

自考乐园<http://tieba.baidu.com/club/5346389>
自考学习交流、资料共享的好去处！自考人自己的家园。



全国高等教育自学考试指定教材 计算机及应用专业（独立本科段）

计算机网络原理

附：计算机网络原理自学考试大纲

课程代码
4741
[2007年版]

组编／全国高等教育自学考试指导委员会
主编／杨明福

本教材附赠网络学习卡

更多优质自考资料尽在百度贴吧自考乐园俱乐部
(<http://tieba.baidu.com/club/5346389>)
欢迎加入...欢迎交流...止不住的惊喜等着你.....

经济科学出版社

☆自考乐园---心境随缘，诚与天下自考生共勉！！
☆自考乐园---分享快乐，你的快乐老家！！
☆自考乐园---引领成功，你的精神乐园！！
自考乐园俱乐部，专注于自考，致力于成为全国最全，
最优的自考学习交流，资料共享平台.....

全国高等教育自学考试指定教材 计算机及应用专业(独立本科段)

俱乐部名称：自考乐园

俱乐部id：5346389（请牢记它哦~在百度贴吧的搜索框中输入俱乐部id，
可以直接进入俱乐部）

俱乐部url地址：<http://tieba.baidu.com/club/5346389>

（您也可以通过此url进入俱乐部。）

俱乐部简介①自考乐园俱乐部，专注于自考，致力于成为全国最全，
最优的自考学习交流，资料共享平台.....

②本人自考计算机网络独立本科段8科，真诚欢迎报考此科目的朋友进来一起交流，进步，提高.....
欢迎加入自考乐园俱乐部，如有需要自考资料，请留言，我们会尽力帮助大家的...祝大家自考快乐.....

③自考乐园诚与天下自考生共勉！！

欢迎加入自考乐园俱乐部.....

（附：计算机网络原理自学考试大纲）

☆☆☆与千万自考生同行，你准备好了吗？

你希望在自考的征途中，有一群和你志同道合的人同行吗？

你愿意在漫长的自考岁月中，有一群人和你分享快乐，分担忧愁吗？

你渴望在一个人奋斗时，有一群人在背后默默支持你吗？

你是否也一直在苦苦寻找这样一个平台，一群志同道合的人，
一片积极向上的心，一个共同的追求，一个诚挚的鼓励，一个坚实的支持.....
对！！！！就是这里！！！！这里有你想要的一切.....

与志者同行，你也将成为志者！！！！

与成功者同行，你也将获得成功！！！！

与千万自考生同行，你准备好了吗？？？

与千万自考生同行，你做好了准备吗？？？

今天我们诚挚的发出邀请，真诚的欢迎广大自考的朋友
（尤其是和我报考相同专业的朋友）加入本俱乐部，一起交流，进步，提高.....
我们正寻找特别的你亲?情加入.....

最后预祝所有的朋友：

自考快乐

天天有份好心情！！！！-----杨尚杰于2010.4.19

经济科学出版社

图书在版编目 (CIP) 数据

计算机网络原理: 附计算机网络原理自学考试大纲 /
全国高等教育自学考试指导委员会组编. —北京: 经济
科学出版社, 2007. 6

全国高等教育自学考试指定教材

ISBN 978 - 7 - 5058 - 6360 - 6

I. 计… II. 全… III. 计算机网络 - 高等教育 -
自学考试 - 教材 IV. TP393

中国版本图书馆 CIP 数据核字 (2007) 第 078106 号

责任编辑: 孙怡虹

责任校对: 杨晓莹

版式设计: 代小卫

技术编辑: 李长建

计算机网络原理

(附: 计算机网络原理自学考试大纲)

全国高等教育自学考试指导委员会 组编

杨明福 主 编

付 歌 副主编

经济科学出版社出版

社址: 北京市海淀区阜成路甲 28 号 邮编: 100036

网址: www.esp.com.cn

电子邮件: esp@esp.com.cn

北京友谊印刷有限公司印刷

787 × 1092 16 开 17.5 印张 430000 字

2007 年 6 月第 1 版 2007 年 7 月第 1 次印刷

印数: 000001 - 010100 册

ISBN 978 - 7 - 5058 - 6360 - 6/F·5621 定价: 26.50 元

(图书出现印装问题, 请与当地教材供应部门联系)

(版权所有 翻印必究)

组编前言

21 世纪是一个变幻莫测的世纪，是一个催人奋进的时代，科学技术飞速发展，知识更替日新月异。希望、困惑、机遇、挑战，随时随地都有可能出现在每一个社会成员的生活之中。抓住机遇、寻求发展、迎接挑战、适应变化的制胜法宝就是学习——依靠自己学习，终生学习。

作为我国高等教育组成部分的自学考试，其职责就是在高等教育这个水平上倡导自学、鼓励自学、帮助自学、推动自学，为每一位自学者铺就成才之路。组织编写供读者学习的教材就是履行这个职责的重要环节。毫无疑问，这种教材应当适合自学，应当有利于学习者掌握、了解新知识、新信息，有利于学习者增强创新意识，培养实践能力，形成自学能力，也有利于学习者学以致用，解决实际工作中所遇到的问题。具有如此特点的书，我们虽然沿用了“教材”这个概念，但它与那种仅供教师讲、学生听，教师不讲、学生不懂，以“教”为中心的教科书相比，已经在内容安排、编写体例、行文风格等方面都大不相同了。希望读者对此有所了解，以便从一开始就树立起依靠自己学习的坚定信念，不断探索适合自己的学习方法，充分利用已有的知识基础和实际工作经验，最大限度地发挥自己的潜能，以达到学习的目标。

欢迎读者提出意见和建议。

祝每一位读者自学成功！

全国高等教育自学考试指导委员会

2007 年 6 月

编者的话

本书作为高等教育自学考试计算机及其应用以及其它相关专业独立本科段《计算机网络原理》课程的自学教材。

计算机网络是计算机技术和通信技术相互渗透、密切结合而形成的一个新兴的交叉科学,它是当今计算机科学与技术学科中发展最为迅速的领域之一,也是计算机应用领域中最为热门的技术之一。在当今信息时代,以 Internet 为代表的网络应用技术更加快速发展和网络经济空前蓬勃繁荣的形势下,基于网络技术的电子商务、电子政务、远程教育、远程医疗与信息安全技术正在以前所未有的速度发展。计算机网络已遍及现代社会的每一个角落,正在改变着人们的工作方式与生活方式。

计算机网络作为一门交叉科学,经过了 50 年左右的发展,已形成了自身比较完善的体系。所涉及的内容多,应用广泛,技术发展迅速,知识更新快,为使读者面对不断变化的技术,具有跟踪、学习的基础与能力,并适合于参加高等教育自学考试选修本课程的学生阅读和自学,本教材立足于让读者能够掌握计算机网络最基本的工作原理,学会处理网络问题的最基本方法,先从叙述计算机网络体系结构和开放系统互连参考模型的整体知识着手,对物理层、数据链路层、网络层、传输层以及应用层作了深入详细的介绍,最后对局域网技术和网络实用技术作了重点介绍。

全书内容共分 9 章。第 1 章概述部分主要介绍计算机网络的基本概念、分类、发展与应用,并对网络的标准化进行了介绍;第 2 章讨论了计算机网络的体系结构与网络协议的基本概念,对开放系统互连参考模型 OSI/RM 和 TCP/IP 参考模型进行了详细分析,并对两个参考模型进行了比较;第 3 章在介绍数据通信基础知识与基本概念的基础上,对物理层基本概念、功能以及主要协议进行了讨论;第 4 章讨论了数据链路层的基本概念、功能和主要协议,并对因特网的数据链路层协议 SLIP 与 PPP 进行了介绍;第 5 章讨论了网络层协议,对网络层的基本概念、功能、路由选择、拥塞控制、服务质量进行了介绍,并对网络互连以及因特网互连层协议 IP、ARP、RARP、ICMP、IGMP 以及 IPv6 进行了详细讨论;第 6 章讨论了传输层协议,对传输层的功能和协议进行了介绍,并重点分析了 TCP 传输控制协议和 UDP 用户数据报协议;第 7 章讨论了应用层的基本概念和 Internet 应用层协议;第 8 章讨论了介质访问控制方法及局域网、城域网技术的发展与应用,并介绍了高速局域网、交换局域网与无线局域网技术;第 9 章介绍目前广泛使用的实用网络技术,包括 X.25、帧中继、ATM、第三层交换技术、虚拟局域网技术、虚拟专网技术以及计算机网络安全技术。

