频分复用技术已被应用于模拟蜂窝和无绳电话系统。当采用频分多址（Frequency-Division Multiple Access，FDMA）时，用于连接移动设备与蜂窝塔的无线电频谱化分为多个独立频率的信道，每个信道能承载一路电话。模拟蜂窝和无绳电话系统中也使用频分双工（Frequency-Division Duplexing，FDD）技术。FDD 中使用的是两个频带，一个频带用于传输上传链路信道（例如，从移动设备到蜂窝塔），另一个频带用于传输下传链路信道（从蜂窝塔到移动设备）。

如第 17 章所述，在蜂窝电话中，时分多址（Time-Division Multiple Access，TDMA）和码分多址（Code-Division Multiple Access，CDMA）技术已广泛替代了频分技术。然而在某些情况下也组合使用频分复用和时分复用技术。例如，在二代 GSM 系统中，蜂窝塔和移动设备之间的无线电频谱划分为多个频率信道，但每个频率信道又进一步划分为多个时隙，每个时隙传输一路语音电话的数据。因此，二代 GSM 系统使用了 FDMA 和 TDMA 的组合。

家庭使用的大部分无绳数字电话系统采用的是 TDMA 或时分双工（Time-Division Duplexing，TDD），这种技术与 FDM 同时使用。在 TDD 中，语音电话的上传链路在其频率信道上采用时分复用技术，该频率信道与语音电话下传链路的频率信道相同。

应用注解

通信技术的变革

跟随数据通信机制的发展来看数据通信会很有趣，特别是对比十年前甚至五年前如何

将数据从一处传输到另一处的技术。像其他技术一样，用来保证正确传输的技术也会过时，会被其他的一些错误消除技术来代替。这些变革并不总是技术进步的结果，大部分是由于通信内容以及通信对象的变化而导致的。

技术通常一直是进步着的，创建新的方法来解决问题。当我们查看广域网，特别是其所使用的协议时，我们发现许多的改变都是用来提高通信的质量和速度。例如，X.25 协议曾经是将站点连接到广域网的一种通用协议，该协议提供了许多功能来保证无错连接，广域网中的所有节点都要实施错误检测。随着数据传输中传输设备和传输介质的改进，这些大量的错误检测就不再需要了，并被认为是浪费开销。

然而，如果没有大量的外部连接需求，这个开销可能不会是个问题。以前单个节点没有大量访问外部资源的需求。随着分布式处理技术的出现，业务站点、Web 站点、hotmail、搜索引擎之间的安全互联，以及一些重要搜索资源的在线提供，这个规则就被完全打破了。逐渐地我们看到人们和机构越来越多地向网站发送数据。

为了避免重传数据堵塞传输线路，我们需要提高传输的速度和准确性。可增加一些新的应用来满足外部连接中这方面的需求。游戏产业投入了大量的财力来开发功能强大的虚拟世界，让他们的大量用户能安全地实现在线移动。在线游戏，如 World of Warcarft 和 Halo3，就是这方面的典型实例。我们看到网络从 X.25 到帧中继，到 T-carrier，到 ATM，其后到 SONET 的迁移。下一代网络可能通过 10Gigabit 或更高速率的以太网链路来完成所有的信息传输。

大学通常是受这种趋势影响的最典型的机构。各个大学都在向各种最先进的列表上竞争一席之地，这些列表可见于 PC 杂志和 Yahoo!Internet Life 报告。而通过定期更新来提升桌面链路速度、路由能力、协议支持、移动性和外部连接，都是为达到先进性的动力所趋。这些目标也包含了维护校园网络可用性和安全性的一些新策略。学生们对网络基础设备的要求通常很高，并且大部分的网络管理员和教授都能保证提供新的工具和技术，以在网络上通信和共享文件，而这些工具和技术则由学生们实现。

不只是到外部世界的有线连接改变了我们交换信息的方式，无线通信是教育网和非教育网络的另一项需求，这确切地反映了我们通信需求的改变。很难想像没有无线网络的世界会是怎样的。无线网络在技术支持、安全和管理方面有着广泛的影响。人们现在希望能随时随地保持联系。这就意味着应用要保持持续服务状态。持续服务指随着用户的移动而网络的拓扑结构、协议和速度发生改变时的网络连接能力。移动网络最常用的技术是 802.11，但也包括 MobileIP（以保证漫游连接）和 IPv6，来满足大量用户以及服务质量的需求。随着我们越来越多地采用基于 IP 的技术，电话系统的变化也在朝着这方面发展。

向无线网络的发展意味着性能方面的问题越来越突出，因为熬受了专用 10Mbps 或 100Mbps 连接的用户之间需要共享速度慢得多且更易出错的链路。因此就需要网络服务提供商保证通信质量，以提高单个节点的访问能力以及无线电干扰控制。

当我们从一种体系结构发展到下一个体系结构，以及从一组协议改变至另一组协议时，相应的流控制和差错控制可能也会改变，但其目标是相同的。链路必须进行管理以减少错误并保证链接。除了理解新的协议，网络服务提供商必需在用户选择不同路径时跟踪用户的信息流，并且改变系统需求。

6.5 总结

由于传输可能出错，并且数据的接收方可能需要对到达数据的速率进行调整，必需在每个通信设备之上加上一个控制层以提供如流控制、错误检测和错误控制的功能。该控制协议称为**数据链路控制协议**。

对于大多数业务提供商来说，传输费用是数据通信预算中的最主要部分。公司面临着越来越多的工作区域内的业务信息共享，因此必须利用一些技术，来提高所使用通信链路的传输效率。

复用是一种常用的提高传输效率的方法。利用复用技术，许多的传输源可共享单条通信链路。这能使业务提供商认识到用少一些的高容量链路而不使用很多的低容量链路所能达到的规模经济。通过复用，更多的传输源能共享一条通信链路的空闲容量，从而保证该链路的高利用率。频分复用技术能用于模拟信号，通过为每个信号分配一个不同的频带，许多信号就可在相同的介质上同时传输。该技术中，调制装置用来将每个信号调制到所分配的频带上，并且由复用装置将调制后的信号组合在一起。该技术用于广播和有线电视分布式系统中，也广泛应用于电话网络中来复用语音信号。然而由于电话网络在向数字操作转变，在电话网络中使用的频分复用技术正逐渐被同步时分复用技术所取代。波分复用和 ADSL 是频分复用的一种形式。

同步时分复用技术能用在数字信号或模拟信号中来传递数字数据。在这种形式的复用中，来自不同传输源的数据在重复的帧中传递。每帧由一组时隙组成，在每帧中为每个传输源分配一个或多个时隙。这种技术广泛应用于数字电话网络以及机构内的数字通信设施中。一种最为通用的同步 TDM 形式是 T-1，这指的是由多个传输源提供的一条租用传输设施（传输速率为 1.544Mbps），以及用于该设施的特定复用格式。T-1 常用于为物理位置上分散的机构构建专用网络，并且越来越多地提供给业务用户来访问公用电话网络。

统计时分复用能比同步 TDM 提供更高效率的服务来支持终端。在统计 TDM 中，时隙不预先分配给一个特定的数据源。用户数据先经缓存，然后利用可用的时隙尽可能快地传递出去。在终端网络应用中，统计 TDM 已在很大程度上取代了同步 TDM。

TDM 也用于 SONET 上，以支持在光纤电路上长距离传输语音、数据以及视频应用。SONET 和 SDH 运用 TDM 达到每秒多个 Gigabit 的数据率。蜂窝电话网络中则使用 TDM 和/或 TDM 与 FDM 的混合。

案例研究Ⅳ：宽带接入：全局和局部问题

这个案例研究涉及的主要概念有宽带固特网接入选项、有线通信和国家、数字鸿沟。

这个案例分析以及其他的案例可访问 www.pearsonhighered.com/stallings。

6.6 关键术语、复习题和练习题

关键术语

Automatic Repeat Request（ARQ，自动请求重发）

Data Link Control Protocol（数据链路控制协议）

Discrete Multi Tone（DMT，离散多音调）
error control（差错控制）
flow control（流控制）
frame（帧）
Frequency-Division Multiplexing（FDM，频分复用）
multiplexing（复用）
synchronous TDM（同步 TDM）
Time-Division Multiplexing（TDM，时分复用）
Wavelength-Division Multiplexing（WDM，波分复用）

复习题

6.1　对于业务计算机网络管理员来说，为什么传输效率是个问题？
6.2　在发送端和接收端之间传递数据时，数据链路控制协议的作用是什么？
6.3　什么是流控制？
6.4　什么是差错控制？
6.5　列举出数据链路控制协议中差错控制的常用要素。
6.6　什么是复用技术？
6.7　简要描述频分复用与时分复用之间的区别。
6.8　FDM 中信道是怎样定义的？TDM 中又是怎样定义信道的？
6.9　为什么业务计算机网络管理员将复用技术视为一种物有所值的数据传输选择？
6.10　给出一些 FDM 实例。
6.11　简要描述怎样将 FDM 用于复用模拟语音信号，以及怎样用 FDM 来复用模拟有线电视信道。
6.12　定义用户线中的上行信道和下行信道。
6.13　简要描述 ADSL 中语音和数据是怎样复用的。
6.14　解释同步时分复用（TDM）是怎样工作的。
6.15　给出 T-1 线路的一些主要应用。
6.16　为什么使用私有 T-1 线路对公司具有吸引力？
6.17　什么是 SONET？
6.18　简要描述数字服务（DS）系列和光传输（OC）服务系列之间的不同。
6.19　简要描述 T-1 帧和 STS-1 帧之间的不同。
6.20　给出蜂窝电话网络中使用的一些复用类型。

练习题

6.1　在因特网上研究数据链路通信协议的主要功能。列举出广泛应用的数据链路控制协议的一些实例。用一篇 250 ~ 500 字的短文来总结你的发现。
6.2　在因特网上研究数据通信网络中的流控制技术。列出一些实例来说明为什么需要流控制，以及如何用它来保证发送端和接收端之间的可靠数据传输。用一篇 250 ~ 500 字的短文来总结你的发现。
6.3　在 YouTube 上查找并观看一些 ARQ（自动请求重发）的介绍。列出三个 URL 推荐给学习数据通信的学生，让他们进一步学习 ARQ 以及其中的错误控制规则。如果你只能推荐其中的一个给其他同学，你将选择哪一个？为什么？
6.4　在因特网上研究频分复用技术。列举出 FDM 应用的一些日常例子。将你的发现总结为

短文（250 ~ 500 字）或 5 ~ 8 页的 PowerPoint 报告。

6.5 在因特网上研究统计时分复用技术。用 250 ~ 500 字短文或 8 ~ 12 页的 PowerPoint 报告，总结出业务主管应该知道的 STDM 与同步 TDM 之间的主要不同点。

6.6 在因特网上研究波分复用技术。找出至少五个你认为比较好地解释 WDM 是怎样工作的图像。将这些图像包含到一个 8 ~ 12 页的 PowerPoint 报告中，该报告用来总结 WDM 是什么、它是怎么工作的以及它为什么应用很广。

6.7 在因特网上研究 DSL 接入复用器（DSLAM）及其在 DSL 中的作用。查找一些介绍 DSLAM 技术的图像 / 图片，将其包含到一个 500 ~ 750 字短文或 8 ~ 12 页 PowerPoint 报告中，该短文或报告关注 DSL 接入复用器及其在 DSL 服务中的重要性。

6.8 在因特网上研究 T-1 复用器以及 CSU/DSU（客户服务单元 / 数据服务单元）技术在 T-1 服务中的作用。用短文（250 ~ 500 字）或 5 ~ 8 页 PowerPoint 报告总结出你的发现。

6.9 为了获得语音和数据流量相关需求的一些印象，考虑如下：

a. 计算利用标准 PCM 传递三分钟的电话呼叫所发送的比特数目。

b. 如果用包含 IRA（ASCII-7 比特）文本的页（每页有 55 行，一行平均有 65 个字符）来表示三分钟电话呼叫，则需要多少页？

6.10 假设你是一个新公司的企业网络主管，并且该公司对你所在区域开放。假设已确定需要使用 T-1 连接到 ISP。研究你所在区域内提供 T-1 服务的 ISP 及其服务价格。利用这些信息完成一个 PowerPoint 报告，来总结可用的 T-1 服务选项。

6.11 假设你在设计一个 TDM 传输器（我们称之为 T-489）来支持 30 路语音信道，该信道采用 6 比特采样以及与 T-1 相似的结构。确定所需的比特率。

6.12 利用频分复用技术来组合 25 路语音信号时，需要多少总的带宽？

附录 6A 高级数据链路控制协议

HDLC 是一种重要的数据链路控制协议，它被广泛应用并且是许多其他重要数据链路协议的基础，这些协议采用与 HDLC 相同或相似的格式以及相同的机制。

1. HDLC 帧格式

介绍 HDLC 的最好方法是看它的帧结构。HDLC 操作涉及两个连接站点之间两种信息的交换。首先，HDLC 从上层软件接收用户数据，并将该用户数据通过链路传递至另一端。在通信的另一端，HDLC 接收到用户数据，并将其传递至该端的上层软件。其次，这两个 HDLC 组件交换控制信息、提供给流控制、差错控制和其他的控制功能。要做到这点，采用的方法是将所交换的信息格式化为**帧**（frame）。帧是一个预先定义的结构，为各种控制信息和用户数据提供特定的位置。

图 6-12 给出了 HDLC 帧的格式。该帧具有如下的字段：

- **标志**（flag）：用于同步。该字段出现在帧头和帧尾部分，通常包含模式 01111110。
- **地址**（address）：指明该传输的次站。该字段在多点线路情况下需要，主站可能向多个次站中的一个次站发送数据，以及多个次站中的一个次站向主站发送数据。该字段长度通常为 8 位，但可扩展，见图 6-12b。
- **控制**（control）：标明帧的目的和功能，这将在本小节后面介绍。

- **信息**（information）：包含待传递的用户数据。
- **帧检验序列**（frame check sequence）：包含 16 位或 32 位的循环冗余校验，用于错误检测。CRC 在第 5 章讨论。



图 6-12　HDLC 帧结构

HDLC 定义了三种类型的帧，每种帧的控制字段都不相同。信息帧（Information frame，I 帧）承载要传递给站点的用户数据。另外，信息帧也包含用于流量控制和差错控制的控制信息。监控帧（Supervisory frame，S 帧）提供了实施流量控制和差错控制的另一种方法。无编号帧（Unnumbered frame，U 帧）提供补充的链路控制功能。

控制字段中起始的 1 或 2 位指明帧的类型，其他的比特位组织成多个子字段，如图 6-12c 和 d 所示。这些子字段的功能在后继讨论 HDLC 操作时给出。注意，S 帧和 I 帧中的基本控制字段用了 3 位的序列号。通过适当的方式设置命令，可运用扩展的控制字段，该字段采用 7 位序列号。

所有的控制字段格式都包含探询 / 终止（P/F）位，它的使用依赖于上下文。典型情况下，在命令帧中，该位称为 P 位，在请求对等 HDLC 实体的应答帧时，设置该位为 1。在应答帧中，该位称为 F 位，该位设置值 1 时表明该帧是一个应答帧，作为请求命令的结果。

2. HDLC 操作

HDLC 的操作由站点间交换 I 帧、S 帧和 U 帧组成。表 6-4 列出了为这些帧类型定义的各种命令和应答。在描述 HDLC 操作时，我们讨论这 3 种类型的帧。

表 6-4　HDLC 命令和应答

名　称	命令 / 应答	说　明
信息帧（I）	C/R	交换用户数据
监控帧（S）		
接收就绪（RR）	C/R	肯定确认；准备好接收 I 帧
接收未就绪（RNR）	C/R	肯定确认；未准备好接收
拒绝（REJ）	C/R	否定确认；否认 N 起的各帧
选择拒绝（SREJ）	C/R	否定确认；选择拒绝
无编号帧（U）		
设置正常响应 / 扩展方式（SNRM/SNRME）	C	设置方式；扩展 =7 比特序列号
设置异步响应 / 扩展方式（SARM/SARME）	C	设置方式；扩展 =7 比特序列号
设置异步平衡 / 扩展方式（SABM/SABME）	C	设置方式；扩展 =7 比特序列号
设置初始化方式（SIM）	C	在编址站中初始化链路控制功能
断开连接（DISC）	C	中断逻辑链路连接
无编号确认（UA）	R	确认收到某个方式设置命令
断开连接方式（DM）	R	应答方已处在连接断开方式
请求断开连接（RD）	R	请求一个 DISC 命令
请求初始化方式（RIM）	R	需要初始化；请求一个 SIM 命令
无编号信息（UI）	C/R	用来交换控制信息
无编号探询（UP）	C	用于请求控制信息
复位（RSET）	C	用于恢复；重置 N（R）, N（S）
交换标识（XID）	C/R	用于请求 / 报告状态
测试（TEST）	C/R	交换标识信息字段以用于测试
帧拒绝（FRMR）	R	报告接收到不能接受的帧

HDLC 的操作涉及 3 个阶段。首先，由一端或另一端初始化一条数据链路，这样帧就可以按有序的方式进行交换。在该阶段通信双方协商确定所使用的选项。初始化后，通信双方交换用户数据以及用于实施流控制和差错控制的控制信息。最后，通信的一方发信号通知操作结束。

（1）初始化

通信双方的任一方都可利用 6 个方式设置命令中的一个来请求建立连接。该命令用于 3 个目的：

1）告知通信的另一方请求了初始化。

2）指明了请求的是 3 种方式中的哪个方式。这些方式与如下情况相关：即通信一方作为主站并且控制数据交换过程，或者通信双方是对等的并且两者在数据交换中合作。

3）指明采用的序列号是 3 比特还是 7 比特。

如果通信另一方接收了这个请求，那么该端的 HDLC 装置发送一个无编号确认（Unnumbered Acknowledgement，UA）帧给初始化请求方。如果拒绝该请求，则发送一个断开连接（Disconnected Mode，DM）帧。

（2）数据传输

当初始化已被请求和接收后，就建立起逻辑连接。两方都可开始用 I 帧发送用户数据，该 I 帧的序列号从 0 开始。I 帧中 N（S）和 N（R）字段存放的序列号用于支持流控制和差错控制。HDLC 装置在连续发送 I 帧序列时，给这些帧按序编号，并依据采用的是 3 比特还是 7 比特序列号，将这些序列号值进行模 8 或模 128 运算，然后将所得的序列号存放于 N（S）。N（R）是对所接收 I 帧的确认，通过该字段，HDLC 装置能指明其所希望接收的下一

个 I 帧的序列号。

S 帧也用于流控制和差错控制中。接收就绪（RR）帧用来确认最后接收到的 I 帧，同时指明所期望接收的下一个 I 帧。当没有反向的用户数据流（I 帧）来捎带确认时，就需要使用 RR 帧。接收未就绪（RNR）与 RR 帧一样，确认一个 I 帧，但也告知对方实体暂停 I 帧的发送。当发送 RNR 帧的实体准备就绪时，它就发送一个 RR 帧。REJ 帧代表了一个回退 N（go-back-N）的 ARQ，表明拒绝最后接收到的 I 帧，并且要求重传序列号从 N（R）开始的所有 I 帧。选择拒绝（SREJ）用于要求重传单个 I 帧。

（3）断开连接

两个 HDLC 装置中的任一个可以发起断开连接请求，可能是由于出现某种错误而主动发起请求，或应高层用户的要求而发起请求。HDLC 通过发送断开连接（DISC）帧来发起断开连接请求，另一方必须通过回复 UA 帧接收该断开连接请求。

（4）操作例子

为了更好地理解 HDLC 的操作，图 6-13 给出了一些操作例子。在示例的操作图中，每个箭头包含一些文字来说明帧的类型、P/F 位的设置，以及在适当的时候给出 N（R）和 N（S）值。当给 P/F 位赋值时，就将 P/F 位设置为 1，如果没赋值，则设置为 0。

图 6-13a 给出了连接建立和断开连接时的一些帧。通信一方的 HDLC 实体向另一方发起 SARM 命令，并启动一个计时器。另一方在接收到 SARM[⊖]时，返回一个 UA 应答，设置本地变量和计数器为其初始值。发起方接收到该 UA 应答后，也设置自己的变量和计数器，并停止计时器。这样逻辑连接就建立起来了，双方都可开始传输帧。如果在收到应答之前计时器时间到，那么发起方就重发 SARM，如图中所示。该过程将一直重复直至收到 UA 或 DM，或者在重试给定的次数之后，发起初始化的实体放弃该初始化过程，并将错误报告给管理实体。在这种情况下，需要更高层次的干预。同一图（见图 16-3a）中也展示了断开连接的过程。通信的一方发送一个 DISC 命令，通信的另一方用 UA 应答来回答。

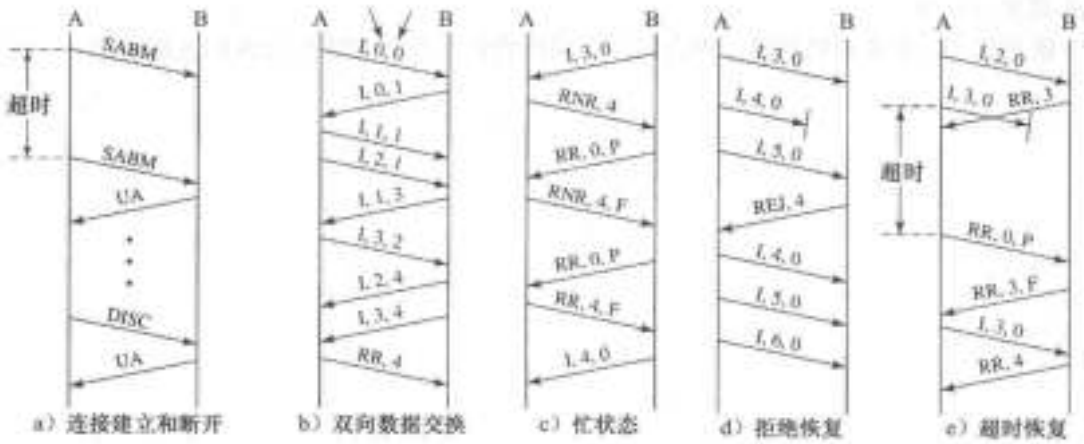


图 6-13　HDLC 操作示例

图 6.13b 展示了 I 帧的全双工交换过程。当一通信实体在输入数据的情况下接连发送一批 I 帧，那么接收序列号 N（R）是简单重复的（例如从 A 到 B 方向的 I，1，1；I，2，1）。

⊖ 这代表设置异步平衡方式。SABM 命令请求开始交换。首字母缩略词中的 ABM 部分表示的是传输方式，其中的细节我们不必考虑。

当一通信实体在没有输出帧的情况下接连接收一批I帧，在下一个输出帧中的接收序列号必须反映出这样的累积活动（如从B到A方向的I，1，3）。注意，除I帧外，数据交换也涉及监控帧。

图6.13c给出了繁忙情况下的操作。出现这种情况是因为HDLC实体不能以I帧的到达速率来处理这些帧，或者目的端用户不能以封装在I帧中的数据到达的速率来接收这些数据。不管对应哪种情况，通信实体中的接收缓冲区将会填满，并且它必需通过使用RNR命令来暂停输入的I帧流。在这个例子中，站点A发送一条RNR命令来要求另一端暂停发送I帧。接收到RNR的站点通常发送设置P位的RR命令，来周期性地探询该繁忙站点，这要求另一端通过RR命令或RNR命令来应答。如果站点A的繁忙情况清除了，则返回RR命令，这样从站点B发送I帧的过程就可重新开始了。

图6.13d给出了一个利用REJ命令进行错误恢复的例子。在该例中，站点A发送序号为3、4、5的I帧。其中帧4中出现了错误，站点B检测到了这个错误，并且丢弃了该帧。当站点B接收到I帧5时，由于该帧是乱序的，就丢弃该帧并发送一N（R）为4的REJ。这就导致了站点A重传自帧4开始的所有帧。在这些重传帧之后，站点A还可能继续发送后继的帧。

图6.13e展示了利用超时实现错误恢复的例子。在该例中，站点A发送I帧3，该帧为一个I帧序列的末尾。该帧在传输过程中出错，站点B检测到该错误，并且丢弃该帧。然而站点B不能发送REJ，这是因为站点B无法知道该帧是否是一个I帧。如果在一个帧中检测到错误，那么该帧中所有的比特都是不可信的，这样接收方就不能对其采取措施。但是站点A在发送一帧时就启动一个计时器，该计时器所设置的时间足够长，能跨越所期望的应答时间。当计时器时间到时，站点A启动恢复过程，这通常通过发送设置P位的RR命令以探询另一端来实现，这样就能确定出另一端的状态。由于探询要求对方应答，该实体将会收到包含N（R）字段的应答帧，这样通信就能继续下去。在该例中，应答指明了帧3的丢失，这样站点A就重传该帧。

这些例子不是面面俱到的，但它们可以给读者留下有关HDLC行为的直观印象。

第三部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

因特网和分布式应用

第 7 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

因 特 网

学习目标

通过本章的学习，读者应该能够：

- 讨论因特网的历史并解释其迅速的发展。
- 描述因特网结构及它的关键组成部分，包括 ISP、POP 和 IXP。
- 解释因特网域和域名。
- 讨论域名系统的操作。

7.1 因特网结构

7.1.1 商业和因特网

因特网是大多数企业网络的核心组成部分，它的公共可用设施、应用程序和协议被广泛应用于商业活动的各个领域。复杂的组织间供应链管理（SCM）系统通常由因特网部署，而外部网通常用于与客户、供应商和其他商业伙伴进行业务联系。当企业资源计划（ERP）和其他企业系统接入因特网时，它们成为了全球性的商业软件平台。不同规模的业务使用因特网作为电子商务平台来销售产品和提供服务，同时因特网市场也已成为广告的常规战场。

很难捉摸不使用因特网的商业会变得怎样不同。大多数商业策略都会考虑如何更好地利用因特网来提高业务流程，而不是弃之不用。对大多数公司来说，没有因特网的生活是不可行的，因为不掌握因特网的基础概念，理解企业网络中的业务数据通信将变得十分困难。

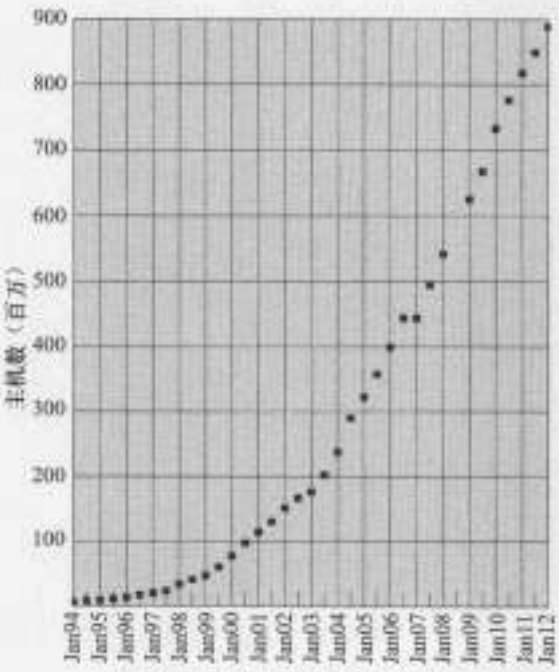


图 7-1 因特网域名调查主机数

来源：因特网软件协会（http://www.isc.org）

7.1.2 因特网起源

因特网的发展源于 ARPANET，这是由美国国防部高级研究计划署（Advanced Research Projects Agency，ARPA） 在 1969 年研制的项目。这是第一个分组交换网络。ARPANET 起初在 4 个地点运行。如今的主机数量数以亿计，用户数量数以 10 亿计，参与的国家数量大约是 250 个。而因特网的连接数将继续成倍增长（见图 7-1）。

ARPANET 采用新的分组交换技术，并

提供了电路交换的优点，这两点在 1.8 节已简要介绍过，本节还将继续讨论。

该网络十分的成功，以至于 ARPA 将同样的分组交换技术应用到战略无线电通信（无线分组）和卫星通信（SATNET）中。由于 3 个网络是在不同的通信环境中运行，所以某些参数（如最大分组大小）的适当值在每一种情况下是不同的。面对这些网络整合的难题，ARPA 的 Vint Cerf 和 Bob Kahn 着手开发网络互联（internetworking）的协议和方法——可以跨越任意多个分组交换网络进行通信。1974 年 5 月，他们发表了一篇非常有影响力的论文 [CERF74]，该论文概述了他们对传输控制协议（TCP）的研究方法。该提案经过提炼后，由 ARPANET 补充了细节，欧洲网络的参与者也提供了巨大的贡献，这些贡献最终成就了 TCP 和 IP 协议，并成为了 TCP/IP 协议族的基础，也成为了因特网的基石。

联邦网络局（后来并入美国政府网络和信息技术的研究与发展 [NITRD] 计划）给出因特网的定义如下：

> 指代全球信息系统的因特网是指：
>
> 1）是逻辑联系在一起的一个全球唯一的地址空间，它基于因特网协议（IP）或其后续的扩展 / 附加协议。
>
> 2）能够支持使用传输控制协议 / 因特网协议（TCP/IP）族或后续扩展 / 附加协议以及其他兼容 IP 协议的通信。
>
> 3）在这里所描述的通信及相关的基础设施上公开或秘密地提供、使用或访问高水平的服务。

7.1.3 分组交换的使用

传统上，电子通信的两个基本模式为电路交换（本质上是语音通信，请参见第 15 章）和报文交换（电报和电传）。在**电路交换**中（见图 7-2），当源 S 与目标 T 通过网络通信时，传输设备建立一个专门的路径（例如 S、A、C、E、T）连接 S 到 T。在一个“呼叫”的持续时间内，所有的设备处于工作状态。特别地，如果会话中发生间歇，这期间传输路径将保持闲置。另一方面，在连接建立后，网络的延迟将达到最小。除此之外，一旦“呼叫”建立，网络基本上可以说是被动的。而另一个优点则是，分组交换往往是机电的。

在**报文交换**（见图 7-2）中，从 S 到 T 发送一条报文分为多个阶段。首先，S 到 A 的传输设备开始使用，报文从 S 传送到 A，并在 A 中暂时存储。传输完毕后，S 到 A 的信道被释放。接着 A 到 C 的信道开始使用，报文传送到 C，以此类推。在这种情况下，传输信道只在需要的时候使用，在不需要的时候不会被浪费。虽然传输比较有效率，但与之伴随的问题是大量且多变的延时。报文在每个中间节点被频繁地存储在慢速设



图 7-2 电路交换与报文交换

备上，如磁盘、磁鼓，更早期的时候还有打孔纸带。这些外设十分缓慢。此外，每条报文发送的时间等于报文的长度除以信道的数据速率。一条很长的报文会在每个节点产生相当长的延时。在从源节点到目的节点的传输路径上，每一个节点都会产生类似的延时。因此，传输导致的延迟会在很大的范围内波动，由报文的长度和传输路径上的节点个数决定。

分组交换是一个特殊的报文交换，但它有许多不同的属性。首先，分组交换的传输单元长度有限制。如果一条报文的长度大于最大的分组大小，报文会被拆分成几个分组进行传输。其次，当分组传送到每个新节点时，它存储在高速随机存取存储器（RAM）中，而不是在较慢的外设（在报文交换系统中使用）中。与报文交换相比，分组交换有一个明显的优势，即延时的大幅缩短。第一个分组的到达延时是第一个分组的传输时间乘以路径上节点的个数。后续的分组紧接着第一个分组立即传输。如果使用高速信道，分组横跨美国的延时也仅仅是几百毫秒。ARPANET 使用 50Kbps 的链路。因此对一个有 5 个节点或更少节点的路径来说，一条少于 1000 字节长度的分组的传输时间少于（1000 × 8）/50 000=0.165。同时，信道的使用效率与报文交换的效率相等。

当电路交换用于数据传输时，发送装置和接收装置的数据传输速率必须是相同的。当进行分组交换时，就没有必要保持相同速率了。分组可以以发送装置的数据传输速率发送到网络中；在网络中以各种不同速率进行传播，通常会高于发送装置的速率；然后再检测出接收装置所要求的数据速率。分组交换网络及其接口可以缓冲备份数据，可以使较高速率变为较低速率。在 ARPANET 网络发明初期，数据速率不统一不是互联的全部难题，缺少完整的开放通信标准才使得不同制造商制造的计算机间电子通信困难。因此，ARPANET 的一个关键贡献是它推动了通信和应用协议标准化的发展，这一点将在之后讨论。另一件令 ARPANET 军事赞助商感兴趣的事是，它还提供自适应路由。每一个分组，在路由到终点的路径上，都会独自选择较快的传输路由。因此，如果部分网络因为故障而阻塞，分组就会自动选择绕开障碍的路由器。

一些早期为 ARPANET 开发的应用程序也提供了新的功能。最初两个重要的应用是 Telnet 和文件传输协议（FTP）。Telnet 为远程计算机终端提供了一个通用的语言。在 ARPANET 引入时，每个计算机系统支持不同的终端。Telnet 应用提供了一个共同终端。假设为每种类型的计算机分别编写软件来支持“Telnet 终端”，那么每个终端都可以与其余计算机类型交互。FTP 提供了一个类似的开放功能。FTP 允许文件通过网络从一台计算机到另一台计算机透明地传输。这不是听起来那么容易的，因为不同的计算机有不同的文字大小，并且它们存储的位顺序和使用的文字格式也不相同。然而，ARPANET 的第一个“杀手级应用”是电子邮箱。ARPANET 之前有电子邮件系统，但它们都是单台计算机系统。1972 年，Bolt Beranek and Newman（BBN）公司的 Ray Tomlinson 编写了第一个分布式的邮件服务系统，为使用多台计算机的计算机网络提供分布式邮件服务。到 1973 年，ARPA 的研究发现，3/4 的 ARPANET 流量源自电子邮件 [HAFN96]。

7.1.4　关键要素

图 7-3 说明了组成因特网的关键要素。因特网的目的，当然是终端系统（称为**主机**）互连，包括个人计算机、工作站、服务器和大型计算机系统等。大多数主机使用因特网连接到**网络**，如 LAN 或广域网（WAN）。这些网络再通过**路由器**相互连接，每个路由器连接两个或多个网络。有些主机，如大型机或服务器，直接连接到路由器，而不通过网络。



图 7-3 因特网的关键元素

在本质上，因特网的运行方式如下所述。主机可以发送数据到因特网上的任何主机上。源主机将数据分为待发送的有序分组，这些分组称为 **IP 数据报**或 **IP 分组**。每个分组包括一个独有的目的主机数字地址。该地址本文称为 **IP 地址**，因为该地址包含在每个 IP 分组中。基于这个目的地址，每个分组通过一系列的路由器和网络从源点传送到目的点。路由器每收到一个分组，就进行路由选择并将分组沿着路线转发到目的地址。我们将在第 8 章对此进行更多的说明。

7.1.5 万维网

1989 年的春天，在欧洲粒子物理研究所（CERN），TimBerner-Lee 提出了有关分布式超媒体技术的想法，旨在利用因特网促进国际间的研究成果交流。两年后，利用 NeXT 计算机作为平台，欧洲粒子物理研究所开发了万维网（WWW 或 Web）的原型。到 1991 年年底，它发布了一个面向行的浏览器或阅读器提供给有限的受众使用。该技术爆炸性增长的同时，第一个图形化浏览器应运而生，Mosaic，于 1993 年由伊利诺伊大学 NCSA 中心的 Mark Andreessen 和其他人员共同开发完成。因特网交付了超过 200 万份的 Mosaic 浏览器副本。今天，具有代表性的 Web 地址 URL（统一资源定位符）无处不在，一个人无论是看报纸还是看电视都会看到这些网络地址。

Web 是一个国际分布式多媒体文件收集系统，它由客户端（用户）和服务器（信息提供者）支持。每一个文件用统一的方式使用 URL 命名。通过使用客户端浏览器可以查看供应商的文件，如 Firefox 或微软的 IE。大多数浏览器都有图形显示器且支持多媒体——文字、声音、图像和视频。用户可以通过使用鼠标或其他指针设备，单击浏览器上显示高亮的文字或图像元素来查阅不同的文件。从一个文件到另一个文件的跳转称为超链接。浏览器显示的布局由超文本标记语言（HTML）标准控制，它定义了在文本文件中嵌入的命令，指定浏览器显示的特征，例如字体、颜色、图像，和它们安置在显示屏上的位置，以及用户可以调用超链接和他们目标的区域定位。网络的另一个重要特性是超文本传输协议（HTTP），它是一种通信协议，用于在 TCP/IP 网络中从超链接所指定的服务器上获取文件。

7.1.6　因特网架构

如今的因特网是由数以千计重叠的分层网络组成的。因此，想要对因特网的拓扑或结构进行详尽描述是不现实的。但是，对其通用的、大致的特性进行概述是可行的。图 7-4 给出示例，表 7-1 总结术语。

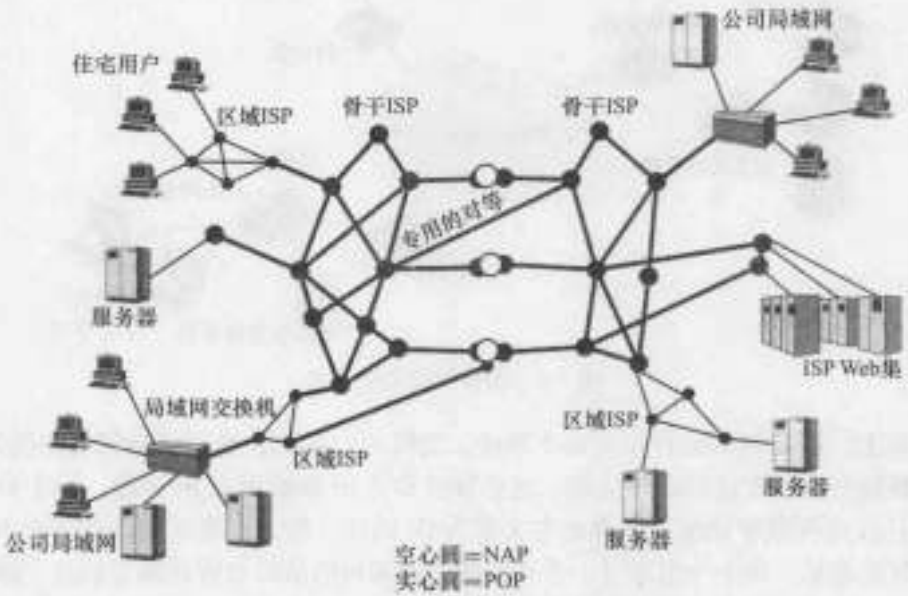


图 7-4　因特网的部分简化视图

表 7-1　因特网术语

中心局（CO） 电话公司端接客户线路的地方，并在那里放置与其他网络互连的交换设备
用户驻地设备（CPE） 位于用户驻地（物理位置）的电信设备，而不是位于供应商驻地或两者之间。手机、调制解调器、有线电视机顶盒、数字用户线路由器都是例子。从历史上看，这个术语指放置在电话线上客户终端的设备，并通常是电话公司拥有的设备。今天，几乎所有的终端用户设备均可称为用户驻地设备，并且可以由客户或供应商拥有
因特网服务供应商（ISP） 向其他公司或个人提供访问因特网服务的公司。ISP 拥有为当地提供接入因特网服务所需的设备和电信线路的使用权限。大型 ISP 公司拥有自己的高速专用线，这样他们不太依靠电信供应商并能提供更好的服务
因特网交换点（IXP） 因特网几个重要的互连点之一，用于将所有的 ISP 连接起来。IXP 通常提供主要的交换设备为大众服务。公司利用 IXP 设施。绝大多数的因特网流量不经由 LXP 处理，而是使用对等安排和同地理区域间的网络互连
网络服务供应商（NSP） 为 ISP 提供骨干网服务的公司。通常，ISP 连接 IXP 到一个区域 ISP，又依次连接到 NSP 骨干
接入点（POP） 收集电信设备的站点，通常指 ISP 或电话公司的站点。一个 ISP 接入点是指 ISP 网络的边界，用户发起的连接要在这里被接受和认证。因特网访问提供者会把多个接入点分散开，以提高用户使用当地电话访问因特网的概率。最大的国有 ISP 在全国各地都拥有接入点

因特网的一个关键要素是连接到它的主机。简单地说，主机是一台计算机。如今，计算机有多种形式，包括移动电话，甚至汽车，所有这些形式都可以成为因特网的主机。主机有时会组合在一起形成一个局域网，这是企业环境中常见的配置。个人主机和局域网通过接入

点（POP）连接到**因特网服务提供商**（ISP），该连接由初始于**用户驻地设备**（CPE）的一系列步骤完成。CPE 是在现场与主机通信的设备。

对于许多住宅用户来说，CPE 是传统的 56Kbps 的调制解调器。这种设备对访问电子邮件及相关服务来说足够了，但只能勉强应付图形密集的网上冲浪。在某些情况下，今天的 CPE 产品提供了更大的容量和服务保证，例如 DSL、电缆调制解调器、地面无线设备和卫星。在工作中，用户通常通过工作站或 PC 连接到因特网，这些工作站和 PC 连接到雇主持有的局域网，局域网又依次通过共享的企业主干网络连接到 ISP。在这些情况下，共享电路往往是 T-1 连接（1.544Mbps），而对大规模的企业来说，有时也会使用 T-3 连接（44.736Mbps）。有时，企业的局域网会挂接在一个广域网中，如帧中继网络，该网络会依次连接到 ISP。

CPE 物理上连接到“本地回路”或“最后一公里”。它是一个位于供应者安装地和主机驻地之间的基础设施。例如，将一个家庭用户的 56-K 调制解调器连接到电话线路上。电话线通常是一对铜线，从房屋到达由电话公司所有和运营的**中心局**（CO）。在这种情况下，本地回路就是从房屋到 CO 的一对铜线。如果家庭用户有电缆调制解调器，那么本地回路就是从家到电缆公司设施的同轴电缆。前述的例子有一点儿简单，但它们足以适用这个讨论。许多情况下，从一个用户家庭输出的电线会与其他家庭的电线聚合在一起，然后转化成一种不同的介质，如光纤。在这种情况下，本地回路依然是指从家庭连接到中心局或电缆设备的路径。本地回路供应者并不一定是 ISP，很多时候是电话公司，而 ISP 则是全国性的大型服务机构。但通常情况下，本地环路的供应者也是 ISP。

CPE-ISP 连接的其他形式不经过电话公司中心局。例如，电缆链路连接本地用户到电缆公司网站，其中包含或连接到一个 ISP。移动用户可以利用 Wi-Fi 的无线连接获得因特网访问服务。企业介入到 ISP 可通过专用的高速链路或通过 WAN，如异步传输模式（ATM）中或帧中继网络。

ISP 通过接入点（POP）提供更大网络的访问。接入点是一个简单的设备，用户可以通过它连接到 ISP 网络。有时，这种设备由 ISP 持有，但大多数情况下，ISP 从本地回路租用空间。一个接入点可以简单地视作调制解调器的银行和安装在中心局（CO）机架的访问服务器。接入点常常在提供服务的地理范围上散布于各地。ISP 作为一个因特网网关，提供了重要的服务。对许多家庭用户来说，ISP 提供了独一无二的数字 IP 地址，用来与因特网的其他主机通信。大多数 ISP 也提供域名解析和其他重要的服务。最重要的服务是连接到其他不同的 ISP 网络。供应商之间通过形式化的对等协议促进了访问服务。物理访问，可以通过连接不同 ISP 的接入点来实现。如果接入点合并，可以通过本地连接实现，当接入点没合并时，可通过租用线路实现。另一种更加常用的机制是**因特网交换点**（IXP）。

IXP 是一种物理设备，它使得两个互连的网络之间可以数据移动。如今，大多数 IXP 都有 ATM 或千兆以太网核心。连接到 IXP 的网络由**网络服务供应商**（NSP）所有和运营。NSP 同样可以作为一个 ISP，但也并非一直如此。对等协议存在于网络服务供应商之间，而且它并没有包括网络访问接入点（NAP）经营者。网络服务供应商将路由器安装在网络访问接入点，并将它们连接到网络访问接入点的基础设施上。网络服务供应商的设备负责路由，IXP 设备提供路由器之间的物理访问路径。在写本书时，有 357 个 IXP 在 91 个国家运行，其中有 85 个位于美国。最新列表保存在 Packet Clearing House（https://prefix.pch.net/applications/ixpdir）。

虽然目前对因特网来说还没有官方的、严格的组织结构，但它通常被视为涵盖了 3 层（见图 7-5），定义如下：

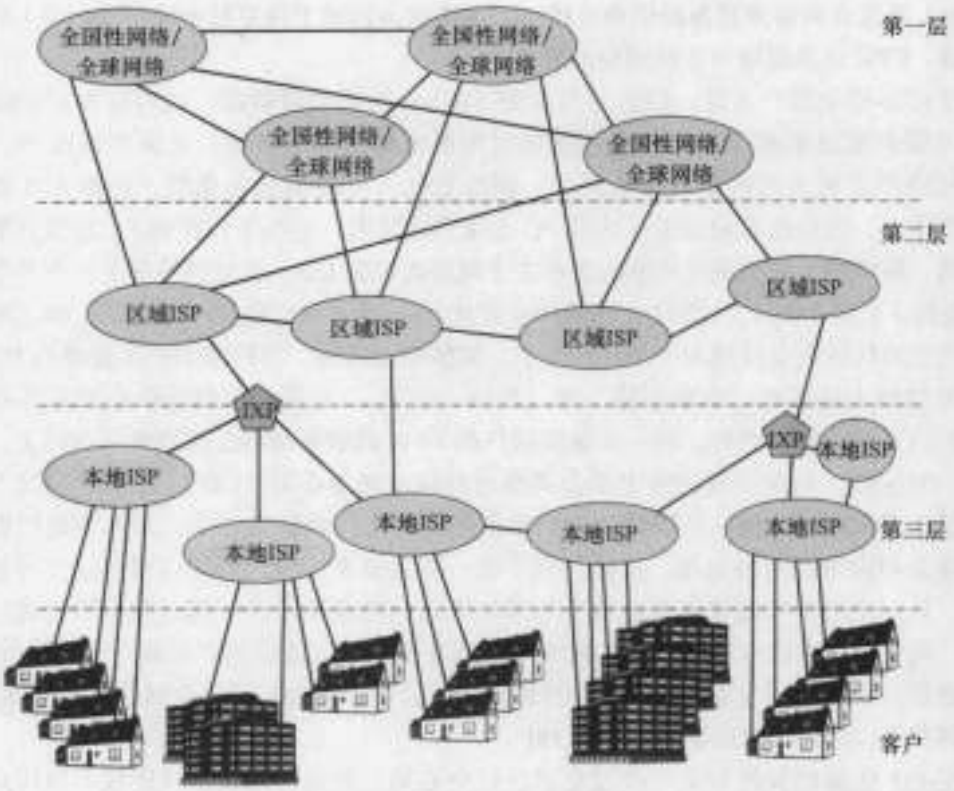


图 7-5　因特网的组织结构

- **第一层**：第一层网络是因特网的顶层网络。有大约十几个第一层网络，其中大部分在美国，包括 AT&T、Global Crossing、Level 3、Qwest、Sprint 和 Verizon（原来的 UUNET）。称为免费对等（settlement-free peering），因为第一层网络是私有网络，它允许从其他第一层网络传输流量到骨干网而不收取费用。第一层网络可以到达因特网中其他任意网络，而不必购买 IP 转接和付费。
- **第二层**：第二层网络在与其他网络对等不收费，但接入大部分因特网时需要付费。通常，第二层网络支付一定的费用给第一层网络以便接入它无法直接访问或无法通过对等网络安排访问的那部分因特网。
- **第三层**：第三层网络总是需要支付费用来通过第二层网络获得更大的主干网络。

我们可以认为第一层网络组成了因特网的主干，通过第一层网络可以访问整个因特网的路由表，这样，就可以知道如何直接访问其他因特网网络。有这样一个概念，其粗略等价于第一层网络和网络服务供应商，虽然没有任何正式的关于两者的定义。第二层网络是局部的 ISP 网络，通常由电信运营商提供。第三层网络提供的仅仅是本地接入点和面向本地住宅及商业客户的服务。

7.2　域

7.2.1　因特网的名称和地址

回忆 7.1 节，数据以分组的形式通过因特网，每一个分组包括一个数字化的目的地址，

这些地址由32位二进制数组成。这个32位的IP地址可以唯一地识别连接到因特网上的设备。该地址可以分成两个部分：网络号，用于识别因特网中的网络；主机地址，用于识别网络中独一无二的主机。使用IP地址带来了两个问题：

1）路由器基于网络号计算通过因特网的路径。如果每个路由器都需要维护一张列出每一个网络和优化路径的主表，那么管理表格将会变得十分麻烦，也很费时间。将网络以某种方式分组以简化路由函数将会更好。

2）32位地址通常写为4个十进制数，与4个8位组对应。这种数字方案对于计算机处理来说很有效，但对于用户来说名字比数字好记得多。

这些问题由两个概念分别解决，那就是**域**和**域名**的使用。总的来说，域是指一群主机处于一个单独个体的管理控制下，如一个公司或政府机构。域是分层的，因此一个给定的域很可能由许多下级的域组成。域名被指定给域，并反映它的分层组织结构。

图7-6展示了部分的域名树。树的顶端是少数的域，它们共同组成了整个因特网。表7-2列举了目前定义的顶层域，这些顶层域由因特网数字分配机构（IANA）分配。每一个下级命名是在其上级域名前添加前缀名。例如，

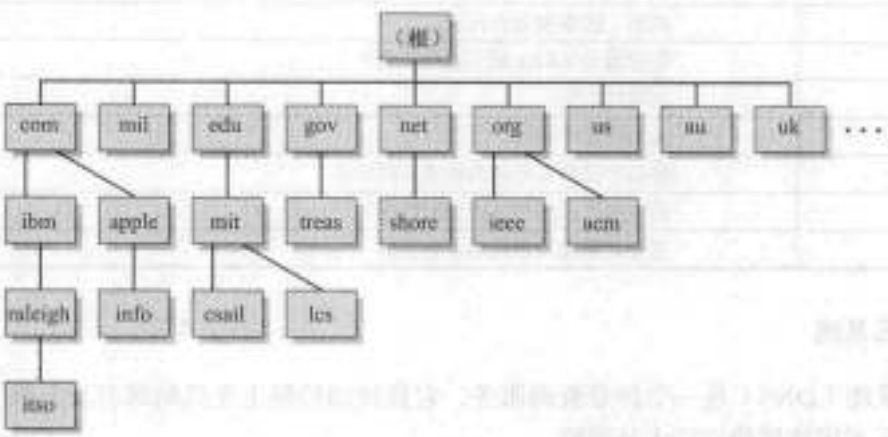


图7-6 部分因特网域名树

- edu是学校级教育机构的域名。
- mit.edu是麻省理工大学（MIT）的域名。
- csail.mit.edu是麻省理工大学计算机与人工智能实验室（Computer Scienceand Artificial Intelligence Laboratory）的域名。

当你沿着域名树往下，你会最终得到一个标识因特网中特定主机的叶子节点。这些主机都被分配了因特网地址。域名按照分层模式分配，这样每一个域名都是独一无二的。在树的最顶层，新建顶级域名和分配域名及地址由因特网名称与数字地址分配机构（ICANN）管理。实际的地址分配是按分层授权下放的，因此mil域分配给了许多地址。美国国防部（DoD）将部分地址空间分配给不同的国防部组织，最终分配到每一个主机上。

例如，MIT的主服务器，域名为mit.edu，IP地址为18.7.22.69。下级域csail.mit.edu的IP地址为128.30.2.121[⊖]。

⊖ 通过将Web浏览器连接到ISP，可以演示说明域名/IP地址的功能。ISP应提供ping或nslookup工具，允许输入域名，获得IP地址的功能。而且，用户操作系统中都有这样的典型工具。

表 7-2　一些因特网顶级域名

域　名	内　容
com	商业组织
edu	教育机构
gov	美国联邦政府机构
mil	美国军事
net	网络支持中心、因特网服务提供者和其他与网络相关的机构
org	非盈利组织
us	美国州以及地方政府机构、学校、图书馆、博物馆
国家代码	ISO 标准双字母标识符，用于不同国别的域名识别（如 au、ca、uk）
biz	专用于私人企业
info	没有限制用途
name	个人，用于电子邮件地址和私人域名
museum	仅限于博物馆、博物馆组织和博物馆职员
coop	成员拥有的合作性组织，如信用合作社
aero	航空团体
pro	医药、法律和会计行业
arpa	暂时属于 ARPA 域（目前仍属于）
int	国际化组织
jobs	人力资源管理局
mobi	移动产品和服务的消费者和供应商
tel	商业和个人用于发表合同数据
travel	主要从事领域是旅游业的实体

7.2.2　域名系统

域名系统（DNS）是一个目录查询服务，它提供因特网上主机的域名及其数字地址间的映射。DNS 对因特网的运行十分重要。

DNS 的 4 个元素如下：

- **域名空间**：DNS 运用树形结构的命名空间来标识因特网上的资源。
- **DNS 数据库**：理论上说，每个节点和叶子节点都在命名空间树形结构中列出了一系列信息（如 IP 地址、为该域名命名的服务器）包含在资源记录（RR）中。所有的 RR 集合都进行了有序组织并存放在分布式数据库中。
- **名称服务器**：服务器程序保存有关部分命名树的结构以及相关的资源记录。
- **解析器**：将信息从名称服务器中提取出来以便响应客户请求的程序。一个典型的客户请求发送至一个与指定域名相对应的 IP 地址。

我们已经了解了域名。DNS 剩余的元素会在后面进行讨论。

1. DNS 数据库

DNS 数据库基于分层数据库，其中包含**资源记录**（Resource Record，RR）。资源记录包括域名、IP 地址以及其他有关主机的信息。DNS 数据库的关键特点如下：

- **多种深度分层的域名**：如前面所述，DNS 允许无限的分层，并在可打印域名中使用点号（.）作为层级分隔符。
- **分布式数据库**：数据库存放在 DNS 服务器中并散布在整个因特网中。

- **数据库分布式控制**：DNS 数据库被划分成数以千计的分散的管理区，每个区由分散的管理者管理。分布和更新记录由数据库软件进行操作。

DNS 服务器运用这种数据库为需要定位特定服务器的网络应用提供了“域名 - 地址”的目录服务。比如，当一封电子邮件被发送或一个网页被访问时，DNS 域名查询必须决定电子邮件服务器或网页服务器的 IP 地址。

2. DNS 操作

DNS 操作通常包括以下几个步骤（见图 7-7）：

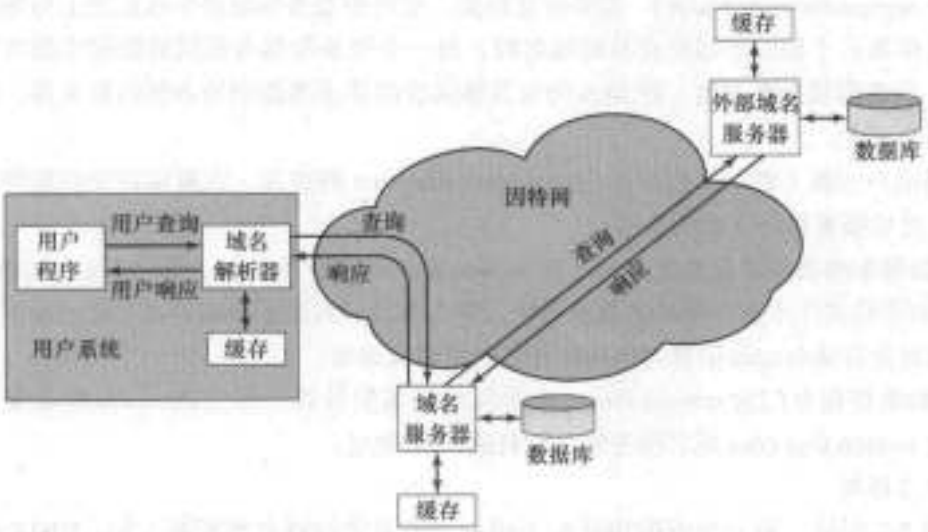


图 7-7 DNS 域名解析

1）用户程序发起对某域名的 IP 地址请求。

2）本地主机或本地 ISP 上的解析器模块查询在同一域中作为解析器的本地域名服务器。

3）本地域名服务器首先检查此域名是否存在于本地数据库或缓存（cache）中。如果存在，就返回对应的 IP 地址；如果不存在，域名服务器就会查询其他可用的域名服务器，如果必要就会访问根服务器，这点之后会做介绍。

4）当本地域名服务器接收到响应时，它将域名或地址映射存储在本地缓存中，并将此条目保存一段时间，时间的长短由 RR 中的生存时间（TimetoLive）指定。

5）用户程序将获得 IP 地址或一条错误信息。

为了支持 DNS 的功能，分布式 DNS 数据库必须频繁地更新，以适应快速、持续增长的因特网。同时，DNS 必须处理 IP 地址的动态分配，如已由 ISP 分配的家庭 DSL 用户。相应地，DNS 的动态更新功能就定义好了。事实上，DNS 域名服务器会在条件允许时自动地向其他相关的域名服务器发送更新。

3. 服务器分层

DNS 数据库是分布式分层的，它存在于因特网上散布的 DNS 域名服务器中。域名服务器可以由拥有域名的组织运营，即任何拥有分层域名空间子树的组织。每一个域名服务器配置了一个域名空间的子集，称作区（zome），区是域内一个或多个（全部）子域的集合，与资源记录（RR）相关。这个数据集是权威的，因为该域名服务器负责为此部分域名空间维护

一套准确的资源记录。分层结构实际上可以扩展至任何深度，因此，部分指派给权威域名服务器的域名空间可以委托给下级域名服务器，通过一种与域名树结构保持一致的方式。例如，一个域名服务器对域 ibm.com 是权威的。部分域由域名 watson.ibm.com 定义，其与 watson.ibm.com 节点及所有 watson.ibm.com 下面的分支和叶子节点保持一致。

在服务器分层的顶层是 13 个**根域名服务器**，它们共同负责顶级区（见表 7-3）。这种复用是为了运行的稳定性以及防止根服务器成为瓶颈。即使如此，每一个单独的根服务器依然繁忙。例如，因特网软件联盟报告，其服务器（F）每天应答超过 3000 万次 DNS 请求（www.isc.org/community/f-root）。需要注意的是，有些根服务器由多个在地理上分布的服务器组成。当存在多个根服务器享有共同域名时，每一个服务器都有相同的数据库副本和相同的 IP 地址。当查询根服务器时，IP 路由协议及算法会将请求连接到最方便的服务器，通常是地理上最近的那个。

试想用户主机上的一个程序发出对 watson.ibm.com 的查询，该查询首先发送到本地域名服务器，然后接着执行下面的步骤：

1）如果本地服务器在其缓存中已有 watson.ibm.com 的 IP 地址，则将其返回给用户。

2）如果域名并不在本地域名服务器中，那么本地域名服务器将请求发送到根服务器。根服务器返回含有 ibm.com 信息的域名服务器的域名及地址。

3）如果存在专门为 watson.ibm.com 委派的域名服务器，那么 ibm.com 域名服务器将转发请求给 watson.ibm.com 域名服务器，它将返回 IP 地址。

4. 域名解析

如图 7-7 所示，每一个查询均开始于用户主机系统的域名解析器（如，UNIX 系统中的 gethostbyname），每一个解析器配置后可以给出本地域名服务器的 IP 地址。如果解析器在缓存中没有被请求的域名，它会发送一个 DNS 查询到本地域名服务器，本地域名服务器要么立即返回地址，要么在重复查询其他服务器后返回地址。

有两种转发请求和返回结果的方式。假设一个解析器向本地服务器 A 发出一个请求，如果 A 在本地缓存或本地数据库中存有域名或地址，那么它会将 IP 地址返回给解析器。如果不存在，那么服务器 A 将执行下面步骤之一：

1）询问另一个域名服务器，并将结果返回给解析器。这种方式称为**递归**技术。

2）将下一个即将请求的服务器 B 的地址返回给解析器。然后，解析器向 B 发出新的 DNS 请求。这种方式称为**迭代**技术。

表 7-3　因特网根服务器

服务器	运营者	地　址	IP 地址
A	VeriSign Global Registry Services（VeriSign 全球注册服务）	美国、德国、香港等 6 地	IPv4：198.41.0.4 IPv6：2001：5.3：BA3E：：2：30
B	Information Sciences Institute（信息科学研究所）	Marina DelRey、CA、USA	IPv4：192.228.79.201 IPv6：2001：478：65：：53
C	Cogent Communications（康茵通信）	美国、德国、西班牙等 6 地	192.33.4.12
D	马里兰大学	College Park、MD、USA	IPv4：128.8.10.90 IPv6：2001：500：2D：：D
E	美国宇航局艾姆斯研究中心	Mountain View、CA、USA	192.203.230.10

（续）

服务器	运营者	地　址	IP 地址
F	因特网软件联盟	美国和其他国家等 49 地	IPv4：192.5.5.241 IPv6：2001：500：2f：：f
G	美国国防部网络信息中心	美国、德国、意大利等 6 地	192.112.36.4
H	美国陆军研究实验室	Aberdeen、MD、USA San Diego、CA、USA	IPv4：128.63.2.53 IPv6：2001：500：1：：803f：235
I	Netnod	美国和其他国家等 38 地	IPv4：192.36.148.17 IPv6：2001：7fe：：53
J	VeriSign Global Registry Services(VeriSign 全球注册服务）	美国和其他国家等 70 地	IPv4：192.58.128.30 IPv6：2001：503：C27：2：：30
K	RESEAUX IP EUROPEENS——网络协调中心	美国和其他国家等 18 地	IPv4：193.0.14.129 IPv6：2001：7fd：：1
L	国际因特网名称和编号分配机构	美国和其他国家等 55 地	IPv4：199.7.83.42 IPv6：2001：500：3：：42
M	WIDE 项目	美国、日本、韩国、法国等 6 地	IPv4：202.12.27.33 IPv6：2001：dc3：：35

7.3 动态主机配置协议

动态主机配置协议（DHCP）是一个因特网协议，该协议在 RFC 2131 中定义，它实现了主机 IP 地址的动态分配。

DHCP 用来处理 IP 地址的缺陷，而这个缺陷需要大规模地将 IP 地址转换为更长的 IPv6 地址才能得以解决。DHCP 使本地网络（如企业网络）可以从可用的 IP 地址池中选择并分配 IP 地址到正在使用的主机上。当主机不再使用时，被分配的 IP 地址就会返还给由 DHCP 服务器控制的 IP 地址池。

即使 IP 地址没有缺陷，对移动系统环境来说 DHCP 依然非常有用，如笔记本电脑和平板电脑，这些系统通常会在不同网络中移动，并且它们只是零星地使用网络。DHCP 还可以为特定系统（如服务器）指派永久的 IP 地址，这样当系统重启时依然可以保有同一个地址。

DHCP 的运行基于客户机 / 服务端模型，每一个主机在启动后都扮演着需求 IP 地址的客户机，DHCP 服务器则提供所请求的 IP 地址和相关的配置参数（见图 7-8）。配置参数涵盖默认路由器的网络地址，该路由器用于与本地网络外部联系，同时还涵盖本地 DNS 服务器的地址。

下面的 DHCP 信息用于协议操作：

- DHCPDISCOVER：客户端广播定位可用的服务器。
- DHCPOFFER：服务器发送给客户端的消息，以便响应 DHCPDISCOVER 并提供配置参数。
- DHCPREQUEST：客户端发送给服务器的消息，包括：（a）请求某个服务器提供的参数，并隐性地拒绝其他服务器提供的参数；（b）确认已经分配的地址的正确性，例如在系统重启后；（c）对某个特定网络地址续租。
- DHCPACK：服务器发送给客户端的配置参数，包括交付的网络地址。
- DHCPNACK：服务器发送给客户端，表明客户端的网络地址不正确（如客户移动到新的子网）或客户的租期已过期。

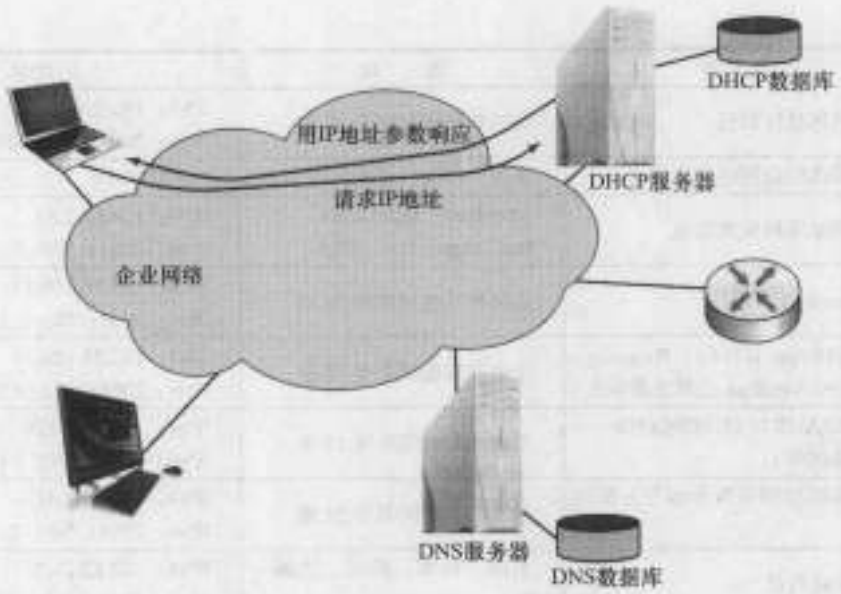


图 7-8　DHCP 角色

- DHCPDECLINE：客户端向服务器表明网络地址已被占用，DHCP 服务器需要通知系统管理员。
- DHCPRELEASE：客户端向服务器放弃网络地址，并取消剩余的租用。
- DHCPINFORM：客户端发送给服务器，只查询本地配置参数，此时客户已有外部配置的网络地址。

图 7-9 解释了一个典型的消息交换，涉及以下几个步骤：

1）客户端在其本地物理网络广播一个 DHCPDISCOVER 消息。该消息包括有关网络地址和租用时间的选项。中继代理会将消息传递到另一个物理网络的 DHCP 服务器上。

2）每一个服务器可以响应一个 DHCPOFFER 消息，该消息包括一个可用的网络地址。

3）客户端从多个服务器接收到多个 DHCPOFFER 消息后，将等待多个服务器响应。之后，客户端选择一个服务器，基于之前获得的 DHCPOFFER 消息中的配置参数，向此服务器请求配置参数。客户端广播一条 DHCPREQUEST 消息，包括服务器的标识符选项，表明它选中了那个服务器，还可能包括一些其他选项，用于指定期望的配置值。该 DHCPREQUEST 消息将通过 DHCP 中继代理传播和中继。当客户端没有收到任何 DHCPOFFER 消息时，将超时并重传 DHCPDISCOVER 消息。



图 7-9　DHCP 消息交换

4）服务器收到客户端广播的DHCPREQUEST后，没有被客户端选中的服务器将DHCPREQUEST消息视为客户端拒绝服务的通知。被选中的服务器为客户端指派绑定以提供持久保存，并且服务器会以DHCPACK消息作为响应，其中包含为客户端提供的配置参数。

5）客户端收到DHCPACK消息和配置参数。此时，客户端完成配置。

6）客户端可能会通过发送DHCPRELEASE消息到服务器放弃对某网络地址的租用。

应用注解

在你的组织结构中配置DNS

域名系统是局域网和因特网通信的基本部分。当在运行于因特网上的程序中键入一个域名或统一资源定位地址（URL）时，该域名必须转换为IP地址。最佳的例子为Web浏览器。DNS使用户放弃难记的IP地址，如207.42.16.185，而是选择“人类可读的”名字，如www.yahoo.com。Yahoo网站实际上由多个服务器组成，在其域名被转换为IP地址后，用户再基于IP地址访问服务器。

DNS通常除了用于访问网站外，还用于许多其他服务。电子邮件、网络共享、FTP等作为因特网资源的一部分，我们连接它们时也使用域名。终端用户通常在与所有的企业服务器通信时使用域名而不是IP地址。例如，命令“ftpwww.georgia.com”应用了域名，所以首先将域名解析成数字地址传给服务器。

大多数的网络交易开始时，计算机（主机）需联系DNS以完成交易。那么DNS处于何处提供服务呢？企业可以选择外部提供的DNS服务，也可以选择将自己运行的DNS连接其他DNS系统。企业网络的规模大小往往决定选择哪种方法。小型网络通常不需要拥有自己的DNS服务器，只有当拥有大量的内部服务器和服务时，才需要选择运行自己的DNS。

你所接受的网络服务，通常是由因特网服务供应商（ISP）提供。ISP也会自动提供其他服务，如为组织计算机分配IP地址或提供电子邮件服务。如果你自动获得了IP地址，通常也会同时获得DNS服务器地址。另一种选择是在个人计算机上手动配置DNS服务器地址。当网络使用私有IP地址进行配置而无需从ISP获得时，往往会选择手动配置。

当企业决定要运行自己的DNS服务器时，有几种可能的配置。DNS实际上是一个巨大的工作在分层结构中的服务器集。这些服务器会在用户现场（你的本地DNS）和异地。异地系统是由其他人连接到因特网时使用的服务器。这意味着除非服务器被设计为孤立的，否则它会与外部DNS服务器和本地网络的上层通信。在实际操作中，当DNS系统收到一个域名解析请求时，最近的服务器会尝试提供应答（如，与请求的域名对应的IP地址）。如果服务器不能应答，该请求会往上传递，直到某个服务器应答并响应。

几乎所有的计算机都可以配置成DNS服务器。具体的技术细节超过了本书的范围，运行自己的服务器增加了额外一层的复杂性和管理需要。DNS服务器必须保持更新并且做好备份。如果本地DNS服务器离线，所有其服务的主机都将出现连网困难。为了缓解这种后果，大多数自己运行DNS服务器的公司会运行一个辅助服务器作为冗余。

要考虑的一点是，公司将多大程度上依赖于Windows活动目录。活动目录是企业对象的仓库或数据库。这些对象可以描述成人员、组、服务及其他。在此之前，Windows网络由域控制器、NetBIOS、DNS支持，但活动目录使得Windows网络更加依赖于DNS。因此，Windows系统对DNS操作的正确性越来越依赖。在这种情况下，运行一个本地DNS服务

器是最好的选择，因为所有的企业特定的信息必须保存在服务器和活动目录系统上。

DNS 是所有数据通信网络的基本的、关键的部分。选择配置自己的 DNS 还是选择外部机构所提供的服务必须经过慎重的考虑，因为这是对时间和管理资源的重要投资。

7.4 总结

对企业来说，最重要的可用网络设备当属因特网。因特网可以连接客户与供应商，也可以作为连接公司设备的广域网络战略的一部分。因特网不是常规的企业工具，因为它并不属于或受管于单一的实体。因此，每个使用因特网的企业必须理解并部署必要的标准化协议，以使其在因特网上通信。

因特网和专用内部网由众多分散的网络构成，而这些分散的网络又通过路由器进行互连。数据以分组的形式从源系统沿着路径，横跨众多网络及路由传送到目的地。路由器接收并将分组转发到其目的地址，它同时负责分组的路由，就像分组交换节点的操作一样。

因特网的另一重要元素是其地址方案。每一个接入的主机都拥有独一无二的地址，对实现数据路由及传输来说至关重要。因此，因特网标准定义了一个 32 位长度的地址方案。域名系统提供了将主机域名转义换为因特网地址的一种方式，这使得用户更容易识别因特网资源。

案例研究 V：网络中立性

案例强调的主要概念包括因特网流量增长和因特网的商业使用。**案例学习和更多信息可查阅 www.pearsonhighered.com/stallings。**

7.5 关键术语、复习题和练习题

关键术语

ARPANET（美国高级计划研究计划署网络）
Central Office（CO，中心局）
Customer Premises Equipment（CPE，用户驻地设备）
domain（域）
Domain Name System（DNS，域名系统）
Dynamic Host Configuration Protocol（DHCP，动态主机配置协议）
host（主机）
Internet Exchange Point（IXP，因特网交换点）
Internet Protocol（IP，因特网协议）
Internet Service Provider（ISP，因特网服务供应商）
IP address（IP 地址）
IP datagram（IP 数据报）
IP packet（IP 分组）
message switching（报文交换）
network（网络）
Network Service Provider（NSP，网络服务供应商）
Point Of Presence（POP，接入点）
root name server（根域名服务器）
router（路由器）
Tier1（第一层）
Tier2（第二层）
Tier3（第三层）
Transmission Control Protocol（TCP，传输控制协议）
World Wide Web（WWW，万维网）

复习题

7.1 ARPANET 和因特网的区别?
7.2 哪两个协议构成了因特网通信方式的基础，并控制这种方式?
7.3 在因特网中，主机、网络、路由器的角色分别是什么?
7.4 列举两个首批投入使用的网络应用程序。
7.5 什么是 IP 地址?
7.6 什么是 Mosaic ?
7.7 哪两种应用程序代替了 Mosaic ?
7.8 用于显示网页的编程语言是什么?
7.9 ISP 与 POP 的区别是什么?
7.10 NAP 和 NSP 的区别是什么?
7.11 什么是因特网域?
7.12 什么是域名系统?
7.13 列举 DNS 中 4 个主要组件。
7.14 DNS 中的域名服务器和解析器有什么区别?
7.15 什么是 DNS 资源记录?
7.16 简单描述 DNS 操作。
7.17 什么是根域名服务器?
7.18 什么是 DHCP ?
7.19 简单描述 DHCP 操作。

练习题

7.1 在网络上调查一下，小型企业和企业家如何使用因特网。查找为什么小型企业选择接入因特网以及使用因特网后从中获得的利润。同时看看小型企业如何利用因特网发展。将收集到的信息写成论文（500 ~ 750 字）或者 8 ~ 12 张 PowerPoint 演示中，需包括多个案例。

7.2 在网络上调查因特网营销。确定广泛使用并相对有效的网络营销策略的主要类型，同时注意网络营销可能观察得到的主要趋势。将收集到的信息写成论文（500 ~ 750 字）或者 8 ~ 12 张 PowerPoint 演示中，需包括有效的网络营销渠道的案例。

7.3 查找并浏览 YouTube 上比较电路交换及分组交换的视频。找出 3 个你认为能最好解释分组交换和电路交换的不同关键点的视频地址。如果你只能向业务数据通信专业的学生推荐一个，你会推荐哪一个? 将你的推荐和判断依据写成论文（250 ~ 500 字）或者 3 ~ 5 张 PowerPoint 演示中。

7.4 两个看似无关的事件分别发生在 1992 年年末和 1993 年年初，并为 90 年代初因特网爆发式的增长埋下了种子。其一是由众议员 Rick Boucher 撰写的法例，另一个是由 MarcAndreessen 撰写的软件。说明这两个事件为何及如何为如今众所周知的因特网状态做出了主要贡献。参考如下网站上的内容：
http://www.neted.org/timeline/http://www.nsf.gov/pubs/stis19913/oig9301/oig9301.txt http://www.Webhistory.org/www.lists/www-talk.1993q1/0262.html。

7.5　挖掘工具提供了与 DNS 的轻松交互。挖掘工具适用于 UNIX 系统和 Windows 操作系统。它同样可以从网络访问。下面是我在写本书时获得的免费提供挖掘工具的网站地址，http://www.Webmaster-toolkit.com/dig.shtml。应用这个挖掘工具获取你的学校域名信息。

7.6　每一个连接到网络的机器都应该有一个 IP 地址。这个地址要么是由 DHCP 服务器分配的，要么就是手动配置的。应用下面的工具来决定你的 IP 地址。每使用一个工具，你需要打开一个 DOSshell（Windows）或者 Bourneshell（最常用的 Linuxshell）。这些 shell 有时称为命令窗口。在 Windows 操作系统里，shell 可以通过在运行窗口键入"command"来访问。对 Linux 来说，shell 可能是默认的，或者可以从任务栏的图标上访问。

Windows XP/7——在 shell 窗口键入"ipconfig"并按"Enter"。Linux——在 shell 窗口键入"ifconfig eth0"并按"Enter"。

7.7　你可以提供计算机的 IP 地址来与服务器交互。对 Linux 来说，你可以使用命令 ifdowneth0，之后是命令 ifupeth0。这两个命令将发送一系列的请求到服务器上。在 Windows XP/7 上，键入命令 ipconfig/？，将显示一系列的选项。键入 ipconfig/all 并且将显示的信息截图保存，将截图粘贴到一个文字处理文档中，并对列表中的每一个元素做简单的解释。

7.8　查找并浏览 YouTube 上有关 DNS 和 DNS 基本操作重要性的视频。确认 3 ~ 5 个你认为能最好描述 DNS 在因特网运行中的角色以及描述 DNS 如何工作的视频地址。如果你只能向业务数据通信专业的学生推荐一个，你会推荐哪一个？为什么？将你的推荐和理由写成论文（250 ~ 500 字）或者 3 ~ 5 张 PowerPoint 演示中。

7.9　Windows XP/7 和 Linux 有一个内置的程序使得用户可以与 DNS 服务器交互，这个程序是"nslookup"。将该程序名键入命令窗口并按"Enter"，你收到的自动反馈是什么？它们都有什么意义？键入"exit"会关闭程序。

7.10　在因特网上进行有关 DHCP 的研究。查找描述 DHCP 工作的信息，以及它的优缺点。将你找到的信息写成论文（500 ~ 750 字）或者 8 ~ 12 张 PowerPoint 演示中。

7.11　在因特网上进行有关静态与动态 IP 地址及其在当今网络下应用的研究。确定各自的优缺点。将你找到的信息写成论文（500 ~ 750 字）或者 8 ~ 12 张 PowerPoint 演示中，需要包括在商业网络中两者的推荐使用场合。

TCP/IP

学习目标

通过本章的学习，读者应该能够：

- 定义术语协议结构（protocol architecture）并解释通信结构的需求以及它所带来的好处。
- 描述 TCP/IP 体系结构，并解释结构中每一层的作用。
- 解释发展标准化结构的动机，并解释为什么用户偏向使用基于协议体系标准的产品而不是基于专有架构的产品。
- 解释对于网络互联的需求。描述在 TCP/IP 下，路由器提供网络互联的操作。

本章将学习支持商业或其他机构中分布式应用的基本通信软件，我们会发现这些软件是很重要的。为了使实现通信软件的过程可管理化，被称作协议结构的模块化体系投入了使用。因特网作为企业网络中的基本组成成分而出现，这意味着 TCP/IP 协议簇成为数据通信业务学生所要了解的最重要的协议结构。

电子通信方式向基于 IP 转变变得十分广泛，也因此产生了新的术语：EOIP（Everything Over IP）和 IPOE（IP Over Everything）。这种转变同样发生在商业企业和其他机构中，包括美国国防部和其防御信息系统代理 [JONE09]。EOIP 俨然成为企业网络中的“圣杯”，同时它也推动了聚合网络中的商业利润。EOIP 鼓励所有主要的业务数据类型（语音、视频、图像和数据），以及基于 IP 或 IP 兼容、电信传输的 IP 应用的发展。

TCP/IP 协议簇有多方面的内容，所以在本章的开始我们将介绍一个简单的协议体系结构，该体系仅由三个模块或三层组成，这样我们可以展示协议结构的关键特征和设计特点，而不会纠缠于繁枝末节。在这样的背景下，我们即将学习世界上最重要的协议体系：TCP/IP（传输控制协议 / 因特网协议）。TCP/IP 是一个基于因特网的标准，同时也是制定一整套计算机通信标准的框架。事实上，所有计算机零售厂家都支持这种体系结构。开放系统互联（OSI）是另一种标准化体系，它经常被用于描述通信函数，但如今很少被使用了，有兴趣的读者可以在附录 L 找到 OSI 的内容。

通过对 TCP/IP 的讨论，我们将学习到有关网络互联的重要概念。当然，在实际业务中会用到多个通信网络，需要通过多种方式将这些网络进行互联，也因此产生了涉及协议体系结构的问题。

8.1 一个简单的协议结构

8.1.1 对协议结构的需求

当计算机、终端以及其他数据处理装置交换数据时，涉及的处理过程十分复杂。以两台

计算机之间的文件传输为例，两台计算机之间肯定存在一条数据路径直接或通过通信网络连接，但这还不够，要执行的典型任务包含以下内容：

1）源系统需要激活直接的数据通信路径，或者需要告知通信网络目的系统的身份。

2）源系统需要确认目的系统准备好接收数据。

3）源系统上的文件传输应用需要确认目的系统上的文件管理程序准备好为用户接收并储存文件。

4）如果文件的格式或数据表现方式在两个系统上不兼容，需要其中一个系统提供格式转化功能。

计算机之间以协同行动为目的的信息交换通常称为计算机通信（computer communications）。相似地，当两个或更多计算机通过一个通信网络互联时，计算机工作组集被称作计算机网络（computer network）。因为终端和计算机之间需要一个相似程度的合作，所以当一些通信实体是终端时会经常用到这些术语。

在讨论计算机通信和计算机网络时，下面两个概念最为重要：

- 协议
- 计算机通信体系结构，或协议结构

协议用于在不同系统中实体间的通信。术语实体（entity）和系统（system）包含的意义非常普遍。实体的例子有用户应用程序、文件传输包、数据库管理系统、电子邮件设备和终端。系统的例子有计算机、终端和遥控传感器。需要注意的是，在某些情况下，实体和其所在的系统是同延的（如终端）。总的来说，实体是能够发送或接收消息的事物，系统是物理上包含一个或多个实体的不同对象。两个实体必须“使用相同的语言”才能通信成功，通信的内容、方式、时间都必须遵循有关实体之间相互达成的约定。这些约定被称为**协议**，特指一系列用于管理两个实体间数据交换的规则。一个协议的核心元素有：

- **语法**：包括数据格式与信号电平等
- **语义**：包括协调与错误处理的控制信息
- **时间安排**：包括速度匹配与排序

附录 8B 提供了一份详细的协议示例，称作因特网标准简单文件传输协议（TFTP）。

在介绍过了协议的概念以后，我们现在可以介绍**协议结构**的概念了。显而易见地，协同应用的两个计算机系统必须高度协作，这种协作的逻辑不是作为一整个模块来实现，而是细分成了多个子任务，每一个单独进行实现。这样就得到了一个分层的体系结构，位于每一层的对等实体（peer entities）会完成适于该层的子任务。举例来说，图 8-1 提出了一种两台连接在同一网络中的计算机之间进行文件传输的实现方式，这种传输方式使用了三个模块。先前列表中的任务 3 及任务 4 可以由一个文件传输模块（file transfer module）来完成，这两个分别位于两个系统上的模块能够互相交换文件及命令。然而，文件传输模块并不被要求来处理实际数据与命令传输的细节，每个文件传输模块都依赖于一个通信服务模块（communications service module）。这个模块负责确保文件传输命令和数据能被可靠地在系统间交换。通信服务模块运行的方式之后探索，在其他事件中，这个模块会完成任务 2。最后，两个通信服务模块之间的交换性质是独立于连接他们的网络的性质的，所以，与其将网络接口的细节建立在通信服务模块，不如设计第三种模块——网络接入模块（network access module），来通过与网络交互完成任务 1。



图 8-1 文件传输的简化结构

总的来说，文件传输模块包含了所有文件传输应用的独特逻辑，例如传送密码，文件命令，和文件记录。这些文件和命令必须被可靠地传送，然而，相同类型的可靠性需求是与不同类的应用相关的（例如电子邮件、文档传送器）。所以，这些需求被一个独立的可以被不同类型的应用复用的通信服务模块所满足。通信服务模块专注于确保两方计算机系统是活动的并准备好传送数据和追踪正在被交换的数据来确保数据的投递。然而，这些任务都是与正在被使用的网络种类无关的，所以，实际用于处理网络的逻辑部分被置于独立的网络接入模块。如果被使用的网络发生了改变，只有网络接入模块会被影响。

因此，我们使用一组结构化的模块来实现通信功能，而不是一个单独的模块，这个结构被称作**协议结构**（protocol architecture）。一个类比在这时应该会有帮助。假设 X 办公室的主管想发送一个文档给 Y 办公室的主管，X 的主管准备好文档并可能会附上一份便条，这与图 8-1 中文件传输应用的动作相类似。然后 X 的主管把该文档交给一位秘书或行政助理，X 的行政助理将文档装入信封并写上 Y 的地址及 X 的退信地址，信封有可能会标记上“机密”字样。行政助理的行为与图 8-1 中通信服务模块的动作相类似。X 的行政助理接着将包裹交给运输部门，运输部门的某人会决定以何种形式来发送这个包裹：平邮、UPS、还是快递然后贴付合适的邮资或货运单据在包裹上并将其投递出去。运输部门的行为与图 8-1 中网络接入模块的动作相类似。当包裹到达 Y 办公室时，相似的一系列动作会再次发生。Y 的运输部门会接收包裹并根据包裹上的姓名将其派送到相应的行政助理或秘书处，行政助理会打开包裹并将内封的文档递交给主管。

协议结构的另一个重要方面在于不同系统的模块只会与同等级的其他模块通信。因此，文件传输模块才能专注于与其他系统上的同等文件传输模块的通信内容（在图 8-1 中用两个模块间的虚线表示）。

在本节剩下的部分中，我们将概括图 8-1 的实例来呈现一个简化的协议结构。之后，我们将研究真实的 TCP/IP 实例。

8.1.2 一种三层协议结构模型

总体来说，分布式数据通信包含三个方面：应用、计算机和网络。在第 10 章中，我们将会研究几个示例应用，包括文件传输和电子邮件。这些应用运行在通常支持多任务并行的计算机上。计算机被接入网络，待交换的数据被网络从一台计算机传输到另一台计算机。因此，从一个应用到另一个应用的数据传输过程是：首先将数据发送到该应用存在的计算机上，接着将数据发送给计算机上的目标应用。

依据这些概念，我们可以自然地将通信任务组织成三个相对独立的层：网络接入层、传输层、和应用层。

网络接入层（network access layer）与计算机和其所连接的网络间的数据交换有关。发送方计算机必须向网络提供目标计算机的地址，这样网络才能将数据路由到正确的地址。发送方计算机有可能需要开启特定的服务，如网络所提供的优先级服务。在该层所使用的特定软件由使用的网络类型所决定，针对电路交换、分组交换、局域网（LANs）和其他类型的网络都制定了不同的标准。例如 IEEE 802 标准明确了接入局域网的方式，该标准会在第三部分中介绍。将与网络访问有关的函数放进单独的层中是有意义的，如此一来，通信软件的网络接入层以上的其余部分不需要考虑使用的具体网络，同样的高层软件也能正确执行而不必考虑计算机所连接的特定网络。

不管数据交换应用的性质如何，通常对数据的可靠交换有所要求。也就是说，我们需要确保所有数据到达目的应用程序，并且所有数据需按照他们发送的顺序到达。正如我们所见，提供可靠性的机制基本上独立于应用程序。因此，在一个多应用共享的公共层中收集这些机制是十分有意义的，这称为**传输层**（transport layer）。

最后，**应用层**（application layer）包含了支持各种用户应用的逻辑。对于不同种类的应用（如文件传输），需要该应用特有的单独模块来执行。

图 8-2 和图 8-3 展示了这种简单结构。图 8-2 显示 3 台计算机连接到一个网络上，每台计算机包含位于网络接入层和传输层的软件，同时还包含应用层中对应一个或多个应用的软件。为了成功地进行通信，整个系统中的每一个实体必须拥有一个独立的地址。在我们的三层模型中，需采用二级地址。网络中每台计算机都有一个独一无二的网络地址，这使得网络可以正确地将数据传递给计算机。每一个计算机上的应用都有一个位于该计算机上的独立地址，这使得传输层能支持每台计算机上的多个应用。后者地址称为**服务访问点**（SAP）或**端口**（port），意味着每个应用都是单独访问传输层的服务的。

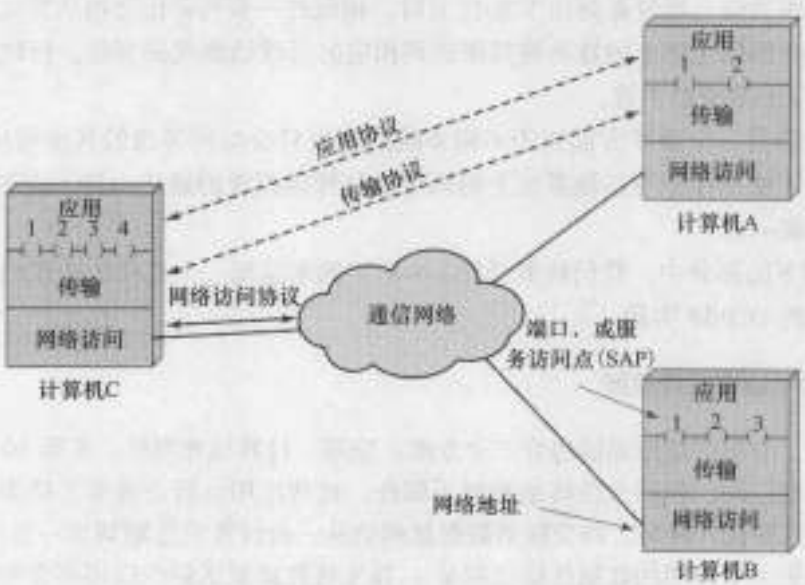


图 8-2　协议结构和网络

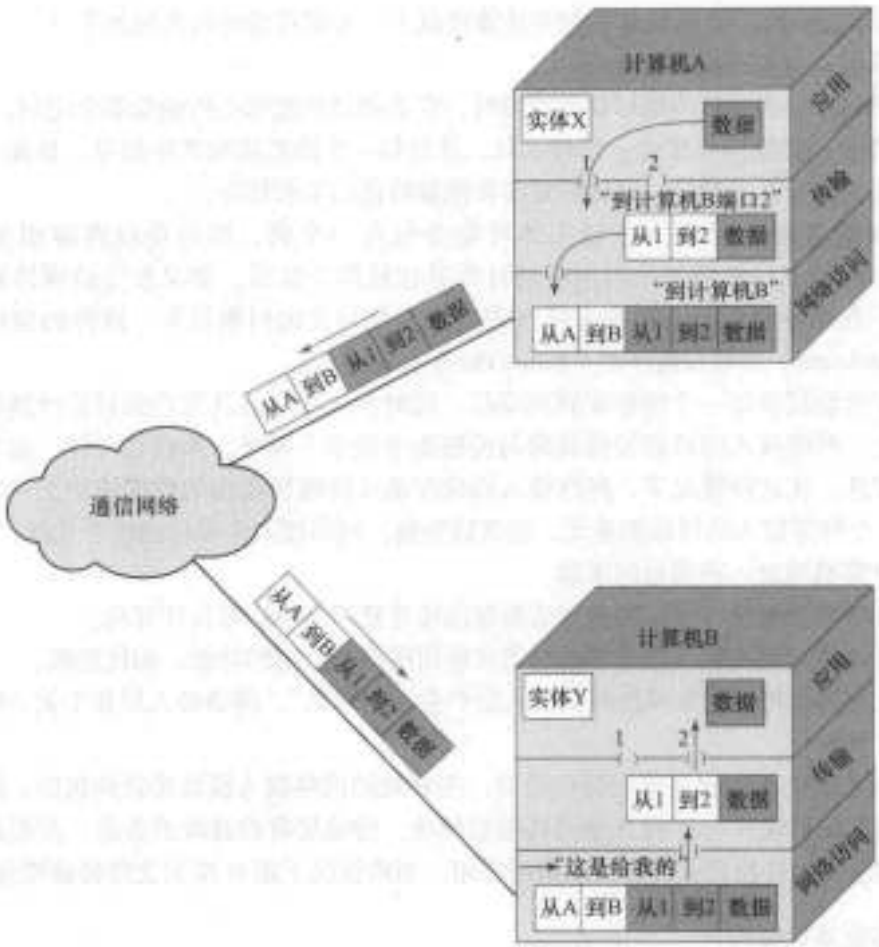


图 8-3 简单结构中的协议

图 8-2 表明不同计算机的同一级模型通过协议进行通信。应用实体（如文件传输应用）在一台计算机内通过应用级协议（如文件传输协议）与另一台计算机内的应用通信，这种交互不是直接的（图中用虚线表示），而是通过传输协议达成，这些传输协议用于处理两台计算机间传输数据的细节。传输协议同样不是直接的，而是依赖网络层的协议来获得网络访问并将数据从网络路由至目标系统。在每一层上，合作的对等实体专注于他们要与对方通信的内容。

让我们跟踪一次简单的操作过程。假定一个应用，连在计算机 A 的端口 1 上，它希望将消息发送到连接在计算机 B 的端口 2 上的应用。A 上的传输将消息传递到其传输层，同时伴随指令将它发送到计算机 B 的端口 2 上。传输层将消息传递到网络接入层，并向其发出指令将消息传输到计算机 B 上。需要注意的是网络并不需要被告知目的端口，它所需要知道的全部信息即数据将发往计算机 B。

为了控制这种操作，控制信息和用户数据将会被一起发送，如图 8-3 所示。我们假设发送端应用产生了一块数据，并将其发送到传输层。为了方便，传输层可能会将整块数据分成两个更小的块，下面会进一步讨论。对每一小块，传输层会添加一个传输头部（header），包含了协议控制信息。上一层数据与控制信息的结合被称为**协议数据单元**（PDU），在当前情况下，是指传输协议数据单元。传输协议数据单元通常被称作段（segment），每一个段的头部

包含的控制信息被用于计算机 B 的对等传输协议上。头部可能的包含项如下：

- **源端口**：指发送数据的应用。
- **目的端口**：当目的传输层接收到段时，它必须清楚数据应传输给哪个应用。
- **序列号**：传输协议发送一序列的段，并且每一个段都被按顺序标号，如此一来，当他们到达时打乱了顺序，目的传输实体能够将他们重新排序。
- **错误检测码**：发送方传输实体可能会包含一个码，该码是段内容相关函数的结果。接收方传输协议执行同样的计算并比较两个结果，如果发生错误传输即会不一致。在这种情况下，接收方可以丢弃这个段并发出纠错操作。这种码也称为**校验和**（checksum）和**帧校验序列**（frame check sequence）。

下一步传输层将每一个段移交到网络层，同时发出指令将其发送到目标计算机。为了满足这种需要，网络接入协议必须将数据与传输指令展示于网络。和以往一样，这个操作同样需要控制信息。在这种情况下，网络接入协议在他从传输层收到的数据前加上一个网络接入头部作为一个网络接入协议数据单元，通常称为**包**。网络接入头部包括以下几项：

- **源计算机地址**：表明包的来源。
- **目的计算机地址**：网络需要知道数据应传送到网络中的哪台计算机。
- **功能请求**：网络接入协议可能会请求使用网络中特定的功能，如优先级。

需要注意的是传输层头部在网络接入层中并不“可见”，网络接入层并不关心传输层段的内容。

网络接受来自 A 的包并将它传送给 B。在 B 处的网络接入模块接收到包后，剥掉包的头部并将封装好的传输段转移到 B 端的传输层模块。传输层将检查段的头部，并根据头部的端口字段的信息将封装的记录传递给正确的应用，当前情况下指 B 端的文件传输模块。

8.1.3　标准化协议结构

当不同厂商生产的计算机间需要进行通信时，软件开发变成了噩梦。不同厂商间使用不同的数据格式和数据交换协议，甚至在同一个厂商的流水线上，不同型号的计算机也可能使用不同的通信方式。

如今计算机通信和计算机网络普遍存在的情况下，每次开发一个特殊用途的通信软件的方法过于昂贵。唯一的解决方法就是所有的厂家接受并执行一套共同的约定，为了实现它，我们需要一套标准，这个标准应当具有以下两个优点：

- 厂商都被鼓励执行这个标准，因为一旦这种标准被广泛使用，非标准产品将不会畅销。
- 客户可以要求任何想向他们提供设备的厂商执行该标准。

两个协议结构成为可互操作的协议标准发展的基础：TCP/IP 协议簇和 OSI 参考模型。TCP/IP 是至今为止使用最广泛的可互操作的体系结构。OSI，虽然比较有名，但并没有实现其早前的承诺。同时还有一个专有的框架被广泛使用：IBM 的系统网络体系（SNA）。尽管 IBM 提供对 TCP/IP 的支持，但它仍然继续使用 SNA，同时后者体系在今后几年中会同样重要。本章接下来的部分会详细讨论 TCP/IP。OSI 和 SNA 会在附录 I 和 F 中分别总结。

8.2　TCP/IP 协议体系

TCP/IP 是由美国国防先进研究项目局（DARPA）注资建立的实验性分组交换网络

ARPANET 的协议研究开发成果，通常被称作 TCP/IP 簇。此协议簇由众多被因特网结构委员会（IAB）指定为标准的协议组成。附录 B 对因特网标准进行了讨论。

8.2.1 TCP/IP 层

TCP/IP 并未像 OSI 那样推出官方的结构模型，然而，基于现有的协议标准，我们可以将 TCP/IP 的通信工作组织成五个相对独立的层：

- 应用层
- 主机对主机层，或传输层
- 因特网层
- 网络接入层
- 物理层

应用层（appilication layer）和**传输层**（transport layer）对应 8.1 节中的三层模型的最顶部两层。在传输层中，TCP 是最常用的协议。

在两个设备连入不同网络的情况下，需要一些步骤来让数据通过多个互相连接的网络，这就是因特网层的功能。因特网层采用了**因特网协议**（IP）在多个网络间提供路由功能，这个协议不仅被实现在终端系统上，也被实现在路由器上。**路由器**（router）是连接两个网络的设备，其主要功能是在一条从源终端到目标终端的路径上将数据从一个网络传送到另一个网络。

网络接入层同样也在三层模型中被讨论过。让我们先考虑两台想要通信的计算机都连入了同一个网络的情况，比如在同一个局域网（LAN）或广域网（WAN）内。发送方计算机必须将目标计算机的地址提供给网络，这样网络才能将数据转发给正确的目标。在两台想要通信的计算机没有连入同一网络的情况下，数据传输必须以一个跳数序列的方式来通过多个网络。在后面这种情况下，网络接入层更关心沿路径来接入一个网络。因此，从源计算机开始，网络接入层为接入的网络提供目标路径上连接此网络到下一个网络的路由器所需的信息。

物理层涵盖了数据传送设备（如工作站、计算机）及传送介质或网络的物理接口。物理层的主要功能是指出传送介质的特性，如信号类型、数据传输率和其他相关的内容。

8.2.2 TCP/IP 操作

图 8-4 标示了 TCP/IP 协议体系结构是怎样为通信配置的。将其与图 8-2 进行比较，其体系上的差别在于因特网层的内容允许路由器连接多个网络。一些网络接入协议，比如以太网或 Wi-Fi 逻辑，是用于连接一台计算机到一个网络的。TCP/IP 协议能让主机通过网络将数据发送到另一台主机，或通过路由器发送到另一个网络中的主机。IP 协议被实现在所有终端系统和路由器中，它作为传递者来将数据块从一台主机通过一个或多个路由器发送到另一台主机。TCP 协议只被实现在终端系统中，它保持对传输数据块的追踪来确保所有的内容都被可靠地发送到正确的应用处。

图中高亮了 TCP/IP 协议体系结构的地址分级。网络中的每个主机都必须用一个唯一的网络地址来在网络上标识出该计算机。另外，每个计算机还有一个唯一的全球因特网地址，这可以保证数据能被投递给正确的主机，这个地址被 IP 用来路由和投递。主机中的每个应用都必须拥有一个唯一的端口号来让主机对主机协议（TCP）投递数据到正确的进程中。

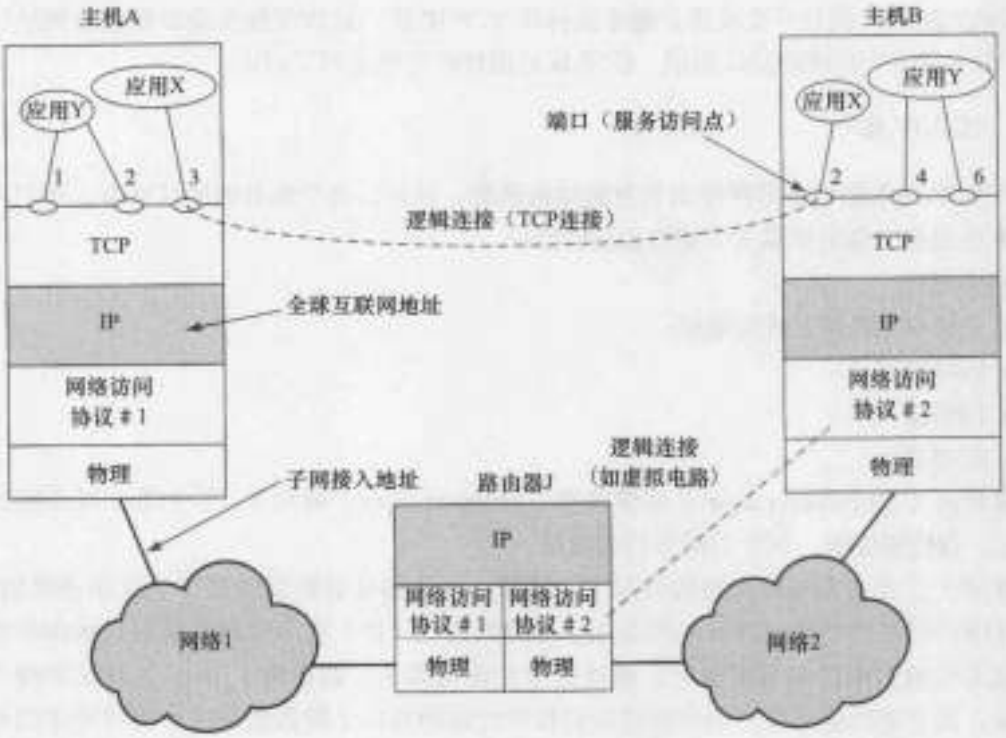


图 8-4　TCP/IP 思想

参考图 8-3 中的三层体系结构，追踪四层结构 TCP/IP 模型的运算相对容易。对于主机 A 应用和主机 B 应用间的传输来说，如图 8-5 所示，控制信息和用户数据一样需要被传送。让我们假设发送进程生成并发送一个数据块给 TCP，TCP 附加控制信息（称作 TCP 头）形成 TCP 片段，控制信息会被主机 B 上的对等 TCP 实体使用。



图 8-5　TCP/IP 体系结构中的协议数据单元

下一步，TCP 将每个片段同指令一起转交给 IP 来发送给 B，这些片段必须经过一个或多个网络传送并经一个或多个中间路由转发。这项操作同样需要使用控制信息，因此 IP 附加一个包含控制信息的头部到每个分段来构造一个 IP 数据报。IP 头部储存的内容的一个例子是目标主机地址（在这个例子里是 B）。

最后，每个 IP 数据报都将传递给网络接入层，以进行通往目的地的第一个网络传输。网络接入层会附上自己的头部来产生一个包，或一个帧。这个包通过网络发送给路由器 J。包的头部包含了网络用以传送数据所需的信息。

在路由器 J 处，包头部被剥离，IP 头部会被校验。在 IP 头部的目标地址信息的基础部分，路由器里的 IP 模块会引导数据报通过网络 2 到 B 处。为了这一点，数据报会被再附上网络接入头部。

当数据被 B 接收到，这些步骤会以倒序再次发生。在每一层上，相应的头部会被除去，

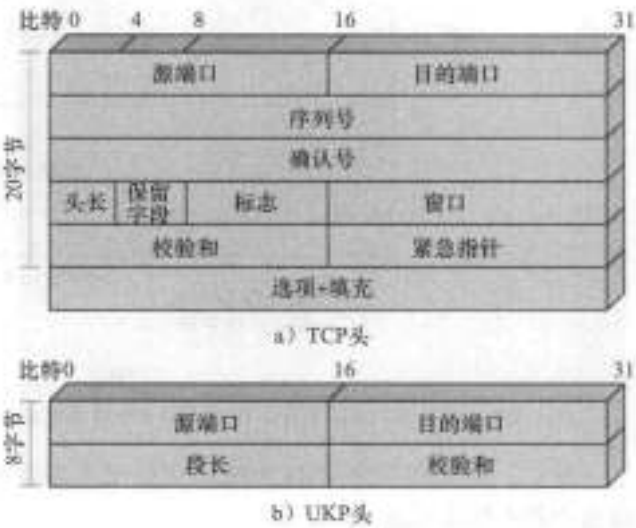
然后剩下的部分会被发送给下一层，直到原始的用户数据被发送给目标进程。

8.2.3 TCP 和 UDP

对多数以部分 TCP/IP 协议体系结构运行的应用来说，其传输层的协议是 TCP。TCP 为应用间的数据传输提供了一个可靠的连接。一个连接仅仅是两个不同系统中进程间的临时性逻辑关系。在连接的时候，为了调整分段流和恢复遗失或受损的分段，每个进程会追踪传入或送出给其他进程的分段。

图 8-6a 展示了 TCP 的头部格式，其最小长度是 20 字节或 160 比特。源端口和目的端口部分标明了源系统和目标系统上的哪个应用在使用这个连接。序号、确认号、窗口部分提供了流控制和错误控制的信息。校验和是一个 16 比特的帧校验序列，用来检测 TCP 分段中的错误。感兴趣的读者可以参考附录 8A 的更多详细内容。

另外，TCP/IP 簇中有另一个常用于传输的协议：用户数据报协议（UDP）。UDP 不保证数据的投递，包序列的维护或对重复数据的避免。UDP 用一个含最少协议机制的进程来发送信息给另一个进程。一些面向交易的应用会使用 UDP：比方说简单网络管理协议（SNMP），这是 TCP/IP 网络的标准网络管理协议。因为它是无连接的，因此 UDP 只需要做很少的事情。实质上，它给 IP 增加了一个端口寻址的功能。通过检查 UDP 头可以清楚地看到，如图 8-6b 所示。



a）TCP头

b）UKP头

图 8-6 TCP 和 UDP 头

8.2.4 IP 和 IPv6

几十年来，TCP/IP 体系结构的关键一直是 IP。图 8-7a 展示了 IP 头的格式，其最小长度是 20 字节，即 160 比特。IP 头和传输层的段共同组成了 IP 层的协议数据单元，通常被称为 IP 数据报或 IP 包。IP 头包括了 32 比特的源地址和目的地址。头部校验和字段是用来检测头部的错误以防止错误传输的。协议字段用来表明哪个高层的协议类型正在使用 IP，如 TCP 或 UDP。ID、标志以及片段偏移字段将会在分段和重组操作中使用。对有兴趣的读者，8.4 节提供了更多的详细内容。

1995 年，制定因特网协议标准的因特网工程任务组（IETF），提出了下一代 IP 的规范，被称作 IPng。该规范之后在 1996 年变成了被称为 IPv6 的标准，IPv6 提供了在已有的 IP 基础上的大量功能性增强。

IPv6 是设计用来适应如今更高速的网络和混合数据流的，包括越来越流行的图片和视频。但是推动发展新协议的力量是对更多地址的需求。现今的 IP 使用的是 32 比特地址以具体指定源或目的端。随着因特网的飞速增长以及专用网络的接入，如今的地址长度变得不足以容纳所有需求地址的系统。如图 8-7b 所示，IPv6 含有 128 比特的源和目的地址字段。

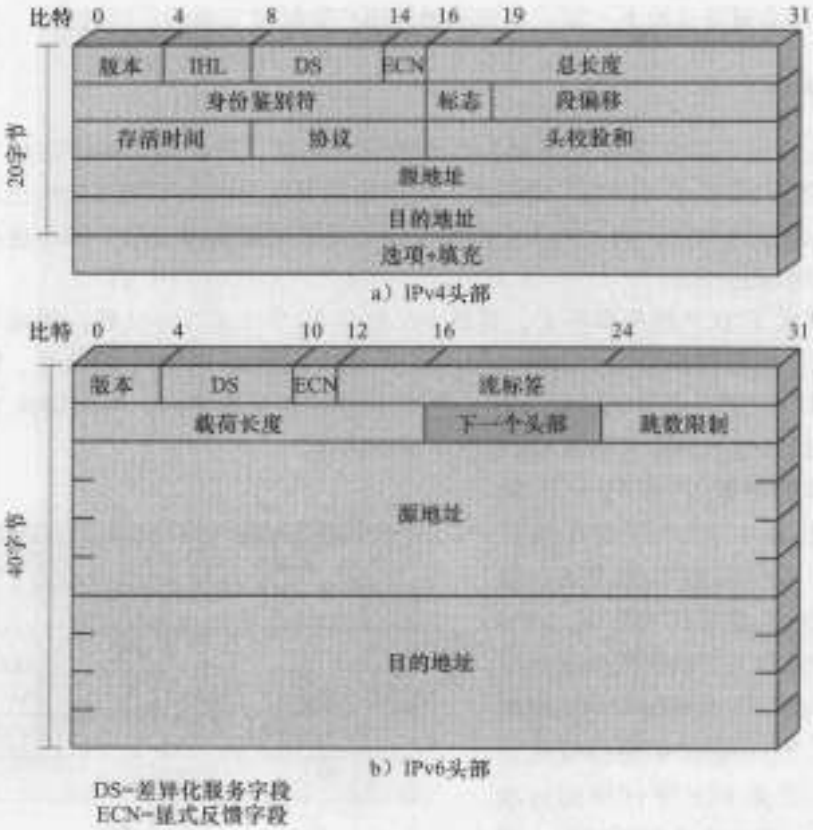


图 8-7　IP 头

注：这 8 比特的 DS/ECN 字段在 IPv4 头部曾被称为服务类型字段，在 IPv6 中称为流量类字段

最后，所有安装使用 TCP/IP 协议的用户都会从如今的 IP 过渡到 IPv6，但是这种过程需要至少数十年来完成。

更多详细内容，请参照附录 8A。

8.2.5　TCP/IP 应用

许多应用已经进行了标准化以便在 TCP 上操作，我们在此介绍几个最常用的应用。

简单邮件传输协议（SMTP）支持基本的电子邮件功能，它提供一种使得信息在分散的主机间传递的机制。SMTP 的特点包括提供邮件列表、收件反馈以及转发功能。SMTP 并不具体指定消息创建的方法，需要一些本地编辑或本地电子邮件设施。一旦消息被创建了，SMTP 将接受消息并利用 TCP 将其发送到另一个主机上的 SMTP 模块，目标 SMTP 模块将利用本地电子邮件软件包把收到的消息储存在用户的邮箱中。SMTP 将会在第 10 章中详细讨论。

文件传输协议（FTP）在用户指令下，将文件从一个系统传输到另一个系统上。它同时支持文本和二进制文件，并且提供了用户访问控制。当用户希望开始文件传输时，FTP 创建一个 TCP 连接到目标系统以交换控制信息，该连接允许用户 ID 和密码传输，并且允许用户指定文件及对文件进行操作。一旦文件传输被批准，第二个 TCP 连接就建立用于数据传输。文件通过数据连接进行传输，传输时并不包含应用层下的任何头部或控制信息。传输完成后，控制连接发出完成信号并接受新的文件传输指令。

SSH（安全外壳协议）提供一个安全的远程登录功能，使得终端或个人用户可以远程地登录计算机和功能，就像直接连接到远程计算机一样。SSH 同样提供在本地主机和远程服务器间的文件传输，它使得用户和远程服务器可以相互认证，双方通信都经过加密。SSH 的通信基于 TCP 连接。

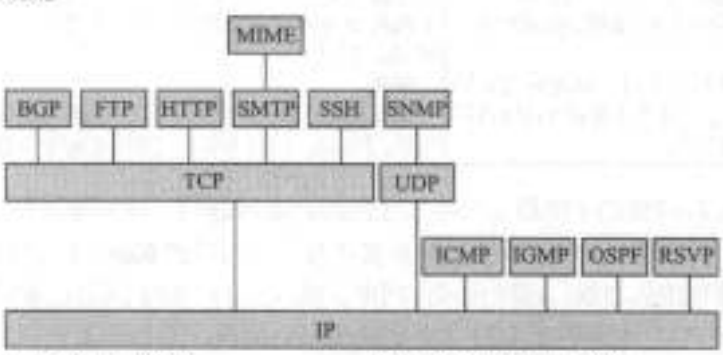
HTTP（超文本传输协议）连接用户系统到因特网中的 Web 服务器，它最基本的功能是与服务器建立一个连接并向用户的浏览器发送 HTML 页面。它同时用于从服务器下载文件到浏览器，或其他使用 HTTP 的应用。

SNMP（简单网络管理协议）是一个被广泛应用的网络监控和控制协议。数据从 SNMP 代理发送到监管网络的工作站控制台，其中 SNMP 代理是指报告各网络设备（如集线器、路由器、桥等）动态的硬件或/和软件进程。代理将返回包含在 MIB（管理信息库）中的信息，MIB 是指一种数据结构，用于定义从设备得到的信息以及可控制信息（如关闭、打开等）。

8.2.6 协议接口

TCP/IP 协议簇的每一层都与它的直接相邻层交互。在源头上，应用层利用传输层的服务并向传输层提供数据，相似的关系存在传输层与网络互联层以及互联层和网络接入层的接口间。在目的端，每一层向其相邻的高层向上传递数据。

体系并不要求使用每一单独的层，如图 8-8 所示，可能会制定某种协议直接触发每一层的服务。大多数应用需要一个可靠的传输协议因此选择使用 TCP，一些针对特殊需求的应用却不需要 TCP 服务。还有一些应用，如 SNMP，使用另一种传输协议，称为用户数据报协议（UDP）。另一些有可能直接使用 IP。不涉及网络互连或不需要 TCP 的应用及其他协议则能够直接调用网络接入层。



BGP=边界网关协议
FTP=文件传输协议
HTTP=超文本传输协议
ICMP=控制报文协议
IGMP=Internet组管理协议
IP=互联网协议
MIME=多用途因特网邮件扩展
OSPF=开放式最短路径优先
RSVP=资源预留协议
SMTP=简单邮件传输协议
SNMP=简单网络管理协议
SSH=安全外壳协议
TCP=传输控制协议
UDP=用户报文协议

图 8-8 TCP/IP 协议簇中的一些协议

8.3 网络互联

大多数情况下，局域网和广域网并不是孤立的实体。机构可能在给定的站点拥有多种类型的局域网以满足一系列的需求，也可能在给定的站点拥有多个相同类型的局域网以满足性能和安全的需求。同时机构可能在不同的站点拥有多个局域网并且需要它们通过广域网互联，

