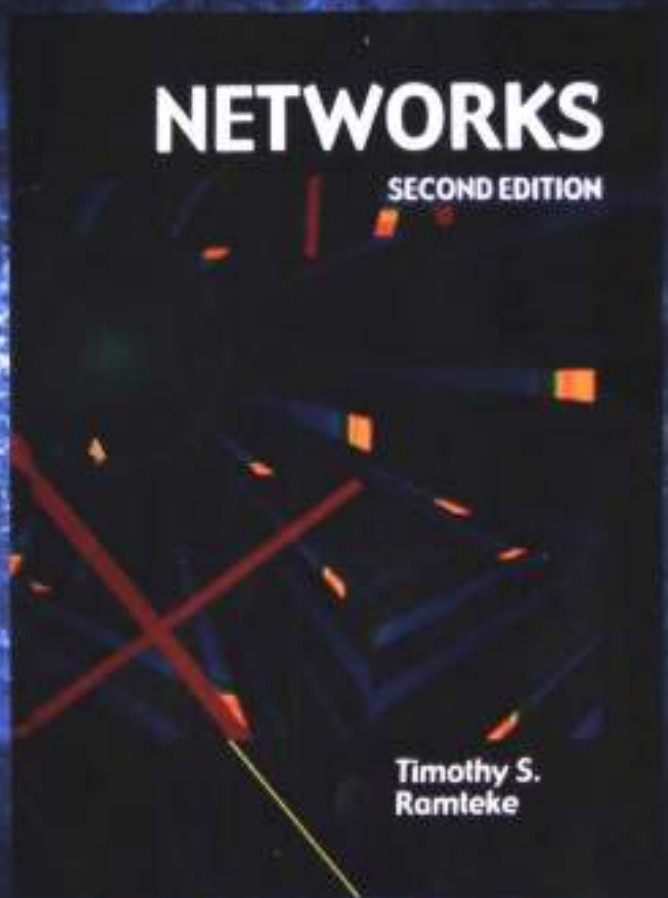
计 算 机 科 学 丛 书

原书第2版

网络

(美) Timothy S. Ramteke 著 李锦 侯春萍 赵宇 曹达仲 张宝育 等译



Networks
Second Edition

机械工业出版社
China Machine Press

本书是作者多年心血所得，他将当前的工业标准与他在先进电子通信技术方面所讲授的课程结合起来，产生了这本有深刻见解的教科书。本书分为四个独立的部分，提供了该学科的完整基础和对现代网络技术的全面评价。

- 第一部分给出了学习网络的基础知识，内容涉及从电信到数字信号以及传输设施和服务等多个方面。
- 第二部分介绍话音网络，内容涉及从信号与交换到话音处理与虚拟网络。
- 第三部分介绍广域网 (WAN) 的数据联网技术，内容涉及SNA、X.25、SS7与ISDN。
- 第四部分介绍局域网 (LAN) 的数据联网技术，内容涉及从LAN到Novell的NetWare，以及从LAN互联到TCP/IP等方面的内容。

每章全面地介绍一个主题，使其相对独立，并且各章均由业界的专家和大学教授审阅以保证行文流畅和用词准确。本书的组织结构以及各章内容相对独立的特点给读者提供了最大的灵活性，既可以顺序学习各章的内容，也可以根据个人需要选择学习。另外，各章配有一组实用的习题以使读者真正掌握书中的内容。

www.PearsonEd.com

ISBN 7-111-15017-1

9 787111 150176

HZ BOOKS
华章图书

华章网站 http://www.hzbook.com

网上购书：www.china-pub.com

北京市西城区百万庄南街1号 100037

读者服务热线：(010)68995259，68995264

读者服务信箱：hzedu@hzbook.com

ISBN 7-111-15017-1/TP・3562

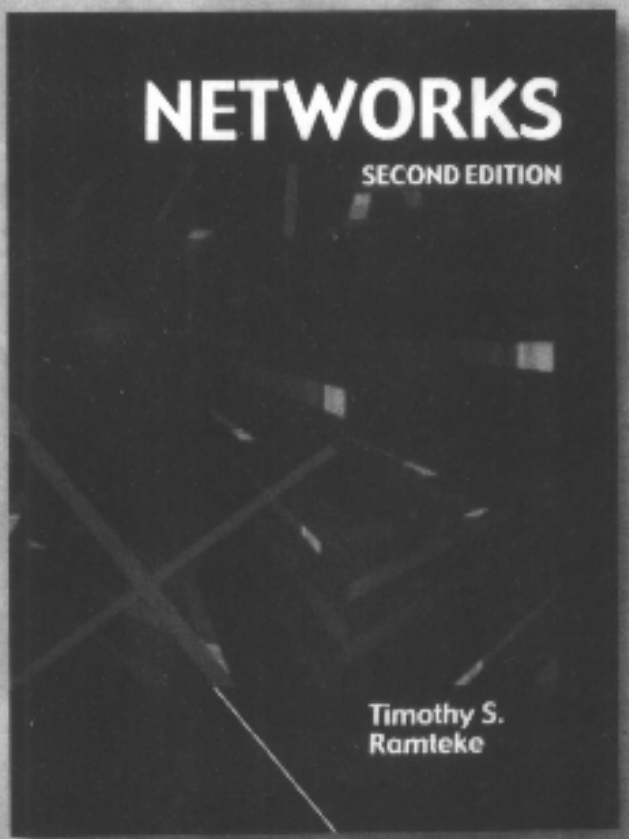
定价：59.00 元

计 算 机 科 学 丛 书

原书第2版

网络

(美) Timothy S. Ramteke 著　李锴 侯春萍 赵宇 曹达伸 张宝育 等译



Networks

Second Edition

机械工业出版社
China Machine Press

本书是讲述网络技术方面的经典教材。本书分二个层次介绍网络。第一个层次综述语音和数据网络的基本概述。第二个层次讨论以后各章将要用到的基本知识。同时，也对通信业务、局域网以及Internet上使用的TCP/IP协议等内容进行了介绍。第三个层次详细介绍组网知识，包括语音网、广域网、局域网和互联网络。本书内容翔实，分析透彻，每章都配有习题，方便教学。本书适合作为高等院校电子、通信、计算机等专业的教材或参考书，也适合工程技术人员参考。

Simplified Chinese edition copyright © 2004 by Pearson Education Asia Limited and China Machine Press.

Original English language title: *Networks , Second Edition* (ISBN 0-13-901265-6) by Timothy S. Ramteke, Copyright © 2001.

All rights reserved.

Published by arrangement with the original publisher, Pearson Education, Inc., publishing as Prentice Hall.

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

版权所有，侵权必究。

本书法律顾问 北京市展达律师事务所

本书版权登记号：图字：01-2001-3770

图书在版编目（CIP）数据

网络（原书第2版）/（美）拉姆提克（Ramteke, T. S.）著；李锵等译. -北京：机械工业出版社，2004.11

（计算机科学丛书）

书名原文：Networks, Second Edition

ISBN 7-111-15017-1

Ⅰ.网… Ⅱ.①拉… ②李… Ⅲ.计算机网络 Ⅳ.TP393

中国版本图书馆CIP数据核字（2004）第081133号

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：李云静

北京中兴印刷有限公司印刷 · 新华书店北京发行所发行

2004年11月第1版第1次印刷

787mm × 1092mm 1/16 · 37印张

印数：0 001-4 000册

定价：59.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

本社购书热线：（010）68326294

出版者的话

文艺复兴以降，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；也正是这样的传统，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，还揭橥了学术的源变，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、从业人员较少的现状下，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图文信息有限公司较早意识到“出版要为教育服务”。自1998年开始，华章公司就将工作重点放在了遴选、移译国外优秀教材上。经过几年的不懈努力，我们与Prentice Hall，Addison-Wesley，McGraw-Hill，Morgan Kaufmann等世界著名出版公司建立了良好的合作关系，从它们现有的数百种教材中甄选出Tanenbaum，Stroustrup，Kernighan，Jim Gray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、研究及庋藏。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襄助，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，有的还专诚为其书的中译本作序。迄今，“计算机科学丛书”已经出版了近百个品种，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，为进一步推广与发展打下了坚实的基础。

随着学科建设的初步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步入一个新的阶段。为此，华章公司将加大引进教材的力度，在“华章教育”的总规划之下出版三个系列的计算机教材：除“计算机科学丛书”之外，对影印版的教材，则单独开辟出“经典原版书库”；同时，引进全美通行的教学辅导书“Schaum's Outlines”系列组成“全美经典学习指导系列”。为了保证这三套丛书的权威性，同时也为了更好地为学校和老师们服务，华章公司聘请了中国科学院、北京大学、清华大学、国防科技大学、复旦大学、上海交通大学、南京大学、浙江大学、中国科技大学、哈尔滨工业大学、西安交通大学、中国人民大学、北京航空航天大学、北京邮电大学、中山大学、解放军理工大学、郑州大学、湖北工学院、中国国家信息安全测评认证中心等国内重点大学和科研机构在计算机的各个领域的著名学者组成“专家指导委员会”，为我们提供选题意见和出版监督。

这三套丛书是响应教育部提出的使用外版教材的号召，为国内高校的计算机及相关专业

的教学度身订造的。其中许多教材均已为M. I. T.，Stanford，U.C. Berkeley，C. M. U. 等世界名牌大学所采用。不仅涵盖了程序设计、数据结构、操作系统、计算机体系结构、数据库、编译原理、软件工程、图形学、通信与网络、离散数学等国内大学计算机专业普遍开设的核心课程，而且各具特色——有的出自语言设计者之手、有的历经三十年而不衰、有的已被全世界的几百所高校采用。在这些圆熟通博的名师大作的指引之下，读者必将在计算机科学的宫殿中由登堂而入室。

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，但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。教材的出版只是我们的后续服务的起点。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：

电子邮件：hzedu@hzbook.com
联系电话：（010）68995264
联系地址：北京市西城区百万庄南街1号
邮政编码：100037

专家指导委员会

（按姓氏笔画顺序）

尤晋元	王　珊	冯博琴	史忠植	史美林
石教英	吕　建	孙玉芳	吴世忠	吴时霖
张立昂	李伟琴	李师贤	李建中	杨冬青
邵维忠	陆丽娜	陆鑫达	陈向群	周伯生
周立柱	周克定	周傲英	孟小峰	岳丽华
范　明	郑国梁	施伯乐	钟玉琢	唐世渭
袁崇义	高传善	梅　宏	程　旭	程时端
谢希仁	裘宗燕	戴　葵		

秘　书　组

武卫东　　温莉芳　　刘　江　　杨海玲

译 者 序

计算机网络是计算机技术与通信技术相互结合的产物，是信息技术中的一门交叉学科。计算机网络在20世纪90年代得到了迅猛的发展，渗透到了各个领域、各种行业，深刻地影响着人们的生活方式和思维方式。随着信息化社会和网络技术的不断发展，网络应用不断推进，在各个领域尤其是电信领域取得了令人瞩目的成就。网络不仅仅简单地将众多的计算机连接起来，更重要的是它从根本上改变了人们生活、工作、学习、交流的方式以及习惯。因此，学习网络方面的基本知识和理论，并且学会使用计算机网络是21世纪工作、学习、生活所必需的基本技能。

本书作者Timothy S. Ramteke花费数年时间完成了这部关于语音与数据网络技术的著作，他把当前的流行工业标准与其所讲授的有关先进电子通信技术方面的课程结合起来，产生了这本有深刻见解的教科书。本书分为四个独立的部分，第一部分介绍了学习网络的基础知识，内容涉及从电信到数字信号直至传输设备和服务等多个方面。第二部分介绍语音网络，包括信令、交换、语音处理与虚拟网络等内容。第三部分介绍广域网（WAN）数据联网技术，内容涉及SNA、X.25、SS7与ISDN。第四部分介绍局域网（LAN）数据联网技术，涉及LAN网络、Novell网络，以及LAN互联和TCP/IP技术等方面的内容。本书的每一章都主题鲜明，内容相对独立；这为读者阅读本书提供了最大的灵活性。因此，读者既可以顺序学习各章的内容，也可以根据个人需要有选择地学习。此外，本书的每章都配有一组实用的习题，用来检查读者对这章内容的掌握情况。本书适合于作为高等院校电子、信息、通信、计算机等专业的高年级本科生或低年级研究生相关课程的教材。它是一本很好的相关领域的教学参考书，同时也是技术方面的经典著作。

本书的第1章、第2章由赵宇负责组织翻译并校对，第3章至第10章由侯春萍负责组织翻译并校对，第11章至第15章和第19章至第24章由李锵负责组织翻译并校对，第16章至第18章由曹达仲负责组织翻译并校对，第25章至第27章由张宝育负责组织翻译并校对。参加本书翻译工作的还有张华、金婕、杨育全、陈静、王劲松、侯方西、宋胜辉、赵慧、陈瑞琪、张育全、王丽娟、李鸿明、刘丽、靳军莉、张桐童、徐涛、王飞、李响、王彬彬、朱宁等，在此表示衷心的感谢。

由于译者的水平有限，译文中难免有不妥乃至错误之处，敬请读者指正。

前　言

本书分三个层次。第一个层次包括第1章和第2章，是语音和数据网络的综述。从第3章到第8章是本书的第二个层次，这部分内容讨论了以后各章将要用到的一些基本知识。同时，也对通信业务、局域网以及Internet上使用的TCP/IP协议等内容进行了介绍。第9章到第27章是本书的最后一个层次，这部分详细地介绍了组网知识。由于这个层次的内容比较多，因此又被分成三部分：语音网、广域网、局域网和互联网络。

本书第2版的结构与第1版差不多，只是将第1版前四章的内容扩展成了八章。前八章介绍了网络协议的优点、用途和基本结构，但并没有就具体的网络协议比特、字节、字段、帧结构等细节展开讨论。而是将大部分具体内容放到了第9章到第27章中进行讨论。对于刚刚接触网络的初学者来说，大致地了解无疑是最重要的，细节尚在其次。一旦他们对协议的用途产生了兴趣，就会去研究协议的具体实现。

图1是本书的组织结构图。在学习的阅读顺序上，本书具有很大的灵活性。可以在学完前四章之后就学习第6章，因为第6章的内容和第7章或以后各章没有什么联系。此外，建议在学习第17章之前，先学习第1章到第5章以及第16章的内容。本书大致是按照各种技术随时间演进的先后顺序组织的，如果可能，应该尽量按这个顺序来阅读。当然，这不是必需的。由于语音网络和数据网络的相互渗透，因此书中与这两种网络相关的内容可能会相互重叠。

在整本书中，我一直尽量避免使用“在写作本书的时候”之类的短语，因为大家都知道，技术和解决方案总是在不断地变化。

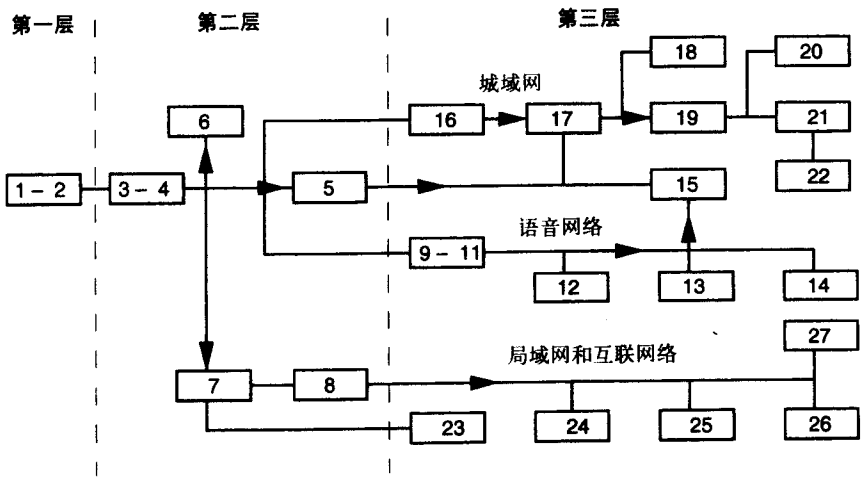


图1　学习各章节的参考顺序

在这里，我首先要感谢第1版的技术编辑们。对于他们的大力协助，我深表谢意。他们是Wally Bartus、Eric Harvie、Joseph Mastriani、David Drosdick、Dan Lawler、Ronald Mitchell、Robert Przybysz、Peter DePrima、Terry Henry、Al Hukle、Michael Zboray、Gary

Morgenstern、Rick Wallerstein、Diane Pozefsky、Atul Kapoor、Peter Locke、Robert Fishel、Ted Haller、Annabelle Soper、Steve Silva、Radia Perlman、Tony Eldridge、Rory Pope和Thomas P. Brisco。

尽管我是一名教师，但每位教师又必须在某个时段内做学生，我当然也不会例外。在这个版本的修订过程中，我得到了许多“神奇”教师的帮助。他们是：研究帧中继和基础网络的Alan Y. Schaevitz、研究xDSL和其他接入技术的Michael F. Finneran、研究CDMA的Darryl Schick以及研究VPN的Gary Kessler。Bill Yodlowsky、Jay Pear和John Goswick曾经都是我的学生，但是在Linux和Windows 98组网方面，他们又是我的老师。Bhupinder Sran也提供了不少帮助。同时，还要感谢我的家人Jonathan、Sarah、Daniel以及Beth。由于英语不是我的母语，我还要特别感谢Bret Workman所做的详细校正。

我希望你能很愉快地阅读和学习这本书，就像我写它的时候一样。我发现了很多有趣的东西，假以时日，相信你也会有大量的发现。

目　录

出版者的话
专家指导委员会
译者序
前言

第一部分　联网基础知识

第1章　欢迎学习电信学……1
1.1　历史回顾……1
1.1.1　19世纪……1
1.1.2　独立电话公司……2
1.1.3　拆分的道路……2
1.2　呼叫处理（1984—1996）……3
1.2.1　本地接入和传送区（LATA）、局间通信公司（IXC）和本地电话公司（LEC）……3
1.2.2　术语定义和呼叫路由选择……5
1.3　进一步了解PSTN……6
1.3.1　蜂窝系统……6
1.3.2　七号信令系统……7
1.3.3　个人通信系统（PCS）……9
1.4　Internet……9
1.4.1　数据网……9
1.4.2　TCP/IP协议簇……10
1.4.3　客户/服务器模型……10
1.4.4　发送e-mail……11
1.4.5　WWW……11
1.5　1984年以来业界的发展……12
1.5.1　竞争接入提供商（CAP）……12
1.5.2　通信代理商和Internet服务提供商（ISP）……12
1.5.3　1996年的电信法案……13
1.5.4　兼并大潮……13
1.5.5　专用集成电路（ASIC）……14
1.6　标准……15
1.6.1　开放系统……15
1.6.2　标准化组织……15
习题……17
第2章　数据组网基础……19
2.1　什么是网络……19
2.2　为什么联网……20
2.3　网络体系结构……21
2.3.1　什么是网络体系结构……21
2.3.2　另一个类比……23
2.3.3　网络体系结构的例子……23
2.4　OSI……24
2.4.1　OSI概述……24
2.4.2　分层处理……25
2.4.3　通信子网……27
2.4.4　一个子网的类比……28
2.4.5　OSI子网……29
2.4.6　各层的描述……29
2.5　分组交换网络……31
2.5.1　分组交换网络的工作过程……31
2.5.2　虚电路……32
2.5.3　分组交换机的职责……33
2.6　数据报交付网络……34
2.7　网络服务……35
习题……37
第3章　模拟信号和数字信号……40
3.1　信号类型……40
3.2　直流电路……40
3.2.1　欧姆定律……40
3.2.2　数字信号……42
3.2.3　幻象供电……43
3.3　模拟信号……43
3.3.1　调制……43
3.3.2　电容器和电感器……44
3.3.3　低通滤波器……45

3.3.4 带宽 ……45
3.3.5 公制单位前缀 ……46
3.4 功率 ……46
3.4.1 *P=VI* ……46
3.4.2 分贝 ……47
3.5 同步 ……48
3.5.1 三种类型的同步 ……48
3.5.2 异步通信 ……48
3.5.3 同步通信 ……49
3.5.4 STM与ATM ……49
3.5.5 定时 ……49
3.6 回波抵消 ……50
3.7 编码和编址 ……50
3.8 多路复用 ……52
3.8.1 频分复用（FDM） ……53
3.8.2 时分复用（TDM） ……54
3.8.3 波分复用 ……55
3.8.4 反复用 ……55
3.9 信息编码 ……55
3.9.1 传输信息的方法 ……55
3.9.2 将语音信号转换成数字信号的优点 …58
3.9.3 脉冲编码调制（PCM） ……60
3.9.4 视频压缩 ……61
习题 ……62
第4章 传输系统 ……64
4.1 简介 ……64
4.2 双绞线 ……64
4.2.1 双绞线的局限性 ……64
4.2.2 双绞线标准 ……65
4.3 同轴电缆 ……66
4.3.1 基带同轴电缆 ……66
4.3.2 宽带同轴电缆 ……66
4.3.3 波导管 ……66
4.4 光纤 ……67
4.4.1 概述 ……67
4.4.2 光纤的结构 ……67
4.4.3 光纤的分类 ……68
4.4.4 如何利用更多的带宽 ……69
4.4.5 海底光缆 ……70
4.4.6 如何降低光纤成本 ……70
4.5 短距通信解决方案 ……71
4.5.1 微波无线电 ……71
4.5.2 红外线 ……71
4.6 卫星通信 ……72
4.6.1 概述 ……72
4.6.2 甚小口径地球站 ……73
4.6.3 无中心站的VSAT系统 ……74
4.7 建筑物的布线 ……74
4.7.1 安装配线架的必要性 ……74
4.7.2 建筑物布线的五个区域 ……75
4.7.3 数字接入和交叉连接系统 ……76
习题 ……76
第5章 商业网络服务 ……79
5.1 服务类型 ……79
5.1.1 交换接入 ……79
5.1.2 专用接入 ……80
5.1.3 专用网络 ……81
5.1.4 虚拟专用网 ……81
5.2 中继线类型 ……83
5.2.1 CO中继线 ……83
5.2.2 DID中继线 ……83
5.2.3 FX中继线 ……84
5.2.4 OPX链路 ……84
5.3 传输载波服务 ……84
5.3.1 T1载波系统 ……84
5.3.2 同步光网络（SONET） ……87
5.3.3 综合业务数字网（ISDN） ……88
5.3.4 带宽按需分配的数字拨号业务 ……90
5.3.5 X.25 ……92
5.3.6 帧中继 ……93
5.3.7 ATM ……95
5.4 虚拟服务 ……98
5.4.1 800服务 ……98
5.4.2 虚拟专用网（VPN） ……98
习题 ……99
第6章 住宅网络服务 ……101
6.1 56K调制解调器 ……101
6.2 有线电视和电缆调制解调器 ……103

6.3 数字用户线（xDSL）……105
6.3.1 使用xDSL的可能性……105
6.3.2 xDSL面临的挑战……106
6.3.3 高速数字用户线（HDSL）……107
6.3.4 ISDN数字用户线（IDSL）……108
6.3.5 非对称数字用户线（ADSL）……108
6.3.6 ADSL采用的调制技术……110
习题……110
第7章 局域网的基本概念……112
7.1 简介……112
7.1.1 局域网（LAN）的诞生……112
7.1.2 局域网与电话网的比较……112
7.2 拓扑结构……113
7.2.1 星型拓扑结构……113
7.2.2 总线型拓扑结构……114
7.2.3 环型拓扑结构……115
7.3 访问协议……115
7.3.1 带冲突检测的载波侦听多路访问协议（CSMA/CD）……115
7.3.2 令牌传送协议……116
7.4 局域网的类型……117
7.5 几种基本的以太网……119
7.5.1 10Base5……119
7.5.2 10Base2……120
7.5.3 10BaseT……121
7.6 以太网的帧结构……128
7.7 扩展局域网的范围……129
7.7.1 中继器……129
7.7.2 网桥……130
7.7.3 路由器……132
7.7.4 交换机……135
习题……138
第8章 TCP/IP的基本概念……141
8.1 计数系统……141
8.2 地址解析协议（ARP）……143
8.2.1 一个办公室的例子……143
8.2.2 应用在以太网上的ARP协议……144
8.3 IP地址……145
8.3.1 点分十进制表示法……145
8.3.2 IP地址的分配……145
8.3.3 地址的分类……147
8.4 子网……148
8.4.1 划分子网的原因……148
8.4.2 划分子网的方法……149
8.4.3 划分子网：例子1……150
8.4.4 地址的损失……151
8.4.5 划分子网：例子2……152
8.5 数据包和帧的分析……154
8.5.1 简介……154
8.5.2 协议分析器……154
8.5.3 解析各层协议……155
8.5.4 举例……157
8.6 TCP/IP层……158
8.6.1 概述……158
8.6.2 网络接入层……159
8.6.3 网际协议……160
8.6.4 UDP……161
8.6.5 TCP……161
8.6.6 ICMP……162
习题……163

第二部分 语音网

第9章 信令……167
9.1 什么是信令……167
9.2 一个呼叫的连接过程……167
9.2.1 发起呼叫……167
9.2.2 呼叫路由……168
9.2.3 应答监视……168
9.2.4 拆线和呼叫清除……168
9.3 信令格式的分类……168
9.4 信令延时和局间信令……169
9.4.1 单条中继线信令……169
9.4.2 公共信道局间信令……169
9.4.3 CCIS的优点……170
9.5 地址信令的类型……170
9.5.1 拨号脉冲……170
9.5.2 双音多频信令……171
9.5.3 多频信令……171

9.6 提供监视功能的信令类型 ……172
9.6.1 单频信令 ……172
9.6.2 环路启动信令 ……172
9.6.3 接地启动信令的优点 ……173
9.6.4 接地启动信令的操作 ……174
9.7 数字载波系统 ……175
9.7.1 夺位信令与无干扰信道信令 ……175
9.7.2 公共信道信令 ……176
9.7.3 带外信令和带内信令 ……176
9.8 信令接口 ……176
9.8.1 四线端接装置 ……176
9.8.2 接收和发送（E&M）信令接口 ……177
9.8.3 数字信令接口 ……178
习题 ……179
第10章 交换 ……180
10.1 交换的基本原理 ……180
10.1.1 为什么要交换 ……180
10.1.2 交换机的组成 ……181
10.1.3 空分交换和时分交换 ……181
10.1.4 产生阻塞的原因 ……182
10.1.5 交换机更细致的分类 ……182
10.2 控制方式 ……183
10.2.1 直接逐级控制 ……183
10.2.2 公共控制 ……184
10.2.3 存储程序控制 ……184
10.3 数字交换 ……185
10.3.1 时分环 ……185
10.3.2 时分总线 ……186
10.3.3 时－空－时交换 ……186
10.3.4 矩阵交换机 ……187
10.4 高级交换的概念 ……188
10.4.1 再论时分交换和空分交换 ……188
10.4.2 单路径结构 ……189
10.4.3 多路径结构 ……189
10.4.4 缓冲和争用解决方案 ……190
习题 ……190
第11章 PSTN ……192
11.1 背景 ……192
11.2 本地电话网 ……193
11.2.1 配线网络设备 ……193
11.2.2 CO的内部结构 ……194
11.2.3 局间信令使用SS7 ……195
11.3 AT&T网络 ……197
11.3.1 概述 ……197
11.3.2 北美网络 ……197
11.3.3 信令网上的呼叫处理 ……198
11.3.4 RTNR（实时网络路由） ……199
11.3.5 NCP ……200
11.4 MCI网络 ……200
11.4.1 物理层 ……200
11.4.2 逻辑层 ……201
11.4.3 管理层 ……201
11.5 Sprint网络 ……202
11.6 基于SS7的虚拟网络介绍 ……203
11.6.1 虚拟网络的用途 ……203
11.6.2 虚拟网络的运营 ……205
11.7 虚拟网络的优势 ……205
11.7.1 易于管理 ……205
11.7.2 公司范围的拨入方案 ……205
11.7.3 更好的性价比 ……206
11.7.4 其他优势 ……206
11.8 接入类型 ……206
11.8.1 交换接入 ……206
11.8.2 专用接入 ……209
11.8.3 远程接入 ……209
习题 ……210
第12章 无线通信与CDMA ……212
12.1 AMPS ……212
12.1.1 概述 ……212
12.1.2 AMPS的优势 ……213
12.1.3 使用不规则小区形状的理由 ……214
12.1.4 小区信道的分配 ……214
12.1.5 频率复用 ……214
12.1.6 操作 ……215
12.1.7 越区切换 ……216
12.1.8 小区分裂 ……216
12.2 现代无线系统 ……217
12.2.1 无线系统模型 ……217

12.2.2 基本无线原理 ……218
12.2.3 无线频谱 ……219
12.2.4 固定无线系统 ……219
12.2.5 PCS ……220
12.3 数字无线系统 ……221
12.3.1 欧洲的GSM ……221
12.3.2 北美的IS-54/136 ……221
12.3.3 欧洲的DECT ……222
12.4 高通的CDMA(TIA/EIA-95) ……223
12.4.1 扩频通信 ……223
12.4.2 基本CDMA ……223
12.5 差错处理 ……225
12.5.1 CRC ……225
12.5.2 卷积码编码器 ……225
12.5.3 维比特译码器 ……228
12.5.4 块交织 ……229
12.6 CDMA与SSMA ……230
12.6.1 一些术语 ……230
12.6.2 Walsh码 ……230
12.6.3 PN码 ……231
12.6.4 PN和Walsh码层 ……232
12.7 CDMA业务信道 ……233
12.8 CDMA的总结 ……235
习题 ……236
第13章 专用交换网络 ……238
13.1 背景介绍 ……238
13.2 Centrex ……238
13.2.1 什么是Centrex ……238
13.2.2 Centrex的优点 ……239
13.2.3 中心局本地局域网(CO-LAN) ……240
13.3 按键系统 ……242
13.3.1 1A2系统 ……242
13.3.2 电子按键系统(EKS) ……243
13.4 其他小型语音系统 ……244
13.4.1 混合系统 ……244
13.4.2 无KSU的系统 ……244
13.5 PBX功能举例 ……244
13.5.1 电话台的功能 ……244
13.5.2 话务员操作控制台的功能 ……245
13.5.3 系统的功能 ……245
13.6 朗讯公司的DEFINITY ……245
13.6.1 电话设备 ……245
13.6.2 站点链路 ……246
13.6.3 DEFINITY 框图概述 ……246
13.6.4 配置 ……247
13.6.5 DEFINITY结构 ……247
13.7 级联专用线路网络 ……249
13.8 专用网络 ……250
13.9 ARS（自动路由选择） ……251
13.9.1 ARS的决策过程 ……251
13.9.2 一个实例 ……251
13.10 网络路由 ……252
习题 ……254
第14章 语音处理、ACD和CTI ……256
14.1 概述 ……256
14.2 提供话音的方法 ……256
14.2.1 录制话音 ……256
14.2.2 文字语音转换 ……257
14.3 录音文字信息系统/计划 ……258
14.4 语音识别 ……258
14.5 语音邮件 ……259
14.5.1 为何需要语音邮件 ……259
14.5.2 VM系统的大小 ……260
14.6 自动值机员（AA） ……260
14.6.1 AA实例 ……261
14.6.2 AA的优点 ……261
14.6.3 AA的特色功能 ……262
14.7 呼叫分配系统介绍 ……262
14.7.1 如何使用ACD ……262
14.7.2 UCD与ACD的比较 ……263
14.7.3 呼叫序列发生器 ……263
14.7.4 呼叫中心 ……263
14.8 呼出电话销售 ……264
14.9 为何使用ACD ……265
14.10 门类 ……265
14.11 时间线 ……266
14.12 ACD的特色功能 ……267
14.13 ACD网络 ……267

14.14 交互式语音响应（IVR）系统 ……269
14.15 CTI（计算机电话集成）……270
14.15.1 什么是CTI ……270
14.15.2 标准API ……270
14.15.3 CTI与网站 ……272
习题 ……272
第15章 T1网络 ……274
15.1 优点 ……274
15.1.1 节省运营费用 ……274
15.1.2 简化 ……274
15.1.3 可靠性 ……275
15.1.4 网络控制 ……276
15.2 T1信号传输 ……276
15.2.1 各种介质上的DS-1 ……276
15.2.2 双极性格式 ……277
15.2.3 B8ZS技术 ……277
15.3 帧类型 ……278
15.3.1 D4帧结构 ……278
15.3.2 超帧（SF） ……279
15.3.3 扩展超帧（ESF） ……280
15.3.4 其他的帧格式 ……281
15.4 网络接口 ……282
15.4.1 客户端 ……282
15.4.2 电信公司端 ……283
15.5 T1网络的交换 ……283
15.5.1 信道处理单元、多路复用器和交换机 ……283
15.5.2 中间节点交换 ……283
15.5.3 使用单链路多路复用器的D/I（卸载插入方式） ……284
15.5.4 添加-卸载 ……285
15.5.5 DACS(数字接入和交叉连接系统) …285
15.5.6 专有网络与DACS ……287
15.5.7 CCR ……287
15.6 网络设计案例研究 ……288
15.6.1 问题陈述 ……288
15.6.2 分析 ……289
15.6.3 设计 ……291
15.6.4 补充的设计问题 ……293
习题 ……293

第三部分 广域网

第16章 SNA（系统网络体系结构）……295
16.1 SNA环境 ……295
16.1.1 SNA的初始应用 ……295
16.1.2 主机的远程处理 ……296
16.2 SNA的硬件 ……296
16.2.1 主机及其I/O通道 ……297
16.2.2 FEP ……297
16.2.3 集群控制器 ……298
16.2.4 连接LAN ……298
16.2.5 AS/400与本地、远端设备 ……299
16.3 NAU与会话 ……299
16.3.1 定义NAU ……299
16.3.2 LU ……299
16.3.3 PU ……300
16.3.4 SSCP、域和寻址 ……300
16.3.5 会话 ……302
16.4 SNA体系结构 ……303
16.4.1 SNA层 ……303
16.4.2 SNA的交换单元 ……304
16.4.3 LU协议子集 ……304
16.5 SDLC ……304
16.5.1 标志字段和地址字段 ……304
16.5.2 控制字段 ……305
16.5.3 SDLC传输交换的一个例子 ……307
16.6 路径控制层 ……308
16.6.1 子域间路由 ……308
16.6.2 端到端路径控制路由 ……310
16.7 记录链锁、调步和分段 ……311
16.7.1 记录链锁 ……311
16.7.2 会话调步 ……312
16.7.3 分段 ……312
16.8 APPC或LU6.2 ……312
16.8.1 简介 ……312
16.8.2 LEN ……313
16.8.3 APPC体系结构 ……314

16.8.4 一个APPC的对话实例 ……315
16.9 APPN ……317
习题 ……318
第17章 X.25 ……320
17.1 发展 ……320
17.1.1 起源 ……320
17.1.2 数据报的概念 ……320
17.1.3 分组的概念 ……321
17.2 目的 ……321
17.3 拨号线路、租用线路与分组网络 ……322
17.4 公共数据网络（PDN） ……323
17.5 分组交换网络的运行 ……323
17.5.1 什么是分组交换 ……323
17.5.2 与X.25相关的协议 ……325
17.6 LAP/B: X.25的数据链路层 ……326
17.7 X.25的网络层 ……327
17.7.1 通过层的通信机制 ……327
17.7.2 永久虚电路和交换虚电路 ……328
17.8 分组的类型 ……328
17.8.1 分组头 ……328
17.8.2 监控分组 ……330
17.9 X.25的特点与功能 ……331
17.10 X.25网络与IBM网络的互联 ……332
17.10.1 在X.25上实现SNA的软件方法 ……332
17.10.2 硬件方法 ……333
17.10.3 XI方法 ……334
17.10.4 在BSC网络使用X.25的优势 ……334
习题 ……335
第18章 SS7 ……337
18.1 概述 ……337
18.1.1 优点 ……337
18.1.2 历史 ……338
18.2 拓扑结构 ……338
18.2.1 节点类型 ……338
18.2.2 链路类型 ……339
18.2.3 AIN ……340
18.3 SS7协议结构 ……341
18.3.1 与X.25的比较 ……341
18.3.2 结构分层 ……341
18.4 信令单元 ……343
18.4.1 SU字段 ……343
18.4.2 SU传输交换的实例 ……344
18.5 MTP第三层 ……345
18.6 SCCP ……346
18.6.1 SCCP的子层 ……346
18.6.2 0层业务举例 ……346
18.7 TCAP ……348
18.7.1 用户请求层 ……348
18.7.2 TCAP的两个子层 ……348
18.7.3 CSL子层 ……348
18.7.4 TSL子层 ……349
18.8 ISUP ……350
18.8.1 承载与补充业务 ……351
18.8.2 ISUP消息 ……351
18.8.3 ISUP信令连接 ……352
18.8.4 ISUP信令方式 ……353
18.8.5 呼叫的建立与释放 ……353
习题 ……355
第19章 ISDN ……357
19.1 定义 ……357
19.1.1 接入接口 ……357
19.1.2 功能设备和参考点 ……357
19.2 电信业务 ……359
19.2.1 业务类型及其属性 ……359
19.2.2 信息传输属性 ……360
19.2.3 接入属性 ……361
19.2.4 用户终端业务属性 ……361
19.3 BRI的物理层 ……361
19.3.1 概述 ……361
19.3.2 ANSI的U参考点 ……362
19.3.3 ITU的S/T参考点 ……363
19.3.4 S/T参考点上成帧 ……366
19.3.5 D信道接入控制 ……367
19.4 PRI物理层 ……369
19.5 数据链路层 ……369
19.5.1 为什么采用LAPD ……369
19.5.2 基本帧格式 ……370

19.5.3 DLCI字段 ……371
19.6 网络层 ……372
习题 ……373
第20章 SONET ……374
20.1 SONET: 同步光网络 ……374
20.2 SONET与T3相比的优点 ……374
20.3 SONET的速率与设备 ……375
20.4 SONET传输结构 ……376
20.5 映射 ……378
20.6 回顾 ……379
20.7 SONET环 ……380
习题 ……382
第21章 帧中继 ……383
21.1 交换网络概述 ……383
21.1.1 X.25、帧中继和ATM中的虚电路 ……383
21.1.2 PVC和SVC ……385
21.1.3 交换网的优点 ……385
21.2 对帧中继的不同认识 ……386
21.2.1 从OSI的角度认识帧中继 ……386
21.2.2 用户对帧中继的认识 ……388
21.2.3 运营商对帧中继的认识 ……390
21.2.4 标准化组织对帧中继的认识 ……390
21.3 帧格式 ……391
21.4 拥塞控制 ……392
21.4.1 再谈CIR ……392
21.4.2 预约水平 ……393
21.4.3 开环流量控制 ……394
21.4.4 闭环流量控制 ……395
21.5 多协议支持 ……395
21.5.1 帧中继上的SNA ……395
21.5.2 VoFR ……397
习题 ……398
第22章 ATM ……400
22.1 ATM基础 ……400
22.1.1 引言 ……400
22.1.2 信元 ……400
22.1.3 ATM的体系结构（分层） ……401
22.2 ATM信元层 ……403
22.2.1 信元的路由选择 ……403
22.2.2 网络接口 ……404
22.2.3 信元头 ……405
22.3 ATM适配层 ……406
22.3.1 应用服务分类 ……406
22.3.2 AAL0 ……407
22.3.3 AAL1 ……408
22.3.4 AAL2 ……408
22.3.5 AAL3/4 ……408
22.3.6 AAL 5 ……410
22.4 UNI 信令 ……410
习题 ……413

第四部分 局域网和互联网络

第23章 LAN: 补充概念 ……415
23.1 软件基础 ……415
23.1.1 NetBIOS ……415
23.1.2 Windows 98网络 ……416
23.1.3 IEEE 802标准 ……419
23.1.4 专用协议 ……421
23.2 以太网 ……422
23.2.1 以太网帧结构 ……422
23.2.2 10Base5 ……424
23.2.3 10Base2 ……425
23.2.4 10BaseT ……426
23.2.5 10BaseF ……429
23.3 令牌环网络 ……429
23.3.1 基本配置 ……429
23.3.2 扩展TRN ……430
23.3.3 活动监视器 ……431
23.3.4 信号编码 ……432
23.3.5 TRN帧结构 ……432
23.3.6 操作实例 ……434
23.4 FDDI ……435
23.4.1 一个基于层的标准 ……435
23.4.2 PMD层 ……436
23.4.3 PHY标准 ……437
23.4.4 MAC层 ……438
23.5 10Mbps以上的以太网 ……439
23.5.1 引言 ……439

23.5.2 以太网PHY ……441
23.5.3 全双工操作 ……442
23.5.4 流量控制 ……442
23.5.5 自动协商 ……443
23.5.6 链路集合 ……443
23.6 快速以太网 ……444
23.6.1 快速以太网的类型 ……444
23.6.2 扩展100BaseX ……445
23.7 千兆以太网 ……445
23.8 VLAN ……446
习题 ……447
第24章 桥接与路由 ……450
24.1 互联网设备 ……450
24.1.1 在网络中加入网桥 ……450
24.1.2 在网络中加入路由器 ……451
24.1.3 骨干的倒塌 ……453
24.2 网桥 ……454
24.2.1 转换和封装网桥 ……454
24.2.2 透明网桥 ……455
24.2.3 生长树算法 ……456
24.2.4 源路由网桥 ……458
24.3 路由协议 ……459
24.3.1 路由、路由协议和可路由协议 ……459
24.3.2 距离矢量路由与RIP ……459
24.3.3 链路状态路由和OSPF ……462
24.3.4 自治系统和BGP ……465
24.4 路由器配置 ……466
习题 ……469
第25章 TCP/IP：其他的概念 ……470
25.1 简介和回顾 ……470
25.2 网络接入层 ……471
25.2.1 地址解析协议（ARP）和反向地址解析协议（RARP） ……471
25.2.2 代理ARP ……471
25.2.3 点到点协议（PPP） ……473
25.3 IPv4 ……474
25.4 IP地址的不足 ……479
25.4.1 无类别域间路由选择（CIDR） ……479
25.4.2 动态主机配置协议（DHCP） ……480
25.4.3 基于IP的专用网络 ……481
25.4.4 网络地址转换设备 ……482
25.4.5 代理服务器 ……483
25.4.6 IPv6 ……484
25.5 因特网控制报文协议（ICMP） ……485
25.6 用户数据报协议（UDP） ……486
25.7 传输控制协议（TCP） ……486
25.7.1 TCP报头的格式 ……486
25.7.2 TCP数据段交换的一个例子 ……488
25.7.3 连接 ……491
25.8 应用层 ……492
25.8.1 简单邮件传输协议（SMTP） ……492
25.8.2 远程登录（Telnet） ……493
25.9 探究网络 ……495
25.9.1 网络接口 ……495
25.9.2 子网掩码 ……497
25.9.3 路由表 ……498
25.9.4 追踪路由 ……498
25.10 建立新的子网 ……501
25.10.1 配置接口 ……501
25.10.2 配置静态路由 ……502
25.10.3 配置动态路由 ……503
25.11 域名服务 ……503
25.11.1 目的和作用 ……503
25.11.2 域名服务器（DNS） ……504
25.11.3 nslookup ……506
25.11.4 DNS查询过程 ……507
25.11.5 反向查询 ……507
习题 ……509
第26章 Linux管理 ……512
26.1 简介 ……512
26.2 安装 ……512
26.2.1 准备 ……512
26.2.2 硬盘分区 ……513
26.3 了解所使用的服务器 ……519
26.4 用户账户 ……521
26.4.1 保护根用户的密码 ……521
26.4.2 创建一个用户账号 ……522
26.4.3 小结 ……524

26.4.4 e-mail ……526
26.4.5 FTP ……527
26.4.6 组内共享文件 ……528
26.5 基本安全性 ……529
26.5.1 超级用户的远程登录 ……529
26.5.2 禁止特定的IP地址 ……531
26.5.3 禁止匿名ftp ……531
26.6 使用X Windows ……531
26.6.1 配置X Windows ……531
26.6.2 Apache Web服务器 ……533
26.7 网络管理 ……533
26.7.1 DNS ……533
26.7.2 静态路由 ……535
习题 ……537
第27章 虚拟专用网 ……540
27.1 虚拟专用网介绍 ……540
27.1.1 什么是虚拟专用网 ……540
27.1.2 按用户类型对虚拟专用网分类 ……541
27.1.3 按所在的OSI层次对虚拟专用网分类 ……542
27.2 虚拟专用网的优点 ……544
27.3 安全问题 ……544
27.3.1 确定安全性的要求 ……544
27.3.2 加密方案 ……545
27.3.3 证书 ……549
27.4 IP安全协议（IPSec） ……551
习题 ……552
缩略语表 ……554

第一部分 联网基础知识

第1章 欢迎学习电信学

电信领域是一个充满活力的领域。在这个领域中，新技术层出不穷，并且被率先开发和采用。前8章为初学者描述通信概况，同时也介绍一些基础知识，以便为读者阅读以后各章作准备。本章特别从历史的角度介绍了电信的发展过程，描述了实现一次简单电话呼叫的全部过程，包括这个呼叫被处理的位置以及在每个不同的话音路段上所采用的承载方式。同时还讨论了构成Internet（因特网）的基本单元。本章还给出了业内的发展动态，并且对各种标准化组织进行了介绍。对于希望了解网络的先进单元的人来说，这里所涉及的每一个话题都是最基本的。

首先，来看一下首字母缩写词。很遗憾，在没有详细讨论网络这个话题之前，我们就必须使用许多首字母缩写词。在碰到一个缩写词时，如果你不知道它是由哪几个单词的缩写构成，千万不要灰心！我注意到，在许多场合下，即使是某个领域的专家，天天使用缩写词，也不一定能正确地给出这些字母所代表的单词。缩写词由哪几个单词组成并不重要，重要的是它们所代表的含义。当然，知道缩写词所代表的单词会帮助你更好地记住这些缩写词的意思。然而更重要的是，你要知道怎样使用这些缩写词，以及它们在整个电信术语图表中的适当位置。如果希望确切地知道缩写词所代表的单词，可查阅书后的“缩略语表”部分。

1.1 历史回顾

1.1.1 19世纪

电信意味着相隔一定距离的通信，就如同望远镜被认为是一种使人们能够看到远距离物体的设备一样。今天的电信始于电报。1831年，一位名叫Henry的物理学家发明了电报，而电报的实际应用则要归功于Samuel Morse发明的中继器（repeater），正是这个装置使电报的长距离传送成为可能。

1845年，西部联合电报公司（Western Union Telegraph Co.，简称西联公司）成立。1861年，第一条横跨美国大陆的电报线路被建立。1865年第一条穿越大西洋的海底电缆铺设成功。从此，整个世界走向了通过网络相互连接的道路。

早在1854年，Philip Reise就已经能够通过电线传送声音了。因此，许多人认为他是电话的发明者。然而直到1876年，Alexander Bell才获得了电话专利。就在Bell发明电话的同一天，Eliza Gray也独立地发明了电话。Bell曾经研究过聋子，试图把声音转化成电能，然后通过某种方式与大脑连接起来。这样，耳聋的人就能够“听”了。Bell第一阶段的工作非常顺利，但遗憾的是，直到今天与大脑连接的工作还没有完成。

Bell原打算把他的发明卖给西联公司，但却遭到了嘲笑和拒绝。这多少有点像第一台数字计算机的发明者——John Atanasoff和Clifford Berry的遭遇，他们曾与IBM联系，却被告知IBM绝不会对电子计算机产生兴趣。1877年6月，Bell成立了自己的公司，取名为贝尔电话公司（Bell Telephone Company）。1879年，贝尔收购了西部电子公司（Western Electric）。1885年，贝尔电话公司与AT&T(美国电报电话公司)合并。

1.1.2 独立电话公司

1893年，在电话专利过期时，涌现出来许多独立的电话公司。刚开始，它们主要在AT&T认为不赚钱的乡村开展业务，很快它们的业务范围就扩展到了城市。对这个时期的用户来说，如果需要与周围几个地区保持联系，一个家庭就必须安装几部电话。也就是说，连接一个电信公司就需要一部电话。这是因为贝尔系统无法与那些独立电话公司实现互连，所以网络服务不得不重叠，至少在城市里是这样的。

不久，AT&T开始收购这些独立电话公司。这时，美国司法部认为AT&T违犯了谢尔曼反托拉斯法（Sherman Anti-Trust Act）。作为回应，AT&T的一位副总裁Nathan Kingsbury，于1913年单方面发布了一封公开信（不是双方都接受的判决），这就是著名的Kingsbury承诺。承诺保证从今以后，AT&T将不再收购独立电话公司，并允许独立电话公司的网络与贝尔系统互连，同时转让AT&T持有的西联公司股票。这意味着从此以后每个用户家里只需要安装一部电话。这也是今天那些独立电话公司还能存在的原因。目前，大约有1400家独立的电话公司。

在认识到AT&T的垄断事实之后，美国国会于1934年签署了通信法（Communications Act）。联邦通信委员会（FCC，Federal Communications Commission）也由此诞生，旨在保护公众免受高价劣质服务的困扰。

现在，FCC的主要任务是规范化州间和国际间的通信。英语前缀词“Inter”表示在两个地方之间，而前缀词“Intra”表示在一个地方之内。例如，“Interstate”（州际）高速公路指的是连接两个州的高速公路，而“Intrastate”（州内）高速公路只在一个州内部存在。在每个州内，还设有公用事业委员会（PUC，Public Utility Commissions），负责控制和规范州内的通信。

1.1.3 拆分的道路

随着时间的推移，1968年这一年通过了Carterfone决议，为专用设备接入电话网开辟了道路。在这项决议中，联邦通信委员会要求AT&T不能拒绝连接，但可以制定接入设备必须满足的标准。这使得一些公司可以从本地电话公司以外的其他公司购买用户交换机（PBX）。

就在同一年，William McGowan遇见了Jack Goeken。McGowan是一名哈佛商学院的毕业生。他注意到Goeken的微波通信公司（MCI，Mircowave Communications, Inc.）未被获准在芝加哥与圣路易斯之间为往返的卡车司机铺设一条微波线路。MCI遭到了来自AT&T、通用电话、伊利诺斯贝尔、西南部贝尔和西联公司的反对。

电信业内的每一个人都知道反对FCC和AT&T不会有什么好结果，然而McGowan对电信业一无所知。他把自己的办公室设在华盛顿特区离FCC不远的地方。在随后的三年里，他不仅为卡车司机提供服务，而且还发展了其他的业务。不用多说，他的业务也发展到了其他城市，还建立了另外几条传输线路。1974年，McGowan发起了一场针对AT&T的反垄断诉讼，

美国司法部也于1975年提出了同样的诉讼，最终在1984年导致了贝尔系统公司（Bell System）的拆分。拆分就是把一家公司分成几家独立的公司。甚至于连AT&T的Robert Allen也认为，正是McGowan把电信这个高度垄断的行业重塑成为一个充满竞争的行业。

早在1949年，美国司法部就打算把西部电子公司从贝尔系统公司分离出来，成立一家独立的公司。然而，1956年的一项双方都接受的判决却允许西部电子公司作为贝尔系统公司的一部分，条件是它的业务仅限于公共传输通信服务。

作为这项判决的修正案，法官Harold Green于1982年签署了最终修正法案（MFJ，Modified Final Judgment）。这项1984年1月1日生效的法案将贝尔系统公司拆分成8家独立的公司，它们是AT&T和7家区域性贝尔运营公司（RBOC，Regional Bell Operating Company）。

那时，全美国共有23家贝尔运营公司（BOC），除了南部新英格兰电话公司（SNET，Southern New England Telephone）和辛辛那提贝尔公司仍属于AT&T之外，其余的21家BOC则分属于不同的区域性贝尔公司。这7家区域性贝尔公司是Ameritech、Bell Atlantic、Bell South、Nynex（NY and New England eXchange）、Pacific Telesis、Southwestern Bell和US West。所创建的贝尔通信研究中心（Bellcore，Bell Communications Research）为所有的区域性贝尔运营公司提供服务；而贝尔实验室仍归属于AT&T。贝尔通信研究中心和贝尔实验室都是通信技术的研究和开发基地。

1.2 呼叫处理（1984—1996）

1.2.1 本地接入和传送区（LATA）、局间通信公司（IXC）和本地电话公司（LEC）

拆分贝尔系统的时候，全美国被分成184个本地接入和传送区（LATA，Local Access and Transport Area）。划分这些区域的目的是为了明确各BOC与各长途电话公司之间的业务范围。1993年共有189个LATA，其中161个是贝尔LATA，另外28个是独立的LATA。到了2000年，共有196个LATA。

LATA的边界由利益集团决定，通常不会改变。尽管在大多数情况下，LATA按州边界和区域码边界来划分，但是也可以不这样做。区域码边界不会超过州边界，但是在许多情况下LATA边界可能会跨越州边界。图1-1是1993年加利福尼亚州的LATA边界和所在位置的区域码。现在区域码更多。在该图中，帕萨迪纳（Pasadena）与洛杉矶（Los Angeles）的区域码不同，但它们属于同一个LATA。而圣克鲁斯（Santa Cruz）和蒙特里（Monterey）的区域码尽管相同，却属于不同的LATA。换句话说，一个LATA可以拥有多个区域码，而一个区域码地区也可包含多个LATA。

当一个区域的号码资源用得差不多的时候，就有必要分成两个区域。这样，可用的号码资源就会增加一倍。由于大量使用调制解调器、蜂窝移动电话和传真机，现在美国人需要的电话号码数目比以前大为增加。从理论上讲，在一个给定的区域码中，7位电话号码可从000-0000一直到999-9999。因此，一个区域码能够提供10^7个号码，也就是1000万个电话号码。引进新的区域码的唯一原因就是要增加可用电话号码的数目。如果所有的区域码都用完了，就必须考虑改变现有的编号系统。如果希望查找分配给美国各州和各城市的区域码及三位数的电话交换局号码，请访问www.nanpa.com网站。

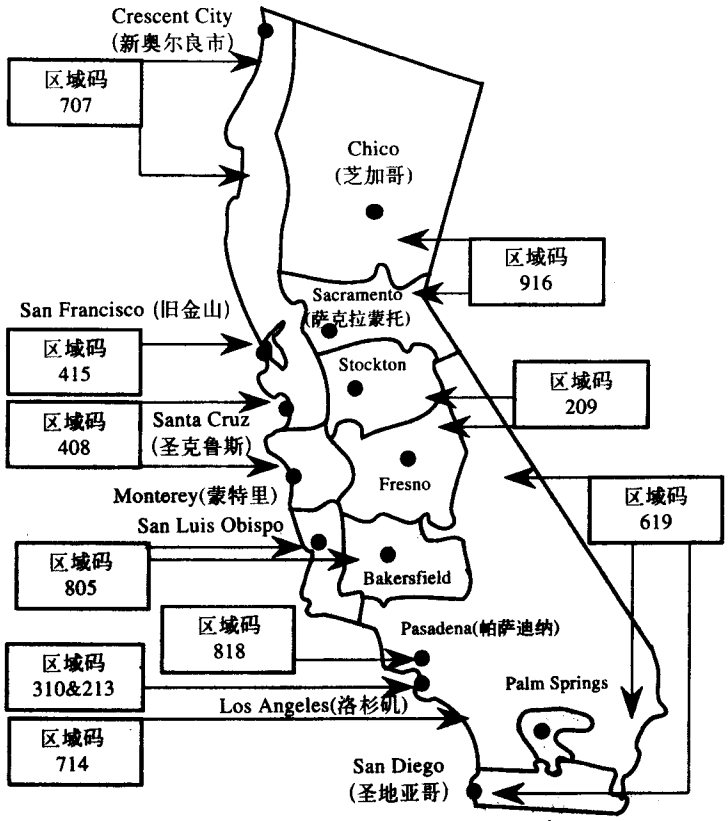


图1-1　从1993年的地图中可以看到加利福尼亚州的10个LATA。今天，有了更多的区域码，但是LATA边界并没有发生变化。注意：一个区域码（如916）一旦跨越两个LATA，某个LATA（如旧金山的LATA）就可能有多个区域码

电话公司（telco, telephone company）这个术语通常是指本地运营公司，它可能是一个BOC，也可能是一个独立电话公司。有时也把电话公司称为本地交换运营商（LEC，Local Exchange Carrier）。这里的“本地”是指一个LATA内，不包括区域码后面的前三位电话号码。在一个LATA中的大部分通信业务由电话公司处理，对于蜂窝运营商来讲，这会增加费用。

长途电话运营商，如AT&T、MCI、Sprint（原南太平洋铁路内部通信网）也被称做局间电话公司（IEC）或局间通信公司（IXC，InterEXchange Carrier），主要负责处理LATA之间的业务。图1-1给出11个LATA，其中的10个是贝尔LATA，由太平洋贝尔公司（Pacific Bell）提供服务，剩下的1个是独立的LATA，由GTE提供服务。在这些LATA内还有许多其他的独立电话公司。是哪一家电话公司暂且不论，其实在一个LATA内的通话，均由LEC处理；而跨越一个LATA边界的通话，则必须由IXC处理。在这种情况下，通常需要两个以上的运营商来处理这个通话：将主叫方连接到IXC的LEC、IXC本身以及将IXC连接到被叫方的LEC。主叫方的LEC和被叫方的LEC可以是相同的，也可以是不同的。

例如在图1-1中，虽然圣克鲁斯（Santa Cruz）和新奥尔良市（Crescent City）相隔很远且区域码不同，但它们属于同一个LATA，所以它们之间的通话由LEC处理。由于这类通话在同一个LATA内，所以不需要IXC提供服务。这是一个长途电话，但话单由LEC产生。

但是，如果一位住在圣克鲁斯（Santa Cruz）的居民希望与住在蒙特里（Monterey）的朋友通话，尽管两者的区域码相同，但也需要IXC提供服务，因为这是LATA之间的通话。通话的话单由IXC——AT&T产生，或者由主叫方的长途电话运营商产生。LEC不仅包括RBOC，也包括一些独立的电话公司，其中最大的是GTE公司。

1.2.2 术语定义和呼叫路由选择

如图1-2所示，先来解释几条术语，这些术语在解释呼叫路由选择时要用到。

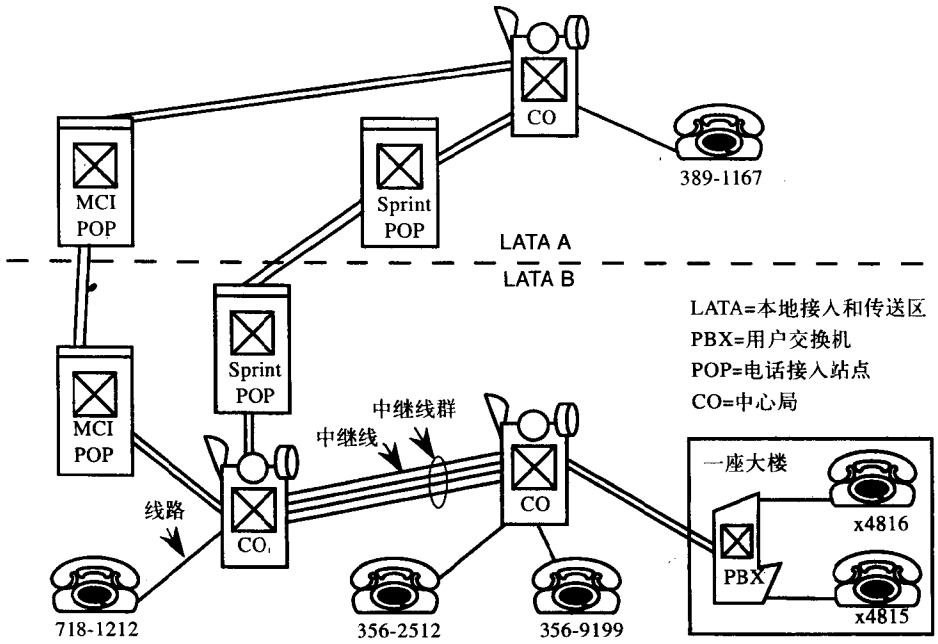


图1-2 大楼内的呼叫由PBX处理，同一LATA内的呼叫通常需要CO提供服务，而LATA间的呼叫则需要属于特定IXC的电话接入站点提供服务

电话线是将终端（如一个电话机）与网络连接起来的线路。交换机是一种典型的电子设备，提供了两条电话线之间或中继线之间的连接。中继线则是两台交换机之间的连接线路。一对交换机之间的若干条中继线的集合就是一个中继线群。

中心局（CO，Central Office）是这样一幢建筑：来自本地区的所有用户的电话线都汇集到这里，并将这些线路与中心局内的交换机相连接。当你拿起话筒给你的邻居打电话时，CO的交换机会检测到你已经摘机，并向你传送拨号音。在你拨完电话号码之后，交换机就会使你邻居家的电话振铃。尽管你们相距很近，但通话连接仍然需要经过本地中心局。

用户交换机（PBX，Private Branch eXchange）是一种专门为一个设施（如一幢大楼）内部的分机提供交换服务的交换机。中心局提供公共服务，而用户交换机主要为大楼内的居民提供服务。第11章和第13章将进一步讨论中心局和用户交换机。

图1-2是前面所介绍的各个单元互相连接的例子。先来看一下各种呼叫是怎样被处理的。如果两部电话与同一个中心局连接，它们之间的呼叫就被称为局内呼叫，这里的“局”指的是中心局CO。比如，号码356-2512与356-9199之间的呼叫就属于局内呼叫，而356-2512与

718-1212之间的呼叫则属于局间呼叫。

在一幢大楼内的电话机通常被看作专用网络的电话机，而其他电话机可以被看成是公共网络的一部分。公共网络的全称是公共交换电话网（PSTN），有时也被称为长途直拨（DDD）网。长途直拨的意思是不通过接线员而直接拨打长途电话。国际长途直拨（IDDD）网是指覆盖全球的公共交换电话网。

当PSTN上的一部电话机呼叫一幢大楼内的总机时，话务员（以前称为交换机接线员）会应答呼叫并将其转接到相应的分机上。

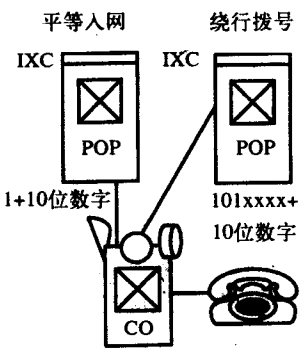
如果是楼内的一部电话呼叫楼内的其他分机，则只需简单地拨打分机号。如果希望呼叫PSTN上的用户，分机上的用户就必须首先从PBX那里获得拨号音。然后，还需要拨打特殊的接入号码，比如9，等待来自中心局的拨号音，接下来就可以拨打公共电话网上任何地方的电话了。当然，还要依赖于PBX授予的特权。

如前所述，IXC必须处理LATA间的呼叫。为了实现这个功能，IXC必须能在某个点把往来于中心局的呼叫连接到自己覆盖全国的网络上。这种点就称为电话接入站点（POP，Point of Presence），同时也是IXC和本地电信公司的连接点。对于一个IXC，如果要覆盖全国，则每个LATA至少要有一个POP，也可以有几个。显然，这些POP点必须连接成网络。在中心局把用户呼叫转移给IXC之前，通常会为用户定义一个默认的IXC，这就称为预订。

现在如果在图1-2中的分机4816上拨打公共网络上的电话389-1167，电话公司的网络就知道应该把这个呼叫传递给哪一个POP。如果这个呼叫被默认设置到Sprint，那么接收方的Sprint POP就会把这个呼叫传递给属于当地电信公司的中心局，然后再连接到389-1167。

楼内呼叫由PBX处理，LATA内的呼叫由中心局处理。而LATA间的呼叫通常由两个或多个中心局、POP以及可能的PBX处理。

由预订的IXC处理LATA间的呼叫，这被称为**平等入网拨号方式**（equal access dialing）。最终修正法案（MFJ）禁止LEC为AT&T提供相对于其他IXC更快、更容易的拨号（如使用较少的数字）。正是基于这样的原因，这种拨号方式才称为平等入网拨号方式。你只需简单地先拨一个“1”，然后再拨后面的10位数字（见右图）。



你可以尝试为某个特定的呼叫选择非默认或非预订的IXC。这时，必须先拨“101xxxx”，然后再拨10位号码。这里“xxxx”标识一个特定的IXC，如AT&T的号码是0288，Sprint的号码是0333。当你在LATA范围之外用这些数字进行呼叫时，你的呼叫首先会连接到指定的IXC。这种在LATA间的拨号过程被称为绕行拨号（dial around），因为你绕过了默认的IXC。无论是平等入网拨号或绕行拨号，IXC都可以委托LEC代收话费，也可以从LEC那里获得你的家庭住址，然后直接向你收费。

1.3 进一步了解PSTN

1.3.1 蜂窝系统

到目前为止，我们已经了解了PBX、CO和POP在公共交换电话网上的作用。但是，还有许多内容必须添加到图1-2中，这样一来这幅图看起来就更为复杂。无线蜂窝系统就是其中之

一。图1-3显示了蜂窝电话公司的移动电话交换局（MTSO，Mobile Telephone Switching Office）与LEC中心局连接的情况。MTSO可以和其他的MTSO直接相连，每个MTSO都与自己的一套基站相连。从CO到MTSO以及MTSO到基站之间采用有线连接，基站与移动电话之间采用无线连接。

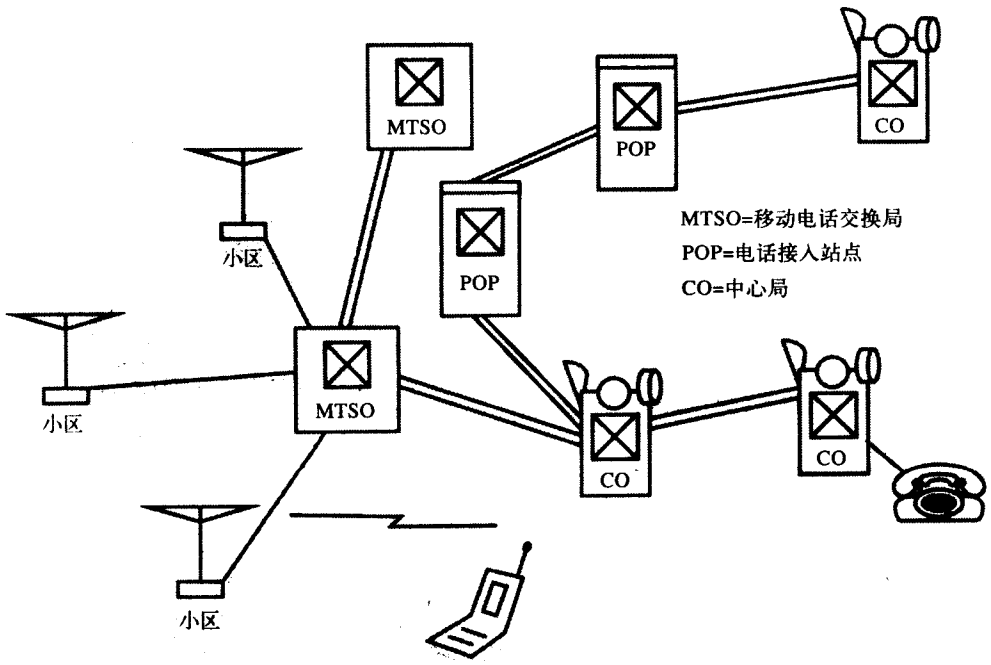


图1-3 无线业务与有线业务的连接

MTSO是一台负责测定哪一台基站接收到的来自指定移动电话的信号最强，然后通过此基站建立与该移动电话的连接。如果移动电话从一个区域移动到另一个区域，当前基站的信号衰减，而另一台基站将更适合处理与该移动电话的通信。MTSO检测到这种情况后，会把这个呼叫切换到新的基站上去。

在图1-3中，当与CO连接的固定电话用户呼叫移动用户时，CO根据拨叫的电话号码决定把这个呼叫交换到某个特定的蜂窝电话公司。就像CO会把LATA间呼叫传递给特定的POP一样，在这里CO会把呼叫切换到特定蜂窝运营商的MTSO上。然后MTSO检测各基站的信号，在可能的情况下建立实际连接。与POP是IXC网络的一部分一样，MTSO也是蜂窝电话公司网络的一部分。属于同一个蜂窝电话公司的MTSO可以实现跨LATA和跨州的互连，而不像其他电话运营商那样受到政府的严格限制。蜂窝电话公司可以处理LATA间的呼叫，并能连接跨越多个州的呼叫。与LEC和IXC不同，蜂窝电话公司根本就不受最终修正法案的限制。

1.3.2 七号信令系统

在PSTN上，七号信令系统（SS7）一直是默默无闻的“幕后英雄”。如果还使用以前的机电式交换机，会浪费大量的PSTN资源，如交换容量和中继线等。要达到今天我们所能享受到的服务水平，运营商需要更多的交换机和中继线容量。

如图1-4所示，如果仍然采用以前的方法完成一次呼叫，当一部话机呼叫另一部话机时，

与呼叫路径上各交换机的连接需要逐个建立。只有在前面的交换机建立连接之后，后面的交换机才能沿语音链路建立连接。这样要花很长的时间。如果完成一次呼叫需要5台交换机，则首先必须建立与第一台交换机的连接，然后才是第二台，第三台，……，直到与所有的交换机都建立了连接。麻烦还不仅如此，如果被叫电话此时正忙，那么所有为这次呼叫建立的连接都将被放弃。虽然这次呼叫没有成功，但仍然需要耗费网络资源。由于用户接收到的是一串忙音，因此电话公司无法从中得到任何好处。

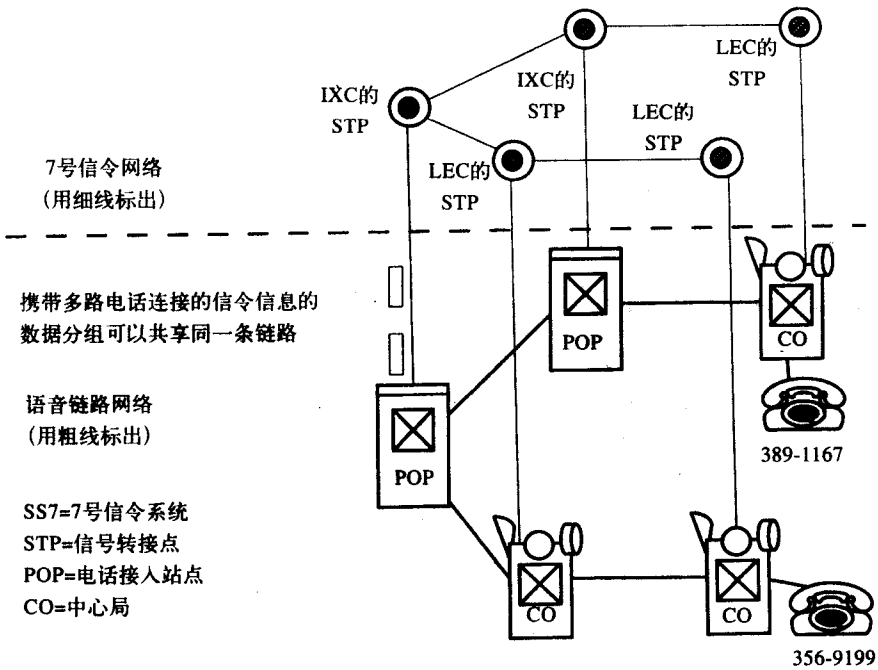


图1-4　从语音链路网络中分离出来的信令网，用于确定实际连接建立之前如何为一次呼叫选择路由

有了七号信令系统之后，PSTN被分成两个部分：语音链路网和信令网。语音链路网仅在必要时使用；而信令信息以数据分组的形式通过七号信令网传送。正是由于这样的原因，尽管七号信令系统是语音网络的一部分，但在本书中却将它放在数据网络部分进行介绍。七号信令系统中使用的分组交换机被称为信令传输节点STP（Signal Transfer Point）。它们通过在信号链路上传输的数据分组来实现与本地CO、POP和MTSO的通信。每条信令链路可以传输多个呼叫的信令信息。由于传输信令信息所需要的时间较短，因此一条信号链路可以由多个用户共享。

当用电话开始拨号时，本地中心局首先将拨打的电话号码封装在数据分组中，传送给它的STP，然后这个STP通过其他的STP为这次呼叫寻找一条最佳路径。一旦呼叫的语音链路被确定，利用STP指定的中继线号码，沿途的所有语音交换机得到统一的交换指令，于是语音链路就建立起来了。在对方中心局传回振铃音之后，表明网络已经成功地为两端用户建立起连接。使用七号信令系统，可以使国际长途电话的连接建立时间从15秒缩短到2秒左右。

如果拨号时远端的用户正忙，语音链路就不会被建立，而由本地中心局产生忙音。这样就不会浪费交换和中继线资源。每条信号链路可同时传输多个连接的数据分组，但每条语音中继线一次只能为一个通话传输信号。

七号信令网络是整个PSTN的“神经系统”。没有它，所有交换机都会瘫痪；就好像没有神经系统，我们身体的各部分无法做任何事情一样。由于七号信令的重要性，因此在实现时预留了大量的冗余度。正是由于有了七号信令系统，我们现在才能开发所谓的先进智能网络（AIN，Advanced Intelligence Network）。七号信令系统支持呼叫信用卡的使用，如800电话，以及其他的一些在电话网上提供的业务，七号信令网中的数据库可以支持这些业务的实现。其中最重要的是，如果想基于电话网提供一种以前不曾有过的业务，只要修改七号信令系统的软件就可以实现。七号信令系统大大地增加了PSTN的灵活性。

1.3.3 个人通信系统（PCS）

在写书的时候，如果我想把自己的电话号码告诉其他人以方便联系，这时仅告诉他人一个电话号码是不够的。要想让他人能够顺利地找到我，在我的名片上必须有我的家庭电话、公司电话和移动电话号码。然而这还不够，还必须提供我的作息时间表，这样才能使别人在适当的时间、通过适当的电话号码找到我。还好我每天的作息时间相对固定。如果名片上仅提供e-mail地址，则只需要一个地址就够了。那么为什么必须留几个电话号码，同时还要给每个号码一个“合适的时间”呢？

个人通信系统（PCS，Personal Communication System）是一种对用户友好的设想。在这个系统中，每个人只需一个电话号码，相应的也只需要一套电话设备。只要电话设备随身携带并且开着，无论我到哪里，PCS都会知道我的位置以及如何与我建立连接。

当我回到家里，位于我家附近的基站检测到我已到家，然后发信号给七号信令网络的数据库，告诉它可以通过我家附近的电话基站与我建立联系。这时我的电话相当于一部无绳电话。如果我去了别人家，那里的基站会向PCS网络登记我的位置。当我工作的时，无线PBX就是我的连接点。这样任何人都可以通过我唯一的电话号码与我建立联系，七号信令网络总会知道我的具体位置，并能以适当的方式与我建立连接。

你也许会说，我是否可以使用当前的电话号码作为唯一的号码。但是在写这本书的时候，所有的PCS通信仅能在PCS基站之间用PCS天线实现。你必须按时间支付占用无线信道的费用，同时还不得不牺牲信号的质量。如果采用其他的通信方式，比如使用家里的无绳基站或者是工作单位的无线PBX，则可以以较低的花费享受优质的信号服务。

为了实现全球的无线覆盖，一些大公司联合组成的财团正在建立被称为低轨卫星（LEOS，Low-Earth Orbit Satellite）的复杂卫星系统。有了LEOS，就不用在每座高山和每个峡谷上安装基站天线了。这些卫星贴近地球运转，可提供低时延的连接，这一点对语音通信非常重要。由于距离移动电话非常近，因此它们也比传统的卫星消耗功率少。同时移动手机消耗的功率也较低。

1.4 Internet

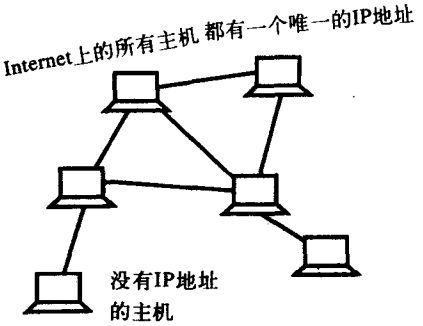
1.4.1 数据网

前面介绍了PSTN的演变过程。PSTN网络最初是为传送语音而设计的，现在已经能被用来传送数据、视频和其他类型的信息。在本节中，将对Internet做一个简短的介绍。最初，Internet是为传送数据而设计的，但它现在已经能够用来传送包括语音在内的各种信息。PSTN

被设计用来承载语音，而Internet被设计用于承载数据。

今天Internet已经成为将许多网络连接起来的网络。它是全球最大的数据网络。这些网络的连接简直天衣无缝，在Internet用户看来，它们俨然就是一个整体。如果一台计算机想与Internet上的其他计算机直接进行通信，那它必须拥有自己的IP地址。在整个Internet上这个IP地址必须是唯一的，通常利用该IP地址进行主机识别。在Internet上，拥有IP地址的设备被称为主机或节点。如果一台主机想和另一台主机通信，这台主机必须知道目的主机的IP地址。一种称为路由器的设备在Internet上的主机之间传送信息。为了描述简单，这里暂时不考虑路由器。

从右图可以观察到，有一台计算机没有IP地址。对于那些通过特定的Internet服务提供商（ISP，Internet Service Provider），如美国在线，连接到Internet上的PC来说，这种情况确实存在。这些计算机上的所有信息在被发送给Internet上的路由器之前必须先经过ISP服务器。ISP还提供其他的一些特殊服务，如保护用户免遭危险站点的侵害。该图中的其他计算机都是直接与Internet上的路由器相连接。相对那些没有IP地址的计算机，它们的响应时间要快得多。



1.4.2　TCP/IP协议簇

Internet上所有拥有IP地址的主机，都运行一簇简单的数据协议，其中的两个协议叫做传输控制协议（TCP，Transmission Control Protocol)和网际协议（IP，Internet Protocol)。这个Internet协议系列被称为TCP/IP协议簇。协议是一种处理某个特定通信任务所采取的统一方法。在以后的章节里，会接触到发送邮件的协议、传送文件的协议等。TCP/IP协议簇为Internet主机之间的通信定义了一套标准的方法，事实上已被所有类型的计算机系统采用。这就意味着不论你使用哪一种硬件类型的计算机，也不管你的计算机运行的是哪一种操作系统，还不必考虑你的连接类型，只要执行TCP/IP协议，就可以直接连到Internet上。

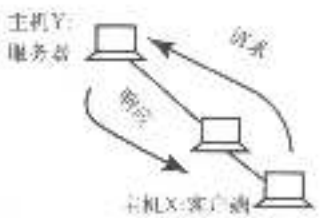
1970年，我在东京火车站里找不到一个懂英语的人。如果我会一点日语，我就可以和那里的人进行“通信”了，因为东京使用的“通信协议”是日语。同样的道理，如果一台计算机要成为Internet上的主机，就必须“理解并能说”TCP/IP协议。尽管我的身体特征（也就是硬件）与日本人不同，文化背景（也就是操作系统）也有差异，但这些其实都不重要。我不能同日本人进行“通信”的根本原因是我不会“操作”日语。由此可以看出，TCP/IP协议对于在Internet上运行来说是多么的重要!

1.4.3　客户/服务器模型

现在Internet上所有主机间的通信都可以使用客户/服务器模型。这就意味着一旦Internet上有事件发生，就有一台主机充当客户，一台主机充当服务器。请求特定服务的主机被称为客户，而提供这种服务或做出响应的主机就是服务器。

在右下图中，如果主机X向主机Y请求传送一个文件。这时主机X就是客户，而主机Y则是服务器。这两台主机将使用文件传输协议（FTP，File Transfer Protocol）进行通信。这时

主机X上运行的是FTP客户软件，而主机Y上运行的则是FTP服务器软件。当两台主机断开它们之间的连接之后，它们可能会交换所扮演的角色。主机X变成服务器，而主机Y则变成了客户。



在微软的Windows环境下，当PC被连接到Internet上的时候，通常得到一个IP地址，这时PC可以充当FTP客户，但不能充当FTP服务器，因为PC上通常不会安装服务器软件。

Internet上有许多服务器，可以提供不同类型的服务。邮件服务器接收和发送邮件，它们必须全天工作，以便随时处理到达的邮件。实际上服务器都是全天工作的，因为它们根本无法知道用户会在什么时候请求它们提供服务。Telnet是Internet上主机提供服务的另一个例子，它允许用户从远端登录到服务器。

一台主机可提供多种类型的服务，服务器上有一些特殊程序在后台不停地运行，这些程序监听客户的请求，一旦有服务请求发生，就为这次连接启动一个服务器软件的备份，然后继续监听其他请求，这种程序称为后台程序（daemon）。

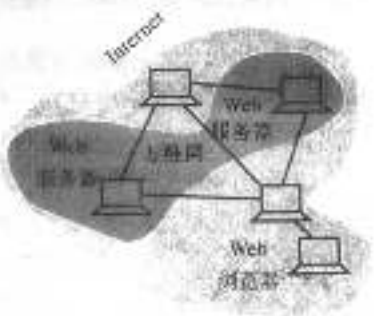
1.4.4 发送e-mail

人们发现直接使用IP地址发送e-mail很不方便。例如，记住ramteke@pilot.njin.net这样的e-mail地址比记住ramteke@[165.230.224.139]容易得多，记忆单词总是比记一串随机数字要容易。在我的e-mail地址中，ramteke是用户名称，pilot是e-mail服务器的名字，njin.net是域名，而pilot是该域的一个成员，net是顶级域名。pilot.njin.net是e-mail服务器的完整地址，在这个服务器上有一个叫ramteke的e-mail用户，在这个例子中，pilot的IP地址是165.230.224.139。

尽管Internet上的主机使用IP地址相互通信，但是可以看出使用诸如pilot.njin.net这样的描述型地址更为方便。这样一来，我们就需要一种把描述型地址转换成IP地址的方法。Internet上有一种特殊的服务器，被称为域名服务器（DNS，Domain Name Service），提供从主机名到IP地址的转换。这类服务器使用DNS协议，每当一台主机需要把主机名转换成IP地址时，就会向一台主域名服务器发出服务请求。如果主服务器不知道被请求主机的IP地址，它会询问其他的域名服务器。Internet上有一个提供这类服务的域名服务器系统。

如果你向ramteke@pilot.njin.net地址发送e-mail，你的主域名服务器会为你找出pilot的IP地址。然后，利用pilot的IP地址，服务器会把你的e-mail以数据分组的形式发送到pilot。如果你使用pilot的IP地址直接发送e-mail，域名解析这一步就不需要了。也就是说如果使用ramteke@[165.230.224.139]代替ramteke@pilot.njin.net，你的e-mail不用域名服务器的帮助就可以直接发送出去。

1.4.5 WWW



万维网（WWW，World Wide Web）是Internet上向客户提供Web页面的服务器集合。Web服务器还能提供与其他Web服务器的连接，因此正如右图所示，WWW是Internet上主机的一个子集。Web页面通常是用超文本标记语言HTML(HyperText Markup Language)设计的，而Web服

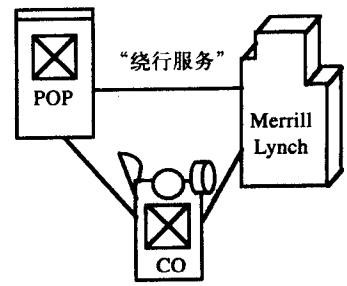
务器和客户运行的是超文本传输协议（HTTP，HyperText Transfer Protocol）。

当你在Internet上，或者更确切地说是在访问一个Web站点时，将会使用一种叫Web浏览器的WWW客户软件。Netscape就是这样的一种Web浏览器。为了访问Web页面，浏览器需要与运行HTTP协议的服务器进行通信。Apache是使用HTTP的Web服务器软件的一个例子。

1.5 1984年以来业界的发展

1.5.1 竞争接入提供商（CAP）

1984年，Merrill Lynch意识到必须通过LEC的CO，才能接入IXC的POP。为了避免连接到LEC的费用，Merrill Lynch成立了Teleport通信公司，专门安装和维护直接连到POP的光缆。这是竞争接入提供商CAP（Competitive Access Providers）提供绕行服务的开端（见右图）。



1987年，伊利诺斯州邻近芝加哥的新斯德尔（Hinsdale）的CO发生了一起火灾。这场火灾使当地的通信瘫痪了两个星期。为了给本地电话公司或LEC提供备份，城市光纤系统（MFS，Metropolitan Fiber Systems）应运而生。

在通常情况下，CAP凭借在市区内提供直接连到IXC的POP的传输设备，与本地运营电话公司竞争。使用绕行传输的用户不必向本地电话公司付费。相对于本地电话公司，CAP一般是通过光纤网络提供服务。这种网络在通信节点之间可以提供双倍的信道，因此服务质量和安全性更好。此外，CAP还提供具有竞争力的价格来吸引本地电话公司的用户。

在很多情况下，绕行传输网络都会跨越LATA边界，因为在美国的大多数州里，它们都不受管制。用户不仅能绕过两个州内的LEC，而且同样能绕过IXC。当然，这些区域性贝尔运营公司（RBOC）不想失去大量的客户。

要提供新的业务，区域性贝尔运营公司（RBOC）必须得到公用事业委员会的批准。而绕行传输则不受这个限制。CAP还通过光纤主干网提供局域网互连和其他一些先进的业务。

管理人员非常喜欢CAP的一个最吸引人的原因就是CAP为他们的网络增加了可靠性。一旦本地承载网络的某条线路遭到破坏，备用线路就会派上用场。CAP还能提供一些网络管理功能，诸如路由重选、远程线路遥测等。由于可从不止一个POP选择路由，因此大大提高了网络的灵活性。CAP给LEC带来了竞争，对双方来说服务质量提高了，同时成本也降低了。

1.5.2 通信代理商和Internet服务提供商（ISP）

通信代理商从主要的运营商如AT&T、Sprint以及区域性贝尔运营公司那里购买通信业务，然后再转手卖给终端用户。一些通信代理商实际上是从大运营商那里租借光缆和交换容量。它们仅对那些通信业务量大、可以获得利润的大的客户提供这项业务。

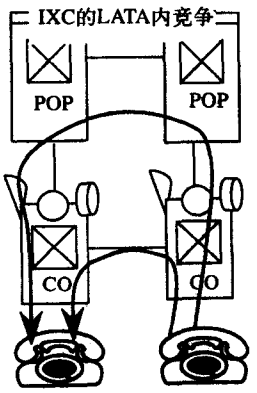
由于上网的人越来越多，ISP也变得越来越重要。ISP主要是提供到Internet的连通性。ISP能够提供电子邮件服务、网页浏览服务以及其他类型的Internet服务。一些ISP提供与Internet的直接连接，而另一些则要通过其服务器进行连接。与Internet直接连接能使信息传递更为快捷；通过ISP的服务器可以增加电子公告牌和诸如过滤危险网站的其他服务。

1.5.3 1996年的电信法案

由于CAP开始瓜分区域性贝尔运营公司的本地市场份额，区域性贝尔运营公司也想得到跨LATA的市场份额。1996年的电信法案允许区域性贝尔运营公司开展这项业务，条件是它们必须同意IXC连接到它们中心局内的交换机上提供本地业务。在1984年，谁提供什么服务已经分得很清楚，即IXC提供LATA间的电话服务，而LEC则提供LATA内的电话服务。由于这项法案，这种划分又变得模糊起来。这就好像是两个孩子在吃午餐，他们都想吃到另一个人盘子里的东西。现在，电缆公司或可能出现的任何其他公司，都可以提供本地接入。

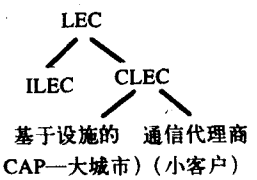
最终修正法案（MFJ）为长途LATA间的电话市场带来了竞争。1996年的电信法案则给本地的LATA内的电话市场带来了竞争。区域性贝尔运营公司需要证明它们能满足14条限制条款的要求，以此说明本地市场确实存在竞争。作为回报，区域性贝尔运营公司获准开展LATA间的电话服务。这14条限制条款仅适用于区域性贝尔运营公司名下的LEC，对独立电话公司的LEC无效。

14条限制条款中包括这样一些内容，比如号码的可移植性。也就是说，如果一个用户改变它的运营商，如从区域性贝尔运营公司变成与之竞争的本地交换运营商（CLEC，Competitive Local Exchange Carrier），这个用户可以不更换自己的电话号码。条款还包括设备的同地点存放问题，也就是CLEC有权力在区域性贝尔运营公司的中心局内放置自己的设备。条款还对平等接入区域性贝尔运营公司的网络作了规定，包括电话线杆、用户信息数据库、911接入等。为了区分CLEC和现有的LEC，现有的LEC称为在职的LEC（ILEC，Incumbent LEC）。



最终修正法案是由法院通过的，而电信法案则是由国会通过的一项法案。最终修正法案促进了长途电话业务的竞争，而电信法案则开辟了本地电话业务的竞争道路。然而结果却适得其反，许多运营商进行了重组，这个行业的竞争者数量反而减少了。在右图中，可以看到一个特定的IXC可以在一个区内（LATA内）拥有多个POP。电信法案允许IXC处理那些通常被LEC作为长途电话收费的区内电话业务。LEC之所以允许IXC进入本地市场，是因为这样他们就可以参与长话竞争了。正如你所看到的那样，IXC和LEC在LATA边界上的差别渐渐地开始消失。

共有两类主要的CLEC：基于设施的CLEC和通信代理商。看边上的图，以前的CAP就是现在的基于设施的CLEC。两个最重要的CAP——MFS和TCI，已经分别被MCI和AT&T收购。这些运营商或者有自己的交换设备，或者有覆盖城区的光纤网，或者两者都有。CAP主要吸引大城市里的大客户。通信代理商只能为一些小客户提供服务，由于盈利率很低，因此不是十分活跃。由于这个原因，MCI和AT&T都不向通信代理商出售本地的代理业务。早在20世纪80年代，长途电话公司经常在午餐时间打电话拉拢新客户。而今天即使颁布了电信法案，本地市场的竞争也没有那样的激烈。



1.5.4 兼并大潮

自从1996年通过电信法案为本地市场引入竞争以后，电信行业经历了巨大的变化。在原

来的七家区域性贝尔运营公司中，Bell Atlantic和NYNEX进行了合并，SBC则和Pacific Telesis、Ameritech合为一家公司。Bell Atlantic随即又收购了GTE这家最大的独立电话公司。AT&T也把McCaw通信公司纳入旗下，使自己有能力提供无线服务。随后，AT&T借机成立了一家叫做Lucent（朗讯）的子公司，专门提供通信设备，如CO交换机、PBX等。这样，Lucent就可以很方便地为AT&T的竞争对手，如Sprint、区域性贝尔运营公司等提供设备。Teleport通信集团——一个覆盖66个城市的CAP和电信公司（TCI）——一家电缆供应商，也先后被AT&T兼并。Worldcom也收购了WilTel和随后的MCI。所有这些兼并据称总资产超过2000亿美元，曾在业界引起了轩然大波。谁也不敢确定在电信行业这个大舞台上，下一步将要发生什么。无线业务、Internet应用和国际市场的增长，是这些大型电信企业之间展开争夺的原因。

1.5.5 专用集成电路（ASIC）

在电信市场出现巨型公司的同时，工程师们却正在硅片上创建微型系统。我还记得，那时电子元件市场上的主角是电子管。它们体积大、占地方、易爆、大量散热、额定电压高，而且需要经常更换。晶体管的引入从本质上克服了所有这些缺点。

再后来，计算机的“心脏”——CPU，把能装一屋子的电子管电路集成在一块集成电路（IC）芯片上。在一块集成电路芯片上可制作数百万计的晶体管。现在，微处理器分为两种基本类型：复杂指令集计算型（CISC，Complex Instruction Set Computing）和精简指令集计算型（RISC，Reduced Instruction Set Computing）。CISC处理器具有一套复杂的机器指令，而RISC处理器则只有较少的一些基本机器指令。要完成一条CISC指令需要执行几条RISC指令的功能，因为一条CISC指令与几条RISC指令在功能上是等价的。由于CISC指令的数量远远大于RISC的指令数量，因此要在指令查询表中查找一条CISC指令需要较长的时间。尽管Intel的奔腾系列仍然采用CISC体系结构，但当前的趋势是采用RISC处理器。

传统的组网设备，如路由器使用RISC处理器。当然，这些设备是靠在RAM中装载的软件程序运行。如果某标准委员会修改了协议，则只需要为路由器下载新版本的软件。软件为路由器这样的设备提供了灵活性。

由于这些年来协议已经得到完整定义并且逐渐稳定下来，因此不必经常更新网络设备的软件。这样设备的生产商就可以在被称为专用集成电路（ASIC，Application-Specific Integrated Circuit）的IC上实现软件功能，并且将逻辑电路直接烧入芯片。ASIC是基于硬件，而不是基于软件的设备。这样做的优点是，ASIC作为一种专用芯片，其运行速度是基于RISC软件处理器的3倍。ASIC的生产成本低且体积小。当然，ASIC的缺点是它们的功能是固定的，不能通过下载软件来更新。设计ASIC芯片需要大约一年的时间，而且需要技术熟练的工程师。有时由于内置的ASIC芯片不能被更换，因此不得不更换整个设备。

正是由于这样的原因，生产商正在研究被称为网络处理器的新一代处理器。这种设备结合了RISC和AISC芯片的优点。利用通用的RISC体系结构实现非标准化的功能，利用AISC体系结构实现固定的功能。56K调制解调器实际上就是网络处理器。新的调制解调器标准还没有制定。然而，一旦确定了新的调制解调器标准，则只需要用新版本软件升级现有的调制解调器。

作为一个受益于这项技术进步的例子，网卡的价格已经从300美元降到了50美元左右。同时这些技术还为移动电话的小型化作出了贡献。

1.6 标准

1.6.1 开放系统

一般情况下，计算机和通信公司都会竭力束缚其用户，使他们接受自己的特定产品系列。由于在该产品中的投资，因此用户往往被锁定在一个生产商的产品上。如果用户收到劣质服务，生产厂商也不会太在意，因为用户放弃他们的投资转向其他厂商设备的可能性极小。而且从用户的角度来说，新厂商可能跟原来的差不多，甚至更差。

现在，生产厂商们仍然竭力劝告用户采用其专用方案，但用户已经开始寻求开放系统。尽管开放系统的定义非常困难，但它意味着用户可以在任何计算机和任何网络上使用他们的现有产品。而且，开放系统产品可以从多个厂商购买——用户不会受制于一个厂商。

让我们来看一下专用产品和开放产品的例子。Intel的奔腾处理器是相对专用的产品，而可缩放处理器体系结构（SPARC，Scalable Processor ARChitecture）芯片则是一个开放的方案或标准。其他厂商也可以自由生产。类似地，大型计算机及其操作系统，如IBM的MVS属于专用方案，而IBM的PC和Unix则是标准的或是开放系统。

PC是开放的，因为很多公司都可以生产。这是因为当初IBM不想再像从前那样销售PC了。但Macintosh却是一个专有产品。在网络领域，开放系统互联（OSI，Open Systems Interconnection）是一个开放的网络体系结构。为OSI操作编写的应用程序可在任何支持OSI的硬件、操作系统或网络上运行。但IBM的SNA（System Network Architecture，系统网络体系结构）既不是开放的，也不是完全专用的。

用户选择开放系统产品的原因很多，其中最重要的一点是保护他们的投资。如果系统是开放的，当用户对自己的生产厂商不满意时，他（她）就可以更换设备生产厂商，同时仍能保护自己的投资。有了竞争之后，生产厂商就会改善服务，而且价格也会下降；即使是正在给用户提供优质服务的生产厂商，也是如此。在这种情况下雇佣熟练技术人员也相对容易得多。许多生产厂商都宣称自己的产品是开放的，但千万不要被它们的宣传误导进一个专用系统（尽管可能有很多理由采用这样的系统）。使用专用系统的一个原因可能是标准还未制定，而用户需要一个临时的解决方案。很多时候一个专用方案会被证明是有效的，而且能提供一些标准方案所没有的功能。

1.6.2 标准化组织

图1-5给出了许多标准化组织。各种组织之间的层次结构并不是一成不变的，它们之间在一定程度上相互关联。

在联合国（UN，United Nations）设有总部在日内瓦的国际电信联盟（ITU，International Telecommunications Union）。国际电信联盟主要由电信标准部（ITU-T，Telecommunications standardization sector）和无线通信部（ITU-R，Radio communication sector）组成。它们的前身分别是国际电报电话咨询委员会（CCITT，Consultative Committee for International Telegraph and Telephone）和国际无线电咨询委员会（CCIR，Consultative Committee for International Radio）。ITU-R在国际范围内分配无线频段，就像FCC在美国国内做的那样。

ITU-T的收入来自各种标准化组织，而各国的邮电总局（PTT；Post, Telegraph and Telephone）

是由政府垄断的，类似于美国的邮政系统。世界上大多数国家都有自己的邮电总局，用于提供电信服务。ITU-T的表决成员全部来自各国的邮电总局和美国国务院（US State Department）。

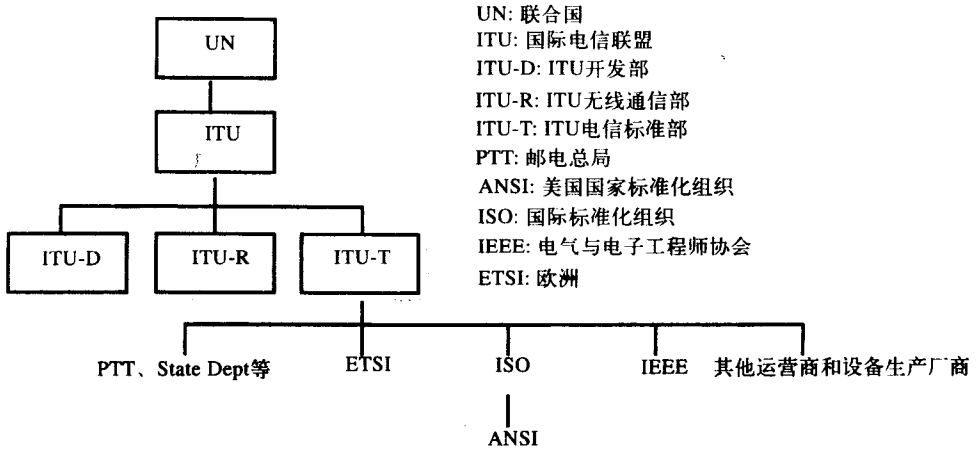


图1-5　一些重要的标准化组织

对我们来说，美国国家标准化组织（ANSI，American National Standards Institute）是另一个重要的组织。该组织在制定美国标准方面具有举足轻重的地位。

国际标准化组织（ISO，International Standards Organization）制定螺母、螺钉、胶卷以及其他许多领域的标准。在电信领域，ISO以其制定的OSI参考模型而著称。

电气与电子工程师协会（IEEE，Institute of Electrical and Electronic Engineers）是一个专业机构，负责制定各种局域网（LAN，Local Area Network）标准。

除了上述组织以外，在ITU-T还有许多运营商和设备生产厂商的代表。

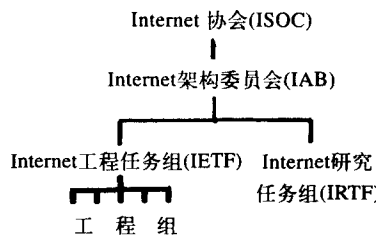
贝尔通信研究中心，即现在的Telcordia，也曾积极地推荐过一些标准，如SONET和SMDS。SONET（Synchronous Optical NETwork，同步光网络）是在光纤上传输数字信号的标准，而SMDS（Switched Multi-megabit Data Service，交换式多兆位数据业务）则用于实现远距离局域网间的互连。

由于建立标准要经过相当长的一段时间，因此许多生产厂商和用户经常组织论坛，以帮助新技术迅速得到实际应用。帧中继论坛就是这种论坛中一个很好的例子。在两年的时间内，这个论坛将概念转变成了现实。目前ATM论坛非常活跃。

这里需要提一下事实标准。它们作为标准不是因为它们得到了一些机构的认可，而是因为它们事实上早已存在，而且得到了广泛应用。有时候官方标准已经得到认可，然后工程师们才把它们用于实际工作。但有时事实标准先在实际应用中被证明有效，然后才得到业界的接受。TCP/IP协议就是事实标准的一个例子，它仅在大量的RFC（Request For Comment，请求注解）文件中有记载。尽管没有标准化组织认可这套网际互连协议，但它远比OSI普及，因为它工作简单有效。

今天的国际Internet由IAB（Internet Architecture Board，Internet架构委员会）管理。它又分成IETF（Internet Engineering Task Force，Internet工程任务组）和IRTF（Internet Research Task Force，Internet研究任务组）。IRTF是一个小组，专门研究Internet上一些需要长期考虑的问题。IETF要大得多，它又分成大约20个工作组。IETF非常活跃，主要从事解决Internet工程问题的

工作。Internet协会（ISOC，Internet SOCiety）是一个旨在促进Internet研究和发展的组织（参见右图）。Internet网络信息中心（InterNIC，Internet Network Information Center）是管理IP地址分配和域名分配的组织。如果需要更多的关于Internet组织的信息，可访问www.internic.net 网站，这个网站还提供了一些与Internet有关的资料，如RFC文档。可以从www.ietf.org网站下载RFC文档。



习题

1.1 节

1. 谁获得了电话专利？
   a. Reise　　b. Morse　　c. Bell　　d. Gray
2. 谁最可能与贝尔系统的拆分有直接关系？
   a. Judge Green　　b. McGowan　　c. Robert Allen　　d. FCC
3. 电话的发明者是哪几个人？
4. 在AT&T的垄断下，美国国会采取了什么措施保护公众的利益？
5. MFJ修改了哪些内容？
6. 简述Kingsbury承诺的内容及其意义？
7. 什么历史事件与西联公司对贝尔的电话不感兴趣相类似？
8. 列出导致贝尔系统拆分的关键事件及其发生的时间。
9. 贝尔系统的拆分给人们带来了哪些好处？缺点是什么？

1.2 节

10. 下面哪一个前缀词表示两个地方之间？
    a. inter　　b. intra　　c. intro　　d. pre
11. 下面哪一个系统提供内部电话交换？
    a. CO　　b. POP　　c. PBX　　d. 中继线群
12. 在哪个区域LEC可以处理整个呼叫？
13. 怎样扩充电话号码资源？
14. 描述一次跨LATA呼叫的建立过程以及经过哪些点。
15. 理论上，在一个区域码内有多少电话号码可用？
16. 下面的交换局或交换机分别属于哪些部门：CO、POP、PBX和MTSO。

1.3 节

17. 移动通信公司在下面的哪个地方实现与CO的连接？
    a. POP　　b. 基站　　c. MTSO　　d. STP
18. 在PSTN中，哪一种网络采用分组交换？
    a. 电话线　　b. 中继线　　c. 七号信令系统　　d. STP
19. 移动通信网络上的无线通信发生在哪两点之间？
20. 七号信令系统中使用的分组交换机叫什么？
21. 如果远端的电话正忙，会不会占用CO和POP之间的中继线？

22. 说出LEO的两个优点。
23. 哪一类通信系统最终能实现只使用一个电话号码、一个电话终端就可以完成各种通信?

1.4 节

24. Internet是建立在下面的哪一个协议簇基础之上的?
    a. TCP/IP　　b. Microsoft　　c. IBM　　d. WWW
25. 直接与Internet连接的主机必须分配下面哪一种地址?
    a. 局域网地址　　b. 调制解调器地址　　c. IP地址　　d. 连接地址
26. 在客户/服务器模型中，哪一台主机发出请求? 哪一台主机做出响应?
27. 简述如何把主机名转换成IP地址?
28. 所有的Web服务器必须运行哪一种协议?
29. Internet和WWW之间有哪些差异? 它们是同一个网络吗?

1.5 节

30. 大多数住宅用户通过哪一类服务商建立与Internet的连接?
    a. CAP　　b. ISP　　c. 通信代理商　　d. IXC
31. 下面哪一项法案导致了本地电信业的竞争?
    a. MFJ　　b. 1996年的电信法案
    c. Carterfone决议　　d. 谢尔曼反托拉斯法
32. 给出两条CAP形成的原因。
33. 简述通信代理商如何让用户以及它购买业务的大运营商两者均受益。
34. 简述1996年电信法案的目的以及它希望获得什么样的结果。
35. 基于RISC和基于ASIC两种设备的折衷方案是什么?

1.6 节

36. 下面哪一个组织是ITU-T的前身?
    a. ISO　　b. IEEE　　c. ITU　　d. CCITT
37. 什么时候你会使用专用方案?
    a. 考虑低成本方案时。
    b. 不希望仅仅依赖一个设备生产厂商时。
    c. 需要与其他公司统一标准时。
    d. 一个更有效的方案是可用而且必需的时候。
38. ITU-T的哪些成员为其提供资金?
39. IETF是怎样划分的?
40. 举两个本章没有提到的事实标准的例子。
41. 与开放系统相对应的是什么?
42. 从用户的角度描述一下开放系统和专用系统的优点。

第2章 数据组网基础

本章将介绍许多与数据网络有关的基本概念，透彻地理解这些概念是弄懂以后各章内容的前提。在本章中将讨论以下内容：在网络结构中所用到的层的概念以及在实际物理网络中的实现方法，路由器和分组交换在网络中扮演的角色，分组交换网络和数据报网络的差异以及其他一些与组网有关的重要话题。

开放系统互联（OSI，Open System Interconnection）参考模型也是本章的内容之一。最初的网络体系结构被规划用于连接各种类型的计算机，能运行各种类型的操作系统、采用各种类型的通信连接并提供各式各样的业务。这项复杂的任务最后被TCP/IP这个非常简单的网络结构所完成。虽然乍看起来学习OSI参考模型好像是一项纯粹的理论练习，但它却是解释其他体系结构的基础。在学习OSI模型时提出的组网问题，是选择其他组网方式同样需要解决的问题。因此学习OSI参考模型是理解数据组网基本原理的起点。

2.1 什么是网络

计算机刚刚问世的时候，大多数企业仅用一台大型计算机来进行数据处理。由于费用昂贵，数据处理通常在大型计算设备上进行，费用按照CPU机时和其他项目计算。那时计算机被安装在一间屋子里，工作人员在那里从事他们的计算工作——给成堆的打孔卡编码，然后交给读卡机阅读。

今天虽然数据中心还存在，但是大部分数据处理工作已经下放到小型计算机上进行，这些小型计算机在多数情况下都是台式机。与以前用一台计算机做所有的工作不同，如今我们可以使用多台小型计算机。此外，与原来必须走到大厅里将需要计算的工作输入到大型机里不同，现在计算机都在工作人员的附近或在办公桌上。

此外，由于许多小型系统（或者计算机）组合在一起的功能远远大于一个大型系统，这些小型系统通过数据通信链路被连接在一起。这些自治的、不受其他计算机控制的计算机互连，就称为网络。Internet则是网络的网络。

现在，就像必须给计算机适当地供电一样，只有把计算机连到网络上才能最大限度地发挥其作用。因此我们让通信和计算机“联姻”。数据通信不能离开计算机的参与；而没有数据通信，计算机也基本上毫无用处。

那么，什么是网络呢？网络可以简单地定义为两台或者更多的计算机或交换机的互连。现代的语音交换机也不过是一台专用计算机。对终端用户来说，一个好的网络看起来应该不像一个网络，而更像一台计算机。终端用户无须指明获得数据的路径，这些应该是网络软件考虑的问题。

目前主要有两类网络：局域网（LAN，Local Area Network）和广域网（WAN，Wide Area Network）。典型的局域网在一个设施（或一幢建筑）内提供连网功能。在校园环境下，局域网也可以扩展到邻近的设施中，能够覆盖两到三英里的范围。广域网可以跨越更广阔的区域，甚至覆盖全球。此外，还有一种城域网（MAN，Metropolitan Area Network），它既不

是局域网也不是广域网。

将网络划分成局域网和广域网的原因是驱动网络的协议通常被分为两大类。由于传输距离比较短，局域网上的数据传输速率远远高于广域网。广域网通常需要电话运营商提供服务，而且由于距离较远，利用广域网传送数据费用较高。因此，广域网的数据传输速率通常较低。由于局域网和广域网的特性存在实质性的差异，因此本书的后半部分将把它们分成两个部分进行讨论。

2.2 为什么联网

联网的一个原因是在网络上容易实现资源共享。资源包括应用程序（如字处理软件包）、数据、打印机、调制解调器等。在局域网环境下，没有必要为每台计算机和工作站都安装一套字处理软件包，只需要在一个文件服务器上安装一次。当然需要得到必要的授权。这样局域网中的用户都可以使用这个软件包。同样的道理，不必为每台计算机购买一台廉价的打印机，取而代之的是可以购买一台高速、高质量的打印机，然后让所有的用户都能访问它。

网络还能提供可靠性。在1960年，如果核心计算机出现了故障，谁也干不了事。但是到了今天，有许多计算机可用，如果一台瘫痪了，还可以依靠其他的计算机。

在晚上通信量较低的时候通过网络备份关键数据比依靠计算机操作员安装磁带和硬盘容易得多，虽然他们同时也在做这项工作。例如，在一所大学的机房里，如果一名学生用的计算机坏了，他可以换到另一台计算机上去取回自己的文件和应用程序，并且可以从网络服务器那里获得相同的工作环境。相反，如果他把所有的工作只存储在一台PC上，而他人占用了这台计算机，他就不得不请这个人离开，以便继续自己的工作。当然，今天我们更加依赖于网络服务器，而网络服务器恰恰是导致所有学生接入失败的一个公共点。此外，对一些服务器做镜像，然后让它们不停地备份，比对每一台计算机都做镜像要容易得多。

20世纪六七十年代，必须通过数据中心的大型计算机存取数据。这就导致了一种“瓶颈”效应。就如同水流过空瓶子的瓶颈一样，所有的工作必须经大型计算机处理，因此在数据中心这个瓶颈处造成了堵塞。现在，数据处理可以分布在整个网络上。各项工作可以在几个地方进行，而不仅仅依赖于一个地方设备的性能。如果一台主机瘫痪了，还可以把任务重新分配给其他的主机。今天的网络使当地部门具有更多的发言权，以决定什么是重要的，什么是不重要的。因为这些部门比远在数英里外的总部更了解当地的情况。

尽管大型计算机的处理能力可能是高端微型计算机的10倍，但造价至少是微型计算机的1000倍。所以，花相同的钱可以购买1000台微型计算机。将这些微型计算机连网之后，获得的处理能力是大型计算机的100倍。

网络还具有很大的灵活性。如果我们在达拉斯的一台计算机上有一个账户，碰巧我们要在旧金山呆上一个星期；则只要这两台计算机在同一个网络上，我们照旧可以从旧金山登录到达拉斯的计算机上。这样我们就不必呆在放置被登录计算机的地方。

在局域网环境下，每个工作人员不必每天都备份自己所做过的工作。管理员可以从一台核心计算机上定期地备份每人的工作。从本质上讲，连网使计算机系统更易于管理。

网络使计算机的管理更容易。对于那些每天都需要管理和维护计算机的人来说，不管网络提供什么样的功能，管理起来都非常困难。设想必须管理100台没有连网的PC工作站，每次更新软件都需要重复一百次。打印机的维护也必须不断地进行。如果这些PC都需要建立与

调制解调器的连接，就必须安装和维护100个调制解调器和100条电话线。利用网络，完成这些任务就容易多了。这时不必靠工作人员备份自己的工作。尽管他们可能暂时还会那样做，但很快就会发现这样做的重要性不大，因为备份能自动完成。

现在组网已经成了“特洛伊木马”，管理变得越来越容易，但安全性却变成另一个主要问题。网络的安全性就像一个移动的靶子，刚刚堵上一个安全漏洞，另一个漏洞又出现了。另外，资深的网络专家很少，熟练掌握网络技术的工作人员薪水很高，但同时还需要不断地培训。此外，网络配置总是在不断地变化。人们发现网络不断变化的原因是由于需要增加和删除节点、更新软件、升级硬件等等。因此，虽然最初的网络和分布系统的造价可能低于大型计算机系统的建设，但持续上扬的网络开销最终可能较高，并且难于详细列举。

网络的优点：

- 容易管理。
- 具有可靠性。
- 性价比高。
- 备份容易。
- 具有灵活性。
- 易于资源共享。
- 更容易实现本地控制。

网络的缺点：

- 安全性差。
- 熟练工作人员缺乏。
- 运行比较昂贵。

2.3 网络体系结构

2.3.1 什么是网络体系结构

现在研究网络体系结构的概念。虽然它不是很复杂，但对于初学者来说要完全理解还是比较困难的。由于本书与局域网和广域网有关的各章都是以这个概念为基础，因此读者必须切实地掌握它。为了加深对这个概念的理解，先来看一个大胆的比喻。

盖房子时，虽然一个人可以干所有的活，但房屋承包商还是会让专长不同的多个工程队来共同完成这项工作。可能是挖掘队挖掘地面，泥瓦队打地基，木工队建造房子的框架。与一个人独自完成整个工程相比，每个队都可以熟练且有效地完成自己的那部分工作。这样一来，建房工程就被分成了几个截然不同的部分。

同样的道理，在设计网络时，由于这也是一项复杂的工作，因此也可以分成几个不同的部分，每个部分称为层。当然，在设计时，也可以把网络看成是一个大实体或一项任务。但这种方法显得笨拙、不灵活，而且难于管理和实施。如同建造房子时聘请专业队承包工程更好一样，在设计网络结构时采用分层的方法会更好。在整个组网方案中，每一层实现一项特定的功能或目标，这些功能可能是传输过程中的检错，数据的加（解）密，或其他一系列使网络能正常运行所必须完成的工作。

用分层的方法设计网络，可以把各种网络功能变成不同的模块。设计单独的模块比把网

络当成一个整体来设计容易得多。对网络进行分层设计，可以将一个大问题变成几个小问题。这样使设计者可以独立地研究和开发每一层，而不受其他层的影响。解决所有小问题的方法集合，就是整个网络的解决方案。分别解决每个小问题通常比解决一个大问题更容易。

通过网络分层，能使网络今后的改动更加灵活。也就是说，一旦发现了完成某一层服务的新方法，只需用新方法替换这一层上所采用的旧方法，而后就可以立即检测网络性能的改善情况。如果性能提高了，证明这种方法可行；如果没有提高，退回到原来的方法也非常容易。在一个层上使用的一套方法和规则称为这一层的**协议**。

打个比方，挖掘队使用的“协议”是使用铁镐和铁铲，现在可以把“协议”改变成使用挖土机，再往后可以是使用锄耕机。每更换一次工具，都要验证一下是否工作得更好。对于瓦工队来说，挖掘队如何挖洞与他们无关。挖掘队向瓦工队提供他们的服务，而瓦工队则在这个服务的基础上继续工作。下一层向上一个相邻层提供的服务称为**接口**。

图2-1给出了主机A向主机B传输数据的情况。在网络上，这两台计算机的生产厂商不同，运行的操作系统也不同。当然，通信也可以在相反的方向上发生。图中所示的网络只分了三层。各层的定义以及层间接口的定义被称为网络体系结构。网络体系结构的建设与通常意义上的楼房建设不同，因为建房过程总是逐层上升的，比如从挖掘队逐渐向封顶队过渡。在数据通信中这被称为**单向传输**，因为数据仅向一个方向传送，如送到打印机。

网络体系结构应该能够处理双向的数据传输（采用半双工或全双工方式）。**半双工**是指在一个时刻，只能向一个方向传输数据；**全双工**是指在同一时刻，可以向两个方向传输数据。在图2-1中，主机A发送的数据经第三层处理后交给第二层，第二层协议对第三层传送过来的数据再进行处理，尔后送至第一层。

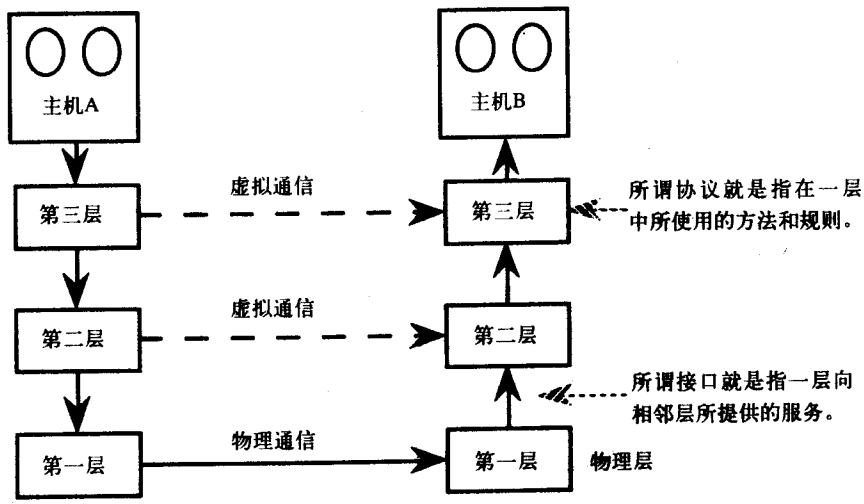


图2-1　网络上从主机A到主机B的数据传输用实线箭头表示。除了物理层之外，没有对等层之间的直接通信

第一层经物理通信链路把数据传输到主机B的第一层。同样的过程再反过来进行，最后数据到达主机B。第一层通常被称为物理层，因为实际数据的发送和接收发生在这一层。因此第一层之间的通信通常被称为**物理通信**，而高层之间的通信通常被称为**虚拟通信**。除了第一层之外，其他层的协议都是由软件实现的。

2.3.2 另一个类比

在进行深入讨论之前，首先来回顾一下图2-1中网络体系结构用到的基本概念。

在图2-2中，有两个用户，A和B，分别代表图2-1中的两台主机。然而这里只有两层，而不是三层。用户A在德国，用户B在印度。他们打算用摩尔斯电码与对方通信。如果我们没有德文和Marathi（一种印度语言）间的翻译，但有英文到这两种语言之间的翻译。因此，当德国的用户用德文说他想回家的时候，第二层的协议就把它翻译成英文。然后，这条消息被传送到电报操作员那里，由他转成摩尔斯电码。

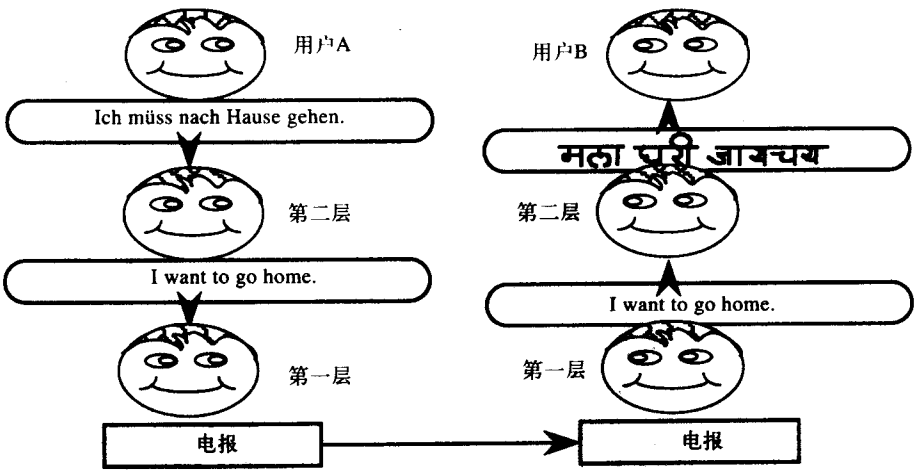


图2-2 网络体系结构的一个类比。表示的是一个德国人与一个印度人间的通信，其中信息要经过多次转换

在印度用户一方，处于物理层的电报操作员收到这条消息以后直接交给它上面的第二层，第二层为印度用户翻译成Marathi文。

如果修改第一层的协议，将电报系统改为电话系统或邮政系统，需要做的只是替换第一层的协议。这样做不会影响第二层，第二层接收到的服务不变。同样地，网络体系结构在各层之间提供特定的组网服务，每一层的协议只与本层有关，不会影响其他层（尽管网络的整体性能依赖于每一层使用的协议）。

2.3.3 网络体系结构的例子

网络体系结构的定义有许多种。其中一些是专用的，由特定的生产厂商使用；另外一些是标准的，许多生产厂商都在使用。

系统网络体系结构（SNA，Systems Network Architecture）是IBM定义的体系结构。最初，它仅用于单一主机或大型计算机，如图2-3所示。在主机（或大型计算机）上连接有一个本地前端处理机（FEP，Front End Processor），由它替主机处理所有与通信有关的事务。FEP再经通信链路连接到可能是位于不同城市的集群控制器。最后，由集群控制器与各个哑终端（无CPU）实现连接。

终端依靠集群控制器来运行操作，而集群控制器的运行操作又依赖于FEP。如果主机或FEP出现故障，整个网络就会瘫痪。尽管主机上的数据可能已经在其他地方做了备份，但所有的终端仍然依赖于主机。



图2-3　SNA网络的一个例子

集群控制器接收所有终端的数据，然后再进行适当的分发。过去SNA就在这种网络上运行，但是现在它已经发展演变成一个非常复杂的网络，被叫做高级对等联网技术（APPN，Advanced Peer-to-Peer Networking）。此外，还有其他的一些专用体系结构，如DECnet，AppleTalk等。

开放系统互联（OSI，Open Systems Interconnection）参考模型是国际标准化组织（ISO，International Standards Organization）制定的国际标准。它能使不同生产厂商的主机实现互连。在第1章中曾经提到的且贯穿全书的TCP/IP，就是这个网络体系结构的一个例子。

局域网体系结构系列是OSI的一个子集，包括IEEE 802.3和IEEE 802.5，分别运行在以太网（Ethernet）和令牌环网（TRN，Token Ring Network）上。图2-4a是以太网，它上面的所有站点都被连到一条称为总线的电缆上。图2-4b是令牌环网，所有的站点被连成一个环形。

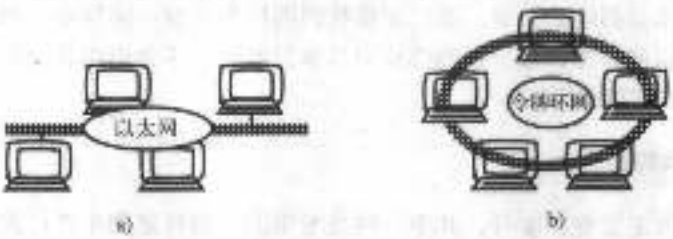


图2-4　a）以太网，b）令牌环网

2.4　OSI

在前面那个不同语言用户之间通信的类比中，每一层只传送了整个消息。然而在网络体系结构中，虽然这种情况也可能存在，但是每一层的协议还会加上相应头部和尾部。现在来看一下OSI各层的情况，这里给出的体系结构将用于与数据组网中其他类型的体系结构进行比较。

2.4.1　OSI概述

图2-5给出了OSI参考模型的七层。它们是物理层，数据链路层，网络层，传输层，会话

层、表示层和应用层。每一层都实现自己的一套功能，这些稍后会简要地介绍。现在首先看一下这些层是如何相互联系的。

当一个主机在网络上传输数据时，被传输的数据首先被交给应用层所采用的协议。应用层将处理这些数据，可能会在称为头部的字段中加上一些控制信息。应用层的头部被接收端的应用层使用，从而形成两个对等应用层间的虚拟通信方式。要传输的数据和应用层头部一起被称为应用层协议数据单元（APDU，Application Protocol Data Unit）。

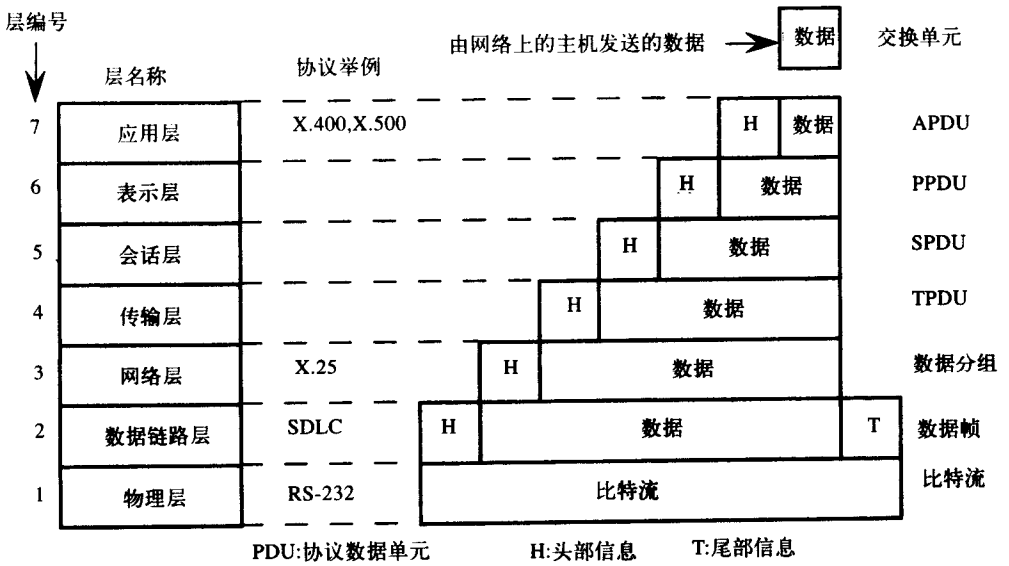


图2-5 OSI参考模型。第一层、第二层、第三层构成通信子网

这个APDU被应用层向前传递给发送主机的表示层。此时，APDU和应用层头部都被视为表示层的协议数据单元（PDU，Protocol Data Unit）中的数据部分，称为表示层协议数据单元（PPDU，Presentation PDU）。表示层头部是发送端表示层和接收端表示层之间实现通信的方法。PPDU被转交给会话层。

这个过程在每一层中重复进行，直至到达数据链路层。在数据链路层，还要增加一个尾部。最后，物理层将第二层传来的数据帧用比特流发送出去。

在接收端，处理过程相反。第一层接收比特流，组成数据帧后转交给第二层协议。在这里，先去掉数据链路层的头部和尾部，并对帧内的所有编码数据进行处理，如检查数据错误，然后帧内的数据部分转交给第三层。

第三层将一个帧的数据部分看作是一个分组，去掉头部并对它进行处理，而后再将这个分组中的数据部分传送给第四层。这个过程不断重复直到应用层把数据交给它的用户，也就是数据到达的地方。如果所有协议都能正确地执行，接收主机就能够理解发送主机的消息。尽管两台主机之间存在差异，比如生产厂商、运行速度和尺寸大小等都不同，这一通信过程也能实现。从本质上讲，为了实现各种系统之间通信的灵活性，所采用的折衷方法明显增大了系统的开销。

2.4.2 分层处理

为了对OSI网络体系结构的工作过程有一个更深的理解，先来看一下当数据从一台主机传送到另一台主机的时候，各层协议是怎样起作用的，见图2-6a至图2-6h。

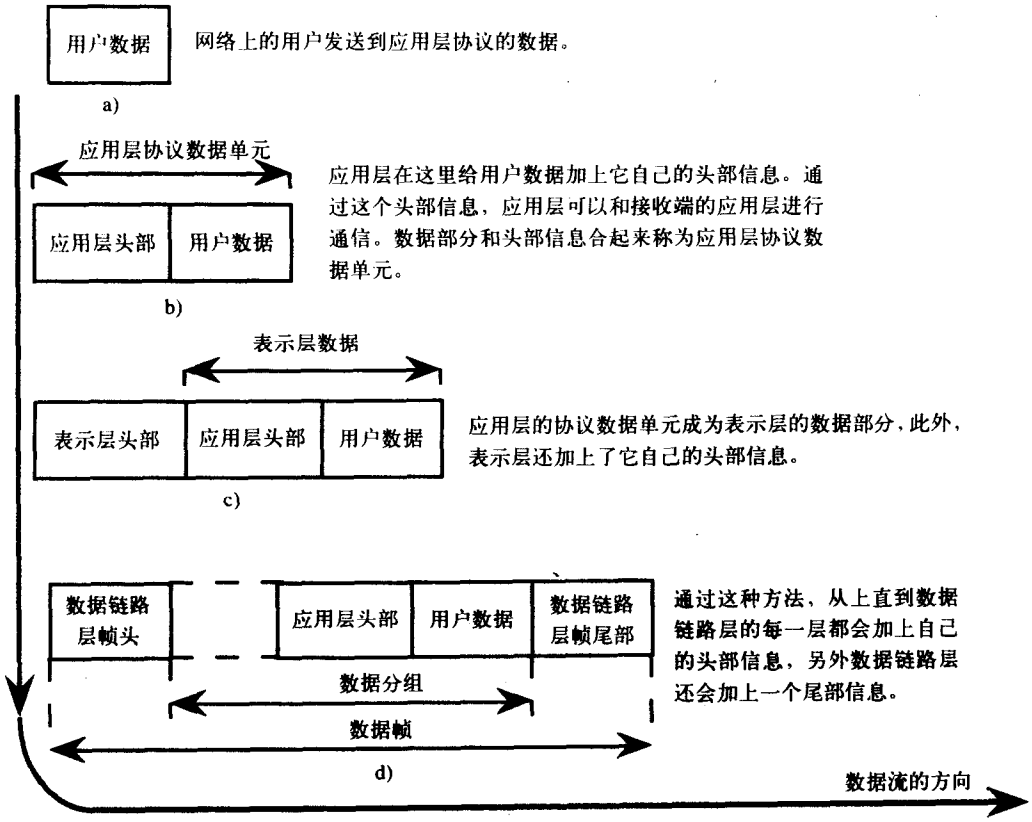


图2-6　在发送端，每一层都加上自己的头部。在接收端，每一层都会移走自己的头部

在图2-6a中，用户向网络发送数据，例如可能是一封email邮件的一部分。黑框表示数据中的所有1和0。应用层协议在数据上加一个头部。应用层头部和原始数据一起构成了一个交换单元，被称为应用层协议数据单元（APDU），或简单地称为一个消息（message），如图2-6b所示。应用层头部的编码信息对接收主机的应用层有意义。

在图2-6c中，表示层在APDU中加上自己的头部。这一层把整个APDU视为数据部分，就如同用户数据一样。表示层协议不知道，或者根本不关心应用层头部是否存在，而只把它作为数据段的一部分来处理。表示层头部的信息供接收主机的表示层使用。这个过程一直持续下去，每一层的协议都会加上自己的头部，直至数据链路层。在数据链路层，还需要加上一个尾部，这个尾部的作用是提供一种检错的方法。然后，数据链路层把比特流传送到物理层，物理层负责将这些比特流发送到网络链路上去。

在图2-6e中，这个由1和0组成的数据流到达了接收端。在这里，数据链路层会从这些1和0中检测出帧的起始位置，帧的头部和头部中各字段的位置，数据部分的起始和结束位置以及尾部的位置。这一层还负责检错。如果发现这一帧有错误，就会请求发送端重传出错的帧。因此，发送端应该在缓冲区中保存已传送的帧，直至收到确认信息以后才能清除。数据链路层会从收到的正确帧中把数据链路层头部和尾部去除，然后将数据部分转发给网络层协议。网络层将这个数据单元称为分组。它在处理完属于自己的头部之后，再把其余的数据交给传输层。

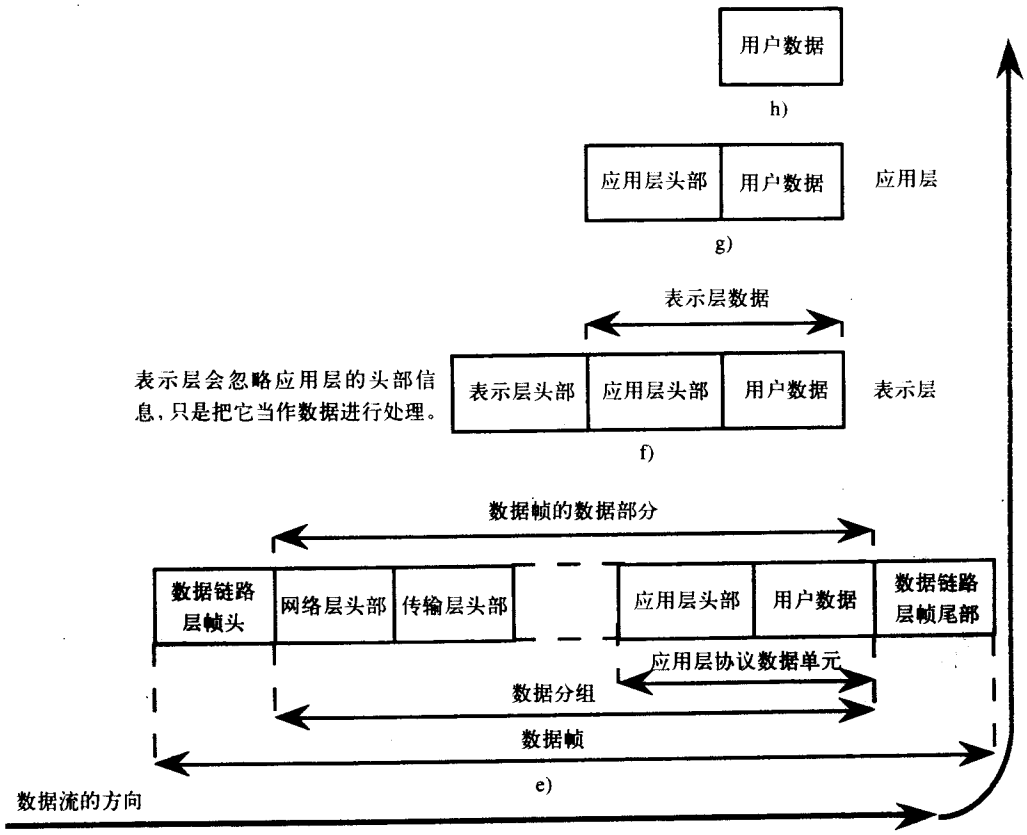
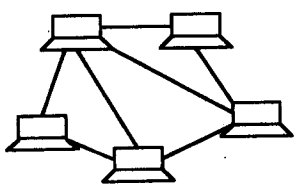


图2-6 （续）

这一过程一直延续到表示层，如图2-6f所示。这层的协议对表示层头部进行处理并把它去除。数据部分被传给应用层，如图2-6g所示。数据在经过了发送端的全部七层又以相反的顺序通过了接收端的全部七层之后，终于到达了用户端，如图2-6h所示。在发送端，每一层都在数据沿协议栈下行的时候添上了一个头部。而在接收端，每一层都对属于自己的头部进行处理并把它从整个数据单元中移走，再把剩下的数据向上层传递。对于数据字段中包含的其他层的头部，当前层都不会进行处理。

2.4.3 通信子网

现在我们已经知道数据是如何从发送主机发送，又是如何被接收主机接收的。现在要看一下，数据是如何在网络节点上传送并且最终到达目的节点的。发送主机和接收主机都称为网络的**端点**。数据在到达目的地之前，可能要经过多条链路，从一个中间节点跳到另一个中间节点（见右图）。这些链路及其中间节点的集合，被称为**通信子网**。在网络端点，OSI的全部七层都需要。然而在通信子网上，只用到OSI的下面三层。（这里所说的子网与第8章中描述的TCP/IP子网没有任何关系。）



数据也许需要跳过许多中间节点才能到达目的地

OSI参考模型的下面三层具有与上面四层截然不同的功能。下面三层考虑的是通过可用的

通信链路和分组交换机把数据传送到正确的网络节点。分组交换机是一种处理器的名称，该处理器使用OSI的下面三层将分组路由到正确的网路节点。分组交换机也可以被看作是一个**路由器**。另一方面，在第7章中还会看到**网桥**（bridge），它只使用OSI模型的下面两层转发数据帧。

OSI的上面四层由主机处理，而且与终端用户使用的应用程序有关。尽管全部七层都可以在一台主机上实现，但下面三层的功能路由分组到正确的节点。在深入学习子网之前，先看一个类比可能会很有帮助。

2.4.4　一个子网的类比

在图2-7中，一位住在圣地亚哥（San Diego）的居民寄了一张生日贺卡给他在芝加哥的表兄。邮件分配中心，在这个例子中充当第四层，把贺卡装在一个标明送往芝加哥的邮包中发送出去。

机场提供第三层服务的邮局工作人员决定邮包必须首先经过丹佛（Denver），尔后，提供第二层服务的工作人员把这个邮包装入空运集装箱送往丹佛。航空线，相当于物理层传输系统，会把集装箱空运到丹佛机场。在那里，第二层的工作人员会从空运集装箱中取出邮包并送给第三层人员去修理。

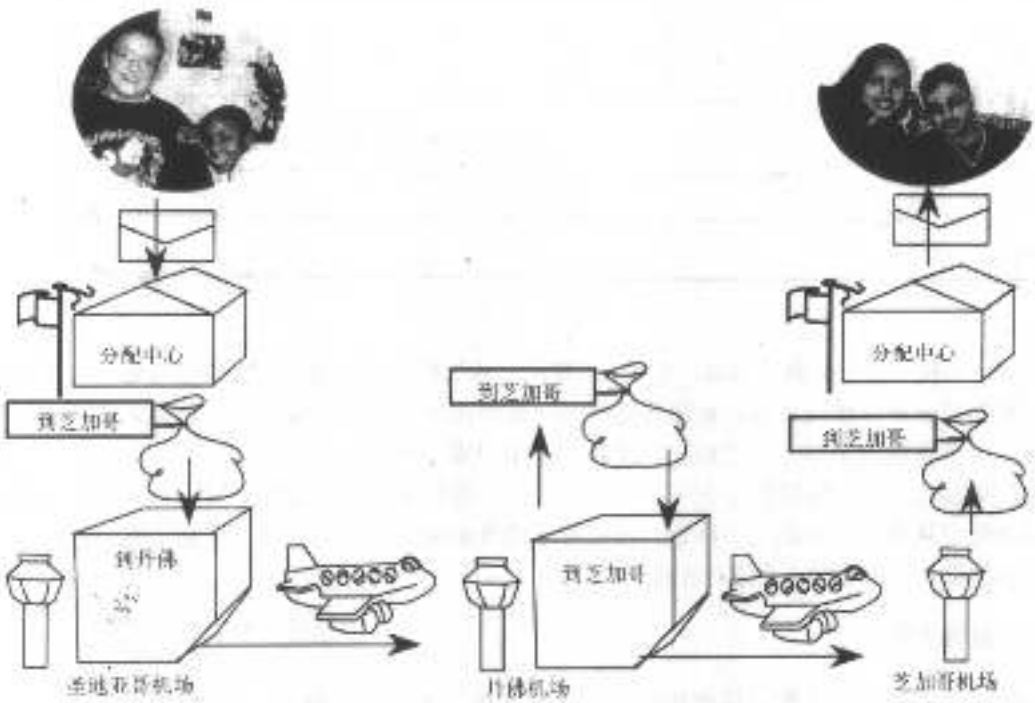


图2-7　在路由邮包到芝加哥的例子中，丹佛的设施被看作是第三层的分组交换机

第三层人员对这些邮包进行整理，发往丹佛分配中心的邮包被挑选出来并被送到那里。在丹佛分配中心，装有生日贺卡的邮包被送往芝加哥，而送往其他城市的邮包也由第三层的人员选择合适的路线分别发送出去。于是第二层的人员就把这里要传送的邮包装在一个集装箱里送往芝加哥。

这一过程在芝加哥重复，第三层的人员把邮包送到分配局，然后将贺卡送到它的目的地。在这个例子中，第一、二、三层使用了中间节点才把邮包送到目的地。网络中实现这三层的就是子网。这个例子只是使用丹佛做中间节点，其他城市或节点也可以被子网用来向芝加哥传送邮包。

2.4.5 OSI 子网

在图2-8中，有三台主机（也称为终端系统）通过三条通信链路互相连接。每一台主机都要同时处理几项任务或应用。为了与其他的主机进行通信，都必须使用子网的三层。

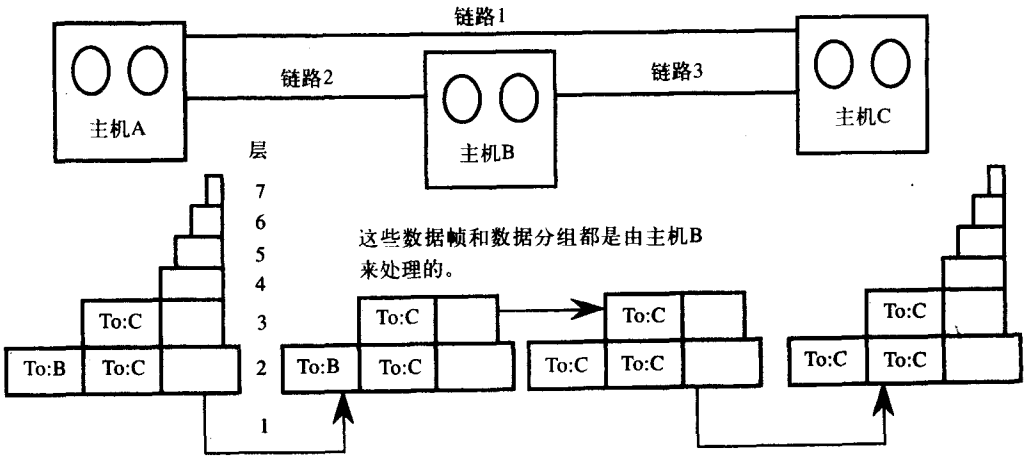


图2-8 主机B在主机A向主机C传送消息时充当分组交换机。箭头表示数据的传输方向

这里，主机A正在向主机C发送数据。主机A的第三层把主机C的目的地址（DA，Destination Address）写入分组中。虽然通信链路1可以直接传输，但这里我们假设由于来自其他应用的业务正在使用这条链路，因而这条通信链路已经被堵塞。这时网络层会选择链路2来传送分组。第二层把主机B的目的地址（DA）写入数据帧，并通过第一层发送出去。

主机B的第二层移走数据帧的头部和尾部，处理数据并检查可能的传输错误。如果确实存在传输错误，就利用帧头部中的地址到达主机A，并请求主机A重传出错的数据帧。一旦收到无差错的数据帧，就将数据部分（分组）转交给第三层。第三层检查主机C的目的地址，重组数据帧然后送回第二层，而不是将数据部分转发给第四层。第二层对主机C的目的地址进行编码，并通过链路3把数据帧发送出去。

如果数据帧由于出现错误而遭到破坏，主机C的数据链路层也会请求主机B进行重传。主机C的网络层在检测是自己的目的地址之后，不再像主机B那样为分组重新选择路由，而是送到第四层。这层的数据最后可以被转送给这台主机的用户。主机B扮演了分组交换机的角色，被叫做中间系统。另外，主机A和主机C是终端系统。

2.4.6 各层的描述

下面根据图2-5描述OSI模型的第一层到第七层。除了物理层之外，其他层都是用软件实现的。

物理层：物理层主要关心的是通过物理链路从一个节点向另一个节点传送比特流，物理链路可能是铜线、卫星、微波或其他的通信媒介。物理层关心的问题有：多少伏电压代表1？多少伏电压代表0？时钟速率是多少？采用全双工还是半双工传输？RS-232端口的电平转换就是物理层协议的例子。总的来说物理层关心的是链路的机械、电气、功能和规程特性。

数据链路层：数据链路层获得从物理层接收的比特，并对它们进行检错。如果出现传输

错误，数据链路层会请求它的对等实体重传数据直到接收无差错为止。错误的检测和纠正简称为差错控制。如果接收端发送的确认帧丢失，发送端就会不断地重复发送数据。删除重复帧也是差错控制的一部分。

除了差错控制，数据链路层还提供**逻辑同步**、流量控制、网络节点的地址转换等服务。在时钟与输入数据流同步之后，接收端必须确定数据帧起始点和结束点。这就是所谓的逻辑同步或区分帧。

数据流量控制是一个过程，通过这个过程接收节点能对发送端实施控制，以确保发送端发出的数据不超过接收端接收数据的能力。有时候，接收端通过不发送确认帧来实现流量控制，强迫发送端在下一次发送前一直处于等待状态。然而，这一层的核心目标还是实现数据的可靠传输。

网络层：当数据链路层把数据分组转发给网络层时，网络层并不关心数据是否有错。正如2.4.3节所讲的那样，这一层要完成路由选择。

再参考图2-8，当主机A的第三层通过主机B向主机C发送分组时，每对主机间的数据链路层检查错误并在必要时重发数据帧。网络层根本不知道某一帧是否必须通过链路进行重传。主机B的网络层只决定分组是否送到主机C，或是否送到主机B的应用层。

除了选择路由之外，网络层还负责建立和维护连接，控制网络上的拥塞以及在必要的时候生成计费信息。X.25就是一个用于网络层的协议，是分组交换网络的具体实现，2.5节将介绍X.25协议。

传输层：如图2-8所示，数据经过一个节点，如主机B时，不会用到传输层。只有数据的源节点（主机A）和目的节点（主机C）使用这一层。上面第四层到第七层被称为端到端层。

传输层把发送消息分成若干个分组，并在接收端对它们进行重组。不同的分组可以通过不同的连接传送到主机B；这样既能获得较高的带宽，又不影响会话层。在建立连接时，传输层可以请求服务质量，该服务质量指定可接受的误码率、延迟量、安全性等参数，还可以实现基于端到端的流量控制功能。

在图2-7中，圣地亚哥的邮件分配中心把许多寄往芝加哥的信件装进一个邮包。传输层可以通过一条通道传送多个终端的对话数据。将多个消息放在一条通道上进行传输的过程被称为**多路复用**。

会话层：会话层管理登入和注销过程。它具体管理两个用户或应用进程之间的对话。如果在某一时刻只允许一个用户执行一项特定的操作，会话层协议就会管理这些操作，如阻止两个用户同时更新数据库中的同一组数据。

假设一个用户通过网络从数据库A向数据库B转账一百美元。如果这一百美元已经从数据库A扣除，而在数据库B中增加一百美元事务处理却丢失了。这时，会话层的职责就是要么把这一百美元退回到数据库A中它原来的位置并向用户发送一条“传送不成功”的消息，要么再次尝试完成转账。

表示层：第六层负责转换文件的记录格式。完成ASCII和EBCDIC字符编码间的转换、数据压缩、在必要时对数据进行加密。还负责终端类型的转换。

应用层：什么是应用？对PC来说，软件应用是一种这样的软件，它决定了用户使用PC的方式。比如有人说他想购买一辆敞篷小货车，所以就在业余时间打零工赚钱。那么为别人做临时工就是一种应用。而这个应用的目的是为了购买小货车。

类似地，网络应用是最初使用网络的原因。无论是召开电视会议、发送医疗图像，还是简单地传送语音，所有这些都是网络应用的例子。

在数据网络的OSI模型中，应用层协议决定了用户如何使用数据网络。

应用层协议可能是X.400，用来提供e-mail服务；也可能是为分布在整个网络上的目录提供目录服务的X.500。这层应用可能还包括完成难题的分解，即用几台主机完成共同的一项大型工作任务。它还能完成分布式数据库的管理。从本质上讲，应用层允许用户基于各种不同的目的使用网络。

2.5 分组交换网络

前面介绍过，X.25是一种协议，是分组交换网络的具体实现，它采用了OSI模型的下面三层。在本节中，将首先讨论这类网络的演进过程，这将有助于对帧中继网、ATM、七号信令系统以及其他组网技术的理解。这些内容是以后各章的基础。对于电信业来说，可以谈论的新技术是那样多，以至于我们常常忽略将网络整合在一起的基本原理。

2.5.1 分组交换网络的工作过程

图2-9a是一个通用的分组交换网络。在该图中，4台主机通过一个有4个分组交换机的网

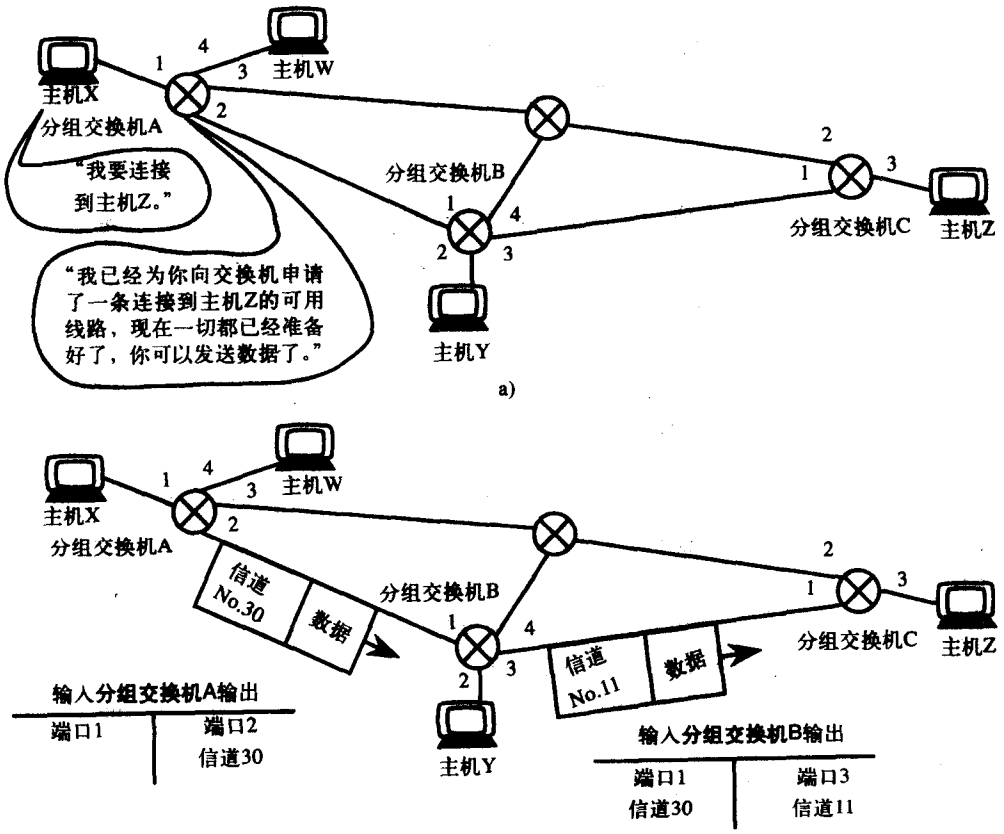


图2-9 a)当主机X请求建立与主机Z的连接时，先发送一个专用分组；
b)为了提供这次连接，分组交换机A、B、C更新它们的转发表

络相互连接。主机X要向主机Z发送数据，所以先向与它相连的分组交换机A发送一个专用分组。分组交换机A决定使用分组交换机B（而不是分组交换机D）来查找到主机Z的路径。类似地，分组交换机B利用分组交换机C来建立通路。在这三个交换机都准备好从主机X接收数据以后，分组交换机A向主机X发送一个专用分组，通知它可以开始传输数据。这样就完成了连接阶段，进入开始传送数据阶段。

图2-9b给出了分组交换机A和分组交换机B的转发表，它们在连接建立以后被更新。分组交换机C增加了一个入口，但在图2-9b中没有画出来。可以看到分组交换机A把从端口1向端口2传送数据分组，在这个分组的头部信道的编号是30。在这条链路上还可能支持其他的连接，每个连接将使用一个不同的信道号。来自主机X和其他主机的几个用户可能请求在这条链路上建立到多个点的连接，信道号可以用来识别一个特定的分组属于哪个连接。

接下来，当分组到达分组交换机B端口1时，交换机B检查它的头部，发现分组的信道号是30。然后，分组交换机B查阅自己的转发表，确定这个分组必须被切换到端口3，并分配一个编号为11的信道。用同样的方式，分组交换机C也会识别出这个分组并将其转发给主机Z。信道号帮助主机Z确定这个分组属于哪个连接。记住，这台主机上可能有几个同时打开的连接使用分组交换机C到主机Z的这条链路。

图2-10a是这个例子的继续，该图显示了一个已经建立的从主机W到主机Y的连接。该图中的转发表表明，分组交换机A在端口2的原有连接和新连接上向分组交换机B发送分组。对分组交换机B来说，确定分组属于哪一个连接的唯一方法是利用分组头部中的信道号。信道号的使用允许一条链路能够支持多个连接。这也是一种**多路复用**方式。每条链路可支持多达4096个复用信道。

2.5.2 虚电路

在分组交换网络中用来完成一次连接的信道号和链路的集合被称为一条**虚电路**。在上面的例子中，已经建立了两个连接，因此形成了两条虚电路，如图2-10b所示。在图2-10b中，我们感兴趣的不是实际的转发表和完成每个连接所需的信道号，所以只画出了两个连接的交换路径或者说是两条虚电路。

假设你正从纽约飞往旧金山，而且必须在芝加哥转机。你在飞机上的座位就如同**信道号**，而飞机则如同分组交换网络中的**物理链路**。通过单独的座位或信道号，每架飞机可被许多乘客“**复用**”。

在芝加哥，机场的工作人员会给你一个登机牌，在登机牌上有下一段旅程的座位号。这位工作人员就如同一个**分组交换机**，把你的座位号从一个换成另一个。在某种意义上说，你去旧金山乘坐的两架飞机和相应的座位号定义了一条虚电路。

图2-10c是删除了实际的链路和交换机之后，分组交换网络的简化形式。用云图代表实际的链路和交换机。此图中只剩下了主机和虚电路。

有两种类型的虚电路：永久虚电路和交换虚电路。永久虚电路（PVC，Permanent Virtual Circuit）一直保留一个特定连接，而不管在这个连接上是否传输业务；交换虚电路（SVC，Switched Virtual Circuit）则更像上面的例子中描述的虚电路。需要时建立交换虚电路的连接，然后在上面传送数据。一旦数据传送完毕，交换虚电路就被断开。然而，永久虚电路也存在这三个阶段，只是需要技术人员来输入建立连接的数据；如果几天或者几个月之后，用户不再需要这条虚电路，连接就被断开。

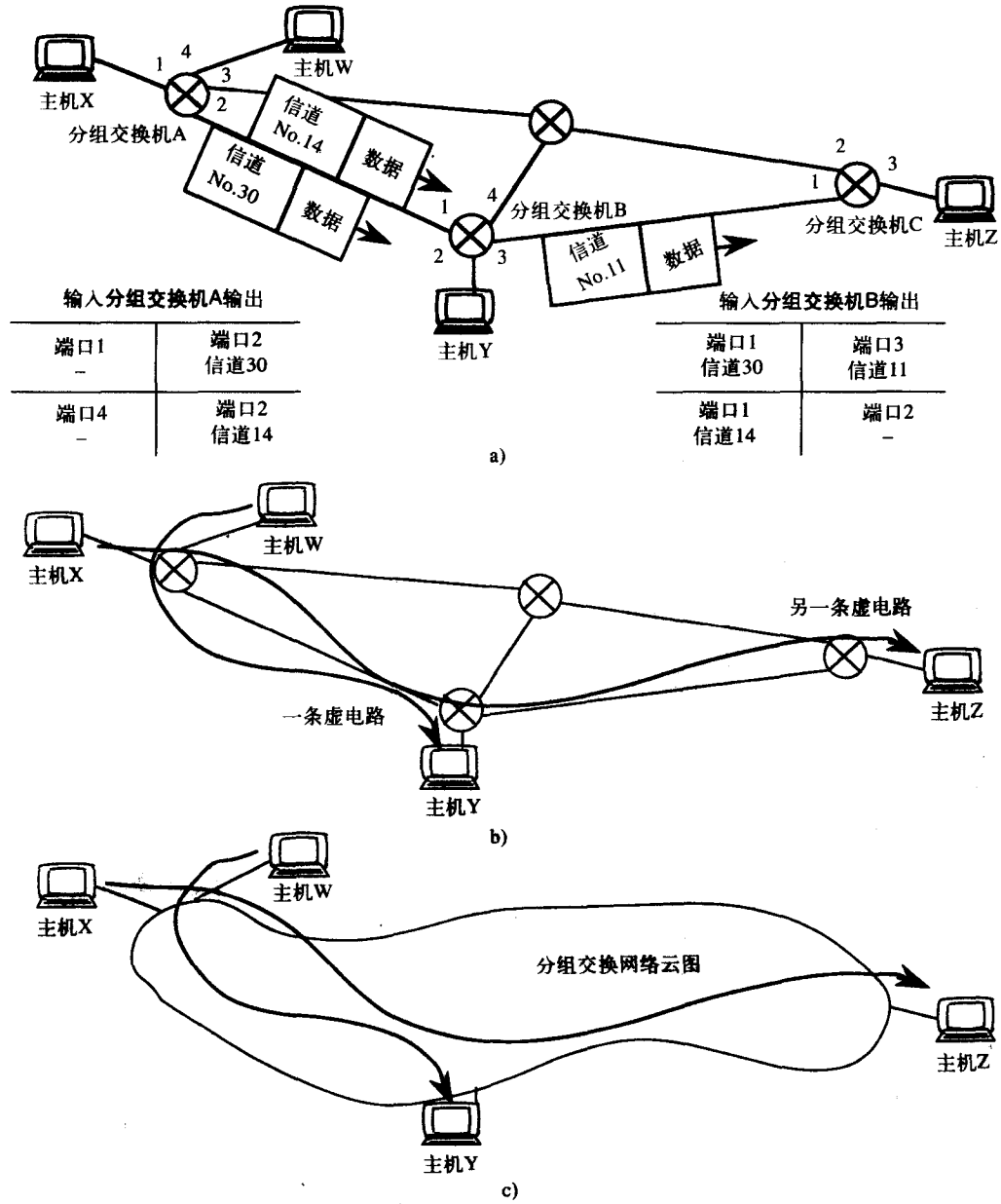


图2-10 a) 建立的另一个连接，b) 虚电路是连接的另一种称谓，c) 云图被用于屏蔽网络的工作细节

2.5.3 分组交换机的职责

在分组交换网络中，发送主机的第四层负责把消息分成若干分组，而接收主机中的第四层则负责把这些分组重新组装起来。分组的被发送次序也是它们的被接收次序，因为它们走的是同一条路径。在图2-10a中，所有的层都可以在主机上实现，但分组交换机只能实现第一层到第三层。如果一条通信链路遭到破坏或一个交换机出现故障，这时就必须通过其他路径重新建立连接，然后重新发送数据。

分组交换机还负责差错控制、流量控制、分组确认、超时重发以及其他基于链路到链路的任务。差错控制意味着检测和纠正错误。如果分组交换机收到一个错误的数据帧，在错误被纠正之前，这个交换机不会把错误帧转发给另一个分组交换机。流量控制是指如果一个分组交换机接收数据帧的速率低于帧到达的速率，它就设法控制发送端的发送速率。如果一些帧已经丢失，在规定的时间内没有到达，接收分组交换机能利用一套规程，与发送交换机一起解决这类超时问题。

2.6 数据报交付网络

在网络上传送数据的另一种方法被称为数据报交付。这种方法相对简单。只需要用一个数据报（而不是五个）就可以解释它的工作过程。数据报就如同分组，但它们在网络上的使用方法不同。通过网络传送时，数据报也常常被称为分组。

在图2-11所示的数据报交付网络中，主机X利用其传输层把一个消息分成两个数据报。这里既没有信道号也没虚电路，主机Z的目的地址被写在数据报的头部中。由于这个原因，数据报可能会经过不同的路径到达主机Z，但可能会出现次序颠倒的情况。这个过程没有建立连接，所以这种网络被称为**无连接**网络。数据只是简单地被送到网络和网络节点上，通称被称为路由器的设备会替数据寻找通往目的站点的路径。路由器使用被称为**路由协议**的特殊协议。路由协议使路由器能够知道网络的物理布局，还能使路由器动态地了解到哪条链路遭到了破坏，哪条链路是新增的，哪条链路的误码倾向越来越严重等等。

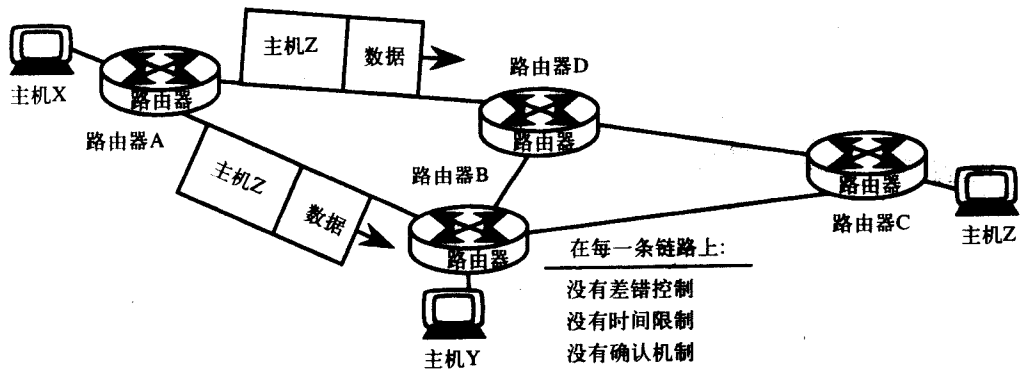


图2-11　通过数据报交付网络传输数据非常简单。数据报中含有最终目的站点的地址

与分组交换网络不同，路由器间没有**数据**检错功能。路由器具有OSI模型下面三层的功能。如果数据报中的数据在到达路由器B时遭到破坏，这个被破坏的数据报还会在网络上传输，最后到达主机Z。这时主机Z的高层，即第四层到第七层，就必须检查和纠正这些错误。

如果数据报的**头部**出现错误，或者存在流量控制问题（数据报到达得太快），或者数据报无法交付，这时路由器就会丢弃这些数据报。另外，终端节点的高层协议必须能解决这些问题，同时还必须能够把次序颠倒的数据报重新组装成原来的消息。注意网络智能是如何从网络节点（交换机或路由器）上被移走的，这种智能仅仅在端点上存在。因此，数据报交付网络被称为不可靠的网络。随着光纤网络的逐渐普及和误码率的逐渐降低，在基于点到点的通信中检错已不是那么重要了。在错误发生率非常低的情况下，为什么还要在所有的链路上检

错呢！由于几乎很少有错误出现，因此只在端点上检查和纠正一次就行了。这使路由器的速度更快，网络本身也更有效。

数据完整性是一个端到端的问题，不是点到点的问题。当决定传送数据到一个目的地的时候，需要由高层建立连接。下面的三层不会知道通过网络正在传送的数据报是同一条消息、会话或连接的一部分。然而，端点的第四层和更高的层会对这些报文进行分类，并了解各种现有的连接和它们的完整性。

本节描述的是Internet。Internet采用的就是这种数据报传递方法。其运行比分组交换网络更好。网际协议（IP，Internet Protocol）是用来传递数据报的协议。路由器可以基于IP协议。传输控制协议（TCP，Transmission Control Protocol）是运行在端点或主机上的第四层协议，它能确保数据的可靠性和先后顺序、连接的建立等。关于这方面的更多知识可参看第8章。

2.7 网络服务

打电话的时候，首先要建立连接，然后才能通话或传送信息。通话结束以后，我们一般是挂上电话或者说是断开连接。接下来，网络会拆除所有分配给这次通话的中继线和交换机连接。这种网络服务称为**面向连接**的服务，它总是采用三个阶段来传送信息。分组交换网络提供面向连接的服务。

相反地，当把一封信投入信箱时，并不需要首先建立一个连接。与IP数据报包含目的站点的IP地址一样，信封上也有目的地址。但投入同一个信箱的两封信到达同样的目的地很可能会经过不同的路线，而且到达的次序也可能颠倒过来，这被叫做**无连接服务**。数据报交付网络，也就是Internet路由器工作的网络，就是一个无连接服务的例子。而TCP为网络用户提供面向连接的服务，它是一种端到端的协议。它使用下层的无连接网络（也就是IP路由器）来提供面向连接的服务。

从图2-12可以看到一个本书后面将要学习的协议清单。这些协议或是无连接的，或是面向连接的。局域网是无连接的，因为从一台主机向另一台主机传送数据帧时，没有事先的连接建立过程，仅仅是在数据帧的头部加入目的站点的地址，然后就将其发送到局域网电缆上。

当一个数据单元，比如说分组通过网络被发送时，一条链路上的信道号定义了这个分组属于哪个连接，这就是前面讨论过的虚连接。然而如果一个连接使用的是一条指定链路，或者在电路路径上用于一个连接的每一条链路和中继线都被预留，则认为存在一个物理连接。在一条物理链路上，不同的连接可以在不同的时间段内传送，这时我们说存在一个时分多路复用（TDM，Time Division Multiplexed）连接。TDM将在第3章讨论，而交换式多兆位数字业务（SMDS，Switched Multimegabit Digital Service）、**异步传输模式**（ATM，Asynchronous Transfer Mode）及其他技术也将在以后的各章中介绍。

服务质量（QoS）：QoS是表征网络性能的一个术语。它是当前新兴网络讨论的热门话题。延时的一致程度与网络提供的QoS有关。QoS的另一个名称称为等时传输服务。

从技术上讲，延时本身并不影响QoS，但是报文其他各部分之间的延时关系却对QoS有影响。如在体育比赛的电视卫星传送过程中，从比赛发生时间到在电视上显示虽然存在一个定量的延时，但是这种业务却有很好的QoS。但是如果转播连续比赛时传输延时不稳定，这种传输的QoS就很差。语音和视频传输对延时的一致性要求很高，但却能容忍一些传输误差存在。相反地，数据传输对QoS要求不高，但却不能接受比特差错。

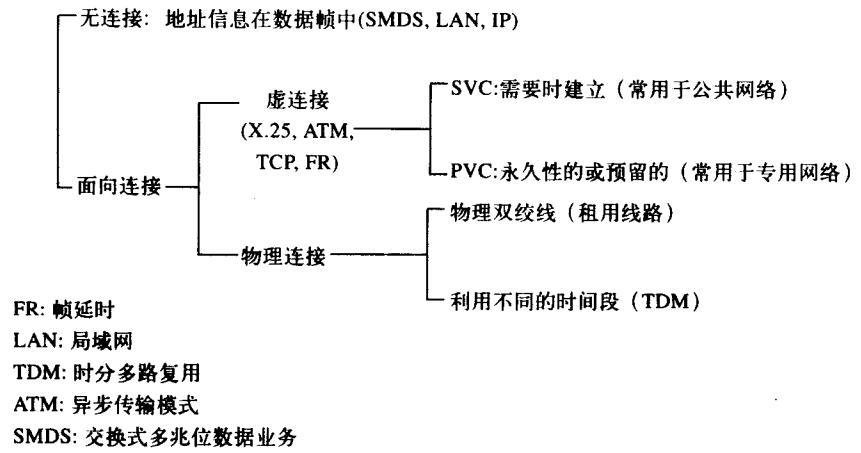


图2-12　通信业务的类型

隧道技术和封装：网络还提供一种被称为隧道的服务。隧道技术采用一种称为封装的机制，要把一种协议的数据传送单元装在另外一种不同的协议里。

很多时候可能需要创建一种特殊的网络，但是我们拥有的却是另外一种类型的网络。如何在现有的网络上使用不兼容的设备开展工作呢？一个答案就是采用隧道或封装技术。隧道技术允许我们用一种网络来传送一种特定类型的帧，而这个网络使用的却是其他类型的数据帧。

从2-13a可以看到，在两台主机之间有一条标准的X.25链路。在图的左边，X.25发送端把应用数据装进X.25的分组内进行传送。然后，这个分组被装入数据帧中并通过一条标准的X.25链路传送。在图2-13b中，碰巧没有可用的X.25链路，只有Internet链路。这时通过将数据

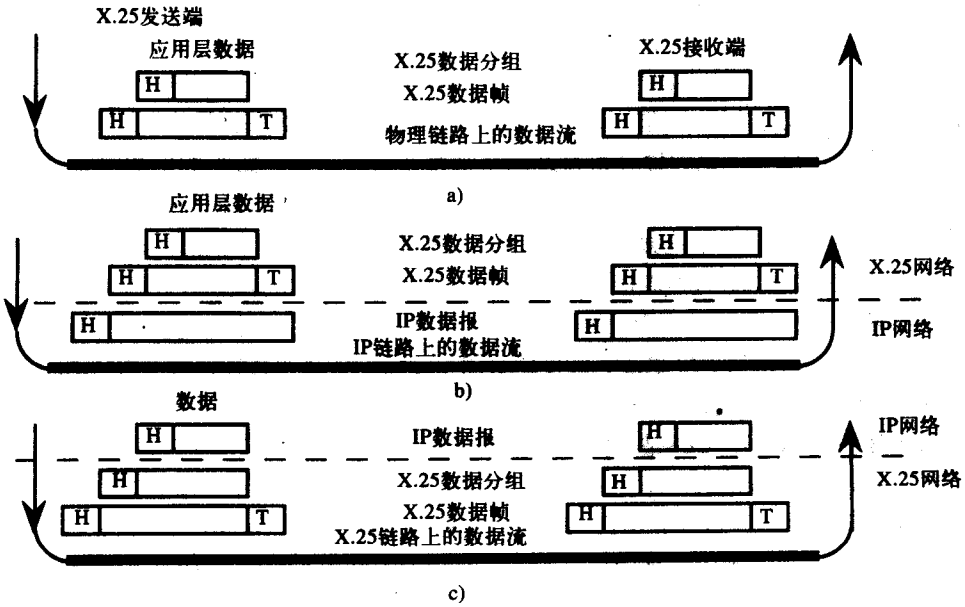


图2-13　a) 纯X.25网络；b) 使用IP隧道的X.25网络，或者说是把X.25的数据帧封装到IP数据报中；c) 把IP数据报封装到X.25协议中

帧封装在IP数据报中，可以让X.25主机认为与以前一样下面还是X.25链路。在这里，X.25帧被封装或密封在IP数据报中并通过Internet传送到接收端的X.25主机。对于X.25主机而言，并不在意X.25协议是否通过了IP隧道，它只负责发送和接收X.25分组。而对于X.25网络而言，只是使用IP网络来传送它的数据帧。而对于IP网络而言，X.25数据帧不过是应用数据罢了。

当然，这里还需要特定的软件来把X.25数据帧封装在IP数据报中。这种软件增加一个额外的网络协议层来处理信息的发送和接收，致使X.25网络比图2-13a中的网络运行得慢。但是如果不需要增加新链路就可以承载X.25业务，牺牲一点响应速度是值得的。如果能够跳过X.25数据链路层，把X.25分组直接封装在IP数据报中，那么只需替换现有的网络层，而不是增加一个网络层，这无疑会改善整个网络的性能。将一个协议封装在另一个协议里的隧道技术在许多网络中都被采用。图2-13c是颠倒过来的例子。在这里，IP业务通过X.25网络传送。IP数据报被封装在X.25分组中，或者说IP通过X.25隧道。

习题

2.1 和 2.2节

1. 下面哪一个选项不是联网的理由？
   a. 容易访问共享资源　b. 增加可靠性　c. 良好的安全性　d. 成员的灵活性
2. 通过在网络上分摊工作量，减少了下面哪一类问题？
   a. 自治主机　b. 安全性　c. 瓶颈　d. 容易与主机连接
3. 用你自己的话给网络下一个定义。
4. 网络怎样分类？描述这些类型。
5. 描述那些所谓的高性价比网络的优点。
6. 如果局域网内的所有用户都可以使用某软件，是利用了组网的哪一个优点？
7. 如果有人进入我的办公室，用我的计算机检查存储在他自己计算机上的文件，他利用了组网的哪一个优点？
8. 讨论为什么网络安装便宜，运行昂贵？

2.3节

9. 由相邻层提供的服务被称为什么？
   a. 接口　b. 协议　c. 虚连接　d. 网络体系结构
10. 下面哪一项不是网络体系结构的例子？
    a. SNA　b. DECnet　c. FEP　d. APPN
11. 用在一层中的规则被称为什么？
12. 采用分层的方法设计网络很重要，因为所有的网络都是这样设计的。为什么？
13. 哪种类型的通信由网络体系结构的高层完成？

2.4节

14. 哪一层负责把报文变成分组？
    a. 网络层　b. 传输层　c. 会话层　d. 表示层
15. 哪一层负责纠错和创建数据帧？
    a. 数据链路层　b. 网络层　c. 传输层　d. 会话层
16. 哪一层的PDU是帧？

a. 数据链路层　　b. 网络层　　c. 传输层　　d. 物理层

17. 网络层使用的传送单元是什么?

18. X.400是哪一层协议的例子?

19. 当数据从应用层向下传到物理层时，PDU是变大了还是变小了?

20. 只使用OSI模型下面三层的网络叫什么?

21. 某事物如何使用被称为_____。

22. 描述数据在OSI各层上下移动的过程和发生在水平对等层之间的虚拟通信。

23. 描述通信子网。

24. 列出数据链路层的功能。

2.5节

25. 下面哪一种网络不采用分组交换?

a. ATM　　b. LAN　　c. X.25　　d. SS7

26. 在数据能够通过分组交换网络传输之前，必须完成下面哪一项工作?

a. 必须建立一个连接。

b.数据的接收端必须先请求一个连接。

c.数据分组必须插入到分组交换机的转发表中。

d.必须在网络的每一条链路上分配相同的信道号。

27. 在一个分组交换网络中，几个连接的通信可以在同一条链路上进行，这被称为什么?

28. 当分组交换机B在端口1接收到一个分组后，它必须采取什么样的步骤来处理这个分组?

29. 描述虚电路PVC和SVC。

30. 如图2-10a所示，如果主机X和主机Z之间的连接被断开，然后要在主机X和主机Y之间建立一个新的连接，每条链路上使用的信道号是22，给出各转发表的内容。

31. 利用图2-14的转发表和图2-10b给出的网络，描述由此建立的虚电路。

输入分组交换机A 输出

输入	输出
端口4 –	端口1 信道10
端口2 信道30	端口4 –
端口1 –	端口2 信道50

输入分组交换机B 输出

输入	输出
端口3 信道20	端口1 信道30
端口1 信道50	端口2 –

输入分组交换机C 输出

输入	输出
端口3 –	端口1 信道20

图2-14　31题的转发表

2.6节

32. 数据报交付网络提供下面哪一种类型的网络服务?

a. 固定路径　　b. 面向连接　　c. 服务质量　　d. 无连接

33. 下面哪一个是数据报交付网络的例子?

a. Internet　　b. SS7　　c. PSTN　　d. ATM

34. 数据报是否可以通过不同的路径传输?

35. 如果数据报到达得太快，路由器如何处理?

36. 数据报交付网络使用什么设备来完成分组交换网络中分组交换机的功能?

37. 数据报与X.25协议中使用的分组之间的区别是什么？

2.7 节

38. 下面哪一个是面向连接的协议？

a. ATM b. LAN c. 把一封信投入信箱 d. IP

39. 下面哪一类服务在新兴的网络中已经变得很重要？

a. 连通性 b. 隧道技术 c. 封装技术 d. 服务质量

40. 描述使用隧道技术的目的。

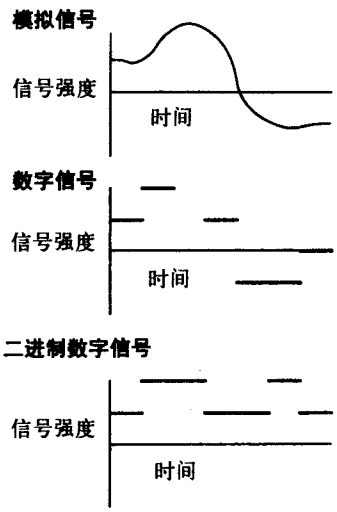
第3章 模拟信号和数字信号

接下来的几章将学习不同的传输方式和各种网络用户可用的服务。为了理解和掌握它们的优点和局限性，首先需要学习模拟信号和数字信号的基本特性。理解了这些概念有助于回答通信原理中的许多“为什么”。由于不懂网络链路上驱动比特流的技术背后的基本概念，许多网络专业人员都处于被动地位。在本章中，将讨论许多与模拟信号和数字信号概念有关的术语。在本书中这些术语会重复出现，所以在这里要花一点时间来解释它们。

3.1 信号类型

模拟信号有一个连续的信号强度的集合。模拟信号可以任意增加或减小强度的数值，而数字信号却不能。数字信号的强度只能增加或减少固定的数值，只存在一些离散的幅度电平值。离散数集合是这样一些数的集合，这些数不是连续的，彼此互不相同，且个数是可数的。连续数集合中数的个数是不可数的，比如模拟信号电平的个数可以有无穷多个。

举例来说，0~9之间的整数的个数是10；而0~9之间的小数却有无穷多个，是不可数的。在0~9之间，有离散的整数，也有连续的实数和小数。物理学家认为电子所能占有的能级是离散的。激发一个电子，它会从一个能级跃变到另一个能级。电子的能级不能逐渐增加。自然界中的粒子能级被认为是数字的。然而，人耳朵里的鼓膜可以感受到幅度连续变化的空气压力波。因此，鼓膜是模拟“设备”。事实上，“模拟信号”源于这样一个事实：电信号模拟了可以被耳朵“听到”的空气压力波（由声音产生）。



在右面的第一幅图是一个强度沿时间变化的模拟信号，其强度变化是连续的。餐厅中的调光灯是模拟设备的一个例子。在模拟信号的下面，是一个数字信号，它具有几个不同信号强度的电平。汽车的前灯开关就是一个3档数字开关的例子：开、关和强光。最后一幅图是一个二进制数字信号，它只有两个信号强度。人们总是错误地认为数字信号就是二进制数字信号。从理论上讲，一个数字信号不仅可以拥有两个信号电平，还可以拥有多个信号电平。二进制数字信号的电平只能有两个，或者都是正的，或者一个正和一个负，或者是其他的组合。闪光灯的开关就是一种二进制设备。

3.2 直流电路

3.2.1 欧姆定律

下面讨论电信号和它们的各种特性。电信号的强度用V（伏特）来测量。

在给定的时间间隔里，直流（DC，Direct Current）电压保持一个恒定的电压值，如图3-1a所示。在这里，不论时间如何变化，电压强度始终保持恒定。将示波器的探头接在直流电压源的两端，可以看到示波器的显示。这时，水平坐标轴表示时间，垂直坐标轴则表示电压，如图3-1b所示。闪光灯和汽车的电池都是直流电压源的例子。

此外，图3-1c给出了一个交流（AC，Alternating Current）电压源。该电源电压的变化范围是－10V到+10V。例如，t=0.5s时，电压是+10V；t=1.0s时，电压是0V；而t=1.5s时，电压变为－10V。交流电压的值在正电压和负电压之间来回变化。家用照明电源是一个交流电压的例子，它的有效值为120V。图3-1d和图3-1e分别给出了直流电源和交流电源的表示符号。

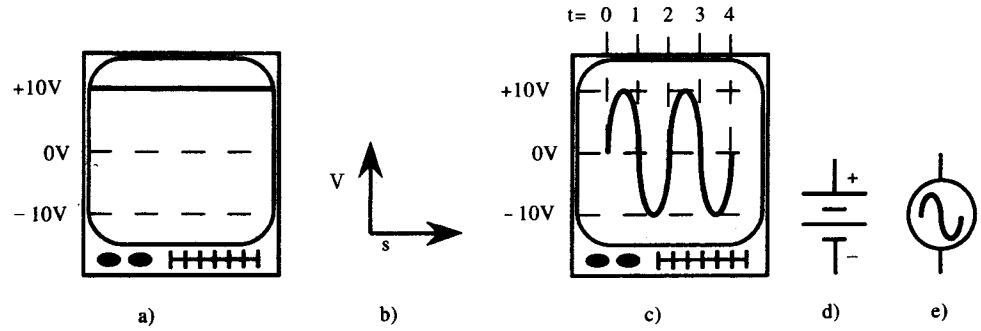


图3-1 a) 直流电压，b) 示波器坐标轴标识，c) 交流电压，d) 直流电源符号，e) 交流电源符号

图3-2给出了一个直流电源与一盏灯连接的示意图。电阻表示对电流的阻碍量。可以人为地在电路中加入电阻，但连接导线、灯泡甚至是电池都可能会存在固定的电阻。电阻的单位是Ω（欧姆）。如果开关断开，电路中没有电流流动；开关闭合，电路中才有电流流过。当开关断开和闭合的时候，灯泡相应地会灭和亮。如果电阻增大，电流会变小。电流的大小由欧姆定律决定：

$$V=IR$$

在这里，V表示电压，I表示电流，R则代表电阻。它们的单位分别是V、A（安培）和Ω。例如，如果电源电压是10V，R是20Ω，那么电流就等于0.5A。

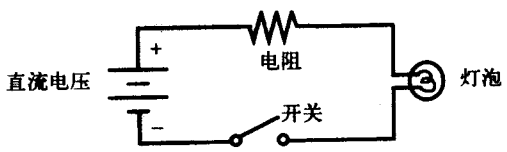


图3-2 当开关闭合时，电流流过，灯泡发光

在图3-3a中，一个10V的直流电压源加在两个电阻上。如果两个电阻的阻值分别为20Ω和30Ω，那么电路的总电阻是50Ω。根据欧姆定律，可以得到电流为0.2A，它流过电路中的所有元件。如果用每个电阻的阻值乘上这个电流，就得到了两个电阻上的电压，分别为4V和6V。用示波器测量$R2$上的电压，结果显示在图中。

现在，如同图3-3b那样断开开关，电路的电流为0。由于必须有电流才能将电压加在电阻的两端，因此这时两个电阻上的电压也为0。注意如果把示波器的探头接在$R2$两端，电压的读数为0V；如果把探头接到断开的开关两端，读数却是10V，因为这时尽管电路中没有电流，但实际测量的是电源两端的电压。

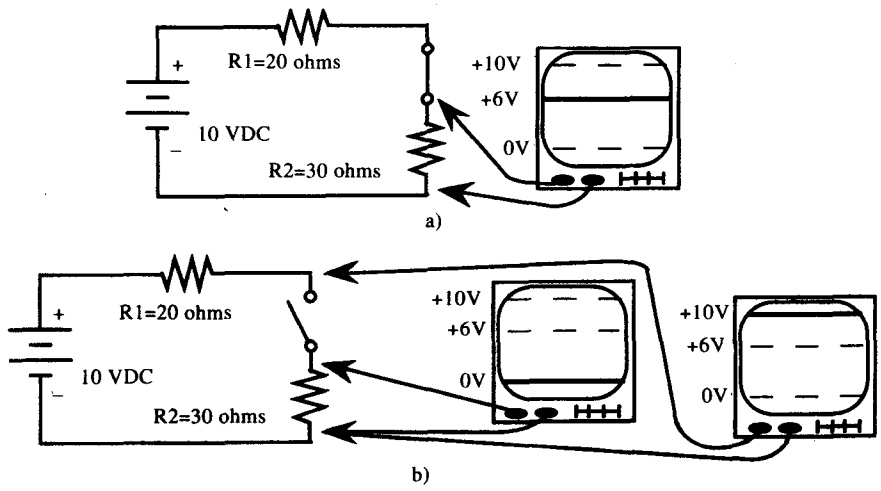


图3-3　a) 当有电流流过时，*R*2上的电压为6V；b) 没有电流的时候，*R*2上的电压为0V，而开关两端却有10V的电压

3.2.2　数字信号

如果在开关闭合的瞬间观察示波器的显示（示波器探头接在*R*2两端），会发现*R*2上的电压从0V跳变到6V，如图3-4a所示。同样在开关断开的那一瞬间，示波器的显示如图3-4b所示。我们把开关闭合（6V）的状态称为二进制的1电平，把开关断开（0V）的状态称为二进制的0电平。二进制电平也被称为逻辑电平，只有两种状态——0和1。

仅有两个电压电平的信号是数字信号的一个例子，而电平连续变化的信号则被称为模拟信号。前面的图3-1c所示的信号就是一个模拟信号的例子。

如果重复地闭合、断开开关，可得到图3-4c所示的波形；如果提高开关状态转变的速度，就能得到图3-4d所示的波形。图3-4d中的波形比图3-4c中的波形频率更高。

计算机的时钟是数字信号的一个例子，它的变化速度是均匀的，或者说是周期性的，如图3-4c和图3-4d所示。计算机的时钟不传送信息，只是以均匀的增量标识时间，以保持计算机各部分的同步。因此时钟被看作是计算机的“心跳”。

与时钟相反，图3-4e中显示的数字信号在0和1之间的时间间隔不是均匀的，或者说不是周期性的。这种不均匀的时间间隔可以用于信息编码，以便语音、数据、视频、图像等信号可以数字化地传输。

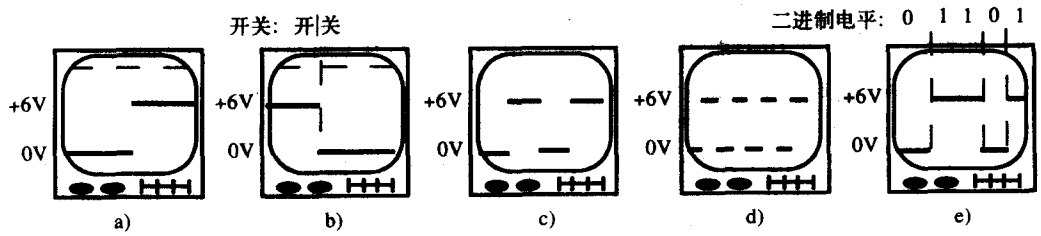


图3-4　a) 开关闭合，b) 开关断开，c) 时钟信号，d) 提高时钟频率，e) 另一种数字信号

3.2.3 幻象供电

许多数字传输线路都需要一种称为再生器的设备。再生器的作用是对差数字信号进行整形再生，并将整形再生后的信号转发出去。为了给这个通常安装在远端的设备供电，传送数字信号的线路还必须用来传送供电电压，这被称为幻象供电。

图3-5给出了这样的一个电路，其中的电阻代表传输线的电阻。电压电源加在被传送的数字信号上面。通过示波器可以看到，在任一时刻都有一个至少10V的电压可用作电源。在10V上面，“骑”着需要传送信息的数字信号。再生器能从10V电压中将数字信号分离出来。10V电压用作电源，而数字信号则被再生器转发。因此，这种传输系统允许在传送信息的同时为在线再生器供电。

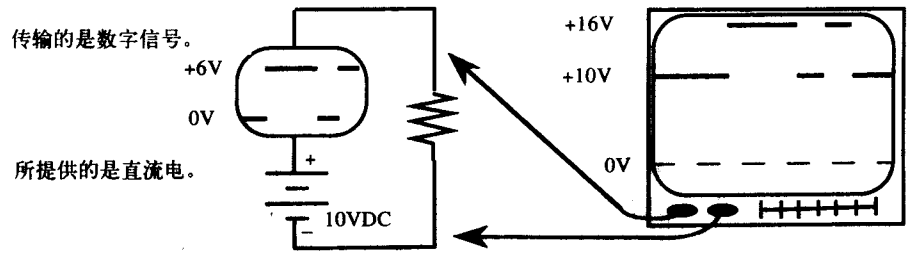


图3-5 幻象供电

3.3 模拟信号

图3-6a给出了一个模拟信号和它的三个参数。幅度是信号的强度，用伏特来测量。图3-6b是信号强度变小的情况，我们减小收音机的音量时就是这样。

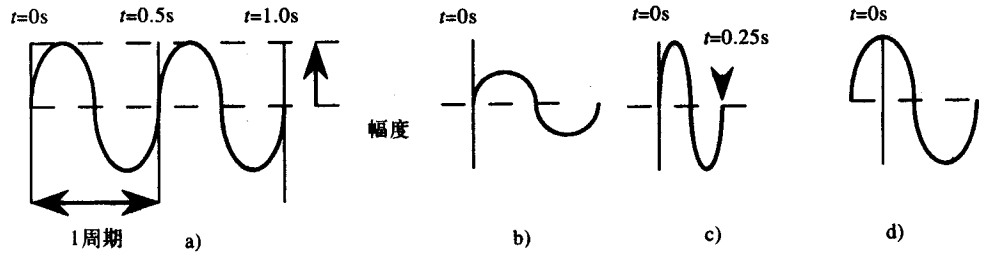


图3-6 模拟信号可以变化的三个参数

周期是信号的另一个特性，它与频率互为倒数。在图3-6a中，信号周期是0.5秒，用重复波形所占用的时间来测量。为了计算频率，只需简单地用0.5秒去除1，得到每秒两个周期。图3-6c是信号周期减半到0.25秒时的波形，这时频率加倍到每秒四个周期。Hz是用来测量每秒内周期数量的单位。举个例子说，当演奏比前一个音符高八度的音符时，频率将会加倍。频率决定了信号的音调。

信号的时间位置由相位给出，相位用度来测量。只有在与一个参考点进行比较的时候，信号的相角才有意义。图3-6d所示的信号比图3-6a中的信号出现得早，所以有一个正角度的相位偏移。

3.3.1 调制

在一个高频信号上对一个低频信息信号进行编码被称为**调制**。可以通过改变前面描述过

的一项或多项信号参数来完成编码。注意“**调制**”和“**改变**”具有相似性。例如，一个音频信号（人耳听得见的信号）可以用来改变一个射频（RF，Radio Frequency）载波。当射频信号的幅度随音频信号的幅度变化时，被称为幅度调制（AM，Amplitude Modulation）；当射频信号的频率随音频信号的幅度变化时，被称为频率调制（FM，Frequency Modulation），如图3-7a所示。AM和FM都是广播电台采用的调制方式。

图3-7b是对一个数字信号分别进行幅度和频率调制。调制方式的变化通常与在模拟线路上传送数字信号的调制解调器有关。在这里，为了能够利用语音线路传送数字信号，载波必须是音频，而不能是射频。

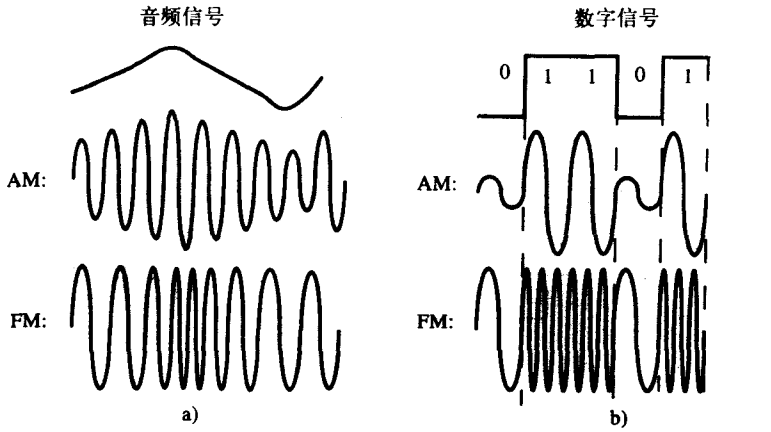


图3-7　a) 在射频载波上调制一个音频信号，b) 在音频载波上调制一个数字信号

3.3.2　电容器和电感器

一个电容器不过是两个互相靠近、但不相互接触的导体。它在电场中储存能量，其效果用法拉来衡量。电容器让交流信号通过，但不让直流信号通过。

两条电话线之间不必要的耦合电容可能导致从一对电话线上能够听到另一对电话线上的通话。这种情况被称为**串话**（crosstalk）。发生这种现象的原因在于两条电话线是彼此分开的导体，只是用产生电容的绝缘体进行了隔离，而语音又恰恰是电线的耦合电容允许通过的模拟信号，所以就出现了串话。

为了补偿这种分布电容的影响，通常把电线互相绞合起来引入所谓的**电感效应**（inductive effect）。因为电感器也能产生电感效应，所以这种效应在本质上对电容有抵消作用。在实际中，是缠绕导线来制作电感器；为了增加电感量，常常把线圈缠绕在磁铁上。因此，电感器也被称为线圈。电感器的量度单位是亨利（henry）。它在磁场中储存能量，允许直流信号通过，阻止交流信号通过。

当电话线的长度超过三英里的时候，必须增加电感器来进一步补偿电容的影响。这种电感器被称为**负载线圈**。当在这种电话线上传输数字信号时，必须先去掉负载线圈，因为它们不适合数字信号的传输。根据微积分学的傅里叶分析，数字信号电压的尖锐的上升沿和下降沿实际上是由许多高频分量组成的，而电感器会阻止这些高频分量通过。电子工程师告诉我们在长途电话线上传输模拟信号时，负载线圈是必需的；但是在传送数字信号时必须把它们去掉。因此当模拟线路被转换成数字线路时，通常用数字再生器代替负载线圈。

3.3.3 低通滤波器

在图3-8a的电路中有一个电容器，其频率响应曲线如图3-8b所示。频率响应曲线与示波器显示有什么不同呢？原来，示波器以时间（秒）作为水平坐标轴，而频率响应曲线则是以频率作为水平坐标轴。改变交流电源的频率，就可以画出频率响应曲线上各点的电压。图3-8b给出了这条曲线上三个点的示波器显示波形。靠近示波器显示波形的分别是低频和高频等效电路。在瞬时频率点上，图3-8a中的电路与等效电路相类似。

在频率接近0时，这个电源似乎就是一个直流电源，因为直流电源能提供一个恒定的电压，正如在低频等效电路中看到的那样，电容器阻止直流通过，电路断开，因此全部电压都加在断开电路的两端，与图3-3b非常相似。

当频率很高的时候，这个电源就好像是一个交流电源；前面提到过，电容器允许交流通过，因此就如同电容器被短路了一样；如高频等效电路所示。由于加在短路元件上的电压为0，因此在高频时电容器上没有电压。

现在已经知道，这个电路低频时在电容器上输出一个电压，而在高频时几乎没有电压；因此这个电路被称为低通滤波器。这种滤波器允许低频信号通过，阻止高频信号通过。

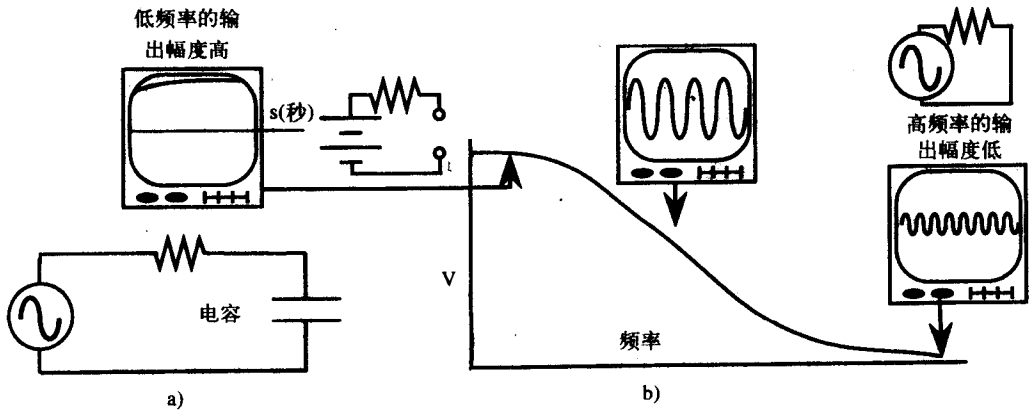


图3-8 a) 一个低通滤波器；b) 它的频率响应曲线，示波器上显示的是曲线上几个点的波形

3.3.4 带宽

在图3-8a中加上一个电感，得到图3-9a所示的电路。这个电路被称为带通滤波器，因为它只允许某一段频率的信号通过，阻止其他频率的信号。它的频率响应曲线如图3-9b所示。

当工程师设计一个放大器或扬声器时，他们试图使频率响应曲线平坦。也就是说，他们设法使某个范围内的所有频率均匀地通过；而不是对一组频率进行放大，而对另一组频率不进行放大。用户也能利用均衡器实现这样的功能。

一个设备或传输媒介允许通过的频率范围被称为带宽。音频设备的带宽在20kHz左右，而语音级线路的带宽仅有大约3kHz。电台音乐节目主持人所发出的语音质量与通过电话线接入到广播电台的听众所发出的语音质量相比，带宽存在明显的差异。在数字传输中，带宽是指每秒传送的比特数或可用的传输容量数。

在谈到模拟信号的带宽和数字信号的带宽时，很容易把它们混为一谈。模拟信号带宽的单位是Hz，而数字信号带宽则用bps（比特/秒）测量。例如对于模拟信号而言，一条普通电

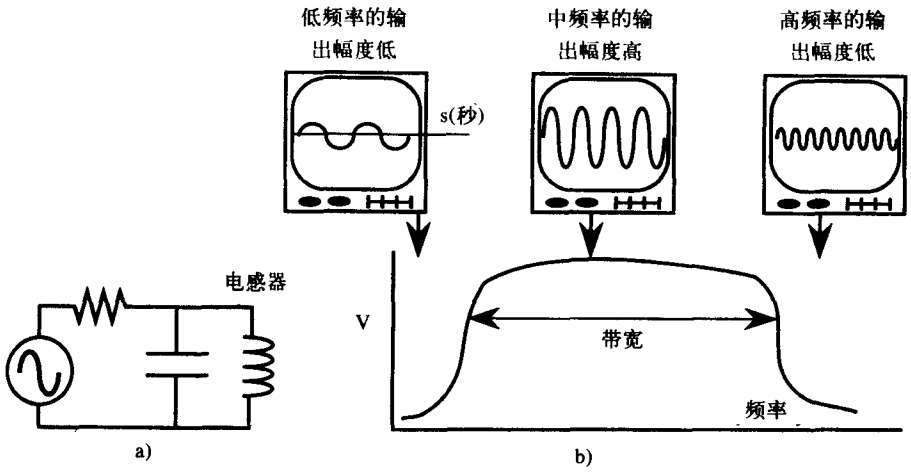


图3-9　a) 带通滤波器，b) 它的频率响应曲线

话线的带宽是4kHz。管理电话线的设备使用这个带宽处理模拟信号。但如果在这条线上安装一个调制解调器并发送数字信号，则这条线能提供56kbps的带宽（通常，小写的b代表比特，而大写的B则代表字节。例如，56kbps指56千比特每秒，而4MB是指4兆字节）。如果增加一个模拟传输信道的带宽，比如说使用同轴电缆，那么对于一个带宽是6MHz的模拟传输信道，数字带宽可以从10Mbps到40Mbps，这取决于具体的编码方式。模拟带宽的数量可以决定从一个传输设备上获得多少数字带宽。

3.3.5　公制单位前缀

现在是总结公制单位前缀的最佳时刻。表3-1是常用的公制单位前缀。第一列是前缀的缩写，中间一列是这些前缀的含义，最后一列是每一个前缀所代表的10的幂指数。例如对于700kHz，它与700（10^{+3}）Hz或700 000Hz相等。只是用前缀（k）替换10的3次幂，或10^{+3}。另一个例子，200毫秒等于200（10^{-3}）秒，或0.2秒。

表3-1　公制单位前缀

前　缀	含　义	数值（10的幂次）
T	tera	+12
G	giga	+9
M	mega	+6
k	kilo	+3
–	–	0
m	milli	-3
μ	micro	-6
n	nano	-9
p	pico	-12

3.4　功率

3.4.1　*P=VI*

功率方程式与欧姆定律（*V=IR*）相似，定义如下：

$$P=VI$$

这里P代表功率，单位是W（瓦特）；V和I则是欧姆定律中用到的常用变量：电压和电流。

回到图3-3a，在电路中的电阻$R1$上加4V的电压，在电阻$R2$上加6V电压，可以得到0.2A的电流。为了计算$R1$上消耗的功率，只需简单地用$R1$上的电压乘以电流，计算得0.8W（4V × 0.2A）。同样地，在$R2$上消耗1.2W（6V × 0.2A）的功率。由于这两个元件总共消耗了2W的功率，所以电源必须能够提供这个数量的功率。

假设有一个额定功率为1200W的吹风机，插在120V的住宅交流电源上。这个吹风机必须使用10A的电流，这个结果是通过把已知变量代入功率方程式，计算I得到。

3.4.2 分贝

贝尔除了发明电话之外，还做过一些工作帮助那些听力失聪的人们。他注意到人耳能按对数规律检测声音的变化。随后，他用对数定义了一个被称为分贝的单位。在电信领域，这个单位用来计算功率。让我们先来复习一下对数，然后再继续讨论分贝。

对数：log是对10的幂求反，在方法上就如同对平方求反出现了平方根一样。如果写成：

$$10^X = 1000$$

就是要计算10自乘多少次才能得到1000？答案（或X）是3。我们也可以在等式的两边取对数得到同样的答案。

$$\log(10^X)= \log(1000)$$

就好像求平方根是把一个数的平方还原成这个数本身一样，求10^X的对数是要把10^X简单还原成X。在上式中，可以认为等式左边以10为底的对数被去掉了，尽管理论家可能不喜欢使用“去掉”这个词。这样问题现在被简化为：

$$X = \log(1000)$$

现在如果用计算器计算的话，会发现1000的对数的确是3。

分贝（dB）：分贝是指功率电平之间的**差异**，不代表绝对功率。分贝的定义如下：

$$\text{dB} = 10 \log(P2 / P1)$$

其中$P1$和$P2$是被比较的、以瓦特（W）为单位的两个功率电平。图3-10是由3个放大器和1个滤波器组成的四级设备，每一点的功率均被标在图中。可以用计算器求对数来计算前3级的增益。

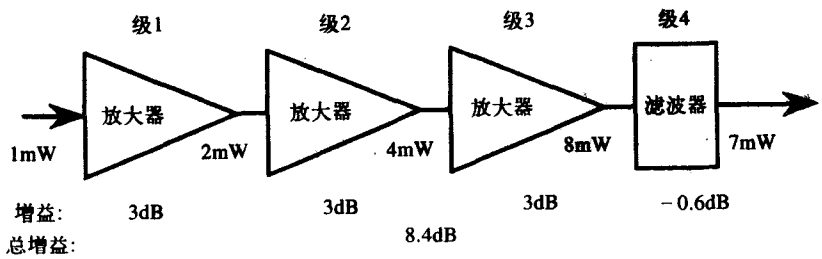


图3-10 功率电平不同的4级放大器

利用公式：对于第一级，$P1$为1mW（毫瓦），$P2$为2mW。将$P1$和$P2$代入方程，得到：

$$\text{dB} = 10 \log(2 / 1)= 10 \log 2 =10(0.3)= 3 \text{ dB}$$

因此第一级的增益是3dB。对于第二级，增益也是3dB:

$$dB = 10 \log(4 / 2) = 10 \log 2 = 10(0.3) = 3\ dB$$

从这两个结果可以看到，只要功率增加一倍，这一级的增益就是3dB。所以第三级的增益一定也是3dB。

累计分贝数：现在计算几级加起来的总增益。例如，对于第一级和第二级的组合增益为:

$$dB = 10 \log(4 / 1) = 10 \log 4 = 10(0.6) = 6\ dB$$

这里$P2$等于4mW，是第1级和第2级两级的总输出；$P1$等于1mW，是第1级和第2级两级的总输入。在计算中我们把前两级组合在了一起。同样地，前三级的增益为:

$$dB = 10 \log(8 / 1) = 10 \log 8 = 10(0.9) = 9\ dB$$

从上面的计算可以很明显地看出，如果我们知道每一级的增益，把它们加起来就可以得到它们的组合增益。

负分贝：当输出功率减少时，如第四级那样，增益的分贝值就变为负数。可以通过计算第四级的增益来证实这一点:

$$dB = 10 \log(7 / 8) = 10(-0.06) = -0.6\ dB$$

毫瓦分贝（dBm）：dB用来表示功率的比值，而单位dBm则用来表示实际或绝对功率。如果输入功率以1mW为参考，计算如下:

$$dBm = 10 \log(P2 / 1mW)$$

因此，第一级的输入功率电平为:

$$dBm = 10 \log(1mW / 1mW) = 10 \log(1) = 10(0) = 0\ dBm$$

而第一级的输出功率则为:

$$dBm = 10 \log(2mW / 1mW) = 10 \log(2) = 10(0.3) = 3\ dBm$$

3.5 同步

从本节开始，我们将更深入地学习数字信号的原理。当传输数字信号时，特别是在数据传输速率越来越快的今天，同步是最基本的问题。只有实现了同步，才能传输数据。

3.5.1 三种类型的同步

一个设备在接收数据流时，首先必须准确地判断每个比特的开始位置，这被称为**比特同步**（也称位同步）。一旦能够准确地判断每个比特开始和结束的时间，接下来就必须知道这些比特是如何被分组构成八位组的，或哪一位是一个八位组的第一个比特，这被称为**字符同步**。判断出八位组之后，它还必须能够判断出哪些八位组构成了地址段，哪些八位组构成了数据段，等等，这被称为**逻辑同步**（或帧同步）；尽管也可以由硬件完成，但通常这些工作都是由OSI模型的第二层来处理的。

3.5.2 异步通信

比特同步和字符同步可以由异步或同步通信建立。图3-11a描述的是异步通信。没有数据传输时，线路空闲；当准备传送一个字符时，首先发送一个起始比特。起始比特中的电压突

变通知接收端正在发送一个字符；在发送完数据比特以后，还会发送一个停止比特。接收端的内部时钟利用起始比特中的电压跳变来建立与接收信号的定时同步。

异步传输方式允许随机地传送字符，因为每个字符都带有同步信息，但每次只能传送一个字符。

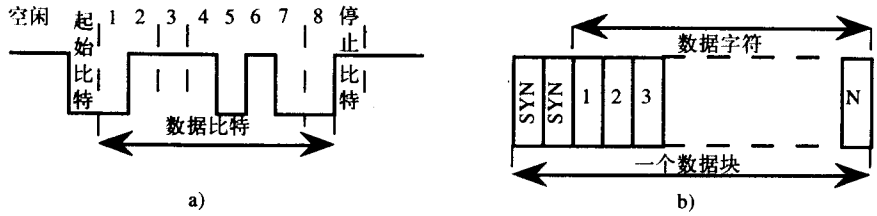


图3-11 a) 异步通信，b) 同步通信

3.5.3 同步通信

如图3-11b所示，同步通信比异步通信更有效。与异步通信每次只传送一个字符不同，它每次传送一个数据块并在每个数据块的开头放置SYN字符来提供同步。由于成组发送字符，因此同步通信需要比异步通信更大的缓冲区。

在同步通信中，数据中常发生的电平跳变被用来维持接收时钟的同步。如果出现太多的连续相同比特（连0或连1），时钟就可能发生偏移。这时必须进行适当的调节，以保持时钟同步。

异步终端的一般速率是300bps到19 200bps，而同步终端的一般速率则为19.2kbps到大约1Mbps。

3.5.4 STM与ATM

这里讨论的同步传输模式（STM，Synchronous Transmission Mode）和异步传输模式（ATM，Asynchronous Transmission Mode）是与同步和异步传输无关的术语。对于STM，不论是否需要，每个输入信道都会被分配一个用来传送数据的时间片。为了发送数据，每个信道要依次占用自己的时间片。如果一个信道在属于它的时间片到来时没有数据发送，那么这段时间就被浪费了。对于STM，接收端知道比特将以规则的时间间隔到达。本章将要讨论的时分复用（TDM，Time Division Multiplexing）就是基于STM的。至于ATM，比特在通过网络传送后到达接收端。在ATM系统中，接收终端可能在某个时刻连续收到多个数据比特，而在另一个时刻，它又可能必须等待。ATM将在后面的章节被讨论。

ATM的部分用途是调节**实时**（isochronous）业务。实时业务意味着对任何等待时间或延时是敏感的。如果在接收时，一个从主机到一个终端的响应很慢，人们或许还能够忍受。因为它是数据而不是实时的。但是，如果一个语音通话被分成数据分组，那么这些分组必须在给定的时间内到达收听端，否则通话听起来就不自然。语音和视频都是实时业务的例子。

3.5.5 定时

随着数字信号的传送速率越来越高，与模拟信号的定时相比，数字信号的定时问题显得越来越关键。**抖动**（jitter）是一个与数字信号有关的问题，它不能在同步中出现。根据精确度的不同，有4种类型的时钟定义。4级时钟是精确度最差的一类时钟，而以原子时钟为基准

的1级时钟，则是最精确的。专用网络可以利用它们的载波网络时钟来进行同步，当然也可以根据劳兰-C导航系统（LORAN-C，LOng RAnge Navigation-C）、Navstar全球定位系统或其他独立的时钟源进行同步。

很多情况下，一个网络同时使用两个或更多的工作时钟。因为即使是1级时钟，工作不久也会失去同步。能调节这种定时差异的网络就称为运行在准同步模式下。同步光网络（SONET，Synchronous Optical NETwork，参见第20章）允许流量从一种载波向另一种高速载波转换。它还允许准同步操作，因为不同载波使用不同的网络时钟，彼此之间不会总是处于同步状态。

3.6　回波抵消

为了实现各种应用，我们需要在一对数字线上传送全双工信号。实现这种全双工传输最常用的方式是在每一端采用回波抵消。在图3-12中，发送端在传输线上发送了一个正脉冲。部分正脉冲通过延时和混合电路被反馈回来。混合电路传送脉冲时，由于传输线路不是理想的，因此一部分传送信号被反射或造成回波。

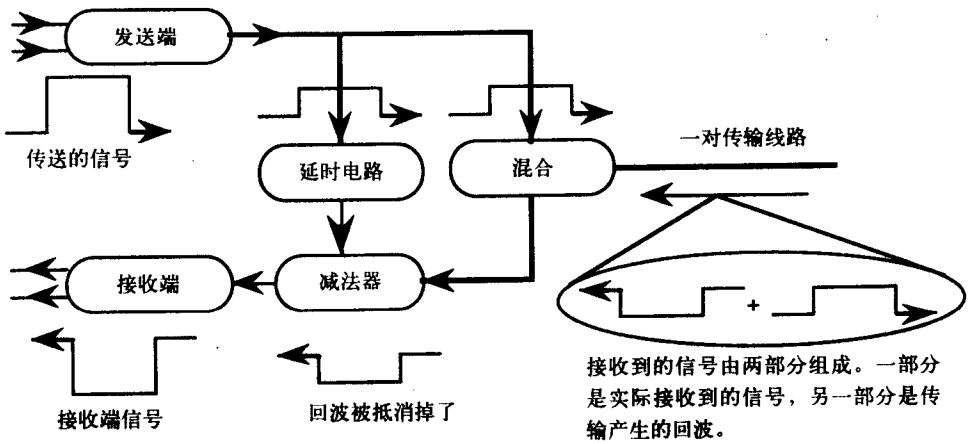


图3-12　回波抵消电路可以在一对线路上提供全双工传输

当发送端发送这个正脉冲时，它也接收到来自另一端的一个负脉冲。这两个信号在同一条线上相互叠加。假设这两个信号电压幅度相同，极性相反，那么它们就会相互抵消，我们看到的是一条直线或0V。

混合电路把这个0V的信号转发给回波抵消器，由它把发送的正脉冲从延时电路中除去。这使得回波抵消器能够恢复输送到这一端的负脉冲。回波信号中出现的一部分反射功率和回波信号中的延时变化可以被回波抵消器自动地检测、补偿或调整。

总之，回波抵消允许在一对线中使用均衡网络实现全双工传输。这是通过从接收到的混合信号中抵消发送效应后提取所期望的接收信号实现的。回波抵消必须在数字线路的两端同时进行。

3.7　编码和编址

在数字系统中，可以收到的最小信息单元是一个比特。两个比特称为双位比特，四个比

特称为半字节，而八个比特则称为八位组。通常，一个八位组也称为一个字节，但是在某些场合，一个字节并不等于八个比特。

如果只传送一个信息比特，那么只能传送两种可能信息中的一种。例如，两个通信终端可以约定：如果发送二进制1，表示晴天；如果发送0，则表示不是晴天。

如果两个终端打算与对方交流更多的信息，就需要用多个比特来为这些信息编码。使用两比特允许通信双方有四种可能的编码。如右图所示，两个灯泡有四种可能的状态组合。

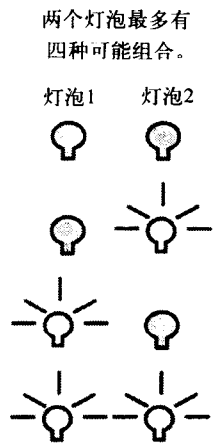


图3-13给出了用两个比特进行编码的两个实例。无论发送端采用哪一种方法编码，接收端必须使用相同的方法解码。编码和解码方法是网络上所有用户使用的通信协议的一部分。

用于通信的数据形式	通信协议A	通信协议B
00	It is sunny.	I want to go home.
01	It is raining.	I am going home.
10	It is snowing.	I am almost home.
11	It is doing none of the above.	I am home.