本书内容安排以基础性和实用性为重点,力图在阐明计算机网络基本工作原理的基础上,注重理论和实际的兼顾。列举了当今流行的网络技术和产品,对网络发展前沿的内容也有所涉及,其目的在于使读者通过本课程的学习,掌握计算机网络的工作原理,理解有关网

络的一系列标准协议和工业标准，并具有网络的组网、规划和设计选型的能力。为开展和从事计算机网络的应用打下扎实的基础。书中每章末都附有与课程内容密切相关的习题。

本书由杨明福主编，付歌副主编。第1、2、3、4章由杨明福编写，第5、6、7、8、9章由付歌编写。由全国高等教育自学考试指导委员会电子电工与信息类专业委员会组织北京邮电大学马跃教授、杭州电子科技大学章坚武教授和复旦大学高传善教授统审了全书，并提出了很多有益建议，编者在此致以衷心的感谢。

书中难免存在错误和不妥之处，恳请广大读者批评指正。

编者

2006年11月

目 录

计算机网络原理

第1章 计算机网络概述	(1)
1.1 计算机网络的发展	(1)
1.1.1 计算机网络的产生和发展	(1)
1.1.2 三大网络介绍	(4)
1.1.3 未来网络发展趋势	(5)
1.2 计算机网络的基本概念	(8)
1.2.1 计算机网络的定义	(8)
1.2.2 计算机网络的组成	(8)
1.2.3 计算机网络的功能与应用	(9)
1.3 计算机网络的分类	(12)
1.3.1 按拓扑类型分类	(12)
1.3.2 按网络的交换方式分类	(15)
1.3.3 按网络的覆盖范围分类	(16)
1.3.4 按网络传输技术分类	(16)
1.4 计算机网络的标准化	(16)
1.4.1 国际标准化组织 (ISO)	(17)
1.4.2 其它标准化机构	(17)
1.4.3 Internet 的组织机构	(17)
第2章 计算机网络体系结构	(19)
2.1 网络的分层体系结构	(19)
2.1.1 协议的要素	(19)
2.1.2 分层体系结构	(19)
2.2 OSI/RM 开放系统互连参考模型	(21)
2.2.1 OSI/RM 简介	(21)

2.2.2	OSI/RM 的结构	(21)
2.2.3	面向连接服务与无连接服务	(23)
2.3	TCP/IP 参考模型	(24)
2.3.1	TCP/IP 简介	(24)
2.3.2	TCP/IP 的体系结构	(25)
2.4	OSI/RM 与 TCP/IP 参考模型的比较	(26)
2.4.1	OSI 模型和协议的缺点	(27)
2.4.2	TCP/IP 模型和协议的缺点	(27)
第 3 章	物理层	(29)
3.1	物理层接口与协议	(29)
3.1.1	物理层接口	(29)
3.1.2	物理层的功能和提供的服务	(30)
3.1.3	物理层协议举例	(32)
3.2	传输介质	(36)
3.2.1	双绞线	(36)
3.2.2	同轴电缆	(36)
3.2.3	光纤	(37)
3.2.4	无线传输介质	(38)
3.2.5	传输介质的选择	(41)
3.3	数据通信技术	(42)
3.3.1	通信信道	(42)
3.3.2	模拟数据通信和数字数据通信	(45)
3.3.3	多路复用技术	(47)
3.3.4	异步传输和同步传输	(50)
3.4	数据编码	(51)
3.4.1	数据编码技术	(51)
3.4.2	调制解调器	(55)
3.5	数据交换技术	(63)
3.5.1	电路交换 (Circuit Switching)	(63)
3.5.2	报文交换 (Message Switching)	(64)
3.5.3	分组交换 (Packet Switching)	(65)
3.5.4	高速交换	(66)
3.5.5	交换技术的比较	(68)
第 4 章	数据链路层	(71)
4.1	数据链路层的功能	(71)
4.1.1	帧同步功能	(71)
4.1.2	差错控制功能	(73)

4.1.3	流量控制功能	(73)
4.1.4	链路管理功能	(74)
4.2	差错控制	(75)
4.2.1	差错检测	(75)
4.2.2	差错控制方法	(75)
4.2.3	奇偶校验码和循环冗余码	(76)
4.3	基本数据链路协议	(80)
4.3.1	停等协议	(80)
4.3.2	顺序接收管道协议	(80)
4.3.3	选择重传协议	(82)
4.4	链路控制规程	(83)
4.4.1	二进制同步通信协议	(84)
4.4.2	高级数据链路控制协议	(86)
4.5	因特网的数据链路层协议	(89)
4.5.1	SLIP 协议	(89)
4.5.2	PPP 协议	(90)
第 5 章	网络层	(93)
5.1	通信子网的操作方式和网络层提供的服务	(93)
5.1.1	虚电路操作方式	(93)
5.1.2	数据报操作方式	(95)
5.1.3	虚电路服务	(95)
5.1.4	数据报服务	(96)
5.1.5	虚电路子网和数据报子网的比较	(96)
5.2	路由选择	(97)
5.2.1	最优化原则	(98)
5.2.2	静态路由选择算法	(98)
5.2.3	动态路由选择算法	(101)
5.2.4	移动主机的路由选择	(103)
5.2.5	广播路由选择	(105)
5.2.6	多播路由选择	(106)
5.3	拥塞控制	(107)
5.3.1	拥塞发生的原因	(108)
5.3.2	拥塞控制的通用原则	(108)
5.3.3	拥塞预防策略	(109)
5.3.4	虚电路子网中的拥塞控制	(110)
5.3.5	数据报子网中的拥塞控制	(111)
5.3.6	负载丢弃	(113)
5.3.7	抖动控制	(113)

5.4	服务质量	(114)
5.4.1	集成服务和区分服务	(115)
5.4.2	标签交换和 MPLS	(116)
5.5	网络互连	(117)
5.5.1	网络互连原理	(117)
5.5.2	网桥技术	(118)
5.5.3	网络互连协议	(120)
5.5.4	网络互连设备	(123)
5.6	因特网的互连层协议	(127)
5.6.1	IP 协议	(127)
5.6.2	ARP 协议与 RARP 协议	(130)
5.6.3	ICMP 协议	(130)
5.6.4	IGMP 协议	(131)
5.6.5	IPv6	(132)
第 6 章	传输层	(134)
6.1	传输层基本概念	(134)
6.1.1	传输服务	(134)
6.1.2	传输协议的要素	(135)
6.1.3	传输层在 OSI 中的地位和作用	(137)
6.2	传输控制协议	(137)
6.2.1	TCP 服务模型	(137)
6.2.2	TCP 数据传输机制	(138)
6.2.3	TCP 连接管理	(139)
6.2.4	TCP 滑动窗口控制	(141)
6.2.5	TCP 重传策略	(142)
6.2.6	TCP 拥塞控制	(142)
6.3	用户数据报传输协议	(143)
6.3.1	UDP 服务模型	(143)
6.3.2	UDP 数据传输机制	(143)
6.3.3	UDP 协议的应用	(144)
第 7 章	应用层	(145)
7.1	域名系统	(145)
7.1.1	IP 地址与域名	(145)
7.1.2	域名系统的概念	(146)
7.1.3	域名解析原理	(147)
7.2	电子邮件	(148)
7.2.1	电子邮件的基本概念	(148)