以此对分布式的信息交换进行集中控制。

表 8-1 列举出了一些与网络互联相关的常用术语。从用户的角度来看，一套互联的网络，只是看起来像更大的一个网络。然而，如果每个网络的组成部分保持其特性，并且需要特殊机制来支持多个网络通信，那么整个配置通常称为一个**互联网络**，同时每一个组成的网络称作**子网**。最重要的互联网络的例子简单地称为因特网。因特网由最初的面向研究的交换网络发展至今，它充当互联网络技术发展的基础和企业间私有网络的模型，后者称为作企业内部网。如果企业通过互联网将内部网的访问提供给特定的用户或供应商时，那么最终配置通常称为**外部网**。

表 8-1　网络互联术语

通信网络 对接入网络的设备提供数据传输服务的设施	**子网** 指因特网络的组成部分。这避免了造成模棱两可的情况，因为从用户的角度去看，整个因特网络是一个单一的网络
计算机网络 通过通信网络交换数据的主机和其他电子设备的集合	**终端系统（ES）** 接入通信子网或因特网络的计算机，它可以使用网络提供的服务来与其他介入的系统交换数据
因特网（Internet） 1）（非大写）通过交换机和 / 或路由器和 / 或网关互连的计算机网络集合 2）（大写）唯一的、互联的、世界性的贸易系统、政府系统、教育系统和其他计算机网络，该网络共享了（a）TCP/IP 协议簇（b）被因特网名称与数字地址分配机构（ICANN）管理的名称和地址空间	参考：**主机** **中间系统（IS）** 用于连接两个网络的设备，使得接入不同网络的终端系统间可以通信
内部网 单独企业的因特网络，提供了重要的因特网应用，其中万维网尤为重要。为满足企业内部的工作，内部网在组织内部运行，同时它可以作为一个独立的、自足的因特网络存在，也可连接到因特网	**二层交换机** 用于连接两个使用相似局域网协议的局域网的中间系统。交换机充当地址过滤器，它从一个被当作目的地的局域网中筛选出数据包并将它们传递出去。交换机并不修改或添加数据包的内容。交换机处于 OSI 模型的第二层（链路层）
外部网 公司内部网向因特网的延伸，以允许选定用户、供应商和移动工作人员能够通过万维网访问到公司的内部数据和应用	**路由器** 连接两个相似或不相似但共享 IP 的网络的中间系统。路由器采用的 IP 出现在每个路由器和每个网络终端。路由器工作在 OSI 模型的第三层
	网关 接入到两个（或多个）计算机网络的中间系统，这两个网络功能相似，但实现过程不相似。此外它还使网络间能够单向或双向通信

每一个组成互联网络的子网均支持接入子网的设备间通信，这些设备被称作**主机**或**终端系统**（ES）。另外，子网与 OSI 协议中提到的设备连接，称为**中间系统**（IS）。IS 提供通信路径以及执行必要的中继和路由功能，这样在因特网中，接入到的不同子网的设备间才能交互数据。

令我们感兴趣的 IS 的两种类型是**二层交换机**和**路由器**，它们两者的区别牵扯到互联网络逻辑使用的协议类型。我们将会在第 12 章学习桥的角色和功能路由器的角色和功能将在本章介绍 IP 时有所介绍。无论如何，路由器在整个网络体系中有着重要的作用，因此它值得在本节中做补充说明。

另一个 IS 的类型为**网关**，它连接两个或多个子网或内部网，而这两者在某些方面有所不同。当两个网络根据它们向主机提供的服务不同而使用了不同的协议时，网关就需要将一个协议解释成另一个协议，或者促使两个主机间进行方便的交互操作。对两个不同的邮件转发协议进行解释即是一个应用级别的网关例子。

8.3.1　路由器

网络互联通过使用中间系统和路由器实现，并以此来连接一些独立的网络。路由器必须实现的重要功能如下：

1）提供网络间的链路。

2）对介入到不同网络的终端系统提供数据的路由和发送。

3）在不修改接入网络的体系结构的基础上提供这些功能。

第三点意味着路由器必须适应网络间的许多不同，如下：

- **寻址方案**：网络可能使用不同的分配地址的方案。例如，每一个接入 IEEE 802 LAN 的设备使用的是 48 比特的二进制地址，而 ATM 网络通常使用 15 位的十进制地址（60 比特长每个数字地址编码成的 4 比特）。因此必须提供一些全球网络地址的格式，如目录服务一样。
- **最大包大小**：发出的数据包有可能被切分为更小的块以传输到另一个网络，这个过程被称为**分段**（fragmentation）。例如，以太网规定最大的数据包大小为 1500 字节，在帧中继网络中，常见的最大数据包大小为 1600 字节，那么从帧中继网络发出的数据包若要传递到以太网局域网时，必须分段为更小的块。
- **接口**：不同网络的软硬件接口都不尽相同，路由器这一概念必须独立于这些不同。
- **可靠性**：不同的网络服务提供或可靠或不可靠的终端到终端虚拟电路服务，路由器的操作不应依赖于网络可靠性的假设。

先前的这些需求可以通过网络互联协议在所有的终端系统和路由器上很好地实现，如 IP。

8.3.2 网络互联的示例

图 8-9 描述了一种配置，我们将用它说明网络互联协议间的交互。在这种情况下，我们将关注点集中在接入在帧中继广域网的服务器和接入到 IEEE 802 局域网（如以太网）的工作站，以及连接两个网络的路由器上。路由器提供了服务器和工作站之间的链路，使这些终端系统可以忽视干涉网络的细节。对帧中继网络，网络接入层仅仅由一个单一的帧中继协议组成。在 IEEE 802 局域网中，网络接入层由两个子层组成：逻辑链路控制层（LLC）和媒体接入控制层（MAC）。为了专注于本章的讨论，我们不详细地描述这些层，但他们会在接下来的章节探讨。

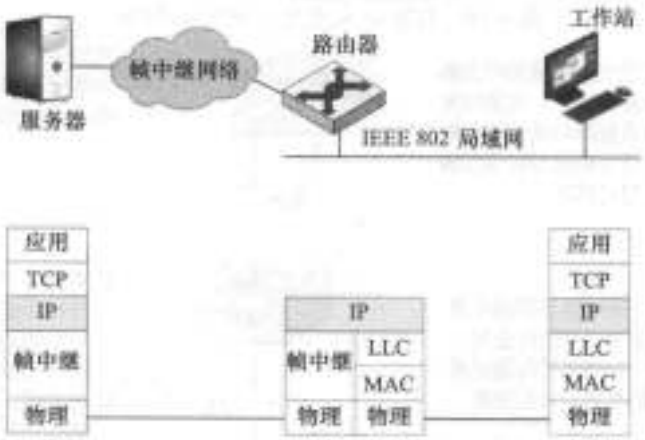


图 8-9 TCP/IP 配置示例

图 8-10 到 8.12 大致描述了发送一块数据的典型步骤，如文件或网页，从服务器，通过互联网络，最终到达应用或工作站上。在这个例子中，消息仅通过一个路由器，在数据被发送之前，服务器上的应用层，传输层以及工作站上的相应层建立了通信会话规则，包括将要使用的字符码或是错误检测方法之类的，每层协议均会用于该用途或消息的传输。

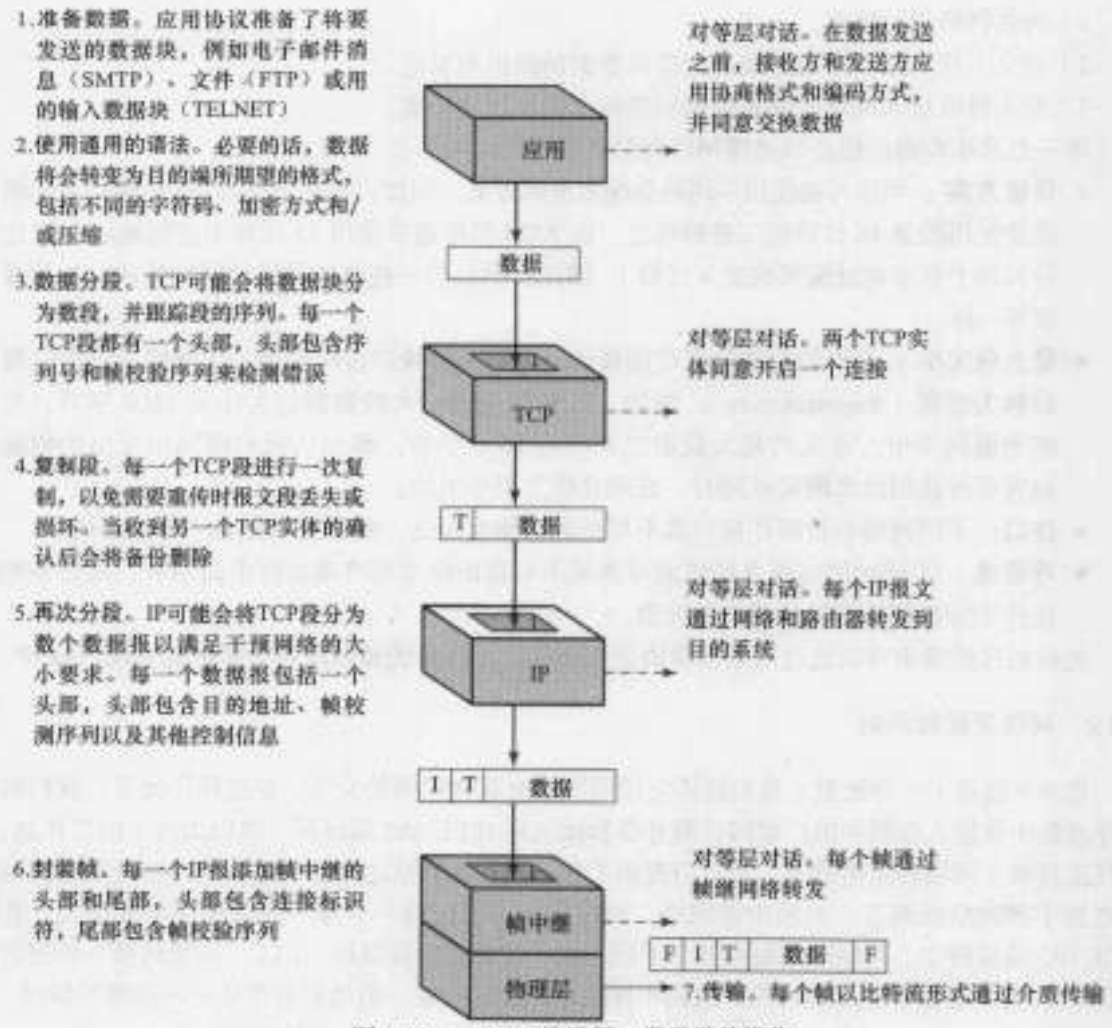


图 8-10　TCP/IP 的运行：发送端的操作

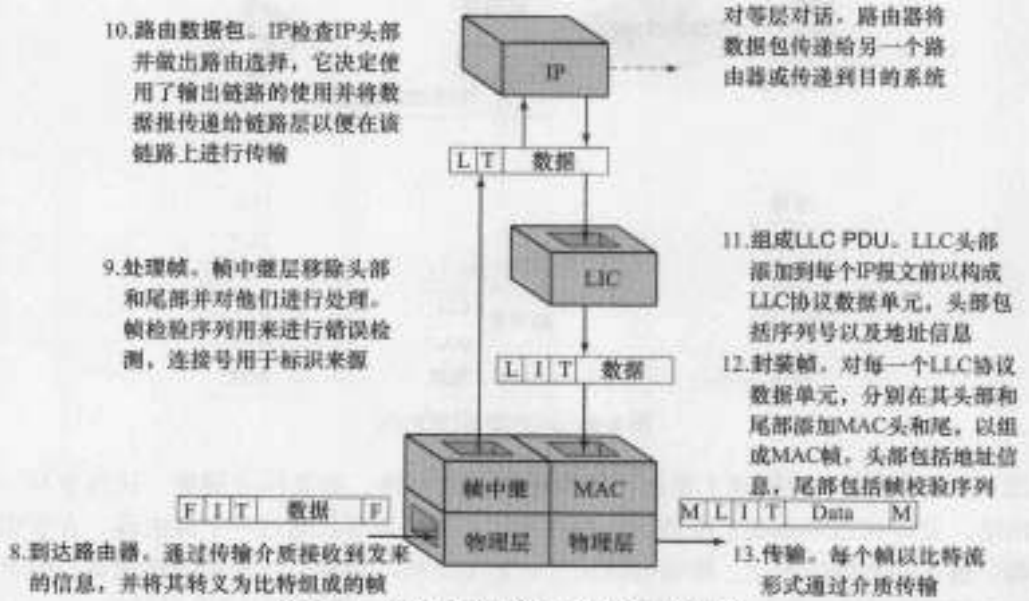


图 8-11　TCP/IP 的运行：路由器上的操作

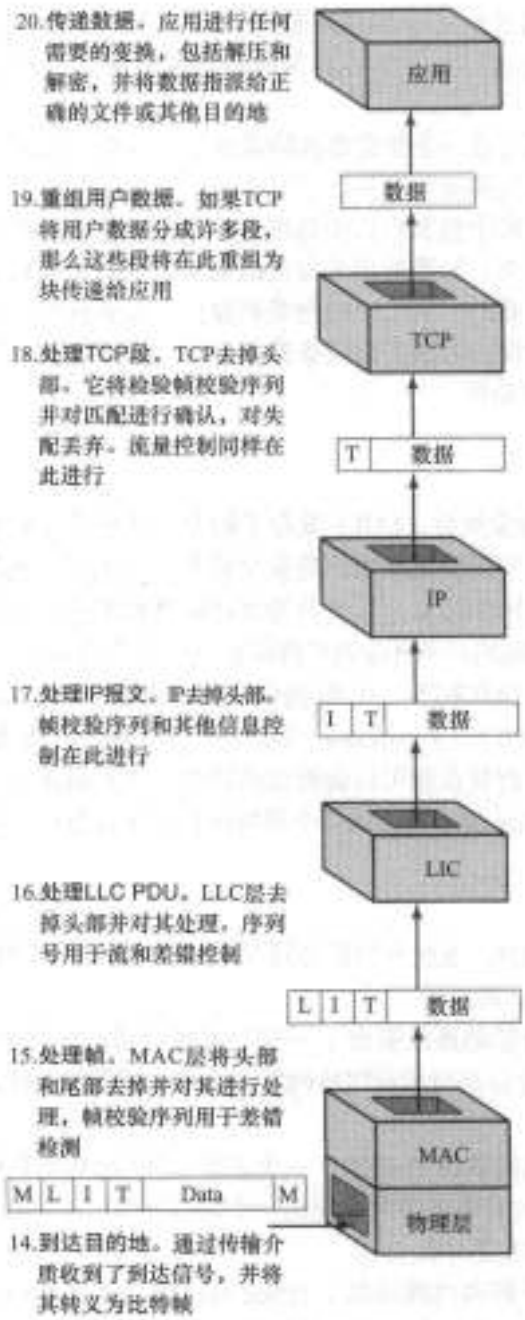


图 8-12 TCP/IP 的运行：接收端的操作

8.4 虚拟专网和 IP 安全

在如今的分布式计算环境下，**虚拟专用网**（VPN）为网络管理员们提供了一个有吸引力的解决方案。本质上来说，一个 VPN 是由一群被一个相对不安全的网络连接起来的计算机所组成的，VPN 使用一些加密方法和特殊的协议来提供安全性保证。在每个企业站点，工作站、服务器和数据库是被一个或多个局域网连接在一起的，这些局域网处于网络管理员的控制下并且能够通过配置和调节来获取高效的性能。因特网或其他公用网络能被用于

相互连接各个站点，能通过使用专用网络来节省成本并为公用网络提供商减小广域网管理负载。同样，公用网络会为远程工作者和其他外出雇员提供一条接入路径来从远程站点登录到公司系统。

但是，网络管理员面对着一个非常基础的需求：安全性。使用公用网络会将公司的流量暴露给窃听者并给未经授权的使用者提供了一个入口。为了解决这一问题，网络管理员可以从多种加密法、身份验证程序包和产品中做出选择。私有化的解决方案带来了一些问题。首先，这个解决方案有多安全？如果使用私有化的加密法或身份验证方案，那么它在技术文献中所述的安全等级是不可靠的。第二个问题是兼容性。没有网络管理员想在选择工作站、服务器、路由器、防火墙等设备时因安全设备的兼容性而受到限制。这是建立因特网标准中网际协议安全性（IPSec）的动机。

8.4.1　IPSec

1994 年，因特网结构委员会（IAB）发布了题为*因特网结构的安全性*（RFC 1636）的报告。这份报告阐述了因特网需要更多更好的安全措施，并为安全机制指定了密钥范围。总的来说就是从未授权监视和网络流量控制方面增强网络基础架构的安全性需求，以及使用身份验证和加密机制来增强终端用户到终端用户网络流量的安全性需求。

为了提供安全措施，IAB 在下一代 IP 协议中将身份验证和加密规定为强制的安全特性，这一特性已经在 IPv6 里推出。幸运的是，这些安全特性被设计成现有的 IPv4 和未来的 IPv6 都可以使用。这意味着厂商现在就可以提供这些特性，并且很多厂商确实现在就在产品里内置了一些 IPSec 功能。IPSec 规范现在以一个因特网标准集合的形式存在。

8.4.2　IPSec 的应用

IPSec 提供了通过 LAN，通过专用或公用 WAN，或通过因特网来增强通信安全的功能。下列是一些使用 IPSec 的示例：

- **通过因特网增强分部的连接安全**：一间公司可以通过因特网或公共 WAN 建立安全的 VPN 连接，这会让公司更依赖因特网并减小对专用网络的需求从而节省成本和网络管理费用。
- **通过因特网增强远程连接的安全**：一个安装了 IPSec 协议的终端用户可以对因特网服务提供商（ISP）进行本地呼叫并获得一个公司网络的安全接入口。这可以节省外派雇员和远程工作者连接的中间费用。
- **同合作伙伴建立外网和内网连接**：IPSec 可以被用来增强与其他公司的通信安全，确保身份验证和保密性并提供密钥交换机制。
- **增强电子商务安全**：尽管一些网络和电子商务应用有内置的安全协议，使用 IPSec 仍然能进一步增强其安全性。IPSec 能确保网络管理员生成的所有流量都被加密并认证，一个额外的安全层会被附加到应用层的任何内容上。

IPSec 这使它的主要特性是它能加密和 / 或鉴别所有 IP 层上的流量能支持多种应用。因此，所有的分布式应用，包括远程登录、客户端 / 服务器、电子邮件、文件传输、网页访问等的安全性都能被增强。

图 8-13 是一种使用 IPSec 的典型场景。一家公司在多个分散地点维护着 LAN，不安全的 IP 流量在每个 LAN 上被传输，通过某种专用或公共 WAN，IPSec 协议在无流量的站点

上被使用。这些协议运行在如路由器或防火墙等网络设备上来将每个 LAN 连接到外部世界。IPSec 网络设备会加密和压缩所有进入 WAN 的流量，并解密和解压所有来自 WAN 的流量，这些操作对 LAN 上的工作站和服务器都是透明的。安全传输对拨号进入 WAN 的独立使用者也是可用的。这些用户工作站必须要实现 IPSec 协议来提供安全措施。

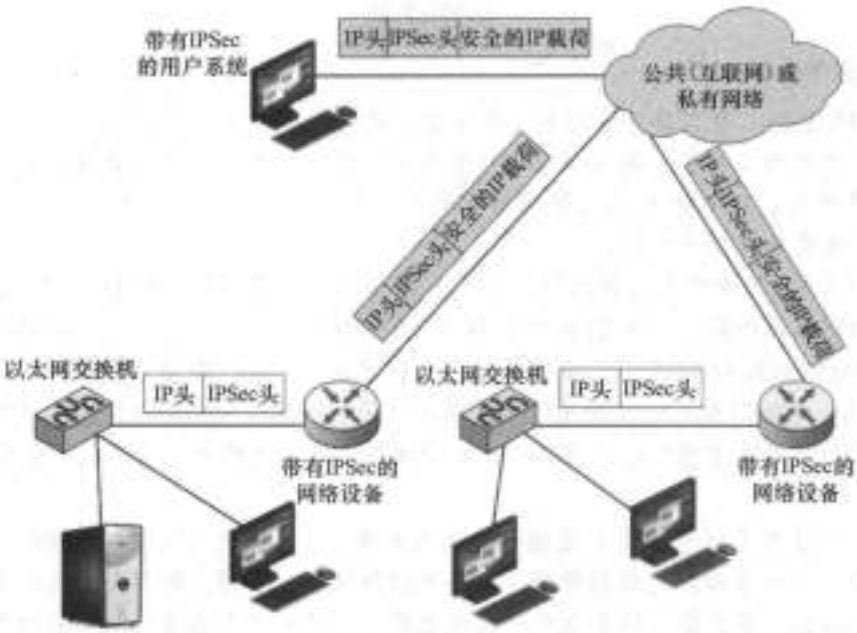


图 8-13 一个 IP 安全方案

8.4.3 IPSec 的益处

下列是一些 IPSec 的有益之处：

- 当 IPSec 被实现在防火墙或路由器上时，它会给所有通过周边的流量带来强健的安全性。公司或工作组内部的流量不会带来安全性相关处理的额外费用。
- 如果所有来自外界的流量必须使用 IP 并且防火墙是从因特网进入该企业的唯一入口，防火墙里的 IPSec 能够抵抗规避防火墙的动作。
- IPSec 位于传输层（TCP、UDP）之下，所以对应用来说是透明的。当 IPSec 被实现在防火墙或路由器上时，不需要对用户或服务器系统上的软件进行改变，甚至当 IPSec 被实现在终端系统、上层软件（包括各种应用）时，也没有影响。
- IPSec 对终端用户也可以是透明的。没有任何必要对使用者进行安全机制方面的训练，只需要对每个使用者发放密钥，或在使用者离开公司时废除密钥。
- 如果有需要的话，IPSec 也能增强独立用户的安全性。这对远程员工以及在公司内部为敏感应用建立安全的虚拟子网都非常有用。

8.4.4 IPSec 的功能

IPSec 提供三个主要功能：一个只有身份鉴别的称为鉴别头（AH）的功能，一个整合身份鉴别或加密的称为封装安全载荷（ESP）的功能，和一个密钥交换功能。对 VPN 来说，通常身份鉴别和加密都是需要的，因为他们对以下两点非常重要：1）确保未经授权的用户不能进入该 VPN；2）确保因特网上的窃听者不能读取在 VPN 上发送的信息。因为这

两个特性通常都是必要的，所以多数实现会采用 ESP 多于采用 AH。密钥交换功能允许自动或手动交换密钥。

IPSec 会在第 19 章进行详细探究。

应用注解

网络实用手册

10 到 15 年前一篇文章描述的关于网络协议的选择和今日有明显的不同。曾经有数个有着竞争型协议堆的模型，每个模型都声称比其他模型更优秀。当多数协议沉浸在他们受欢迎的程度中时，TCP/IP 作为因特网语言最终胜出。如今的网络架构几乎已完全标准化了——至少在使用的协议方面。

在多种 LAN 传输机制之间选择的日子已经过去，令牌环网，FDDI 和 LocalTalk 都被不同形式的以太网所取代。与 TCP 和 UDP 竞争的传输协议也不再存在，Novell 协议（IPX 和 SPX）、Appletalk 和 SNA 都已被替代。在这些竞争的中心，IP 协议登顶称王，而即将到来的是 IPv6。当所有核心协议对我们来说都是可选的时候，我们仍需做出很多选择。新的架构和方法总是期待着推广他们自己的规则和操作，最重大的两个改变是 802.11 无线网络和 IP 语音（VoIP）。

无线网络带来了以下优点：连接不受线路束缚，更快或更低成本的部署和地理上的远程站点连接。另一方面，它同样带来了安全风险的增加、管理上的难题和支持员工需求的增加。这就是说，在选择一项无线网络技术之前，公司必须先决定它是否真的想要支持一个无线网络。甚至即使决定不使用 WLAN，网络管理员仍然需要担心无线连接方面的问题，因为他们被内置在非常多的设备里。所以无论是否在网络管理员的协助下，无线网络通常都会被部署。

当决定采用 802.11，我们现在就必须决定使用哪一个版本。802.11b 让 WLAN 流行起来，但是它不能真正经得起产品网络的严峻考验。因此，两个新标准 802.11g 和 802.11a 被部署。它们有相同的速度峰值，但它们在运行频率、域、覆盖范围和设计参数上都有本质的不同。理论上来说，802.11a 似乎拥有所有的优点，因为他运行在频谱上相对清净的 5-GHz 部分。事实上，因为 802.11g 遵循着与 802.11b 相似的足迹，802.11g 更受欢迎。但不管 WLAN 标准有多受欢迎，他们是设计来增补而不是替代以太网的。然而，最近 802.11n 版本的开发承诺其速度能与有线网络架构匹敌，并且在实际应用中能取代终端节点的以太网连接。

之前我们提到过 IP 是“王”，并且没有任何地方体现得比 VoIP 更明显了。这说明当 IP 成为因特网语言的时候，它同样成为了电话系统的语言。这项技术变得非常高效几乎任何公司都可以提出一个切换到 VoIP 的可行商业案例。所以，现在在数据网络上部署语音时必须为使用何种协议作出更多决定。再一次地，我们有多个有竞争力的解决方案，包括会话发起协议（SIP）、H.323 和 SKINNY。当 VoIP 越来越得到认同，我们开始看到 SIP 在通信领域也得到了更多的支持。可是，H.323 和思科 SKINNY VoIP 电话有着巨大的安装基数，并且还有更多面临投入使用。然而，他们都有各自的难处：H.323 是一个老旧的标准，而 SKINNY 是思科的私有产品。

尽管大部分厂商标准化了 TCP/IP 网络模型，在建立整个通信系统的时候仍有非常多的协议和技术可供选择。很多时候，正确的选择会在越来越多公司采用某些标准集的时候显露出来，但我们必须在正确的时候为我们自己决定是否应该更换标准，或是更换哪一个标准。

8.5 总结

分布式应用需求的通信功能是非常复杂的，这种功能通常被实现为一个结构化的模块集合。这些模块被排列成一个垂直并分层的形式，每一层提供一个部分特定的功能并且在原始功能上依赖下面一层。这种结构被称作协议体系架构。

一个使用这种类型结构的动机是它简化了设计和实现任务。对任何大型软件来说，将功能细分为能够单独设计和实现的模块是一种标准做法。在每个模块被设计和实现出来之后，就可以进行测试了，然后模块们可以被整合并一起进行测试。这一动机引导计算机厂商开发私有的分层协议体系，IBM 的系统网格体系结构（SNA）就是其中一个例子。

一个分层的体系结构也可以被用于建立标准化的通信协议集合。在这种情况下，模块化设计的优点都被保留了。另外，分层体系结构尤其适合标准的开发。在体系结构的各层的协议标准可以同时进行开发，这将工作细分，变得可管理，并加速了标准开发过程。TCP/IP 体系是用于这个目的的标准协议体系。这个架构包含了五层，每一层提供了分布式应用需要的通信功能的一部分，每一层都开发了相应的标准。开发工作仍在继续，尤其在顶层（应用层），并且新的分布式应用仍然在被定义中。

8.6 关键术语、复习题和练习题

关键术语

application layer（应用层）
checksum（校验和）
end system（终端系统）
extranet（外部网）
Frame Check Sequence（FCS，帧检验序列）
header（头部）
intermediate system（中间系统）
Internet（因特网）
Internet Protocol（IP，网际协议，IP 协议）
internetworking（网络互联）
intranet（内部网）
IP datagram（IP 数据报）
network layer（网络层）
Open System Interconnection（OSI，开放式系统互联）
packet（包）
peer entity（对等实体）
physical layer（物理层）
port（端口）
protocol（协议）
protocol architecture（协议体系结构）
Protocol Data Unit（PDU，协议数据单元）
router（路由器）
Service Access Point（SAP，服务接入点）
subnetwork（子网）
Transmission Control Protocol（TCP，传输控制协议）
TCP segment（TCP 字段）
transport layer（传输层）
User Datagram Protocol（UDP，用户数据报协议）

复习题

8.1 什么是协议？
8.2 列出数据通信协议的主要元素。
8.3 什么是协议体系结构？

8.4　什么是协议体系结构中的对等实体?

8.5　列出并简单描述网络接入层中的主要通信功能。

8.6　列出并简单描述传输层中的主要通信功能。

8.7　什么是端口?

8.8　传输协议数据单元（PDU）和网络接入 PDU 有什么区别?

8.9　什么是 TCP/IP ?

8.10　列出并简单描述 TCP/IP 的五个层。

8.11　简单描述以下各 TCP/IP 应用层协议：SMTP，FTP，HTTP。

8.12　简单描述以下子网部件间的区别：主机、终端系统、中间系统。

8.13　简单描述以下中间系统类型间的区别：第 2 层交换机、路由器、网关。

8.14　什么是 VPN ?

8.15　什么是 IPSec ?

8.16　列出一些 IPSec 的应用和优点。

8.17　简单描述 TCP 和 UDP 之间的区别。

8.18　简单解释 IPv4 和 IPv6 之间的区别。

8.19　列出并简单描述路由器的主要功能。

练习题

8.1　在因特网上对 EOIP 和 IPOE 进行一定研究。搜索关于 EOIP 和 IPOE 的资料来源、EOIP 和 IPOE 日益流行的商业原因以及运用 EOIP 和 IPOE 最佳实践的案例。用 750~1000 字的论文或者 8~12 张 PPT 总结你的发现。

8.2　运用图 8-14 的分层模型描述订购和运送披萨的每层交互过程。

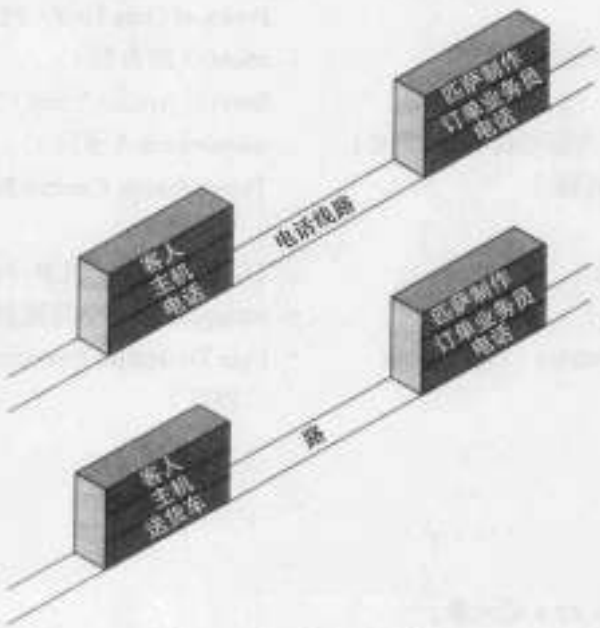


图 8-14　练习题 8.2 的结构

8.3 a. 法国总理与中国总理需要通过电话达成某个协议，但是他们都不会对方的语言。同时，他们也没有翻译人员将一种语言翻译成另一种。然而两个总理都有英语翻译人员。请绘制一幅与图 8-14 相似的图以描述当前场景和各层之间的交互。

b. 现在假设中国总理的翻译人员仅能翻译日语，并且法国总理有一个德语翻译。现在德国有一个德语和日语的翻译。请绘制一幅新的图以反映相应的安排，并且描述这个假设的电话通信。

8.4 为什么分层常见于通信协议中？分层通信协议的优点有哪些？

8.5 列出协议分层方法的主要缺点。

8.6 一个含 1500 比特数据和 160 比特头部的 TCP 分段被发送到 IP 层，然后被附加上另一个 160 比特的头部。然后这个分段会通过两个网络被传送，每个网络使用一个 24 比特的头部。目标网络允许的最大包大小为 800 比特。多少比特（包括头部）在目标网络处被投递给网络层协议？

8.7 对使用 UDP 而不是 TCP（或 TCP 和 UDP 都使用）的协议做一些网络调查研究。写一篇简要的文章来列出并简要描述这些协议。

8.8 IP、TCP 和 UDP 都会直接抛弃到达时存在校验和错误的包，并不会尝试去通知发送者。为什么？

8.9 寻找并观看一些说明 TCP/IP 是怎样工作的 YouTube 视频。列出三个你认为最能清楚描述 TCP/IP 是怎样工作的视频的 URL。说出你认为总体最好的视频并简要说明你选择的理由。

8.10 为什么 TCP 头部包含了头部长度字段而 UDP 没有？

8.11 TFTP 规范的早期版本 RFC783 描述了下面的内容：

除非超时，所有包（用来标识结束的包除外）都会被单独进行确认。

新规范将其修订为如下内容：

除非超时，所有包（重复的 ACK 和用来标识结束的包除外）都会被确认。

这项修订是用来解决被称为“魔法师的学徒”的问题。推论并解释这个问题。

8.12 使用 TFTP 时，影响传送文件所需时间的限制性因素是什么？

注意：接下来三个问题会使用 Wireshark——一款免费的允许用户从 LAN 上捕获网络流量的包嗅探器。本书的讲师材料中包含了一个 Wireshark 工程包。这些练习是供你尝试的额外迷你工程。Wireshark 能运行在多种操作系统上，并且能直接从 Wireshark 网站上下载：www.wireshark.org。

8.13 在从 Wireshark 开始一次捕获后，启动一个基于 TCP 的应用，例如 SSH、FTP 或 HTTP（网络浏览器）。你能从你捕获到的内容中找出下面内容吗？

a. 源和目标的第二层地址（MAC）

b. 源和目标的第三层地址（IP）

c. 源和目标的第四层地址（端口号）

8.14 抓包软件或嗅探器能被作为强大的管理和安全工具。通过使用内置的过滤功能，用户能基于不同的准则来追踪流量并排除掉其他内容。使用 Wireshark 内置的过滤功能来进行下列操作：

a. 只抓取来自你的计算机 MAC 地址的流量

b. 只抓取来自你的计算机 IP 地址的流量

c. 只抓取基于 UDP 的传输流量

8.15　图 8-8 展示了一些直接在 IP 之上运行的协议。Ping 是一个用来测试机器间连接的多系统可用程序。哪一个是 Ping 使用的内置协议？它的载荷由什么组成？提示：你可以使用 Wireshark 来帮助你寻找答案。

8.16　在你的操作系统中安装了哪些解决连接问题或提供连接反馈信息的应用？

8.17　对网络连接详细窗口截图，需要包括主机 IP 和物理地址。

8.18　在 Youtube 上查找并观看路由器工作的视频。记下三个你认为最能够表述路由器工作原理的视频。找出你认为最好的一个，并说明选择的理由。

附录 8A　TCP、UDP 和 IP 详细内容

在学习了 TCP/IP 体系结构和网络互联的基本功能之后，我们现在可以回到 TCP 和 IP 来学习一些细节。

1. TCP

TCP 仅使用一个单一类型的段。图 8-6a 展示了 TCP 头部。因为头部需要适用于所有的协议机制，所以它往往较大，最小长度达到 20 字节。一些字段如下：

- **源端口（16 比特）**：源 TCP 用户。
- **目的端口（16 比特）**：目的地 TCP 用户。
- **序列号（32 比特）**：段中第一个字节数据的序号，设置了 SYN 标记时除外。当设置了 SYN 时，该字段包括初始序列号（ISN）并且段中第一个字节数据的序列号为 ISN+1。
- **确认号（32 比特）**：包括 TCP 实体期望从另一个 TCP 实体收到的字节数据的序列号。
- **头部长（4 比特）**：头部 32 比特字的字数。
- **保留（4 比特）**：保留字段供未来使用。
- **标识（8 比特）**：对于每个标记，当设置为 1 时，其含义如下：

  CWR：拥塞窗口控制。

  ECE：ECN 回应，RFC 3168 中定义的 CWR 和 ECE 位，用于显示的拥塞通知。

  URG：紧急指针字段。

  ACK：确认字段。

  PSH：推送功能。

  RST：重置功能。

  SYN：同步序列号。

  FIN：发送端不再有更多数据。
- **窗口（16 比特）**：流量控制的缓冲额度分配，字节为单位。包括从确认字段中的序列号代表的字节开始，发送端准备接收的字节数据的个数。
- **校验和（16 比特）**：对数据段加上伪头部中每 16 比特字进行求和，再对得到的 16 比特和取反码，将在后面说明。（附录 E 对校验和进行描述）
- **数据紧急指针（16 比特）**：该值，当加入到段序号时，包含了紧急数据序列最后字节的序列号。这样能够使接收器了解即将到来的紧急数据大小。
- **选项（可变）**：包括零个或多个选项。

源端口和目的端口是指发送方和接收方的 TCP 用户。一些固定的号码指派给常用的 TCP

用户；表 8-2 展示了部分示例，因此在任何操作中，这些数字都需保留。其他端口号必须由通信双方共同协商分配。

表 8-2 已分配端口

5 远程作业入口	79 Finger
7 Echo	80 万维网（HTTP）
20 FTP（默认数据）	88 Kerberos
21 FTP（控制）	119 网络新闻传输协议
23 TELNET	161 SNMP 代理端口
25 SMTP	162 SNMP 管理端口
43 Whols	179 边界网关协议
53 DNS	194 因特网中继聊天协议
69 TFTP	389 轻量级目录访问协议

序列号和确认号与字节绑定，而不是与段绑定。例如，如果一个段包含序列号 1001 以及 600 个字节的数据，序列号是指数据字段的第一个字节的序号，下一个逻辑段将包含序列号将是 1601。这样一来，TCP 在逻辑上是面向数据流的：它从用户端接收字节流，按其认为适合的方式组成段，并对数据流中每个字节标注序号，这些序号与窗口一起用于流量控制。这种方案按如下方式工作，对一个从 X 发送到 Y 的 TCP 段来说，确认号是指 X 所期望收到的下一个字节的序数。也就是说，X 已经收到了在此序数之前的所有数据。窗口表明 X 即将从 Y 收到的额外字节数。通过限制窗口值，X 可以限制从 Y 到达的数据速率。

校验码用于错误检测。校验码是基于整个数据段与伪头部计算得出的，其中伪头部为传输端和接收端进行计算时的头部前缀。发送端计算出校验码，并将其添加到段中。之后，接收端对到来的段执行同样的计算，并与收到的段中校验码进行比较。如果两者并不相等，那么在传输中一个或多个比特被意外的改变了。伪头部包括以下几个来自 IP 头部的域：源地址和目的地址、协议以及段长。通过包含该伪头部，TCP 可以保护数据不被误传。也就是说，如果 IP 将一个段传送到错误的主机，即使段没有包含任何错误，接收方 TCP 实体能够检测到传输错误。

2. UDP

UDP 只使用一种类型的段，如图 8-6b。头部包括源端口和目的端口。长度域包括整个 UDP 段长，即头部和数据部分。校验和的计算同 TCP、IP，使用同样的算法。对 UDP 来说，校验和应用于整个 UDP 段加上计算时前缀于 UDP 头部的伪头部，这个伪头部与使用 TCP 协议时的伪头部相同。当检测到错误，整个段被丢弃并且不会做进一步的动作。

校验码域在 UDP 中是可选的，未使用时将其置零。但是，需要指出的是 IP 校验码仅仅适用于 IP 头部，并不适用于数据部分，该数据部分由 UDP 头部以及用户数据组成。因此，当 UDP 并不执行检验和计算时，用户数据无论在传输层或者 IP 层都不会经过任何检测。

3. IPv4

图 8-7 展示了 IP 头部结构，其最小长度 20 字节（160 比特）。包含的域如下：

- **版本（4 比特）**：表明版本号以允许协议更新。值为 4。
- **报头长度（IHL）（4 比特）**：头部字长（32 比特每字）。最小值为 5，因此最小头长度为 20 个字节。

- **DS/ECN（8 比特）**：优先于差异化的服务介绍，该域是指**服务类型**（TOS），并明确说明可靠性、优先级、延迟、以及吞吐量。但这种解读已经被替代。TOS 域的头 6 比特是指 DS（差异化服务），我们将在 11 章进行讨论。剩余的 2 比特为 ECN（显示拥塞通知），这超出了我们的学习范围。
- **总长度（16 比特）**：总共的报文长度，包括头部及数据，以字节为单位。
- **身份证明（16 比特）**：源地址、目的地址、及用户协议等一序列数字用于单独的鉴别数据报。因此，该数应该对数据报的源地址、目的地址、用户协议，在数据报存留于因特网的时间段内保持独一无二。
- **标志（3 比特）**：如今只定义了两个比特。更多比特用于分段及重组，如先前所述。当禁止分段比特位置 1 时表示禁止分段。当了解到目的端不能对片段重组时，该比特就发挥了作用。但是，如果设置了该比特，当数据报超过了途中网络的最大长度限制的话将被丢弃。因此，当设置了该比特，建议使用源路由来避免包长度上限较小的网络。
- **段偏移（13 比特）**：表明段在原始数据报中的位置，以 64 比特为单位计量。这表明除了最后一个分段，其余的数据域必须包括 64 倍数的比特长度。
- **存活时间（8 比特）**：明确指出数据报在因特网中被允许的存留时间，以秒为单位。每个路由器处理数据报时必须将 TTL 至少减一，因此 TTL 在某种程度上与跳数相似。
- **协议（8 比特）**：表明目的端接收数据的更高层协议。如此一来，该域可以鉴别数据报中 IP 头后的下一个头部的类型。
- **头部校验和（16 比特）**：只应用于头部的错误检验码。因为一些头部域在传输过程中可能会改变（如存活时间、分段相关的域），需要通过每个路由器时进行验证及计算。校验和是对头部中所有 16 位字做反码求和运算再取反码得到的。为了计算的需要，校验和域初始化为零。（附录 E 描述该校验码）。
- **源地址（32 比特）**：编码以允许可变化的比特分配来明确表明网络及接入到指定网络中的终端系统，下面将继续讨论。
- **目的地址（32 比特）**：同源地址同样的性质。
- **选项（可变）**：根据发送方用户的需求编码选项。
- **填充（可变）**：用于确保数据报的头部长是 32 比特的倍数。
- **数据（可变）**：数据域必须是 8 比特倍数的整数长度。数据报的最大长度（数据域加上头部）为 65535 字节。

协议域表明了 IP 数据报该发往哪个 IP 用户。虽然 TCP 是最常见的 IP 用户，其他协议也可以访问 IP。对于一些使用 IP 的常见协议，特殊协议号会被分配和使用。表 8-3 列举了部分分配。

表 8-3　一些分配的协议数

1　因特网控制消息协议	17　用户数据报协议
2　因特网组管理协议	46　资源预留协议（RSVP）
6　传输控制协议	89　开放式最短路径优先（OSPF）
8　外部网关协议	

4. IPV6

IPv6 头部的固定长度为 40 个字节，由如下几个域组成（图 8-7b）：

- **版本（4 比特）**：IP 版本数，值为 6。
- **DS/ESN（8 比特）**：对原节点和 / 或转发路由器提供差异化服务和拥塞功能，如 IPv4 DS/ECN 域所描述。
- **流量标签（20 比特）**：主机对需要被网络中的路由器特殊处理的数据包打上标签，将在下面讨论。
- **载荷长度（16 比特）**：IPv6 数据包中紧跟在头部后的剩余数据的长度，以字节为单位。换句话说，这等于所有的扩展头加上传输层的协议数据单元的长度。
- **下一个头部（8 比特）**：鉴别紧跟着 IPv6 头的头部类别，要么是 IPv6 扩展头部，要么是高层协议头，如 TCP 或 UDP。
- **跳数限制（8 比特）**：数据包所允许跳转的剩余次数。跳数由源设置成所期望的最大值，并且每经过一次转发剩余数减一。当跳数限制为零时，数据包将被丢弃。这就是 IPv4 中存活时间的简化版。大家一致认为在 IPv4 中，在计算时间间隔中的花费并没有对协议体现重要的价值。实际上，IPv4 的路由器，按照一般规则，将存活时间看做跳数限制。
- **源地址（128 比特）**：发起数据包的地址。
- **目的地址（128 比特）**：将接收数据包的地址。当路由头是暂时的时候，该地址有可能不是最终的目的地址，将在下面解释。

虽然 IPv6 头部比 IPv4 强制部分长度更长（分别为 40 个字节与 20 个字节），但是 IPv6 包含更少的域（分别为 8 与 12）。因此，路由器对每个头部将做更少的处理，以此将提高路由速度。

附录 8B 简单文件传输协议

附录将简单概括因特网标准简单文件传输协议（TFTP）。我们的目的想向读者提供更丰富的协议介绍。

1. TFTP 介绍

TFTP 比因特网标准文件传输协议（FTP）要简单得多。TFTP 不提供访问控制或用户身份鉴定，因此 TFTP 仅适用于公开访问的文件目录。因为它的简单特性，TFTP 可以轻松紧凑地实现。例如，一些无盘设备利用 TFTP 在启动时下载固件。

TFTP 运行在 UDP 的顶层。TFTP 实体在初始传输时向目标系统 69 端口发送一条 UDP 段的读写请求。该端口被目标 UDP 模块识别并作为 TFTP 模块的标识符。在传输过程中，两端使用传输标志（TID）作为其端口号。

2. TFTP 包

TFTP 实体使用包作为交换命令、响应和文件数据的形式，保存在 UDP 段中。TFTP 支持五种类型的包（图 8-15），头两个字节包含一个操作码用于表明包类型：

- RRQ：读请求包从其他系统请求传输文件的权限，包括由 ASCII[⊖]字节序列组成并以

⊖ ASCII 是信息交换的美国标准编码，由美国国际标准机构制定。它对每一个字母指定独一无二的 7 比特字串，第 8 位用作奇偶校验。ASCII 等价于国际参考字母（IRA），其由 ITU-T T.50 定义。附录 D 提供了对 IRA 编码的描述及列表。

零字节终结的文件名。TFTP 接收实体通过零字节的方式了解文件名何时终结。包还包括了模式域，以此表明数据文件应解释为 ASCII 字节字串还是原始 8 比特数据字节。



图 8-15　TETP 包格式

- WRQ：写请求包请求传输文件到其他系统的权限。
- 数据：数据包块号从 1 初始，并且每个新的数据块号加一。这种规定使得程序可以通过单一数字区分新数据包和包的复制。数据域跨越 0 - 512 字节长度。如果块长度为 512 字节，那么该块不是最后一个数据块；如果块长为 0 - 511 字节，那么它代表传输的终结。
- ACK：该包用于确认收到的数据包或 WRQ 包。数据包的 ACK 包括了已确认的块号。WRQ 的 ACK 包括块号 0。
- 错误：错误包为其他任何类型包的确认。错误码由一个整数表明错误的性质（见表 8-4）表。错误信息是供人类阅读的，因此应使用 ASCII 码展示。和其他字串一样，它将以零字节作为终止符。

表 8-4　TFTP 错误码

值	含　义	值	含　义
0	未定义，请参照错误信息	4	非法 TFTP 操作
1	未找到文件	5	未知传输 ID
2	访问冲突	6	文件已存在
3	磁盘空间已满或超出分配	7	没有该用户

所有除了 ACK 的包（将在下面解释）以及用于终结的包都需要被确认。所有包都能够被错误包确认。如果没有发生错误，将执行下面的例行步骤：WRQ 或者数据包由 ACK 包确认。当 RRQ 发出，在没有错误的情况下另一端开始传输文件作为响应，这样，第一个数据块就作为了 RRQ 包的确认。除非文件传输完毕，每一个从一端发出的 ACK 包都紧跟随着从另一端发出的数据包，这样的话数据包就可以作为一个确认。错误包可以根据环境的不同被任何其他类型的包确认。

3. 传输概述

图 8-17 的例子说明了简单文件从 A 传输到 B 的操作。没有发生错误并且没有讨论选项规范的详细内容。



图 8-16 TFTP 包

操作开始于系统 A 中的 TFTP 模块向系统 B 的 TFTP 模块发送了写请求（WRQ）。WRQ 包作为 UDP 段的主体传输。写请求包括了文件名（在这里为 XXX）和字节的模式码，或原始数据。在 UDP 头部，目的端口号为 69，这告知了 UDP 接收实体该消息是传递给 TFTP 应用的。源端口是由 A 选择的 TID，在这里为 1511。系统 B 准备接收文件，因此返回带有 0 块号的 ACK 作为响应。在 UDP 头部，目的端口为 1511，这使得 A 系统的 UDP 实体将到来的包路由到 TFTP 模块，这样使得该 TID 与 WRQ 的 TID 保持一致。对该文件的传输，源端口是由 B 选择的 TID，在这里为 1660。

在这项初始交换之后，文件传输继续进行。此传输由一个或多个来自 A 的数据包构成，并且每一个都是被 B 承认的。最后一个数据包包含至少 512 字节的数据，它标识着传输的结束。

4. 错误和延迟

如果 TFTP 运行在一个网络或因特网络（与直接数据连接相反）上，包就有可能被丢失。因为 TFTP 是运行在 UDP 上的，它并不能提供一个可靠的传输服务，所以 TFTP 里需要一些机制来处理丢失的包。TFTP 使用常见的超时机制技术。假设 A 发送一个包给 B 来请

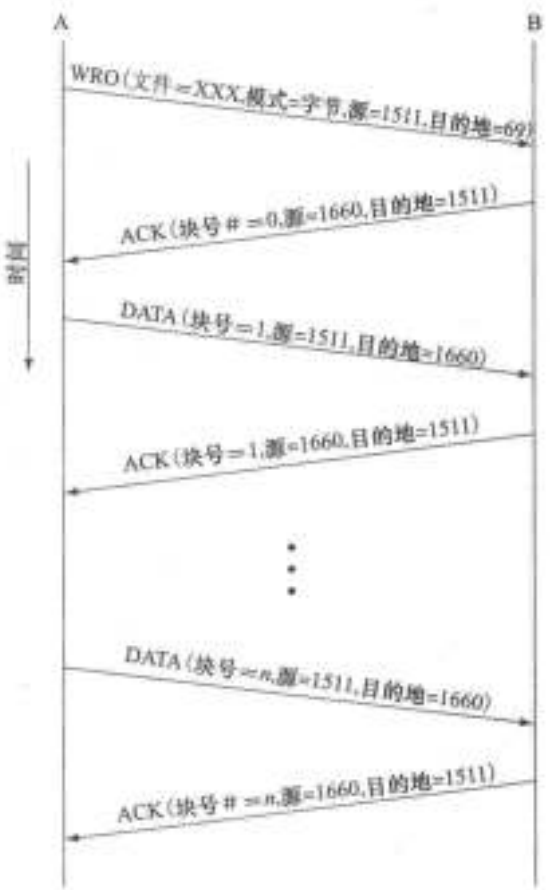


图 8-17 TFTP 操作示例

求一个确认（例如除复制的 ACK 和用于结束通信的包以外的任意包）。当 A 发送了包后，它会启动一个计时器。如果计时器在收到 B 的确认以前过期的话，A 会重新发送同样的包。如果初始的那个包确实丢失了，那重新发送的那个包将是 B 收到的第一份副本。如果初始包没有丢失，但是来自 B 的确认却丢失了的话，B 将会收到两份同样的副本并简单地都对它们进行确认。因为使用了块序号，所以这并不会引起混淆。这项规则里唯一的例外是重复的 ACK 包，第二个 ACK 会被忽略。

5. 语法、语义和时间安排

在 8.1 节中提到过，一个协议的核心特性可以被归纳为语法、语义和时间安排。这些分类可以很容易在 TFTP 里看到。不同 TFTP 包的格式构成了协议的语法。协议的语义体现在每种类型的包和错误代码的定义中。最后，包被交换的顺序、块序号的使用和计时器的使用都是时间安排在 TFTP 中的体现。

客户 / 服务器、内部网及云计算

学习目标

通过本章的学习，读者应该能够：

- 讨论客户 / 服务器计算系统利润增长的原因，以及系统的可用性。
- 描述客户 / 服务器计算的特点和性质。
- 描述客户 / 服务器应用的体系结构。
- 说明中间件在客户 / 服务器系统中的角色。
- 评价客户 / 服务器计算的网络需求及影响。
- 定义内部网，并将其与因特网比较。
- 比较客户 / 服务器与内部网的分布式计算方法。
- 列举外部网的好处和通信选项。

大多数商业环境下的分布式应用都涉及一种分布式计算，称作客户 / 服务器计算。首先，本章对客户 / 服务器原理和它对商业的意义进行大致描述。其次，我们将了解客户 / 服务器架构提供的应用支持的性质。最后，我们将学习重要的中间件概念。

通过对客户 / 服务器计算的调查，我们将学习到一种较新的方法——内部网。内部网使用因特网技术和应用（特别是基于网络的应用）为分布式应用提供内部支持。之后，本章会介绍外部网的概念。最后，我们将学习越来越重要的面向服务体系结构（SOA）。

9.1 客户 / 服务器计算的增长

客户 / 服务器计算及相关概念在信息技术系统中越来越重要。正如计算机领域的其他新浪潮一样，客户 / 服务器计算拥有它自己的一套术语。表 9-1 列举了在客户 / 服务器产品和应用描述中经常使用的一些术语。

表 9-1 客户 / 服务器术语

应用程序编程接口（API）
允许用户和服务器相互交流的一系列函数和调用程序
客户
联网信息的请求者，通常是个人计算机或者是工作站查询数据库或从其他服务器获取信息
中间件
一系列驱动器、API 或其他用于改善客户应用程序和服务器间连通性的软件
关系数据库
一个数据库，其中的数据访问仅限于满足所有查询条件所选择的行
服务器
计算机，通常是一台高性能的工作站或是一台大型机，用于管理联网客户端操作的信息
结构化查询语言（SQL）
由 IBM 开发并由 ANSI 标准化的语言，用于寻址、新建、更新或查询关系数据库

图 9-1 试图阐述这些主题的本质。典型的**客户**机是为终端用户提供较高友好性接口的单一用户个人计算机或工作站。基于客户端的工作站通常对用户展示最舒适的图形化界面，包括窗口和鼠标的使用。常见的界面例子如 Windows 和 Macintosh OS X。基于客户端的应用专门为易用性而设计，包括电子表格等常见工具。

每个在客户 / 服务器环境中的**服务器**都为客户提供一系列共享的用户服务。最常见的服务器类型是数据库服务器，通常控制着一个关系数据库。服务器允许多个用户共享同一个数据库的访问权限，还允许使用高性能的计算机系统来管理数据库。



图 9-1　通用客户 / 服务器环境

除了客户和服务器，**网络**是客户 / 服务器环境中第三个重要的成分。客户 / 服务器计算是一种分布式计算。用户、应用和资源为了满足商业需求，以分布式存在并且由单一的局域网或广域网或由互联网连接。

客户 / 服务器有许多特性使得它区别于普通的分布式进程：

- 客户 / 服务器非常依赖于提供用户友对性应用的用户系统。这使得用户能够很好地对时间及计算机的使用类型进行掌控，同时部门级经理能够对本地需求做出相应的响应。
- 虽然应用程序是分散的，但将企业数据库、网络管理和工具函数进行集中化有着重要的意义。这使得企业管理能够覆盖在计算和信息系统上整个资本投资的控制，企业管理还能够提供互操作性使得系统可以紧密地绑在一起。同时，它减少了个别部门维持复杂计算机基础设施所需的管理费用，并允许它们选择只用于获取数据和信息的任意类型的机器和接口。
- 开放性模块化系统有着重要的作用。它意味着用户在选择产品时和从多个买主的产品中组合设备时有更好的选择。
- 网络是操作的基础。因此，网络管理和网络安全在组织和操作信息系统中有着高优先级。

一方面，从产品的观点看，客户 / 服务器计算是一种自然的解决方案，因为它利用了成本下滑的微型计算机和网络。另一方面，客户 / 服务器计算可能是支持业务组织的商业方向的最理想的选择。

后者观点需要进一步的阐述。客户 / 服务器计算在行销中的成功不仅是因为旧的解决方案上的新术语，客户 / 服务器计算确实是相对新鲜的分布式计算技术方法。除此之外，客户 / 服务器计算能够响应组织业务的新方法，还能为组织业务创造实在的条件。让我们考虑工业中可以解释这个观点的两个重要趋势。

第一个例子是公司为了在激烈竞争的市场中取得成功，进行永久的裁员以缩小规模和简化结构。为什么公司需要裁员以保持竞争力？如何快速提高生产率以增长销量并控制薪资增长？因强制福利增加带来的工资上涨，每名雇员的成本在迅速增加。同时，业务设备成本也在以极其平缓的速度增加，尤其是计算机和网络设备及服务。这将导致可以预见的计算机及其他信息技术投资的潜在增加，以弥补较小的员工基数。

这种趋势发生在大小型业务中，并影响中层管理者如文职人员。客户/服务器计算提供的是自动化任务和消除获取信息障碍的方式，这使得公司能够排除重重管理，同时新增业务而不增加员工。

另一个可以说明客户/服务器计算功效的趋势被称为内部市场。这是一个业务策略，它作用于主要的大型业务，这种策略将创业热情和企业实力相结合以追寻两个优势：大型业务的经济规模以及小型业务的灵活性。在科技和市场迅速变化的时代，许多大型企业摒弃了传统的功能性层次结构并收集相对独立的业务单元来代替，这些单元需要与外部企业竞争。在内部市场中，每一个业务单元作为独立的公司来运行。每一单元从内部资源（公司中的其他单元）或外部供应商那里采购原料，包括传统"管理部门"，如信息系统、财务、法律，都需要向其他单元销售自己的服务并与外部的供应者进行竞争。

这种内部竞争可以用于改变传统商业方法的瑕疵。如 MIT 的 Jay Forrester 所说 [ROTH93]："一些美国公司是世上最大的官僚主义。他们有中央计划、中央对资本的所有权、中央的资源分配、对人类主观的评估，而缺少内部的竞争，并且顶层管理会根据政治压力做决策。"

内部市场已经改变了一些公司，并很有可能继续影响其他公司。但是，至今为止还存在一个不能克服的障碍。在一个大型公司中，使用内部市场会导致关于自身和外部成千的决策需要确定。这样的话，产生的交易总账就需要协调了。分析认为管理账户中的开销和复杂性会毁掉内部市场带来的好处。计算机技术的发展克服了这个障碍，如今，许多跨国公司使用架设在客户/服务器网络的最新数据库软件来建设内部市场。

9.2 客户/服务器应用

客户/服务器体系结构的主要特点是分配应用级的任务给客户和服务器。图 9-2 列出了通用实例。在客户和服务器端，最基本的软件是运行在硬件平台的操作系统。客户和服务器的平台及操作系统可能有所不同。实际上，在一个单一环境中可能存在许多不同类型的客户平台和操作系统，还有其他不同类型的服务器平台、操作系统。但只要特定的客户和服务器共享相同的通信协议并支持相同的应用，这些级别较低的差别无关紧要。

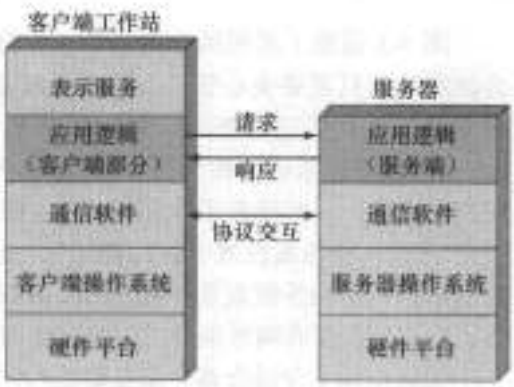


图 9-2 通用客户/服务器体系结构

通信软件使得客户和服务器进行相互操作。最基本的例子是 TCP/IP 协议。当然，这种辅助软件（通信和操作系统）的全部作用是为分布式应用提供基础。理想情况下，应用所提供的实际功能可以通过某种方式拆分为客户和服务器部分，这样一来可以优化网络资源和平台，并加强用户执行各种任务的能力，以及与另一个使用共享资源的用户合作的能力。在一些情况下，这些要求决定了许多应用软件在服务器端执行，另一些情况下，大多数应用逻辑处于客户端。

客户/服务器环境成功的一个关键要素是用户与系统交互时，把系统视作一个整体。这样一来，为客户机设计用户界面至关重要。在大多数客户/服务器中，提供**图形用户界面**（GUI）十分重要，图形界面使用容易、学习简单，并且它还十分强大、灵活。这样一来，我

们能够想出一种在客户工作站的展示服务模型[⊖]，客户工作站负责为分布式应用提供环境中可用的用户友好界面。

9.2.1　数据库应用

作为阐述客户和服务器间分布式应用逻辑的例子，我们考虑最常见的客户/服务器应用家族——使用关系数据库的应用。在这种环境下，服务器本质上是一个数据库服务器。客户服务器间的交互是交易的形式，即客户发出一个数据库请求，并接收到一个数据库响应。

图 9-3 表明这种系统的大致结构。服务器负责维护数据库，为了实现这个目的，需要一个复杂的数据库管理系统。那些使用数据库的应用可以安装在客户端上，链接客户和服务器的桥梁是软件能够使用户向服务器数据库发出访问请求。结构化查询语言（SQL）是这种逻辑的常见例子。

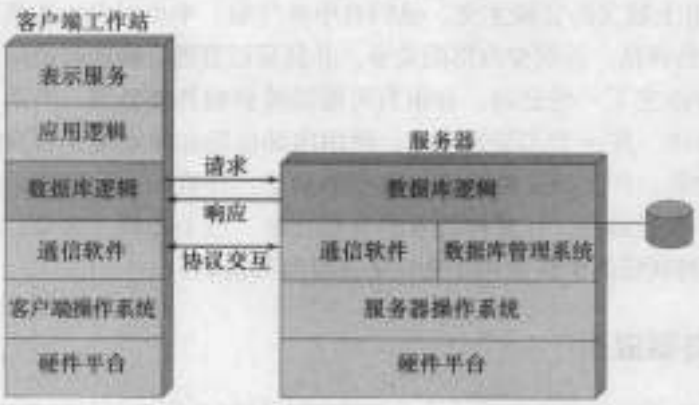


图 9-3　数据库应用的客户/服务器结构

图 9-3 说明了所用的应用逻辑——位于客户端的数字压缩和其他数据分析的软件，另一方面服务器只需要关心管理数据库。配置的正确与否依赖于应用的风格和意向。例如，主要目的是提供在线记录查询。图 9-4a 表明了它是如何工作的。假定服务器维护 100 万条记录（在关系数据库术语中称为行），并且用户若执行查询，服务器会返回 0 条、1 条或多条结果。用户可以使用一些搜索条件来查询这些记录（例如，早于 1992 年的纪录；俄亥俄州的个人相关记录；有特殊属性或事件的记录）。最初的客户查询会产生 100 000 条记录符合搜索条件，之后用户新增额外搜索条件并发出新的查询。这次，响应表明有 1000 条可能的记录返回。最终，客户发出带有额外条件的第三次查询，符合搜索条件的结果只有一条，记录返回给客户。

上述应用十分适合客户服务器结构，原因有两点：

1）排序和查询数据库的工作量巨大。这需要大容量硬盘或多个硬盘、高速处理器和高速 I/O 结构。对单一用户工作站或个人计算机来说，这样的容量和功率太过昂贵了。

2）将整个百万记录的文件传输到客户端以供搜索会对网络带来极大的负担。因此，对服务器来说，仅代表客户获取记录还不够，服务器还需要拥有数据库逻辑以代表客户执行搜索。

现在考虑图 9-4b 的场景，服务器也拥有同样的百万记录的数据库。在这样的情况下，单

⊖ 不应把客户工作站的表示服务模块与 OSI 模型的表示层混淆。表示层涉及数据格式的转换，以便于两个通信机器之间能够正确解释通信数据。表示服务模块涉及用户与应用之间交互的方式、屏幕上呈现给用户的布局与功能。

条查询导致了300 000条记录通过网络传输。这种情况会在当用户需要在多条记录（甚至整个数据库）中找到关于某个域的整个累计值或中值时发生。

显而易见的是，后者的场景是不能被接受的。一种解决方法是，在保留客户/服务器结构所有优势的情况下，将部分应用程序逻辑移交到服务器上。也就是说，服务器拥有了应用程序逻辑来执行数据分析和数据获取以及数据搜索。



图 9-4 客户/服务器数据库使用方法

9.2.2 客户/服务器应用的类别

在大体的客户/服务器框架下有着不同的执行方法，这些方法将客户服务器之间的工作区分开来。具体的数据传输和应用程序的执行依赖于数据库信息的属性、支持的应用类别、供应商设备的可互操作性以及在企业中的使用模式。

图 9-5 说明了一些数据库应用的主要选项。也可以进行另一些拆分，对其他类型的应用来说这些选项会有不同的属性。在任何情况下，理解该图并试图学习均衡的理念是十分有用的。

图 9-5 描述了四种类别：

- **基于主机的运算**：基于主机运算并不是真正意义上术语上讲的客户/服务器计算。相反，基于主机的运算指的是传统的主机环境下，所有或几乎所有虚拟计算均由中央主机完成。通常用户接口是通过一个非智能终端。即使用户使用了一台微型计算机，用户工作站点始终也仅仅扮演终端模拟器的角色。
- **基于服务器的运算**：最简单的客户/服务器配置类别，客户主要负责为用户提供图形界面，而几乎所有的运算都在服务器完成。
- **基于客户端的运算**：另一种极端情况是，所有的应用程序运算在客户端完成，除了对数据有效性例行检测和数据库逻辑函数在服务端完成。通常，一些更为复杂的数据库逻辑函数处于客户端。这种结构可能是现今使用的最常见的客户/服务器模式，它使得用户可以根据本地的需求量身定制应用程序。
- **合作运算**：在合作运算的配置中，应用运算以一种最优化的方式执行，这种方式既利用了客户端和服务器端的优势，还利用了数据传输的优点。这种配置建立和维护起来更为复杂，但是从长远的角度考虑，这种类型的配置比起其他客户/服务器方式来说能够提供更好的用户生产力和网络效率。

图 9-5c 和图 9-5d 表明了相当一部分的工作处于客户端时的配置。这种被称为**胖客户端**的模型在应用开发工具中十分流行，如 Powersoft 公司的 PowerBuilder。由这些工具开发的应用程序通常在大体范围上是分部的，它可以支持 25 到 150 个用户。胖客户端模型的主要优势是他可利用台式机能源，从服务器加载应用程序并使它们更有效率且更不容易成为瓶颈。

然而，胖客户端策略也有许多缺点。随着额外功能的迅速增长，客户端的体积已超过台式机的容量，这使得公司不得不更新设备。当这种模型的范围超过现有的分部而无法合并更多用户时，公司必须安装高容量的局域网以支持在胖客户端和瘦服务器间的大量传输。最后，这种模式很难维护、升级以及替换分散在数千台计算机上的应用。

图 9-5b 是**瘦客户端**、胖服务器方式的代表。这种方式几乎是模仿传统的中央主机模式，同时它还可用于将企业级应用从主机模式改变为分布式环境。

图 9-6 表明五种在客户端和服务器间，基于分布式计算服务的客户 / 服务器的类别。每一种类别由客户端的功能定义。



图 9-5　客户 / 服务器应用分类

	瘦客户端 ← → 胖客户端				
计算服务	分布式演示	本地演示	分布式应用逻辑	本地应用逻辑	
演示服务	共享	客户端	客户端	客户端	客户端
应用服务	服务器	服务器	共享	客户端	客户端
数据服务	服务器	服务器	服务器	服务器	共享

图 9-6　客户 / 服务器三级结构框架

9.2.3　三层客户 / 服务器结构

传统的客户服务器结构包括两个级别（层）：客户层和服务器层。近年来，三层结构变得越来越常见了（图 9-7）。在这种结构中，应用软件分布在三种类型的机器中：用户机、中层服务器、终端服务器。用户机就是我们讨论过的客户机，在三层模型中，通常是一个瘦客户端。中层机本质上是瘦客户端和数种终端数据库服务器的网关。中层机还可以转换协议和将一种数据库类型的查询映射到另一种上。除此之外，中层机还可以将不同数据源的结



图 9-7　三层客户 / 服务器结构

果融合。最后，中层机可以作为台式机应用和后端遗留应用间的网关，对两个世界进行调节。

中层服务器和后端服务器的交互同样遵循客户/服务器模型。因此，中层系统同时扮演客户端和服务器。

9.3 中间件

客户/服务器产品的发展和使用已经从物理层到应用层各方面远远抛弃规范的分布式计算。这种标准的缺失使得执行一个整合的、多供应商的、企业范围客户/服务器的配置十分困难。因为客户/服务器方法的优势与它自身的模块化属性和混合并匹配多平台和应用以提供业务方案息息相关，因此，互通性的问题必须解决。

为了实现客户/服务器方法带来的确实利益，开发者需要一套可以提供统一方法和风格的跨平台系统资源访问工具。这样可以使程序员开发的应用程序在不同的个人计算机和工作站上不仅仅表面上相似，更能够使用相同的访问数据方法而不考虑数据的位置。

最常见的解决方法是在应用程序和通信软件以及操作系统间使用标准编程接口和协议。这种标准接口和协议被称作**中间件**。有了标准编程接口，在不同类型的服务器和工作站上实现同一个应用变得容易起来。不仅客户从中获利，供应商同样愿意提供这种接口。原因是客户需要购买的是应用程序而不是服务器，客户仅会选择可以运行应用程序的服务器产品。标准化协议同样需要将不同的服务器接口与需要访问服务器的客户端连接。

中间件组件有许多不同的种类，从最简单的到非常复杂的。他们的共同点是可以将不同网络协议和操作系统的复杂度和差异性隐藏。客户和服务器供应商通常提供许多流行的中间件组件作为选择。这样一来，用户可以选定一个特殊的中间件策略并从不同供应商中选择支持这种策略的设备进行组装。

9.3.1 中间件结构

图 9-8 表明中间件在客户/服务器结构中的角色。中间件成分的实际角色由客户/服务器计算的风格所决定。重新观察图 9-5，回忆一下有哪些不同的客户/服务器方法，由应用程序划分方法决定。但无论如何，图 9-8 表明了这种结构的大致想法。

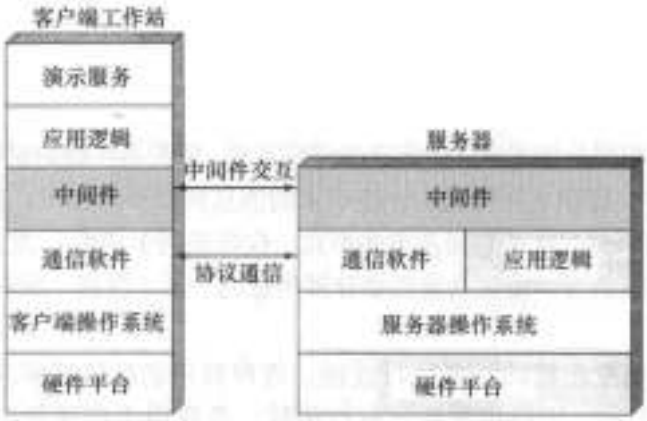


图 9-8 中间件在客户/服务器结构中的角色

值得注意的是，客户端和服务器部分都有一个中间件。中间件的主要目的是使客户端的

用户或应用程序可以访问服务器上的不同服务而不必碍于服务器之间的差异。一个具体的例子是结构化查询语言（SQL），其提供给本地或远程用户一个标准化访问关系数据库的方法。然而许多关系数据库供应商，虽然他们支持 SQL，但还是添加了许多他们自己拥有的扩展。这使得供应商能够差异化他们的产品但同时也带来了潜在的不兼容性。

举一个例子，一个分布式系统，除了其他部门外，还用于支持人事部门。基本的雇员数据，如雇员名和地址，储存在 Gupta 数据库，而工资信息储存在 Oracle 数据库。当人事部门的用户查询特殊的记录时，用户并不想知道究竟哪个供应商数据库包含了他所需要的记录。中间件就提供了这样一个软件层用于统一对不同系统的访问。

从逻辑的角度而不是实现的角度来观察中间件的角色很有启发性。这种角度在图 9-9 中展示。中间件实现了分布式客户 / 服务器计算的承诺。整个分布式系统可以看做一组对用户可用的应用程序和资源。用户不需要考虑数据的位置或应用程序的确切位置，所有的应用操作通过统一的**应用程序编程接口**（API）进行。中间件，横跨了整个客户和服务器平台，负责将用户请求路由到正确的服务器。

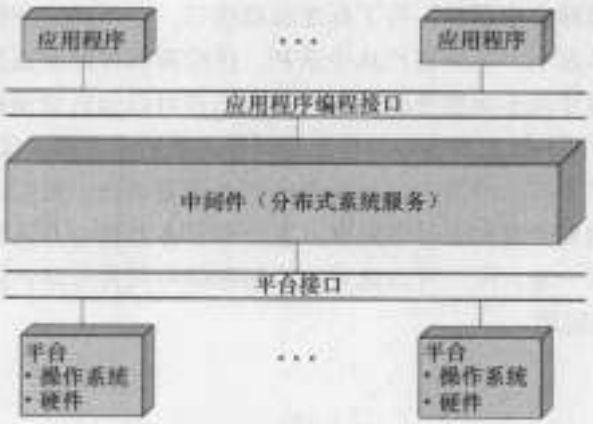


图 9-9　中间件逻辑视图

虽然有许许多多不同种类的中间件产品，但这些产品通常都基于以下三者之一的机制：信息传递、远程过程调用以及面向对象机制。本节剩余部分将会对这些机制做简单的概述。

9.3.2　消息传递

图 9-10a 展示了利用分布式消息的传递来完成客户 / 服务器功能的过程。客户进程需要一些服务（如读取文件、打印）并发送包含该请求的消息到服务器进程。服务器进程执行该请求并发送含有回复的消息。这是它最简单的形式，仅需要两个功能：发送和接收。发送功能制定目的地并包括信息内容。接收功能需要分辨信息的来源（包括“所有人”）并为即将到来的消息提供缓冲区。

图 9-11 展示了消息传递的一个执行过程。进程利用消息传递模块的服务。服务请求可以由原语和参数表示。原语用于指定执行函数，参数用于传递数据控制信息。原语的确切格式由信息传递软件决定。它有可能是进程调用或者它自身是传递给操作系统进程的消息。

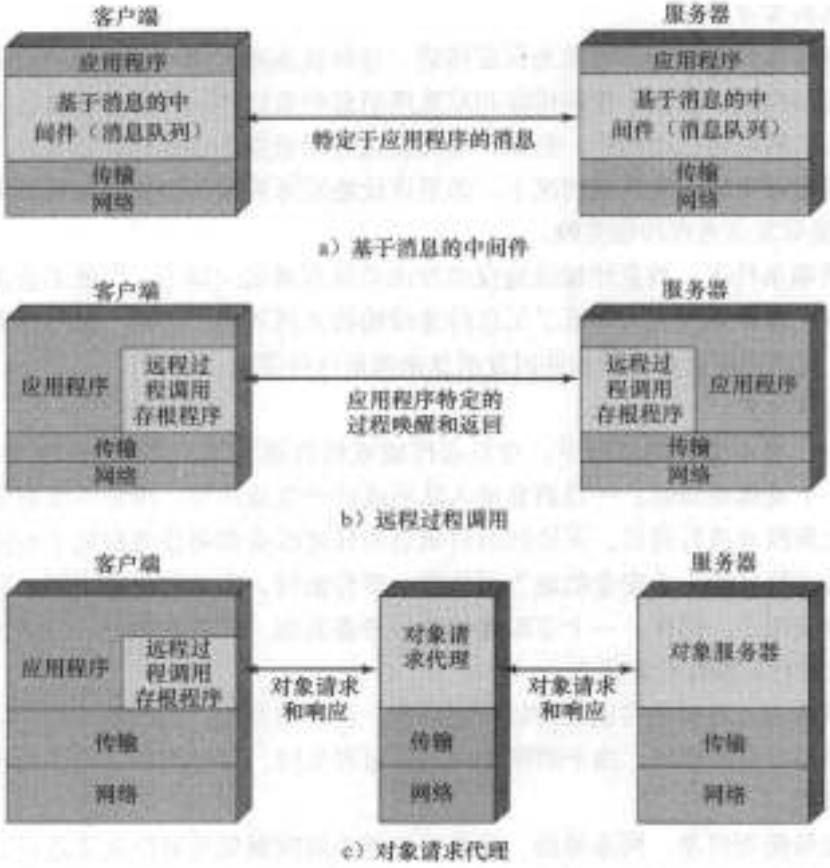


图 9-10 中间件机制



图 9-11 基本消息传递原语

发送原语用于进程发送消息，它的参数是目标进程的标识符和消息的内容。这种数据单元通过一些通信工具（如 TCP/IP）被发往目标进程的主机。当数据单元在目标系统被接收，它由通信设备路由到消息传递模块，该模块检验进程 ID 并为目标进程将消息储存在缓冲区里。

在这种情况下，接收进程必须告知它准备接收消息并为消息指定一块缓冲区域，同时使用接收原语通知消息传递模块。另一种方法不需要发出这种通知，而是当消息模块接收到消息时，它通过一种接收信号通知目标进程，并使已接收的消息存放在共享缓冲区中。

有许多设计问题涉及分布式消息传递，这些问题都会在章节剩余部分着重说明。

1. 可靠性和不可靠性

可靠消息传输设施能够尽可能地保证传输。这种设施将利用可靠传输协议或其他类似的逻辑来执行差错检测、确认、重新传输和对乱序消息的重排序。因为传递被保证了，没有必要让发送进程了解消息已经到达。然而，通知发送进程消息已经被确认很有用，这样的话它就能知道传递已经完成。在其他情况下，如果该设施发送失败（如长时间网络失败、远端系统崩溃），会通知发送进程传输失败。

在其他极端条件下，消息传输设施仅会发出消息到通信网络中，但既不会报告成功，也不会报告失败。这种替代大大降低了消息传递设施的处理和通信开销。对那些需要确保消息传递的应用，应用程序自身会请求并回复消息来满足这种需求。

2. 阻塞和非阻塞

在非阻塞、异步原语的情况下，在发起传输或接收原语时，进程是不会中止的。因此，当进程发起一个发送原语时，一旦消息进入队列或已经完成拷贝，操作系统就会将控制权返还给进程。如果没有进行拷贝，无论何时对消息的任何改变都将使进程处于危险之中。当消息已经被传输或拷贝到一个安全的地方用作进一步传输时，发送进程被中断，它被告之消息缓冲区可能被重用了。同样，一个非阻塞接收由进程发起，并接着执行。当消息到达时，进程被中断，或进行周期性轮询状态。

非阻塞原语为进程提供对消息传输设施高效、灵活的使用。它的缺点是难以测试以及难以调试使用这些原语的程序。由于时间序列的不可再生性，与时间相关的序列可能会带来微小但困难的问题。

替代方法是使用阻塞、同步原语。阻塞发送并不将控制权返回给发送进程，直到消息已经被传输（不可靠服务）或直到消息已经被发送并收到消息确认（可靠服务）。阻塞接收并不返还控制权，直到消息已经被放置在分配的缓冲区中。

9.3.3　远程过程调用

基础消息传递模型的一种演变即是远程过程调用（RPC），它是一种在分布式系统中常见的封装通信方法。这种技术的本质是允许不同机器上的程序可以通过使用简单的调用/返回语义过程进行交互，就像两个程序运行在同一台机器上。也就是说，过程调用是用于远程访问服务的。这种方式的流行源于以下几个优势：

1）过程调用是被广泛接受、使用以及可以抽象理解的。

2）RPC 的使用使得远程接口可以被指定为一组带有指定类型的命名操作。这样一来，接口可以清楚地归档，同时分布式程序可以从数据上进行类型差错检测。

3）因为指定了标准化的、精确定义的接口，应用程序的通信代码可以自动生成。

4）因为指定了标准化的、精确定义的接口，开发者可以写出客户和服务器模块，这些模块可以在计算机和操作系统之间转移并且只需要很少的修改和重新编码。

RPC 机制可以被视作一个改良的可靠阻塞消息传输。图 9-10b 表明了大致的结构，图 9-12 提供了一个更详细的介绍。调用程序发出一个带有其机器上参数的正常过程调用。例如：

$$\text{CALL } P(X, Y)$$

其中，P= 过程名，X= 传递的参数，Y= 返回值。

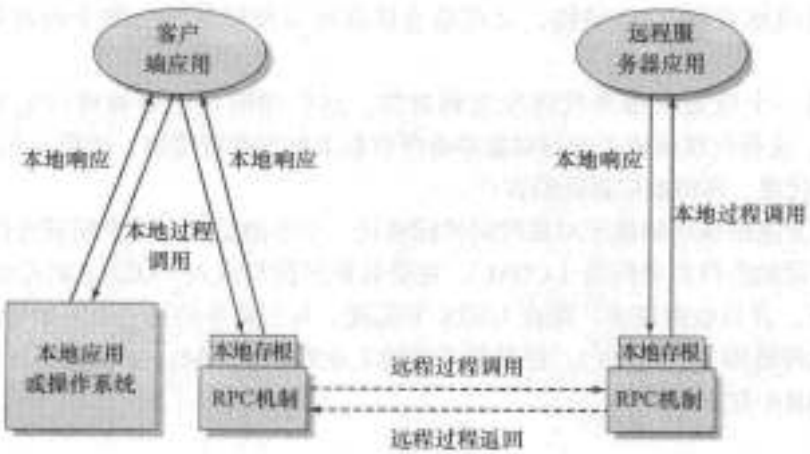


图 9-12 远程过程调用机制

对用户来说，唤起其他机器上远程过程的意图可能不是透明的。虚拟过程 P 必须包含在调用者的地址空间中或在调用时动态连接到的地址空间中。该过程创建一条用于标示被调用过程的消息，同时包含参数。之后它将消息传送给一个远程系统并等待回复。当收到回复后，这个虚拟过程将返回值返回给调用程序。

在远程机器上，另一个虚拟程序与调用过程联合在一起。当消息到来时，它首先被检查并且生成本地的 CALL $P(X, Y)$。这个远程过程被本地调用，因此它关于如何找到参数、栈的状态等设想与纯粹的本地过程调用完全相同。

图 9-13 表明了控制 RPC 操作的流程。

3. 客户/服务器绑定

绑定是指在远程过程和调用程序之间的关系建立的过程。绑定在两个应用程序已经建立了逻辑连接并准备交换命令和数据时形成。

非长期绑定是指在两个处于 PRC 的进程之间建立逻辑连接，并且当返回值时，该连接被拆除。因为连接需要两个终端维护信息状态，因此会消耗一定的资源。这种非持久性绑定就用于保存资源。从另一方面来说，当远程过程被同一调用器频繁调用时，非持久性绑定建立连接的开销就变得不那么合适。



图 9-13 RPC 流程

有了**长期绑定**，建立的 RPC 连接在过程返回后将继续保持，这个连接可以用作之后的 RPC。如果在特定的某段时间内没有连接活动，那么该连接将会被终止。对重复调用远程过程的应用来说，长期绑定将维护逻辑连接并允许一序列的调用和返回使用同一连接。

9.3.4 面向对象机制

随着面向对象技术在操作系统设计中越来越流行，客户/服务器的设计者开始接纳这种方法。在这种方法中，客户和服务器将消息传递在对象之间。对象间的通信可能会

依赖于底层的消息或者 RPC 结构，又或是直接在顶层操作系统上基于面向对象性能进行开发。

客户需要一个服务将请求代理发送到对象，这就像网络中所有可用远程服务的目录（见图 9-10c）。这种代理调用正确的对象并将所有相关数据进行传递。之后远程对象服务处理请求并回复给代理，再将响应返回给客户。

面向对象方法的成功依赖于对象机制的标准化。不幸的是，在这个领域有许多竞争设计。一个是微软公司的组件对象模块（COM），它是对象连接与嵌入（OLE）的基础。COM 使用在 Windows 下，并且也由许多厂商在 UNIX 下实现。与它竞争的是，由对象管理组开发的公共对象请求代理结构（CORBA），它有着广泛的工业背景。IBM、Apple、Sun 和其他许多厂商都支持 CORBA 方法。

9.4　内部网

内部网是指在公司组织内部使用因特网技术，而不是将其连接到全球因特网。这种概念使得商业数据通信历史发生了剧大的方向性改变。各方面测评显示，包括厂商的产品结果、客户意向结果、实际产品部署甚至书店中的上架书，内部网都以非常快的速度吸引着企业的注意，超过了个人计算机、客户服务器计算，甚至因特网和广域网。

这些变化的原因在于内部网企业计算引人注目的特点和优势，包括以下几项：

- 快速的原型制作和新服务部署（几小时或几天内）。
- 有效扩展（根据需要从小规模做起）。
- 几乎不需要对用户、开发者做培训，因为服务和用户的接口与因特网相似。
- 可以在几乎所有平台上完成，并保持完整的互操作性。
- 开放式结构意味着可以从不同平台上获取越来越多的附加应用。
- 支持大部分分布式计算结构（少数中央服务器或许多分布式服务器）。
- 结构化来支持对传统信息源的整合（数据库、现有的文字处理文档、组建数据库）。
- 支持大部分多媒体类型（音频、视频、可交互应用）。
- 低廉的起步，以及对新软件或新设施的少量投资。

使内部网成为可能的技术是高速处理器和对个人计算机的储存能力，以及高速率的局域网。

虽然术语内部网是指基于因特网应用的所有范围，包括网络新闻、电子邮件、FTP，但 Web 技术是使内部网很快被大众接受的关键。因此，本章将致力于讨论 Web 系统。

Web 浏览器是最常见的信息接口。越来越多的雇员都体验过因特网 Web 并对它的访问模式感到满意。内部网 Web 利用了这种经验基础。

9.4.1　Web 内容

企业可以使用内部网 Web 加强对雇员通信加强管理，并轻松、快速地提供与工作相关的信息。图 9-14 表明，从顶部来看，这一类的信息可以由公司 Web 提供。通常，雇员需要通过一个内部公司主页作为访问企业内部网的接入口。在这个主页面，有许多公司范围内感兴趣的区域链接，也有其他雇员部门的链接，包括人力资源、财务、信息系统服务。同时也有雇员部门所关注领域的链接，如销售和制造。

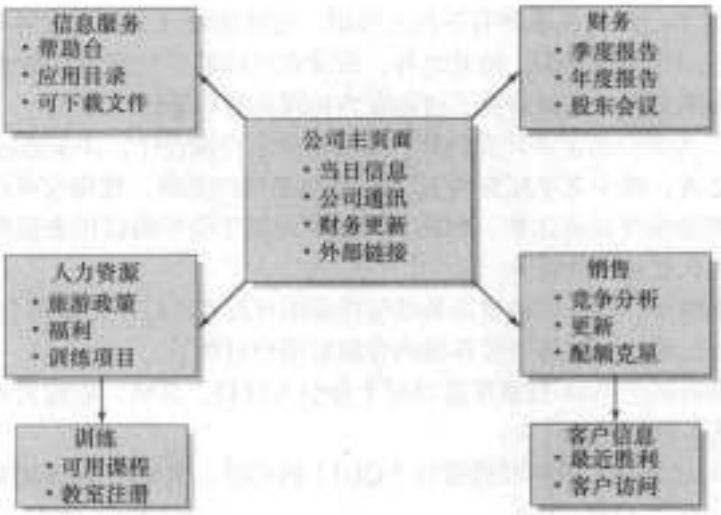


图 9-14　公司 Web 页面结构示例

除了这些广泛使用的 Web 服务，内网 Web 对提供部门和项目级信息服务来说十分理想。一个小组可以建立他们自己的 Web 页面来传播消息和维护项目数据。随着 WYSIWYG Web 授权工具（如 Adobe Dreamweaver）的广泛应用，对在信息服务小组之外的雇员来说，发展他们自己的特定需求的 Web 页面相对简单。

9.4.2　Web / 数据库应用

虽然 Web 是一个强大灵活并能满足公司需求的工具，使用 HTML 来构建 Web 页面仍然在维持一个大量、改变的基础数据方面有所局限。为了使内部网变得真正效率，许多公司希望使用他们自己的数据库管理系统将 Web 服务连接到数据库。

图 9-15 展示了一个 Web / 数据库由简单术语组合的大致策略。首先，客户机（运行 Web 浏览器）通过 URL 引用的形式发起对信息的查询。这个引用激发服务器端的程序并发出正确的数据库指令查询数据库服务器。输出结果返回到 Web 服务器并转化为 HTML 格式返还给 Web 浏览器。



图 9-15　Web/ 数据库的连接

[WHET96] 列举了 Web/ 数据库系统相比于传统数据库的优点：

- **易于管理**：唯一连接到数据库的是 Web 服务器。新增的数据库服务器类型不要求所有的客户端类型对必要的驱动和接口进行配置。相反，需要的仅仅是 Web 服务器将数据库接口能够转换到 HTML 即可。

- **部署**：浏览器已经在几乎所有平台上可用，这就使得开发者不用对不同的客户机和操作系统设计用户图形界面。除此之外，开发者可以假定只要内部 Web 服务器可用，客户即会使用浏览器，这就避免了诸如安装和同步的部署活动。
- **开发速度**：大部分的正常开发周期，如部署和客户端设计，并不适用于基于 Web 的项目。除此之外，基于文字标签的 HTML 支持迅速的更改，使得它可以轻松地根据客户的反馈不断改善外观和体验。相反，对典型的基于图形的应用来说改变它的内容和格式是一项工作量较大的任务。
- **灵活的信息展示**：Web 的超媒体基础使得应用开发者可以应用最适合应用的信息结构，包括使用分层格式，这样进度详细内容就对用户可用了。

这些优点在部署基于 Web 数据库接口时十分引人注目。然而，管理者同样需要注意潜在的缺点，同样列举在 [WHET96] 中：

- **功能性**：对比复杂的用户图形接口（GUI）的功能，常见的 Web 浏览器接口可能存在局限性。
- **无状态操作**：HTTP 的属性是每一次浏览器和服务器的交互都是分开的，独立于之前或未来的改变。通常情况下，Web 服务器不会保留用户的状态记录。这种历史信息十分重要。例如，一个应用允许用户查询数据库中汽车和卡车部分的信息。一旦用户查询了指定卡车的信息，子菜单应该仅显示有关卡车的部分信息。解决这个问题是可能的，但却很棘手。

9.4.3　内部 Web 和传统的客户 / 服务器

虽然传统的客户 / 服务器系统变得越来越广泛和流行，并代替了以前的公司计算模型，然而他的使用并不是没有问题的，主要问题如下：

- 较长的开发周期
- 将应用分为客户端和服务器模型的困难性，以及根据用户反馈修改这种分布所带来的更大困难。
- 对分布式客户端升级的工作量。
- 在分布式环境中，根据不断增长的负载调整服务器规模所带来的困难。
- 不断需求更强力的台式机

大多数的问题可以追溯到典型的客户 / 服务器设计，它将太多的负载划分到客户端上，这种胖客户端策略可以在图 9-5c 和 9-5d 中找到对应。正如之前所提到的，这种策略并不能适应广泛的公司应用。因此，许多公司选择了胖服务器方法。内部网 Web 可以视作胖服务器的一种实现。

内部网 Web 被视作其他胖服务器方案的一种替代，它有着部署简易、使用少量通用标准和与其他基于 TCP/IP 应用结合的优点。然而，内部网 Web 不太可能会胜过甚至减缓传统客户 / 服务器的部署，至少在近期来说不会。从长远来说，内部网 Web 可能会占据公司计算或与其他客户 / 服务器策略一样共同发展。

9.5　外部网

外部网与内部网概念相似，它也使用 TCP/IP 和内部网的应用，尤其是 Web。不同的是，外部网给外端客户提供公司资源访问，通常是公司的供应商和客户。这种外部访问可以通过

因特网或其他数据通信网络。外部网提供的不仅是现在几乎所有的公司都提供的公共 Web 访问。相反，外部网络提供更多对公司资源的扩展访问，常常还执行安全策略。和内部网一样，典型的外部网络操作模型是客户/服务器。

外部网重要的特点是它使得公司间的信息共享成为可能。[BIDG08b] 列举了外部网的如下优点：

- **减少成本**：信息共享由一种自动化很高的形式完成，并将印刷制品和人力资源的消耗最小化。
- **协调**：来自合作伙伴的关键信息可以迅速地传递到另一方。例如，制造商可以将其生产量与客户的库存状态相协调。
- **客户满意度**：将客户与公司连接起来，外部网络可以提供更多关于当前供应商产品和服务的状态信息。
- **加急通信**：外部网络通过连接内部网，增加了业务伙伴之间通信的效率和效用，以供对关键信息的即刻访问。

另一个有关外部网的重要因素是安全性。因为公司 Web 资源和数据库资源对外部的各方可用，并且有关这些资源的交易是允许的，保密性和认证因素需要着重考虑。通常可以使用虚拟专网（VPN）完成，这将会在第 19 章介绍。我们将简单地列举一些开放式公司内部资源对外部人员的选项，以此来创建一个外部网：

- **长距离拨号接入访问**：这使得外部人员可以直接访问内部网，使用一个登入进程对用户进行认证。这种方法将提供最简单的安全保护，因为用户会有被冒充的危险，而几乎没有防御工具来对抗这类危险。
- **安全地从因特网接入到内部网络**：对用户的认证和用户与内部网间通信的加密加强了安全性。加密防止了窃听，认证用于阻止非法访问。然而，和拨号访问一样，如果黑客能够对付这些认证机制，那么整个内部网的资源就变得非常脆弱。
- **通过因特网接入含有公司内部网部分数据拷贝的外部服务器**：这种方法降低了黑客渗透的危险性，但是同样降低了对外部伙伴的外部网价值。
- **通过因特网接入外部服务器，它将会对内部网服务器数据库发起查询**：外部网络服务器实际上扮演防火墙的角色来执行公司的安全策略。防火墙可能会对与外部用户的通信进行加密，认证外部用户，并且过滤信息流以对基本用户做出限制访问。如果防火墙本身可以抵御黑客攻击，那么这将是一种强力的方法。
- **虚拟专网**：VPN 实际上来说是防火墙的概括，它利用了 IP 协议安全能力的优势来允许外部用户和公司内部网之间的安全访问。VPN 将会在第 19 章进行讨论。

9.6 面向服务架构

面向服务架构（SOA）是一种客户/服务器体系结构，它如今在企业系统中广泛使用。一份最新的 Forrester 调查表明截止到 2011 年超过 70% 的企业使用了 SOA[KANA11]。

[WELK11] 从三个角度列举了 SOA 不同于客户/服务器方法：

1）服务的功能范围从最低级或细粒的功能到直接映射到范围、术语、业务用户利润的服务。为了确保范围的可能性，SOA 将业务功能组织为模块化结构，而不是部门的单个应用程序。因此，常见的功能可以被不同的部门内部使用，也能被外部业务伙伴使用。越细粒化的功能就越容易被重复使用。总的来说，SOA 由一组服务和一组使用这些服务的客户应用组成。

客户请求通常涉及一个单一的服务，或者也可能涉及两个或多个服务来协作完成某项活动，这要通信服务彼此服务于对方。这些服务可以通过公开或可发现的接口使用。

2）一个发展良好并一直在发展的一套开放标准定义了所有事物，从服务描述，到通信服务，到发现并连接服务，到将服务组合成一个复合服务的细节，交易完成，到安全性。标准化接口的使用使服务模块与另一个模块通信变为可能，并且使得用户应用可以与服务模块通信。最为流行的接口是通过 HTTP（超文本传输协议）的 XML（可扩展标记语言），被称作 Web 服务。SOA 同样使用其他的标准，如 CORBA（公共对象请求代理体系结构）。

3）不考虑范围的情况下使用服务进行通信的手段，即为因特网协议。这意味着服务可以是远程或者是本地的，并且可以由企业提供也能由外部服务供应商提供。另外，服务过程细节可以改变而不影响到用户，因为通信是通过标准化接口和协议进行的。

从顶层来看，SOA 包含三种体系元素 [BIH06]，如图 9-16 所示。

- **服务提供者**：网络节点对负责管理特定任务的软件集提供服务接口。服务提供节点可以代表业务实体的服务或者它可以简单地代表可重用子系统的服务接口。
- **服务请求者**：发现并唤起其他软件服务以提供业务方案的网络节点。服务请求者节点通常代表一个业务应用中的一部分，其执行 RPC 连接到分布式对象——服务提供者。在一些情况下，提供者节点可能会处于内网本地，另一些情况可能会处于远程因特网。SOA 的概念属性将网络互联、传输协议以及安全细节遗留给具体的实施。

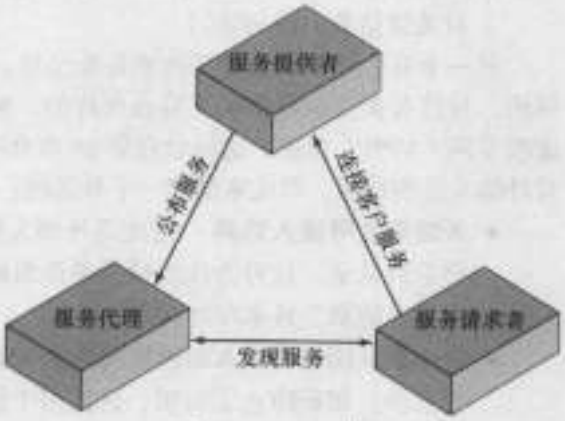


图 9-16　SOA 模型

- **服务代理**：一个具体的服务提供者类型，它充当注册处，并允许查找服务供应者的接口和服务坐标。服务代理将服务请求传递给一个或多个服务提供者。

接下来是使用高效服务的关键特点：

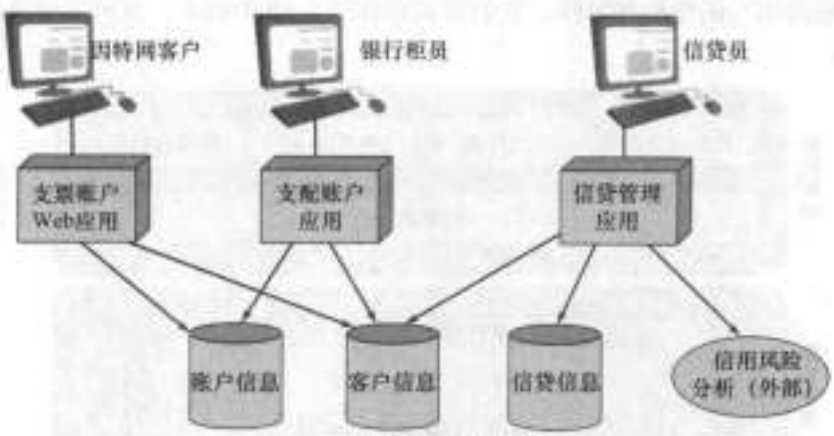
- **粗粒**：对服务的操作是频繁执行的，与分量接口设计比较，它涵盖更多功能，对更大的数据集进行操作。
- **基于接口的设计**：服务执行由接口分别定义。这样的好处是多重服务可以实现公共接口，并且一个服务可以实现多重接口。
- **可发现**：服务需要在设计时和执行时被发现，并且服务不仅可以通过独一无二的标识符，还需要通过接口标识符和服务类型被发现。
- **单一实例**：不同于基于组件的设计开发（其组件按需实例化），在 SOA 中，每一个服务是与各个客户通信的单一、持续运行的实例。
- **松耦合**：服务与其他服务连接，并且用户使用标准、少依赖、去耦的基于消息的方法，如 XML 文档交换。
- **异步**：大体上说，服务使用异步消息传输方法。然而，这不是强制的。实际上，许多服务有时使用同步消息传输。

为了使读者对 SOA 的使用有更深的理解，我们来学习一个例子。图 9-17a 展示了一种针

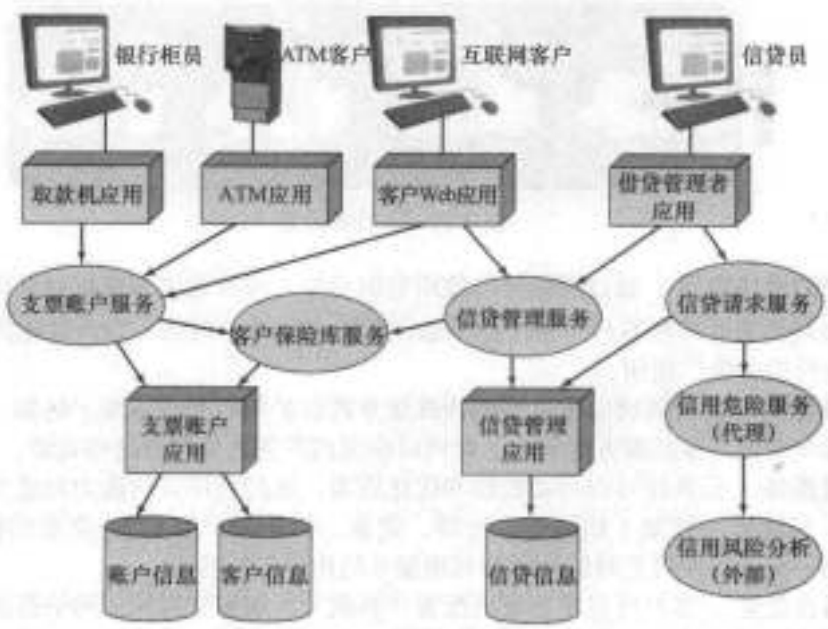
对特定用户类别构造应用的常见方法。对每个特定的应用来说，一个单一的自包含应用模块建立了。在企业中将不同应用连接在一起的是一个独立的应用数据库管理系统，它支持多个数据库。例如，在这个配置中所有的三个应用要求访问用户信息数据库，这样安排的好处就显而易见了。将数据从应用中分离并且提供一个统一的数据库接口，多个应用就可以彼此独立地开发和修改。

典型的方法，即多个应用使用一个共同的数据库集，存在着一些缺陷。新增的用户服务，如 ATM（自动取款机），通常会要求构造一个新的独立于现有应用的应用，尽管大多数必要的逻辑已经在相关的应用中实现。

我们可以移植到 SOA 以追求更好的效率和灵活性，如图 9-17b。这里，策略是将大多数应用会使用的公共服务独立出来，并且实现这些独立的服务模块。在这个特别的 SOA 例子里，有许多核心的应用应对不同的数据库。这些应用由服务模块通过应用程序编程接口（API）调用来实现公共服务。最后，这些对用户可见的特定应用主要解决演示问题和具体的业务逻辑。



a）典型应用结构



b）反映SOA原则的架构

图 9-17 SOA 使用示例

9.7　云计算

在许多企业中，将大部分甚至所有信息技术（IT）操作搬移到一个连接因特网的被称作企业云计算的基础设施中有越来越突出的趋势。本节将会对云计算做一个概述。

9.7.1　云计算元素

NIST 这样定义云计算，在 NIST SP-800-145（NIST 关于云计算的定义）如下：

> **云计算**：一个普及、方便、按需的网络模型，其接入到共享的可配置计算资源池（如网络、服务器、存储、应用、服务）中，这些资源可以通过最小化管理或与服务提供者交互进行迅速的配置和释放。这种云模型可以改善可用性，并且由 5 个关键的特性、3 个服务模型以及 4 个部署模型组成。

这个定义是指不同的模型和特性，它们的关系在图 9-18 中展示。这种云计算的**关键特性**包括以下几点：



图 9-18　云计算元素

- **广泛的网络访问**：通过网络可以使用它的功能，并且通过标准机制获得访问，标准机制由异构的胖或瘦客户平台（如手机、笔记本电脑、PDA）以及其他传统的或基于云的软件服务推广使用。
- **快速弹性**：云计算可以根据你的特殊服务需求扩展和削减资源。例如，你在特定的任务周期需要大量的服务器资源。你可以在完成任务之后释放这些资源。
- **测量服务**：云系统可以自动控制和优化资源，通过利用计量能力对适当的服务类型进行一定程度的抽象（如储存、处理、贷款、活动用户账户）。资源的使用可以监视、控制、报告，使得它对提供者和利用服务的用户保持透明。
- **按需自服务**：客户可以单方面地配置计算能力，如服务时间、网络存储等自动按需分配而不需要人员与每个服务提供商进行交互。因为服务是按需的，所以资源并不是永久属于你的 IT 基础设施的一部分。

- **资源池**：供应者的计算资源被放入池中以服务多个用户，这使用了多租户模型，根据客户的需求，将不同的物理和虚拟资源动态地分配及重新分配。客户基本上对供应者的资源的位置没有控制权和确切的了解，但是他们有可能指定更高级别的抽象位置（如国家、州，或者数据中心），因此关于位置信息是独立的。资源的例子包括储存、处理、内存、网络带宽、虚拟机。甚至在同一组织的不同部分，私有云也进入到资源池。

NIST 定义了三种**服务模型**，他们可以被视作巢式服务选择：

- **软件即服务（SaaS）**：运行在云设施上的供应者应用，为用户提供服务。

这些应用可以通过不同的客户设备从瘦客户端接口（如 Web 浏览器）进行访问。企业从云服务获得了相同的功能，这代替了获得台式计算机与服务器的软件产品执照的方法。SaaS 免除了软件安装、维护、升级、补丁的复杂性。这种级别服务的例子有如 Gmail（谷歌电子邮件服务）和帮助公司跟踪客户信息的 Saleforce.com。

- **平台即服务（PaaS）**：云设施为用户提供兼容的编程语言和工具以支持用户开发的应用或收购的应用。PaaS 通常提供中间件式的服务，如数据库和应用调用的组件服务。实际上，PaaS 是云中的一个操作系统。
- **基础设施即服务（IaaS）**：向客户提供处理、存储、网络以及其他基础计算资源的配置，使得用户能够部署并运行任意软件，包括操作系统和应用。IaaS 使得用户对基础计算服务进行组合，如乱序和数据储存，来建立高适应性的计算机系统。

NIST 定义了 4 个**部署模型**：

- **公共云**：云基础设施对全部公众和大部分工业群体可用，并且它的拥有者是销售云服务的企业。基础设施和云的控制属于服务的提供者。
- **私有云**：云基础设施由企业单独操作。它可能由企业或第三方管理，并可能是内部部署或外部部署的。云提供者仅负责提供基础设施，但不提供对云的控制。
- **社区云**：这种云由几个组织共享，并且支持特定的团体，这个团体有共同的关注点（例如，任务、安全要求、政策、合约考虑）。它可能由组织或第三方管理，并可能是内部部署或外部部署的。
- **混合云**：这种云设施有两种或多种云（私有、社区、公共）混合而成，它使得云保持各自独立的实体但是又由标准化或私有技术连接在一起，这样一来数据和应用就有可移植性了（例如，在两朵云之间平衡负载的云爆发）。



图 9-19 云计算背景

图 9-19 展示了典型的云服务背景。企业工作站处于企业局域网或局域网集中，这些局域网由路由器通过网络或因特网连接到云服务提供者。云服务提供者维持了大量的云服务集，通过一系列的网络管理、冗余和安全工具进行管理。在图中，云服务基础设施被展示为一群常见结构的刀片服务器集合。

9.7.2　云计算参考结构

NISP SP 500-292（NIST 云计算参考结构）建立了一个参考结构，描述如下：

> NIST 云计算参考结构聚焦在对云服务的什么需求，而不是怎么设计解决方案和实现方法。这个参考结构用于帮助对云计算操作性的复杂性的理解。它不代表云计算系统的详细系统结构，而是它是一种描述、讨论的工具，同时可以使用常见的参考框架对指定的系统结构进行开发。

NIST 为开发这个参考结构设定了以下几个目标：

- 在总体的云计算概念模型中，展示并理解不同的云服务。
- 提供一个技术参考给用户用作理解、讨论、分类和比较云服务。
- 便于分析安全候选标准、互操作性以及可移植性和实施参考。

参考结构在图 9-20 中进行描绘，它定义了 5 个主要的角色以及它们在条款中的角色和责任：

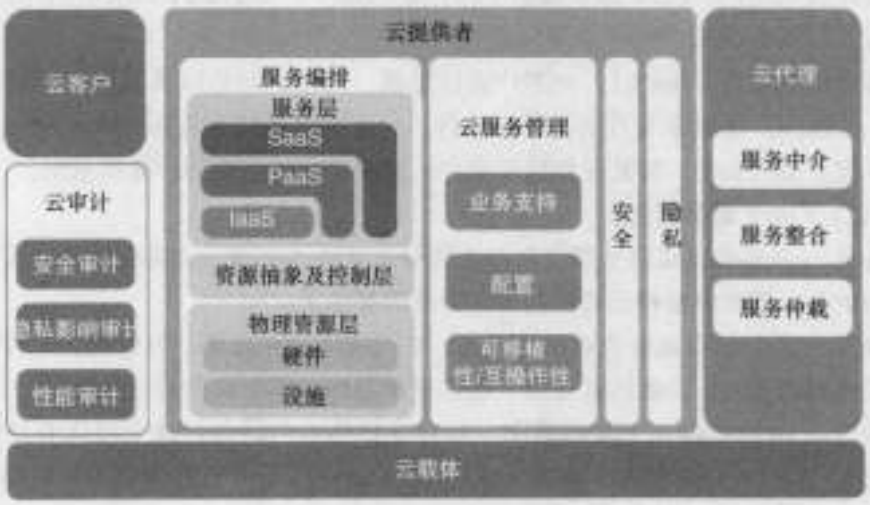


图 9-20　NIST 云计算参考结构

- **云客户**：与企业维持商业关系的人、使用云提供者服务的人。
- **云提供者**：对感兴趣的群体提供服务的个人、企业、单位。
- **云审计**：可以对云服务、信息系统操作、性能、云运行安全进行独立评估的组织。
- **云代理**：管理云服务的使用、性能、传输的实体，并且协调云提供者和云顾客之间的关系。
- **云载体**：提供云提供者和云客户之间的连接，是云服务传输的中介。

云客户和云提供者的角色在之前已经被讨论过。总的来说，**云提供者**进行可以提供一个或多个云服务来满足 IT 和**云客户**的业务需求。对 3 个服务模型（SaaS、PaaS、IaaS）中的每一个模型来说，云提供者需要提供存储和运行设施以支持服务模型，此外还需要对云客户提供云接口。对 SaaS 来说，云提供者部署、配置、维护、更新云基础设施中的软件应用操作，这样一来，云服务就能给客户配置他们想要的云服务级别。SaaS 的客户可以是提供给员工访问软件应用服务的企业，也可以是直接使用软件的终端用户，还可能是为终端用户配置应用

的软件应用管理员。

对 PaaS 来说，云提供者管理平台上计算的基础设施，并且运行云软件以提供平台组件，如运行软件执行堆栈、数据库以及其他中间件组件。PaaS 的云客户可以使用工具并执行由云提供者提供的资源来进行开发、测试、部署并管理在云环境下的应用。

对 IaaS 来说，云提供者购置物理计算资源相关服务，包括服务器、网络、存储以及搭建主机的基础设施。IaaS 云客户反过来使用这些计算资源，如虚拟计算机，用于满足他们的基本计算需求。

云载体是一个因特网络设施，它提供在云客户和提供者间的连接以及传输云服务。通常，云提供者会与云载体建立服务等级协议（SLA），使得对用户能提供与 SLA 级别一致的服务，提供者可能会要求云载体在云提供者和云客户间提供专用且安全的连接。

云代理在云服务对客户过于复杂难以管理时比较有用。云代理提供三方面的支持：

- **服务中介**：这些是增值服务，如身份管理、性能汇报、安全强化。
- **服务集合**：代理组合了多个云服务以满足客户的需求，而不仅是由单一的服务供应者提供服务，它还能优化性能或提供最小化成本。
- **服务仲裁**：这与服务集合相似但它所提供的组合服务并不是固定的。服务仲裁意味着中介可以灵活地从多个代理中选择服务。例如，云代理可以使用评分服务来测评各个代理，并从中选择分数最高的那个。

云审计可以评估由云提供者提供的服务，包括安全控制、隐私影响、性能等方面。审计是个独立的实体，它可以确保云提供者符合一系列标准。

应用注解

胖还是瘦——这是一个问题

最流行的通信结构是客户/服务器模型。图 9-2 展示了这种关系。简而言之，客户机有一个小型程序向服务器发出特定的请求。例如，当你通过 Web 页面访问一个 Web 服务器，你正通过 Web 浏览器发出请求。浏览器就是你的客户端应用。常见的计算机配置拥有硬盘、处理器、内存、一系列办公程序（如 Microsoft Office）以及一系列连接到其他主机或资源的应用。后者被称作客户端应用或简称为“客户”。这种配置对网络组件来说同样适用。除了硬盘、路由器、交换机以及接入点，它们都有处理器、内存以及软件。在大多数情况下硬盘已经被高速缓存所代替。这种类型的计算机和设备被称作“胖”，因为他们拥有所有他们需要的东西。

然而，这并不是配置计算机或其他网络机器仅有的方法。有许多产品舍弃了一个或多个部分以降低成本或用作特殊用途。下面的例子会展示网络和系统的配置是如何被修改的。

当你建立一个家庭打印机，它由直接连接的计算机专用。甚至对小型公司来说，为每个员工配备个人打印机也是可行的。但当用户的数目增加之后，这将会变得越来越不可行。在这种情况下，打印机进行共享较为可行，同时其中一个服务器会作为打印服务器，处理客户的所有打印请求。

库存软件是一个运行在服务器或主机上的应用。客户通过系列网络连接进行工作，同时客户端很少发生运算或储存。这是为了确保数据库信息是准确并且最新的。用户的击键传递到主机或服务器，并且在经过“数据处理”后，信息返回给用户。对于这种应用，客

户端就是“瘦”的。用户在没有连接或认证之前不能进行工作。这种安装类型可以进行使用控制并要求软件许可。

软件许可会花费许多钱，并且不正确的管理很有可能面临罚款。服务器可以在任何时候对使用应用的用户进行控制。同样，当用户数量超过许可证所允许的最大用户数时，不对软件许可进行更新会带来许多问题。这样会造成许多用户不能使用网络应用，因为已经有足够多的用户登入系统。

像文字处理和电子表格类应用通常完整地处于计算机内。同样，这种类型的客户端称为胖。在完整的分布式胖客户端环境下，用户可以不使用网络连接完成一系列应用操作。

文字处理应用也有可能整个或部分处于服务器。实际上，计算机本身可能被配置成瘦客户端，它自身不能提供资源。硬盘仅能够容纳操作系统的重要组件，其余所有的应用储存并运行在网络中的服务器。在这种情况下，安装可以潜在地为客户机省下空间。瘦客户机的优点是便宜且易于使用，他们也会降低数据被损坏和盗窃的风险。下行十分依赖于网络，这会导致可预见的网络拥挤以及在失去网络访问的情况下效率的降低。

网络设备同样可以根据他们的使用需求配置为胖或瘦。大型公司的无线网络部署了许多接入点。通常管理所有接入点的方法是对每一个进行单独配置，并且允许它处理分区的安全和数据转发，换句话说，即“胖”接入点。这种方法十分花费时间，特别是如今无线网络面临不同的威胁等级。替代的方法是将所有的接入点连接到网络控制器上，而所有的决策都通过这个中央位置。所有的接入点只需要有足够的处理能力反馈给控制器，所有的操作性决定同样通过中央位置。这的却会便于管理，但是单一的控制器却是一个大问题。即使控制器失效了很短一段时间，整个无线网络可能会完全宕机。