图3-13 给定比特组合的实际含义是由所用的通信协议事先确定的

如果把用来传送信息的比特数增加到3位，就有8种不同的可能编码组合。3位和4位比特的编码组合如图3-14a和图3-14b所示。从这些例子可以看出，在给定比特数之后，可以用下面的公式计算可能的编码组合数：

$$\text{可能的编码组合数}=2^{\text{可用的比特数}}$$

000	100	0000	0100	1000	1100
001	101	0001	0101	1001	1101
010	110	0010	0110	1010	1110
011	111	0011	0111	1011	1111
a)		b)			

图3-14 a) 3比特可能的编码组合，b) 4比特可能的编码组合

让我们看一下这个公式的应用实例。如果一台计算机上只有128个八位组数据，为了能让CPU访问这些八位组中的任意一个，必须用7个比特为每个八位组编址，因为对于7比特，共有128（或2^7）种组合，每一种组合可以用来标识一个八位组。然而，每个八位组本身又可能是256（或2^8）种数据组合中的一种。为了访问一个特定的位置，需要7条地址线，每条线上都是数字信号0或1。另一方面，为了把数据并行地传送到指定的位置，还需要8条数据线。

假设一个局域网有30台计算机，发送计算机必须在它所发送的每一个数据帧中对接收计算机的地址进行编码。在这种情况下，地址编码需要用多少个比特呢？见图3-15。如果只用4个比特为目的地址进行编码，仅有2^4或16台计算机可被访问。如果用5个比特编码，就可以从32种可用组合中选择30种分配给计算机做地址，剩下的两个空闲地址则预留给将来新增的计算机。

这只是一个虚构的网络习题。我们通常没有权利选择地址字段的比特数，更不用说为计算机分配地址了。实际上，以太局域网网卡有48位地址。每个局域网网卡还有一个独一无二的物理地址写在它的只读存储器（ROM，Read Only Memory）芯片中。前24个比特标识以太

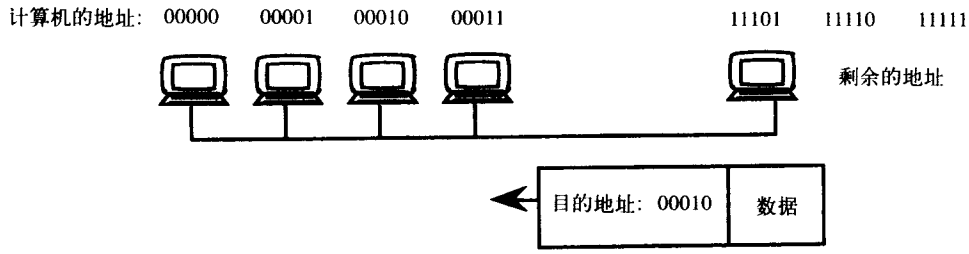


图3-15　在这个虚构的网络中，如果有30台计算机，只要5比特就可以为它们编址了。在这里，数据帧在局域网上传送，目的地址被写在它的头部

网网卡的生产商，而后24个比特则是生产商分配的系列号。这样，就有2^{24}个生产厂商号码，对于每一个生产厂商号码，各厂商又可以分配2^{24}个系列号。总共有2^{48}个可能的以太网网卡。

在Internet上每一台主机必须有一个独一无二的IP地址。对于IPv4，只给每个IP地址分配了32比特，这是因为在制定TCP/IP协议的时候，人们没有想到这个协议族会一直使用到现在。人们认为其他的协议族，如OSI，将会成为主流协议。IPv4的可能主机数目仅有2^{32}，而对于IP协议的新版本IPv6，用作地址的比特数增加到128位。

如果地址字段从32位增加到33位，可用的IP地址数目就会增加一倍。地址字段增加2或3位，相应的地址数目就会分别增加到原来的4倍或8倍。因此，比特数从32位增加到128位将使可用的IP地址数量大幅度增加。

3.8　多路复用

在一条链路上同时传送几个通信信道（或会话）信息的过程被称为**多路复用**。在接收端把分离这些信道的过程称为**解复用**。多路复用和解复用由多路复用器完成，多路复用器也被简称为复用器。

多路复用以各种形式出现。例如，当我的女儿Sarah给她所有在印度的朋友寄短信时，我只是简单地把这些短信装在一个信封里寄给他在孟买的舅舅。然后他会对这个信封“解复用”，并把这些短信送到它们各自的最终目的地。对我来说，用一个大信封寄所有的信比单独寄每一封信便宜多了。

在第2章的图2-7中，我们曾用到一个通过一条航空线把一张贺卡送到芝加哥的例子。在这个例子中，许多消息在同一个邮包或容器中多路复用。在图2-10a中，我们也看到过在一个分组交换网络中的许多分组是怎样在同一条链路上进行多路复用的。实际上，多路复用可以发生在OSI参考模型的任何一层。图3-16说明了多路复用如何在物理层或在比特水平上发生。

在图3-16a中，如果两地用户之间没有采用多路复用，那么他们必须每月为每条单独的通信线路付费。这不仅昂贵，而且带来了管理上的问题。如图3-16b所示，如果在每一个地点安装一个多路复用器，就只需要为一条线路付费，而且维护一条线路比维护几条线路容易得多。这时会有一个与多路复用器有关的最初成本，但解决了这个成本问题以后，每月都会节省不少长途通信费用。因此，两点之间的距离越远，节省的费用越多。使用多路复用器，主机之间必须成对地进行通信。你还无法使地点1上边的主机（与地点1的端口1相连接的主机）与地点2下边的主机（与地点2的端口3相连接的主机）进行通信。

另外，还要注意多路复用器的输入速率的总和不能超过通信链路的速率。每台主机轮流利用自己的时间片向通信链路发送数据。如果一台主机空闲，而另一台主机有大量的数据需要发送，这样就太糟了。繁忙的主机必须等候把它的数据送到另一端，而空闲的主机则在浪费分配给它的时间。

这就给了我们一个使用统计多路复用器的理由，如图3-16c所示。这里，如果有两个端口繁忙而其中一个有大量的数据需要传送，这时统计复用器会为繁忙的主机连续发送所有业务。但是现在接收端的统计复用器怎样才能知道数据是送往哪一台主机呢？这是通过用帧来发送数据并在帧的头部写上接收端地址来实现的。统计复用器必须具有比普通多路复用器更多的缓冲区或RAM，以便存储和转发它所收到的帧。

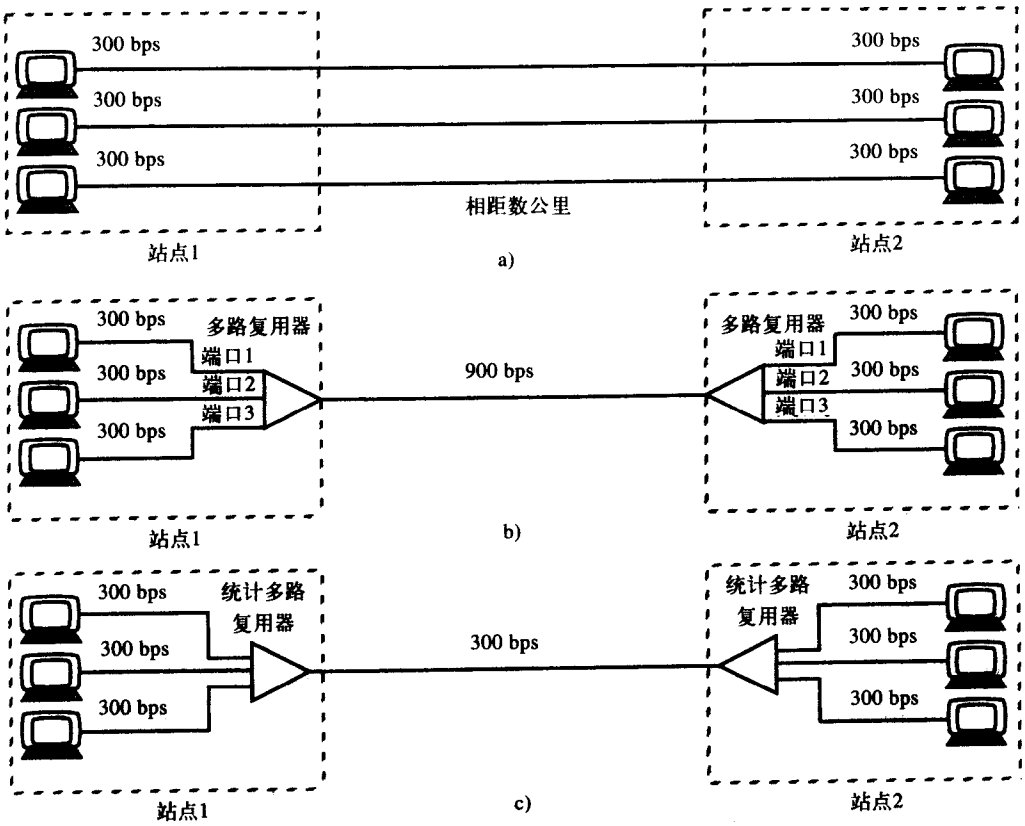


图3-16 a) 没有多路复用器，对于每一对主机来说，单独的一条通信链路花费很高。b) 所有的通信信道被多路复用在一条链路上，降低了通信费用。c) 如果主机不是连续发送，那么它们可以利用统计多路复用器共享一条低速链路。如果我们希望数据能够传送到任何一台主机，那么必须用分组交换机代替统计复用器

如果链路上的业务量很低，也就是说线路利用率很低，那么一条低速链路就够了。这会减少每月在链路上的花费。然而，两个统计复用器之间只有对应的端口才能相互通信。如果希望在地点1上复用器的任一端口都能与地点2上复用器的任一端口通信，就必须用分组交换机代替统计复用器。在分组交换机中，每个分组头部可以将该分组引向正确的端口。这就产生了一个两节点分组交换网络。紧接着，所有交换机都同时提供了交换和统计复用功能。下一步来看一些常用的多路复用方法，并简要地了解一下它们是如何工作的。

3.8.1 频分复用（FDM）

图3-17给出了一个FDM多路复用器。这个复用器将接收到的12路语音信道输入组合在一起，

并在一条通信链路上传输。每一条信道使用3kHz带宽。不过，为了防止相邻信道之间互相干扰，这些信道之间使用了一个保护频带相互隔开，所以每条信道实际分配的带宽是4kHz。

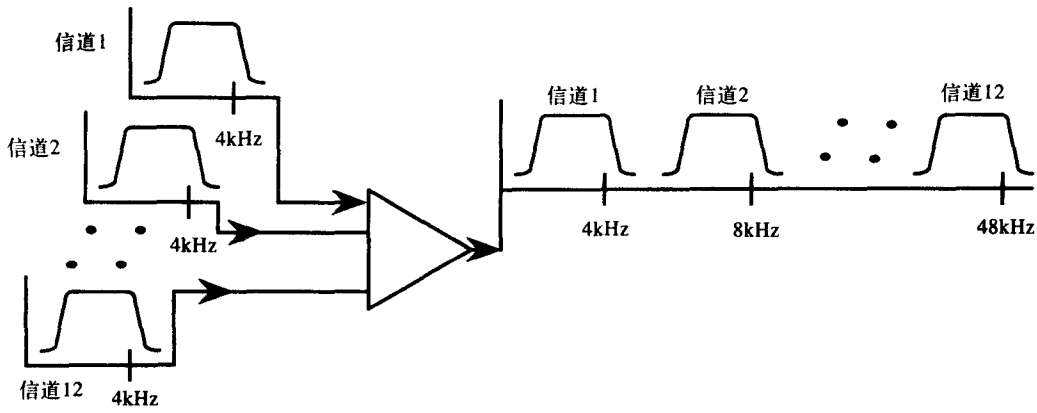


图3-17　通过为每条信道分配一部分带宽，FDM可在一条链路上同时传输多个模拟信道的信息

每条信道可以根据输出频谱进行调整，以使所有的信道可以分享可用的带宽。用这种方法，多个语音信道的信息可以在同一条链路上传输。

FDM也可用在模拟有线电视中。每个电视频道占用6MHz带宽，因此拥有100个频道的有线电视系统需要至少600MHz的容量。为了减少频道间的干扰，还要用到保护频带，这就使得整个有线电视系统的工作频带达到750MHz。

3.8.2　时分复用（TDM）

除了用频率区分信道之外，还可以用传输时间区分信道，这称为时分复用（TDM，Time Division Multiplexing）。如图3-18所示，两条信道向一个TDM复用器输入数字信号。根据自己的时钟，复用器在每个奇数时隙内传送来自第一路的输入数据，在每个偶数时隙内传送第二路的输入数据。用这样的方法，两路输入数据在同一个输出上被传输。为了能在一个输出信号上传输两个输入信道的数据比特，输出速率必须是输入速率的两倍。

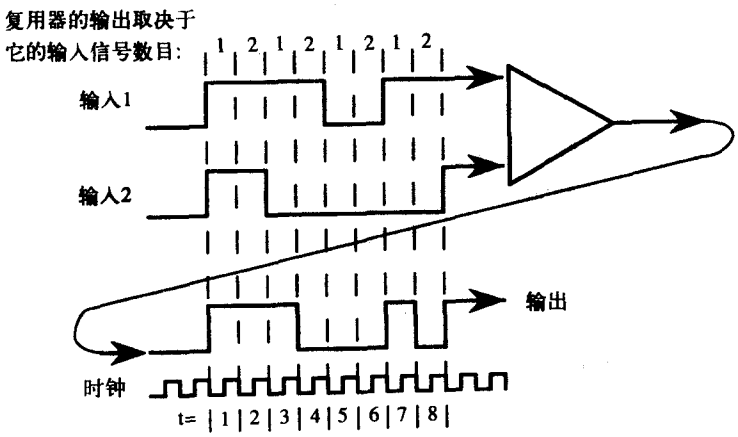


图3-18　通过为每条信道分配一个可用的时间段，TDM可在一条链路上传送多个数字信道的信息

例如，在t=3和t=4时刻，第一路输入要传输的是二进制1，第二路输入要传输的是二进制0。第一路输入的二进制1在t=3时刻被传送，而第二路输入的二进制0在t=4时刻被传送。这样，复用器交替传输两路的输入信号。当然在接收端，TDM的解复用器必须与发送端的TDM复用器保持同步，以便为各接收端转发正确的比特。

图3-18说明了**比特交织**的原理，因为复用器每传送一个比特就改变一次信道。此外，如果每条信道上8个比特一起被传送，那么就要采用被称为**字节交织**的多路复用。

可以很容易地理解如何将TDM扩展到多个信道，但链路速率必须大于输入速率的总和，就如同FDM多路复用器的输出带宽必须大于输入信号带宽的总和一样。对于TDM不需要太多的额外时间开销；但是对于FDM，为了使信道相互隔离，必须使用超过实际需要的带宽。因此通常认为TDM 比FDM更有效。

3.8.3 波分复用

波分复用（WDM，Wave Division Multiplexing）与FDM相似。FDM被用于模拟电信号的传输，而WDM则被用于在光纤上传输光信号。FDM和WDM采用的都是频分多路复用。然而在光波段上，工程师们更多的是用波长代替频率来描述光子的特性。因此在光波段，FDM就被WDM这个术语所取代。回想一下3.3节，一个波的波长等于其频率的倒数。因此，如果波长增加则频率下降，反之亦然。每一种波长都对应一种不同的颜色。

没有使用WDM时，一条光纤只使用一个光源，向一个方向传送光信号。因此老的光纤设备必须使用两条光纤，一条用于发送，另一条用于接收。利用WDM使现在的光纤配置可以实现双向全双工传输。就像两只闪光灯的光束能够无干扰地互相交叉一样，光纤两端的发送器可以使用不同波长（或频率）的光源。

除了双向全双工传输之外，WDM还允许多个输入信道的电信号通过不同的光波波长在同一条光纤中传输。这极大地增加了光纤的容量，使光纤能够用比以前宽得多的带宽传送数据。在第4章中还将继续讨论光纤。

3.8.4 反复用

多路复用允许在一条高速链路上传送多个慢速信道信号。然而在很多情况下，没有可用的高速链路；相反，由于这样或那样的原因，使用几条低速的链路会更为灵活。这时，可以在相互通信的两端各使用一种被称为反复用器的设备。

在图3-19中，可以看到一个很大的X射线文件正从西海岸的某一地点发向东海岸的一位专家。这里使用了三条低速链路，它们可能是一些廉价的拨号连接。然而，通过各端使用的反复用器，大量的数据可以在一个合理的时间内传送完毕。发送反复用器以某种方式分解数据流，而接收反复用器则能以原来的顺序对它重新组装。

3.9 信息编码

3.9.1 传输信息的方法

正如3.7节讨论的那样，信息是用户进行通信想获取的内容。信息包括语音、数据、视频、传真、医疗图像等。信令决定了如何建立一个到接收方的连接，同时接收方已经准备好接收

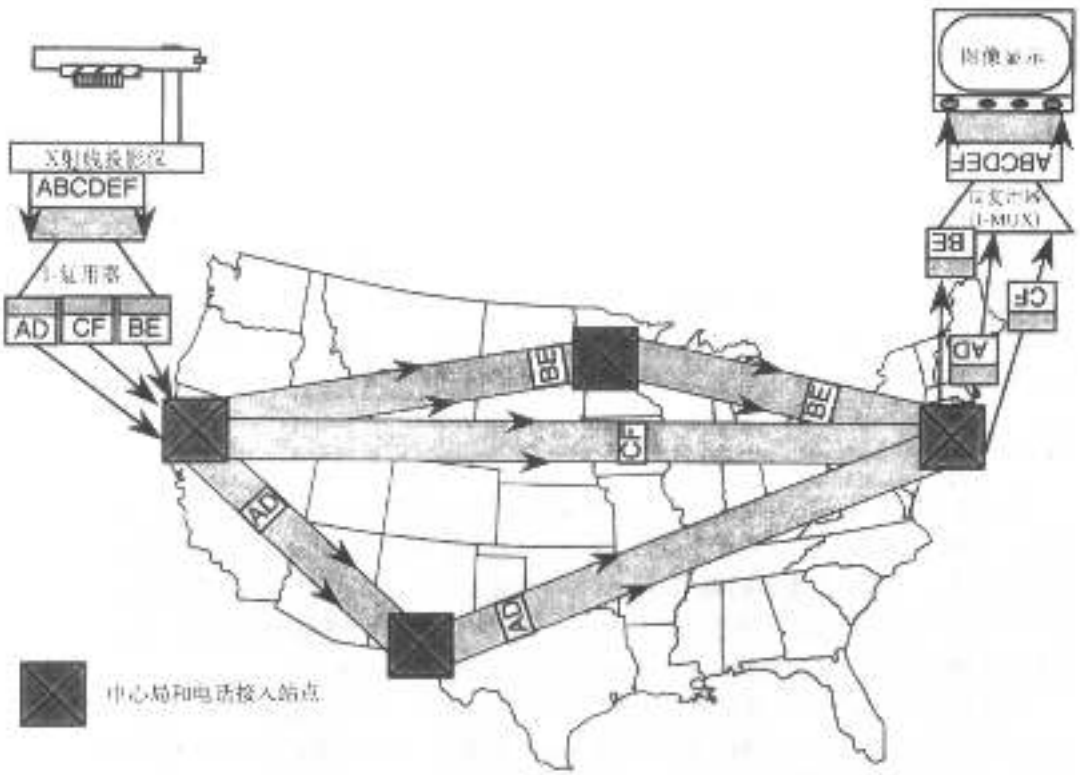


图3-19　一个很大的X射线文件可以利用几条低速链路和各端的反复用器在较短的时间内被传输完毕

这些信息。既可以使用模拟线路传输信息，也可以使用数字线路传输信息。线路的类型不是由其看上去的特征所决定，而是由另一端与之相连接的终端设备的类型所决定。

例如，中心局用模拟设备连接来自住宅的电话线，因此电话线就是典型的模拟线路。如果中心局在那条线上连接了数字设备，那么它就变成了一条数字线路。综合业务数字网（ISDN，Integrated Services Digital Network）只是通过将中心局和用户的终端设备替换成了数字设备，就将现有的模拟线路转变成了数字线路。必须记住的是：如果在传输线路上有许多像负载线圈之类的模拟设备，就应该把它们去掉并用数字设备代替。

在图3-20a中，一部简单的电话提供了通过模拟线路传送语音信号所必须的全部电路。该图还说明要把语音信号转换为数字信号，还需引进编解码器（编码器和译码器，Coder and DECoder）。语音编解码器把语音信号转换为数字信号，而视频编解码器则是把视频信号转换为数字信号。

现在，几乎所有的语音信号都采用数字方式传输。因此，当语音信号通过电话线到达中心局的时候，中心局的线路卡就把模拟语音信号转换为相应的数字信号，反过来，当数字语音信号通过电话线到达用户的时候，线路卡首先将它转换成原来模拟形式的语音信号。现在的大多数用户交换机（PBX）也以这种方式工作。因此，如果你有一部连到PBX上的数字电话机，那么编解码器就在电话机的内部，在电话线上以数字方式进行传输之前语音信号被转换。另一方面，如果你有一部模拟电话机，编解码器在PBX的线路卡上。

为了在模拟线路上传送数据，需要图3-20b所示的调制解调器。在3.3.2节，我们曾提到过数字信号实际上是由许多高频分量组成的，而模拟电话线不能处理这些高频分量。因此不能

将数字信号直接放在模拟电话线上传输：数字信号在模拟线路上传不了多远就会变得模糊不清，难以识别。我们必须用调制解调器把原本是数字信号的数据编码变成模拟形式，以便这些数据能在模拟线路或设备上可靠地传输。可以形象地认为调制解调器就是计算机的“电话”。为了让计算机与PSTN“交谈”，必须有一个调制解调器。

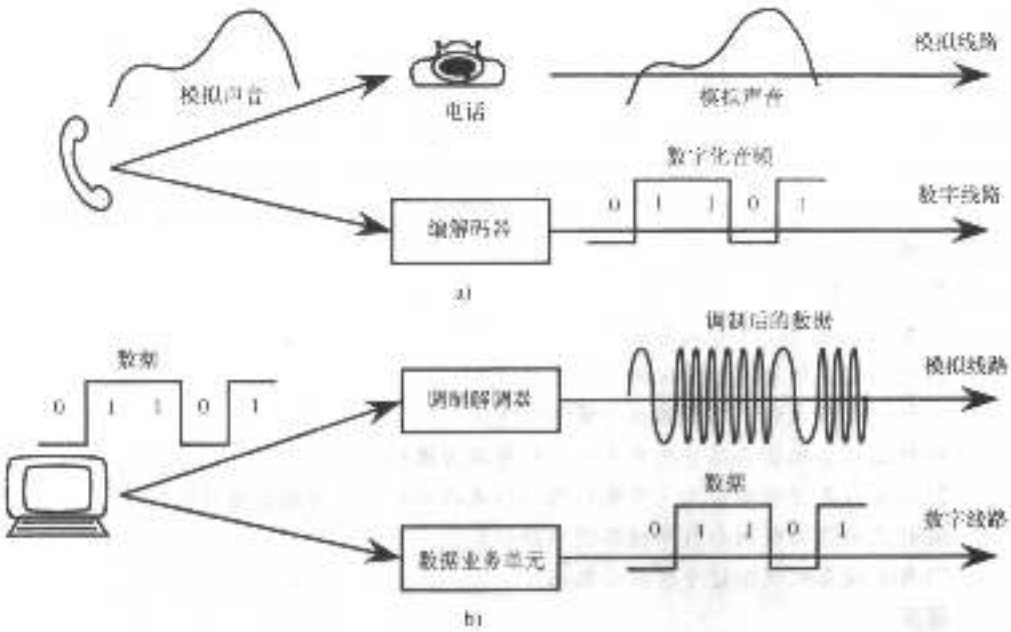


图3-20 a) 在模拟和数字线路上发送语音，b) 在模拟和数字线路上发送数据

不能把调制解调器看成是一个简单的模数转换或数模转换设备。从这个角度说，编解码器也不是。考虑图3-21，在这里，来自PC的数据以数字形式发送给调制解调器，调制解调器将数字数据转换成模拟形式。这样做是为了适应中心局里的那些希望信号落在语音频率范围内的模拟设备。模拟信号一到中心局，就被转换为脉冲编码调制（PCM，Pulse Code Modulations）信号，如同语音信号一样，而这个PCM信号代表的是受数据调制的模拟信号。在接收端，这两次转换的顺序相反，以便能得到被传输的数据。

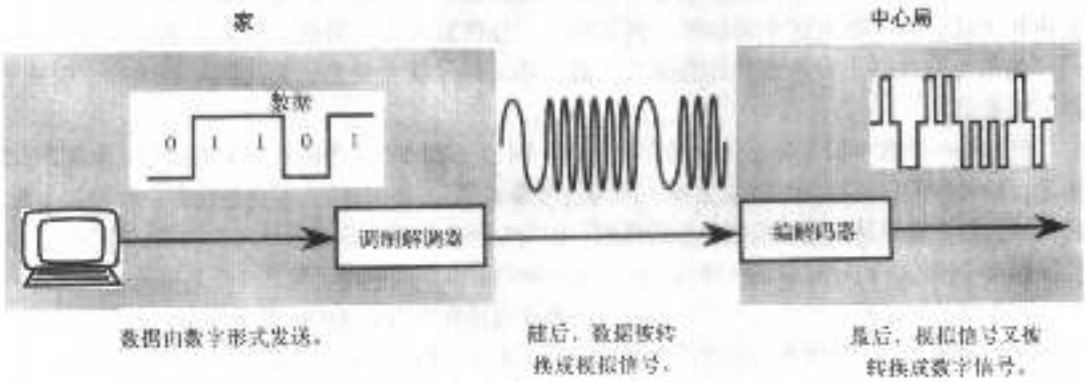


图3-21 数据在电话线上被传输并被转换成模拟信号，而后中心局又利用PCM把它转换成数字信号

通过数字线路传输数据需要数据业务单元（DSU，Data Service Unit；也称为数字业务单

元（Digital Service Unit））。DSU提供在数字线路上传送数据所必需的接口，确保信号电平处在合适的电压范围内，同时还保持与终端设备的同步。此外，DSU还使技术人员可以从远端中心局进行回路测试。实际上，DSU经常与内置的数据通道服务单元（CSU，Channel Service Unit）一起出现，但通常我们把它们统称为DSU。在介绍T1的那一章中将深入讨论DSU。

在理解调制解调器和编解码器之间的差异时，极容易弄混淆。两者都具有模数或数模转换功能。但是，要牢记每一种设备所处理的信息类型。例如，文本使用7位ASCII码编码。这种码只有文本显示和打印机能够识别。调制解调器能把这种数据转换成模拟形式。为了从模拟信号中再次恢复数据，需要的是调制解调器，而不是编解码器。另一方面，语音编解码器只能对数字化语音信号（与ASCII码无关）进行解码并把它转化为我们能够听得见的语音信号。同样的原因，没有人会向打印机发送数字化的语音信号，也不会指望调制解调器把数字化的语音信号转换为音频信号。

几个复习题

1) 数据原来以什么形式存在？

2) 什么设备把模拟信号转换为数字信号？

3) 什么设备把数字信号转换为模拟信号？

4) 什么设备把语音信号（空气压力）转换为模拟信号？

5) 什么设备把语音信号（原来以模拟形式存在）转换为数字信号？

6) 什么设备为数据和数字线路提供接口？

7) 什么设备把模拟信号转换为数据？

答案

1) 数字；2) 调制解调器和编译码器；3) 调制解调器和编译码器；4) 电话；5) 编码器；6) DSU；7) 调制解调器。

3.9.2 将语音信号转换成数字信号的优点

下面讨论一下为什么大多数语音传输都转换成数字形式。一般地讲，这里讨论的很多问题对数字信号传输也是适用的，即使是视频信号传输也不例外。

语音信号数字化最重要的原因可能是数字信号受噪声影响较小。在图3-22a中，一个模拟信号正在一种传输媒介中传送。当它到达第一级线性放大器时，信号已经衰减而且叠加上了噪声和干扰。为了放大这个弱信号，需要加一个线性放大器。但是，放大器也同时放大了噪声。如果传输线路上有几部分都需要放大器，那么信号就会变差，无法满足所谓的“收费质量”的要求。

但如果一个数字信号也在这个媒介中传送，则另一端的再生器能重新生成信号，如图3-22b所示。信号中的任何模糊都能被去掉，因为信号要么是1，要么是0，不会是它们之间的其他数。线性放大器不能轻易去除模拟信号中的模糊，因为它不能把噪声从信号中区分出来。尽管过去工程师们花了相当多的时间和心血努力设计最大可能消除噪声的电路，但这些电路都是很昂贵的。

即使到了20世纪70年代，人们仍能分辨出越洋电话和市内电话的区别。现在，由于采用数字化传输，因而人们已经很难辨别通话质量的差异。用在一路模拟信号上的线性放大器的最大数目是有限的，典型值是5个，但用在一路数字信号上的再生器的最大数目实际上是没有限制的。再生器使数字信号对距离不敏感。用于数字设备上的电路易于设计（如果它还没有设计出来与计算

设备一起使用的话)。正是由于这一点，数字设备廉价而可靠。模拟信道采用的FDM低效而昂贵，还需要采用防护频带来隔离相邻信道之间的信号。这种附加的带宽不能传送任何信息，但却是减少邻道干扰所必需的。数字信道上采用的TDM有效得多，使用的额外开销少，也更便宜。

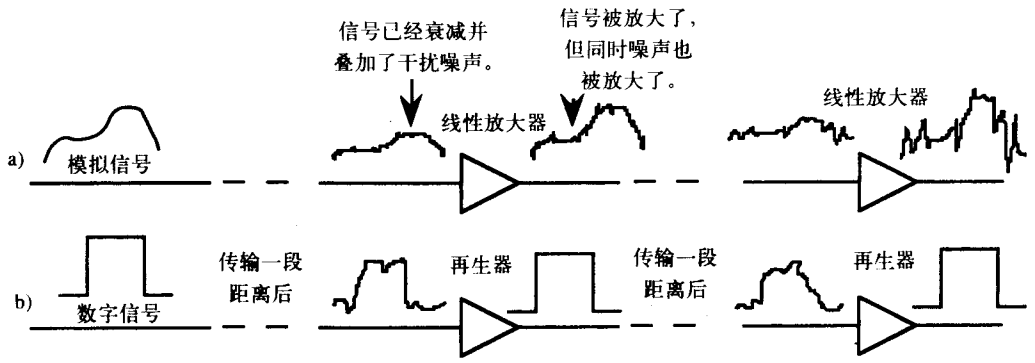


图3-22 a) 传输一段距离后模拟信号的衰落，b) 传输一段距离后数字信号的再生

过去，由于一路数字语音信号需要的带宽（64kbps）大大超过了原始数据信道的带宽(300bps)，因此极大地排除了数字化语音更为流行的可能性。现在，网络链路上可用的带宽越来越多，并且随着这一领域的研究开发不断进行，满足收费质量要求的语音信号所需的带宽也不断下降。例如，在1978年，电视会议需要6Mbps的带宽，并且还要采用复杂的压缩算法；而到了1993年，只需要0.08Mbps的带宽就可以提供相同质量的信号。

数字化语音的另一个显著优点是我们可以对数字语音信号进行分组。一旦语音被编解码器数字化以后，这些比特就可以作为分组中的数据通过数据网络（如Internet）传输。如果语音没有被数字化，那就不能在Internet上传送；同样地，也不能传送音乐或视频信号。伴随语音分组化的问题是所设计的数据网络一般对延时波动是不敏感的。如果我们正在等待文本出现在屏幕上，数据慢一点关系不大。但是如果一个语音分组比前一个语音分组到达得晚，我们会发现通话的质量是难以接受的。

数字信号的传输依赖于误差有限的同步。如果同步保持不好，就会出现我们不希望见到的、被称为“**抖动**”的现象。模拟信号转换为数字信号时还会引入**量化噪声**，3.9.3节将会讨论PCM的量化噪声。

语音数字化的优点:

1) 抗噪声干扰。
2) 有效的多路复用。
3) 廉价的电路。
4) 分组化处理。
5) 可靠传输。
6) 对距离不敏感。

语音数字化的缺点:

1) 存在量化噪声。
2) 同步很关键。
3) 对延迟敏感。

3.9.3 脉冲编码调制（PCM）

图3-23a给出了一种简单的语音数字化方法。语音信号被放在假想的网格中，网格上的离散电压电平就代表数字编码。然后以均匀的速率对语音信号进行抽样，并传输数字化的语音信号电压。例如，在抽样点1，语音信号靠近01电平，而在抽样点2，靠近10电平，等等。然后传输这些比特，接收端根据它们重建信号。实际语音信号和重建信号之间的差异被称为**量化噪声**。只有多次将模拟语音信号转换成数字信号时，量化噪声才是一个值得考虑的问题。再生器不能完成这类转换，只有编解码器才具有这样的功能。在端到端之间传送数字语音信号是最好的选择，尽管各国之间的编码方式可能不同。

图3-23b说明了如何利用编解码器的译码器部分重建数字化语音。由于译码电路对语音信号进行了四舍五入，因此要准确地再现原始语音信号是不可能的。这都是因为存在量化噪声。

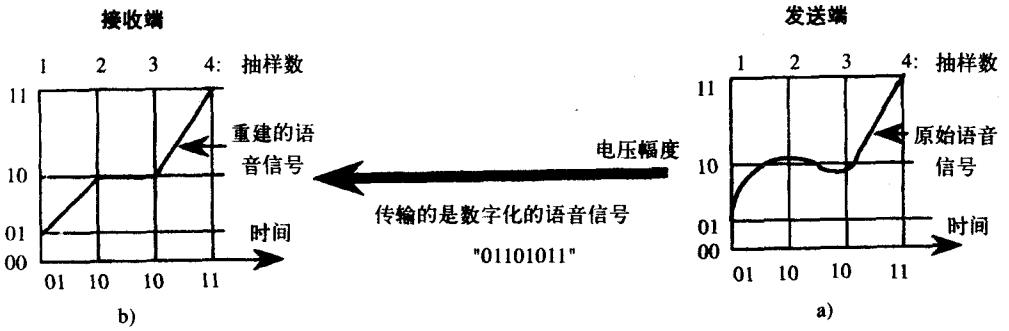


图3-23　a) 将语音信号转换为数字信号的一个例子；b) 语音信号被重建以后，它的波形和原信号波形之间的差异就被称为量化噪声

如果希望将语音信号转换成为更精确的数字信号，就需要在提高抽样速率的同时增加电平数目。这样做会增加网格上的矩形数目，同时减少了它们的尺寸。为了准确地把语音信号编码成数字形式，抽样速率至少是模拟语音信道中最高频率的两倍。这就是奈奎斯特抽样定理。

这种被称为PCM（Pulse Code Modulation，脉冲编码调制）的编码方式采用每秒8000个样本的抽样速率，大约相当于模拟信道带宽的两倍（即4kHz的两倍）。它用8比特为每个样本信号的电平编码，总共提供2^8或256种电平。然而0电平未使用，因为对保持同步的时钟来说，它的连0太多了（实际上是8个0）。

因此，对于每秒8000个样本的抽样速率和每个样本8个比特的编码，采用PCM，一条语音信道的编码速率为64kbps。北美和日本采用的PCM编码方式称为μ律，而欧州采用的PCM编码方式则称为A律。

另一种流行的数字化语音处理方式称为自适应差分脉冲编码调制（ADPCM，Adaptive Differential PCM）。它对每个样本使用4比特，但是只对预测电平和实际电平的差异进行编码。所以每个样本不需要像PCM那样多的比特。ADPCM的32kbps带宽提供的语音质量和PCM不相上下。

采用PCM，存储一分钟通话产生的语音信号数据需要大约0.5MB的存储器。这是因为每分钟等于60秒，而每秒产生64 000个比特，这样共3 840 000个比特，除以8，就得到480 000字节。当然，采用语音压缩技术可以大大减少这个数字。

与PCM相比，光盘（CD，Compact Disc）需要更多的带宽，因为它提供高质量的音频信号。

一个带宽为20kHz的模拟信号要求抽样速率必须达到44.1kbps，大约是音频信号带宽的两倍。每个样本采用16比特代替PCM的8比特编码，把44.1kbps、16和2（因为有两个立体声道）相乘，得到一个1.4112Mbps的速率，这大大超过了PCM所需的64kbps速率。然而，再加上纠错编码、同步比特以及其他的处理之后，光盘的实际速率将达到4.3218Mbps。

3.9.4 视频压缩

与音频信号在光盘上编码不同，视频信号的数字化依靠复杂的压缩算法。注意在光盘中没有采用到压缩技术。如果不采用压缩，彩色广播电视信号需要4.7Mbps的带宽，高清晰度电视（HDTV，High Definition TV）需要100Mbps带宽。但压缩之后，速率最多能减少到原来的1/100，且画面的质量没有明显的下降。医疗图像，如X射线透视图，可以压缩到原来的1/3，但在不损失分辨率的前提下，压缩率不会超过这个数字。

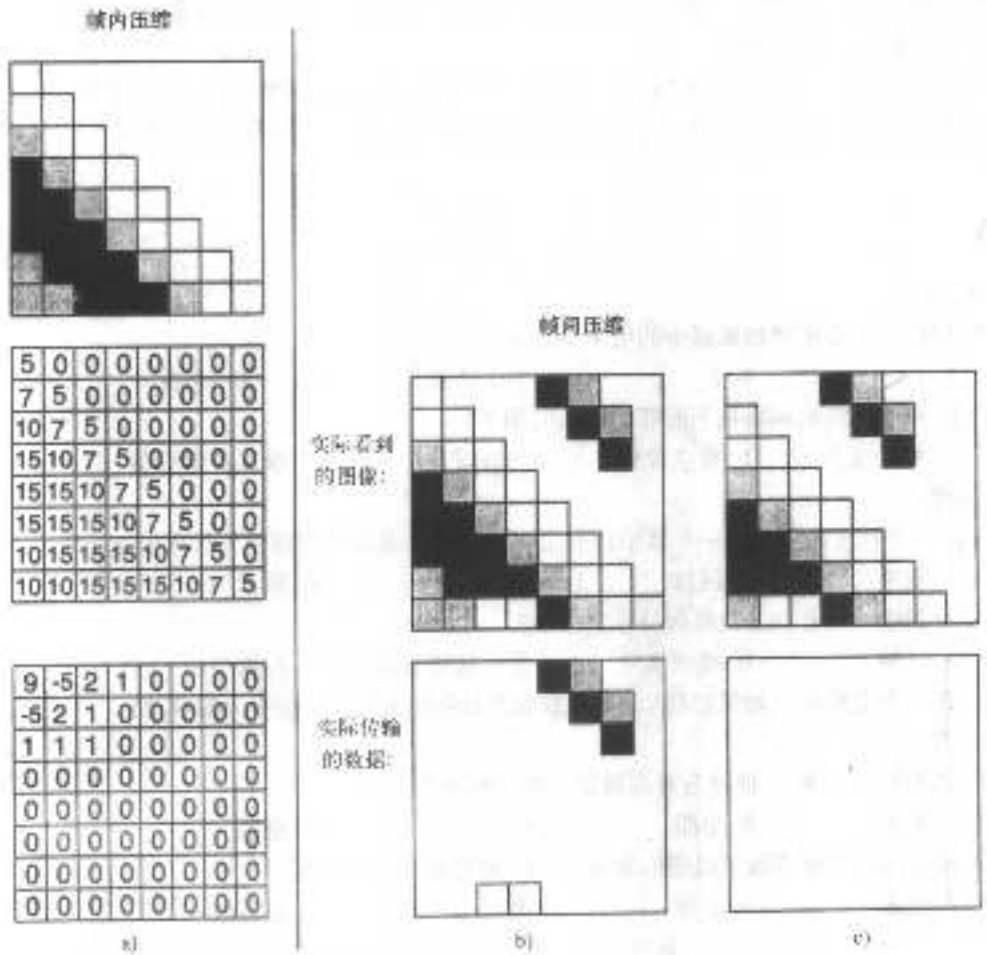


图3-24 a) 对于帧内压缩，用一套数字标记一个8×8像素块中的每一个像素，完成数字化。然后通过压缩数据和丢弃一些信息来进一步简化这个像素块。左上角的数字给出了这个像素块的平均特性。

b) 图a)中图像被改变的情形。根据下图，只有相对于上一帧发生变化的像素被传送。

c) 如果物体进行了简单地移动，那么只有移动像素的方向和数量被传送

有两类视频压缩技术：帧内压缩和帧间压缩。帧内压缩可以减少发送一帧所需的数据量。帧间压缩是基于这样一个事实：一般情况下相邻的两帧都很相似，可以只传送它们之间的差异。这两类压缩技术都用到了人眼的视觉特性，在不传送所有细节的情况下，图像看起来仍然不错。

例如，由于人眼对亮度比对色彩敏感，因此，在每一帧中对亮度编码使用的比特数比对色彩编码使用的比特数要多。又如，人眼对图像的突变比对缓变的敏感度差。因此，对突然变化编码使用的比特数比对缓慢变化编码使用的比特数少得多。再有，对于微小的变化，传送的信息非常少，因为目前大多数流行的应用都是电视会议（只是演讲者的头部），其变化比杂耍动作的变化少得多。

简而言之，典型的视频压缩技术通常是把一幅图像划分成多个8 × 8的像素块，如图3-24所示。根据颜色、亮度和其他特性，每个像素被赋予一个值，如图3-24a中间的网格图所示。在对每个图像块平均之后，细节信息被删除，得到该图最下方构造更为简单的网格图。这个例子总结了帧内压缩的特点。

在图3-24b中，相对于图3-24a这一帧有一些变化。不是传送整个帧，只有图3-24b下图所示的变化被传送。同样，如果这个块中的物体移动了，那么只传送与移动有关的信息，见图3-24c。

习题

3.1节

1. 模拟信号电压增加或减少的电平量是多少？

a. 1　　b. 2　　c. 一个连续量　　d. 一个离散量

2. 四档位车窗雨刷器是下面哪种设备的例子？

a. 模拟设备　　b. 数字设备　　c. 三级设备　　d. 模态逻辑设备

3.2节

3. 把一个直流电压加到一个数字信号上实现传输供电的过程被称作什么？

a. 复用　　b. 过滤　　c. 幻象　　d. 放大

4. 下面哪一项有助于电路保持稳定同步？

a. 时钟　　b. 模拟信号　　c. 数字化语音信号　　d. 幻象电压

5. 在一个电路中，如果把70V的电压加在35Ω电阻上，会产生多大的电流？

3.3节

6. 在图3-9中，哪一种设备对高频信号如同短路？

a. 电池　　b. 电阻　　c. 电容　　d. 电感

7. 模拟线路转换成数字线路的时候，下面哪种器件应该去掉？

a. 电池　　b. 电阻　　c. 电容　　d. 负载线圈

8. 除了图3-7中用到的那些参数以外，还有哪些信号参数可用于模拟信号调制？

9. 电容器和电感器有什么不同？

10. 画一个高通滤波器电路并解释它的工作原理。

11. 画一个调制数据为10010的幅度调制信号。

12. 频率为200Hz的信号的波长是多少？如果波长增加，频率怎样变化？200Hz等于多少kHz？

3.4节

13. 如果图3-3中的电阻R2为20Ω，它上面的电压和功率为多少？
14. 在图3-12中，如果第三级的输出为12mW，那么这一级的增益为多少分贝？
15. 如果放大器的增益为6dB，输入功率为2mW，那么它的输出功率是多少？
16. 计算一个输入功率为5mW，输出功率为4mW的滤波器的增益。

3.5节

17. 在异步传输中，很多时候会用到一个奇偶校验位对字符进行纠错。在这种情况下，传送一个字符需要多少比特？
18. 描述同步传输和异步传输之间的差异。
19. 异步传输和ATM有哪些共同点？
20. 时钟有多少个精度等级？哪一级最准确？如果不能保持同步，会出现哪种现象？

3.6节

21. 下面哪一类传输方式提供回波抵消？

    a. 单工　　b. 全双工　　c. 半双工　　d. 三态传送

22. 怎样实现回波抵消？

3.7节

23. RAM中16比特的空间可以存储多少整数？如果这些整数一半是正的，一半是负的（还有一个是0），那么可存储的最大正数是多少？
24. 如果要用一个计算机系统表示4096种颜色，那么对这些颜色进行编码需要多少比特？
25. ASCII码用7比特为字符编码。为了把字符数量增加到原来的8倍，应该在代码中增加多少比特？

3.8节

26. 多少个300波特终端可以通过TDM多路复用器连接到一条2400波特的链路上？
27. 数字信号、模拟信号和光信号分别采用哪种多路复用方式？
28. 为什么说TDM比WDM更有效？
29. 在一个有两个端口的TDM多路复用器中，如果输入为1101和1001，输出比特序列是什么？假设第一路输入先传送。

3.9 节

30. 下面哪一种设备把语音信号转换为数字形式？

    a. 调制解调器　　b. 多路复用器　　c. 编解码器　　d. DSU

31. 语音信号数字化未采用压缩技术。如果传输速率为16kbps，抽样速率为每秒4000个样本，那么能对多少个电压电平编码？
32. 以数字形式传送信号的优点是什么？
33. 用你自己的话描述视频信号是怎样数字化的，它与采用PCM编码的数字化语音信号有何异同。

第4章 传输系统

4.1 简介

20世纪70年代末期光纤技术诞生时，许多人怀疑它是否能够替代其他传输介质成为电信行业的主导选择。虽然光纤在实现点对点高速远距传输业务时得到广泛应用；但其他传输介质成本在不断地降低，因此在连接许多分散且距离远的用户终端时仍起着重要作用。即便是廉价的双绞线也在不断地发展，目前在有限距离内它的传输速率可达到1Gbps。

由于最初光纤的价格十分昂贵，因此人们认为它不可能用于连接桌面终端。但是目前由于光纤价格的快速滑落以及光纤连接器的不断改进，在桌面台式机上使用光纤已成为可能。一旦光纤能够进入我们的家庭连接台式机，那么毫无疑问我们肯定能找到某种方法来充分利用其带宽。

本章的第一部分将对某些传输介质进行介绍。我们将按空间分布的顺序首先介绍贴近地面的传输介质，其次是半空中的，最后介绍用于宇宙空间中的介质。本章的后一部分将讨论有关话音传输和用户交换机（PBX）的问题，有关蜂窝系统的内容将放在后面的章节介绍。

4.2 双绞线

4.2.1 双绞线的局限性

所谓电话线通常是中心局(CO)提供的并与住宅用户相连接的双绞线；由于其带宽是3kHz，因此也被称为音频线。

如第3章所述，电话线中存在固有的电容干扰，这将导致串话现象，即一对话线上的通话和邻线上的通话相互干扰。为减小串话的影响，通常将一对话线绞合在一起，这样就可以将串话的干扰相互抵消。每英尺双绞线绞合的次数越多，发生串话的可能就越小。如图4-1a在远距离传输时，还可以采用负载线圈的方法来减少串话的影响。

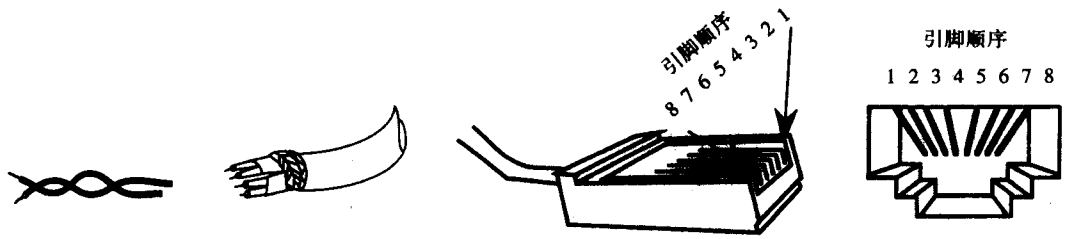


图4-1 a) 双绞铜线，b) 1类STP线，c) RJ-45插头，d) RJ-45插座

虽然普通的铜线价格低廉，但安装时人们也必须注意到它的许多隐患。随着双绞线长度的增加，信号的衰减和丢失愈发严重，数据传输速率也会下降；同时，双绞线对电磁干扰

(EMI, Electromagnetic Interference)和射频干扰(RFI, Radio Frequency Interference)越来越敏感。在施工时将双绞线安装在远离电力线、发电机、升降机及复印机的地方，可以减少电磁干扰的影响。若在工业环境中无法避免靠近上述设备，则可以在线的周围采用金属屏蔽。这种类型的双绞线称为屏蔽双绞线(Shielded Twisted Pair, STP)；没有干扰保护层的双绞线被称为非屏蔽双绞线(Unshielded Twisted Pair, UTP)。图4-1b给出了1类STP双绞线的例子。这种类型的双绞线较昂贵，但比非屏蔽双绞线(UTP)的传输距离远。

通常电话线的尺寸从22AWG(美国电缆标准)到26AWG，其中22AWG的直径为0.025in，26AWG的直径为0.016in。随着AWG序号的减小，双绞线的线径增加，导线的电阻降低，同时传输带宽增加。

在安装双绞线时，必须注意考虑其**阻抗值**。阻抗就是对交流电(AC)的阻碍，它不仅包括直流电源(DC)的电阻，还包括由电容和电感效应引起的电阻。电气工程师告诉我们：在双绞线一端安装电气负载时，其阻抗通常应该等于电线的阻抗；否则信号将在线缆中引起反射，不能有效地传送到负载。他们在设计电路时也是考虑这些细节。必需记住：在正确的位置上安装对双绞线合适的电子设备，同时应保证电线的阻抗与设备的阻抗相匹配。

4.2.2 双绞线标准

美国电子和电信工业委员会(EIA/TIA, Electronic Industries Association / Telecommunications Industries Association)在其制定的568号商业建筑物布线标准中，规定了双绞线的各种类型和安装方法。EIA/TIA将不同类型的UTP分成1~5种类型进行定义。其中，1类和2类UTP电缆不适合用于商业建筑物布线。另外3种电缆传输阻抗为100Ω。安装时，从插线板到墙壁出口的长度不能超过90m，电缆两端设备之间的距离不能超过100m。

3类电缆或语音级的UTP在传输数据时速率可达10Mbps，传输模拟信号时带宽可达16MHz。3类UTP每英尺至少应该绞绕3次，主要用于语音信号的传输；4类UTP主要用于传输数据，实验证明其传输速率可达到16 Mbps，带宽可达20MHz。制造商在生产电缆时，若每英尺双绞线的缠绕次数达10次以上，电缆会有更好的性能。

1991年随着标准的制定，5类线很快流行起来。5类线每英尺至少缠绕36次，能以100 Mbps的速率传输数据。虽然STP也能以100Mbps的速率进行传输，但其线径为0.5in，而5类线的线径只有0.25in。显然，在拐角处或管道中布线时，使用5类线更为方便。

5类UTP由4对线组成，其价格比3类UTP稍贵一点。它使用通常的RJ-45 (Register Jack - 45)接口连接器，图4-1c和图4-1d是RJ-45插头和插座的例子。不要将这个插头与用于T1的RJ-48插头相混淆(有关T1的内容将在第5章介绍)。它们外形虽相同，但使用的是不同的引脚排列。

RJ-45插头使用方便，与我们家里使用的标准4(或6)线电话线接口RJ-11非常类似。RJ-45插头有8个针；而RJ-11插头一般只有6个针，更常用的是4个针。RJ-45插头有两种规格：568A和568B。在568A中，将引脚3和6定义为2号、引脚1和2定义为3号，而在568B中定义的次序相反。请注意不要将这两种布线规则相混淆。

5类线的标准化使运营商不必担心自己的供货商违约，因为还有其他的供货商可用。同时由于标准化引入了竞争机制，因而使电缆的价格下降。可用的UTP还有其他的一些类型，如5E类(增强型)，它具有更吸引人的速率；同时，6类和7类电缆也正在推向市场，但因其尚未标准化，所以目前还不能进行实际应用。而此时光纤传输正显示出其越来越强大的优势，或

许有一天光纤会成为这些“层出不穷”的UTP标准的掘墓者。IEEE（美国电气与电子工程师协会）还制定了1394标准，即所谓的高速串行连接总线标准（FireWire）。这个标准是为个人计算机、电视和其他用户设备提供的电缆方案。

EIA/TIA同时也注意到IBM的STP传输距离可达800m，电缆阻抗150Ω。1类STP由金属箔或屏蔽层包裹的4股铜芯组成，可以传输速率为16Mbps的数字信号，带宽为20MHz的模拟信号。而1A类STP的传输速率可达155Mbps，带宽可达300MHz。EIA/TIA在TSB-53规范中定义了这类电缆。

上述类型的电缆最初是为局域网的令牌环网络定义的，最初它们使用的是笨重的1in连接头。但是，3类UTP电缆也可使用RJ-45接口，其传输距离可达45m。

4.3 同轴电缆

当需要在一种介质中传输多路电话信号时，双绞线无法提供所需的带宽。而同轴电缆（coaxial cable 或coax）传输载频可达到10GHz。同轴电缆由一个内嵌的导体和另一个被编织成丝状网的导体组成，网状导体环绕在内嵌导体的周围。两种导体共用同一个中心轴，因此被称之为“同轴”，如图4-2a所示。同轴电缆根据用途不同可分为两类——基带同轴电缆和宽带同轴电缆。

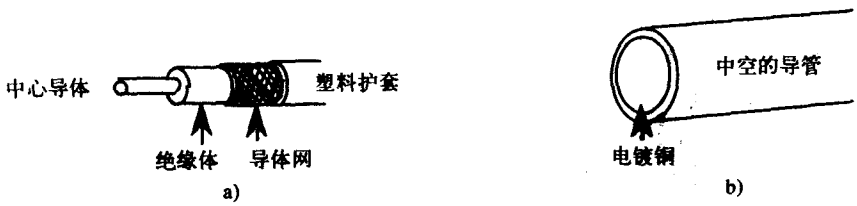


图4-2　a) 同轴电缆，b)波导管

4.3.1 基带同轴电缆

基带同轴电缆曾广泛地应用在以太网中，它只有一条传输通道，即任意时刻电缆上只能有一个数据传输存在。在这个介质中传输数字信号，速率达到10Mbps非常容易，且可以双向传输。基带同轴电缆的传输阻抗为50Ω。

4.3.2 宽带同轴电缆

宽带同轴电缆的传输阻抗为75Ω，通常用在有线电视（CATV，Cable TV）系统中。在CATV中，只能实现模拟信号的单向传输。要实现双向传输，必须安装双电缆系统。由于能提供300MHz到450MHz的带宽，因此宽带同轴电缆可以同时传输多路信号。用户可以用其同时传输视频、音频和数据信息。但由于这是一个模拟系统，因此在传输数据时必须使用调制解调器。

对宽带同轴电缆系统，一些复杂的设备，如放大器、分路器等是必需的；同时还需要技术娴熟的工程师来安装和维护系统。

4.3.3 波导管

波导管并不是某种类型的同轴电缆。然而，当同轴电缆中传输信号的频率高到一定程度时，就可以不用导体而直接在大气空间中传输。为了引导这类信号沿特定的路径传输，就需要使用

一种中空的金属管来传送信号，这种金属管就称为波导管，如图4-2b所示。目前使用的大多数波导管在连接处呈矩形，长宽比是2∶1。波导管可用来传输100GHz左右的微波信号。

4.4 光纤

4.4.1 概述

如同用波导管限制微波信号传播一样，光信号（或说成光）也可用类似的方法进行处理，在光纤（光导纤维）中传输。这是因为只要增加微波发射机的工作频率，就非常接近光波了。尽管光波频率比无线电波和微波的频率高很多，但无线电波和光波都是电磁波。

光的利用最早可以追溯到1880年，Alexander Graham Bell发明了光电话并获得此项专利。这种光电话利用日光光线传输语音信号，传输距离高达200m。

1971年，康宁公司的工作人员Kapron、Keck和Maurer首次利用光传送信号，传输距离只有几百米，信号衰减为20dB/km。然而21年以后，在不使用任何中继器和信号再生器的情况下，5Gbps光信号可以被传输超过5000英里。目前传输一个1.55μm波长的红外信号，信号的衰减可小于0.2dB/km。相比之下，若采用同轴电缆传输，1MHz的信号衰减为2.5dB/km。同时光纤的纯度也在逐步提高，一块3英里厚的高质量光纤，其透明度与一块1/4in厚的普通窗玻璃一样。

利用光波传送信息可以有效地避免来自电源、无线电波、雷电等的干扰，可使误码率低于10^{-9}。这个数字意味着每传输10亿个比特只产生一个误码。光纤不但能达到极低的误码率，还可以提供非常高的数据传输率。

光纤像铜缆一样不易腐蚀，传输不易被窃听，能提供很好的保密性，也不会发生串话。而且光纤体积轻巧，易于搬运。但由于光纤价格昂贵，安装工作难度大，因此其他传输介质仍有一定的竞争力。

光纤的优缺点

优点：1) 无噪声干扰。
2) 传输距离长。
3) 信号损耗低。
4) 安全性高。
5) 重量轻。
6) 传输速率高。
7) 不易腐蚀。

缺点：1) 价格昂贵。
2) 安装困难。

4.4.2 光纤的结构

光纤通常都是成对地安装：一条光纤用于发送信号，另一条光纤用于接收信号。大多数光纤的结构与图4-3给出的结构相类似。纤芯和包层由玻璃制成，光能通过这两个部分传播，纤芯和包层外面是防潮保护层。为增加强度，在光纤中加入Kevlar（一种合成纤维）层和其他一些材料，这样光纤就不易折断。光纤的最外层是一层聚氨酯。由于光纤无法为远端的中继器携带电能，因此如果越洋光缆中的中继器需要供电时，还必须加装铜缆。

由于纤芯和敷层的折射率不同，这样入射角相同的光束就能够在纤芯中保持不变，而使其他光束泄漏。如图4-4所示，不论光来自发光二极管（LED，Light Emitting Diode），还是发

注入式激光二极管（I.D. Injection Laser Diode），光束进入光纤后，由于全反射的作用都会沿光纤传输。

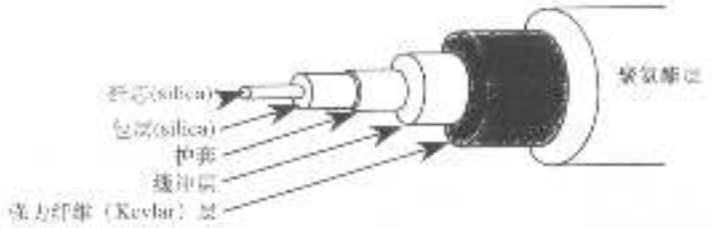


图4-3　典型的光纤结构

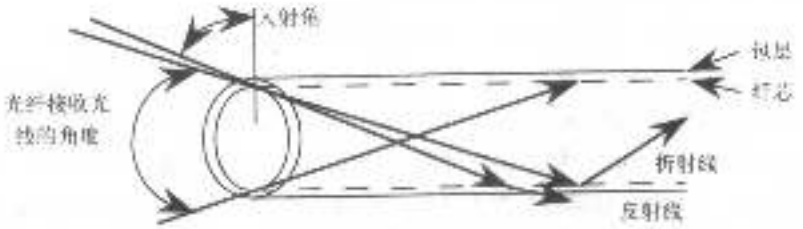


图4-4　光纤可以接收到的光束的入射角范围与纤芯的直径有关

4.4.3　光纤的分类

当光纤的纤芯直径较大时，会使更多的具有不同入射角的光束进入光纤。这种由入射角决定的光束的传输方式被简称为**模式**。所以，随着纤芯直径的增大，传播模式的数量也随之增加。这种光纤被称为**多模光纤**。在多模光纤中，很多的光束传输到终点时由于相位的不同会引起相互间的严重干扰。而单模光纤由于只有一种模式，传输光束时就不会受到来自其他模式的干扰。

根据纤芯和包层的不同构造，基本上可将光纤分为三大类：阶跃型多模光纤，渐变型多模光纤和阶跃型单模光纤。图4-5给出了上述光纤纤芯和包层的典型线径，剖面图显示了光纤各层的折射率分布。注意阶跃型光纤只有两种折射率值，这是因为在此类光纤的纤芯或包层中，折射率没有发生改变。而渐变型光纤其纤芯由折射率渐变的同心层物质构成。

阶跃型多模光纤中多个模式间存在严重的相互干扰，因此其带宽被限制在10MHz左右，传输距离仅为1km。阶跃型多模光纤的大部分能量在纤芯中传输，它是最易制造的光纤。

渐变型多模光纤的纤芯构成物质具有多种折射率，所以光线传输时不是发生突然的方向改变，而是在芯线中进行渐变的折射，如图4-5b所示。此类光纤的带宽约为10GHz。

单模光纤仅能高效地传送一种模式，其中约50%的能量在光纤包层中传输，其余的在纤芯中传输。由于不存在模式间的相互干扰，因此单模光纤的传输带宽可达到50GHz。此类光纤适用于长途传输，但因其芯径太小，故在使用时会造成一定难度。

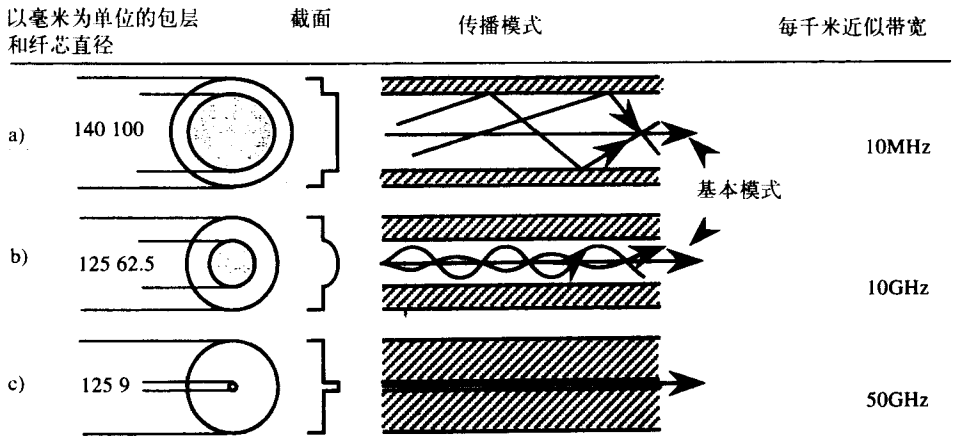


图4-5 a) 阶跃型多模光纤，b) 渐变型多模光纤，c) 阶跃型单模光纤

4.4.4 如何利用更多的带宽

20世纪80年代末期，电子再生器被用来沿光纤再生光信号，此过程可分为三步：首先将光信号转变成电信号，再对电信号进行再定时和波形再生，最后利用半导体激光将电信号再变回光信号。这种再生器不仅价格昂贵，而且在某一个特定的时刻只能对同一频率的光信号进行再生，还要求各种光信号的调制方式均为一种形式。

1987年，英国南安普顿大学的几位研究人员发明了掺铒光纤放大器。这种放大器可直接对光信号进行放大，不需先将其转化为电信号。现在，在同一根光纤中可传输由光源产生的不同波长的光信号，并由一个光信号放大器对它们同时进行放大。同时这种掺铒放大器还可以放大传输速率不同和调制方式不同的光信号。

掺铒光纤放大器是通过对小段硅光纤掺加铒离子而发明的。由二极管激光器发射的红外光束称为泵浦光束，铒离子吸收这种能量后被激活至高能态，如图4-6a所示。处于高能态的铒离子极不稳定，遇到入射信号光子就会释放能量回复到基态。吸收铒离子能量而产生的大量新的信号光子和原信号光子具有相同的波长和相位，因此光信号被放大了。

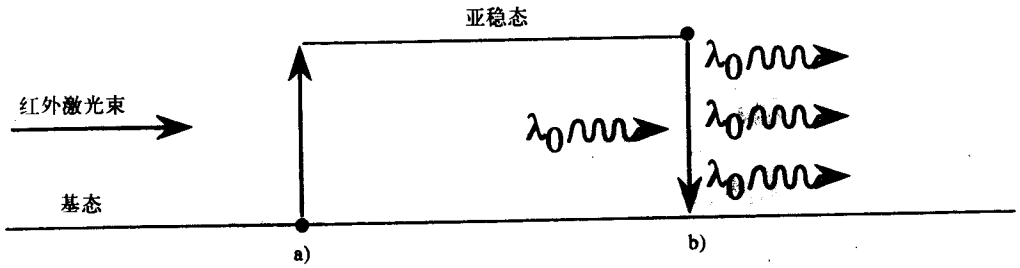


图4-6 a) 铒离子被红外光束激活到较高的能级；b) 由于该离子不稳定，所以会受到入射信号光子的激发回到基态，这一能级的跃迁会产生与入射光子相干的新光子

铒离子可发射1.53~1.56μm波长的光信号，这一波段恰好落在硅光纤的低损耗波长的范围内。掺铒光纤放大器的放大增益大于30dB。3dB增益即是将信号放大一倍，30dB增益意味着可将信号强度放大1000倍。这个数字是相当可观的。同时，由掺铒光纤放大器引起的噪声功

率也很低。

掺铒光纤放大器的许多优点使得在光纤中采用WDM（波分复用）变得简单易行。WDM已经在第3章中介绍过。同时光技术领域还包括许多其他的先进技术，比如光滤波器、光交换机和光路由器。

4.4.5　海底光缆

目前，光纤常被铺设在海底。铺设一条横跨大西洋的光缆需耗资5亿美元。但在完工之前，光缆容量就被抢购一空。投资商在两年内即可收回成本并获得可观的效益。

铺设海底光缆，只需安装光放大器而不必安装信号再生器，通常每隔60~120km安装一个放大器。信号再生器只再生原始信号，而光放大器会将有用信号连同噪声和干扰一起放大。所以在设计海底光缆工程时应慎重考虑，才能在接收端解调出正确的信号。

与光放大器相比，再生器更加昂贵、结构更为复杂、容易失效而且与频率有关。光放大器或掺铒光纤放大器就显得坚固耐用多了。利用WDM技术在海底光缆中传输多个不同波长的光信号时，光放大器也能对其进行放大。光放大器对频率变化不敏感，能再生任何频率的输入信号。海底光缆信号放大器或再生器的置换更新是一项耗资巨大的工作。因置换点的电缆必须从海底打捞到船上，所以精确的地图和定位方法对维护人员来说是至关重要的。海底光缆另一吸引人之处在于光缆两端都有能量源为光放大器提供能量，而且在光纤中传输的电能对光信号也不会造成干扰。这也是光纤的优点之一。

4.4.6　如何降低光纤成本

光缆末端通常使用SC和ST连接器。老式的ST连接器在制造中需要手工接合、胶固和抛光，这些工序都会使成本增加。在ST连接器顶端有一针状锁定装置，安装时插入插槽扭合后接头处即被锁定。进行传输时需要两个这种连接器分别用于收、发信号。使用时应先插入插槽后再扭合固定。图4-7a显示了新型的SC连接器。它顶端有一推进式锁定装置。目前，有的SC连接器也使用一种卷曲式锁定器进行安装。这种方式能令安装时间减少到2~4分钟。ST和SC这两种连接器体积均是常用RJ-45连接器的二倍，且安装不便。

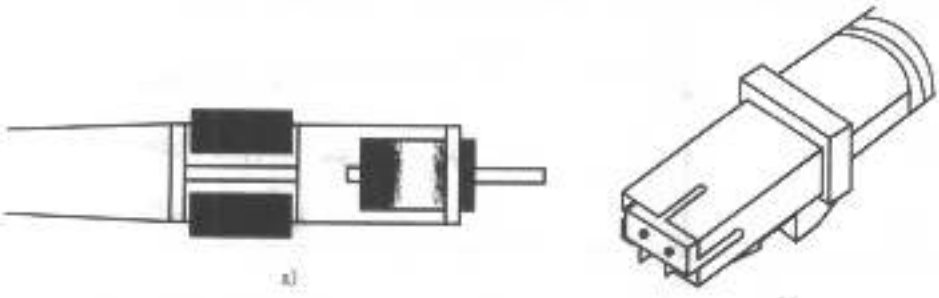


图4-7　a) SC光纤连接器，b) MT-RJ光纤连接器

在建筑物中铺设光纤，大约有1/3的成本要耗费在光纤连接器部分。鉴于此，生产商研制出一种只有ST和SC连接器一半大的新型光纤连接器。这种连接器和RJ-45连接器体积相同，能与RJ-45墙式插槽相匹配。而且安装时也会发出嗒嗒的声音来确认安装到位。这种连接器在

制造时不需进行环氧胶固及抛光，因此其成本较低，但在有些地方它容易折损。

目前，对光纤连接器TIA还未制定出统一标准。图4-7b是一种称为MT-RJ的光纤连接器。使用这种连接器的光纤系统能给用户带来诸多好处。例如当某些局域网设备如集线器、交换机和路由器等需要增加多个光纤出口时，使用MT-RJ连接器会更加经济合算。光纤可以进行长途传输，因此在建筑物中进行布线时只需很少的配线架（有关配线架的内容留在本章最后介绍）。这些因素使安装光纤的成本低于安装某些新型双绞线的成本。在认真考虑过光纤的诸多优点之后，人们就会对使用5类双绞线是否实用产生怀疑。

4.5 短距通信解决方案

4.5.1 微波无线电

铺设长距离的光纤是一项耗资巨大的工程。首先铺设光纤必须获得许多部门的批准，这通常是很难办到的。光纤铺设完工后，如遇到其他不知情人员在施工中的猛烈撞击，可能会导致光纤受损，使通信中断。如果通信中断的时间过长，光纤通信运营商不久就会面临破产的窘境。

比较而言，建造两座发射塔进行微波传输来满足通信要求就简单多了。微波通信工作在2~23GHz的频率范围，此波段共分为5个等级。微波通信的传输距离主要受塔高和地球曲率半径的限制，一般只有60英里左右。用微波传输数字信号的传输速率可达44Mbps。

搭建一个微波通信系统可在一天内完工并投入运营，其成本要比使用铜缆或光纤低很多。微波通信系统的寿命理论值为20年。在投资初期，运营商可选用低成本设备，在用户数增加到一定数量时再进行扩容。

目前，很多通信网利用微波系统作备用设施。例如：使用光纤接入中心局的站点可同时将接入备用中心局的微波线路作为备用，这样便能有效防止通信线路的中断。微波系统可通过高能变换器（LEC）使信号输出功率达到峰值（POP）。

微波通信的主要问题是它正处在向美国联邦通信委员会（FCC）申请运营许可证的过程中。当然，FCC已颁发了微波通信的临时许可证。微波通信的另一缺点是若传输路径上有高大建筑物阻挡，那就只能选择另一条通信路径。

4.5.2 红外线

短距离通信也能通过激光和红外线实现。微波属于无线电信号，而红外线属于光信号。它们都是电磁波，在电磁波的频谱范围内，如图4-8所示。在红外系统中，由于天气原因（如雾、雨等）造成的信号衰减，比微波系统严重得多。所以红外系统的通信距离一般只有1英里左右。

与微波通信一样，红外系统的传输速率也能达到44Mbps，而且同样价格低廉，易于安装。红外线波长甚至比微波还小，它们均可用于室内局域网通信。建立局域网的最大花费是安装布线，而且一旦建成后再改变其位置非常困难。因此，在局域网中使用红外线或其他的无线接入手段会使整个网络运用更加灵活。与微波相比，红外线有一重要优点，即不需要任何运营许可证。

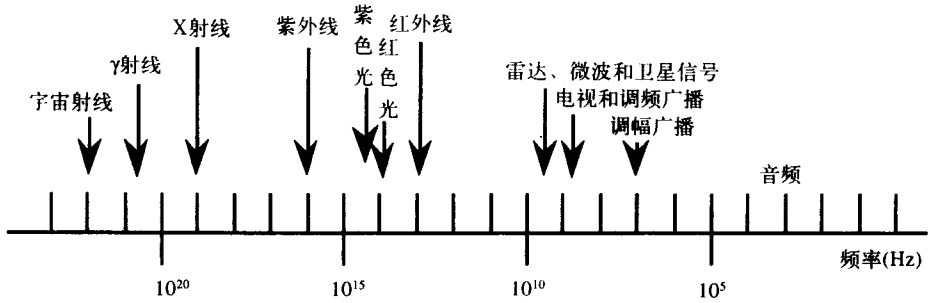


图4-8　电磁波的频谱，其中可见光频率为10^{14}Hz。从站点www.fcc.gov/oet/spectrum可以查到完整的表格

4.6　卫星通信

4.6.1　概述

单通道短距通信系统可实现本地电话接入，而卫星通信基本上能实现全球范围内的通信，使用户接入整个PSTN。放置在距地面22 300英里的高空，自转周期和地球相同的人造卫星称为**同步**卫星。一个典型的卫星通信系统通常使用10~46个收发器即可实现全球覆盖。这些收发器实际上是一种微波中继器；它先对来自上行链路的同频信号进行放大，然后再以不同的频率将它们转发出去。（低轨道卫星（LEOS）是较为新型的卫星。）

地面上可以接收到卫星发射信号的范围称为**覆盖区**。卫星信号在空间传输一个来回的传播时延一般为300ms左右，这比地面通信的传播时延大得多，因此在用于远端数据通信时有很大的局限性。

卫星通信属于广播系统，处于覆盖区内的任何一个站点能同时收到卫星发射的下行链路信号。比如：在美国，不同地区印刷的报纸通过卫星能更快地传播，比地面点对点通信节约很多时间。但从安全性考虑，卫星通信的保密功能较差，通常为提高保密性都会对信号进行加密。

表4-1列出了卫星通信的三个工作频段。其中C频段，即6/4GHz频段，是使用最早也是应用最广泛的频段。目前C频段容量已满，人们开始更多地使用Ku频段。与Ku频段相比，C频段信号强度较弱，地面站规模也较大，而且更易受到微波无线电波的干扰。但C频段信号较Ku频段抗雷雨和其他天气干扰的能力更强。

表4-1　卫星频段

频段名称	频段别名	上行链路频率	下行链路频率	有效带宽
C	6/4	5.925~6.425 GHz	3.700~4.200 GHz	500 MHz
Ku	14/12	14.00~14.50 GHz	11.70~12.20 GHz	500 MHz
Ka	30/20	27.50~30.00 GHz	17.70~20.20 GHz	2500 MHz

人们最初在规划卫星通信时，采用频分多址接入（FDMA，Frequency Division Multiple Access）方式在不同用户间划分频率资源。目前，更常用的是时分多址接入（TDMA，Time Division Multiple Access）方式。在图4-9中，有3个站点分别使用这两种接入方式，同时使用相同的卫星。

若采用FDMA，则各站点同时发送信号，每个信号被分配一部分有效带宽；使用TDMA方式，各站点只需要依次轮流发送信号，但每个信号在发送时可占用整个有效带宽。



图4-9 a) FDMA，地面站采用不同的频率同时发送；b)TDMA，划分时间，在相应的时隙中轮流发送

4.6.2 甚小口径地球站

20世纪60年代末人们就利用同步卫星进行通信，但只有大规模的商业运营其投资才是经济合算的。直到1984年甚小口径终端（VSAT，Very Small Aperture Terminal）的出现才使卫星通信普及起来。VSAT是根据这种人造卫星的微型小天线来命名的，过去这种天线的尺寸范围是1.2~2.4m，而现在只有18in。VSAT可工作在C频段，但更多的时候工作在Ku频段。

VSAT系统常用于低速信息传输如信用卡授权、库存控制和生产监控等，因此VSAT系统的大客户多来自自动化、零售和金融领域。图4-10是20世纪80年代末星型结构的VSAT系统。目前，有些VSAT系统也使用网状结构。

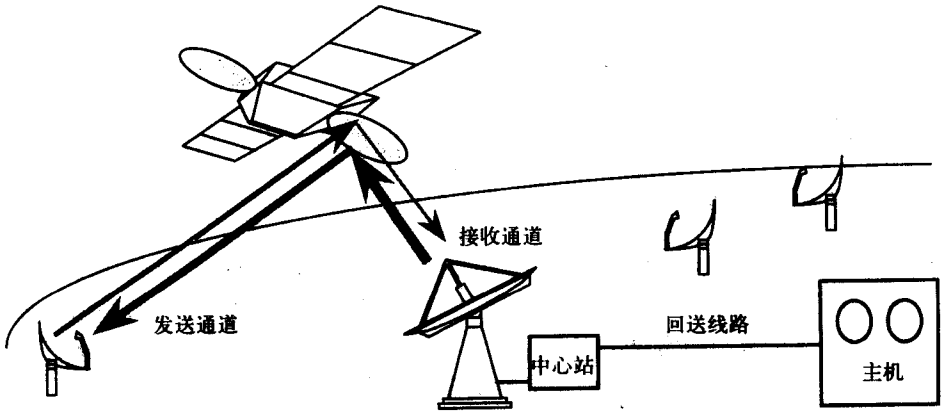


图4-10 星型结构的VSAT网络，箭头的宽度表示被传输信号的强度

在星型结构的VSAT系统中，需要一个装有大天线的中心站为那些装有小型天线的远端小站提供服务。Shell Oil在其网络中设置了5000多个远端小站。中心站的大型天线能发射强度足够大的信号，使任一小站均能收到下行信号。同时它具有很高的灵敏度，能接收到VSAT小站发出的微弱信号。从中心站到每一VSAT的通路被称为**发送通道**，传输速率可达20Mbps；而从VSAT到中心站的通路被称为**接收通道**，传输速率为1.7 Mbps。

VSAT系统的这种星型网络结构要求所有通信业务共用一个中心站。因此当两个远端VSAT之间要建立通信时，必然会出现时延。而且，由于中心站造价昂贵，因此，通常是多个用户共享从卫星服务提供商那里租用的一个中心站。

VSAT通信系统有很多优点，它使相距很远的地区的通信变得简单快捷。全球范围内电信标准的不断融合，使得VSAT系统在安装运行时不会遇到什么障碍。但只有VSAT服务提供商能对网络进行维护、排障和调整，即便是覆盖几个不同国家的VSAT系统也是如此。当VSAT系统跨国境接入不同的地面通信系统时，新建一个通路能减少通信冲突和时延。在欧洲建立一条ISDN专线需要等三个月，而建立一个VSAT站点则只需一个工程师一天的时间。而且即

便是在没有良好地面系统的国家，建立VSAT站点并投入运行也是丝毫不成问题的。目前，VSAT的新型小天线安装起来更简便，从原来需要两个技术人员减少到只需一个，而且也减轻了屋顶的承重，并使视觉效果更美观。

与地面通信方式不同，VSAT系统的通信费用与通信距离无关，而是与VSAT站点的数目相关。而且在必要时，VSAT站可调整到不同位置来实现网络优化。VSAT系统通信质量良好，可靠性高于99.5%，误码率可达10^{-7}，而铜线的误码率有10^{-5}。同时，VSAT通信系统的非对称式传输使它成为因特网应用的最佳选择。非对称式传输是指发送通路和接收通路的传输速率不同。Web服务器和浏览器之间的数据通信就是典型的非对称式传输。而且，VSAT系统可在不添加任何硬件设备的条件下增大信道带宽。

VSAT的优点：

1) 一个业务提供商。

2) 较小的天线。

3) 管理灵活。

4) 动态带宽分配。

5) 安装迅速。

6) 非对称式传输，适合因特网应用。

7) 不依赖地面网络的结构。

VSAT的缺点：

中心站：易出现单点故障。

4.6.3 无中心站的VSAT系统

当VSAT站点的天线增大到5m时，站点间的通信就不需再经过中心站转接，而可直接进行通信。不需中心站的系统对卫星的要求更低，这样的网络结构称为无中心站结构或网状结构。由于VSAT系统的故障通常集中在中心站，因此无中心站VSAT系统的网络运行会更加稳定。同时VSAT站点规模的扩大（天线增大）也会使传输速率得到提高。

这种网络结构使VSAT系统能传输双路视频和局域网业务，而且可以在不丢失任何数据的情况下进行实时配置，如调整站点间的带宽，甚至在必要时对站点进行添加或删除。但这种结构在实际应用中一般不超过100个站点，不像星型结构那样通常可带有数百个VSAT小站，究其原因可能是，网状结构的VSAT小站的投资要比星型结构的投资大得多。

4.7 建筑物的布线

在本节中，将介绍如何在建筑物中对传输介质进行布线。建筑物的布线规划、安装、维护以及建立文档是网络规划的重要部分。合理安排这几项内容会使网络专业人员的工作得到简化，同时也能使电缆的使用寿命延长，并可使服务质量得到提高。

4.7.1 安装配线架的必要性

从用户办公室的电话机到用户交换机(PBX)不论是使用双绞线还是使用光纤，都需要进行规划。我们不可能用一根5类线将电话机直接连到交换机背板的接口上。那么我们需要变更电话时怎么办呢？如果电缆直接与电话机相连，需要变更时只好将其电缆割断，然后再重新接

在新话机上。实际中通常是将电缆接到室内的分线盒上，这种方式能使以后的变更更加灵活，例如接新话机时只需一个抽头就足够了。同理，在更新交换机设备时也不必将所有的连接点都断开重新连接。可以使用**配线架**来连接交换机和不同地点话机之间的电缆，在配线架上用跳线便可将两端接通。

在图4-11中，一部使用RJ-45接头的电话机通过配线架与交换机连接。从交换机引出的电缆接入配线架的一组下推式模块上，同样从用户端引出的电缆与另一组模块相接，模块端子间使用交叉的跳线相连。所以，配线架也被称作**交叉连接系统**。

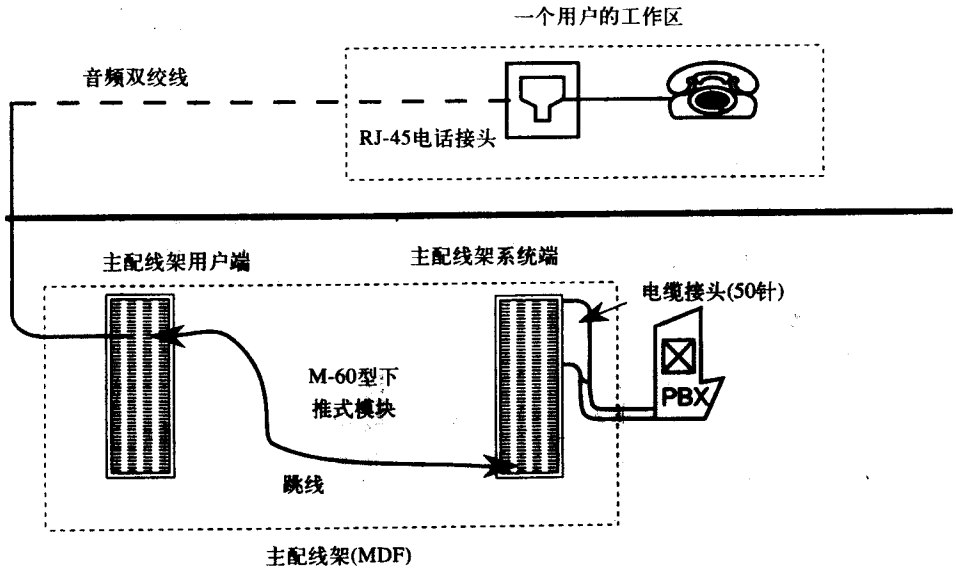


图4-11 墙上的插槽和配线架提供了更大的灵活性

如果一个搬家到另一个局所辖区的用户想保留原来的电话号码，则可将接至交换机的原配线架端子用跳线接入到连接用户的新端子口。在配线架上使用跳线进行变更比直接在交换机背板上变更更为简单、整齐，而且故障检修也可直接在配线架上完成。由于配线架具备使用灵活和易于管理的特点，因此大型建筑通常在不同地方放置若干个配线架。其中，中心配线架被称为主配线架（MDF，Main Distribution Frame），较小的配线架被称为中间配线架（IDF，Intermediate Distribution Frame）。这样的配置使楼宇布线更加系统化和层次化。图4-12是一个配线系统。

4.7.2 建筑物布线的五个区域

图4-12显示了建筑物内布线的各组成区域，这些布线区域包括工作区电缆、水平电缆、骨干网电缆、远程通信机柜和机房。从工作区到中间配线架由水平电缆连接；目前，骨干网电缆越来越多地采用光纤，它是连接中间配线架到主配线架的电缆，同时也与来自中心局CO的电缆入口设备相连接。从中间配线架到主配线架的电缆一般总是垂直安装的，因此也被称为直立电缆。在规划水平布线时必须周密仔细，因为水平电缆不仅数目繁多，而且更换也很麻烦。

数据电缆的布线规划也是一样。大部分的工作区不仅布有话音线，同时还有数据线。5类双绞线既适合传输话音又适合传输数据，所以话音线和数据线均可采用5类双绞线。这样布线工作变得更简单、廉价，但必须做适当的标签或记录来区分它们。

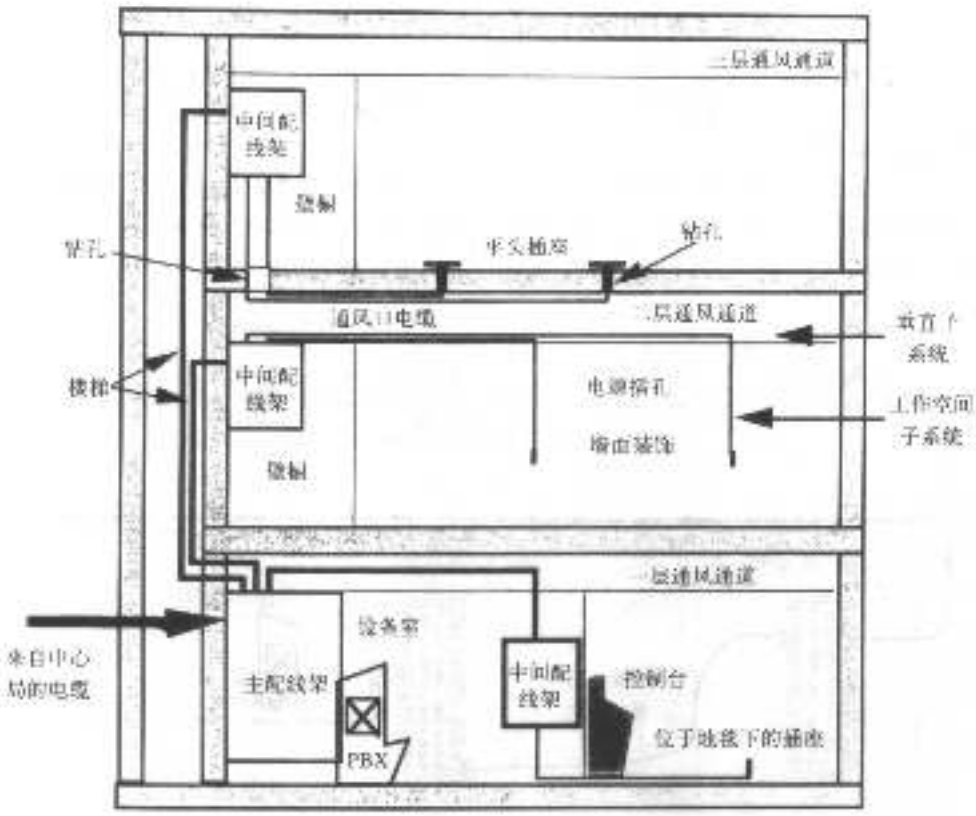


图4-12　配线系统各组成部分（被Robert Bronson采用）

4.7.3　数字接入和交叉连接系统

由于大多数工作人员在配线架上添加或删除跳线时没有做记录的习惯，因此可以使用数字接入和交叉连接系统（DACS，Digital Access Cross-connect Systems）来代替配线架。如果用数字交叉连接交换机取代了所有的中间配线架和主配线架，那么今后技术人员就不用再到中间配线架所在的大楼、房间，任何线路的变更都可以在管理控制台上完成。控制台的工作人员只需执行相应的操作，就可以实现线路的更换、添加或删除，不再需要跳线。使用这种在交叉连接系统上所做的电子连接，就无须再担心跳线的连接是否到位、是否工作正常；在配线架布线的施工人员离开公司或生病时，也不必再依靠那些过去的工作记录和个人的记忆。因为DACS管理控制平台会保存精确的记录，几乎不会错，利用数字交叉连接系统完成线路的改变，发生错误连接的可能性非常小。

习题

4.2 节

1. 下面哪一种双绞线抗外部干扰能力最强？

a. STP　　b. 3类线　　c. 4类线　　d. 5类线

2. 下面哪一种方法不会使双绞线的传输可靠性降低？

a. 减小AWG　　b. 增加电缆中的线对
c. 增加每英尺的缠绕次数　　d. 增大电缆的传输距离

3. 什么原因可能导致传输线中的电能无法正常传输而被反射回去?
4. 3类、4类和5类双绞线的规范分别是什么?
5. 为什么说5类UTP是一种性能优良的传输线缆?讨论使用它的原因。

4.3 节

6. 宽带同轴电缆没有下面哪一种特性?
a. 用于CATV　　b. 可传输模拟信号
c. 用于以太局域网　　d. 使用放大器和分路器
7. 为什么在局域网中多采用基带同轴电缆,而很少采用宽带同轴电缆?
8. 从发射机到天线微波信号采用的传输介质是什么?

4.4 节

9. 光纤核心层在所有其他层的内部,是下面的哪一部分?
a. 纤芯　　b. 聚氨酯包层　　c. 包层　　d. Kevlar层(一种合成纤维)
10. 下面哪一个不是光纤的优点?
a. 抗噪音　　b.带宽更宽
c. 安装容易　　d. 可用于长距离通信
11. 什么样的光束能沿光纤传播?什么样的光束会泄漏?
12. 说出三种主要类型光纤的名称并讨论它们之间的区别。
13. 解释掺铒光纤放大器的工作原理及其优点。
14. 说出一些光纤连接器的名称并描述它们的使用方法及其特点。

4.5 节

15. 红外线传输比微波传输更为可取的是哪一点?
a. 不需要FCC的批准　　b. 可用于更远距离的传输
c. 不必担心电缆断裂　　d. 雨天对它的影响小
16. 与光纤传输相比,不是微波传输优点的是下面哪一项?
a. 不需要接入权　　b. 安装时间较短
c. 不必担心光缆的断裂　　d. 能提供更宽的带宽
17. 哪一种短距离解决方案受到天气变化的影响较小?

4.6 节

18. 在卫星系统中,下面哪一种多址接入方法使用户可以分享有效带宽?
a. CDMA　　b. DAMA
c. FDMA　　d. TDMA
19. 与光纤系统相比,下面哪一点是VSAT系统的优点?
a. 安装迅速　　b. 传输比特率更高
c. 不易出错　　d. 更易于管理
20. 哪一个卫星传输频段受天气和微波信号的影响较小?
21. 什么时候星型结构的VSAT系统优于网状结构的VSAT系统?
22. 老式卫星处于哪一种轨道?

4.7 节

23. 配线架的优点什么?

a. 噪音少　　b. 易于改变

c.带宽更宽　　d. 不需要记录

24. 下面哪一个术语与配线架没有关系?

a. IDF　　b. MDF

c. RDF　　d. 交叉连接系统

25. 数字接入和交叉连接系统的优点是什么?

26. 讨论建筑物布线系统的5个区域，并说明采用的原因。

第5章 商业网络服务

在本章中我们将快速地浏览可供商业用户使用的各种电信服务。在第6章，将研究住宅用户可以使用的服务。在本书的以后各部分中，将整章讨论这些业务以及支持这些业务的技术。开始学习细节内容以后（对这本书而言，是在开始学习某一技术的比特和格式之后），常常会忘记我们所关注的目的。利用这一章，我们希望找到每项业务出现的目的和这项业务的特性，具体到这些业务的实现细节将留给后面的章节讨论。

5.1 服务类型

5.1.1 交换接入

童年时代我们就熟知的最基本的网络业务被称为一般电话业务（POTS，Plain Old Telephone Sevice）。使用一对双绞铜线，连接一部住宅电话到一个中心局，从这个中心局住宅用户可拨打在PSTN或全球范围内的其他电话。与我们家相连的一条POTS线是**交换线路**的一个例子。尽管这条线路只从中心局连接到我们家，但正是这条线路使我们能够交换接入到电话网中。

交换接入提供了到PSTN上各点的连通性。我们不仅仅可以直接拨打一部电话，还可以利用众多的交换机，如CO、POP、MTSO等等，与PSTN上的任何人进行联系，交换机组可以支持我们完成这样的连接。因此，POTS线路为我们提供了交换接入的能力。

对于这条链路，通常需要根据通话时间和距离付费。在一次通话完毕线路断开之后，用过的中继线和交换容量可以被其他的用户再次使用。对于交换接入，所有的用户**共享**电信设备。因此，拨号链路为用户提供了**共享接入**，从而也降低了每个用户的费用。

在图5-1中，两个终端用户（或者说是电话机）之间建立了一个连接。只要连接存在，交换机和中继线就被保留。CO（中心局）和POP（电话接入站点）通过中继线相互连接，而这些中继线先被连接在配线架上，然后再通过配线架与交换机相连。

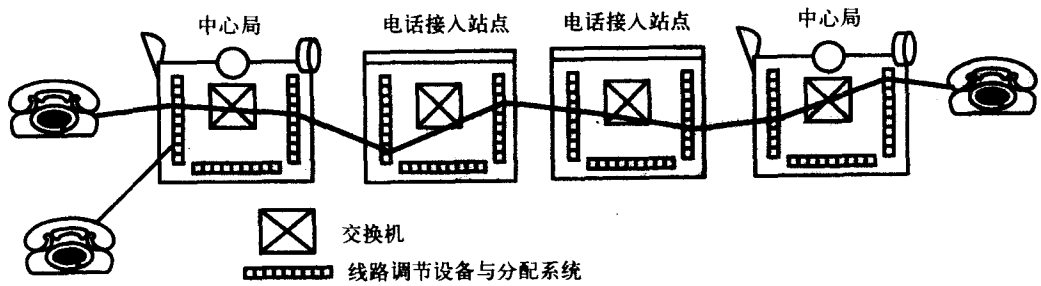


图5-1 交换接入连接仅在通话时使用交换机和中继线

如果在发起呼叫时，路径某一段出现拥塞，用户只能稍后再试。但是今天PSTN中的备用

路由降低了呼叫拥塞的可能性。由于接入交换机采用模拟线路，因此连接质量低，数据传输速度通常会受到限制，仅能用于低速传输。此外，由于与公共电话网上的其他用户共享网络设备，因此安全性也是交换接入需要考虑的问题。然而，通过让被呼叫地的用户给呼叫用户回电话确认其地址（或电话号码）可以解决安全性问题，但是这样做需要花费更多的时间，无形中增加了通话的费用。

5.1.2 专用接入

在图5-2中，工作在不同城市的公司员工经常需要在整个工作日内连续不断地互通电话。如果PBX使用交换接入，且每次都通过PSTN连接到另一个城市，话费会非常高。在如图所示的两个固定端点间业务量非常大的情况下，更经济有效的方法是在这两个端点之间建立一条永久的**专用线路**。这样，不管专用线路被占用多长时间，每月只需向电信运营商缴纳固定的费用。与交换接入按通话时间的长短收费不同，专用线路的费用是固定的。专用线路还被称为**直通线路**和**专用线**，用于提供特定用途的接入。

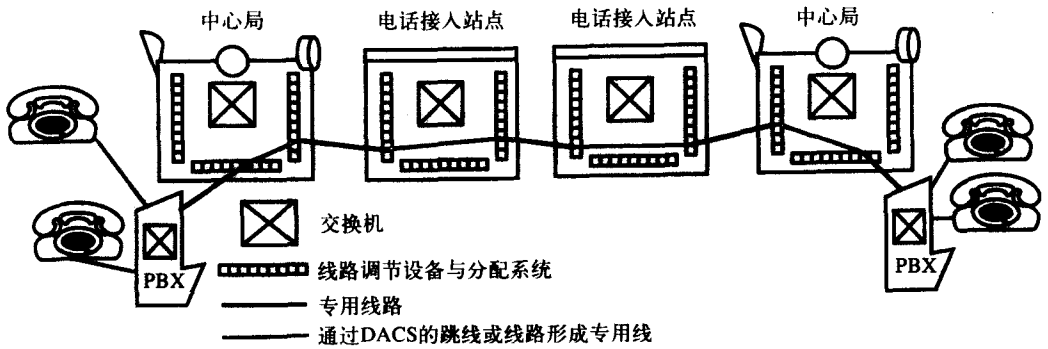


图5-2　一条连接了两台PBX设备的专用线路，这两台PBX（用户交换机）在不同地点。这条专用线路可以在两点之间建立永久的、非交换连接

注意在图5-2中，中心局的配线架是来自PBX中继线的终止点。为了与通往POP的中继线实现交叉连接，在两个配线架之间必须使用物理跳线将对应的点连接起来。在专用线路供商业用户使用之前，技术人员必须正确配置每个CO和POP内的跳线。事实上，目前使用更多的是第4章提到的数字接入和交叉连接系统（DACS，Digital Access Cross-connect Systems），而不是实现配线架互连的物理跳线。无论情况如何，建立一条专用线路都需要一定的时间（也许是一个月），这与这条线路上被连接点的多少有关。这个过程被叫做**提供直通线路**。

如果一条专用线路被频繁地使用，就说明它的存在是必要的。如果这条线路的使用率不高，那么拆除这条线路并用交换接入替代它可能会更好。典型的做法是，即使有了专用线路，但在专用线路繁忙或者是出现了故障时，还会使用交换接入。增加还是拆除专用线路，需要根据统计理论对业务量状况进行详细的研究。

专用线路比交换接入线路安全。使用线路调节设备可以在配线架处对专用线路进行微调，因此与交换接入线路相比，专用线路的数据传输可靠性和传输速率更高。表5-1总结了这两种接入方式的差异。

表5-1 交换接入和专用接入的比较

	交换接入	专用接入
其他的术语	拨号链路共享接入	租用的、专用的或直通线路
例子	POTS、Sw64,ISDN	T1
可实现的连接	多点连接	与一点连接
计费	基于通话时间	每天的费用相同
安全性	差	好
连接质量	不好	好
总带宽	低	高，但质量越高，价格越昂贵
是否有多条路径	是	必须事先规划
接入快慢	拨号后几秒钟	安装配置完毕，立即接通
建立连接方式	信令连接	在DACS手工操作
建立连接需要的时间	2-4秒	提供时间大约30天
连接持续时间	典型值2-4分钟	几个月或几年
拆除连接需要的时间	1秒左右	几天，需要顺序拆除
扩展连接到一个新地点	只需拨号，是否连通与网络的可用性有关	必须等待安装，但可以为用户保留电路

5.1.3 专用网络

将一个单位在不同地点的多个办事机构连接起来的专用链路的集合被叫做**专用线路网络**。一个专用网，或者是WAN，可以把多个PBX（用户交换机）连接在一起，如图5-3所示。所有的CO、POP和其他的中间点都简单地被看作是一个PSTN云图。为了访问那些不在专用网络中的客户和节点，还需要PBX到PSTN的交换接入链路。交换接入链路还能为专用链路网的业务，也就是各PBX之间的通信业务提供备用路径。

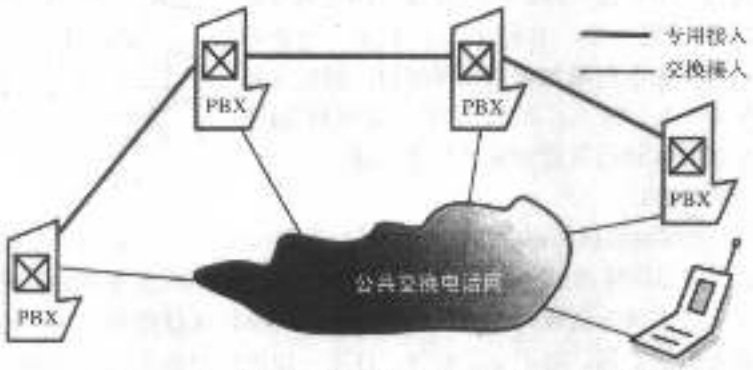


图5-3 在专用网中，利用专用链路可以将许多专用的PBX互连在一起。然而利用交换接入链路，这些PBX还能与PSTN中的任一节点建立连接

这样一来，单位内部的业务大多数利用专用网络传送，需要与其他地点建立连接的业务通过PSTN传送。这个专用网所拥有的单位下属的各办事机构，如一个旅游销售点或一个小型异地办公室，都可以通过PSTN与专用网相连。如果需要LAN与专用的WAN相连接，则需要用路由器来代替PBX。

5.1.4 虚拟专用网

在一个专用网络中，如果一些地方使用交换接入，另外一些地方使用专用接入，就使网

络管理变得十分复杂。为了节省费用，用户就必须不断地监视业务，以决定如何配置网络。另外一种创建专用网的方法是让一个局间交换运营商IXC（如AT&T或Sprint）处理所有的业务。不论这个业务是发送给专用网上的节点（如PBX），还是发给公共网络上的节点（或PSTN），这种用公共网络上的设备组建的专用网被称为**虚拟专用网**（VPN，Virtual Private Network），或简称为虚拟网络，如图5-4所示。

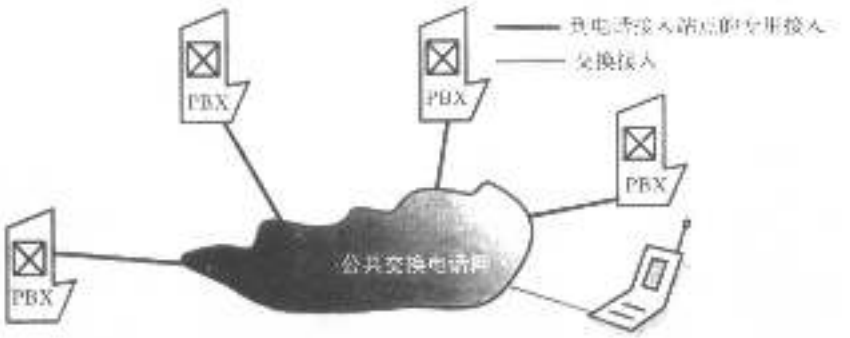
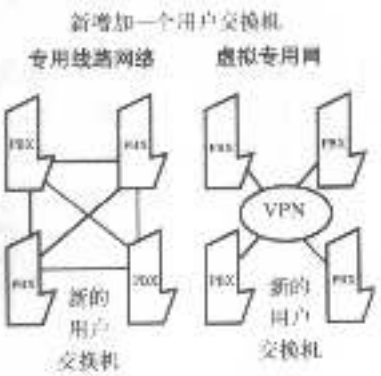


图5-4　为了实现交换接入，必须使用PSTN云图。既然这样，为什么不利用PSTN来承载专用网业务呢？用公共网构建的专用网被称为虚拟专用网

现在，专用链路不是建立在PBX之间，而是建立在从PBX到POP内的交换机之间。一旦专用网的业务到达运营商的POP，这些业务就利用运营商的公共交换机实现路由。可以将这种结构想像成一个星型拓扑，在这个拓扑中运营商的网络是其中的一个节点，或者想像成是一个集线器，所有PBX都被连接在这个集线器上。业务不再通过专用联络网络的PBX转接，而是通过虚拟专用网（VPN）实现交换。在这个拓扑上加一个新的PBX非常简单。PBX也不需增加新的物理端口；同时在新增的PBX和已有的PBX之间，不必架设新的长途专用链路。这时，只需要在新PBX到运营商的交换机之间建立一条短距离接入链路（见右图）。



运营商或IXC如何解决虚拟网络的配置问题？运营商的SS7（7号信令系统）上的各种节点和数据库决定了虚拟网络的配置。7号信令系统还了解话费状况并知道如何处理呼叫。管理这样的网络现在已经变成运营商的事情，顾客或者一个单位仅仅是使用它。还有，对顾客仅收取占用运营商资源的费用。对于专用网络，在某一段时间内如果用量增加，可以被分配额外的带宽。然而在其他大多数的时间里，这种过量的提供可能会造成浪费。

因特网也可以使用这种方法。当一个单位利用因特网在两个不同的地方之间传送信息时，也被称为VPN。在这里，公共网再次（这时因特网代替了PSTN）被用来创建专用网络。利用公共因特网创建的VPN比刚刚谈到的VPN对安全性问题更加关注，这是因为通过因特网的业务要经过多个环节和多个单位来路由，没有任何一个运营商负责处理所有的业务，就如同在一个PSTN中，只使用了IXC的一部分来创建VPN一样。对于因特网VPN，每一个单位负责监视自己VPN的完整性和安全性；但对于话音VPN，情况却大不相同。由于拥有POP，SS7网络的各部分及其数据库，因此IXC能较好地控制所管理的VPN上流过的业务。另一方面，因特

网VPN更便宜，许多小公司都可以配置创建它。因特网VPN是第27章的主题。

5.2 中继线类型

我们已经知道在专用网络中，一个PBX如何与另一个PBX、POP以及CO（中心局）相连接，也曾经提到PBX需要通过交换接入链路才能连接到PSTN上。本节将简单介绍一些PBX经常使用的特定类型的连接线。

在配线系统中，用户配线电缆和电信公司配线电缆的连接点称为**电缆的分界点**，或简称为分界点。

直通中继线、专用线路和租用链路，实际上都是一回事。直通中继线如图5-5所示。现在看一下其他方式的连接线。

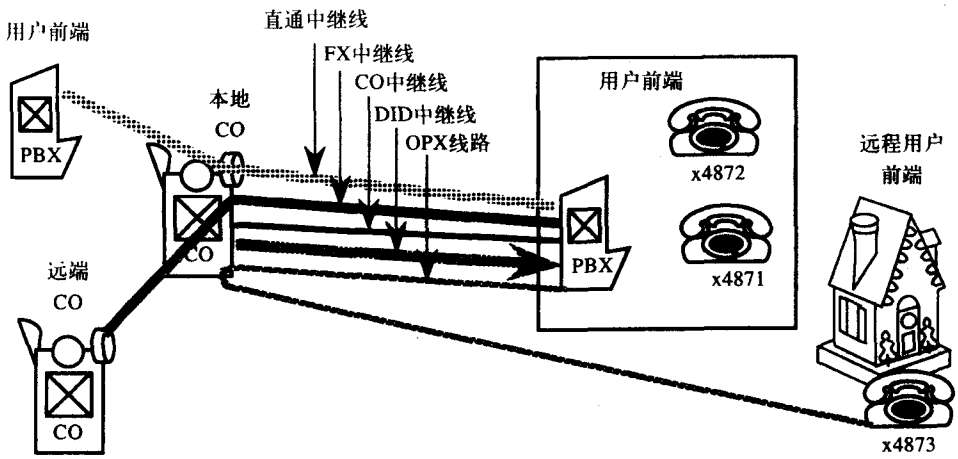


图5-5 用于PBX的各种中继线

5.2.1 CO中继线

与PBX连接的电话几乎不可能同时都需要对外通话。在布线时，大多数情况下并不是让每一部电话都拥有一条单独的外线，通往本地CO的中继线数量要比电话数少得多。所有的电话共享这些中继线，这样在保证每部电话都能接入到PSTN的同时，降低了费用。

图5-5所示的CO中继线是用于CO和PBX之间最常见的中继线，它使PBX能够交换接入到PSTN。公共网络上的人能通过CO中继线拨号进到PBX，专用网络上的电话也可以通过CO中继线向外拨出，因此CO中继线是一条双向中继线。

5.2.2 DID中继线

直接拨入电话（DID，Direct Inward Dialing）是单向中继线，仅用于将呼叫连进专用系统。通过CO中继线进入PBX的来话，通常需要话务员转接才能到达相应的分机；而与PBX一起工作的DID中继线可以将来话直接传送到相应的分机。

通常的做法是，分配给用户一个电话号码，这个号码可以是公共电话簿中的号码，也可以不是。这个号码即使用于分机也不需要添加额外的数字。当公共网上的人拨打DID号码时，CO会向PBX发出信号，通知它有一个呼叫正通过一条特殊的DID中继线到达。在PBX准备好

之后，CO发出至少4个左右的数字，以便PBX能够完成连接。在其他的时间，这条中继线同样可以被用来连接不同的PBX电话。

5.2.3 FX中继线

与CO中继线相类似的是外部交换（FX，Foreign eXchange）中继线。当客户需要拨打大量的外地电话甚至是国外电话时，使用FX中继线。如果呼叫通过LATA边界，那么IXC和它的POP都会加入到提供中继线的行列中来。有了FX，顾客能以每月统一的费用并按本地市话的价格从外地的一个地方拨打长途电话到本地。如果这个顾客有许多用户需要从外地拨打电话，这些用户拨打进入PBX的长途电话就如同拨打本地电话一样。换句话说，在考虑了每月固定的费用之后，再拨打外地长途电话只需按本地电话付费。

5.2.4 OPX链路

最后一种中继线不是真正的中继线，而是一条线路。因为它不是与交换机相连，而是与电话相连。建筑物外扩展（OPX，Off-Premise eXtension）线路通常将一个远端客户端连接到PBX上。如果主要的客户端与远端客户端被分开，比如被高速公路分开，这时不允许客户把自己的电话线连接到公共区域。电信公司允许客户通过所提供的OPX链路进行连接。

5.3 传输载波服务

5.3.1 T1载波系统

在一定的距离内数字信号通常通过铜线传输。用一对双绞线传送数字信号的方法通常称为T1载波系统。T1是在两对相互缠绕的双绞线（或4条线）上发送，其中一对用于发送，另外一对用于接收。T1是数字链路，所以要在这条直通链路的两端使用DSU（数据业务单元）。在这条链路两端的设备必须是数字的，而且如果在传输链路上装有负载线圈时，则必须去掉该线圈，通常是用数字再生器来代替。

T1从1963年由贝尔系统发展而来。1977年，T1第一次被开发并不是因为电话公司需要使用它。那时，在纽约市有两幢楼被一条拥有600个信道的铜质电缆连接起来。这条电缆的容量已经用到了极限，没有额外的线对与新的话音电路相连接。铺设另外一条电缆将意味着必须挖开街道，并且有可能破坏其他埋在地下的电缆和管道。采用的替代方法是在这条电缆的两端安装了一个信道处理单元（带有编码的多路复用器），并且仅仅使用了两对信道，就有24路语音信道可以被使用，如图5-6所示。

从20世纪60年代起，电话公司就已经开始使用这种T1多路复用技术，甚至比FDM（频分多路复用）技术用得都早。然而，在T1上的业务被故意抬高了价格，因为T1的安装会导致用户付费减少，从而使电话公司的收入下降。在摆脱了人为因素之后，T1的价格变得越来越现实，并且出现了将话音等级链路转变成为T1的热潮。

一个T1载波系统可承载PCM技术编码的24路话音信道（PCM技术在第3章中讲过。它以64kbps传输一路话音信号）。信令比特在一些经过数字化的话音比特之前传送。所以，用于一路话音信道的每64kbps不仅包含话音比特还包含信令比特。信令是传送摘机状态、拨叫音调、拨叫数字等内容的信息，将在第8章中讲述。

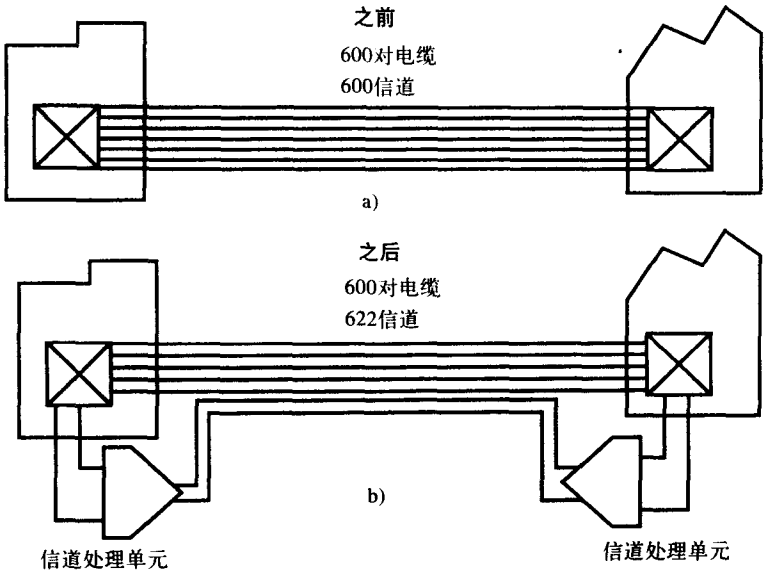


图5-6 a) 在纽约两幢楼之间配置T1前，用600对电缆来传送600路话音信号；b) 在已有的两对信道上安装了一对信道处理单元之后，增加了22个可用的话音信道

24路信道乘以64kbps，PCM的速率是1.536Mbps。然而，为了实现同步（或被称为成帧），还需要加上另外的8kbps，因此总速率达1.544Mbps。术语“T1”是指使用双绞线对来传送这个信号。但是，这个信号通常称为DS1（数字信号级1）。DS1可以在任何介质上传送，包括光纤。你可以认为T1是双绞线上的DS1，尽管在其他介质，如微波、卫星、同轴电缆或光纤上传输DS1时，人们常常错误地使用术语T1。

欧洲国家和大多数非北美国家使用一种不同的系统，叫做CEPT（欧洲邮政和通信管理委员会）系统。它定义速率从E1（European-1）级开始。E1级来自对30路信道的PCM编码。然而与T1不同，PCM编码不包括每个信道所需要的信令信息。E1专门使用一条64kbps的信道，为全部的30路信道传送信令信息，还专门用另外一条64kbps的信道传送帧同步信息。因此，总共有32条64kbps的信道，提供的总速率为2.048Mbps。从T1和E1派生出来的其他信号级别如表5-2所示。

表5-2 数字信号的层次结构

用于澳大利亚、加拿大、日本和美国				用于欧洲和大多数其他的国家			
信号类型	载波系统	速率（Mbps）	承载的信道数	信号类型	载波系统	速率（Mbps）	承载的信道数
DS0	—	000.064	1	CEPT0	—	000.064	1
DS1	T1	001.544	24	CEPT1	E1	002.048	30
DS1C	T1C	003.152	48	CEPT2	E2	008.448	120
DS2	T2	006.312	96	CEPT3	E3	034.368	480
DS3	T3	044.736	672	CEPT4	E4	139.264	1920
DS4	T4	274.176	4032	CEPT5	E5	565.148	7680

记住：在国际连接时必须想到T1不能直接与E1连接。除了信道数和信令方式不同外，用编解码器将声音转换成数字信号的方式也不同。如第3章所述，北美和日本使用μ律的PCM，其他相当多的国家使用A律。

另一个通用的可用服务是T3。再次声明，T3的名字用词不当，因为DS3从不在双绞线上传输。事实上，同轴电缆可以传输DS3，但仅在短距离通信中使用。T3的速率为44.736Mbps，可多路复用672个话音信道。使用M-13多路复用器，28个DS1信号可以被复用在一个DS3中。如果某些单位发现使用T1速率太高，使用DS-0信道(64kbps)速率又太慢，可以选择“部分T1”(FT1，Fractional T1)。FT1可提供从DS0到DS1间的各种速率。原则上，运营商可以根据FT1向部分使用T1服务的客户报价。此外，顾客需要的带宽大于T1，但小于T3时，也可以使用部分T3服务。

T载波系统的一个主要问题是需要在比特流中随机地添加额外的比特来保持传输的同步。这些细节将在有关T1的章节中进一步讨论。因此，T1的速率不恰好是1.544Mbps，可能上下变化75bps，这就导致了**非同步多路复用**。在非同步的多路复用中，设备无法只访问其中的一路信道，同时也无法下载它和使用它，或者说当其他的信道都正在通过一个设备直接传输时，该设备无法增加另一路信号。换句话说，当所有的被传输信道通过一个节点时，如果需要对其中的一个信道解多路复用，那么首先必须对所有的信道解多路复用，然后再将传给下一个节点的信道重新多路复用。

为了解释清楚这一点让我们来看一个例子。在图5-7a中，在丹佛（Denver）的一个站点使用多路复用器向奥马哈（Omaha）传送两路信号。其中一路信号的目的地是奥马哈，另一路的目的地是圣路易斯（St. Louis）。使用同步多路复用技术，通往圣路易斯的信号可以直接通过奥马哈的多路复用器。传给奥马哈的信号被下载之后，通往圣路易斯的T载波上有一路信道被释放。在那条被释放的信道上，可以加上另一路信号，如图所示。奥马哈的这种结构被称为增减多路复用器，或者被称为下载-加载多路复用器。因为一条线路可以从载波中被去掉，而不会影响到其余的线路。其他的线路也可以被插入或者被加入。

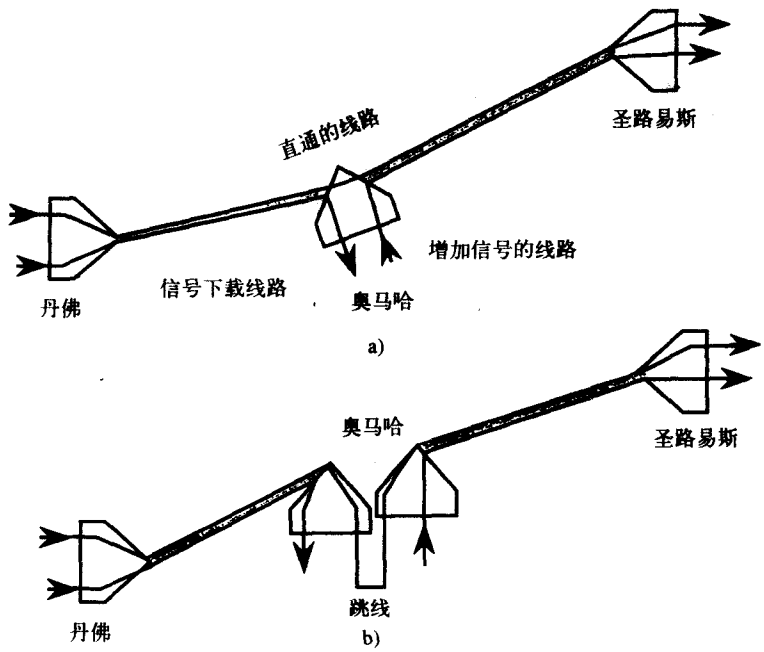


图5-7　a) 不用解复用，同步多路复用技术就可以直接加载线路；b) 对于非同步多路复用，必须使用两个紧接的多路复用器先对所有的线路解复用

然而，对于T载波情况就不同了。如图5-7b所示，T载波使用非同步多路复用技术，这种技术需要所有的信道都被解多路复用，而且通往圣路易斯的那个信道必须使用另一个多路复用器再次被多路复用。这是因为每秒可能要插入或删除最高达75个比特，使多路复用器很难确定哪些比特属于哪个信道。如此一来系统的效率变低，费用升高，同时还难于管理。奥马哈站点使用的结构被称为“紧接多路复用器”。5.3.2节要讨论的同步光网络（SONET，Synchronous Optical NETwork），通过采用同步多路复用技术，解决了这个问题。

使用一个可笑的比喻：设想商用飞机能够让小型的“子飞机”附着在它的机身下面。那么一架从丹佛到圣路易斯的飞机就不必为放下那些下飞机的乘客而在奥马哈降落。到奥马哈的乘客可以乘坐主飞行器下的“子飞机”在奥马哈着陆。类似地，那些从奥马哈前往圣路易斯的乘客能够乘坐类似的“子飞机”，“加”到主飞行器的下面。这种运送乘客的方式与同步多路复用技术相似，而目前采用的运送乘客的方式实际上相当于非同步多路复用技术。记住，多路复用是在同一条链路传送许多路通信信号，这类似于在同一架飞行器上运送许多乘客。

5.3.2 同步光网络（SONET）

贝尔实验室设计了T1，用于在金属线传输24路数字话音信号。T3技术是T1技术的扩展，引入的目的是为了在微波系统上支持672路话音信号的传输。由于T1和T3都是基于电信号的传输方式，因此还需要一种适合于光信号传输的新技术。这种技术应该尽可能地解决T载波系统中存在的固有问题，使组网更加容易。

1985年，贝尔通信研究中心（Bellcore）在同步光网络（SONET，Synchronous Optical NETwork）的规范中提出了解决这些问题的方案。从那时起，SONET逐渐变成美国国家标准化组织(ANSI)的标准，并被ITU-T称作同步数字层系列（SDH，Synchronous Digital Hierarchy）。其中“光纤”一词被ITU-T去掉了，因为那时正在用其他的介质，如数字微波来传输SONET。

SONET是使用电路交换同步多路复用技术传输高速信号的多层协议。通过图5-7a，我们已经知道了同步多路复用技术的优点。它是WAN能使用的唯一一个高速光纤系统标准，而WAN是使宽带业务成为现实的载体。各种光载波类型可以参见表5-3。由于SONET是一个标准，因此不同制造商生产的终端设备都是兼容的。在SONET中，这种能力被叫做向中对齐（Mid-Span Meet）。SONET还提供了管理信道，这种管理信道使网络的管理、故障排除、重新配置和监视更加容易。

表5-3 SONET的各种关系

光载波表示	同步传输信号	与SDH相对应	线路速率（Mbps）	有效负载速率（Mbps）
OC-1	STS-1	-	51.84	50.112
OC-3	STS-3	STM-1	155.52	150.336
OC-9	STS-9	STM-3	466.56	451.008
OC-12	STS-12	STM-4	622.08	601.344
OC-18	STS-18	STM-6	933.12	902.016
OC-24	STS-24	STM-8	1244.16	1202.688
OC-36	STS-36	STM-13	1866.24	1804.032
OC-48	STS-48	STM-16	2488.32	2405.376
OC-96	STS-96	STM-32	4976.64	4810.752
OC-192	STS-192	STM-64	9953.28	9621.504

国际互联比T1与E1之间的互联简单。从表中可知，信令标准匹配，SONET和SDH在其他方面也同样是兼容的。大多数设备有一个简单的开关，用户可以选择SONET接口的终端，或SDH 接口的终端。

5.3.3 综合业务数字网（ISDN）

目的：设想一下在我们的家里，电冰箱、收音机、烤面包机等需要不同的电源，每种电器都必须有自己的电线，而且插头又互不兼容。那么我们就不能像现在一样随心所欲地移动各种电器，因为这些电器不能插到其他类型的电源插座之中。尽管这听起来有点古怪，但是我们现在的电信服务就是这样一种连接状态。顾客必须在不同的网络上传输话音、交换数字数据、分组数据等，因为这些网络的运行标准是不同的。

综合业务数字网（ISDN，Integrated Services Digital Network）将这些业务集成在一起。现在，一个公共的插座（RJ-45），类似于普通的AC插座，可被用来综合访问各种业务。目前，许多建筑物中都有分别布线的网络，用于传输话音、视频、数据和安全警报信息等，这些网络之间是相互独立的，如图5-8a所示。有了ISDN，所有的业务可以使用相同的电线（和插孔），成为一个综合体，如图5-8b所示。实际上，每个设备不需要像以前那样使用单独的电线，多台设备可以享用同一根电线。因此，ISDN提供了灵活性，促进了现代的便携式终端的出现；ISDN也提供了有效性，使多个终端可以共享一条线路。

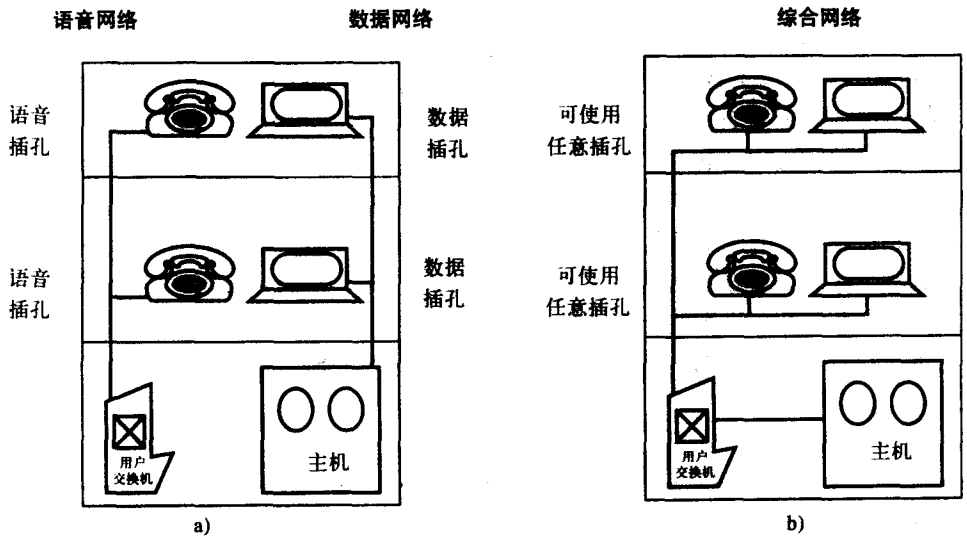


图5-8　a) 没有ISDN，声音和数据终端需要分别连线；b) 有了ISDN，所有的终端可以使用同样的导线，所有的插头可进入相同的插座

ISDN是PSTN的自然演变。PSTN起初是为在模拟线路上传送话音而设计的。但是到了20世纪50年代，又开发了调制解调器来传送数据。然而，由于传输速率和调制解调器质量的限制，运营商们不得不建立独立的数字传输网络来支持高速度、高质量的数据业务。然而，为了消除各种网络服务的不兼容性，ISDN的概念应运而生。

尽管现在转换成ISDN的成本相当高。但随着时间的推移，可能会证明在ISDN 上传输声音和数据比在现有的一般电话业务（POTS，Plain Old Telephone Service）上传送声音和数据

更加经济。居民可连续地使用同样的两根电话线作为本地回路。由于网络将全部被数字化，各种部件的成本将下降，功耗也会减少。又由于设备生产厂商之间的竞争，会促进ISDN设备价格的下降。还由于存在一整套限定接口的标准，设备的生产成本也会不断地降低。

然而，用ISDN代替POTS给一个家庭提供话音线路，需要的改变非常小。从概念上说，ISDN的想法非常好，就是使本地回路数字化。没有人从一开始就计算出各种开销的实际价格。不论是对业务用户还是对运营商，转变到ISDN都是非常昂贵的。但是，ISDN正在不断地被实际应用。

ISDN所提供的BRI：ISDN有两种版本或两种特色：基本速率接口（BRI，Basic Rate Interface）和主速率接口（PRI，Primary Rate Interface）。BRI对住宅用户或小型/家庭办公室（SOHO，Small Office/Home Office）客户更适合，而PRI对商业客户更适合。一条模拟的POTS线对可以被转换成一对数字BRI线，但PRI业务需要两对数字线。每种ISDN都定义了许多被称为B信道的承载信道。B信道是信息的传送信道，像话音、视频等都在这个信道上传输。BRI和PRI 还使用D信道，用于传送信令信息。

信令将在第9章详细介绍。信令反映了线路的状态，如电话是否挂断，被叫是否正忙等。信令还是一种方法，通过信令可以将电话号码传送给交换机，以使交换机了解正在呼叫哪一部电话或哪一个终端设备。在T1上，为了传输信令就必须丢弃一些信令所占用的话音比特。能这样做是因为人耳不能分辨出是否有一个用于话音传输的比特被丢失。这些信令被称为**带内信令**，带内信令在语音信道上工作良好，但是在数据信道上则不然。在数据信道中，如果我们丢失了一比特，将会被视为错误帧并需要重传。然而在ISDN中，所有的信令都在D信道上传送，这些信令被称为**带外信令**（信令在话音比特段之外编码），或被称为**净信道信令**（在话音比特段内没有信令比特，所以话音比特是干净的）。

在5.3.4节里，我们将讨论SW56业务。我们将会了解到，许多时候只有56kbps的信息需要通过64kbps的信道传输，这是因为用于传送话音的设备将某些比特看作是信令比特而不是信息比特。对于数据，我们不能冒险丢失任何比特，所以信令比特（伴随其他一些比特）根本不用，这样就只能达到56kbps的速率，所以是SW56。如果承载网络使用的是带外信令，那么就可以用SW64取而代之，这时在整个64kbps信道上，所有的比特都可以被用来传送信息。

在任何情况下，ISDN的BRI都提供两条64kbps的B信道，用于传送话音、数据等信息，同时还为信令提供一条16kbps的D信道，产生的总速率是144kbps。实际上，加上用于帧同步和其他目的的比特开销，总的速率还要高（160kbps）。但是BRI可以在一对双绞线上使用。换句话说，POTS线路换成BRI线路非常简单：只要更换终端设备即可。

ISDN所提供的PRI：在北美和日本，ISDN的PRI提供23条64kbps的B信道和一条64kbps的D信道。PRI也可以被配置成24条B接入信道，没有D信道。包括各种开销，加起来PRI的总速率为1.544Mbps，与T1的速率相同。在世界的其他地方，PRI能被配置成30B+D（64kbps）或31B，总速率达2.048Mbps，与E1的速率相同。既然PRI的速率与T1的速率相匹配，那么ISDN能够做哪些T1做不到的事情吗？初步看来，那个问题的答案是D信道。

在图5-9中，一个单位在各地的办事机构遍及全国。在两个地点之间需要大量的带宽，所以一条T1线路专门为其提供服务。然而，在其他的地点之间带宽的需要量是变化的，与每天的具体时间有关。因此，可以使用一个拥有全部的23条B信道的ISDN连接。随着新连接需求的出现，或者是带宽的需要量增加，D信道可以对网络做相应的调整。有了ISDN，工作人员就可以利用ISDN接入与其他的任何地方相连接，而不管对方是否属于本公司。从这一点上看，ISDN

更像POTS服务，但它在提供高质量和可靠的连接方面更加灵活，并且本质上是数字信号。图5-9显示，在提供给一个地方的23条B信道中，目前仅有13条B信道正在使用，其中一些被用于电视会议、语音呼叫、传送数据，或其他类型的业务，以后只要需要，就可以用D信道建立另外的10条信道。这样，T1提供的是一条点到点的专用链路，而ISDN提供的则是可以改变的连接。D信道为B信道提供信令，也允许它们组合在一起提供多速率信道，这种信道是DS0的好几倍。

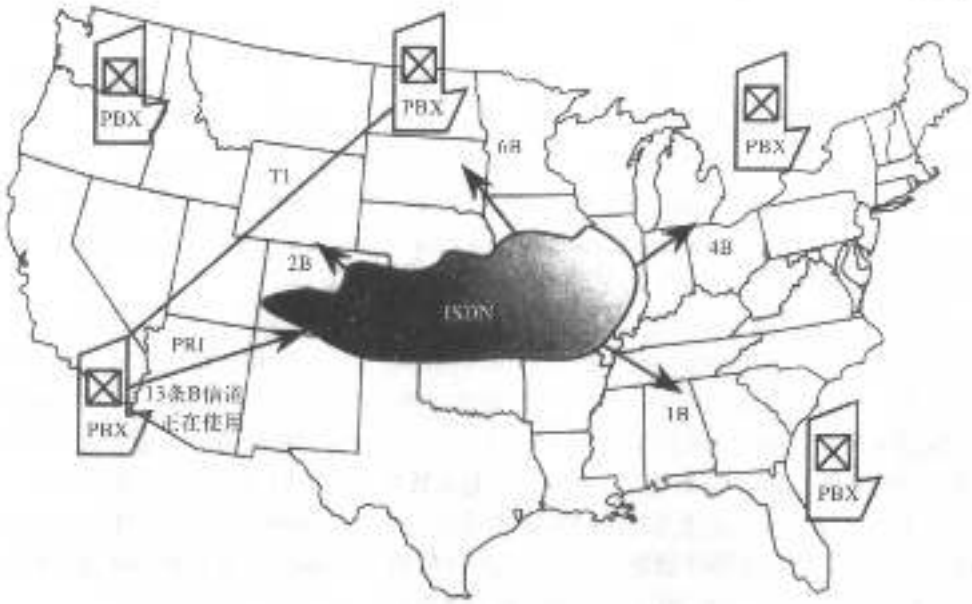


图5-9　T1网络只对一个地区提供专用的接入方式，而ISDN可以根据D通道的信号动态配置网络的接入方式

然而对于T1，每个信道的信令能在每个DS0信道内部发送，那么对于连到POP上的T1，可以在单独的信道上进行交换，与图5-9所示的ISDN一样。另一方面，使用所谓的**公共信道信令**，一条DS0信道可集中为其他23条信道发送信令信息，这时T1与ISDN具有相同的灵活性，但成本较低。

5.3.4　带宽按需分配的数字拨号业务

SW56：传输声音能被数字化，数据（和视频，或者其他类型的信息）也同样能被数字化并在语音网络上传输。只要一个语音信号出现在运营商的网络上，它都是在64kbps的信道上传输。现在，用户可以采取任何自己所喜欢的方式使用语音信道，传送64kbps的数据与传送64kbps的语音一样容易。

此外为了提高传输效率，制造商正在出售用户端设备（CPE，Customer Premises Equipment），这种设备可以将几路话音、数据和传真组合成一路，并把它们压缩到一个64kbps的话音通话中。这样用一次通话的费用，就可以免费获得另外三条话音线路和一条9600bps线路。当然这需要使用声音压缩技术，使一个话音信道的带宽低于16kbps。设备若使用了专有协议，则在网络的端点就只能使用一个厂商的产品。但是，面对用一次通话的费用，就可以使如此多的线路被压缩、转换从而节省大量的联网费用，真希望提供给你专用设备的

生产厂商不会破产。这就是为什么使用标准设备更好的原因。在标准的网络中，不是基于标准的解决方案不会存在。

1985年，AT&T推出了可交换的56kbps数据业务，并将它命名为“Accunet 可交换56 kbps”业务。这项业务允许用户拨打一条56kbps的信道，建立到任何点的连接。当时这项业务基本上是用作专用链路的备份。

今天，所有运营商都提供了这项业务，并称其为SW56（可交换56）业务。另一方面，由于SW56不是一项国际标准，因此这项业务渐渐地变得不像过去那样受欢迎。

数字拨号业务：SW56再向前发展，紧接着出现的业务被称为带宽按需分配的数字拨号业务。除了带宽按需分配意味着带宽量可以实时按照客户需求的变化调节之外，这项业务非常类似于可交换的数字业务。就如同一个人可以通过普通电话呼叫任何其他人来进行通话一样，数字拨号业务可以为数字传输提供同样的功能；与话音呼叫在两个端点之间提供一条固定的4kHz话音信道不同，带宽按需分配使用户不仅可以建立连接，同时还可以指定带宽。因此客户需要根据通话距离远近、通话时间长短以及通话带宽大小来付费。

用户不需要再对T1或FT1（部分T1）的数字直通线路进行调整。对于T1线路，在晚上或其他时间空闲或不能被充分利用时，用户仍要为这条链路付钱。然而对于带宽按需分配数字拨号，用户只需在有数据要发送时创建一个链路，数据传输完毕时就断开这条链路。

举一个例子，如果信用卡公司通过一个大型的数字直通线路网络在全国范围内提供信用卡的鉴权。一个非常关键的问题是这个网络在任何时候都不能被阻塞。因此，这个网络在大多数时间里，比如感恩节后的第一个星期一，都必须被很好地优化。为了应付一年中最忙的几天，这个网络必须具有足够的容量。但是在这一年中剩下的日子里，网络的利用率就非常低。

如果用带宽按需分配业务取代原来的网络，信用卡公司就只需为他们所需要的带宽付费。这样，即使在最忙的日子也不会出现令人担忧的业务阻塞；而在其他的时间，费用会明显减少。总之，带宽按需分配业务提供了最大的灵活性，而费用代价最少。

这项业务另外一种流行的应用是在几个地方同时召开的视频会议。用T1网络，人们必须按计划在一个特定的时间内召开视频会议。如果一个地方的主管经理因为其他突发的事情决定推迟会议，那么为电视会议安排的带宽将无法再被利用。对于按需业务，可在最后一分钟拨通电视会议，不需要事先规划。另外，还可以在开会时根据图像质量的要求选择带宽。

当然，这里有一个转折点，在这个点开始转而使用直通线路网络会更经济有效。例如，如果业务量不断升高，比如说达到了每天5个小时，那么使用T1或FT1将是更好的选择。所以必须知道目前现有的业务量，才能就使用直通线路还是使用交换业务这个问题做出合适的决断。然而，如果将在国际边界上的直通线路转换成交换数字业务，那么这样所节省的费用要比从国内业务所节省的费用更可观。

实现数字拨号业务：刚开始，SW56业务通过一条SW56接入链路提供，那时这两种术语交替使用。现在，接入SW56网络业务可以通过一条SW56链路、BRI、T1或PRI实现。LEC或IXC可以提供这些服务。如果CPE使用T1接入LEC，那么通过这个承载网络可以建立24条SW56线路。在这种情况下，客户需要支付从CPE到CO间固定的T1费用。现在，客户可以灵活地呼叫24条单独的线路，因为他具有使那么多的线路连到这个承载网络中的必须的通路。

如果用PRI 接入网络，用户就有最高的灵活性。因为他可接入SW56、SW64、SW384、SW1536或多速率业务。相反，SW56接入不能接入SW64或更高速率的业务。

多速率业务的速率是64kbps的ISDN信道的倍数，如64kbps、128kbps、192kbps等等。用户定制的业务类型通过ISDN的D信道传送。SW384和SW1536分别被称为H0和H11 ISDN线路。一条H信道的带宽必须在网络中作为一个整体存在，也许仅能在CPE中被分开。目前，SW56业务是使用范围最广的业务。利用它，人们可在任何接入类型间进行通信，不论它是SW56、SW64，还是BRI、PRI。

对于使用ISDN H0、H11的运营商，当接收到一个带宽请求时，网络负责管理带宽的分配，用户仅需确定需要多少带宽，这被称为基于网络的带宽按需分配业务。另一方面，用户的I-Mux（反向多路复用器）也使他可以自动地拨通一个应用（如电视会议、文件传输等等）所需要的那么多条线路，在这里是用户的设备在管理带宽的分配，而不是运营商的网络。

一个I-Mux在几条单独的线路上分割用户的数据，然后再把这些数据送到目的I-Mux。在目的地，由于路由路径的不同，数据单元到达的顺序可能不同。所以远程的I-Mux将调整延时，以正确的顺序排列这些到达的单元，并将这些数据提交给接收应用程序，就好像数据是从一条信道上发送过来的一样。

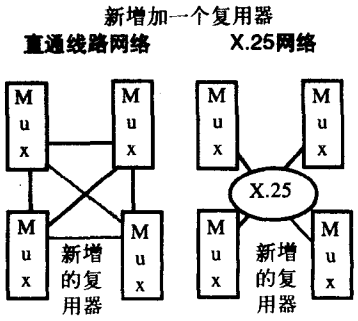
5.3.5 X.25

在2.6节中讨论了分组交换网络，本节将就分组交换的运营问题与数据报交换网络的运营问题进行比较。我们曾经提到X.25是用于分组交换网络的协议，IP是数据报交付网络的协议。这里还将详细地讨论如何在X.25网络上创建虚电路，以及数据被传送后如何断开虚电路。我们这里所说的VC（Virtual Circuit，虚电路）是信道号和路径上链路的集合，通过这个路径可以定义一条虚电路。我们所说的PVC（Permanent Virtual Circuit，永久虚电路）是一条专用的VC，SVC（Switched Virtual Circuit，交换虚电路）是一条根据需要被创建或被拆除的VC。表5-4回顾了PVC和SVC的比较。

表5-4　PVC和SVC的比较

	PVC(永久虚电路)	SVC（交换虚电路）
相似的链路	租用的链路	电话链路
连接类型	固定的，点到点	变化的，任何到任何
是否需要业务规划	是	不
是否需要信令	不	是
是否需要地址	不	是
在网络中是否冗余	是	是
相对的灵活性	较差	较高
相对的复杂性	较低	高
创建方法的类型	用一个管理控制台手工操作	基于呼叫到呼叫，按需分配

X.25是第一个使用了虚电路而不是物理直通线路来创建一个网络的协议之一。从那时起，SS7、帧中继和ATM都在X.25网络基础上做了改进，但是它们都仍然使用虚电路而不是专用电路的概念。边上的图对直通线路网络和X.25网络做了比较。在直通线路网络中，线路必须被提供，它的成本基于距离的远近。直通线路越长，成本越高。流量工程必须不断地根据网络的情况实施，因为要考虑许多方面的因素，例如应该订购较多还是较少的电缆，应该规划的容量是多还是



少，等等。

对于X.25和其他“虚拟型”网络，线路的成本只是从一条接入链路到网络“云”的成本。到网络的连接对距离不敏感。由于许多用户共享X.25网络，因此服务提供者可以超量占用线路。这是可行的，因为每个用户不是每时每刻都在使用X.25网络上的设备。分组的头部决定这些分组被传送的目的地。这些都是X.25网络比自己拥有专门的直通线路网络便宜的原因。

前面的边图是一个直通线路网络，已经有三个用户站点，现在要加入第4个。为了使每个站点都能与其他的站点直接连接，在多路复用器中必须存在多个硬件连接。如果创建的不是全网状的网络，那么两个站点之间的流量必须通过第3个站点转发，第3个站点是卸载流量的中间站点。当需要加入一个新站点时，必须在每个站点安装新设备以支持与新站点的连接。尽管现在有了热交换设备，不需要再切断设备的电源，但是从前面的边图中可以看到，对于直通线路网络需要提供较多连线。而对于X.25网络，加一个新站点非常简单。不必增加新的端口；老站点只需要更新转发表，而不做任何物理上的变动。将一个站点从一个地方移到另一个地方与从X.25网络中去掉一个站点一样简单，即使用户有一个大得多的网络也是如此。但是对于直通线路网络而言，随着网络规模的增大，移动站点和增减站点的复杂性会大大增加。

今天，在美国，尤其是发展中国家X.25的应用非常重要。X.25的数据率通常大于64kbps，帧中继的速率从64kbps开始一直到45Mbps，而ATM的速率从1.5Mbps开始增加。X.25在每一条虚电路的数据链控制层和网络层上都进行检错和纠错。

5.3.6 帧中继

与T1相比帧中继的优点：用于实现LAN相连的网络必须能够处理突发业务。这是因为通常LAN业务的发送时间无规则，且传输速率可达4Mbps到100Mbps。这些业务不适合于传统的T1技术，因为T1最初是为传输话音设计，而话音不是突发性的。此外，改变T1网络的配置太困难了，无法适应某个应用需要突然需要增加带宽的要求。

例如在图5-10a中，有3个站点被T1网络互连起来。前端处理器为IBM大型机提供通信，同时还提供了与低速率PSN（Packet Switched Network，分组交换网络）之间的连接。

如果一个路由器需要能与网络上的其他3个路由器进行通信，那么每个路由器与各自的复用器之间还需要有3个连接。如果对于复用器来说，路由器不在本地，那么这些连接的成本将增加。无论如何，在复用器上需要有三个端口专门用于路由器。

分配给一个复用器各个端口的带宽需要事先被设定。如果一个路由器有突发业务需要通过网络，而前端处理器和PDN的信道又恰好是闲置的，路由器也不能使用这些信道，因为每个端口的带宽是事先分配好的。

在图5-10b中，将一个专用的T1网络转换成了一个专用帧中继网络。在这里，带宽可以根据系统的需求瞬时地被再分配（或者动态分配）。还有，设备间的相互通信仅需要一个端口。这是因为统计多路复用器可以使用帧中继网络上的信道号来实现。

在图5-10c中，再来看一下公共帧中继网络。假设我们已经安装了帧中继拆装设备（FRAD，Frame Relay Assembler / Disassembler），FRAD类似于X.25网络中的PAD，可以使不是帧中继的设备能兼容地用在帧中继网络。现在不必租用T1的设备，因此降低了运营成本。

这里，一个附加的好处是不必为租用的T1专用链路付费。与在虚拟网络中一样，我们只需在使用业务时付费。由于帧中继网络由许多用户共享，因此运营商可以制定诱人的价格。

再有，在T1网络中安装一个新的站点需要重新配置网络，而对于帧中继网络只需加入一条新的接入链路。最后，帧中继网络的价格与距离基本无关。

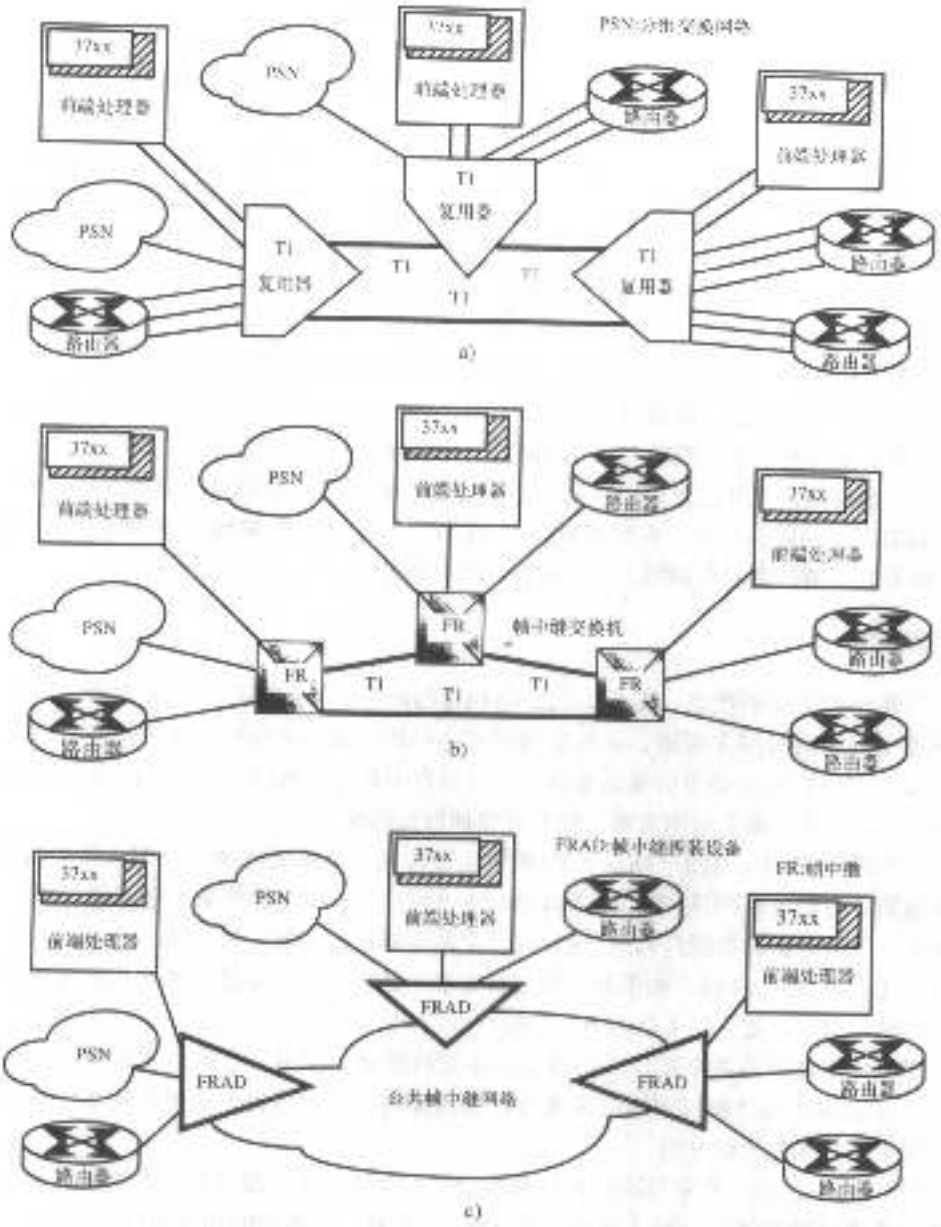


图5-10　a) 基于T1的网络，b) 转换成一个专用帧中继网络，c) 转换成一个公共帧中继网络

与X.25相比的优点：帧中继技术最初是由ITU-T的ISDN和X.25标准发展而来。尽管这些标准是为使用SVC网络的64kbps电路设计的，但4个设备制造商（Cisco，DEC，NT，StrataCom）还是提高了拨叫DS-1的速率，并把协议简化成仅仅处理PVC，这个协议被称为本地管理接口（LMI，Local Management Interface）。现在帧中继既是ANSI的标准，也是ITU-T的标准。

在X.25被引入的那个时期，许多模拟链路的误码率为10^{-2}（1/100），也就是每发送100比特错1个。那时沿传输路径上每一对节点的第二层和第三层完成相应的检错。最好在发现错误时立即进行检错和纠错，而不是将这些错误向前传到下一个节点。

今天，我们的网络更多地使用了光纤，误码率可达10^{-15}，所以差错检测次数明显地过多了。每星期可能只出现一个误码，为什么要每秒都检查误码呢！没有必要让网络承受这样的负担，要求它们检查不存在的误码并纠正这些误码，这样只会使网络的效率降低。

帧中继被视为X.25的简化版，因为没有X.25的那么多开销。它的网络层被取消，差错控制不是在传输协议中完成，而是留给了末端节点。注意帧中继与IP非常相似。在因特网中，IP不做任何误差校正工作，而是把纠错的工作留给了网络末端节点的上一层。帧中继也将差错控制工作交给网络末端节点来做。实际上，帧中继进行差错校验。那么如果一帧的目的地址出现错误会怎样呢？这一帧会被送到错误的目的地点，从而浪费了网络的带宽。由于这个原因，帧中继只进行差错校验，一旦发现了误码，也不会请求重发，出错的帧只是被简单地中止或丢弃。这是基于这样的一个假设：如果接收端的用户（或应用）发现确实丢失了一帧，它会向发送端的应用请求重发这一帧。

在帧中继中不采用差错控制使它具有如下优点——可以高效且快速地传输。帧中继交换机比分组交换机快10倍，节约的时间与一条路径上的交换机数有关。此外，分组交换机使用存储和转发方法，通常采用较小的帧窗口尺寸进行配置。达到窗口限制时，下一个分组不能再被发送，必须等到当前的分组都被确认之后，才能重新开始发送。帧中继中不存在此类瓶颈，尽管在以后的章节中可以看到，它可能会引起拥塞控制的问题。

作为总结，下面列出公共帧中继网络的优点。由于只是使用了第二层，而不是所有三个层，因此帧中继的头甚至比X.25第二层的头还要小，因而帧中继的开销非常低。故此帧中继是一个快速协议，即使是在LAN之间传送突发业务也如此。由于在一个公共网络中有许多可用的冗余路径，因此公共帧中继网络是一个可靠的方案，且规模恰当，这意味着可以容易地添加或删除多个接入点。同时它还是一个已经制定完善的标准，这样设备的价格就较低且容易获得。当用作PVC时，它被认为是租用链路的另一种替代方案。然而，当帧中继的SVC也能被运营商使用时，帧中继方案的灵活性将大大增加。

5.3.7 ATM

为什么没有别的协议？现在让我们把注意力转向ATM（Asynchronous Transfer Mode，异步传输模式）。最初，希望ATM能综合所有类型的网络，无论它是LAN还是WAN，无论它是传输话音、数据还是多媒体。ATM被假设可以将每一种网络的各种不同协议和技术综合成一体。在WAN中ATM确实这样做了。但是对于高速LAN，ATM没找到解决办法。为了了解ATM的美妙之处，首先将它与现有技术做一比较。

在图5-11中，假设有一个话音源和一个数据源，正在竞争传输链接上的一个固定的带宽。记住数据业务通常都是突发的且比话音业务量大，但是被传送到目的地之前可以等待一小会儿。这与被分组的话音业务恰恰相反。通常话音的业务量较小，但在被传送到听话方时不能等待。

在t=0，或时间帧0处，我们有需要发送的话音业务，业务量被标为V1；但是在同一时刻，有一个突发的数据流到达，其数量是V1的3倍，这些数据单元用D1~D3标记。

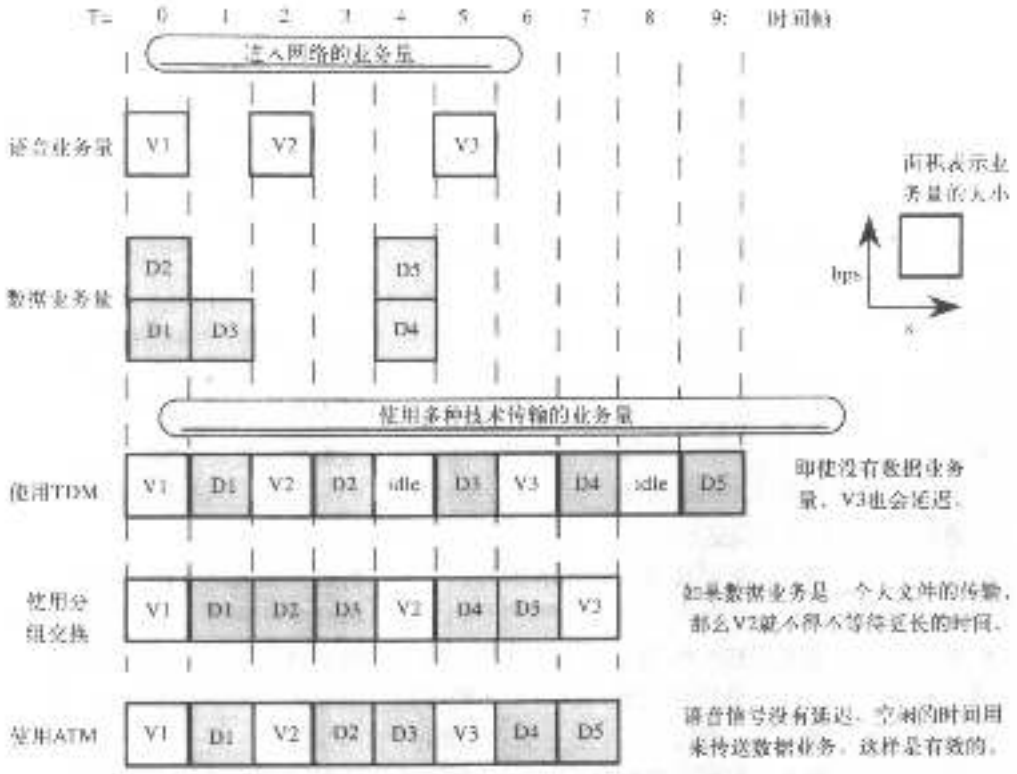


图5-11　3种技术的比较

这些单元的高度代表了传输速率，也就是每秒多少比特；宽度表示时间。因此，速率乘以时间（或高度乘以长度）就代表在通信信道上需要传送的数据量（比特）。在这个例子中，话音在t=0,2,5时被发送，而数据在t=0,1,4时被发送。在t=4时发送的数据量是在t=0,2,5时发送的话音量的两倍。

如果使用TDM（Time Division Multiplexing，时分多路复用）技术来传输混合业务，就像T1多路复用器所做的那样，那么每个信源只能占用被传输帧中分配给它的时隙。在这个例子中，偶时隙被分配给了话音信道，而奇时隙被分配给了数据信道。

如果我们仍然沿用这个例子，让t=4时没有话音业务，但有数据业务，但我们不能把数据业务放在这个时隙中，由于这个时隙属于话音信道，因此这个时隙被浪费了。接收方同步解调属于话音信道的所有偶时隙和属于数据信道的奇时隙，所以不允许将时隙用错信道。

现在，需要在t=5时发送话音，但我们无法发送它，因为这条信道属于数据。这样话音业务就不得不被延迟到t=6时刻。对于这个时间帧的其他部分，还可以看到尽管在t=8时有带宽可用，但是数据不得不被延迟到t=9时刻。

在这里，浪费了两个时间帧。如果话音信道空闲，那么它的所有5个时间帧都将被浪费。这样不仅带宽的利用率低，而且数据还不得不延迟传送（尽管数据的延迟要求不像同步业务延时要求那样苛刻）。

让我们看一下TDM上分组交换的优点。这里不再交替发送两种信源，而是每次发送一个单元而不再将它们分成许多时间帧。V1首先被发送，然后是D1到D3做为一个单元。因为这个

数据包，V2直到 t=4时才能被发送。由于同样的原因，V3被延时两个时间帧。

分组交换技术，如X.25和帧中继有效地利用了带宽。在这个例子中，所有的数据都比TDM早发送3个时间帧。但是，话音信道被延时了4个时间帧（V2延迟两个时间帧，V3延迟两个时间帧）。而用TDM传输，话音仅被延时1个时间帧。如果在t=0时发送的数据是一个较长的文件传输，那么V2必须等待一段相当长的时间。然而，语音不能像数据那样承受延时。因此，TDM有利于话音传输，而分组交换有利于数据传输。

对于ATM，所有的业务都被分成固定的53个八位组的信元；5个八位组用于信元头，48个八位组用于信息。在t=2处，尽管数据已经等待了较长的时间，但是话音信元首先被发送。分组交换与ATM有相同的优于TDM的优点，它们都充分利用了带宽。它们都可以在t=8前完成传输，而没有浪费时间帧。然而，ATM优于分组交换的优点是时间延时为0（分组交换的延时是4）。实际上，这里已经证明ATM优于TDM，因为TDM的话音延时是1个时间帧。注意尽管ATM以恒定的速率传送数据，但它也适用于以变化速率传输的那些应用。

对于TDM，由时间帧所处的位置我们可以知道信息的目的地。而对于ATM，我们需要用信元头和标签指出信元的目的地。因此，ATM被称为使用了**标签多路复用**格式。

表5-5总结了话音和数据传输的不同特点。所有的电话都产生相同的业务。但是对于打印机、LAN服务器、Web服务器、主机和PC等并非如此。数据产生各种形式和大小不同的业务。过去，正是这些业务的差异，使网络必须分别设计，或者为语音设计，或者为数据设计，但现在ATM将它们统一在一个无缝的网络中。

表5-5 话音和数据网络的差异

	话 音	数 据
原始信号	模拟信号	数字信号
信息到达的速率	恒定	变化、突发
信息块的大小	小	从小到大
对延时是否敏感	敏感	在合理范围内不敏感
对误比特是否敏感	不敏感	敏感

对于ATM，哪部分是不同步的？在图5-5中，D1和D2间的延时是一个时间帧，但D2和D3之间没有延时。送入ATM网络的信息速率与网络输出的信息速率可以不同，因此被说成是不同步的。人们无法确定地知道下一个数据单元的到来时刻。同样，在不同步传输中使用起始和结束比特，接收方不知道下一个字符的到达时刻，或者说不知道下一个起始比特何时到来。

与之相比较而言，TDM应该被看作是STM（Synchronous Transfer Mode，同步传输模式）。两个传输数据之间的间隔是已知的，并且是固定的。

尽管在术语上有点混乱，但我们所说的STM通常是使用异步多路复用技术传输，而ATM通常是使用同步多路复用技术传输（或SONET）。由于输入信号来自不同的信源，所以STM需要比特填充。每个输入信道可能与公共时钟不同步，但是SONET要求所有的输入必须与一个公共时钟同步。

其他的好处：ATM获得的最大的优点好像是：一个网络可以为所有的应用提供服务。正如我们所看到的，同步业务可以被快速地传输，大文件传输也可以在不浪费带宽的情况下被传送。但是除此之外ATM还有其他好处，它可以以任何速率有效传输信号，且不会强制应用服从网络的限制。

例如，为了在T1的设备上实现50kbps的传输信道，通常的做法是使用整个DS0信道，从而浪费了14kbps。同样，如果要以10Mbps的速率发送，则需要使用反向多路复用器和7个T1，这样就会有0.7Mbps的带宽剩余。此外，这些网络还必须事先提供。

另一方面，ATM能提供连接所需的带宽量，不会强制应用接受固定增长的带宽，不像以前的技术那样强制应用服从网络，而是反过来顺应网络应用的需求。

自由地选择带宽数只是ATM的优点之一。只要需要，ATM还能在不同的端点之间交换业务。这样做不需要事先提供，如事先设置DACS交换机。此外，用户仅需要为所使用的内容付费。

ATM同样提供基于硬件的交换。大小固定的信元使交换可以由简单的硬件电路来完成，而不必通过软件。交换速度可达每秒千兆比特，非常快。当光交换可用时，这种硬件交换能力可以平滑地过渡到光交换机上。利用这种几乎是瞬间就完成的交换能力，ATM打破了LAN和WAN的界线，并使它们几乎是一样的。

总之，无论是在其传输速率上还是在其业务性质上，ATM都能随应用变化。长度固定的信元使ATM能实现快速处理和交换。同时，ATM是一个面向连接的协议，可以提供PVC连接和SVC连接。

5.4　虚拟服务

5.4.1　800服务

1967年，AT&T引入了800服务，这项服务允许呼叫者能够免费拨打800号。800号的拥有者根据呼叫量为来话呼叫支付费用。目前，800免费服务是一项高利润的业务，通常与话音虚拟网紧密相关。在写作本书的时候，888和877也属于这种服务。

在1993年之前，一个中心局收到一个800呼叫进行连接时，都是通过先扫描800号后面的3个数字，再把这个呼叫转发到正确的IXC的POP上。这3个数字被称为NXX数字。与其他的运营商相比，AT&T被分配了更多的NXX数字。

如果一个客户要更换运营商，首先必须改变他的800号号码，因为800号的NXX属于原来的运营商。由于运营商的改变导致800号号码的改变，在商业上是需要避免的；因为对这个新号码做广告并让大众都知道这个改变是一项既费时又费力的工作。借助使用SS7（7号信令系统）网络，客户可以只改变运营商而不改变已有的800号号码。这被称为800号的可携带性。

有了800号，商店可以关上店门，通过电话进行销售。许多人正在使用这个号码进行购物。通过800号，公司有能力提供出色的服务。如果这些公司有了800号，用户更愿意通过打电话来购买东西。

800号也同样有不足的地方。如果800服务取消了，用户很难发现，尤其是在800号上的活动很少的情况下更是如此。还有，如果某个用户拨错了800号号码，公司也必须为这个呼叫付费。如果一个公司错误地广告了其他公司的800号号码将会怎样？这时拥有这个号码的公司必须为拨入的电话付费，更糟糕的是可能会由于线路忙个不停，而使公司失去了商机。

5.4.2　虚拟专用网（VPN）

在5.1.4节中我们曾提到，VPN（Virtual Private Network，虚拟专用网）是如何使一个商业客户利用公共网创建自己的专用网络的。这样做客户不必管理他的网络，且费用可以比专门租用链路网络低得多。

AT&T的VPN被称为SDN（Software Defined Network，软件决定的网络）。MCI的VPN被称为Vnet，Sprint的VPN通常被简称为VPN。这些网络将在后面有关虚拟网的章节中讨论。

目前因特网VPN已经启用，这些内容是第27章的主题。VPN的主要问题是安全性。一旦安全问题得到解决，因特网的VPN将会被普遍使用。今天所说的VPN，通常被认为是因特网VPN。

习题

5.1节

1. 当在两个CO或POP之间的一个物理连接被保留给某个特定用户，它可能是哪种连接？
   a. 专用的　　b. 可交换的
   c. 虚拟的　　d. 逻辑的
2. 配线架上的物理跳线可以将一个针与另一个针连接起来，下面哪一项能替代物理跳线？
   a. MDF　　b. POP
   c. CO　　d. DACS
3. 下列哪一个不是专用链路的名称？
   a. 专用链路　　b. 直通线路
   c. 租用链路　　d. 虚拟链路
4. 对下面每一项，指出它描述的是交换接入还是专用接入。
   a. 可以与任意数量的节点相连接。
   b. 不根据用量多少付费。
   c. X.25的SVC或帧中继的SVC。
   d. 必须使用信令的方式拨号。
5. 在专用网络中，商业地点之间的互连使用哪一种链路？对于PSTN，又使用哪一种链路？
6. 专用链路通过PSTN连接吗？通过CO连接吗？
7. 给出虚拟网的一般定义。
8. 列出两种虚拟专用网，并给出优于对方的优点。

5.2 节

9. 下列哪一种中继线将一个PBX连接到远程CO？
   a. CO　　b. DID
   c. 联络链路　　d. FX
10. 下面哪一种连接允许外部号码通过PBX直接拨号，而不必通过接线员？
    a. OPX链路　　b. DID中继线
    c. FX中继线　　d. 联络中继线
11. 哪一种连接允许将经理家的电话直接连接成为公司PBX的一个分机？
12. 在POTS链路上使用联络中继线的优点和缺点是什么？

5.3.1节和5.3.2节

13. 为了建设一个T1，需要多少对双绞线？
14. 一条T1联络链路的速率是多少？它通常能复用多少路话音信道？
15. 国外的T1技术有何不同？
16. 描述ADM和一对紧接的多路复用器的工作原理。
17. 列出SONET优于T1的原因。

5.3.3 节

18. 下面哪一种连接器用于ISDN？

a. RJ-45　　b. RJ-31

c. RJ-11　　d. DB-25

19. 用于BRI，下面每一种速率有多少条信道？

a. 2~64 kbps和1~16 kbps　　b. 1~64kbps和23~16kbps

c. 1~64kbps和1~16kbps　　d. 24~64kbps

20. 给出信令事件的例子。

21. 当话音比特被信令占用时，使用的是哪一种信令？ISDN也使用这种信令吗？

22. PRI和BRI的D信道有何不同？

23. D信道如何使PRI不同于T1？

5.3.4 节

24. 在全数字的PSTN中，在一路话音信道上能传送的最大比特率是多少？

25. 当一个客户发现DS0的比特率太低而DS1的比特率太高时，哪一种服务适合于这个客户？

26. 举出说明基于网络的按需分配带宽的业务。

5.3.5 节

27. 下面的哪一条较好地描述了PVC或SVC？

a. 复杂　　b. 需要信令

c. 可替代租用链路　　d. 手工建立连接

e. 灵活，能与多个节点连接

5.3.6 节

28. 帧中继是从下面哪一个协议演变过来的？

a. T1　　b. ATM

c. X.25　　d. 以太网

29. 帧中继在哪两点之间进行差错校验？

a. 从一跳到另一跳或在每一个链路　　b. 在每个FRAD中

c. 在网络的末端节点上　　d. 帧中继不做任何差错校验

30. 列出帧中继好于T1的优点。

31. 列出帧中继好于X.25的优点。

5.3.7 节

32. 用于ATM中的传输单位是下面哪一个？

a. 帧　　b. 信元

c. 分组　　d. 消息

33. 对于ATM，异步指的是什么？

34. ATM有哪些优点？

5.4 节

35. 运营商通过什么管理在市场中运行的虚拟网络？

a. 话音交换机　　b. CO

c. SS7　　d. ATM

36. 拥有自己的800号码且还能改变运营商的能力被称为什么？

37. 列出市场上AT&T、 MCI Worldcom和Sprint管理的VPN的名称。

第6章 住宅网络服务

本章所要考虑的某些网络服务内容原本是针对商用需求的，但由于使用的技术与住宅用户的连网有关，因此也包括在本章中。

6.1 56K调制解调器

目前PSTN工作的速率为2400波特，这里1个波特等于一个模拟信号的周期。调制解调器（modem）的设计者将若干个比特信息编码后形成1波特信息。例如，若将4个比特编码构成1个波特，则调制解调器传输速率为9600bps。调制解调器的传输速率理论值可达到34kbps左右，不过也曾有其速率只能达到14.4kbps上下的说法。当一个调制解调器首次和另一调制解调器接通时，它们之间首先完成信号握手过程。这一过程的目的是检测可以使用何种协议。通常，高级协议可以和所有低级协议建立通信关系。

在下面的列表中给出了调制解调器使用的不同协议。信号握手过程是确定线路上能进行通信的最低级协议的过程。信号握手关系建立后，就开始训练过程。这个过程是确定调制解调器安全工作（也就是误码最少）的比特率。就好像你的汽车可以达到的最大时速是100mph，这并不意味着你能以此速度安全地到达目的地。同样的道理，在握手之后，如果调制解调器协商同意使用V.34协议，但是在训练过程中它们可能协商以24kbps的速率运行，因为这样才能使误码率最小。所谓调制解调器间的训练，就是要在协议给定的情况下决定调制解调器可达到的最大速率。再打个比方，握手过程决定了使用哪一辆汽车，而训练过程决定了用什么样的速度驾驶这辆车。

国际调制解调器协议标准

协议名称	速　率
V.32	9.6 kbps
V.32bis	14.4 kbps
V.34	28.8/33.6 kbps
V.90	56 kbps

在写作本书的时候，人们大多采用56kbps调制解调器。这种调制解调器被认为是基于话音频带的，它克服了以往调制解调器存在的很多问题。基于话音频带的调制解调器仅工作在3.1kHz的语音带宽中。尽管以前我们曾讲过每一路话音占据的带宽为4kHz，其实更精确的值应该是3.1kHz，即从300~3400 Hz。现在先来看一下基于话音频带的56kbps调制解调器是如何工作的（下面将56kbps 调制解调器简称为56K调制解调器）。

在图6-1中，可以看到一台与ISP（Internet Service Provider，Internet服务提供者）相连的家用计算机。在这个设置中，ISP服务器必须首先将数据转换成模拟信号，使之能在模拟线路上传输。调制解调器完成这项任务。由于数字信号有许多优点，因此今天在PSTN上的所有通信都采用数字信号。CO（Central Office，中心局）中线路板上的编解码器将模拟话音信号转换成PCM（Pulse Code Modulation，脉冲编码调制）信号。因此，被调制成模拟信号的数据被转换成PCM信号，也就是说在PSTN中传输的信号都是数字信号。最后，在接收端要对信号进行相反的转换。

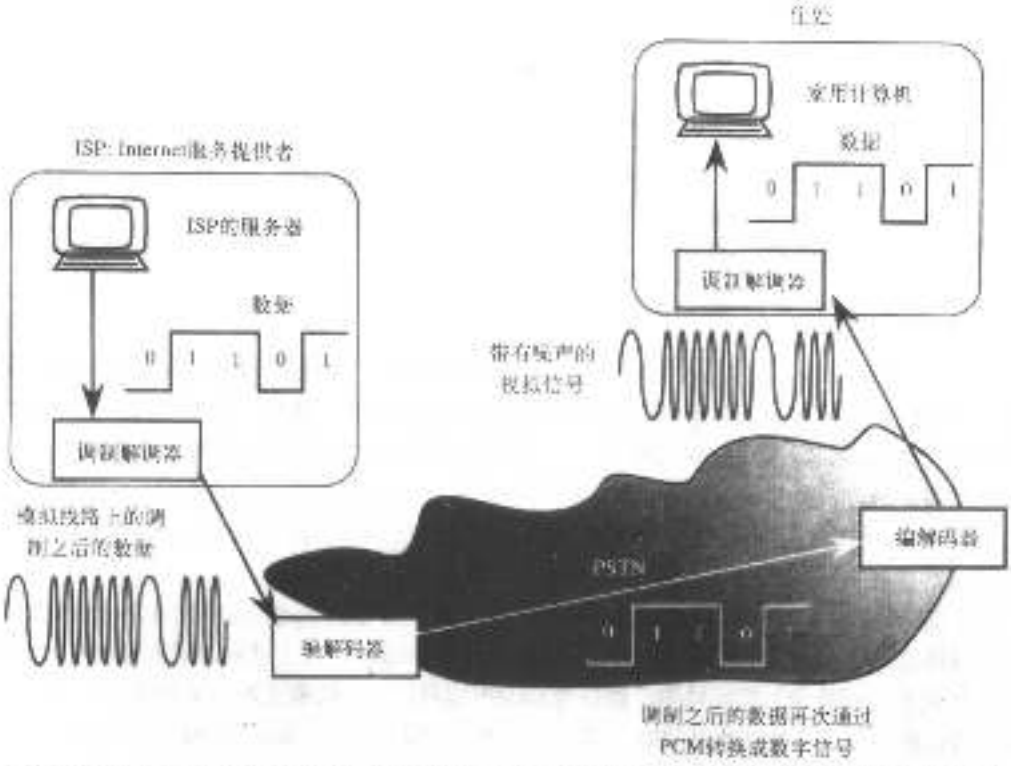


图6-1　在许多电话网络（即PSTN）的节点上，基于语音频带的调制解调器完成信号的模数和数模转换，在这个过程中会引入模拟线路噪声、量化噪声，并会受到语音频带滤波器的限制

但采用这种传输方式时会产生许多不利因素，妨碍调制解调器获得最大速率。首先，在两个传输末端节点的模拟线路上传送模拟信号时会引入噪声，数字信号的传输不会出现这种情况。第二，量化噪声被引入，所谓的量化噪声是由原始信号电平和量化后信号电平之间的差异造成的。最后，编解码器中的带通滤波器电路将信号带宽限定在3.1kHz，而56K调制解调器能利用没有经过滤波器限制的整个4kHz的模拟带宽。

如图6-2所示，使用56K调制解调器时，发送端（这里指的是ISP）必须通过一个数字接口与CO连接，通常使用的是ISDN的PRI接口。数字链路两端还应各有一个DSU（Data Service Unit，数据业务单元）或类似的设备。ISP服务器使用一种特殊的调制解调器，被称为PCM调制解调器。这种调制解调器并不将数据转换成模拟信号，而是将其转换为数字信号，就如同这个信号在ISP中进行模数转换一样，然后在编解码器中进行PCM编码。所有这些转换都是在同一块电路板中完成的，以便抵消模拟链路噪声、量化噪声和编解码器中带通滤波器的限制。从ISP到最后一个CO的编解码器，信号仅仅是被传送而没有丝毫改变。这样，56K调制解调器便能达到设计者所设计的最大工作速率，这个速率只是从ISP的或服务器到用户端的速率。而从用户端到ISP的速率通常只有33.6kHz。当然，如果由于某些原因使线路无法处理这样高的速率，传输速率会自动调整到较低的水平。导致网络中传输比特率降低的原因可能是由于模拟和数字信号的多次转换，或者是需要在某些地方对PCM信号进行压缩。

调制解调器的一个主要优点就是在网络传输环境恶化时能自动降低传输速率。应该注意56K调制解调器是非对称式设备，即在不同的传输方向上的传输速率是不同的。非对称式设备

通常下行工作速率总是比上行工作速率高。这是因为从互联网到用户端传输的信息量要比用户通过鼠标或键盘传送到Web服务器的信息量大得多。

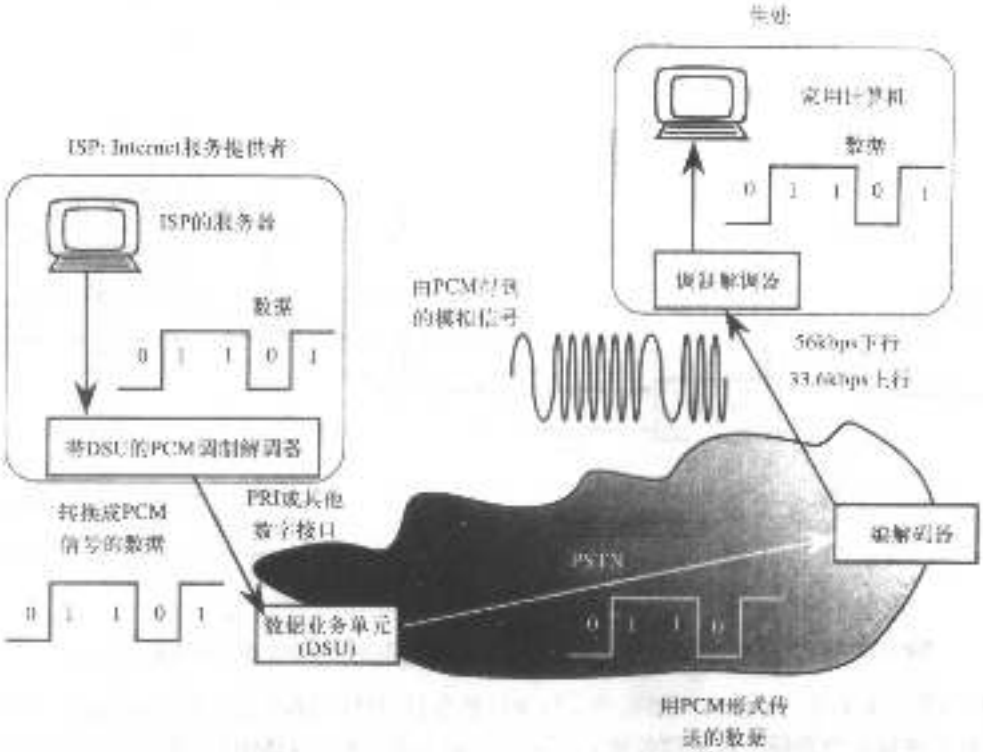


图6-2 56kbps调制解调器依靠发送ISP将数据直接转换成PCM信号，而ISP必须通过ISDN-PRI或其他类型的数字接口与电话网相连。一个类似于DSU的设备为数字线路提供接口。在接收端，也就是从编解码器到家用计算机，信号仅受到网络模拟线路噪声的影响

6.2 有线电视和电缆调制解调器

在美国，使用有线电视（Cable TV，CATV）系统已经有相当长的历史了。这种系统使用宽带同轴电缆，可以为许多家庭提供大量的优质电视节目。CATV通常使用RG-59型同轴电缆，进行射频（RF，Radio Frequencies）传输，传输阻抗为75Ω。实际上，传统的CATV都是传送模拟信号。与POTS线路大约4kHz的带宽相比，同轴电缆具有的350，750或1000 MHz带宽，吸引力相当大。但是这种电缆的带宽为所有用户共享，而一条POTS线路的4kHz带宽是一个用户所专有的。显然，电缆的带宽越大，它的信道容量也就越大。每一个电视信道（频道）占用6MHz带宽，那么带宽为750MHz的电缆可以提供100个电视信道。

更新的CATV系统采用1GHz带宽的电缆，并且支持数字传输标准。但在这里，我们主要讨论当前最流行的模拟系统。

图6-3是一个通用CATV系统，经过重新配置后可提供到因特网的接入。所有的传输都从转发局开始。通常每个城市都有一个由有线电视公司建立的转发局（除非没有一家公司具备占有该城市CATV市场的经济实力）。一般地说，转发局通常经过卫星天线接收广播电视节目，电视节目还可以通过各地方电视台获得，或者通过视频重放装置进行重播。采用FDM

(Frequency Division Multiplexing，频分复用）方式，多个电视信道首先被多路复用，然后通过有线电视设备发送。其中，**分路器**被用来分离不同信号，而放大器则被用来增大有线电视设备的传输范围。同时还可以使用微波或光纤链路将信号传输到与转发局相距较远的下一个站点。子站作为这些传输链路所必需的截止点，同时还完成一个地理区域内的信号分配。

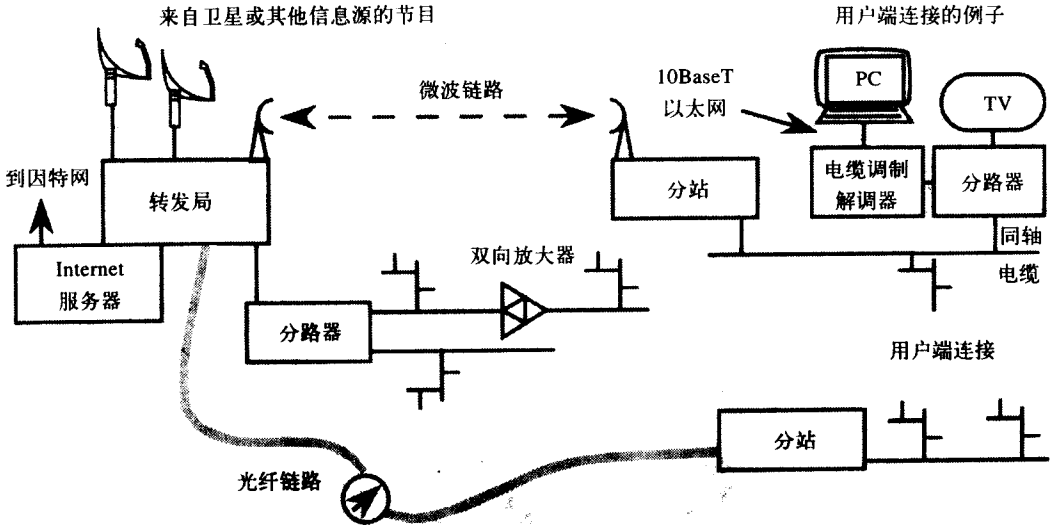


图6-3　CATV网络从转发局开始，通过分路器和放大器将信号分发送至城市的各个角落

CATV基本上是一种单向广播系统。按次计费节目通过PSTN或电话获取来自客户的信息，这被称为**电信反馈路径**。FCC曾经规定：下行传输不得使用5~42MHz频段，这个频段被预留给未来的互动电视上行传输。所以，CATV系统从未使用过这个频段，所用的放大器也都是单向、下行放大器。

目前同轴电缆的基本结构正在逐渐被改变以提供因特网接入，上述频段的低端频谱被用于提供上行链路传输。这样就需要将原来的放大器变成双向放大器，这种放大器被称为**带分放大器**，因为它们用一条通路放大下行频率信号，用另一条通路放大上行频率信号。非常遗憾的是5~42MHz频段信号很容易受到冰箱、车库门开启系统和汽油发动机等的干扰。

有线电视公司通常也提供因特网接入服务，在很多情况下它们是有线电视客户的ISP。有线电视的用户通过电缆调制解调器（cable modem）接入因特网，收看电视节目。由于可以使用滤波器来分离不同的信号，因此用户就可以边看电视边上网。在装上电缆调制解调器后，安装人员可以为用户选择用来接收下行信号的信道。6MHz的下行信道可以为用户提供30~40Mbps的接入速率。由于所有的用户共享这个信道，因此如果许多用户同时接入因特网，有效传输速率是相当低的。信道共享还引出了安全问题。一旦接入信道过于拥塞，有线电视公司会预先配置一条节目信道，作为另外一条因特网接入信道。

一些企业通常为PC选择廉价的以太网卡与电缆调制解调器相连接，这些以太网卡通常被用在局域网中的PC上。在第7章中我们会看到，以太局域网支持的传输速率可达10MHz或更高，且与因特网的连接总是通的，不必进行拨号和等待连接的建立。而且，打开一个浏览器的速度就像打开WordPerfect一样快。

图6-4对电缆设备如何利用有效带宽的方式进行了总结。用于因特网接入的6MHz下行传

输信道被使用相同设备的所有用户所共享。没有其他用户同时在线时，单个用户的接入速率可达30~40Mbps。一旦有其他用户同时在线传输，比特率将会下降。另一方面，每个用户可使用的上行信道的传输速率是100kbps到3Mbps。

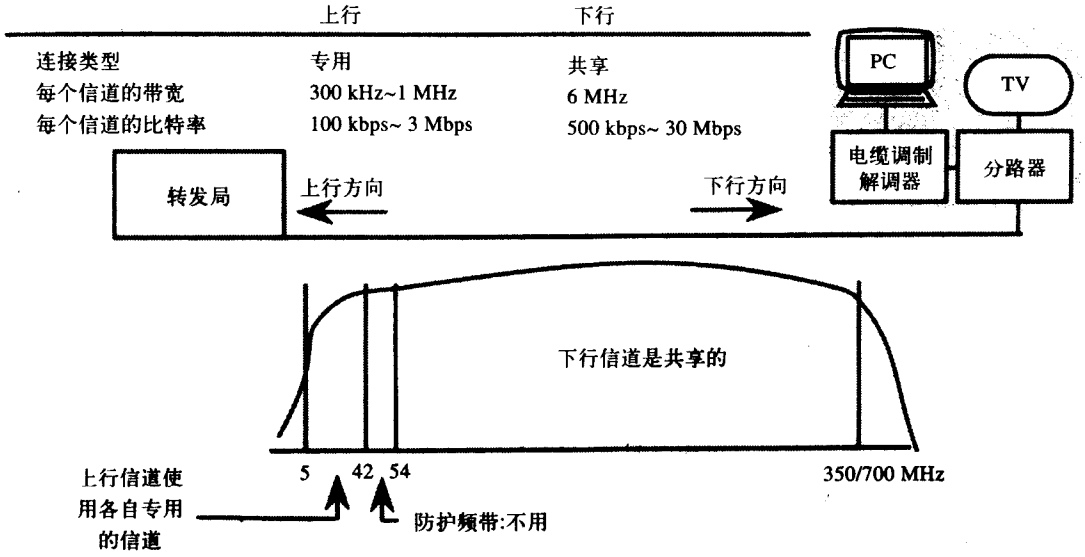


图6-4 电缆调制解调器可用频段的低端进行上行传输，节目信道和因特网接入的上行传输在可用频段的高端进行

6.3 数字用户线（xDSL）

6.3.1 使用xDSL的可能性

提供POTS服务的本地环路线一般都使用UTP电缆，这种非屏蔽双绞线的规格为24~26AWG（美国电缆标准）。尽管提供基本电话服务的本地环路带宽仅为4kHz，但它可以在高于1 MHz的带宽上工作。我们家中的双绞线具有高达1MHz的带宽，但是基本话音业务只需要4kHz的带宽，因此与POTS有关的电子设备都被设计成4kHz。如果换掉这些设备，就可以选择更高的频率并以更高的速率发送数据。然而具体的设计和实现可不像听起来这样简单。

这意味着要获得相应的宽带，必须更换CO线路板和家中的相关设备。如果完成了这项工作，就可以使双绞线的传输速率大幅度提高。例如DSL技术之一的超高速数字用户线（VDSL，Very high Digital Subscriber Line），可以在双绞线上以52Mbps速率传输信息达1000英尺远。随着万维网（WWW，World Wide Web）的应用与日俱增，人们渴望在家中也能获得较高的信息传输速率。在光纤到路边之后，再从光纤接线端经双绞线进入家庭，VDSL就可以实现高速的传输。当xDSL技术普及时，我们在家中进行视频点播也就只是个时间问题了。

再有，倘若半数以上的用户都采用高速线路获取信息，就必须提高因特网骨干网的比特传输速率。然而，本地接入（也被称为“最后一公里”）通常是大多数网络的瓶颈，业内都将其视为需要首先解决的技术难题。同时，LEC（Local Exchange Carrier，本地交换运营商）一直积极致力于寻找有效的解决方案，其他一些公司例如有线电视、无线、卫星领域中的公

司或CLEC(Competitive LEC，LEC的竞争对手)都在积极地寻求解决这个问题的办法。此外，1996年的电信法案也极大地加剧了运营商争夺宽带用户接入市场的竞争。

有许多不同的DSL技术，集合起来被称为xDSL。小写字母x表示一个预留位置的字母，可以用不同的字母代替。而不同版本的DSL技术所要共同面对的首要问题是：电话公司在多年前构建本地环路时，并未考虑要用双绞线传输高于4kHz的信号，即本地环路是为传输话音信号而建的。这就对现在推广xDSL技术造成了巨大障碍。

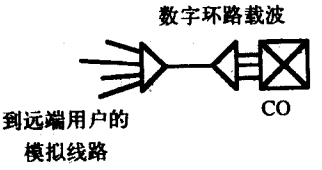
6.3.2 xDSL面临的挑战

在本地环路上进行高速传输的一个基本问题是双绞线的有效传输距离受到限制。与双绞线不同，同轴电缆的传输比特率不会受到距离的限制。使用铜线，工作频率越高，导线中的能量损耗就越大。当然，降低工作频率可以减小损耗，但是传输比特率也会随之降低。所以这里有一个协调权衡的问题。如果需要达到较远的传输距离，就只好牺牲传输比特率；同样，要进行高速传输，就必须缩短传输距离。

如果本地环路的传输距离超过18 000英尺（3.4英里），通常会装有**负载线圈**，这些负载线圈必须被去掉。与电容不同，负载线圈或电感会阻碍高频信号的通过。放置负载线圈的目的是为了补偿传输线路电容的影响。在去掉负载线圈之后，电容的影响会使相邻线路之间的**串话**增加，导致一对双绞线上的信号对相邻另一对双绞线上的信号产生干扰。这是因为许多对双绞线通常一起被架在一根电话线杆上，或者是一起被埋入地下（记住：这些双绞线之间没有任何金属屏蔽网，仅仅是用绝缘层进行了简单隔离）。此外，传输高频信号也会使串话现象更加严重。这就是为什么在测试一条DSL线路时，当一条线路被转换为一种特定类型的DSL时，其他的相邻双绞线不能正常工作的原因。

很多年前，共用线路十分流行。这种线路允许若干个用户共享一条电话线，在需要时轮流使用电话。那时的本地环路线都装有**桥接抽头**（bridge tap），需要电话服务的用户就是通过桥接抽头接通共用线路的。桥接抽头对线路上的低频信号传输没有影响，但现在若使用DSL技术在双绞线上进行高速传输，桥接抽头的影响就不能忽略，此时就不能再使用桥接抽头。

很多时候，一些用户可能会远离CO。这时可以利用T1技术对多个用户进行多路复用，而不必将每个用户的POTS线分别接入到CO。这样只用很少的线路就能将全部用户以数字化形式接入到CO，在CO再通过解复用恢复成多个用户线路。当然，POTS线上的传输是双向的，因此两端都需要多路复用和解复用，这样的系统被称为数字环路载波（DLC，Digital Loop Carrier）系统。DLC系统可以像典型的T1电路一样在两对线上传送24条POTS线路的信息。光纤也可以用在DLC系统中（见右图）。



数字多路复用器只能改变4 kHz的模拟信号。现在，如果希望让含有高频成分的xDSL信号通过服务区，那么高于4 kHz的频率分量不能被传输，从而无法实现高比特率的传输。因此，可以将通常放在CO的xDSL设备安装在这些多路复用器的周围。然后，再使用光纤从相邻的集线箱与CO相连接。据统计大约1/4的POTS用户采用这种数字环路载波系统。

xDSL面临的挑战如下：一条电缆的延长线路上导线的规格不统一，并且两对导线在连接处的类型不同，对高频信号的传输造成困难。此外铜线还容易被腐蚀，埋入地下时更是如此，同时线缆的老化也使传输高频信号变得很困难。下面介绍几种可行的DSL方案。虽然xDSL技

术族中有很多成员，但真正可行的并不多。与56K调制解调器和电缆调制解调器不同，HDSL和IDSL属于对称式传输（即两个方向的传输速率相同）；而ADSL属于非对称式传输。

6.3.3 高速数字用户线（HDSL）

本书第1版提到的HDSL是第一个被实现的DSL技术。其实在此之前，ISDN是最早将POTS线路转变成为数字用户环路的技术。采用HDSL技术可以在双绞线上以1.554Mbps的速率进行双向传输，这个速率与T1相同。由于不需要使用中继器，因此HDSL更简单廉价，因而也更容易维护。与HDSL连接的接口和T1相同。一般来说，大约每隔1英里T1就需安装一个中继器，而HDSL在没有中继器的情况下可以传输12 300英尺（2.3英里）。如果使用距离扩展器，设备生产厂商可以将这个传输距离增大一倍。另外，增大线径也同样可以达到增加传输距离的目的。例如若使用19AWG的双绞线，在没有中继器的情况下传输距离可达22 800英尺。相信在不久的将来可以看到，在没有中继器的情况下HDSL比T1可传输更远的距离。

T1技术诞生于20世纪60年代，而HDSL出现于1990年。因此T1和HDSL采用的编码方式不同。T1技术采用AMI（符号交替反转码，Alternate Mark Inversion），而HDSL采用的编码被称为2B1Q（2 Binary，1 Quarternary，二进制四电平（编码））。有关这部分的详细内容将在有关T1和ISDN技术的章节中介绍。2B1Q采用4个电平而不是两个，这种编码方式不易受串话影响。HDSL较之T1的另一优势在于可实现回波抵消，这已在第3章中介绍过。请看图6-5。

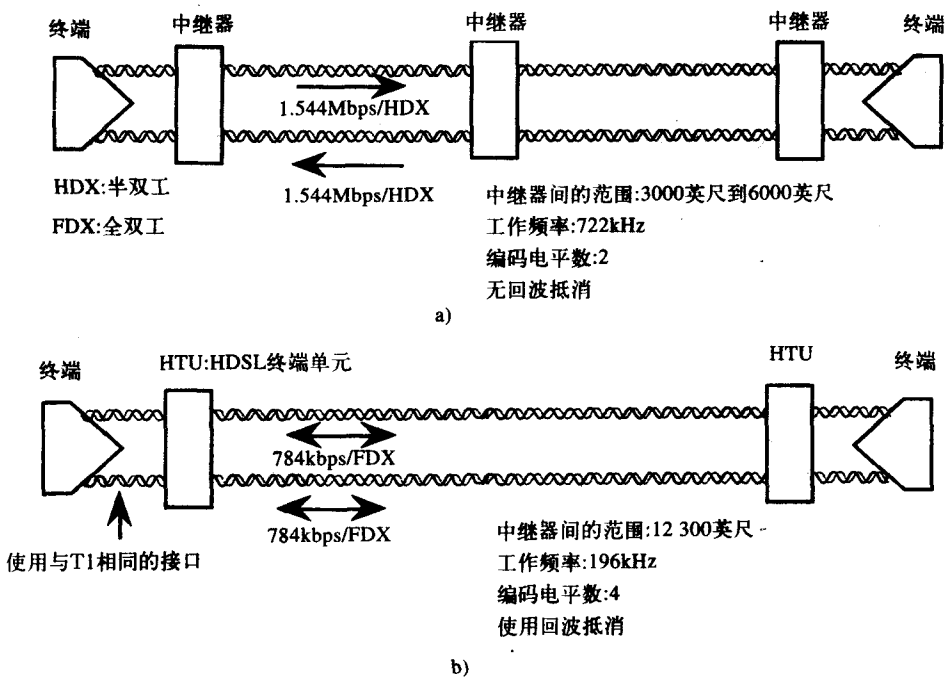


图6-5 a) 在一段T1线路上需要3~4个中继器；b) 在同样的传输距离上，HDSL不需中继器

HDSL比T1传输距离更远的主要原因是HDSL的工作频率（模拟信号）只有T1的1/4。T1工作在772 kHz，而HDSL工作在196kHz。为说明如何从772kHz 和196kHz带宽中获得相同的比特传输速率，我们需要做一些简单的计算。

将772kHz带宽扩展1倍就可获得1.544Mbps的比特速率。这意味着使用AMI编码，T1的每

一个模拟信号周期要用两比特来编码。HDSL采用2B1Q编码，即每一个周期用4比特表示，所以在196 kHz带宽上可获得784kbps的比特速率。此外，由于使用了回波抵消，HDSL在两条线路上都能实现全双工传输，那么在每个方向上的总传输速率就为1.544Mbps。

需要指出的是在同一传输设备上，HDSL不能像其他的DSL技术那样提供模拟话音业务。另一方面，HDSL在业内销售得很好。HDSL的HDSL/2版本使用无载波调幅/调相和正交幅度调制（CAP-QAM，Carrierless Amplitude / Phase and Quadrature Amplitude Modulation）技术，能在一对双绞线上进行双向传输，并使双向速率都达到1.544Mbps。

如果只使用一对HDSL线，那么在两个方向上的速率为784kbps。其中，768 kbps可以用于用户业务，其他部分用于帧同步和额外的开销。这种HDSL被称为单对DSL（SDSL，Single pair DSL）。

6.3.4 ISDN数字用户线（IDSL）

另一种对称的DSL服务是IDSL（ISDN Digital Subscriber Line，ISDN数字用户线）。在一对双绞线上，IDSL能以144kbps或160 kbps的速率进行全双工传输。它通常使用ISDN的BRI接口。由于不需要D信道提供交换接入，因此只采用B信道用来传送用户信息。然而，IDSL可以为交换业务提供专用的链路。例如IDSL能提供到帧中继交换机的连接，这是一种典型的交换业务。IDSL的一大优点是在很多情况下可以重新使用那些已有的ISDN线路，使之容量更大。另外，读者还会记得DSL所面对的挑战之一是DLC系统，因为它可将多路POTS线路多路复用在一条数字链路上进行传输。而IDSL可使用ISDN的低速率即4kHz话音频带，因此是一种不受这些载波环路系统限制的DSL。

6.3.5 非对称数字用户线（ADSL）

回顾一下图6-3，我们介绍了如何配置有线电缆系统，以便能在有线电视上传输因特网业务。在图6-6中又讨论了如何修改POTS服务，以便能在话音频带上传输因特网业务。ADSL（Asymmetric Digital Subscriber Line，非对称数字用户线）工作带宽为1MHz，而话音调制解调器的工作带宽只有4kHz，这就是为什么ADSL能提供的下行速率可达8Mbps、上行速率可达1Mbps的原因。

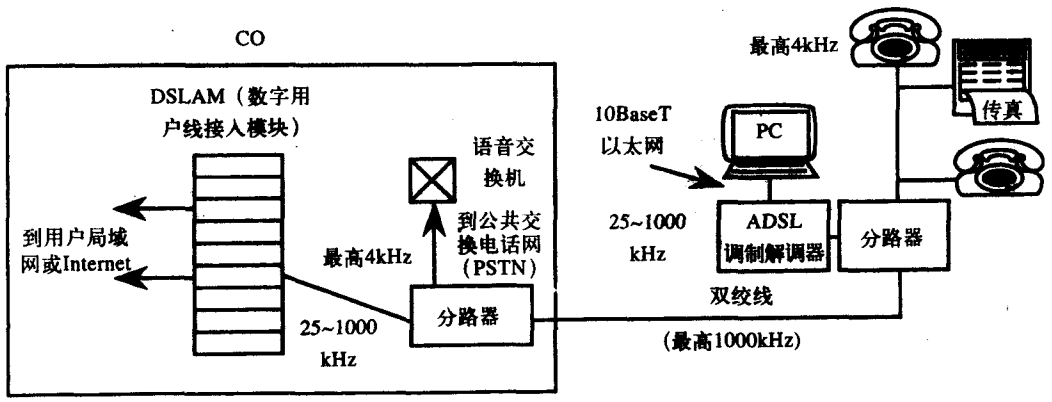


图6-6　使用从25kHz至1MHz频率，高速ADSL数据可以在一对双绞线上传输，同时话音业务也不会受到影响

ADSL和POTS线路一样也是接入到家庭中的双绞线。只不过分路器将低于4 kHz频率分配给老式的电话或传真线路，而将较高的频率分配给ADSL调制解调器。其中4kHz ~25kHz

是保护频带，其目的是减少话音信道和ADSL信道间的干扰，如图6-7a所示。与电缆调制解调器一样，PC和ADSL调制解调器间也是由以太网接口连接，这样在一个人在打电话的同时另一个人还能使用PC。与电缆调制解调器相同，ASDL一直连通，不需拨号与ISP建立连接。

在CO一侧，用一个分路器将频率分开。4kHz信号被直接送到PSTN或话音交换机，其他频率的信号被送至数字用户线接入模块（DSLAM，Digital Subscriber Line Access Module）。事实上，DSLAM是ADSL 调制解调器的集合，每一个ADSL 调制解调器对应一个用户。当然，每一用户都有独立的分路器和连接器接至DSLAM。用户端的ADSL 调制解调器称为ADSL用户端单元（ATU-R，ADSL Terminal Unit-Remote），对应的CO中的设备被称为ADSL 局端单元（ATU-C，ADSL Terminal Unit-CO）。ADSL是一种模拟技术，也就是它将数据调制在模拟信号上，并且传送模拟形式的话音信号。另一方面，HDSL和IDSL都是数字传输技术，它们是以数字形式来传送信息。

使用分路器对用户和交换局都有好处。对客户端而言，分路器使用户能利用原有双绞线继续享受电话业务，同时室内的其他应用也不需再重新布线。同样，对于提供服务的CO来说，话音交换机只需像往常一样提供话音业务，因特网业务的路由选择由专用设备提供。与话音连接相比，因特网连接通常要持续更长时间。此时，话音交换机内会寄存相当一部分因特网业务，这就要求话音交换机具备更大的容量来进行数据处理。将话音交换机内的数据业务移交给因特网路由器处理，能使资源的利用更加合理。电话公司喜欢ADSL的另一个原因是它提供了与有线电视运营商竞争的手段。

最初ADSL的概念是Bellcore为解决视频拨号音问题提出来的。这种技术允许住宅用户拨号点播视频节目，并在设备上播放。要实现视频点播，在长度为18 000英尺的铜线上需要的下行速率为1.544Mbps，上行速率为64kbps。但目前，人们似乎对利用它来提供因特网服务更加感兴趣。所有的ADSL线路的速率都是自适应的，即它们在各种不同环境下均可自动调整以达到最高的速率。调制解调器开启后，ADSL会自动检测所能达到的最高数据传输速率。若在数据发送过程中一个人用电子打火机点燃气炉，或者制造了其他类型的干扰，数据传输速率会自动地被调整降低；一旦干扰消除，传输速率又会自动地增加并复原。

安装每一条ADSL线路时电话公司都要派专业人员安装频率分路器。显然，电话公司希望能避免在整个国家内为每一个用户进行这种繁琐的铺设工作。为解决此问题，一种ADSL的简化版应运而生，即通用ADSL（UDSL，Universal aDSL）。UDSL也被称为G.Lite或无分路器的ADSL。尽管在CO端仍然需要安装分路器，但是G.Lite使电信公司不必再为挨家挨户地安装分路器而头痛。然而，G.Lite的数据传输速率低于ADSL。使用G.Lite，电话机和PC都与同一对线相连接，这样会使数据信道中的高频信号串入话音电路，同时又会使话音电路中的信息进入到数据信道。但是由于G.Lte的数据传输速率降低了，因此这种话音和数据信道间的相互干扰也可忽略不计。

图6-7a介绍了如何利用FDM（Frequency Division Multiplexing，频分复用）在频谱的低端发送话音信号。其中，上行数据被调制在25~200kHz的载波上，而下行数据使用的带宽范围为200kHz~1MHz。使用回波抵消技术，下行数据的带宽还可增加，如图6-7b所示。FDM技术使上行和下行信号的带宽分离，而回波抵消使它们重叠，这就是ADSL的工作方式。

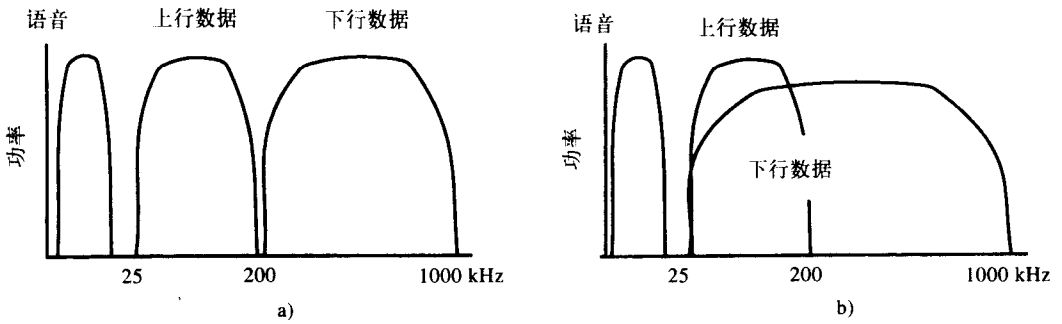


图6-7　a) 使用FDM技术，上行和下行信号的带宽被分离；b) 采用回波抵消技术，上行和下行信号被重叠

6.3.6　ADSL采用的调制技术

最初在一个模拟载波上采用AT&T的CAP(Carrierless Amplitude/Phase Modulation，无载波幅度/相位调制，无载波调幅调相)技术，这是一种应用于调制解调器的老式技术标准，大部分工程师都很熟悉。同时它也是一种可靠实用的调制技术。

后来ANSI提出一种被称为离散多音调传输 (DMT，Discrete Multitone Transmission)的调制方案。这是一种高效智能的解决方案，它使用256个不同载波，每一载波带宽为4kHz。在一般的传输线路中，在传输频谱中的某些频率点上总存在一些反常点，在这些频率点上无法传输信息。这是因为导线总存在着损耗，正如我们在前面指出的那样。例如，不匹配的导线规格和桥接抽头的影响等。利用256个载波，DMT自动地舍弃一些无法使用的载波，使其他的载波工作效率最高。此外，DMT还使用了回波抵消技术，使传输比特率得到提高。

理论上，DMT 256个载波中的每一个都可以以0~60kbps的速率传输信号，全部加起来总的传输速率为15Mbps。实际上，每个载波的传输速率只能达到32kbps，总传输速率为下行链路8Mbps，上行链路为832kbps。在进行这些计算时，要注意这里使用了回波抵消技术，这样下行载波有250个，上行载波有26个。图6-8给出了一些DMT载波的计算数据。

	每个信道	语音频带	上行频带	下行频带
信道标号	—	1~6	7~32	7~256
信道数量	—	6	26	250
带宽(kHz)	4.3125	25.875	138	1104
比特率(kbps)	32	—	832	8000

图6-8　DMT的一些相关数据

习题

6.1节至6.3节

为下面的四个问题选择相应的答案:

a. 56K 调制解调器　b. 电缆调制解调器　c. ADSL　d. IDSL

1. 哪些业务是非对称的?
2. 哪些业务一直连通?
3. 在数据连接的同时，哪种业务能提供另一个连接?

4. 哪种业务在实现时需要使用以太网卡?

6.1 节

5. 对56K 调制解调器而言，传输路径的哪一部分是模拟的?

a. 从ISP到PSTN b. PSTN内 c. 从PSTN到客户 d. 用户的PC内

6. 当调制解调器开始建立连接时，决定使用哪一种协议的过程叫什么?

a. 聚焦 b. 握手 c. 训练 d. 学习

7. 在每一个方向上56K 调制解调器的最高速率是多少?

8. 解释握手和训练的差异。

9. 56K 调制解调器连接两端的设备相同吗? 如有不同，指出不同之处。

10. 列出几种56K 调制解调器获得最高速率的方式。

6.2 节

11.为了支持上行链路传输，有线电视公司需要做什么?

a. 安装光纤 b. 安装不同类型的放大器 c. 安装双向电缆 d. 在用户端安装电话线

12. 在哪一个方向上电缆调制解调器的连接与其他的相邻用户共享? 哪个方向为用户提供了专用信道?

a. 只有上行链路被共享 b. 只有下行链路被共享

c. 上下行链路都被共享 d. 上下行链路都是专用的

13. 电缆调制解调器的哪部分使用了以太局域网技术?

14. 采用哪种设备将有线电视信号分送给不同用户?

15. 有线电视公司通常使用哪种设备来增强电缆中信号的强度?

16. 在一个城市中有线电视公司通常设置多少个头端局?

17. 描述在750MHz电缆设备中使用的频谱和信道分配情况。

6.3 节

18. 在本地环路上提供数字业务时，下面哪一项不是干扰因素?

a. 天气状况 b. 没有连接的桥接抽头 c. 导线规格不统一 d. 负载线圈

19. 下列哪种DSL可支持无中继的T1操作?

a. HDSL b. IDSL c. VDSL d. ADSL

20. 对于19题，给出两种实现方案。

21. 描述DLC及其实现的目的。

22. DLC是哪种DSL发展的障碍?

23. ADSL 调制解调器和DSLAM的其他名称是什么?

24. 哪种ADSL支持无分路器操作? 为什么使用分路器被看作是一种缺点?

25. 为什么电话公司对ADSL的推广感到忧虑?

26. 哪种ADSL调制技术只使用一个载波?

第7章 局域网的基本概念

7.1 简介

7.1.1 局域网（LAN）的诞生

从20世纪80年代早期始，PC开始广泛地应用在商业上，在办公室工作的人们就很少再使用中心主机了，很多的工作在他们桌前的PC上就可以完成。他们也可以独立地完成一些任务，不用再跑到数据处理部门等着用中心主机来做了。

很明显，由于工作人员都需要与他人相互协作，这些处理工作需要联网来完成。最初，“暗地联网（sneaker-netting）”（携带磁盘从一个PC到另一个PC）就可以满足需要。但不久，随着数据量的增加，联网变成了必然的趋势。

局域网是一种让与计算机相关的设备间进行通信的专用网络，它一般分布在不到一英里的范围内，典型的是分布在一幢大楼内。计算机及其外围设备相互连接在一起，可以进行非集中的控制。

局域网本质上允许资源的共享。这些资源包括信息，诸如数据文件、多媒体文件、电子邮件、语音邮件或者各类软件，还可以是一些外围设备， 例如专用打印机、扫描仪、绘图仪或者存储设备等。在局域网中，各工作站还可以通过共享以利用其他工作站的处理能力或者是进入中心主机。当然，局域网也有其自身的缺点，最主要的就是文件和计费的安全性问题。

7.1.2 局域网与电话网的比较

局域网中也使用一些电话网中的设备， 比如安装在一幢大楼内的本地用户交换机。尽管交换机网络最初是为传送话音而设计的，而局域网是为传送数据设计的，但是它们的一些设备具有类似的功能。

如表7-1所示，这两种网络都有终端设备，就是网络的终止的末端点或者是发送信息的节点。网卡（NIC，Network Interface Card）或者网络适配器被插在局域网的一个节点（如PC、打印机、路由器等）上。附着在网络上的设备只有其网卡的类型匹配时才能从相应的节点接入网络。在每一块网卡内都预先置入了唯一的一个物理地址，只要接通电源，它就可以检测到自己的物理地址。电话没有这样的地址。电话号码由这个电话插孔内插入的插头所决定。然而对于网卡来说，不论被插入在什么设备中，其物理地址都是一样的。这种地址是预先烧在只读存储器（ROM，Read Only Memory）中的硬编码。以后将会了解到，这个地址还被称为MAC地址、硬件地址或者NIC地址。

表7-1 电话网与局域网的比较

	电 话 网	局 域 网
终端设备	电话	网卡（NIC）
传输介质	双绞线	UTP、光纤
拓扑结构	星型结构	星型或环型
接入方式	拨号	CSMA/CD和令牌传送
通信方法	西班牙语、英语等	NetWare、TCP/IP

电话网使用电话线连接形成星型拓扑结构。类似地，局域网也需要传输介质连接形成某种拓扑结构。然而对于局域网来说，可以选择的传输介质和拓扑结构更多。

通过拨号一部电话可以“访问”另一部电话。类似地，也一定有相应的接入方法使一个网卡可以访问另一个网卡。但是如果一个人与另一个人通话，但讲的不是同一种语言，他们之间将无法进行交流。同样的道理，如果一个操作系统通过网卡访问另一个操作系统时，如果使用的通信协议，如NetWare或TCP/IP不同，操作系统之间也不能正常通信。

因此，为了使局域网正常地工作，需要确定一种访问协议，这种协议由所选择的局域网类型所确定。我们还需要确定使用的通信协议，这由所运行的应用来决定，或者看操作系统是否能够支持。还要注意的是，在PBX网络中，只使用一种“访问协议”（即拨号），却可以允许同时存在多种“通信协议”（西班牙语和英语）。同样的道理，在局域网中只有一种访问协议，也可以同时存在两种或多种不同的通信协议。换句话说，当一台计算机“讲”Netware时，另一台计算机却可以“讲”TCP/IP。实际上，如果在一台机子上打开两个视窗，在其中一个上用Netscape运行TCP/IP，而同时另一个可以用当地的Novell服务器运行Netware。

现在我们已经初步了解了局域网的五个主要组成部分，网卡、介质、拓扑结构、访问和通信协议。接下来，我们要逐个深入地学习这些内容。第4章已经介绍了各种传输介质。在本章的下面两节中，我们将讨论拓扑结构和访问协议。在第8章中将学习现在应用最为广泛的通信协议——TCP/IP协议。访问协议作用在OSI模型中的最下面两层，而通信协议作用在上面几层。

7.2 拓扑结构

在建设局域网之前，首先要仔细地规划一下该如何布线，或者说需要规划网络的物理布局。一旦网建成以后，再改变布局非常困难，而且花费不小，可能这就是为什么称之为“拓扑”的来由吧。正是由于这个原因，利用无线技术连接的局域网越来越受到重视。现在让我们来看一下三种最基本的拓扑结构以及从它们派生出来的其他类型的结构。

7.2.1 星型拓扑结构

由于室内的电话线网已经存在，因此，当利用这些已有的电话线来建设局域网时，可以采用星型拓扑结构，如图7-1a所示。在这种情况下，局域网的建设非常容易，尤其是在一些电话线没有被使用的情况下更是如此。

星型拓扑结构只有一个中心节点，或者叫集线器，各工作站分别被连接在这个节点上面。尽管这种网络的可靠性完全依赖于中心节点的可靠性，但是网络的管理、控制和故障诊断因此也变得容易。每个站点都需要两个接口，一个在工作站端，一个在中心节点端。另外从集线器到工作站还需要一个线路或链路。

当星型网络被级联时，就形成了一棵“树”，如图7-1b所示。由于星型网络在管理上的特殊优点，因此很多网络在物理布线上都采用了这种结构。

7.2.2　总线型拓扑结构

有一段时期总线型拓扑结构十分流行，如图7-1c所示。网络的各组成部分都被连接在一条公共的线路上，这条线路被称为总线。网络各部分通过这条总线进行通信。各站点都可以侦听总线上的业务。这些业务由发送设备广播，只有与业务的目的地址一致的设备才能接收这些数据业务。

有时，主电缆（总线）与网卡之间通过一条引入线连接；有时，总线就直接连在网卡上。如果将主电缆截断，把两根电缆分别连在网卡两端的连接器上，如图7-1d所示，这种拓扑结构被称为“菊花链总线型”。这种情况下没有公共的总线，信号的接收和重发都需要经中间节点转发。

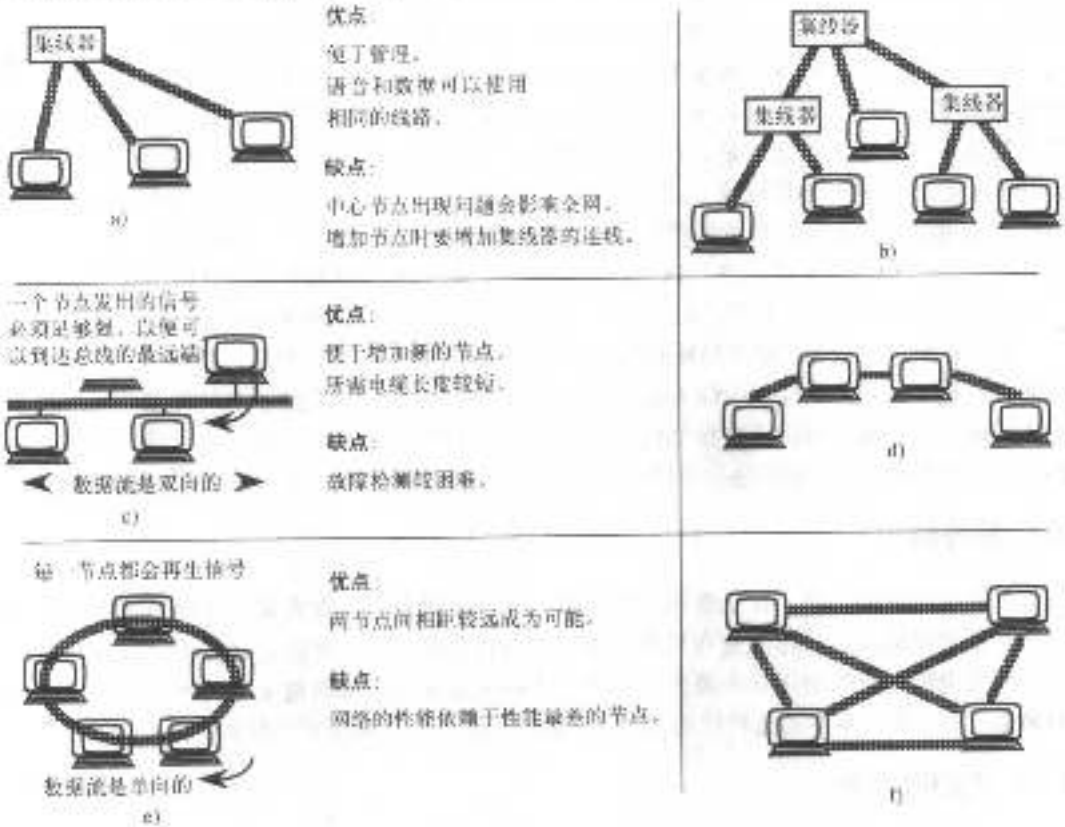


图7-1　图的左侧是三种主要的拓扑结构，右侧是从它们派生出来的其他类型的拓扑结构。
a)星型，b)树型，c)总线型，d)菊花链型，e)环型，f)网状型

总线型是一种简单且便于建设的拓扑结构，它不必向星型结构那样，每个站点都必须有一条到中心集线器的独立连接。尽管总线型结构去掉了常见的故障节点——集线器，但总线型结构似乎更容易出错，因为在诊断故障时，要孤立一个故障非常困难。只要有一个网卡连接不好，整个网络都会受到影响，很难找到出现故障的网卡。所以总线型结构会严格限制各站点的位置以及数量。

然而，总线型（菊花链型除外）之所以流行的一个原因是，它的网卡是一个典型的无源的设备（不会转发信号），当有一个站点出问题时，网络可以照常运行。因为网卡是无源的，所以价格就比较低。

7.2.3 环型拓扑结构

环型拓扑结构有点像菊花链型，就是所有的节点连在一起形成一个环，如图7-1e所示。当环上的各节点再进行连接时，如图7-1f所示，这时网络对可能的故障具有恢复能力，这种拓扑称为网状结构，一般应用在广域网中。图7-1f是一个完全连接的网状网络。

各节点间通过点到点的连接连在一起，所有的节点都连上以后就形成一个环。这使得环型拓扑结构更适合基于光纤的局域网，因为光纤链路的传输需要一个发射机和一个接收机，业务的传输只能朝一个方向。所有的节点接口都是有源的，能够再发送接收到的信号，这样的网卡就比较贵，但是相邻两个节点之间的传输距离要比总线型的大得多。

理论上，环形拓扑结构是一种相对简单的设计，而且电路费用也比星型拓扑结构要低一些。信号传输速率与吞吐量的比值要高于总线型结构。不过，由于环型中使用的是具有存储转发交换功能的有源节点，因此更容易发生错误。更进一步说，如果某个节点传输速率较慢，或者在中继时发生错误，整个网络的性能都会下降。

7.3 访问协议

7.3.1 带冲突检测的载波侦听多路访问协议（CSMA/CD）

在局域网按选定的拓扑结构布置好以后，还需要访问方法，以使一个节点能够知道有另外一个节点存在，并能向其传送数据。现在应用最为广泛的访问方法就是带冲突检测的载波侦听多路访问（CSMA/CD，Carrier Sense Multiple Access with Collision Detection）协议。

这种协议的规则是相当简单的。实际上，CSMA/CD就像是一些讲礼貌的人们在房间里聊天时所遵守的约定一样。假设几个人在房间里，有一个人想发言；这时如果没有其他人讲话，他就可以开始说话。再假设，大家都很懂礼貌，不会打断这个人的发言，直到这个人完成了他的“发送”。当房间里又安静下来后，有两个人都想发言，就可能同时开始讲话。但马上他们都停了下来，因为这时出现了“冲突”，两个消息会被混淆在一起。他们就会各自等待随机的时间后，重新开始讲话。

现在再来看一看CSMA/CD如何在局域网中使用。一个站点如果想使用传输介质发送数据，必须首先侦听一下线路中是否有其他的网卡正在发送。如果没有，这个站点就可以立即发送；在传输过程中，发送站点还必须继续侦听是否有其他的站点开始了发送。如果有，这个发送站点就必须中断发送，等待一定的随机时间后，再重复侦听、发送的过程。这一过程要一直持续到所有的数据全被成功地发送出去，并且没有被其他站点发送的数据毁坏。

现在看一个例子。在图7-2中，总线型拓扑结构中有三个节点，节点X、Y离得比较近，而Z离它们较远。起初，节点X侦听线路以确保没有人正在使用，然后就开始发送。在一小段时间之后，由于X的信号很快就会到达Y点，所以这时Y不会进行传输；但是由于Z离X比Y远，还没有侦听到线路上的X的信号，所以开始进行发送。

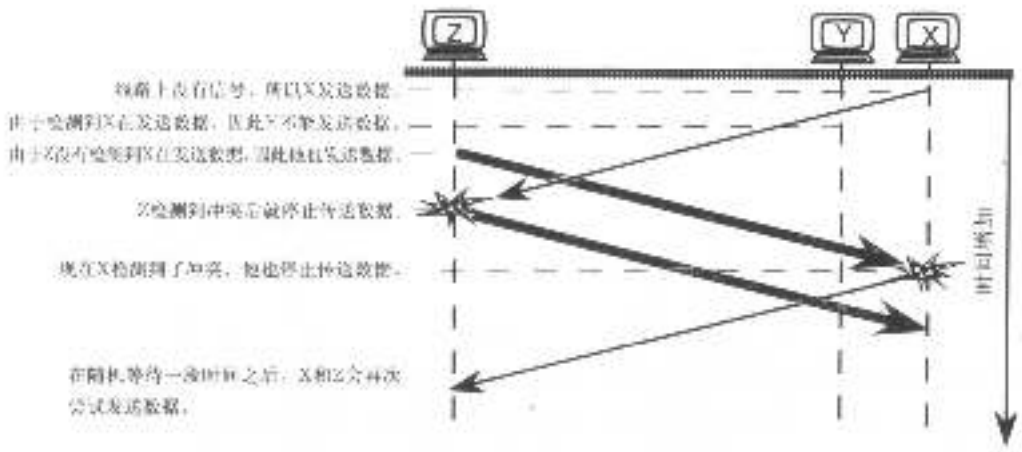


图7-2　CSMA/CD访问方法示意图

最终，节点Z侦听到了X的信号并停止了发送；相应地，X也听到了Z的信号，也停止发送。它们都会在随机等待一段时间后，再尝试发送其数据。

要注意的是，一旦检测到冲突，前面已经发送的数据就无法使用了，整个数据块都必须重发。换句话说，数据的吞吐量总是小于介质的带宽。由于这个原因，在使用CSMA/CD的以太网中，数据的吞吐量近似为介质可用总带宽的30%。当然，这个数字还与如何配置网络和如何使用网络有关。因为基于“只要可能就发送”的原则，对于业务量较大的大型网络，CSMA/CD协议无法正常工作。

虽然如此，对于介质业务负载较轻的网络，这种访问协议的表现还是不错的，只是在有许多站点试图同时发送数据时，表现得才比较糟。这时候，可以使用网桥和路由器把网络分成几个小型的局域网。

在关于ISDN的那一章里，我们还会介绍CSMA/CR（CSMA with Collision Resolution），即带冲突分辨的载波侦听多路访问协议。这个协议能提供优于CSMA/CD的吞吐量。因为在CSMA/CR中，数据不必重新发送；而在CSMA/CD中，发生碰撞之后必须重发整个数据块。

7.3.2　令牌传送协议

CSMA/CD是一种竞争的，或者说是随机的访问方式，这意味着可能会有几个节点同时争用介质带宽。也就是说，这是一种带有不确定性的访问方式。因为一个节点究竟要等多长时间才能访问网络与那个时刻的业务量有关。

与CSMA/CD相反，令牌传送协议是一种无竞争的访问方式。保证每个节点都有一定量的带宽。也就是说，排除了不确定因素，它被认为是确定的，因为访问网络的时间是可以预知的。

令牌传送方式主要用于环型和总线型网络。在这些网络中所有的节点有一定的逻辑顺序。数据信号从一个节点被传到另一个节点，直到又回到出发点。当数据在环中被传送时，接收数据的节点将数据拷贝到自己的缓冲器中。如果一个节点想要发送数据，必须拿到一个被称为**令牌**的特殊比特组合。一旦拿到令牌，这个节点不是再进行传递，而是将数据放在一个帧中进行发送。当接收方从这个帧中识别出目的地址是自己的地址时，就接收这一帧并进行误差校验。

如果这一帧无错，接收节点就在这个帧的结尾加一个拷贝比特，再把其回送给发送节点。

发送节点检查拷贝比特就能知道这一帧是否被正确接收。如果是，就将令牌释放给环中的下一个节点。否则就重发这一帧。图7-3解释了节点C向节点E发送数据的整个过程。在图7-3a中，A把令牌传给B，而B并没有数据要发送，就把令牌传给想发数据的节点C，如图7-3b所示。

在图7-3c中，C从环中拿到令牌，发送数据帧给节点E；而节点D知道这一帧是给别人的，就让其通过，并传给下一个节点；在图7-3d中，E查阅这一帧并确定没有错误，就在帧的结尾加上拷贝比特，又送还给C，见图7-3e。最后图7-3f表示，节点C从拷贝比特中了解到这一帧已经被正确接收，故此删除已发送的帧并释放令牌，使环上的其他人有机会发送。

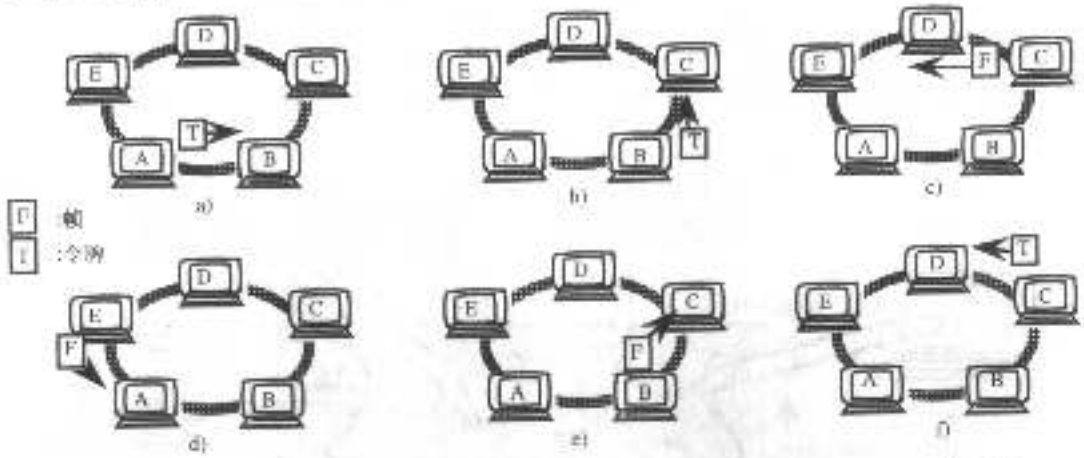


图7-3 a) 由于节点B没有数据要发送，令牌直接通过它。b) 节点C有要发的数据，所以拿到令牌。c) 节点C向节点E发送数据帧。d) 节点E收到数据后在其后添加拷贝比特，完成确认。e) 节点C得到确认。f) 节点C释放令牌，以使环上的其他节点有机会发送数据

7.4 局域网的类型

表7-2给出了现在使用的三种主要局域网的类型，它们分别是：以太网，令牌环网和光纤分布式数据接口（FDDI，Fiber Distributed Data Interface）。在本章中，我们只涉及以太网和它的各种变化形式，在以后的有关局域网的章节中再详细介绍令牌环网、FDDI和高速以太网。

表7-2 第一代局域网的几种类型

	以太网	令牌环网	FDDI
传输介质	同轴电缆和UTP	STP	光纤
拓扑结构	总线型和星型	星型连接的环型	环型
访问方式	CSMA/CD	令牌传送	令牌传送
传输速率	10Mbps或更高	4Mbps和16Mbps或更高	100Mbps
典型的帧长	1526B	4500B	4500B
标准	Ethernet II 和IEEE的802.3	IEEE的802.5	ANSI 的X3T9.5

以太网：以太网有很多版本，但它们几乎都使用CSMA/CD协议，它们都使用相同的帧结构，最大帧长度都为1526B。在逻辑上，它们都使用总线型结构；但是在物理上，较新的以太网使用星型拓扑结构。传输介质可以是同轴电缆、无屏蔽双绞线（UTP，Unshielded Twisted Pair）和光纤，传输速率为10Mbps、100Mbps和1Gbps。因为它们都使用CSMA/CD，所以其

吞吐量的典型值只有30%~50%，因此，一个10Mbps的以太网只能成功地传输3Mbps的数据。因为碰撞和帧头所需要的额外开销，所以相当一部分带宽被浪费掉了。IEEE标准化了以太网，其规范是802.3。

令牌环网：令牌环网使用有源的网卡，也就是说，各网卡将信号沿环转发给下一个节点。这就是为什么在相邻两个网卡之间的距离可以达到300m的原因。这个距离比以太网的传输距离长得多。另外，令牌环网的帧长度也大于以太网的帧长度。

图7-4表示一个被称为多站点接入单元（MAU，Multistation Access Unit）的布线集中器是如何把各节点连接成一个令牌环网的。可以看到，因为所有的节点都与一个MAU相连接，所以物理上其拓扑结构是星型的，但在逻辑上其拓扑结构却是环形的。传输的信号路径依次从一个网卡到另外一个网卡，直到最终回到原先发送它的站点。所以，可以将令牌环网理解成是一个星型连接的环。

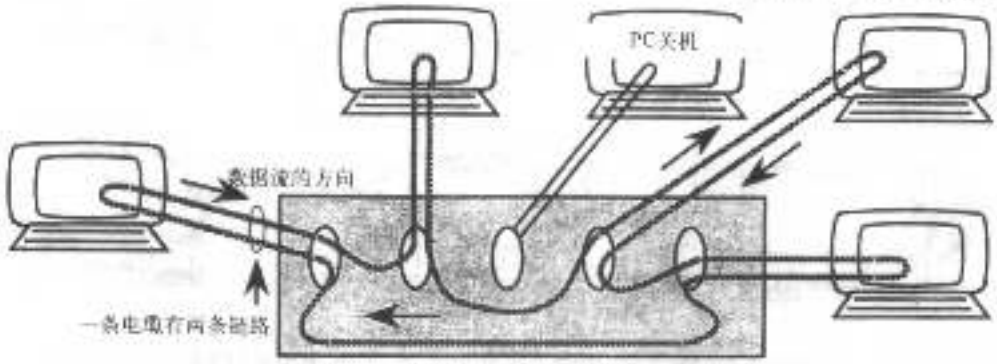


图7-4　令牌环网络使用星型连接的环型拓扑结构。逻辑上，数据在一个环中流动；物理上，局域网中的所有节点都是星型连接的。如果一台PC关机或有一个网卡不工作，MAU会将这条支路与网络隔离

最初，这些网络都是用屏蔽的双绞线（STP，Shielded Twisted Pair），但是今天UTP和光纤也被使用。刚开始，令牌环网络的工作速率只有4Mbps或16Mbps。而且只要有一个网卡的速率是4Mbps，整个网络就被限制在这个水平上。由于使用了令牌传送协议，因此能获得95%的吞吐量。其余的带宽被用于成帧的开销、帧头和相邻帧之间所需要的间隙。IEEE的令牌环规范是802.5。

令牌环和FDDI都可以被配置成双环结构，如图7-5a所示。其中一个环被称为主环，在局域网正常工作时用来传输数据。另一个环是备用环。如果有一个节点崩溃，如图7-5b所示，或者两个节点间的电缆被意外切断，如图7-5c所示，那么邻近节点中的网卡就会发现到这个问题，然后会自动环回这些数据，利用备用环，重构一个传输回路。当有其他问题发生时，局域网就会被分成两个部分。因此这个网络可以尽快地纠正问题，而不是继续工作在一种"环绕"的模式中。

FDDI：图7-6是一个经过简化的FDDI网络。FDDI使用光纤，能提供100Mbps的运行速率。美国国家标准化组织（ANSI）在X3T9.5规范中对FDDI进行了标准化。它典型地被用在远距离传输的骨干网中承载数据，比如用在高层建筑中或者用在一个校园的几幢建筑物之间。因此，FDDI通常被建设成环形。由于它要承载局域网间的大量数据，因此使用双环结构可以抵抗网络故障。

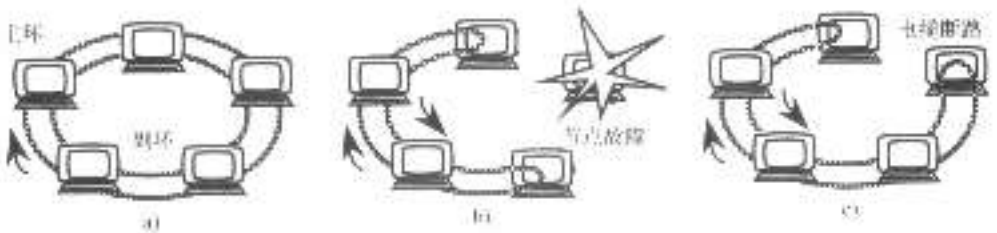


图7-5 a) 是一个双环结构，使用主环传送数据；b) 如果一个节点不能工作，副环可以使环路自愈；c) 如果某处的电缆被意外地切断，这个环路也可以自愈

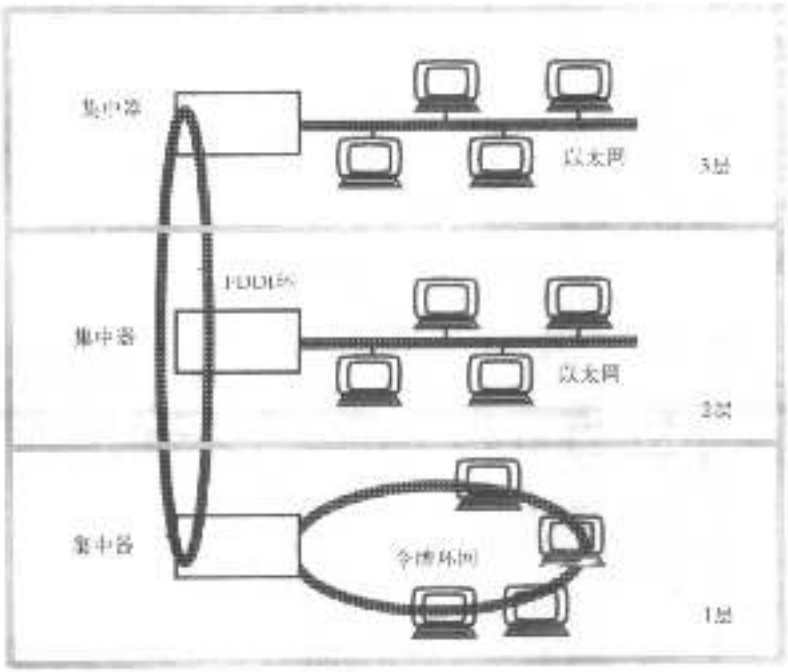
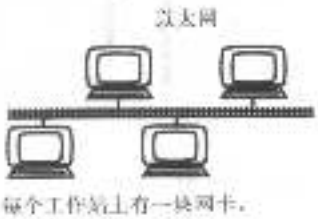


图7-6 FDDI可用于一幢大楼内不同楼层间的局域网互连，还可用于校园环境中不同建筑之间的局域网互连

7.5 几种基本的以太网

表7-3给出了三种基本类型的以太网（见右图），分别是10Base5、10Base2和10BaseT。它们使用相同的帧结构和CSMA/CD访问协议。尽管有很多种类型的以太网，但它们都是利用右侧图所示的总线型拓扑实现相互连接。在物理上它们采用的连接方式可能不同，但是在逻辑上都是共享一条信道。也就是说，在任何一个时刻，只有一个网卡能够成功地传输数据。下面来看一下各种类型的以太网是如何布线的。



7.5.1 10Base5

10Base5是最早的一类以太网，你可以发现它至今仍然用在骨干网络上。骨干网是将其他网络互连起来的网络。如果不算使用光纤，这种以太网提供的范围最大，但是它所使用的粗

缆比较昂贵，且因体积大而施工不便。

表7-3　几种10Mbps的以太网

	10Base5	10Base2	10BaseT
标准化的时间	1983	1988	1990
IEEE标准	802.3	802.3a	802.3i
传输介质	粗缆	细缆	Cat3,4,5
物理结构	总线型	总线型	星型连接为总线型
访问方式	CSMA/CD	CSMA/CD	CSMA/CD
分段的最大距离	500m	185m	100m
每个段的节点数	100	30	与集线器有关

从图7-7可以看到局域网的总线实际上是被安装在天花板上或墙的背后。由于电子工程的需要，总线的两端都需要一个终端匹配器。如果总线端接不良，整个网络都不会工作。对网卡来说，与总线连接的收发器完成CSMA/CD的功能，网卡被安装在PC内部，与收发器通过一条15针的引出电缆相连。在引出电缆的两端使用DB 15的连接器。

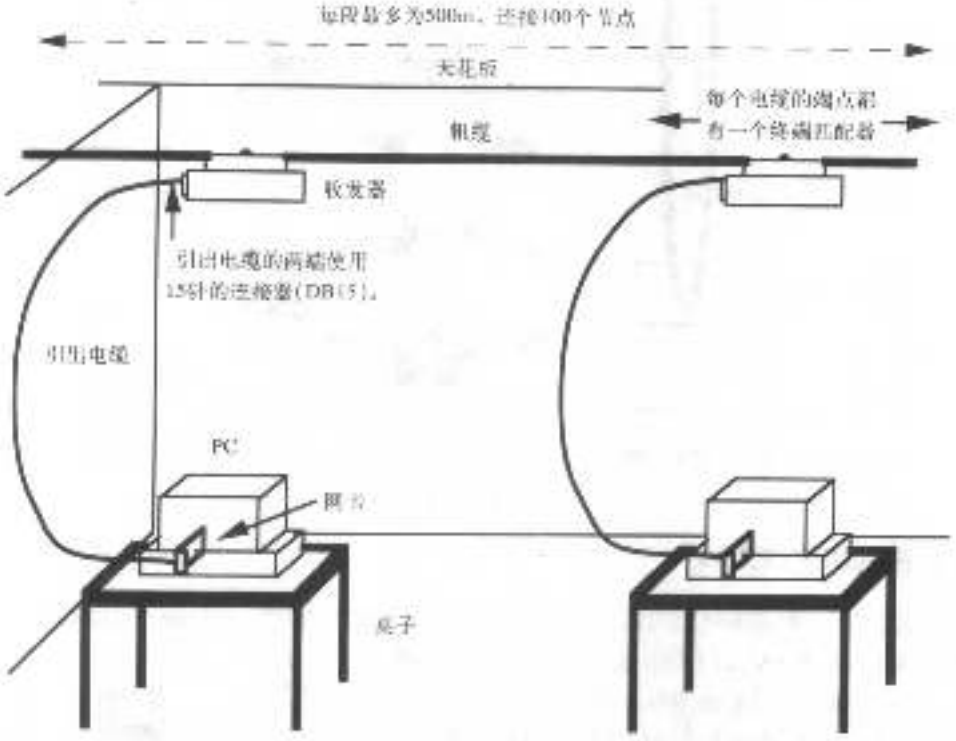


图7-7　常用的10Base5连接

7.5.2　10Base2

10Base2是一种比较简单的以太网的版本，与10Base5不同，它的网卡中包括了收发器，使用的同轴电缆比10Base5的电缆细（见图7-8），电缆两端的终端匹配器同样是必需的。它的电缆不是远离终端用户，而是实际上就被安装在PC里。如果一个用户想移动它的PC，很可能

就会错误地破坏计算机后面的电缆。这种端接不良的同轴电缆，很容易会导致整个局域网瘫痪。当然，没有人会故意地破坏电缆。但是如果你不得不搬到其他的办公室去，就必须检查所有的连接。只要有一个连接头松动，都必须费很大的力气才能查出问题的所在。

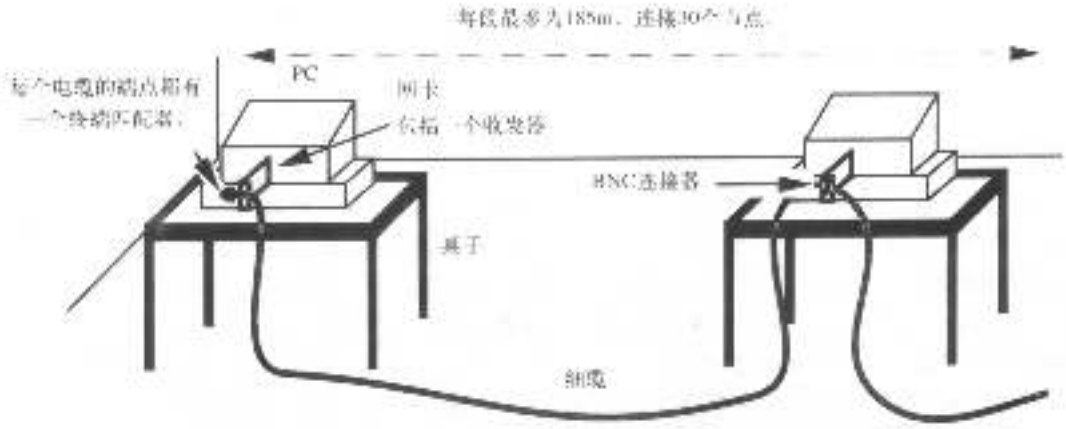


图7-8 10Base2连接，采用细缆并将收发器集成在网卡中

在任何情况下，10Base2都采用纯总线型拓扑结构，只有一条通信信道存在，所有的网卡共享这条信道。尽管它比10Base5经济，但应用范围比10Base5小，而且，在每个局域网网段上允许连接的站点也较少，可以连接站点的实际数目参见表7-3。

7.5.3 10BaseT

从拓扑结构上说，10BaseT的布线与其他类型完全不同。图7-9a给出以太网的基本布线结构，10BaseT与这个图在逻辑上是一致的。更确切地讲，它的结构应该如图7-9b所示。与其他的长度达数十米的总线不同，10BaseT的总线在集线器内。这个集线器可能是一个放在某个人桌上的小盒子，也可能被安装固定在一个19in或23in宽的机柜上。但无论如何，总线都是在集线器内。

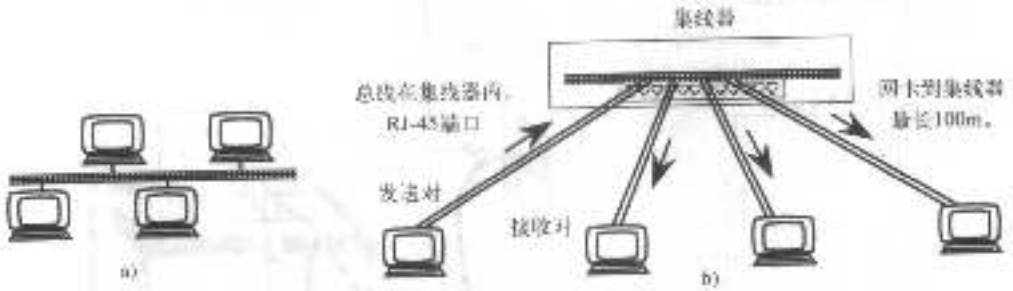
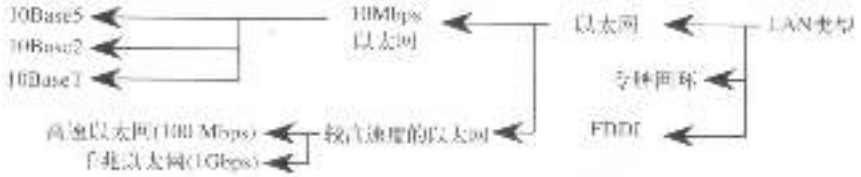


图7-9 a) 最初的以太网结构。b) 10BaseT网络结构。在这里，总线不是延伸数米，而是在集线器内。最左端的网卡发现总线上空闲，于是向集线器发送一个数据帧。集线器将数据依次转发给其他的活动节点

集线器由交流电供电。这是因为它们要把从一个端口接收到的信号再转发给其他端口。在图7-9b中，有一个8端口集线器，每个端口通过一个RJ-45插头接入。UTP电缆通常都是5类线，用其中的一对线发送，另一对线接收。尽管5类线固定地有4对线，但在10BaseT中只用了其中的两对。两端带有RJ-45插头的网线连接网卡到集线器上，连接形成一个星型结构。由于总线在集线器里，这种拓扑结构也被称为星型连接的总线。在物理上，它看起来更像星型结

构；但是在逻辑上，它的确是地道的总线型。10BaseT（见下图）通常用在更局域化的环境中，因为它的传输距离比老式以太网要小得多。集线器和网卡之间的最大距离不能超过100m。这样，如果要大范围地安装而又不使用光纤的话，就需要更多的集线器和机柜。



在图7-9中，最左端的网卡检测到总线上没有载波，就发送一个数据帧给集线器。集线器是OSI物理层设备，只是简单地转发这个信号（或数据帧）给其他所有的端口。它并不知道这一帧的目的地址指向的是哪一个网卡，就发给了其他所有的端口。如果某个网卡出现了问题或者正在发送“垃圾”，集线器可以隔离这条链路，从而保证局域网的其余部分能正常工作。当问题被解决之后，集线器可以自动地恢复与这条链路的连接，不需要人工干预。集线器上的光发射二极管（LED，Light Emitting Diode）可以很清楚地表明每一条链路的工作状态，是正在工作，还是没有工作，或者是出了差错。集线器还可以收集业务管理数据，从中可以发现哪些节点需要更多的带宽容量。

我们将根据图7-9b来描述10BaseT网络。不妨先想一下在物理上这种结构是如何布线的？图7-10不像原理图那样规范，但注意图7-9b中的所有部分都能在图7-10中找到，只不过是从网卡到集线器的路径有点混乱。

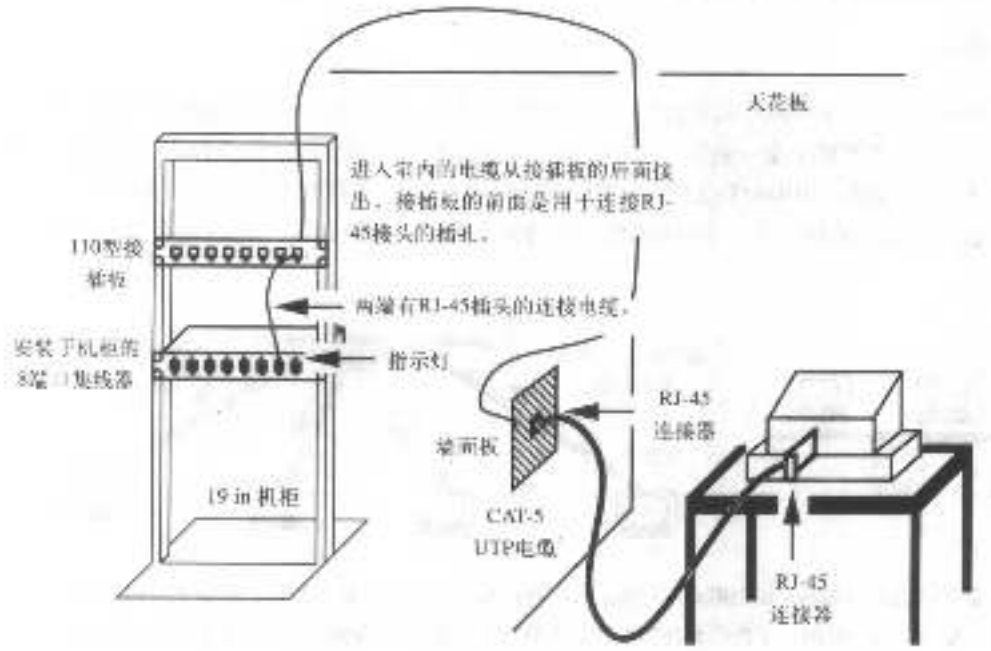


图7-10　10BaseT站点的物理结构。所有的电缆都采用5类线，并用RJ-45插座和接头。其他的PC和站点的连接方式与此相同，都在集线器内终止

从网卡开始，可以看到有一条电缆把网卡连在办公室的墙面板上。从墙面板到机柜所在的机柜室也有一条连接电缆。这条电缆必须要固定好，因为它从墙内和天花板上穿过。最后连接在机柜的接插板上。接插板的类型通常是110或EIA/TIA568。由于这根电缆通常不会被替

换。因此一般都被直接冲压在接插板的后面。

从接插板到集线器用一根跳线连接。集线器和接插板通常被安装在同一个机柜上，当然不在一起也可以，跳线的两端使用的都是RJ-45插头，同时采用类似办公室中的导线容易替换和移动。如果希望将图中的网卡与另一个集线器连接，只需要找到相应的那根跳线，拔出来插到另一个集线器上就可以了。由于在这个图中给出了许多实际布线的中间点，所以看上去比较复杂，只看图7-9所示的简化图也是一样的。

一旦集线器上的所有端口都被插满，我们可能又需要增加新的硬件。这时只要增加集线器，或者将现有的集线器更换成端口较多的集线器。从图7-11中可以看到，使用前面板上的端口所有的集线器都被连在了一起。如果集线器要被连成这种样子，一定要注意在每条传输路径上集线器的数量不能超过4个。这是因为以太网在当初被设计时就规定在两个节点之间中继器不能超过4个。作为中继器的多个集线器必须按相同的规则安装配置。尽管图7-11中共有6个集线器，但是在任意一条传输路径上集线器的数量都不超过4个。举个例子，如果最左端的节点发送了一个数据帧，与这个节点连接的集线器转发这一帧，在这个集线器上连着的节点和它上面的集线器都同样收到了这个数据帧。同时，所有的节点都得到了这一数据帧，但信号走过的每一条路径上，集线器的数目都不超过4个。顺便说一下，只有与数据帧的目的地址相匹配的网卡才能将这个数据帧读进它的缓冲区，其他的的网卡都会忽略这个帧。

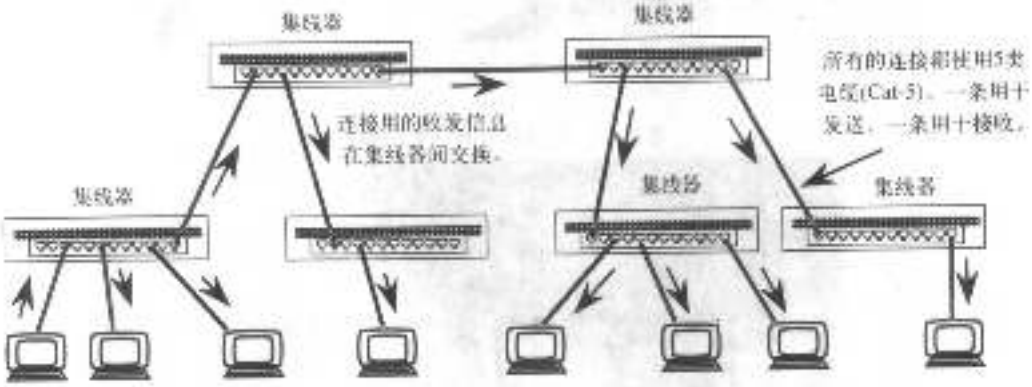
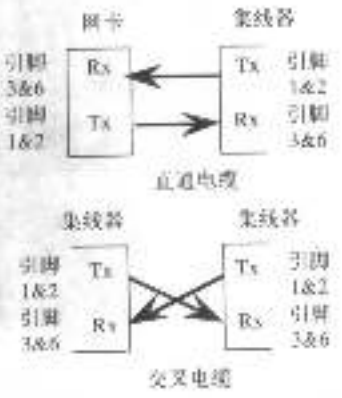


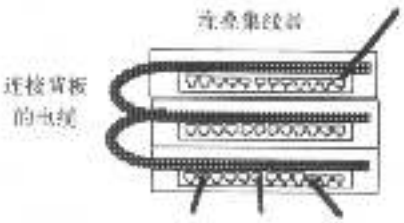
图7-11 最左端节点发送的数据帧被所有的集线器转发。不过，在任意两对节点之间最多只允许有4个中继器存在。记住，在这个传输过程中，其他的网卡都无法成功地发送

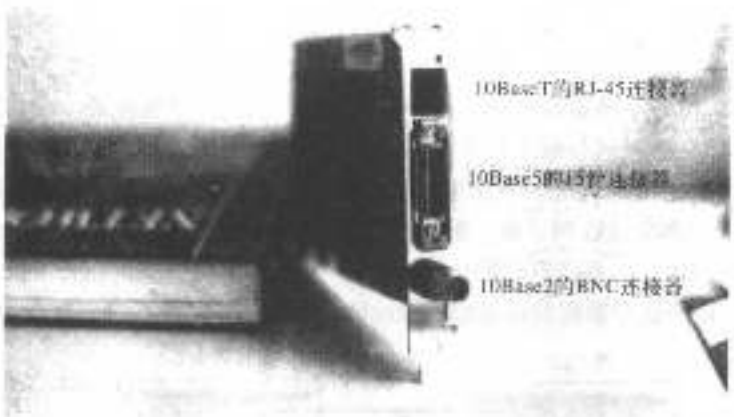
网卡与集线器端口的连接使用直通的电缆。这条电缆中的引脚或者导线必须按顺序排列，这样才能使集线器的发送线对与网卡的接收线对连接起来。在右侧的图中，发送引脚用“Tx”表示，接收引脚用“Rx”表示。但是，如果是两个集线器的两个端口互连时，就要用一条交叉的电缆，以保证发送端和接收端的线对相互匹配。这是因为我们不希望两端都用同一条线发送，或都用同一条线接收。在一些端口上有MDI/MDI-X按钮，利用这些按钮可以使直通电缆的引脚交叉。还有一些集线器有自适应端口，可以自动进行转换。任何情况下，两个集线器的端口直接连接时，都必须交叉线对。出于同样的原因，不用集线器而直接连接两个网卡时，也必须用交叉电缆。



现在一个10BaseT网络上可以连接大量的节点。然而，多

个集线器可以使用一种被称为堆叠集线器的方式集成在一起。参见侧面的图。当集线器叠放在一起时，使用一种被称为堆叠电缆的特殊电缆来连接它们的总线和背板。这种电缆被接在集线器的背面或侧面，而不是通过端口从前面连接。在套用只能使用4个集线器的规则时，一个堆叠集线器被认为是一个集线器。有关10BaseT网络配置的更详细情况请参见照片7-1到7-8。

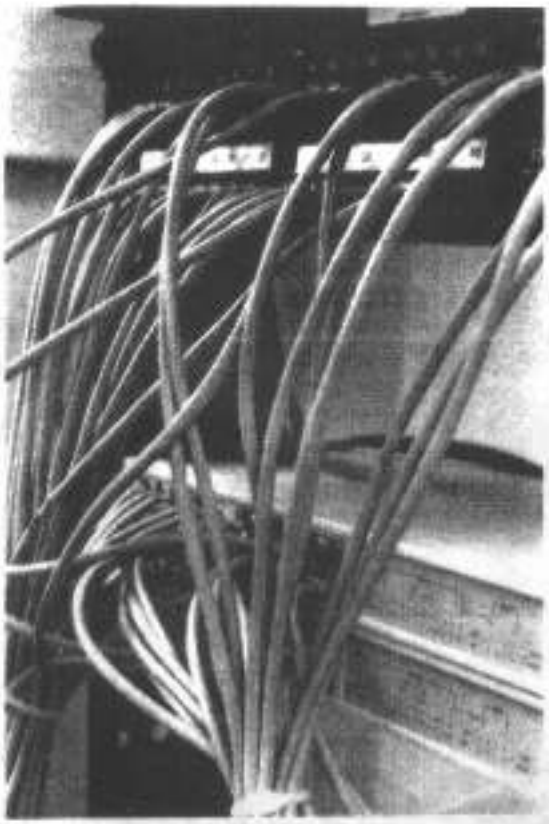




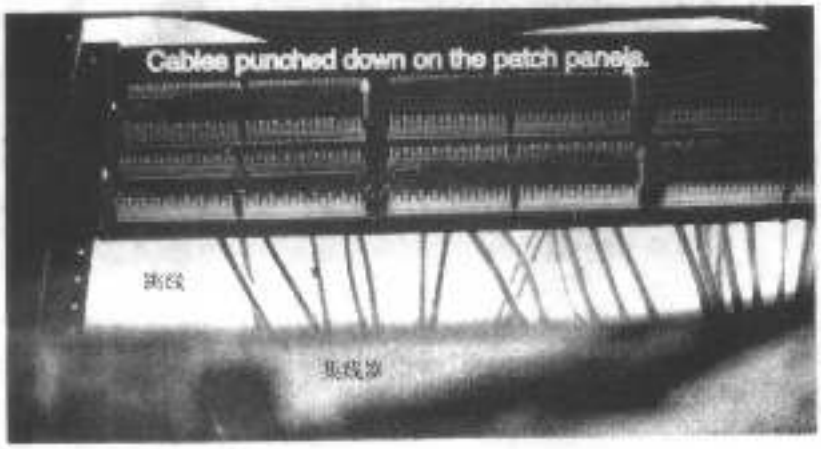
照片7-1　多种接口的以太网网卡



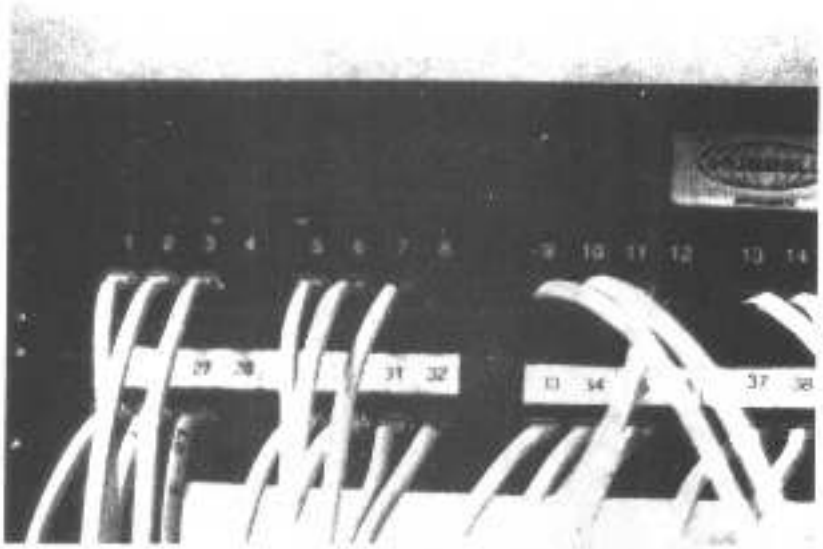
照片7-2　10BaseT配线分配中心的一个实例



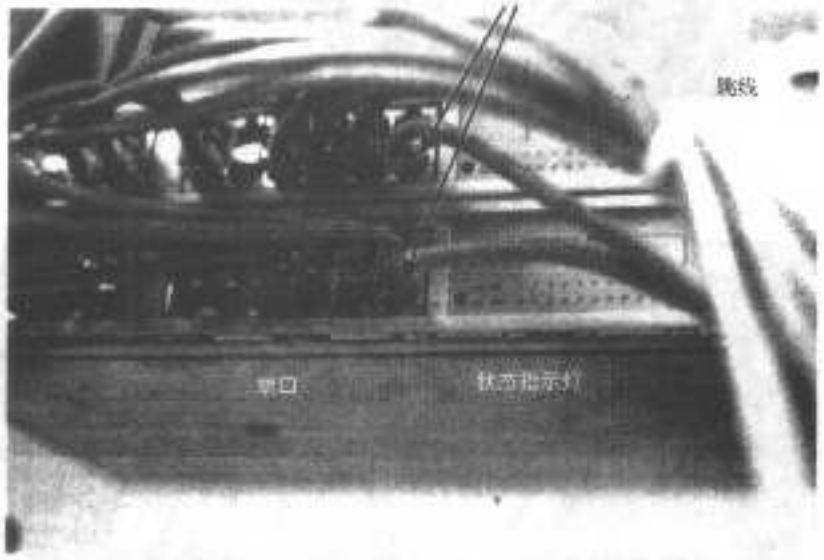
照片7-3 接插板和两个集线器的近距离照片



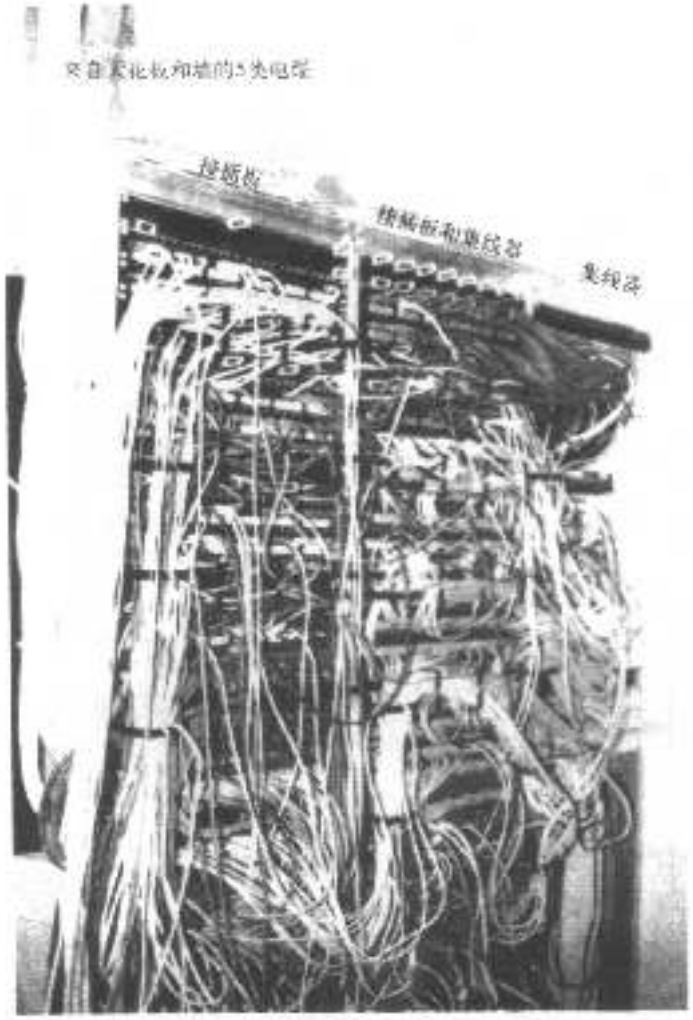
照片7-4 从后面观看接插板



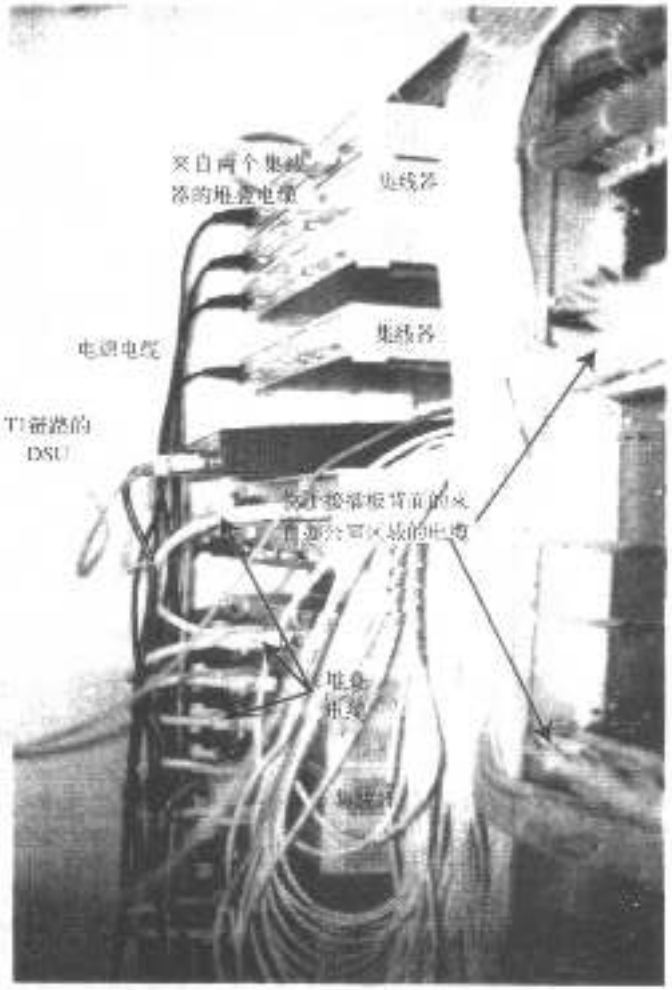
照片7-5 从前面观看接插板



照片7-6 从前面看两个24端口的集线器



照片7-7 10BaseT配线中心的另一个实例。注意这里看到的跳线电缆



照片7-8 从后面看照片7-7中的机柜

7.6 以太网的帧结构

网卡地址：在第3章中已经提到，以太网的网卡有一个48比特的编码硬件地址。通常这个地址被烧在一个ROM芯片中，所以只要所在的节点一接通电源，网卡就可以知道自己的地址。这个地址开始的24比特被称为生产厂商代码，后24比特是序列号。从前面的24比特，我们可以知道生产这个网卡的厂商是哪一家（见右图）。网卡地址还被称为硬件地址、物理地址或者媒体接入控制（MAC，Media Access Control）地址。

以太网地址的厂商代码
以十六进制给出。
前导数字为0。

3Com	6010至6040
3Com	608c
AT&T	3d,55
Cisco	00000c
HP	80009
Intel	00aa00
Motorola	8700至8710
Sun	80005

基本的以太网帧结构：使用前面所说的网络配置，在以太网上传输数据时，所有的比特都要被封装在一个数据帧里。就如同寄信时要把信装在一个信封里一样，数据比特也要根据以太网协议放入恰当的帧中。数据所在的以太网数据帧的具体帧格式如图7-12a所示。在帧的起始处，1、0比特交替出现，其目的是使目的网卡和发送网卡保持同步。这个字段被称为帧头或前同步码，在图7-12a中没有画出来。在前同步码之后，是这一帧要到达的目的网卡地址，这个目的地址是由发送网卡加上去的；紧接着是发送网卡的NIC地址。正如我们所看到的，这两个地址都是48比特（即6字节）。再往后是类型字段，用来指出被封装数据所采用的协议。如果类型字段是0800（十六进制），表示这个帧携带的是IP信息；如果类型字段是8136或8137，表示信息字段携带的是NetWare业务。借助这个方法，一个局域网上可以承载多种不同的协议，而它们的数据不会被混淆。

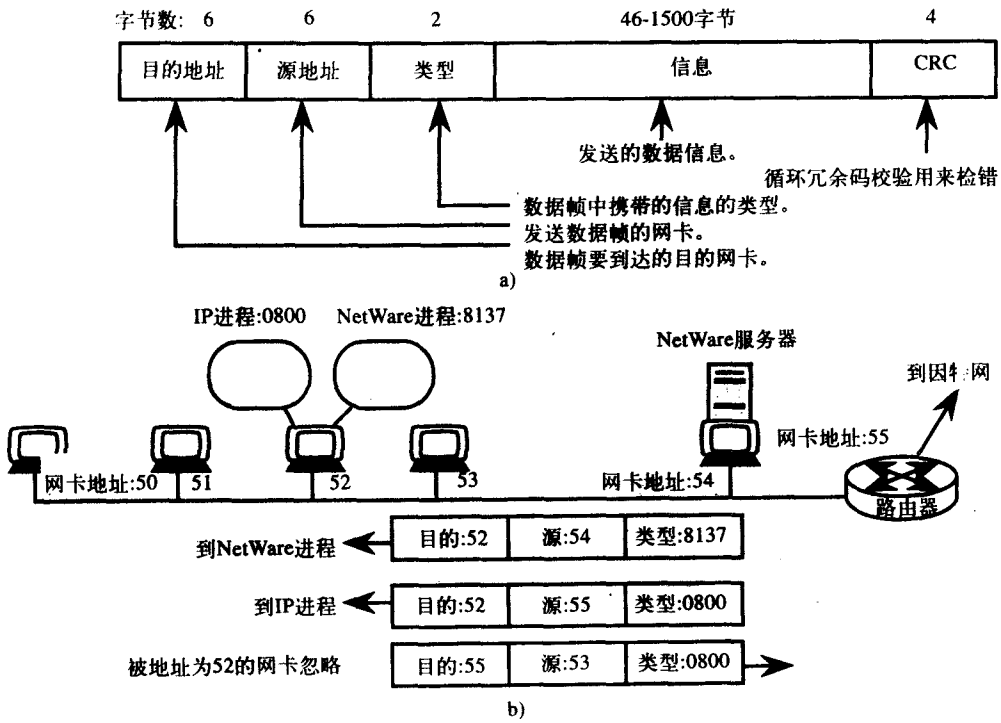


图7-12　a) 以太网帧的基本结构。b) 网卡地址被简化显示。地址是52的网卡将接收前面的两帧，因为目的地址指向它。第一帧的类型字段与NetWare程序匹配，因此被转给它。第二帧被转发给IP程序，最后一帧会被52号网卡忽略

信息字段是数据被放置的字段，而循环冗余校验（CRC，Cyclic Redundancy Check）字段是发送网卡设置的校验码，以使接收网卡能通过其来检查接收到的帧是否有错。如果由于出现错误，接收网卡就会丢弃这一帧。现在你可能很想知道：正在等待响应的程序发生了什么？如果由于出现错误，某些帧被网卡丢弃，这些程序又如何正常地工作呢？为什么这个网卡不请求重发呢？是这样的，假设一个程序正在等待网卡已经成功地传输了数据帧的响应，如果等待的时间过长，这个程序本身就会请求重发。可以这样设想，当网卡丢弃了一帧之后就会对它自己说，“如果我的程序需要哪个被丢弃的帧，它自己就会请求重发。”

类型字段：现在利用图7-12b，举一个例子来说明地址和类型字段的作用。图中局域网网卡的地址是从51到55。当然，网卡的地址应该是6个字节长，但是在这里对它们进行了简化。在这个局域网上运行着两个协议。有一个NetWare服务器与本地设备进行通信，使用的是NetWare协议。另外还有一个路由器，使局域网可以访问Internet（因特网）。这个路由器与局域网客户之间使用的是IP协议。

网卡地址为52的PC打开了两个窗口。一个窗口运行着与NetWare服务器进行通信的应用。另一个窗口运行着Netscape，用IP分组通过路由器与Internet进行通信。图7-12b显示有三个以太网的数据帧到达了52号网卡。为了简单起见，只画出了三个字段，信息字段和CRC字段没有被画出。第一帧来自54号网卡，它的类型字段是8137，对应着NetWare协议。由于目的地址52与自己的硬件地址相匹配，52号网卡把这一帧拷贝到自己的缓冲区中。然后对其进行误差校验，如果有错，就简单地把它扔掉。假设这一帧没有错误，PC就开始检查它的类型字段，然后将所包含的信息或者说这一帧的数据部分发送给Netware程序。根据接收到的数据，这个程序会进一步确定做什么。

第二帧也是指向52号网卡的，所以52号网卡将这一帧也复制在自己的缓冲器中，经误差校验后，将这一帧发送给正在运行NetScape的IP程序。最后一帧目的地址不是52，所以52号网卡忽略这一帧。用这样的方法，在一个局域网上就可以运行许多不同的协议。我们甚至可以把Macintosh和PC连接在同一个局域网上，并利用类型字段识别这个帧属于哪一个程序等等。如果发生碰撞，网卡将重发传送失败的那些帧。

7.7 扩展局域网的范围

OSI层		设备	传输单元
3.	网络层	路由器	数据分组
2.	数据链路层	网桥	数据帧
1.	物理层	中继器	比特流

标准以太网的范围是500m，而10Base2的范围只有185m。以太网和局域网的各段的互连有什么不同的方法吗？各种方法被列在侧面的图中。中继器是最简单的解决方法，它工作在OSI参考模型的物理层。这意味着在中继器上只能处理比特。它并不介意比特是如何被放在帧里或者是数据里。从中继器一端读入的比特等于放在另一端的输出比特。

网桥稍复杂一些，但是不像路由器那样复杂。网桥工作在第二层，它从其到达端口读入比特，并将这些比特组织成字节和字段，然后再把这些字段集成为一个完整的帧。同时，它还从这些帧中读取NIC（网卡）地址或MAC地址，并决定如何处理每个帧。路由器需要知道网络层地址，典型的就是IP地址。路由器根据IP地址做决定。

7.7.1 中继器

扩展范围的最简单的解决方案是用中继器连接更多的以太网段。对于存在较多网段的网

络，可以加入更多的节点。图7-13是用四个中继器连接的五个网段。根据标准规范，使用5-4-3规则不可以连接4个以上的中继器。5-4-3规则指出，使用4个中继器，网段最多不能超过5个，但其中只有3个网段可以连接节点。也就是说，在两个网段上不能有任何节点。不同建筑物或不同楼层间的局域网网段互连使用这个规则。5-4-3规则只是一个通用的规则，但是在局域网中成功地连接更多的中继器和更多的网段也是可能的。

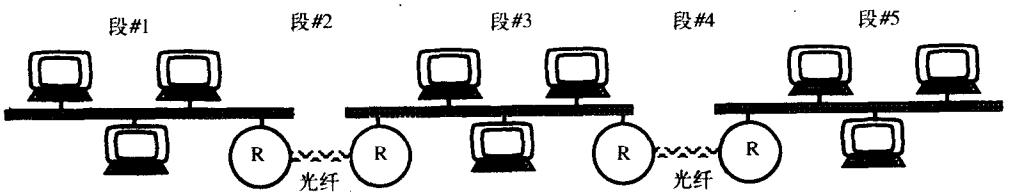


图7-13　5-4-3规则。五个网段使用四个中继器连接，其中只有三个网段可以连接节点。基于光纤的网段用于延长传输距离

使用中继器连接更多的网段可以扩展局域网的范围。举例来说，如果图7-13中的五个网段都是10Base5网段，每一个网段的最大距离是500m，那么这种配置获得的总距离是2500m。这不仅仅让我们把局域网的范围从500m扩展到2500m，同时还使我们可以在局域网上加入更多的节点。每个网段都有一个允许的最大附着节点数。对于10Base5，每个网段所允许的最大节点数是100个，所以图7-13中的配置能为300个节点提供服务。根据5-4-3规则，另外两个网段上不允许有节点。

下面要使用中继器互连多个网段，以便能为更多的节点提供服务。但是所有的节点都必须共享同一条通信信道。假设大多数节点在大部分时间内都是空闲的，或者说不与网络上的其他节点进行通信，而是在各自的PC上进行一些本地处理，那么可以证明在这种情况下增加节点是可行的。如果假设局域网上的节点只是偶尔地互传一些数据分组，那么它们之间共享同一条通信信道就不是一个性能问题。

如果在局域网上各节点相互之间有大量的业务，不论是一个网段，还是五个网段，都会持续地出现碰撞。当前的业务量越大，碰撞的可能性就越大。随着碰撞的增加，局域网的性能就会下降。图7-13中五个网段上的所有节点都处在同一个**冲突域**。冲突域是局域网网段的集合，在这个集合上所有的节点都必须共享同一条通信信道。例如，在7-13图中一个节点正在发送信息时，其他的节点就不能成功地发送。否则的话，就会出现碰撞。

总之，对于扩展局域网范围、增加节点数量来说中继器是一个比较好的解决方案。它们安装容易，不需要任何技巧。同时设备简单，工作在OSI模型的物理层，并且只是将一端出现的电信号转发到另一端，所以速度快且经济。

7.7.2　网桥

在图7-14中，用网桥代替了中继器。网桥工作在OSI模型的数据链路层，所以它不是简单地把一个端口的比特转发到另一端，而是根据MAC地址来决定是否转发这一帧。在做出决定之前，网桥要先读入数据链路层上帧内的NIC地址或MAC地址。因此，中继器是转发比特，而网桥则是转发帧。如果一个网桥决定让一帧通过，从一个网段到另一个网段，则被称为**转发**；如果网桥不让一个帧通过以便到达相邻的网段，则被称为**过滤**。由于网桥比中继器更智能，因此在局域网上就可以同时存在几条通信信道。在图7-14中，有三个可能的通信信道。

在局域网环境中的每一个通信信道都被称为一个**冲突域**。因为在不同的信道上，存在着不同的碰撞。

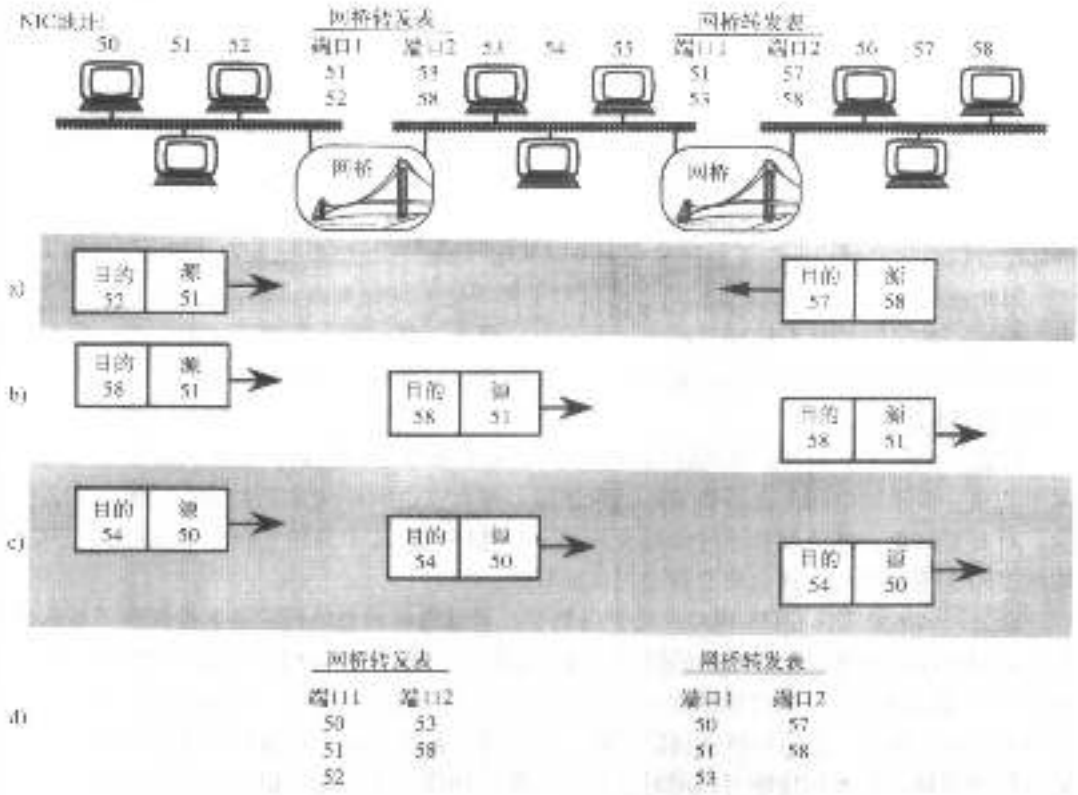


图7-14 a) 使用网桥，51号网卡可以与58网卡同时发送。网桥通过查表可以知道它们工作的网段，可以滤除发往其他网段的数据帧。b) 需要时，51号网卡也可以向另外一个网段上的节点发送。c) 利用源地址，网桥可以更新转发表。d) 更新后的转发表

例如在图7-14a中可以看到在最左端，MAC地址为51的网卡正在向同一网段上的52号网卡发送信息。与此同时还存在一个传输，另一网段上的58号网卡也正在向57号网卡发送信息。在这个例子中，在两个不同的网段上，同时存在两条通信信道，每一条通信信道对应着不同的冲突域。那么，为了避免碰撞并成功地传输，网桥是如何知道应该过滤哪些数据帧，并且不把它们转发给局域网另一个网段上的其他人的呢？

每个网桥都维护一个**转发表**。这个表给出了网卡地址与端口的对应关系。例如，左边的网桥知道52号网卡在它的1号端口上。这样当这个网桥接收到发给52号网卡的一个帧时，就知道不必把这个帧转发到端口2、然后再过渡到中间网段，所以就把这帧过滤掉。类似地，右边的网桥通过转发表了解到57号网卡在它的2端口一侧，因此也没必要转发那一帧。

然而，在图7-14b中，当51号网卡向58号网卡发送数据时，左边的网桥从转发表了解到58号网卡在它的2端口上，因此就转发这一帧。这个网桥只要知道58号网卡在它右侧的某个地方就足够了，而不必知道它是否与右边那个网段直接相连。事实上，58号网卡不是直接附着在中间网段上，所以右边的网桥在得到指向58号网卡的这一帧时，也将其转发到它右边的网段上。右边网桥也是根据转发表做出决定的。在整个过程中没有其他帧能够发送成功，因为传

送这一帧经过了所有的三个网段。

网桥是如何建立转发表的呢？利用这些转发表，它们可以确定哪些数据帧被转发，哪些数据帧被滤除。利用每个网段上传输的数据帧内的**网卡源地址**可以建立这些转发表。例如在图7-14c中，可以看到50号网卡正在向54号网卡发送信息。收到这一帧的网桥发现，在它的转发表中找不到54号地址。这样，每个网桥都会把这一帧转发给下一网段，希望在沿线的某个地方网卡54会接收到这一帧。注意到，右侧网桥没有意识到它不必再把这一帧转发给更右侧的网段，它还是继续做，这被叫做**扩散**（flooding）。扩散是一个过程，在这个过程中由于网桥不知道一个帧的目的地在哪里，于是就转发这一帧穿过许多网段。在这个传输中，两个网桥都没有找到54号网卡的位置，但是它们可以从这一帧的源地址中知道50号网卡的位置。

因此在图7-14d中，可以看到两个网桥都更新了它们的转发表，都在端口1加上了50号网卡。现在，如果54号网卡给50号网卡（或其他的网卡，都一样）发送了一个应答，那么每个网桥都会将54号网卡加在相应的端口上。也就是说，54号网卡会被加在左边网桥的端口2上、右边网桥的端口1上。

转发表中的某个条目如果长时间不被使用，就会被删除。例如，假设从来没有发往52号网卡的帧，或者这个网卡也不曾发送过数据帧，那么左边网桥转发表中的相应条目就会被删除。有必要的话，这个条目还可以再次被加上。维持条数最少的转发表，不但可以占用较少的网桥RAM存储空间，还会使查找过程更加有效。

总之，网桥是工作在OSI模型的数据链路层，这就意味着它处理的是数据帧而不是单个的比特。网桥使局域网的业务更加局部化。假设图7-14中每一个网段都代表了一个不同的部门，在每一个部门内都有大量的数据业务；但是在部门之间业务量很小，比如说大约只占全部业务量的20%。那么，使用网桥就可以提供一个较好的解决方案。用网桥连接各网段可以创建额外的冲突域，较多的传输可以同时进行——每个网段一个传输。但是，网桥需要比中继器做更多的处理工作，所以它们的速度较慢，价格也较贵，但维护和安装同样不需要那么多技巧。表7-4给出了中继器和网桥的比较。

表7-4　中继器和网桥的比较

	中 继 器	网　桥
运行在OSI模型的哪一层？	物理层	数据链路层
传送什么？	比特	数据帧
向其他网段转发哪些帧？	所有的帧	需要的帧
转发广播帧吗？	是	是
转发出错的帧吗？	是	否
能够连接不同的局域网（包括FDDI）吗？	否	是
能够连接不同速率（包括100Mbps）的网吗？	否	是
能生成更多的信道和冲突域吗？	否	是
哪一个更快？	这一个	—
哪一个连接和配置更容易？	这一个	—
哪一个用于回路环中，可提供链路连接冗余？	—	这一个

7.7.3　路由器

纽约市邮局的邮递员知道或者关心旧金山的某条街道在哪里吗？当然不会，他们只需要知道纽约市各条街道是如何分布的就可以了。当他们拿到一封要发往旧金山某个特殊街道的

信时，他们首先会把这封信寄交给旧金山邮局的邮递员。当然了，旧金山邮局的邮递员知道这条街道在哪儿，什么人住那儿。如果整个世界只是由居住在一个城市内的少数人组成，那么我们就不需要像今天这样的复杂邮政系统了。

同样的道理，当一个局域网的范围扩大时，只有网桥是不够的。如果局域网中只有网桥，就如同是纽约的邮递员必须知道旧金山的所有街道在哪儿一样。与让所有邮局了解世界上所有的街道布局相比，只让邮局了解自己所在城市的街道布局更容易实现和管理。

这就是为什么局域网中还需要路由器的原因。回去看图7-14c，当一个帧被发往50号网卡时，网桥不知道它在哪里，那么这帧就会被扩散到整个局域网和所有的网段上。如果局域网的范围很小的话，这种扩散不会导致那么多的网络需求。但是如果局域网的范围很大，我们就需要采取措施使扩散局部化。路由器帮助我们做到了这一点。广播是另一种现象，可以使局域网内的所有网卡都读到一个帧，并尽可能做出响应，这一点要在第8章中讲到。网桥无法使广播信息局部化，但路由器可以。

网络上的每一个节点都有一个NIC地址，或者叫MAC地址、硬件地址、物理地址、以太网地址。除了这个地址外，每个节点还被分配了一个IP地址，被保存在此节点的某个配置文件中。当节点被启动时，就会读到这个文档，并且能够知道存储在那个文件中的IP地址。另一方面，NIC地址或MAC地址是被烧在网卡内，只能通过替换网卡而改变。表7-5中总结了这两种地址的不同。第8章，我们将更多地讨论这些地址。

表7-5 MAC地址与IP地址的比较

	MAC	IP
与OSI模型的哪一层相关?	第二层	第三层
是哪一种类型的地址?	物理的	逻辑的
这种地址用在哪里?	网桥	路由器
占用多少比特?	48	32
采用几进制?	十六进制	点分十进制
举一个地址的例子	00:aa:00:52:3f:e4	129.117.202.178
地址是如何构造的?	不分层的	分层的
这种地址和谁有关?	网卡生产厂商	机构
替换网卡，地址会改变吗?	会	不会
地址被存储在哪里?	网卡的ROM	配置文件

图7-15a中给出了当一个IP分组需要通过局域网传输时，是如何被封装在一个以太网帧内的。这个IP包包括这个包最终到达的目的地址，而网卡地址被放在帧头中，给出了下一跳的目的地址。

图7-15b给出了三个路由器，可以将每个路由器想像成属于一个特定城市的邮局。每个路由器只了解它所连接的局域网的布局。例如，路由器1只知道局域网1和局域网2上所有节点的网卡地址，或者说这些网卡只能被路由器1找到。类似地，路由器3只知道局域网3上的网卡地址。路由器2是为其他路由器服务的，没有局域网与它连接。

当局域网1上的一台PC向地址129.117.300.21发送一个IP包时，这个PC很清楚，IP地址以129.117.100开头的所有PC肯定和它一样连接在局域网1上，而以129.117.300开头的地址应该在其他的地方。因此，发送这个包就变成了它的默认路由器（即1号路由器）的任务。换句话说，这个包正在“出城”。因此，这台PC先将这个包放在一个以太网帧里，并指向路由器1的网卡地址（52号网卡）。注意，这个网卡并不知道局域网3上的最终PC的网卡的地址。

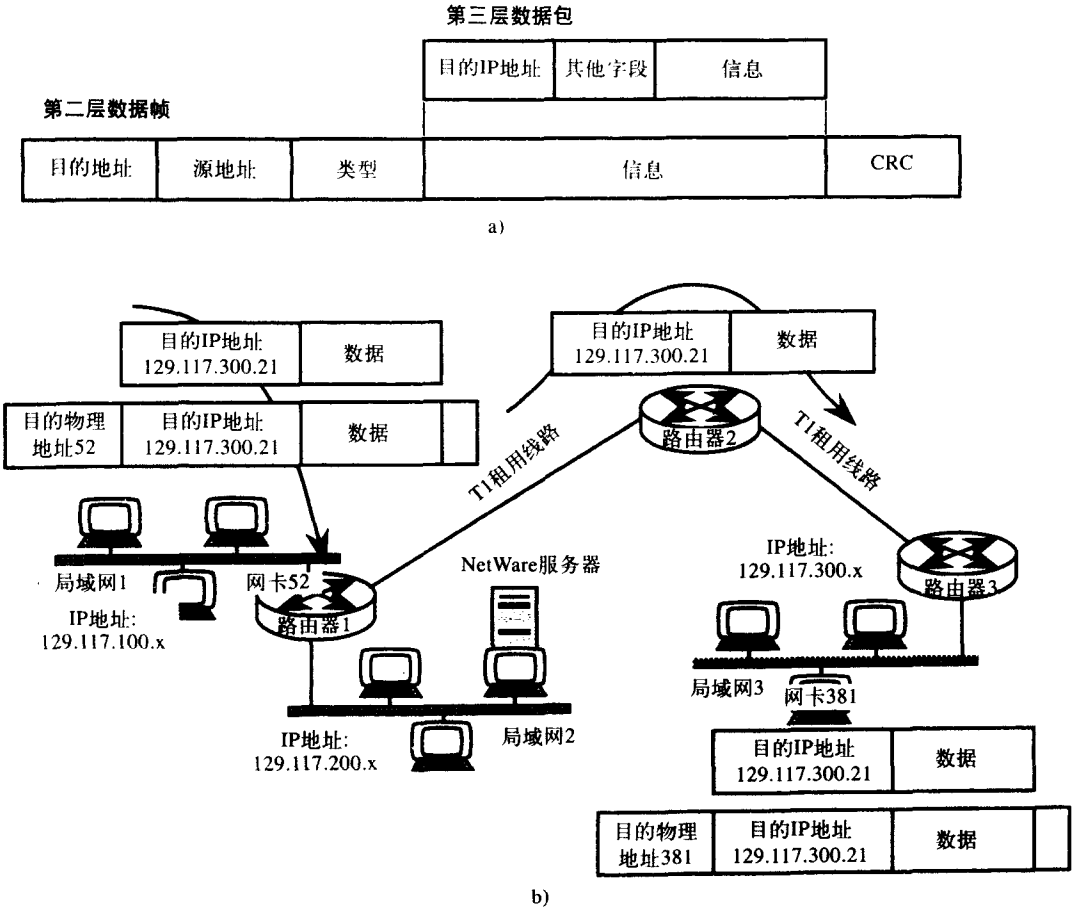


图7-15　a) 一个OSI模型第三层的数据包被放在了第二层的数据帧中；b) 一个数据包的通过路径，从局域网1上的一个节点到局域网3上的一个节点

路由器1首先查看自己的路由表，决定把这个包通过T1链路发送给路由器2。这个包被封装在T1帧内（没有给出）传送给路由器2，路由器2又将其转发给路由器3。路由器2知道所有以129.117.300开头的地址在路由器3的管辖范围内。因此，路由器3就把这个包装载在另一个以太网帧内，直接传送给网卡381。在这三个路由器中，只有路由器3需要知道IP地址129.117.300.21被分配给了网卡为381的PC。用这种方式，路由器就可以在它们之间有效地路由IP包，而不需要知道所有节点的详尽信息。例如，路由器2就不需要知道任何一个网卡地址，它的主要功能是为其他的路由器转发数据包。

从图7-15b中可以看出MAC地址只是一个物理地址，不能标识网卡的物理位置。MAC地址为52的网卡可能在局域网1上，而地址为53的网卡却可能在局域网3上或其他的某个地方。然而，与MAC地址是物理地址相对应，IP地址是逻辑地址。如果你用其他的PC和网卡来替换网卡号为381的PC，新的PC仍然会被分给相同的IP地址，只是MAC地址不同而已。IP地址是分等级的，这样可以使地址之间的路由更容易。

路由器是比网桥更为复杂的设备，它能够选择路径。可选的路径都被列在一个矩阵表中，给出了每条路径的可靠性、安全性、开销或速度。路由器还可以提供防火墙的功能，可以决

定哪些包可以进入与之相连的局域网网段，而哪些包不允许进入，这要根据很多不同的参数进行判断。现在的路由器还能优化业务，并保证服务质量（QoS，Quality of Service）。为了在被路由的网络中传送话音，这是非常必要的。对于以上提到的这些功能，网桥根本无法实现。表7-6是路由器和网桥的对比总结。

表7-6 路由器和网桥的比较

	路 由 器	网 桥
OSI模型的哪一层做决定?	第三层	第二层
基于什么地址做决定?	典型的是IP	MAC
典型的用于哪种范围的网络?	大范围的	小范围的
相关的造价如何?	高	低
处理速度如何?	低	高
配置它需要的技巧如何?	高级的	一般的
有多条可选路径吗?	多条	很少
业务需要的额外开销多吗?	少	多
安全性如何?	好	差

7.7.4 交换机

交换机产生的原因：路由器也有自身的缺陷。其中之一是造价高而且需要专门的技术人员进行维护。对于以太局域网，所有的节点都共享可用的带宽，但随着网络需求的大量增加，对带宽的需求也显著增加。例如，一个有15个节点的以太网网段，每个节点平均只能分到大约0.3Mbps的带宽，相对于以太网的10Mbps可用带宽，这只是很小的一部分。这个数字是由以下假设得到的近似值：由于以太网上使用的是CSMA/CD访问协议，或者说存在一定数量的碰撞，因此有效利用率被认为是45%，这就使有效带宽下降到了4.5Mbps。对于共享这个带宽的15个节点而言，每个节点的平均带宽就只有0.3Mbps，即300kbps。如果需要再往网络里添加一些节点，不仅瓜分这4.5Mbps带宽的用户数量增多，而且由于冲突增加，这4.5Mbps的有效带宽会进一步减小。

一个网络管理人员在各节点之间安装路由器之前，通常会首先安装一种被称为交换机的第二层设备。这样不用做太多工作且花费很小，就可以使网络性能有所提高。图7-16给出了这样一种网络。在这里，有一个带6个端口的交换机，根据每个节点所需的带宽和它们通常需要与哪些节点进行通信，来决定局域网的分段。例如，上面的两个节点需要大量的带宽，所以它们就直接与交换机的端口相连接。这样每个节点都可以得到10Mbps的带宽。

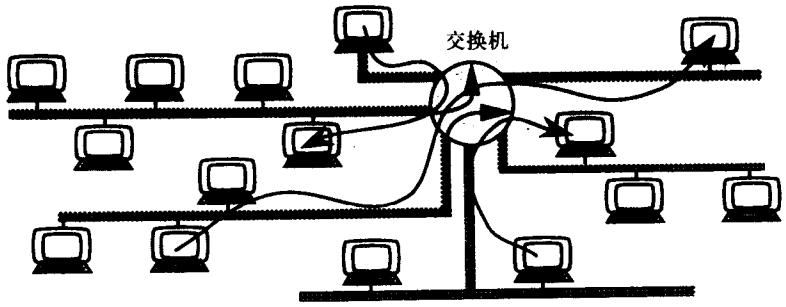


图7-16 这里给出了一个第二层交换机，正在同时与三个不同的节点或网卡进行通信

与原来只有一条通信信道存在不同，现在在任意给定的时刻里最多可以有6条信道同时存在。当相同网段或者相同端口上的节点都在相互通信时，可以有6条信道。图7-16中最顶端的两个节点也能与交换机进行通信，但交换机的缓冲区只能保存有限数量的帧。

这样总的带宽就从10Mbps增加到了60Mbps。而且，由于每个网段上参与带宽竞争的节点减少了，冲突也就减少了，这样就增加了整个网络的有效性。假设整个网络的效率提高到75%，总共的带宽就变成45Mbps，每个节点可平均分得3Mbps。这个数量是加装交换机之前的10倍，难怪交换机很快就流行开来，用以克服网络业务增加带来的影响。

回想以前的住宅用户们在电话电路上采用合用线的那些日子。与我们今天使用的专用线相比，这种类型的服务费用较低。对于合用线，如果你想打一个电话，就得先看看你的邻居们有没有占用这条线路。如果有的话，你只能先挂机，过一会儿再打。当专用电话线的速率提高到一定程度时，每个居民用户都可以使用自己的专用电话线了，再打电话时就不需要再等待了。在以太网上安装一个交换机也是基于同样的道理。一些节点可以直接连在交换机的端口上，允许它们使用10Mbps的带宽而不会发生碰撞。

交换机的工作过程：在图7-16中，有三个节点同时与其他三个网段上的节点进行通信。交换机的构造，或者说实现交换的电子学技术，允许在交换机中同时存在几条帧信道。交换机内部带宽的大小叫做**底板速率**（backplane speed）。这个速率决定了可以同时交换多少帧和任一时刻到达帧所遭遇的阻塞量。

当然，对于从两个网段发往第三个网段内节点的那些帧，交换机不会同时转发。如果两个帧竞争交换机的同一个输出端口，其中一个帧要么被阻塞（或丢弃），要么被临时存储在缓冲区中直到那个端口空闲为止。在这种情况下，也至少会有一个帧被传送到正确的网段上。

一帧到达某个端口时，交换机会先查看它的目的MAC地址，然后将其转发给目的地址所在的端口。除非交换机不知道这个MAC地址，或者在它的转发表中没有这个MAC地址，否则其他的所有端口都不会收到这一帧。在交换机不知道某个帧的MAC地址的情况下，这一帧就会被扩散到所有的端口，希望目的地址在其中的一个端口上。

这样看起来不是有点像网桥吗？是的，本质上交换机就是一个现代的高级网桥。网桥能做的，交换机能做，而且做得更多。但是，生产厂商仅仅对网桥进行了升级，增加了一些性能，然后称之为第二层交换机！这是一种市场策略。因此，昨天的网桥就变成了今天的第二层交换机。从表7-7中可以看到这两种设备的基本不同之处。

表7-7　网桥与第二层交换机的比较

	网　桥	交 换 机
依赖于什么来决定转发和过滤？	软件	硬件
用什么设备做出决定？	RISC CPU	ASIC
一般有几个可用端口？	两个	很多
每个端口的相关造价如何？	高	低
速率如何？	慢	快
一次能够转发几个帧？	一个	很多
传送时能使用存储转发方式吗？	能	能
传送时能够采用直通方式吗？	不能	能

网桥基本上是由软件程序驱动，需要一个处理器，如RISC处理器来执行命令。而交换机被制造出来时，在专用集成电路（ASIC，Application Specific Integrated Circuits）芯片中就

已经实现了所有的软件功能。在第1章中已经深入讨论了ASIC技术。在交换机中，转发决定不是由软件来完成的，而是由ASIC芯片中的硬件逻辑电路实现的。与基于软件做决定相比，这样做不仅提高了运行速度，造价也较低，且每个单元需要的空间也较小。基于硬件交换的缺点是，无法升级新的软件。因此，生产厂商用硬件来实现大部分逻辑功能，用软件来实现一部分逻辑功能，当然这部分功能是可以被更新的。

交换机比网桥运行速度更快的另一个原因是它们可以同时转发几个帧。例如，如果用网桥代替图7-16中的交换机，那么图中的那三个帧就不得不被顺序转发。

交换机和网桥的每个端口都需要有一些缓冲区，来临时性地存放需要这个端口转发的帧，直到这些帧的目的端口空闲，或者可用。网桥采用存储转发方式来传送数据帧，而交换机不但可以使用存储转发方式，还可以采用直通转发方式。这两种方式在图7-17中都有体现。在存储转发方式中，设备接收整个帧，包括帧尾的帧校验序列（FCS，Frame Check Sequence）码。利用这个字段，设备对帧进行错误校验，只要没有错误，就把它转发给相应的端口。这个方法的另一个优点是它不需要所有的端口以同样的速率（均是10Mbps或均是100Mbps）运行。

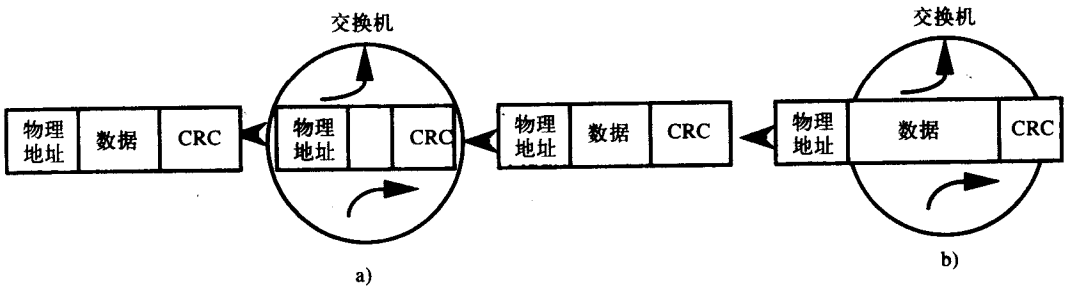


图7-17 a) 存储转发方式，b) 直通方式

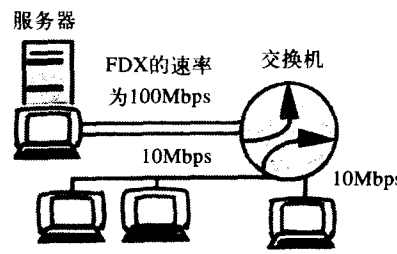
在直通转发方式中，交换机一读到目的MAC地址就开始转发这一帧。因此，当这一帧正被接收时，它的前面一部分就已经被转发给了相应的端口，当然要假设这个MAC地址没有错误。然而，缓冲区没有接收到完成的一个帧，是无法进行验证的。可以采用一个折衷方案，即如果这个网络容易出错，就采用存储转发方式。否则，采用直通转发方式，因为当所有的端口以同样速率运行时，直通方式的速率会更快一些。

如果用交换机来代替10BaseT的集线器，还有一些好处。使用集线器，如果一个节点发现了许多错误帧，所有的节点都会受到影响而使性能下降。但利用存储转发方式的交换机，就可以删除从网络中发过来的那些垃圾帧。与集线器把每个帧都转发给所有端口相比，交换机比10BaseT集线器的安全性更高，因为交换机只是向一个端口转发数据帧。

基本上，交换机的性能由4个特性决定，在购买时需要考虑，它们分别是端口处理速率、底板容量、帧转发方式以及转发表和端口缓冲区的存储容量。一个底板速率是40Mbps的10BaseT交换机，在任意时刻只能交换4个端口。然而10Mbps和100Mbps的交换机就能实现不阻塞。如果转发表的RAM的容量不够，只能更经常地删除表中的条目，迫使交换机必须不断地“学习”新地址。当交换机既有10Mbps的端口又有100Mbps的端口时，就需要更大的缓冲区，因为从100Mbps端口出来的数据的速率要大于10Mbps端口的接收速率。

交换机之后是什么？ 在图7-16中，最顶端的两个节点各拥有一个专用的交换机端口，因为它们产生的业务量比其他的节点大。然而如果它们是服务器，就还必须与其他节点经常保

持通信，这样它们的10Mbps的链路就变成了瓶颈。也就是说，如果有几个10Mbps的节点同时点击服务器，交换机只能以同样的速率传送给服务器，这样交换机的缓冲区很快就会被填满。现在有一些协议，使交换机能够实现流量控制，避免缓冲区溢出。但是如果让通向服务器的“管道”速率比其他网段的运行速率高很多，就可以较好地解决这个问题。



因此，在侧图中一个服务器运行速率为100Mbps，而其他几个节点的运行速率为10Mbps。这样，服务器网段高出10倍的容量完全能够处理来自各网段的业务。以100Mbps速率运行的以太网被称为高速以太网（FE，Fast Ethernet），而运行速率能达到1Gbps的以太网被称为千兆（GE，Gigabit Ethernet）以太网。

如果服务器链路采用全双工式的链接，就可以进一步减轻拥塞问题。这时从交换机到服务器有全双工的连接，服务器可以同时发送和接收。这意味着不需要再使用CSMA/CD协议，因此也不会发生碰撞。一对导线用于发送，另一对导线用于接收，有效速率可达200Mbps。在结束本章之前提醒大家注意，这里只讨论了第二层交换机。而第三层交换机，也就是基于硬件或ASIC的路由器将在第23章中讨论。

习题

7.1 节

1. 最原始的组网是利用简单的3.5寸软盘实现的。描述这种联网方式的是下面哪一项？
   a. snickering　b. sancking　c. sneaker-netting　d. sneaking
2. 电话网使用哪一种访问方式？
   a. CSMA/CD　b.轮询　c.令牌传送　d.拨号
3. 局域网有哪些优点？
4. 局域网有哪些缺点？
5. 访问协议和通信协议有什么不同？与OSI模型的关系如何？

7.2节

6. 广域网中主要采用哪一种拓扑结构？
   a. 星型　b. 环型　c. 网状型　d. 总线型
7. 下面哪一个优点与星型拓扑结构无关？
   a. 没有容易出错的单个节点　b. 易于故障诊断
   c. 易于管理　d. 易于进行流量统计
8. 哪种拓扑结构使相邻节点之间的距离比较长？
9. 哪一种拓扑结构故障诊断最困难？
10. 哪种拓扑结构与电话网使用的住宅电线相同？

7.3节

11. 如果我们在房间中传递一根小棍，而且约定只有拿到小棍的人才能开口讲话。哪种协议与此类似？
    a. CSMA/CD　b. 需求优先　c. 轮询　d. 令牌传送
12. 在CSMA/CD中，两个网卡同时发生传输的情况被称为什么？

a. 轮询 b. 碰撞 c. 载波侦听 d. 多址接入

13. 下面哪一项不是CSMA/CD使用的规则?

a. 发送前侦听 b. 发送后侦听 c. 发送时侦听

d. 如果有人在线就不发送

14. 如果两个网卡使用CSMA/CD同时发送，哪一个网卡首先停止发送：是第一个开始发送的网卡，还是第二个开始发送的网卡?