7.2.2	简单邮件传输协议 SMTP	(149)
7.2.3	邮局协议 POP	(150)
7.2.4	Internet 消息访问协议 IMAP	(151)
7.3	万维网	(152)
7.3.1	WWW 的工作原理	(152)
7.3.2	超文本传输协议 HTTP	(152)
7.3.3	统一资源定位器 URL	(153)
7.4	其它服务	(153)
7.4.1	文件传输 FTP	(153)
7.4.2	远程登录 Telnet	(154)
7.4.3	电子公告板系统 BBS	(154)
第 8 章	局域网技术	(156)
8.1	介质访问控制子层	(156)
8.1.1	信道分配策略	(156)
8.1.2	介质访问控制协议	(157)
8.2	IEEE 802 标准与局域网	(168)
8.2.1	IEEE 802 标准概述	(168)
8.2.2	IEEE 802.2: 逻辑链路控制子层	(170)
8.2.3	IEEE 802.3: CSMA/CD	(171)
8.2.4	IEEE 802.4: 令牌总线	(175)
8.2.5	IEEE 802.5: 令牌环	(176)
8.2.6	IEEE 802.6: 分布队列双总线	(181)
8.3	高速局域网	(184)
8.3.1	FDDI 环网	(184)
8.3.2	快速以太网	(187)
8.3.3	千兆位以太网	(188)
8.3.4	万兆位以太网	(190)
8.3.5	交换型以太网	(191)
8.4	无线局域网技术	(192)
8.4.1	无线局域网概述	(192)
8.4.2	IEEE 802.11 协议	(193)
8.4.3	IEEE 802.11 系列标准	(194)
8.4.4	蓝牙技术	(196)
8.4.5	IrDA 和 HomeRF 技术	(197)
8.4.6	无线应用协议 WAP	(198)
8.5	移动 Ad Hoc 网络	(199)
8.5.1	Ad Hoc 网络的发展和特点	(199)
8.5.2	Ad Hoc 网络的结构	(200)

8.5.3 Ad Hoc 网络的路由协议	(201)
8.5.4 与其它移动通信系统的比较	(203)
8.6 局域网操作系统	(203)
8.6.1 局域网操作系统概述	(203)
8.6.2 典型局域网操作系统简介	(206)
第9章 实用网络技术	(210)
9.1 分组交换技术	(210)
9.1.1 X.25 协议	(210)
9.1.2 帧中继	(214)
9.2 异步传输模式	(216)
9.2.1 ATM 交换	(216)
9.2.2 ATM 的特征	(218)
9.2.3 ATM 的层次结构	(219)
9.2.4 ATM 的工作方式	(222)
9.3 第三层交换技术	(223)
9.3.1 第三层交换的引入	(223)
9.3.2 局域网 L3 交换技术	(224)
9.3.3 广域网 L3 交换技术	(225)
9.4 虚拟局域网技术	(226)
9.4.1 虚拟局域网的交换技术	(226)
9.4.2 虚拟局域网的划分方法	(227)
9.4.3 虚拟局域网的互连方式	(228)
9.5 虚拟专用网 VPN	(229)
9.5.1 何谓 VPN	(229)
9.5.2 VPN 的特点	(229)
9.5.3 VPN 的安全技术	(230)
9.5.4 VPN 的发展趋势	(230)
9.6 计算机网络管理与安全	(231)
9.6.1 网络管理基本功能	(231)
9.6.2 网络安全	(232)

计算机网络原理自学考试大纲

出版前言	(241)
一、课程性质与设置目的	(243)

二、课程内容与考核目标	(245)
第1章 计算机网络概述	(245)
第2章 计算机网络体系结构	(246)
第3章 物理层	(247)
第4章 数据链路层	(250)
第5章 网络层	(251)
第6章 传输层	(253)
第7章 应用层	(255)
第8章 局域网技术	(256)
第9章 实用网络技术	(258)
三、关于大纲的说明与考核实施要求	(261)
附录：题型举例	(263)
后记	(264)

第1章 计算机网络概述

本章在介绍网络形成与发展历史的基础上对网络定义、组成、功能和应用、分类和拓扑结构以及网络标准化等问题进行详细的介绍。

今天，“计算机网络”(Computer Network)这个名词已是家喻户晓，成为人们工作、日常生活中不可缺少的一部分。例如，去银行存取款，出行预订飞机票，网上购物以及上网浏览等。计算机网络的应用领域已遍及现代社会的每一个角落。

人类社会已经进入了信息时代。信息是当今世界最重要的资源之一，它与物质及能源一起构成了三大资源支柱。与其它两类资源相比，信息资源最显著的特点是它在使用中非但不会损耗，反而会通过交流和共享得到增值。要充分地利利用信息资源，就离不开处理信息和传输信息的高科技手段，处理信息的计算机和传输信息的互连计算机网络便是在这样的社会需求背景下成为了信息时代的基础。

20世纪90年代各国政府都提出了以建立高速计算机通信网络为核心的信息高速公路计划。从此，在世纪之交的历史时刻，掀起了一场全球信息高速公路的浪潮。

信息高速公路是信息社会的基础建设，在信息的搜索、积累、处理和应用至关重要的今天，它将对社会的发展起到不可替代的作用。计算机网络是信息高速公路的重要组成部分，被认为是信息高速公路雏形的因特网(Internet)，已逐渐演变成为一个全球性的政府、经济、学术和生活信息交换网，它向人们展示了全球联网的广阔前景：全世界的计算机联合起来，让每个人都拥有对任何一种可能想像得到的信息的前所未有的、无可比拟的访问能力。

当今的世界，每天都有数千万人在使用因特网。可以预料，计算机网络将无处不在。并将最终改变人们的理念和生活，从而塑造出一代全新的网络文化。

1.1 计算机网络的发展

1.1.1 计算机网络的产生和发展

计算机网络从20世纪70年代开始发展至今，已形成从小型的办公室局域网到全球性的大型广域网，对现代人类的生生产、经济、生活等各个方面都产生了巨大的影响。

追溯计算机网络的发展历史，它的演变可以概括为面向终端的计算机网络、计算机—计算机网络、开放式标准化网络以及因特网广泛应用和高速网络技术发展等四个阶段。

1. 面向终端的计算机网络

以单个计算机为中心的远程联机系统，构成面向终端的计算机网络。

所谓联机系统，就是由一台中央主计算机连接大量的地理上处于分散位置的终端。早在 20 世纪 50 年代初，美国建立的半自动地面防空系统 SAGE (Semi-Automatic Ground Environment) 就将远距离的雷达和其它测量控制设备的信息，通过通信线路汇集到一台中心计算机进行集中处理，从而开创了把计算机技术和通信技术相结合的尝试。

这类简单的“终端—通信线路—计算机”系统，成了计算机网络的雏形。严格地说，联机系统与以后发展成熟的计算机网络相比，存在着根本的区别。这样的系统除了一台中心计算机外，其余的终端设备都没有自主处理的功能，还不能算计算机网络。为了更明确地区别于后来发展的多个计算机互连的计算机网络，就专称这种系统为面向终端的计算机网络。

随着连接的终端数目的增多，为减轻承担数据处理的中心计算机的负载，在通信线路和中心计算机之间设置了一个前端处理机 FEP (Front End Processor) 或通信控制器 CCU (Communication Control Unit)，专门负责与终端 T 之间的通信控制，从而出现了数据处理的分工，更好地发挥了中心计算机的数据处理能力。另外，在终端较集中的地区，设置集中器或多路复用器，它首先通过低速线路将附近群集的终端连至集中器或复用器，然后通过高速通信线路、实施数字数据和模拟信号之间转换的调制解调器 (Modem) 与远程中心计算机的前端处理机相连，构成如图 1-1 所示的远程联机系统，从而提高了通信线路的利用率，节约了远程通信线路的投资。