有许多重要的决策在决定究竟是胖还是瘦服务器。客户端时需要考虑。这些决定对成本、安全、性能和对终端用户的作用有着至关重要的影响。对胖客户端和瘦客户端来说他们分别适用于特定的场合，并且每一个安装都影响着后续过程。理解安装系统的能力、需求的服务以及客户机的使用十分重要。

9.8　总结

客户/服务器计算是挖掘企业中信息系统和网络潜力以提升效率的关键。有了客户/服务器计算，对单一用户工作站和个人电脑的用户来说，应用是分布式的。同时，共享和维护在服务器系统上的资源对所有的客户可用。因此，客户/服务器结构是分散与集中计算的混合体。

通常，客户端系统提供图形用户界面（GUI）使用户能够在很少的训练下相对容易地使用各种应用。服务器支持共享功能，如数据库管理系统。实际上应用被分为客户端和服务器端以追求最大化的性能和简易使用。

因为没有普遍接受的客户/服务器网络标准，许多产品作为连接客户和服务器的桥梁，并使用户能够使用多个供应商的配置。这种产品通常被称作中间件，中间件产品是基于消息传递或远程过程调用机制的。

在企业中，一个更为与客户/服务器模型竞争的常见模型是内部网。内部网利用了现有的因特网应用，尤其是 Web，来提供适用于企业需求的一套内部应用。内部网的建立很简单，

使用了标准化的软件，并且可以部署在多个平台上，几乎不需要对用户进行培训。

面向服务结构（SOA）是客户 / 服务器计算的一种形式。SOA 系统建立在部署为服务的松耦合软件模块，通常通过网络进行通信。这允许了不同的模块可以以不同的方式进行部署和运行，例如，属于不同企业的，由不同队伍开发的，由不同语言编写的，运行在不同硬件和操作环境的。实现这一切的关键是互操作性和使他们满足标准，这样模块才能交换数据。

云计算是指通过因特网对处理器、储存、软件和其他计算服务提供访问的任何系统，常使用 Web 浏览器进行访问。通常这些服务会从维护和管理服务的外部公司租借。

案例学习 VI：流沙：Chevron 向云的迁移

在该案例中涉及的主要概念是云计算和 Web 服务。**案例学习的更多内容在 www.pearsonhighered.com/stallings。**

9.9　关键术语、复习题和练习题

关键术语

Application Programming Interface（API，应用程序接口）
client（客户）
client/server（客户 / 服务器）
cloud auditor（云审计）
cloud broker（云代理）
cloud carrier（云载体）
cloud computing（云计算）
cloud consumer（云客户）
cloud provider（云提供者）
community cloud（社区云）
extranet（外部网）
Graphical User Interface（GUI，图形用户界面）
Infrastructure as a Service（IaaS，基础设施即服务）
intranet（内部网）
message（消息）
middleware（中间件）
object-oriented middleware（面向对象的中间件）
Platform as a Service（PaaS，平台即服务）
private cloud（私有云）
public cloud（公共云）
Remote Procedure Call（RPC，远程过程调用）
server（服务器）
service aggregation（服务集合）
service arbitrage（服务仲裁）
service intermediation（服务中介）
Service-Oriented Architecture（SOA，面向服务结构）
Software as a Service（SaaS，软件即服务）

复习题

9.1　什么是客户 / 服务器计算？
9.2　客户 / 服务器计算与其他分布式数据处理的区别是什么？
9.3　讨论应用放置在客户端、服务器或分开放置在客户服务器的合理性。
9.4　机器之间的相互通信可分为哪四种不同的处理方式？

9.5　与通常的笔记本和台式机相比，怎样与基于客户服务器的系统进行交互？
9.6　什么是胖客户端和胖服务器，并且两者从原理上说有什么不同？
9.7　请说明胖客户端和胖服务器的优点和缺点。
9.8　什么是中间件？
9.9　对处于不同地点的客户来说，访问数据需要中间件的支持。Telnet 和 FTP 的应用软件需要中间件吗？
9.10　我们已经有 TCP/IP 和 OSI 标准，为什么还需要中间件？
9.11　什么是内部网？
9.12　客户 / 服务器和内部网的区别？
9.13　什么是外部网？
9.14　说出外部网提供共享信息的优点。
9.15　将内部网转化为外部网的可用通信选项有哪些？

练习题

9.1　你被聘请为首席信息官，并且公司最近收购了另一个较小的公司来增加市场份额。原公司组织了巴士车队计划沿着美国东海岸的北部进行旅游。所有的计算机应用处于马里兰州，巴尔的摩市公司总部的中央主机上。收购的的公司组织在纽约市和华盛顿的直升机观光。所有的系统是基于 C/S（主要是胖客户端访问瘦数据库服务器），同时他们处于巴尔的摩市的外部，靠近巴尔的摩国际机场。因为兼并的缘故，公司的 IT 结构现在是不同计算机系统和人员配置的结合。给定以下利益相关者群体并运用在图 9-5 中定义的大概的 C/S 类型，准备一份适用于新公司融合的 IT 结构，并将它提交给 CEO。陈述从不同利益相关群体的角度计划的所有优缺点。

- 巴士 / 直升机的维护工人和机械师（10 人）
  - 订购部件 / 耗材的系统
- 司机 / 飞行员（20 人）
  - 日志以及路线 / 行程信息
- 行政部 /HR（5 人）
  - 人员记录
  - 财务记录
- 市场（8 人）
  - 市场活跃度
  - 顾客交互（CRM）
- 管理者（9 人）
  - 报告

9.2　Java 编程语言因为它独立于平台的特性被称作 Web 语言。Java 使用了 RPC 和 CORBA 的混合形式，称作 RMI（远程方法调用）。RMI 与这两种技术的不同之处是什么？并且 RMI 在哪一种环境下是适用的，或是最优化选择？参考 http://www.kuro5hin.org/story/2001/2/9/213758/1156。这篇论文的拷贝收纳在本书最优内容中的文档章节。

9.3　Web 服务作为一个相对新鲜的术语引入了 Web 环境。什么是 Web 服务？它和 Web 应用的概念有何不同？参考：http://www.w3.org/TR/2003/WD-ws-gloss-20030514/。

9.4　你的操作系统中基于客户 / 服务器的应用有哪些？

9.5　在你本地网络中，哪些服务器是客户 / 服务器形式？它们处于什么位置？它们的 IP 地址是？它们的域名是？

9.6　本章讨论了胖客户端。瘦客户端在过去和现在一直是一个很好的客户端。你怎么刻画瘦客户端？

9.7　本章介绍了内部网术语。在这之前我们介绍了因特网。根据你对这些术语的了解，用一幅图来描绘你本地的内部网（学校网络）以及你的企业（学校）是如何连接到因特网的。

- 网络的大小？
- 谁是因特网服务提供者？
- 多少网络组成了学校网络？
- 网络服务多少用户？
- 你得到了怎样的网络性能？

第 10 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

基于因特网的应用

学习目标

通过本章的学习，读者应该能够：

- 讨论电子邮件的应用。
- 解释 SMTP 的基本功能。
- 解释为什么需要使用 MIME 对原有的电子邮件进行加强。
- 描述 MIME 的要素。
- 解释网络运行中 HTTP 的作用。
- 描述 HTTP 代理、网关及隧道的功能。
- 解释网页缓存。
- 讨论可接受使用策略的作用与应用。

在第 2 章和第 3 章中我们已经说过，分布式信息处理在所有商业中都非常重要。大部分分布式处理局限于特定类型的数据并仅能由专有供应商的软件所支持。然而，公司内部和公司之间都需要信息交换，这就要求分布式应用要满足通用目的和国际标准或实际的工业标准。这些应用对行业的效率与竞争力都有很大的影响。在这一章中，我们将讨论最重要、传播最广的三种分布式应用：电子邮件（E-mail）、网络访问和多媒体支持。对每一种应用都制定了相应的国际标准。随着这些标准被电脑厂商和软件公司广泛践行，这些应用在商业环境中变得日趋重要与有效。本章还将仔细讨论基于因特网和网络的应用的可接受使用策略。

10.1 电子邮件

电子邮件是一种使工作站和终端用户能够处理和交换消息的设施。除非用户（发件人或收件人）想要消息的纸质副本，不然不需要纸张来记录消息。一些邮件系统只服务于单台计算机上的多个用户，另一些则为整个网络的计算机提供服务。表 10-1 列出了电子邮件设施提供的一些常用功能。

表 10-1 典型的电子邮件设施

准备邮件
文字处理 新建或编辑邮件。一般来说电子邮件文档的内容都比较简单，所以电子邮件设施不需要像文字处理器一样全面功能。不过，大部分电子邮件系统允许“离线”使用文字处理器，用户可以使用计算机上的文字处理器创建消息并存成文件，再将此文件作为电子邮件设施中的邮件准备功能输入
批注 一般回复邮件的内容都十分简短。批注功能允许用户在来信上直接附上批注寄回收件人或第三方

（续）

发送邮件
用户目录 系统使用，也可能对用户开放以查找地址
定时发送 允许用户指定邮件送达的时间或日期。邮件送达是指邮件到达收件人的邮箱
多地址 邮件抄送至多个地址。在邮件头中列出所有收件人地址或使用通信组列表。通信组列表是一个包含所有收件人地址的文件，它可以由用户或者中央管理功能创建
邮件优先级 邮件可以标注优先级。高优先级邮件以可能的更快速度传递，同时，收件人收到高优先级邮件时会收到提醒
状态信息 用户可能需要邮件的送达或收件人实际收取的提示。用户也可以查询邮件的当前状态（如等待发送，已发送但还未收到确认回执）
连接其他设施的接口 这包括其他电子系统，如电报和物理分发设施，如投递员或公共邮件系统（例如美国邮政服务）
接收邮件
邮箱扫描 允许用户扫描当前邮箱的内容。每个邮件被标识了主题、作者、日期、优先级等
邮件选择 用户可以选择邮箱中的单个邮件进行显示、打印、另存为独立文件或删除操作
邮件提醒 大部分系统会提醒在线用户新邮件的到达，并且当用户登录时提醒用户收件箱中的邮件
邮件回复 用户可以立即回复选中的邮件而不用键入收件人姓名和地址
邮件重递送 当用户暂时或永久改变地址时可以重递送收到的邮件。加强功能允许用户为不同类别的邮件指定不同的转发地址

这个部分将介绍标准因特网邮件架构并讨论支持电子邮件应用的关键协议。

10.1.1　因特网邮件架构

先对因特网邮件架构有个大致的了解，可以帮助我们理解电子邮件系统的操作及其支持的协议。因特网邮件架构由 RFC 5598（因特网邮件架构）规定，从最基础的层面来说，因特网邮件架构包括用户部分（邮件用户代理（MUA）和传输部分）由邮件传输代理（MTA）组成的**邮件处理服务**（MHS）。

邮件处理服务从一个用户那里接受邮件并传送给一个或多个用户，创造一个虚拟的 MVA 对 MVA 的交换环境。这个架构包含了三种类型的互操作性。一种是用户之间的，邮件用户代理代表邮件作者格式化邮件，使得终点邮件用户代理可以将邮件内容展示给邮件收件人。邮件用户代理和邮件处理服务之间也存在互操作性——邮件先从一个邮件用户代理提交给邮件处理服务，然后邮件处理服务再将邮件传送到终点的邮件用户代理。在传输路径上的邮件传输代理组件彼此也需要相互操作。

因特网邮件架构的关键组成部分如图 10-1 所示。

- **邮件用户代理**（MUA）：代表用户的行动和应用，是用户的在邮件服务中的代理。一般此功能在用户的计算机中，被称作电子邮件客户端或本地网络的邮件服务器。发件人的邮件用户代理格式化邮件并通过邮件提交代理提交给邮件处理服务。收件人的邮

件用户代理处理收到的邮件，存储并 / 或显示给收件人。

- **邮件提交代理（MSA）**：接收从邮件用户代理提交来的邮件，并执行主机域名的策略和因特网标准的要求。这一功能可能与邮件用户代理在一起或独立为一个单独的功能模块。在后一种情况下，邮件用户代理和邮件提交代理之间使用简单邮件传输协议（SMTP）。
- **邮件传输代理（MTA）**：在应用层的邮件代理之间实现邮件中继。它就像分组交换机或者 IP 路由器，进行路由评估将邮件送往收件人。一连串的邮件传输代理不断中继邮件直到最终将邮件送达终点邮件投递代理。邮件传输代理还在邮件的头部添加了追踪信息。邮件传输代理之间以及邮件传输代理和邮件投递代理或邮件提交代理之间都使用 STMP 协议。
- **邮件投递代理（MDA）**：负责将邮件从邮件传输服务转到邮件存储区（MS）。
- **邮件存储区（MS）**：邮件用户代理可以部署一个长期的邮件存储区。存储区可以位于远程服务器也可以和邮件用户代理处于同一台机器上。一般来说，邮件用户代理通过 POP（邮局协议）或 IMAP（因特网邮件访问协议）从远程服务器获取邮件。



图 10-1　因特网邮件架构中的功能模块和其中使用的标准化协议

除此之外，还需要定义两种概念。**经营管理域（ADMD）**是因特网邮件的提供者。如运行本地邮件中继（MTA）的部门、运行企业邮件中继的 IT 部门和运行公共共享邮件服务的因特网服务提供商。每个经营管理域可以有不同的运行协议和基于信任的决策。举一个浅显的例子，一个组织内部和不同组织之间的邮件传递是不一样的，处理这两种邮件传输的规则有明显不同。

域名系统 (DNS) 是提供因特网上的域名与其数字地址映射的目录查找服务，在第 7 章中我们会详细讨论。

邮件用户可以看到用户代理的功能，包括准备邮件和提交邮件以路由到终点设施和

帮助用户填写、收取、回复、转发的实用功能。邮件处理服务从用户代理处接收邮件，然后在单个网络或因特网络中传输邮件。邮件处理服务还参与传输和投递邮件所需的协议操作。

用户不直接与邮件处理服务交互。如果用户为邮件指定了一个本地收件人，邮件用户代理将邮件存入本地收件人的邮箱。如果用户为邮件指定了远程收件人，邮件用户代理将邮件转给邮件传输服务去传送到远程邮件传输代理并最终到达远程邮箱。

要实现因特网邮件架构，还需要一组标准。其中有 4 个值得关注的标准：

- **邮局协议（POP3）**：电子邮件客户端（用户代理）可以通过 POP3 从电子邮件服务器（MTA）下载电子邮件。POP3 用户代理通过 TCP/IP 协议连接到服务器（一般端口为 110）。用户代理输入用户名和密码（为了方便内部存储或为了安全每次由用户键入）。通过验证后，用户代理使用 POP3 指令收取和删除邮件。
- **因特网邮件访问协议（IMAP）**：与 POP3 相同，电子邮件客户端可以通过 IMAP 从电子邮件服务器下载邮件。IMAP 也使用 TCP/IP 协议，TCP 服务器端口 143。IMAP 比 POP3 更为复杂，它提供更强的验证及其他 POP3 不支持的功能。
- **简单邮件传输协议（SMTP）**：这个协议用于用户代理到 MTA 和 MTA 之间的邮件传输。
- **多用途因特网邮件扩展（MIME）**：MIME 完善了 SMTP 并允许在标准 SMTP 邮件中封装多媒体（非文字）邮件。

在本章剩下的部分，我们将详述这些标准。

10.1.2　简单邮件传输协议

SMTP 是 TCP/IP 协议簇中主机间传输邮件的标准协议，由 RFC821 所定义。

尽管我们之后会提到 SMTP 传输的邮件一般遵从 RFC822 定义的格式，但是除了两种例外情况，SMTP 本身并不关心邮件的格式和内容。通俗地说，SMTP 只使用邮件信封上写的信息（邮件头），而不会看信封里的内容（邮件正文）。

两种例外情况：

1）SMTP 将邮件中的字符集标准化为 7 比特的 ASCII 码。（附录 D 中介绍了美国信息交换标准代码。）

2）SMTP 在被传送邮件最开始处加上指示传送路线的日志信息。

基本电子邮件流程

图 10-2 说明了典型的分布式系统中电子邮件的总体流程。尽管整个过程中有很多部分在 SMTP 范畴之外，这幅图说明了 SMTP 典型操作内部的一些内容。

首先，邮件由用户代理程序响应用户输入创建。每个创建的邮件包含邮件头和邮件正文。邮件头包含了收件人的邮件地址和其他信息，邮件正文包含要发送的信息。接下来，这些邮件以某种方式进入队列，作为 SMTP 发送程序的输入。一般 SMTP 发送程序始终在线。

尽管传出邮件队列的结构会因主机的操作系统而有所不同，但是每个队列的邮件概念上来说有两个部分：

1）邮件文本，包含：

- 822 头：822 头构成了邮件的信封，包含了一个或多个收件人。

- 用户所写的邮件正文。

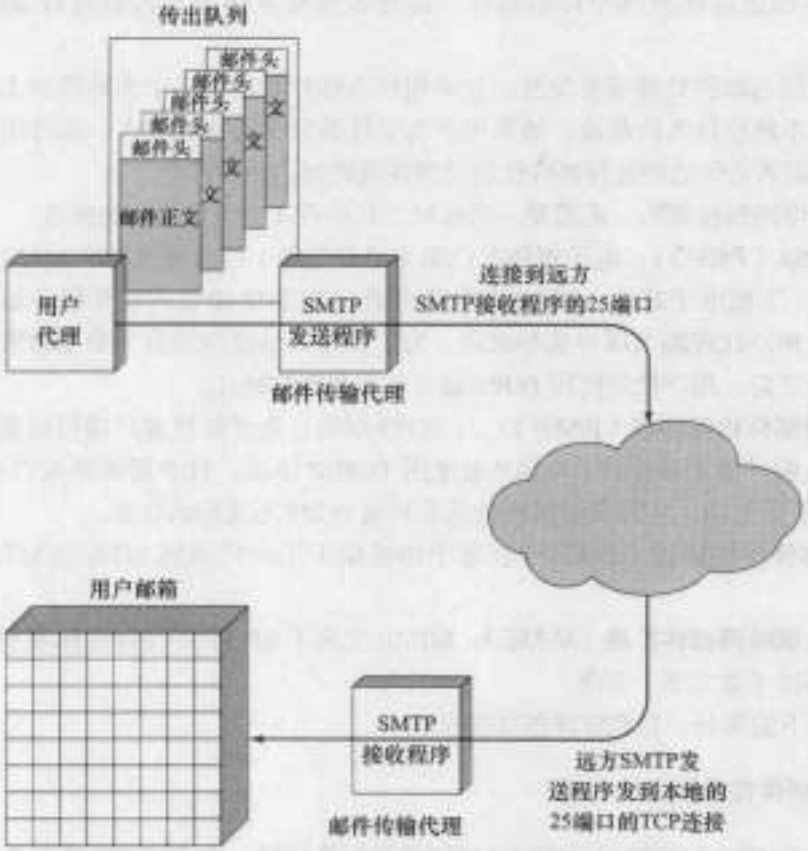


图 10-2　SMTP 邮件流程图

2）邮件终点列表。

邮件终点列表由用户代理从邮件头中生成。有时，邮件头中文字写明了终点。有时，用户代理需要扩展邮件列表名、移除重复项并将备注名替换为真实的邮箱名。如果需要密件抄送邮件，用户代理还需要使邮件满足该要求。基本的思想就是要将用户界面输入的多种格式和样式转换为适合 SMTP 发送程序的标准列表。

SMTP 发送程序从传出邮件队列中取出邮件，通过一个或多个 TCP 连接上的 SMTP 事务传递到目标主机的端口 25。如果一台主机上有大量传出邮件，那么可能有多个 SMTP 发送程序同时运行。同时这台主机也应按需求创建 SMTP 接收程序，防止邮件在从一台主机传递到另一台主机时有所延迟。

当 SMTP 发送程序将某封邮件发送到了特定主机上的用户，它就从此邮件终点列表中移除相应的终点。当 SMTP 发送程序完成某封邮件所有终点的发送，它就从队列中删除此邮件。SMTP 处理队列时会进行很多优化。如果一封邮件收件人是单台主机上的多个用户，邮件文本只需要发送一次。如果多封邮件要送到相同主机，SMTP 发送程序可以只建立一个 TCP 连接来传输多封邮件，而不是为每封邮件建立一个连接。

SMTP 发送程序要处理许多错误。终点主机可能无法送达或已停止运行，邮件传输过程中 TCP 连接可能失败。发送程序需要重新将邮件加入队列，而如果一直出现错误发送程序会在一定时间后放弃此邮件而不是让邮件永远在队列之中。错误的收件地址是一个常见错误，

很有可能是用户输入错误或者收件人换了不同主机上的新地址。SMTP 发送程序要么将邮件重定向要么向发件人发回一个错误报告。

我们使用 SMTP 将邮件从 SMTP 发送程序通过 TCP 连接传输到 SMTP 接收程序。SMTP 旨在提供一个可靠的操作，但并不保证能恢复遗失的邮件。SMTP 不向发件人发回邮件送达成功的端到端确认，错误报告也不保证发回，然而我们一般认为基于 SMTP 的邮件系统是可靠的。

SMTP 接收程序接收每封到达的邮件并将放到合适的用户邮箱中，如果需要转发则复制到本地传出邮件列中。SMTP 接收程序必须要能够验证本地邮件终点并处理错误，包括传输错误和硬盘空间不足。

在 SMTP 接收程序在指示传输完成之前负责整个邮件。然而，这只表明邮件已到达 SMTP 接收程序处，并不表示邮件送达并被最终收件人收取。SMTP 接收程序的错误处理能力有限，当 TCP 连接失败或长时间失效时，它只能放弃此连接。因此，发送程序负责恢复大部分错误。在完成传输的过程中，错误可能导致数据重复，但不会导致数据的丢失。

在大多数情况下，邮件直接通过一次 TCP 连接从邮件发送者的机器传输到邮件接收者的机器。然而邮件偶尔也会利用 SMTP 转发能力经过中间机器，这时邮件就必须经历一系列的 TCP 连接完成从源点到终点的传输。这种情况可能是由于发送程序指定了到达终点路径经过的服务器序列。更常见的一种可能是由于用户地址改变而必须进行转发。

我们需要注意，SMTP 协议只局限于 SMTP 发送程序与 SMTP 接收程序之间的对话。尽管 SMTP 具有一些处理邮件终点验证和操作的辅助功能，其主要功能是邮件传输。在图 10-2 中所画出的余下的邮件处理功能超出了 SMTP 的范畴，每个系统也有所不同。

RFC822 RFC822 定义了电子邮件文本的格式。SMTP 标准采纳了 RFC822 的格式作为 SMTP 传输中邮件的构造标准。RFC822 中，邮件由信封和内容两部分组成。信封包含了完成传输和投递所需的所有信息。内容是要投递给收件人的对象。RFC822 标准只应用于邮件内容，然而，内容标准包括了一组头部域，邮件系统可能使用这些头部域来创建信封，RFC822 标准可以帮助程序识别这些信息。

RFC822 邮件由文本行序列组成，并使用“便签”结构。邮件的开头是数个规定格式的头字段，其后是任意文本的字段内容部分。

头子段通常由关键字、冒号、关键字的参数组成，格式允许将长行分成多行。最常用的关键字有 From、To、Subject 和 Date。下面是一个例子：

```
Date: Mon, 10 Mar 2008 10:37:17 (EDT)
From: "William Stallings" <ws@host.com>
Subject: The Syntax in RFC 822
To: Smith@Other-host.com
Cc: Jones@Yet-Another-Host.com

Hello. This section begins the actual message body, which
is delimited from the message heading by a blank line.
```

Message-ID 也是 RFC 822 头里经常出现的字段。这个字段包含了与这封邮件有关的一个唯一标识符。

10.1.3　多用途因特网邮件扩展

多用途因特网邮件扩展（MIME）是 RFC822 框架的一个扩展，用来解决电子邮件使用

SMTP 和 RFC822 时遇到的一些问题和限制。

[PARZ06] 列出了 SMTP/822 方案中的一些限制：

1）SMTP 不能传输可执行文件或二进制对象。可以使用一些方案将二进制文件转化为 SMTP 邮件系统使用的文本形式，如常用的 UNIX 的 uu 编码 / 解码方案。但是这些方案都不是一个标准甚至不是约定俗成的惯例。

2）SMTP 不能传输包含国际语言字符的文本数据，因为这些字符由值为十进制 128 或更大的 8 比特码组成，而 SMTP 只允许使用 7 比特 ASCII 码。

3）SMTP 服务器可能拒绝超过一定大小的邮件消息。

4）SMTP 网关将 ASCII 码转译为字符码 EBCDIC 时，不使用统一的映射集。因此会导致转译出现问题。

5）SMTP 连接 X.400 邮件网络的网关无法处理 X.400 邮件里的非文本数据。

6）有些 SMTP 实现时不完全遵照 RFC821 中规定的 SMTP 标准。以下列出常见问题：

- 增减或重排回车和换行符
- 截断或覆盖超过 76 字符的行
- 删除尾部的空格（tab 或空格符号）
- 将邮件中的行补齐同一长度
- 将 tab 符号转换成多个空格符

这些限制使加密电子邮件以及用 SMTP 传输多媒体文件和电子数据交换（EDI）邮件变得很困难。MIME 旨在与现存的 RFC822 实现兼容的同时解决这些问题。

概述　MIME 规范包含以下要素：

1）定义了 5 种新邮件头字段，这些头字段可能在一个 RFC822 头的内部。这些字段提供邮件体的信息。

2）定义了一些内容格式，规范支持多媒体邮件的表示。

3）定义了传输加密，对所有内容格式的邮件进行转换，防止其在邮件系统中被篡改。

以下是 MIME 定义的 5 种邮件头字段：

- MIME-Version：参数值必须为 1.0。这个头字段表明此邮件遵从 RFC 框架。
- Content-Type：详细描述邮件体中包含的内容，接收用户代理可以选择合适的代理或机制向用户显示数据或合理地处理数据。
- Content-Transfer-Encoding：将邮件内容表示为适合邮件传输的格式所使用的转换类型。
- Content-ID：用以在多种环境下唯一识别 MIME 实体。
- Content-Description：对邮件体对象的纯文本描述。当对象不可读（如音频数据）时有很大用处。

一个普通 RFC822 头中可能会出现一部分或全部这些头字段。兼容实现必须支持 MIME-Version、Content-Type 和 Content-Transfer-Encoding 头字段，Content-ID 和 Content-Description 是可选的，可能被收件方忽略。

MIME 内容类型　MIME 规范的大部分内容是关于各种内容类型的定义。这是因为在多媒体环境下，我们需要一个标准方法去处理这些多种多样的信息。

表 10-2 列出了 MIME 内容类型。一共有 7 种主类和 14 种子类。一般来说，内容类型表明了数据的总类型，子类具体解释了数据类型的特定格式。

表 10-2　MIME 内容类型

类　型	子　类	描　述
Text	Plain	未格式化文本，可能是 ASCII 码或 ISO8859 字符
Multipart	Mixed	各部分独立但是一起传输
	Parallel	它们应以在邮件中的顺序展示给收件人
	Alternative	除了没有规定展示给收件人的顺序，其余与 Mixed 一样
	Digest	各部分是对同样信息的多个版本。它们与原版的相似度递增排序，收件方邮件系统应该选择最好的版本
		与 Mixed 相似，但是每个部分的默认类型 / 子类是 message/rfc822
Message	rfc822	内容本身是一个封装的 RFC822 邮件
	Partial	大邮件内容分块时使用，对收件人透明
	External-body	包含指向位于别处的对象的指针
Image	jpeg	JPEG 格式 JFIF 加密的图片
	gif	GIF 格式图片
Video	mpeg	MPEG 格式
Audio	Basic	单信道 8 比特 ISDN，以采样频率 8kHz 进行 μ 律编码[⊖]
Application	PostScript	Adobe PostScript
	octet-stream	由 8 比特字节组成的一般二进制数据

10.1.4　POP 和 IMAP

邮局协议和因特网邮件访问协议支持从保存邮件的服务器（邮件存储区）收取邮件到客户端系统（邮件用户代理）。

邮局协议　POP 第三版，即 POP3，是在 RFC1399 中定义的因特网标准。POP3 支持邮件收取的基本功能——下载邮件和删除邮件。MUA 使用端口 110 建立到 MS 的 TCP 连接以完成收取功能。这种交互经历 3 个不同阶段：

- **验证阶段**：这个阶段中，客户端向服务器验证自己的用户身份。一般使用简单的用户 ID/ 密码的组合，当然也有更为复杂的选项。
- **交易阶段**：当服务器成功验证客户端，此客户端就可以访问邮箱，收取和删除邮件。
- **更新阶段**：在这个阶段中，服务器确认完成客户指令指示的所有改动，然后关闭连接。

因特网邮件访问协议　IMAP 第 4 版由 RFC3501 定义。与 POP 类似，IMAP4 服务器存储邮件，不同用户通过客户端请求获取邮件。但是 IMAP4 模型向用户提供更多功能，包括以下特性：

- 客户端可以拥有多个远端邮箱。
- 客户端可以详细指定下载邮件的要求，如不在链接缓慢时传输大邮件。
- IMAP 始终在服务器保存邮件，向客户端复制邮件的副本。
- IMAP4 允许客户端在连接服务器和没有连接时进行操作。当客户端未连接到服务器（称为未连接客户端）时，通过服务器和客户端间的周期同步使客户端进行的改变在服务器生效。

10.2　网页访问和 HTTP

超文本传输协议（HTTP）是万维网（WWW）的基础协议，可以在包含超文本的任何客户 /

⊖ 是音频编码的一种方法。

服务器应用中使用。这个名字有些误导人，其实 HTTP 并不是一个传输超文本的协议，而是一个以超文本跳转所需要的效率传送信息的协议。协议可以传送纯文本、超文本、音频、图像或任何因特网可以访问的信息。

我们先概述 HTTP 的概念和运行，然后介绍一些细节，讨论将要使用的因特网标准 HTTP1.1 版本。表 10-3 列出了 HTTP 规范所定义的一些重要术语，在之后的讨论中都会一一介绍。

表 10-3　HTTP 相关的关键术语

缓存 程序对响应消息的本地存储和控制消息存储、获取和删除的子系统。缓存存储可缓存地响应以减少未来相同请求的响应时间和网络带宽消耗。任何服务器和客户端都可以包含缓存，但当服务器作为隧道时无法使用缓存	**源服务器** 资源所处或将要创建的服务器
客户端 建立连接以发送请求的应用程序	**代理** 同时扮演服务器和客户端的角色以代表其他客户端发出请求的中介程序。它们对经过的消息进行一些翻译再转送到其他服务器上。代理在转发前必须翻译甚至重写消息。代理通常作为客户方通过网络防火墙的门户并作为帮助应用处理用户代理没有实现的协议的请求
连接 两个应用程序为通信建立的一个传输层虚拟电路	**资源** 网络数据对象或服务，由 URI 表示
实体 数据源或服务器回复的一种表示，可能包含在一个请求或响应消息中。实体包括实体标题和实体主体	**服务器** 接收连接以响应服务请求的应用程序
网关 扮演其他一些服务器的中介角色的服务器。不像代理，网关像请求资源所在的源服务器一样接收请求，发出请求的客户端不会意识到是在跟网关通信。网关一般用于服务器方通过网络防火墙的门户，并作为访问非 HTTP 系统资源的协议翻译器	**隧道** 扮演两个连接中的盲中继角色的中介应用。尽管隧道可能有一个 HTTP 请求发起，但隧道一旦启用，就不在是 HTTP 通信中的一方了。当中继连接中的两端关闭，隧道就终止退出。隧道在需要门户但是中介无法或不应翻译中继通信时使用
消息 HTTP 通信中的基本单元，由一串结构化八字节序列组成	**用户代理** 发起请求的客户端。一般是浏览器、编辑器、搜索引擎或其他终端用户工具

10.2.1　HTTP 概述

HTTP 是面向事务的客户 / 服务器协议。最典型的 HTTP 应用就是网页浏览器和网络服务器之间的连接。为了传输可靠性，HTTP 使用 TCP。然而，HTTP 是一个**无状态协议**，每个事务独立处理。相应的，尽管规范没有定义事物间的一对一连接及连接的寿命，一般的实现会为每个事务创建一个新的客户端和服务器间的 TCP 连接，一旦事务完成就关闭连接。

HTTP 协议无状态的特性非常适合基于它的常见应用。用户与网络服务器之间的一次普通会话包括获取网页和文档序列。理想状态是这个序列的获取十分迅速，网页和文档可以位于很多广泛分布的服务器上。

HTTP 的另一个重要特性是它可以处理多种格式。当客户端向服务器发起一个请求，请求中可能包含它所能处理的格式优先列表，服务器以合适的格式回复客户端。比如，Lynx 浏览器无法处理图像，网络服务器就无需在网页中传送图像。这种安排防止传输无用的信息并提供了新标准化和专有规范扩展格式集的基础。

图 10-3 给出了 HTTP 运行的 3 个例子。最简单的例子是用户代理与源服务器直接建立连接。**用户代理**是发起请求的客户端，如终端用户运行的网页浏览器。**源服务器**是需求资源所

在的服务器，比如想浏览的网页所在的网络服务器。这种情况下，客户端建立一个到服务器的端到端 TCP 连接，然后发送 HTTP 请求。HTTP 请求包含一个特定的命令（即方法）、地址[即统一资源定位符（URL 的附录 C 中给出了一些关于 URL 的信息）]、包含请求参数的类 MIME 消息和客户端的信息，有可能还有一些附加内容信息。

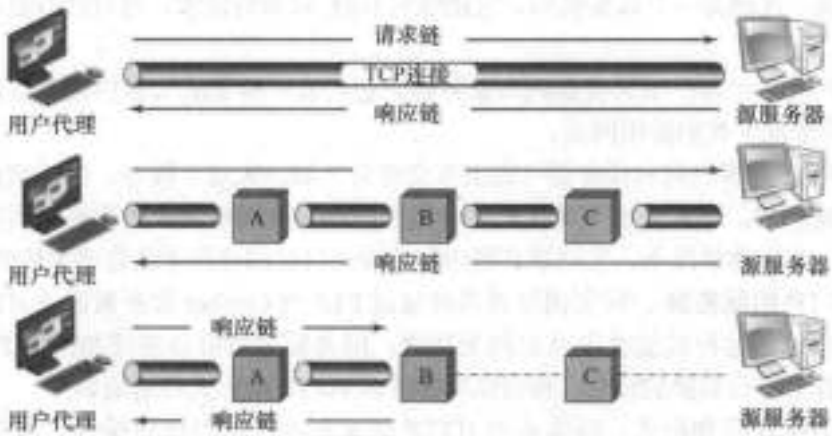


图 10-3　HTTP 运行举例

当服务器接收到请求，它就进行所请求的行为并返回一个 HTTP 响应。响应包括状态信息、成功 / 错误码、包含服务器信息的类 MIME 消息和关于响应本身的信息，有可能还有一些正文内容。之后 TCP 连接就关闭了。

图 10-3 的中间部分给出了一个不是端到端的 TCP 连接的例子，在用户代理和服务器之间有一个或多个中介系统和逻辑上毗邻系统间的 TCP 连接。每个中介系统作为一个中继，所以客户端发起的请求通过这些中介系统中继到服务器，服务器的响应再这样中继回客户端。

图 10-4 画出了 HTTP 规范定义的 3 种形式的中介系统：代理、网关和隧道。

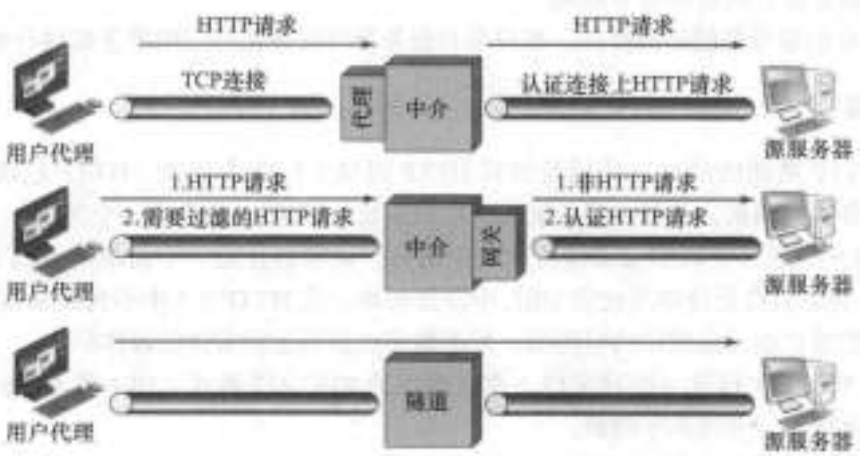


图 10-4　HTTP 中介系统

代理　代理作为其他客户端的代表向服务器发送客户端的请求。代理与客户端交互时就如同是一个服务器，而在于服务器交互时如同一个客户端。有两种情况下我们使用代理：

- **安全中介**：客户端和服务器可能由安全中介（如防火墙）隔开，代理位于防火墙隔开的客户端所在的一边。一般，客户端在防火墙所保护的安全网络之中，而服务器则在

安全网络之外。在这种情况下，服务器必须向防火墙验证自己的身份才能与代理建立连接。当响应通过防火墙后代理才接受响应。

- **HTTP 版本不同**：如果客户端和服务器运行在不同的 HTTP 版本上，代理可以实现两种版本并建立所需的映射。

总的来说，代理是一个转发机构，它接收对 URL 对象的请求，进行修改后再转发到目标服务器上。

网关　网关对于客户端来说如同源服务器。它代表一些无法与客户端直接连接通信的服务器。有两种情况下我们使用网关：

- **安全中介**：客户端和服务器可能由安全中介（如防火墙）隔开，网关就作为服务器端通过防火墙。通常，服务器在防火墙所保护的安全网络之中，而客户端则在安全网络之外。在这种情况下，客户端必须向网关验证自己的身份才能将请求传到服务器。
- **非 HTTP 的服务器**：网页浏览器具有通过 FTP 或 Gopher 服务器而非 HTTP 连接服务器的功能，这种功能也可以由网关提供。网关服务器可以连接相关的 FTP 或 Gopher 服务器来得到需要的结果，再将结果转换成 HTTP 的形式传送给客户。

隧道　不像代理和网关，隧道不对 HTTP 请求和响应进行任何操作。隧道仅仅是两个 TCP 连接的一个简单的中继点，其中传输的 HTTP 消息不会发生任何改变，就如同用户代理和源服务器中间只有一个 HTTP 连接。当客户端和服务器中需要一个中介系统但又不需要理解消息的内容时我们就使用隧道。比如在防火墙之外的一个客户端或服务器可以建立一个认证的连接，而这个连接仍用于 HTTP 事务。

缓存　再看一看图 10-3，图的最后一部分是缓存的例子。缓存是一个可以存储之前请求和响应以处理新的请求的设施。如果新到的请求与已存储的请求一致，缓存就直接给出已经存储的响应而不去访问资源的 URL。缓存可以在客户端、服务器以及除了隧道以外的中介系统中。在图上，中介 B 缓存了一个请求 / 响应事务，所以相应的新请求不需要再通过整个过程连接到源服务器，而直接由 B 处理。

不是所有的事务都能够被缓存，客户端和服务器可以指定特定的事务被缓存的时间限制。

10.2.2　消息

解释 HTTP 功能的最好方式就是解释 HTTP 消息中的每个要素。HTTP 包含两类消息：客户端向服务器的**请求**，和服务器回复客户端的**响应**。图 10-5 给出了一个例子。

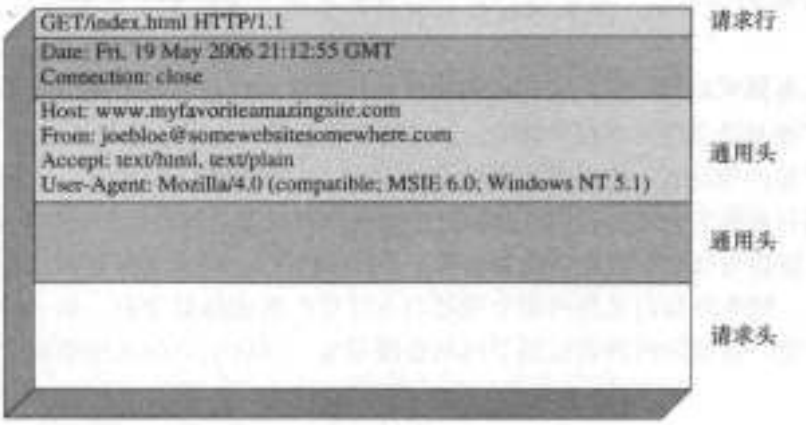
HTTP/0.9 中定义了简单请求和简单响应消息。请求消息是一个简单的 GET 命令和所请求的 URL，响应消息是简单的包含 URL 中信息的块。在 HTTP/1.1 中不再鼓励这种简单的形式，因为这使客户端无法使用内容协商，服务器无法指明返回实体的媒体形式。

所有的 HTTP 头包含一序列字段，遵从通用的 RFC 822 格式（10.1 节）。每个字段新起一行，包括字段名、分号和字段值。

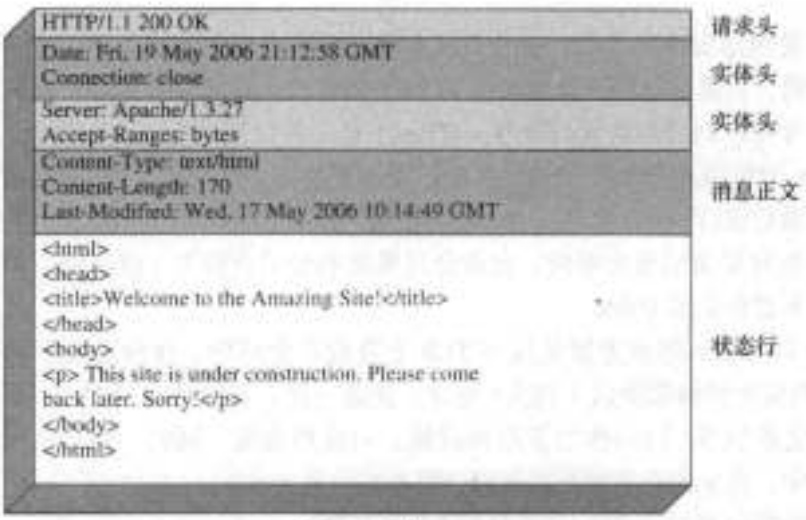
一个完整的请求包含以下字段：

- **请求行**：表明是一个请求消息，说明请求的资源和消息所用的 HTTP 版本。
- **通用头**：包含适用于请求消息而不是传输实体的字段。
- **请求头**：包含请求和客户端的信息。比如请求可能是有条件的，请求头中会指明在什么条件下进行请求。请求头中的字段也可能指明客户端能够处理的格式和编码。
- **实体头**：包含所请求资源的信息和实体正文的信息。

- **实体正文**：消息的正文。



a）HTTP请求



b）HTTP响应

图 10-5　HTTP 消息格式举例

响应消息结构与请求消息相同，但是将请求行和请求头由以下头部替换：

- **状态行**：指明消息所用的 HTTP 版本并提供响应的状态信息。如“OK”表示请求成功完成。
- **响应头**：提供状态行中状态信息的扩展信息。

10.3　网络安全

万维网的本质是运行于整个因特网和 TCP/IP 内网的一个客户 / 服务器应用。[GARF02] 中指出网络的使用面临以下安全挑战：

- 网络难以无法抵御因特网中对网络服务器的攻击。
- 网络中公司和产品的信息都一目了然，网络也是商业交易的平台。因此当网络服务器被攻击会造成大量的名誉和金钱损失。
- 网页浏览器易于使用，网络服务器也易于配置和管理，网页内容则越来越便于开发，

但是相关的软件却十分复杂。这些复杂的软件可能隐藏了很多潜在的安全缺陷。在网络短短的历史中，最新更新正常安装的系统无法抵御多种安全攻击的例子比比皆是。

- 网络服务器可以用作进入公司或机构全部计算机的跳板。一旦网络服务器被破坏，攻击者可能有机会访问不在网络中，但连接到服务器的本地数据和系统。
- 网络应用的使用者一般是任意的未受过训练（安全方面）的用户。这种用户可能无法意识到存在的安全风险，也可能没有工具或知识对安全风险做出合理的应对。

网络安全威胁可以根据威胁的位置分类：网络服务器、网页浏览器和浏览器与服务器之间的网络通信。服务器和浏览器的安全问题归入计算机系统的安全中，本书的第六部分将大体介绍系统安全，这部分内容也适用于网络系统安全。通信安全归入网络安全，将在本节中介绍。

10.3.1　网络通信安全防护

有许多防护网络安全的手段，这些各式各样的防护手段在其所提供的服务和使用的机制上是大致相同的，但是在适用的领域和在 TCP/IP 协议栈中的相对位置各不相同。

第 8 章中介绍的因特网协议安全性（IPSec）是一种保护网络安全的技术。使用 IPSec 的优势在于 IPSec 对终端用户和应用透明并提供通用解决方案。另外，IPSec 具有过滤功能，可以选中特定的通信进行 IPSec 处理。IPSec 的缺点是需要在支持网页浏览器和服务器的所有系统上设置一个相对复杂的安全架构。允许公司系统和公司合伙人（供应商、顾客）系统接入的公司网络就不适合使用 IPSec。

另一个相对通用的解决方案是仅在 TCP 上进行安全防护，这种安全手段由安全套接层 (SSL) 和之后的安全传输层协议（TLS）定义。在这一层，有两种实现方式。为了达到完全通用性，SSL（或者 TLS）可以作为下层协议簇，对应用透明。同时，SSL 也可以嵌入特定的包中。在网络中，几乎所有的浏览器和网络服务器均包含 SSL。

本章剩下的部分将讨论 SSL/TLS 和相关的 HTTPS。

10.3.2　安全套接层

图 10-6 说明了 TCP/IP 架构中 SSL 所处的位置。在讨论这个架构之前，我们需要先定义套接字。本质上，套接字就是在 TCP/IP 网络中将数据指向相应应用的方法。主机的 IP 地址和 TCP 端口号组成套接字地址。从应用的角度来看，套接字接口是应用程序编程接口（API）。套接字接口是一个通用通信编程接口，在 UNIX 和许多其他系统中实现。两个应用通过 TCP 套接字通信，一个应用通过套接字地址连接 TCP 并向 TCP 告知请求的远程应用的套接字地址。



图 10-6　SSL 在 TCP/IP 架构中的位置

配置了 SSL，一个应用就具有一个 SSL 套接字地址并可以与远程应用的 SSL 套接字通信。SSL 所提供的安全功能对应用和 TCP 透明，因此不需要对 TCP 和应用进行修改就可以使用 SSL 的安全特性。如图 10-6 所示，SSL 不仅支持 HTTP，还支持任何使用 TCP 的应用。

SSL 提供 3 类安全性：

- **保密性**：两个应用（如两个 HTTP 模块）间传递的所有数据经过加密，防止在网络中被窃听。
- **信息完整性**：SSL 确保信息不在传输途中被篡改或替换。
- **身份验证**：SSL 验证信息交换一方或双方的身份。

SSL 包含两个阶段：握手和数据传输。在握手阶段，双方互相验证身份并创建数据传输使用的加密密钥。在数据传输阶段中，双方使用加密密钥加密所有传输数据。

10.3.3　HTTPS

HTTPS（SSL 上的 HTTP）指结合 HTTP 和 SSL 实现网页浏览器和网络服务器间的加密通信。所有当前的网页浏览器都具有 HTTPS 功能。如果网络服务器支持 HTTPS 通信就可以使用其安全功能，搜索引擎不支持 HTTPS。

HTTP 和 HTTPS 的主要区别在于，用户在浏览器中看到的 URL 地址不是以“http://”开头，而是“https://”。普通的 HTTP 连接使用 80 端口，如果指定了 HTTPS，则指定 443 端口，就会开启 SSL。

使用 HTTPS 时，通信的以下内容被加密：

- 请求文档的 URL
- 文档的内容
- 浏览器表单的内容（由用户填写）
- 浏览器发送给服务器和服务器发送给浏览器的 cookie
- HTTP 头的内容

10.4　多媒体应用

宽带技术的普及引发了人们越来越多的对于基于网络和因特网的多媒体应用的兴趣。术语多媒体和多媒体应用在文献和商业出版物中使用得比较随便，并没有统一的定义。首先，我们在表 10-4 给出了术语的定义。

表 10-4　多媒体技术

媒体
指信息的形式，包括文本、静态图像、音频和视频
多媒体
使用文本、图像、声音和视频的人机交互。多媒体也指存储多媒体内容的存储设备
流媒体
指当计算机收到文件后立即可以播放的多媒体文件，如视频剪辑和音频。这类媒体类型不必等到整个文件下载完才开始播放

一种把多媒体相关概念组织起来的方法是了解这一领域依据多个维度分类的方式。图 10-7 从 3 种角度分析了多媒体应用：媒体类型、应用、支持应用的技术。

10.4.1　媒体类型

一般来说，多媒体指 4 种不同的媒体类型：文本、音频、图像和视频。

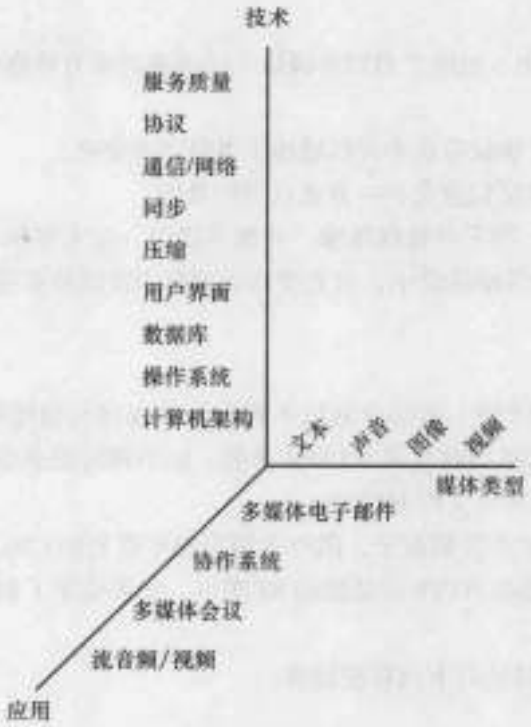


图 10-7　多媒体分类

从通信的角度，**文本**不言自明是指可以通过键盘输入或直接可读可打印的信息，例如文本消息、即时消息、文本（非 html）邮件、聊天室、留言板等。然而，文本也经常用于更广泛的意义，指可以存储在文件和数据库中与另三类不同的数据。例如，某个企业的数据库中存储的数字数据文件，这些文件以比可打印字符更紧凑的格式存储。

音频一般包括两种不同的声音范围。语音或讲话指人所发出的声音。一般来说，传输语音只需要较低的带宽（低于 4kHz）。电话技术和相关的应用（如语音邮件、电话会议、电话营销）是常见传统语音通信技术的应用，音乐应用（包括下载音乐文件）需要更宽的频谱。

图像服务支持单个图片、图标或图画的传输。基于图像的应用包括传真、计算机辅助设计（CAD）、出版、医疗成像等。图像可以由矢量图形格式表示，例如在画图程序和 PDF 文件中。光栅图形格式的图像表示为点的二维数组，即像素[⊖]。压缩的 JPG 格式就是由光栅图形格式衍生而成的。

视频服务按时间传送图像序列。实际上，视频使用光栅扫描图像序列。

10.4.2　多媒体应用

以前，因特网主要由信息检索应用、邮件、文件传输和注重文本和图像的网页界面占据。现在，网络越来越多地用于多媒体应用，包含大量可视化数据，支持实时交互。流音频和视频可能是这些应用中最知名的。包含分布式仿真和实时用户交互的虚拟培训环境就是一种交互应用。表 10-5 中介绍了其他一些例子。

⊖　像素（或图像元素）是指数字图像中可以指定灰度的最小元素。像素同时也是图像点阵表达中的一个点。

表 10-5　多媒体信息领域和应用实例

领　域	应用实例
信息管理	超媒体、多媒体数据库、基于内容检索
娱乐	电脑游戏、数字视频、音频（MP3）
通信	视频会议、共享工作区、虚拟社区
信息发布 / 送达	网上培训、电子书、流媒体

多媒体应用领域包括以下部分：

- **多媒体信息系统**：数据库、信息站、超文本、电系数、多媒体专家系统。
- **多媒体通信系统**：计算机协作、视频会议、流媒体、多媒体远程服务。
- **多媒体娱乐系统**：3D 电脑游戏、多人网络游戏、娱乐资讯、交互视听产品。
- **多媒体商务系统**：仿真电子交易、营销、多媒体展示、视频说明书、虚拟购物等。
- **多媒体教育系统**：电子书、多样的教学材料、仿真系统、自动测试、远程学习等。

图 10-7 中高亮的部分值得注意。尽管传统的多媒体意味着同时使用多种媒体类型（如文本文档的辅助视频），现在多媒体一词也指实时处理和通信的单独视频或音频应用。因此，尽管像 VoIP、流音频、流视频只有单个媒体类型，也被归为多媒体应用。

10.4.3　多媒体技术

图 10-7 中列出了一些支持多媒体应用的相关技术。可以看到，多媒体应用包含了许多技术。列表中最底下的四项本书将不涉及，其他几项仅是多媒体通信和网络技术中的一部分，我们将在本书中讨论这些技术。这里我们先对每一部分简要介绍一下。

- **压缩**：数字视频和一小部分音频会消耗大量网络流量，传送至多个用户的流应用更加增加了流量。为此开发了标准，压缩这些内容以大大减少流量的消耗。最著名的标准是静止图像中的 JPG 和视频中的 MPG。
- **通信 / 网络**：这个大类指支持大容量多媒体流量的传输和网络技术（例如 SONET、ATM）。
- **协议**：许多协议帮助支持多媒体的传输。比如实时传输协议（RTP），设计这个协议是为了支持非弹性的传输。RTP 通过缓冲和弃置策略保证终端用户接受流畅连续的实时传输。比如会话发起协议（SIP），是一个应用层控制协议，用以建立、修改、终止 IP 数据网络中的实时会话。
- **服务质量**：因特网和其下层的局域或广域网必须包含服务质量（QoS）功能以向不同类型的应用传输提供不同级别的服务。QoS 功能可以处理优先级、延时限制、延时可变性限制和其他类似要求。

10.5　可接受使用策略

在办公环境中，几乎每个员工都可以使用电子邮件或访问因特网，即使在其他环境比如工厂中，也至少有一部分员工可以享受这些功能。越来越多的公司将指定的电子邮件和因特网使用策略纳入组织的安全策略文档中。这一部分详细介绍这些策略的重要内容。

10.5.1　动机

电子邮件和因特网在员工中的普及给雇主带来了一些顾虑：

1）大量员工可能浪费工作时间做一些跟工作无关的事情，如上网、玩网络游戏、网上购物、网上聊天或发送和阅读私人邮件。

2）大量计算机和通信资源被与工作无关的活动耗费，影响 IS 资源本应支持的任务。

3）过度和随意使用因特网和电子邮件增加了恶意软件入侵组织 IS 环境的风险。

4）员工经常进行与工作无关的活动会损害企业或企业以外个人的利益，进而造成企业的损失。

5）员工可能使用电子邮件和因特网骚扰其他员工。

6）员工不合适的网上行为可能影响公司的名誉。

10.5.2　策略

完整的邮件和因特网使用策略的开发包含许多策略问题。以下是基于 [KING06] 的推荐策略集：

- **仅供商业使用**：公司邮件和因特网访问仅供员工进行公司商务时使用。
- **策略范围**：策略覆盖电子邮件的访问、电子邮件的内容、因特网和内部网通信以及电子邮件、因特网和内部网的纪录。
- **内容所有权**：电子通信、文件、数据在通过非公司所有的设备传输时所有权仍归公司所有。
- **隐私**：员工在使用公司提供的电子邮件和网络访问时没有隐私，即便通信内容是私人的。
- **行为标准**：员工在使用公司提供的电子邮件和网络访问时应具备良好的判断力、礼仪和专业素养。
- **合理的私人使用**：在不影响员工本人职责，不侵犯公司策略，不过分占用公司设施的情况下，员工可以合理地使用公司提供的电子邮件和网络访问处理私人事宜。
- **禁止非法行为**：员工不可以使用公司提供的电子邮件和网络访问进行任何非法行为。
- **安全策略**：员工使用电子邮件和网络访问时必须遵从公司安全策略。
- **公司策略**：员工使用电子邮件和网络访问时必须遵从公司其他的策略。公司策略禁止查看、储存或分发色情内容，禁止在通信中骚扰或歧视他人，禁止未经授权泄露公司机密或专有信息。
- **公司权利**：公司可以访问、监控、截听、拦截、检查、复制、揭发、使用、毁坏、恢复或保留任何此策略中涵盖的通信、文件或任何数据。员工需按要求提供密码。
- **纪律处分**：违反此策略将立即解除雇佣关系或给予其他适宜的处分。

表 10-6 给出了可接受的使用策略在企业中如何使用的建议。

10.5.3　策略制定指南

制定电子邮件和因特网使用策略时可以参考西澳大利亚电子政府办公室给出的《电子邮件和因特网使用策略制定协助指南》（2004.7），或者也可以参考 SANS 研究所给出的《可接受使用策略文档》中的例子（2003），本书的附加内容网站上也有一些相关文档。

表 10-6　可接受使用职责

行　为	执行发起人	所有经理	系统管理员	CISO	所有员工	审计师
通知用户	X	X		X		A
处分用户	X	X		C		A
合理获取硬件和软件	X	X		C		X/A
遵守版权和许可	X	X	X	X	X	X/A
遵守私人财产策略	X	X	X	X	X	X/A
保护知识产权	X	X	X	X	X	X/A
遵守电子邮件策略	X	X	X	X	X	X/A
遵守电子邮件加密策略	X	X	X	X	X	X/A
遵守因特网策略	X	X	X	X	X	X/A
遵守信息资源策略	X	X	X	X	X	X/A

注：CISO 指首席信息安全官，X 指负责完成，C 指提供咨询支持，A 指独立合规审计。

应用注解

提供服务与否

网络服务器和邮件服务器可能是最难管理的一类系统。这些服务器时常拥塞一堆来自有效用户的请求，也时常被非有效用户攻击。在一个企业决定部署其中一种服务器前首先需要自问几个问题。很多时候，其实并不需要内部管理这类服务。

可能最合适的第一个问题是决定系统需要做什么，也就是说你想要什么。对于邮件服务器，需要考虑需要多少账户、怎样的安全性、内部邮件还是外部邮件。小公司和私人企业可以使用免费的邮件服务，比如 Gmail。这样虽然无法提供组织身份但可以解决通信的问题。

小型家居办公（SOHO）一类的公司可能使用因特网服务提供商（ISP）或特定托管公司托管他们的网页。这样他们既可以拥有公司的主页又不需要自行运行一个网页服务器。除此之外，网站托管服务或 ISP 一般会替你注册一个域名。只需要很少的花销（一般少于 100 美元 / 年）就可以提供企业身份，多半还包括一些电子邮件账户、安保和登录工具以及管理服务。

使用网站托管和 ISP 或托管公司的邮件服务可以满足员工较少的公司的需求。多支付一些钱可以增加账户的数量，扩展网站空间和脚本。然而有时这种外部服务不那么合适。对于拥有上百人的大型企业，复杂的人力资源和内部通信需求以及完整的 IT 部门，这种情况下显然自己运行服务会更为合适。

对于没有准备好的人来说，建立内部电子邮件和网络服务器是一项艰巨的任务。和大多数安装一样，在机器上安装软件或建立一些账户并不难，维护系统和系统的安全问题才是麻烦所在。另外，安装内部服务会影响其他系统。比如如果你自行运行个人网站来进行销售或提供支持服务，该如何应对网站出问题关闭的情况？网站受到几次攻击？网络利用率如何？在安装系统前理解系统的运行和要求十分重要。

当运行公司外部网络可以访问的网络或邮件服务器时，所有配置的防火墙需要更新以允许这种通信。这直接与应用使用的端口有关。防火墙规则也可以根据 IP 地址来写。另外，必须要考虑客户端软件的类型，因为不是所有的外部系统都符合要求。用户是不

是随身携带笔记本？如果是，他们可能需要额外支持和一整套应用。他们从外部访问内部资源吗？他们需要虚拟专网（VPN）访问吗？从餐厅无线热点接入的访问是不是需要额外的安全防护呢？

对于那些经常处理敏感数据或需要满足合规事宜的企业，允许外部访问有些棘手。这种情况下，安全将是第一要务，加密和防火墙是重点。建立安全策略时应谨慎考虑允许外部接入内部系统的员工。一般公司有两套运行的服务器，内部和外部使用分开。比如，员工信息和福利运行在内部服务器上，而公司网站和联系信息运行在外部服务器上。认证服务器结合网站特征部署。

对于运行服务器的员工，无止境的安全补丁和病毒防护花费大量的时间。在我们筛选掉现有的安全装置时，新的安全装置就出现了，就跟旧的漏洞被去除，新的病毒又来了一样快。病毒非常棘手，很多管理员不得不自己在服务器上过滤大量邮件。就是说许多邮件到达终端用户时附带了潜在危险文件如何从原始邮件被自动删除的备注，尤其是可执行文件。终端用户也应该在本地机器上运行病毒防护软件检查收到的邮件。最后，真正的问题是病毒可能绕过安装的防护软件或者防护软件无法发现病毒。要解决这个问题只能对所有人进行培训。

自己运行服务有利有弊。一方面，本地设置允许量身定制安全变化，加快创建账户以及定制内容。另一方面，服务器管理的问题、花销和人力使得外部维护更具优势。

10.6　总结

标准化分布式应用对于商业十分重要的三大理由：

- 标准化应用比专用应用更易于获取和使用，专用应用可能没有足够的支持和培训。
- 标准化软件允许用户从不同供应商中获得计算机并使这些计算机一起工作。
- 标准利于不同公司间交换数据。

本章介绍三个重要的分布式应用。为这些应用指定了标准，这些标准也被越来越多的应用采纳。

通用邮件设施提供交换非结构化消息（一般是文本消息）的方式。电子邮件是一种方便快捷的通信方式，可以辅助甚至替代电话和纸质通信。电子邮件本质上就具有通用的特点，所以它可能是最受欢迎并且最有用的分布式应用。

电子邮件传输最广泛使用的协议是 SMTP。SMTP 假定邮件的内容是简单的文本块。最近的 MIME 扩展了 SMTP 以支持多媒体信息的传输。

网络能快速普及归功于支持网络应用所有要素的标准。其中一个要素是 HTTP，负责网页浏览器和网络服务器间信息交换的协议。HTTP 网络中可以使用三种中介设备：代理、网关和隧道。HTTP 使用请求 / 响应式通信。

案例学习 VII：Guardian Life 的电子商务

本案例中的主要概念包括电子商务 / 数字商务、门户网站。**本案例学习的更多内容请参考** www.pearsonhighered.com/stallings。

10.7　关键术语、复习题和练习题

关键术语

acceptable use policy（可接受使用策略）
Administrative Management Domain（ADMD，经营管理域）
Domain Name System (DNS，域名系统）
electronic mail（电子邮件）
HTTP gateway（HTTP 网关）
HTTP method（HTTP 方法）
HTIY proxy（HTTP 代理）
HTIY tunnel（HTTP 隧道）
Hypertext Transfer Protocol（HTTP，超文本传输协议）
Intemet Message Access Protocol（IMAP，因特网邮件访问协议）
Mail Delivery Agent（MDA，邮件投递代理）
Message Handling Service（MHS，邮件处理服务）
Message Store（MS，邮件存储区）
Mail Submission Agent（MSA，邮件提交代理）
Message Transfer Agent（MTA，邮件传输代理）
Message User Agent（MUA，邮件用户代理）
multimedia（多媒体）
Multipurpose Intemet Mail Extensions（MIME，多用途因特网邮件扩展）
Post Office Protocol（POP，邮局协议）
Simple Mail Transfer Protocol（SMTP，简单邮件传输协议）
Uniform Resource Locator（URL，统一资源定位符）

复习题

10.1　SMTP 使用哪个端口？
10.2　RFC 821 和 RFC 822 的区别是什么？
10.3　SMTP 和 MIME 标准分别是什么？
10.4　MIME 弥补了 SMTP 的哪些不足？
10.5　HTTP 是个无状态协议是什么意思？
10.6　解释 HTTP 代理、网关和隧道的区别。
10.7　HTTP 中缓存的作用是什么？
10.8　HTTP 使用哪个端口？

练习题

10.1　每个电子邮件系统处理多收件人的方式不同。在一些系统中，原始发件人用户代理进行所需的拷贝然后分别送往不同的地方。另一种方法是先决定到每个终点的路径，然后在共同的路径上传输单个邮件，只有路径分叉了才复制邮件，这个过程叫做邮件装袋。请对两种方法的优缺点进行讨论。

10.2　不考虑连接的建立和结束，请问使用 SMTP 传送一封小的电子邮件所需的最少的网络往返次数是多少？

10.3　假设你需要传送一个邮件给 3 个不同的用户：user1@example.com, user2@example.com, user3@example.com。请问分别传送 3 个用户分开的信息和只传送一次信息但有 3 个接收者有什么不同吗？并解释。

10.4　用户可以自由地定义和使用额外的头部字段（除在 RFC 87 中定义的头部字段），该头部字段必须以“X-”开始，请问为什么？

10.5　假设你对于邮件账户 user@example.com 遇到了一些技术问题，你应该联系谁去解决这些问题？

10.6　HTTP 缓存可以分别在服务器端、中间节点或者客户浏览器被控制。请问这种机制潜在的优点和缺点是什么（分别从服务端和客户端两个角度考虑）？

10.7　在 RFC 3298 中描述了 Spirits 协议的需求。请问什么是 Sprits？它与 SIP 和 PINT 有什么关系？

10.8　许多邮件客户端允许你查看邮件头部并显示该邮件传送的路径。请问你的邮件客户端是否有该功能？如果有的话，你会追踪邮件从发送端到接收端的路径吗？

10.9　请问你的邮件系统使用哪个 TCP 端口？

10.10　在观察你的邮件系统使用哪个端口时，请问你的机器使用哪个端口？

10.11　为什么对于本地系统的管理员来说了解哪些端口正在被程序使用是很重要的？

10.12　什么是 POP3 和 IMAP？

10.13　什么是 HTTPS？

10.14　Netmeeting 是一款 Windows 系统自带的网上聊天软件。它可以进行视频、语音或者视频语音结合的聊天。通过使用 Netmeeting 和一些基本聊天工具，如麦克风、喇叭、摄像头，可以在两端建立一个会话。请问这其中用到了哪些协议和编码？

因特网操作

学习目标

通过本章的学习，读者应该能够：

- 描述因特网寻址的原理并领会地址分配的关键点。
- 理解内部网关协议和外部网关协议的区别。
- 解释路由协议的基本原理。
- 理解服务质量。
- 解释弹性数据流和非弹性数据流的区别。
- 讨论由一个差异化服务设施提供的服务。

本章关注的是因特网底层的细节。我们首先解释了相对复杂的在一个分布广、数量大和动态的环境下的寻址问题。然后我们概述了路由协议，即如何通过路由器间的相互合作在因特网上寻找到一条从发送端到接收端的路径。之后我们引入了服务质量，着重于因特网上最重要的提供服务的方法，即差异化服务。最后我们介绍了关于服务水平协议和 IP 性能度量的相关内容。

11.1 因特网寻址

为了在因特网上识别一台主机，每个主机都需要被分配一个唯一的 IP 地址。一个 IP 地址由两个逻辑字段组成，其中一个字段是网络号，它标志一个主机所连接到的网络。第二个字段是主机号，它标志了之前网络号所表示的网络内的一台主机。主机号部分在它所分配的网络内必须是唯一的。因此，IP 地址可以表示成如下形式：

IP 地址 = < 网络号 >< 主机号 >

一个 IP 地址的网络号部分是由五个区域性的网址分配组织之一所管理的，主机号部分是由该网络的管理人员所分配。

在一台主机的操作系统启动时，一个 IP 地址被分配到该主机的网络接口。就如在第 7 章中所讨论的，IP 地址的获得可以通过查询配置文件或者动态地通过 DHCP 协议获得。

在这节中，我们分别查看 IPv4 和 IPv6 的形式。

11.1.1 IPv4 地址

IPv4 使用 32 位来表示一个 IP 地址。我们经常把 IP 地址中的每 8 位用其等效的十进制数字表示，这称为**点分十进制记法**。比如，一个 IP 地址为 11000000 11100100 00010001 00111001 可以写成 192.228.17.57。

1. 分类的 IP 地址

一般情况下，32 位的 IP 地址的最右端即低字节指明了一台主机，最左端即高字节指明

了所属的网络。一种固定的分配方式如16位表示网络号16位表示主机号，被认为对于整个因特网是不够分配的，因为有些组织可能会有很少的网络但是有很多主机而有些组织可能拥有很多网络但是只有一些主机。因此，分类的IP地址被大家接受。

分类的IP地址允许32位可以变化地分配为网络号和主机号。在这种体系下，最左边的几位表示了剩下的几位如何被分开成网络号和主机号。这种编码方式提供了一种灵活的分配方式并且允许因特网存在有不同大小的网络。A类地址最适合用在网络少但是每个网络都有许多主机的情况。A类地址有如下格式：

0	网络号（7位）	主机号（24位）

B类地址最适合用在网络数量中等、每个网络都有中等数量主机的情况。B类地址有如下格式：

1	0	网络号（14位）	主机号（16位）

C类地址最适合用在网络多但是每个网络只有不多的主机的情况。C类地址有如下格式：

1	1	01	网络号（21位）	主机号（8位）

一个组织可能会从这些类地址中分配到一个或多个块。

2. 子网和子网掩码

由于以下的需求子网的概念被引入。考虑到因特网包括一个或多个广域网以及许多站点，并且每个都会包含多个局域网。为了抵抗快速增长的网络数量以及路由算法的复杂度，我们要在一个组织内允许有任意复杂的互相连接的局域网结构，同时能够将它与整个因特网隔离。一个解决该问题的方法是分配一个单一的网络号给这个站点中的所有局域网，这样从其余的因特网的角度来看，那个站点对外表现为一个网络，从而简化寻址和路由。为了让在一个站点中的路由器能够正常工作，每个局域网需要分配一个子网号。将IP地址的主机号部分分为子网号和主机号以适应这种寻址方式。

在一个有子网的网络内，当地的路由器的路由规则必须基于一个扩展的网路号是由IP地址的网络号部分以及子网号组成。子网掩码表明了扩展的网络号所包含的比特数。子网掩码的使用可以让主机决定一个发出的数据包是传送给同一个局域网内的一台主机（直接传送）或者是在其他局域网内（将数据包发送给路由器）。这里假设有一些方法（如手动配置）创建了子网掩码并且使得本地的路由器都知晓该掩码。

表11-1展示了如何利用子网掩码进行计算。可以看到子网掩码的作用就是消去主机号的部分，剩下的就是网络号和子网号。

表11-1　IP地址和子网掩码

a）点分十进制和二进制表示的IP地址和子网掩码

	二进制表示	点分十进制
IP地址	11000000.11100100.00010001.00111001	192.8.17.57
子网掩码	11111111.11111111.11111111.11100000	255.255.255.224
IP地址与子网掩码按位与	11000000.11100100.00010001.00100000	192.28.17.32
子网号	11000000.11101011.00010001.001	1
主机号	00000000.00000000.00000000.00011001	25

（续）

b）默认的子网掩码		
	二进制表示	点分十进制
A 类地址默认子网掩码	11111111.00000000.00000000.00000000	255.0.0.0
A 类掩码示例	11111111.11000000.00000000.00000000	255.192.0.0
B 类地址默认子网掩码	11111111. 11111111.00000000.00000000	255.255.0.0
B 类掩码示例	11111111. 11111111.11111000.00000000	255.255.248.0
C 类地址默认子网掩码	11111111. 11111111.11111111.00000000	255.255.255.0
C 类掩码示例	11111111. 11111111.11111111.11111100	255.255.255.252

示例　图 11-1 展示了一个使用子网的例子。图中是一个本地的复杂网络，由 3 个局域网和 2 个路由器所组成。对于外部的因特网来说，这个网络就是一个简单的拥有 IP 形式为 192.228.17.x 的 C 类地址的网络，其中最左边的 3 个八位比特是网络号而右边的八位是主机号 x。路由器 R1 和 R2 都设置子网掩码为 255.255.255.224（见表 11-1a）。如果一个数据包无论是来自外部因特网还是局域网 Y 达到了 R1 并且其目的地址为 192.228.17.57，R1 使用子网掩码发现这个地址是子网 1 中的，也就是局域网 X，就将该数据包转发至局域网 X。同样的，如果一个数据包来自局域网 Z 到达了 R2，R2 使用子网掩码并根据其路由表决定该数据包的目的地是在子网 1 内，应该转发给 R1。各个主机都要配置子网掩码使得路由能正常工作。

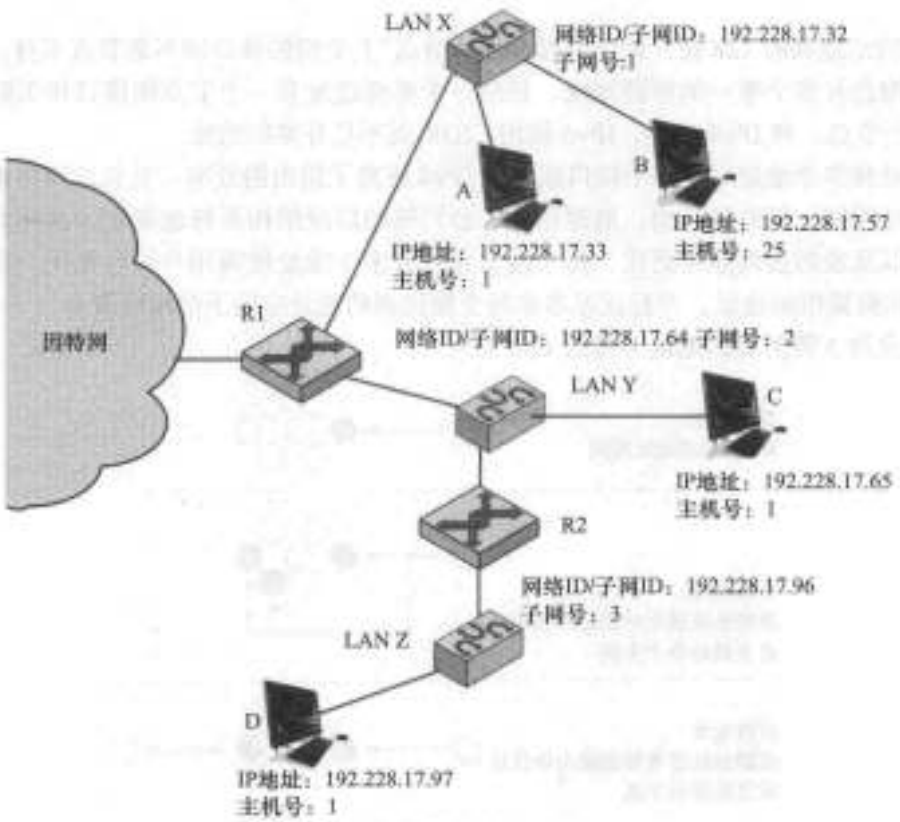


图 11-1　子网示例

默认的子网掩码对于一个给定类别的地址来说是个没用的掩码（见表 11-1b），因为它表示了与不使用子网相同的网络号和主机号。

3. 无分类域间路由选择（CIDR）

从 20 世纪 90 年代中期开始，因特网的设计者以及管理人员发现 32 位的分类的 IP 地址模式无法满足快速增长的对于 IP 地址的需求。一个长远的解决该问题的方案是使用 128 位的 IPv6 地址，这在第 8 章中提过。使用 128 位的地址几乎能够使得能使用的唯一的地址的数量增加为只有 32 位地址的 10^{29} 倍。

然而 IPv6 的部署需要许多年才能完成，因此 CIDR 作为一个过渡的方法被采用。由于更加有效地利用了地址空间，CIDR 较之分类的地址更加有效地利用了 32 位的地址。在使用分类的地址时，一个组织可以请求一块地址包含有 8、16 或者 24 个比特位所组成的主机地址。因为典型的因特网对于某个特定的类只以块为单位进行分配，所以造成很多地址被浪费。

CIDR 去除了以类进行分配的方式并利用前几个比特去识别一个类。作为替代，每个 32 位的地址由最高位的比特作为网络号部分以及由地位比特作为主机号部分，所有的 32 位比特都被用于寻址。每个 IP 地址都有一个和它相联系的前缀用于指明该地址网络部分的长度。一个采用 CIDR 的 IP 地址被写成 a.b.c.d/p 的形式，其中 a 是地址的第一个字节，b 是地址的二个字节，c 是地址的第三个字节，d 是地址的第四个字节，每个数字的值都在 0 ~ 255 之间。而前缀 p 的值在 1 到 32 之间，指明了该地址中网络部分的长度。

11.1.2　IPv6 地址

IPv6 的地址共有 128 位。地址是被分配给节点[⊖]上个别的接口而不是节点本身。一个单独的接口可能会有多个唯一的单播地址。任何一个单播地址和一个节点的接口相关联用于唯一地识别那个节点。和 IPv4 一样，IPv6 使用 CIDR 而不是分类的地址。

长地址和多个地址对应一个接口相比于 IPv4 提高了路由的效率。更长的网络地址使得地址能够通过网络、服务供应商、地理位置、公司等的层级结构更好地聚合。这种聚合使得路由表更小以及表的查询速度更快。每个接口允许有多个地址使得用户可以在同一接口使用多个服务提供商提供的地址，并且让原本在每个提供商的地址空间下的地址聚合。

IPv6 允许 3 种类型的地址（见图 11-2）：

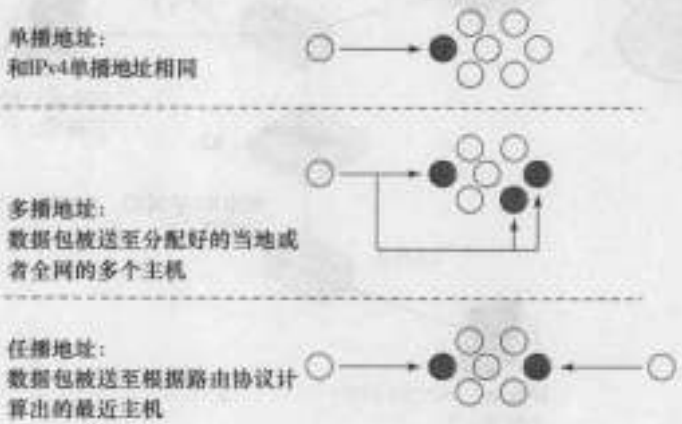


图 11-2　IPv6 地址

单播：一个单一接口的标识符。一个数据包发送至一个单播地址就是发送给那个地址所

⊖ 在 IPv6 中，结点指实现 IPv6 的任何设备，包括主机和路由。

标识的接口。

任播：一组接口的标识符（一般情况下属于不同的节点）。当一个数据包发送至一个多播地址时，它会被发送到那个地址所标识的一组接口中的一个（根据路由协议的距离度量方法选择一个最“近”的接口）。

多播：一组接口的标识符（一般情况下属于不同的节点）。当一个数据包发送至一多任播地址时，它会被发送到那个地址所标识的所有接口中。

IPv6 的地址使用冒号十六进制记法，使用 8 个十六进制数来表示 8 个由 16 位组成的块，共 128 位的地址，并且中间用冒号隔开，如：

FE80:0000:0000:0000:0001:0800:23E7:F5DB

为了使得记法更加紧凑，数字前面的 0 可以省略。前面那个例子中的地址可以表示为：

FE80:0:0:0:1:800:23E7:F5DB

为了再次压缩表示方法，一连串连续的 0 可以由一对冒号表示，上述地址可以变为：

FE80::1:800:23E7:F5DB

11.2　因特网路由协议

路由器在因特网中负责在相互连接的一组网络中接收和转发数据包。每个路由器所做的路由判定是基于自己所知的网络拓扑结构和流量、延迟情况的。在一个简单网络中，一个固定的路由策略是可行的，即为网络中每一对发送端和接收端都配置一条路由规则。这个路由是固定的，或最多仅在网络的拓扑结构发送变化时才改变。因此被用来设计路由的链路代价不能基于任何动态变量如流量。它们可以基于估计不同端与端之间的流量的大小或者每根链路的容量。

在更复杂的网络中，路由器之间一定程度上的动态合作是需要的。特别地，路由器必须能够避开网络中无法到达的部分并且能够回避网络中堵塞的部分。路由器之间通过特定的路由协议互相交换路由信息，以此来做出动态的路由判断，因此有关哪个网络能通过哪个路由器到达以及不同路线的延迟特性的信息是必需的。

考虑到路由功能，下面两个概念的区分是很重要的：

路由信息：有关网络拓扑结构以及延迟的信息。

路由算法：结合当前的路由信息对于某个特定的数据包做出路由判断。

11.2.1　自治系统

为了进一步讨论路由协议，我们首先引入自治系统（AS）的概念。一个 AS 有如下性质：

1）一个 AS 是由一个组织管理的一组路由器和网络。

2）一个 AS 由一组路由器组成，并且路由器之间通过一个公共的路由协议进行信息交换。

3）不考虑时间上的失败，一个 AS 从图论的角度看是连通的，即在每两个节点间都有一条路径连接。

在一个 AS 中的路由器间传递路由信息的共享的路由协议，我们称它为**内部网关协议**（IRP）。在一个 AS 中使用的协议不必在系统的外部也实现该协议，这种灵活度允许内部网关协议能够根据特定的应用和需求进行自主定制。

然而因特网可能由不只一个 AS 所组成，比如所有在一个站点的局域网，如一个办公室

或者校园，可能由路由器连接成为一个 AS。而这个系统可能通过广域网连接至其他 AS，见图 11-3 中所示。这种情况下，在不同 AS 中的路由器可能使用的是不同的路由算法以及路由表中是不同的路由信息。尽管如此，一个 AS 中的路由器需要有一个最基本的关于外部网络的信息，即外部网络是可达的。我们称在不同 AS 中的路由器互相传递信息的路由协议为**外部网关协议**（ERP）[⊖]。

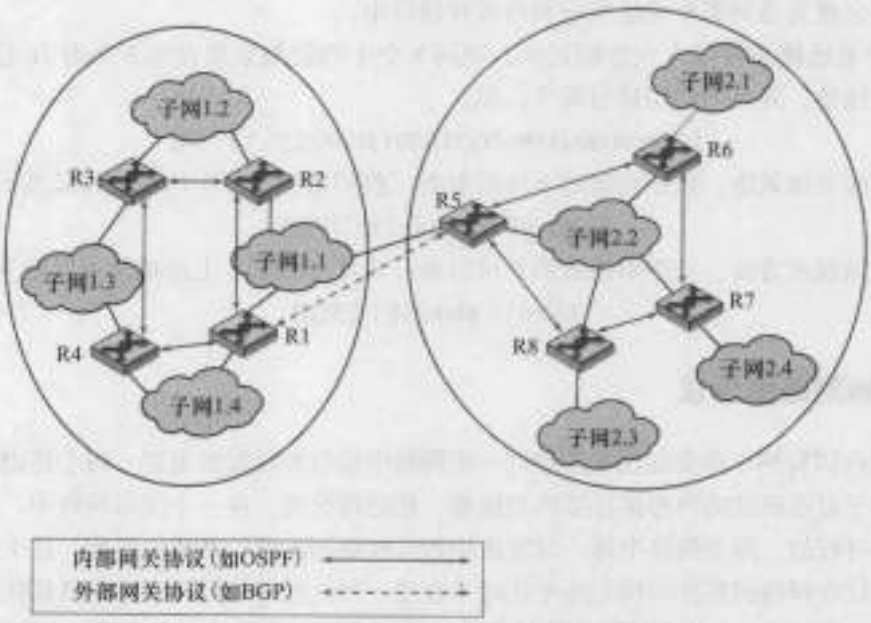


图 11-3　外部和内部网关协议的应用

一般来说，内部网关协议和外部网关协议在一定程度上有不同的特点。一个内部网关协议需要在一个 AS 中为路由器之间的连接建立一个相对详细的模型，并通过该模型计算出从某一路由器到 AS 中任意网络的最短花费路径。而外部网关协议支持在被分开管理的 AS 间进行概要的可达信息的交换。通常，这种概要信息说明外部网关协议要比内部网关协议简单，并且使用更少的详细信息。

在本节接下来的部分，我们来看可能是两类中最重要的协议：BGP 和 OSPF。

11.2.2　边界网关协议

边界网关协议（BGP）是为了能与部署了 TCP/IP 套件的因特网协同工作而发展起来的，即使这个概念已经被应用到了任何因特网上。BGP 已经成为了因特网上最受欢迎的外部网关协议。

BGP 被设计用来使得路由器（标准上称为网关）在不同的 AS 之间进行合作来交换路由信息。该协议的信息传送通过 TCP 来完成，目前最新的版本是 BGP-4。

BGP 中包含有 3 个功能过程：

- 邻站获得。
- 邻站可达性。
- 网络可达性。

⊖ 文献中，术语“内部网关协议”（IGP）和“外部网关协议”（EGP）经常被使用，为此，这里将它看作 IRP 和 ERP。然而，由于术语 IGP 和 EGP 也指具体协议，所以我们避开它们的具体使用定义通用的概念。

两个路由器被认为是邻站如果它们附属于同一个网络。如果两个路由器在不同的自治系统中，那么它们可能需要交换路由信息。为了达到这个目的，首先需要获得邻站。邻站指的是共享同一网络的两个路由器。大体上邻站的获得在两个相邻的但属于不同自治系统的路由器达成协议定期交换路由信息时发生。一个正式的获得过程是必需的，因为其中一个路由器可能并不想参与路由信息的交换。比如说，路由器已经负荷过重不想再为来自 AS 外部的网络流量负责。在邻站获得的过程中，一个路由器发送一个请求信息给另一个，对方可能同意或者拒绝该请求。该协议不解决关于一个路由器如何知道另一个路由器的地址甚至是否存在，也不解决它如何决定与某一特定路由器进行路由信息的交换。这些问题必须在配置时处理或者由网络管理员动态介入。

为了开始邻站获得，一个路由器首先向另一路由器发送一个打开（Open）报文。如果目标路由器接受这个请求，它就回复一个保活（Keepalive）报文。

一旦邻站关系建立了，邻站可达性过程被用来维持该关系。邻站关系的双方都需要确保对方依然存在并且在邻站关系中正常工作。为了这个目的，两个路由器需要周期性地互相发送保活报文。

BGP 协议中的最后一个过程是网络可达性。每个路由器维护一个网络情况的数据库，其中包含了各个网络是否可达以及各个网络的最优先路径。无论何时当该数据库中有变化时，这个路由器需要发送一个更新（Update）报文广播至所有与它拥有邻站关系的路由器。由于更新报文是广播的，因此所有的 BGP 路由器可以建立和维护它们的路由信息。

11.2.3　开放最短路径优先协议

开放最短路径优先协议（OSPF）在 TPC/IP 网络中被当作内部网关协议广泛使用。OSPF 使用的是链路状态算法。每个路由器维护了本地网络中链路状态的描述，并且时不时地传送更新后的状态信息至所有的路由器。每个路由器接收到一个更新的数据包后必须向发送端进行确认。这种更新信息所产生的流量是最少的路由流量，因为链路描述很小而且很少被发送。

OSPF 通过用户设置的代价度量方法计算因特网上代价最小的路径。用户可以设置一个代价的函数，变量可以有延迟、数据率、花费或者其他因素。OSPF 可以均衡多条代价相同路径上的负载。

每个路由器都维护了一个数据库，数据库中反映了它对于自治系统中已知的拓扑结构，该拓扑结构可以表示为一个有向图。图中包括以下几个部分：

- 顶点或者节点，有两种类型：
  - 路由器
  - 网络，有两种类型：
    - 传输网络：如果网络可以携带数据并且不会是一个系统的起始端或者终结端。
    - 末节网络：如果它不是传输网络。
- 边，两种类型：
  - 一个图的边连接了两个路由器节点，并且这两个路由器之间有一条直接连接的链路。
  - 一个图的边连接了一个路由器节点和一个网络节点，且路由器和网络之间是直接连接的。

图 11-4 展示了一个自治系统（只画了一个主机）。链路代价表示的是每个路由器中的接口与直接连接的路由器或者网络的代价。如果一个路由器连接了其他自治系统，则该条链路

的代价必须通过外部网关协议获得。

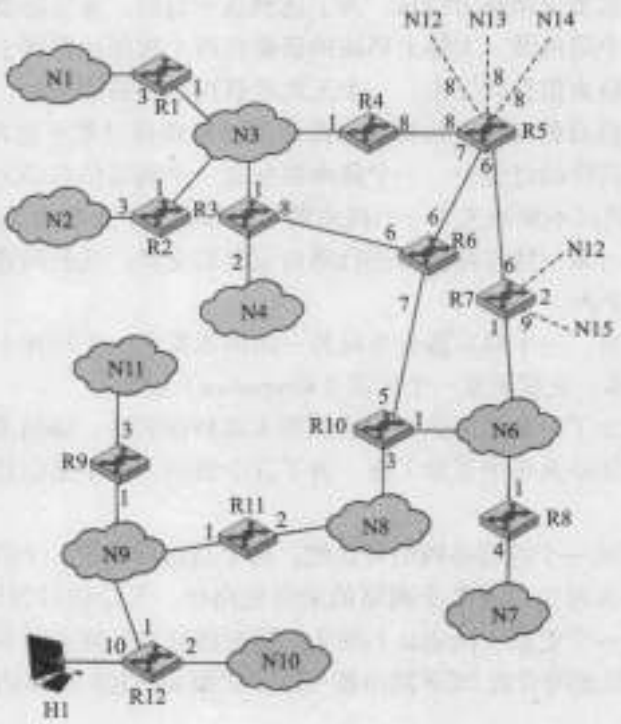


图 11-4　一个自治系统的例子

11.3　IP 多播

一般来说一个 IP 地址对应了一个具体网络上的单一主机。IP 同时也支持地址表示了一个或者多个网络上的一组主机。这种地址认为是多播地址，而通过多播地址从一个发送端发送一个数据包到该地址的一组主机的过程称为多播。

多播有很多实际应用，如：

多媒体：很多用户在一个多媒体的站点调至一个视频或者音频。

远程电信会议：一组工作站来形成一个多播组，这样任意一个成员发送的数据包都会被组中其他成员接收到。

数据库：一个复制文件的所有副本或者数据库同时进行更新。

分布式计算：中间计算结果被发送到所有参与者。

实时工作组：文件、图片和消息在一个活动组的成员中进行实时交换。

多播在一个单一的局域网中实现是直截了当的。IEEE 802 和其他局域网协议都包括了 MAC 层的多播地址。当一个多播的数据包在一个局域网上传播时，属于相关联的多播组中的成员识别出这个多播地址并且接收这个数据包。在这种情况下，只有一份数据包的副本在网络中传输。这种技术能够工作的原因是局域网本身的广播特性，即一个局域网中从一个主机发送的数据包会被局域网中其他所有用户接收到。

11.3.1　多播传送

在一个因特网环境中，多播的实现变得困难许多。为了说明这个，我们首先看图 11-5 中

的配置，图中是由路由器相互连接的许多局域网。路由器互相连接通过高速链路或者一个广域网（网络 N4）。每个路由器旁边的数字表示了数据在该链路或者网络上传输，并且是从该路由器离开所需要的代价。假设多播服务器在网络 N1 中，正在传送一个数据包，其中的多播地址代表了在网络 N3、N5、N6 中的主机。假设该服务器不知道多播组内成员的具体位置。那么一个确保数据包被所有成员接收到的方法就是复制每个包并且将其通过最小代价路径广播至设置好的所有网络中。比如有一个数据包的目的地址在 N3，那么它就会穿过 N1，链路 L3 到达 N3。路由器 B 负责在传送至 N3 前将其 IP 层的多播地址转换成 MAC 层的多播地址。表 11-2 总结了通过该方法传送一个数据包至一个多播组时每个链路和网络所产生的数据包数量。在表中，数据源是在图 11-5 中唯一 N1 中的多播服务器，多播组成员在 N3、N5、N6 中。表中的每一栏表示从数据源端至在一个目的网络中的目的路由器的路径。每一行指的是图 11-5 中的一个网络或者链路。表中的每一格是数据包在该网络或者链路上穿过的数量。如果使用广播技术的话一共需要有 13 份数据包的拷贝。

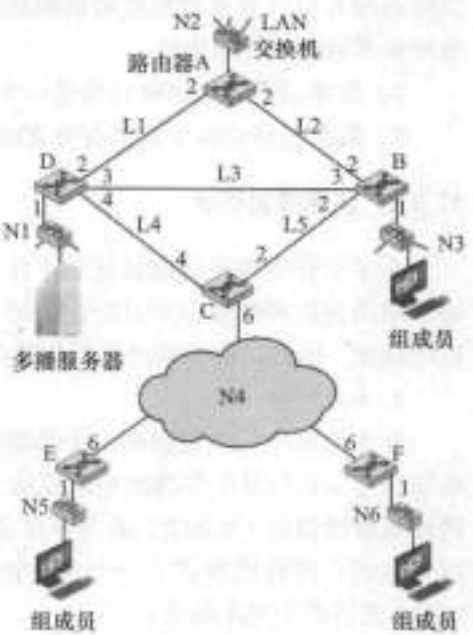


图 11-5　说明多播的实例配置

表 11-2　不同多播策略产生的流量

	广　播					多个单播				多播
	S->N1	S->N3	S->N5	S->N6	总计	S->N3	S->N5	S->N6	总计	
N1	1	1	1	1	4	1	1	1	3	1
N2										
N3		1			1	1			1	1
N4			1	1	2		1	1	2	2
N5			1		1		1		1	1
N6				1	1			1	1	1
L1	1				1					
L2										
L3		1			1	1			1	1
L4			1	1	2		1	1	2	1
L5										
总计	2	3	4	4	13	3	4	4	11	8

现在假设发送端系统知道每个多播组成员的位置，也就是说有一张将多播地址和多播组成员属于哪个网络关联起来的表。这种情况下，发送端只需要将数据包发送至这些包含有组员的网络中即可。我们把这称之为多单播策略。表 11-2 中展示了这种情况，总共需要 11 个数据包。

无论是广播还是多单播策略都是不够高效的，因为它们都产生了不需要的源数据包的副本，在实际的多播策略中，使用以下 3 个方法：

1）从发送端至多播组中成员的代价最小的路径是确定的，这就导致了生成树的设置。生成树是所有包含有多播组成员的网络集合，在网络之间添加足够的链路，建立一个从发送端至所有多播组成员的路径。

2）发送端沿着生成树只传送一个数据包。

3）数据包只会在生成树有分支时被路由器复制。

11.3.2　多播路由协议

为了能让多播机制能够正常工作，因特网上的路由器和发送多播数据包的发送端必须能够识别出包含有数据包中目的地址的主机的网络，并且能够决定出一条能够到达组中所有主机的路线。因此，许多地址发现和路由协议在因特网架构的不同层上面被使用。

1. 本地网络

在本地层中，主机需要一个参加和离开多播组的方法。主机需要能够告知本地网络的路由器它是否还是某个多播组中的成员。在一个广播的网络中，如以太网或者一个无线局域网，**网际组管理协议**（IGMP）被用来在主机和路由器之间交换多播组成员信息。IGMP 利用局域网本身的广播特性提供了一个高效的技术，在多个主机和路由器之间交换信息。总的来说，IGMP 支持两个基本操作：

1）主机向路由器发送加入一个多播组或者离开一个多播组的消息。

2）路由器周期性地检查哪些主机还是某个多播组的成员。

2. 内部网关协议

IGMP 使得一个路由器知道哪些主机在与自己连接的网络中正在使用一个特定的多播 IP 地址。接下来，路由器之间必须合作穿越一个组织的互联或者因特网成功路由并且发送多播 IP 数据包。路由器之间必须交换两种类型的信息。首先，路由器需要知道对于给定的多播组其成员在哪些网络中。其次，路由器需要足够的信息来计算至各个包含组成员网络的最短路径。这些需求说明了一个多播路由协议是必需的。

在一个 AS 中，有许多多播路由协议可供选择，我们在这里介绍其中的两种。**开放最短路径优先的多播扩展**（MOSPF）是为了能够交换多播路由信息而对 OSPF 的增强。每个路由器周期性的洪泛关于本网内组成员信息至 AS 中的其他路由器。这样做的结果就是 AS 中的所有路由器都能建立一张完整的所有多播组中所有成员信息的图。每个路由器都可以建立一个从一个源网络至所有包含该多播组成员网络的最短路径生成树。

协议无关多播（PIM）提供了一个比 MOSPF 更加通用的解决方案。如同该方式的名字，PIM 是一个独立的路由协议，独立于任何已有的单播路由协议。PIM 被设计从任一单播路由协议中提取到所需的路由信息，并且可能支持多个使用不同单播路由协议的 AS 之间的合作。

3. 外部网关协议

早期的许多多播网络关注于在一个单一的域中多播。在域内路由中，许多新的路由协议开始出现，但所有的都是实验性的。然而这个关于多播中与内部和外部路由协议都有关的问题还没有被成功解决。一个通用的有关多播路由和穿越因特网传送的解决方案还没有出现。

11.4　服务质量

因特网和其他因特网中的流量是持续增长和变化的。传统的基于数据的应用，如电子邮

件、新闻组网络新闻、文件传输和远程登录，由这些应用产生的需求足够对网络系统造成挑战。而最关键的因素是万维网的大量使用，由于它的实时响应需求和日益增长的音频、图片和视频在因特网上的使用。

这些因特网机制本质上都是路由器当作转发器的数据包转发技术。这些技术不是被设计用来处理声音与视频的，面对目前的需求非常有压力。

为了处理这些需求，仅仅增加因特网的容量是不够的。明智而有效的管理流量和控制拥堵的方法是必需的。历史上，基于 IP 的因特网曾经能够提供给使用因特网的所有应用一种简单的尽最大努力发送的服务。但是现在用户的需求变了。一个公司可能花费数以万计的金钱安装，因而，我们十分需要对有不同的 QoS（服务质量）需求的各类 TCP/IP 架构下的网络流量做出支持。

在这部分，我们对一些影响到 QoS 的终端用户方面的因素进行了研究。首先，我们从商用环境下对高速 LAN（局域网）的需求着手，因为这类需求是最先诞生的并且迫使了网络的发展。接下来，我们考察了商用 WAN（广域网）的需求。最后，我们将 QoS 的需求与因特网联系了起来。

11.4.1　高速 LAN 的出现

传统上，办公室局域网提供了基本的连接服务——将个人电脑和终端与那些运行企业级应用和提供部门 / 科级工作组连接服务的中型系统和大型机连接起来。在这两种情况中，网络数据传输负担相对较轻，主要在于文件传输与电子邮件这两方面。那些能够处理这类工作负担的局域网，主要是以太网和令牌环网，对这样的环境适应良好。

近几年，两项重大的趋势改变了个人计算机的角色以及局域网上的需求：

1）个人计算机的运行速度和计算能力持续地剧烈增长。这些更加强大的平台支持图形密集型应用以及更加细腻的操作系统用户图形化界面。

2）IT（信息技术）组织已经认可了局域网是一种可行的且必需的计算平台，这导致了专注于网络计算的研发。这一趋势从客户 / 服务器计算开始，在商用环境及近期的着重于 Web 的内部网中，已经成为了一种主导的架构。这两种方法在面向事务处理的环境中，都需要频繁传送潜在的大量数据。

这些趋势导致了局域网需要处理的数据量的攀升。因为计算机应用的交互性变得更强了之后，人们对数据传输延迟的接受能力有所下降，早期的 10 兆以太网和 16 兆令牌环网已经无法简单地负担这些需求了。

11.4.2　企业广域网的需求

在 20 世纪 90 年代初期，许多组织都主要使用一种中央数据处理模型。在一个典型的场景中，一些地区办公室内可能会有大量的由大型机或配置优良的中型系统组成的计算设备。这些中央设备能够处理大多数的企业级应用，包括基本的财务处理、会计、个人程序以及许多业务特有的应用。在面向事务处理的环境中，会为稍小一些的、边远的办公室（如银行分行）配备上可以连接到地区中心的终端或者基本的个人计算机。

这一模式从 20 世纪 90 年代早期开始发生变化，并在整个 20 世纪 90 年代的中期加速变化。许多组织将他们的员工分散到多个较小的办公室中。于是远程通信的频率增加了。最重要的是，应用结构的性质改变了。首先，客户 / 服务器计算以及之后的内部网计算，已经从

根本上重构了组织的数据处理环境。现在我们对个人计算机、工作站和服务器的依赖性变强了，与此同时，使用中央大型机和中型系统的时候则变少了。而且，几乎普及全球的桌面用户图形化界面使得终端用户能够开发图形应用、多媒体以及其他数据密集型应用。除此之外，基本上所有的组织都能够访问到因特网。由于用鼠标点击几下就能产生巨量的数据流动，网络数据流量变得更加难以预测，同时平均负荷也上升了。

所有这些趋势都意味着会有更多的数据必须离开本地并通过广域网进行传输。我们过去认为，在典型的商用环境中，大约 80% 的网络流量是来自于本地的，而约 20% 的数据则是通过广域网传输的。然而这一规律对于大多数企业而言已经被打破了，通过广域网传输的数据比重大幅上升。这一网络数据流的转移加重了局域网骨干以及企业广域网设备的负担。因此，单就局域网而言，企业流量的改变推动了高速广域网的诞生。

11.4.3　因特网流量

在网络或者因特网上的数据流量能被宽泛地划分成两大类：有弹性的及无弹性的。考虑到两者的不同要求后，明确了对增强型因特网架构的需求。

有弹性的数据流能够在很大程度上适应因特网上数据延迟和吞吐量的变化，并且仍然满足其应用需求。这就是传统上的以 TCP/IP 为基础的因特网所支持的网络流量，且因特网也是为这类数据流量而设计的。在 TCP 协议中，单个连接的数据流量靠降低数据提交给网络的速率来避免拥塞。

有弹性的应用包括普通的因特网应用，如文件传输、电子邮件、远程登录、网络管理以及 Web 访问。但是这些应用之间的需求存在着差异，例如：

- 电子邮件一般对延迟上的变化不敏感。
- 当文件传输是（它也往往都是）交互式地进行时，用户希望数据传输的延迟是与文件大小成比例的，因此文件传输对吞吐量上的变化是敏感的。
- 对网络管理而言，延迟一般不是我们着重考虑的问题。然而，如果因特网中的传输失败是由数据拥塞引起的，那么对于在尽可能小的延迟内传递网络管理消息的需求随着拥塞的增加而提升。
- 交互式应用，如远程登录和 Web 访问，都对延迟敏感。

所以，即使我们将注意力局限于弹性数据流，一个基于 QoS 的因特网服务也是能够获益的。若是没有这类服务，路由器就会不论应用的类型以及这些分组是来自于一个大型的还是小型的传输，都公正地处理到达的 IP 分组。在这种情况下，如果拥塞继续恶化，资源是不可能在满足所有应用需求的条件下被公正分配的。当无弹性数据流加入之后，事情就变得更加不令人满意了。

无弹性数据数据流无法轻易地，或者说根本无法，适应因特网上的数据延迟和吞吐量的变化。最典型的例子就是实时数据传输，如声音与视频流。无弹性数据流的需求可能包括以下几点：

- **吞吐量**：我们可能需要一个最低的吞吐量值。不像大多的弹性数据流，它们能够在可能降低服务质量的情况下持续传输数据，许多的非弹性应用需要规定一个最低吞吐量值。
- **延迟**：一个对延迟敏感的应用的例子是股票交易系统，那些持续获得滞后服务的用户也将持续行动滞后，这会带来巨大的劣势。

- **抖动**：延迟变化的幅度，称为“抖动”，它在实时应用中是一个重要的参数。由于因特网带来的延迟变化，两次分组抵达目的地的时间间隔并不是维持在一个恒定的值。为了补偿这一点，传来的分组被缓存了起来，等到能足够弥补抖动后，数据才被以一个恒定的速率释放给希望获得固定实时流的软件程序。允许的延迟变化越大，数据传输时的实际延迟就越长，接收端需要的延迟缓存也越大。实时交互型应用，如远程会议，可能需要一个合理的抖动上限。
- **丢包率**：实时应用的丢包率在其可以承受的范围内不断地变化。

这些需求在排队延迟浮动和拥塞数据丢失的环境下是很难被满足的。从而，无弹性的数据流为因特网架构引入了两个新的要求。首先，我们需要一些手段来为那些有苛刻需求的应用提供优惠的待遇。应用程序要能够表明它们的需求，要么提前在一些服务请求函数中说明，要么运行时在 IP 包头的某些域里说明。

第二个要求是在支持无弹性数据流的因特网架构中仍能同时支持弹性数据流。相比基于 TCP 的应用，无弹性应用往往不会在拥塞的状况下撤回和削减需求。因此，除非使用一些调控机制，否则在拥塞的时候，无弹性数据流将会继续产生高负荷数据传输，而弹性数据流则将被挤出因特网。

能在因特网上提供 QoS 服务的几项技术现已被提出。其中最为广泛采纳的一项技术即为差异化服务。接下来我们将探讨这个话题。

11.5　差异化服务

随着因特网负担的不断增长与应用种类的不断增多，我们急需为不同的用户提供不同级别的 QoS。差异化服务（Differentiated Services，DS）架构被设计为一种能提供简单的、易于实现的、低开销的工具以支持一系列不同性能的网络服务。本质上，**差异化服务**不是根据流量，而是根据不同用户组的需求来提供 QoS。这就意味着因特网上所有的数据流量都会被按照不同的 QoS 需求划分在不同的组别中，然后路由器根据 IP 包头中的标签识别不同的组别。

差异化服务的几项重要特性使之变得高效且易于部署：

- IP 分组通过在 IPv4 和 IPv6 的包头中使用 6 位的 DS 域（见图 8-7）来标记不同的 QoS 待遇。不需要对 IP 协议做改变。
- 我们在服务提供方（因特网域）与客户之间设立了一个服务等级协议（Service-Level Agreement，SLA），它优先于差异化服务的使用。这避免了将差异化服务技术并入到应用中去。从而，我们不需要对现有的应用进行改动就可以使用差异化服务。
- 差异化服务提供了一种内置的聚合技术。所有有着相同 DS 字段的数据流将获得相同的网络服务待遇。比如，多种语音连接是共同聚合处理的而不会被单独处理。这为更大型的网络和数据流量负荷提供了良好的可扩展性。
- 差异化服务通过在单个路由器中排队和转发包含 DS 字段的分组来实现。路由器单独地处理每个分组，并且不需要在分组流中保存状态信息。

如今，差异化服务是在企业网中最为广泛认可的一种 QoS 技术。

11.5.1　服务

差异化服务的类型在 DS 域内表明，它在因特网中被定义为连续的一个部分，并且由因

特网管理这一组连续的差异化服务策略。通常，一个 DS 域由一个管理实体管理。DS 域提供的服务在服务等级协议中定义，服务等级协议是一项客户和服务提供方之间的服务合约，合约中写明了客户的不同组别的分组应获得的转发服务。客户可以是一个用户组织或者另一个 DS 域。一旦服务等级协议成立了，客户提交带有 DS 字段标记的分组来表明该分组的组别。服务提供方必须确保客户能够获得最基本的约定中对应分组级别的 QoS 服务。为了提供这种 QoS，服务提供方必须在每个路由器上配置好合适的转发策略（根据 DS 字段的值），并且必须根据一个不断完善的标准，监测提供给各个组别的服务表现状况。

如果客户递交了目的地位于 DS 域之内的分组，那么我们希望 DS 域能够提供约定好的服务。如果目的地超出了客户的 DS 域，那么 DS 域将会尝试将该分组通过其他域转发，并要求与被请求的服务类型最为接近的服务。

一份差异化服务架构文件列出了如下的性能参数细节，这些也可能被包含在一个服务等级协议中：

- 服务性能参数，如期望的吞吐量、丢包率和延迟。
- 在服务提供的入口点和出口点加以限制，明确服务的范围。
- 被请求提供的服务必须要遵守的数据流量配置。
- 当超过既定范围时需要提供的数据流量部署。

架构文件同时还给出了一些可能提供的服务的例子：

1）来自服务等级 A 的数据流量将以低延迟转发。

2）来自服务等级 B 的数据流量将以低丢包率转发。

3）90% 的数据流量配置范围内的、以服务等级 C 转发的分组不会经历超过 50ms 的延迟。

4）95% 的数据流量配置范围内的、以服务等级 D 转发的分组将会被转发。

5）来自服务等级 E 的数据流量将被以两倍于来自服务等级 F 数据流量的带宽转发。

6）比起丢弃优先级为 Y 的分组数据，丢弃优先级为 X 的更可能被转发。

11.5.2　DS 域

IP 数据包通过在 IPv4 和 IPv6 的包头中使用 6 位的 DS 域（见图 8-7）来标记不同的服务处理方式。DS 域的值，称为 DS 码点，被用作区分不同组别的分组差异化服务的标志。

6 位的码点理论上可以定义 64 种不同的流量组别。这 64 种码点被分成了如下三大类：

- 格式为 xxxxx0 的码点，其中 x 可以为 0 或 1，被保留为标准分配。
- 格式为 xxxx11 的码点，被保留为实验或本地使用。
- 格式为 xxxx01 的码点，也被保留为实验或本地使用，但可能会在需要时，被分配到未来的标准行为中。

在第一大类中，码点 000000 是默认的分组组别。这一默认组别在现有的路由器中将被以最大的努力转发。这类分组只要在链路状况允许的情况下，就会按照它们被接收时的顺序被转发。如果其他的来自另外的 DS 域中具有更高优先级的分组在等待被转发，它们的优先级将优先于默认的最大努力转发分组。

码点的设定中明确了数据报的紧急度或优先级。如果一个路由器支持差异化服务，它有三种方式进行响应：

- **路由选择**：一条特定的路由可能会被选中，当路由器中该路由上的队列较短或者该路

由的下一跳具有网络优先权时（例如，一个令牌环网享有优先权）。

- **网络服务**：如果下一跳的网络享有优先权，那么那个网络的服务将被调用。
- **排队规则**：一个路由器可能会使用优先级策略来影响它如何处理队列。比如，一个路由器可能会给予队列中具有更高优先级的数据报以优惠待遇。

11.5.3　差异化服务的配置与运行

图 11-6 表明了差异化服务文件中设想的配置方式。一个 DS 域由一组邻近的路由器组成，这意味着，我们从域中的任一路由器开始，都能找到一条不包含域外部路由器的路径，到达域中其他的路由器。在域内，DS 码点的语义是统一的，从而能够提供一套统一且连贯的服务。

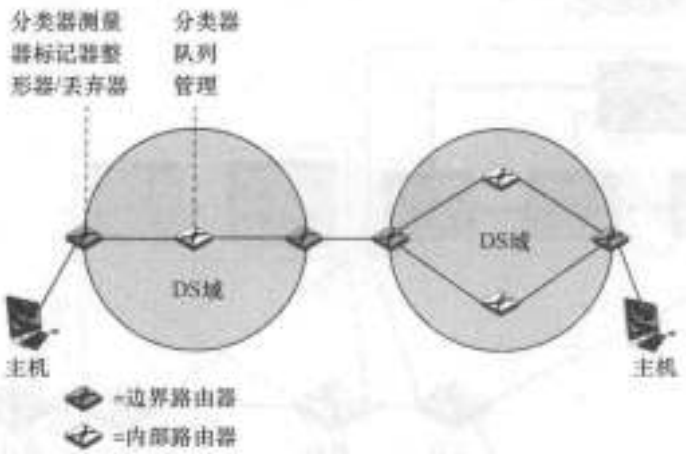


图 11-6　DS 域

DS 域中的路由器要么是边界节点，要么是内部节点。通常，内部节点根据分组的 DS 码点使用简单的技术来处理它们。这其中包含了一种排队规则——根据码点给予分组优惠待遇，以及一种丢包规则——决定当缓冲饱和时哪类分组会被优先丢弃。在差异化服务规范中把单个路由器中的转发行为叫做逐跳行为（Per Hop Behavior，PHB）。这种逐跳行为必须在所有的路由器上都是有效的，并且逐跳行为往往是差异化服务实施在内部路由器上仅有的部分。

边界节点不仅包含 PHB 逐跳技术，还包含了更复杂的数据流量调控技术以到达提供期望的服务的目的。因此，内部路由器在提供差异化服务上的功能和开销都被最小化了，而大部分的复杂性都存在于边界节点上。边界节点的功能也能由一个附加在域上的主机系统中的应用程序提供。

数据流量调控功能由五种组件组成：

- **分类器**：将递交上来的分组分成不同的组别，这是提供差异化服务的基础。一个分类器可能只是根据 DS 码点来分组（行为聚合分类器）；或者根据数据包头中的多个域，甚至是分组的负载（多域分类器）。
- **测量器**：根据配置文件的内容测量提交上来的数据流量，测量器将判定一个特定的分组流组别是否超出了保证分配给该组别的服务等级范围。
- **标记器**：在需要时使用一个不同的码点重标记分组。这可能在分组超出配置规定时实施。例如，如果一部分特定的吞吐量被承诺分配给了某一特定的服务组别，当任何属于该组别的分组超出了给定吞吐量的规定范围时，我们可能在某些指定的时间间隔将

这类分组重标记成尽最大努力转发分组。此外，在两个 DS 域的交界处也可能会使用到重标记。例如，如果我们想要指定一个特定的流量组别获得最高的优先级，但是这个代表最高优先级的码点值在一个域里是 3，而在另一个域里是 7，那么当码点值为 3 的分组穿过前一个域，进入后一个域时，将会被重标记成 7。

- **整形器**：在必要时推迟分组的传输，从而特定组别的分组流在数据流量中所占的比例不会超出在配置中规定的份额。
- **丢弃器**：当一特定组别的分组比例超过了在配置中规定的份额时，将该分组丢弃。

图 11-7 阐明了数据流量调控组件间的关系。当某条数据流被分类之后，我们必须测量它造成的资源损耗。测量器组件测量在一段特定的时间间隔内的分组量，从而判定这条数据流是否遵守了流量协议的规定。