15. 哪一种访问协议常被用于总线型，哪一种用于环型?

16. 在令牌传送过程中，哪个比特是接收端加上去的，用以表示它已经拷贝到了这些数据?

7.4节

17. 令牌环网使用的集中器被称为什么?

a. 多站点接入单元（MAU） b. 集线器 c. 根 d. 集中器（centralizer）

18. 哪一个是令牌环网的标准?

a. IEEE 802.3 b. IEEE 802.5 c. IEEE 802.6 d. ANSI X3T9.5

19. 哪些类型的局域网采用令牌传送协议?

20. 哪一种类型的局域网适合用于校园内各建筑物之间的互连?

21. 如果在一个令牌环网络中，有10个16Mbps的网卡和20个4Mbps的网卡，那么这个局域网的运行速率是多少?

22. 哪种拓扑结构允许FDDI更容易地从故障中恢复?

7.5节

对于紧接着的五个问题，请从下面这些选项中选择正确的答案:

a. 10Base5 b. 10Base2 c. 10BaseT d. 以上三个

23. 哪种类型的以太网使用与网卡分离的收发器?

24. 哪种类型的以太网提供最长距离的网段?

25. 哪种类型的以太网提供最好的管理?

26. 哪种类型的以太网只用总线而不需要引出电缆?

27. 哪种类型的以太网采用CSMA/CD?

28. 从10Base5到10Base2，获得了什么优点和缺点?

29. 从10Base2到10BaseT，获得了什么优点和缺点?

30. 使用直通线、交叉线和堆叠电缆的目的是什么?

7.6 节

31. 以太网卡的地址需要多少比特?

a. 10 b. 24 c. 32 d. 48

32. 当一个网卡接收到一个数据帧时，这个网卡利用下面哪一项内容来判断这个帧是不是发给它的?

a. MAC地址 b. 类型字段 c. 数据字段 d. CRC字段

33. 对于上面的四个选项，请解释以太网数据帧采用每个字段的目的。

34. 在以太局域网中能同时运行NetWare和WindowsNT软件吗?

7.7节

对于紧接着的六个问题，请从下面的这些选项中选择正确的答案:

a. 中继器　　b. 网桥　　c. 交换器　　d. 路由器

35. 10BaseT上的集线器更像哪一个设备？
36. 哪一种设备工作在OSI模型的网络层？
37. 哪一种设备不对帧进行校验就直接让其通过？
38. 当局域网变得越来越大时，哪一种设备是必需的？
39. 哪一种设备是网桥的现代版本？
40. 哪种设备对分组进行处理？
41. 在图7-14中，转发表被更新之后，网卡54将向网卡50发送一个应答帧，哪些网桥将转发包，哪些网桥过滤包？依据是什么？
42. 利用网桥向局域网上的所有网段广播一个帧时，这个过程被称为什么？
43. 与网桥相比，中继器的优点是什么？
44. 与网桥相比，交换机的优点是什么？
45. 与网桥相比，路由器的优点和缺点各是什么？

第8章 TCP/IP的基本概念

在第1~3章中，我们已经提到过因特网和它的一组协议（TCP/IP）。本书还提到过TCP/IP协议对于连接在因特网上的主机是很重要的。没有TCP/IP，就没有万维网（WWW）。在本章中我们主要讨论IP协议，同时还研究IP协议与其他协议的关系。由于TCP/IP对今天的网络是那样的重要，因此我们还将在第26章中深入地讨论它。然而，你会发现这里讨论的内容不是前面章节的重复，同时也不会重复后面章节的内容。

在本书的第1版中，还有其他协议并占据了大量的篇幅。但是，现在所有的那些协议都在渐渐地向IP/IP靠拢。这样对于这个领域的初学者来说学习会容易一些。因此在这个版本中，我们可以多花些时间较深入地研究TCP/IP协议。

8.1 计数系统

在本章里我们将涉及不同的计数系统。如果你对不同进制系统以及它们之间的相互转换都比较熟悉，则可以跳过这一节。这样做不会失去连续性。

可能因为我们有10个手指，所以人们比较习惯使用十进制计数系统。然而众所周知，计算机工作于二进制计数系统。这是因为处理二进制数字的电路设计和制造容易，运算速度快，且造价低。因此，我们必须知道这两种计数系统之间是如何转换的。然而，二进制数是由一连串的0和1构成，可能相当长，所以通常采用十六进制数来表示二进制数，这样可以使二进制数的表示变得简洁。因此，我们首先要复习一下不同进制之间的转换方法，这些方法在本章各节中都会用到。

十进制、二进制和十六进制分别使用10个、两个和16个不同的字符来代表不同的数字。这些进制的基数分别是10、2和16。由图8-1a可以看到，因为数字2在二进制中不存在，所以在二进制中1加1的和是10；在图8-1b中，10和1相加是11（即十进制的3）；再有，1和11相加是二进制的100（即十进制的4），这是因为二进制只有两个符号：1和0。

而十六进制需要16个符号，除了0~9这10个数字之外，还借用了英文字母表中的前6个字母来表示数字。当然，可以使用其他的任意6个字母，但是在习惯上这里使用了前6个字母。图8-1b给出了这3种计数系统是如何计数的以及3种不同进制的数是如何相互转换的。

图8-1c解释了一个较大的十进制数是如何计算的。加法计算是按照各位的系数把多个1、10和100等相加，就得到该十进制数的数值。转换到二进制计算时，所做的事情是一样的，所不同的是基数是2而不是10，见图8-1d。因此，也是将1的个数、2的个数和4的个数等相加。由于二进制数只能是“1”或“0”，还有一种更简单的转换方法（在图中没有给出）将在后面介绍。最后在图8-1e中，可以看到将十六进制数转换成十进制数的方法，类似的也就是将1的个数、16的个数和256的个数等累加起来。注意十六进制的“D”对应的是十进制的13，这也可以从图8-1b的转换表中查到。

数的转换：下面介绍一种将二进制数转换成十进制数的简单方法。在图8-2a中，二进制数11010011被转换。首先如图所示，在二进制数各比特位的上方写对应的幂值，然后把不为零的二进制数的幂值相加。在这个例子中，是把幂值128、64、16和2相加。因此，二进制数11010011等于十进制数211。

```
  1
 +1
-----
 10
```

二进制系统

a)

5 3 7　十进制系统

$7(10^0) = 7(1) = 7$

$3(10^1) = 3(10) = 30$

$5(10^2) = 5(100) = 500$

537

c)

十进制	二进制	十六进制
0	0	0
1	1	1
2	10	2
3	11	3
4	100	4
5	101	5
6	110	6
7	111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F
16	10000	10
17	10001	11

b)

1 0 1　二进制系统

$1(2^0) = 1(1) = 1$

$0(2^1) = 0(2) = 0$

$1(2^2) = 1(4) = 4$

5

d)

2 3 D　十六进制系统

$13(16^0) = 13(1) = 13$

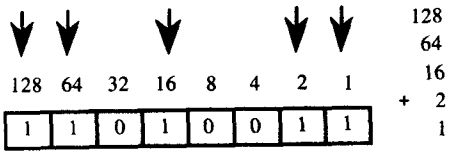
$3(16^1) = 3(16) = 48$

$2(16^2) = 2(256) = 512$

573

e)

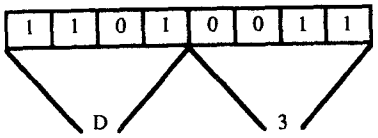
图8-1　a) 在二进制中，1加1得10；b) 3种进制的计数系统之间的转换表；
（c-e）在3种计数系统中，转换的方法是相同的，不同的只是基数



128
64
16
+ 2
1

211

a)

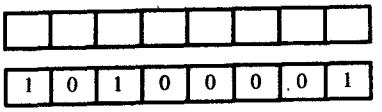


c)

161
- 128

33
- 32

1



b)

图8-2　a) 当将“11010011”转换成十进制数时，只需简单地将“1”所出现位置的2的各次幂相加。
b) 将“161”转换成二进制数时，从2的最高次幂开始，逐步减去它们所对应的2的各次幂。
c) 从二进制转换到十六进制，通常以4个比特为1组

在图8-2b中，要把十进制数161转换成二进制数。将十进制数转换成二进制数时，首先需

要找到可以从这个十进制数中减去的2的最大整数次幂值。例如对于161，最大的可减幂值是128，然后再找到可以减去的次大整数幂值，以此类推，直至减到0为止。在被减去幂值的位置插入1，否则为0。在这个例子中，在从161中减去128之后，所得差值为33，无法减64，下一个被减的数只能是32。因此，转换后的二进制数应该以101开始。减去32之后还余1，所以十进制数161等于二进制数10100001。

如果要将二进制数转换成十六进制数，就需要从右边开始分成4个比特为一组。在我们的例子中，共有8个比特，因此无论是从左边还是从右边分组都无所谓。但如果不是这种情况，一定要记住，必须从最低位（也就是从右边的比特）开始分组。

在图8-2c中，被转换的二进制数是11010011，转换时分别用与之等价的十六进制数代替每组4个比特的二进制数，与之等价的十六进制数可以从8-1b中的表上查到。例如，二进制数0011的等价十六进制数是3，二进制数1011等价的十六进制数是D。这样每组4个比特的二进制数就能简单地用一个十六进制数表示，即十六进制数可以简化二进制数的表示。转换十六进制数到二进制数只需简单地按相反次序进行，给每个十六进制数分配4个二进制比特即可。如A0F转换之后是1010 0000 1111，而不是1010 1111。（在每四位二进制数之间的空格只是为了阅读起来比较方便。）

如果考试中允许使用计算器，转换会更加容易。美国的计算器上通常会有3种进制之间的转换。例如对于TI-30（德州仪器公司）计数器，为了转换成二进制数，首先按 [3rd] 键，再按 [bin] 键，这时计数器屏幕上显示的数就是二进制数。按 [3rd] 键激活了计算器上的第3组函数功能，包括计数系统。现在输入二进制数，要想知道相应的十六进制数，只要按 [3rd] 再按 [hex] 即可；同理，想得到十进制数，按 [3rd] 再按 [dec] 键即可。其他不同进制之间的转换可以用类似的方法实现。

8.2 地址解析协议（ARP）

8.2.1 一个办公室的例子

让我们先从一个简单的协议开始，这个协议被称为地址解析协议（ARP，Address Resolution Protocol）。假设我在一个大房间分隔而成的老式办公室里工作，那里还有许多工作人员，都在各自的小隔间里工作。大家都可以接听外面打来的电话，时不时就需要将一个电话转给其他的员工。为了能够转接电话，我的办公桌上存放着一张电话分机号码查询表，上面有办公室内部员工的电话分机号码。图8-3a就是我在一天早晨上班时所使用的电话分机号码表。

可以肯定，如果我接到一个打给Magan的电话，我首先会查阅分机表，然后毫无疑问地把电话转换给Magan。但是在那之后，我又接到了打给Serena的电话，我还是先查阅分机表，但是没有找到她的分机号，这时我只能让对方等一下，然后打听Serena的分机号；因此我站在自己的隔间里大声地问（广播）“Serena在吗？你的分机号是多少？”此时，所有的工作人员都会停下手头的工作来听我的问话，但是当他们发现这条消息与自己无关时，就会丢弃这条消息。只有Serena会回答我，告诉我（单播）她的分机号，于是我会把她的分机号码添加到我的分机表中，如图8-3b所示（为了让这个类比更准确一些，如果需要的话，Serena也会更新她的分机表，把我的名字和分机号加进去）。然后，我转接这个电话给Serena，并使她办公桌上的电话振铃。下一次如果我再接到打给Serena的电话，就不用再大声喊叫了，只要查一

下分机表并将电话转给她就可以了。当然，如果Serena不在办公室，我也无法转接，对方只有以后再试着打过来。

我的记性不好，所以每一次转接电话都要查一下分机表，如果没有的话，还要问一下才行。此外，我每查一次分机号码，都要把已查找过的次数写在后面。查表很费时间，所以每当我发现某个分机在最近的两天没有被用过时，就会将其从表中删除。如果需要的话，我可以通过使用“YP”(Yelling Protocol，大声询问协议)再获得这些分机号。如图8-3c所示，通过从分机号码表中删去这两天没用过的两个分机号，缩短了该分机表，这样一来，查找工作就能快一些。

Melissa	802
Jon	895
Varsha	844
Magan	858
Kristen	861

a)

Melissa	802
Jon	895
Varsha	844
Magan	858
Kristen	861
Serena	879

b)

Melissa	802
Varsha	844
Magan	858
Serena	879

c)

图8-3　a) 电话分机号码表；b) 加入了Serena的分机号；c) 由于Jon和Kristen的分机号最近连续两天都没有用到，所以从表中删除他们俩的分机号

8.2.2　应用在以太网上的ARP协议

ARP的工作原理与上面的例子几乎是一样的。而且，用ARP协议可以使IP地址与MAC地址相匹配，就如同工作人员的名字与电话分机号码相匹配一样。与不知道接收端电话分机号码无法转接电话的情况一样，不知道目的端MAC地址也无法进行以太网上的通信。以太网上的所有通信都要用到以太网的帧，而所有的以太网帧在目的地址（DA，Destination Address，）字段内都必须有一个MAC地址。一个IP数据报不能直接放在局域网上，它必须首先被封装在以太网的帧中。在本章和第25章，我们将使用IP协议数据单元（PDU，Protocol Data Unit）作为数据报，而不使用数据包，尽管术语“包”更为通用。

图8-4中是一个与因特网相连的局域网。从因特网，一个IP数据报到达路由器，路由器检查其IP地址，验证其是否在它的局域网上；之后查看这个IP地址在它的ARP列表中是否存在。路由器需要得到与该目的IP对应的MAC地址，才能通过以太网把IP数据报传递给目的主机。如果目的IP地址不在路由器的ARP列表中，那么路由器将以广播的形式在一个以太网帧内发出一个ARP请求，询问与这个局域网相连每一个主机，IP地址是否为129.117.200.204。局域网上的所有节点都会接收这个帧，但只有IP地址与之相同的节点做出响应。注意，发送ARP请求的那一帧使用全“1”的广播地址，用十六进制表示为全F。

在这个例子中，MAC地址为51的主机会做出响应（在这里我们将48个比特或12个十六进制数组成的MAC地址简化成51）。可以将响应帧看作是发送的第二个以太网帧。主机51可以在源地址段（SA，Source Address）中找到发出ARP请求的节点地址。由此主机51知道节点55正在查询自己的MAC地址，因此只向节点55发送一个ARP应答，并在这个应答中放入自己的MAC地址51。与此同时，节点51更新自己的ARP表，将节点55的MAC地址和IP地址加进去。一旦节点55（路由器）得到了节点51的MAC地址，它就能把等待传送的IP数据报发到目的地。同时，路由器也会更新它的ARP表留作后用。

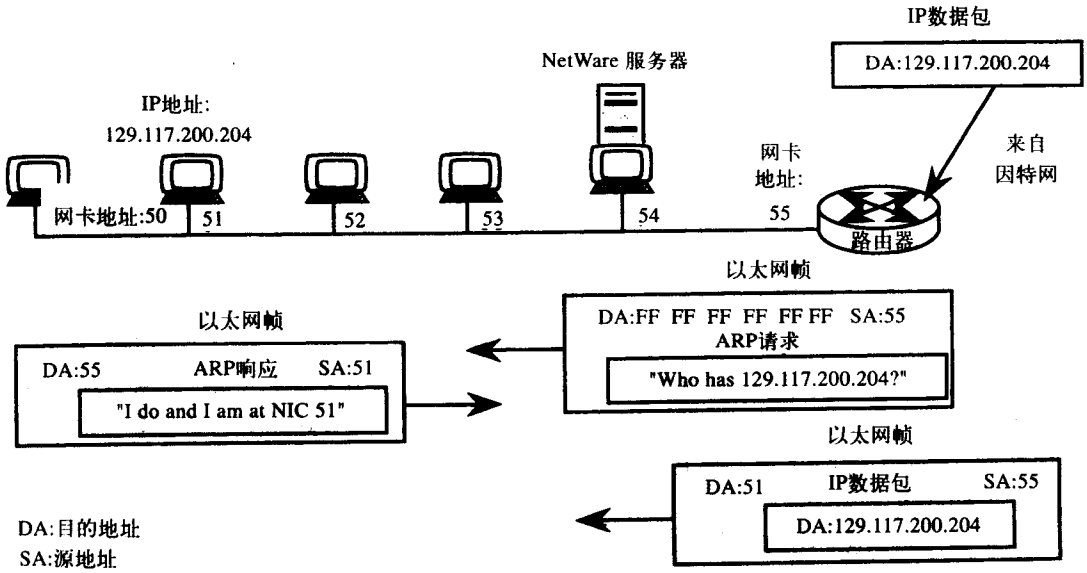


图8-4 ARP（地址解析协议）的工作原理

8.3 IP 地址

8.3.1 点分十进制表示法

在第3章中，我们已经提到IP版本4（IPv4）使用32个比特表示IP地址。下一代IP，即IP版本6（IPv6）使用128个比特表示IP地址。本书中主要采用IPv4。现在需要花一点时间复习一下3.7节有关编码和地址划分的内容。

图8-5给出了一个32比特的IP地址是如何被转换成点分十进制形式的。这些比特首先被分成4组，每一组8个比特；然后，每一组被转换成一个十进制数，并用点“.”将4个十进制数分开。注意这4个十进制数可能的最大值是255，这时8个比特都为1。

与这种二进制数的简化表示方式相对应的是MAC地址的简化表示法。为了简化由48个比特组成的MAC地址的表示方法，可以采用十六进制数。每4个比特可以用一个十六进制数表示，因此得到12个十六进制数。IP地址习惯上使用点分十进制表示法。

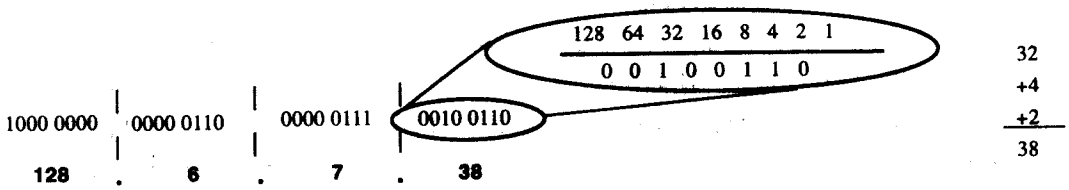


图8-5 二进制的IP地址被转简化成点分十进制形式。8个比特一组，每个“1”所在位置的权值相加

8.3.2 IP地址的分配

回忆第3章，在讨论2的幂的概念时，说明了以太网卡的MAC地址是如何分配的。48个比

特被分成两组：24个比特用来对网卡的生产厂商进行编码，另外24个比特用来对网卡的序列号进行编码。中心授权机构（目前是IEEE）只是简单地管理哪些生产厂商被分配了哪些厂商编号。这些编号官方的名称是组织唯一标识符（OUI，Organizational Unique Identifier）。这样每个生产厂商可以生产多达2^{24}个网卡，每一个都有唯一的序列号。也就是说，每一个生产厂商被分配了一个MAC地址块，这些特定的地址块由生产厂商的编号来标识。

这个方案的问题是，生产规模大的制造商需要几个厂商编号，而生产规模小的制造商却用不完所分配的2^{24}个序列号。IP地址的分配方法与此不同，IP地址的分配既考虑到了大型机构需要较多的地址，小型机构只需要较少的地址，同时还考虑到了中等规模网络地址的需求。

在图8-6中，可以看到IP地址块被分成3类：A类、B类和C类。一个大型机构，比如GE（美国通用电气公司），需要大量的地址，所以分配给它们一个A类网络（很快就会看到如何用IP地址来区分不同类型的网络），这样GE的地址范围可以从3.0.0.0到3.255.255.255，总共有2^{24}个地址。再比如Rutgers大学，尽管还能有其他的地址块，但被分配了一个B类网络，IP地址范围从128.6.0.0到128.6.255.255，在这个地址块中只有2^{16}个地址。同样，小规模的网络只有较少的地址，这些地址块被称为C类网络。

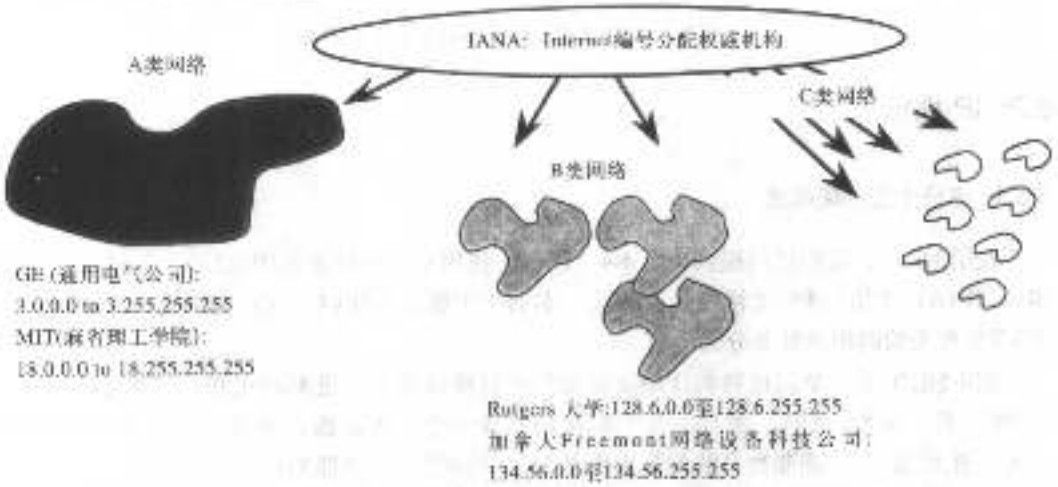
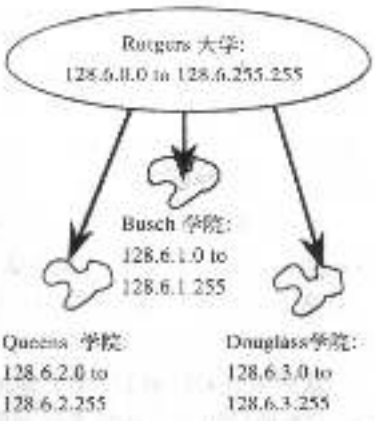


图8-6　大、中、小规模网络的IP地址的分配。上面的例子可以从www.arin.net/whois上获得

A类网络的个数较少，但每一个A类网络都由许多主机组成；C类网络的个数较多，但网络上的主机却不多。通用电气公司的网络简单地被标记为3.0.0.0或简记为3。Rutgers大学的网络由128.6.0.0标识，或简记为128.6。我是从www.arin.net/whois上查到这些信息的。从这个网站，你也可以检索这些信息，比如说谁有什么样的地址，哪一个地址被分配给了谁，以及其他的各种有趣的信息。因特网编号分配权威机构（IANA，Internet Assigned Numbers Authority）通过美国因特网编号登记处（ARIN，American Registry for Internet Numbers）管理IP地址的分配，其他的大陆都有各自的地址注册机构。另外两个有趣的网址是www.internic.net和www.iana.net。

利用分类可以简化IP地址分配的管理，同时也使分组的路由更为有效。当需要传送IP数据报时，路由器不必知道目的主机的确切位置，它只需知道把这个数据报路由到哪个网络就可以了。例如，Rutgers大学的路由器接收到一个目的地址为3.121.7.203的IP数据报，它首先

查看第一个点分十进制数3，不必再检查其他的比特，就可以把这个数据报发送给通用电气公司的网络。通用电气公司的路由器检查其他的比特，直到把这个数据报送到目的主机为止。



与因特网上其他许多的事情相同，IP地址的分配是层次化的。就如同中心授权机构将地址块分配给不同的组织机构一样，不同的组织机构又将其所得到的地址分成更小的地址块，提供给该机构的不同部门使用。从右边的图中可以看到，Rutgers大学负责管理从128.6.0.0到128.6.255.255的所有地址。网络地址的分配不是由一个网络管理员为每一个网络节点分配IP地址，而是由管理员把一组IP地址分给某一幢楼或某一所大学的局域网的管理员。由图可见，以128.6.3.0开头的全部地址归Douglass学院管理，而以128.6.1.0开头的全部地址归Busch校园的管理员负责管理，等等。这样分散了地址的管理，也就是说，IANA记录谁拥有哪个网，而这些网络的管理员记录谁拥有哪些子网。接下来让我们看一下如何识别各类网络。

8.3.3 地址的分类

如果我们把一个IP地址的前8个比特的所有二进制数都写出来，就可以得到一个如图8-7左边所示的列表，这个表从“0000 0000”一直到“1111 1111”。现在要做的事情是将这套地址（总共2^{32}个）分成五个地址类，最后两类地址是不能分配给用户的。

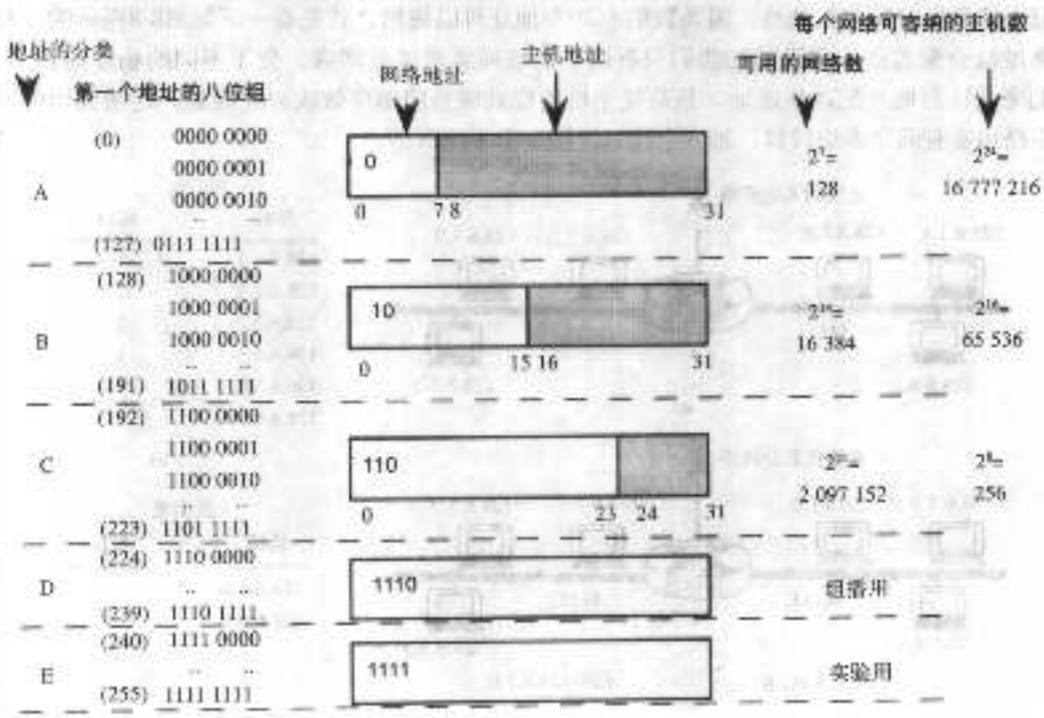


图8-7 IP地址的分类

如果IP地址第一个八位组的第一比特为零，那么这个地址就是A类地址。通过计算可以知道，A类地址的第一个点分十进制数必须落在0~127这个范围之内。类似地，继续往下走，可以看到B类地址以二进制数“10”开头，第一个点分十进制数的范围是128~191，C类地址以二进制数“110”开头，第一个点分十进制数在192~233范围之内。类似地，D类和E类地址如图所示，它们分别用于组播和实验。

A、B和C类地址又可以进一步分成两个部分，一部分用于表示网络地址，另一部分用于表示网络上的主机地址。如图所示，A类地址只用7个比特来标识网络，剩下的24比特用于标识网络上的主机。这意味着A类地址只能拥有128个网络，但是每一个A类网络上最多可以连接2^{24}，即16 777 216个主机。

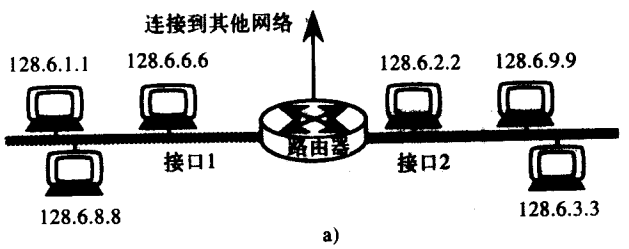
从图中还可以看到，B类地址用14个比特来标识网络地址，用16个比特来标识主机；类似地，C类地址用21个比特来标识网络，8个比特来标识主机。

Rutgers大学的许多主机和网络使用B类地址，因为这些地址都是以128开头。注意，以128开头的B类网络有256个，但是以26开头的A类网络只有一个。这是因为B类网络用最开始的16个比特（两个点分十进制数）来表示网络，而A类网络只使用最开始的8个比特来表示网络。因此，Rutgers大学的主机都以两个点分十进制数开始，即128.6。

8.4 子网

8.4.1 划分子网的原因

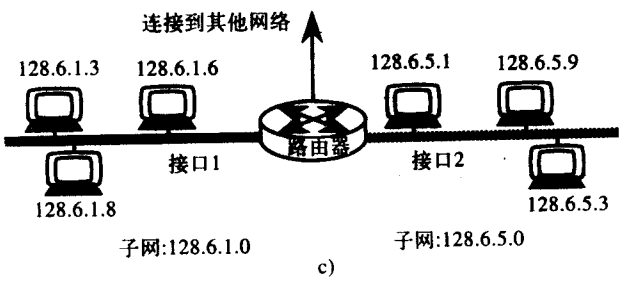
假设我们是Rutgers大学的管理员，并且分配得到的B类网络地址是128.6.0.0。那么我们可以随心所欲地分配主机地址，因为我们有2^{16}个地址可以使用。首先看一下如图8-8所示的一种网络地址分配方法。假设最初我们只有两个局域网或者说是网络，位于不同的物理地点上。我们毫无计划地分配这些地址，只是按主机连接到网络的顺序依次分配地址。连接到因特网的主路由器有两个本地接口，每一个接口连接一个本地网络。



路由表

地址	接口
128.6.1.1	1
128.6.2.2	2
126.6.3.3	2
126.6.6.6	1
126.6.8.8	1
126.6.9.9	2

b)



路由表

地址	接口
128.6.1.0	1
128.6.5.0	2

d)

图8-8　a) 随机地分配地址，b) 随机分配的路由表，c) 使用子网，d) 使用子网对路由表的影响

现在看一下这时的路由器该如何工作。首先它必须维持一个路由表，上面记录了每一个主机的IP地址以及与之相连的接口号，如图8-8b所示。随着网络上节点的不断增加，路由表渐渐变大。此外，路由器还需要与其他的路由器共享路由表，以便让其他路由器知道这个路由器连接了哪些网络。由于要定期地在网络上传送这张庞大的路由表，因此加重了网络的负担。同时查找路由表其中的各个条目也要花费较多的时间，更不用说掌握所有IP地址的位置这项管理工作有多么繁重了。

回忆一下，对地址进行分类的目的就是为了识别一个特定的IP地址在哪一个网络上。由于数据报在路由传递过程中不需要检查所有的32比特，因此把一个数据报传递给通用电气公司的网络很简单。类似地，我们可以再进一步区分网络，把网络128.6.0.0分成几个子网，如图8-8c所示。这样路由器只需知道所有以128.6开头的主机都位于自己的网络上，同时还知道以128.6.1开头的所有地址都与自己的本地接口1相连接，以128.6.5开头的所有地址都与自己的第2个可用接口相连接。根据地理位置的不同来划分地址组会使路由表更为简单。这时，路由表易于查找，方便与其他路由器共享，IP地址的管理也轻松不少。随着主机和路由器数量的不断增加，这个优点会变得更加显著。

划分子网的另一个原因是出于不同工作组之间的安全性的考虑。通过划分子网可以使不同工作组相互独立，业务数据不会被发送到与之无关的其他子网中去。再有，当两个网络在地理上是分开的，或者使用了两种不同的MAC协议，或者被路由器分开时，都必须划分子网。

8.4.2 划分子网的方法

让我们先看一下如何识别一个子网。现在有以128.6.0.0开始的地址空间。根据图8-7，B类地址分配16比特给主机。这些用于标识主机地址的比特可以进一步被再分成子网地址和主机地址。在Rutgers大学，由于有许多地点，子网的划分以一个八位组为界线。尽管情况并非总是如此，但是这会使数字地址的解析更加容易。如何划分子网和如何使用这个子网，只是一个局部网络的问题，并不涉及因特网的其他部分。

为了方便路由，使用一种被称为子网掩码的比特掩码来区分IP地址中的子网地址和主机地址。利用子网掩码，路由器可以知道IP地址中的哪些比特被用于标识子网地址，哪些比特被用于标识主机地址。在图8-9中的上面，再次画出了B类地址的表示方式；在这个B类地址的下面，是将一个八位组用于子网后的B类地址划分方式。在这里，第3个八位组被用于表示子网地址，第4个八位组被用于表示主机地址。在这种情况下，子网掩码是255.255.255.0。

现在让我们来看一下如何利用IP地址和子网掩码来形成子网地址和主机地址。IP地址128.6.7.38的子网地址是128.6.7.0,这是子网掩码与IP地址做“与”运算得出的结果。如果做“与”运算的对应比特都是1，“与”运算的结果才是逻辑1；否则结果为逻辑0。另一方面，由于主机地址只使用掩码的0比特，因此主机地址从IP地址中被“掩盖”掉。利用给出的掩码，IP地址128.6.7.38表示在子网128.6.7.0上主机编号为38。

一个子网的广播地址是在子网地址上设置所有的主机比特为1。例如，如果一个主机（控制主机），要在其子网上向所有的节点广播一条消息，就得把目的地址设置成128.6.7.255。由于在应聘面试时常常会问到有关子网的问题，所以我们这里就多举一些例子来说明。

没有划分子网的B类地址		网络地址		主机地址	
用8个比特划分子网的B类地址		网络地址		子网地址	主机地址
IP地址	(128.6.7.38)	1000 0000	0000 0110	0000 0111	0010 0110
子网掩码	(255.255.255.0)	1111 1111	1111 1111	1111 1111	0000 0000
子网地址	(128.6.7.0)	1000 0000	0000 0110	0000 0111	0000 0000
子网内的主机地址	38	0000 0000	0000 0000	0000 0000	0010 0110
子网的广播地址	(128.6.7.255)	1000 0000	0000 0110	0000 0111	1111 1111

图8-9　IP地址和子网掩码比特相“与”形成子网地址。对应于掩码比特为0的那部分IP地址是主机地址。主机比特部分都为1的IP地址为广播地址

8.4.3　划分子网：例子 1

解释从下面的IP地址中所能够获得的全部信息，最后5个比特是主机地址。IP地址如下：1101 0110 1001 0010 1110 0111 0100 1101。在这些例子中，主机比特都用黑体标出。

结论：由于第一比特不是0，说明它不是A类地址；由于紧接着的第二个比特也不是0，因此它也不是B类地址；这是一个C类地址，用点分十进制表示为214.146.231.77。侧面的表格可以帮助你计算各种地址。有5个主机比特，意味着有27个子网比特。根据侧面的表格，对应的子网比特被设置成1，对应的主机比特都被设置成0，因此得到子网掩码为1111 1111 1111 1111 1111 1111 1110 0000 。转换成点分十进制数为255.255.255.224。值得注意的是，当用二进制表示地址（或掩码）时，不必考虑转换成十进制时用到的4个8比特的分界线，只要分清哪些是子网比特，哪些是主机比特就可以了。

再有，在把二进制表示的IP地址转换成点分十进制表示时，不必关心哪些是主机比特，这里需要关心的问题是8比特组的分界线在哪里。接下来看一下子网地址。

根据侧面图中的表格，子网比特与IP地址比特相同，标识主机的比特被设置成0。这样子网的地址为1101 0110 1001 0010 1110 0111 0100 0000 ，即为214.146.231.64。再使用侧面图中的表格，主机比特给出了网络上主机的编号。因此，01101表示主机的标识符（id）为13。换句话说，IP地址214.146.231.77又可以理解成214.146.231.64子网上的13号主机。

	子网比特	主机比特
掩码	1	0
子网地址	IP比特	0
主机地址	（无）	IP比特
广播地址	IP比特	1

还可以使用表格中的最后一项，得到子网的广播地址。也就是说，使用相应的IP地址作为子网比特，而标识主机的比特为全置成1。这样做之后，可以得到广播地址214.146.231.95。最后的十进制数由二进制数 0101 1111产生。最后由黑体表示的5个比特是主机地址位，而这一组中的前3个比特来自子网比特。图8-10总结了计算结果。

IP地址	1101 0110	1001 0010	1110 0111	0100 1101	214.146.231.77
子网掩码	1111 1111	1111 1111	1111 1111	1110 0000	255.255.255.224
子网地址	1101 0110	1001 0010	1110 0111	0100 0000	214.146.231.64
主机号码				0 1101	13
广播地址	1101 0110	1001 0010	1110 0111	0101 1111	214.146.231.95

图8-10 例1的计算结果

掩码指出了子网比特位的数目和主机比特位的数目，IP地址和它的子网掩码可以用“IP地址／子网前缀长度”这样的格式表示。子网前缀的长度是指在子网掩码中值为1的比特数。因为子网掩码的前27位为1，所以在前面例子中的IP地址和它的子网掩码可以表示为214.146.231.77/27。

8.4.4 地址的损失

我们接着用上例中的IP地址继续讨论。我们已知214.146.231.77这个IP地址表示的是在214.146.231.64子网上的第13号主机。现在的问题是在这个子网上可以有多少台主机，在整个网络中又有多少个子网可以使用这个子网掩码。

对主机ID的编码共使用了5个比特，所以在这个给定的子网上可能有2^5或者32台主机。在这些地址中，0 0000被用来标识子网，这可以从子网地址214.146.231.64看出。再有，全1或者是1 1111被用作在这个子网上向所有节点广播数据报的广播地址。这样分配给主机的可用地址只剩下30个。通常，路由器还需要一个地址来表示与该子网的接口。在任何情况下，最多只有30个可分配的地址。事实上，与数学计算的可能结果相比，总会少两个可用地址，因为全0被用作子网地址，而全1被用作广播地址。

现在让我们看一下在214.146.231.0/27网络上可能有多少子网。由于只为子网部分保留了三个比特，因此有2^3也就是8种可能的组合。这里同样也失去了两种组合，000被用作网络地址，111表示整个网络中所有的子网，所以能分配的只有6个子网地址。由于这个原因，因而总是要损失掉2个子网。正因为这样，一个网络中的子网数目也要比计算出来的少两个。如果用4个比特来表示子网的话，在总共的16个子网中我们实际可以用的子网数目为14个。

图8-11给出了6个可用的子网，每个子网最多只有30个可用的主机地址，所以我们总共有180个可分配的地址。如果不划分子网，可以有254个地址。尽管如此，使用子网还是利大于弊。

6个子网	乘以	每个子网30个地址			等于180个地址
~~000~~		~~00000~~	01000	10000	11000
001		00001	01001	10001	11001
010		00010	01010	10010	11010
011		00011	01011	10011	11011
100		00100	01100	10100	11100
101		00101	01101	10101	11101
110		00110	01110	10110	11110
~~111~~		00111	01111	10111	~~11111~~

图8-11 划分子网减少了可用地址的数目

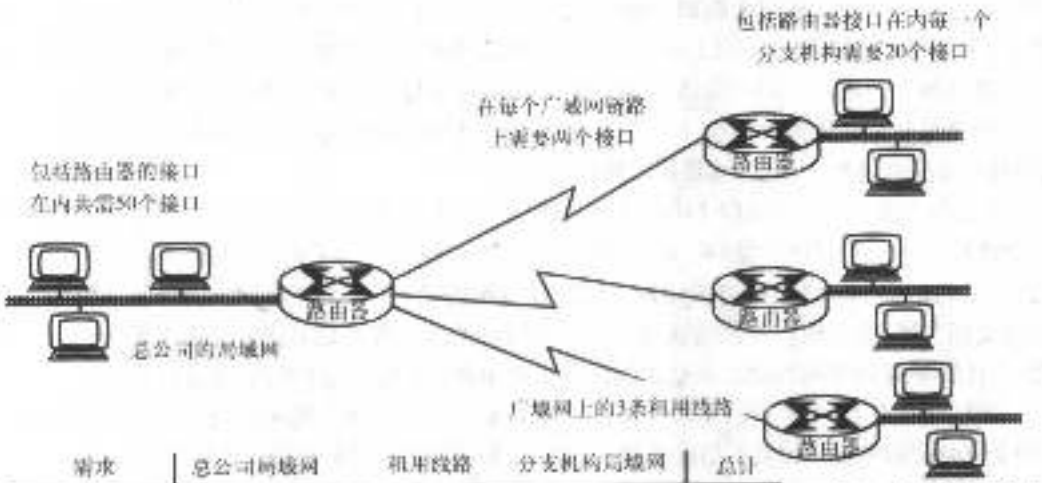
如果我们将子网和主机比特的边界向右移动一个比特，结果会怎样呢？这时子网的数目和每个子网中的主机数目会发生什么样的变化呢？如果我们减少主机的比特数，相应地就减少了每个子网中主机的数目，但同时增加了子网的数目。那么这时可用IP地址的数目又会发

生怎样的变化呢？

如果使用4个比特作为主机比特，那么在每个子网中就有14个可用的主机地址，同时还有4个子网比特，可以给出14个子网地址，两个数相乘我们共有196个IP地址。如果将主机和子网比特的边界再向右移一位，即使用3个比特作为主机比特，那么在每个子网中就可有6台主机，但可以得到30个子网。因此，如果想得到最大的可用IP地址数，应该使主机比特数和子网比特数相等。如果你有一个B类网络，要实现最大的地址数，分配8个比特给子网部分，8个比特给主机部分，尽管这可能并不是对于所有情况都适用的正确决定。

8.4.5　划分子网：例子2

下面再来看一个关于子网划分和地址分配的例子。在图8-12中，有一个机构分配得到的网络地址是200.200.200.0，这是一个C类地址，所以只有254个地址是可用的。在大量的研究和讨论之后，该机构决定总公司最多留50个接口。接口这个术语比主机更准确，因为一个主机可能会有几个接口。三个分支机构每一个可能需要20个接口。假设我们决不增加新的分支机构（至少在这个例子中是这样的）。此外，使用租用的链路将每个分支机构的路由器与在总部的路由器连接起来。这些链路的每一端还各需要一个IP地址，每一条链路都应该位于自己的子网上。



需求	总公司局域网	租用线路	分支机构局域网	总计
地址	50	每条2个	每条20个	116
子网	1	总共3个	总共3个	7

图8-12　创建子网的例子

根据图8-12的表格，对IP地址和子网的数量进行统计，共需要116个接口和7个子网。假设使用4个子网比特和4个主机比特来划分网络，那么最多在14个子网上每一个有14个主机地址。但是这样是不符合要求的，因为总公司和分支机构的局域网分别需要50和20个地址。如果使用3个子网比特，则最多可以得到6个子网，也同样不符合要求。如果3个比特作为主机比特，我们的4个子网显然还是没有足够的地址可用。解决这个问题的方法是采用所谓的**变长子网划分**（variable-length subnetting）。对于变长子网划分，子网比特或者说掩码是根据子网改变的，然而你必须确定每一个路由器都了解每种网络的掩码，或者你所使用的路由协议，比如OSPF和RIP-2协议在广播路由表的同时还广播掩码。

结论：开始解决这个问题的最好方法是使子网所能容纳的主机数满足主机数最多的子网

的需求。总公司需要50个地址，能提供这么多地址的最小子网是只有2个比特的子网。如果使用2个子网比特，就会给出6个主机比特，这样就能提供多达60个主机，完全可以满足总公司的需要。

如侧面的图所示，我们列举了2个子网比特所有可能的组合。第一行和最后一行都不能使用，因为它们分别代表网络地址和广播地址。这里使用10作为子网，将子网地址01留给其他需要分配地址的接口。子网10的地址范围是从1000 0000 到1011 1111，即从128 / 26到191 / 26。与局域网接口的地址可以配置成200.200.200.129，而总公司的其他主机可以分配从130到190的地址。记住，200.200.200.128是这个子网的子网地址，200.200.200.191是这个子网的广播地址。

~~00~~ 不能使用
01 给其他的主机
10 用于这个子网
~~11~~ 不能使用

~~000~~ 不能使用
001 由分支机构1使用
010 由分支机构2使用
011 由分支机构3使用
100 由总公司使用
101 由总公司使用
110 不使用
~~111~~ 不能使用

~~0000 00~~ 不能使用
0000 01 用于链路1
0000 10 用于链路2
0000 11 用于链路3
0001 00 未使用
.....

接下来，让我们为分支机构分配地址，因为它们是第二大子网。在这里，可以容纳20个主机的最小子网是拥有3个子网比特的子网，这样在每个子网上可以提供30个可用的主机地址。在侧面的图中，还列举了使用3个子网比特的所有可能组合。同样，000和111不能被使用，因为它们分别代表子网地址和广播地址。以100和101开始的地址已经被分配给了总公司的局域网，不能再分配这些地址。剩下的地址以001、010、011或110开始。为了选择相邻的地址块，所以使用前3个。

分支机构1使用的地址范围从0010 0000到0011 1111，也就是从200.200.200.32到200.200.200.63。地址32是它的子网地址，63是它的广播地址。分支机构2的地址范围从0100 0000 到 0101 1111，即从64到95；这次省略了前缀200.200.200。分支机构3的地址范围从0110 0000到0111 1111，即从96到127。

最后，就剩下租用链路的地址没有分配了。因为链路的每一端都需要一个地址，在3个子网的每一个子网上仅需要2个接口。能够提供2个接口的最小子网是拥有6个子网比特的子网，这时有两个主机比特，使每个子网可以拥有2个主机地址，同样00和11不能被使用。我们决定采用以0000开始的地址。在给总公司局域网分配地址时，不能使用这个范围的地址，因为以00开头的地址是子网地址，而所有分支机构的地址也没有使用000开始的这部分地址。因此，我们选择这段地址是安全的。对于链路1，使用0000 0100或者4做为子网地址，它的广播地址是0000 0111或写为7。那么可以分配的子网地址为0000 0101（5）和 0000 0110（6）。对于链路 2，采用0000 1001（9）和0000 1010（10）。最后对于链路3，采用0000 1101（13）和0000 1110（14）。在图8-13中总结了这些地址，可以看到确实没有地址的重叠。

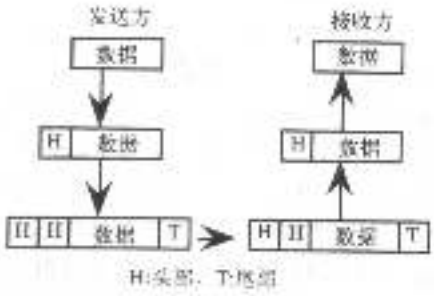
(00)0 (01)1 (10)2 (11)3	这些地址落在子网掩码为六位的地址范围内。	32 至 63	分支机构1
		64 至95	分支机构2
4至7	链路1	95 至127	分支机构3
8 至11	链路2		
12 至15	链路3	128至191	总公司

图8-13 所有以200.200.200开始的地址。每个分支机构地址都包括作为子网地址的第一个地址和作为广播地址的最后一个地址。例如，在链路1上200.200.200.4是子网地址，200.200.200.7是广播地址，而5和6是可分配的地址

8.5 数据包和帧的分析

8.5.1 简介

现在看一下在一个网络上如何辨别以太网帧？我们将会看到IP数据报和其他的协议数据单元（PDU，Protocol Data Unit）如何被封装在以太网帧中。在第2章中曾经解释过，OSI如何逐层封装PDU以在一个网络上传输数据。正如图中的图所示，每一层都是把自己的头信息加进去。同时，我们还知道在接收端，每一层都将这些PDU抽取出来，去掉各个头部。在本节中，通过从局域网上捕获一帧的例子，解释这个过程是如何实现的。在此之后，会在适当的地方描述构成TCP／IP协议族的各层。



8.5.2 协议分析器

在图8-14中，利用UNIX以太网分析器截获了一个以太网帧，这个软件在Linux下运行是免费的。在这个图中，有三个可调节的窗口，最上面的窗口标记为图8-14a，并且高亮度地显示捕获到的帧，被高亮显示帧的细节出现在下面的两个窗口中。在下面两个窗口的右边都有一个滚动条，可以方便地选择分析器缓冲区中捕获到的以太网帧。

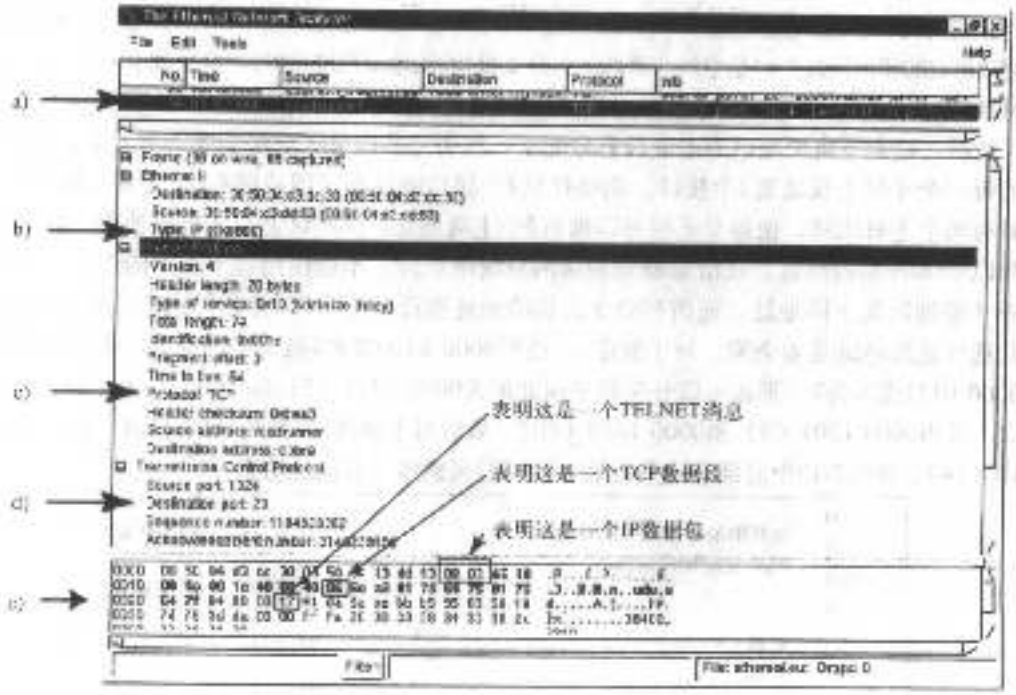


图8-14　a) 被分析的帧；b) 在以太网帧的类型字段，十六进制数0800表示这是一个IP数据报；c) 在数据报头部，协议号表示数据报内是TCP数据段；d) 在TCP头部，目的端口号字段表明这段数据中携带的是TELNET消息；e) 这一帧中的原始数据

最后一个窗口也就是图中被标记成图8-14e的窗口，显示的是构成正在分析的帧的实际数据。数据的每一个字节用2个十六进制的数表示。记住每一个十六进制数可以代表4个比特。最左边的一列（或者说垂直排列）的数是0000、0010、0020，等等，简单地表示每个字节的位置编号。这些位置也是用十六进制标记的，因此数据以16个字节为一组被显示，每一组占了一行（水平排列）。用十六进制表示的数据还被转换成了ASCII字符，显示在第3个窗口的右边。一般情况下，除非我们看到的这一帧所传输的内容是真正的文本信息，否则ASCII字符看起来通常是一些乱码。

为了帮助我们理解这一帧所显示出来的数据，中间的窗口给出了组成这一帧的各部分信息，用图8-14b~图8-14d标记的各项分别表示当前各个字段的具体数值。尽管这里给出了许多字段，但我们只关心其中少数的几个字段。这里的目的不是为了解释协议的构成，而是要说明网络中的各层是怎样按照协议来处理数据的。

注意，中间窗口的“Internet Protocol”被高亮显示，同时在下面的窗口中IP层头信息部分的数据也被高亮显示，分析器用粗体显示这些字节，从第一行结尾的“45”开始，一直到第三行的“7F”结束，所有这些字节都是IP头的内容。IP头有20个字节长，都用黑体显示出来。那么IP头之前的那些字节是什么字节呢？它们是更上层协议的头部信息，可能是来自应用层的数据。现在，让我们像剥洋葱一样层层“剥去”这一帧的所有头部。利用图8-15a，试着计算一下十六进制数据，以便更好地理解在这个数据中每一字节的位置，在这里一些字节已经被移走。

8.5.3 解析各层协议

以太网层：当网卡接收到一个数据帧时，首先检查帧尾的误码，这些误码没有在被捕获的分组中显示出来。如果存在误码，就抛弃这一帧。然后网卡检查这一帧中的目的地址，以确定是否与自己的地址相匹配。当以太网的驱动器收到这一帧时，只对前面的14个字节感兴趣（其他的以太网帧以及它们之间的区别将在23章中讨论）。最开始的6个字节被标记为MAC 目的地址（MAC DA，Media Access Control-Destination Address），告诉主机这一数据帧属于谁。SA表示发出帧的MAC地址。类型字段0x0800表示以太网帧中封装的是IP数据报，在数前面的“0x”用来表示这个数采用的是十六进制格式。由于以太网的驱动器（MAC层）只关心自己的头部信息，因此剩余的数据被显示成灰色。由于这是一个IP数据报，因此MAC层软件会把这个帧的其他部分送给IP层处理。在类型字段中还可以是其他的值，来表示不同协议，如侧面的图所示。类型字段总是出现在数据帧的0xC和0xD位置上。

类型	协议
0800	IP
0805	X.25
0806	ARP
8035	RARP
809B	Appletalk
80D5	SNA
8137	Novell
8138	Novell

协议字段	过程
0x01	ICMP
0x02	IGMP
0x06	TCP
0x08	EGP
0x11	UDP

IP协议：现在MAC层已经把数据帧中的其他部分转发给了IP层，接下来IP层就会处理它的头信息。IP层的头部通常是20个字节。IP层通过计数得到这些字节，并只查看这些与头部有关的字节。IP层要检查数据报的源地址，这些信息出现在数据帧的0x1A、1B、1C、1D的位置。如图8-15c所示，那些圈起来的字节“81 75 64 75”就是源地址的十六进制表示。接下来的4个字节“81 75 64 7F”是目的端的IP地址。在完成与头部信息有关的其他工作之后，IP层需要知道数据帧中剩下的那些数据应该转交给哪个过程来继续处理。图中其他的数据都用深灰色覆盖住了，IP层不对这些数据进行处理。0x17位置的字节告诉IP层这些剩余的数据应该交给TCP协议处理。数据帧中的“0x06”，与十进制数06相同，被称为协议号。在这里它是TCP协议的编号。其他协议的编号如侧面的图所示。

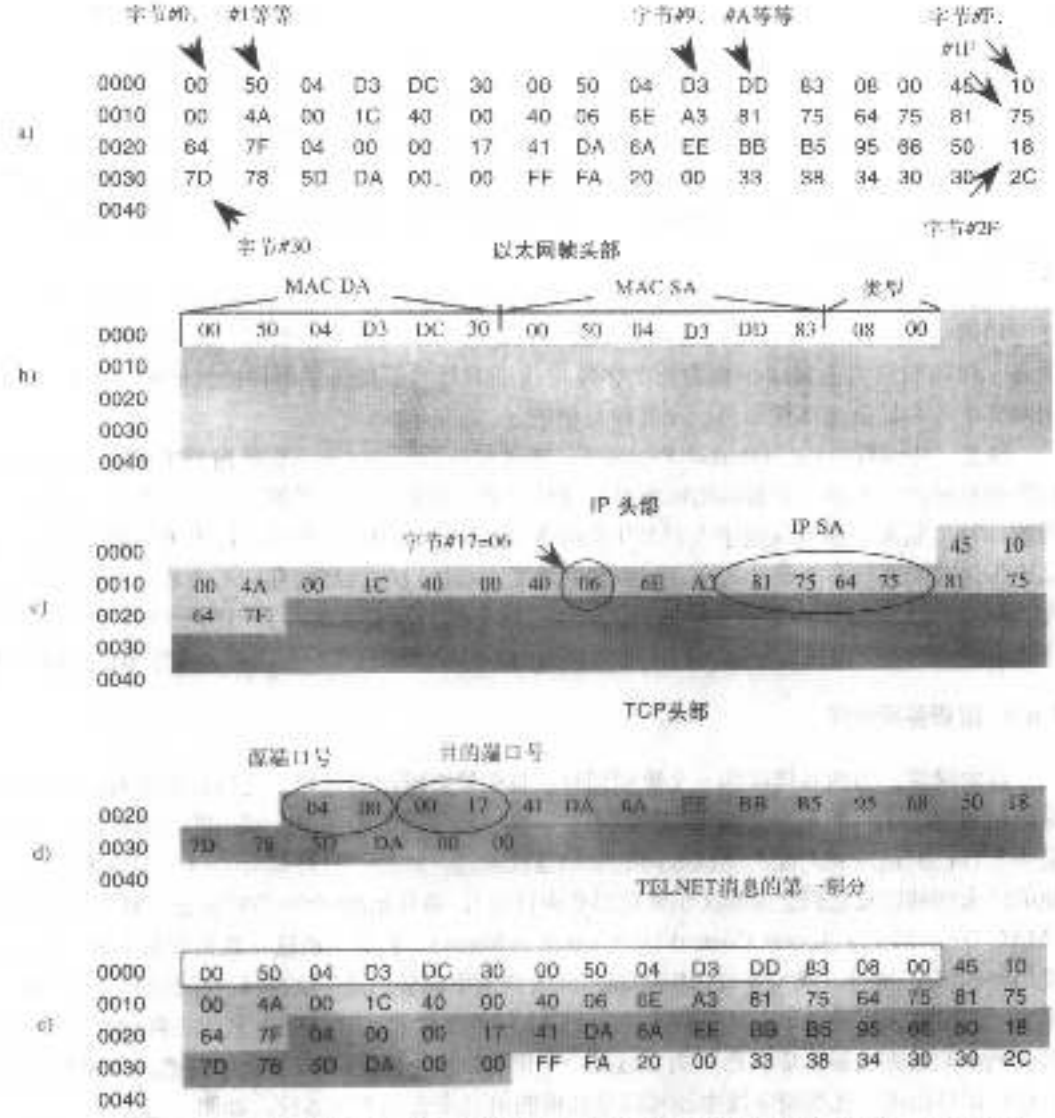
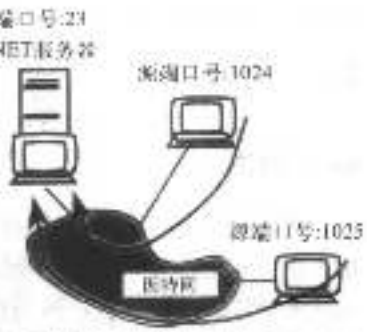


图8-15　a) 确定数据字节的位置。b) 类型字段值0x0800表明这一帧传输的是IP数据报。c) 协议号06指出数据包携带的是TCP数据段。d) 目的端口号17表明数据段携带的是TELNET消息。e) 3个头部信息的位置

TCP协议：现在TCP过程来处理数据帧中的剩余部分，如图8-15d所示。通常情况下，TCP层也是通过计数得到20个字节的头信息，忽略其他的字节，在图8-15d中被忽略掉的字节用深灰色来表示。TCP的头信息和在头信息之后的数据内容一起被称为TCP段(segment)。换句话说，TCP的协议数据单元就是一个段，TCP层需要确定将除了头字节之外的数据前转给哪一个应用程序，这是TCP层所要做的众多工作之一。完成这个功能所需的信息可以从TCP头信息中的**端口号**（port number）字段中获得，在图8-14中间的窗口中，可以看到有一个源端口和一个目的端口，在这里我们比较感兴趣的是较小的端口号0x0017，即十进制的23，这是一个目的端口号，它告诉TCP处理过程在TCP段中封装的是一个TELNET消息。接下来，TCP处

理过程把TCP段中的数据部分传递给TELNET处理过程。在这个例子中，TELNET是一个在应用层的协议。在侧面的图中列出了一些常用的端口号。

UDP/TCP	端口号	应用程序
TCP	0×14–20	FTP(data)
TCP	0×15–21	FTP(control)
TCP	0×17–23	telnet
TCP	0×19–25	SMTP
UDP&TCP	0×35–53	DNS
UDP	0×43–67	Bootp server
UDP	0×44–68	Bootp client
UDP	0×45–69	TFTP
UDP&TCP	0×50–80	http(WWW)
UDP&TCP	0×89–137	NetBIOS



对于输入的数据分组，源端口可以使得服务器区分不同的连接。

应用层协议：在实际应用中可能会有许多用户同时远程登录到我们的服务器（任何一台非本地计算机的主机都可以被称为远程主机），每一个用户都可能开启他自己的TELNET应用进程。这时，TCP处理过程怎样知道应该把接收到的数据发送给哪一个TELNET应用进程呢？这可以通过源端口号加以区别。源端口号使TCP处理过程准确地分辨出接收到的数据是属于哪一个连接。可以看到，源端口的端口号1024，即十六进制的400，与目的端口号23相比较它是比较大的。当用户在这个帧中要求建立一个TELNET会话时，服务器就把1024号端口分配给该用户。下一个登录到该服务器的用户则会被分配给另一个不同的端口，比如说1025号端口，如侧面的图所示。在会话建立的过程中，运行telnet客户端程序的用户可以得到一个端口号，在此之后只要这个连接没有被断开，它将一直使用这个端口号。通过这种方法，TCP过程可以同时处理来自多个信源的TELNET消息，而不会造成信息混淆。应该注意的是，当一个TELNET数据分组反向传送时，比如从服务器到客户端，源地址和目的地址应该交换位置。较小的端口号总是用于常见的端口或应用程序，而较大的端口号则通常是用来区分不同的连接。

8.5.4 举例

在各个字段中，还有可以使用其他的数值，这些值前面已经给出。下面使用这些数值来解析图8-16中给出的帧。分析结果如下。

a)	0000	00	50	04	D3	DC	30	00	50	04	D3	DD	83	08	00	45	10
	0010	00	4A	00	1C	40	00	40	11	6E	A3	81	75	64	75	81	75
	0020	64	7F	04	00	00	50	41	DA	6A	EE	BB	B5	95	68	50	18
	0030	7D	78	5D	DA	00	00	FF	FA	20	00	33	38	34	30	30	2C
	0040																
b)	0000	00	50	04	D3	DC	30	00	50	04	D3	DD	83	08	22	45	10
	0010	00	4A	00	1C	40	00	40	06	6E	A3	81	75	64	75	81	75
	0020	64	7F	04	00	00	17	41	DA	6A	EE	BB	B5	95	68	50	18
	0030	7D	78	5D	DA	00	00	FF	FA	20	00	33	38	34	30	30	2C
	0040																
c)	0000	00	50	04	D3	DC	30	00	50	04	D3	DD	83	08	00	45	10
	0010	00	4A	00	1C	40	00	40	06	6E	A3	81	75	64	75	61	75
	0020	64	7F	00	15	04	00	41	DA	6A	EE	BB	B5	95	68	50	18
	0030	7D	78	5D	DA	00	00	FF	FA	20	00	33	38	34	30	30	2C
	0040																

图8-16 以太网帧解析的三个例子

在图8-16a中，类型字段中的值是0x0800。这意味着在以太网帧中封装的是一个IP数据报。再往后走，看位置0x17处的数据，其值是0x11。从前面图中可知，这说明传输的数据是一个UDP数据报。幸运的是，在UDP数据报头中，源端口和目的端口的位置与在TCP数据报头中的位置一样。因此，在位置0x25上的值是0x0050，表示这是一个HTTP应用。

在图8-16b中，类型字段中的值不是0x0800，所以它不是一个IP数据报。此外它的值也不是0x0806，说明它也不是一个ARP数据包。它也不是Novell数据包。因此，第二层使用的是另外一种协议，就我们目前所知，还无法判断它是什么协议。

图8-16c所给出的是一个IP数据包，封装了一个TCP数据段，在0x22和0x23位置上的值是0x0015，所以它一定是一个FTP应用。

8.6 TCP/IP 层

8.6.1 概述

利用对以太网帧捕获过程的分析，我们观察到了如图8-17所示的4个层。第一层叫做网络接入层，在这一层中使用的是以太网协议。接下来的是网络层、传输层和应用层。把TCP/IP层次和OSI结构相对应，网络接入层对应的是OSI中的第一层和第二层。互联网层对应的是OSI中的第三层即网络层。两种模型的传输层和应用层可以很好地对应。然而，在TCP/IP体系结构省略了会话层和表示层，从而简化了网络的体系结构。

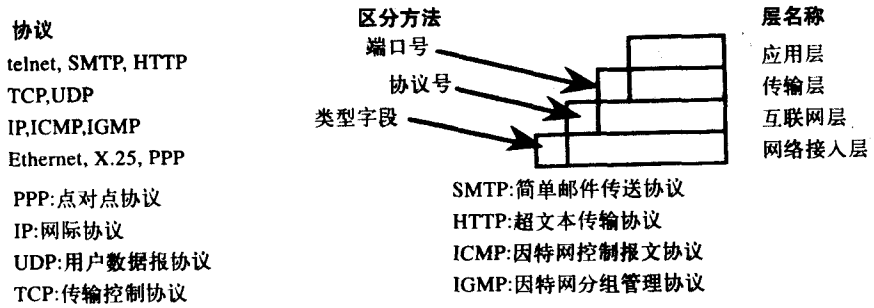


图8-17　TCP/IP网络的体系结构

如你所看到的那样，在TCP／IP协议簇中有许多协议。在本章中仅介绍其中的一些协议，剩下的协议将在第25章讨论。

图8-18较详细地给出了TCP／IP协议的各层结构，在不同层中所使用的协议都显示在这个图中。其中IP协议必须用在互联网层，另外因特网控制报文协议（ICMP，Internet Control Message Protocol）和因特网分组管理协议（IGMP, Internet Group Management Protocol）也可以用在这一层。但是，它们都必须被封装在IP数据报中。传输层只有两种协议可以选择：TCP协议和UDP协议（User Data Protocol，用户数据报协议）。传输层上面的应用层决定是使用TCP还是UDP。

使用TCP的应用层发送字节串，TCP程序将所发送的字节串按“段”（segment）分组。应用层不必考虑字节串的大小，因此TCP负责将这些数据按正常的顺序传输。

使用UDP的应用层必须知道被传输的数据块的大小。因为UDP不对数据进行分段，不管从应用层接收到的数据块有多大，UDP都直接把它传送给IP程序。如果数据块过大，超过了网络接入层的限制，IP层就必须对较大的数据报进行分段，变成较小的数据包。

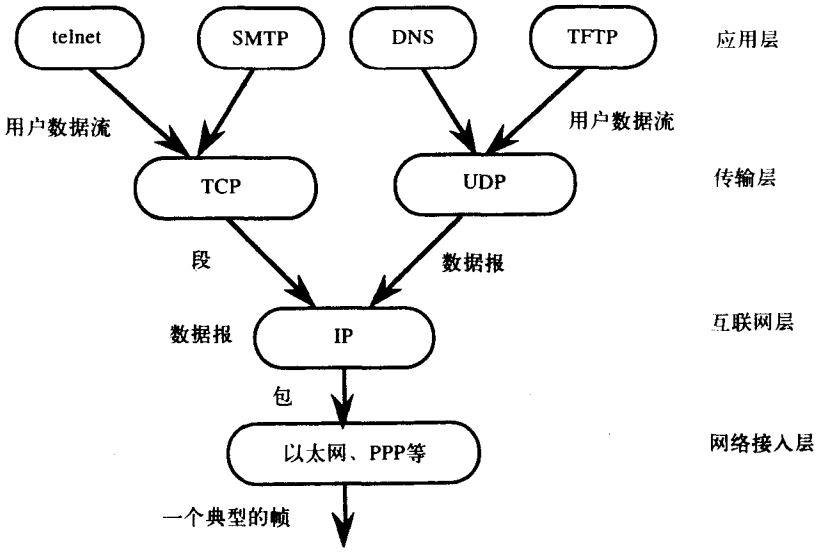


图8-18 此图显示了因特网的各种协议以及它们之间相互传输的数据单元。一个包可以是一个数据报或是一个数据报的分片

例如，包括头部的开销，以太网上允许的最大字节数是1500个字节。如果需要，IP层就会把数据报拆分成1500个字节的段。在实际网络上，允许的最大字节数被称为最大传输单元（MTU，Maximum Transfer Unit）。传输数据的实际网络的类型决定了MTU的取值大小，MTU取值的单位是字节。如果要在多个实际网络上传输数据，那么在这些网络当中MTU最小的网络决定了全部路径的MTU，即具有最小MTU的网络是限制最大数据传输单元大小的决定性因素。

2.6节介绍了IP数据报如何在因特网上传输；2.7节又讨论了面向连接和无连接的传输的区别。此外我们还讨论了隧道和封装技术。在继续学习之前，你可能需要复习一下这些内容。

8.6.2 网络接入层

因特网是由许多网络互连而成。事实上，这就是美国国防部（DoD，Department of Defense）支持TCP/IP发展的原因。因特网不要求所有的研究机构和大学购买新的计算机并运行相同的操作系统，只要安装了相应的协议，连接在网络上的主机可以是不同的类型、安装不同的操作系统、使用不同的连接方式（高速或低速）等。今天，这一切都成为了现实，各种类型的主机和网络都能与因特网相连。

从技术角度讲，网络接入层并没有在TCP／IP协议簇中定义。然而，这一层允许采用多种方式与因特网相连。图8-19说明局域网、广域网和专用连接都可以通过这一层与因特网连接。

如果从局域网接入或采用点到点协议（PPP，Point-to-Point Protocol），那么网络接入层包括两层。如果从X.25网络接入，网络接入层就包括三层，如图2-13所示。如果是SNA网络接入因特网，网络接入层就提供OSI七层模型中的所有服务。总之，不管采用什么样的网络，网络接入层都是这些网络与因特网连接的桥梁。

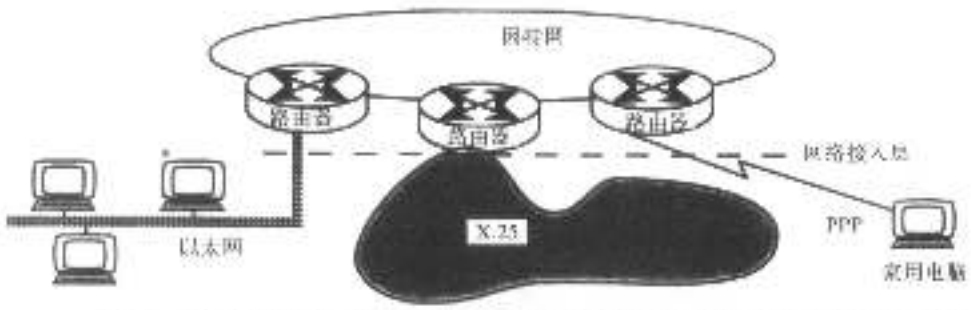
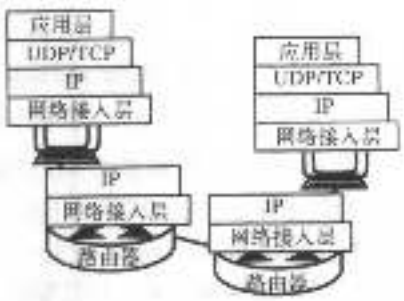


图8-19　因特网由许多网络互连而成。这些网络可以是局域网、广域网和专用接入线。网络接入层为网络的互连提供了各种方法

8.6.3　网际协议



下面使用表8-1来描述和比较三种协议：IP、UDP和TCP。从表中可以看到，典型的IP头是20B。IP被认为是数据报传输路径中所有主机都必须使用的协议。UDP和TCP被认为是端到端（end-to-end）协议。这些协议只由终端主机处理，也可以说由发送端和接收端主机处理，如侧图所示。

在2.6节和2.7节中讨论过，IP（网际协议）是无连接的协议。也就是说传输数据时不建立连接，只要有数据就可以送入网络，这也是处理IP数据报速度快的原因之一。在因特网上路由器必须使用IP协议转发数据包。属于同一个数据报或消息的所有数据包在传输过程中是彼此独立的，因为每个数据包的头部都含有目的IP地址。

表8-1　IP、UDP和TCP协议的比较

	IP	UDP	TCP
头部典型的字节数	20	8	20
协议数据单元(PDU)的名称	数据报	数据报	数据段
是一个端到端的协议吗?	不	是	是
是面向连接的吗?	不	不	是
处理速度快还是慢?	快	快	慢
能提供可靠的数据传输吗?	不能	不能	能
校验和包括头部吗?	包括	包括	包括
校验和包括数据吗?	不包括	包括	包括
必须使用校验和吗?	是	不	是
当发现错误时，重传吗?	不	不	不
发出重传请求吗? 是仅仅简单地丢弃PDU吗?	不	是	是

然而，这样传输数据并不可靠。可靠意味着不管是正面的还是负面的，都要有反馈信息。数据包可能会发生顺序颠倒、重复和丢失等错误，但这里没有请求重传的信息。如果数据包到达中间路由器的速度过快，就可能会被丢弃。当然，路由器会尽力转发数据包。正是由于这个原因，IP协议被称为是尽最大努力（best effort）提供服务的协议。但是，IP协议无法保

障数据包一定能够到达目的地址。当丢弃数据包时，IP协议将试着发送一条ICMP报文，告诉发送端这个数据包已被丢弃。然而，需要时TCP可以提供可靠的服务。

IP头中含有一个被称为头部校验和的域。这个域用来帮助主机检验头部是否出错。在数据报的数据域中没有任何校验方式。因此当一个数据包到达时，很可能是这个包到达了正确的目的地，但是所携带的数据存在错误。另一方面，如果头部不采取校验措施，那么数据包可能到达错误的目的地，白白地浪费了网络的带宽资源。传输数据包沿途的路由器只校验头部的错误信息，不对数据进行校验，这是IP协议处理速度快的另一个原因。此外，由于IP头通常只有固定的20个字节，因此处理开销较低。

在表8-1提到的三个协议中，如果发现一个PDU中存在错误，该PDU就会被丢弃。但是，如果在IP模块发现头部的错误信息，不会一声不响地丢弃，而是会试着将“ICMP参数问题”消息和错误数据报的头部返回给发送端。另外，数据报的前64个字节，也会被封装在ICMP报文中一起发送，这64个字节包含了其他各层的头信息。

UDP、TCP、ICMP和IGMP都检查数据错误，并且都采用IP协议来传送PDU。如果IP协议也检查数据错误，显得有些多余，所以IP不进行数据校验。

8.6.4 UDP

如表8-1所示，UDP仅有一个很小的头，共有8个字节，它也是无连接的协议。UDP工作速度快得益于两个原因，一个是与IP一样，UDP不关心可靠性问题。被传输的数据报不论是否被正确接收，都不传送反馈信息。如果一个应用需要可靠传输，必须使用TCP而不是UDP。然而UDP可以检查头部和数据域错误。如果发现错误，它仅仅丢弃数据报，而不产生任何重传的请求或错误报告。UDP中的校验和是可选项，但通常情况下总是使用校验和。

既然UDP是无连接的，不提供可靠性保障，或者说没有数据反馈信息，为什么应用还要首先选择UDP呢？使用UDP的主要目的是因为UDP提供了一种对应用的端口号进行编码的方法。该应用可能不需要连接，或者维护其自身的连接。换句话说，有时候可靠性可能不是应用关心的问题。例如，路由信息协议（RIP，Routing Information Protocol）就是使用UDP规则地发路由表。如果一次传输被丢失，还会有更多的传输到来。在这种情况下，为什么要为建立一个连接花费几个字节呢？在这个例子中建立一个连接所花费的开销要高于实际数据的传输。这就是为什么有时应用会倾向于使用UDP而不是TCP的原因。在IP上使用UDP得到的好处是可以获得数据的完整性和端口地址，同时它的处理速度要比TCP快。

8.6.5 TCP

如果一项应用仅仅考虑速度问题，那么UDP足以满足要求。然而TCP优于UDP的地方是，TCP能够提供面向连接的数据传输和可靠性。数据流能够按照正确的顺序到达目的地，错误可以被纠正，重复发送的数据可以被丢弃。如果一个应用需要多个服务，那么就一定要使用TCP。要获得TCP的这些好处，就必须花费比UDP更多的时间。此外，TCP头也大于UDP头。

从表8-1中可以发现，当TCP利用校验和检测到一个错误时，这个段就会被一声不响地丢弃，不发送任何出错报文，也就是说TCP不发送负面的信息。那么TCP是如何提供可靠性保障的呢？对于TCP，只发送数据包被接收的正面信息。当传输TCP模块发送一个数据段时，它同时会启动一个计时器，如果在一定的时间内没有接到正面的反馈信息，它就会重传这个数据段。

重传会导致到达目的地的TCP模块的数据段产生重复，删除这些重复的数据段是TCP的责任。另外，封装在IP数据报中的TCP数据段在传输过程中可能会发生顺序颠倒，按正常顺序排列这些数据段也同样是TCP的责任。

在传输数据之前，TCP会与目的地建立一个连接；在数据传输完毕之后，TCP会拆除这个连接。在连接建立和数据传输阶段，TCP协议会发送已经使用的缓冲区的大小，这样可以告诉TCP模块，有多少数据已经被发送但还没有收到返回的到达确认信息。如果TCP模块发送完了所有的数据，发送模块就必须等待，直到计时器超时。如果仍没有接到任何确认信息，就开始重传。TCP利用这个机制进行流量控制。

简而言之，TCP丢弃重复的数据段，对接收到的数据段进行排序，恢复丢失的数据段。TCP检测错误，但只有在没有发现错误时，才发送确认信息。没有经过确认的数据一定会被重传。TCP也能提供流量控制，换句话说，TCP提供了面向连接的服务和可靠的数据传输。

8.6.6 ICMP

用因特网控制报文协议（ICMP, Internet Control Message Protocol）传送的数据单元被称为消息（报文）。它的头部是固定的4个字节，数据部分的长度是可变化的。尽管一个应用可以既不使用TCP也不使用UDP来调用ICMP的服务，但是ICMP协议主要用来实现两个IP软件之间的通信。因为IP没有发送错误消息的机制，所以ICMP就被IP用于这个目的。另外，其他ICMP错误信息不会产生差错。否则一个错误就会产生更多的错误。为了进一步限制所产生的错误消息的数量，当几个数据段构成的一组中的一个数据段出现错误时，则只发送一条ICMP错误消息。在使用IP的地方，所有的主机中（也包括路由器）就都要使用ICMP。

错误消息：典型的ICMP为IP产生错误消息，这一点在前面已经提到过。一个ICMP错误消息包括头和出错数据报的前64个字节。接收这个信息可以帮助源主机找到出错的原因。但是ICMP只报告出错，而没有纠错机制。源主机在接到ICMP的出错消息之后，必须通知产生该数据报的应用来纠正这个错误。ICMP本身不能纠正错误。通常状况下是源主机引起错误而不是中间的路由器。另外，检测到一个错误时，只能使用数据报中的源主机地址。正是由于这样的原因，ICMP的错误报文通常只发送给源主机，而不发送给中间路由器。

错误消息只有五类。它们是："目的地不可到达"（不知道网络、协议、端口等等）；"源站抑制"（减慢到达某个源节点数据报的速度）；"超时"（数据分组可能在环路中发生阻塞）；"参数问题"（IP头出错）；"重定向"（通知源主机采用一个更好的路由）。

查询消息：除了错误报告之外，ICMP还发送查询消息（Query Message）。一般情况下，查询消息被分成两类：查询请求和查询响应。Ping就是一个利用ICMP查询消息的应用，被称为回送请求（Echo Request）和回送应答（Echo Reply）。利用Ping可以查看到一个主机的物理连接是否存在，这个主机是否在工作。通常，如果无法Ping通一个主机，那么到这个主机的所有网络应用（如telnet、ftp、DNS以及其他任何类型的应用）都不能工作。反之，如果一个网络应用能够在某个主机上工作，那么就一定能Ping通这个主机。这是因为Ping是最基本的检查连接是否存在、主机是否工作的方法。

但是，使用Ping方法将引起服务器上的安全漏洞，因此主机的管理员可能会禁止使用Ping。如果是这样的话，即使Ping不通，一个应用仍然可以工作；在这种情况下，即使应用工作，也可能Ping不通。

习题

8.1节

1. 最常采用的缩短二进制数字长度的计数系统是什么？

   a. 十六进制　　b. 八进制

   c. 十进制　　d. *e*进制

2. 利用第1题的答案，几位二进制数被缩减成下面的计数系统中的一个数？

   a. 2　　b. 4

   c. 10　　d.16

3. 101101可能在下面哪一种计数系统中出现？

   a. 二进制　　b. 十六进制

   c. 十进制　　d. 全选

4. 将十六进制数C0、A0、D3、49转换成十进制数，然后再转换成二进制数。

5. 将二进制数1011010111转换成十六进制数，然后再转换成十进制。并将十六进制数A09转换成二进制数和十进制数。

6. 在十六进制计数系统中，从1到100有多少个数？在同样的计数系统中，19、99、AF、3F、39和FF后面是什么数？40、C0、DD和500前面是什么数？

8.2 节

7. 一个MAC地址要与一个IP地址对应。在什么情况下，不发送ARP请求数据包？

8. 哪一种ARP数据包是单播数据包？

9. ARP请求在网络上传播是否经过路由器？说明理由。

10. 解释ARP表如何增加或减少？什么时侯增加或减少？

11. ARP协议的主要作用是什么？

8.3节

12. 下面哪一类地址不能被用作主机地址？

    a. A类　　b. B类

    c. C类　　d. D类

13. 将120.243.118.3转换成二进制，然后再转换成十六进制。

14. 最大的点分十进制数是什么？例如，在1024.893.0.260点分十进制数中哪一个数是无效的？

15. 假设一个B类地址以“10”开始，紧接着的10个比特是网络地址。如果IP地址的总长度是32个比特，存在多少个B类网络？每个网络能容纳多少个主机？

16. 登录网址www.arin.net/whois，查看谁的网络使用了地址129.117？这是哪一类地址？这个网络的主机地址范围是什么？

17. 中心授权机构分配以太网MAC地址和IP地址的方法有什么不同？

18. 使用地址分类的两个优点是什么？缺点是什么？

8.4节

19. 说明地址1101 0010 0110 1110 0001 1101 1001 0110 的类型、子网地址、广播地址和主机地址。如果使用子网，最后的4个比特用于主机，用二进制和十进制两种形式表示。这个子网有多少主机？这个网络的类型是什么？这个网络有多少个子网？使用这

种子网划分方案，总共有多少个可用的IP地址？如果不划分子网，又有多少可分配的IP地址？

20. 在什么情况下，需要增加主机比特数和减少子网比特数？在什么情况下做法相反？在什么情况下你不需要任何主机比特，或是说根本不划分子网？
21. 为什么要划分子网？
22. 假设可以支配的地址范围从198.8.234.0开始，到198.8.234.255截止。如果你需要创建20个子网，每个子网需要容纳5个主机。列出利用这种方案得到的前3个子网和最后一个子网的子网地址、子网掩码和广播地址。对第一个和最后一个子网，列出它们所有可能的IP地址。
23. 本题使用长度可变的子网掩码。假设分配给我们的网络是203.45.3.0，总部办公室的局域网上需要58个主机，另外的三个异地分部办公室通过广域网链路与总部相连，3个局域网分别需要容纳10、20和24个主机。给出子网划分方案，解释如何给不同的端口分配地址？使总部办公室局域网的子网地址为203.45.3.64,这样做有利于地址间的相互比较。
24. 继续上面的问题，假设有5个异地分部，对于每一个分部可用的IP地址为多少？解释如何给异地分部和广域网链路分配地址？

8.5节

25. 在数据报头中，哪一个字段规定了数据报中的数据部分是送给TCP还是送给UDP?

    a. 服务类型　　b. 目的端口号

    c. 协议　　d. 目的地址

26. Ethereal协议分析器的内容如图8-14中所示，其中间部分表示内容的是什么?

    a. 所选数据包的数目　　b. 数据包的目的

    c. 实际数据　　d. 数据字段的解释

27. 从以太网的数据包开始，各种协议利用哪一个字段来解释将数据部分转发给上层?
28. 对每个数据包的解码如图8-20所示。用本章所学的知识和图中给出的各种值，说明如果有一个值没有给出，那么在那一层标识的协议就是未知的。

8.6 节

29. 下面哪一层没有在TCP/IP协议体系结构中定义?

    a. 数据链路层　　b.应用层

    c. 互联网层　　d.传输层

30. 如果主机的TCP层接收的数据段中有一个错误，会如何做?

    a. 发送一个NAK。　　b. 要求发送进程减少窗口大小。

    c. 丢弃该数据段，并只是简单地等待数据段被重发。

    d. 把ACK标志复位成0。

31. 通过TCP／IP协议处理的所有数据必须由哪一层处理?
32. 说明传输层协议是不可靠的。
33. OSI参考模型和TCP／IP体系结构有哪些不同?
34. 哪一个应用必须使用ICMP报文?
35. 说出ICMP的5种错误报文的名称。

a)

```
0000  FF FF FF FF FF FF 00 00 C0 D3 DD 83 08 06 00 01
0010  08 00 06 04 00 00 00 00 C0 D3 DD 83 C0 75 B9 64
0020  FF FF FF FF FF FF 41 DA 6A EE BB B5 95 68 50 18
0030  7D 78 5D DA 00 00 FF FA 20 00 33 38 34 30 30 2C
```

b)

```
0000  00 00 0C D3 DD 83 00 00 0C D3 DD 53 08 00 45 00
0010  00 2C 00 01 00 00 40 06 8B 3A C0 99 B8 2C C0 99
0020  B8 21 04 2B 00 19 41 DA 6A EE BB B5 95 68 50 18
0030  7D 78 5D DA 00 00 FF FA 20 00 33 38 34 30 30 2C
0040
```

c)

```
0000  00 50 04 D3 DC 30 00 50 04 D3 DD 83 08 00 45 00
0010  00 38 30 BC 00 00 80 01 A8 03 C0 99 B7 64 C0 99
0020  B0 02 05 00 04 47 C0 99 B7 32 45 00 00 68 50 18
0030  7D 78 5D DA 00 00 FF FA 20 00 33 38 34 30 30 2C
0040
```

d)

```
0000  00 50 04 D3 DC 30 00 50 04 D3 DD 83 08 00 45 00
0010  00 38 30 BC 00 00 80 11 A8 03 C0 99 B7 64 C0 99
0020  B7 02 00 89 04 47 C0 99 B7 32 45 00 00 68 50 18
0030  7D 78 5D DA 00 00 FF FA 20 00 33 38 34 30 30 2C
```

图8-20 习题28中被解码的4个以太网帧

36. IP和UDP协议的相同点和不同点是什么?

37. 与TCP相比，UDP的优点是什么?

38. 与UDP相比，TCP的优点是什么?

第二部分 语 音 网

第9章 信 令

9.1 什么是信令

想像一下如果我们只拥有身体的各个部分及其各种器官，但是没有神经系统，那么我们就无法指挥腿来走路，甚至无法完成一些最简单的动作，这就如同瘫痪了一样。类似地，从一个非常简单的意义上讲，在一个连接了许多复杂的数字交换机的电话网络中，如果交换机之间没有确定的通信方法，这个网络没有任何用处。因此，信令被认为是网络的神经系统，它使网络的两个节点能够交换控制信息。这些控制信息可以用于建立、维护或是拆除一个连接。

9.2 一个呼叫的连接过程

9.2.1 发起呼叫

利用图9-1，可以概括地说明完成一次局间呼叫的步骤。在这里的“局”指的是中心局（CO，Central Office）。在电信业，术语端局（EO，End Office）通常是指用于处理呼叫并与电话机直接相连的交换设备，在这里我们把它们都简称为CO。

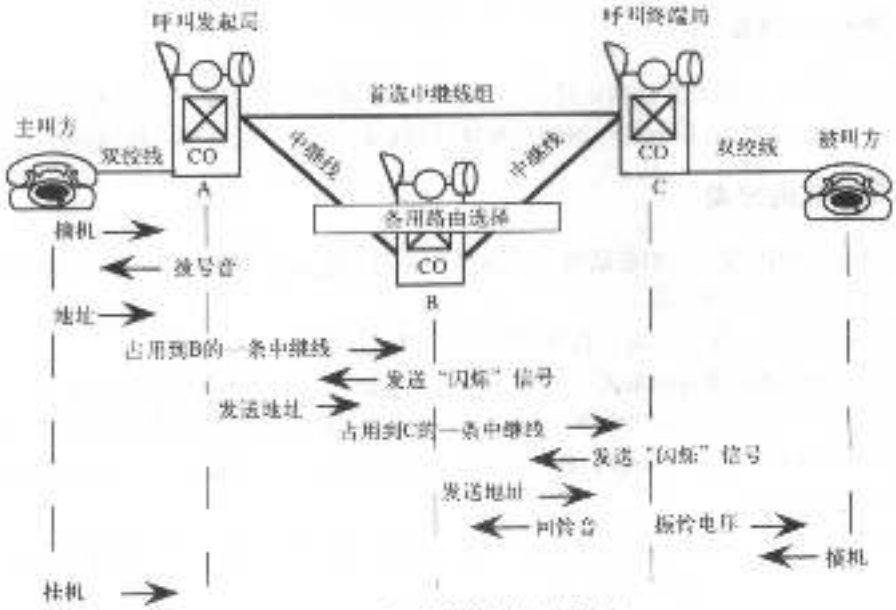


图9-1 局间中继线上的交换信令

首先，主叫方拿起电话机，摘机这个动作通过双绞线形成了一个电路。这时电流开始流过，CO中的交换设备可以检测到这个电流；然后CO会给这条线路接通一个寄存器，用于存储用户拨打的电话号码；之后交换设备会提供一个拨号音，通知主叫方开始拨号。

当挂上电话时，没有来自CO的电流，这时被称为闲置状态。相反摘下听筒，就会产生电流，被说成处于繁忙状态或者是占线状态。

9.2.2 呼叫路由

中心交换局A（用CO-A表示）研究其路由指南，发现被叫方与CO-C连接。路由指南还指出到CO-C的直接相连的中继线是这个呼叫的第一种路由选择。然而，由于所有的与C直接相连的中继线都已经被占用，CO-A需要再次查找路由指南，发现了另一种路由选择：利用到CO-B的中继线群。

CO-A找到并占用一条空闲的中继线与CO-B连接；CO-B将一个寄存器与这个电路相连，并且发送一个“闪烁”信号，这个信号相当于在挂机之后又拿起了听筒的动作，这意味着CO-B已经准备完毕，CO-A可以发送主叫方所拨打的电话号码了。

从接收到的号码，CO-B了解到被叫方并没有直接与自己连接。因此，与CO-A获得和CO-B连接的方法相同，CO-B建立与CO-C的连接。CO-C经过查询之后，知道被叫方与自己直接相连，不需要再与其他的CO建立连接。当被叫方空闲时，CO-C向被叫方的话机发送振铃电压信号，同时CO-C还将一个回铃音回传给主叫方。

9.2.3 应答监视

当被叫方拿起听筒接听电话时，CO-C就停止发送振铃电压信号和回铃音信号。这时一个摘机信号，又被称为应答监视信号，被传送给CO-A。这样CO-A就可以知道被叫方已经接听了电话。如果有必要，通话计费开始，这个呼叫连接就被建立起来了。

9.2.4 拆线和呼叫清除

如图9-1所示，主叫方先挂断电话，当然也可以是被叫方先挂断电话，这个阶段称为拆线阶段。在呼叫清除阶段，所有的中继线都恢复到原来的空闲状态，CO-A也同时停止计费。

9.3 信令格式的分类

信令只有两种状态，比如电话听筒的摘机和挂机、电流的有无、某个频率信号的存在与否等等。信令提供了监视功能。

当电话号码出现在信令中时，信令提供的是寻址信令功能。

信息信令以音调或录音的形式来实现其功能，比如“……这个号码无法接通。”

拨号音由350Hz信号和440Hz信号构成；回铃音由440Hz和480Hz的信号组成；忙音或者占线音是480Hz和620Hz信号每秒间断地组合。记录音或所有中继线忙音与占线音相同，但发送频率是占线音的两倍。

提醒功能由振铃、闪跳或者接收端摘机信号完成。振铃信号是一个90V的交流电压，频率为20Hz，可以使电话机的振铃器发出响声。在一般情况下，振令信号的铃声持续2s，然后间断4s。

在连接刚刚被建立之后，用户端会发出一个闪跳信号，这个信号相当于用户刚刚挂机又立刻摘机。由于挂机的时间非常短暂，交换机不会错误地理解成拆除连接。闪烁信号使拆线员可以从线路上得到反馈，以便通知PBX（用户交换机）下面是特殊功能码或一次呼叫。

9.4 信令延时和局间信令

在处理网络上的呼叫时，会出现三种类型的延时：拨号延时、应答延时和拨号后延时。拨号延时是指从听到拨号音开始到拨出电话号码的最后一个数字为止所花费的时间。使用双音频拨号方式来代替过去的脉冲拨号方式有助于减少这种信令延时。应答延时是指被叫方从听到第一声振铃开始到被叫方摘机所需要的时间。

最后，拨号后延时或振铃延时是指上述这两种延时之间所占用的时间，是指从主叫方拨完最后一个数字开始到被叫方电话铃响起为止所花费的时间。

9.4.1 单条中继线信令

现在回过头来再看一下图9-1，如果从CO-A到CO-C有一条直达中继线，时延就比较短。相反地，如果一个呼叫不得不通过多个交换机，那么延时就会增加。这是因为位于呼叫所经线路上的所有交换机都必须分别对呼叫进行交换处理。例如在图9-1中，CO-C要等到CO-B从CO-A接收到电话地址之后才可能开始进行交换处理。

在图9-1中所描述的信令是单条中继线信令，也称为随路信令 (CAS，Channel Associated Signaling)。随路意味着所有的信令（如监控信令、寻址信令、信息信令和提醒信令等）都与语音信息使用同一个物理路径来传送。

9.4.2 公共信道局间信令

现在电话运营商都采用公共信道局间信令 (CCIS，Common Channel Interoffice Signaling)。从本质上讲，它与随路信令是完全不同的。公共信道局间信令的本质想法是避免使用价格昂贵的语音级中继线来传送信令，而是把信令传送从语音路径中分离出来，利用另外一个完全不同的网络来传送信令。进一步说，由于信令基本上是表示摘机还是挂机的状态、地址信息之类的数据，因此信令网可以采用分组数据网。

图9-2显示了三台交换机是如何通过公共信道局间信令(CCIS)彼此建立连接的。在这里，语音路径与信令路径是分开的。在信令网中使用信令传输节点 (STP，Signaling Transfer Point)来为信令分组确定合适的路由。如果CO-A要建立一个呼叫连接但发现到CO-C没有中继线可用，就会注意到到CO-B存在空闲的中继线。这时CO-A会将它要连接的目的电话号码发送给STP。当STP网络发现目的电话机是空闲的并可以进行通话之后，沿途所有的交换机都被指定并且同时得到一个建立到CO-C的话音路径的通知。在完成对这条语音信道的连续性检测之后，振铃信号被激活。

由于STP对网络的运行起着关键性的作用，因此它们通常是成对使用的。这样即使其中的一个出现故障不能工作了，另一个也能够承担起所有的信令业务。7号信令系统（SS7，Signaling System 7)是当前正在使用的CCIS系统。有关这个问题，将在第18章中作详细介绍。由于7号信令系统是一种分组交换网络，因此我们把它留在本书的后面进行讨论。

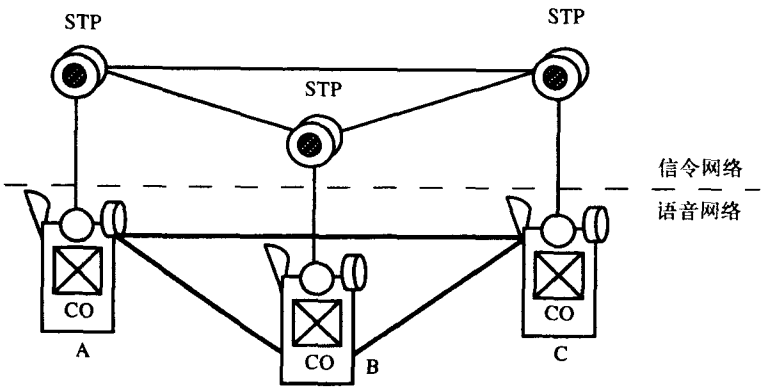


图9-2　CCIS使用一个与语音网络相分离的数据分组网络。STP（信令传输节点）是构成信令网络的分组交换机

9.4.3　CCIS的优点

CCIS有许多优点。首先，在CCIS中的拨号后延时被大大地缩短了。在一个LATA内，最后一个号码一被拨出就可以立即建立起连接。一个越洋呼叫的典型延迟时间是4s，这与采用随路信令需要20s的延时时间相比较要少很多。

另外，与以前相比，不再需要那么多的话音中继线。因为话音中继线现在只是处理话音，从而减少了每一个呼叫占用话音中继线的时间。对于随路信令系统，被叫方的交换机负责提供话音中继线上的忙音信号。但是对于CCIS，在这种情况下话音中继线根本无法使用。这时，远方电话占线的信息会通过信令网络中继给主叫方的交换机，然后再由主叫方交换机向话机发出忙音信号。

早期引入CCIS的一个原因是希望提供800号服务。但从那时起，CCIS逐渐成为提供电话卡、虚拟网络、ISDN和其他新型的复杂服务必不可少的工具。

信令网络作为一种分组交换网络，传输数据的效率非常高。每一个话音线路不需要拥有自己的信令链路，所有电路的信令都通过一条从交换机到STP的公共链路来处理。

这就是CCIS被称为公共信道信令的原因。对于所有呼叫的信令信息都在这条公共信道上传输。与CCIS不同的是，随路信令系统中每对交换机之间，每一个呼叫的信令都在不同的信道上传输。

9.5　地址信令的类型

9.5.1　拨号脉冲

采用旋转拨号盘来产生拨号脉冲是传统的产生呼叫地址（电话号码）的方法。一旦电话摘机，就会收到一个拨号音，这时就可以开始拨电话号码的第一个数字了。在图9-3中，被发送的数字是4和2。线路断续的次数决定了拨出的数字，由于中断的时间非常小，只有大约60ms，因此交换机不会注意到这些短暂的断线信号，从而也不会断开与话机的连接。拨号脉冲中断比，被定义为断开的时间与一个脉冲周期占用时间的比值，这个值在通常保持在60%。

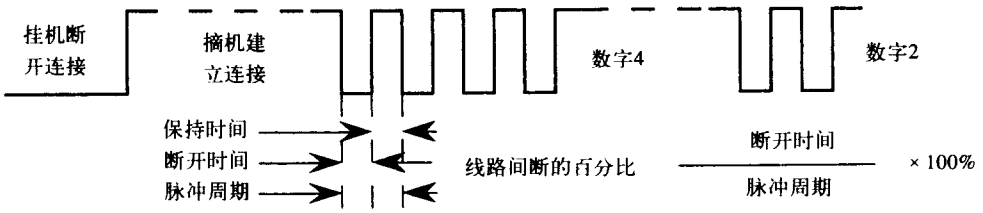


图9-3 典型的旋转拨号脉冲序列

尽管拨号脉冲从波形上看像是一个数字信号，但是拨号的速度很慢，且拨号延时的长短取决于所拨出的数字。拨打“0”这个数字需要10个脉冲，由于每个脉冲周期为100个ms，所以拨打“0”这个数字就要花费1s的时间。

9.5.2 双音多频信令

对于音调信令或者说是双音多频(DTMF,Dual-Tone MultiFrequency)信令，所有被传输的数字都具有相同的延迟，大约为120ms。如图9-4所示，这些数字被放在一个矩阵中。在这里，每拨一个号码都会激活两个不同的信号发生器，一个用于决定拨打数字所在的行，另一个用于决定拨打数字所在的列。例如：当拨“1”时，1209Hz和697Hz的音频信号被叠加并被发送。

1	ABC 2	DEF 3	11	697 Hz
GHI 4	JKL 5	MNO 6	12	770 Hz
PRS 7	TUV 8	WXY 9	13	852 Hz
*	OPER 0	#	14	941 Hz
1209	1336	1477	1633Hz	

图9-4 DTMF使用一个由行频和列频组成的表格为每个数字分配一对频率，11~14目前还未被使用

DTMF提供了两个在旋转拨号中找不到的字符，它们是“*”和“#”，但是仍然没有英文字母“q”和“z”。在最右边一列的四个位置上，还没有定义所代表的字符，可以预留给其他的一些特定目的的应用。

表面上看上去，所使用的频率是随意选取的。但是实际上，选择这些频率可以最小化由于谐波和语音干扰而导致的假信令。假信令是由于意想不到的原因而引起的对控制信令的错误理解。

DTMF降低了拨号延时，特别是减少了预先存储号码的拨号时间。它使用固态设备，因此也减少了交换机所需要的设备数。同时它还能与现代的电子交换机相兼容，并且能提供端到端的信令。

端到端的信令允许一个电话机与电路被叫端的计算机相互联系。没有DTMF，第9章所讲到的语音处理应用就不会像今天这样先进。简而言之，DTMF使一个普通的电话机能够具有计算机终端的功能。

9.5.3 多频信令

DTMF用于用户线，而多频（MF,MultiFrequency）信令则是用在交换机之间或者是局间中继线上。MF信令出现在DTMF信令之前，现在已经逐渐被7号信令系统所取代。它是把6个可能频率中的2个组合起来使用。从表9-1中看到，这些频率是如何被使用的。在MF信令中，

由于人类的话音可能与这些控制信令相似（出现假信令），因此增加了音调的时间间隔。另外，在号码的数字被传输之前，由2个频率组成起始地址信令先被发送；在传送完号码数字之后，还要发送由另外2个频率组成的结束地址信令。

表9-1　MF 频率对分配表

频率（Hz）	数　字	频率（Hz）	作　用
900+700	1	1700+700①	投币呼叫控制的回铃
1100+700	2	1700+900①	延迟操作
1100+900	3	1700+1100①	地址开始
1300+700	4	1700+1300	转接码
1300+900	5	1700+1500	地址结束
1300+1100	6		
1500+700	7		
1500+900	8		
1500+1100	9		
1500+1300	0或10		

① 表示这些频率的结合还有其他的功能。

9.6　提供监视功能的信令类型

9.6.1　单频信令

与仅仅提供描述信息的地址信令方式不同，单音频(SF，Single Frequency)信令用于交换通、断状态，或者是用于提供监视信令。对于SF，当一个用户线空闲时，就会发送一个连续的音频信号；如果这个连续的信号中断了，那么CO就认为这个用户正在占用这条线路。如表9-2所示，如果CO提供了一个音频信号，这将解释为振铃现象；如果没有这个音频信号，则被认为是空闲状态。此外，如果音频信号随拨号脉冲的通、断而变化，SF也能提供地址信息。

表9-2　SF（单频）工作方式

	从用户线到CO	从CO到用户线
有声音	空闲	振铃
没声音	占线	空闲和忙

DTMF、MF和SF信令是独立于传输设施的信令格式，也就是说这些信令可以通过双绞线、同轴电缆、微波、光纤或其他任何形式的传输介质进行传输。而拨号脉冲则是依赖于传输设施的信令，它只能通过两端直流电压为－48V的双绞线进行传输。拨号脉冲也属于直流信令的一种，它必须有直流电压和直流电流才能工作。下面要介绍的信令——环路启动信令和接地启动信令也属于直流信令。

9.6.2　环路启动信令

在分析带有直流（DC）环路电流的电路时，要牢记交流（AC）信号可以叠加到直流电压之上。拨号音、双音多频信号和语音信号都属于交流信号。如果在电路中使用电容器，对于直流信号这个电路相当于开路，而对于交流信号则相当于短路。这样描述的目的是为了更好地研究直流环路电流，而不考虑可能存在的交流电压。

环路启动信令通常用在住宅环路或者说用户环路中，它只需要一对电线。这对电线中的一条被称为T线（tip），另一条被称为R线（ring）。

图9-5a所示是一个处于挂机状态的电话机。注意此时话机中的触点是断开的，任何方向都没有电流流过。没有电流流过，这意味着3个电阻的两端电压为0。因为电压等于电流与电阻的乘积，3个电阻上的电流为零，所以电压也为零。进一步讲，这对导线T线的电压为0V，R线的电压为－48V。

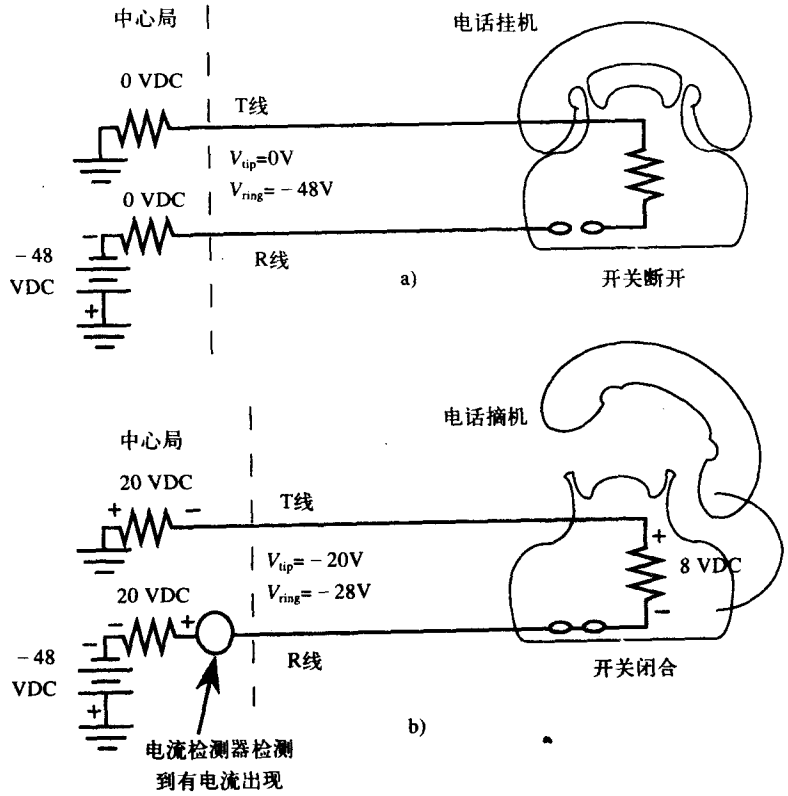


图9-5 a) 在环路启动信令中，当电话挂机时，没有电流流过，R线两端的电压为－48V。 b) 当电话摘机时，有电流流过，R端的电压为－28V。CO注意到在环路中检测到电流，会连接一个数字接收寄存器并发出拨号音

图9-5b给出了一个处于摘机状态的电话机，这时话机内的触点闭合，形成了电路，电流可以在环路中流动。在CO端，T线和R线上的电压都是20V，在电话机两端仅有8V的直流电压。CO一旦检测到直流存在，就会为这个电路分配拨号音频发生器和数字接收器。所有的交流电压都叠加在直流电压之上。

当一个呼叫到来时，电话机就会接收到一个90V的交流振铃电压信号，该电压叠加在直流电压之上并且使振铃器振铃。

9.6.3 接地启动信令的优点

接地启动信令使用直流环路电流和一对与环路启动信令相似的双绞线。但是，接地启动信令主要用于PBX而不是用户环路。在PBX中使用环路启动信令就会带来一些问题，如果使用接地启动信令这些问题就不会出现。首先我们要弄清楚一个定义，就是在CO和PBX之间的接地启动线，在PBX一侧被称为中继线，而在端局一侧，被称为链路。

假设一个没有检测拨号音功能的PBX在环路上发送了一个摘机信号，那么它必须等待预

先规定的一段时间之后才能开始拨号，这是为了有足够长的时间接收拨号音。但是在某些特殊的情况下，如果CO还没有发送拨号音，也没有准备好接收所拨叫的数字，那么拨出的号码就可能丢失。使用接地启动信令，就可以解决这个问题。

如果在一条线路上，接收到的振铃信号是以持续4s的静音开始，而不是以持续2s的铃声开始，同时PBX又占用了那条线路来建立呼叫，那么这时两个主叫方就会建立一个意想不到的连接，被称为主叫对峙（glare）。这在使用环路启动信令的家用电话系统中常常见到。然而在商业环境中，不希望出现这种现象。使用接地启动信令，CO提供一种主动占用中继线的方式。

接地启动信令的最后一个优于环路启动信令的优点是，前者提供了应答监督的功能。这意味着如果远端用户挂机，而PBX还在保持这个连接的话，CO就会通知PBX中继线已经处于空闲状态，可以把它分配给其他的呼叫连接使用。

9.6.4　接地启动信令的操作

图9-6a给出了接地启动信令系统中的空闲状态，图9-6b和图9-6c显示了如何完成一个去话呼叫，图9-6d和图9-6e显示了如何接收一个来话呼叫。注意在环路启动中，使用的是一个双掷开关，而在这里则使用两个三掷开关。

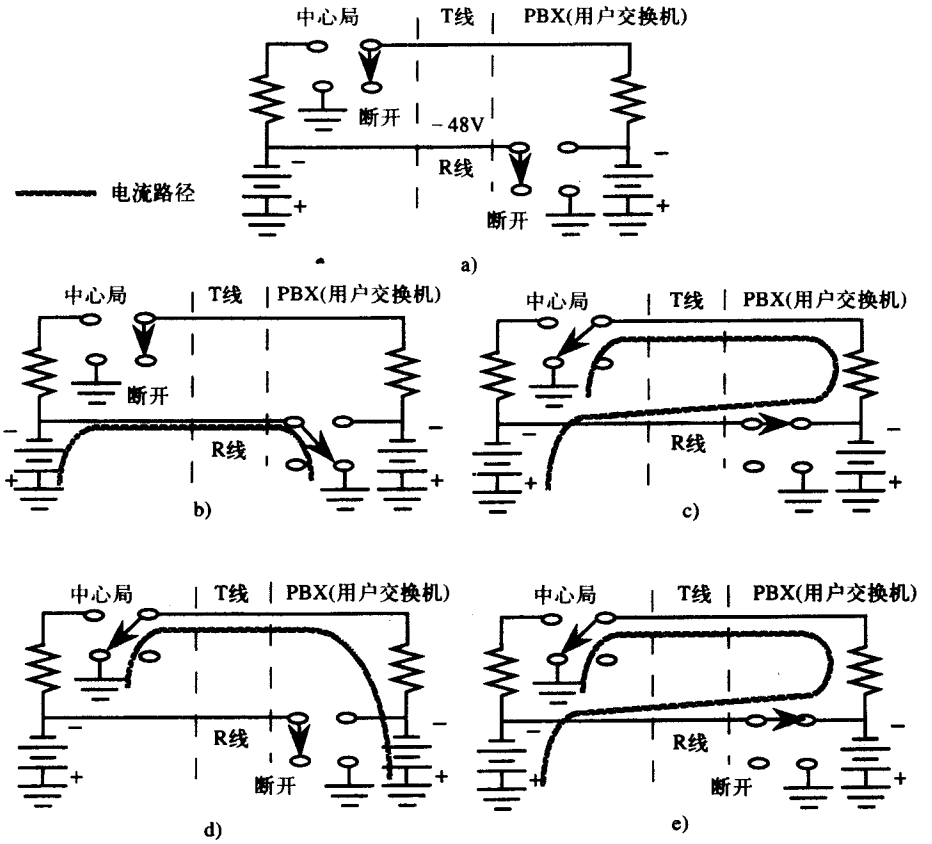


图9-6　接地启动的工作方式。a) 当线路空闲时，CO的T线和用户端的R线是断开的。b) 在发起一个去话呼叫时，用户使R线接地。c) CO检测到变化，使T线接地，然后用户完成环路。d) 在接收一个来话呼叫时，CO首先使T线接地。e) 然后由用户完成环路

在空闲状态下，由于两个开关都是断开的，因此两组电池都不产生电流。在图9-6b中，PBX正在通过将R线接地发起一个呼叫，这样就会有CO可以检测到的电流在R线中流过。这时CO意识到PBX已经处于“摘机”状态，就会为之连接一个数字接收器，并发出拨号音，同时把CO端的T线接地。在T 线上形成的电流又会被PBX检测到，这样一来PBX也就知道CO已经准备好接收数字了。这时PBX会首先把R线上的环路接通。现在一个环路已经建立起来了，可以开始拨号了。

现在来看一下在线路空闲之后，PBX如何接收一个来话呼叫。如图9-6d所示，CO把它的T 线接地以此来通知PBX有一个来话呼叫到达。

这时PBX注意到在T 线上有电流出现，它就会限制其他呼叫使用那条有来话呼叫的线路。在PBX检测到振铃电压之后，它会在T线和R 线之间形成一个闭合环路，如图9-6e所示。

CO检测到环路闭合以后，会终止振铃信号，并提供到PBX的语音路径。如果远端用户首先挂机，CO将断开T线，当这个动作被PBX检测到之后，PBX也会断开R线。

另一方面，PBX也可以首先断开R线来终止这个呼叫，这样就可以使环路电流变为零。CO检测到这种情况之后，也会断开T 线，使线路就恢复到先前的如图9-6a所示的空闲状态。

9.7 数字载波系统

信令本质上是数据，所以很自然地会用比特对其进行编码。我们已经看到，存在电流或某一种频率的信号可以代表一种含义，不存在电流或某个频率的信号则可以表示另外一种含义。类似地，在数字载波中，如在常见的T1系统中，任何信令功能都可以通过将某些比特设置成“1”或“0”来实现。携带这类信息的比特被称为信令比特，把所有的信令比特都集中到一个语音信道中时，这个信道就称为信令信道。

9.7.1 夺位信令与无干扰信道信令

从表9-3的倒数第二行可以看到，对于T1系统不存在单独的信令信道；而在欧洲的E1系统存在单独的信令信道。这是因为在T1系统中，在任何一条给定的话音信道上，每48个话音比特中就会有一个话音比特被信令比特所占用，然而这些临时丢失的话音比特并不会被人耳所觉察。因此在T1系统的64kbps的话音信道中，不仅包含话音比特，还包括信令比特。由于这些信令比特实际上“抢占”了某些话音比特的位置，所以被称为夺位（robbed bit）信令。

表9-3 TI和E1 格式的比较

（带宽= 每秒比特带宽）	T1	E1
每个话音信道的带宽	64k	64k
话音信道的总数	24	30
所有话音信道占用的总带宽	1536k	1920k
每帧信号占用的带宽	8k	64k
独立信令信道占用的带宽	–	64k
载波系统的总带宽	1544k	2048k

另一方面还可以看到，在E1系统中存在一条单独的只传输信令的信道。这是因为E1系统的信令比特并不抢占话音比特的位置，在64kbps的话音信道中只传送话音信息。

所有30路话音信道的信令被集中在一个单独的64kbps的信令信道中传送。由于信令比特

不出现在话音信道中，因此认为信道是无干扰的，即E1提供无干扰信道（clear channel）信令。不论是国内还是国外，ISDN呼叫都使用这种无干扰信道信令。

9.7.2 公共信道信令

公共信道信令有两种含义。如图9-2所示的公共信道局间信令，提供了一个独立于话音网络的信令网。从交换机到相应的STP对的链路是一条公共链路，可用于承载与给定交换机相关的所有话音电路的信令信息。

在E1系统中，我们可以了解到什么是公共信道数字信令。30组不同话音信道的信令与它们的话音信道相分离，构成了一个公共信令信道。在第10章中会看到，另外一种被称为M44格式的T1系统方案，也使用无干扰信道和公共信道数字信令技术。

9.7.3 带外信令和带内信令

夺位信令也被称为带内信令，因为信令比特占用了原来计划用于传出话音的比特，即带内比特。同样，如果信令比特不占用语音比特进行传输，这种信令比特被称为话音比特之外的“带外信令”。因此带外信令与无干扰信道信令的含义相同。

有时一个数字网络管理信道伴随话音信道一同发送，以实现误差统计和其他一些功能。在这种情况下，这个管理信道也被称为带内信道（尽管这个管理信道不是在话音信道中发送的，而是在其他不同的介质中发送的）。这种情况将在第10章中介绍。

在这里所描述的是带内和带外数字信令方式，注意不要与带内和带外模拟信令方式相混淆。

在一条通常的话音级线路上，300Hz ~ 3300Hz的带宽就可以满足传输话音的要求。使用这个频率范围的任何信令都被称为带内（模拟）信令。MF、DTMF和SF信令使用的频率都在这个范围之内，所以它们都被认为是带内模拟信令方式。已经过时的N1载波系统使用3700Hz的信令信号，超出了话音带宽的范围，因此它是带外模拟信令的一个例子。

9.8 信令接口

到目前为止，我们已经知道信令信息可以在各种传输介质上传送。在本地环路中，使用金属线或铜线来传送直流环路电流。另一方面，在各个交换局之间大多使用MF信令。如果交换局之间使用微波或光纤来连接，就不能发送直流电流信号，而只能发送模拟或数字信号。

为了使信令系统之间能够相互转换，必须在信令系统之间使用接口。换句话说，接口就是一种特定的设备，该设备利用一种技术使两个不同的传输介质或信令系统互相沟通。

9.8.1 四线端接装置

在中心局（CO）处，2线的用户线使用四线终端设备（4WTS，4-Wire Termination Set）与具有4线的金属介质相连，如图9-7所示。本地环路采用2线电路比较经济，但是它只能用于短距离传输。4线电路需要两对导线，一对用于传输（图中的T和R），另一对用于接收（图中的T1和R1）。4线结构提供了较好的传输质量，并且可用于长距离传输。与本地环路不同，在长途传输介质上，不同方向的信息是分开传输的，所以4WTS在这里被用作接口。4WTS也被称为混合电路，它仅仅提供了2线电路到4线电路的接口。

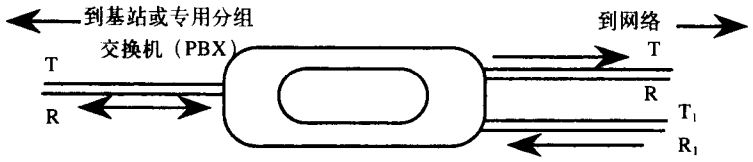


图9-7 4WTS或混合电路用于转换1对线与2对线的连接。在1对线上，接收端和发送端共享同一对导线，而对于混合的2对线，发送和接收信号是彼此分开的

9.8.2 接收和发送（E&M）信令接口

在金属介质设备和模拟介质之间常用的接口被称为接收和发送（E&M）接口。这个接口用于直流环路电流信号到带内模拟信令信号间的转换。它专用于PBX之间的连接中继线。“e”表示接收端(rEceive或Ear)中的“e”，而“m”表示发送端（transMit或Mouth）中的“m”。SB和SG分别代表信号电源(Signal Battery)和信号地(Signal Ground)。

图9-8给出了2个PBX之间的4线连接中继线。在这种情况下，连接中继线被认为是一个模拟传输介质。通常，在每一个PBX中都有一个E&M接口。这个接口包含一个金属介质终端（MFT，Metallic Facility Terminal）和一个模拟介质终端（AFT，Analog Facility Terminal）。图9-8给出了空闲状态下接口的状况，这时在任何一端都没有电流，在连接中继线上也没有SF信号。

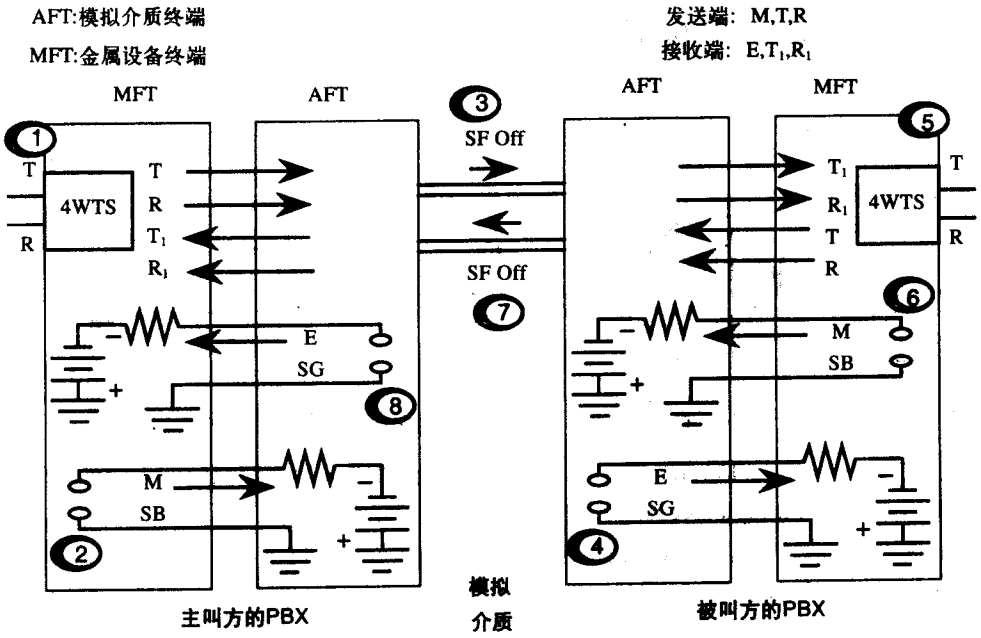


图9-8 对于空闲的4线连接中继线，E&M信令接口的各种状态。(1) PBX找到一个空闲的中继线，来发起一次呼叫。(2) M端闭合，电流流过。(3) SF信令被传输。(4) E端闭合产生电流。(5) 被叫方的PBX准备好接收这个呼叫。(6) M端闭合。(7) AFT回传SF信号。(8) E端闭合，现在所占用的中继线可以用来传输拨叫的号码

如果主叫方的PBX要替它的某个用户发起一次呼叫，并且已将拨打的号码存储在寄存器中了，它就需要一条连接中继线来传递这个呼叫。接下来介绍占用中继线的过程，并解释图

中用数字标记的各个步骤。

第一步，完成2线到4线的转换；第二步，MFT提供一个闭合环路连通M和SB端，这个环路中产生的电流被AFT检测到；AFT随即在连接中继线上产生一个SF信号。回想一下直流电流不能被长距离地传输，所以在这个模拟介质上选用SF信令，这是第三步。

第四步，要求被叫方PBX的AFT能够检测到SF信令。然后在第五步中，被叫方的PBX接通E和SG端形成环路，产生的电流可以被其MFT检测到，从而使PBX连接上一个寄存器来接收拨叫的号码。完成这些工作之后，就是第六步，M和SB端被连通。

第七步，AFT注意到这个电流，发送一个SF信令。这个SF信令能被主叫方PBX的AFT设备检测到，从而闭合E 端环路，使电流从这里流过。最后在第八步中，当MFT检测到电流之后，主叫方的PBX通过它的T端和R端发送存在寄存器中的拨号数字，被叫方通过T1和R1端接收这些数字。

一旦远端PBX建立了到相应电话机的连接，通话就在T、R、T1和R1端之间进行，这时信令的连接阶段也就结束了。

9.8.3 数字信令接口

图9-9解释了传统的模拟信令如何与T1的数字信令相互连接。这里，一条T1专线将PBX和远端的一些电话机连接在一起，这些电话机就好像是这个PBX系统的一部分。PBX端的信道处理单元接收多达24个来自PBX的话音信道，并把这些信道复用在数字T1载波，远端的信道处理单元工作过程相反。

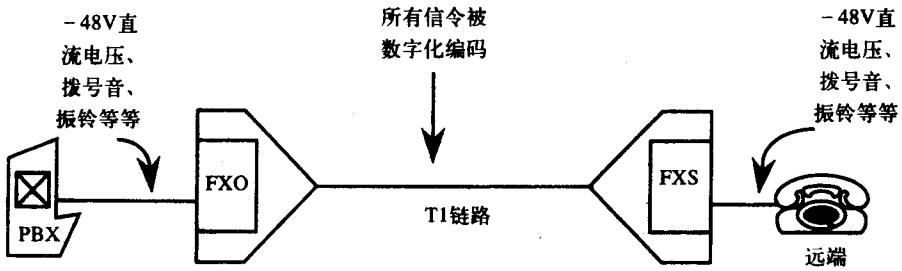


图9-9　给出了类似于T1的数字载波的电路。在这里所有的模拟信号都被转换成特定的“0”、“1”模式

外部交换局（FXO，Foreign eXchange Office）在PBX端形成模拟到数字转换接口，而外部交换用户(FXS，Foreign eXchange Subscriber)是远端的接口。

在电话空闲的时候，在PBX的线路板为其信道处理单元提供－48V的直流电压，并且FXO把话音信道的信号转换成“0”、“1”格式的数字信号，以便在T1信道上传输。远端的FXS识别出接收到的“0”、“1”格式信号，就会提供－48V的直流电压给远端电话机。在这个方法中，PBX认为有一个电话机直接与之相连，而电话机则认为有一个PBX电路板直接与之相连，而实际上它们之间的信令已经变成了数字形式，并且是通过T1传输的。

现在，如果远端的电话摘机，FXS接口就会检测到这个信号，并会通过T1系统发送一组由1和0组合的特定模式的信号。这个信号如同对PBX形成了闭合环路，就好像电话摘机一样，由FXO负责解释。这时PBX会提供一个拨号音，而FXO将其转换成另外一种格式的数字信号；而FXS依次再将这个数字信号转换成在电话机中可以听到的拨号信号。

用这种方式，FXO和FXS接口完成端点的模拟信令和T1载波的数字信令之间的转换。在

前面讨论的E&M接口中，可以很容易地看到在一个数字传输介质上如何用数字“1”来代替SF信号，用数字“0”来表示无SF信号，因此数字信令接口容易组合，可以用来替代许多类型的模拟信令。

习题

1. 主叫方摘话机时，可以说成:
   a. 提供应答监督　b. 占线　c. 进入后拨号模式　d. 发起呼叫寻路
2. 挂机后立即摘机的情况可以被称为什么?
   a. 一个数字　b. 断开连接　c. 监督　d. 闪烁
3. 本章中没有提到下面哪一个信令功能?
   a. 监督　b. 信息　c. 测试　d. 提醒
4. 下面哪一个信令是介质独立的信令?
   a. 环路启动　b. DTMF　c. E&M信令　d. 接地环路启动
5. 2线和4线信号间的信令转换采用什么设备?
   a. E&M信令的E端　b. E&M信令的M端　c.普通话机　d .4WTS
6. CO让与之连接的PBX知道远端已经挂机，这种情况被称为什么?
7. 当话机摘机过久时，从电话机上可以听到的声音很大的一个脉冲音，这是哪一种信令功能?
8. 拨号延时和应答延时之间的时间间隔被称为什么?
9. 拨号和应答延时之间的时间如何通过载波减少?
10. 用于MF信令的频率对的总数是多少? 它们当中有多少已经被使用?
11. 在传输中有一种信令比特占用话音比特的位置，请说出这种信令的两种叫法。
12. 说明当CO-A和CO-C间的一条中继线空闲时，如何建立局间呼叫。
13. 不同类型信令的功能是什么? 它们的意义是什么?
14. 解释CCIS为什么优于随路信令。
15. 如果你可以为图9-4中的最后一列频率对定义4个字符，你将选择哪4个字符? 为什么?
16. 解释接地启动信令优于环路启动信令的原因。

第10章 交　换

10.1 交换的基本原理

10.1.1 为什么要交换

如果有4个家庭希望彼此能互相沟通，在没有交换机的情况下，他们不得不如图10-1a所示的那样进行连接。每一个家庭需要三部电话分别与其他的三个家庭进行通话，而且这三部电话的线路也都是相互独立的。想像一下如果整个城市以这种方式组成电话网会是什么样子！每当一个家庭要与一个新地点的用户进行通话时，电话局就不得不铺设一条新的线路，并且在两端各安装一部电话。这样一来仅仅是标记每一部电话的通话对象就是一项工程浩大的任务。

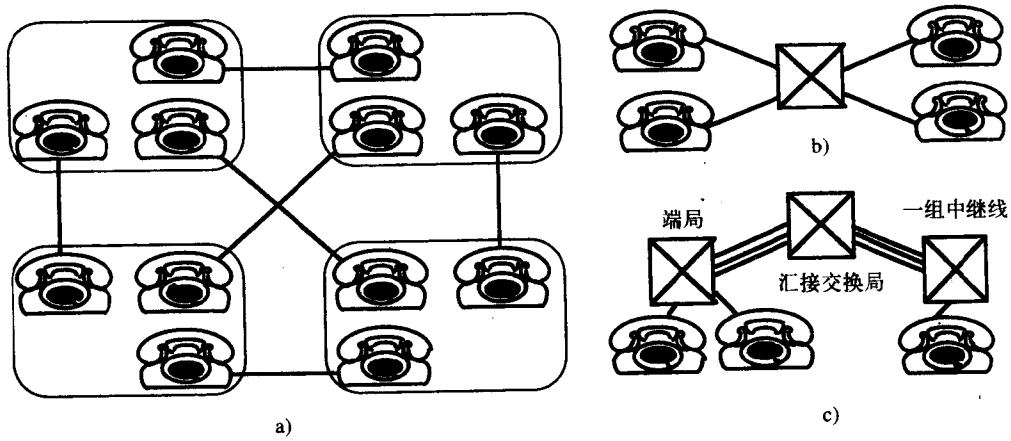


图10-1 a) 在没有交换机的情况下4个家庭的相互连接方式。b) 这里使用了一个交换机。
c) 利用汇接交换机来实现交换机之间的互连

不使用交换机，每个位置点都需要n－1部电话，整个网络则需要n(n－1)/2条电话线，这样才能使得网络中的所有位置点完全互连。这里，n表示网络中的不同位置点的数目。所以一个只有1000个用户的小城市也需要铺设近50万条电话线。

幸好，我们的电话网络是通过位于中心局（CO）的交换机连接在一起的，如图10-1b所示。这种情况下，每一个位置点只需要一部电话机和一条电话线，然而，整个网络依赖于CO的可靠性。所以，CO的建设要确保不受洪水、地震和其他灾难的影响。

引入交换机的另一个缺点是：必须再建立一套交换机之间以及交换机与终端用户之间进行通信的方法。这一点对于保证主叫方能够准确连接到被呼方是非常必要的。从第9章的讨论可知，实现这个功能的是信令。信令被用于在用户与交换机之间或者在两个交换机之间传递信息。

随着需要互联的CO数量的不断增加，再次出现需要交叉连接的线路越来越多的问题，但是这次该问题出现在中心局之间而不是用户端。为了缓解这个问题，出现了汇接交换机，如图10-1c所示。汇接交换机是一个为交换机提供服务的交换机，基本上与图10-1b所示的为电话

机提供服务的交换机具有相同的功能。

10.1.2 交换机的组成

一个交换机是由两个基本部分组成的：交换结构（或称为交换网络）和交换控制。所谓交换结构是指由相互独立的线路或者中继线相互连接而形成通信路径的地方；控制机制是指如何通知结构中的各个单元建立连接以及在什么时间建立连接。

即使是由交换台和话务员组成的那些最原始的交换机，也能显示出这两条基本的属性。话务员本身就起到了控制作用，他可以决定哪一条转接线应该与哪一个插孔相连接。布满插头、转接线、插孔和指示灯的交换台就是交换结构，因为通信路径是在交换台上连接建立起来的。

10.1.3 空分交换和时分交换

可以采用两种方法设计交换机，它们分别是时分交换和空分交换方法。图10-2给出了每一种结构的例子。在这两种结构中，输入A、B、C都分别与输出E、F、D相连接。这两个图只显示了交换结构，而决定整个交换机运行状况的控制设备并没有给出。

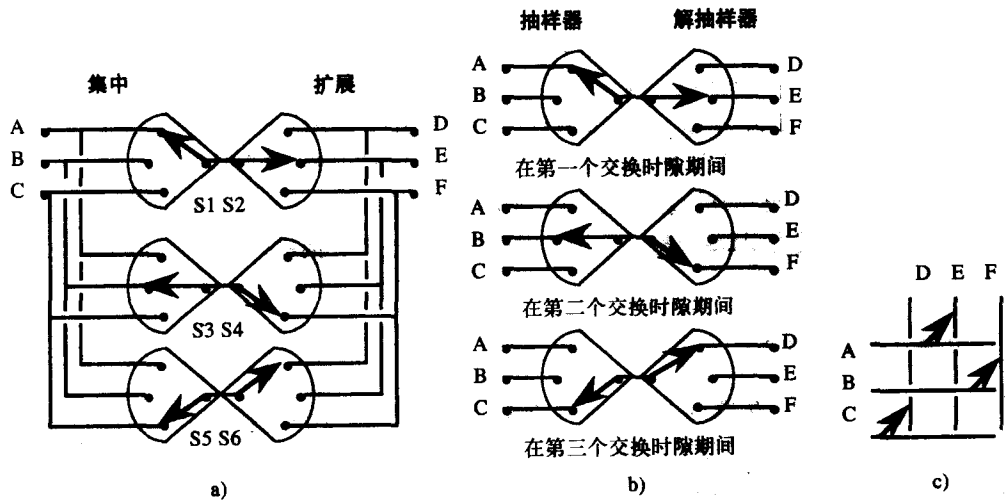


图10-2 a) 空分交换机。b) 时分交换机。c) 矩阵交换机。每一种交换机都是将A与E、B与F、C与D相连接

在图10-2a中，左边的三个交换开关正在完成所谓的集中功能，因为每一个交换机都将多个输入减少集中在一条路径上，它们分别选择了三个输入中的一个。右边的三个交换开关正在完成所谓的扩张功能，因为它们要为这个连接选择合适的输出端。

在这里，交换开关被设置好之后，在整个的通话过程中都不会改变。两个同时发生的连接可以在不同的物理链路上建立。因为交换机中的物理链路在空间上是彼此分离的，所以这种构成方式被称为空分交换方式。

与此相对应的是如图10-2b中所示的时分交换方式。这里给出了一台交换机不同时刻的工作状态。在第一个时间间隔内，交换机为A建立了连接；在第二个时间间隔内，为B建立了连接，以此类推。这个过程不断地重复，每个连接依次被建立，不同的输入端到输出端的信息顺序被传递。由于三个连接必须共享一条物理路径，因此它们不得不按照顺序轮流使用这条路径。

注意这些连接并不是在空间相互分离的，而是利用不同的时间间隙来分离的。因此这种方式被称为时分交换，它与图3-11中所描述的时分复用非常相似。它们之间的唯一区别是时分复用中的输入与输出之间的连接是固定的。也就是说，输入1与输出1相连，输入2与输出2相连等等。而对于时分交换，一个给定的输入能与任何一个输出相连接，具体与哪一个输出相连由控制机制实时地决定。

10-2c给出了一个矩阵交换机（或称为纵横交换机），这种交换机使用的是时分还是空分方式呢？注意图的左边有三个输入，图的上边有三个输出。为了在它们之间实现所有连接，总共需要9个交换开关。由于每个连接都使用不同的物理路径，因此认为这种交换机使用的是空分交换。在这种交换机中使用的交换开关数要远远多于图10-2a中所使用的交换开关数。但是这种交换机使用的是双掷交换开关，而图10-2a中使用的是三掷交换开关。目前，这种矩阵结构的交换都采用半导体技术来实现，比如采用在一块芯片上聚集了许多三级管的超大规模集成电路（VLSI，Very Large Scale Integration）技术。

10.1.4　产生阻塞的原因

图10-2a和图10-2c中的两种空分交换机被认为是无阻塞的。也就是说，所有的输入都可以与一个处于空闲状态的输出端建立连接。会发生阻塞的交换机是根据这样的理念设计的，即所有端口根本不会同时建立连接，因此交换机的结构不必那样庞大和昂贵。

可以这样来想像一个会发生阻塞的交换机，它是从图10-2a所示的交换机中去掉了S5和S6两个开关之后的剩余部分。在这种情况下，三个输入中的任何两个可以同时建立连接，但这时如果第三个输入也需要建立连接，就会收到一个忙音信号。由于在交换机满负荷运行时，第三个输入被阻塞，或者说2/3个输入没有被阻塞，因此这个交换机的阻塞率为33%，或者说它的无阻塞率为67%。

10.1.5　交换机更细致的分类

除了时分交换和空分交换方式以外，交换机还可以更细致地分成如图10-3所示的各种类型。最初的交换机是手工操作的，也就是利用“塞绳”控制台。接下来出现的一代交换机主要是机电式的，这意味着它们使用由电流驱动的继电器。这些交换机通常都采用时分交换技术，这部分内容在10.2节中将详细介绍。

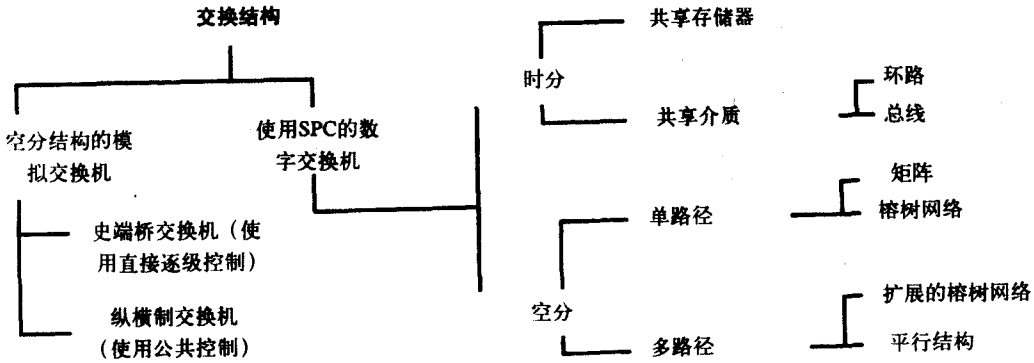


图10-3　各种交换结构

在机电式交换机之后出现的是数字交换机。数字交换机既可以使用时分交换也可以使用空分交换。控制每一种交换机的技术都是不同的，对这些交换机而言每种技术都是唯一的。史端桥交换机采用一种被称为直接逐级控制的控制技术，而纵横制式的交换机采用的是一种被称为公共控制的方法，但大多数数字交换机中都是使用一种被称之为存储程序控制(SPC，Stored Program Control)的方法。我们首先来研究这些控制技术，然后概述图10-3中其他一些类型交换机的操作方法。

10.2 控制方式

10.2.1 直接逐级控制

在1892年，Almon B. Strowger发明了史端桥交换机或者称为步进制交换系统，并首次安装在独立的电信中心局中。但令人奇怪的是，Bell电话系统在大约25年之后才安装了这种自动化的系统。步进制交换机采用直接逐级控制机制来决定交换状态并提供所需要的连接。从用户电话机发出的拨号脉冲直接用来选择和控制开关，从一个交换机到下一个交换机，逐步完成连接。拨号脉冲所选择的路径就是传输话音信号所经过的路径。

图10-4中说明了步进制交换机是如何进行局间呼叫的。这里，左边的电话机通过拨叫427-5587这个号码来呼叫右边的电话机。这些交换机工作的三个阶段要经过寻线器、选择器和连接器。当左边的用户拿起听筒开始拨打一个电话时，寻线器将这条用户电话线与第一个选择器相连接。

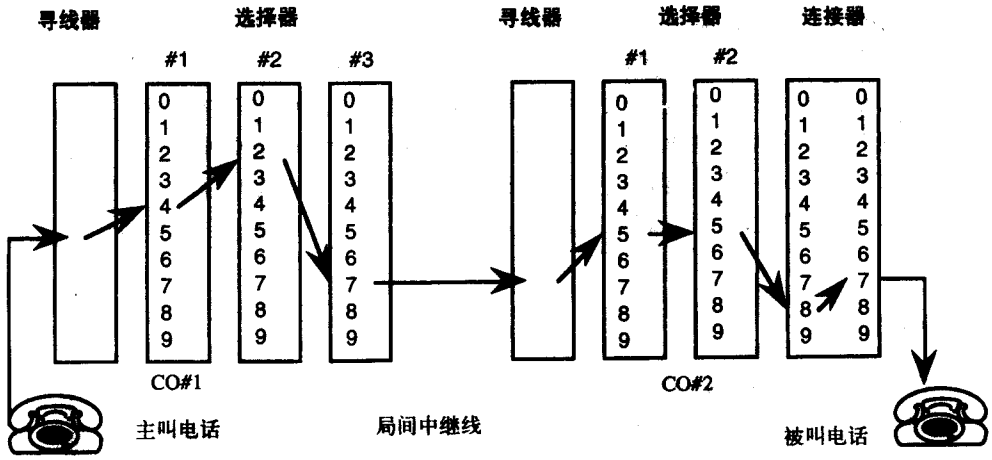


图10-4 利用步进制交换机完成到427-5587的局间呼叫切换

第一个选择器发出拨号音，在接收到第一个拨打的数字（在这个例子中第一个数字是4）后，这个选择器会选择交换机的第4个开关或者说第4个位置，然后再寻找一条空闲线与下一个选择器相连接。类似地，选择器2和选择器3的开关与第二个和第三个拨入的数字相对应。在这个例子中，三个数字指定了到不同中心局的交换。这样只要使用硬布线的中继线就可以实现到427的交换。主叫方的电话机继续控制这个交换中的开关，直到连接器的开关根据最后拨出的两位数字做出切换，才完成了这个连接的建立。

10.2.2 公共控制

控制交换结构的另一种方法叫公共控制。这类控制机制通常用在纵横制交换机中。纵横制交换机是在步进制交换机发明10年之后，由瑞典人L.M.Ericsson 发明的。在数字交换机被广泛应用之前，纵横制交换机发挥了主导作用。

图10-5是纵横制交换机的原理框图。线路连接架是一台矩阵交换机，就如同中继线连接架一样。前者用来连接用户线链路，而后者则是用来将中继线与交换机相连。被称为连接线的导线位置将这两个交换架连接在一起。

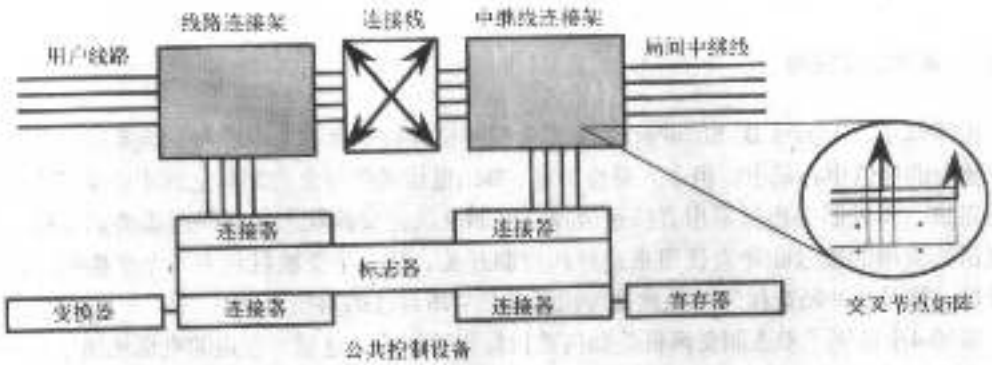


图10-5　一个典型的公共控制交换机的功能方框图

当一个电话摘起时，一个寄存器提供拨号音，并存储拨叫的地址。利用存储的数字，一个被称为标志器的逻辑电路预留一条空闲的中继线，并且分别给这个路径上的交换机发出命令，建立所需的连接。翻译器用来帮助标志器将拨打的号码转换成特定的交换设置。

只需要花费不到1s的时间就可以建立好连接。如果以前建立起来的连接仍然在通话，就不再需要标志器和其他的公共控制设备提供的服务，并且可以用它们来建立另外一次呼叫连接。由于这些控制设备可以由多个呼叫共享，因此被称为公共控制交换。除了不需要那么多设备之外，这种交换的一个主要优点是可以提供选择性路由。也就是说，如果通向交换机的一条路径被另一个呼叫占用了，就可以选择另外一条路径。对于步进制交换机而言，这是不可能的。

10.2.3 存储程序控制

前两代交换机都是硬布线的，灵活性很差。如果要提供新的电话业务（比如呼叫等待、电话会议等），交换机就必须被重新设计，且还要单独地重新布线。而对于存储程序控制（SPC，Stored Program Control），交换机在中央处理器（CPU，Central Processing Unit）和运行软件的控制下工作。如果要增加新的业务，通常只需重新编写软件并完成相关的测试，然后再在每台交换机上拷贝和安装升级的软件，这样就可以提供新的业务了。此外，每台交换机所需要的专门技术减少了。例如，尽管AT&T的4ESS系统（Electronic Switching System）是1976年问世的，但目前仍然是AT&T的主要交换机，因为从那时起运行在它上面的软件已经升级过无数次了。

图10-6概括了SPC系统的功能。这个交换机的核心是一个专用CPU，它被用来进行实时的逻辑处理和输入输出操作，而不是为算术运算而设计的。它可以访问两种类型的存储器，一

个是软件程序存储器和保持客户配置信息的数据库，另一个是用来存放呼叫相关信息的存储器。为了防止意外的操作覆盖掉交换机的运行程序，程序存储器是被写保护的，只有在安装新版本的升级软件或终端用户增加新的业务时才能对它进行修改。

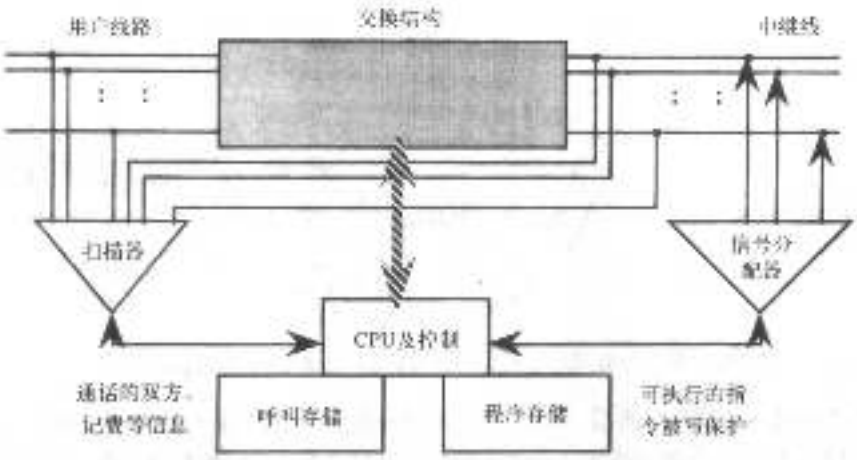


图10-6 存储程序控制交换机的简化方框图

呼叫存储器用于存放接收到的主叫方的拨叫号码、用户线和中继线的状态等信息。高速扫描器会时常查看用户线路和中继线的状态，以确定它们的状态是否改变。例如，如果一条用户电话线摘机，CPU就会提供一个拨号音，当用户拨出第一个数字之后，扫描器就会去扫描其他的线路并为之提供服务。当接收到来自中继线的一个来话呼叫时，扫描器就会检测到它，程序会控制相应的电路，并根据情况进行相应的处理。在每一种情况下，都会明确地指示在交换结构中如何为呼叫建立连接，什么时候发出振铃信号或忙音信号等。如果是一个局间呼叫，分配器的电路会通过中继线把信号发送给下一个CO。

10.3 数字交换

到目前为止，我们已经考虑了最初用于处理话音交换的模拟格式的交换机。4ESS是一种数字式交换机，但是与之相连的中继线最初都是模拟的，因此需要被转换成数字的。现在来看一下数字交换机，这种交换机用于完成话音、数据、传真等信息的交换，它所使用的信号是数字格式的。

10.3.1 时分环

为了理解时分环的工作原理，让我们先来看一下图10-7所示的一个类比示例。这个火车共有4节车厢，这代表4个时隙，用来为8部电话切换呼叫。这些电话都以64kbps的速率把它们各自的话音比特（或者说是经过数字化的语音）放在各自的传输平台上，这些平台被标记为A到H。由于来自电话机的数据以64kbps的速率到达，那么火车本身就必须以每秒64 000圈的速率旋转。另外，由于火车只有4节车厢，即4个时隙，那么每秒钟总共256 000个时隙在旋转。

我们不妨认为这列火车的司机就是交换机的控制机构。当电话机G告诉司机希望与电话机A建立连接时，火车司机会分别通知A和G，告诉它们已经把车厢W分配给了它们来建立这个连接。所以当G看到火车经过时，它就在W上放一个比特，然后A可以从W上接收到这个比特。

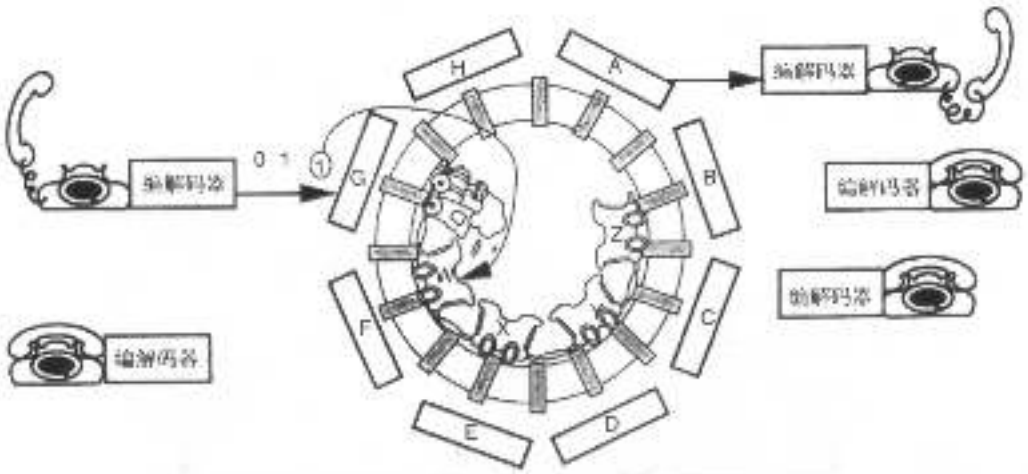


图10-7　基于时分环的交换机可以支持4个通话或8个无阻塞的电话

类似地，如果A需要与G通信，那么司机可以分配另一节车厢，比如说车厢Z，来传输话音比特。所以，对于一个连接来说，需要2节车厢或2个时隙，每个方向一个。在这个例子中，无阻塞比率是多少呢？如何才能使无阻塞的比率增加呢？

由于有8部电话但仅有4个时隙，因此只有4部电话可以同时通信，故无阻塞的比率是50%。要使无阻塞的比率提高到75%，至少得增加2节车厢（即2个时隙）。要使这个交换机完全无阻塞，需要一列具有8节车厢的火车。为了处理这些通话（或者实现8路数据的转接），环的运行速率每秒必须为8乘以64 000转，即512kbps。正如所看到的一样，这个类比恰如其分地说明了时分环的工作原理。

10.3.2　时分总线

简单地说，如果把时分环从相对点拉直就可以得到所谓的时分总线。在这里，每一个通话还是需要分配2个时隙。有时把时分总线称为时隙交换。

作为一个例子，下面来计算一下对于200个话音终端，要提供无阻塞的交换，时分总线所需的最小速率是多少？

200个语音终端可以产生100个对话，所以需要200个时隙。假设采用PCM语音编码，速率为64kbps，那么需要的总线速率为200乘以64kbps，即12.8Mbps。

10.3.3　时－空－时交换

时－空－时是一种在PBX和电信交换机中经常使用的技术。它可以使许多时分交换总线无阻塞地连接在一起。如图10-8所示，在整个设备中有4组这样的总线，分别记为模块A到模块D。这些总线通过一个矩阵交换机互相连接，从而可以提供完全无阻塞的容量。

同一模块内的呼叫，或者说是同一个模块内的两部电话之间的呼叫，不必通过矩阵交换机就可以在模块内建立连接。模块间的呼叫首先在主叫方的模块内进行时间交换，之后在矩阵里进行空间交换，最后再在被叫方的模块内进行时间交换。因此，用“时－空－时”来描述这种交换类型。

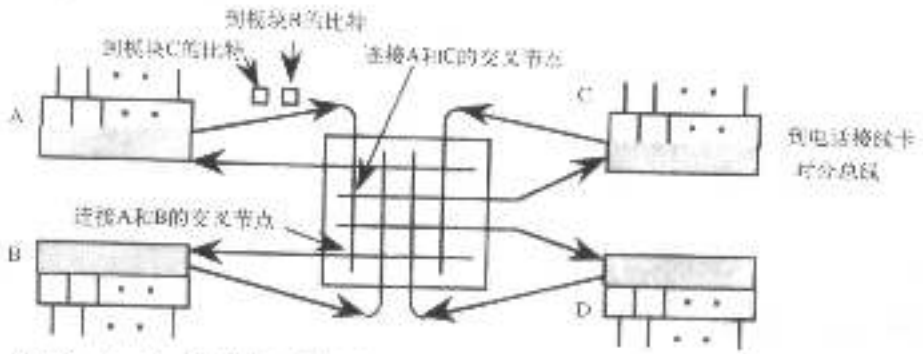


图10-8 时-空-时交换机。从模块A传给模块B和模块C的两个比特被显示。在不同时间内这两个比特被交换。矩阵为每一个其他模块交换1个比特

图10-8显示出在模块A的总线上有两个比特，它们要被交换传送到B和C模块。首先建立到B的连接，然后建立到C的连接。通过这种方式，信息比特被传送到它们各自的目的地。矩阵交换机的时钟速率必须是时分总线时钟速率的4倍，这样它才可以在一个总线的时钟周期内处理所有4个模块的数据交换。模块内部呼叫所使用的比特，只是简单地完成重定向功能。显然，这种交换机的控制单元是非常复杂的，因为它们必须能使交换机的各个组成部分保持严格的同步。

举例来说，每一个模块能够以64kbps的速率提供256个无阻塞的呼叫。每一个呼叫需要2个时隙。所以我们需要512个速率为64kbps的时隙，这就意味着总线速率应为32.768Mbps（64kbps乘以512）。假设连接到空分交换机的模块最大数为10，那么矩阵必须提供的交换速率为327.68Mbps。

10.3.4 矩阵交换机

当一个数据中心的许多主机正在通过连接中继线与其他多个地点进行通信时，中心内设备之间的相互通信管理起来可能非常困难。比如，如果一个调制解调器失灵，网络操作人员就要赶快把连接切换到其他空闲的调制解调器上。但是这样匆忙行事可能会导致整个工作电路瘫痪，也可能由于将电缆与连接线相混淆，把一个工作良好的调制解调器变成了一个有问题的调制解调器。

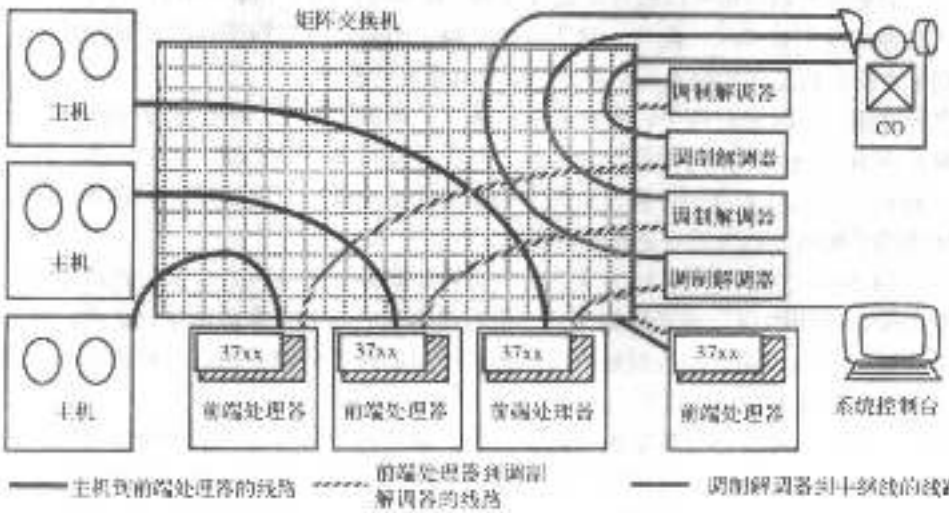


图10-9 一种被称为矩阵交换机的设备（这个术语并不是指矩阵交换结构）可以提供非常好的网络管理

要是利用矩阵交换机，管理者可以制定可靠的恢复方案，实现设备间的正确切换。矩阵交换机并不是前面所提到的交换结构的类型，而是一种设备。

如图10-9所示，主机、前端处理器、调制解调器和连接中继线都是通过矩阵交换机连接在一起的，空闲的设备和系统控制台也连接在矩阵交换机上。由于出现了错误，一个正在工作的调制解调器要被替换掉，这时只需要简单地点击系统控制台上的一个图标。通过系统控制台，可以对交换机进行编程，自动地完成切换过程。此外，矩阵交换机还可以对所有的连接进行监视，并还可完成链路统计功能。

10.4 高级交换的概念

第5章曾经提到过异步传输模式（ATM，Asynchronous Transmission Mode），这里只谈一下在ATM中经常用到的交换技术。由于这方面的技术比较复杂并且在不断地变化，所以只对这个方面做一个简要的介绍。在本节中讨论交换时，假设所传递的信息都被打成大小固定的包，这些包被称为信元(cell)。一个信元的长度是53个字节，包含48个字节的数据和5个字节的信头。信头用于将信元切换到正确的输出端。

10.4.1 再论时分交换和空分交换

回到图10-3，回顾一下适用于数字信号的两种类型的交换机——时分交换机和空分交换机。我们已经讨论了时分环、时分总线和矩阵交换机。现在，再看一下剩下的几种交换操作。

时分交换：图10-10给出了一个共享内存的时分交换。当接收到样点数据时，交换机会把这些数据放入缓冲器中，缓冲器的输出端则按照完成交换所需要的顺序被依次选择。

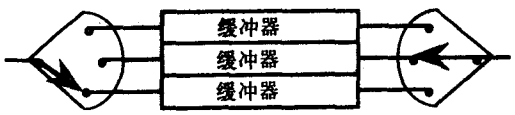


图10-10　一个共享内存的交换机

这种时分交换结构用于组播（从一个源到多个目的地）或广播（一个源到所有目的地）是非常有效的。这是因为被传输的比特要经过所有的输出。不是只有一个端口被控制来复制该比特，而是多个端口都可以被控制进行复制。比如在图10-7中除了A可以从车厢H中读取比特外，其他的端口也可以。此外，对于时分交换，不要求所有的端口以相同的速率工作，可以根据每个端口所允许的输入速率动态地改变对带宽的需求。

空分交换：在时分交换中，所有的端口共享一条传输路径；而在空分交换中，在任意给定的时间内有多条可用的传输路径。因此，对于一点对多点的传输，比如广播，时分交换更适用；而对于多点对多点的传输，空分交换则更合适一些。空分交换机的容量由交换中可以同时使用的平均路径数与端口速率的乘积决定。

在图10-3中，空分交换又被划为单路径交换和多路径交换两个类型。这意味着，对于一对给定的输入输出端口，前者只能提供一条物理路径；而对于多路径空分交换，从一个特定输入端口到特定输出端口的数据每次可以经过不同的路径传输。在这两种情况下，交换结构中都可能同时出现多个传输连接。

通常，数据信元头都放有路由标记，可根据这些标记为结构中的交换单元提供快速的数据交换，这种方式被称为自选路由。在另外的一些情况下，还可以使用依赖于查表的标记路由方法。标记路由方法可以提供有效的组播交换，但是需要对这些路由表进行维护。

10.4.2 单路径结构

图10-2c中的矩阵交换机的一个缺点是：所需要的交叉点开关的数量由输入端口和输出端口的乘积决定。所以如果有8个输入和8个输出，这个交换结构就需要64个开关。

图10-11是榕树交换结构图，要完成8个输入和8个输出的交换，仅仅使用了24个交换单元。尽管这里使用的开关要比矩阵结构中所使用的复杂两倍，但是节省了开关还是有价值的。同时，大部分的控制信息是由这个结构本身发出的。

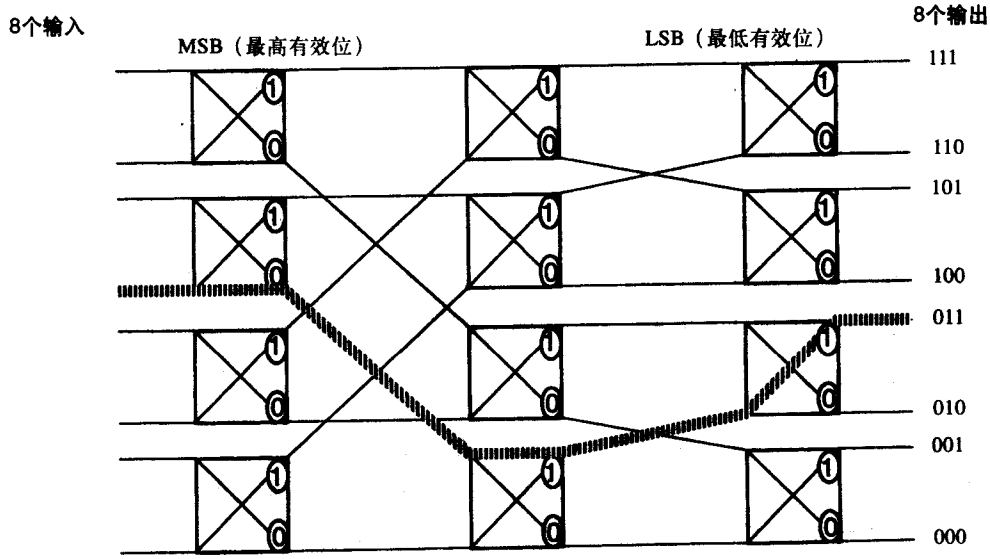


图10-11 榕树交换结构，其中有一条路径到达输出端011

榕树网络交换机由二进制交换单元组成，这些交换单元根据一个地址比特把一个呼叫切换到两条路径中的一条。在图10-11中，8个输入与左边第一列的4个开关相连接。到达这8个输入的信元都会被立刻切换到右边的一个输出上。当一个信元到达其中的任何一个二进制交换单元时，交换单元都会把它路由到0或1的输出端。

举一个例子。假设有一个信元到达第4个输入端，其信头中输出的目的地址为011。地址的最高有效位（MSB，Most Significant Bit）是0，根据这个0先将这个信元切换第一个交换单元的0输出端。接着中间的交换单元开关将信元切换到二进制输出端1，最后一个开关也如此进行。

由于到达该输入端而目的地址是011的信元都经过同一条路径，因此这种结构被称为单路径传输。而且，其他的传输也可同时发生，比如说可以从第一个输入端传输一个目的地址为000的信元。

如果两个信元要到达同一个输出端，则在输出点只能实现一个信元的切换。与矩阵交换机不同，榕树交换机是一种阻塞交换机。

如果把榕树交换机的交换单元变成4个输入和4个输出（而不是2个输入和2个输出），则将这种结构称为δ（delta）网络。δ结构中根据2个或更多的地址比特交换信元，而不是像在榕树网络中仅使用1个地址比特。

10.4.3 多路径结构

在图10-12a中在基本的榕树交换结构中增加了一列开关，使之成为扩展的榕树交换结构。

它可以为一对输入和输出端提供不止一条可用的路径，从图中可以看到有两条路径。因此，这种结构被称之为多路径结构。每增加一列开关（或者说增加了开关的状态），可用的路径数就会成倍增加。

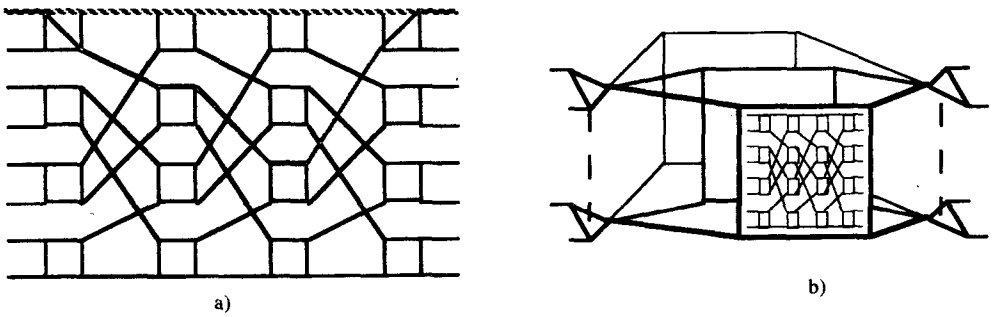


图10-12　两种多路径结构：a) 扩展的榕树结构，在这里将一对端口间的两条路径高亮显示；b) 并行面结构

图10-12b是另一个多路径结构的例子，称为并行面交换结构。这种结构能提供更好的可靠性，性能更佳，因为即使其中某个平面出现了故障，仍然可以保持一定的交换容量。

10.4.4　缓冲和争用解决方案

不论使用哪种交换结构，都需要使用缓冲。在一个交换单元里，两个信元可能要同时使用一个输出端口。如果在交换结构外面使用缓冲，不论是在输入端还是在输出端，都需要一种机制来解决交换结构内部的端口争用问题。

一种简单的解决争用问题的方法就是丢弃一个信元。另一种方法就是在结构内把信元转换到另一个方向。如果结构内有足够多的级数，就可以把数据传输到正确的输出端口上。否则，信元就不得不循环传送回到输入端口。也可以根据信元的优先级进行路由选择。还有一种可用的方法就是为输入端口预留所需的输出端口。对于这种交换结构的许多研究工作还在进行当中。

习题

1.下面哪一种交换不是空分交换?
　a. 步进制交换　　b. 纵横制交换　　c. 共享内存交换　　d. 矩阵交换
2.下面哪些设备不属于纵横制交换机?
　a. 标志器　　b. 寄存器　　c. 连接器　　d. 选择器
3.利用头部的信息进行路径选择的交换方法是哪一种?
　a. 标记路由　　b. 自选路由　　c. 直接路由　　d. 头部路由
4.下面哪一个是时分交换的优点?
　a. 适合组播　　b. 多路径交换　　c.需要较少的交叉点　　d. 需要维持的交换表较小
5. 存储程序控制交换机的哪个部分最先注意到摘机?
　a. 分配器　　b. CPU　　c. 传输介质　　d. 扫描器
6. 如果在图10-12a中再增加一级交换单元，那么在这个扩展榕树交换中，每一对输入和输出端口之间有几条路径可用?

a. 2 b. 3 c. 4 d. 6

7. 目前已经公布的基于ATM的局域网交换机最多可以支持16个155Mbps的端口，它的总线速率是多少?
8. 在图10-11中，可同时存在的最大和最小的路径数目是多少?
9. 使交换机可以互相连接的交换机叫什么?
10. 在步进制交换机被发明之前使用哪一种交换机?
11. 在图10-2a中，如果左边的三个开关与5个输入相连，而右边的三个开关与5个输出相连，那么无阻塞率是多少?
12. 假设图10-8中的每个模块都与512部电话相连，它们都使用32kbps的数字化语音信号。如果每个模块的无阻塞率为40%，那么这些模块的总线速率是多少?
13. 说出交换机的两个组成部分。
14. 怎样分辨时分交换和空分交换? 你能设计一个频分交换机吗?
15. 列出三种控制方法，并解释它们。说明后面的两种方法在哪些方面优于第一种方法。
16. 模拟开关和数字开关有什么差别?
17. 试着画出带有4个输入和4个输出的榕树交换结构。
18. 对于高容量的交换系统，空分交换有什么优点?

第11章 PSTN

在本章中，我们将介绍PSTN（Public Switched Telephone Network，公共交换电话网）的发展，它也可以称为DDD（Direct Distance Dialing，长途直拨）网络。最初建立用来承载电话业务的PSTN，如今已经组建发展成为一个信息化网络，其承载的不仅仅是话音业务：正是由于这个原因，我们将其命名为公共交换信息网可能更为恰当。

11.1 背景

直到20世纪80年代初期，电话在PSTN内的传播使用的仍是一种称为分级路由的方法，如图11-1所示。一个国家的所有交换中心分为大区交换中心、地区交换中心、中继线交换的第一级、长途交换中心局或端局。当低等级局不能直接完成到远距离目的局的通话时，需要高等级局的服务。

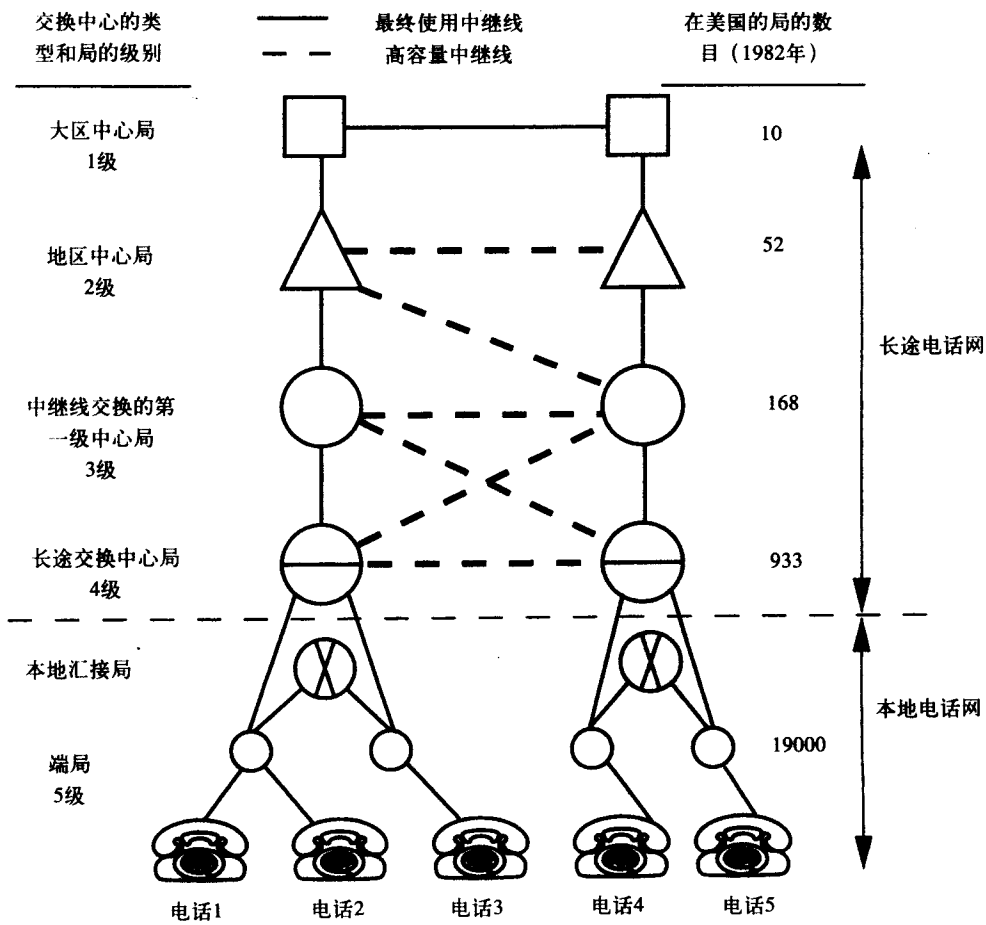


图11-1 过去采用的分级路由方案

每一个低等级局都直接从属于高等级局，并且这些高等级局之间的中继线称为最终中继线。在两个不同地区的局之间，如果中继线的使用率很高，就必须建立高容量的中继线。所以当使用这种类型的中继线完成一次呼叫时，就可以绕过高等级的最终中继线和它们的局，并且利用更少的节点就能够完成该呼叫。

在图11-1中,不论何时电话1呼叫电话2，仅由连接两个电话的本地局就能够全权处理该呼叫。如果电话1对电话3发出本地呼叫，该呼叫就要经过汇接交换局，但是如果在两个端局之间有可用的直接中继线，那么就会使用直接中继线。如果呼叫跨越更广阔的区域，比如电话1呼叫电话4，这时就不得不经过两个长途交换中心局。

在上述这种情况下，如果在两个长途交换局之间存在高容量的中继线，那么会使用该中继线。否则，将找到与高等级局相连的空闲的中继线来完成这次呼叫。在极端情况下，呼叫不得不经过所有上级局的交换和所有最终中继线才能找到到达目的地的路由。使用多级交换会在语音呼叫中引入噪声、干扰以及连接时延。

采用以上这种方式，完成端到端的一次呼叫所花费的时间高达20s，同时多级交换还会带来噪声和干扰。如今，IXC（局间交换运营商）采用数字化语音在6s内就能完成这种呼叫，并且只需要2次或3次交换，这是因为今天的网络不再是分级式的（即每一个交换机都有一条主要路径与唯一一个其他交换机相连，呈阶梯状），而是每一个交换机到其他所有交换机之间都有一条直接链路，这种结构的网络称为平面网络。本章的后续内容将介绍这种平面网络的运行。

11.2 本地电话网

11.2.1 配线网络设备

如图11-2所示，POTS（Plain Old Telephone Service，一般电话业务）连接的布线是从住处到中心局。

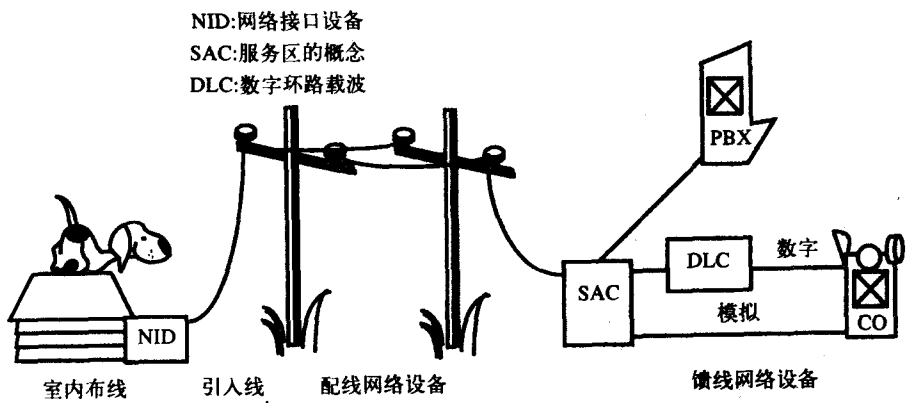


图11-2 从住宅到CO的本地网络设施

在住宅内的布线称为IW（Inside Wiring，室内布线），并且由于产权脱离，因此室内布线所需的时间和材料都要由用户购买和维护，他（她）可能让电话公司提供这种服务或由他（她）自己来做。室内布线要与NID（Network Interface Device，网络接口设备）相连，而网络接口设备就是电话公司职责的起始端。NID是房间的分界点，并且对于老式的布线是不存

在的。它配有接线盒和过压保护装置。

有时也使用SNID（Smart NID，智能NID），提供来自CO的远程回路。这使得电话公司可以在CO直接检测线路对的连续性，而无须派技术人员前往用户住所进行检测。CO向SNID发送一个特殊信号，之后SNID将其自身设置为回路反馈模式，就可以完成这种检测工作。

在NID和电话线杆之间利用引入线进行连接。在某些新开发的地区，如果电缆被埋的话，则可以通过支架进行连接。从SAC（Serving Area interface Concept，服务区接口概念）到家中用户线的配线装置称为线路馈送设备或简称为配线设备。

SAC是一个配线座，安全地放置在远离危险的地方，它是馈送方与配线设备之间边界的标志。与IDF（Intermediate Distribution Frame，中间配线架）为一层楼或一幢楼里的一定范围服务一样，电话公司利用SAC把电话线分配到一个服务区域或配线区域。

从SAC有两条路可以通过馈线网络到达CO,一种方法是简单地在包含许多电线对的电缆中发送模拟信号。另一种方法是使用一个T1多路复用器，通常称之为SLC-96（Subscriber Loop Carrier，用户环路载波）,读作“slick 96”，（这是一个AT&T的商标：它的原名为DLC（Digital Loop Carrier，数字环路载波））。这个多路复用器允许4组24路语音复用到10对电话线上。采用T1时，一对线用于发送，一对线用于接收。因此，对于4组T1来说，需要8对线，额外的两对用于在连接失败的情况下做自动备份之用，这里也可以用光纤替代铜线。DLC系统更经济，能用更少的线路对为更多的用户服务，易于维护，也易于与办公室内的数字中继线兼容。

11.2.2　CO的内部结构

如果中心局要为用户激活一个电话，它必须有TN（telephone number，电话号码）、CP（Cable Pair number，电缆对号码）和OE（Office Equipment designation，局设备名称）。

TN是指定的电话号码，即出现在电话簿上的号码，CP指明CO中与用户的NID相连的电缆对号码，最后，OE指明在CO交换机上的实际线路。当电话号码改变时，CP和OE保持不变；然而，在电子交换系统中，对于当前的OE，TN是通过软件，也就是说通过终端来改变的。

来自CO服务的所有交换区内的电缆都进入电缆室或电缆接入设备中，这些设备通常位于CO的基础设备里，该基础设备数量高达200 000对线。电缆对在这里被VMDF（Vertical side of the Main Distribution Frame，总配线架直列侧）的终端接线板切断，热线圈和碳精块在这里起到保护作用，如图11-3所示。

所有线对从VMDF交叉连接到HMDF（Horizontal side of the Main Distribution Frame，总配线架横向侧），并且从HMDF拨号电路被送至交换机，同时直接通信线路被送至长途局设备。换句话说，从街上来的线路到VMDF，而与交换机和长途局设备相连的线路到HMDF，在MDF两侧的跳线把线路交叉连接到合适的设备上。

来自交换设备的线路与HMDF相连。根据CP指定的不同用户需要与不同的OE相连，交叉连接跳线会在两点之间闭合。

线路也可以从长途局设备到HMDF。长途局设备允许CO对租用线路进行调整，从而使得CO发出的信号电平正确。在图11-3中，1001~1004的线对与交换机相连，而1005线对与长途局设备相连，经过调整后，返回至1006线对从而连接到一个不同的目的地。

从CO引出的中继线共有四种不同类型，一种是连接到其他CO的局间中继线，另外几种分别为连接至PBX的中继线、连接至POP的IXC中继线和连接至蜂窝MTSO（Mobile Telephone Switching Office，移动电话交换局）的中继线。

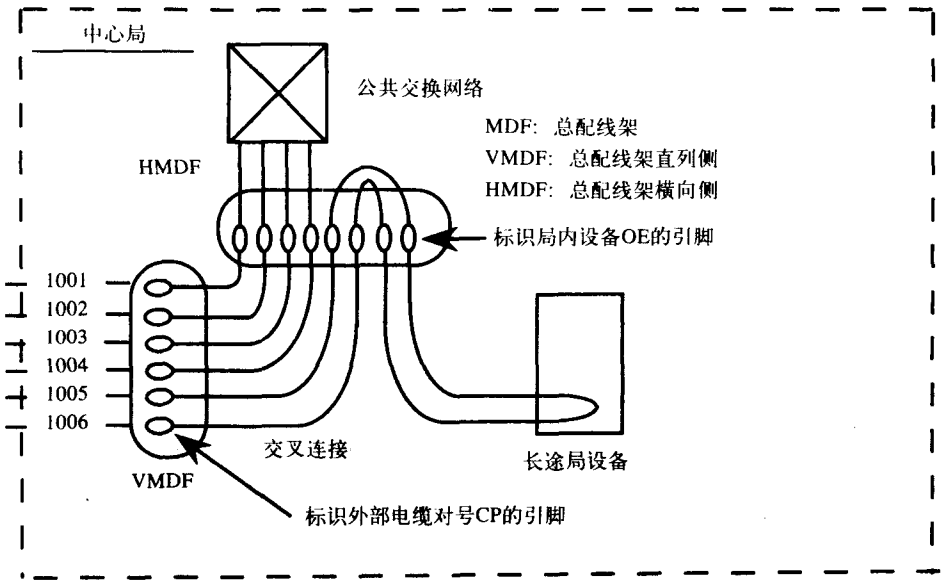


图11-3 进入CO的拨号线路连接至交换网络，而在长途局设备中对专用线路进行调整并路由到其他地点

11.2.3 局间信令使用SS7

现在以新泽西北部的LATA网络为例解释局间信令，这样就可以用一些真实的名字和真实的网络。记住SS7（Signaling System 7，7号信令系统）是分组交换网络，并且通过该网络的所有信息都是采用数据分组传递的。

新泽西贝尔（New Jersey Bell）公司在该地区大约有130个CO，有4个本地的汇接局和2个同类型接入汇接局。如图11-1所示，当两个CO之间没有直接的线路相连时，就采用本地汇接局。在本地区最多需用两个本地汇接局来完成一次呼叫。在新泽西州，本地汇接局也称为地区汇接局。另一方面，同等的接入汇接局允许IXC接入本地网。

如图11-4所示，新泽西州北部的LATA网络有一对STP（Signal Transfer Point，信令传输节点），其中一个STP位于内瓦克（Newark），另一个位于大约30英里以外的新不伦瑞克（New Brunswick）。这两个STP是#2A型的并由朗讯（Lucent）技术公司生产制造。作为SS7组成部分的所有CO均与这两个STP通过56kbps的信令信道直接相连。这两个STP分担它们的工作量，并不断地监视彼此的性能。如果有一个STP发生故障，另一个STP将独自承担所有的信令流量，并发出警报指出另一个STP不能正常工作。

只要仅有信令通过LATA网络边界，而没有别的流量，在两个不同的LATA处放置一对STP对于LEC来说就是可以接受的。图中所示的STP也有与邻近LATA的STP的链路，所以有优先级的呼叫可以在LATA边界附近进行。有优先级的呼叫是本地呼叫，可以由一个位于LATA边界附近并通过该边界的LEC来处理。

STP支架有每个CO的一个电路单元，并且每一个信令信道都有一个DSU（Digital Service Unit，数字业务单元），DSU仅通过数字线与设备接口。每一个CO的电路单元利用CNI（Common Network Interface，公共网络接口）环互相交换信令数据，该CNI环采用与令牌环网络相同的工作机理。

与STP对不直接相连的CO可以通过与SSP（Signal Service Point，信令业务节点）相连成为智能网的一部分，在这样的CO与SSP之间使用MF信令。SSP可以在与STP对相连的链路上把

MF信令转换为7号信令。

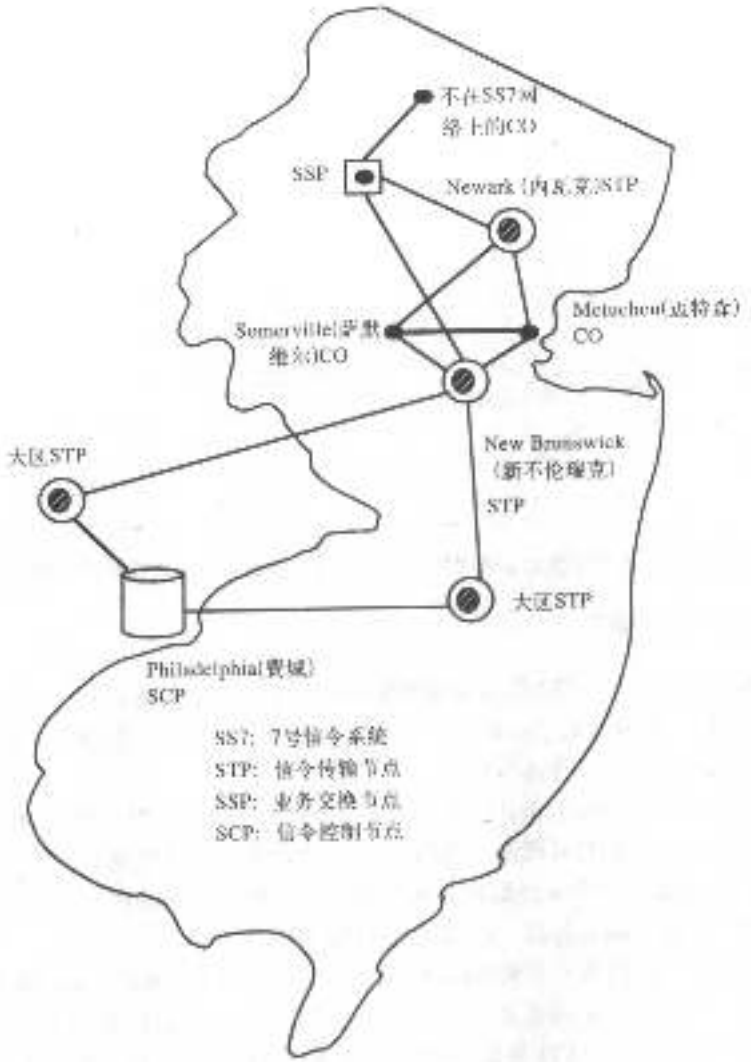


图11-4　贝尔大西洋公司在新泽西州北部的7号信令系统。为了简明起见，从地区的STP到内瓦克（Newark）STP的线路没有显示

现在让我们考虑一下一个呼叫怎样跨过本地网络建立起来。假设一个在萨默维尔（Somerville）的主叫用户拨打迈特森（Metuchen）的555-6789，位于萨默维尔的CO意识到555交换局不在萨默维尔，它就会通过信令网络请求位于新不伦瑞克（New Brunswick）的STP建立对555-6789的呼叫。如果555交换局就位于萨默维尔，那么就不需要使用STP，而萨默维尔本地CO就可完成这次呼叫。

位于新不伦瑞克的STP意识到555是迈特森区内的交换局，并询问迈特森的CO电路6789是否空闲。如果电话555-6789空闲，就会通知STP，接着STP将给萨默维尔和新不伦瑞克的CO之间发送信令包，指示在中继线上建立起本次呼叫的连接。之后这两个CO将检测留给该呼叫的这条中继线的连续性，并且位于迈特森的电话会振铃，发送给萨默维尔的主叫的回铃音信

号则是由萨默维尔的CO提供的。

相反，如果555-6789忙，则迈特森的CO将通知STP，接着STP将通知萨默维尔的CO，此时忙音信号由萨默维尔局提供给主叫，注意CO之间的中继线并不用于提供该忙音信令，这一点同过去使用的信令方式相同。

如果有人想使用贝尔大西洋（Bell Atlantic）信用卡进行呼叫，那么授权是从位于费城（Philadelphia）的SCP（Signal Control Point，信令控制节点）数据库得到的，当STP需要将一个贝尔大西洋800号码转换成一个POTS号码时也会用到SCP，所有800号码都必须被转换为其相应的POTS号码之后，呼叫才可以进行。对SCP的访问是由SS7网络的地区STP提供的。

11.3 AT&T网络

11.3.1 概述

现在让我们把注意力转向LATA之间的通信网络。AT&T是一个IXC（IntereXchange Carrier，局间载波）的例子，它提供LATA之间以及和外国之间的通信服务。其处理的呼叫次数已由1993年的140 000 000次上升到现在的每天230 000 000次呼叫，1996年创下了处理680亿个呼叫的记录，其中99.99%的呼叫在首次连接时就被接通。

为了便于管理，AT&T把网络划分为4部分：传输设备、国际网络、北美网络和网络服务。网络控制中心位于新泽西州的白明斯特（Bedminster），而大区控制中心位于亚特兰大（Atlanta）和丹佛（Denver）。

整个网络传输设备有超过30亿（这个数字在1993年为20亿）英里的电路，大约可绕地球12 000圈。AT&T属于TAT8、TAT9和TPC的所有者组织，这些都是跨大西洋和跨太平洋的光缆，每一条可以支持多达40 000到80 000的通话。FASTAR是一个全自动的网络恢复系统，如果一条光纤断了，管理系统能够在2分钟之内将95%的电路改道。

AT&T网络发展最快的部分是国际网络。IDDD（International Direct Distance Dialing，国际长途直拨）可以到达200多个国家。这意味着呼叫者无须接线员的帮助，AT&T就可以将呼叫传送到这些国家，该网络可以到达总共270个国家，其中只有一小部分由于政治上的限制而无法到达。

11.3.2 北美网络

在美国国内，AT&T有135个4ESS（Electronic Switching Systems，电子交换系统），其中7个用于国际网关。4ESS是一个长途汇接交换系统，也就是说，电话线不可以与之相连，它只能与其他交换机的中继线相连。与5ESS相比，它可以在一小时之内处理700 000次呼叫，而5ESS在一小时内仅可处理200 000次呼叫。在需求低的地区，通常使用5ESS，而美国的骨干网则是由4ESS组成的。

第一个4ESS于1976年安装在芝加哥，最后一个4ESS于1999年安装在亚特兰大，AT&T计划使用更小的交换设备如朗讯技术公司的5ESS和Nortel公司的DMS，这样它可以为更多的小范围的用户提供直接连接。核心部分采用基于ATM的网络将最终提供这些技术的融合，ATM网可以用来提供所有类型的业务包括语音、数据、视频、IP等。

实际上4ESS的配置构成了完全互联的网状网络，每个4ESS与其他的4ESS之间都有一条直接中继线相连，这些中继线可以穿过其间的4ESS站点但并不在那里进行交换。如图11-5所示，大多数的交换机都有直接链路与其他交换机相连，这些链路均是共享的或是复用在公共的物理介质上。

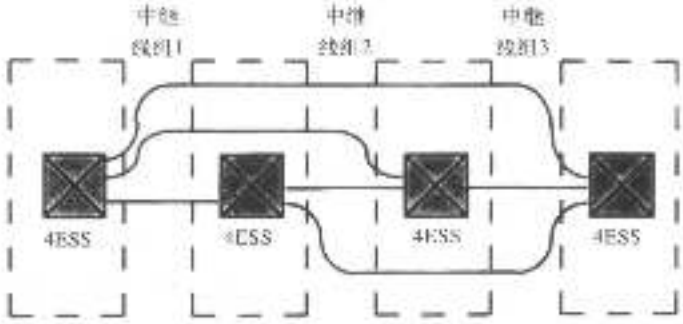


图11-5　位于一条直线上的四个城市的交换机可以只用三组中继线，通过链路复用，使它们完全互连

在4ESS之间的中继线仅传递语音，数据或图像；信令是通过一个称为信令网络的独立网络传送的。物理上，信令网可以共享4ESS网络的传输设备，而在逻辑上这两个网络是分离的。

信令网由12个STP匹配对组成，互联成网状网络，也就是说，每一对STP与其他的STP对有链路直接相连。出于可靠性考虑，给定的STP对可以分离几百英里，而流量由它们均担，每个STP处理50%流量，如果必要的话，可处理全部呼叫。所有信令链路的速率为56kbps，并且每个4ESS仅与一对STP相连，如图11-6所示。

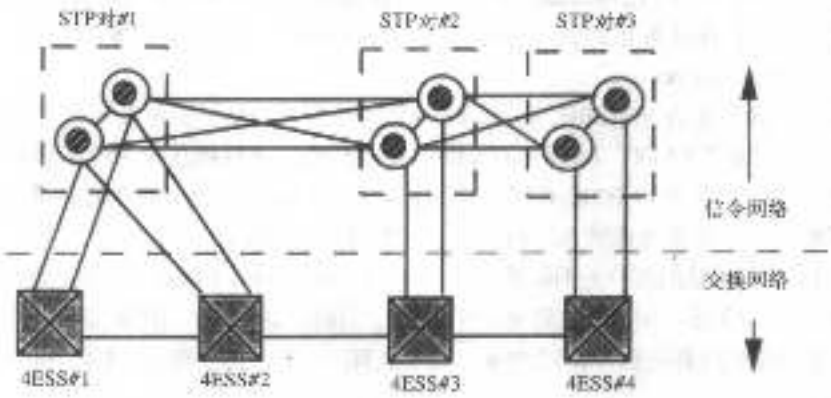


图11-6　AT&T的SS7网络的一部分，在STP对之间和4ESS之间的链路没有全显示出来

11.3.3　信令网上的呼叫处理

在图11-6中，如果一个呼叫产生于4ESS#1，并且需要到达4ESS#2的信道，那么它会发送一个分组到STP#1对请求一个信道。如果存在到达呼叫目的地的路径，STP#1对将与4ESS#2协商，并提供被叫的电话号码。如果4ESS#2不能完成该呼叫，它会通知STP#1对，并且该STP对会将此情况通知给4ESS#1。之后，4ESS#1将给主叫方提供忙信号，并且没有利用4ESS之间的中继线路。

然而，如果4ESS#2可以完成呼叫，STP对就将发送继续进行的信号给交换机，同时，切换到4ESS#1原始请求的中继线上，之后，会在该中继线上进行连续性与质量校验并完成该呼叫，这样就不再需要STP对的服务了。

如果在与不同的STP对相连的两个4ESS之间请求呼叫，例如，在4ESS#1和4ESS#3之间的呼叫，也要用同样的程序，只是现在需要两对STP相互通信来决定使用哪一条中继线。

如果在两个交换机之间没有可用的空闲中继线，那么必须使用第三个中间交换机来路由

这个呼叫，如果二个交换机相连二个不同的STP对，那么这二对STP均需处理这个呼叫。例如在图11-6中，4ESS#1须与4ESS#3通信，而这两个交换机之间没有空闲容量，那么该呼叫可以通过4ESS#4进行路由，在这种情况下，二个交换机与三个不同的STP对相连，并且所有这些STP都必须发送数据包来完成这次呼叫。

11.3.4 RTNR（实时网络路由）

在任何情况下都不能用两个中间4ESS交换机来完成呼叫，而只能用一个中间交换机来完成呼叫。然而，由于大多数交换机都是相互连接的，并且这样的交换机超过120个，所以也就存在许多可能的替代路径。

RTNR动态地计算利用另外一个4ESS完成呼叫的134条以上的可能路径。通过限制只使用一个另外的交换机，RTNR可以保持高质量的信令，并且可以在4~6秒完成呼叫，而采用老式的分级路由，则需20多秒。

在RTNR之前，AT&T使用DNHR（Dynamic Non-Hierarchical Routing，动态非分级路由），这并非真正的动态路由方法，在每个4ESS对之间，它允许每个呼叫有14条路径，这些路径在4ESS中被预先规划，分配给一天中10个不同的时段。

RTNR允许根据每一个呼叫计算最有效的路径。如果到远处4ESS没有可用的直接线路，它会通过信令网向远处4ESS询问与其相连的中继线的容量和状态，之后通过比较与自己相连的中继线的流量和与远处4ESS相连的中继线流量，主叫4ESS就会决定使用其他哪个4ESS作为中间交换机，接着通过信令网络建立合适的连接。在图11-7中，主叫4ESS接收到远处4ESS与其他120个交换机之间的流量负载，从这些数据中，主叫交换机就会决定使用双方中继线路负载最轻的中间交换机。

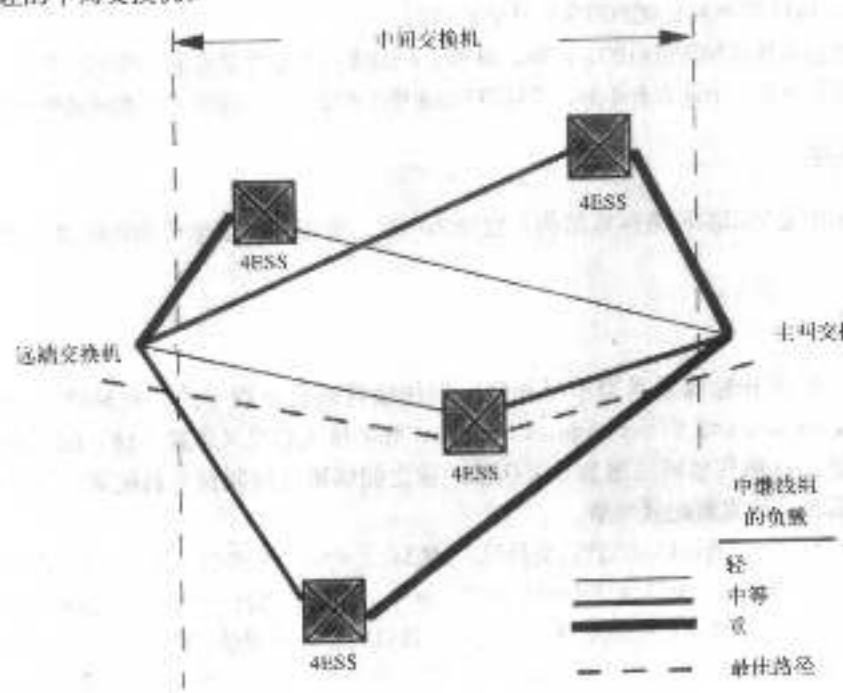


图11-7 RTNR通过评估不同中继线组的利用情况动态地决定最佳的中间交换机来完成一次呼叫

11.3.5 NCP

AT&T通信网络的最后一部分是网络服务。这些服务包括SDN（Software Defined Network，软件定义网络）、虚拟网络、800和900服务以及呼叫卡。它们是由许多称为NCP的数据库提供的。NCP（Network Control Point，网络控制节点）是信令网的一部分并与STP相连，如图11-8所示。这些是与本章中本地电话网络部分描述的新泽西贝尔SCP等价的AT&T网络组成部分。NCP形成了一个分布式的数据库，存储支持800号码、SDN客户等的数据。

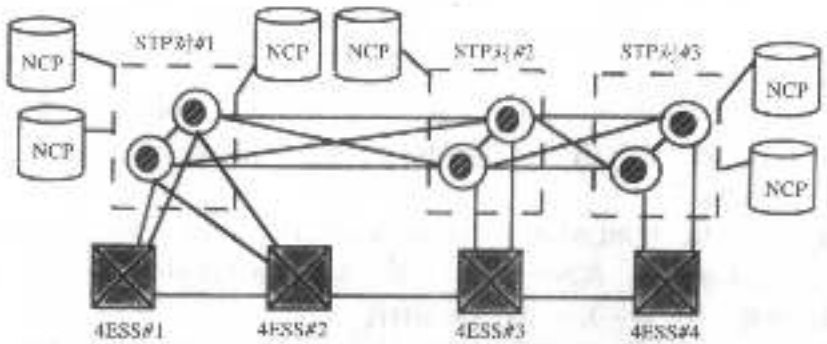


图11-8　与STP相连的NCP(网络控制节点)提供先进的网络服务

例如，当STP要路由800号码时，它知道哪个NCP中存有与之对应的POTS（Plain Old Telephone Service，一般电话业务）号码。通过该NCP，800号码转换成POTS号码，于是STP就可以完成这次呼叫，例如，1-800-544-3498可以转换成圣何塞（San Jose）的408-345-3277。先进的800号码提供分地域或时间的不同路由，也就是说根据呼叫者所处地点的不同或发起呼叫的时间不同，该呼叫所对应的POTS号码是不同的。

呼叫卡的授权是通过NCP进行的，同样，SDN客户的虚拟网络数据库也存储于NCP中。NCP中所有的数据至少在另外一个地方有备份，并且STP知道哪个NCP中有给定客户的数据或呼叫的号码。

11.4 MCI网络

图11-9所示的是MCI的网络体系结构，它分为三层：管理层、逻辑层和物理层。我们首先讨论物理层。

11.4.1 物理层

在这一层，尽管传输媒质类型不尽相同，但传输网络是全数字的。该网络与一个称为DACS（Digital Access and Cross connect System，数字接入和交叉连接系统）的受软件控制的分配框架相连。这给传输网络增加了灵活性，使之能够通过控制台重新配置。用户可以利用管理层的界面轻易地重新配置网络。

来自传输网络的信令通过DACS到达交换机。MCI有大约90个交换机，其中一部分是Nortel公司的DMS-250，另一部分是DSC公司的DEX6000E。每一个交换机都有一个AP（Adjunct Processor，附属处理器）用于减轻其非交换处理负载，这使得交换机的工作更灵活、快捷。AP为每一个呼叫提供CDR（Call Detail Recording，呼叫详细记录）以方便记账，同时提供欺诈检测以防止非授权用户进入专用网络。它也提供MCI网络中MCI交换机和其他计算机系统的协议转换功能。

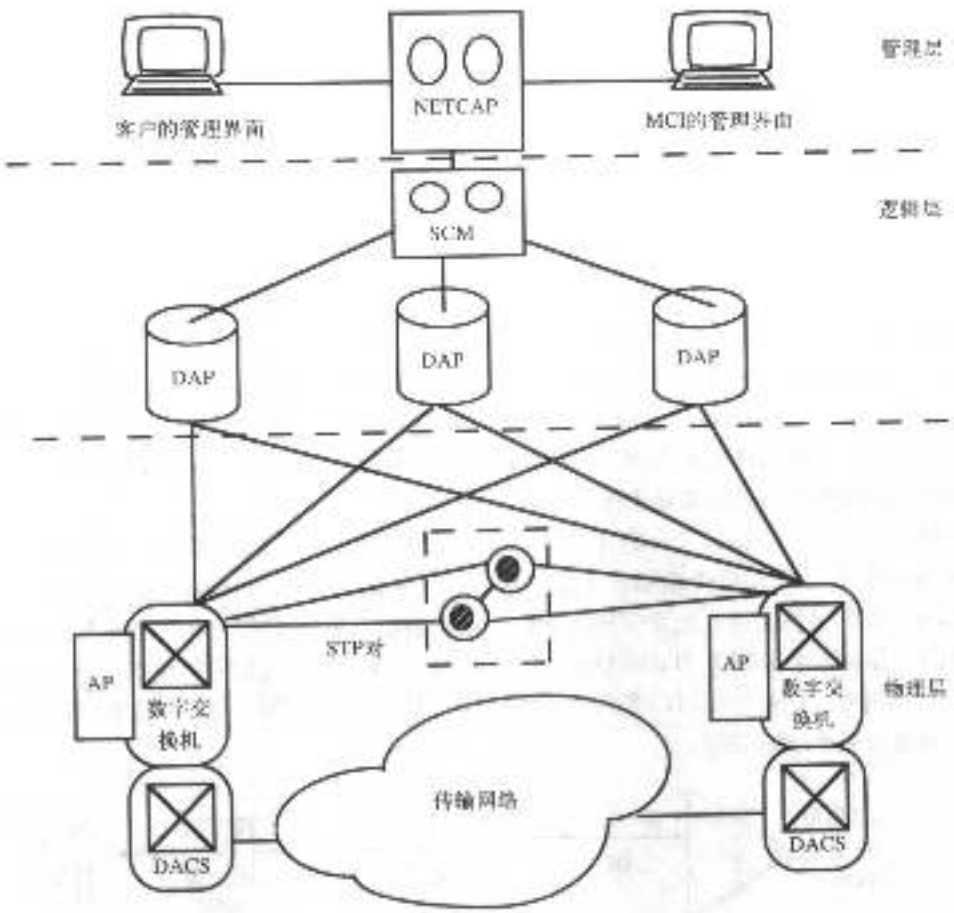


图11-9 MCI的网络体系结构

每一个交换机仅与5对STP中的一对相连。STP网络使用的是SS7的ANSI版本，称为TR-TSY-950。与AT&T网络一样，一个普通的POTS电话呼叫只用物理网络资源即可。

11.4.2 逻辑层

800号码的转换、信用卡授权和虚拟网络使用的是DAP（Data Access Point，数据接入节点），它类似于AT&T网络中使用的NCP。这里的一个显著不同在于，DAP是与交换机直接相连的。DAP采用的是DEC制造的VAX8700小型计算机。所有90个交换机与这三个DAP中的每一个都有直接链路，所以即使两条链路失效，第三个DAP链路仍可继续工作，这些链路上采用的是X.25协议。

这三个DAP中的数据是保持同步的，亦即数据是相同的。这是由SCM（Service Control Manager，业务控制管理器）来完成的。SCM是IBM 3090大型机，它不断地从NETCAP（NETwork CAPabilities manager，网络容量管理器）下载数据。

11.4.3 管理层

NETCAP也是一个大型机，它为管理系统和网络其余部分提供一个接口。当用户或MCI

配置或重新配置满足用户需求的网络时，NETCAP提供一个必要的安全认证。之后它监视用户的请求和命令以确保它们符合正确的格式，并防止用户因疏忽而错误地配置自己的网络。NETCAP还要通知网络组件和合适的计费计算机。

11.5 Sprint网络

Sprint网络的骨干由50多台Nortel制造的DMS-250交换机组成。它还有三台DMS-300交换机用作国际网关。它也是一个完全互联的网状网络，每一个交换机与其他交换机之间都有链路。两个交换机之间的中继线称为IMT（Inter-Machine Trunk，机器间的中继线）。整个网络使用26 000英里的单模光纤及321个POP，并且每一个LATA中至少有一个POP。根据IMT所需的流量不同，光纤的带宽从565Mbps到1000Gbps。如果使用DWDM技术，容量还会继续增加。

与AT&T一样，Sprint采用平面无等级的网络结构。它使用更少的交换节点来降低噪声和失败的可能性。其路由机制称为DCR（Dynamic Controlled Routing，动态控制路由），DCR使用时间区和峰值时间负载的差异来优化其路由。

1993年，光纤网络由23个环路组成。今天，它由228个SONET环组成，这增加了在失败情况下网络的生存性。当传输路径上出现故障时，RDPS（Reverse Direction Protection Switching，反向保护交换）允许交换流量自动重新路由。图11-10给出了光纤在交换机处是如何接口的。首先，采用FOT（Fiber Optic Terminal，光端机）将光信号转换成电信号并解复用为许多DS-3信号，之后一组M13多路复用器将DS-3信道分隔成DS-1信道，交换机再根据需要把DS-1信道分隔为DS-0信道。

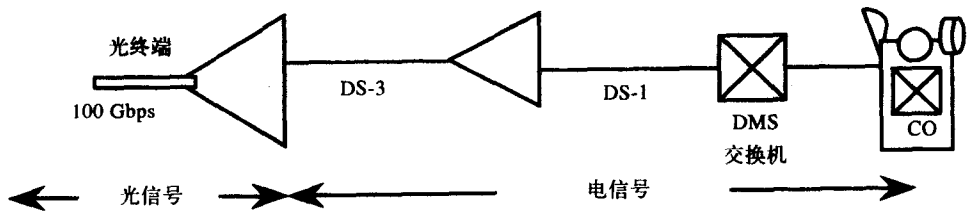


图11-10 来自光纤的光信号被解复用成DS-3信号，之后再进一步解复用为DS-1信号，DS-1为Sprint 交换机接收的信号电平

Sprint为SONET环采用4F-BLSR体系结构，其工作原理将在后面第20章中讨论。光纤骨干网络是用于传输来自七个独立的逻辑网络的流量的物理网络。它并不是为各种类型的网络建立物理上不同的光纤网络，而是把来自这些网络的流量聚集在一个单独的光纤网络中。以下是这些逻辑网络：

1）用于拨号呼叫的电路交换网络；2）为交换机承载信令的SS7网络；3）用于商业目的的专用租用线路，需要点到点的固定带宽；4）世界上最大的X.25网络SprintNet，即以前的Telenet；5）帧中继，所有这些逻辑网络共享光纤网上的带宽；6）Sprint的ISDN以及7）内部骨干网。与公众因特网完全分离的内部骨干网使用TCP/IP提供了一种信息传递的安全方式。

1988年12月，Sprint对SS7进行了一些改动。图11-11显示了DMS交换机中的SP（信令节点），这些SP帮助STP和DMS交换机更有效地执行呼叫处理。

STP与SCP（Service Control Point，业务控制节点）相连，SCP与AT&T网络中的NCP作用类似，也就是说，它们为800号码转换、信用卡业务处理与虚拟网络路由提供所需的“数据库预览”（database dips）。

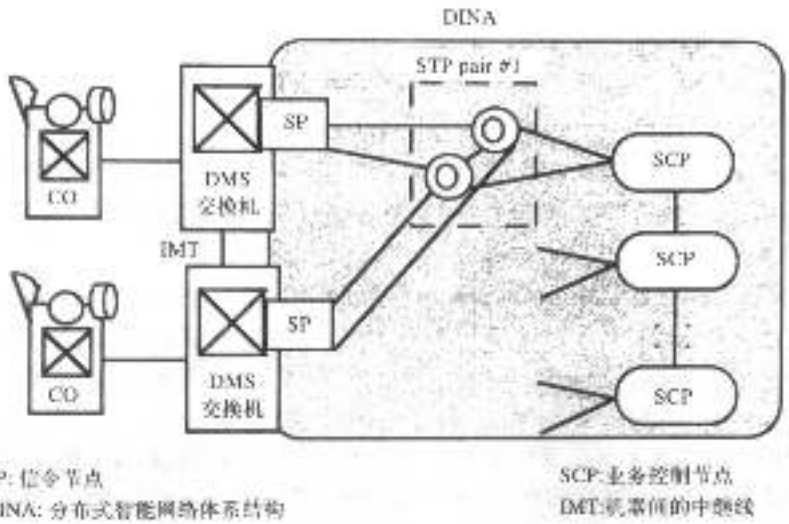


图11-11 Sprint的网络体系结构

与AT&T的分布式NCP网络一样，Sprint也从集中放置的SCP管理系统转化为一个分布式网络。Sprint的智能网络系统称为DINA（Distributed Intelligent Network Architecture，分布式智能网络体系结构）。

Sprint的网络受到位于堪萨斯城（Kansas City）的NOCC（Network Operations Control Center，网络运营控制中心）的控制和管理，该NOCC由两个RCC（Regional Control Center，区域控制中心）支持，其中一个位于萨克拉曼多（Sacramento），另一个位于亚特兰大。OSSC（Operational Support Systems Center，运营支持系统中心）提供更多的额外支持。所有的中心相互联系，并且网络一直在各地人员和软件的监视之下。这大大减少了任何人为因素的错误发生的几率。美国所有国内的和国外的交换机每隔15分钟向NOCC报告它们目前的状态，帮助中心决定在正常和出现故障的情况下，怎样重新选择路由。

11.6 基于SS7的虚拟网络介绍

在5.1.4节，我们介绍了虚拟专用网络，虚拟网络使用公共网来创建专用网络。尽管用户在使用公用网络的设施，但对用户而言仿佛拥有自己的专用网络。公共网络可以是PSTN的一个IXC部分，受到SS7网络的控制，或者是公用因特网。1993年，基于SS7的虚拟网络变得非常普及，这里我们将介绍各种不同类型的虚拟网络。基于因特网的虚拟网络称为VPN（Virtual Private Network，虚拟专用网），是第27章讨论的主题。尽管今天基于SS7的虚拟网络不像以前那样普遍，但它们仍然随处可见。AT&T称其虚拟网络为SDN（Software Defined Network，软件定义网络），MCI称其虚拟网络为Vnet，而Sprint称其虚拟网络为VPN（Virtual Private Network，虚拟专用网）。

11.6.1 虚拟网络的用途

设计并维护一个基于直接通信线路的专用网络会附带许多问题。专用网络的设计者必须决定一个呼叫是否和怎样跳出专用网从而获得对公共网络的访问。在决定是否需要为某些链路增加更多的中继线，或为其他链路减少一些中继线时，使用者必须不断地监视流量情况，还要定期做成本分析，看如何对网络进行最优化。同时，为不同地点服务的费用问题也必须

不断地评估，从运营商每月的账目中整理数据也是一项很繁琐的工作；而且如果专用网络节点数增加得越多，管理问题就越令人困扰。

虚拟网络是由ISACOMM（后来成为Sprint的组成部分）于1984年首先引入的，它减轻了管理专用网络的负担，而是让运营商的信令网络来负责管理。因为无论如何，大多数来自专用网络的流量，如WATS和DDD业务，都要通过公共设备发送，为什么还要对流量进行划分，使一些流经直接通信线路而剩余的经过PSTN呢？让PSTN承载所有经过其交换设备的流量，并停止为用户提供节省和先进的网络特性。

图11-12a给出了一个专用网，远端局并不承载足够的流量，不足以授权直接通信线路，所以从公司的专用网到远端局必须拨打10位数字的公共号码，这使得远端局感觉不属于该公司。而在图11-12b中，使用的是虚拟网络，所有这些位置都是专用虚拟网络的一部分，这样就不需要这些位置满足最小尺寸的要求或产生一定量的流量。运动中的人们，不管是在家还是用公共电话，或用手机都可以成为虚拟专用网络的一部分，产生的所有这些流量都经过PSTN，换句话说，虚拟网络提供了专用网络拥有的特性，而它的呼叫却要经过公共交换网络设备。

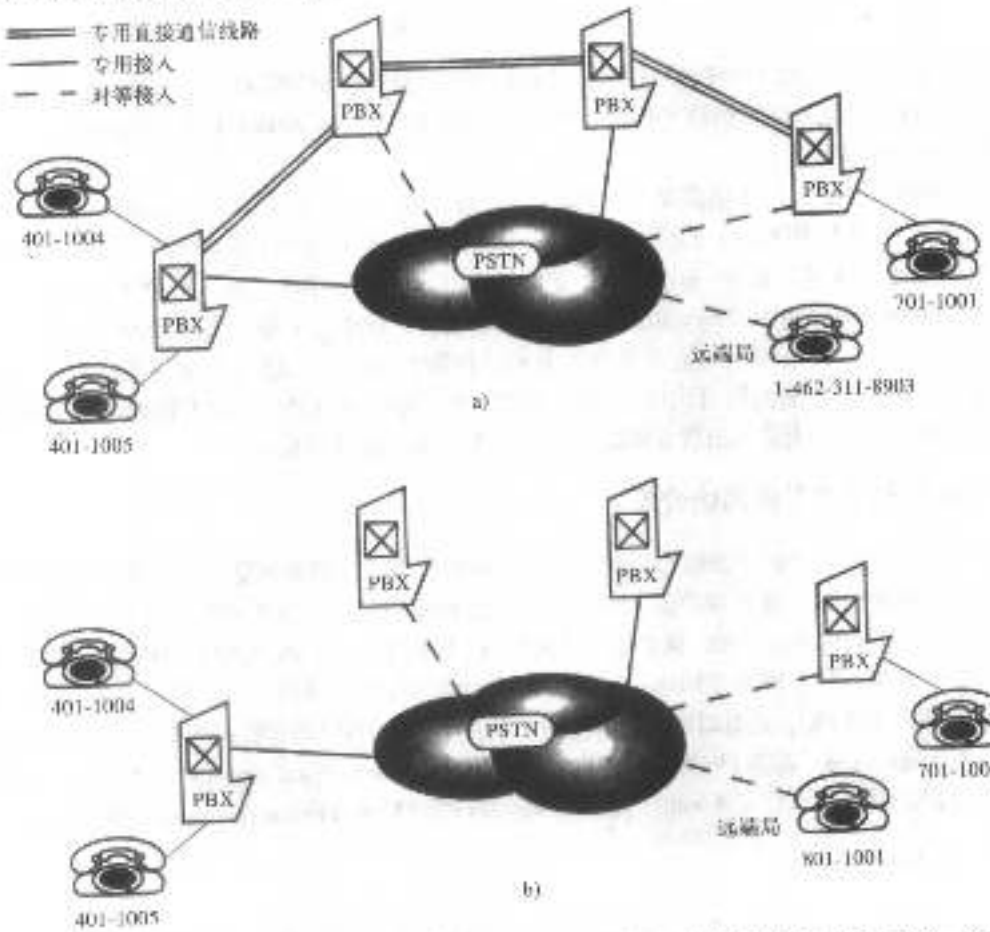


图11-12　a）显示了一个专用的直接通信线路网络，其中所有的PBX都是7位统一拨号方案的一部分，用10位公共拨号方案接入外地局；b）一个等价的虚拟网络，其中所有的位置都使用7位专用拨号方案，注意没有点到点的直接通信线路

呼叫的处理和路由方式是由为运营商的智能信令网络提供参数的用户规定的。虚拟网络与长途中央交换机业务类似，本地运营商利用中央交换机来进行交换。类似地，IXC通过虚拟网络为专用网络进行交换（然而，BOC同样提供虚拟网络业务）。

许多公司将专用直接通信线路网络与虚拟网络结合起来使用，这两种类型网络的结合称为混合网络。当两个或多个节点间的负载过重，以至于使用这些节点之间的直接通信线路比使用PSTN会大大节省开销时，就可以使用这种网络。

11.6.2 虚拟网络的运营

当呼叫由电话发起时，它会通过VN（Virtual Network，虚拟网）接入的方法（稍后将会介绍）之一进入运营商的POP，运营商的交换机将检测哪一个VN用户进行呼叫并把客户号码、主叫方号码、被叫方号码通过STP（Signal Transfer Point，信令传输节点）送给SCP（Signal Control Point，信令控制节点）。回忆一下，SCP是AT&T的NCP和MIC的DAP的统称。Sprint称之为SCP，SCP负责把7位数专用电话号码转换为相应的10位数公用电话号码或POTS号码，整个呼叫可以在4~6秒中完成。

虚拟网络并不是一种新技术，而是先进打包技术的一种新形式，对于用户而言，它仅仅是低成本长途服务的另一种形式。VN所依赖的先进技术是运营商的SS7网络，信令网的智能化使虚拟网络更加有效。与以前的信令技术不同，SS7是由软件控制的，要给虚拟网络新增特性，运营商只需修改软件并对所有的安装进行升级。

VN服务被认为由四部分组成。第一部分是由每个客户端接入POP的方法，第二部分是运营商网络的传输和交换机制，第三部分是存储在运营商信令数据库中的客户的VN描述，最后一部分是执行网络监视、重新配置以及流量分析的网络管理。

11.7 虚拟网络的优势

11.7.1 易于管理

前面已经提到VN的最大优势在于不像专用直接通信链路网络那样，需要不断地进行网络优化。由于所有的流量都经过PSTN，因此管理网络就变容易了。昂贵的直接通信线路被与POP相连的低成本接入线所取代。

11.7.2 公司范围的拨入方案

典型地，图11-12a所示的传统直接通信线路网络采用专用的7位数字拨号方案来呼叫专用网络中的任何电话，采用10位数字拨号方案来呼叫公共网络中的任何电话。所以，专用网中的用户呼叫专用网中另一个用户时需拨打一个7位数字的号码；而呼叫专用网外的用户时则需拨打一个10位数字的号码。专用网外的用户不论呼叫网内用户还是网外用户，都必须拨打10位数字。

当建立一个虚拟网（VN）时，任何电话的拨号方案都可以与以前相同。并不必使用户注意到虚拟网络的建立，也就是说对于用户来说它是透明的。拨7位数字的用户可继续拨打同样的7位数字，而拨10位数字的用户也可照旧拨打同样的10位数字。用户不必在意网内还是网外。由PSTN来完成必要的号码转换。7位数字的专用网络拨号方案可以与10位数字的公共网络拨号方案共存于同一个VN。如果用户选择，他（她）还可以使用7位数字的拨号方案。

11.7.3 更好的性价比

预备（provision）过程是一个建立VN并使其工作的过程，它不仅仅是线路和软件的安装。当运营商在VN中要建立一个新节点时，对于现存用户而言这个改变是透明的。开始这样的服务就称为预备网络。

以前需要花费10天~45天来预备一个虚拟网络的改变。现在，虚拟网络能很快地适应以满足新的网络需求，并为网络提供最佳性能。用户本身也可以做一些预备工作。

并不一定需要资金投入，在最初引入VN时，只有大的企业才能负担起高额的初建费用，但是由于免去税费的改革，现在就可能避免这些费用。例如，公司每年通过转向使用VN而节省了上百万美元。简而言之，VN用户享有专用网的所有优点而不用承担它们的问题和造价。

在任何地方都不需要接受过训练的人员来维护网络。在一个传统的专用直接通信线路网络中，如果可靠性关乎于两个城市，那么通常在它们之间建立一条多余的直接通信线路，这样就增加了网络的造价。然而，使用虚拟网，运营商的网络本身就存在许多位置之间的多余路径，这样整个VN就不可能出现瘫痪。事实上，VN声称有99.8%或更好的可靠性，也就是说出故障的时间每年少于2小时!