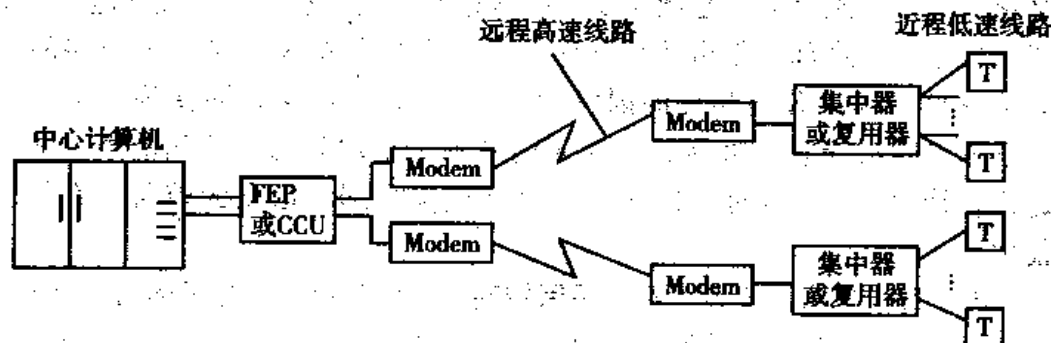


图 1-1 单计算机为中心的远程联机系统

2. 计算机—计算机网络

20 世纪 60 年代中期，出现了由若干个计算机互连的系统，开创了“计算机—计算机”通信的时代，并呈现出多处理中心的特点。60 年代后期，由美国国防部高级研究计划局 ARPA (现称 DARPA, Defense Advanced Research Projects Agency) 提供经费，联合计算机公司和大学共同研制而发展起来的 ARPA 网 (ARPANET)，标志着目前所称的计算机网络的兴起。ARPANET 的主要目标是借助于通信系统，使网内各计算机系统间能够共享资源。ARPANET 是一个成功的系统，它是计算机网络技术发展中的一个里程碑，它在概念、结构和网络设计方面都为后继的计算机网络技术的发展起到了重要的作用，并为 Internet 的形成奠定了基础。

此后，计算机网络得到了迅猛的发展，各大计算机公司都相继推出了自己的网络体系结

构和相应的软、硬件产品。用户只要购买计算机公司提供的网络产品,就可以通过专用或租用通信线路组建计算机网络。IBM 公司的 SNA (System Network Architecture) 和 DEC 公司的 DNA (Digital Network Architecture) 就是两个著名的例子。凡是按 SNA 组建的网络都可称为 SNA 网,而按 DNA 组建的网络都可称为 DNA 网或 DECNET。

3. 开放式标准化网络

虽然已有大量各自研制的计算机网络正在运行和提供服务,但仍存在不少弊病,主要原因是这些各自研制的网络没有统一的网络体系结构,难以实现互连。这种自成体系的系统称为“封闭”系统。为此,人们迫切希望建立一系列的国际标准,渴望得到一个“开放”的系统。这也是推动计算机网络走向国际化的一个重要因素。

正是出于这种动机,开始了对“开放”系统互连的研究。国际标准化组织 ISO (International Standards Organization) 于 1984 年正式颁布了一个称为“开放系统互连基本参考模型”(Open System Interconnection Basic Reference Model) 的国际标准 ISO 7498,简称 OSI 参考模型或 OSI/RM。OSI/RM 由七层组成,所以也称 OSI 七层模型。OSI/RM 的提出,开创了一个具有统一的网络体系结构、遵循国际化协议的计算机网络新时代。

OSI 标准不仅确保了各厂商生产的计算机间的互连,同时也促进了企业的竞争。厂商只有执行这些标准才能有利于产品的销路,用户也可以从不同制造厂商获得兼容的开放的产品,从而大大加速了计算机网络的发展。

4. 因特网的广泛应用与高速网络技术的发展

20 世纪 90 年代网络技术最富有挑战性的话题是 Internet 与高速通信网络技术、接入网、网络与信息安全技术。Internet 作为世界性的信息网络,正在对当今经济、文化、科学研究、教育与人类社会生活发挥着越来越重要的作用。宽带网络技术的发展为全球信息高速公路的建设提供了技术基础。

Internet 是覆盖全球的信息基础设施之一。对于广大 Internet 用户来说,它好像是一个庞大的广域计算机网络。用户可以利用 Internet 实现全球范围的电子邮件、WWW 信息查询与浏览、电子新闻、文件传输、语音与图像通信服务功能。它对推动世界科学、文化、经济和社会的发展有不可估量的作用。

在 Internet 飞速发展与广泛应用的同时,高速网络的发展也引起人们越来越多的注意。高速网络技术发展表现在宽带综合业务数字网 B-ISDN、异步传输模式 ATM、高速局域网、交换局域网与虚拟网络。

Internet 技术在企业内部网中的应用也促进了 Intranet 技术的发展。企业 Intranet 之间电子商务活动的开展又进一步引发了 Extranet 技术的发展。Internet、Intranet 与 Extranet 和电子商务已成为当前企业网研究与应用的热点。更高性能的 Internet II 也正在发展之中。

信息高速公路的服务对象是整个社会,因此它要求网络无所不在,未来的计算机网络将覆盖所有的企业、学校、科研部门、政府及家庭,其覆盖范围甚至要超过目前的电话通信网。为了支持各种信息的传输,网络必须具有足够的带宽、很好的服务质量与完善的安全机制,支持多媒体信息通信,以满足不同的应用需求。为了有效地保护金融、贸易等商业秘密,保护政府机要信息与个人隐私,网络必须具有足够的安全机制,以防止信息被非法窃

取、破坏与损失，网络系统必须具备高度的可靠性与完善的管理功能，以保证信息传输的安全与畅通。毋庸置疑，计算机网络技术的发展与应用必将对 21 世纪世界经济、军事、科技、教育与文化的发展产生重大的影响。

1.1.2 三大网络介绍

当前，在我国通信、计算机信息产业以及广播电视领域中，实际运行并具有影响的有三大网络：即电信网络、广播电视网络以及计算机网络。

1. 电信业务网

电信业务网是以电话网为基础逐步发展起来的。电话系统由三个主要的部件构成：

- (1) 本地网络：使用双绞线进入家庭和业务部门，承载的是模拟信号；
- (2) 干线：通过光纤将交换局连接起来，承载的是数字信号；
- (3) 交换局：使电话呼叫从一条干线接入到另一条干线。

图 1-2 表示了一个中距离连接的电话系统。

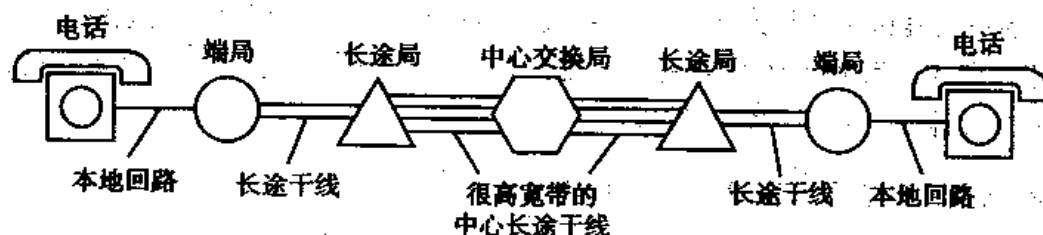


图 1-2 中距离连接的电话系统

在过去，整个电话系统中传输的信号都是模拟的。随着光纤、数字电路和计算机的出现，现在所有的干线和交换设备几乎都是数字的，仅剩本地回路仍然是模拟的。之所以优先选择数字传输，是因为它不需要像模拟传输那样，当一个长途呼叫的信号经过了许多次放大之后，还需要重新精确地产生模拟信号。对于数字传输而言，只需要能够正确地区分 0 和 1 就足够了。这种特性使得数字传输比模拟传输更加可靠。而且，维护工作更加容易，维护成本更加便宜。

整个网络虽有非对称用户环路 (ADSL) 和高速用户环路 (VDSL) 等方式，速率可从几 Mbps 到几十 Mbps，但受到双绞线传输容量这一瓶颈的抑制，目前电话双绞线上网的主流速率为 56Kbps，其物理极限为 64Kbps。

电信业务网除了传统的电话交换网 (PSTN) 之外，还有数字数据网 (DDN)、帧中继网 (FR) 和异步转移模式 ATM 网等。在 DDN 网中，它可提供固定或半永久连接的电路交换业务，适合于传输实时多媒体通信业务。在帧中继网中，是以统计复用技术为基础，进行包传输、包交换，速率一般在 64Kbps ~ 2.048Mbps 之内，适合传输非实时多媒体通信业务。在 ATM 网中，ATM 是支持高速数据网建设、运行的关键设备，可支持 25Mbps ~ 4Gbps 速率的传输，不仅可以传语音，而且可以传数据、图像，包括高速数据和活动图像。电信网除上述几种网之外，还有 X.25 公共数据网、综合服务数字网 ISDN 以及 CHINANET 网等。目前电信网除提供传统的话音服务外，主要还有传真和数据通信等。