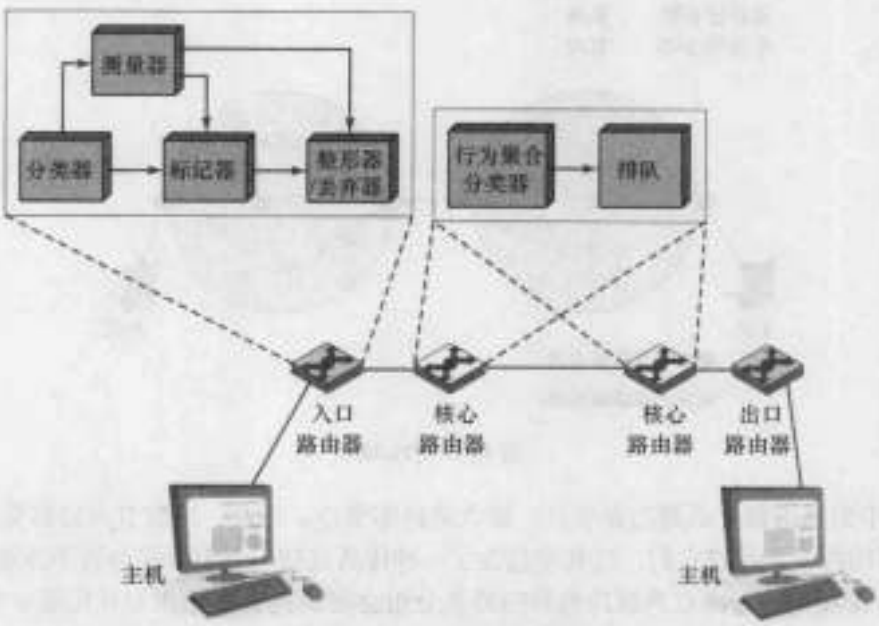


图 11-7　差异化服务功能结构

如果一条数据流超出了某些配置参数的规定，有几种措施可以采取。单个的超出规定的分组可被重标记成更低质量处理分组，然后被允许进入 DS 域。流量整形器可能会一下子从缓冲中吸收到一大堆分组，然后花上一长段时间来调整这些包的传输节奏。丢弃器可能会在用来调整传输节奏的缓冲饱和时丢弃分组。

11.6　服务等级协议

服务等级协议（SLA）是网络提供方与客户间的一项合约，协议中规定了所要提供的服务明细。这些规定是正式的，且往往还定义了必须要遵守的数值界限。一份服务等级协议常常包含以下信息：

- **描述所要提供服务的性质**：一项基本的服务是提供企业内部的基于 IP 协议的网络互联以及到因特网的访问。这项服务中可能包含了附加的功能，如虚拟主机、域名服务器的维护以及运行和维护方面的任务。
- **服务所期望达到的性能等级**：服务等级协议使用具体的数值界限规定了一系列的参数

标准，如延迟、可靠性以及可用性。

- **监测与报告服务等级的方式**：这一部分内容描述了如何测量与报告性能等级。

图 11-8 展示了一种典型的配置，这种配置将自身出借给 SLA。在这个案例中，网络服务提供方维护了一个基于 IP 协议的网络。客户在不同的站点拥有许多个私有网络（如局域网），客户网络在接入点通过接入路由器连接到提供方的网络。服务等级协议为提供方网络内的接入路由器间的数据流量规定了服务与行为的等级。此外，提供方的网络与因特网相连，并以此为企业客户提供到因特网的访问。举一个例子，由一个主要载体提供的因特网专用服务，服务等级协议包含了如下的项目：

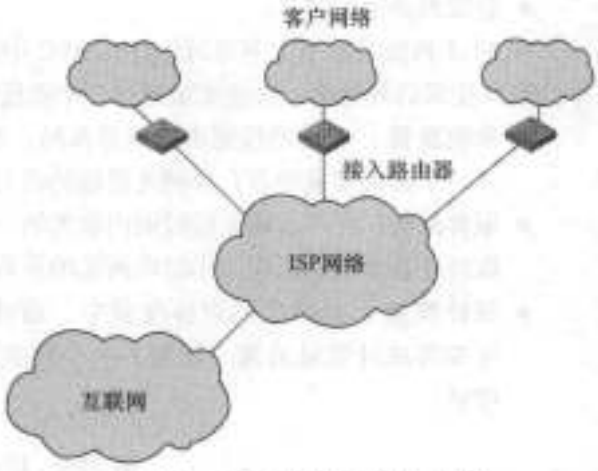


图 11-8　典型的服务等级协议架构

- **可用性**：100% 的可用性。
- **延迟**：在美国内的接入路由器之间的平均往返传输时间 ≤ 45ms。在一个纽约市区的接入路由器和一个伦敦市区的接入路由器之间的平均往返传输时间 ≤ 90ms。延迟是由路由器间一个月的样本测量均值计算得出的。
- **网络分组转发（可靠性）**：成功转发的分组率 ≥ 99.5%。
- **拒绝服务（DoS）**：自客户开出一张完整的故障报告表起，在 15min 内响应客户报告的拒绝服务攻击。MCI 将拒绝服务攻击定义为超过 95% 的带宽使用率。
- **网络抖动**：抖动被定义为接收到的 IP 数据包或数据包流之间的端到端延迟的变化或者差异。接入路由器间的抖动表现不会超过 1ms。

服务等级协议能定义所有的网络服务。除此之外，网络等级协议还能定义载体网络上特定可用的端到端服务，比如，一个虚拟的私有网络，或者差异化服务。

11.7　IP 性能度量

IP 性能度量工作组（IP Performance Metrics Working Group, IPPM）是 IETF 特别成立的专门制定与因特网数据转发的质量、性能和可靠性相关的度量标准的工作组。两项趋势决定了我们需要这样一个标准度量方案：

1）因特网正在成长并且以一个戏剧化的速度持续成长。它的拓扑结构正变得越来越复杂。随着它的容量增长，因特网上的负荷也以一个更快的速率增长。与此同时，私有网络，如企业内网和外网，在复杂度、容量与负荷这些方面也表现出了相似的增长。这些网络的飞速增长使我们很难去判定其质量、性能和可靠性这些性质。

2）因特网通过越来越多不同的应用为一大群不断增加的商业和个人用户提供服务。相似的，私有网络在用户基数和应用种类范围这两方面也都在增长。其中一些应用对某些特定的 QoS 参数敏感，使得用户需要精确和易懂的性能度量。

一套标准化且有效的度量方案能使用户和服务提供方对因特网和私有内部网的性能有一个精确且普遍的认识。测量数据在多种情况下都是有用的，包括：

- 为大型复杂的内部网提供容量规划与故障修理的支持。
- 通过在服务提供方之间给出统一的比较度量来鼓励竞争。
- 在诸如协议设计、拥塞管理和服务质量等领域支持因特网研究。
- 验证服务等级协议。

表 11-3 列出了在本文书写时已经在 RFC 中定义了的度量。表 11-3a 列出的度量由一项简单的取样技术估算得出。这些度量通过三个阶段被定义：

- **单例度量**：特定的性能度量最基本的，或者说最原子化的，可测量的数量。比如，对于一个延迟度量而言，单例度量指的就是分组单次传输中经历的延迟。
- **取样度量**：在一段特定的时间内取得的一组单例度量。比如，对于一个延迟度量而言，取样度量指的就是在一小时内测得的所有传输延迟的值的集合。
- **统计度量**：从特定的取样度量中，通过计算一些由样本定义的单例度量的统计值，来获得统计度量的值。比如，一个样本的所有单程延迟的均值可能会被定义为统计度量。

表 11-3　IP 性能度量

a）取样度量

度量名	单例定义	统计定义
单程延迟	延迟 =dT，其中发送端在 T 时刻发送分组的第一个位，接收端在 T+dT 时刻收到分组的最后一个位	百分数、中位数、最小值、逆百分数
双程延迟	延迟 =dT，其中发送端在 T 时刻发送分组的第一个位，发送端在 T+dT 时刻收到接收端及时转发回来的分组的最后一个位	百分数、中位数、最小值、逆百分数
单程遗失	分组遗失 =0（表示成功地传送并接收到分组）；=1（表示分组被遗失）	平均值
单程遗失图形	遗失距离：展现了一系列连续的分组中分组遗失间隔长度的图形 遗失周期：展现了突发遗失数量的图形（包括连续的分组遗失）	在限定范围内的遗失距离的数量或比率，遗失周期的数量，遗失周期长度图形，内部遗失周期长度图形
分组延迟变化	分组流中的一对分组的分组延迟变化（pdv）= 指定分组单程延迟间的差异	百分数、逆百分数、抖动、峰间 pdv

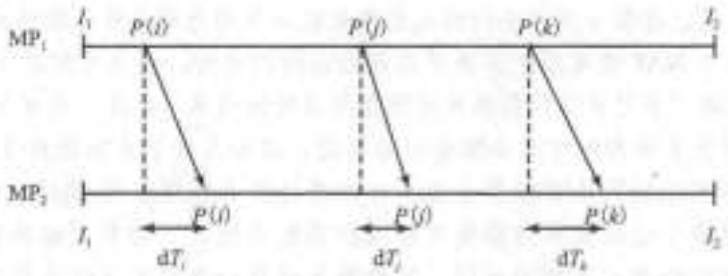
b）其他度量

度量名	一般定义	度　量
连通性	在一条连接中转发分组的能力	单程瞬时连通性、双程瞬时连通性、单程间隔连通性、双程间隔连通性、双程临时连通性
批量传输能力	在单次发现拥塞的传输连接中的长期的平均数据率（bps）	BTC= 发送的数据 / 经历的时间

测量技术可以是主动的，也可以是被动的。**主动的**技术需要将仅用于测量目的的分组注入网络中。这种方法有几个缺点。它加重了网络的负荷，这会反过来影响我们需要的测量结果。例如，在一个高负荷的网络中，注入测量分组会加重网络延迟，从而测得的延迟将大于它原本没有这些测量数据流量时的情况。此外，主动测量策略能让拒绝服务攻击通过伪装成正当的测量活动而被滥用。**被动的**技术从现有的数据流量中观察和提取度量值。这种方法会把因特网流量的内容曝光给非计划中的接收者，导致安全和隐私问题。迄今为止，IPPM 工作

组定义的度量都是主动的。

图 11-9 诠释了分组延迟变化的度量。这一度量在分组在网络中传播的延迟中测量抖动，或者可变性。单例度量由选取两个分组并测量两者延迟间的差异来定义。统计度量利用延迟的绝对值测得。



I_1, I_2 = 标记了进行单例测量的分组流的起止时间区间
MP_1, MP_2 = 进行测量的源点与目的地
$P(i)$ = 分组流中第 i 个被测量的分组
$dT_i = P(i)$ 的单程延迟

图 11-9　分组延迟变化定义模型

表 11-3b 列出了两项不是通过统计量定义的度量。连通性度量反映了传输层的连接是否由该网络维持的问题。当前的规格文档（RFC 2678）不给出各项取样度量和统计度量的明细，而是给出了一个框架，度量能够在这个框架内被定义。连通性由一段限定的时间内，一条连接中转发分组的能力决定。其他的度量，批量传输能力也是类似地（RFC 3148）不通过取样度量和统计度量给出，而是使用多种拥塞调控技术来解决测量网络服务传输能力的问题。

应用注解

我的网络地址来自于哪里？

所有与因特网相连的计算机必须被分配一个网络地址，这个地址称为 IP（一种因特网协议）地址。如果你的网络连入了因特网，那么每个节点必须至少拥有一个在公共网络上有效的可用地址。这个地址通常是由因特网服务提供商或 ISP 分配的。为内部网络和网络节点分配地址的方法常常基于有多少电脑会拥有全球独一无二的因特网地址。

全球唯一的地址在公共的因特网空间中只能被一台电脑所使用，所有连接到因特网的通信接口都拥有一个全球唯一的地址。这些电脑或者接口有时候被称为“可见的”机器，可见指的是这些电脑是直接连接到公共的因特网上的，可见同时也意味着这些机器更容易受到黑客的攻击——这确实属实。

一个组织可能会决定让它内部所有的机器都使用全球唯一的地址并成为可见的。在这种情况下，ISP 必须分配许多地址给这个组织，可以分配出一个全类地址或分类地址。因特网地址空间由 A 类、B 类和 C 类组成，A 类网络范围很大，C 类的则稍小。ISP 通常控制着地址空间的大型分支，并将它们分配给自己的客户。例如，一家拥有 200 个节点的公司可能需要分配到一个 C 类的网络地址。

大型的 ISP 可能控制着数百万个 IP 地址。通过使用子网掩码，可将这些地址空间中的一小部分分配给他们的客户。子网掩码决定了主机是什么网络和该网络的大小。例如，一

家 ISP 公司时代华纳，它可能控制着一个 A 类网络内的部分地址空间，这些地址中的一小部分能被分配给一家独立的公司，分配完之后，我们往往还能看到该 ISP 公司继续为这家独立的公司处理一系列的相关事务，如 DNS、域名注册、安全维护和邮件。

另一个选择是拥有少量的 ISP 分配的全球唯一地址，然后使用这些地址作为公司防火墙的外部连接。可以将部分或者全部的电脑隐藏在一个运行网络地址翻译或 NAT 的路由器之后，使用到这个 NAT 的电脑都将使用相同的因特网地址，使得它们被有效地隐藏起来。这并不意味着这些“不可见”的机器被困在与因特网的通信之外，或者免于被攻击。

然而，这引出了为内部节点分配地址的问题。这些内部节点的地址并不是来自于 ISP 的，所以必须由本地的网络管理员分配，可以通过静态配置或者 DHCP 的方式分配内部地址。我们必须要小心避免在内部使用标准的因特网地址。如果内部的机器被分配到了一个与外部的可见机器相同的地址时，因特网上的路由器将无法把分组路由回公司内部的那台机器。

由于这个原因，我们设立了私有的 IP 地址。如下的地址段被保留下来，以供想要用上述方法部署自己网络的公司使用：

10.0.0.0 ~ 10.255.255.255

172.16.0.0 ~ 172.31.255.255

192.168.0.0 ~ 192.168.255.255

RFC 1918 中描述了私有地址的细节。除了有利于保障内部机器的安全性，这一方案还帮助缓解了因特网用户数量急增的问题。随着用户数量的急剧增长，全球唯一的 IPv4 地址的数量已经不够让每个人都拥有自己唯一的公共地址。

上面提出的每个方法都有它们各自的优缺点。私有地址分配往往需要投入更多的管理，但它确实保证了更高的安全性，并降低了公用地址空间的使用量。全部使用公共地址的确更易于管理，并潜在地简化了连通性问题。然而，它使得这一组织需要依赖于 ISP 帮它解决一大堆包含安全性等的问题。

11.8　总结

因特网中十分重要的一部分就是其地址分配方案。每个与因特网相连的主机都必须拥有一个独一无二的地址，使得分组能被路由和转发至该主机。因特网标准定义了一个 32 位的地址方案来达到这一目的。

因特网路由协议用于交换关于可达性和传输延迟的信息，允许每个路由器都为因特网中的路径建立一个下一跳的路由表。通常，相对较简单的路由协议被用于一个大型网络的两个自治系统之间，而更复杂的路由协议则在各自治系统内部使用。

不断增长的应用数据率（容量）需求刺激了数据网络和因特网数据传播向更高速的方向发展。更高的可用容量也反过来刺激了更加数据密集型应用的发展。为了处理因特网上不断变化的需求，我们引入了服务质量的概念。一个 QoS 设备使得因特网能以不同的方式对待不同类型的网络数据流量，以此为所有的客户优化服务的质量。

差异化服务架构被设计为一种能提供简单的、易于实现的、低开销的工具以支持一系列不同性能的网络服务。我们以 IP 包头中的 6 位标志为基础提供差异化服务，这个标志将网络

数据流量按照路由器提供给这类流量的服务种类进行分类。

11.9　关键术语、复习题和练习题

关键术语

anycast（任播）
Autonomous System（AS，自治系统）
availability（可用性）
best effort（尽最大努力）
Border Gateway Protocol（BGP，边界网关协议）
broadcast（广播）
Classless Inter-Domain Routing（CIDR，无类型域间选路）
delay（延迟）
denial of service（拒绝服务）
differentiated services（差异化服务）
dotted decimal notation（点分十进制记法）
elastic traffic（弹性流量）
exterior routing protocol（外部路由协议）
inelastic traffic（无弹性流量）
interior routing protocol（内部路由协议）
Internet Group Manageme Protocol（IGMP，因特网组管理协议）
jitter（抖动）
latency（时延）
multicast（多播）
Multicast Extensions toOSPF（MOSPF，组播扩展 OSPF）
neighbor（邻居）
neighbor acquisition（相邻的路由器）
neighbor teachability（相邻路由器可达）
network reachability（网络可达）
Open Shortest Path First（OSPF，开放式最短路径优先）
packet loss（丢包）
Protocol IndependentMulticast（PIM，协议独立多播）
quality of service（QoS，服务质量）
routing（路由）
routing algorithm（路由算法）
routing protocol（路由协议）
Service Level Agreement（SLA，服务等级协议）
subnet（子网）
subnet mask（子网掩码）
supernetting（超网）
throughput（吞吐量）
unicast（单播）

复习题

11.1　描述因特网地址的 5 个类别。
11.2　什么是子网？
11.3　使用子网掩码的目的是什么？
11.4　什么是自治系统？
11.5　内部路由协议和外部路由协议的区别是什么？
11.6　列出并简要说明 BGP 的 3 个主要功能。
11.7　OSPF 使用了哪种路由算法？
11.8　OSPF 被设计成了什么类型的路由协议？
11.9　给出服务质量（QoS）的定义。
11.10　解释弹性数据流和非弹性数据流的区别。
11.11　非弹性数据流中的四项潜在的需求指标是什么？

11.12　DS 码点有什么作用?

11.13　列出并简单解释 DS 数据流量调控中的 5 个主要组件。

练习题

11.1　请按如下要求分别给出 A、B、C 类网络对应的参数值，并确保在计算中考虑到任何特殊或保留的地址：

a. 网络地址部分有多少二进制位

b. 主机地址部分有多少二进制位

c. 允许有多少个不同的网络

d. 每个网络允许有多少个不同的主机

e. 第一个八位二进制的整数范围

11.2　A、B、C 类网络各占总 IP 地址空间的百分之多少?

11.3　子网 ID 为 16 位的 A 类地址和子网 ID 为 8 位的 B 类地址的子网掩码有什么区别?

11.4　255.255.0.255 是一个有效的 A 类地址子网掩码吗?

11.5　假设有一个网络地址为 192.168.100.0，且其子网掩码为 255.255.255.192，问：

a. 它有多少个子网?

b. 每个子网有多少个主机?

11.6　假设一家公司有 6 个独立的部门，每个部门有 10 台计算机或联网的设备，该公司的内网应用怎样的掩码才能使所得的子网平均地分配网络?

11.7　在当代的路由和寻址中，常用的标记方法称为无类域内路由选择（CIDR）。利用 CIDR，掩码的二进制位数用这样的方法表示：192.168.100.0/24，这代表掩码为 255.255.255.0。如果在 256 主机地址网络中使用这一方法，如下情况分别提供了多少个地址?

a. 192.168.100.0/23

b. 192.168.100.0/25

11.8　如果每 1/10 秒就分配出去一个 IPv4 地址，那么多少年后所有的 IPv4 地址就会被全部分配? 如果每秒就分配出去一个 IPv6 地址，那么多少年后所有的 IPv6 地址就会被全部分配? 假设共有 2^{128} 个可用的 IPv6 地址。

11.9　查看自己的网络。使用命令“ipconfig”“ifconfig”或“winipcfg”，我们不仅可以看到自己的 IP 地址，还可以同时看到其他的网络参数。你能自己定义你的掩码、网关及你网络上的可用地址数量吗?

11.10　用你的 IP 地址和掩码，算出你的网络地址是多少。这需要先将 IP 地址和掩码转换成二级制数，再按位进行逻辑与运算。例如，IP 地址为 172.16.45.0，掩码为 255.255.224.0，则我们将会算出网络地址是 172.16.32.0。

11.11　分别给出 3 个弹性因特网数据流和非弹性因特网数据流的例子，并证明所给出的例子属于它们各自的类别。

11.12　为什么一个 DS 域由一系列连续的路由器组成? 在 DS 域中，边界节点路由器和内部节点路由器有什么区别?

第四部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

局域网

第 12 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

局域网体系结构和基础设施

学习目标

通过本章的学习，读者应该能够：

- 定义各种类型的局域网（LAN），并列举出每种类型 LAN 所需满足的条件。
- 描述办公网络、骨干 LAN、工厂 LAN 和层叠 LAN 的主要特征。
- 讨论 LAN 中常用的传输介质。
- 讨论结构化布线系统和 LAN 协议体系结构的特征。

局域网（Local Area Network，LAN）广泛应用于各种规模的商业机构中。今天，它们是构建企业网络的标准构件，许多的业务用户通过连接到 LAN 的设备来日常访问因特网。熟悉 LAN 并且知道它们如何工作，对关于业务计算基础设施做出明智决定非常重要。

近几年，LAN 的技术、设计和商业应用发生了快速改变。这种演进的主要特征是各种新的高速局域网组网方案的引入。这些改变在多方面给商业机构带来了好处，特别是能利用 LAN 在决策制定者之间共享各种类型的业务数据，如语音、数据、图像和视频等。相应地，越来越多的数据和信息共享能提高业务的灵活性、反应敏捷性和创新性。

在这章中，我们将察看 LAN 中采用的技术。第 13 章和第 14 章主要讨论一些特定的 LAN 系统。本章开始时讨论 LAN 的各种类型以及各种 LAN 配置选项。然后我们将看一下可选的有线传输介质，无线传输将在第 14 章中讨论。其后我们再讨论 LAN 协议体系结构。

12.1 背景

LAN 应用具有非常广的多样性。为了解 LAN 应满足的需求类型，这节讨论这些网络最重要的常用应用领域。下一节中我们将看一下 LAN 配置的具体含义。

12.1.1 个人计算机 LAN

LAN 的一个常用配置是支持个人计算机。由于个人计算机价格相对低廉，机构的管理者通常利用个人计算机实现部门应用，如合作和项目管理工具以及因特网访问。台式系统是传统上最常用的一种个人计算机类型，来帮助工作单位中的用户。但近年来，便携式计算机（有或者没有基座）在业务 LAN 中用得越来越普遍。在一些机构中，台式计算机正逐渐被便携式计算机和平板计算机淘汰。

在大型商业机构中，将多个部门级处理器集中在一起并不能满足机构的所有计算需求，集中式的计算机处理设施仍是计算领域的重要组成部分。这种情况也存在于一些机构中，这些机构运用企业资源规划（Enterprise Resource Planning，ERP）系统以及其他企业系统，来支持工作地之间的集成化业务处理。

一些应用（如经济预测模型）因其规模太大或太复杂，不能有效地在某办公室的个人

计算机上执行。在这种情况下，将这些应用运行在位于集中式数据中心的高性能服务器上会更明智。如第 3 章所述，“大数据”应用最可能部署在集中式设施上，内存计算（in-memory computing）应用以及高性能分析应用（High-Performance Analytic Appliance，HANA）盒支持的实时分析也是这样的。一些为项目组和其他业务组提供支持的内部合作软件应用，如 SharePoint 或 SAP 的 StreamWork，也可部署在集中式设施上。当员工需要共享工作和信息时，目前最有效的就是采用数字化方法。

一些昂贵的资源，如复印机、高速黑白或彩色激光打印机和高容量网络连接存储（Network-Attached Storage，NAS）系统，可通过部门 LAN 由所有用户共享。另外，支持单个工作单元的 LAN 可连接起来形成更大规模的、公司范围内的网络设施。例如，某公司可能在每个工作地有一个大楼范围内的 LAN，这些 LAN 组成一个广域的专用网络。由通信服务器为每个工作地提供企业资源的访问控制。

用于支持个人计算机和工作站的 LAN 已在各种规模的机构中广泛应用。即使一些仍旧依赖大型机和集中式数据中心的站点，也已将它们大量的处理负载转移到个人计算机网络中。可能有关个人计算机使用的最常用例子是实现一些客户 / 服务器形式的业务应用。

12.1.2　后端网络和存储区域网络

后端网络（backend network）用来连接大型系统（如大型机、超级计算机和大存储设备），典型地这些系统之间需要传递大量的数据。后端网络有时称为机房网络（computer room network），因为由这些网络连接的大型设备通常物理上位于集中的、温度受控的机房里。这就意味着后端网络的物理范围比较小，因为它们所连接的机器彼此都相距很近。通过将这样的大型设备放于同一网段中，它们之间交换的数据流量就不太可能压垮 LAN 以及降低网络的总体性能。创建后端网络的一个重要需求是在小范围内数量有限的设备之间传递大量数据。通常高可靠性也是一个需求。后端网络的典型特征包括如下：

- **高数据率**：为了满足大数据量传输的需要，数据率需要达到 1000Mbps 或以上。
- **高速接口**：大型主机系统和大存储设备之间的数据传输操作典型地通过高速并行 I/O 接口实现，如光纤通道（fibre channel），而不是低速的通信接口。需要高速接口是因为大型机和超级计算机之间需要通过网络交换大量的数据。
- **分布式访问**：为使得所有设备获得公平、有效和可靠的网络接入，需要一些分布式媒体接入控制（Media Access Control，MAC）技术来做保证。
- **有限的距离**：典型地，一个后端网络部署在一个机房或者少量相连的房间里。
- **有限的设备数目**：由于价格昂贵，后端网络包含的大型机、超级计算机和大存储设备的数量通常是比较少的。同时，有限数量的机器能提高网络效率。

后端网络通常存在于一些集中设施中，这些设施由具有大量数据处理预算的大型公司或研究基地所有。由于后端网络所涉及的规模，即使在后端网络能力方面小的提升都值上亿美元。

我们来考虑一个业务计算站点，该站点利用专用大型计算机运行企业范围内的 ERP 系统或者机构范围内的一组应用。一些功能强大的应用，如医学图像、电子商务、社交媒体和数据仓库，它们需要能处理比以往更大的文件以及更快地移动数据的服务器。由于站点数据处理需求的增长，已有的大型机可能会被功能更强大的单处理机系统或多处理机系统（如服务器群）替代。在一些站点中，仅用单个系统替代还不能满足要求，特别是当用户需求增加的

速度超出设备性能提升速度时。在这种情况下，可能就需要多个独立的大型机（或服务器群）来满足用户需求。因此就有令人信服的理由来将这些系统互连起来。例如，如果网络损坏的代价非常大，那么将这些高性能大型机互连起来，就可将应用简单、快速地转移到备用系统中。通过将一个系统备份到另一个系统中，可在备份系统中测试新的过程和应用，而不影响原有系统。

随着后端网络中计算能力和设备的增加，将大量的存储文件移到存储系统中就比较合适了，该存储系统可被多台计算机访问。由于负载均衡技术能使得系统的利用率和性能最大化，该技术也因此更具有吸引力。

从以上简短介绍可看出，后端网络的关键需求通常与个人计算机 LAN 的需求不同。为了使后端网络正常工作，需要高的数据率，因为这些工作涉及大量的数据传输。获取高速度的设备比较昂贵。幸运的是，为提升计算性能和能力以更好地服务企业范围内的业务用户，在这方面的投资是有合理解释的。

与后端网络相关的概念是**存储区域网**（Storage Area Network，SAN）。SAN 可被描述成一个由多个存储设备组成的独立网络，这些存储设备物理上从网络中移出，但仍旧与网络相连。SAN 由如下概念发展而来：将存储设备和存储流量从 LAN 脱离出来，创建一个独立的专注于处理数据的后端网络。

本质上 SAN 是一个独立的网络来处理存储需求。SAN 将存储事务从特定的服务器剥离出来，并在高速网络之上创建共享存储设施。通过网络相连的存储设备可包括硬盘、磁带库和光盘阵列。大部分的 SAN 运用光纤通道，光纤通道的描述在网上的附录 G 中。

在早期的客户 / 服务器 LAN 中，数据存储在设备上（典型的设备为磁盘驱动器），这些设备在服务器内部或与服务器直接连接在一起。附网存储（Network-Attached Storage，NAS）系统是 LAN 存储系统演化中的下一步。NAS 将存储设备从服务器中分离出来，并将它们直接连接到网络上。SAN 则更进一步，将这些存储设备组成自己独立的网络，并且设备之间采用高速接口直接通信。业务用户则通过服务系统来访问这些存储设备，该服务系统与 LAN 和 SAN 都相连。SAN 的布置能提高客户访问存储设备的效率，此外能提高存储设备到存储设备的直接通信，该通信用于备份和复制功能。

图 12-1 给出了一个典型 SAN 配置的建议。连接在因特网上的用户将文件请求（存储、取回）发送到一排服务器中。这些服务器本地不维护文件，但是与支持许多大型存储设备的 SAN 相连。该 SAN 中包含一些专为处理存储业务而优化过的网络设备。

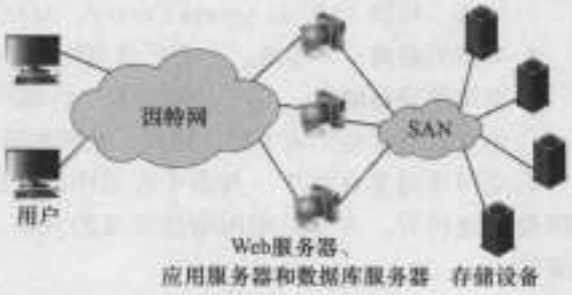


图 12-1　存储区域网络配置

作为 SAN 或 NAS 的补充，固态存储技术越来越多地应用在企业网络中。与传统存储技术不同的是，固态存储设备不需要移动机械部件，如旋转磁盘和可移动读写头。此外，大部分固态存储设备运用了闪存，并且能在不加电情况下保存数据。与磁盘存储相比较，固态存储技术具有较低的时延和数据访问时间，并且制造的噪声较少（基本没有噪声）并且更耐用（更不易受物理撞击影响）。固态存储方案因其快速的数据访问，被云计算服务提供商广泛采用。

12.1.3　高速办公网络

办公环境通常包括多样化的具有低速到中速数据传输需求的设备。然而，办公应用的发展需要将业务转移到高速 LAN 上。一些带宽消耗大的应用，如视频、音频或数据会议基于计算机的训练和电子学习系统，前所未有地增大了网络数据流的需求。其他一些独占带宽的 LAN 应用包括传真机、文档扫描仪、交互式制图和合作软件程序。即使使用了压缩技术，这些应用仍旧能产生巨量的数据流负载。这些新的需求需要高速 LAN，与后端网络相比，这些 LAN 要能支持更多数量的机器，并且支持更大地理范围内的传输。

12.1.4　骨干 LAN

分布式处理应用和个人计算设备（包括移动设备）的使用增长导致了本地连网的灵活策略需求。我们通常需要一个互连设备来支持建筑物范围的数据通信，该设备要能扩展通信所涉及的距离，以及能将单幢大楼或楼群内的设备互连起来。虽然可能只用单个 LAN 将建筑物内所有数据处理设备连接在一起，在大多数情况下这不是一个实际的选择。采用单个 LAN 策略具有许多的不足：

- **可靠性**：在单个 LAN 中，即使很短时间的服务中断都会对用户造成严重破坏。
- **容量**：当连接到网络的设备数量随时间增长时，单个 LAN 很快就达到饱和，特别是带宽消耗大的应用使用也在增加时。
- **成本**：单个 LAN 技术通常无法针对多种多样的连接和通信需求进行优化。大量存在的低成本微型计算机要求支持这些设备的网络也是低成本提供。支持低成本连接的 LAN 通常无法满足企业网络的整体通信需求。

一种比较有吸引力的做法是，在大楼或部门内采用低成本、低容量的 LAN，而用高容量的 LAN 将这些网络互连起来。后一种网络称为骨干 LAN。如果局限在单幢大楼或一楼群内，一个高容量 LAN 能完成骨干功能。骨干网提供基础设施，以实现所连接 LAN 之间的数据和信息交换。通常骨干网的容量要大于其所连接的任一网络的容量。

12.1.5　工厂 LAN

在工厂环境中自动化装置越来越占主导地位：可编程控制器、自动化材料处理设备、机器视觉检测设备和各种各样的机器人。为了管理生产或处理过程，非常有必要将这些装置连接在一起。

制造业机构中变化最多且数据最集中的部分是工厂。运用于生产的微处理设备能从商店收集信息并且接收命令。生产线上可能存在来自多个厂商的各种专用设备。其中每一个设备都可能包括可编程逻辑控制器（Programmable Logic Controller，PLC），如果在生产过程中的每一步都能发现这些可编程逻辑控制器，那么就可以提高生产环境中的数据处理和信息传输。

总的来说，一个工厂的自动化程度越高，则越需要整体的通信。只有通过将设备互连，并且为它们提供合作机制，一个自动化工厂才能发掘出其所有潜力。总体上，一个工厂 LAN 应该达到如下要求：

- 高容量。
- 能处理多种的数据流量。
- 能覆盖大的范围。

- 高可靠性。
- 能指定和控制传输时延。

工厂 LAN 是个很好的商机，与典型的商务办公环境相比，工厂 LAN 通常要求具有更高的可扩展性和可靠性。

12.2　LAN 配置

12.2.1　分层 LAN

现在来考虑一个典型业务机构支持的数据处理设备的类型。初略地，我们可以将该设备分成三类：

个人计算机和工作站：大多数工作场所的工具是微型计算机，包括个人电脑和工作站。在许多机构中，便携式电脑和移动平板电脑也作为业务用户设备。大部分的这种设备用于部门内，由个别专家和秘书使用。当用于网络应用时，依据应用（职员用该应用来完成工作）的属性，该设备产生中等到大量的负载。

服务器：用于部门或部门间用户共享的服务器能完成多种功能。常见的例子包括支持昂贵的外设（如大量存储设备）、提供需要大量处理器资源的应用，以及维护多个用户访问的数据库。由于共享使用，这些机器可能产生大量的流量。

大型机：对于大型数据库以及科学应用，大型机通常是首选机器。当这些机器互连起来以在它们之间交换信息时，大量的数据传输说明需要使用高容量的网络，如后端网络。

上述设备类型所暗示的需求表明了，将所有这些技术组合在一单个 LAN 中通常不是最划算的解决方案。单个网络将不得不具有较高的速度以支持聚集的命令。然而，LAN 的开销将会以网络数据率函数的形式增长。例如，一个 10Gbps 的以太网络适配卡能值几百美元，而 100M/1000Mbps 以太网络适配卡可能只值 15 美元或更少。因此，将低成本的个人计算机连接到高速 LAN 中可能花费比较多。

另一种可选的方案是采用两个或三个层次式的 LAN（见图 12-2），这种方案变得越来越常用了。在部门内部，用一个成本低、速度中等的 LAN 来支持一个由个人计算机和工作站组成的群。这些部分 LAN 通过高容量的骨干 LAN 连接在一起。此外，共享系统也用该骨干 LAN

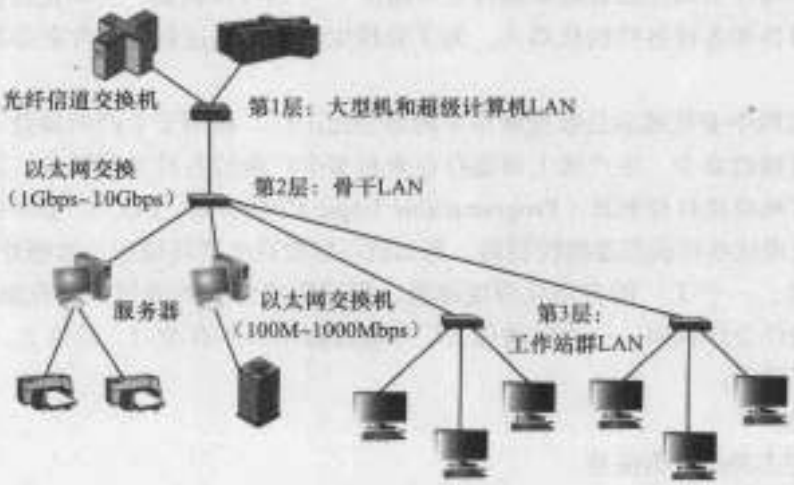


图 12-2　层次式的局域网

来提供支持。如果大型机也是办公设备套件中的一部分，那么一个支持这些设备的单独高速后端网络可作为一个整体连接到骨干 LAN，以支持大型机和部门 LAN 之间的流量。我们将看到解决所有这三种类型 LAN 需求的 LAN 标准和产品。

12.2.2　演进场景

有关层次结构需提及的最后一个方面是：层次网络在机构中的实施方法。不同的业务机构之间所采用的方法各不相同，但可定义两种通用场景。对这两种场景都进行了解是有用的，因为它们蕴含着 LAN 的选取和管理。

在第一种场景中，采用自底向上方式确定 LAN 的决策，其中每个部门几乎独立做决策。在该场景中，每个部门的特殊应用需求通常知道得很清楚。例如，一个工程部门有着非常高数据率的需求来支持部门的 CAD 环境，而销售部门只有中等数据率的需求，用于满足订单登记和订单查询需要。由于熟知应用，每个部门 LAN 需要的基础设施决策很快就能确定下来。部门的预算通常能涵盖这些网络的所有开销或大部分开销，因此可不征得上级管理部门的同意。当遵循自底向上的场景时，每个部门开发自己的网络群（第 3 层）是可能的。与此同时，如果是一个大型机构，其信息服务部门可能需要一个高速 LAN（第 1 层）或者后端网络来将其大型机连接起来。

随着时间的推移，自身拥有群层次 LAN 的部门认识到需要和企业中的其他网络相连，以访问其他的计算资源。例如，市场部门可能从财务部门访问成本信息以及来自销售的上个月订单数量。当群对群的通信需求变得越来越重要时，公司就做出明智的决定来提供互连功能。该互连功能可通过骨干 LAN（第 2 层）来实现。

该场景的优势在于，由于部门管理者贴近部门需求，局部互连策略能对部门内工人使用的特殊应用反应灵敏，并且能及时获得结果。该方案也有一些不足。首先，该方案存在局部最优化问题。如果采购不是由机构集中处理，那么逐部门的购买需求最终会使公司付出更多的成本，特别是当购买相似类型的装置时。另外，大量的购买会带来折扣量和软件许可等方面的有利条件。再者，公司最终都会面对将所有部门 LAN 互连的需求。如果存在很多种不同的群层次 LAN，并且这些 LAN 的硬件来自多个不同的供应商，那么将它们之间互连的问题将会更具挑战性。

基于这些原因，另外一个场景变得越来越通用：自上而下设计 LAN 策略。在该方案中，由公司决定出整个的局域网络策略规划。该决策影响的范围是整个地区或公司，因此它是集中式的。该方案的优点是其固有的兼容性来连接用户。这方案的困难之处在于需要反应灵敏和及时，以满足部门级的需求。

12.3　有导向传输介质

在数据传输系统中，**传输介质**是发送者和接收者之间的物理路径。传输介质可分为有导向和无导向两类。在两种情况下，通信的形式都是电磁波。在**有导向介质**（guided media）中，电磁波沿着固体介质传导，如铜双绞线、同轴电缆或光纤。大气层和外太空则是**无导向介质**（unguided media）的例子，无导向介质提供了传输电磁信号的途径，但不引导信号的传播。这种类型的传输通常称为**无线传输**。

数据传输系统的特征和质量由传输介质的特征和传输信号的特征共同决定。在有导向传输介质中，介质本身是限制传输的重要因素。对于无导向介质，在决定传输特征方面，传输

天线所产生信号的带宽比介质的影响更大。由天线传输的信号的一个关键特性是其方向性。通常低频信号是全方向的，这就是说，信号从天线处开始沿各个方向传播。在高频时，可将信号聚焦为一个定向波束。

在设计一个数据传输系统时，需考虑的包括数据率和传输距离；数据率越高和传输距离越远，则更需要一个精心设计的网络。与传输介质和信号相关的一些设计因素决定了数据率和传输：

- **带宽**：在其他因素保持不变时，信号的带宽越大，则能获得越高的数据率。
- **传输损伤**：损伤（如衰减）限制了有效的传输距离。对于有导向介质，双绞线通常所受的损伤比同轴电缆大，而同轴电缆的损伤也比光纤大。
- **干扰**：由于频带的重叠，竞争信号之间的干扰能使信号失真或导致信号消失。干扰是无导向介质的特别关注点，也是有导向介质的一个问题。对于有导向介质，干扰可由相邻电线的辐射导致。例如，双绞线通常是捆绑在一起的，一个管道通常包含多个的电缆束。无导向传输中也能体验到干扰。将有导向介质恰当地加保护罩能使该问题最小化。
- **接收端数目**：有导向介质能用来构建点到点链路或者具有多个连接点的共享链路。在后一种情况下，每一个连接点都会带来线路上的一些衰减和失真，这些限制了传输距离和/或传输速率。

图 12-3 给出了电磁频谱，并指明了每种有导向传输介质和无导向传输介质工作的频率范围。在这一节中，我们看一看 LAN 中可选的有导向介质，LAN 中可选的无导向传输介质将在第 14 章中讨论。

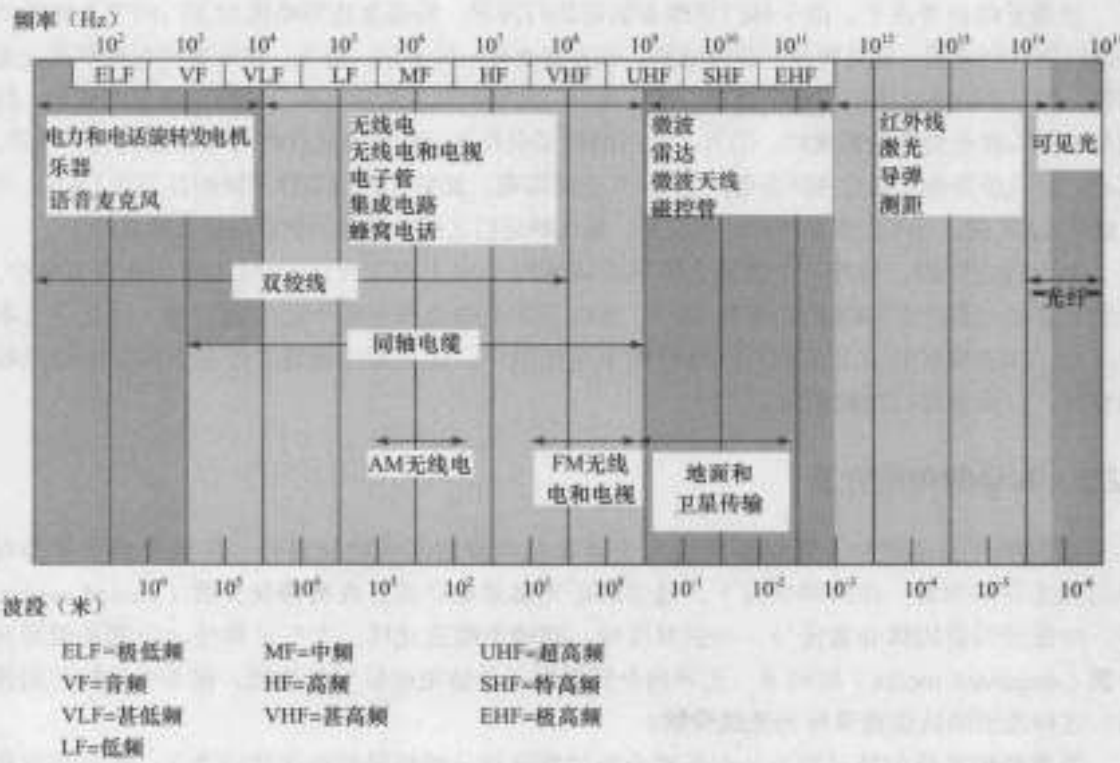


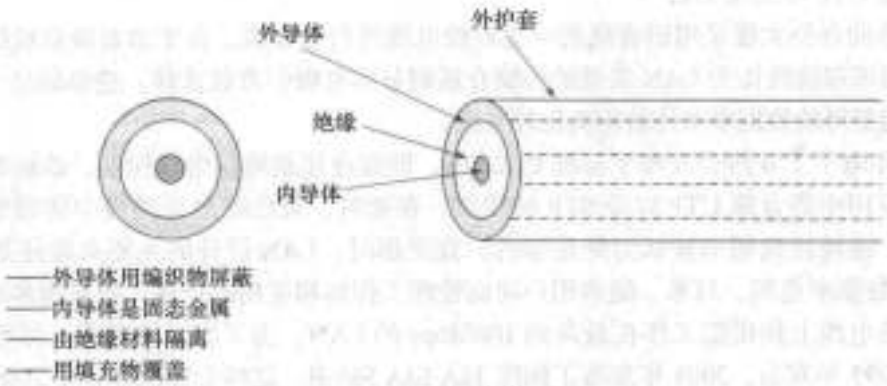
图 12-3　电信中的电磁波频谱

12.3.1　双绞线

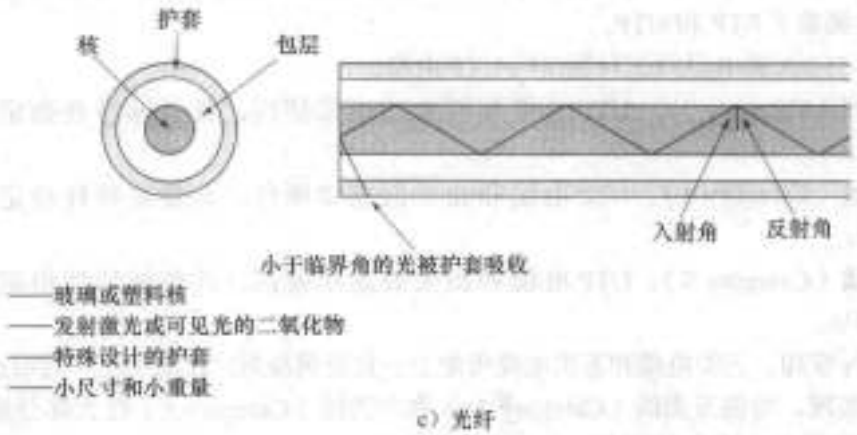
双绞线由两根绝缘的铜线组成，这两根铜线以螺旋形式绞合（twist）在一起，见图 12-4a。一电线对以单个通信链路的形式工作。通常将许多这样的线对用保护套进行保护，并捆成一束放至一电缆中。在远距离传输时，电缆可能包含上千条的线对。



a）双绞线



b）同轴电缆



c）光纤

图 12-4　有导向传输介质

双绞线比其他常用的有导向介质（如同轴电缆、光纤）便宜得多，并且易于操作。与其他传输介质相比，双绞线在传输距离、带宽以及数据率方面都比较受限。由于存在电磁耦合的可能性，双绞线特别容易受干扰和噪声的影响。例如，并行工作在 AC 电力线上的电线将选择 60Hz 能量，脉冲噪声很容易引入到双绞线中。

可采取多种方法来减少损伤。用金属编织物或护套将电线屏蔽起来，可减少干扰。电线绞合在一起可减少低频干扰，而相邻线对之间采用不同的绞距（twist length）可减少串扰。

1. 无屏蔽双绞线和有屏蔽双绞线

双绞线分为两种：无屏蔽和有屏蔽。知道得最多的一种**无屏蔽双绞线**（Unshielded Twisted

Pair，UTP）例子是普通电话线。一种常用的做法是将办公大楼用大量的 UTP 进行预先布线，而不仅仅是单独支持电话的需求。商业大楼也用一种或多种类型的用于数据通信的 UTP 进行布线。由于 UTP 是用于 LAN 的所有传输介质中最便宜的，并且易于操作和安装，它是企业网络中应用最为广泛的通信介质。

UTP 易受外界的电磁干扰，包括来自相邻双绞线的干扰以及环境产生的噪声的干扰。提升这种介质特征的方法是用金属编织物或护套将双绞线进行屏蔽，以减少干扰。这种屏蔽双绞线（shielded twisted pair，STP）在数据率较低时提供更好的性能。然而由于 STP 比 UTP 价格贵并且难于操作，在商业网络中 STP 没有 UTP 应用得广泛。但在噪声较多的工作环境中，选择 STP 或光纤则比选择 UTP 要好。

2. 三类 UTP 和五类 UTP

大部分的办公大楼采用语音级的一类双绞电缆进行预布线。由于语音级双绞线已经安装好了，利用该双绞线作为 LAN 实现的传输介质则是具有吸引力的选择。遗憾的是，利用语音级双绞线能获得的数据率和传输距离比较有限。

1991 年电子工业协会发布了标准 EIA-568，即商业建筑通信电缆标准，该标准描述了在构建数据应用中语音级 UTP 以及 STP 的使用。在那时，对已有办公环境中的频率范围和数据率来说，该规格说明书被认为是足够的。直至那时，LAN 设计的主要兴趣还是 1Mbps 到 16Mbps 的数据率范围。后来，随着用户向高性能工作站和应用的迁移，越来越多的兴趣关注于在便宜的电缆上提供能工作在最高到 100Mbps 的 LAN。为了满足该需求，标准 TIA/EIA-568-A 在 1995 年发布，2001 年发布了标准 TIA/EIA 568-B。这两个标准都被在 2009 年发布的标准 TIA/EIA 568-C 所替代。这个新标准反映了在电缆和连接器设计上的进步，以及测试方法的进步。它涵盖了 STP 和 UTP。

TIA/EIA-568-A 和 B 认可三种类型的 UTP 电缆：

- **三类线**（Category 3）：UTP 电缆和相关的连接硬件，其传输特性指定为最高至 16MHz。
- **四类线**（Category 4）：UTP 电缆和相关的连接硬件，其传输特性指定为最高至 20MHz。
- **五类线**（Category 5）：UTP 电缆和相关的连接硬件，其传输特性指定为最高至 100MHz。

对于 LAN 应用，三类电缆和五类电缆历史上一直受到最为广泛的关注。然而近几年，对于新的 LAN 实现，增强五类线（Category 5e）和六类线（Category 6）已大部分地取代了五类线。增强五类线和六类线在 TIA/EIA 568-C 中描述。

在传输距离有限并且正确设计基础上，五类线能达到最高至 100Mbps 的数据率。五类线和增强五类线能支持快速以太 LAN，如 100BASE-TX 和 1000BASE-T。六类 UTP 提供的性能最高能达到 250MHz，能支持 100BASE-TX（快速以太网）、1000BASE-T/1000BASE-TX（千兆以太网）或者 10GBASE-TX（10 千兆以太网）。这些不同的以太网标准中的“T”或“TX”代表的是双绞线。就如你可能猜想的，由于能支持快速 LAN，增强五类线和六类线越来越普遍地预先安装在新办公大楼中。

各类型双绞线之间的关键不同在于电缆中每单元距离内的绞合次数。例如，五类线比较紧地绞合在一起，它典型的绞距是 0.6 ~ 0.85cm（每英寸绞合 3 ~ 4 次），而三类线的绞距是 7.5 ~ 10cm（每英尺绞合 3 ~ 4 次）。增强五类线每英寸内的绞合次数要比五类线多。增强五

类线和五类线比较紧地绞合在一起，这是它们比三类线昂贵的因素，同时这也是它们能比三类线提供更好性能的原因。

表 12-1 总结了五类 UTP、增强五类 UTP、六类 UTP 以及 STP（在标准 EIA-568 中详述）的性能。图中直接给出了对比的第一个参数，即衰减。在任何传输介质上，信号传输得越远，其强度降低得越多。对于有导向介质，衰减通常是呈指数级，因此通常用单位距离内的常量分贝数来描述（见附录 12A）。

表 12-1　屏蔽双绞线和无屏蔽双绞线的对比

	衰减（分贝 / 每 100 米）				近端串扰（分贝）			
频　率	五类线	增强五类线	六类线	STP	五类线	增强五类线	六类线	STP
1	2.0	2.0	2.0	1.1	62	65.3	74.3	58
4	4.1	4.1	3.8	2.2	53	56.3	65.3	58
16	8.2	8.2	7.6	4.4	44	47.2	56.2	50.4
25	10.4	10.4	9.5	6.2	41	44.3	53.3	47.7
100	22.0	22.0	19.8	12.3	32.2	35.3	44.3	38.5
250	—	—	32.8	21.4	—	—	38.3	31.3

网络设计者需考虑由衰减带来的三个方面。第一，所接收的信号必须具有足够的振幅，以便接收器里的电路能检测到并解析信号。第二，为了信号能被无错误地接收到，信号电平必须要足够地高出噪声电平。第三，衰减是频率的递增函数。

近端串扰（Near-end crosstalk，NEXT）是由于一对导体之间信号与另一对导体之间信号的耦合，双绞线布线系统中存在近端串扰。这些导体可能是连接器中金属针或者电缆中的电线对。近端指的是当进入到链路的信号又返回连接到位于链路同一端的接收导体时所产生的耦合，即就近发送的信号被就近的接收对得到。

自从标准 TIA/EIA-568-C 发布以来，为了建筑内布线，相关的标准改进工作一直在进行。这样的工作由两个因素驱动。一是，千兆以太网规格说明书需要定义一些参数，而这些参数在以往发布的布线标准中没有完整地说明。二是，需要描述更高级别的布线性能，即增强五类线、六类线、增强六类线（Category 6e）、加强六类线（Category 6a）和七类线。表 12-2 中将这些方案与已存在的标准进行对比。

表 12-2　双绞线类型与种类

	五类线 D 类	增强五类线	六类线 E 类	增强六类线	加强六类线	七类线 F 类
带宽	100MHz	100MHz	250MHz	500MHz	500MHz	600MHz
电缆类型	UTP, STP	UTP, STP	UTP, S/UTP	S/UTP, S/STP	S/UTP, S/STP	S/STP
链路成本（五类线 =1）	1	1.2	1.5	1.6	3.0	10.0
与以前标准的不同	取代了只用两对电线的三类线	比五类线的每英寸绞合数多；每条电缆内需要四对电线	与增强五类线相比，采用较厚的电线规范，以及每英寸的绞合数多	比六类线的每英寸绞合数多；采用接地的箔屏蔽	采用比 6e 连接器性能高出 3dB 的新 6a 连接器	比 F 类双绞线有更严格的串扰和噪声需求
速度	100Mbps/100m	350Mbps/100m 1Gbps/50m	1Gbps/100m 10Gbps/50m	10Gbps/100m	10Gbps/100m	10Gpbs/100m 40Gbps/50m

12.3.2 同轴电缆

与双绞线类似，同轴电缆也由两个导体组成，但该导体是通过不同方式构建，以允许其工作在一个较宽的频率范围内。同轴电缆有一个中空的外圆柱形导体，该导体包裹了单个内电线导体，见图 12-4b。

内导体可由规则摆放的绝缘环或固体绝缘材料进行固定。外导体上覆盖有一层外套或护罩。单个同轴电缆的直径为 1 – 2.5cm。由于采用有覆盖的、同轴的构建方式，同轴电缆比双绞线更不易受干扰和串扰的影响。与双绞线相比，同轴电缆能用来远距离传输，并且在共享线路上能支持更多的站点。

像 STP 一样，同轴电缆对电磁干扰有比较好的免疫力。同轴电缆比 STP 成本高，但能提供更多的容量。

同轴电缆是传统的用于 LAN 的重要传输介质，它随着以太网的早期流行而开始使用。然而近几年，关注重点是利用双绞线提供低成本、有限传输距离的 LAN，以及利用光纤提供高性能的 LAN。结果是在 LAN 的实现中逐渐越来越少地使用同轴电缆，直至当前，同轴电缆仅存在于一些传统 LAN 中。

12.3.3 光纤

光纤是一种细的可扩展的传输介质，该介质能传导光射线。各种各样的玻璃和塑料能被用来制作光纤。利用超纯石英制作的光纤能获得最低的信号丢失率。超纯光纤难以制造，而高信号丢失率、多组件的玻璃光纤则更经济且能提供较好的性能。塑料光纤成本甚至更低，能用于短途链路，对该链路而言较高的信号丢失率是可接受的。

光纤具有圆柱外形，并由三个同轴区域组成，见图 12-4c。最里面的两区域是具有不同折射率的两类玻璃，最中间的称为纤芯，另外一层是覆层。这两个由玻璃组成的区域外面包裹着一层具有保护功能且能吸收光的外套。多条光纤成组封装在光缆中。

在信息传输中最重要的技术突破是发明了实用的光纤通信系统。光纤已在长距离电信中得到广泛的使用，它在军事应用中的使用也在逐渐增长。由于性能的逐步提升、价格的下降，以及使用的固有优势，光纤在局域网中的吸引力越来越大。将光纤与双绞线或同轴电缆区别开来的具体特征如下：

容量更大：光纤的潜在带宽以及相应的数据率是无限的。目前已验证了在几十 km 传输距离上能达到几百 Gbps 的数据率。与之相对比的是，同轴电缆在 1km 传输距离上实用的最大数据率是几百 Mpbs，双绞线在 1km 传输距离上仅有几 Mbps 的数据率以及在几十米距离上最多 100Mbps 到 10Gbps 的数据率。

尺寸更小且更轻：对于类似的信息传输容量，光纤比同轴电缆以及成束的双绞线电缆要细很多，至少要细一个数量级。对于大楼内以及沿着公共路权的狭窄导管，小尺寸的优势非常明显。相应的重量减轻也减少了支撑结构的要求。

衰减更低：光纤中的衰减比同轴电缆和双绞线的衰减要低得多，该衰减在一个较广的频率范围内均为常量。

电磁隔离：光纤系统不受外部电磁场的影响。因此，该系统不易受干扰、脉冲噪声或串扰的影响。出于同样原因，光纤不辐射能量，对其他设备几乎不造成干扰，提供很高的安全性以防网络偷听。另外，光纤很难被监听。

光纤系统工作的频率范围为 10^{14} ~ 10^{15}Hz，该频率范围覆盖了部分的红外线和可见光频谱。光纤传输的原理如下。从信号源发出的光进入到圆柱形的玻璃或塑料纤芯。倾角较小的光束经反射沿着光纤传播，其他光束则被周围材料吸收。这种形式的传播称为**阶跃折射率多模**（step-index multimode），指的是多样化的反射角。在多模传输中存在多条传播路径，每条传播路径的长度不同，因此穿过光纤的时间也不同。这造成了信号元素（光脉冲）随时间发生散射，限制了数据能被正确接收的速率。换句话说，需要在光脉冲之间预留间隙，从而限制了数据率。这种类型的光纤最适合很短距离的传输。当减少纤芯的半径时，能反射的倾角就更少了。当将纤芯的半径减少至一个光的波长时，只能有一个入射角或模能通过：近轴光纤（axial ray）。**单模**（single-mode）传播因如下的原因提供杰出的性能。在单模传输中仅有一条传输路径，这样就不会发生多模中出现的信号失真。单模通常应用于长距离应用，包括电话和有线电视。最后，通过调整纤芯的折射率，就形成第三种类型的传输，称为**渐变型多模**（graded-index multimode）。这种类型传输模式的特征介于其他两种类型的特征之间。纤芯的折射率越高，沿着轴前进的光线比靠近覆层的光线传播得越慢。在纤芯内，光线不是在覆层下呈 Z 形前进，而是由于渐变折射率呈螺旋形前进，因而减少了它的传输距离。变短的路径和增大的传播速度使得外围的光线与沿着纤芯轴直的光线的传播时间相近。渐变折射光纤通常运用于 LAN。

光纤系统中采用两种不同类型的光源：发光二极管（Light-Emitting Diode，LED）和注入型激光二极管（Injection Laser Diode，ILD）。两者都是一种半导体设备，当加载电压时就可发射出光束。LED 成本低一些，能工作在较广的温度范围内，并且使用寿命较长。ILD 基于激光理论工作，效率高且能保持高的数据率。

所采用的波长、传输类型和所能获得的数据率之间存在关系。单模和多模都支持多种不同的光波长，并且能使用激光或 LED 作为光源。在光纤中，光线传播得比较好的三种不同波长窗口分别以 850nm、1300nm 和 1550nm 为中心。这些光线的频率都在频谱中红外线对应的部分，比可见光部分（波长为 400 ~ 700nm）的频率低。光的波长越长则信号的丢失率越高，这就允许在更长的传输距离上获取更高的数据率。大部分的本地应用都采用 850nm 的 LED 光源。虽然这种组合的成本相对较低，通常数据率受限于 100Mbps 以下，并且传输距离受限于几公里。为了获取更高的数据率和更长的传输距离，需要运用 1300nm 的 LED 或其他激光源。如果需要最高的数据率和最长的传输距离，则需要 1500nm 的激光源。

12.3.4　结构化布线

作为一个实际问题，网络管理员需要一个布线计划来处理电缆的选择以及大楼内电缆的布线。布线计划应能方便实施且能适应未来的网络增长。在校园环境中，布线计划也包括校园网络（Campus Area Network，CAN）内大楼之间的电缆连接。

为了帮助布线计划的制定，已发布了一些标准来指定电缆类型以及分别用于办公大楼、数据中心和部门大楼的布线。这些标准称为*结构化布线系统*（structured cabling system）。结构化布线系统给出一种通用的布线方案，具有如下特征：

- 该方案指明了一座建筑或一个校园内电信基础设施的布线。
- 该系统支持所有信息传输类型的布线，包括语音、LAN、视频和图像传输以及其他形式的数据传输。
- 电缆布线以及电缆选取独立于产品供应商和端用户设备。

- 布线的设计应遍布建筑物内所有的工作区和生活区，因此设备位置的移动不需要重新布线，只需将设备插入新位置中预先布好的插座即可。

这些标准的一个好处就是为新建筑物内的预先布线提供了指导，这样在未来出现语音和数据连网需求时，不需在该建筑内重新布线就能满足这方面的需求。这些标准也简化了网络管理员的电缆布线设计过程。目前已发布了两个结构化布线系统的标准：TIA/EIA-568，该标准由电子工业协会（Electronic Industries Association）和电信工业协会（Telecommunication Industry Association）联合发布；ISO 11801，该标准由国际标准化组织（International Organization for Standardization）发布。这两个标准比较相似，这节介绍的内容来自于标准 TIA/EIA-568 文档。

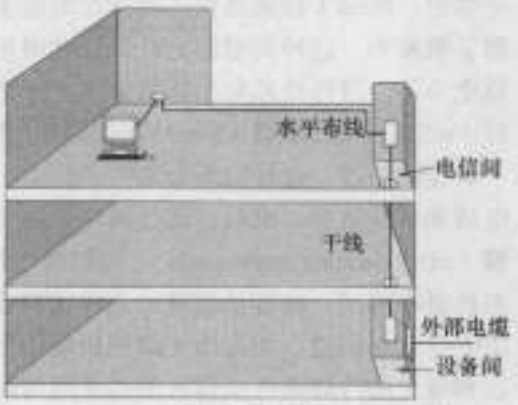


图 12-5　结构化布线布局中的元素

结构化布线策略以层次化、星形的电缆布线为基础。图 12-5 给出了一个典型商务大楼的关键元素。从当地电话局以及广域网（wide area network，WAN）来的外部电缆终止于一个设备间，该设备间通常位于一楼或地下室。设备间内的插线板和交叉互连设备将外部电缆与内部布线相连接。典型地，布线中的第一层由干线（backbone cable）组成。在一种最简单的实现中，单条干线或电缆组从设备间延伸到每层的电信间（称为布线室，wiring closet）。与设备间不同，电信间比较简单，通常包含交叉互连设备以将每层的电缆连接到干线上。在单层楼面上所布的电缆称为水平布线（horizontal cabling）。该布线将干线与服务于电话和数据设备的壁装插头连接在一起。

结构化布线计划的使用有助于企业系统化、标准化地使用符合应用需求的传输介质。图 12-6 指明了结构化布线层次中的每部分推荐的介质。对于水平布线，不论采用何种类型的传输介质，推荐的最大距离是 90m。这个距离能够覆盖许多商业大楼的整个楼层。对于楼层面积特别大的建筑，也可用干线来互连单个楼层上的多个电信间。对于干线布线，根据电缆的类型以及在层次结构中所处的位置，距离范围为 90 ~ 3000m。



介质类型	A	B	C	D
CIP (voice transmission)	800m	500m	300m	90m
Category 3 UTP up to 16 MHz	90m	90m	90m	90m
Category 5 UTP up to 100 Mbps	90m	90m	90m	90m
STP up to 300 MHz	90m	90m	90m	90m
62.5-μm optical fiber	2000m	500m	1500m	90m
Single-mode optical fiber	3000m	500m	2500m	90m

图 12-6　EIA-568-A 中规定的电缆距离

12.4　LAN 协议结构

LAN 体系结构重点关注硬件和传输介质来提供网络平台，以便在所连接设备之间传递数据和信息。如我们在前面小节中所见到的，布线是 LAN 体系结构中的关键方面，特别是在层叠 LAN 环境中。LAN 体系结构与物理设备之间的互连不是紧密相关的。实际上它更关注 LAN 设备为共享传输介质而使用的协议。

LAN 体系结构最好的描述是依据协议层次来组织 LAN 的基本功能。这节首先给出 LAN 的标准化协议体系结构，包括物理层、介质接入控制（MAC）和逻辑链路控制（LLC）层。其后概述 MAC 层和 LLC 层。

12.4.1　IEEE 802 参考模型

为 LAN 和 MAN 传输特别定义的协议要解决的是在网络上传递数据块相关的问题。在开放系统互连（Open System Interconnection，OSI）术语中，高层协议（第 3 或 4 层及以上）独立于网络体系结构，可应用于 LAN、MAN 和 WAN。因此 LAN 协议的讨论主要集中在 OSI 模型中的底层协议，特别是第 1 层和第 2 层。

图 12-7 将 LAN 协议与 OSI 体系结构（见图 1-1）联系起来。该体系结构由 IEEE 802 委员会开发，并且被致力于 LAN 协议规格的所有组织采用，它通常称为 IEEE 802 参考模型。



图 12-7　IEEE 802 协议层次与 OSI 模型的比较

自底向上工作起，IEEE 802 参考模型的最底层对应 OSI 的**物理层**（physical layer），包括如信号编码 / 解码以及比特发送 / 接收这样的功能。此外，物理层也包括了传输介质的规格说明。通常传输介质被认为是位于 OSI 模型最底层以下。然而，传输介质的选择对 LAN 的设计很关键，因此也包含介质的规格说明。

在物理层以上的功能与为 LAN 用户提供服务相关。这些功能包括如下：

- 在发送时，将数据封装在帧内，其中包含地址和差错检测字段。

- 在接收时，解封帧，识别地址并检测错误。
- 控制对 LAN 传输介质的接入。
- 对上层提供接口，并进行流量控制和差错控制。

以上功能典型地与 OSI 第二层相关联。最后一个条目的功能归类进**逻辑链路控制**（Logical Link Control，LLC）层，最前面三个条目的功能则被当成一个独立的协议层对待，称为**介质接入控制**（Media Access Control，MAC）。将这些功能独立出来有如下的原因：

- 传统的第二层数据链路控制中不存在管理共享介质接入所需的逻辑。
- 对于相同的 LLC，可提供多种的 MAC 选择。

图 12-8 给出了体系结构中协议层之间的关系。高层数据（如 IP 报文）向下传递至 LLC，由其添加控制信息做为头部，这样就构建成了 **LLC 协议数据单元**（Protocol Data Unit，PDU）。该控制信息用于 LLC 协议操作中。然后，整个 LLC PDU 向下传至 MAC 层，由其在数据包的首部和尾部添加控制信息，形成 **MAC 帧**。再次，帧中的控制信息用于 MAC 协议的操作中。为了体现上下文，图中也显示了 TCP/IP 的使用以及在 LAN 协议之上的应用层。

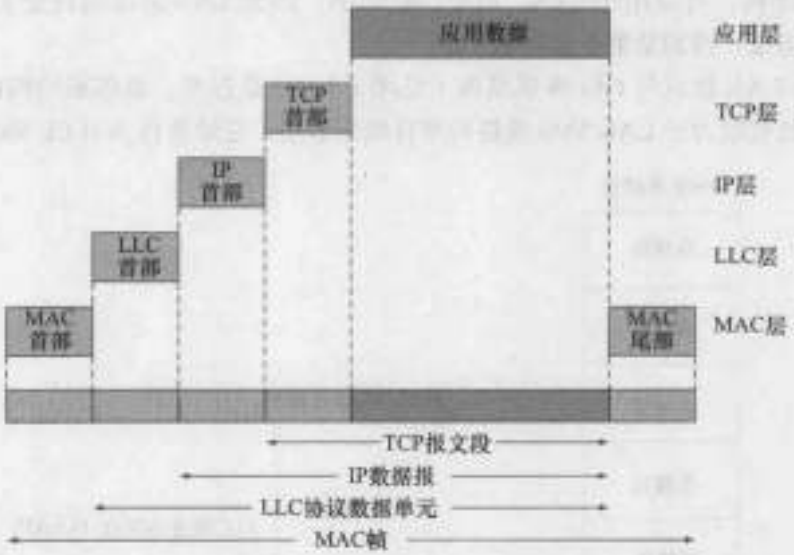


图 12-8　上下文中的 LAN 协议

12.4.2　逻辑链路控制

逻辑链路控制（LLC）是所有 LAN 中的通用链路协议。LLC 描述了传输介质上站点编址的机制以及两用户之间数据交换的控制机制。LCC 层可被认为位于网络层和数据链路层的介质接入控制子层两者之间。LLC 使得 LAN 可用不同的 MAC 协议（如以太网、令牌环）来与通用的网络层协议（如 IP）接口。使用 LLC 能为所连接的设备提供三种可选的服务：

- **无确认无连接服务**（unacknowledged connectionless service）：这种服务是一种数据报类型的服务。它是一种很简单的服务，不需要涉及任何的流量控制和差错控制机制，因此无法保证数据的传递。然而在大部分的设备中，由软件中的高层来处理可靠性问题。
- **连接模式服务**（connection-mode service）：该服务与典型的数据链路控制协议（如 HDLC，见第 6 章）提供的服务相似。在交换数据的两个用户之间建立逻辑连接，并

提供流量控制和差错控制。

- **确认无连接服务**（acknowledged connectionless service）：该服务是前两种服务的交叉。该服务为传递的数据报提供确认，但预先不建立逻辑连接。

无确认无连接服务需要最少的逻辑，在两种上下文中比较有用。第一，通常软件中的高层提供必需的可靠性机制以及流量控制机制，避免重复这些可提高效率。第二，在一些情况下，连接建立和保持的开销太大，甚至是达不到预期目标的。一个例子就是数据收集动作，涉及周期性地对数据源采样，如传感器以及来自安全设备或网络组件的自动自测报告。在监控应用中，偶尔的数据单元的丢失不会导致灾难，因为下一个报告会在很短的时间内到达。因此在大部分情况下，无确认无连接服务是首选。

连接模式服务可被用在很简单的设备中，如终端控制器。这样的设备几乎没有软件工作在该层之上。在这些情况下，就需要提供流量控制机制和可靠性机制，而这两种机制在通信软件中通常是由高层实现的。

确认无连接服务适用于多种场合。在连接模式服务中，逻辑链路控制软件必需维护保存每个活动连接的某种表，以便追踪每个连接的状态。如果用户需要有保证的传递，但数据有非常多的目的地，这样连接模式服务就因为需要大量的表而变得不可用了。一个例子就是处理器控制或者自动化工厂环境，其中的集中控制点需要与大量的处理器和可编程控制器通信。确认无连接服务的另一种应用是处理工厂中重要的、时间紧急的警报或突发事件控制信号。因为它们的重要性，需要确认以便发送者确定信号已到达。由于信号的紧急性，用户可能不愿花费时间先建立连接，然后再传输数据。

LLC PDU 包含目的服务访问点（Destination Service Access Point，DSAP）地址和源服务访问点（Source Service Access Point，SSAP）地址。这些地址关系到使用 LLC 的上层协议，典型地为 IP。LLC PDU 也包含一个控制字段，以提供序列号和流量控制机制。这样的控制字段在数据链路控制协议中具有典型性，这在第 6 章有描述。

12.4.3　介质接入控制

所有的 LAN 和 MAN（Metropolitan Area Network）由一系列需要共享网络传输容量的设备组成。需要一些控制接入传输介质的方案来提供有序、高效的容量使用。这是**介质接入控制**（Media Access Control，MAC）协议的功能。

可通过考虑 LLC 协议与 MAC 协议所涉及的传输格式看出这两个协议之间的关系。用户向下传递至 LLC 层，由该层封装成链路级帧，称为 LLC 协议数据单元（PDU）。然后该 PDU 向下传递至 MAC 层，在该层封装成 MAC 帧。

MAC 帧的确切格式依据所使用 MAC 协议的不同而有所区别。通常，所有的 MAC 帧具有如图 12-9 所示的格式。MAC 帧的字段如下：

- **MAC**：该字段包含 MAC 协议功能所需的任意协议控制信息。例如，优先级可在这指明。
- **目的 MAC 地址**：该帧在 LAN 中的目的物理连接点。该地址是 LAN 中设备的物理（MAC）地址，指明帧的预定接收方。
- **源 MAC 地址**：该帧在 LAN 中的源物理连接点。该地址是帧发送方的物理（MAC）地址。
- **LLC PDU**：来自上层的 LLC 数据，包括用户数据加上源服务访问点（DSAP）地址和

目的服务访问点（SSAP），指明 LLC 的用户。

- CRC：循环冗余校验字段，也称为帧校验序列（Frame Check Sequence，FCS）。这是一种错误检测码，像在其他数据链路控制协议（见第 6 章）中使用的一样。错误控制过程中 CRC 的作用在第 5 章给出。基于整个帧中的比特计算出 CRC 值。发送方计算出 CRC 值，将其放入帧中。接收方对接收到的帧进行相同的计算，并将其与接收帧中的 CRC 字段进行比较。如果两者值不匹配，那么帧在传输过程中发生了一比特或多比特的异常改变，这通常会触发发送方重传该帧。

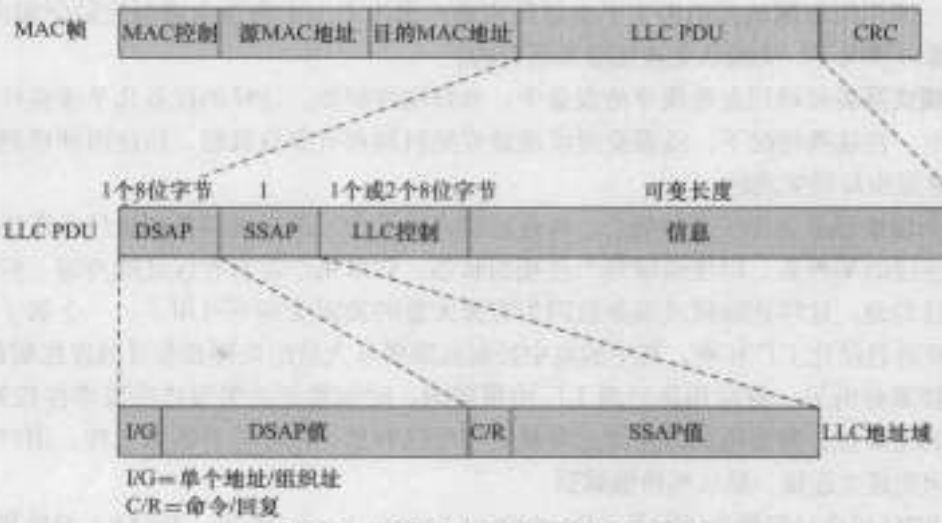


图 12-9 通用 MAC 帧格式的 LLC PDU

在大部分的数据链路控制协议中，数据链路协议实体不仅要负责利用 CRC 检测出错误，还要负责通过重传损坏帧来恢复这些错误。在 LAN 协议体系结构中，这两个功能在 MAC 层和 LLC 层之间分开。MAC 层负责检测错误并丢弃任何包含错误的帧。LLC 层记录哪些帧已正确接收，并且重传不正确的帧。

应用注解

布线基础设施

一个结实的布线基础设施是所有可靠通信的基础。对于新建筑物的布线，必须依据正确的流程，这样才能保证网络按期望的方式工作，并且任务能遵循预算要求。对于已存在布线基础设施的建筑物，很好地了解电缆设备有助于我们理解该系统的不足以及故障瓶颈。即使随着无线通信应用的强势增长，电缆设备仍然是非常重要的，因为无线设备最终都要连接到有线骨干网中。

布线基础设施中有许多重要的组件，布线仅是其中的一部分。网络将是建筑物系统中必需的部分，因此必须为布线间分配地方，并且考虑数据电缆的布置地点。这与需为电气和管道系统要考虑的方面相似。布线间是所有布线的终端，联网设备将放置在这里。布线间包括与数据中心或骨干网的连接，最终连接到因特网上，需提供充足的空间、制冷、排水和净化，已保证设备的长的使用寿命以及可靠连接。通常布线间被认为是一个痛苦的必需品，并被放置在建筑物中环境最差的地方。由于锈蚀、高温、灰尘和干扰都能降低通信

容量，这就会导致较差的网络性能。

布线间存放的位置也不能超出距离的限制。每一个通信标准都有其自身的最大范围。例如以太网中，对于 10Mbps 和 100Mbps 传输，其每一段的长度不能超出 100m。该 100m 包括每一端安装的布线和连接电缆。即使许多建筑物的长或宽都没有 100m，电缆在穿越楼层、天花板以及障碍物时会快速地增加其距离。

布线的质量也会大不相同。有一种说法“通信可在铁丝网上实现，只是不会有高的质量”。虽然五类线、增强五类线、六类线能节约成本，投资时需采用最好的、可用的布线，以增加网络的使用寿命并提供最好的数据率。由于不需频繁地升级，在长远看来通常能节约成本。

其他的布线安装问题包括（不局限于此）如下：接近电力布线，靠近电缆安装的设备（马达、排气管等）、电缆运行中的管理（电缆槽、系带、电缆圈）、电缆的正确使用、备用零件、安装过程中和安装后的损坏、足够长的电缆以允许终端位置的改变（办公室位置决定了要移动的插座）、标签。所有的布线都需要在插座和布线间两端贴上标签，以方便检测故障和更新。随着以太网供电（Power on Ethernet，PoE）的逐渐流行，需要网络设计者重新考虑如何在建筑物内布置电缆的走线。这在高电压的 PoE 系统中是更需要考虑的，因为在这种情况下不可能再将电缆捆成束放置于导体内。

终端的质量也非常重要。越来越多的组合式设备用于新的网络中，这意味着连接可以简单地移动并且很快地结束，但必须要保证购买到正确的组件。每种类型的电缆和应用都有各自独立的终端设备类型。例如，六类实芯电线使用的插座与五类标准电缆的不同。所有的终端设备都需要用适当的网络测试设备（如 Fluke 电缆测量仪）进行检测，该测试设备将检测电缆的串扰、回路、衰减和电路映射，以保证在规格说明书内运行。

在布线间内部需使用适当的电缆管理。电缆管理用来对安装进行组织和整理。如果没有该管理，布线间内将会一片混乱，这样就无法检测故障、维护和添置设备。电缆管理包括一些条目，如水平和垂直管理、前/后片、覆盖物、指南和用于将电缆捆成束的电缆圈。

最后，整个电缆安装需要干净和整洁。没人希望电缆悬挂在墙上或在办公室有一块弯曲的墙体板。也没有网络技术人员希望工作在像意大利面条厂那样的工作间。干净、专业的安装能快速地检测到故障和容易维护，有助于后继的更新，并且不占用不必要的楼层、天花板或布线间的场地。

由于缺少人力或专家，大部分公司利用承包商来进行安装。在这种情况下，需要一个能理解这些问题的本地监督员，他能知道好安装与差安装之间的差别。机构应该研发出自己的用于安装的标准，并且要确保在付款之前已达到这些标准。

12.5　总结

单个建筑物内的连网需求与广域网的需求一样强烈。每一个商业环境中的数据处理设备越来越多。需要局域网（LAN）来将这些设备连接在一起，以保证办公室之间的通信，并提供到广域网（WAN）合算的连接。

LAN 包含共享的传输介质，并包含一组硬件与软件来提供设备与介质的接口并控制对介质的有序接入。

用于传递信息的传输介质可分为有导向和无导向两类。有导向介质提供物理路径，信号可沿着该路径传播。有导向介质包括双绞线、同轴电缆和光纤。无导向介质利用天线透过大气、真空和水进行传输。传统上，双绞线被用于各种通信。近年来，光纤开始起主导作用，在许多应用中已取代其他的介质。两者中，光纤最具有光明的未来，能得到最广范围内的应用。

目前已为 LAN 定义了一组标准，来指定数据率的范围以及传输介质的种类。这些标准被广泛接受，市场上大部分的产品都遵从这些标准中某一个。

结构化布线系统指导建筑物的布线以支持 LAN。存在一些指导原则来帮助网络和建筑设计者来放置电信间、连接 WAN 服务以及在建筑物内水平和垂直地布置网络电缆。

LAN 协议体系结构很少考虑布线基础设施，更多的是考虑提供服务来为连接到网络的设备共享 LAN 传输介质。这些能直接映射到 OSI 参考模型中的数据链路层，专注于介质接入和逻辑链路控制。

实例研究 VIII：卡尔森公司

这个实例研究关注的主要概念包括大存储系统、存储区域网络、后端网络。**有关这个实例研究以及其他更多的信息参见 www.pearsonhighered.com/stallings。**

12.6 关键术语、复习题和练习题

关键术语

backend network（后端网络）
backbone LAN（骨干局域网）
coaxial cable（同轴电缆）
optical fiber（光纤）
server farm（服务器群）
Shielded Twisted Pair（STP，屏蔽双绞线）
Storage Area Network（SAN，存储区域网络）
decibel（dB，分贝）
guided media（有导向介质）
structured cabling（结构化布线）
tiered LAN（分层 LAN）
transmission medium（传输介质）
twisted pair（双绞线）
Logical Link Control（LLC，逻辑链路控制）
Media Access Control（MAC，介质接入控制）
unguided media（无导向介质）
unshielded twisted pair（UTP，无屏蔽双绞线）
wireless transmission（无线传输）

复习题

12.1 计算机房网络与其他个人电脑本地网络不同的关键需求是什么？
12.2 后端 LAN、SAN 和骨干 LAN 之间有什么不同？
12.3 除了大的存储容量，SAN 还能提供哪些优势？
12.4 存储区域网络使用的典型协议有哪些？
12.5 区分有导向介质和无导向介质。
12.6 在双绞铜线中为什么将电线绞和在一起？
12.7 双绞线有什么重要局限？

12.8　无屏蔽双绞线和有屏蔽双绞线之间有什么区别？
12.9　描述光缆的组件。
12.10　光纤与双绞线或同轴电缆有什么不同？
12.11　多模传播和单模传播有什么区别？
12.12　结构化布线系统有什么特征？
12.13　按照带宽从高到低的顺序给下列介质排序：UTP、光纤、同轴电缆。
12.14　按照成本从高到低的顺序给下列介质排序：UTP、光纤、同轴电缆。
12.15　IEEE 802 委员会的目的是什么？
12.16　列举并简单描述 LLC 提供的服务。
12.17　列举并简单描述 LLC 协议提供的操作类型。
12.18　列出 MAC 层实现的一些基本功能。

练习题

12.1　半导体工业需要更大程度的自动化来处理微电子设备。这是因为大部分的半导体操作处理容忍度非常小，因此半导体制造厂必须比普通的医院外科设备还要洁净好多倍。例如，金属氧化物半导体场效应晶体管（MOSFET）的导电电路其长度通常小于 1 微米。相反地，人类头发直径近似 50 微米。因此表面上看来，微小的生物污染（如单个的皮肤薄皮）能使大量的晶体管无法工作。因为人类处理操作对半导体生产流程是有害的，机器人技术和自动化只要有可能就需建立起来。为了实现自动化，SEMI 机构研发了 SECS/GEM（Semiconductor Equipment Communication Standard/Generic Equipment Model）协议。利用因特网研究 SEMI/GEM，提供该标准的基本概述，并讨论与工厂 LAN 设计和操作相关的好处，以及对通常制造通信的影响。用包含 500 ~ 750 字的短文或 5 ~ 8 页 PowerPoint 报告来总结你的发现。

12.2　在校园环境中，布线计划包括为外部服务设备（Outside Service Plant，OSP）的布线。利用因特网研究用于指导布线基础设施的 OSP 标准和指导原则，以将校园环境中建筑物互连起来。

12.3　在一个科学研发机构内，为层次 LAN 设计一个成本效益高的结构化布线方案，该机构正在建造一个五层的研究设施。第一层将包括大厅和管理办公室。第二层和第三层包括一些使用大型高能耗设备（如小的线性加速器和反应离子室）的实验室。许多的技术人员和科学家将工作在这层楼上，数据需求包括高带宽数据（如彩色视频）的高速传输。第四层包括一些实验室人员的办公室，第五层包括一些行政办公室。你的布线方案将描述和说明每层中的水平布线和垂直布线。

12.4　一些机构正实现一个广域网作为高速骨干网，以提高整个特定领域内服务的通信效率和有效性。这样的一个例子有 Network Virginia，该网络为弗吉利亚整个州的机构提供因特网和内部网服务。Network Virginia 也为因特网 2 成员提供区域连网点。利用因特网研究 Network Virginia，并讨论该概念在连网策略演化方面的重要性，其中特别要参照企业网络中的 LAN 支持。用包含 750 ~ 1000 字的短文或 8 ~ 12 页 PowerPoint 报告来总结你的发现。

12.5　利用因特网研究结构化布线，收集一些能说明企业网络中结构化布线含义范围的图像。

将这些图像放到 8 ~ 12 页的 PowerPoint 报告中，来总结商务网络中结构化布线的多个侧面。

12.6 利用因特网研究以太网供电（PoE）的布线以及它与传统以太网布线的区别。说明从传统以太网转换到 PoE 时的布线或重布线需求，也要描述 PoE 电缆中功率电平的趋势。用包含 500 ~ 750 字的短文或 8 ~ 12 页 PowerPoint 报告来总结你的发现。

12.7 收集多个图像来说明增强五类线、六类线和七类线的区别。将这些图像放进 5 ~ 8 页 PowerPoint 报告中来总结这些电缆在物理上有何区别。

12.8 利用因特网研究横贯大陆的光纤电缆布线以及实施海底光纤电缆布线的船只。收集一些图像来说明各大洲之间主要的光纤连接。用 8 ~ 12 页 PowerPoint 报告来总结你的发现。

12.9 利用 Wireshark 抓取你网络中的报文。截取一些视频来说明以太网 LLC PDU 和 MAC 帧的内容。

附录 12A 分贝和信号强度

任何传输系统中的一个重要参数是信号强度。当信号沿着传输介质传播时，其信号强度就会产生损失或衰减。作为弥补，可能在传输路径中插入一些放大器来增加信号强度。

习惯上用分贝（decibel）来表述增益（gain）、损失（loss）和相对电平（relative level），因为：

- 信号强度呈指数级下降，因此很容易用术语分贝（分贝是对数单位）来表述损失。
- 级联传输路径中的净增益或损失可用简单的加法和减法来计算。

分贝是两信号电平比率的一种衡量方法。分贝增益给出如下：

$$G_{dB}=10\log_{10}\frac{P_{out}}{P_{in}}$$

其中：

G_{dB}= 增益，以分贝为单位

P_{in}= 输入功率电平

P_{out}= 输出功率电平

$\log_{10}$= 以 10 为底的对数

表 12-3 给出了分贝值与功率（以 10 为底的指数）之间的关系。

表 12-3 分贝值

功率比	dB	功率比	dB
10^{1}	10	10^{-1}	-10
10^{2}	20	10^{-2}	-20
10^{3}	30	10^{-3}	-30
10^{4}	40	10^{-4}	-40
10^{5}	50	10^{-5}	-50
10^{6}	60	10^{-6}	-60

文献中有关术语增益和损失的使用有些不一致。如果 G_{dB} 为正值，它代表的是功率上实际的增益。例如，3dB 的增益意味着功率加倍。如果 G_{dB} 为负值，它代表的是功率的实际损

失。例如，-3dB 的增益意味着功率减半，这是功率的损失，通常将它表述为损失 3dB，然而有些文献中表述为损失 -3dB。用负的增益来对应正的损失则更有意义，因此我们定义以分贝为单位的损失为：

$$L_{dB}=-10\log_{10}\frac{P_{out}}{P_{in}}=10\log_{10}\frac{P_{in}}{P_{out}}$$

例子　如果一个具有功率电平为 10mW 的信号插入到传输线路上，其后在一段距离外测量到的功率为 5mW，那么损失可表述为 $L_{dB}=10\log(10/5)=10(0.3)=3dB$。

注意分贝描述的是相对差的衡量，而不是绝对差。从 1000mW 到 500mW 的损失也是 3dB 的损失。因此，3dB 的损失将功率减半，3dB 的增益将功率加倍。

分贝也用来衡量电压的差值，考虑到功率与电压平方成比例：

$$P=\frac{V^2}{R}$$

其中：

P= 穿过电阻 R 时消耗的功率

V= 穿过电阻 R 的电压

因此

$$L_{dB}=10\log_{10}\frac{P_{in}}{P_{out}}=10\log_{10}\frac{V_{in}^2/R}{V_{out}^2/R}=20\log_{10}\frac{V_{in}}{V_{out}}$$

例子　分贝能用来确定一系列传输元素上的增益或损失。考虑一系列传输元素，其中输入的功率为 4mW，第一个元素是一条损失为 12dB（即增益为 -12dB）的传输线路，第二个元素是具有 35dB 增益的放大器，第三个元素是一条具有 10dB 损失的传输线路。净增益为（-12+35-10）=13dB。通过下式计算输出功率 P_{out}：

$$G_{dB}=13=10\log_{10}(P_{out}/4mW)$$

$$P_{out}=4\times10^{1.3}mW=712.8mW$$

第 13 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

以太网、交换机和虚拟 LAN

学习目标

通过本章的学习，读者应该能够：

- 解释在以太网类型系统（其数据率越来越高）上的持续兴趣。
- 描述各种各样的以太网替代品。
- 解释网桥、集线器、二层交换机和三层交换机之间的区别。
- 描述以太网供电（PoE）的特征。

近年来，局域网（LAN）的技术、设计和商业应用的变化非常快速。这种演变的主要特征是新的高速局域连网方案。为了与商业中局域连网的变化保持同步，一些高速的 LAN 设计方案在企业网络中变得普遍起来。这些方案中最重要的包括如下：

- **快速以太网和千兆以太网**：从 10Mbps CSMA/CD（Carrier Sense Multiple Access with Collision Detection）迁移到更高速的以太网是一个逻辑策略，因为它能帮助对现存系统保持投资。
- **高速无线 LAN**：无线 LAN 技术和标准都已成熟，已出现了高速的标准和产品。
- **光纤通道**：如第 12 章所述，该标准提供低成本、易扩展的方案来获得高数据率，该标准用于存储区域网络以及其他类型的存储网络。

表 13-1 列出了这些方案的特征。该章的其他部分专注于以太网，无线 LAN 在第 14 章中介绍，光纤通道在附录 G 中介绍。

表 13-1 一些高速 LAN 的特征

	高速以太网	千兆以太网	光纤通信	无线 LAN
数据率	100Mpbs	1Gbps、10Gbps、100Gbps	100Mbps – 3.2Gbps	1Mbps – 600Mbps
传输介质	UTP，STP，光纤	UTP，屏蔽电缆，光纤	光纤，同轴电缆，STP	2.4GHz、5GHz 微波
接入方法	CSMA/CD	交换	交换	CSMA/ 轮询
支持标准	IEEE 802.3	IEEE 802.3	光纤通道协议	IEEE 802.11

13.1 传统以太网

广泛应用于目前企业网的 LAN 称为以太网，它是由 IEEE 802.3 标准委员会发布的。以太网和类似以太网的 LAN 是有线 LAN 市场的主导力量。与其他 LAN 标准一样，以太网标准的多数内容都关注在介质接入控制子层和物理层，这对应于开放系统互连（OSI）参考模型中的第二层和第一层。

早期的以太网遵从原始的 IEEE 802.3 标准组网，该标准工作于 10Mbps。后来发展出分别用于工作在 100Mbps、1Gbps 和 10Gbps 以太网的标准。今天，IEEE 802.3 委员会正在规划

40Gbps 和 100Gpbs 以太网标准。以太网供电（PoE）是 802.3 网络的另一个重要发展方向。

在看 PoE 和高速以太 LAN 前，我们简要回顾传统的 10Mpbs 以太网，因为该传统以太网有助于理解以太网中的传统介质接入控制（MAC）协议。我们也介绍交换 LAN 概念，来帮助更好地理解为什么全交换以太网统治了今天的商务网络。

传统的以太网工作在 10Mpbs，并且是采用总线型拓扑结构的 LAN，其中使用 CSMA/CD（载波侦听多址接入和冲突检测）的介质接入控制协议。在本节，我们将介绍总线型 LAN 概念以及 CSMA/CD 操作，然后简要讨论一下可选的传输介质。

13.1.1　总线型拓扑 LAN

早期以太网 LAN 具有总线型拓扑结构（bus topology），原始的 IEEE 802.3 标准假设有一个总线型拓扑在那儿。在总线型拓扑 LAN 中，所有站点通过称为接头（tap）的硬件接口，直接连接到一条线形的传输介质或总线上。

站点和接头之间的全双工操作允许数据传递到总线上并从总线接收数据。来自任何站点接头的数据传输双向传播至整个长度的介质上，能被总线上的所有其他站点接收到。总线的两端分别是一个终结器，能吸收任意信号，将其从总线上去除以免信号反射回介质。

总线型 LAN 中存在两个通信挑战。一，由于从任一站点的传输可以被所有其他站点接收到，就需要某种方法来指明该传输是传输给谁的。二，需要方案来管理站点的传输。为了明白必须采取管理方案的原因，考虑以下情况：如果总线上有两个站点打算同时发送数据，这样它们所传递的信号就会重叠并且发生改变；或者一个站点决定连续传输很长一段时间，这样就阻碍了其他站点接入到传输介质中。

为了解决这些挑战，站点需要以小数据块的形式传输数据，称为帧（frame）。每帧由站点想发送的数据部分组成，再加上包含控制信息的帧头。总线上每个站点分配一个唯一地址或标识，帧接收方的目标地址包含在帧头中。

图 13-1 给出了传输方案。在该例中，站点 C 打算传递一帧数据到站点 A。帧头中包含站点 A 的地址。当帧沿着总线传播时，它经过了站点 B。站点 B 观察到站点 A 才是该帧的预期接收方，因此就忽略该帧。另一方面，站点 A 看到该帧的目的地址是自身，因此在帧经过时从帧中拷贝出数据。

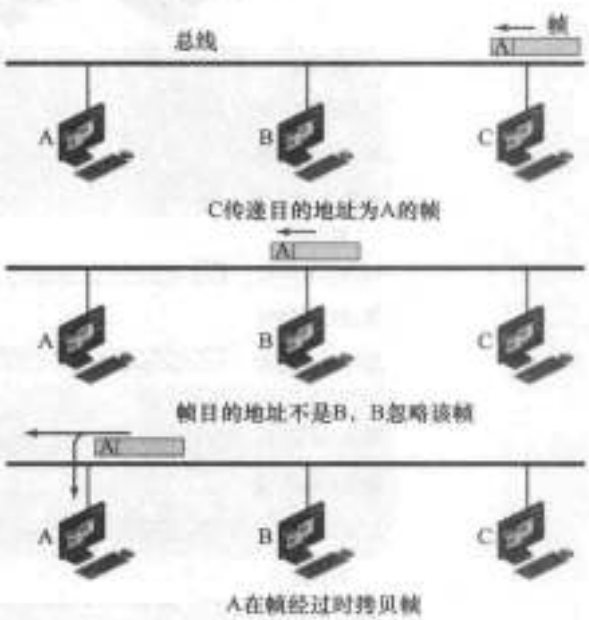


图 13-1　总线型 LAN 中的帧传递

因此帧结构解决了前面所述的第一个挑战：它提供机制来指明数据的预期接收方。它也提供了基本工具来解决第二个挑战，即接入管理。特别是所有站点以某种合作方式轮流发送帧，这将在下一节中描述。

13.1.2　介质接入控制

在 CSMA/CD 中，站点希望先向介质（总线）发送监听帧以确定是否有其他站点正在发

送（载波侦听）。如果介质空闲，该站点就可以发送数据。可能碰巧有两个或多个站点打算在同一时间发送。如果这样的情况发生了，就存在**冲突**（collision）。两个传输的信号将发生改变，它们的预期接收方就不能正确接收到对应的信号。CSMA/CD 的本质是规定了待发送数据的站点在介质繁忙时如何操作，以及在冲突发生时如何操作。具体的操作过程如下：

1）如果介质空闲，则传输；否则转到步骤 2）。

2）如果介质忙，持续侦听直至介质空闲，然后立即传输。

3）如果在传输过程中检测到冲突，传输一简短的干扰信号来确保所有其他站点都知道发生了冲突，从而停止各自的传输。

4）发送干扰信号后，随机等待一段时间，称为**退避**（backoff）时间，然后再准备下一次的传输（重新从步骤 1）开始）。

图 13-2 描述了该技术。图中的上部分展示了总线型 LAN 的布局。图中其他部分描述了四个后继时刻总线上的行为。在时间 t_0，站点 A 开始传输目标地址为 D 的报文。在时间 t_1，站点 B 和 C 都准备好传输。站点 B 检测到线路上正有传输，因此推迟了自己的发送。然而站点 C 仍不知道站点 A 正在传输，就开始自己的传输。当站点 A 的传输在时间 t_2 到达站点 C 后，站点 C 检测到冲突并停止自己的发送。该冲突传播回站点 A，站点 A 在稍后的时间，即时间 t_3，检测到该冲突后停止自己的传输。

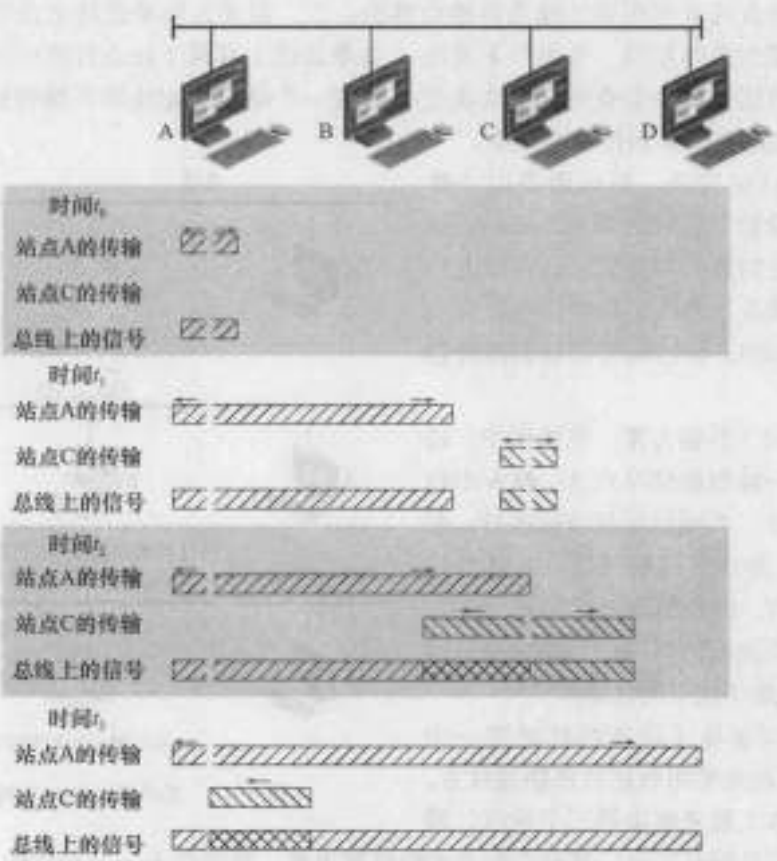


图 13-2　CSMA/CD 操作

CSMA/CD 的好处是其简单性。该协议所需的逻辑很容易实现。此外，该协议的执行很少出错。例如，如果由于某种原因站点没有检测到冲突，最坏的情况是该站点继续传递它自己

的帧，这样就浪费了介质的传输时间。一旦该次传输结束，算法重新恢复如以前一样的功能。

13.1.3　MAC 帧

图 13-3 给出了 802.3 协议的帧格式，它包含如下的字段：

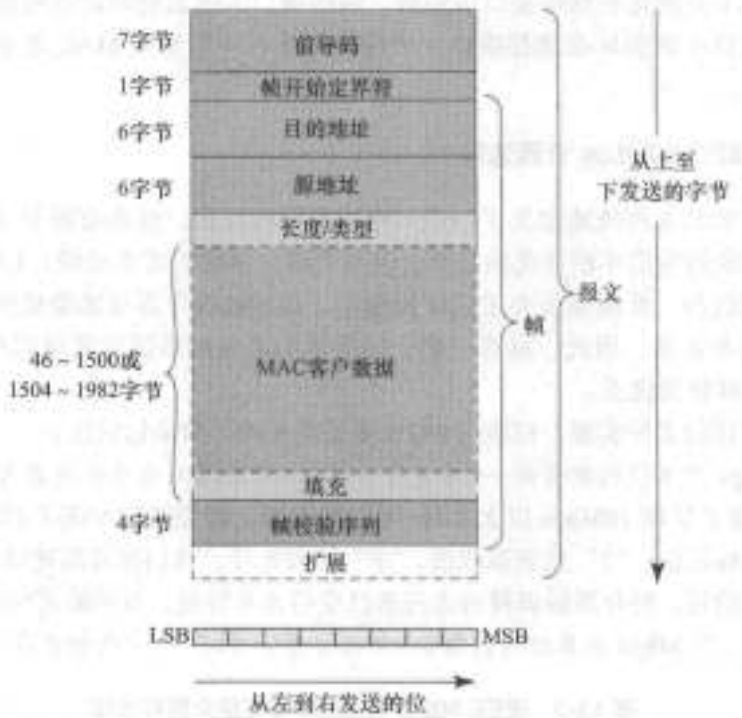


图 13-3　IEEE 802.3 MAC 帧格式

- **前导码**（preamble）：由 0 和 1 交替的 7 字节模式，接收方用来建立位同步。
- **帧开始定界符**（Start Frame Delimiter，SFD）：序列 10101011，用来指明帧真正开始，以便接收方确定帧中其他部分的开始位。
- **目的地址**（Destination Address，DA）：指明该帧的预期接收站点。它可能是一个唯一物理地址、一组地址或一个广播地址。
- **源地址**（Source Address，SA）：指明发送该帧的站点。
- **长度 / 类型**（length/type）：依据该字段的值，从两种意思中取其一种。如果该字段的值小于或等于十进制 1500，则该字段表明基本帧中后继 MAC 客户数据字段包含的 MAC 客户数据长度，即该字段以长度理解。如果该字段的值大于或等于十进制 1536，则该字段表明的是 MAC 客户协议，即该字段以类型理解。该字段是以长度还是类型理解是互斥的。
- **MAC 客户数据**（MAC client data）：LLC 提供的数据单元。对于一个基本帧，该字段的最大长度是 1500 字节，对于 Q-tagged 帧该字段长度为 1504 字节，对于信封帧（envelope frame）该字段长度为 1982 字节。
- **填充**（pad）：在帧中添加的一些字节以使得帧足够长，从而保证正确的冲突检测（CD）操作。
- **帧校验序列**（Frame Check Sequence，FCS）：基于帧中除前导码、SFD 和 FCS 之外所

有字段计算出的 32 比特循环冗余校验。

- **扩展**（extension）：如果由于 1Gbps 半双工操作的需要，则添加该字段。当介质工作在半双工模式且工作速率为 1Gpbs 时，需要扩展字段来加强最短的传输时间持续时间。

站点的源地址也称为其 MAC 地址。如果一站点为个人计算机（PC），它的 MAC 地址是在生产网络接口卡时固化在网络接口卡中的。网络接口卡的退避时间也可能在生产时随机分配。如果网络接口卡因损坏必须替换掉，则该机器将有一个新的 MAC 地址，也可能有一个不同的退避时间。

13.1.4　IEEE 802.3 10Mbps 介质选择

IEEE 802.3 委员会传统地定义了一系列可选的物理配置。这既有好处又有坏处。从好的方面来说，该标准能响应不断变化的技术，包括光纤。从坏的方面来说，LAN 客户需面对越来越多的一系列选择。然而委员会正在痛苦地保证多种选择可容易地集成到一个配置中，以满足多样化的商务需求。因此，具有一套复杂需求的企业网络设计者可以在 802.3 标准中看到可扩展性和多样性的优点。

为了区别可用的多种实现，初始的 802.3 委员会采纳了简练标记法：

<以 Mbps 为单位的数据率><信号传输方法><以百米为单位的最大段长度>

表 13-2 总结了早期 10Mbps 以太 LAN 可用的选择。注意 10BASE-T 和 100BASE-F 不是特别符合如下的标记法："T" 代表双绞线，"F" 代表光纤。我们在对高速以太 LAN 的讨论中将变得显而易见的是，将介质标识符包含进来已变得非常普遍，目前的简练标记法如下：

<以 Mbps 为单位的数据率><信号传输方法><介质标识符>

表 13-2　IEEE 802.3 10Mbps 物理层介质可选项

	10BASE5	10BASE2	10BASE-T	10BASE-F
传输介质	同轴电缆	同轴电缆	无屏蔽双绞线	850nm 光纤对
拓扑	总线型	总线型	星形	星形
最大段距离（米）	500	185	100	500
每段中的节点数	100	30	—	33
线缆直径	10mm	5mm	0.4 ~ 0.6mm	62.5/125μm

13.2　网桥、集线器和交换机

在继续讨论以太网之前，我们需要绕点弯路来介绍网桥、集线器和交换机的概念。

13.2.1　网桥

实际上在所有情况下，都有突破单个 LAN 限制的扩展需求，来提供与其他 LAN 以及广域网（Wide Area Network，WAN）的互连。为了达到这个目的，通常使用两种通用的方案：网桥和路由器。网桥（bridge）是这两种设备中较简单的，提供相似 LAN 之间的互连。路由器是一种更具通用目的的设备，能提供多种 LAN 和 WAN 之间的互连。

桥接（bridging）和路由（routing）都是数据控制的形式，但它们通过不同的方法工作。桥接工作在 OSI 参考模型的数据链路层，路由工作在网络层。这种不同意味着网桥使用 MAC 地址来引导帧，而路由器将它的转发决定建立在网络层地址（如 IP 地址）基础之上。

基本网桥设计用在 LAN 之间或 LAN 的网段之间，它们在物理层和网络层中使用相同协议（如都遵守 IEEE 802.3 标准）。由于所有设备都使用相同协议，网桥处所需的处理总量是最少的。更复杂的网桥能从一种帧格式映射到另一种帧格式，如将以太网和光纤通道 LAN 互连。

由于网桥应用于所有 LAN 拥有相同特征的情况下，读者可能会问，为什么不简单地组建一个大的 LAN 呢？依据实际环境，使用通过网桥相连的多个 LAN 或多个 LAN 网段来取代一个大的 LAN，其原因有如下几种：

可靠性（reliability）：将一个机构内的所有数据处理设备连接成一个网络的危险在于，网络中的一个错误将使得所有的设备之间不能相互通信。使用网桥后，网络被分为多个独立的单元。每一个独立单元称为一个冲突域（collision domain），因为该单元内是一组会发生数据冲突的计算机。将大型网络分段成多个冲突域，有助于避免一个网段内的错误影响到整个网络。

性能（performance）：通常 LAN 的性能随着设备数量的增加或电缆长度的增加而下降。向以太 LAN 中添加设备增大了冲突的概率，而冲突的增加能降低网络的性能。将一个大的 LAN 划分成多个规模小些的网段能提升网络性能，特别是当设备集结成群使得网络之间的通信流量严重超出网络内通信流量时。

安全性（security）：多个 LAN 的创建可能提升通信的安全性。将具有不同安全需求的不同类型通信流量（例如审计、）分布在物理上独立的介质上，这更具合理性。同时，具有不同安全等级的不同类型用户，他们需要有通过控制和监督机制的通信。

地理位置（geography）：显然地，需要有两个独立的 LAN 来分别支持在两个地理上相距较远的位置聚集成群的设备。即使在两座大楼被一条公路隔开的情况下，用一个微波网桥链路也比试着在两座大楼之间布置电缆要容易得多。

图 13-4 给出一个网桥连接两个 LAN（A 和 B）时的动作，这两个 LAN 使用相同的 MAC 协议。在这个例子中，用一个简单的网桥来连接两个 LAN，通常网桥的功能通过两个“半网桥（half-bridge）”实现，每一个半网桥在一个 LAN 中。网桥的功能少且简单：

- 读入 A 传递的所有帧，接收传递给 B 内任意站点的帧。
- 为 B 使用介质接入控制协议，重传 B 中的每帧。
- 为从 B 到 A 的通信流量做相同的工作。

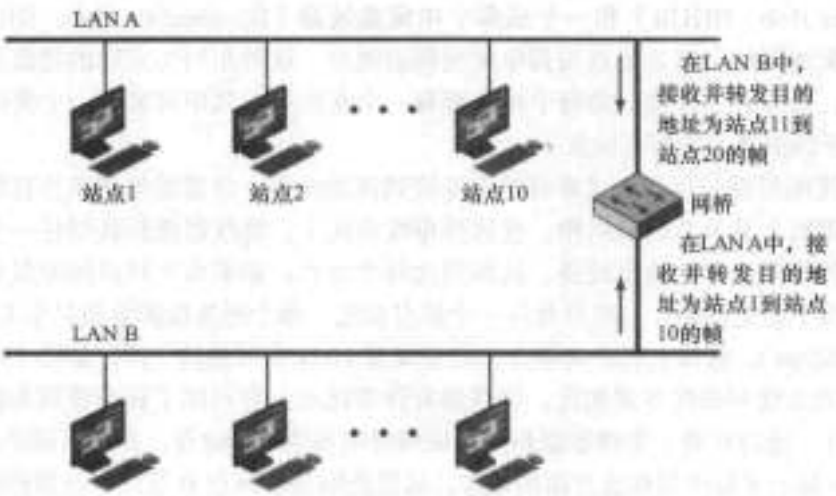


图 13-4　网桥操作

有关网桥设计方面，有如下一些值得注意的：

- 网桥不修改所接收帧的内容或格式，也不将其用一额外的头部进行封装。仅从一个LAN中拷贝一份每个传输的帧，然后按其完全相同的比特模式转发到另一LAN中。由于两个LAN使用相同的LAN协议，是允许这样做的。
- 网桥应该包含足够的缓冲区空间以应对峰值需求。在一较短的时间内，帧的到达速度可能比转发速度快。
- 网桥必须有寻址和路由能力。至少网桥应该知道那个地址属于哪个网络，这样才能知道要传递哪些帧。进一步地，可能有多于两个的LAN通过一些网桥连接在一起。在这种情况下，一帧在从源端到目的端的传递过程中可能需要经过多个网桥的路由。
- 一个网桥可能连接多于两个的LAN。

总的来说，网桥为LAN提供了扩展，而不需要修改连接到LAN的站点上的通信软件。在两个（或以上）LAN中的所有站点看来只有单个LAN，其中每个站点拥有唯一的地址。每个站点都使用唯一地址，不需要将相同LAN内的站点与不同LAN内的站点进行准确区分。网桥会关心这个。

13.2.2　集线器

近年来，除了网桥和路由器外，越来越多类型的设备用于将LAN互连起来。这些设备可方便地归类为第二层交换机和第三层交换机。我们以讨论集线器（hub）开始，其后探讨这两个概念。

集线器可取代总线型拓扑结构。每个站点用两根线（分别用于发送和接收）连接到集线器。集线器像中继器（repeater）一样工作：当一个站点发送时，集线器将信号转发到与输出线路相连的每个站点。像其他中继器一样，集线器是工作在OSI参考模型物理层（第一层）的相对简单的网络设备。集线器不管理流经它们的流量。从集线器一个端口来的任何帧，广播或转发到该集线器中除了来的端口外的所有其他端口。由于每个数据包是转发到其他所有端口的，可能会发生冲突，从而影响到整个网络的性能。

通常，连接站点和集线器之间的线路由两根无屏蔽双绞线组成。由于UTP的高数据率和高传输质量，线路的长度限定为100m左右。可使用光纤链路作为可选的线路，在这种情况下，线路的最大长度为500m左右。

多级的集线器可用层次式的配置串联在一起。图13-5描述了两级配置，其中有一个**头集线器**（Header Hub，HHUB）和一个或多个**中间集线器**（Intermediate Hub，IHUB）。从下层连接到每个集线器的可以是站点与其他集线器的混合。这种布局与实际的建筑布线情况相吻合。典型地，每座办公大楼中的每个楼层都有一个布线间，其中可放置一个集线器。每个集线器可服务于该层楼上的所有站点。

集线器使用星型的布线方式来将站点连接到该集线器。注意虽然该拓扑在物理上是个星型结构，它逻辑上是个总线型结构。在这种布线方式下，集线器能接收到任一个站点发送的数据，将其转发到所有的输出线路，从而到达每个站点。如果两个站点同时发送，就会产生冲突。因此为了避免冲突，一次只允许一个站点发送。每个所连接的设备共享LAN中的所有传输（如10Mbps），就像它们在共享介质的总线型LAN中所做的一样，如图13-6a所示。

与简单的总线型布线方式相比，集线器有许多优点。它利用了标准建筑布线方式中的线缆布局。此外，通过配置，集线器能识别造成网络堵塞的故障站点，并且将该站点从网络中去除。图13-6b显示了集线器在这方面的操作。这里仍旧是由站点B发送，该数据经过传输线路从站点B到达集线器，然后从集线器开始，经由与每个其他所连接站点的接收线路继续传递。