11.7.4 其他优势

虚拟网络的其他优势包含虚拟办公室和虚拟公司的概念。现在一名员工的办公室不必固定在某一位置，员工出现在哪儿，办公室就可以在哪儿，如在家中、在汽车上或在公共场所。

许多不同的公司互相依赖，为它们的客户提供一个无缝的服务，比如广告代理的生意。通过将这些在物理上分离但又相关的机构的网络相互连接成一个虚拟的网络就可以创建虚拟公司，这在某种定义上在它们之间建立了一种共同体并帮助其更好地工作，从而提供更周到的服务。

其他优点还包括：可以按照需要来改变网络，从而增加了灵活性。当出现问题时，有单一联系点。随着使用率的增加，提供的速率就会变小。使用户从每月必做的大量的流量研究中解脱出来。最后，可以赋予虚拟网络呼叫高于普通交换呼叫的优先权。紧急呼叫具有更高的优先权。如果在一个国家的某地区发生灾难，比如地震，此时每个人都想呼叫自己的朋友询问是否平安，这个优点就很显著。

在每个节点无须使用同一个生产厂家的PBX，这一点与专用网络是一样的。当建立VN时，你不必替换PBX，你可以给呼叫卡用户虚拟网的价格优惠，即使呼叫是来自网外的。在专用网内，一条中继线一次只能传送一个呼叫，所以如果两点间有更多的呼叫需求，那么就需要更多的中继线。然而，使用虚拟网时，用户不必关心是否有足够的中继线——由PSTN支持长距离的流量。

11.8 接入类型

VN优于专用直接通信线路网络的另一个优势在于除了传统的专用接入线外，VN还提供给用户多种接入方法。用户使用他们的本地中继线来提供交换接入VN，之后随着流量的增加，可以增加更多的本地中继线或可以使用专用的接入设备。这里概括的接入方法不仅适用于VN而且适用于其他的长途业务。

11.8.1 交换接入

如图11-13所示，PBX可以通过CO交换接入到POP，从PBX到POP的呼叫可以经过图中所

示的两条路径之一。如果直接路径忙，则呼叫被切换至另一条路径。类似地，本地电话通过POP进行长途呼叫也利用交换接入到POP。

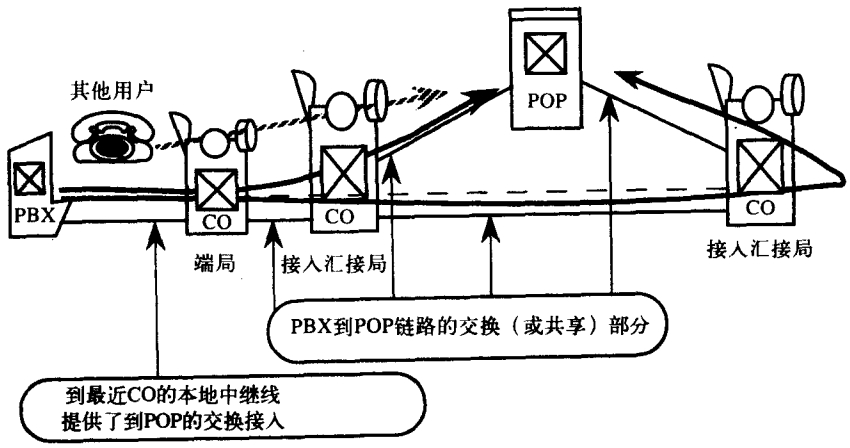


图11-13 交换接入到一个IXC的现有节点不提供预定的路径。同样，其他用户共享这条路径，该路径也可经过任何一个汇接交换机

当CO和POP之间的中继线由许多用户共享时，到该CO中继线的用户线被称为交换接入线，虽然该线只被那个用户使用。

通过交换接入到一个POP有四种类型，它们被称为“特征组”（feature group），图11-14所示为四种类型的特征组。在左边，PBX有一个本地中继线与最近的CO或端局相连，之后这个CO可以使用特征组C来提供交换接入到一个AT&T POP，或使用特征组A、B或D经由别的CO接到其他IXC的POP，现在让我们讨论一下这些特征组。

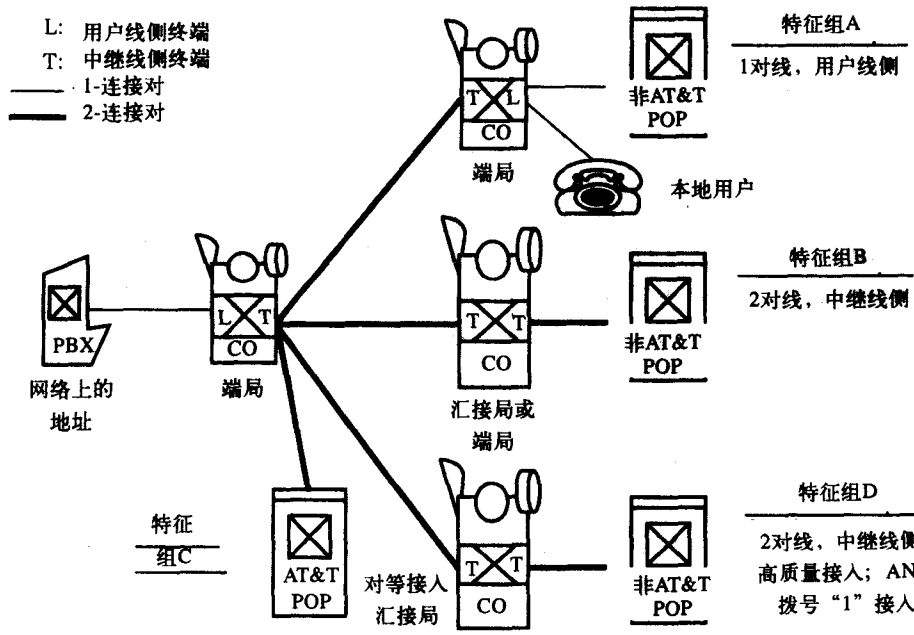


图11-14 交换接入的四个特征组，其中特征组D提供非AT&T的POP的质量最高的连接。然而，由于存在预脱离连接，因此交换接入到AT&T要比接入其他承载网络更快

交换接入的特征组A，在脱离到达一个非AT&T的POP之后可用。用户必须使用DTMF信令而不是旋转拨号电话来到达“替代运营商”，所以使用非AT&T的运营商打长途电话，就必须拨本地电话号码，之后呼叫者听到从POP传来的第二个拨号音。

与POP的连接是由“线路”这边提供的，而不是由电话公司的交换机的“中继线”那边提供（尽管这是一个低成本的连接，发送和接收的话音线路仅使用一对线）。但为了提供高质量的话音传输，中继线这边交换机的连接使用4条线来保持发送和接收路径分离。

特征组A使得POP看上去与普通电话号码类似。这种接入方式不必经由汇接局，因此这种接入类型变得越来越不常用了。

特征组B是一种预脱离（predivestiture）本地接入方法。这种接入方法需使用免费电话950-0XXX或950-1XXX。例如，要接入MCI，用户必须拨打950-1022，对于Sprint而言，需拨打950-1033，这是一个美国全国通用的号码。

听到一个语音或一个提示音之后，用户必须拨打另外的数字。这种接入方法由两对线提供，并且在电话局交换机的中继线这一侧有更好的传输质量，该交换机可以位于一个端局或位于一个接入汇接局。汇接局交换机必须升级为一个电子交换系统，以提供特征组B接入。由于使用这种接入必须键入授权号码，因此在接入IXC时，特征组B也变得不常用了。

然而，最近，美国全国性的大公司比如Pizza连锁店正在使用这种接入类型，作为廉价地得到800号码容量的方法。不必拨打与800号码相关的11个数字，Pizza的用户可以在美国全国任何地方拨一个950号码，就会被连到Pizza连锁店的全国网络上，在这种情况下，图11-14中的特征组B的POP将代表Pizza连锁店的网络节点交换机。这个交换机与服务CO位于同一个LATA。因为给这种接入方式分配的号码为950-1XXX，所以只有1000个可用号码，但是NANPA（North American Numbering Plan Administration，北美号码方案管理委员会）正在与BOC（Bell Operating Companies，贝尔运营公司）合作新增额外的9000个号码。这种接入方式不仅提供了高质量的4线连接，而且也提供了ANI（Automatic Number Identification，自动号码识别）和应答监督。使用特征组B而不用800号码需要用户拥有自己的网络以使LATA间的专用节点相连。正是因为这种950接入的可能开销，大多数公司发现800业务更适合一些。

特征组C的接入仅由AT&T公司提供，用户只需拨1就可接入AT&T公司的POP，这种接入提供4线连接和自动号码识别，由于这些线因存在预先脱离情况而直接送往AT&T的POP，因此这种接入类型提供了一个非常短的呼叫建立时间，参见图11-14。

特征组D的电路也是4线中继线连接，并且提供比特征组A和B更高的质量。这种高质量是由联邦法庭维持的，最多需要一个汇接局来容纳这些电路，并且汇接设备必须是完全电子化的。用户无需拨打7个数字来接入POP，而是仅需拨打1即可。

根据MFJ，接入任何IXC都应该与接入AT&T一样容易，因此，这些电路也称为同等接入电路。由于LEC为POP提供呼叫的ANI（Automatic Number Identification，自动号码识别）功能，所以也可以使用旋转脉冲拨号电话。

用户可以用两种方法接入POP：提前预订（presubscription）或者初始接入需要用户拨打区号1，之后是7位数字；而非提前预定或再次接入需要用户拨区号10XXX，之后是七位数字，这也称为“临时呼叫者”（Casual Caller）。

使用上述任何一种交换接入特征组接入VN都称为交换接入。使用交换接入来接入VN的地点称为网上（on-net）地点，因为这个地点预订了IXC并且所有呼叫都被连接到POP。这种

接入方式对于那些不需要专用线路来传送流量的小站点是非常理想的。

11.8.2 专用接入

DAL（Dedicated Access Line，专用接入线）或特殊接入线用于提供对VN的专用接入。严格地讲，这条线是专门供一个用户使用的而非共享的。不是按每次呼叫来计费，而是用户按月来付费。电路不通过CO的交换机，而是有硬件线路路由到POP。当然，只有流量高的用户会觉得DAL很经济，这通常就是现在的T1。

DAL与WAL（WATS Access Line，WATS接入线）是不同的，因为DAL提供的是与POP的专用连接而WAL提供的是与同等接入点的专用连接。如图11-15所示，在同等接入点处被交换。同样，WAL不能用于发送本地呼叫或接收任何呼叫。

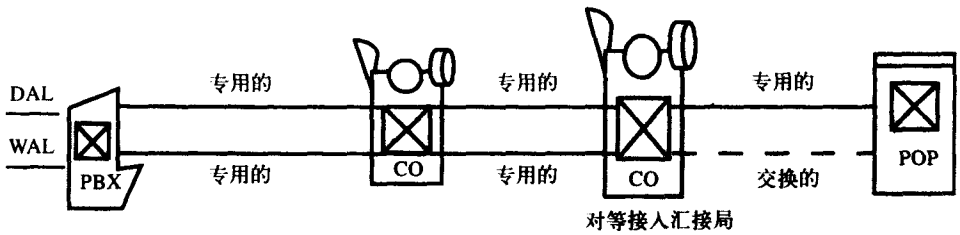


图11-15 上面的线路是一个DAL（Dedicated Access Line，专用接入线）提供一条到达POP的专用信道。下面的线路是一条WAL（WATS Access Line，WATS接入线）提供一条到达对等接入汇接局的专用信道。WAL不能用于发送本地呼叫或接收呼叫

一个DAL可以是单信道的模拟线或者是大容量的数字线路，比如说T1或T3。通常至少由6根单线组成的DAL的造价与一根T1专用接入线的造价相同，在这种情况下，用户几乎不用另外的花销就可以得到18个信道（24减去6）。收支平衡点是6线DAL还是14线DAL只是一个经济问题，它由单线DAL的成本与T1专用线路的成本相比决定，这些成本也由用户和POP之间的距离以及各自的税率所决定。

11.8.3 远程接入

当一个人外出旅行或无法接入公司的电话时，他/她可以使用800号码接入VN。这叫做远程或800号码接入，被认为是网外呼叫。远程接入也有多种方式。

一般来说，用户拨打的800号码可能是一个授权号码，也是一个被叫号码。于是，他/她可以接入VN的任何位置（网上位置）或任何DDD呼叫（网外位置）。然而，对于专用直接通信线路网络，用户呼叫在某些地区是受限的。

AT&T的远程接入称为NRA（Network Remote Access，网络远程接入）。不久BOC将提供800号码便携功能，用户可以保持同样的800号码并能交换它的IXC。

最后，网上位置是用户的VN描述中定义的任何位置，它存储在运营商的数据库中。这些地方可以通过交换方式或专用方式接入。它甚至可以是老板的住处（只要它定义在数据库中）。相反，任何没有在数据库中定义的地方称为网外。

与专用网相比，VN提供了更多的接入方式，这些方式把专用网络的优点带给了最小的客户站点，甚至带给了客户的暂时雇员。

习题

11.1 节

1. 1982年，电话网络被分为几部分？参见图11-1。

a. 10　　b. 40　　c. 52　　d. 100

2. 说明为什么过去的电话分级路由要比现在的方法花费更多的时间？

3. 在本地网中，什么类型的局把两个CO相互连接起来？

11.2节

4. 什么设备是与住宅室内线与本地电话网相连的接口？

a. SAC　　b. NID　　c. SLC　　d. IW

5. 当一个人从同一地区的一所房子换到另一所房子，想要保持原电话号码不变，那么必须为该用户改变什么才行？

a. TN　　b. OE　　c. CP　　d. HMDF

6. 在SS7网络中，两个CO之间的语音信道传送的是什么类型的信令？

a. 忙回音　b. 振铃回音　c. 拨号音　　d. DTMF

7. 什么设备采用10对线多路复用到CO的96条用户线上？

8. 指出哪些SS7类型的局允许不在SS7网络的CO成为该网络的一部分。

9. 用图11-2解释一下，交换线路和专用线路怎样路由到CO？

10. 用图11-4描述从迈特森（Metuchen）发起的对位于萨默维尔（Somerville）的贝尔大西洋800号码的呼叫所发生的步骤。

11.3节

11. 如果AT&T有117个4ESS，那么在使用另外一个中间交换机的两个交换机之间的备用路径共有多少？

a. 100　　b. 115　　c. 116　　d. 117

12. AT&T的哪种寻路（路由）技术需要使用机器间中继线的同时负载容量？

13. 描述AT&T信用卡呼叫怎样进行。

14. AT&T扩展其网络的未来计划是什么？

11.4节

15. 下面哪个不属于MCI网络中的一层？

a. 应用层　　b. 逻辑层　　c. 管理层　　d. 物理层

16. 帮助MCI交换机处理非交换相关任务的处理器是什么？

17. MCI使用的是什么类型的交换机？它们是由唯一一个生产厂商制造的吗？如果是这样，优势是什么；如果不是，又有什么优势？

11.5节

18. AT&T. MCI和Sprint的SCP分别用什么来命名？

19. Sprint使用的寻路方法的名称是什么？

20. 和AT&T相比，Sprint的传输线有多少英里？列出传输线比较长的优点和缺点？

21. Sprint正在把光纤环转换成哪种类型的SONET环？

22. Sprint正在做什么来增加其现有光纤的容量？

11.6节

23. 下面哪一个不是虚拟网络的优势？
    a. 它们需要在网络产品上大量的投资，如果在二级市场出售这些产品的话可以回收其投资。
    b. 它们急剧减少了在专用网络上必须做的流量工程。
    c. 网络配置的改变可以在合理的时间内完成。
    d. 它提供比传统直接通信线路网络更好的可靠性。
24. MCI称它的虚拟网络为
    a. VPN　　b. SBS　　c. Vnet　　d. SDN
25. 在虚拟网络中，用户的数据存储在什么地方？三个主要运营商分别如何命名该数据库？
26. 列出虚拟网络的4个组成部分。

11.7节

27. 专用网的拨号方案通常有多少位数字？
28. 讨论一下虚拟网络在管理方面的优势。
29. 讨论一下虚拟网络在统一拨号方案上的优势。

11.8节

30. 在虚拟网络中哪一个特征组是最不常用的？
    a. 特征组A　　b. 特征组B　　c. 特征组C　　d. 特征组D
31. 用WAL可以进行哪种类型的呼叫？
    a. 接收本地呼叫　　b. 接收LATA之间的呼叫
    c. 发送本地呼叫　　d. 发送LATA之间的呼叫
32. 哪一种特征组用来提供到非AT&T POP的高质量的接入？从练习2的选项中的选择。
33. 哪一种特征组为POP使用中继线侧的终端？
34. 典型地，哪一种接入方式允许外出的人使用虚拟网络？
35. 讨论一下对等接入的特点和两种方法。

第12章 无线通信与CDMA

12.1 AMPS

本章的开始将全面介绍AMPS（Advanced Mobile Phone Service，高级移动电话业务），这是现在在美国仍广泛使用的模拟通信系统。之后我们将了解与现代数字系统相关的内容和问题。现代数字系统被视为是第二代解决方案。在本章最后一部分，我们将介绍CDMA，这是广为使用的无线接入方法，也是第三代无线标准许多建议的基础。

12.1.1 概述

现代蜂窝电话系统的正式名称为AMPS。EAMPS（Extended AMPS，扩展的AMPS）用来指分配给蜂窝服务的一组新频率集，这组频率总共提供了832个信道，而不是AMPS的666个信道。

AMPS（或EAMPS）的基本概念是简单的，但其设计和实现却是复杂的。一个地理区域被划分为圆形区域，称为小区，半径大约为2~12英里。出于设计的需要，通常表示为六边形区域。在图12-1中，各小区由一个小区基站提供服务，该基站包括一个发射机、一个接收机、天线以及相关设备。小区的基站直接与MTSO（Mobile Telephone Switching Office，移动电话交换局）相连接，该交换局又与汇接局或本地电话网的五级局（或CO）相连。本地电话公司也指有线电话公司，可以是BOC（Bell Operating Company，贝尔运营公司）。对于蜂窝系统而言，MTSO类似于CO，在给定的区域，半数的可用蜂窝业务由本地的有线公司提供，而另一半靠各公司相互竞争提供。

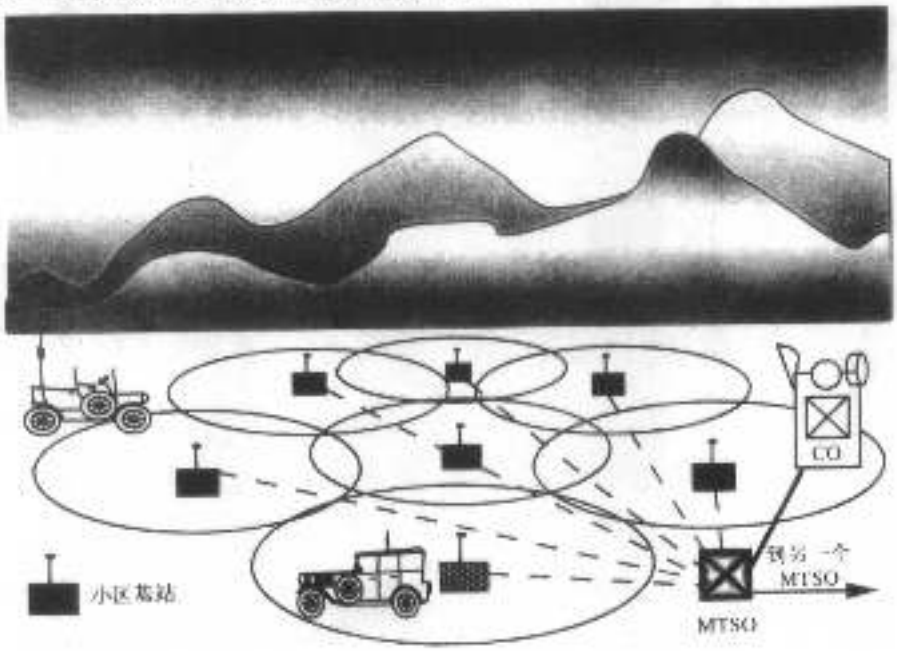


图12-1 蜂窝电话系统的布局图

来自本地电话网的所有呼叫被交换到合适的小区基站，在那里移动电话可以得到最好的接收效果。同样，来自移动电话的所有呼叫由小区基站发送至信号最好的MTSO，之后MTSO将呼叫转至CO。

根据哪个小区基站提供最佳质量的信号，移动单元可在任何时间锁定到相应的基站，并且所有的通信都发生在那个基站。当汽车从一个小区进入另一个小区时，小区基站注意到信号电平的衰落，会在MTSO的帮助下把通信切换到另一个小区基站，这就叫做越区切换。

12.1.2 AMPS的优势

事实上，在AMPS和IMTS（Improved Mobile Telephone Service，改进的移动电话业务）之前，我们有各种LMR（Land Mobile Radio，陆地移动无线电）系统。这些也称为双向无线电，现在仍广泛用于救护车、出租车等。在移动无线电安装进交通工具之前，其频率由技术人员设定，并且该频道专用于特定的无线电，在给定区域中其他任何人都不能使用那个频道（即使它是空闲的）。对于警车和装备卡车而言，这并不是对频带的浪费，因为它们都在不断地利用这些频道。然而对于个人使用而言，并不会整天都在使用移动电话，所以证明这种系统的效率不高。

IMTS引入后（这还是在AMPS之前），它提供了一种按需分配信道的无线系统。当用户挂断电话后，相应的信道就被释放，并可以分配给其他用户使用。通过这种方法，IMTS可以为多于可用信道数目的更多用户提供移动电话业务，这可能是因为每个人并不是一天24个小时都需要无线服务。

IMTS采用大的覆盖区域，通常半径在20英里，这需要发射机的功率高达250W。同时，同样的无线频率也不能在相距75英里以内的两个区域中重复使用，否则将在其他基站使用的频道内存在干扰。

这样一来就限制了移动电话可用信道的数目。例如在20世纪70年代中期，纽约市只有12个信道服务于550个用户，还有近4000用户处于等待状态。如果该地区的需求增加也没办法快速地扩展服务。

另一方面，由AT&T公司研发的AMPS可以在一个服务区使用许多小区。但是这些小区的面积小于以前的小区，小区发射机的发射功率也降至100W，移动发射机的发射功率为3W，而便携式单元的发射功率为0.6W。由于输出功率降低了，因此两个小区之间的距离可以仅为2英里（即间隔一个小区），并且仍然可以使用相同的频率集。来自使用相同信道的相邻小区的干扰称为同信道干扰，只要C/I（Carrier-to-Interference，载波比干扰）之比大于17dB，同信道干扰就可以忽略不计。这就意味着只要所选小区的信号强度高于干扰小区的信号强度17dB，那么使用同一组信道的两个小区就不会引起干扰。

所有这些为可用带宽提供了更多的信道。如果某地区的服务需求增加，那么小区还可以进一步分裂为更小的小区，分裂后小区的发射机要进一步降低其有效输出功率。这样做的效果就是在给定小区增加了可用信道的数量。当然，小区分裂的设计和规划都是一个复杂的过程，但至少这是可行的。

小区扇区化技术也可提高频谱或可用带宽的利用率。小区扇区化包括把小区划分为三个扇形区域，此时不是在一个小区的所有方向传输所有可用信道（使用全向天线），而使用定向天线在三个扇形区域之一来传输1/3的可用信道。小区扇区化通过把使用相同信道的扇区相对反方向安置，可以使小区之间距离更近，这样就增加了系统的信道容量。

12.1.3 使用不规则小区形状的理由

通常，为设计的需要，常用六边形形状描绘小区。然而实际上，天线是以圆形方式发送信号的，如图12-2所示，圆形辐射的形式不是最终获得的形式。

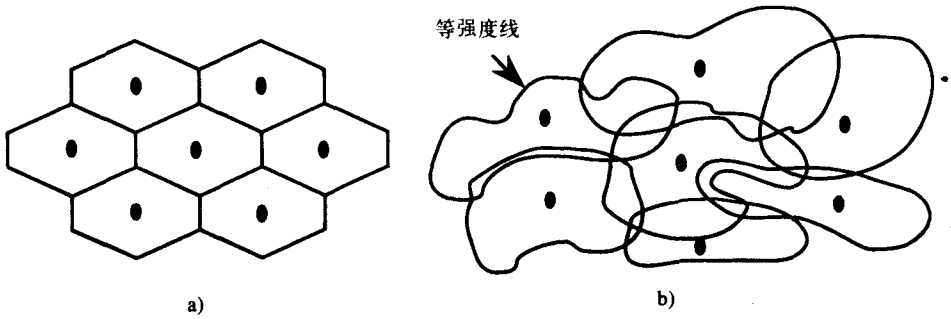


图12-2 a) 设计蜂窝网络时所使用的六边形形状，b) 小区的实际形状通常是不规则的

蜂窝系统的最初应用只是简单地在一些人口和车流高度集中的地区设立小区，并不是蜂窝状布局。而且，如果小区的中心恰巧落在河上或落在一个塔或城市建筑物上，那么小区所覆盖的区域就要稍作移动。有时，使用定向天线来避免其他系统的干扰。有些区域不允许有发射塔楼，因此向下倾斜的定向天线就要设置在城外。通常，一个小区覆盖区域的地形如高大建筑物、山脉、峡谷等等，改变了小区覆盖区域的期望形状。所有这些因素破坏了小区的对称性，使小区变成了不规则的形状。

12.1.4 小区信道的分配

如表12-1所示，FCC（Federal Communications Commission，联邦通信委员会）已经将824MHz到851MHz和869MHz到896MHz分配给蜂窝系统，这就是说发射可用带宽为25MHz并且接收可用带宽为25MHz。因为每一个单向信道需要0.03MHz，所以可以带宽25MHz除以0.03MHz就得到蜂窝系统总共有832个信道。

832个信道被等分为2个416信道组，称为A组和B组，其中一组信道由有线公司来使用，另一组信道由非有线公司使用。在任何情况下，移动电话的接收信道频率要高于发射频率45MHz，例如，第333号信道以835MHz的频率发射，而在880MHz的频率接收来自移动台的信号。

表12-1 信道分配

	移动手机发送频率	移动手机接收频率
每信道带宽	0.03MHz	0.03MHz
A组与B组的频率范围	824~849MHz	869~894MHz
包括未用部分的总频谱	824~851MHz	869~896MHz
A组的信道数	416	416
B组的信道数	416	416
信道总数	832	832

12.1.5 频率复用

只考虑一组信道，或某蜂窝电话公司在一个地区的带宽分配，共有416个可用信道，其中21个用于传输信令，剩余395个信道用于传输话音。各小区基站仅需要一个信令信道与其覆盖

区域内的所有移动电话进行信令信息的通信。所以每21个小区都使用相同的信令信道。

如果每个小区使用所有395个信道进行通信，那么相邻小区的信道就会相互干扰。因此，为了降低同信道干扰，就要将小区划分成不同的组，使得分配给一个小区的信道在该小区组中是唯一的。这样一组中的小区数目称为频率复用因子或简记为k，也就是说，395个信道被划分成k个信道组。通过这种方法，两个使用相同信道组的小区彼此就不是相邻的而是分离的。

例如，图12-3所示的蜂窝系统中k为12，那么各小区就大约有32（395/12）个可用话音信道。标号相同的小区使用同一组32个信道，然而，两个这样的小区之间的信道干扰是可以忽略不计的，因为它们之间的距离足够远。k的典型值为7，但是可以在4到21之间变化。当k减小时，每个小区可用的信道数就增加，但同信道干扰的机会也增加了。为了进一步降低同信道干扰，小区通常被划分为3个扇区，相应的可用信道也分成3组，每一组支持1/3小区范围内的通信。在图12-3中，这意味着每个扇区有10个或11个（32/3）信道。

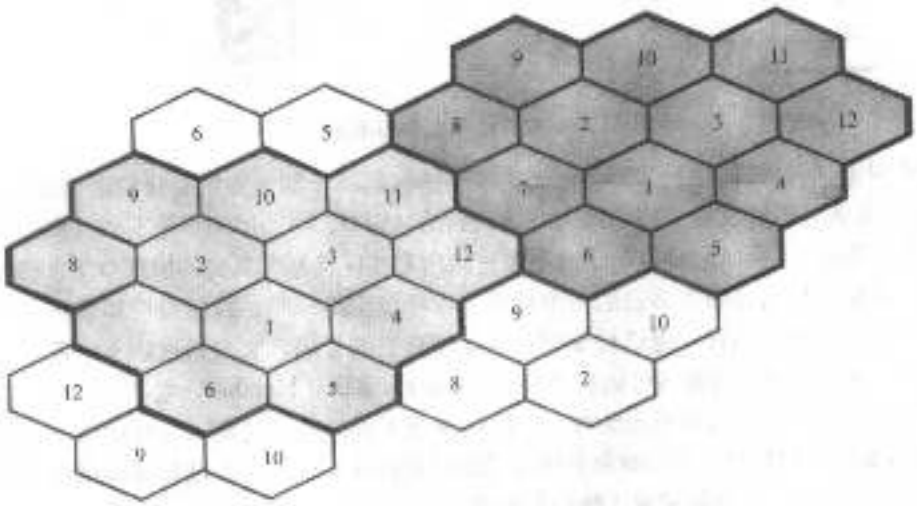


图12-3 K=12的频率复用模式

12.1.6 操作

当移动单元开机之后，并且没有拨打或接听任何呼叫，则称它处于空闲状态。处于空闲状态时，移动单元扫描21个信令信道，并锁定信号最强的小区基站，通常是距离最近的基站。现在移动单元就可以接收或发起呼叫了，因为它已经建立了和基站的无线链路。如图12-4所示，这称为自定位。小区基站并不知道哪些移动单元正在收听其信号。在大约1分钟之后，移动单元重新扫描21个信道，并可以每次锁定一个不同的基站（或监测信令信道）。

在某些蜂窝系统中，移动台可以通知基站与之锁定，这称为注册。该信息在MTSO需要知道位置信息来完成一个对它的呼叫时是很有帮助的。

当移动单元要进行呼叫时，它会通过信令信道向所选小区基站发送被叫号码。基站将该电话号码转发给MTSO，之后MTSO把基站与有线CO相连起来。与此同时，MTSO分配一个从所选小区基站到移动电话的空闲全双工话音信道。小区基站通过信令信道通知移动单元为本次呼叫分配了哪个信道，之后将其发送机和接收机调整到这个话音信道。最后，当目的地的电话铃起振时，蜂窝电话就会收听到。

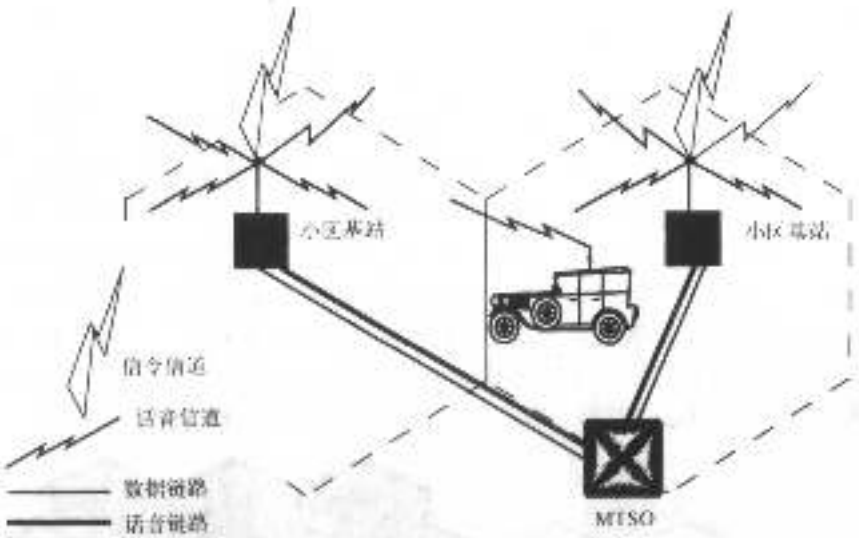


图12-4　两个小区之间的系统操作

当呼叫来自有线网络时，CO会检测到该电话号码属于某个特定的蜂窝电话公司。之后，CO将这个电话号码转发给相应的蜂窝电话公司的MSTO。因为MSTO并不知道移动电话的位置（除非注册过），所以它将该电话号码发送到所有小区基站和其他的MTSO及它们各自的小区基站。之后小区基站将在各自的信令信道上寻呼该电话号码，希望被叫移动单元开机并位于其中一个小区内。当移动电话检测到正在寻呼自己的号码，它会通过信令信道对小区基站作出应答，并将其自己的电话号码和ESN（Electronic Serial Number，电子序列号）重新发送给小区基站。ESN证实移动单元的身份，以便进行正确的电话计费（当移动单元进行呼叫时也要发送ESN）。MTSO检查ESN和电话号码之间是否匹配，并在基站和移动单元之间分配一个全双工话音信道。这样就完成了呼叫的处理。

不论谁发起呼叫，一旦移动单元关闭发射机，信令信道中就会传输一个特殊的信令，并且MTSO将释放该话音信道供其他呼叫使用。

12.1.7　越区切换

通过基站进行通信的移动单元最终可能会进入另一个小区，原小区基站注意到来自该移动单元的信号强度正在减弱，之后它将请求MSTO分配其他基站与该移动单元进行通信，接着MTSO将要求邻近小区检测正在使用的话音信道的信号强度，能最佳接收该移动单元信号的基站将被通知与其进行通信，但此时的通信需利用一个不同的信道，即一个空闲的新话音信道，并且是分配给该基站的信道之一。越区切换过程中断通信长达200毫秒，这并不会严重影响话音通信，但对数据传输影响较大。

12.1.8　小区分裂

蜂窝通信系统的优点之一在于如果通信流量增加到接近给定小区的负载时，小区可以被分裂成几个小区，从而增加这个地区的信道数目。

图12-5所示为小区分裂的两种方法。第一种方法是不使用原小区的基站，而是将小区分

成四部分，创建4个新的小区。另一种方法更为常见，即原小区面积减小，而新创建的6个新小区围绕着它。

假设原小区基站有70个信道，它被分裂成6个新小区，那么总共7个小区，其中每一个使用10个信道。然而，这样的每个小区能够最终将它们的容量增加到70个信道，从而增加该地区的可用信道数。说起来容易做起来难，工程师在分裂小区时必须万分小心，这样才能使系统的其他部分正常工作，不受干扰或中断。

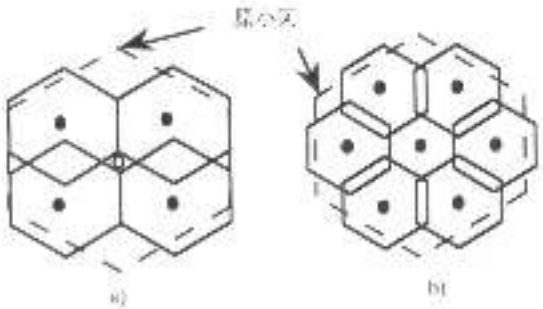
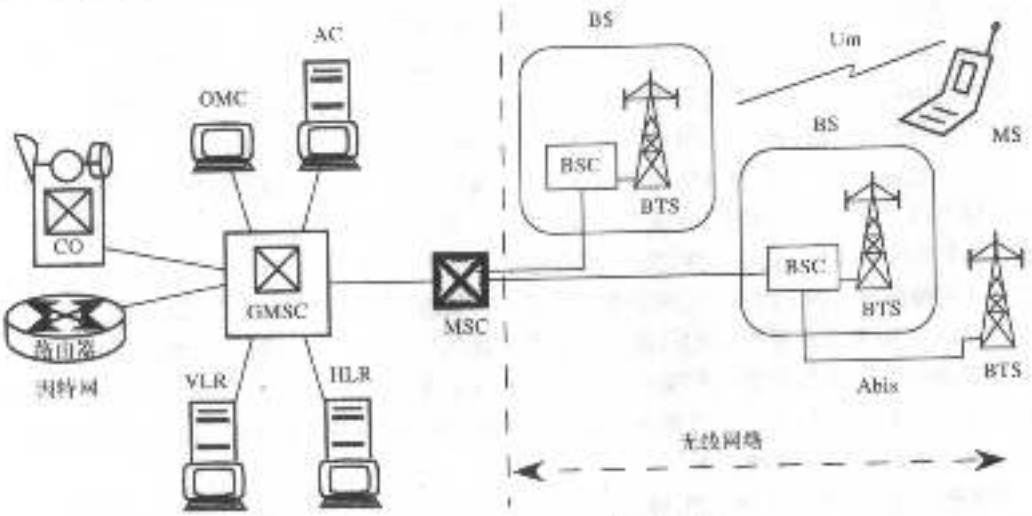


图12-5 小区分裂的两种方法：a) 没有原小区，b) 减小了原小区的有效面积

12.2 现代无线系统

12.2.1 无线系统模型

AMPS是第一个重要的蜂窝系统。今天，在数字系统的许多前沿研究工作的基础上，出现了许多协议。为了说明第2代和第3代系统中所使用的多种方法的功能部件，常采用图12-6所示的典型模型。



GMSC: 网关移动交换中心
MSC: 移动交换中心
BTS: 基站收发台
BSC: 基站控制器
BS: 基站
Um: 空中接口

HLR: 归属位置寄存器
VLR: 访问位置寄存器
AC: 鉴权控制器
OMC: 操作和维护中心
MS: 移动台
Abis: BSC与BTS之间的接口

图12-6 现代无线网络的组成

这些组成部分可分成5类：无线部分、交换机、数据库、处理器和外部网络。图12-6所示的无线发射部分为移动电话和基站。BS（Base Station，基站）包括BSC（Base Station Controller，基站控制器）和BTS（Base Transceiver Station，基站收发台），BSC可控制多个

BTS，它们之间的接口称为Abis（BSC-BTS Interface，BSC-BTS接口）。Um（Air Interface，空中接口）定义了MS（Mobile Station，移动台）与BS之间的通信是怎样进行的。

图中所示的交换机为MSC（Mobile Switching Center，移动交换中心）和GMSC（Gateway Mobile Switching Controller，网关移动交换中心），它们代替了在传统的AMPS系统中所使用的MTSO。GMSC正如其名称所指示的，用于将外部网络连接到移动网络，这些外部网络包括PSTN（在图中由CO代表）、因特网、ATM以及包括SS7网络在内的其他类型的网络。

数据库与处理器连接到交换中心。数据库被称为HLR（Home Location Register，归属位置寄存器）和VLR（Visitor Location Register，访问位置寄存器），HLR永久存储与网络智能相关的用户数据，而VLR暂时存储由该地区网络所服务的客户的用户数据，AC（Authentication Center，鉴权中心）提供移动用户身份的认证。AC和其他提供话音消息与公告的部件都是处理器的具体实例。

12.2.2 基本无线原理

接入方法：发射机接入空中接口以向指定接收机发射的基本方法有三种。FDMA（Frequency Division Multiple Access，频分多址接入）使用不同的频率进行接入。AMPS使用的是FDMA。发射机可以利用不同的频率在同一时间进行发送。

发射机利用TDMA（Time Division Multiple Access，时分多址接入）可以在同一频率轮流发送。CDMA（Code Division Multiple Access，码分多址接入）与前二者不同。使用CDMA的发射机可在任何时间利用全部频率发射，然而，发送给特定接收机的发射信号是由加载在发射信号中的特定数字码字来识别的，接收机将自己的码字应用到复合发射信号中对发射给它的消息进行解码，将自己的码字与发射信号进行相关运算之后，发送给它的消息就会清楚地被解码。如果复合接收信号中没有发射给接收机的编码消息，接收信号就表现为噪声。下面我们做一个类比。

假如你走进机场，人们都在使用中国普通话、葡萄牙语、西班牙语和阿拉伯语进行交谈。如果你只懂英语，那么你听到的只有噪音。另一方面，如果你仅懂阿拉伯语，那么你只能听懂阿拉伯语。如果你仅懂西班牙语，那你就能听懂西班牙语和少量葡萄牙语，因为这两种语言有点相近，CDMA工程师称这两种语言不正交而称中国普通话、英语、西班牙语和阿拉伯语彼此是正交的。

CDMA必须考虑功率控制的问题。如果你只懂阿拉伯语，当说阿拉伯语的人们在机场的另一个角落时，那么你只能听到噪声。即使你和他们很近，但一个说中国普通话的人正在使用扩音器大声讲话，那么你也只能听到噪音。在CDMA系统中，功率控制是一个非常重要的问题，这一点将在后面详细叙述。

声码器：在PSTN中使用的PCM（Pulse Code Modulation，脉冲编码调制）需要每个信道有64kbps的带宽。今天在电话网中使用光纤变得越来越普遍，64kbps的信道带宽并不是很理想。然而，无线系统所分配的频带容量是固定的。这里急需降低话音信道的比特率。

PCM使用的编解码器实际上是数字化话音信号之后再进行解码。声码器（一种特殊类型的编解码器）不是对话音进行数字化，而是对描述话音信号的参数进行编码，将话音信号的比特率降为8~13kbps，大大低于64kbps。通过降低比特率，同一频段在给定的时间内就可允许更多的用户。比特率还可以瞬时进一步降低，这是因为在通话过程中，人们并不是连续发送话音，而是常常处于听或暂停状态。

PCM编解码器类似于给某人演奏钢琴进行录音，之后在另一个时间再重新播放。而一个声码器类似于在纸上记下一个人演奏钢琴的乐谱，之后由另一个人来重新演奏乐谱。而录音

要比记录乐谱使用更多的比特。正如转录器记录下弹奏乐谱的参数一样，声码器也仅发送声音的参数。这使得声码器能以比基于PCM的编解码器低得多的速率运行。

12.2.3 无线频谱

图12-7给出了各种不同的无线系统和它们处在电磁谱中的位置。移动发射信道的所有频带出现在移动接收信道之前。正如我们已经看到的，AMPS的频带范围是从824MHz到849MHz和869MHz到894MHz，这与第二代数字系统的频带相同，第二代系统是指IS-54、IS-136和IS-95，这些将在后面讲到，IS-95现在称为TIA/EIA-95。

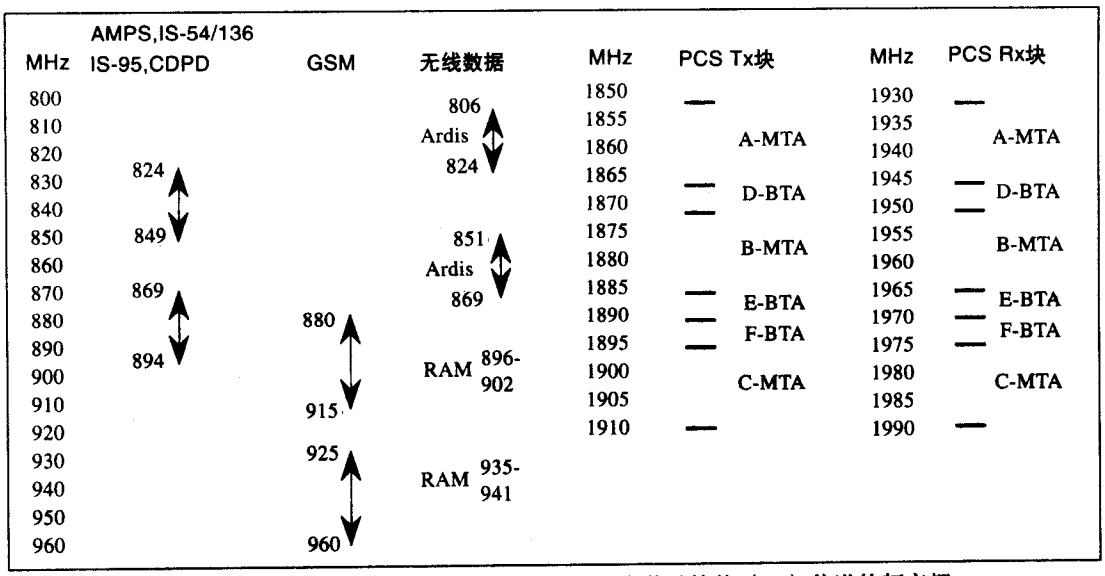


图12-7 主要无线业务的频率分配。现有的所有移动接收（Rx）信道的频率都高于移动发射（Tx）信道的频率

摩托罗拉公司的Ardis（Advanced Radio Data and Information Server，高级无线数据和信息服务器）和RAM广播与贝尔南方公司的RAM移动数据提供高达19.2kbps的数据业务。Ardis给用户提供称为“bricks”的专用终端，而RAM则提供与任何笔记本电脑一起工作的调制解调器。

一个更标准化的发送无线数据的方法称为CDPD（Cellular Digital Packet Data，蜂窝数字分组数据），它可以与现存蜂窝网处于同样的频率范围，即使它用在蜂窝区域，也使用数字化传输，它采用一种称为“信道跳变”（channel hopping）的技术，使得在传输的同时可立刻转换信道。而且，它被设计用于以19.2kbps的速率传输数据。然而9.6kbps的速率是更为普遍的。在后面我们将介绍主要用于欧洲的GSM，它运行于880MHz到960MHz的频段。

PCS（Personal Communications Services or Systems，个人通信业务或系统）运行于2GHz附近，如图12-7所示。这里有六个频率组，其中称为A、B和C的三组频率用于MTA(Major Trading Areas，主要贸易区)，而D、E、F三组频率用于BTA（Basic Trading Areas，基本贸易区）。各MTA频带为30MHz，其中15MHz用于发送，15MHz用于接收。各BTA频带只有10MHz。这个频率范围所使用的协议包括TIA/EIA-95、IS-136、GSM和包括第三代系统在内的其他协议。

12.2.4 固定无线系统

这段频率范围之后就是高于2GHz的频率。这里定义了几个ISM（Industrial, Scientific, and

Medical; 工业、科学和医疗）频段，参见图12-8。这些都是未经许可使用的频带，使用这些频带工作的设备能很快投入使用。这些频带也用于宽带无线接入。在ISM频带内使用的设备大多使用DSSS（Direct Sequence Spread Spectrum，直接序列扩展频谱）技术，这与CDMA是类似的。在这些区域、设备之间的相互干扰很普遍，所以不同的公司期望使用不同的编码方法来最小化干扰。

2.150-2.162	MMDS				
2.400-2.4835	IEEE 802.11b Unlicensed ISM				
2.596-2.644	MMDS			27.500-28.350	LMDS
2.650-2.656	MMDS			29.100-29.250	LMDS
2.662-2.668	MMDS	5.725-5.875	未经许可使用的 UNNI	31.000-31.075	LMDS
2.674-2.680	MMDS	24.000-24.250	未经许可使用的 ISM	31.075-31.225	LMDS
				31.225-31.300	LMDS

MMDS: 多点多信道分布式业务　　ISM: 工业，科学和医疗

LMDS: 本地多点分布式业务　　UNNI: 未经许可使用的国家信息基础设施

图12-8 固定无线频谱。所有频率都以GHz为单位

IEEE已经在这个频段定义为802.11b标准，该标准提供了无线局域网的连接，承诺提供高达11Mbps的数据传输速率。由于在无线环境中很难发觉冲突，因此在这个标准里使用了特殊的避免冲突的技术。使用扩展频谱技术不能轻易断定接收到的噪声是由冲突引起的还是由正常噪声引起的。因此，这种接入方法称为CSMA/CA（CSMA with Collision Avoidance，带有冲突避让的CSMA）。一种称为CCK（Complementary Code Keying，补码键控）的复杂编码方案用于传输几个数据比特，这使得IEEE 802.11b协议的传输速率从2Mbps提高到11Mbps。

我们在12-8图中看到的接下来的频带集合称为MMDS（Multipoint Multichannel Distribution Services，多点多信道分布式业务），这里“多点”和“多信道”也是可以交换的。这些信道从1990年就已经分配了。然而，它们被分配用于提供无线电视节目；因此，这个频段也称为无线电缆。1999年，Sprint和MCI Worldcom公司成立了这些频段的运营公司，而且若FCC允许双向通信来支持因特网接入，该市场就有望免税。

在MMDS以上的频段是LMDS（Local Multipoint Distribution Service，本地多点分布式业务）频段。MMDS分配了200MHz的频段，而LMDS分配了1GHz的频段。然而，LMDS设备的造价更高，并且覆盖范围更小，它更易受到大气环境的影响。

12.2.5 PCS

传统上，我们利用拨号通过PSTN进行通信。而在PCS（Personal Communications System，个人通信系统）中，不论一个人在哪里，都能呼叫到这个人。定位被叫方并提供连接是信令系统关心的问题。人们不再需要提供家庭电话号码、办公电话号码、手机号码和他们的日程安排，我们只需知道个人的号码就可以在电话上与之联系。

一个人只需携带一个低功率的便携式电话，如果他在家里，那便携式电话的作用类似于无绳电话，与家中的基站通信；如果他在车里，便携式电话的作用就像手机；如果他在购物中心，便携式电话就与微蜂窝基站通信；如果他在工作场所，便携式电话就与无线PBX系统通信。每次都选择最低廉的无线通信方法。通过使用最近的基站（它可以是PBX或是无绳基站），你可以得到最好的接收效果。

这是使用PCS的最终目的。现在PCS可以提供比蜂窝系统更多的功能和服务，而且在PCS频段内的所有服务都必须是数字化的。通常，PCS小区要小于蜂窝小区。

12.3 数字无线系统

12.3.1 欧洲的GSM

欧洲统一的数字蜂窝系统标准于1982年建立起来。它与PSTN中的非统一的拨号方案不同，也与当时存在的非兼容模拟移动蜂窝系统不同。它成为众所周知的GSM（Global System for Mobile Communication，全球移动通信系统）。

GSM同时采用TDMA（Time Division Multiple Access，时分多址接入）和FDMA，为用户提供蜂窝接入。话音被一种称为LPC-RPE（Linear Predictive enCoding with Regular Pulse Excitation，带有规则脉冲激励的线性预测编码）的技术以13kbps的速率数字化。GSM的基本单元是时隙，每个时隙为0.577ms，一个时隙传输156.25比特，如图12-9所示。一个时隙的开始和结束均为3个全零尾比特。在8.25比特的保护时隙期间，不进行任何传输，以适应RF（Radio Frequency，射频）的上升和下降的延时。

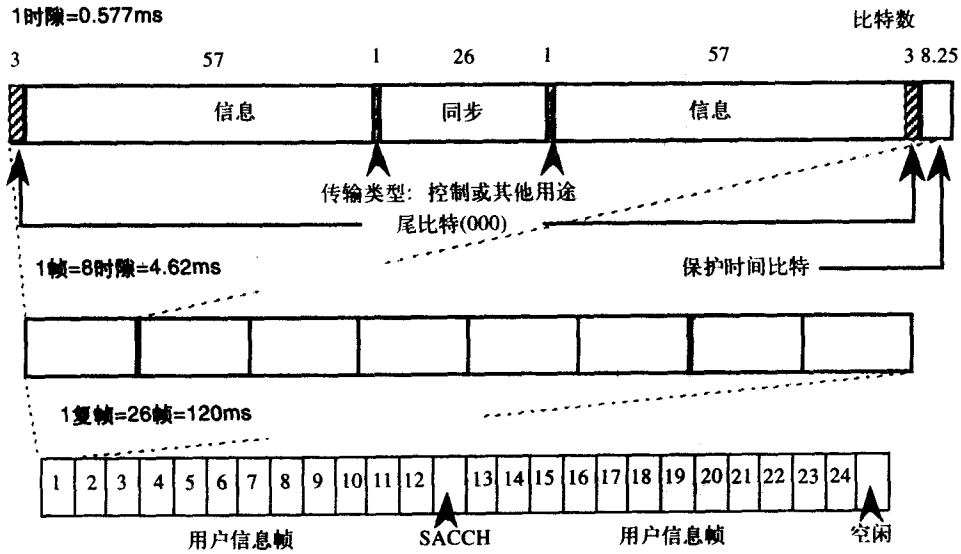


图12-9 GSM中的时隙和帧格式

两组57比特用于传输用户信息。与一组信息比特临近的单个比特用于指示是否发送了控制信息、中断话音或数据信道。最后，26比特用于保持数字系统的同步。每一个移动终端都分配有它自己的时隙。

1帧包括8个时隙，26帧组成一个复帧。在这26帧中有两帧用于其他目的，其中一帧称为SACCH（Slow Associated Control CHannel，慢速辅助控制信道），用于发送低带宽控制信息，另一帧空闲。

12.3.2 北美的IS-54/136

与欧洲同时拥有5个不同的模拟蜂窝标准不同，加拿大和美国只有一个标准——AMPS。但是，欧洲已为GSM系统分配了一个新的频段，而北美则是限制在已有的模拟蜂窝系统上演化一个数字系统。因此，这个系统被称为双模（dual-mode）系统，即“EIA的IS-54标准”（Electronics Industry Associations Interim Standard 54，电子工业协会临时标准）。

IS-54采用一种称为VSELP（Vector Sum Excited Linear Prediction，矢量和激励线性预测）的技术以13kbps的速率数字化话音，其时隙的结构根据移动电话处于发射还是接收状态而不

同，参见图12-10。一帧由1944比特组成，用40ms进行发射。一帧被分为6个时隙。在移动单元发送的帧中有6比特的时隙间隔用于停止传送，另有6比特的时间用于使功率恢复至工作电平。这两个6比特的时间间隔分别称为保护时间和返回（ramp）时间。总共有260比特用于发射或接收，用于同步的28比特模式由帧中时隙的位置来决定。

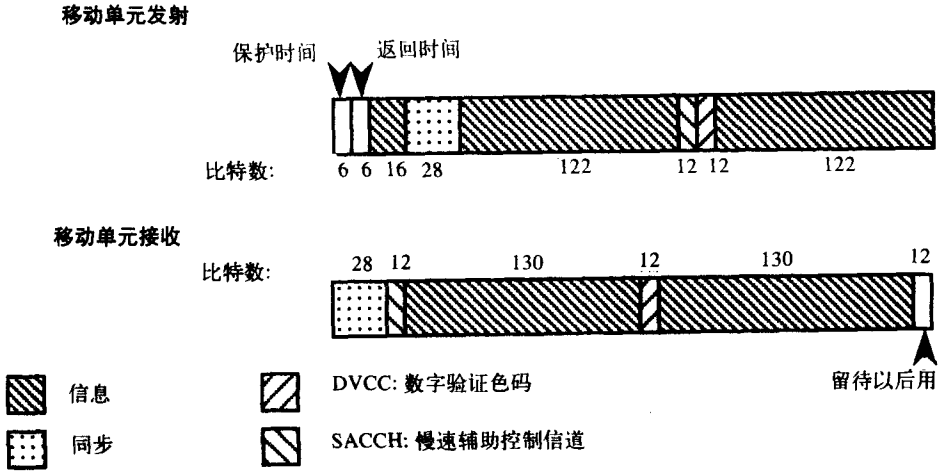


图12-10　IS-54/136的时隙，六个时隙组成一帧

DVCC（Digital Verification Color Code，数字验证色码）防止移动电话与干扰小区基站通信。没有使用AMPS系统中的“blank和burst”信号，而是使用SACCH提供小区基站与移动台之间的消息交换。通过中断用户数字域，也可以使用FACCH(Fast Associated Control CHannel，快辅助控制信道)发送紧急信息。

IS-136是IS-54的升级标准，它与AMPS系统兼容，并且双模电话可以在IS-136系统与AMPS系统间切换。与IS-54标准相比，IS-136提供了更先进的特点，即在空中编程，更长的电池使用寿命，呼叫方ID以及其他智能网络的特征。

12.3.3　欧洲的DECT

DECT（Digital European Cordless Telecommunications，欧洲数字无绳电话）是一个欧洲标准，有别于GSM或IS-54。它使用覆盖于GSM小区之上的微小区。由于DECT是一个低功率系统，因此它不能处理在高速行驶的汽车中的呼叫。然而，它可以通过GSM作为蜂窝电话使用，并且在商业环境中，可以与无线PBX固定端口通信。它也可以用作住宅无绳电话，代替到CO的本地环路，提供无线局域网，与远程站一起工作，以及支持其他应用。远程站是无线公共付费电话。

诸如无绳PBX和无线局域网等一些应用是与环境紧密相关的。也就是说，只有一个生产厂商来提供系统的所有设备。这些系统的标准并没有完全指定，这使制造商可以设计自己想要的系统，只要他们的系统可以与其他DECT系统共存。然而，其他应用需要遵守称为PAP（Public Access Profile，公共接入协议）的规定，该规定保证了一家制造商的基站可以与其他制造商生产的移动设备一起工作。

简而言之，DECT使用10个1.728MHz宽的RF载波。各载波支持一帧，每一帧利用24个时隙支持12个全双工信道。每一帧为10ms时隙，每个时隙包含480比特，其中16比特为帧头，16比特用于同步，64比特用作控制信道，320比特为用户信息，64比特为保护时间。DECT以及GSM和IS-54的其他特点总结在表12-2中。

表12-2 TDMA蜂窝系统总结

	GSM	IS-54/136	DECT
移动电话发射频率（MHz）	890~915	824~849	1880~1900
移动电话接收频率（MHz）	935~960	869~894	1880~1900
系统使用的频谱（MHz）	50	50	20
每载波占用的带宽（MHz）	0.200	0.030	1.728
频道数	125	832	10
每个载波支持的用户数	8	3	12
用户信道总数	1000	2496	120
信道的数据调制速率（kbps）	271	48.6	1152
数字话音速率（kbps）	13	8	32
包括差错控制的话音速率（kbps）	22.8	13	32
话音编码方法	LPC-RPE	VSELP	ADPCM
使用的调制类型	GMSK	DQPSK	GFSK
控制信道的名称	SACCH	SACCH	C
移动输出功率（毫瓦）	3.7~20 000	2.2~6 000	250

注：ADPCM：自适应音频脉冲编码调制
C(Control information channel)：控制信息信道
DECT：欧洲数字无绳电话
DQPSK：差分四相相移键控
GMSK：高斯最小频移键控
GSM：全球移动通信系统
IS-54/136：美国数字蜂窝EIA临时标准
LPC-RPE：带有规则脉冲激励的线性预测编码
SACCH：慢速辅助控制信道
VSELP：矢量和激励线性预测编码

12.4 高通的CDMA(TIA/EIA-95)

12.4.1 扩频通信

自从第二次世界大战以来，扩频通信技术就已经被用在军事领域，用于阻止敌军干扰通信信号。20世纪80年代期间，大多数工程机构认为扩频技术不能与数字蜂窝系统共同工作，因为该技术过于复杂，而且代价昂贵。幸运的是，在一个名为Qualcomm（高通）的公司中，几位可称之为当今“爱因斯坦”的科学家证明事实并非如此，并开发了CDMA。

在扩频通信中，每个人可以拥有一个独一无二的号码来解码自己的信息，这对别的用户几乎不会造成干扰。在军事通信中，一旦敌军检测到某一频段的信息传输，信号干扰就可能发生。但扩展频谱信号是很难被检测到的。信息的传输不是在一段很窄的频带内而是覆盖在很宽的频带内，因此发射功率分布在整个信号带宽内，其结果就是敌方“侦听”到的只有噪声，而且这些信号可以使用加密算法使其更加安全。

基本上有两种类型的扩频信号：直扩和跳频。CDMA使用直扩类型，各发射信号都有自己的扩频码；跳频必须周期性改变载波的频率。在这两种情况下，为了使接收机正确地解码，同步是一个非常重要的要求。本章的其余部分将详细介绍CDMA的TIA/EIA-95标准。

12.4.2 基本CDMA

CDMA采用一种称为64码片（chip）的Walsh码。Walsh码使得小区以61个话音信道运行，

另外三个用于系统本身。这些信道称为彼此正交，也就是说，任何给定信道的通信不会被其他信道检测到。在几何上，x、y、z轴称为是正交的，就是因为每个轴都可以独立变化而不受其他轴的影响。

图12-11所示为CDMA的工作原理，这里用户1的Walsh码为“++－－”，不论何时用户1发送二进制的“1”时，它发送的是“++－－”；而要发送二进制的“0”时，只发“0”即可。类似地，用户2分配的Walsh码是“+－+－”，所以当要发送二进制的“1”时，该用户就发送“+－+－”；而要发送二进制“0”时，只发送0即可。这些符号在本例中由4个码片组成。用户3的Walsh码是“+－－+”。

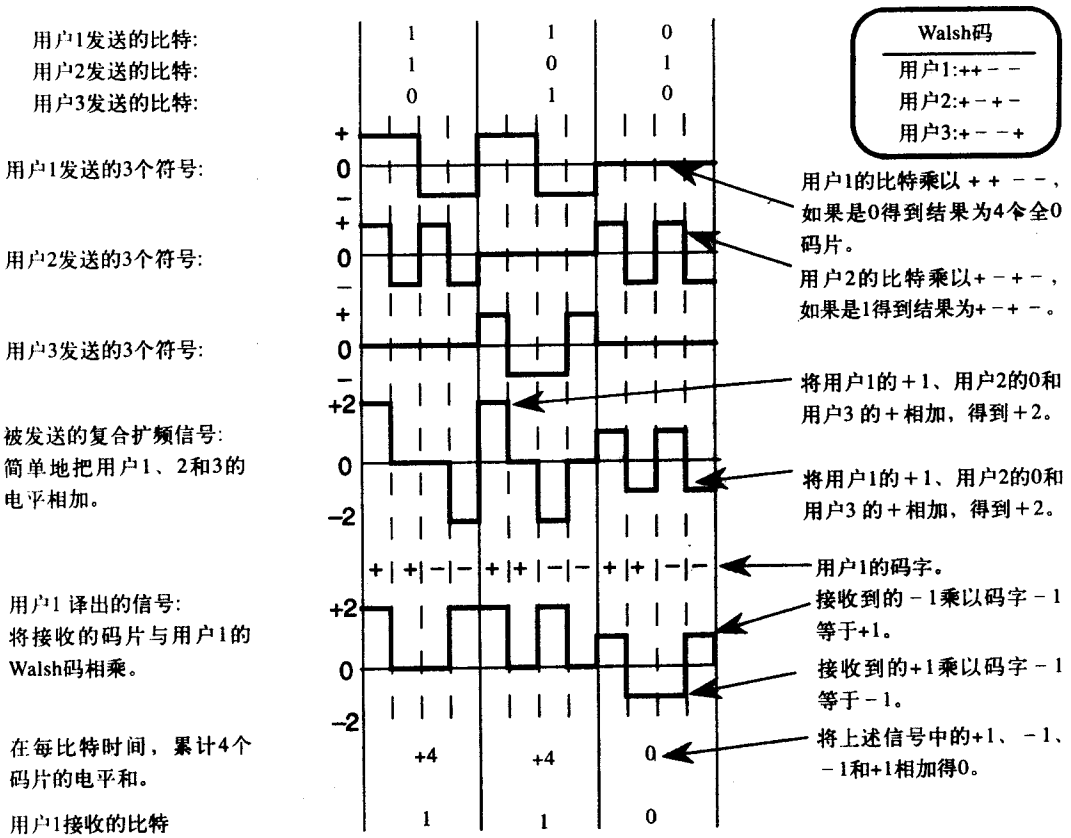


图12-11　三个用户发送的信息在一个载波上传送以及用户1是如何解码出“110”的。各用户的码字如图所示

如图12-11所示，让我们看一下当用户1发送比特序列“110”，用户2发送“101”，用户3发送“010”时会发生什么。利用上述编码方法，可将这些序列中的比特转换成4个码片，所以用户1发送“++－－++－－0000”，用户2发送“+－+－0000+－+－”，用户3发送“0000+－－+0000”。现在将每个用户的对应码片垂直相加，结果得到“200－220－20+1－1+1－1”，例如对于第一个码片而言，用户1是+1，用户2是+1，而用户3是0，相加之后结果为+2，依此类推。

现在，所有的用户接收由0、+1、－1、+2、－2组成的同样的序列，他们怎样译出属于自己的信息呢？我们仅考虑用户1，他将把接收到的码片与自己码字的码片即“++－－”相乘。所以对于第一个码片，+1乘以+2得+2；对于第2个码片，+1乘以0得0，依此类推。因此，前

四个码片为“2002”，之后这些值加起来得4，如图所示，用户1接下来4个码片得到的和为4，再接下来4个码片得到和为0。如果4被解码为二进制1，而0被解码为二进制0，那么用户1将从这个复合信号中接收到原来的信息“110”。用户2和用户3使用相同的解码方法，用户2得到“101”，用户3得到“010”。

这种方法之所以奏效是因为用户的码字是彼此正交的。注意到，如果用户1码字（++－－）的相应码片与用户2码字（+－+－）的相应码片相乘，我们得到“+－－+”。将它们相加之后所得的结果为0。类似地，如果用户1的码字与用户3的码字相乘，则码片积之和的结果也为0。然而，如果用户码字自乘，例如“++－－”乘以“++－－”，则码片积之和为4，因此，称这些码字是正交的。

12.5 差错处理

12.5.1 CRC

为编码话音的每22个比特，加上6比特的CRC（Cyclic Redundancy Check，循环冗余校验）码。如果接收机检测到错误，并不对这22比特进行解码，而是在接收端暂时保持沉默。其主要思想是，与其听到不属于这段时间的声音还不如听不到任何声音。况且人耳也无法检测到接收信号中丢失了22比特。

但数据是不能丢失的，必须进行纠错。用于纠错的一种方法是为每个数据帧发送一个CRC码，如果接收机查出错误，则重传此帧。在无线系统中，频谱资源是非常宝贵的，重传错帧是很费资源的，也要花费时间。一个减少错误的方法就是增大发射机的功率，但这就意味着在给定的时间只能为更少的用户服务。另一种方法是将每比特发送两次，也就是说1发送为11，0发送为00。但如果1被接收为10，接收机就不能分辨是1被发送为10，还是0被发送为10，错误也就没有被纠正，当然我们也可以将每比特发送2次以上，但现在有一个更好的使用卷积码的方法称为FEC（Forward Error Correction，前向纠错）。

12.5.2 卷积码编码器

TIA/EIA-95和所有CDMA都使用FEC的连续编码方法，而不使用分组编码方法，特别地，TIA/EIA-95使用连续码中的卷积码，该方法比其他方法所花费的时间短，易于设计和实现，并且能很好地纠错。现在我们将举例说明卷积码是怎样进行前向纠错的，但这可能需要很长时间。

产生卷积码的电路如图12-12所示，它是基于异或逻辑电路的，其真值表也列在图12-12中。如果该电路的两个输入端同时为0或1，则输出为0，否则输出为1。电路也可以有3个输入，在这种情况下，可以先异或任何两个比特，得到结果再与第三个比特异或，三输入比特时的真值表如侧图所示。

异或逻辑

输入	输出
000	0
001	1
010	1
011	0
100	1
101	0
110	0
111	1

回到图12-12，在卷积码编码器中有两个这样的异或电路：上面一个有两个输入端，下面一个有三个输入端，该编码器还有1比特的延时电路，用于暂时存储已经到达编码器的最后两个比特，左边是输入，异或电路的输出送到一个TDM（时分多路复用器），一次输出一个比特。

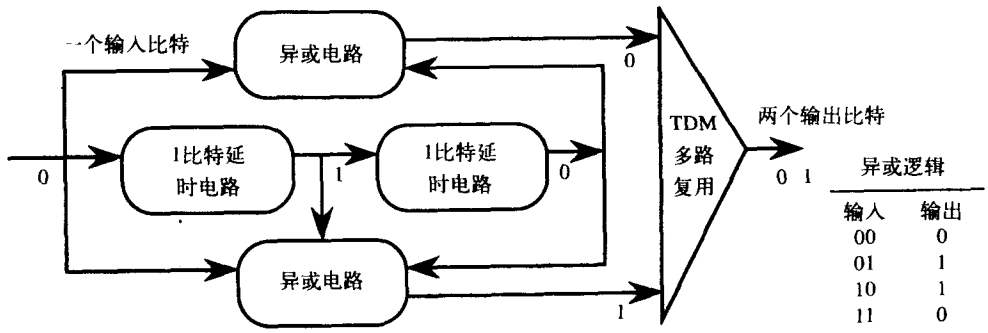


图12-12　是基于异或逻辑的卷积编码器。当前，有一个0在输入端，在前一个时钟输入为1，在前两个时钟输入为0，多路复用器的输入是其输出端出现的0和1

目前电路的输入端为0，其前一个比特为1，即第一个1比特延时电路的输出端所示。其前面第二个比特为0，即第二个1比特延时电路的输出所示，用这几个比特，我们可以得到两个异或电路的输出。上面的异或电路输出为0，因为它的两个输入均为0，下面的异或电路输出为1，因为它的输入为0、1、0。根据两个异或电路的输出，可得多路复用器的输出为01。让我们再看一些例子。

在图12-13a中，我们给该电路连续输入0，在输出端得到了一对0，对于每个输入比特而言，每个时钟周期输出2比特。在图12-13b中，我们给该电路输入比特“1”，它将左边的两个0推向右边，并且最右边的0从电路中消失，此时两个异或电路的输入为奇数个1，所以复用器的输出为11。

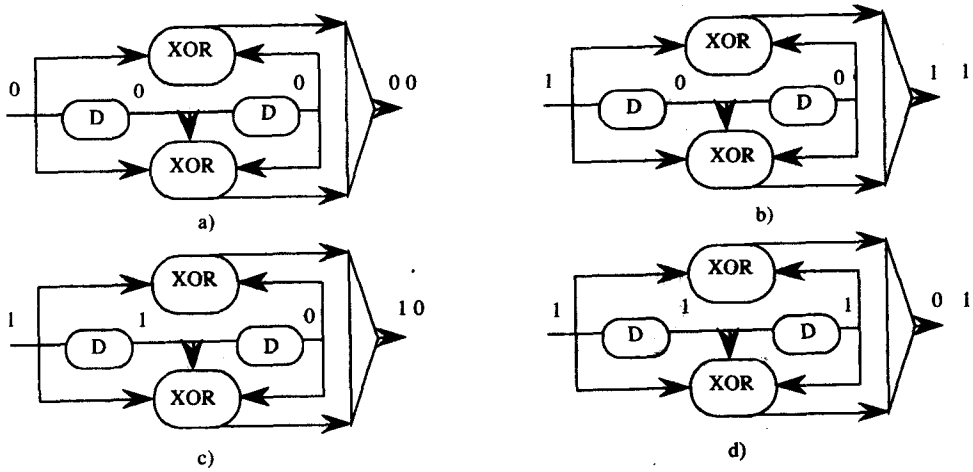


图12-13　a) 最初，所有编码器清零；b) 输入1，输出为11；c) 再输入1，输出为10；d)又输入1，输出为01

在图12-13c中，又输出了一个1，它将左边两比特右移一位，此时下面的异或电路输入为两个1，所以其输出为0，而上面的异或电路输入有一个1，所以其输出为1。图12-13d是输入第三个1时的情况。

在图12-14a表格的“当前输入比特”一栏中给出了与上例相同的比特序列，我们从图12-13中取出相同的输入比特并增加了一些输入比特，即输入为0、0、1、1、1、0、1、0、0。各时钟周期的输出为表中最后一栏的比特对，中间两栏为两个1比特延时电路的输出。

我们可以取任何两栏来定义编码器所处的状态。比如我们可以取前两栏，这样就得到图12-14b所示的四个状态。让我们用图12-14b跟踪在图12-14a输入比特的情况下，编码器的状态转移路径。最初，我们处于状态00。第1个时钟输入为0，使得编码器仍回到状态00，编码输出00没有在图12-14b中显示出来。第二个时钟时，输入为一个1，使得编码器进入状态10，输出为11。对于每一个输入比特，编码器不是保持原状态就是进入另外一个状态。于是，该图中跟踪了编码器在8个时钟周期所经过的路径。

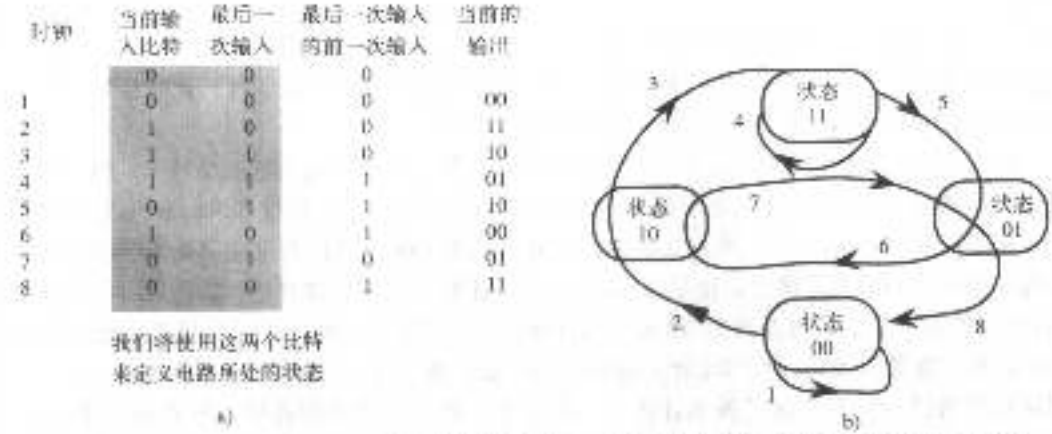


图12-14 a) 由给定输入数据流得到最后一栏的输出结果；b) 在状态图中，跟踪输入比特得到的路径

在研究了该编码器之后，我们给出一个更一般的状态图，如图12-15所示。该图显示了编码器可能处于的四种状态。还显示了状态转移的情况。粗实线箭头给出了输入为0时状态的转移，另一箭头给出了输入为1时状态的转移情况。在每个方框中的比特对为状态转移过程中卷积码编码器的输出。

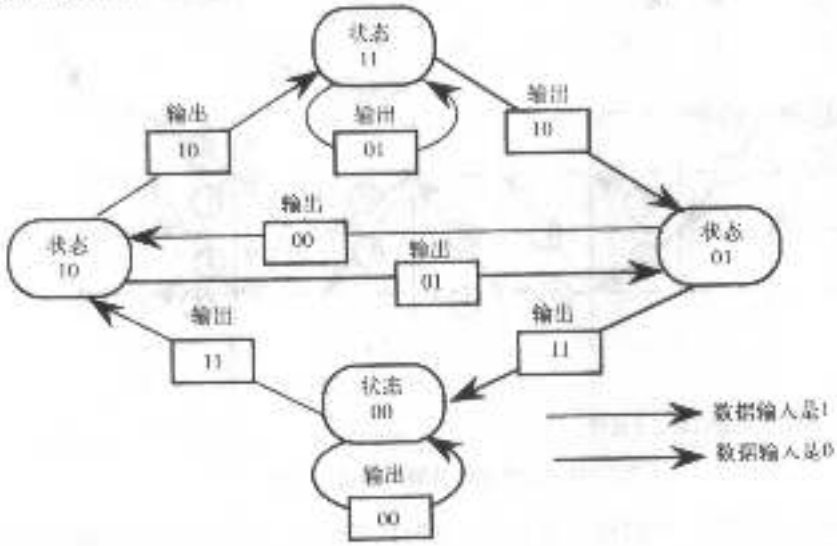


图12-15 卷积码编码器的通用状态图

例如，假定我们处于状态10，在图的最左端，此时，如果输入为1，则转到状态11并输出10。另一方面，如果输入为0（粗实线所示），则转到状态01并输出01。由于状态的值可能与

输出的值相混淆，所以在该图中都进行了标注。值得注意的是从状态10不能转到状态00或者停留在状态10，这一特征将会用于纠错。

12.5.3　维比特译码器

现在让我们研究一下维比特译码器（又称为解码器），它是以一位高通（Qualcomm）的工程师的名字命名的。让我们将图12-14a中输出栏内的输出结果，排成图12-16上部的一行。输出比特分别是00、11、10、01、10、00、01、11。假设右边数第二对的第二个比特不正确接收，希望维比特译码器能够予以纠正。可以证明大多数的错误可以被纠正。然而，接连出现的错不易纠正，这一点将在本例中验证。因为最右边即最后一对（11）正确接收，所以译码器能够把00译成01。在讨论过程中，需参考图12-15。

在进行输入信号流的解码之前，我们要估计度量值。两个可能的状态转移中的每个都有度量值，考虑到解码器当前的状态和输入的比特对。累积的路径长度值使得解码器可以纠正错误。

从图12-15可以看出，如果处于状态00，并且输出为00，则最有可能仍处于00状态。对于最有可能发生的状态转移指定度量值为0，表示两比特可以无差错到达。即图12-16中从时间1到时间2的水平箭头。现在图12-15的输出值即图12-16的输入值，对于1比特无错到达的状态转移，指定度量值为1；对于2比特无错到达的状态转移，指定度量值为4。这些数（0、1、4）用向量代数进行计算，这里就不详述了。实际上，通常用精确的模拟电压值来计算长度值，这样做要比逻辑值具有更好的纠错能力。

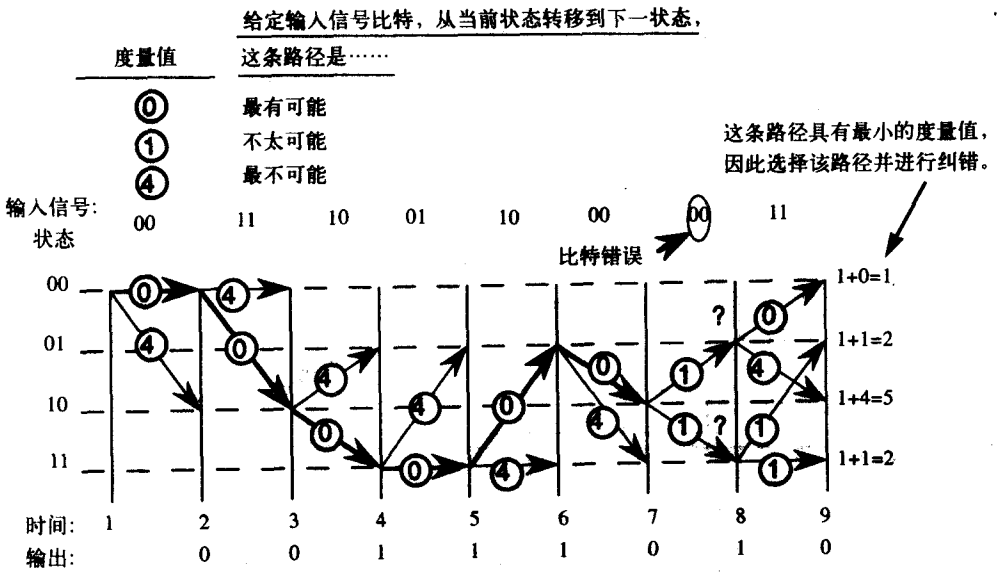


图12-16　使用维比特解码器进行纠错

开始，解码器被清零。此时处于状态00，如时间1所示。如图12-16所示输入也为00。如果处于状态00并且输入也为00，那么因为没有比特改变，处于该状态的度量值为0。然而，根据图12-15可知，也可以从状态00转移到状态10，在那种情况下，输入应为11。但是，由于接收到的输入为00，亦即这两比特都必须改变，所以分配给这个转移的度量值为4。在这两个度

量值中，我们选择最小的一个，仍处于状态00，如粗箭头所示。这个时钟周期的输出将为0，会在另一个时钟周期之后得到。输出是新状态的第二比特。新状态为00，其第二比特为0。因此，0即为输出，如时间2所示。

我们再举几个例子。考虑时间3时的解码器，当前状态为10，根据状态图可知，可以从该状态转移到状态01或状态11。输入为10，即转移到状态11所需的输入。因此那条路径的度量值为0，也就是最有可能出现的情况。根据状态图可知，要转移到状态01。输入必须为01。然而，输入为10，也就是说，如果实际发送的是01，那么由于我们接收到的值为10，所以这两比特都必须翻转。因此，转移到状态01的度量值为4，是最不可能的值。我们选取0值的路径，使我们处于状态11，则输出为该状态的第二比特，即输出为1。

注意到，时间线下面的输出与图12-14中第一栏的输入值相同。然而，在时间7我们遇到了解码困难。此时的状态为10，输入为00。无法知道哪个比特因差错而发生了翻转。因此，我们计算两条可能的转移的度量值。如果我们要从状态10转移到状态01，第二比特发生了翻转，所以我们分配该转移的度量值为1。另一方面，如果从状态10转到状态11，第一比特发生了翻转，所以我们分配该转移的度量值也为1，这使我们不得不看下个时钟周期发生的情况。

在时间8，需计算4个度量值，其中两个从状态01出发，另外两个从状态11出发，这4个值在图中分别为0、4、1和1。之后我们累加各支路之和，得到1、2、5和2，我们选最小的值1。现在，我们就处于一个更好的位置，知道T＝8时发生什么。在时间8输出1，在时间9输出0。这与发送相同并且接收错误被纠正了。

卷积码编码器的R因子为1/2。这意味着产生的符号是输入比特数的二倍，也称为半速率编码器。1/3速率编码器会提供更佳的纠错性能，也可用于CDMA系统中。延时电路的数目加1由K因子给定。在这个编码器中K=3。CDMA系统中采用K=9的编码器，这进一步改进了纠错能力。

12.5.4 块交织

如前所述，使用模拟电压能得到更好的纠错性能。同时，如果T＝8时间的输入比特对出错，那么将不太可能纠正过来。在一个通常的无线网络中，当一辆小汽车绕一座高大建筑物行驶时，信号功率会发生时高时低的突变，很可能出现相距很近的比特出错的情况。为了使错误发生的位置分散开从而不会连续接收到错码，需采用一种称为块交织的技术，该技术还会减少不可纠正错误的数量。

例如在图12-17中，发射机发送12个比特。如果比特连续发送，由于信号衰落引起的错误出现在第5、6、7比特，这样的错误是不易纠正的，因为这些差错是彼此相邻连续出现的。如图12-17右边所示将这12个比特进行交织，将会打乱比特顺序。现在，如果连续出错，当接收机将比特排列为合适的顺序之后，错误就彼此分离了，这样就可能更好地纠错。

这种方法的缺点是发送之前由于要进行块交织，因此会增加时延；同时，在接收端解交织时也会引入时延。在TIA/EIA-95的下行链路中，块交织矩阵为16列24行的矩阵，共有384个符号，这样会引入20ms的时延；在上行链路中使用18 × 32的交织块，总共576个数据符号。

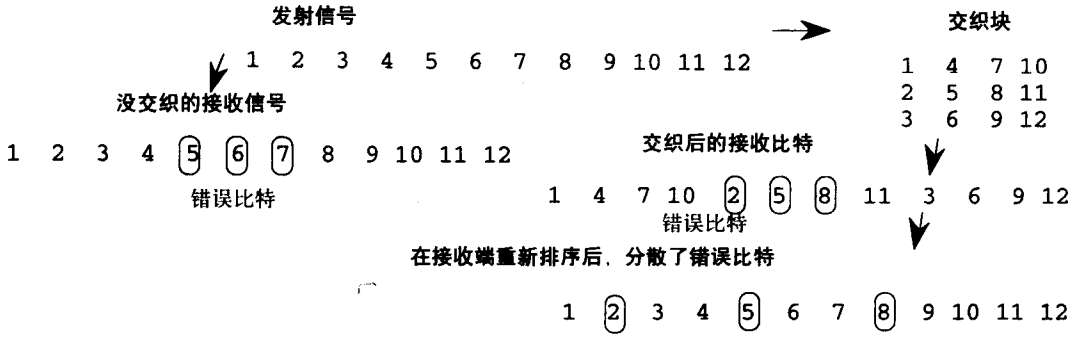


图12-17 块交织分散了错误，使维比特解码器更易于纠正错误

12.6 CDMA与SSMA

12.6.1 一些术语

事实上，CDMA（Code Division Multiple Access，码分多址接入）的实现也用到SSMA（Spread Spectrum Multiple Access，扩频多址接入）。CDMA本身使用Walsh码，SSMA使用PN（伪随机噪声）码。各种类型的码都有其各自的功能，在同一标准中采用两种类型的码与仅采用一种类型的码相比，允许访问更多的MS（Mobile Station，移动台）和更多的BS（Base Station，基站）。与仅采用一种编码方法相比，采用两种编码方法可以使我们识别更多的发射源和更多的接收台。术语**码流层**（code layering）用来表示**数据流**可以先用一种码进行编码，之后再用另一种码进行编码。在本节的其余部分，我们用SSMA来表示使用PN码进行的调制，用CDMA表示使用Walsh码进行的信号调制。

在我们仔细研究CDMA（或Walsh码）和SSMA（或PN码）之前，先讨论几个术语。一个术语是**扩展**（spreading），有两种类型的扩展，一种称为正交扩展，它使用Walsh码，另一种称为频谱扩展，它使用PN码。在12.4.2节中，每个比特被转化为4个码片，码片数量和比特数量之比被称为正交扩展因子，这里扩展因子是4。

当一个信道在很宽的频率范围发射而不是在很窄的范围发射时，会发生频谱扩展。在CDMA中所采用的频谱扩展的全称为DSSS（Direct Sequence Spread Spectrum，直接序列扩展频谱）。

相关（correlation）是另一个重要术语，它指的是一种系统关联，在这里是指如何更好地从接收信号中进行译码。在12.4.2节，我们了解到Walsh码能够很好地分离传输信道。被分配有特定Walsh码的CDMA接收机能够从接收信号中挑选出应属于自己的信号，这就称为自相关。接收机也能够拒绝不属于自己的信号，这称为互相关。

在12.2.2节提到的类比中，如果你说阿拉伯语，那么你与说阿拉伯语的乘客具有很好的自相关，而与说中国普通话的乘客则具有很差的互相关。为了提供良好的信道分离，上述自相关和互相关是我们需要的，理想情况下自相关为100%，互相关为0%。

12.6.2 Walsh码

Walsh码也称为正交码，因为在一个信道上传输的数据对其他信道上传输的数据流不会造成干扰。立体几何中所使用的坐标x、y和z称为是正交的，因为其中一个量的改变，比如说x的改变，并不会影响其他两个坐标。在我们的类比中，中国普通话与其他语言是正交的。

与PN码相比，Walsh码提供了非常好的信道分离，其自相关的百分比远高于互相关的百分比。然而，Walsh码需要在所有发射信道之间非常精确地同步。因此，Walsh码被BS（Base Station，基站）所采用，其原因是基站更容易控制发射信道的同步。另一方面，Walsh码没有被MS（Mobile Station，移动台）的发射机所使用，要保持多个MS的发射信号之间的同步几乎是不可能的。

TIA/EIA-95采用长度为64的Walsh码，正交扩展因子为64。图12-18给出了这些码是怎样产生的。在图的顶部从1开始，如果要得到这些码中的两个，就要向下进入到树的第二层，如果要得到四个码，就要进入到第三层，依此类推。每向下一层就会得到两个新码，其长度为父节点码的两倍。每一对新码的前半部分与父节点码具有相同的比特模式。第一个新码的后半部分也重复同样的模式；第二个新码的后半部分虽然重复着同样的模式，但比特是逆序的。

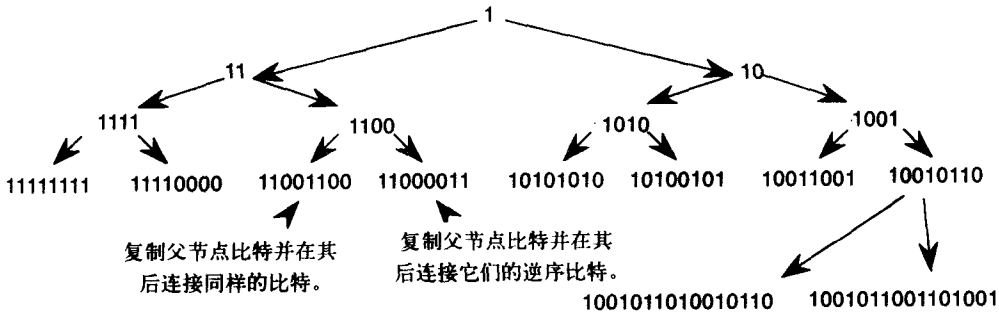


图12-18 产生Walsh码

例如Walsh码的第二层是11和10，要得到第三层码1111、1100、1010和1001，需由11产生两个码字，由10产生两个码字，请看10为父节点码、1010和1001为子节点码的分支，这里我们取10作为这两个子节点码的左半部分，再给一个子节点码加上10，给另一个子节点码加上其逆序01。

注意到，码的长度也就是在那一层可用码的数量。TIA/EIA-95使用64比特长的码，所以有64个这样的码。这意味着同时可以发送64个不同的信号，每个信号用一个不同的码。但是，由于工程和设计的问题，实际上通常可行的只有20个信道，而系统只用其中7个信道。如果增加码的长度，CDMA就可以支持更多的信道，然而，每个信道的数据率也会下降。

OVSF（Orthogonal Variable Spreading Factor，正交可变扩展因子）码是另一种与Walsh码相关的编码方法，因为这种码允许信道以不同的传输速率发送。回到图12-18，我们从第三层为两个信道分配码字，即1111和1100，并从第四层为四个信道分配码字，即10101010、10100101、10011001和10010110。我们现在已经做到的，正如其名字所暗示的，就是给信道变化扩展因子，现在这两个信道能够以两倍于分配有第四层码字的信道速率来工作，这使无线系统有更大的灵活性。那些需要立即增加带宽的，可以在需要时为其分配更短的码字，当需要降低带宽时，再增加其码字长度。

12.6.3 PN码

在发射信号上，重叠或增加PN（Pseudorandom Noise，伪随机噪声）码，所得到的接入方法称为SSMA（Spread Spectrum Multiple Access，扩谱多址接入）接入方法。正如Walsh码扩展信号速率为原比特率的64倍一样，PN码也增加了另一个扩展层。与Walsh码不同的是，每个PN码中1和0的个数相同，PN码之所以这样命名是因为尽管对于其他用户而言，传输信息就像随机噪声，但被接收机译为纯净信道。PN码为长码，允许SSMA分配超过40 000亿个码来提供个人服务。

图12-19给出了两个MS（Mobile Station，移动台）在两个不同的信道利用两个不同的PN码发射信号的示意图。在CDMA将每秒的比特数增加到每秒更多的码片速率的同时，SSMA将该信号从窄带扩展成宽带，因此，有术语“扩展频谱”（扩频），实际上就是“展宽频谱”。

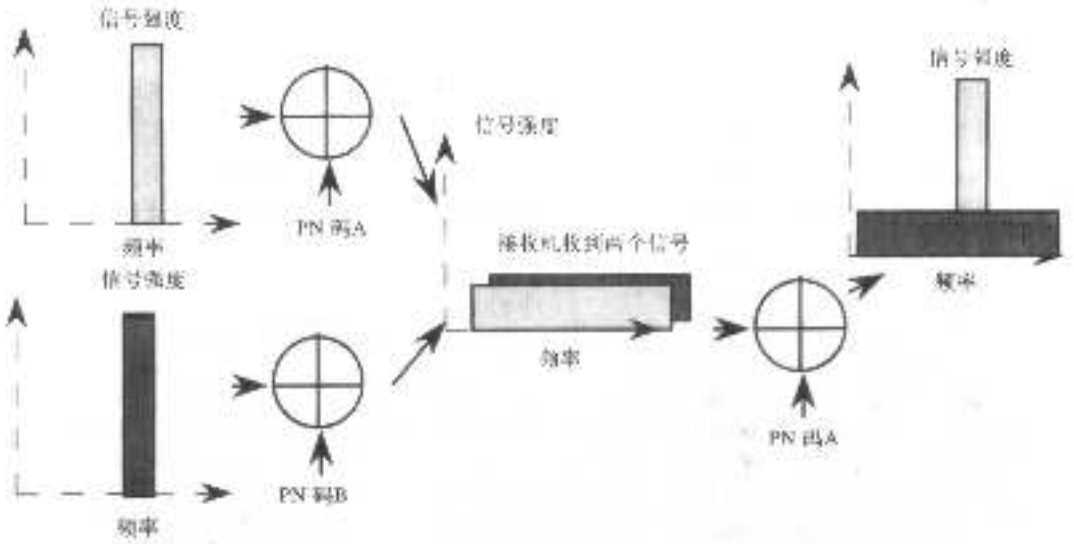


图12-19 两个移动台的两个信道用两个PN码扩频。复合载波表示两个信号在空中被合并传播，接收机用自己的PN码A与复合信号做相关运算，之后，发送给接收机A的信号被恢复，而发送给接收机B的信号则表现为低干扰

每个信道所占用的频谱很宽并在接收机处合并，为了从A中译码出信号，接收机将使用PN码A，之后，来自A的原始信号就被恢复而来自B的信号则表现为低干扰。由于许多信道共同占用同一频谱，因此干扰的电平将开始增加，这使得接收机难于从各信道分离出信号。

既然所有的信道占用相同的带宽，对于TIA/EIA-95而言是1.23MHz，这就使工程师在这一带宽内设计无线系统变得容易了。而在其他系统中，频率的规划变得很麻烦并且同信道干扰也非常严重；在SSMA系统中，相邻小区可以使用相同的频率范围。PN码提供了发射机之间的分离。频率复用因子可以是1而不是图12-3所示的7或12。因此，这种设计是由编码规划来完成的，而不是频率规划来完成。

有两种类型的PN码。短的PN码规定为15比特屏蔽，共有32 768个或2^{15}个码片，长PN码用42比特屏蔽。这两种长度是TIA/EIA-95标准中的长度，而在第三代标准中使用更长的码。这两种类型的PN码的目的是不同的。短的PN码用于标识BS信号，而长的PN码用于标识MS信号。

12.6.4 PN和Walsh码层

PN码可以提供**很好的**（good）信道分离，它取决于码片速率与数据流比特速率之比。而Walsh码可以提供**极佳的**（excellent）信道分离，而且Walsh码需要发射信道精确地同步，而PN码则不需要。

因此，Walsh码被用于下行链路，这样MS就能够将来自一个基站的数据信道区分开。BS能够保持其所有发射信道之间的严格同步，所以它使用Walsh码来标识发射信道。

短PN码用于标识BS，而长PN码用于标识MS。长PN码基于MS的ESN（Electronic Serial

Number，电子序列号）。所有上行链路传输都是仅采用PN码来完成的。

短PN码：为了更清楚地说明短PN码，参见图12-20。图中有两个BS（Base Station，基站）分别称为A和B，有两个MS（Mobile Station，移动台）分别称为C和D，基站用短的PN码发送。结果是虽然所有BS都使用相同的短PN码，但仅靠其相位不同就可以彼此进行区分，这使得MS更容易在不同的相移中仅寻找一个短PN码。BS也可以使用短PN码进行发射，这使得BS易于发现传给自己的信号。

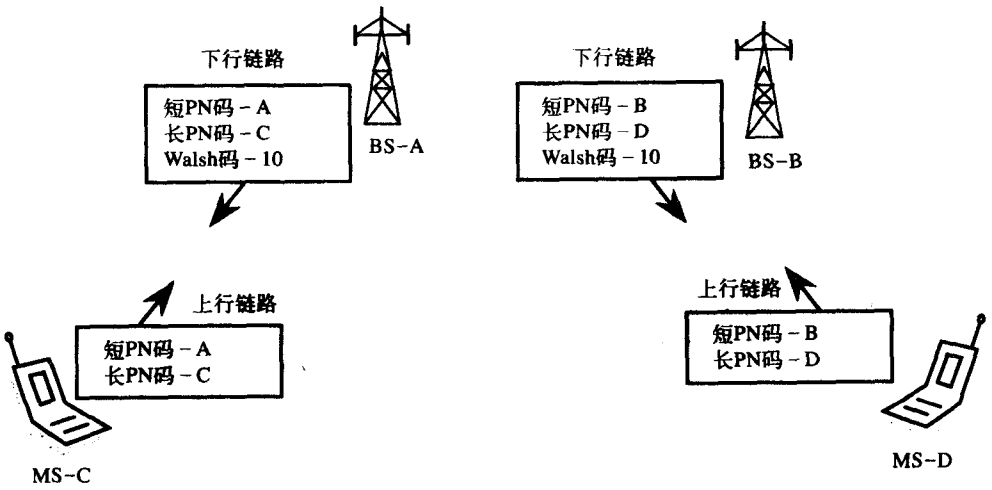


图12-20 Walsh码标识前向信道，短PN码的相位标识BS，长PN码标识MS

长PN码：BS也会通过将长PN码扩展到其发射信道上进行发送。可使用两种类型的长码中的一种。其中一种称为公共码，它由知道MS的ESN来决定；另一种称为私有码，它用于安全，由鉴权和加密过程决定。MS也在上行链路使用这些长PN码。要花费42天的时间才能使长PN码发生重复，这样入侵者就不可能检测到这种码。在下行链路信号中，长PN码用于加密；而在上行链路中，它用于信道分离和识别。

Walsh码：所采用的第三种类型的码就是我们已经见过的Walsh码。因为基站可以很容易地保持Walsh码的准确同步，所有它们仅被BS所采用。每个Walsh码识别一个被占用的信道。在图中，两个BS使用同一个Walsh码10发射信号。

12.7 CDMA业务信道

下面通过业务信道来研究基本的CDMA系统。有两种类型的下行链路信道和两种类型的上行链路信道。下行链路信道类型为业务信道和广播信道。上行链路信道分为业务信道和接入信道。下行链路信道用Walsh码进行分离，广播信道就是导频、同步和寻呼信道。导频信道提供初始同步，同步信道提供BS识别，寻呼信道将进入的呼叫连接到正确的MS。接入信道允许MS发出呼叫。让我们仔细研究一下业务信道从而了解信号是怎样进行处理的。

图12-21给出了下行链路业务信道的电路方框图。声码器的输入为64kbps的PCM信号。该声码器称为QCELP（Qualcomm Code Excited Linear Prediction，高通码激励线性预测编码器）。这样的声码器有两种类型，通过它们的速率集编号来识别。速率集1的声码器可以将话音速率压缩至1.2kbps、2.4kbps、4.8kbps和9.6kbps，速率集2的声码器可以提供速率为1.8kbps、3.6kbps、7.2kbps和14.4kbps的更高质量的信号。所有系统必须能够处理速率集1的编码。当话音活动减少时，使用更低速率的编码。



图12-21　前向下行链路业务信道的功能框图，阴影模块在上行链路信道中不存在

之后该信号被送入CRC编码器，CRC允许接收机检测错误帧，并确定话音信号的速率，接着将信号送入半速率卷积编码器，将比特数加倍。

下面就是符号重复器，这个单元将低速率信号的速率增加到合适的速率。出这个单元之后，所有速率集1的信号被调至19.2ksps（千符号每秒），而速率集2的信号调整到28.8ksps。如果需要增加速率，那么将重复符号。然而所有被重复的符号的合成功率与没有被重复时的相同。

接下来是冲孔（puncturing），只有速率集2的声码器需要使用这个功能，为了使用相同的块交织器，要从每6比特中去掉2比特，这样就将符号速率从28.8ksps降至19.2ksps。接收机的前向纠错将纠正任何错误。

经过冲孔后进入我们前面讨论过的块交织器，接着由长PN码，Walsh码和短PN码进行信号的扩展。这里还有一个功率控制发生器，它每秒钟发送800次预先置入数据比特流中的单个功率控制比特，再由接收机来纠正错误。根据这个比特的值，接收机将增加或减小它的发射功率1dB，BS会连续要求MS的输出功率增加或减少1dB。在我们前面提到的类比中，讲中国普通话的人使用扬声器使得懂阿拉伯语的人很难听到那些讲阿拉伯语的人的谈话。我们需要使到达BS的MS的发送功率相同。基本上这就是下行链路业务信道的设计方法。

图12-22给出了上行链路业务信道的基本工作原理，许多部分与下行链路业务信道是相同的。半速率的卷积编码器用于速率集2的声码器，而1/3速率的卷积编码器用于速率集1的声码器。速率集2的声码器提供更好的话音质量，因此不会受到低质量的半速率卷积编码器的阻碍。

6比特	64比特
000000	第一 Walsh码
000001	第二 Walsh码
000010	第三 Walsh码
000011	第四 Walsh码
⋮	⋮
111111	第64 Walsh码

正如我们已经在CDMA中看到的那样，Walsh编码器并不提供任何频率的扩展，它也不提供任何信道分离或识别。每6个比特用一个相应的64比特的Walsh码来代替，完成码之

间的一一对应。这里所有64个Walsh码出现在比特流中，如上页侧图所示，这样处理的目的是增加更强的前向纠错的能力。64比特有2^{64}种可能的组合。由于空中接口中会出现错误，因此这些组合都可能发生。然而，这64码中只有64个是有效的。它提供了前向纠错的另一级。

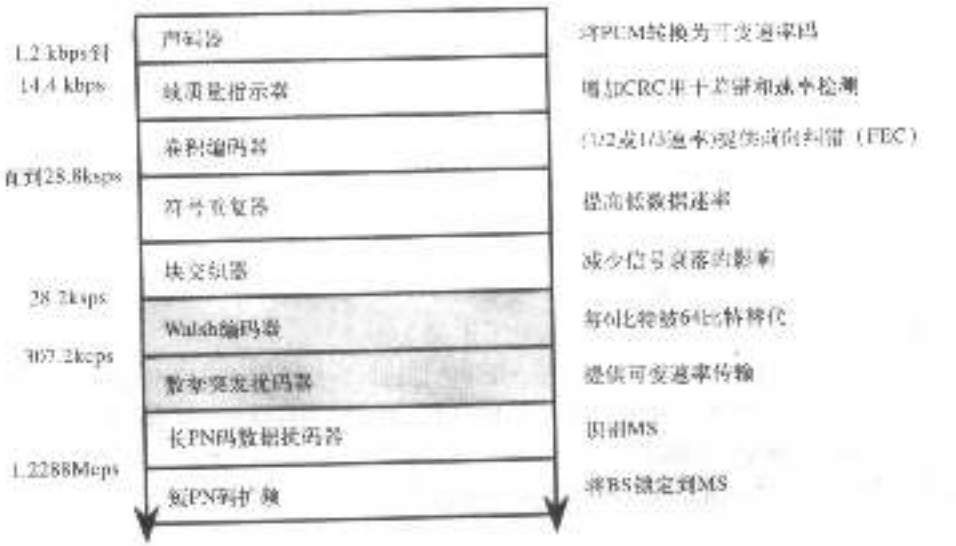


图12-22 反向上行链路业务信道的功能框图。阴影模块在下行链路信道中不存在

数据突发扰码器补偿了变速率传输。当话音活动很低，几乎不需要发送比特时，发射机会暂时关闭，保存能量。扰码器在一段时间内的不同间隔发送话音帧而不是在相同的时间段发送。最后，用长PN码和短PN码进行扩展，这已讨论过了。

12.8 CDMA的总结

CDMA不仅提高了容量，而且由于k为1，所以大大简化了网络的规划和小区的布局。在越区切换的过程中，从移动单元正在离开的小区到正在进入的小区，两个小区的基站均与该单元保持联系，所以在两个基站间并没有突然的切换。这类似于AMPS中的情况。这种切换称为小区之间的软切换，并且它工作良好，特别是在传输数据时更是如此。硬切换只发生在一个单元改变它的工作频率时，即从一个1.25 MHz的频段切换到另一个1.25 MHz的频段。

AMPS和TDMA都易受到由多径衰落所造成的干扰。当传输信号遇到高山或建筑物发生反射时会干扰主接收信号。CDMA将多径信号转变成了一个优势。通过使用RAKE接收机，它将经过不同路径传输的多达三路的不同信号合成一个强相干信号，使得在难于接收的地方具有很好的接收效果。

CDMA必须克服的障碍之一是远近问题。当基站接收到的来自距离其较近的移动单元的有效功率大于距离其较远的移动单元的有效功率时，就会发生远近问题。可以使用多种方法进行功率控制。开环功率控制根据接收功率电平来调整发射功率。基站控制来自移动台的功率总量，使得来自附近移动单元的功率不会淹没来自远处移动单元的功率。这称为闭环功率控制。外环功率控制保持一个来自每个移动单元的特定的错误速率。整体效果是移动单元需要最小的工作功率。

当一个区域出现流量拥塞时，许多人使用他们的移动电话，这使得系统过载。CDMA提

供了一种负载平衡的复杂方法，即把增加的流量分配到邻近的小区，从而使该地区的容量暂时增加。

习题

12.1节

1. 如果蜂窝系统中每个信道的带宽为0.025MHz 而不是0.03MHz，那么在各覆盖区域内有多少可用信道?

   a. 500　　b. 832　　c. 1000　　d. 1200

2. 下面哪个系统不是用于数字无线通信的?

   a. IMTS　　b. LMR　　c. TDMA　　d. EAMPS

3. 当k=12时，每个小区可同时发生多少呼叫?

   a. 12　　b. 18　　c. 26　　d. 32

4. 当一个蜂窝无线台在空闲时锁定到信令最强的信道时，这个状态称为什么?
5. 当移动台从一个小区离开并进入另一个小区时，小区基站应执行什么操作?
6. 画出一个k=4的频率复用模式。
7. 描述一个有线电话如何完成一次对移动电话的呼叫。

12.2节

8. 下面哪一个是MTSO的新名称?

   a. BTS　　b. MS　　c. MHC　　d. HLR

9. 上面哪一个是无线系统中所使用的数据库系统?
10. 如果我们有两对操两种不同语言的人在不同的地方通信，各对可以同时通话吗？如果可以的话，他们使用哪种接入方式呢?
11. 如果我们有两对操同种语言的人，那么这两对可以同时通话吗？他们需要采用哪种接入方式?
12. 在AMPS蜂窝频段内，使用的是哪种无线标准呢?
13. MMDS优于LMDS之处是什么?
14. 蜂窝系统相对于PCS系统的特点有哪些?

12.3节

15. 列举几种使用TDMA的第二代无线标准。
16. GSM和IS-136的不同之处有哪些?
17. GSM和IS-136的相似之处有哪些?
18. 为什么DECT用在GSM存在的地方?

12.4节

19. 列举两种类型的扩频接入方法?
20. 假定在图12-11中，你正在接收第四条信号路径所示的复合信号。如果你是用户4并且Walsh码为++++，那么你提取的信号是什么?
21. 如果你是用户3并且Walsh码如图12-11所示，提取表示相同中间轨迹的信号。
22. 还是在图12-11中，如果用户1的输入为+ − +，用户2的输入为++ − ，用户3的输入为 − + − ，画出同样的信号图。

23. 在某地区使用的Walsh码被认为彼此有一定的关系，这种关系是什么？

12.5节

24. 在图12-13的时间5，卷积编码器从哪个状态转移到哪个状态？
25. 对于上面的问题，像图12-13那样画一个电路，标出各位置的所有比特。
26. 重新创建图12-14，然而这次使用输入比特为0、0、1、0、1、1、1、0、0。画出状态图的表格和路径。
27. 现在为你从上题答案中得到的输出画格型图或图12-16等价的图，并给出你的输出。
28. 对于图12-16，如果输入为00、10、11和01，写出输出结果，错误被纠正了吗？
29. 重做27题，这一次在第10比特增加一个错误比特，通过计算说明错误是否被纠正。

12.6节

30. 在发射信号上叠加两种编码方法称为什么？
31. 输出的码片数与输入比特数之比称为什么？
32. 当接收机拒绝不属于它的信号时，称为什么？
33. 描述SSMA与CDMA的不同之处。
34. 在SSMA和CDMA中使用的不同种类的码是什么?使用这些码的目的是什么？

12.7节和12.8节

35. 不同类型的下行链路信道是什么？它们被用于什么场合？
36. 不同类型的上行链路信道是什么？它们被用于什么场合？
37. 半速率的卷积编码器和1/3速率的卷积编码器有什么区别？哪一种更好？为什么？
38. 在CDMA的声码器中使用几种速率集？需要使用哪种类型？
39. 在CDMA中使用的是哪种类型的切换？为什么它比传统的越区切换优越？
40. 在CDMA中使用的是哪两种类型的功率控制？

第13章 专用交换网络

13.1 背景介绍

本章将主要讨论PBX的概念，也可以认为是有关基于话音的LAN（本地局域网）的章节。提到PBX，就会想到现代的一些复杂设备。然而，其实在20世纪早期PBX就已经存在了。这些PBX称为手工操作的PBX，它们由交换板组成，接线员利用电线和插孔来完成连接操作。后来到了20世纪20年代，利用步进交换设备的自动PBX诞生了。到了20世纪50年代，PBX变成四通交换机。

今天PBX和相配套的设备能够执行许多功能，将在第14章予以介绍。这些设备/交换机既能支持话音通信又能支持数据通信。

美国的PBX曾经被电话公司所拥有，并出租给其商业用户。1968年，FCC在Carterfone决议中规定只要使用能提供载波保护的耦合设备，那么提供给用户的设备就可以直接连到公共电话网络上，这就是互连产业的诞生；它刺激了许多来自日本和欧洲的制造商销售基于话音的各种产品。商业竞争中所有令人兴奋的事件都促进了新产品的进一步发展。

13.2 Centrex

13.2.1 什么是Centrex

Centrex 这个词出现在1965年，是单词“central”和“exchange”的缩写。Centrex是在中心局租用一个“PBX”，而不是在用户所在地拥有一个PBX。由于所有话音交换是在CO完成的，因此，所有的电话必须有它们自己连到CO的一对线路。当要考虑做出Centrex决定的可行性时，租用连接到CO的线路对将是一项最昂贵的开支。

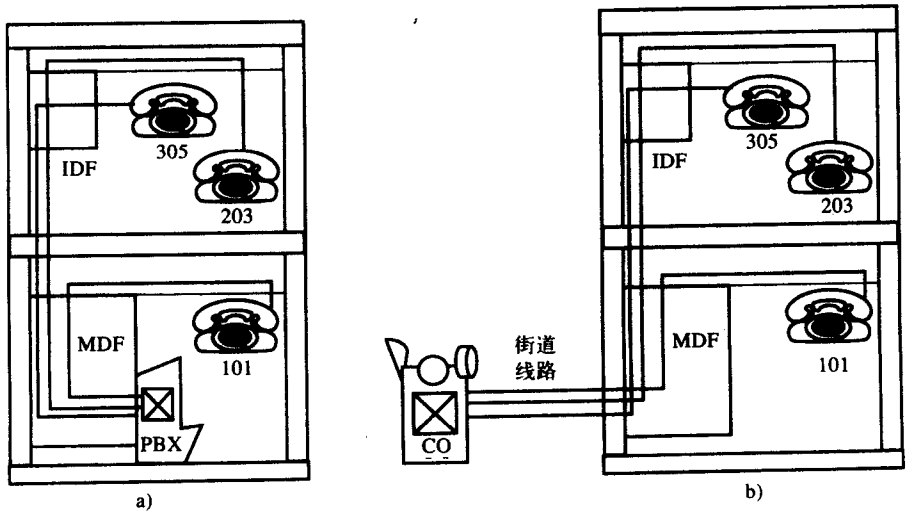


图13-1 a) PBX 进行楼内交换，b) Centrex服务通过CO处的租用线路进行楼内的交换

图13-1给出了一个PBX和Centrex的简化框图，注意在PBX系统中，因为交换能在本地完成，所以仅仅使用内部配线，电话101就能对电话203进行呼叫。然而，在Centrex系统中，在进行同样的呼叫时，它们的连接要在CO处的Centrex交换机上进行。这里利用通向CO的两对“街道”线路来完成一幢楼内的两个电话的连接。

Nortel的S/DMS超级节点DMS-100和朗讯的5ESS是普通Centrex交换机的例子。

13.2.2 Centrex的优点

尽管Centrex需要从用户所在地到CO的许多线路，这使得Centrex要比拥有自己的一个PBX更加昂贵；但是对电信管理者来说，Centrex较PBX具有更大的吸引力的原因有很多。

Centrex服务等级是不断地被调整的，并且根据电话局提供服务的不同，在很多地区的Centrex低租费使得它比使用PBX系统更具有吸引力。如果用户所在地位于当地的CO附近，Centrex线路由于距离所耗费的费用会很低。

考虑到一个公司资金的流动，Centrex是一个具有吸引力的选择。为了获得在税费方面的优势而购买PBX的原因也在逐年变化，而且这还需要调查。如果公司不确定它的大小增加还是减小或者说不确定如何增加和减小，在话音交换系统的容量方面就无法进行估算。实际上，一些PBX系统在容量上具有局限性，但是Centrex则没有这样的限制。

利用PBX建立一个城市网络需要经过CO的从许多地区到达所有待建PBX的线路和中继，因为所需的线路无论如何也要通过中心局。自然，交换工作要在那里进行；而不是把这些线路带到另一个地方进行交换，之后再通过中心局路由到它们的目的地，如图13-2所示。

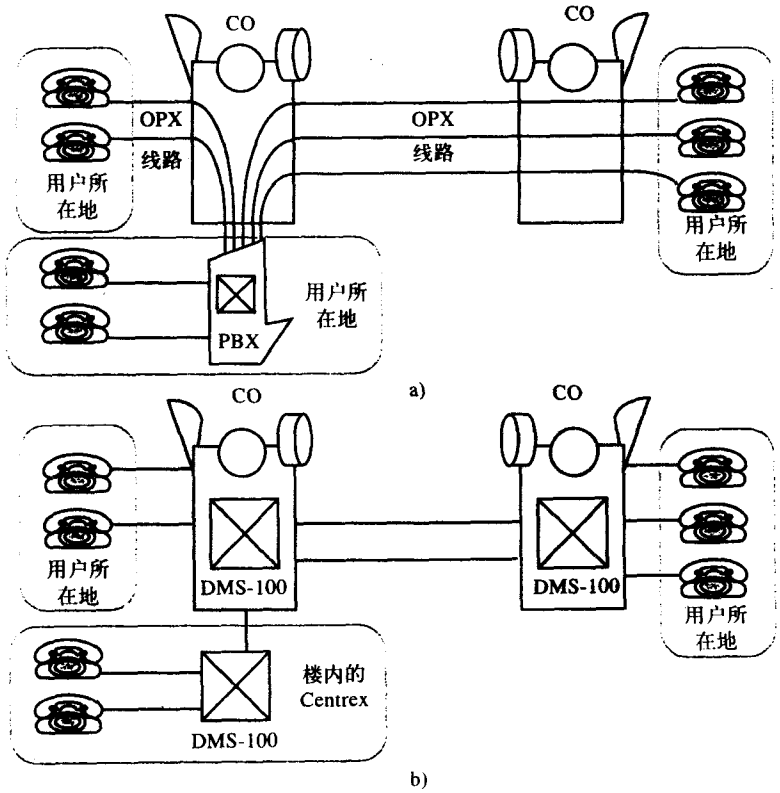


图13-2 a) 市区中联网分散的位置需要租用许多线路，b) 用Centrex联网是市区网络的更好解决方案

Centrex可以通过在远处增加远端模块使网络扩展到一个城市的外部区域。这些就是安装在楼内的Centrex系统，如图13-2b所示，这样就会省去许多街道配线。

对于一个单位或组织而言，Centrex也允许使用一种统一的拨号方案，也就是说当用户从城市里的一个地方到达城市外的另一个地方，如果这两个地点均为一个Centrex系统的组成部分，那么用户还可以继续使用原来的电话号码。而且，在这种情况下，仅需要一个接线员就足够处理呼叫了，每个地点无需其自己的接线员。

而且，Centrex系统的用户端也不需要什么维护。交换机的所有维修程序都是由电话局完成的。SMDR(Station Message Detail Recording，站点消息详细记录)给出了谁呼叫谁、通话多长时间以及所花费用的记录，每个月会由CO以磁带的形式邮寄给用户。现在，Centrex用户可以使用调制解调器随时从终端获取这些报告。

同样地，当用户想从一个地方搬到另一个地方，还想使用原来的电话号码时，这种电话的“搬移”就需要Centrex技术员来完成。现在用户拥有自己的终端，通过它用户不仅可以自行完成电话的搬移过程，而且可以改变电话台的特征，增加新号码等。这类行为称为将执行MAC（Moves-Adds-and-Changes，搬移，增加与改变）转换为软件的修改。

选择Centrex而不选择PBX的最重要的原因，可能是它相对于PBX来说具有更高的可靠性（虽然PBX系统的可靠性也不低）。安置在CO的Centrex可以更好地防止由于地震、火灾和各种蓄意破坏所引起的损害。经过严格培训的技术员要一天24小时在现场进行看护，要保证技术员和零件很快地到达PBX系统的各个地点。当然，许多大型的PBX系统肯定需要一个训练有素的技术员在工作时间进行维护；但是在Centrex系统中，即使是个人用户也能拥有快速的全方位服务。

Centrex的其他优点还有：它并不需要用于保持冷却的PBX室，不需要设备保险，也不需要很多的职员来管理Centrex。然而，Centrex需要FCC和政府部门严格控制。其经过所有的LATA的服务并不是相同的，并且可利用的SMDR信息有时也会有局限。

13.2.3 中心局本地局域网(CO-LAN)

1985年贝尔大西洋公司首次提供CO-LAN服务。CO-LAN允许用户通过他们的话音网络发送及交换数据，这种话音网络是一种话音/数据集成形式。用户完成数据的发送与交换的第一种方法就是，使用在语音线路上传输数据（Data Over Voice，DOV）的调制解调器。这样的调制解调器要在CO和用户的建筑中使用，如图13-3a所示。使用DOV调制解调器能使话音和（速率高达9600bps的）数据在一对线路上传输。因此，对话音网络使用同样的线路，用户仅仅付出不大的费用增加就能接收网络数据。

数据在话音线路上的同时传输是通过将数据调制到100kHz左右的模拟信号上实现的。然后，携带数据信息的模拟信号被频分复用而输出。由于话音的频率是在3kHz左右，而调制数据在100kHz，因此在CO用滤波器就很容易将数据信号从话音信号中分离出来，参见图13-3b。

但是问题在于，在话音线路上，每3英里就需要负载线圈，并且这些线圈会阻止4kHz话音频带的低端和高端的信号传输。DOV调制解调器在带宽的范围内将调制后的数据复用，这样就不能使用负载线圈。因此，使用DOV调制解调器的CO-LAN就被限制在3英里的范围。

位于CO内部的DOV调制解调器也做同样的事情，只是顺序相反。解复用之后的话音进入话音交换机，数据直接进入分组交换机，话音和数据均能够被交换机送回到用户的房屋或者

通过PSTN和分组网络发送到远处某地点。如在图13-3的框图中，数据也可以使用T1链路经交换后回到用户所在地的主机。

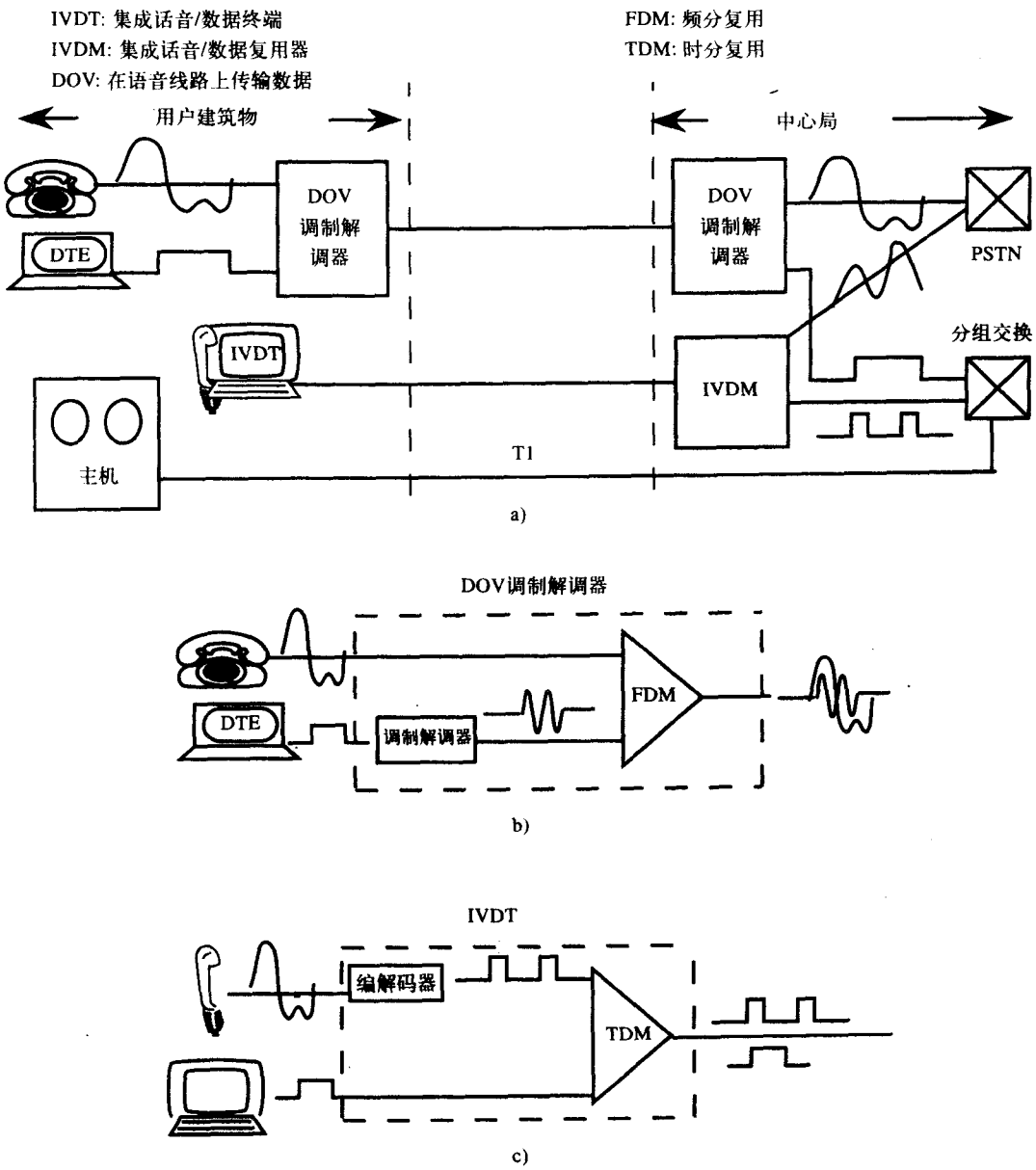


图13-3 a) 使用DOV调制解调器的模拟信号以及使用IVDT的数字信号的CO-LAN的操作，b) DOV调制解调器将话音和数据结合为模拟信号，c) IVDT将话音和数据结合为数字信号

随着ISDN的引进，出现了一种更可靠的也更昂贵的可选方案，它采用IVDT(Integrated Voice/Data Terminal，集成话音/数据终端)，如图13-3c所示。它允许以高达64kbps的速率进行数据传输。从信号方面说，这正好与DOV调制解调器所做工作互易。它不是对数据进行调制，而是将话音数据数字化，也并不进行模拟信号的频分复用，而是对数字信号进行时分复用。然而，对于最终用户而言，这两种方法的实际效果都是一样的。

13.3 按键系统

13.3.1 1A2系统

随着贝尔电话公司将1A1系统推向市场，按键系统也在1953年被首次提出。10年之后，1A1系统的换代产品1A2系统在很长的一段时间内成为很受欢迎的产品。采用按键系统能使拥有50部或更少电话的公司只要投资很少的线路就可以了，而且线路的数量要比所拥有的座机（或电话）数目要少，因为公司的电话可以共享外面进来的线路，所以公司使用很少的电话线路是可行的。

图13-4给出了一个3×5配置的简单1A2系统，其中3代表来自CO的线路数，5代表所连接的座机数。这些电话线路均从CO定制，并且在安装过程中使用任何组合的电话号码能够终止于任何一部按键电话。例如从外部呼叫内部的电话号码238-1001，那么内部所有这个号码的电话机都会振铃，用任何一部都可以接听。若某个人接了这个电话，则在其他电话机上该号码的指示灯就会发亮，表明线路正在被使用。对于从内部向外部的呼出而言，座机从CO得到它们的拨号音。

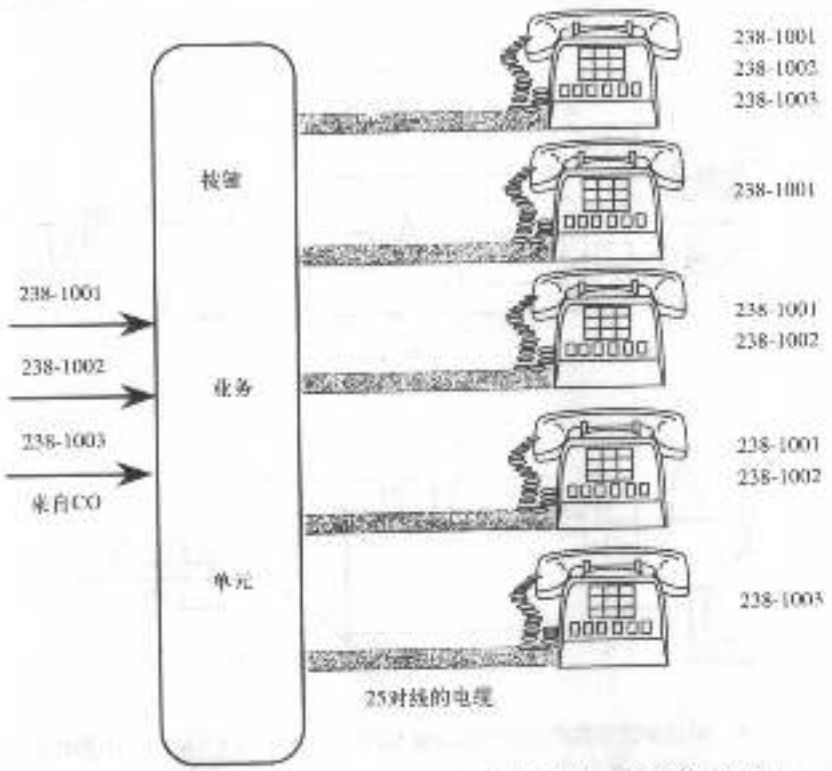


图13-4　一个不是很典型的3×5配置的1A2按键系统。在典型的系统中，三个进来的号码将在所有按键电话处终止

1A2按键系统过去被称为“粗电缆”按键系统，这是因为不管有多少个电话号码被分配给一个按键式电话机（在大多数情况之下，最多有5个号码），则必须有一个25对线的电缆连到一个座机上，其原因是5个可能的电话号码中的每一个都需要3对线。在设备周围安装这样的

粗电缆代价很高，而且体积庞大。

与使用细电线的PBX电话机相比，1A2按键电话机会比较复杂。采用1A2系统拨号的重点在于使用外部的电话线路；而使用PBX，用户必须先拨打接入号码，例如“9”，才能获得一条外部拨号。在PBX系统中，通常由服务人员或自动化系统来处理进来的呼叫。但是在1A2系统中，拥有终端座机电话号码的任何人都可以处理进来的呼叫。1A2与PBX之间的另一个不同点是1A2系统很简单地就能通过CO的拨号音，而PBX系统提供其自己的拨号音。由于没有SMDR（Station Message Detail Recording，站点消息详细记录），因此1A2系统也是有局限性的。这样的按键系统不支持连接中继线或者DID（Direct Inward Dialing，直接拨入电话）中继线。系统不包括任何交换智能，实际上这种智能只是指选择按键电话各种按钮的用户的集合而已。

13.3.2 电子按键系统(EKS)

1983年，也就是出现1A2系统的20年之后，许多厂商开始将EKS（Electronic Key System，电子按键系统）推向了市场。与1A2系统中的座机不同，这种系统的座机仅仅使用两对或三对线路就够了，因此这种按键系统称为“细线”（skinny-wire）系统。该系统中的KSU要比以前的小得多，它们采用的是微芯片而不是机电部件，并且易于安装。它们有连接中继线和DID中继线，进来的呼叫可以由接待员处理，类似于PBX系统。实际上，今天在PBX上可获得的几乎所有功能都可以在EKS上获得，这样就很难区别EKS系统与小型PBX系统。

北电网络（Nortel）公司的Norstar就是一个EKS的例子。它拥有一个开放结构接口，允许第三方为其编写特殊目的的软件。可以用PC为Norstar进行编程，这也鼓舞了很多具有创造性头脑的人来进行应用程序的编写，而不仅仅局限于NT工程师。就传统而言，这在PBX市场上还从来没有听说过，PBX的制造商不会将其系统软件核心与他人分享，因为只有这样他们才能增强其PBX设备的功能。

这样就使得EKS系统在某些方面要优于PBX系统。例如在PBX系统中，如果一个用户要改变办公室，并且想保留原来的电话号码，那么技术人员必须改变PBX上面的编码；而采用Norstar的用户仅需要把电话机带到新办公室并插到相应的接口就行了，KSU会检测到电话机的移动，根本没有必要去改变原有的程序。这是由厂家在按键式电话机里面设置的硬件物理地址完成的，这在PBX系统中还没有被广泛地应用。

按键系统也可以被应用到PBX或Centrex之后。这里的“之后”（behind）是指交换机的用户端，“之前”（in front）是指交换机的公共网络端。在图13-5中，KSU通过OPX线路连接到PBX之后。尽管OPX线路通常经过一个或多个CO，但在逻辑上，它们使得按键系统成为CO的一部分。

如果没有按键系统的话，远端的四个电话通常需要租用来自电话公司的四条OPX（Off Premise Extension，建筑物外扩展）线路。而在远端使用EKS系统时，可以证明仅需要两条OPX线路就足够了。在这种配置中，如果远端的两个电话正在使用这两条OPX线路向外进行呼叫，那么第三个远端的电话机就不能呼叫其自己设备以外的任何用户。

顺便指出，在这个例子里，如果来自PBX的呼叫者通过远端的按键式电话机转接到该PBX中的另一个用户，按键电话机就有可能发信号通知PBX，而不是KSU去进行这种转接操作。如果是通过KSU进行此项转接操作，那么两条OPX线路未必会被连在一起。

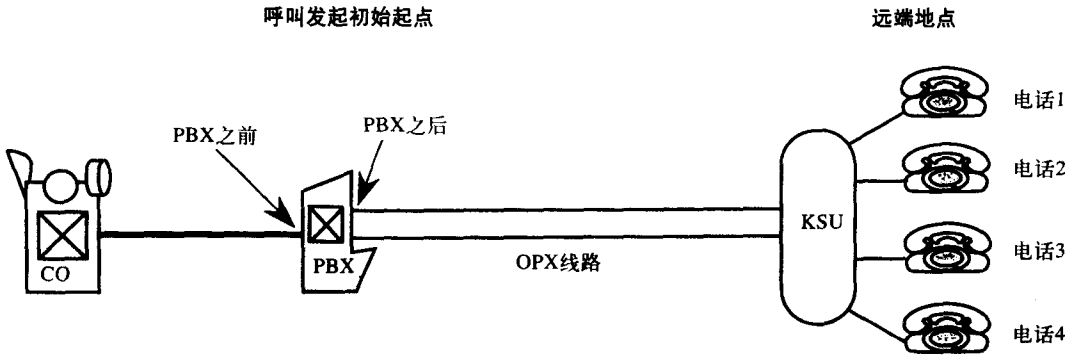


图13-5　连接到一个PBX或Centrex后的按键系统能最大程度地提高整个系统利用率

13.4　其他小型语音系统

13.4.1　混合系统

混合语音系统类似于按键系统，所不同的是在按键系统中，呼叫方选择线路进行呼叫；但是在混合系统中，呼叫方所做的只是接电话，而由类似于KSU的设备选择空闲线路进行呼叫。因此，在混合系统中可以用许多线路发起呼叫；而在按键系统中，如果分配给一个设备的所有线路都忙，那么即使有其他的空闲线路，该设备也不能发起向外的呼叫。按键系统线路的税费要比混合系统的低。这两个系统的区别仅在于所携带的软件不同。

13.4.2　无KSU的系统

最后所要讲的是，无KSU的系统对于拥有少于10部电话机的电话系统来讲是很理想的。而且比按键系统要便宜，无须KSU，非常容易安装。

13.5　PBX功能举例

本章的其余部分将主要讨论PBX。PBX的功能通常可以归结为三类：电话台的功能，话务员操作控制台（即传统的交换台）的功能和整个系统的功能。这里将给出有这些特征的一个例子，这样就能够说明PBX的功能。大多数PBX都可以找到数百个特征。

13.5.1　电话台的功能

电话台的两个最常见的功能是：呼叫转接（call-transfer）和呼叫传递（call-forward）。呼叫转接允许被呼叫方将呼叫转交给第三方，从而使得第三方与原呼叫可以进行通信。

另一方面，呼叫传递允许用户在吃午饭或者缺席时，由其他人用他们自己的电话机来应答他们的呼叫。

呼叫等待（call-park）是电话台的又一功能，通常是用在医院里。例如，如果外部主叫方拨打医院的电话找一名专业大夫，那么接线员将告诉主叫方不要挂断，然后话务员将该呼叫设置到一个虚的电话号码，也就是说并没有任何电话连接的一个分机。接着接线员会通过扩音器告诉这位大夫，请他拨打那个虚的电话号码。这样，这位大夫就能通过医院里的任何一部电话机进行呼叫，拨打接入号码后，该分机就会接通主叫方。主叫方听不到任何回铃音。

13.5.2 话务员操作控制台的功能

PBX话务员操作控制台的一个功能称为中途截听。它避免了话务员（接线员）不得不对呼叫者说："无效电话号码，请您查询。"而且这样也防止了电话系统因为只有呼叫没有回答而阻塞的情况。

自动回拨功能使通话中的一方能够获得在线服务反馈。

系统中也可以使用PC，而不使用话务员操作控制台。使用基于Windows的环境，话务员就能很容易地对几个呼叫进行跟踪并根据需要对呼叫进行特殊的记录。这就使得话务员的工作变得更容易，同时也为外部呼叫者提供了一个专业的氛围。在同一台机器上的呼叫之间进行文字处理和电子表格的应用促进了效率的提高。

13.5.3 系统的功能

服务等级是一个重要系统功能。对于语音终端（如电话机）就是一个优先等级问题。可以指定64个不同的优先级。最重要的电话设备被赋予第1优先级，而最不重要的（如自助餐厅里的）电话机就被赋予第64优先级别。通常为简单起见，仅分配8个不同的服务等级。服务等级高的电话机具有更多的电话台功能，它可以进行长途呼叫，还会有其他一些特权。与各个等级有关的服务是由电信管理人员进行规划的。

在关于Centrex一节的介绍中提到的SMDR（Station Message Detail Recording，站点消息详细记录）提供了哪一个分机被呼叫，被谁呼叫，在什么时候被呼叫，通话多长时间以及呼叫费用的记录。这类信息有助于电信资费、票务部门的管理，同时可以控制电话的滥用。它又可以称为CDR（Call Detail Recording，呼叫详细记录）。

13.6 朗讯公司的DEFINITY

作为PBX系统的一个例子，本节介绍朗讯公司的DEFINITY ECS（Enterprise Communications Server，企业通信服务器）。学习一种特定的PBX要比一般性地学习PBX更有好处。面对市场的激烈竞争，所有大型生产厂商都在不断地改进自己的产品。

13.6.1 电话设备

与其他PBX一样，朗讯的DEFINITY支持2500型座机，它们都是目前家庭常用的桌式或壁挂式电话机。它们有两对信号线，但只有其中一对线被使用。这些话机均为模拟电话机，因为话音是以模拟波形的形式通过一对线从话机传出的，并且与这对线相连的交换机线路卡的编码器将话音信号转换为数字信号。

朗讯的8400、9400和6400系列的电话机都是数字电话机。数字电话机将话音转换为数字形式后，才将其发送到线路上，这样，PBX中的线路卡就不必再对话音信号进行数字化了。数字化的过程可以在听筒里完成，这些类型的电话机都可以说是功能电话机。采用一个普通的2500型座机，通过输入拨打接入码来激活或者解除其功能，这种电话的电话站功能就体现出来了。然而，用户要想激活这些功能只需要按下预设按钮，而不是电话键盘上的按键。这种电话机也属于特定厂商的电话机，也就是说它只能与一家厂商的设备共同工作。

以前特定厂商的电话机通常是与两对线相连的，然而，如果用一对线的话，连接到PBX的线路卡上的电话机数就是原来的两倍。前面提到的DEFINITY电话机既可以使用一对线进行连接，也可以使用两对线进行连接，包括ISDN BIR的连接。

集成话音/数据工作站包括一台数字电话机和一台运行PC/ISDN平台软件的PC。把一个接口卡插入到PC的一个八位扩展槽中，而且这台PC使用标准电话插孔连接到话音终端（电话机）上。利用连接到DEFINITY系统上的工作站，一个人就能在与其他地方的另一人对话的同时与一台主机或者其他PC进行通信。这样的PC/ISDN平台为那些能够创建他们自己的应用软件的客户和独立开发人员提供了一个开放的软件接口。现在，可以得到很多为先进的消息中心、终端仿真器以及话务员工作站设计的应用软件。

在DEFINITY 产品系列中，我们可以见到Quorum A-28 Conference Bridge和SoundStation。这种会议桥可以允许多达28个电话机连接到电话会议上。通过连接该桥，可以使所有连接方进行通话，如果使用演讲模式的话，则仅仅可以允许一方通话。SoundStation拾取房间内许多人的正常谈话，并提供电话会议环境。

13.6.2 站点链路

以前，从话音终端到DEFINITY的连接是用四对线来实现的:.第一对是用于承载速率为64kbps的数字话音信号，第二对承载64kbps的数据信息，第三对用于传输速率为32kbps的信令信号和帧信号，第四对从配线间到工作站传输直流电。两个64kbps的信道称为信息信道，它连同8kbps的信令和24kbps的控制和帧比特就形成了朗讯的专有DCP（Data Communications Protocol，数据通信协议），其速率为160kbps。今天的发展趋势是使用较少的线对以减少安装和线路卡的成本。利用多路复用技术和直流电源幻像（phantoming），线路的数目就可以减少到两对。目前，可以使用的是仅有一对线路的DEFINITY链路。所谓幻像就是说用相同的线路来传输数字信号和直流电源。例如，9400和6400电话机就仅用一对线路，而8400电话既可以使用一对线路又可以使用两对线路。

13.6.3 DEFINITY 框图概述

图13-6是一个简化的DEFINITY ECS框图。根据其配置不同，DEFINITY每小时可以支持的呼叫多达250 000个。

各种不同类型的计算机都可以连接到DEFINITY，提供非交换类型的应用程序，例如文字处理、终端仿真、消息中心处理、呼叫信息记录、ACD环境和UNIX下的呼叫管理系统以及局域联网等。Audix是朗讯的话音邮件系统。DEFINITY也能支持TCP/IP协议，并且在使用IP中继线时提供路由服务。

PPN（Processor Port Network，处理器端口网络）是DEFINITY系统的主控制器，可以有多达800个终端直接连接到它上面。当需要更多的终端时，可以把EPN（Expansion Port Network，扩展端口网络）连接到PPN上面，直至所增加的终端和EPN数量达到了限制，这时，其他DEFINITY系统就可以通过增加更多的PPN并再次开始扩展处理进行联网。两个DEFINITY系统的网络连接如图13-6所示。

EPN可以与其各自的PPN位于同一位置或者通过光纤连接位于距离PPN 5英里以外的地方，更甚者，可以使用T1连接将EPN放在100英里以外的地方。每个T1连接能够提供多达24个终端，最多能够支持4路T1连接，即96路信息信道，但96个信道中有两个信道为系统所需。不管使用光纤还是T1/ISDN链路连接到EPN上面的终端，都是作为同一DEFINITY系统的一部分。

DEFINITY连接到多达126个基站上面，这些基站可以为多达500台电话提供无线服务。所设计的无线系统能够覆盖的区域高达400万平方英尺。它采用PWT（Personal Wireless Telecommunications，个人无线电信）技术，并能为无线手机提供对DEFINITY所有功能的支持。

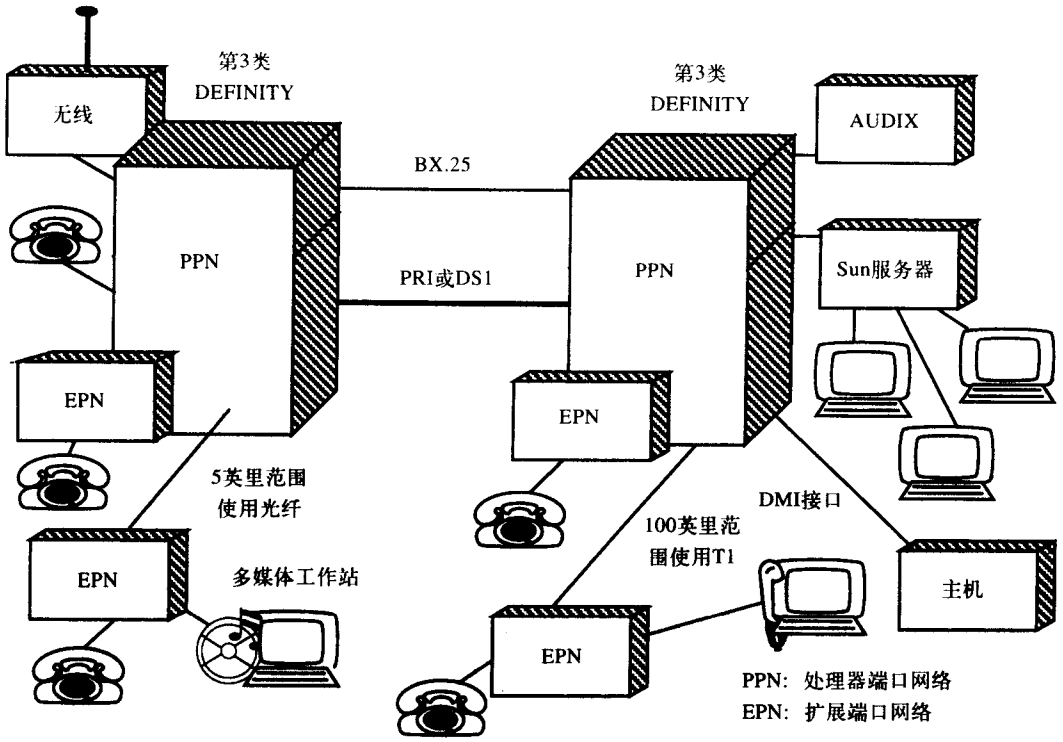


图13-6 一个DEFINITY ECS（企业通信服务器）的框图

多媒体呼叫仅能够依靠话音或者视频建立。一旦发起呼叫，就要增加数据信道。MMCH（Multimedia Call Handling，多媒体呼叫处理）允许用户利用电话机控制话音、数据和视频等功能。选择使用多媒体可以使PC应用程序的共享成为可能。

13.6.4 配置

图13-7a说明仅用一个PPN就足以容纳一个端口数不超过800个的PBX系统。当需要增加更多的线路和中继线时，可以将两个EPN相互连接起来，如图13-7b所示。如果必须加第三个EPN，那么就需要更复杂的配置，即如图13-7c所示能容纳多达15个EPN的配置。在这种配置中，必须在PPN设备箱或EPN设备箱中增加称为CSS（Center-Stage Switch，中心级交换机）的载波或电路。

如果需要附加的EPN，那么必须在CSS中增加SN（Switch Node，交换节点），这样就可以容纳多达43 个EPN，如图13-7d所示。在图13-7e中用ATM交换机代替CSS，就可以实现一种更为标准的配置，这种情况所采用的接口称为ATM-PNC（Asynchronous Transfer Mode-Port Network Connectivity，异步传输模式-端口网络连接）。通过这个接口，DEFINITY系统就能为解决非专有网络的扩展问题做好准备。ATM-PNC也能直接用在PPN中。

13.6.5 DEFINITY结构

图13-8所示为DEFINITY的框图，它是由PPN、EPN和CSS模块构成的。在PPN的中心是一个RISC（Reduced Instruction Set Computer，精简指令集计算机）。由于采用RISC后CPU提取指令时查找的指令表变小，因此这种结构使得计算机指令的运行速度更快。

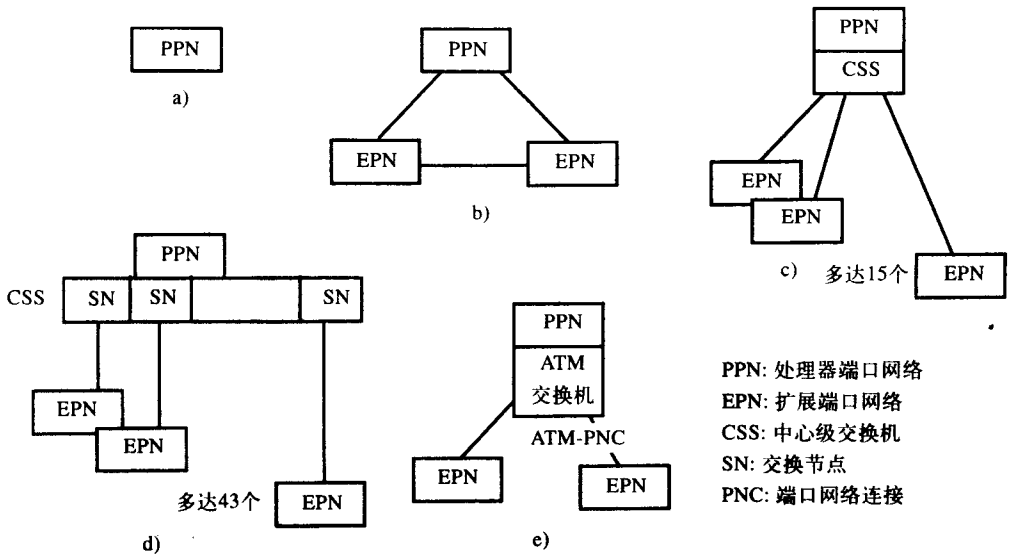


图13-7　a) 对于800台以下的配置，一个PPN就足够了。b) 2000台以下时，可配置为一个PPN和两个EPN。c) 对于更多的端口，可以采用一个PPN、一个CSS以及多达15个EPN。d) 带有SN的CSS能够容纳43个EPN。e) CSS也可以被ATM交换机所取代

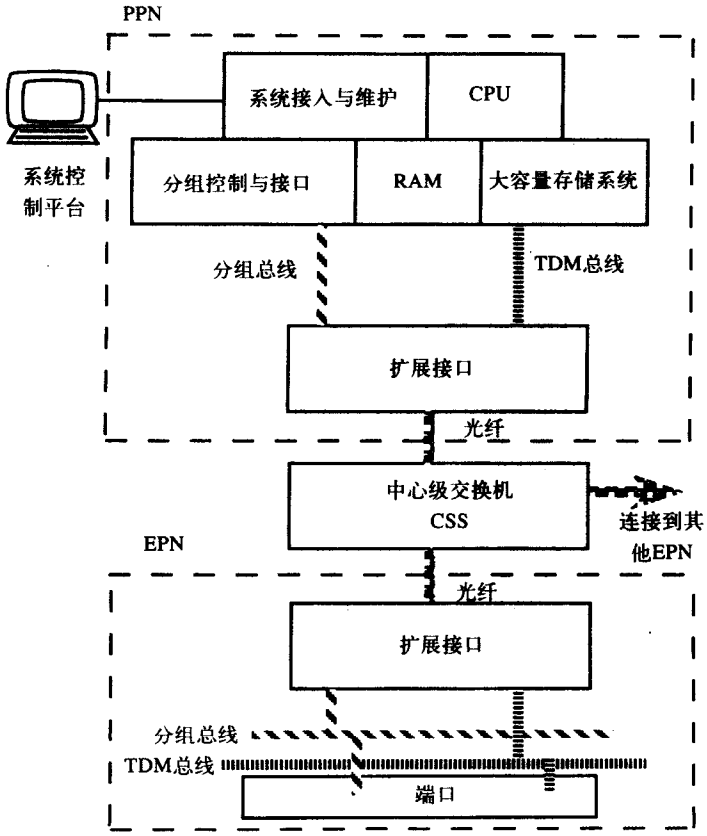


图13-8　DEFINITY ECS（企业通信服务器）的结构框图

PPN也可以包含RAM。呼叫处理、系统程序以及管理程序都是通过这里的RAM进行处理的。大容量的存储系统提供了与基于SCSI磁带和磁盘存储设备的连接。系统的接入和维护为DEFINITY管理终端提供了接口，该终端可以监视线路状况并从中央位置管理整个系统。

DEFINITY采用了分组总线，为系统中各个不同模块提供高效率的通信。分组总线是通过EPN来扩展的。与分组总线相并行的是一个载有实际信息的TDM总线。在PPN中所示的最后一个模块是扩展接口。它提供了PPN、EPN和CSS等各种不同模块彼此互连的统一方法。一般来说，这些模块之间是通过光纤链路进行互连的。

CSS在所有的端口网络之间提供了一个完全的非阻塞连接。这是通过具有扇出、扇入和多路复用电路的空分交换机完成的，这些电路在端口网络的时隙之间提供了必需的交叉点的连接。因此，当CSS用在一个系统中时，PBX就被称为“交换连接”的，或者说是“直接连接”的。

每一个EPN包含一个Intel处理器、一个时隙交换机、一个TDM（Time Division Multiplexed，时分复用）总线、一个分组总线和端口电路。EPN内部的处理器通过分组总线与PPN内部的CPU进行通信。该处理器扫描端口，为任何摘机的用户提供拨号音。它既可以进行模块内交换又可以执行其他实时集中处理。

EPN处理器从TDM总线上提取出需要和其他EPN通信的信息（语音、数据等）比特，之后将它们放在通往CSS的时分复用信道上。这样，CSS就可以将这些比特交换给它们各自相应的EPN。因此，EPN主要在本地TDM总线与连接到CSS的光纤信道之间传输比特信息。一次模块内呼叫是由一台EPN来处理的，并不需要CSS，但是模块内呼叫需首先通过TDM总线交换到主叫EPN上，然后通过CSS进行空分交换，最后再时分复用交换到被叫EPN。这称为时-空-时结构，广泛地用在所有的PBX系统中。

13.7 级联专用线路网络

图13-9所示的是20世纪60年代使用立即启动专用线路的PBX网络。在该网络中，如果电话1想呼叫电话2，它将会得到其所属的PBX的拨号音，之后拨打电话2的分机，之所以这样是因为它们都是一个PBX的一部分。但是，如果位于迈阿密（Miami）的电话1要呼叫位于休斯顿（Houston）的电话4，那么电话1要首先听到迈阿密的PBX的拨号音，再拨打中继组接入号码3。然后它就能听到位于亚特兰大（Atlanta）的PBX的拨号音，接着拨打接入号码5来获得位于休斯顿的PBX的拨号音。现在电话1就能拨打电话4的分机号建立起它们之间的连接。

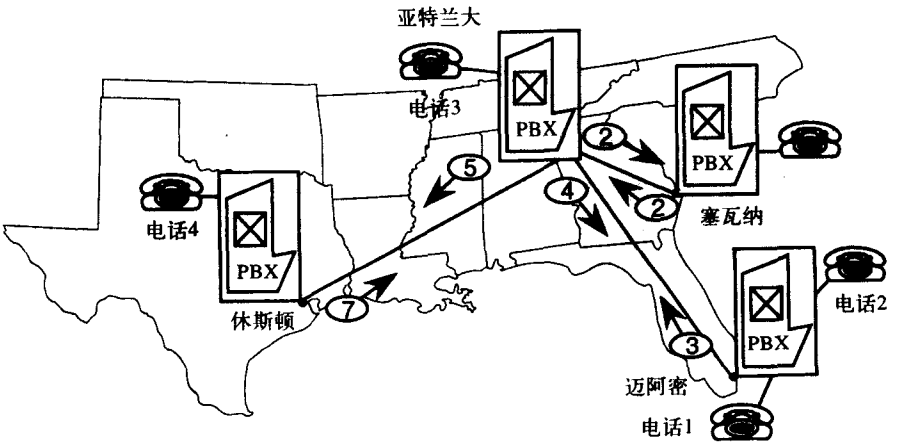


图13-9 一个级联专用线路网络，对特定PBX给出了接入所需的节点

需要注意的是在这样的网络中，节点之间的所有交换都由呼叫者人工完成。如果从亚特兰大到休斯顿的中继组很忙，则呼叫者必须不断呼叫，直到到达目的地的所有链路都空闲为止。而且呼叫者还必须知道中继组的接入号码以及网络是如何配置的，只有这样才能进行网络呼叫。同时，由于两部电话的分机号码可以是相同的，因此在网络中通过电话号码唯一地确定一部电话机是不够的，这是因为还必须知道电话机的位置。如果呼叫者不知道听到的是哪台PBX的拨号音，那么他就会迷失在网络中，必须重新开始。

13.8　专用网络

北电网络（Nortel）将其PBX网络方案称为ESN（Electronic Switched Network，电子交换网络），朗讯（Lucent）将其PBX网络方案称为ETN（Electronic Tandem Network，电子级联网络）和DCS（Distributed Communication System，分布式通信系统），其他公司也用不同的名称来称呼各自的PBX网络。我们不考虑这些网络的厂商，将它们统称为专用网络。ESN与ETN之间的主要区别是ESN使用一个叫做CMC（Communications Management Center，通信管理中心）的中央管理中心，CMC具有连接到所有交换机的数据链路。所有的网络操作在这个中心点执行并监视。应用13.7节介绍的级联专用线路网络之后，专用网络的优点就变得越来越突出了。

专用网络的功能

与早期的网络相比，专用网络具有很多以前的网络所不具备的功能。其中之一就是统一的拨号方案，采用这种方案可以使每个终端在其公司范围内的网络里面有它自己唯一的识别码（电话号码）。通常，各PBX都有一个唯一的3位代码，与CO的交换机类似，各终端都有一个4位数的分机号码。这就是7位专用拨号方案。现在位于迈阿密的电话机只需要听到一个拨号音即可拨打位于休斯顿的电话4的7位号码。于是，迈阿密的PBX检测前3位数码之后，就将呼叫传递到亚特兰大的PBX，该PBX同样会将呼叫传递到休斯顿的PBX。

位于休斯顿的PBX识别出它自己的前3位号码，并利用后4位号码完成此次呼叫。这里PBX之间的交换是自动完成的，而不是由呼叫者人工操作的。而且，无论呼叫发生在什么地方，所拨叫的号码总是一样的。这样所有地方都使用一个电话号码簿即可。而采用级联专用线路网络时，呼叫电话4的接入号码取决于呼叫者所处的位置。

CAS（Centralized Attendant Service，集中式话务员服务）允许在一个地方为所有PBX位置处理话务员（或者交换台操作员）服务。因此，没有必要在每个地点都安排一位话务员，但是，如果PBX没有联网，则每个地方都需要一位话务员。

不管用户在什么地方，这种功能透明性为所有用户提供了相同的功能和PBX的相似性。在用户看来，它更像一个大型的PBX系统，而不是PBX的一个网络。

对于一些公司而言，DISA（Direct Inward System Access，直接拨入系统接入）简直就是噩梦，它允许公司的授权用户拨入PBX，提供授权号码之后就有权访问PBX内部的任何资源。这样，用户就可以拨打专用网络的任何其他地方，或者不通过话务员就可以拨入到公共网络中。一些具有授权号码的DISA号码已经在黑市上出售，购买者就可以在损害专用网络所有者利益的情况下，为自己拨打国际电话。因此，在使用DISA时，应该在PBX内部采取有效的安全措施。

如果存在通往目的地的备用路径，那么要完成一次呼叫可以有两种方法。其中一种方法称为AAR（Automatic Alternate Routing，自动交替路由），它能够通过专用线路网络提供最佳的路径。另一种方法是使用PSTN来完成一次呼叫，称之为ARS（Automatic Route Selection，自动路由选择）。

13.9 ARS（自动路由选择）

13.9.1 ARS的决策过程

ARS软件可以确定出通过公共网络完成一次长途呼叫的最廉价方式。LCR（Least Cost Routing，最低费用路由）与ARS很相似，不同点在于它是基于日期折扣来选取最佳路由的。在很多情况下，我们会交替使用这两个术语的。

ARS本身就是一个表驱动的选择，这在购买PBX的时候就能得到。它能够根据区号、交换机、甚至终端的电话号码来阻塞900个不必要的呼叫。

当进行长途呼叫时，例如图13-9中从亚特兰大到休斯顿的呼叫，ARS就会监视通往休斯顿的连接中继线，并试图利用它来完成呼叫。于是从休斯顿就可以使用DDD（Direct Distance Dialing，长途直拨）服务。

如果连接中继线忙，则可以采用WATS（Wide Area Telephone/Telecommunications Service，广域电信业务）线路直接连接到休斯顿。如果连接中继线和WATS线路都不空闲，PBX通常会等10s后再看它们中间的一个是否有空闲。如果均无空闲，PBX就会发出5s的提示音，让呼叫者挂掉电话稍后再试。但是如果呼叫者想立即再试并不挂掉电话，则PBX将通过DDD网络直接拨号到休斯顿。

这就是一个PBX利用ARS完成一次呼叫的决策过程的例子。通常，让至少50%的呼叫利用连接中继线以控制长途呼叫的成本；对于它们而言，每分钟呼叫的成本是最低的。一般35%的呼叫是通过WATS线路来完成的，接近15%的呼叫使用的是DDD服务。

13.9.2 一个实例

堪萨斯城（Kansas City）的一家公司有到旧金山（San Francisco）的大量呼叫需求。旧金山的区号是415，因此它们之间有一条FX中继线。在西海岸，该公司还有一个WATS的服务区域3用于呼叫其客户，参见图13-10。

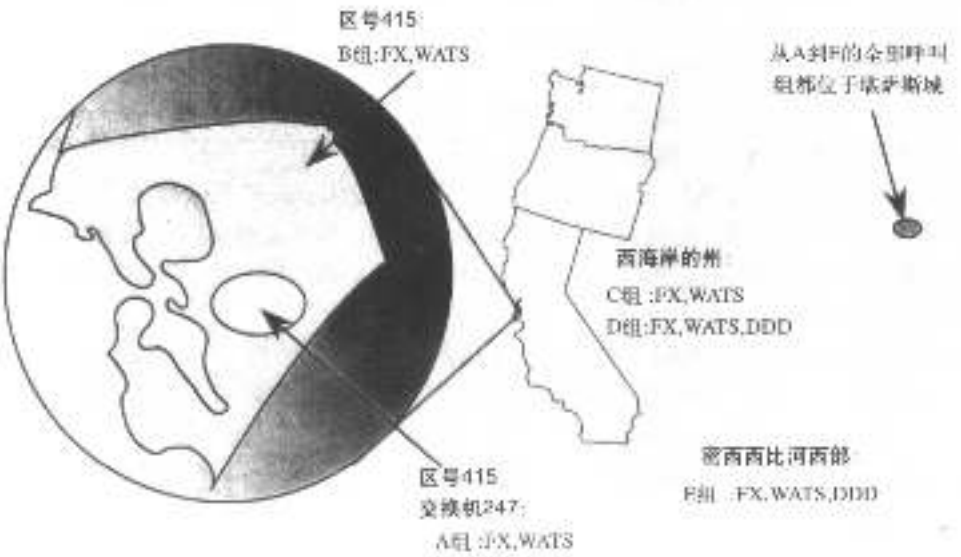


图13-10 实例中位于堪萨斯城的各组员工的ARS约束

A组的员工仅需要呼叫415区的号码，该区有一个交换机247，也就是说他们拨打的号码为415-247-xxxx。他们必须将FX中继组作为第一选择，将WATS服务作为第二选择，并且限制他们使用DDD服务。

要求B组的员工呼叫415区的所有号码，而不管交换机是哪个。C组的员工可以呼叫西海岸的任何一个州的电话机。B组和C组的员工只能使用FX和WATS服务。D组的人员也能呼叫西海岸任何一个州的电话，但所不同的是他们还可以使用DDD服务。

最后，允许E组的员工在需要时使用DDD服务可以呼叫密西西比河西部的任何电话。当然，当E组员工呼叫位于内布拉斯加（Nebraska）的电话时，FX中继线和WATS服务是不可用的。描述对PBX进行编程时所需的呼叫模式和FRL（Facilities Restriction Levels，设备限制级别）。每个地区的各中继组都指定有一个号码，称为FRL，如果一条中继线的FRL的级别高，则该中继组就有更多的呼叫限制。当呼叫者通过中继组进行呼叫时，PBX会在让该呼叫通过之前，检查呼叫者的FRL级别是否比分配给中继组的FRL级别高。

解决方案：首先定义所需的路由模式。第一种模式称为模式02，仅提供对415-247-xxxx的呼叫，而模式03则提供除了247交换机以外的对415的呼叫。模式04包括除415以外的加利福尼亚（California）、俄勒冈（Oregon）和华盛顿（Washington）的区号。模式05除了包括西海岸区号外还包括密西西比河西部的所有区号。这些就是PBX允许呼叫的地区，需要注意的是这些路由模式互不重叠。

下一步，我们必须找到所需的FRL。我们从呼叫限制最多的组（A组）开始，接着是呼叫优先级逐渐增高的组。A组仅能向路由模式02通过FX或者WATS中继线发起呼叫，因此，它们具有最低的FRL级别，即为1，参见表13-1。对于具有较少限制的下一个组，我们赋予它的FRL级别为2，将2这个数字填入到表13-1中采用FX和WATS进行传输的模式03所对应的位置。当一个FRL级别为2的电话机向415-217-xxxx（模式02）发起呼叫时，它就会按照表13-1的第一行处理。由于表中的1小于呼叫者的FRL级别2，所以此次呼叫可以连接，连接时首先使用FX中继线，之后是WATS中继线。一般来说，如果FRL等于或者大于中继组的FRL，则会允许呼叫通过该中继组完成。

表13-1　设备限制级别

模式	FX	WATS	DDD
02	1	1	4
03	2	2	4
04	3	3	4
05	5	5	5

类似地，由于C组的员工需要额外的特权，因而我们就要设置一个新的FRL级别，其值要比前两者的大，设为3。这样，由于较高级别的FRL有权使用较低级别的FRL，因此FRL为3的C组员工就能够呼叫模式02、模式03和模式04，但不能利用DDD服务。D组员工需要使用DDD服务的额外特权，为其分配的FRL为4。最后，由于E组员工可以呼叫更多的区域，于是为其分配的FRL为5。

总之，当建立外部的呼叫时，首先要选择模式（表13-1中的行），之后从左到右检查设备（表13-1中的列），看哪一个可用。如果由表中的行和列指定的数字小于或者等于呼叫者的FRL级别，则呼叫可以建立。否则，发送忙音。如果系统提供中继队列，那么当利用他/她的FRL可以使用中继线时，会给呼叫者发送回呼。

13.10　网络路由

假设我们的公司刚吸纳了一家西部的公司，该公司在亚特兰大（Atlanta）和拉斯维加斯

(Las Vegas) 之间用高容量中继线将两个网络互联起来，参见图13-11。这两个主站点称为节点，它们需要专门的软件进行升级，从而像所期望的那样处理网络路由。

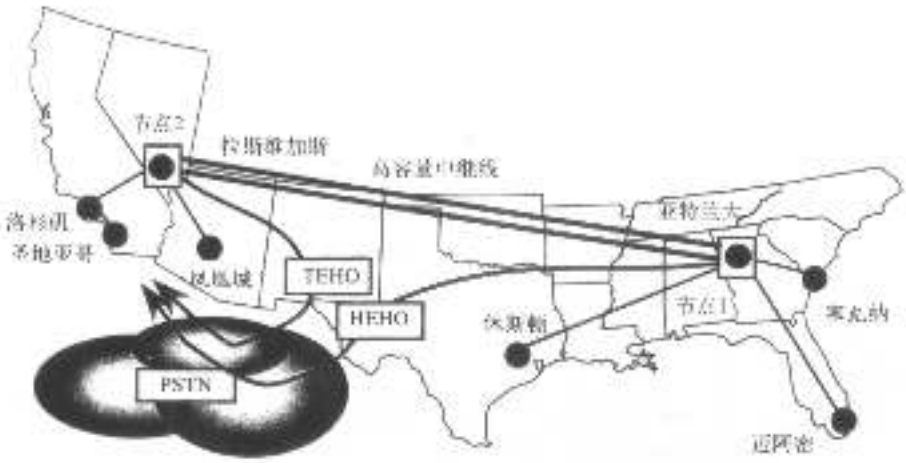


图13-11 通过公共网络离开专用线路网络的两种方法

我们假设迈阿密的电话机1正在呼叫位于圣地亚哥（San Diego）的一部电话机，其最佳路径当然是通过拉斯维加斯节点、洛杉矶PBX，最后到达圣地亚哥。如果从拉斯维加斯到洛杉矶的中继线路忙，那么为了完成此次呼叫，位于拉斯维加斯的节点就有两个选择。

第一种选择是，它将7位的专用电话号码转换成公共的10位电话号码，如果需要分机的话，还会转换为更多位的电话号码。之后它就可以通过公共网络拨打圣地亚哥的终端了。这种方式称为TEHO（Tail-End Hop-Off）。

另一种选择是将通信流量返回到亚特兰大，由亚特兰大进行电话号码的转换，并使用DDD网络通往圣地亚哥。这种方式称为HEHO（Head-End Hop-Off）。

在决定从什么地方脱离专用网络并进入公共网络时，是比较难于处理的。如图13-12a所示，如果节点2距离目的地很近，那么从该处离开会更好，并且比从节点1离开时的DDD费用低。然而，它在节点之间使用了电路，如果该电路是最后一个可以使用的电路，则下一个从节点1到节点2的呼叫也就必须使用DDD网络了。

如图13-12b所示，对于呼叫1使用HEHO，让呼叫2通过专用网络，而不是让这两个呼叫都通过公共网络进行路由，效果可能会更好。

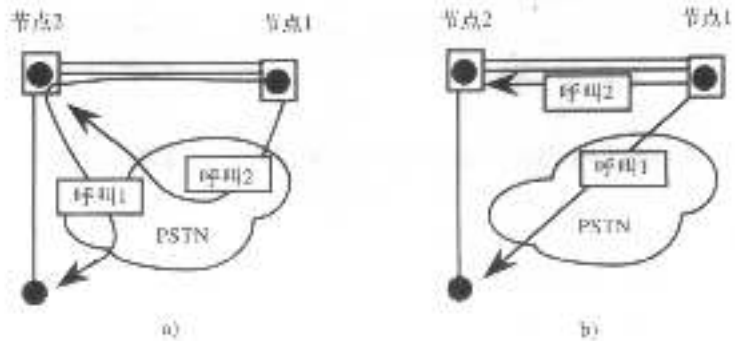


图13-12 两种脱离类型的折中

对专用网络做成本估算、流量工程研究、中继线利用率分析以及各种各样的这类任务都是非常冗长乏味的。虚拟网络正在很快地代替这些专用线路网络。虚拟网络取消了局间中继线路，对所有的呼叫使用DDD网络，并允许在承载网络中使用智能来决定如何对呼叫进行路由分配，这也是第11章讨论的问题。

习题

13.2节

1. 使用PBX比使用Centrex有什么优点？
   a. 可靠性　　b. 快速服务　　c. 高数据率　　d. 容易扩展
2. 在Centrex设置中用什么设备来建立局域网？
   a. 调制解调器　　b. DOV调制解调器　c. EKS　　d. ISDN
3. 什么类型的话音交换系统使用CO来进行楼内（on-premise）交换？
4. IVDT是将话音转换为数字还是将数据转换为模拟的？它使用了哪种类型的多路复用？
5. 使用Centrex与使用PBX相比有什么优缺点？
6. DOV调制解调器是如何工作的，应该怎么使用？

13.3与13.4节

7. 下面哪一个不是1A2按键系统的特点？
   a. 它用两对线连接到话音终端。
   b. 通常，不必拨打接入号码就可以获得外部线路。
   c. 不允许连接局间中继线路。
   d. 进入的呼叫通常不是由接线员处理的。
8. 下面哪一种话音系统使用外部线路“池”，而不是分配给特定站点的外部线路？
   a. 无KSU系统　　b. EKS　　c. 1A2系统　　d. 混合系统
9. 在PBX之后使用什么样的设备能使从PBX到远处地点的OPX线路减少？
10. 解释PBX系统优于EKS系统的原因。
11. 按键系统与混合系统之间有哪些不同之处？

13.5 节

12. 下面哪一个PBX特征使得话务员可以将进入的呼叫连接到不在其电话机旁的用户？
    a. 呼叫转接　　b. 呼叫等待　　c.呼叫截听　　d.服务等级
13. 用PC作为话务员控制台有哪些优势？
14. 对于更高的服务等级而言，电话终端具有更高的特权还是更低的特权？
15. SMDR的另一个名称是什么？

13.6 节

16. 对于话音、数据和信令而言，朗讯的DCP分别采用什么速率？
17. CSS中的交换与EPN中的交换是如何区分的？
18. 解释分组总线与TDM总线之间的区别。
19. 普通住宅电话机的命名法是什么？
20. 解释图13-6中所示各个模块的功能。
21. 扩展EPN范围的两种方法是什么？

22. PPN与EPN之间的区别是什么?

13.7 与13.8 节

23. 以下哪种类型的网络要求主叫在发起一次呼叫时知道各个不同地点的中继接入号码?

a. 级联专用线路 b. 分布式通信系统 c. 电子交换网络 d. 电子级联网络

24. 指出提供PBX类似特征的专用网络较级联专用线路网络的优势。

25. 与专用线路网络相比，哪类网络是首选的?

26. 当专用网络的各PBX有其自己的3位数代码，并且其各附属电话机均有4位数号码时，利用了哪个特征?

13.9与13.10 节

27. 当执行返回时，执行哪种类型的脱离?

28. 分别解释采用TEHO与采用HEHO的原因。

29. 描述如下ARS问题的模式和设备限制级别，并画出表格。

一家波士顿（Boston）的公司拥有一条通往纽约（New York）的FX中继线和一条通往底特律（Detroit）的FX中继线。A组员工可以利用DDD服务呼叫该州的任何地方（所有国际呼叫均被自动阻塞）。B组员工能够首先利用FX，其次利用WATS，之后利用DDD向纽约发起呼叫，但是，他们仅能够利用FX向底特律发起呼叫。C组员工恰好与B组员工的特权相反，即他们可以利用这三种传输服务中的任何一种向底特律发起呼叫，但仅能利用FX向纽约发起呼叫。

第14章 语音处理、ACD和CTI

14.1 概述

语音处理系统能够自动完成进出呼叫而不需要任何人处理这些呼叫，它可以自动处理电话业务。进来的呼叫需要连接到一个专门的分机上面，访问某些信息，需要在被叫方无法接通时存储话音消息的设备，或者这类服务的组合。传统地，这些服务都是由话务员或秘书来操作的。现在技术的进步把一直是由人来完成的任务变成自动完成。如果在设计和实现方面更细心的话，还能够节省一大笔资金，并且为呼叫者提供更好的服务。与电话呼叫接口的计算机是不会疲惫的，也不会发脾气，不会渎职，不需要经受训练，而是会同时处理许多呼叫，并且能够全天工作。

本章的第一部分会讲到各种各样的语音处理系统，然后会阐述ACD（Automatic Call Distribution，自动呼叫分配）和IVR（Interactive Voice Response，交互式语音响应）系统。说到ACD 系统，它是类似于PBX的语音交换机，但是这种系统的设计是为了满足一组代理的需要，这些代理中的任何一个都能回应进来的呼叫并能向外发出呼叫。例如，当某人想预定飞机票时，那么可以通过任何一个代理为呼叫方提供服务，并且这种呼叫经过ACD的可能性很大。ACD将这些呼叫编入队列，按照某种顺序将它们路由到代理。更多的内容还会在后面介绍。我们现在先来介绍各种各样的语音处理系统。

大多数语音处理系统可以作为独立的单元，或者集成在一个PC、一个主机或者一个PBX中。基于PC的产品起到两个作用，既可以作为PC又可以作为语音处理系统。这些基于PC的产品提供一种开放结构，可以选择不同的功能部件，提供多种技术。它们具有与LAN联网或集成在大规模系统中的灵活性。

本章涉及到的所有技术在采用CTI（Computer Telephony Integration，计算机电话集成）后达到顶点。CTI给出了一个允许数据服务器与ACD系统通信的标准方法。这样向呼叫中心呼叫的客户就能够获得快速而有效的服务。以前的所有技术都试图在为客户服务时，减少对操作人员的依赖性。CTI虽然认识到代理与客户接触的重要性，但采用语音交换机与数据服务器的集成来使它们满意地交互。如今，CTI还能从万维网上更有效地为客户提供服务。

14.2 提供话音的方法

14.2.1 录制话音

最早的语音处理系统是由亚特兰大的Audichron公司于1931年提出来的，位于CO的这一处理系统是由可口可乐公司提供的。呼叫者拨叫这个号码，在听到一段简短广告之前，会得到两个78rpm记录的当前时间和温度。这就是一个语音文字的例子,是一种话音处理系统。

这种语音文字或者语音处理系统所能提供的信息通常是通过麦克风录制的声音，如图14-1a所示。今天这种任务能够用数字化语音完成。使用与PCM（Pulse Code Modulation，脉冲编码调制）类似的技术将自然模拟语音转换成数字形式，但是为了更好地利用存储空间，

同时采用了压缩技术。记得在第3章中讲过，采用PCM技术数字化后的一分钟话音占用0.48MB的存储空间。然而，通常采用ADPCM（自适应差分脉冲编码调制）以及其他更有效的语音编码方法，因此它们占用更少的空间。

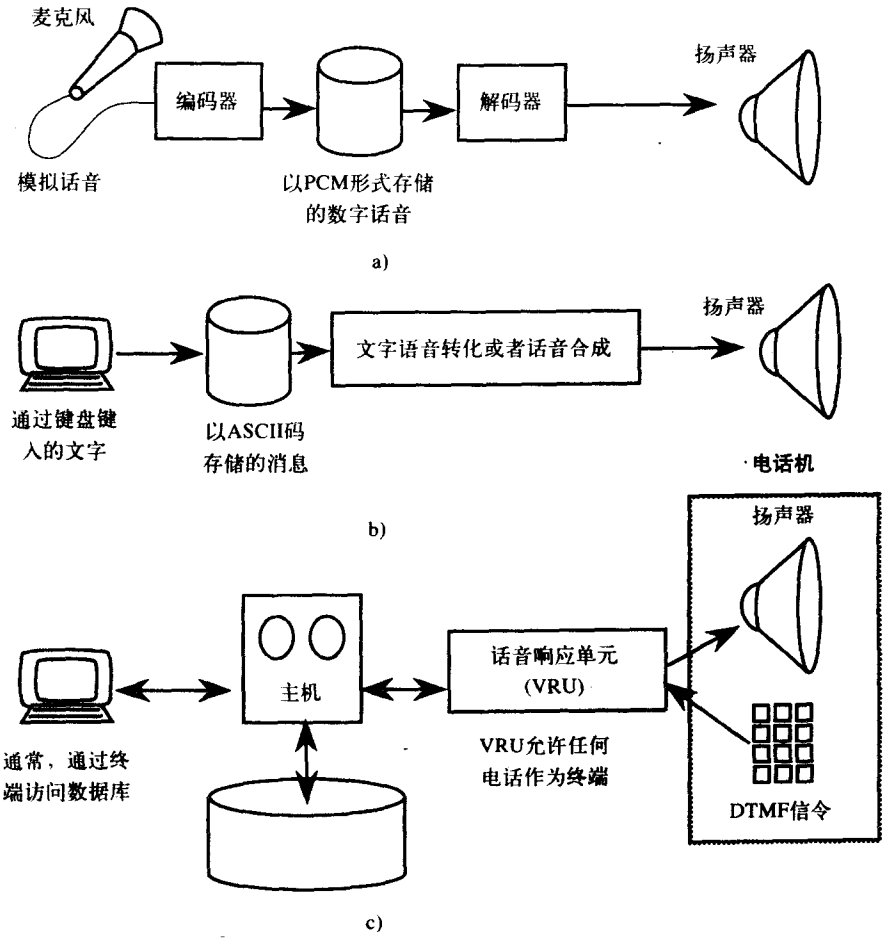


图14-1 a) 录音文字或数字播音器存储可以被任何人呼叫的信息的方式，这些信息既可以通过数字化语音又可以通过语音合成进行回放。b) TTS（文字语音转换）系统“读出”存储的文本。c) VRU 允许私人信息通过电话进行访问，这里数据可以通过使用DTMF进行升级更新

PCM格式的语音数据不是用来打印的，语音就是要在扬声器上听到，而不是在终端被看到。同样地，通过键盘键入的文字就是要让人在屏幕上看到，不是用电话去听到。因此，诸如PCM这样的协议就被应用在电话的通信上，像ASCII这样的协议就被应用在终端之间。

14.2.2 文字语音转换

以前，语音处理系统仅存储数字化语音。但是现在，TTS（Text-To-Speech，文字语音转换）或者**合成语音**技术已经可以从许多厂商处得到。现在无需让某人对着麦克风讲话，而是简单地通过键盘键入信息就能录下一段新的语音，如图14-1b所示。这样做的好处在于，将语音以文本的形式存储比以数字化形式存储占用的存储空间大大减少，这样做也便于进行编辑。现在TTS

也开始用于实现需要存储在数据库中的大量信息重播的应用以及频繁变化的信息重播的应用。

使用英语的话，TTS技术会比较难以设计。比如一个以“ough”结尾的单词可以有7种不同的发音，如单词“dough”、“rough”、“through”和“cough”等等。而且，还有大约100个单词，其发音由上下文决定，例如在这个句子“...did you read what I read about the present which was presented...”里面就是如此。另一个例子就是这个简单的词“the”，根据它的用法可以有“thee”和“thuh”两种发音。许许多多这样的语言规则就使得文字语音转换技术难以实现。

14.3　录音文字信息系统/计划

录音文字系统也称为信息中心邮箱和语音公告牌，是比原先的audichron系统更为复杂的系统，并且还能为呼叫者提供他/她所期望信息的选择。它们可以用在查询股票报价、剧院演出次数、训练安排和商店位置等场合。呼叫者通过录音菜单进行选择类目就可以获得所需的信息。例如，如果你想知道今天比赛的分数，按“1”；如果想知道昨天比赛的分数，则按“2”。

数字播音器也称为被动拦截设备，与公告牌很类似，但是它们通常提供预先录制的声音，诸如电话号码的变更、运行时间、滑雪的气候条件等等。

传真机常用来增加话音处理系统的种类，传真机处理应用的种类包括：请求即传真（fax-on-demand）、传真邮件和传真广播。请求即传真类似于话音公告牌，但信息不是回放给收听者的，而是被传真给主叫方。传真邮件数字化地在接收端保存传真信息，并在接收端准备好后打印出来。传真广播能将图像发送到很多目的地，这些目的地在分配表中是预先定义好的。

如图14-1c所示的系统有大量的数据，必须存储在计算机数据库中。这里，数据通常是通过终端键盘输入的，而不是通过麦克风输入的。为了将这种类型的数据转换成话音，可以使用TTS（Text-To-Speech，文字语音转换）或者将信息传真出去，比如电话银行的应用就是其中一个例子。这种能将电子数据转换成话音并将DTMF（或者按键音）信号转换成数据的系统称为IVR（Interactive Voice Response，交互式语音响应）系统。IVR这个术语使用非常广泛并被用作语音处理系统的同义语。与以上提到的其他系统不同，IVR不仅能够回放信息，而且还能让呼叫者通过电话机的DTMF输入与系统“交互”，从而输入或者改变数据库中的数据。

这些系统之间另一个不同之处，就是图14-1a和图14-1b中的系统一般提供的信息是针对公众的，而IVR在向呼叫者提供私人信息之前能够执行安全校验。后面将对IVR做更多的介绍。

14.4　语音识别

DTMF信令是AT&T公司于1958年开发的，尽管我们现在已经接受了它，但它在加速语音处理技术发展方面还是很关键的。在某些情况下，讲话是接入并控制语音处理设备的唯一方法。用户无需在键盘上面按键，就能通过发出音频指令来命令系统。用户仅需回答“是”或者“否”，或者用数字“0”到“9”作为问题的回答，系统就能解码出进入电话话筒的话音，一些系统还能识别出更多的词汇。

VR（Voice Recognition，话音识别）也称为语音识别或者ASR（Automated Speech Recognition，自动语音识别），它有两种形式。其一是SIVR（Speech-Independent VR，不依赖语音的语音识别），它能检测出所说单词而与讲话人无关。其二是讲话人确认（speaker verification），它能通过他或她的话音来识别讲话人的身份。

基本上，SIVR设备从英语的发音来执行“辨识”，而不是依靠DTMF信号进行识别，完成

这一功能的四个具体步骤如图14-2所示。第一步，为了减少需要处理的数据量，从输入的波形中提取话音的特征，这是由DSP（Digital Signal Processing，数字信号处理）芯片来完成的。第二步，用给定单词的特征与一个可能正确的模型进行匹配，语音模型也称为单词模型或模板，是预先存储在一个集合内的。第三步，称为DTW（Dynamic Time Warping，动态时间偏移），按照讲话人说话的语速，调整所选择的词汇模板，这是因为每个人说话有快有慢的缘故。最后，要由一个通常采用HMM（Hidden Markov Modeling，隐式马尔科夫模型）的事件检测电路决定所说的单词是与模板足够接近，还是应该将其标记为还不存在的单词。对于不依赖于讲话者并且是连续语音，即所说单词之间不需要停顿而言，HMM已经被证明很精确。在这种技术中，人工智能起到了很重要的作用。

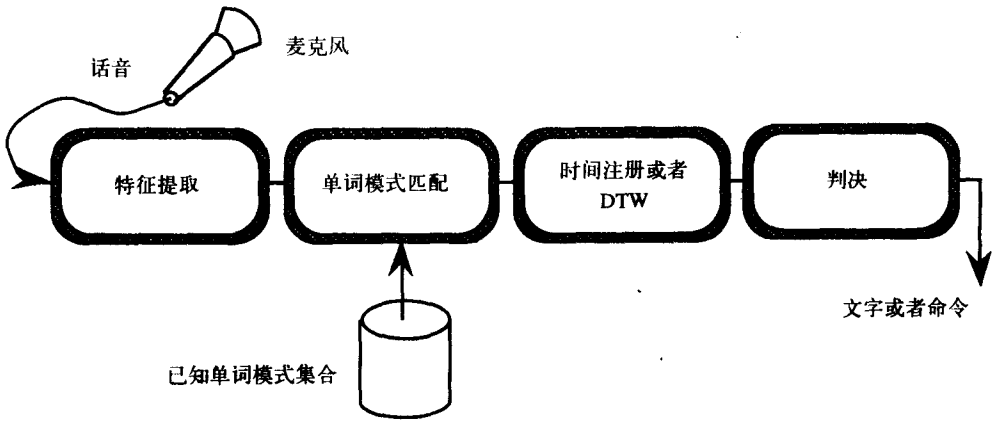


图14-2 匹配所说的话来“识别”语音的四个步骤

依赖于讲话者的话音识别可以识别出主叫方。Sprint公司已经发明了一种“话音”信用卡，采用这种卡呼叫时无需拨打信用卡号，主叫方通过他们的声音进行识别。这样做比采用密码安全多了，因为密码容易被偷。而且，主叫方仅需说一句“CALL HUSBAND”就能拨叫正在工作的丈夫。将来在这类技术的应用方面还有很大的潜力。

常常被忽视的一点是语音识别也能通过比较自然的接口连到计算机上面。例如人不必在仓库里将键盘拖来拖去，有与话音识别系统有接口的便携式电话就足够了。它可以使用户以每分钟200字的速度而不是通常30wpm的速度输入数据。与键入数据相比，话音识别是数据输入的一种更为准确的形式。在手眼都忙的工作环境中，话音识别系统同时提供了一种输入数据的方法。

14.5 语音邮件

1979年，VMX公司的Gordon Matthews获得一个话音邮件的专利，并建立了第一个话音邮件系统。如果被叫方不可用或忙，VM（Voice Mail，话音邮件）允许主叫方在听到预先录制的一段问候之后留言。VM也称为话音消息，是所有用户或分机的一个集成系统，它比电话应答机具有更多的特征。它还能让用户从任何地方（而不仅仅是从他们自己的电话机）取回他们的消息。

14.5.1 为何需要语音邮件

有时候丢失了一次呼叫就等于丢掉了一次生意、一个业务，或者丢失了更重要的东西——个人的信用。如果因为你不在电话旁边而使客户呼叫不到你，他们就会找别处。因为你还有

其他必须履行的职责，所以你不可能总呆在电话旁，秘书可以在你离开时用便条作记录让你知道有谁打过电话，但是糟糕的是有时桌子上面很乱，记录的东西丢失也是在所难免的。而且这些便条也容易出现人为错误，因为秘书的失误，可能很重要的信息就这样完全丢失了。

当需要人为接口处理个人信息时，就可以使用消息中心了。这里，消息中心的话务员为不能接通的被叫人键入主叫者的姓名、号码及其信息。当被叫人呼叫信息中心时，话务员就会将信息读给他。但是，采用消息中心很难强调某些重点，并且很难给主叫方留下具有正常对话时所听到的音调的个人消息。只有当有人在服务时，才可以从消息中心获得消息。而VM消息即使在深夜也能接收。

无论将消息记录在便条上还是输入到终端里，都额外需要一个人参与。即使对于重要的呼叫希望有人工服务，但疲劳的甚至是愤怒的话务员的声音一定不如录制的VM问候。

使用VM的另一个原因是防止“电话标记”（telephone tag），当两部双方同时互相呼叫，被叫方无法接听他/她的电话时，就会出现这种情况。在这种情况下，应用VM就能发送一条完整而又详细的消息，比如“我试图使用你建议的“修改程序”的命令，但是号码000512错误，我下一步该怎么做？”。这也许不如直接与对方说话更有效，但是至少有助于解决问题。在这个例子里，业务技术员在回应呼叫前有时间思考问题或者要求同事给予帮助。

既然众多大小公司在国际舞台上同场竞技，那么当主叫方在工作并且被叫方却在睡觉时，这种电话标记就变得越来越普通了。当员工在不同时区工作时，VM对于他们就变得非常有吸引力。

采用VM之后，人们就不能像实际生活中那样长时间的聊天，因此通常讨论的也仅仅是生意上的事情。与由人来提取信息相比，VM也提供了更好的保密性。如果部门经理想召集一次部门会议，她就要先打出备忘录，再进行复制，最后将它们分发给部门成员并希望每人都可以拿到。如果使用VM，则所要传递的信息仅需记录一次；而且已经知道部门成员的系统就会给每个人的语音信箱发送一份消息的备份。不仅如此，VM还能告诉发送者谁在什么时间听到了这个消息。对于业务技术员来说，VM也是大有用武之地的，它能让业务技术员和管理人员保持联系从而找到客户需要的下一个服务。

14.5.2 VM系统的大小

一个VM端口一次只能为一个用户提供从PBX对VM系统的访问。因此，如果希望10个用户同时接入VM系统时，就必须有10个端口。所建议的VM系统对于每40个用户就要有一个话音端口。然而，当系统就位后，一旦数据可用，端口的数量是可以调整的。每个端口40个用户是一个非常保守的比例。在任何给定时刻，一个端口只能允许一个用户接入VM。

一个存储容量的简单规则是给每个用户6分钟的存储空间，而且这个数量也能随着用户利用系统的方式的不同而有很大的不同。例如，1000个用户的系统应该至少需要1000/40，即25个端口，而且存储容量为6分钟的1000倍，也就是100小时。

14.6 自动值机员（AA）

1984年，Dytel公司提出了第一个自动值机员系统。它试图取代话务台的话务员，也就是以前的交换台的话务员。当主叫方拨打办公室电话时，就会听到如下录音：“如果是按键电话并且知道对方分机号，请直接拨号；找销售代理，请拨1，等等……”。通常，这样的系统就使用AA，并且在多数情况下与话音邮件系统和其他话音处理设备结合使用。

14.6.1 AA实例

通常使用专用语音交换系统，比如PBX、centrex或按键系统，都会有很多来自CO(Central Office，中心局)的中继线，同时还有很多线路连接到电话机或分机。这种应答呼入呼叫的方法会引起众所周知的“沙漏”效果，如图14-3所示。许多中继线进入话务台并且还有许多线路从这里出去，就像沙子都必须经过沙漏中间很窄的小洞似的，所有进来的呼叫都必须经过话务员的操作。使用DID（Direct Inward Dialing直接拨入电话）中继线和DISA（Direct Inward System Access，直接拨入系统接入）特征就有可能解决这一瓶颈问题，但这还是不够的。

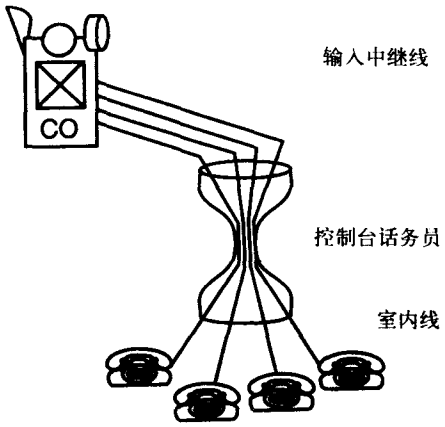


图14-3 由于单个控制台话务员造成的“沙漏效应”

事实上，已经有研究表明在所有呼叫中仅有25%会在第一次连接尝试中成功。正是因为这个原因，为了成功完成一次呼叫连接，话务台话务员必须很多次地处理呼叫尝试。在话务员这一方，失败的次数会在忙时进一步增加，通常是在上午10点到11点和下午2点到3点。

解决这一问题的一种办法是再增加一个话务台，但这就需要再雇佣一名话务员。另一种解决办法是增加更多的DID中继线，但是，这样做不仅会增加成本，而且对于那些需要首先得到分机号码的呼叫者是没用的。

14.6.2 AA的优点

一名话务台话务员一次只能处理一个呼叫，但是AA能够一次处理10个、20个或者50个呼叫。话务台的话务员不得不让所有进来的呼叫不停振铃，因为一名话务员不能同时处理多个呼叫。即使一名劳累过度的话务员在主叫方挂断电话之前的确接听了该呼入呼叫，话务员的服务也未必令人满意。话务员的工作是烦闷而且枯燥无味的。但使用AA之后，进入呼叫在一次振铃后就会被应答，并且他们听到的声音既有礼貌又令人愉快，其原因在于AA系统是不会感到疲劳的。

因此，即使是一位深得上司赏识的精力充沛的话务员，也会因为它而失业。话务员还很容易出现操作错误，比如将呼叫连接到错误的目的地，令主叫方感到失望。

如果外部的呼叫方想在几小时后，并且话务员已经下班后向内部人员传达一些消息，这时，外部的呼叫是不能进入的，只有内部的呼叫者可以向外部发出呼叫。AA系统就能让外部呼叫者直接呼叫内部的设备，根本不需要话务员。即使没有可用DID中继线，外部主叫方也能够直接拨打一部分机。它还允许用户在几个小时之后从外部访问VM。

使用AA，外部的呼叫者能够很快地与单位内部的人员建立连接，特别是在呼叫者知道他们想要的分机号时，连接会建立得更快。AA以较低的价格完成一项乏味的工作。一台价格适度的基于PC的AA系统大约需要10 000美元，这比付给话务员的薪水要少得多，而且AA还能24小时工作。

呼叫是怎么处理的，有多少呼叫连接因为什么原因中断，以及应该增加更多的中继线还是应该减少中继线的数量，这些问题的回答就需要问话务台的话务员了。而现在AA系统就能

够通过统计来提供呼叫管理数据，这些数据很精确，不依赖于任何人的记忆，可用于提高操作过程的效率。

最后，一家小公司的管理人员必须在完成其他任务的同时做话务员的工作。现在，不管是大公司还是小公司，AA都能给外部的呼叫者一个很专业的印象。表14-1概括总结了AA的优点。

表14-1　自动值机员的优点

1. 同时处理多个呼叫
2. 不会被进入的呼叫激怒
3. 主叫方能够控制其呼叫路由
4. 每天24小时服务
5. 快速响应时间
6. 提供呼叫管理数据
7. 不比雇佣话务员的费用高

14.6.3　AA的特色功能

话务员位于任何地方：这一功能可以防止出现空端呼叫。不管主叫方位于哪个话音菜单上面，他都可以通过拨“0”来接通话务员。

呼叫队列：如果许多呼叫者都等待，该功能就会将他们按照呼入的顺序排成一个队列，这样第一个进入等待状态的呼叫就可以首先被回应。

呼叫筛选：要求主叫方立即提供他或她的名字，这些名字被录制下来，之后系统呼叫想要接通的分机，并回放“某某先生/女士在线”。如果被叫方想被接通，只要按下键盘上的一个按钮即可；否则，就按不同的按钮。在这种情况下，被叫方可能会听到类似“某某先生现在还不能立刻接通，但是如果你想与他的助手Back Jack先生讲话，请按1……”等的一段话。利用这一功能时必须非常小心，因为人们更习惯于由秘书来做这件事，而不是机器，况且机器远远不如人有策略。

筛选转接：假设在前面的例子中，“某某先生/女士”请按“1”就被转到助手Back Jack先生那里。如果这是一次筛选转接的话，在让其转到另一方、转到VM信箱或者转到话务员之前，拥有主叫方姓名的系统就会询问Back Jack先生是否想与此人讲话。

监听转接：假设跟前面一样“某某先生/女士”已经按过1，但是现在AA系统在挂断前还要确定呼叫已经完成，并且Back Jack先生也确实应答了呼叫。这样就防止了主叫方听到忙音或回铃音，以及被困在在呼叫路径中。

号簿协助：VM同样支持这一功能。AA系统通过让呼叫者提供姓氏的头几个字母就能向他提供分机号码。

14.7　呼叫分配系统介绍

14.7.1　如何使用ACD

“请不要挂机，现在所有代理都很忙，很快我们将为您提供服务……”。对此我们已经非常熟悉了，这就是ACD的使用。销售价目、全国旅馆连锁、汽车租赁代理以及其他一些应用都使用ACD将进入的呼叫分配给代理商。在ACD环境中，所有代理商处理呼叫的能力都是一样的。当主叫方想要某人为其做一个订单，建立一次预约，或提供一项服务，并且不愿意与某个特定的人建立连接，此时就很有可能通过ACD系统对呼叫进行路由分配。

ACD系统可以作为独立单元购买，或者使用适当的软件也可以将PBX配置为ACD系统。这种独立的单元比PBX的相应部分拥有更高流量并且提供更好的报告功能。目前，BOC（贝尔运营公司）强力推出了基于CO的ACD服务。这对于呼叫中心雇佣那些有残疾的高素质合格

代理或者由于某些原因愿意在家工作的人们有很强的吸引力。由于该项服务是租用的，因此根本就不需要初始投资。在第13章中讲到的Centrex的大多数优点基本上也适用于基于CO的ACD服务。

14.7.2 UCD与ACD的比较

UCD（Uniform Call Distributors，统一呼叫分配器）虽然不能处理大流量业务，但能提供一种ACD的备用选择。它们总是将进入的呼叫分配给同一组代理。在图14-4中，ACD将第一个呼叫发送给第一个代理，将第二个呼叫发送给第二个代理，如此轮流进行，而不管代理1当时是否成为空闲。因此下一个进入的呼叫就被自动路由到空闲时间最长的代理了。

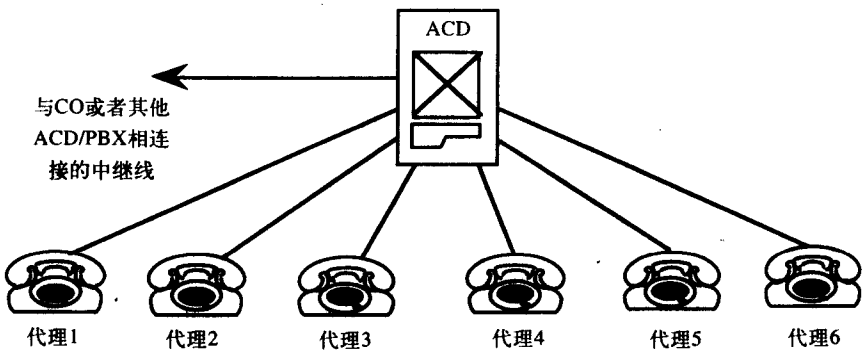


图14-4 ACD为呼入的和呼出的呼叫均匀分配业务量

但是，如果该图中的ACD设备被配置为一个UCD，那么呼入的四个呼叫就会按序列分配给代理1、代理2、代理3，并且如果代理1空闲则又会分配给代理1。按照这样的方法，代理6只有在其他的5个代理都忙的时候才能处理一次呼叫。呼叫的分配与PBX系统在搜寻组中呼叫的分配相同。使用UCD，有顺序问题；而使用ACD时，业务量均匀地分配给各个代理。UCD系统在小一些的办公室里工作良好，那里专门处理进入呼叫的工作人员可以比较少。当呼叫流量比较低时，其余的工作人员就能够处理其他工作，但是在业务高峰期，他们也能很好地缓解流量负载。

14.7.3 呼叫序列发生器

一个比UCD更简单的设备称为呼叫序列发生器或者ACS（Automatic Call Sequencer，自动呼叫序列发生器）。使用呼叫序列发生器时，与代理台相连接的每条线路都有指示灯和按钮。当主叫方进入呼叫等待时，那条线路上的指示灯就会闪烁，并且随着呼叫者在线等待时间的增加，指示灯的闪烁频率就会加快。当有一个代理变为空闲，能应答呼叫时，他/她就会选择指示灯闪烁最快的那条线路。指示灯闪烁最快的那条线路就表示在线等待时间最长的呼叫。

这里的交换智能总起来说就是那些决定按下哪个按钮或下一步应答谁的一组代理，而使用ACD（或UCD），设备就提供了这样的交换智能。

14.7.4 呼叫中心

ACD系统仅仅是一个被称为呼叫中心的一部分。在呼叫中心，有从CO进入ACD的中继线，

ACD为呼叫分配代理。类似地，终端为各代理提供了对主机中数据的访问，参见图14-5。同时，呼叫中心管理员能够监视整个操作过程，并在需要时提供帮助。ACD被用来处理进入的和外出的呼叫。电话销售就是一个将ACD用作呼出设备的例子。

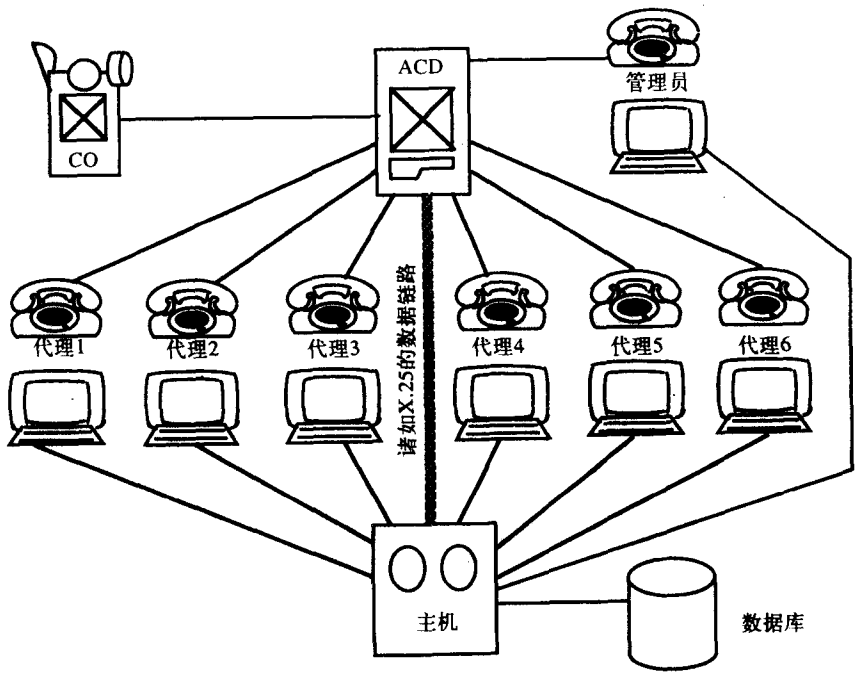


图14-5　ACD仅是一个被称为呼叫中心的一部分

ACD系统首先是由柯林斯无线电公司（Collins Radio）于1973年提出的，当时纽约市大陆航空公司（Continental Airline）的订票办公室需要一个高容量、有专门用途的交换机来处理进入的大量呼叫。后来，柯林斯公司被罗克韦尔国际公司（Rockwell International）收购，今天罗克韦尔已经拥有了独立ACD市场分额的50%，其Galaxy型号的GVS-3000能支持1200个代理。

14.8　呼出电话销售

ACD系统不仅提供向可用代理分配呼叫的方法，而且还提供今天的电话销售所使用的呼出呼叫。电话销售是一种商业类型，代理商可以通过给消费者打电话销售他们的产品或者服务。

快速拨号（speed dialing）是电话销售的雏形。当代理完成了一次呼叫时，“下一个呼叫”按键就被按下。自动拨号机会从数据库中拨打下一个电话号码，代理会听到呼叫过程音，直到有应答或者代理挂机。

快速拨号之后就是比较先进的智能拨号（power dialing）。它包含一个姓名和电话号码的数据库，并且可以预先设置自动拨出这些号码的速率。因为通常情况下，每四个被拨打的电话号码中只有一个被接通，所以智能拨号机进行拨号呼叫的次数比代理数量多，而且只有当在接收端响应呼叫后，呼入的呼叫才能定向到下一个可用代理。拨叫速率是预先设置的并且是固定的。因此，如果建立的连接比预期的还多，系统就不得不放弃一些呼叫。而且，在这种情况下，需要的交换机和中继容量比代理商所能提供的要多。

与这些方法相比较，预测拨号（predictive dialing）采用复杂的数学算法和实时统计来调

整拨号速率。这里，一台拥有客户姓名和电话号码数据库的计算机通过数据链路连接到ACD。当拨打下一个电话时，驻留在主机里的步长算法就会给ACD发出指令。它通过比较ACD发给它的代理统计来决定以多快的速度向ACD发送要拨出的号码。

ACD系统能够检测出远端振铃、无应答、忙音和有人应答之间的不同。振铃、无应答和忙音状况均被返回给主机以便进行下一步动作。这些电话号码都会被存储起来，并自动重新安排回呼。然而，应答呼叫的人会让ACD将呼叫连接到一个代理处，同时将该信息提供给主机。之后，主机就会用被呼叫者的数据更新代理的屏幕。实际上，与其他系统相比，预测拨号系统仅仅使用很少的资源就可以帮助商业企业销售更多的产品。

14.9 为何使用ACD

与PBX系统不同，ACD是能够用来赚钱的设备，是使用该设备的公司不可缺少的一部分。许多商店已经关上它们的大门，正在使用呼叫中心和800电话来开展业务。ACD在呼叫中心起了如此重要的作用，这使得对可靠性的要求非常严格，并且用户也不会介意为每个设备支付1500万美元。

通常，为了让新客户知道他们的产品或者服务，企业必须制作并提高有创意的广告，同时支付供呼叫的电话的广告费用。在赢得一位新客户的费用中，有95%都用在这方面，而只有5%的成本花在包括中继线、员工和设备在内的呼叫中心上。ACD的成本通常只占总开支的1%，错误地管理呼叫中心或者ACD系统不合格都是非常愚蠢的。呼叫中心既能很好地利用以前做广告的成绩，也能让它们变得毫无意义。

呼叫中心给未来的客户提供了公司的第一印象，因为通过广告吸引新客户比保持现有客户更昂贵，所以企业就通过800电话提供卓越的服务，从而让现有的客户满意，这通常是通过ACD来运作的。

ACD的目的就是通过快速处理客户呼叫来为其提供更好的服务。随着应答呼叫时间的降低，客户找其他商家购物的机会就更低了。同时，ACD所提供的报告对于达到这一目标的价值是不可估量的。

14.10 门类

很多情况下，代理商被分成具有不同功能的组，这样的组就称为门类（gate）或划分（split），进入的呼叫会被路由到适当的门类。这些功能组的类别包括销售代理商、供应代理商等等。当ACD接收到呼叫时，这些呼叫就排成一个队列或者是一个等待列表，该队列中的顺序是按它们被接收的先后顺序排列的，就像在银行大厅里客户在等候出纳员为其服务时就会排成一行（或者一个队列）一样。等待时间最长的呼叫首先被连接到下一个可提供服务的代理商。

在ACD系统中，每个门类都有它们各自的呼叫队列，如果在一个门类中的队列太长，即主叫方必须等待很长时间才能接受服务，那么呼叫就会溢出到其他队列较短的门类中。有时，来自某些中继组的呼叫可能比其他呼叫的优先级高，在这种情况下，这些呼叫就要“插队”，进入队列中已经存在的呼叫之前。尤其是在溢出的呼叫被转至其他门类时，就会发生这种情况，因为这些呼叫已经在原先的门类中等了很久。为了处理来自其他门类的溢出呼叫，应该训练代理商向其他门类的客户提供服务。

这就类似于一座桥，有单独的供小汽车和卡车行驶的车道。如果桥上的卡车比小汽车多很多，这时供卡车行驶的车道就会很拥挤，而供小汽车行驶的车道却还是半空。但是，如果允许小汽车和卡车共用车道，那么发生交通堵塞的可能性就会很少。同样，经过交叉训练的代理可以处理来自不同门类的呼叫就会防止主叫进入“永远的等待”。

呼叫溢出到其他门类可以由呼叫中心的管理员来手动处理，也可以被自动处理。自动溢出是通过用两种方式对溢出门限进行编程实现的，其中一种方法是根据呼叫等待时间的长短编程，另一种方法是根据处于等待状态的呼叫数量进行编程。在一个ACD系统中，呼叫从原先门类溢出到其他门类称为系统内部溢出；从一个ACD进入另一个ACD的溢出则称为系统间溢出。为主叫方提供在语音信箱留言、请求传真等可选项也能够减少呼叫队列的长度。

14.11　时间线

1. 网络设置

图14-6中说明了一个进入呼叫的时间线。根据终止于ACD的中继类型不同，建立连接所需的时间是不同的。

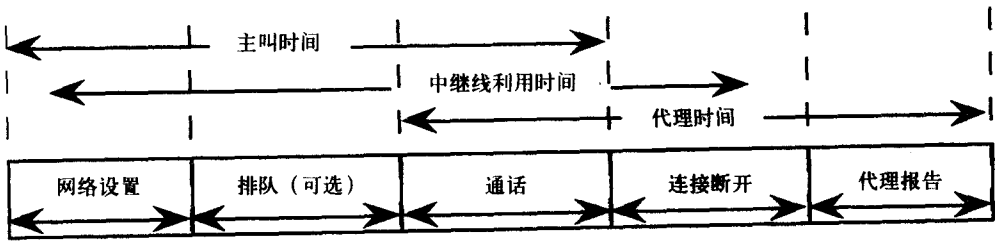


图14-6　表明一个进入呼叫的各呼叫进程的时间线

呼叫中心可以使用WATS中继线来接收进入的呼叫，这时ACD一响应呼叫，就开始计费。如果队列中有呼叫等待，则ACD无需在第一次振铃时就应答呼叫，因为不管怎么样主叫都要先等待一段时间。让电话振铃数次之后再进入在线等待状态就会减少中继线的成本。

2. 排队

排队时间是时间线上的一个重要部分。对于因为在线等待时间太长而挂机的每个主叫方，公司的收益就会较少。大多数人都会在无音乐的情况下等待40秒钟，在有音乐的情况下等待60秒钟。一般来说，通过配置系统都会使主叫方在线等待的时间不超过20秒钟。

当然，随着更多代理的不断加入（同时必须增加更多的中继线），队列的长度就会变得更短，在线等待的呼叫也会变得更少，这是我们在忙时所期望的。但是，在一天的大多数时间里，呼叫中心并不忙，这样就会有更多的代理和中继线处于空闲状态。因此，呼叫中心的管理人员就必须考虑这些问题，从而使得不会因为资源（中继线和代理）不足而引起呼叫的丢失，也不会因为呼叫量不足而浪费资源、增加开销。排队有助于高效地利用代理和中继线，并且ACD报告也为管理提供了调整这些资源数量的数据。

许多呼叫中心保存有数月和数年的历史数据以便预计在商业繁忙的特殊时段所需要的代理数目。

如果ACD与主机集成在一起，并且可以使用ANI（Automatic Number Identification，自动号码识别），那么不管主叫方位于什么地方，这种ANI服务都会为主机提供一种知道主叫方完整电话号码的方式。如果主叫方是老客户，主机就可以在其数据库里查找该电话号码，确定主叫方的身份，并且找到该主叫方的记录。因此，当客户在队列中等待时，主机实际上就在做这样的

工作，从而获得相应的记录。

在呼叫被转接到一个代理的同时，来自主机的数据记录也会出现在该代理的屏幕上。这样就简化了代理的工作，而且能为客户提供更快的服务，从而更快地释放中继线。这就是一个交换-主机集成的例子。如果不能使用ANI，VRU就会让主叫方键入身份证号以便在等待时能提供同样的记录查询服务。

3. 通话

如果平均通话时长为2分钟（这也是一个典型值），那么中继线和代理数目之比应该为1.2：1。对于通话时长仅为5秒的应用，比如信用卡确认等，这个比值可以高达3.0：1，即对于每个在线的代理商来说，有3条可以使用的中继线。

4. 连接断开和报告时间

通话完成之后，在代理一挂断电话而不是等主叫方挂断电话，ACD就能够给CO发出信号要求将呼叫连接断开。这样就可以尽早地为新的呼叫释放中继线。代理也可以在完成与上次呼叫相关的文字工作时按下一个特殊的键，使其不再接听呼叫。

14.12 ACD的特色功能

ACD的功能多达130多个，这里仅仅列出其中一小部分。首先给出一些呼叫处理的功能，之后再给出一些管理信息功能。

1. 呼叫处理的功能

直接向外拨号：不需要话务员的帮助，代理就能发起向外的呼叫。

进入呼叫确认：不管是受话器上还是代理控制台或者终端上的消息都能确定出主叫方的城市或者中继组。这就有助于代理在通话开始之前知道一些关于主叫方的信息。

中继线组的优先级：这使得优先客户或者某些中继线组等待的时间比其他主叫方少。

呼叫强制：该功能允许ACD在代理一挂断电话后就将下一个进入的呼叫分配给该代理。如果没有这一功能的话，代理在结束一次呼叫之后，就要按下一个按钮通知ACD他已经为下一个呼叫做好了准备。

2. 管理信息功能

管理信息报告：对于呼叫中心来说，这些报告与呼叫处理功能同样重要。ACD中可以使用所有类型的报告：标准型、用户专用型；在任何时间段产生的类型（从实时数据和小时报告到年度报告）以及由每个门类、每条中继线、每个代理或每个系统产生的报告类型。

代理级报告：这些报告提供了已经处理的呼叫的数目、平均通话时间，汇报呼叫所花费的平均时间、中断的数量以及其他可以想到的情况。尽管处理更多个呼叫的代理未必能够销售出更多的产品，但他可以为客户提供更好的个性化的服务。

排队呼叫报告：这样的报告详细说明了每5分钟内每个门类在线等待的呼叫数目，还提供了在主叫方被应答之前或者主叫方放弃呼叫（挂机）之前，他所等待的平均时间。

中继线活动报告：这类报告说明了一个中继线组中的所有中继线何时忙，有多少中继线用于呼出，以及频率是多少等等。

14.13 ACD网络

图14-7给出了一个与专用线路连接在一起的ACD网络。被洛克卫尔（Rockwell）称为

RMC（Resource Management Center，资源管理中心）的网络控制中心就是一台小型计算机，网络管理员在这里监督并控制ACD的各种活动。RMC利用X.25型数据链路与所有ACD相连接。这些网络可以由2个到大约20个相互连接的ACD组成，每个交换机服务于一个地区。

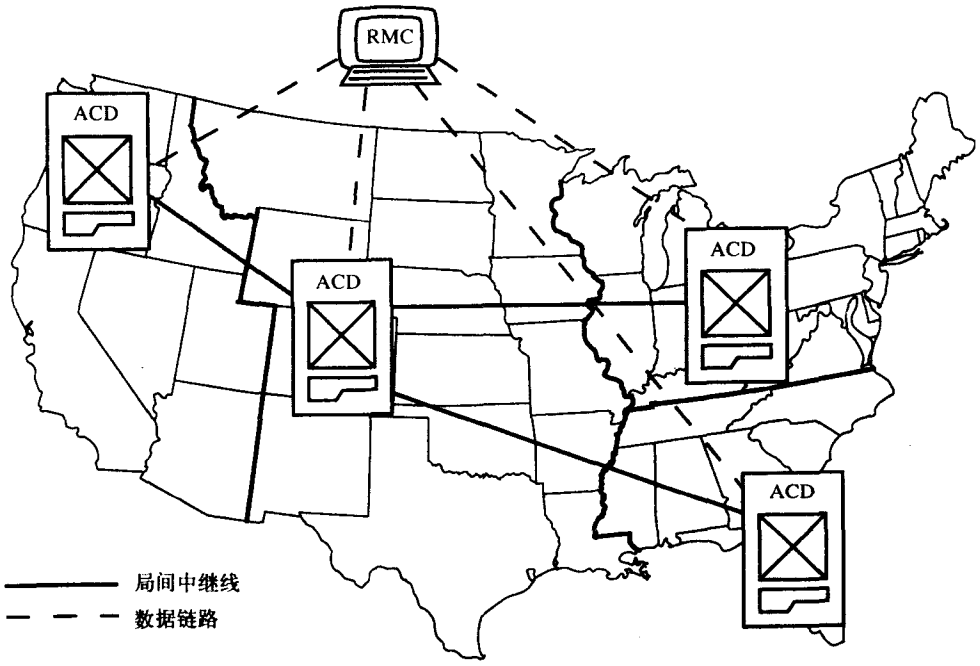


图14-7　一个规划完善的ACD网络看起来应该像一个ACD系统，而不是分立单元

1. 优点

建立ACD网络最重要的原因就是它能够生成包括所有交换机活动在内的一份详细报告。彼此隔离的ACD会产生许多独立的报告，这就需要让人来手工整理这些数据。这会持续数天或数星期。非常希望拥有一份呈给上层管理层的报告。这就为网络管理人员提供了最新的报告，使他们能够据此做出会影响整个呼叫中心系统健康运转的英明决策。

呼叫的溢出和转移是建立ACD网络的另一个重要原因。溢出的意思是说如果一个呼叫中心因为那个地区的产品升级而充满呼叫时，这些呼叫就会自动地被连接到其他负载较轻的呼叫中心。管理人员可以设置服务等级门限。100%的服务等级说明所有的呼叫都正在被应答，没有一个被丢弃的。通常，选择85%的服务负载，在这种情况下，当服务等级接近这个值时，呼叫就会被自动交换到其他呼叫中心。呼叫转移的意思是一个门类或者ACD的所有呼叫都被直接连接到另一个ACD。

卡车和小汽车共享车道的类比适用于从一个门类到另一个门类的溢出呼叫，在这里同样可以适用于呼叫从一个系统溢出到另一个系统。如果10个孤立ACD中的每一个都有500个代理，那么即使其他ACD上的代理空闲，每一个ACD也至多有500个可用的代理。然而，将这10个ACD连接成网络就可以实现资源共享，从而拥有一个包括5000个代理的大型系统。

网络能够将业务量在呼叫中心之间进行分配。如果一个地区由于某种流行性感冒而造成大量代理无法工作，其他中心就可以减轻该中心的负担。网络还可以增加系统的可靠性，这是因为如果一个中心出现故障，则来自该呼叫中心的呼叫就会转移到其他地方。

另一个优点是很容易为中心配备职员提供24小时呼叫服务。使用独立的ACD，每个中心必须全天24小时有人坚守岗位才能提供全天候服务。但是，当建立如图14-5所示的网络后，美国东海岸的代理在下午5点钟就可以回家，因为此时在西海岸才是下午2点钟，那里的代理就能够处理东海岸的呼叫业务。类似地，东海岸的代理上午9点钟上班，他们可以处理西海岸早晨6点钟的呼叫业务。虽然国际ACD网络还非常少，但它们却能比国内的网络更容易提供全天候的服务。

2. ACD网络链路

虽然T1专用线路成本高并且还不如DDD服务灵活，但仍有大约一半的ACD网络在交换机之间的链路上使用T1专用线路。ACD提供直接的T1接口，而不用模拟中继线提供对ACD系统的接入，这是因为模拟中继线容易受到电气噪声和过多的信号电平损耗的影响。

其他ACD网络利用DDD服务在各ACD站点之间分配呼叫，这是通过诸如AT&T的路由控制服务终端这类的终端来完成的。如果一个ACD中心充满呼叫，而其他中心却没有，该终端就会允许网络管理人员从发生变化开始的5分钟之内将800号码呼叫从一个ACD重新转到另一个ACD。这实际上影响了存储用户联网数据的IXC中的SCP（Signal Control Point，信令控制点）。

以前，美国国内不同地区都有它们相应的800号码可拨打，如果ACD需要容量来接收来自其他地区的呼叫，它就需要为每个这样的地区提供独立的中继线组。DNIS（Dialed Number Identification Service，被拨号码识别业务）就避免了必须为每个800号码使用独立的中继线组，因为每个800号码都会有它自己的4位数DNIS码。这样，在进入呼叫之前运营商给ACD发送4位DNIS数字仅需要一个中继线组就足够了。

DNIS通常由4位数字组成，但是公共网络能发送7位。DNIS也能用来识别最初发起呼叫的地区号码或地区号码组。于是，当呼叫进入ACD时，DNIS就会通知ACD这个呼叫从哪里来，该信息还能提供给代理的受话器或者他/她的数据终端。知道呼叫从哪里来就能够适当地选择代理，从而为客户更好地服务。ACD MIS系统和主机数据库也收集这些信息，并用于市场研究。

14.14 交互式语音响应（IVR）系统

从14.13节我们已经知道，呼叫中心雇用代理，这些代理通过ACD接通呼叫并通过主机完成请求或者事务处理。本节介绍这样一种技术，它自动完成主叫方到主机的接口过程而不需要任何呼叫中心代理。

回到图14-5，假定六个代理及其相关的设备被一个IVR设备取代。使用呼叫中心时，在代理利用数据终端与计算机通信的过程中，代理完成了主叫方话音与驻留在数据库中的数据之间的转换。插入到话音中继线和主机之间的IVR系统使得主叫方可以直接同数据库相互作用。IVR允许将主叫方的按键电话用作数据终端，并且由IVR来完成主叫方的话音（包括DTMF脉冲）与主机数据之间的转换。采用呼叫中心时，代理与主机交互工作并且解释其在监视器上所看到的。使用合成语音的IVR 能够“读出”（read off）通常在代理屏幕上所看到的内容。如果主叫方没有DTMF电话机，IVR就能够使用语音识别来解释主叫方的可听到的响应。脉冲音频转换器也能在有限的基础上将拨号脉冲转换为数字。

使用过电话的人要比使用过数据终端的人多得多。IVR使主叫和被叫双方都受益，它为客户提供了更好更快的服务（更少的等待时间），并且大大地节省了公司的开销。

但是IVR不仅仅是呼叫中心的替代，它还能够提供更多的功能。它能够将本章中前面介绍的所有话音处理技术融合到一个单元里。可以使用C语言对其进行编程，但这样会消耗一定的

时间；同时也可以使用应用程序生成包对其进行编程。应用程序生成包使用预写宏（程序代码单元）和菜单帮助用户创建一组IVR的指令，这样，在客户呼入时，就可以得到适当的服务。这些指令可以是给主机的命令，进行信用卡校验，升级数据库，或者其他类似的操作。

IVR使得电话相对于主机来说就是一个数据终端，使主机相对于主叫方来说就是一个代理。一些IVR系统提供了对两种不同类型主机的同时接入，这也是某些应用程序所要求的。

IVR是交互式的，意思是说用户与主机之间可以相互按照对方的要求操作。因此，不仅可以通过主机获取信息，IVR还允许用户命令主机，并且能够给预先授权的厂商划款、付款，或者下订单以及执行其他交易。IVR系统允许大学申请者跟踪他们的入学申请或者允许用户获得一个订单或装运的状态。

14.15 CTI（计算机电话集成）

14.15.1 什么是CTI

在IVR通过先进技术代替呼叫中心代理的同时，CTI也认识到了与人接触的重要性并利用一定的技术来辅助代理和呼叫用户。CTI（Computer Telephony Integration，计算机电话集成）可以使代理的工作效率更高，也使得客户的呼叫过程更加轻松愉快。将语音交换机如PBX和ACD与使用标准的数据库服务器集成在一起可以提高呼叫中心的效率。

当客户将他的地址和个人信息提供给一名代理，该代理又将这次呼叫转接给一个更适合为该客户服务的专业代理时，我们不想让用户向这位新代理重复他的地址和个人信息。当客户拨打呼叫中心并进入等待状态时，我们可以通过ANI（Automatic Number Identification，自动号码识别）从数据库服务器提取他的记录，一旦有代理空闲，就将这一信息显示在代理的屏幕上。在CTI中，这些功能被称作“屏幕弹出”（screen pop）。当客户访问公司的Web服务器并要求立即响应他的问题时，CTI能够实现与呼叫中心的无缝接口。

CTI通过功能和物理上的集成为呼叫中心提供了自动化的操作。这种自动化操作被标准化，从而不仅使大公司可以提供CTI，而且小公司也同样可以提供CTI。当交换机需要向数据服务器发指令或者当服务器需要用几条信息响应交换机时，我们就需要定义一个API（Application Programming Interface，应用程序接口）。API能够使话音交换机和数据服务器彼此相互通信。下面我们介绍一些业界定义的标准API。

14.15.2 标准API

当话务员在PBX控制台接收到一次呼叫时，他可以转接该呼叫或者以很多种不同的方式处理该呼叫。当呼叫正确连接到被叫方后，话务员便会自动从呼叫中退出，在这种情况下，话务员就称为**第三方**。

另一方面，当位于普通电话线上的雇员将呼叫转移到另一个分机上时，该雇员则被认为是第一方。第三方处理呼叫比起第一方处理呼叫具有更多的功能，这是因为第三方直接控制着整个PBX，而一个普通的分机只能控制其电话线所提供的功能。

两种主要的CTI解决方案可以用同样的方式进行分类：第一方方法和第三方方法。第三方方法称为TSAPI（Telephony Services API，电话业务API），它是在1992年由AT&T（现在的朗讯技术公司）和Novell公司正式确定的。朗讯公司（Lucent）在它们的Definity交换机上提供了一个CTI接口而Novell则提供了LAN软件。后来其他的PBX生产厂商与TSAPI合并。在此之前，IBM已经提出了CSA（CallPath Services Architecture，呼叫路径服务体系结构）和为各种

类型的交换机提供接口的DEC。

图14-8a给出了CTI的TSAPI解决方案。呼叫中心代理商的电话与PC没有直接相连。话音和数据路径通过独立的网络被相互隔离开。被称为CTI服务器的专用服务器通过TSAPI接口将LAN连接到话音交换机上。例如，现在有一个向内部的呼叫进入，交换机就会与数据库服务器通信，利用ANI通过CTI服务器提取该客户的记录。

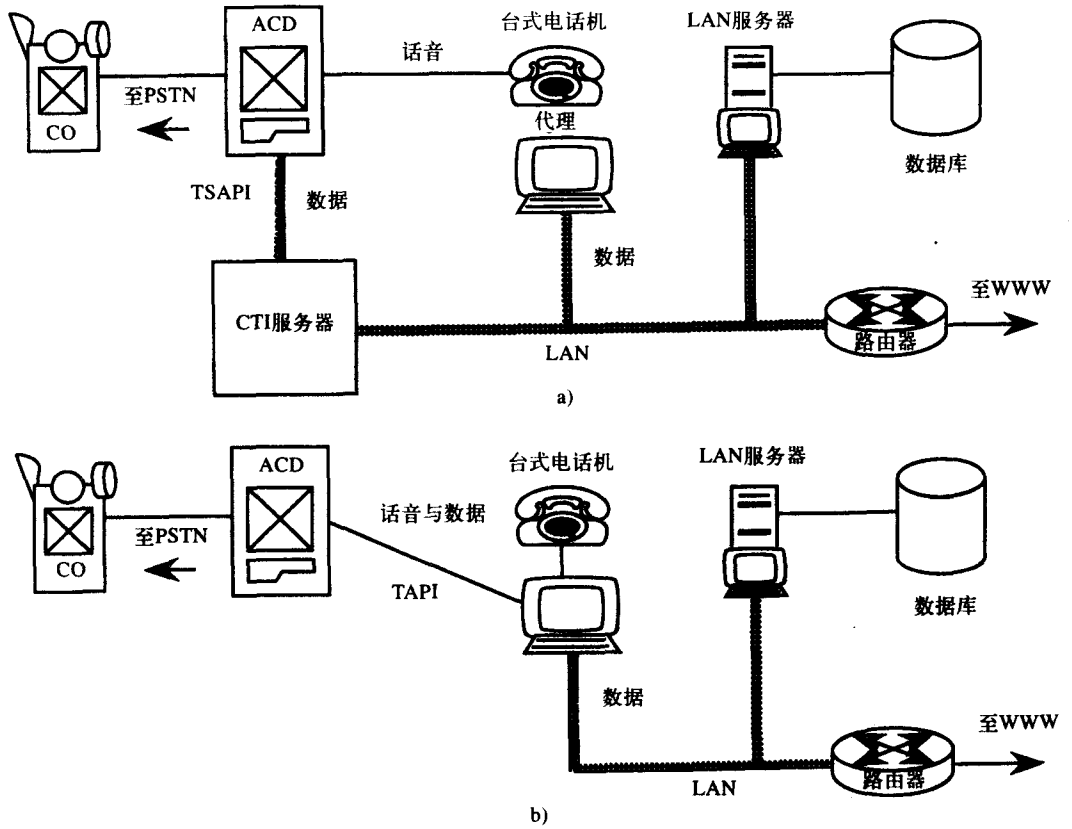


图14-8 a) TSAPI使用控制交换机和数据服务器的CTI服务器，
b) TAPI利用电话线将PC上的CTI应用直接连接到交换机

1993年，Intel公司设计了TAPI（Telephony Application Programming Interface，电话应用程序接口），微软和其他公司也很快加入了这一CTI解决方案。TAPI提供了一种第一方呼叫控制模型，如图14-8b所示。注意，图中没有使用CTI服务器，而且数据库服务器与话音交换机之间的通信是通过电话线来完成的，话音交换机上也不需要特殊的物理接口。话音和数据信号在同一条电话线上传输。Windows程序员可以通过DLL（Dynamic Link Library，动态链接库）访问交换机。为TAPI编写的应用程序只能工作在Windows环境下。

TMAP（Tapi-to-tsapi MAPping，TAPI到TSAPI的映射）可以在一定程度上将TAPI转换为TSAPI，但其自身并不能提供完整的CTI控制。不能与任何一个这样的API竞争的API就称为JTAPI（Java Telephony API，Java电话API），它位于TSAPI和TAPI的顶层，提供多家厂商的可以工作在所有平台上的电话Java小程序（applet）。Sun、Lucent（朗讯）、Dialogic（现在是Intel的一部分）、Intel以及Nortel都是JTAPI的最早开发商。

CTI的其他发展包括1995年ECTF（Enterprise Computer Telephony Forum，企业计算机电话论坛）的成立，S.loo与H.100就是经ECTF标准化的两个重要规范。JAIN（Java Api for Integrated Network，集成网络的Java应用程序接口）是基于JavaBeans架构的，该架构集成了AIN（Advanced Intelligent Network，高级智能网络）、传统的有线和无线网络以及Internet网。

14.15.3 CTI与网站

客户通常通过PSTN呼叫呼叫中心，可能使用的就是800号码。现在客户可以通过企业的Web服务器接入到呼叫中心。在Web页面上会有一个“Call Me”的图标，请求主叫代理用其电话线呼叫客户，而他是通过其数据线连接到公司网站的。当主叫代理和用户同时看同一个“屏幕”时，文本和其他的信息就会很容易地在他们之间共享，这项功能称为网页回访（Web Callback）。

在客户不需要代理通过电话线回呼时，他可以请求建立一个聊天室。在这种情况下，双方可以进行聊天，同时代理在查阅该目录下的相同网页之后，也能够帮助回答客户的问题。当用户没有独立的话音和数据线路时，这种聊天方式是最合适的。

在网页上进行呼叫也是可能的，该项功能利用通过因特网连接来发送话音的H.323标准或者VoIP（Voice over IP）。这样，客户在与呼叫代理通话的同时还能够保持与Web服务器的连接。

习题

将下列语音处理系统与习题1到习题4正确匹配。

a. 话音信箱　b. 自动值机员　c. 语音文本　d. 语音响应单元

e. 交互式话音响应单元　f. 事务处理　g. 语音识别

1. 通过使用键盘，用户能够卖出股票。
2. 通过拨号，用户可以听到预先录制的今天的天气预报。
3. 通过使用键盘，从数据库中选择并提取数据。
4. 如果被叫方不在，则主叫方的消息就会存储在那里。
5. 什么是呼叫处理？
   a. 与话音处理不同。
   b. 与呼叫记录一样，里面保存有呼叫双方、在什么时候进行的呼叫以及通话多长时间的统计信息。
   c. 是一种自动系统，不用人工协助就能处理进入的呼叫。
   d. 是一种将模拟话音转换成数字话音的技术。
6. 下列哪种形式的呼叫分配系统总是将呼入的呼叫连接到某组代理那里？
   a. ACD　b. UCD　c. 呼叫队列器　d. IVR
7. ACD时间线的哪个阶段不包括代理的时间？
   a. 连接断开　b.汇报　c. 排队　d. 通话
8. ACD的哪个功能描述了一天中主叫等待的最长时间？
   a. 呼入呼叫确认　b. 队列呼叫报告　c. 中继线活动报告　d. 代理等级报告
9. 从功能上说，与话音合成相对的是什么？
10. 给出两个信息提供商的例子。
11. 许多呼入的呼叫被几个话务员交换所造成的效果称为什么？

12. 对于400个用户而言，需要多少小时的存储空间以及多少个端口？
13. 自动值机员系统的哪一项功能会记录主叫方的姓名，并且询问被叫方是否应该应答呼叫？
14. ACD首先被用在哪个领域中？
15. 建立ACD网络的一个原因是在原中心充满呼叫时将呼叫转到其他中心，这一特征称为什么？
16. 什么类型的电话销售系统拨打的电话号码比可用代理多，并且不依赖于当前中心的活动？
17. 话音消息为什么被存储在DASD（Direct Access Storage Devices，直接存取存储设备）中？
18. 给出建立VM网络的原因。
19. 给出建立ACD网络的原因。
20. 解释ANI与DNIS之间的不同之处与相似之处。
21. 何谓划分门类？它是如何改进呼叫中心的运行的？
22. 为什么认为IVR系统正在不断地增长，而VM系统则达到一种稳定的发展水平？
23. ACD、UCD与ACS之间有什么区别？
24. CTI提供了哪些IVR所不能提供的功能？
25. 哪种CTI解决方案提供了第三方呼叫控制？为什么称为第三方？
26. 列出几种CTI标准。
27. 你知道哪些已经出现的但本章并未提及的基于网络的呼叫中心功能？

第15章 T1 网络

15.1 优点

15.1.1 节省运营费用

节省运营费用是许多公司转而使用T1网络的唯一原因。T1多路复用器和带宽管理器在每个地方的花销高达100 000美元；然而，电话账单一年之内节省的费用就可以支付这些投资。

15.1.2 简化

T1线路可以使网络简化。在图15-1中，西雅图（Seattle）和明尼阿波利斯（Minneapolis）两地通过单独的线路连接在一起。2个PBX之间需要12条语音线路，4条CAD（Computer Aided Design，计算机辅助设计）线路以56kbps的速率工作，同步终端需要许多9600bps的线路，一组IV的传真线路需要另一条56kbps的线路。

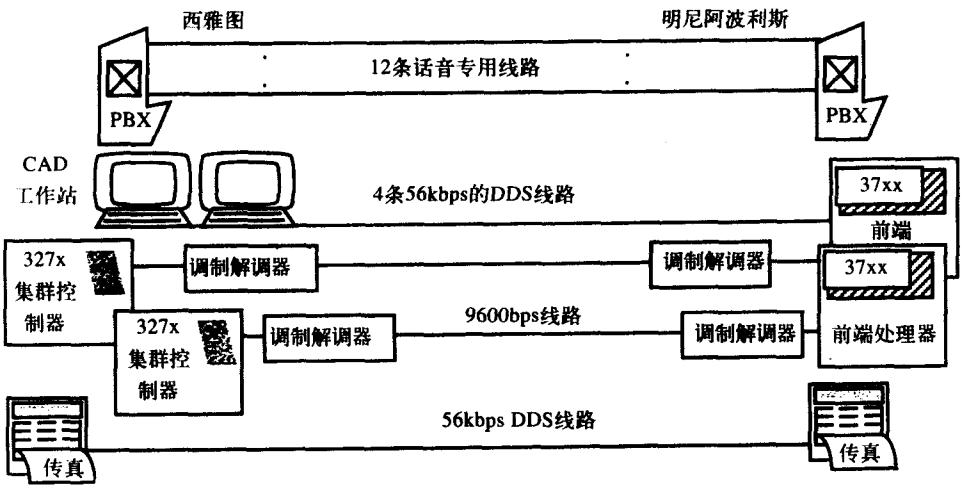


图15-1 各应用的分立线路使得两节点网络难于管理

图15-2给出了如何仅用一条T1来集成相同的应用。这一电路比很多分立电路更易于管理、监视和控制。在这个例子当中，12条话音线路占用12条DS-0（0级数字信号）信道，5条56kbps的信道占用5条DS-0，3条9600bps的信道可以被复用到1条DS-0信道中。这些加起来一共是18（12+5+1）条DS-0信道。将这些信道多路复用到一条T1链路上，该T1链路可以提供24条DS-0信道，其中6条空闲DS-0信道可以留给以后功能扩展使用。以上采用的就是标准的T1格式。如果采用专有格式，每条T1线路甚至可以得到更大的容量。

这里我们仅仅简化了一个两节点网络。试想将15个或者甚至100个节点的网络转化为全T1网络时会得到什么样的简化。我们还可以从简化网络这个优点得到T1的其他优点。

15.1.3 可靠性

管理者们公认，对于大多数网络来说，可靠性要比节省费用重要得多。网络的崩溃会使管理者的能力受到质疑。网络崩溃的每一分钟，收入都在损失，并且很容易超过转换为T1网络所节省的开支。

有人可能会认为，在图15-1中的一个电路的损失不会像图15-2中T1的损失那样严重。然而，要在图15-1中引入冗余的话，所有的电路都需要冗余电路；而采用一个T1时，仅仅需要一个冗余电路。在T1网络中，任意两个节点之间存在许多路由可用，这样如果主路由出现了问题，就可以自动选择一条备用路由来代替。

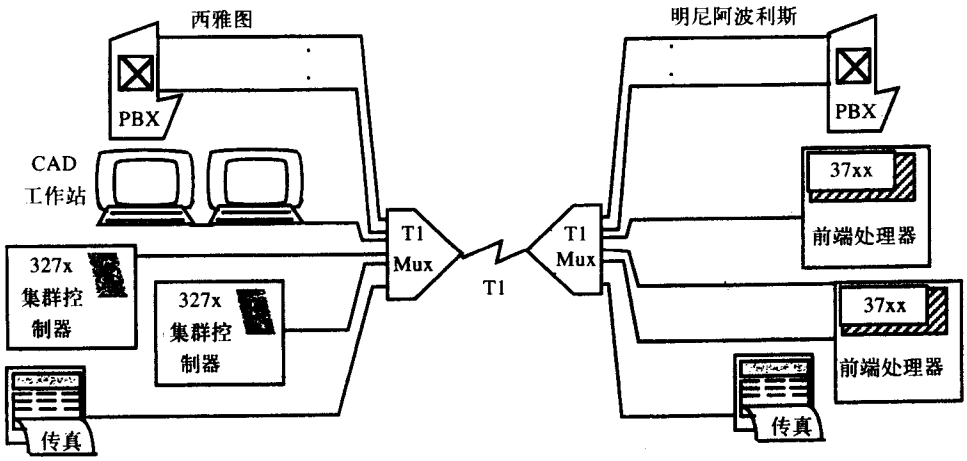


图15-2 将所有应用合并在单个T1上极大地简化了网络

IXC会在你购买T1时提供内置的冗余。此时，如果T1链路中的IXC部分出现故障，该链路会在1秒钟内自动重新建立路由。通常情况下，链路的接入部分最为脆弱，所以应该租用空闲线路或者通过CAP（Competitive Access Provider，竞争接入提供商）或其他方法来探测备用线路。应该记住的是，一旦包含实际使用和空闲线路的电缆被切断，那么很可能两条线路都会被切断。类似地，如果LEC和CAP的电缆通过同一座桥或者地区，那么在相应位置发生的事故将会导致两个接入网络都被破坏掉。换言之，在不同的服务商那里购买备用线路不一定能避免事故的发生。

在图15-3中，如果从A到D的链路出现故障，就可以通过编程使T1多路复用器自动地从节点B和C对流量进行路由。如果备用路由没有足够的容量，则不重要的电路将被“杀死”以便给从A到D的重要电路腾出位置。当然，电路的优先权必须预先确定并编程。

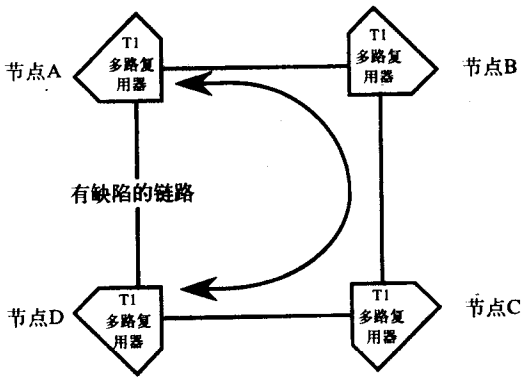


图15-3 网络中有可供使用的备用路径，当链路出现故障时，两节点之间的流量可以自动地重新路由，图中节点A与D之间的流量通过节点B与C进行路由

控制卡、数据交换组件、供电装置以及T1复用器的所有重要部件都应该备份。端口卡不需要备份，除非它们连接的设备也要避

免故障或者它们支持了很多信道。备份的部件如果不进行不断的测试，则需要使用时也可能发生故障。

15.1.4 网络控制

T1网络并不是像雕刻在石头里那样，它们是灵活的并且可以根据需要来改变。这就使网络的使用者对网络有了更大的控制权。某些电路可以暂时被切断以便给视频会议的信道提供带宽。一旦会议结束，网络上的正常通信将被恢复。类似地，在晚上的某个时段，可以自动分配大块的带宽来支持一个数据中心。可以很容易做一个这样的实验，看看分中心的效率是否因为增加终端传输速度而得到提高。如果没有观察到效率得到明显改善，传输速率可以重新配置成网络原先的状态。

通过拥有一个控制管理中心可以获得控制T1网络方面的主要优点。网络操作员再也不需要靠工作人员人工地在正确的引脚上放置一个跨接线来进行环路反馈测试；再也不需要靠远程站点工作人员人工地再接一个电路重新路由到网络的一条分支上。取而代之的是，中心站的操作员可以使用操作控制台发信号来命令T1设备提供环路反馈测试、重新路由信道、获得线路质量统计数字等等。

图15-4给出了从点A到点B、C、D远距离的环路反馈测试是如何执行的。已知路径上T1设备的环路识别码，逐一命令这些设备进入环路反馈模式，然后对它们进行测试来看发射的测试模式是否与收到的模式相匹配。如果到B和C的测试结果都很好，但是到D的测试结果并不好，那么故障应该确定在C和D之间。这样就可以通知故障的责任人而不会在设备生产厂商和运营商之间产生很多争吵。

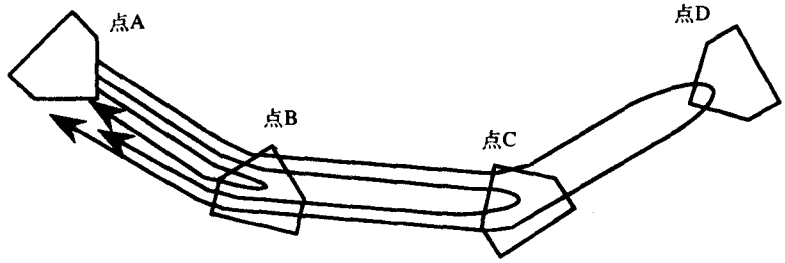


图15-4　从点A起始的远距离反馈环路测试能够协助隔离发生故障的电路，反馈环路测试通常会检查到发射信号格式是否被接收端接收到，在本例中，如果到点B和C的反馈环路良好，但是到点D的反馈环路不良，则故障发生在点C与D之间的链路

回到图15-2中的设置，还剩有超过6条DS-0的带宽可用。所以如果需要安装新的电路，所需的容量已经有了，用户不需要等待运营商为其安装线路。

15.2 T1信号传输

15.2.1 各种介质上的DS-1

最原始的T1电路使用两对铜线双向传输1.544Mbps的信号。这是通过每隔一英里去掉负载线圈后再插入中继器来实现的。一英里是美国城市街道的下水道出入孔之间的典型距离。通过其他介质也可以发送这些DS-1信号速率。每隔40英里需要一个同轴电缆中继器，每隔

30~100英里需要一个光纤中继器。通过微波或者卫星也可以传输DS-1信号。然而，通过上述介质中的任何一种所进行的DS-1速率的传输目前都称为T1。

15.2.2 双极性格式

如果采用如图15-5所示的双极性格式进行信号传输，T1信号在铜线上传输的最大距离可以加倍为1英里，这归功于同步状况的改善。对每个信号来说，双极性方式在+3V和－3V之间改变电压，这种方式也被称为AMI（Alternate Mark Inversion，符号交替反转码）。它提供了一个内置的检错系统。如果某一比特因为错误而丢失，也就是说，“1”被误译为“0”或反之，就会检测到两个连续的相同极性的脉冲，这样它就会标志为一个错误。这种情况称为双极性扰乱（BPV——bipolar violation），因为它违反了变更信号极性的原则。

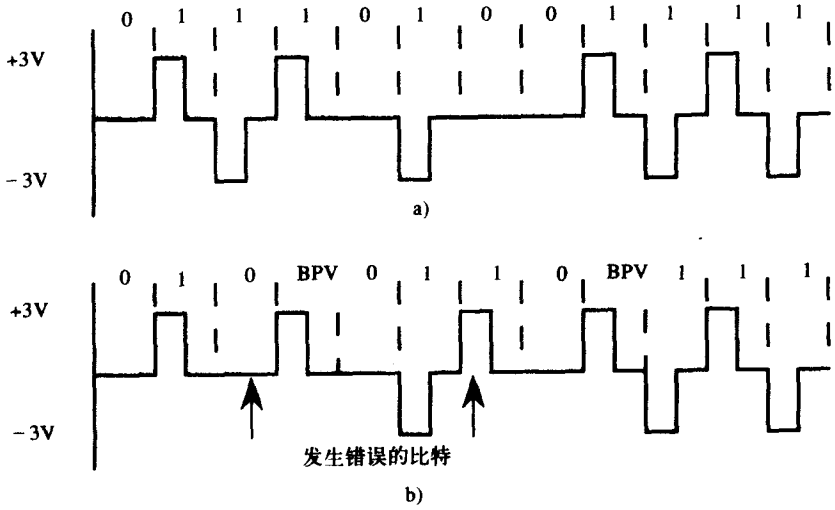


图15-5 a) T1信号的双极性格式要求每个逻辑1的极性与前一个逻辑1的极性相反，逻辑0永远用0V表示。b) 由于线路出错，如果图a)中第二个1误译为0，或者图a)中第三个0误译为1，这两种情况均违反了双极性规则，称之为双极性扰乱或简称为BPV

比如说，在图15-5a中，如果第一个－3V的脉冲丢失了，那么就会在第二个+3V脉冲处发生双极性扰乱，如图15-5b所示。同样地，如果第三个“0”丢失并且变成一个“1”，那么在第四个+3V脉冲处会检测到双极性扰乱。

从图15-5b中我们注意到每个信号都在+3V 或者－3V和0V之间变化。这种变化帮助接收机保持其与发射机之间的时钟同步。因此，T1采用了一种被称为“1密度准则”（ones density rule）的规则来保证接收机是同步的。这个规则要求至少平均每8个比特就有一个1或者说最少12.5%的比特应该是同步标志。

15.2.3 B8ZS技术

图15-6a给出了在数据流中连续发送9个0的情形。这些0不会提供电压极性的变化。有这么多的0，接收时钟可能发生漂移，从而将它们误译为8个或者10个0。为了符合“1密度准则”，这些信号需要一些标志使接收机保持同步。

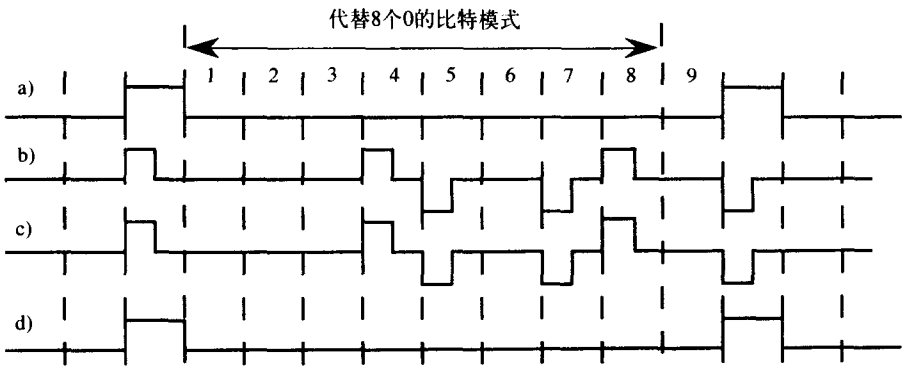


图15-6　a) 被发送到T1多路复用器的具有8个或更多连续0的数据。b) 在T1时间段发送的信号，在第4个和第7个0处插入BPV用以指示全0数据流。c) 发射信号被远处的多路复用器接收。d) 确定第4个和第7个位置处的BPV为连续0指示信号，并将原始数据流提供给终端设备

根据编码方案，数字化的话音不可允许出现8个连续0。可是对于数据来说，长串的0是很可能出现的。我们在后面将看到，56kbps DDS（Digital Data Service，数字数据业务）信道在每8个比特中仅使用了7个比特来传输数据，这样第8个位置就会有一个强制的标志来满足“1密度准则”。

图15-6b给出了执行“1密度准则”的另一种方法。采用这种方法的发射机一旦发现8个连续的0，就会在第4个和第7个0处引入BPV，同时在第5个和第8个0处引入与AMI相兼容的符号。这种编码告诉接收机，这些BPV并不是真正的数据错误，而是代替了数据中的一串0。因此，在将数据送到终端设备以前，接收机会把这种模式变回8个0，如图15-6d所示。这种技术称为B8ZS（Binary 8 Zero Substitution，二进制8零替换），它使得T1网络可以在保持T1设备同步的状态下发送连续的0。

15.3　帧类型

正如第2章和第3章提到的以及图15-7所描述的那样，一个T1信道处理单元接收24路语音信道。采用PCM方式，每条信道每秒钟采样8000次，再对每个采样电平用8个比特进行编码，这样每条信道的速率为64kbps。各路信号速率为64kbps的24路语音电路总共需要的带宽是1.544Mbps。这个速率的计算是将64kbps乘以24后再加上帧同步使用的8kbps得到的。帧结构使得接收设备知道哪些比特属于哪条信道等等。现在让我们看一下这些比特是如何组织或者说如何构成帧的。

15.3.1　D4帧结构

图15-7给出了D4帧结构是如何构成的。这种帧是把24路信道中每路的一个采样信号即8个比特组合到一起，得到192个比特。帧结构中还要使用一个比特以使接收机知道帧结构的起止位置。因此，一个D4帧总共占用193个比特。一个时隙被认为是一个采样点或者8个比特。

需要注意的是，所形成的数据流是字节交织的而不是比特交织的。这就意味着来自信道1的第一个字节放在帧的第一个位置，接下来是信道2中得到的第一个字节，依此类推。比特交织的帧结构首先放置所有24条信道中得到的第一个比特，接下来是所有的第二个比特，依此类推。

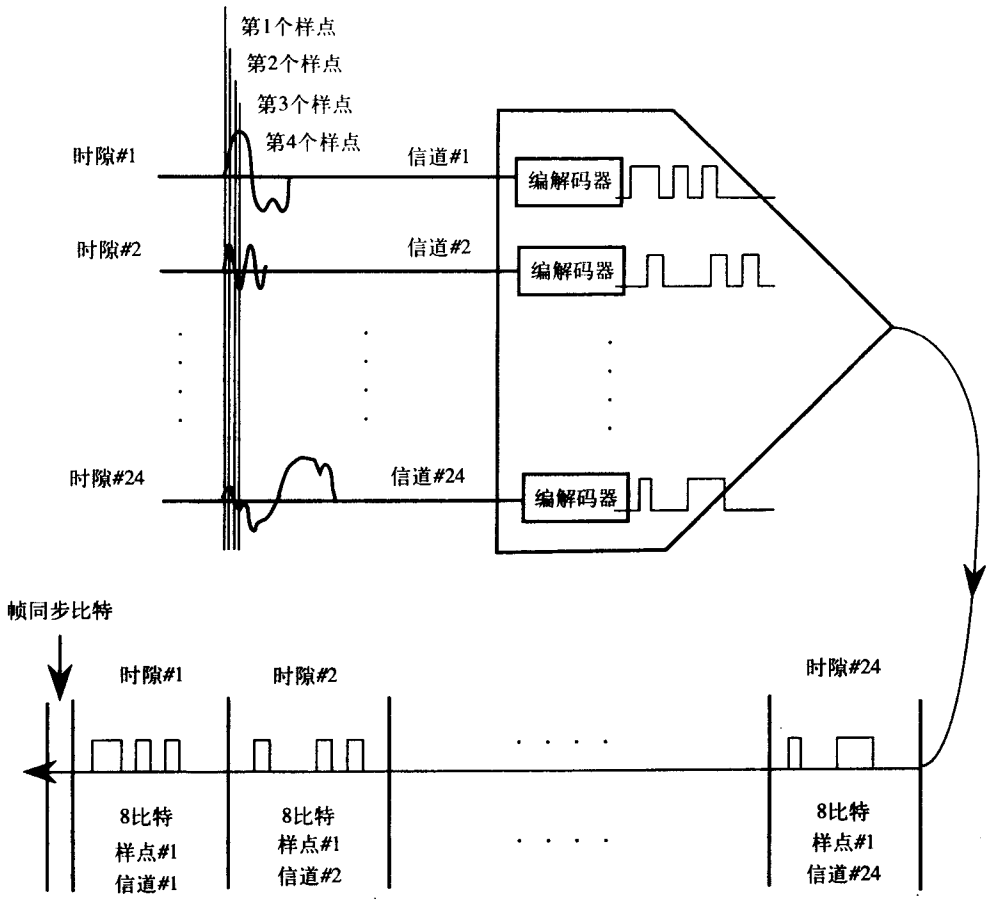


图15-7 T1多路复用器I/O端口的编解码器数字化24路话音信道。在D4帧结构中，来自24路信道的相应8比特样本利用字节交织进行多路复用，连同一个帧比特在内，D4帧结构共需193比特

15.3.2 超帧（SF）

如图15-8中所示，一个SF（SuperFrame，超帧）是由12个D4帧组成的。因此，一个超帧由来自24路语音信道的12个语音样本组成。再加上12个帧比特，得到超帧的长度是2 316个比特。帧比特的内容固定为“100011011100”，它使得接收机知道帧的起止位置。注意到帧比特中的1和0出现时是以1个、2个或者3个为一组的。这些帧比特使得接收机能够封锁帧并且保持逻辑的同步。

每隔6个D4帧的最低比特被用作信道的信令，这一比特最初是来自语音样本，在此被信令信息所替换。正如第5章中提到的那样，这个比特称为盗取比特信令（robbed-bit signaling）。

对于音频（或者视频）信号来说，如果每6个字节损失1个比特，人耳（或者眼睛）是无法察觉的；然而，当数据和话音一起集成到一个T1多路复用器时，我们无法承受任何数据比特的损失，因为数据中的任何一个错误就意味着监视器上出现一个错误的字符，或者在数量错误上作出标记，或是其他诸如此类的不正常现象。