2. 广播电视网

广播电视网主要是有线电视网 (CATV), 目前还是靠同轴电缆向用户传送电视节目, 处于模拟水平阶段, 但其网络技术设备先进, 光缆为主干线, 贯通各城镇。宽带双向光纤同轴电缆混合网 (HFC) 入户的优点, 与电话接入方式相比, 其传输带宽约为电话线的一万倍左右, 而且在有线电视同一根同轴电缆上, 可以同时看电视、打电话、上因特网, 且互不干扰。目前, 它的信息源是以单向实时及一点对多点的方式连接到众多的用户, 用户只能在当时被动地选择是否接收 (主要是语音和图像的广播)。宽带双向的点播电视 (VOD) 及通过 CATV 网接入因特网进行电视点播、CATV 通话等是 CATV 网的发展方向, 最终目的是使 CATV 网走向宽带双向的多媒体通信网。它的业务除了广播电视传输仍然是主要业务之外, 还应包含电视点播 (VOD) 或准视频点播业务 (NVOD)、远程电视教育、远程医疗、电视会议、电视电话、电视购物和电视商务等。

3. 计算机网

计算机网初期主要是局域网 (LAN), 广域网 (WAN) 是在 Internet 大规模发展后才进入平常家庭的, 目前主要依赖于电信网, 因此传输速率受到双绞线的限制。CHINANET 网是依托强大的 CHINAPAC (分组交换网)、CHINADDN (数字数据网) 和 PSTN (电话交换网) 等公用网, 采用先进设备, 而成为我国 Internet 的主干网。在计算机网中, 用户之间的连接可以是一对一的, 也可以是一点对多点的, 用户之间的通信在某些情况下可以认为是实时的, 而在大多数情况下都是非实时的, 采用的是存储—转发方式。通信方式可以是双向交互的, 也可以是单向的。主要提供的业务如: 文件共享、信息浏览、电子邮件、网络电话、视频点播、FTP 文件下载和网上会议等。

从以上三个网络所能提供的业务来看, 未来的信息社会, 人们决不会仅满足使用传统的只能传语音的电话机; 只能单向接收电视节目的电视机以及使用仅仅能提供文件共享和上 Internet 的计算机。用户需要能有更多、更快、更直接的信息交流, 同时包括语音、图像和数据在内的多媒体技术, 这就需要将三网融合 (也称三网合一)。近年来, 三网合一也成为最热门的话题之一。从全世界范围来看, 也是现代通信和计算机网络发展的大趋势。所谓“三网合一”就是把现有的传统电信网、广播电视网和计算机网互相融合, 逐渐形成一个统一的网络系统, 由一个全数字化的网络设施来支持包括数据、语音和图像在内的所有业务的通信。

1.1.3 未来网络发展趋势

未来的计算机网络将覆盖所有的政府部门、企业、学校、医院、科研机构、社区以及家庭, 计算机网络将无所不在。可视电话、可视图文、图像传输和视频会议等多媒体业务对网络传输的实时性和带宽提出了很高的要求, 为了支持各种信息的传输, 未来的网络必须具有足够的带宽、很好的服务质量与完善的安全机制, 以满足电子政务、电子商务、远程教育、远程医疗、分布式计算、数字图书馆与视频点播等不同的应用要求。

在 Internet 飞速发展与广泛应用的同时, 高速网络的发展也引起人们的特别注意。高速网络技术发展主要表现在: 宽带综合业务数字网 B-ISDN、异步传输模式 ATM、高速局域网、

交换局域网以及虚拟网络。基于光纤通信技术的宽带城域网与宽带接入网技术已经成为当前研究、应用与产业发展的重点。

Internet 的广泛应用和网络技术的快速发展,使得网络计算技术也成为当今重要的网络研究与应用领域。网络多媒体计算、移动计算网络、网络并行计算、网络计算以及网络分布式对象计算等各种网络计算技术正在成为新的研究与应用的热点。

此外,为了有效地保护政府涉密信息和个人隐私,保护金融、贸易等商业秘密,网络必须具有可靠的安全机制,以防止信息被非法窃取、破坏和泄露。人们对网络与信息安全的需要越来越强烈,网络与信息安全也引起了社会的高度关注,网络与信息安全的研宄、应用和产业发展越来越受到重视。

1. 宽带网络

宽带网络的建设正在全球范围内掀起一个高潮,很多国家的政府与企业投入巨资,把宽带网络作为战略产业来发展。

宽带网络可分为宽带骨干网和宽带接入网两个部分。骨干网又称为核心交换网,它是基于光纤通信系统的,能实现大范围(在城市之间和国家之间)的数据流传送。通常采用高速传输网络、高速交换设备(如大型 ATM 交换机和交换路由器)。电信业一般认为传输速率达到 2Gbps 的骨干网称做宽带网。接入网需要覆盖所有类型的用户。接入网技术可根据所使用的传输介质的不同分为光纤接入、铜线接入、光纤同轴电缆混合接入和无线接入等多种类型。也就是说,宽带接入技术基本上可分为有线接入和无线接入。光纤、铜线和同轴电缆接入属于有线接入,而宽带无线接入技术已成为一种新的不可忽视的宽带接入发展趋势。

2. 全光网络

全光网(All Optical Network, AON)是以光节点取代现有网络的电节点,并用光纤将光节点互连成网,采用光波完成信号的传输、交换等功能,克服了现有网络在传输和交换时的瓶颈,减少信息传输的拥塞、延迟,提高网络的吞吐量。全光网已被认为是未来通信网向宽带、大容量发展的优选方案。

3. 多媒体网络

多媒体网络是指能够传输多媒体数据的通信网络。多媒体网络需要满足多媒体信息传输所需的交互性和实时性的要求。主要表现在:

(1) 高传输带宽要求:以分辨率为 640×480 真彩色图像(像素分辨率为 24b)为例,如以每秒 25 帧动态显示,则需要通信带宽为 184Mbps ($640 \times 480 \times 24 \times 25$)。这样的带宽要求是很难实现的,一般采用压缩技术来减少对带宽的要求,常用的压缩标准有 ITU-T 的 H.261、H.263 和 ISO 的 MPEG 等。

(2) 不同类型的数据对传输要求也不同:语音数据的传输对实时性要求较强,而对通信带宽的要求则不高。而高质量的视频通信对实时性和通信带宽的要求都很高。另外多媒体对误码率的要求不相同。视频压缩后的关键帧出错将可能导致一段数据流无法恢复、解压和回放。非关键帧出错仅会导致回放中某些画面质量下降,在一定程度上却是可以容忍的。

(3) 对多媒体传输有连续性与实时性的要求。

(4) 对多媒体传输有同步的要求：即要在传输过程中必须保持多媒体数据之间在时序上的同步约束关系。同步要求之一：是指单一时间相关媒体数据内各媒体元素之间的时间关系，如音频流的各个分组之间的连续等时性；同步要求之二：是指有时空约束关系的时间相关媒体，或时间相关媒体与时间无关媒体之间的时间关系。如必须严格保持音频与视频的同步。