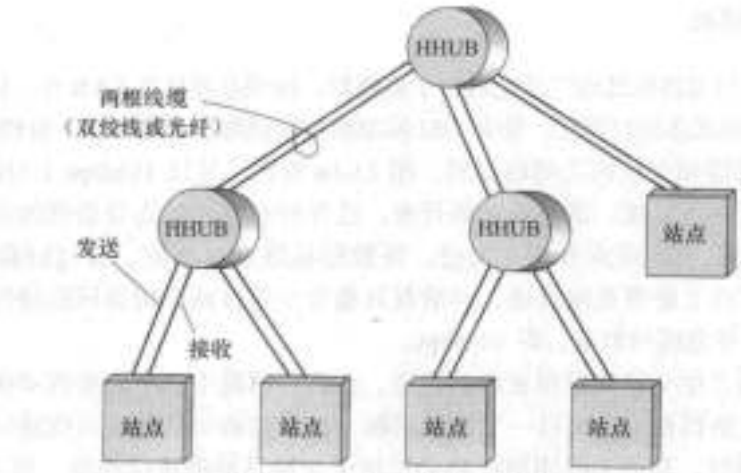
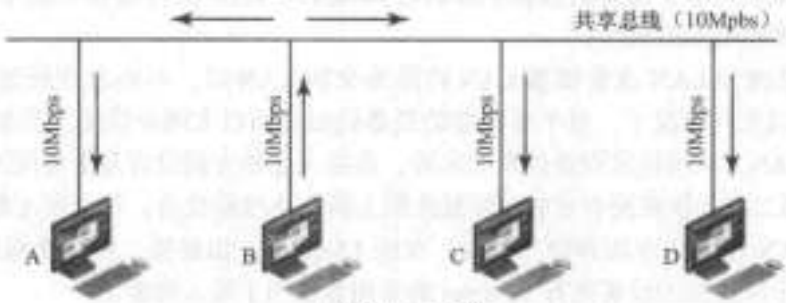
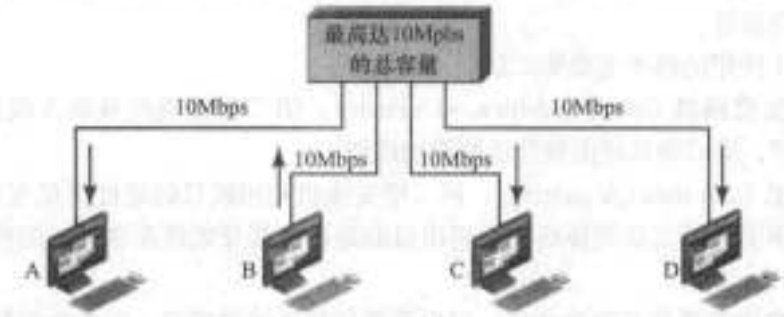


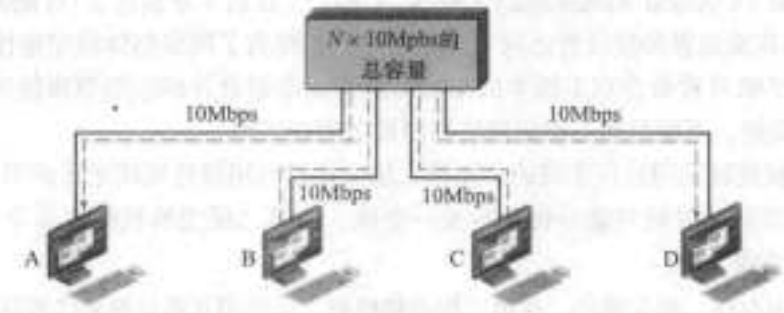
图 13-5　两级星形拓扑结构



a）共享介质的总线



b）共享介质的集线器



c）第二层交换机

图 13-6　LAN 中的集线器和交换机

13.2.3　第二层交换机

近年来，第二层交换机已经广泛地取代了集线器，特别是在高速 LAN 中。第二层交换机有时被称为交换集线器或多端口网桥，能在 OSI 模型的数据链路层（第二层）处理和路由数据。

为了阐明集线器和交换机之间的差别，图 13-6a 展示了传统 10Mbps LAN 的典型总线型布局，其中安装了一条总线，该总线铺展开来，这样所有待连接的设备都能合理地接近于总线上的接入点。在图中，站点 B 正在发送。该数据从站点 B 出发，穿过链路从 B 点到达总线，然后在两个方向上沿着总线传递，再沿着其他每个连接站点的访问线路传递。在该配置中，所有的站点分享总线的容量，即 10Mbps。

我们能通过第二层交换机获得更高的性能。在这种情况下，中心集线器像交换机一样工作，与数据分组交换机相似。来自一个站点的帧，被交换到合适的输出线路以便传递到预期的目的地。与此同时，其他未使用的线路仍可用于交换其他的通信流量。图 13-6c 展示了一个传输例子，其中站点 B 正在向站点 A 传递一帧，同时站点 C 正在传递一帧给站点 D。因此在该例子中，虽然每单个设备的数据率限制为 10Mpbs，LAN 的当前吞吐量为 20Mbps。第二层交换机有许多吸引人的属性：

1）在将总线型 LAN 或集线器 LAN 转换为交换 LAN 时，不需改变所连接设备中的软件或硬件。在以太网情况下，每个所连接的设备仍旧使用以太网介质接入控制协议（CSMA/CD）来接入 LAN。从所连接设备的角度来看，在接入逻辑方面没有发生任何改变。

2）假定第二层交换机拥有足够的容量来跟上所有连接的设备，每个所连接的设备则具有与整个原始 LAN 相同的专用容量。例如，在图 13-6c 中，如果第二层交换机能支撑 20Mbps 的吞吐量，每个所连接的设备则有 10Mpbs 的专用容量用于输入和输出。

3）第二层交换容易扩展。通过在第二层交换机上连接额外的交换机，就可以相应地增加第二层交换机的容量。

商务网络中使用的两类主要第二层交换机如下：

存储－转发交换机（store-and-forward switch）：第二层交换机从输入线路上接收一帧，短暂地将其缓存，然后将其路由到合适的输出线路。

直通交换机（cut-through switch）：第二层交换机利用帧目的地址出现在每个 MAC 帧的开始处这样的事实。第二层交换机一识别出目的地址，就开始将正在输入的帧转发到合适的输出线路上。

直通交换机能获得最高的吞吐量，但也冒着传播坏帧的风险，因为交换机不能在转发前做循环冗余检测（Cyclical Redundancy Check，CRC）（在第 5 章描述）。存储转发交换由于要做 CRC 校验，在发送者和接收者之间引入了延迟，但提高了网络整体的完整性。

第二层交换机可看做全双工版本的集线器。它也能够合并相应的逻辑使得自己具有多端口网桥一样的功能。下面是第二层交换机与网桥之间的区别：

- 网桥的帧处理是用软件实现的，而第二层交换机利用硬件实现地址识别和帧转发功能。
- 网桥通常同一时刻只能分析和转发一个帧，而第二层交换机拥有多个并行数据路径，能同时处理多帧。
- 网桥使用存储－转发操作。在第二层交换机中，可使用直通交换来代替存储－转发操作。

由于第二层交换机具有更高的性能，且能合并网桥的功能，在今天的 LAN 中网桥已不像以往那样使用得普遍了。新的布线通常采用具有网桥功能的第二层交换机，而不使用网桥。

13.2.4　第三层交换机

与共享介质的集线器相比，第二层交换机提供高的性能以满足 PC 机、工作站和服务器产生的大量通信流量的需求。然而，随着大楼内的设备数目增加或大楼复杂性的增加，第二层交换机也显示出一些不足。

通常来讲，第二层交换机具有与桥接网络相同的限制。与网桥相似的是，如果网络的设计遵循 80/20 规则并且用户将他们 80% 的时间用于与他们本地网段内设备之间的通信，那么第二层交换机就工作得比较好。此外，虽然网桥和第二层交换机将一个网络分成多个冲突域，整个网络仍然是一个广播域。大的广播域会带来问题，随着网络的增长，能造成网络的性能问题。由于这些问题，第二层交换机不能完全取代路由器。

由第二层交换机连接的一批设备和 LAN 认为是处于一个平面地址空间（flat address space）。术语平面表示所有的用户共享一个通用的 MAC 广播地址。因此，如果任意设备产生出一个带有广播地址的 MAC 帧，那么该帧将会传递至由第二层交换机和 / 或网桥连接的整个网络中的所有设备。在一个大型网络中，频繁地传输广播帧能产生很大的负载。更坏的是，故障设备能产生广播风暴（broadcast storm），其中大量的广播帧阻塞了网络，并将合法的通信流量排挤在外。

使用网桥和 / 或第二层交换机的与性能相关的第二个问题是，现有网桥协议标准要求网络中不能有封闭环路。就是说，任何两个设备之间只有一条通信路径。因此在基于标准的实现中，在设备之间的多个交换机之间提供多条路径是不可能的。该条件既限制了网络的性能，也限制了网络的弹性。

为了解决上述问题，将一个大型局域网络划分成由路由器连接的多个**子网**（subnetwork）比较合理。这样，一个 MAC 广播帧就限制在单个子网内的设备和交换机内传递。此外，基于 IP 地址的路由器采用复杂的路由算法，以允许穿越不同路由器的子网之间使用多条路径。

然而，使用路由器来解决网桥和第二层交换机部分不足的问题是，路由器通常采用软件而不是硬件来实现转发 IP 通信流量时所涉及的 IP 层处理。高速 LAN 或高性能第二层交换机可能每秒产生几百万个数据包，而基于软件实现的路由器可能每秒只能处理少于一百万个的数据包。为了适应现阶段高速 LAN 产生的高通信流量负载，一些生产商已开发出第三层交换机，它采用硬件实现路由器的数据包转发逻辑。因此，第三层交换机能描述成基于硬件的路由器。

市面上有多种的第三层方案，但从根本上可归为两类：逐包（packet-by-packet）的和基于流（flow-based）的。逐包第三层交换机像传统的路由器一样工作。然而，由于转发逻辑是用硬件实现、与基于软件的路由器相比，逐分组交换能获得指数级的性能增长。

基于流的第三层交换机通过识别具有相同源地址和目的地址的 IP 数据包流来增强性能。这可通过查看流经的通信流量或数据包头中的特殊流标签（仅在 IPv6 中允许，IPv4 中不支持，见图 8-7）来做到。一旦识别出一个流，就可为之建立通过网络的预定义路由，以加速其后的转发过程。通过这种方案，能再次获得比基于纯软件的路由器高得多的性能。

图 13-7 给出了一个典型的解决方案例子，该方案应用于拥有大量 PC 机和工作站（几千台到几万台）机构的局域组网中。桌面系统通过 100 ~ 1000Mpbs（1Gbps）链路连接到由第二层交换机控制的 LAN 中。移动用户也可使用无线 LAN 连接。第三层交换机位于局域网络的核心处，形成一个局域骨干网。典型地，这些交换机以 1Gbps 或 10Gbps 的速率互连，并且以 1 ~ 10Gbps 的速率连接到第二层交换机。服务器以 1Gbps 或可能到 10Gbps 的速率直接

连接到第二层或第三层交换机。由较低成本的基于软件的路由器提供到 WAN 的连接。图中的圆圈标识独立的 LAN 子网，MAC 广播帧限制在它自己所在的子网内。

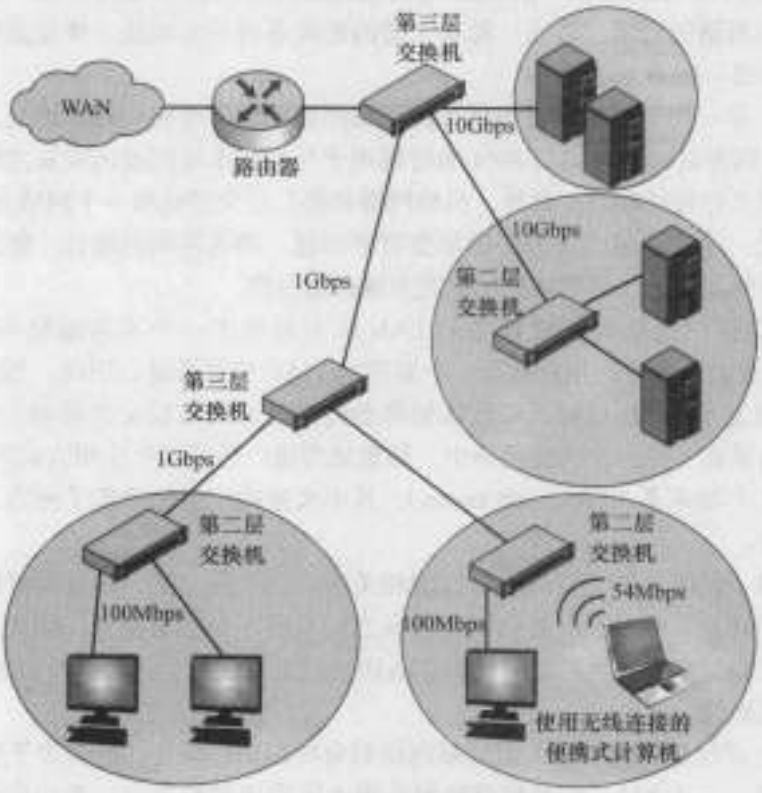


图 13-7　典型的驻地网配置

13.3　高速以太网

13.3.1　快速以太网

如果有人要重新开始设计一个高速（100Mpbs 或以上）LAN，他将不会选择 CSMA/CD 作为设计的基础。CSMA/CD 实现简单，并且对错误的鲁棒性好。然而，它的扩展性不好。随着总线上负载的增长，冲突的数量也会增加，从而影响了性能。此外，随着给定系统的数据率增大，其性能也会下降。这是因为在高的数据率下，站点在识别出冲突前能发出更多比特的数据，因此当出现冲突时，会传递更多的无用比特数据。

这些问题是可以解决的。为了适应更高的负载，系统可设计成拥有多个不同的网段，这些网段之间通过交换集线器互连。如前面所述，这些交换机可像障碍物一样工作，将 LAN 分成多个冲突域，因此发生在一个域内的冲突不会传播到其他域内。使用交换以太集线器能很好地减少冲突，进而提高网络的效率。

尽管用 CSMA/CD 作为 MAC 协议存在一些不足，目前已开发出工作在 100Mbps、1Gbps 和 10Gbps 的以太类型 LAN。这里面的原因很具有启发性。从生产商角度来说，CSMA/CD 协议很好理解，并且生产商有为这些系统生产硬件、固件和软件的经验。将这些系统升级至 100Mpbs 或更高，可能比实现一个新的代替协议和拓扑要容易。从客户角度来说，如果所有系统采用相同的帧格式和相同的接入协议，那么将工作在 10Mpbs 的旧以太系统与工作在更

高速率的新系统集成在一起，会相对比较简单。换句话说，继续使用以太类型的 LAN 是具有影响力的，应为以太网已在那儿了。在数据通信的其他领域也会碰到相同的情况。生产商和客户不经常甚至在大部分情况下不会选择技术领先的解决方案。成本、易管理性以及与已有设备基础相关的其他因素通常是选择新 LAN 中设备的更重要因素，这些因素比技术领先的候选方案更重要。这就是以太类型系统继续统领 LAN 市场的原因，在可见的将来这种局面仍然会持续。

快速以太网（Fast Ethernet）指由 IEEE 802.3 委员会指定的一系列规范，提供工作在 100Mbps 的低成本、兼容以太网的 LAN。对这些标准全面进行设计的是 100BASE-T。该委员会为不同的传输介质定义了一系列的备选项。

表 13-3 总结了 100BASE-T 选项的关键特征。所有的 100BASE-T 选项使用了 IEEE 802.3 MAC 协议和帧格式。100BASE-X 指使用物理介质规范的一系列选项，所有的 100BASE-X 方案在节点之间使用两个物理链路，一个用于发送，另一个用于接收。100BASE-TX 使用屏蔽双绞线（Shielded Twisted Pair，STP）或高质量的 UTP（五类线或更高。有关三类线缆和五类线缆参见第 12 章的讨论）。100BASE-FX 使用光缆。

表 13-3　IEEE 802.3 100-Mbps 物理层介质备选项

	100BASE-TX		100BASE-FX	100BASE-T4
传输介质	2 对线，STP	2 对线，五类 UTP	2 根光纤	4 对线，三类、四类或五类 UTP
最大网段的长度	100m	100m	100m	100m
网络跨度	200m	200m	400m	200m

对于所有的 100BASE-T 选项，其拓扑结构与 10BASE-T 的拓扑结构相似，称为星形布线拓扑结构。

传统的以太 10Mbps 总线型 LAN 是半双工的：一个站点可发送一帧或接收一帧，但它不能同时做这两件事。对于全双工操作，一个站点可同时发送和接收。工作在全双工模式下的 100Mbps 以太网中，理论的传输率为 200Mbps。为了在全双工模式下工作，所连接的站点必须有全双工适配卡，这些全双工适配卡现在是交换以太环境中的标准设备。

全交换以太网络中的中心点是交换机。每个站点连接到一个交换机，交换机与站点之间的链路本质上是一个独立的冲突域。在全双工以太 LAN 中，通信流量可在站点和交换机之间同时在两个方向上传递，这本质上意味着没有冲突并且不再需要 CSMA/CD 算法。然而，在全双工以太 LAN 中使用相同的 802.3 MAC 帧格式，所连接的站点能继续执行 CSMA/CD 算法，即使没有检测到冲突。

13.3.2　千兆以太网

千兆以太网（Gigabit Ethernet，也称为吉比特以太网）的策略与快速以太网的策略相同。虽然定义了新的介质和传输规范，千兆以太网保留了其 10Mbps 和 100Mbps 前身的 CSMA/CD 协议和帧格式。该以太网与 100BASE-T 和 10BASE-T 都兼容，这样就保留了一条平滑的迁移路线。大部分的商务机构已转向使用 100BASE-T，许多机构已跳转到千兆以太网，这些千兆以太网至少作为他们 LAN 中的一部分。这些 LAN 将巨量的流量负载加到骨干网络中，这样进一步增加了千兆以太网和 10 千兆以太网的需求。

图 13-8 给出了千兆以太网的一个典型应用，其中一个 1/10Gbps LAN 交换机为中央服务器和高速工作组交换机提供骨干网络连接。每个工作组 LAN 交换机既支持 1Gbps 链路，以连接到骨干 LAN 的交换机并且支持高性能工作组服务器，又支持 10Mbps 链路，以支持高性能工作站、服务器和 100/1000Mpbs LAN 交换机。

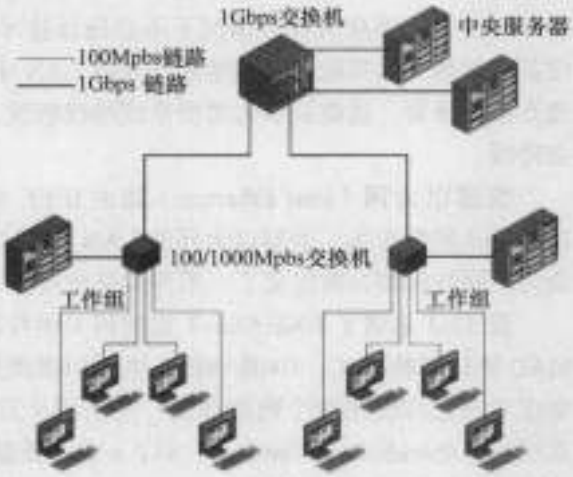


图 13-8　千兆以太网配置例子

现有的 IEEE 802.3 1Gbps 规范包括以下的物理层可选项（见图 13-9）：

1000BASE-LX：此长波长选项支持由 62.5μm 或 50μm 光纤组成的长度最长为 550m 的全双工链路，或者由 10μm 单模光纤组成的长度最长为 5km 的全双工链路。波长在 1270 ~ 1355nm 范围内。

1000BASE-SX：此短波长选项支持使用 62.5μm 多模光纤、长度最长为 275m 的全双工链路，或使用 50μm 多模光纤、长度最长为 550m 的全双工链路。波长在 770 ~ 860nm 范围内。

1000BASE-CX：此选项使用铜跨接线（一种特殊的 STP 线缆，长度不超过 25m），支持位于单个房间内或设备架上的设备之间的 1Gbps 链路。每条链路由一条工作在每个方向的独立 STP 组成。

1000BASE-T：此选项使用 4 对五类 UTP 来支持最高范围达 100m 的设备。

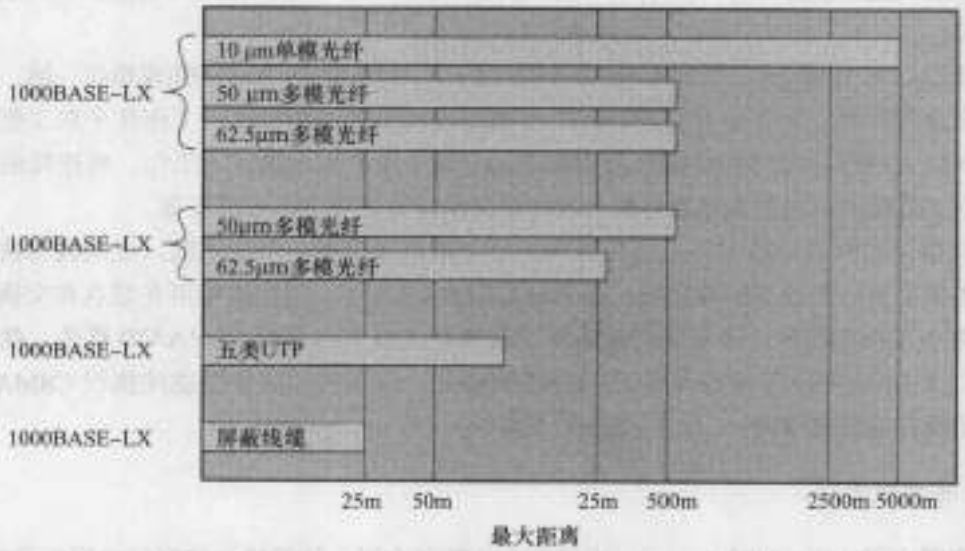


图 13-9　千兆以太介质可选项（对数标尺）

13.3.3　10Gbps 以太网

近几年来，10Gbps 以太交换机在 LAN 市场上取得较为瞩目的进展。对 10 千兆以太网重要的、强劲的需求是因特网和网间流量的增加。有很多因素导致了因特网与网间流量的爆炸

式增长：

- 网络连接数目的增长。
- 每个端站点连接速度的增长（例如，10Mpbs 的用户移至 100Mbps，模拟 56Kbps 用户移至 DSL 和电缆调制解调器）。
- 带宽密集型应用部署的增长，如高质量视频。
- 网站托管（Web hosting）和应用托管（application hosting）流量的增长。

最初，网络管理者利用 10Gbps 以太网在大容量交换机之间提供高速、本地骨干互连。随着带宽需求的增加，10Gbps 以太网将部署于整个网络中，并且包括数据中心、骨干网和整个校园范围的互连。该技术使得因特网服务提供商（Internet Service Provider，ISP）和网络服务提供商（Network Service Provider，NSP）能在并置排列的电信级交换机和路由器之间，以较低的成本创建非常高速的链路。

该技术也允许建立城域网（Metropolitan Area Network，MAN）和 WAN，以将校园或访问点（Points of Presence，PoP）之间地理位置松散的 LAN 互连起来。因此，以太网现在与 ATM 和其他广域传输 / 组网技术进行竞争。电信级以太网、城域以太网和广域以太网服务是企业网络中逐渐增长的通用组件。在大部分情况下，其中商务通信流量的基本形式是数据并且 TCP/IP 是传输的首选模式，10Gbps 以太网能为网络终端用户和服务提供商提供比 ATM 传输更实用的价值：

- 不需要实现以太网数据包和 ATM 信元之间既昂贵又消耗带宽的转换。网络端到端之间都是以太网。
- 利用 IP 和以太网的组合提供接近于 ATM 的服务质量和流量策略功能，以便用户和服务提供者能使用先进的流量工程技术。
- 10Gpbs 以太网中已定义出广泛的标准光纤接口（以支持不同的波长和链路距离），从而为 LAN、MAN 或 WAN 应用优化其操作和成本。

10Gbps 以太网最大链路距离范围为 300m – 40km。该链路使用各种各样的光纤物理介质，只工作在全双工模式。10Gbps 以太网中定义了 4 个物理层选项（见图 13-10）：

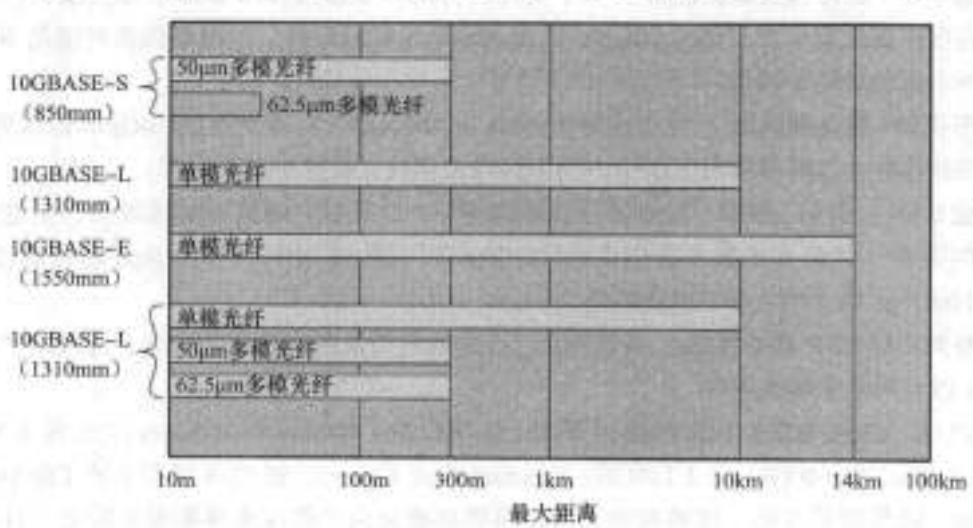


图 13-10　10Gbps 以太网距离选项（对数标尺）

- 10GBASE-S（短）：定义在多模光纤上的 850nm 传输。该介质能达到的最远距离为 300m。
- 10GBASE-L（长）：定义在单模光纤上的 1310nm 传输。该介质能达到的最远距离为 10km。
- 10GBASE-E（扩展）：定义在单模光纤上的 1550nm 传输。该介质能达到的最远距离为 40km。
- 10GBASE-LX4：定义在单模光纤或多模光纤上的 1310nm 传输。该介质能达到的最远距离为 10km。该介质使用波分复用（Wavelength-Division Multiplexing，WDM）技术将比特流复用在四个光波中。

13.3.4 100Gbps 以太网

以太网的应用比较广，并且是有线局域网络的首选技术。以太网在企业 LAN、宽带访问和数据中心网络中占主导地位，并在 MAN 甚至 WAN 的通信中变得越来越流行。并且以太网是首选的电信级电缆布线，以用于将无线技术（如 Wi-Fi 和 WiMax）桥接到本地以太网络。

以太网技术的流行归因于来自多个厂商的成本合理、可靠和互操作性好的网络产品。多年来，很多工业联盟已参与更快版本以太网的开发，包括快速以太网联盟（Fast Ethernet Alliance，100Mpbs）、千兆以太网联盟（Gigabit Ethernet Alliance）、10 千兆以太网联盟（10Gigabit Ethernet Alliance）、以太网联盟（Ethernet Alliance）以及通往 100G 联盟（Road to 100G Alliance）。作为以太网持续发展的证明，上述前三个联盟已不存在。以太网联盟正致力于提升以太网的开发，诸如以太网速度之类。通往 100G 联盟关注于 100Gbps 以太网的标准和技术的开发。

像联盟的演变所反映的那样，融合和统一通信的发展、数据中心的演变以及 VoIP、TVoIP、Web 2.0 应用的持续爆发，所有这些驱动了更快速以太网交换机的需求。[HUFF06] 列举了 100Gbps 以太网如下的市场驱动力：

数据中心 / 因特网媒体提供者：为了支持因特网多媒体内容和 Web 应用的增长，内容提供者一直在扩展数据中心，使得 10Gbps 以太网显示出其局限性。这些提供者可能是 100Gbps 以太网的大批量早期采用者。

都市视频 / 服务提供者：视频点播（video on demand）一直在促进 10Gpbs 以太网都市 / 核心网络的构建。这些提供者可能是 100Gbps 以太网的大批量中期采用者。

企业 LAN：音频 / 视频 / 数据融合的持续增长，以及统一通信的持续增长，促进了网络交换机的需求。然而大多数企业仍在依赖 1Gbps 以太网或 1Gbps 与 10Gbps 混合的以太网，在采用 100Gbps 以太网方面可能比较慢。

因特网交换 /ISP 核心路由：随着网络节点之间所交换的巨大通信流量，这些站点可能是 100Gbps 以太网的早期采用者。

2007 年，IEEE 802.3 工作组授权了 IEEE P802.3ba 40Gb/s 和 100Gb/s 以太网工作小组（the IEEE P802.3ba 40Gb/s and 100Gb/s Ethernet Task Force）。表 13-4 指明了该工作小组的物理层目标。就像所看见的，这些高速交换机将被标准化为工作在多种物理介质上，且距离为 1m – 40km。

表 13-4　40Gpbs 和 100Gbps 以太网的介质选项

	40Gbps	100Gbps
1m 背板	40GBASE-KR4	
10m 铜线	40GBASE-CR4	1000GBASE-CR10
100m 多模光纤	40GBASE-SR4	1000GBASE-SR10
10km 单模光纤	40GBASE-LR4	1000GBASE-LR4
40km 单模光纤		1000GBASE-ER4

命名法：
铜线：K= 背板；C= 电缆组件
光纤：S= 短距离（100m）；L= 长距离（10km）；E= 扩展长距离（40km）
编码方案：R=64B/66B 块编码
最后的数字：通道数目（铜线数目或光纤波长个数）

图 13-11 给出了一个 100Gbps 以太网的应用例子，该例子来自于 [NOWE07]。拥有大量刀锋服务器库的大型数据中心[⊖]，其趋势是每个服务器上部署 10Gpbs 的端口，以处理这服务器提供的大量多媒体数据流量。这样的安排加大了现场交换机的压力，这些交换机为互连大量的服务器所必需。这样就期望 100 千兆以太网速率来提供所需的带宽，以处理增长的流量负载。在数据中心内，需要 100 千兆以太网来部署在上行的交换链路中，就与为企业网络提供建筑之间、校园之间、MAN 和 WAN 的连接一样。

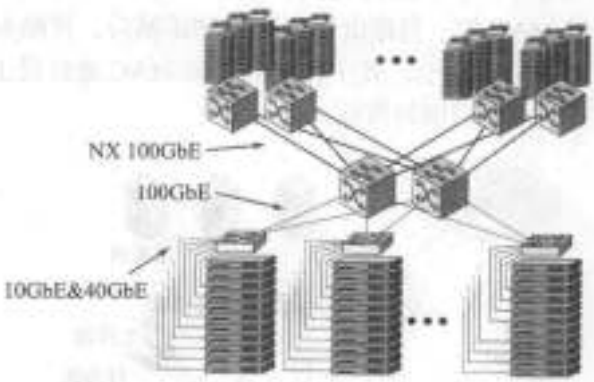


图 13-11　多刀锋服务器场所的 100Gbps 以太网配置例子

快速以太网、千兆以太网和 10Gbps 以太网的成功突出了在选择网络技术时网络管理考虑的重要性。随后研究的 ATM 以及光纤通道，由于其可扩展性和伸缩性，对高速骨干网来说是技术上的更优选择。然而，以太网可选项提供了与已安装 LAN、网络管理软件和应用的兼容。该兼容性使得 30 年的旧技术在今天快速发展的网络环境中生存下来。

13.4　虚拟局域网

图 13-12 显示了相对通用的层次式 LAN 配置类型。在该例中，LAN 中的设备组织成四组，每组由一个 LAN 交换机提供服务。其中三个较低层次的组可能对应于在物理上分离的不同部门，并且较高层次的组可能对应一个所有部门都使用的集中式服务器场或数据中心。

让我们考虑来自工作站 X 的单个 MAC 帧的传递。假定帧中的目的 MAC 地址是工作站 Y（见图 12-9）。该帧由工作站 X 传递至本地交换机，然后该交换机将该帧沿着链路传递至工作站 Y。如果工作站 X 传递目的地址为工作站 Z 或 W 的一帧，那么它的本地交换机将路由

⊖ 刀锋服务器是一种服务器结构，它在单个底架上安放了多个服务模块（即刀锋）。该服务器广泛用于数据中心，以节省空间和提升系统管理。不管是自立式还是机架式刀锋服务器，其底架均提供电源，并且每个刀锋有其自己的处理器、内存和硬盘。

该 MAC 帧，使其通过合适的交换机而传递到特定的目的端。所有这些例子都是单播寻址（unicast addressing），其中 MAC 帧的目的地址指明唯一的一个目的端。MAC 帧也可包含广播地址（broadcast address），在这种情况下目的 MAC 地址表明 LAN 中所有设备都应接收该帧的拷贝。因此，如果工作站 X 传递具有广播目的地址的一帧，图 13-12 中所有交换机上的设备都会收到一份该帧的副本。互相接收广播帧的所有设备的集合称为一个广播域（broadcast domain）。

在许多情况下，广播帧用于特定的目的，如网络管理或传递一些警告类型的信息，这些目的具有一定的本地意义。因此，在图 13-12 中，如果广播帧中的信息仅对特定的部门有用，那么 LAN 中其他端口和其他交换机上的传递容量就浪费了。

提高效率的一种简单方案是从物理上将 LAN 分为几个广播域，如图 13-13 所示。我们现有 4 个独立的 LAN，这些 LAN 通过一个路由器相连。在这种情况下，一个从工作站 X 传递给工作站 Z 的 IP 数据包经过如下处理：工作站 X 的 IP 层确定发往目的端的下一跳是经过路由器 V。该信息传递至工作站 X 的 MAC 层，由该层准备好一个目的 MAC 地址为路由器 V 的 MAC 帧。当路由器 V 接收到该帧后，将帧头剥离掉，确定出目的端，并且将该 IP 数据包封装到一帧中，其中该帧的目的 MAC 地址是工作站 Z。该帧然后发送到合适的以太网交换机，进行后继的传输。

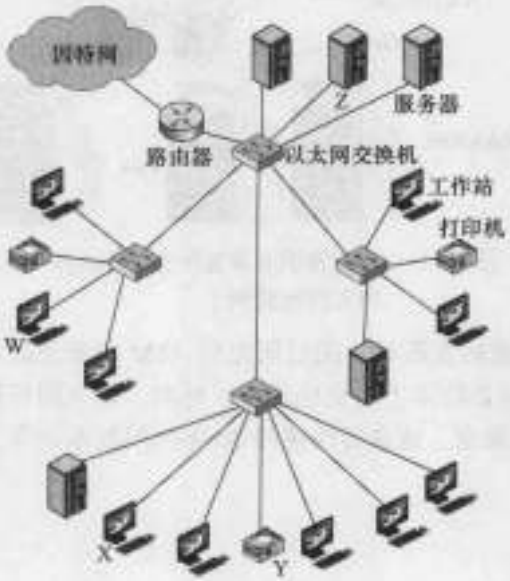


图 13-12　LAN 配置

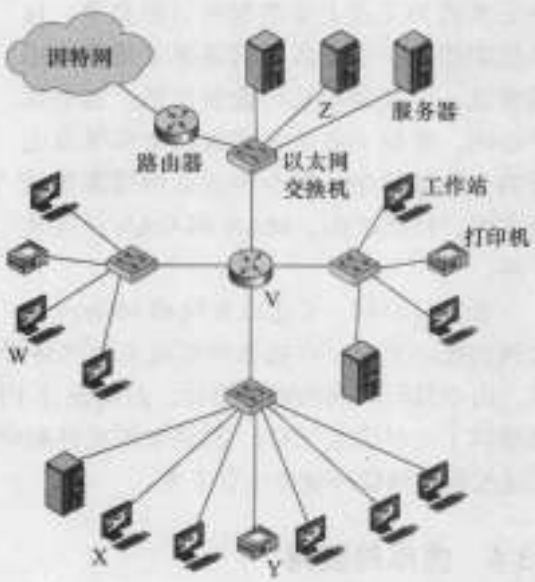


图 13-13　分割的 LAN

这种方案的不足是流量模式（traffic pattern）可能与设备的物理分布不一致。例如，一些部门的工作站可能与中心服务器中的一个服务器产生出大量的流量。另外，随着网络的扩展，需要更多的路由器来将用户隔离到广播域内，并且为广播域之间提供连接。由于路由器需要对数据包做更多的处理以确定目的端，并且将数据路由到合适的端节点，因此路由器比交换机引入更多的时延。

13.4.1　虚拟局域网的使用

一个更有效的可选方案是虚拟局域网（Virtual LAN，VLAN）的构建。从本质上来说，

VLAN 是 LAN 中的一个逻辑子组，它是通过软件创建而不是通过物理地移动和隔离设备来创建。它将用户站点和网络设备组合进单个的广播域，而不管这些站点和设备是连接到哪个物理的 LAN 网段，并且允许通信流量在具有双方利益的用户之间更有效地传递。VLAN 逻辑在 LAN 交换机中实现，并且在 MAC 层起作用。由于 VLAN 的目标是隔离 VLAN 中的通信流量，需要路由器来将一个 VLAN 连接到另外一个 VLAN。路由器可实现为一个单独设备，这样从一个 VLAN 到另一个 VLAN 的流量被定向到一个路由器上，或者将路由逻辑作为 LAN 交换机中的一部分实现，如图 13-14 所示。

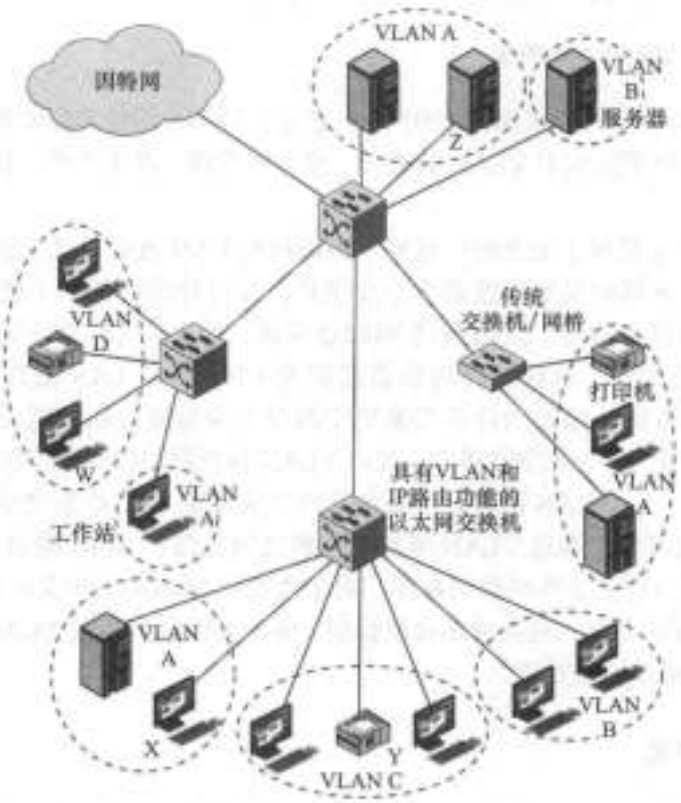


图 13-14　VLAN 配置

VLAN 提供这样的功能：任何机构单元可物理上分布于整个公司内，而仍能维持其组身份（group identity）。例如，全体会计人员可位于购物层、研发中心和现金支出办公室，然而同时他们都位于同一虚拟网络内，并且仅在他们之间共享通信流量。

在图 13-14 中，定义了四个 VLAN。从工作站 X 到服务器 Z 的传递在同一个 VLAN 内，因此它在 MAC 层有效地进行交换。来自工作站 X 的广播 MAC 帧被传递到同一个 VLAN 中所有端口连接着的所有设备。但是从工作站 X 到打印机 Y 的传输从一个 VLAN 传递到另一个 VLAN。相应地，需要 IP 层的路由逻辑来将 IP 数据包从工作站 X 传送到打印机 Y。在图 13-14 中，路由逻辑集成到交换机中，因此由交换机决定所输入 MAC 帧是否路由到位于相同 VLAN 中其他设备。如果不是，交换机在 IP 层路由所封装的 IP 数据包。

该图中也包括了一个传统的交换机，该交换机中没有实现 VLAN 软件。在这种情况下，该传统设备的所有端系统必须属于相同的 VLAN，因为该传统交换机不能识别出由不同 VLAN 区分的通信流量。

13.4.2　表明 VLAN 成员身份

当网络通信流量从另外一个交换机到达时，交换机必须有一种方法来理解 VLAN 的成员身份（即哪个站点属于哪个 VLAN），否则 VLAN 将受限于单个交换机。一种可能的方法是人工配置信息或利用一些类型的网络管理信令协议，使得交换机能将输入的帧与相应的 VLAN 关联起来。

更通用的一种做法是帧标签（frame tagging），其中通常是将一头部添加到跨交换机流量中的每一帧中，来唯一标明特定的 MAC 层帧属于哪个 VLAN。IEEE 802 委员会已为帧标签颁布标准，即 IEEE 802.1Q，该标准我们在下节中描述。

13.4.3　IEEE 802.1Q VLAN 标准

IEEE 802.1Q 标准（最后更新在 2005 年）定义了 VLAN 网桥和路由器的操作，许可了在桥接 / 交换的 LAN 体系结构中 VLAN 的定义、操作和管理。在本节中，我们关注将该标准应用于 802.3 LAN 中。

要记得 VLAN 是管理上配置的广播域，由连接到 LAN 的端系统子集组成。VLAN 不局限于一个交换机，它可扩展到互连的多个交换机。在这种情况下，交换机之间的通信流量必须指明其 VLAN 成员身份。这可利用 802.1Q 实现，插入一个表示 VLAN 标识符（VLAN identifier，VID）的标签，该标识符的取值范围为 1 到 4094。LAN 配置中为每个 VLAN 分配一个全局唯一的 VID。通过为许多交换机中的多个端系统分配相同的 VID，一个或多个 VLAN 广播域可扩展到一个大型网络中。表示 VLAN 标识符的标签也包含有优先级。

图 13-14 展示了一个 LAN 配置，其中包括三个实现了 802.1Q 的交换机和一个没有实现 802.1Q 的交换机或网桥。通过 VLAN 感知交换机之间链路的 MAC 帧包含 802.1Q 标签，该标签在该帧路由到一传统交换机前剥离掉。对于连接到 VLAN 感知交换机上的端系统而言，MAC 帧可根据实现的不同，包含或不含该标签。重点是该标签用于 VLAN 感知交换机之间，以便能实现合适的路由和帧处理。

13.5　以太网供电

以太网供电（Power over Ethernet，PoE）是以太网的另一种形式，这种形式的网络越来越多地在企业网络中见到。就如名字所表示的那样，PoE 使得利用以太电缆配电和传递数据成为可能。PoE 的 IEEE 标准中，要求为低功率电平配备三类线，为高功率电平配备五类线或更高类型的线。PoE 使用以太电缆中的两对或更多对的双绞线对来配电，其他的双绞线对用来传递数据。PoE 网络的基本电力供应由 POE 交换机和 DC 电池阵列提供。

PoE 为网络设计者在部署 LAN 设备时提供了更多的灵活性。在许多情况下，PoE 减少了将设备布置到离 AC 电力源较近位置的需求。如图 13-15 所示，PoE 能用于给 VoIP 电话、Wi-Fi 接入点和 LCD 监视器供电。PoE



图 13-15　以太网供电（PoE）

也能用来给如下的设备供电：IP 监视摄像头、Web 摄像头、工业设备（如传感器、控制器和测量仪）、照明控制器、远程网络交换机、接入控制设备（如无钥匙进入和对讲机系统，keyless entry and intercom system）和远程销售点（Point Of Sale，POS）亭。工业评论员预测 PoE 将更多地用来给连接到网络的工作站的主板供电。

PoE 有许多优点。例如，在 AC 电源比较昂贵、不可用或不方便给网络设备供电的情况下，可以用 PoE。在这种情况下，虽然也可使用 USB 作为一个选择，通常 PoE 是比 USB 或 AC 电线更优的一种选择，因为：

- 它可部署在五类 UTP 之上，这比使用 USB 放大器或 AC 电线要便宜。
- 千兆连接是可能的，这比 USB 2.0 和 AC 电源线的网络能力要快，并且 10Gbps PoE 标准正在开发之中。
- 在全球具有多个分部的公司可在任何地方部署 PoE，而不必考虑不同地点处 AC 功率电平、插头、插座或可信度的不同。它也可部署在大楼内，而不必担心 AC 电缆建筑规范。

像其他版本的以太网一样，PoE 标准也在不停地发展之中。初始的 IEEE 802.3af-2003 PoE 标准能给每个设备提供高至 15.4W 的直流功率（或最低提供 44V DC 和 350mA）。由于一些功率在线缆中消耗掉了，该标准仅保证 12.95W 功率给每个受驱动的设备。

自初始的 PoE 标准发布后，在高功率 PoE 系统和低功率 PoE 系统两方面的工作都在继续。IEEE 802.3af 工作组正致力于节能的以太网标准，该标准期望比初始 PoE 标准要节约 60% 的电力。另一个委员会正开发传送更多功率给设备的 PoE 标准。IEEE 802.3at-2009 PoE 标准提供高达 25.5W 的功率，该标准也称为 PoE+。一个 60W 的 PoE 标准也在研发中。

PoE 的功率电平越高，越可能利用其来给工作站主板供电。然而，随着越多的功率通过以太电缆配电，在结构化布线方案中需要有合适的设施。在 PoE 中利用电缆束有时会具有火灾隐患，因为将电力从 PoE 交换机输送到连接到网络上的设备时会产生热量。虽然这不能被排除，也没有很强的支持证据。然而在高功率的 PoE 中，更明智的做法是将电缆槽和电缆管道中的电缆隔离开，以实现散热。使用六类线、加强六类线和七类线也是比较明智的，因为这些线缆的散热性比五类线好。在 PoE 电缆束内增加温度感知热电偶，也是一种比较明智的体系结构方面的投资。

应用注解

以太网组网

过去的 20 年间出现了许多局域网（LAN）协议，但它们中的大部分现在已不再使用。目前部署的大部分网络都是基于快速以太网构建，如 100/1000BASE-TX、100BASE-FX、千兆甚至 10Gpbs 以太网。现如今以及在可见的未来，以太网是主导性的 LAN 协议。以太网甚至开始打入最后一公里的公共电话（common carrier）市场。以太网的强大之处在于向下兼容、公司支持和简单。组建一个以太网就像从盒子里拿出设备并将其插入那样简单。此外，通用的以太网组件变得越来越便宜。而相反的是，维护或安装任何不太流行的传统系统则要昂贵得多。

虽然以太网的后台（under the hood）操作提供了好的工程化理解，以太网还有一些很实际的方面，理解这些方面有利于从网络中获得更多。一个组织必须分析其通信需求，

并且决定现在和未来适用所需的带宽为多少、在该网络体系结构上运行哪些程序、将要花费多少资金。

多年来，大部分销售的组网设备具有 10/100/100Mbps 以太网端口。这意味着设备端口和计算机中的网络接口卡（Network Interface Card，NIC）会自动感知网络环境，并且决定什么速率是可用的。然而，计算机的总线速率和操作系统的延迟为网络运行于千兆（也称为吉比特）速率设置了障碍。此外，没有那么多的计算机需要发送如此多的数据。对于标准计算机来说，100Mpbs 或 100/1000Mpbs 接口卡通常就足够了，这种情况在不久的将来也不会改变。即使没有千兆容量，网络接口卡和设备能设置成全双工操作模式，这样双向吞吐量提高至 200Mbps。

对于新安装网络或计划的网络升级，购买千兆设备可能比较合理，这在大数据增长情况下特别正确，而大数据的增长是许多商务网络能预料的。然而，企业级设备每个端口的成本仍然是比较贵的，并且对于许多应用来说，高速设备的代价除在特定场合外难以证明其合理性。吉比特、10Gbps 甚至 40Gbps 以太网络特别适合如布线间之间的光纤骨干网连接、异地之间的网络连接以及重负载服务。当然光纤也加大了任何实施中的成本。

虽然实际上没有新网络将安装少于 100Mbps 的速率，一些老的网络可能运行在更低的速率上并且使用混合的技术。在该环境下使用的任何新购买设备必须是 10/100/1000Mbps 模式，以保证旧系统与任何新购买设备之间的兼容。然而，新设备只能按布线允许的速率发送数据。老的五类布线不能达到吉比特速率。即使是增强五类布线，依据其覆盖距离，也可能不支持更高的速率。问题是，除了替换设备需要花费某些固定成本外，当需要替换电缆设备时就极大地提高了成本。

集线器是另一个终将消失的物品。在早期的以太网络中，网桥和交换机每个端口的成本使得转换到这些设备是非常昂贵的。然而在过去的几年里，这些部件的成本就降到不需要解释的购买点了。交换机提供的高级特性使得其更容易管理和安全化网络。例如，许多交换机内部集成了统计功能并支持虚拟局域网（VLAN）。此外，交换机还提供了防火墙的过滤功能和错误隔离功能，作为它们标准操作的一部分。

对于任何新的网络安装，购买单上一定要包括最好质量的 UTP 布线、10/100/1000Mpbs 全双工操作的网络接口卡、具有 10/100/1000Mpbs 全双工操作端口的交换机。当升级已有的旧系统时，网络管理员必须遵循如下的指导原则：要明白具有最优性能的设备必须与适当的布线体系相匹配。

13.6　总结

高速以太网已是企业信息系统（corporate information system）中的关键元素。这样的 LAN 不仅被用来提供连接部门 LAN 的内部骨干网，也能为基于图形的客户 / 服务程序和内网应用程序提供高性能需求的支持。

对于大多数应用而言，快速以太网和吉比特以太网技术主导了企业高速以太网的选择。这些系统为管理者提供了最低的风险和代价，其原因包括：与已安装的大型以太网兼容、基本技术的成熟、与已有网络管理和配置软件兼容。

在大部分情况下，一个机构将有多个 LAN 需要相互连接。满足该需求的最简单方法是使

用网桥或第二层交换机。然而在企业网络中，也可能使用第三层交换机来保证性能。

以太网供电（PoE）使用得越来越多。在 PoE 下，同一条以太电缆既可用来传递数据，也可用来对所连接的设备供电。

13.7　关键术语、复习题和练习题

关键术语

bridge（网桥）
cut-through switch（直通交换机）
Ethernet（以太网）
Fast Ethernet（快速以太网）
Fibre Channel（光纤通道）
frame（帧）
Frame Check Sequence（FCS，帧校验序列）
hub（集线器）
Power over Ethernet（PoE，以太网供电）
store-and-forward switch（存储 – 转发交换机）
switch（交换机）

复习题

13.1　对于商务数据通信专业的学生而言，为什么对以太网有基本的了解很重要？
13.2　解释为什么 100Mbps、1Gbps 和 10Gbps 的数据率在商务网络中越来越普遍？
13.3　什么是 CSMA/CD？它是怎样工作的？
13.4　网络的功能是什么？
13.5　集线器和第二层交换机之间有什么区别？
13.6　存储转发交换机和直通交换机之间有什么区别？
13.7　网桥和交换机有什么区别？
13.8　第二层交换机和第三层交换机有什么区别？
13.9　快速以太网的传输介质选项有哪些？
13.10　千兆以太网的传输介质选项有哪些？
13.11　10 千兆以太网的传输介质选项有哪些？
13.12　虚拟局域网（VLAN）有什么特征？
13.13　什么是以太网供电（PoE）？
13.14　为什么企业网络中 PoE 变得越来越流行？

练习题

13.1　确定出你计算机上安装的网络接口卡类型。描述该接口卡的主要性能，包括它的速率、第二层协议、用来连接到通信媒体的介质类型。
13.2　利用数据包抓取软件（如 Wireshark）和一些内置的程序（如 ping、nslookup、ipconfig），发现和现实如下信息的屏幕条：
- 你计算机的 Mac 地址（使用 ipconfig 和 ifconfig）。
- 你所抓取帧中的 IP 协议代码值，该值可在以太网帧中的控制字段找到。

13.3　使用 Wireshark 来抓取你计算机发出的帧（提示：在开始抓取后，打开浏览器并访问一些 Web 页面）。研究所抓取帧中的一帧或几帧，展示其中的源 MAC 地址和目的 MAC 地址。所获得的你的 MAC 地址与问题 13.2a 中发现的其中一个地址相匹配吗？

13.4 现在出现了一种争论，即是 ATM 还是千兆以太网是高速组网解决方案的最好选择。在因特网上做一些研究，比较这两种技术，并形成 500 – 1000 个字的建议书来列举每种技术的特定应用场景，说明在该场景下该技术是企业的优选方案。

13.5 解释 IEEE 802.3 帧中将 FCS 字段放在帧尾而不是帧首的好处。

13.6 令牌环（Token-Ring）是以太网中的一种可选（大部分时候被认为是过时的）技术。在因特网上做一些令牌环的研究，确定出在如今网络中很少用令牌环的主要原因。将你的发现总结形成一篇 500 – 750 的短文或者 5 – 8 页的 PowerPoint 报告。

13.7 在 YouTube 上查找并观看一些解释 CSMA/CD 怎样工作的视频。列出你认为在解释 CSMA/CD 方面做得最好的三个视频的 URL。如果你仅能选择其中的一个来推荐给其他商务数据通信专业的学生，你将选择哪一个？为什么？

13.8 在 YouTube 上查找并观看一些比较集线器和交换机的视频。列出你认为在解释集线器和交换机之间区别方面做得最好的三个视频的 URL。如果你仅能选择其中的一个来推荐给其他商务数据通信专业的学生，你将选择哪一个？为什么？

13.9 在因特网上做一些比较存储转发交换机和直通交换机的优点和使用方面的研究。列出一些场合，其中存储转发交换机是比直通交换机更好的选择。列出直通交换机是更好选择的场合。将你的研究结果总结成 500 – 750 字的短文或者 5 – 8 页的 PowerPoint 报告。

13.10 在因特网上做一些企业怎样使用 VLAN 方面的研究。确定出企业中使用 VLAN 的优势，并列出一些企业怎样从创建和使用 VLAN 获利的特例。将你的研究结果总结成 500 – 750 字的短文或者 5 – 8 页的 PowerPoint 报告。

13.11 在因特网上做一些研究，以找到至少五张以太网供电（PoE）图像，这样的图像要能很好地解释 PoE 的能力和部署基本要素。形成一个有关 PoE 的 8 – 12 页 PowerPoint 报告，该报告需提供有关 PoE 如下方面的清晰解释：PoE 是什么，为什么要部署 PoE，PoE 是怎样使用的。该报告中还要包含你在做 PoE 研究时查找到的用作说明的图像。

13.12 在因特网上做一些有关企业网内以太网供电（PoE）中结构化布线的应用。将你的发现总结成 500 – 1000 字的短文或者 8 – 12 页的 Powerpoint 报告。

13.13 在因特网上研究家庭或小型企业网络中可替代 PoE 的电力线组网方式。识别电力线网络的主要特征。将你的发现点结成 50 – 1000 字的短文或者 8 – 12 页的 Powerpoint 报告。

无线局域网

学习目标

通过本章的学习，读者应该能够：

- 讨论无线局域网的重要性。
- 描述无线局域布线的多种方法。
- 解释 IEEE 802.11 无线局域网体系结构的关键元素。
- 描述 IEEE 802.11 提供的服务。
- 讨论 IEEE 802.11 协议结构中每层提供的功能。

无线局域网已成为局域网市场的重要组成部分。机构正在使用无线局域网作为传统有线局域网的重要补充，来满足其对于移动性、迁移、自组织组网以及覆盖难以布线区域的需求。

该章提供无线局域网的综述。我们首先概述使用无线局域网的动机，总结目前使用的各种方法。然后讨论使用最为广泛的无线局域网方案，即 IEEE 802.11，也称为 Wi-Fi。附录 H 概述另一种流行的方案，即蓝牙。

14.1 概述

顾名思义，无线局域网是一种使用无线传输介质的网络。

14.1.1 无线 LAN 应用

像有线 LAN（如以太网）一样，无线局域网（Wireless LAN，WLAN）提供的也是有限地理位置范围内的连接。WLAN 具有有线 LAN 无法提供的一个重要属性是移动性，即在保持连接的同时能四处移动。对于这样的一个环境，其中员工需要移动但又必须与局域网保持长时连接，WLAN 就变得必不可少。一个好的例子是：当医院里的医生和护士在医院里移动时，他们需要随时访问病人的信息、医院记录和其他医疗信息。

WLAN 也提供户外连接，如在许多场合可以看到的、以 Wi-Fi 热点（hot spot）形式允许员工在办公楼附近也能保持安全的网络连接，或者如在市里看到的、以公开接入热点形式提供非安全的网络连接。

作为有线 LAN 的补充，WLAN 在一些场合非常有用，如在有线连接困难、成本高或由于介入了公共区域不可能用有线连接时，就可用 WLAN 来连接相邻大楼内的有线 LAN。

图 14-1 给出了一个简单的 WLAN 配置，该配置在许多环境中都具有代表性。其中，存在一个骨干有线 LAN（如以太网）来支持服务器、工作站以及用来与其他网络相连的一个或多个桥或路由器。此外还有一个控制模块（Control Module，CM），以 WLAN 接口的形式工作。该控制模块包括桥或路由器的功能，以将 WLAN 连接到骨干网。该模块包括某种接入控制逻辑，如轮询或令牌传递方案，来管理端系统的接入。注意一些端系统是标准设备，

如工作站或服务器。用于控制有线 LAN 大量站点的集线器（hub）或其他用户模块（User Module，UM）也可以是 WLAN 配置的一部分。

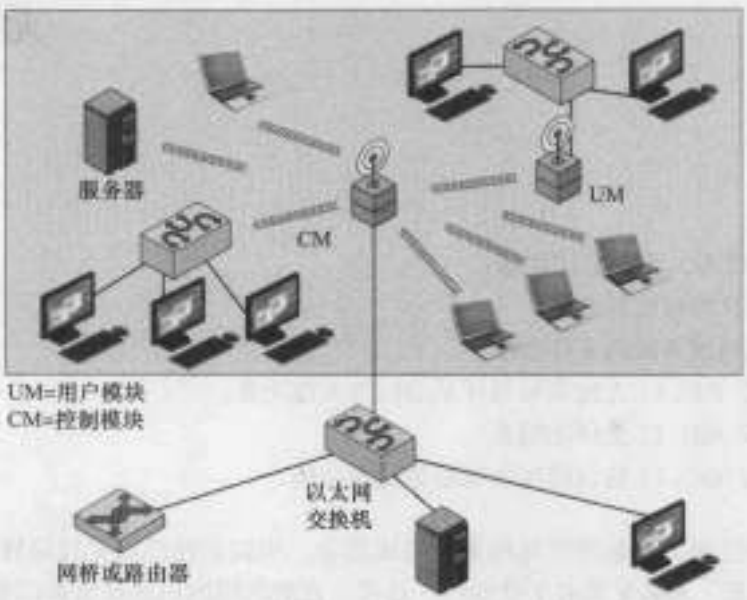


图 14-1　单蜂窝无线 LAN 配置的实例

图 14-1 的配置可称为单蜂窝 WLAN，所有的无线端系统在单个控制模块的范围内。图 14-2 所建议的另一种配置是一个多蜂窝 WLAN。在这种情况下，存在许多控制模块，这些模块用有线 LAN 互连起来。每个控制模块在其传输范围内支持多个无线端系统。例如，红外 LAN 的传输限制在单个室内，因此在需要无线网络支持的办公大楼内，每个房间都要一个蜂窝。

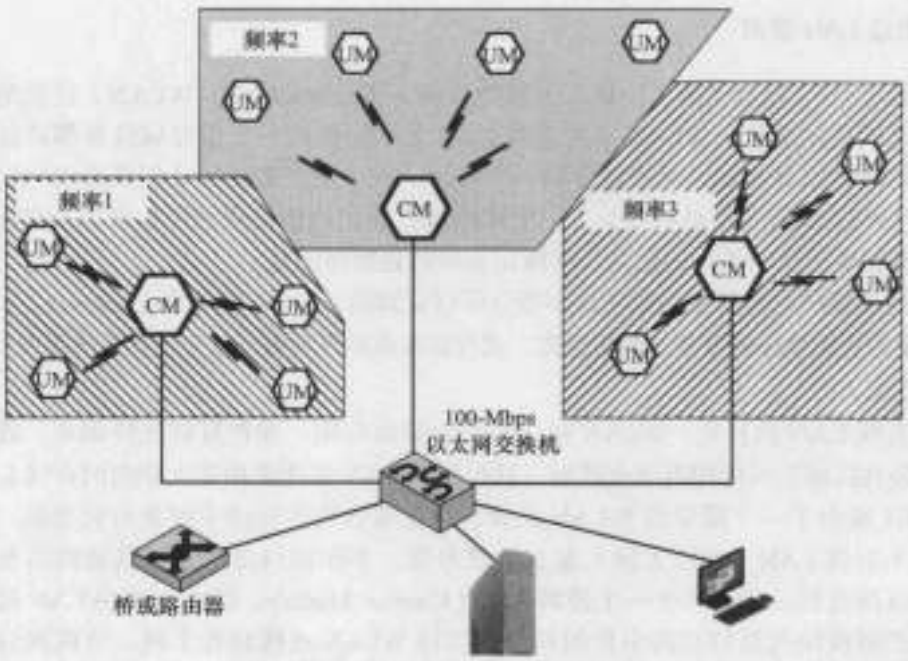


图 14-2　多蜂窝无线 LAN 配置实例

14.1.2　无线 LAN 需求

WLAN 必须满足与任何一个 LAN 相同的需求，包括高容量、短距离覆盖、相关站点间的完全连接以及广播功能。此外，WLAN 对环境有大量的特定需求，其中最重要的需求如下：

- **吞吐量**（throughput）：为了使容量最大化，介质接入控制协议（MAC）应尽可能高效地利用无线介质。
- **节点数**（number of nodes）：WLAN 可能需要在多个蜂窝内支持成百个节点。
- **与骨干 LAN 的连接**（connection to backbone LAN）：在大多数情况下，WLAN 需要与有线骨干 LAN 中的站点互连。对于 WLAN 的基础设施而言，很容易使用控制模块来连接两种类型的 LAN。对于移动用户和无线自组织网（ad hoc wireless network）而言，也需要该功能。
- **服务区域**（service area）：WLAN 的典型覆盖范围为 100 ~ 300m。
- **电池功率消耗**（battery power consumption）：当使用无线网卡时，移动工作人员使用由供电时间长的电池供电的工作站。这就意味着，如果 MAC 协议要求移动节点不间断地监视接入点或不停地与基站频繁握手，那么这样的 MAC 协议是不适当的。在使用网络时，典型的 WLAN 实现应具有减少功率消耗的特点，如提供睡眠模式。
- **传输的鲁棒性和安全性**（transmission robustness and security）：除非被正确设计，WLAN 可能易于被干扰和窃听。WLAN 的设计必须允许即使在噪声环境下，仍有可靠传输并应提供一些安全级别来避免窃听。
- **配置的网络操作**（collocated network operation）：随着 WLAN 变得更为普及，很可能在同一个区域内存在两个或多个 WLAN 的操作，或者在某个区域内可能出现 LAN 之间的干扰。这样的干扰可能阻碍 MAC 算法的正常操作，以及可能允许非授权接入某特定 LAN。
- **免许可证操作**（license-free operation）：用于更愿意购买和操作不需要对该 LAN 所用频段给予安全许可的 WLAN 产品。
- **跨区切换 / 漫游**（handoff/roaming）：WLAN 中所用的 MAC 协议应能使移动站点从一个蜂窝移动至另一个蜂窝。
- **动态配置**（dynamic configuration）：LAN 的 MAC 寻址和网络管理方面应允许动态和自动地添加、删除，以及在不影响其他用户的情况下重定位终端系统。

14.1.3　无线 LAN 技术

总体上，WLAN 根据所用的传输技术进行分类。当前所有的 WLAN 产品分别属于以下几类：

- **扩频 LAN**（spread spectrum LAN）：这种类型的 LAN 利用扩频传输技术。在大多数情况下，这些 LAN 工作在 ISM（industrial，scientific，and medical）2.4GHz 微波频段上，因此在美国，这些频段的使用不需要联邦通信委员会（Federal Communication Commission，FCC）的许可。
- **OFDM LAN**：对于高速网络，称为正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）的技术比扩频技术优越，并且采用这种技术的产品现在非常普遍。这些 LAN 典型工作在或者 2.4GHz 的频带或者 5GHz 的频带。
- **红外**（infrared，IR）**LAN**：由于红外线不能穿透不透光的墙，IR LAN 的单个蜂窝限制在单个房间内。

14.2　Wi-Fi 体系结构和服务

1990 年，IEEE 802 委员会组建了一个新的工作组 IEEE 802.11，特别致力于 WLAN，来研发 MAC 协议和物理介质规格说明。从那时起，各种频率和数据率的 WLAN 需求呈爆发式增长。为了与需求保持同步，IEEE 802.11 工作组发布了永远可扩充的标准列表（见表 14-1）。表 14-2 简单定义了 IEEE 802.11 标准中使用的术语。

对于任何组网标准而言，需要考虑的是不同厂商的产品是否能成功互操作。为了满足这方面的考虑，1999 年建立了一个工业联盟，即无线以太网兼容联盟（Wireless Ethernet Compatibility Alliance，WECA）。这个机构后来重命名为 Wi-Fi（Wireless Fidelity）联盟，创建了一个测试套件来验证 802.11 产品之间的互操作。用于经测试产品的术语为 Wi-Fi。Wi-Fi 联盟涉及 WLAN 的广大市场区域范围，包括企业网络、家庭网络和热点网络。

表 14-1　主要的 IEEE 802.11 工作组

标　准	范　围
IEEE 802.11a	物理层：5GHz OFDM，数据率为 6Mbps 到 54Mbps
IEEE 802.11b	物理层：2.4GHz DSSS，数据率为 5.5Mbps 到 11Mbps
IEEE 802.11c	802.11 MAC 层上的桥接操作
IEEE 802.11d	物理层：将 802.11 WLAN 应用到新管理域（如国家）的扩展操作
IEEE 802.11e	MAC 层：增强以提高服务质量，以及增强安全机制
IEEE 802.11g	物理层：扩充 802.11b 的数据率，使其大于 20Mpbs
IEEE 802.11i	MAC 层：增强安全和认证机制
IEEE 802.11n	物理层 /MAC 层：增强以获得更高的吞吐量
IEEE 802.11T	802.11 无线性能评估的操作规程建议
IEEE 802.11ac	物理层 /MAC 层：增强以支持 5GHz 频带范围且数据率为 0.5Gbps 到 1Gbps
IEEE 802.11ad	物理层 /MAC 层：增强以支持 60GHz 频带范围且数据率大于等于 1Gbps

表 14-2　IEEE 802.11 术语

接入点（AP）	任何具有站点功能并通过无线介质（用于联合站点）提供分布式系统接入的实体
基本服务集（BSS）	由单个协调功能控制的站点集合
协调功能	为逻辑功能，用于决定工作在 BSS 中的站点什么时候允许传输，以及什么时候能接收 PDU
分布式系统（DS）	用于将 BSS 集合和集成 LAN 互连的系统，用来创建 ESS
扩展服务集（ESS）	由一个或多个互连的 BSS 和集成 LAN 组成的集合。对于与这些 BSS 中任何一个相连的任何站点的 LLC 层而言，该集合就像是一个单独的 BSS
MAC 协议数据单元（MPDU）	使用物理层服务的两个对等 MAC 实体间的数据交换单元
MAC 服务数据单元（MSDU）	在 MAC 用户之间以单元形式传递的信息
站点	任何包含有 IEEE 802.11 MAC 层和物理层协议的设备

14.2.1　IEEE 802.11 体系结构

图 14-3 描述了 802.11 工作组开发的模型。WLAN 的最小构成单元是**基本服务集**（Basic Service Set，BSS），它由一些执行相同 MAC 协议和竞争接入相同共享无线介质的站点组成。一个 BSS 要么是孤立的，要么是通过一个**接入点**（Access Point，AP）与骨干**分布式系**

续（Distribution System，DS）相连。接入点的功能像网桥和中继点（relay point）。在 BSS 中，客户站点之间不直接通信。相反地，如果 BSS 中的一个站点想与位于同一 BSS 中其他站点通信，MAC 帧首先从产生站发送到 AP，然后再由 AP 传递到目的站点。类似地，如果 MAC 帧要从一 BSS 个中的站点传递到远方的站点，则该帧首先由本地站点发送至 AP，然后由沿途 DS 中的 AP 中继到目的站点。BSS 通常对应于文献中的蜂窝。DS 可以是一个交换机、一个有线网络或者一个无线网络。



图 14-3　WLAN 扩展服务集实例

如果一个 BSS 中的所有站点都是移动站点，并且与其他 BSS 没有连接，那么该 BSS 称为**独立 BSS**（Independent BSS，IBSS）。IBSS 是一个典型的自组织网络，在 IBSS 中所有的站点之间直接通信，不涉及任何 AP。

图 14-3 显示了最简单的配置，这里的每个站点属于一个单独的 BSS。就是说，每个站点所在的无线区域与同一个 BSS 中其他站点所在的无线区域相同。两个 BSS 可能在地理位置上有重叠，这样一个单独站点可能参与的 BSS 不止一个。更进一步地，一个站点与一 BSS 之间的关联关系是动态变化的，站点可能关闭、进入 BSS 区域和从 BSS 区域移出。

扩展服务集（Extended Service Set，ESS）由两个或多个通过分布式系统互连的 BSS 组成。分布式系统是一个典型的有线骨干 LAN，但可以是任意的通信网络。对于逻辑链路控制层 LLC 而言，扩展服务集看起来像一个单独的逻辑 LAN。

图 14-3 展示了将 AP 作为站点的一部分实现。AP 在站点中是逻辑存在的，该站点除了本身作为站点的功能之外，还通过提供 DS 服务提供对 DS 的接入。为了将 IEEE 802.11 结构与传统的有线 LAN 相集成，使用了一个**入口**（portal）。入口逻辑是在一个诸如网桥或路由器的设备中实现，该设备是有线 LAN 中的一部分并且连接到 DS。

14.2.2 IEEE 802.11 服务

IEEE 802.11 定义了需由 WLAN 提供的九种服务，以获取与有线 LAN 的固有功能相等价的功能。以下是这些服务的两种分类方法。

1）服务提供者可以是站点或者是分布式系统。每个 802.11 站点，包括 AP 站点，都要实现站点服务。分布式服务在 BSS 之间提供，这些服务可实现在 AP 或其他与分布式系统相连的专用设备中。

2）这些服务中的三种服务用来控制 IEEE 802.11 LAN 的接入和机密性，其他的六种服务用来支持在站点间发送 MAC 服务数据单元（MAC service data unit，MSDU）。MSDU 是由 MAC 用户下传到 MAC 层的数据块，这通常是一个 LLC PDU。如果 MSDU 过大而无法在一个单独的 MAC 帧发送，它就可能被分片，在一组 MAC 帧中发送。

在 IEEE 802.11 文档之后，下面按一种为阐明 IEEE 802.11 ESS 网络操作而设计的顺序来讨论这些服务。作为基本服务的 **MSDU 发送**（MSDU delivery）已经被提到过了。与安全相关的服务将在 14.3 节介绍，并在第 19 章讨论。

1. DS 中的消息分发

DS 中消息分发所涉及的两种服务是分发和集成。当帧必须由一个 BSS 中的站点穿过 DS 到达另一个 BSS 中的站点时，**分发**（distribution）就是用来在站点间交换帧的基本服务。例如，假定有一帧要从图 14-3 的站点 2（STA2）发送到 STA7，该帧由 STA2 送至作为此 BSS AP 的 STA1，AP 将帧传递至 DS，DS 的任务是将帧传给与目标 BSS 中 STA5 相关联的 AP。STA5 接收到该帧并将它转发给 STA7。关于消息如何通过 DS 传送则不在 IEEE 802.11 标准的范围内。

如果正在通信的两个站点在同一个 BSS 中，那么分发服务逻辑上要通过那个 BSS 的单个 AP。

集成（integration）服务使得 IEEE 802.11 LAN 中站点与集成 IEEE 802.x LAN 中站点之间的数据传输成为可能。术语集成（integrated）指的是物理上连接到 DS 的有线 LAN，而它的站点可能在逻辑上通过集成服务与一个 IEEE 802.11 LAN 相连。集成服务负责数据交换所需要的任意地址转换和介质转换逻辑。

2. 与关联相关的服务

MAC 层的主要目的是在 MAC 实体间转发 MSDU，此目标由分发服务实现。该服务为实现功能需要与关联相关的服务提供关于 ESS 中的站点信息。在分发服务向某个站点传递或从某个站点接收数据之前，该站点必须是关联的（associated）。在关注关联这个概念之前，我们需要描述移动性这个概念。标准定义了基于移动性的三种变动类型：

- **无变动**（no transition）：此类型的站点要么是固定的，要么仅在单个 BSS 通信站点的直接通信范围以内移动。
- **BSS 变动**（BSS transition）：被定义为站点从一个 BSS 移动到相同 ESS 的另一个 BSS。在这种情况下，把数据传送到站点需要寻址能力以认出站点的新位置。
- **ESS 变动**（ESS transition）：被定义为从一个 ESS 的 BSS 移动到另一个 ESS 的 BSS。仅在站点能移动时，才支持这种情况。此时，不能保证对 802.11 所支持上层连接的维护。实际上，很可能发生服务中止。

为了在一个 DS 中传送消息，分发服务需要知道目的站点设置在哪里。确切地说，为了让消息到达目的站点，DS 需要知道报文要被传到 AP 的标识。为了满足这种需要，一个站点必须维持与它当前 BSS 的 AP 之间的关联。与这需求相关的三种服务有：

- **关联**（association）：在一个站点和 AP 之间建立一条初始关联。在站点能在 WLAN 上发送或接收帧之前，必须知道它的标识和地址。为了达到这个目的，一个站点必须建立与特定 BSS 的 AP 之间的关联关系。然后该 AP 与 ESS 内的其他 AP 通信，以实现经编址的帧的路由和传递。
- **重关联**（reassociation）：在允许一个移动站点从一个 BSS 移动至另一个 BSS 的情况下，使得已建立的关联能由一个 AP 转到另一个 AP。
- **中断关联**（disassociation）：由站点或 AP 发出通知，告知现存的关联被终结。站点必须在离开 ESS 或关闭之前给出这个通知。然而，MAC 管理设施会保护自身以避免站点未发出通知就消失。

14.3　IEEE 802.11 MAC 层和物理层标准

14.3.1　IEEE 802.11 介质接入控制

IEEE802.11 MAC 层覆盖了三个功能区：可靠数据传递、接入控制和安全。在该节中，我们讨论可靠数据传递和接入控制，有关安全的功能在 14.4 节进行描述。

1. 可靠的数据传递

与所有的无线网络一样，使用 IEEE 802.11 物理层和 MAC 帧的 WLAN 被认为是不可靠的。噪声、干扰和其他传播影响能导致大量的帧丢失。即使带有纠错码，大量的 MAC 帧也可能无法成功收到。可通过在诸如 TCP 的高层使用可靠性机制来处理这种情况。然而，在高层中用于重发的计时器一般是以秒为单位的，因此在 MAC 层处理错误会更有效。为了达到这个目的，IEEE 802.11 包括了帧交换协议。当一个站点收到另一个站点发来的数据帧时，它向源站点返回一个确认（acknowledgment，ACK）帧。此交换被作为一个原子单元处理，它不会被其他站点发出的传递打断。如果因为数据帧损坏或因为返回的 ACK 帧损坏，源站点在一个短的时间周期内没有收到 ACK 帧，会重传该帧。

这样，IEEE 802.11 中的基本数据传输涉及两个帧的传递。为了更进一步地增强可靠性，可以使用四帧交换。在此模式中，源站点首先向目的站点发送一个请求发送（Request to Send，RTS）帧。然后目的站点用一个清除发送（Clear to Send，CTS）帧响应。在收到 CTS 帧后，源站点发送数据帧，而目的站点以一个 ACK 帧响应。RST 帧警告所有位于源站点接收范围内的其他站点正在进行着一个交换，这些站点就会抑制自己帧的发送，以避免因两个帧同时传递而产生冲突。类似地，CTS 帧也警告所有位于目的地址接收范围内的其他站点正在进行着一个交换。交换中的 RTS/CTS 部分是 MAC 需要的功能，但也可以被禁用。

2. 接入控制

802.11 工作组为 MAC 算法考虑了两类方案：1）分布式接入协议。像以太网一样，利用载波侦听机制将发送的决定权分散到所有节点；2）集中式接入协议。由集中决策者来控制传输。对于由对等工作站组成的自组织网络而言，分布式接入协议是更有效的。分布式接入协议对于主要由突发通信组成的其他 WLAN 的配置也有吸引力。集中式接入协议自然地适用于这样的配置，其中有大量无线站点相互连接，并且由某个基站与骨干有线 LAN 相连。如果有一些数据具有时间敏感性或高优先级，这时集中式接入协议就特别有用。

802.11 的最终成果是一个称为基于分布方式的无线介质访问控制（Distributed Foundation Wireless MAC，DFWMAC）的 MAC 算法，来提供一个分布式接入控制机制以及在其上建立

的可选的集中控制。图 14-4 给出了该结构。MAC 层下的子层是分布式协调功能（Distributed Coordination Function，DCF）。DCF 使用一个竞争算法为所有通信提供接入。普通的非同步通信直接使用 DCF。点协调功能（Point Coordination Function，PCF）是一个集中式的 MAC 算法，用于提供无竞争服务。PCF 建立在 DCF 之上，并利用 DCF 属性保证它的用户的接入。最后，由逻辑链路控制 LLC 层提供到高层的接口，并实现如差错控制这样的基本链路层功能。

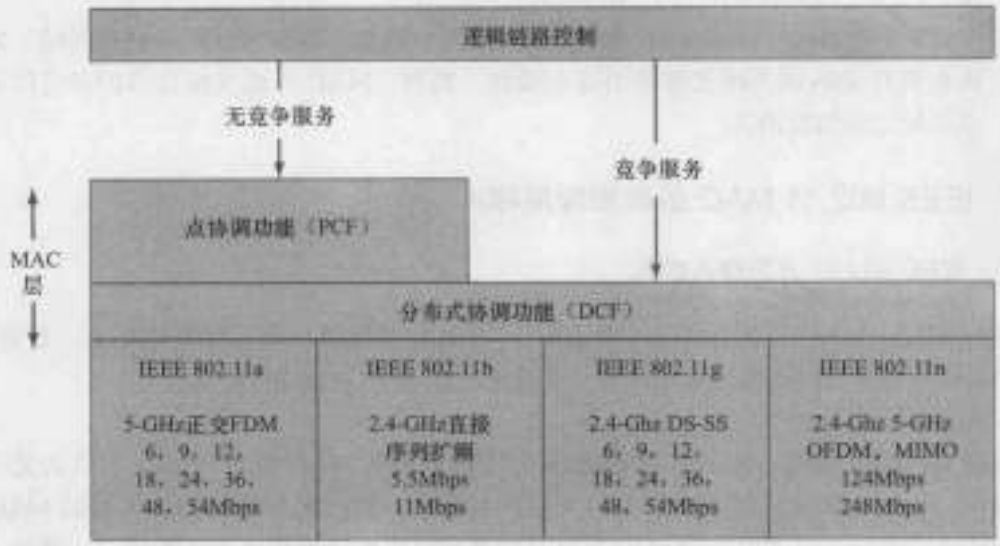


图 14-4　IEEE 802.11 协议体系结构

14.3.2　IEEE 802.11 物理层

IEEE 802.11 物理层分五个阶段发布。第一部分，简称为 IEEE 802.11，包括 MAC 层和三个物理层规范，其中两个工作在 2.4GHz 波段（ISM），另外一个工作在红外波段，这三个都工作在 1Mpbs 和 2Mpbs 数据率。IEEE 802.11a 工作在 5GHz 波段，数据率最高达 54Mbps。IEEE 802.11b 工作在 2.4GHz 波段，数据率为 5.5Mpbs 和 11Mbps。IEEE 802.11g 也工作在 2.4GHz 波段，数据率最高为 54Mbps。最后，IEEE 802.11n 或工作在 2.4GHz 波段或工作在 5GHz 波段，数据率为几百 Gbps。表 14-3 给出了一些细节，我们讨论其中的每一个标准。

表 14-3　IEEE 802.11 物理层标准

	802.11a	802.11b	802.11g	802.11n
峰值数据吞吐量[①]	23Mbps	6Mbps	23Mbps	60Mbps（20-MHz 信道） 90Mbps（40-MHz 信道）
峰值信号率	54Mbps	11Mbps	54Mbps	124Mbps（20-MHz 信道） 248Mbps（40-MHz 信道）
RF 波段	5GHz	2.4GHz	2.4GHz	2.4GHz or 5 GHz
信道宽度	20MHz	20MHz	20MHz	20MHz or 40 MHz
空间流数目	1	1	1	1，2，3，or4

①这是在理想条件下使用真实设备获得的实际数据吞吐量，真实世界中由于噪声的影响，实际性能要比这低。容量也是由无线客户之间共享。当两个设备使用同一接入点时，容量通常是一分为二，虽然有可能一些客户占用的容量比另一些客户占用得多。参见 [OU07]。

1. 初始 IEEE 802.11

初始 802.11 标准中定义了 3 种物理介质：

- 直接序列扩频（Direct-Sequence Spread Spectrum，DSSS），工作在 2.4GHz ISM 波段，数据率为 1Mbps 和 2Mbps。
- 跳频扩频（Frequency-Hopping Spread Spectrum，FHSS），工作在 2.4GHz ISM 波段，数据率为 1Mbps 和 2Mbps。
- 红外（infrared），数据率为 1Mbps 和 2Mbps，工作在波长范围为 850 – 950nm 的波段。

红外选项一直得不到市场的支持。其他两种方案使用扩频技术。本质上，扩频涉及使用比实际需要多得多的带宽，以达到给定的数据率。利用宽的带宽的目的是最小化干扰，从而大大地减少出错率。在 FHSS 中，通过频繁地从一个载波频率跳到另一个载波频率实现扩频。因此，如果在一个给定频率下存在干扰或性能退化的情况，这只会影响一小部分的传输。DSSS 通过将每一个数据比特映射到一个比特串，有效地提高了信号的数据率，其中用一个比特串表示二进制 1，用另一个比特串表示二进制 0。数据率越高，则使用的带宽越大。效果就是将每一比特在一段时间上扩展开来，这样就将干扰和退化的影响最小化。FHSS 比较简单，应用于多数早期的 802.11 网络。随后是使用 DSSS 的产品，DSSS 在 802.11 方案中更为有效。然而所有的初始 802.11 产品因其数据率较低，使用范围较为有限。

2. IEEE 802.11b

IEEE 802.11b 是 IEEE 802.11 DSSS 方案的扩展，在 2.4GHz 波段上提供 5.5Mbps 和 11Mpbs 的数据率。利用更复杂的调制技术可获得更高的数据率。802.11b 规格快速地指导出产品的上市，包括芯片组、PC 卡、接入点和系统。苹果计算机是提供 802.11b 产品的第一家公司，它的 iBook 便携计算机使用了 AirPort 无线网络选项。其他公司，如 Cisco、3Com 和 Dell，随后也跟进。虽然这些新产品都是基于相同的标准，通常还是有人会担心这些来自不同生产商的产品是否能成功地互通。为了解决这些担心，无线以太网兼容性联盟（Wireless Ethernet Compatibility Alliance，现在称为 Wi-Fi 联盟）创建了一个测试套件，来验证 802.11b 产品间的互通性。互通性测试已开始实施，并且许多产品已获得证书。

初始 802.11 和 802.11b 产品的另一个担心，是与其他工作在 2.4GHz 频带产品之间的干扰问题，这些产品包括蓝牙、HomeRF，以及利用该频带的其他设备，如宝宝监视器和车库开门器等。有一个协同研究组（IEEE 802.15）正在研究这个问题，到目前为止这前景是令人鼓舞的。

3. IEEE 802.11a

虽然 802.11b 获得了一定的成果，但其受限的数据率导致了吸引力有限。为了满足对真正高速 LAN 的需求，开发了 IEEE 802.11a。IEEE 802.11a 使用了称为通用网络信息基础设施（Universal Networking Information Infrastructure，UNII）的频带，该频带分为三部分。UNNI-1 波段（5.15–5.25GHz）计划在室内使用，UNNI-2 波段（5.25–5.35GHz）既能用于室内也能用于室外，UNNI-3 波段（5.725–5.825GHz）用于室外。

与 2.4GHz 规格说明书不同的是，IEEE802.11a 不使用扩频方案，但使用**正交频分复用**（Orthogonal Frequency Division Multiplexing，OFDM）。OFDM 也称为多载波调制，使用工作在不同频率的多个载体信号（多达 52 个信号），每个信道发送一些比特。IEEE 802.11a 可能的数据率有 6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps 和 54Mbps。

在高数据率下，OFDM 在处理无线网络中称为**多径干扰**（multipath interference）的关键问题时特别有效。该问题的本质是信号从一个天线传输至另一个天线时，接收天线可接收到

该信号的多个复制，其中一个是直线传输的信号，其他的都是经过附近物体反射而产生的复制信号。由于这些信号经过具有不同长度的路径的传输，它们分别在相差不多的时间点到达接收天线，从而造成干扰。数据率越高，干扰造成的损失越大。代替在给定信道上以高数据率发送单个数据流的是，利用 OFDM，将该信道分为多个子信道，每个子信道上传递部分的数据流。简单地举例说，如果共有 10 个子信道，那么每个子信道以原数据率的 1/10 来传递部分的数据流。有关多径干扰和 OFDM 的详细讨论，参见附录 I。

4. IEEE 802.11g

虽然 802.11a 能提供的数据率比 802.11b 的数据率高，该新方案的接受度比较有限。这是因为设备相对比较贵，并且该方案与初始 802.11 或者 802.11b 都不兼容。因此，工厂和客户开始转向更新的标准，即 802.11g。

IEEE 802.11g 是 IEEE 802.11b 的高速扩展，提供高达 54Mbps 的数据率，与 IEEE 802.11a 的相同。像 IEEE802.11b 一样，802.11g 工作在 2.4GHz 波段范围，因此两者兼容。相应的标准被设计出来，以便 802.11b 设备在连接到 802.11g AP 时能正常工作，以及 802.11g 设备在连接到 802.11b AP 时也能正常工作，这两种情况下都使用较低的 802.11b 数据率。

IEEE 802.11g 提供更多的数据率选择范围和调制方案选项。在高数据率下，802.11g 采用 802.11a 的 OFDM 方案，该方案调整到 2.4GHz 的数据率，称为 ERP-OFDM，其中 ERP 代表可扩展速率物理层（extended rate physical layer）。

IEEE 802.11 标准不包括有关速度与距离比的目标方面的说明。不同的生产商依据环境分别给出不同的值。依据 [LAYL04]，表 14-4 给出了典型办公环境中的估计值。

表 14-4　距离与数据率比的估计值

数据率（Mbps）	802.11b	802.11a	802.11g
1	90+	—	90+
2	75	—	75
5.5（b）/6（a/g）	60	60+	65
9	—	50	55
11（b）/12（a/g）	50	45	50
18	—	40	50
24	—	30	45
36	—	25	35
48	—	15	25
54	—	10	20

5. IEEE 802.11n

随着 WLAN 需求的提高，802.11 委员会开始寻找方法来提高 802.11 网络的数据吞吐量以及整个的容量。这方面努力的目标不仅要提高传输天线的比特率，也要提高网络的有效吞吐量。提高有效吞吐量不是简单地提高信号编码方案，这涉及改进天线体系结构和 MAC 帧结构。这方面的成果是包含在 802.11n 中的提高和增强方案包。该标准定义工作在 2.4GHz 和 5GHz 两个波段，因此可与 802.11a 或 802.11b/g 实现向下兼容。

IEEE 802.11n 包括三个通用领域的改变：使用 MIMO、无线电传输的增强、MAC 增强。我们下面简单介绍其中的每一个。

多输入多输出（Multiple-Input-Multiple-Output，MIMO）天线结构是 802.11n 所提供增强

中最重要的。有关 MIMO 的讨论超出我们的范围，因此用简短的复习来满足我们的需要（见图 14-5）。在 MIMO 方案中，发送方采用多个天线。源数据流分为 n 个子数据流，每个子数据流利用 n 个传输天线中的一个来发送。单个的子数据流作为传输天线的输入，即多输入。在接收端，m 个天线接收来自 n 个天线源的传输，这 n 个天线源通过直线传输和多径传输的组合到达接收端。这 m 个接收天线的输出（多输出）与来自其他接收无线电的信号组合在一起。基于许多复杂的数学，结果是接收到的信号比通过单个天线或者多个频率信道传输的信号要好得多。802.11n 标准定义了发送者数目和接收者数目多种不同的组合，从 2×1 到 4×4。系统中每一个额外的发送方或接收方都能增加信噪比。然而，从每个额外的发送方或接收方获得的增量收益则快速地减少。从 2×1 到 2×2 以及到 3×2 的每一步，SNR 中的收益都是比较大的，但是对于 3×3 及以上，其收益的增加相对比较少 [CISC07]。

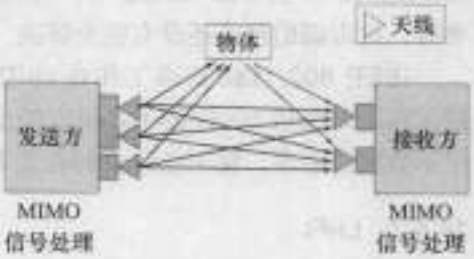


图 14-5　MIMO 方案

除了 MIMO，802.11n 在**无线电传输方案**（radio transmission scheme）上做了许多改进以提高容量。这些方案中最重要的叫做信道捆合（channel bonding），将两个 20MHz 的信道组合起来形成一个 40MHz 的信道。通过利用 OFDM 技术，这样的信道捆合允许两倍的子信道数目，传输率从而加倍。

最后，802.11 提供一些 **MAC 加强**机制。最重要的改变是将多个 MAC 帧聚合进单个块中以供传输。一旦一个站点请求介质用以传输，它就以传输之间不大的延迟间隔来传输长报文。接收方则发送单个的块确认。帧聚合使得在传输容量使用方面的效率大大提高。

图 14-6 指明了与 802.11g 对比的 802.11n 有效性 [DEBE07]。该图显示了在一个共享系统中每个用户的平均吞吐量。如期望的那样，越多的活动用户竞争无线容量，每用户的平均吞吐量越小。IEEE 802.11n 提供了很大的改进，特别是对只有很少的活动用户竞争传输时间的网络。

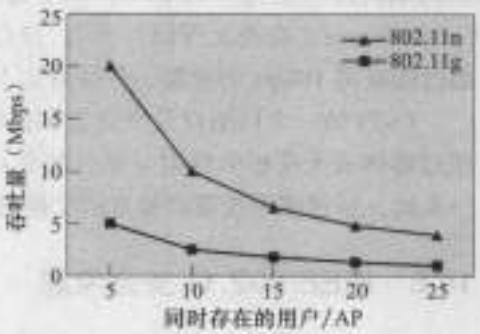


图 14-6　每个用户的平均吞吐量

14.4　千兆 WLAN

就如有线 LAN 已发展到千兆范围，以满足持续不断提高传输容量的需求，无线 LAN 也正朝着相同范围发展。我们来看一下这个领域内的两方面的发展区域。

14.4.1　千兆 Wi-Fi

目前正在实施有关千兆无线 LAN 的一些方案。IEEE 802.11 正在开发两个标准，这些标准将决定可用的产品。

IEEE 802.11ac 标准是旧 802.11a Wi-Fi 标准的下一步安排。回想一下，802.1a 是 5GHz 标准，数据率最高达 54Mbps。生产商在将 802.11a 设备应用于户外方面进展得很缓慢。当

802.11g 出来后，该标准工作在 2.4GHz 范围，能产生相同的速度，且能与旧的、慢速的 802.11b 兼容，802.11a 则成为一种孤立的技术。伴随着 802.1ac，802.11a 正在重新获得关注。这个新标准的频带为 5-GHz，但能提供更宽的信道以获得更高的数据吞吐量。IEEE 802.11a 使用宽度为 20MHz 的信道，802.11ac 使用宽度为 40MHz 或 80MHz 甚至 160MHz 的信道来传递数据。802.11ac 也可以使用多用户多输入多输出（Multiuser Multiple-Input Multiple-Output，MU-MIMO）。在 MU-MIMO 中，在相同的信道中可同时传递到不同用户的数据流。到写这本书时，这方面的细节还没有完全解决，但已经有产品宣称能支持最高达 1Gbps 的数据率。

IEEE 802.11ad 标准工作在 60GHz 频带，并被期望在最高达 6Gpbs 的数据率下传递数据。该毫米频带 Wi-Fi 的不足是它的范围是在英尺内而不是码内。802.11ad 能覆盖一个房间，但不能覆盖更多。就 802.11ac 标准而言，到写这书时，已宣称有相关产品，并且很快会面世。

14.4.2　Li-Fi

2011 年 10 月，一些公司和工业团体组建了 Li-Fi 联盟，该联盟的目标是促进高速光无线系统。发展光 WLAN 的动机是光系统能帮助解决迫在眉睫的容量问题。随着基于无线电的无线网络变得越来越普遍，越来越多的设备使用 WLAN 频率来传递大量数据，但是可用的无线电频谱总量有限。可见光波的使用则通过利用电磁频谱中完全独立的一部分，为解决这个问题提供了可能。该类可见光波由于被用来照明，因而是普遍存在的。

基本的技术方案是：将来自光源的可见光变化其密度来编码二进制数据。光的闪烁很弱，以致于人眼无法觉察到。白炽灯和荧光灯不适合用来进行所需的快速调制。然而作为快速取代这些老技术的 LED，则非常适合用来进行高速调制。一些产品已装配上光敏器件（photosensor，在晚上可以打开），并且在已有产品上添加光敏器件不是很大的技术挑战。目前已能获得 10Gps 的速度，并且高达 100Gpbs 的速度也在酝酿之中。

Li-Pi 的一个局限性是发送方和接收方之间需要在对方的视线之内，它们可直接可见，或通过墙体或天花板的反射可见。然而对于安全应用而言，这样的特性反而可能是个优点。进一步地，通过使用按策略放置的交换机和路由器，有关视线范围内的限制是可控制的。

14.5　IEEE 802.11 安全考虑

有线 LAN 中有两个特征，这两个特征不是固有存在于 WLAN。

1）为了在有线 LAN 上传输，站点必须物理连接到 LAN。从另一方面来说，在一个 WLAN 中，一个站点只要在 LAN 上其他设备的无线电范围内，它就可传输。在某种意义上，有线 LAN 中有一种鉴别形式，其中需要某种积极的、大概可观察的行为来将一个站点连接到有线 LAN。

2）相似地，为了从有线 LAN 上的一个站点接收传输，接收站点必须连接到有线 LAN 上。从另一方面来说，在一个 WLAN 中，任何在无线电范围内的站点都可接收。因此，有线 LAN 提供了一定程度的私密性，限制仅连接到 LAN 上的站点才可接收数据。

14.5.1　访问和私密性服务

IEEE 802.11 定义了三种服务来为 WLAN 提供上述的两种特性。

鉴别（authentication）：用来为每个站点建立区别于其他站点的身份标识（indentify）。在有线 LAN 中通常假定：访问一个物理连接，则转让了连接到该 LAN 的授权。这对 WLAN 来

说不是一个合法的假设，在 WLAN 中只要有一个经正确调谐的连接天线，就可简单地获得连接。IEEE 802.11 支持多种鉴别方案，并且允许这些方案进行功能扩充。该标准不强制使用任何特殊的鉴别方案，这些方案的范围可从相对不安全的握手方案一直到公钥加密方案。然后，IEEE 802.11 要求一个站点在与 AP 建立关联前，相互之间需要经过可接受的、成功的鉴别。

清除鉴别（deauthentication）：当需要终止已存在的鉴别时，触发该服务。

私密性（privacy）：用来防止消息内容被目的接收方以外的站点读到。该标准提供可选的密码算法来保证私密性。

14.5.2　无线 LAN 安全标准

初始的 802.11 规范包含一些私密性和鉴别的安全属性，但安全性都很弱。对于**私密性**，802.11 定义了有线对等保密（Wired Equivalent Privacy，WEP）算法。802.11 标准中的私密性保护部分包含很大的脆弱性。继 WEP 开发之后，802.11i 工作组已研发出一系列功能来解决 WLAN 中的安全问题。为了加快将强安全性引入到 WLAN 的进程，Wi-Fi 联盟颁布 **Wi-Fi 网络安全存取**（Wi-Fi Protected Access，WPA）算法作为 Wi-Fi 的标准。WPA 是一组安全机制，这些安全机制解决了大部分的 802.11 安全问题，并且是基于 802.11i 标准的当前状态研发出来的。随着 802.11i 标准的发展，WPA 也将发展以保持兼容性。WPA 将在第 19 章详细介绍。

应用注解

部署 WLAN

许多组织面临着决定是否部署无线局域网（WLAN）的问题。当考虑到 WLAN 的一些安全因素（如安全性、所部署设备的管理和标准混乱等）时，这个问题就变得更为严重了。最后，WLAN 的部署加重了支持部门的责任，如果不给他们提供必需的培训或专家来管理该网络。

即便如此，还是有一些原因来部署 WLAN 的：移动性、安装方面的开支减少、部署速度、自组织组网、连接地理位置分布远的节点的能力。一个组织应该自问的第一件事就是，WLAN 是必需的还是仅仅拥有就好了。许多公司由于无线网络表现出来的安全漏洞，决定不部署 WLAN。可能会有太多的风险或者管理噩梦而不能部署，这是可以理解的。这种方案会带来一些危险，特别是当公司也决定不干扰无线培训时。大部分的终端设备内置了无线功能。此外，员工、学生和访客也会未经公司允许而安装无线设备。这通常不是为了攻击公司的网络，仅仅是因为越来越多的设备装备上无线功能。便携式电脑就是一个很好的例子。

无线设备也有一个恼人的能力，即自动发现连接。这在 Windows XP 系统下就更严重了，该系统透明地处理许多无线问题，并且有连接共享的功能。连接共享允许多个用户通过单个电脑的网络连接来访问网络。进一步地，Windows 系统无线连网客户端不提供很多的控制属性。如果你决定不部署无线网络，你仍然需要为你机构内的其他人部署无线网络做好应对准备。

选择合适的标准可能会很困难。802.11 家族有许多代的标准，其中 802.11b 最为成功。然而 802.11 标准中也有很多重要问题，包括相对低的带宽，能在一个区域内工作的访问点的数目少，来自其他共享 2.4GHz 频谱设备的干扰。

下一代标准，802.11a 和 802.11g，都在尝试解决这些问题，其中 802.11a 在避免干扰方面更为成功，因为它已转移到 5GHz。但这引入了更小覆盖范围的问题，因为频率越高，越不能传播得远。如果你已有了一个无线网络，那么你的决定就与从零开始部署无线网络的有一些不同。为了与已有的 802.11b 网络兼容，你可能选取 802.11g，该网络有更高的数据容量，但仍能与 802.11b 节点直接通信。802.11g 成为大部分商务网络的选择。

依据预期的使用情况，新安装的网络可在新标准中唯一选择其中的一个标准。记住已有的网络中 802.11b 设备非常多，因此在选择时需要支持 802.11b。对许多人来说，由于数据率高、干扰低和可用信道数目多的原因，802.11a 是最佳选择。802.11b 的强处也是它的弱点。基于无线电的通信中一个基本经验法则是：频率越高，传输距离则越近。因此，由于 802.11a 使用了更高的频率，其传输范围比 802.11b 短。另一个基本经验法则是：随着频率的增长，信号越容易破坏。这最后一个问题高度依赖于操作环境。由于这些原因，802.11g 可能是最好的选择，因为它与 802.11b 模型紧密匹配。

我们最后的讨论点是关于安全。虽然在安全评估方面没有银弹，还是有一些基本的实践来帮助减少暴露和漏洞，包括如下：

- 将接入点置于公司的防火墙之外，以保证公司数据不被广播。
- 打开 WEP 或 WPA-PSK。虽然它们有问题，但它们能阻止大部分的网络偷听和带宽占用。
- 将接入点置于交换机之后，而不是集线器 hub 之后，这样能提供更多的流量过滤。
- 完成对无线场所的调查，以确定暴露程度。
- 为无线节点采用 VPN。
- 采取一些基本的第二层和第三层过滤，以实现安全的访问。
- 当有疑问时，对数据进行加密。
- 要了解大部分的问题（包括恶意的和偶然的）不是来自外部攻击，而是来自于内部用户。

无线通信的真正问题是非常少的网络管理者曾在这方面花费时间。结果就是非常缺乏在这些问题方面的理解和体验。虽然短的讨论不是意味着对无线网络的最终指导，但它能帮助你理解一些有关 WLAN 的较严重的问题和思维过程。

14.6 总结

近些年出现了一种全新的局域网（LAN），该网络提供基于双绞线、同轴电缆和光线的 LAN 之外的另一种选择：WLAN。WLAN 的最大优点是减少了布线成本（这通常是 LAN 中最昂贵的组成部分），并且能容纳移动工作站。

WLAN 采用三种传输技术中的一种：扩频、窄带微波和红外光。WLAN 的最重要标准集由 802.11 委员会定义。

案例研究 IX：St.Luke 保健系统：利用移动性来促进保健传输

这个案例研究中的最重要概念包括无线 LAN、移动应用。该案例研究以及其他更多的信息参见 www.pearsonhighered.com/stallings。

14.7 关键术语、复习题和练习题

关键术语

Access Point（AP，接入点）
ad hoc networking（自组织组网）
Basic Service Set（BSS，基本服务集）
Distribution System（DS，分布式系统）
Extended Service Set（ESS，扩展服务集）
Independent BSS（IBSS，独立 BSS）
infrared LAN（红外 LAN）
narrowband microwave LAN（窄带微波 LAN）
OFDM（正交频分复用）
portal（入口）
service area（服务区域）
spread spectrum LAN（扩频 LAN）
wireless LAN（WLAN，无线 LAN）

复习题

14.1 列举和简短定义 WLAN 的 4 个应用领域。
14.2 列举和简短定义 WLAN 的关键需求。
14.3 单蜂窝 WLAN 和多蜂窝 WLAN 有什么区别？
14.4 802.11 WLAN 的基本组成是什么？
14.5 定义一个扩展服务集。
14.6 列举和简单定义 IEEE 802.11 服务。
14.7 接入点和入口之间的区别是什么？
14.8 分布式系统是无线网络吗？
14.9 与移动性概念相关的关联概念是怎样的？
14.10 概括地说，蓝牙支持的应用领域有哪些？
14.11 核心规范（core specification）和轮廓规范（profile specification）之间有什么区别？
14.12 什么是使用模式（usage model）？

练习题

14.1 回答以下有关你所使用的无线网络的问题：
a. 什么是 SSID？
b. 设备生产商是谁？
c. 你所用的是什么标准？
d. 网络的规模有多大？
14.2 使用你所知道的关于有线网络和无线网络的知识，画出你所用的网络的拓扑结构。
14.3 有很多免费的工具和应用来帮助解密无线网络，其中使用得最多的是 Netstumbler。从 www.netstumbler.com 获得该软件，跟踪下载链接。该网站有一个所支持的无线网卡的列表。使用 Netstumbler 软件，确定下列问题的答案：
a. 你的网络有多少个拥有相同 SSID 的接入点？
b. 到接入点的信号强度是多少？

c. 你能发现多少其他的无线网络和接入点？

14.4 大多数的无线网卡有一些应用集能做与 Netstumbler 相似的工作。使用你自己的客户端软件，确定出与你用 Netstumbler 确定的相同条目。它们是一致的吗？

14.5 试做如下实验：你能走出多远而仍与网络保持连接？这在很大程度上依赖于你所处的物理环境。

14.6 比较和对比有线 LAN 和无线 LAN。什么只是 WLAN 网络设计者需要考虑的？

14.7 与无线传输介质的安全考虑相关的两个文档为：FCC OET-65 Bulletin 和 ANSI/IEEE C95.1-1999。简单描述这些文档的目的，简要概述与 WLAN 技术相关的安全考虑。

第五部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

广域网

第 15 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

广域网技术和协议

学习目的

通过本章的学习，读者应该能够：

- 解释用于广域电话和数据通信的通信网络的需求。
- 定义电路交换并描述电路交换网络的关键要素。
- 讨论电路交换的重要应用，包括公用网络、私有网络和软定义网络。
- 定义分组交换并描述分组交换技术的关键元素。
- 讨论分组交换的重要应用，包括公用网络和私有网络。
- 讨论电路交换和分组交换各自的优点，分析每种交换技术适用的场合。
- 概述 VoIP 网络。
- 解释存在概念及如何实现。

交换技术广泛应用在企业网络中。全交换式以太网络是企业局域网的标准，交换机也是广域网基础服务占主导地位的网络互连设备。企业使用广域网（Wide Area Network，WAN）服务，实现地理位置分散的操作站互连。对于理解当今企业网络中语音和数据的传输，掌握基本的交换技术是十分必要的。

首先，本章给出交换式通信网络的概要性讨论，其次，集中讨论广域网，尤其是广域网设计的传统方法：电路交换和分组交换。再次，研究通过因特网提供传统 WAN 服务的重要例子：IP 语音。最后，讨论存在的概念，即基于广域网和局域网基础设施建立的服务。

15.1 交换技术

对于局部区域之外的数据传输[⊖]，这种通信典型地通过中间交换节点网络实现从源到目的地的数据传输。而且，这种交换式网络设计也用于实现局域网（LAN）。交换节点不关心数据的内容，其目的是提供交换设备，将数据从一个节点传送到另一个节点，直到数据到达目的地。图 15-1 给出一个简单的网络。希望通信的终端设备称为站，可以是计算机、终端、电话或其他通信设备。把以提供通信为目的的交换设备称为节点。

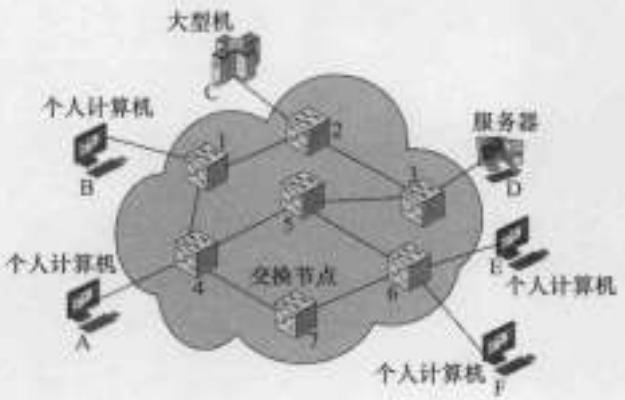


图 15-1 简单交换网络

⊖ 术语“数据”的意义在这里比较广泛，包括语言、图像、视频以及普通数据（数字、文本）。

在网络拓扑中，节点之间通过传输链路相互连接。每一个站连接到一个节点，节点的集合称为通信网络。

在交换式通信网络中，来自于某站的数据进入通信网络，通过节点之间的交换把数据路由到目的地。

例子　在图 15-1 中，从站 A 到站 F 的数据被传送到节点 4，这些数据可以通过节点 5 和 6 或者节点 7 和 6 路由到目的地。以下几点值得注意：

1）有些节点只连接到其他节点，它们的唯一任务是数据的内部（到网络）交换。另一些节点还与一个或多个站相连，这些节点除了交换功能外，还要接收连接站的数据或发送数据到连接的站。

2）节点 – 站链路通常是专用的点对点链路，节点 – 节点链路通常是多路复用，使用频分复用（FDM）或时分复用（TDM）。

3）通常，网络不是全连通的，就是说，在每一个可能的节点对之间并不总有一条直接的链路。然而，总是希望网络中每一对站之间存在一条以上的可能路径，这有助于提高网络的可靠性。经常使用部分网状网络来确保多条路径。

在广域交换式网络中使用两种不同的交换技术：电路交换和分组交换。它们的不同之处在于从源到目的路径上，从一个链路到另一个链路时节点交换信息的方式。接下来介绍这两种技术的细节。

15.2　电路交换网络

15.2.1　基本操作

通过电路交换的通信意味着在两个通信站之间有一个专用的通信路径，而且这条路径是网络节点之间连通的链路序列。在每一个物理链路上，有一个专用通道用于该连接。电路交换的常见例子是电话网络。

通过电路交换的通信包含 3 个阶段，结合图 15-1 对这 3 个阶段给予解释。

1）**电路建立**。在任意信号传送之前，必须建立端到端（站到站）的电路。比如，站 A 发送一个请求给节点 4，要求与站 E 建立连接。典型地，从站 A 到节点 4 的链路是一条专用线，因此这部分连接已经存在。节点 4 必须查找通向节点 E 的路由的下一个节点，基于路由信息和可用性、成本度量指标，节点 4 选择到节点 5 的链路，并使用 TDM 或 FDM 方法在这条链路上分配一个空闲通道，发送请求与站 E 建立连接的消息。到目前为止，从站 A 经由节点 4 节到节点 5 的专用路径已经建立。由于许多站与节点 4 相连，所以节点 4 必须能够建立从多个站到多个节点的内部通道，在本节后面将讨论如何建立内部通道。电路建立过程的后面节和前面相似，节点 5 分配一个空闲通道给节点 6，并从内部把这个通道与来自节点 4 的通道绑定在一起。节点 6 完成与站 E 的连接。一旦连接完成，接着执行站 E 的状态测试，以确定站 E 是处于繁忙状态还是准备接受连接。

2）**数据传输**。现在数据可以通过网络从 A 传送到 E。数据类型依赖于网络本质，可以是模拟语音、数字化语音或二进制数据。随着载体向完全集成的数字网络发展，语音和数据的数字化（二进制）传输成为主流方法。传输路径如下：A—4 链路，节点 4 的内部交换；4—5 通道，节点 5 的内部交换；5—6 通道，节点 6 的内部交换；6—E 链路。一般地，建立的连接

是全双工的，可以在两个方向上同时传送信号。

3）**电路断开**。数据传输一段时间后，由两个站中一个站终止连接。而且，终止信息必须传送给节点 4、5 和 6 以便释放占用的资源。

值得注意的是，数据传送开始之前建立连接路径，因此路径上每对节点之间必须预留通道容量，而且每个节点必须有可用的内部交换能力以处理请求的连接。交换机必须有能力进行资源分配和设计网络路由。

电路交换是十分低效的。在连接持续期间即使没有数据传输，通道容量一直被占用。对于语音连接，利用率相当高，但仍然没有达到 100%。对于客户机 / 服务器连接，在连接的大部分时间通道容量或许是闲置的。而且，在用于呼叫建立的信号传送之前有延迟。然而，一旦电路建立起来，网络对用户是十分透明的。数据以固定的速率传送，而且除了通过传送链路的传输延迟以外几乎没有延迟，在每一个节点的延迟是可以忽略的。

过去，电路交换用于处理语音流量，但是现在也用于处理数据流量。一个非常出名的电路交换网络例子是公用电话网络（见图 15-2）。这实际上是形成国际服务的互连国家网络集合。虽然电路交换的最初设计与实现目的是服务于模拟电话用户，但是它通过调制解调器处理真正的数据流量，现在成为一个主要的数字网络。电路交换另一个非常出名的应用是用户交换机（Private Branch Exchange，PBX），用于实现一栋楼或一个办公室电话的互连。电路交换也应用于私有网络。典型的是由某个公司或其他大组织为了连接其各种站点而组建的网络，这种网络通常由 PBX 系统组成，在每个站点 PBX 系统通过从运营载体，如 AT&T，获得专有的、租用的线路互连。

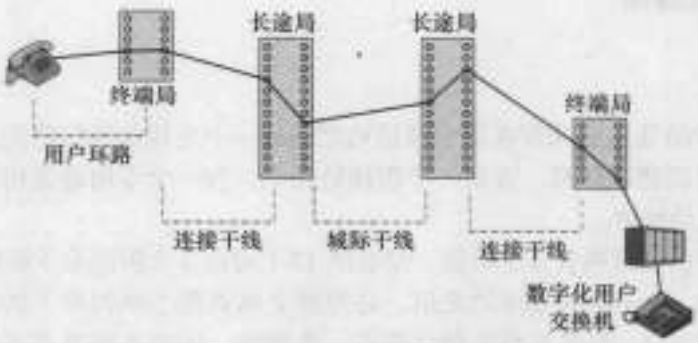


图 15-2　公共电路交换式网络的连接样例

通过介绍 4 个通用的结构组件来描述公共电信网络：

- **用户**：连接到网络的设备。目前，连接到公共电信网络的大多数用户设备仍然是电话，但是数据流量的百分比逐年增加。
- **用户线**（subscriber line）：用户和网络之间的链路，也称为*用户环路*或*本地环路*。而且几乎所有的本地环路连接使用双绞线，本地环路的长度通常地在几公里到几十公里内。
- **交换中心**：网络的交换中心。直接支持用户的交换中心称为终端局。典型地，在本地化区域中一个终端局将支持上千个用户。在美国，共有 19 000 多个终端局。因此，很显然任意两个终端局之间都有直接的链路是不切实际的，这将需要 2×10^8 数量级的链路。相反，使用中间交换节点以减少链路的数量。
- **干线**（trunk）：两个交换中心之间的分支。干线可以使用频分复用或时分复用技术，承载多路音频电路，这些也称为*话载系统*。

用户直接连接到某个终端局，实现两个用户之间或用户与其他交换中心之间的流量交换。相反，其他交换中心负责终端局之间的流量路由与交换。图 15-3 给出终端局和交换中心的差异。如果是连接同一终端局的两个用户之间建立连接，那么它们之间的电路建立方式与前面描述的一样。如果两个用户连接到不同的终端局，那么它们之间的电路由经过一个或多个中间局的电路链组成。图 15-3 中，线 a 和 b 之间的连接仅仅通过终端局建立连接即可实现。线 c 和 d 之间的连接就比较复杂，c 连接的终端局与中间交换机 TDM 干线的一个通道建立连接，中间交换机的这个通道与 d 的终端局 TDM 干线的一个通道建立连接，最后终端局的这一通道连接到线 d。

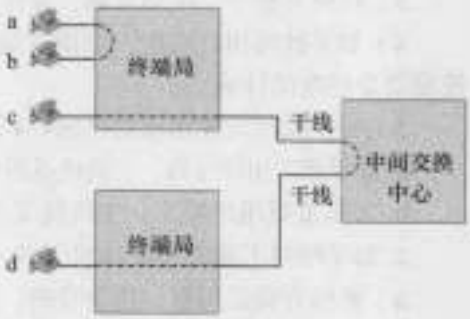


图 15-3　电路建立

电路交换技术一直受语音流量传输驱动。语音流量的一个关键需求是不能有传输延迟，而且延迟不能有变化。由于传送和接收以同一个信号传输速率进行，所以语音流量传输必须维持固定的信号传输速率。对于人类的正常交流，这些需求是必需的。而且，接收信号的质量必须足够高，以提供最低限度的理解识别（intelligibility）。