因此，为了在T1链路上传输数据，每个时隙仅仅使用了前7个比特，第8个比特强制设定

为1。这就阻止了数据使用信令比特。于是，DS-0信道的最高数据速率不是64kbps而是这个速率的7/8，即56kbps。这个限制仅仅适用于由经典信道处理单元处理的信号，不包括专有T1多路复用器。

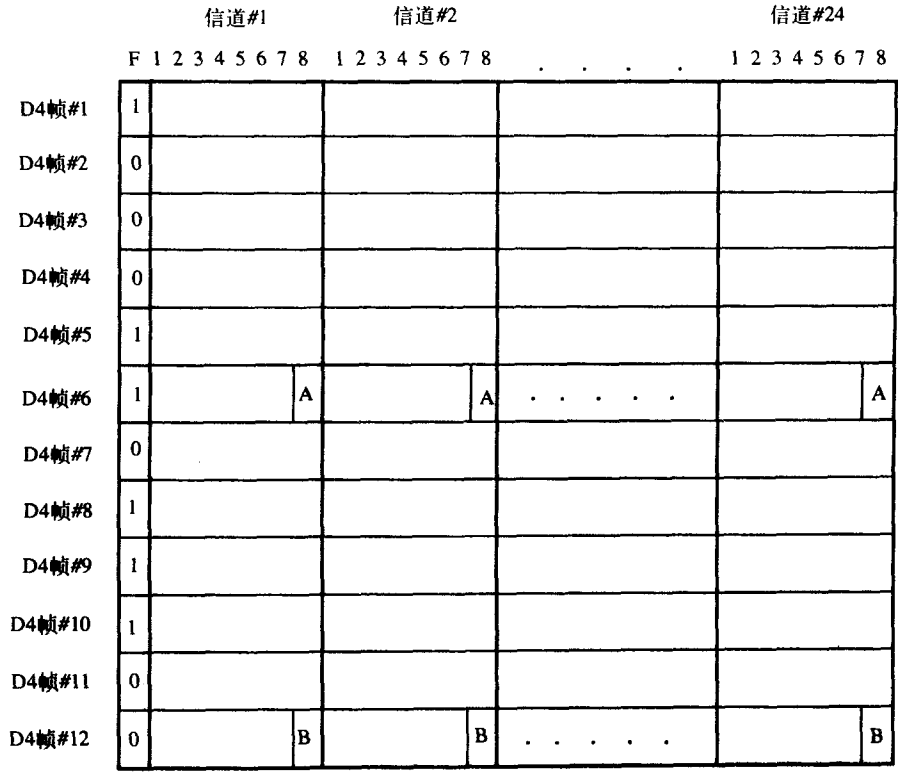


图15-8　一个SF（超帧）由如图15-7所示的D4帧组成，一个SF包含来自24路话音信道的12个样本及帧比特。同时，每6个样本的第8个话音比特被一个信令比特所取代。该比特称为盗取比特（robbed-bit）信令

15.3.3 扩展超帧（ESF）

图15-9给出了一个扩展超帧（ESF——Extended SuperFrame），它的长度是超帧的两倍。它的信令比特不再是每帧每信道2个信令比特，而是4个，用从A到D的四个字母标记。同时，ESF中有24个帧比特，而不是SF中的12个。

在扩展超帧的24个比特中，只有其中的6个被用作逻辑同步，而超帧中使用了所有的12个帧比特。这种超帧结构为其他的应用提供了每帧18个比特的冗余。这18个比特还包含利用CRC（Cyclic Redundancy Check，循环冗余校验）进行错误校验的6个比特。

其余的12个比特用于实现一条称为FDL（Facilities Data Link，设备数据链路）的T1管理信道。根据这些比特在该信道上如何设置，我们可以在流量通过T1网络实时传输的情况下获得线路质量的统计数据。通过FDL传送环路启动码到远端的设备，就可以命令它们进入环路反馈模式。类似地，通过FDL传送环路断开码到远端的设备，可以使它们恢复到正常的服务模式。以上这些功能使得ESF格式成为一种很好的发送T1数据的方式。

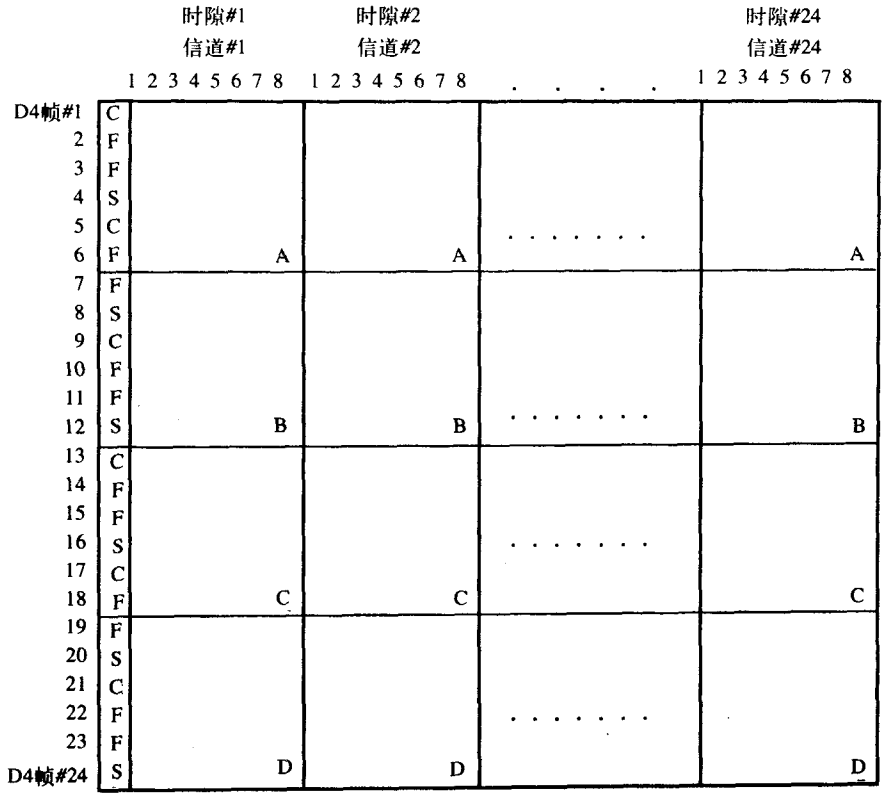


图15-9 ESF仅使用六个“S”比特进行同步，它们是“001011”，“C”比特用于错误检测，“F”比特用于FDL（设备数据链路）信道

15.3.4 其他的帧格式

当T1电路的DS-0在公共网络中交换时，它必须符合D4、SF、ESF的帧格式。但是，如果是专有的T1链路，则用户可以使用任何一种数据格式以获得更高的带宽效率。当然，它的前提是终端设备是兼容的并且对T1网络进行了帧划分。就终端设备兼容而言，一般要求网络由同一个设备提供商提供。**帧划分的**T1网络意味着每隔193个比特必须是一个帧比特，其余的192个比特如何组织完全由用户决定。一个格式化的T1链路也称为划分信道的T1链路或者说DS-1，意味着把一个T1链路划分为24路DS-0并主要用于话音。然而，一个帧划分的T1网络则可以用于传输任意速率（比如256kbps或者768kbps）的信号，只要它符合DS-1的规范。由于限制很少，因此帧划分的T1网络可以很容易地用于很多应用中，包括计算机辅助设计或者视频。

通用的局间音频格式化技术是M44格式。这种为音频设计的格式将44路清晰的话音信号压缩到一条T1链路上，参见图15-10。还有一种M48格式，它是利用盗取比特信令在一条T1链路上容纳48路话音信号。

M44格式将T1的24路DS-0（64kbps）都分成两半，从而产生了48路32kbps的信道。这48路信道划分为4个群，每个群由12条信道组成。每个群包含11路使用32kbps ADPCM编码的话音信道，以及一个32kbps信道，这条信道包含了其他11路信道的控制信令。由于语音比特没有被控制信令盗取，因此这些话音信道被认为是清晰的。要是有人想使用56kbps的数据信道就需要两个32kbps的信道来实现。

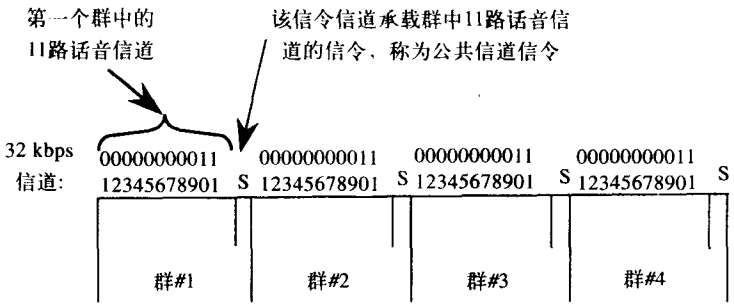


图15-10　M44格式采用ADPCM，各话音信道仅需32kbps的带宽。在一路T1中有48路32kbps的信道，这48路信道划分为4个群，每个群包含12条信道，各群中有11路话音信道和1路信令信道

M44格式使用公共信道信令，这就是说一个公共信道传输了一个群的11路语音信道的信令。由于这些信令和语音分离，信道无法在DS-0进行交换。对于M44格式来说，整个的群必须保证在一起交换。如果必须在DS-0进行交换，M44格式就要转化为其他在话音中包含信令的格式。

15.4　网络接口

15.4.1　客户端

T1范围内客户端的主要网络接口设备是CSU/DSU(Channel Service Unit/Data Service Unit，信道业务单元/数据业务单元)。该设备就是将CSU和DSU放在一个盒子里组合而成。CSU提供了一种得到网络回环（loopback）的方式，而DSU则提供了获得本地回环来检测CPE的方法。CSU还可以阻止网络发送不希望的状态，以及再生输入信号。DSU可以实现单极性和双极性格式的相互转换。

图15-11给出了一条T1链路是如何从中心局CO引入用户的住宅的。在DSU和CSU之间曾经有分界点，这样CO就要通过T1线路来为CSU供电。这使得即便客户端发生电源故障，中心局CO也可以进行回环测试。后来FCC允许客户在设备符合FCC规范的情况下同时拥有DSU和CSU，所以今天的分界点已经移到了CSU的网络端。

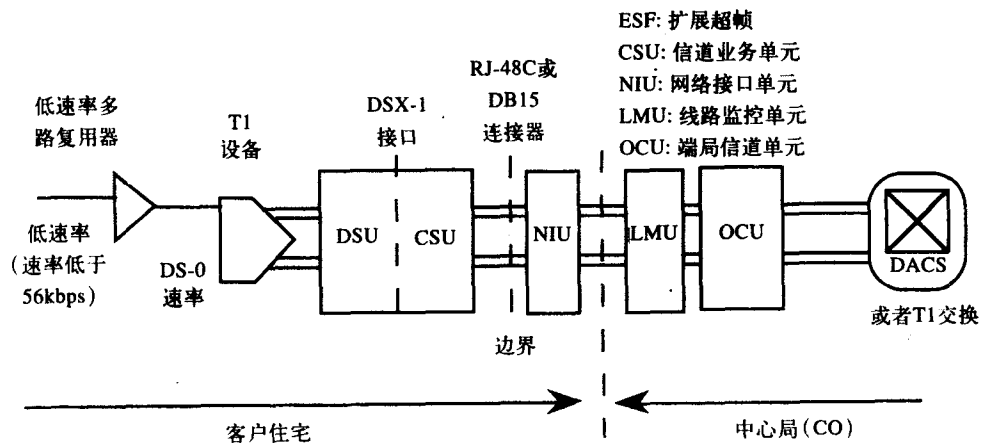


图15-11　T1电路仅需要2对铜线，其中一对用于发射，一对用于接收，本图给出了位于用户住宅和CO的所有T1信号处理单元

既然CSU是靠客户供电的，一些电信公司在客户端设立了NIU（网络接口单元）或者智能插座，从而使其即使在客户无法供电的情况下，也可以执行回环测试。

CSU的功能之一就是在CPE出现故障的情况下保证T1网络的运行。保持运行信号通知中心局CPE出现了故障，并且与电信公司无关。保持运行信号可以是被中心局发现的回环信号，也可以是经过帧划分或未经帧划分的连1数据流。

通常CSU同样负责通过B8ZS技术或其他方法实现“1密度准则”。这也是再生输入信号和显示警报状态的最后一个地方。

15.4.2 电信公司端

OCU（Office Channel Unit，端局信道单元）与CSU类似，不过OCU是位于中心局的。CO利用LMU（Line Monitor Unit，线路监控单元）就可以在OCU和CSU之间进行环路反馈测试。当然，如果T1网络还没有停下来的话，要做这个测试就必须将T1链路停下来。当线路处于活动状态时，LMU可以利用ESF的FDL信道命令CSU提供所需的线路质量统计信息。

15.5 T1网络的交换

15.5.1 信道处理单元、多路复用器和交换机

最初，将24路模拟语音信道合并到一条DS-1中的装置称为信道处理单元（channel bank）。信道处理单元不能复用数据，因为它们主要是话音电路设备。另一方面，T1的多路复用器一般可以接收音频或者数据信号，它们也可以执行低速的多路复用。也就是说，将许多低速的（2.4kbps、4.8kbps等等）数据信道多路复用到一条DS-0信道中。SRDM（SubRate Data Multiplexing，低速数据复用）就是这种技术的一个标准。T1多路复用器可以通过终端进行管理和控制，在终端的信道处理单元则用于更稳定的网络并通过设置DIP交换机进行控制。今天，信道处理单元和T1多路复用器之间的区别正在变得越来越模糊。典型的说法是，信道处理单元比较廉价而多路复用器则更加复杂。带宽管理设备是用于高端T1多路复用器的一个术语。

通常意义的T1多路复用器也被称为M24多路复用器，这种说法是从它们复用的话音信道的数量得来的。多路复用器与交换机的区别在于多路复用器会把输入的T1线路分到24路DS-0信道中，其中各信道与远端对应的信道进行通信。另一方面，T1的交换机可以按任意顺序把信道变换为低于或者等于64kbps速率的信道，于是发送端的任意一条信道都可以和接收端的任意一条信道进行连接。

15.5.2 中间节点交换

如图15-12所示，如果两个T1网络连接着丹佛（Denver）、奥马哈（Omaha）和圣陆易斯（St. Louis）三地，我们将位于奥马哈的站点称为中间节点。丹佛有一些信道的终端在奥马哈，例如信道A，而有一些信道则延续到圣陆易斯，例如信道B。类似地，圣陆易斯也有到达其他两个地方的信道。奥马哈的节点就要负责对来自两端的信道进行分类，或者把它们“卸载”在奥马哈，或者把它们继续传送到“其他”链路上。

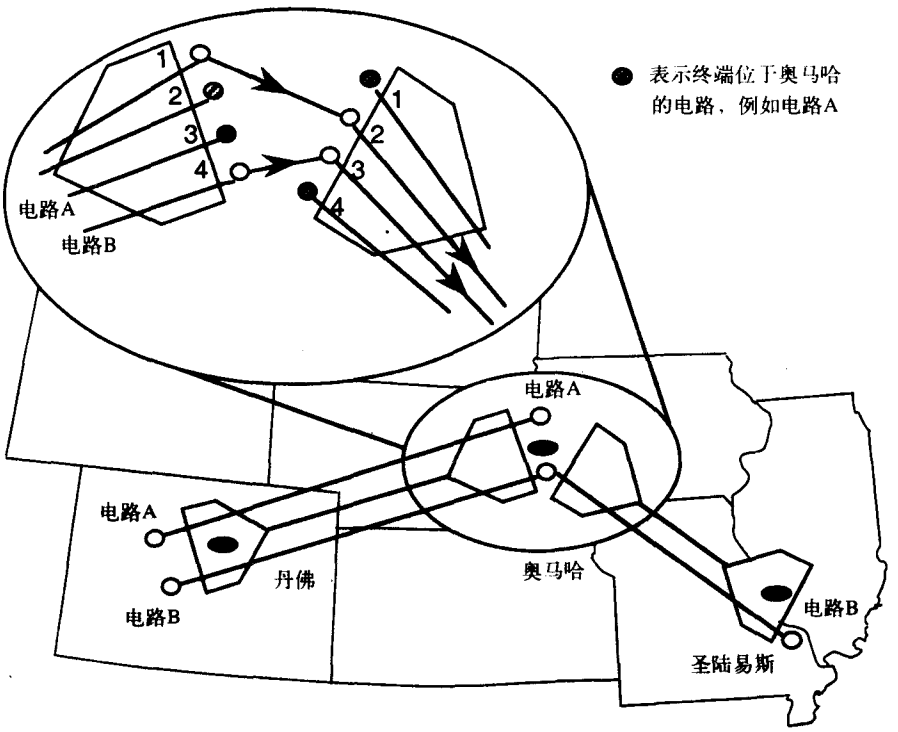


图15-12 电路A从丹佛到奥马哈，而电路B首先在奥马哈“卸载”到信道4，之后再“插入”到通往圣陆易斯的信道3

15.5.3 使用单链路多路复用器的D/I（卸载插入方式）

图15-12示意了使用两个单链路多路复用器的“卸载插入”路由方式。为了简便起见，在该图中位于奥马哈的每个T1装置只显示了4条信道。在这种设定下，所有的电路都被解复用到基带，对信道处理单元来说就是DS-0，而对多路复用器来说就是低速率信道。这些信道可通过多路复用器的I/O（输入/输出）端口直接定向到它们正确的目的地。终端位于奥马哈的电路可以简单地进行卸载，而需要路由到下一跳的电路则必须先进行卸载，再插入到下一个链路中去。例如，图中电路B在信道4进行卸载，然后将其插入到下一个多路复用器的信道3。

这是中间节点最简单的可行交换方式，这种方式有很多缺点。也就是说，所有信道I/O端口的花费将会很贵，但是更为重要的是连接两个多路复用器的电缆所导致的“连线”混乱。而且所有的T1网络都必须使用比特缓冲器同时保持同步。

管理这个节点的电路是件困难的事情，特别是在有两个以上的T1链路需要中继的情况下更是如此。如果某个I/O端口出现故障，就必须人为地拔掉对应的电线，再把它重新插入正确的插孔上。如果两个多路复用器之间的接插线可以用软件控制，那么上面的工作就变得简单，并且可以通过远端的中心站点来完成。

这种网络配置的另一个问题是在话音信道中引入量化噪声。在话音进行数字化时，每个样本都将引入微小的误差，随着话音-数字信号转换次数的增加，量化噪声就会变得明显。在图15-12中的话音电路B将经过两次话音向数字信号的转换（分别在丹佛和奥马哈）和两次

数字信号向话音的转换（分别在奥马哈和圣陆易斯），这种转换也称为D/A/D（Digital to Analog to Digital，数字-模拟-数字）转换。一个话音信道在没有任何衰减的情况下通常可以经过3个到5个这种卸载-插入节点。上述分析假定采用PCM。当话音信道的数据速率降低到64kbps以下时，衰减就会变得更加严重。

15.5.4 添加-卸载

添加-卸载设备也被称为D/I多路复用器，如图15-13中的奥马哈处所示。这种网络配置在逻辑上与图15-12类似，不同点是这种配置不再由两个背靠背的多路复用器分别连接两条T1链路，而是由单独一个多路复用器连接两条T1链路。

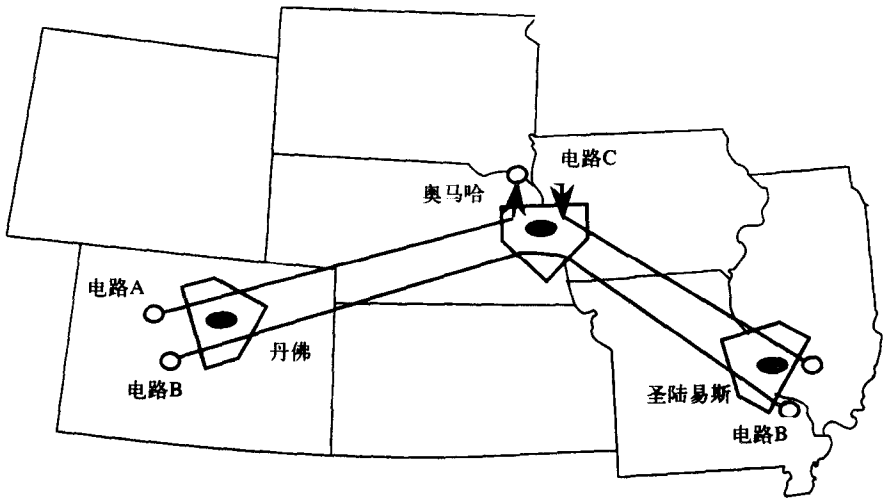


图15-13 奥马哈有一个添加-卸载型多路复用器，来自丹佛的电路B简单地经过这里到达圣陆易斯，而未进行解复用。电路A在奥马哈被卸载而电路C则在那里被添加（这些均为真正的双向电路）

来自丹佛的单个信道B在奥马哈通过这种设备时没有再进行信号的多路解复用和多路复用。因此，经过的信道不再需要I/O端口。而且，由于数据比特在进入该节点后紧接着就发射，因此没有引入量化噪声。

15.5.5 DACS(数字接入和交叉连接系统)

对传统的私人租用线路来说，终端是固定的。在图15-14中可以看到这样一条语音级的专用线路，它通过三个城市在CO和POP处的分布结构从丹佛到达圣陆易斯。如果线路需要重新布线以使它连接圣陆易斯和明尼阿波利斯，则在相应的POP和CO处的技术人员就不得不通过它们的分布结构改变跨接线，从而建立新的线路。这将会花费几天的时间来完成。

对于T1网络来说，将CO和POP处的分布结构和大量跨接线取而代之的是一种称为DACS（也可以缩略为DCS）的可以由软件控制的分布结构。现在，只要在明尼阿波利斯的站点和它的CO有连接，电信公司的操作员几乎可以马上通过一台终端通知位于奥马哈的DACS将T1网络交换为从圣陆易斯到明尼阿波利斯的连接。用户真正地体会到了私人T1网络中使用这种“电子接线板”所带来的灵活性。同时，通过使用DACS也会使灾难恢复计划变得容易实现，因为通过DACS可以按需要使用带宽。

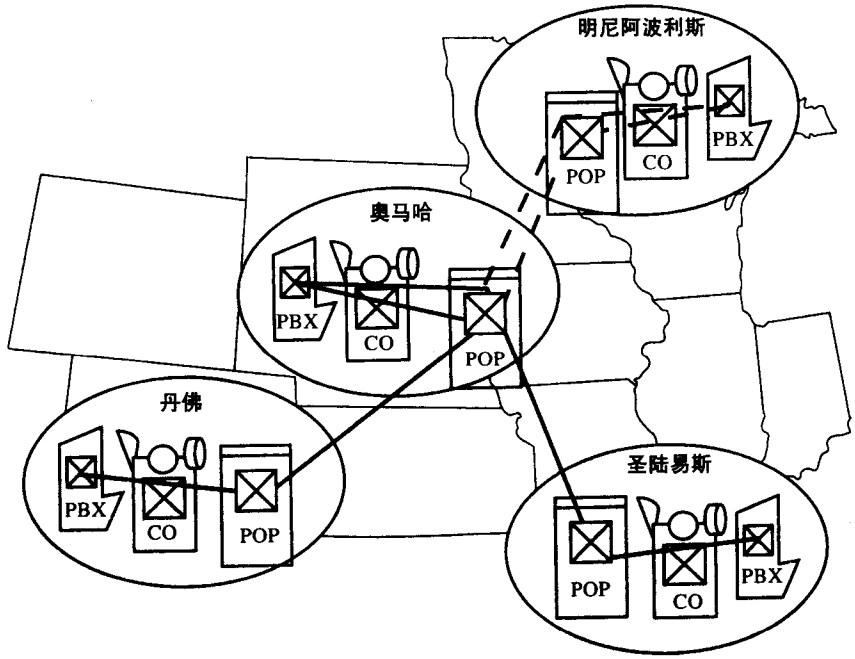


图15-14　实线表示安装从丹佛经由奥马哈到达圣陆易斯的话音级专用线路必须利用位于所有CO、POP和客户处的分布结构。如果该电路需到达明尼阿波利斯而非圣陆易斯，则虚线表示位于分布结构处的跨接线必须安装在奥马哈的POP以及明尼阿波利斯的所有三个地方

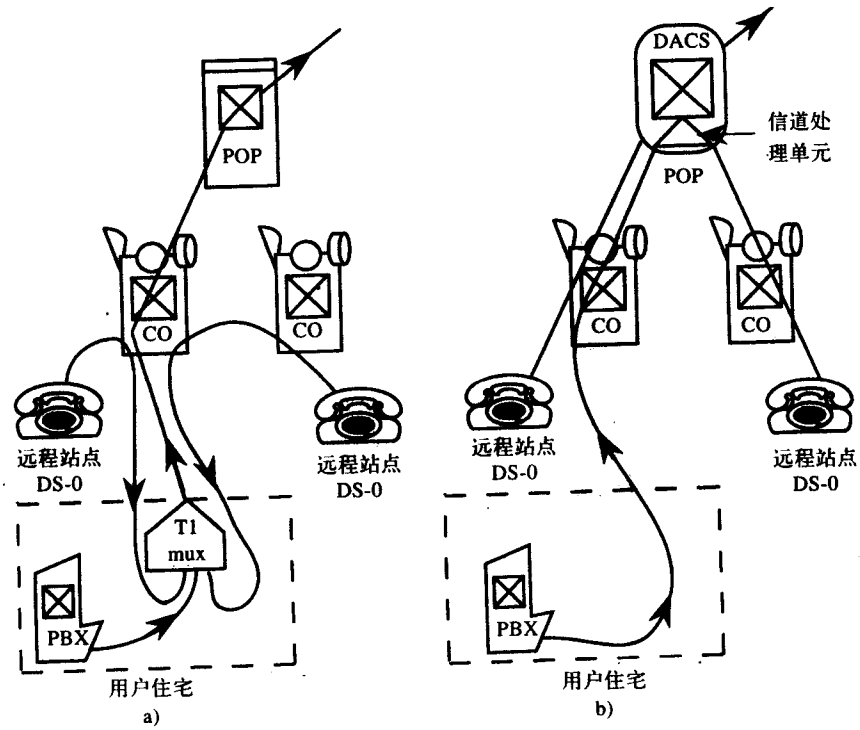


图15-15　a) 未采用DACS时，为了将所有远程站点线路多路复用到一路T1线路上，必须将它们都引入用户住宅。b) 采用位于POP的DACS和信道处理单元后，无须上述要求

DACS不仅仅可以在DS-1级，也可以在DS-0级进行电路交换。如图15-15a所示，如果一个用户在LATA中有很多远程站点，每个站点需要一条DS-0信道，那么如果没有DACS的话，就必须将所有这些DS-0信道连接到用户的住宅，在那里这些信道将会被复用，然后将复用后的信道组发送到目的地。然而，使用DACS情况就不一样了，用户无须购买T1设备，可以将这些DS-0信道直接连接到POP，在那里这些信道会被集中然后发送出去，如图15-15b所示。

由于DACS的关系，因此私人网络没有长时间处于“固定”状态，现在它已经演化为“云”或交换网。

15.5.6 专有网络与DACS

然而，DACS确实存在一些缺点。通过FDL信道的带内信令不能控制DACS。事实上，DACS破坏了FDL比特，使它们对终端用户不再有用。DACS控制器需要一个单独的信令网络，这样，集中式管理系统就能够进行监视和控制。当需要输入或者修改网络映射关系时，必须由技术人员通过使用DACS控制系统来进行输入或修改。与通过带内信令信道改变T1多路复用器的配置不同，DACS要由终端用户通过独立链路进行控制。

DACS也不能交换速率低于64kbps的信道，因此，当一条话音信道速率为32kbps的M44 T1链路必须通过一个DACS时，该T1信道必须转换为两个24路信道的T1信道。当然，两个T1网络之间总共只能分配44路信道。这种类型的转换是通过BCM（Bit Compression Multiplexer，比特压缩多路复用器）来实现的。

通过DACS的交换可以由透明连接或者逐个信道来实现。在透明连接中，一个超帧中的D4帧未必按照顺序排列，但是超帧使用了D4帧的一种不同顺序进行重新装配。这使得通过DACS的延迟保持为两个字节的时间。逐个信道的DACS连接保留了每个超帧的内容，可是这将使得通过DACS的延迟长达48字节的时间。

DACS主要用于电信公司，在专用网络中它的大部分缺点将不会表现出来，因为在专用网络中使用的是专用的信道交换多路复用设备。例如，Timeplex公司的Link100可以交换400bps粒度的信道，这就意味着，DACS交换信道的速率可以以64kbps增加，而Link100交换时可以以0.4kbps的速率增加。DACS不允许带内信令，而专有的多路复用器提供这样的功能。

15.5.7 CCR

AT&T在新泽西州的Freehold有一台计算机，控制着公司遍布于全国的所有DACS。其他的公司也有类似的设备。通过安全分级，用户可以通过拨号或者直接接入这台计算机来改变他们的网络设置。利用自己住宅中的终端，用户就可以按需要重新配置网络，而无须等待电信公司来完成这项工作。AT&T称这项服务为CCR(Customer Controlled Reconfiguration，客户控制下的重新配置)。MCI称这项服务为“数字重新配置服务”。

由AT&T提供的一个更为复杂和昂贵的服务称为BMS-E(Bandwidth Management Service-Extended，带宽管理扩展服务)。它比CCR的重新配置速度甚至更快，还可以为客户提供AAR（Automatic Alternate Routing，自动替换路由）、性能监控、话务量测量和自发测试等功能。

所有的运营商都在发展管理系统，使得它们的客户能够更多地接入公司的设施。虽然这些系统为专用网络提供了附加的控制，但是这也引起了人们对公共网络基础设施安全性和稳定性的关注。

15.6　网络设计案例研究

15.6.1　问题陈述

让我们看一个关于T1主干网络设计的简单案例的研究。

图15-16给出了堪萨斯城（Kansas City，下面简称为KC）某连锁零售商店的公司端局和主数据中心。除堪萨斯城外，还有6个远端站点。如图15-16所示，全国还有4个其他地区的配售中心有其相应数量的商店或远端站点。亚特兰大（Atlanta，下面简称为ATL、AT）除了作为一个地区中心以外，也是一个备份数据中心，它的数据是主数据中心的备份，以防堪萨斯城的数据中心遭遇故障。

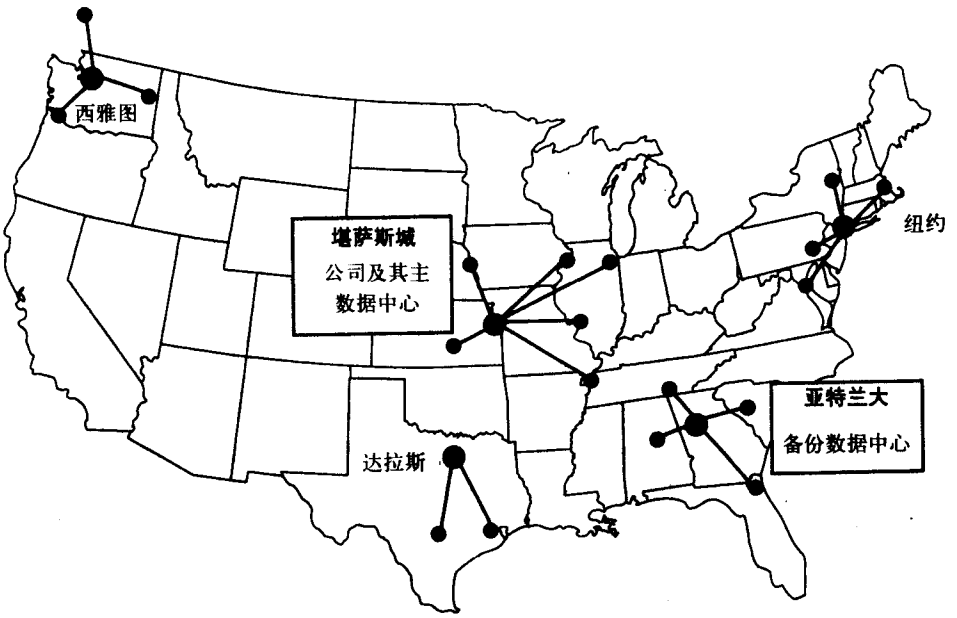


图15-16　来自周围站点的话务量集中到4个地区中心和堪萨斯城的一个公司中心，数据中心位于堪萨斯城，其备份位于亚特兰大，我们将建立一个T1骨干网络以支持这些接入网

话务工程部已经进行了广泛的话务分析，得出的需求如表15-1和表15-2所示。表15-1的第一行表示我们需要7条从堪萨斯城到亚特兰大的56kbps信道、3条从堪萨斯城到西雅图（Seattle，下面简称为SE）的56kbps信道、3条从堪萨斯城到达拉斯（Dallas，下面简称为DAL）的56kbps信道、3条从堪萨斯城到纽约（New York，下面简称为NY）的56kbps信道。从堪萨斯城到亚特兰大不需要9.6kbps的信道，但是从堪萨斯城到西雅图、达拉斯和纽约各需要5条9.6kbps的信道。类似地，从亚特兰大到西雅图、达拉斯、纽约都各需要3条56kbps和5条9.6kbps的信道。

表15-1　地区数据需求

起/止	亚特兰大	西雅图	达拉斯	纽约
KC 56k	7	3	3	3
KC 9.6k	0	5	5	5
ATL 56k	0	3	3	3
ATL 9.6k	0	5	5	5

表15-2 地区话音需求

起/止	KC	AT	NY	SE
Atlanta(亚特兰大)	40	—	—	—
New York(纽约)	0	25	—	—
Seattle(西雅图)	5	3	2	—
Dallas(达拉斯)	11	9	7	1

对每个商店的数据要求是如下9.6kbps的线路：2条到堪萨斯城，2条到亚特兰大的数据中心，5条到它对应的地区配售中心。这些信息在表格中没有给出，但是所有这些数据需求在图15-17中以图形的方式总结出来了。

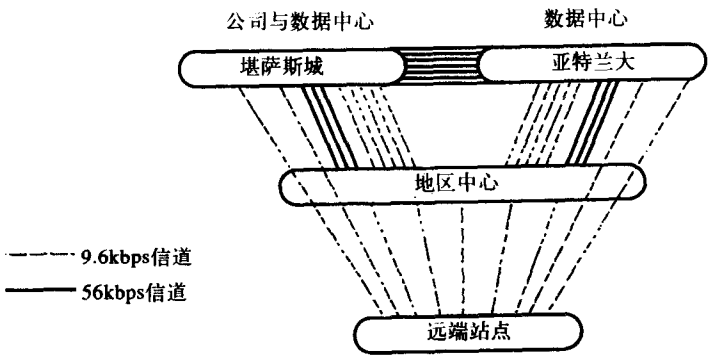


图15-17 该图总结了案例问题的所有要求，从每个远端站点都有2条9.6kbps的线路分别通向两个数据中心，5条9.6kbps的线路通向相应的地区中心，3个地区中心的每一个都有5条9.6kbps和3条56kbps的线路通向两个数据中心

表15-2给出了话音信道的需求。从亚特兰大到堪萨斯城需要40条，从纽约到堪萨斯城和亚特兰大分别需要20条和25条信道，等等。表格的一半为空是因为相应的数字已经在表中别的格子里提供了。远端的商店不需要语音专用线路。

15.6.2 分析

表15-3给出了使用上面所列的数据需求从纽约的各商店到它的地区中心以及到亚特兰大和堪萨斯城需要的9.6kbps线路的数据需求。例如，从纽约的4个商店（用NY1到NY4表示）到纽约的地区中心需要5条线路，到亚特兰大和堪萨斯城各需要2条线路，参见图15-17。

表15-3 纽约的9.6k需求

起/止	AT	KC	NY
NY1	2	2	5
NY2	2	2	5
NY3	2	2	5
NY4	2	2	5

表15-4给出了西雅图商店的3行数据，因为那个地区共有3个商店。类似地，在达拉斯仅有2个商店，因此表15-5关于达拉斯的数据仅有2行。

表15-4　西雅图的9.6k需求

起/止	AT	KC	SE
SE1	2	2	5
SE2	2	2	5
SE3	2	2	5

表15-5　达拉斯的9.6k需求

起/止	AT	KC	DAL
DAL1	2	2	5
DAL2	2	2	5

注意到在关于亚特兰大的表15-6中，尽管对应4个商店它有4行数据，但它仅有两列：一列对应亚特兰大区，一列对应堪萨斯城的公司端局。对于亚特兰大区的每个商店，我们需要5条9.6kbps的线路连接地区中心，2条9.6kbps的线路连接备份中心。因为对亚特兰大来说地区中心和备份中心是相同的，所以总共需要7条这样的线路。

表15-6　亚特兰大的9.6k需求

起/止	AT	KC
AT1	7	2
AT2	7	2
AT3	7	2
AT4	7	2

同样的道理，表15-7所示的堪萨斯城的商店也只有两列：一列是到亚特兰大，一列是到堪萨斯城。

表15-7　堪萨斯城的9.6k需求

起/止	AT	KC
KC1	2	7
KC2	2	7
KC3	2	7
KC4	2	7
KC5	2	7
KC6	2	7

为了设计出骨干网络，现在让我们将所有的流量需求简化到DS-0级。在此之前，让我们先假定使用PCM编码，这样每个话音信道需要64kbps。对于56kbps的信道，我们也需要使用一条DS-0。最后，因为一条DS-0典型情况下传输的最大数据率是56kbps，所以它不能支持6条9.6kbps信道（9.6kbps乘以6是57.6kbps）。因此每条DS-0只能承载5条9.6kbps的信道。

表15-8依据两个城市之间的DS-0总结了总的数据需求。首先，让我们看一下在堪萨斯城和亚特兰大之间的需求量11是怎样得来的。从表15-1中可以看出，需要7条56kbps的信道。同样地，根据表15-6，亚特兰大的每个商店到堪萨斯城需要8条9.6kbps的线路；从表15-7看出，堪萨斯城的每个商店到亚特兰大需要12条9.6kbps的信道。这两个城市之间总共需要20条9.6kbps线路，因为每条DS-0只能支持5条9.6kbps的信道，因此，所需信道可以简化为4条DS-

0。于是，根据7条56kbps线路需要7条DS-0，20条9.6kbps线路需要4条DS-0，得出两个城市之间总共需要11条DS-0。

表15-8 DS-0数据需求

起/止	KC	AT	NY	SE
Atlanta(亚特兰大)	11	-	-	-
New York(纽约)	6	6	-	-
Seattle(西雅图)	6	6	0	-
Dallas(达拉斯)	5	5	0	0

让我们考虑一下纽约和亚特兰大之间的需求，根据表15-8，应该是6。从表15-1的第3、4行看出，我们需要3条56kbps的线路和5条9.6kbps的线路。这样得到纽约地区中心需要4条DS-0。

看一下表15-3，从这些商店到亚特兰大需要8条9.6kbps的线路，所以额外需要2条DS-0；再加上前面由表15-1得到的4条DS-0，总共需求是6条DS-0，如表15-8所示。

表15-8中的其他数字也可以类似地计算出来。注意到纽约、西雅图和达拉斯之间没有需求，所以就没有DS-0。同样地，注意表15-3中全是5的最后一列，并不包含在表15-8中。这最后一列的5是到纽约中心所需要的带宽总数，并不通过到其他城市的骨干网络，而开始两列的2是通过骨干网的，所以包含在表15-8中。

最后，表15-9给出了传输话音和数字所需的DS-0的总需求。这些数字是通过将表15-2（话音的总需求）和表15-8（数据的总需求）中对应的项加到一起得到的。比如说，在亚特兰大和堪萨斯城之间，根据表15-2传输话音需要40条DS-0，根据表15-8传输数据需要11条DS-0，所以得出共需要51条DS-0。

表15-9 总的DS-0需求

起/止	KC	AT	NY	SE
Atlanta(亚特兰大)	51	-	-	-
New York(纽约)	26	31	-	-
Seattle(西雅图)	11	9	2	-
Dallas(达拉斯)	16	14	7	1

15.6.3 设计

这个案例问题的下一步骤是根据每条T1 中有24条DS-0来设计网络图。表15-9用于这个过程。我们首先从表中较大的数字开始设置T1链路，这样在亚特兰大和堪萨斯城之间我们首先需要2条T1来容纳51条DS-0。还有3条DS-0（51－24×2）需要路由，所以我们在这条链路上标上3。参见在图15-18a中堪萨斯城和亚特兰大之间的连接。类似地，按照先满足大数需求的原则，图15-18a中给出了其他的链路，其中链路上标出的正数表明还需要路由的DS-0的数量，负数表明空闲可用的DS-0的数量。

举例来说，当在堪萨斯城和达拉斯之间为其16条DS-0放置T1时，还有8条空闲的DS-0可以使用，所以在那条链路上标上－8。通往西雅图的速率可能会比通向其他城市的速率高，所以我们希望限制通向那里的链路的数量。

在满足了图15-18a中所示的链路之后，表15-9中记录的9、2、7、1仍然需要在网络中加以考虑。下一个需要考虑的最大数字是亚特兰大和西雅图之间的9条DS-0。

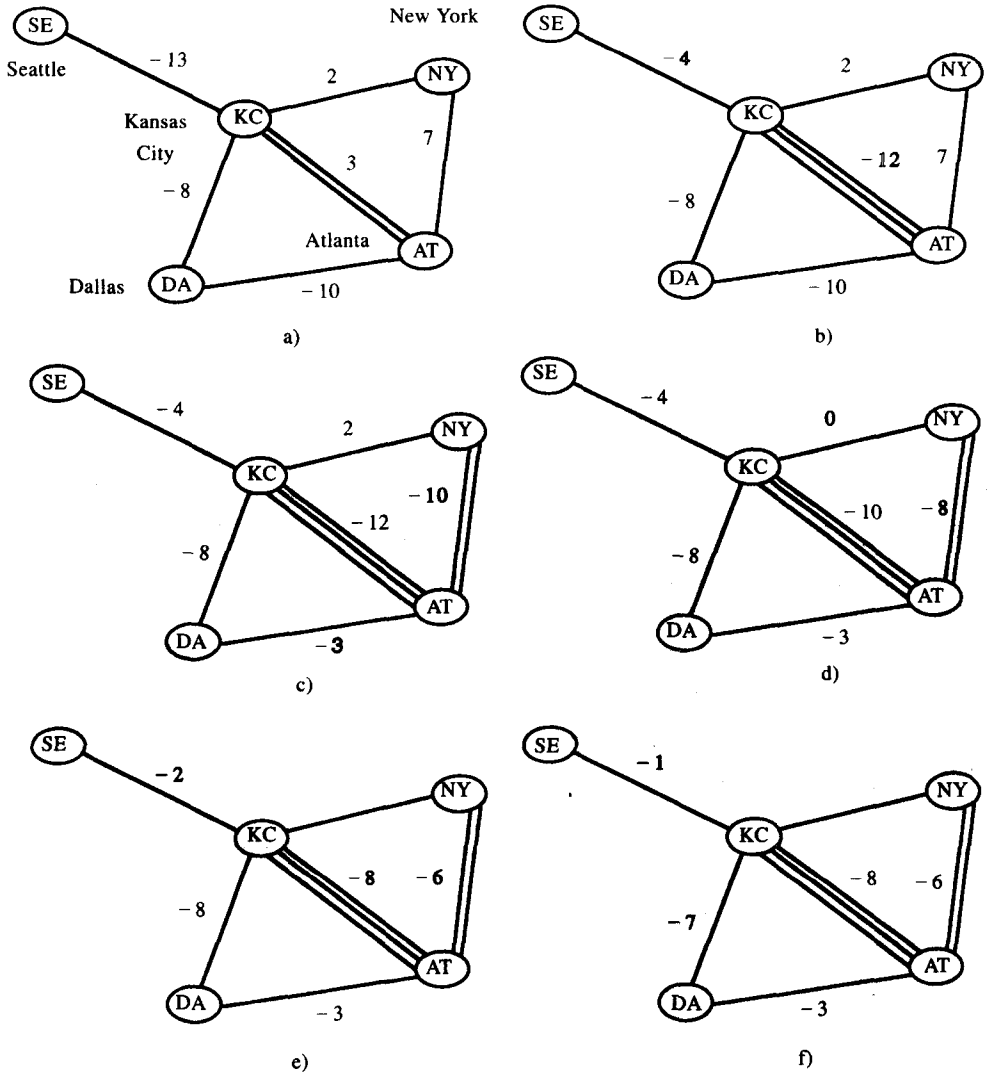


图15-18　链路上的正数表示仍需满足的DS-0数量，负数表示空闲的DS-0数量。从前一个图得到的各链路的新值用粗体表示。a) 初始设置；b) 增加从西雅图到亚特兰大的9条信道，注意增加了另一路T1；c) 增加的另一路T1增加了从达拉斯到纽约的7条信道；d) 将纽约与堪萨斯城之间的2条信道重新进行路由；e) 从纽约到西雅图增加2条信道；f) 最后，从西雅图到达拉斯增加1条信道

让我们在堪萨斯城和亚特兰大之间放置第三条T1链路，如图15-18b所示。如图15-18a所示，现在两个城市之间的3和连接到西雅图的额外的9占据了第三条T1链路中的12条DS-0。还剩余12条空闲。对于堪萨斯城到西雅图的链路，来自亚特兰大的9条信道需要连接到西雅图。所以，现在堪萨斯城到西雅图的空闲信道的数量从13减少到4。

如图15-18c所示，满足纽约和达拉斯之间额外7条DS-0的方法是在纽约和亚特兰大之间增加一条链路，然后路由7到达拉斯。这就使达拉斯和亚特兰大之间的空闲DS-0数量减少到3。此外，在图15-18b中纽约和亚特兰大之间还需要路由的7条信道加上连接到达拉斯的7条信道

在新的T1链路中占据了14条DS-0，剩余10条空闲，结果如图15-18c所示。

图15-18d给出了图15-18c中的纽约和堪萨斯城之间经过亚特兰大路由2条DS-0以后剩余的空闲信道的数量。图15-18e给出了由表15-9在纽约和西雅图之间经过亚特兰大和堪萨斯城增加所需的2条DS-0之后的网络图。最后，图15-18f给出了由表15-9在达拉斯和西雅图之间经过堪萨斯城增加1条DS-0之后的网络。

15.6.4 补充的设计问题

这里得到的最后网络未必是最佳的解决方案，也可能存在其他更好的答案。有经验以后，你就可以进行方案的优化。然而，这里还是应该强调一些重要的概念。一是没有考虑T1的税费，应该在设计网络之前获得这方面的材料。在纽约和堪萨斯城之间的链路全部用掉了，而通过亚特兰大的链路还有富余的容量。为此，链路之间的话务量应该平衡，并且应该有一对DS-0通过亚特兰大来连接。

如果使用ADPCM或者其他的话音压缩技术代替PCM，则整个设计将需要重新考虑，从而得到可观的节约。我们也将T1网络假定为格式化的或者信道化的。如果它们进行了简单的帧划分，我们就不需要将网络设计为DS-0组的格式，比如说每个DS-0需要容纳5条9.6kbps的信道。

最后，如图15-18f中所示的最后网络，我们在两个城市之间建立一个有富余的T1网络将会增加网络的可靠性和遭遇故障后的恢复能力，这是因为网络有更多的路径可以用于路由信道。有富余的T1网络在灾难性打击后受到的损失将会比满负荷的T1网络要小。

习题

1. 传输T1信号时需要多少对双绞铜线?
   a. 1　　b. 2　　c. 4　　d. 都不是；普通的线不能用于传输T1信号
2. “只需要一条电路而不是很多种”说的是下面哪个优点?
   a. 花钱少　b. 简化　c.可靠性　d.网络控制
3. 什么是双极性格式?
   a. 使用两个电平：+3V和0V
   b. 每个符号用与前一个符号相反的电压极性（+3V或者－3V）进行编码
   c. 所有的空位用－3V编码，所有的符号用+3V编码
   d. 所有的空位用0V编码，所有的符号用+3V编码
4. 一个D4帧在每条信道中包含多少8比特话音样本？对应多少路话音信道?
   a. 一路话音信道包含24个样本
   b. 一路话音信道包含1个样本
   c. 12路话音信道中的每一路包含12个样本
   d. 24路话音信道中的每一路包含1个样本
5. 哪种T1接口设备能进行单极性向双极性的转换?
   a. NIU　　b. DSU　　c. CSU　　d. LMU
6. 什么是多链路的多路复用器?
   a. 有许多输出端的多路复用器
   b. 有许多端口的多路复用器
   c. 被很多DACS使用的多路复用器

d. 一个和很多多路复用器连接的DACS

7. 什么设备将44信道的T1线路转换为2个22信道的T1线路?

a. DACS

b. BCM

c. 反向多路复用器

d. CCR

8. 下面哪一项不是DACS的缺点?

a. 透明交换需要T1信号延迟48字节

b. 用户不能通过带内数字信令进行控制

c. 不能在64kbps以下速率进行交换

d. 不能保持D4帧的顺序相同，并且仍然获得最小的延迟

9. 为了满足视频会议的需要，可以通过暂时放弃一些信道来改变T1信道的带宽，这揭示了T1的哪项优点?

10. 就可靠性而言，通常T1网络的哪个部分是连接最脆弱的地方?

11. 如果传输的数据是“110001000000000000100111”，第一个“1”是+3V，那么这些比特转换为输出信号后的电压应该是多少?（有连续12个0的数据串）

12. 百分之多少的超帧传输了帧同步比特?那么对扩展超帧又如何呢?

13. 在客户端无法供电的情况下，电信公司使用哪个单元来进行回环测试?

14. 哪种多路复用器可以将话音信道从一个链路转到另一个链路上而无须进行D/A/D转换?

15. 在POP处，什么设备可以用来将远端的DS-0信道结合起来?

16. 在表15-8中，解释在堪萨斯城和达拉斯之间DS-0的数量5是怎样计算出来的?

17. 在列出的T1的所有优点中，你认为哪一个是最重要的?为什么?

18. 双极性格式的意义何在?它是如何实现的?

19. 解释FDL信道的意义?它建立在哪里?除了文中提到的功能，你还希望它支持哪些功能?

20. 解释图15-11中各种接口的意义。

21. 和其他方式相比，列举一下采用单一链路的多路复用器实现卸载-插入方式的缺点。

22. 列举一下DACS和CCR的优点。

23. CSU提供哪些功能?

24. 使用文中讨论的技术来设计下面的T1网络:

在这个练习中，洛杉矶（Los Angeles）是总局，而波特兰（Portland）、盐湖城（Salt Lake City）和丹佛（Denver）是地区局，丹佛和洛杉矶是两个数据中心。所有的4个城市都有3个销售局或是远端站点，总共12个销售局。

数据需求如下：每个销售局到LA局需要两条9.6kbps的线路。每个地区局到LA需要10条9.6kbps的线路。每个地区局到两个数据中心分别需要一条56kbps的线路。两个数据中心之间需要4条56kbps的线路。

话音需求如下：从丹佛到LA要有23条话音信道。从波特兰到LA和丹佛分别需要7条和3条话音信道。从盐湖城到LA、丹佛和波特兰分别需要15条、6条和2条话音信道。

画出话务量矩阵并像例子所示的那样设计网络。画出最后得到的网络图并在每条链路上标出空闲的DS-0数量。正确的答案未必是唯一的。

第三部分 广 域 网

第16章 SNA（系统网络体系结构）

16.1 SNA环境

SNA是IBM公司在1974年提出的，它是消除当时存在多种类型的网络协议所导致的混乱的一种专有解决方案。现在它已成为世界上40 000多个网络中最具影响力的网络结构，而附着在这些网络上的工作站的数目实际上已远远超过了这些。在详述SNA体系结构、协议及其如何实现之前，我们先大致介绍一下SNA及其目的。

16.1.1 SNA的初始应用

图16-1显示了地域上分散分布的一些终端，它们通过网络连接到一台主机（host），该主机在IBM术语中称为大型机（mainframe），它位于公司数据中心。举个例子来说，它用于为班机代理提供一个数据库访问。

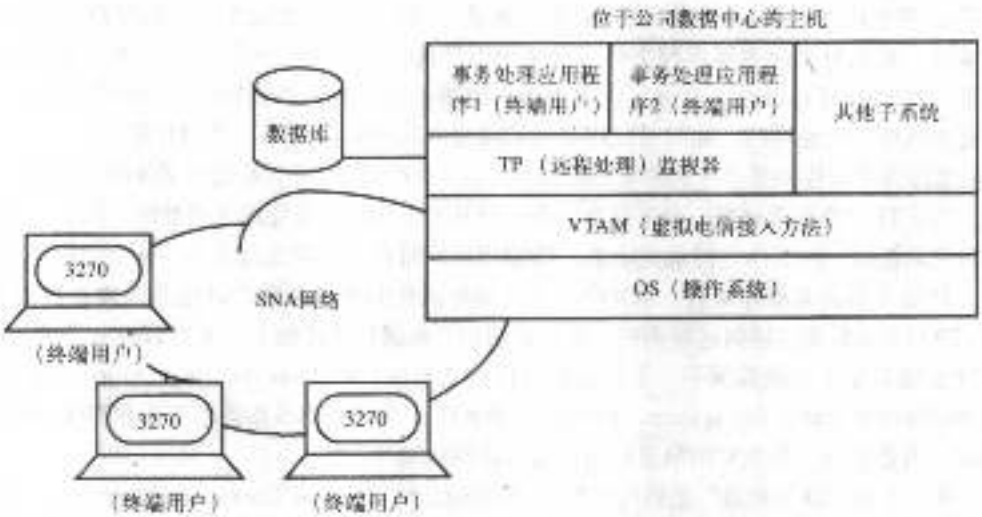


图16-1 SNA网络的高层视图，其中突出了网络的终端用户

数据库是一个复杂的、有组织的数据记录的集合，这样就可以高效地完成对那些数据记录的访问。IBM的两个流行的数据库管理系统称为IMS（Information Management System，信息管理系统）和DB2（DataBase/2，数据库/2），其中，IMS是一种传统方法，采用的是分层的方法管理数据，该方法使用父-子型或相反的树型结构。而DB2采用的是关系数据库的结构，其数据按照逻辑关系排列在表中。

例如在远端，终端可能是具有数据库访问权限的旅行社代理，这些代理会向数据库发出处理请求，称为事务处理。这些请求可能是申请一个指定日期特定班机的座位，或者请求取消一个预订，或者是提出一些询问等。这些由全国的许多旅行社代理发出的数据库请求由一个称为事务处理的程序进行处理。在访问数据库之后，这些应用程序就给代理商发送一个回复，说明是否可以满足请求。和代理商相互作用的这些应用程序与代理商一样都是SNA网络的用户，因此，这些应用程序也被称为终端用户。

虽然这个SNA最初是如何实现的非常微不足道，但是现在SNA已经演化为一个更为成熟的网络体系结构。它可以支持诸如文件传送、分布式处理、分布式数据库以及电子邮件等复杂的业务。

16.1.2 主机的远程处理

现在让我们简要地描述一下主机的主要软件组件，这些软件在主机处理来自远端的事务应用程序时会用到。如图16-1所示，它们是操作系统、VTAM(Virtual Telecommunication Access Method，虚拟电信接入方法)和TP(Tele Processing，远程处理)监视器。

主机本身由操作系统管理和控制，它负责安排所有的工作并管理所有的资源。MVS（Multiple Virtual System，多虚拟系统）是IBM主机上最常使用的操作系统。与AT&T公司的UNIX不同，MVS并没有设计成在网络上处理通信；这其中的部分原因是其复杂程度和大小。因此，MVS需要VTAM来处理与通信相关的任务。之后，VTAM再与一个TP监视器相接，在TP监视器控制之下进行事务处理。现在各种类型的TP监视器无须处理通信程序，因为这些功能是由VTAM模块提供的。

两种常用的TP监视器是：CICS(Customer Information Control System，用户信息控制系统)和IMS/TM(Information Management System/Transaction Management，信息管理系统/事务管理器)，其中IMS/TM以前也称为IMS/DC。如果应用程序直接在操作系统而非TP监视器的监控下执行，那么每个应用程序都需要一个单独的存储分区或者地址区，这将使得操作系统负载加重。TP监视器通过在一个分区内管理所有的事务可以极大地减轻操作系统的负担。这样可以使主机更高效地运行，同时可以用高效的流水线完成软件应用程序的开发。

就像操作系统控制整个主机和资源的操作一样，TP监视器控制着处理事务的事务处理应用程序。由于TP监视器通过在一个存储分区内运行几个应用程序来完成上述处理，因此，操作系统认为它只在做一件工作。但是实际上，TP监视器同时在做几项处理工作。从应用程序的角度来看，TP监视器就是操作系统，从VTAM或者操作系统的角度来看，TP监视器就是应用程序，因此VTAM必须首先连接到远端用户，然后远端用户根据其选择建立一条与TP监视器的连接。

TP监视器是子系统的例子；子系统的其他例子包括TSO(Time Sharing Option，时间共享选择)和JES(Job Entry Subsystem，任务项目子系统)。TSO和JES都是不工作在TP监视器下的子系统，但是必须工作在VTAM等电信接入方法的环境下。

目前，术语“TP监视器”也被用在基于UNIX的OLTP（Online Transaction Processing，在线事务处理）系统中。这些TP监视器与客户机/服务器系统集成在一起，客户机/服务器系统最初是为少数客户机工作站提供关系数据库的。与诸如CICS等传统的TP监视器相比，这些系统提供了更好的性价比和GUI（Graphical User Interface，图形用户界面）。与基于客户机/服务器的数据库系统相比，TP监视器可以支持大量的同时发生的事务，可以提供对传统数据的接入和更好的安全性。

16.2 SNA的硬件

到目前为止，我们主要讨论了主机，并对连接终端和主机的SNA网络进行了很少的介绍。

就传统而言，SNA是具有定向的、分层的网络，网络中的设备都是被其他设备控制的，并最终受到主机的控制。

而现在SNA变成了一种所谓的“平面”网络，终端对主机的依赖性越来越小。这个新的快速变化的体系结构称为APPN（Advanced Peer-to-Peer Networking，高级对等网络）。但我们在这里仍然认为SNA是一种分层网络，并且在本章的最后讨论一下目前的趋势。现在让我们来揭示图16-1中的SNA云图，看一看在下面的图16-2中SNA网络所用到的典型硬件。

16.2.1 主机及其I/O通道

在图16-2左上角的是SNA中的主机。在纯分布式环境中，任何一个智能工作站也可以称为主机。基于系统370的主机家族包括30xx、43xx和93xx系列。在产品命名中的字母“x”用不同数字替代时表示其他相关的型号。例如，30xx标识包含型号3090、3080和3030。

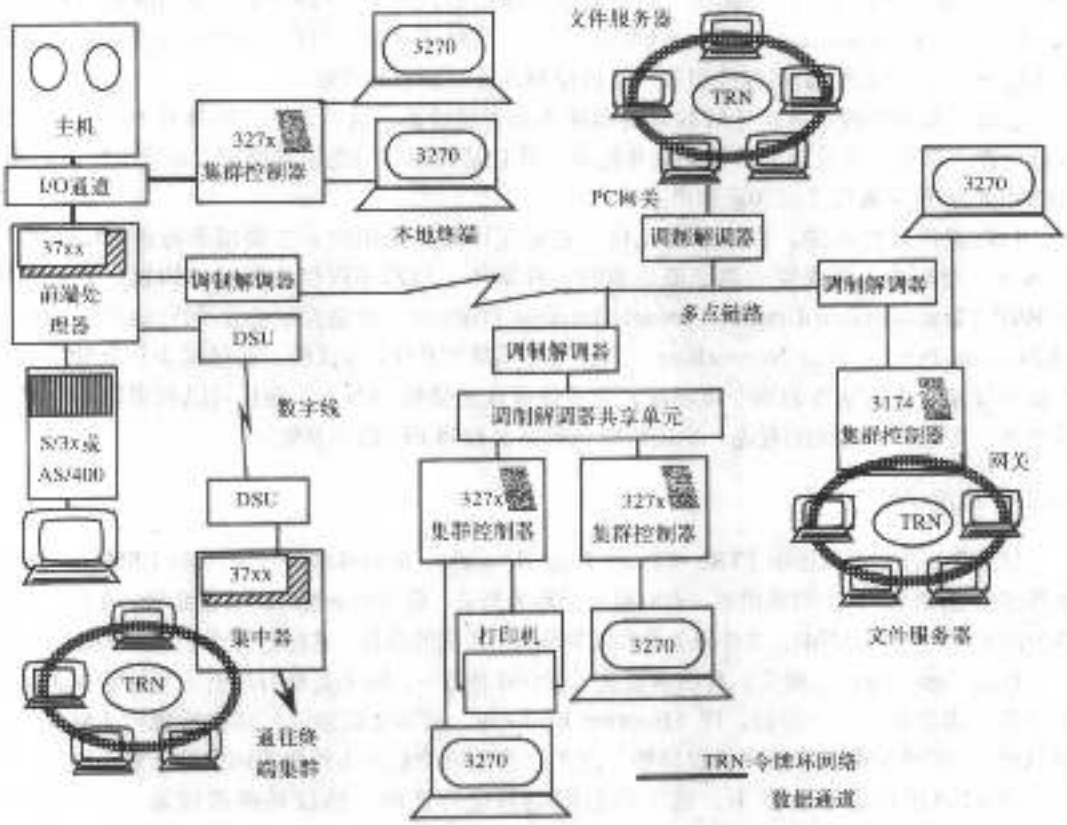


图16-2 SNA的硬件组成

和主机相连的是一个负责主机全部输入和输出操作的处理器，这个处理器称为I/O（Input/Output，输入/输出）信道。它负责在主机和与主机相连的本地设备之间的信息交换，这些与主机相连的设备有：磁盘和磁带驱动器、集群控制器、通信控制器等。

16.2.2 FEP

通信控制器既可以用作与主机相连的FEP（Front End Processor，前端处理器），又可以用

作位于主机远端的集中器。我们简单地把它们都认为是FEP。所有的网络传输线都和FEP相连，FEP是协助主机的通信处理器。它的其他任务还有检错和纠错、封装和拆分分组、作为从低速数据线到主机的高速数据通道的缓冲器等等。其SNA标识为3705、3720、3725和3745。

如果许多传输线都是从同一个地区连到FEP的，那么这些传输线的成本就会变得很高。在这种情况下，就需要在这些传输线的起始位置放置一个通信控制器。该通信控制器可以用来收集来自这些点的数据，并通过一条高速链路发送出去。在这里通信控制器可以称为集中器。图16-2就显示了一个使用数字链路的集中器。

16.2.3 集群控制器

一般来说，附属于FEP上的是集群控制器。其型号有3174、3274和3276。在图16-2中有三个集群控制器，它们共享一条多点链路，而其中的一个连到了信道上。它们一般采用SDLC（Synchronous Data Link Control，同步数据链路控制）协议与FEP通信，采用BSC（Binary Synchronous Communication，二进制同步通信）与终端通信。SDLC由SNA定义，但是BSC的出现比它早。FEP轮询集群控制器，集群控制器就轮询它的终端。

通常，与集群控制器相连的327x终端称为非智能设备。这是因为这些终端不能完成任何本地处理。但它们是使用最广泛的同步终端，并且是利用同轴电缆按照BSC协议工作。然而，LAN中的PC迅速取代了3270系列产品。

3172是比较特殊的，应该多讲几句。它是在1989年提出的，主要用来将各种LAN连到SNA上，对所有应用来说它都是低成本的一种器件。3172不仅仅支持SNA协议，它还支持TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议）、APPN（Advanced Peer to Peer Networking，高级对等网络）和OSI协议栈。通过减少TCP/IP堆栈的负载可以减少主机所需的指令周期数。它不仅可以连接到LAN上，而且可以利用T1与主机及其外围设备进行信道级的互连。它还可以执行许多3745 FEP路由功能。

16.2.4 连接LAN

虽然我们在图中只显示了TRN（Token Ring Networks，令牌环网络），但实际上SNA中可以使用许多类型的LAN。中间路由器，有时也可以称为网关，就是用来把LAN连接到SNA上的。比较典型的是，在一个LAN中，文件服务器和网关是两个不同的设备，这样它们两个就会分担业务量。

单词“gateway”（网关）有很多意思。在OSI术语中，网关是执行所有七层协议转换的最复杂的一类设备。另一方面，IP（Internet Protocol，网际互联协议）路由器也称为网关，这里只进行OSI模型中低三层的协议转换。之所以称为网关是因为两侧的网络地址是不同的。最后，在SNA市场营销文献中，这个词指的是只进行低两层协议转换的设备。在本章中，“gateway”采用的是SNA网关的含义。

SNA网络中网关的功能由PC、3745、3174集群控制器和其他几个设备提供。图16-2给出了三种方法。网关通过SDLC接口连接到SNA网络，通过NIC（LAN Network Interface Card，LAN网络接口卡）或TIC（TRN Interface Card，TRN接口卡）连接到LAN。

网关一旦接收到一个来自SNA网络的SDLC帧，就将该SDLC帧的头和尾去掉，再将MAC（Media Access Control，媒体接入控制）头、LLC（Logic Link Control，逻辑链路控制）头和MAC尾附加到该帧的数据段，之后才将该帧发送给LAN中的正确目的地。当LAN中的工作站要给主机发送数据时，这个过程恰好相反。换句话说，只有第二层的头和尾被替换了，而更

高层的头和数据都保持原封不动。

LAN中的PC可以模拟3270终端，这样主机就认为它在和3270终端会话。而且FEP一般轮询3174或者代表环路中工作站的PC网关（这称为组轮询），否则，FEP还必须轮询环中每个独立的工作站。

16.2.5 AS/400与本地、远端设备

AS/400（Application System 400，应用系统/400）是小型计算机，也称为中型计算机或分布处理器。它运行OS/400操作系统，可以为商用环境提供强大的多用户处理功能。AS/400的前身是36和38系统。

最后，连接到I/O通道上的任意设备都被认为是本地设备，而连接到FEP上的设备则称为远端设备。例如，在图16-2中，即使AS/400在物理位置上与FEP距离很近，但因为它与FEP相连，所以被认为是远端设备。

16.3 NAU与会话

16.3.1 定义NAU

回过头去看图16-1，终端用户可以是一个应用程序或者通过终端使用程序的人。任何一个终端用户都通过RU（Request/response Units，请求/响应单元）来产生和发送数据。为了将RU送到正确的目的地，SNA定义了NAU（Network Addressable Units，网络寻址单元）。NAU是与SNA网络相连的逻辑通信端口。通过NAU，终端用户和SNA设备就能够接入SNA网络。终端、集群控制器、应用程序、VTAM和TP监视器都是NAU的实例。任何想要在网络中发送和接收数据的设备必须具有NAU。LU（Logical Units，逻辑单元）、PU（Physical Units，物理单元）和SSCP（System Services Control Point，系统业务控制节点）是三种类型的NAU。

16.3.2 LU

LU是NAU的一种类型，终端用户利用它来接入网络。图16-3显示了LU在SNA网络中的位置和它们的类型。LU本身是在支持特殊设备的软件中定义的。这个软件提供了非常广泛的功能和智能应用，均属于LU的类型。

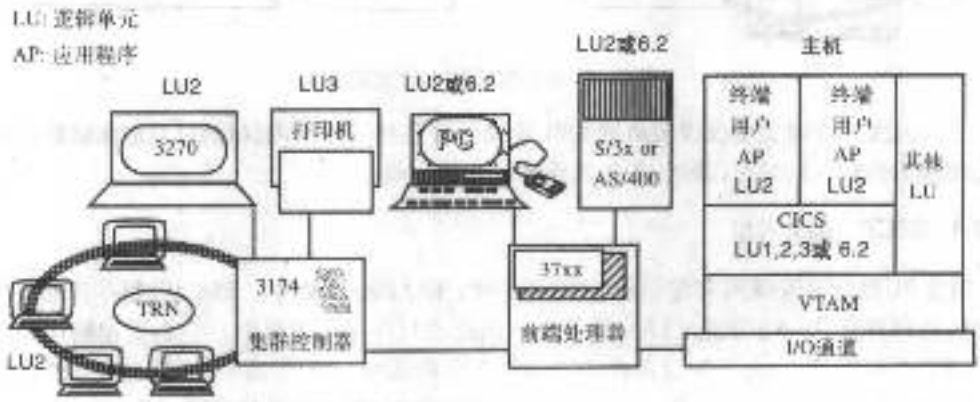


图16-3 各种类型的LU的位置示例

0型LU支持诸如BSC 3270终端的前-SNA协议。1型LU用于批量传输数据的终端，而3型LU用在打印机上。应用程序与采用SNA数据流的交互式设备如3270之间的通信使用2型的LU。最初，3270的LU功能实际上都位于运行在集群控制器上的软件中。然而，在PC中，该软件可能是运行在PC本身的。

6.2型的LU是一个通用的程序到程序（Program-to-program）LU，它可以使两个终端在使用主机的最少资源的情况下彼此通信。这与传统的分层网络的概念有所不同。这种LU的另一个名字是APPC（Advanced Program to Program Communication，高级程序到程序通信），稍候我们会讨论到。依据通信时使用的LU类型不同，CICS TP监视器可作为任何一种类型的LU。因此，LU的类型就是由双方会话能力决定的NAU。

16.3.3　PU

PU不是一个物理设备，而是在需要网络接入的设备的软件中提供的功能和程序。PU是SNA设备的资源管理器。它提供配置服务、请求软件下载、产生诊断信息等功能。PU管理并控制与其相连的LU。

和LU一样，PU也分为几种类型，称为PU类型。PU类型也称为SNA节点类型。目前重要的节点类型是2、2.1、4和5，如图16-4所示。5型PU在VTAM中执行，而4型在NCP（Network Control Program，网络控制程序）中执行，NCP是在FEP中运行的。2型PU是和集群控制器相联系的；2.1型PU是用来支持APPN的，它是所有PU中最高级的类型。它可以在不需要主机功能的情况下直接和对等的或者相邻的PU2.1通信。

图16-4中显示了网关或TRN中的PC提供的PU的功能。如果PU的功能由PC提供，那么网关只用来进行MAC/LLC到SDLC的转换。然而，主机必须维护表并管理与各PC的会话。

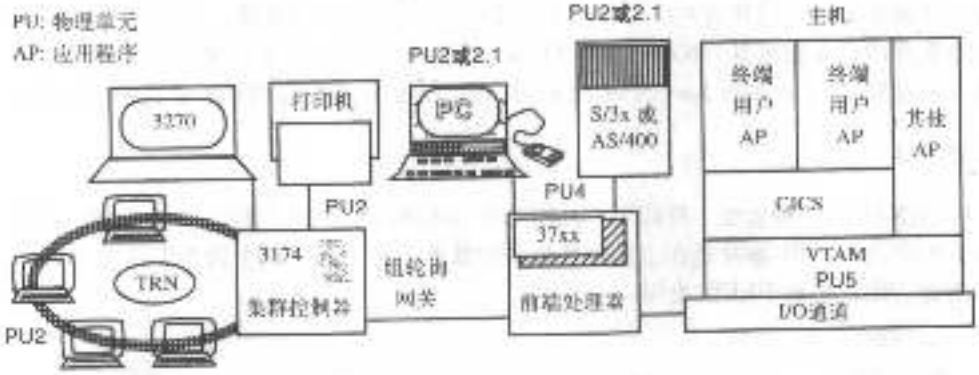


图16-4　各种类型的PU的位置示例

另一方面，在网关中仅设置单独的PU定义，并且在工作站内仅提供LU定义就能够减轻主机处理器的负载，同时可以减少工作站所需的存储空间。

16.3.4　SSCP、域和寻址

就像PU控制并管理所有与它相连的LU一样，除APPN以外中，SSCP控制并管理逻辑上与它相连的PU和LU。SSCP是VTAM的子集，因此它只存在于主机中。它负责初始化和释放网络。所有在SSCP控制之下的设备都被认为是在它的域中。PU帮助SSCP管理网络的资源，例如，在激活终端用户的LU之前，SSCP或VTAM必须激活NCP中的PU和集群控制器。

图16-5给出了一个多域网络，该网络包含一个以上的域。一个域由一个5类节点（主机）和它相关的包括4类节点（FEP）的网络组成。每个域又进一步分为子域，每个子域由一个4类或5类节点及其相关网络组成。主机和FEP本身被称为子域节点。任意一个不是子域节点的SNA节点都称为外围节点。

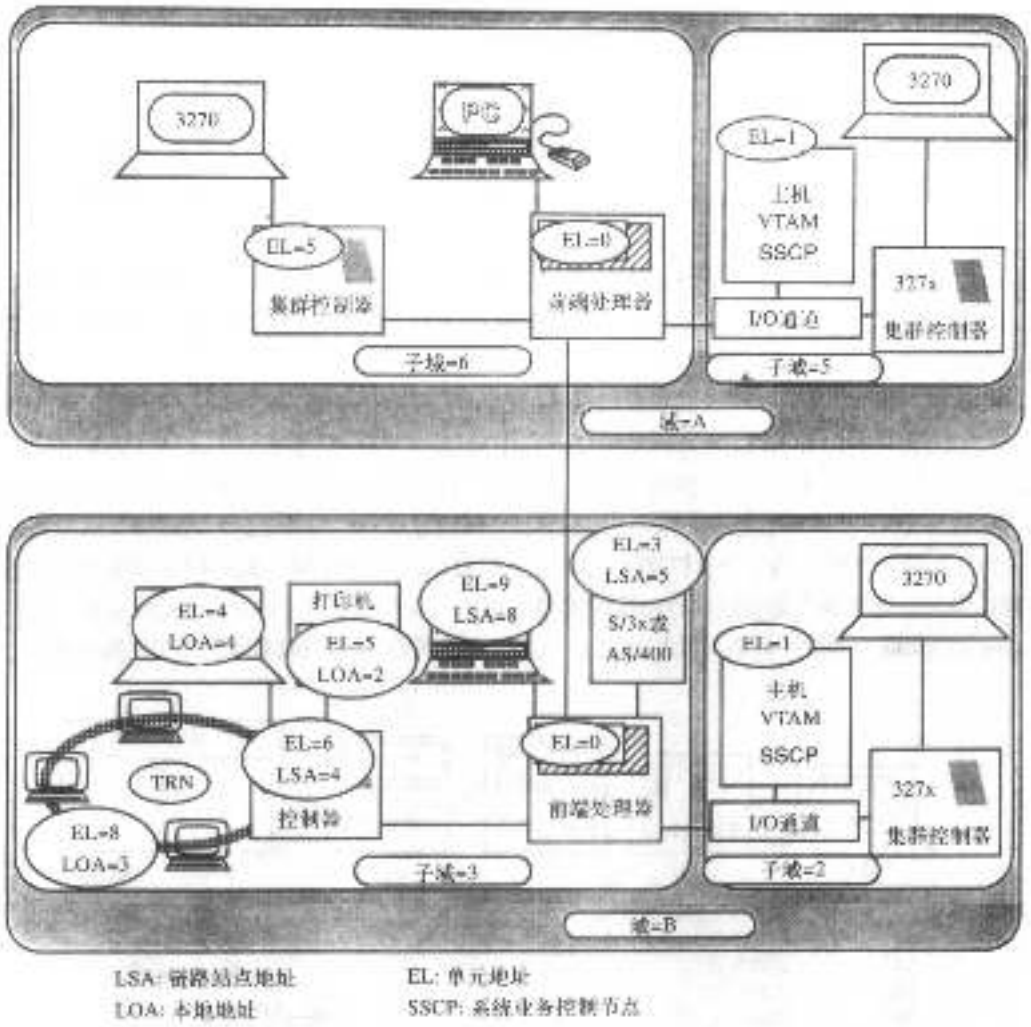


图16-5 采用LOS-LSA寻址形式的子域内的流量与采用子域-单元寻址形式的子域之间的流量

在多域网络中，每个子域都分配了一个唯一的标识符，称为子域号。图16-5给出了4个子域。而且在每个子域中，每个NAU都分配有一个单元号。因此要标识一个NAU，必须在提供单元号的同时提供子域号。外围节点在寻找和它们相连的设备地址时并不使用子域-单元号对。它们使用的是本地形式的寻址，称为本地地址和链路站地址。为了简化，我们把它们分别缩写为LOA（local addresses）和LSA（link station addresses）。

这些LSA和LOA对在每个子域中都是唯一的。例如，图16-5中LSA为4和LOA为4是子域3中3270终端的地址。LSA标识控制器，LOA标识终端。这个LSA和LOA对虽然可以在其他子域中出现，但是不能再分配给这个子域中其他任何一个设备。

现在，当主机内的应用程序向3270发送消息时，它知道并使用子域-单元地址对。然后，在将此消息发往目的地之前，NCP把这个地址对翻译成驻留在FEP中的本地标识符。

由于FEP进行了地址类型的转换，因此它也称为边界功能节点。主机也可以作为其外围设备的边界功能节点，这些外围设备是通过I/O通道连接在主机上的。总的来说，子域-单元对用来对子域内的设备寻址，而子域节点是通过本地寻址表单从边界功能中找到外围设备节点的。

16.3.5 会话

当两个终端用户的NAU建立会话之后，它们就可以彼此通信了。换言之，两个NAU之间的SNA会话对于二者之间的有序通信来说是必需的。在会话的初始化过程中，NAU决定它们之间使用的协议是否兼容，如果不兼容，那么这个会话就不能初始化。共有四种类型的会话，其中三种涉及到SSCP，另外一种是在两个LU之间建立的。这些会话类型分别称为SSCP-SSCP（用于多域网络中）、SSCP-PU、SSCP-LU和LU-LU。

SSCP会话一般在网络组建时建立。这些会话在各种可用网络资源之间提供网络控制，而LU-LU会话在应用程序之间提供通信能力。只有在路径上的所有NAU都建立了必要的SSCP类型的会话后，LU-LU会话才能建立。

图16-6说明的是为了使一个网络终端接入CICS，而在这个单域网络中建立一个会话所涉及的步骤。在这里主机LU称为PLU（Primary LU，主LU），而网络LU称为SLU（Secondary LU，次LU）。PLU可以参与许多LU-LU会话，但SLU只可以参与一个。这些主要用在相关的LU上，而不是独立的LU6.2上。CICS首先初始化一个和VTAM的会话，从而建立SSCP-LU会话，这样就可以使其他LU登录到它上面。然后，为了所有PU都在物理上连接到LU上，VTAM（或SSCP）就初始化和所有PU间的会话。这些操作是通过发布ACTPU命令完成的：先发给第一个FEP，然后发给第二个FEP，接着再发给集群控制器。最后，就初始化了一个和LU之间的会话，该LU是和3270终端相连的。

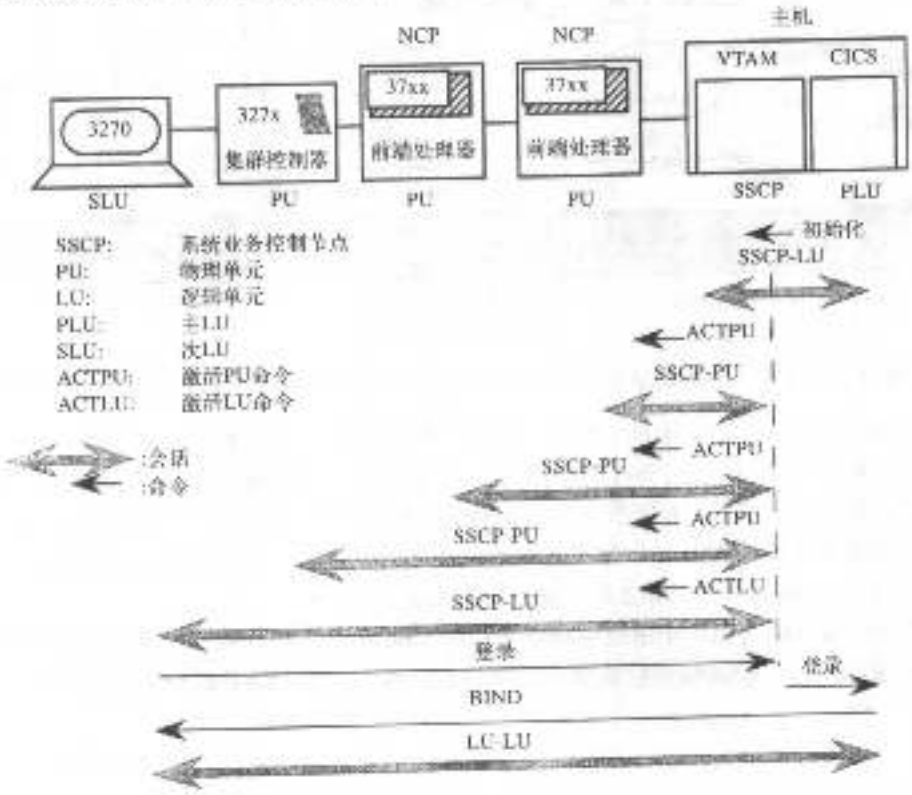


图16-6　在建立一个网络时，会话建立的顺序

这样用户就登录到CICS即主机LU上了。SSCP将提供了SLU记录的登录信息发给主机LU，通过这个信息，主机LU可以确定它是否能够支持与网络LU的会话，如果可以，主机LU就会

发布一条BIND命令，那么LU-LU会话就建立了。这个建立LU-LU会话的过程称为捆绑。

16.4 SNA体系结构

16.4.1 SNA层

图16-7给出的是SNA的七层结构。第一层，也就是物理层，通常由调制解调器和采用RS-232协议的DSU来实现。第二层一般由SDLC（Synchronous Data Link Control，同步数据链路控制）协议来实现。这两层的功能与OSI参考模型中低两层的功能类似。SDLC是SNA定义的一部分，但RS-232不是。

与OSI的网络层（X.25）在传输网络上执行路由和拥塞控制一样，SNA网络的第三层——路径控制层也执行相同的功能。然而，与X.25不同，SNA没有永久虚电路和交换虚电路。路径控制层还提供分段功能，即将长信息分成小段。

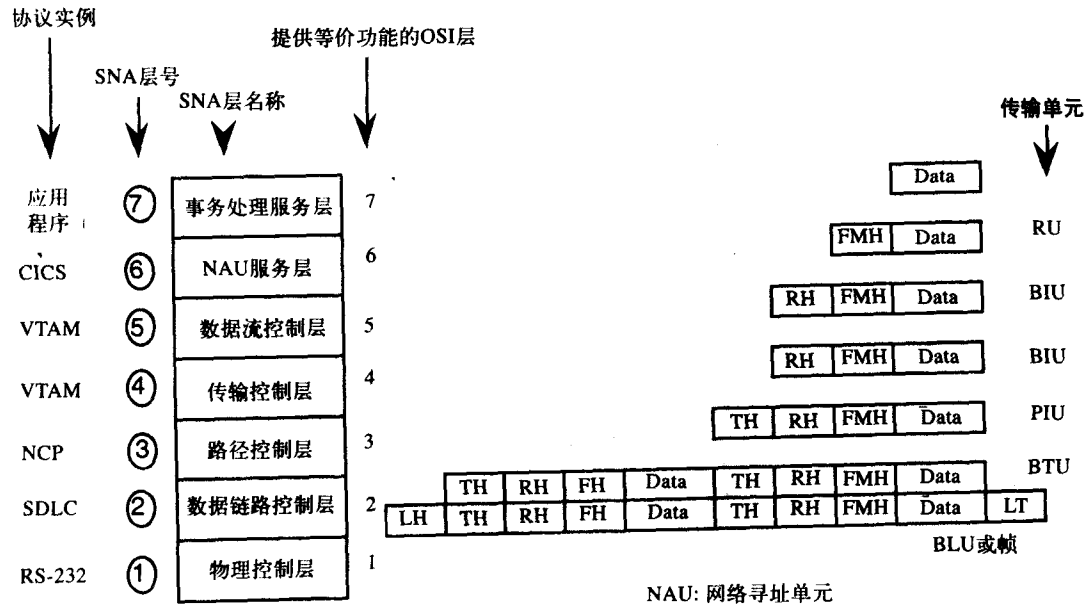


图16-7 SNA体系结构。一般情况下，主机支持所有层，而FEP支持第一层到第三层

一个面向连接的服务将所有的信息单元都沿着一条物理路径发送出去进行会话，而这条路径是在通信流量传输之前确定的。SNA就提供了这样一种面向连接的服务。第四层即传输控制层，检查会话的序列号、调步（或称为步测）和加密。调步防止了NAU发送数据的速率比接收方可以接受的速率快。这个功能称为数据流控制，但是，该功能是由其他层提供的，而不是由数据流控制层提供的。

第五层即数据流控制层，其功能有链接、会话应答、分配会话序列号等等。第六层称为

NAU服务层，其功能类似于OSI的表示控制层。NAU服务层包括事务处理子层和表示服务子层。表示服务提供程序接口和数据格式化，以及任务处理服务，该层将在16.8.3节中介绍。最后一层即应用或事务处理服务层，就是终端的用户或主机中运行的应用程序。

16.4.2 SNA的交换单元

由于数据是由应用层发出的，于是在第六层加上了FMH（Function Management Header，功能管理头），这样得到的组合称为RU（Request/response Unit，请求/响应单元）。RU可以是请求RU、响应RU或者控制RU，控制RU也是一个请求RU并用于网络管理。第五层将RH（Request/response Header，请求/响应头）加到了RU上，这样就得到了BIU（Basic Information Unit，基本信息单元）。

路径控制层又加了一个TH（Transmission Header，传输头），TH规定了路由信息，还说明了和BIU相关的是整个消息还是组成长消息的几段中的一段。根据第二层可以缓冲多少数据，它可以将多个PIU合并为一个SDLC协议处理的BTU（Basic Transmission Unit，基本传输单元）。SDLC处理帧或者BLU（Basic Link Unit，基本链路单元）。接下来让我们更详细地讨论第二、三层和更高层的协议。

16.4.3 LU协议子集

表示服务（NAU服务的一部分）层、数据流控制层和传输控制层都支持一系列的协议。SNA为三层中的每一层选择协议集，并把它们归类到协议子集，这样，特定的PS（Presentation Service，表示服务）协议子集代表了PS层支持的协议集。在建立一个会话时，根据需要什么样的功能集，选出合适的协议子集号。类似地，数据流控制层和传输控制层支持的协议集分别称为FM(Function Management，功能管理)和TS(Transmission Services，传输服务)。

这些协议子集号是用于标识LU及其性能的，这样每个LU就利用这三层中每层的协议子集号予以定义。例如，类型2的LU采用的是2号PS协议子集、3号FM协议子集和3号TS协议子集；类型6.2的LU采用的是6.2号PS协议子集、7号FM协议子集和19号TS协议子集。

16.5 SDLC

SNA支持许多数据链路控制协议，我们现在来讨论其中的一个，即SDLC。SDLC在第17章到第20章的讨论中都会用到。

图16-8给出了SDLC中使用的三种类型的BLU的格式。这三种BLU称为信息帧、监控帧和未标号帧。在本节的后续学习中，会不断地用到该图。与BSC（Binary Synchronous Communication，二进制同步通信）不同，SDLC是面向比特的全双工协议。因此，SDLC比BSC会更高效地使用传输功能。而且它还可以将数据、应答和轮询合并在一帧内。

16.5.1 标志字段和地址字段

SDLC帧都是以固定的比特格式“01111110”作为开始和结束的标志。同一个标志可以作为上一帧的结束，同时也可以作为新一帧的开始。为了使帧中的其他地方不再出现这种格式，使用了一种称为“比特填充”的技术。这就要求发送端在5个连续的1后面多传一个额外的0，接收端就会将5个连续的1后面的0删除。如果接收端在5个连续的1后面收到的不是0，而在6个连续的1后面有一个0，那么，它就是结束标志。参见图16-9给出的图解说明。

标志: "01111110"
Nr: 希望接收的帧
Ns: 发送帧的编号
p/f: 轮询或结束帧
CRC: 循环冗余校验
FCS: 帧校验序列

mmmmm: 未标号帧标识符
监控帧编码:
00 RR接收准备好（同ACK）
01 RNR接收未准备好（同WACK）
10 REJ拒绝（同NACK）

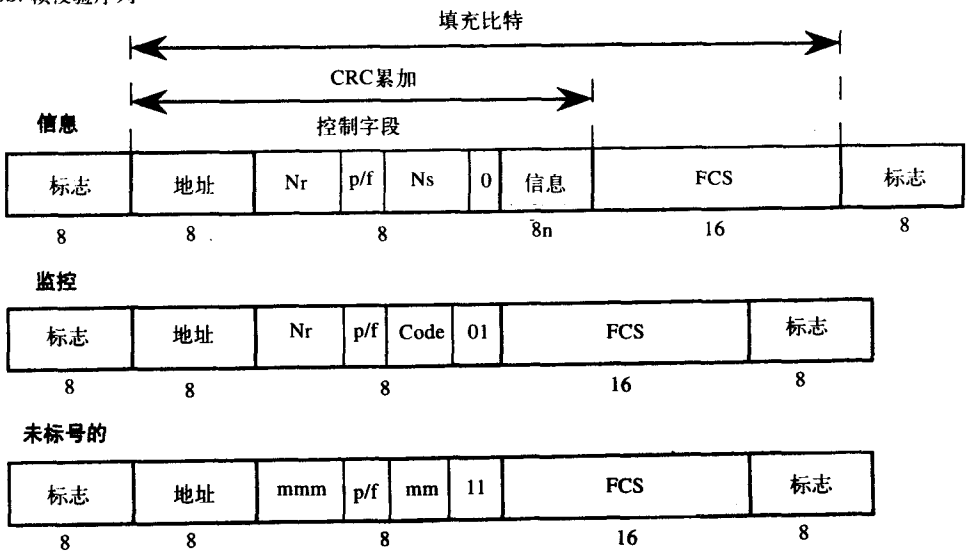


图16-8 三种SDLC帧的格式。隐藏所有类型中都不存在的字段，并标明了每个字段的比特数

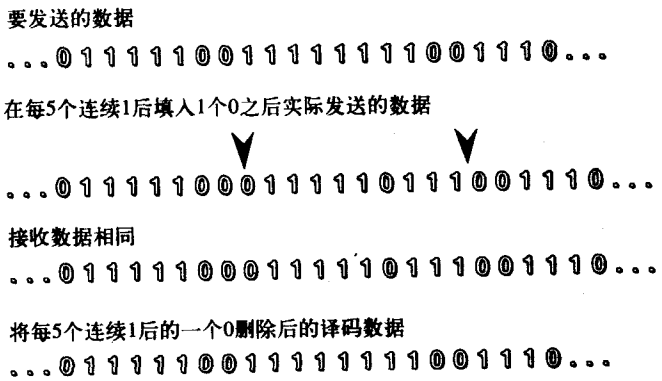


图16-9 比特填充可以防止标志（01111110）在帧中的任何位置出现

在这个标志之后的字段就是8比特地址，该地址给出的是LSA（Link Station Address，链路站地址）或者集群控制器ID。这是一个独立地址的例子。当作为网关使用的3174在一个TRN上轮询所有的PC时，就是一个组地址的例子。FCS是用于对前面的字段检错的16比特CRC字符。

16.5.2 控制字段

控制字段有许多功能。如果最后一个比特是0，就表示这个帧携带的是信息。信息字段把从更高层帧传下来的信息封装起来。另外两种类型的帧即监控帧和未标号帧都不会携带来自更高层的信息。除填充比特外，这个字段的长度是8比特的倍数。

Ns是一个3比特字段，代表的是传输帧的帧号。它也称为帧序列号。由于给Ns分配了3个比特，因此帧号可以从0（二进制数000）到7（二进制数111），即有8个可能值。Nr规定了发送端希望从远端获得的下一帧的帧号。如果A站发送了一个Ns等于2的帧，那么当B站发送它的帧的时候，它会将其Nr设定为3，表明3号帧是它希望从A站获得的下一帧。

因为这里仅为Ns和Nr各分配了3个比特，所以，在不需要接收端响应的情况下，可以发送的帧的最大帧号是7，这个数字称为窗口大小。设想一下，如果发送端真的按照从Ns=0到Ns=7的行发送了8帧，之后等待来自对方的确认信息。如果对方的响应中Nr为0，发送端就不知道它是要求重传第一帧0，还是确认第7帧并请求发送一个0号新帧。为了避免这种模糊性，为SDLC帧设定窗口大小为7。SDLC还可以将窗口大小设定为127，但这需要对Ns和Nr的字段进行扩展。

轮询/结束比特可以用在主从连接上。在这些类型的连接中，主设备控制着次设备。例如，FEP是集群控制器的主设备，集群控制器又是终端的主设备。轮询/结束比特在主设备中用作帧起始的轮询比特，在次设备中用作帧起始的结束比特。也就是说，在轮询次设备时，该比特会由主设备设置为1，否则设置为0。对于由次设备产生的帧，如果不是帧序列中的最后一帧，那么该比特就被设置为0，否则被设置为1。

通过显示FEP送出的两帧和控制器送出的一帧之间的交换，图16-10总结了控制字段和地址字段的功能。首先，控制器送出了0号帧，之后是1号帧，如Ns字段所示。由于第一帧不是最后一帧，因此第一帧的P/F字段设置为0，而第二帧将此字段设置为1，告知控制器这是一个轮询。然后控制器将送出0号帧，并将Nr设置为2，以此来确认FEP的1号帧。

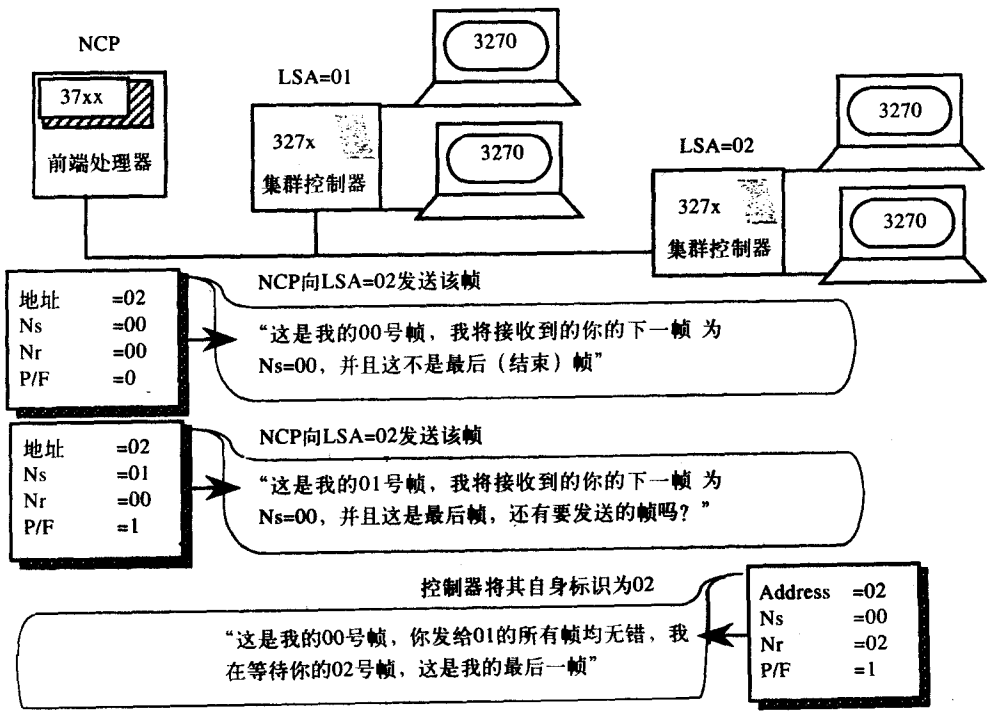


图16-10　在多点链路上帧交换的例子

现在，让我们把注意力转向图16-8中所示的另外两种类型的帧上。如果控制字段的最后

一个比特是1，那么就没有信息发送。换句话说，这个帧既可以是监控帧又可以是未标号帧。监控帧的控制字段以"01"结束，未标号帧的控制字段以"11"结束。

在BSC的术语中，监控帧用于发送ACK、NACK和WACK。确认的监控编码是RR（接收准备好），否定确认的编码是REJ（拒绝），等待确认的编码是RNR（接收未准备好）。RNR是通知发送站暂时停止发送，其原因是接收端的缓冲器已满。

最后，SDLC拥有14种类型的未标号帧，这些帧具有初始化连接、删除连接或者其他功能。这些类型的帧在X.25和ISDN中也有，对于它们的讨论就放在第17章和第20章了。

16.5.3 SDLC传输交换的一个例子

图16-11给出了一个通过调制解调器和一个提供多点链路的CO连接到两个集群控制器的FEP（Front End Processor，前端处理器）。这里，FEP和集群控制器分别是主站和次站的例子。在FEP与其调制解调器之间插入了一个协议分析器，用于监视链路的流量情况。分析器的左半部分显示了FEP发送的帧，右半部分显示了集群控制器发送的帧。地址字段规定了这些帧被发送到哪个集群控制器，或者被哪个集群控制器接收。

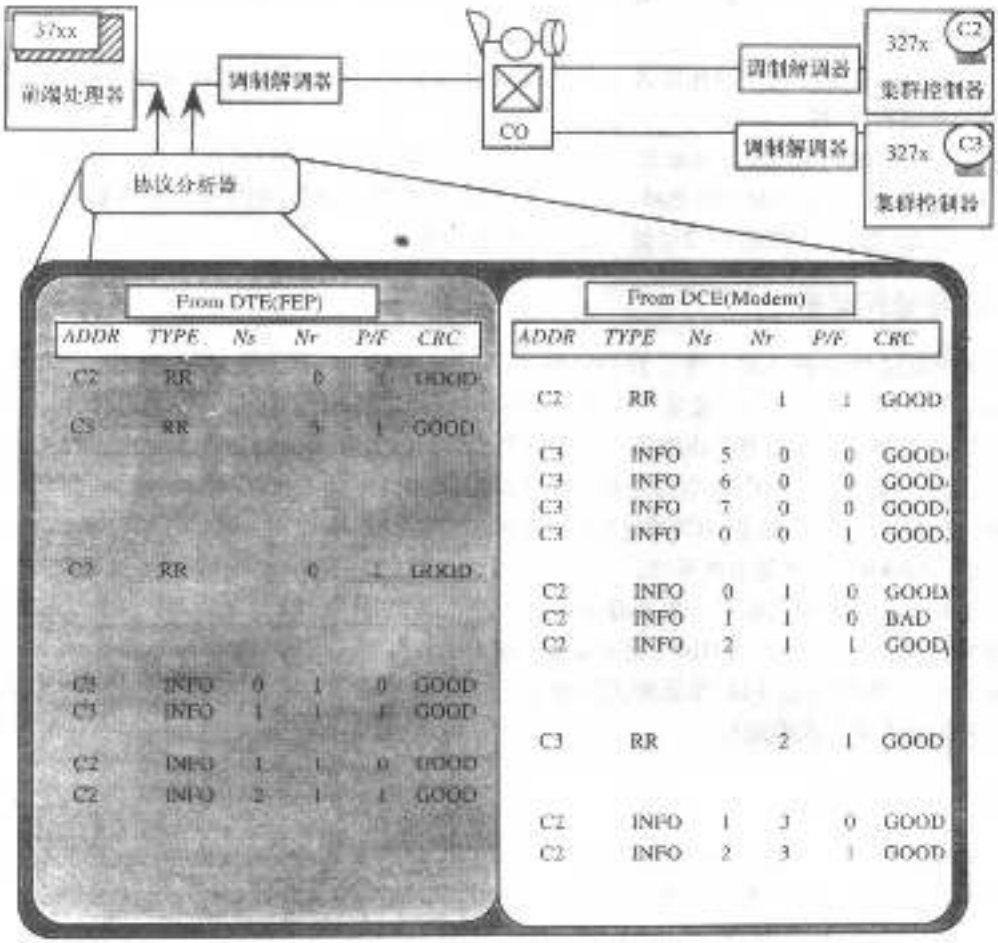


图16-11 从协议分析器上看到的在FEP和两个集群控制器之间交换SDLC帧的图解

开始时，由于FEP没有未处理的错误，因此FEP给集群控制器C2发送了一个编码为RR的监控帧。由于是FEP将P/F设置为1，因此该比特就表明正在轮询C2。监控帧没有Ns字段，但是有Nr字段。Nr字段的0比特向C2表明 FEP希望得到的下一帧是0号帧。正确的CRC表明此帧在这一点上没有错误。

在图中，由于C2刚刚被轮询，因此它就发送出了下一帧。它可以选择发送信息帧，但是它显然没有任何信息，因此它就发送了一个类型为RR的监控帧。它希望从FEP接收到的下一帧是1号帧，因此Nr为1。同样，由于这一帧后面没有其他的帧，因此P/F为1，并且，通过分析器的帧状态良好。

接着FEP轮询C3，它希望从C3接收到的下一帧是5号帧。与C2不同，C3有数据需要发送，因此它从5（即Ns）号帧开始发送信息帧。它要发送4帧，由于Ns域只有3比特长，因此在7号帧后，Ns又重新回到0。所有的帧都是无误接收，除最后一帧外，它们的P/F比特都设置为0。当集群控制器设置P/F比特时，它具有这是否是最后一帧的意思。轮询仅由主设备（此时指的是FEP）完成。

之后，FEP再次轮询C2，看看是否有数据发送。这次C2有数据要传送，它发送0、1和2号帧。注意，1号帧有错，但是在FEP通知C2这个错误之前，它先给C3发送信息并轮询它。由于FEP希望从C3接收的下一帧是1号帧，因此它发送的Nr为1，由此确认已收到C3的四个帧（5、6、7和0号帧）。

C3没有信息要发送，因此发送了一个RR帧；但是，它通过将Nr字段设置为2来确认收到FEP的0号帧和1号帧。

现在FEP又回到了C2。它通过将Nr设置为1来表明它接收到的1号帧有错。在FEP通知C2这个错误时，它发送了两个信息帧。之后，C2从错误帧即1号帧开始重新发送所有帧，同时通过设定Nr为3来确认FEP的1、2号帧。这样交换继续进行。

16.6 路径控制层

从数据链路控制层向上移，我们就到达了SNA体系结构栈的路径控制层。它负责路由SNA网络中各个节点之间的流量。这些节点包括外围节点和子域节点。根据会话的路径不同，子域节点又进一步分为边界功能节点和中间节点。边界功能节点是最接近正在进行的会话的端节点的子域节点，而中间节点是那些位于边界功能节点和主机之间的路径上的子域节点。例如，在图16-12中，如果CICS通过SA7（子域节点7）和LUa进行会话，那么SA6就是边界功能节点，SA4和SA7就是中间节点。

在本节，让我们先来看一看处理子域之间路由的术语和问题，之后再扩展到子域内路由问题的讨论。一般说来，FID4（格式ID4）是子域节点间使用的TH（Transmission Header，传输头），它携带的是子域-单元形式的地址。FID2是子域节点及其外围节点之间使用的TH，它携带的是本地形式的地址。

16.6.1 子域间路由

虚拟路由：TG（Transmission Group，传输组）是两个子域节点之间并行链路的集合。为了增加可靠性或者提供更多种类型的服务，可以在它们之间放置多个TG。各种TG如图16-12所示。由于PIU（Path Information Unit，路径信息单元）在TG上传送，因此在TH字段中给它们分配了TG序列号。

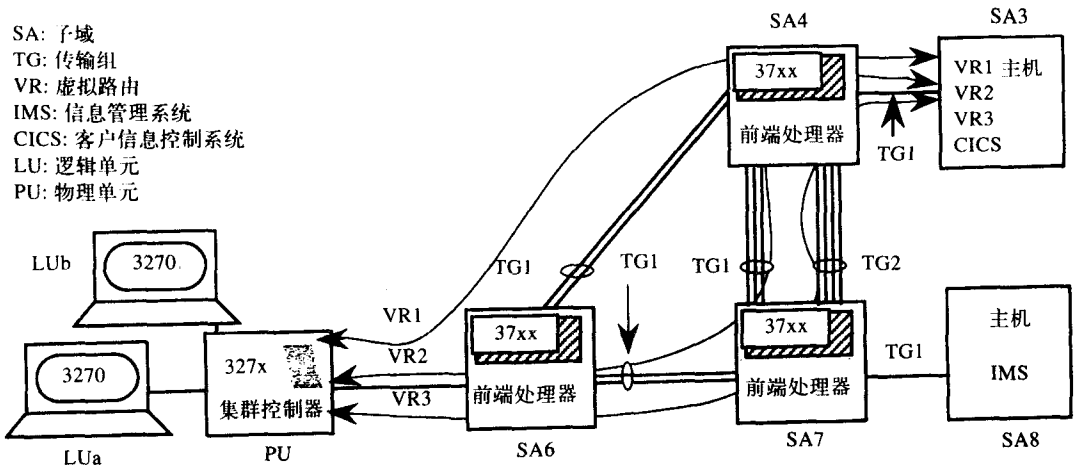


图16-12 子域间的传输组以及SA3与PU间的三种可能的虚拟路由

由于PIU从一个子域节点传送到另一个，其TH携带着目的子域节点或边界功能节点的地址，这些地址可以帮助中间节点正确地路由PIU。例如，在图16-12中，SA3知道应该把所有去往SA6的PIU送到SA4，但是并不知道SA4将要把这些PIU送到哪里去。SA3关心的只是下一个节点为SA4。在SNA中，这种完全由各SA（Subarea Node，子域节点）决定的端到端路径称为虚拟路由，各SA会将PIU转发到下一个SA节点。我们将在第17章中看到这与X.25的虚电路是不同的。

在图16-12中可看到三种可以用于CICS和LUa之间流量的虚拟路由。它们是VR1：S3-SA4-SA6，VR2：SA3-SA4-（经过TG1）-SA7-SA6以及VR3：SA3-SA4-（经过TG2）-SA7-SA6。这些虚拟路由路径都在所有相关SA节点的路由表中定义。同时，所有的虚拟路由不在任何一个SA节点中定义，但每个SA节点只具有通过它的虚拟路由的转发地址。

在会话建立的过程中，可以定义一条虚拟路由为主要路由，其他的是备用路由。会话中两个方向的所有流量都会沿着已经选定的虚拟路由进行传送。如果这个虚拟路由在会话期间出现了故障，那么该会话就会失败，当重新建立这个会话时，会选用一条新的虚拟路由。

虚拟路由是双向路由，它们由两条称为显式路由的单向路由组成。换句话说，虚拟路由可以由一条输入显式路由和一条输出显式路由定义。这些路由都是在存储于VTAM和NCP的路径表中定义。

服务类型：为了提供流量的优先级，SNA节点中还有COS（Class Of Service，服务类型）表。表中规定了网络中开始于或结束于节点的流量的优先级。因此，在图16-12中，如果LUa的优先级高于LUb，那么LUa的主路由就是VR1（Virtual Route1，虚拟路由1），备用路由是VR2和VR3。同样LUb的主路由是VR2，备用路由是VR1和VR3。

现在，如果VR1发生了故障，由于SA6与SA4之间的TG1会发生中断，那么LUa的流量就会转换路由到VR2，如果必要的话，也可以转到VR3。但是，不论在哪种情况下，它都会比LUb流量的优先级高。这种流量的“冲击”类型，或者谁可以冲击谁都写在COS表中。每个COS都有一个在登录过程中选择的COS名称。

虚拟路由调步（pacing）：当子域节点由于缓冲器满，而暂时不能接收更多的数据时，它就会不发送调步响应，使发送端停止发送更多的PIU。当缓冲器变空又可以接收更多的数据时，它就发送调步响应。这就通知子域节点发送另一组PIU。

上面所描述的技术称为路径控制调步或虚拟路由调步。该技术可以使子域节点通知发射

节点是否发送更多的PIU。在不需要接收端的响应时，发射节点可以发送的PIU的数量称为窗口大小。窗口大小的增加或减小取决于接收节点出现的拥塞和活动数量。

虚拟路由调步影响两个相邻子域间所有会话的PIU的数据流。类似地，SNA也有会话调步（在16.7节中介绍），它的会话调步控制着两个终端用户之间的数据流，并只影响它们之间的特定会话。提供两种类型的调步是很必要的。当所有受影响的用户都工作良好但支持它们的资源很紧张时，需要虚拟路由调步。会话调步的作用是应用程序发生故障时切断那个会话。

16.6.2 端到端路径控制路由

到目前为止，我们已经讨论了SA之间的流量路由问题。下面我们将讨论流量是如何从边界功能节点路由到外围节点的，但首先回顾一下SNA的地址类型。

地址的子域-单元形式只用在SA间，它是在FID4类型的PIU的TH中提供的。外围节点不使用这种地址类型。相反，它们使用LSA（Link Station Address，链路站地址）和LOA（LOcal Address，本地地址）的地址形式。子域节点不使用本地的地址形式，但是边界功能节点提供了这两种地址形式之间的转换。

在图16-13中，IMS给LUa发送消息。VTAM不知道LUa的本地地址对（LSA和LOA），但是它知道在FID4 TH中提供的子域-单元对（SA=6，EL=2）。主机和FEP之间的数据链路协议没在图中显示。

SA7的NCP发现PIU的目的子域地址是6，而不是它自己的地址。在其表中查询之后，由于SA6是这个链路的另一端，因此增加了SDLC地址4。

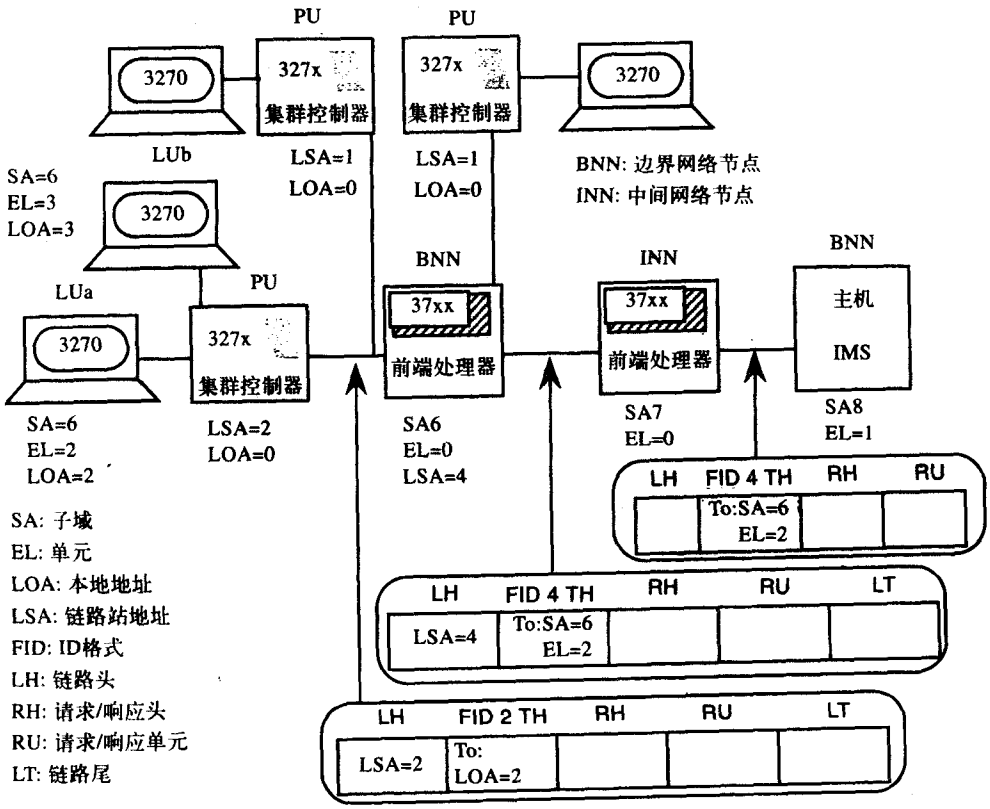


图16-13 前端在传输头内将地址从子域-单元形式转换到本地形式

SA6的NCP发现它自己的地址6在TH中，因此它去掉了SDLC的头、尾和FID4的传输头。之后再加上类型为FID2的新TH，此时LOA为2，该参数对应着子域6和单元2，同时还加上了一个地址（LSA）为2的新的SDLC头和尾。注意，尽管除地址形式之外在两种类型的TH中还有其他不同，这个边界功能节点进行了地址类型的转换，还进行了TH类型的转换。

接着，在LSA为2的控制器检测到这个帧是它的，通过给定TH中的LOA为2将该信息发送给LUa。

16.7 记录链锁、调步和分段

本节主要讨论SNA高层提供的功能，即NAU服务、数据流控制和传输控制。

16.7.1 记录链锁

在许多事务处理系统中，为了维持数据库的完整性，在一个工作单元中识别一定数量的请求是十分必要的。如果所有的请求都成功了，那么这个数据库就可以提交了；否则，利用所有变化的存储记录，它可以回滚到初始状态。将逻辑数据或RU看作一个实体的机制称为记录链锁。属于一个记录链锁的PIU称为单元（element）。

当一个LU-LU会话开始建立时，PLU（Primary LU，主LU）找到SLU（Secondary LU，次LU）缓冲区的大小，PLU确定以多大的数量来划分消息，或以什么大小来发送PIU，这样SLU的缓冲区就不会溢出了。

在图16-14中，一个应用程序有一个4800B的消息要发送给SLU。因为缓冲区只有1600个

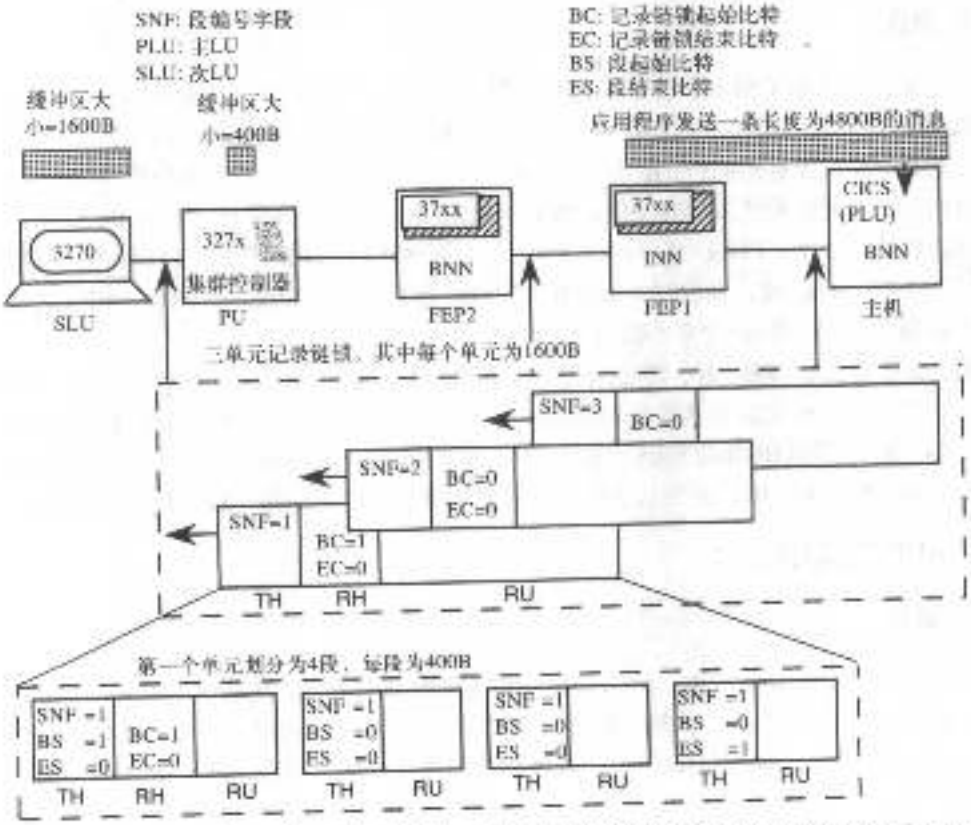


图16-14 由于SLU的缓冲区只有1600B，因此一个长度为4800B的消息必须划分为3个单元记录链锁。同样，由于PU的缓冲区只有400B，因此，FEP2必须将每个PIU分成4段

字节，所以在会话激活期间，PLU或CICS发送的单元不能大于1600B，这将使SLU分三部分接收消息，每部分都刚好放到缓冲区中（图中还显示了每个单元如何分成四段，以适应集群控制器的缓冲区大小，我们以后再讨论）。记录链锁中的每个单元都在TH中给了一个序列号，这个号码称为SNF（Segment Number Field，段号码字段），记录链锁单元就以SNF=1到SNF=3来标记。在RH中有两个字段，称为BC（Begin Chain，开始记录链锁）和EC（End Chain，结束记录链锁），它们让SLU知道哪个单元是开始单元，哪个单元是最后单元，哪个单元是中间单元。第一个单元的BC比特为1，最后一个单元的EC比特为1，所有单元的其他比特都为0。

16.7.2 会话调步

有时，发送的PIU大小比接收端的缓冲区小。在这种情况下，只要SLU有足够的缓冲区空间放下多个单元，那么，PLU就可以在不需要SLU响应的情况下连续发送几个PIU。在SLU处理完这些PIU之后，它就会给PLU发送一个响应，让它发送下一组PIU。这个程序可以使SLU控制PIU发送的速率，这称为会话调步，它与16.6.1节中描述的虚拟路由调步不同。连续发送的PIU的数目称为调步窗口的大小。而且，在端点间不存在拥塞时，SNA可以使用调步机制来提供平稳的通信流量。

所以，记录链锁将信息分成了小的单元，这样这些单元就可以放在SLU的缓冲区中，而会话调步允许接收方在下一组数据到来之前，有足够的时间处理缓冲区中的数据。

16.7.3 分段

当记录链锁送到了SLU，该单元通过边界功能节点（或图16-14中的FEP2）发送到PU。由于PU缓冲区的尺寸更小，因此在FEP2，PIU或记录链锁单元应该进一步拆分。通过边界功能节点将PIU拆分成更小的PIU称为分段。然而，分段比特在所有FID类型中都进行了编码，因此分段可以在网络的任何地方发生。当采用APPN时，分段会在主机之间发生。

在我们的例子中，PU缓冲区只有400B大小，而到达FEP2的PIU长度为1600B。因此FEP2必须将每个PIU分成4段，即发送全部4800B的消息总共需采用12段。在图16-14中显示了第一个记录链锁单元被分段为4个更小的PIU的情形。

和记录链锁单元的RH一样，RH仅在第一段发送，在其他段中不发送。然而，TH在每段都有。

在这里，为了标识所有这些段都属于同一个记录链锁单元，SNF部分在每段都复制。而且，类似于RH字段的BC字段和EC字段，TH字段的BS（Begin Segment bit，开始段比特）字段和ES（End Segment bit，结束段比特）字段都被置位，以标识第一段、最后一段和中间段。

16.8 APPC或LU6.2

16.8.1 简介

自从1974年出现SNA以来，SNA就是一种主机驱动的网络。所有的资源和用户都依赖于主机，如果主机出现了故障，整个网络就会停顿。1984年，IBM提出了APPC（Advanced Program to Program Communications，高级程序到程序通信），开始将SNA转向了并非完全面向主机的网络。1991年，提出了APPN（Advanced Peer to Peer Networking，高级对等联网技术），它根本不需要SNA网络拥有主机。本节介绍APPC，并在16.9节介绍APPN。

为了方便APPC网络的实现，提出了一种新的LU类型，称为LU6.2，这两个术语是可以互换的。

与此同时，还提出了LEN（Low Entry Networking，低入口网络）。于是，两个外围LU就可以彼此通信，并且在它们之间建立会话。这与已建立的、所有的LU-LU会话都需要主机的SNA环境具有很大的不同。如图16-15所示。但是，LEN需要建立一种称为PU2.1的新PU类型。如果没有LEN，各外围LU在一个时间内仅可以保持与主机LU的一个会话，而且在这样的会话中，外围LU必须是SLU。随着LEN的出现，网络LU可以在同一时间内保持几个会话，并且可以作为PLU。

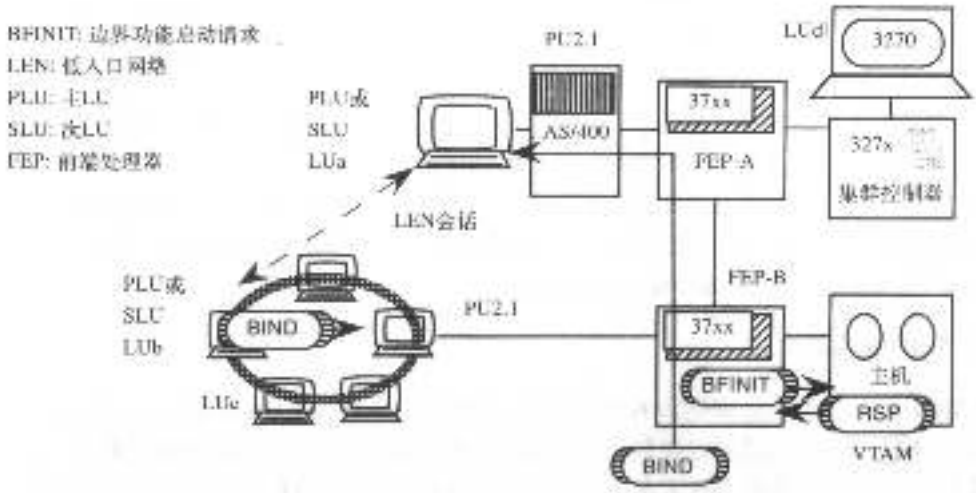


图16-15 建立一个LEN会话的步骤

APPC允许实时的分布式事务处理。这意味着，当事务处理程序在主机上运行，终端操作员发起一次请求时，该事务仍然可以向另一台主机发起另一个事务处理。原主机一旦接收到响应，它或者满足操作员的请求，或者拒绝请求；或者在给终端发送响应之完成另一个事务处理。在这里术语“主机”指的是大型机、小型机或微型机。

让我们回过头再来看看本章开始时介绍的旅行社代理的例子。假定该代理的顾客预订了在特定日期从迈阿密（Miami）到里约热内卢（Rio de Janeiro）的航班A。由于计划的改变，顾客想先到巴西利亚（Brasilia），然后再通过国内航空公司的航班B到里约热内卢。但是，代理商在没有查询两条航线的数据库之前，他不能确定这两条航线是否连接良好。航线C也是从迈阿密到巴西利亚的。如果这条航线可以提供更好的连接，那么预订就可以转到这条航线上来。代理商发起一个与三条航线数据库接口的分布式事务处理。在必要的时候取消预订或建立预订。

不管在各种节点上采用的是哪些厂商生产的硬件，运行的是何种应用程序或者操作系统，只要它们是LU6.2节点，APPC就允许旅行社代理为其顾客提供这类实时的服务。换句话说，APPC提供了一个不依赖于厂商的开放的系统体系结构接口。

16.8.2 LEN

最初，LEN只能存在于直接相连的两个节点之间，如图16-15中LUb和LUa之间。然而，从NCP的5.2版本和VTAM的3.2版本开始，主机和FEP开始支持LEN。即使LUa和LUb并没有直接相连，但是，子域节点软件的这些新版本都允许LUa与LUb彼此通信。它们之间的LEN会话用虚线表示。

为了建立跨越子域边界的LEN会话，VTAM必须知道或找到这些LU位于何处，并提供给需要这一信息来建立会话的NCP。

在建立一个LEN会话时，首先，VTAM必须要和每个相关的FEP建立SSCP-PU会话。2.0型的逻辑单元需要VTAM建立一个LEN会话，而2.1型的逻辑单元根本不需要VTAM的服务。

利用该地址信息，VTAM与控制器及其终端建立一个SSCP-PU会话和一个SSCP-LU会话。然而，它仅需将各独立LU的名称和地址增加到资源定义（Resource Definition）表中，并没有与2.1型节点或相关LU建立会话。

现在，如果LUb想要建立与LUa的会话，它就会给FEP-B发送一个BIND请求。然后，FEP-B给VTAM发送一条BFINIT（Boundary Function INITiate，边界功能启动请求）消息，希望从它那里获得LUa的网络地址。VTAM以这个地址作为响应，然后BIND由FEP-B转发给LUa。这就在LUa与LUb之间建立了一个LEN会话，并且不再需要VTAM，即使在结束会话时也不需要VTAM。由此注意到，VTAM仅提供了地址的映射。

APPC允许我们在会话的两端使用智能实体。如果没有智能实体，LU2.0特别是3270终端一次只能参与一个会话，但是LU6.2允许同时参与多个会话。当LU6.2和另一个远端LU6.2之间存在多个会话时，这些会话就称为是并行的。

16.8.3 APPC体系结构

如果图16-15中所示的网络没有提供LEN，那么，在LUa与LUb之间只存在连接。但是，通过引入LEN，这些LU就可以通信了。APPC通过允许节点上的事务处理应用程序利用LEN会话进行通信，于是就使这些节点在更高的层次上进行网络互联。两个LU之间的通信称为LU-LU会话（session），两个TP（Transaction Programs，事务处理程序）之间的通信称为对话（conversation）。鉴于这种“对话”的概念，使用了术语“程序对程序通信”。

为了分配一个对话，如果没有空闲的会话，就先自动建立一个会话。对话必须使用一个会话，并且一个会话每次只能支持一个对话。对话也可以称为一个线程，如果一个TP需要与其他TP的几个对话，则该TP称为多线程TP。

图16-16说明了很多APPC概念。现在我们注意到有两个站点使用SNA的全部7层在彼此通信。在协议栈的顶端，TP显示为参与了彼此间的对话的ATP（Application TP，应用程序TP）。而且为了支持这些对话，LU提供了两条可用的并行会话。

这些会话在对等的表示服务层之间为对话建立了一条路径。NAU服务层（第6层）分成了两层：事务处理服务层和表示服务层。

表示服务层提供了事务处理程序与LU6.2之间的接口，称之为LU6.2 API（Application Program Interface，应用程序接口）。该层确认TP发出的呼叫具有正确的格式，并转换为正确的数据流。

事务处理服务层提供了LU6.2与STP（Service Transaction Program，服务事务处理程序）服务之间的会话管理。STP与TP类似，但是，STP作为增强性能的一部分写入了LU6.2分组。当许多TP需要一个服务时，这个服务就会作为APPC的一个附加功能预先打包成一个单元。由于STP要执行大量的编码，这就使TP的写入变得很容易。ATP与STP之间的接口称为STP定义的API。

STP的例子有DIA（Document Interchange Architecture，文件交换体系结构）、SNADS（SNA Distributed Services，SNA分布式业务）和CNOS（Change Number Of Services，改变服务数量）。DIA提供了一种集中式的文件库，还提供了在办公室环境中管理和分发文件所需的服务。然而，它实际上并不使用LU6.2协议。SNADS是DIA站点之间的一种分布式服务；由于用户必须登录DIA服务，因此他们就不需要再登录SNADS了。CNOS允许增加或减少LU之间的并行会话的数目。

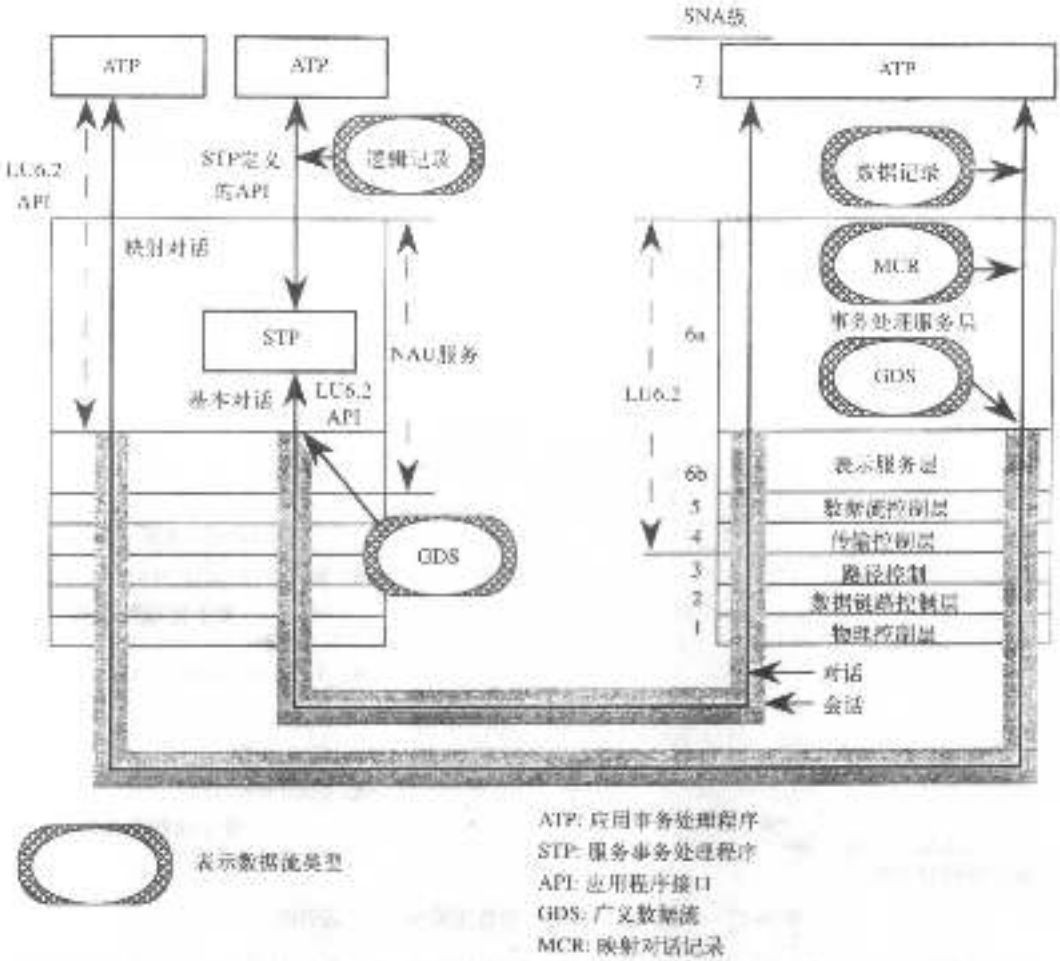


图16-16 对话类型及其关键点的数据流类型

图16-16还显示了两种类型的对话，如果对话使用了STP，就称之为基本对话（basic conversation）；如果直接与ATP接口，就称之为映射对话（mapped conversation）。STP使用基本对话。由于基本会话使用了硬件到程序的低层程序调用，因此它更为灵活和有效。另一方面，映射对话使用起来更为容易，但是效率不高。被普遍使用的TP已经设计出来，并且是兼容的和可得到的。在LU6.2之前，应用程序设计组必须编写那些不能和其他设计组编写的TP进行通信的TP。有了APPC，程序员的大部分工作已经完成，他/她所需要知道的只是远端LU和远端TP的名字。

在没有详细介绍各种接口之间的数据流之前，我们仅在图16-16中标出它们，在映射对话和基本对话的最底层的数据流称为GDS（Generalized Data Stream，广义数据流）。它包括一个GDS头和数据，几个GDS可以合并为一个RU。

映射对话使用了数据记录，数据记录在变换为GDS之前先要转换为MCR（Mapped Conversation Record，映射对话记录）。采用基本对话的TP使用的是称为逻辑记录的数据流。

16.8.4 一个APPC的对话实例

现在让我们来看一个数据如何在APPC对话上传输的例子。在图16-17中，A站点的TP有一个文件需要传送到B站点的TP。TPa需要在每8条记录之后从TPb获得一个确认。

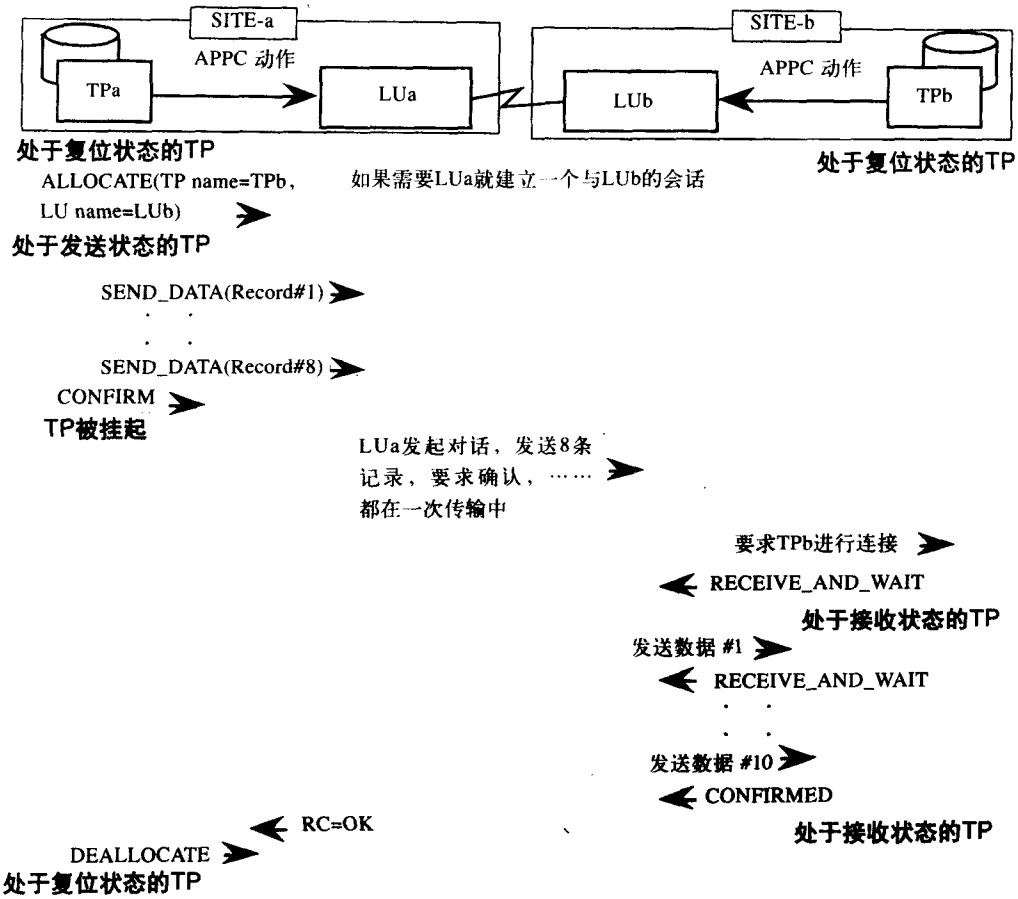


图16-17　分配和取消分配传输数据的APPC对话的例子

为了发起一个对话，TPa给它的LU发送一条ALLOCATE命令，目的LU与目的TP的名字作为参数在命令中给出。为了完成这项工作，TP最初应该在复位状态，然后进入发送状态。为了创建一个对话，两个LU之间必须有一个会话可用。如果没有，LUa会创建一个会话。之后TPa将8条数据记录和8条SEND_DATA命令一起发送给它的LU。由于8个记录后需要确认，TPa就向它的LU发送一个CONFIRM命令，并等待确认。

在这个时间内，没有信息从TPa传到TPb，但是它被LUa缓冲。RU可以在满了的时候自动发送出去，也可以由用户显式发送。现在LUa刷新它的缓冲区，并把这条信息发送给LUb。然后LUb启动TPb。TPb一接收到对话分配请求，就给其LU发送一条RECEIVE_AND_WAIT命令，将它的状态由复位改为接收。

然后，LUb将数据分块，数据块的大小要符合TPb的缓冲区的尺寸。注意，这里TPb缓冲区的尺寸比记录的尺寸小，因此多个数据单元（在我们的例子中是10个）被发送到TPb，而不是最初的个数（8个）。在每个数据单元之后，TPb发送一条RECEIVE_AND_WAIT命令，在发送了CONFIRMED命令之后就进入了接收状态。

LUa将CONFIRMED命令翻译成了“OK”的RC（Return Code，返回代码），表明TPb正确接收了所有的数据。这样，直到数据被远端TP确认，TPa才会通过发送SEND_DATA命令来发送另外8条记录，否则TPa会给LUa发送一条DEALLOCATE命令来中断对话。之后，两个TP都进

入了复位状态。

需要注意的是，在发送状态，TP只能发送数据、请求确认、发送错误信息和取消分配对话。同时，在接收状态，TP只可以接收数据。对话是半双工的传输，它与大多数与商业相关的事务处理是一致的，因为这些事务处理本身也是半双工的。

16.9 APPN

APPN（Advanced Peer to Peer Networking，高级对等联网技术）提出了在SNA网络中的分布式处理，它完全是面向远离中心主机的网络设备的。这种体系结构是与LAN和路由器环境相兼容的，这种环境产生了今天的大多数商业。因此，APPN也称为新型SNA体系结构。但是它并不使用诸如PU、SSCP或子域等体系结构的概念。旧的SNA体系结构，特别是与4类、5类节点相关的体系结构，是在特定的设备上实现的，这就使得SNA看起来是依赖于设备的网络。相反，APPN并不把自己束缚在特定的设备上，而是使其可以在任何智能设备上实现。APPN是从APPC得出的SNA的另一个逻辑派生。在建立一个会话时，APPC仍然需要VTAM存储并提供子域间的路由信息，而APPN就可以不需要VTAM。

APPN在实现的时候可以仅使用PC和AS/400，而不需要任何昂贵的主机或前端设备（然而，一般的用户都在旧的SNA网络中，他们需要转换到基于局域网的传输上去）。这种做法可以使他们增加可靠性、更好地利用链路并且对FEP端口的需求更少。这使用户不必替换已有设备就可以扩展其网络。图16-18显示了旧的SNA网络与APPN的结合。

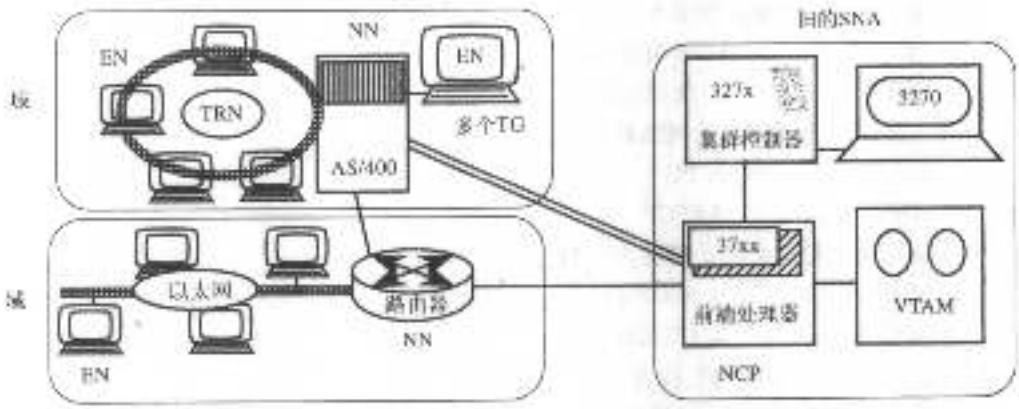


图16-18 一个将新SNA和旧SNA结合的例子

APPN定义了两种类型的节点。EN（End Node，端节点）存在于网络的端点，需要连接到NN（Network Node，网络节点）上，才可以全部接入网络。一个NN和所有连接到它上面的EN称为一个域。NN对于它的域内的EN来说就是一个网络服务器。

当EN需要远端LU的地址时，它可以动态地从NN获得，并将该地址存储在自己的网络地址目录中，以备将来之用。有几种类型的设备，可以作为EN或NN，也可以既作为NN又作为EN。

每个APPN节点包含两种类型的NAU，LU6.2是其中一种类型。另一种称为CP（Control Point，控制点）。一般说来，CP代替PU，并且每个节点只能有一个CP。这个新提出的NAU类型也就带来了一种新的会话类型，称之为CP-CP会话，或简称为CP会话。CP会话是全双工的，需要使用两个并行的半双工LU6.2会话。在节点传送寻址和路由信息时，CP会话是必需的。

NN有两种类型的目录，一种是包含了域内EN和LU信息的本地目录，另一种是含有其他域及其相应LU信息的分布式目录。NN可以确定APPN中两个节点之间的最佳路由。

新旧SNA网络的结合如图16-18所示。两个NN都作为SNA进入VTAM及其资源的网关。EN可以通过这个网关功能和3270终端模拟来与主机LU通信，或者通过作为网络服务器的NN与另一个EN通信。没有人可以预测这种从多个厂商的SNA演变到LAN和基于路由器的网络会带来多少可行的选择。

习题

1. 什么是终端用户?
   a. 只是一个主机应用程序
   b. 只是一个使用接入SNA的终端的人
   c. 只是一个终端
   d. 一个主机应用程序和一个使用SNA的人
2. 什么是远端连接的设备?
   a. 与I/O通道相连接的设备
   b. 与FEP相连接的设备
   c. 与主机相距至少1英里的设备
   d. 与主机相距至少10英里的设备
3. 下面哪一个是通信控制器?
   a. FEP　　b. 调制解调器
   c. DSU　　d. 集群控制器
4. 接入SNA时需要的逻辑网络地址称为什么?
   a. LU　　b. PU
   c. NAU　　d.SSCP
5. 在绑定发生时建立的是哪种类型的会话?
   a. SSCP-SSCP　　b. SSCP-PU
   c. SSCP-LU　　d. LU-LU
6. 下面哪一项是LU的特有特点?
   a. 会话序列号　　b. 虚拟路由
   c. 显式路由　　d. 协议子集
7. 在SDLC中，哪个字段决定了帧的类型?
   a. 地址　　b. 信息
   c. 控制　　d. 编码
8. 下面哪一项不是路径控制层的功能?
   a. 分段　　b. 虚拟路由调步
   c. 在FID 4 TH与FID 2 TH之间的转换
   d. 服务等级
9. 哪个软件部件辅助诸如MVS的主机操作系统与远端终端的通信?
10. 集群控制器中应用最灵活的类型叫什么?

11. 具有一台以上主机运行的网络叫什么？
12. 两个子域节点之间的并行链路的集合称为什么？
13. 虚拟路由是用哪两种类型的路由定义的？
14. APPC提出了哪种新型的会话？
15. APPN提出了哪种新型的会话？
16. 使用一个会话（session），在两个TP间可以有多少个对话（conversation）？
17. 讨论使用FEP的各种不同方法。
18. LU与PU之间的基本区别是什么？
19. PU与SCCP之间的基本区别是什么？
20. 在旧的SNA和新的SNA中是如何定义一个域的？
21. 什么是虚拟路由？它是如何定义的？
22. 讨论一个LEN会话发起的步骤。
23. 用自己的话解释图16-16中的各个项目。
24. 比较分段（segmenting）与记录链锁（chaining）。哪一个基于LU缓冲区的大小？哪一个基于PU缓冲区的大小？哪一个是由PU完成的？哪一个是由LU完成的？哪一个确定了SNF号？哪一个确定了调步窗口？

第17章 X.25

17.1 发展

17.1.1 起源

在20世纪60年代早期，Rand公司的Paul Baran首先将分组交换网络概念化。之后，DoD（Department of Defense，美国国防部）和Rand公司合作开发这种类型的网络用于传送话音和数据。这种网络的传输安全性和容错性深深吸引了DoD。

这种网络由许多交换机或节点组成，这些交换机或节点分布在很广的区域内，是通过租用线路相互连接在一起的。分组交换网络可以分为两大类，在这里我们将逐一介绍。

17.1.2 数据报的概念

最初，Paul Baran在分组交换网中用到的是数据报交换（详见第2章）的概念。DTE（Data Terminal Equipment，数据终端设备）就是诸如远程终端或计算机等终端设备。当一个DTE向连接在网络中的另一个DTE发送消息时，它将把消息分解为小部分，这些小部分就叫做数据报。如图17-1所示，在这些数据报的前面加了个报头，用于提供目的地址、源地址、数据报号和其他的信息。数据报可以通过各种链路发送到网络中。节点通过查看数据报报头和它自己的路由表，依据其目的地址决定将数据报转发到哪条链路或者保持在本节点。

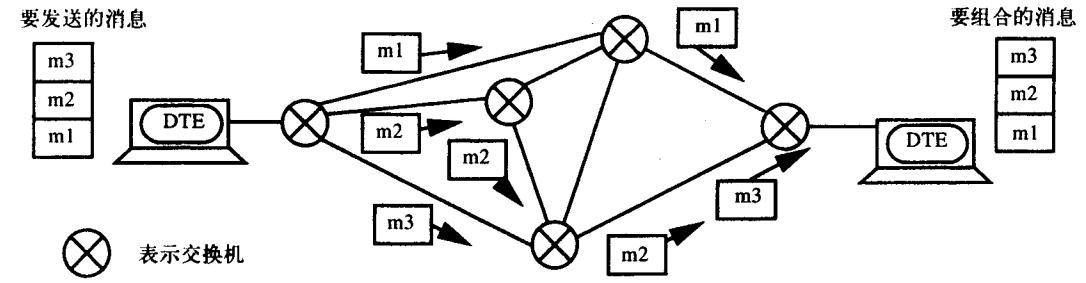


图17-1 数据报进入分组交换网络

如果有人想截获一条链路，他只会得到传送的一个片断，所以在这种网络中安全性得到了增强。当一条链路或者一个节点发生故障或被破坏时，数据流将选择其他的路由，因此该网络不会存在单一故障点。对这种网络的控制被分散到了许多节点上，这与AT&T公司的PSTN（Public Switched Telephone Network，公共交换电话网络）以及后来出现的IBM的SNA数据网络所采用的分层网络结构形成了鲜明的对比。在SNA网络中，如果主机发生了故障，那么整个网络都会瘫痪，但是分组网络对故障就不十分敏感。

在1967年，DoD就开始建设ARPANET（Advanced Research Projects Agency NETwork，美国国防部高级研究计划局建立的计算机网），将全国许多大学和政府部门连接起来。该网络是第一个分组交换网络的试验床，它采用的是数据报类型的协议，速度很快，执行性能可以

达到理论水平。这种网络显而易见的价值得到了认可，因此很快就有许多研究机构开始在这个基本概念上开展进一步的研究。

17.1.3 分组的概念

为了将DTE与分组交换网络相连接，已经提出了许多协议。ITU于1974年将这个接口标准化并称其为X.25。ISO（International Standards Organization，国际标准化组织）也采用了X.25作为其OSI（Open System Internconnect，开放系统互连）参考模型前三层的协议。

X.25在许多方面有别于Paul Baran最初的数据报概念。数据报仍然被用在TCP/IP协议族中，但ARPANET现在运行的还是X.25。X.25应用的是分组，它利用一次呼叫的连接阶段与远端的DTE建立一条链路。绝大多数X.25在呼叫的连接阶段，通过节点和链路选择路径，在数据传送阶段所有的数据都通过这一给定路由传递。这个固定的路由被称为虚电路。与X.25不同，由一条消息形成的数据报根据当时的可用链路来采用不同的路由。当然，由于所有的分组都使用一条路由，因而也就不可能提供最好的安全性。然而，因为呼叫的路由和时间长度已知，所以，连接的费用就与客户使用PSTN那样是可以预期的。你也许还记得我们曾在2.5节和2.6节讨论了X.25与数据报网络在因特网中应用的不同。在本章的其余部分，X.25、分组交换网络和分组网络这几个术语是等同的，会交替使用。

17.2 目的

自从1880年以来，PSTN（Public Switched Telephone Network，公共交换电话网络）就因为其费用低、可靠性高、连接快和质量好而发展成为应用广泛的网络。分组交换网络的基本目标也是如此，但它不是用来传送话音和电话呼叫的网络，它是被设计用来传送数据和实现交互式数据连接的网络。分组交换网络也提供了高质量、高可靠性、低费用连接和快速连接。

PSTN最初只是设计用来处理话音的，但在20世纪50年代人们开始通过调制解调器在PSTN上传递数据。然而，数据的传输被电话系统的模拟设备所限制，因此专门为数据终端与主机的联网引入了分组网络。这些数据终端和主机称为DTE或数据终端设备。

电话网络和分组网络采用的都是网状拓扑结构，这使得终端可以接入其他任何终端，而不管这个终端是电话还是DTE。网状拓扑结构在网络中可以提供高的可靠性，这是因为如果一条链路或者一个节点发生故障，数据流可以很容易地通过其他链路或者节点进行重新路由。

在PSTN中，一旦建立了连接，通话过程中就可以使用任何协议。可以使用英语或者其他语言，数据可以使用ASCII、EBCDIC或者其他协议进行调制。类似地，分组网络可以提供连接（connectivity），两个使用同种协议的端节点可以进行对话。有些时候，可能会对分组网络产生误解，认为它可以进行协议转换，比如说一个IBM的主机可以与DEC的主机进行对话，但实际上分组网络所能够提供的只是连接。诸如协议转换等服务都是由OSI模型中的高层提供的。

现在我们把注意力转移到PSTN与分组交换网络的不同点上来。电话网络本身其实就是一个电路交换网络。这就是说在两个端节点间一旦建立了一个连接，就会有一条专用电路来承载通话，其他任何通话都不能在同一条电路上传送。在分组网络中，两个端节点之间的链路是与其他连接共享的。数据传送的典型分组长度为128字节，这些分组是统计复用到连接通过的各条链路上的；而在PSTN中，数字化的话音是时分复用到交换机中继线上的。统计多路复用已经在3.8节中介绍过了，在此做一个简短回顾。在X.25网络上传输的信息单元是以8比特

或者字节为单位的，而PSTN主要支持4kHz的话音。PSTN和分组网络的另一个主要区别是在PSTN中建立一个长距离连接需要大约10s的时间，而在分组网络中通常只需要不到1s的时间。

17.3 拨号线路、租用线路与分组网络

利用电话网络的拨号上网线路是很容易实现的，并且可以很容易地提供到许多节点的连接，如图17-2所示。用户只需根据连接的时间付费。然而，用模拟线路接入交换机降低了连接的质量，并且数据速率通常被限制在9.6kbps。对于安全性问题，它们是通过主机回呼主叫方以验证其地址（或其电话号码）的方法来解决的。但是这样会浪费时间，并且花销也大。

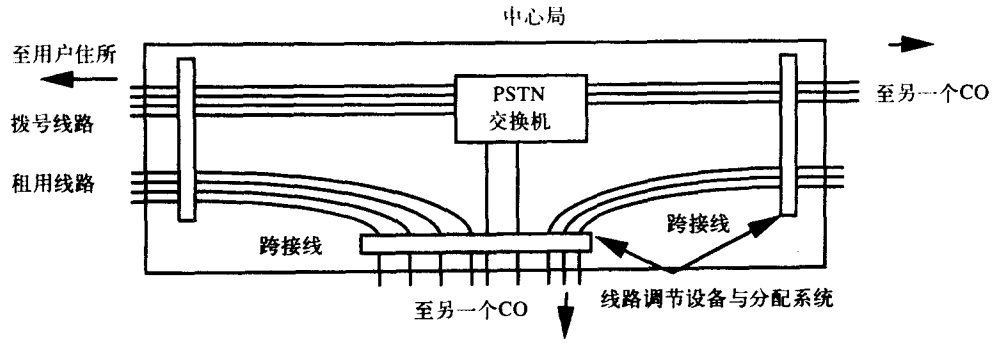


图17-2 在中心局(CO)中安装拨号线路与租用线路的不同。跨接线可用DACS（数字接入和交叉连接系统）代替

另一方面，租用线路可以提供更好的安全性，话音级线路的数据速率也可以提高到19.2kbps。它们并不通过交换机。由于按照24小时进行付费，因此这些线路都用于传送大量的数据流。然而，其价格非常昂贵并且安装起来也很花费时间，并且不会为增加可靠性而提供冗余的路径。你也许记得在5.1节中讲到的这些区别。

如图17-3所示，分组交换网络试图采纳拨号网络和租用线路的优点。分组交换网络的可靠性高于99.9%，即一年内只有几个小时发生中断。如果网络中的一个节点或者一条链路失效，则该网络就会通过其他路由自动“治愈”。这个处理过程不会损失任何数据，并且不会使终端用户察觉到任何故障。它们可以提供高达64kbps的数据速率而误码率仅为10^{-9}，这就是说10亿个比特中只会有一个误码！这使典型的分组网络成为高精度网络。

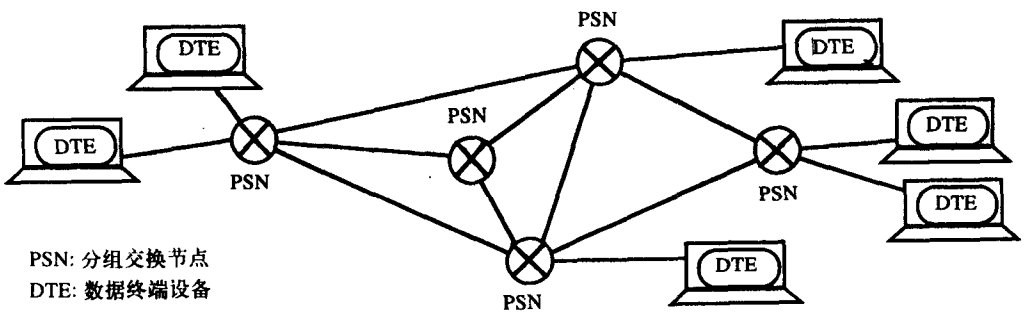


图17-3 分组网络允许位于不同地域的终端彼此通信

许多用户可以共享同一条链路。如果一个用户瞬间停止传送，属于其他通话的数据分组

就可以占用同一条链路。当然，不同用户在同一链路上使用的协议不必是相同的。

分组网络还可以通过各节点的缓冲区来提供速率的转换。意即一个工作在64kbps的主机可以与一个1200bps的终端通话。

17.4 公共数据网络（PDN）

分组交换网络有两种基本类型。私有公司的专用分组交换网络是靠租用线路来连接各个节点的。顾名思义，专用网络只允许一个公司接入和使用，而公共数据网络（PDN）通常对任何公司或者个人都是可用的，就像PSTN对公共话音呼叫都是可用的一样。

在这两种情况下，这些网络是MAN(Metropolitan Area Network，城域网)或者WAN（Wide Area Network，广域网）。MAN将其所有的网络接入点都限制在一个城区的范围内，而WAN则将其区域扩展到许多城市、许多州或者许多国家。例如，纽约电话公司所拥有的Infopath可以为纽约市区的所有用户提供服务。同样，Sprint公司所拥有的SprintNet，即以前的TelNet，对美国的所有用户都是可用的。因此，Infopath可以看作MAN，而SprintNet则是WAN。

PDN在很多情况下被认为是VAN，即增值网络，因为PDN不仅仅提供许多节点之间的连接，而且还提供计算或数据库功能。

在美国两个使用最广泛的PDN是英国电信（British Telecom）的BT Tymnet和SprintNet。还有很多其他公司都提供X.25连接。在法国，Transpac是进入到大部分家庭的电话系统。它提供小型的数据终端用来获得在线号码查询服务，这就省去了电话号码簿的打印和销售问题，并且可以方便地删除旧号码，保持号码的更新。Tanspac还被用在教育上。第一数据资源（First Data Resource）等网络还提供了采用信用卡结算的方式。通过一条连接分组网络中一个节点的专用线路，公司就可以在票据交换所用5到6秒钟的时间获得信用卡结算。

许多国家都至少有一个PDN。在欧洲，PDN归属于PTT（Post Telephone and Telegraph），它是一个类似于美国邮政服务局的政府机构。墨西哥的TELPAC和菲律宾的EASTNET也是PDN的实例。

PDN并不用来传送大量的数据，但对于少量或者中等数量的数据其价格还是十分合算的。它们不是按照呼叫的距离收费，而是按照传送的数据量和连接的时间收费的。PDN具备了典型分组交换网络的所有优点，在专用网络发生了故障或者负荷太大而必须寻找其他路径的情况下，通常可以用PDN代替专用网络。

接入PDN的基本方法有两种，选择哪一种方法取决于PDN具有多大的使用率。如果PDN的利用率很高，则应该在PDN的一个专用端口安装一条租用线路。如果使用率低，就用拨号线路来接入PDN。PDN的拨号端口必须具有足够多的调制解调器来容纳呼叫的用户，否则呼叫方就会被阻塞。

17.5 分组交换网络的运行

17.5.1 什么是分组交换

为了更好地理解分组网络的操作，最好简短地回顾一下统计复用。

采用统计多路复用可能会使链路的速率小于终端速率之和。在设计这一类网络时，总是假定并非所有的终端都同时工作。在图17-4a中，我们可以看到，x1只能与另一端的y1通话，

因此各终端都是与其远端所对应的终端进行通信的。

图17-4b是一个很简单的X.25网络，就是将图17-4a中的统计多路复用器换为分组交换机，也称为节点。这些终端都是与X.25相兼容的。在这个网络中，x1不仅可以与y1通话，还可以与其他任何终端通话，这是因为分组交换机不仅可以提供统计多路复用，还可以实现交换功能。然而，x1必须知道它想通话的终端的地址。节点之间的链路同样是统计复用的，因此链路的速率之和可以小于终端的速率之和。

图17-5中是一个更有用的X.25网络，它具有的许多链路和交换机相互连接成了网状拓扑结构，从而提供备用路由和更高的可靠性。而且，只要地址已知，任何终端都可以与网络中的其他任何终端相连。

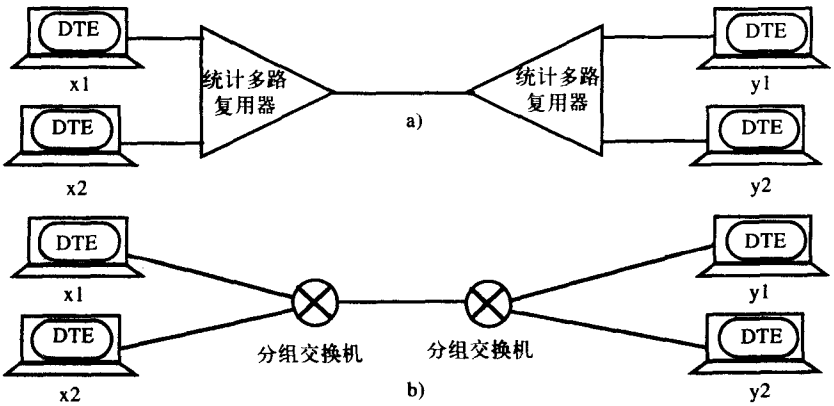


图17-4　a) 在统计多路复用连接中，x1只可以与y1形成链路；b) 在分组交换连接中，x1可以与其他任何终端相连接

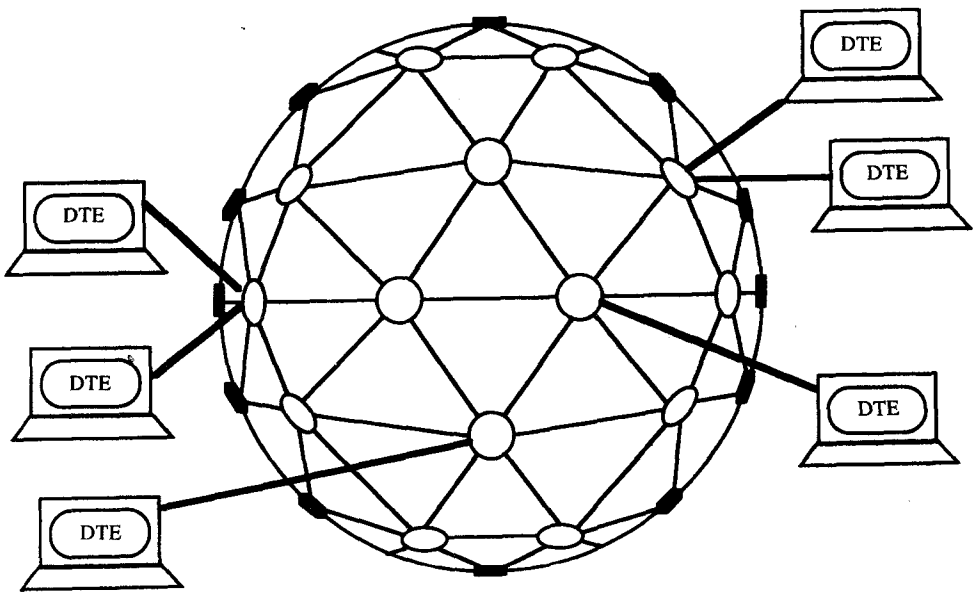


图17-5　分组交换网络提供了许多备用路径

在X.25的术语中，终端被称为DTE（Data Terminal Equipment，数据终端设备）。DTE可

以是数据终端、主机或者数据的其他终端或源端设备。与DTE接口的交换设备部件是DCE，即数据通信设备（有时也被称为数据电路终端设备）。许多情况下，根据它所含有的端口数目，交换机或节点可以作为一个交换机也可以作为一组DCE。分组网络由节点、链路和DCE组成，但是不包括DTE。通常将分组交换网络简称为“云”。

X.25是定义在DCE和DTE之间的标准。没有定义在节点之间的标准，因此通常在这种分组交换网络中，采用一个厂商的设备时，应在云中使用其专用协议。

17.5.2 与X.25相关的协议

许多情况下，DTE并不是与X.25兼容的，在这种情况下必须使用PAD（Packet assembler/disasembler，分组组装器/拆分器）来实现与网络的互连。PAD提供许多端口，这些端口可以是同步的也可以是异步的，这取决于用户接入网络时所采用的终端类型。如果PAD与终端都位于同一个地方，PAD就可以位于终端附近；如果PAD与终端不在同一个地方，PAD就可以和DCE放置在一起。

ITU-T在X.3中定义了异步PAD提供的服务，在X.28中定义了PAD和非X.25终端的接口，如图17-6所示。分组网络可以相互连接，在这种情况下，各网络为了彼此间通信，X.25层的网关是必不可少的。该网关也叫STE（Signaling Terminal Equipment，信令终端设备）。用于STE之间的ITU-T协议是X.75协议。X.121是提供寻址的互连网络之间的正确路由的协议。它规定了国家代码、网络代码和终端号。

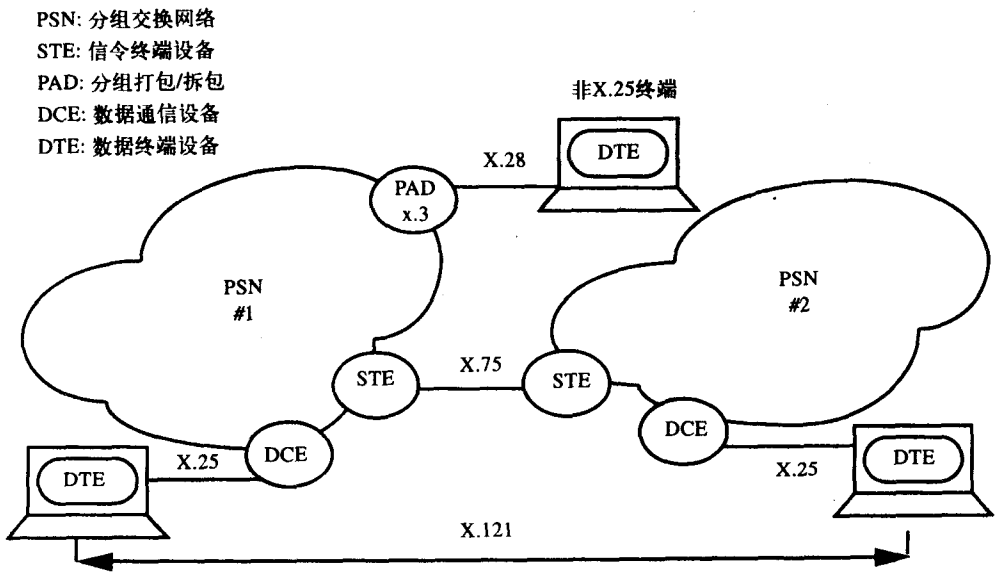


图17-6 ITU的X.25相关协议

国际地址可以长达14位，再加上一个“0”或“1”的可选前缀。在美国，对于国际呼叫而言，前缀为“1”。可选前缀之后的四位数字指明了国家以及该国家中的PDN。这四位数字被称为DNIC（Data Network Identification Code，数据网络标识码）。最后的10位数字标明了附属于那个网络的DTE。通过这种方法DTE就可以和世界上其他PDN中的DTE通信。

例如在国际地址“31101234567890”中，“31”表明是美国，“10”说明了是SprintNet PDN，“1234567890”则为SprintNet中的终端号。

17.6 LAP/B: X.25的数据链路层

在X.25的物理层中，ITU-T建议采用X.21协议。15引脚的连接器中真正用到的只有7个引脚。虽然X.21是X.25协议的一部分，但是用处并不是十分广泛。大多数设备在物理层采用的是EIA的RS-232标准或V.35标准。

对于数据链路控制层而言，ITU-T建议采用与SDLC或HDLC类似的LAP/B（Link Access Procedure/Balanced，链路接入规程/均衡）。SDLC已经详细地介绍过了，就如其中所提到的那样，有三种类型的帧，即信息帧、监控帧和未标号帧。前面已经对信息帧和监督帧作了详细介绍，因为未标号帧要在建立和拆除通信链路时用到，所以现在就来介绍未标号帧。

在数据链路层有三种基本的操作模式。第一种是SNRM（Set Normal Response Mode，设置普通响应模式），用多点协议来执行轮询和选择。第二是种SARM（Set Asynchronous Response Mode，设置异步响应模式），它被用于半双工、点对点操作。最后一种是用于全双工、点对点操作的SABM（Set Asynchronous Balance Mode，设置异步平衡模式）。X.25的LAP/B就采用最后一种操作模式来建立和拆除链路。称一条链路是均衡的，那就是说两个端点都可以发起连接；在LAP/B中这个端点指的是DTE或者DCE。

LAP/B具有5种类型的未标号帧：SABM、UA（Unnumbered Acknowledge，未标号确认）、DISC（DISConnect，断开连接）、FRMR（FRaMe Reject，帧拒绝）和DM（Disconnect Mode，连接断开模式）。UA帧是用来确认SABM或DISC帧的。SABM帧是在连接模式中用于连接DTE或DCE的，而DISC帧是用来断开它们的连接的。如果一个信息帧被发送到处于断开模式的DTE或者DCE，就会回复一条DM以指明接收方没有连接上。在连接模式下只有SABM帧可以获得DCE或者DTE。

如果接收到非法帧，就会发送FRMR帧。这是与监控帧的REJ类型相反的，这表明在所传数据中存在一个错误。如果接收到无效控制域、长度错误的帧、无效Nr或非预期的ACK，就会发送FRMR帧。FRMR还会重发被拒帧的控制域，以通知接收方被拒绝的原因。

这些要点可以总结为图17-7所示的传输交换的例子。DTE发出信息帧，DCE以DM帧应答，

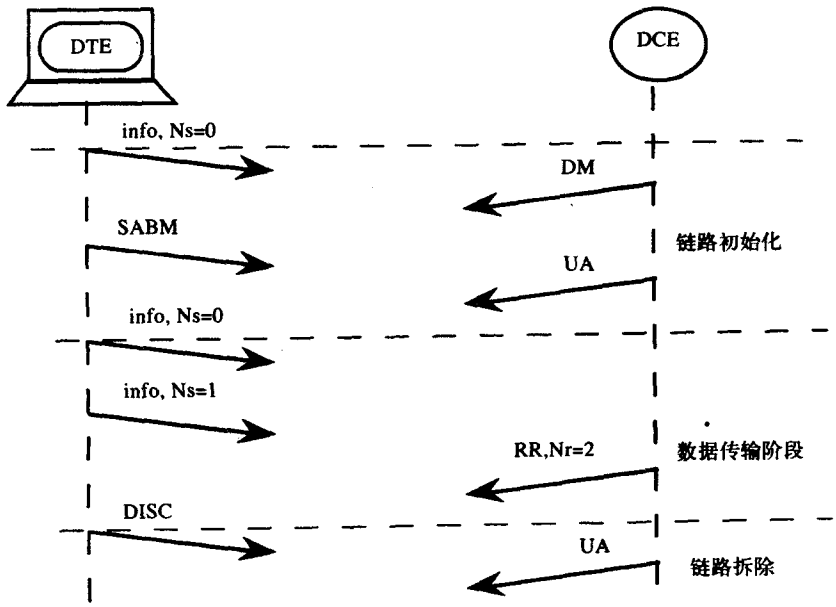


图17-7 DTE-DCE链路上的帧交换

告知DTE现在处于非连接模式。之后DTE就通过发布SABM来使DCE进入连接模式。接着DCE就通过发送UA来完成连接，这样链路就进入了数据传输模式。这里DTE发出了两个标号为0和1的帧。DCE就做出了Nr为2的响应，表明它期望得到DTE标号为2的帧。最后，链路断开。DTE和DCE都可以请求链路断开。

17.7 X.25的网络层

17.7.1 通过层的通信机制

当数据在网络中传送时，它首先要到达如图17-8所示的网络层。网络层通过给数据加入一个头把它封装成分组。之后网络层就把该分组送到数据链路层，在这里可以形成信息字段，数据链路层中的分组就被称为信息字段。信息字段通过加入图中所示的字段来封装成帧。最后，物理层会将实际的比特以合适的速率、使用正确的电压等发送出去。接收端的处理过程正好相反。

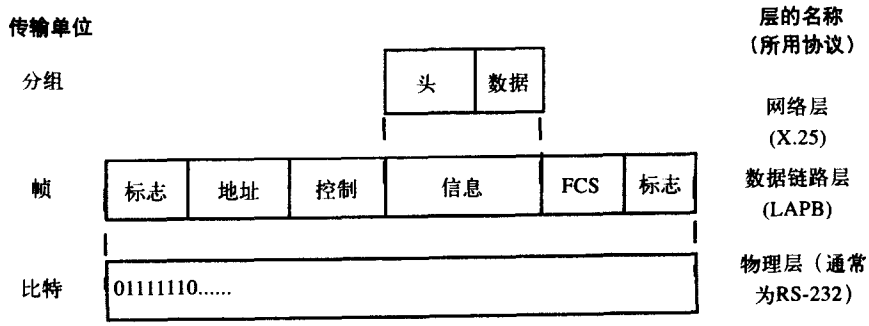


图17-8 X.25的三层

在图17-9中，DTE1给DTE2发送信息。DCE1的物理层将接收原始比特，其数据链路层将在与DTE1的链路上检错和纠错。之后网络控制层会从数据链路层接收到无误的分组。接着从分组头中确定如何路由该分组，这样将分组向其目的地方向发送。选择了链路之后，从DCE/交换机到下一个交换机之间会有同样的操作过程。当分组在网络中传送时，各层的处理过程将在每条链路上重复，直至分组到达目的DTE。在设备或分组交换机之间的每条链路上，物理层发送和接收比特，数据链路层控制链路上的误码，网络层处理分组的路由。

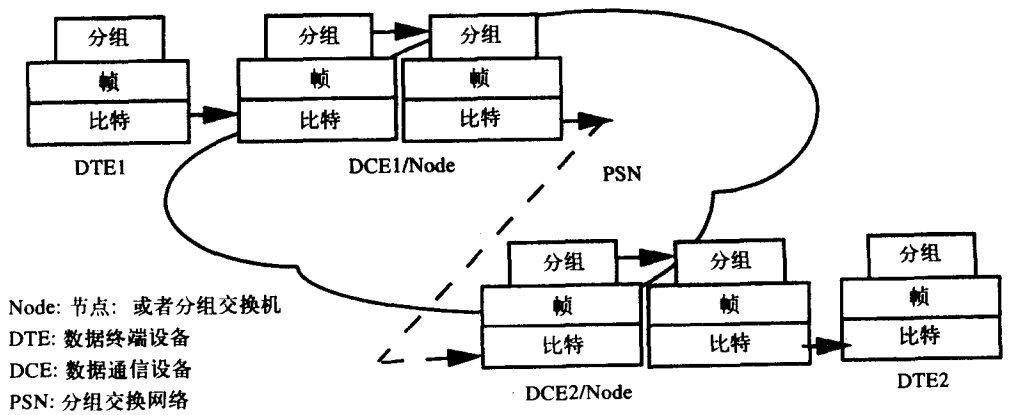


图17-9 分组网络上的数据传输

17.7.2 永久虚电路和交换虚电路

当DTE建立起一个呼叫时，它必须提供远端DTE的X.121地址。交换机可以通过各种可用链路来找到通过网络的路径。这种在PSN（Packet Switched Network，分组交换网）中两个DTE之间的双向连接被称为虚电路。

交换机之间的物理链路是统计复用的，因此这些链路被许多连接共享。每条链路大约有4096条可用逻辑信道，这些逻辑信道可以分配给许多数据通信。逻辑信道由LCI（Logical Channel Identifier，逻辑信道标识符）标识，并在分组头中给出。当交换机接收到了一个分组时，它会根据其LCI将分组路由到合适的链路，并且在另一条链路上改变LCI。

例如，在图17-10中，一个分组交换节点在接收三个分组。它将LCI为1500的分组路由到PSN-A，并将LCI更改为600；将LCI为1000的分组路由到PSN-B，并将其LCI更改为1100。接收到这些分组的PSN继续执行类似的路由过程，因此虚电路不仅仅由其使用的物理链路决定，而且还与它们在各自链路上占用的LCI有关。

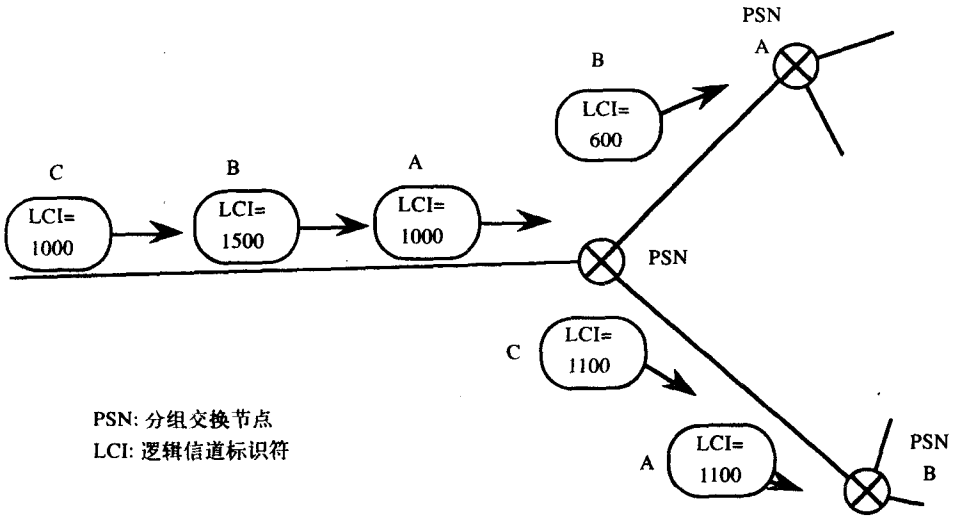


图17-10 分组通过一个交换机时的路由

每个节点都具有一个标明了哪条链路上的哪个LCI路由到哪个新的链路和LCI上的表。新的表项在呼叫建立阶段加入到表中。这个例子是内部节点间链路的一种虚电路实现方法，但事实并非总是如此。

虚电路的类型有两种，一种是PVC，即永久虚电路；另一种是SVC，即交换虚电路。在4096条可用信道中，信道0是用来网络诊断的。剩余的信道分成以下几组：PVC、输入SVC、双向SVC、输出SVC。LCI在呼叫建立时分配，当呼叫断开时释放。

PVC在两个用户之间提供了一条专用信道，不需要呼叫建立阶段。PVC与X.25的带宽需求原理不同，因此它们并没有得到广泛的使用。交换虚电路在两个DTE之间提供了一个临时的逻辑连接，并在发起呼叫时建立。

17.8 分组的类型

17.8.1 分组头

分组有三种类型：数据、流量控制和监测。我们首先来研究数据分组的基本分组头。图

17-11显示了一个典型的6个半字节（即3个字节）长的分组头。第一个半字节是GFI（General Format Identifier，通用格式标识符），后面的三个半字节是LCI（Logical Channel Identifier，逻辑信道标识符）。LCI由LCGN（Logical Channel Group Number，逻辑信道组号）和LCN（Logical Channel Number，逻辑信道号）组成。有意思的是，很多情况下，LCI就被称为LCN。剩下的两个半字节是分组类型标识符。

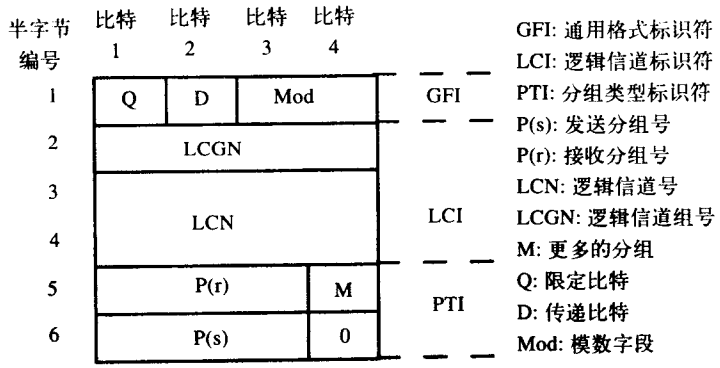


图17-11 三个八位字节的分组头

GFI中的Q比特（限定比特）决定分组是发送到远端的DTE还是远端PAD。D比特（传递比特）指明确认是本地的还是端到端的。

在图17-12中说明了这两种类型确认的不同点。在本地确认中，ACK或RR（Receiver Ready，接收机准备好）是由本地DCE提供的，它证实分组到达了该网络，但不一定到达了目的地。这类似于一个孩子将一封信投入邮筒，回家后说信发出去了，但是并不能确定信是否真的到了目的地。同样地，本地确认只是确定了分组到达了网络，但并没有说明分组到达了目的地。

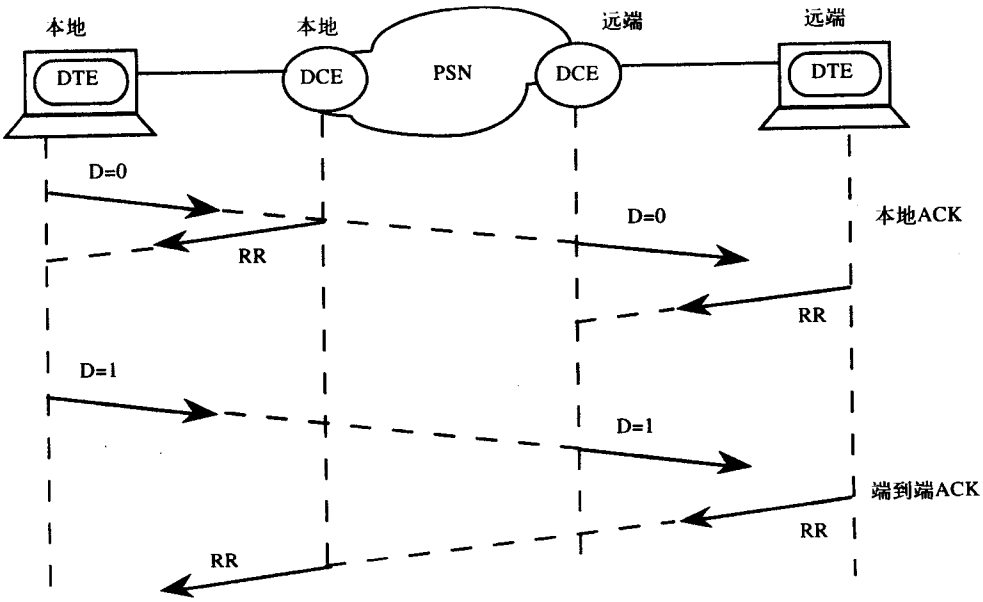


图17-12 本地确认与端到端确认

端到端的确认类似于邮局提供的“返回回执”。在邮局的服务中，这种确认的接收时间长并且花销大。

PTI中的P(s)和P(r)字段，类似于SDLC帧中的N(s)和N(r)字段，不同的是这里的P(s)和P(r)指的是分组号而不是帧号。P(s)是发送的分组号，P(r)是发送方希望从接收方接收到的下一个分组的分组号。例如，一个DTE发送了P(s)为3、P(r)为2的一个分组，这就表明DTE发送的分组号为3，并且已经接收到了来自远端的分组号小于等于1的所有分组。

GFI的模数字段确定传输模式是普通控制还是扩展控制。在普通控制模式下，P(s)和P(r)分别用3个比特表示，如图17-11所示。在扩展模式下，用7个比特表示这两个域。这种情况的分组头与图17-11所示的有所不同，它是4个字节长。窗口大小决定了在不需要响应的情况下，可以连续传送的分组数；在普通模式下，窗口大小为7，而在扩展模式下为127。扩展模式更适于延时比较长的传输，如卫星传输。

长度为4比特的LCGN允许有2^4（16）种LCGN。长度为8比特的LCN允许有2^8（256）种LCN。由于16组中的每一组（LCGN）都有256个信道，因此总共有4096个信道（LCI）。

最后，“more”字段只是用来通知远端是否需要额外的分组。这个字段被更高层用来进行信息单元的分段（即将信息单元分解为更小的单元）和组装。

17.8.2 监控分组

数据分组是在PTI的第8个比特中用“0”来表示的，如图17-11所示。如果PTI的第7比特和第8比特是“01”，则分组的类型就是流控制。流控制分组用来肯定或否定确认传输。

如果PTI的第7比特和第8比特是“11”，则分组的类型就是监控分组。这些分组用来建立和拆除（断开）连接，并且在有问题的情况下暂停电路。

图17-13不仅表示出连接在第三层是如何建立和拆除的，而且总结了最低两层的连接是如何建立和拆除的。现在我们集中关注第三层。

当DTE想要建立一个呼叫时，它就将DTE的地址通过CALL REQUEST分组提供给DCE。当这个分组找到其目的DTE时，该地址就在相应的链路转换为LCI。呼叫一旦建立起来，就不再需要地址，而只需要LCI。当分组到达被叫DCE时，它将会给其DTE发送一个INCOMING CALL分组。之后被叫DTE会给DCE发送一个CALL ACCEPTED分组，主叫DTE就会接收到来自DCE的一个CALL CONNECTED分组。呼叫建立起来后，数据传输就可以开始了。

在数据传输阶段之后，任意一个DTE都可以断开虚电路，这是通过发送CLEAR REQUEST来实现的。在另一端，DTE会收到一个CLEAR INDICATION分组，并发送一个CLEAR CONFIRMATION分组。呼叫拆除的DTE也会收到CLEAR CONFIRMATION分组。

在建立一个呼叫时，如果网络不想接受这个呼叫，主叫DCE就会给主叫DTE返回一条CLEAR INDICATION。如果被叫DTE不想接受这个呼叫，它就会发送一个CLEAR REQUEST分组而不是CALL ACCEPTED分组。

当在数据传输阶段存在异常情况时，有一系列的规程用来暂停电路。首先发送一个RR，请求远端DTE响应。如果没有响应，DTE就会发送INTERRUPT、RESET、CLEAR，再不行时，最后发送RESTART。让我们逐一进行讨论。

INTERRUPT分组是在数据传输阶段发送的，用于获得远端DTE的快速响应。之后，远端DTE必须发送一个INTERRUPT CONFIRMATION分组。该过程使P(s)和P(r)保持同步。

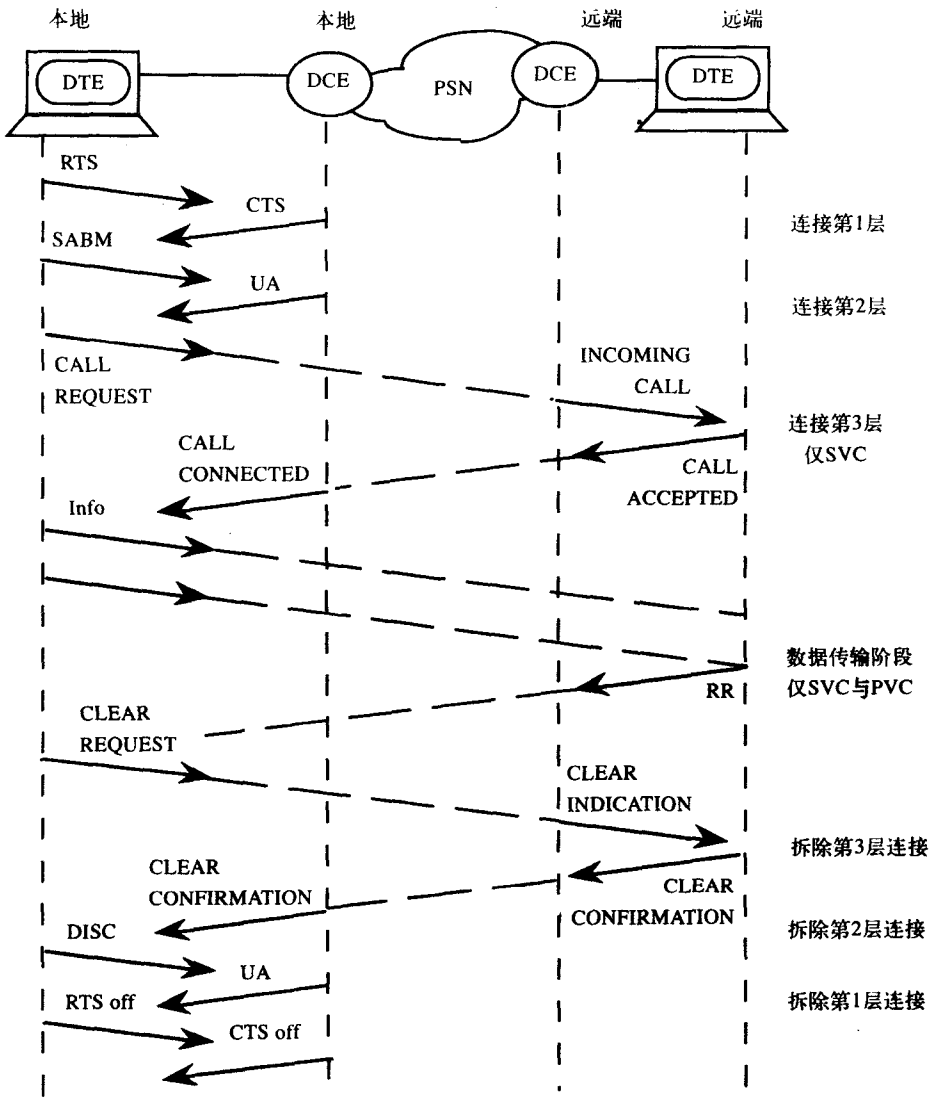


图17-13 利用X.25的三层建立一个连接

如果没有收到INTERRUPT CONFIRMATION，DTE就知道虚电路存在问题，之后它就会发送一个RESET分组。这种类型的监控分组会将P(s)和P(r)计数器复位为零。

如果没有收到来自远端的RESET CONFIRMATION，在电路为交换虚电路的情况下，DTE就会发送一个CLEAR REQUEST。该请求拆除虚电路，并且附属的LCI也被释放了。

如果清除没有被确认，最后的办法就是发送RESTART分组。这个分组会清除与请求DTE相关的所有SVC和PVC。这时所有的临时数据都将丢失，因此主要在电源出现故障时才会这么做。RESET、CLEAR和RESTART分组中都包含了一个指明发送原因的码。

17.9 X.25的特点与功能

与PBX在语音环境下的特点一样，X.25在分组网络中也具有很多特点。这里列举几个有关其特点的例子。

呼出呼叫禁止：这个功能能够限制DTE发起呼叫。

呼入呼叫禁止：这个功能限制DTE接收呼叫。

封闭的用户组：这个功能是在一个大型的公共网络中建立了一个虚拟网络，DTE只能与同组的其他DTE进行对话。但是，一个DTE可以属于几个这样的组。

快速选择：这个功能用于信用卡授权。数据在CALL REQUEST分组中发送给主机，提供信用卡的卡号、购物的数量等。主机会立即发送一个CLEAR REQUEST分组，而不是CALL ACCEPTED分组，来认可是否购买。这里并没有用到数据传送阶段。

呼叫转移：类似于PBX中的呼叫转移，这个功能允许DTE将其接收到的呼叫转移给其他的DTE。

受话人付费：类似于对方付费电话，DTE可以在分组网络中改变费用的负担。PDN的拨号端口广泛地利用了这个特点。

17.10　X.25网络与IBM网络的互联

众所周知，IBM是最主要的计算机设备厂商，SNA（System Network Architecture，系统网络体系结构）是IBM用于组建其计算机网络的专用协议。在商业界，SNA网络有着广泛的用途。连接SNA网络的传统方法是利用租用线路作为主链路，拨号线路作为备用链路。然而，公共或者专用分组交换网络提供了一种连接SNA网络链路的更好的办法。分组网络更不易发生故障，可以提供最好的传输质量。鉴于连接的费用将由许多用户共同分担，所以并不昂贵。因此，许多组织都选用X.25作为骨干网来运行它们的SNA网络。

我们现在来介绍互联的三种方法。

17.10.1　在X.25上实现SNA的软件方法

图17-14给出了将SNA与X.25网络互联的一种方法，它是通过使用一种叫做NPSI（NCP Packect Switched Interface，NCP分组交换接口）的软件包来实现的。NPSI是在前端处理器，即3725或3745中的NCP（Network Control Program，网络控制程序）中运行的。NPSI将SNA单元封装成X.25分组。NCP将包含RU（Request/response Unit，请求/响应单元）和SNA头的PIU（Path Information Unit，路径信息单元）发送给NPSI，这样就给PIU加上了分组头和尾。这就为分组网络准备好了数据。将数据或者RU封装到PIU，再把它放入分组中，这叫做双封装。对来自网络的分组的处理过程与此相反。

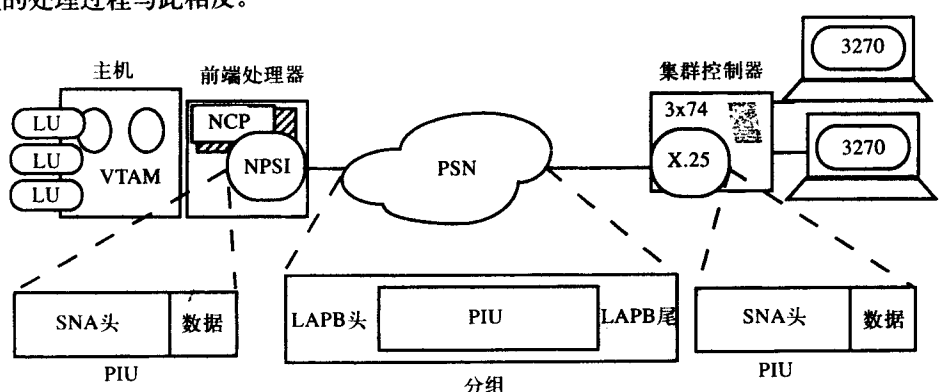


图17-14　利用NPSI在X.25上运行SNA

由于分组中不仅包含X.25头而且还有SNA头，因此可以发送的数据的最大长度就变小了。这就意味着要发送和接收更多的分组。因为这个原因，3725的性能降低了30%，3745的性能降低了15%。我们可以通过将分组长度由128字节增加到256字节来改善它们的性能。

同样地，在后面的电路中，一个X.25接口包能够合并在集群控制器中。就其功能上来说，这个包与NPSI是相同的，但它是为类型2的节点设计的。

只需在两端简单地增加合适的软件，分组网络就可以用来传送SNA数据流了。这使得用户既可以保留在SNA设备上的投资，又可以获得分组网络的优势。虽然LU交换通常都是由SNA完成的，但是，采用这种软件方法，也可以使用PU交换。回顾前面讲过的内容，PU交换允许集群控制器中的每个人都可以接入一台主机上的唯一一个应用程序，而LU交换则允许集群控制器中的每个人可以接入任意主机中的任意应用程序。

17.10.2 硬件方法

解决SNA-X.25互连问题的硬件方法如图17-15所示。在主机一侧，主机PAD（即HPAD）被连接在FEP与网络之间。同样地，终端PAD即TPAD被连接在另一端。虽然这需要额外的单元和线缆，但是这比使用NPSI方法的花销小得多，并且被广泛采用。这种方法的一个主要优点在于它没有使FEP过载。就像前端减轻主机通信相关操作的负担一样，HPAD将FEP从组装和拆分分组的工作中解脱出来，从而使FEP的注意力只集中在SNA协议上。采用NPSI时，如果通向网络的线路质量变差，那么，前端的性能将急剧下降。HPAD负责进行纠错，并使前端不再从事这项工作。

HPAD还可以改善主机的处理时间。它们提供了更好的网络管理性能和LU交换。如果预先进行适当的规划，则诸如增加、减少PU或集群控制器等网络的变动就变得十分容易了。

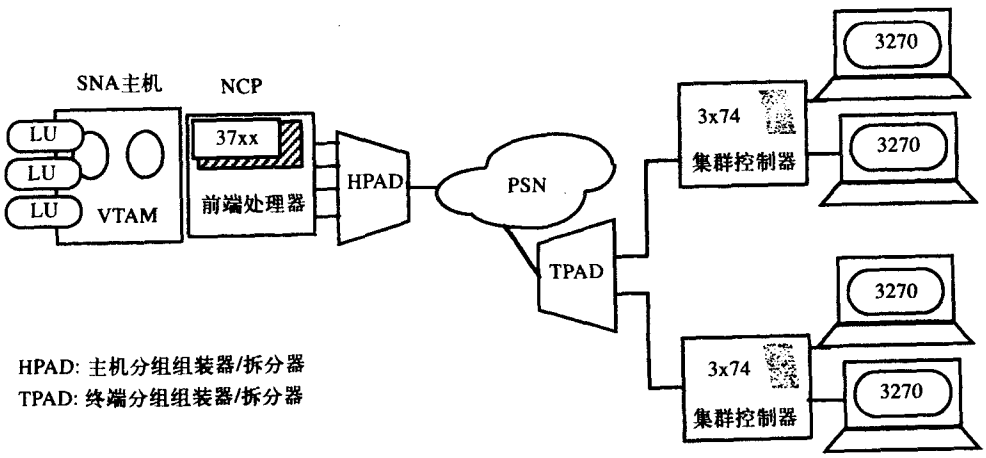


图17-15 利用PAD在X.25上运行SNA

TPAD和HPAD在功能上都是互补的，但它们是为末端电路设计的。TPAD提供本地轮询，因此只有有效负荷通过网络。TPAD可以和位于主机端的NPSI共同使用。

通过使用QLLC（Qualified Logical Link Control，合格逻辑链路控制），软件方法和物理方法可以合并在一个网络中。这个协议可以与NPSI共存，并且可以存在于PAD中。QLLC分组在X.25网络上传送SDLC命令和响应，这些命令和响应可以在端点处转换为SDLC等价帧。

17.10.3　XI方法

另一种由美国IBM公司在1988年提出的在SNA上互连X.25的方法称为XI（X.25与SNA互连）。前面我们曾经提到过X.25协议是定义在DTE和DCE之间的，并且用在DEC和交换机之间的协议通常是专用的。如图17-16所示，这个与XI共同使用的专用协议是SNA的SDLC，DTE和FEP之间的接口仍然是X.25。使用XI涉及到使用由FEP和SDLC链路连接的分组网络。所有的DTE都必须与FEP相连。XI位于FEP的NCP下面，所有的分组都必须通过XI。一个XI副本最多可以提供256个DTE接口。

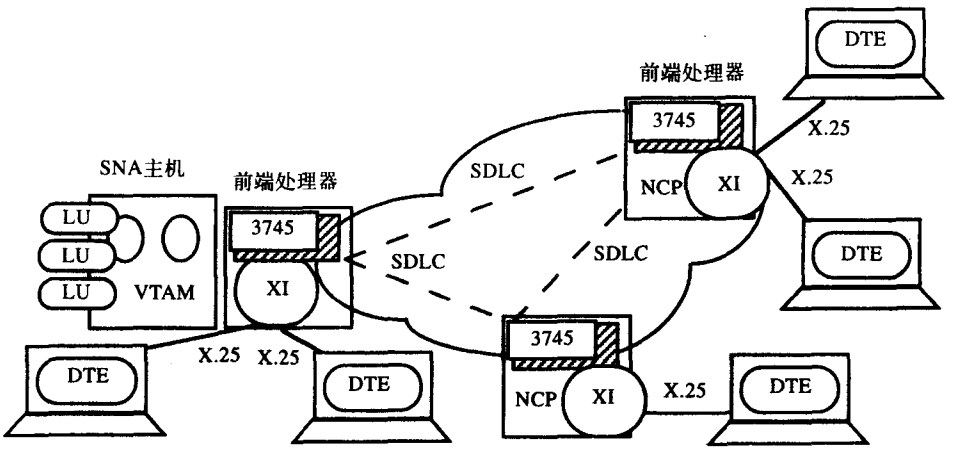


图17-16　利用XI在X.25上运行SNA

在各种FEP或XI节点之间存在单个的LU-LU会话，这些单个LU-LU会话就在X.25虚电路上多路复用。由于会话不必动态地产生和终止，因此，这样做可以改善性能。虚电路通过已经可用的会话传递。分组的大小可以达到1024个字节，这也改善了FEP的性能。XI还支持IBM公司用于网络管理的NetView。

最近，第三方厂商已经采用通信处理器来代替37x5 FEP，这些FEP看上去像主机的类型4的节点。这些处理器在设计时都考虑到了X.25，因此SNA/SDLC和X.25的功能重复被最小化，并且为SNA提供了非分层结构。

17.10.4　在BSC网络使用X.25的优势

在研究前SNA（pre-SNA）双同步或者BSC网络时，X.25的其他优势是显而易见的。在图17-17a中，BSC主机与一个半双工多点终端相连。典型模拟线路的最高速率是14.4kbps。轮询是由FEP完成的，这会带来很大的延迟。由于在一个时刻，主机只能支持一台设备，因此主机没有得到充分利用。

在分组网络的两端都插入BSC的PAD，如图17-17所示，传输就可以成为全双工的。只有从FEP到HPAD以及从TPAD到终端的传输是半双工的，这些地方都不是链路的关键部分。通过分组网络的速率可以从14.4kbps升到64kbps。由于轮询是由TPAD在本地完成的，而不是通过整个网络完成的，因此轮询延时也被最小化。现在终端也不再限制在一台主机的一个应用程序上了，由于TPAD提供的LU交换，它们可以同时接入任一主机的任一应用程序中。从SDLC骨干网中我们也可以得到类似的优点。

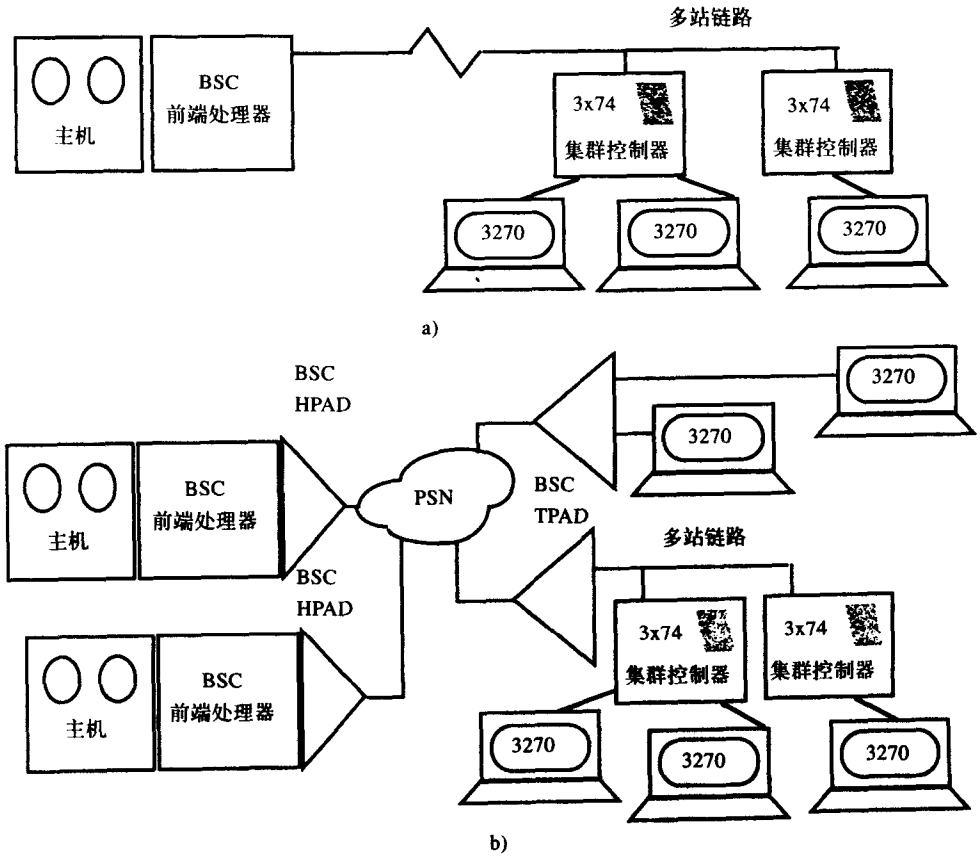


图17-17 a) 典型的BSC网络，b) 在分组交换网络上实现BSC网络可以带来很多新的优势

习题

1. PDN也被称为什么?
   a. LAN　　b. MAN
   c. VAN　　d. WAN
2. 分组交换网络并不提供
   a. 可靠性　　b. 安全性
   c. 低花费　　d. 高传输速率
3. LAP/B利用以下哪种类型的传输模式?
   a. SNRM　　b. SARM
   c. SABM　　d. SNBM
4. 以下哪个字段决定了请求的确认应答的类型?
   a. P(r)和P(s)　　b. mod
   c. Q 比特　　d. D比特
5. 呼叫请求分组在接收端变为了什么类型的分组?
   a. 呼叫接受　　b. 呼叫连接

c. 呼叫确认　　d. 呼入呼叫

6. 在哪种类型的X.25和SNA的互联方式中，需要把SDLC用作网络中节点间的链路协议？

a. NPSI　　b. HPAD-TPAD

c. XI　　d. BSC方法

7. 哪个协议定义了两个不同的分组网络之间的接口？

a. X.21　　b. X.3

c. X.75　　d. X.121

8. X.25的哪个特点不允许用户建立任何呼叫？

a. 呼出呼叫禁止　　b. 呼入呼叫禁止

c. 受话方付费　　d. 呼叫转移

9. X.25标准是由哪个组织制定的？

10. 哪种类型的线路可以使每月的费用变得适中？

11. 在LAP/B中，哪个帧是对DISC帧的确认？

12. 当一个呼叫通过分组网络在两个端节点之间建立起来的时候，网络中各链路之间的目的地址被转换为什么？

13. 哪个分组是用来发起两个端点之间链路的拆除的？

14. 分组头中哪个字段是用来确定窗口大小的？

15. NPSI在哪个设备中、哪个协议下运行？

16. 在分组网络上运行的BSC网络中，终端轮询是由哪个设备完成的？

17. 讨论使用数据报和分组的区别。

18. 讨论拨号线路和租用线路之间的区别。在分组网络中存在这些优点中的哪些？

19. 分组交换和统计复用的相同点和不同点是什么？

20. 列出与X.25相关的协议并说明各自的功能。

21. 解释说明分组是如何通过一个网络的。给出每层的功能。

22. 画出传输扩展模式的四字节分组头，并说明窗口大小是127，而分组数是128（0到127）的原因。

23. 描述在X.25网络中没有收到远端响应时所发生的一系列事件。

24. 使用NPSI传送SNA数据流的优缺点是什么？使用HPAD和TPAD呢？

第18章 SS7

18.1 概述

在第9章中，我们向大家介绍了各种信令，包括单条中继线（per-trunk）与公共信道局间信令（Common Channel Interoffice Signaling，CCIS）的区别。本章继续介绍CCIS，尤其是SS7。学习完第11章后，读者应该对SS7有了基本了解。在北美被广泛应用的版本称为CCS7（Common Channel Signaling number 7，7号公共信道信令），它与ITU-T 的版本SS7稍有些差别。日本亦有自己的变体（这些变体的主要区别在于节点代码（point code）的长度和MTP。ITU-T的节点代码长度为14，美国采用的节点代码长度为24，日本则为16，稍后我们将对这些术语作更详尽的解释）。虽然下面的讨论主要基于CCS7，但我们仍称之为SS7。然而，当通过国际边界时应采用ITU-T的版本。所有这些版本将来总会有一天融合在一起。

18.1.1 优点

SS7是分组交换网络中话音网络的一个应用实例，它拥有第17章中所讨论的分组交换的许多优点。除了这些优点以及第9章中提到的CCIS的优点以外，我们再介绍几个优点。

SS7最大的特点便是灵活性。由于这种信令用软件驱动来代替电子-机械驱动，因此通过修改软件并向网络中所有节点发送备份就能够实现新的性能。这比每引入一个新的信令功能便要为所有位置重新设计信令接口容易得多。然而，SS7不利的一面是其程序代码相当复杂，并且程序中的一个小缺陷就会导致一个国家某地区的所有通信瘫痪。

SS7允许IXC、LEC、国际运营商，将来甚至是大型专用网络的设备采用一种标准语言彼此对话。这允许用户使用一个800号码根据一天中的不同时段、通信量或收费结构，在不同IXC的网络中路由呼叫。用户能够管理直接与运营商的信令网络相互影响的自己的数据库。简言之，SS7为用户开辟了一个广阔选择空间。

SS7出现在ISDN和OSI之前，已经被选作运营商网络交换机之间的接口。SS7提供了许多ISDN无法实现的功能，并因此成为实现ISDN的必要条件。这样ISDN就成为SS7的一种用户应用。最后，SS7提供了管理信号，这使网络的维护、监控和管理变得更容易。

图18-1给出了各种不同的信令系统是如何共存于一个现代数字环境中的。在终端用户与

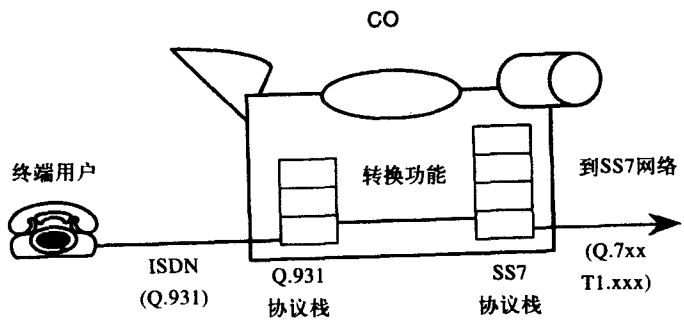


图18-1 终端用户（subscriber）用ISDN传输信令，位于CO处的数字交换机是SS7信令网络的用户（user）

本地CO之间，ISDN或DTMF可以用作信令。Q.931是规定用户的ISDN信令的标准协议，这些协议在CO处被转换成SS7。应该记住贯穿本章的SS7与用户（subscriber）无任何直接接口。另外，"用户"（subscriber）是指电话用户，而"用户"（user）是指SS7节点，例如CO处的数字交换机。

18.1.2 历史

在SS7之前，ITU-T已经规定了其他的信令系统，而且它们在欧洲比在北美洲应用得更普遍。SS1专门用于手工操作的振铃呼叫（ringdown）电路，即一个电话只能与另一个电话相连接。因此，当该电话振铃时，只能是同一个电话在呼叫它。SS2将600Hz和750Hz音频信号用作监控和寻址信令。SS3专门规定了一种2280Hz信号，在功能上类似于2600Hz的SF音频信号。SS4（使用2040Hz和2400Hz）与SS5（使用2400Hz和2600Hz）均为SS3的不同变体。

上述5种信令系统均采用CAS（Channel Associated Signaling，随路信令）。CAS就是我们所说的单条中继线（per-trunk）信令的正规术语。之后在1976年，北美网络中出现了SS6。它在信令网络中采用2.4kbps的数据链路，后来加倍为4.8kbps。它可以提供800号码服务，并且是为模拟话音网络所设计的。

而在20世纪80年代末，SS7被IXC所采纳，它采用56/64kbps的信令链路，并且需要在语音网络中使用程控数字交换机。

18.2 拓扑结构

18.2.1 节点类型

图18-2给出了SS7网络中的节点类型，它们可分为SP（Signaling Point，信令节点）和STP（Signal Transfer Point，信号传输节点）两类。SP可以考虑作为网络分组、呼叫信息产生和结束的终端节点；而STP则是分组交换机，它将信息路由到正确的目的地。

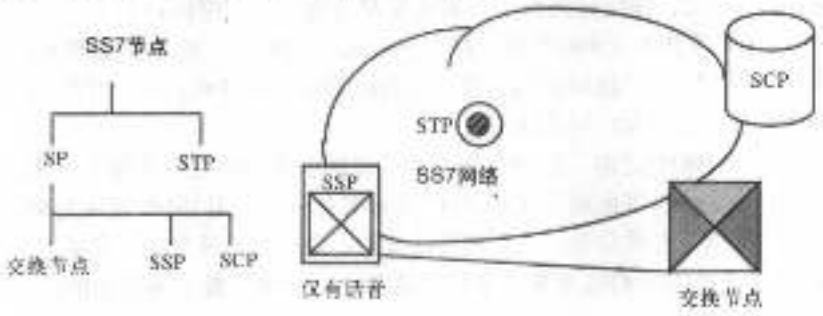


图18-2　SS7节点的类型

SP又可进一步分为交换节点、SSP（Service Switching Point，业务交换节点）和SCP（Service Control Point，业务控制节点）三种类型。其中交换节点是指数字交换机中的硬件和与其相关的软件，它用于将外部的信令协议如ISDN或DTMF转换成SS7格式的消息，以便STP进行译码。交换节点是4ESS、DMS-250或其他如SS7网络中数字交换机的组成部分。其他与SS7不兼容的交换机可以通过SSP接入智能网络。

最后，SCP是一个数据库系统，用于信用卡认证、虚拟网络的用户记录、计费信息、800号码转换表以及其他特殊服务功能。SCP服务可通过一个独立的交换机获得，或通过一个与STP相连的智能外设提供，也可以作为SSP/STP上的附属处理器。

18.2.2 链路类型

图18-3中给出了三种类型的SP与STP相连接的情况。STP成对使用，并且共享它们之间的传输负载。相互连接的两个STP对称为STP四元组。

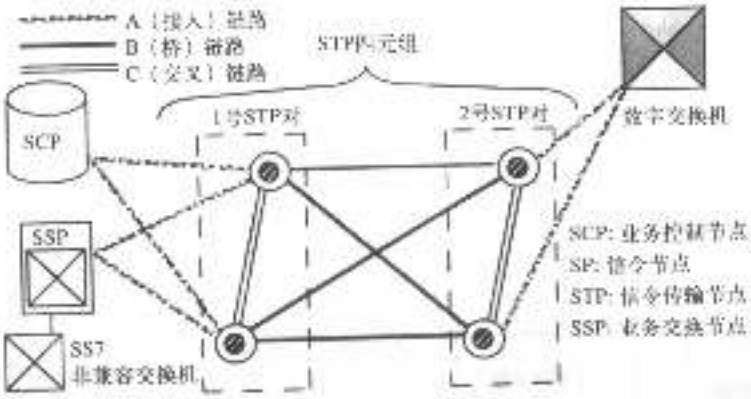


图18-3 STP四元组配置，给出了三类SP和它们之间的信令链路

从各SP出发都有两条链路与一个STP对相连接，这种链路称为A链路或接入链路。同一对中的STP的连接是通过C链路或交叉链路实现的。由于两个STP之间的流量由两条链路共享，因此其中一个出现故障时，另一个有足够的容量承担全部流量负载。

每对中的每个STP与另一对STP之间的链路称为B链路（桥链路）。信令网络中所有部件的冗余使得该网络不容易出现故障，即使网络中的一半设备和链接出现故障，整个网络仍然能够保持运行。

图18-4所示为一个更通用的网络，在该网络中，信令链路被完全集成在IXC与LEC网络之

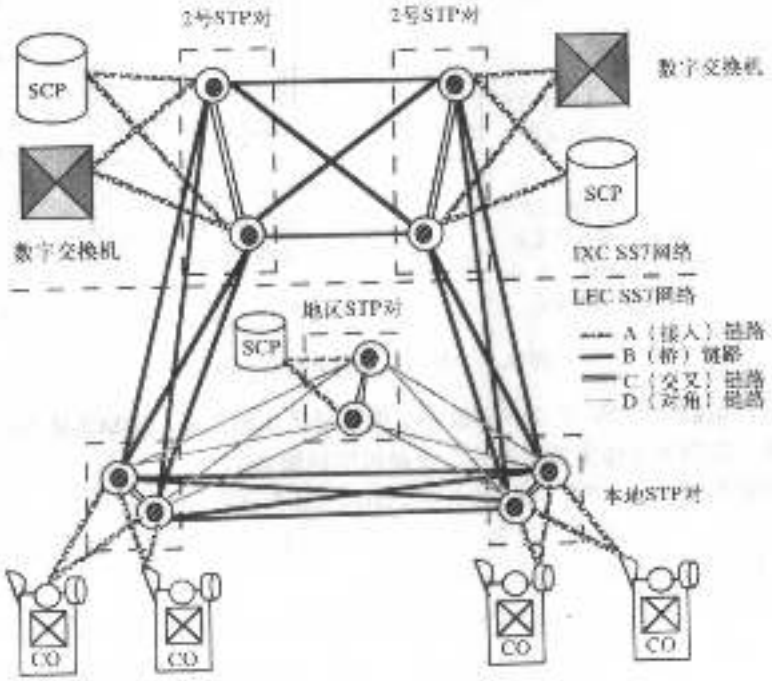


图18-4 LEC和IXC同完全互联的SS7网络

间，注意LEC网络中的地区STP对比本地STP对高一层。本地STP对和地区STP对分别称为次STP和主STP。这两类STP对之间的链路称为D链路或对角链路。

18.2.3　AIN

图18-5给出了AIN（Advanced Intelligent Network，先进智能网络）的功能框图。在分布式环境中，智能网络利用SS7提供数据库、服务逻辑和使用中的辅助功能。图中给出了这类网络中的各个部件。

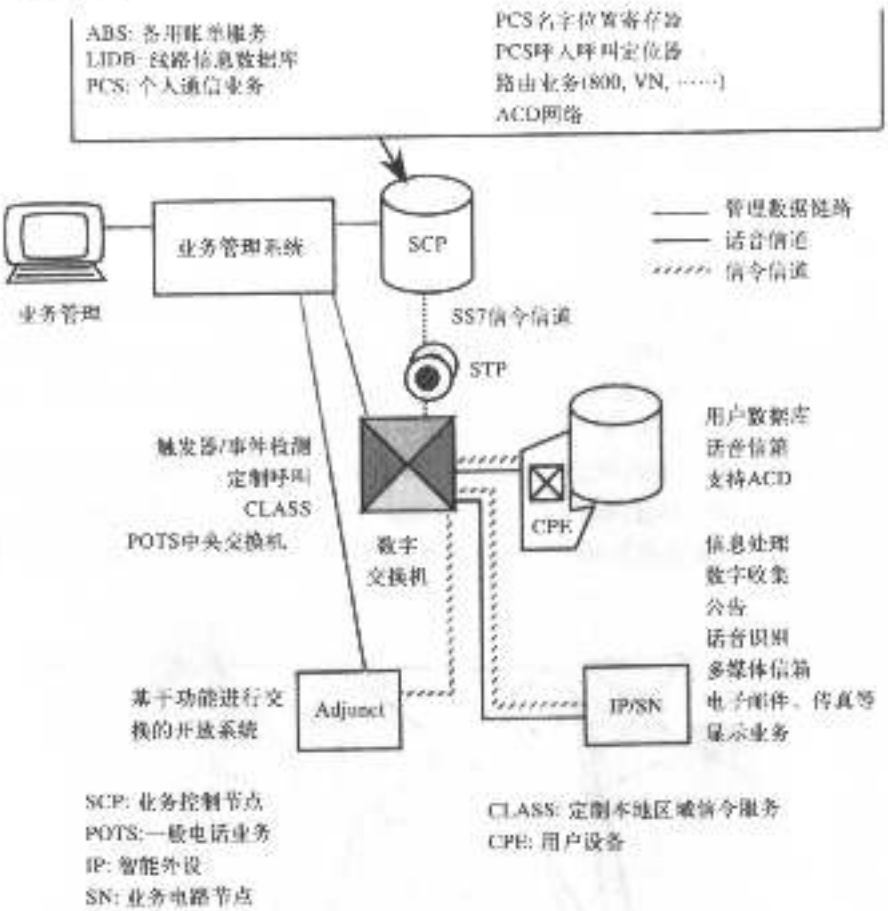


图18-5　AIN（先进智能网络）体系结构

附属部件类似于SCP，它为AIN数字交换机提供本地服务。但SCP是为众多交换机提供集中式数据源，而附属部件主要仅为一个交换机提供服务。

在其他服务当中，IP/SN（Intelligent Peripheral/Service-circuit Node，智能外设/服务电路节点）提供公告、话音合成与识别，以及传真的存储与转发服务。这些服务均提供给附属部件和SCP。IP/SN可通过ISDN连接至AIN交换机。

ABS（Alternate Billing Service，备用账单服务）允许用户使用受话方付费、第三号码计费和信用卡付费。相关细节的信息均存储在LIDB（Line Information Data Base，线路信息数据库）中。CLASS（Custom Local Area Signaling Services，定制本地区域信令服务）为用户

提供以下七种服务：回答呼号、优先呼叫、重复呼叫、选择转发、呼叫部件（call block）、主叫ID和电话跟踪。

在处理呼叫的过程中的触发允许交换机查询SCP。触发的例子：如当用户回电话或虚拟网络号码被呼叫时。最初建立的仅用于路由800呼叫的简单的信令协议，很快就会被用于执行更复杂的服务。

18.3 SS7协议结构

18.3.1 与X.25的比较

在X.25中用户通过PDN（Public Data Network，公共数据网络）的DCE与DTE相接。与SS7类似，用户的电话或PBX与一交换节点连接。在X.25两个终端DCE之间传输数据时将先建立一个虚电路。类似地，在SS7两个终端SP之间有一个虚连接，称之为SCCP（信令连接控制部分）连接。我们与X.25的DCE类似的SP提供了进入SS7网络的输入节点。另外，STP与X.25的分组交换机很相似。

SS7网络中的各网络节点都有各自唯一的PC（Point Code，节点代码），用来给出节点的地址。这些PC由SS7的SCCP层实现，这与X.25中第三层地址的实现类似。

18.3.2 结构分层

图18-6给出了SS7的四个层次及其各个子层，同时还给出了传输单元及其头部。图中各项将在本章其余部分予以介绍，所以在这里无须完全理解这些内容。该图给出了SS7的四层如何映射到OSI的七层。SS7的第一层称为MTP-L1（Message Transfer Part，Level 1，消息传输部分，第1层）或信令数据链路。该层类似于OSI的物理层，它规定了信令链路的电气性能和物理性能。

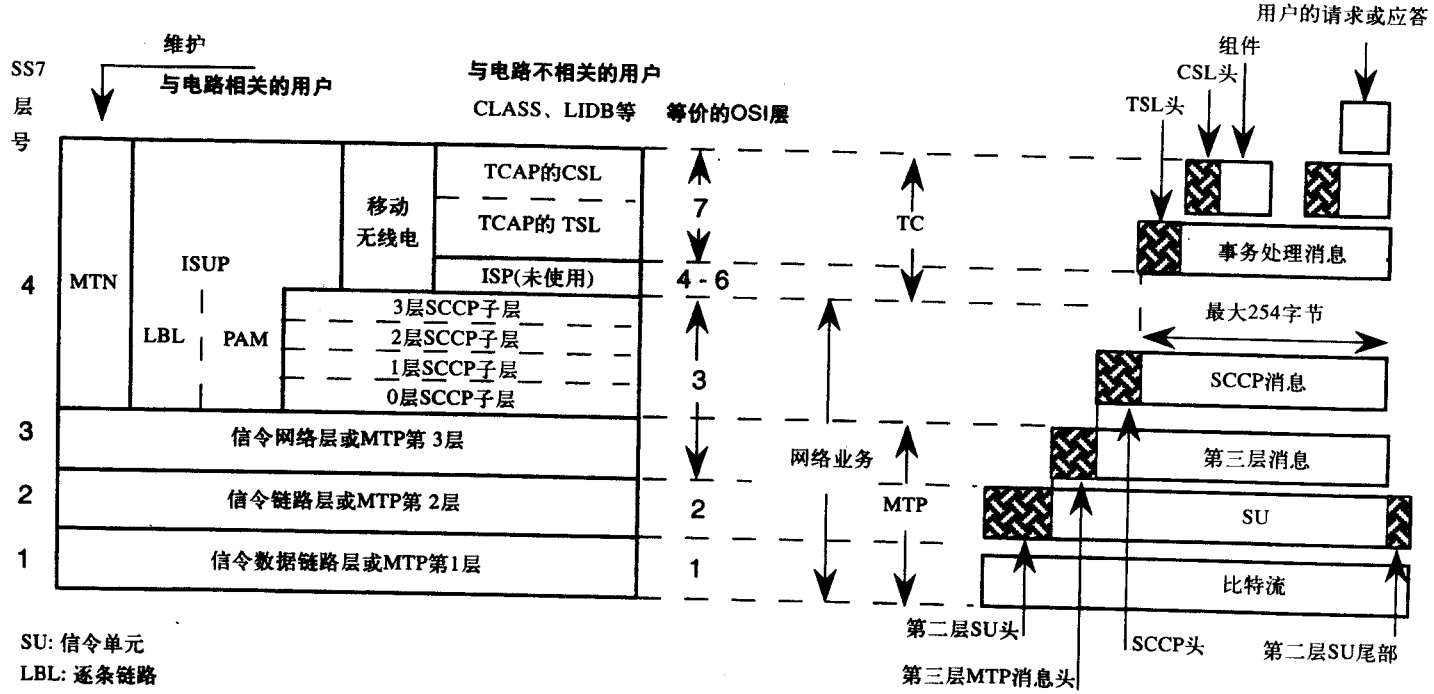
第二层简称为信令链路层或MTP-L2，它提供了信令链路的检错和纠错功能。MTP-L3也称为信令网络层，它接收来自信令链路的消息，在检测完节点代码之后，决定是将接收到的消息路由到另一个链路还是提交给本地的第四层。

SCCP是第四层的最低子层，提供基于随选机制的消息流控制和顺序控制。它与MTP共同提供与OSI模型中的前三层功能相同的完整的网络服务。

第四层的其他部分纵向可分为两类，一类称作ISUP（ISDN User Part，ISDN用户部分），用于端到端的呼叫，例如简单的电话呼叫，它提供了两个端用户之间的信令信息传输；另一类称为TCAP（Transaction Capabilities Application Part，事务处理应用部分），它通常需要一个给SCP的呼叫，从而可以为ISUP呼叫获取路由信息，例如将800号码转换成POTS号码就是一个TCAP呼叫的例子。因此，ISUP呼叫需要与电路相关的功能，而TCAP呼叫则需要与电路不相关的功能。

ISUP和TCAP还可以进一步划分出其他功能。ISUP可以通过采用LBL（Link-By-Link，逐条链路）信令方法、传输PAM（Pass-Along Message，直通消息）信息或使用SCCP消息来与MTP-L3交换信息。由于ISUP不总占用SCCP，因此图中将其“切断”，而并不占用ISUP的全部子层。

TCAP可分为CSL（Component SubLayer，组件子层）和TSL（Transaction SubLayer，事务处理子层）两个子层。TCAP实际上是TC（Transaction Capabilities，事务处理功能）和ISP（Intermediate Signaling Part，中间信令部分）的子层。然而，由于现在还没有定义ISP，故认为TC与TCAP是类似的，稍后对它们进行说明。



SU: 信令单元
LBL: 逐条链路
ISP: 中间信令部分
PAM: 直通消息
ISUP: ISDN用户部分
MTP : 消息传输部分
SCCP: 信令连接控制部分
TCAP: 事务处理应用部分

TC: 事务处理功能
TSL: 事务处理子层
CSL: 组件子层

MTN: 维护
LIDB: 线路信息数据库
CLASS: 定制本地区域信令服务

图18-6 SS7分层体系结构与传输单元

18.4 信令单元

SS7中的帧称为SU（Signaling Unit，信令单元）。与HDLC中有三种类型的帧一样，也有三种类型的SU，但它们的功能并不是对应的。图18-7给出了SU的各种类型。

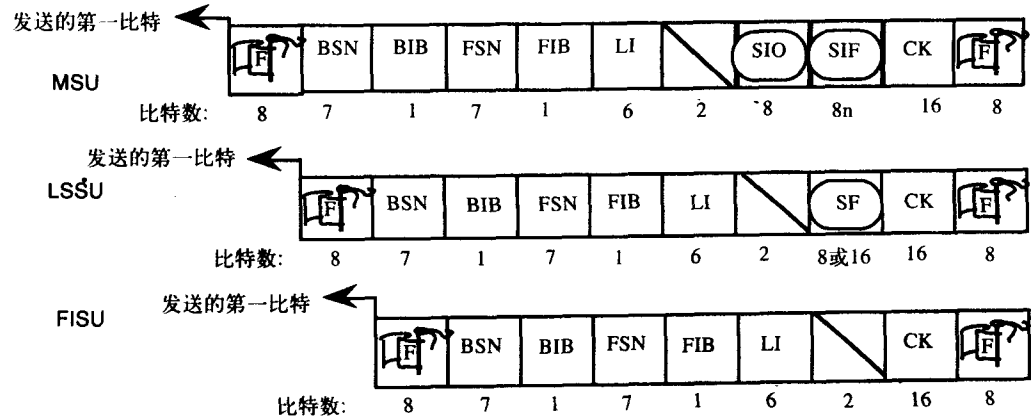


图18-7 三类信令单元，每一类信令单元所特有的唯一字段用阴影表示

MSU（Message Signal Unit，消息信令单元）封装或承载来自上层的信息。它也用来建立和终止连接并且提供用于网络管理的状态信息。LSSU（Link Status Signal Unit，链路状态信令单元）也提供关于链路的状态（如链路是否阻塞，或者是否需要调整等等），但是并不包含任何来自上层的信息。当链路空闲并且不传送任何信息时发送FISU（Fill-In Signal Unit，填充信令单元），这样接收端就知道另一端空闲但可用。

18.4.1 SU字段

SU的第一个和最后一个字段为标志字段‘01111110’，这就要求其余的字段进行比特填充，从而保证在中间位置不出现标志字段。但这一层比较活跃，并且在连续发送的帧之间只有一个标志字段。

LI（Length Indicator，长度指示器）用8比特规定了MSU的SIF（Signal Information Field，信令信息字段）长度或LSSU的SF（Status Field，状态字段）长度。对于FISU而言，LI设置为0；对于LSSU而言，LI设置为1或2；对于MSU而言，LI则设置为3～63。若MSU长度小于或等于63个字节，则LI字段的长度为实际长度。当长度扩展直至272字节时，该字段的长度仍然为63。该字段的值被限制为63是因为它只有6比特长。SIF包含用户发出的信息，SIO（Service Information Octet，业务信息字节）则规定该信息属于哪个用户。SF字段提供链接的状态。

16比特CRC字段为SU提供差错检测。FSN（Forward Sequence Number，前向序列号）为被发送的MSU的标识号；而BSN（Backward Sequence Number，反向序列号）则给出了正确接收的最后一个MSU的编号。如果FIB（Forward Indicator Bit，前向指示位）的值与前一个FIB的值

不同，则表示MSU被重新发送；如果FIB的前一个值与当前值相同，则表明MSU是首次发送。

若BIB（Backward Indicator Bit，反向指示位）的值与前一次相反，则表明有错误，同时请求再次发送；若BIB值不变，则表示无错误信息。

18.4.2 SU传输交换的实例

下面我们通过一个例子看看这些字段是怎样应用的，希望大家藉此对它们的功能有更清晰的认识。在图18-8中有两个节点彼此交换一个SU序列，各链路终端有一个SP和一个STP，但它们可以是有效SS7节点的任意一对。SU的类型为MSU和FISU两种，但其实际类型则取决于信息是否被发送。时间自顶向下进行，并且我们在大部分情况下将用一个新的图表来讨论每个SU。

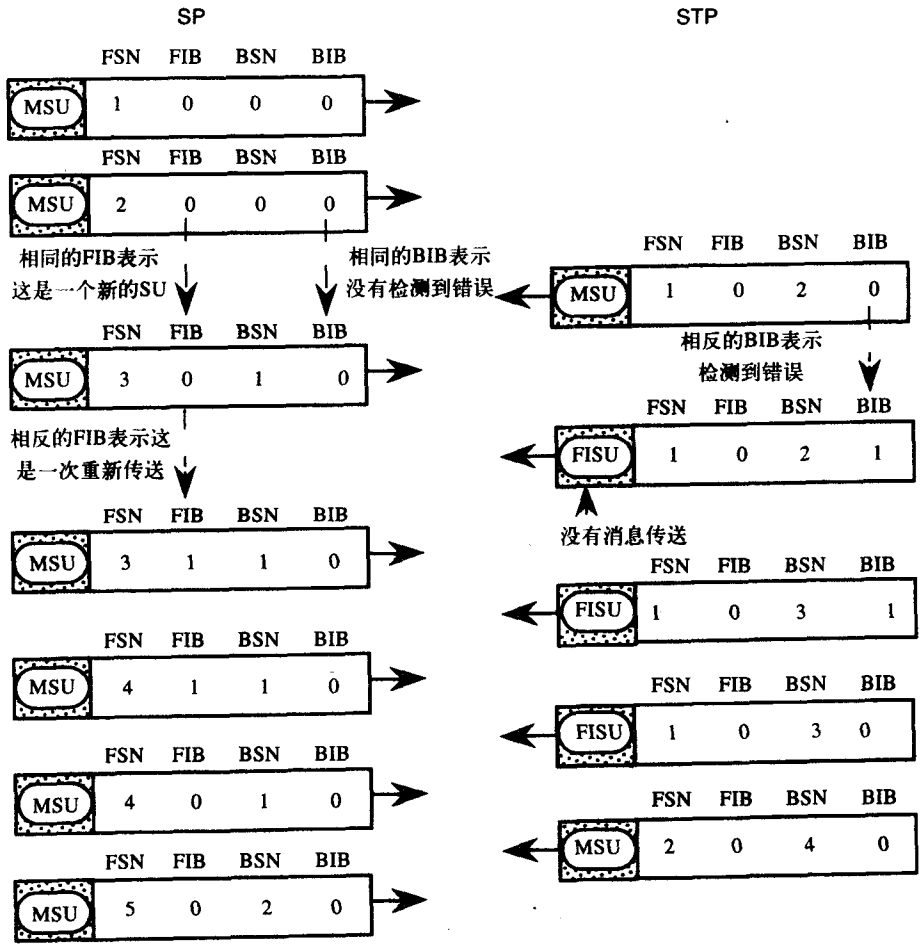


图18-8 信令单元交换的实例

首先，SP发送序号为1的MSU，由FSN标识。

之后，SP发送序号为2的MSU。

位于链路另一端的STP发送1号MSU，于是其FSN被置为1。同时，STP确认SP的2号MSU，这是由其BSN中的2表示的，意即STP接收到了SP的2号MSU。

SP发送3号MSU，并通过将BSN设置为1来确认STP的1号MSU。这时FIB等于0，这与前

一个MSU的FIB相同。由于这些FIB相同，因此进一步向STP确认3号MSU首次被发送。类似地，因为对SP发送的这些MSU而言BIB等于0，所以没有要求STP再次发送信息。

现在STP发送FISU告诉SP在传输3号MSU时出错。由于此时没有信令信息要发送，因此发送的是FISU而不是MSU。下面我们比较STP发送的FISU的各个字段和MSU的各个字段。因为只有MSU增加了FSN字段，所以FSN仍然保持为1。即使SP发送了3号MSU，但BSN仍然为2，说明3号MSU没有被正确接收。BIB发生了变化，向SP表明STP请求重新发送该SU。

SP再次发送MSU-3。FIB由0变为1，说明SU正在被重新发送。BSN仍然为1，这是因为从STP接收到的最后一个无错的SU为1号。

现在BSN字段为3，表明STP正确接收了SP的MSU-3。由于BIB与前面的FISU保持相同，因此没有给出重新发送请求。

SP发送MSU-4，同样FIB保持为1，表明这是一个新的MSU。

但是，STP这次接收异常，将BIB位改变，请求重新发送，同时保持BSN为3。

FIB改变，SP重新发送，STP正确接收，但是因为有信令信息要由一个用户发送，所以SP会封装其2号MSU，在该序列中SP发送的最后一个MSU为5号，它将其BSN设置为2来确认STP的MSU-2。

以上我们看到的是一个半双工通信交换，但SS7要求全双工链路，速率为56kbps或者64kbps。采用这种方法，所有的MSU都是从造成差错的那个MSU开始重新发送。对于卫星链路而言，这样会导致附加延迟，因此应该采用一种称为预防循环重新发送的方法。

18.5 MTP第三层

SS7的第三层的功能是提供路由，从而使得接收消息的节点知道所接收的消息是否要传送到本地的第四层，还是转发到另外的节点，如果是后一种情况，应该采用哪条链路。

ANSI标准中这一层的信息头为64比特长，ITU-T标准中则为 32比特长。它包括SLS（Signaling Link Selection，信令链路选择）、OPC（Origination Point Code，源节点代码）和DPC（Destination Point Code，目的节点代码）几个字段。网络中各个节点不论是SP还是STP均分配有唯一的节点代码，它对应于节点的地址。然而，连接多个SS7网络的网关可以拥有不止一个节点代码，其中一个节点代码对应一个网络。

在任意一个交换节点和其相邻的STP之间最多有16条链路。因为每个交换节点都与两个STP相连，所以一个交换节点最多有32条可能的链路，每一组为16条链路。为了清楚起见，图18-9中的每一组仅给出了3条这样的链路。

当有消息要发送到STP时，第三层会随机地从32个可能值中选取一个SLS，各个值都对应一条可能的链路，这样就确保了两个STP之间的流量是共享的、均衡的。

在图18-9中，由交换节点发出的SLS为1、4、6等的消息将跨过节点代码为3的STP，而SLS为0、2、3等的消息将跨过节点代码为2的STP。以同样的方式，当消息从一个STP对传送到另一个STP对时，流量是均衡的。

必须注意的是，当一个应用要求多个消息以它们发送时的顺序到达时，这一层就会给这些消息指定同样的SLS。这样就可以确保消息沿着相同的路径传递，从而按照相同的顺序到达目的地。

例如，所有SLS等于6的消息将被先传递到节点代码为3的STP，然后再到节点代码为4的

STP。总之，SLS的安排保证了网络中负载的平衡；同时，在需要时也可以为消息安排固定的路径。无须第3层信息单元的头部再请求序列号字段，就可以提供这一固定路径，这与X.25是不同的。

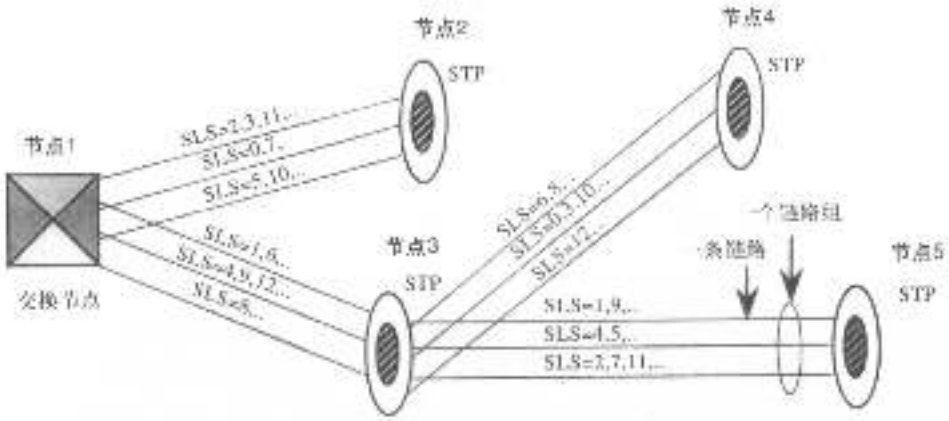


图18-9　第三层MTP信息单元头的SLS字段提供一种平衡网络负载的方法和需要时提供固定路径

第二层的FSN仅用于在两个节点代码之间进行差错控制，而SLS将一直维持不变，直到消息到达DPC（Destination Point Code，目的节点代码）。而且，第3层并不是通过指定相同的或不同的SLS来提供虚拟连接或数据报服务，该功能是由SCCP提供的。

18.6　SCCP

18.6.1　SCCP的子层

在图18-6中，SCCP是SS7体系结构中第四层的较低子层。它对于与电路不相关的协议即TCAP来说，总是必需的；而对于与电路相关的协议即ISUP来说有时也是需要的。SCCP段以279字节为单元（MSU）为低层协议发送消息，并在接收端重新组合成消息。

SCCP又进一步被划分为4个子层，分别为0－3层，其中，0层和1层用于无连接消息传输。也就是说，接收协议无法将逻辑上相同的消息与同一个传输过程联系在一起。利用这些层，高层的协议在查询-响应连接服务中包含该事务处理的字段。然而，2层或3层协议能够组合这些消息单元，但1，2层协议却不能。

0层和1层均可提供无连接服务，但1层可确保保持信息传输的序列。

通过在SCCP信息单元头部使用本地参数，第二层可提供一种虚拟连接。这与X.25的LCI类似，并且与X.25类似，在传送数据以前必须在端节点之间建立连接。最后，第三层用来控制数据流并通过附加字段来提供数据恢复功能。

18.6.2　0层业务举例

图18-10给出了一个SCCP子层提供的0层业务的例子。尽管这种配置在美国非常普遍，但也存在其他不同的可能配置。设话机呼叫800-123-4567，这时消息单元在节点代码为07的交换节点被组织起来。交换节点必须将该消息发送给能够把800号码转换成POTS号码的SCP。关于哪个800号码由哪个SCP进行转换的信息全部存储在STP中。因此，交换节点可以将该消

息发送给一个STP。拨打该号码的人称为终端电话用户（end subscriber），而在SP和STP执行的应用程序则称为用户（user）。

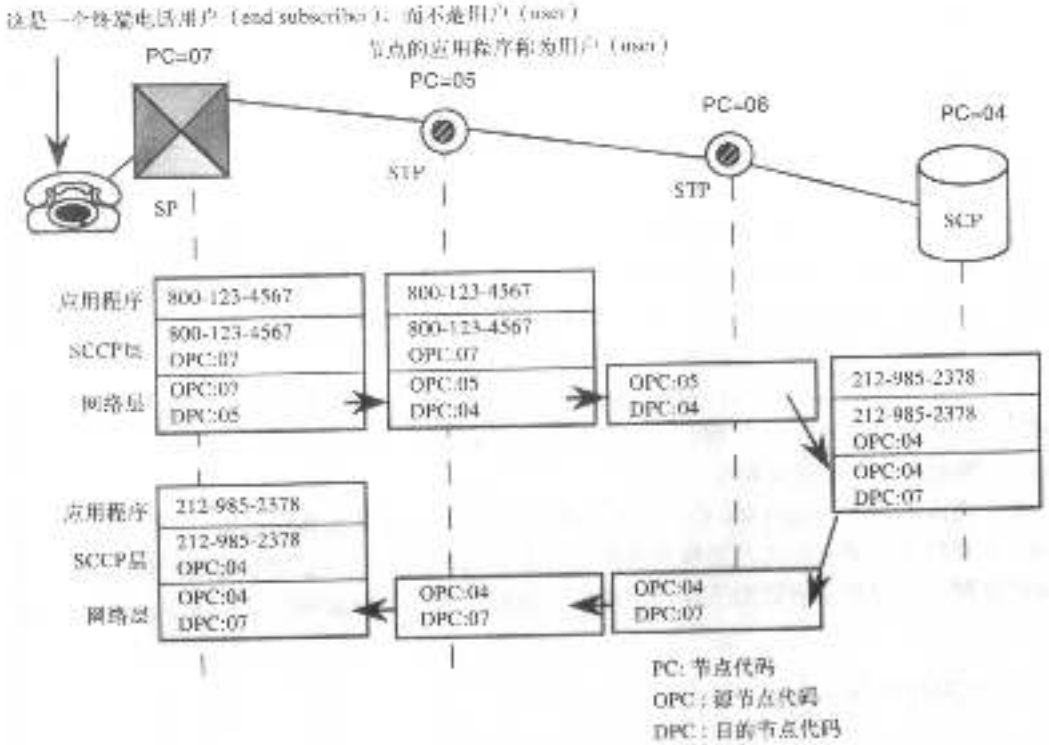


图18-10 一个800号码被SP送往其STP。之后STP找到SCP的节点代码，SCP有自己的POTS号码，并且发送要转换的800号码。整个消息是通过各个节点发送的，但是这些节点只执行了网络层功能，列出了网络层标题。用户是运行在7、5和4号PC上的应用程序

首先，在7号节点，应用层提供800号码，SCCP在头部也提供800号码，这时OPC为7。在7号节点的网络层在其信息单元的头部复制OPC，并将DPC=5插入。在随机选择一个SLS之后插入DPC。

消息单元到达节点5，在这里SCCP层被激活，因为端节点代码等于5。STP在找到该800号码之后，就知道这个号码的SCP位于何处，并且选择其DPC（4）。而SCCP层中的OPC在返回时始终处于节点7，STP必须能够给正确的SP发送消息。然而，由于在节点5产生该消息，故MTP层中OPC被设为5。

消息单元可以通过另一个STP，例如框图中所示的节点8，但不能得到SCCP层的处理。即使如此，网络层还是被用来选择到达SCP的正确链路。

SCP的所有层均要处理该消息，并且应用程序会将800号码转换成POTS号码，并复制在SCCP信息单元头部。同时，节点7从原SCCP头部的OPC被复制到新的网络层头部的DPC。在返回过程中，因为终端节点（DPC=7）不再是任何中间STP而是SP，所以直至到达节点7后才启动SCCP功能。位于SP的用户（user）一旦获得了POTS号码，就必须使用ISUP层为终端用户（end subcriber）连接实际电路。不过还是让我们先了解一下TCAP层。

18.7 TCAP

本节主要介绍如图18-6所示的SS7的两个垂直层的第一层，即TCAP（Transaction Capabilities Application Part，事务处理应用部分）。前面所介绍的数据库查询范例是一个与电路不相关的用户功能。非电路连接功能给SCP发出一个呼叫，以便从中获取路由信息，这是该层的主要目的。通常，采用TCAP之后，需由ISUP完成呼叫。

18.7.1 用户请求层

返回去再看图18-6，我们可以看到TCAP层被分为CSL（Component SubLayer，组件子层）和TSL（Transaction SubLayer，事务处理子层）两层。一个TCAP用户或一个在SS7节点执行的网络应用程序可以向网络中另一个节点的对等用户发送请求或响应。此类请求分为四类操作，它们基于所期望的不同响应而定。

第一类请求需远端用户执行所请求的操作，并且响应该操作是否成功；第二类请求要求远端节点仅在操作失败后作出响应；而第三类请求则仅在操作成功后作出响应；最后，第四类请求无须接收端作出任何响应。

第一类请求的例子如将800号码转换成POTS号码，这总是需要作出响应的。第二类请求的例子为执行路由测试，仅当出现某类问题时才作出响应。第三类请求的例子如向多个节点发送消息时，仅有消息所属的节点作出响应。最后，第四类请求的例子是向多个节点广播预警信息。

18.7.2 TCAP的两个子层

由图18-6可知，当向下发送请求或应答时，首先由TCAP的CSL来处理（该消息单元称为一个组件）。之后通过TSL层，此时一个或多个组件被组织成一条事务处理消息，一个组件仅可以包含一条请求或一条响应，但一条事务处理消息可包含多个组件。

一个组件可包含上述四种请求中的一种，或一个表明操作是否成功的响应，或一个表明接收到的请求（或响应）是否明白的响应。

TSL为CSL对等实体彼此利用组件进行通信提供了面向连接对话，这是通过SCCP 0层和1层所提供的无连接功能实现的。换言之，利用SCCP的无连接服务，TSL为CSL子层提供了连接。

18.7.3 CSL子层

CSL元素分为5种：INVOKE元素有且仅有一种请求；RETURN RESULT-NOT LAST组件包含操作成功的报告以及属于该报告的更多组件要服从的信令。RETURN RESULT-LAST组件是一个包含多个组件的报告中的最后一个组件，由于SCCP消息最大为254字节，因此一个报告必须被划分为多个组件。

若一个请求操作失败，将会发送RETURN ERROR组件，并且若接收消息无法理解，将会返回REJECT组件。

各组件均由一个CID（Component IDentifier，组件标识符）进行标识，这样即使请求是由两个不同的应用程序发给相同的目的节点，返回响应也能够与所发送的请求相对应（或相匹配）。

图18-11给出了一个对等用户之间组件交换的例子。开始时，交换机预将一个800号码转换成POTS号码，于是它就发送一个INVOKE组件，并指定其CID为3。CID也称为启动ID。

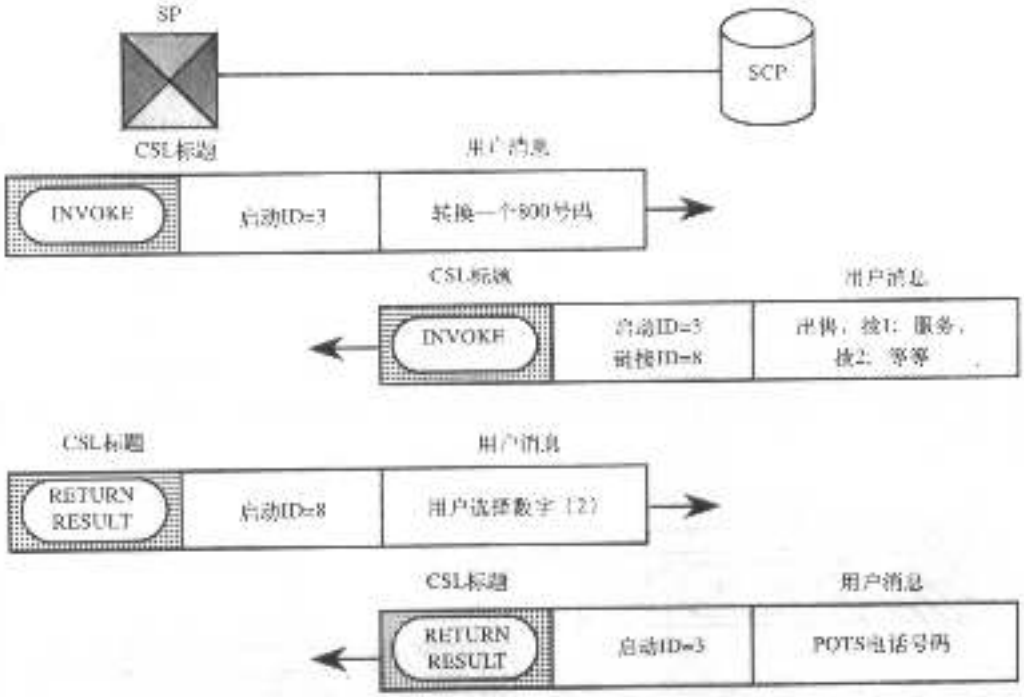


图18-11 一个组件序列交换的范例

SCP接收到这一请求之后还不能返回任何响应，因为它还需要来自交换机的更多信息，例如，800号码被转换成不同的POTS号码是由用户所需的业务决定的。因此，SCP会返回一条请求，比如转销售部门请拨1等等。这个由于最初的请求而产生的请求，也变成CSL层的一个调用组件，并接收到其ID为8。由另一次调用所产生的调用称为链接调用。类似地，由另一次请求所产生的请求称为链接操作。

交换机用户（user）或者应用程序从其终端用户（end subscriber）接收到正确的数字，比如"2"，这个选择由一个CID值为8的RERURN RESULT组件返回。现在，CID为8与链接ID为8的匹配SCP用户就能够为RETURN RESULT组件（CID=3）提供正确的POTS号码。于是，交换机就能够为调用标识符为3的组件发起的进程完成一个呼叫。

18.7.4 TSL子层

如前所述，TSL通过SCCP的无连接服务为CSL层提供一个端到端的连接。这种端到端的连接称为一个对话（dialogue）或一个事务处理。为了提供一个连接，TSL消息头包含一个类似于X.25的LCI的字段，称为TID（Transaction IDentifier，事务处理标识符）。用户能够利用TID来发起、维持并终止其与其他用户的对话。CID允许端节点进行接收响应与所发送请求的匹配处理。

共有5种TSL消息类型：BEGIN、END、CONTINUE、UNIDIRECTIONAL和ABORT。如果BEGIN和CONTINUE消息不包含任何元素或者上层消息，则它们就分别类似于X.25的

CALL REQUEST和CALL ACCEPTED分组。

消息END类似于X.25的CLEAR REQUEST，可由两个TSL实体中的任何一方发出；然而，与X.25所不同的是，END消息没有获得确认。

如果BEGIN包含一个INVOKE组件（即第4种类型中的任何一种），并被一条END消息响应，则如图18-12a所示的对话就类似于X.25的快速选择特性。在这种情况下，END消息可为空，也可以包含无须响应的第4类INVOKE，或者可以包含RETURN RESULT、RETURN ERROR或REJECT组件。如果出现问题，使得TSL层不能维持该对话，则发送带有诊断信息的ABORT消息。

图18-12b给出了用来提供第四类操作的UNIDIRECTIONAL消息，这里无须任何响应。

下面看图18-12c所示的简单TSL对话的最后一个例子，例中节点请求信用卡呼叫授权。用户将递交图中所示的请求项目，例如主叫方号码，来提出请求。由于该操作需要响应，因此CSL将编码其信息单元头部发出第一类INVOKE；TSL则产生一条快速选择消息并发出一条BEGIN消息；SCP一收到该消息就使该呼叫有效，并发出第四类INVOKE要求限定呼叫时间为3分钟。

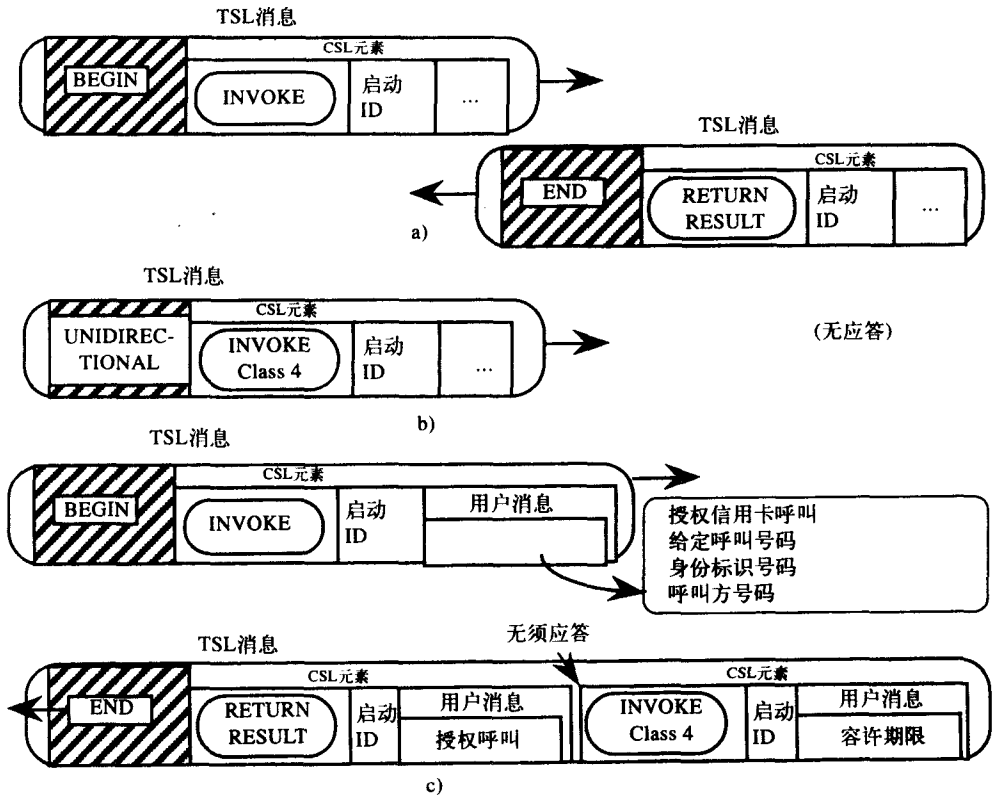


图18-12　TSL消息交换的三个例子

18.8　ISUP

ISUP（ISDN User Part，ISDN用户部分）是一种通信协议，提供交换机之间的电路连接

功能。它是用在ISDN终端用户之间，在数字环境下支持话音、数据、视频和其他应用的协议。TUP（Telephone User Part，电话用户部分）作为ISUP的前身，主要通过模拟用户线支持话音通信。

18.8.1 承载与补充业务

ISUP业务分为基本承载业务和补充业务。承载业务是为交换机提供的业务，该业务允许在终端用户之间建立64kbps电路交换连接。它们还规定了这些连接的管理与释放。围绕图9-1展开的讨论说明了在模拟域如何使用CAS(Channel Associated Signaling or per-trunk signaling，随路信令或单条中继线信令）实现这些功能。在数字网络中可由SS7的基本承载业务实现这些功能。

补充业务是直接为终端用户提供的高级业务，不能用CAS信令方法实现。它们为普通的ISDN终端用户提供各种服务，类似于PBX提供的各种特性。下面简单介绍其中几个：

- **呼叫线路识别**：一般称为呼叫ID，该项业务是提供给被叫用户的，它给出了主叫方的电话号码，如果有的话还会给出分机号码或子地址。
- **呼叫线路识别限制**：这一业务是提供给主叫方的，这样他/她的电话号码就不会呈现给被叫用户。
- **呼叫转移**：这项业务可以使连接的任一端能够建立与第三方的连接，之后再进行释放，若用户不释放连接，则变成一个会议电话。
- **呼叫遇忙转移**：当两个终端用户之间建立起通信连接并有新的呼叫进入时，会用到这项业务，此时该新呼叫将被转接至另一个预先设置的号码。
- **直接呼叫**：终端用户无须与接线员协调呼叫，就能够通过ISDN直接呼入一个PBX，然后进入分机或子地址。
- **封闭用户组**：类似于X.25特性，多个用户可以形成一个子网，并且不在一个组中的用户被限制只能呼叫该组中的用户，或反之。一组中的用户可以有附加的特权并且可能属于多个这样的组。

18.8.2 ISUP消息

ISUP的协议数据单元简称为ISUP消息，该消息由特性参数和相关信息组成。前两个参数CIC（Circuit Identification Code，电路标识码）和MT（Message Type，消息类型）总是必需的，并且均为8位。CIC指定了该消息所属的两个交换机之间64kbps的物理电路，而MT指出消息的类型和该消息其余部分的格式。在以前的模拟系统中，一条中继线承载一路话音电路。这里的CIC与一条中继线类似，不仅仅限于话音，而且还可以携带运营商需要在64kbps信道上发送的任何信息。

ISUP消息的其他参数分为强制的固定长度参数、强制的可变长度参数和任选参数。一条消息中这些参数的组合定义了该消息的类型。表18-1总结了这些分类和ISUP消息的类型，我们将作一个简短的介绍。

表18-1　ISUP消息类型的种类（仅给出某些消息类型）

I.呼叫控制	2.呼叫管理
1.呼叫建立	ANM：应答消息
A）前向建立	RBL：释放
IAM：初始地址消息	SUS：暂停
SAM：后续地址消息	RES：继续
B）反向建立	FOT：前向传输
ACM：寻址完成消息	3.端到端信令
CPG：呼叫过程	PAM：传递消息
CON：连接	4.补充业务
C）普通建立	5.终人更正
INR：信息请求	II.电路管理
INF：信息	1.单电路
COT：连贯性	2.电路组

18.8.3　ISUP信令连接

图18-13给出了在三个交换机之间的CIC链路，在这些链路上仅发送64kbps的用户信息，而不发送任何信令。从一个交换机到另一个交换机，给定的CIC仅出现一次。从PC3到PC4，仅有一条CIC等于5的电路，但是CIC=5也可以存在于通往PC2的链路上。因此，CIC和DPC（Destination Point Code，目的节点代码）共同规定了从交换机连接出来的电路。每对交换机之间的CIC数量取决于它们之间流量的需求。

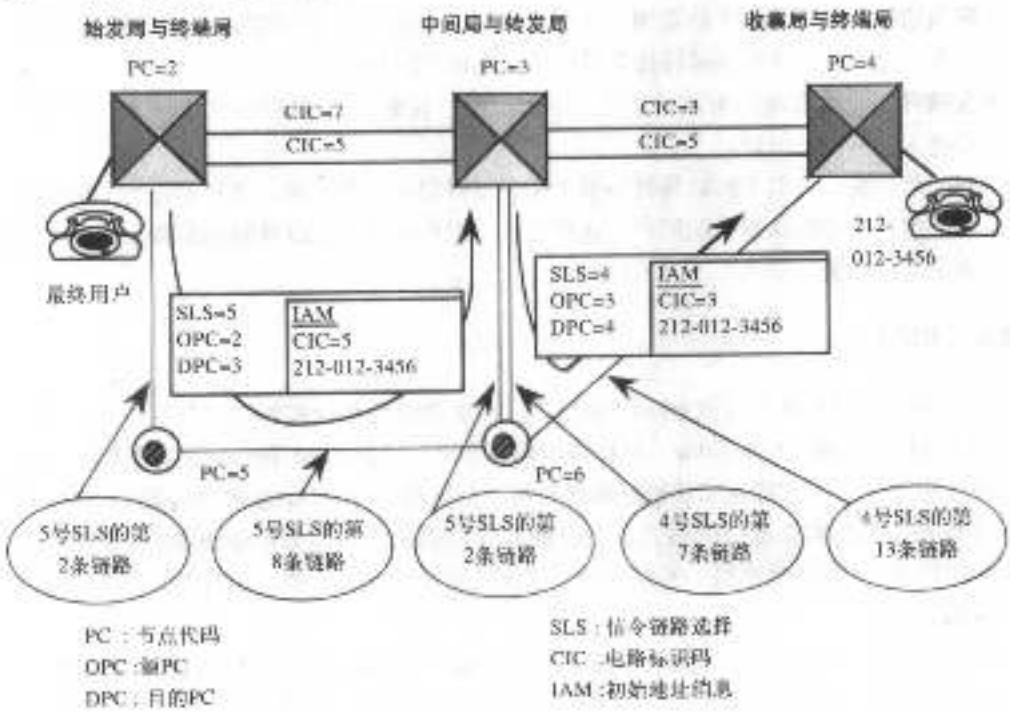


图18-13　利用ISUP建立一次连接

图18-13还进一步给出了两个终端局PC2与PC4之间如何建立起电路交换连接。PC3是一个中间局，通过它进行连接的交换。首先，用户呼叫212-012-3456，PC2决定通过PC3建立连接，这也许是因为没有到达PC4的直接的CIC（中继线）。PC4则是唯一能够完成建立与被叫用户的连接的交换机。

于是，PC2就找到了连接至PC3的空闲电路CIC=5，它产生一条表18-1中所列的IAM（Initial Address Message，初始地址消息）消息，并通过信令网络经由PC5和PC6发送给PC3。IAM消息包含被叫方的号码和所有必需的路由信息。第三层网络层指定SLS=5并在其消息头部设置OPC=2和DCP=3。

PC3打开ISUP消息后便会知道应该与PC4建立连接，之后它找到一条空闲电路（CIC=3），并将其自己的ISUP消息经过组装后发送给PC4，第三层选择4号SLS，同时发送一条新的IAM消息，如图18-13所示。

现在只要呼叫一直有效，从PC2到达PC3的所有CIC＝5且SLS＝5的消息就会在PC3重新产生，并发送给CIC=3且SLS=4的PC4，这样就建立起一个单向信号通道。两个交换机之间总保持相同的SLS就可以确保消息将按发送时同样的次序到达，而CIC则确定了呼叫过程所使用的电路。

图18-13中仅给出了前向信令路径的建立，还需要利用相同的CIC组在链路上建立一条反向路径，但未必是前向路径上所采用的SLS组。注意目的局并不接收始发局的PC，但是通过中间节点的CIC-SLS对被用来给始发局发送返回消息。通常，一个完整的ISUP连接由一条前向信令路径和一条反向信令路径组成。

18.8.4 ISUP信令方式

前面我们已经介绍了LBL（Link-By-Link，逐条链路）信令传播方式，这里所有的ISUP消息均被转发局解释并修改。换句话说，当消息没有被转发局所解释而是仅被终端局解释时，它就称为端到端信令。端到端信令是通过发送PAM（Pass-Along Message，传递消息）或者利用SCCP面向连接或无连接层实现的。图18-6描述了这些选择，而表18-1也列出了PAM。

下面是一个何处需要端到端信令的例子。当目的交换机接收到一条IAM消息后，为了完成此次呼叫，还会向始发局呼叫请求并且接收更多的信息，这时就要用到端到端信令。这里转发交换机不必知道信息交换的内容。

当一条PAM消息（一种ISUP消息）到达转发交换机时，它仅关心MT和CIC参数。检查MT是为了知道它是否是一条PAM消息，检查CIC是为了在下一条正确的链路发送消息。但是这类交换机并不解释或者再生该消息的其余内容。

18.8.5 呼叫的建立与释放

最后，简要介绍电路交换呼叫是如何利用发送在用户的电话机和交换机之间的D信道上的ISUP消息和信令消息建立连接以及断开连接的。

我们将在第19章中介绍，住宅用户的电话线复用着两个B信道（可以同时发送话音和数据）和一个D信道（用于向CO处的交换机发送信令）。摘机后，ISDN电话通过D信道向交换机发送一条SETUP消息，而不是像POTS线路那样关闭本地环路，并设置DC电流，前三步如图18-14所示。之后会接收到来自交换机的SETUP ACK消息，而不是拨号音。类似地，当呼叫一个号

码时，ISDN电话机会发送一条INFO消息，并且当远端的电话振铃时，它就会接收到ALERTING消息，而不是回铃音。

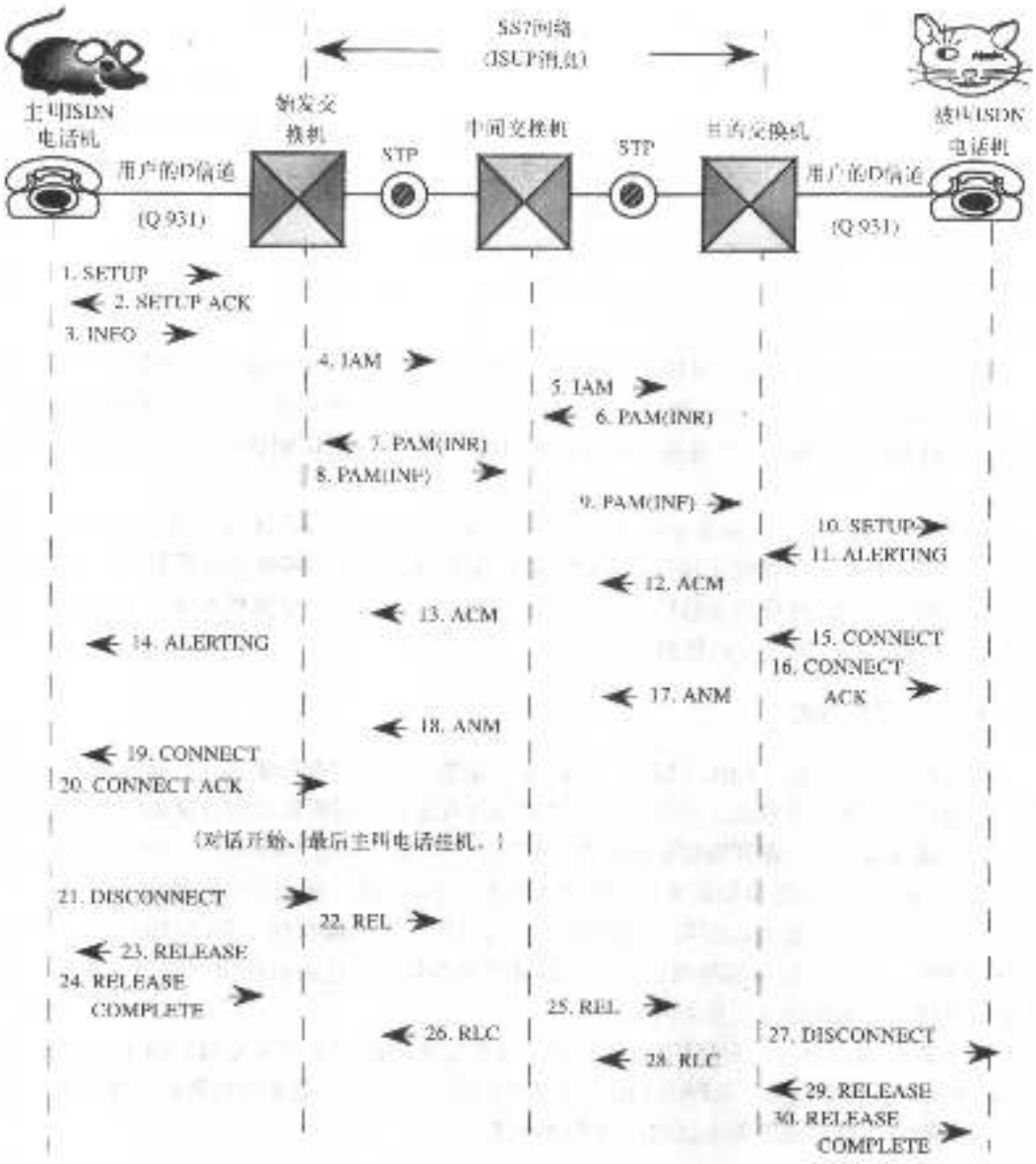


图18-14　一个呼叫的连接和断开过程，显示了用户电话机的Q.931消息和交换机之间的ISUP消息

所有这些信令消息都是通过用户与交换机之间的D信道发送的，并在ITU-T的Q.931协议中进行了规定。对话是通过B信道传送的。尽管数字消息通过用户的电话线传送，但用户仍然能够接收到采用POTS线路可以听到的模拟信号。为了达到这一目的，拨号声音、回铃以及其他模拟信号均由用户终端提供，而不是由本地交换机提供。保持这个用户接口与ISDN电话的相一致，就像使用POTS电话那样，就可保证电话用户向ISDN的平滑过渡。

图18-14给出了一个通过ISDN建立和撤销连接的例子。交换机与电话之间的消息为通过D

信道发送的ISDN的第三层消息，而交换机（经由STP）之间的消息为表18-1所列的ISUP消息，即Q.931消息。每一步均按顺序进行编号。

如上所述，电话机与交换机之间通过D信道交换SETUP、SETUP ACK和INFO消息，之后产生ISUP消息（IAM）并被发送到中间交换机，由中间交换机再生新的IAM消息发送至目的交换机。如果所需发送的信息比IAM消息所能包含的多，则始发交换机会在发送完IAM消息之后再发送一条SAM（Subsequent Address Message，后续地址消息）消息。这里并没有给出SAM消息。（好像标准化委员会仅是在选择首字母缩略词时完成了一次Seuss's Green Eggs博士与Ham的激烈讨论，显然，ham被错误地命名为PAM。）

在图18-14中，目的交换机需要更多的信息来完成连接，且发送一条封装在PAM（传递消息）中的INR（INformation Request）消息给呼叫始发交换机。要求从INR中获得主叫方的电话号码以便实现正确的计费，或者用于其他目的。步骤8中，始发交换机用一条INF（INformation）消息作出应答，目的交换机则向远端电话发送SETUP消息，于是电话开始振铃，并通过D信道发送一条ALTERING消息。之后交换机产生一条ACM（Address Complete Message，寻址完成消息），转换为ALTERING消息后发送给主叫方。

当被叫用户摘机时，将会发送一条CONNECT消息，同时交换机给该用户发送一条CONNECT ACK消息并通过网络发送ANM（ANswer Message，应答消息）。在主叫端完成CONNECT和CONNECT ACK消息的交换之后，对话就可以开始了。

图中给出了交换机在接收到来自电话机的ALERTING消息之后发送ACM（寻址完成消息）消息，但是，交换机也可以在接收到ALERTING信号之前先发送ACM信号。在这种情况下，交换机一接收到来自电话机的ALERTING信号就会发送一条CPG（Call ProGress）消息。也有可能被叫用户立即接起电话，直接发送CONNECT消息，而根本不发送ALERTING消息。

最后，电话可由任意一方先挂断，从而产生DISCONNECT消息。这时，主叫方发送一条DISCONNCT消息给中间交换机，该消息会映射为REL（RELease，释放）消息。同时，始发交换机会给电话机发送一条RELEASE消息，并接收一条RELEASE COMPLETE的返回消息。之后，中间交换机向目的端发送一条REL消息并在相反方向上发送一条RLC（ReLease Complete）消息。类似地，DISCONNECT、RELEASE和RELEASE COMPLETE消息的交换发生在被叫方的D信道。注意某些诸如SETUP、CONNECT和DISCONNECT之类的Q.931消息既可以由电话机发送又可以由交换机发送。

习题

1. 为什么SS7信令比CAS信令更灵活？
   a. 它是软件驱动的 b.它采用数字交换 c. 它采用高速数据链路 d. 它采用机电技术
2. STP对与其他STP对的连接使用哪种类型的链路？
   a. A接入链路 b. B桥链路 c. C交叉链路 d. D对角链路
3. SS7的第四层分为哪几个主要的子层？
   a. CSL、TSL和MTP b. CSL、SCCP和ISUP c. TCAP、SCCP和MTP d. TCAP、SCCP和ISUP
4. 下面哪个SU（Signaling Unit，信令单元）只有其他两类SU的共同字段？
   a. MSU b. LSSU c. FISU d. 没有

5. 哪一类操作只有在请求操作失败时才响应?

a. 第1类 b. 第2类 c. 第3类 d. 第4类

6. 下面哪一个Q.931消息仅由主叫电话发送?

a. DISCONNECT b. SETUP c. CONNECT d. INFO

7. 哪一个ITU-T信令系统与我们的SF信令相似?