(5) 具有多方参与通信的特点：例如视频会议要求任何成员之间可以通信；视频点播要求视频服务器可以同时将视频数据发向多个用户。

由于传统的基于 IP 协议的网络的通信协议基本上没有考虑多媒体网络应用的要求，因此传统的 IP 网络对于多媒体网络应用是不适合的。必须研究一些改进的措施，主要是增大带宽与改进协议。增大带宽方面除了改进传输介质的性能之外，在路由器方面进行了很大的改进，产品的结构已从基于软件实现路由功能的单总线单 CPU 路由器，发展成基于硬件专用 ASIC 芯片的路由交换功能的高性能的交换路由器。改进协议方面主要表现在支持 IP 多播、资源预留协议 (Resource Reservation Protocol, RSVP)、区分服务 DiffServ 与多协议标识交换 (Multi-Protocol Label Switching, MPLS) 等方面。RSVP 允许应用程序在源与目的节点之间建立一条数据通道，根据应用的需求在各个交换节点预留资源，从而保证沿着这条通道传输的数据流满足 QoS 要求。区分服务是利用 IP 分组头对数据的服务级别进行标识，路由器根据标识来建立一条能满足 QoS 的传输通道；MPLS 技术是为了更好地将 IP 协议与 ATM 高速交换技术结合起来，实现 IP 分组的快速交换。MPLS 的核心是标记交换。标记 (Label) 是一个用于数据分组交换的、短的、固定长度的转发标识符。当数据分组到达 MPLS 域时，由入口的边界标记交换路由器 (Label-Switched Router, LSR) 分析 IP 分组头，给该分组加上相应的标记，然后传送到下一个 LSR。后续的 LSR 只需要根据标记进行转发，因此可以大大减少路由器转发分组的处理时间，提高了网络的性能。

4. 移动网络

移动计算是将计算机网络和移动通信技术结合起来，为用户提供移动的计算环境和新的计算模式，其作用是在任何时间都能及时、准确地为任何地理位置的用户提供服务。涉及的主要技术有：

(1) 蜂窝式数字分组数据 (Cellular Digital Packet Data, CDPD) 通信平台：其特点是无线和可移动。在无线覆盖区域内，从固定点到时速 100 Km/s 的各种无线移动数据终端，均可通过该移动数据通信平台，进入各种数据通信网络，实现各类数据通信。CDPD 业务有无线数据遥测遥控、定位信息服务、传送电子短消息以及销售等服务。第三代移动通信系统的发展除了能满足人们不断增长的对于数据传输能力的要求，同时还要实现统一的全球标准，具备多媒体传输能力，增加分组交换业务，提高传输质量。

(2) 无线局域网 (Wireless LAN, WLAN)：以微波、激光、红外线等无线电波来部分或全部代替有线局域网中的同轴电缆、双绞线、光纤，实现移动计算网络中移动节点的物理层和数据链路层功能，构成无线局域网，传输速率可达几十 Mbps。

(3) Ad hoc 网络：Ad hoc 网络是一种由一组用户群构成，不需要基站，没有固定路由器的移动通信模式。所有用户都可能移动，并且系统支持动态配置和动态流控制。每个系统都具备动态搜索、定位和恢复连结的能力。Ad hoc 网络在军事上十分重要，它可以支持野外联络、独立战斗群通信和舰队战斗群通信、临时通信要求和无人侦察与情报传输。在民用

领域它支持会议、紧急状态、临时交互式通信等相关应用。这种技术在未来移动通信市场上将扮演非常重要的角色。

(4) 无线应用协议 WAP (Wireless Application Protocol) 是一个崭新的、开放的全球化的协议。它能让用户使用内置浏览器在移动电话的屏幕上访问 Internet, 可以使具备 WAP 功能的手机直接上网。它是移动电话由基本的通话业务迈进 Internet 接入业务的关键技术。WAP 开发遵循的原则是基于 Internet 广泛应用的标准, 如 HTTP、TCP/IP、SSL、XML 等, 提供了一个对无线 Internet 的解决方案, 同时支持未来的开放标准。

5. 下一代网络

下一代网络 NGN (Next Generation Network) 是一个基于分组的核心网络 (有别于先前的时分复用网络)。能够提供包括电信业务在内的多种业务, 支持多种宽带能力和具有按需的服务质量 (QoS) 进行传送的技术, 实现与业务相关的功能与底层传送技术的独立。ITU-T 和相关的标准组织都对 NGN 的基本特征进行了描述:

- 控制功能从承载、呼叫/会话、应用/业务中分离;
- 业务提供与网络分离, 提供开放接口以及与传统网络的互通;
- 利用基本的业务组成模块, 提供广泛的业务和应用 (包括实时、非实时、流媒体和多媒体业务), 同一种业务具有统一的业务特性;
- 具有端到端 QoS 保证能力和透明的传输能力;
- 支持多种标识体系, 并能将其解析为 IP 地址以用于 IP 网选路;
- 具有通用移动性, 支持固定与移动业务融合;
- 业务功能独立于底层传送技术, 允许用户自由地接入不同业务提供商;
- 适应所有管制的要求, 如应急通信、安全性和私密性等要求。

1.2 计算机网络的基本概念

1.2.1 计算机网络的定义

计算机网络是现代计算机技术与通信技术互相渗透、密切结合的产物, 是随着社会对信息共享和信息传递的日益增强的需求而发展起来的。所谓计算机网络, 就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来, 以功能完善的网络软件 (即网络通信协议、信息交换方式和网络操作系统等) 实现网络中资源共享和信息传递的系统。

1.2.2 计算机网络的组成

图 1-3 为典型的计算机网络系统示意图。从图中可见, 一个计算机网络是由资源子网和通信子网构成的。资源子网负责信息处理, 通信子网负责全网中的信息传递。

资源子网包括提供资源的主机 HOST 和请求资源的终端 T (Terminal), 它们都是信息传

输的源节点或宿节点，有时也统称为端节点。

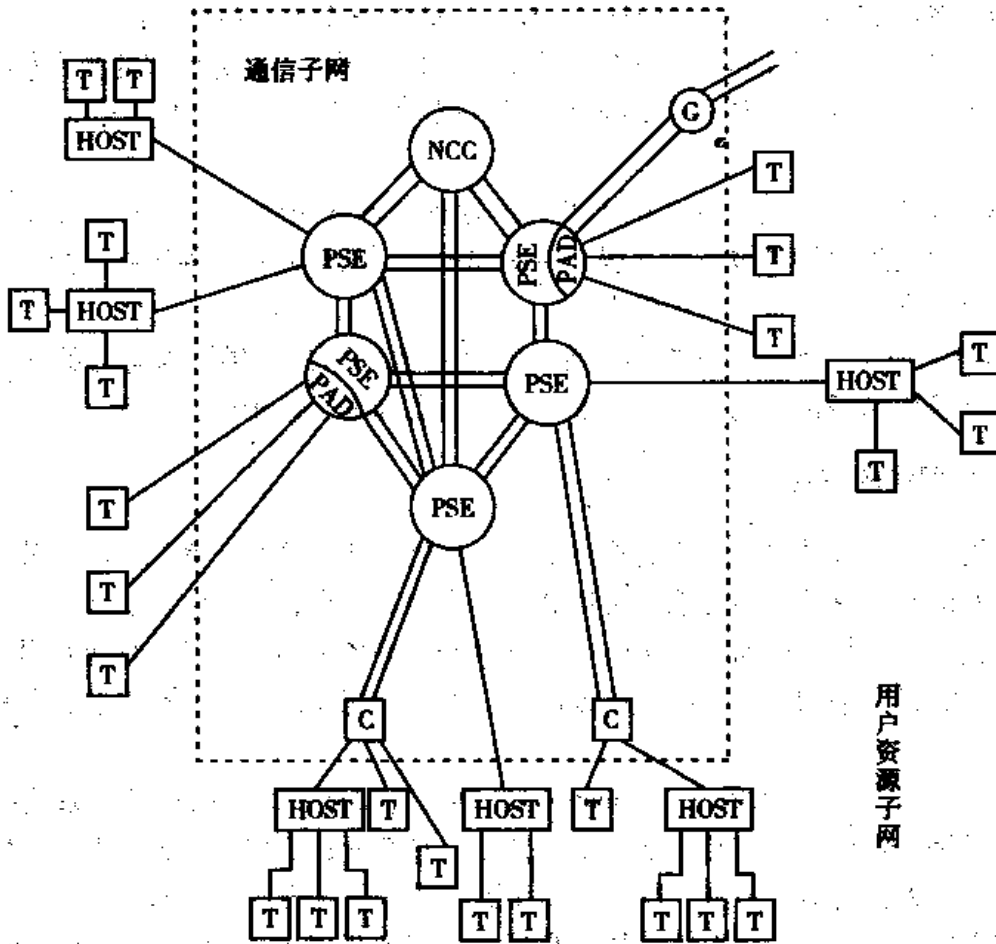


图 1-3 一个典型的计算机网络示例

通信子网主要由网络节点和通信链路组成。网络节点也称为转接节点或中间节点，它们的作用是控制信息的传输和在端节点之间转发信息。根据不同的作用，网络节点可以是分组交换设备 PSE (Packet Switching Exchanger)、分组装配/拆卸设备 PAD (Packet Assembler Disassembler)、集中器 C (Concentrator)、网络控制中心 NCC (Network Control Center)、网间连接器 G (Gateway) 也称网关或它们的组合。这些功能一般都由专用于通信的计算机来完成，所以也常将网络节点统称为接口信息处理机 IMP (Interface Message Processor)。