由于电路交换非常适合模拟语音信号的传输，所以应用广泛，占据了主导地位。但是在当今的数字化世界，它的缺陷也变得比较明显。然而，即使电路交换存在缺点，但目前它仍然是局域网和广域网非常有吸引力的选择，而且以后也将仍然是一个好的选择。这主要归因于电路交换的优势之一是透明。一旦建立了电路，看起来好像是与用户相连的两个站的直接连接；站上不需要任何特殊的连网逻辑。

15.2.2　控制信令

控制信令是管理电信网络，建立、维持与终止呼叫的方法。呼叫管理和整个网络管理都需要在用户与交换机之间、交换机之间、交换机与网络管理中心之间交换信息。对于大型的公共电信网络，需要一个相对复杂的控制信令方案。

控制信令影响网络行为的许多方面，包括用户可见的网络服务和内部机制。随着网络变得越来越复杂，控制信令执行的功能也随之增加。下面是控制信令的一些主要功能：

1）用户可听得见的拨号音、响铃、忙音等。

2）所拨的电话号码传输到企图完成连接的交换局。

3）交换局之间表示呼叫不能完成的信息传输。

4）交换局之间呼叫已经结束、路径可以断开的信息传输。

5）使电话响铃的信号。

6）用于计费的信息传输。

7）携带网络中设备或干线状态的信息传输，这些状态信息可用于路由和维护目的。

8）用于诊断和隔离系统故障的信息传输。

9）特殊设备的控制，如卫星通道设备。

作为控制信令使用的例子，典型的从一个线路到处于同一中心局的另一个线路的电话连接序列如下：

1）呼叫之前，双方的电话都没有在使用（挂机）。当一端用户拿起话筒（提机），呼叫开

始，这个动作行为自动发信号到终端局交换机。

2）交换机以可听得见的拨号音响应，示意用户可以拨电话号码。

3）呼叫者拨一个电话号码，并作为被叫地址传递给交换机。

4）如果被叫用户空闲，交换机通过响铃信号告知被叫用户有一个来电。而且，这个响铃控制信令使电话铃响。

5）交换机将反馈信息提供给呼叫用户：

a. 如果被叫用户空闲，交换机返回可听得见的响铃音给呼叫者，同时响铃信号发送给被叫方。

b. 如果被叫用户繁忙，交换机发送可听得见的占线信号给呼叫者。

c. 如果呼叫不能通过交换机完成，则交换机发送一段语音录音信息给呼叫者。

6）被叫方提起话机、接受呼叫，这些信息自动传送给交换机。

7）交换机终止响铃信号和可听得见的铃音，在两个用户之间建立连接。

8）当呼叫双方中的一方挂机，连接释放。

当被叫用户与呼叫用户连接的交换机不相同时，要用到下面的交换机－交换机干线信令功能：

1）发起交换机利用一个闲置的交换机交换机－交换机干线，在干线上发送提机信号指示，以便传递通信地址。

2）终点交换机在挂机信号后发送提机信号，叫做“眨眼”（wink），指示注册就绪状态。

3）发起交换机向终点交换机发送地址位。

这个例子说明使用控制信令执行的一些功能。按照功能，信令也可以分为监控、地址、呼叫信息和网络管理。

监控通常用来指使用二进制字符（真/假；关/断）的控制功能，如服务请求、应答、告警和返回闲置。这些监控信令处理被叫用户及所需网资源的可用性，用来确定某个所需资源是否可用，如果可用就利用。同时，它们也用于交流所需求资源的状态。

地址信号标识用户，当呼叫用户拨电话号码时产生初始地址信号。产生的地址信号通过网络传输以支持路由功能和定位、响铃被叫用户的电话。

呼叫信息指给用户提供呼叫状态信息的信号，这与交换机之间用于呼叫建立和终止的内部控制信号相对比。这些内部控制信号是模拟或数字电气信息，相比之下，呼叫信息信号是可听见的声音，通话者或接线员使用合适的电话设备（phone set）可以听得到。

在呼叫建立和终止过程中，直接涉及监控、地址和呼叫信息控制信号。**网络管理**信号用于网络的维护、故障排除和全面运营，这些信号可以是以消息形式出现，比如发送到基站用于更新路由表的预先规划好的路由列表。网络管理信号覆盖很广的范围，这种信号将扩展交换式网络日益增加的复杂性。

15.3　分组交换网络

大约在1970年，开始研究一种远距离数字化数据通信的新结构形式：**分组交换技术**。自从该技术提出以来，分组交换发生了实质性的演化，但异乎寻常的是：1）当今分组交换的基本技术从根本上与20世纪70年代早期的网络相同。2）分组交换技术仍然是远距离数据通信有效的技术之一。两种新出现的广域网技术（帧中继和ATM）实质上是基本分组交换方法的变种。本节将回顾仍在使用的传统分组交换技术，有关帧中继和ATM将在第16章讨论。

15.3.1　基本操作

长途电路交换电信网络在设计之初用于处理语音流量，而且在这些网络上传送的大部分流量仍然是语音。这种电路交换网络的一个主要特征是网络资源专用于特定的通话，不能被其他业务占用。对于语音连接，由于大多数时间一方或另一方一直在讲话，所以建立的电路利用率比较高。然而，随着电路交换网络开始逐渐被用于数据连接，以下两个缺陷变得明显：

- 在典型的用户 / 主机数据连接中（比如，PC 用户登录到数据库服务器），线路的大部分时间是空闲的。因此，对于数据连接，电路交换式方法是低效的。
- 在电路交换网络中，连接提供的是固定数据速率的传输。因此，相连接的每个设备必须与另一个设备以相同速率发送和接收数据，这限制了网络连接多种主机和工作站的可用性。

为了理解分组交换技术是如何处理这些问题的，先简要总结分组交换操作。数据以短数据分组的形式传输，而且典型的分组长度上界大约不超过 1500 字节。如果源端发送的消息比较长，则该消息被分解成一系列的短分组（见图 15-4）。每一个短分组包含一部分用户数据（或者所有短消息）和一些控制信息，而且最低限度下控制信息必须包括通过网络路由分组及把分组传送到目的地需要的信息。在路由路径上的每一个节点，分组被接收、简要存储并传递送下一个节点。



图 15-4　分组的使用

图 15-5 举例说明了基本操作。发送计算机或其他设备以分组序列的形式发送信息（见图 15-5a），且每个分组含有说明目的站（计算机、终端等）的控制信息。最初，分组被发送到与发送站连接的节点。当每一个分组到达这个节点时，节点简要地存储分组的信息、确定路由的下一跳，并对那条链路上要发送的分组排队。当链路可用时，把所有分组传送到下一个节点（见图 15-5b）。最终，所有分组经由网络按照同样的机制，发送到期望的目的地。

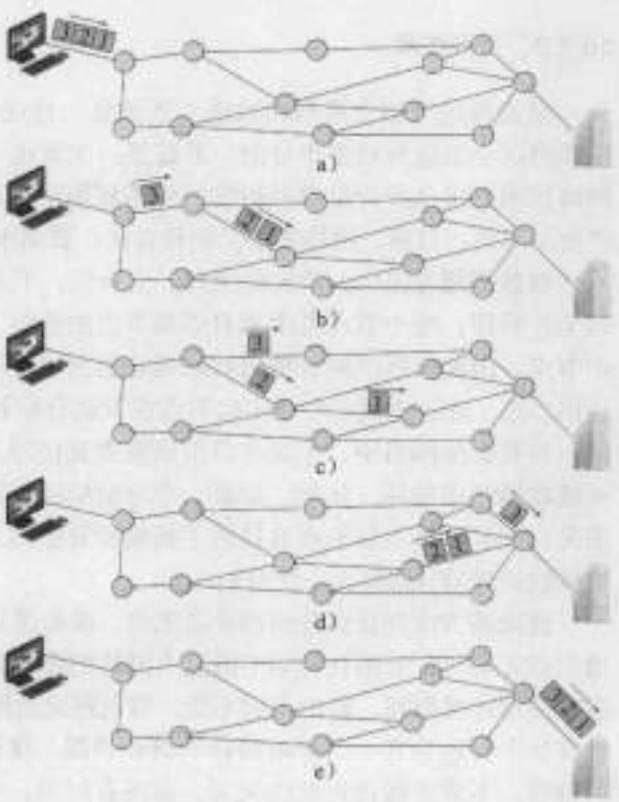


图 15-5　分组交换：数据报方法

与电路交换相比，分组交换方法有许多优势：

- 线路效率较高。这主要是由于单一的节点到节点的链路可以随时间推移，由多个分组动态共享。而且，在链路上分组排队，并尽可能快地传输。与此相反的是，电路交换方法中，节点到节点的链路上时间由同步时分复用（TDM）预先分配，

大部分时间这样的链路或许是空闲的，因为时间的一部分专用于空闲的连接。

- 分组交换网络可以执行数据速率转换。因为每个站以它合适的数据速率连接其节点，所以具有不同数据速率的两个站能够交换分组。
- 对于电路交换网络，当流量变大时，一些呼叫会被阻塞。就是说，网络拒绝接受额外的连接请求直到网络负载减小。对于分组交换网络，在网络流量增大的情况下，分组仍然可被接收，但传输延迟会增加。
- 可使用优先级。如果一个节点有许多分组在排队等候传输，分组交换网络可以首先传送高优先级的分组。这样，与低优先级的分组相比，高优先级的分组经历的延迟小。

相对于电路交换，分组交换也有一些不足之处：

- 当分组通过分组交换节点时，会遭受传输延迟，这在电路交换节点中不存在。最低限度，分组经历的传输延迟为分组的长度（位数）除以接收信道速率（位/秒），这是吸纳分组到内部缓冲区所需要的时间。另外，可能有节点处理和排队带来的可变延迟。
- 由于在某一源和目的之间的分组可能长度不同，所以采用不同的路由，遭受所遇交换机的可变延迟，整个分组的延迟可能发生实质性的变化，这种现象称为**抖动**。对于某些应用来说，比如电话语音和实时视频之类的实时应用，抖动现象是不期望存在的。
- 为了实现网络中分组路由，包括目的地址和序列信息在内的开销信息必须添加到每一个分组中，这一机制减少了用于携带用户数据的可用通信容量。在电路交换中，一旦建立了电路，不需要添加任何额外的开销信息。
- 与电路交换相比，在每一个节点，分组交换的信息传输涉及的处理过程多。对于电路交换，一旦建立了电路，在每个交换机几乎没有任何处理。

15.3.2　交换技术

站点通过分组交换网络发送一条消息，且这条消息的长度大于最大分组的长度。因此，需要将这个消息分成多个分组，并按照一次发送一个分组的方式把这些分组发送到网络。当网络试图路由这些分组流并把它们传送到期望的目的地时，在网络如何处理这些数据流方面产生了问题。目前，网络使用了两种方法：数据报（datagram）和虚电路（virtual circuit）。

在**数据报**方法中，单独处理每一个分组，不参考以前转发的分组。图 15-5 给出这种方法的工作原理，每个节点考虑来自邻居节点的流量、线路故障等，选择某个分组路径上的下一个节点。因此，每个拥有相同目的地址的分组并不是都遵循同一路由，它们或许不按顺序到达出口点。在这个例子中，出口节点在发送分组到目的地时，把分组恢复为它们的原始顺序。在一些数据报网络中，不是出口节点负责重排序工作，而是由目的主机完成。因此，分组有可能在网络中损坏。比如，如果一个分组交换节点瞬间崩溃，它缓存的数据分组队列可能会丢失。而且，由出口节点或目的主机检测分组的丢失并决定怎样恢复。在这种技术中，每个被单独处理的分组称为一个分组。

虚电路方法在任意分组被发送之前，首先建立一个预先规划的路由。一旦路由建立完毕，通信双方的所有分组在网络中沿这个同样的路由传送，其原理在图 15-6 中给予说明。由于在逻辑连接持续期间，路由固定不变，与电路交换网络中的电路有些相似，所以被称为虚电路。现在每个分组包含一个虚电路标识符和数据，在预先建立的路由上每个节点知道把分组导向的位置，不需要做任何路由决策。在任意时刻，每个站可以有一条以上的虚电路与任意其他的虚电路相连，可以有虚电路与多于 1 个的站相连。

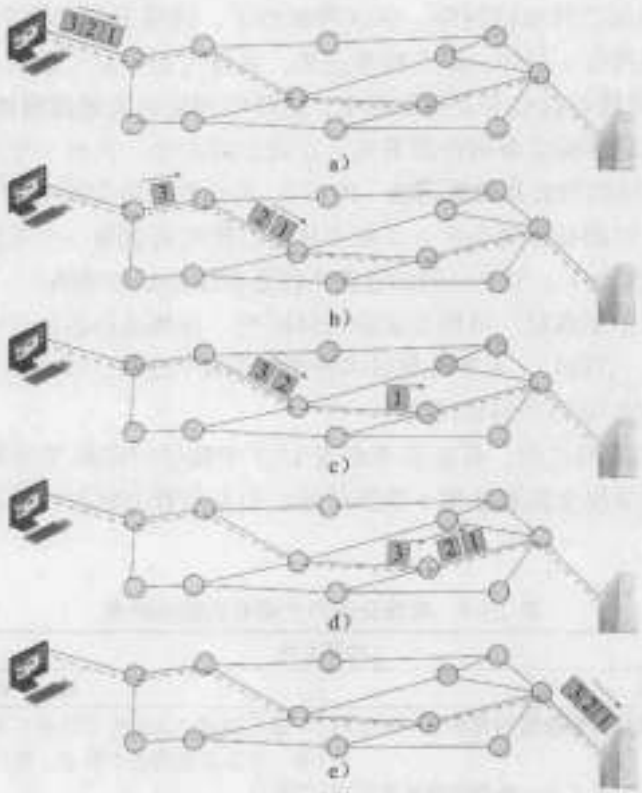


图 15-6　分组交换：虚电路方法

因此，虚电路技术的主要特征是在数据传输之前，预先建立站之间的路由。这里值得注意的是，这并不意味着这是电路交换中的专用路径。分组仍然要在每个节点缓存，在线路上排队等待输出。虚电路方法与数据报方法的差异是不需要为每个分组做路由决策，只需要为使用虚电路的所有分组做一次路由决策。

如果两个站之间希望在扩展的时间段内交换数据，这时虚电路方法具有一定的优势。首先，网络可以提供与虚电路相关的服务，包括排序和差错控制。排序是指这样的事实：因为所有分组沿同一个路由传送，它们以初始的排序到达。差错控制是一种不仅确保分组以适当的顺序到达，而且确保所有分组正确到达的服务，例如，从节点 4 到节点 6 的序列中某分组不能到达节点 6，或者带有错误地到达，节点 6 可以请求来自节点 4 的分组重发。另一个优势是使用虚电路时，分组在网络中传输比较快，没有必要在每个节点为每个分组做路由决策。

数据报方法的一个优势是避免了呼叫建立阶段，因此如果一个站仅想发送一个或几个分组，数据报发送将是比较快的。数据报服务的另一个优势是由于它比较原始，所以它比较灵活。例如，如果网络的一部分设计了拥塞控制，进入的数据报可能被路由拥塞。对于使用虚电路的情况，所有分组沿一个预先定义的路线，因此网络很难适应拥塞。第 3 个优势是数据报发送本质上比较可靠。对于虚电路，如果一个节点失败，通过那个节点的所有虚电路将消失。对于数据报，如果一个节点失败，随后的分组可以发现其他的路由，以绕过那个节点。

15.4　传统广域网实例

正如有公共和私有的电路交换网络一样，也有公共和私有的分组交换网络。公共分组交

换网络的工作机制很像公共电话网络。在这种情形下，网络为各种用户提供分组传送服务。典型地，网络提供商拥有一系列分组交换节点集，并使用运营商（比如，美国电话电报公司AT&T）提供的租用线路将这些节点链接起来，这样的网络称为**增值网络**（VAN），其很好地反应了网络增加了基础传输设备的价值事实。在许多国家中，只有一个由政府拥有或控制的公共网络，这样的网络称为**公共数据网络**（PDN）。其他的分组交换实例专用于单一组织需求的网络，这个组织可以拥有分组交换节点或者从网络提供商租用一个完整的专用分组交换网络。在上述任何一种情况下，节点之间的链路再次是租用的电信线路。

因此，企业往往面临满足广域网需求的选择阵列，这些选择包括许多高速选项，比如帧中继和异步传输模式（ATM）。本节将探讨多种传统 WAN 选项，以得到涉及折中类型的一些感觉。这些问题将在第 16 章中再次讨论。

在开始评估这些实例之前，有必要考虑表 15-1 中提供的电路交换和分组交换的总体分析。虽然电路交换和分组交换都能用于数据传输，但是每种方法对于某种应用而言，具有自己特殊的优点和弱点。

表 15-1　电路交换和分组交换的优缺点

电路交换	
优　点	缺　点
兼容语音。使用同一网络传输数据和语音，可以实现规模经济 语音和数据的呼叫过程具有共性，处理数据流量不需要特殊的用户训练和通信协议 数据流量的速率可预测，而且是固定的	遭受拥堵。这使得难以适当地量化网络。由于使用动态、非层次化的路由技术，所以这个问题变得不是特别严重 需要用户兼容性。因为电路是透明连接的，所以电路每个终端的设备必须在协议和数据速率方面兼容 大量处理和信号负担。对于事务型应用，数据呼叫持续时间比较短，需要瞬间建立，这按比例增加了网络开销负担
分组交换	
优　点	缺　点
提供速率转换。具有不同速率的两个相连设备可以交换数据，网络缓存数据并以合适的数据速率传送 无阻塞。随着网络负载的增加，延迟增大，但通常允许新的交换 高效利用。交换机和干线按需使用，而不是专门用于某个呼叫 逻辑的多路复用。一个主机系统通过唯一线路可同时与多个终端会话	复杂的路由与控制。为了实现效率和弹性，分组交换网络必须使用一套复杂的路由和控制算法 延迟。延迟是负载的函数，这个延迟可能比较长，而且是变化的

15.4.1　语音广域网

传统地，对于广域语音通信，偏爱的业务实例都使用电路交换。随着近年来日益增加的竞争和技术发展，管理者有许多电路交换网络替代品，包括私有网络、软定义网络、普通电话服务和各种特殊服务，如免费数字。

对于这些所有选择，由于各种选择的价格经常变化，所以很难泛化。可以说业务紧密依赖于公共电话网络和相关的服务。私有网络适用于拥有许多分支机构，且分支机构之间有实质性语音流量的组织。

在竞争中，一个新的项目是 IP 语音（VoIP），它使用通过因特网的数据传输方法。VoIP 作为一个替代，正渐渐获得越来越多的接受。15.5 节讨论 VoIP 的相关知识。

15.4.2　数据广域网

对于数据流量，可选的广域网络数目甚至更多。粗略地，我们列举下面几种作为替代：

- **公共分组交换网络**。美国有许多这样的公共分组交换网络，而且大多数工业化国家至少有 1 个。典型情况是，从用户的计算设备到最近的分组交换节点，用户必须租用一条线路。
- **私有分组交换网络**。在这种情形下，用户拥有或租用分组交换节点。而且通常情况下，这些节点与用户的数据处理设备搭配连接。使用租用线路，典型情况是使用 56Kbps 或 64Kbps 数字线路，实现这些节点的互连。
- **私有租用线路**。在两个站之间使用专有线路，不需要任何交换，只需要在希望交换数据的任意一对站点之间存在一个租用的线路。
- **公共电路交换网络**。随着调制解调器或交换式数字服务的使用，用户可以使用拨号电话线实现数据通信。
- **私有电路交换网络**。如果用户通过租用 56Kbps 的线路或 T-1 线路，拥有互连的数字专用交换机（PBX）集合，那么这个网络能够承载数据以及语音。
- **综合业务数字网**（ISDN）。ISDN 以综合服务的形式，提供分组交换和传统的电路交换。

在语音流量的基础上最后两种替代才有可能被合理说明，数据流量仅仅作为出自这种网络的一点奖励。由于这种方法不能直接与其他方法相比较，所以本章不再进一步考虑。

对于语音，选择数据网络的方法十分复杂，并依赖于当前的价格。在比较各种广域数据网的选择时，我们首先考虑比较容易量化和分析的成本和性能，接下来考虑选择网络时也比较重要的一些其他问题。

1. 成本 / 性能考虑

数据通信流量可大致划分为两种：流和突发。流式流量的特征是长时间、相对连续的传输，常见的例子是文件传输、遥测、其他种类的批数据处理应用和数字化的语音通信。突发流量的特征是持续时间短、间歇性的传输。交互式的客户机 / 服务器流量，如事务处理、数据录入和时间划分，具有突发流量的特点。同时，传真发送也是突发性的。

公共电路交换网络方法利用拨号线路，成本基于数据速率、连接时间和距离。正如我们所说，对于突发流量，公共电路交换网络是十分低效的。然而，对于临时性的面向流的需求，这种方法是非常合适的选择。比如，一个公司有分布在其他地方的办公室。在工作一天快要结束的时候，每个办公室需要传送文件到总部，报告这一天的活动。对于来自每个办公室的单一传输，使用拨号线路是非常具有成本效益的方案。当多个办公地址之间有大容量的流式流量时，非常经济的方案是在各个办公地址之间获得专用电路。这些电路也称为租用线路或半永久电路，可以从电信提供商（比如，电话公司）或卫星提供商那里租用。专用电路的成本基于数据速率保持固定不变，有些情况下基于距离计算成本。如果传输流量足够高，则线路的利用率将非常高，使这个租用线路的方法非常有吸引力。

另一方面，如果流量主要是突发性的，那么分组交换网络具有优势。而且，分组交换网络允许不同数据速率的终端与计算机端口互连。如果流量主要是突发性的，而且对于组织而

言流量的容积相对适度，那么公共分组交换网络提供了最佳解决方案。在这种情况下，网络为具有适度流量需求的各种用户提供分组传送服务。如果有许多不同的用户，总流量非常高足以导致高利用率。因此，从提供商的角度来看，公共网络是具有成本效益的。用户得到了分组交换网络的优势，同时没有固定的实现和维护网络的成本，用户的成本是基于连接时间和流量大小，而不是基于距离。

如果组织的突发流量大，且集中在一些小数量的站点，那么私有分组交换网络是最好的选择。对于站点之间有许多突发流量，私有分组交换网络提供了非常好的利用率，而且比电路交换或简单专用线路成本低，私有网络的成本仅仅是基于距离计算。因此，私有网络结合了公共分组交换网络的效率和专用电路的时间和流量独立性。

2. 其他考虑

除了成本和性能问题之外，网络选择也应该考虑控制、可靠性和安全要素。当一个组织足够大，需要广域数据网时，将会严重依赖那个网络。因此，管理能够维护网络的适当控制并能够为用户提供高效率、有效益的服务是十分重要的。在第六部分中，我们将以比较多的篇幅探讨这个主题。在本节中，为了我们的目的，我们能够说在比较各种网络方法时，策略控制、生长控制和网络连续运行 3 个方面的控制是非常重要的。

策略控制涉及为了满足组织独特需求的设计和实现网络的过程。对于公共分组交换网络，用户虚拟上没有对服务水平、可靠性或维护的策略控制，网络意在作为一个公共工具服务于大多数一般客户。对于专用线路或私有分组交换网络，用户组织能够决定他希望支付的容量和冗余级别。**增长控制**允许用户规划由于他们需求的变化而带来的网络扩展和修改，私有分组交换网络在增长需求方面提供了极大的灵活性，额外的分组交换节点、更多的干线和高容量干线能够根据需求增加，这些可提升网络的整个容量和可靠性。虽然在专用线路设计方面，用户有对线路数量和容量的控制，但在日益庞大的网络增长方面灵活性较差。而且，对于公共分组交换网络，用户没有对网络的增长控制。仅仅当用户需求碰巧在公共网络的能力范围内时，用户需求得到满足。关于**连续运行**，用户关心流量高峰时的容纳能力以及错误的快速诊断和修复。分组交换网络能够使用集中化的、有效的网络控制来进行设计，以便允许调整网络以适应变化的条件。当然，在公共网络下，用户依靠网络提供商来实现连续运行。与任意的公共工具一样，比如传输系统，当服务水平下降时公共网络倾向于是高峰时段。对于专用线路，连续控制很难实现自动化。由于我们不是在处理一个统一的网络，所以可用的工具也比较少和原始。

分组交换网络的内在可靠性比专用线路集合高。网络由共享的设备集合组成，而且配以集中化的、自动化的网络控制设备。错误容易被发现和隔离，流量可以转移到网络的健康部分。公共网络可以在冗余和控制工具方面给予较大的投资，这主要是由于成本分散给许多用户。而且，用户不需要培养保持大的数据通信网络运行的技能，从这个重担中解脱出来。

最后，对于大多数公司而言，**数据安全**是非常重要的。我们在第六部分详细探讨了这个主题。为了现在讨论的目的，我们可以说私有网络或专用线路的使用将明显地比公共分组交换网络更安全。公共网络能够使用各种访问控制机制来限制用户跨网络获得数据的方式。由于组织希望隔离各种用户群体，所以那些同样的控制机制在私有网络中是有用的。

表 15-2 总结了各种通信方法的差异。

表 15-2　广域网的特征

特　征	专有（租用线路）	公共分组	私有分组
策略控制	网络设计、服务和维护能够给予优先级，并可由用户控制	服务局限于满足一般的客户	网络设计、服务和维护能够给予优先级，并可由用户控制
增长控制和运行控制	非集成的；昂贵的非集中化容错检测	由服务供应商提供的，满足一般需求	集成到所有设备，集中化容错隔离和检测
可靠性	从故障中人工和用户可见的方式恢复	从故障中透明和自动地恢复	从故障中透明和自动地恢复
安全	只有私有用户	公共用户，网络访问控制	只有私有用户，网络访问控制

15.5　IP 语音

在本书中，我们已经多次提及使用基于 IP 的网络实现数据、语音及视频传输聚合的趋势。这个聚合使得以非常低的成本，为居民用户、多种规模的企业用户和服务提供商推送高级服务成为可能。而且，这个聚合背后的关键技术之一是 IP 语音（VoIP），这个技术在各种规模的企业中已经变得越来越流行。

本质上，VoIP 通过基于 IP 的网络传输语音。主要通过信息编码技术，将语音信息编码成数字格式，以离散分组的形式在 IP 网络中传输。与传统电话相比，VoIP 有两个主要优势：

1）通常情况下，VoIP 系统的运行成本比使用 PBX 的等价电话系统和传统电话网络服务的成本低，这主要归功于几个原因。一是 VoIP 使用分组交换，允许传输容量共享，而传统电话网络使用电路交换为语音通信分配专用电路。而且，分组的语音传输能很好地适应 TCP/IP 协议族，使得应用层和传输层协议能够用来支持通信。

2）VoIP 容易与其他服务集成，如通过单个 PC 或终端将 Web 访问与电话特征结合。

15.5.1　VoIP 信令

在能够使用 VoIP 传输语音之前，必须放置一个呼叫。在传统电话网络中，呼叫者输入被叫号码的数字，然后提供商的信令系统处理电话号码，以使被叫者的电话响铃。对于 VoIP，呼叫用户（程序或个体）提供统一资源标识符（URI，URL 的一种形式）形式的电话号码，接着呼叫号码触发导致呼叫放置的协议交互集。

VoIP 呼叫放置过程的核心是 RFC 3261 中定义的会话发起协议（Session Initiation Protocol，SIP）这是一个用于 IP 数据网络的参与者之间建立、修改和终止实时会话的应用层控制协议。

图 15-7 说明了 SIP 组件之间的关系和使用的协议。用户代理（alice）使用 SIP 与充当服务器的用户代理（bob）建立会话，这个会话发起对话使用 SIP，而且涉及 1 个或多个代理服务器来转发两个用户代理之间的请求和响应。代理服务器组件主要起路由的角色，意味着它的主要工作是确保请求被发送到较接近目标用户的另一个实体。同时，代理对于实施策略也是有用的，如确保允许一个用户拨打电话。另外，用户代理也利用用于描述媒体会话的会话描述协议（Session Description Protocol，SDP）。

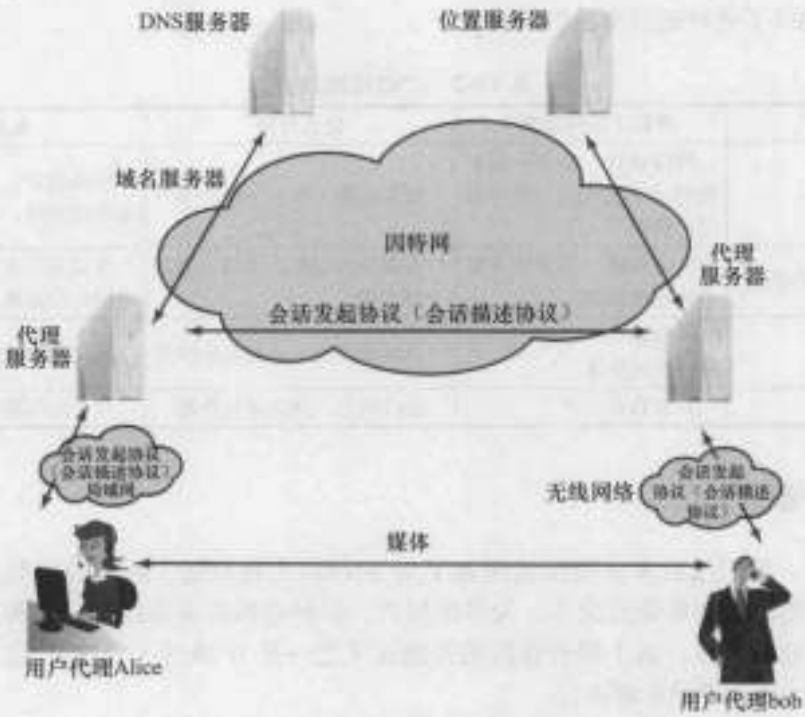


图 15-7　SIP 组件和协议

代理服务器或许需要确定被叫设备的地址，如果是这样的话，代理服务器咨询位置服务数据库。DNS 组件也是 SIP 操作的一个重要部分，典型情况是呼叫者使用被叫代理的域名产生请求，而不是使用被叫代理的 IP 地址，这时代理服务器需要咨询 DNS 服务器以发现面向目标域的代理服务器。

与 SIP 相关联的是在 RFC 4566 中定义的 SDP。SIP 用来邀请一个或多个参与者到会话中，而 SIP 消息的 SDP 编码的实体包含双方能使用和将要使用的媒体编码（比如语音、视频）信息。一旦这个信息被交换和应答，所有参与者都会意识到参与者的 IP 地址、可用的传输能力和媒体类型。然后使用合适的传输协议，开始传输数据。典型地，使用后面将要描述的实时传输协议（RTP）。在整个会话中，参与者能够使用 SIP 消息对会话参数做一些改变，包括会话的新媒体类型或新参与方。

15.5.2　VoIP 处理

被叫方一旦响应，即可在双方之间建立逻辑连接，可以双向交换语音数据。如果是会议电话，则在多方之间建立逻辑连接。图 15-8 说明了 VoIP 系统一个方向的语音数据的基本流程。在发送方，模拟语音信号首先被转换成数字位流，并被分成分组。然后，使用 RTP 协议执行分组。这个 RTP 协议包括分组标记机制，以便于在接收端以合适的顺序重组分组。另外，这个协议还有用于平滑接收和以连续流传送语音数据的缓存功能。下一步使用用户数据报协议（UDP）和 IP 协议，通过因特网或私有因特网传输 RTP 分组。

在接收端，过程正好与发送端相反。使用 RTP 协议重组数据，并以适当的顺序排序。然后，数据解压缩，数字化的语音由数字模拟转换器处理以产生模拟信号，并传送到接收者的电话或耳机扬声器。

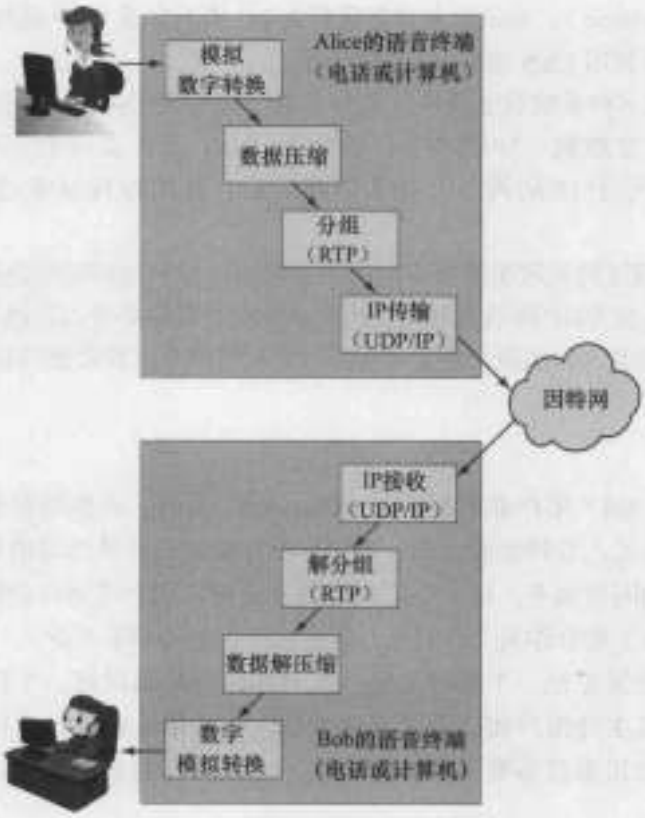


图 15-8　VoIP 处理

15.5.3　VoIP 上下文

最终，使用基于 IP 网络的 VoIP 可以替换今天使用的公共电路交换网络。但是对于可预见的未来，VoIP 必将与现存的电话基础设施共存。图 15-9 表明新老技术共存涉及的一些关键元素。

VoIP 基础设施的部署由以下各种终端用户产品伴随：

- **传统电话**：这些有绳或无绳电话非常像传统电话，但具有 VoIP 电话功能。它们有许多典型的额外特征，利用屏幕并提供智能移动电话的功能。
- **会议（conferencing）单元**：这些单元提供传统会议呼叫语音系统的相同基本服务，也允许用户协调其他的数据通信服务，如文本、图形、视频和白板。
- **移动单元**：智能电话和其他具有 VoIP 能力的手机电话能够直接接入 VoIP 网络，不需要通过任意种类的网关系统。



图 15-9　VoIP 上下文

- **软电话**（softphone）：术语软电话指运行在 PC 机上实现 VoIP 的软件。典型地，PC 机配有耳机或者利用 USB 连接到 PC 的电话。

目前，已经开发多种基础设施设备以支持 VoIP，这里我们提及两种值得注意的类型：

- **IP 专用分支交换机**（IP PBX）：设计 IP PBX 用来支持数字和模拟电话，使用 VoIP 连接到基于 IP 的网络，如果需要的话，使用传统技术连接到公共交换电话网络。
- **媒体网关**：媒体网关用来连接不同的物理网络以提供端到端的连接。媒体网关的一个重要类型是连接 VoIP 网络到电路交换电话网络，提供必要的转换和信令。

VoIP 环境继续随着为提供商、企业和居民 / 个人用户开发的大量产品而演化发展。

15.6　存在

任何即时消息（IM）用户都熟悉存在（Presence）服务，在他的好友列表中以显示某人是否在线的小图标形式，看到他的证据。不过，存在服务已经从即时消息和相似应用的支持特征演化到一个基础网络服务，这个基础网络服务受到应用和电话在内的公司通信服务的敲击（tapped）。对于员工的合作与交流方式，存在服务正变得必不可少。

充分实现的存在服务是一个实时通信、消息和路由基础设施，不仅支持用户对用户交互的合作应用，而且支持用户和应用之间的通信。存在服务也支持应用对应用的集成，据此存在基础设施可以用来宣布哪一个应用在线，它们的功能是什么，它们接收的协议类型是什么。

本节的讨论基于因特网工程任务组（IETF）在几个 RFC 文档中定义的存在服务规范，RFC 2778 定义了用于描述提供存在信息系统的模型和术语，RFC 2779 定义了存在协议必须实现的需求。

15.6.1　存在服务结构

存在系统允许用户彼此订阅，相互通知状态变化。存在服务有两种客户端：存在实体和观察者。任意实体可以担当一种或两种类型的客户端状态。

存在实体（presence entity）为存在服务提供存在信息。通常，存在服务内没有定位存在实体，仅有存在实体的存在信息的最近版本。存在实体发起存在信息的变化，而且这些信息由存在服务发布。

观察者向存在服务请求获取存在实体的存在信息，或者自身的观察者信息。观察者信息由已经收到关于某一实体最近一段时间范围内存在信息的观察者的信息组成。观察者信息由存在服务维护，这个服务能够选择与存在信息同样的形式存在。就是说，服务能使观察者看起来像一种特殊的实体形式。RFC 2778 定义了 3 种类型的观察者：

- **获取者**：获取者发挥主动角色的作用，向存在服务请求某一存在实体的存在信息当前值。这个角色与希望知道在某一时段内另一用户、应用或服务是否可用的用户相对应，与希望知道用户、应用或服务的相关存在信息的用户相对应。
- **轮询者**：轮询者是一个具体类型的获取者，它有规律地获取信息。
- **订阅者**：订阅者使用存在服务来即时通知一个或多个存在实体的存在信息变化，用户可以使用这个角色来请求通知另一用户、应用或服务可用的时间。

图 15-10 给出存在服务的通用模型。除了观察者和存在实体外，模型还包含下面一些关键组件：

- **主体**（principal）：指单个的人、程序，或人与程序的集合体，或者选择对存在服务看起来像单一演员、不同于其他主体的人或程序。主体使用存在系统作为协调和通信的手段。
- **用户代理**：指主体与存在系统交互的手段。用户代理是实现存在协议的软件，使代理能够以主体的名义唤起存在服务。
- **存在服务**：接收、存储和分发系统中存在服务得知的存在实体的存在信息。

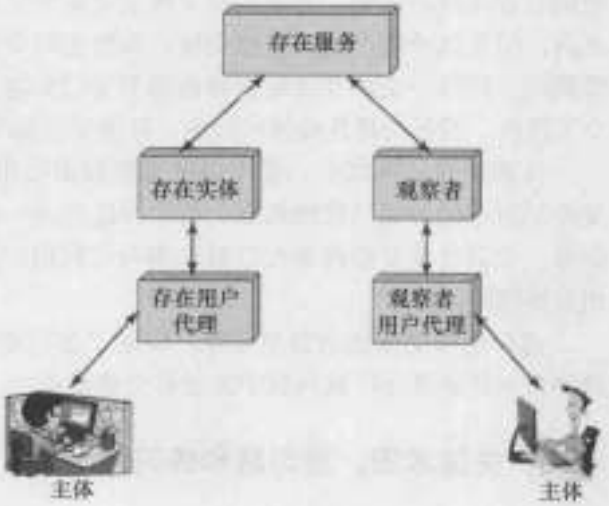


图 15-10　存在服务元素

这里给出存在服务的一个使用例子。部门经理希望在一天开始与任务领导者进行电话会议，以协调需要采取的合作行动。这个会议不是很紧急，而且还没有安排。因此，部门经理请求当所有任务领导者空闲时被告知。

15.6.2　存在信息

存在信息与系统中每个存在实体相关联，由存在服务维护。存在用户代理使用存在协议，将存在实体状态的任意变化传送给存在服务。

存在信息由两个元素组件组成：

- URL：存在实体的统一资源标识符。
- **存在元组**：特征化存在实体信息的一个或多个元组。

存在元组的数目是可变的，考虑了与某一用户相关联的多个存在属性。每个元组包括 STATUS（状态）标记，传送如在线 / 离线、忙、离开、勿扰等信息。存在元组也可以包括说明通信手段的 COMMUNICATION ADDRESS（通信地址），比如电话号码、电子邮件地址、共享云元素的统一资源标识符 URL（例如文件或文件夹），或者其他的联系和通信方式。最后，存在元组可以包含其他存在标记（OTHER PRESENCE MARKUP）元素，用以包含其他的相关信息，样例包括优先级、元组最近 1 次发生变化的时间、存在实体从事的活动、物理位置、通信是否可能是私有或被其他人观察到以及各种其他参数。

因此，存在信息结构允许组织创建面向简单合作和通信任务，提供基本信息的存在系统，或者创建更加复杂的方案，以支持高级的合作和通信应用。

15.7　总结

对于信息通信，直接使用点对点链路是不切实际的，除非非常有限的需求。为了成本 - 效益和实用的信息通信，需要某一种类的通信网络。在一栋大楼或楼群范围之外的通信，要使用广域网（WAN）。在广域网中，使用的两种基本技术是：电路交换和分组交换。

电路交换应用在公共电话网络中，是建立在租用线路之上、使用现场（on-site）电路交换的私有网络的基础。开发电路交换主要是为了处理语音流量，虽然处理数字化数据的效率不高，但也能处理。对于电路交换，需要在两个站之间建立专用路径供通信使用。在连接持续期间，网络中交换和传输资源被保留专门为这个电路使用。而且，连接是透明的，一旦建立了连接，看起来像是连接的设备，好像是直接的连接。

在数据通信网络中，使用分组交换提供使用共享设备的一种有效方式。对于分组交换，交换站以小的分组块传输数据，每个分组包含一部分用户数据加上网络正常运营需要的控制信息。公共分组交换网络可以被许多独立的用户团体共享，这种技术也可以用于建立私有分组交换网络。

选择电路交换还是分组交换，取决于多种考虑，包括成本、性能、可靠性和灵活性。这两种技术将继续是广域网络中的重要交换技术。

15.8 关键术语、复习题和练习题

关键术语

circuit switching（电路交换）
control signaling（控制信令）
datagram（数据报）
exchange（交换）
local loop（本地回路）
packet（分组）
packet switching（分组交换）
presence（存在）
Public Data Network（PDN，公共数据网）
subscriber（用户）
subscriber line（用户线路）
subscriber loop（用户环路）
trunk（干线）
Value-Added Network（VAN，增值网络）
virtual circuit（虚电路）
Voice over IP（VoIP，IP 语音）

复习题

15.1 在网络中每对站之间，为什么有一条以上的可能路径是有用的？

15.2 对于交换式通信网络，判断下面的句子是正确还是错误：

a. 所有交换节点都连接到其他每个节点。

b. 交换节点之间的链路使用复用技术。

c. 交换节点提供面向单一终端局的连接。

15.3 在公共通信网络中，4 个通用的结构组件是什么？定义每个术语。

15.4 对于电路交换，回答下面语句是正确还是错误：

a. 在数据传输之前，必须完成端到端的完整连接。

b. 有 3 个基本的阶段：连接建立、数据传输和连接终止。

c. 电路交换是非常有效的。

15.5 驱动电路交换网络设计的主要应用是什么？

15.6 解释数据报和虚电路操作的差异。

15.7 私有网络的优势是什么？

15.8 对于数据传输，使用电路交换网络的限制是什么？

15.9 什么是增值网络？

15.10　VoIP 的优势是什么？

15.11　简要描述 VoIP 应用中 SIP 和 SDP 的角色。

15.12　识别和简要描述存在服务的主要特点和组件。

练习题

15.1　你的企业或家离你的本地交换中心有多远？

15.2　在公共交换式电话网络中，基于所拨的号码建立呼叫并交换。事实上，这些号码给交换中心提供不同频率的声音或音调。这个信令叫做什么？

15.3　发现和看几个 YouTube 视频，以比较电路交换和分组交换。针对你认为做了特别好工作的至少 3 个视频识别 URL，解释和说明电路交换和分组交换的差异。如果你必须选择仅仅一个视频推荐给业务数据通信专业的学生，你将选择哪一个？为什么？

15.4　考虑一个简单的电话网络，由两个终端局组成，在每个终端局和中间交换机之间存在 1MHz 全双工干线（trunk）的中间交换机。电话的平均使用情况是，每 8 小时工作日呼叫 4 次电话，每个呼叫的平均持续时间是 6 分钟，且 10% 的电话是长途。终端局能支撑的最大电话数目是多少？

15.5　做因特网调查，比较分组交换网络中的数据报方法和虚电路方法。识别使用数据报方法且执行性能可接受的几个业务数据通信应用，同时也识别比较适合于虚电路方法的几个业务应用。

15.6　分组交换网络支持临时的和永久的虚电路，其中临时的虚电路也叫做交换式虚电路。对有关交换式和永久虚电路方法的差异展开因特网调查，并识别应用在业务数据通信网络中的应用类型的例子。

15.7　给定具有 N 个节点的分组交换网络，其中的 N 个节点由以下拓扑连接：

a. 星形：一个没有站点相连的中心节点，所有其他节点连接在这个中心节点。

b. 环形：每个节点连接在两个其他节点，以形成闭环。

c. 全连通：每个节点直接连接在所有其他节点。

15.8　针对无线电话网络中使用的交换技术，展开因特网调查。无线电话网络是电路交换式网络的例子吗？为什么是或为什么不是？以 500 – 570 字的论文形式给出你的决策理由。

15.9　随着业务网络中有源以太网（PoE）的部署增加，VoIP 的普及度大大增加。开展因特网调查，集中在这些系统能够怎样平行地演化发展以及共同演化的原因，并把调查结果写成 500 – 570 字的论文或 5 – 8 页幻灯片。

15.10　针对 SIP 和 SDP，集中在其每个支持的服务范围展开因特网调查，解释这些协议在统一通信中是怎样使用的，以及混合 VoIP 和存在服务。最后，把调查结果写成 500 – 570 字的论文或 8 – 12 页幻灯片。

第 16 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

广域网服务

学习目的

通过本章的学习，读者应该能够：

- 讨论对广域网络的兴趣日益增长的原因及高速广域网络可用的选择。
- 描述帧中继网络的特征和特点。
- 描述异步传输模式（ATM）网络的特征和特点。
- 描述多协议标签交换（MPLS）和广域以太（WAE）服务的特征和特点。

由于局域网（LAN）的数量和速度无休止地增长，导致对广域分组交换网络的需求日益增加，以支持这些局域网络产生的巨大吞吐量。在广域网络的早期，出现 X.25，用以支持长距离终端和计算机的直接连接。在速度达到 64kbps 时，X.25 能够很好地处理这些需求。随着企业网络中高速局域网的增生，发现用于互连地理位置分散的企业局域网的强健壮性选择的需求很快得到实现。面向广域网的几代高速交换服务已经建立在 X.25 技术基础上，今天已经有许多纳入企业网络的高速可用的广域网服务。

的确，企业网络管理者在解决容量问题时经常面临很多的选择，而且在每种选择上所花费的大量功夫导致方案选择成为一个十分耗时的事情。在本章，我们首先回顾各种广域网络选择，以及它们各自的强势和弱点。接着，我们集中在企业使用的或许是 4 种非常重要的 WAN 服务：帧中继、异步传输模式（Asynchronous Transfer Mode，ATM）、多协议标签交换（Multiprotocol Label Switching，MPLS）和广域以太网（Wide Area Ethernet，WAE）。

在大多数企业网络中，公共互联网经常被用作主要的或次要的 WAN 基础设施，连接分布在各个站点的计算机。目前，企业不存在公共互联网接入的情况越来越少见，这正如我们在前面章节观察到的情况：许多组织已经利用 Internet 技术开发内部网、外部网和虚拟专用网（Virtual Private Network，VPN）。然而，由于本章讨论的各种广域网技术能够对传输速度、应用性能的质量和一致性实施更加直接的控制，许多企业使用他们增补因特网的公共通信基础设施。因此，投资于本章描述的广域网服务的根据与企业为什么投资于第 6 章描述的 T-1 设备或 SONET 服务的原因是相似的。

16.1 广域联网方案

当考虑面向企业或其他组织的广域网络策略时，需要分析两个不同但是相关的趋向。第一个是用于支撑业务应用和通信需求的分布式处理结构，另一个是满足这些需求的可用网络化技术和服务。

16.1.1 WAN 服务

为了满足公司新的计算范例需求，服务和设备提供商已经开发了多种高速服务，这包括

较快速的多址线路方案，比如 T-3、SONET/SDH，以及快速的交换式网络方案，包括帧中继、ATM、MPLS 和 WAE。

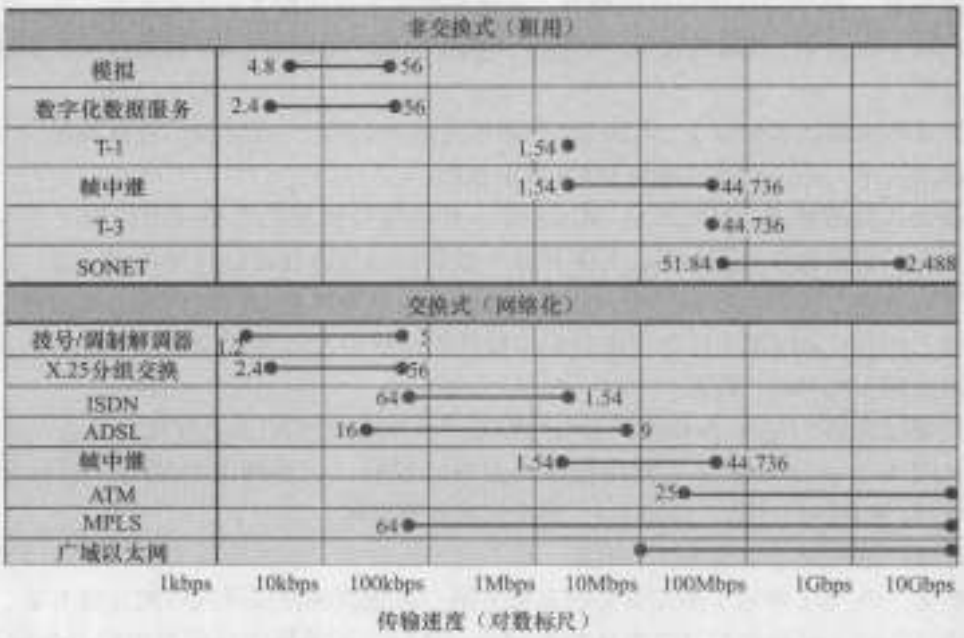


图 16-1　美国运营商的通信服务

图 16-1 展示了来自美国公开运营商的可用的主要选择，在其他国家相似的混合也是可用的。一条非交换式或专用线路是以某一固定价格租来的传输链路，这样的线路可从某一载体供应商处租用，以连接组织的办公室。常见的服务包括以下：

- **模拟**：不太昂贵的选项是租用一条双绞模拟链路，使用专用的私有线路调制解调器，常见的数据速率是 4.8 – 56kbps。
- **数字化数据服务**：要求数字化信令单元而不是调制解调器的高质量数字线路是比较昂贵的，但是能够被以较高的数据速率租用。
- **T-1、T-3**：对于高流量的语音和数据需求，许多年来非常常见的租用线路是 T-1。直到今天，T-1 线路仍然十分流行。对于更高的需求，T-3 线路广泛可用。
- **帧中继**：帧中继是一种交换式网络技术，帧中继协议能够被使用在专用线路，用以提供方便的、灵活的多址技术。对于这种方法，客户的场所需要帧中继设备。
- **SONET**：一些可用的超高速租用线路使用第 6 章讨论的 SONET/SDH。

公共交换式服务包括以下：

- **拨号 / 调制解调**：连接到公共电话网络的调制解调器提供了一种相对便宜的获得低速数据服务的方法。调制解调器本身价格便宜，对于适中的连接时间电话速率是适当的，这是面向居民用户的接近全球通用的访问技术。在一些组织机构，许多局域网和专用分支交换（PBX）配有调制解调器库存，用以提供低成本、增补的数据传输服务。
- **X.25 分组交换**：虽然在北美，这种技术大多数已经被帧中继服务所替代，但这个较老的备用品仍然在世界范围的网络中使用。典型地，X.25 网络基于传输的数据流量收费。
- **综合业务数字网（ISDN）**：ISDN 通过 64kbps 的 B 通道提供电路交换和 X.25 分组交

换，而且较高的数据速率也是可以实现的。典型地，网络收费是基于连接的持续时间，不考虑传输的数据量。

- **帧中继**：帧中继提供交换式能力，其速率等同于租用的 T-1 线路速率，在一些服务场合速率高达 T-3 线路的速率，它的低开销特性使之使用于 LAN 和高速独立系统之间的互联。
- **异步传输模式（ATM）**：从 20 世纪 90 年代到 2005 年，ATM 被广泛认为是一个通用的网络技术，注定替代其他的 WAN 服务选择。
- **多协议标签技术（MPLS）**：MPLS 是一种高度可扩展的数据携带机制。在 MPLS 网络中，数据包被分配标签，并采用基于独特的标签内容的包转发机制。这一方法取消了检查整个包的内容的需求，使得穿越任意传输媒体类型的端到端电路的建立成为可能。而且，MPLS 可以封装来自大多数其他通信协议的数据报文，包括 T-1、帧中继、以太网和数字用户线路。
- **广域以太网（Wide Area Ethernet,WAE）**：WAE 使用以太连接传送高速 WAN 服务。从根本上说，WAE 是一种简化连接远程位置的以太局域网的 VPN，被标记为传统 WAN 服务的替代品，诸如 T-1、租用线路和帧中继。

在各种广域网服务中做选择的确是一件不容易的任务，可供选择的替代品的增生增加了选择的难度。表 16-1 展示了美国常见的定价方案，其他国家使用可比较的定价方案。可以看出，各种服务的定价结构不可以直接相互比较，这是方案选择中需要考虑的复杂问题之一。导致这个选择过程复杂的其他问题还有难以预测广域网用户未来的流量大小，而且由于应用的灵活性和用户移动性的增加，难以预测流量的分布。

表 16-1 广域网络的可供选择（美国定价）

服务	按使用量收费率	按距离收费率
租用线路	对于具体容量，每月价格固定，而且没有额外的使用费用	距离越远，费用越高
综合业务数字网（ISDN）	服务费用每月价格固定，另外加一个基于连接时间的使用费用	应用长途收费
帧中继	对于端口连接，每月价格固定，同时对于永久的虚电路（PVC），使用基于链路容量的统一费用	不按距离收费
异步传输模式（ATM）	定价策略变化	不按距离收费
多协议标签交换（MPLS）	定价策略变化	不按距离收费
营运/电信级以太网	定价策略变化	不按距离收费

16.1.2 WAN 结构的演化

图 16-2a 给出在企业网络中至今仍占据主导地位的 WAN 结构类型，而且这些结构将继续是流行的模型。对于一个典型的配置，客户端所有设备通过同步时分多路复用器输送到高速用户线路，进一步传送到电信运营商。这包括控制电话和传真机、面向语音和传真流量的专用分支交换机，以及到局域网的接口。典型地，局域网接口由第 3 章讨论的路由器和 3 层交换机实现。同时，典型配置中也可能有连接到控制器的许多哑终端和瘦客户端，控制器进一步与多路复用器交换数据。线路本身可能是 T-1 或 T-3，而且随着需求的增加，SONET 链路（比如 OC-1）也变得比较常见。



a）使用专有通道的综合网络访问



b）使用公共交换式广域网的综合网络访问

图 16-2　综合的网络策略

在运营商端，多路复用的流量进一步被拆分为许多租用电路，为客户组成专用网络，实现 PBX、LAN 和在其他位置的大型主机的连接。另外，对于数据流量，运营商能提供连接一个或多个公共高速交换式网络的接口，比如帧中继、ATM、MPLS 或 WAE。最后，典型的配置提供到因特网的连接。

对于企业而言，图 16-2a 的配置是非常有吸引力的，它集成组织所有的语音和数据流量到一条单一外部线路，这大大简化了网络管理与配置。存在的一个缺陷是缺乏相对的灵活性，同步时分多路复用线路的容量被划分成固定的部分，分配给客户端站的各种元素，诸如 PBX、LAN 和终端控制器，如果不使用比较昂贵的统计时分多路复用器，很难根据需求动态分配容量。

随着越来越快的交换式网络的出现，现在有了更加灵活的解决方案，图 16-2b 给出其中的一个例子。在这个安排中，高速外部线路直接连接到公共交换式网络，比如帧中继或 ATM，虚连接被用来建立临时的管道或被用来连接到各个目的地。另外，主要的帧中继、ATM、MPLS 和 WAE 供应商提供所谓的永久虚连接，等同于专用同步 TDM 通道，能够被用来建立专用网络。为了获得最大的灵活性，企业客户可以依赖动态地建立和拆毁的交换式虚拟连接。每当连接建立的时候，为了达到传输某个容量的流量，客户能够配置这个连接。这样随着进出这个网站的语音、数据、图像和视频混合流量的变化，客户能够动态改变容量的

混合配置以提供优化的性能。

在 20 世纪 90 年代早期，大多数企业和大型组织，包括美国的国防部选择帧中继和 ATM 服务作为主要的广域网络实现方法。虽然 ATM 被看作技术上具有优越性，考虑到大安装基础的发展，帧中继仍然继续享有客观的市场份额，这主要是由于它使用的时间较长。MPLS 和 WAE 已经开始抢占 ATM 和帧中继的市场份额，并且工业界评论员预料 MPLS 和 WAE 将压倒 ATM 和帧中继的流行度，在下一个 10 年将被广泛使用。

16.2　帧中继

帧中继在设计之初，被用来提供比传统分组交换更加有效的传输方案。帧中继的相关标准比 ATM 标准成熟得早，而且来自电信运营商和其他提供商的帧中继服务也出现得早。因此，帧中继产品拥有大的安装基础。

16.2.1　背景

传统分组交换的方法使用用户和网络之间知名的 X.25 协议，这个协议不仅确定了用户与网络之间的接口，而且影响网络的内部设计。X.25 方法几个关键的特征如下：

- 用于建立和终止虚电路的呼叫控制包，与数据包在同一通道和虚电路中传输，事实上即是使用的带内信令。
- 虚电路的多路复用发生在第 3 层。
- 在第 2 层和第 3 层包括了流量控制和差错控制机制。

X.25 方法导致相当大的开销，在网络中的每一跳，数据链路控制协议涉及数据帧和应答帧的交换。进一步，在每一个中间节点，必须为每个虚电路维持状态表，以处理呼叫管理和 X.25 协议的流量控制 / 差错控制。当网络中链路发生错误的概率相当高时，所有这些开销可以做出合理解释。这种方法不适合现代的数字通信设施，因为这些设施的链路错误率非常低。今天的网络针对高质量、可靠的传输链路，尤其多数是光纤的情况，使用可靠的数字通信技术。另外，光纤和数字传输的使用实现了高速数据速率，在这种环境下，X.25 的开销不仅是不必要的，而且降低了可用的高容量链路的有效使用。

为了取消 X.25 给终端用户和分组交换网络带来的大量开销，帧中继被设计提出。帧中继与传统 X.25 分组交换服务之间的主要差异如下：

- 用于建立和管理连接信息的呼叫控制信令与用户数据不在同一连接中传输，而是在一个分离的逻辑连接中传送。因此，中间节点不需要以独立的每个连接为基础，维持与呼叫控制相关的状态表或过程信息。
- 逻辑连接的多路复用和交换发生在第 2 层，而不是在第 3 层，取消了一个完整层次的处理工作。
- 取消了逐跳的流量控制和差错控制。如果使用端到端的流量控制和差错控制，这变成较高层的责任。

因此，使用帧中继，发送者的数据帧从源传送到目的地，较高层产生的应答帧可以响应帧的形式传送回来，没有数据帧和应答帧的逐跳交换。

接下来，我们考虑这种方法的优势和劣势。与 X.25 比较，帧中继主要的潜在劣势是丢失了执行逐链路流量和差错控制的能力（虽然帧中继不提供端到端的流量和差错控制，但这一

点很容易在较高层实现）。对于 X.25，单一物理链路上承载多个虚拟电路，链路层协议提供从源到分组交换网、从分组交换网络到目的地的可靠传输。另外在网络中的每一跳，链路控制协议被用来寻求可靠性。使用帧中继取消了逐跳的链路控制，然而由于传输和交换设备不断提高的可靠性，这不再是一个主要的缺陷。

帧中继的优势在于把通信过程简单化，用户与网络接口层需要的协议功能被简化，正如同内部的网络处理，因此达到较低的延迟和较高的吞吐量。一系列研究显示，与 X.25 相比，使用帧中继的吞吐量提高了一个数量级，甚至更高 [HARB92]。国际电信联盟远程通信标准化组织（ITU-T）建议 I.233 显示，帧中继技术在访问速度达到 2Mbps 的场合使用，不管怎样现在已经有更高数据速率的帧中继服务。但是，最终帧中继或许被 MPLS 和 WAE 网络代替。最近的一份市场研究展现出，帧中继服务连接在 2011 至 2016 年期间以每年 2% 的速率增长，2016 年以后随着这些帧中继网络被 MPLS 替换，这些遗留系统将开始衰退。

16.2.2　帧中继协议结构

图 16-3 描述支持帧中继的协议结构。协议有两个分离的操作平面：1）控制平面（C），它涉及逻辑连接的建立和终止。2）用户平面（U），负责用户之间的数据传输。因此，用户与网络之间的是 C 平面协议，而端到端之间则是 U 平面协议。



图 16-3　帧中继用户 – 网络接口协议结构

1. 控制平面

帧中继传输服务的控制平面类似于电路交换服务中的公共通道信号的控制平台，为控制信息提供分立的逻辑通道。在数据链路层，D 通道链路接入规程 Q.921 提供可靠的数据链路控制服务，为用户（TE）和网络（NT）之间进行差错控制和流量控制。数据链路服务用于交换 Q.933 控制信号报文。

2. 用户平面

用于终端用户之间的实际信息传输的用户平面协议是 Q.922 中定义的数据链路层帧方式接入协议（Link Access Procedure for Frame Mode Service，LAPF）。帧中继仅仅使用了 LAPF 的核心功能：

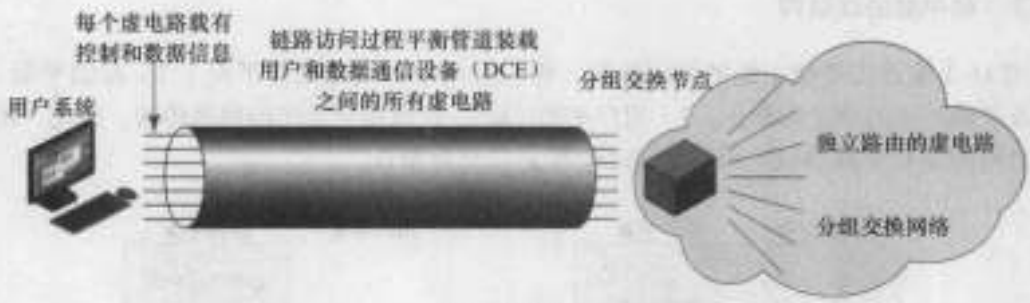
- 帧定界、同步和透明。
- 使用地址域的帧多路复用 / 分用。
- 帧长度检测，确保数据帧不能太长，也不能太短。

- 传输错误检测。
- 拥塞控制功能。

用户平面的 LAPF 核心功能构成了数据链路层的一个子层，提供了用户之间的数据链路帧传输的基本服务，而且没有流量控制或差错控制。在这个子层之上，用户可以选择不属于帧中继服务部分的额外数据链路或网络层端到端的功能。基于这些核心功能，网络提供帧中继就像具有以下特性的面向连接的链路层服务：

- 从网络的一个边沿到另一边沿的帧传输顺序保持。
- 小概率的帧损失。

如同 X.25，帧中继涉及使用逻辑连接，在这种情况下呼叫的数据链路连接而不是虚电路。图 16-4b 强调这些数据链路连接中传输的帧，不能被使用流量和差错控制的数据链路控制管道保护。



a）分组交换



b）帧中继

图 16-4　虚电路和帧中继虚连接

帧中继专门将一个分离的数据链路连接用户呼叫控制，这是 X.25 与帧中继之间的另外一个差异。数据链路连接的建立与拆毁总是通过这个永久的面向控制的数据链路连接执行。

帧中继结构大大减少了网络的工作量，用户数据以帧的形式传输，实质上不需要中间节点的任何处理，除非错误检查和基于连接号的路由。对于错误帧，所采取的动作是丢弃，将错误恢复交给较高层。

16.2.3　用户数据传输

对于用户数据传输，以图 16-5 给出的帧格式开始，解释说明帧中继的操作。帧中继格式与第 6 章描述的 HDLC 之类的其他数据链路层协议相似，删除了控制域这个字段。

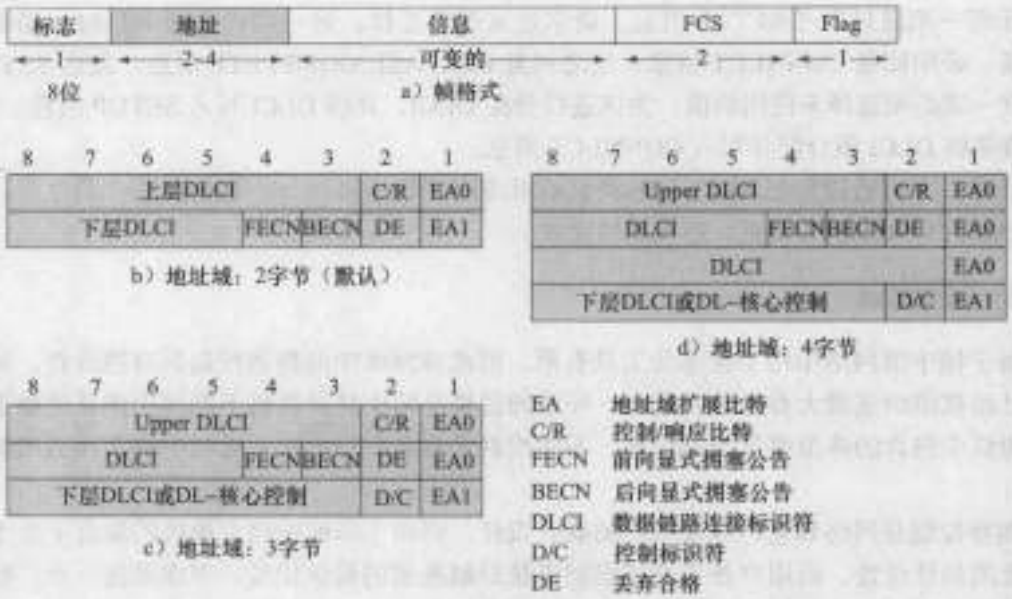


图 16-5　LAPE 核格式

帧中继格式中缺乏控制域，这意味着建立和拆毁连接过程必须在上层的软件执行，通过分立通道实现，同时意味着在数据链路层不可能执行流量控制和差错控制。

标志和帧校验序列（FCS）域的功能如同 HDLC 中的相应字段，标志域是独特的模式，限定帧的开始与结束，FCS 域用于错误检测。传输开始，计算 FCS 校验和，并存储在 FCS 域中。接收到数据后，重新计算一次校验和，并与发来数据帧中存储的值进行比较。如果两个数值不匹配，那么认为数据帧中有错误，作丢弃处理。

信息域携带高层数据，包括用户数据或呼叫控制信息。

地址域有 2 个 8 位字节的默认长度，也可以扩展到 3 或 4 个字节，携带的是 10、16 或 23 位的数据链路连接标识符（DLCI），允许多个逻辑帧中继连接复用单一通道。

地址域和 DLCI 的长度由地址域扩展比特（EA）决定。C/R 比特与具体应用相关，标准的帧中继协议不使用此比特。地址域中其他的比特位必须处理拥塞控制，将在后面给予解释。

16.2.4　帧中继呼叫控制

帧中继呼叫控制过程的实际细节取决于使用的上下文，本章总结帧中继呼叫控制的必要元素。

帧中继支持单一链路的多个连接，且每个连接有本地独特的 DLCI。数据传输涉及以下阶段：

1）在两个端点之间建立逻辑连接，并为这个连接分配独特的 DLCI。

2）以数据帧的形式交换信息，且每一帧包含 DLCI 域以标识连接。

3）释放逻辑连接。

逻辑连接的建立与释放通过专用呼叫控制连接的信息交换实现，这个控制连接的 DLCI=0。DLCI 取值为 0 的数据帧在信息域中包含呼叫控制信息，且至少包括 4 种控制消息类型：建立（SETUP）、连接（CONNECT）、释放（RELEASE）、释放完成（RELEASE COMPLETE）。

任何一端通过发送 SETUP 消息，请求建立逻辑连接。另一端接收到消息时，如果它接受连接，必须回复 CONNECT 信息，反之回复 RELEASE COMPLETE 信息。发送 SETUP 信息的这一端必须选择未使用的值，为该连接分配 DLCI，并将 DLCI 写入 SETUP 消息。否则，由接收端将 DLCI 值分配并写入 CONNECT 消息。

任意一方可通过发送 RELEASE 消息请求清除逻辑连接，另一侧收到这个消息后，回复 RELEASE COMPLETE 消息，连接撤销完成。

16.2.5　拥塞控制

由于帧中继网络中用于拥塞的工具有限，因此该网络中的拥塞控制具有挑战性。帧中继协议已经被组织成最大吞吐量和效率，导致的后果是帧中继交换机不能使用像其他数据链路控制协议中包含的典型流量控制机制，不能控制来自企业用户或邻近帧中继交换机的数据帧流量。

拥塞控制是网络和它的终端用户的联合责任，网络（即帧中继交换机的集合）处于监控拥塞度的最佳位置，而用户处于通过限制流量控制拥塞的最佳位置。考虑到这一点，帧中继支持两种通用的拥塞控制策略：拥塞避免和拥塞恢复。

拥塞避免流程在拥塞发生时使用，以减小对网络的影响。当网络检测到队列长度和拥塞危险时，对于终端用户来说可用的拥塞加剧的证据很少。因此，网络中必须有用于激发拥塞避免的显式信令机制。

拥塞恢复流程在面临严重拥塞时使用，阻止网络瘫痪。当网络因拥塞开始丢弃数据帧时，典型地做法是激发该流程。这些丢弃的数据帧由高层软件报告，用作隐含的信令机制。

对于显式信令，每个帧地址域提供 2 位比特，任何 1 位都可能被检测到拥塞的帧中继交换机置位。如果某一交换机转发的数据帧中 2 个比特的 1 位或全部被置位，就不把这些位清零。因此，这些位构成了从网络到终端用户的信号。2 位的信息如下：

- **后向显式拥塞公告（BECN）**：通知用户对于接收帧的反方向数据流，如果可应用的话，应启动拥塞避免流程。这个比特显示，用户通过这个逻辑连接发送的数据帧会遭遇到拥塞资源。
- **前向显式拥塞公告（FECN）**：通知用户对于接收帧的同向数据流，如果可应用的话，应启动拥塞避免流程。该位显示，通过这个逻辑连接的数据帧已经遭遇到拥塞资源。

当网络丢弃数据帧时产生隐式信令，且这个事实被高层的终端用户检测到。当然，网络的角色是必要时丢弃数据帧，由每个数据帧的地址域中 1 位提供指导：

- **丢弃合格（DE）**：当丢弃帧必要时，显示 DE 位被置 1 的数据帧应该被丢弃，而不是丢弃该位没有置位的数据帧。

DE 的能力使得帧中继用户能够暂时发送更多的帧，可以超出允许的平均值。此情况下，用户将多余帧的 DE 位置位。如果网络具有这个能力的话，将转发这些数据帧。

DE 位也可以被处理帧的帧中继交换机置位。网络能够监控来自用户的帧的流入，使用 DE 位保护网络。也就是，如果与用户直接相连的交换机判断出输入潜在地过多，交换机将每个帧的 DE 位置 1，进一步转发到网络。

利用 DE 位，能够为丢弃决策提供指南，同时作为提供服务保证水平的工具。这个工具在每个数据链路连接的基础上使用，以保证大容量用户能够得到需求的吞吐量，同时不惩罚小容量用户。具体的工作机制为：在连接建立时，每个用户协商承诺信息速率（CIR），即每秒比特

数。请求的 CIR 代表用户对繁忙时间正常流量的估计；准许的 CIR 是出现错误的情况下，网络承诺的数据传输速率，而且准许的 CIR 小于或等于请求的 CIR。接着，用户站连接的帧中继交换机执行测量功能（见图 16-6）。如果用户正在以小于 CIR 的速率发送数据，接收交换机不对 DE 位做任何改变。如果速率超过 CIR，接收交换机将把多余帧的 DE 位置位，然后再转发。如果遇到拥塞，这些 DE 置位的数据帧或许通过转发，或许被丢弃。最后，定义最大速率，使得在帧中继交换机入口超过最大速率的帧就被丢弃。

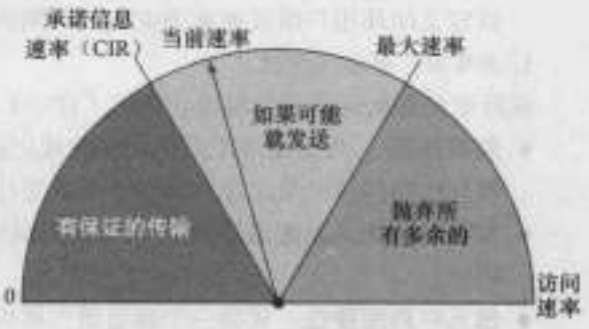


图 16-6　承诺信息速率（CIR）的操作

16.3　异步传输模式

帧中继设计之初，用以支持的访问速度达到 2Mbps。虽然帧中继已经发展到提供 45Mbps 的速度，但仍然不能满足需要成百或成千兆位每秒的广域网访问速度的企业需求。**异步传输模式**（ATM）是适应这种巨大需求的第一批技术之一，这一技术也称作信元中继。

在概念上，信元中继与帧中继相似，这两种方法均利用现代数字设施的可靠性和可信任性，提供比 X.25 速度快的分组交换。在功能上，信元中继比帧中继更简单化，能够支持比帧中继高几个量级的数据速率。

16.3.1　虚通道和虚路径

ATM 是面向包的传输模式，如同帧中继和 X.25，允许一个物理接口复用多个逻辑连接，且每一个逻辑连接的信息流组织成固定尺寸的包，称之为**信元**。与帧中继相同，ATM 的逻辑连接也没有差错控制和流量控制。

在 ATM 服务网络中，逻辑连接称为**虚通道**，这与 X.25 的虚电路、帧中继数据链路连接类似，是 ATM 网络的基本交换单元。虚通道在网络的两个终端用户之间建立，通过这个连接交换可变速率、全双工的固定大小信元流。同时，虚通道也可用于用户 – 网络之间的交换（控制信令）和网络 – 网络交换（网络管理和路由）。

对于 ATM 网络，引入第二个处理子层，包括建立和管理虚路径（见图 16-7）。**虚路径**为拥有同一端点的一批虚通道，因此单个虚路径中所有虚通道中传输的所有信元被一起交换转发。



图 16-7　ATM 连接关系

使用虚路径的优势列举如下：

- **简化的网络结构**：网络传输功能分离为与独立的逻辑连接（虚通道）相关和与一组逻辑连接（虚路径）相关的功能。
- **增加的网络性能和可靠性**：网络处理较少的聚合实体。

- **精简处理和短连接建立时间**：虚路径建立时执行大多数工作，现有虚路径中增加新的虚拟通道涉及最小的处理。
- **增强的网络服务**：虚路径在网络内部使用，同时终端用户也是可见的。因此，用户可以定义闭环用户组或虚通道束的闭环网络。

1. 虚路径 / 虚通道特性

国际电信联盟远程通信标准化组织（ITU-T）的建议 I.150 列出虚通道连接的特点如下：

- **服务质量**：为虚通道用户提供参数规定的服务质量，诸如信元丢弃比率（丢弃的信元数与传送的信元数之比）和信元延迟变化。
- **交换和半永久的虚通道连接**：能够提供需求控制信令的交换连接和所谓的半永久的专用通道。
- **信元序列完整性**：保持一个虚通道内被传送信元的序列。
- **流量参数协商和使用监控**：对于每个虚通道，能够协商用户和网络之间的流量参数，网络能够监控输入虚通道的信元，以保证不违反协商的参数。

在 ATM 网络中，可协商的流量参数类型包括平均速率、高峰速率、突发性和高峰持续时间。网络也许需要许多策略来处理拥塞和管理现有和请求的虚通道。最原始级别的做法是，网络可以简单地拒绝虚通道的新请求，以避免拥塞。另外，如果违犯协商的参数或者如果拥塞情况变得严重了，信元可以被丢弃。一个极端的情形是，可以终止已存在的连接。

I.150 也列出了虚路径的特点，给出的前 4 个特点与虚通道的前 4 个特点相似，也就是服务质量、交换和半永久的虚通道连接、信元序列完整性、流量参数协商和使用监控是虚路径的所有特性。虚路径与虚通道的重复特性有很多原因。首先，为网络如何管理对虚路径的需求提供一定的灵活性。第二，网络必须关注虚路径的全面需求，在一个虚路径内可以协商具有某些特点的虚电路建立。最后，一旦建立了虚路径，对于终端用户而言，协商新的虚通道建立是可能的，虚路径的特点为终端用户可做的选择施加了约束。

另外，虚路径的第 5 个特性列举如下：

- **虚路径内虚通道标识符限制**：对于虚路径的用户，一个或多个虚通道标识符或数字或许不可用，而是留作网络使用，比如用于网络管理的虚通道。

2. 控制信令

在 ATM 网络中，虚路径和虚通道的建立与释放需要一种机制，这个过程中涉及的信息交换称作控制信令，且信息交换发生在与当前被管理的连接分离的连接上。

对于虚通道，I.150 提供了建立和释放设施的 4 种方法，在任意网络中将使用 1 种或这些方法的组合。

1）半永久虚通道可以用于用户对用户的交换。这种情况下，不需要使用控制信令。

2）如果没有预先建立好的呼叫控制信令通道，必须建立。因为这个用于建立信令通道，所以称为元信令通道。

3）元信令通道可用于在用户和面向呼叫控制信令的网络之间建立虚通道。

4）元信令通道也可用于建立用户与用户之间的信令虚拟通道，允许两个终端用户之间在没有网络干预的情况下，建立和释放传输用户数据的用户对用户的虚通道。

对于虚路径，I.150 定义了 3 种方法：

1）根据先前的协议，在半永久基础上建立虚路径。这种情况下，不需要使用控制信令。

2）用户可以控制虚路径的建立 / 释放。在这种情况下，客户使用信令虚拟通道来请求网

络中的虚路径。

3）虚路径的建立 / 释放可以由网络控制。在这种情况下，为了自己的便利，网络建立虚路径，可以是网络对网络、用户对网络和用户对用户。

16.3.2　ATM 信元

ATM 使用固定大小的信元，由 5 字节的头部、48 字节的信息域组成。使用小的、固定尺寸信元具有的优势为：第一，小信元的使用可以减少高优先级信元的排队延迟。如果高优先级信元稍微晚于已经获得资源（比如发送器）访问的低优先级信元到达，它等待时间比较少。第二，固定尺寸的信元交换效率高，这对于 ATM 的非常高的数据速率而言是非常重要的。第三，固定大小的信元易于通过硬件实现交换机制。

图 16-8a 给出用户 – 网络接口层的头部格式，图 16-8b 给出网络内部的信元头部格式。

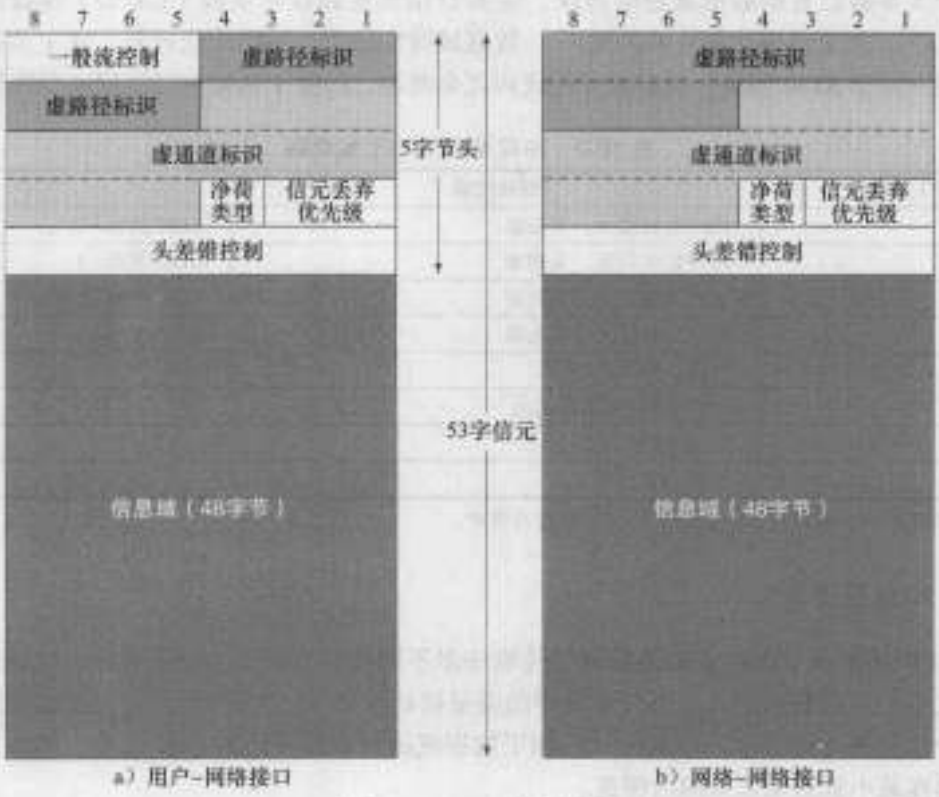


图 16-8　ATM 信元格式

一般流控制（GFC）：此域仅在用户 – 网络接口出现，在网络 – 网络接口的头部中不包含该字段。因此，该字段仅仅在本地用户 – 网络接口控制信元流。GFC 机制用于减缓网络中短期过载形式。

虚路径标识符（VPI）：组成网络的路由域，在用户 – 网络接口是 8 位，在网络 – 网络接口是 12 位，允许网络内部支持更多的虚路径。

虚通道标识符（VCI）：用作终端用户之间的路由，因此其功能就像服务接入点。

净荷类型（PT）：标识信息域中的信息类型。表 16-2 对 PT 域中的所有位进行解释：第 1 位取值为 0，标识用户信息（来自邻接高层的信息。在此种情况下，第 2 位显示是否经历拥

塞。第 3 位是一个比特的域，也称作服务数据单元（SDU）[⊖]类型位，用来区分与连接相关的 ATM 服务数据单元的两种类型。术语 SDU 指信元的 48 字节净荷。净荷类型域的第 1 位取值为 1，标识这个信元携带的是网络管理或维护信息，这个显式允许网络管理信元插入到用户的虚通道，而不影响用户数据。因此，PT 域能够提供带内控制信息。

信元丢弃优先级（CLP）：在出现拥塞情况下，此位为网络提供指南。取值为 0，标识优先级相对较高的信元不应该被丢弃，除非没有可用的其他选择。取值为 1，显示这个信元在网络内会遭到丢弃。在网络不拥塞的情况下，用户可以利用这个域，将其他 CLP 值为 1 的信元（超出协商速率）插入到网络中，并发送到目的地。对于违反网络和用户之间流量参数约定的任意信元，网络可以将 CLP 域置 1，除非交换机能处理这些信元。在随后的点，如果网络拥塞，该信元被标记为丢弃，其次才丢弃在约定流量范围内的信元。

头部错误控制（HEC）：8 位的错误代码，用于纠正数据包头部的单位错误和检测双位错误。对于大多数已有的数据链路层协议，诸如 D 信道链路接入规程（LAPD）和数据链路控制（HDLC），用于错误代码计算的输入：数据域通常比产生的错误代码长，这主要是考虑到错误检测。对于 ATM 网络，也有充分的代码冗余机制，以便于从某些错误模式中恢复。

表 16-2　净荷类型（PT）域编码

PT 编码	解释说明	
000	用户数据信元，无拥塞	SDU 类型 =0
001	用户数据信元，无拥塞	SDU 类型 =1
010	用户数据信元，有拥塞	SDU 类型 =0
011	用户数据信元，有拥塞	SDU 类型 =1
100	OAM 分段相关信元	
101	OAM 端到端相关信元	
110	资源管理信元	
111	留作将来使用	

注：SDU= 服务数据单元，OAM= 操作、管理与维护。

16.3.3　ATM 服务种类

ATM 网络被设计的初衷是能够同时传输许多不同类型的流量，包括语音、视频和突发式 TCP 流之类的实时数据流。虽然每种这样的流量被处理成 53 字节的信元流，在虚拟通道中传输，每个数据流在网络中处理的方式依赖于数据流的特点和应用的 QoS 需求。例如，实时数据流必须在最小延迟变化范围内传送。

在这个子部分，我们总结终端用以识别需求服务类型的 ATM 服务种类。ATM 论坛定义的服务种类如下：

- **实时服务。**
  - 固定比特率（CBR）。
  - 实时可变比特率（rt-VBR）。
- **非实时服务。**
  - 非实时可变比特率（nrt-VBR）。

⊖ ATM 论坛文档中使用此术语。ITU-T 文档中，SDU 类型位称作 ATM 用户 -ATM 用户（AAU）标识位，意义是相同的。

- 可用比特率（ABR）。
- 未说明的比特率（UBR）。
- 保证的帧速率（GFR）。

1. 实时服务

应用之间最重要的区别涉及延迟大小及应用所能容忍的抖动，即延迟变化。典型地，实时应用涉及发送给用户的信息流倾向于在源端被复制。例如，用户期望语音或视频信息流以连续、平滑的方式呈现，连续性丧失或过度损失导致服务质量的严重损失。涉及人际交互的应用有严格的延迟约束，任意超过几百微妙的延迟变得十分明显和烦人。因此，ATM 网络中对于实时数据交换和传送的要求是非常高的。

固定比特率服务（CBR）是定义的最简单服务，由需求固定数据速率和具有相对紧上界传输延迟的应用使用，而且这个数据速率在连接生命周期内连续可用。CBR 通常用于未压缩的语音和视频信息，CBR 应用的例子如下：

- 视频会议。
- 交互式语音（比如电话）。
- 语音 / 视频分发（比如电视、远程学习，收视付费）。
- 语音 / 视频获取（比如按需视频、语音图书馆）。

实时可变比特率（rt-VBR）类型倾向于时间敏感型应用，也就是那些需求严格约束的延迟和延迟变化的应用。适合于 rt-VBR 的应用和适合于 CBR 的应用之间主要的差异在于，rt-VBR 应用以随时间变化的速率传输。等同地，rt-VBR 源能够被特征化为有点突发式。例如，视频压缩的标准方法导致变尺寸的图像帧序列。由于实时视频需要均匀的帧传输速率，因此实际的数据速率是变化的。

与 CBR 相比，rt-VBR 给网络更多的灵活性。统计上，网络能够在同一专用容量上实现许多连接的复用，仍然能为每个连接提供需求的服务。

2. 非实时服务

非实时服务面向具有突发式流量特征、对延迟和延迟变化无紧约束的应用。因此，网络在处理这些数据流时有更大的灵活性，能够更加充分地利用统计复用，增加网络效率。

对于一些非实时应用，可以将期望的传输流量进行描述，因此网络能够在丢失和延迟方面，提供实质改进的服务质量。这些应用能够使用**非实时可变比特率**（nrt-VBR）服务，终端系统通过这个服务规定峰值信元速率（PCR）、可持续或平均信元速率、信元或许是突发或集群的测量。网络使用这些信息，能够分配资源，提供相对的低延迟和最小信元丢失。

具有关键的响应时间需求的数据传输使用 nrt-VBR 服务，例子包括航空预定、金融交易和过程监控。

在任意时刻，ATM 网络的一定数量的容量被消耗在 CBR 和两种类型的 VBR 流量。由于接下来的 1 个或 2 个原因，另外的容量是可用的：1）并不是所有的资源用于 CBR 和 VBR 流量。2）VBR 流量的突发特征意味着在一些时间，使用的容量少于承诺的容量。所有这些未使用的容量能够被用于**未声明的比特率**（UBR）服务，该服务适合于能容忍可变延迟和一些信元丢失的应用，比如基于 TCP 的流量就是一种典型的情况。使用 UBR，信元在先入先出的基础上转发，使用未被其他服务占用的容量，延迟和变化的丢失有可能出现。对 UBR 源头不做初始承诺，不提供有关拥塞的反馈，这称作尽力而为（best-effort）的服务。UBR 应用的例子包括：

- 文本 / 数据 / 图像传输、发送、分发、获取。

- 远程终端（比如远程办公）。

使用可靠的端到端协议（比如 TCP）的突发式应用，能够使用增加的往返延迟检测网络拥塞和报文丢弃。然而，TCP 缺乏在许多 TCP 连接中公平共享网络资源的机制。进一步，TCP 不能像使用来自网络中被拥塞节点的明显信息一样高效地最小化拥塞。

为了改善提供给突发式源头的服务，定义了**可用比特率**（ABR）服务。否则，该源头将使用 UBR 服务。使用 ABR 的应用规定将要使用的峰值信元速率（PCR）和需求的最小信元速率（MCR）。网络分配资源，以致所有的 ABR 应用至少以它们的 MCR 容量接收。然后，任意未使用的容量以公平和可控的方式共享给所有 ABR 源。ABR 机制给源头提供明显的反馈，以确保容量被公平分配，ABR 源不使用的任意容量仍然可为 UBR 流量使用。

使用 ABR 的一个典型应用例子是 LAN 互连，在这种情况下，连接到 ATM 网络的终端系统是路由器。

ATM 服务种类中最近新添加的是**保证帧速率**（GFR），该服务被设计用来支持 IP 骨干子网。对于基于帧的流量，包括 IP 和以太网（Ethernet），GFR 提供比 UBR 更好的服务。GFR 的主要目的是优化基于帧的流量处理，这些流量从局域网通过路由器发送到 ATM 骨干网。这些 ATM 网络正在被越来越多的大企业、运营商和因特网服务提供商网络使用，加强和扩展广域网中的 IP 服务。虽然 ABR 也是一种 ATM 服务，意味着通过 ATM 骨干网提供保证的报文性能的更大测量，但在 ATM 网络中路由器之间实现 ABR 相对困难。由于使用 ATM 支持基于 IP 流量的着重点的增加，尤其是发起于以太局域网的流量，GFR 为提供 ATM 服务提供了非常有吸引力的选择。

16.4　多协议标签交换

多协议标签交换（MPLS）服务是基于 IP 的网络服务，目前从许多运营商那里均可得到此服务。设计 MPLS 服务是用来加速 IP 报文转发过程，同时保留流量管理类型和 ATM 网络中出现的面向连接的 QoS 机制。

MPLS 经常被描述为“协议不可知者”，因为它能传输许多不同种类的流量，包括 ATM 信元、IP 报文、Ehternet 或 SONET 帧。运营商已经能够高效地实现 MPLS 基础架构，这主要是由于 MPLS 使能的路由器能够与普通的 IP 路由器共存。通过 MPLS 使能的 ATM 交换机和 MPLS 使能的帧中继交换机，MPLS 也已经被设计可与 ATM 和帧中继网络共同工作。

由于 MPLS 提供较高性能的网络容量，MPLS 有潜力完全替代帧中继和 ATM。MPLS 的设计者知道在 40Gbps 或更高速度的现代光网络核心中，不需要小 ATM 信元。在这些环境里，53 字节的信元和全长 1500 字节的报文都不经历实时队列延迟。另外，MPLS 保持流量工程和带外网络控制机制的许多特征，这些机制使得帧中继和 ATM 成为对企业用户有吸引力的 WAN 服务。

16.4.1　MPLS 操作

MPLS 网络由称为标签交换路由器（LSR）的节点集合组成，这些路由器节点能够以附加到每个报文的标签为基础，交换和路由报文。标签定义了两个终点之间的报文流，对于每个不同的流定义经由 LSR 网络的一条具体路径，这条路径称为转发等价类（Forwarding Equivalence Class，FEC）。每个 FEC 有相关联的流量特征，为这个流定义 QoS 需求。LSR 基于报文的标签值进行转发，不需要检查或处理报文的 IP 头，这意味着 LSR 的转发过程比 IP

路由器的简单、快速。

图 16-9 阐述了 1 个 MPLS 使能路由器域内的 MPLS 操作。过程的第一步涉及为需要被路由和发送的报文建立标签交换路径（Label Switched Path，LSP），以及为 LSP 建立 QoS 参数，参数包括针对路径上每个 LSR 的队列和丢弃策略，以及需要给路径承诺的资源。建立 LSP 和它的 QoS 参数的过程导致 FEC 的生成，这由图 16-9 中的①给予解释说明。一旦 FEC 生成，就能够为 FEC 的报文分配标签。

报文通过处于 MPLS 网络边沿的入口 LSR 进入 MPLS 交换域，入口 LSR 处理报文、确定需求的 QoS 服务和为报文分配 FEC 和 LSP，然后附上合适的标签并转发报文到沿标签交换路径的下一个 LSR，这一过程由图 16-9 的②给予解释说明。在 MPLS 网络内部，标签交换路径上的每一个 LSR 接收打标签的报文，并将其转发到沿 LSP 的下一个 LSR，见图 16-9 中的③。当报文到达最接近目的地的网络边沿的出口路由器时，边沿 LSR 剥去报文中的标签，读取 IP 报文头部，并转发报文到最终目的地。在图 16-9 ④给出的例子中，最终的目的地是服务器。

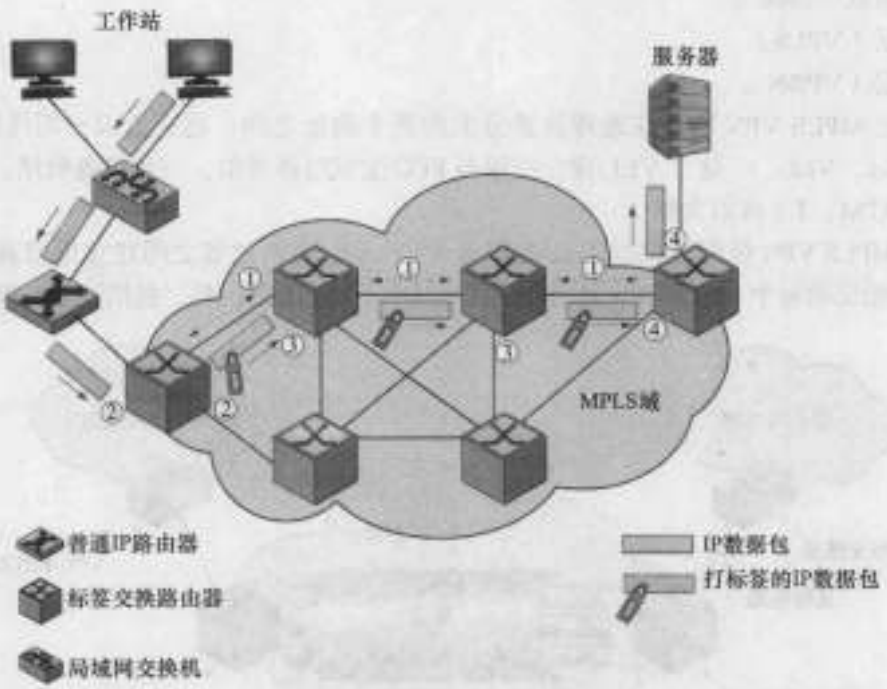


图 16-9　MPLS 操作

正如从图 16-10 观察，MPLS 标签是一个 32 位的域，包括下列元素：

- 局部值：具有局部重要性的 20 位标签。
- 流量类型：象征 QoS 优先级和明显拥塞告知的 3 位标签。
- 栈底位：如果这位设置为 1，显示当前标签是堆栈中的最后 1 个。
- 生存时间：8 位，用于编码跳数或生存时间值。避免由于错误路由造成的环路或报文在网络中停留的时间太长。

简言之，通过 MPLS 报文第一次进入网络时，被分配具体的 FEC，这个 FEC 显示在分配标签中。由于网络中每个路由器拥有一张显示如何处理某一具体的 FEC 类型报文的表，MPLS 网络能够一贯地处理具有某一特点的报文（比如来自某个端口的报文或携带某个应用类型的流量）。把报文分配给转发等价类意味着携带实时流量的报文能够被映射到网络中的低

延时路由，比如语音或视频。重要的是标签提供了一种附加额外信息到每个报文的方法，这给难以在 IP 网络和其他 WAN 服务中实现的流量工程提供便利。

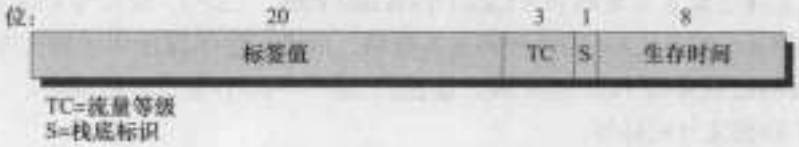


图 16-10　MPLS 标签格式

16.4.2　MPLS VPN

多协议标签交换虚拟专用网（MPLS VPN）指通过 MPLS 网络创造虚拟专用网（VPN）的方法，目前部署的网络中主要有 3 种主要类型的 MPLS VPN：

- 点对点（伪线）。
- 二层（VPLS）。
- 三层（VPRN）。

点对点 MPLS VPN 涉及在地理位置分散的两个地址之间，建立虚拟专用线路（Virtual Leased Lines，VLL，）。这个 VLL 建立过程与 FEC 生成过程类似，一旦准备就绪，VLL 能够用于封装 ATM、T-1 或以太帧。

二层 MPLS VPN 使用虚拟专用 LAN 服务（VPLS），在两位置之间建立虚拟通道。比如，图 16-11 中给出的每个 MPLS VPN 通道能够用于路由不同类型的流量，包括语音、视频和数据。



图 16-11　2 层 MPLS VPN 概念

三层 MPLS VPN 利用虚拟专用路由网（Virtual Private Routed Network，VPRN）为每个使用服务的客户划分网络流量，为每个客户建立具体的路由表，用于路由客户位置之间的网络流量。例如，企业可以使用三层 MPLS VPN，实现企业办公室和数据中心之间的流量路由。

VPN 在企业中流行，这是因为虚拟专用网络使得通过共享的 WAN 电路建立专用网络成为可能。由于 MPLS VPN 合并的隐私和高性能网络能力，使得它在企业网络中变得越来越常见。

16.5　广域以太网

广域以太网（Wide Area Network，WAE）使用以太连接传送 WAN 服务，它是传统广域网服务的高速替代，包括帧中继、租用线路、ATM 或 T-1 服务。WAE 维持着 2 层以太网的简单、高带宽和平滑网络设计。对于 WAE 用户，互联的站点看起来像单一逻辑网络。WAE 实质上是链接远程位置的 VPN 服务。

大多数 WAE 的实现使用虚拟专用 LAN 服务（VPLS）互联网络端点。VPLS 允许运营商定义广域连接的 QoS 级别和用于视频或语音应用的投入资源，比如充足的带宽。VPLS 也允许运营商从包括 IP 或 MPLS 网络的各种 WAN 服务中创造逻辑以太网络。

WAE 服务有时称作以太广域网（Ethernet WAN）或营运以太网（Carrier Ethernet），其中营运以太网包括 WAE 和城域以太网。营运以太网以几种方式部署，包括传统以太网、以太网映射同步数字分层（Synchronous Digital Hierarchy，SDH）和以太网映射 MPLS。营运以太网服务能够容纳居民和企业用户的混合。

使用营运以太技术建立城域网络（MAN）通常称为城域以太网（Metro Ethernet），经常用于为企业 LAN 和居民用户提供互联网和其他 WAN 服务的接入。政府部门、教育机构和公司越来越多地使用城域以太网服务建立内部网，实现分支办公室或校园的互联。

营运以太网常利用光纤和密集型光波复用（DWDM）基础设施，为用户提供广域网（WAN）和城域网（MAN）服务。图 16-12 提供了广域以太网的 1 个高层例子。

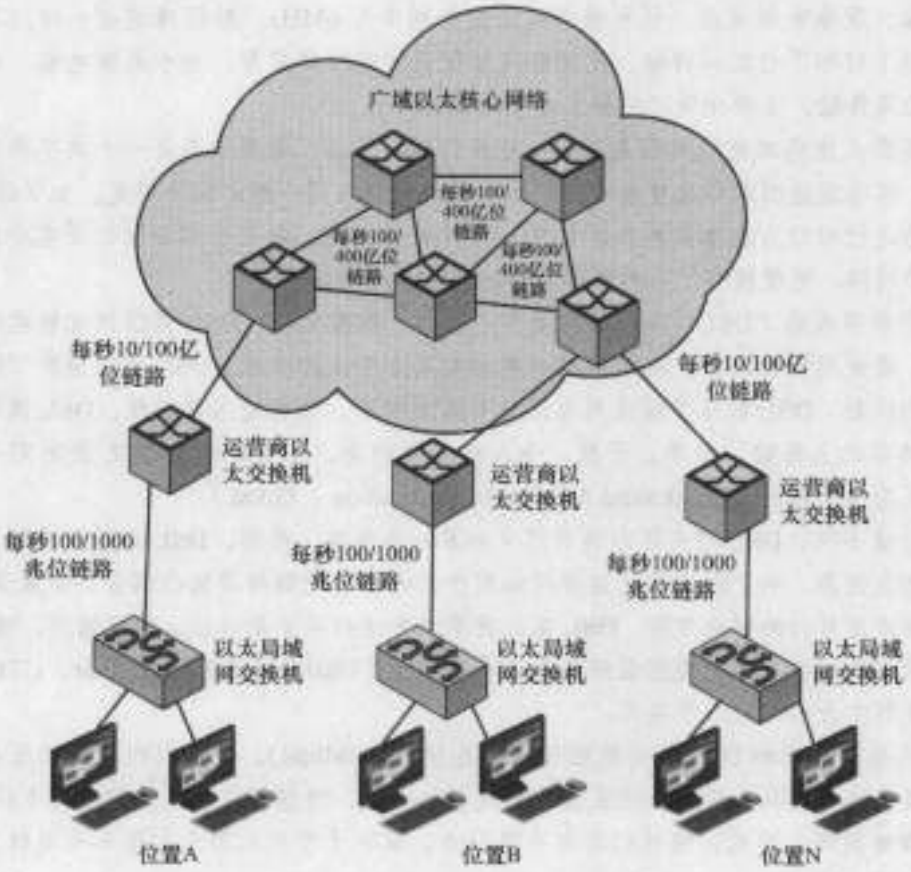


图 16-12　广域以太网

应用注解

远程连接解决方案

过去有一个称为80/20规则的经验法则，描述数据的流动方向。事实上有几个这样的规则，但这个规则陈述大约80%的网络数据是本地局部的，20%是流向远程，这称作“访问局部性”。我们越来越多地看到组织将这个规则颠倒了，他们发送/接收数据的80%流向远程处所，作为他们正常业务流程的一部分。因此，传统方法将不能充分地处理负载。除了本章已经提到的协议和服务之外，已经出现了其他传输系统，作为普遍的连接选择。初始被看作家用解决方案的电缆和数字用户线路（DSL）系统已经证明，它们对于企业是合适的，应该成为任意网站评估的部分。

像ATM和帧中继一样，电缆和数字用户线路（DSL）可能被阻塞，这意味着数据传输速率可以被修改，以满足某一需求。正如在第5章和第6章看到的，DSL有几种可用的服务类型，电缆提供商有不同的面向企业的服务规划。

如同大多数服务一样，这些服务同样有区域可用性的问题，地区优惠变化非常多，区域之间的定价也有很大的不同。例如在东北部，帧中继一直非常流行，而ISDN和ATM保持可用，但是昂贵的解决方案。在同一区域，电缆和DSL服务均可用，事实上在广告战中彼此直接竞争。

电缆仅仅意味着数据被发送到提供有线电视的同一电缆基础架构，分配另一通道用于这种传输，就像电视通道。所有通道被分配的频率是6MHz，数据通道也一样。不同的运营商提供上行和下行数据传输，调制解调器仅调制或解调信号。由于同轴电缆，电缆能够进行长距离传输，这种介质可保护信号免受外部干扰。

大多数人抱怨的电缆问题是在某一分段的用户数目，电缆分布是一个共享介质，由于这一点，在邻近范围或邻近建筑楼内的所有用户经常在同一线路竞争带宽。由于这种竞争，电缆开始运行时行为就像共享的以太网；用户数目越高，每个个体分配的带宽越低。即使具有这种缺陷，电缆提供了一种值得考虑的高速选择方案。

用户数字线路（DSL）与电话使用同一线路。就像电缆，DSL提供商宣称在传输数据的同时，能使用你的电话。虽然电缆系统使用完全不同的系统，DSL需求面向“绕过”电话交谈的机制。DSL数据传输使用与语音不同的频率，语音输出是低频，DSL调制解调器在这个频率之上传输，以防止干扰。令人感兴趣的是，注意电缆和DSL使用同一调制技术——正交幅度调制（Quadrature Amplitude Modulation，QAM）。

与电缆不同，DSL用户不与其他用户共享一条线路。然而，DSL有其他限制，非常突出的问题是距离。这个限制加上连接网站到中心办公室的铜线质量的耦合，能取消DSL在一些区域作为可行的解决方案。DSL在几英里之外运行得不是很好，距离越远，噪声越大，因此数据速率越低。即使使用最好的非屏蔽双绞线（Unshielded Twisted Pair，UTP），最大距离也限制在大约一万八千英尺。

虽然当前电缆和DSL都不能胜任高速连接（100Mbps），但它们代表传统服务的成功选择。提供这些解决方案的公司正在不断地添加带宽，使他们自己越来越有竞争性。另外，服务经常被捆绑，这或许使他们非常有吸引力。取决于组织的需求和服务可用性，电缆和DSL绝对值得考虑。

如果不考虑最后一英里的另外连接方案——千兆（Gigabit）和万兆（10 Gigabit）以太网，这个讨论将是不完整的。这个方案具体针对某一市场，提升了著名的技术（Ethernet），并通过光纤运行。结果是对于能够长距离传输的其他服务，该方案是一个极高速的选择。相比较，像大学之类的高数据速率网站，或许购买达到 155Mbps 速率的昂贵 OC-3 设备，能够得到比原来快 60 倍的万兆比特率连接。

然而，设备仍然非常昂贵，服务或许是不可用的。离线连接解决方案的列表已经十分长，我们继续增加不同的技术。由于公司将越来越多的数据推向他们的外部链路，仅仅几个较老的技术将不能跟上带宽需求的是时间不会太长。

16.6 总结

广域电信服务的提供方式已经发生了重大变化。分布式计算系统日益增加的容量需求，以及与高速和高可靠性传输设备的引入，已经导致各种广域网服务的出现，远远超出传统报文交换技术的能力。

历史上，对于企业用户而言，帧中继一直是非常流行的 WAN 服务之一。帧中继被全球性地使用，大量提供商提供此服务，用于公共和私有网络配置。帧中继使用称为帧的变尺寸报文，是一种比传统分组交换网络简单的处理方案，可实现的数据速率达到 44.736Mbps。

异步传输模式（ATM）与帧中继相比，更简单，提供 Gbps 范围的容量。ATM 技术在当今的企业网络中广泛可见，尤其是广域网络中。

多协议标签交换（MPLS）基于短路径标签而不是长 IP 网络地址，将数据从一个网络节点导向下一个网络节点，这加速了包转发过程。MPLS 能够封装各种协议的报文，支持宽范围的访问技术，包括以太网、T-1、ATM、帧中继和数字用户线路（DSL）。

广域以太（WAE）作为帧中继和 ATM 之后另一个高速 WAN 服务选择出现了。由于以太网在企业局域网（LAN）中遍布，WAE 已经成为对于企业网络管理者的一种有吸引力的 WAN 服务。

16.7 关键术语、复习题和练习题

关键术语

Asynchronous Transfer Mode（ATM，异步传输模式）
Available Bit Rate（ABR，可用比特率）
cell（信元）
Constant Bit Rate（CBR，固定比特率）
frame relay（帧中继）
Guaranteed frame rate（GFR，保证帧速率）
Multiprotocol Lable Switching（MPLS，多协议标签交换）
non-real-time Variable Bit Rate（nrt-VBR，非实时可变比特率）
Unspecified Bit Rate（UBR，未说明的比特率）
Variable Bit Rate（VBR，动态比特率）
virtual channel（虚拟通道）
virtual path（虚拟路径）
Wide Area Ethernet（WAE，广域以太网）
Wide Area Network（WAN，广域网）

复习题

16.1 对于广域网，可用的主要高速网络服务是什么？
16.2 帧中继与分组交换的不同体现在哪里？
16.3 与报文交换相比较，帧中继的相对优势和劣势是什么？
16.4 为什么现代通信设施不需要 X.25 系统使用的所有错误检查？
16.5 帧中继网络是如何处理拥塞控制的？
16.6 ATM 与帧中继的不同是什么？
16.7 与帧中继相比较，ATM 的相对优势和劣势是什么？
16.8 虚路径与虚通道的不同是什么？
16.9 列举并简要定义 ATM 实时服务。
16.10 列举并简要定义 ATM 非实时服务。
16.11 MPLS 网络的特点是什么？
16.12 简要描述 MPLS 网络中转发等价类（FEC）的角色。
16.13 MPLS VPN 的特点是什么？
16.14 广域以太网络的特点是什么？

练习题

16.1 对帧中继、ATM、MPLS 和运营商以太服务的增长速率做互联网调查，对于这些广域网（WAN）技术的未来能得出什么结论？用 750 ~ 1000 字的论文或 8 ~ 10 页幻灯片演示文稿总结你的发现。

16.2 对虚拟专用网和它们在企业组织中的使用做互联网调查，描述 VPN 及部署 VPN 使用的技术、协议和服务的主要类型，也描述 VPN 的企业利益。用 750 ~ 1000 字的论文或 8 ~ 10 页幻灯片演示文稿总结你的发现。

16.3 企业网络中移动性和移动应用的支持越来越多，已经增加了用以支持移动企业用户的移动 VPN 的重要性。对移动 VPN、与传统 VPN 的不同之处及支持的企业应用类型做互联网调查。用 500 ~ 750 字的论文或 5 ~ 8 页幻灯片演示文稿总结你的发现。

16.4 做互联网调查，识别主要的运营以太服务的供应商。后面的网址或许有助于信息收集：www.carrierethernetservices.com。集中在至少 3 个提供国家和 / 或国际的运营以太服务的供应商，并总结他们提供给用户的访问速度、传输速度和 VPN 服务。用 500 ~ 750 字的论文或 5 ~ 8 页幻灯片演示文稿总结你的发现。

16.5 考虑下面的情形，在每一种情况显示你是否愿意使用帧中继、ATM、MPLS 或营运以太网服务。假定设备可用，而且具有竞争性的价格。对于每种情形，确定哪一种服务能够用来满足应用的功能需求，并解释选择原因。

a. 在一个城市区域，你有许多场所。在每个场所，有许多需要处理的实时数据事务。有关事务的信息必须被独立发送，且处所之间几乎是随意的。也就是事务不是成批的，也不是成群地发生。性能需求是延迟必须短，在每个处所的流量容积是合适的，但总的速度达到几个 Mbps。

b. 在相对偏远的区域，你有一个国家广域网，大约有 6 个处所，传输设施多样化，包括语音链路、卫星链路和使用调整解调器的电话链路，数据速率相对适中。

c. 在这种情况下，你有多媒体应用，包括图像通信和重要的实时视频和语音服务，这些和大量的其他数据服务交织在一起。处所数目小，但有图像和视频应用，流量容积十分大，接近 Gbps 的范围。这里也有大量用户和应用，因此即使处所少，但需要大量的虚电路。

16.6　做因特网调查，识别一些主要的 MPLS 服务供应商。Web 网址 www.mplsprovider.com/mpls-service-provider.asp 或许有助于你的信息收集。集中在 3 或 4 个你认为做得比较好的供应商，描述 MPLS 对潜在用户的企业利益，并解释你对这些供应商印象深刻的原因。如果现在你是主管且必须为你的企业选择 MPLS 服务供应商，你将选择哪一个？为什么？

16.7　在做 MPLS 和以太网调查的时候，你有可能遇到虚拟局域网（VLAN）的讨论。对 VLAN 和它们在企业组织中使用的方式做因特网调查，以 5 ~ 8 页幻灯片演示文稿或 500 ~ 750 字的论文总结 VLAN 的特点、典型使用和业务优势。识别非常有利于支持 VLAN 的广域网服务（ATM、帧中继、MPLS、运营以太网）。

第 17 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

无线广域网

学习目标

通过本章的学习，读者应该能够：

- 识别非导向无线通信与导向通信的优势与劣势。
- 区分四代移动电话。
- 理解时分多址（TDMA）与码分多址（CDMA）方法与移动电话的相对优势。
- 描述第 3 代和第 4 代蜂窝网络的特点。
- 理解低轨道地球卫星（LEOS）、中轨道地球卫星（MEOS）和地球静止轨道卫星（GEOS）的特性和应用。

我们已经进入后 PC 时代，在 2011 年智能手机比个人 PC 卖得多，Web 服务 / 应用占据新开发软件的大多数。移动设备和 Web 应用的增多强调了这样的事实：电子信息系统影响我们生活的每个方面，被拘束到这些有线设备越来越伤脑筋。无线通信给我们提供了移动性及其更多，当面临以下情况时，无线通信有可能被看作企业网络基础设施的必要部分：

- 需要移动通信。
- 通信必须发生在敌意或困难的地形，这种情况使有限通信难以实现或变得不可能。
- 通信系统必须快速地部署。
- 同一信息必须被广播到许多处所。

然而，企业网络设计者不能忽略无线通信相对导向介质的劣势，诸如双绞线、同轴电缆或光纤：

- 无线通信运行在不太受控的环境，因此对于干扰、信号丢失、噪声、搭线窃听比较脆弱。
- 通常情况下，与导向设备相比，无线设备有较低的数据速率。
- 用导向介质的频率比使用无线介质的频率更加容易重复使用。

在本章，我们考虑广域无线系统，包括移动电话、第 3 代和第 4 代无线系统以及卫星通信，无线局域网在第 14 章中讨论过。

17.1 蜂窝无线网络

在数据通信和电信领域所有重要的进展中，非常重要的革新之一是蜂窝网络的开发与演化。蜂窝技术是移动无线通信的基础，支持处于不易被有线网络服务的位置的用户，是移动电话、个人通信系统、无线互联网、移动 Web 应用等的基础技术。

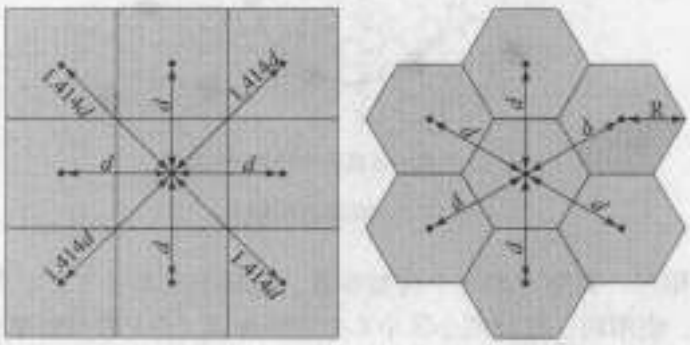
蜂窝无线电是一种增加移动无线电话服务可用容量的技术，在蜂窝无线引入之前，仅仅由高功率发射器 / 接收器提供移动无线电话服务。典型的系统支持大约 25 个信道，有效半径为大约 80 公里。增加系统容量的方法是使用具有较短半径的低功耗发射器和使用无数的发射