8. SCCP层和MTP层一起被称为什么?

9. 在图18-6中，如果STP在最后的SU中没有任何信息需要传送到SP，那么是哪种类型的SU?

10. 如果两个节点代码之间的链路数减少，那么在每个链路上的SLS的数量是减少、增加还是保持不变?

11. 在图18-8中，位于哪些PC的用户（应用程序）在“发送过程”（send trip）提供它们的业务？位于哪些PC的用户（应用程序）在“返回过程”（return trip）提供它们的业务?

12. ISUP信令路径是由路径上各对交换机之间的哪对规定的?

13. 描述SP及其三种类型。

14. 如果STP发送的第二个MSU被SP不正确地接收，试述为了容错，接下来发送的SU的内容。

15. TC的三个子层是什么？各自有哪些功能?

16. 在图18-9中，如果SCP在其数据库中找不到要转换的800号码，会返回什么类型的CSL元素？假设该元素在其头部有错，SCP会发送什么类型的元素？SCP如何响应？画出这种情形的框图。

17. 你希望实现文中没有列出的哪项ISUP附加业务？换言之，你想用自己的家庭电话实现哪些你认为现在不能实现的服务?

18. 描述ISUP获得MTP层服务的三种方法，何谓端到端信令？它与这些方法有关吗?

第19章 ISDN

19.1 定义

尽管ISDN（综合业务数字网）的概念在1968年就被首次提出，但直到1984年ITU发表红皮书之后，它才成为一个标准。从那时起，ITU每隔四年出版一次新的建议。与SS7一样，ANSI（美国国家标准化组织）也推出了北美版的ISDN，该版本与ITU的版本略有不同。本章将延续5.5.3节的内容继续进行讨论。

19.1.1 接入接口

接入ISDN的方法有两种：BRI（Basic Rate Interface，基本速率接口）接入是为住宅用户、小型商业用户以及业务量较大的个人用户设计的；PRI（Primary Rate Interface，主速率接口）接入则主要是为大型商业用户设计的。BRI由两条64kbps的B信道和一条16kbps的D信道构成。B信道即承载信道的上层协议是灵活的，因此用户能够以任何需要的格式传输任何信息。通过一对连接到CO的金属线，用户可以在一条B信道上采用PCM编码进行通话，同时也可以通过另一条B信道以64kbps的速率与不同地点建立数据连接。

如果两个端点处的话音都被压缩到16kbps，那么它们之间的一条B信道就可以传送四路独立的话音信号。端点要完成这四条信道的多路复用、多路分解以及交换功能。B信道还能传送慢速运动视频信号、传真和任何其他信息；但有一点，接收端的终端要与所发送的信息相兼容。另外，128kbps的数据流可以送入一个反多路复用器，再通过两条B信道发送出去，最后在远端重新组合成128kbps的信号。

D信道（即δ信道）根据需要提供所需的信令来建立和拆开B信道连接。D信道上传输的消息分别由ITU的Q.931和Q.932，或者I.451和I.452予以定义（当ITU的两个小组一致同意同一组建议时，协议就会以两种不同的命名结束）。尽管D信道的主要目的是控制信令，但它也可以用在低速分组交换和遥测上，例如电表自动抄表。BRI可以配置成2B+D、B+D或者仅仅为D。

北美和日本的PRI接入采用T1速率，而欧洲则以E1为接入速率。PRI的D信道速率为64kbps，不同于BRI中D信道的16kbps。以T1速率接入时，规定信道结构配置为23B+D或24B。与T1不同的是承载信道为空，没有因实现信令功能而抢占的比特。以E1速率接入时，PRI配置成30B+D或31B。通常，PRI商业用户都有一条连接到中继线的一台PBX或一台主机。

除了B信道和D信道以外，还有H信道（即更高速率的信道）。H0、H11和H12三种信道的速率分别为384kbps、1536kbps和1920kbps，这都是64kbps的整数倍。H4信道的速率为135.168Mbps，可以传输基于PCM的标准彩色电视信号。

19.1.2 功能设备和参考点

为了充分认识各个设备的目的和功能，ISDN描述了有限的一组设备以及这些设备之间的接口，如图19-1所示。如果这些接口都能够正确实现，那么一家生产厂商的设备就可以很容易地被另一家生产厂商的设备所取代。

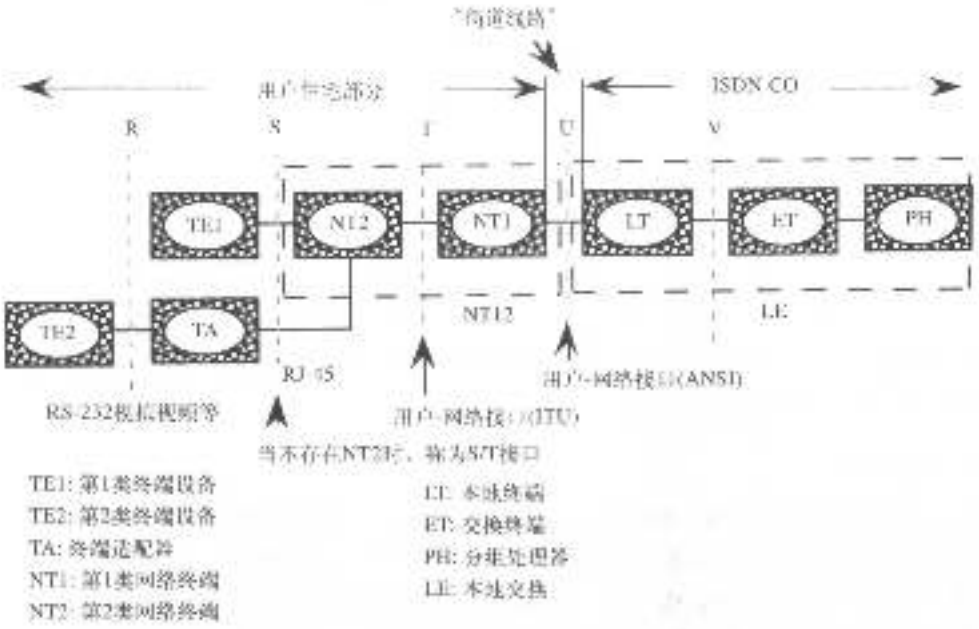


图19-1　功能群及其接口

与ISDN不兼容的设备被归为TE2（Terminal Equipment 2，第二类终端设备），可以是模拟电话机、PC、3270终端等等。为了将TE2设备连接到ISDN上，必须采用TA（Terminal Adapter，终端适配器）。对于网络中的其他设备而言，该TA可以使TE2看上去像一个ISDN终端；该TA也可以使网络中的其他设备与TE2通信，仿佛TE2就是一个ISDN终端。TA与TE2之间的接口称为R参考点，它取决于所连接的TE2的类型。

TE1（Terminal Equipment 1，第一类终端设备）是与ISDN完全兼容的设备，通过S接口连入ISDN，它可以是数字电话机、IVDT、工作站或其他各种设备。

NT2（Network Termination 2，第二类网络终端）是为用户住宅部分提供信息的交换、多路复用、集中或分配的设备，例如，LAN服务器、多路复用器、FEP或PBX。通常，PRI连接需要NT2而BRI不需要NT2。

NT1（Network Termination 1，第一类网络终端）是在用户住宅部分提供正确的线路终端的设备，它们能够提供线路监测、电源馈送、错误统计、准确定时的功能，可以将它们看作是DSU/CSU设备。

NT1的功能很容易集成在一张卡上，成为PBX或PC的一部分。在这种情况下，将集NT1和NT2功能于一身的设备称为NT12设备。这些设备之间的参考点称为T接口。在BRI中不需要NT2，这时NT1与TE之间的参考点称为S/T接口。在本章的其余部分，我们将TE1和TA-TE2的组合简称为TE。而且，将用NT来代替NT1或NT2，具体情况要取决于是哪类设备与TE相连。

与ANSI不同的是，ITU把NT1看作是本地网络的一部分，而并未提到U参考点。但是，FCC将NT1归属于用户，因此，ANSI将U参考点定义为通往CO的线路。在ISDN术语中，CO被称为LE（Local Exchange，本地交换）。LE本身又是由LT（Local Termination，本地终端）、ET（Exchange Termination，交换终端）和PH（Packet Handler，分组处理器）构成的。

LT在LE一侧实现NT1的功能，并且与15.4.2节中讨论的OCU（Office Channel Unit，局信道单元）是类似的。ET就是ISDN的电路交换机，而PH则类似于一个通往PDN的网关。

19.2 电信业务

由于ISDN集成了许多种类的业务，因此我们有必要定义什么是一项业务或者说一项业务由什么构成。ISDN用一个有限的属性（即不同的特征）集合很好地定义了各种业务。通过规定这些属性，就可以很清楚地描述ISDN的业务。这样，就基本消除了设备制造商、运营商和用户之间的误解，从而更好地实现ISDN的所有业务。当请求某种业务时，例如建立电话连接，这些属性就会发送到D信道上。

19.2.1 业务类型及其属性

电信业务（telecommunication service）分为承载业务（bearer service）、用户终端业务（teleservice）和补充业务（supplementary service），它们都是由其属性进行定义的。用户终端业务包含了承载业务，而补充业务是为承载业务和用户终端业务提供的。

由图19-2可见，承载业务是网络业务，因为它们是以OSI参考模型的前三层为特征的；而用户终端业务为终端用户之间的通信提供终端设备的功能，这些业务需要与OSI参考模型的所有7层之间相互作用。承载业务又分为接入属性、信息属性和补充业务属性。

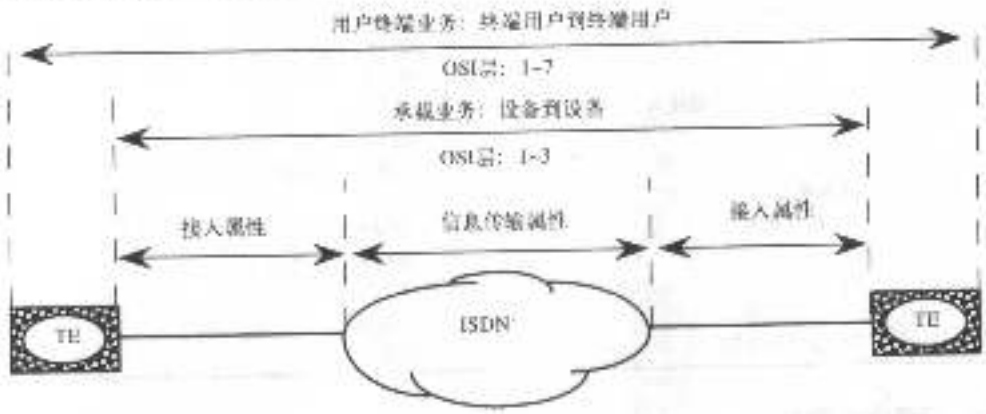


图19-2 电信业务的分类与范围

补充业务已经在18.8.1节中讨论ISUP时进行了介绍，在此不再作进一步的讨论。

表19-1给出了承载业务的三种属性：信息属性（它规定了通过ISDN传输信息的能力）、接入属性（提供了接入网络功能的方法）和通用属性。通用属性在表19-1中的第10项到第13项中列出。它们包括补充业务，规定可以接受的延时、误码率以及ISDN与ISDN或非ISDN网络如何交互工作。

表19-1 承载业务属性

属 性	属性描述
信息传输属性	
1.信息传输模式	电路交换 分组交换
2.信息传输速率	比特率（单位：kbps） 64、128、384、1536、1920 吞吐量（单位：PPS）

（续）

属　性	属性描述
3. 信息传输能力	非受限数字
	音频（单位：kHz）：3.1、7、15
	话音、视频
4. 结构	业务数据单元完整性
	未结构化
	8kHz完整性
	TSSI、RDTD
5. 通信的建立	即时
	预留
	永久
6. 对称性	单向
	双向对称
	双向非对称
7. 通信配置	点对点
	多点
	广播
接入属性	
8. 接入信道和速率	D（16 kbps）
	D（64 kbps）
	B、H0、H11、H12
9. 信令接入和信息接入	I.430/431
	I.451、I.461/462
	HDLC、LAPB、LAPD及其他
通用属性	
10. 补充业务	呼叫线路ID
	呼叫转移及其他
11. 服务质量	未定义
12. 交互工作	未定义
13. 运营和商用	未定义

19.2.2 信息传输属性

本节我们将按照表19-1中的顺序介绍七个信息传输属性。

第一个属性称为信息传输模式，它包括两种类型的模式：电路交换和分组交换。信息传输速率属性在电路交换模式中以kbps为单位，在分组交换中以PPS（Packet Per Second，分组/秒）为单位。用户建立呼叫时若需要连接两个B信道，则提供2 × 64kbps的信息速率。在这种情况下，用户就必须在网络中独立地传送这两个信道。

信息传输能力属性被规定为采用数据压缩的正常话音通话时的话音。相反地，当采用调制解调器时，规定这个属性为3.1kHz音频就不再要求数据压缩了。7kHz用于传输单声道无线电广播而15kHz用于传送立体声广播。电路交换模式的传输默认设置是话音而分组交换模式的默认设置为非受限的。非受限数字信息允许在数据流的任何地方出现任何比特格式，例如，业务不关心比特是否被填充，只要它在SDLC帧内即可。

结构属性的非结构化值是指在数据流的传送中不必保留八位组的边界；而8kHz完整性（电路模式的默认值）就要求保留这些边界，以使每个话音样本的8位总在一起。

TSSI（Time Slot Sequence Integrity，时隙序列完整性）要求在多址接入信道中，例如2 ×

64kHz信道，信息按发送端传至网络中的顺序传送到远程终端。RDTD（Restricted Differential Time Delay，受限微分时延）规定通过ISDN的延迟不能超过50ms，这是传输话音所必需的。

通信可根据需要即时建立，即在有请求的时候建立连接并在不需要的时候终止连接，正如拨打电话一样。使用预留属性可以提前建立通信，这里，连接的建立与释放都是由网络而不是由用户来自动发起的。最后，这个属性还可以指定为永久，类似于租用线路，在业务订购期间，两点之间的这一连接始终存在。

如果对称性属性规定为单向的，则数据只能朝一个方向流动，就像一个播音室向无线电发射机传送广播一样。如果该属性规定为双向对称的，则传输发生在两个方向上，并且具有相同的数据速率。双向非对称业务也是双向传输信息，但是速率却不同。这种类型的对称性属性用于一端正在传输数据而另一端不时地用ACK或NACK来应答的情况。

最后，通信配置属性规定了业务是只涉及两个用户（如点到点），还是涉及到多个用户（多点）的双向通信，或是仅有一点向多点发送信息（广播）。

19.2.3 接入属性

信息传输属性规定了信息是如何通过ISDN传输的，而另一方面，接入属性则规定了用户是怎样接入网络的：使用哪些信道，以什么速率，采用哪些协议。表19-1列出了这些属性的几个值。信令接入协议描述的是用户和网络之间采用什么信令方法，信息接入协议描述了信息是怎样从一个端用户交换到另一个端用户的。

19.2.4 用户终端业务属性

这些业务不仅包括承载业务，还包括OSI的高层属性。这些已经概括在表19-2中，这里就不再展开讨论了。

表19-2 用户终端业务属性

属 性	属性描述
低层属性	
信息传输、接入属性、补充业务	与承载业务相同
高层属性	
用户信息类型	话音（3.1kHz）、声音（15kHz）、文本等
第四层协议	x.224、T.70
第五层协议	x.225、T.62
第六层协议	T.73、T.61、T.6、T.100
分辨率(如果可适用)	单位ppi：200、240、300、400
图形模式（如果可适用）	字母镶嵌图、几何图、摄影图
第七层协议	T.60、T.500

19.3 BRI的物理层

19.3.1 概述

我们已经说过，多个设备可以共享同一个ISDN接口。也就是说，许多设备都可连接到同

一个2B+D接口。为实现这一点，ISDN定义了与OSI参考模型低三层相似的三层协议：物理层、数据链路层和网络层。

如图19-3所示，ISDN建议仅为D信道规定了这三层。但是，涉及到B信道的ISDN建议仅限于物理层。B信道第二层到第七层的协议是由TE负责的。ISDN在网络上只为B信道传输比特流。这个图表面看上去，B信道和D信道在连接到LE的线路上是物理分开的，但实际上它们是时分复用在同一物理链路上的。

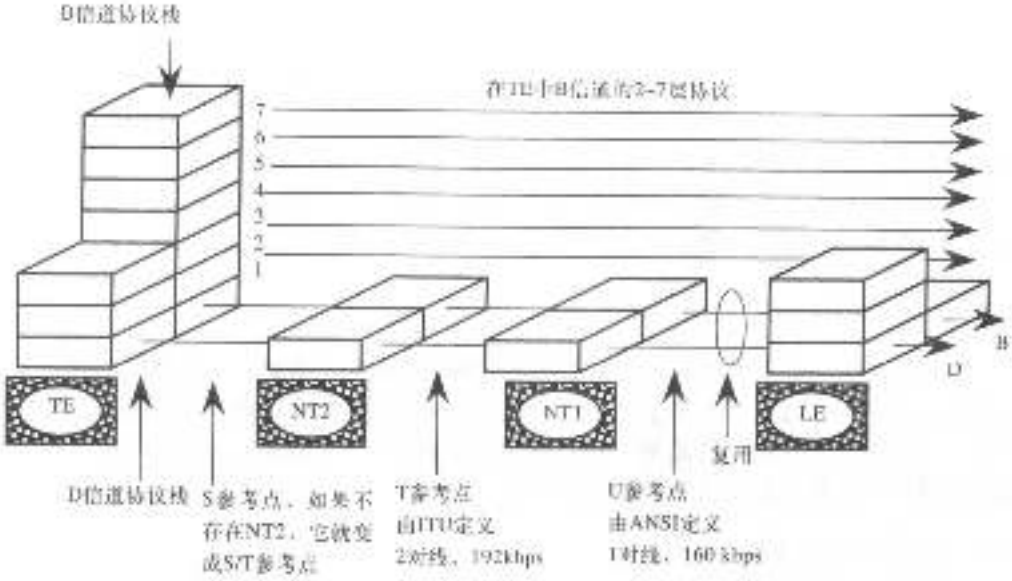


图19-3　ITU只在S和T参考点规定了ISDN协议，并且仅为D信道规定了低一层协议。B和D信道通过同一链路在物理层多路复用。ANSI规定了U参考点。但U点和S/T点仅在物理层有所区别

该图还给出了ITU定义的包括NT1的网络边界，而ANSI则不包括它。在这两种情况下，NT1都属于用户住宅部分。本节，我们将会分别讨论各个边界。

物理层除了为B信道和D信道提供传输能力外，还能提供定时及同步。该层还描述了激活和不激活终端的信令能力，以及有序接入D信道的信令能力。

BRI接入能够提供给住宅用户、集中式交换机用户或PBX用户，并且采用2B+D配置（通常在一对线上）。各个B信道都能分配其自己的电话号码。虽然本地环路还跟以前一样，但住宅用户却需要一个高级的NT1，内部线路必须换成两对或三对，模块插孔必须换成8针插孔，就更不用说TE的价格高于现在的POTS电话了。

19.3.2　ANSI的U参考点

在这个参考点处，NT1提供一个称为RJ-45的8引脚模块插头来终止本地环路。在这8个引脚中，仅使用了中间两个。因为S/T接口用到四条线，所以NT1必须提供一种将室内的四条线转换成通往LE的两条线的方法。为了在同一对线上进行发送和接收而不损失可用带宽，必须使用回波抵消技术。这已经在3.6节讨论过了。

2B1Q线路编码：U参考点所采用的线路编码称为2B1Q（2 Binary1 Quaternary，二进制四

电平），图19-4给出了2B1Q的一个例子。数据流被分成2比特一组，称为夸特（quat）。它们共有四种可能的夸特值，在旁边的表里给出了它们的电平。在图示的数据流中，“00” 夸特通过传输－3V发送，“11” 夸特通过＋1V发送等。

夸特	近似值
00	－3V
01	－1V
10	+3V
11	+1V

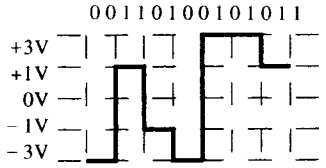


图19-4 ANSI T1.601的U参考点所采用的2B1Q信令方案

但是，这种编码的问题是链路的DC电压不平衡。也就是说，与T1所采用的双极性格式不同，它的正脉冲数目与负脉冲数目不相等。因此，为达到直流电压平衡，必须要在发送侧采用扰乱算法，在接收侧采用解扰算法。只有直流电压平衡后，链路才可以得到延伸。

帧：通过U参考点的比特是采用2B1Q传输帧发送的。这样的8帧组合在一起就形成一个超帧，如图19-5所示。从图中我们看到每帧以比特格式固定的SW（Synchronizing Word，同步字）开始。但是，超帧中的第一帧是以ISW（Inverted SW，反相SW）字段开始，它仅仅是SW各比特取反码，即1变0，0变1。这个字段接下来是12组2B+D比特。一组2B+D中，每个B信道8比特，D信道2比特。最后，这帧以6个开销比特结束，这6个比特称为M字段。该字段用于在线路上发起环路反馈、获得错误统计并执行其他维护程序。SW有18比特，12组2B+D有216比特，M字段有6比特，于是由它们组成的一帧为240比特。

比特数:	18	8+8+2	8+8+2		8+8+2	6
2B1Q帧#1	ISW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#2	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#3	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#4	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#5	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#6	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#7	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
2B1Q帧#8	SW	B1+B2+D	B1+B2+D	…	B1+B2+D	M
	同步字	第1组	第2组	…	第12组	开销

图19-5 2B1Q超帧格式。一帧包含240比特（18＋18×12＋6），而一个超帧包含1920比特（240×8）

通过回答下面这个问题我们可以看出，每帧的比特数与U参考点的速率是一致的：如果在这240个比特中，只有其中的216个比特用于B和D信道，那么传输这些信道所需的总速率是多少？根据下面的比例式求出未知数，就可得出U参考点的正确带宽为160kbps。

$$\frac{\text{每帧中B和D共216比特}}{\text{每帧总共240比特}} = \frac{\text{B和D信道速率144kbps}}{\text{U接口的总速率}}$$

19.3.3 ITU的S/T参考点

配置：现在我们把注意力转移到NT的另一侧，看看它与TE之间的接口。图19-6给出了配

置TE和NT的四种可能方式。第一种简称为点对点配置，NT和TE之间允许的最远距离为1km。这种配置以及其他配置中，D信道回波比特（稍后予以讨论）的传输延迟限制了最大距离和各终端之间的间隔。

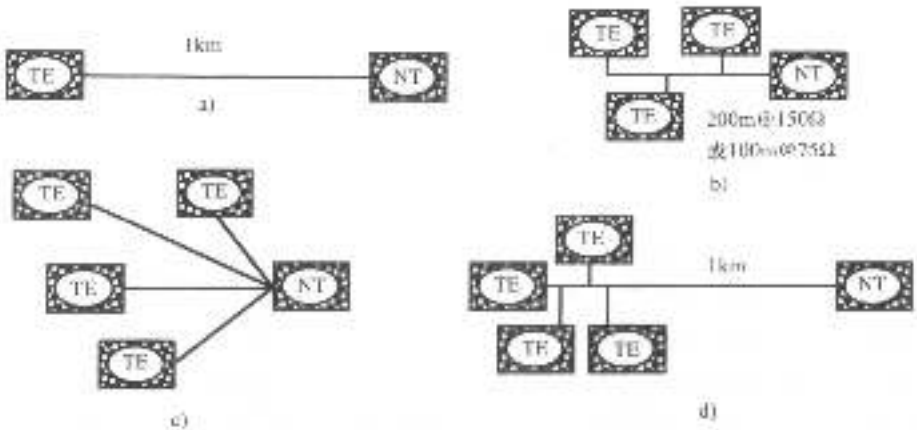


图19-6　S/T接口的四种可能配置方式：a) 点对点，b) 短距离无源总线，c) 星型，d) 延长的无源总线

其他三种类型均是由一点对多点配置演变而来的。在各种情况下，均可连接多达8个TE。至于哪个终端可通过总线传输，则是由D信道协议决定的。S/T接口使用两对线，这两对线与多个TE是并行连接的。

图19-6b使用了一条短距离无源总线。除了总线与终端之间的最大距离为10m这一限制外，对于这些终端的放置并没有限制。但是，对于阻抗为150Ω的电缆而言，最大距离被限制到200m；而对于阻抗为75Ω的电缆，最大距离则为100m。

图19-6d给出的是延长的无源总线连接，它将距离限制增加到1km；但是，所有的终端都必须集中在总线的远端，终端之间的距离必须保持在25~50m。线路配置（图19-6c）采用星型拓扑，由多达8个点到点连接构成。这些连接都终止在NT的一张卡上。

连接器：无论采用哪种配置，插头都是标准化的，称为I.430连接器或RJ-45，如图19-7所示。它有8个引脚，与一般的RJ-11相似。如果一个6引脚的连接器插入到8引脚的插孔中，那么引脚1和8都不能建立连接；同样，如果将一个4引脚的连接器插入到8引脚的插孔中，则引脚1、2、7、8不能连接。图中的表格给出了各引脚相对于TE的功能。这些功能恰好与相对于NT的引脚功能相反。也就是说，引脚3~6供TE使用时当作发送，而供NT使用时则当作接收，诸如此类。



图19-7　RJ-45或I.430连接器相对于TE的引脚功能分配。电源1和2位在引脚3、4、5、6上

PRI和BRI都可以使用RJ-45。但是，在本地环路上，PRI使用两对线而BRI只使用一对线。图19-7所示的引脚功能分配是对S/T接口而言的。该接口仅出现在BRI接入中而不出现在PRI接入中。两种接入类型都必须使用中间四个引脚。

图19-8给出了利用这8个引脚怎样建立一点对多点的配置。这里要注意的是NT在引脚4和5上的发送会被总线上所有的TE接收。类似地，所有TE都通过引脚3和6发送而NT则在这些引脚上接收。在任一给定时刻，哪个TE在总线上发送是由D信道比特及其回波比特决定的。现在就让我们来看看适用于这个接口的复杂而又灵活的配电方案。

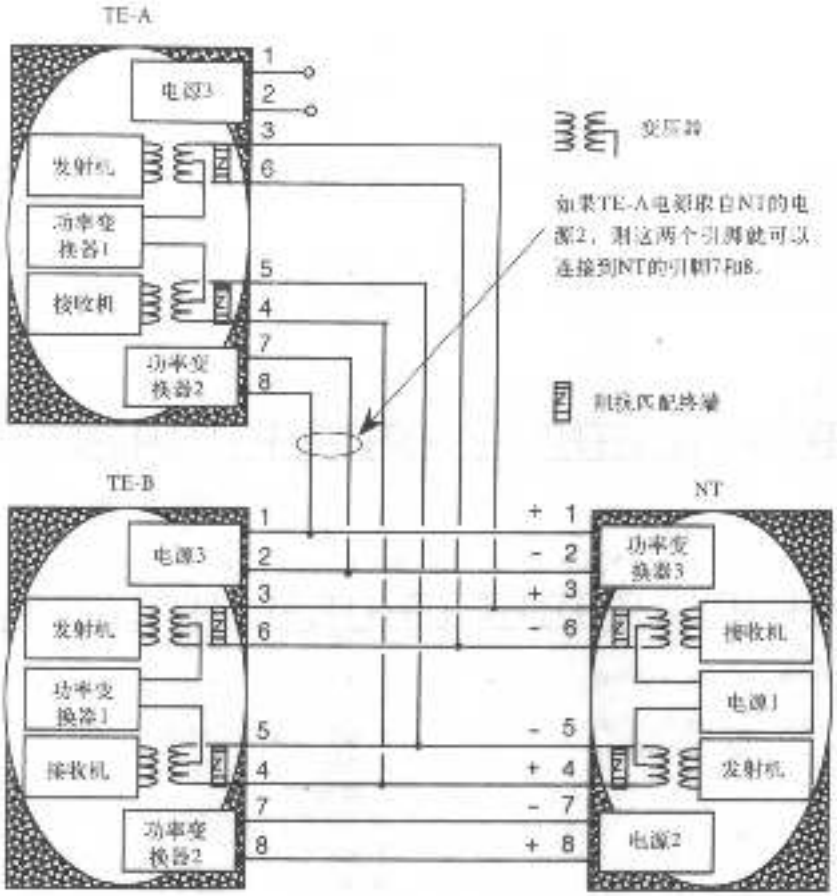


图19-8 带有功率分配的无源总线型配置范例

配电：在POTS中，网络（即CO）为电话运行提供电源。对用户来说，这在本地电网出现故障时是非常有利的，因为CO有更好的装备来应付断电。但对于ISDN而言，电源可以从多处得到，它可以来自网络、NT1、NT2或TE。由于驱动设备的电源可以来自各种不同的地方，因此便携式终端就不希望从插入的插座中获得电源。

如图19-8所示，共有三个电源（以及功率变换器）可以利用。所有电源均为40V直流电压。NT可以通过将电源幻像在所需的4个引脚（3到6）上来供电，称为电源1。这里，发送和接收的数字信号和DC电压共享同一条金属线。其功率为1W，并且可用来驱动与之相连的所有TE。NT则可以从网络获得电能，也可从本地AC插座或者电池获得电能。

电源2可以在NT的引脚7和8上得到，它为TE提供了高达7W的功率。并不是每个设备都配有其自己的电源，通过少数几个设备（NT和TE）驱动这些设备是非常有利的。这样，就不再需要那么多的电源备用系统。

图19-8进一步说明了TE利用电源3可以给其他的TE和NT供电。这个电源并不是ITU建议的一部分，它的具体使用也依情况而异。

19.3.4 S/T参考点上成帧

对BRI，S/T接口上的信令采用所谓的伪三进制编码，如图19-9所示。逻辑1是由发送0V表示的，逻辑0是用+1V或-1V表示的。电压的极性随着每个0比特交替变化；如果两个连续的0是用相同的极性发送的，则称之为编码违例（code violation）。编码违例的目的是为了保持同步。

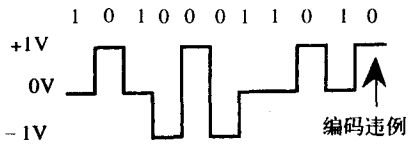


图19-9　伪三进制线路编码举例

图19-10给出了S/T接口上I.430传输帧的格式，由48比特构成，共250μs。从NT到TE方向与从TE到NT方向的帧格式是不同的。TE需从NT获得同步，所以TE的传输要延迟两个比特。

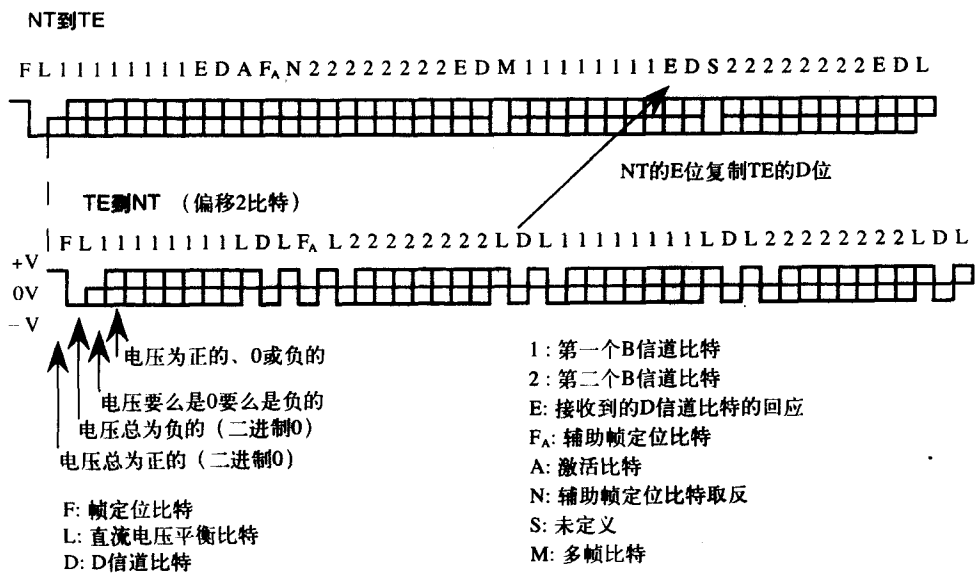


图19-10　S/T接口上的48比特I.430帧格式

该图画出了各比特所有可能的伪三进制值。在各帧的48比特中，两个8比特组用于B1信道，还有两个8比特组用于B2信道，每帧有4个D信道比特，这总共是36比特。在一帧的48比特中，还剩下的12比特用作辅助比特。像计算U接口的线速率那样，我们对S/T接口线路速率做同样的计算，可以得到S/T接口速率为192kbps。

$$\frac{\text{B和D信道共36比特}}{\text{每帧共48比特}} = \frac{\text{B和D信道速率为144kbps}}{\text{S/T接口速率}}$$

现在我们来看看辅助比特的作用，其中D和E比特留在下一节讨论。

F（帧定位）比特的极性总是正的，它标志着一帧的开始。紧跟其后的是L（平衡）比特，它总是负极性，从而为F比特提供直流电压平衡。同样地，其他平衡比特根据前一比特的极性分别设置为+1V、0V或-1V。

在NT到TE方向，Fa（辅助帧定位）比特每隔4帧设置成1，而M（复帧）比特在每隔19帧后设置成1。它们在其他帧中都设置为0。这些比特有助于组成复帧并保持线路同步。N比特总是设置为与Fa相反，所以如果Fa比特为0，那么N比特就为1。

在TE到NT方向，除了在每个第五帧外，其余Fa比特都设置为0，每个第五帧的Fa比特构成一个称为Q信道的子信道，其用途尚未定义。同样，S比特的作用也尚未定义。

NT将A（激活）比特传送给TE，用于指示接口是激活的，可以正常使用。图19-11概括了这一激活过程。TE发送INFO0信号。当然它也可以由NT发送。这个信号说明没有任何信号传送，它表示线路尚未激活。回顾一下以前的内容，可知0V表示二进制1，而二进制0用正的或负的电压表示。

之后，TE上电，并发送一个INFO 1信号，即传送连续的"+-111111"。该信号通知NT，TE欲激活线路，于是，NT发送一个INFO 2信号，其中B、D、E和A比特都置为0，在线路上0迅速改变信号极性，以使得接收机能够迅速同步。现在TE就可以用INFO 3信号来传输有用数据了，NT也可以用INFO 4信号传输有用数据。这时，A比特将被置为1，表示线路是激活的。

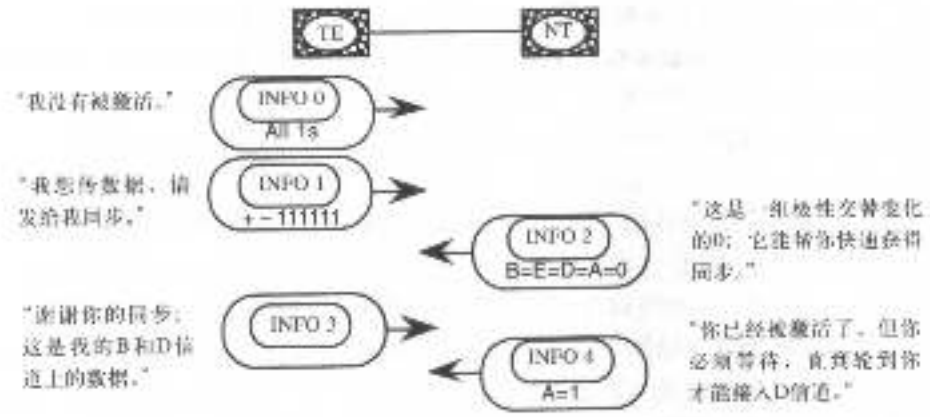


图19-11 用来激活TE的INFO信号交换过程。在此期间A比特被置为1

19.3.5 D信道接入控制

前面已经讲过，D信道是用来传输信令的，ISDN为其运行定义了三层模型。就ISDN而言，B信道只是涉及到第一层，仅传输它自己的比特。

采用BRI，TE可以连接成一个点对多点的拓扑结构，如图19-6和19-8所示。终端只能在通过D信道接入以后，才能在总线上传输B信道。因此，B信道上没有竞争问题。但是，D信道就不一样了。我们必须解决多个TE争用D信道的问题，也就是说，由于TE必须共享与NT连接的总线，我们应该如何决定在任一给定时刻由哪个TE使用D信道进行传输呢？

TE和NT均可以发送D比特，但是，E比特是由NT从TE的最后的D比特反射回来的。这些E比特可以帮助TE得知NT接收到谁传输的信息。如果一台终端发送的D比特为0，而另一台终端发送的D比特为1，那么NT将接收谁到谁的比特呢？

这个问题的答案是，NT将接收发送0的那个TE的数据。因为线路采用伪三进制编码，无论其他终端发送的是什么，只要有一台终端发送二进制0，NT就会接收这个0。记住，在线路上，二进制1根本没有电压，而0有电压。

D信道的使用分成如表19-3所示的两个优先等级。优先级1用于传输信令信息的ISDN的第二层帧，优先级2用于传输其他信息的帧，例如低速分组交换数据或遥测数据等。

表19-3　D信道接入优先级

	优先级=1 信令信息	优先级=2 非信令信息
正常	8	10
较低	9	11

在每个优先级中又分为两个级别，即正常级别和较低级别。优先级设置成终端传送给NT的某种信息。如果一台终端还没有发送任何级别2的帧，那么它会将其优先级别设置为正常。按照表中各等级和级别所对应的数，TE必须先对在E信道上接收到的来自NT的连续1（即0V电平）进行计数，直至计到表中给出的数量，才被允许传输。

传输完成后，TE将会降低自己的优先级别，以便给其他TE传输的机会。一旦它能够计数到较低优先级别对应的数，就知道其他想要传输的TE已经传完了。因此，如果有需要，它会将自己的优先级别升回到正常，开始另一次传输。

注意，一台想要传送数据的TE收到的1的个数必须大于6。这是因为，如果有其他TE在线路上传输，那么它的第二层帧里最多有6个连续的1。在第16章关于SDLC的讨论中，因为进行了比特填充，所以允许每帧最多有6个连续的1，甚至在标志字段里也是如此。后面我们将讨论ISDN的第二层帧，它与SDLC类似。现在，让我们看一个实例。

如图19-12所示，只有两个终端A和B共享同一线路。它们的终端号称为TEI（Terminal End-point Identifier，终端端点标识符），并且已在图中给出，它是第二层的继标志字段（“01111110”）之后的地址字段的一部分。两终端的TEI分别为16（“0010000”）和0。因为它们都有信令信息要传输，所以它们都已被激活，并且优先级别值设为8。它们都在D信道上传送逻辑1（0V），由于没有其他终端连在线路上，因此NT将用E比特回应这些1。

它们两个都计数到8个连续的1，都开始发送级别2的帧。它们的标志字段是一样的，因此它们在E信道上收到相同模式的回波比特。就在这些标志之后，它们同时开始传送各自的TEI，因为它们的第三个地址比特不同，于是B的二进制0会在线路上形成一个电压，A的二进制1（0V）则不会。NT“看到”一个二进制0就把它返回，但终端A不会接收到它的1被返回，因此终止传输。B并不需要重新开始传输而是继续传输直到传输完毕，并在传完后将其优先级别降到9。

A会一直试图连续计数到8，但是不会成功。因为B的标志中有连续6个1，所以A也只能最多接收到6个连续的1。实际上，一帧里出现7个连续的1是有可能的，比如在帧被取消的时候。

B在传完之后，不得不停下来（没有电压），A就能计数到8，并开始它的传输。B现在不能传输，因为它必须计数到9。最后，当B的传输完成后，它就将其优先级别设为9。如果没有其他终端正在传输的话，它们俩就都能计数到9，并把优先级别重新设为8。这种控制D信道的方法称为CSMA/CR（Carrier Sense Multiple Access with Collision Resolution，带有冲突分辨的载波侦听多路访问）。

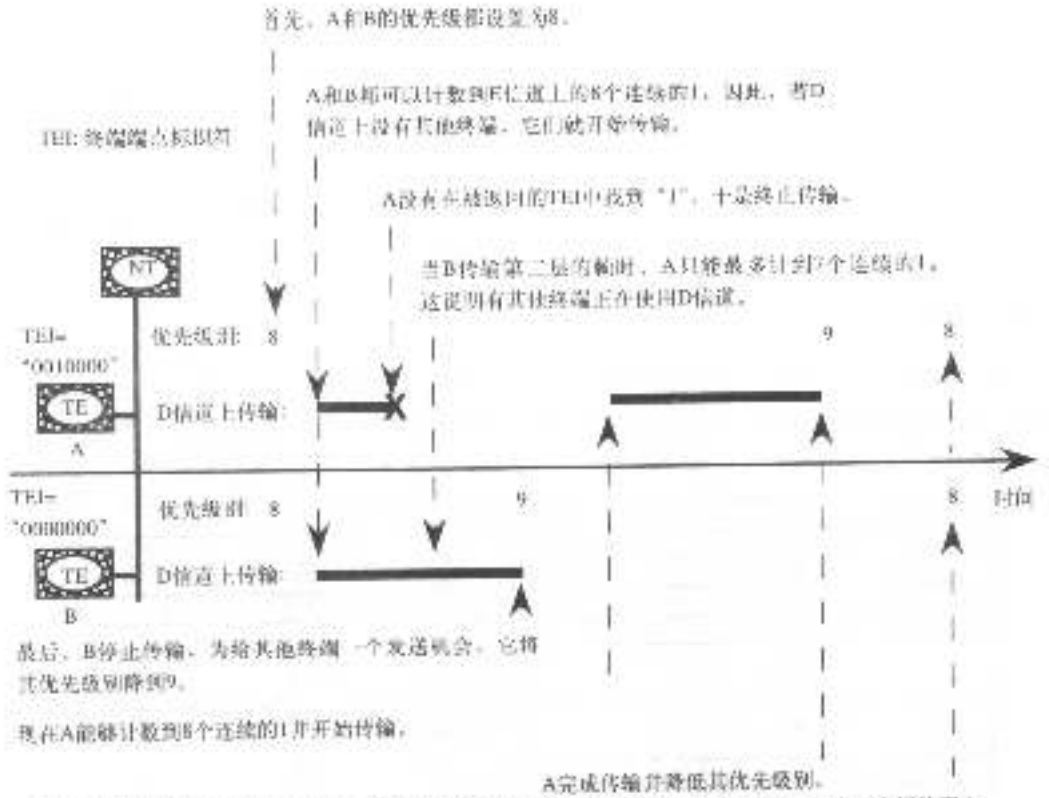


图19-12 如本例所示，即便A在X点处检测到冲突之后，CSMA/CR（带有冲突分辨的载波侦听多址访问）也允许B继续传输

19.4 PRI物理层

PRI一般终止于NT2，因此并没有为TE定义S/T接口。换句话说，PRI提供用户侧PBX与本地交换机之间的中继线连接。在该接口处有两种可能的情况，分别称为1.544Mbps和2.048Mbps接口，或称为ITU的G.703和G.704建议。

基于T1的1.544Mbps接口使用带有无干扰信道（clear channel）信令的ESF格式。也就是说，23条B信道的所有信令都在一条64kbps的D信道上传输。这就允许实时地进行逐个呼叫业务选择，亦即各信道能够为不同的业务建立，也能够被连接到不同的目的地。虽然采用T1是可能的，但必须预先就分配好，不能像PRI那样动态地配置。因此，正是D信道使得PRI有这么大的吸引力。如果没有D信道，该接口就与第15章中介绍的T1没有多大区别了。

19.5 数据链路层

19.5.1 为什么采用LAPD

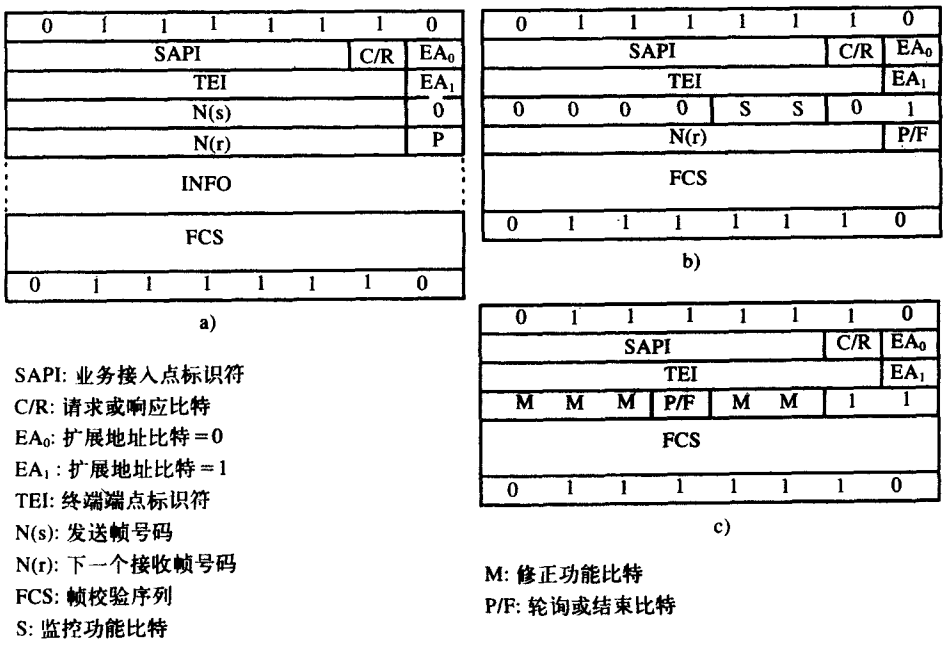
前面已经提到，ISDN的第二层和第三层仅关系到D信道。第二层（数据链路层）所采用的协议

称为LAPD（Link Access Procedures over the D channel，D信道链路接入规程），它与第16章和第17章中分别讲述的SDLC和LAP/B是类似的。本节是基于这些内容的，所以必要时可以参考一下这些章节。

与LAPD不同，LAP/B仅是用在DTE-DCE链路上的点到点协议。而LAPD却可以用在NT与多个TE之间，它是一种全双工的点到多点协议，SDLC也是这样一种协议。ISDN为什么不选用这个能运行在多点配置下的SDLC呢？原因之一就是SDLC使用查询方式，这使得可用带宽得不到充分利用。正如我们在前面所看到的那样，CSMA/CR能以更少开销、最小延迟进行多点传输。现在我们将只讨论LAPD与LAP/B和SDLC的不同之处。

19.5.2 基本帧格式

图19-13给出了现有的三种类型的帧格式，即信息帧、监控帧、未编号帧。发送第一个标志之后，接着发送值为0的EA（Extension Address，扩展地址）比特，表明该地址字段中还有一个八位组。8比特传完之后，发送一个值为1的EA比特，表示这是地址字段的最后一个八位组。



SAPI: 业务接入点标识符
C/R: 请求或响应比特
EA_0: 扩展地址比特＝0
EA_1: 扩展地址比特＝1
TEI: 终端端点标识符
N(s): 发送帧号码
N(r): 下一个接收帧号码
FCS: 帧校验序列
S: 监控功能比特

M: 修正功能比特
P/F: 轮询或结束比特

图19-13　LAPD帧的三种类型：a) 信息帧；b) 监控帧；c) 未编号帧，阴影字段为这些特殊帧类型的特征

如果发送帧是一条命令的话，C/R（Command/Response，命令或响应）比特就会被用户设置为0，被LE设置为1。如果发送帧是对一条命令的响应，则该比特的设置恰好相反。所有的信息帧都是命令；所有的监控帧类型（RR、RNR和REJ）既可以是命令又可以是响应；在未编号帧中，SABME、DISC、UI是命令，UA、DM、FRMR是响应，XID可以是两者中的任何一种。

SABME（Set Asynchronous Balanced Mode Extended，设置异步平衡模式扩展）、UI（Unnumbered Information，未编号信息）与XID（eXchange IDentification，交换标识符）对我们来说都是新的帧类型。SABME用于建立一条能传输127个连续帧而不需要响应的链路。我们很快就能看到UI用于发送不需要确认的信息，XID用来自动建立一条数据链路。

两个S比特给出监控帧的类型，5个M比特给出未编号帧的类型。与在SDLC中的一样，P/F比特被用作差错控制。

19.5.3 DLCI字段

DLCI（Data Link Control Identifier，数据链路控制标识符）是由SAPI（Service Access Point Identifier，业务接入点标识符）字段和TEI（Terminal Endpoint Identifier，终端端点标识符）字段组成的。TEI识别接口上的终端，SAPI可为终端的LAPD网络层进程识别接入点，该终端与LE中的对等进程有逻辑连接。图19-14给出了各种不同的终端及其业务接入点是怎样与它们在LE中的对应实体建立逻辑链路的一个例子。因此，帧不仅必须指定要连接的终端，而且必须指明连接到该终端的哪个业务接入点。

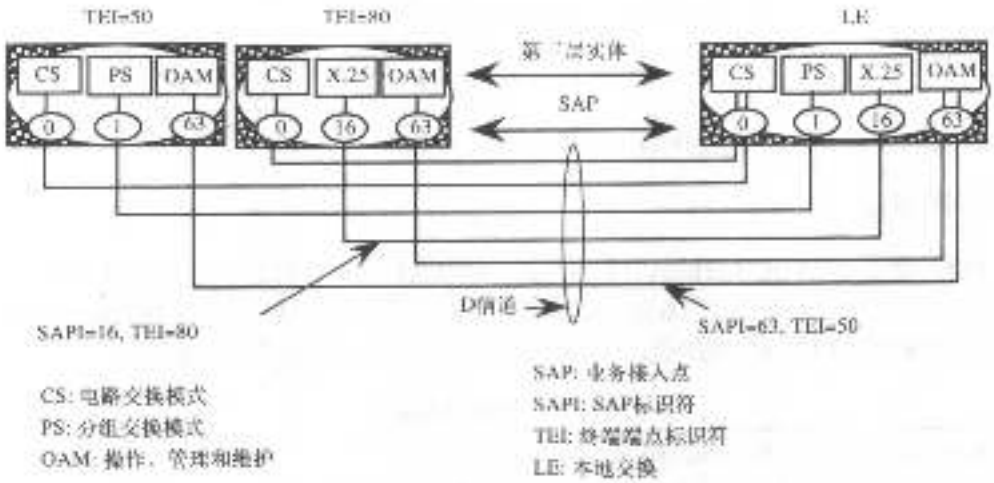


图19-14 由SAPI和TEI构成的DLCI（数据链路控制标识符）提供帧地址，不仅指明终端，而且指明SAP，即提供所需的第二层进程的接入

SAPI为0用于指定控制电路交换过程的业务接入点；SAPI为1用于分组交换模式下的传输；SAPI为16用在X.25通信中；SAPI为63则用在OAM（Operations、Administrations and Maintenance，操作、管理与维护）过程中。

共有三种类型的TEI分配：广播、自动和非自动。TEI为127，即全1，是广播地址，带着这个地址的帧被发送到线路上的每个终端。非自动TEI在终端中靠硬连线实现，可以通过在ROM（Read Only Memory，只读存储器）进行地址编码，也可以通过设置开关或其他物理办法来完成。在使用非自动TEI之前，必须经过网络侧即LE或NT2的允许。这些TEI的取值范围从0到63而自动TEI的取值范围则从64到126。

自动TEI分配是由通过LAPD协议向网络请求TEI的终端完成的。参见图19-15中的例子，我们能看出，其具体实现过程是由终端首先发送一个UI帧给LE。该帧的信息向LE表明终端正在请求一个TEI，因为这样一个操作是一个管理细节，所以它使用的SAPI为63；又因为终端还没有TEI，所以它采用通用的TEI值127。

LE也用一个UI帧来应答，该UI帧与其接收到的UI帧具有相同的SAPI和TEI值。但是，在该帧的信息部分，LE设定TEI值为101。现在，TE通过发送一个SABME并接收一个UA来建立逻辑链路之后，就可以交换数据了。注意SAPI为0对应于电路交换连接，而TEI为101对应于由LE分配的TEI。

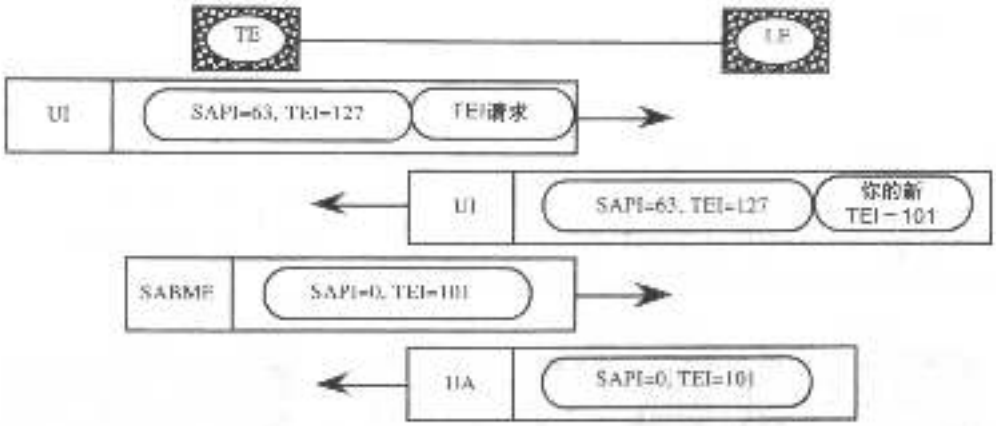


图19-15　向LE请求TEI，并且建立一条链路

19.6　网络层

因为D信道网络层所涉及的内容相当复杂，所以我们就不对其进行更详细的研究了。在讨论图18-14时我们已经介绍了它在电路交换模式中的功能。在那里，呼叫连接的建立与释放被看作是与SS7的ISUP层接口的D信道网络层。表19-4对网络层消息进行了总结。

表19-4　网络层消息类型

左边的两列规定相应的ACK和REJ消息类型是否存在
右边的两列规定该消息是由用户发送还是由网络发送，或者由两者传送

ACK	REJ	消息类型	简要描述和目的	用户	网络
呼叫建立消息					
*		SETUP	请求呼叫建立	*	*
*		CONNect	呼叫方应答呼叫	*	*
		ALERTing	被叫电话振铃	*	*
		CALL PROC	呼叫进行，接收所有信息		*
呼叫信息阶段消息					
		USER INFO	用于给另外一个用户发送信息	*	*
*	*	SUSPend	呼叫暂停，但信道仍然连接	*	
*	*	RESume	继续一个暂停的呼叫	*	
呼叫清除消息					
*		DETach	呼叫信息保存，信道拆除	*	*
		DISConnect	信息保存直到接收到REL COM	*	*
		RELease	信道和呼叫信息被释放	*	*
		REL COM	释放完毕，信道再次空闲	*	*
其他各种消息					
*	*	CANcel	请求取消一个设备	*	
*	*	FACility	请求设备，即前向呼叫	*	*
*	*	REGister	在数据库中进行设备注册	*	*
		STATUS	报告呼叫状态	*	*
		CON CON	用来控制或流量控制	*	*
		INFOrmation	建立呼叫或其他事由	*	*

网络层能够建立、保持并终止应用进程或实体之间的ISDN连接。它提供了一个用户到网

络层的接口。到ISDN目的地的地址是由三个可变长度的部分组成，它们是国家代码（最多3位数字）、国内有效号码（最多17位数字）以及子地址（最多40位数字）。

对ISDN的讨论就到此为止，下面我们将把注意力转向另一个重要的标准上，即SONET（Synchronous Optical NETwork，同步光网络），它是建立BISDN（Broadband ISDN，宽带ISDN）所必需的。

习题

1. 下面哪个ISDN功能设备用来将非ISDN设备变成ISDN的一部分？
   a. TE1　　b. TE2
   c. TA　　d. NT12
2. CO里与ISDN兼容的 DMS100交换机对应于下面哪个功能设备？
   a. NT1　　b. LT
   c. ET　　d. PH
3. 下面哪种电信业务既可以提供给承载业务又可以提供给用户终端业务？
   a. 补充业务　　b. 信息传送
   c. 普通业务　　d. 接入业务
4. BRI的U接口比特率是多少？
   a. 144kbps　　b.160kbps
   c. 196kbs　　d. 1.544Mbps
5. U接口是由哪个标准化组织定义的？
   a. IEEE　　b. ANSI
   c. ITU　　d. ISO
6. U参考点采用的是哪种线路编码？
   a. 伪三进制　　b. AMI
   c. 2B1Q　　d. 单极性
7. 如果A的TEI为12，优先级为9，B的TEI为14，优先级为10，C的TEI为10，优先级为9，D的TEI为8，优先级为10，那么哪一个站将首先传输？
   a. A站　　b. B站
   c. C站　　d. D站
8. 指出识别连接是电路交换还是分组交换的承载业务属性。
9. NT使用哪些引脚来传输数据？又采用哪些引脚为TE供电？
10. 一帧中有多少E比特从TE传送到NT？
11. NT给TE传送哪个INFO信号为其提供同步？
12. LAPD信息帧中的哪些字段是LAPB信息帧中没有的？
13. TEI为10说明是以什么方式为终端分配TEI？
14. 尽可能多地列出一个普通电话呼叫所涉及到的默认属性。
15. 讨论如何用电源3进行配电的各种不同方法以及它们各自的优点。
16. 激活与接入D信道的区别是什么？
17. 尽可能简单地解释一下接入D信道。
18. LAPD与LAPB相比的优点是什么？
19. 解释DLCI字段的各个部分以及它们的作用。

第20章 SONET

20.1 SONET：同步光网络

T1是贝尔电话实验室在20世纪60年代为在金属线上数字化传输24路话音信道而设计的。作为T1的扩展，T3技术支持通过微波系统传输672路话音信道。由于T1和T3都是建立在电信号传输的基础上，因而需要一种更适用于光信号传输的新技术。所设计的这种新技术应该使T承载系统的固有问题最小化，从而使其更易于组成网络。

1985年Telcordia（即后来的Bellcore）在其名为SONET（Synchronous Optical NETwork，同步光网络）的技术说明中提出了这些问题的解决方案。此后，SONET成为ANSI的标准并由ITU-T将其标准化为SDH（Synchronous Digital Hierarchy，同步数字系列）。ITU-T从中将“光”这一术语删除掉，这是因为当时SONET是通过其他介质比如数字微波来传送的。

SONET是一种多层协议，利用电路转换同步多路复用来传输高速信号。它是高速光纤系统的唯一标准，并可以促使宽带ISDN、ATM（Asynchronous Transfer Mode，异步传输模式）等未来新一代通信服务早日实现。

20.2 SONET与T3相比的优点

当一个M13多路复用器在其输入端口接收DS1信号时，这些DS1未必与公共时钟同步。DS1信号的传输速率并不是精确的1.544Mbps，允许有上下75bps的浮动。因此，M13多路复用器必须在需要的地方添加额外的比特以补偿比特率的不同。这样才可以将DS1帧正确地转换为DS3帧。这种添加额外比特的技术就被称作“比特填充”，不巧的是，这个名词也被用来描述在SDLC中每5个连续的1就在其后填充一个0的技术。由于比特填充被用在T3中，因此称其为异步多路复用或异步格式化。需要注意的是，这里采用异步这一术语与起始和终止比特无关。

异步多路复用的一个问题是当两点相互发送多路复用信号时，这两点之间的第三点如果不先对所有信道进行多路解复用就不能选择出其中的一个信道。这是因为在异步比特流中，属于某一特定信道的比特不会在规则间隔处出现，并且还有根据输入源的时序而填充的额外比特。因此，一个必须从信号流中提取信道（或添加信道）的中间节点必须有一个M13多路复用器进行多路解复用，有一个接线板进行交叉连接，以及有另一个M13多路复用器对新的信号流进行多路复用。该过程是非常难于运行和管理的，并且需要非常昂贵的设备。

另一方面，由于SONET的设备可以进行同步多路复用，故不需要比特填充。属于各信道的字节很容易被识别出来，这样SONET就可以使用ADM（Add and Drop Multiplexer，添加与提取多路复用器）。这种设备可以仅“捡出”（或提取）所需信道的比特而使其余的数据流无干扰地通过。SONET的同步多路复用可以在毫秒级的时间内将信道从一条链路交换或路由到另一条链路。与之形成鲜明对比的是T1 DCS（或DACS）要花费30分钟才能建立交叉连接。现在已经成为可能的光交换，可以以光速直接进行信号交换而无需先转换成电信号。

SONET的这种近乎瞬间交换的能力为其赋予了APS（Automatic Protection Switching，自动保护交换）的特性，也就是说可以将数据流从一条出现故障的链路重新路由到另一条激活的链路，而没有任何数据丢失。采用异步网路（比如T1网络），APS也是可能的，但是

会存在短时脉冲波形干扰并丢失部分数据。当没有提前通知需要带宽时，比如在灾难恢复时，网络会自动进行重新配置。

以上的管理能力是SONET备受推崇的一些优点。因为大量的数据都依赖于这些光纤链路，所以这些能力比以往的各种方法显得更为必要。将近5%的SONET带宽用于对数字网络进行监视、控制、重新配置、测试和预备，而用于ESF格式化的仅占0.5%。而且，正如我们在图20-1中所看到的那样，网络的管理能力是由分层体系结构中的各层提供的，用户可以像运营商一样管理属于他们的那一部分网络。这部分功能由SONET的OSS（Operation Support System，操作支持系统）来实现。

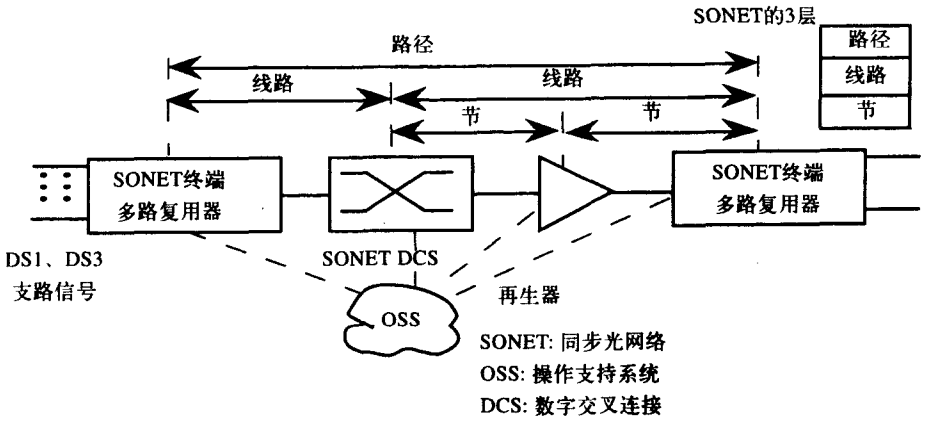


图20-1 SONET传输

采用SONET后，终端用户和运营商不必像在使用T3设备时那样成为设备制造商的“抵押品”。这是因为T3格式是专有的。相反，SONET是针对终端用户以及运营商和设备制造商的国际标准接口。这就使得客户可以自主选择设备制造商并将不同生产厂商生产的设备互相连接起来，这种功能就被称为“中间跨距连接”（mid-span meet）。尽管专用T3设备不得不保持其高价位，但SONET的价格最终会使T3的价格降低，这是因为会有更多的厂商提供基于SONET的标准设备。

顺便指出，SONET的标准传输速率为2 488Mbps，远远高于DS3的速率，而且还准备提速到13Gbps。另外，SONET仍然可以传输诸如DS3、DS1和E1等现有的信号格式。

20.3 SONET的速率与设备

表20-1列出了常用的SONET物理接口标准。STS（Synchronous Transport Signal，同步传输信号）帧承载电形式的数据，而其相应的光形式的信号称为OC（Optical Carrier，光载体）。为了从STS中产生OC信号，需要对STS信号进行加扰编码。需要注意的是，由于采用同步多路复用，因此STS的速率水平彼此恰为整数倍关系，而DS3的速率（44.736Mbps）就不是DS1信号速率（1.544Mbps）的28倍。

表20-1 常用的SONET接口标准

SONET同步传输信号	SDH同步传输模式	线路速率（Mbps）	有效载荷速率（Mbps）	光载体名称
STS-1	STM-0	51.84	50.112	OC-1
STS-3	STM-1	155.52	150.336	OC-3
STS-12	STM-4	622.08	601.344	OC-12
STS-48	STM-16	2 488.32	2 405.376	OC-48
STS-192	STM-53	9 953.28	9 621.504	OC-192

图20-1给出了三种类型的SONET设备：终端多路复用器、DCS（Digital Cross-connect System，数字交叉连接系统）和再生器。终端多路复用器既可以作为SONET网络的本地接入点又可以作为远程接入点。如果它被本地环路提供商使用，则称之为DLC（Digital Loop Carrier system，数字环路承载系统）。在这种情况下，它将被用作DS0信号的集中器，与CO交换机进行本地或远程连接。

DCS以DS1、DS3和其他速率提供直接的同步转换。它可以被一个ADM所取代，从而根据需要添加或提取信道。对于光纤来说，每35英里需要一个再生器，这些再生器除重建信号外，还可以提供检错、设备维护以及其他复杂的服务。

网络跨距（span）的三种类型是根据这些设备之间的链路进行定义的。对应于这些跨距又定义了三层，最低层是节层（section layer）。它用于成帧、加扰编码和定位错误。

两个节点之间存在一条线路，用于对SONET信号进行多路复用、同步、交换和交叉连接，它还用来为网络管理收集数据。最后，客户之间的端到端逻辑链路称为路径，它是SONET云中两个入口节点之间的电路。它为用户提供高级的维护服务。ADM是路径层的设备，故如果它取代了图中的DCS，则图中将存在两条路径而不是一条。

20.4　SONET传输结构

在如图20-2b所示的STS-1帧中，有90列9行，共810个字节。这一帧被分成传输开销和

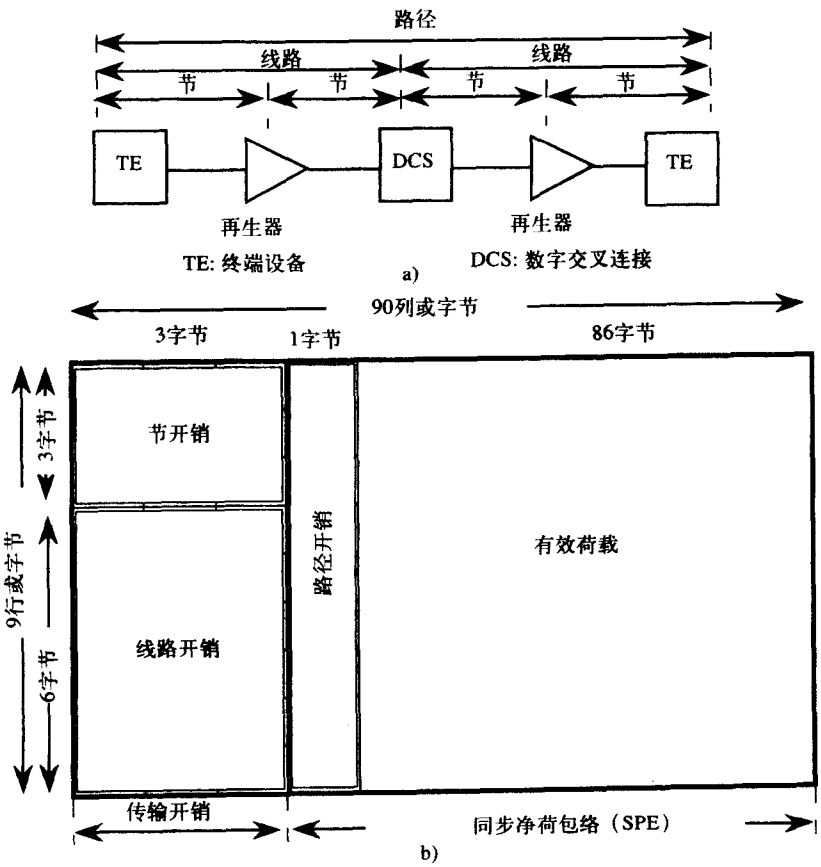


图20-2　a) SONET中三个不同的段类型：路径、线路和节。b) 带有路径开销、线路开销和节开销定位的STS-1帧格式

SPE（Synchronous Payload Envelope，同步净荷包络），分别由3列和87列组成。传输的顺序如下：首先发送传输开销的3个字节，之后是SPE的87个字节，接着再发送下一行的3+87个字节，以此类推。传输开销被进一步分为节开销和线路开销，而SPE被分成路径开销和承载支路数据的有效载荷。

图20-3提供了同一帧的更详尽的细节。传输开销中的DC（Data communication Channel，数据通信信道）字段用作网络管理信息。SPE的有效载荷被分成7个VT（Virtual Tributary，虚拟支路）组和18个打包字节。各VT组宽度为12列，可以包含一个或多个同类型的VT。VT类型是可以为用户承载固定数量带宽的给定数据块。VT1.5用于传输一路DS1信号，VT2用于承载一路E1信号，如图20-3所示。如果用整个SPE去承载一路DS3信号，则不再需要VT。因此VT是SPE的一部分，并且所使用的VT类型由支路发送的内容来决定。两列额外的“填充”（padding）字节可以用作异步信号的多路复用。

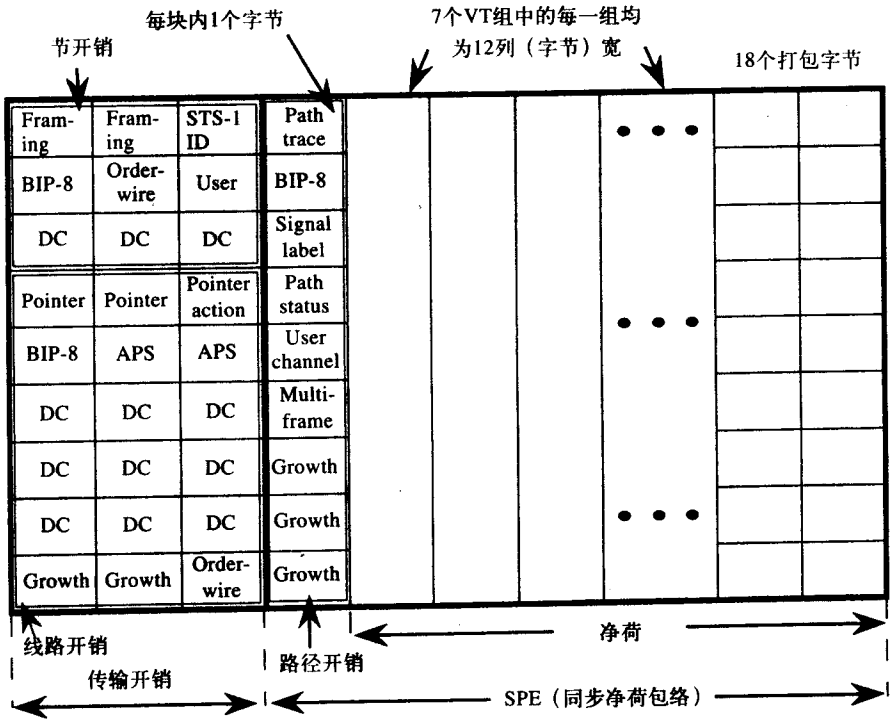


图20-3 90×9的STS-1帧格式，总共810字节长，每帧的传输时间为125μs，即每秒传送8000帧。有效载荷的传输能力是49.54Mbps。VT后面的括号内是一组所能容纳的VT数量和VT所能提供的数字信号速率

SPE在终端节点处集成，其路径开销包含端到端的管理信息。例如，信号标签就表示该有效载荷是包含一个DS3还是包含低速率信号的组合，即所使用的VT的类型和数目。路径开销紧随SPE，直至SPE到达目的节点，即形成了“路径”。同样，线路开销要经过所有节点处理，节开销则既要经过所有节点处理又要经过再生器处理。

SONET的优势之一就在于一个完整的SONET信号可以在载体（LEC或IXC）之间批量地进行

传递，而无需将信号解复用成DS0。然而，许多运营商都在使用他们自己的第一层时钟以保持网络的同步，不过这些时钟之间的确存在一些微小的差异，这称之为准同步（plesiochronous）。SONET并没有使用比特填充而是通过使SPE起始于STS帧的任何位置来允许这些时钟差异。因此，SPE通常是起始于一帧而终止于紧接着该帧的另一帧，如图20-4所示。这被称为“有效载荷漂移”。

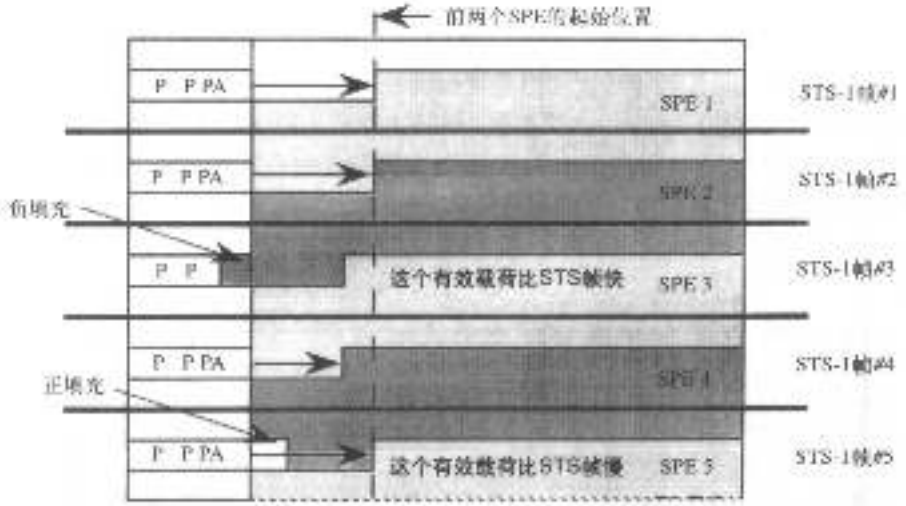


图20-4　SPE在STS帧内浮动以补偿微小的时钟差异，下一个SPE的起始位置可能只相差一个八位组

为了通知接收节点SPE的起始位置，在线路开销中使用了指针。指针就是STS帧中能够指示有效载荷起始字节的字节地址。如图所示，所有的SPE都不是起始于STS帧的开端，因此指针就包含SPE起始的字节地址。在图20-4中，SPE3过早地载入到STS帧中，因此指针动作字节用于包含给SPE2的数据，以使得SPE3尽早开始。这被称作“负填充”（negative stuff）。相反，SPE5载入得比较迟，就需要在SPE4中插入一个“正填充”（positive stuff）字节，这样就允许SPE5中的时钟差异。

除了这些可以表明各SPE在STS帧中的起始位置的STS指针外，VT也含有指针用于指示各VT在SPE中的起始位置的指针，因此，VT也是可以浮动的。

20.5　映射

VT被载入帧中的方法称为映射。映射的类型取决于VT是否浮动，支路信号是否与SONET时钟同步等等。如果VT在SPE中是浮动的，则需要附加指针来指示VT的起始位置。下面让我们看一看四种常见的映射，为此将它们画在图20-5a到图20-5d中。

最简单并且固定不可变的映射类型是异步DS3。它允许最常用的DS3信号作为一个“信息块”载入到SPE中去。这里，DS3比特未必与SONET的时钟同步，并且DS3信号也不能同步交换，但是它仍然允许传输现存的DS3信号。需要注意的是51Mbps的SPE速率低于DS3的速率，因此必须添加附加比特来弥补这种差异。

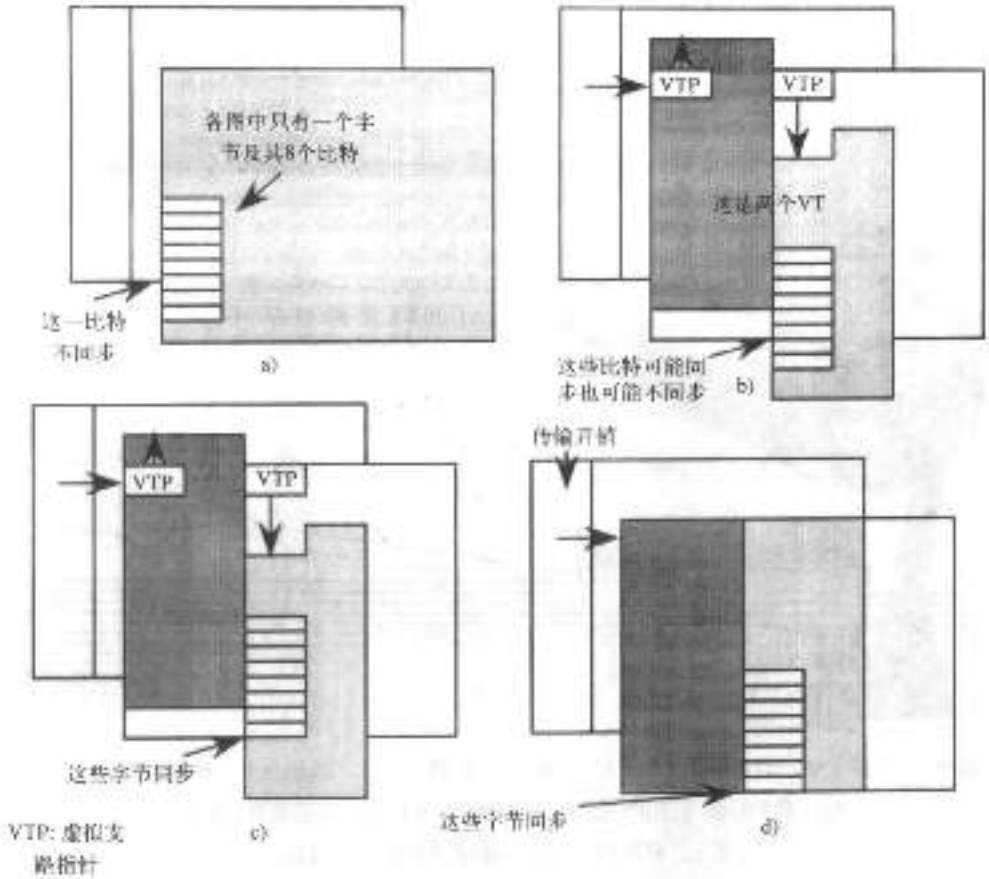


图20-5 四种映射：a) 异步DS3映射，b) 未信道化浮动VT，c) 信道化浮动VT，d) 信道化锁定VT

未信道化浮动模式的DS1映射允许VT浮动，并且支路比特可以与SONET时钟同步也可以与之不同步。这里，设备必须处理更多的指针，但是VT的同步转换是可以实现的。例如，这就意味着一个DS1信号可以被“动态”（on the fly）寻址、添加或提取，而DS0信号却不能。

信道化或字节同步浮动模式DS1映射要求DS1信号的字节与SONET的字节同步。这里，不仅DS1信号能够被识别和交换，而且DS0信号也可以被识别和交换。

最后一种是信道化或字节同步锁定模式DS1映射，它不允许VT浮动，因此需要很少的指针处理。然而，相位和频率都需要保持，这样才能获益于DS0信道便捷的交叉连接和交换。从图的下侧可以看到，锁定模式比浮动模式有更多的延时。

20.6 回顾

我们通过将SONET与19世纪火车、汽车发明之前的运河系统相比较，来回顾一下SONET的基本概念，如图20-6所示。

运河的水路就像SONET光纤的“光路”。驳船连同骡子队和赶车人就类似于一个STS帧。假设驳船就是一个SPE，骡子队及其赶车人就是传输开销，传输开销进一步分为节开销（骡子队）和线路开销（赶车人）。船上的货物从一条船运到另一条船上，就像SPE从一个STS帧浮动到另一帧一样。

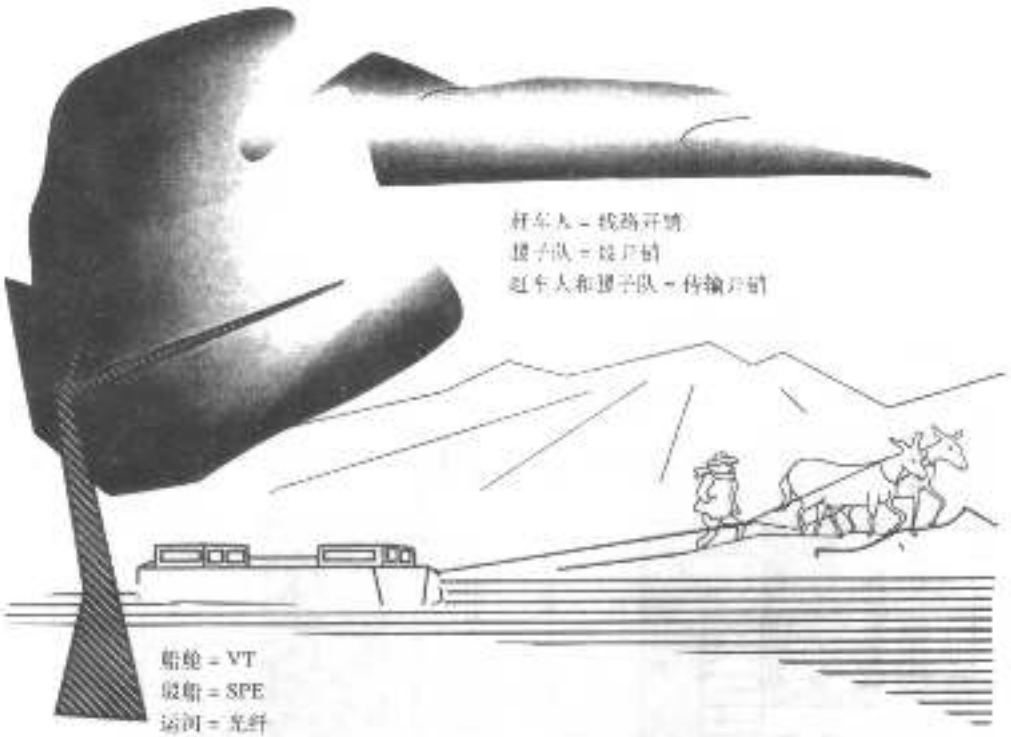


图20-6　在19世纪初，将驳船从奥尔巴尼（Albany）拖到布法罗（Buffalo）只需要9天时间，平均每吨花费6美元；而用四轮马车需要20天，平均每吨需要花费100美元。现在，SONET能以更快的速度传输数字信息

驳船的船长要一直随船而行直到目的地。我们所说的船长就是路径开销。他/她知道船上装有什么货物以及这些货物的位置。但是，为了便于类比，我们假设驾驭骡子队的赶车人仅到达下一个运河交叉处。在那里，驳船将获得一个新的传输开销（骡子队和赶车人）并继续其行程，到达下一个交叉点驿站或者它的终点目的地。

在两个交叉点之间，骡子队也就是节开销，需要进行“补给再生”，即摄取食物和水，或者是就地休息由驳船商的另一支骡子队代替。

我们可以把驳船上的三个船舱类比为VT组。每个船舱都有特定的用途，比如，一个船舱仅用来装食物。另外两个船舱只装煤和木料。类似地，VT组仅承载一种类型的VT。VT本身可以认为是一些装谷物的口袋或者装有某种东西的其他容器，至于装有什么东西就要取决于用户想要运输的货物是什么。因此，在许多方面，通过SONET传输信息就类似于通过运河系统运输货物。

20.7　SONET环

由于SONET可以承载大量的数据，因此某段光纤出现断裂或者是时序出现问题都会导致用户通信中断。为了防止这种灾难性故障的发生，SONET一般都配置成环形。

图20-7所示为一个两根光纤的ULSR（Unidirectional Line Switched Ring，单向线路交换环）。其中一个环路称为保护环路，通常不承载任何流量；另一个是有效（或服务）环路，它承载所

有的流量。因此，当NE（Network Element，网络元素）-A想要和NE-B通信的时候，它只需通过一个跨距（span）。然而，NE-B却要通过四个跨距才能与NE-A通信，这是因为所有流量是单向传输的。一个方向的通信业务延迟时间要比另一个方向的延迟时间长。我们只有在第二个图所示的通信出现故障的情况下才使用逆时针方向。

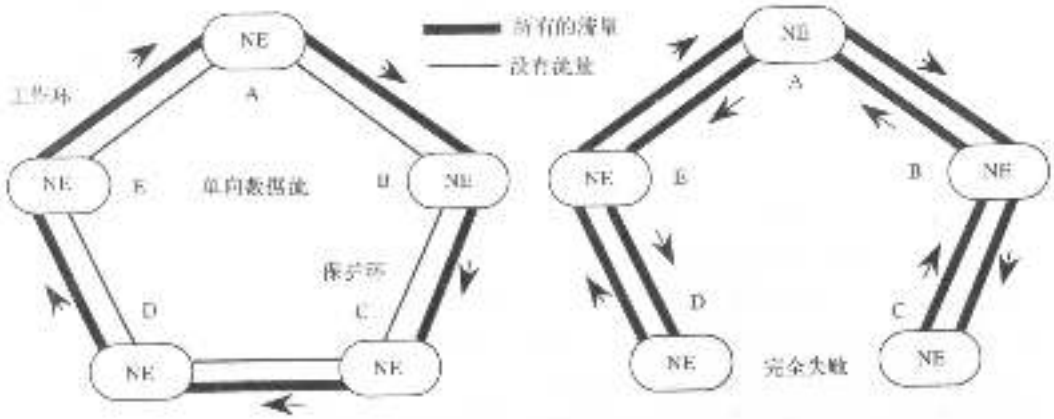


图20-7 两根光纤的ULSR（单向线路交换环）用一个环正常工作。如果两根光纤都被切断，两个环就组合成一个圈

这些类型的环路通常应用在大城市或延时差异可以忽略的城市里。因为一根光纤的全部容量可以从一个环路传输到另一个环路，所以这是一个线路转换环路。如果是路径交换环路，则只有部分光纤容量可以在必要的时候交换到备用环路中。例如，如果图20-7中的各链路容量为OC-12，则整个OC-12都需要进行转换。但是在路径交换环路中，却只能交换其中的一部分容量，比如只能在OC-3或OC-1信号级别甚至VT级别上进行交换。

图20-8是一个四根光纤的BLSR（Bidirectional Line Switched Ring，双向线路交换环路）。在双向环路中，正常运行的流量都是双向传送的，因此，NE-A传送到NE-B或者相反的情况所产生的延迟都是相同的。实际上存在四个环路，在正常运行期间流量仅在两条环路上传输，而另外两条环路则处于保护模式。

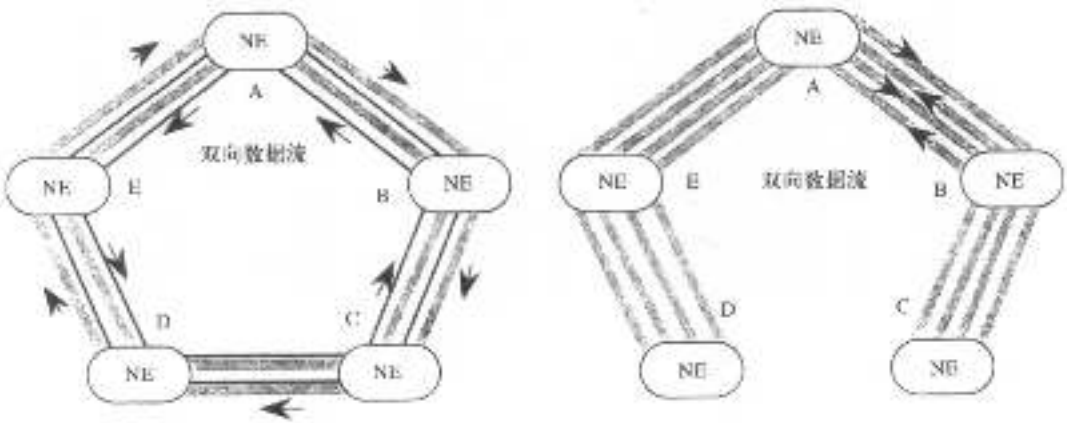


图20-8 四根光纤的BLSR（双向线路交换环）在每个环上传送一半的流量，一旦线路出现故障，所有环就环绕成两个圈

如果由于设备故障而使得四根光纤链路中的一根或两根线路不起作用，则环路的其余仍完好无损。在这种情况下，就只能在受影响的区域进行交换，称为**区域交换**（span switching）。但是，如果是挖土机导致了中断，那么很有可能这个跨距上的四根光纤链路都被切断。这样的话，就会发生如图所示的**环路交换**（ring switching）。

四根光纤的双向环路被广泛用于广域承载商和IXC。采用这种环路，区域交换和环路交换都是可能的。由于它的光纤链路是两根光纤环路的两倍，因此，这些环提供了双重的保护。

习题

1. SONET的管理方案被称为什么？
   a. ADM　b. OSS　c. APS　d. 中间跨距连接（mid-span-meet）
2. 说出SDH与SONET之间的一个不同点。
3. 在SONET中，有效载荷与路径开销一起被称为什么？
4. 写出ISDN与传统POTS服务相比有哪些优势和劣势。
5. SONET与T3相比，有哪些优势和劣势？
6. SONET中使用比特填充吗？如果不使用，用什么来代替它？
7. 精确地讲，一个OC-48内有多少个OC-3？
8. ADM是路径设备、线路设备还是一个段设备？
9. 给出STS-1帧中现有的3种类型的开销。再生器可以修改哪种开销？
10. 三种类型的开销长度分别为多少字节？
11. 给出并解释SONET中的四种映射。
12. 写出下列各种类型环路之间的差异：单向和双向，线路交换和路径交换，2根光纤和4根光纤。

第21章 帧 中 继

帧中继网络业务在过去的7年里几乎每年都以50%的速度增长。帧中继是X.25网络的一个简化版,它来源于ITU-T对ISDN所做的标准化工作，而且已经成为取代专用线路的一种廉价方式。采用帧中继通常可节省30%的费用，若用于取代专用线路，那么所节省的费用会更多。帧中继业务比较简洁，也容易理解，在市场占有率方面有很好的业绩。虽然公共运营商正在用ATM交换机替代原先的网络结构，但帧中继已经有了很坚实的根基，并将在以后很长的一段时间内被应用。

21.1 交换网络概述

第2章的结尾讨论了在分组交换网络中的信道标识符的概念，我们看到在这样的网络中各物理信道中的这些信道号是如何在两个端用户之间创建一个虚电路的。随后，在5.1.1节，我们比较了交换电路与专用线路，表5-1总结了它们的区别。在表5-4和5.3节中，我们对PVC（Permanent Virtual Circuit，永久虚电路）、SVC（Switched Virtual Circuit，交换虚电路）、X.25、帧中继和ATM有了初步的了解。如果你学习这些内容已经很长时间了，现在最好再复习一下，由于虚电路的概念对于帧中继和下一章的主题——ATM都非常重要，因此在学习帧中继之前应进一步了解这些内容。

21.1.1 X.25、帧中继和ATM中的虚电路

图21-1给出了一个分组交换网络，图中三个分组交换机为：A、B和C，交换机之间由三条专用线路相互连接，各交换机有三个端口，编号为1、2、3。每台交换机的一个端口连接到用户端的某设备上，该设备标为CPE（Customer Premises Equipment，用户端设备），这样就给出了由分组交换网络连接起来的三个用户端。

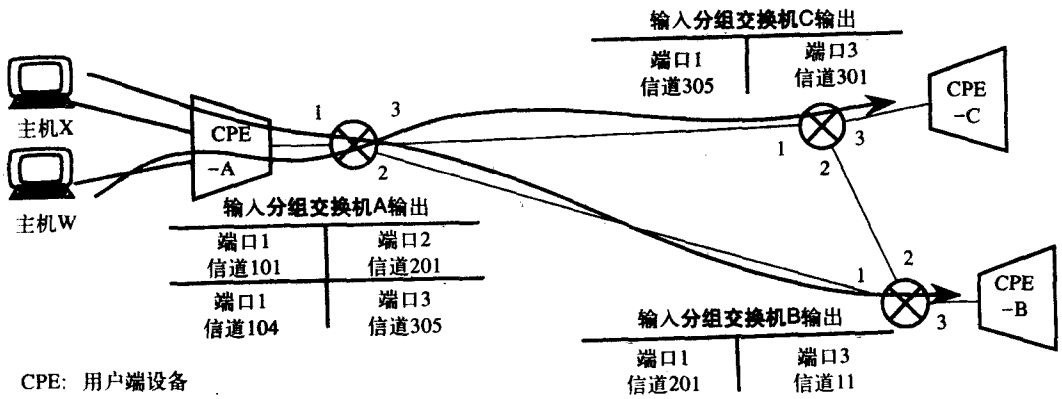


图21-1 通过一个分组交换网络建立的两个虚电路，其中每一个由分组交换表定义

分组交换网络可以是X.25、帧中继和ATM网。对于ATM网而言，由于传输单元有长度固定，因此“分组”一词用“信元”代替。在OSI第三层中可变长度的数据单元称为“分组”。

帧中继主要运行在OSI参考模型的第二层，因此相应的数据单元便称为“帧”。在任何一种情况下（X.25中的分组、帧中继网络中的帧或者ATM网络中的信元），虚电路的操作都可以用图21-1表示。本节使用分组和分组交换机来说明这三种类型的网络。

分组交换网可以是专用交换网。在这种情况下，一个组织将拥有所有的交换机，同时租用所有与其相连的专用线路。然而，这些类型的网络通常是公用网络，因为网络运营商拥有网络及其设备，而私人组织仅仅是将他们的设备连接到这些网络上。因此，就使用了CPE这个术语，CPE就是用户连接到服务提供商网络上的设备。

在帧中继网络中，CPE最有可能是一台路由器，也可能是为某组织提供话音电路交换的PBX，抑或一个将来自用户的不同类型的数据流合并到交换网中的复用器。CPE也可以称为集线器（hub）。在上述任一种情况下，CPE都会知道交换机中所使用的协议（不管是X.25、帧中继还是ATM）。CPE必须能够与其使用特定协议连接的分组交换机进行通信。

当用户设备没有帧中继接口时，用户必须购买一个FRAD（帧中继接入设备），这是一个能够将诸如SNA、X.25等协议连接到帧中继网络中的非常便宜的设备。VFRAD是一种特殊的FRAD，它将话音连接到网络中。图21-1中的CPE可以是这些FRAD中的任何一种。

在图21-1中，分组交换机PSwitch A在端口1接收分组，根据交换机的交换表，在分组头中以信道101编码的那些分组被交换到端口2。这些分组的信道号在新分组头中将变为201。当分组经过一台交换机时，数据部分保持不变，仅仅是分组头发生变化，并且分组头中的信道号是根据交换机的交换表而改变的。

这些分组到达分组交换机PSwitch B的端口1，按照交换表，它们被交换到端口3的信道11，然后CPE-B将从来自不同信道号的分组中筛选出信道11的分组。在CPE之后的用户端会出现什么情况并不是我们现在所关注的问题，我们所知道的就是那里的CPE将处理那些细节问题。由各物理链路上的信道号所定义的、通过网络的路径描述了两个端点之间的虚电路。同时，图21-1还给出了从主机W经由CPE-A并到CPE-C结束的虚电路。

你可能会记起乘客在一个城市换乘班机的类比。乘客在每一次登机前拿到的登机卡如同一个分组头，定义他所乘坐班机的座位号（信道号）。乘客如同一个数据分组，从一个城市出发到另一个城市结束。他所经过的路线包括两驾飞机和相应的座位，这描述了一个虚电路。在他旅程的每一段可以为其分配相同的座位，但这往往是不可能的。分组交换网络中的信道号的分配与之类似。

这些信道号在我们讨论的三种技术中的名称不同。在X.25中，它们被称为LCI（Logical Channel Identifier，逻辑信道标识符），每个LCI包含两部分，其中一个称为LCGN（Logical Channel Group Number，逻辑信道组号），另一个称为LCN（Logical Channel Number，逻辑信道号）。类似地，ATM的通路号用VPI（Virtual Path Identifier，虚通道标识符）和VCI（Virtual Channel Identifier，虚通路标识符）描述。帧中继仅使用一个称为DLCI（Data Link Connection Identifier，数据链路连接标识符）的信道标识符，它没有像其他两种技术那样使用一对信道号。

应该从以前的讨论中记起，这里用到了多路复用。给主机X和W的数据分组是通过从CPE-A到分组交换机A的一条物理链路发送的。更确切的说，在这里进行了统计多路复用。也就是说，如果信道101使用了这条链路中所有的带宽，而信道104处于空闲状态，这样是可以的。统计多路复用允许共享不同数据源之间的网络链路，它使网络资源的利用率更高。在新泽西州收费公路的某些地段，卡车不允许在小汽车车道上行使，那里的交通流量不是统计复用。如果小汽车车道正处于空闲状态，而卡车车道阻塞了，也决不允许卡车占用小汽车车道。

21.1.2 PVC和SVC

我们一定会想到的一个问题是：这些交换表是如何在第一时间产生的？如何使用表中的条目定义一条通过网络的虚电路？有两种基本方法来解决这个问题。如果该电路是操作员在网络管理终端上手工进入通道产生的，它就称作PVC（Permanent Virtual Circuit，永久虚电路）。由于操作员也可手工去除这条虚电路，所以该虚电路事实上不是永久存在的，因此，我们倾向于称这种虚电路为“供给虚电路”（Provisioned Virtual Circuit）。

PVC每次可以保持数天，虽然产生PVC只需简单地沿着电路路由增加一项条目，但是运营商需要用两天时间去准备这样的电路。事实上，填写文件资料比实际在交换机进行更新需要花费更多的时间。

当一台CPE通过网络拨通另一台CPE，并创建一条虚电路时，此虚电路就叫做SVC（Switched Virtual Circuit，交换虚电路）。电话机并不能完成此种拨号功能，该功能是由CPE呼叫另一台CPE完成的。为了建立一条SVC，CPE必须知道目的地址，之后由一个信令协议去更新交换表并建立连接。这与在话音网络中所使用的7号信令在功能上类似。

目前，虽然运营商已经开始谈及SVC，但是帧中继并不提供SVC。因此，本章将不讨论SVC。由于X.25和ATM均支持SVC，所以在第22章我们将讨论ATM是如何处理信令的。

21.1.3 交换网的优点

假如你有一个如图21-2a所示的专用线路网络，将来自不同地方的多路复用器相互连接起来。除了租用这些线路的费用外，你需要为每条线路连接一个单独的端口卡，这不仅增加了费用，而且增加了管理的复杂性。

假设你要在网络中增设一个新的站点，如图21-2b所示。为实现一个完全的网状网络，即实现任何两个端点之间都有连接的网络，那么你必须另外增加三条专用线路，必须为每一个现有的多路复用器增加一个端口，并购买一个3端口的多路复用器。为开通这个新的网络，你首先必须关闭整个网络，停止所有站点的运行。每次为网络增加新的站点时，如果出现故障，你不得不花费足够长的时间去排除故障。如果超过了开通网络的时间限制，就必须再做一个援助计划，以便在其他时间重试。这些副作用只会随着网络规模的扩大而增加。

图21-2c说明了帧中继迅速流行起来的一个原因。不仅每一个多路复用器只需一个端口接到网络中，而且当有一新站点加入到网络中时（图21-2d），对网络的其他部分也不会有任何影响。唯一需要做的就是在某一地方的控制台上输入新的PVC。这项工作通常由运营商完成；当然，如果运营商提供给用户控制台的话，用户也可以自己完成。

帧中继（广义交换网）的最大优点是CPE可以容易地收集业务流量的测量结果。从这些统计结果，用户可以推算出是否需要更大的容量，或者用户通过减小其网络容量来进一步节省费用。

交换网络的成本总是比专用线路网络至少低30%，这是因为在交换机之间的中继线是由许多用户共享的，运营商可以把那些节省下来的费用转嫁给用户。对于端用户而言，网络的整体复杂性明显下降。用户不用关心运营商如何在网中进行数据交换，所关心的仅仅是从一个地点开始，结束于另一个正确的地点的虚电路，至于流量跳了多少跳及其所在的通路号，他都不用关心。如图21-2c与图21-2d所示，网络仅仅被看作是一个“大云团”，用户可以自由地接入。

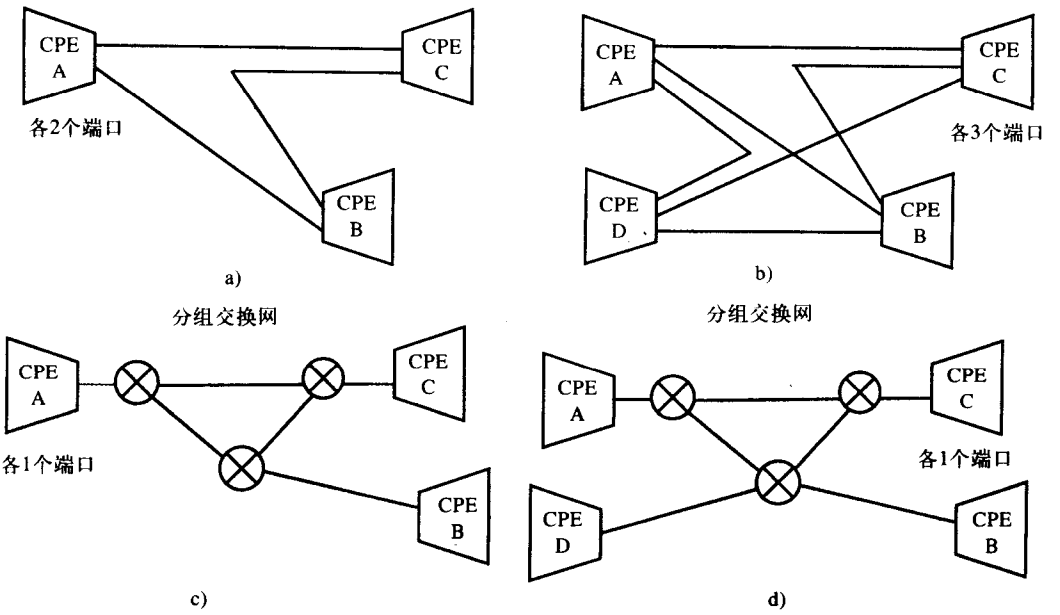


图21-2 a) 被扩展为，b) 的租用线路网络， c) 被扩展为，d) 的分组交换网

由于网络中存在大量的备用线路，因此交换网具有更高的可靠性，网络的灵活性也提高了。是否从一开始就完全正确地设计网络并不那么重要，网络的容量和PVC线路可以随时进行调整。然而，在签定合同时，应当规定允许这样的灵活性存在，但价格不会急剧上升。

许多组织利用帧中继网络将他们的公司办公室与许多地区和分支机构的办公室相连。在这种情况下，公司的数据中心需要在其他地方设置一个数据备份中心，主数据中心和备份数据中心需要保持其数据的同步。如果一个中心发生了故障，另一个中心要能很容易地承担起整个工作。

在一个租用线路的网络中，必须提供备用线路。然而，采用交换网时，线路备用非常容易。PVC可以从所有分站点输入到两个数据中心，这样用户可以事先明白：正常情况下，他的流量将只在结束于主数据中心的PVC上传送。只有在主数据中心发生故障的情况下，才使用结束于副数据中心的PVC。这种备用PVC的成本仅仅是主PVC成本的5~10%。这是因为运营商知道用户只是偶尔使用备用PVC。

21.2 对帧中继的不同认识

21.2.1 从OSI的角度认识帧中继

当从帧中继如何与OSI参考模型相关联的角度看待帧中继时，我们基本上将它看作第二层协议。毕竟，第二层将帧作为交换的基本单元。但是，正如图21-3a所示，并非第二层的所有功能都合并到帧中继中去了。此外，帧中继还有一些第三层的功能，这些第三层功能都是SVC所需要的信令处理。

该信令协议称为Q.933，它是ISDN 的D通道所用协议Q.931的一部分。因为目前在帧中继业务中还没有SVC，所以帧中继实际上只支持OSI模型的低层一层半协议。

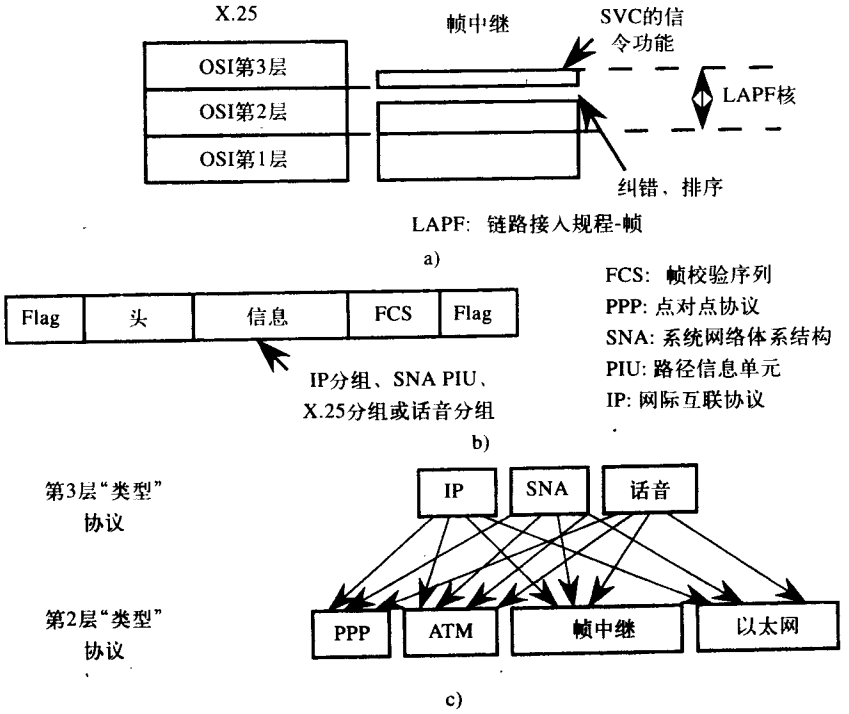


图21-3 a) 帧中继借用OSI参考模型的三层功能; b) 帧中继基本上是第二层协议; c) 任何"第三层"类型的数据单元都可以被封装在帧中继帧的信息字段中,即封装到任何"第二层"类型帧的信息字段中

有几个第二层的功能是帧中继所不支持的，这使得帧中继不仅是X.25的一个简化版本，而且也是X.25的第二层协议HDLC的一个简化版本。这使得帧中继服务速度快，但是支付的费用却比其他服务少。这个协议的名称叫做LAPF（Link Access Procedure-Frames，帧链路接入规程-帧）核。LAPF核是用于SVC的LAPF的一个子集。目前，网络中使用的都是LAPF核，因为所有运营商都支持PVC。

依次对帧进行编号是帧中继省去的第二层功能。缺少帧序列号就不允许设备因错误而要求重新发送。错误能够被检测到，但是在这种情况下，不必通知发送方这些帧有错，而是简单地将它们丢掉。与HDLC不同，LAPF核并不提供任何流量控制措施，例如使用一个窗口字段。如果数据帧到达的速率超过了设备所能处理的速率，那么这些帧必须被丢弃。

图21-3b给出了帧中继（LAPF帧）的基本格式。它看起来与SDLC和HDLC非常相似，唯一的区别在于头部所用字段的定义。我们将在以后再研究头部。信息字段几乎可以封装任何协议。我们可以封装IP分组、SNA分组等等。因此，我们可以用任何第二层协议进行同类型层的复用。图21-3c表明我们可以将IP、SNA或话音封装到一个PPP帧、一个ATM信元、一个帧中继帧或一个以太网帧等的内部。

图21-4给出了在整个网络中OSI各层的运行。在端用户的CPE上，七层协议均得到实现，而在网络中只实现了第一层和第二层（实际上仅是第二层的一半）。这表明CPE-A发送的分组被封装在一个LAPF帧中，该帧从一台交换机发送到另一台交换机，直至到达CPE-B。从该帧中提取出分组，并传递给应用程序。记住：该帧在网络中使用PVC传输时，在每一跳仅DLCI发生变化，这种情况就像乘客在机场换乘班机时座位号的改变。

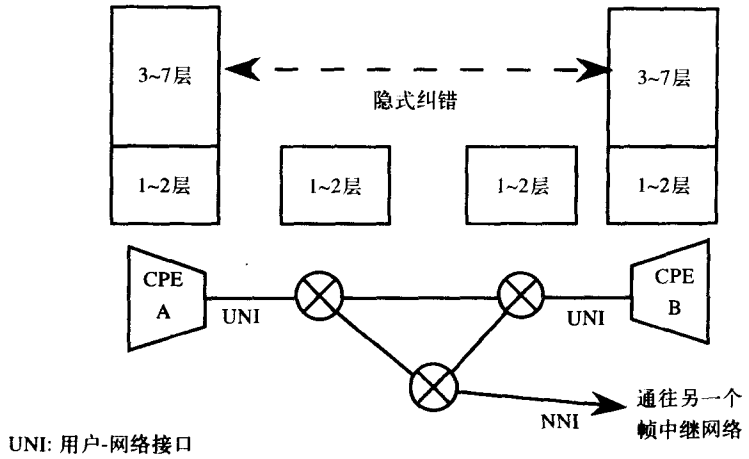


图21-4　在用户终端七层协议都被实现，但是通过网络接口和穿越网络时，仅低两层协议被实现

该图还表明纠错是由上层协议完成的。如果网络不做任何通知就丢弃某些帧，那么这些帧怎样重新发送呢？当NIC通过LAN发送帧并且因为差错丢弃帧时就会出现这个问题。IP协议是这样的，这里的帧中继也是如此。对于IP协议而言，我们期望第四层协议——TCP能够对分段进行排序，检测并纠正错误，提供流量控制等功能。如果没有TCP，而纠错又确实需要，那么就由位于端用户处的某些其他应用程序或软件来负责纠错。因此，与IP数据报网络一样，帧中继网络给终端留下了更多的工作，网络本身并不具有纠错的健壮性。所以，“隐式纠错”意味着错误不是由网络来处理，而是由终端来处理。

21.2.2　用户对帧中继的认识

就用户而言，对帧中继的认识非常有限。用户对帧中继的认识仅局限于他要付多少钱以及他从网络中得到多大的带宽。

图21-5给出了形成用户对网络的认识的六个因素。它们是CPE、接入线、端口、网络本身、PVC和CIR（Committed Information Rate，承诺的信息速率）。

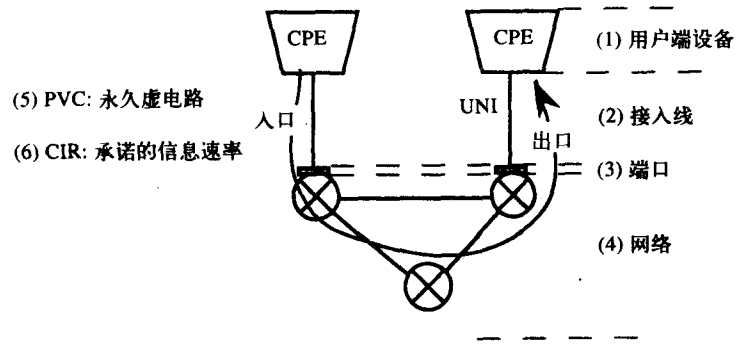


图21-5　从用户角度看到的网络的六个组成部分，PVC开始于网络的入口一侧，到达网络的出口一侧

接入线：接入线将CPE连接到第一台交换机的帧中继接口上，该接口称作UNI（User-to-Network Interface，用户-网络接口）。从一家运营商的帧中继网络到另一家运营商的帧中继网

络的接口称为NNI（Network-to-Network Interface，网络-网络接口）。UNI和NNI如图21-4所示。例如，AT&T公司的帧中继网络与贝尔大西洋公司（Bell Atlantic）的帧中继网络的接口就使用NNI接口。然而，运营商不喜欢做那样的事，因为管理信息不能够非常容易地通过NNI接口传递。但对于需要连接到海外帧中继网络的用户而言，运营商别无选择，只能提供这种互联。

通过接入线，终端用户节点每30秒发送STATUS ENQUIRY消息来查询网络，这称为心跳式查询。网络通过给用户返回STATUS消息做出回应，这些消息说明哪些虚电路是新的，哪些正在被拆除等等。缺少这两种消息中的任何一种都说明连接已经中断。这种查询是由UNI上的LMI（Local Management Interface，本地管理接口）所支持的。

接入线可以是56kbps的线路,也可以是FT1（Fractional T1，部分T1）或T1线路。FT1线路的好处在于，如果你需要提高接入速率，比方说，从256kbps提高到384kbps，仅仅需要改变终端设备的配置参数，这在一夜之间便可完成。如果你的传输速率下降了，那么为了节省费用，接入速率可以很容易地调低。

接入IXC的帧中继网络可以通过LEC的帧中继网络实现。当许多邻近的区域需要联合起来组成一个长距离网络时，这种配置更加合适。但是如果仅使用一台LEC帧中继交换机来连接所有邻近的区域，那么这台交换机会成为发生故障的中心节点。

你可能想通过拨号备用线路接入到为你提供服务的运营商的网络中，该线路可以是BIR、PRI或者是SW-56kbps备用线路。但是应该当心，如果基本速率线路和拨号线路通过同一管道或者到达设备的同一点，那么这种备用就毫无意义了。同时，应当记住你的DSU（Data Service Unit and channel service unit，数据业务单元和信道业务单元）能够自动地交换到一个ISDN备用设备。然而，当你的基本速率线路恢复正常时，DSU不会自动回到主线路上。如果你忘记从DSU交换回来，那你可能在月底吃惊地收到一个大额的ISDN账单。

端口卡：第一台交换机上的接口称为端口或者端口卡，它是接入线的连接处。现在端口的速率可以低于接入线的速率。事实上租用一个比接入线所支持的速率高的端口是毫无意义的。就在最近，运营商已经开始提供DS-3或者45Mbps速率的帧中继服务。然而，通常你仅以T1/E1速率或更低的56kbps的速率接入帧中继网络。

PVC：在一条接入链路上通过一个端口的PVC（Permanent Virtual Circuit，永久虚电路）有许多，各PVC以UNI上唯一的DLCI（Data Link Connection Identifier，数据链路连接标识符）进行标识。用户不必关心网络运营商如何在网络中切换电路。事实上，规范中并未提及此事。如果大量的报务员同时在网络中以达成协议的速率发送数据帧，那么就标准而言，这是非常好的。用户所关心的全部内容仅仅是在其入口处以某DLCI标识的一个特定PVC以一个指定的DLCI到达其出口处。因此，甚至是PVC所途径的距离（除非国际线路）也不影响价格。帧中继计价对距离不敏感，交换机并不理会账单信息。这也是帧中继服务快捷的另一个原因。

CIR：用户认为帧中继是一项服务而不是一个网络。他不关心也不需要知道虚电路是怎样实现的。他购买以某种速率到达某个地点的PVC，他唯一关心的是服务提供商为其提供的服务。运营商同意在一条给定的PVC上传送终端用户的业务的速率称为CIR（Committed Information Rate，承诺的信息速率），它应该是用户在这一给定PVC上发送的平均业务量。即使用户以CIR发送数据，仍然不能保证网络能够传送所有数据，某些数据帧可能因为拥塞而不得不丢弃。相反，如果其他用户或者其他PVC没有在给定的时间内传送，那么用户就可以以高于CIR的速率传送业务，这称为**突发**（burst）。分配给一条接入线的CIR总量应该小于或等于接入线的速率。例如，假设在你的位置，有两条CIR为32kbps的PVC，那么接入线的速率和端口的速率应该是64kbps或更高。

21.2.3 运营商对帧中继的认识

基本上，运营商认为网络就是提供给客户的服务，网络内部怎样连接并不是客户需要知道的事情。当首次提供帧中继业务时（大约在1992年），还没有像帧中继交换机这类产品。因此，采用了X.25交换机，并为其装上新软件来代替帧中继交换机。帧中继基本上是一个基于软件的协议，客户没有必要知道他们正在使用旧的分组交换机，他们所关心的只是其PVC能够达到CIR。

后来，这些交换机都被帧中继交换机所取代，这时客户所知道的大概只是PVC的性能正在提高。现如今已经没有厂家再生产帧中继交换机了。从1998年开始，主要运营商的所有交换机已经被ATM交换机所代替。但是，因为ATM不为公众所接受，并且只是被看作一种大肆宣传，所以运营商没有宣传他们的网络是基于ATM的。

现在，客户将业务传输到第一台交换机上的帧中继接口，这台交换机实际上就是ATM交换机。运营商将这些帧分割成ATM信元，并通过网络将它们传送到出口ATM交换机，在那里将信元重新组装成帧，之后传送给客户。当然，网络运营商不可能实现ATM交换机所赋予的所有特点，这是因为UNI不支持。然而，如果制定出来新的规范使帧中继的UNI能够支持附加业务，那么运营商只需要更换端口卡就可以了。他们的ATM交换机会准备好在网络中传送这些新的特征。

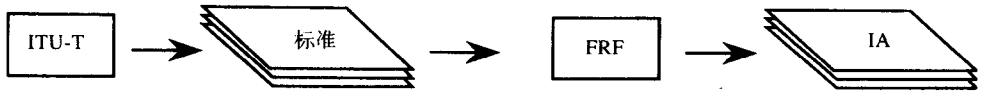
实际上，帧中继是在ATM上运行的，但ATM却从未在帧中继上运行。以ATM作为骨干网，网络的可靠性会得到增强。运营商正在只使用一种网络即ATM网来承载所有不同类型的业务。现在，ATM网不仅承载帧中继业务，而且还承载话音、视频、IP以及其他业务，这就称为融合（convergence，或称为会聚）。只使用一个普遍存在的网络，可以降低运营商的运营成本，这样价格也就有希望降下来了。用ATM网代替帧中继作为骨干网的另一个优势在于交换机之间的中继线可以升级到OC-3水平的传输或者更高速率。直到最近，帧中继交换机才能够处理T1/E1速率的业务，现在采用高速ATM骨干网可以很容易地为帧中继服务提供DS-3接口。

承载帧中继的ATM骨干网的另一个好处是ATM交换机之间的接口被明确定义，并且易于理解。而帧中继交换机却不是这样。因此，不能将不同厂商生产的不同型号的帧中继交换机混在一起使用。这是因为它们之间并没有统一的标准；但是，运营商可以根据当时哪个厂商供货情况最好，来购置不同厂商生产的ATM交换机。ATM交换机厂商之间的竞争不仅使产品价格降低了，同时还有利于提高交换机的质量。

21.2.4 标准化组织对帧中继的认识

如图21-6所示，帧中继事实上源于ITU-T（International Telecommunications Union-Telecommunication standardization sector，国际电信联盟-电信标准分部）。这个组织制定标准并不断地增强它们的性能。大多数帧中继标准的命名都是以字母Q开头的，比如Q.933和Q.922。

这些标准由FRF（Frame Relay Forum，帧中继论坛）审阅，FRF由100多个成员组成，这些成员是运营商和设备制造商。FRF的主要工作基本上是如何实现这些标准，以使服务尽快成为现实。它也要审阅这些实现规程，以保证不同供应商的设备的互操作性，这些规程叫做IA（Implementation Agreements，实现协议）。



FRF: 帧中继论坛
IA: 实现协议
ITU-T: 国际电信联盟-电信标准部

图21-6 ITU-T与FRF的关系

21.3 帧格式

图21-7给出了帧中继的帧格式。与SDLC（和HDLC）一样，帧中继帧以一个标志开始并结束，帧内包含一个FCS字段，交换机用FCS来无警告便丢弃任何已被破坏的帧。在第二、三字节的字段与ISDN中所用字段类似。

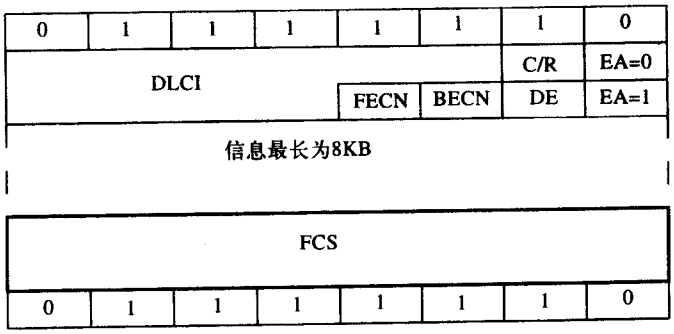


图21-7 使用常用的2字节头的帧中继的帧格式

DLCI类似于X.25第三层所用的LCI，它允许进行帧交换。它仅有10比特，总共提供1024个通路。还有其他版本的帧中继帧允许有更多的DLCI，但这些版本均未被使用。C/R（Command and Response，命令与响应）比特由终端系统设置，经网络传输，只能被接收端的应用程序所读取，网络忽视该位的存在。这个比特主要被封装在一帧内的SNA分组用来指示SNA是一条命令，还是一个响应。

前面我们说过由于帧中继不受 X.25的窗口大小的限制，因此它允许更快的帧中继通过网络。但是去除窗口机制也使网络失去了流量控制的能力。也就是说，在发生网络拥塞时，帧中继交换机不能够发信号通知发送方减速或放缓传输速率。这是在帧中继网络中存在的一个主要问题。现在我们考虑一下拥塞控制的方法。

一种方法是使用FECN（Forward Explicit Congestion Notification，前向显式拥塞指示）和BECN（Backward Explicit Congestion Notification，后向显式拥塞指示）位。例如，如果网络发生拥塞，部分原因是由于用户B向用户A发送了大量数据，这时被阻塞的网络交换机就会在发往B的帧中设置BECN位，希望用户B减缓发送速度。同样，交换机也会在发往A的帧中设置FECN位，希望用户A减少请求B发送的数据量。值得注意的是，并不强制要求终端设备对这两个比特做出响应。如果网络不能处理业务负荷，它就会开始丢弃一些帧。

假使端点处的路由器确实想要帮助公共帧中继网络使之不发生拥塞，它也无法通知LAN应用程序立即停止发送数据。而且当由于拥塞而发生帧丢失时，LAN一般会重发帧，这更加重了问题的严重程度。

另一方面，当网络丢弃数据时，智能终端设备可能认为是由于拥塞而发生数据丢失，于是立即停止数据发送，这称为**隐式拥塞检测**（implicit congestion detection），因为终端节点没有直接被告知问题的发生。

这种情况下存在的问题是，如果没有从A发往B的帧，那么就没有办法通知发送方获取BECN位，甚至即使BECN位的确到达了发送端的应用程序，但当它到达时，拥塞也可能已经不存在了。类似地，A的应用程序不能阻止B发送更多的帧，同样，当该信息到达B时，拥塞也可能已经不存在了。因此，实际上这两个比特仅适于用来统计月度报告，从中你可以了解网络在什么时候、什么地方发生了拥塞。如果这些比特被设置了相当多的次数，那么提高虚电路的CIR或许是更明智的做法。

如果终端节点传送那些它并不介意丢失的帧，比如路由更新信息帧，那么它就会将这些帧的DE（Discard Eligibility，可合法丢弃帧）位设置为1。如果可能的话，这些DE比特被设置为1的帧将被正常发送；否则，它们会成为首先被丢弃的帧。最初的想法是用这一位来设置优先级。如果用户以高于CIR的速率传输业务，那么用户意识到某些帧可能被网络丢弃时，他就会将低优先级帧的DE位设置为1。但是，如果PVC通道上没有发生拥塞，那么DE位为0或1的帧都会通过网络。另一方面，如果发生严重拥塞，则所有的帧都可能被丢弃，而不管它们的DE位的设置如何。只有在适度拥塞的情况下，DE位的设置才能在决定哪些帧被传送出去，哪些帧不能传送时起作用。从理论上讲，这正是设置DE位的目的。然而，我们将在21.4.3节和21.4.4节看到，现在的运营商都不再处理DE位了，所以这一位也就不再发挥任何有益的作用。

21.4 拥塞控制

21.4.1 再谈CIR

我们已经提到过运营商如何通过为“固定”在网络中的每个PVC定义一个CIR（Committed Information Rate，承诺的信息速率），来为用户分配流量的。用户期望在一条PVC上传送的流量由CIR限定。运营商将尽最大努力以CIR速率传送流量；用户以高于这一速率传送流量时，称之为突发。如果存在突发的容量，那么它是允许的，并且流量将会成功地通过网络。否则，这些帧就可能丢失，从而为其他以不超过CIR速率发送流量的用户留出所需的容量。用户能够突发的最大速率称为最大协商速率（Maximum Negotiated Rate）。所有超过此速率发送的帧都将被丢弃。这个速率通常等于接入线的速率，但是它也可以低于接入线的速率。

下面看一下如图21-8所示的一个特定PVC中的业务流。水平轴坐标表示时间单位，通常是以1s为间隔；垂直坐标轴表示速率。客户与运营商已协定好的CIR为32kbps，但允许突发业务速率达到48kbps。接入线的速率为64kbps，因此，客户可以以该速率发送流量，但是会丢失帧。

例如，在时刻1，用户以他的CIR速率32kbps传输业务，到时刻2，他还没有提高其发送速率，因此他的所有帧都被成功地传送。但在时刻3、4之间，情况就不同了，在这段时间内，用户发送业务的速率超过了他的CIR，运营商尽力传输这些帧，但是并不承诺以高于这一速率发送这些帧。在时刻5、6点之间，所有的帧都努力以48kbps的速率发送，但是在这段时间结束时到达网络的帧以及超过这一极限速率的帧都会被丢弃。

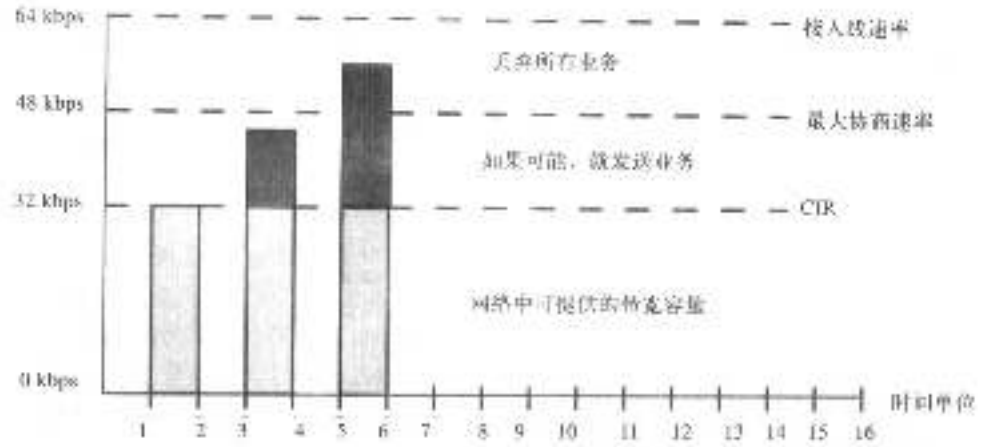


图21-8 CIR表示运营商承诺提供给一条PVC的传输速率。突发速率允许超过CIR但要低于最大速率

21.4.2 预约水平

在一条通过交换机端口的接入线上，可以设置多个PVC，参见图21-9。PVC的CIR的总和与最大端口速率的比值叫做**预约水平**（subscription level）。如果CIR的总和超过端口速率，那么预约水平就大于100%；反之，预约水平就低于100%。一个用户的预约水平可以超过100%，这意味着该用户并未在同一时间通过一个端口以其所有的PVC的CIR速率发送信息，而是各个PVC依次轮流传输业务。所有PVC都以它们的峰值速率传输业务的情况非常少见。在这种十分偶然的情况下，我们会丢失一些帧；但是这不会经常发生，所以我们可以忍受。如果由于这个原因，用户不断地丢失帧，那么就需要重新考虑预约水平，并降低它们的值。

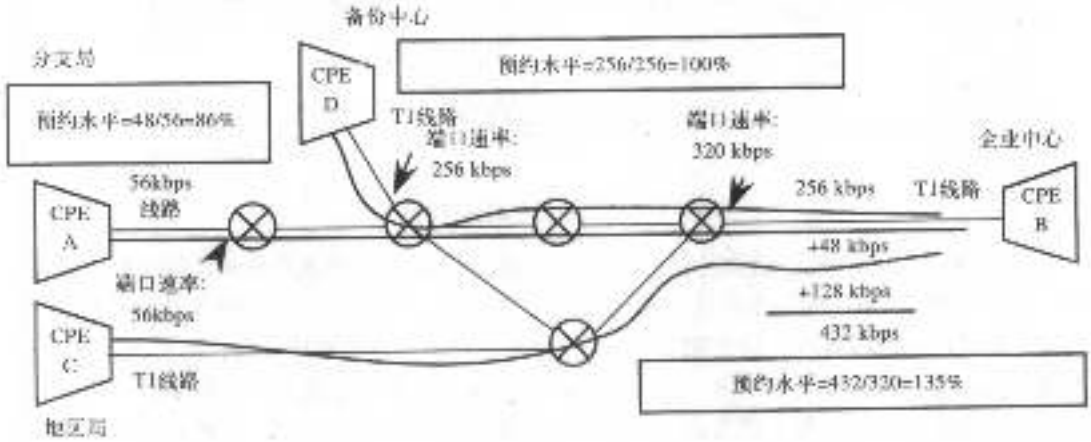


图21-9 预约水平是一个端口提供的PVC的CIR总和与端口速率的比值

下面举个例子进行说明，图21-9给出了四个地点：一个企业数据中心、一个备份数据中心、一个地区局和一个分支局。为了简化起见，图中只画了三个PVC，这三个PVC均包括企业数据中心。从这里到达其他三个地点的PVC的CIR分别是256kbps、48kbps和128kbps，于是CIR总和为432kbps。如果到达最近交换机的端口速率是320kbps，那么预约水平就是135%。

类似地，图中还计算出其他两个地点的预约水平。设计这样一个网络，需要一定的时间和规划，而且必须知道在每一个站点运行什么样的应用程序以及数据如何通过网络的统计数据。这只能靠经验获得，但是对于帧中继业务而言，很容易进行改动。只要这些改动包括在最初的合同中就没有问题。

21.4.3 开环流量控制

Sprint公司是首批提供帧中继服务的运营商之一，时间大约在20世纪90年代早期。当时还没有专为帧中继设计的交换机，因此Sprint公司在制造出帧中继交换机之前只能使用传统的分组交换机。这些分组交换机没有CIR的概念，所以Sprint决定提供CIR为0的服务。由于这个原因，因此所有帧都有可能被丢弃，所有帧的DE比特均设置为1，这就使得DE比特变得毫无意义。事实上网络中所有帧的传输率都高于99%。现在所有的运营商都不考虑DE比特的值。网络中所采用的拥塞控制方法称为开环流量控制。

图21-10是网络如何尽力传输所有帧的原理示意图。图中不仅给出了PVC通道上的交换机，而且也给出了缓冲器的状态。注意到A正在向B传输大量的业务，接近B的缓冲器逐渐被填充满。这些交换机正在向B传送业务，但速率低于从A获取数据的速率。当向B传送业务的交换机达到它们处理能力的70%时，它们就给邻近A的交换机反向发送一个特殊专用信号，要求它们放慢发送速度，这称为反压力信号。

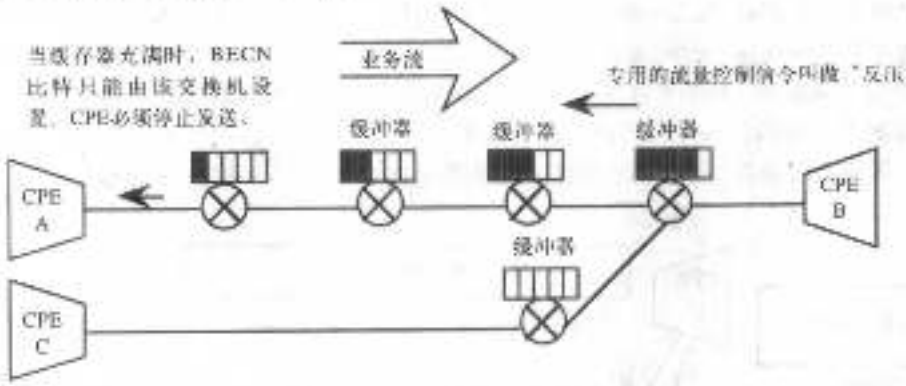


图21-10　网络的开环流量控制管理

当A方向上的交换机开始接近它们的处理上限时，它们就会依次告知前面的交换机减慢速率。最后，当与A相连的交换机达到处理能力的70%时，它就发出一个BECN比特，告知A完全停止发送，这是因为不仅与它直接相连的交换机正在接近它的处理上限，而且所有通往B的交换机也正接近它们的处理上限。当你想向网络中发送大量业务或者要占用更长一段时间进行突发业务时，这种流量控制方法是好的。它不需要降低速率。但是，当所有交换机达到它们的最大处理能力时，你就不得不完全停止业务发送。同时，注意到因为C没有突发业务，所以甚至在A占用了大量网络带宽的情况下，它仍然能够发送业务。

开环流量控制用0值CIR提供了一种高突发能力。因为更多用户会传送更多业务，所以网络费用在更多用户之间平摊，运营商可以提供更好的价格。这种类型的流量控制与IP处理业务的方法是非常一致的。IP向网络中发送数据分组后，让前面的路由器决定应该如何处理它们。因此，这种类型的流量控制更适合于处理IP网络。

21.4.4 闭环流量控制

运营商网络中所采用的另一种流量控制方法称为闭环流量控制，如图21-11所示。图中A正在向B发送业务，每当A向B发送业务时，距离A最近的交换机都要查询一下网络中是否还有所用PVC的容量。这是通过发送一个信用请求（Credit Request）信号来完成的。如果能够接收到一个返回的信用许可（Credit Granted）信号，那么这个交换机就可以继续发送帧。这里，网络正在预先做好准备，看是否有容量可用以便发送业务；如果有，它就会继续发送业务。

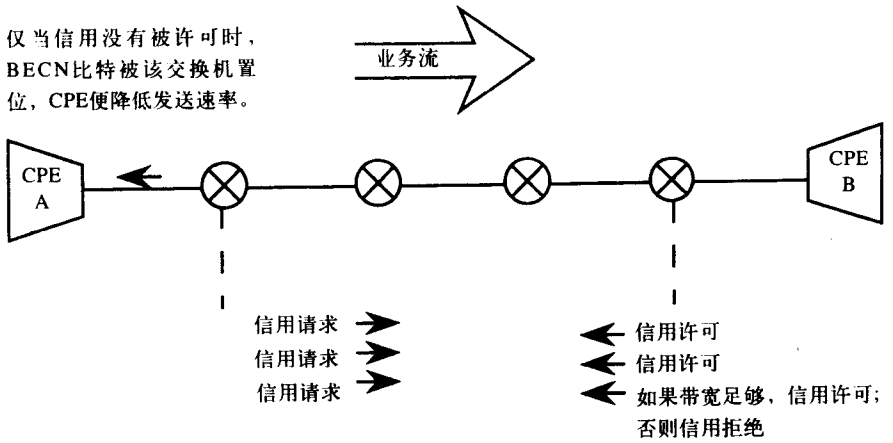


图21-11 网络的闭环流量控制管理

假设A在它的PVC上以高于CIR的速率突发业务，信用请求信号仍然被发送出去，但是这时，就有可能接收到信用拒绝（Credit Denied）信号。此时A处的交换机向后给A发送一个BECN。在这种情况下，CPE并不需要完全停止发送数据，而仅仅需要将发送速率降低到CIR的水平。所有的DE比特没有被置为1而是全部置为0，这个值仍然没有意义，并且完全被网络交换忽略。当A处的交换机接收到一个返回的信用许可信号时，这个交换机就将BECN比特设置为0，表明A交换机现在可以以高于CIR的速率突发业务。

对于闭环流量控制的网络，其用途更具一致性，延迟也更为统一。总是存在你可以传送业务的速率等级。它更适合于IBM的SNA网络。由于SNA网络中存在一个不间断的轮询机制，所以该网络对时间很敏感。例如，FEP可以循环轮询各控制器是否有业务要传送。SNA要求轮询时有一个应答，因为它最初被设计时，专用线路更普遍，并且得到立即响应也更平常。因为PVC通路上的缓冲器不会被填充满，所以这些网络的拥塞较少。因此，网络只能接受更少的用户及其发送更少的业务流量，价格也因此而相对更高一些。

21.5 多协议支持

21.5.1 帧中继上的SNA

传统SNA网由于使用固定的专用线路而很昂贵，采用帧中继网络可以为这样的网络节省50%的通信费用。然而，正如我们已经指出的，SNA网络是一个对时间非常敏感的网络，并且很难在帧中继网络上运行。

图21-12给出了SNA运行于帧中继上的一个粗略的解决方案。LAN用于通过以太网帧的形式传送被称为PIU（Path Information Unit，路径信息单元）的SNA分组。PIU被封装在以太网帧内。图中所示的路由器起到网桥的作用，主要是完成将以太网帧封装到帧中继的帧中。因此，这里进行了两级封装，都是在OSI的第二层进行的。

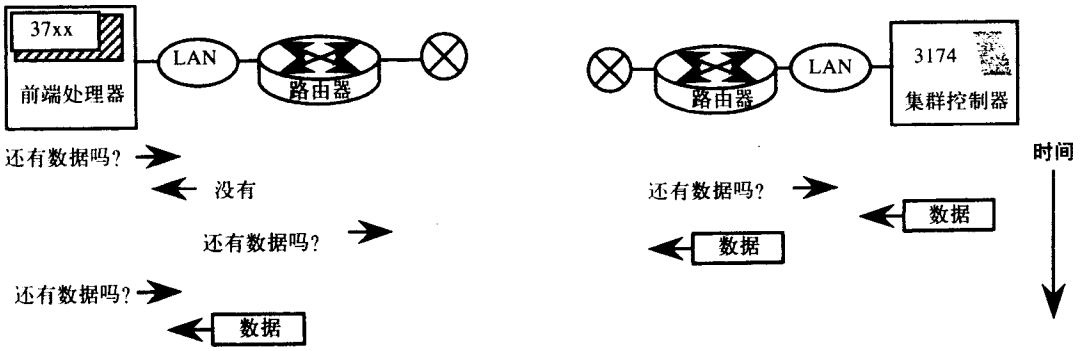


图21-12　电子欺骗由位于网络边界的路由器和网桥完成，从而支持帧中继上运行的SNA

当FEP（Front End Processor，前端处理器）在WAN中轮询到集群控制器时，第一个路由器对其做出响应。在集群控制器的终端，路由器轮询该控制器，仿佛认为它是FEP。远端路由器从该控制器收集数据，并传送给与FEP相连的路由器。当FEP的路由器被轮询时，它将数据转发给FEP，FEP就认为它有一个与集群控制器的直接连接，这称为**电子欺骗**（spoofing）。

对于小型网络而言，这种方式可以运行得很好，但当网络的规模扩大时，就会产生太多的开销和延迟。网络性能急剧下降，以至于终端用户根本不能接受这样的服务质量。

为了解决这些问题，已经提出了许多解决方案，但没有一个完全令人满意，这是由于SNA本身不能容忍延迟的特性造成的。图21-13给出了两种解决方案。一种是称为RFC 1490标准的方案，另一种是IBM设计的被称为DLSw（Data Link Switching，数据链路交换）的方案。这两种方案都要求用户所在地的路由器上必须安装恰当的软件。

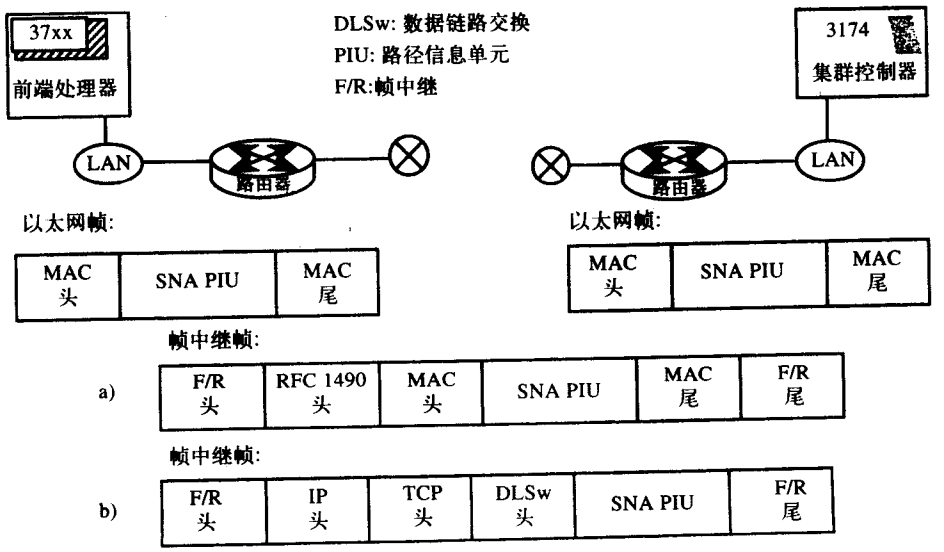


图21-13　a) 路由器添加并处理RFC 1490头，b) 或者它们能够添加并处理TCP/IP头和DLSw头

图21-13a表明RFC 1490解决方案将以太网帧原封不动地加上自己的头，一起封装到一个帧中继帧中，之后再将它通过网络发送出去。这种方法称为RFC 1490多协议封装。用于头的字节数很少，使得该方案非常简洁。许多路由器和帧中继交换机支持业务优先级，如果是这样的话，SNA帧都优于其他帧传送，这样就降低了超时次数。

图21-13b是DLSw解决方案的示意图。DLSw与传输TCP/IP（包括帧中继在内）的WAN一同运行。它不处理PIU中的任何SNA字段。TCP层帮助远端的SNA设备维护连接。DLSw在大型网络上工作状况并不是很好，它在头部使用的字节数超过了其他方案所需要的字节数。这两种方案没有一种容易实现，并且都需要大量的人为干预。

21.5.2 VoFR

在基于ATM的网络上运行帧中继业务，使得话音传输成为可能。为此，在帧中继接口需要制定更好的接口规范。这些规范称为FRF.11和FRF.13，均由帧中继论坛制定。VoFR（Voice over Frame Relay，帧中继上的话音业务）可以节省大量的资金，特别是话音穿越国际线路接口时更是如此。虽然运营商目前在数据网络上的投资大大超过在话音网络上的投资，但是话音通信仍然比数据通信贵得多。如果运营商决定对数据通信的收费高于话音通信，那么在数据业务上运营话音业务是否划算就值得怀疑了。但是，今天的数据网络相当便宜，因此，VoFR是一个值得关注的解决方案。

为了实现VoFR，必须对PVC进行精心设计，即应该购买更高的CIR，并具有比正常用来传输数据的端口速率更高的端口速率。这是因为话音分组不能等待，而且话音分组通常比数据分组小。当话音分组阻塞在一个正被处理的长数据分组之后时，我们称之为**队首阻塞**（head-of-the-line blocking）。为了补偿由此带来的问题，数据分组被分割成更小的块，允许话音分组插入到它们之间。将数据分割为更小的块使得接口看起来更像一个ATM接口。

图21-14的右侧给出了一个与PBX相连接的VFRAD（Voice Frame Relay Access Device，话音帧中继接入设备）。VFRAD从PBX接收PCM格式的话音，对其进行压缩并分割成分组，之后再将其封装在一个帧中。在网络中传输更小的分组节省的时间超过压缩它们所用的时间。通常话音帧的长度为40~80字节。

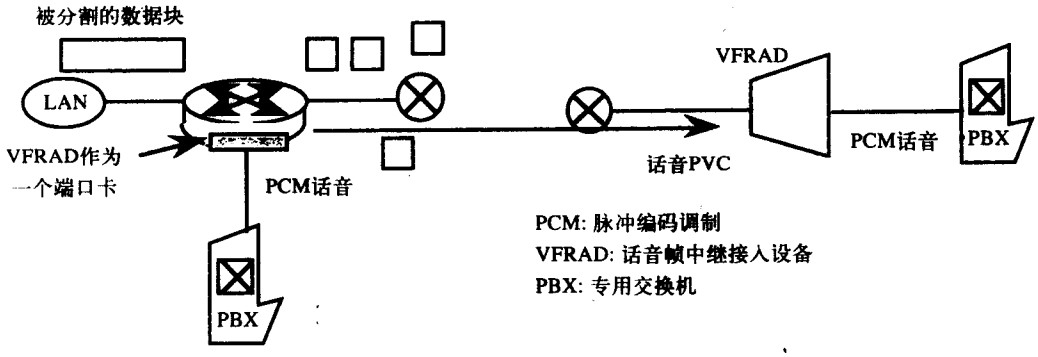


图21-14 VoFR（帧中继上的话音业务）的配置

有时不能从网络中接收到传给VFRAD的话音分组。当缓冲器中没有帧回传给会话的收听方时，我们称这些缓冲器处于**饥饿**（starving）状态。为了减少缓冲器的饥饿，将抖动缓冲器包含在VFRAD中，从而平滑进入的话音。

图的左侧是一个与帧中继网络相连接的路由器，它负责管理进入右侧的PBX的话音帧和

传输到图中没有显示出的其他地方的数据帧。路由器有两个本地接口，一个是服务于数据的LAN卡，另一个是置于另一端口卡中供PBX使用的VFRAD。路由器会对可能引起队首阻塞的数据块进行分割。两地之间的PVC允许话音从PBX进入网络中进行传输。

与SNA一样，FRAD应该使话音业务具有优先级。运营商也开始在他们的网络中支持为SNA和话音业务设计的优先级。由于这些特征的存在，为话音进行PVC配置是比较难的。我们必须保证分组的延迟在可接受的范围内，延迟的变化也在可接受的范围内，同时PVC的速率也必须保证超过平均所需的速率。由于分组打包、拆包和在网络中帧传输所造成的延迟必须予以考虑。

习题

21.1节

1. 从图21-15找出分组交换网络的交换表中输入了多少条PVC；之后指出各PVC的起始点和目的地，以及它们所经过的交换机的数目。

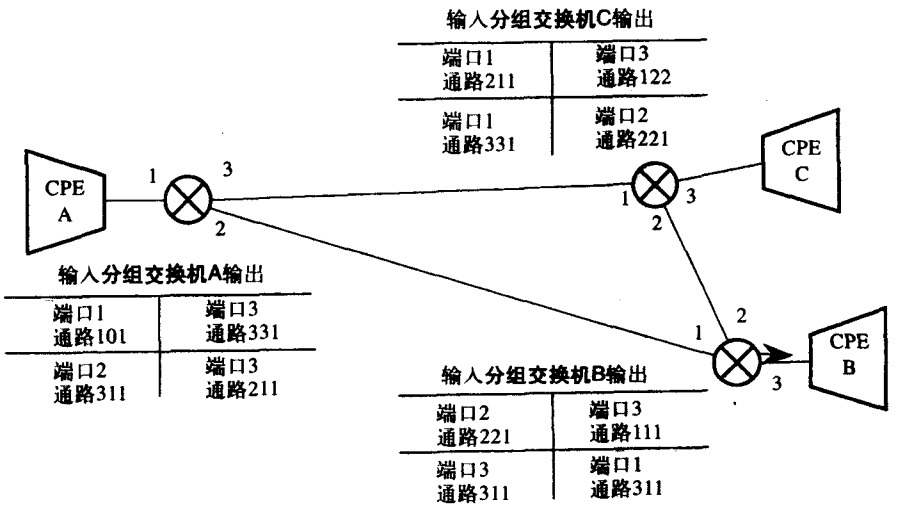


图21-15　分组交换机(习题1)

2. 在帧中继网络中，CPE可以代表哪些设备？
3. 在帧中继网络中，什么是通路号？在X.25网络以及ATM网络中呢？
4. 比缩写PVC实际代表的内容更好的描述是什么？为什么？
5. 比较SVC和PVC。为什么SVC的讨论留在下一章进行？
6. 用自己的话谈谈交换网络与专用线路网络相比的优点和缺点。

21.2 节

7. 比较帧中继协议和OSI模型的分层。
8. 哪些协议可以被封装在帧中继的帧信息字段内？如何与可以用ATM信元封装的协议相比较？
9. 按照标准观点，在帧中继中何谓一帧？
10. 在帧中继中定义的两个接口是什么？哪一个使用得更少？为什么？

11. 在帧中继服务中，谁负责纠错？
12. 运营商保证可以从用户那里接收的业务的速率称为什么？当用户以超过该速率发送业务时，又称为什么？
13. 使用自动ISDN备用电路的危险是什么？
14. 运营商出售的是公共帧中继网络还是帧中继服务？两者有什么不同？
15. 哪一个术语描述了运营商正在使用一种类型的骨干网络传输话音、数据和视频等业务的事实？
16. 在ATM网络上承载帧中继帧比在帧中继网络上承载帧中继帧有什么优势。
17. 就帧中继标准而言，描述一下ITU-T与帧中继论坛的区别。

21.3节

18. C/R比特的用途是什么？
19. DE比特的设计初衷是什么？
20. 在送往发送端的帧中设置FECN比特还是在送往接收端的帧中设置FECN比特？
21. 当携带BECN比特或者FECN比特的帧到达时，用户或CPE将如何处理？
22. 帧中继的帧头包含多少个字节？
23. DLCI的可能值有多少个？
24. 一般而言，各PVC必须有自己的DLCI吗？

21.4节

25. 最大允许的突发速率由哪些参数限定？
26. 在CIR速率范围内传输的帧都能到达它们的目的地吗？
27. 在图21-9中，假设从C到D增加了另一条PVC，C处交换机的端口速率是320kbps。重新计算连接到C和D的两台交换机的预约水平。
28. 希望预约水平低于100%的原因有哪些？而要求它高于100%的原因又是什么？
29. 比较一下开环流量控制与闭环流量控制的异同点。
30. 在哪种类型的流量控制机制中，DE比特发挥重要作用？

21.5节

31. 为什么说在帧中继服务上运行IBM的SNA是一个比较棘手的任务？
32. 电子欺骗是什么意思？
33. 哪一种运行于帧中继服务上的SNA解决方案传输整个LAN帧？哪一种解决方案首先将其封装在一个IP帧中？
34. 请列出为VoFR提供PVC时必须注意的几个问题。
35. 准备将话音通过帧中继服务传输的设备叫什么？

第22章 ATM

22.1 ATM基础

22.1.1 引言

学习本章要求理解我们在前面介绍的许多内容。在2.5节中，我们已经知道分组交换网络是以虚电路为基础的，包括PVC和SVC。在5.3.7节介绍了ATM（Asynchronous Transfer Mode，异步传输模式）并讨论了它在长度方面的优势。在第21章再次讨论了虚电路并解释了如何被应用于帧中继网络，也提到过为什么ATM为帧中继网络提供了更好的骨干网。现在，我们已对虚电路和ATM网络有了一定的了解，但未必清楚ATM是如何实现的。这正是本章要讨论的问题。

ATM背后的总体思想很简单：建立一种网络基本结构，来传输各种类型的信息。采用这样一个网络可以减少运营成本。以前，运营商用一套电路交换机和传输设备传送话音流量，这就是运营商的PSTN部分。为了传送数据，设有与话音传输网络完全不同的独立网络。如果考虑传送视频和多媒体信号，那么，这两种类型的网络都是不够的。但是为了这些应用再建立和运营一个新的网络又会浪费资源。

现在，运营商正在认真考虑创建一种基于ATM的网络，所有话音、数据、视频和多媒体以及其他信息都可以通过ATM网络来传输。AT&T声明已经安装了一台其最新的4ESS交换机，并计划转向完全基于ATM交换机和传输设备的网络。帧中继、IP以及将来发明的所有新协议都将在此网络上传输。于是，所节约的成本将会给用户带来更多的实惠。

当然，对各种信息的需求是不同的。话音信号增量小但是需要同步传送，即以恒定速率传输。速率有波动的话音传输是不可取的。数据则以较大信息块出现，但通常不需要同步；另外，与话音信号相比，它对错误更敏感。数据也会突然到来，传送一个很大的文件之后数据率下降，或降至零。视频和多媒体传输需要很大带宽并且要求同步。

即使是话音和视频信号，也可以用两种不同的方式传输。一种是CBR（Constant Bit Rate，恒定比特率），即不论信道传送信号与否都分配恒定的带宽，比如64kbps。这种方法对应于TDM（Time Division Multiplexing，时分复用），T1电路就是用这种方式建立的。一种更有效的传输话音和视频的方法是先把信号打包，这样，当一条信道上没有分组包要传输时，可以把其他信道上的分组包插入此信道传输。话音和视频信号的打包与压缩需要一种称为VBR（Variable Bit Rate，可变比特率）的服务。

我们正在寻求一种可以传送所有这些类型信息的网络基础设施，这不会是一个容易的过程。然而，在这样的网络中投入更多的才智和技术会使终端用户非常容易地传送所需要传送的信息。因此，ATM使用一套复杂的协议。

22.1.2 信元

为了满足这些要求，ATM把所有信息PDU（Protocol Data Unit，协议数据单元）都分解成为信元而非帧。信元是定长的，而帧的长度是变化的，而且信元比帧小。变长的帧的延迟

是不确定的。一个长的数据帧可能延误需要立即传送的话音分组包，这称为**线路头阻塞**（head-of-the-line blocking）。信元长度较小，如果话音分组到达网络，它几乎可以立即接受服务，使阻塞达到最小。这使得ATM可以采用统计时分复用。

长度小且定长的信元不仅适于传送话音和视频，也适于硬件交换。而帧处理过程基本是由软件操作的。由于信元是定长的，因而用硬件芯片就很容易处理它们。各信元的首和尾很容易标识，这与帧的情况不同。帧以标志字段标识各域的首和尾，这些字段，即SYN字段，在信元中是不需要的。硬件交换比软件交换速度快且成本低。

所有的ATM交换都是直接切入式（cut-through）交换，具体地说，这些交换不必等整个信元到达交换结构中，而是一旦读入信元的首部，数据的其他部分还没有到达时就被引导到交换的输出端口。这种交换比帧所用的存储转发式交换要快。在帧传输中，整帧读入到缓存中，校验是否有错，然后再交换给输出端口，如图22-1所示。



图22-1 a) 存储转发式交换机必须读进整个帧才能将其传送到输出端口；b) 直接切入式交换机一读到信元的头并进行处理后就能将该信元转发出去

运用统计时分复用，长度小且恒定的的信元，可以使得ATM完成开始设置的工作，即网络可以在任意距离上（不管是局域的还是广域的）传送任何类型的信息。此外，还需要定义一组统称为QoS（Quality of Service，服务质量）的重要参数，规定延迟级别、延迟变化（或抖动量）、误码率及ATM传输服务上所要求的其他指标。

22.1.3 ATM的体系结构（分层）

既然我们已经明确了对ATM网络的需求，就需要制定实现这些需求的方案了。首先设计它的体系结构，如图22-2所示。总的来说，ATM分为三层，物理层对应OSI参考模型的物理层。在此层之上为ATM的信元层和AAL层（ATM Adaption Layer，ATM适配层），这两层对应于OSI的第二层。由于ATM的信元是用硬件进行交换的，因此这层中的一部分作为属于OSI的第一层在图中给出。AAL的功能是取得所有类型信息并加载到信元，如图所示。ATM信元层的功能是交换信元并把它们发送到适当的目的地。

如果要将来自局域网的帧通过ATM信元层传输，则AAL与局域网的LLC（Logical Link Control，逻辑链路控制）层相连接。LLC是IEEE局域网标准的数据链路层的上半层，这个标准将在第23章讨论。如果要进行IP通信，则AAL与网络层相连接。ATM要求提供连接到目的地的信令，该信令由网络层功能支持，将在以后讨论。

在ATM模型各层之间进行传递的单元称为SDU（Service Data Unit，业务数据单元），而不是PDU（Protocol Data Unit，协议数据单元）。ATM层处理由信元头和净荷组成的ATM信元。发送时，AAL将净荷转发给ATM层；接收时，AAL从ATM层接收净荷。物理层负责提供HEC（Header Error Correction，信元头错误校正）。

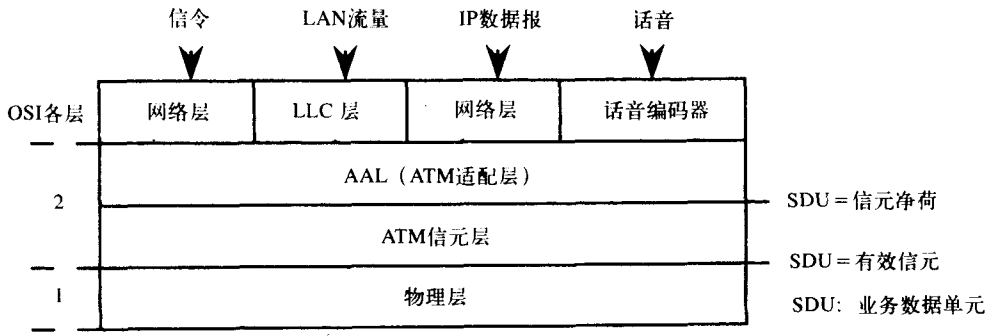


图22-2　ATM模型可看作OSI模型第一层和第二层的一部分，但是，根据网络传输业务的不同，ATM可以与属于OSI不同层的应用相接口。层与层之间的传输单元称为SDU（Service Data Unit，业务数据单元）

由于AAL接收的信息要加载到信元，因此它的业务只需要在网络端点进行。在接收端，信元重新组合成用户应用的PDU（Protocol Data Unit，协议数据单元），这由图22-3可见。注意，在网络交换中必须处理的是物理层和ATM层。

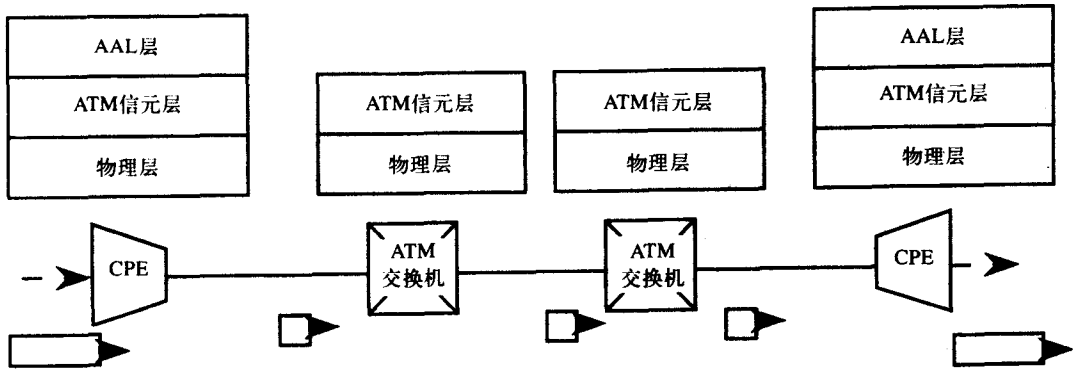


图22-3　AAL（ATM Adaption Layer，ATM适配层）是一种端到端协议,不能在ATM交换机中实现。它将应用传输单元划分成通过交换机转发的信元。在接收端AAL将信元重新组合到一起

这个三层的ATM模型进一步分成一些子层，如图22-4所示。物理层分成传输会聚

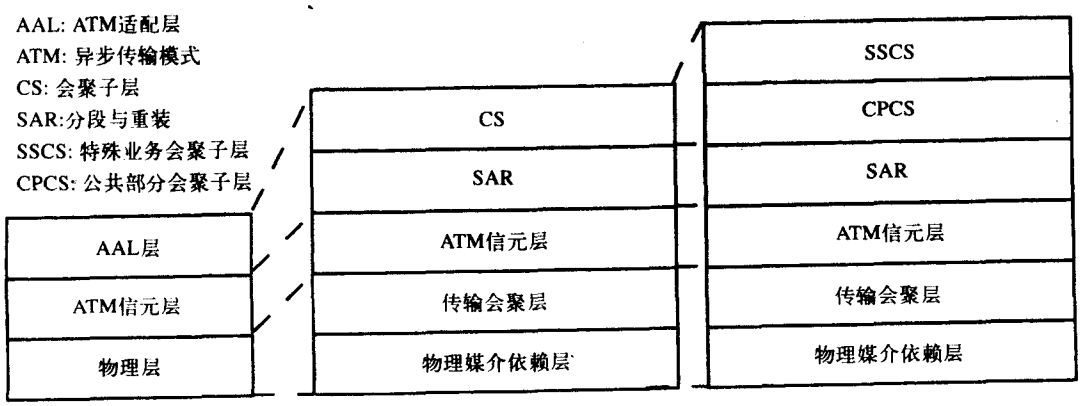


图22-4　ATM模型的三层可以划分为总共五个子层。CS子层还可以进一步划分

(Transmission Convergence) 子层和物理媒介 (Physical Media Dependent) 子层，物理媒介子层大部分是通过SONET或其他诸如DS3的物理传输系统来实现的。它提供同步和线路编码。传输会聚子层则负责信元边界标记、HEC、分帧、多路复用及其他物理功能。当发送信元时，该子层添加HEC字段；当接收信元时，它检验是否有错，放弃错误的信元而不向ATM层转发。这个子层使ATM信元适应于所采用的任何物理媒介，并使ATM能够灵活应用于任何实际媒介。

AAL层分成CS (Convergence Sublayer，会聚子层) 和SAR (Segmentation And Reassembly，分段与重装) 两个子层。在发送时，SAR子层将应用数据流分成信元；在接收时，它又将信元重新组合成适于应用的数据流。CS子层指明应用的需求，并在传输单元被SAR子层分解之前对其提供保护。CS子层又分成SSCS (Service Specific Convergence Sublayer，特殊业务会聚子层) 和CPCS (Common Port Convergence Sublayer，公共部分会聚子层)。关于这些子层的细节问题将在本章的后面讨论。

22.2 ATM信元层

22.2.1 信元的路由选择

在ATM网络的核心，信元是用虚电路的方式传输的。然而，虚电路不单是由电路通过的各链路上的虚通路 (virtual channel) 定义的，也用虚通道 (virtual path) 方式定义。因此，一个ATM信元头有两个字段用于标识通过哪条电路进行传输，也就是信元的路由是由VPI (Virtual Path Identifier，虚通道标识符) 和VCI (Virtual Channel Identifier，虚通路标识符) 共同决定的。正如在其他协议中看到的，ATM不但支持PVC (Permanent Virtual Circuit，永久虚电路)，而且支持SVC (Switched Virtual Circuit，交换虚电路)。与以前一样，PVC由手动进入，SVC是由信令协议建立、维护和撤销的。

为了说明在ATM中是如何处理虚电路的，考虑图22-5。用户A建立了从交换机1到交换机3的一条虚通道，由一组VPI标识。在此例中标识为PVC或SVC都可以。如果是PVC，该连接就是永久有效的；否则，该连接不久就会被断开。这个虚通道在三个交换机的查找表中定义，定义如下：

交换机1把所有来自用户A的VPI为100的信元传送至VPI为120的交换机2。

交换机2把所有来自交换机1的VPI为120的信元传送至VPI为110的交换机3。

交换机3把所有来自交换机2的VPI为110的信元传送至VPI为130的用户D。

用户A和用户D关心VCI之间的区别，但交换机并不关心这一点。如果有许多应用程序在用户A和用户D之间运行，那么在这两个位置之间使用虚通道会比较方便。用户设备整理出哪些信元属于哪个应用程序，而ATM网络只需要处理VPI。这就进一步加快了交换机的处理速度。注意，通过虚通道时，VCI保持不变。在图22-5中，由阴影信元表示的虚通道包含相同的VCI，即VCI为2000和2010。

上面介绍的就是**虚通道交换** (virtual path switching)。在虚通道交换中，VPI可以随着交换机的不同而变化，但VCI保持不变。VCI为2000和2010通过从用户A到用户D之间同样的虚通道，这就好像乘客在机场换乘另一个同类型的飞机并坐在与原来相同的座位上一样。

虚通道交换可以人工进入以建立永久的通道，这就叫做PVP (Permanent Virtual Path，永久虚通道)。另一方面，SVP (Switched Virtual Path，交换虚通道) 是通过信令建立的。与SVP相比，运营商更愿意销售PVP，因为SVP需要更复杂的信令机制，它们很有可能运行不善。这种情况在交换机是由不同的制造商生产而不能100%彼此兼容的时候尤为突出。

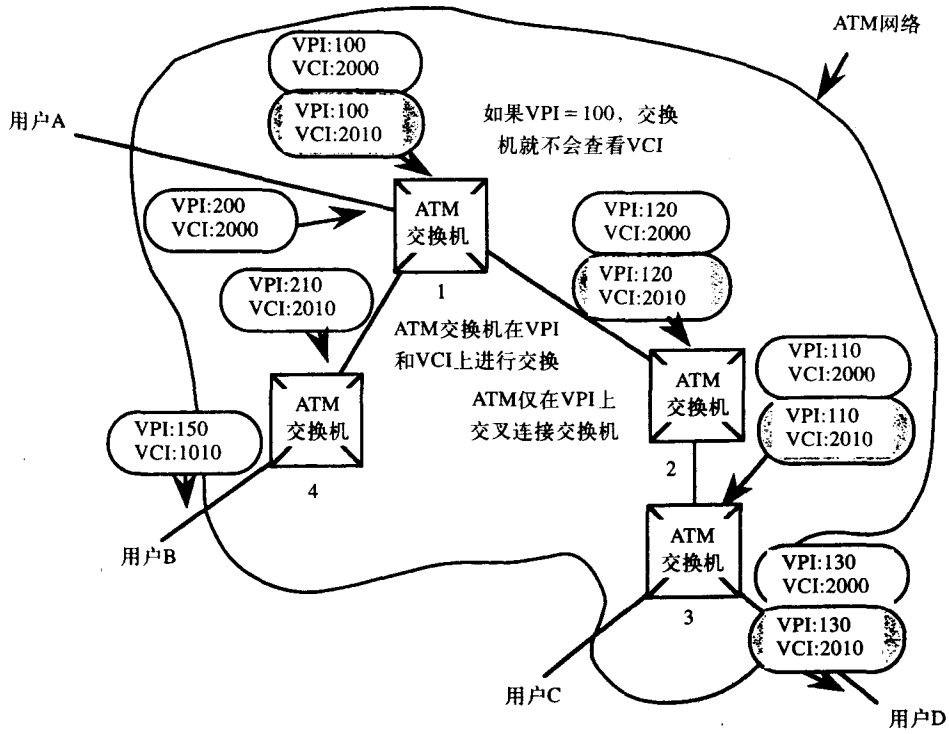


图22-5　所有带阴影的信元属于同一个由交换机1、2和3定义的虚通路.

在两站点之间已经准备好PVP的用户可以通过该PVP在这两个站点之间建立SVC（交换虚电路）。这些SVC是从用户所在地挑选出来的，称之为**软PVC**（soft PVC）或**交换PVC**（switched PVC）。所谓软PVC是指端点根据需要可以通过它建立和断开SVC的PVC。它的实现是有专利权的，因此PVC两端的设备必须出自相同的制造商。然而，在ATM交换中并不需要信令，这只是在终端所需要的功能。

对于只需要一条通路而不是一组通路的用户，ATM交换机也必须处理VCI。在图22-5中，虚通路由从用户A到用户B的无阴影信元表示，称之为**虚通路交换**（virtual channel switching）。虚通路交换是指信元的交换是依照VPI和VCI的值进行的。这里，与软PVC不同，VCI没有绑定在VPI中。

能够只依靠VPI进行交换的交换机称为ATM DCS（Digital Cross-connection System，数字交叉连接系统），而同时依靠VPI和VCI进行交换的交换机称为ATM交换机。

22.2.2　网络接口

与帧中继一样，ATM定义了用户与第一个ATM交换机之间的接口，称为UNI（User-to-Network Interface，用户-网络接口）。如果ATM交换机是专用的，也就是完全被用户拥有和操作，那么这个接口就称为专用UNI。用户与公共ATM交换机之间的接口称为公共UNI，如图22-6所示。

与帧中继不同的是，ATM还定义了各个交换机之间的接口，称为NNI（Network Node Interface，网络节点接口）。PNNI（Private Network to Network Interface，专用网络－网络接口）是NNI的一种特殊实现。由于定义了NNI，因此运营商就可以购买不同厂商的交换机，而不必只与一家厂商合作，这使得他们可以得到最佳的价格和服务。不同的运营商之间的ATM网络接口称为B-ICI（Broadband Inter-Carrier Interface，宽带运营商间的接口）。

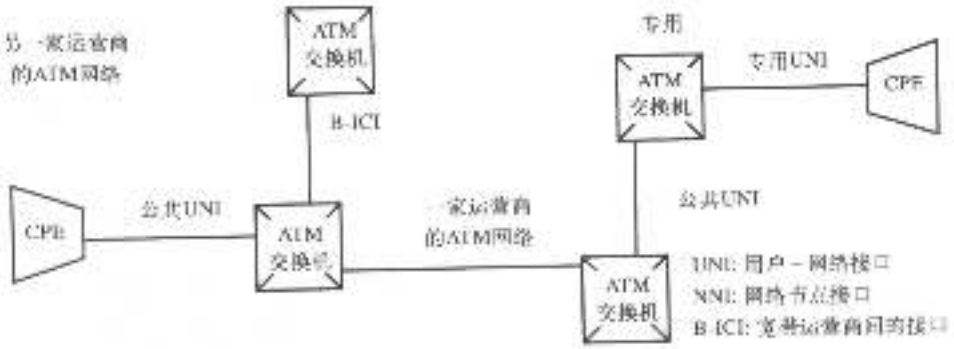


图22-6 ATM交换机接口

22.2.3 信元头

我们已经介绍的ATM信元都是长度固定的，为53个字节，信元头占用5字节，AAL提供的净荷部分占48个字节（见图22-7）。

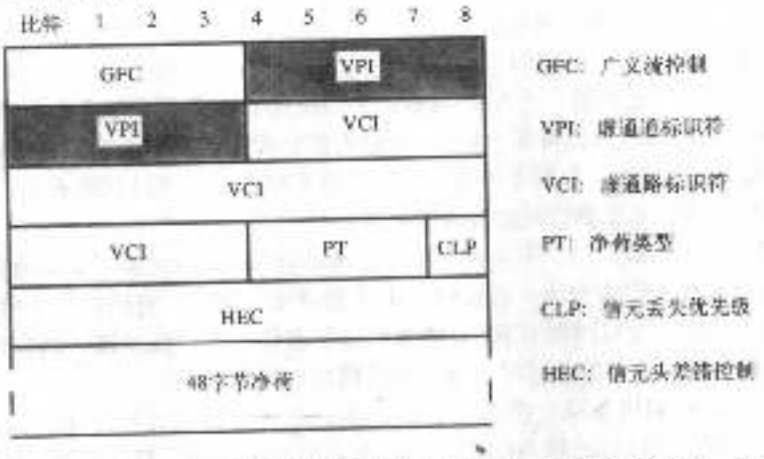


图22-7 在ATM信元中，信元头占用5字节，净荷为48字节，信元共为53字节。NNI中并不用GFC，但GFC却成为了VPI字段的一部分

我们已经描述了VPI和VCI，它们的长度分别为8比特和16比特。这样，每条物理链路可以有256条虚通道，其中每一条虚通道包含65 535条虚通路。旁边的图给出了一些被保留下来用于提供特殊功能的VPI和VCI。当链路空闲时，链路连续发送一些未分配的信元。ILMI代表集成链路管理接口，并通过UNI提供管理信息，例如地址注册。呼叫信令将在后面讨论。

预留的主要VPI和VCI

描述:	VPI:	VCI:
未分配的信元	0	0
呼叫信令	Any	5
ILMI	0	16
PNNI	0	18

GFC字段：信元头中的第一个字段叫做GFC（Generic Flow Control，广义流量控制），该字段仅对UNI有意义。一旦信元通过NNI进入网络，这个字段就不再有用了。但是，这些比特可用来使VPI从8比特扩展到12比特。这个字段用于提供数据流量控制：或者在CPE（Customer Premises Equipment，用户端设备）以高于网络所能够处理的速度传输数据时，用户降低来自CPE的数据速率。但是，它目前还没有定义，而总是被设为全0。

PT字段：PT（Payload Type，净荷类型）字段标识信元的类型。这是一个3比特的字段，表

22-1给出了各比特的含义。如果第一个比特为0，则表明它是一个用户数据信元；如果为1，则为网络信息信元。第二个比特表示接收信元在网络中是否经历过拥塞，它也称为EFCI（Explicit Forward Congestion Indicator，显式转发拥塞指示）比特。与帧中继相同，CPE或其他边缘设备负责对拥塞做出反应。

表22-1　净荷类型指示

Bit1	Bit2	Bit3	描　述
0	0	0	用户数据，没有拥塞，SDU类型0
0	0	1	用户数据，没有拥塞，SDU类型1
0	1	0	用户数据，有拥塞，SDU类型0
0	1	1	用户数据，有拥塞，SDU类型1
1	0	0	分段 OAM F5 相关流量
1	0	1	端到端 OAM F5 相关流量
1	1	0	为将来预留（流量管理）
1	1	1	为将来预留

除了在AAL5的情况外，第三比特并没有明确定义。在AAL5中，如果信元不是一帧的最后一个信元，这一位就置为0；否则就置为1。我们将在后面介绍AAL5。

信元丢失优先级：CLP（Cell Loss Priority，信元丢失优先级）比特是由CPE或者入口交换机（从CPE接收到信元的第一个ATM交换机）设置的。如果CPE以高于网络允许的速度发送信元，ATM交换机则将该比特置为1，表示它为低优先级信元。即该位置0表示高优先级信元，置1表示低优先级信元。在拥塞的情况下，低优先级信元首先被网络丢弃。然而，发生严重拥塞时，即使是高优先级的信元也可能被丢弃。

HEC：ATM信头的最后一个字段称为HEC（Header Error Control，信头差错控制）。它提供了一种检查信头有效性的方法，确保信头中没有差错，同时，它还提供了确定信元边界的方法。它基本上是用一个8比特的CRC算法来检错。若信头中存在差错，则会被纠正或丢弃。信头中发生一比特或两比特的差错时，可以非常精确地得以纠正。

HEC还可以使ATM设备确定出各信元的开始。从一个特定比特开始，设备计数32比特（即4个字节），假设随后的8比特为HEC，并检查是否存在差错。若有差错，则假设该起始比特不是信元的开始，而后它转向该起始比特后面的一比特，重复前面的过程。最终会检查到HEC无错误，于是该设备就假定这时的起始比特为信元的开始。

换言之，就是从假定为信头的连续的比特开始计数5个字节。假定这个经过HEC检查的5个字节数据块是正确的信头，也就是信元的开始。

这种检错过程将重复至少两个以上的信元，以确定每个信元的起止。为了更精确地描述信元，可将净荷进行乱序，从数学角度上减少将HEC误判为净荷的一部分的可能性。

注意到信元没有像诸如SDLC和LAP/B等第二层协议那样给出序号，这是因为信元仅通过一条物理通道传输，因此必然会以传输时相同的顺序到达。ATM交换机比分组交换机快的另一个原因是分组交换机的第二层协议必须对所有数据进行检错，而ATM交换机仅检查前5个字节而不必检验后面的48个字节。

22.3　ATM适配层

22.3.1　应用服务分类

位于ATM层之上的是AAL（ATM Adaptation Layer，ATM适配层），见图22-2。该层不是链路到链

路（或节点到节点）的处理，但与ATM层不同的是它仅涉及端节点。ATM为不同类型的应用提供服务，可以是图像、视频等。顾名思义，AAL使不同种类的应用适应于ATM提供的单一种类的传输模式。AAL提供与X.25中的PAD（Packet Assembler/Disassembler，分组组装/拆分）相同的功能，但是更具灵活性。正是该层使得ATM能混合传送各种信息。因为AAL只在终端或CPE上执行，而非在ATM网络的交换机上执行，所以网络交换机仅需涉及信元的路由，而不需关心净荷所携带的数据类型。

为了解决在ATM上运行的与各种应用类型有关的不同问题，CS子层规定了这些应用的需求，并将这些需求划分为图22-8所示的A、B、C、D四类。A类应用需要面向连接的传输和CBR（Constant Bit Rate，恒定比特率）服务。延迟必须非常短，这使得该类适合于基于话音和视频的应用。

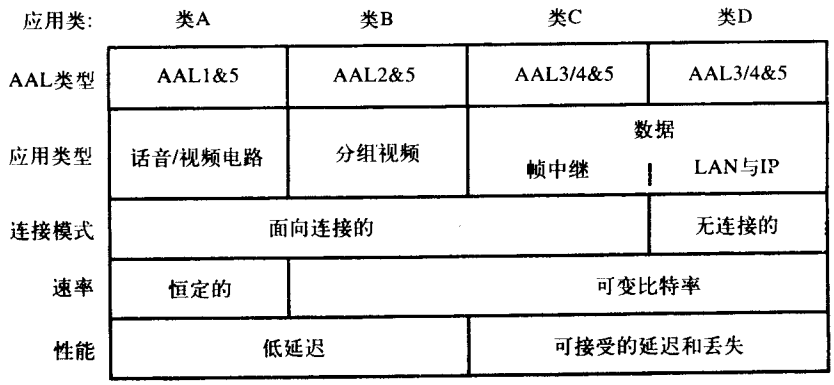


图22-8 ATM根据应用的不同要求定义了从A到D四种服务类型。1类到5类AAL提供了满足这些要求的标准

需要面向连接的服务、可变比特率传输和低延时的应用可归为B类应用。分组视频就是一个需要B类服务的例子。换句话说，发送端的AAL将视频分解为信元并要求网络提供B类服务，而当信元到达接收端时，该层再把它们还原成原来的视频信号。

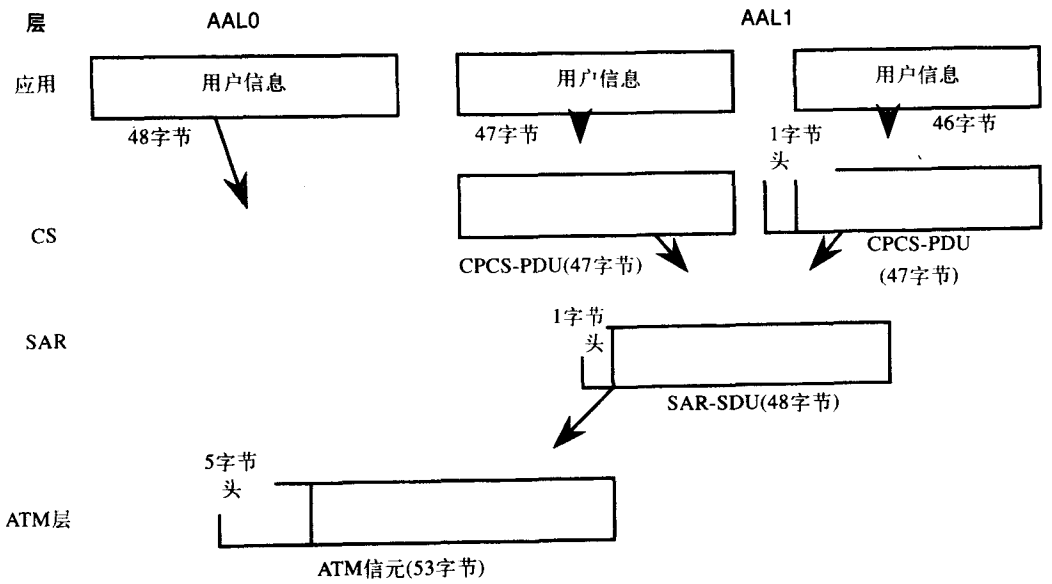
LAN与IP流量为D类应用，它们是基于VBR（Variable Bit Rate，可变比特率）的、无连接和对延时不敏感的应用。

为了兼容各种不同类型的应用，ATM已经定义了几组称为AAL类型的标准。各AAL类型提供一种AAL层的特定的实现方法，以满足这些需要，见图22-8，这就是AAL类型1~5。尽管不同的服务类型提供了对各种应用需要哪些服务的概念模型，但是AAL类型则给出了实现它们的具体方法。因此，现在AAL类型已经比AAL服务类型具有更重要的意义。

22.3.2 AAL 0

如果应用程序是用ATM API（Application Programming Interface，应用程序接口）编写的，则所有传输单元都正好为48个字节，可以很好地符合ATM信元，在这种情况下就不需要AAL层了。应用程序不需要与ATM信元适配：将准备好的数据单元加载到信元中。此时，AAL是不存在的，并将这种类型的AAL称为AAL 0。但是，应用程序必须把帧分割成信元，并在终端重新组合起来。在这种情况下，应用程序就仅能要求重传一个信元，而不是其所属的整帧或分组。

在图22-9左边给出了一个为ATM网络提供48字节信息单元的应用。这里没有用到AAL的子层CS（Convergence Sublayer，会聚子层）和SAR（Segmentation And Reassembly，分段和重装）。因为现在大多数的应用程序并未考虑ATM的要求，所以还是需要实现AAL。在后面将会看到CS和SAR子层在其他AAL中的实现。



PDU: 协议数据单元
SDU: 业务数据单元
CS: 会聚子层
CPCS: 公共部分会聚子层
SAR: 分段和重装子层

图22-9 0类AAL根本不使用AAL。这种应用程序在编写时考虑了ATM的要求。1类AAL的应用程序绝大多数只使用SAR层。电路仿真、DS1、DS3、话音和实时视频都是1类AAL应用的例子

22.3.3 AAL 1

一个需要仿真诸如DS1或DS3电路的应用程序可以使用AAL 1格式。这些应用包括话音和实时视频，它们以恒定比特率传送并对延迟敏感。

图22-9所示为一个正在发送恒定比特流的应用。每组47字节，加上一个SAR头并置于一个信元中。以这种方式处理的比特流称为被“截切并抛入”（chopped and dropped）到信元中。当一个比特块的开始需要标出时，CS层会使用信头的一个额外字节，这由图22-9的右边可见。这时是只有46个字节的用户消息加载到了CS PDU。对于多数信元而言，CS层是不存在的，这可以使1类AAL的延迟减小。因此，AAL 1适用于话音和视频。

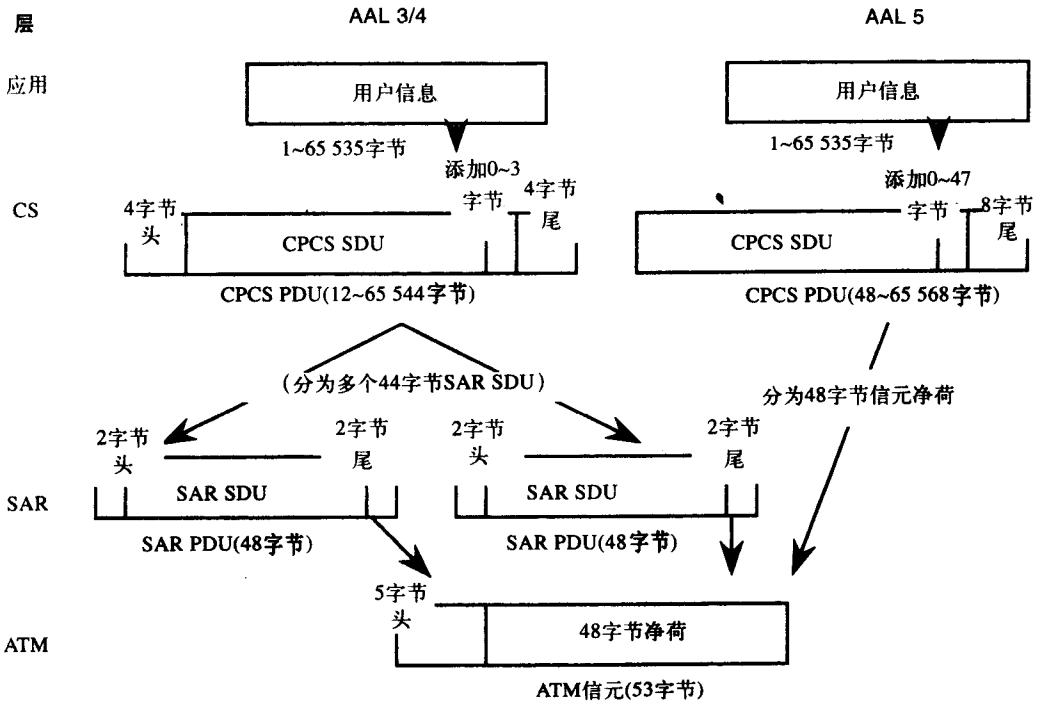
22.3.4 AAL 2

最初，AAL 2是为了支持分组和压缩话音以及分组和压缩视频而设计的。后来，放弃了实现AAL 2，这些应用现在由AAL 3/4和AAL 5格式来完成。

22.3.5 AAL3/4

AAL 1适用于话音和视频，而AAL 3/4适用于数据。起初，AAL 3是为C类服务设计的，AAL 4 则是为D类服务设计的。它们之间的区别在于C类是面向连接的，D类是无连接的。对于数据传输而言，低误码率比连接模式更重要。因此，现在这两种AAL类型已经合并在一起称为AAL 3/4。

由图22-10的左边可见用户信息是如何用AAL 3/4加载到ATM信元的。消息可以以最大长度为65 535字节的数据块到达CS层。如果需要，该层将添加一个4字节的头和一个4字节的尾，以使PDU的长度为半字节的偶数倍。这种传输单元称为CPCS PDU，可以长达65 544字节。这些信头提供了一种检查在重装用户信息时是否有信元丢失的方法，它也提供了其他类型的错误检查。这一层提供的其他功能现在已经不多用了。



PDU: 协议数据单元
SDU: 业务数据单元
CS: 会聚子层
CPCS: 公共部分会聚子层
SAR: 分段和重装子层

图22-10 为可变长的分组和帧提供纠错，AAL 3/4增加了相当多的开销。相反，AAL 5更简洁，效率更高

CPCS（Common Part Convergence Sublayer，公共部分会聚子层）子层将该PDU转发给SAR（Segmentation And Reassembly，分段和重装子层）子层。它是通过将PDU切割为44字节的SAR SDU来完成的，这是因为SAR在将PDU发送到ATM层之前要给每个4字节的SDU加上它自己的开销。

每个SAR SDU都有自己的2字节头和2字节尾。该层为数据的44个字节都提供比特错误校正，但是，如果应用程序本身提供错误校正的话，这里的检错和纠错就不必要了。而且，随着光纤的普及，检错也越来越不必要了。

SAR头也可使许多数据流在一条虚电路上复用。这样，当一个应用程序在某时刻空闲时，其他应用程序的数据就可以通过相同的ATM连接进行多路复用。这个特性主要用于SMDS（Switched Multi-megabit Digital Service，交换式多兆位数字业务），SMDS主要是由贝尔大西洋（Bell Atlantic）公司为高安全性电路提供的服务。除此之外，SMDS基本不用。

因此，采用AAL 3/4的最主要原因是为数据传输提供了检错机制，因为只需要重传单个的SAR PDU而非整个CPCS PDU。

22.3.6 AAL 5

如果错误控制对于数据、话音和视频传输不是很重要，那么，就此而言AAL 5则是快速而高效的。由图22-10的右边可知，如果需要的话，AAL 5只加上一个8字节的尾和一些填充字符，从而将CPCS PDU变成48字节的偶数倍。该图表明SAR层被略过了。事实上，SAR层将用ATM信元头PT字段的第三位来标识该信元是否为给定CPCS PDU的最后一个信元。因此，AAL 5也叫做SEAL（Simple and Efficient Adaptation Layer，简单高效适配层）。

CPCS层没有增加任何信头，SAR层也没有增加任何信头和尾，这就意味着AAL 5格式需要处理的工作很少。起初，AAL 5是为了传送IP分组而设计的，IP分组采用TCP进行纠错。AAL 5也进行纠错，但是只限于CPCS层，这比AAL 3/4对每个SAR PDU都要检错要少得多。AAL 3/4并没有为整个CPCS PDU提供检错机制。

一般而言，AAL 3/4的开销约为20%，然而，当帧为64个字节时，这一开销可达到40%。这与AAL 5用于传送64字节信息时的开销大致相同。因此，只有在信息帧较大时，AAL 5才优于AAL 3/4。

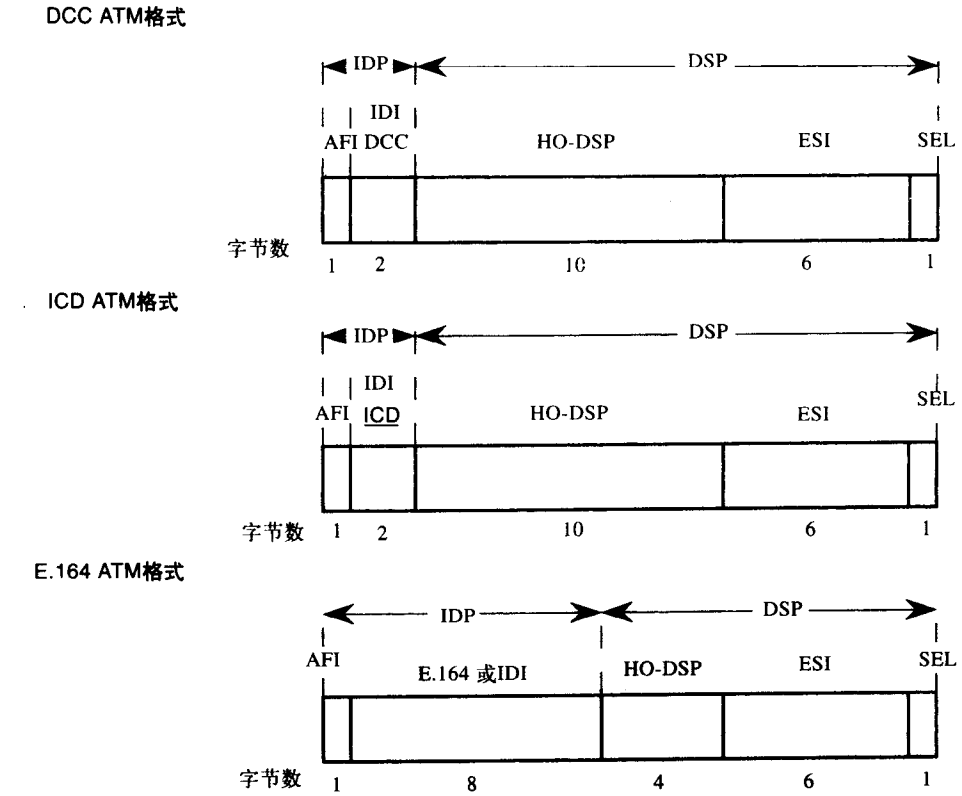
22.4 UNI 信令

本节讨论UNI（User-to-Network Interface，用户-网络接口）上的信令。信令所用的AAL称为SAAL（Signaling AAL，信令AAL）。实际上它在CPCS（Common Part Convergence Sublayer，公共部分会聚子层）和SAR子层中使用AAL 5。在这些层之上，SAAL使用SSCS（Service Specific Convergence Sublayer，特殊业务会聚子层）。回顾图22-4，SSCS和CPCS都是CS层的子层，而CS和SAR都是AAL的子层。正如我们在前面描述用户数据时提到的，AAL 5根本就不使用SSCS层，SSCS层主要为SAAL所用。SSCS子层提供了AAL 5所缺少的可靠的数据传输。

所有的ATM终端和交换机在整个网络中必须有唯一的ATM地址。ATM地址长度为20字节，即160比特。ATM地址有三种格式，但是不论是哪种格式，都有三个基本部分。前缀部分为13个字节，用于标识ATM交换机；地址的终端系统部分为6个字节，用于标识与交换机相连的CPE或主机。最后一个字节叫做网络选择器部分，其作用由终端系统的供应商决定。这三种特定格式的细节部分由图22-11给出，这些地址的名称就称为AESA（ATM End Station Address，ATM终端站地址）。

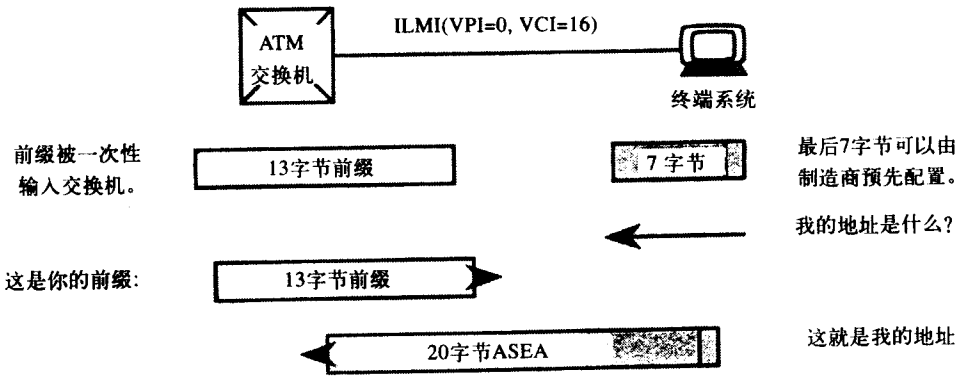
图22-12给出了终端如何接收它的AESA。一般来说，利用MAC地址或其他嵌入硬件的地址，终端就可以得到它的AESA地址的一部分，这些是AESA的最后7个字节。与终端系统相连的ATM交换机的管理员要一次人工输入13个字节的前缀，而不需考虑交换机上可用端口的数量。

一旦它们之间建立起连接，终端系统利用SNMP（Simple Network Management Protocal，简单网络管理协议）指令就会自动地计算出它的完整地址。这个对话发生在ILMI（Integrated Local Management Interface，集成本地管理接口）通路。它总是在VPI为0和VCI为16上。终端系统会告知交换机它要在交换机上注册地址。交换机将首先给终端系统发送前缀，之后，终端系统将计算出完整的AESA并在交换机上注册。



HO-DSP: 高阶域特定部分
IDP: 初始化域部分
IDI: 初始化域标识符
DCC: 数据国家代码
ICD: 国际代码指示符
ESI: 终端站标识符
DSP: 域特定部分
AFI: 授权格式标识符
SEL: 网络选择器

图22-11 ATM中所用的三种地址格式



ILMI: 集成本地管理接口
AESA: ATM终端站地址

图22-12 自动地址注册

终端系统一旦知道了地址，它就可以建立信令链路。只有信令链路建立起来以后，才可

以进行呼叫，这个过程如图22-13所示。该链路是用VPI为0和VCI 5建立的。SSCP从终端系统向ATM网络的第一个节点发送一个Begin（开始）帧，该帧由一个开始确认（Begin Acknowledge）帧应答，这就完成了链路建立阶段。如果网络在收到Begin帧时没有就绪，就会返回一个开始未被确认（Begin Negative Acknowledgment）帧。

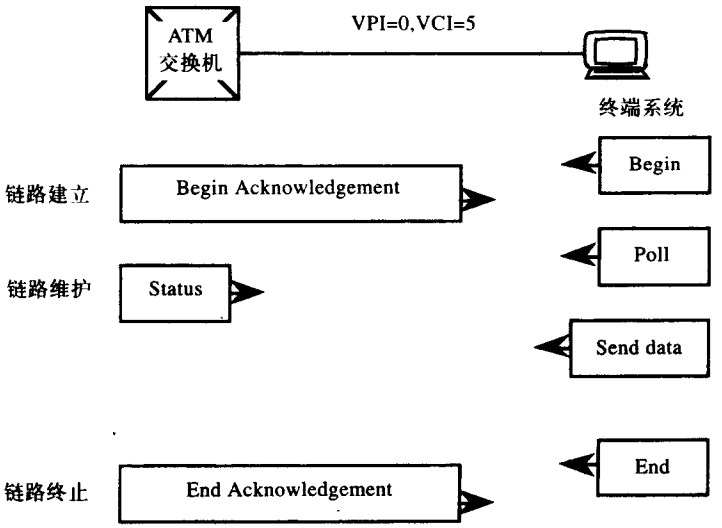


图22-13　在UNI上建立、保持、拆除一条信令链路

一旦建立起链路，“心跳”信号就通过UNI发送，这包括一个由终端系统发送的轮询（Poll）帧和网络发出的状态（Status）帧。这些帧从信令激活并就绪的各端得到确认。当信令帧必须通过UNI发送时，发送数据（Send Data）帧就被发送出去，这些帧带有发送和接收的顺序号。SSCP利用这些顺序号保证网络的可靠性，这些号码在两端发送轮询（Poll）帧和状态（Status）帧时达到同步。

图22-13的最后一部分表示链路被断开。终端系统发送一个结束（End）帧，网络回应一个结束确认（End Acknowledge）帧，所有这些帧都是通过VPI为0 和VCI为5发送的。

一旦解决了地址问题，就建立了信令链路，于是就可以通过ATM网络进行呼叫了，该过程如图22-14所示。左边的终端系统通过向第一个ATM交换机发送一个建立（Setup）帧来发起一次呼叫，该过程由一个高层应用程序发起。这个交换机将会执行两个任务：运用NNI（网络节点接口）在网络中找到一个电路，并给终端系统返回一个呼叫处理（Call Proceeding）帧，这个呼叫处理（Call Proceeding）帧包含了分配给终端系统的VPI和VCI。

出口ATM交换机一收到连接请求，就会向目的终端系统发送一个建立（Setup）帧，该帧将包含终端应该使用的VPI和VCI。如果终端系统接受此次呼叫，它就发送一个连接（Connect）帧，最后入口ATM交换机将发出另一个连接（Connect）帧。通过各UNI的两个连接确认（Connect Acknowledge）帧完成此次呼叫。注意，图中所示的所有帧都通过本地接口传送。

一旦呼叫结束，就应该终止连接，这是由任一方向ATM交换机发送一个释放（Release）帧完成的。这个终止请求是利用NNI通过网络发送的，直至该帧到达另一端的交换机。出口ATM交换机也会发出一个释放（Release）帧，收到这些释放（Release）帧的节点将依次用释放完成（Release Complete）帧回应，由此撤销连接。

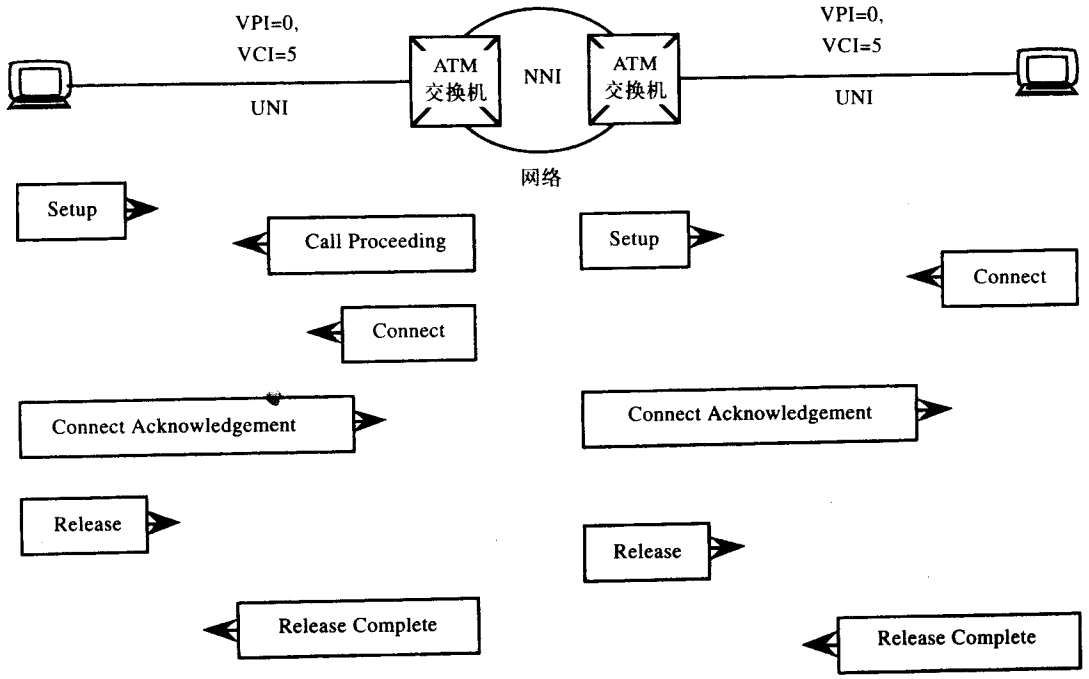


图22-14 通过ATM网络建立和释放一次呼叫

习题

22.1节

1.哪种类型的流量是同步的?

a. 视频　　b. 图像

c. 数据　　d. 局域网

2.分组话音利用哪种类型的应用业务?

a. CBR　　b. UBR（非指定码率）

c. VBR　　d. ABR（实用码率）

3. 下列哪个不是采用信元的优点?

a. 允许直切式交换

b. 产生较小的开销

c. 减小线路头的阻塞量

d. 由硬件而不是软件完成交换

4. 决定延迟大小、延迟变化和误码率等的参数叫什么?

5. 给出ATM结构的三层的名字，并描述它们的作用。给出可以进行再划分的层的名字以及子层的名字。

6. 哪一层处理ATM信头的HEC字段?

7. ATM网络中的交换机处理AAL吗?

22.2节

8. 终端系统与第一个ATM交换机之间的接口叫做什么?

a. LMI　　b. NNI
c. AMI　　d. UNI

9. 信元头中的PT字段中的哪一位不常用到?
a. 第一位　　b. 第二位
c. 第三位　　d. 第四位

10. 在哪种类型的交换中，VPI随着链路的不同而改变，但VCI却在一次连接中保持不变?
11. 在哪种类型的交换中，VPI和VCI都随着链路的不同而改变?
12. ATM信元的开始是怎么确定的?
13. UNI中的VPI字段多长? NNI中的呢?
14. GFC字段的值应该是多少?
15. CLP比特如何使用和设置?

22.3节

16. 哪类业务类提供低延迟、面向连接的传输以及可变比特率?
a. A类　　b. B类
c. C类　　d. D类

17. 哪个AAL层现在已经几乎不存在了?
a. AAL 0　　b. AAL 1
c. AAL 2　　d. AAL 3/4

18. 哪种应用会利用AAL 0层业务?
19. 需要仿真专用电路的话音应用程序会使用哪种AAL?
20. AAL 3/4在哪些方面优于AAL 5?
21. AAL 5在哪些方面优于AAL 3/4?
22. 假设一个应用发送的用户信息长度为80个字节。该信息将产生多少个CPCS PDU? 其中各PDU的长度为多少个字节? 该信息会产生多少个SAR PDU? 其中各PDU的长度又是多少个字节?

22.4节

23. 描述AESA的三个部分以及这三个部分定义了什么。
24. AESA存在几种不同的格式?
25. 描述一台终端工作站如何在ATM交换机注册自己的地址。
26. 描述一条信令链路建立后应如何保持。
27. 哪一帧开始建立一个ATM连接?
28. 当呼叫建立期间，哪些帧提供将要用到的VPI和VCI?