通信链路即传输信息的信道，它们可以是电话线、同轴电缆或光缆线，也可以是无无线电、卫星或微波信道。信息在两端节点之间传输时，可能要经过多个中间节点的转发，这种传输方式称为“存储—转发”，广域网 WAN (Wide Area Network) 中一般都采用这种传输方式。需要说明的是，局域网 LAN (Local Area Network) 一般采用“广播”传输方式，局域网中的网络节点都简化为安装于主机或工作站中的网卡。

1.2.3 计算机网络的功能与应用

1. 计算机网络的功能

计算机网络的实现，为用户构造分布式的网络计算环境提供了基础。它的功能主要表现

在硬件资源共享、软件资源共享和用户间信息交换三个方面。

(1) 硬件资源共享。可以在全网范围内提供对处理资源、存储资源、输入输出资源等昂贵设备的共享,如巨型计算机、具有特殊功能的处理部件、高分辨率的激光打印机、大型绘图仪以及大容量的外部存储器等,从而使用户节省投资,也便于集中管理和均衡分担负荷。

(2) 软件资源共享。允许互联网上的用户远程访问各类大型数据库,可以得到网络文件传送服务、远地进程管理服务和远程文件访问服务,从而避免软件研制上的重复劳动以及数据资源的重复存贮,也便于集中管理。

(3) 用户间信息交换。计算机网络为分布在各地的用户提供了强有力的通信手段。用户可以通过计算机网络传送电子邮件、发布新闻消息和进行电子商务活动。

2. 计算机网络的应用

计算机网络在资源共享和信息交换方面所具有的功能,是其它系统所不能替代的。计算机网络所具有的高可靠性、高性能价格比和易扩充性等优点,使得它在工业、农业、交通运输、邮电通信、文化教育、商业、国防以及科学研究等各个领域、各个行业获得了越来越广泛的应用。计算机网络的应用范围实在太广泛,本节仅能涉及一些带有普遍意义和典型意义的应用领域。

(1) 办公自动化 OA (Office Automation)。办公自动化系统,按计算机系统结构来看是一个计算机网络,每个办公室相当于一个工作站。它集计算机技术、数据库、局域网、远距离通信技术以及人工智能、声音、图像、文字处理技术等综合应用技术之大成,是一种全新的信息处理方式。办公自动化系统的核心是通信,其所提供的通信手段主要为数据/声音综合服务、可视会议服务和电子邮件服务。

(2) 远程教育 (Distance Education)。远程教育是一种利用在线服务系统,开展学历或非学历教育的全新的教学模式。远程教育可以提供几乎大学中所有的课程,学员们通过远程教育,同样可得到正规大学从学士到博士的所有学位。这种教育方式,对于已从事工作而仍想完成高学位的人士特别有吸引力。

远程教育的基础设施是电子大学网络 EUN (Electronic University Network)。EUN 的主要作用是向学员提供课程软件及主机系统的使用,支持学员完成在线课程,并负责行政管理、合作协同等。这里所指的软件除系统软件之外,包括 CAI 课件,即计算机辅助教学 (Computer Aided Instruction) 软件。CAI 课件一般采用对话和引导式的方式指导学生学习,发现学生错误还具有回溯功能,从本质上解决了学生学习中的困难。

(3) 电子银行。电子银行也是一种在线服务系统,是一种由银行提供的基于计算机和计算机网络的新型金融服务系统。电子银行的功能包括:金融交易卡服务、自动存取款作业、销售点自动转账服务、电子汇款与清算等,其核心为金融交易卡服务。金融交易卡的诞生,标志了人类交换方式从物物交换、货币交换到信息交换的又一次飞跃。

围绕金融交易卡服务,产生了自动存取款服务,自动取款机 (CD) 及自动存取款机 (ATM) 也应运而生。自动取款机与自动存取款机大多采用联网方式工作,现已由原来的一行联网发展到多行联网,形成覆盖整个城市、地区,甚至全国的网络,全球性国际金融网络也正在建设之中。

电子汇款与清算系统可以提供客户转账、银行转账、外币兑换、托收、押汇信用证、行间证券交易、市场查证、借贷通知书、财务报表、资产负债表、资金调拨及清算处理等金融通信服务。由于大型零售商店等消费场所采用了终端收款机 (POS)，从而使商场内部的资金及时清算成为现实。销售点的电子资金转账是 POS 与银行计算机系统联网而成的。

当前电子银行服务又出现了智能卡 (IC)。IC 卡内装有微处理器、存储器及输入输出接口，实际上是一台不带电源的微型电子计算机。由于采用 IC 卡，持卡人的安全性和方便性大大提高了。

(4) 证券及期货交易。证券及期货交易由于其获利巨大、风险巨大，且行情变化迅速，投资者对信息的依赖显得格外重要。金融业通过在线服务计算机网络提供证券市场分析、预测、金融管理、投资计划等需要大量计算工作的服务，提供在线股票经纪人服务和在线数据库服务（包括最新股价数据库、历史股价数据库、股指数据库以及有关新闻、文章、股评等）。

(5) 校园网 (Campus Network)。校园网是在大学校园区内用以完成大中型计算机资源及其它网内资源共享的通信网络。一些发达国家已将校园网确定为信息高速公路的主要分支。无论在国内与国外，校园网的存在与否，是衡量该院校学术水平与管理水平的重要标志，也是提高学校教学、科研水平不可或缺的重要支撑环节。

共享资源是校园网最基本的应用，人们通过网络更有效地共享各种软、硬件及信息资源，为众多的科研人员提供一种崭新的合作环境。校园网可以提供异型机联网的公共计算环境、海量的用户文件存储空间、昂贵的打印输出设备、能方便获取的图文并茂的电子图书信息，以及为各级行政人员服务的行政信息管理系统和为一般用户服务的电子邮件系统。

(6) 企业网络。集散系统和计算机集成制造系统是两种典型的企业网络系统。

集散系统实质上是一种分散型自动化系统，又称做以微处理机为基础的分散综合自动化系统。集散系统具有分散监控和集中综合管理两方面的特征，而更将“集”字放在首位，更注重于全系统信息的综合管理。20 世纪 80 年代以来，集散系统逐渐取代常规仪表，成为工业自动化的主流。工业自动化不仅体现在工业现场，也体现在企业的事务行政管理上。集散系统的发展及工业自动化的需求，导致了一个更庞大、更完善的计算机集成制造系统 CIMS (Computer Integrated Manufacturing System) 的诞生。

集散系统一般分为三级：过程级、监控级与管理信息级。集散系统是将分散于现场的以微机为基础的过程监测单元、过程控制单元、图文操作站及主机（上位机）集成在一起的系统。它采用了局域网技术，将多个过程监控、操作站和上位机互连在一起，使通信功能增强，信息传输速度加快，吞吐量加大，为信息的综合管理提供了基础。因为 CIMS 具有提高生产率、缩短生产周期等一系列极具吸引力的优点，所以已经成为未来工厂自动化的方向。

(7) 智能大厦和结构化综合布线系统。智能大厦 (Intelligent Building) 是近十年来新兴的高技术建筑形式，它集计算机技术、通信技术、人类工程学、楼宇控制、楼宇设施管理于一身，使大楼具有高度的适应性（柔性），以适应各种不同环境与不同客户的需要。智能大厦是以信息技术为主要支撑的，这也是其具有“智能”之名称的由来。有人认为具有三 A 的大厦，可视为智能大厦。所谓三 A 就是 CA（通信自动化）、OA（办公自动化）和 BA（楼宇自动化）。概括起来，可以认为智能大厦除有传统大厦功能之外，主要必须具备下列基本构成要素：高舒适的工作环境、高效率的管理信息系统和办公自动化系统、先进的计算