器 / 接收器。

17.1.1　蜂窝网络组织

蜂窝网络的实质是使用多个低功耗发射器，在 100 瓦或更小的数量级。由于那种发射器的范围小，一个区域被划分成多个小区（cell），每个小区由它自己的天线服务。同时，每个小区被分配一个频段，由基站（Base Station，BS）提供服务，这个基站由发射器、接收器和控制单元组成。邻近的信元被分配不同的频率，以避免相互干扰或串话。然而，彼此相距比较远的小区能够使用同一频段。

要做的第一个决策是覆盖一个区域的蜂窝形状。方形矩阵将是定义的最简单设计（见图 17-1a），然而这个几何形状不理想[⊖]。当小区内移动用户向小区边界移动时，最好的情况是所有邻接的天线是等距离的，这可以简化确定何时切换用户到邻近的天线和选择哪个天线的工作。六边形模式提供了等距离（见图 17-2b）[⊜]。事实上，没有使用精确的六边形模式，与理想模式的偏差主要是由于地形限制、本地信号传播条件和实际的选址天线限制。



a）方形模式　　b）六边形模式

图 17-1　小区几何形状

不受约束的信号可能会相互干扰，即使地理上是分离的。无线蜂窝系统限制了不同通信使用同一频率的机会，能够同时支持许多通信的系统需要保留频谱的机制。

1. 频率重用

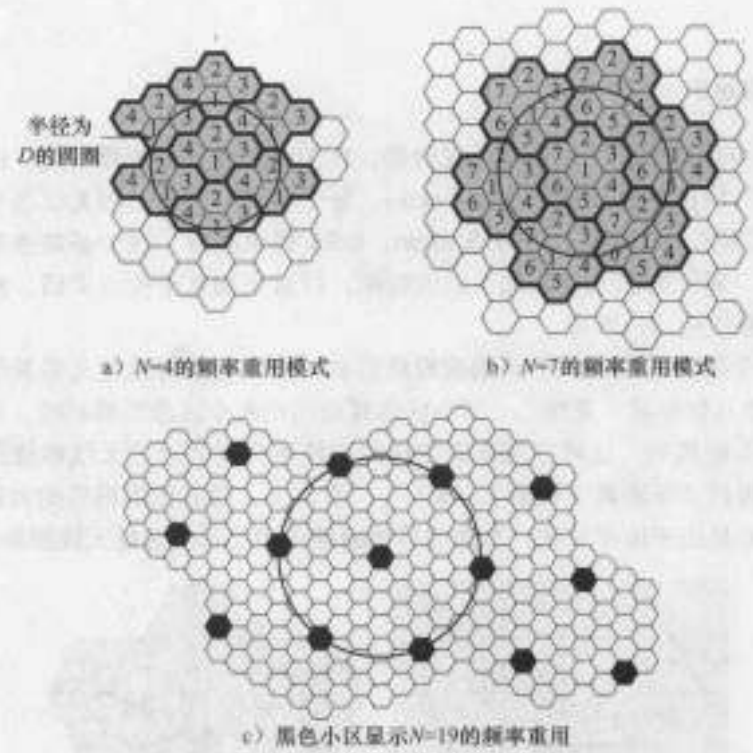
在蜂窝系统，每个小区有一个基站发射器。基站的发射功率被仔细控制，允许小区内使用某一频率通信，同时限制功率到从本小区逃进邻近小区的频率。目的是在其他附近的（不是紧接着的）小区使用同一频率，因此允许该频率被多个会话同时使用。通常情况下，10 ~ 50 个频率被分配到每个小区，具体分配多少个频率取决于预期的流量。

必要的问题是确定多少个小区必须介于使用同一频率的两小区之间，才能使得这两个小区不相互干扰。各种频率重用的模式是可能的，图 17-2 给出一些例子。如果模式由 N 个小区组成，且每个小区分配相同数目的频率，每个小区能有 K/N 个频率，这里 K 是分配给系统的频率总数[⊝]。

⊖ 如果方形蜂窝的宽度是 d，那么一个蜂窝在 d 距离处有 4 个邻居，在 $\sqrt{2}d$ 距离处有 4 个邻居。

⊜ 六边形的半径定义为围绕它的圆的半径（等同地，从中心到每个定点的距离，也等同于六边形边的长度）。对于小区半径 R，小区中心与每个临近小区中心的距离是 $d=\sqrt{3}R$。

⊝ 对于 AMPS（广泛使用的第 1 代蜂窝方案—高级移动电话服务），K=395，N=7 是能够在两个使用相同频率的小区之间提供充分隔离的最小模式，这意味着每个小区平均至多有 57 个频率。



a）N=4的频率重用模式　　b）N=7的频率重用模式

c）黑色小区显示N=19的频率重用

图 17-2　频率重用模式

当确定频率重用时，需要考虑几个典型参数，包括小区半径（R）、邻接小区中心之间的距离（$d=\sqrt{3}R$）、使用同一频段的小区中心之间的距离（D）和与频率重用相关联的其他参数[⊖]。

2. 增加容量

经过一段时间，随着小区中使用这个系统的客户越来越多，流量或许增进以致于没有足够的频率分配给这个小区来处理呼叫。许多方法已经被提出，用于处理这种形势。包括以下几种方法：

- **添加新信道**：典型地，当一个系统安装在某区域后，并不是使用所有的信道，以一种比较老的方式——添加新信道来管理增长和扩充。
- **频率借用**：在这个最简单的情形，通过扼塞一些小区的方式，从邻接小区借用频率，

⊖ 在频率重用计算中，通常使用的参数包括：

D= 使用同一频段的小区中心之间的最小距离（称为同信道）；

R= 小区半径；

d= 邻接小区中心之间的距离（$d=\sqrt{3}R$）；

N= 处于重复模式的小区数（模式中每个小区使用一个独特的频段），称作重复因子。

在六边形小区模式，N 仅可能取下面的值：

$$N=I^2+J^2+(I\times J),\quad I,J=0,1,2,3,\cdots$$

因此，N 的可能值为 1，3，4，7，9，12，13，16，19，21 等等，且有下面关系成立：

$$\frac{D}{R}=\sqrt{3N}$$

这个关系也可以表示为 $D/d=\sqrt{N}$。

这个频率可动态分配给小区。

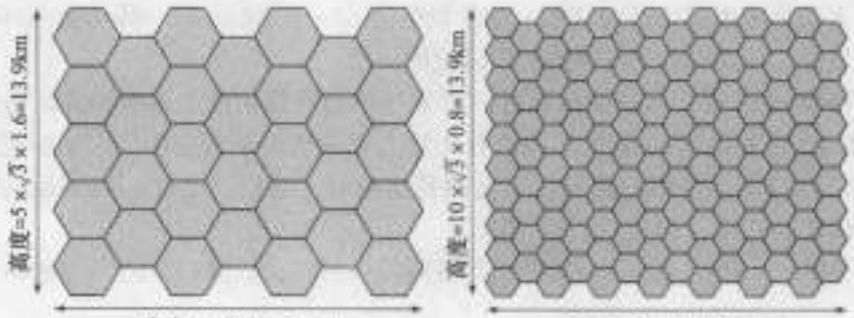
- **小区切分**：事实上，流量和地形特征的分布是不均匀的，这也表示着容量增加的机会。使用率高的蜂窝可被切分成较小的蜂窝。一般而言，初始蜂窝大约 6.5 – 13km，小蜂窝自身可以切分。然而，1.5km 的蜂窝接近通用方案的实际最小尺寸（随后讨论的微蜂窝是另一部分）。为了使用较小的蜂窝，使用的功率水平必须降低到保持信号在小区内。同时当移动单元移动时，它们在小区中穿越，这要求呼叫从一个基站发射器转移到另一个，这个过程叫做切换（handoff）。随着小区变小，这些切换变得越来越频繁。小区半径减小 F 倍，覆盖区域减少，所需的基站数增加 F^2 个。
- **小区扇形化**：使用小区扇形化，一个小区被划分成许多楔形的扇区，且每个扇区拥有自己的信道，典型情况是每个小区 3 或 6 个扇区。每个扇区给予分配小区信道的分离子集，并且在基站的方向天线用于集中在每个扇区。
- **微蜂窝**：由于小区变得越来越小，天线从高楼或山脉的顶部移动到小建筑物的顶部或大建筑物的侧面，最后移动到路灯柱，在这里形成微蜂窝。在小区尺寸上的每一个减少都伴随着基站或移动设备的辐射功率级别的降低。在城市街道、沿高速路的拥挤区域和大的公共建筑物内，微蜂窝十分有用。

表 17-1 建议传统蜂窝，称为宏蜂窝，和使用当前技术的微蜂窝的典型参数。其中，平均延迟范围指多路径延迟范围（即同一信号沿用不同的路径，在接收端最先到达和最后到达的信号之间有个时间延迟）。正如表 17-1 显示，较小小区的使用使低功耗成为可能，并提供优越的传播条件。

表 17-1　宏蜂窝与微蜂窝的典型参数

	宏蜂窝	微蜂窝
小区半径	1 ～ 20km	0.1 ～ 1km
发射功率	1 ～ 10W	0.1 ～ 1W
平均延迟范围	0.1 ～ 10μs	10 ～ 100ns
最大比特率	0.3Mbps	1Mbps

例子　图 17-3a 给出一个近似的方形模式。半径为 R 的六边形面积是 $1.5R^2\sqrt{3}$，半径 1.6km 的六边形面积是 6.65km^2，总的覆盖区域是 6.65 × 32=213km^2。对于 N=7 的情形，每小区的信道数目是 336/7=48，总的信道容量是 48 × 32=1536。对于图 17-3b 的布局，覆盖区域是 1.66 × 128=213km^2，每小区的信道数目是 336/7=48，总的信道容量是 48 × 128=6144。



a）小区半径=1.6km　　b）小区半径=0.8km

图 17-3　频率重用例子

17.1.2　蜂窝系统运行

图 17-4 给出蜂窝系统的主要元素。在每个小区的近似中心位置是一个基站（BS），包括天线、控制器和许多发射器，所有这些用于通过分配给该小区的信道进行通信。其中，控制器用于处理移动设备与网络其他部分之间的呼叫过程。在任意时刻，许多移动用户单元可以是在线的，在小区内移动，以及与基站通信。每个基站连接到 1 个移动通信交换局（MTSO），且用一个 MTSO 服务于多个基站（BS）。典型地，MTSO 与 BS 之间的链路是有线线路，虽然无线线路也是可能的。MTSO 负责连接两个移动设备之间的呼叫，也连接到公共电话或电信网络，在与公共网络相连的固定用户和与蜂窝网络相连的移动用户之间建立连接。进一步，MTSO 为每个呼叫分配语音信道、执行切换和监控呼叫获取账单信息。

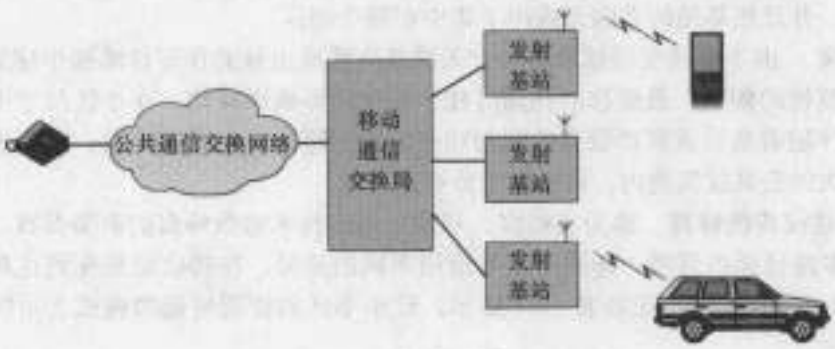


图 17-4　蜂窝系统概观

蜂窝系统的使用是全自动化的，不需要用户部分的参与，除非打电话和接电话。在移动设备和基站之间，有两种类型的可用信道：控制信道和流量信道。**控制信道**用于交换信息，与建立和维护呼叫以及在移动设备和最近的 BS 之间建立联系相关。**流量信道**用于携带用户之间的语音或数据连接。图 17-5 给出一个区域内两个移动用户之间的典型呼叫步骤，这个呼叫受单一 MTSO 控制。具体的步骤如下：

- **移动单元初始化**：当移动设备打开时，扫描和选择供系统使用的最强的设置控制信道（见图 17-5a）。具有不同频段的小区不断地向不同的设置信道广播，接收器选择最强的设置信道并监控那个信道。这个过程的影响是移动单元已经自动地选择了小区的 BS 天线，并将在这个小区内运行[⊖]。然后移动设备和控制这个小区的 MTSO 之间发生握手，识别用户并注册用户的位置。只要移动设备打开着，这个扫描过程就定期重复执行，主要是考虑到设备的移动。如果设备进入一个新的小区，那么要选择一个新的基站。另外，移动设备还在监控随后讨论的页面。
- **面向移动的呼叫**：移动设备通过向预先选择的设置信道上被叫单元的号码发起呼叫（见图 17-5b）。移动单元的接收器首先检查设置信道是否空闲，这主要是通过检查转发（来自基站）信道的信息。当检测到空闲时，移动设备在相应的反向信道（到基站）传送。基站向 MTSO 发送请求。
- **分页（paging）**：MTSO 企图完成与被叫设备的连接。MTSO 向某些基站（BS）发送

⊖ 通常，但不总是，天线和因此选择的基站是距移动单元最近的一个。然而，由于传播异常，并不总是这种情况。

分页信息（见图 17-5c），具体哪些基站取决于被叫移动号码。每个基站在它自己分配的设置信道发送分页信号。

- **接受呼叫**：被叫移动设备在被监控的设置信道上认出自己的号码，并响应那个基站，这个基站发送响应给 MTSO。MTSO 在呼叫和被叫基站之间建立一条电路。同时，MTSO 在每个基站的小区内选择可用的流量信道，并通知每个基站，这些基站再依次通知它的移动单元（见图 17-5d）。这两个移动终端调整到它们各自分配的信道。
- **呼叫进行中**：两移动设备在维持连接的同时，通过它们各自的基站和 MTSO 交换语音或数据信号（见图 17-5e）。
- **切换**：如果移动设备移出一个小区的范围，在连接期间进入另一个小区的范围，流量信道必须改变到新的信道，这个信道是新小区分配给基站的（见图 17-5f）。在没有打断呼叫或改变用户的情况下，系统做了切换。

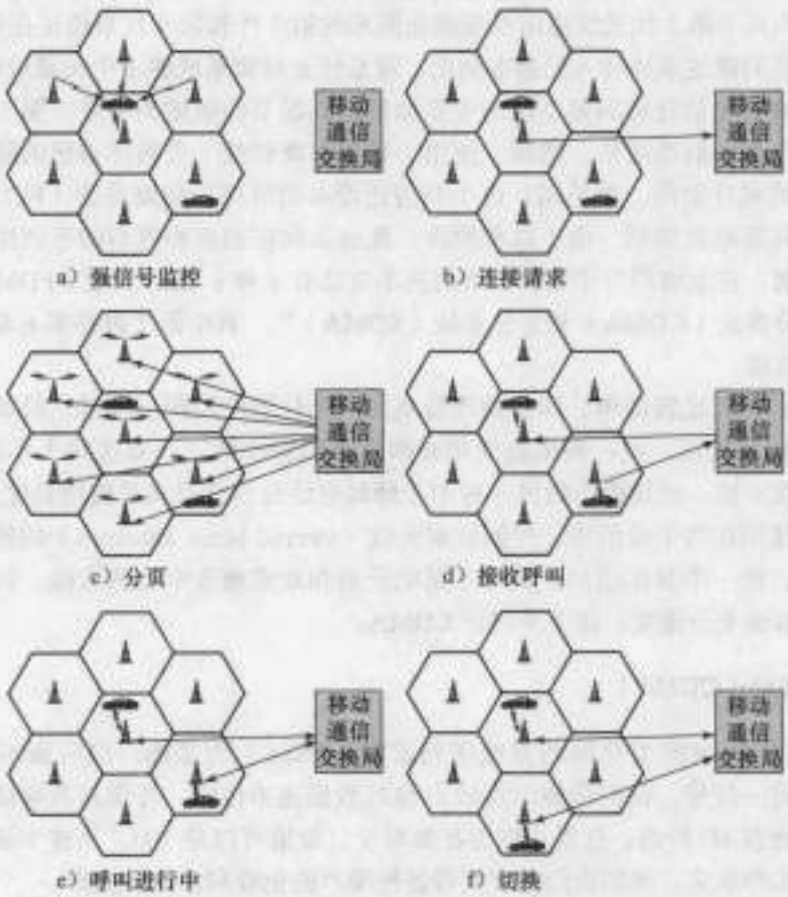


图 17-5　移动蜂窝呼叫例子

系统执行的且在图 17-5 中没有给予说明的其他功能，包括以下：

- **呼叫阻塞**：在移动呼叫发起初始阶段，如果分配给最近 BS 的所有流量信道都是繁忙，那么移动设备预先配置数次重复尝试。一定数量的失败尝试之后，给用户返回忙音。
- **呼叫终止**：当两个用户中的一个挂机时，通知 MTSO，释放两个基站的流量信道。
- **呼叫丢弃**：在连接期间，由于某些区域的相互干扰或弱信号出现，如果基站在一段时间内不能维持需求的最小信号强度，给用户的流量信道被丢弃，并通知 MTSO。

- **来自 / 到达固定和远程移动用户的呼叫**：MTSO 连接到公共交换电话网（PSTN），因此 MTSO 能够通过电话网络为所在区域的移动用户和固定用户建立连接。进一步，MTSO 通过电话网络或专用线路，能够连接到远程的 MTSO，能够为所在区域的移动用户和远程移动用户建立连接。

17.2　多址接入

人们把移动电话系统划分成几代。第 1 代系统基于模拟语音通信，使用频率调制。广泛使用的第 1 代系统是高级移动电话系统（AMPS），从 20 世纪 80 年代到 21 世纪，广泛应用在南美、北美、澳大利亚和中国。由于第一代移动电话被消费者和企业快速采纳，高效使用频谱的系统变得十分必要，这有助于减少拥塞。这个需求由第 2 代通信技术处理，它使用数字技术和时分多址（TDMA）或码分多址（CDMA）用于信道接入，而且也出现了高级的呼叫处理特征。从几个第 2 代无线通信系统演化而来的第 3 代和第 4 代系统正在推出。

在这里，我们描述多址接入的基本概念，这是任意蜂窝系统的 1 个关键设计元素。

从第 1 代蜂窝电话迁移到第 2 代的主要动机是满足节约频谱的需要。第 1 代系统极其成功，几年间用户呈指数级增长。然而，使用（和提供商利益）受频谱容量的限制，这造成了频谱有效使用的额外费用。在美国，这个利益还没有被联邦通信委员会（FCC）最近的拍卖频谱而不是放弃策略所抑制。由于这些原因，理解如何在当前和规划的系统用户中划分频谱是重要的。目前，在上线用户中划分频谱的基本方法有 4 种：频分多址（FDMA）、时分多址（TDMA）、码分多址（CDMA）和空分多址（SDMA）[⊖]，其中前 2 种在第 6 章讨论，这里讨论剩下的 2 种方法。

空分多址的观点比较简单，即在物理分离的两个位置使用同一频谱，简单的例子是本章讨论的小区中频率复用，同一频率能使用在两个不同的小区，只要这两个小区相距足够远，使得信号不相互干扰。已经提出的另一种用于蜂窝电话的空分形式是使用高度有方向的天线，使得同一频率使用在两个通信中，控制波束天线（steered beam antennas）的使用进一步向前推动这个观点。在一个具体用户，实际上是电子地和动态地选中这些天线。码分多址的观点有些复杂，而且也十分重要，接下来讨论 CDMA。

17.2.1　码分多址（CDMA）

CDMA 以第 14 章简要介绍的直接序列扩频（DSSS）为基础，以后面不违反直觉的观点为根据。给定一信号，我们希望以每秒 D 位的数据速率传输，并将其转换成一条较长的信息，以较高的速率 kD 传送，这里 k 称为扩频因子，取值可以是 100。从这个显然的频谱浪费中，可以获得几种事实，例如我们能够获得各种噪声的免疫和多路径变形。

频谱最早使用在军事领域，被用于人为干扰的免疫，也可被用于隐藏和加密信号。然而，令我们感兴趣的是几个用户能够独立使用同一（较高）带宽，而且相互干扰非常小。图 17-6 给出 3 个用户 A、B 和 C 的编码，这 3 个用户均与同一基站接收器 R 通信。

事实上，CDMA 接收器能够过滤掉无用用户或者看起来像低级噪声的贡献。然而，如果有许多用户和接收器正在试图监听的用户竞争信道，或者如果一个或多个竞争信号的功率太

⊖ 术语 FDMA、TDMA、CDMA 和 SDMA 实质上分别等同于属于 FDM、TDM、CDM 和 SDM。短语多址（multiple access）强调单一信道被多个用户共享。

高，这可能是因为与接收器距离太近（“近/远”问题），系统会失败。编码增益可以大于100，这样我们的解码器过滤无用编码的能力可以十分有效。有关 CDMA 更加详细的讨论在附录 M 中提供。

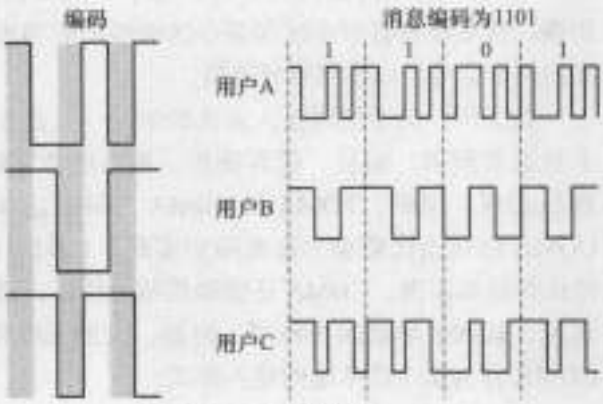


图 17-6　CDMA 例子

17.2.2　使用哪种接入方法

图 17-7 说明了 FDMA、TDMA 和 CDMA 之间的不同。归纳起来，使用 FDMA，每个用户能够在自己狭窄频段与基站通信。对于 TDMA，多用户共享较宽的频段，依次和基站通信。对于 CDMA，许多用户能同时使用同一宽频段，每个用户的信号使用独特的编码搅乱（scrambled），以至于对其他用户来说，看起来相似随机背景噪声。基站使用同一编码来复原（unscramble）不同的用户信号。与 FDMA 和 TDMA 相比，CDMA 允许更多的用户共享某一带宽。

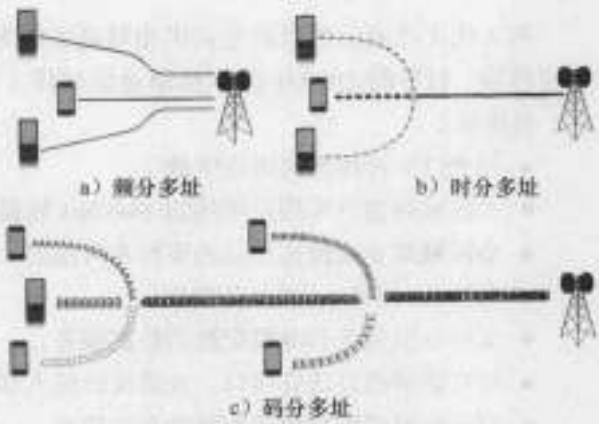


图 17-7　蜂窝多址方案

除了切分信道的单一形式之外，比如 FDMA、TDMA、CDMA 和 SDMA，混合形式也是可能的。比如著名的第 2 代系统 GSM（全球移动通信系统）使用 FDM 把分配的频谱划分成 124 载体，然后使用 TDMA 将每个载体切分成 8 个部分。在任意小区的潜在用户数是数不清的，区域中的任意用户能够进入小区，另外整个漫游者世界能呈现。幸运的是，某个时刻在某小区的用户数目、正在使用设备呼叫的用户数目通常是十分适中。问题是如何确定小区中哪些用户是在线以及如何给在线用户分配空闲的子信道。通过切换进入小区的移动设备/用户（mobiles/user），由移动交换局直接分配信道。问题仍然是对于刚刚上线的移动设备/用户做些什么，常见答案是使用随机接入信道（random access channel），这种方式可使任意用户在任意时间发送数据。如果两个用户在近似同一时间发送，他们的信号相互干扰，每个必须重新发送。因为来自移动设备/用户（mobiles/user）的声称其存在的信息十分短，且不频繁，随机接入信道的低利用率的特点不成问题。相似地，发起于移动设备/用户的控制信息可以在同一随机接入信道模式中传送。当会话或数据传输必要时，使用控制信息为移动设备/用户分配一条专用信道。

因此，相对短和少的信道分配和其他控制功能可使用随机接入方法发起，而较高流量活动在专用的会话子信道中执行，这个子信道通过多址接入方案获得。

在蜂窝电话（以及卫星通信）中，主要使用的多址接入方案是 FDMA（第 1 代系统 AMPS）、TDMA（比如数字 AMPS、数字 AMPS 的后续和也使用 FDM 的 GSM）和由高通公司（Qualcomm）开拓领先的 CDMA，这个列表是以实现复杂性增加和频谱利用率增高的顺

序。使用 TDM 技术，AMPS 的数字 AMPS 30kHZ 信道被分成子信道，在频谱利用上给出大约 3：1 的改进。高通公司声称，对于 AMPS 的 CDMA 系统有 10 倍的改进。CDMA 使用软切换，移动设备将旧小区和新小区中编码的功率相加。在其他方向，两个基站发射器比较接收的两个信号，以达到更好通信。

在美国，关于使用接入方法的争论一直存在。对于属于同一时期的系统，明显地 FDMA 十分浪费频谱。而且，随着廉价、高性能数字信号处理芯片的开发，FDMA 不再比 TDMA 容易实现。但是，TDMA 和 CDMA 之间的选择仍然是一个争论点。TDMA 的坚持者认为 CDMA 的理论优势难于在实际中实现，TDMA 有许多成功的经验。CDMA 的支持者辩论理论优势能够实现，CDMA 还能提供额外特征，诸如增加的范围。TDMA 系统在世界范围内的实现，起到了早期领头作用。但是，大的无线提供商很快开始与 CDMA 供应商签约，选择 CDMA 作为第 3 代系统的接入方式。

17.3　第 3 代无线通信

第 3 代无线通信的目的是提供相对高速的无线通信，支持除语音之外的多媒体、数据和视频传输。ITU 的 2000 年国际移动通信倡议（IMT-2000）定义了 ITU 关于第 3 代能力的观点，具体如下：

- 与 PSTN 可相比的语音质量。
- 大区域高速汽车用户可用的 144kbps 数据速率。
- 小区域站立或慢速移动的步行者可用的 384kbps 的数据速率。
- 支持 2.048Mbps 的办公使用。
- 支持分组交换和电路交换的数据服务。
- 与互联网的自适应接口，高效反映流入和流出流量之间的常见不对称。
- 以通用模式可用频谱的更加有效使用。
- 支持更广范围的移动设备。
- 为新技术和新服务的引入提供更好的灵活性。

服务提供商之间的竞争已经酿成了多种 3G 网络，以及满足或已超过 ITU-2000 种描述的最小能力的各种服务。许多供应商已经将他们的产品集中在围绕通用个人通信和通用通信接入等概念，第 1 个概念指个人通过唯一账户容易识别自身的能力，以及在一个国家、大陆甚至全球方便使用任意通信系统的能力；第 2 个概念指在各种环境，使用计算设备连接信息服务（比如便携式设备可以在办公室、街道和飞机上工作）的能力。正在进行的个人计算革新已经形成无线通信在几个重要方面的演化。

个人通信服务（PCS）和个人通信网络（PCN）是与全球无线通信的这些概念相隶属的名字，它们也形成第 3 代无线通信的目的。总而言之，概括地说，PCS 和 PCN 已经依赖 TDMA 或 CDMA，提供频谱的有效使用和高容量。

个人通信服务手机被设计成低功耗、相对小和轻，国际上已经做了几种努力以提供通用 PCS。例如，世界范围地将第 2 代无绳电话的频率分配在 800MHz 区域，对于更加高级的个人通信分配在 1.7 – 2.2GHz 的频段。

1992 年世界无线电行政大会（WARC 92）识别出未来公共陆地移动通信系统（FPLMTS）的世界分配，这个概念包括陆地和基于卫星的服务。另外，也为用于支撑低地球轨道卫星服

务（LEOS）做了分配。

归入个人通信服务的一些技术包括：美国数字蜂窝系统、日本数字蜂窝系统、第 2 代无绳电话（CT-2）、面向数字蜂窝服务的欧共体 GSM 和数字化欧洲无绳电话（DECT），这些涉及高级无线电话，也受 LEOS、对地球静止地球轨道卫星（GEOS）以及陆地天线的支持。已经成为第 3 代服务标志的技术是移动电话（智能手机）和能访问 Web 服务的其他移动设备。

第 3 代移动网络于 2003 年由美国发起，声称为北美第 1 个移动宽带网络。提供商们已经开发了许多种 3G 网络，具有范围从 400kbps ~ 4Mbps 或更高的互联网速度。

从消费者购买模式上，已经观察出 3G 技术和服务的流行性，智能手机的销量数目大于个人计算机。这一现象导致一些工业专家宣告我们已经进入企业数据通信的“后 PC”时代。

访问因特网、查收电子邮件、发送文本信息和运行移动应用的能力已经助燃了消费者对智能手机的需求，使用智能手机进行语音通信（电话呼叫）看起来也像是一些移动用户后来添加的东西。这些能力也强调了企业通信网络中移动设备的增多。另外消费者中移动应用的流行，业务也正在快速确保移动平台支持他们的业务软件。

到 2012 年，4 个主要的移动设备平台出现，主导着移动业务市场，它们分别是：iPhone、Blackberry（来自 RIM）、Droid 和 iPad。大多数大公司针对他们的移动性倡议，采用的态度是“装置竞赛”或带自己的设备（BYOD），而不是告诉用户他们将支持什么或不支持什么，公司把决策留给他们的移动决策者的偏好。对于 iPad 的支持与 ITU 初始的通用通信服务的愿景是一致的。虽然 iPad 没有被用于蜂窝语音服务，但它能使用蜂窝网络访问因特网。

智能手机和移动平板设备访问因特网的能力是它们在企业用户中如此流行的主要原因，这些能力是基于无线应用协议的演化。

17.3.1　无线应用协议

无线应用协议（Wireless Application Protocol，WAP）是 WAP 论坛开发的通用、开放标准，给移动用户提供访问电话和信息服务的能力，包括互联网和 Web。WAP 的设计能够与所有无线网络技术一起工作（比如 GSM、CDMA 和 TDMA），也是尽可能基于现有的互联网标准，诸如 IP、XML、HTML 和 HTTP。而且，它包括安全能力。爱立信、摩托罗拉、诺基亚和 phone.com 于 1997 年建立了 WAP 论坛，后来于 2002 年并入开放移动联盟，就是这个组目睹 WAP 的演化。1999 年 6 月，WAP 论坛发布了 WAP v1.11，截至 2012 年，WAP 2.0 是 WAP 的当前版本。

开发 WAP 主要是用于处理蜂窝和其他无线网络的限制，向移动设备提供数据服务。相对于个人计算机，传统上移动设备具有有限的处理器、内存和电池生命。某些设备用户接口也有限，显示屏幕比较小。与基于有线的 WAN 服务相比，无线网络具有相对低的带宽、高延迟和不可预测的可用性与稳定性。而且，所有这些特征对于不同的移动设备、对于不同的无线网络其变化很大。最后，移动无线用户有不同的预期期望，以及来自其他信息系统用户的需求。例如，移动设备必须极度容易使用，比桌面工作站、台式机和个人计算机更加容易使用。起初开发 WAP 的目的是处理这些挑战，它的演化已经与它运行所在移动设备的演化并行。

WAP 规范包括下面内容：

- 基于 WWW 编程模型的编程模型。
- 遵循 XML 的标记语言——无线标志语言（Wireless Markup Language，WML）。

- 适合于移动、无线设备的小浏览器规范。
- 轻量级通信协议栈。
- 无线电话应用（WTA）框架。

17.3.2　WAP 编程模型

WAP 编程模型基于 3 个元素：客户端、网关和源服务器（见图 17-8），在网关和源服务器之间使用 HTTP 传输内容，网关作为无线域的代理服务器，它的处理器提供卸下手提式终端、移动无线终端有限能力的服务。例如，网关提供域名系统（DNS）服务，负责 WAP 协议栈和 WWW 栈之间的转换（HTTP 和 TCP/IP），把来自 Web 的信息编码成一种更加紧凑的形式，以最小化无线通信，在另外 1 个方向解码紧凑压缩形式成标准的 Web 通信规程。另外，网关也频繁缓冲请求的信息。



图 17-8　WAP 编程模型

17.3.3　无线标记语言

无线标记语言 WML 没有假定标准键盘或鼠标作为输入设备，而是设计与移动无线设备常见的电话键区、书写笔和其他输入设备一起工作。WML 文档被划分成小型、定义好的用户交互单元，这一单元称为卡片（card）。用户通过前后移动卡片实现导航，使用适合基于电话系统的标记标签集合。

17.3.4　微浏览器

设计 WAP 1.1 版本规定的微浏览器主要是用于向用户提供因特网访问，使用传统 12 个键的手机键盘输入包括字母与数字的字符。用户使用上下滚动键而不是鼠标，实现 WML 卡之间的导航，也提供来自 Web 的相似导航特征，比如返回、主页以及书签。

当前使用的微浏览器更加健壮，它们有多个名字，包括移动浏览器、迷你型浏览器或无线因特网浏览器（Wireless Internet Browser，WIM），所有这些是在移动设备上使用的浏览器，诸如移动电话、平板电脑或个人数字助理系统（PDA）。

微浏览器被优化，可在便携设备的小屏幕上有效显示 Web 内容。典型地，浏览器软件小且高效，主要为适应无线设备的有限存储能力和它们访问因特网使用的低带宽连接。实质上，移动浏览器是传统 Web 浏览器的分解。然而，自从 21 世纪 00 年代中期以来，一些移动浏览器已经发展到可处理最近的技术，诸如 Ajax、CSS 2.1 和 JavaScript。

移动 Web 是 Web 站点集合和无线门户的另一个名字，面向来自移动浏览器的访问而设计。一些网站为使用移动设备访问 Web 站点的用户，自动生成 Web 网页的“移动”版本。移

动浏览器通过蜂窝网络和 / 或通过无线 LAN，使用标准 HTTP 协议链接，而且大多数显示使用 HTML、WML 或 XHTML 移动轮廓（WAP 2.0）编写的 Web 页面。

17.3.5　无线电话应用

无线电话应用（Wireless Telephony Application，WTA）为局域和广域电话系统提供一种接口。因此使用 WTA，应用开发商能使用微浏览器发起电话呼叫和响应来自电话网络的事件。

17.3.6　配置样例

图 17-9 示出一个可能的 WAP 配置框图，图中有 3 个网络：因特网（排除无线网）、PSTN 和无线网络（比如蜂窝或 Wi-Fi）。客户端可能是手持式设备、无线网络中的智能手机，在图 17-9 的例子中，客户端与两个网关通信。一个是与因特网相连的 WAP 代理，这个代理代表设备与互联网上的服务器通信，将 HTML 信息转变成 WML、HTML 或 WAP 2.0，并将其发送到设备。移动 Web 的资料直接传递给移动设备，不需要进行翻译转换。另一个网关是 WTA 服务器，连接到 PSTN 的网关，因此移动设备能通过微浏览器访问基于电话的功能，诸如呼叫控制、电话本访问和即时消息。



图 17-9　WAP 网络原理图

17.4　第 4 代无线通信

智能手机和蜂窝网络的演化已经开辟了新一代能力和标准，这些统称为 4G。设计 4G 系统是为了给多样的移动设备提供超宽的带宽访问因特网，包括便携式电脑、智能手机和平板式 PC。4G 网络被设计用于支持移动 Web 访问和高带宽应用，诸如高清晰度移动电视、移动视频会议和游戏服务。

17.4.1　第 4 代网络需求

ITU 已经发布了 4G 网络的指示。根据 ITU，高级国际移动通信（IMT-Advanced）蜂窝系统（或 4G 系统）必须满足许多最小需求，包括以下几个方面：

- 基于全 IP 分组交换式网络。
- 面向高移动性设备，支持高峰期数据速率近似达到 100Mbps；面向低移动性访问，比如本地无线访问，高峰期数据速率近似达到 1Gbps。
- 动态共享和使用网络资源，以支持每小区更多的并发用户。
- 支持跨异构网络的平滑切换。
- 支持下一代多媒体应用的高服务质量。

到 2012 年，2 个系统：移动 WiMAX 标准和长期演进（LTE）标准出现了，它们作为 4G 网络的标准。移动 WiMAX 标准于 2006 年由韩国发起，于 2008 年年初首先由美国 Sprint Nextel 采用。LTE 标准于 2009 年在斯堪的纳维亚发布，从 2010 年起来自美国 MetroPCS 和其

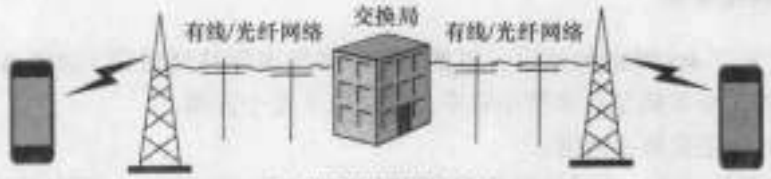
他蜂窝提供商的服务一直可用。LTE 智能手机和 WiMAX 智能手机分别从 2011、2010 年起开始可用，但是截至 2012 年，WiMAX 和 LTE 智能手机在欧洲市场均不可用。

与较早的几代通信系统相比，4G 系统并不支持传统电路交换式电话服务，仅支持 IP 电话。正如在表 17-2 中观察到的，3G 系统的扩频无线电技术特征已经被 4G 系统的正交频分复用（OFDMA）多载波传输和频域均衡方案代替。

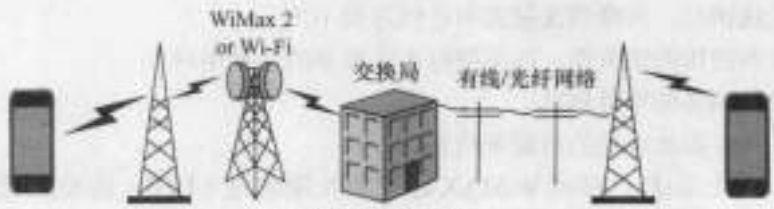
表 17-2　第 3 代与第 4 代网络

因素	3G	4G
频段	1.8 – 2.5GHz	2 – 8GHz
网络	基于广域小区	无线 LAN+广域
服务	CDMA2000、EDGE、UMTS	WiMAX2、LTE-Advance
高峰上传速率	50Mbps	500Mbps
高峰下载速率	100Mbps	1Gbps
静止带宽	2Mbps	1Gbps
移动带宽	384kbps	100Mbps
数据速率	每秒 3M 字节	每秒 1G 字节
交换技术	分组交换；电路交换	分组交换（IP）
无线电技术	扩频；TDMA；CDMA	OFDMA；MIMO；OFDM

图 7-10 展示出 3G 与 4G 蜂窝网络之间的几个主要差异。正如从图 17-10a 中观察到的，3G 网络中基站与交换局之间的连接典型地是基于电缆的，或许是铜或光纤。支持电路交换，能启用移动用户与连接到 PSTN 的电话之间的语音连接。另外，3G 网络中的因特网访问也可以通过交换局实现路由。相比较而言，在 4G 网络中，正如用于因特网访问的 IP 分组交换连接，IP 电话是规范，由基站和交换局之间的无线连接（诸如 WiMAX）实现 IP 电话（见图 17-10b）。使用具有 4G 功能智能手机的移动用户之间的连接，从来不通过基于电缆、电路交换连接实现路由，它们之间的所有通信是基于 IP，由无线链路处理，这种组织为移动到移动视频呼叫 / 视频会议服务的部署及语音和数据服务的同时传送提供便利，比如电话呼叫的同时浏览 Web 页面。4G 移动用户仍然能连接 3G 网络用户和 PSTN 用户，这主要是通过交换局之间的电缆 / 光纤电路交换连接。



a）第3代蜂窝网络(3G)



b）第4代蜂窝网络(4G)

图 17-10　第 3 代与第 4 代蜂窝网络的比较

17.4.2 正交频分多址（OFDMA）

在 4G 系统中，新的频谱共享方案很重要，曾经被看作是带宽浪费者的频分多址（FDMA）被带回到应用中来。新的多路复用方案包括单载波 FDMA（SC-FDMA）、正交 FDMA（OFDMA）、交织 FDMA 和多载波 CDMA（MC-CDMA），这些均是以快速傅里叶变换（FFT）和频域均衡机制为基础。共同地，这些使 4G 服务提供商可灵活地控制带宽和频谱。然而，它们也需要高级能力，比如动态的信道分配和流量自适应调度。

OFDMA 与 CDMA 的扩频相似，这主要是由于通过分配不同的扩频因子，用户能达到不同的数据速率。它也支持把许多不同的扩频节点分配给每个用户，OFDMA 被描述为频域和时域多路复用的组合。使用 OFDMA，传输资源可根据某一分配的频率范围内的时间槽划分。

人们认为，OFDMA 高度适合于宽带无线网络，它被使用在 WiMAX、IEEE 802.16 无线城域网（MAN）标准和 IEEE 802.20 移动无线城域网络，它还被使用在 LTE- 高级下行链路信道。OFDMA 的一些主要优势包括可扩展性、MIMO 友好性和频率信道选择性的提升，新的 4G 技术的一个关键优势是接收端为了均衡而需求的复杂性低。这一点在 MIMO 环境中可能是特殊的优势，因为在这种环境中空间复用传输固有地要求接收端的高复杂性均衡。

17.4.3 4G 网络演化

人们预期 4G 网络、设备和服务在下个十年会快速发展。截至 2012 年，4G 服务地理分布十分有限。在美国，仅仅大都市才可用 4G 服务。因为它们使用新的复用方案，比如 OFDMA，支持相当高的上行和下行速度，4G 网络服务的首次展出也将被 4G 功能的智能手机的进化所缓和。例如，截至 2012 年 iPhone 不是一个 4G 设备，这意味着 iPhone 的支持者在设备和 4G 服务之间有一项选择，他们不可能有这两个。毫无疑问，当 4G iPhone 变得可用时，它将有高需求，但是成千上万的 iPhone 用户将必须买新的手机，才能连接到 4G 网络。

工业专家预计，进入 21 世纪 20 年代，CDMA 和 OFDM 将在蜂窝网络中共存。4G 网络在发展和成熟的同时，以 CDMA 为基础的 3G 方案仍然有可能是移动运营商的核心蜂窝服务选择。随着时间的推移，全世界的无线用户基地将迁徙到 4G 技术，但是由于移动设备使用数量的日益增加，迁徙周期可能是冗长的。

17.5 卫星通信

在电信和数据通信的发展过程中，卫星通信的重要性是可以与光纤相比拟的。

处于地球之上的稳定轨道里，卫星通信系统的心脏是基于卫星的天线。在卫星通信系统中，处于地球附近的两个或多个基站通过 1 个或多个卫星进行通信，这些卫星起到空间中继站的作用。在地球上或接近地球的天线系统称作**地面接收站**（earth station），从地面接收站到卫星的传输称为**上行链路**（uplink），相反从卫星到地面接收站的传输称为**下行链路**（downlink）。卫星通信系统中，接收上行链路信息并把其转为下行链路信号的电子设备称为**转发器**（transponder）。

17.5.1 卫星轨道

对地球静止地球轨道卫星 今天非常常见的通信卫星类型是对地球静止地球轨道（GEO）卫星（GEOS），这个卫星于 1945 年由科幻作者 Arthur C. Clarke 首次提出。如果卫星处于地面上空 35 863 公里的圆形轨道，且朝着地球的赤道平面运转，它将以地球同样的角速度运

转，将保持在赤道上同一个地点的上方[⊖]。图 17-11 以地球大小成比例地描绘 GEO，图中的许多卫星符号用于表明 GEO 中有许多卫星，且这些卫星彼此相距很近。



图 17-11　对地球静止地球轨道（GEO）

GEO 有以下几个优势值得推荐：

- 由于卫星相对地球是静止的，不存在由卫星和地球天线相对运动带来的频率变化问题（多普勒效应）。
- 按照地面接收站追踪卫星的过程大大简化。
- 在地面 35 863 公里的高度，卫星可以覆盖地球表面大约 1/4 的通信。GEO 中按照 120 度分离开的 3 个卫星能够覆盖整个地球的大多数居住部分，除非接近南极和北极的区域。

另一方面，GEO 也有一些问题：

- 穿越 35 000 公里后，信号会变得十分微弱。
- GEOS 在极地区域和较远的南、北半球的服务质量差。
- 即使以光的速度，大约每秒 300 000 公里的速度，从卫星下方赤道上一点到卫星之间发送信号及其返回的延迟不可忽略。

事实上，处于卫星正下方的地球上两个位置之间的通信延迟是（2×35 863）/300 000≈0.24s。对于不在卫星正下方的其他位置，延迟甚至更长。如果卫星链路用于电话通信，一个人说话和另一个响应之间增加的延迟是两倍，几乎达到 0.5s，这明显可以觉察到。GEO 的另一个特征是它们在非常大的面积使用分配的频率，对于一点对多点的应用，比如广播电视节目，这是比较可取的，但是对于点对点通信非常浪费频谱。限制卫星信号覆盖区域的特殊点和控制波束天线，能够被用来控制“脚印”或信号区域。为了解决这些问题，为卫星设计了多种轨道：低地球轨道卫星（LEOS）和中地球轨道卫星（MEOS），而不是 GEO。对于第 3 代个人通信，LEOS 和 MEOS 是非常重要的。

1. LEOS

LEOS（见图 17-12a）有以下特点：

- 在小于 2000 公里的圆形或轻微椭圆轨道，假定的和实际的系统在 500 ~ 1500 公里的范围内。
- 轨道周期在 1.5 - 2 小时的范围。
- 覆盖范围直径大约 8000 公里。
- 往返信号传播延迟小于 20ms。
- 从地球上某个固定点（无线电水平线之上）可见卫星的最大时间达到 20 分钟。
- 由于卫星相对地球上某个固定点的运动比较快，LEOS 系统必须能够处理大的多普勒

⊖ 术语与地球的位置相对不变（geosynchronous）经常用在对地球静止（geostationary）的地方。对于纯粹主义者，差异为：与地球的位置相对不变轨道是在 35 863 公里高度的任意圆形轨道，对地球静止轨道具有 0 倾斜的与地球的位置相对不变的轨道，因此卫星盘旋在地球赤道上一个位置的上方。

频移，这个频移改变信号频率。

- 在 LEOS 上大气阻力很大，导致渐进的轨道恶化。

这个系统的实际使用需要涉及多个轨道平面，且每个平面轨道中有多个卫星。两个地面接收站之间的通信典型地涉及从一个卫星到另一个的信号切换。

与 GEOS 相比，LEOS 有许多优势。除了前面提到的传播延迟减小之外，对于同一个传输功率，接收的 LEOS 信号比 GEOS 信号强。LEOS 范围能够比较好地局部化，因此能够很好地节约频谱。由于这个原因，当前这个技术被提议用于需要较强信号运行的移动设备和个人计算设备通信。另一方面，为了提供超过 24 小时的广范围覆盖，需要使用许多卫星。



a）低地球轨道：在500到1500公里高度的极地轨道



b）中地球轨道：倾向于赤道，在5000到12000公里高度

图 17-12　低地球轨道和中地球轨道

迄今为止，已经提出许多使用 LEOS 簇的商业化提案，以提供通信服务。这些提议能够划分成两类：

- 小 LEOS：倾向于工作在通信频率低于 1GHz，使用不超过 5MHz 的带宽，支持的数据速率达到 10kbps。这些系统旨在针对寻呼、跟踪和低速率消息，Orbcomm 是这种卫星系统的一个例子。它是第一个在运行的 LEOS，而且它的前两个卫星在 1995 年 4 月发射。设计 Orbcomm 主要是为了寻呼和突发通信，优化处理长度在 6 ~ 250 字节的小突发数据。企业使用它跟踪拖车、有轨车、重型设备和其他远程移动资产。它也能用于监控远程公用表、油与气存储箱、井和管线，也能用于与世界任何地方的远程工作者保持联系。Orbcomm 到卫星使用的频率在 148 ~ 150.05MHz 的范围，离开卫星的频率在 137 ~ 138MHz 的范围。在低地球轨道，它有 30 多个卫星，支持到卫星的用户数据速率为 2.4kbps，下行的数据速率为 4.8kbps。
- 大 LEOS：工作频率在 1GHz 以上，支持的数据速率达到几兆比特位每秒。这些系统倾向于提供与小 LEOS 相同的服务，另外添加语音和定位服务。Globalstar 是大 LEOS 系统的一个例子，它的卫星相对不成熟。与其他小 LEOS 系统不同，它没有卫星之间的板上处理和通信，大多数处理工作由系统的地面接收站执行。它使用 CDMA 就像在 CDMA 蜂窝标准中，使用 S-Band（大约 2GHz）实现到移动用户的下行链路。Globalstar 与传统语音载体紧密集成，所有呼叫必须通过地面接收站处理。整个卫星群由 48 个运行卫星和 8 个备用卫星组成，它们在 1413 公里高的轨道运行。

2. MEOS

MEOS（图 17-12b）有以下特点：

- 圆形轨道在 5000 – 12 000 公里的高度。
- 轨道周期大约 6 小时。
- 覆盖范围直径从 10 000 到 15 000 公里。
- 往返信号传播延迟小于 50ms。
- 从地球上某个固定点（无线电水平线之上）可见卫星的最大时间是几个小时。

MEOS 需求的切换次数比 LEOS 少得多。虽然从那些卫星到地面的传播延迟和需求的功率比 LEOS 大，但仍然比 GEOS 实质上小很多。1995 年 1 月成立的新 ICO 提出一个 MEOS 系统，并于 2000 年开始发射。包括 2 个备用在内的 12 个卫星被规划在 10 400 公里高的轨道，这些卫星被等分在与赤道成 45 度倾斜角的两个平面之间，建议的应用是数字语音、数据、传真、高穿透通知和消息服务。

17.5.2　卫星网络配置

图 17-13 以通用的方式描述了两个常见的卫星通信配置。第一个配置中，卫星用于为两个远距离的地面天线提供点对点链路。第二个配置中，卫星为一个地面发射器和多个地面接收器提供通信服务。

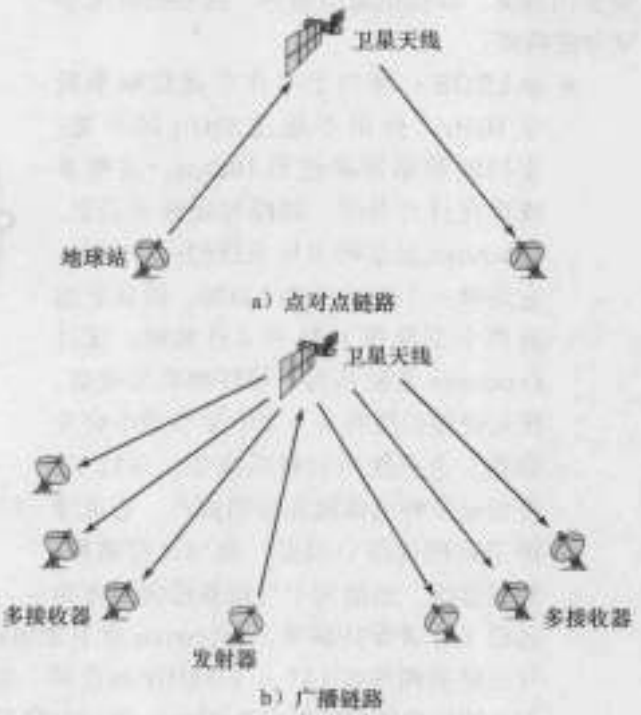


图 17-13　卫星通信配置

17.5.3　应用

通信卫星是像纤维光学一样重要的技术革新。对于卫星而言，非常重要的应用如下：

- 电视分配。
- 卫星无线电服务。
- 长途电话传输。
- 专用企业网络。

由于它的广播本质，卫星非常适用于电视分配，出于这个目的，在美国甚至整个世界被广泛使用。它的传统使用是提供来自于中央位置的编程，程序被传送到卫星，接着向下广播到许多接收站，它们进一步将程序分发到个人观众。对于电视分配，卫星技术的另一个应用是直接广播卫星（Direct Broadcast Satellite，DBS），在这种应用中卫星视频信号直接传送给家庭用户。

卫星无线电服务，比如 Sirius XM 和 Worldspace，允许移动用户听同一个音频节目，无论他们走到哪里，尤其是某些用户有大陆范围的足迹。其他音频节目，比如 Music Choice 或 Muzak 的卫星传送内容，需要一个类似盘子的天线和一个固定位置的接收者。在固定位置和移动无线电服务中，天线必须对卫星有个清晰的视野。在高楼、桥梁或停车库等使信号模糊

的区域，可使用中继器使信号对接听者可用。无线电服务通常是基于订阅，使用私有信号，需求专用的接收硬件实现解码和回放。提供商使用户能够访问新闻、天气、体育、谈话、喜剧和音乐频道等多种节目范围，比如 Sirius XM，而且大多数音乐频道是无商业化广播。

卫星传送也用于公共电话网络中电话交换局之间的点对点干线，对于使用率高的国际干线，它是一个有用的媒体，而且对于许多长距离国内链路，尤其是在偏远不发达地区，可在地面系统中竞争胜出。

最后，卫星也有许多企业数据应用，卫星提供商能够把总容量划分成许多信道，并租用这些信道给个别的企业用户。在许多位置配有天线的用户，能够使用卫星信道做专用网络。传统上，这些应用一直是十分昂贵的，局限在有高容量需求的大型组织。今天，甚小口径天线地球站（VSAT）系统提供了一个低成本选择，图 7-14 给出一个典型的 VSAT 配置。许多用户站配有低成本的 VAST 天线，这些站使用某一原理共享传送到中转站的传输容量，这个中转站能和每个用户交换信息，以及在用户之间中转信息。

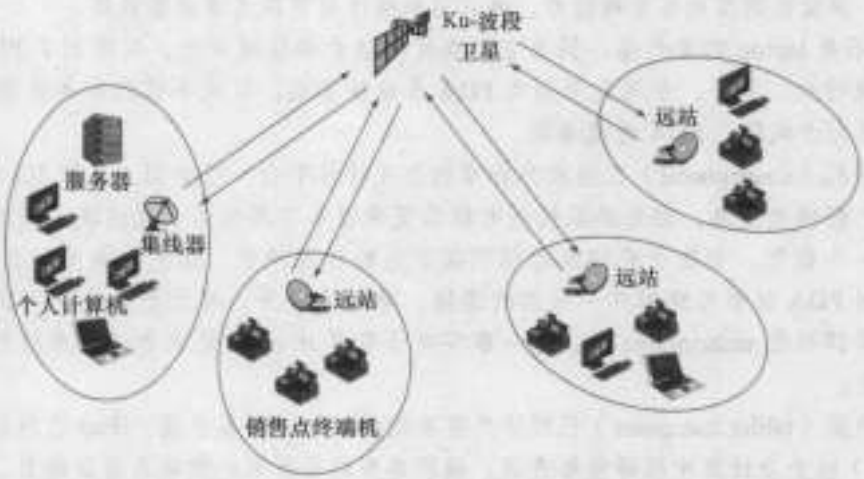


图 17-14　典型甚小口径天线地球站（VSAT）配置

应用注解

便携式电脑（Laptop）、上网本（Netbook）、掌上电脑（PDA）和手机（cell phone）

企业面临着与计算资源相关的几个问题。虽然一个组织购买几十、甚至上百台台式机非常常见，但越来越多的组织也必须做移动计算设备的决策，这个选择真正取决于设备的预期应用或用途。不只一个公司由于购买超过应用能力的设备已经使预算捉襟见肘，或者是对于购买这些设备支持的任务而言，这些设备不令人满意，剩下的是让设备收集灰尘。为了能够做正确的决策，必须做企业工具与人物的匹配分析。

当企业想起移动设备时，传统上便携式电脑一直是想起来的第 1 个选项。便携式电脑有大量的处理能力、内存和硬盘容量，典型情况下它们都配有内置的 Wi-Fi 连接，这使得便携式电脑非常有吸引力，因为不需要购买无线网卡，除非需要通过蜂窝网络获得 Internet 访问。与扩展坞（docking station）结合，便携式电脑能够扩展双倍性能，就像台式机。便携式电脑有较暗的边，这使得它一样有吸引力。由于键盘风格和内嵌的是触摸板而不是鼠标，导致便携式电脑有时比较难以使用。当在桌面模式工作时，许多用户倾向于

有较大的显示器、扩展的键盘和一个额外鼠标。购买便携式电脑的另一个负面是，如果laptop实际上用作移动工作站，电池运作起来很少像所宣传的待机时间。每个活动进一步耗尽电池，真正的移动用户必须熟悉节能模式设置，或者手边备有第2个电池。然而，对于需求处理能力、大的存储容量和易于访问他的/她的文件的用户，当从家里移动到办公室时，laptop或许代表最好的方案。

在移动工作者之间，上网本和迷你型laptop已经经历了一波流行潮。它们重量上小又轻，电池寿命经常比标准型号的laptop要好。许多用户认为，旅行时他们便于携带，比较舒适。然而，典型情况下上网本处理器的能力不如laptop中安装的处理器能力强，这使得他们难以处理大的文件的上传或下载。

个人数字助手（PDA）是一种移动设备，移动工作者使用它作为个人信息管理者。PDA也称为掌上型电脑或个人数字助理，大多数PDA有连接因特网的能力。由于PDA有可视化显示，典型地它支持微浏览器。大多数通过Wi-Fi或蜂窝连接访问因特网、内部网或外部网。当前的模型也有音频能力，使它们能够作为便携式媒体播放器。

PDA不是laptop的替代品，因为它没有处理能力和存储能力，这限制了PDA作为计算设备的流行性。另外，今天几乎所有PDA是智能手机，智能手机的发展及其替代PDA的能力已经大大减弱了PDA的销售额。

智能手机（smartphone）已经成为标准的企业计算平台。在美国，虽然3G和4G移动Web服务已经快速发展，但是美国提供的移动宽带服务与其他几个发达国家提供服务的水平不在同一个级别。智能手机的真正强项在于它的任意地点、任意时间的语音和Internet连接。虽然PDA经常可提供同一网络的连接，典型情况下，对于企业用户而言，PDA提供的功能多样性比smartphone少，这一事实对于需要Internet访问和语音支持的laptop用户同样适用。

平板电脑（tablet computer）已经作为重要的移动计算设备出现。iPad已经帮助苹果公司（Apple）在企业计算中取得重要进展。虽然典型的平板式电脑缺乏语音能力，但它们提供WiFi和/或蜂窝网络连接。这一点加上平板式PC操作系统提供的用户友好的触摸屏接口，已经使它们在企业用户和消费者之间极度流行。

情况经常是这样的，我们必须首先问自己，“我们正在试图做什么？”或者“我们需要做什么？”。一旦回答了这些问题，一般情况下比较容易发现满足组织需求的解决方案。上网本、智能手机、平板式电脑，虽然经常被认为是必需的工具，但通常不是计算能力强的laptop或台式计算机的替代品。从纯粹便携式角度来看，携带一个钱包大小的或者便笺簿尺寸的设备比正常尺寸的laptop可行。另一方面，想要和需求之间会存在比较大的差异，尤其是涉及底线的地方。在购买智能手机之前或之后，会建议公司看看使用模式，以确定智能手机是否真的必要。即使如果laptop的能力是当前最好的解决方案，智能手机和平板电脑的改进已经让我们努力判断哪一个设备对于下一代连接是最好，因为它们之间的界限不再清晰地定义。

17.6　总结

传统上，蜂窝无线网络支持移动电话，但是现在也支持无线因特网访问和其他无线数据网络应用。蜂窝网络遍布世界，传送的长距离语音和数据流量的比例一直在增加。蜂窝系统的基础原理是使用大量相对小的地形区域（称为小区，cell），来覆盖大的区域。每个小区分

配一个频段，由发射器、接收器和控制单元组成的基站提供服务。邻接的小区分配不同的频率，以避免相互干扰和串话。然而，彼此相距充分远的小区可使用同一频段。

通过某种复用方案，许多用户共享每个小区内可用的容量。对于某一系统，复用是基于 TDMA、FDMA、CDMA 或这些方法的组合。

蜂窝网络的演化还在进行中，3G 和 4G 的技术与方案已经开发出来。4G 的技术和服务正在由移动运营商铺开，有潜能为用户提供重要的性能增强。然而，在未来的 10 年，3G 和 4G 有可能共同存在。

无线通信的另一个重要形式是卫星通信。传统上，大多数卫星流量由 GEOS 传送，最近引入了使用 LEOS 和 MEOS 的网络。

案例研究 X：旅馆选择

在这个案例研究中，讨论的主要概念包括基于卫星的通信和无线广域网。**读案例研究和更多细节可参照网址：www.pearsonhighered.com/stallings。**

17.7　关键术语、复习题和练习题

关键术语

base station（基站）
cell sectoring（小区扇形化）
cell splitting（小区分裂）
cellular wireless network（蜂窝无线网络）
downlink（下行链路）
earth station（地面接收站 / 转播站）
Fourth Generation（4G，第 4 代）
Geostationary Earth Orbit Satellite（GEOS，对地球静止地球轨道卫星）
microcell（微蜂窝）
multiple access（多址）
Orthogonal Frequency Division Multiple Access（OFMDA，正交频分多址用）
transponder（发射机应答器）
uplink（上行链路）
Wireless Markup Language（WML，无线标记语言）

复习题

17.1　在蜂窝网络中使用什么样的几何形状？
17.2　在蜂窝网络中，频率重用的原理是什么？频率重用为什么是重要的？
17.3　在蜂窝网络中，控制信道和流量信道之间的差异是什么？
17.4　蜂窝切换是什么？
17.5　当多址接入应用于蜂窝通信时，描述多址接入意味着什么？
17.6　识别当今蜂窝网络中非常流行的多址接入方法。
17.7　简要解释 CDMA 的原理。
17.8　无线应用协议（WAP）是什么？
17.9　第 3 代（3G）网络的主要特征是什么？
17.10　第 4 代（4G）网络的主要特征是什么？

17.11 识别并简要描述卫星通信系统的关键部件。

17.12 解释 GEOS、LEOS 和 MEOS（包括缩写表示什么），就轨道尺寸和形状、信号功率、频率重用、传播延迟、用于全球覆盖的卫星数和切换频率这几个因素，比较这 3 种类型。

17.13 识别组织怎样分别使用 GEOS、LEOS 和 MEOS。

17.14 识别和简要描述 VSAT 系统的特征和使用。

练习题

17.1 在每个地形区域，有许多蜂窝提供商提供服务，且每一个可使用不同的技术。

a. 在你的区域，谁是提供商，使用的多址接入技术是什么？

b. 你或你的家人 / 朋友使用的蜂窝电话采用的是什么技术？

17.2 对人口密度稠密的城市区域的微蜂窝做因特网调查，定位与微蜂窝大小、基站与交换局部署的相关信息。用 500 ~ 750 字的论文或 5 ~ 8 页幻灯片演示文稿总结你的发现。

17.3 描述与图 17-5 中相似的事件序列，主要是面向：

a. 从移动设备到固定用户的呼叫。

b. 从固定用户到移动设备的呼叫。

17.4 对移动 Web 做因特网调查，定位移动 Web 与传统因特网资源相比的信息。识别消费者中十分流行的移动 Web 应用例子，并把这些例子与在企业用户中流行的应用作比较。用 500 ~ 750 字的论文或 5 ~ 8 页幻灯片演示文稿总结你的发现。

17.5 对美国的蜂窝网络系统及服务与世界上其他高度发达国家的进行比较，就此做因特网调查、定位这些比较信息。美国是怎样发展起来的？一些高度发达国家的蜂窝系统优于其他国家的原因是什么？用 500 ~ 750 字的论文或 5 ~ 8 页幻灯片演示文稿总结你的发现。

17.6 对典型甚小口径天线地球站（VSAT）系统的商业应用展开因特网调查，识别企业通过 VSAT 可能支持的应用类型的相关信息，与其他业务数据通迅设施相比较，确定 VSAT 系统的成本。用 500 ~ 700 字的论文或 5 ~ 8 页幻灯片总结你的发现。

17.7 全球移动通信系统（GSM）是数字蜂窝通信的国际标准，针对 GSM 网络的 3 个主要功能实体对 GSM 做基本的回顾。GSM 策略是优于还是劣于 CDMA？提供你的答案。

17.8 目前，人们已经提出了关于使用移动电话的潜在健康危险。讨论与移动电话技术相关的潜在健康危险，并思考应该采取什么措施来最小化这种危险。

第六部分

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

管理问题

第 18 章

Business Data Communications: Infrastructure, Networking and Security, Seventh Edition

计算机和网络安全威胁

学习目标

通过本章的学习，读者应该能够：

- 描述保密性、完整性和可用性的关键安全需求。
- 描述计算机和网络威胁的主要分类。
- 讨论入侵者以及入侵者访问计算机系统使用技术的类型。
- 讨论恶意软件的种类。

本章给出了安全威胁的概述。我们首先讨论计算机安全的含义。本质上，计算机安全处理与计算机相关的资产，这些资产受到各种威胁。为了保护这些资产，人们采取了各种措施。本章剩余部分着眼于两大类计算机和网络安全威胁：入侵者和恶意软件。

加密算法（例如，加密和哈希函数），在计算机安全威胁和计算机安全技术中都发挥着作用。附录 J 给出了这些算法的概述。

18.1 计算机安全概念

NIST 计算机安全手册 [NIST95] 定义计算机安全为：

> **计算机安全**：为达到保持信息系统资源（包括硬件、软件、固件、信息 / 数据和通信）完整性、可用性和保密性的适用目标，给自动化信息系统提供的保护措施。

这个定义引入了位于计算机安全核心中的 3 个关键目标：

- **保密性**：这个术语涵盖了两个相关的概念：
  - **数据[⊖]保密性**：确保未经授权的个体无法获得和发现私有信息或者机密信息。
  - **隐私**：确保个人能够控制或者改变与他们相关的信息的收集和保存，以及该信息能够被谁查看、对谁公开。
- **完整性**：这个词包含了两个相关的概念：
  - **数据完整性**：确保信息和程序的更改只能按照指定的和授权的方式进行。
  - **系统完整性**：确保系统按照未受损的方式完成其预定的功能，不受对程序有意或无意的非法操作的影响。
- **可用性**：确保系统即时工作，不会拒绝授权用户的服务请求。

这三个概念组成了所谓的 CIA 三要素（见图 18-1），体现了数据、信息和计算机服务的

⊖ RFC 2828（因特网安全词汇）定义信息为“用来表示多种数据形式的事实和观点”，定义数据为“以具体物理表示的信息，通常是有意义的符号序列，尤其是能够由计算机处理和产生的信息表示”。安全文献并不典型地做过多区分，本章也不做区分。

基本的安全目标。例如，NIST 标准 FIPS 199（联邦信息和信息系统安全分类标准）将保密性、完整性、可用性列为信息和信息系统的 3 个安全目标。FIPS PUB 199 从安全缺失的定义和需求两个方面，为这 3 个目标提供了一种有用的解释：

- **保密性**：维护信息获取和泄露的授权限制，包括保护个人隐私和专有信息的方法。保密性缺失是指信息的非授权泄露。
- **完整性**：防止不适当的信息修改与破坏，包括确保信息的不可否认性和真实性。完整性缺失是指对信息未经授权地修改与破坏。
- **可用性**：确保及时、可靠地访问和使用信息。可用性缺失是信息或者信息系统访问或使用的中断。



图 18-1　安全需求三要素

虽然利用 CIA 模型来定义安全目标已经较为完善，但安全领域中的有些人认为需要一些额外的概念来展示一个完整的图。两个最常提及的概念为：

- **真实性**：真实的并且能够被认证和信任的特性；对一次传送、一条信息、信息源正确性的信心。这意味着确认用户确实是其所说的人以及每次到达系统的输入来自可信源。
- **可追踪性**：产生一个实体的行为可以唯一地追溯到那个实体的安全需求目标。它支持不可抵赖、威慑、故障隔离、入侵检测和保护以及事后恢复和合法行动。因为真正的安全系统是一个还未达到的目标，所以我们必须能够跟踪安全违反到责任方。系统必须保存他们行为的记录，以便之后的对追溯安全违规或者协助事务纠纷的取证分析。

注意，FIPS PUB 199 将真实性包含在完整性中。

18.2　威胁、攻击和资产

我们现在来看看与计算机安全相关的威胁、攻击和资产。

18.2.1　威胁和攻击

表 18-1 基于 RFC 2828 描述了 4 种安全威胁的后果，并列出了造成相应后果的攻击类型。**未经授权的泄露**是对保密性的一种威胁。下列攻击方式能导致这种威胁结果：

- **暴露**：这种方式可以是故意的，比如内部员工故意将敏感信息（如信用卡账号）提供给外人。这种方式也可能是由于人、硬件或软件造成的错误，导致实体得到未经授权的敏感信息。像这样的例子有很多，例如学校偶然地将学生的机密信息公布在互联网上。
- **窃听**：窃听是一种在上下文通信中常见的攻击。在共享局域网中，例如无线局域网或者广播局域网，任何一台接入局域网中的设备都能接收到发送给其他设备的数据包。在因特网中，一个有决心的黑客可以获得电子邮件流和其他的数据传输。所有这些情况给未经授权访问数据创造了可能性。
- **推断**：推断的一个例子是流量分析。在流量分析中，敌方通过观察网络上的流量模式来获得信息，例如网络中特定两台主机之间的通信量。另一个例子是具有有限访问权

限的用户从数据库中推断出详细信息，这是通过反复查询来完成的，查询的组合结果能够进行推断。

表 18-1 威胁后果及造成每个威胁后果的威胁行为类别（基于 RFC 2828）

威胁后果	威胁行为（攻击）
未经授权的泄露 未经授权的实体获得数据访问权限的情况或者事件	**暴露**：敏感信息直接公布给未经授权的实体 **窃听**：未经授权的实体直接访问授权的源和目的之间的敏感数据流 **推断**：未经授权的实体通过特征推理或者通信的副产品直接访问敏感数据（但是该数据不一定包含在通信中）的威胁行动 **入侵**：未经授权的实体绕过系统的安全保护措施而获得敏感数据的访问权限
欺骗 可能导致一个授权实体收到虚假信息并认为该信息是真实的情况或事件	**伪装**：未经授权的实体获得系统的访问权限或者冒充授权实体实施恶意行为 **篡改**：用虚假数据欺骗一个授权实体 **抵赖**：一个实体通过故意地拒绝对一个行为的责任来欺骗另一个实体
中断 中断或阻止系统服务和功能的正确操作的情况或事件	**失效**：通过使系统控件失效来阻止或者中断系统操作 **毁坏**：恶意修改系统功能或者数据，非预期地改变系统操作 **干扰**：通过阻止系统操作来中断系统提供服务的一种威胁行为
篡夺 导致未经授权的实体控制系统的服务或功能的情况或事件	**滥用**：一个实体取得对系统资源未经授权的逻辑或物理控制 **误用**：使系统控件执行对系统安全不利的功能或者服务

- **入侵**：入侵的一个例子是，攻击者通过克服系统的访问控制保护，获得对敏感数据的未经授权的访问。

欺骗对系统的完整性或者数据的完整性都是威胁。以下类型的攻击能够导致这类威胁结果：

- **伪装**：伪装的一个例子是，一个未经授权的实体企图通过冒充授权实体，从而获得系统的访问权限。当未经授权的用户获得了另一个用户的登录名和密码时，这种情况将有可能发生。另一个例子是恶意代码，例如木马，它看起来似乎执行有用或期望的功能，但实际上获得系统资源的未经授权访问权限或诱骗用户执行其他恶意代码。
- **篡改**：指的是修改或者更换有效数据或者将虚假数据输入文件或者数据库中。例如，学生可能修改存储在学校数据库中的分数。
- **抵赖**：在这种情况下，用户否认发送过数据或者否认接收或拥有数据。

中断是对可用性或者系统完整性的一种威胁。以下类型的攻击将会导致这类威胁结果：

- **失效**：这是对系统可用性的一种攻击。这种攻击可以是由物理破坏或者系统硬件损坏造成的。典型地，恶意软件，如木马、病毒、蠕虫，可以通过这种方式使系统或者系统的某些服务失效。
- **毁坏**：这是对系统完整性的一种攻击。这种情况下，恶意软件可以让系统资源或者服务按照非预期的方式工作。或者用户可以获得未经授权的系统访问权限，并改变系统的一些功能。后者的一个例子是，用户在系统中安置了后门，提供对系统以及系统资源的后续访问权限，而不是通过普通的过程来获得。
- **干扰**：干扰系统操作的一种方式是，通过使通信链路失效或者改变通信控制信息来干扰通信。另一种方式是通过在通信流量或者处理资源上添加多余的负载，使系统过载。

篡夺是对系统完整性的一种威胁。以下类型的攻击将会导致这类威胁结果：

- **滥用**：这种类型包括服务的偷窃。一个例子是分布式拒绝服务攻击，大量主机上被安装了恶意软件，并且这些主机被用来作为向目标主机发送流量的平台。这种情况下，恶意软件未经授权使用处理器和操作系统资源。
- **误用**：误用可由恶意逻辑或者获得了未经授权的系统访问权限的黑客造成。任何一种情况下，安全功能将会失效或者被阻止。

18.2.2　威胁和资产

计算机系统资产可以归类为硬件、软件、数据、通信线路和网络。在本节中，我们简要介绍这 4 类资产，并将它们与 18.1 节中介绍的完整性、保密性、可用性这几个概念联系起来（见图 18-2 和表 18-2）。

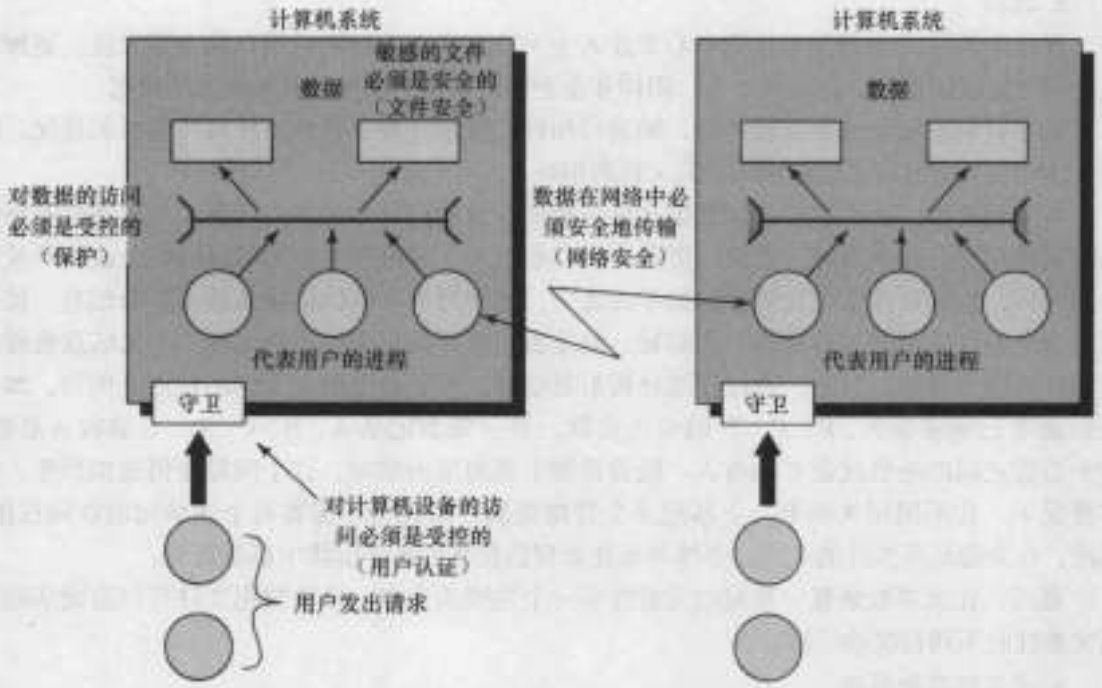


图 18-2　系统安全的范围

表 18-2 计算机和网络资产的威胁举例

	可 用 性	保 密 性	完 整 性
硬件	设备被偷或者失效，由此导致拒绝服务		
软件	程序被删除，拒绝用户的访问	制造一个非法的软件副本	运行中的程序被修改，造成程序执行过程中失败或者完成一些非预期的任务
数据	文件被删除，拒绝用户的访问	非法读取数据。对统计数据的分析揭示底层数据	现有文件被修改或者伪造新的文件
通信线路	消息被破坏或者被删除。通信线路或网络不可用	读取消息。观测消息的流量模式	消息被修改、延迟、记录或者复制。制造虚假消息

1. 硬件

对计算机系统硬件一种主要的威胁是对可用性的威胁。硬件是最容易受到攻击并且最容

易被自动控制的。威胁包括无意和故意的损坏设备以及失窃。个人计算机、工作站的增加以及局域网的广泛使用增加了硬件方面损失的可能性。CD-ROM 和 DVD 的失窃将导致保密性的损失，需要采取物理和管理安全措施来应对这些威胁。

2. 软件

软件包括操作系统、实用工具和应用程序。对软件的一个主要威胁是对可用性的攻击。软件，特别是应用软件，往往容易被删除。软件也可以被修改或者被破坏以至于失效。精心的软件配置管理，包括对最新版本的软件进行备份，可以保持较高的可用性。一个要解决的更为棘手的问题是软件的修改，它导致该程序仍然在运行但是它的行为和之前有所不同，这是对完整性/真实性的一种威胁。计算机病毒和相关的攻击属于这个方面。最后一个问题是防范软件盗版，虽然可以使用某些对策，但是软件的非授权复制问题一直没有得到解决。

3. 数据

硬件和软件安全通常是计算中心专业人士关注或者个人计算机用户的个别关注。更加广泛的问题是数据安全，它涉及个人、团体和企业组织控制的文件和其他形式的数据。

对于数据的安全关注比较广泛，涵盖可用性、保密性和完整性。针对可用性的情况，我们关注的是无意或者恶意造成的数据文件的损坏。

对于保密性，未经授权读取数据文件或数据库是我们非常关注的问题。与计算机安全的其他领域相比，这个领域一直获得更多的研究和投入。对保密性不太明显的安全威胁涉及数据的分析，它的具体表现为统计数据库的使用，这种行为可以提供摘要或者汇总信息。就算汇总信息的存在可能不会威胁个人隐私，但是由于统计数据库使用的增长，个人信息泄露的可能性也随之增加。其实，通过仔细分析汇总信息，可以确定组成个体的特点。例如，如果一张表里记录被告 A、B、C、D 的收入总数，另一张表记录 A、B、C、D、E 的收入总数，两个总数之间的差值就是 E 的收入。随着数据汇集愿望的增加，这个问题变得更加严重。很多情况下，在不同层次的聚合上匹配多个数据集的一致性工作需要对个体单元的访问权限。因此，作为隐私所关注的主题，个体单元在处理数据集的各个阶段中都能获得。

最后，在大多数装置中数据的完整性是一个主要关注点。修改数据文件可以造成从轻微到灾难性的不同程度的后果。

4. 通信线路和网络

网络安全攻击可分为被动攻击和主动攻击。被动攻击企图获得或者使用来自系统的信息，但是不影响系统资源。主动攻击企图改变系统资源或者影响它们的相关操作。

被动攻击类似于信息传输的窃听或者监控，攻击者的目的是获得传输的信息。消息内容的发布和流量分析就是两种被动攻击。

消息内容的发布很容易理解。电话交谈、电子邮件以及传输的文件可能包含敏感或者机密的信息，我们要阻止攻击者获得这些传输的内容。

第二种被动攻击方式，**流量分析**，是比较微妙的。假设有一种方法可以隐藏消息的内容或者其他信息流，那么即使攻击者获取了消息，他们也无法从消息中提取信息。常见的内容隐藏技术是加密。如果我们在内容部分进行加密保护，攻击者可能仍然能够观察到这些消息的模式，能够判断通信主机的位置和身份，能够观察到交互频率和交换信息的长度，这些信息对于猜测正在发生的通信的性质是有帮助的。

被动攻击很难被检测到，因为它们不涉及任何信息的改变。通常，信息流按照非常正常的方式发送和接收，不管是发送者还是接收者都不会知道第三方正在读取消息或者观察流量

模式。然而，阻止这种攻击却是可行的，通常用加密的方式。因此，应对被动攻击的重点是防范而不是检测。

主动攻击涉及对数据流的改动或者制造虚假的数据流，它可以分为4类：重放、冒充、修改消息和拒绝服务。

重放涉及被动捕获数据单元然后进行重发，以产生未经授权的效果。

当一个实体假装是另一个不同的实体时，**冒充**就发生了。一次冒充攻击通常包含另一种其他形式的主动攻击。例如，认证序列可以被捕获并在一次合法认证序列发生之后被重放，因此仅有少量特权的授权实体可以通过冒充其他拥有更多特权的实体，而获得额外的特权。

修改消息仅仅意味着一条合法消息的某些部分被修改了，或者消息被延迟或重新排序以达到未授权的效果。例如，一条消息申明“允许 John Smith 读取机密文件 accounts”被修改成“允许 Fred Brown 读取机密文件 accounts”。

拒绝服务阻止或妨碍通信设备的正常使用或管理。这种攻击有一个特殊的目标，例如，一个实体可以强制使所有消息到达一个特定的目标（例如，安全审计服务）。另一种拒绝服务的方式是整个网络中断，这通过使网络失效来实现或者用大量消息使网络过载而降低其性能。

主动攻击体现出与被动攻击相反的特性。一方面，被动攻击难以检测，但是却存在措施可以阻止它。另一方面，完全阻止主动攻击是相当困难的，因为这需要一直对所有的通信设备和路径实施物理保护。另外，对主动攻击的防御目标是检测它们并恢复它们所造成的中断或延迟。因为检测可以达到威慑的效果，所以有助于防御的实现。

18.3　入侵者

入侵者是最广为人知的两个安全威胁之一（另一个是病毒），它通常指的是黑客或者破坏者。在对入侵的一个早期重要研究中，Anderson[ANDE80] 定义了入侵者的 3 种类型：

- **伪装者**：没有权限使用计算机的个体，通过渗透系统的访问控制，利用合法用户的账户。
- **滥用权限者**：未经授权地访问数据、程序或资源的合法用户或者经过授权获得访问权限但是误用特权的用户。
- **秘密客**：篡夺系统管理员控制权限的人，利用这个控制能力来逃避审计和访问控制或阻止审计的进行。

伪装者可能是外部人员，滥用权限者一般是内部人员，秘密客可能是外部人员也可能是内部人员。

入侵攻击造成的危害从轻微到严重都有可能。轻微时，很多人仅仅希望探索互联网，看看外边是什么。严重时，有些个体试图读取秘密信息，对数据进行非法篡改或者扰乱系统。

以下是入侵的例子：

- 执行电子邮件服务器的远程 root 登录权限攻击。
- 破坏 Web 服务器。
- 猜测、破译密码。
- 复制一个存有信用卡号的数据库。
- 未经授权浏览敏感信息，包括工资记录和医疗信息。
- 在一个工作站上运行数据包嗅探器抓取账号和密码。
- 利用匿名 FTP 服务器上的权限漏洞，散布盗版软件和音乐文件。

- 拨号接入一个不安全的调制解调器，获取访问内网的权限。
- 冒充经理发送邮件，呼叫帮助台，重置经理的电子邮件密码，从而获得新的密码。
- 未经允许使用无人值守已登录的工作站。

18.3.1　入侵者的行为模式

入侵者的行为模式和使用的技术处于不断变化中，这不仅是为了利用新发现的漏洞，也是为了逃避检测和防护策略。即使这样，入侵者也往往遵循一些可识别的行为模式，这些行为模式通常有别于正常用户。接下来，我们来看看入侵者行为模式的 3 个例子，以便读者能够感受安全管理人员所面临的挑战。

表 18-3　入侵者行为模式的例子

a）黑客
1. 利用 IP 查找工具（例如，NSLookup、Dig 或者其他工具）来选择目标主机
2. 利用 NMAP 等工具在网络中寻找可访问的服务
3. 识别可能有漏洞的服务（本例中是 pcAnywhere）
4. 暴力破解（猜测）pcAnywhere 的密码
5. 安装远程管理工具 DameWare
6. 等待管理员登录，获取他的密码
7. 用获取的密码访问其他的网络
b）犯罪企业
1. 行动快速而准确，使得他们的行为难以检测
2. 通过有漏洞的端口渗透边界
3. 利用木马（隐蔽的软件）为下次登录留下后门
4. 利用嗅探器获得密码
5. 不要因滞留而被发现
6. 尽量少犯错或者不犯错误
c）内部威胁
1. 为自己或者朋友创建网络账户
2. 访问他们日常工作中不常用的账户或者应用
3. 为离职的雇员或者即将入职的雇员发送电子邮件
4. 偷偷摸摸进行即时通信聊天
5. 访问理合心怀不满的员工的网站，例如 f*dcompany.com
6. 大规模下载或者复制文件
7. 下班后访问网络

1. 黑客

传统意义上，指那些为了获得震撼或地位而侵入计算机的人。黑客社区有一种强烈的氛围，即黑客在社区的地位由能力水平决定。因此，黑客通常寻找有入侵机会的目标，然后将相关信息与其他黑客分享。一个典型的例子是 [RADC04] 中报道的一次对一家大型金融机构的入侵。入侵者利用了企业网络中运行了未加保护的服务，其中的一些服务甚至是不需要的。在这个案例中，入侵的关键是 pcAnywhere 应用。Symantec（赛门铁克）公司宣传这个程序是一个远程控制解决方案，能够实现安全连接到远程设备。但是黑客很容易就获得了 pcAnywhere 的权限，管理人员使用了 3 个字母长度相同的用户名和密码。这个案例中，在这个 700 个节点的企业网络内没有入侵检测系统。直到副总裁走进她的办公室，发现鼠标在她

的工作站上移动文件，才发现有入侵者。

没有恶意的入侵者也许是可以容忍的，虽然他们确实消耗资源并且降低合法用户的性能。然而，管理员无法提前预知一个入侵者有没有恶意。因此，即使对于没有特别敏感资源的系统，依然有必要对这个问题进行控制。

第 19 章会提到的入侵检测系统（IDS）和入侵防御系统（IPS），主要是用来对抗这种类型的黑客威胁。除了使用这些系统外，相关组织可以考虑限制远程登录到特定的 IP 地址，或者使用虚拟专用网技术。

人们对入侵者问题的认识不断增加，由此相继建立了一批计算机应急响应小组（CERT）。这些合作公司收集系统漏洞的相关信息并把这些信息交给系统管理员。黑客也会经常阅读 CERT 报告。因此，对于系统管理员，快速为发现的漏洞打上软件补丁显得尤为重要。不幸的是，面对众多 IT 系统的复杂度和补丁发布的速度，没有自动更新的帮助来完成这项工作越来越困难。即使有自动更新功能，由软件更新造成的不兼容问题依然存在（因此管理 IT 系统的安全威胁需要多层次的防御）。

2. 犯罪

对于基于因特网的系统，有组织的黑客团体已经成为它们的一种普遍而常见的威胁。这些团体可能被企业或者政府雇佣，但常常松散地隶属于黑客帮。通常情况下，这是一群年轻人，他们往往是来自东欧、俄罗斯、东南亚的在网络上做生意的黑客 [ANTE06]。他们相聚于 DarkMarket.org 和 theftservices.com 等这样的地下论坛，交易技术和数据，协商发起攻击。一种常见的攻击目标是电子商务服务器中的信用卡文件，攻击者企图获得 root 权限。这些信用卡号被有组织的犯罪团伙用来购买贵重物品，之后被发布到盗卡网站，那里其他人能够获得和使用这些账号。这让信用卡的使用模式变得模糊，使调查变得复杂。

传统黑客寻找有攻击机会的目标，而犯罪黑客经常有具体的目标，或者至少在心里面有某几类目标。一旦一个站点被突破，攻击者迅速行动，尽可能多地挖掘出有价值的信息，然后撤退。

IDS 和 IPS 也能够用于这几类攻击者，但是由于这种攻击迅速入侵并撤离的本质，所以可能不那么有效。对于电子商务网站，将数据库加密用于敏感的客户信息，特别是信用卡。对于托管电子商务网站（由外部服务器提供），电子商务组织应该利用专用服务器（不用于支持多用户），并且密切监视供应商的安全服务。

3. 内部攻击

内部攻击属于最难被检测和防御的攻击方式。雇员已经获得了企业数据库的访问权限并了解其架构和公司数据库的内容。内部攻击可能是出于报复或者获利的感觉。关于前者的一个例子是，Kenneth Patterson 担任 American Eagle Outfitters 公司的数据通信经理并被解雇。之后，Patterson 使公司在 2002 年假期中的 5 天丧失处理信用卡消费的能力。至于获利的感觉，经常会有很多员工觉得有权获得额外的办公用品补贴家用，而现在扩展到了公司数据。例如，股票分析公司的销售副总裁辞去职务，去应聘一份新的工作。在她离开之前，她复制并带走了客户数据库。冒犯者觉得对于前雇员并没有恶意，她仅仅希望获得这份数据，因为这份数据可能对她有用。

虽然 IDS 和 IPS 设施可以用于抵御内部攻击，但是可以优先考虑其他更直接的方式。这包括以下措施：

- 行使最小特权，即仅允许雇员访问他们工作所需的资源。
- 设置日志，用于查看用户访问的内容和输入的命令。

- 用强认证方式保护敏感资源。
- 解雇后，删除用户访问计算机和网络的权限。
- 解雇后，在重新把硬盘分配给雇员之前对其制造一个镜像。如果公司信息在竞争对手那里出现，可能需要这些证据。

18.3.2　入侵技术

入侵者的目的是获得访问系统的权限或者增加访问系统的权限范围。最初始的攻击利用系统或者软件漏洞，使用户可以执行在系统中设置后门的代码。入侵者可以利用以某特定权限运行的程序的缓冲区溢出漏洞，发起攻击来获得系统访问权限。

另外，入侵者试图获得应该被保护的信息。在某些情况下，这个信息是用户密码。知道了其他用户密码的情况下，入侵者可以登录系统并行使与合法用户一样的特权。

18.4　恶意软件概述

也许对计算机系统而言，这是最高级的威胁类型，它是利用计算机系统漏洞的程序，这些威胁称为**恶意软件**（malicious software 或 malware）。在本节中，我们所关心的是应用软件和实用软件，例如编辑器和编译器。设计恶意软件主要是用来对目标计算机制造损害或者耗尽目标计算机资源，它经常隐藏在正常软件内或者伪装成正常软件。在某些情况下，它通过电子邮件或者感染光盘将自己传播到其他计算机。

本节的术语会造成一些困扰，因为这些术语未广泛地达成一致。表 18-4 是一个有用的指南。

表 18-4　恶意软件术语

名　字	说　明
病毒	运行时试图将自己复制到其他可执行代码中的恶意软件。复制成功后，我们称代码被感染了。当被感染的代码执行时，病毒也会执行
蠕虫	能够独立运行并将自身的一个完整工作版本传播到网络中其他主机的一种计算机程序
逻辑炸弹	入侵者插入软件中的一段程序。逻辑炸弹一直处于潜伏状态，直到满足预先设定的某种条件之后，程序将会触发未经授权的行为
木马	一个似乎具备有用功能的计算机程序，但是也有逃避安全机制的隐蔽的、潜在的恶意功能，这里安全机制的躲避有时利用激活木马程序的系统实体的合法授权
后门（陷门）	任何能够绕过正常安全检查的机制，它允许未经授权而使用相关功能
移动代码	对于不同的平台，能够不用修改而以相同的语法运行的软件（例如，脚本、宏或者其他可移植的指令）
漏洞利用	针对一种漏洞或者一类漏洞的代码
下载器	在被攻击的机器上安装其他事项的软件。通常，下载器通过电子邮件发送
自动登录器	用来远程入侵一台新机器的恶意黑客工具
工具箱（病毒制造器）	自动生成新病毒的一套工具
垃圾邮件程序	用来发送大量不受欢迎的电子邮件
洪水	使用大量流量攻击网络上的计算机系统，进而导致拒绝服务攻击
键盘记录器	在被入侵的系统上捕获键盘输入信息
Rootkit	攻击者入侵到计算机系统、获得 root 级别的访问权限后使用的工具集合
僵尸程序（Zombie、bot）	在被感染机器上激活的程序，用来针对其他机器发动攻击
间谍软件	从计算机上收集信息并发送到其他系统的软件
广告软件	整合到软件中的广告，可以导致弹出式的广告或者将浏览器重定向到一个商业网站

恶意软件可以分为两类：需要宿主程序的恶意软件和独立的恶意软件。前者称为**寄生**，其本质是一种不能独立于实际应用程序、实用程序或者系统程序的程序片段，这类恶意软件的例子包括病毒、逻辑炸弹和后门。后者是自我包含的程序，可以由操作系统调度和运行，这类恶意软件的例子包括蠕虫和僵尸程序。

我们也可以将恶意软件区分为不能复制的和可以复制的。前者是由触发器激活的程序或程序片段，例如逻辑炸弹、后门和僵尸程序。后者要么含有一个程序片段，要么是独立的程序，执行后可以产生一个或者多个自身的副本，随后在同一个系统或者其他系统中被激活，这样的例子包括病毒和蠕虫。

在本节的剩余部分中，我们简要讨论一些主要的恶意软件，对病毒、蠕虫和僵尸程序的主要话题将放到下一节讨论。

18.4.1　后门

后门，也称为**陷门**，是一个程序的秘密入口点，它允许那些知道该后门存在的人不需要通过通常的安全访问过程而获得权限。多年来，程序员已经合理地使用后门来调试和测试程序，这样的后门称为**维护钩子**。这种方式通常用于程序员在开发一个需要认证过程的应用程序时，或者这个程序漫长的安装过程中需要输入很多不同的值来运行这个应用程序。为了调试这样的程序，开发人员希望获得特殊的权限或者绕过所有必需的安装和认证。如果潜入应用的认证过程出现错误，程序员可能还需要确认存在一种可以激活程序的方法。后门是一种可以识别一些特殊输入序列的代码，可以被一个特定的用户账号或不太可能发生的事件序列触发。

当不怀好意的程序员利用后门获得未经授权的访问权限时，后门就变成了威胁。后门是电影《War Games》中所描绘漏洞的基本思想。另一个例子是在 Multics 的发展过程中，由一只名为“飞虎队”（模拟对手）的空军来进行渗透测试。他们采用的一种策略是发送一个假的操作系统更新到运行 Multics 的网站，这个更新里有一个可以被后门激活从而允许飞虎队获得权限的木马（稍后描述）。这个威胁实施得如此之好，以至于哪怕被告知了这个漏洞的存在，Multics 的开发者都没能够发现它。

对于后门防御，实施操作系统的控制难以实现，安全措施必须集中在程序开发和软件升级上。

18.4.2　逻辑炸弹

逻辑炸弹是最早的几种程序威胁之一，它早于病毒和蠕虫。逻辑炸弹是嵌入在一些正常程序中的代码，当满足某些特定条件时它将会“引爆”。例如，作为逻辑炸弹触发器的条件可以是某些文件的出现或者消失，一个星期的某一天或者某个日期，或者特定的用户运行应用程序。一旦被触发，逻辑炸弹可能会修改、删除数据或整个文件，导致死机或者造成其他的危害。一个典型的如何使用逻辑炸弹的例子是 Tim Lloyd 案例，他被告设置了一个逻辑炸弹，使他的雇主 Omega Engineering 公司损失了 1000 万美元，同时使得该公司的发展战略发生偏移，最后导致 80 名工人下岗，他也因此而被定罪 [GAUD00]。最后，Lloyd 被判处了 41 个月的监禁，并被责令支付 200 万美元作为补偿。

18.4.3　木马

木马是一个有用的，或者说再有用不过的包含隐藏代码的程序或命令序列，当它被调用

时，它会执行一些无用的或者有害的功能。

木马程序可以用于间接地实现未经授权的用户无法直接完成的功能。例如，为了获得共享系统中其他用户文件的访问权限，用户可以编写一个木马程序，当执行它时，改变相关用户的文件权限，这个文件就可以被任意用户读取。之后编写者通过将木马放在公共目录下，并把它命名得像一个有用的工具程序或者应用程序，诱使用户执行它。例如，某个程序从表面上看是按某一格式产生用户文件列表，当另一个用户运行这个程序后，程序的编写者就能够访问该用户文件中的信息。一个难以检测的木马程序的例子是，一个编译器被修改成在某些程序被编译时（例如系统登录程序）往里面插入额外的代码。这些代码在登录程序里设置一个后门，允许编写者用特殊的密码登录系统中。这种木马永远无法通过查看登录程序的源代码来发现。

木马另一种常见的动机是破坏数据。一个程序看起来执行一个有用的功能（例如，一个计算器程序），但是它也可能正在暗地里删除用户文件。例如，CBS 执行总裁的计算机被木马侵害后，他计算机内存中的所有信息都被破坏了【TIME90】。过去，木马被植入在电子布告栏系统提供的图形程序中。

木马符合以下 3 种模型中的一种：

- 继续执行原程序的功能，同时额外执行一个分开的恶意行为。
- 继续执行原程序的功能，但是修改其功能进行恶意行为（例如，用于收集口令的登陆程序的木马版）或者掩盖其他恶意活动（例如，不展示某些恶意进程的进程列表程序的木马版）。
- 执行完全取代原程序功能的恶意功能。

18.4.4　移动代码

移动代码指的是在不同平台之间可以不用修改而以相同语义执行的程序（例如，脚本、宏、可移植指令）。这个术语也适用于大型同类平台（例如，Microsoft Windows）的情况。

移动代码从一个远程系统上传播到一个本地系统，然后不需要用户明确的指令就可以在本地系统上执行。移动代码经常作为病毒、蠕虫或者木马的一种机制，使它们可以传递到用户的工作站。在其他情况下，移动代码利用漏洞来执行自己的攻击，例如未经授权的数据访问或者获得 root 权限。流行的移动代码载体包括 Java 小程序、ActiveX、JavaScript 和 VBScript。使用移动代码在本地系统上进行恶意操作最常用的方式是跨站点脚本、交互式动态网站、电子邮件附件，以及从不受信任的网站下载或者下载不受信任的软件。

18.4.5　多重威胁的恶意软件

病毒和其他恶意软件能够以多种方式活动。由于相关术语很不一致，所以本节对几个与多重威胁的恶意软件有关的概念做简要介绍。

多态病毒通过多种方式感染。通常，多态病毒可感染多种类型的文件，因此消灭这种病毒必须处理所有可能的感染方式。

混合攻击利用多种感染或者传播方法，以最大化感染的速度和攻击的严重程度。有些作者将混合攻击定性为包含多种类型恶意软件的包。混合攻击的一个例子是 Nimda 病毒攻击，它曾被错误地认为是一种简单的蠕虫。Nimda 使用了 4 种传播方法：

- **电子邮件**：用户在有漏洞的主机上打开了受感染的电子邮件附件，Nimda 搜索这台主

机上的电子邮件地址，然后将自己的副本发送到这些地址。

- **Windows 共享**：Nimda 扫描主机寻找不安全的 Windows 文件共享，之后它能够利用 NetBIOS86 作为传输机制感染这台主机上的文件，以期待一个用户会运行被感染的文件，这样将会激活主机上的 Nimda。
- **Web 服务器**：Nimda 扫描 Web 服务器，寻找 Microsoft IIS 的已知漏洞。如果发现了一个有漏洞的服务器，它会试图传送自己的一个副本到服务器上，感染服务器以及服务器上的文件。
- **Web 客户机**：如果有漏洞的 Web 客户机访问一个被 Nimda 感染的 Web 服务器，那么客户机所在的工作站将会被感染

因此，Nimda 具有蠕虫、病毒和移动代码的特点。混合攻击也可以通过其他服务传播，比如即时通信和端到端（P2P）文件共享。

18.5　病毒、蠕虫、僵尸程序和垃圾邮件

18.5.1　病毒

计算机病毒是一种软件，它通过修改其他程序来感染它们。这些修改行为包括把复制病毒程序的例程注入原程序中，之后通过这种途径继续感染其他的程序。

生物病毒是微小的遗传代码序列（DNA 或者 RNA）碎片，它可以接管活细胞的机能并诱骗它产生成千上万的一模一样的原病毒副本。就像生物学中对应的功能，计算机病毒在引导代码中携带了用于制作完美自身副本的配方。典型的病毒嵌入在计算机程序中，只要当被感染的计算机接触到一个未被感染的软件，一个新产生的病毒副本就传递到这个程序中。因此，感染可以利用没有防备的用户交换磁盘或者把程序发送给网络中另一人，从一台计算机传播到另一台计算机。在网络环境中，访问其他计算机的应用程序或者系统服务的能力，为病毒的传播提供了很好的环境。

1. 病毒的本质

病毒可以做其他程序可以做的任何事情，唯一的不同点在于病毒将自己附在其他程序上，在宿主程序运行时偷偷执行。一旦病毒被执行，它可以执行当前用户权限允许的所有功能，例如删除文件和程序。

计算机病毒包含 3 部分：

- **感染机制**：病毒传播的方式，使其能够自我复制。这种机制也称为**感染向量**（infection vector）。
- **触发器**：决定病毒什么时候激活或者传播的事件或条件。
- **负载**：除了传播之外，病毒所做的事情。负载可能涉及破坏活动或者无害却引人注目的活动。

在病毒的生命周期中，一个典型的病毒经历如下 4 个阶段。

- **潜伏阶段**：病毒是闲置的。病毒最终会被某些事件激活，例如日期、另一个程序或文件的出现或者磁盘的容量超过某一限度。不是所有的病毒都有这个阶段。
- **传播阶段**：病毒将其自身的副本放到磁盘上的其他程序中，或者放到特定的系统区域中。每个被感染的程序将携带病毒的副本，这些副本能够自己进入传播阶段。
- **触发阶段**：病毒被激活，执行预定的功能。与休眠阶段一样，触发阶段可以由各种各

样的系统事件引发，这些事件包括病毒制造副本的统计次数。

- **执行阶段**：执行功能。这些功能可能是无害的，例如在屏幕上显示一条消息；也可以是有害的，例如破坏程序和数据文件。

大多数病毒根据某种方式进行工作，这种方式针对一个特定的操作系统，在一些情况下针对一个特定的硬件平台。因此，病毒为利用特定系统的某个细节或者漏洞而设计。

2. 病毒结构

病毒可以前置或后置到可执行程序，或者以其他的方式内嵌在可执行程序中。其运作的关键在于，当感染的程序被调用时，先执行病毒代码然后再执行程序的原代码。

病毒结构的一般性描述如图 18-3 所示（基于 [COHE94]）。在这种情况下，病毒代码 V 前置在被感染的程序上，假设被调用时程序的入口点在程序的第一行。

```
    program V :=
{goto main;
    1234567;

    subroutine infect-executable :=
      {loop:
      file := get-random-executable-file;
      if (first-line-of-file = 1234567)
         then goto loop
         else prepend V to file; }

    subroutine do-damage :=
      {whatever damage is to be done}

    subroutine trigger-pulled :=
      {return true if some condition holds}

main: main-program :=
      {infect-executable;
      if trigger-pulled then do-damage;
      goto next;}

next:

}
```

图 18-3　简单病毒

被感染的程序从病毒代码开始执行，工作原理如下。代码的第一行跳转到病毒的主程序。第二行是一个特殊的标记，病毒利用其判断可被感染的程序是否已经被病毒感染了。当程序被调用时，控制权立即转交给病毒的主程序。病毒程序首先寻找没有被感染的可执行程序，并使其感染。然后，病毒执行一些通常对系统有害的动作。以上过程可以在每次程序被调用时执行，也可以是在特定条件下才会被触发的逻辑炸弹。最后，病毒将控制权交给原程序。如果程序的感染阶段足够迅速，用户不太可能察觉到执行被感染的程序和执行未被感染的程序有什么不同。

刚刚所描述的病毒比较容易被检测到，因为被感染版本的程序比与之对应的未被感染版本的更长。一种干预这种简单检测病毒方法的途径是压缩可执行文件，这样被感染的版本和未被感染的版本长度就会一样。图 18-4 以通用的术语展示了需要的逻辑。病毒中重要的地方用数字标明。我们假设程序 P_1 被病毒 CV 感染了，当这个程序被调用时，控制权转交给病毒，病毒执行如下步骤：

1）对于每个发现的未被感染的文件 P_2，病毒首先将此文件压缩为 P'_2，压缩后的文件比原程序短，病毒缩小了原程序的长度。

2）病毒的副本被前置到压缩程序中。

3）将已被压缩的原感染程序 P'_1 解压缩。

4）执行解压缩后的原程序。

在这个例子中，病毒仅仅是传播，其他什么事情都没做。正如之前所提到的，病毒可能包含一个逻辑炸弹。

3. 初始感染

一旦病毒通过感染单个程序进入系统，执行被感染的程序时，病毒将处于可能感染系统

中某些或者所有其他可执行文件的状态。因此，首先通过阻止病毒进入系统可以完全阻止病毒感染。不幸的是，阻止显得非常困难，因为病毒可以是系统外任何程序的一部分。因此，除非编写自己的系统和应用程序，并且除了这两者以外其他东西都不使用了，否则系统就是易受攻击的。许多类型的感染可以通过拒绝正常用户修改系统中程序的权限来阻止。

```
    program CV :=

{goto main;
    01234567;

    subroutine infect-executable :=
        {loop:
            file := get-random-executable-file;
        if (first-line-of-file = 01234567) then goto loop;
      (1)   compress file;
      (2)   prepend CV to file;
      }

main: main-program :=
            {if ask-permission then infect-executable;
      (3)   uncompress rest-of-file;
      (4)   run uncompressed file;}
      }
```

图 18-4　压缩病毒的逻辑

传统的基于机器码的病毒在早期个人计算机的系统中迅速传播，其关键原因在于这些计算机缺乏访问控制。相比之下，虽然写一个针对 UNIX 系统的机器代码病毒非常简单，但是在实际中几乎看不到，因为这些系统中存在的访问控制有效阻止了病毒的传播。传统的基于机器码的病毒现在很少流行，因为现代个人计算机的操作系统具备更有效的访问控制。然而，病毒制造者发现了其他方式，例如宏病毒和电子邮件病毒，这些将在随后讨论。

4. 病毒分类

自从病毒第一次出现开始，病毒编写者和防病毒软件编写者之间一直在进行斗争。当针对已知病毒类型的有效对策出现时，新类型的病毒也会出现。本缩后的文件比原文件短了大小 ceries::Food:Food 对于病毒的分类策略，不存在简单或达成一致的分类方案。在本节，我们沿着两个正交轴对病毒进行分类：病毒尝试感染的目标类型以及病毒用以隐藏自己防止用户或杀毒软件检测到的策略。

根据**感染目标**的不同，病毒分为以下类型：

- **引导扇区感染**：感染主引导记录或者引导记录，当系统从携带病毒的磁盘启动时传播。
- **文件感染**：感染操作系统或者 shell 认为可执行的文件。
- **宏感染**：感染含有宏代码的文件，这里宏代码由某个应用程序进行解析。

根据隐藏策略的不同，病毒可分为如下类型：

- **加密病毒**：典型的方式为，病毒的一部分产生随机加密密钥，然后加密病毒的剩余部分，密钥存储在病毒中。当一个被感染的程序被调用时，病毒用存储的随机密钥对病毒解密。当病毒复制时，将选择一个不同的随机密钥。由于对于每个病毒，其主体都用不同的密钥加密，所以没有固定的位模式来观察。
- **隐形病毒**：病毒的一种形式，明显地设计为隐藏自己，躲避防毒软件的检测。因此，

不仅仅是负载部分，整个病毒都被隐藏起来。

- **多态病毒**：每次感染时都会发生变异的病毒，这使得通过“签名”来检测病毒不可行。
- **变形病毒**：与多态病毒一样，变形病毒每次感染时都会发生变异。不同之处在于，每次传染时变形病毒都会完全地重写自身，增加检测的难度。变形病毒可以改变它们的行为以及外形。

隐形病毒的一个例子在前面讨论过：病毒使用压缩的方法，使被感染的程序与未被感染的版本长度完全一样。隐形病毒可能使用更复杂的技术，例如病毒可以在磁盘的 I/O 例程中放置拦截逻辑，当该例程被调用而试图读取磁盘的相关区域时，病毒将会感染未被感染的原程序。因此，隐形并不仅仅是适用于这类病毒的一个术语，而是指病毒用以逃避检测的一种技术。

多态病毒复制时制造自己的副本，这些副本功能上是相同的，但是有不同的位模式。与隐形病毒一样，其目的在于挫败检测病毒的程序。在这种情况下，病毒的“签名”随着每个副本的不同而不同。为了实现这种变异，病毒可能随机地插入多余的指令或者交换独立指令的顺序。一种更有效的途径是利用加密。加密病毒的策略如下：负责产生密钥以及进行加密与解密的病毒部分称为变异引擎。每次使用时变异引擎都会发生改变。

5. 病毒工具箱

病毒编写者武器库中的另外一件武器是病毒制造工具箱。这种工具箱能够使初学者可以快速制造大量不同的病毒。虽然通过工具箱制造出来的病毒往往没有从头开始设计的病毒那么复杂，但是利用工具箱生产出来的新病毒的数量很多，对防病毒策略带来了麻烦。

6. 宏病毒

在 20 世纪 90 年代中期，宏病毒成为当时最流行的病毒类型。宏病毒因为某些原因显得特别危险：

1）宏病毒不依赖平台。很多宏病毒感染 Microsoft Word 文档或者其他 Microsoft Office 文档。任何支持这些应用的硬件平台或者操作系统都可以被感染。

2）宏病毒感染文档，而不是代码的可执行部分。传送到计算机系统中的大多数信息是文档的形式而不是程序。

3）宏病毒很容易传播。很常见的一种方法是通过电子邮件。

4）因为宏病毒感染用户文档而不是系统程序，所以传统文件系统的访问控制在阻止病毒传播方面作用有限。

宏病毒利用在 Word 或者其他 office 应用，例如 Microsoft Excel 中发现的一个特性，这个特性就是宏。本质上，宏是嵌入在文字处理文档或者其他类型文件中的可执行程序。通常，用户利用宏使重复性的工作自动进行而减少键盘输入。宏语言的形式一般体现为 BASIC 编程语言，用户可以在宏里定义一系列键盘输入并进行设置，当功能键或者特殊的短组合键输入时，宏将被调用。

后续版本的 MS Office 产品针对宏病毒提供了更好的保护。例如，Microsoft 提供了一个可选的宏病毒保护工具，检测可疑的 Word 文件并警告用户打开宏文件的潜在风险。各种防病毒产品供应商也开发工具来检测和更正宏病毒。与其他种类的病毒一样，宏病毒领域中的斗争一直在继续，但它们不再是最主要的病毒威胁。

7. 电子邮件病毒

恶意软件中一个较新的发展是电子邮件病毒。第一代快速传播的电子邮件病毒，比如梅

丽莎（Melissa），利用嵌入电子邮件附件中的 Microsoft Word 宏。如果接收者打开电子邮件中的附件，Word 宏就被激活。之后病毒执行以下两个功能：

1）电子邮件病毒将自身发送到用户电子邮件包中邮件列表上的每个人。

2）病毒在用户的本地系统上制造破坏。

1999 年，一种更具威力的电子邮件病毒出现了。这种更新的病毒仅仅通过打开含有病毒的电子邮件就被激活，而不需要打开附件。这种病毒利用电子邮件包所支持的 Visual Basic 脚本语言。

于是，我们看到了新一代的恶意软件，它们通过电子邮件传播，利用电子邮件软件特性在因特网上复制自己。一旦被激活（无论是通过打开电子邮件附件还是打开电子邮件），病毒向被感染主机上已知的所有电子邮件地址传播自己。因此，病毒过去经常利用几个月或者几年的时间传播，而现在它们在几小时之内就能完成。这使得防病毒软件在严重损失出现前进行响应变得非常困难。最终，我们需要在因特网设施以及个人计算机的应用软件上建立更深度的安全机制来应对不断增长的威胁。

18.5.2　蠕虫

蠕虫是可以复制自己并通过网络连接从一台计算机向另一台计算机发送自己副本的程序。到达新的计算机后，蠕虫再次被激活复制和传播。除了传播外，蠕虫通常执行一些用户不需要的功能。电子邮件病毒具备蠕虫的一些特性，因为它从一个系统向另一个系统传播自己。然而，我们依旧将其归类为病毒，因为它利用修改过的文档携带病毒的宏内容，并且在传播过程中需要人为的动作。蠕虫主动搜索更多的机器去感染，而且每台被感染的机器充当攻击其他机器的自动化跳板。

网络蠕虫程序利用网络连接，从一个系统传播到另一个系统。一旦在一个系统中活动起来，网络蠕虫表现为计算机病毒或细菌，或者它可以植入木马程序或执行大量的扰乱或破坏性的行为。

为了复制自己，网络蠕虫利用某种网络媒体。下面给出了几个例子：

- **电子邮件设施**：蠕虫将自己的一个副本复制到其他系统，因此当电子邮件或附件被接收或查看时，将执行蠕虫代码。
- **远程执行能力**：蠕虫通过利用一个明显的远程执行设施，或者利用网络服务中的程序缺陷，执行存储在其他系统上自己的副本来破坏系统的正常运行。
- **远程登录能力**：蠕虫作为一个用户登录到远程系统，然后利用命令把自身从一个系统复制到另一个系统，然后在远程系统上执行。

然后，蠕虫程序的新副本在远程系统上运行，除了在这个系统中执行功能之外，它还继续以相同的方式传播。

网络蠕虫表现出与计算机病毒相同的特征，主要有：潜伏阶段、传播阶段、触发阶段和执行阶段。通常，蠕虫在传播阶段执行如下功能：

1）通过检查主机列表或者相似的远程系统地址资源，寻找其他要感染的系统。

2）与远程系统建立连接。

3）将自身复制到远程系统并使副本运行。

在把自己复制到远程系统之前，网络蠕虫也试图判断系统是否在之前已经被感染过。在多道程序（multiprogramming）系统中，蠕虫还通过将自己命名为系统进程或者使用其他不会