第四部分 局域网和互联网络

第23章 LAN：补充概念

本章我们将接着第7章继续讨论。在第7章我们对LAN有了一个大概了解，这里将讨论更多的细节问题。比如第7章给出了以太网帧结构的一个粗略描述，本章我们将看到，以太网的帧结构不止一种以及它们是如何构成的。同时我们还会在本章讨论诸如以太网、令牌环网和FDDI等多种网络的特点。最后以对新型以太网即高速以太网和千兆以太网的讨论结束本章。

23.1 软件基础

本节我们将注意力转向构建LAN所必需的软件部件上。假设以IBM PC作为网络节点，我们来讨论网络组成，并对Windows 98网络的基本特点作简要介绍。最后我们将讨论扩展到IEEE 802以及一些专有协议，并说明它们彼此之间以及OSI参考模型之间有什么关系。

23.1.1 NetBIOS

在讨论IBM PC的网络性能之前，首先简要地了解一下BIOS（Basic Input/Output System，基本输入/输出系统）以及DOS（Disk Operating System，磁盘操作系统）在PC中所起的作用。

BIOS和DOS：BIOS（Basic Input/Output System，基本输入/输出系统）是ROM（Read Only Memory，只读存储器）芯片中的一组机器语言程序，它在物理上位于计算机内部。当计算机上电时，ROM或BIOS首先启动一个简单的检测程序察看有哪些设备与之相连，这称为POST（Power On Self Test，上电自检），它检测CMOS（Channelized Metal Oxide Semiconductor，沟道型金属氧化半导体）芯片以获得计算机的配置。由于BIOS使用CMOS来启动计算机，因此许多人误认为BIOS与CMOS是同一设备。CMOS需要少量电池来跟踪时间、存储密码设置、引导顺序以及许多其他配置选项。这之后BIOS将在硬盘或其他驱动器上寻找引导记录并加载操作系统。在这之前计算机一直由BIOS控制。

与BIOS不同，DOS（Disk Operating System，磁盘操作系统）来自光盘或硬盘并被BIOS加载到计算机的RAM（Random Access Memory，随机访问存储器）。DOS使用比BIOS高级的指令。我们所使用的术语DOS包含Windows 98操作系统。

除了启动PC外，BIOS的主要功能是对与计算机相连的显示器、键盘和磁盘驱动器等提供基于软件的控制。任何时候当用户通过键盘键入一个字符时，BIOS都会接收它并将其提供给应用程序。与之类似，当应用程序需要在显示器上显示时也必须通过BIOS。

DOS为用户和应用程序提供了一个更高级的接口，这样用户使用DOS命令就会比调用BIOS容易得多。如图23-1所示，应用软件既可以执行BIOS调用又可以执行DOS调用。然而，由于BIOS调用无需经过DOS，故其执行速度更快。进行DOS调用的应用具有更高的可移植性，也就是说它们可以在多种模拟BIOS和使用特定版本的DOS的机器上运行。但是，以前不同厂

商提供的各种BIOS版本并没有统一到同一个标准，这使得它们对于同一软件的工作方式并不相同。

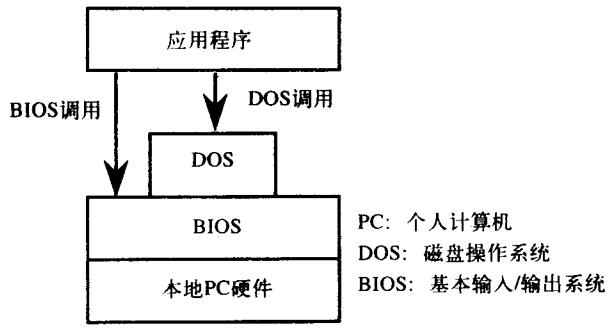


图23-1　执行BIOS调用的应用程序更高效，但是执行DOS调用的应用程序则具有更好的移植性

NetBIOS和NOS：对于独立的PC，让我们给它加一个NIC（Network Interface Card，网络接口卡）使之成为LAN的一部分。这里我们并不关心它是TRN、Ethernet（以太网）或者其他种类的NIC。在任何一种情况下，控制NIC的机器语言代码都驻留在NetBIOS（Network BIOS，网络BIOS）中。在早期的NIC中，NetBIOS存储在NIC的ROM芯片中，后来，无论是Novell的NetWare还是Windows 98，该代码都是由网络软件进行仿真的。NetBIOS处理OSI模型中所有的会话层功能，而NIC则支持该层及其以下的所有层，如图23-2所示。

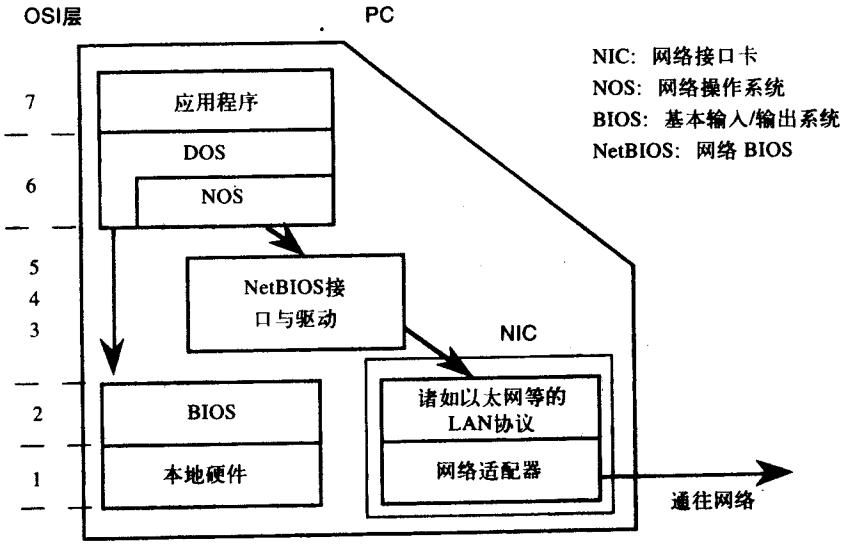


图23-2　DOS能够通过BIOS访问本地硬件，或者通过NetBIOS访问网络设备

NetBIOS从本地系统接收数据帧，并将其传输到网络上。为了与NetBIOS相接口，我们需要一个LAN操作系统，称之为NOS（Network Operating System，网络操作系统）。NOS与NetBIOS之间的相互作用类似于DOS与BIOS之间的相互作用。

如果应用程序需要访问本地磁盘，那么DOS将通过BIOS实现，如果应用程序需要访问一个网络磁盘或资源，则该请求由NOS通过NetBIOS实现。

23.1.2　Windows 98 网络

存在两种类型的NOS，Windows 98是点对点NOS（或简称为对等NOS）的一个例子。这些NOS通常比与它们相对的基于服务器的NOS慢。基于服务器的NOS又称为集中式NOS或客

户-服务器NOS。

基于服务器的NOS运行在一台专门作为服务器的机器上，网络工作站或客户访问它的文件。基于服务器的NOS功能更加强大，因为它们不是运行在DOS下的，而由NOS掌管整个服务器。它们不受DOS的限制，并且能够处理比对等NOS更多的客户。

然而，对等NOS提供了一种网络节点之间的低成本互连方案。任何具有硬盘的计算机都可以成为文件服务器。网络几乎不依赖于机器。如果愿意的话，任何一台机器都可以出现在任何其他机器的程序中。但是这种小规模网络不能很好地与更大型的、企业级网络互连，这使得它们难以扩展。为了了解点对点网络如何工作，让我们首先简单了解一下Windows 98是如何用在网络中的。

假设我们家里有两台运行Windows 98的PC，它们都安装有各自的以太网NIC。由于只有两台PC，因此没有必要使用网络集线器。它们使用5类双绞线通过RJ-45标准连接器相互连接，我们称其中一台PC为host23，另一台为host2。我们不想通过软盘在这两台PC之间传递文件以及安装应用程序，而是希望能够在它们之间共享文件。下面看一看使用Windows 98自带的点对点网络软件如何实现这一功能。首先，我们进行host23需要的步骤。

在host23上，我们需要安装NIC的驱动程序。从Start（开始）按钮开始，点击Settings（设置），之后是Control Panel（控制面板），最后点击Network（网络设置）图标。Network（网络设置）窗口如图23-3a所示，该窗口有三个标签：Configuration（配置）、Identification（标识）和Access Control（访问控制）。出现Configuration 标签和在Icon X所指位置安装的3Com以太网卡。如果尚未安装，则按下列给定顺序选择：Start（开始）、Settings（设置）、Control Panel（控制面板）、Network（网络设置）、Add（添加）、Adapter（适配器）、Have Disk（从磁盘安装）、Browse（浏览）。接着高亮度选择你的以太网卡驱动程序并重新启动PC。你也许需要重新启动两次，并通过一个驱动器向导让你的PC识别NIC。

接着，将我们的PC标识为host23并使其成为cis238工作组的一个成员。这可以通过点击Identification 标签看到，如图23-3b所示。为了让两台PC彼此共享文件和打印机，它们必须在同一个工作组中。标识完PC之后，你必须重新启动PC并且它也会引导你这样做。在重新启动过程中你将在屏幕上看到如图23-3c所示的窗口，即会看到屏幕上出现host23。这时不要简单地关闭或取消该对话框，而要点击OK或按Return（回车键）。这样就完成了host23在网络上的正确配置和标识。下面对我们的另一台PC host2做相同步骤的操作，完成其在网络上的配置和标识。

在任何资源可以被共享之前，我们必须完成如图23-3a所示的步骤。如前所述，进入Network（网络设置）对话框，点击File and Print Sharing（文件和打印机共享）按钮，即图中的Click 2所示，于是出现File and Print Sharing窗口。这里我们只想共享host23上的文件资源，因此选中Click 3所示的复选框，接着点击OK，再点击Network窗口的OK。这一过程使我们能够将文件与网络中属于cis238工作组的主机共享。如果想要共享打印机，则选中File and Print Sharing窗口中的另一项。

host23将与网络上的其他主机共享文件，这就意味着host23上的文件将可以被其他主机访问。在我们的网络中，唯一的其他主机就是host2，但是也可以有很多其他主机。与共享相对的是使用，host2将使用host23为其共享的文件资源。换句话说，使用意味着其他主机上的文件或资源是可以被访问的。



图23-3　a) 设置host23使其能够共享文件

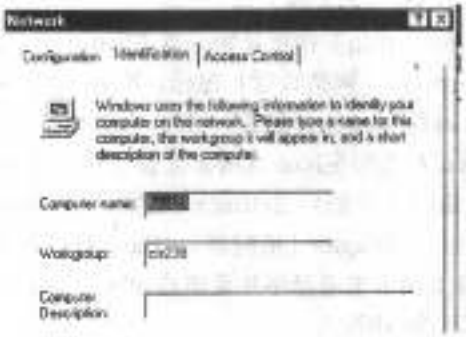


图23-3　b) 确定host23的标识

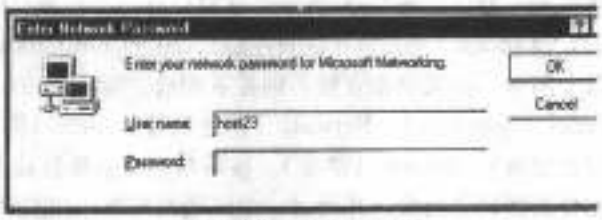


图23-3　c) 登入host23

图23-3a给出了如何在host23上实现共享，图23-4a表示C：驱动器如何被共享给host2。host23同样可以将其他本地设备共享，比如其他驱动器、文件夹甚至是个人文件。这里，整个C：驱动器都被共享。

点击My Computer（我的电脑）图标，右键点击C：驱动器，你将看到如图23-4a所示的菜单，下拉至Sharing（共享）并点击，将会出现Properties（属性）窗口。点击Shared As（共享为）单选按钮，C：驱动器就会出现如图23-4a所示的情况。点击Read-Only（只读）单选按钮，这将禁止host2在C：驱动器上改变、删除和创建新文件，然后点击OK。之后你就会看到C：驱动器图标下面出现一只手，如图23-4a所示，这表明C：驱动器正处于被共享状态。

现在再来看看host2，假设它的NIC安装正常，正确配置并对网络功能进行了重新启动，点击桌面上的Network Neighborhood（网上邻居）图标，我们应该在所出现的窗口中看到host2和host23，如图23-4b中最上方的窗口所示，这就确认了host2检查到自己和host23都位于同一个网络上。我们想在host2上访问host23的C：驱动器，因此在host2上点击host23，于是就出现如图23-4b所示的标记为host23的窗口。接着在host23上点击C：驱动器文件夹，就在host23窗口中进入到C：驱动器。这里我们找到一个叫做testfile的小文件，testfile是之前在host23上创建的。当用Notepad（记事本）将其打开时，我们会看到该文件的内容，即"This file is to be shared"，改变文件并试图保存，在Save As（另存为）对话框中我们得到一个错误，

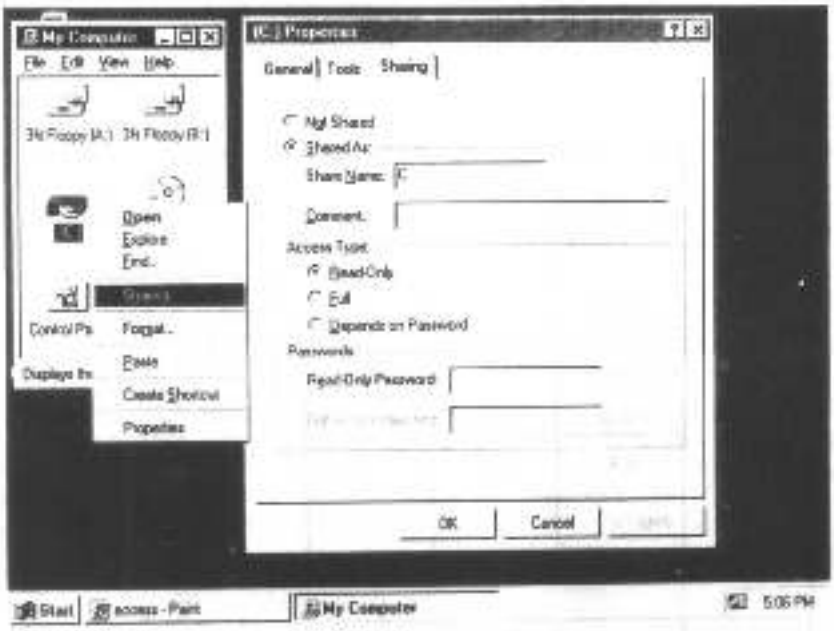


图23-4 a) host23以只读访问方式共享其C: 驱动器

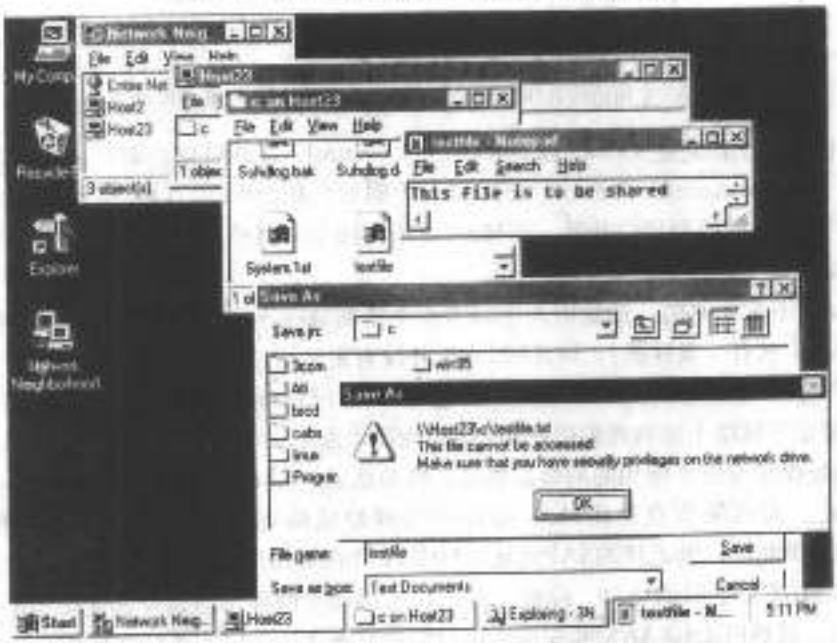


图23-4 b) host2正在使用host23的testfile，但不允许对其进行写（或保存）操作

说明我们没有权利在host23的C: 驱动器上保存文件。这是因为我们已经在图23-4a中点击了host23上的Read-Only（只读）单选按钮。

23.1.3 IEEE 802 标准

1980年2月，IEEE决定将LAN标准化，并使用该年月数字，启动了802工程。此工程的目

的是将现存的许多LAN协议统一在“一把伞”下，称之为802标准。

现在我们撇开图23-5的上半部分，仅看由IEEE 802协议组定义的第一层和第二层。

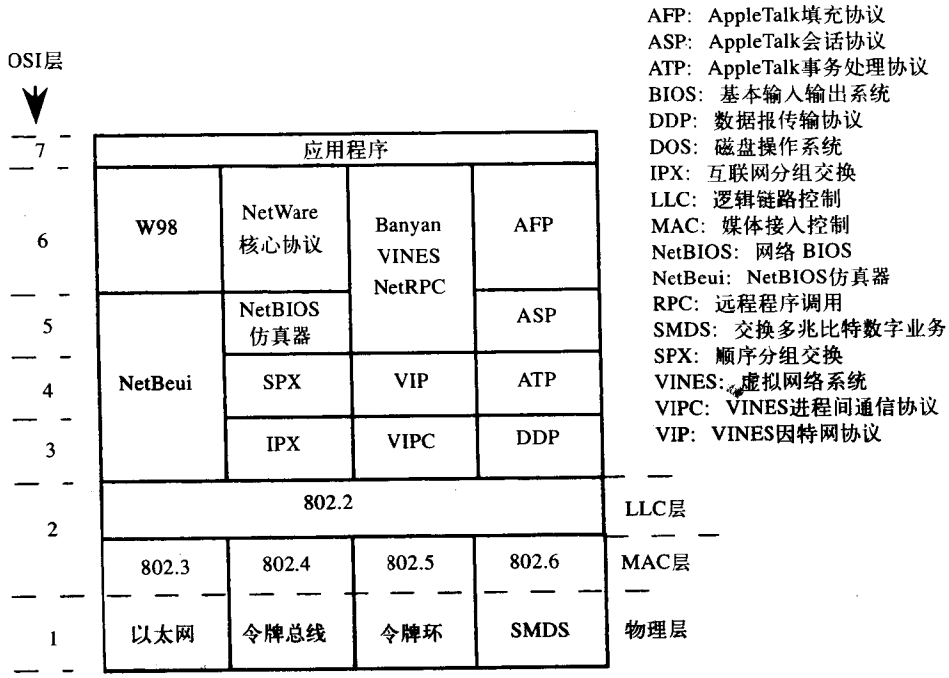


图23-5　专用协议和IEEE 802协议组，它们均与OSI参考模型有关

802协议栈的上部是定义LLC（Logical Link Control，逻辑链路控制）层的802.2规范，下面是MAC（Media Access Control，媒体接入控制层）和物理层。LLC层和MAC层共同提供OSI模型中数据链路控制层的功能，而MAC层和物理层共同描述了特定类型LAN的细节。例如802.3规定了以太网标准。

由于LAN不需要路由，这是因为中间节点不需要通过不同的链路将接收到的帧重新发送（因为在LAN中只有一条链路），因此802协议并没有定义网络层。当某个节点收到一帧时，其中包含一个MAC地址和一个LLC地址，称之为SAP（Service Access Point，业务接入点）。MAC地址规定了网络上被物理编码在NIC中的物理节点。

SAP地址提供通信中所用的网络层协议，换句话说，SAP为第三层即网络层协议提供了一个逻辑地址，而网络节点是由MAC地址和物理地址确定的。比如说，十六进制的E0是NetWare的SAP地址，06是IP的SAP地址，F0是IBM的NetBIOS的SAP地址。LLC层提供了一个网络层与MAC层之间的接口，除此之外，LLC层对令牌环网络以及其他类型的802族LAN都是相同的。虽然FDDI是ANSI的标准，但它能很好地适合于LLC并与之兼容。

图23-6进一步详细讨论了LLC层并说明了其如何加入MAC帧中。MAC头和尾由特定的网络协议如以太网或TRN决定。MAC层将来自上层和LLC头的数据看作信息。

LLC层用其三个字段管理LLC的帧头：DSAP（Destination SAP，目的SAP）、SSAP（Source SAP，源SAP）和控制字段。控制字段又有三种类型，分别由它所处理的LLC帧的类型决定，它们是信息帧、监控帧和未标号帧。未标号帧的控制字段只有8比特，而其他两类帧的控制字段均为16比特。

上述所有字段在介绍SNA和X.25时都已经讨论过。最后，存在两种类型的LLC业务，第1类

用于非确认的、无连接的或数据报传递型业务；第2类用在通信SAP之间面向连接的业务。此图描述了未标号帧的类型，并将其标识为命令和响应。稍后在以太网部分我们将继续讨论LLC。

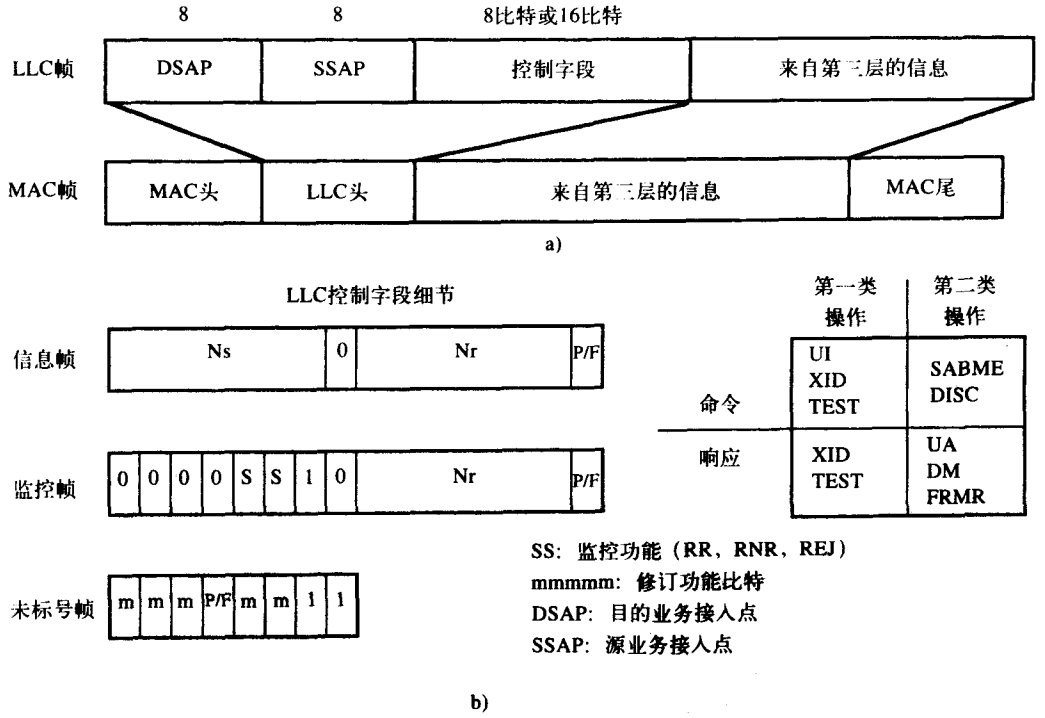


图23-6 a) 当信息被LLC层接受时，它会加入其自己的头，由SAP规定协议类型，之后MAC层加入其头和尾。b) 这三类帧的LLC头具有如图所示的修订功能

23.1.4 专用协议

将注意力转向图23-5的上半部分，我们看到各种专用协议的实例以及它们是如何安排在整个LAN协议图中的。高层（3~6）的协议栈的每一个都可以通过802.3至802.6层实现。否则，它们也可以通过其他的专用低层协议实现。例如，最右列所示的AppleTalk可以运行在一个称为LocalTalk的专用协议上或者运行在如图所示的一个低层协议上。图中第一个栈表示使用IBM的NetBIOS协议的Windows 98系统。

在图23-5中，我们还可以看到Novell的NetWare协议栈。NetWare基于Xerox的XNS（Xerox Network System，Xerox网络系统）。XNS在定义ISO模型中具有非常大的影响，同时Xerox还为我们提供了图形用户接口和以太网等一些很好的事物。

应用程序可以在各层与NetWare相接口。当一个网络节点使用DOS请求访问一台服务器上的文件时，它会使用称为工作站命令解释程序接口（Workstation Shell Interface）的应用层接口。在会话层，应用程序可以发起与NetBIOS相兼容的呼叫，这是由于NetWare的NetBIOS是对IBM的NetBIOS的模拟。传输层可以为请求面向连接的分组传递的应用程序提供虚拟连接接口，这是通过使用SPX（Sequenced Packet eXchange，顺序分组交换）头中的顺序号实现的。最后，应用程序可以在网络层为无连接的数据报通信提供接口，这是通过IPX（Internetwork Packet eXchange，互联网分组交换）协议完成的。

Banyan系统公司的VINES（VIrtual NEtwork System，虚拟网络系统）是一种基于Unix操作系统的NOS。它可以用在各种类型的网络和平台上。在一个DOS平台上，工作站是基于DOS的；但在一台服务器上，它是运行在一个Unix核下的。这些协议中的很多最初都是在Unix下开发的。

苹果计算机公司的AppleTalk主要应用在Macintosh计算机上，这些计算机均已带有LocalTalk网络接口。AppleTalk栈的最底层是DDP（Datagram Delivery Protocol，数据报传输协议），它将网络节点的合适进程提供给通信接口。

虽然有很多协议可以在高层实现，但图中仅给出了主要的几个。在传输层ATP（Apple Talk Transaction Protocol，AppleTalk事务处理协议）提供有序而可靠的分组传递，而ASP（AppleTalk Session Protocol，AppleTalk会话协议）则管理并维护插口（或进程）之间的会话。最后，AFP（AppleTalk Filing Protocol，AppleTalk文件协议）支持远距离文件传输。

23.2 以太网

23.2.1 以太网帧结构

以太网最初是由Xerox公司、DEC公司和Intel公司开发的。1985年，IEEE将其标准化为802.3，与最初版本稍有不同。在23.1节特别是在图23-6中，我们看到怎样将一个头加到LLC层收到的信息上并转发给MAC层。现在我们来看看以太网的MAC层添加的头和尾。之后在谈到TRN和FDDI时，我们将复习它们的MAC标准。LLC层对它们来说都是相同的。

图23-7表示了以太网帧结构的三种类型。虽然以太网II应用更为广泛，但本节我们将其简称为以太网，它是最初的以太网标准。接着出现了不带SNAP（子网接入协议）的802.3帧结构和带有SNAP的802.3标准。如前所述，802.2帧被封装在802.3帧中。

最常见的以太网就是图中第一种，它的结构最简单，因此在“以太网协议大战”中获得了胜利。然而，带有SNAP的802.3格式仍然存在于一些LAN中，所以也在这里给出，而对它的理解最好是从不带SNAP的帧开始，所以也列出了这种帧结构。当然还有一些其他的以太网帧结构并未在这里给出。下面首先看看所有这些帧结构所共有的字段，之后再讨论它们之间有何区别。

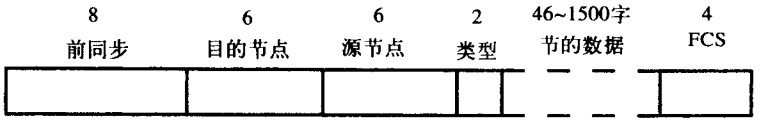
所有帧的最大长度为1518个字节，最短长度为64个字节。以太网的前同步（或称为前导、帧头）字段长度为8字节，并非官方以太网帧的一部分。其目的是使接收NIC与发送NIC同步。前同步有一串以“11”结尾的“10”。IEEE帧定义了7字节前同步和一个一字节的SFD（起始帧分隔符）字段，它们共同定义了与以太网的8字节前同步相同的比特模式。由于有许多1到0的跳变，因此这8个字节可以提供同步。

接下来的两个字段规定了源节点与目标节点的MAC地址和物理地址，该地址字段长度通常为6个字节，其中前3个字节由IEEE管理（最初由Xerox管理）并分配给了NIC生产厂商。后3个字节由生产厂商分配管理，这样在全球范围内所有以太网卡的地址都是唯一的。

通常情况下，这个地址都被烧入NIC的ROM内，但它也可以使用诊断磁盘来分配。如果物理地址需保持相同，那么在更换板子时，ROM芯片也应该一起更换。

在两种类型的帧中，如果I/G（单个/组）地址位被发送方置为0，则该帧将被发送给单个用户，反之将发送给一组用户，称为组播传输。当所有48比特都被置为1，就发生广播，并且所有用户均会接收到该帧。IEEE帧使用U/L（全局/本地）地址位来表明地址字段是符合IEEE寻址标准还是使用了某些其他的本地寻址方案。

以太网II帧结构

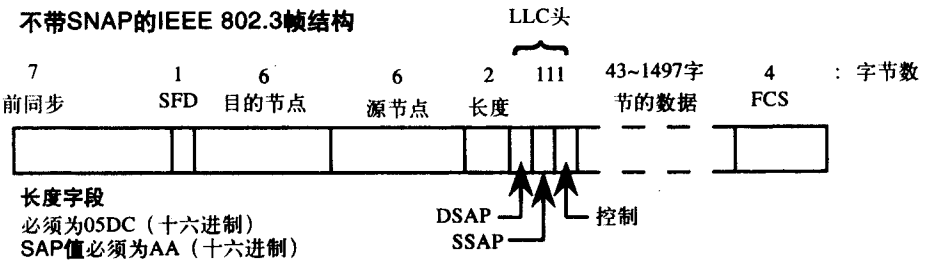


类型字段

所有值必须大于1500（十进制）或05DC（十六进制）

所用值的例子（十六进制）：0800：IP，0805：X.25，0806：ARP（地址解析协议），80D5：SNA，8137－8138：Novell

不带SNAP的IEEE 802.3帧结构



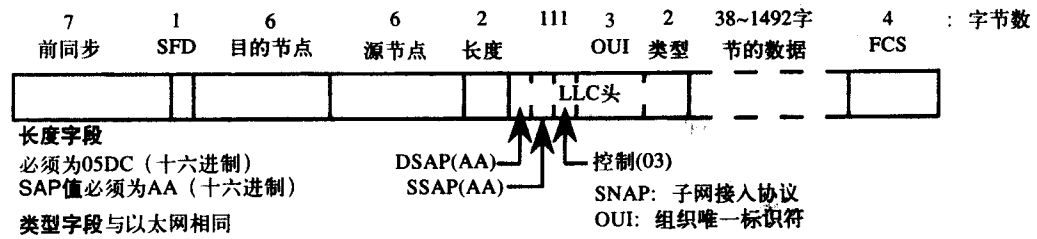
长度字段

必须为05DC（十六进制）

SAP值必须为AA（十六进制）

SAP值的例子（十六进制）：06：IP，7E：X.25，98：ARP，E0：Novell，F0：NetBIOS

带有SNAP的IEEE 802.3帧结构



长度字段

必须为05DC（十六进制）

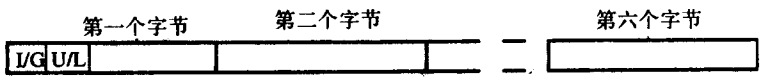
SAP值必须为AA（十六进制）

类型字段与以太网相同

SNAP：子网接入协议

OUI：组织唯一标识符

地址字段



I/G U/L	地址管理	寻址类型
0 0	由IEEE完成	独立
1 0	由IEEE完成	组播
0 1	由本地完成	独立
1 1	由本地完成	组播

I/G：单个或组

U/L：全局或本地

以太网前同步："1010...101011"

802.3前同步："1010...1010"

SFD："10101011"

SFD：起始帧分隔符

图23-7 三类以太网的帧结构以及MAC地址字段。在源路由中，源地址中的I/G比特设置为1，否则设置为0

所有三种格式的最后一个字段都是FCS（Frame Check Sequence，帧校验序列）。它采用CRC32检错。被NIC检测到有错误的帧将被丢弃，MAC层不需要重发，而由高层协议负责请求重新发送丢失的帧。

类型字段给出了数据字段所采用的以太网协议的类型，比如IP为0800，X.25为0805等等。我们注意到，IEEE帧中不包含类型字段，因为它的功能是由LLC的SAP地址提供的。

802.3帧的长度字段给出数据的长度。如果该长度需要传送给以太网中的接收机，那么高

层协议必须负责处理这一过程。同时，在以太网中，高层必须确保数据字段长度至少为46个字节，而在IEEE帧中，MAC层会在需要时填充补充比特。

所有有效帧长都小于十进制的1500或十六进制的05DC，所有有效类型字段值都大于这个值。因此，当一帧被一个节点接收到时，源地址后的两字节就会被检查。如果它们大于05DC，则该帧就被理解为一个以太网的帧，否则就是一个802.3的帧。

如果源地址字段之后的两个字节小于或等于05DC，则检查后一个字节。如果其值为AA，则被解释为带有SNAP的802.3帧，否则被认为是不带SNAP的802.3帧。旧版本的802.3不使用SNAP，所以SAP字段指示出正在被传输的数据字段所使用的协议。注意到SAP字段的值与802.3帧不同。然而，带有SNAP的802.3使用与以太网相同的类型字段，同样也存在很多具有这种格式的类型代码。因此，我们将IEEE 802.3标准和纯的以太网标准简称为以太网。

23.2.2　10Base5

以太网的各种类型称为：10Base5、10Base2、10Broad36、10BaseT等等。第一个数字（10）代表在媒质中以Mbps为单位的传输速度，最后一个数字代表以100m为单位的最大单段传输距离。Base和Broad表示使用基带信令还是宽带信令，这些差别在第4章讨论过。现在我们来介绍被称为标准以太网的10Base5，它是使用单段最大长度为500m以10Mbps传输的以太网的最初标准，它使用基带电缆系统。

这种以太网的组成如图23-8所示，主电缆或总线使用RG-4（无线4级）同轴电缆，该电缆的特性阻抗为50Ω。在主电缆上有相距2.5m及其整数倍的AUI（Attachment Unit Interface，附属单元接口），它们也被称为MAU（Media Access Unit，媒体接入单元）或收发器。一段上的最大抽头数量为100，这些AUI使用冲孔吸附式（piercing vampire）或直插式BNC型连接器相连。

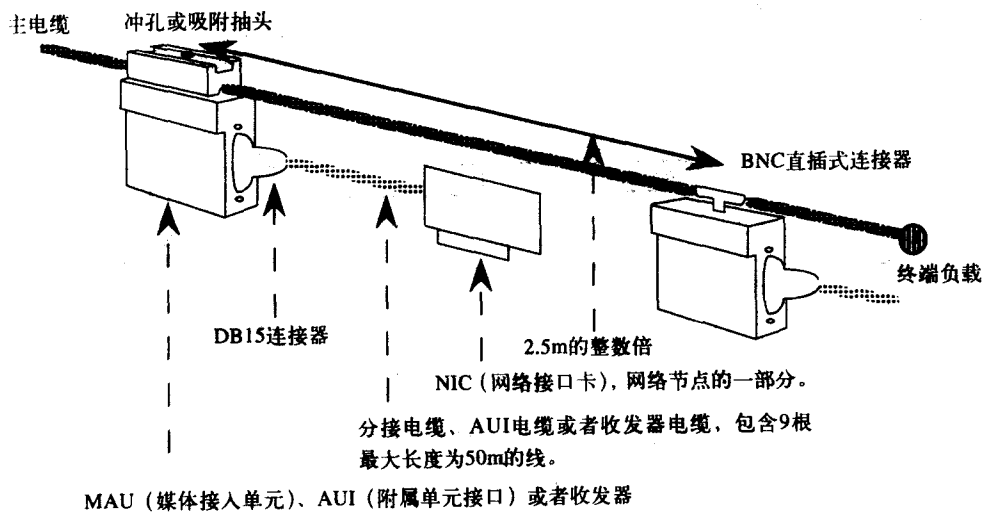


图23-8　10 Base5（标准）以太网的组件

工作站从AUI通过一根AUI电缆（也称为分接电缆）进行连接。它不是同轴电缆，而是9线电缆。其最大长度为50m，一端通过DB15连接器与收发器相连，另一端与工作站内部的NIC相连。主同轴电缆两端必须接50Ω的终端负载，并且其中一个应该接地。

收发器提供多项功能，它能够检测电缆上是否有信号以及电缆是否可用于传输。如果可

用，AUI就会发送信号；如果探测到冲突就会停止传输。当某个终端不停地发送（或者超时）时，收发器就会终止其发送，并将通信机会留给其他节点。最后，AUI向终端发出心跳信号，指出它已启动，并可进行操作。

当电缆上主机太多或者主电缆长度超过500m的最大长度而使性能开始下降时，可以添加其他段来扩展网络，这是通过在各段之间连接中继器来完成的。中继器并不能消除位于不同段的工作站之间的冲突，它们只能扩展LAN的覆盖范围。第24章我们将看到网桥和路由器如何将各段的流量进行隔离。

在网络的任何两个节点之间，中继器的最大数量为4个。在图23-9的右边给出一个采用垂直主干网的多层建筑网络，各层网段都使用中继器与主干网相连。注意，任何两层的节点只能使用两个中继器彼此通信。在图左边是与该LAN相连的校园的一部分，通常情况下，为了得到更高质量的信号，像这种距离的连接最好采用光纤。这里，一幢建筑中的任何工作站最多可以使用3个中继器与其他建筑中的另一个工作站进行通信。

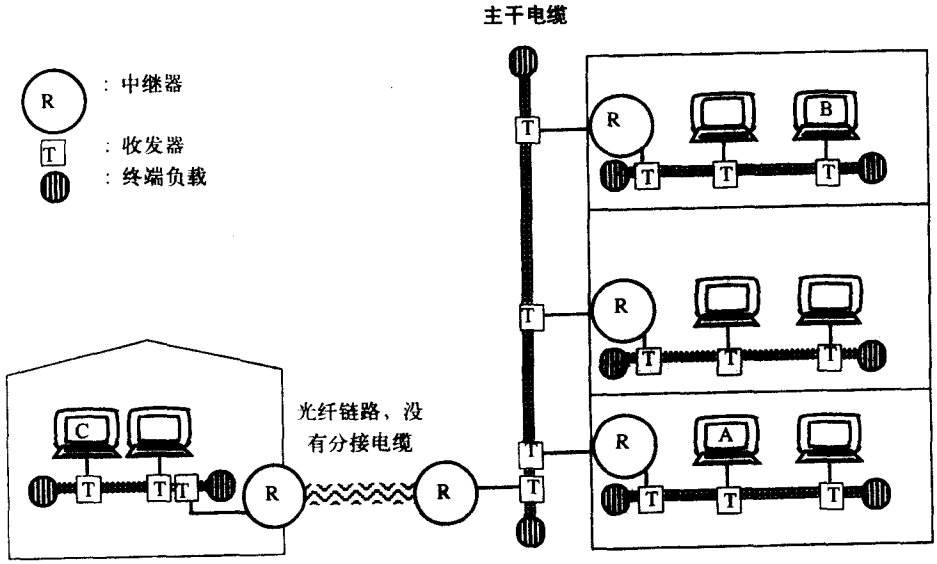


图23-9 利用中继器可将以太网的覆盖范围从500m扩展到2500m

23.2.3 10Base2

1985年，一种成本较低的以太网版本被标准化为10Base2。由于使用了容易安装的细同轴电缆，因此它又被称为ThinNet或CheaperNet。该版本仍然使用基带信令技术，与10Base5有许多相同的特点。然而，10Base2有更多的距离和节点放置限制。

图23-10给出了在通常情况下，NIC是如何不使用AUI电缆而直接与主同轴电缆相连的。NIC提供BNC连接器和收发器电路。将NIC连接到主电缆上很简单，无需穿过同轴电缆，而且每个节点的成本也比10Base5低很多。除此之外，名为RG-58的电缆只有0.25in厚，这使得它不仅价格低廉而且便于携带安装。

遗憾的是，10Base2也有局限性，其最大段长度仅有185m，节点之间间隔0.5m，并且单段最多30个抽头。包括中继器在内，每个网络中的最大节点数为1024，这一数字与10BaseT和10Base5的相同。但是，采用中继器的最大网络长度仅为925m，而10Base5则为2500m。

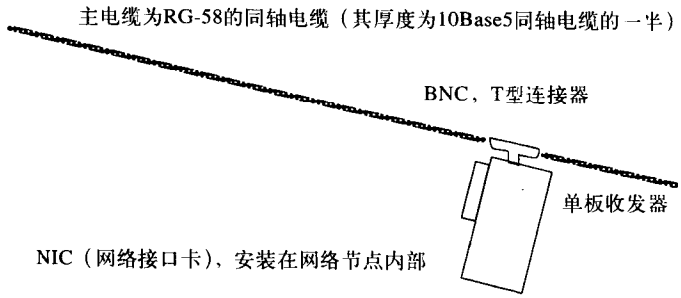


图23-10　10Base2硬件

23.2.4　10BaseT

产生：由于ThinNet成本低并且易于安装，因此它很快变得比标准以太网还普遍。正是因为它的迅速成功，一种新型的更加廉价和容易安装的以太网产生了，它就是10BaseT。

10BaseT使用标准的24 AWG电话线代替同轴电缆。通常情况下，多数建筑物都装有这种电话线，从而使得安装很方便。而且，10BaseT能够与其他类型的以太网共存，使其易于扩展网络而不需代替旧的技术。

最初，10BaseT是由Synoptics（Xerox Palo Alto研究中心的一个分支）开发的，作为UTP（Unshielded Twisted Pair，非屏蔽双绞线）上运行的以太网，并于1990年被IEEE采纳作为一个标准。

以集线器为中心的LAN：在网络的中心是一个集线器。当它置于一个可以添加其他扩展模块的底板上时也被称为集中器。从集线器出来的（参见图23-11）是标准的50线电话电缆，该电缆又与一个旧的M-66型穿孔（punch-down）模块相连，这可以使用标准的50引脚RJ-21连接器来实现。从穿孔模块出来采用与电话电路相同的布线方式。

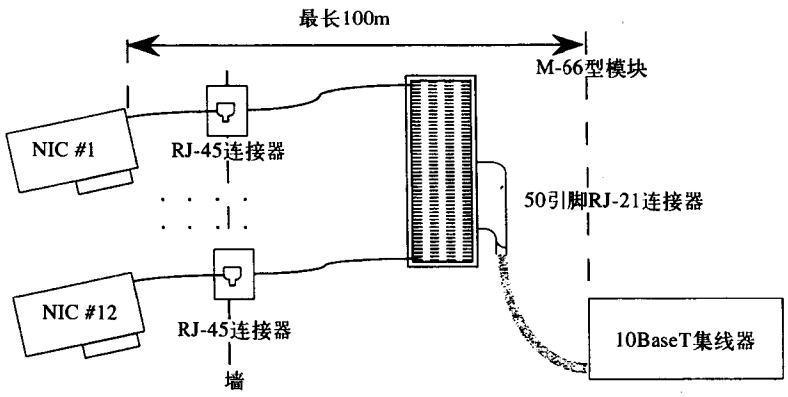


图23-11　10BaseT可以用50线电话电缆中的48条线连接到穿孔模块，从这里，可以为多达12个网络节点提供连接，各节点需要4条线

从模块出来的电路通常连接到一个墙上的连接器，从那里使用标准的RJ-45连接器和电话线，就可以建立与NIC的连接。在RJ-45的8个引脚中，有2个用于发送，2个用于接收，4个未用。由于每台工作站只使用4根线，因此从集线器引出的一个50线电缆可以支持多达12台工作站。

注意，这种星型总线拓扑与其他类型以太网的拓扑有很大不同，但是，与其他以太网一

样，它仍然使用相同的帧结构和CSMA/CD（带有冲突检测的载波帧听多址接入）媒体接入方法。冲突出现在集线器内部的总线上，当一台工作站发送数据时，信号就会到达集线器，被转发之后，将在所有端口被重新发送，这就是为什么集线器又被称为多端口中继器的原因。

集线器通过发送测试信号不断地监督各个支路上的工作站，允许响应该测试信号的支路与其他支路进行通信，而那些没有响应的支路则被集线器关闭。集线器各端口上的状态指示灯表示哪些端口处于工作状态，而哪些端口没有处于工作状态。当一个老式的不能对这个链路完整性测试信号做出响应的以太网适配器连接到端口上时，其链路测试可以人工关闭。这就允许现有的以太网与集线器相连。一般情况下，NIC还会点亮一个LED，以表示链路完整性测试信号的存在。该指示灯证明NIC在与另一端的集线器连接正确，但不能说明噪声电平对正确的数据传输是可以接受的。

有时采用10Base2，用户拔掉背后的T型连接器就可以移动工作站。由于总线从此连接器通过，这一操作将无意中破坏网络，这是因为抽头被非正常地终结。

另一方面，在10BaseT网络中，如果一台工作站或其链路发生故障，那么网络其他部分是不会受到影响的，这是因为集线器将关闭损坏的节点，因为它们不能通过链路测试。这称为隔离端口。当集线器隔离一个被损坏的端口之后，它还会不断地测试该端口看它是否被修复。当链路或其端口确实被修复后，由于集线器在不断地测试该链路，因此会注意到这一变化，会将其自动恢复。

超时传输就是传输过长的帧。如果在网络中发生这种情况，集线器很容易检测到是哪一个节点并将其隔离。这在其他以太网上并不是那么容易的。集线器同时可以充当网络监视设备，为各端口提供全天候的错误和冲突统计。这种数据可以从远端获得并由软件包生成一个易读的报告。

由于集线器提供了一种更好的网络管理与控制方法，因此使它具有很强的吸引力，并成为网络的一个重要部件。但选择和购买集线器时必须小心，因为整个网络的可靠性在很大程度上取决于集线器。

扩展的第一阶段：图23-12a给出了图23-9中的标准以太网LAN是如何扩展为包括10BaseT的，图23-12b给出了该网络扩展的第二阶段。在图23-12a中，一个拥有20台工作站的新LAN加到某层，并通过AUI电缆与10Base5主干网相连。我们先来看看这个20台工作站的LAN。

假设我们决定使用12端口集线器组成10BaseT LAN，这样就至少需要两个集线器才能容纳20台工作站。将这两个集线器的一个端口连接在一起，就得到级联的集线器。然而，这两个端口的发送对和接收对必须交叉，这需要使用电缆或者加一个开关。这样就只剩下22个端口来连接工作站。

我们已经说过集线器类似于一个中继器，因为它将从一个端口接收到的信号重新发送到其余端口。所以，IEEE规定在网络中的任何两个节点之间，信号最多经过4个集线器。我们可以很容易地发现，当将一组集线器级联在一起时，即呈菊花链拓扑，此时可用端口数要比使用树型拓扑时少很多。

为了将拥有20个节点的10BaseT LAN连接到现有的10Base5主干网上，我们就很简单地将其中一个集线器连接到主干网上。这是通过使用从集线器到主干网上的收发器的AUI电缆来完成的。

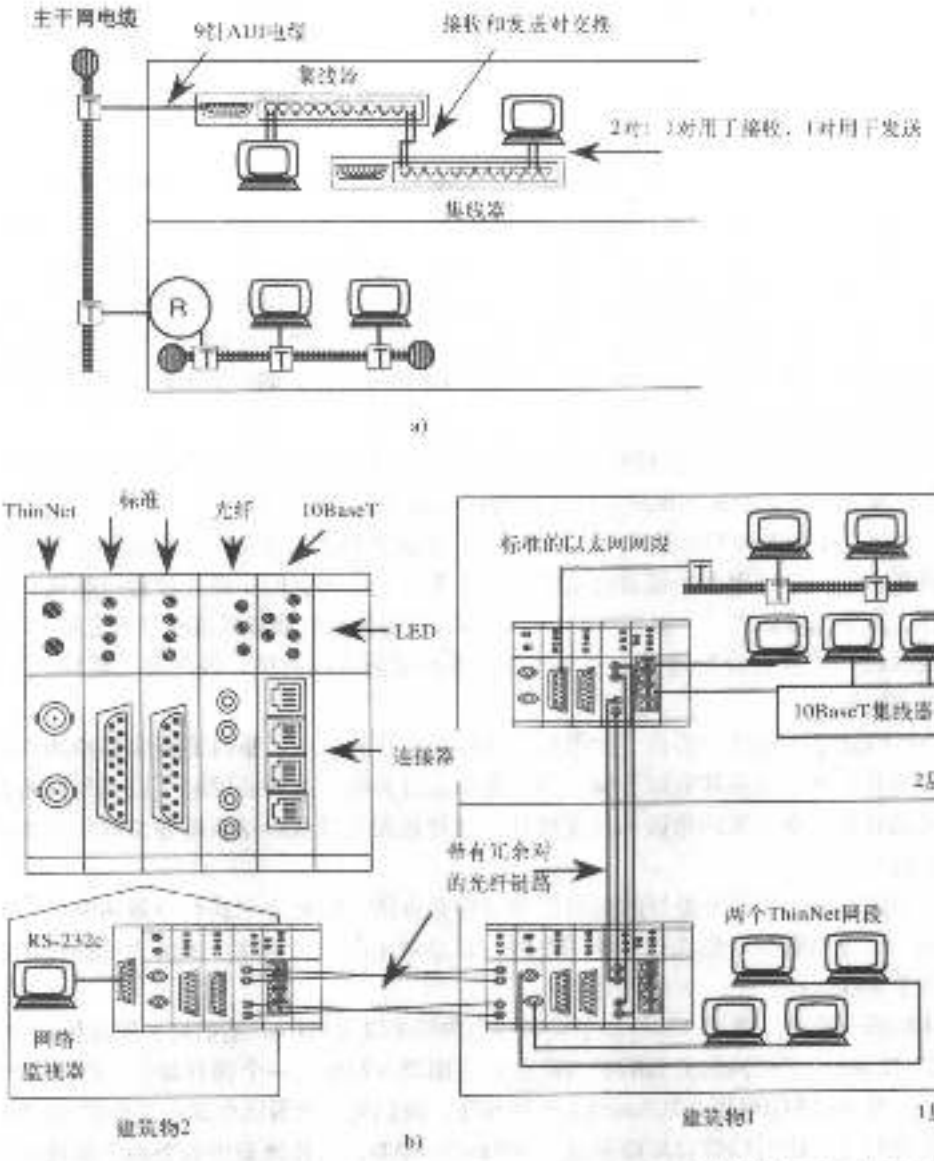


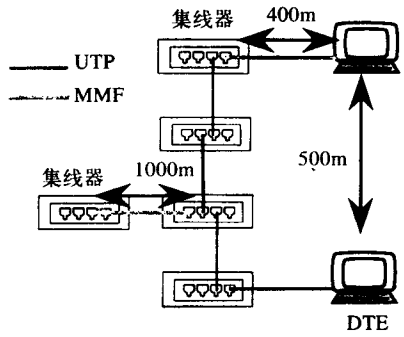
图23-12　a) 扩展图23-9中的网络以容纳多达20台10BaseT工作站。b) 用集中器在各层安装光纤主干网。以太网集中器如插图所示。各种类型以太网的不同模块可以根据需要插入到底板。一般而言，在各层与建筑物之间采用光纤。其发送对和接收对绞在一起，因为这是必需的

扩展的第二阶段：当更多新的和现存的LAN要融合到网络中时，可以在每一层都增加集中器（也称为集线器），如图23-12b所示的网络扩展的第二阶段。这里，旧的同轴线主干网被去掉，集中器使用光纤相互连接起来。这经常安装成冗余双环路对。

根据各层现有网络的类型，将集中器的底板用合适的模块进行装配。虽然图中所有集中器都以同样的方式配置，但这并不是必需的。当需求发生变化时，集中器允许即插即用。最后，我们加入一个监视器执行对网络的管理功能。随着需求的持续增长，我们可以在底板加入网桥和路由器。

23.2.5 10BaseF

1987年，FOIRL（Fiber Optic Inter-Repeater Link，光纤中继器间链路）被标准化，成为利用光纤进行以太网中继器互连的标准；这有助于增加中继器之间的距离。1993年，IEEE将基于FOIRL的10BaseF标准化。10BaseF典型情况下使用直径为62.5/125μ的MMF（Multi Mode Fiber，多模光纤）来安装。通常，一根纤用于发送，一根纤用于接收。光纤用LED供电并使用在第4章介绍的ST连接器。



10BaseFL的最大距离

10BaseF有三种“风格”：10BaseFL、10BaseFB和10BaseFP，其中10BaseFL占统治地位。在10BaseFL中，集线器与NIC之间的最大距离是400m，中继器之间的距离是1000m，交换机之间的距离是2000m。在使用多达4个中继器和任何种类电缆的两个节点之间，最大距离是500m，如侧图所示。

23.3 令牌环网络

23.3.1 基本配置

TRN（Token-Ring Networks，令牌环网络）在一个环形拓扑上使用令牌接入控制方法。正如集线器在10BaseT网络中提供强大的管理能力一样，TRN使用有线集中器达到同样的目的。有线集中器又称为MAU（Multistation Access Unit，多站点接入单元），这一缩写不要和10Base5中的收发器MAU相混淆，它代表媒体接入单元。

如图23-13a所示，TRN的MAU通常为8台工作站提供连接。图中给出了1类数据级电缆，它是一种STP（Shielded Twisted Pair，屏蔽双绞线对），包括两个屏蔽在内部的22-AWG双绞线对。屏蔽可以抵抗电磁干扰。该电缆的连接器没有方向性，并可以直接连接。电缆使用DB9插头与工作站相连。

很多时候，标准电话UTP（Unshielded Twisted Pair，非屏蔽双绞线）电缆也用来连接工作站和MAU，称为3类电缆连接。它在MAU和NIC都使用RJ-45连接器。由于这种电缆按话音分级，因此它比1类电缆有更严格的距离限制。

从物理上看，TRN像一个星型，但逻辑上却是一个环。如图23-13b所示，当数据从一个节点传向另一节点时，它必须首先经过MAU。所以，TRN被称作一个星型连接的环。与此相似，10BaseT被称为星型连接的总线。从NIC到MAU的连接称为一个分支（lobe）。TRN运行速度为4Mbps或16Mbps；但是要以更高的速度运行，所有NIC都必须设为16Mbps。

当一台工作站连接到MAU上并加电时，它会在电缆上产生一个5 VDC的幻像电压。该电压向后拉动MAU的连接器上的继电器，使该节点成为环的一部分，如图23-13b端口3、4、7所示。如果由于某种原因，工作站的NIC不能给MAU端口提供这个电压，则MAU就会将那个节点从环上脱离出去。这可能是由于工作站被关闭（如图中端口1）、误操作（如图中端口5）或由于电缆断开所造成的。

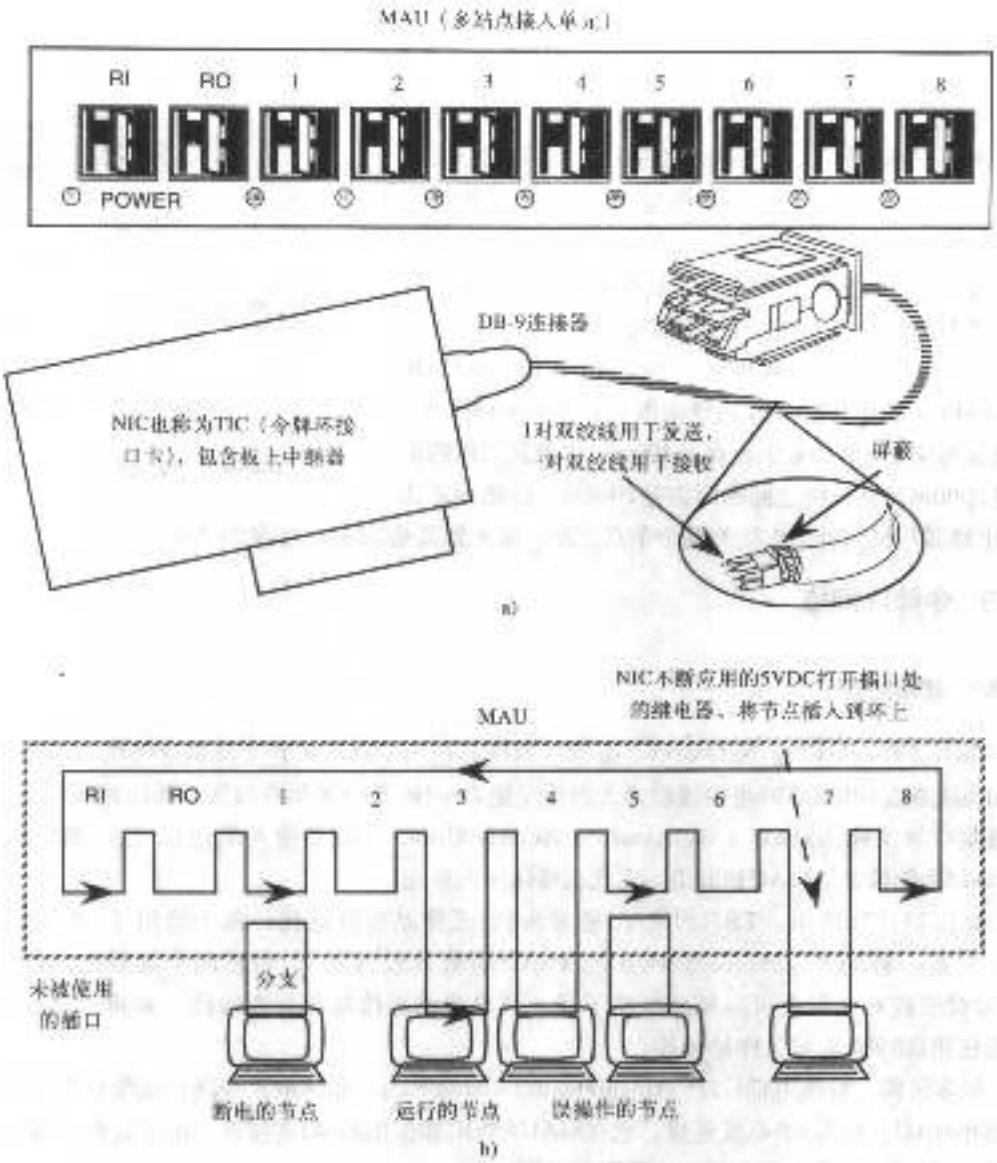


图23-13　a) MAU与1类连接器和STP（Shielded Twisted Pair，屏蔽双绞线对）。
b) MAU及其工作站成为星型环网络

23.3.2　扩展TRN

图23-14a给出了TRN如何很容易地扩展到8台工作站以上。这可以简单地通过在它们自己的环上添加几个MAU再将工作站连接到MAU上来实现。通过连接MAU所形成的环称为主环。将电缆从一个MAU的RI（Ring In，环入）端口连接到另一个MAU的RO（Ring Out，环出）端口就会将MAU连接到环内。主环上的所有MAU可以置于一个机柜上，或者放在不同的配线间里。图中底端的两个在一个配线间里，顶端的一个在另一个配线间里。

注意到现在所有节点都成为环的一部分。各节点都充当一个中继器。因此，对于4Mbps网络而言，分支的最大长度是300m，而以太网中整个网段的最大距离是500m。各配线间之间

的最大距离是200m。若在它们的连接链路各端设置一对中继器，则可将该距离扩展到730m。若使用光纤，这一范围甚至可以扩展到3000m。

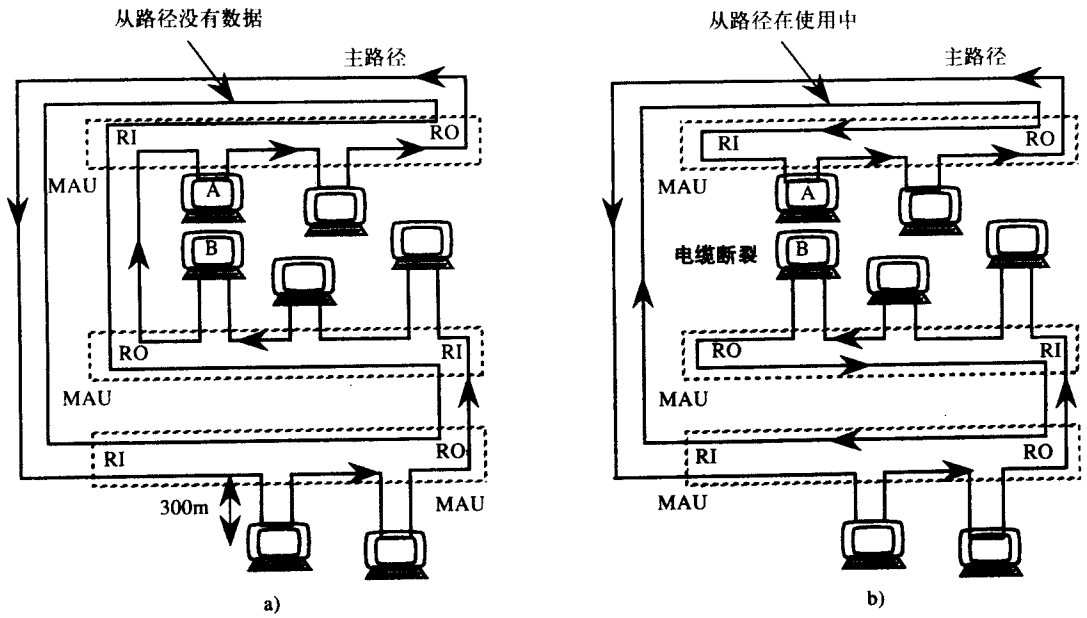


图23-14 a) 底端的两个MAU在一个配线间里，顶端的一个MAU在另一个配线间里。它们都利用RI和RO端口相互连接。b) 如果配线间之间的一根电缆出现故障，则使用备用路径可以恢复这个环

有时只有一个分支（lobe）需要扩展，在这种情况下，只用一个中继器就可以将其范围从300m扩展到610m。MAU和工作站的最大数量分别为33和260。当网络变得更大时，必须将网络划分成通过网桥相互连接的较小的网络。上述所有规定都是使用1类电缆连接的4Mbps网络的最大值。如果采用16Mbps的速度或者使用UTP电缆，那么随着网络的增大这些限制将变得更加严格。

注意在图23-14a中，当信号从一个节点传到另一节点时，只使用了外部路径，而没有使用内部路径，内部路径只是作为备用。每一台工作站都有NAUN（Nearest Active Upstream Neighbor，最近有效上行流邻居），就是它接收信号的节点，例如图中的B是A的NAUN，因为A从B接收信号。

如果电缆在两个MAU之间断裂，如图23-14b所示，我们可以在两端去掉该连接电缆，环通过备用路径可以自行恢复。在一些智能MAU中，修复是自动完成的。这里，即使信号经过其他所有节点，但B仍然是A的NAUN。

23.3.3 活动监视器

当网络第一次上电运行时，节点彼此发送MAC帧以决定自己的NAUN。在此期间，它们还要分配NIC，通常将拥有最高地址的NIC作为活动监视器。这个特殊的“网络监督员”为所有工作站提供同步。它同时会在其移位寄存器中缓冲24比特，目的是为了让一个长度为24比特的完整令牌能适配到环上。当环非常小时，这个缓存很有必要。

一旦活动监视器被选定，它通过清除环并产生一个新的令牌来初始化这个环。如果它在每10毫秒间隔内没有检测到环上有任何活动，或者发现高优先级的令牌或帧在环上循环超过

一次，也会进行这样的初始化。令牌或帧每次出现时，将其监视比特置1，这样就可以检测到这类令牌或帧。发送令牌或帧的工作站将其监视比特置为0，如果活动监视器发现此位已被置位，就重新启动该环。而且，活动监视器还向所有节点广播其仍然处于控制地位，否则备用监视器就会取而代之控制网络。

23.3.4 信号编码

以太网使用曼彻斯特编码发送数字信号，其优点是每一比特都会出现一个由高到低或由低到高的电平跳变，有利于接收机保持同步。图23-15a给出了这种编码方法，二进制的1总是一个由低到高的电平跳变，而0则恰好相反。

另一方面，TRN使用差分曼彻斯特编码，这就要求二进制的1从前一个比特结束时的相同电平开始。换言之，在1的开始处没有电平跳变，而在0开始处有一个电平跳变，参见图23-15b。

除了提供对数据比特1和0的编码方法外，TRN同时还使用了两个非数据比特J和K。这些比特都是差分曼彻斯特码的扰码（violation），因为它们不会出现中点电平跳变。如图23-15c所示，J的信号电平与前一比特相同，而K却不是。

既然现在是讲信号编码方法，下面就看看FDDI是如何处理信号编码的。FDDI使用NRZI（NonReturn to Zero with Invert on ls，非归零1倒转）编码方法。这里0和1都以与前一比特结束时相同的电平开始。然而，二进制的0不包含电平跳变，二进制1则包含电平跳变。由于这一原因，FDDI数据流中有最大数目的连续0，并且越向后越多。

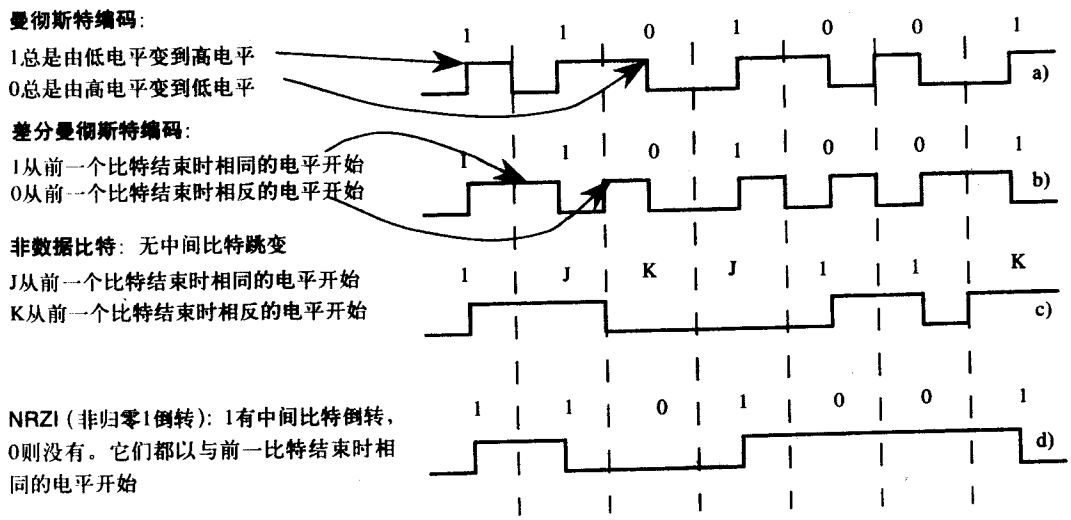
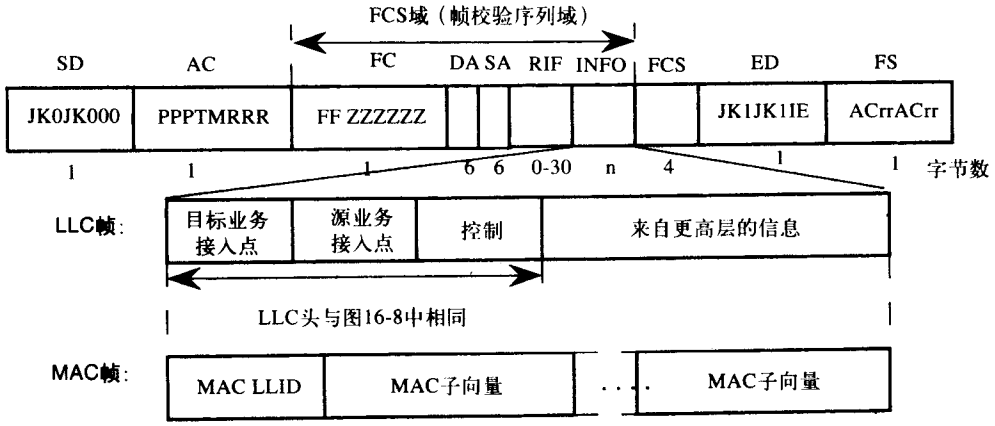


图23-15　令牌环网络所采用的曼彻斯特编码、差分曼彻斯特编码以及非数据比特

23.3.5 TRN帧结构

MAC 帧：由图23-16可见，TRN的帧结构比以太网的更加复杂，但它有更多特点。TRN帧分为两大类：LLC（Logical Link Control，逻辑链路控制）帧和MAC（Medium Access Control，媒体接入控制）帧。LLC帧用于发送用户数据，它的头结构和图23-6所示相同；MAC帧用来传输管理和控制帧。



SD：起始分界符
AC：接入控制
FC：帧控制
DA：目的地址
SA：源地址
RIF：路由信息字段
P：优先级比特
T：令牌比特
M：监视计数
F：帧格式（LLC或MAC）

FCS：帧校验序列
FS：帧状态
DSAP：目标业务接入点
SSAP：源业务接入点
MAC：媒体接入控制
LLC：逻辑链路控制
LLID：MAC长度ID
R：预留比特
A：被识别的地址
C：被复制的帧

图23-16 令牌环网络的帧格式。如果FF＝01，则该帧为LLC帧；如果FF＝00，则该帧为MAC帧

在FC（Frame Control，帧控制）字段中的FF（Frame Format，帧格式）比特表明该帧是LLC帧还是MAC帧。Z比特主要用来编码各种不同类型的MAC帧，例如这可以成为所有工作站清除环的信号，或者通知它们监视器仍然存在。信标也在这里进行编码。信标MAC帧由一个在一段时间内没有接收到来自其NAUN信号的节点发出，这可能是由于电缆断裂造成的。当此帧到达它的NAUN时，它会将自己从环上断开以执行分支（lobe）测试。如果测试失败，它将保持断开，否则发出信标的工作站将进行自检。

图23-16给出了MAC帧的结构。由图可见，它有自己的头，称为LLID（MAC长度ID），其后是一组称为子向量的字段。读者没有必要研究这些字段的细节。

一般帧格式：所有的帧以编码的SD（Starting Delimiter，起始分界符）开始，如图23-16中的“JK0JK000”。该字段仅仅标志一帧的开始。与此类似，倒数第二个字节是ED（Ending Delimiter，结束分界符），编码为“JK1JK1”，再加上一个I（Intermediate frame，中间帧）比特和一个E（Error detected，检错）比特。

I比特虽然很少使用，但是如果目前帧后还有更多的帧要发送，则该比特将被置为1。如果某帧在通过一个节点时被检测出错误，它的E比特就会被环上任何节点置位。因此，帧在环上传输时，错误检测是由每个NIC完成的。各节点记录其对E比特进行置位的频率，这样就很容易检测出容易出错的链路。

在SD字段之后是AC（Access Control，接入控制）字段，该字段包含M（Monitor count，监视计数）比特。正如我们已经看到的，它被监视器用来检测那些不止一次通过环的高优先级帧和令牌。它还包含令牌位，设为1代表帧，设为0代表令牌。令牌仅由SD、AC和ED字段组成，总计24比特。

在AC字段内还有PPP（优先级）比特和RRR（预留）比特。令牌可以包含从0到7的一个

优先级，并且当令牌到达一个有数据要发送的节点时，它就会取消令牌并发送数据。这只有当待发送数据的优先级大于或等于令牌中所给出的优先级时才会发生。如果不是上述这种情况，只要令牌或帧中的预留比特不超过所请求的优先级，该节点就会将预留比特置位，以预留令牌的下一次可用机会。后面我们用一个例子进一步说明这些字段。

SA和DA（Source and Destination Address，源和目的地址）字段与802.3以太网的地址字段类似。然而，经常使用源路由网桥将TRN互连起来。在这种情况下，RIF（Routing Information Field，路由信息字段）用来编码网桥的地址。为了在一帧内使用RIF字段，SA的最低位必须置为1，也就是I/G位必须置为1。当DA和SA不在同一个环时，RIF以帧所经过的网桥顺序来包含网桥地址。由于将环互连起来的网桥无需决定路由，因此使得源路由效率很高。但是，发送节点必须首先寻找路由才能编码RIF。

FCS（Frame Check Sequence，帧校验序列）字段用来检错。FS（Frame Status，帧状态）字段包含C（Copy，复制）和A（Address recognized，地址识别）比特。由于这些比特没有累积到FCS中，因此它们被复制。C和A比特均被发射机置为0，r比特目前还未被使用。

A比特被接收机置位，E比特被除发射机外的任何节点置位。接收节点通过将A比特置为1来确认其明白该帧是给它的。如果接收机发现E比特为0并且FCS校验无误（checks out），它就将数据复制到缓存中并将C比特置1。

23.3.6 操作实例

下面来看图23-17，该图说明了关于TRN的一些概念。在环上有4台工作站，其中工作站40为活动监视器。帧和令牌向右移动，之后向下进入到下面一行。它们在离开各自的节点时被表示出来，如果保持不变就不会被表示出来。当引入新概念时，仅显示必需的字段，这样就可以更好地突出它们。图中的小方框为令牌（T=0），大方框为帧（T=1）。需要注意的是DA、A和C这几个字段均不是令牌的一部分。

E、A和C比特：最初，节点40给节点10发送令牌，节点10没有数据需要发送，于是就将该令牌延着环向下传。工作站20得到令牌并向节点10发送一帧，将E、A和C比特置为0。该帧在环中传输直至到达节点10，节点10复制该帧并将A和C比特置为1，表明它知道该帧是发给它的并且已经正确无误地复制。之后，节点20收到返回的这一帧并产生一个新的令牌，从而使其他节点有机会发送。

在图中的第3行，节点10发送一帧给节点30。但当帧经过节点20时，检测到FCS字段中有错误并将E比特置1。于是节点30确认它明白该帧是发给它的，但要通过将C比特置为0来指示出错。该帧在第4行传回节点10，并被重新发送，于是节点30得到无错帧，此帧在第5行到达节点10。

P和R比特：当此帧在回到节点10时，节点40通过将R比特置为2以优先级2预定令牌。于是节点20发送一个P为2的令牌，防止其他低优先级的节点在节点40得到该令牌之前捕获此令牌。在第6行，节点40将其紧急数据帧发送给节点20，之后返回到节点40，这时节点40在第7行发出一个优先级为2的令牌，节点10接收到该优先级令牌。

将令牌优先级升高的工作站必须将其恢复为原优先级，所以节点10一接收到这个有优先级的令牌之后，就会立刻发出一个优先级为0的令牌。接着，节点20发送一帧，而节点30在第7行末尾以优先级2预定一个令牌。

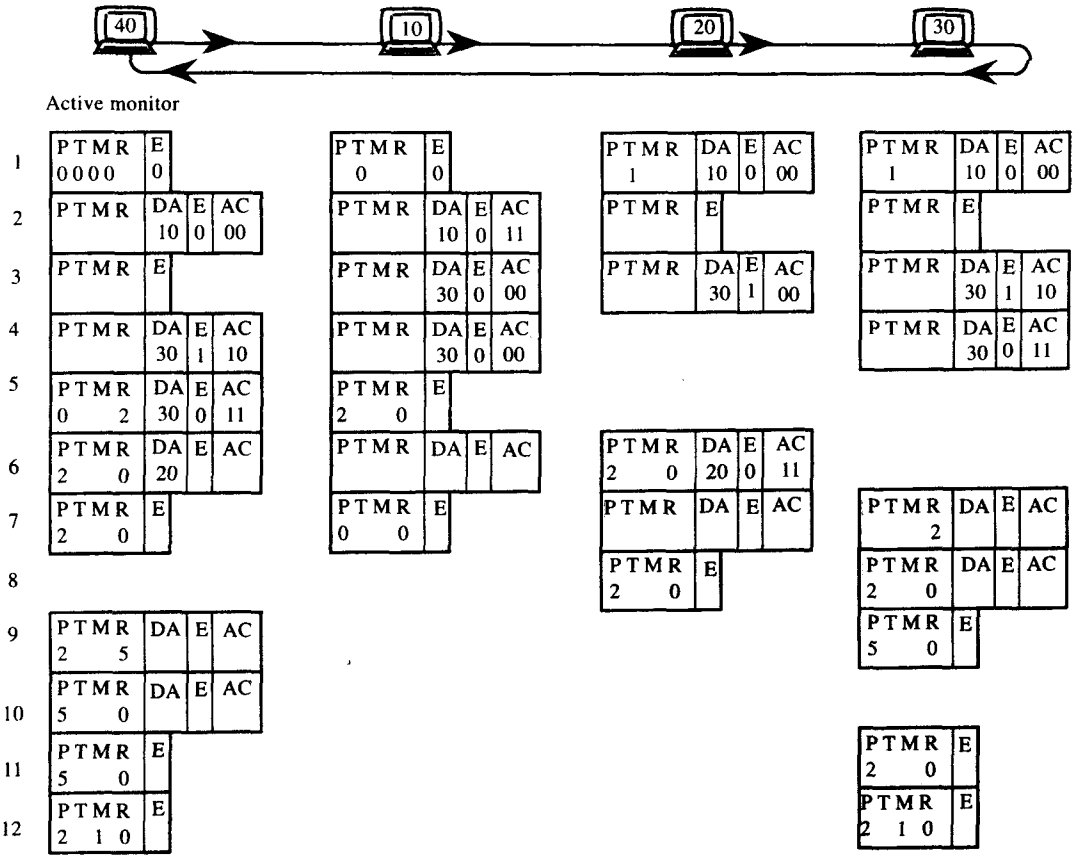


图23-17 帧（大方框）和令牌（小方框）绕环向右循环。如果未被节点所改变，那么就不会被该节点提取。图中仅给出了理解所述概念所必需的值，从而防止不必要的信息造成该图混乱

进一步提高优先级：由于节点20在第8行接到一个R为2的令牌，因此它会发送一个P为2的令牌。这就允许节点30以更高优先级发送数据。当节点30发送数据时，节点40以优先级5预定令牌（第9行开始）。节点30以P为5发出一个令牌，这就允许节点40以P=5发送帧。在第11行，节点40发出P=5的一个令牌，被节点30接收到，节点30想起自己将优先级从2升到5，所以又将其降到2。最后，优先级为2的令牌将到达节点20，节点20本应将优先级降为0，但它断开了自己。

M比特：活动监视器在第12行将优先令牌的M比特置为1，由于节点20不能将优先级降低，因此这个令牌会返回到活动监视器，它看到M比特在13行仍然是1，于是清除环并重新初始化该环。

23.4 FDDI

23.4.1 一个基于层的标准

FDDI（Fiber Distributed Data Interface，光纤分布式数据接口）最初是由ANSI的X3T9.5工作组定义的一个高容量LAN标准。该标准运行在100Mbps并与以太网和其他LAN标准互补共存。虽然基于铜线的FDDI也已定义，但我们仅讨论基于光纤的标准。

图23-18表示出FDDI怎样适配到IEEE的802家族标准中，在最底层PMD（Physical Medium Dependent，物理介质相关层协议）负责电缆、连接器及其相关设备。

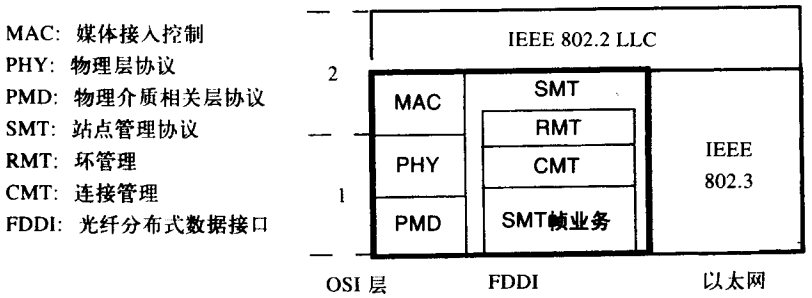


图23-18　FDDI标准在IEEE的LAN家族标准中的位置

PHY（PHYsical layer protocol，物理层协议）定义了时钟、编码、如何产生称为符号的信号和其他一些功能。PMD层与PHY层共同组成了OSI的第一层。在PHY层之上是MAC（Media Access Control，媒体接入控制）层，它负责环的初始化、令牌管理、成帧和寻址等功能。最后，为所有上述层服务的SMT（Station ManagemenT，站点管理协议）标准为连接和环提供管理和监视服务。SMT又进一步划分为图23-18所示的几个部分。

23.4.2　PMD层

共有4种类型的PMD：第一种称为简单PMD，它在多模光纤上使用LED；SMF-PMD使用单模光纤和激光；LCF-PMD在低成本多模光纤上使用LED；最后TP-PMD将STP和某些种类的UTP标准化。

FDDI使用两个反向旋转的环，这使它具有很高的可靠性。连接到两个环上的设备称为双附件设备，只连到一个主环上的设备称为单附件设备。另外，将其他设备连接到主环上的设备称为集中器，而那些实际使用网络的设备如主机称为站点（station）。将这些分类结合起来，FDDI设备就可以定义为：SAS（Single-Attached Station，单附件站点）、DAS（Dual-Attached Station，双附件站点）、SAC（Single-Attached Concentrator，单附件集中器）和DAC（Dual-Attached Concentrator，双附件集中器）。比如：一个DAS与两个环相连接，并不为其他设备提供直接的FDDI环连接；而SAC仅与FDDI主环相连，可以为其他设备提供环连接。

图23-19给出了一个FDDI网络树型配置的两个环。注意到除1号建筑中的DAS被用作一个SAS外，其余双附件设备是两个环的组成部分。无论是DAS还是SAS站点都不为其他设备提供连接的接口；而不论单附件集中器还是双附件集中器均提供这种接口。

与TRN相同，当连接两个MAU的电缆出现故障时，环能够自愈。必要时FDDI可以使环绕回（wrap around），同时也可以在光纤和设备连接处安装光纤旁路中继。如果设备发生故障，环仍然不会受损；因为光信号可以旁路那个设备，但是由于信号不会经过中继再生，因此两个站点之间的新距离可能超过最大允许限制。

由于双附件设备连到两个环上，因此它们不会经常从环上断开。将这类设备从环上断开将导致环的缠绕，而将两个这类设备从环上断开就可能导致整个环的瘫痪。服务器、网桥和路由器中的双附件适配器，可以为设备提供一个与集中器相连的热链路以及与另一个集中器相连的备用链路，这样如果一个集中器断开，备用链路就开始工作，这称为“双归宿”。

MIC（Media Interface Connector，媒体接口连接器）用来将多模光纤与站点或集中器相连。图23-19中有四种连接器，它们以这种方式出现使得网络不会发生配置错误。

SAS：单附件站点
DAS：双附件站点
SAC：单附件集中器
DAC：双附件集中器

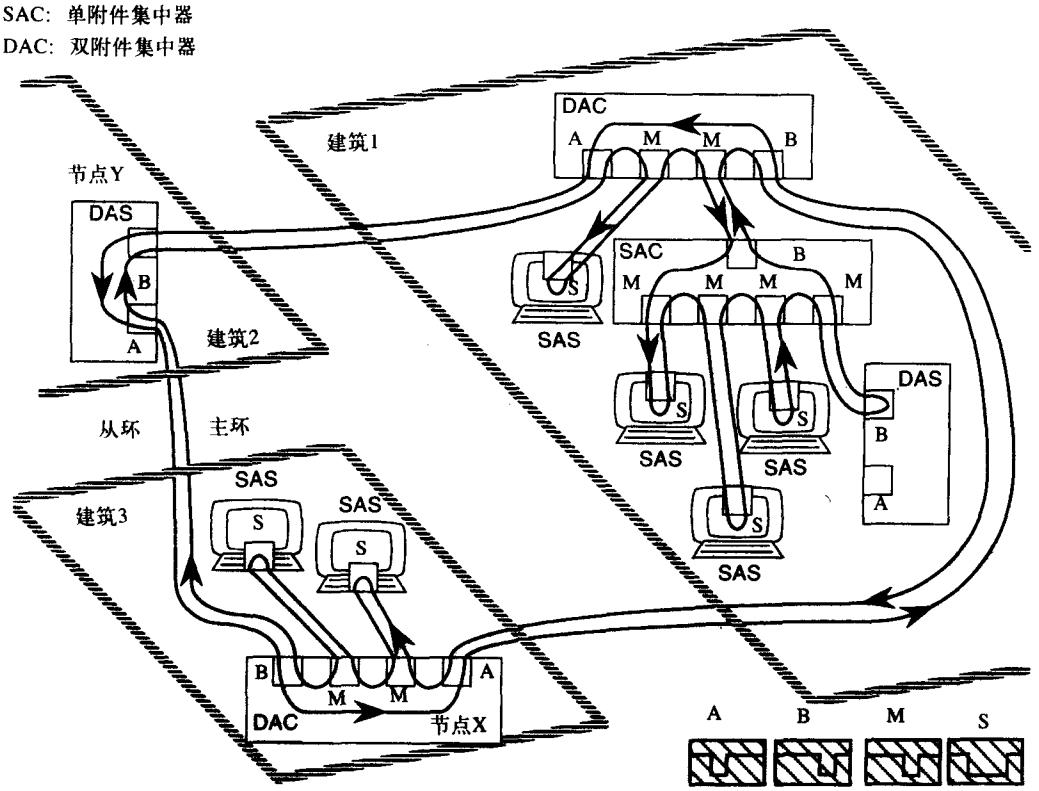


图23-19 FDDI的从环不经过单附件设备。DAS可以是小型计算机。在该图下方，画出了四种类型的MIC（媒体接口连接器）。SAC及其站点可以位于1号建筑旁的另一栋建筑

MIC A（即端口A）用来连接DAS或DAC的主环的输入端口和从环的输出端口。在图中找到A类MIC，注意上述特点。端口B（即MIC B）与之互补。端口M仅通过主环将一个集中器连接到另一个集中器或者站点。端口S将SAS连接到集中器上。

23.4.3 PHY标准

采用高速运行的FDDI必须保持时钟同步。如图23-15所示的FDDI使用NRZI（NonReturn to Zero with Invert on ones，非归零1翻转）编码，这种编码只为二进制1提供电平跳变，这种跳变对于保持时钟同步是必要的。为了保证接收端的很好同步，FDDI不允许发送三个以上的连续0。为了确保满足这一规则，PHY标准将每个4个数据比特（称为符号）的数据组转换为至少包含两个1的一个5比特码组，这称为4B/5B符号编码方法。

例如，当发送数据符号“0000”时，它首先被变换为“11110”码组。表23-1给出了数据的4比特码组是如何转换为5比特码组的。我们注意到任一对有效符号中都不存在3个以上的连续0。产生3个以上连0的码字是不会被实现的并且是无效的。因为我们通过加入额外的1来帮助接收机保持同步，所以就必须将FDDI设备的时钟频率增加到125Mbps，这样才能保证数据以100Mbps的速度发送。

表23-1　符号的码组分配

码组	符号	码组	符号	码组	符号	码组	符号
00000	Q(静止)	01000	无效	10000	无效	11000	J
00001	无效	01001	1(0001)	10001	K	11001	S(置位)
00010	无效	01010	4(0100)	10010	8(1000)	11010	C(1100)
00011	无效	01011	5(0101)	10011	9(1001)	11011	D(1101)
00100	H(停止)	01100	无效	10100	2(0010)	11100	E(1110)
00101	无效	01101	T	10101	3(0011)	11101	F(1111)
00110	无效	01110	6(0110)	10110	A(1010)	11110	0(0 0 00)
00111	R(复位)	01111	7(0111)	10111	B(1011)	11111	I(空闲)

进行这种4比特到5比特的变换不仅可以使时钟保持同步，而且还提供了可用于在设备之间传送控制信号的8个额外的有效组合，它们是J、K、T、R、S、Q、I和H。例如，当站点接收到超过15个连续Q符号时，它会认为连接中断；如果收到8对HQ符号，则认为一个设备正在被初始化。

23.4.4 MAC层

帧格式：如图23-20所示，FDDI定义了与IEEE 802.5类似的帧格式。一帧的最大长度为4500个字节。它以一个包含16个连续I符号的PA（PreAmble，前同步）字段开始，这个稳定的连1数据流使得接收机很快获得同步，J、K符号紧跟在PA之后。

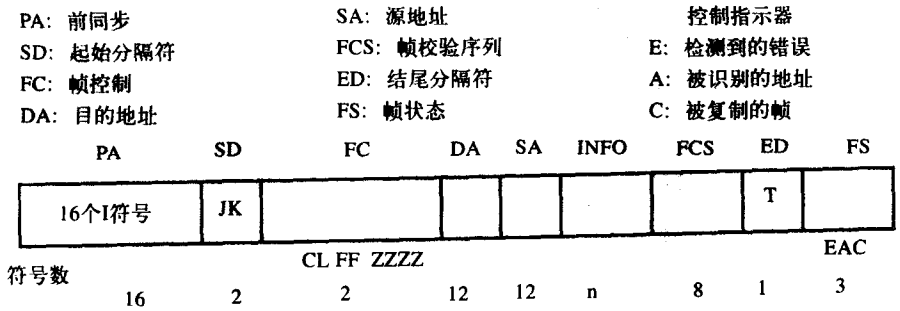


图23-20　FDDI帧格式。令牌仅包含PA、SD、FC和ED字段，其中ED包含两个T符号

FC（Frame Control，帧控制）字段有8位，第一位为类型字段，指出服务类型是同步的还是异步的。异步类服务意味着与传输话音不同，数据对延迟是不敏感的。在业务同步传输中，要保证站点拥有提前指定好的100Mbps带宽的一部分，以满足延迟敏感的业务。

L位即地址长度位指出一个6字节或2字节的地址字段，典型情况下地址长度为6个字节。FF和ZZZZ位定义令牌、SMT、MAC或LLC帧。SMT帧用来传递站点地址和端口状态，从而创建物理环路的拓扑结构（即图）。SMT和MAC帧不会像LLC帧那样穿过网桥和路由器到达其他LAN。

ED字段包含两个用于令牌的T符号和一个用于帧的T符号。最后，帧状态使用R和S两个符号来编码控制指示器。它们是E（Error detected，检测到的错误）、A（Address recognition，被识别的地址）和C（frame Copied，被复制的帧）控制指示器。

环的初始化：在环初始化之前，SMT组件在相邻节点之间交换关于端口类型和所有链路

地址的信息。接着运行链路可靠性测试以确定其链路质量，一执行完上述这些操作，所有工作站就会逐一相继接入环内。这一过程称为建立邻居之间的连接，它是SMT的一个主要功能。

一旦环上所有站点都建立了这一连接，站点就会发出请求决定谁发出第一个令牌，这就称为环初始化，这一步是由一个称为“发言”（claiming）过程的程序完成的。

在此，所有的站点都发出发言帧给出各自的SA和TTRT的值，TTRT（Target Token Rotation Time，目标令牌易手时间）等于一个令牌从发出到返回所需时间的一半。不像拍卖中开价最高的获胜，这里TTRT值最小的站将获得发送第一个令牌的权利。

最初，来自所有站点的很多发言帧同时涌向环内，在这一过程中，如果一个站点接收到一个TTRT值比自己低的发言帧，它就会让该发言帧通过，并且停止发送自己的发言帧。最后，只有一个站点的发言帧在环内循环一周，这时获胜的站点发送第一个令牌。当这个令牌在环内传输时，每个站点将此TTRT值复制到自己的缓冲区内，当该令牌第二次在环上通过时，主机就可以发送同步数据，并在此之后发送异步数据。

稳态操作：FDDI使用与4Mbps的TRN协议不同的时控令牌协议。在4Mbps协议中任何时候只有一帧可以在环内传输，同时，发送帧的站点直到接收到其返回时才会释放令牌。然而，在FDDI中，只允许站点持有令牌一段时间，这段时间是由THT（Token Holding Timer，令牌持有定时器）规定的。因此，即使一个站点还没有结束发送，它也必须停止发送并释放令牌给下一个用户。注意，帧一旦被发送，令牌就会立刻被释放，而不是等帧返回后再释放。这称为早的令牌释放，它允许环上同时存在多个帧。16Mbps的TRN也允许多个帧同时出现在环上，然而两种类型的TRN在每次令牌接入时仅发送一帧，而FDDI则可以发送多个4500字节的帧。

在IEEE 802.5中有一台活跃监视器维护整个环；与此不同，在FDDI中该功能是分散开的，所有站点都负责环的维护，各站点各自维护一个TVX（Valid Xmission Timer，有效传输定时器）。这里X是‘trans’的简写，TVX用来确定在一条链路上是否没有传送发生。如果由于噪声或丢失令牌而使该定时器超时，那么它将首先启动发言过程。让我们看看上行链路站点（即节点X）和下行链路站点（即节点Y）在连接它们的链路因为某些原因而使性能下降时，它们所采取的步骤。图23-19给出了节点X和节点Y。

首先，Y的TVX将溢出，因为它没有从X收到任何信息。它将开始发送发言帧。由于电缆损坏，X不能将这些帧转发给Y，因此发言过程失败，没有令牌产生。接着X开始信标过程，就像灯塔的信号等警告船只有危险一样，信标帧通知所有节点，环可能已损坏。

X再一次无法将信标帧转发给Y。大约10秒钟之后，发出一个定向信标帧，通知节点，信标被阻塞。如果这也失败，将使用PHY信令或线路状态来启动跟踪功能。跟踪消息通过从环由Y发送到X，强迫它们进行自检。如果检测成功，这些节点将加入环中，否则环将发生绕回，自己进行修复。

23.5 10Mbps以上的以太网

23.5.1 引言

本章的其余部分，我们接着第7章继续进行讨论，那里我们已经看到了交换机如何运行并提到了快速以太网和千兆以太网LAN的优点。这里我们将介绍各种标准并给出更多的细节。图23-21给出了一些以太网标准以及最终定稿（或称为“定案”）的时间。

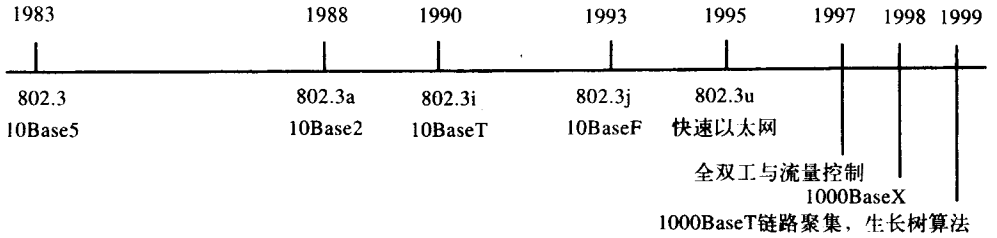


图23-21　以太网IEEE标准的发展过程

图23-22说明了将以太网速度提高到10Mbps以上的促动因素。在图23-22a中，一个简单的集线器使用10Mbps的链路与一台服务器和其他节点相连接。但这样做的效率并不高，所以第

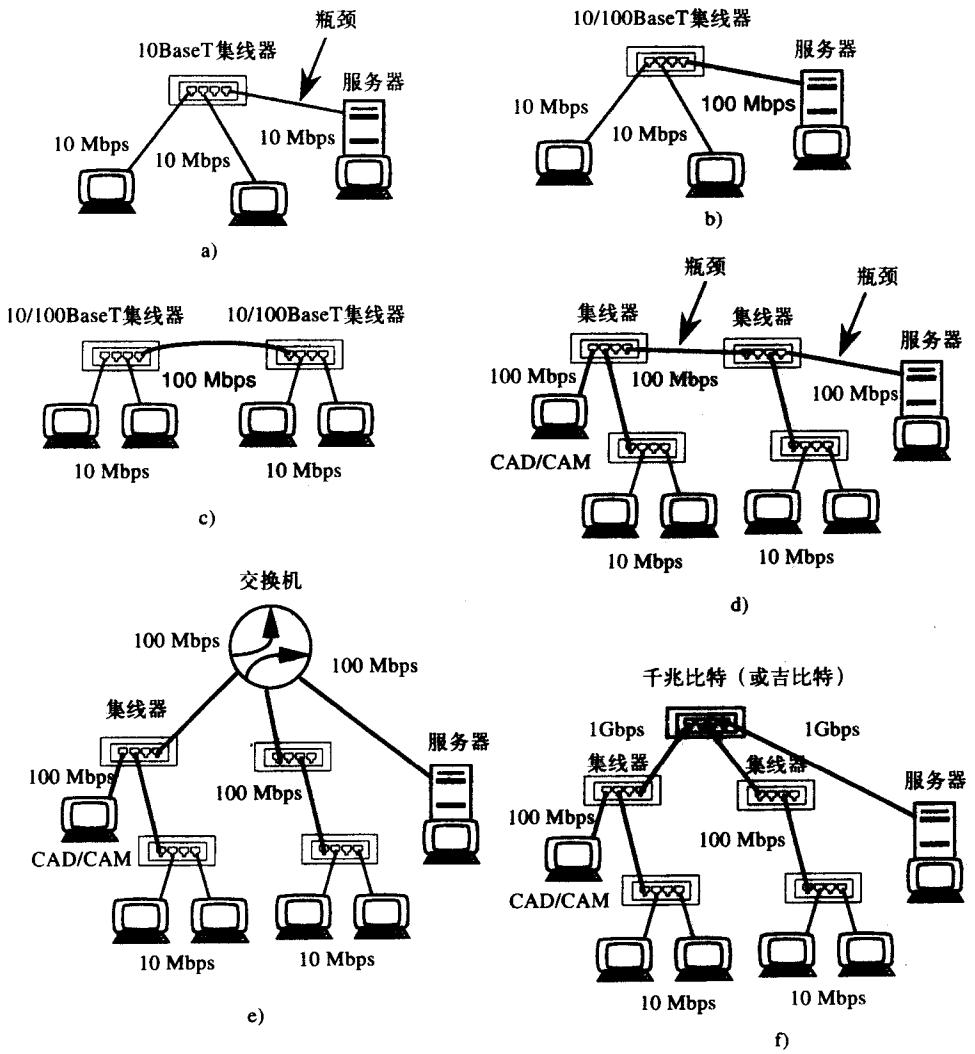


图23-22　a) 许多节点共享的服务器成为一个瓶颈；b) 给服务器增加一条100Mbps的链路增强其性能；c) 用100Mbps的链路代替中继器间链路；d) 顶部高速以太网的树型拓扑与向下延伸的标准以太网链路是合理的，但开始出现阻塞；e) 交换机或千兆比特集线器；f) 解决了这一问题

一步在服务器上安装一块100Mbps的NIC，并用10/100 Mbps集线器代替10BaseT集线器。如图23-22b所示。这种类型的集线器可以提供两种速度的连接。相对于网络其他部分而言，由于服务器可以以更高速度通信，因此它可以处理施加给它的请求。

在图23-22c中，通过增加一条100Mbps的链路可以缓解两个集线器之间的拥塞。同一对集线器之间还可以增加两条或多条这样的链路以进一步减轻拥塞。

在图23-22d中，网络被扩展。许多终端站点仍然工作在10Mbps，而其他的比如CAD/CAM工作站和服务器升级为100Mbps，这就在100Mbps的链路上产生瓶颈。

图23-22e和图23-22f给出了两种解决方案，增加一台交换机或者一个千兆以太网集线器就可以消除以前低速率以太网所经历的瓶颈。

23.5.2 以太网PHY

是什么决定了这么多类型的以太网仍然可以统称为以太网？那就是MAC层协议的定义。MAC层协议对所有类型的以太网都是相同的，而不管它们的速度如何，采用了什么样的连接器和电缆。在图23-23a中，我们看到由标准定义的10Mbps以太网组件，典型物理介质采用电缆，可以是10Base5中使用的粗缆，也可以是10Base2中使用的细缆，或者是10BaseT中使用的UTP。MDI（Medium-Dependent Interface，依赖于介质的接口）代表了与所用电缆相对应的连接器，无论它们是DB15、BNC还是RJ-45连接器。在10Base5中，MAU代表与同轴线相连接的收发器，而AUI（Attachment Unit Interface，附属单元接口）代表从收发器到NIC的下行分接电缆。

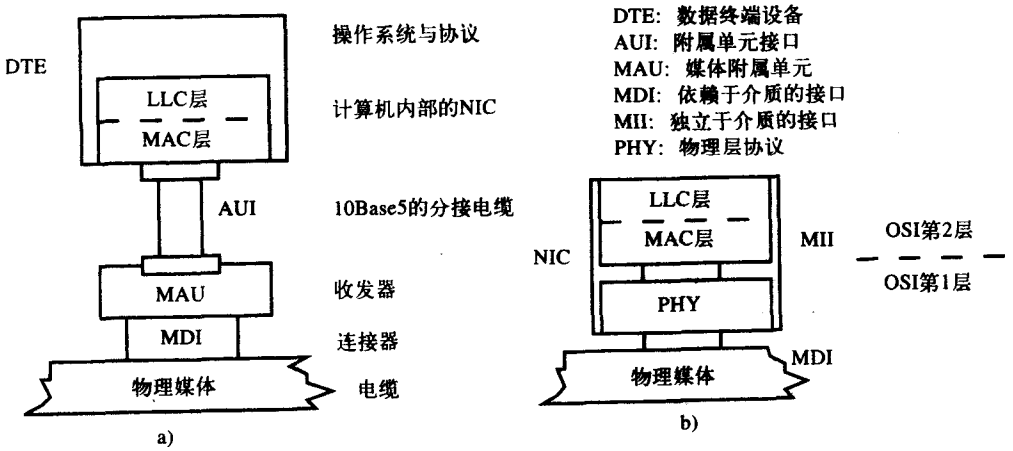


图23-23 a) 10Mbps以太网的IEEE术语，b) 高速以太网的IEEE术语

采用10Base2时，由于MAU被集成在NIC上，因此AUI接口仅仅是NIC的一个电气特性。并不存在什么AUI电缆。这里的MDI就是一个BNC连接器。然而，NIC中MAC层接收到的帧与采用10Base5时相同。对于10BasdT而言，物理介质是UTP电缆，MDI是RJ-45，MAU和AUI都集成在NIC上。

对快速以太网而言，IEEE定义了PHY组件，你可能会回忆起来这就是FDDI的PHY。事实上，在FDDI上取得的发展，很快就被重新利用而产生了快速以太网标准。PHY组件如图23-23b所示，这里MDI仍然是连接器，但又定义了一个新的称为MII（Media Independent Interface，独立于介质的接口）的接口，并取代了10Mbps以太网中的AUI。不管在快速以太

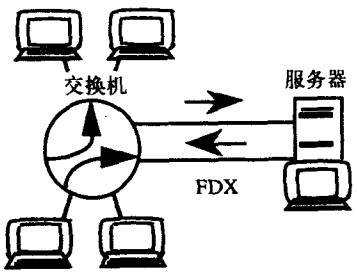
网中所使用的连接器和介质如何，MII确保到达（和来自）MAC层的信号都是一致的。

PHY位于每个NIC以及各集线器和中继器的端口。对于给定的媒质，它均使用相同的电气特性。PHY将电和光信号专门为MII转换成适合MII的电信号。对千兆以太网，MII被重新定义为GMII（Gigabit MII，千兆MII）。

23.5.3 全双工操作

对于10Base5和10Base2来说，只有半双工操作是可能的。这是因为连接到公共电缆的所有节点必须共享该电缆来传送数据。在这种情况下，只能有一个节点进行传输。如果一个节点正在发送数据，那么其他节点将均无法成功传送。因此，一个节点不能同时发送和接收信息。

当引入10BaseT作为解决方案后，人们发现它的传输介质是能够进行全双工传输的。它安装时所使用的UTP电缆通过集线器用一对线接收，用另外一对线发送。通过提供独立的用来发送和接收数据的线对，就实现了全双工。现在所要做的就是设计全双工的NIC和集线器。



实际上，引入交换机后全双工的功能就已经实现了，因为与集线器不同，交换机对帧提供缓冲。在旁边的图中，服务器正忙于为其所有客户提供服务。为其提供全双工连接就可以减轻拥塞。如果图中所示的所有链路都工作在10Mbps，那么在服务器和交换机之间就有20Mbps的信息交换能力。交换机在其各个端口提供缓冲，使它很像一个繁忙路口的交通警察。如果任何一个缓冲器满了，交换机就无法接受更多的帧了。

由该图我们可以清楚地看到，要建立全双工连接，在一条链路上必须只有两个节点。如果在该链路上还有第三个节点，这些节点就不知道某一特定的节点是否繁忙。全双工电缆的每对引脚只能发送或者只能接收，于是就不再需要CSMA/CD机制。这就意味着NIC在发送信息之前没有必要先监听媒质。另外，当与光纤配合使用时，设备之间的距离可以变得更长。全双工链路在两台交换机之间也很常见。

在千兆以太网中已经引入了全双工中继器，这些设备又称为**缓冲分配器**（buffered distributor）。多端口中继器或集线器通常会把接收到的信号在所有其他端口重新发送，但是中继器在接收到整个帧之后，要进行错误检测，根据需要就将其放入缓冲区，最后再将此帧重新发送到其他所有端口。与之不同，交换机只将信号传给与目的节点相连接的端口。该设备的所有端口都工作在全双工状态，并以1Gbps速率运行。它们都有输入和输出缓冲器。该设备的后台速率为1Gbps，所以它一次只能转发一帧而不像交换机可以同时管理几个连接。

23.5.4 流量控制

在前面的边图中我们已经看到，交换机和服务器之间的全双工链路如何在它们之间提供专用的20Mbps的带宽。在那个图中，当有更多的帧从其他节点发往服务器时，交换机可以先将其缓冲，再以接收时的速度将它们发往服务器。当交换机的缓冲器变满时，会发生什么情况呢？交换机怎样通知其他节点立刻停止发送呢？这类控制方法就称为流量控制。

在半双工的以太网中这很容易做到。当交换机不再希望从某个端口接收任何数据帧时，

它可以在那条链路上发送一帧，特意引起冲突。该帧并不包含任何有用信息，它唯一的目的是使发射机停止发送。在全双工链路中，由于不存在CSMA/CD，因此不会发生冲突。

图23-24给出了交换机怎样在一条半双工链路上产生冲突，同时还说明了在一条全双工链路上流量控制是如何处理的。在全双工链路上，交换机可以给服务器发送特殊的PAUSE帧以阻止服务器发送数据，这些帧中的暂停次数会通知服务器暂停多长时间。所有的全双工链路都提供这种功能，并且是由IEEE 802.3X标准规定的。注意，图中的交换机能够以不同的速率支持各个端口。

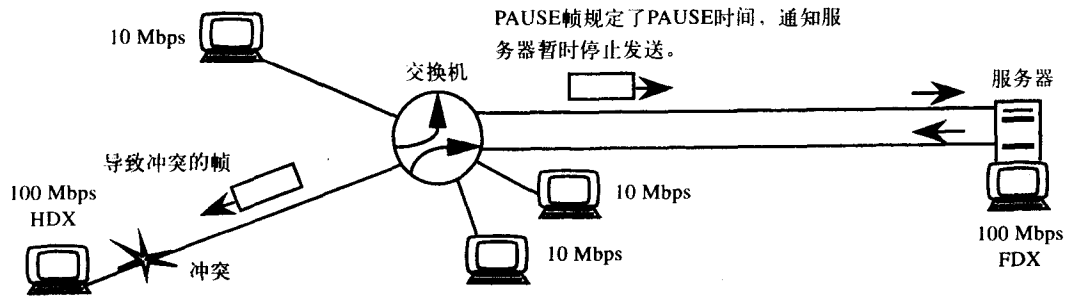


图23-24 交换机在半双工链路上产生冲突，并在全双工链路上发送一个PAUSE帧以减慢其他节点的数据传输

23.5.5 自动协商

由于以太网提供了诸如线路速率（10Mbps、100Mbps、1Gbps）、全双工或半双工以及其他正在不断增加的特征等许多选择，因此链路的一端有必要了解另一段能够处理什么功能。在10BaseT中，能做的只有链路完整性测试，通过它可以知道链路的另一端连接是否正常。随着新标准被加入到以太网中，各端口还必须知道链路另一端的端口能够支持哪些功能，这就称为**自动协商**（autonegotiation），它是在快速以太网标准中首先规定的。

如果可能，自动协商允许一个使用RJ-45连接器的UTP链路工作在最高速率和全双工状态。如果使用光纤，则只需在全双工或半双工运行模式之间作出判断。目前光纤端口不能以多种速率运行，而铜线端口却可以多种速率运行。

全双工相对于半双工有更高的优先级。1Gbps比100Mbps具有更高优先级而后者又比10Mbps的优先级高，这使得链路可以其最佳容量运行。10BaseT使用NLP（Normal Link Pulses，常规链路脉冲），我们称之为链路完整性测试信号。这个信号允许每一端都能验证另一端的连接是否正确。相反，快速以太网设备则连续发送FLP（Fast Link Pulses，快速链路脉冲），这包括NIC、中继器和交换机。

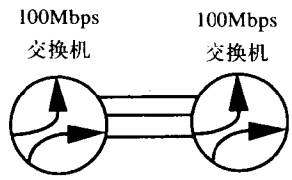
例如，如果一台10/100M交换机与许多10Mbps的NIC相连，则当资金允许时应该将这些NIC换为100Mbps的NIC。当交换机没有收到来自NIC的FLP，而只收到NLP时，它将采用半双工方式以10Mbps的速率工作。FLP是比NLP更复杂的信号，它表明了传输速率和通信方式。

另一方面，如果去年购买的NIC对10Mbps和100Mbps均支持，那么旧的10Mbps集线器就能够用更高速的集线器或中继器代替。这种升级可以很容易地在网络中完成，而无需配置任何设备。自动协商中所使用的FLP可以自动地将各链路调整到其最佳状态。

23.5.6 链路集合

假设两个由单个链路连接在一起的100Mbps的交换机以满容量运行。然而，它们之间的链

路造成了一个瓶颈。一种解决方案是在它们之间加入一个1Gbps的交换机，但这样做成本太高。通过将交换机之间的多个端口相互连接起来，我们也能够减轻一些拥塞而不必购买新的设备，如侧图所示，三个全双工的端口提供了一个600Mbps的“肥管”。



600Mbps/FDX的链路集合

IEEE 802.3ad规定了如何实现上述功能的标准。理论上，该标准允许不同厂商生产的的两台交换机以上述这种方式相互连接。在后面关于LAN互联的一章中，描述了网桥和交换机之间的生长树算法（IEEE 802.1d）。这个算法允许有多条链路，但任何时刻只允许一条链路处于活动状态，其他链路只是用作冗余。802.3ad链路集合标准克服了802.1d的这一限制。

23.6 快速以太网

23.6.1 快速以太网的类型

既然我们已经了解到快速以太网和千兆以太网所提供的各种特点和优势，下面就更详细地讨论有关的标准。事实上，有4种已经批准的快速以太网标准。然而，只有其中的两种标准在市场上占主导地位，它们是5类双绞线和光纤标准。存在于3类电缆的两对或四对上的两个标准实际是不存在的，它们分别被称为100BaseT2和100BaseT4。更常见的100BaseT类型有100BaseTX和100BaseFX，典型情况下，100BaseTX用于水平电缆而100BaseFX用于垂直骨干电缆。

100BaseT：100BaseTX通常被称为100BaseT。这种高速以太网虽然可以使用更高等级的UTP电缆进行安装，比如5类增强型、6类或更高，但它通常使用5类UTP电缆安装，也可以使用1型STP。如果安装正确，5类电缆可以提供四对线支持高达100Mbps的速率。

10BaseT和100BaseT之间有很多相似之处。在可用的四对线中仅使用了两对，一对用于接收，一对用于发送。它们都使用相同的RJ-45连接器；都采用星型总线拓扑结构和CSMA/CD接入网络；从集线器到NIC的距离与10BaseT的相同，也是100m。

100BaseT与FDDI（更确切地说是CDDI，即铜线FDDI）也有很多相似之处。首先，两者的速率相同，均为100Mbps。我们已经看到在定义与MAC层的物理接口时，IEEE没有使用10Base T的AUI，而是用了MII。类似地，MAU也被PHY所取代，其他来自CDDI的技术包括线路信令的MLT-3（多级门限-3）方法，以及在本章FDDI一节中介绍的4B/5B符号编码方法。

我们看到FDDI使用NRZI编码方法，而CDDI要求一种带宽利用率更高的方法。称为MLT-3法。由于这种方法采用三种电平，因此可以在双绞线上使用，但不能用于光纤，因为光纤只有开和关两种状态。MLT-3在铜线上可以获得更高的速度但易受噪声干扰，你也许记得FDDI的工作频率是125M波特时，但有效频率却是100Mbps。如果100BaseT不使用MLT-3，那么在100m范围内要想获得100Mbps的速率，就必须工作在200M波特；而使用MLT-3时，工作频率只需125MHz。

100BaseF：这种光纤型的100BaseX同样来自于FDDI。100BaseF使用MMF（Multi Mode Fiber，多模光纤），其纤芯到敷层的直径为62.5/125μm。然而，也可以使用SMF（Single Mode Fiber，单模光纤）扩展光缆工作范围。一束用于发送，另一束用于接收。最初ST连接器很常用，但现在SC连接器则变得更加流行。

23.6.2 扩展100BaseX

最初的100BaseX定义了两类中继器。I类永远不会断开，因为在一个冲突域内它们只允许有一个中继器存在。II类最多允许存在两个中继器，所以下面仅深入讨论II类中继器。

图23-25给出了使用UTP和光纤时的最大传输距离，其中括号内为采用光纤时的值。当使用UTP时，两台DTE（数据终端设备）之间的最大传输距离是100m，如图23-25a所示。在图23-25b中，增加了一个中继器，使网络的范围扩展到200m，增加两个中继器会使网络的范围扩展到205m，如图23-25c所示。由此注意到通过使用UTP，网络从包含一个中继器到两个中继器只获得了很小的范围扩展。但是，如果使用光纤，范围会缩短将近100m。从DTE到DTE使用MMF的全双工方式范围为2000m，使用SMF的全双工方式范围为10 000m。

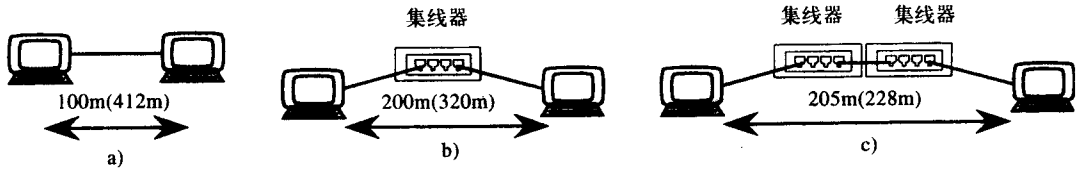


图23-25 100BaseT的最大距离，括号中是100BaseF的最大距离：a) 两个DTE之间，b) 采用一个集线器或中继器，c) 采用两个集线器

图23-26说明了包含两个中继器的网络怎样扩展其范围，图23-26a表示最多包含两个中继器的原始网络，图23-26b表示集线器可以堆成栈，使每个栈看起来就像单个集线器。栈中集线器的数量取决于其建立的方法和类型，典型数字是4。

图23-26c表示加入一台交换机（或网桥）可以使网络范围（使用UTP）由200m再增加200m；若加入一个全双工光纤链路，则范围可扩展到2000m甚至更多。

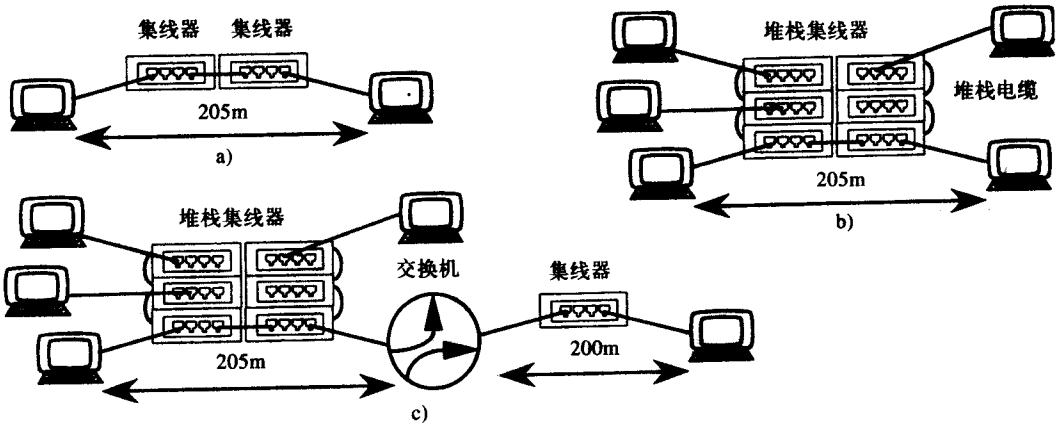


图23-26 a) 采用两个中继器的网络似乎达到了其最大尺寸；b) 然而，更多的集线器可以分层叠加形成集线器栈；c) 可以增加交换机

23.7 千兆以太网

千兆以太网是在被称为光纤通道标准的ANSI X3T11标准所做工作的基础上发展起来的。光纤通道工作在1G波特，提供的有效速率为800Mbps。千兆以太网的速率增加到1.25G波特，从而使其数据传输速率为1Gbps。千兆以太网再次使用了与光纤通道相同的符号编码方法，即

8B/10B编码方法。它们都使用GMII（Gigabit Media Independent Interface，独立于介质的千兆接口），这使工程师可以很容易地重用为光纤通道设计的PHY。

在定义不同类型的以太网时，规定了一个被称为时隙的参数。该时隙是NIC发送一帧所需要的最短时间。如果以太网的帧太小，那么将无法检测到冲突。正是由于这个原因，当帧长度小于某个值时，就应该增加额外的PAD（填充）字符。回到图23-7，可以看到不包括Preamble（前同步）在内，最小以太网帧长度为64个字节，这64个字节对应一个512比特的时隙，使用正确的度量单位即512比特时间。

引入高速以太网后，线路的速度增加了10倍。这意味着小帧将无法被大型网络中的其他NIC检测到。于是决定减小网络直径，而不是增加比特时间；因此，在高速以太网中只允许最多有两个中继器。千兆以太网须进一步减小网络的直径，这将使集线器与NIC之间的距离降低到10m或更小。所以，对于千兆以太网而言，时隙应提高8倍，即4096比特时间。这里，以太网的帧大小不变，然而，在小帧末尾增加额外的承载扩展比特以示一帧在电缆上的存在。

千兆以太网有三种可行版本，分别被称为1000BaseSX、1000BaseLX和1000BaseT，其中“SX”代表短波，“LX”代表长波，我们所熟知的“T”代表双绞线。1000BaseSX只使用MMF和短波（850nm）光二极管。根据所用光纤的类型不同，1000BaseSX允许运行的网段长度达550m。一种成本稍高的以太网类型为1000BaseLX，它使用MMF或者SMF，并采用1300nm的激光产生信号。使用SMF（10/125μm）时，它可以将LAN扩展到5km。

为了在5类线上获得1Gbps的速率，必须出现一些技术上的奇迹。从集线器到节点的最大距离仍然是100m。5类线最初设计为100Mbps，即使在当时，基于UTP的100Mbps似乎也是不可能的。对1000BaseT所做的就是使用全部4对线发送并接收。第3章讨论的回波抵消允许在同一对线上同时发送和接收。早期的以太网也是用一对发送一对接收。这种在同一对线上同时进行发送和接收的传输模式称为**双向双工**（dual-duplex）。现在每对线均以250kbps的速率发送，并以250kbps的速率接收。1000BaseT使用5级PAM（Pulse Amplitude Modulation，脉冲幅度调制）编码系统，每个脉冲代表两位（00、01、10和11）。另外，利用FEC（Forward Error Correction，前向纠错）减少双绞线上可能的错误量，这就是工程师们能够在5类电缆上运行1Gbps的主要原因。

23.8 VLAN

图23-27a表示如果仅使用集线器/中继器互连LAN，那么在LAN的一个网段的每次传输必须在其他网段上重复，除了TCP/IP以外，许多LAN协议会产生大量的广播帧，来发现谁在网络上或通知其他人他们仍然在网上，这类开销流量称为广播。仅由集线器连接的网段同样要重复所有广播流量。将冲突限制在一个网段内的主要方法是增加一台交换机，如图23-27b所示。如果我们加入一台路由器而不是交换机，我们还可以将广播限制在LAN的一部分。

VLAN（Virtual LAN，虚拟LAN）允许定义我们的广播域和冲突域而不必考虑节点的物理位置。使用VLAN就不必将雇员束缚在建筑物或校园的某特定地点，可使他们成为任意逻辑网段（即后面会见到的任何子网）的一部分。雇员的物理位置并不会强迫他们属于某特定的组织机构。如果雇员更换部门，他没有必要移动。这一过程可以由LAN管理员在VLAN交换机上编程实现。

IEEE已经定义了VLAN标准，即802.1Q，它使用一个4字节帧标签来标识各帧，标签字段主要规定VLAN ID以及用户优先级。由于标签字段占用了4个字节（在源地址字段和类型/长度字段之间），因此，以太网的帧长度又增加了4个字节，这是由IEEE 802.3ac标准规定的。

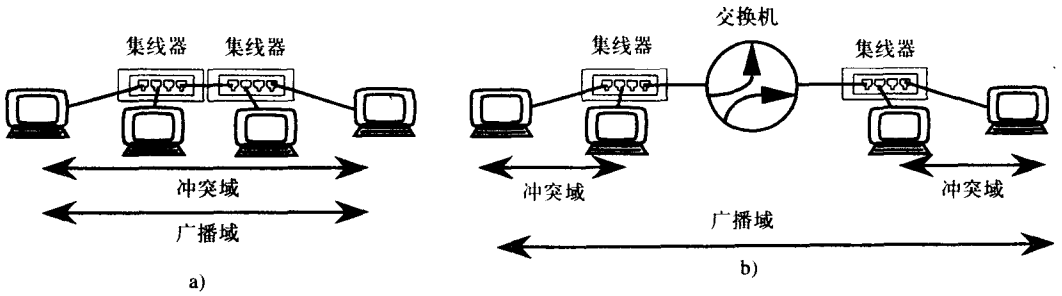


图23-27 a) 一个集线器的冲突或广播被发送到其他集线器；b) 交换机能够分割冲突域，但不能够分割广播域，只有路由器才能分割广播域

VLAN组的成员既可以隐式识别又可以显式识别。隐式成员是由以太网帧中的MAC地址、类型字段或IP地址确认得到的，显式成员是由标签字段的标识规定的。所以，交换机知道哪些帧属于哪些VLAN，并且不存在重复ID，所有的VLAN ID都应该由一个管理位置分配。

习题

23.1节

1. PC上的什么软件部件直接负责向网络发送数据？
   a. NetBIOS　b. BIOS　c. DOS　d. 应用程序
2. 下列哪个术语与基于服务器的NOS无关？
   a. 基于客户机-服务器的NOS　b. 集中式NOS　c. 对等NOS　d. NetWare
3. 下列哪个协议栈与Unix关系最为密切？
   a. NetWare　b. Vines　c. AppleTalk　d. DOS
4. 叙述BIOS与CMOS之间的区别。
5. 在一个点对点网络中共享与使用有什么区别，服务器能提供什么功能？
6. 在图23-4b中，我们看到一条错误信息，操作host23的用户如何避免该错误信息？操作host2的用户仍然保存testfile又如何？
7. 描述host23怎样在host2的打印机上打印文件的步骤。
8. 任何LAN协议都能与图23-5所示的任何通信协议共同使用吗？
9. IEEE 802 族协议的哪两层组成OSI的数据链路层？
10. MAC头对于所有类型的LAN都相同吗？LLC头呢？
11. 哪个头规定了帧的目的地址？
12. 哪个头规定了帧的网络层协议？哪个字段表明这一信息？

23.2节

13. 下列哪个字段名在两种类型的以太网中都未使用？
    a. Type　b. FCS　c. Preamble　d. SA
14. 下列哪种类型的以太网使用光纤？
    a. 10BaseF　b. 10Base5　c. 10BaseT　d. 10Base2
15. 下列哪一个不是收发器？
    a. AUI　b. MAU　c. NIC　d. 以上均不是

16. 不算前同步在内，以太网帧的最小长度为多少？给出以字节为单位的答案。
    a. 18　　b. 46　　c.64　　d.1500
17. 在下列各问题中，以太网帧头的字节数以十六进制的形式给出，每个字节需要两个十六进制位。因此，前6组两位数字代表NIC的目的地址；后6组代表源地址。没有表示出前同步。对于各个问题而言，给出了目的地址、源地址以及后面的4个字节。
    回答下列问题：
    1）这是哪种类型的帧？是以太网或带有SNAP的802.3，还是不带SNAP的802.3？
    2）网络层使用什么协议？IP，Novell还是其他的？
    3）你能确定用十六进制表示的帧长吗？
    a）00 aa 00 01 de e4 00 aa 00 01 df 07 08 00 aa bb
    b）00 aa 00 01 de e4 00 aa 00 01 df 07 04 00 aa aa
    c）00 aa 00 01 de e4 00 aa 00 01 df 07 00 aa e0 e0
    d）00 aa 00 01 de e4 00 aa 00 01 df 07 01 1a 06 06
    e）00 aa 00 01 de e4 00 aa 00 01 df 07 81 38 aa aa
18. 只使用10BaseT时，网络中可以容纳的最大节点数为多少？假设没有将集线器堆在一起，而是将它们级联起来，并且每个集线器都有8个端口。画出该网络，并确定两个节点之间的最大距离？

23.3 节

19. MAU怎样知道是否在环中设置节点？
20. 在TRN中，接收所有被发送的信息的站点称为什么？
21. 哪种类型的TRN帧发送数据？
22. TRN中的两种特殊的扰码称为什么？
23. TRN中的RIF字段有什么功能，如何使用？
24. 给出活动监视器的功能？
25. 画出发送00101110的曼彻斯特、差分曼彻斯特及NRZI波形，假设第一比特的前一个比特为0。

23.4节

26. 给出四种FDDI设备及四种FDDI连接器的名称。
27. 在FDDI中，拥有最小_____值的站点获得发送第一个令牌的权限？
28. 在FDDI中，将4位数据组变换到5位编码组的原因是什么？

23.5节

29. 全双工操作不使用下列哪个以太网特点？
    a. MAC 头　　b. 逻辑总线拓扑　　c. 冲突检测　　d. 无连接数据传输
30. 下列哪种以太网不采用全双工操作？
    a. 10Base5　　b. 10BaseT　　c. 10BaseF　　d. 100BaseT
31. 10Base5中的AUI被千兆以太网的哪个接口所取代？
    a. 收发器　　b. PHY　　c. MII　　d. GMII
32. 在全双工和半双工模式中如何实现流量控制？
33. 当电缆的两端决定运行在哪种模式以及以什么速度运行时，称为什么？

34. 如果5个全双工端口集中在两个100Mbps交换机上，总的有效带宽是多少？

23.6 节

35. 在UTP上开发100BaseT时采用了下面哪个标准？

a. 10Base5 b. FOIRL c. 光纤通道 d. CDDI

36. 当100BaseT达到最多两个集线器时，下列哪一项不适合增加更多的端口或者扩展LAN的网络范围？

a. 增加一台中继器 b. 增加一台路由器 c. 增加一台交换机 d. 集线器堆栈

37. 仅使用两个集线器，100BaseT的最大距离是多少？100BaseF呢？

38. 设计100BaseT时利用了10BaseT的哪些特点？

23.7节

39. 光纤和铜线两种千兆以太网中采用了哪种编码方法？

40. 工程师采用了什么办法使100Mbps的标准5类线可以工作在1Gbps？

41. 什么技术有助于设计千兆以太网？

42. 光纤型千兆以太网称为什么？它们有什么区别？

第24章 桥接与路由

24.1 互联网设备

个人计算机一连入LAN后，就出现了将LAN和WAN连接成复杂的互联网的需要。互联网（internetwork，或者简写为internet）是由许多网络组成的网络。互联网通常利用一系列基于TCP/IP（传输控制协议/网际协议）的协议将不同的网络连接在一起。这些互联网中最大的被称为因特网（Internet，拼写时使用大写字母“I”）。因特网是由DARPA（Defense Advanced Research Project Agency，美国国防部高级研究计划局）资助的，它所连接的计算机超过了1 500 000台，是世界上最大的网络。本章将介绍与互联网相关的设备、协议和服务。

24.1.1 在网络中加入网桥

回到图7-13中，我们可以看到如何利用中继器将一个LAN由一个楼层扩展到整栋楼的许多楼层甚至扩展到整个校园的其他楼。中继器的作用是放大电缆中的信号从而使LAN不局限于某个特定区域。对于Ethernet而言，利用四个中继器可以将LAN的范围从500m扩展到2500m。

当我们希望使用比10Base5廉价的LAN技术时，我们可以在网络中的不同位置增加一些集线器，如图23-12所示。这样我们就能够混合使用各种各样的局域网技术。同时，集线器不仅提供了信号再生的位置，而且还提供了更好的管理和故障查找能力。

然而，中继器仅仅是再生信号，如果我们不断在LAN中加入更多的站点并且更频繁地使用网络而增大网络的流量时，那么网络的吞吐量最终会下降，其原因是冲突的数量增加了。如果中继器两端的节点同时想与对方通信，这是不可能实现的，因为中继器不能隔离流量，而只是简单地在LAN的各个网段之间传递信号。

例如，在图24-1a中，在A与B通信的同时，E与F不能通信。解决这个问题的一种方案是将网段隔离，如图24-1b所示。现在，A和E可以同时发送数据，但是，它们之间却不能相互通信了。因此，为了同时具备上述两项功能，我们在这些网络之间增加一个网桥。网桥具有滤波的功能，也就是说，当A与B对话时，那么它就不会让传给E和G的帧通过。然而，A发送给E的数据帧是可以通过网桥的，参见图24-1c。在图24-1a中，因为所有节点之间仅存在一条通信路径，所以只有一对节点可以相互通信。而在图24-1c中，网络被分成两个网段，通信可以在各网段同时发生。

然而，必须仔细考虑在什么地方设置网桥，从而将网络划分成现有的逻辑组。也就是说，网桥每一侧的站点应该主要在它们自己之间通信，与另一侧的站点通信只能是偶然的。一个通用的经验规则是80%的流量限定在同一个网段内，仅有20%的流量需要通过网桥，一旦两个百分比相等的话，就需要增加更多的网桥，进一步划分网络。使用网桥还可以超越LAN的距离限制。

另一方面，如果不是过度地使用网络，中继器也提供了一个很好的解决方案。它们是不依赖于协议的，意即它们并不在意帧中各字段的含义，因为它们只是把桥这边的比特复制到

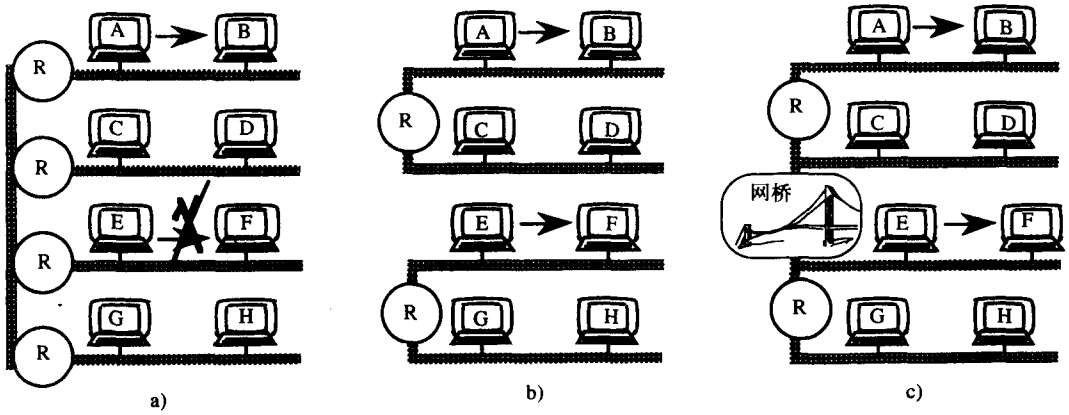


图24-1 a) 在A与B通信的同时，E不能通过中继器与F进行通信；b) 将网络分隔开后，这种情况就会成为可能，但现在A却根本不能与E－H通信；c) 采用网桥后，便可实现上述两项功能

另一侧。它们在网络中仅表现为一比特或两比特的延迟，有时，它们会增加或丢失比特。由于它们运行于OSI的物理层，因此并不进行错误校验。网络的端节点并不知道它们的存在，而且由于不对中继器进行配置，因此它们经常被其他的模型替代。

24.1.2 在网络中加入路由器

网桥容易安装而且可以在硬件层次上提供基本的安全保障。例如，可以禁止某些用户访问自身所在网段以外的网络。网桥易于管理并且在正常运行时不需要专业的技术。然而，在带有环路的桥接网络中，一个网络中的小故障都可引起整个网络的瘫痪，接下来的故障排除也是非常困难的。

同时，网桥也不隔离广播（向所有节点发送信息）和组播（向一组节点发送信息）。广播的类型有两种：正常广播和异常广播。正常广播就是各节点周期性地向网络中的所有节点发送信息，表明它们与网络的连接状态，这会占用一个大型网络相当大的带宽。异常广播也叫广播风暴；它是由于网络部件的故障所引起的。带有网桥的网络无论看起来还是运行起来都是一个简单的网络。

一旦开始在互联网中加入其他站点，尤其是那些使用WAN链路的站点，我们就希望在拓扑结构上形成环路从而提供可选路由，如图24-2a所示。这里，我们一旦用网络执行关键任务型应用程序，就要求它具有很高的可靠性，那么最好用路由器取代网桥。

以前，必须为需要路由的各种类型的协议安装独立的路由器和WAN链路。现在，多协议路由器可以同时处理多个协议，可以将广播流量和组播流量隔离开。网络中不同部分的流量类型是可以控制的，网络的安全和管理比采用网桥更具有鲁棒性；如果网络性能下降，那么故障可以很容易地隔离到路由器的一个端口，从而有可能迅速地恢复网络。

网桥不能高效地利用WAN链路，最好在短距离范围内使用并且通常仅使用两个端口；而路由器则要首先查看网络层的头部信息，之后再由内部路由表确定最佳路径。如果有拥塞、延迟或额外开销时，路由器会做出令人满意的选择。因此，路由器比网桥更智能。

网桥是不依赖于协议的，与运行在OSI模型网络层的路由器不同，网桥则工作在数据链路层。对于没有第三层的协议，如DEC的LAT（Local Area Transport）和NetBIOS，不能进行路由，必须通过桥接。

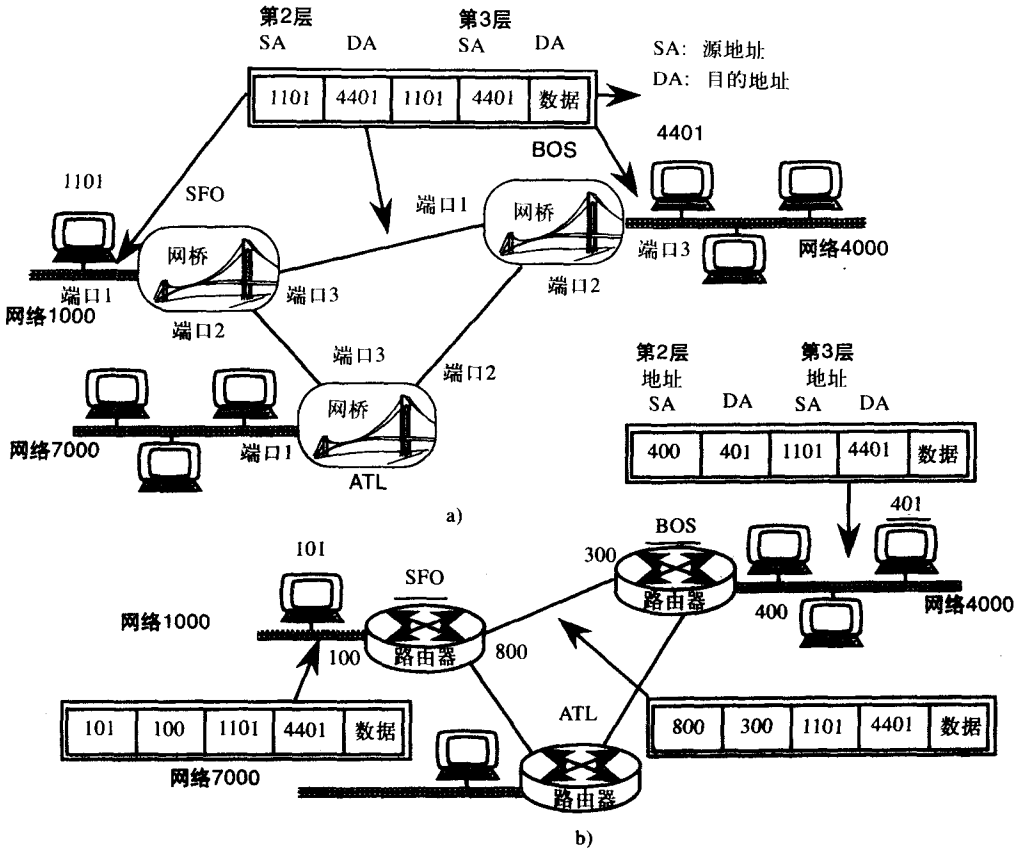


图24-2　a) 帧在通过网桥后保持不变，这是一个大型网络；b) 网桥被路由器所取代，当帧通过路由器时，数据链路地址保持不变

采用多协议网桥/路由器时，可以先将它们安装为网桥，在了解网络如何运行和发展之后，可将其配置成路由器。也可以将它们配置为对于一些协议建立桥接，而对其他协议建立路由连接。

下面我们用图24-2来说明工作在数据链路层和网络层的设备是什么意思。假设有三个网络（分别编号为1000、4000和7000）相互连接。节点有一个三位数字的ID，因此，网络ID与节点ID结合起来就可以唯一地确定网络中的任何一个节点。

假设节点1101（网络1000上的节点101）正在向节点4401发送分组数据包。在图24-2a中，该节点将对第二层的SA（Source Address，源地址）和DA（Destination Address，目的地址）进行编码，使其与第三层的SA和DA相同。在这种情况下，SA和DA分别为1101和4401。位于旧金山（San Francisco）的网桥SFO将通过第二层的DA决定让这一帧通过它的端口3。类似地，网桥BOS（即位于波士顿的网桥）将根据第二层的DA确定4401在自己的网络中并将该帧转发给节点401。

但是，如图24-2b所示，在基于路由器的网络中，分组是从一条链路路由到另一条链路的。首先，当节点101组装好一个分组数据包后，就会在其第三层的头部将SA设置为1101，将DA设置为4401。之后再利用第二层将该分组封装到一帧内，使其SA为101，DA为100，即路由器在网络1000的端口地址。

帧到达SFO路由器，经过检错之后，该路由器就会丢弃第二层的头和尾。如果出现错误，

则请求重发。该路由器在读取分组头中的DA之后，就决定通过直接链路将这一分组发送给BOS路由器。这是通过将相同的分组封装在SA和DA分别为800和300的新帧中完成的。这样就能使该分组到达BOS路由器。

接着，BOS路由器进行差错校验，并将帧头和帧尾去掉。之后，决定将该分组直接传给接收端。于是，它将SA编码为400（路由器本身的第二层地址），将DA编码为401。最后，节点401接收并解码所接收到的数据。

这样，网桥仅读取并处理数据链路控制信息，而路由器则还要处理网络层的信息。由于网桥处理的信息比路由器少，因此网桥每秒钟发送的数据帧比路由器每秒钟发送的分组数要多。同时，因为帧在通过网桥后不会发生改变，因此图24-2a的布局被认为是一个大型网络，而图24-2b的布局则被认为是六个独立的网络。

24.1.3 骨干的倒塌

在图23-12中，我们可以看到如何在各层的网络中加入集线器和集中器来扩展网络。为了使网络进一步扩展，可以在这些集线器中加入网桥卡或路由器卡。

然而，这种骨干网延伸至几层楼或几栋建筑的结构存在几个问题。如果其中一个集线器中的卡出现故障的话，那么技术人员首先必须带着LAN分析仪到各个地方查找这些故障。在那些装有各类线路和设备的配线间，接入这些集线器是非常困难的。即使检测到某个卡出现故障，技术人员也必须回到端局进行替换。同时，将这些集线器分散在各地也阻碍了网络及时地提供服务。况且，即使在正常运行期间，各个楼层的文件服务器也不像它们都位于一间专用的屋子里那样容易保证安全性。

第三代集线器，即倒塌的骨干网络，将所有对网络运行至关重要的部件放在一个安全的屋子里。我们称之为NOC（Network Operations Center，网络运行中心）。参见图24-3，骨干并没有延伸到很大的区域，而是完全位于一个地方，所有重要的网络部件以及所有网段都与此处相连接。从逻辑上讲，可以把NOC中的集线器看作超级集线器。对于网路本身而言，把一个楼层的所有部件都集中在一个“密闭的”集线器中与把所有部件都集中在NOC中的中心集线器上会获得同样的好处。

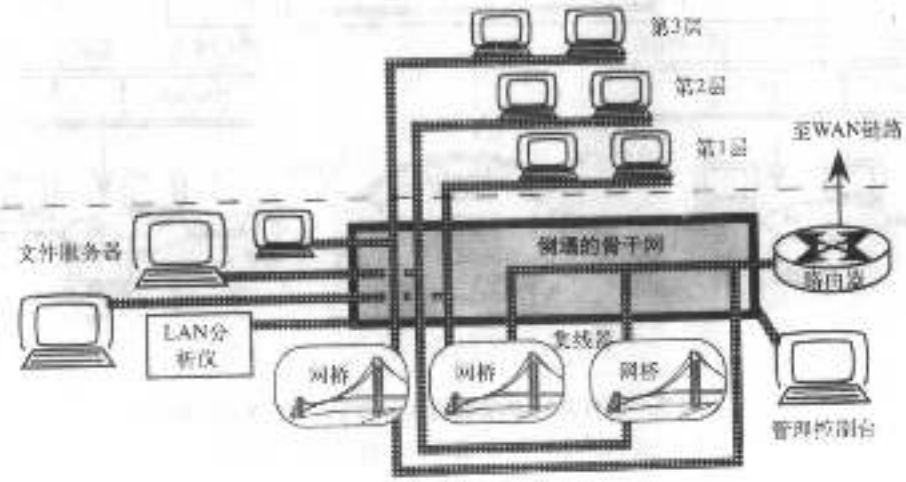


图24-3 位于网络运行中心的集成集线器和所有网络设备如虚线以下所示

集成在管理控制台的LAN分析仪使得网络管理员在一个有利的地点就可以对网络进行全面的控制。夜晚，为了保障文件服务器的数据安全，网络管理员可以确认所有的文件服务器被正常关闭。这里只需保证一个房间而不是与其他设备共用的多个配线间的安全。

如果一个网段出现问题，管理员可以快速地从控制台将该网络隔离。所有的设备，包括备用设备都已经插进了集线器，这使得通过集线器的软件来改变配置成为可能。如果服务器或网桥需要进行临时交换，仅需通过控制台的操作就可以完成，而不需要物理的插拔设备。因此，第三代集线器能够大大地改进对扩展LAN的管理、使用和控制，但必须要注意集线器本身具有相当高的容错能力。

24.2 网桥

24.2.1 转换和封装网桥

图24-4给出了两种很不常见的网桥。图24-4a表示转换网桥的运行情况，它用于连接在第一层和第二层不相同的两个网络。在令牌环上要到达一个以太网节点的帧是由网桥进行转换的，该网桥将TRN的帧头和帧尾丢弃并加入以太网的帧头和帧尾。当数据反向传递时，处理过程也相应颠倒。

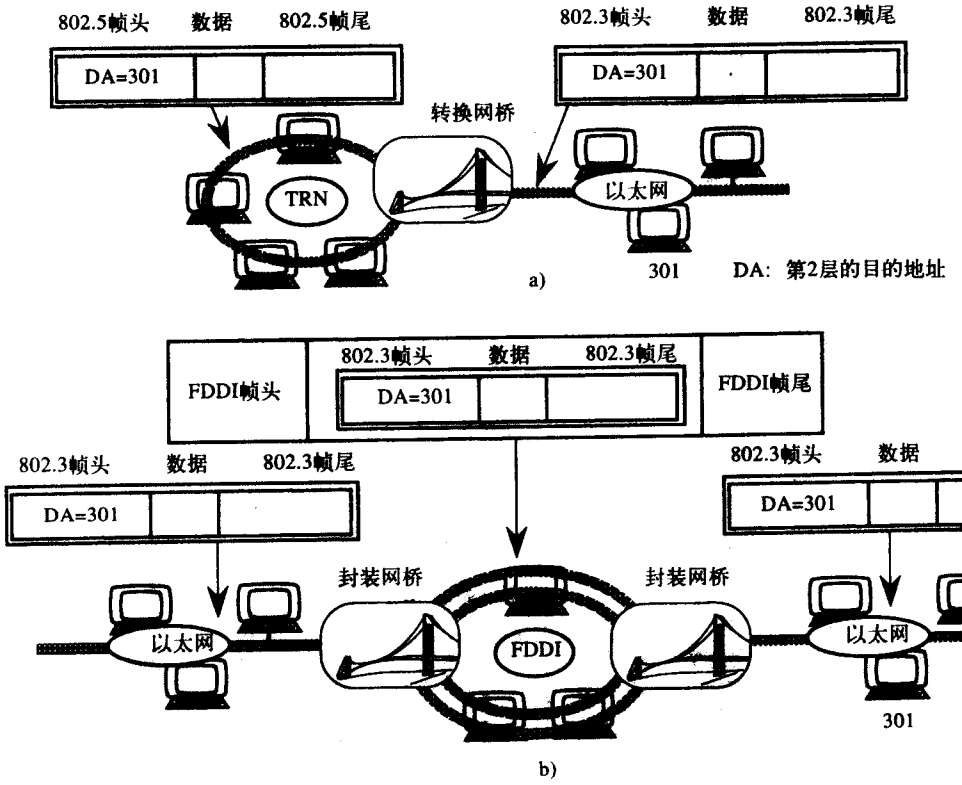


图24-4 a) 转换网桥将第2层的头和尾从一种格式转换为另一种格式，
b) 封装网桥将一个第2层的帧安装到另一个里面

传送给同一个网络中的节点的任何帧都不用经过网桥转发。最后，网桥不能执行分段操

作。分段是在数据传输网络不能够处理很长的帧时，将较大的帧分割成较小的单元的处理过程。因此，必须对连接在转换网桥上的节点进行配置以使它们不传送很长的帧。

封装网桥如图24-4b所示，它用在诸如FDDI环这样的骨干网络之上。这里，终端系统最低两层的协议必须相同，并且骨干网络将它从分支网络或接入网络接收到的帧进行封装。如图24-4b所示，左边的以太网LAN向右边的以太网LAN发送一个802.3帧。第一个网桥将该帧封装在一个FDDI帧中，之后右边的网桥将FDDI的帧头和帧尾去掉，再向其目的地发送原始的以太网帧。

24.2.2 透明网桥

如24.2.1节所述，传统的网桥是一种特殊类型的透明网桥。这里的透明是指终端系统（或主机）无需知道网桥在网络中的存在，即，网桥的运行，相对节点来说是透明的。透明网桥仅让那些应该转发给另一个端口的帧通过，而丢弃其他帧。透明网桥找到与其端口相连接的节点的方法称为“学习”。图24-5说明了它是怎么工作的。

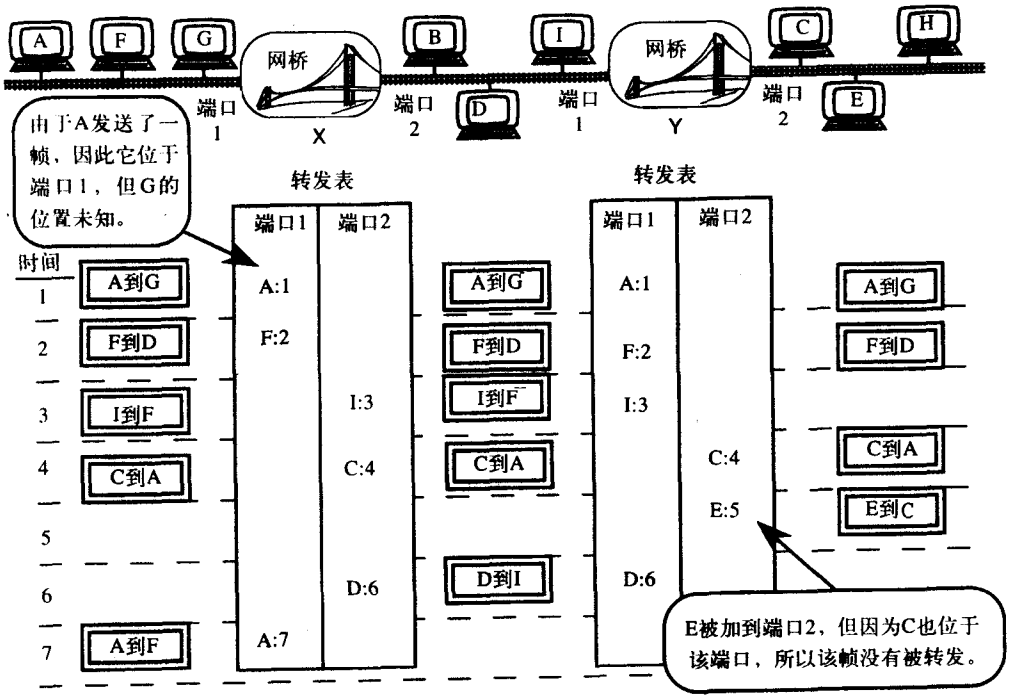


图24-5 网桥如何知道其端口上的地址。观察到帧的次数在冒号后给出

在图中有一个带有两个网桥的级联网络，时间单元如最左边所示。在各网桥下给出了其转发表，随着网桥学习各网段中节点的存在，这些表会变得越来越大。表中各项规定了哪些节点在哪个端口以及最后一次见到该节点的时间。网桥通过所发送的帧中的源地址来学习节点的位置。

首先，当网络上电后，网桥的表为空。当t＝1时，节点A向节点G发送一帧，于是网桥X就会在其表中增加一项记录，表示在t＝1时在节点A的端口1可以看到节点A。X不知道G的位置或是否已经上电，因此，它仅将该帧转发给Y，由Y以相同的方式处理该帧。因为没有节点知道该帧的目的地址，所以称该帧遍历了整个网络。

然后，F向D发送一帧，与前面的过程一样，有两个表进行了更新，只是这次t=2。接下来，I给F发送一帧，X和Y都接收到了该帧并对其进行过滤，但两者处理该帧的方式却不同。X知道F位于其端口1，所以它将该帧转发到该端口。与此同时，它将I位于端口2加入表中。而Y知道F位于其端口1，所以转向端口2的网段将该帧丢弃。

接下来，C向A发送一帧，使得各网桥都将C加入到其转发表中。此时两个网桥各自都有四个项目。注意，相对于X而言，I和C位于相同的网段或相同的端口。X在这个处理过程中不知道Y的存在。如果X和Y是路由器，它们就应该知道。同样，Y也不知道A、F和I存在于哪个网段。因此，X对Y是透明的。

在t=5时，E给C发送一帧。Y在其表中包括C，说明C也位于端口2，因此该帧被丢弃，不再进行转发。同样，当D向I发送帧时，两个网桥均将此帧丢弃，因为它们已经知道了I所在的端口。最后，当A给F发送帧时，X将A出现在端口的时间更新为7。如果网桥允许广播和组播模式，则那些信息同样会被转发，否则会被丢弃。

24.2.3 生长树算法

为了提供备用路由并增加网络的可靠性，必须在网路中加入环路，这样，当一条链路出现故障时，就可以利用其他可用链路。然而，对于带有网桥的网络可能会出现问题。

网桥W、X、Y和Z如图24-7所示相互连接。现在，我们只看该图上部所示的拓扑结构而忽略其余部分。假设位于网桥X端口1的一个节点（称为A）向位于其他网段的一个节点发送一帧，则X记录A位于其端口1并将此帧转发给Y，之后Y再将该帧转发给W和Z。现在所有这四个网桥都记录了A位于与其端口1相连的网络。当W复制的帧传到Z的端口3会发生什么情况呢？Z会记录A的位置由端口1转到端口3，并将此信息传给Y。Y也会记录此变化并将该帧发给X和W。这样，一帧就会产生更多的复制帧，而这些帧将在各网桥之间跳来跳去，从而造成网桥不必要的繁忙。所以，网桥的表并不会保持稳定。

因此，直到DEC的Radia Perman提出了生长树算法之后，网桥才能放在环路中。为了保证网络的可靠性，最好在网络中加入环路。这种方法是在网桥之间传送特殊的配置消息来确定网络的拓扑结构。链路被移走直到需要时再建立。各网桥将其自身设置在一个逻辑树中，其中只有一个网桥位于树根，其余的网桥形成了分级结构的树支。这样就消除了网桥网络中的环路问题。

在其他字段中，配置消息包含根网桥的ID、代价和发送网桥的ID。所有的网桥都有唯一的一个48比特的地址。当网桥发送配置消息时，它认为是树根的网桥以及距离该树根的逐跳次数均被编码在该消息中。网桥周期性地在它们之间发送这些消息以消除引入到网络中的环路。当一条链路出现故障并有备用路径可用时，这些路径或链路就会被该算法再次激活。

当网桥在其端口上接收到配置消息时，它将从这些可以发送的消息中确定最佳的消息。所谓最佳的消息是指根ID最小的消息。如果根ID号相同，就会用代价字段作为约束条件（tie breaker）。如果这些值仍然相同，则用发送网桥ID来确定最佳的配置消息。

如果一个端口接收到最佳配置消息，则该端口被认为是根端口。如果该网桥可以发送最佳消息，则它将认为自己是根网桥。如果存在这样的端口，网桥就不能向其发送出比接收到的消息更好的消息，则认为那些端口被堵塞了。但是如果存在网桥能向其发送更好消息的端口，则那些端口就可以包含在生长树之中。当端口包含在生长树中时，就可以在该端口接收

并转发数据；当端口堵塞时，则不能接收和转发数据。

例如，图24-6a给出的网桥，其ID－70，共有六个端口。该图还给出了到达各个端口的最佳配置消息。由于40-2-80（代表根ID、代价和发送网桥ID）比其他任何消息都小，于是该网桥确定端口4拥有最佳消息。端口1、5、6的消息较差，因为它们的根ID大于40。端口3也较差，因为虽然其根ID为40，但代价值大于2。端口2同样比端口4差，因为它的发送端ID较大，于是端口4被认为是根端口，因为在代价方面它与它所认为是根的网桥最接近。

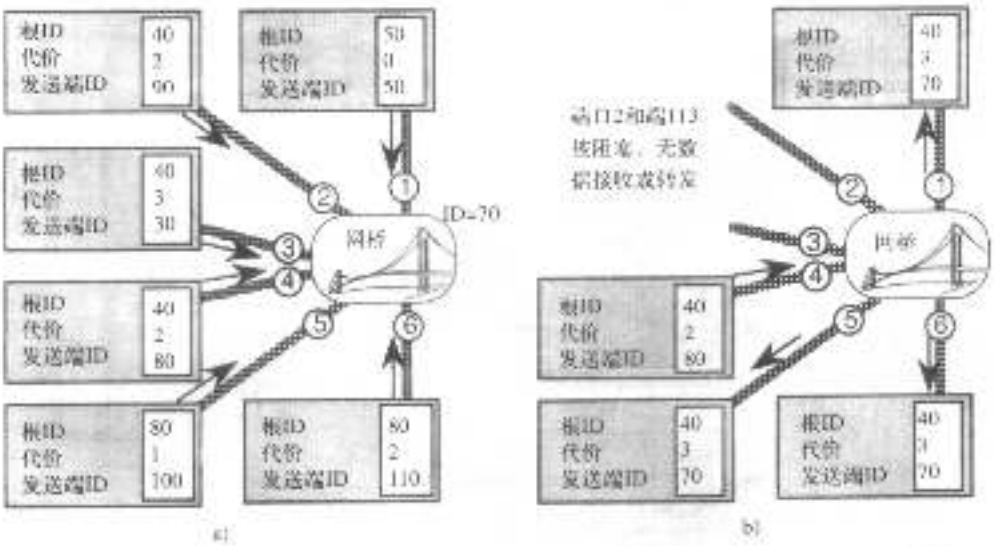


图24-6 a) 图示网桥的ID为70，它在其六个端口接收来自其他网桥的消息；b) 应用生长树算法之后，该网桥确定端口4最接近根，并且端口2和端口3会形成环路

于是该网桥确定它能发送的最佳消息是40-3-70，只比它在端口4接收到的消息多一跳，因为这个消息比它从端口1、5、6接收到的消息更好，所以它将给这些端口发送40-3-70，参见图24-6b。但是，来自端口2和端口3的40-2-90和40-3-30比该网桥发送的消息更好，所以这些端口被删除或被堵塞。虽然通过这些端口可以继续读入配置消息，但不能从这些端口读入数据或向这些端口转发数据。

图24-7说明网桥网络如何使用该算法删除环路。首先假定X认为它是根并在两个端口发送20-0-20消息，Y意识到它自己的ID 40比20差，所以它在其他两个端口发送20-1-40消息。该消息表明网桥40与它认为是根的网桥距离一跳。Y同时将端口1标记为根端口，因为它知道X是其端口1的根。同样，Z也在端口1和3发送类似的消息。

W接收到来自Y和Z的这些消息时，就认为自己比它们优越，因为其ID是10，于是W给Y和Z发送10-0-10消息。Y和Z便记录下根变为10，并且该根与它们相距一跳。X从Y接收到10-1-40并且从Z接收到10-1-30，它将Z看作是距离根最近的，从而决定它可以发送的最佳消息为10-2-20。这比它从40接收到的（10-1-40）要差，因此会将端口2阻塞并认为端口1是根。

Y也将端口2阻塞，因为它能发送的消息（10-1-40）比它在该端口接收到的消息（10-1-30）差，但它继续在端口1发送10-1-40。Z能够发送的消息（10-1-30）比从端口1和2接收到的消息都好，于是它就这样发送。

现在将网络图重新画为图24-7b，最后的根为10，并且所有的环路被删除。在W出现故障

的情况下，它将停止发送消息。其他网桥会确定W已经很长时间没有发送消息，于是它们认为W超时，并在没有W的新配置的情况下重复整个过程。但是如果W重新开始工作，则会自动恢复配置，而无需人为干预。

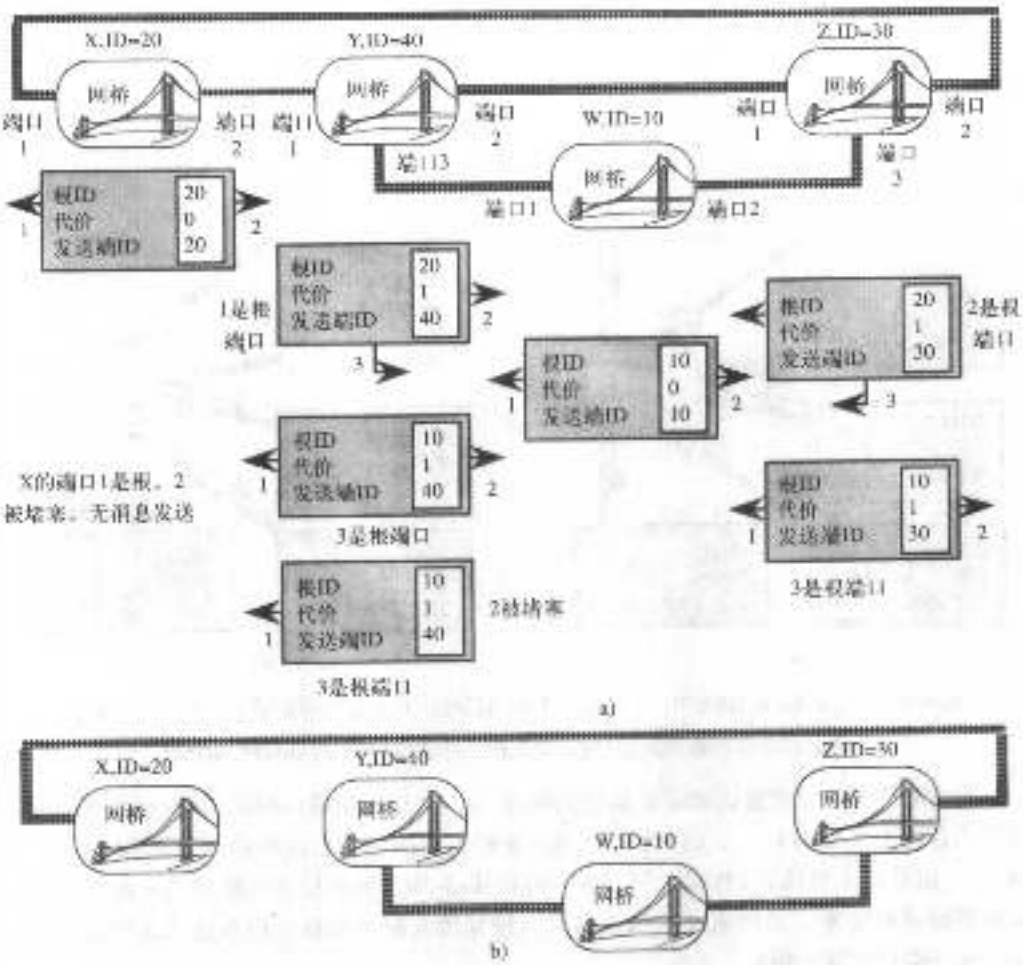


图24-7　a) 生长树算法中发送配置消息的过程，b) 删除所有环路后最终得到的网络

24.2.4　源路由网桥

与具有转发表的透明网桥不同，源路由网桥依靠帧的源地址来提供通过网桥的路径。当终端系统（主机）发送一个必须穿过几个网桥的帧时，它会在该字段中以适当的顺序对网桥地址进行编码来规定其必须执行的路由。通过这种方法，网桥便知道将该帧发送到哪个端口。

源路由网桥主要用在TRN（Token-Ring Network，令牌环网络）中，回到图23-16，注意到802.5帧允许使用RIF字段。如果源地址的I/G位（图23-7）被置为1，则RIF（Routing Information Field，路由信息字段）就会被使用；若该位为0，则不能在该帧中使用RIF字段。这一位可用来表示RIF字段的存在，因为即使一帧可以拥有组播目的地址，它也不能拥有多个站的源地址。

如果设备不知道到达期望目的节点的路由，那么它必须首先找到这一路由。该设备是通过发

送搜索帧来完成的，该帧也称为路由搜索帧。当各个网桥都向其他网桥发送此帧时，此帧会在网络中泛滥。网桥通过其端口转发一帧之前，它将自己的地址复制到该帧的RIF字段，最后很多这样的搜索帧到达目的地，由它决定两个端节点之间的最佳路径，通常这是根据最先到达的搜索帧决定的。之后，接收方仅向发送方返回一帧，于是发送方将定义到达该目的地的路径复制下来以备将来参考，接着它就可以发送它自己的消息。如果机器关机后又重新在线，则必须再次经历上述过程。我们可以看到，在每个网络中的各个站点执行路由搜索会在大范围的扩展LAN网络中产生过多的流量。

搜索帧有两类，一类是在所有方向上发送这些帧，称为全路径搜索；另一类是生长树搜索帧，只沿着生长树的树枝发送搜索帧。因此，有必要定义三种类型的RIF字段，一类是路由已知并明确规定其目的地，其他两类分别对应两种类型的搜索帧，网桥地址均集中在该字段中。

透明网桥与源路由网桥之间的几个区别在于，采用透明网桥时网络对于端节点而言只是一个单一的网络，也就是说网桥对于端节点来说是透明的。然而，源路由网桥对端节点不是透明的，端节点必须知道它们的存在并能处理源路由。虽然源路由网桥成本较低，但智能端节点的成本却远远超过了源路由网桥所节约的成本。透明网桥通常可以交换，而源路由网桥必须通过给每个网段和网桥分配一个唯一的编号来配置。在源路由网桥网络中寻找路由的计算是由端节点完成的，而在透明网桥系统中则是由网桥完成的。

最后，SRT（Source Route Transparent，源路由透明）网桥具有两类网桥的功能。根据IEEE标准，所有网桥都必须是透明的，源路由只作为一个附加特征。SRT网桥仅仅根据帧中源地址的组播位来决定该帧应使用透明桥接还是源路由桥接。

24.3 路由协议

24.3.1 路由、路由协议和可路由协议

本节讨论路由协议及其工作方式，路由协议、可路由协议和路由本身是不同的术语。路由器（router）是互联LAN时使用的分组交换机，其中包括路由表，路由表用于决定如何将接收到的数据报（或分组）转发到下一个目的地址，这就称为路由（routing）。路由仅仅是在路由表中寻找路径从而将数据报发往下一个路由器或端系统的过程。

路由本身相对于产生路由表的过程要简单很多。路由表（routing table）产生和更新的方法称为路由算法（routing algorithm），而其特定的实现则称为路由协议（routing protocol）。路由协议仅存在并工作在路由设备中，而诸如IP（Internet Protocol，网际协议）、NetWare或DECnet等网络协议是可以通过路由器进行路由的，称为可路由协议（routed protocol）。下面详细讨论路由协议RIP、OSPF和BGP。

24.3.2 距离矢量路由与RIP

基本算法：第一个得到广泛使用的路由协议称为RIP（Routing Information Protocol，路由信息协议），它最初于1980年使用在XNS中，现在主要应用在Unix中。RIP属于一类被称为距离矢量路由的路由算法，即到达目的地的最佳路径是跳数最少的路径，然而，最佳路径也可以由除跳数以外的其他度量指标决定。既然RIP是一种规定路由表如何建立的路由协议，下面就看看它是如何处理这一过程的。

RIP的基本思想是各路由器首先确定与其相邻的路由器。接着每隔30s向其相邻路由器发送一条更新消息。路由器每次从它的一个邻居接收到更新消息后，就查看该相邻路由器能够达到的地址及其各自的距离。如果相邻路由器能到达一个它现在无法到达的目的地，它就会将该目的地增加为可以到达。同时该表中还包含到达不同节点的距离。与目的地之间的距离是以跳数来衡量的。

如果另一个相邻路由器可以以较少的跳数到达某目的地，它也会将该路由器加入到路由表中。如果到达某目的地所需的跳数超过15，该目的地就不会进入路由表，从而被认为是不可到达的。因此，RIP只适合那些在两个节点间的路由器数不超过15的网络。当网络“直径”超过该值时，必须借助于其他协议，下面通过一个例子来看看RIP是如何工作的，之后由所遇到的问题给出精简的描述。

举例：图24-8a给出了从A到D的四个网络，由三台路由器（R1到R3）相互连接在一起。本例说明了通过使各路由器相互发送更新消息，RIP如何在各路由器中建立路由表。各路由器下图示出的路由表有四列，更新消息列在它们所经过的网络下面。

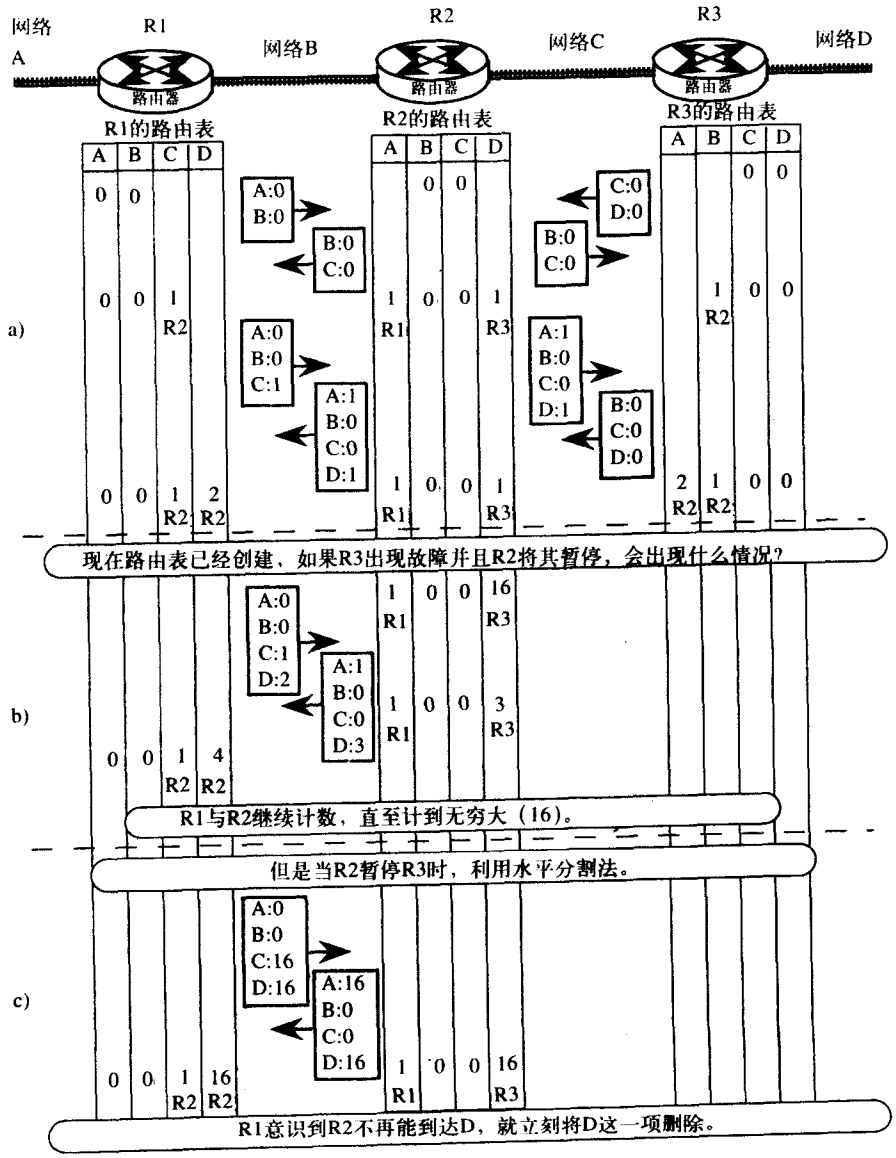


图24-8　a) RIP（Routing Information Protocol，路由信息协议）的基本工作方式；b) 计数到无限的问题；c) 利用水平分割后很快出现收敛

最初，除了与它们直接相连的网络之外，路由表是空的。例如由于网络A和B直接与R1的端口相连，因此R1加入到路由表中到达网络A和B的距离或代价是0；R1还不知道C和D的存在。

经过30s后，所有路由器给其相邻路由器发送更新消息。R1通知R2它可以以0跳的代价到达A和B，R2分析这一消息后放弃关于R1可以直接到达B的信息，因为它自己也可以直接到达B。然而，R2得知R1可以直接到达A。所以它将A加入到其路由表，并且所加入的代价比R1大1，这是因为R1与R2之间的距离为1。现在R2也可以以代价1到达A，这样，发送完第一轮更新消息之后，R2就可以到达所有4个网络，而R1和R3只能到达其中3个网络。

直到另一个30s之后，R2发出另外一组更新消息，R1和R2才发现它们可以到达远端的网络。换句话说，R1从R2得知R2可以以代价1到达网络D，于是R1将D加入其路由表，使其代价值为2。类似地，R3以代价2将A加入其路由表。现在称网络是收敛的，即所有路由器拥有如何到达网络中的所有可达目的地的适当信息。

计数到无限：现在，如果R3无法工作会出现什么情况？怎样通知R1？如果没有通知R1，它将给R3发送数据报，但未必占用网络带宽。为了避免这一问题，即使发送方的数据库未变，RIP也要求每隔30s发送一次更新消息。这样，每个路由器的路由表都是最新的，并为表中每个条目设置一个计数器。

如果路由器连续180s没有从网络中接收到其路由表中的某个确认信息，它会将跳数设为16，表明该网络不可达。再经过120s之后，如果它仍然没有收到消息，它将从表中删除该项，这称为垃圾收集（garbage collection）。垃圾收集可以防止“无法到达该网络”的消息占用网络带宽，这在稍后就变得没有必要了。

参见图24-8b，我们看到当R3无效时的另一个问题，这时R2不能收到来自R3的任何消息。经过180s之后，它将D的代价值设为16，即不可达。下一次R2给R1发送消息时，说明其到D的代价为16，即被认为是RIP中的无限。然而，R2知道R1能够以代价2到达D，却没有意识到R1是通过自己到达的D，R2仅仅更新自己的数据库，将到达D的路由代价设为3，比从R1到达D的代价大1。

接着R1从R2了解到R2到达D的代价是3，因此，R1更新其到达D的代价为4之后，R2又将其代价增加为5，直到两台路由器中到达D的代价都为16并且两者均超时为止。这称为“计数到无限”，它是由路由环路造成的。这里，网络已经慢速地收敛或稳定，因为R1认为自己可以通过R2到达D，R2又认为自己可以通过R1到达D。因此，RIP有目的地将无限计数值设为16。

分割水平线：为了避免路由环路，采用一种称为分隔水平线的技术，该技术避免了路由器向其接收开始信息的相邻路由器发送更新消息。比如，由于R1第一次是从R2获得对D的可达信息的，因此R1不能向R2发送该消息。因此，如果像图24-8b所示的那样，R3出现故障，不发送值为16的代价，R2将根本不发送网络D的条目并让R1暂停D，这样每台路由器就确认了对某个节点的不可达性。

RIP事实上使用了一种称为有害相反分割水平面法的机制。图示说明见图24-8c。图中R2并非不发送D的条目而是发送一个代价为16的条目。R1一旦注意到R2到达D的代价增大为无限大，并且R2知道了它的路由，就认为16“有害”并立刻将关于D的条目删除。这样就可以迅速收敛，而且可以防止R1给其他节点发送错误信息。同时注意到R2发送给R1关于A的代价为16，这是因为R2是从R1获得该消息的。

然而，对于其他配置而言，在RIP中仍存在路由环路，比如当R1认为它可以通过R2到达D，

R2认为它可以通过R3到达D并且R3又认为它可以通过R1到达D时，就存在这种环路。这里，称为触发更新的机制将及时发送关于拓扑结构的新信息以减少环路问题。即使当这种方法不起作用时，通过计数到无限仍然可以获得不可达性。

24.3.3 链路状态路由和OSPF

链路状态协议：链路状态路由协议有两种类型，即OSPF（Open Shortest Path First，开放最短路径优先）和IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）。尽管它们各有优缺点，但这里我们将主要介绍OSPF。但是，必须注意到，对于其中一种类型的详细讨论并不表示它比另一种好，只不过是让我们能够更深入地研究相关概念而已。

在距离矢量算法中，我们看到各节点是如何将其整个路由表仅发送给其相邻节点的。这使得网络收敛速度较慢，其原因是彼此相距许多跳的两台路由器直到中间路由器已经更新并转发它们的路由表之后才会知道对方的存在。

采用链路状态路由协议后，上述情况就发生了改变。各路由器不是将整个数据库的信息仅发送给其相邻路由器，而是将关于其相邻路由器的信息发送给互联网上的所有节点。当两台远距离端路由器之间的中间路由器建立路由表时，为端路由器建立路由表的信息已经在传输中，这使得网络收敛非常快。而且在发生变化时，发送给所有节点的仅仅是该变化而不是整个数据库。OSPF就是执行这种链路状态路由算法的路由协议。

在RIP中两台路由器之间的代价以跳数计算，与此不同，OSPF允许根据很多称为度量标准的链路特征来选择路径。这些度量标准是根据可靠性、延时、带宽、链路代价、链路负载和其他一些项目来规定的。这些度量标准中的许多标准是相互依赖的，这取决于网络的配置。在某种情况下，可靠性可能是最重要的标准，在另外一些情况下，代价或其他标准可能是最重要的标准。使用OSPF，我们就可以根据这些度量标准而不仅仅是跳数来选择两点之间的代价。

OSPF路由表：图24-9中给出了一个利用点到点链路的路由器组成的网状网络。对于路由器而言，了解它们的相邻路由器是很重要的，这可以通过问好协议（Hello protocol）实现。最初各路由器向其各相邻路由器发送一个问好分组（Hello Packet），通知对方自己的路由器地址。周期性地发送这些问好分组来检测相邻链路的变化，并且接收路由器不会将这些分组转发出去。例如，R1将通过其各接口向R2和R3发送问好分组，当它们返回包含R1地址的问好分组时，R1就会与它们建立双向通信链路，此时将建立起链路的代价。

各路由器一旦确定下来自己的相邻路由器，相邻对就会同步它们的数据库。于是，LSA（Link State Advertisement，链路状态广告）就会大量地涌入网络。LSA是各路由器发送的规定其当时链路状态的信息分组。

图中显示了在链路初始化后各路由器发送的四个LSA。例如R1向所有节点广播其数据库（说明R2和R3分别与它相距4个和1个单元）。因此，即使R4没有与R1直接相连，它也会很快接收到该LSA。这些LSA同时涌入各个方向。但是，为了方便解释，我们假设各LSA每次只到达其他路由器中的一个，这将帮助我们了解“最短路径”路由表是怎样建立的。

最初，R1不知道R4的存在，但是，当它接收到R2的LSA时，就会计算出到R4的代价为7，到R2的代价为4，进而再计算出到R4的代价为3。R2一旦接收到R1的LSA后，便注意到R1和R3之间的代价仅为1，所以它选择到达R3的最短路径通过R1，因为5（即4+1）比直接到达R3的代价（即6）要小。

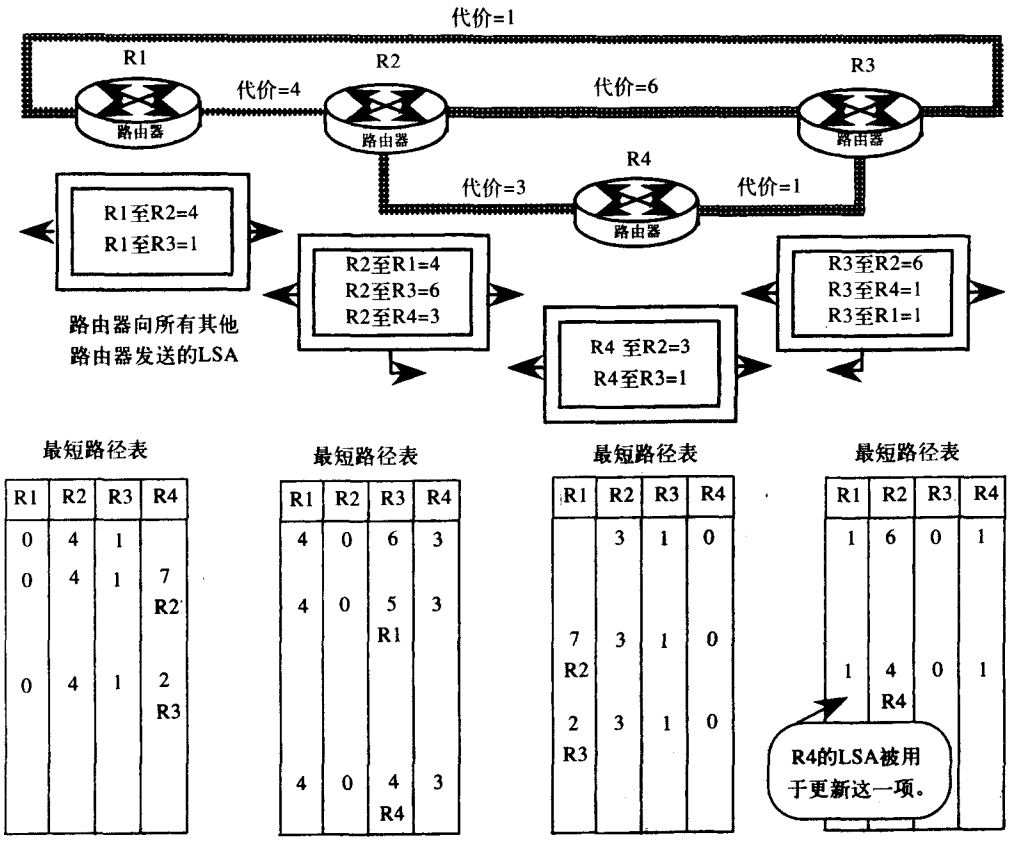


图24-9 当来自不同源的LSA（链路状态广告）到达多个目的地时，各路由器的最短路径表就建立起来了。表中各项下的路由器编号表示路径不是直接路径，而是下一跳的路由器名。在本例中，它还表示LSA被用于更新特定表项的路由器

假定R4首先接收到R2的LSA，并注意到现在以代价7也可以到达R1。接着R3一接收到R4的LSA后，就将其通过R4到达R2的代价更新为4（即3+1），比直接到达R2的代价小。类似地，R1利用R3的LSA，将到达R4的代价调整为2。同样，R4也进行类似的调整。最后，R2将其通过R4到达R3的代价调整为4。

这里，每台路由器均建立了描述网络拓扑结构的相同的链路状态数据库。利用该数据库，各路由器创建了相对自己的、基于最短路径树的路由表。各路由器的路径树都是以其自身为树根得到的。

多用户访问网络：在上一节中，只能有一对路由器可以通过网络或链路相互通信。参见图24-10，R4、R5和R6可以通过以太网彼此相互通信，并且它们能够利用PSN（Packet Switched Network，分组交换网络）和其他路由器通信。以太网和交换网都被称为多用户访问网络（multiaccess network）。它与多站网络（multidrop network）不同，多站网络中每一点仅能对一台控制器进行直接访问。在多用户访问网络中，每台路由器可以与其他任何路由器直接通信。交换网是典型的非广播网络，而以太网则是广播型多用户访问网络。

在多用户访问网络中，各路由器并不建立与其他路由器的相邻关系，而是基于它们的ID选择DR（Designated Router，指定路由器）。同时选择一台BDR（Backup DR，备用指定路由

器），在DR出现故障时替代DR。接着，各路由器只与DR建立相邻关系，这就消除了与各路由器的一对多组合，大大减少了网络中没有必要的协议通信。之后DR为其网络分配一个名字，这其中包括它自己的名字。图中，R4被选为两个网络的DR，并且它分配给交换网络的地址为R4.1，分配给以太网的地址为R4.2。于是DR代表网络和它本身发送LSA，这样各台非DR路由器只公告它仅与自己的网络有链路，而与网络中的其他所有路由器均无链路。

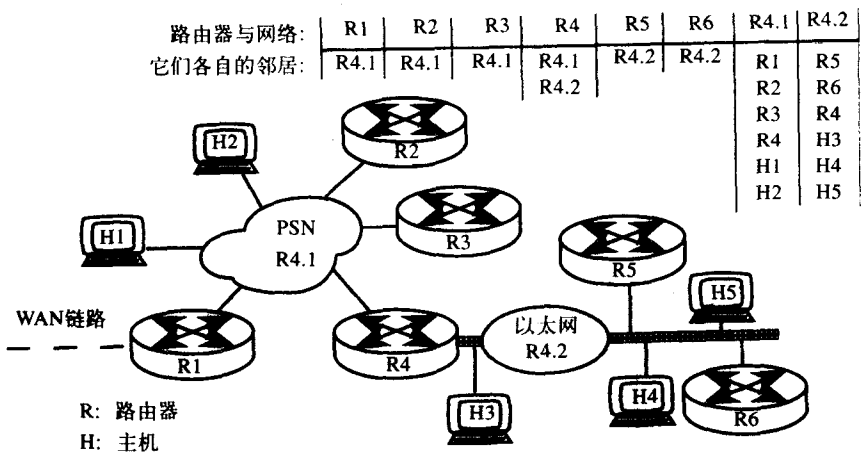


图24-10　在多用户访问网络中建立邻居

图24-10中的表说明与R4.1网络相连的链路是由R1到R4公告的，与R4.2网络相连的链路是由R4到R6公告的。R4.1公告自己有与R4到R1以及主机H1和H2相连的链路。类似地，R4.2也公告了一系列的路由器和主机，R4、R4.1和R4.2的LSA传输都是通过R4处理的。

现在，如果R1接收到来自其WAN链路的并且必须转发给交换网络中的所有路由器的LSA，R1就会将该LSA组播给DR和BDR，之后DR又将它组播给R1到R3，并等待对该LSA的显式确认。对于不提供确认的路由器，R4将通过数据链路层重新发送该LSA。

OSPF区域：当越来越多的路由器加入到互联网时，路由器之间的路由流量急剧增加，消耗大量的网络带宽。无论选择何种路由算法，最终必须将互联网划分为更小的网络，称之为区域。这样，路由协议的备份就能够在所有区域中独立地工作，并且大量的路由流量均发生在区域内部。

在某个区域内的所有路由器都有它们自己的数据库，如果发生变化，这一变化仅被传播给该区域内的所有路由器。这就将LSA流量仅限制在有关的区域，从而降低了区域之间的流量。以上是对1级区域的介绍。

然而，为了提供对1级区域以外的路由器的访问，采用2级区域将它们互联起来。图24-11给出了将两个1级区域分层互联起来的2级区域（称为骨干区域）。虽然所有这些路由器都可以运行OSPF协议，但可以将它们分为4种类型的路由器，图中也给出了各路由器的类型。

内部路由器（R2、R5、R6、R8、R9和R10）除了与其自己的区域直接相连外，与其他任何区域没有直接连接。骨干路由器（R1到R4、R7）是与骨干网有接口的路由器。区域边界路由器（R1、R3、R4和R7）是一种至少与两个区域相连接的骨干路由器。最后，AS（Autonomous System，自治系统）边界路由器是与其他被称为AS的更高级区域相连的路由器。下面将简要介绍AS。

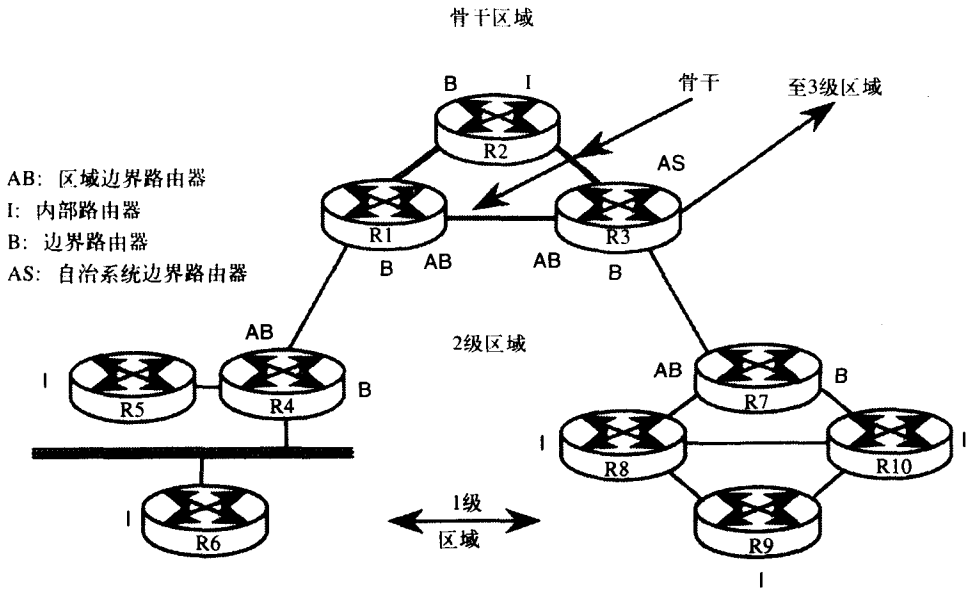


图24-11 OSPF路由器的类型

IS-IS：OSPF实际上来源于IS-IS，所以两者十分相似。IS是指OSI中的路由器，而ES（End System，端系统）是指端主机节点。虽然OSPF仅路由IP协议，但因为它是封装在IP数据报中，所以IS-IS可以对所有可路由协议进行路由。它是由Radia Perlman领导的DEC公司从事OSI CLNP（ConnectionLess Network Protocol，无连接网络协议）的研究人员设计的。

当某个网域被分割开，比如说是因为失去关键链路而被分割开的，IS-IS就可以使用虚拟链路自动进行修复，而当采用OSPF时，虚拟链路必须人工设置。IS-IS中对于确认分组而言，每条链路都有不同的密码进行发送和接收，但在OSPF中只使用一个密码。因为OSPF只路由IP数据报，所以它对路由而言是最优化的，而IS-IS则对存储和处理需求是最优化的。在任何情况下，选择路由协议都需要在上述问题之间进行权衡折衷。最后，IS-IS可以使用在AS之间及AS内部的路由，但OSPF只能用于AS之间的路由。

24.3.4 自治系统和BGP

在因特网的早期，ARPANET作为骨干网传输长途流量。骨干网称为因特网的核心，其路由器称为核心网关。分级连接在这些核心网关上的其他路由器称为外部网关。外部网关是进入称为AS（Autonomous System，自治系统）的其他网络的接入点。参见图24-12a。

由于AS是由大量的网络和路由器组成的，并由诸如大学之类的单个机构单元管理，因此它通常是由一个实体维护和付费。它会尽量避免其他AS中出现的路由问题。必须向DDN（Defense Data Network，美国国防部数据网络）的NIC（Network Information Center，网络信息中心）申请获得AS号。正如在关于OSPF一节中所讨论的那样，在一个AS内部可以有2级区域和1级区域。在那种情况下，AS之间的路由可以认为是3级路由。

传统上，AS之间的路由是由核心网完成的。但随着因特网的发展，核心网变得越来越拥挤而难以管理。现在我们以前所说的核心网已经不存在。AS之间彼此直接相连，这使得这个高层网络拓扑变成水平的而不是分级的。如图24-12b所示，虽然仍使用AS这一术语，但正确的术语应该是域（domain）。

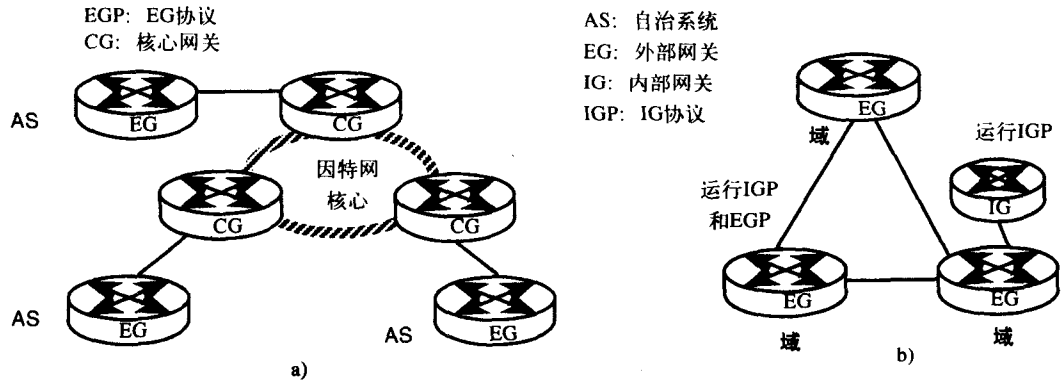


图24-12　a) 传统上，当AS连接到核心上时，就形成了因特网的分级结构；
b) 目前，AS也称为域，它们彼此之间可以直接访问

在域间交换流量的路由器称为域间路由器（或网关）。它们使用一组称为域间路由协议或简称为EGP（Exterior Gateway Protocol，外部网关协议）的路由协议。用在一个域内的路由协议称为域内路由协议或IGP（Interior Gateway Protocol，内部网关协议）。RIP和OSPF均是IGP的实例。

EGP的例子包括BGP（Border Gateway Protocol，边界网关协议）和本身就称为EGP的协议。因此，EGP既可以指一组域间协议又可以指名为EGP的协议。

BGP是一个距离矢量算法。通过该算法，两个相邻域之间的所有外部网关使用全连接的网状拓扑相连。它们使用TCP（Transmission Control Protocol，传输控制协议）在彼此之间传送可靠信息。BGP提供了比OSPF更加强大的分组认证方法。这实际上更好，因为这种在各网络中保持安全性的方法是秘密的。

路由信息块在发送时，在其路由路径中列出了AS号，从这个意义上，BGP采用的是源路由。所有消息在其头部都有一个称为标志的16字节字段，它保留用作认证，可能的话使用数字签名机制。BGP使用OPEN、UPDATE、NOTIFICATION和KEEPALIVE消息。

当两台路由器首次连接时使用OPEN消息，除了用于认证的头部标志外，该消息本身还有另外13个字节，留作将来认证方法的实现。它同时提供AS号并规定保持时间，这指接收方从相邻网关得到消息的时间间隔。当路由器没有消息发送时，它会发送一条仅包含19个字节的BGP消息头的KEEPALIVE消息。这可以防止连接路由器将发送路由器暂停。

UPDATE消息用于传输路由信息，它指出该信息是来自内部网关协议还是BGP或者其他方式。同时，它还与其他属性共同规定了AS路径和路径上的下一台路由器的地址。最后，当一台路由器想要中断与其相邻路由器的连接时，它会发送一条NOTIFICATION消息指出原因。

24.4　路由器配置

现在让我们将重点从算法转移到实际当中设置路由器的协议上，下面列出Cisco公司的具有两个端口的 M－Chassis型路由器的配置。这决不是一个训练指导，而仅仅是在配置一台典型路由器时所要完成的任务的浏览。这里我们还将使用一种特定产品进行讨论以使解释更有意义。应该向读者说明的是，这里使用Cisco路由器进行介绍并不是说其他路由器质量不好。事实上，每个供应商都有一组独特的特点和服务，用户在形成某种观点之前必须仔细地评估。这里说明一种特定的产品如何工作会使学习其他供应商的产品变得更容易。

这台双端口路由器将一个孤立的以太网LAN连接到因特网。因此，为了进行安装，需要从网络管理员那里获得两个因特网地址（每端口一个）。首先，在工作台上对其进行配置，将一台ASCII终端连接在其终端端口上，以太网端口不连接任何东西。接着将其带到现场，安装两个以太网连接并加电，这之后它将运行Cisco的IGRP专用路由协议，如果一切正常的话，我们就不需要再做其他任何事情。

这台路由器在后面板上有两个以太网接口，它们都连接到内部的以太网板上。该路由器还有一个处理器板。这个处理器板在针对9处有一个跳线，如果路由器要在本地启动还应该在针对1处有一个跳线。如果启动是脱离网络完成的，则（对于CSC3处理器板而言）应该在针对3处跳线。在以太网板上有双列直插式开关，它必须根据以太网板在底板上的插槽位置来设置。下面我们打开机器!

在所连接的终端上会显示:

```
CSC3 (68020) processor with 4096k bytes of memory.
1 MCI controller (2 Ethernet, 0 Serial)
2 Ethernet/IEEE 802.3 interface
32k Bytes of non-volatile configuration memory
4096k bytes of flash memory on MC+ card (via MCI)
```

该信息说明这台机器（即路由器）使用Motorola公司的具有4KB RAM的 68020 微处理器，它支持两个以太网接口，还有32KB非易失性存储器和4KB闪存EPROM。 闪存EPROM在机器内就可以编程而无需将其取出编程。

接着它将询问:

```
Would you like to enter the initial configuration dialogue?[yes]:no
```

方括号内为缺省设置，此时我们选择no。之后会出现带有供用户接入的路由器名的提示符。用户接入显示为“>”，输入“enable”我们会获得优先接入，显示为“#”。这在稍后是受到密码保护的。接着键入“setup”，就能够完成如下所示的配置对话框:

```
Router>enable
Router#setup

Configuring global parameters:

Enter host name: matchbox
Enter enable password: matchhead
Enter virtual terminal password: matchstick
Configure SNMP Network Management? [yes]: no
Configure IP? [yes]:
    Configure IGRP routing? [yes]:
          Your IGRP autonomous system number [1]:
Configure DECnet? [no]:
Configure XNS? [no]:
Configure Novell? [no]: yes
Configure AppleTalk? [no]: yes
  Multizone network? [yes]:
Configure CLNS? [no]:
Configure Vines? [no]:
Configure bridging? [no]:

Configuring interface parameters:

Configuring interface Ethernet0:
    Is this interface in use? [yes]:
    Configure IP at this interface? [yes]:
          IP address for this interface: 128.6.1.1
          Number of bits in subnet field [0]: 8
```

```
        Class B network is 128.6.0.0, 8 subnet bits;
          mask is 255.255.255.0
    Configure Novell on this interface? [yes]:
        Novell network number [1]:
    Configure AppleTalk on this interface? [yes]:
        Extended AppleTalk network? [yes]:
```

全局参数的设置决定了我们在设置各个端口时使用哪种协议。例如，因为在全局设置中Novell被设为“yes”，所以在建立以太网接口0时会询问我们有关设置。IP地址和掩码的概念在第8章中介绍过。与该接口的设置方式相同，可以设置以太网的端口1，对话框的最后将出现如下问题：

```
Use this configuration? [yes/no]: yes
```

此时这一图片被存储在非易失性EPROM中。它被保存为命令脚本。在每次启动时使用。当然，它可以被改变。这些参数及其设置在设置对话框中产生时就被存入一个称为命令脚本文件的文件中，简单地键入以下命令就可以查看该脚本文件：

```
matchbox#write terminal
```

注意到提示符说明了设置时指定的路由器名称。如果键入下述文字，我们就会看到特定接口发出的信息：

```
matchbox#show interface ethernet 0
Ethernet 0 is administratively down, line protocol is down
Hardware is MCI Ethernet, address is 0000.0c03.e1f8
MTU 1500 bytes, BW 10000 kbit, DLY 1000 usec, rely 255/255,
load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10sec)
ARP type: ARPA, ARP timeout 4:00:00
Last input never, output 0:27:17, output hang never
Last clearing of "show interface" counters never
Output queue 0/40, 0 drops, input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec,
      0 packets/sec 0 packets input, 0 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
            0 abort
      26 packets output, 5193 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface reset,
            0 restarts
```

注意到此接口处于关闭状态，它的MAC地址是0000.0c03.elf8。这个硬件地址可以保存在网络服务器上，该服务器利用ARP（地址解析协议）将MAC地址映射为IP地址。最后的输入字段表示数据最后接收到此端口的时间，最后的输出字段表示最后发送数据的时间，这些在调试时非常有用。其他字段提供关于此端口活动的其他数据。

如果键入“configure”，就可以唤醒该接口，如下所示：

```
matchbox#configure
Configure from terminal, memory, or network? [terminal]:
Enter configuration commands, one per line.
Edit with DELETE, CTRL/W, and CTRL/U; end with CTRL/Z
interface ethernet 0
no shutdown^Z

matchbox#
```

现在如果键入“show interface ethernet 0”，我们会看到以太网0没有关闭并且线路协议正在运行，这是因为我们进行了“no shutdown”的操作。configure命令改变RAM中的设置，但

并不是为了启动。如果从非易失性存储器引导系统启动，则键入“write memory”将那些变化保存在非易失性存储器中。

至此，我们基本上完成了设置过程。现在就可以连接路由器，希望它能够正常工作。如果出现问题，我们可以从操作间远程登录到机器上（这就好像我们在现场一样），并执行与前面介绍的相类似的任务。

习题

1. 下列哪个设备工作在OSI模型的物理层？
   a. 中继器　b. 网桥　c. 路由器　d. 网关
2. 下列哪个设备不会隔离两个网段之间的流量？
   a. 中继器　b. 网桥　c. 路由器　d. 网关
3. 经过下列哪个设备时第二层的帧头发生改变？
   a. 中继器　b. 网桥　c. 以太网交换机　d. 路由器
4. 骨干网崩溃有什么缺点？
   a. 安全性差　b. 难以维护　c. 依赖于单个设备　d. 难以管理
5. 哪种类型的网桥网络需要发送节点知道路径上的网桥地址？
   a. 学习网桥　b. 封装网桥　c. 源路由网桥　d. 转换网桥
6. 哪种域内路由协议要求各节点向其相邻节点发送有关网络的信息？
   a. RIP　b. OSPF　c. IS-IS　d. BGP
7. 哪种域内路由协议要求各节点向所有节点发送有关其相邻节点的信息？
   a. RIP　b. EGP　c. IS-IS　d. BGP
8. 哪种类型的第二层设备将一种帧格式转换为另一种帧格式？
9. 哪种类型的第二层设备既执行电路交换又执行分组交换？
10. 查找路由表并将分组发送到正确的路由器的过程称为什么？
11. RIP以怎样的频率发送更新消息？以跳数为单位，可能的最大网络直径是多少？
12. 在RIP中，两个节点不断地增加到达某故障目的地的跳数直至加到16，这称为什么？
13. 给出两个链路状态路由协议的实例？
14. 哪种路由协议使用源路由？
15. 在配置路由器之前，必须知道哪些地址？
16. 基于路由器的网桥有什么优点？
17. 基于网桥的路由器有什么优点？
18. 用一两句话描述一下本章介绍过的各种类型的网桥。
19. 列出崩溃的骨干网的优点。
20. 描述生长树算法怎样消除网桥网络中的环路？
21. 什么是分割平面？
22. 建立OSPF区域的目的是什么？

第25章 TCP/IP：其他的概念

25.1 简介和回顾

在1974年，Vinton G. Cerf和Robert E. Kahn在《IEEE Transactions of Communications》杂志上发表的一篇文章中提出了一套协议设计方法。该协议在不考虑网络接入协议或网络设备供应商的情况下，能够使多种不同类型的网络相互连接。美国国防部（DoD，Department of Defence）有一个需求，那就是要把分属于如美国国家科学基金会（NSF，National Science Foundation）、美国宇航局（NASA，National Aeronautics and Space Administration）及各种研究和教育机构等不同组织的网络相互连接在一起。正是因为这个需求，DoD通过美国国防部高级研究计划局（DARPA，Defense Advanced Research Projects Agency）为BBN(Bolt，Beranek和Newman)这三个人提供资金，让他们根据上述的那篇论文来实现一套网络互连的协议。

TCP/IP协议首先是在BSD（Berkeley Software Distribution，伯克利软件分布）的Unix平台上实现的，也正是由于这个原因，Unix操作系统在TCP/IP中还发挥着非常重要的作用。虽然现在这些协议已经在许多操作系统中实现了，但是本章讨论的内容主要是基于UNIX操作系统。与其他操作系统不同，UNIX 是用高级的程序设计语言编写的，这使它可非常方便地移植到各种类型的硬件平台中去。此外，UNIX本身比其他任何操作系统对网络的互联贡献都要大。

在第8章，已经非常详细地介绍了TCP/IP。在图25-1中，可以看到TCP/IP结构是如何被分为4个层次的。这4层分别是网络接入层、网际层、传输层和应用层。如果物理层使用的是以太网协议，并且头部信息的类型字段值是0800（十六进制），那么这就决定了它的数据部分是一个IP数据报。IP头中的协议编号决定了它的数据部分是否转发给ICMP、ICP、UDP等协议。最后，在TCP或UDP头中的端口号决定了在数据部分携带的是那一类应用的数据。这些协议之间的相互联系和它们的特性都已经被详细地讨论过了。

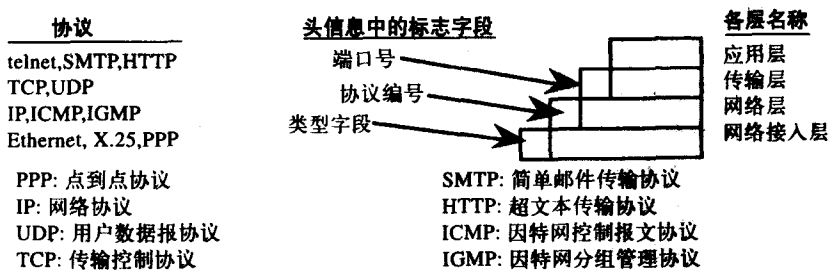


图25-1 TCP/IP协议的网络结构

这一章将尽量避免重复。如果你忘记了前面讲过的一些内容，可以回到前面的章节复习相关的知识。这里将从最低的网络接入层开始，通过协议栈向上攀升，讲述第8章中没有涉及到的内容。这次，我们将全面地学习主要协议内容以及它们是如何使用的。

25.2 网络接入层

25.2.1 地址解析协议（ARP）和反向地址解析协议（RARP）

Internet标准（草案）RFC 826、903和1700详细地描述了这两个协议。反向地址解析协议（RARP，Reverse Address Resolution Protocol）常用在无盘工作站或X终端设备上。这些设备上由于没有硬盘，因此它们不能像其他的主机那样读取存储在硬盘上的IP配置文件。如果它们不知道自己的IP地址，就不能连接到网络上。要连接到网络上，首先要做的是从它的NIC(网卡)上读取它的MAC地址（或称为硬件地址），然后用广播方式将这个地址告诉网络上所有的主机。这个广播包中的意思是："谁知道我的IP地址？"这就是所谓的RARP请求。

在网络上会有一台服务器保存着一张列表，表中列出了整个网络中每一个MAC地址所对应的IP地址。在收到RARP请求之后，该服务器会给无盘工作站发送一个单播的RARP响应，告诉它正确的IP地址。然后这个工作站就可以正常工作了。

图25-2给出了ARP、RARP信息包的格式。最左边的一列给出了每个字段所占用的字节数，接下来的一列给出了各个字段的名字。最后的两列给出了这些字段的应用例子以及相应的描述。以后每当需要描述协议的头信息时，将遵循这种格式。

字节数	字段名称	例子	描述信息
2	Hardware Type(硬件类型)	0001	硬件是Ethernet、LocalTalk或者其他?
2	Protocol Type(协议类型)	0800	使用的是IP或其他的地址协议?
1	Hardware Length(硬件长度)	06	硬件地址占用的比特数
1	Protocol Length(协议长度)	04	协议地址占用的比特数
2	Operations(响应操作)	0001	
可变长度（6）	Source HW Address(源主机的硬件地址)	00aa0001bfdc	这是一个ARP还是RARP信息，是请求信息还是响应信息?
可变长度（4）	Source IP Address(源主机的IP地址)	abcdef02	
可变长度（6）	Target HW Address(目的主机的硬件地址)	000000000000	
可变长度（4）	Target IP Address(目的主机的IP地址)	abcdef01	

图25-2 ARP和RARP的头字段。圆括号中的数字表示用在以太网上时所需要的字节数

以太网的帧头在图中没有显示出来。对于ARP协议，十六进制的以太网的帧类型（frame type）值是0806；而对于RARP协议，是0835。ARP和RARP不仅可以用在以太网和IP协议中，而且还可以用在其他的协议中。硬件类型由头信息的前两个字节给出。对于以太网来说，该值为1；对于IEEE的802协议，该值为6；而对于帧中继，该值为F。

IP协议的协议类型值为0800。由图25-2所给的数据包的例子可知，硬件类型是以太网，而使用的协议类型是IP协议。因此，硬件地址的长度是6个字节。这48个比特与以太网的MAC地址相匹配。而对于IP地址，协议的长度是4个字节，即32个比特。

接下来的操作（Operation）字段表示出所携带的数据包的类型。对于一个ARP请求信息包，代码是1；而对于ARP应答包，代码是2。对于RARP请求包，该值是3；对于RARP应答包，该值是4。最后，给出的是硬件地址和IP地址。由于在这个例子中的操作字段的值为1，因此它是一个ARP请求包。在这个信息包中，源主机会尽力去寻找目的主机的硬件地址。因此，现在目的主机的硬件地址段是空的。

25.2.2 代理ARP

代理ARP是既简单又微妙的方法，它可以用来确定本地主机和所要到达的远程主机之间

使用的网关。远程主机通常是指与本地主机不在一个子网上的一台主机，即代理ARP是一种避免出现大量的静态路由的方法。

“代理”ARP是一种响应ARP请求的方法（而不是一个协议）。通常可以给它规定正确且适当的行为。

在代理ARP中，如果网关发现ARP请求的IP地址不在本地网络上，并且知道如何到达IP所在的那个网络，它会响应并返回一个ARP响应。但是在返回的ARP响应中，网关用自己的以太网地址代替远程主机的以太网地址。因此，使用“代理”这个词。实质上，网关欺骗了提出ARP请求的主机，并使主机认为网关就是远程主机。

下面是在主机上输入的标准Unix路由命令：

```
route add default <my_own_ip_address> 0
```

这实际上暗指整个世界的网络都与本地以太网连接在一起。“route add”这条命令在本书的后面会更深入地介绍。

现在只要出现了一个远程地址的ARP请求，网关就会用“把它发送到这里”（基本内容）信息包来响应这个请求，并且转发相应的数据包。对于所有的目的主机，发出请求的本地主机总是认为网关就是它要找的远程系统。

下面来分析一个运行在Rutgers大学名为pilot主机上的终端对话。ping命令仅仅用来检查主机是否工作。

```
%arp -a
. .
(no entry for foghat or vax003.stockton.edu systems)
%ping foghat
foghat.rutgers.edu is alive
%ping vax003.stockton.edu
vax003.stockton.edu is alive
%arp -a
. .
foghat.rutgers.edu (128.6.13.13) at aa:0:4:0:98:f4
vax003.stockton.edu (134.210.1.6) at aa:0:4:0:98:f4
```

注意：根据它们的IP地址，名为foghat的这台主机位于子网128.6.13.0上，而vax003.stockton.edu这台主机位于子网134.210.1.0上。然而，名为pilot的主机却不在这些子网上。但是，通过观察foghat和vax003的以太网地址，pilot看到两台主机的以太网地址都是lil-gw。lil-gw刚好位于子网128.6.7.0上。lil-gw被作为foghat和vax003的代理服务器。

当然，这将会产生一个巨大的ARP表，但是ARP条目都被设置成超时关闭的。这就可以避免在路由表中出现过多的路由条目。

路由信息会告诉主机，为了去访问远程系统，应该将数据包发送到哪一个网关。在Rutgers大学，有150个子网在使用，显而易见，对所有的网络都使用静态路由将会产生一个巨大的路由表。通常ARP表平均约有20个条目左右，因为主机通常是与其他主机的一个“闭集”进行通信。

同时，还用注意到负面的影响。如果你只有一个到特定网关的路由入口。当这个网出现故障时，你所发送的所有数据包都会丢失。

如果使用了代理ARP，可能会因为等待一个响应而超时，你的主机就会从其ARP表中删除相应的条目，并再次发出ARP请求。如果在本地以太网上有多个网关，其他的工作网关可以做出响应（如果它知道怎样到达远程的目的网络），这样就可以恢复IP会话。在不影响连通

性的情况下，可以在不同的网关之间动态地切换。

通常，ARP表会提供连接在本地子网上的所有主机和路由器的地址，也就是直接连接在同一个局域网上的主机系统。另一方面，路由表也提供了没有连接在本地子网上的系统地址。这样一来，代理ARP的目的是什么？

设想一台主机用路由表去访问一台已经关闭的远程主机。在路由表被路由协议更新之前，到那台主机的TCP会话已经被断开。然而使用了代理ARP，ARP表会在TCP会话被断开之前更新。

25.2.3 点到点协议（PPP）

Internet标准(草案)RFC 1661中描述了点到点协议（PPP，Point-to-Point Protocol）。PPP允许将各种协议的数据包通过串行链路进行传送，这条串行链路可以是专用链路也可以是拨号链路。较早使用的串行链路协议称为串行线IP（SLIP，Serial Line IP），它仅仅支持IP协议。另一方面，PPP可以支持IP之外的其他一些协议。PPP协议还为在串行链路上的错误校验和IP地址的动态分配提供了循环冗余校验（CRC，Cyclic Redundancy Check）。这些优于SLIP的性能使得PPP更加引人注意。当然，为了提供这些优越的性能和灵活性，PPP协议必须花费更多的开销，因为PPP在每个数据帧中加入了额外的字段，并且在传输过程中加入了更多控制帧。

PPP的基本帧格式如图25-3a所示。与信号线DSL（SDLC）相似，帧的开始和结尾处都有一个相应的标记符，用来指示帧开始和结束。可以参看第16章关于系统网络体系结构（SNA）中对SDLC帧的讨论。比特填充一定是出现在帧的其他区域，所以标记符只能出现在帧的特定位置上。在这个标记符之后，由于在通信的另一端只有一台主机，因此地址都有相同的值。此外，由于有一套特定的控制协议帧类型，因此在这里可以不使用控制字段。大多数情况下，在开始的链路协商阶段，通常忽略掉开始的两个字段。校验和字段（checksum field）用于校验数据和头部信息中可能存在的错误。虽然图中给出的数据字段可以有1500个字节，但是对于交互式业务，数据字段也许减少到296个字节。在低速率链路上，较小的数据帧能够为实时应用提供更好的响应时间。

比特数	字段名称	例子	详细描述
1	标志符	7e	总是0111 1110
1	地址	ff	总是1111 1111，可以省略
1	控制	03	总是0000 0011，可以省略
2	协议类型	0021	协议，可减少到一个比特长
0-1500	数据	---	数据
2	校验和	024a	差错检测
1	标志符	7e	总是0111 1110

a)

协议ID号		网络控制协议(NCP)号		链路控制协议号
0021	IP	8021	IP-NCP	c021 LCP: 链路控制协议
0023	X.25	8023	X.25-NCP	c023 PAP: 口令认证协议
002b	Novell IPX	802b	IPX-NCP	c025 LQR: 链路质量报告
0201	802.1d	8031	Bridging-NCP	c223 CHAP: 询问-握手认证协议

b)

图25-3 a) 类似于SDLC或者HDLC的PPP帧结构；b) 各种不同的协议类型大体上可以分为三类

当线路处于非激活状态时，PPP被说成是处于**失效状态**。当一台主机想通过串行链路与另

外一台主机建立连接时，会通过传送链路控制协议（LCP，Link Control Protocol）包来配置和建立连接，这被称为链路**建立**（Establish）状态。如图25-3b第三列所示，LCP协议的ID号是c021。一旦链路建立起来，如果进行了设置，就会开始认证。这时被称为**认证**（Authentication）状态。默认情况下不进行认证。口令认证协议（PAP，Password Authentication Protocol）和询问-握手认证协议（CHAP，Challenge Handshake Authentication Protocol）是认证过程最常用的两种方法。

接下来进入**网络**（Network）状态。在这个状态中，传送的是网络控制协议（NCP，Network Control Protocol）包，以此来控制通信过程中使用到的协议。对于IP协议，根据图25-3b中间一列所示，NCP的值是8021。现在，利用图25-3b左边一列给出协议ID，就可以在这条链路上传输数据了。最后，在**结束**（Terminate）状态，LCP包使链路回到失效状态。

概括起来，LCP提供了从一个状态转化到下一个状态的转换。NCP允许一种网络协议被初始化，同时通过使用列在最左边一列中的协议的ID来传送相关协议的数据。

25.3 IPv4

在Internet标准(草案)RFC 791中描述了IP协议。迄今为止，我们仅仅提到了IP数据包头中的协议字段和IP地址字段。从图25-4中可以看到，包头中还有许多其他的字段，下面按顺序来看一下其余的部分。你可以参考图8-14，看一下一个IP头中的各个字段是如何被以太网分析器解码的。在图25-6a中，用方块图的形式给出了IP协议的头信息。

字节数	字段名称	例子	详细描述
4	IP Version(IP版本)	4	IP协议的版本
4	IP Header Length(IP头的长度)	5	仅指出IP头部信息的长度
8	Type of Service(服务类型)	00	所需的服务质量要求
16	Total Datagram Length(数据报的总长度)	05dc	数据报的长度
16	Datagram Identification(数据报标识)	890c	分段中使用的数据报的数量
3	Flags(标志符)	0	在分段中也用到了标志符
13	Fragement Offset(分段偏移量)	0	分段起始处的字节编号
8	Time-to-Live(存活时间)	fd	数据报在丢弃前可经过的传输跳数
8	Protocol(协议)	01	ICMP、IGMP、TCP或UDP
16	Header Checksum(头信息校验和)	902a	仅对头部信息进行的差错检测
32	Source IP Address(源IP地址)	b081d01	发送数据报的主机的IP地址
32	Destination IP Address(目的IP地址)	09cd00a	目的主机的IP地址
变量	Options(选项)	-	很少用到的选项
变量	Padding(填充)	-	保证头部信息以完整的32比特边界结束

图25-4　IP数据报的头通常是20个字节

头部最开始的4个比特规定了数据报的版本号。在本例子中，这个值是4。在IPv4中，大多数IP数据报的头只有20个字节长。由于以32个比特长度作为一个字（word），因此头部的长度通常是5。只有在使用选项时，头部的长度才可能大于5个字。由于头部是一个4个比特的字段，因此最长只能有60个字节。也就是把二进制1111转换成十进制，就可以得到15个字，即60个字节。通过检查IP头长度字段，就可以知道头部是否包含选项。

服务类型：如果这个字段在路由器中使用，那么它就变得非常重要。一般来说，除了DoD之外，很少使用这个字段。它可以被分成两部分，第一部分长3个比特，被称为优先比特。其余的5个比特属于第二部分，称为服务比特。通常，为了进行数据报的输送，优先比特的值

被设置成000。然而，如果把优先比特设置成111（二进制），那么这个数据报就具有最高的优先级。这些具有高优先级的数据报可以诊断或管理数据包，使它们在网络发生拥塞时或者出现其他问题时也能顺利通过网络。在这种情况下，这些数据包首先通过网络，这意味着要丢弃那些优先级较低的数据包。在侧面的图中给出了这些优先级的列表。

数据优先级

服务类型字段的1至3比特	
111	国家网络控制
110	互联网络控制
101	CRTIC/ECP
100	超高速
011	高速
010	紧急
001	优先
000	常规传送

拥有高优先级代码的用户能以高速度传送数据。那些有着更高优先级代码的用户叫做超高速用户，能够抢占那些高速级别的用户位置。超高速级别以上的优先级通常用于网络控制。

接下来的4个比特被称为服务比特，它们使用的比较频繁。但是，由于许多路由器并不能处理这些比特，这样设置这些比特就没有什么用了。最后1个比特总是0。在这4个比特之中，只有一个比特在任何情况下都能设置。服务比特表示最小延迟量、高的数据吞吐量、高可靠性和最低的费用。远程登录协议（Telnet）和其他的交互式协议需要最小的延迟。文件传输协议（FTP，File Transfer Protocol）和简单邮件传输协议（SMTP，Simple Message Transfer Protocol）的数据传输需要高吞吐量。简单网络管理协议（SNMP，Simple Network Management Protocol）和开放式最短路径优先（OSPF，Open Shortest Path First）路由协议的数据包需要高可靠性。最小的花费比特很少被使用，但是当进行路由选择把数据报发送到最低费用的链路上时，OSPF协议会使用这个比特。这些服务比特被汇总在侧面的图中。

服务比特（字段中的4至8比特）

00000	通常服务
10000	最小延迟需求
01000	高吞吐量需求
00100	高可靠性需求
00010	最低的费用

（其他的组合无效）

包括了头和数据部分的数据报的总长度以字节为单位，在数据报的总长度字段中给出。尽管最大的数据报可达2^{16}或64KB，但是这个最大值很少使用。所有的主机都希望接收到的是576个字节长的数据报。如果要发送比较大的数据报，那么数据包的长度值必须事先被核实，这个值就被称为最大传输单元（MTU，Maximum Transfer Unit）。为了了解在一个数据包中数据占据了多少个字节，可以用数据报的长度减去IP头的长度。例如，如果IP头的长度是5，而数据报的总长度是100，那么，5乘以4是20个字节，这是头部的长度，从100中减去这个长度得到80个字节，也就是说在这个数据报中携带的数据是80个字节长。

一个以太网帧所包含的最小数据量是46个字节。如果实际的数据长度小于46个字节，则需要在帧中填充比特以使数据的长度达到46个字节。在这种情况下，总的数据报长度字段会指出多少个字节是真正的数据，多少个字节是填充比特。在图25-4的关于数据报的例子中，05dc表示的是数据报的总长度。共1500个字节，这是以太网所能承载的最大数据量。这个数据报有20个字节的头部，1480个字节是IP数据。由于协议字段的值为1，这1480个字节的IP数据实际上包含有一个ICMP分组。这个ICMP数据包含有4个字节的头以及ICMP数据。对于一个802.3帧，由于3个字节被LLC使用，5个字节被SNAP头使用，则其最大值是05d4或1492个字节。

分段：IP头部的其余部分会受到**分段**（fragmentation）的影响。当一个大数据报从一个网络传向另一个网络时，由于目的网络只能接收较小的帧（或称为较小的MTU），路由器就不得不将数据包分割成许多分段。只有这样才能将分段数据传送到MTU较小的网络中去。

如果一个数据报被分成多个分段，目的主机必须能将这些分段重新组合起来，并且恢复

成一个数据报。如果分段数据来自多个不同的数据报，一个主机如何才能分辨出哪些分段属于哪一个数据报的呢？要做到这一点就要使用数据报中的标识（Identification）字段。发送主机给每一个数据报都赋予了唯一的一个标识号。因此，由同一个数据报产生的所有分段都拥有相同的标识符。来自于不同主机的两个数据报可能会有相同的标识符。然而在这种情况下，源IP地址的不同可以区分出它们是不同的数据报。由于标识字段足够的长（16个比特），因此在任何一个特定的时间内来自同一个主机的两个数据报不可能有相同的标识符。下面让我们通过一个分段的例子来更好地理解这些字段的含义。

在图25-5的顶部，可以看到1580个字节的数据被主机A放在了1600个字节长的数据报中。这个数据报通过令牌环网被传送到第一个路由器上。这个令牌环网允许承载的最长数据长度是4500个字节。因此，1600个字节的数据报可以顺利地在这个网络上传输。注意，十进制数1580和1600在图中也被转换成十六进制数，因为我们需要这些数来合成数据报的头。为了生成其他的头信息，也需要十六进制的数字，因此其他的字节也被换成十六进制形式。

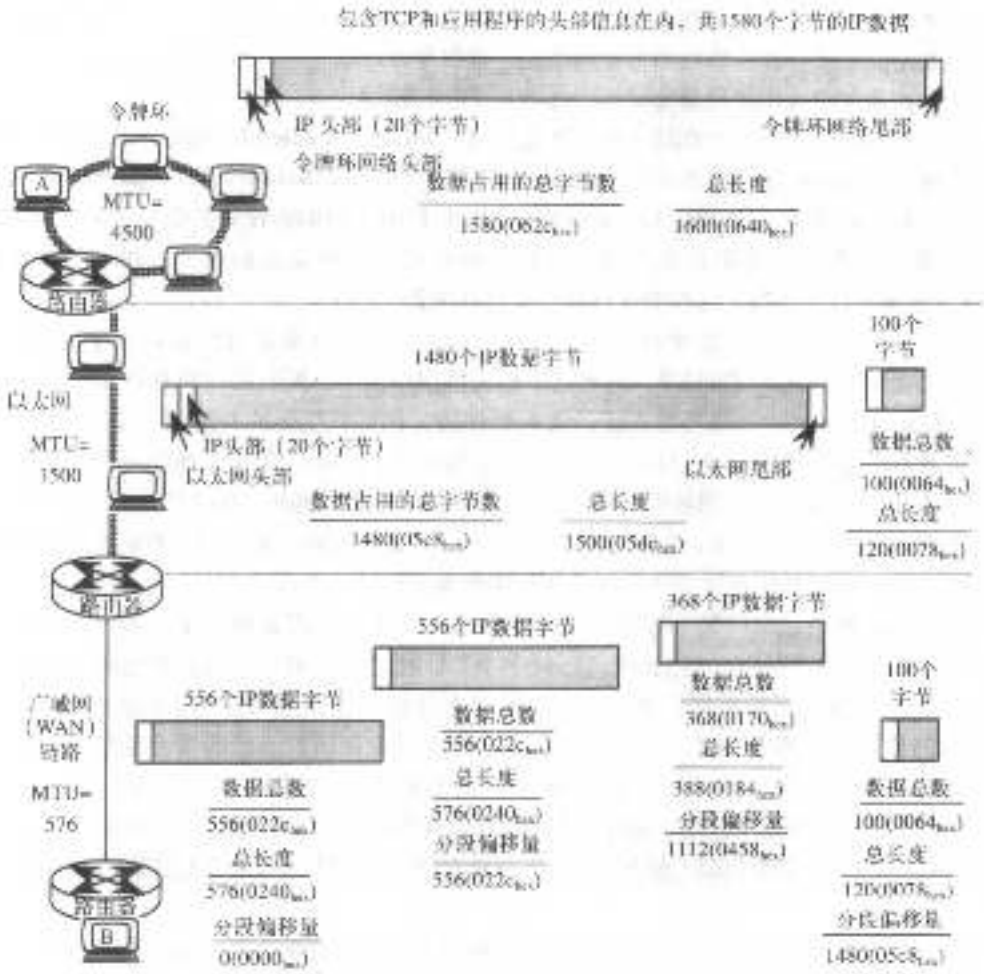


图25-5　令牌环网络上的主机A发送数据报给主机B，路由器必须把数据报分成两段，因为在以太网帧中的数据不能超过它的最大MTU，即1500个字节。这些分段中的第一个分段又必须再次被分段，从而使数据的长度不会超过广域网链路的MTU，即576个字节

现在，这个数据被路由到最多只能支持1500个字节的以太网上。这就需要路由器将这个1600个字节长的数据包分成一个1500字节的分段和一个120字节的分段。第二个分段的IP头部还需要额外的20个字节。因此，1580个字节的数据被分成两个分段，它们分别携带1480个字节和100个字节的数据信息。

接下来，图中以太网下面的路由器必须将这两个分段路由到广域网链路上去。但是路由器可能不知道接收主机所能接收的最大数据包尺寸。根据规范，包括头部在内的最小的数字是576字节。因此，路由器可能会将这些分段后的数据再次分割成556个字节的分段。第一个分段被分成2个576字节的分段和1个388字节的分段。556 556和368相加就是第一个以太网数据帧传送的1480个字节的数据。第二个以太网数据帧不需要再进行分段。通过用这种方法，一个数据包就被变成了4个分段。

只有接收主机才会重新组合这些分段。如果分段的到达顺序是混乱的，那么接收主机是如何知道重组它们的顺序呢？**分段偏移量**（Fragmentation Offset）字段就提供了这种功能。从图25-5的底部可以看到，在最左边的那个分段的偏移量字段的值为0，这就表明它是第一个分段。下一个分段的偏移量的值是556，这表明从0~555的字节数据在前一个分段中。556加556是1112，这就是第三个分段的偏移量。最后，对于120个字节的分段的偏移量是1480，表示这个数据包前面的那个数据包所携带的字节数。用这些数字，目的主机就可以重组这些分段了。通过把这些数字转化成十六进制数形式，就能得到为每一个数据包建立IP头所需要的信息。注意，一个数据报既可以被称作一个分组也可以被称作一个分段。分段能够在链路之间传输，但数据报的传输却是一个端到端的传输。在这个例子中，目的主机接收到的是一个数据报，这个数据报编码形成了4个包。

现在是为所有的这些IP分组编码头部的时候了。在仔细察看图25-6的头信息时，可以参考图25-5。在图25-6a中，再一次显示了IP头。在图25-6b中，看到的是在令牌环网络上的数据报头。**标志**字段占用了3个比特，而**偏移量**字段使用了余下的13个比特位。注意这里的版本为IPv4，头的长度是5个字。**服务类型**字段使用了默认值0。接下来，给出数据包的**总长度**，为640_{hex}（十六进制）。

数据报的标识号是$007a_{hex}$（十六进制）。接下来的是3个比特长的**标志**字段。在这里第一个比特总是为0。第二个比特表示数据报可以被分段，如果第二个比特是1，那么这个数据报不能被分段。如果这种情况发生，这个数据报就会被丢弃，同时一个ICMP错误信息会被发送给源主机，用来说明发生了什么事情。第三个标志比特也是0，它表明在这个包的后面没有其他的分段了。可参看侧面的图表。

标志比特	
000	允许分段且后面再无分段
001	允许分段且后面还有其他分段
010	不允许分段且后面再无分段

在第三个字的开始处，可以看到**生存时间**（Time to Live）字段被设置成20_{hex}。这实际上是数据包在被丢弃以前可以经过的跳数。这意味着这个包能够通过的最大路由器个数是32个。它防止了数据包在网络中无限制地循环。上层的协议字段的值是06，表示TCP协议。计算出来的**头部校验和**（Header Checksum）的值是$352d_{hex}$（十六进制）（这个值实际上不是计算出来的）。最后两个字给出了源主机和目的主机的IP地址。

现在来看一下在以太网上传送的两个分段的头部，它们显示在图25-6c和25-6d中。所有从原来的数据包中照抄过来的字段都被阴影覆盖没有显示出来。而所有非阴影覆盖的字段就是

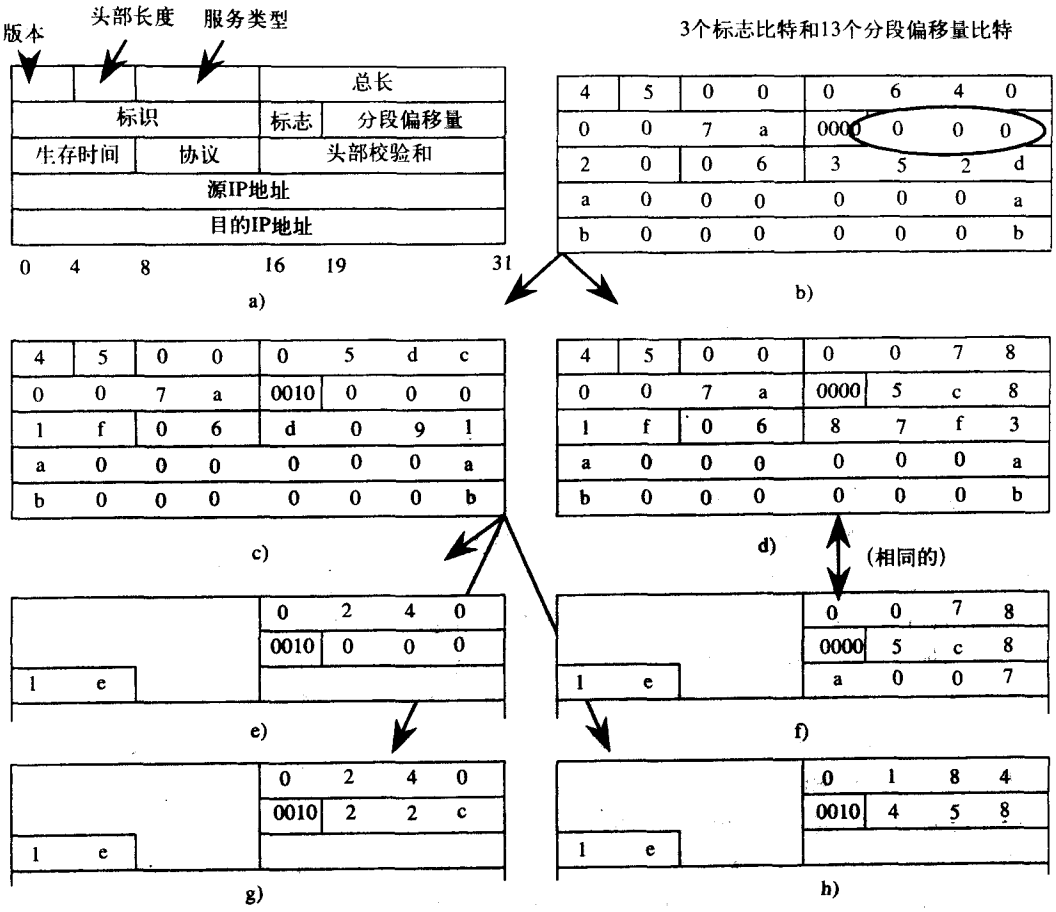


图25-6　a) IP头的结构。b) 原始数据报的IP头通过令牌环网传输。(c和d)首先，数据包被分为两个分段。所有阴影字段值都与原始数据报相同，也与广域网链路的分段头相同。(e、g和h) 从第一个以太网分段分出的三个分段。f) 第二个以太网分段不必再重新分段

现在要讨论的字段。在图25-6c中，**总长度**（Total Length）字段是$05dc_{hex}$（十六进制），它就是图25-5中以太网上第一个分段的长度。最后的**标志**（Flag）比特被设置成1，表明有一个或更多个分段跟在这个分段后面。偏移量的值是0，表明这是第一个分段，同时跳数也从20_{hex}（十六进制）减小到$1f_{hex}$（十六进制），说明这个包已经通过了一个路由器。头部校验和与在令牌环网中的头部校验和也是不同的。

对于图25-6d所示的头部信息，它的总长度是0078_{hex}（十六进制）。偏移量为$5c8_{hex}$（十六进制），表明在这个分段之前已经发送了多少个字节。更多分段的标志比特为0，表明这是数据报的最后一个分段，同时得到的校验和与其他包的校验和也是不同的。

接下来是在广域网链路上传输的4个包，它们如图25-6e至图25-6h所示。在图25-6h中，120个字节长的包头基本上没有什么变化。由于又一次通过了一个路由器，因此只有**生存时间**（Time to Live）字段发生了变化，值减1后变成$1e_{hex}$（十六进制），这使得头部的检验和也随之发生了变化。由于同样的原因，前面3个包中的这两个字段也会发生相同的变化。头部的长度和偏移量值的变化与图25-5的相同。注意，除了最后一个分段之外，其他所有分段中的“更

多分段标志比特”都为1。

25.4 IP地址的不足

在开发TCP/IP协议的初期，它一直都被认为是美国国防部的一个临时解决方案，这种观念一直持续到OSI最后被定稿。所以当时认为32位的IP地址足够用了。然而，由于TCP/IP自身的优点，使得它被广泛地采用，以至于现在没有足够的IP地址可用。IPv6提供了128位的IP地址，另外关于IP地址不足问题的其他解决方法也纷纷出现，但是其中一些只是暂时性的措施。

25.4.1 无类别域间路由选择（CIDR）

Internet标准(草案)RFC 1518和RFC 1519中对无类别域际路由选择（CIDR，Classless InterDomain Routing）进行了描述。例如中国为了得到B类网络已经申请了6次，但是由于没有那么多的B类地址，所以每次申请都遭到了拒绝。还有一些可用的C类网络地址，因此它们被分配用来代替A类或B类地址。用一组C类地址来代替一个B类地址存在的问题是，这组网络地址会使路由表变大。对于每一个C类网络，路由器上必须存在一个独立的路由条目。CIDR所做的就是要忽略不同类型网络的主机和网络地址的边界，使这个边界变得比较灵活，以便能使用路由表中的一个条目而不是多个条目来路由多个C类网络。现在，多个网络可以使用路由表中的一个条目进行路由。

当使用分类路由时，网络比特和主机比特位的边界是固定的，网络中的路由器都知道这个边界。例如，对于一个C类网络，24个比特用来表示网络地址，8个比特用来表示主机地址。然而，由于在CIDR中网络比特和主机比特位的边界是可变的，因此在传送每一个IP地址的同时还需要传送边界的位置信息。较早的路由协议不支持这种可变长的边界。然而OSPF和RIP-2都支持这种可变长边界。网络比特和主机比特的边界由超网掩码来表示，多个C类网络被组合在一起被叫做一个**超网**（supernet）。

当将几个C类网络集成变为超网时，最好将它们放在同一个地域或拓扑结构中。属于同一个超网的C类网络应当在同样的区域或属于同一个ISP或同一组织机构。这样，当属于某个超网的路由器收到传给自己网络的数据包时，就可以迅速地把数据包发送到正确的目的地。让我们看一个例子。

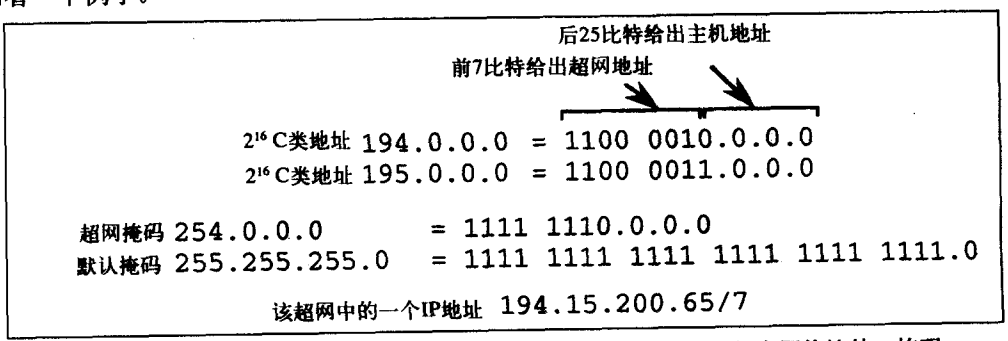


图25-7 两个包含2^{16}个C类地址的网络可以合并成为一个超网。对于7个网络比特，掩码由255.255.255.0变成了254.0.0.0。最后一行给出了掩码与IP地址写在一起的方法

图25-7表示了所有以二进制数1100001开始的C类地址。每一个C类地址的网络上有256个主机地址，这样的C类网络共有2^{17}个。通过使用超网掩码254.0.0.0，代替C类网络的默认掩码

255.255.255.0，这样所有的C类网络都被归到一个超网中。当给出IP地址时，超网掩码的7个比特可以用“/7”的形式表示出来。例如，IP地址194.15.200.65/7表明该地址用7个网络比特、25个主机比特。

这个地址范围全部都位于欧洲。在美国，转发给欧洲这2^{17}个网络的所有数据包，只需要在路由器中加一个条目就可以了。如果没有CIDR，路由表中就需要2^{17}个路由条目。注意，无类别的地址也可用符号“/”表示。 例如，由于A类地址使用8个网络比特，所以IP地址72.9.0.34可以被写成72.9.0.34/8。

25.4.2 动态主机配置协议（DHCP）

Internet标准(草案) RFC 1541描述了动态主机配置协议（DHCP，Dynamic Host Configuration Protocol)。在DHCP出现以前，局域网上的每一台主机都被分配了自己的IP地址。这些地址是静态的，并且写入了主机的配置文件中。在整个的引导过程中，该IP地址一直被分配给固定的那台主机。即使在使用RARP的情况下，无盘工作站虽然不知道它自己的IP地址，它也可以从RARP服务器上获得其固定IP地址。无论在什么时候，每一台主机（或每个MAC地址）都有一个固定的IP地址。

如果一台主机仅在它所在的局域网上进行内部通信，就不需要IP地址，这时分配的那个IP地址就被白白地浪费了。更进一步说，如果主机死机或被关闭了，那么它的IP地址也就不再被使用了。对于一个拥有IP地址的主机，当需要时就必须永远维护一个IP地址。DCHP解决这个问题的办法是，需要时动态地分配一个IP地址。设想你有一个可用的C类网络，只有254个可用的IP地址。如果不使用DHCP，这个局域网只能支持最多254台主机。然而，使用DHCP后，你可以为500台左右的主机提供因特网服务。能够被支持的主机的数目依赖于IP地址的使用情况。要支持500台主机，必须假设在任何一个给定的时间里，在500台主机中只有254台主机需要IP地址，而其他的主机处于空闲状态或者只是使用本地网。

DHCP的概念非常简单。它用一个DHCP服务器来管理所有可被动态分配的IP地址。当一台主机需要IP地址时，它会向DHCP服务器申请一个IP地址，当它不再使用IP地址时，主机将会把这个地址释放给DHCP服务器。 通过这种方法，重新释放给DHCP服务器的IP地址又能够被其他的主机使用。注意，当主机向DHCP服务器申请IP地址的时候，每次得到的IP地址可能是不同的。这又给域名服务器（DNS，Domain Name Server）服务带来了问题。因为域名服务器准确地将主机名字映射成IP地址。在一天的过程中，如果主机使用了几个不同的IP地址，那么对于域名服务器来说跟踪它们是很困难的。由于这个原因，许多经常处于工作状态的服务器都使用固定的IP地址。而DHCP却为客户端的使用提供了更多的好处。

DHCP的处理方式源于RARP。RARP为每个局域网网段提供IP地址解析。在每一个由路由器隔开的局域网上都需要有各自的RARP服务器。为了避免这种需求的产生，出现了BOOTP协议，它使用UDP协议并且是可路由的。RARP是网络接入层的协议，而BOOTP和DHCP是TCP/IP协议的应用。在一个多网段的网络中，只需要一个BOOTP服务器就可以为无盘工作站提供其IP地址。使用BOOTP时，每一个物理地址对应一个IP地址。而用于管理一组IP地址的DHCP服务器，只是把IP地址“借”给那些需要地址的主机。

图25-8给出了一个DHCP消息的头结构。除了标志和选项字段之外，这个结构和BOOTP的消息结构是相同的。这里给出了一个用操作代码1进行请求，用操作代码2进行响应的例子。请

求消息由用户发送到DHCP服务器，以请求租用一个IP地址。响应消息是由DHCP服务器发出的。

字节数	字段名称	请求的例子	响应的例子	详细描述
1	操作代码	01	02	请求或响应
1	硬件类型	01	01	以太网、令牌环网等
1	硬件长度	06	06	MAC地址的长度
1	跳数	01	01	允许通过的路由器数量
4	事务处理ID	3f00910a	3f00910a	请求的确认
2	秒	0000	0010	请求发出后已经过的时间
2	标志符	0000	0000	只使用最左边的比特
4	客户端IP地址	00000000	00000000	IP地址，通常是未知的
4	你的IP地址	00000000	a10045b8	从服务器得到的地址
4	服务器的IP地址	00000000	a10045b9	DHCP服务器的地址
4	网关的IP地址	00000000	a10045b9	默认网关的地址
16	客户端硬件地址	b081d01..	b081d01..	MAC地址
64	服务器主机名	0000000..	0000000..	DHCP服务器的名称
128	启动路径及文件名	0000000..	0000000..	初始化配置信息
变量	选项	0000000..	0000000..	厂商特定信息

图25-8 DHCP消息结构

硬件类型和硬件长度字段与ARP和RARP结构中的相同，可以参考图25-2。跳数字段的值规定了这个消息可以通过多少个路由器。传输ID用来匹配相应的响应消息和请求消息。请求发出后已经过的时间由用户端在第1个字段中给出。

在这里的标志字段中，只使用最左边的一位。如果这一位被设置为1，这表明客户请求使用硬件广播来发送响应信息。在这个例子中，这个比特是0，因此，响应使用单播帧的形式发送给客户。因为客户不知道它自己的IP地址，这个字段被设置成0。在来自DHCP服务器的响应消息中，客户的IP地址在“你的IP地址”这个字段中给出。然而，DHCP服务器和默认路由器的IP地址在接下来的两个字段中提供。如果知道服务器的主机名，就可以对这个主机编码。然而，像其他的字段一样，如果不知道它的值，该字段就用0来填充。

25.4.3 基于IP的专用网络

一个像通用电子（General Electric）这样的私有企业，能用TCP/IP来创建自己的专用网络。像这样的组织都有它自己的路由器，并且可以租用线路来把局域网和广域网互连起来。这样的网络就被叫做专用网，用一个小写字母“i”来表示。它拥有并可以操作这个互联网上的基础设施。虽然要花很高的费用来维持，但这将会给它带来更多的安全控制。由于它不连在公共因特网上，因此它可以用任何一个IP地址。我们用一个大写字母”I”来表示公共因特网。

有的专用网络也可能想与公共因特网相连接，这就必须要注册一个IP地址。在这种情况下，如果能为那些内部主机申请到足够的IP地址，就需要为内部主机重新分配IP地址。解决这个问题较好的方法是在一开始就为这些内部主机分配专用IP地址。当需要连接到公共因特网上时，内部主机会得到真正的IP地址，这时只要在边界处放置一个网络地址转换（NAT，Network Address Translation）设备就可以了。

指定的专用IP地址可以被任何专用网络使用，这是因为这些专用地址都不能在公用因特网上进行路由。只要某个携带专用IP地址的IP包到达一个公共因特网的路由器，就会被丢弃。因此，如果你想连接到公共因特网上，就可以使用这些专用地址中的任何一个而不必进行注册申请，但是你不能向公共因特网发送数据包。

RFC 1918规定了3组专用网络使用的IP地址，分别属于A、B和C类地址空间。它们被列在图25-9中，分别是10/8、172.16/12和192.168/16。在第26章有关Linux的讨论中，在我们的实验室中就是用了这组地址作为了主机地址。

分类		地址范围	可用地址数量
A类	10/8	(10.0.0.0-10.255.255.255)	2^{24}
B类	172.16/12	(172.16.0.0-172.32.0.0)	2^{20}
C类	192.168/16	(192.168.0.0-192.168.255.0)	2^{16}

图25-9　不能在公共因特网上路由的专用IP地址范围

首先，如果一个组织能够申请得到公用IP地址，那么当他们连接到Internet时，变换就会简单一些，也不必重新分配本地主机的地址。使用专用IP地址是退一步的解决方案。

25.4.4　网络地址转换设备

图25-10a所示是一个使用172.16/12地址的专用网络，它通过一台NAT设备连接到公共因特网上。NAT地址或者说申请注册的IP地址，在201.117.30/24这个子网上。每当一个主机需要连接到公共因特网上时，NAT设备都要找到一个未使用的公用IP地址，并动态地为该IP地址和本地专用地址创建一个转换条目。这样在会话期间，每次内部主机发送一个IP数据包时，NAT会将该数据包的源地址转换为公用IP地址。与此类似，当一个数据包到达该NAT地址（公用IP地址）时，NAT也会将它的目的地址转换为内部的专用地址。

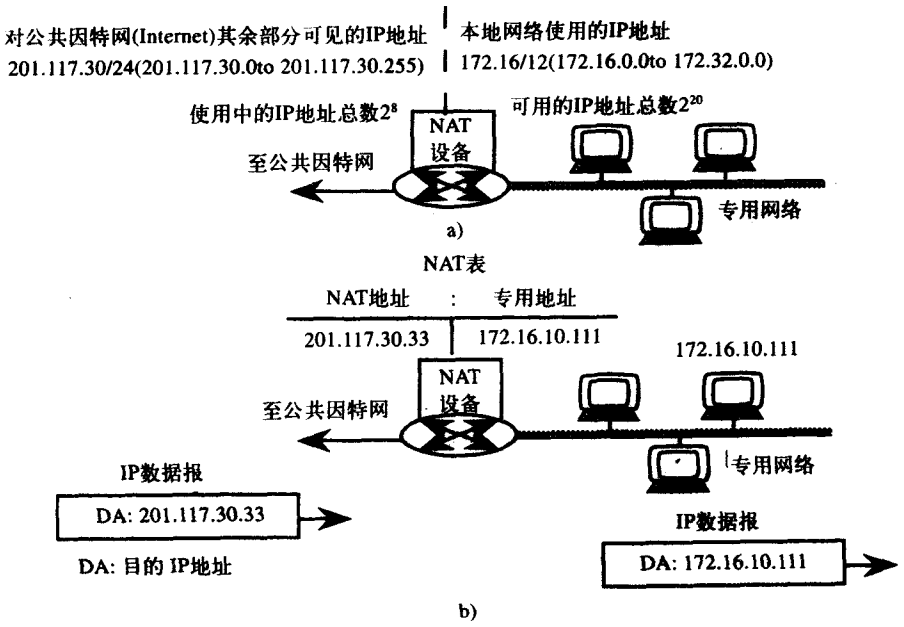


图25-10　a) 一个网络地址转换（NAT）设备可以服务的本地主机数目比已经申请注册的IP地址要多。
b) 例如，NAT设备将一个由外部到达的IP数据包的公用IP地址转换为专用的本地IP地址

这一点在图25-10b中显示出来。一个来自公共因特网的IP数据包到达NAT，它的目的IP地址为201.117.30.33。NAT设备会查看它的内部地址转换表，然后将该数据包的IP报头中的目

的地址改为172.16.10.111。220个专用主机地址要共享28个可供使用的公用地址。然而，由于并不是所有的内部主机都在同一时间访问公共因特网（许多主机只是访问内部网络中的其他主机），因此该解决方案是可以接受的。如果在NAT中没有可以使用的公用IP地址时，NAT设备就会返回一个ICMP错误消息，表明目的地址是不可到达的。

NAT设备也可以用于其他的目的。如果用户想要更换他们的ISP服务商，但是还想要保留原来ISP提供给他的IP地址，那么原来的ISP服务商的NAT设备能够将数据包发送给新的ISP。同样，当2个公司合并时需要把2个专用网络合二为一，一种解决方案就是在这2个网络的边界处设置一个NAT设备。

NAT还为防止IP地址的欺诈行为增加了安全性控制。所谓的IP地址欺诈行为是指，黑客发送IP数据包到你的本地网络，并且这些数据包的源IP地址被伪装成你所在网段的IP地址。这样一来这些数据包就可以发送到你的网络中，并使你的网络认为这些数据包来自本地主机。但是如果你使用专用IP地址，那么这种情况就不可能发生了。这是因为公共因特网中的路由器会把使用专用IP的数据包丢弃掉。

这是IP发展史上的第一次：使得设备可以改变IP数据包头部信息中的IP地址。在更改IP地址之后，每个头的校验和都必须重新计算，所有这些工作都会降低路由器处理数据的速度。

25.4.5 代理服务器

NAT设备可以使许多本地主机共享一个地址池内的公共IP地址。另一方面，一种被称作“代理服务器”的更特殊的专用NAT设备，可以使几台本地主机共享一个公用IP地址。在Linux中，这称作“**IP伪装**（IP masquarading）”。

从图25-11中可以看到，一台代理服务器的官方IP地址为201.117.30.33。这一个地址能够同时为本地网络上的多台主机提供多个连接。在Linux中，默认的最大限制是4096台主机。代理服务器使用连接端口来区分不同的连接，而不是使用IP地址映射的方式进行区分。这些端口的编号是从TCP协议的报头中得到的。

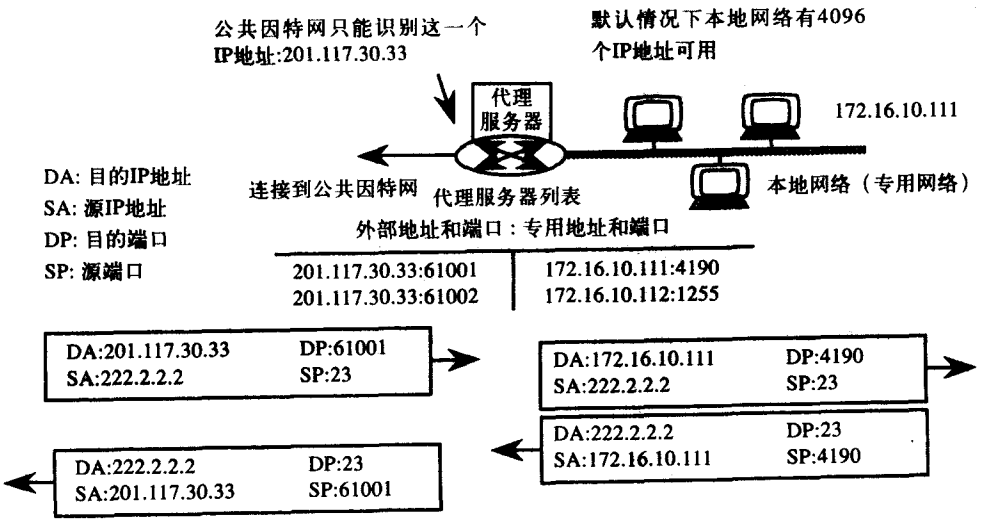


图25-11 代理服务器只使用一个官方的IP地址来连接多台本地主机。在这个例子中，所有本地主机都隐藏在IP地址201.117.30.33的后面。端口号用来区分每台本地主机

在图中的例子中，一个输入的IP数据分组的目的端口号是61001。大于61000的端口号被用于代理服务器功能。服务器会查询它的代理服务器列表，发现这个端口被映射成本地网络中地址为172.16.10.111的主机的4190端口。这样就会对IP数据包做相应的转换并发送到目的主机。要注意，发生改变的不仅仅是IP报头，传输层即TCP的报头也要做相应的改变。此外，图中还显示了代理服务器是如何使用它的代理服务器列表对向外发送的数据包进行转换的。

通常，代理服务器仅适用于小型的专用网络，而NAT设备一般用于规模较大的网络。也就是说，NAT设备更适合用于高端。因为所有的本地主机都隐藏于一个公用IP地址的后面，这样就可以在代理服务器的每一层中配置相应的安全性，所以代理服务器的安全性能要高于NAT设备。另外，获得一个IP地址要比获得多个IP地址容易一些。这些区别都列在表25-1中。

表25-1　NAT与代理服务器的比较

	NAT设备	代理服务器
目的	变换地址	提供安全性
IP地址是否改变	是	否
外部网络能看到多少个地址	一组地址	只有一个
连接如何分辨内部主机	IP地址	端口
安全等级	低	所有层次
适用于何种规模的网络	大型	小型

NAT设备或者代理服务器的一个主要缺点是，它们不支持一个称为“IP安全性”（IPsec，IP Security）的新协议。这个新协议要求，数据加密应该是一个端到端的问题，IP数据包传输途中的任何设备都不能以任何方式改变数据包中的内容。如果不再另外增加软件使NAT设备成为应用层的网关，则其他的一些新协议也不能与NAT设备一起工作。而这样做又会进一步降低数据的处理速度，使流媒体不能被正常接受。近期正在开发的一个称为特定区域IP（RSIP，Realm Specific IP）的协议会解决NAT和代理服务器存在的问题。

25.4.6　IPv6

历史总是在重复。在OSI成为互联网络标准之前，TCP/IP协议只是作为DoD的一个临时解决方案。然而，TCP/IP却代替OSI成了事实上的标准。类似地，前边提到的用来解决IPv4地址问题的方法，开始的时候也是一个临时的解决方案，一直到IPv6协议定稿才改变。在制定IPv6时的书面工作要比最初的预期时间长。

IPv6将IPv4中的地址长度从32个比特扩展到了128个比特。这样就可以使地球上每平方英寸的土地拥有50个IP地址。此外，IPv6还有其他的优点。这些优点主要是，鉴权（认证）功能的扩展，还有更好的安全、隐私和完整性的加密扩展。除了网络、子网和主机外，还有更多的寻址层次。流标签为实时应用提供了更好的服务质量（QoS，Quality of Service）。这个字段显示在图25-12b中。通过使用区域性集群寻址和简化的报头格式，可以获得对更广泛的IP地址提供更高效的路由支持。

图25-12a和图25-12b中显示了IPv4和IPv6的报头。还记得IPv4中3个比特的标志字段和13个比特的分段偏移量字段吗？在新的报头格式中它们并不存在。所有字段都在4、8、16、24和128比特边界处分界。这使得路由器可以更容易地处理分组数据。另外，这样一来要检查的字段也减少了。与IPv4中计算数据长度不同，IPv6中的数据长度直接放置在报头中。IPv6中的跳数(Hop Count)字段类似于IPv4的生存时间(Time to Live)字段。

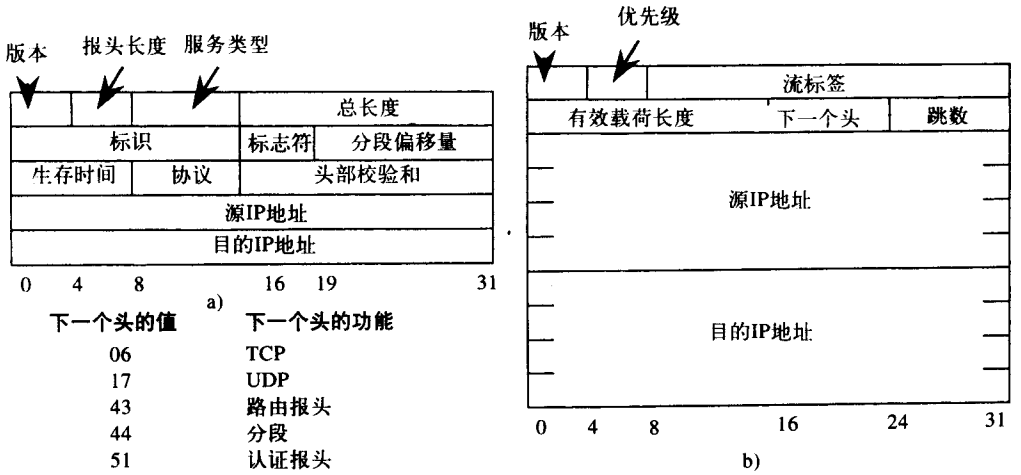


图25-12 a) IPv4的报头。b) IPv6的报头。表格所示是下一个头字段的值及其使用方法

虽然绝大多数情况下要对报头进行简化，但是一个IP分组也可能有若干报头。下一个头字段中给出的值指定了是否还有额外的报头附加于现有的IP报头中。如图25-12所示，如果下一个头字段的值为17，那么这个报头的下一个报头就是一个UDP报头。此时，该字段的功能类似于IPv4中的协议字段。IP报头和传输层报头之间的额外报头被称为扩展报头。

图25-13所示是一个例子。IP报头中的下一个头字段显示出，下一个报头是路由报头。从图25-12的表格中可以看到，值43代表路由报头，这是第一个扩展报头。这个路由报头的下一个头字段的值是44，这表明接下来的一个报头是分段报头，所以下面出现的是分段报头，这是第二个扩展报头。分段报头还拥有它自己的下一个头字段，它的值为06，这表明下一个报头是TCP报头。所以接着显示的是TCP报头和它的数据。

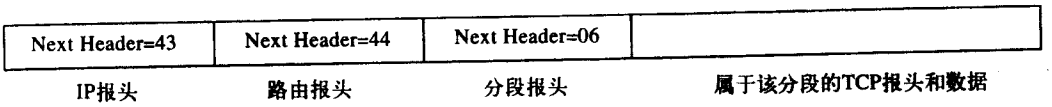


图25-13 带有1个IP报头和2个扩展报头的IP包的例子

25.5 因特网控制报文协议（ICMP）

在第8章中，我们介绍了ICMP和UDP。在这里，将对它们进一步地讨论，其中包括它们的报头格式等内容。图25-14中显示了ICMP消息的格式，它的报头有32个比特，其中包括类型、编码和校验和等字段。一个ICMP消息除了有一个报头，还可能含有可变长的数据，这些数据是由ICMP消息中的类型和编码字段来确定的。使用整个ICMP消息（包括报头和数据）来计算校验和。

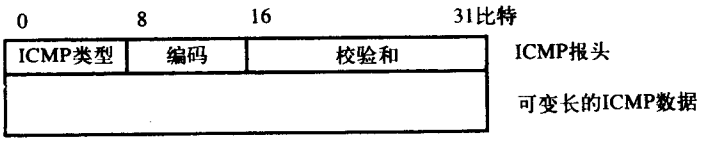


图25-14 ICMP报文的格式

有许多可用的类型值，它们都列在表25-2中。每个报文类型都有一个相关的含义，或是查询报文，或是错误报文，这些也在表中给出。错误报文不能再产生另一个错误报文。ICMP的报文类型有若干个编码。例如，“目的地不可达”(Destination Unreachable)报文有16种可能的编码值。这16种编码值分别表示该IP数据报不能传送的原因。因此，类型字段可以告诉你出了什么错误，编码值可以告诉出现错误的原因是什么。但是，只有4种类型的值有多个编码。

表25-2　ICMP报文类型

类型（十进制）	这种类型的编码数	查询或错误报文	这类报文的含义
0	1	查询报文	与ping一起使用的回波应答
3	16	错误报文	目的地不可到达
4	1	错误报文	源节点关闭
5	4	错误报文	主机、网络或TOS的重定向
8	1	查询报文	与ping一起使用的回波请求
9	1	查询报文	路由器通告
10	1	查询报文	路由器请求
11	2	错误报文	与traceroute一起使用的超时
12	2	错误报文	参数问题或损坏的IP报头
13	1	查询报文	时间戳请求
14	1	查询报文	时间戳应答
15	1	查询报文	信息请求（作废的）
16	1	查询报文	信息应答（作废的）
17	1	查询报文	地址掩码请求
18	1	查询报文	地址掩码应答

根据消息类型的不同，数据被放在不同的ICMP报文中。这些数据可以包含IP地址，或者是报告错误时，可能包含整个IP报头并加上64个字节的数据。这64个字节的数据用来帮助接收主机检查传输层和应用层的包头以确定出现问题的原因。在后边讲到ping和traceroute命令时还会讨论与这些消息有关的例子。

25.6　用户数据报协议（UDP）

UDP报头显示在图25-15中。与TCP长20或24个字节的报头相比，它只有8个字节。长度字段给出了整个UDP数据报的长度；类似地，校验和也是由整个UDP数据报计算出来的。校验和字段只能由目的主机验证。

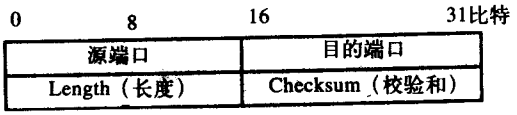


图25-15　UDP报头。这里的长度是指包括报头在内的整个数据报的长度。校验和用整个数据报计算

目的端口标识了数据的其他部分应该转发给哪一个应用。另一方面，源端口字段是可选项，可以用0来填充。一些服务器的应用程序就是这样做的。

25.7　传输控制协议（TCP）

25.7.1　TCP报头的格式

在RFC 793中描述了TCP协议。现在，来了解一下TCP报头的各个字段的内容。此后，将

会举例说明数据交换的目的和使用方法。图25-16所示是TCP报头的具体格式。因为没有使用选项（Options）字段和填充（Padding）字段，所以，通常TCP报头的长度是5个32比特的字。在这种情况下，报头长度（Header Length）字段的编码值为5。在一些特殊情况下，使用了选项字段之后，报头长度字段的编码值为6。

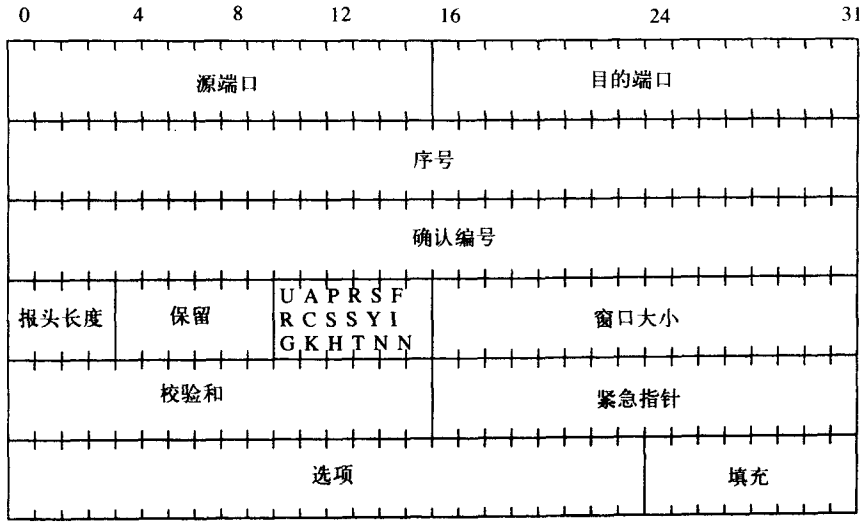
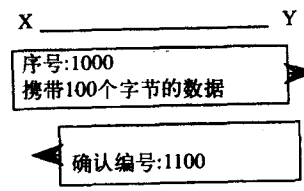


图25-16 在保留字段后含有6个标志符的TCP报头

最常使用的选项是最大段（segment）长度这个选项。建立TCP连接时，它通常只出现一次。发送端TCP模块用这个选项告诉接收端TCP模块它可接收的段的最大长度。可能会发送多个TCP段，但每一个段的长度都不能超出这个限制。

在第8章中，已经讨论了源端口和目的端口字段。如同UDP报头中一样，这些字段提供了区分不同应用的方法。

当一个TCP模块发送数据时，它将每个字节的数据加以编号或排序。TCP段（紧随TCP报头之后，可以是应用层报头的一部分）中数据的第一个字节的编号就是这个字段的值。这个字段不是用来说明数据段中有多少个字节的，它只表示数据的第一个字节的序号。如果想知道TCP段中有多少个字节的数据，只能用IP报头中总长度字段中的值减去IP报头和TCP报头的长度才可得到。建立连接时，最开始的字节是由内部时钟中得到的，它们几乎不会为0。



只有当ACK标志置1时，确认（Acknowledgement）编号才会有效。在图25-16中，标志符（Flags）显示在保留（Reserved）字段的旁边（保留字段未使用）。确认编号具体指定了接收机期望TCP模块发送的下一个序号。例如从旁边的图中可以看到，X正在向Y发送100字节的数据。第一个字节的序号为1000，其中，最后一个字节的序号应为1099。这是因为从1001到1100有100个数字，所以从1000到1099也有100个数字。由于Y已经无差错地接收到了序号为1099的这个字节，因此Y将会等待下一个序号为1100的字节，所以接收端发出的确认字段编号为1100。

可以看到的第一个标志位是URG（Urgent）标志。如果设置了这一项，即它的值为1，则紧急指针（Urgent Pointer）字段变为有效并被使用。ACK标志与URG标志相似，如果设置了

这个字段，则确认编号字段变为有效并被使用。紧急指针字段的目的是要指出需要进行紧急处理的数据所在的位置。这个字段的值是个偏移量，指出了从TCP段数据的首字节到紧急数据位所经过的字节数。此字段的具体应用要根据实际情况来确定。

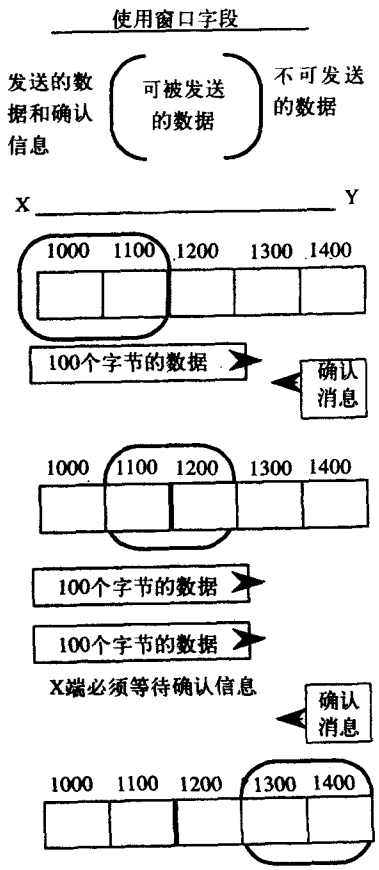
设置PSH（Push）标志位意味着在其余的数据到齐之前即刻发送数据。例如，当两个终端在进行一个实时的会话通信时，每按下回车键都会将数据“推”入网络，这样可以使数据段的长度变短。

设置了RST（Reset）标志位意味着应该立刻复位整个连接。接收端的TCP模块将清除缓冲中的所有内容，正在被传输的所有数据都被认为已经丢失。

SYN（Synchronize）标志位用来建立TCP连接。与此相类似，设置FIN（Finish）标志会终止一个连接。如果主机设置了FIN标志位，那么这就是说它没有数据要传送了。但这时该主机还可以接收数据，直到连接的另一端也将它的FIN标志位设置为1。

IP报头中的校验和（Checksum）字段只用于检测IP报头中是否有错误。但是在这里，TCP校验和不仅检测TCP报头中的错误，同时还检测数据中的错误，也就是说要检测整个TCP段的错误。

TCP用窗口大小（Window Size）字段来实现流量控制的功能。如果接收端TCP模块在不知道数据大小的情况下，希望放入自己缓冲器中的数据最大值为200个字节，那么这时窗口大小这个字段的值就是200。接收端在连接的生存期内可以改变这个字段的值，以便接收数量更大或更小的未知数据。



在旁边图的上部画出了一个窗口。这个窗口是虚构的，就好像所有的数据都在这个窗口中传输一样。窗口左侧的所有数据都已被发送并得到了确认；窗口中的数据是正在等待发送并还需接收端确认的数据；窗口右侧的所有数据是还不能发送的数据。一旦某些发送的数据得到了接收端的确认，这个窗口就会向右移动。来看一个例子。

在旁边的图中可以看到，X端有1500个字节的数据要发送到Y端。Y端通告X端的窗口大小为200，因此，X端可以发送200个字节数据，然后等待确认。X端发送了100个字节并得到了Y端的ACK响应。这时，由于收到了ACK，因此窗口向右移动100个字节。

然后X端发送2个数据段，每段含有100个字节的数据，并等待ACK响应。如果X端在给定的时间内没有收到对第一个段的ACK确认响应，就会重新传送这个数据段；如果X端在给定的时间内也没有收到第二个段的ACK响应，它也会重新发送第二个数据段。然而，如果X端在超时之前收到了第二段的ACK响应，就意味着Y端也正确地接收到了第一段。此时，X端会把这个虚构的窗口向右移动200个字节，继续传送这个窗口中的数据。

25.7.2　TCP数据段交换的一个例子

在图25-17中，只使用了TCP数据段报头的相关字段。图中显示了TCP协议是如何建立连接，

如何通过一个可靠的数据连接来传输数据，以及如何拆除这个连接的。TCP并不像其他协议那样给每一个数据帧编号，它是分别给数据中的每个字节编号。一个段的顺序号标识了在这个被传输的段中，第一个字节数据的编号，而确认号则指出了接收端希望从发送端接收的下一个字节数据的编号。ACK、SYN和FIN字段都是一个比特的标志，它们都是TCP报头的一部分。