被系统操作员注意的名字来掩饰它的存在。

和病毒一样，网络蠕虫难以防治。

目前蠕虫使用的技术包括以下几种：

- **多平台**：新的蠕虫不仅限于 Windows 机器，也可以攻击多种平台，特别是流行的 UNIX 版本。
- **利用多种漏洞**：新型蠕虫利用 Web 服务器、浏览器、电子邮件、共享文件和其他基于网络的应用漏洞，通过各种途径侵入系统。
- **极快的传播**：加快蠕虫传播的一种技术是事先进行网络扫描，获得有漏洞机器的网络地址。
- **多态**：为了躲避检测、绕过过滤器、挫败实时分析，蠕虫采用了病毒的多态技术。利用功能上相同的指令和加密技术，蠕虫的每个副本都具有在传播时产生的新代码。
- **变异**：除了改变它们的外形外，变异蠕虫在传播的不同阶段展现出所有可能的行为模式。
- **运输工具**：由于蠕虫可以迅速地感染大量的系统，所以它们适用于传播其他分布式攻击工具，例如分布式拒绝服务攻击的僵尸程序。
- **零日漏洞**：为了使效果震撼和传播效果最大化，蠕虫利用一个不为人知的漏洞，这个漏洞在蠕虫感染时才被普通的网络社区发现。

18.5.3　僵尸程序

僵尸程序，也称为僵尸（zombie）或者无人机（drone），它偷偷接管另一台连接到因特网的计算机，然后利用这台计算机发起攻击，这种攻击难以追踪到僵尸程序的制造者。僵尸程序通常放置在数百或数千台的计算机上，这些计算机属于受信任的第三方。僵尸程序之间常常能够按一种协调的方式行动，这样的集合称为**僵尸网络**。

僵尸网络表现出 3 个特征：僵尸程序功能、远程控制能力和用以传播僵尸程序和构建僵尸网络的传播机制。我们依次探讨这些特点。

1. 僵尸的用途

以下是僵尸的用途：

- **分布式拒绝服务攻击**：分布式拒绝服务（DDoS）攻击是一种对于计算机系统或者网络的攻击，使用户无法获得服务。
- **垃圾邮件**：在僵尸网络和数以千计的僵尸程序的帮助下，攻击者能够发送大量的垃圾邮件。
- **嗅探数据流**：僵尸程序也可以利用报文嗅探器来监控进出受害机器的有趣的明文数据。嗅探器大多数用于获得敏感信息，例如用户名和密码。
- **键盘记录器**：如果受害机器利用了加密通信信道（例如 HTTPS 或者 POP3S），那么仅仅嗅探受害计算机上的网络报文是没用的，因为没有对应的密钥解密报文。但是通过利用键盘记录器捕获被感染机器的击键，攻击者可以获得敏感信息。已实现的过滤机制（例如，“我只对关键词‘paypal.com’附近的击键序列感兴趣”）进一步帮助偷窃秘密数据。
- **传播新的恶意软件**：僵尸网络用于传播新的僵尸程序。这非常容易做到，因为所有的僵尸程序实现了通过 HTTP 或 FTP 下载并执行文件的机制。一个包含 1 万台主机的

僵尸网络作为蠕虫或邮件病毒的初始基地，使它们非常快速地传播并因此造成更大的危害。

- **安装广告附加组件和浏览器帮助对象（BHO）**：僵尸网络也可以用于获取金融优势。这通过建立刊登一些广告的虚假网站来完成：网站的操作人员与一些支付广告点击费的托管公司达成协议。通过僵尸网络的帮助，这些点击能够“自动化”，几千个僵尸程序瞬间点击弹出的广告。如果僵尸程序劫持了受害机器的起始页，这个过程可以进一步加强，每次受害者使用浏览器时都会执行“点击”。
- **攻击 IRC 聊天网络**：僵尸网络也可以用于攻击因特网中继聊天（Internet Relay Chat，IRC）网络。这类攻击中较流行的是所谓的克隆攻击：在这种攻击中，控制器命令每个僵尸程序将大量的克隆程序连接到被攻击 IRC 网络，被攻击的网络被数以千计的僵尸程序发送的服务请求或者信道连接淹没。通过这样的方式，被攻击的 IRC 网络被击垮，这类似于 DDoS 攻击。
- **操作网上投票 / 游戏**：网上投票 / 游戏受到越来越多的关注，并且用僵尸网络对它们进行操作显得更加容易。由于每个僵尸程序都有一个不同的 IP 地址，所以每张选票都具有和真实的人所投的选票相同的可信度。网络游戏可以通过相似的方式进行操作。

2. 远程控制设施

远程控制设施是将僵尸程序和蠕虫区分开来的一个特征。蠕虫传播自身并激活自身，而僵尸程序受某些中心设施控制，至少在最初阶段是这样。

实现远程控制设施的典型方式是，在 IRC 服务器上，所有僵尸程序连接到这个服务器的一个特定通道，把接收的信息作为指令。较新的僵尸网络倾向于不使用 IRC 机制，而是通过 HTTP 等相关协议的隐蔽通信信道。为了避免单点控制失效，也利用了分布式控制机制。

一旦控制模块和僵尸程序之间建立了通信路径，控制模块就可以激活僵尸程序。在最简单的方式中，控制模块只是向僵尸程序发出命令，让僵持程序执行已经布置好的例程。为了更加灵活，控制模块可以发出更新指令，命令僵尸程序从因特网中的某些位置下载文件并执行。在后面这个例子中，僵尸程序成为了一个可发动多种攻击的更加通用的工具。

3. 构造攻击网络

对于攻击者而言，僵尸网络攻击的第一步是利用僵尸软件感染很多机器，这些机器最终用于发起攻击。攻击阶段的基本要素为：

1）能够发起攻击的软件。软件必须能够在大量机器上运行，能够隐藏其存在，能够与攻击者通信或者具备某种时间触发机制，能够向目标发起预定的攻击。

2）大量系统中存在的漏洞。攻击者必须知道很多系统管理员和个人用户修补失败的漏洞，这些漏洞使攻击者能够安装僵尸软件。

3）用于定位和识别具有漏洞的机器的策略，即称为**扫描**或**指纹识别**的过程。

在扫描过程中，攻击者首先寻找一些有漏洞的机器并感染它们。然后，安装在被感染机器上的僵尸程序通常会重复同样的扫描过程，直到建立一个由被感染机器组成的大型分布式网络。以下是扫描策略的分类：

- **随机**：每台被感染的机器用不同的种子，在 IP 地址空间中随机扫描地址。这种技术会产生大量的网络流量，可能会在实际的攻击发起之前造成网络大范围中断。
- **目标机器列表**：攻击者首先编制一份可攻击的有漏洞机器的长名单。为了躲过对攻击

的检测，这可能是一个缓慢的过程，需要在很长一段时间内完成。一旦名单编制好了，攻击者开始感染名单列表中的机器。每台被感染的机器分配到扫描名单中的一部分。这种策略导致扫描周期非常短，使得检测感染是否正在发生变得困难。

- **拓扑结构**：这种方式利用被感染机器携带的信息，寻找更多的主机去扫描。
- **本地子网**：如果在防火墙后的主机能够被感染，那么这台主机在它所处的本地网络中寻找目标。这台主机利用子网地址的结构，寻找其他被防火墙保护的主机。

18.5.4　垃圾（大量不请自来的）邮件

随着因特网过去几十年爆发式的增长，电子邮件的广泛使用以及发送大量电子邮件只需极低的成本，迎来了大量不请自来的电子邮件的增长，这种电子邮件俗称为垃圾邮件。最近的一些估计表明，在所有发送的邮件中垃圾邮件占了 90% 或者更多。不管对于转发流量的网络构架，还是对于需要从大量邮件中过滤自己正常的电子邮件的用户，这都大大增加了开销。为了应对这样爆炸式的增长，反垃圾邮件行业也相应快速增长，他们提供检测和过滤垃圾邮件的产品。这已经导致了垃圾邮件发送者与防御者之间的竞争，前者开发技术使垃圾邮件能够穿透防线，而后者努力阻止它们。

虽然有些垃圾邮件是从合法邮件服务器发送的，但是目前大多数垃圾邮件是僵尸网络利用受害的用户系统发送的。很大一部分垃圾电子邮件的内容是广告，试图说服接收者在线购买一些产品，例如药品，或者股票欺诈、洗钱工作之类的骗局中使用的广告。垃圾邮件也是恶意软件的重要载体，电子邮件可以携带一个附件文档，如果被打开，能够利用软件漏洞在用户系统上安装恶意软件，这正如我们在前面章节讨论的。或者，电子邮件可以附带木马程序或者脚本代码，如果运行，也会在用户系统上安装恶意软件。有些木马通过利用软件漏洞避开户许可的需要，以达到安装自己的目的，这点我们接下来讨论。最后，垃圾邮件可以用于钓鱼攻击，它通常将用户引导至镜像某些正当服务的虚假网页，例如网上银行页面，这里虚假网页试图获得用户的登录名、密码。或者引导用户完成足够详细的个人信息表格，让攻击者在身份盗窃中冒充用户。所有的这些用途使垃圾电子邮件成为一个重大的安全性问题。然而，在很多情况下，它需要用户主动选择查看电子邮件和所有附件，或者允许一些程序的安装，以使损害发生。

18.6　键盘记录器、钓鱼和间谍软件

我们现在考虑负载（payload），通过它恶意软件收集用户存储在被感染系统上的数据，供攻击者使用。常见的目标是用户银行、赌博以及相关网页的登录名与密码凭证，攻击者利用这些凭证冒充用户登录网页获取利益。不太常用的负载是为了侦查或者间谍活动的文档或者系统配置详细信息，这些攻击的目标为信息的保密性。

18.6.1　凭据盗窃、键盘记录器和间谍软件

通常，用户将他们的账户、密码凭证通过加密通信信道（例如，HTTPS 或 POP3S）发送到银行、赌博以及相关的网页，这些加密通信信道保护它们不被网络流量监控器捕获。为了绕过这个机制，攻击者可以安装一个**键盘记录器**，捕获被感染机器上的击键，允许攻击者监控敏感信息。由于这会导致攻击者接收到受害机器上所有文本输入的副本，所以键盘记

录器往往会应用某种形式的过滤机制，仅仅返回与所需关键字（例如，“账户”、“密码”或“paypal.com”）接近的信息。

为了应对键盘记录器的使用，有些银行和其他网站转而使用图形小程序输入关键信息，例如密码。由于这样不通过键盘进行文本输入，传统的键盘记录器不会捕获这些消息。作为回应，攻击者开发了更通用的间谍软件，破坏受害机器以允许监视系统上较大范围的活动。这可能包括监视浏览活动的历史和内容，将某些 Web 页面请求重定向到攻击者控制的虚假网站，以及动态修改在浏览器和某些感兴趣网站之间交互的数据。所有的这些都对用户私人信息造成重大威胁。

Zeus 银行木马是这类负载的一个突出的例子，它由自身的犯罪软件工具制作，在最近几年被广泛使用【BINS10】。它通过使用键盘记录器和捕获或修改某些网页的表单数据来偷窃银行和金融凭据。它往往利用垃圾电子邮件或通过被攻破的“由下载驱动”的网站进行部署。

18.6.2　钓鱼和身份盗窃

另一种用于抓取用户账户和密码凭据的途径是在垃圾邮件中包含 URL，它链接到攻击者控制的虚假网页，而这些网页伪造成一些银行、赌博或者类似网站的登录页面。这个 URL 通常包含在建议用户需要立即采取行动认证他们的账户或防止账户被锁定的信息中。如果用户粗心没有意识到他们被欺骗了，然后进入链接并提交所需要的详细信息，将会导致攻击者使用获取的凭证利用他们的账户。

更普遍的是，这样的垃圾邮件可能引导用户到攻击者控制的一个虚假网站，或者引导用户完成一些附带的表格并返回到一个攻击者可以打开的电子邮件，这个电子邮件用于获得用户的个人隐私信息。获得足够的详细信息后，攻击者可以冒充用户的身份，达到获得信用卡或者其他资源的敏感权限的目的。这就是所谓的**钓鱼**攻击，利用社会工程学，通过伪装成来自可信源的通信来提升用户的信任 [GOLD10]。

这种普通的垃圾邮件通常利用僵尸网络，广泛地发送给大量的用户。由于对于大部分接收者来说，邮件内容与适当的信任源不匹配，所以攻击者只能依靠垃圾邮件传递到足够多的将其命名为可信源的用户，他们中的少部分人会回应，因为这是有利可图的。

垃圾邮件的一种更危险的变种是**鱼叉式网络钓鱼**攻击。这依旧是一封声称来自信任源的电子邮件。但是，攻击者仔细研究了接收者，每封电子邮件都被仔细制作，适合于特定的收件人。邮件常常列出一系列的信息，使接收者相信它的真实性。正如攻击者所期望的，这大大增加了接收者回复的可能性。

18.6.3　侦查和间谍活动

凭据盗窃和身份盗窃是侦查负载的特例，更一般的侦查负载目标在于获得所需要的特定种类的信息并返回给攻击者。这些特例当然是最常见的，然而其他的目标也为人所知。2009 年的极光行动（Operation Aurora）利用一个木马获得一系列高科技、安全和防御承包公司的源代码库权限，并进行偷偷地修改【SYMA11】。2010 年发现的震网（Stuxnet）蠕虫为了判断要攻击的特定目标系统是否已经受到损害，收集系统硬件和软件配置的详细信息。这个蠕虫的前期版本返回同样的信息，然后这些信息用于开发后续版本中用到的攻击方式 [CHEN11]。

18.7　计算机安全趋势

为了评估各种威胁的相对严重程度，并保证计算机安全的各种方法的相对重要程度，参照相关组织的经验是有用处的。2010 年 /2011 年 CSI 计算机犯罪和安全调查报告提供了一个有用的观点，该报告由计算机安全研究所【CSI10】给出，调查对象包括超过 350 家美国的公司、非盈利组织和公共部门。

图 18-5 给出调查对象遭受过的 9 种主要的攻击种类[⊖]。非常值得注意的是，大规模并且日益盛行的恶意软件攻击。另一个值得注意的地方是，大多数攻击种类表现出有点下降的趋势。CSI 报告推测在很大程度上归功于相关组织安全技术的提升。

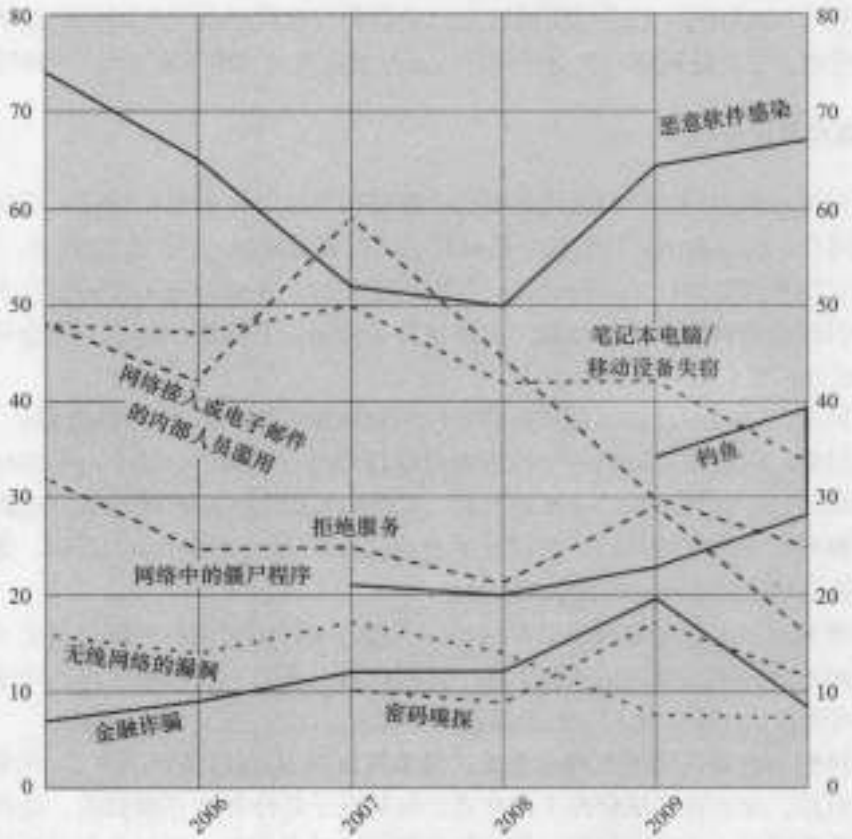


图 18-5　遭受过的攻击类型（根据调查对象的比例）

来源：计算机安全研究所 2010 年 /2011 年 CSI 计算机犯罪和安全调查报告

图 18-6 指出，相关组织用以应对威胁的安全技术种类。防火墙和杀毒软件用得最广泛。这种受欢迎程度反映了许多因素：

- 这些技术的成熟度意味着安全管理者对这些产品非常熟悉，并对它们的有效性很有信心。
- 因为这些技术比较成熟并且有大量的供应商，所以它们所带来的开销往往是合理的，并且提供友好的用户界面。
- 这些技术对抗的威胁属于安全管理员面临的最重要的威胁。

⊖ 包含低发电率攻击种类的完整列表见该书优质内容网站的文档目录中 Types-of-Attacks.pdf 文件。

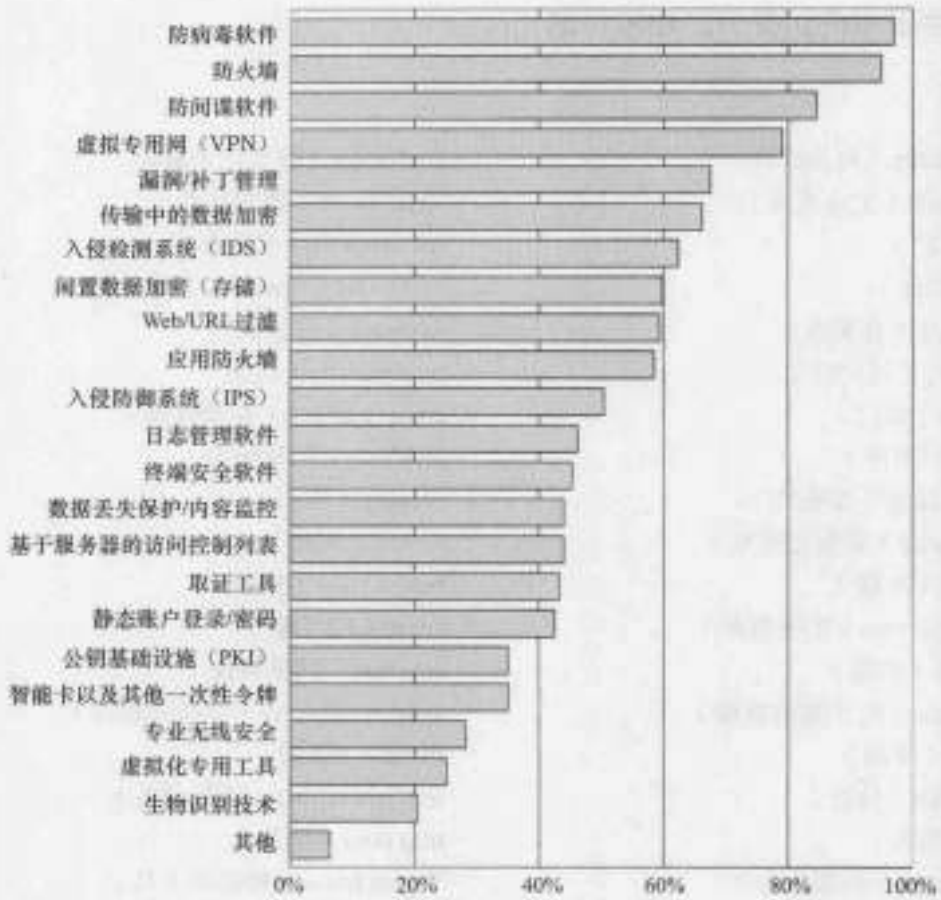


图 18-6　使用的安全技术

来源：计算机安全研究所 2010 年/2011 年 CSI 计算机犯罪和安全调查报告

18.8　总结

任何计算机或者网络安全系统的主要目标是保密性（确保数据保密以及维护个人的隐私），完整性（确保数据不会通过未经授权的方式被修改以及确保系统正常运作）和可用性（确保系统服务不会拒绝授权用户）。其他的目标还包括真实性（确保消息以及消息源是合法的）和可追踪性（实体的行为能够唯一地追溯到那个实体的需求）。考虑到这些目标，安全威胁可以基于某给定的攻击如何威胁到给定的目标进行分类。

两个最重要的安全威胁是入侵者和恶意软件。入侵者表现出各种行为模式，并且利用各种技术获得未经认证的系统资源访问权限。

恶意软件是为了给目标计算机造成损害或耗尽目标计算机资源而设计的软件。它经常隐藏在正常软件中或者伪装成正常软件。在某些情况下，它通过电子邮件或者感染磁盘传播到其他计算机。恶意软件中两个最重要的类别是病毒和蠕虫。计算机病毒是软件，可以通过修改其他程序而“感染”它们；修改行为包括通过例程注入原程序从而制造病毒程序的副本，然后继续感染其他程序。蠕虫是一个可以复制自身、通过网络连接将副本从一台计算机发送到另一台计算机的程序。到达另一台计算机后，蠕虫可以再次被激活进行复制和传播。除了传播外，蠕虫通常会执行一些不需要的功能。

18.9 关键术语、复习题和练习题

关键术语

accountability（可追踪性）
active attack（主动攻击）
asset（资产）
attack（攻击）
authenticity（真实性）
availability（可用性）
back door（后门）
bots（僵尸程序）
confidentiality（保密性）
data integrity（数据完整性）
deception（欺骗）
denial of service（拒绝服务）
disruption（中断）
e-mail virus（电子邮件病毒）
exposure（暴露）
falsification（伪造）
hacker（黑客）
insider attack（内部攻击）
integrity（完整性）
interception（窃听）
intruder（入侵者）
intrusion（入侵）
keylogger（键盘记录器）
logic bomb（逻辑炸弹）
macro virus（宏病毒）
malicious software（恶意软件）
malware（恶意软件）
masquerade（伪装）
passive attack（被动攻击）
phishing（钓鱼攻击）
privacy（隐私）
replay（重放）
repudiation（抵赖）
spam（垃圾邮件）
spyware（间谍软件）
system integrity（系统完整性）
threat（威胁）
traffic analysis（流量分析）
trap door（陷门）
Trojan horse（特洛伊木马）
usurpation（篡改）
virus（病毒）
virus kit（病毒工具箱）
worm（蠕虫）

复习题

18.1 描述计算机安全的定义。
18.2 计算机安全解决的基本需求是什么？
18.3 主动安全威胁和被动安全威胁的不同点是什么？
18.4 列出并简要阐述 3 种入侵者。
18.5 列出并简要阐述入侵者的行为模式
18.6 病毒操作中压缩的作用是什么。
18.7 病毒操作中加密的作用是什么。
18.8 病毒或者蠕虫操作有哪几个典型阶段？
18.9 从总体上看，蠕虫是如何传播的？

练习题

18.1 考虑一台自动柜员机（ATM），用户提供个人识别号（PIN）以及用于账户访问的磁卡，

给出与这个系统相关的保密性、完整性、可用性需求的例子，在每个例子中指出需求的重要程度。

18.2　针对电话交换系统重述练习题 18.1，该系统根据呼叫者拨打的电话号码，通过交换网络决定拨号的途径。

18.3　考虑一个用于为不同机构生成文档的台式打印系统。

a. 给出一个打印的例子，其中存储数据的保密性是最重要的需求。

b. 给出一个打印的例子，其中数据完整性是最重要的需求。

c. 给出一个系统可用性是最重要需求的例子。

18.4　针对以下每个资产，为保密性、可用性、完整性的缺失分别指定低、中、高的影响程度。解释你的答案。

a. 一个组织管理 Web 服务器上的公开信息。

b. 一个执法机构管理非常敏感的调查信息。

c. 一个金融组织管理的日常管理信息（不涉及隐私的信息）。

d. 合约组织中用于大型收购的信息系统，包含敏感的预招揽阶段合同信息和常规管理信息。分别评估两个数据集的影响，然后将信息系统作为一个整体进行评估。

e. 发电厂有一个 SCADA（监督控制和数据采集）系统，为大型军事设施控制电力分布。SCADA 系统包含了实时的传感器数据和常规的管理信息。分别评估两个数据集的影响，然后将信息系统作为一个整体进行评估。

18.5　假设密码从 26 个字母中挑选 4 个字母的组合得到，假定对手按每秒一次的频率尝试密码。

a. 假设敌手直到完成每次尝试后才获得反馈，那么发现正确密码的期望时间是多少？

b. 假设一旦输入任何不正确的字母，敌人就会得到反馈，那么发现正确密码的期望时间是多少？

18.6　在图 18-3 的病毒程序中有一个缺陷，这个缺陷是什么？

18.7　是否可能开发能够分析软件、判断其是否是病毒的程序。假设我们有一个程序 D 能够完成这个功能，对于任意程序 P，如果运行 D（P），返回的结果是 TRUE（P 是病毒）或者 FALSE（P 不是病毒）。现在考虑如下程序：

```
Program CV :=
 {...
 main-program :=
   {if D(CV) then goto next;
        else infect-executable;
   }
next:
 }
```

在以上程序中，infect-executable 是扫描内存寻求可执行程序并将自己复制到那些程序中的一个模块。判断 D 能否正确判断 CV 是否是病毒。

18.8　本题的要点是说明设计恶意软件时必须要解决的问题种类，继而阐释应对这样的攻击需要采取的思维方式。

a. 考虑下面的 C 程序。你认为这个程序想要做什么？它能够运行吗？

```
begin
  print (*begin print (); end.*);
end
```

b. 针对以下程序，回答同样的问题。

```
char [] = {'0', ' ', '}', ';', 'm', 'a', 'i', 'n', '(',
          ')', '{',
and so on... 't', ')', '0');
main ()
  {
    int I;
    printf("char t[] = {");
    for (i=0; t[i]!=0; i=i+1)
          printf("%d, ", t[i]);
    printf("%s", t);
  }
```

c. 本题与本章节所讨论的问题有什么关联？

18.9 考虑以下片段，这是什么类型的恶意软件？

```
  legitimate code
if data is Friday the 13th;
  crash_computer();
legitimate code
```

18.10 考虑认证程序中的如下片段，这是什么类型的恶意软件？

```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
  return ALLOW_LOGIN;
if username and password are valid
  return ALLOW_LOGIN
else return DENY_LOGIN
```

18.11 下面代码段显示的是病毒指令序列或病毒变形体版本，描述变形体代码产生的影响。

原始代码	变形体代码

mov eax, 5
add eax, ebx
call [eax]
	mov eax, 5
	push ecx
	pop ecx
	add eax, ebx
	swap eax, ebx
	swap ebx, eax
	call [eax]
	nop

计算机和网络安全技术

学习目标

通过本章的学习，读者应该能够：

- 讨论使用 IPSec（Internet Protocol Security）来创建一个虚拟专用网（VPN）。
- 讨论安全套接字层（SSL）在网站安全中的作用，并说明其基本功能。
- 说明 Wi-Fi 保护访问（Wi-Fi Protected Access，WPA）在 802.11 网络中的使用。
- 了解入侵检测系统的基本原理和技术。
- 说明防火墙的特点和类型。
- 学会抵御不同类型恶意软件的方法。

本章介绍用来抵御第 18 章中所讨论的安全威胁的常见措施和协议。

19.1 虚拟专用网和 IPSec

在第 8 章介绍的虚拟专用网（VPN）和 IPSec 中，我们看到 IPSec 的应用和优点。本节我们将介绍一些技术细节。

19.1.1 IPSec 的功能

IP 级的安全性包括 3 个功能区：身份鉴别（authentication，也称为身份认证）、保密性（confidentiality）和密钥管理（key management）。事实上，鉴别机制（authentication mechanism，也称为认证机制）可以确保所接收的数据包是由数据包头中的源地址所表明的实体发送的。此外，这种机制确保在传输过程中，该数据包没有被篡改。保密设施是对通信节点的信息进行加密，防止第三方窃听。密钥管理机制关心的是密钥的安全交换。当前版本的 IPSec 为 IPSecv3，使用封装安全负载（ESP）协议实现鉴别和保密性。密钥管理机制是由因特网密钥交换标准 IKEv2 协议提供。

19.1.2 传输模式和隧道模式

ESP 支持两种使用模式：传输模式和隧道模式。

传输模式主要为上层协议提供保护。也就是说，传输模式的保护延伸到 IP 数据包的有效载荷。通常，传输模式用于两个主机（例如，一个客户端和一个服务器，或两个工作站）之间端到端的通信。传输模式对 IP 数据包的有效载荷进行 ESP 加密和选择性的鉴别，但不包含 IP 头（如图 19-1b 所示）。对于相对较小的网络，配置传输模式是有用的，其中每一台主机和网站服务器都配备 IPSec。然而，对于一个完全成熟的 VPN，隧道模式的效率会高得多。

隧道模式对整个 IP 数据包提供保护。为了实现这一点，将 ESP 字段添加到 IP 数据包后，将整个数据包加上安全字段视为一个新的外部 IP 数据包的有效载荷，该外部 IP 数据包带有

一个新的外部 IP 头。整个原始或内部数据包穿过“隧道”从一个站点到另一个 IP 网络，整个转发路径都没有路由器能够检查内部 IP 头。由于原始数据包被封装，所以新的、更大的数据包可能有完全不同的源地址和目的地址，这样就增加了安全性。当两端中的至少一个是装有 IPSec 的防火墙或路由器的安全网关时才使用隧道模式。使用隧道模式，网络上防火墙后的大量主机无需安装 IPSec 就可以进行安全的通信。这样的主机所产生的未受保护的数据包使用隧道模式通过外部网络，这种隧道模式就是在本地网络的边界利用 IPSec 软件安装在防火墙或安全路由器上建立的。

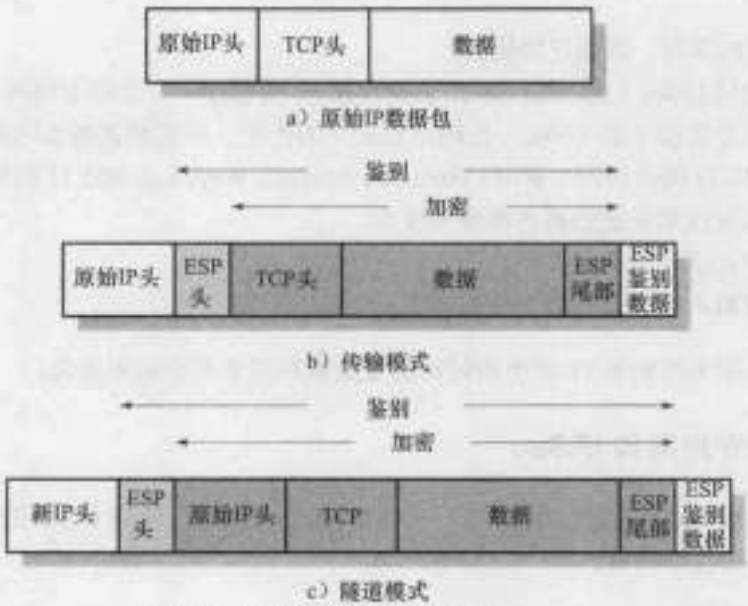


图 19-1　ESP 加密和鉴别的范围

下面是一个在隧道模式下 IPSec 如何运行的例子。网络上的主机 A 产生一个 IP 包，该包带有另一个网络上的主机 B 的目的地址。这一数据包从源主机 A 路由到 A 本地网络防火墙或安全路由器。防火墙过滤所有传出的数据包，以确定是否需要进行 IPSec 处理。如果此数据包从 A 到 B 需要 IPSec，则防火墙进行 IPSec 处理，并将数据包封装外部 IP 报头。外部 IP 数据包中的源 IP 地址可能就是该防火墙地址，而目的地址是 B 的本地网络防火墙地址。该数据包发送到 B 的防火墙前通过中间路由器时仅检查外部 IP 报头。在 B 的防火墙将外部 IP 头剥离，将内部数据包传送到主机 B。

隧道模式中的 ESP 对包括内部 IP 头的整个内部 IP 数据包进行加密并有选择地进行鉴别。

19.1.3　密钥管理

IPSec 的密钥管理部分涉及密钥的产生和分配。IPSec 架构文档要求支持两种类型的密钥管理：

- **手动配置**：系统管理员（SA）用自己的密钥和其他通信系统的密钥手动配置每个系统。这对于小的、相对静态的环境比较适用。
- **自动配置**：这种方式在配置不断变化的大型分布式系统中按需创建密钥并更好地使用这些密钥。自动化管理方式是比较灵活的，但也需要更多的配置工作和更多的软件，所以较小的设施可能会选择手动密钥管理。

19.1.4　IPSec 和 VPN

促使企业接受和部署安全 IP 的驱动力是，用户可将自己的 WAN/ LAN 基础设施和因特网相连并达到以下目的：1）访问因特网服务；2）将因特网作为广域网传输系统的一个组成部分使用。用户需要保护他们的网络，同时还能通过因特网发送和接收信息。安全的 IP 鉴别和加密机制是提供安全策略的基础。

由于 IP 安全机制的定义独立于当前的 IP 或 IPv6 的使用，所以部署这些机制不依赖于 IPv6 的部署。事实上，我们很可能会看到在 IPv6 流行之前的很长时间中，IP 安全功能会得到广泛使用，因为与当前 IP 相比较，对 IP 层安全性的需要远大于 IPv6 提供的增值功能。

随着 IPSec 的到来，管理人员有一个标准化的方式实现对 VPN 的安全性。此外，IPSec 中使用的所有加密、鉴别算法和安全协议都得到很好的研究，并在多年的审查下一直适用。因此，用户可以放心的是，IPSec 设备确实提供了强大的安全性。

IPSec 可以安装在组织拥有或操作的路由器或防火墙上，这使网络管理员对 VPN 的安全方面得以完全掌控，这是网络管理员非常渴望做到的。然而，IPSec 是一组复杂的功能和模块，它管理和配置的任务艰巨。另一种方法是从服务提供商寻求解决方案。服务提供商可以简化基于因特网的 VPN 的规划、实施和维护，从而可以安全地访问网络资源并进行网站之间的通信。

19.2　SSL 和 TLS

第 10 章介绍了安全套接字层（Secure Sockets Layer，SSL）和后续的因特网标准传输层安全（Transport Layer Security，TLS）。本节提供一些技术细节。

19.2.1　SSL 架构

SSL 使用传输控制协议（TCP）来提供可靠的端到端安全服务。SSL 不是一个单独的协议，而是如图 19-2 所示的两层协议。

SSL 记录协议为各种高层协议提供基本的安全服务。特别是，超文本传输协议（HTTP），它可以在 SSL 的顶部操作，为 Web 客户机 / 服务器的交互提供传输服务。3 个高层协议：握手协议、改变密码规范协议和告警协议是 SSL 中定义的一部分，这些特定的 SSL 协议用来管理 SSL 的交互，并在本节后面研究。



图 19-2　SSL 协议栈

SSL 会话和 SSL 连接是 SSL 的两个重要概念，它们在规范中定义如下：

连接：连接（在开放系统互连（OSI）分层模型中的定义）是一个提供了合适的服务类型的传输。对于 SSL，这种连接是对等关系。连接是短暂的，每个连接都与一个会话相关联。

会话：SSL 会话是在客户端和服务器之间的关联。会话由握手协议建立，定义了一组可在多个连接之间共享的加密安全参数。会话用于避免每个连接所需的新安全参数的高昂协商。

任何各方（如 HTTP 客户端和服务器上的应用程序）之间可能有多个安全连接。理论上，在各方之间也可以同时进行多方会话，但在实践中不使用此功能。

19.2.2　SSL 记录协议

SSL 记录协议为 SSL 连接提供两种服务：

保密性：握手协议定义了一个共享密钥，用于 SSL 有效载荷的对称加密。

消息完整性：握手协议还定义了一个共享密钥，用于形成一个消息鉴别码（MAC）。

图 19-3 表示 SSL 记录协议的完整操作。第一步是**分块**。每个上层的消息被分割成 2^{14} 个字节（16 384 字节）或更小的块。接着，选择性地应用压缩。下一步骤处理的是对压缩的数据计算**消息鉴别码**。接下来，使用对称加密方法对压缩的消息和 MAC 进行加密。（本章引用的密码学概念在附录 J 中论述。）

SSL 记录协议处理的最后一步是在前面加一个报头，它包括一个长度字段和指明哪些更高层协议（见图 19-2）用来处理封装的块的标识域。

接着，记录协议发送 TCP 段中产生的结果单元。对接收的数据进行解密、鉴别、解压缩、重新组合，然后将它传送给更高层的用户。

19.2.3　握手协议

有 3 个 SSL 特定协议使用 SSL 记录协议。改变密码规范协议更新该连接上使用的密码套件。告警协议用于对等实体传递与 SSL 相关的警告。

SSL 中最复杂的部分是握手协议。该协议允许服务器和客户端相互鉴别并协商加密、MAC 算法和用于保护 SSL 记录中传送数据的密钥。握手协议使用在任何应用程序的数据被发送之前。

握手协议包含一系列客户机和服务器交换的消息。消息交换具有 4 个阶段。

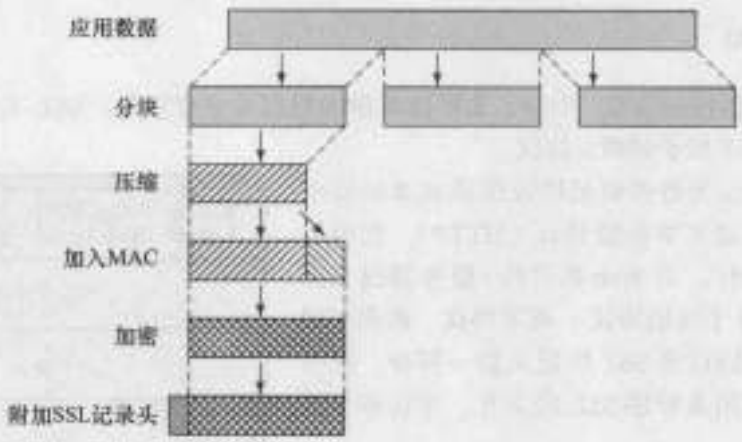


图 19-3　SSL 记录协议操作

第 1 阶段用于初始化一个逻辑连接，并建立与它相关联的安全能力（security capability）。交互由客户机发起，以优先权递减顺序发送一个包含客户机支持的加密算法组合的 CLIENT_HELLO 消息。列表中的每一个元素（每个加密套件）定义了密钥交换算法和加密规范。

客户机发送 CLIENT_HELLO 消息后，等待包含与 CLIENT_HELLO 消息相同参数的 SERVER_HELLO 消息。

第 2 阶段的具体情况依赖于使用的底层公钥加密方案。在某些情况下，服务器传递证书给客户机，有可能包含额外的密钥信息和来自客户端证书请求。

第 3 阶段如果需要，客户机认证服务器提供证书的有效性，并检查确认该 SERVER_HELLO 参数是合适的。如果一切满足，客户机依赖于底层公钥方案发送一个或多个消息返回到服务器。

第 4 阶段建立一个供双方通信的安全连接，确保交互已经成功。

19.3　Wi-Fi 网络安全接入

正如在第 14 章中讨论的，802.11i 任务组已经开发了一套用于解决无线局域网（WLAN）安全问题的能力集。为了加快将强安全机制引入无线局域网的速度，Wi-Fi 联盟发布 Wi-Fi 网络安全接入（WPA）作为 Wi-Fi 标准。WPA 是一套安全机制，基于 802.11i 标准的当前状态，同时消除了 802.11 的大部分安全性问题。随着 802.11i 标准的发展，WPA 也会随之演化以保持兼容性。

IEEE 802.11i 解决了 3 种主要的安全问题：身份鉴别、密钥管理和数据传输的隐私性。为了提高鉴别能力，802.11i 需要使用鉴别服务器（AS），并定义一个更可靠的鉴别协议。AS 还在密钥分发中起到重要作用。对于隐私性，802.11i 提供了 3 种不同的加密方案。提供长期解决方法的方案使用 128 位密钥的高级加密标准（AES）。然而，因为 AES 的使用需要对现有设备进行高代价的升级，所以也定义了基于 104 位的 RC4 的替代方案。

图 19-4 给出了 802.11i 操作的概述。首先，站点和无线接入点（AP）之间的交流使得双方就使用的安全能力集达成一致。然后，AS 和站点的交换提供安全认证。AS 负责给无线接入点（AP）分发密钥，反过来 AP 管理和分发密钥给站点。最后，用强加密机制来保护站点和无线接入点（AP）之间的数据传输。



图 19-4　802.11i 的操作步骤

802.11i 标准的架构包括 3 个主要成分：

身份鉴别：用来定义用户和 AS 之间消息交换的协议，这里 AS 提供相互认证的功能，并产生客户端和 AP 之间无线链路上要使用的临时密钥。

接入控制：此功能强制使用认证功能，正确地路由消息，并提供密钥交换的便利。它可以与各种身份鉴别协议协同工作。

消息的完整性和隐私性：对 MAC 层数据（例如 LLC PDU）和消息完整性代码进行了加密，确保数据没有被篡改。

鉴别工作在 LLC 和 MAC 协议层以上进行，并被认为是超越了 802.11 的范围。目前有许多主流的身份鉴别协议可以使用，包括可扩展认证协议（EAP）和远程身份认证拨入用户服务（RADIUS）。这些内容不包括在本书中。本节其余部分考察接入控制和信息的完整性与保密性。

访问控制

EEE 802.11i 标准使用对局域网提供接入控制功能的另一个标准 IEEE 802.1X，该标准为基于端口的网络接入控制，使用术语请求者（supplicant）、认证装置（authenticator）和认证服务器（Authentication Server，AS）。在 802.11WLAN 的条款中，前两个术语分别对应无线站点和 AP。在网络的有线端（如分布式系统的访问），认证服务器（AS）是一个典型的隔离设备，但也可以直接驻留在认证装置中。

请求者在被使用身份鉴别协议的认证服务器（AS）认证之前，认证装置仅仅在客户端和 AS 之间传递控制或认证消息。此时 802.1X 的控制通道是畅通的，但 802.11 数据通道被阻塞。一旦某用户的身份经过鉴别并提供了密钥，认证装置按照预定义的请求者访问控制限制，将来自请求者的数据转发到网络。这种情况下，数据通道是畅通的。

如图 19-5 所示，802.1X 使用受控和非受控端口的概念。端口是定义在认证装置的逻辑实体，看做物理的网络连接。对于一个无线局域网，认证装置（即 AP）可能只有两个物理端口：一个连接到分布式系统（DS），另一个用于它的基本服务集（BSS）的无线通信。将每个逻辑端口映射到这两个物理端口中的其中一个。非受控端口允许请求者和其他 AS 之间交换协议数据单元（PDU），而不管请求者身份鉴别的状态如何。受控端口仅在请求者的当前状态授权这样的交换时，才允许在客户端和局域网上其他系统之间交换协议数据单元（PDU）。

带有上层认证协议的 802.1X 框架非常适用于 BSS 架构，它包括许多无线站点和 AP。然而，一个独立的 BSS（IBSS），没有 AP。802.11i 提供了一个更复杂的解决方案，本质上涉及 IBSS 上站点两两之间的相互认证。

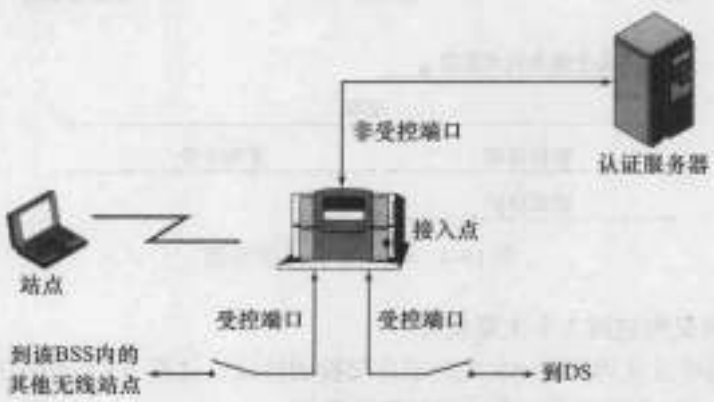


图 19-5　802.11i 的接入控制

19.4　入侵检测

来自 RFC 4949（因特网安全术语表）的以下定义与本书的讨论相关。

入侵：一个安全事件或多个安全事件的组合，其构成入侵者获得或试图获得未授权系统（或系统资源）访问的安全事故。

入侵检测：一种监控和分析系统事件的安全服务，目的是发现试图在未经授权的方式下访问系统资源的活动，并提供实时或近实时的警告。

入侵检测系统（IDS）可以分为以下几种类型：

- **基于主机的 IDS**：监控一台主机内发生的可疑事件的特点。
- **基于网络的 IDS**：监控特定的网段或设备的网络流量，分析网络、传输和应用协议以识别可疑活动。

入侵检测系统包括 3 个逻辑组件：

- **传感器**：传感器负责收集数据。传感器的输入可以是包含入侵证据的系统的任何信息，输入可包括网络数据包、日志文件和系统调用痕迹。传感器收集这些信息并转发到分析器。
- **分析器**：分析器接收来自一个或多个传感器或从其他分析器的输入。分析器负责确定是否发生了非法入侵。此组件的输出用于表明是否发生了非法入侵，也可以包括支持入侵发生结论的证据，以及在入侵情况下给予应该采取行动措施的指导性建议。
- **用户界面**：在 IDS 的用户界面上，用户能够查看系统输出或控制系统的行为。在某些系统中，用户接口可能等同于管理者、引导者或控制台组件。

19.4.1　基本原理

身份认证机制、访问控制设施和防火墙都在入侵防御中发挥重要作用。而一道防线就是入侵检测，这一直是近年来大量研究的重点。这主要是受多方面因素的驱动，包括以下几个方面：

1）如果足够快地检测到入侵，识别出入侵者就可以被识别，并在发生损害之前或数据遭到威胁之前把他从系统中驱除。即使检测没有足够及时地驱除入侵者，但是越早检测到入侵，产生的损害就越少并且可以实现更快速的恢复。

2）有效的 IDS 可以作为一种遏制措施，从而采取行动阻止入侵。

3）入侵检测能够收集入侵技术的信息，用来加强对入侵的预防措施。

入侵检测的工作前提是：假设入侵者的行为不同于合法用户的行为，并且这种不同可以进行量化。当然，我们不期望入侵者的攻击和授权用户的正常使用之间存在清晰、准确的区分，我们必须预期二者行为之间会有一些重叠。

图 19-6 给出了 IDS 设计者所面临的任务本质。虽然入侵者的典型行为不同于授权用户的典型行为，但这两种行为之间仍有重叠。因此，对入侵者的行为定义宽松一些将捕捉到更多的入侵者，但也会使正常用户得到更多的**误报**，或者使得经授权的用户被认定为入侵者。而对入侵者的行为定义严格一些会减少误报，但也会导致**漏报**的增加，或者入侵者没有被识别出来。因此，在实际的入侵检测中会进行一定的折中处理。

在 Anderson 的研究 [ANDE80] 中，假设能以合理的置信度区分出假冒者和合法用户。通过观察过去的历史记录来建立合法用户的行为模式，并检测与这种模式的显著偏离。Anderson 认为，检测滥用权限者（misfeasor）（合法用户进行未授权的行为）的任务是比较困难的，因为异常行为和正常行为之间的区别可能比较小。Anderson 认为如果仅仅通过搜索异

常行为，这种违规行为将无法被检测出来。然而，滥用权限者的行为通过未授权使用条件的智能定义是可能被检测出来的。最后，检测秘密用户（clandestine user）被认为是超出纯粹的自动化技术范围。这些在 1980 年得出的结论，今天仍然适用。

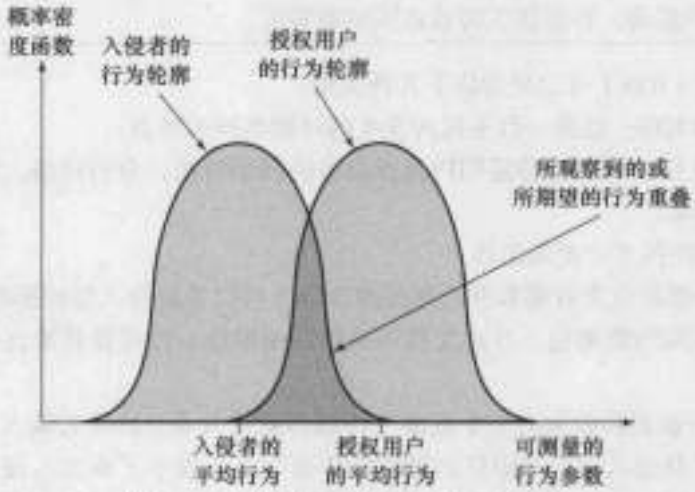


图 19-6　入侵者和授权用户的行为轮廓

在本节的其余部分，我们将重点介绍基于主机的入侵检测。

19.4.2　基于主机的入侵检测技术

基于主机的入侵检测系统给脆弱的、敏感的系统添加一个专门的安全软件层，例如数据库服务器和管理系统。基于主机的 IDS 用各种方法监控系统活动，检测可疑行为。在某些情况下，IDS 可以在造成损害之前阻止攻击，但其主要目的是检测入侵、记录可疑事件和发送告警。

基于主机的 IDS 的主要优点是，它不仅可以检测到外部入侵，也可以检测到内部入侵，这对于基于网络的入侵检测系统和防火墙是不可能实现的。

基于主机的入侵检测系统采用以下两种常用方法检测入侵。

1）**异常检测**：收集在一段时间内合法用户行为有关的数据集合，然后将统计检验应用于观察到的用户行为，以较高的可信度来确定该行为是否是合法的用户行为。以下是统计异常检测的两种方法：

- 阈值检测：此方法定义独立于用户的各种事件发生频率的阈值。
- 基于轮廓的检测：建立每个用户活动的轮廓，用来检测单个账户行为的变化。

2）**特征检测**：定义一组规则或攻击模式的集合，用来判断给定的行为是否为入侵行为。本质上，异常检测试图定义正常或预期的行为，而基于特征的方法试图定义某种行为。

就之前列出的攻击者类型列表而言，异常检测对于伪装者检测是有效的，因为他们不可能模仿占用账户的行为特征。另一方面，这种技术无法处理滥用权限者。对于这样的攻击，特征检测方法通过识别事件和序列来揭示入侵渗透行为。在实践中，系统可使用这两种方法的组合，更有效地对抗更广范围的攻击。

19.5　防火墙

与 IDS 一样，防火墙是另一种基于主机的安全服务。通常，防火墙位于企业网络和因特

网之间，用于建立一个受控的连接，树立一道外部安全屏障或边界。此外部边界的目的是保护企业网络免于遭受基于因特网的攻击，并提供实施安全和审计的唯一瓶颈点。

防火墙提供了一个额外的防御层，将外部网络和内部系统隔绝。它遵循经典的“纵深防御”军事学说，这也适用于 IT 安全。

19.5.1　防火墙特性

[BELL94] 列出了防火墙的设计目标，如下所示：

1）从内到外的所有流量必须通过防火墙，反之亦然。即物理阻断除通过防火墙外的所有本地网络访问。这样的配置有很多种，在本章的后面会加以解释。

2）根据本地安全策略，只允许授权的流量通过。本章的后面解释使用不同类型的防火墙来实现不同类型的安全策略。

3）防火墙本身对渗透（penetration）免疫。这意味着需要使用具有安全操作系统的安全强化系统。可信计算机系统适合安装防火墙，在政府应用中通常要求这样。

[SMIT97] 列出了防火墙用于实现访问控制和加强站点安全策略的 4 种常用技术。最初，防火墙主要关注服务控制，但后来发展到提供如下 4 种技术：

- **服务控制**：确定因特网服务类型，可以是访问、入站或者出站。防火墙可以基于 IP 地址、协议或者端口号过滤流量；可以提供代理服务器软件，在转发流量之前接收并解释每一个服务请求；或者充当服务器软件自身，如 Web 或者邮件服务。
- **方向控制**：确定特定服务请求可以被发起的方向，并允许通过防火墙。
- **用户控制**：依据访问服务的用户名或类型来实现服务的访问控制。此功能通常适用于防火墙边界内部的用户（本地用户），也可以应用到来自外部用户的传入流量。后者需要某种形式的安全认证技术，比如 IPSec 提供的认证机制。
- **行为控制**：控制如何使用某一特别的服务。例如，防火墙可以过滤电子邮件，达到消除垃圾邮件的目的，或能够从外部访问本地 Web 服务器的部分信息。

在讨论防火墙的类型和配置的细节之前，最好总结人们期望从防火墙得到什么。以下这些能力是防火墙可以达到的：

1）防火墙定义了单一的阻塞点，使未经授权的用户无法进入受保护的网络，禁止潜在的易受攻击的服务进入或离开网络，并提供各种方法防止 IP 欺骗和路由攻击。使用单一的阻塞点简化了安全管理，因为安全功能整合在一个系统或一套系统内。

2）防火墙提供了监控安全相关事件的定位，可以在防火墙系统实现审计和报警。

3）防火墙是提供安全不相关的多个因特网功能的平台。这些功能包括将本地地址映射为因特网地址的网络地址翻译功能和审计与记录因特网使用的网络管理功能。

4）防火墙可以作为 IPSec 平台。使用 19.1 节中描述的隧道模式功能，防火墙可以用来实现虚拟专用网（VPN）。

防火墙有其局限性，包括以下问题：

1）防火墙不能防止绕过防火墙的攻击。内部系统可能有拨号连接到网络服务提供商（ISP）的能力。内部局域网可提供一个调制解调器池，为出差员工和远程办公人员提供拨号连接功能。

2）防火墙可能会无法充分防范内部威胁，如心怀不满的员工或与外部攻击者合作的雇员。

3）配置不当的安全无线局域网可能受到来自组织外部的访问，分隔企业网络的内部防火

墙不能防范防火墙不同方面的本地系统之间的无线通信攻击。

4）如果笔记本电脑、平板电脑或便携式存储设备在企业网络之外使用并被感染，然后在内部接入和使用，防火墙也无法控制这种情况。

19.5.2　防火墙类型

防火墙作为一个数据包过滤器，它可以作为一个正向过滤器，仅仅允许满足特定条件的数据包通过，或者作为反向过滤器，拒绝任何符合特定条件的数据包。根据防火墙的类型，它或许检查每个数据包的一个或多个协议包头、每个数据包的有效载荷或一系列数据包所产生的模式。本节介绍防火墙的主要类型。

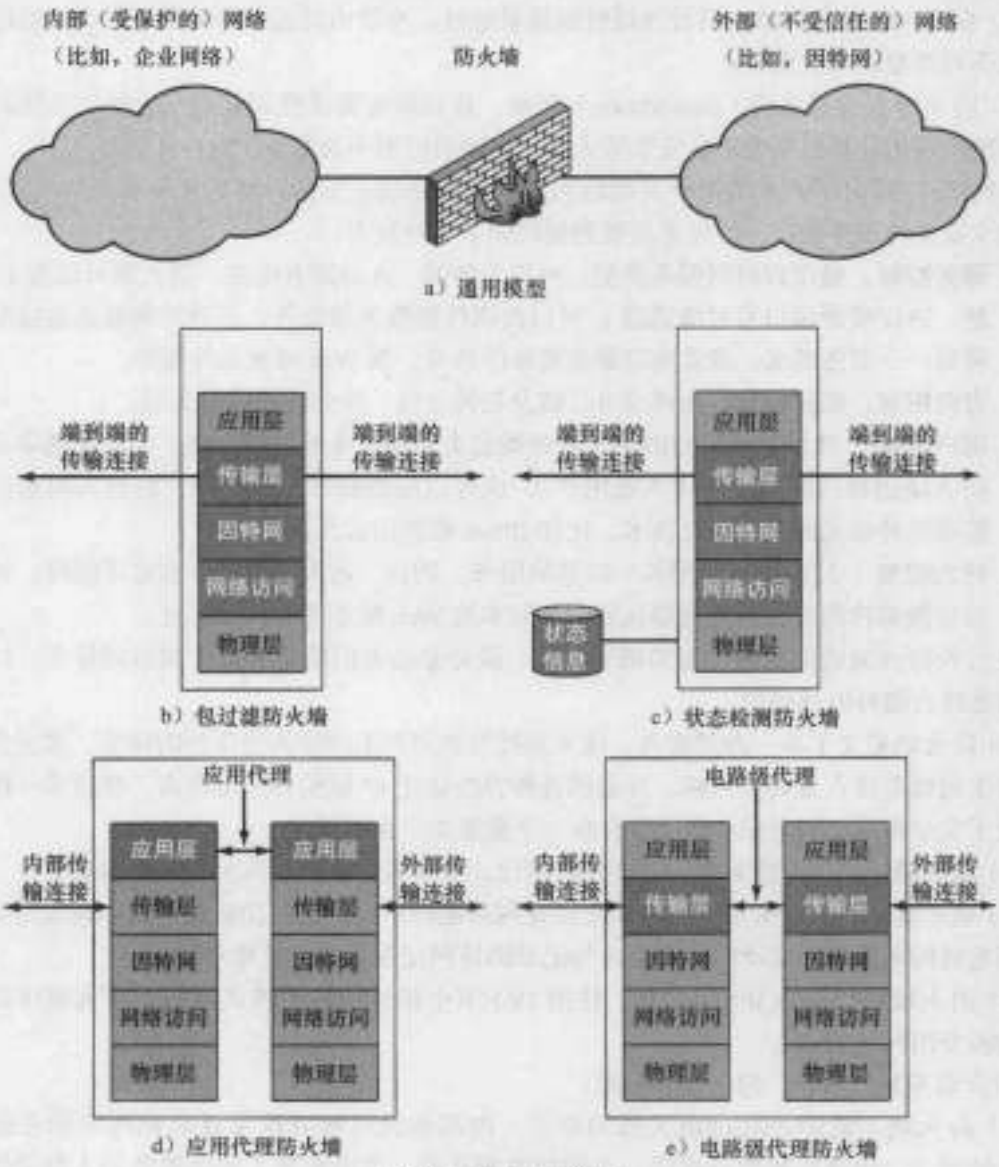


图 19-7　防火墙类型

1. 包过滤防火墙

包过滤防火墙对每个传入和传出的 IP 数据包应用一组规则，然后决定转发或丢弃该数据

包（见图 19-7b）。防火墙通常在两个方向上（进入或流出内部网络）配置过滤数据包。过滤规则基于网络数据包中包含的信息，如源地址和目的地址等。

包过滤器通常设置为基于 IP 或 TCP 报头中字段匹配的规则列表。如果有一个规则匹配，该规则被触发以确定是转发还是丢弃该数据包。如果没有任何规则匹配，则采取默认措施。两个可能的默认策略是：

- **默认丢弃策略**：没有被明确允许的都是禁止的。
- **默认转发策略**：没有被明确禁止的都是允许的。

默认丢弃策略较为保守，最初封锁一切，服务必须逐条添加上。这个策略使得用户将防火墙看做障碍，然而企业和政府组织却更倾向于这个策略。随着规则的逐步创建，用户的能见度也随之减少。默认转发策略为终端用户提高了易用性，但降低了安全性。实质上，当安全管理员认识一个新的安全威胁时，他必须对其做出反应。这一默认转发策略通常被大学这样比较开放的组织使用。

包过滤防火墙的一个优点是简单，因此数据包过滤器通常是对用户透明的，且速度非常快。[WACK02] 列出了包过滤防火墙的缺点：

- 包过滤防火墙不能阻止利用具体与应用相关的漏洞或功能的攻击。主要是因为包过滤防火墙不检查上层的数据。比如，包过滤防火墙不能阻止具体应用的命令。如果防火墙允许转发某一应用的数据流，那么该应用相关的所有功能都将被允许。
- 由于可通过包过滤防火墙的信息比较有限，所以其日志记录功能是有限的。通常情况下，数据包过滤日志包含的信息与用于访问控制决策的信息（如源地址、目的地址、流量类型等）相同。
- 大多数包过滤防火墙不支持高级用户的身份鉴别方案，这种限制再次主要是由于防火墙缺乏上层的分析功能。
- 对于利用 TCP/IP 规范和协议栈问题的攻击，比如网络层地址欺骗的问题，包过滤防火墙通常是无法防御的。许多包过滤防火墙无法检测到网络数据包的 OSI 第三层的寻址信息已被更改，这通常被入侵者利用发动欺骗攻击，绕过防火墙平台安装的安全控制器。
- 最后，由于包过滤防火墙在访问控制决策中使用的变量数目少，所以导致防火墙容易受到配置不当引起的安全违规的影响。换句话说，很容易故意地配置包过滤防火墙允许转发的流量类型、源地址和目标地址。基于组织的信息安全策略，应该避免这种情况。

2. 状态检测防火墙

传统包过滤器基于单一数据包进行过滤，并没有考虑到任何更高层的上下文信息。为了理解上下文（context）的含义，以及为什么就上下文而言传统包过滤器存在局限性，我们需要一点儿背景知识。大多数标准化的运行在 TCP 之上的应用程序采用客户机 / 服务器模型。例如，对于简单邮件传输协议（SMTP），电子邮件从一个客户端系统发送到服务器系统。客户端系统根据用户输入生成新的电子邮件消息。服务器系统接收传入的电子邮件，并将它们放在相应的用户邮箱中。SMTP 在客户端和服务器之间建立一个 TCP 连接，这个 TCP 连接服务器使用的端口号是 25，用于标识 SMTP 服务器应用程序。SMTP 客户端的 TCP 端口号由 SMTP 客户端产生，是 1024 – 65 535 之间的一个数字。

一般情况下，当应用程序使用 TCP 与远程主机建立会话时，它创建一个 TCP 连接，连

接的远程（服务器）应用程序的 TCP 端口号是一个小于 1024 的数字。本地（客户端）应用程序的 TCP 端口号是 1024 – 65 535 之间的一个数字。小于 1024 的数字是一个“众所周知”的端口号，永久地分配给特定的应用程序（例如，为服务器 SMTP 分配端口号 25）。从 1024 – 65 535 之间的数字是动态生成的，并且只在这一个 TCP 连接的生命周期有短暂的意义。

一个简单的包过滤防火墙必须允许所有这些基于 TCP 端口的入站网络流量，这创建了一个可以被未经授权的用户利用的漏洞。

状态检测防火墙不仅检测包过滤防火墙使用的相同的数据包信息，还记录 TCP 连接信息（见图 19-7c）。有些状态检测防火墙还跟踪 TCP 序列号，以防止依赖于序列号的攻击，如会话劫持。有些防火墙甚至针对一些已知协议，比如 FTP、即时消息（IM）和会话初始协议（SIP）的命令，检查有限的应用数据来识别和跟踪相关的连接。

3. 应用级网关

应用程序级网关也称为**应用程序代理**，可以作为应用级流量的中继器（图 19-7d）。用户使用 TCP/IP 应用程序连接网关，如 Telnet 或 FTP，网关要求用户提供要访问的远程主机的名称。当用户做出响应并提供一个有效的用户 ID 和身份鉴别信息时，网关连接远程主机上的应用程序，并在两个端点之间传递包含应用程序数据的 TCP 报文段。如果网关没有为特定的应用实现相应的代理代码，则该服务不被支持，不能通过防火墙转发。进一步，应用代理网关可以配置为只支持网络管理员认为可接受的某一应用程序的特定功能，而拒绝其他所有功能。

应用级网关往往比数据包过滤器更安全。应用级网关只需要仔细检查某些允许的应用，而不是试图处理在 TCP 和 IP 层允许或禁止的无数种可能的组合。此外，它很容易在应用层记录和审计所有传入的流量。

这种类型网关的一个主要缺点是，在每个连接上有额外的处理开销。实际上，在两个终端用户之间存在两个拼接的连接，而网关就处于该接续点上，它必须检查并转发两个方向上的所有流量。

4. 电路级网关

第四种类型的防火墙称为电路级网关或**电路级代理**（见图 19-7e）。它可以是一个独立的系统，或者对于某些应用通过应用层网关实现的一个特定功能。与应用级网关相比，电路级网关不允许端到端的 TCP 连接。然而，该网关设置了两个 TCP 连接，一个在网关自身和内部主机的 TCP 用户，另一个在网关自身和外部主机的 TCP 用户。一旦建立了两个连接，网关通常不检查其内容，只是从一个连接转发 TCP 段到另一个连接。安全功能主要体现在确定哪些连接被允许。

电路级网关的典型应用是系统管理员信任的内部用户，对于入站连接，网关可以配置为支持应用层或代理服务；对于出站连接，网关配置为电路级功能。在此配置中，为了实现阻止功能，网关检查进入的应用数据所带来处理方面的开销，但在输出数据时不会产生处理开销。

19.6　恶意软件防御

19.6.1　防御病毒的方法

病毒侵入的理想解决方法是预防：不允许病毒进入系统是摆在首位的。一般而言，虽然

预防措施可以减少一些病毒攻击成功的机会，但这个目标是不可能实现的。次好的办法是做到以下几点：

- **检测**：一旦发生感染，确定它已经发生并定位病毒。
- **识别**：一旦检测到病毒，识别特定的病毒感染的程序。
- **清除**：确定特定的病毒后，从被感染的程序删除所有的病毒痕迹，将其恢复到原来的状态。从所有受感染的系统删除病毒，使病毒不能进一步蔓延。

如果成功检测到病毒，但无论识别或删除都不能成功，那么另一种方法是丢弃受感染的程序，并重新装入一个干净的备份版本。

病毒与反病毒技术的发展齐头并进。早期病毒是相对简单的代码片段，相对简单的防病毒软件程序包可以识别和清除它们。然而，由于病毒军备竞赛的发展，病毒和与之对应的防病毒软件已经变得越来越复杂和先进。日益成熟的防病毒方法和产品层出不穷。在本节中，我们强调非常重要的防病毒方法之一：**行为拦截软件**。

行为拦截软件与一台主机的操作系统相结合，实时监控程序的行为来防范恶意行为。行为拦截软件在潜在的恶意行为有机会影响系统之前加以阻拦。监控行为可以包括：

- 尝试打开、查看、删除或修改文件。
- 尝试格式化磁盘驱动器和其他不可恢复的磁盘操作。
- 修改可执行文件或宏的逻辑。
- 修改重要的系统设置，如启动设置。
- 电子邮件和即时通信客户端的脚本发送可执行的内容。
- 启动网络通信。

图 19-8 说明了行为拦截的操作。行为拦截软件运行在服务器或台式计算机上，并通过由网络管理员设置的策略，让良性的行为发生，但阻止未经授权的或可疑的行为发生。模块阻止任何可疑的软件执行。拦截器把代码隔离在一个沙箱中，阻止其对各种操作系统资源及应用程序的访问。然后拦截器就会发出警报。

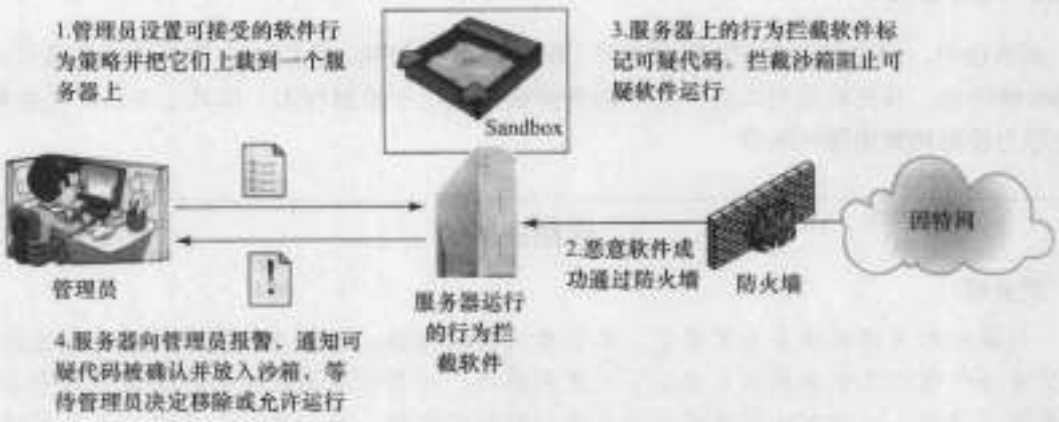


图 19-8　行为拦截软件操作过程

由于行为拦截器可以实时拦截可疑的软件，所以与已建立的防病毒检测技术，如指纹识别或启发训练相比，行为拦截器具有一定的优势。虽然有上万亿种不同的方法来混淆和重新排列病毒或蠕虫的指令，这些方法是为了逃避指纹扫描仪或启发式训练检测，但最终恶意代码必须对操作系统提出一个明确的请求。鉴于此，行为拦截器可以拦截所有这些请求，它可

以识别和阻止恶意行动，不管程序逻辑看起来是如何混乱。

行为拦截也有局限性。在所有行为被识别之前，恶意代码必须在目标机器上运行，而这在行为被检测到并阻止之前可能对目标机器造成了危害。例如，一种新的病毒在感染一个单一文件并被拦截之前，可能会在硬盘驱动器里乱置一些看似不重要的文件。即使实际的感染被拦截了，用户可能也无法找到他的文件，造成生产力的损失或者可能更糟的损失。

19.6.2　蠕虫防御

处理病毒和蠕虫的技术上有相当大的重叠。一旦蠕虫病毒驻留在一台机器上，可用防病毒软件来检测。另外，由于蠕虫病毒的传播产生相当大的网络活动，网络活动和使用情况是防范网络蠕虫的基础。

下面是防范蠕虫有效措施的要求：

- **通用性**：所采取的方法应该能够处理各种蠕虫病毒的攻击，包括多态蠕虫。
- **及时性**：该方法应迅速做出反应，以限制受感染系统的数量和从受感染的系统中产生的信息传输。
- **弹性**：该方法应该可以阻止攻击者利用逃避技术逃避蠕虫防治措施。
- **最小的拒绝服务成本**：该方法应该把防御软件的动作对系统容量或服务的影响降到最小。也就是说，为了限制蠕虫传播，防治措施不应显著扰乱正常操作。
- **透明度**：防御软件和设备不需要修改现有的（传统）操作系统、应用软件和硬件。
- **全局和局部的覆盖**：这种方法应该既能处理来自企业网络外部的攻击源，也能处理内部的攻击源。

任何现有的蠕虫防御方案似乎都不满足所有这些要求。因此，系统管理员通常需要使用多种方法来防范蠕虫的攻击。总体而言，蠕虫防御集中在识别可疑的蠕虫内容或识别蠕虫行为的流量模式。

19.6.3　Bot 防御

在本章中，讨论了许多有效防治僵尸（Bot）病毒的措施，包括 IDS 和行为拦截软件。一旦 Bot 被激活，并正在进行攻击，这些防御措施可以用于检测攻击。但其主要目标是在构建阶段尽力检测和禁用僵尸网络。

应用注解

安全层

计算机和网络的安全非常混乱，不仅有大量的威胁，而且各种需要保护的系统和技术使安全专家的工作看起来几乎是不可能完成的。分割任务或区域对找到最好的安全方法是有帮助的。一种方法是将域分为系统和网络安全组。另一种方法是确保不同网络边界区域的安全。

也许安全的第一条规则是，不管什么领域，你必须了解威胁的本质。公司在设备和人员方面花费数百万美元来保护不需要保护的事情。大多数组织认为他们自己的用户，无论是有意的或者无意的，已经成为最严重的安全问题。问题包括：下载的病毒、公司资源的不正当使用、自己的密码和别人密码的低劣控制。最近的一项实验表明，人们愿

意为了一杯免费的咖啡放弃自己的密码。但密码高手通过防火墙盗取珍贵的公司研究成果已经不是个例了。来自系统外部的坏人通常利用某种形式的拒绝服务攻击或使用公司资源试图关闭某服务或使用公司资源。另一个常见的问题很简单，就是未经授权的计算机使用你的带宽获得免费服务。

当从事系统安全时，网络管理员通常关注服务器和终端用户的计算机。这是最常见的受到损害的设备。检查所有近期的攻击，你会看到，大多数问题通过各种升级、系统补丁或个人防火墙最终得到解决。每次服务器或服务上线时，必须是最新的操作系统，而且只打开所需的通信端口，其他的端口必须禁用。

为了保证网络的安全性，我们一直在努力阻止未经授权的通信。但问题是，今天我们使用许多协议，并且开放无数的服务。因此，阻断某种类型的流量可能会导致有效的服务被打乱。因此，网络管理员不仅对初始配置，而且对协议如何操作必须有深刻的理解。这对保护网络设备免遭攻击也是很重要的，就像保护服务器一样。

通常，我们将在安全方面使用的方案和技术作为工具箱。对于网络安全分析师，最简单的方式是将这个工具箱对应到 TCP/IP 或 OSI 网络模型的层级上。TCP/IP 协议层的工具如下：

1）**物理层**：此问题与实际信号有关，相应的方法非常直接——锁门、最大限度地减少对端口的访问、选择天线的位置和使用低层加密，如 AES、3DES 或 WPA。这种类型的加密包括对第 2 层的保护。

2）**网络层**：从协议栈往上移，我们现在处理的是网络设备增加的智能，可以开始应用低层的防火墙，如基于 MAC 地址的过滤器。其他的工具包括 VLAN 和 802.1x。

3）**互联网络**：第 3 层暴露 IP 报头，所以过滤器或防火墙就可以应用到 IP 地址。其他有价值的方法包括 VPN 和网络地址转换（NAT）。

4）**传输层**：TCP 和 UDP 端口是主要点，所以现在我们的过滤器针对特定的通信流（如 HTTP 或 FTP）。过滤器有时也称为标准或扩展的访问控制列表。

5）**应用层**：这里我们可用的工具通常集中在用户密码和认证。这些都可以结合前面提到的其他工具，例如 802.1X 和 VPN。此外，还有其他形式的加密，例如应用 SSH 和 SSL。

上面仅仅是部分列表，并没有单一的方法可以针对所有的威胁。其实，如果只使用单独的技术，即使最安全的技术也可以被击败。但是，采取分层的方法，这些技术组成的防御攻势便可以成为入侵者难以克服的障碍。

无论关注的是系统还是网络，最重要的是选择与安全和可接受的使用相关的策略。对用户的教育也很重要，很多时候，用户无意地绕过安全措施而使得安全措施无效，病毒就是一个极好的例子。为了保护网络和系统资产，策略及有关最佳实施的一些基本教育任重而道远。

19.7 总结

IPSec（IP Security）是一组为 IP 提供加密、身份鉴别和密钥管理的协议。IPSec 为实现虚拟专用网（VPN）的安全提供了标准化的手段。

安全套接字层（Secure Sockets Layer，SSL）和后续的互联网标准传输层安全（Transport Layer Security，TLS），在 TCP 之上提供可靠的端到端的安全传输服务。SSL（和 TLS）提供

了两级协议栈。这些标准提供保密性、信息完整性和密钥管理。SSL 或 TLS 的一个常见用途是使用 HTTP SSL 或 TLS 为客户端计算机和 Web 站点之间提供安全连接。

对于无线局域网络（WLAN），WPA 标准包含了一套用于确保 WLAN 之间安全通信的机制。WPA 提供保密性、身份鉴别和接入控制。

入侵检测系统（IDS）是一种安全服务，监控和分析系统事件以发现试图以未经授权的方式访问系统资源的行为，并提供实时或近实时的警告。IDS 包括用来观察用户行为的数据收集组件、确定是否发生了未经授权的入侵行为的分析组件，以及用户接口。总之，入侵检测系统（IDS）用来寻找不同于合法用户所预期的用户行为。

防火墙是处于需要保护的系统或网络和因特网或其他外部接入网络之间的硬件或软件实体，用于控制双向数据流，以实施安全策略。防火墙通过监控流量内容或流量模式来实现它们的目标。

抵御恶意软件的方法随着恶意软件威胁的进化而持续发展。恶意软件防御是包含预防、检测和清除方法的组合。

研究案例 XI：云计算安全

在这个案例中，涉及的主要概念包括云计算、网络安全和网络设计。**本案例及更多资料可访问 www.pearsonhighered.com/stallings**

19.8 关键术语、复习题和练习题

关键术语

antivirus（杀毒）
behavior-blocking software（行为拦截软件）
bot（僵尸）
firewall（防火墙）
host-based IDS（基于主机的 IDS）
intrusion detection（入侵检测）
Intrusion Detection System（IDS，入侵检测系统）
IP Security（IPSec，IP 安全）
malware（恶意软件）
packet-filtering firewall（包过滤防火墙）
Secure Sockets Layer（SSL，安全套接字层）
stateful inspection firewall（状态检测防火墙）
Transport Layer Security（TLS，传输层安全性）
Wi-Fi Protected Access（WPA，WiFi 安全接入）
Worm（蠕虫病毒）

复习题

19.1 IPSec 提供哪些服务？
19.2 什么协议组成 SSL？
19.3 SSL 连接和 SSL 会话之间的区别是什么？
19.4 SSL 记录协议提供哪些服务？
19.5 IEEE 802.11i 解决了哪些安全问题？
19.6 解释异常入侵检测和特征入侵检测之间的区别。
19.7 列举防火墙的 3 个设计目标。

19.8　列举防火墙访问控制和强制执行安全策略的 4 种技术。

19.9　典型的数据包过滤路由器使用什么样的信息？

19.10　包过滤路由器的缺点有哪些？

19.11　包过滤路由器和状态检测防火墙之间的区别是什么？

19.12　行为拦截软件如何工作？

19.13　描述一些蠕虫防治策略。

练习题

19.1　在 IPSec 的 ESP 报头包括一个完整性校验值（ICV），它对所有除了 IP 头字段的 IPSec 报文的所有字段进行计算，这里 IP 头字段在传输途中不改变，在抵达终端时其值也是可预测的。为了计算源地址和目的地址，在传输过程中发生改变和字段值到达时不可预测的字段设置为 0。

a. 对于 IPv4 报头中的每个字段，指出该字段是否是不变的、可变但可预见的或者仅仅是可变的。

b. 对于 IPv6 报头，做与 a. 中同样的工作。

在每一种情况下，证明你对每个字段的判断。

19.2　在 SSL 和 TLS 中，为什么会出现一个单独的密码变化协议，而不是在握手协议中包括一个 change_cipher_spec 消息？

19.3　对于入侵检测系统（IDS），我们定义误报为对于实际正常的行为产生了 IDS 报警。漏报是指在应该产生报警的情况下没有产生报警。使用下面的图，大致描绘误报和漏报的两条曲线。



19.4　图 19-6 的两个概率密度函数的重叠区域表示潜在的误报和漏报的区域。此外，图 19-6 是理想化的情况，并不一定代表两个密度函数的相对形状的描绘。假设每 1000 个授权的用户有 1 个实际的入侵，重叠区域覆盖 1% 的授权用户和 50% 的入侵者。

a. 画出这样一组密度函数，并证明这是不合理的描述。

b. 发生在这一区域的事件是授权用户的概率是多少？请记住，所有入侵的 50% 属于这个区域。

19.5　基于主机的入侵检测工具的一个例子是 tripwire 程序，这是一个文件完整性检查工具，定期扫描系统上的文件和目录，发现任何变化并通知管理员。对每个检查文件，它使用加密校验和的保护数据库，将该值与每个文件扫描重新计算的校验和值进行比较。必须为该工具配置待检查的文件和目录列表，如果有变化，针对每个文件说明哪个变化是被允许的。例如，允许日志文件附加有新的条目，但不改变已存在的条目。使用这种工具的优点和缺点是什么？考虑确定哪些文件应该只改变很少，哪些文件可能经常发生变化，以及如何改变，哪些因为变化频繁而不能进行检查。考虑该程序的配置

和系统管理员监测所产生的响应的工作量。

19.6 可以在下列网站 http://grc.com/default.htm 上测试一台机器的脆弱性。按照 ShieldsUP！链接进行页面中间部分给出的一系列免费测试。

19.7 极小数据分段攻击是防火墙攻击的一种形式。入侵者使用 IP 数据分段选项来创建非常小的数据段，并迫使 TCP 报头信息变成一个单独的数据包片段。这种攻击的目的是规避依赖于 TCP 报头信息的过滤规则。通常情况下，一个数据包过滤器依据一个数据包的第一个片段进行过滤决策。由于第一个片段被拒绝，同时由于该数据包的所有后续片段是它的一部分，所以它们都会被过滤掉。攻击者希望过滤防火墙只检查第一个片段，剩余的片段也能通过。极小数据段攻击是可以通过执行一个规则来打败，即第一个数据包片段必须包含一个预定义的最小数量的传输头。如果第一个片段被拒绝，过滤器可以记住这个数据包，并丢弃所有后续片段。然而，IP 的本质是数据包可能会无序到达。因此，中间片段可能在初始片段被拒绝之前通过过滤器。这种情况如何处理？

19.8 在 IPv4 的数据包中，按 8 位一组，第一个片段的有效负载的大小等于：总长 –（4 × 数据包协议头长度）。如果此值小于所需的最小值（用于 TCP 的 8 个 8 位组），然后该片段与整个数据包被拒绝。推荐另一种可以达到相同结果的方法，只使用分片偏移量字段。

19.9 RFC 791，即 IPv4 协议规范，描述了一个使新的片段覆盖任何先前接收到的片段重叠部分的重组算法。鉴于这样的重组实施，攻击者可以构造一系列的数据包，其中最低的（零偏移）片段含有无害的数据（从而通过管理数据包过滤器），其中一些后续具有非零偏移的数据包将重叠 TCP 报头信息（例如目的端口），并导致它被修改。第二个数据包将通过大多数过滤器，因为它并没有零片段偏移。建议数据包过滤器对付这种攻击可使用的方法。

企业业务数据通信教学项目

许多教师认为，对于数据通信和网络概念的清晰理解而言，实施项目的研究是极其关键的。对于学生而言，没有项目，他们难以掌握一些基本概念和组件之间的交互。大量项目加强了书中引入的概念，让学生对协议和传输机制的工作原理有更深的理解，激发学生并给他们已经掌握材料的信心。

在这本教材中，我们已经尽力清晰地提出业务数据通信的概念，提供无数的家庭作业问题，以加强那些概念。许多教师希望用项目来增补这个材料。该附录提供了一些这方面的指南，描述本教材**教师资源中心**（Instructor's Resource Center，IRC）可用的支撑材料。对于教师，可通过普伦蒂斯霍尔出版社（Prentice Hall）访问本教材。支撑材料涵盖 7 种类型的项目和其他学生练习：

- 动画和动画片项目。
- 实践练习。
- Wireshark 工程。
- 研究项目。
- 安全案例学习。
- 阅读 / 报告任务。
- 写作任务。

A.1 动画和动画片项目

动画提供了强有力的工具，帮助理解网络协议的复杂机制，17 个基于 Web 的动画用于说明协议行为。每个动画允许用户逐步执行协议操作，这通过在协议交换的每个点选择下一步实现。表 A-1 按章节列出动画，单击本教材相应网站 http://williamstallings.com/businessDataComm 的旋转球可访问这些动画。

表 A-1 各章节业务数据通信动画

第 6 章 数据链路控制及复用	
交替位协议	两个协议实体之间朝一个方向传输消息的无连接协议，这是窗口长度为 1 的滑动窗口协议的简单形式
滑动窗口协议（3 列）	解释不显示终端用户的滑动窗口操作
滑动窗口协议（5 列）	解释显示终端用户的滑动窗口操作
Abracadabra 协议	面向连接的协议，允许数据使用交替位协议向任意方向发送
多路寻址	解释数据如何通过共享的通信通道在多个源和目的之间寻址
第 7 章 因特网	
启动协议（Boot Protocol）	简单无连接协议，典型地由无盘工作站使用，以发现它的因特网地址和 / 或它的 bootstrap 文件名
第 8 章 TCP/IP	
协议栈	解释数据如何通过典型协议栈流动

（续）

第8章　TCP/IP	
TCP客户/服务器	使用TCP支持客户/服务器交互
TCP端到端	使用TCP支持端到端交互
TCP慢启动（slow start）	说明使用慢启动的动态窗口管理
UDP	演示UDP操作
IP	演示IP操作
简单文件传输协议（TFTP）	演示TFTP操作
第10章　基于因特网的应用	
SMTP	仿真器处理这些主要命令：HELO、MAIL FROM、RCPT TO、DATA、QUIT
HTTP	仿真器处理这些主要命令：GET、HEAD、POST、PUT
第11章　Internet操作	
多播	解释数据如何通过网络从单个源发送到多个目的地
第13章　以太网	
CSMA/CD	说明多个系统如何使用CSMA/CD共享公用通信媒体

可以通过两种方式使用动画，分别是被动模式和主动模式。对于被动模式，学生可以在动画的每个点或多或少地点击下一步并观察给定概念或原理的解释。两种类型的任务使用主动模式：第一，给学生激发和观察动画的具体步骤，接着要求学生分析和评价结果；第二，给学生一个具体的端点，要求设计实现期望结果的步骤序列。IRC包括每个动画的任务集，加上建议的解决方案，以便于教师能够评估学生的工作。

这些动画由苏格兰斯特林大学的Iain Robin和Ken Turner开发，Paul Johnson和Kenneth Whyte做出了一定贡献。同时，斯特林大学的Larry Tan开发了动画作业。

A.2　实践练习

IRC包含Web页面，这些页面针对LAN中IP的使用简介，提供实践练习集。然而，不需要一个接一个地尝试，4个练习可比较容易地在4个分离场合执行。设计实践练习是为了帮助学生理解以太LAN和IP网络的运行。练习设计在大多数计算机上可用的简单网络命令。做所有4个练习需要大约1个小时，这些练习涉及下面主题：你自己的网络连接，局域网中的计算机，远程网络的计算机和因特网。

A.3　Wireshark工程

Wireshark以前称为Ethereal，被全世界网络安全专业人员用于发现并修复故障、分析软件和协议的开发以及教育。它具有协议分析器期望的所有标准特征，同时具有其他产品中看不到的几个特征。它的开源证书允许网络社区中有天赋的专家添加改进功能，可运行在所有常见的计算平台，包括UNIX、Linux、Windows和Mac OS X。

Wireshark是一个理想的工具，允许学生掌握协议的行为，这不仅仅是因为它的许多特征和多平台运行的能力，而且因为学生在他们随后的职业生涯中使用Wireshark。

IRC包含学生用户手册，同时专门针对业务数据通信使用建立的Wireshark项目作业集。另外，还有非常有用的视频教程，用于给学生介绍Wireshark的使用。

印第安纳大学Michael Harris最先开发了Ethereal练习和用户指南，新西兰奥塔哥理工学院Dave Bremer更新了Wireshark最新发布版的材料，他也开发了在线视频教程。

A.4　研究项目

加强来自课程的基本概念和教学生研究技巧的有效方法是分配一个研究项目。这样的研究项目涉及文献搜索以及开发商产品的 Web 搜索，研究实验室活动和标准化努力。项目可以分配给团队，对于较小的项目，可分配给个人。在任何情况下，最好是在学期早期要求某种项目建议书，给教师时间用于评估合适主题的建议书和适当的努力级别。研究项目的学生建议应包括：

- 建议书格式。
- 最终报告格式。
- 中间和最后截止日期的安排。
- 可能的项目主题列表。

学生能够从列出的主题中选择一个或者设计他们自己的项目。IRC 包括建议书和最后报告的建议格式，以及可能的研究主题列表。

A.5　安全案例研究

通过案例研究进行教学，会使学生进入主动学习状态。IRC 包括处理安全问题的案例研究，涉及的区域如下：

- 灾难恢复。
- 事件响应。
- 物理安全。
- 风险。
- 安全策略。
- 虚拟化。

每个案例研究包括学习目标、案例描述和一系列案例讨论问题，基于实际世界形势，包括描述案例的论文或报告。

所有的案例研究由北卡罗莱纳州 A&T 州立大学开发。

A.6　阅读 / 报告任务

另一种加强出自课程的基本概念和给予学生研究经验的极好方法是分配该领域的论文，让学生去阅读和分析。IRC 网站包括建议的待分配论文列表，且这些论文按章节组织。优质内容 Web 站点为每篇论文提供一份拷贝。IRC 也包含建议的任务用词。

A.7　写作任务

对于数据通信和网络之类的技术学科，写作任务对学习过程有强有力的乘数效应。跨课程写作（WAC）行动（http://wac.colostate.edu/）的支持者报告，写作任务在于促进学习的实质性收益。写作任务导致对某一主题更加详细的和完整的思考。另外，写作任务帮助学生克服用最小的个人投入仅仅学习事实和解决问题的技术，不为深入理解课程而学习一门课程的倾向。

IRC 包含许多建议的写作任务，且按章节组织。最终，教师或许发现这是他们教学课程材料及方法的非常重要的部分。我们非常感激有关这个区域的任何反馈意见和附加的写作任务的任何建议。

术 语 表

amplitude（振幅） 电压或电流波形的大小。

amplitude-shift keying（幅移键控） 一种调制，其中两个二进制值分别表示两种不同的载波频率振幅。

analog data（模拟数据） 由连续可变的物理量表示的数据，它的幅度直接与数值或函数值成比例。

analog signal（模拟信号） 在各种介质中传播的连续变化的电磁波。

analog transmission（模拟传输） 模拟信号的传输而不考虑传输的内容，传输的信号有可能被放大，但传输中不会试图从信号中恢复数据。

application layer（应用层） OSI 模型的第 7 层，该层确定了用户和系统的接口，并提供有用的面向应用的服务。

Asynchronous Transfer Mode（ATM，异步传输模式） 一种分组交换的形式，由固定大小的 53 个八位字节单元组成。该模式中没有网络层，其他许多基本功能都已经简化或取消，以提供更大的吞吐量。

asynchronous transmission（异步传输） 一种传输方式，其中每个信息字符都被单独同步，往往是通过使用开始符和结束符实现。

attenuation（衰减） 电流、电压、信号的功率在点与点传输中的大量减少。

Automatic Repeat Request（ARQ，自动重复请求） 当传输中的错误被检测到时，自动发起一个回传请求。

availability（可用性） 特定功能或应用对用户可用所占的时间比。

bandwidth（带宽） 连续频带上，两个限制频率之差。

baud（波特） 信号传输速度的单位，等于离散条件的数目，或等于每秒发生事件的数目，或等于最短信号元素传输时间的倒数。

best effort（尽力交付） 网络或互联网传输技术不能保证传输所有数据，并公平对待每一个数据包。所有的数据包是在先来先服务的基础上被转发，并没有提供基于优先级或其他因素的优先策略。

bit（位或比特） 二进制数字，0 或 1 所表示的信息的单位。

bridge（桥接器） 连接两个使用相同 LAN 协议的相似 LAN 的网络互联设备。

byte（字节） 把一串位串视作一个单位，通常位串长度为 8 位，并且能在本地字符集中用一个字符表示。

cellular network（蜂窝网络） 一种无线通信网络，网络中的固定天线被安置为六边形图案，移动站点的通信通过附近的固定天线。

Central Office（CO，中心局） 地方电话公司端接客户线路的地方，并在此定位与其他网络互联的交换设备。

checksum（检验和） 一种错误检验码，通过对待检验比特进行求和操作实现。

ciphertext（密文） 加密算法的输出；消息或数据的加密形式。

circuit switching（电路交换） 通信的方法，其中一个专用的通信路径建设在两个设备之间，并通过一个或多个中间交换节点。不同于其他分组交换，数字数据以连续的比特流形式发送。这种方法可以保证数据速率，延迟主要受传播时间限制。

client/server（客户 / 服务器） 一种常见的分布式系统，其中软件部分分为服务端任务和客户端任务。客户根据特定的协议向服务器发送请求，请求包括信息和操作，然后服务器做出响应。

cloud computing（云计算） 对一个系统的松散定义的术语，此系统提供处理能力、储存、软件和服务，往往是通过 Web 浏览器访问。通常从持有和管理这些服务的外部公司租用。

coaxial cable（同轴电缆） 一个较大直径的绝缘铜管或铜编织物和内部的导体，通常是小铜管

或铜线，两者一起组成的电缆。

codec（编解码器） 编码/解码器。将模拟数据转化为数字比特流（编码器），并将数字信号转化为模拟数据（解码器）。

code division multiple access（码分多址） 使用扩频的复用技术。

common channel signaling（公共信道指令） 将信令从一组语音或数据中选取，并放置在不同的专用于信令的信道上，从而使网络控制信号（如呼叫请求）从相关语音或数据路径中分离的技术。

Customer Premises Equipment（CPE，客户端设备） 位于客户的处所（物理位置）的电信设备，而不是位于供应商的处所或两者之间。

Cyclic Redundancy Check（CRC，循环冗余校验） 一个错误检验码，等于待检比特除以事先决定好的二进制数所得到的剩余。

database（数据库） 相互关联的数据的集合，经常带控制冗余，被组织用于多种应用场合。数据被存储以便它们可以使用不同的方案，而不用关心其内部数据结构或组织。

data gram（数据报） 一个自包含的数据包，在分组交换中独立于其他的数据包，在不依赖于早期的终端设备和网络之间的交流的情况下，它有充足的信息从始发数据终端设备（Data Terminal Equipment）路由到目的地的 DTE。

data link layer（数据链路层） OSI 模型的第 2 层。将不可靠的传输通道转换为一个可靠的通道。

decibel（dB，分贝） 两个信号相对强度的计量单位。对应的分贝数是 10 倍的信号功率之比的对数，或者 20 倍的电压之比的对数。

decryption（解密） 将加密的文字或数据（称为密文）翻译成原始的文字或数据（称为明文）。通常也称作解密。

differentiated services（差异化服务） 因特网和私有内网的功能，以支持特定服务质量要求的一组用户，这些用户在 IP 报文中拥有相同的服务标签。

digital data（数字数据） 离散值或条件表示的数据。

digital signal（数字信号） 离散或不连续的信号，如电压脉冲序列。

digital signature（数字签名） 身份验证机制，使消息的创造者附加一段检验码，作为一个签名。签名保证了消息的来源和完整性。

digital transmission（数字传输） 传输的数字数据或模拟数据已被数字化，通过使用模拟信号或数字信号实现，其中数字内容被恢复并且在中间点重复，以减少数据损伤如噪声、失真和衰减的影响。

direct sequence spread spectrum（直接序列扩频） 扩频的一种形式。利用扩频码，使原始信号中的每个比特由多个传输比特代表。

distributed database（分布式数据库） 没有被储存在一个单一的位置，而是分散在相互连接的计算机网络上。

distributed data processing（分布式数据处理） 数据处理方式，其中的部分或全部处理、储存、控制功能、输入输出功能，被分散到数据处理站之间。

domain（域） 因特网的一部分网络，由单一的实体进行行政控制，如公司或政府机构。

Domain Name System（DNS，域名系统） 目录查询服务，提供因特网上主机的名字与数字地址的映射。

downlink（下行链路） 从卫星到地球的通信链路。

electronic mail（电子邮件） 在工作站之间通过网络传播的消息形式的响应。支持电子邮件最常见的协议是简单邮件传输协议（Simple Mail Transfer Protocol）。

encryption（加密） 通过数学计算装置将明文或数据转化成难以理解的形式。

error control（差错控制） 检测和纠正差错的技术。

error detecting code（纠错码） 这种代码中，每个数据信号符合特定的构建规则，因此，这种结构在所接收信号中的偏离是可以自动检测的。

extranet（外部网） 在因特网上，公司的内部网的延伸，以允许选定特定的用户、供应商和移动工作人员能够通过万维网访问到公司的内部数据和应用。这是与公司的公网相对的，公网是可以被所有人访问的。区别有时候会被模糊，但总的来说外部网隐含着实时访问通过防火墙实现的含义。

frame（帧） 一组位（比特），含有一个或多个地址和其他协议的控制信息数据。通常是指一

个链路层（OSI第二层）的协议单元数据。

Frame Check Qequence（FCS，帧检验序列） 错误检验码。插入要被发送的数据块作为一个字段。该码用于检验接收数据时出现的错误。

frame relay（帧中继） 一个基于分组交换的形式，使用可变长度的链路层帧。没有网络层，同时许多基本的功能都已简化或取消，以提供更大的吞吐量。

frequency（频率） 周期信号每秒的振荡率。

frequency-division multiplexing（FDM，频分复用） 将传输设施划分为两个或多个通道，将设备的传输频带分为几个窄的频带，每一个频带都能被用来构成不同的信道。

frequency-shift keying（频移键控） 一种调制，其中两个二进制值表示载波频率附近的两个不同频率。

guided medium（导向介质） 一种传输介质，其中电磁波被引导沿着固体介质如铜双绞线、同轴电缆铜、光纤等进行传输。

header（头） 系统定义的控制信息，在协议数据单元中的用户数据之前。

host（主机） 任何终端系统，如PC、工作站或连接到因特网的服务器。

Internet（因特网） 基于TCP/IP协议的一个全球性的因特网络，将数以千计的公共和私人网络以及百万计的用户连接在一起。

Internet Protocol（IP，网际协议） 一个标准化的协议，在主机和路由器中执行，将一些独立的网络互连。

Internet Service Provider（ISP，因特网服务供应商） 向其他公司或个人提供访问互联网的服务。

internetworking（网络互联） 跨越多个网络设备之间的通信。

intranet（内部网） 一个企业的互联网络，提供了重要的互联网应用，特别是万维网。为了内部作用，内部网在组织内部运行，同时它可以作为一个独立的、自足的互联网存在，或可连接到互联网。一个最常见的例子是，为了公司内信息的分布，公司在一个或多个万维网服务器上使用内部网TCP/IP网络。

Local Area Network（LAN，局域网） 一个通信网络，面积较小，通常是一个单一的建筑物或建筑群，用来连接各种不同的处理设备，包括个人电脑、工作站和服务器。

local loop（本地环路） 传输路径，通常用双绞线架设在个人用户和最近的公共电信网络交换中心之间，通常也称为用户环路。

Medium Access Control（MAC，介质访问控制） 对于一个通信网络，该方法确定了哪一个站点能在任何时候访问传输介质。

modem（调制解调器） 调制器/解调器，将数字数据转化为模拟数据，使其能够在电子通信线路传播，并且将收到的模拟信号转化为数字数据。

multiplexing（复用） 在数据传输中，允许两个或多个数据源共享一个共同传输介质，使每个数据源有自己的信道。

Network Access Point（NAP，网络接入点） 在美国，一个网络接入点是几个主要因特网互联点之一，它们将所有的因特网供应商（ISP）连接在一起。

network layer（网络层） OSI模型的第三层，负责从通信网络中路由数据。

Network Service Provider（NSP，网络服务供应商） 一家向ISP提供骨干网络服务的公司，大多数网络用户通过它访问互联网。

noise（噪声） 不需要的信号，会导致发送和接收的信号失真。

octet（八位字节） 一组相邻的8位，通常当作一个单元操作。

Open Systems Interconnection（OSI）reference model（开放系统互联参考模型） 一种在合作设备之间的通信模式。它定义了一个7层体系结构的通信功能。

optical fiber（光纤） 一种玻璃薄灯丝或一种透明的材料，通过该材料，信息编码的光束可以内部全反射。

packet（分组） 一组位包括数据和控制信息。一般是指在网络层（OSI）的第三层协议数据单元。

packet switching（分组交换） 发送长消息的方法，通过一个通信网络，其中长消息被划分成短分组。对每个节点来说，整个消息收到，简要的存储，然后传递到下个节点。

parity bit（奇偶校验位） 一个检验位附加到一个二进制数组中，使得二进制数的总和，包括奇

偶校验位，总是为奇数或偶数。

period（周期） 相同特性的周期性波形，再次出现的最小时间间隔的绝对值。

periodic signal（周期信号） 若信号$f(t)$满足$f(t)=f(t+nk)$，n为所有正整数，k为一个常数，则该信号是周期信号。

phase（相） 对于一个周期信号，相位等于一个周期P内，t/P的小数部分。其中为相对于原点前进了的任意距离。通常采取最后一个从负经零到正的点作为相位的零点。

phase-shift keying（相移键控） 一种调制，用载波信号的相位偏移来表示数字的数据。

physical layer（物理层） OSI模型的第一层，关注电气、机械和定时方面的信号传输介质。

plaintext（明文） 待加密的输入或解密后的输出。

Point Of Presence（POP，接入点） 一个站点，它收集了电信设备，通常指的是ISP或电话公司的站点。一个ISP接入点是ISP网络的边界，用户发起的连接要在这里被接受和认证。因特网访问的提供者会把数个接入点分散开，以提高用户使用当地电话访问因特网的几率。

point-to point（点对点） 两个且仅有两个站点之间共享传输路径的配置模式。

port（端口） 一个传输层的地址，用于标识用户使用的传输层协议。

presentation layer（表示层） OSI模型的第6层，关系到数据的格式和显示。

protocol（协议） 一组语义和语法规则，描述了如何传输数据，特别是在网络上。低层协议定义已观察到的电气和物理标准、比特和字节排序和传输的位流中的误差检测和校正。高层协议处理格式化的数据，包括消息的语法、消息的语义、字符集和排序的消息。

protocol architecture（协议的体系结构） 软件结构实现了通信功能，通常情况下，协议的体系结构由一组分层的协议组成，每一层上有一个或多个协议。

Protocol Data Unit（PDU，协议数据单元） 一种信息，作为网络中两个对等实体间的传输单元。一个协议数据单元（PDU）通常包含控制信息和信息头报文中的地址信息。协议数据单元也可包含数据。

public-key encryption（公钥加密） 一个加密系统的形式，其中加密和解密使用两个不同的密钥，其中一个称作公钥，另一个称作私钥。

Pulse Code Modulation（PCM，脉冲编码调制） 一种调制方法，其中信号进行采样，每个采样的大小分别相对于一个固定的参考被量化且被编码转化成数字信号。

Quality Of Service（QoS，服务质量） 一组描述特定数据流中质量的参数（如数据传输率、及时性、缓冲区使用、优先级）。最小的QoS是最好交付的，其策略为公平对待每一个报文，且基于先来先服务策略。QoS能通过路由器决定传输的路径，该路径上下一个网络中的路由器请求的网络服务，以及等待从路由器转发的数据包的顺序。

router（路由器） 连接两个计算机网络的网络互联设备。它使用网际协议并假设所有的网络设备在网络层及以上使用同一个协议体系结构。

routing（路由） 决定数据单元（如帧、包、消息）传输路径的起点和终点。

Service Access Point（SAP，服务接入点） 识别协议实体服务的用户。协议实体提供一个或多个SAPs，供高层实体使用。

Service-Oriented Architecture（SOA，面向服务的体系结构） 一种商务功能的模块化，它提供更好的灵活性和可用性。SOA通常将商业软件组织成颗粒状的方式，而不是为每个部门建立整体式的应用程序，如此一来，公共的功能可以被不同的内部部门和外部商业伙伴交换使用。其中，组件越多（越细），越能提高它们的使用率。

session layer（会话层） OSI模型的第5层。管理两个通信进程或程序的逻辑连接（会话）。

signal（信号） 用来传达信息的电磁波。

signaling（信号发生） 产生电磁信号，表示模拟或数字信号，并且沿着传输介质传输。

spectrum（谱） 指的是一个绝对的、连续的频率范围。

symmetric encryption（对称加密） 加密形式的一种，使用相同的密钥进行加密和解密，也称为常规加密。

synchronous time-division multiplexing（同步时分复用） 时分复用的一种方法，其中一个共享传输线的时隙按照固定的、预先决定的基础分配到设备。

synchronous transmission（同步传输） 数据传

输方式，其中，每一比特代表的信号发生的时间与固定的时间帧相关。

Time Division Multiplexing（TDM，时分多路复用） 通过将公共通道置于多个不同的信息通道（一次一个），从而使传输设备划分为两个或多个通道。

transmission（传输） 数据的通信，通过传播和处理信号实现。在数字信号或模拟信号编码数字数据时，中继器会被使用。对于模拟信号来说，放大器也可使用。

transmission medium（传输介质） 数据站之间传送数据的物理介质。

transport layer（传输层） OSI模型的第4层，在两个端点间提供可靠、有序的数据传输。

twisted pair（双绞线） 一种传输介质，它由两根绝缘的导线扭在一起，以减少噪声。

unguided medium（无导向介质） 一种传输介质，如大气或外太空，用于无线传输。

uplink（上行链路） 从地球站点到卫星的通信链路。

virtual circuit（虚电路） 一个数据交换机制，其中逻辑链接（虚电路）在传输初始时于两站点间建立。所有的数据包通过同样的路线，并不包含完整的地址，并且按序到达。

Virtual Private Network（VPN，虚拟专用网） 在较低协议层中使用加密或认证的方式以提供不安全网络中的安全链接，通常在互联网中。VPN通常比真正专用线路上的私有网络便宜，但其依靠于两个端点具有相同的加密系统和身份认证系统。加密通常可以通过防火墙软件或路由器实现。

white noise（白噪声） 在感兴趣的频率范围内具有平坦或均匀的频谱的噪声。

wireless transmission（无线传输） 由天线发送，通过空气、真空或水的电磁传输。

World Wide Web（WWW，万维网） 联网的、图形化的超媒体系统。信息储存在服务器中，并在服务器和浏览器之间交换，在浏览器上由数页的图片和文字展示。

参考文献

缩写

ACM：计算机协会

IBM：国际商业机器公司

IEEE：电气电子工程师协会

ANDE80 Anderson, J. *Computer Security Threat Monitoring and Surveillance.* Fort Washington, PA: James P. Anderson Co., April 1980.

ANTE06 Ante, S., and Grow, B. "Meet the Hackers." *Business Week*, May 29, 2006.

BELL94 Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications Magazine*, September 1994.

BIDG06 Bidgoli, H., editor. *Handbook of Information Security.* New York: Wiley, 2006.

BIDG08a Bidgoli, H., editor. *Handbook of Computer Networks.* New York: Wiley, 2008.

BIDG08b Bidgoli, H., editor. "The Internet Fundamentals." In [BIDG08a].

BIH06 Bih, J. "Service Oriented Architecture (SOA): A New Paradigm to Implement Dynamic E-Business Solutions." *ACM Ubiquity*, August 2006. acm.org/ubiquity/views/v7i30_soa.html

BINS10 Binsalleeh, H.; Ormerod, T.; Boukhtouta, V; Sinha, P.; Youssef, A.; Debbabi, M.; and Wang, L. "On the Analysis of the Zeus Botnet Crimeware Toolkit." *Proceedings of the 8th Annual International Conference on Privacy, Security and Trust*, IEEE, September 2010.

BRAG00 Bragg, A. "Which Network Design Tool Is Right for You?" *IT Pro*, September/October 2000.

CAHN98 Cahn, R. *Wide Area Network Design.* San Francisco: Morgan-Kaufmann, 1998.

CERF74 Cerf, V., and Kahn, R. "A Protocol for Packet Network Interconnection." *IEEE Transactions on Communications*, May 1974.

CHEN11 Chen, T. M., and Abu-Nimeh, S. "Lessons from Stuxnet." *IEEE Computer*, 44(4), pp. 91–93, April 2011.

CISC07 Cisco Systems, Inc. " 802.11n: The Next Generation of Wireless Performance." Cisco White Paper, 2007. cisco.com

CLAR03 Clark, E. "Dallas County Plugs into eGovernment." *Network Magazine*, April 2003.

COHE94 Cohen, F. *A Short Course on Computer Viruses.* New York: Wiley, 1994.

CONN99 Connor, D. "Data Replication Helps Prevent Potential Problems." *Network World*, December 13, 1999.

CORM10 Cormen, T.; Leiserson, C.; Rivest, R.; and Stein, C. *Introduction to Algorithms.* Cambridge, MA: MIT Press, 2010.

CSI10 Computer Security Institute. *2010/2011 Computer Crime and Security Survey.* New York, NY: Computer Security Institute, 2010.

DEBE07 Debeasi, P. "802.11n: Beyond the Hype." *Burton Group White Paper*, July 2007. www.burtongroup.com

DWYE92 Dwyer, S., et al. "Teleradiology Using Switched Dialup Networks." *IEEE Journal on Selected Areas in Communications*, September 1992.

ELSA02 El-Sayed, M., and Jaffe, J. "A View of Telecommunications Network Evolution." *IEEE Communications Magazine*, December 2002.

ENGE80 Enger, N., and Howerton, P. *Computer Security.* New York: Amacom, 1980.

GARF02 Garfinkel, S., and Spafford, G. *Web Security, Privacy & Commerce.* Sebastapol, CA: O'Reilly, 2002.

GAUD00 Gaudin, S. "The Omega Files." *Network World*, June 26, 2000.

GOLD10 Gold, S. "Social Engineering Today: Psychology, Strategies and Tricks." *Network Security*, November 2010.

GOLI99 Golick, J. "Distributed Data Replication." *Network Magazine*, December 1999.

GUYN88 Guynes, J. "Impact of System Response Time on State Anxiety." *Communications of the ACM*, March 1988.

HAFN96 Hafner, K., and Lyon, M. *Where Wizards Stay Up Late*. New York: Simon and Schuster, 1996.

HARB92 Harbison, R. "Frame Relay: Technology for Our Time." *LAN Technology*. December 1992.

HOFF02 Hoffer, J.; Prescott, M.; and McFadden, F. *Modern Database Management*. Upper Saddle River, NJ: Prentice Hall, 2002.

HUFF06 Huff, D. "Perspective on 100 Gb/s Ethernet." *100 Gb/s Ethernet Workshop*, Optoelectronics Industry Development Association, September 2006. www.ethernetalliance.org/technology/presentations

INSI12 Insight Research Corp. *Private Line and Wavelength Services 2011–2016*. Mountain Lakes, NJ: Insight Research Corp., January 2012.

JONE09 Jones, P. "Everything over IP Transitions to IP over Everything. *Defense*, September 2009. defensesystems.com/articles/2009/09/02/Industry-Perspective.aspx?p=1

KANA11 Kanaracus, C. "Forrester: SOA is Alive and Well." *Network World*, March 23, 2011.

KING06 King, N. "E-Mail and Internet Use Policy." In [BIDG06].

KLEI75 Kleinrock, L. *Queueing Systems, Vol. I: Theory*. New York: John Wiley, 1975.

KNAU05 Knauer, B. "Voice Goes Wireless." *Cisco Packet Magazine*, Third Quarter, 2005.

LAYL04 Layland, R. "Understanding Wi-Fi Performance." *Business Communications Review*, March 2004.

LAZA07 Laxar, I. *Unified Communications: What, Why, and How?* Issue Paper, Nemertes Research, 2007.

LELA94 Leland, W.; Taqqu, M.; Willinger, W.; and Wilson, D. "On the Self-Similar Nature of Ethernet Traffic (Extended Version)." *IEEE/ACM Transactions on Networking*, February 1994.

MART88 Martin, J., and Leban, J. *Principles of Data Communicanon*. Englewood Cliffs, NJ: Prentice Hall, 1988.

MILO00 Milonas, A. "Enterprise Networking for the New Millennium." *Bell Labs Technical Journal*, January–March 2000.

NG11 Ng, J. "Global Data Traffic to Hit 60,000 Petabytes by 2116." May 12, 2011. Retrieved online from http://www.zdnet.co.uk/news/networking/2011/05/12/global-data-traffic-to-hit-60000-petabytes-by-2016-40092753/

NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. Gaithersburg, MD: National Institute of Technology, October 1995.

NOWE07 Nowell, M.; Vusirikala, V.; and Hays, R. "Overview of Requirements and Applications for 40 Gigabit and 100 Gigabit Ethernet." *Ethernet Alliance White Paper*. Beaverton, OR: Ethernet Alliance, August 2007.

OU07 Ou, G. "The Role of 802.11n in the Enterprise." *White Paper*, zdnet.com, July 2007.

PARZ06 Parziale, L., et al. *TCP/IP Tutorial and Technical Overview*. IBM Redbook GG24-3376-07, 2006. http://www.redbooks.ibm.com/abstracts/gg243376.html

PAXS94 Paxson, V., and Floyd, S. "Wide-Area Traffic: The Failure of Poisson Modeling." *Proceedings of SIGCOMM '94*, 1994.

RADC04 Radcliff, D. "What Are They Thinking?" *Network World*, March 1, 2004.

ROTH93 Rothschild, M. "Coming Soon: Internal Markets." *Forbes ASAP*, June 7, 1993.

SENS02 Sens, T. "Next Generation of Unified Communications for Enterprises." *Alcatel Telecommunications Review*, Fourth Quarter 2002.

SEVC96 Sevcik, P. "Designing a High-Performance Web Site." *Business Communications Review*, March 1996.

SEVC03 Sevcik, P. "How Fast Is Fast Enough?" *Business Communications Review*, March 2003.

SHNE84 Shneiderman, B. "Response Time and Display Rate in Human Performance with Computers." *ACM Computing Surveys*, September 1984.

SMIT88 Smith, M. "A Model of Human Communication." *IEEE Communications Magazine*, February 1988.

SMIT97 Smith, R. *Internet Cryptography*. Reading, MA: Addison-Wesley, 1997.

SRIR88 Sriram, K., and Whitt, W. "Characterizing Superposition Arrival Processes in Packet Multiplexers for Voice and Data." *IEEE Journal on Selected Areas in Communications*, September 1988.

STAL11 Stallings, W. *Data and Computer Communications, Ninth Edition*. Upper Saddle River, NJ: Prentice Hall, 2011.

STAL12 Stallings, W., and Brown L. *Computer Security: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall, 2012.

SYMA11 Symantec. "Internet Security Threat Report, Vol. 16." April 2011.

TEGE95 Teger, S. "Multimedia: From Vision to Reality." *AT&T Technical Journal*, September/October 1995.

THAD81 Thadhani, A. "Interactive User Productivity." *IBM Systems Journal*, No. 1, 1981.

TIME90 Time, Inc. *Computer Security, Understanding Computers Series*. Alexandria, VA: Time-Life Books, 1990.

VANS86 Van Slyke, R. "Computer Communication Networks." In *Handbook of Modern Electronics and Electrical Engineering*, Charles Belove, editor. New York: John Wiley and Sons, 1986.

WACK02 Wack, J.; Cutler, K.; and Pole, J. *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication SP 800-41, January 2002.

WHET96 Whetzel, J. "Integrating the World Wide Web and Database Technology." *AT&T Technical Journal*, March/April 1996.

WELK11 Welke, R.; Hirschheim, R.; and Schwarz, A. "Service-Oriented Architecture Maturity." *Computer*, February 2011.