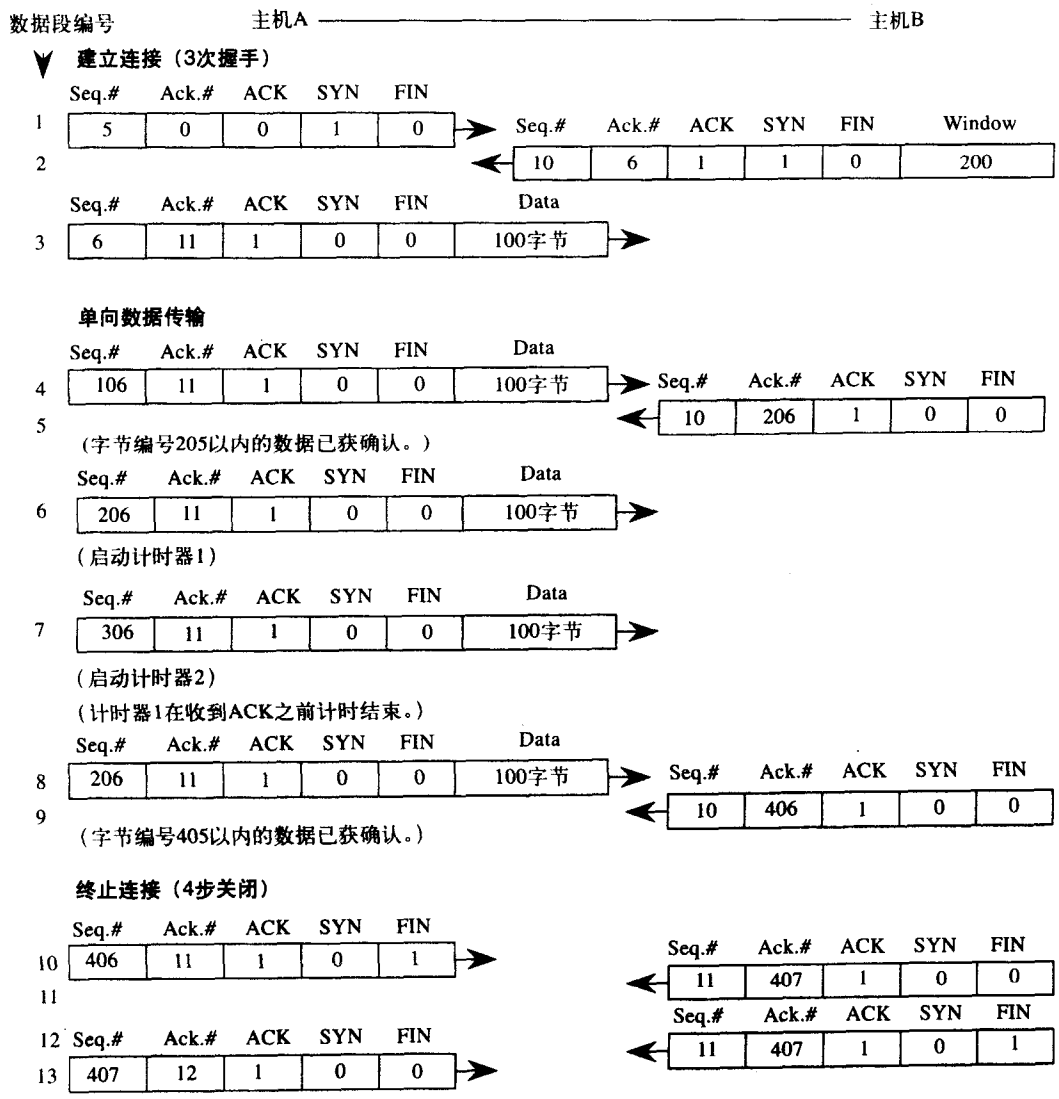


图25-17 建立TCP连接，传输数据，并终止连接

连接阶段：在图25-17中，主机A发送的第一个数据段，SYN（SYNchronize）标志位被设置为1，序列号是5。这样就等于告诉了主机B的TCP模块，主机A从5开始给它的数据段编号。由于主机A还不知道主机B的起始段编号，因此确认字段的值为0，说明这是用来建立连接的第一个数据段。另外，由于SYN标志位被设置，却没有设置ACK标志位，这也说明现在是连接建立阶段。这时，主机A可以把它的最大段长度字段（Maximum Segment Size）作为一个选项发送出去，这使得报头的长度变为6而不是通常的5。A还可以在数据中同时给出其窗口的

大小，但由于本例中只有主机A向B传送消息，故这个字段没有给出。

在第2个数据段中，主机B产生了它自己的顺序号为10，并把它的SYN标志位设置成1，表明它也需要通过另外一条路径建立的连接。主机B也会把它的ACK标志位设置为1，说明确认编号是有效的，并表明愿意与A建立连接。确认的编号为6，说明主机B已正确接收到A发送的前5个字节的数据。虽然是在连接阶段，但这只说明主机A发送的数据的第一个字节编号应该为6。主机B已经将它自己的窗口大小设置为200，以此来告诉主机A在本次传输中主机B只能在缓冲中存储这么多个字节的数据。这样主机B就可以控制主机A传送过来的数据量，从而使A的传送速度不会大于B的接收速度。

在第3个数据段中，主机A通过将自己的ACK标志位设置为1并将确认编号的值设置为11来相应主机B，告诉B它已同意建立连接。如果主机B要传送数据（在这个例子中不会传送数据），那么B就将把数据的第一个字节的编号设置为11。主机A发送第一个数据包，并使其序列号的值是6。这样，就通过3次握手的方式完成了一个连接的建立，这时主机A和B都可以传送数据了。

数据传输阶段：A选择在第一个数据段中发送100个字节的数据，所以它就已经发送了字节编号从6到105的数据。在第4个数据段中，A发送编号从106到205的数据，即又发送了100字节的数据。此时可以看到，A已在没有收到ACK的情况下发送了200个字节的数据。在第2个数据段中，B已说明它的窗口大小为200，所以主机A此时只能在一个规定的时间段内等待ACK的确认信息。

在第5个数据段中，主机B确认已经接收了200个字节的数据，这是通过将确认编号的值设置为206并把ACK标志位置1来完成的。

通过第6个和第7个数据段，主机A再次发送200个字节的数据。这时A受到主机B 的窗口大小的限制。A每发送一个数据段，就会为该数据段启动一个计时器（又称定时器）。因此，A为第6个和第7个数据段分别启动了一个计时器。此时，主机A会等待来自主机B的响应信息，而这个响应还未到达。

为第6个数据段启动的计时器停止计时，所以这个数据段作为第8个数据段被重新发送。主机A未能收到主机B的ACK响应的原因很多。或许是因为当6个数据段到达主机B时，数据中出现了错误，在这种情况下，主机B的TCP模块的校验和字段可以发现错误。当某一到达数据段出现错误时，这些数据就会被简单地丢弃掉，这会导致发送主机等待超时，并重新传送这个数据段。

主机A没有收到ACK的另一个原因可能是，主机B收到数据段迟了（但数据是正确的）。这种情况下，主机A也会再次发送第6个数据段，而这时主机B会收到两个重复的数据段。从这些数据段的序号上，主机B可以判断出它们是两个重复的数据段，因此丢掉其中的一个。也有可能是主机B发送的ACK响应迟到或丢失。这时主机A也会重新传送第6个数据段。

最后，主机B发送第9个数据段，确认已收到了全部的405个字节，这个ACK说明收到了2个数据段。

终止连接阶段：第10个数据段是用来中断连接的第一个数据段。将FIN标志位设置为1表明主机A发起了终止连接。每个主机都可以这样做。B通过把确认编号的值增加1并将ACK标志位设置为1来确认收到了终止连接的请求，这可以在第11个数据段中看到。此时，主机B如果还要发送数据，则仍可发送；如果它要终止与主机A的连接，则可通过将第12个数据段中的FIN标志位设置为1来实现。在第13个数据段中，A确认收到B的终止连接请求。

25.7.3 连接

就像我们所看到的一样，能够在两个主机间传送数据还不够，主机还必须知道这些数据应该属于哪个过程。例如，在图25-18中有两个用户A和B，它们正在远程登录到同一台远程主机上。Telnet允许用户登录到远程主机上并使用服务。而互联网络必须分清哪个传输连接是属于哪个用户的。

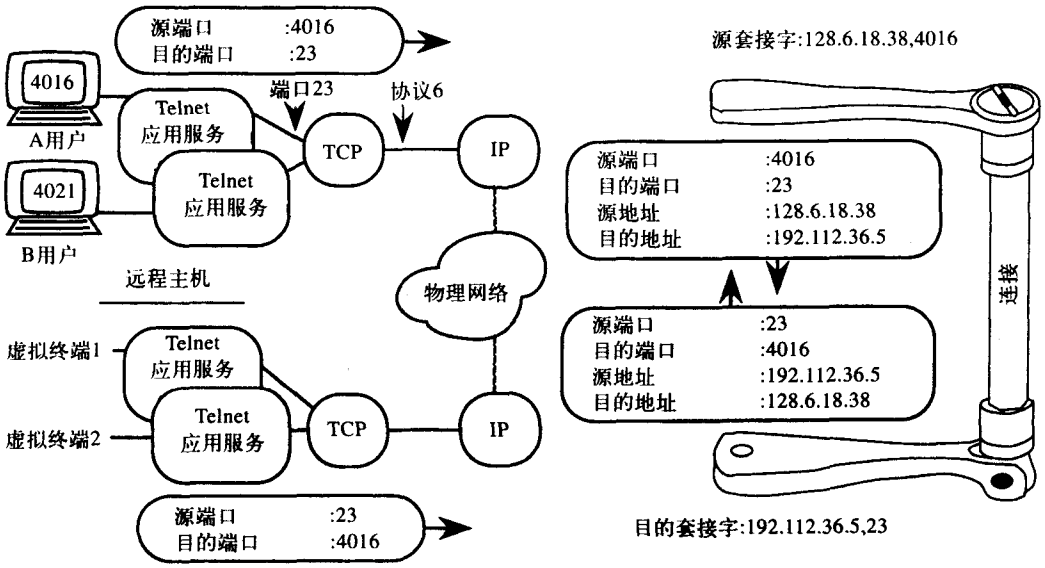


图25-18 一对套接字规定了用户和主机之间的连接

从第8章中我们知道，IP通过将协议设置为6来访问TCP协议，而TCP则是通过将端口号设置为23来访问Telnet应用。所使用的协议号和端口号在数据报头和数据段头中指定。

当一个用户要远程登录到主机上时，就必须为这个发起连接的用户提供远程登录的一个拷贝。连接是通过发起主机的操作系统分配给用户一个端口号（用户A为4016）来提供的。远程主机将连续地运行一个程序，监听端口23上的连接请求。在Unix中，这种在后台连续运行的程序被称为后台驻留程序（daemon），也被专门称为internet.d。一旦在用户与远程主机之间建立起连接，二者就使用telnet协议来进行通信。

在图25-18中，主机 A使用的端口号为4016，主机B的端口号为4021，这些端口号可以帮助TCP区分来自两个不同用户的数据流。图25-18显示了数据如何在远程主机和用户A之间相互交换。当主机A发送一个数据流时，数据的源端口号为4016，目的端口号为23。当这个数据到达主机时，TCP协议从目的端口号23知道这是telnet应用的数据。在相反的方向上，当数据被用户端口的TCP接收到时，TCP通过查看其目的端口号来区别不同的用户。

IP地址被用来唯一地标识Internet中的主机。源端口号与源IP地址的组合被**源套接字**（source socket）。在图25-18中，源IP地址为128.6.18.38，源端口号为4016。这两个数据的组合就是源套接字。与此类似，目的IP地址与目的端口号的结合被称为目的**套接字**（destination socket）。两个套接字之间的通信（在OSI术语中称为“会话”）被叫做连接。一对套接字在整个Internet中被用来唯一地确定一个连接。

25.8 应用层

25.8.1 简单邮件传输协议（SMTP）

基本协议：电子邮件可能是TCP/IP网络中最流行的应用了，它本质上是一种备忘录转发协议。在TCP/IP协议中最上层关于传输邮件的协议就是简单邮件传输协议（SMTP，Single Mail Transfer Protocol），它实际上是一种“对话”协议，可以建立关于邮件消息的某种信息。“对话”协议不像某些协议那样使用二进制码，而是使用7个比特的ASCII码来交换通信控制的消息。像“message number 220”或“MAIL FROM: . . .”等基于ASCII码的消息，使协议的编写和调试更加方便。另一方面，FTP是用二进制码编写协议，为了解释它的各种命令，一个人必须了解十六进制计数系统。

邮件消息实际上分为两个主要部分：“信封”和“正文”。“信封”包含“发给那儿”（To:）与“来自那儿”（From:）两个字段，它们的含义是显而易见的。“正文”部分被当作数据来传送，而且从不被作为协议的一部分来检查。SMTP使用TCP协议作为SMTP会话的基础。在TCP会话建立以后，SMTP的会话类似于下面所示的内容：

```
%mail -v ramteke@pilot.njin.net
220 pilot.njin.net, Sendmail 5.59/SMI4.0/RU1.5/3.08
HELO hercules.rutgers.edu
250 pilot.njin.net Hello hercules.rutgers.edu, nice to meet you
MAIL FROM: <brisco@hercules.rutgers.edu>
250 postmaster... Sender ok
RCPT TO: <ramteke@pilot.njin.net>
250 <ramteke@pilot.njin.net>... Recipient ok
DATA
354 Enter mail, end with a "." on a line by itself
[data is transferred]
.
250 ok
QUIT
221 pilot.njin.net closing connection
```

在这里，mail是发送邮件的命令。“-v”显示SMTP的会话。所有以数字开头的行均来自远程主机或接收主机；所有以字符开始的行均来自本地主机或发送主机。可以看到整个协议是7个比特的ASCII字符，协议单元与英文单词相对应。“Hello”声明区分本地机器和远程机器。“MAIL FROM:”指定了邮件的发送者。“RCPT TO:”明确了最终应该把信息传递给谁（不一定在本地）。“DATA”声明将远程系统置于数据收集模式，它将连续地收集邮件消息的正文，直到某一行中只出现一个“.”字符。“QUIT”声明中止这个SMTP会话。

解释响应：用数字开始的行使发送程序容易分辨返回来的内容，其后的英文注释使人更容易阅读程序。SMTP的响应代码分为5种不同的类别：

100系列的消息是初步的肯定应答。命令已经被收到，但所请求的动作还处于未完成状态，等待确认。

200系列的消息是完成的肯定应答。所请求的动作已经被成功地完成。

300系列的消息指出一个状态的变化。命令已经被收到，但还处于未完成状态，等待接收进一步的信息。

400系列的消息指示出了一个临时性的错误。命令没有收到，所请求的动作并未发生，过

后可以再试。

500系列的消息指示出了一个永久性的错误。命令没有收到，所请求的动作并未发生，不要再试了。

通过学习这些消息类型的例子，对理解它们的分类是有帮助的。100系列的消息不常见。当通过一个网络而不是因特网发送邮件时，才会遇到这类消息。此消息说明，邮件发出去了，但不能确定其是否到达了目的地。

从上面给出的SMTP输出的例子，可以看到200系列和300系列的消息的应用方式。在例子的输出中，“250 Recipient OK”可以替换为一个400系列的消息“420 File system is full”。这个消息说明，接收方的文件系统中没有地方来接收邮件了，发信方应该过一会儿再试。如果用户地址或用户名出现错误，那么在同样的位置就会返回“520 No such user”错误信息。这个500系列的消息告诉发信人不要再尝试发送邮件给这个用户了。

根据第一个数字的不同，发送程序可以决定是否提供另外的信息（即继续发送消息），是否存储信息等待一段时间以后重发（对于临时性错误），或者把消息返回给用户（对于永久性错误）。其他的数字也有类似的含义，这里不再讨论。读者可以参考RFC 821来得到SMTP的详细论述。

协议的各个部分：好在电子邮件的用户不必记忆完整的SMTP协议（实际中的响应代码比上面所提及的更多）。多数邮件系统能从概念上分成3个不同的部分：1) 邮件用户代理（MUA，Mail User Agent）；2) 邮件发送代理（MTA，Mail Transfer Agent）；3) 邮件转发代理（MDA，Mail Delivery Agent）。这3种程序可以作为任何一种电子消息传送系统的模型。

一般情况下，MUA关注于从用户收集特定信息之类的事情，比如消息要发送给谁，主题是什么（这是作为数据来发送的），抄送副本（CC，Carbon Copy）、暗送副本（BCC，Blind Carbon Copy）和文件副本（FCC，File Carbon Copy），以及消息的正文部分。从CC、BCC、TO和FROM字段，可以明确地看出电子邮件是模仿备忘录的。通常MUA还可提供上面没有列出的一些特征，但它可以不这样做。

MTA通常是携带文件（文件中包含电子邮件）的单元，通过对它的充分分析可以确定邮件的发送人与收件人；然后它就与远程系统建立了SMTP会话。当从MTA接收到MDA时，MDA将邮件消息传送给系统中的正确用户（它负责诸如分配可用磁盘空间等工作）。

通常这3种代理由3个不同的程序负责，但不一定要这样做。在某些情况下，特别是在Unix系统中，MTA和MDA通常是相同的——发送邮件就是这样。发送邮件还能够区分通过局域网和因特网所发送邮件的不同方法。

人们开发出了其他的电子邮件协议，如多用途的网际邮件扩充协议（MIME，Multipurpose Internet Mail Extensions），可以支持8位二进制信息和多媒体信息，以及7个比特的纯ASCII文本。

25.8.2 远程登录（Telnet）

RFC 854定义了Telnet协议。这是一个旧术语，是指通过电话网络（TELephone NETwork）建立的拨号连接。此协议比较灵活，可以使不同类型的终端与一台远程主机进行通信，就好像直接操作那台主机一样。为了在一个大的范围内为各类终端提供兼容性，连接的两端设置了一些选项。如果某一端不能够支持某个telnet选项，那么另一端也会被强制不能使用这个选

项。但是，一台拥有众多功能的终端，即使在另一端的低级终端不支持这些功能，也仍旧可以使用这些功能。

在图25-18中可以看到，每个用户（或客户机）与远程主机（即服务器）上的一个虚拟终端之间建立了一个telnet会话。客户机和主机使用被称作网络虚拟终端（NVT，Network Virtual Terminal，）的一系列命令相互进行通信。这些命令可以在一个连接的整个生存期内发送，只有当开始建立连接时这些命令才需要初始化。为了区分数据和NVT命令，要求所有的NVT命令以十六进制的FF开头，以此来通知另一端这是一个NVT命令而不是数据流。RFC 854到RFC 861以及其他一些文档详细说明了这些选项和命令。用十六进制给出它们的细节并不会带来太大的麻烦。

在表25-3中仅列出了4种命令和响应。它们是：DO、WILL、DON'T和WON'T。它们中的每一个既可以是命令也可以是响应，必须与特定的选项一同发送。客户机或者服务器都可以发出这些命令或响应。

表25-3　选项协商可以采用的6种方法

命　令	描　述	响　应	描　述
DO	发送端要求另一端（即接收端）激活此选项	WILL	接收端能够激活此选项
		WON'T	接收端不能激活此选项
WILL	发送端自己希望激活此选项	DO	接收端允许发送端激活选项
		DON'T	接收端不允许发送端激活选项
DON'T	发送端要求接收端关闭此选项	WON'T	接收端不得不同意此选择
WON'T	发送端自己想关闭此选项	DON'T	接收端必须遵从

当一个选项与DO命令一起发送时，要求命令的接收者激活该选项。这时接收端有两种选择：可以通过返回WILL命令而激活选项，或者以WON'T来响应而不激活选项。这些响应列在表25-3的前两行中。

下一行显示了发送端可以通知另一端它自己要激活某个选项。在这种情况下，发送端发送WILL命令。而接收端（可以是服务器也可以是客户机）可以发送DO来做出肯定响应，或者发送DON'T做出否定的响应。

发送端可以发送DON'T来期待另一端关闭某选项。在这种情况下，接收端别无选择只能以WON'T来响应。与此类似，当发送端自己要关闭此选项时，它会发送WON'T，这将迫使接收端发送DON'T来响应。这些是用来激活和关闭选项的信号，使telnet协议可以足够灵活地为任何类型的主机提供远程登录的服务。下面来看一个例子。

参考图25-19，首先，可以看到通过3次握手程序建立了一个TCP连接。所有的TCP报头用深颜色框图显示；它们的标志位已经被设置，并且也显示在这些报头中。

然后主机A为选项Suppress_Go_Ahead发送DO和WILL命令。Go_Ahead选项意味着每次传输之后要发送一个“Go ahead”信号，这个信号就好像用户通过民用无线波段（CB radio）说“通话完毕”一样，使其构成一个半双工信道。关闭该选项会使信道变为全双工信道。请注意，发送了PUSH标志位使该命令立刻传送。

当A发送DO Suppress_Go_Ahead命令时，它会要求B激活此选项。当它发送WILL时，是告知B它（或A）要激活此选项。

主机B确认A的数据段。然后它会将2个单独的telnet响应回传给A。B的WILL用来响应A的DO命令，而B的DO用来响应A的WILL命令。现在连接是全双工的了。

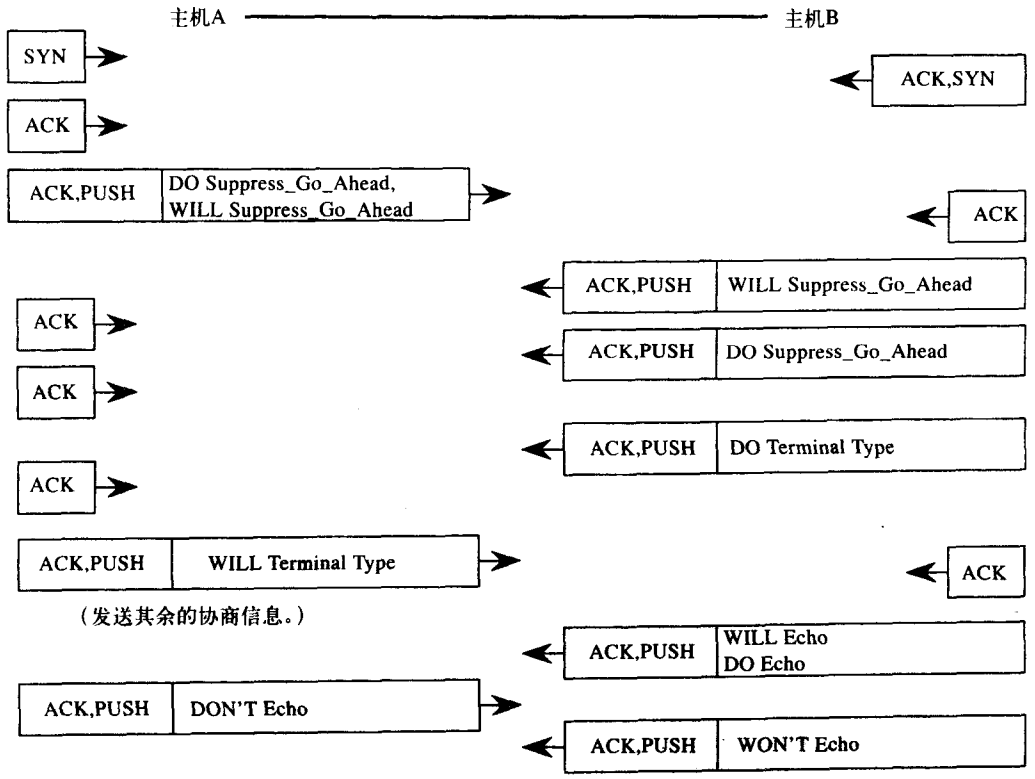


图25-19 一个交换NVT（Network Virtual Terminal，网络虚拟终端）命令和响应的telnet会话的例子。TCP数据段的报头和关键标志设置也显示在框图中

下面，主机B想与A设置终端类型（terminal type）选项，A同意了。此后，它们就将要对所使用的终端类型的细节达成了一致意见，这叫做再次协商，这些信息未示于图中。接下来，主机B要为自身激活Echo选项，同时也要求A激活它。A以DON'T来响应。现在B被迫不能使用该选项，所以会用WON'T来响应。最后信息中的ACK标志被从数据报中去除了。所有这些信息可以在用户得到登录提示信息之前在2台主机之间传送。

25.9 探究网络

25.9.1 网络接口

现在要改变研究方向，来探究一下TCP/IP网络。这里将使用位于Rutgers大学的一台服务器，我在那里有一个账号。该服务器的地址为pilot.njin.net。我们要登录pilot，并看看有什么其他机器连接在它的上面，然后再看看本地网段之外还有什么连接。先来看一下它的ARP表。虽然是在Unix系统中使用这些命令的，但其他操作系统中也有类似的信息。

```
% arp -a
plinius (128.6.18.45) at 08:0:20:9:3e:be
hardees (128.6.18.2) at 08:0:20:9:43:dd
lil-gw (128.6.7.5)  at aa:0:04:0:98:f4
waller (128.6.7.41) at 00:0:0c:1:08:38
```

在这个显示中，主机名称、IP地址以及相应的6个字节的十六进制以太网地址一并被给出。

以太网地址的开始3个字节决定了以太网卡的制造商。plinius和hardees的开始3个字节为8:0:20，说明它们的制造商为美国的Sun公司。 lil-gw正在运行美国数字设备公司（DEC）的网络，所以要求它具有DEC的以太网地址；而waller，即终端服务器的网卡是由Cisco公司制造的。

现在可以得到与pilot有关的部分网络的结构图，如图25-20所示。同时还可以知道（将很快被证明），主机pilot还作为子网128.6.18.0和128.6.7.0之间的网关。当一台主机连接在2个或更多的子网之间时，它就是一个网关设备。因此，所有的网关都是主机，但不一定每台主机都是网关。这里使用术语网关来表示路由器，因为通常都是这样做的。

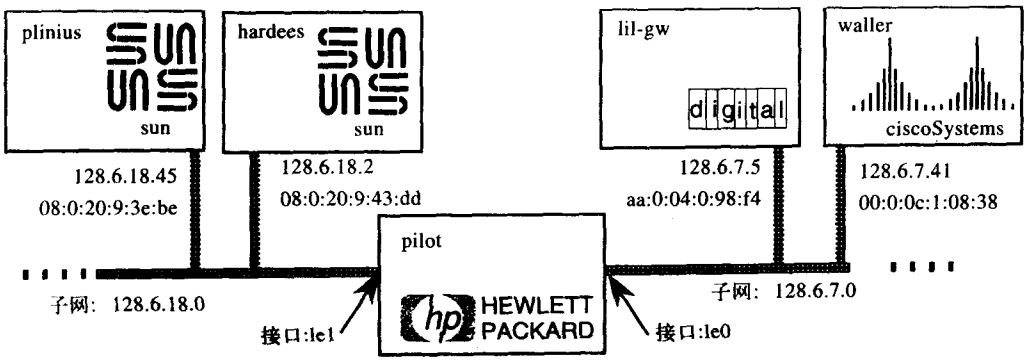


图25-20　从pilot的ARP表得到的部分网络的结构图

为了避免网络出现问题，有关制造商的信息应该与网络系统的物理信息相匹配。举个例子来说，waller确实是Cisco生产的主机，但是如果waller的物理地址以0:0:c开头，那么ARP表可能出现错误。

当一个人配置一台主机时，他很可能给这台主机一个其他主机正在使用的IP地址。例如，如果plinius被配置为不正确的IP地址128.6.18.2，这个地址也是hardees的地址，则主机hardees将会把这个错误消息存入日志，消息的内容是8:0:20:9:3e:be（主机plinius）正在使用重复的IP地址。这样的消息可以在hardees的usr/adm/messages文件夹中找到。

再有，通过在pilot上使用arp -a命令，还可以知道plinius确实正在通告此错误的IP地址。当然，最好的方法是用正确的IP地址重新配置plinius，然后让ARP表自动地更新。但是，也可以手动删除ARP表中关于hardees的错误条目，并在pilot端键入下列命令而增添正确的条目：

```
#arp -d hardees
hardees (128.6.18.2) deleted
#arp -s hardees 8:0:20:9:43:dd
```

符号（#）也被叫做tic-tac-toe，或者说是音乐的升号，用来指示这个命令只能在超级用户的账号下使用。带有-d选项的命令将hardees从ARP表中删除；而带有-s选项的命令使用正确的ARP地址将hardees添加回ARP表中。手动增加条目到ARP表中可以防止ARP表的自动更新。换句话说，plinius不会使pilot认为它在使用hardees的IP地址。hardees决不会接收到来自plinius的数据分组，因为plinius中hardees的MAC地址是错误的。因此plinius的问题无论如何都应该被纠正。

如图25-20所示，通过使用netstat命令，可以证明在pilot上带有2个可以使用的网络接口：

```
pilot%netstat -ain
Name  Mtu        Net/Dest      Address  Ierrs Opkts Collis Queue
le0   1500       128.6.7.0     128.6.7.38   .   ..    ...
```

```
le1  1500      128.6.18.0    128.6.18.38  .   ..      ...
lo0  1536      127.0.0.0     127.0.0.1    .   ..      ...
```

命令中的-i选项要求显示被配置的接口；-a选项要求显示所有这些接口；-n选项采用数字的格式显示地址。如果不使用-n选项，则显示的内容为：

```
pilot%netstat -ai
Name  Mtu      Net/Dest            Address  Ipkts  Ierrs Opkts
le0   1500     BROAD-7-0.RUTGERS.EDU  pilot  .  ..   ...
le1   1500     broad-18-0.rutgers.edu pilot  .  ..   ...
lo0   1536     loopback            localhost  .   ..
```

在这两个显示中，各条目的次序是相同的：唯一的不同之处在于给出的是数字格式的地址还是主机名称。先不管用点表示的字段，因为对于理解基本接口配置并不需要它们。从这两个显示中可以看到，被配置的接口名称为le0、le1和lo0。“le”被用来指代以太网接口，这样的接口有两个：le0和le1。

lo0接口在所有的主机上都存在，被称作本地接口或者环回（lookback）接口。le接口在图25-20的网络结构图上显示出来了；但由于环回接口是一个内部接口，因此不会出现在这样的网络结构图中。环回接口用来在本地主机上进行环回测试，以便检测它是否适于连接到外部网络。在默认情况下，所有主机的环回端口地址都为127.0.0.1。

这两个显示中的地址字段说明了分配给每个接口的IP地址，每个地址都与6个字节的以太网地址相对应。Network/Destination字段显示了通过这个接口可以访问的网络或主机。由于这两个以太网接口的地址均以“.0”结束，因此可以知道它们是子网地址而不是主机地址。例如，假如将一个le2接口添加到pilot上，而这个端口的Net/Dest地址被配置为128.6.10.1，这样就可以知道这个接口只连接到了一台主机，该主机的地址为128.6.10.1。在这种情况下，这就是一个点到点的连接，它只可以访问一台计算机，而不像le0和le1接口那样可以访问整个子网。

25.9.2 子网掩码

我们已经知道在pilot上有2个网络访问接口，现在看一下用IP地址的最后一个字节来划分子网。我们已经通过netstat -ain命令知道了可用接口的名称。使用这些接口名称，可以看到如何使用下面所示的3条命令来配置它们：

```
%ifconfig le0
le0: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
    inet 128.6.7.38 netmask ffffff00 broadcast 128.6.7.255

%ifconfig le1
le1: flags=63<UP,BROADCAST,NOTRAILERS,RUNNING>
    inet 128.6.18.38 netmask ffffff00 broadcast 128.6.18.255

%ifconfig lo0
le0: flags=49<UP,LOOPBACK,RUNNING>
     inet 127.0.0.1 netmask ff000000
```

此处再次看到了分配给每个接口的IP地址，但是现在还要确认子网掩码是否也被正确设置了。注意，子网掩码由十六进制给出。 还要注意，le0和le1的前3个字节是子网掩码，最后1个字节为主机的编号。广播地址要与所设置的子网掩码相符。划分子网的问题已经在第8章讨论过了。

如果子网掩码设置错误，那么一台主机就只能与它自己所在子网上的主机进行通信，而不能与其他子网上的主机进行通信。很快就会看到如何配置子网掩码。

25.9.3 路由表

下面来看看pilot当前的路由表，这是通过使用带有-r选项的netstat命令来完成的。这里，再一次看到了主机和网络名称以及它们地址的数字形式。

```
%netstat -r
Routing tables
Destination          Gateway                Flags        Inter
localhost            localhost              UH           lo0
igor.rutgers.edu     nb-gw.rutgers.edu      UGHD         le0
okapi.rutgers.edu    lil-gw.rutgers.edu     UGHD         le0
default              pilot                  U            le0
broad-18-0.rutgers.  pilot                  U            le1
BROAD-7-0-RUTGERS.E  pilot                  U            le0

%netstat -nr
Routing tables
Destination          Gateway                Flags        Inter
127.0.0.1            127.0.0.1              UH           lo0
128.6.13.26          128.6.7.1              UGHD         le0
128.6.11.3           128.6.7.5              UGHD         le0
default              128.6.7.38             U            le0
128.6.18.0           128.6.18.38            U            le1
128.6.7.0            128.6.7.38             U            le0
```

在这两个显示中，表中条目的顺序也是相同的。从它们的最后一列我们可以找到3个熟悉的接口：lo0、le0和le1。最后2个路由的目的主机（Destination）是128.6.18.0和128.6.7.0。它们均以“.0”结束，所以是指向子网的路由而不是到主机的路由。如果某个目的主机以非0数字结束，那么它一般是一个到主机的路由。另外，通过主机标志(H)的设置也可以看出这一点，H被设置为到主机的路由，未被设置为到子网的路由。

如前面所见，最后2个条目是与pilot直连的2个子网的路由。这些路由条目表明，这些子网的网关都是pilot这台主机。其中一个子网的网关是le1接口（128.6.18.38）；另一个子网的网关是le0接口（128.6.7.38）。显然，所有的路由均已经启动并正常运行，这是因为它们的U（Up）标志都被设置了。

环回接口提供了到本地主机的路由，它总是在路由表中存在。当在路由表中找不到可用的路由条目时，这些数据包就会被传送给默认路由指定的那个网关。这个默认条目可以使路由表不至于太长。举个例子来说，如果想发送数据到NIC.DDN.MIL（192.112.36.5）——它未列在路由表中——那么数据包就被发送到默认网关来进行路由。

最后，有2个路由，一个通向igor，另一个通向okapi。这2个路由均使用远程网关，即连接到其他子网的网关。可以通过设置G标志来表明这一点。在第一种情况下，为igor提供接入的远程网关称为nb-gw；在第二种情况下，为okapi提供接入的远程网关称为lil-gw。这些路由同样设置了它们自己的D标志，表明这些路由是由于有了ICMP重定向而加上去的。

从netstat -nr命令的显示中可以看到，nb-gw的地址为128.6.7.1，lil-gw的地址为128.6.7.5。这表明，这2个网关均在子网128.6.7.0上，这个子网连接到pilot的le0接口。现在，我们的网络结构图如图25-21所示。

25.9.4 追踪路由

怎样才能知道igor和okapi是否恰好直接连在nb-gw和lil-gw的网络中呢？它们中间是否还

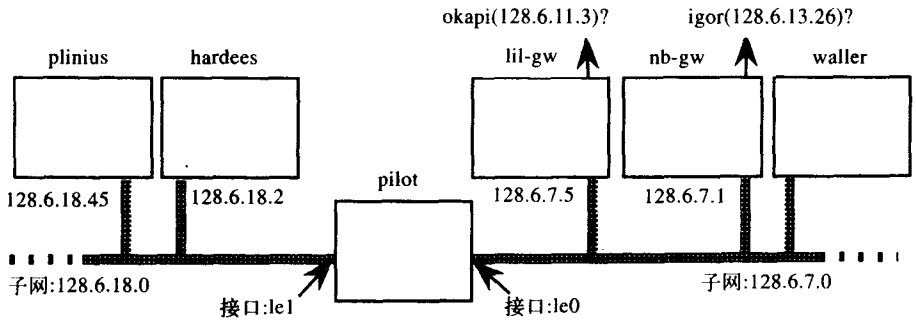


图25-21 查找igor和okapi是否存在。我们可能希望知道它们距离pilot有多远

有其他的网关呢？使用traceroute命令，可以很容易地得到答案。先对igor执行一次traceroute命令。

```
%traceroute igor
traceroute to igor.rutgers.edu (128.6.13.26), 30 hops max,
     40 byte packets
1. nb-gw.rutgers.edu (128.6.7.1) 4ms 2ms 2ms
2. monster.rutgers.edu (128.6.4.3) 2ms 2ms 2ms
3. igor.rutgers.edu (128.6.13.26) 3ms 2ms 2ms
```

pilot会把40个字节的UDP分组传送给traceroute命令中指定的目的地。发送分组使用的是一个非法的端口号33434。发送的第一个UDP分组，它的生存时间（TTL，Time To Live）字段已经被设置成了1。TTL字段是IP数据报头的一部分。当去往主机igor的路由上的第一个网关接收到这个分组时，它会把TTL的值减1，因此路由器不会把这个分组传送到目的地，如图25-22a所示。这时路由器会向发送主机返回一个ICMP消息，说明这个UDP分组的TTL已经超过了。

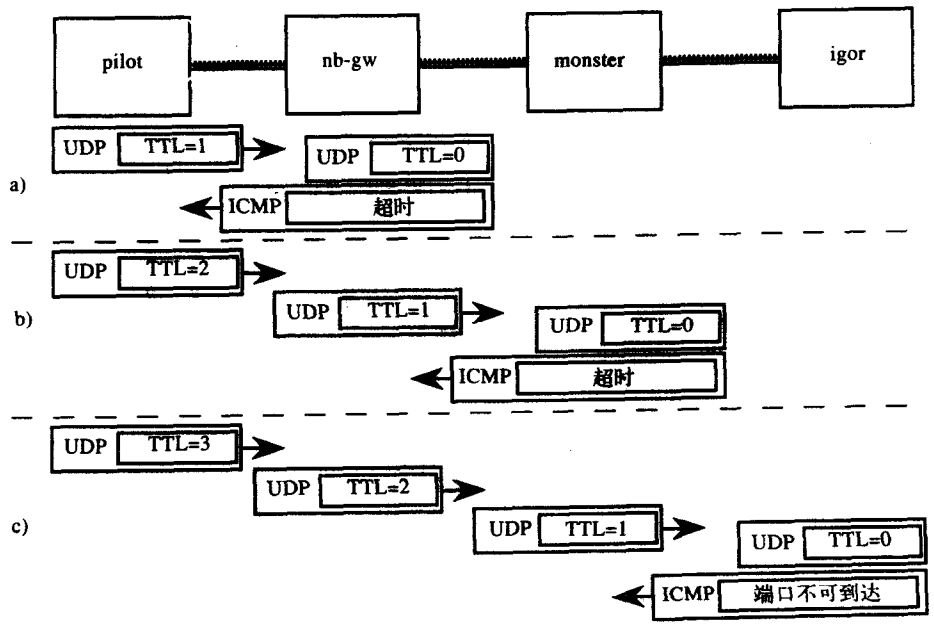


图25-22 当对某个地址执行traceroute命令时，pilot会不停地发送UDP分组，并将TTL的值逐步提高，每次增加1，直到它接收到发送回来的端口不可到达的ICMP报文

通过ICMP消息中的IP数据报源地址，pilot会知道这个ICMP消息是谁发送的。在这里，ICMP消息是nb-gw发送的。pilot还会测量分组到达目的地所需的往返时间。TTL设置为1，这个过程重复3次，每次均测量时间。在这个例子中，3次测量的时间分别为：4 ms、2 ms和2 ms。

现在如图25-22b所示，pilot会进行相同的过程，但这次TTL的值设置为2。nb-gw将TTL减1，并将分组转发到monster。但是monster将TTL的值减为0，这样就不能再继续转发分组了。所以，monster将一个ICMP超时消息发送回pilot。现在，pilot知道了第2跳的网关和到达它所需的往返时间。

最后，在图25-22c中，pilot发送UDP分组并把TTL的值设置为3。因为发送的数据能够到达目的地，所以这次pilot不会再接收到超时的消息，但是会收到端口不可到达的报文。pilot知道数据已经到达了最后的目的地。UDP数据分组中的端口号被特意设置成一个非法端口号，以此来检测ICMP消息。请注意，TTL的值为2的3个UDP数据分组每一个的往返时间都是2 ms，而TTL的值为3的3个UDP数据分组的往返时间则分别为3 ms、2 ms和2 ms。

现在我们知道在通往igor的路上，还存在另一个称为monster的网关。类似地，当我们对okapi执行一次traceroute命令时，就会遇到另一个叫做waks-gw的网关，它是lil-gw和okapi之间的网关。这次，使用okapi地址的数字形式来执行下列的traceroute命令：

```
%traceroute 128.6.11.3
traceroute to 128.6.11.3 (128.6.11.3), 30 hops max,
     40 byte packets
1 lil-gw.rutgers.edu  (128.6.7.5)  9ms 2ms 2ms
2 waks-gw.rutgers.edu (128.6.12.3) 5ms 3ms 3ms
3 okapi.rutgers.edu   (128.6.11.3  3ms 3ms 4ms
```

数据报经过不同的路由传送并且彼此独立，所以traceroute命令中显示的时间不是保持不变的。现在整理从traceroute命令得到的所有信息，新的网络结构图如图25-23所示。

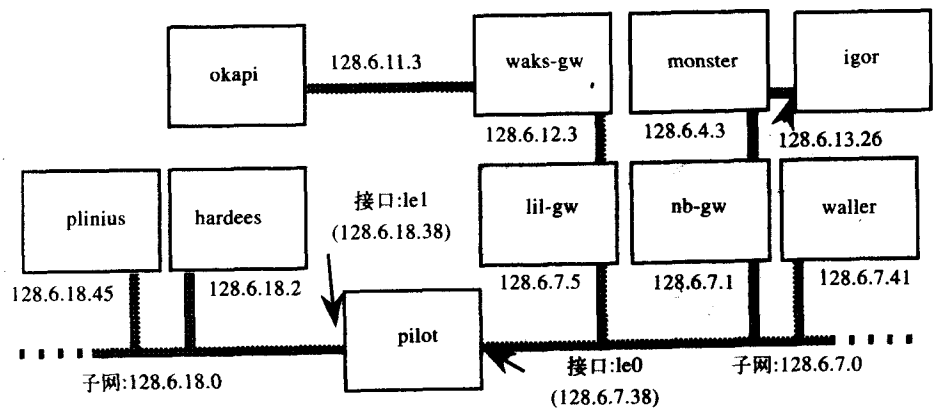


图25-23　在网络中加入更多的网关和接口

图25-24a显示了对一台在日本的主机rins.st.ryukoku.ac.jp执行的一次更有意义的traceroute命令。.jp说明这个主机在日本。在这条路由上的许多网关都是根据它们所处的城市来命名的。例如，可以很容易地看出，该路由在到达位于日本的最后3个网关之前，经过了芝加哥、旧金山和夏威夷。还可以看到，当到达位于夏威夷或日本的第1个网关时，所需时间的显著波动。依靠链路延迟的情况，这些测量到的时间不是固定不变的。

图25-24b显示了一次失败的traceroute命令。这里，ru-alternet-gw后面显示了1组3个通配符，表明问题出现在该节点和以后的某节点之间。这些通配符最多可重复30次。

```
%traceroute rins.st.ryukoku.ac.jp
traceroute to rins.st.ryukoku.ac.jp (133.83.1.1), 30hops max, 40byte packets
 1  lil-gw (128.6.18.30)  3 ms  2 ms  2 ms
 2  ru-alternet-gw (128.6.21.8)  2 ms  3 ms  2 ms
 3  Washington.DC.ALTER.NET (137.39.18.1)  11 ms  9 ms  10 ms
 4  ENSS136.t3.NSF.NET (192.41.177.253)  14 ms  12 ms  12 ms
 5  t3-1.Washington-DC-cnss58.t3.ans.net  (140.222.58.2)  14 ms  13 ms  16 ms
 6  t3-3.Washington-DC-cnss56.t3.ans.net  (140.222.56.4)  17 ms  13 ms  16 ms
 7  t3-0.New-York-cnss32.t3.ans.net  (140.222.32.1)  18 ms  20 ms  19 ms
 8  t3-1.Cleveland-cnss40.t3.ans.net  (140.222.40.2)  34 ms  34 ms  41 ms
 9  t3-2.Chicago-cnss24.t3.ans.net  (140.222.24.3)  44 ms  46 ms  40 ms
10 t3-1.San-Francisco-cnss8.t3.ans.net  (140.222.8.2)  83 ms  83 ms  80 ms
11 t3-0.San-Francisco-cnss9.t3.ans.net  (140.222.9.1)  81 ms  85 ms  84 ms
12 t3-0.enss144.t3.ans.net  (140.222.144.1)  83 ms  83 ms  84 ms
13 ARC2.NSN.NASA.GOV  (192.52.195.11)  93 ms  96 ms  87 ms
14 imp.Hawaii.Net (132.160.249.1)  141 ms  141 ms  148 ms
15 menehune.Hawaii.Net (132.160.1.1)  138 ms  146 ms  144 ms
16 132.160.251.2 (132.160.251.2)  257 ms  409 ms  392 ms
17 jp-gate.wide.ad.jp (133.4.1.1)  392 ms  341 ms  251 ms
18 wnoc-kyo.wide.ad.jp (133.4.7.2)  336 ms  351 ms  331 ms
19 rins.st.ryukoku.ac.jp (133.83.1.1)  355 ms  373 ms  484 ms
```

a)

```
%traceroute rins.st.ryukoku.ac.jp
traceroute to rins.st.ryukoku.ac.jp (133.83.1.1), 30hops max, 40byte packets
 1  lil-gw (128.6.18.30)  3 ms  2 ms  2 ms
 2  ru-alternet-gw (128.6.21.8)  2 ms  3 ms  2 ms
 3  * * *
 4  * * *
 .  .
30  * * *
```

b)

图25-24 a)对日本的主机执行traceroute命令，b) 一次失败的traceroute命令

要检查某台主机是否启动并运行，一个较好的方法是使用ping命令，它不像traceroute命令那样占用过多的网络带宽。这里有一个例子，是使用56字节数据对位于澳大利亚的一台主机执行了两次ping命令：

```
%ping -s csuvax1.murdoch.edu.au 56 2
PING csuvax1.murdoch.edu.au
64 bytes from csuvax1.murdoch.edu.au (134.115.4.1):
     icmp_seq=0. time = 3299 ms
64 bytes from csuvax1.murdoch.edu.au (134.115.4.1):
     icmp_seq=1. time = 2975 ms
2 packets transmitted, 2 packets received, 0% packet loss
```

很显然，如果对子网128.6.12.0中的所有可能地址执行ping命令，那么就可以找出与lil-gw直连的所有主机，并可以扩展图25-23所示的网络映射图。类似地，可以用同样的方法探测其他子网，但是你的网络管理员可以容易地将网络结构图提供给你以供使用，从而防止你占用过多的网络带宽。

25.10 建立新的子网

25.10.1 配置接口

现在，通过增加一个标记为128.6.101.0的新子网来扩展网络。在这个子网上，需要增加

一个被称为pascal（128.6.101.2）的工作站，并把它通过称为ada的网关与子网128.6.18.0连接起来。图25-25是由网络管理员为它们分配的地址。首先为pascal配置接口，然后是ada。

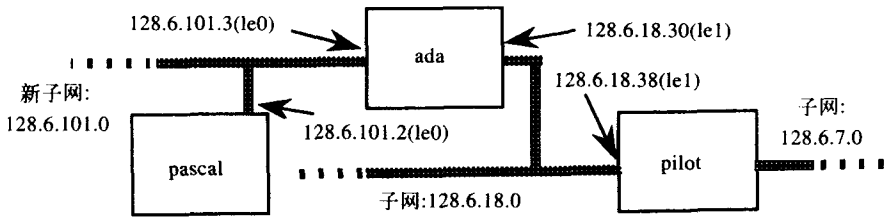


图25-25　增加一个新子网（128.6.101.0）

在pascal的启动文件/etc/rc.boot中，增加了这些行（斜线是一个连接符，可以使一条命令占用多行）：

```
ifconfig        lo0 127.0.0.1
ifconfig        le0 128.6.101.2 netmask 255.255.255.0 \
                    broadcast 128.6.101.255
```

这样，每次pascal启动后，环回接口和le0接口都能正确地被设置。与以前一样，还是用地址的最后一个字节来划分子网。

如果由于某种原因需要从网络中禁止le0接口，则可以输入：

```
#ifconfig le0 down
```

要使这个接口重新启动，则可以输入：

```
#ifconfig le0 128.6.101.2 up
```

同样地，对于ada的启动文件，可以加入以下行：

```
ifconfig lo0 127.0.0.1
ifconfig le0 128.6.101.3 netmask 255.255.255.0 broadcast \
             128.6.101.255
ifconfig le1 128.6.18.30 netmask 255.255.255.0 broadcast \
             128.6.18.255
```

25.10.2　配置静态路由

执行过这些ifconfig声明后，pascal的路由表如下：

```
%netstat -nr
Routing tables
Destination        Gateway          Flags  ...   Interface
127.0.0.1          127.0.01         UH            lo0
128.6.101.0        128.6.101.2      U             le0
```

注意，因为只给出了到它本身子网的路由器，所以pascal还不能连接到pilot。

```
%ping pilot
Sendto: Network is unreachable
```

要添加从pascal到pilot的路由，可以输入如下的命令：

```
#route add 128.6.18.38 128.6.101.3 1
```

这会在pascal的路由表中添加128.6.18.38的路由条目，把ada上的le0端口128.6.101.3作为它的网关。128.6.101.3这个接口一定是pascal所在子网的一个网关。这样的网关与pascal之间只有一跳的距离。命令行中最后的1表明跳数是1。

但是，为什么只为一台主机增加路由呢？让我们为128.6.18.0这个子网来增加路由。

```
#route delete 128.6.18.38
#route add   128.6.18.0  128.6.101.3  1
```

路由删除命令可以删除到pilot的路由条目，路由添加命令可以为子网128.6.18.0增加路由。接下来做进一步的配置，把apa作为其他所有子网的默认网关。这可通过下令命令实现：

```
#route -n add default   128.6.101.3 1
add net default: gateway 128.6.101.3
```

所以，现在pascal的路由表应该如下所示：

```
#netstat -rn
127.0.0.1          127.0.0.1          UH        lo0
default            128.6.101.3        UG        le0
128.6.101.0        128.6.101.2        U         le0
```

下列的命令会把pilot作为ada的默认网关。

```
#route -n add default 128.6.18.38 1
```

所以，现在ada的路由表应该如下所示：

```
#netstat -rn
127.0.0.1          127.0.0.1          UH        lo0
default            128.6.18.38        UG        le1
128.6.101.0        128.6.101.3        U         le0
128.6.18.0         128.6.18.30        U         le1
```

25.10.3 配置动态路由

与把ada配置成静态路由相比，把它配置成动态路由是一个更好的选择。这就是说，在网关上运行路由协议。在我们的例子中，由于仅连接了两个子网，使用RIP路由协议就足够了。如果与另外一个不同的域互连，也许还需要运行EGP或BGP协议。用于运行RIP的路由后台程序称为可路由的协议，而运行RIP、Hello、EGP和BGP的后台程序称为网关路由协议。

为了运行可路由的程序，仅需要输入：

```
#routed
```

当从启动文件开始可路由程序时，可路由的程序将搜索/etc/gateways文件夹中的文件，看看是否有路由被预先设定了。在ada上，在这个文件中规定了默认路由如下：

```
net 0.0.0.0 gateway 128.6.18.38 metric 1 active
```

这里，net把这个地址定义为一个网络地址。如果它是一个主机地址，那么这一行将以关键字host开始。0.0.0.0这个网络地址表示的是默认路由。跟在关键字gateway后面的地址表明128.6.18.38是这个路由所使用的网关。metric 1表明到目的地的跳数；而active意味着，如果有必要RIP协议就可以更新这个路由。如果在所分配的时间帧内没有接收到更新消息，RIP 就删除它。也就是说这个网关可以把更新消息发送给其他网关。相反地，被动的路由将指定的路由作为静态路由，这样RIP就不能更新或删除它。

25.11 域名服务

25.11.1 目的和作用

到目前为止，我们一直在交替地使用主机名和地址，然而，并没有提到如何将一个名字转换成与它相对应的IP地址，而这又是产生数据包时所必须完成的。例如，在图25-24中，当

要求主机pilot执行到rins.st.ryukoku.ac.jp的traceroute命令时，pilot是如何知道目的主机的IP地址是133.83.1.1的呢？这是由一个叫做域名服务（DNS，Domain Name Service）的服务来完成的。它允许人们使用主机名称来代替IP地址，这样更便于人们记忆。将名称转换成正确的IP地址则是DNS的工作。

DNS使用一个分布式层次结构的数据库来实现这个功能，数据库中包含有主机名和相对应的地址信息，如图25-26所示。在最顶层是一个根域，这个域由一系列名称服务器为之提供服务，这些服务器中仅存储着顶级域名服务器的信息。net、mil等都是顶级域名的例子。在顶级域的服务器中，存储的则是关于二级域服务器的信息，以此类推。每个服务器存储着它下面低一级的域服务器信息，这样就不必用一个巨大的文件来存储因特网上成千上万的主机名称和地址。

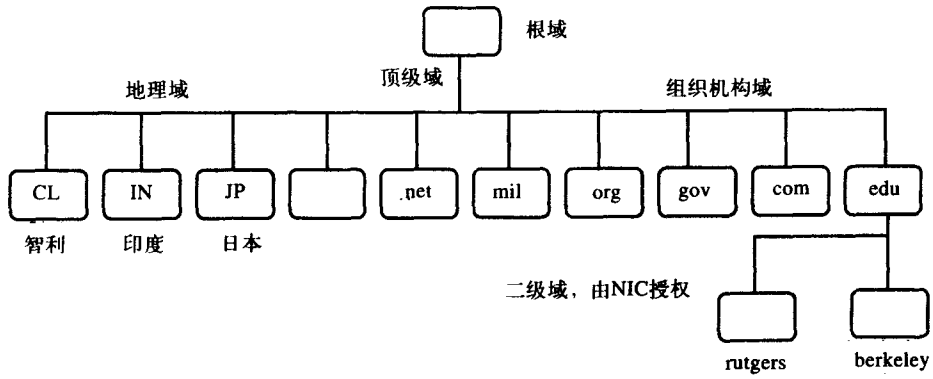


图25-26　域的层次结构图

如果一个本地服务器，比如pilot.njin.net，想找一个名为rins.st.ryukoku.ac.jp的主机的地址，pilot首先会在自己的内存（或存储器）中查找。如果没有找到所需的地址，那么它就会根据所给的主机名称去寻找相关子域的服务器地址。如果这些服务器也不能在它们的内存中找到所需的地址，就会到根域服务器去查询。根域服务器将会把jp域服务器的地址告诉主机，从根域得到的那个服务器将会同样把ac.jp域服务器的地址告诉主机。这个过程会不断重复，直到pilot得到rins.st.ryukoku.ac.jp的IP地址。

本地服务器就会把这个主机的地址连同所有它遇到的域服务器的地址一同存储起来，这样做是为将来作为参考使用。那么如果主机需要连接在st.ryukoku.ac.jp子域中的另一台主机，那么主机就会知道到哪个域服务器去查找所需的地址。需要注意的是在一个名称中，使用小数点来区分每一个子域。例如，ac是jp域中的一个子域；而ryukoku是ac域中的一个子域。还要注意的是子域和子网络没有必然联系。

25.11.2　域名服务器（DNS）

大多数UNIX系统使用伯克利因特网命名域（BIND，Berkeley Internet Name Domain）软件来实现DNS功能。这个软件是基于客户端和服务器模型的。如图25-27所示，所有的计算机都作为客户端可以直接去查询服务器，服务器可以响应客户端的查询请求。如果服务器不能响应请求，那么它至少可以提供一个可响应这个请求的服务器地址，或者是提供一个名称服务器，这个名称服务器转发这个请求，查找可以响应这个请求的另一个名称服务器。这就是具有高速缓存功能的名称服务器获得新地址的过程。在BIND中，客户端被称为解析器，而服务器被叫做名称服务器。

如图25-27所示，共有三种服务器。主服务器从本地硬盘中装载域名的信息，这个信息被称为区域文件。在这里，区域这个词被用于表示域。这个区域文件由域管理员来维护，其中包含了域中的最新信息。其他的服务器从主服务器获得它们所需的信息。每个域中仅有一台主服务器。

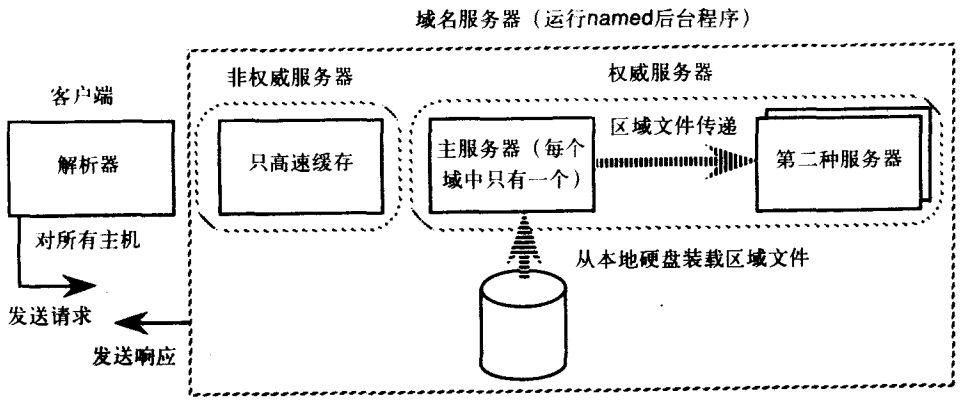


图25-27 DNS服务所使用的客户端-服务器模型

第二种服务器被用来对主服务器进行备份，并通过执行区域文件的传递，定期地从主服务器获得相关的信息。主服务器和第二种服务器都被认为是权威或控制服务器。

还有只完成高速缓存功能的服务器，它不是权威服务器。只有在一个解析器查询它们所没有的信息时，缓存服务器才会更新域的信息。缓存服务器会查找可以响应这个请求或知道谁能响应这个请求的服务器。一旦获得所需的信息，缓存服务器会把该信息存储起来，这些信息可以为将来提供参考。

配置一个解析器，只需要/etc/resolv.conf文件。这个文件是BIND常规库所必需的。另外，服务器要运行一个叫做named的后台程序，它由以下5个文件来配置：named.boot文件规定了在哪里提供可用的域信息；named.ca文件规定了根域服务器的位置；named.local文件规定了本地环回域；而named.hosts和named.rev则是区域文件，它们将主机名称转换成IP地址，或者把IP地址转换成主机名称。

named.boot文件包含配置命令，而其他4个文件使用资源记录来存储信息。资源记录有一个标准模式，每个记录可由它的记录类型来分类。一些记录类型如表25-4所示。

表25-4 DNS中使用的资源记录类型

类 型	类型含义	功 能
A	地址	把主机名映射为IP地址
CNAME	规范名称	主机的别名
HINFO	主机信息	CPU和操作系统的名称
MINFO	邮箱信息	邮件列表或者邮箱信息
MX	邮件服务器	域中邮件服务器的名称
NS	名称服务器	域中管理服务器的名称
PTR	指针	把IP地址映射为主机名称
SOA	授权开始	规定区域实现的参数

25.11.3 nslookup

下面，使用一个叫做nslookup的工具来更好地熟悉DNS。先看看下面图25-28所示的对话框。

```
%nslookup
nslookup: command not found
%wherels nslookup
/usr/etc/nslookup
%/usr/etc/nslookup

Default Server: pilot.njin.net
Address:        128.6.7.38

>hardees.rutgers.edu.    (Default record
non-authoritative answer:  type is A.)
Name:    hardees.rutgers.edu
Address: 128.6.18.2

>set type=NS
>.
Default Server: pilot.njin.net
Address:        128.6.7.38

non-authoritative answers:
(root) nameserver = NS.NIC.DDN.MIL
(root) nameserver = Terp.UMD.EDU
(root) nameserver = NS.NASA.GOV
   :          :              :
authoritative answers can be found from:
NS.NIC.DDN.MIL inet addr. 192.112.36.4
Terp.UMD.EDU   inet addr. 128.8.10.90
NS.NASA.GOV    inet addr. 128.102.16.10
    :              :              :
>server terp.umd.edu.
Default server: terp.umd.edu
Address:        128.8.10.90

>nasa.gov.
Default server: terp.umd.edu
Address:        128.8.10.90
non-authoritative answers:
nasa.gov nameserver = NS.NASA.GOV
    :          :              :
authoritative servers can be found from:
NS.NASA.GOV inet addr. 128.102.16.10
NS.NASA.GOV inet addr. 192.52.195.10
        :          :              :

>berkeley.edu.
        :          :          :
authoritative servers can be found from:
Vangogh.cs.Berkeley.edu  addr = 128.32.130.2
VIOLET.Berkeley.EDU inet addr =
128.32.136.22
UCBVAX.Berkeley.EDU inet addr =
128.32.133.1

>server vangogh.cs.berkeley.edu.
Default Server: vangogh.cs.berkeley.edu
Address:        128.32.130.2

>cs.berkeley.edu.
        :          :          :
ucbvax.berkeley.edu inet addr. = 128.32.130.12
ucbvax.berkeley.edu inet addr. = 128.32.149.36
vangogh.cs.berkeley.edu addr. = 128.32.130.2

>set type=A
>ls cs.berkeley.edu > ourfile
>view ourfile              (Security concern: ls)
CS      128.32.131.12
CS      server = ucbvax.Berkeley.edu
CS      server = vangogh.cs.berkeley.edu
acacia  128.32.131.120
adder   128.32.130.64
al      128.32.131.144
 :         :      :

>al.cs.berkeley.edu.
Default server: cs.berkeley.edu
Address:        128.32.131.12

Name:           al.cs.berkeley.edu
address:        128.32.131.144

>set query=HINFO  (Security concern: HINFO)
>al.cs.berkeley.edu.
Default server: cs.berkeley.edu
Address:        128.32.131.12

al.cs.berkeley.edu  CPU= ti/explorer, OS=lisp
```

图25-28　使用nslookup的一个会话实例

开始先键入“nslookup”，但是在当前的路径下找不到这个命令。向系统询问它的位置，系统发现它在/usr/etc文件夹中。在这个路径下，再次执行nslookup进入程序。

首先它列出默认服务器pilot，如果不做修改，那么它就是处理所有请求的名称服务器。向它提出一个请求，要查询一个主机（hardees）的IP地址。由于nslookup默认情况下的记录类型被设置为A，如表25-4所示，这个记录类型是把主机名称映射为相应的IP地址，因此pilot可以找到这个地址。

可以通过set命令改变记录类型，就像接下来所做的一样。把记录类型改为NS（Name

Server)，这个记录类型将一直保持为NS直到再次改变它。

现在通过键入一个小数点来进入根域。由于记录类型被设为NS，因而可以获得根域的服务器（见前面的图25-26)。在这些显示中，我们不想看到所有的服务器。使用server命令，现在就可以把默认的名称服务器从pilot改为一个之前列出的根域服务器terp.umd.edu。

接下来，看一下域的下一个层次，并列出nasa.gov子域中的服务器，之后再列出berkeley.edu子域中的服务器。在这里，将默认服务器改为berkeley.edu域中的一个服务器，并寻找子域cs.berkeley.edu中的服务器。

现在，将记录类型重新设置为A，并使用如图25-28所示的ls命令。这会把cs.berkeley.edu域的信息（或源记录）记录到pilot主机上一个名为ourfile的文件中。通过view命令，可以看到这个文件的内容。这个文件保存了cs.berkeley.edu子域中的主机名和相对应地址的全部列表；如果记不住在这个子域中主机名的正确拼写，那么这个文件是非常必要的。

当然，如果仅仅需要cs.berkeley.edu域中一个特定主机的地址，也可以只查询cs.berkeley.edu服务器，而不用传送整个列表。像图中接下来所示的那样，查询也可由pilot自己来响应。最后，发送对主机信息的查询请求，从而得到al.cs.berkeley.edu这台主机的CPU类型和它所使用的操作系统。

25.11.4 DNS查询过程

最后举一个例子，从DNS的角度看一下DNS的信息查询。从这里可以看到在不需要其他名称服务器为整个网络提供信息的情况下，每个域如何控制和管理它的子域名称服务器。如果要让DNS给出al.cs.berkeley.edu的IP地址，那么它就会很快地把结果告知我们。下面逐步深入，看看DNS如何获得所需要的IP地址。

在图25-29的上部，将记录类型设为NS（Name Server)，这样就只会显示那些与请求相关的记录。就像在图25-28中所示的一样，输入根域（“.”）就可以得到它的名称服务器。

然后输入“edu.”，这样可以得到“edu ”域的名称服务器。要注意在“edu”后面的小数点(“.”)。从提供的服务器列表中，通过使用server命令来选择ns.nic.ddn.mil作为edu域的名称服务器。

从这个名称服务器，再查看berkeley.edu域的名称服务器。从列出的服务器中，选择vangogh.cs.berkeley.edu作为berkeley.edu域的服务器。然后从vangogh.cs.berkeley.edu上查询cs.berkeley.edu域的名称服务器，并选择ucbvax.berkeley.edu作为cs.berkeley.edu域的服务器。现在把ucbvax.berkeley.edu作为可查询的名称服务器，来查询关于主机al.cs.berkeley.edu的信息。

在这里，会得到一个错误消息，这是因为记录类型还被设置为NS，而al.cs.berkeley.edu是一台主机而不是一个域，所以它并没有名称服务器。将记录类型的值改为“any”，这样就可以获得这台主机的许多信息，其中包括这台主机的IP地址。最后，退出nslookup程序。

25.11.5 反向查询

根据一台主机的IP地址查找它的主机名的功能同普通主机名查找非常近似。在图25-30中，正在寻找一台位于澳大利亚且IP地址为134.115.4.1的主机的名称。要查找与IP地址134.115.4.1对应的主机名，名称服务器的库会形成一个名称“1.4.115.134.IN-ADDR.ARPA.”，注意，这个地址是反向的，而且是在IN-ADDR.ARPA域中寻找——“IN-ADDR”是指因特网地址(Internet Address)。

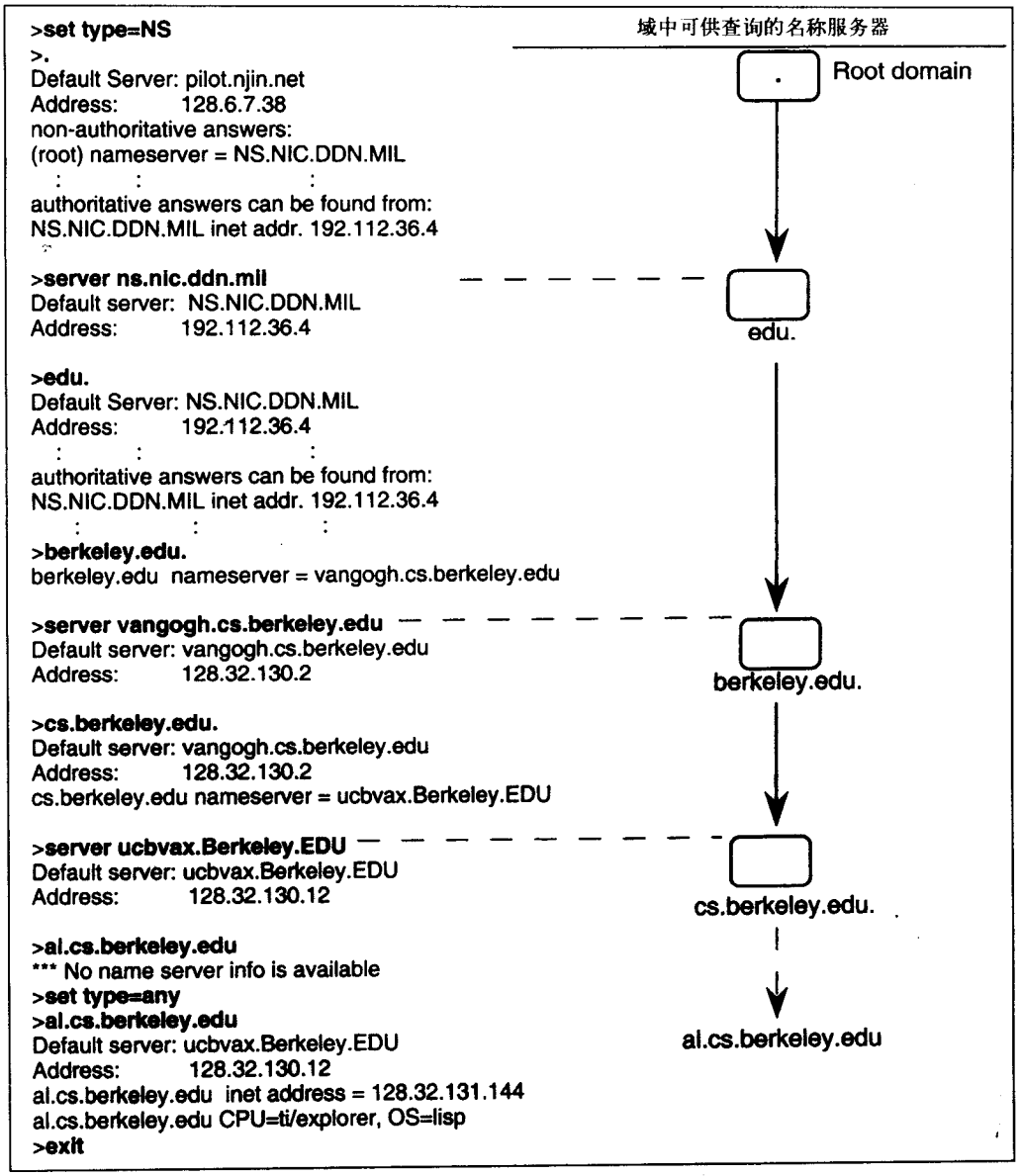


图25-29　对al.cs.berkeley.edu做查询。每次查询只显示了一台名称服务器

当查找“IN-ADDR”名时，一个名称服务器在它的内存中查找IN-ADDR.ARPA名称服务器的地址。如果找不到，那么就要连接到根域名称服务器。在同IN-ADDR.ARPA名称服务器的会话中，本地名称服务器会询问根域名称服务器关于134.IN-ADDR.ARPA这个域的名称服务器。当本地名称服务器查询115.134.IN-ADDR.ARPA域的名称服务器时，它就会接收到一个“edu.au”的地址，这是因为134.115这个网络属于“edu.au.”。本地服务器将会继续查找，直到找到1.4.115.134.IN-ADDR.ARPA的名称服务器。当询问名称服务器关于1.4.115.134.IN-ADDR.ARPA的名称服务器时，就会产生错误信息，这是因为它根本就没有名称服务器。这时会得到“PTR”类型的记录，也就能知道1.4.115.134.IN-ADDR.ARPA（134.115.4.1的地址）的主机名是“csuvax1.murdoch.edu.au.”。

```
>set type=any
>.
Default Server: pilot.njin.net
Address:        128.6.7.38
authoritative answers can be found from:
NSINTERNIC.NET inet addr.  198.41.0.4
   :          :                :
>server 192.112.36.4
Default server: [198.41.0.4]
Address:        198.41.0.4
                          (Don't forget this dot.)
>in-addr.arpa.
Default server: [198.41.0.4]
Address:        198.41.0.4
*** No any type information is available . . .

>134.in-addr.arpa.
Default server: [198.41.0.4]
Address:        198.41.0.4

>115.134.in-addr.arpa.
Default server: [198.41.0.4]
Address:        198.41.0.4
115.134.in-addr.arpa
  nameserver=ns.adelaide.edu.au

>server ns.adelaide.edu.au
Default server: ns.adelaide.edu.au
served by:
  MUNNARI.OZ.AU
        128.250.1.21

>4.115.134.in-addr.arpa.
Default server: ns.adelaide.edu.au
served by:
  MUNNARI.OZ.AU
        128.250.1.21
4.115.134.in-addr.arpa
  nameserver=csuvax2.csu.murdoch.edu.au

>1.4.115.134.in-addr.arpa.
Default server: ns.adelaide.edu.au
served by:
  MUNNARI.OZ.AU
        128.250.1.21
1.4.115.134.in-addr.arpa.
  hostname=csuvax1.murdoch.edu.au

>exit
```

图25-30 对134.115.4.1进行反向查询

当给出主机名时，会有已定义的层次结构以便查找它的地址。而当给出地址的时候，也会有一个镜像的层次结构以便查找它的主机名。这两个过程是非常相似的。

习题

25.2节

1. 假设你看到一个以太网帧的头信息，你如何确定这个帧是一个ARP数据包还是一个RARP数据包？
2. 在一个数据包中，如果要知道这是一个ARP/RARP的请求还是响应，应该察看数据中哪个字段的值？
3. 代理ARP的目的是什么？
4. ARP是否只能与IP协议一同工作？PPP和SLIP又如何？
5. 在一个PPP数据帧中，哪个字段没有用到？
6. 把下面PPP的各状态与它们的正确描述连接起来：

认证状态（Authentication State）	A. LCP数据分组已被发出
网络状态（Network State）	B. 空闲状态
停滞状态（Dead State）	C. 这里可以使用PAP或CHAP
建立状态（Establish State）	D. 数据可以在这个状态传输

25.3节

7. 在IPv4的报头中，哪个字段用来决定是否使用选项字段？
8. 在IPv4的报头中，哪个字段用来控制数据报可以经过的跳数？

9. 所有主机都可以接收的数据报长度的上限是多少?
10. 如果一个路由器无法传送一个较大的数据报，那么它会如何处理数据报?
11. 从同一个数据报派生出来的所有分段，哪些字段是相同的?
12. 是中间路由器还是终端主机将数据分段重新组合成一个数据报?
13. 如何计算一个数据报中数据部分的长度?

25.4节

14. 假设我们希望把从196.0.0.0到199.255.255.255这个地址范围化为一个超网，那么
    a. 超网地址需要用多少个字节?
    b. 主机地址可以用多少个字节?
    c. 超网掩码是什么?
    d. 如何用“/”来表示IP地址198.183.20.34?
15. CIDR使用的是什么路由协议?
16. DHCP派生自什么协议?
17. 下面的每一种协议如何保存IP地址：CIDR、DHCP、NAT服务器和代理服务器?
18. 在DHCP帧中，哪一字段决定是否使用以太网?
19. 当创建你自己的基于IP的网络时，使用RFC 1918中描述的专用IP地址有什么优点和缺点?
20. 比较并对比一下NAT服务器和代理服务器。
21. 你能说出将IPv4转换成IPv6的原因是什么吗?

25.5节和25.6节

22. 一个UDP报头有多长? 一个ICMP报头有多长?
23. TCP报头中的哪些字段也同样出现在UDP报头中?
24. 哪一个类型的ICMP报文使用的编码最多? 这个类型的十进制形式是什么? 你能指出收到这个错误报文的原因吗?

25.7节

25. 如果一台主机在TCP层收到一个出错的数据段，那么它会怎么办?
    a. 它会发出一个NAK信号。
    b. 它会请求传送进程减小窗口的大小。
    c. 它只是等待这个数据段被重新发送。
    d. 它会将ACK标志置为0。
26. 主机A怎样才知道它已从主机B接收到1000个字节的数据? 描述一下各字段以及它们的值。
27. 主机A如何减缓来自主机B的数据传输速度?
28. 主机A如何确认TCP数据段通过网络被立即发送了?
29. 通过另外哪一个字段的值可以知道确认编号字段是有效的? 如何确定紧急指针字段是有效的?
30. 在什么阶段、哪一台主机可以设置SYN标志值?
31. 在什么阶段、哪一台主机可以设置FIN标志值?
32. 如何确定一个TCP数据段的长度?
33. 一个源套接字由哪两个字段组成?

25.8节

34. SMTP使用哪个端口？它调用哪个传输层协议？
35. 在SMTP消息中，哪些表明一个永久的错误？
36. 通过什么样的十六进制顺序，一个主机可以知道数据流结束，将下一个字节看作是一个NVT命令？
37. 哪两个NVT命令需要接收者遵从发送者的请求？
38. 远程登录（Telnet）应用使用了什么样的机制来为不同类型的终端提供灵活的服务？

25.9节和25.11节

39. 哪个命令可以显示路由表的状态？
40. 哪个命令能列出到远端主机所经过的网关？
41. 显示一个路由表时，可以使用什么标志？它们的含义是什么？
42. 解释一下什么是环回地址？
43. 在BIND软件中使用什么类型的服务器？
44. 子网和子域的相同点和不同点是什么？

第26章 Linux管理

26.1 简介

从本书中我们已经学到了一些组网知识，然而真正理解这些概念的最佳方法是在实际的网络中使用它们。在本章中，我们将建立一个网络，并且做一些基础性的管理工作以便更好地理解基于TCP/IP体系结构的网络。我们将给其他一些用户创建账户，从其他用户那里接收电子邮件，并向其他用户发送电子邮件，实现文件共享，创建一个小型的万维网，同时完成另外的一些任务。此外，还会完成一些网络管理任务，诸如创建子网，增加安全性，甚至于做一些DNS配置。当然，本章不是要对管理问题给出详尽的指导，只是重点介绍一些关键内容，以便能帮助你详细地了解一些必要的细节。

利用本章的内容，你可以方便地为自己设计一个“实验室”并作为一个可运行的实际网络的“练习场”。这里所要做的主要工作是搭建一个不与因特网相连接的实验室环境。在没有对网络做深入研究之前，不要在实际应用的服务器上尝试这些操作。然而，对于一个连接在因特网上并可运行的服务器来说，所使用的命令和操作与这里所讨论的在实验室中用到的自封闭系统完全相同。

这里选择Linux作为实验的原因是它实际上是免费的，从客户端接入服务器不需特殊的费用。但是，不久还会看到选择Linux的另外一些更重要的原因。在这些原因中，一个主要的原因是Linux的源代码是开放的。如果出现问题或者在操作系统中出现软件故障，世界各地的程序员都能够查看代码，并纠正错误。这样，用户就可以不依赖操作系统提供商的编程专家。此外，如果一个公司的操作系统较大，这个公司通常不会特别为你在系统中加入你想要的功能。有了开放的源代码，你就可以自己添加一些功能并实现一些改进。Linux源于Unix。而Unix已经使用了20年，是很成熟的操作系统，工作稳定可靠。Linux的这些优点比它的低费用更加重要，这些费用既包括初始的使用费，也包括运行费用。

虽然不同配置的Linux“心脏”或者说内核是相同的，但是由于所包含的软件包不同以及文件夹被存储的地点不同，使Linux的实际配置彼此间有一定的差别。对于大多数的用途来说，它们能提供相同的服务。Red Hat 和Caldera的Linux提供技术支持。Red Hat使用容易，因为它具有对用户非常友好的管理工具。这里选择了具有很好教学目的的Slackware 4.0。用手工操作代替点击用户图形界面上的菜单，可以更好地了解发生在后台的事件。但是，如果一个组织机构使用Linux服务器来实现商业运作，则最好选择能够提供完整技术支持的其他Linux版本。

从www.cheapbytes.com上在线定购Slackware，包括运费仅需要4美元。正版的4-CD装的一套软件可以到Walnut Creek去购买，电话是1-800-786-9907。关于Linux的资源可以在sunsite.unc.edu/LDP、www.linux.org和www.linux-howto.com上找到。你会发现与其他操作系统相比，人们更愿意针对Linux软件和其他一些免费软件向你提供帮助。

26.2 安装

26.2.1 准备

对于所使用的硬件，要选择那些可靠的和实用的硬件，最新和最好的硬件并不一定是最

佳的选择。这是因为新的硬件在你得到的软件中可能不被支持。当一个光盘制造出来的时候，一个新设备可能还没有上市，所以新软件就可能不支持新的硬件。记住，ISA组件不允许任何冲突存在，而PCI组件则允许冲突存在。同样，PCI卡比较容易设置并能在较高的速度下运行。这里将使用一个已安装了Windows的2.3GB的硬盘，这个硬盘空间将被分配给Slackware 4.0这个Linux版本。

安装步骤

1. 在硬盘上创建空间
2. 创建两张安装软盘
3. 在Linux下启动电脑
4. 对硬盘重新分区
5. 开始安装
   - 格式化交换分区
   - 格式化主分区
   - 安装磁盘
   - 创建启动软盘
   - 安装LILO
   - 配置网络
6. 重新启动和关机

一旦安装完毕，所有的服务都是可用的，所有的功能都会被安装进去。在旁边的图中列出了需要完成的工作。第一步是在这个被Windows占用的硬盘上为Linux创建一定的空间。下一步是从Windows中创建两个安装盘，我们将使用这两个软盘在Linux（或UNIX）下启动电脑。

然后就可以对硬盘进行重新分区。通过重新分区，可以规定为每个操作系统分配的硬盘空间大小。同样也可以规定分区的文件系统。Windows系统只需要一个分区，而Linux系统则至少需要两个分区。一个叫交换分区（swap partition）。这个分区将被用来扩展内存（RAM）的范围，它是硬盘空间的一部分，被叫做是虚拟内存。另一个分区被叫做Linux主分区（Linux native partition），这是存储Linux操作系统的地方。这里将使用一个大的分区以便使事情简单一些。交换分区将被指定为/dev/hda1，而主分区将被指定为/dev/hda2，其中“hd”代表硬盘，“a”代表第一块硬盘，数字1和2代表硬盘上的分区数。

一旦在硬盘上创建了分区，就可以开始安装程序了。在这个过程中，程序将格式化这些分区，并且提示希望在哪个盘上安装系统。这样基本的安装就结束了。在这之后，可以创建一个启动软盘，以便在服务器的文件系统损坏时使用这个启动软盘来启动服务器。之后需要安装Linux装载程序（LILO，LInux LOader），这样服务器就可以实现双启动，也就是既可以在Windows下启动，也可以在Linux下启动。做完这些之后，使用服务器信息以及它的网络环境信息来配置服务器。最后，重新启动系统，看看是否已经可以进行网络通信了。

图26-1给出了在本章中要创建并使用的小型以太网。这里仅有4台服务器，每个都有自己的IP地址和主机名。每台主机的管理员都是学生，他们的名字也分别标在图上。这4台主机的安装过程都是一样的，我们将查看一下jim是怎样安装配置他的服务器的。

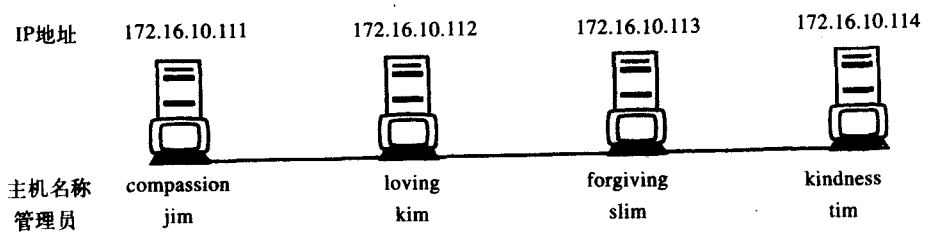


图26-1 具有多个Linux服务器的小型以太网，服务器所在的区域被命名为lab.small.edu

26.2.2 硬盘分区

在为Linux分区以前，必须给它腾出一点空间，因为硬盘上已经安装了Windows系统。可以使用名叫fips或“分区魔术师”（Partition Magic）的软件来完成分区的工作。“分区魔术师”

软件可以买到，而fips软件则可以在Slackware的光盘上找到。如果你仅仅是安装Linux或者是重新安装Windows，那就不必减小现在分区的容量；可以直接跳到创建磁盘，硬盘分区和安装那一步。如果你还要安装Windows，那就要创建磁盘，硬盘分区，先安装Windows，然后再安装Linux。在这里，Jim已经安装了Windows系统，因此使用fips来对硬盘重新分区。

使用fips：首先，把Windows下的所有重要文件都进行备份，防止因重新分区失败而丢失硬盘上的重要数据。fips程序没有任何保证，如同图26-2中第一步所示的那样。第二步显示了在Windows下如何知道硬盘上还有多少可用空间。然后在Windows下对硬盘碎片进行整理，这会使所有的剩余空间都转移到硬盘空间的尾部用来安装Linux。图中的第三步，创建了一张DOS系统盘，使我们能够在DOS下启动计算机。然后从光盘上将文件fips.exe、restorrb.exe和errors.txt复制到软盘上。在这里，将e盘作为CD-ROM而将a盘作为软驱。现在可以读一下readme文件，确定没有遗漏的地方。

```
1. Save the registry and backup the Windows system.
2. MyComputer -> Right Click on C: drive ->
   Properties ->
   a. General Tab -> find amount of free disk space.
   b. Tools -> "Defragment now . . ."
   c. General Tab -> find amount of free disk space.
3. Go to MS-DOS prompt and insert CD (my e: drive)
   c:\> format a: /s          (Create a DOS boot disk.)
   c:\> copy e:\install\fips-20\fips.exe a:
      (Also copy restorrb.exe, errors.txt to a: drive.)
4. With floppy in a: drive, restart PC and run fips.
   a:\> fips.exe
```

Partition Table

Part	Bootable	Start Head	Start Cyl	Start Sector	System	End Head	End Cyl	End Sector	Start Sector	Number of Sectors	MB
1	yes	1	0	1	0Bh	254	299	63	63	4779437	2351

```
Which partition do you want to split (1/2/3)? 1
Do you want to make a backup copy of your root and boot sector? y
Enter start cylinder for new partition (157-299):
Use cursor keys to choose cylinder,  <enter> to continue

Old Partition   Cylinder    New Partition
1222            157         1129  <---- 硬盘分区空间分配的第一种建议方案。

1313            167         1038  <---- 按向下键，给出分配方案。
```

New Partition Table

Part	Bootable	Start Head	Start Cyl	Start Sector	System	End Head	End Cyl	End Sec.	Start Sector	Number of Sectors	MB
1	yes	1	0	1	0Bh	254	166	63	63	2669247	1313
2	no	0	167	1	0Bh	254	299	63	2669310	2110190	1038

```
Ready to write the new partition scheme to disk. Proceed (y/n)? y
Windows is restarting
```

图26-2　运行fips对硬盘进行重新分区

将光盘取出并将软盘放入软驱，之后重新启动电脑和fips.exe程序。在本章中，只需要第一张光盘。

如图26-2所示，一个分区的信息显示在屏幕上。它从0磁道一直到299磁道，“0Bh”表明这是一个用在Windows 95系统上的FAT-32类型的分区。软件将提示我们要对哪个分区进行操作，由于这里只有一个分区，所以只需输入“1”。然后fips对引导扇区进行备份以便在遇到问题时，可以恢复硬盘的引导信息。这些引导信息存储在软盘上，文件名为rootboot.000，这是一个安全特性。

由于Windows占用了硬盘上的前156个扇区，因此软件会提示是否从第157个扇区开始新

的分区。根据图中提示，分配1.222MB硬盘空间给Windows系统，1.129MB给Linux系统。按向下的箭头，会出现下一组分配硬盘空间的方案，图中新的分区方案是从167扇区开始，可以用上、下箭头键来选择大小。在图中通过按Enter键，选择Linux分区从167扇区开始。现在会显示新的分区表，一旦按下y键表示同意，分区表就会保存在硬盘上。

创建启动映像：现在通过Windows进入DOS环境，创建三张软盘，分别标记为“boot”（启动）、“root”（引导）和“rescue”（恢复）。前两张盘用于安装过程。当你启动服务器出现问题时使用boot和rescue这两张盘。图26-3说明了这三张盘是如何创建的。每一个rawrite命令都会让你更换一张软盘。rawrite命令能在DOS系统下创建UNIX格式的软盘。所有的软盘首先都被格式化，然后检查是否存在坏扇区，因为rawrite命令并不能核实所写的内容。

```
C:\> format a:                          E:\> cd rootdsks
C:\> chkdsk a:                          E:\ROOTDSKS> rawrite color.gz a:
(Insert the Slackware CD in drive.)     Track 74 . . .
C:\> E:                                 done
E:\> cd \bootdsks.144
E:\BOOTDSKS.144>rawrite net.i a:        E:\ROOTDSKS> rawrite rescue.gz a:
Track 35 . . .                          Track 76 . . .
done                                    done
```

图26-3 从Windows中创建启动、引导、恢复盘

启动映像包括启动Linux系统所必需的内核。因为需要使用网络功能，所以net.i允许在安装系统后连接到网络上。否则，内核将不得不重新编译。这里还有scsi.i的启动映像，这被用于SCSI卡；而bare.i的启动映像包含了基本的IDE支持。读一下bookdsks.144文件夹中的readme文件，可以得到更多的相关信息。

color.gz文件是一个随机存取存储器的映像，它允许电脑中的RAM像硬盘一样启动系统。这个文件包含了引导文件系统。对于膝上电脑来说，可以使用pcmcia.gz文件。将rescue盘保存好，以便将来启动机器出现问题时使用。

硬盘分区：一旦你准备好了这些软盘，在Windows下关闭电脑。将启动软盘放入软驱中再打开电脑。如果你使用可移动硬盘，首先确认电脑中使用的硬盘是正确的。在描述过程时，请参见图26-4。不久你就会看到一个“boot:”的提示符，按下Enter键。过了一会儿，将提示插入引导软盘。按照提示去做，会得到一个slackware的登录提示。如果是作为根用户(root)或超级用户(superuser)来登录，则不需要密码。现在电脑已经运行在Linux系统下，并且已经准备好了对硬盘重新分区。如图26-4所示，输入fdisk命令，这个命令能够对硬盘重新进行分区。

首先试着用“m”命令列出fdisk可以接受的命令列表，图中只列出了一小部分命令。在本章中，不会将文本所有的行都显示在屏幕上，这有两个原因：一个原因是希望简化输出，使读者了解系统是如何工作的；二是为了节省版面。因此，屏幕上的所有显示不会全部列出，但是为了帮助你了解整个过程而列出这些内容已经足够了。

就像“m”命令标注的一样，“d”命令是删除一个分区的命令；“n”命令是创建一个新的分区的命令；“t”命令是更改一个分区的类型命令等等。如果你不想改变分区表就结束fdisk程序，可以键入“q”命令不存盘退出。相反，“w”命令是将修改的分区表保存到硬盘上。

这里做的第一件事就是输入“p”命令来查看当前的分区表。这会显示出已经存在一个Windows分区。接下来，输入“n”命令来创建一个新的分区，这是第二个分区，占据从167扇区到186扇区的空间，并把它作为交换分区。通常交换分区大约有64KB到100KB就足够了。

```
(放入安装启动盘，打开计算机)
boot: (按回车 (Enter) 键)
VFS: Insert root disk    (放入引导盘、按回车键)
slackware login: root
# fdisk /dev/hda                    (输入fdisk命令)
Command (m for help): m
d      delete a partition            q    quit without saving changes
n      add a new partition           t    change a partition's system id
p      print the partition table     w    write table to disk and exit

Command (m for help): p              (注意到已经存在一个Win95的分区)
Device Boot    Start    End     Id   System
/dev/hda1      1        166      b   Win95 FAT32

Command (m for help): n              (创建交换分区)
Command action:    e   extended,    p   primary partition (1-4)p
Partition number (1-4): 2
First cylinder (167-524, default 1): 167
Last cylinder or +size or +sizeM or +sizeK (1-524, default 524): 186

Command (m for help): n              (创建主分区)
Command action:    e   extended,    p   primary partition (1-4)p
Partition number (1-4): 3
First cylinder (187-524, default 101): 187
Last cylinder or +size or +sizeM or +sizeK (187-524, default 524): 299
Command (m for help): p
Device Boot    Start    End      Id   System
/dev/hda1      1        166      b    Win95 FAT32
/dev/hda2      167      186      83   Linux native
/dev/hda3      187      299      83   Linux native

Command (m for help): t              (为交换分区设置正确的类型)
Partition number (1-4): 2
Hex code (type L to list codes): L
0  Empty           c  Win95 FAT32 (LB 63  GNU HURD        a6  OpenBSD
1  DOS 12-bit FAT  e  Win95 FAT16 (LB 64  Novell Netware  a7  NEXTSTEP
2  XENIX root      f  Win95 Extended  65  Novell Netware  b7  BSDI fs
6  DOS 16-bit >=32 17 Hidden OS/2 HPF 82  Linux swap      e1  DOS access
7  OS/2 HPFS       1b Hidden Win95 FA 83  Linux native    e3  DOS R/O
8  AIX             40 Venix 80286     85  Linux extended  eb  BeOS fs
b  Win95 FAT32     52 Microport       a5  BSD/386
Hex code (type L to list codes): 82
Changed system type of partition 2 to 82 (Linux swap)
Command (m for help): p
Device Boot    Start    End      Id   System
/dev/hda1      1        166      b    Win95 FAT32
/dev/hda2      167      186      82   Linux swap
/dev/hda3      187      299      83   Linux native

Command (m for help): w              (把新的分区表写入硬盘)
#
```

图26-4　使用fdisk对硬盘重新进行分区

采用同样的步骤，创建一个Linux主分区，从187扇区到299扇区。当再次显示分区表时，注意由于默认分区类型是Linux主分区，因此两个新建的分区都被创建为Linux主分区。

因此，要改变分区2的类型。使用“t”命令，输入“L”列出Linux所能创建的所有分区类型。实际上，分区的类型比这里显示的要多。将类型改为Linux交换分区，再显示分区表，并将新的分区表保存到硬盘中。现在已经为安装系统做好准备了。

安装操作系统：在#提示符的右边输入“setup”。# 提示符表明你是一个超级用户，在这种情况下要对你的操作十分小心，因为这是一个有特权的账户。将光盘放入驱动器中，接下来按照图26-5所示的步骤来安装操作系统。在图中，每一个新的显示都在开头行中用一个等于号（=）来表示。在每一行的尾部也有一个等于号表示显示的结束。每一屏的底部都有一个诸如yes、no的提示符，正确的选项都被标在第二个等号后面。下面就开始吧!

```
#setup
== SLACKWARE LINUX SETUP
      HELP                KEYMAP
      ADDSWAP <-          TARGET
      SOURCE              SELECT
      INSTALL             CONFIGURE
      EXIT                      == <OK>

= Swap space detected= <YES>
= Formatting Swap Partition...
= SWAP SPACE CONFIGURED = <EXIT>
= CONTINUE WITH INSTALLATION?     = <Yes>
= Select Linux installation partition
    /dev/hda2     Linux Native    = <Ok>
= Format Partition
    Format        Quick format    = <Ok>
= SELECT INODE DENSITY FOR /dev/hda2
    4096 1 inode per 4096 bytes   = <Ok>
= Formatting /dev/hda2 ...
= Done Adding Linux Partition     = <Exit>

= FAT/FAT32/HPFS PARTITIONS DETECTION
  would you like to make these
  partitions visible for linux?   = <No>
= Continue? = <Yes>
= Source Media Selection
    1 Install from Slackware CD   = <OK>
= autoscan                        = <Ok>
= Place disk in CD ROM drive      = <Ok>
= Scanning . . .
= CHOOSE INSTALLATION TYPE
    Slackware Normal              = <Ok>
= Continue?                       = <Yes>
= PACKAGE SERIES SELECTION
  [X] Base
  [X] Apps          . . . etc.
  (Use the default selections.)   = <Ok>
= Continue?                       = <Yes>
= Select Prompting Mode
    FULL                          = <Ok>
=
    Bootdisk                      = <OK>
  (Insert the install boot disk.)
= Insert Install boot disk = <OK>
= Copying . . .
= Make Boot Disk
    Continue                  = <Ok>
= Continue                    = <Ok>
= Modem Configuration
    no modem                  = <No>
= Screen Font Configuration = <No>
= LILO Installation
    simple                    = <Ok>
= SELECT LILO DESTINATION
    MBR                       = <OK>
= CONFIGURE NETWORKING?       = <Yes>
= Configuration Network       = <ok>
= Enter Hostname (Use lower case.)
    [compassion]
= Enter Domain Name
    [good.stuff.edu]
= IP ADDR (Don't use number pad.)
    [172.16.10.111]
= Eneter Netmask
    [255.255.255.0]           = <Ok>
= GATEWAY
    [172.16.10.1]
= Use a Name Server           = <yes>
= IP address for Name server
    [172.16.10.111]           = <Ok>
= NETWORK SETUP COMPLETE      = <ok>
= MOUSE CONFIGURATION
    ps2                       = <Ok>
= GPM configuration           = <yes>
= Sendmail
    SMTP+BIND                 = <ok>
= TIMEZONE CONFIGURATION
    US/Eastern                = <Ok>
= Warning: Would you like to
    set root password?        = <No>
= Setup Complete              = <ok>
= Slackware Linux Setup
    EXIT                      = <ok>
# reboot
# shutdown -h now
```

图26-5 安装Linux时使用的菜单和屏幕显示。在每行开头处的“=”表示新的一屏信息，每行后面的“=”和提示信息表示所选择屏幕的响应。提示信息都用符号“<>”括起来了

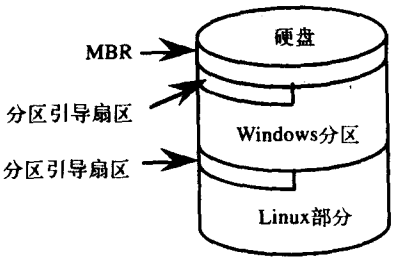
输入“setup”之后，你会看到第一屏。选择“ADDSWAP”，这将格式化并配置交换分区。然后安装过程会提示你格式化主分区。在这几步中，你会看到一系列的信息。除非有错误，否则可以忽略它们。如果有错误，你可以选择那个能检测坏扇区的格式化类型，而不是图26-5中所示的那个格式化类型。在这种情况下，你可能要对硬盘重新进行分区，使用那些没有坏扇区的磁盘空间，或者干脆换一个新硬盘。

由于使用的硬盘已经有了一个Windows分区，因此会得到“FAT PARTITION IS

DETECTED”的信息。当提示是否要让这个分区在Linux下可视时，选择“NO”。这样，在Linux系统中就不能使用Windows的文件了。

由于已经放入了光盘，因此让setup程序自动监测它并选择安装标准的Slackware。之后安装程序会询问是否需要安装程序包或diskset。使用上下键和空格键，你可以改变默认的选择。如果你有足够的硬盘空间，可以选择安装所有的默认选择。选择FULL这个安装方式，以后你可以看到这时所有的软件都会被安装。

现在是从启动软盘上得到Linux内核并把它复制在硬盘上的时候了。把引导磁盘取出并用启动磁盘代替。现在Linux的内核文件已经复制到硬盘上去了，所以可以使用硬盘来启动了。在图26-5中，对于Make Boot Disk这个菜单，选择了“Continue”来跳过这一步。然而，你可能想要创建一个启动盘。如果是这样的话，在显示这个菜单时，用另一张盘（这已经是第4张盘了）并把它标记为“Running Boot”。然后在显示这个菜单时，选择“Format，1.44kB，Simple”然后选择“Continue”。再往后就是调制解调器配置（Modem Configuration）这一步了，这里选择了“NO”。



在硬盘上，分区表和启动引导程序保存在MBR（Master Boot Record）上。同样，每个分区都有它自己的引导扇区，这个扇区可以帮助分区中安装的操作系统来启动电脑，如侧面的图所示。在安装Windows以后，一个标准的DOS MBR文件就被装载到MBR中。当BIOS启动电脑时，DOS MBR和Windows分区中引导扇区的程序就会被使用，这时Windows分区就被标记成激活（active）的。由于想实现两个系统的双启动，因此要把MBR中的DOS MBR替换为LILO（LInux LOader）程序。LILO使我们可以选择用哪个分区来启动电脑。因此在图26-5中，选择安装一个简单的LILO，以后我们还可以修改它。

现在，安装过程到了设置网络的部分了。这里，需要主机名、IP地址、子网掩码和路由器或网关IP地址等信息，这些都可以从图26-1中获得。也可以使自己的主机成为一台DNS服务器。另外，可以通过随时输入netconfig命令来改变这些信息并重新启动电脑使新的信息生效。如图26-5所示，使用netconfig命令，从“CONFIGURE NETWORKING?”一直到“NETWORK SETUP COMPLETE”。

最后，提供鼠标类型和时区。另外，不要设置root密码。再回到setup的第一个菜单之后，就可以退出了。现在在根提示符下输入reboot命令，也可以用CTL-ALT-DEL来重新启动PC。但这只对Linux系统有效并能够用来关掉服务器，而关闭UNIX服务器的方法是用shutdown -h now命令。

修改LILO：当重新启动时，进入LILO菜单，它会询问是在DOS（或Windows）下启动，还是Linux下启动电

```
:~# cat /etc/lilo.conf
# LILO configuration file
# generated by liloconfig
# Start LILO global section
boot = /dev/hda
message = /boot/boot_message.txt
prompt
timeout = 60
vga = normal

#Linux partition config begins
image = /vmlinuz
root = /dev/hda2
label = Linux
read-only

# DOS  partition config begins
other = /dev/hda3
label = DOS
table = /dev/hda

:~#lilo
Added Linux *
Added DOS
:~#
```

脑。如果按下Enter键，默认选项是DOS，但我们可能希望将默认选项改为Linux。此外，默认的延迟时间是120s，而我们可能想把它减为6s。这样在提示菜单出现时，先不要按下Enter键。让电脑等待6s，LILO就会自动启动电脑到Linux。

要做这两个更改，需要把你的目录改为/etc，然后编辑一下lilo.conf这个文件。对某些任务，需要使用vi编辑器。在这里，pico编辑器就足够了。使用这两个编辑软件中的一个来编辑这个文件，就像旁边的图中显示的那样。注释用#表示，文件共有三个部分，一个是全局部分，另外两个对应着每个不同的引导分区。

在全局部分中，将时间超时（timeout）从1200改为60。这样在电脑启动时，如果6s内没有按下Enter键，就会进入默认分区。然后把属于Linux分区配置的5行（包括注释行）从文件尾部移到文件的开头，来代替放在前面的DOS分区配置。把Linux配置放在最前面会使电脑把Linux作为默认的启动选项。

在pico编辑器中，连续5次按下CTR-K，然后把鼠标指针移到正确的位置，再按CTR-U就能把被删掉的5行移到指定的位置。最好在编辑一个重要文件之前先做一个备份。如果编辑时出现了错误，可以使它回到原来的样子。在编辑lilo.conf文件之后，你必须运行lilo，以使LILO将其安装到引导扇区中去，就像旁边图中的最下边所做的那样。可以使用liloconfig命令去配置LILO并安装它，就像在setup中做的那样。

26.3 了解所使用的服务器

参照图26-6来了解一下服务器的配置（如果你需要学习或者复习基本的UNIX命令，则可以

```
compassion:~#  ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:04:D3:DE:13
          inet addr:172.16.10.111  Bcast:172.16.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:301 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:10  Interrupt:10 Base address:0x1000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1

compassion:~#  cd /etc
compassion:/etc#  ping 172.16.10.112
64 bytes from 172.16.10.112: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 172.16.10.112: icmp_seq=1 ttl=255 time=0.2 ms
compassion:/etc#  ping loving
ping: unknown host loving
compassion:/etc#  more hosts
127.0.0.1            localhost
172.16.10.111        compassion.good.stuff.edu compassion

compassion:/etc#  pico /etc/hosts
compassion:/etc#  cat hosts
172.16.10.111        compassion.good.stuff.edu compassion
172.16.10.112        loving.good.stuff.edu     loving
172.16.10.113        forgiving.good.stuff.edu  forgiving
172.16.10.114        kindness.good.stuff.edu   kindness
compassion:/etc#  ping loving
64 bytes from 172.16.10.112: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.10.112: icmp_seq=1 ttl=255 time=0.2 ms
```

图26-6 了解服务器的网络环境

参考《UNIX By Experimentation》一书，(Prentice Hall出版)。为了确保工作的完整性，这里不得不写出这些程序)。在启动电脑之后要做的第一件事就是用ifconfig命令来检查网络的接口。本地环路项表明它的IP地址为127.0.0.1，并且已启动并正常运行。如果所使用的服务器不能与这个接口进行通信，那么也就不能与网络进行通信。这个接口可以保证所使用的主机本身不存在问题。

eth0接口是我们的以太网接口。如果看不到这个接口，就必须重新编译Linux内核。然而，因为这里使用的是3Com公司生产的以太网卡，所以net.i引导图标使我们可以立即看到这个接口。硬件地址显示了十六进制的NIC地址和网络配置阶段输入的信息。

接下来，将进入到/etc目录，需要从当前目录转换到这个目录下。现在要看一看kim是否已为她的服务器完成了Linux的安装，所以ping一下她的机器。结论是她已经完成安装。但是这时如果我们利用她的主机名“loving”，就会发现我们的主机（更准确的说是jim的主机）无法识别loving的IP地址。当输入“more hosts”命令时，可以发现我们的主机仅仅知道自己的IP地址。而主机loving的IP地址还是不能被输入。因此，再次使用pico编辑器来将其他三台服务器的IP地址都添加进去。命令“cat /etc/hosts”显示文件已被更新了。现在，当再次ping 主机loving时，服务器将会从 /etc/hosts文件里找到相应的IP地址来完成ping命令，这样就可以确定我们的主机已经连接到网络上了。

在开始进行与网络有关的其他操作之前，首先参考图26-7来看一看服务器的某些基本配置。在图26-7中，可看到文件 /etc /HOSTNAME含有主机的全名。全名中第一个圆点前的就是主机名，在它之后的部分则是所属域的名称。hostname命令同样可以显示主机名，也可以用这个命令来更改主机名。例如，可以将主机名改为winter。接下来应用pico编辑，又可以将主机名重新改为compassion。根据你个人的喜好，可以将主机名更改为其他的名称。在注销或者重启之后，在命令提示中就可以看到新的主机名了。

```
compassion:/etc#  more HOSTNAME
compassion.good.stuff.edu
compassion:/etc#  hostname
compassion
compassion:/etc#  hostname winter
compassion:/etc#  pico HOSTNAME
compassion:/etc#  more rc.d/rc.inet1
IPADDR="172.16.10.111"
NETMASK="255.255.255.0"
NETWORK="172.16.10.0"
BROADCAST="172.16.10.255"
GATEWAY="172.16.10.1"

:~# cd /etc /rc.d
:/etc/rc.d#  ls rc.inet1.orig
:/etc/rc.d#  cp rc.inet1 rc.inet1.orig
:/etc/rc.d#  ls -l rc.inet1*
-rwxr-xr-x    Nov 24  rc.inet1
-rwxr-xr-x    Nov 24  rc.inet1.orig
:/etc/rc.d#  chmod 400 rc.inet1.orig
:/etc/rc.d#  ls -l rc.inet1*
-rwxr-xr-x   Nov 24  rc.inet1
-r--------   Nov 24  rc.inet1.orig
:/etc/rc.d#  pico rc.inet1
```

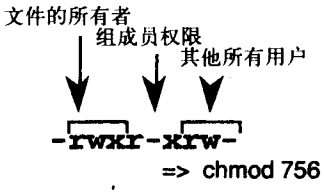
```
compassion:~#  dmesg | grep eth0
eth0: 3Com 3c905B 00baseTx 0x1000,
00:50:04:d3:de:13, IRQ 10
compassion:~#  uname -a
Linux compassion 2.2.6 #2 Tue May 4
21:50:43 CDT 1999 i686 unknown
compassion:~#  cd /proc
compassion:/proc#  cat interrupts
 10:        360          XT-PIC  eth0
compassion:/proc#  cat ioports
0000-001f : dma1
compassion:/proc#  cat pci
  Bus  0, device  15, function  0:
    Ethernet : 3Com 3C905B 100bTX.
compassion:/proc#  ps
  PID TTY          TIME CMD
  188 ttyp0    00:00:00 bash
  202 ttyp0    00:00:00 ps
compassion:/proc#  ps -aux
USER    PID  START   TIME COMMAND
root      1  13:38   init [3]
root    203  13:48   ps -aux
compassion:/proc#  cat /etc/fstab
/dev/hda1   swap  swap defaults   0   0
/dev/hda2   /     ext2 defaults   1   1
none        /proc proc defaults   0   0
```

图26-7　更改网络配置并查看其他服务器的设置

如果你更改了ISP，则必须同时更改IP地址。文件/etc/rc.d/rc/inet1含有网络配置的信息。这是一个关键性的启动文件，所以在更新这个文件之前应该先用扩展名orig对其进行备份。它表示这是更新以前的文件。首先，我们输入“ls rc.inet1.orig”来确定在安装过程中没有生成这个文件。如果别的管理员也更改了这个文件并以扩展名orig作了同样的备份，我们的更改将会覆盖已存在的同名文件。因此可先用命令 ls来确认 .orig文件原来并不存在。

对文件应用ls -l命令可以显示它们是可被覆盖的。所以，为了保护.orig备份文件，使用chmod 400命令，再次使用ls -l命令可以看到它的属性已经更改，从而可以避免意外的覆盖。现在，用pico或者其他的编译器，对文件的网络配置进行更改。更改主机名或其他一些网络地址最安全的方法是使用 netconfig命令，我们在安装过程中曾经介绍过这个命令。

在旁边的图中显示出Unix中文件的权限。ls -l命令列出的第一个符号“-”表示这是一个文件，而不是文件夹或链接。接下来分三组显示了该文件的所有者、组成员、所有用户对该文件所拥有的权限。要改变显示的权限就要对该文件使用chmod 756命令。其中的r、w、x分别代表可读(read)、可写(write)、可执行(executable)。



r	w	x	chmod
-	-	-	0
-	-	x	1
-	w	-	2
-	w	x	3
r	-	-	4
r	-	x	5
r	w	-	6
r	w	x	7

在图26-7第二列的首行可以看到dmesg命令。这个命令将会显示机器启动时屏幕上显示的所有信息。如果想要知道我们使用的是什么网卡，可以输入dmesg | grep eth0命令来查看eth0的信息。它会显示所用的网卡型号是3c905B。接下来，用uname -a命令显示所使用的Linux系统的内核版本为2.2.6。

在/proc目录下，还有几个有意义的文件。为了简洁，在图中每个文件的内容只显示了一行。interrupts文件包含着关于中断的配置。接下来，I/O端口和能识别的PCI卡被显示出来。命令ps显示了登录时运行了哪些进程，命令ps -aux将显示所有的进程。

当服务器启动以后，会读取文件/etc/fstab，它被称为文件系统表。这个文件决定了在启动的过程中哪些文件将被加载。在这里，我们可以看到交换分区和Linux主分区分别被标识为/dev/hda1和／dev/hda2。还有一个文件系统被标识为“none”。它不是一个真正的文件系统而是一个名为／proc的目录。这个目录是所有Linux系统所必需的，而且不能被修改。

显示的第二列表示安装点。swap和“/”是两个文件系统或分区的安装点，swap和ext2是文件系统的类型。接下来的一列显示了默认选项的设置。最后两列设置表示文件系统被检查的时间。

26.4 用户账户

26.4.1 保护根用户的密码

jim应该做的第一件事便是为根用户（root）设置密码。这可以在超级用户提示符#下，简单地输入命令“passwd”，然后再输入一个好的密码来完成。在许多情况下，常常会有人忘记了自己机器的根用户密码。当这种事情发生时，可以按照图26-8的步骤找回密码。

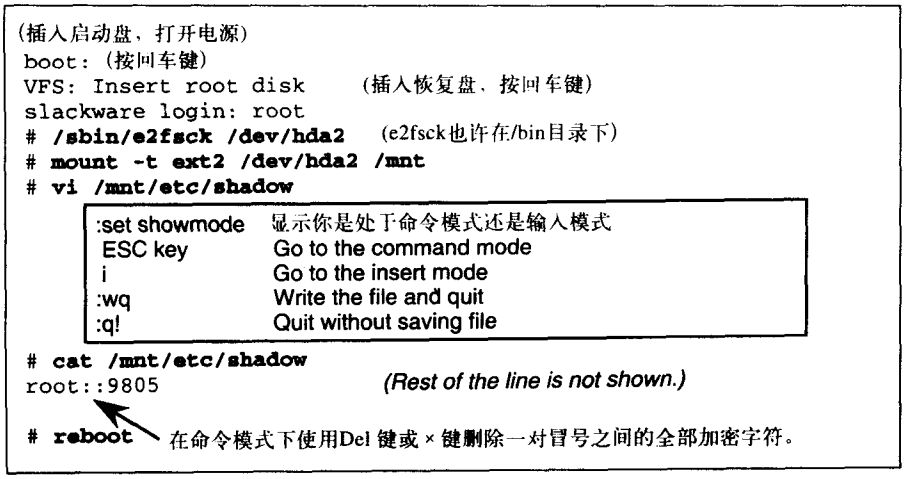


图26-8　用恢复盘删除根用户的密码

这时需要使用一些命令和最终找到的文件。如果你忘记了根用户密码，又想进入服务器，现在就来尝试一下。

将安装时制作的启动盘插入软驱，然后打开电源。在出现“boot:”提示时输入回车。这时会提示你放入引导盘，将按照如图26-3所示的过程制作的恢复盘插入软驱。然后根据对应的硬盘分区输入e2fsck命令，它将会检查并清除文件系统。当出现提示时，只需输入回车。因为其他的选项没有任何意义。接下来输入“mount”命令来安装硬盘驱动程序，这样基本上就可以通过 /mnt目录来实现对硬盘的访问。

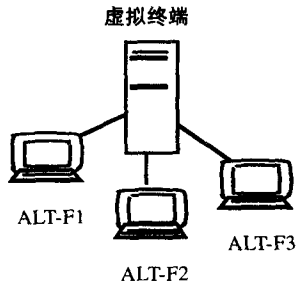
现在就可以用 vi 来编辑硬盘上的密码文件了。在此有必要先了解一下 vi 编辑器：它有两种基本的工作模式，你需要了解自己正处于哪种模式。按ESC键可以进入命令模式。在命令模式下，可以输入命令。按i键可以进入文本模式。这样你就可以编辑输入字符了。我喜欢时时刻刻都知道自己是处在哪个模式里。因此，我总是打开 vi 编辑器，并按下ESC键并输入冒号（:），接着输入“set showmode”。这样就会在编辑的时候显示所处的模式。如果在编辑的过程中发生了错误而你又想重新开始，就按下ESC键，输入“: q! ”。如果完成编辑后你想要保存并退出，就按下ESC键，并输入“: wq”。

现在回到原来的问题上，为了取回密码，我们需要做的就是将shadow文件中描述根账户语句中第一对冒号之间的字符全部删除。如果操作正确的话，根记录的起始项应该与图中所示的相同。现在可将恢复盘取出，然后重启机器。这样你就又可以以根用户登录了，这时无须输入任何密码。进入系统后，就可以为根用户重新设置密码了。

26.4.2　创建一个用户账号

现在是为我们自己创建一个用户账号的时候了。以jim为例，虽然他是这台机器的管理员，但是除了根账号之外，他还需要另外一个用户账号。他账号的用户名将被设为jim。当他需要以管理员的身份进行管理时，能以根用户的身份登录；而当他需要远程登录别的机器，查收他的电子邮件或者仅仅只是查看他的服务器时，他只需以jim的身份登录。处理所有日常事件时都以根用户的身份登录是不明智的。以根用户身份登录以后，如果不慎删除了某些重要文件该怎么办？所以，只是在必要的时候才需以根用户的身份登录，而在其他的时间里，用jim

的身份登录就可以了。



与其先以一个用户账号登录，然后注销，再以另一个用户账号登录，不如同时打开两个窗口。虽然到现在为止我们还没有配置X Windows（它是为Unix系统设计的一个图形用户界面(GUI)），但是Linux提供了另外一种选择。通过ALT键和功能键(F1、F2等等)，可以模拟出最多六个虚拟的终端，如侧面的图中所示，这样就不需要额外的实际物理终端了。

第一次登录时，我们就在第一个虚拟终端上。想要打开另一个登录窗口，只需同时按ALT键和F2键。在图26-9中，左边一列是jim以根用户身份登录的显示，右边是他以jim账号登录的显示。通过按ALT+F1、ALT+F2，他可以在这两个虚拟终端之间进行切换。在ALT-F2的显示中，jim正在检测他为自己创建的用户账号。可以看到，在ALT-F1的显示中出现的提示符号是#，这表明他是以根用户的身份登录的；而在ALT-F2的显示中提示符号则是$，这表明这个用户账号只是服务器的一个普通用户。

root on compassion: ALT-F1

```
compassion:~# adduser
Login name for new user []:    jim
User id [ defaults to next available]:
Initial group for jim [users]:
Additional groups for jim []:
jim's home directory [/home/jim]:
jim's shell [/bin/bash]:
Account expiry date (YYYY-MM-DD) []:
Changing the user information for jim
Enter the new value, or press return
       Full Name []:  Prof. Jim Thomas
       Room Number []:
       Work Phone []:
       Home Phone []:
       Other []:
Changing password for jim
New password:  jim
Bad password: too short.    jim
Warning: weak password.
New password:  jim
Re-enter new password:    jim
Done...
compassion:~#  cat /etc/passwd
root:x:0:0::/root:/bin/bash
operator:x:11:0::/root:/bin/bash
guest:x:405:100::/dev/null:/dev/null
nobody:x:65534:100::/dev/null:
jim:x:1000:100:Prof. Jim Thomas,,,:
                    /home/jim:/bin/bash
compassion:~#  grep jim /etc/shadow
jim:kDPngBVvSnjrs:10919:0:99999:7:::
compassion:~#  ls -l /etc
-rw-------   1 root    367 /etc/shadow
-rw-r--r--   1 root    611 /etc/passwd
compassion:~#
```

jim on compassion: ALT-F2

```
compassion login:  jim
password:  jim     (Password is not echoed.)
compassion:~$  who
root      tty1      Nov 24 14:04
jim       tty2      Nov 24 14:04
compassion:~$  grep jim /etc/passwd
jim:x:1000:100:Prof. Jim Thomas,,,:
                    /home/jim:/bin/bash
compassion:~$  grep jim /etc/shadow
/etc/shadow: Permission denied
compassion:~$  pwd
/home/jim
compassion:~$  telnet loving
loving login:  jim
Password:
loving:~$  more /etc/passwd
kim:x:1000:100::/home/kim:/bin/bash
jim:x:1001:100::/home/jim:/bin/bash
slim:x:1002:100:/home/slim:/bin/bash
loving:~$  more /etc/shadow
/etc/shadow: Permission denied
loving:~$  telnet compassion
compassion login:  jim
Password:
compassion:~$  who
root      tty1      Nov 24 14:04
jim       tty2      Nov 24 14:04
jim       ttyp1   (loving.good.stuf)
compassion:~$  logout
Connection closed by foreign host.
loving:~$  logout
Connection closed by foreign host.
compassion:~$  logout
compassion login:
```

图26-9 创建并测试一个用户账号

像这样同时打开两个登录界面是十分方便的。现在，如果需要jim与别的服务器进行通信，有人向他申请一个用户账号或者申请类似的服务，他需要做的只是切换到ALT-F1上进行操作。

当他在ALT-F1上完成了为那名用户的服务之后，只需用ALT-F2再切换回来就可继续刚才的工作了。

jim输入命令“adduser”来创建一个新的用户账号。首先输入的是他的用户名“jim”，我们这里都是用小写字母。接下来的几个提示项中只需按回车选择默认的内容就可以。默认的选项都在中括号“[]”中给出。为了简便，jim给他的用户账号设置的密码和用户名是相同的，也就是“jim”。因为我们并没有连接到因特网而只是在一个教学的环境中，所以这样的密码就可以了；否则，使用一个如此简单的密码肯定是极不明智的。

jim给自己创建完用户账号之后，让我们再来看看/etc/passwd这个文件。在这里，存储了所有用户账号的资料，jim的账号同样也在这里。每个用户的资料都会占用文件的一行，每一行中不同的字段用冒号分割。最前面的字段是用户名jim，接下来的字段就是相应的密码（处于保护模式并不可见）。基于安全性的考虑，Slackware使用另一个文件/etc/shadow来储存用户的密码。

以任何身份登录的用户都可以查看文件/etc/passwd，但是却不能查看文件/etc/shadow。这样做是为了防止有人将这个密码文件下载以后，破解并窃取用户的密码。

在密码之后的字段是uid（用户id），其中jim的uid是1000。接下来的字段是gid（组的id），jim的gid是100。当我们如后面的图26-13那样来研究/ect/group文件时，会看到这个组的名称是users，这是一个默认的组。

接下来的一行命令显示jim可以用grep命令查看他的密码以及密码文件/etc/shadow。他之所以能这样做，是因为他是以根用户的身份登录的。加密以后的密码与真实的密码“jim”截然不同。使用ls命令可以看到passwd文件对任何用户都是可读的，但是shadow文件只对根用户是可读的。

现在，让我们看一下图26-9的右面一列，jim通过ALT-F2切换到另一个虚拟终端。在此可以看到熟悉的登录提示。jim登录以后，输入了“who”命令，就可以看到根用户是从tty1（ALT-F1）登录的，而用户jim是从tty2（ALT-F2）登录的。文件/etc/passwd是所有登录用户都可以读到的。由于jim不再是超级用户，而是以jim身份登录的，所以他不再有权力查看/etc/shadow文件。如果他尝试查看shadow文件，会返回错误信息“Permission denied”（无权访问）。

现在让我们看看kim是否已经在她的机器loving上给jim创建了用户账号。jim通过Telnet远程登录到kim的机器。登录后，jim想知道kim还给谁分配了用户账号。于是，他查看了kim机器上的/etc/passwd文件。jim发现kim除了给她自己分配了一个账号以外还给slim创建了一个账号。他又尝试想要查看kim机器上的/etc/shadow文件，同样还是没有查看的权限。

从kim的机器上，jim可以重新远程登录回到自己的机器上。当他这样做后，用who命令查看到自己用jim这个账号登录了两次。第一次是从tty2登录的，而第二次是从机器loving登录的。现在jim从主机loving注销回到自己的主机compassion。当从主机compassion注销以后，又可以看到登录的提示。

26.4.3　小结

现在我们将回顾一下在本章中遇到的一些概念。jim和kim都往他们的服务器里添加了bug，我们要做的就是从jim的视角来找出并解决这些问题，如图26-10所示。

```
                                jim on compassion ALT-F2
compassion:~$ telnet loving
loving: Host name lookup failure          (Problem, can't telnet to loving.)
compassion:~$ ping loving                 (Can't ping loving either.)
ping: unknown host loving                 (Can't recognize host name, loving.)
compassion:~$ ping 172.16.10.112          (Can't ping using IP address either.)
PING 172.16.10.112 (172.16.10.112): 56 data bytes
7 packets transmitted, 0 packets received, 100% packet loss
                                          (Boot up loving. It was turned off.)
compassion:~$ ping 172.16.10.112          (Start the ping while it is booting up.)
PING 172.16.10.112 (172.16.10.112): 56 data bytes
64 bytes from 172.16.10.112: icmp_seq=31 ttl=255 time=0.6 ms
64 bytes from 172.16.10.112: icmp_seq=30 ttl=255 time=1000.7 ms
31 packets transmitted, 2 packets received, 87% packet loss
compassion:~$ telnet loving               (Can't recognize host name again.)
loving: Host name lookup failure
compassion:~$ grep loving /etc/hosts      (Entry for loving is commented out.)
# 172.16.10.112            loving.good.stuff.edu      loving

                                root on compassion ALT-F1
compassion:~#pico /etc/hosts              (jim as root removes the comment.)

                                jim on compassion ALT-F2
compassion:~$ grep loving /etc/hosts      (jim checks the file to be ok.)
172.16.10.112        loving.good.stuff.edu      loving
compassion:~$ telnet loving               (Now he can telnet to loving.)
loving login: jim
Password:                                 (However, he cannot log in.)
Login incorrect
                                root on loving ALT-F1 for kim
loving:~# grep -i jim /etc/passwd         (kim checks and finds that jim does
jim:x:1001:100:,,,:/home/jim:/bin/bash     have an account, so she resets
loving:~# passwd jim                                jim's password.)
                                jim on compassion ALT-F2
compassion: telnet loving
loving login: jim
password:
loving:~$                                 (Finally, jim can log on loving.)
```

图26-10 改正jim用户登录到loving时出现的问题

在主机compassion上用ALT-F2以jim用户登录。要远程登录到主机loving，但是却失败了。接着我们ping主机loving。如果不是因为安全的原因而ping不通主机loving，那么Telnet和其他高层的操作当然也不能进行。当我们用IP地址ping主机loving的时候依旧不行。这时，我们走过去看到主机loving已经关机了。因此重新启动它。

在它启动的过程中，我们开始运行了一个ping命令。当主机loving最终启动以后，开始得到返回的数据包。不用再去loving那边看它是否已经启动，我们通过ping命令返回的数据包就可以知道它已经启动了。同时按住Ctrl和C键可以终止ping命令。我们可以注意到发送了31个数据包而只返回了2个，这是因为有29个数据包在loving启动的过程中丢失了。

现在既然loving已经启动了，就可以尝试远程登录到这台主机上，但是却发生了“host name lookup failure”问题。于是我们查看文件etc/hosts来查找字符loving，发现jim在关于loving的条目前加了一个反斜杠，这使得这个条目成为了注释从而不能被辨认。于是，我们在ALT-F1下用根用户登录，用pico编辑器把loving前面的注释删去。

现在回到用户jim的登录界面，并且检查loving的注释性斜线是否已经被删除。现在可以

远程连接到主机loving了，但还是不能登录。因此，我们查看了kim的机器，并首先检查这台机器上是否为jim创建了账号。-i选项使得检索忽略包含jim的字符串而要求完全符合的。经过检索发现jim的用户账号确实存在。于是我们让kim再为jim的用户账号重新设置一遍密码。这样便可以登录了。

26.4.4 e-mail

现在用户账号已经建立并可以正常工作了。让我们运行一些基本的网络功能，先从e-mail开始。在图26-11中可以看到，jim登录到主机loving并创建了一个.forward文件。这个文件包含一个e-mail地址，所有给jim的信件都可以发送到那里。转寄地址是jim@[172.16.10.111]或jim@compassion。现在如果有人在loving给jim发送e-mail，那么这个邮件会为jim转寄到主机compassion。尽管jim可能在很多服务器上都有用户账号，但是他可以只从一台主机上查收他的邮件。他也可以在compassion上创建.forward文件而把邮件转寄到loving。

```
compassion:~$ telnet loving
loving login: jim
loving:~$ echo jim@[172.16.10.111] > .forward
loving:~$ cat .forward                (The dot-forward file is created.
jim@[172.16.10.111]                    on loving.)
loving:~$ logout

compassion:~$ telnet loving 25        (Telneting to SMTP of loving.)
Connected to loving.good.stuff.edu.
220 loving.good.stuff.edu ESMTP
helo compassion                       (Identification of compassion's SMTP)
250 loving.good.stuff.edu Hello jim@compassion,
pleased to meet you
mail from:<jim@compassion>            (Mail from jim@compassion.)
250 <jim@compassion>... Sender ok
rcpt to:<jim@loving>                  (Mail for jim@loving)
250 <jim@loving>... Recipient ok
data                                  (Data for mail to follow.)
354 Enter mail, end with "." on a line by itself
Dear Jim,
       I am testing the .forward file.
Jim
.                                     (Finished entering data for mail.)
250 LAA00201 Message accepted for delivery
quit                                  (Terminate the SMTP session.)
221 loving.good.stuff.edu closing connection
Connection closed by foreign host.
You have mail in /var/spool/mail/jim
compassion:~$
```

图26-11　在主机loving上创建一个.forward文件并把jim的所有邮件转寄给主机compassion。然后在loving上手工发送邮件给jim，测试一下。通过“You have mail…”消息确认可知设置已经成功

jim在创建文件以后，从主机loving注销，回到compassion的会话中。为了检验邮件的转寄是否成功，他可以给自己发一封邮件,这可以使用pine或者其他邮件程序来发送邮件。这将在主机loving上建立一个SMTP会话。首先他要使主机loving上的SMTP服务器确定他是从compassion发送邮件，这是用helo来命令完成的。然后他指明邮件是从jim@compassion发往jim@loving的，这是分别通过mail和rcpt命令来完成的。接着他使用data命令来输入e-mail的内容，然后在单独的一行中输入一个点来终止数据输入。最后，退出SMTP会话。这就是一个手

动发送e-mail的例子。

邮件一旦发送到主机loving后，就会被转寄给主机compassion。因为jim是以他自己的用户名登录的，所以邮件消息便会显示在屏上。使用CTRL－L可以清除屏幕显示，他可以接着阅读邮件或者删除它们。这些操作证明主机loving上的.forward文件创建的是正确的。

26.4.5 FTP

现在我们将测试ftp。在图26-12中，jim使用echo命令在主机compassion上创建了一个local.file文件。这个文件的内容是“This is a file on compassion.”。接着他远程登录到主机loving，用类似的方法创建了一个叫做remote.file的文件，内容是“This is a file on loving.”。

```
compassion:~$ echo This is a file on compassion > local.file
compassion:~$ cat local.file
This is a file on compassion
compassion:~$ telnet loving
loving login: jim
loving:~$ echo This is a file on loving > remote.file
loving:~$ cat remote.file
This is a file on loving
loving:~$ logout
```

```
compassion:~$ ftp loving
 220 loving FTP server ready.
 Name (loving:jim):
 331 Password required for jim.
 Password:
 230 User jim logged in.
ftp> get local.file
 200 PORT command successful.
 550 local.file: No such file.
ftp> put remote.file
 local: remote.file: No such file
ftp> get remote.file
 200 PORT command successful.
 150 Opening BINARY mode connection.
 226 Transfer complete.
  25 bytes received
ftp> put local.file
 200 PORT command successful.
 150 Opening BINARY mode connection.
 226 Transfer complete.
  29 bytes sent
```

```
ftp> get local.file
 200 PORT command successful.
 150 Opening BINARY mode connection.
 226 Transfer complete.
  29 bytes received
ftp> cat local.file
 ?Invalid command
ftp> quit
 221 Goodbye.

compassion:~$ ls
local.file   remote.file
compassion:~$ telnet loving
loving login: jim
loving:~$ ls
local.file remote.file
loving:~$ cat local.file
This is a file on compassion
loving:~$ cat remote.file
This is a file on loving
```

图26-12 在两个服务器上创建文件，使用ftp来传送它们。最后，验证传送成功

通过输入ftp命令，可以把local.file文件传送到主机loving，也可以把文件remote.file传送到主机compassion。首先，他以自己的用户名登录，这样就建立了连接到主机loving的ftp会话。当他从loving执行get命令时，会出现错误提示，这时因为local.file在主机loving上并不存在。同样地，因为remote.file在主机compassion上也不存在，所以执行put命令上传到主机loving时也会出现错误。

但是，我们可以执行get remote.file和put local.file命令，这就不会出现错误。实际上，在图26-12第二列的上部，我们已经可以执行get local.file命令了，尽管之前这个命令会产生错误。这是因为现在在远程主机loving上也存在文件local.file了。这时不能执行cat命令和其他一些命令，这是因为ftp程序不允许你执行全部shell命令，但是它允许你在服务器之间传送文件。相

反地，telnet程序允许你使用所有shell命令，但是不允许使用传送文件。jim退出ftp程序后，他看到这两个文件真的可以在两个服务器之间传送了。

26.4.6 组内共享文件

接着，tim和slim来找jim，他们要求jim把他们分在一个组里，以便使他们之间能够共享文件，但其他人则不能共享他们的文件。tim和slim希望把netgroup作为他们组的名称。

在图26-13里，jim检查tim和slim在他的主机上是否都有用户账号。结果是他们都有账号，这可以从/etc/passwd文件中看出。jim进入pico编辑器，添加了一个叫做netgroup的组。为防止文件由于误操作而被损坏，应该为/etc/passwd文件作一个备份。通过tail命令，可以看到文件的最近的三行，包括为netgroup添加的行。

jim on compassion creating the group netgroup

```
compassion:~# tail /etc/passwd
jim:x:1000:100:Prof. Jim Thomas,,,:/home/jim:/bin/bash
kim:x:1001:100:,,,:/home/kim:/bin/bash
slim:x:1002:100:,,,:/home/slim:/bin/bash
tim:x:1003:100:,,,:/home/tim:/bin/bash
compassion:~# pico /etc/group
compassion:~# tail -3 /etc/group
users::100:games
nogroup::-2:
netgroup::1001:tim,slim
```

tim on compassion creating the netgroupfile

```
compassion:~$ echo echo This file is executable > netgroupfile
compassion:~$ cat netgroupfile
echo This file is executable
compassion:~$ ls -l
-rw-r--r--   1 tim      users          29 Dec 17 11:49
netgroupfile
compassion:~$ chmod 740 netgroupfile
compassion:~$ chgrp netgroup netgroupfile
compassion:~$ ls -l
-rwxr-----   1 tim      netgroup       29 Dec 17 11:49
netgroupfile
compassion:~$ echo date >> netgroupfile
compassion:~$ cat netgroupfile
echo This file is executable
date
compassion:~$ netgroupfile
This file is executable
Fri Dec 17 11:51:31 EST 1999
```

slim on compassion checking netgroupfile's permissions

```
compassion:~$ whoami
slim
compassion:~$ grep netgr /etc/group
netgroup::1001:tim,slim
compassion:~$ cd ~tim
compassion:/home/tim$ cat netgroupfile
echo This file is executable
date
compassion:/home/tim$ echo hostname >> netgroupfile
bash: netgroupfile: Permission denied
compassion:/home/tim$ netgroupfile
bash: ./netgroupfile: Permission denied
```

图26-13　jim创建了一个组，tim创建了组内共享的文件，slim浏览共享文件

首先是组的名称，然后是组的ID。netgroup组的ID是1001。ID数值较低的组应该保留用做系统组。因此，从1001开始为组创建编号。这个组里仅包括tim和slim两个成员。注意到users组的ID是100。这是一个包括所有普通用户的基本组，在/etc/passwd文件中有对它的说明。因此，在/etc/passwd文件中，不提供这个组里的用户名。

jim告诉tim和slim他已经创建了所需的组，这时tim登录到主机compassion，使用echo命令创建了一个名为netgroupfile的文件。这个文件的内容是“echo This file is executable.”。tim使用cat命令显示这个文件，并做了一个ls -l的操作。从访问权限中，tim注意到即使不属于这个组的用户kim也可以阅读这个文件。实际上，这个文件属于users组而不是netgroup组。为了解决这两个问题，他使用chmod命令把权限设定为740，使用chgrp命令更改文件所属的组。再次执行ls -l命令可以看到这些修改。

根据这些访问权限，这个文件的所有者tim，可以浏览、写入和执行这个文件。这个组的成员slim，应该只能浏览这个文件。既不是文件所有者、也不是组成员的kim，对这个文件应该没有任何权限。tim首先检查了他自己的权限。

使用echo命令，他为netgroupfile添加了date命令。接着使用cat命令，显示这个文件，最后，键入文件名，他执行了这个文件的每一行。

接下来是slim。他首先检查/etc/group文件以确保他属于netgroup这个组。然后他改变工作目录为tim的根目录。当他执行cat netgroupfile命令时，文件会被显示。然而，当他试图添加或者执行文件时，他将看到一个“Permission denied”的错误信息。如果kim试图对这个文件进行这三个操作，她将被拒绝，因为操作权限是由tim设定的。

26.5 基本安全性

26.5.1 超级用户的远程登录

假设jim是一个正在运行的服务器的系统管理员，他希望能在家里登录到服务器上完成他的管理工作。当他从家里进行远程登录时，希望能够使用超级用户权限，但又不希望别人拥有这个权力。图26-14显示了jim从主机compassion登录loving。主机loving就像jim家里的PC一样，他希望从这里以超级用户的身份登录到服务器compassion上。

他直接使用根用户登录主机compassion，这是因为他知道根用户的密码。这种设置有两个问题。如果系统密码泄漏了，那么其他人也可以用根用户登录系统。如果进入系统需要至少两个密码，这样会好一些。第二个问题是compassion不能在它的日志文件中记录谁获得了系统密码，这可能是任何人。如果在授予系统密码之前可以确认登录者的身份，这样做会好一些。当然，一个好的黑客都会删除日志文件，但是保留一个谁曾登录过的记录是比较好的。

为了解决这两个问题，jim使用ALT-F1转换到根用户会话。他进入/etc目录，会看到允许登录系统的终端。为了节省空间，它们是被浓缩的。可以在图26-9中看到这些tty（终端类型）。会话结束前，jim使用who命令看到他自己从一个tty登录。tty1到tty6是六个虚拟终端，可以使用ALT-F1到ALT-F6获得。ttys是用于串行连接的，而ttyp则用于telnet远程登录。删除ttyp0到ttyp3以禁止直接用telnet登录系统。jim使用pico编辑器完成这些操作，再次使用tail命令他可以看到这些条目已经被删除了。

jim on compassion: ALT-F2

```
compassion:~$ telnet loving
loving login: jim
loving:~$ telnet compassion
compassion login: root
Password:
compassion:~# logout
```

jim on compassion as root: ALT-F1

```
compassion:~# cd /etc
compassion:/etc# cat securetty
console  tty1       tty2     tty3
tty4     tty5       tty6     ttyS0
ttyS1    ttyS2      ttyS3    ttyp0
ttyp1    ttyp2      ttyp3
compassion:/etc# pico securetty
compassion:/etc# tail -5 securetty
tty6
ttyS0
ttyS1
ttyS2
ttyS3
```

jim on compassion: ALT-F2

```
loving:~$ telnet compassion
compassion login: root
Password:
Login incorrect
loving:~$ telnet compassion
compassion login: jim
compassion:~$ su -
Password:
compassion:~# exit
logout
compassion:~$ logout
```

```
loving:~$ telnet compassion
compassion login: slim
compassion:~$ su -
Password:
compassion:~# exit
logout
compassion:~$ exit
Connection closed by foreign host.
```

jim on compassion as root: ALT-F1

```
compassion:/etc# grep SU_W login.defs
SU_WHEEL_ONLY no
compassion:/etc# pico login.defs
compassion:/etc# grep SU_W login.defs
SU_WHEEL_ONLY yes
compassion:/etc# pico group
compassion:/etc# grep jim group
root::0:root,jim
wheel::10:root,jim
compassion:/etc#
```

jim on compassion: ALT-F2

```
loving:~$ telnet compassion
compassion login: slim
compassion:~$ su -
You are not authorized to su root
compassion:~$ exit
logout
loving:~$ telnet compassion
compassion login: jim
compassion:~$ su -
Password:
compassion:~# exit
logout
compassion:~$
```

图26-14 超级用户远程登录的安全设置

jim切换到主机loving上的会话，这时就不能再用根用户登录到主机compassion。他必须首先以自己的用户名登录，然后再使用su -命令转换到超级用户。这样，compassion就能知道谁执行了su（超级用户接入命令）操作。

在图26-14第二列的上部，可以看到jim装成slim登录主机compassion。然后他发现甚至slim这个用户都可以进行su-操作而成为一个超级用户。这就意味着任何一个用户，只要得到超级用户的密码就可以成为超级用户登录。让我们继续加强安全措施。

转换到根系统的会话，jim发现/etc/login.defs文件中SU_WHEEL_ONLY的值被设为no。使用pico编辑器，jim把no改为yes，这在第二个grep命令中可以看到。接着他修改/etc/group文件，以便使他自己属于根用户组和wheel组。这两个修改使得只有wheel组的成员才能执行su命令操作。

然后，jim假装成slim从loving登录到compassion。服务器会拒绝slim执行su操作。这就是我们想要的。接着他以自己的用户名登录到compassion，会发现这次可以使用su命令来得到超级用户权限。

在公共互联网上，安全对于服务器来说是个大问题。某些漏洞被修补后又会出现其他新的漏洞。我们应该时刻注意最新的网络安全漏洞。刚刚举例说明的修补可以用Slackware 3.6完成。使用更新版本的Slackware，这些修补可能是不必要的，因为更新的安装版本会比以前的版本更安全。

26.5.2 禁止特定的IP地址

当你的服务器被某个特定IP地址使用e-mail攻击时，你希望能够禁止对这个IP地址的一切服务。现在让我们来看看这时该怎么做。

daemon是指一个运行在服务器后台的进程，它可以查看服务请求。在Unix里有个叫做telnetd的telnet后台进程，它在时刻监听是否有终端试图远程登录到服务器。还有一个叫做smtpd的后台进程，它时刻监听是否有人想发送e-mail给服务器等等。同样，后台也有一个叫做inetd的管理进程，它会监控所有的子进程。文件/etc/inetd.conf是inetd的配置文件。这个文件里有如下所示的一行:

```
telnet stream tcp nowait root /user/sbin/tcpd wu.telnetd
```

这一行表示: 在启动过程中，inetd将启动/user/sbin/tcpd，使用wu.telneted作为参数。这会使根系统启动一个进程。一个叫做/etc/services的文件包含所有能列出的TCP应用程序的端口号。

现在如果我们在/etc/hosts.allow文件中添加下面所示的一行文字，中间没有空格:

```
in.telnetd:172.16.10.115:DENY
```

所有来自这个IP地址的远程登录请求都将被服务器拒绝。如果想拒绝所有IP地址以128.117.100开头的主机的请求，则只要在刚才的行里简单地删除115就可以了，如下所示。

```
in.telnetd:172.16.10.:DENY
```

26.5.3 禁止匿名ftp

匿名ftp允许任何人，即使是在服务器上没有账号的人下载那些可以被公共浏览的文件。由于这种形式的ftp不需要密码，因此许多管理员认为这是一种安全隐患。因此，如果有的文件需要使任何人都能浏览，管理员会建立一些专门的匿名ftp服务器。这样，那些不希望被他人看到的私有文件将得到更好的保护。

我们可以在/etc/ftpusers文件里简单地添加下面的一行，就可以禁止匿名ftp访问:

```
anonymous
```

你将发现根用户和其他一些用户已经在这个文件中列出来，这意味着这些用户能进行文件传输。由于添加了anonymous，现在这些用户也不能进行文件传输了。

26.6 使用X Windows

26.6.1 配置X Windows

X Windows是一个由MIT（美国麻省理工学院）开发的免费用户图形界面（Graphical User Interface，GUI），这些年几乎所有版本的UNIX上都在使用X Windows。让我们为服务器运行X Windows做些准备。根据图26-15，可以知道如何配置X Windows。尽管图中有些行被删除了，有些行被缩短了，但所有的重要条目都在图中显示出来，没有任何删除。

开始，运行SuperProbe软件来获取一些关于主机显示的信息。我们有一块不错的Mach64显卡。选择的设置不要使用显卡最大性能指标，不过一旦X Windows在最低配置状态下运行起来，还可以重新配置以获得更好的性能。在我们的这个显卡上有8M的显存。

```
compassion:~#  SuperProbe
WARNING - THIS SOFTWARE COULD HANG
YOUR MACHINE.
First video: Super-VGA
 Chipset: ATI 264GT3 (3D Rage III)
 Memory:  8192 Kbytes
 RAMDAC:  ATI Mach64 integrated
       15/16/24/32-bit DAC w/clock
 Attached graphics coprocessor:
       Chipset: ATI Mach64
       Memory:  8192 Kbytes

compassion:~#  xf86config

This program creates aXF86Config file,
Press enter to continue.   <ENTER>

First specify a mouse protocol type.
 1.  Microsoft compatible
 2.  Mouse Systems (3-button protocol)
 3.  Bus Mouse
 4.  PS/2 Mouse
 5.  Logitech Mouse
Enter a protocol number:   4

Want to enable Emulate3Buttons?   n

Now give the full device name
Pressing enter will use the default.
Mouse device:  <ENTER>

Do you want to use XKB?   n

If you want non-ASCII characters. . .
Want to enable these bindings?   n

Now we want to set the monitor.
Press enter to continue.   <ENTER>

You must indicate the horizontal sync.
 1  31.5; Standard VGA,
 2  31.5 - 35.1; Super VGA
 3  31.5, 35.5; 8514 Compatible
 4  31.5, 35.15, 35.5; Super VGA
 5  31.5 - 37.9; Extended Super VGA
Enter your choice (1-11):   4

You must indicate the vertical sync.
 1  50-70
 2  50-90
 3  50-100
 4  40-150
Enter your choice:   4

Your monitor definition:   asdf
Enter the vendor name:   asdf
Enter the model name:   asdf

Now we must configure video card.
Database about the chipset.
Do you want to look at the database?   n

Determine which server to run.
 3  The XF86_SVGA server.
 4  The accelerated servers.
Which of these screen typess(1-4)?   3

The server is selected by changing the
       symbolic link 'X'.
Want me to set the symbolic link?   y
Want to set it in /var/X11R6/bin?   y

Information about your video card.
 1  256K
 2  512K
 3  1024K
Enter your choice:   3

Enter a few identifications
Identifier for your video card:   asdf
Vendor name of your video card:   asdf
Model name of your video card:   asdf

 1  Chrontel 8391
 2  ICD2061A and compatibles
Clockchip setting (1-12)?   <ENTER>

Want me to run 'X-probeonly' now?   n

 1  Change the modes for 8pp
 2  Change the modes for 16bpp
Enter your choice:   1

Select modes from the following list:
 1  "640x400"
 2  "640x480"
 3  "800x600"
 4  "1024x768"
Which modes?  3

Do you want a virtual screen ?   n
 4  Change the modes for 32bpp
 5  The modes are OK, continue.
Enter your choice:   5

Shall I write it to /etc/XF86Config?   y
compassion:~#  startx
```

图26-15 配置X Windows

键入“xf86config”开始进行配置。首先系统会询问鼠标类型。键入“4”来选择PS/2鼠标。然后选择在键盘或者扩展键盘映射里不使用外来字体。

接着开始设置显示器。首先，选择Super VGA显示器，选择标准的垂直同步设置。其他给出的选项在图中没有显示。接下来看图26-15第二列的上部，可以在这里只敲三次回车，不过图中输入了一个虚拟的名字“asdf”。

现在显示器被设置好了，下面继续设置显卡。选择一个Super VGA服务器，让系统链接

到指定的服务器。再一次，输入虚拟的身份和名字，这次是为了设置显卡。接着使用默认的时钟频率设置，而且不运行X-probe。我们不想使用比实际的物理屏幕大的虚拟屏幕，并键入“5”来确认这个屏幕的工作模式。最后，把设置好的配置写入XF86Config文件，开始运行X Windows。

注意，为了在主机上运行X Windows，你需要了解其系统信息。对你的PC了解得越多，你就越容易在这个配置对话框里选择正确的选项。记住，SuperProbe也能在你的视频设置中给出相当数量的信息。即使得到了所有这些信息，你也许仍要多次运行xf86config命令来进行配置，每次尝试那些稍有不同的设置。经过一些试验和错误，你就可以在服务器上运行X Windows了，这个过程需要一些耐心。

26.6.2 Apache Web服务器

一旦X Windows建立起来，我们就可以运行Netscape，它是和Slackware系统绑定在一起的。当我们安装Linux时，Apache Web服务器就会作为默认项被安装。从这时开始，主机上就有一个Web服务器在运行，但是我们很少访问它。可以简单地在浏览器中键入自己的IP地址访问自己的Web服务器，如下所示:

```
http://172.16.10.111
```

上面的例子显示了jim如何从他自己的浏览器中访问他自己的主页。为了添加一个到kim主机的链接，jim可以在/var/lib/apache/share/htdocs目录下的index.html文件中添加下面这行信息:

```
<A HREF="http"//172.16.10.112/'>loving</A>
```

现在jim的主页有了一个到kim主机的链接。以这种方式，可以添加到实验室其他Web服务器的链接，这样可以构成一个小型的WWW（万维网）环境。

26.7 网络管理

26.7.1 DNS

现在把compassion设置成为一个DNS服务器。让loving把compassion作为它的DNS服务器，代替使用/etc/hosts文件完成把主机名转化为IP地址的任务。

要完成这项功能，需要compassion上的六个文件。在图26-16a和图26-16b可以看到这些文件的内容。两个文件在/etc目录下建立，其他四个文件在/var/named目录下建立。named子目录要建立在/var目录下。这些文件分别叫做/etc/named.conf、/etc/resolv.conf、/var/named/named.local、/var/named/root.cache、/var/named/good.stuff.hosts和/var/named/good.stuff.rev。文件中的每一个逗号、圆括号等都需要像图中一样正确地输入。这些文件已经尽可能地简化了。如果不连接到公共因特网上，这些文件还可以更简单一些。但是，图中所列出来的文件足以解决因特网上遇到的IP问题。

这次将不在这些文件的结构上花费时间，因为可以参考man文件来理解它们。在图26-17中，只来看一下一个文件，这个文件是主机loving把主机compassion作为DNS服务器所必需的，这个文件叫做/etc/resolv.conf。

/etc/named.conf

```
/* A simple BIND 8 configuration */
options {
        directory "/var/named";
};
zone "good.stuff.edu." in {
        type master;
        file "good.stuff.hosts";
};
zone "10.16.172.in-addr.arpa." in {
        type master;
        file "good.stuff.rev";
};
zone "." in {
        type hint;
        file "root.cache";
};
zone "0.0.127.in-addr.arpa." in {
        type master;
        file "named.local";
};
```

/etc/resolv.conf

```
search good.stuff.edu
nameserver 127.0.0.1
```

/var/named/named.local

```
@   IN   SOA   compassion.good.stuff.edu.
               hostmaster.good.stuff.edu. (
               1986012101 ; Serial
               3600       ; Refresh
               300        ; Retry
               3600000    ; Expire
               14400 )    ; Minimum

    IN   NS    compassion.good.stuff.edu.
1   IN   PTR   localhost.
```

/var/named/root.cache

```
; formerly NS.INTERNIC.NET
.                        3600000   IN  NS  A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000       A   198.41.0.4

.                        3600000       NS  B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000       A   128.9.0.107

.                        3600000       NS  C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000       A   192.33.4.12
```

a) 所需的DNS服务器compassion的六个文件中的四个

/var/named/good.stuff.hosts

```
@               IN      SOA     compassion.good.stuff.edu.
                        hostmaster.good.stuff.edu. (
                        19991124        ; serial
                        10800           ; refresh 3 hours
                        3600            ; retry 1 hour
                        3600000         ; expire 1000 hours
                        86400) ; minimum 24 hours

                IN      NS      compassion
                IN      MX      10 compassion
                IN      MX      50 loving

compassion      IN A    172.16.10.111
loving          IN A    172.16.10.112
```

/var/named/good.stuff.rev

```
;/var/named/good.stuff.rev
;
@       IN      SOA     compassion.good.stuff.edu.
                        hostmaster.good.stuff.edu. (
                        19991123        ; serial
                        10800           ; refresh 3 hours
                        3600            ; retry 1 hour
                        3600000         ; expire 1000 hours
                        86400) ; minimum 24 hours

        IN      NS      compassion.good.stuff.edu.

111     IN      PTR     compassion.good.stuff.edu.
112     IN      PTR     loving.good.stuff.edu.
```

b) 所需的DNS服务器compassion的其他两个文件

图26-16　所需DNS服务器compassion的六个文件

从图26-18上部，可以看到在主机loving上已经在其/etc/hosts文件中注释出compassion的条目。因此，当ping主机compassion时，必须通过由loving指向compassion 的/etc/resolv.conf文件来解析IP地址。为了进一步确定这一点，使用mv命令重命名resolv.conf文件。现在我们ping不通主机compassion了。用它原来的名称重命名后，又可以解析IP地址，从而能ping通主机compassion了。nslookup命令用来检查DNS服务器是否已正确地设置，结果是DNS正常工作了。

```
loving:# cat /etc/resolv.conf
search good.stuff.edu
nameserver 172.16.10.111
```

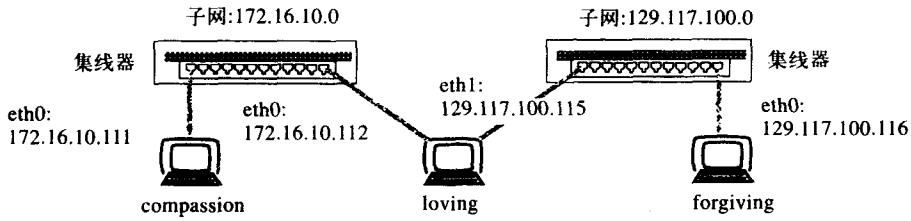
图26-17 为loving提供DNS服务所需的文件

```
(注意/etc/hosts已经注释出compassion的IP地址)
loving:/etc# grep 111 hosts
#172.16.10.111 compassion.good.stuff.edu compassion

(因此，compassion的IP地址由DNS服务器予以解析)
loving:/etc# ping compassion
PING compassion.good.stuff.edu (172.16.10.111): 56 data bytes
64 bytes from 172.16.10.111: icmp_seq=0 ttl=255 time=0.3 ms

(将resolv.conf重新命名可以防止loving从DSN服务器获得IP地址)
NOW RESOLV.CONF DOESNT EXIST AND PING DOESNT RESOLVS
loving:/etc#mv resolv.conf resolv.conf.old
loving:/etc#ping compassion
ping: unknown host compassion

(恢复resolv.conf后，可以再次解析IP地址)
loving:/etc# mv resolv.conf.old resolv.conf
loving:/etc# ping compassion
PING compassion.good.stuff.edu (172.16.10.111): 56 data bytes
64 bytes from 172.16.10.111: icmp_seq=0 ttl=255 time=0.2 ms

loving:~# nslookup
Default Server:  compassion.good.stuff.edu
Address:  172.16.10.111

> compassion
Server:  compassion.good.stuff.edu
Address:  172.16.10.111
Name:    compassion.good.stuff.edu
Address:  172.16.10.111

> 172.16.10.112
Server:  compassion.good.stuff.edu
Address:  172.16.10.111
Name:    loving.good.stuff.edu
Address:  172.16.10.112

> exit
loving:~#
```

图26-18 访问loving的DNS服务器

26.7.2 静态路由

可以做的另一个实验是把其中的一个服务器配置成为路由器。让我们把loving作为路由器。这时需要在loving上再装上一块以太网卡。图26-19显示使用两个集线器创建了两个子网。服务器compassion和loving的一块网卡处在一个子网上，而主机forgiving和loving的另一块网卡处在另一个子网上，如图中所示。也可以只用交叉电缆把两个网卡连接在一起，不过，这样的话就不能在两个子网上增加其他主机了。




```
loving:/etc/rc.d# cat rc.inet1
#! /bin/sh

HOSTNAME=`cat /etc/HOSTNAME`
# Attach the loopback device.
/sbin/ifconfig lo 127.0.0.1
/sbin/route add -net 127.0.0.0 netmask 255.0.0.0 lo

# Edit for your setup.
IPADDR="172.16.10.112"      # REPLACE with YOUR IP address!
IPADDR2="129.117.100.115"   # IP Address for second eth card
NETMASK="255.255.255.0"     # REPLACE with YOUR netmask!
NETMASK2="255.255.255.0"
NETWORK="172.16.10.0"       # REPLACE with YOUR network address!
NETWORK2="129.117.100.0"
BROADCAST="172.16.10.255"   # REPLACE with YOUR broadcast address, if you
BROADCAST2="129.117.100.255" # have one. If not, leave blank and edit below.
GATEWAY="172.16.10.112"     # REPLACE with YOUR gateway address!
GATEWAY2="129.117.100.115"

/sbin/ifconfig eth0 ${IPADDR} broadcast ${BROADCAST} netmask ${NETMASK}
/sbin/ifconfig eth1 ${IPADDR2} broadcast ${BROADCAST2} netmask ${NETMASK2}

# Uncomment these to set up your IP routing table.
/sbin/route add -net ${NETWORK} netmask ${NETMASK} eth0
if [ ! "$GATEWAY" = "" ]; then
   /sbin/route add default gw ${GATEWAY} netmask 0.0.0.0 metric 1
fi
```

图26-19　把主机loving配置成两个子网之间的路由器

要把主机loving配置为路由器，必须修改它的/etc/rc.d/rc.inet1文件，这也在图26-19中给出。这里，用大写字母来定义变量，如IPADDR和IPADDR2。主机loving的每一个接口都需要自己的IP地址、子网掩码和网络地址等。

注意到文件中的两个/sbin/ifconfig命令。它们分别用来配置两个网卡的接口：eth0和eth1。字符串${IPADDR}提供了上面定义的变量的值。在这些行下面是一个/sbin/route add命令。这将把第一个子网添加到路由表中，我们需要手工添加另一个子网。

在图26-20中，启动主机loving，可以看到以太网接口eth0和eth1都已经被设置了。检查一下它们的地址，确保它们都是正确的。netstat -nr命令显示出第一个子网已经被加入到路由表中，但是另一个子网却不在路由表中。所以，我们要执行route add命令把另一个子网添加到路由表中，其中“gw”代表网关。接口129.117.100.115是子网129.117.100.0的网关。从路由器loving，我们可以ping通两个子网上的服务器。

我们是否已经拥有一个从compassion经过loving到forgiving的路由了呢？为了验证这个问题，可以看图26-21。这里，使用给loving增加路由同样的方法，给compassion增加一个默认的路由。从主机compassion上可以ping通主机loving和主机forgiving，这便证明了loving被正确地配置为两个子网之间的路由器。一个从forgiving到compassion的反向测试证明反向路径也被正确地配置了。

```
loving:~# ifconfig
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Bcast:127.255.255.255  Mask:255.0.0.0
        UP BROADCAST LOOPBACK RUNNING  MTU:3584  Metric:1

eth0    Link encap:Ethernet  HWaddr 00:50:04:D3:D9:98
        inet addr:172.16.10.112  Bcast:172.16.10.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth1    Link encap:Ethernet  HWaddr 00:10:4B:70:9A:C6
        inet addr:129.117.100.115  Bcast:129.117.100.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

loving:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.10.0     0.0.0.0         255.255.255.0   U      1500 0          0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U      3584 0          0 lo

loving:~# route add -net 129.117.100.0 gw 129.117.100.115

loving:~# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.10.0     0.0.0.0         255.255.255.0   U      1500 0          0 eth0
129.117.100.0   0.0.0.0         255.255.255.0   U      1500 0          0 eth1
127.0.0.0       0.0.0.0         255.0.0.0       U      3584 0          0 lo

loving:~# ping 129.117.100.116
PING 129.117.100.116 (129.117.100.116): 56 data bytes
64 bytes from 129.117.100.116: icmp_seq=0 ttl=64 time=0.3 ms
64 bytes from 129.117.100.116: icmp_seq=1 ttl=64 time=0.2 ms

loving:~# ping 172.16.10.111
PING 172.16.10.111 (172.16.10.111): 56 data bytes
64 bytes from 172.16.10.111: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 172.16.10.111: icmp_seq=1 ttl=255 time=0.2 ms
```

图26-20 给loving增加一个新的路由

```
compassion:~# netstat -nr
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
172.16.10.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U         0 0          0 lo
0.0.0.0         172.16.10.112   0.0.0.0         UG        0 0          0 eth0

compassion:~# ping 172.16.10.112
PING 172.16.10.112 (172.16.10.112): 56 data bytes
64 bytes from 172.16.10.112: icmp_seq=0 ttl=64 time=0.3 ms
64 bytes from 172.16.10.112: icmp_seq=1 ttl=64 time=0.2 ms

compassion:~# ping 129.117.100.116
PING 129.117.100.116 (129.117.100.116): 56 data bytes
64 bytes from 129.117.100.116: icmp_seq=0 ttl=63 time=0.6 ms
64 bytes from 129.117.100.116: icmp_seq=1 ttl=63 time=0.5 ms
```

图26-21 对loving进行路由器的测试

习题

26.1节

1.下面哪一个不是Linux的一个版本?

a. Red Hat b. Open BSD

c. Slackware d. Caldera

2.简述Linux的优点？在各种资料中有很多相关的描述。

3. 不同版本的Linux有什么共同点？

26.2节

4. 允许对硬盘驱动器重新分区的软件是什么？

5. Linux需要多少个分区？每个分区的名称是什么？它们的作用是什么？

6. /dev/hdb3指的是哪块硬盘？哪个分区？

7. Slackware的安装过程中需要哪些软盘？

8. 描述LILO以及它的作用。

9. fdisk的哪些命令可以完成下面的功能：查看分区列表，改变分区类型，删除一个分区，创建一个新的分区？

10. 什么命令可以改变IP地址或主机名？

11. 关闭Unix服务器的正确方法是什么？

26.3节

12. 当改变IP地址时，什么文件被更新？当改变主机名时，又是哪个文件被更新？

13. 在什么情况下你需要改变IP地址？

14. 什么文件可以让你根据主机名寻址一个主机而不是IP地址？

15. 什么命令可以查看下列内容：

a. 在当前服务器上运行的接口

b. 服务器启动时显示屏上显示的信息

c. 文件系统列表

d. 服务器上的CPU类型

26.4节

16. 当删除根密码时需要哪一张软盘？

17. 完成以下任务需要什么命令？

a. 找出在服务器上哪些人拥有用户账号

b. 创建一个新的用户

c. 查看james是否在服务器上拥有用户账号

18. jim希望只在forgiving上阅读他的e-mail，而他在forgiving、loving、compassion上都有用户账号。

a. 他应该在哪个（些）服务器上创建哪个（些）文件？

b. 显示这些文件的内容。

c. 每次有人给他发e-mail到loving或者compassion上时，jim应该怎么做？（如果需要的话）

19. 解释ftp和telnet的不同。

20. 解释get和put这两个命令的不同。

21. 什么命令可以让文件所有者不能对文件进行任何操作，让组成员只能写入文件，其他任何人都可以读取和执行文件？假设该文件的文件名为file1。

26.5节

22. 为了防止直接用telnet进入根目录，要从哪个（些）文件中删除哪一个tty?
23. 哪个命令可以授予超级用户权限?
24. 如果希望只有本人拥有超级用户权限，jim应该把他加在哪个组里？并用什么样的方式修改哪一个文件?

第27章 虚拟专用网

20世纪90年代初期，当本书的第1版出版的时候，公共交换电话网(PSTN)上的虚拟网络刚刚兴起。现在，因特网上的虚拟网络，已经在很多领域取代了以前在PSTN上的虚拟网络。本章中所介绍的内容，只涉及到“在写作本书的时候”的一些知识。由于虚拟专用网（Virtual Private Network，VPN）的技术发展得很快，因而你也许不愿意学习本章内容。但是由于虚拟专用网已经变得越来越重要，因此我们不能不对它做相关的介绍。

27.1 虚拟专用网介绍

27.1.1 什么是虚拟专用网

在5.1.4节中，我们曾经讨论了基于公共交换电话网(PSTN)的虚拟专用网和基于因特网（Internet）的虚拟专用网的不同之处。今天，在谈论到虚拟专用网的时候，通常是指基于

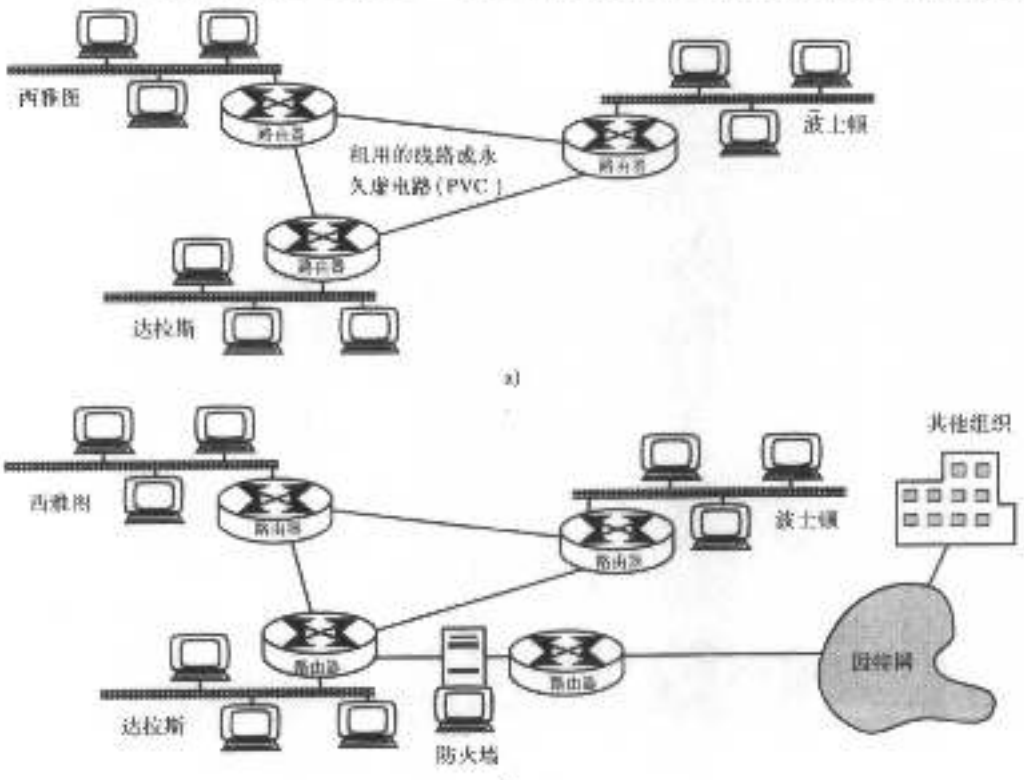


图27-1 a) 企业内部网络是一个TCP/IP网络。一个组织拥有或租用了这个网络的全部设备、连接和线路，企业外部的人不能直接访问它。b) 企业内部网络可以通过防火墙与公共Internet相连。这时的企业内部网络对其他公共网络用户来说就是外联网

Internet的虚拟专用网。事实上，也可以在帧中继网和ATM网络上建立虚拟专用网。从广义上说，**虚拟网络**就是利用诸如Internet、PSTN、帧中继等网络的公共设施来建立一个专用的网络。虚拟网络就如同一个专用网络，但是它所使用的是公共网络的资源。这看起来就好像是你有一个自己的专用网络，或者有与各种站点直接的连接。

对企业内部网（intranet）的介绍是引出基于Internet的虚拟专用网的第一步。**企业内部网**是归属于一个企业或组织的网络，由TCP/IP协议的设备和链路构成。在这里，这个组织想要建造自己的互联网（internet），但又想避免因连入Internet而带来的安全性上的风险（公共Internet用大写字母“I”拼写，而专用internet用小写字母“i”拼写）。图27-1a所示是一个跨越三个城市的企业内部互联网的例子。

当一个组织想与Internet具有连通性时，它可以通过防火墙把自己的网络连入到Internet上。这样，这个组织中的成员就能进入公共网络，同时从公共网络也可以访问这个内部网络。从图27-1b可以看到这一点。通过设置，防火墙可以过滤一些数据包，从而允许特定的数据包发送到企业内部网，阻止其他的数据包向外发送。防火墙也可以允许特定的数据包进入企业内部网络，并滤除其他一些公共数据包。实际中有很多种策略来定义过滤的机制。可以被Internet中的其他人（在图27-1中被描述成其他组织）访问的企业内部网络被称作外联网（extranet）。当Internet被用来建立两个站点之间的通信链路时，这条链路被称作**隧道**。在第2章的结尾，我们介绍过隧道和封装的概念。

27.1.2 按用户类型对虚拟专用网分类

虚拟专用网的种类很多，所以我们只能描述其中的一部分。可以通过对这些种类进行分组来介绍它们。通常有两种基本的分类方法，即按照终端用户使用的方式或者根据所在的OSI的层次来对虚拟专用网进行分类，如图27-2所示。

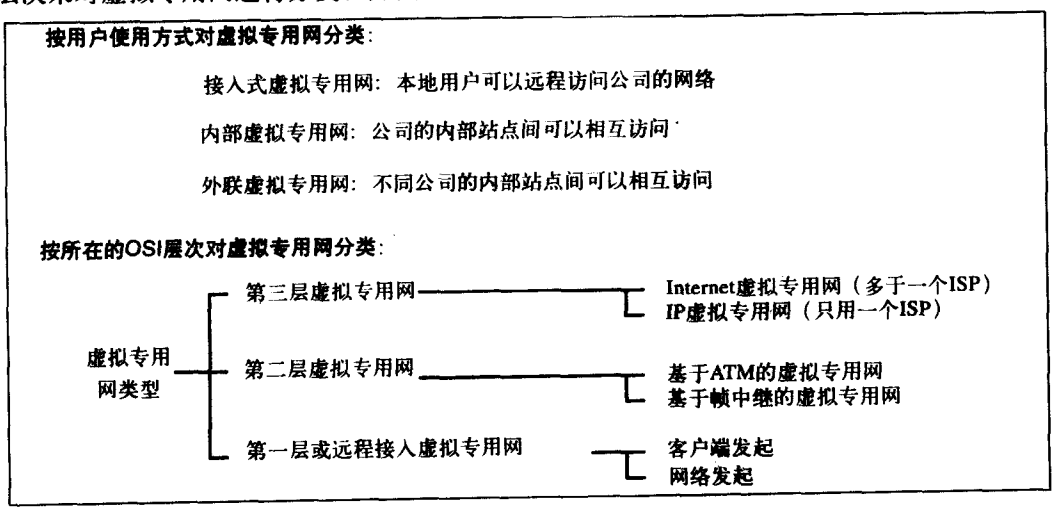
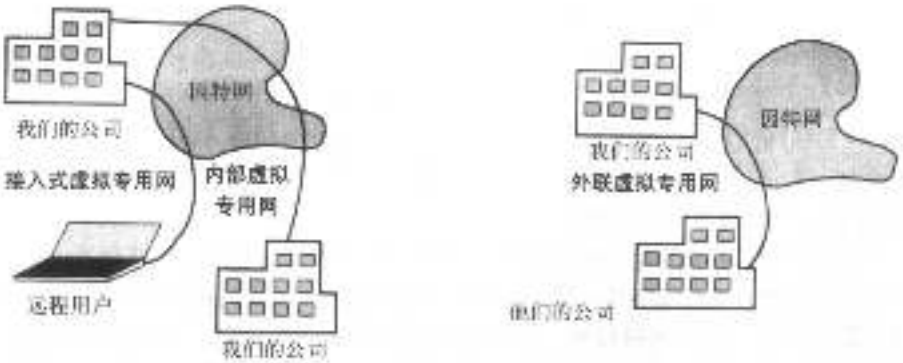


图27-2 对虚拟专用网分类的两种方法

如果按照用户类型进行分类，就可以把虚拟专用网络分为接入型、内部网络型和外联型虚拟专用网。如果一个商人临时住在一个旅馆里或者正在访问一个客户的站点，这时他又要访问他自己公司的网络，那么他所需要的网络就被称作**远程接入虚拟专用网**，或简称为接入

式虚拟专用网，如下边的左图所示。当两个站点同属于一个组织的内部网络，它们彼此之间通过Internet互相连接，这样的网络被称为**内部网络虚拟专用网**（VPN），这也同样在下边的右图中给出。



一个组织可能需要通过Internet访问其他组织的内部网络，完成采购订单或者其他的一些事情。这种类型的虚拟专用网允许一个组织的内部网络通过Internet连接到另一个组织的内部网络中，这就被称为外联虚拟专用网，如上边的图所示。

27.1.3　按所在的OSI层次对虚拟专用网分类

图27-2中所示的第二种对虚拟专用网分类的方法就是按照所在的OSI层次分类。让我们先从第二层开始讨论。在这一层中，帧中继和ATM网络能被用来实现虚拟专用网。由于在这些网络中可以在两个站点之间建立永久虚电路（PVC，Permanent Virtual Circuit），因此使用这些网络是比较安全的。由于其他数据都不能在你所建立的永久虚电路中传输，这样一来你不仅可以得到更好的安全性，而且还能规定其服务质量（QoS，Quality of Service）。因为这种类型的虚拟专用网络没有那么重要，因而以后不会再提到它们。如果你真的要为两个站点间的虚拟专用网选择Internet或者第二层虚拟专用网，你就要认真考虑这些第二层虚拟专用网。如果你相信带有数据的数据流在租用的线路中传输是安全的，那么就可以使用帧中继和ATM网络。

在OSI结构的第三层，有两种类型的虚拟专用网：Internet虚拟专用网（Internet-VPN）和IP虚拟专用网（IP-VPN）。这些虚拟专用网是基于IP协议的，通过IP协议可以实现路由或其他的第三层协议，它们都是利用Internet。如图27-3所示，当一个公司通过一个Internet服务提供商（ISP，Internet Service Provider）接入Internet时，就被称为IP虚拟专用网或者单一ISP虚拟专用网。如图27-3a所示。如果一个公司的不同机构遍布全国，这就需要一个全国范围的ISP来提供服务。公司所有站点间的所有业务都在属于同一个ISP的Internet骨干网上传输。只有当分组数据需要传输到其他公司时，才会使用不同的ISP，只有这时才会建立与其他ISP的连接。

通过同一个ISP来传输所有站点之间的业务可以使这个ISP提供更好的安全性。ISP可以提供一系列契约，被叫做服务等级协议（Service Level Agreements，SLA）。服务分级协议为商业客户提供了保证，明确了他们可以从ISP那里得到的服务级别，服务的可用性、吞吐量和延迟时间、平均的修复时间、通信的优先级和服务质量，这些都是服务分级协议所要保证的特性。如果不止一个ISP参与创建虚拟专用网，那么就不要指望和预先规定服务等级。现在，规定了服务质量的等级，在能够接受的性能等级上语音和视频也可以在站点之间进行传输。

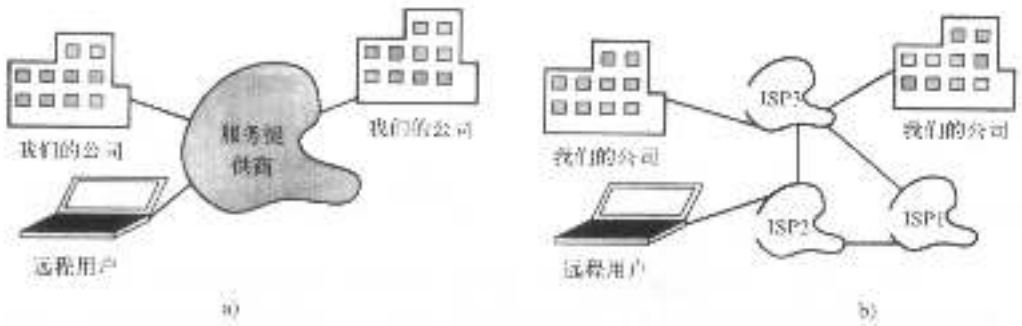


图27-3 a) IP-VPN; b) Internet-VPN

在为远程站点创建连接时如果涉及到多个ISP，就不要指望服务得到保证，如图27-3b所示。这种类型的虚拟专用网被称为Internet虚拟专用网。然而，通过Internet虚拟专用网，我们的VPN可以覆盖全球，连接到更多地方。没有哪一个ISP会在世界各地都存在。

图27-4a给出了一个用户端发起的远程接入虚拟专用网。图27-4b给出了一个网络端发起的远程接入虚拟专用网。对于用户端发起的远程接入虚拟专用网，公司的工程师必须在终端用户的电脑中安装接入虚拟专用网的软件，且这个软件必须与公司网络中安装的软件相兼容。这样才能在终端用户和其公司的办公室之间建立起虚拟专用网。终端用户可以从任何地方拨号连接到Internet上的任何一个ISP。

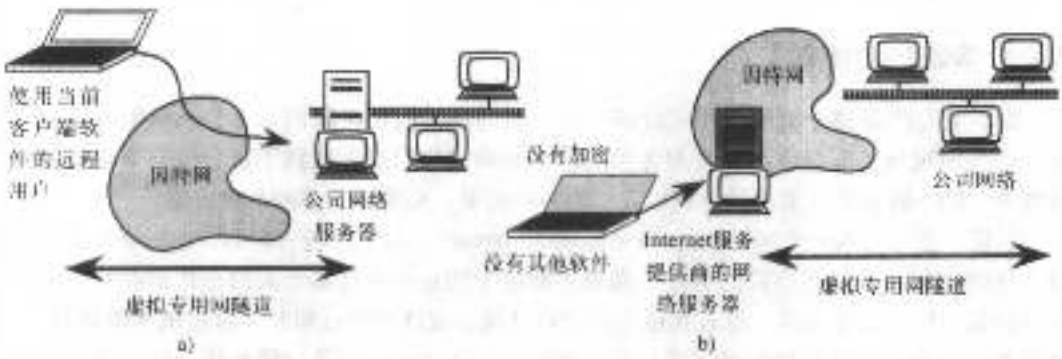


图27-4 a) 对于用户端发起的远程接入，远程用户直接拨入公司网络，建立一个端到端的虚拟专用网隧道。b) 对于网络发起的远程接入，远端用户通过一个给定的号码拨入网络服务器，这个ISP的网络服务器会创建一个虚拟专用网（VPN），连接到这个公司的网络

在网络发起的虚拟专用网络中，终端用户不需要在他们的机器中安装虚拟专用网软件，也不需要去兼容公司内部网络的虚拟专用网软件。用户只需拨出一个预先规定的号码，这样他就可以连接到由ISP提供的为该公司特别分配的虚拟专用网服务器上。在这两点间建立的连接中是不加密的。

这时ISP的网络服务器将通过Internet代替该用户来建立虚拟专用网的连接。这种建立连接的过程存在一个问题，如果用户距离ISP的网络服务器很远，那么使用电话连接的费用就会变得很可观。在美国国内，如果用户拨出800电话号码，这是可以禁止的。这种类型的虚拟专用网更适合身处大城市的用户使用。

27.2 虚拟专用网的优点

我们已经讨论了IP虚拟专用网如何提供较好的服务。首先，创建虚拟专用网是因为它可以减少网络的运行费用。但是，它的优点不只于此。在大多数地方，每天通过Internet接入已经变得越来越普遍了。如果使用Internet，就能从更多的地方接入网络。如果一个公司需要一个临时的连接，采用租用线路可能需要等一个月或更长的时间，这取决于运营商。虚拟专用网提供了到公司网络更好的连通性。

当然，对所有虚拟专用网的用户来说安全性是一个值得特别关心的问题。在过去的几年里，为了得到更好的安全性已经开展了大量的研究，现在在虚拟专用网上安全地传输敏感数据已经成为可能。因此，公司的雇员不仅可以在任何地方接入公司的网络来收发他们的数据，而且还可以安全地存取这些数据。公司的客户可以进入公司的网站，传送信用卡的信息而不必担心这些信息会被其他人得到。公司的不同部门之间可以通过安全的虚拟专用网通路互相传送信息。另外，你还可以进入其他公司的虚拟专用网，并且安全地交换信息。

在20世纪90年代中期，没有人想到网络会成为一个主要的交易平台。那些通过网络使自己知名的人能够得到更多的利益。虚拟专用网也与此类似。使用虚拟专用网可以给公司带来通过其他途径所得不到的机会，这也许是使用虚拟专用网最大的理由。随着新的应用不断出现，公司可以通过虚拟专用网增加资本，加快发展。

27.3 安全问题

27.3.1 确定安全性的要求

保证安全性是建立虚拟专用网时的一个主要问题。因此，我们并不是只给出安全性的定义，而是通过列出安全性所包含的各项内容，来确定我们是否达到了安全性的要求。你将会发现单一的一种加密方案不足以满足我们的各种需要，必须采用多种加密方案。

认证：当你进入一个网站比如www.prenhall.com时，为了订购一本书，你需要出示信用卡号，这时你怎么确信在连接的另外一端确实是这个站点而不是某个人的恶作剧呢？你怎么确认在你发出信用卡号之前，没有其他用户把自己伪装成这个站点呢？（这也被叫做欺骗。）认证就是要保证在网络连接的另一端存在一个站点，这个站点正是你所要访问的，而不是其他的站点。

信息的完整性：你怎么保证从信源发出的信息在传输过程中没有被别人修改过？信息的完整性使我们可以保护自己的信息，确保它没有被修改过。

不可否认性：某个人发送电子邮件给他的股票经纪人让他帮助买进大量的股票。第二天那些股票的价格跌了。如果那个顾客声称没有事先要求订购股票，那么在这个事件中股票经纪人又怎样保护自己呢？不可否认性可以提供一种方法来证明一个发送过的信息的实际发送者是谁。

保密性：怎么能确定信息在传输过程中没有被泄漏呢？你也许不会在意关于你下学期选课的电子邮件被别人阅读。但是对于某些人来说，如果一些信息让未被授权的人看到，结果将是灾难性的。保密性提供了所需的隐私保证。

授权和审核：在连接另一端的人有权去提交订单吗？授权功能可以确定这一点。也许还会需要证实文件或交易所经过的几道程序。审核可以保留这样的“电子账簿”。

27.3.2 加密方案

散列法：正像前面所述，为满足所有这些为了达到安全性所提出的要求，需要一种以上的加密方案。散列法就是一种加密方案。它可以得到较完整的信息数据。散列法不使用密钥来加密，它也被称为单向加密方法。这是因为散列法可以把明文转换成密文。一旦变成密文，就不能再恢复出明文了。所以，这种加密方式是单向的。

HMAC、MD2、MD4、MD5和SHA都是实现散列法的功能函数。为了便于说明，我们将用较为简单的模数函数。这个模数函数的返回值是用一个数除去另一个预定数的余数。比如40mod37得3，77mod37也得3。3是40或77除以37的余数。如果得到的密文是3，那么我们就不能确定原来的明文是40。这是因为有许多其他的数字被37除后也余3。

从图27-5中可以看到被传输的数字是6249。用模为37取余后得到的余数是33。把33附加在6249后面。在图的右上部分，假设接收端得到的数据是6248而不是6249，那么怎么知道在连接过程中是否有某些地方修改过这个信息呢？

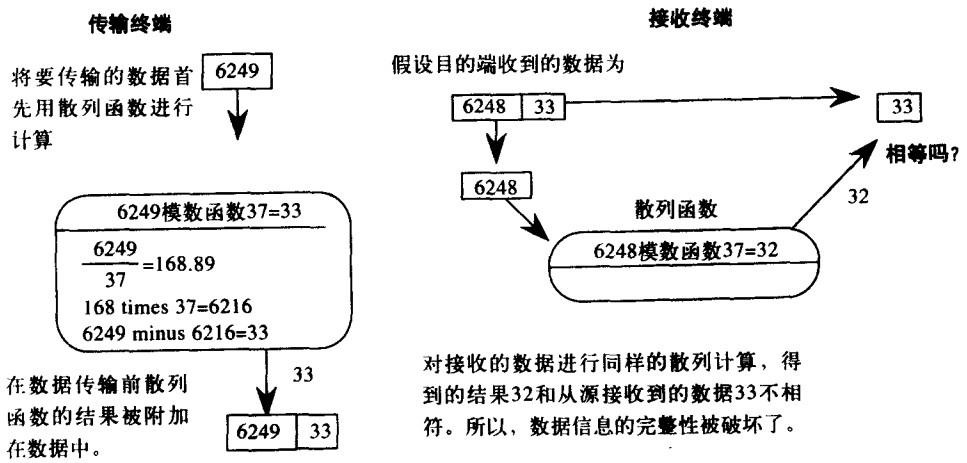


图27-5 散列函数怎样检查信息的完整性

这可以通过由散列函数所得到的数据来确定这一点。6248mod37等于32。散列函数的计算结果是32，这与我们在散列数据位置的33不相符。所以可以确定数据的完整性被破坏了。

密钥加密：使用密钥的加密方法被称为双向加密或对称加密。对于使用密钥加密的方法，发送端可以把明文转换成密文，而在接收端还可以把密文转换回所发送的明文。密钥加密的方法主要用于实现隐私或保密。密钥加密的算法有DES、3DES、IDEA、CAST、RC4和RC5。与前面一样，这里将用一个较简单的算法来介绍密钥加密的方法，如图27-6所示。

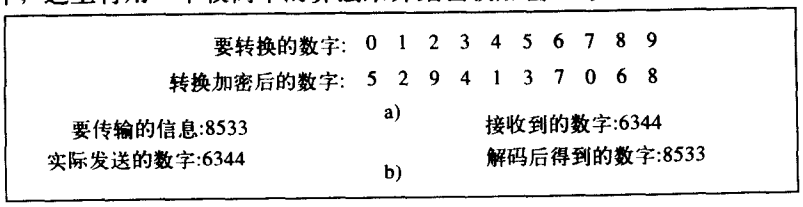


图27-6 a) 两个终端使用的密码表；b) 信息在传输之前加密，在接收后被解密

密钥加密的方法就像在接收端和发送端保存着一份相同的密码编码表，也只有对应的两

端才有这张编码表。图27-6a所示就是这样的一个编码。0变成5，1变成2，等等。图27-6b是信息8533使用这种编码方法加密后变成了6344。6344又在接收端通过同样的编码表来解码。

公共密钥加密：在公共密钥加密法（Public Key Cryptography，PKC）中，密钥都是成对出现的。其中一个密钥称为私有密钥而另一个则称作公有密钥。公有密钥对任何人都是公开的，通过它可以把用私有密钥加密的信息数据恢复出来。这是因为只有拥有私有密钥的人才能发送加密的信息，这些加密信息也只有通过相应的公有密钥才能被解码。同样地，通过特定的公有密钥加密的信息只能通过相应的私有密钥才能被解码。

当分配这些密钥时，任何一个密钥既可以作为私有密钥也可以作为公有密钥。但是，一旦密钥分配好之后，就要保护好私有密钥的安全，不要让其他人知道，这一点是非常重要的。信息通过私有密钥加密后，这个信息就可以被任何拥有公有密钥的人解密。但是在解密的时候，接收者只能解密这个信息的内容却不能解出加密所用的私有密钥。

斯坦福大学的Diffie和Hellman最早证实了这一系统的可行性，麻省理工学院的Rivest、Shamir和Aldeman随后创建了RSA（用他们的名字命名）公共密钥系统。密钥的长度越长，那么这个加密方案就越安全，但需要的解密时间也就越长。所以，PKC更多的时候是用会话过程中随机使用的SKC密钥进行加密。另外PKC也用来实现认证和不可否认性。

下面介绍两个PKC的应用示例。其中的一个非常简单但并没有实际应用价值，另一个则介绍了RSA加密方法的工作过程。图27-7是忽略进位的加密方法的工作过程。在图中，有两个密钥3和7。可以任取其中的一个作为私有密钥，另一个作为公有密钥。在本例中，选择7作为公有密钥，3作为私有密钥。然后你告诉每个人，7是你的公有密钥，但要把私有密钥3对外保密。

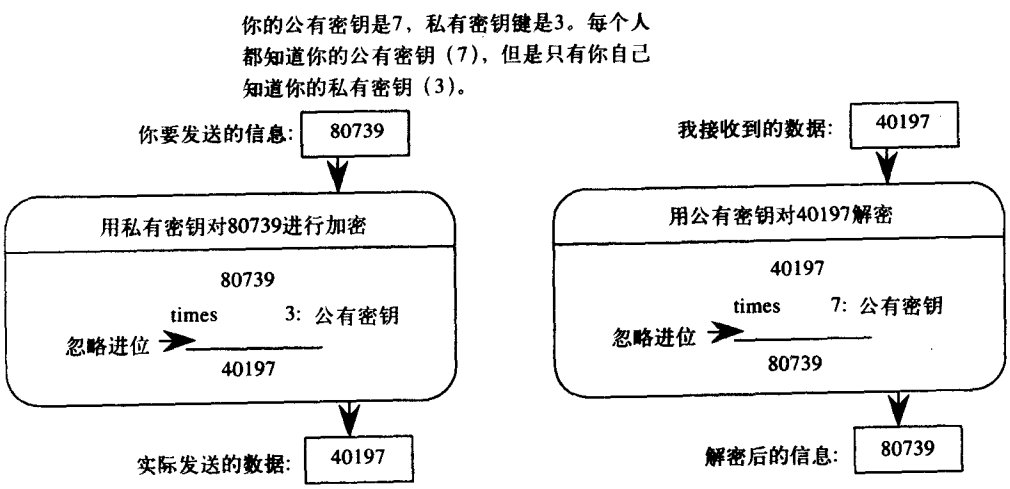


图27-7　公共密钥加密法

假设你要发送一个信息80739。你把这个数字乘以3，并如图中所示忽略掉所有进位，得到的结果是40197。如果你把这个加密后的信息发送给我，我就可以用你的公有密钥来对它解密。当然，任何人知道你的公有密钥都可以对该信息解密。但是，我们必须知道这个信息一定是你发出的，因为只有你才可以用你的私有密钥对该信息进行加密。

RSA算法则更加复杂一些，所以只看一个较简单的RSA版本。RSA用一对素数来产生它的私有密钥和公有密钥。图27-8举例说明密钥的一种计算方法，然后又给出了一个对信息进行加密和解密的应用示例。首先来看一下密钥是如何计算出来的。

计算密钥的基本规则

选两个素数记作p和q。
算出它们的乘积记作n。
算出$p-1$和$q-1$的乘积记作s。
选一个不能被s整除的数记作e。
选一整数，使得下面的除法结果为整数，并记作d

$$((e)(d)-1)/s = \text{an integer}$$

现在用这个公式对每个数字进行加密：

$$C_i = M_i^{\,e} \bmod n$$

M_i是要加密的数字，C_i是加密后的数字

用这个公式进行解密：

$$M_i = C_i^{\,d} \bmod n$$

私有密钥是n和e，公有密钥是n和d

举例

$p = 5$ and $q = 3$
$n = 15$
$s = (4)(2) = 8$
$e = 11$
$d = 3$

$((3)(15) - 1) / 8 = 32 / 8 =$ an integer

3个数字的加密和解密

If M_i is 3, then 3^{11} is 177,147.
177,147 mod 15 is 12,
the remainder after dividing 177,147 by 15
Hence C_i is 12.
If C_i is 12, then 12^3 is 1728
and 1728 mod 15 is 3.
Hence M_i is 3.

加密的转换图

M_i	0	1	2	3	4	5	6	7	8	9
C_i	0	1	8	12	4	5	6	13	2	9

解密的转换图

C_i	0	1	2	4	5	6	8	9	12	13
M_i	0	1	8	4	5	6	2	9	3	7

图27-8 计算用于RSA中的公有密钥和私有密钥的方法

首先找出两个素数p和q，我们的示例中选择5和3。然后把它们的乘积记作n，这里n为15。然后由$p-1$和$q-1$的乘积得到s，例中s为8。再找一个不能整除s的素数，比如11，把它记作e。下一步，找到一个整数d使它满足$((e)(d)-1)/s$是一个整数，在本例中选择d的值是3。这样就得到两组密钥：(n, e)和(n, d)。可以选择n和e即15和11作为私有密钥，而选择n和d即15和3作为公有密钥。

加密所用的公式为：

$$C_i = M^e_i \bmod n \quad \text{或者} \quad C_i = M_i\ 11 \bmod 15$$

其中

M_i是明文的字符，C_i是密文的字符；解密所用的公式为：

$$M_i = C_i d \bmod n \text{或者 } M_i = C_i 3 \bmod 15$$

例如M_i是3，则加密后的C_i为12，也就是如果C_i是12，则M_i解密后为3。在图中给出了所有数字与加密后的数字的对应表。可以看到，其中有一些数字并没有被很好地加密，比如4、5、6和9在加密前后数字的值都是一样的。如果我们选择通过计算机得到非常大的素数用来产生密钥，那么这样的加密方法会好一些。

一个例子：上面介绍的所有方法都能用来发送信息，已达到安全传输的要求。通过一个例子看一下加密传输的工作过程。

假设我要发送一些数据给你。按照图27-9来介绍加密的过程。为简单起见，这个例子中使用前面介绍过的算法和密钥。我的私有密钥是（15，11），你的公有密钥是7，现在我要把信息8533安全地传送给你。

首先我必须随机产生一个SKC密钥，它将用来对会话进行加密。这里我们使用图27-6中所示的密钥，用5代替0，用2代替1，等等。由会话使用的密钥和要发送的数据，根据SKC算法就能得到加密后的数据6344，将这个数字发送给你。

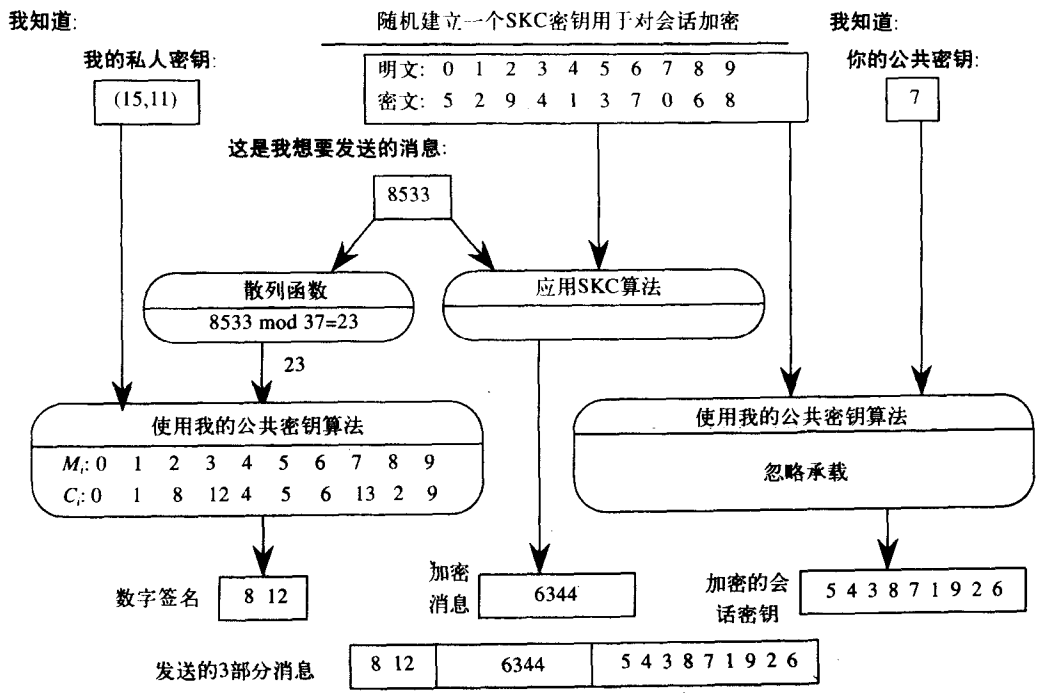


图27-9　怎样运用三种加密方法使信息安全传输的一个例子

下一步，我要发送的信息用散列法进行处理，结果为23。这样当你收到这个信息的时候，就能确认在传输过程中是否有人修改了数据。然后我使用私有密钥（15，11），对散列法处理的结果用公共密钥算法加密，这样就得到（8，12），它也被称作**数字签名**。对散列法处理的结果用公共密钥算法加密可以让你知道这些散列值是我发送的，而不是别人发送的。

现在，除非我把随机产生的那个用于会话加密的密钥也发给你，否则你就无法对信息进行解密。我会把公有密钥7发送给你，并用这个公有密钥对会话中使用的密钥(SKC密钥)进行加密。5乘7得35，忽略3发给你5。2乘7得14，忽略1发给你4，如此类推，这样就得到了加密后的会话密钥。由于只有你知道这个私有密钥，所以也只有你才能对会话进行解密。上面提到的这三个部分都会发送给你。

你接收到数据后可以把这三个部分彼此分开。如图27-10中所示，你知道我的公有密钥和你的私有密钥。首先，你要用你的私有密钥3来对会话中使用的密钥进行解密，如图所示的5、2、9等等。这些可以让你确认这个信息是发送给你的。通过这个会话使用的密钥，你现在可以把信息解密，从信息6344得到8533。但是现在，你仍需要确认在传输过程中没有其他人修改这个信息，并且这个信息确实是由我发送的。

为了确认这两件事情，你必须先将解密的信息通过散列法得到23。然后你需要用我的公有密钥及其算法来得到相应的签名。最后你还要检测你收到的数据流中的签名和你计算出的签名是否一样。如果签名一样，那么你就可以确定我的信息在传输过程中是安全的。但是如果它们不一样，那么就说明信息的传输过程是不安全的。

当然，所有这些过程是在用户不知道的情况下执行的。如果使用一个浏览器，则这些工作过程已经被嵌入到浏览器中。另外，使用哪一种私有密钥、公有密钥和散列算法必须在传送信息之前确定。在数据传输中包括很多的冗余数据，所以要先对数据进行压缩，然后再加密。

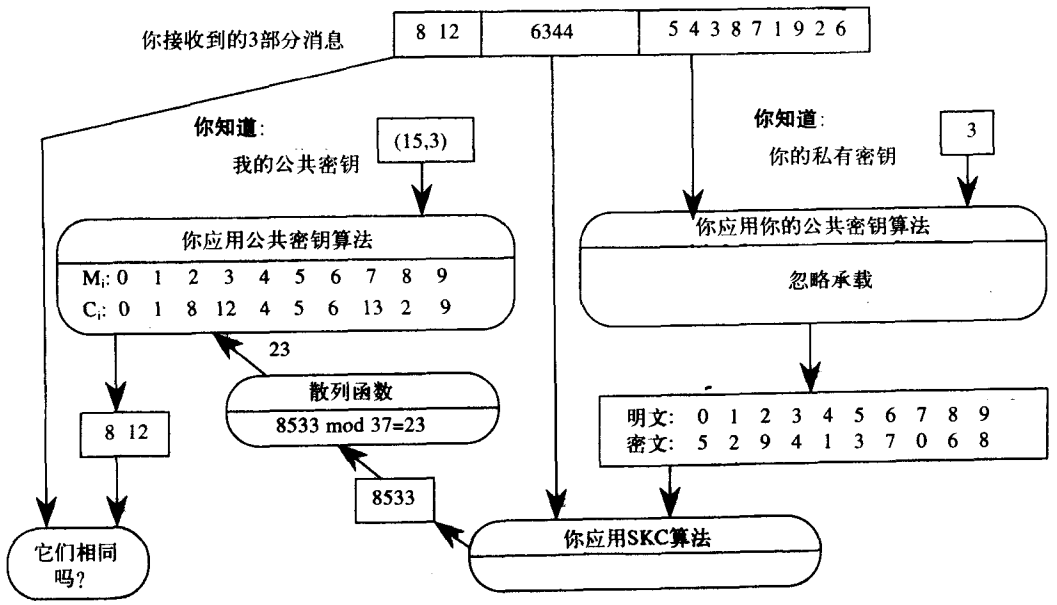


图27-10 图27-9中发送数据的解密过程

27.3.3 证书

公有密钥是通过非安全的电子邮件或者通过某个网站随意分配的。现在设想一个人需要和其他公司的外联网络进行安全的通信：这个人将需要不同公司各自对应的公有密钥。如果他只和少量的公司进行通信，那么他只需保存少量的公有密钥。但是随着所需安全通信的公司数量的增加，则所要保存的公有密钥的数量将变得越来越多。这时，就需要一个更好的方法，在不用保存大量公有密钥的情况下，能够安全地与大量的公司进行通信。

公有密钥认证让我们可以做到这一点。在这种方式中，如果某个人宣布某个公有密钥是属于他的，那么这个公有密钥就分配给他使用。这种方式还能够让我们确认公有密钥是否到期或者被取消。它还能够让我们得到可靠的公有密钥。

证书提供了一种确认一个人或者实体（如商业实体）的方法。在证书中可以表明发出证书的用户、证书的期限、序列号码和使用该证书的区域等信息。信用卡、驾驶执照和护照都是证书应用的例子（它们的类型与我们这里所讨论的不同），这些都可用来确定持有者的身份。这些人证书上都有一个唯一的序列号、有效的使用期限以及应用范围的相关信息。例如，信用卡可以确定这张卡的信用度是多少，驾驶执照规定持有人是否允许驾驶、驾驶何种车辆并且驾车时是否需要配戴眼镜等。

任何人都可以颁发证书，而证书信息的可靠性则取决于所颁发证书的权威性。比如作为身份的证明，由美国联邦政府所颁发的护照的可信度就要比信用卡或由杂货店发放的消费卡的可信度高得多。

数字证书（digital certificate）的特性在ITU-T的X.509标准中作了规定。它所包括的条目和我们通常所提到的证书所包括的内容差不多。比如，它也包括有效期限、颁发者的名称、公有密钥、持有该证书实体的名称及其公有密钥。另外，它还包括这个证书的用途和它的级别。证书通常分为四个等级，表明了在身份得到确认之前，你需要接受多少次检查来验证你

的身份。可以把由杂货店发放的证书的等级视1，而护照的等级定为4。

证书权威(CA，Certificate Authority)是指一个证书的颁发者。一个CA的可信度取决于证书发布的策略和所颁发的证书的等级。一个CA必须能够颁发和取消证书所用的密钥，必须能够使用相应的策略来验证和注册一个用户的身份，还必须能够提供一系列序列号来确定哪些用户是非法的。

医院可以给它的病人发放证书，学校可以给学生们发放证书。还有一些公司比如美国邮政局、VeriSign、GTE CyberTrust等等，他们专门发放各种证书，这是因为他们所发放的证书和他们的经验值得信赖。

你可以去这些公司的网站查看一下他们的证书展示。比如，在Netscape Communicator 4.7中，按照下面的操作就会看到你当前浏览器所使用的证书机制：Tools→Security Information→Signers。然后选择一个证书并点击Edit，你就可以看到十六进制的公有密钥。

证书链能够让一个实体或组织自己进行安全性验证。假设你想在Prentice Hall网站上使用你的信用卡来订购商品。但是你怎么知道连接的另一端确实是Prentice Hall而不是其他别的网站？你不用保存所有零售商的公有密钥，通过证书链你就可以完成上述的确认任务。

我们就用一个例子来看看这些任务是怎么完成的。已经提到了所有的浏览器都装有根CA的公有密钥，这些根CA是PKI（Public Key Infrastructure，公共密钥体系结构）所信任的，并且是可以为其他的公司或组织。提供担保的CA浏览器中来自根CA的证书，如图27-11第一步所示。

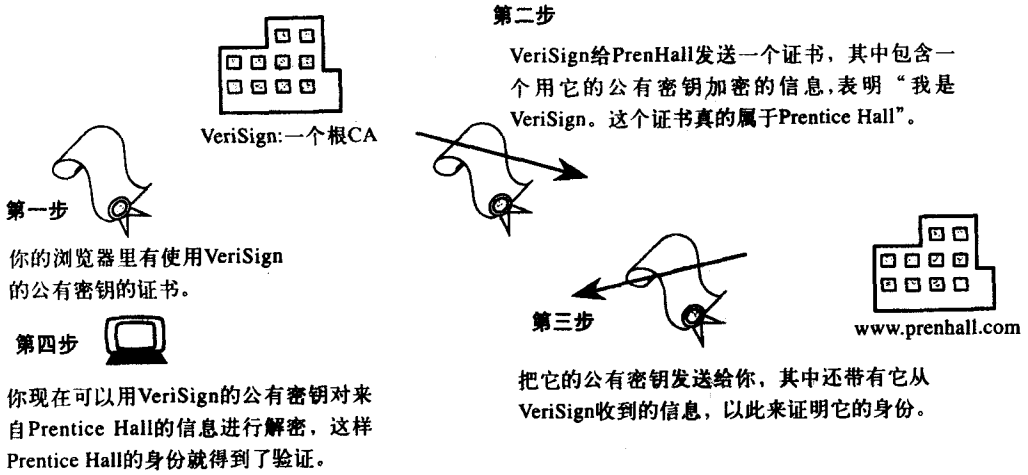


图27-11　在证书链中，通过一个根CA来证明其他组织的身份

在你发送信用卡的卡号给Prentice Hall之前，你希望先确认Prentice Hall的真实身份。（你并不关心零售商是否确认了你的身份。）如图的第二步所示，假设一个根CA是VeriSign，VeriSign把信息用它的私有密钥加密后发送给Prentice Hall。这个信息基本上校验了Prentice Hall的身份。

然后Prentice Hall会发给你一个证书和它的公有密钥，其中包括VeriSign发出的那个信息，如图第三步所示。因为在你的浏览器中存有VeriSign的公有密钥，通过这个公有密钥你可以对收到的那个信息进行解密，这样一来你就可以验证他是否真是Prentice Hall了，如图第四步所示。

如果你不信任VeriSign，就可以到浏览器中关掉VeriSign的条目，这样对来自Prentice Hall的证书验证就不再使用VeriSign而是通过其他的根CA进行。现在Prentice Hall发给你的证书中

包含有来自多个根CA的信息。现在你就可以准备发送你的信用卡卡号了。这时会出现一个警告提示对话框。你将注意到你运行的https（不是http）端口是443（不是80），这用的是SSL（Secure Sockets Layer，加密套接层）。注意VeriSign只能证明你的通信会话的另一端的确是Prentice Hall，但它并不能证明Prentice Hall本身是否值得信任。在你发送信用卡卡号时，你自己必须对它的可信度作出判断。

27.4 IP安全协议（IPSec）

可以在RFC 2401中看到关于IPSec的描述。在写作本书之时，实际应用中存在许多虚拟专用网的协议。但是，这里将主要讨论IP安全协议（IPSec，IP Security protocol）。IP安全协议的观点是在IP协议本身建立安全体系，而不是在每个网络应用中建立安全体系。由于所有的数据流传输都要使用IP协议，这样IPSec就可以保证整个因特网上通信的安全性。通过确保IP协议的安全性，从而得到整个因特网的安全性。

IP安全协议的一个突出优点是作为一种体系结构它并没有规定具体的实现方法。IP安全协议的实现方式取决于不同应用的各自需求，因此IP安全协议是十分灵活的。当出现新的安全技术的时候，可以轻易地把它应用于IP安全协议的实现中。另外，IP安全协议与将被广泛使用的IPv6协议相互兼容。

IP安全协议包括三个部分，包括AH（Authenticated Header，鉴权字头，或称头校验）、ESP（Encapsulation Security Payload，封装安全有效负荷）和IKE（Internet Key Exchange，因特网密钥交换）。头校验和封装安全有效负荷协议增加了IP包的头部。

校验是用来确认身份的，头校验的作用就是这样，并且它还可以确保传送的数据不被别人修改。对于多数应用来说这样的安全级别已经足够了，但是对于那些要使用不规则数据来进行加密的应用来说，就要用封装安全有效负荷来代替头校验。封装安全有效负荷实现了头校验不能实现的安全性，提高了安全的等级。头校验使用的是应用MD5(RFC 2403)或SHA1（RFC 2404）的HMAC，而封装安全有效负荷使用了相同的协议并且采用DESCBC（RFC 2405）来进行加密。

因特网密钥交换是一个灵活的安全策略协商协议。它允许对给定的通信会话选择验证、加密和散列的方法，另外它也提供了安全通信所需的其他参数。

如图27-12所示，ESP既可以用于传输模式，也可以用于隧道模式。在传输模式中，ESP的头部信息加在IP和TCP头部之间，如图27-13a所示。在数据报的结尾也加入了ESP的尾部。除IP头外，整个数据分组均要进行验证。TCP头部、数据和ESP的尾部字段都是加密的。

在隧道模式中，如图27-12b所示，整个IP数据包被看作一个整体，在它的前后分别加入了ESP的头部和尾部。同时新加入一个IP头部，里面包括安全网关的IP地址等信息。这样一来，如果有黑客在网络里截获了这个数据包，他也只能发现网关的IP地址和数据包目的端的信息。所有从ESP头部到ESP尾部的字段都被验证，从原IP头部到结尾的数据都被加密了。

图27-13简单介绍了IKE（Internet Key Exchange，因特网密钥交换）的工作过程。图中的两个路由器是某种安全网关，它们通过密钥或证书建立起一个安全通道。它们可以用主要模式和主动模式之一来做到这些。主要模式更为安全，主动模式更为快捷。一个连接可以从主要模式开始，然后进入主动模式。

在安全网关之间建立安全隧道之后，终端主机可以相互协商使用哪种加密、签名和散列的方法，就如图27-13中的第二阶段所示。

加密套接层：使用加密套接字协议层（SSL，Secure Sockets Layer）是Internet上保证应

用安全的另一种方法。这是一种处于应用和TCP协议之间的协议。对TCP来说，它就像是一个应用。比如它的端口号是443，它在浏览器的地址栏中的名字是https。加密套接字协议层在安全连接的客户端和服务器端都可以实现。它可以被应用于http、telent、ftp等应用中。

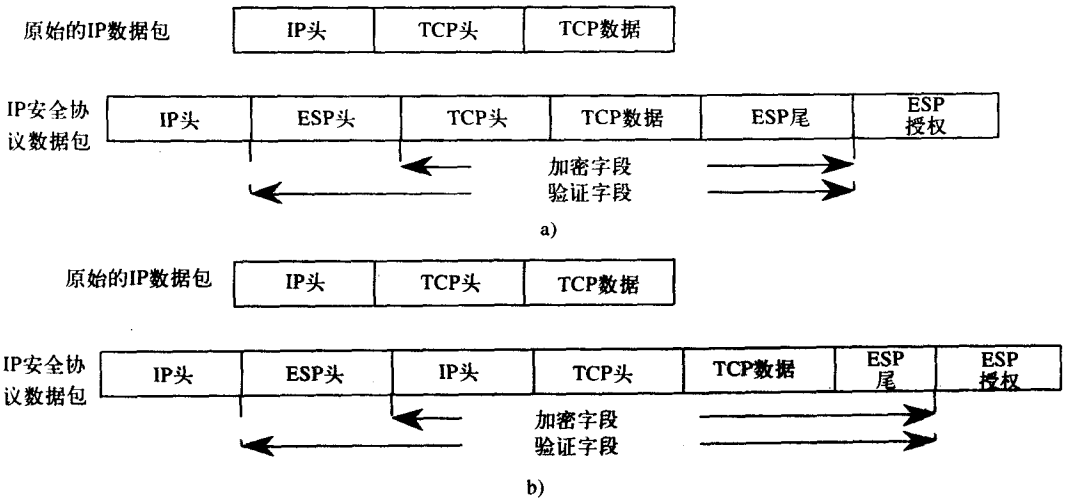


图27-12　a) 封装安全负荷应用在传输模式中；b) 封装安全负荷应用在隧道模式中

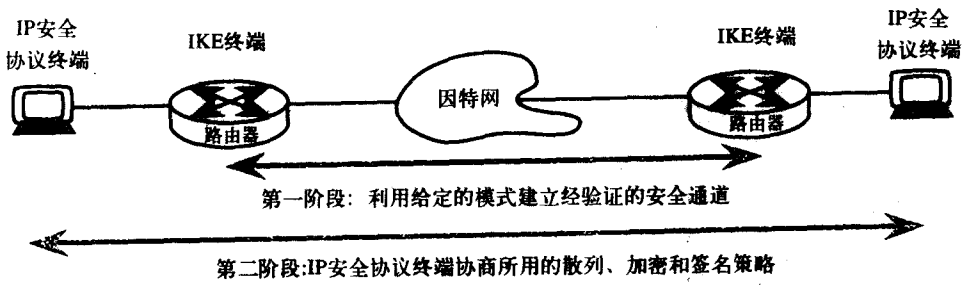


图27-13　IKE通过两个阶段来交换密钥和协商相关协议

加密套接字协议层使用加密套接字协议层握手协议来初始一个会话，用加密套接字协议层记录协议来传输数据。它保证在服务器和客户端之间进行数据的保密性和完整性传输。在银行业事务中，一个从加密套接字协议层扩展演变的方法SGC（Server Gated Cryptography，服务器门控加密）采用128位的密钥进行加密。

习题

27.1节

1. 在公共网络上建立的专用网络被称作什么？
2. 用TCP/IP设备建立的专用网络被称作什么？
3. 当一个组织通过Internet接入到另一个组织的内部网络时，这个专用网络可被看作哪一种类型的网络？
4. 哪一种类型的第三层虚拟专用网被认为是更为安全的？为什么？这类虚拟专用网的局限性是什么？

5. 第二层的虚拟专用网被认为比第三层的虚拟专用网络更安全吗？为什么？这类虚拟专用网络的优点是什么？
6. 在哪一种第一层的虚拟专用网中对整个路径进行加密？这类虚拟专用网对在一定地理区域中的用户适合吗？为什么？

27.2节

7. 给出建立虚拟专用网的理由。
8. 列出建立虚拟专用网时所要考虑的问题以及解决这些问题的方法。

27.3节

下面给出了五个问题，从下列选项中为每个题选择正确的安全方案。

a. 验证 b. 接入次数 c. 完整性 d. 机密性 e. 不可否认 f. 授权

9. 哪一种方法能找出传输丢失？
10. 哪一种方法能够确定在另一端是否可以获得公司的许可下订单？
11. 哪一种方法能够使传输的数据不会被分割？
12. 哪一种方法能够证明对方的身份？
13. 哪一种方法可以提供身份证明和信息内容？

下面给了出七个问题，根据所描述的加密方式，在下面的选项中进行选择。

a. 散列法 b.SKC c. PKC

14. DES和三重DES是哪一类安全性的例子？
15. RSA是用于哪一类安全性的常用算法？
16. MD（信息摘要）和SHA（安全散列算法）是哪一种方法的例子？
17. 哪一方法可用于提供数据的完整性？
18. 不管源文本的长度为多少，哪一种加密方法总是能得到相同长度的结果？
19. 哪种加密方法使用时需要交换密钥？
20. 哪一种方法是对称加密方法？
21. 用图27-7所示的忽略进位加密法，如果明文为3859，换算出密文。
22. 用图27-8所示相同的密钥和算法，如果明文为5091，构造被传输的加密信息的三个部分的内容。
23. 用图27-8所示的方法，对上面一题得到的信息进行解码。
24. 重新整理图27-8中的图表，使有效性不是采用数字签名来验证，而是采用散列值来验证。
25. 采用较长密钥的优缺点是什么？
26. 不断加快计算机的运行速度的缺点是什么？
27. 证书能够证明一个组织的哪些方面？不能证明什么？
28. 描述如何使用证书。
29. 在你的浏览器中，哪一类CA有最大的证书号？

27.4节

30. 说出IPSec协议的三个主要内容以及它们的用途。
31. 说出IPSce协议的两个优点。
32. Internet密钥交换的两个阶段是什么？
33. 与在传输模式中运行相比，在隧道模式中运行ESP有什么好处？
34. 尽管在1998年就发现了SSL中的问题，与IPSec相比，它采用了什么样的方法来提供安全性？

缩略语表

2B1Q	2 Binary, 1 Quaternary	二进制四电平（编码）
4WTS	4-Wire Terminal Set	4线终端设备
AA	Automated Attendant	自动值机员
AAL	ATM Adaptation Layer	ATM适配层
AAR	Automatic Alternate Routing	自动交替路由
Abis	BSC-BTS Interface	BSC-BTS的接口
AC	Alternating Current	交流电
AC	Authentication Center(wireless)	鉴权中心（无线）
ACD	Automatic Call Distributor	自动呼叫分配器
ACK	ACKnowledgement	确认
ACM	Address Complete Message	寻址完成消息
ACP	Action Control Point	行为控制点
ACS	Automatic Call Sequencer	自动呼叫序列发生器
ADM	Add-and-Drop Mux	添加与提取多路复用器
ADPCM	Adaptive Differential PCM	自适应差分脉冲信号编码调制
ADSL	Asymmetric DSL	非对称数字用户线
AESA	ATM End Station Address	ATM终端站地址
AFT	Analog Facility Terminal	模拟介质终端
AH	Authentication Header	鉴权字头
AIN	Advanced Intelligent Network	先进智能网络
AMI	Alternate Mark Inversion	符号交替反转码
AMPS	Advanced Mobile Phone Service	高级移动电话业务
ANI	Automatic Number Identification	自动号码识别（系统）
ANSI	American National Standards Institue	美国国家标准化组织
AP	Adjunct Processor(MCI)	附属处理器（MCI）
AP	Action Point(SDN)	行为点（SDN）
API	Application Program Interface	应用程序接口
APPC	Advanced Program-to-Program Communications	高级程序到程序通信协议
APPN	Advanced Peer-to-Peer Networking	高级对等联网技术
APS	Automatic Protection Switching	自动保护交换
ARIN	American Registry for Internet Numbers	美国因特网编号登记处
ARP	Address Resolution Protocol	地址解析协议

（续）

ARPANET	Advanced Research Projects Agency NETwork	美国国防部高级研究计划局建立的计算机网——ARPA网
ARS	Automatic Route Selection	自动路由选择
AS	Autonomous System	自治系统
ASCII	American Standard Code for Information Interchange	美国标准信息交换码
ASIC	Application-Specific Integrated Circuit	专用集成电路
ASR	Automated Speech Recognition	自动语音识别
AT&T	American Telephone & Telegraph Co.	美国电话电报公司
ATM	Asynchronous Transfer Mode	异步传输模式
ATP	Application Transaction Program	应用事务处理程序
ATU-C	ASDL Terminal Unit - CO	ASDL局端单元-CO
ATU-R	ASDL Terminal Unit - Remote	ASDL用户端单元-Remote
AUI	Attachment Unit Interface	附属单元接口
AWG	American Wire Guage	美国电缆标准
B8ZG	Binary 8-Zero Suppression	二进制8零替换
BBN	Bolt, Beranek, and Newman	波特，柏拉尼克与纽曼
BCM	Bit Compression Mux	比特压缩多路复用器
BECN	Backward Explicit Congestion Notification	后向显式拥塞指示
Bellcore	BELL Communications REsearch	贝尔通信研究中心
BGP	Border Gateway Protocol	边界网关协议
BIB	Backward Indicator Bit	反向指示位
B-ICI	Broadband Inter-Carrier Interface	宽带运营商间的接口
BIND	Berkeley Internet Name Domain	伯克利因特网命名域
BIOS	Basic Input/Output System	基本输入/输出系统
BISDN	Broadband ISDN	宽带ISDN
BIU	Basic Information Unit	基本信息单元
BLSR	Bidirectional Lines Switched Ring	双向线路交换环
BLU	Basic Link Unit	基本链路单元
BOC	Bell Operation Company	贝尔运营公司
BPV	BiPolar Violation	双极性扰乱
BRI	Basic Rate Interface (2B+D)	基本速率接口(2B+D)
BS	Base Station	基站
BSC	BS Controller	基站控制器
BSC	Binary Synchronous Communications	二进制同步通信
BSN	Backward Sequence Number	反向序列号

（续）

BT	British Telecom	英国电信公司
BTA	Basic Trading Area	基本贸易区
BTS	Base Transceiver Station	基站收发台
BTU	Basic Transmission Unit	基本传输单元
C/I	Carrier-to-Interference ratio	载波干扰比（载干比）
CA	Certificate Authority	认证权威
CAD	Computer-Aided Design	计算机辅助设计
CAP	Competitive Access Providers	竞争接入提供商
CAP-QAM	Carrierless Amplitude/Phase and Quadrature Amplitude Modulation	无载波幅度/相位正交幅度调制
CAS	Centralized Attendant Service(PBX)	集中式接线员服务
CAS	Channel-Associated Signaling	随路信令
CAT-5	CATegory 5 cabling	5类电缆
CATV	Cable TeleVision	有线电视系统
CBR	Constant Bit Rate	恒定比特率
CCIR	International Radio Consultative Committee	国际无线电咨询委员会
CCIS	Common Channel Interoffice Signaling	公共信道局间信令
CCITT	Comité Consultatif Internationale de Telegraphiqué et Telephoniqué	国际电报电话咨询委员会
CCK	Complementary Code Keying	补码键控
CCR	Customer-Controlled Reconfiguration	客户控制下的重新配置
CCS7	Common Channel Signaling 7	7号公共信道信令
CD	Compact Disc	压缩光盘
CDMA	Code Division Multiple Access	码分多址接入
CDPD	Cellular Digital Packet Data	蜂窝数字分组数据
CDR	Call Detail Recording	呼叫详细记录
CEPT	Conference on European Posts & Telecommunications	欧洲邮政和通信管理委员会
CIC	Circuit Identification Code	电路标识码
CICS	Customer Information Control System	用户信息控制系统
CID	Component IDentifier	组件标识符
CIDR	Classless InterDomain Routing	无类别域间路由
CIR	Committed Information Rate	承诺的信息速率
CISC	Complex Instruction Set Computing	复杂指令集计算
CLASS	Custom Local Area Signaling Services	定制本地区域信令服务
CLEC	Competitive Local Exchange Carrier	争用本地交换运营商
CLNP	ConnectionLess Network Protocol	无连接网络协议

（续）

CLNS	ConnectionLess Network Service	无连接网络服务
CLP	Cell Loss Priority	信源丢失优先级
CM	Configuration Management	配置管理
CMA	Communications Managers Association	通信管理协会
CMB	Credit Manager Association	信用卡管理协会
CMC	Communications Management Center	通信管理中心
CMOS	Channelized Metal Oxide Semiconductor	沟道型金属氧化半导体
CNAR	Customer Network Administration Report	用户网络管理报告
CNI	Common Network Interface	公共网络接口
CNOS	Change Number Of Services	改变服务数量
CO	Central Office	中心局
Codec	Coder-Decoder	编解码器
COS	Class Of Service	服务类型
CP	Cable Pair number	电缆对号码
CPCS	Common Port Convergence Sublayer	公共端口会聚子层
CPE	Customer Premises Equipment	用户端设备
CPI	Computer-PBX Interface	计算机到PBX间的接口
CPI	Common Programming Interface	通用编程接口
CPU	Central Processor Unit	中央处理单元
CRC	Cyclic Redundancy Check	循环冗余校验
CS	Convergence Sublayer	会聚子层
CSL	Component SubLayer	组件子层
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance	带冲突避让的载波侦听多址接入
CSMA/CD	CSMA with Collision Detection	带冲突检测的CSMA
CSMA/CR	CSMA with Collision Resolution	带冲突分辨的C S M A
CSS	Center-Stage Switch	中级交换机
CSU	Channel Service Unit	信道服务单元
CTDR	Customer Traffic Data Report	用户业务数据报告
CTI	Computer Telephony Integration	计算机电话集成
DA	Destination Address	目的地址
DAC	Dual Attached Concentrator	双附件集中器
DACS	Digital Access and Cross-connect System	数字接入和交叉连接系统
DAL	Dedicated Access Line	专用接入线
DAP	Data Access Point	数据接入点
DARPA	Defense Advanced Research Projects Agency	美国国防部高级研究计划规划局

（续）

DAS	Dual Attached Station	双附件站点
DATTS	Direct Access Trunk Test System	直接接入干线实验系统
dB	Decibel	分贝
DC	Direct Current	直流电
DCE	Data Communications Equipment	数据通信设备
DCP	Data Communications Protocol	数据通信协议
DCR	Dynamic Controlled Routing	动态控制路由
DCS	Distributed Communications System	分布式通信系统
DCS	Digital Crossconnect System (or DACS)	数字交叉连接系统（或DACS）
DDD	Direct Distance Dialing	长途直拨业务
DDN	Digital Data Network	数字数据网
DDN	Defense Data Network	美国国防部数据网络
DDS	Digital Data Service	数字数据业务
DDS	Dataphone Digital Services	数据电话数字业务
DE	Data Eligibility bit	数据合格比特
DEC	Digital Equipment corporation	美国数字设备公司
DECT	Digital European Cordless Telecommunications	欧洲数字无绳电话标准
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DIA	Document Interchange Architecture	文件交换体系结构
DID	Direct Inward Dialing	直接拨入电话
DINA	Distributed Intelligent Network Architecture	分布式智能网络体系结构
DIP	Dual In-line Package switch	双列直插开关
DISA	Direct Inward System Access	直接拨入系统接入
DISC	DISConnect	断开连接
DLC	Digital Line Carrier	数字链路载波
DLCI	Data Link Control Identifier	数据链路控制标识符
DLL	Dynamic Link Library	动态链路库
DLSw	Data Link Switching	数据链路交换
DM	Disconnect Mode	断开模式
DMI	Digital Multiplexed Interface	数字复用接口
DMT	Discrete Multitone Transmission	离散多音调传输
DNHR	Dynamic NonHierachical Routing	动态非分级路由
DNIC	Data Network Identification Code	数据网络标识码
DNIS	Dialed Number Identification Service	被拨号码识别业务
DNS	Domain Name Service	域名服务
DoD	Department of Defense	美国国防部
DOD	Direct Outward Dialing	直接拨出电话

（续）

DOS	Disk Operating System	磁盘操作系统
DOV	Data Over Voice	在语音线路上传输数据
DPC	Destination Point Code	目的节点代码
DQDB	Distributed Queue Dual Bus	分布式队列双总线（标准）
DR	Designated Router	指定路由器
DS-0	Digital Signal, level 0	数字信号，级别0
DS-1	Digital Signal, level 1	数字信号，级别1
DSAP	Destination SAP	目标SAP
DSL	Digital Subscriber Line	数字用户线
DSLAM	Digital Subscriber Line Access Module	数字用户线接入模块
DSP	Digital Signal Processing	数字信号处理
DSSS	Direct Sequence Spread Spectrum	直接序列扩频
DSU	Digital Service Unit	数字业务单元
DSX-1	Digital System cross-connect 1	数字系统交叉连接1
DTE	Data Terminal Equipment	数据终端设备
DTMF	Dual Tone MultiFrequency	双音多频
DTW	Dynamic Time Warping	动态时间偏移
DVCC	Digital Verification Color Code	数字验证色码
DWDM	Dense Wave Division Multiplexing	密集波分多路复用
E&M	Ear and Mouth signaling	接收和发送信令，听说信令
EA	Extension Address	扩展地址
EAMPS	Extended AMPS	扩展AMPS
ECS	Enterprise Communications Server	企业通信业务
EFCI	Explicit Forward Congestion Indicator	显式转发拥塞指示
EGP	Exterior Gateway Protocol	外部网关协议
EIA	Electronics Industries Association	美国电子工业协会
EKS	Electronic Key System	电子按键系统
EMI	ElectroMagnetic Interference	电磁干扰
EMS	Element Management System	网元管理系统
EN	End Node	终端节点
EO	End Office	端局
EPN	Expansion Port Network	扩展端口网络
ES	End System	终端系统
ESF	Extended Super Frame	扩展超帧
ESN	Electronic Serial Number	电子序列号
ESP	Encapsulation Security Payload	封装的安全净荷
ESS	Electronic Switching System	电子交换系统
ETN	Electronic Tandem Network	电子级联网络

（续）

FACCH	Fast Associated Control CHannel	快速辅助控制信道
FCC	Federal Communications Commission	美国联邦通信委员会
FCS	Frame Check Sequence	帧校验序列
FDDI	Fiber-Distributed Data Interface	光纤分布式数据接口（网）
FDL	Facility Data Link	设备数据链路
FDM	Frequency Division Multiplex	频分多路复用
FDMA	Frequency Division Multiple Access	频分多址接入
FDX	Full DupleX	全双工
FEC	Forward Error Correction	前向纠错
FECN	Forward Explicit Congestion Notification	向前拥塞指示
FEP	Front End Processor	前端处理器
FIB	Forward Indicator Bit	向前指示比特
FID	Format ID	格式标识符
FISU	Fill-In Signal Unit	填充信令单元
FLP	Fast Link Pulse	快速链路脉冲
FMH	Function Management Header	功能管理头
FOIRL	Fiber Optic InterRepeater Link	光纤中继器间链路
FOT	Fiber Optic Terminal	光端机
FR	Frame Relay	帧中继
FRAD	Frame Relay Assembler/Disassembler	帧中继装配/拆卸设备
FRF	Frame Relay Forum	帧中继论坛
FRL	Facility Restriction Level	设备限制级别
FRMR	FRaMe Reject	帧拒绝
FSN	Forward Sequence Number	向前序列号
FT1	Fractional T1	部分T1
FTP	File Transfer Protocol	文件传输协议
FX	Foreign eXchange	外部交换
FXO	Foreign eXchange, Office	外部交换局
FXS	Foreign eXchange, Subscriber	外部交换用户
GDS	Generalized Data Stream	广义数据流
GE	Gigabit Ethernet	千兆以太网
GFC	Generic Flow Control	一般流量控制
GFI	General Format Identifier	通用格式标识符
GMMI	Gigabit MMI	千兆MMI
GMSC	Gateway Mobile Switching Controller	网关移动交换控制器
GPS	Global Positioning System	全球定位系统
GSM	Global System for Mobile communications	全球移动通信系统

（续）

GUI	Graphical User Interface	图形用户接口
HDLC	High-level Data Link Control	高级数据链路控制规程
HDSL	High-speed Digital Subscriber Line	高速数字用户线路
HEC	Header Error Correction	信头差错控制
HEHO	Head-End Hop-Off	首端点跳转
HIVR	Host-Interactive Voice Response	主机交互语音回应
HLR	Home Location Register	归属位置寄存器
HMDF	Horizontal Main Distribution Frame	总配线架横向侧
HMM	Hidden Markov Modeling	隐式马尔科夫模型
HPAD	Host Packet Assembler/Disassembler	总配线架横向侧
HTML	HyperText Markup Language	超文本标准语言
HTTP	HyperText Transfer Protocol	超文本传输协议
I/G	Individual/Group bit	独立/组比特
I/O	Input/Output	输入/输出
IANA	Internet Assigned Numbers Authority	因特网编号分配权威机构
IBM	International Business Machines Corp.	国际商用机器公司
ICMP	Internet Control Message Protocol	因特网控制报文协议
IDDD	International DDD	国际DDD
IDF	Intermediate Distribution Frame	中间配线架
IDSL	ISDN DSL	ISDN 数据用户线
IEC	InterExchange Carrier	局间电话公司或局间通信公司
IEEE	Institute of Electrical and Electronics Engineers	电气与电子工程师协会
IETF	Internet Research Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	因特网分组管理协议
IGP	Interior Gateway Protocol	内部网关协议
IKE	Internet Key Exchange	因特网密钥交换
ILEC	Incumbent Local Exchange Carrier	在职本地交换运营商
ILMI	Integrated Link Management Interface	集成链路管理接口
IMS	Information Management System	信息管理系统
IMT	InterMachine Trunk	机器间的中继线
IMTS	Improved Mobile Telephone Service	改进的移动电话业务
IMUX	Inverse MUltipleXer	反向多路复用器
INMS	Integrated Network Management Systems	集成网络管理系统
INSITE	Integrated Network System Interface and Terminal Equipment	集成网络系统接口和终端设备
IP	Internet Protocol	网际互连协议
IPsec	IP Security protocol	IP安全协议

（续）

IRTF	Internet Research Task Force	因特网研究任务组
IS	Intermediate System	中间系统
IS-IS	IS to IS protocol	IS到IS协议
ISDN	Integrated Services Digital Network	综合业务数字网
ISO	International Organization for Standardization	国际标准化组织
ISOC	Internet SOCiety	国际因特网协会
ISP	Internet Service Provider	因特网服务提供者
ISSI	Inter-Switching System Interface	内部交换系统接口
ISUP	ISdn User Part	ISDN用户部分
ITU	International Telecommunications Union	国际电信联盟
ITU-R	ITU Radio communication sector	国际电信联盟无线通信标准部
ITU-T	ITU Telecommunications standardization sector	国际电信联盟电信标准部
IVDT	Integrated Voice/Data Terminal	集成话音/数据终端
IVR	Interactive Voice Response	交互式语音响应
IXC	IEC	局间通信公司
JAIN	Java Api for Integrated Networks	集成网络的Java API
JTAPI	Java Telephony API	Java电话API
JES	Job Entry Subsystem	任务项目子系统
KSU	Key System Unit	密钥系统单元
LAN	Local Area Network	局域网
LAP/B	Link Access Procedure/Balanced	链路接入规程/均衡
LAPD	Link Access Procedures over the D Channel	D信道链路接入规程
LAPF	Link Access Procedure-Frames	链路接入规程-帧
LAT	Local Area Transport	局域传输（协议）
LATA	Local Access and Transport Area	本地接入和传送区
LCI	Logical Channel Identifier	逻辑信道标识符
LCP	Link Control Protocol	链路控制协议
LCR	Least-Cost Routing	最低费用路由
LE	Local Exchange	本地交换
LED	Light-Emitting Diode	发光二级管
LEN	Low-Entry Networking	低入口网络
LESA	Local Exchange Switched Access	本地交换切换接入
LILO	LInux LOader	Linux装载程序
LLC	Logical Link Control	逻辑链路控制
LMDS	Local Multipoint Distribution Services	本地多点分布式系统

（续）

LMI	Local Management Interface	本地管理接口
LMU	Line Monitor Unit	线路监控单元
LOA	LOcal Address	本地地址
LORAN-C	LOng RAnge Navigation-C	劳兰- C导航系统
LPC-RPE	Linear Predictive Encoding with Regular Pulse Excitation	带有规则脉冲激励的线性预测编码
LSA	Link State Advertisement	链路状态通告
LSB	Least Significant Bit	最低有效比特
LSSU	Link Status Signaling Unit	链路状态信令单元
LT	Local Termination	本地终端
LU	Logical Unit	逻辑单元
MAC	Media Access Control	媒体接入控制
MAN	Metropolitan Area Network	城域网
MAU	Media Access Unit (Ethernet)	媒体接入单元（以太网）
MAU	Multistation Access Unit (TRN)	多站点接入单元（TRN）
MCI	Microwave Communications Inc.	微波通信公司
MCR	Mapped Conversation Record	映射对话纪录
MDA	Mail Delivery Agent	邮件传递代理
MDF	Main Distribution Frame	主配线架
MF	MultiFrequency	多频
MFJ	Modified Final Judgment	最终修正法案
MFS	Metropolitan Fiber Systems	城际光纤系统
MFT	Metallic Facility Terminal	金属设备终端
MIC	Media Interface Connector	媒体接口连接器
MID	Message ID	消息ID
MMDS	Multipoint Multichannel Distribution Services	多点多信道分布式业务
MMF	MultiMode Fiber	多模光纤
MMI	Media-Independent Interface	与媒质无关的接口
MS	Mobile Station	移动台
MSB	Most Significant Bit	最高有效比特
MSC	Mobile Switching Center	移动交换中心
MSU	Message Signal Unit	消息信令单元
MTA	Mail Transfer Agent (SMTP)	邮件传递代理（SMTP）
MTA	Major Trading Area (wireless)	主要贸易区（无线）
MTP	Message Transfer Part	消息传输部分
MTS	Message Telecommunication Service	消息电信业务

（续）

MTSO	Mobile Telecommunications SwitchingOffice	移动电信交换局
MTTR	Mean Time To Repair	系统平均修复故障时间
MTU	Maximum Transfer Unit	最大传输单元
MUA	Mail User Agent	邮件用户代理
MUX	MUltipleXer	复用器
MVS	Multiple Virtual Systems	多虚拟系统
NACK	Negative ACKnowledgement	否定应答
NANPA	North American Numbering Plan Administration	北美号码计划管理局
NAT	Network Address Translation	网络地址转换
NAU	Network Addressable Unit	网络寻址单元
NAUN	Nearest Active Upstream Neighbor	最近有效上行邻居
NCP	Network Control Program (SNA)	网络控制程序(SNA)
NCP	Network Control Point (PSTN)	网络控制节点(PSTN)
NEMOS	NEtwork Management Operation Support System	网络管理操作支持系统
NetBIOS	Network BIOS	网络基本输入/输出系统
NETCAP	NETwork CAPabilities manager	网络容量管理器
NFS	Network File System	网络文件系统
NIC	Network Interface Card	网络接口卡
NID	Network Interface Device	网络接口设备
NIMS	Network Information Management Systems	网络信息管理系统
NIU	Network Interface Unit	网络接口单元
NLP	Normal Link Pulse	常规链路脉冲
NNI	Network-Network Interface	网络到网络接口
NNMC	National Network Management Center	国家网络管理中心
NOC	Network Operations Center	网络运行中心
NOS	Network Operating System	网络操作系统
NPSI	NCP Packet Switching Interface	NCP分组交换接口
NRA	Network Remote Access	网络远程接入
NRAMS	NRA Monitoring System	NRA监视系统
NRZI	Non-Return to Zero Inverted	非归零倒转
NSC	Network Service Complex	网络业务综合
NSF	National Science Foundation	国家科学基金
NT	Northern Telecom	(加拿大) 北方电信
NT1/2	Network Termination 1 and 2	网络终端1和2
NTI	Northern Telecom Inc.	北方电信公司

（续）

OAI	Open Architecture Interface	开放体系结构接口
OAM	Operations, Administrations, and Maintenance	操作、管理和维护
OC-1	Optical Carrier, level 1	光载波，级别1
OCU	Office Channel Unit	端局信道单元
OE	Office Equipment designation	局设备名称
OLTP	On-Line Transaction Processing	在线事务处理
OPC	Origination Point Code	源节点代码
OPX	Off-Premise Extension	建筑物外扩展
OSI	Open Systems Interconnection	开放系统互联
OSPF	Open Shortest Path First	开放最短路径优先(协议)
OSS	Operation Support System	操作支持系统
OUI	Organizational Unique Identifier	组织唯一标识符
OVSF	Orthogonal Variable Spreading Factor	正交可变扩频因子
PAD	Packet Assembler/Disassembler	分组组装/拆分
PAM	Pass-Along Message	传递消息
PAP	Public Access Profile	公众接入协议
PBX	Private Branch eXchange	用户交换机
PC	Personal Computer	个人计算机
PCM	Pulse Code Modulation	脉冲编码调制
PCS	Personal Communications System	个人通信系统
PDN	Public Data Network	公共数据网
PDU	Protocol Data Unit	协议数据单元
PHY	PHYsical layer protocol	物理层协议
PIU	Path Information Unit	路径信息单元
PKC	Public Key Cryptography	公共密钥加密
PKI	Public Key Infrastructure	公共密钥体系结构
PLCP	Physical Unit Control Point	物理单元控制点
PLU	Primary Logical Unit	主逻辑单元
PMD	Physical Medium Dependent	物理介质相关层协议
PN	Pseudorandom Noise	伪随机噪声
PNNI	Private Network-to-Network Interface	专用网络－网络接口
POP	Point of Presence	电话接入站点
POTS	Plain Old Telephone Service	一般电话业务
PPN	Processor Port Network	处理器端口网络
PPP	Point-to-Point Protocol	点到点协议
PPS	Packets Per Second	每秒分组数
PRI	Primary Rate Interface (23B or 30B+D)	主速率接口(2 2B或3 0B +D)

（续）

PSN	Packet Switched Network	分组交换网
PSTN	Public Switched Telephone Network	公共交换电话网
PT	Payload Type	净荷类型
PTT	Postal, Telephone, and Telegraph	邮电总局（邮政、电话和电报）
PU	Physical Unit	物理单元
PUC	Public Utility Commission	公用事业委员会
PVC	Permanent Virtual Circuit	永久虚电路
PVP	Permanent Virtual Path	永久虚通道
QCELP	Qualcomm Code Excited Linear Prediction	Qualcomm码本激励线性预测
QLLC	Qualified Logical Link Control	合格逻辑链路控制
QoS	Quality of Service	服务质量
RAM	Random Access Memory	随机存储器
RARP	Reverse Address Resolution Protocol	反向地址解析协议
RBOC	Regional BOC	区域性贝尔运营公司
RDPS	Reverse Direction Protection Switching	反向保护交换
RFC	Request For Comments	请求注释
RFI	Radio Frequency Interference	射频干扰
RH	Request/response Header	请求/响应头
RIF	Routing Information Field	路由信息字段
RIP	Routing Information Protocol	路由信息协议
RISC	Reduced Instruction Set Computing	精简指令集计算(技术)
RJ	Register Jack	寄存器插口
ROM	Read-Only Memory	只读存储器
RSA	Rivest, Shamir, and Aldeman	用人名Rivest、Shamir和Aldeman命名的RSA公共密钥系统
RSIP	Realm-Specific IP	特殊区域IP
RTNR	Real-Time Network Routing	实时网络路由
RU	Request/response Unit	请求/响应单元
SAAL	Signaling AAL	信令AAL
SABM	Set Asynchronous Balanced Mode	设置异步平衡模式
SABME	SABM Extended	扩展SABM
SAC	Serving Area Concept (PSTN)	服务区概念(PSTN)
SAC	Single Attached Concentrator (FDDI)	单附件集中器(FDDI)
SACCH	Slow Associated Control CHannel	慢速辅助控制信道
SAP	Service Access Point	业务接入点
SAPI	SAP Identifier	SAP标识符
SAR	Segmentation And Reassembly	分段与重装子层(ATM)

（续）

SAS	Single Attached Station	单附件站点
SBS	Satellite Business Systems	商业卫星系统
SC	Stick-and-Click fiber connector	光纤连接器
SCCP	Signaling Connection Control Part	信令连接控制部分
SCM	Service Control Manager	业务控制管理器
SCP	Service Control Point	业务控制节点
SCPMS	SCP Management System	S C P管理系统
SDDN	Software-Defined Data Network	由软件定义的数据网络
SDH	Synchronous Digital Hierarchy	同步数字系列
SDLC	Single-pair DSL	同步数据链路控制
SDN	Software-Defined Network	由软件定义的网络
SDNCC	SDN Control Center	S D N控制中心
SDSL	Single-pair DSL	单对D S L
SDU	Service Data Unit	业务数据单元
SEAL	Simple and Efficient Adaptation Layer	简单高效的适配层
SF	Single Frequency	单音频
SFD	Start Frame Delimiter	起始帧分隔符
SIO	Service Information Octet	业务信息字节
SIP	SMDS Interface Protocol	S M D S接口协议
SIVR	Speech-Independent Voice Recognition	不依赖语音的语音识别
SKC	Secret Key Cryptography	密码学
SLA	Service Level Agreement	服务等级协议
SLC-96	Subscriber Line Carrier	用户线路载波
SLS	Signaling Link Selection	信令链路选择
SLU	Secondary LU	辅助LU
SMDR	Station Message Detail Recording	站点消息详细记录
SMDS	Switched Multi-megabit Digital Service	交换式多兆位数字业务
SMF	Single-Mode Fiber	单模光纤
SMS	Service Management System	业务管理系统
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNA	Systems Network Architecture	系统网络体系结构
SNADS	SNA Distributed Services	S N A分布式业务
SNF	Segment Number Field	段号码字段
SNI	Subscriber Network Interface	用户网络接口
SNID	Smart NID	智能N I D
SNMP	Simple Network Management Protocol	简单网络管理协议
SOHO	Small Office/Home Office	家庭办公
SONET	Synchronous Optical NETwork	同步光网络

（续）

SP	Signaling Point	信令节点
SPARC	Scalable Processor ARChitecture	可升级处理器体系结构
SPC	Stored Program Control	存储程序控制
SPE	Synchronous Payload Envelope	同步净荷包络
SRDM	SubRate Data Multiplexing	低速数据复用
SRT	Source Route Transparent Bridge	源路由透明网桥
SS	SMDS Switching system	SMDS交换系统
SS7	Signaling System 7	7号信令系统
SSAP	Source SAP	源SAP，源业务接入点
SSCP	System Services Control Point	系统业务控制节点
SSCS	Service-Specific Convergence Sublayer	特殊业务会聚子层
SSL	Secure Sockets Layer	加密套接层
SSMA	Spread Spectrum Multiple Access	扩频多址接入
SSP	Signal Service Point	信令业务节点
ST	Stick-and-Twist fiber connector	Stick-and-Twist光纤连接器
STE	Signaling Terminal Equipment	信令终端设备
STM	Synchronous Transmission Mode	同步传输模式
STP	Signal Transfer Point (PSTN)	信令传输节点
STP	Shielded Twisted Pair (LANs)	隐蔽双绞线
STS	Synchronous Transport Signal	同步传输信令
SU	Signaling Unit	信令单元
SVC	Switched Virtual Circuit	交换虚电路
SVP	Switched Virtual Path	交换虚通道
TA	Terminal Adapter	终端适配器
TAPI	Telephony API	电话应用程序接口
TAT	TransATlantic cable	大西洋海底电缆
TCAP	Transaction Capabilities Application Part	事务处理应用部分
TCP	Transmission Control Protocol	传输控制协议
TDM	Time Division Multiplex	时分复用
TDMA	Time Division Multiple Access	时分多址接入
TE	Terminal Equipment (1 or 2)	终端设备（1或2）
TEHO	Tail-End Hop-Off	尾端点跳转
TEI	Terminal Endpoint Identifier	终端端点标识符
Telco	TELephone COmpany	电话公司
TFTP	Trivial File Transfer Protocol	琐碎文件传输协议
TG	Transmission Group	传输组
TH	Transmission Header	传输头
THT	Token Holding Timer	令牌持有定时器

（续）

TIA	Telecommunications Industries Association	电信工业协会
TIC	Token Ring Interface Card	令牌环接口卡
TID	Transaction IDentifier	事务处理标识符
TMPA	Tapi-to-tsapi MAPping	电话应用程序接口映射
TN	Terminal Number	终端号码
TP	Transaction Program	事务处理程序
TP	TeleProcessing	电信处理
TPAD	Terminal PAD	终端PAD
TPC	TransPaCific cable	太平洋海底电缆
TRN	Token Ring Network	令牌环网络
TSAPI	Telephony Services API	电话业务应用程序接口
TSL	Transaction SubLayer	事务处理子层
TSO	Time Sharing Option	时间共享选择
TSSI	Time Slot Sequence Integrity	时隙序列完整性
TTL	Time To Live	生存时间
TTRL	Target Token Rotation Time	目标令牌轮换时间
TTS	Text-To-Speech	文字语音转换
TVX	Valid Transmission Timer	有效传输定时器
U/L	Universal or Local	全局或本地
UA	Unnumbered Acknowledge	未标号确认
UCD	Uniform Call Distributor	统一呼叫分配器
UDP	User Datagram Protocol	用户数据报协议
UDSL	Universal aDSL	通用ADSL
UI	Unnumbered Information	未编号信息
ULSR	Unidirectional Line-Switched Ring	单向线路交换环
Um	Air Interface	空中接口
UN	United Nations	联合国
UNI	User-to-Network Interface	用户－网络接口
UNMA	Unified Network Management Architecture	统一网络管理体系结构
UTP	Unshielded Twisted Pair	未屏蔽双绞线
VAC	Volts AC (Alternating Current)	交流电压
VAN	Value-Added Network	增值业务网络
VBR	Variable Bit Rate	可变比特率
VC	Virtual Circuit	虚电路
VCI	Virtual Channel Identifier	虚通路标识符
VDC	Volts DC (Direct Current)	直流电压
VDSL	Very high DSL	超高速数字用户线
VFRAD	Voice-FRAD	话音帧中继接入设备

（续）

VINES	VIrtual NEtwork System	虚拟网络系统
VLAN	Virtual LAN	虚拟局域网
VLR	Visitor Location Register	访问位置寄存器
VLSI	Very Large Scale Integration	超大规模集成电路
VMDF	Vertical MDF	总配线架直列侧
VoFR	Voice over Frame Relay	帧中继上的话音业务
VoIP	Voice over IP	在IP网上传输语音
VPDS	Virtual Private Data Service	虚拟专用数据业务
VPI	Virtual Path Identifier	虚通道标识符
VPN	Virtual Private Network	虚拟专用网
VR	Voice Recognition	语音识别
VSAT	Very Small Aperture Terminal	甚小口径终端
VSELP	Vector Sum Excited Linear Prediction	矢量和激励线性预测
VT	Virtual Tributary	虚拟支路
VTAM	Virtual Telecommunications Access Method	虚拟电信接入方法
WAL	WATS Access Link	WATS接入线
WAN	Wide Area Network	广域网
WATS	Wide Area Telecommunications Service	广域电信业务
WDM	Wave Division Multiplexing	波分复用
WWW	World Wide Web	万维网
XID	eXchange IDentifier	交换标识符