机网络和远距离通信网络及楼宇自动化。

智能大厦及计算机网络的信息基础设施是结构化综合布线系统 SCS (Structure Cabling System)。在建设计算机网络系统时, 布线系统是整个计算机网络系统设计中不可分割的一部分, 它关系到日后网络的性能、投资效益、实际使用效果以及日常维护工作。结构化布线系统是指在一个楼宇或楼群中的通信传输网络能连接所有的语音、数字设备, 并将它们与交换系统相连, 构成一个统一、开放的结构化布线系统。在综合布线系统中, 设备的增减、工位的变动, 仅需通过跳线简单插拔即可, 而不必变动布线本身, 从而大大方便了管理、使用和维护。

1.3 计算机网络的分类

可以按许多不同的方法对计算机网络进行分类。

1.3.1 按拓扑类型分类

“拓扑”这个名词是从几何学中借用来的。网络拓扑是指网络形状, 或者是它在物理上的连通性。网络的拓扑结构主要有: 星形拓扑、总线拓扑、环形拓扑、树形拓扑、混合形拓扑及网形拓扑, 如图 1-4 所示。

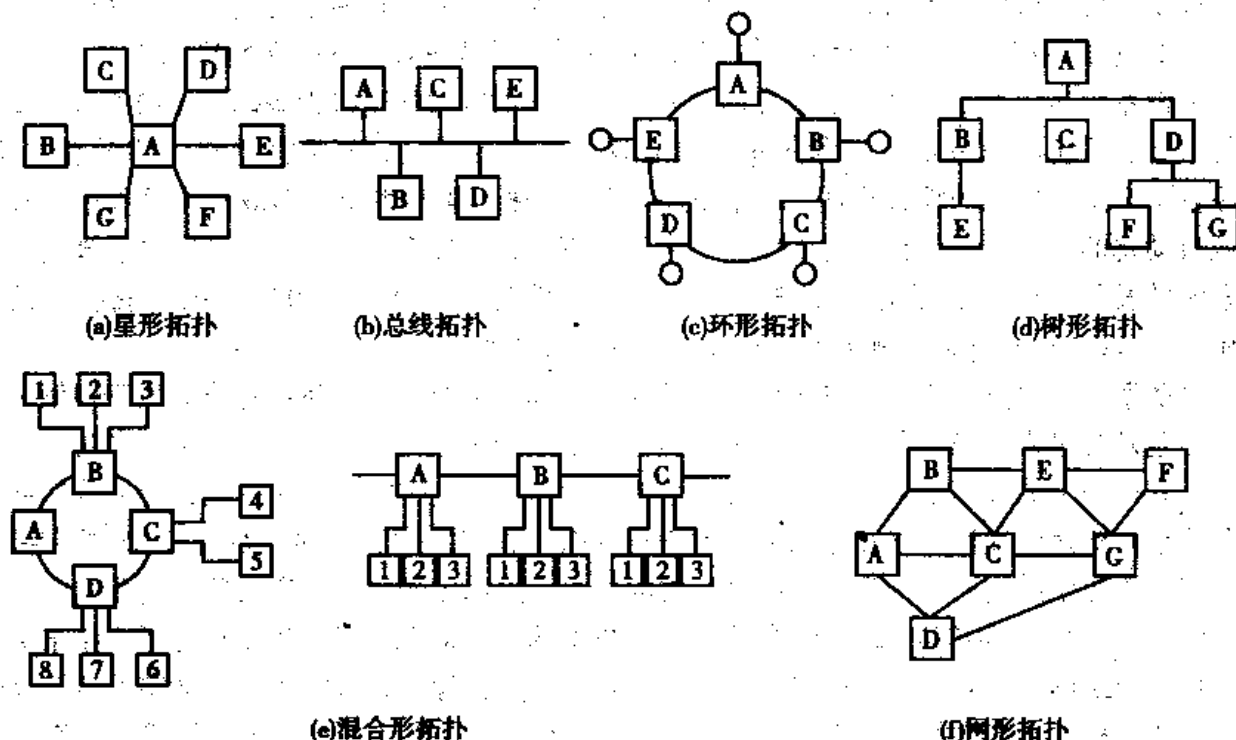


图 1-4 各种网络拓扑

拓扑结构的选择往往与传输介质的选择及介质访问控制方法的确定紧密相关。在选择网络拓扑结构时, 应该考虑的主要因素有下列几点:

(1) 可靠性。尽可能提高可靠性,以保证所有数据流能准确接收;还要考虑系统的可维护性,使故障检测和故障隔离较为方便。

(2) 费用。建网时需考虑适合特定应用的信道费用和安装费用。

(3) 灵活性。需要考虑系统在今后扩展或改动时,能容易地重新配置网络拓扑结构,能方便地处理原有站点的删除和新站点的加入。

(4) 响应时间和吞吐量。要为用户提供尽可能短的响应时间和最大的吞吐量。

网络拓扑可以根据通信子网中通信信道类型分为两类:

(1) 点一点线路通信子网的拓扑。

(2) 广播信道通信子网的拓扑。

在采用点一点线路的通信子网中,每条物理线路连接一对节点。采用点一点线路的通信子网的基本拓扑构型有4种:星形、环形、树形、网状形。

在采用广播信道的通信子网中,一个公共的通信信道被多个网络节点共享。采用广播信道通信子网的基本拓扑主要有4种:总线形、树形、环形、无线通信与卫星通信型。

以下是几种典型网络拓扑的特点。

1. 星形拓扑

星形拓扑是由中央节点和通过点到点通信链路接到中央节点的各个站点组成,中央节点往往是一个集线器,如图1-4(a)所示。中央节点执行集中式通信控制策略,因此中央节点相当复杂,而各个站点的通信处理负担都很小。

星形拓扑结构具有以下优点:

(1) 控制简单。在星形网络中,任何一站点只和中央节点相连接,因而介质访问控制方法很简单,致使访问协议也十分简单。易于网络的监控和管理。

(2) 故障诊断和隔离容易。在星形网络中,中央节点对连接线路可以逐一地隔离开来,进行故障检测和定位,单个连接点的故障只影响一个设备,不会影响全网。

(3) 方便服务。中央节点可方便地对各个站点提供服务和网络重新配置。

星形拓扑结构的缺点:

(1) 电缆长度和安装工作量可观。因为每个站点都要和中央节点直接连接,需要耗费大量的电缆,安装、维护的工作量也骤增。

(2) 中央节点的负担较重,形成“瓶颈”。一旦发生故障,则全网受影响,因而对中央节点的可靠性和冗余度方面的要求很高。

(3) 各站点的分布处理能力较低。

星形拓扑结构广泛应用于网络的智能集中于中央节点的场合。

2. 总线拓扑

总线拓扑结构采用一个广播信道作为传输介质,所有站点都通过相应的硬件接口直接连到这一公共传输介质上,该公共传输介质即称为总线。任何一个站发送的信号都沿着传输介质传播,而且能被所有其它站所接收。总线拓扑结构如图1-4(b)所示。

因为所有站点共享一条公用的传输信道,所以一次只能由一个设备传输信号。通常采用分布式控制策略来确定哪个站点可以发送。

总线拓扑结构的优点:

- (1) 总线结构所需要的电缆数量少。
- (2) 总线结构简单, 又是无源工作, 有较高的可靠性。
- (3) 易于扩充, 增加或减少用户比较方便。

总线拓扑结构的缺点:

- (1) 总线的传输距离有限, 通信范围受到限制。
- (2) 故障诊断和隔离较困难。
- (3) 分布式协议不能保证信息的及时传送, 不具有实时功能, 大业务量降低了网络速度。站点必须是智能的, 要有介质访问控制功能, 从而增加了站点的硬件和软件开销。

3. 环形拓扑

环形拓扑网络由站点和连接站点的链路组成一个闭合环, 如图 1-4 (c) 所示。每个站点能够接收从一条链路传来的数据, 并以同样的速率串行地把该数据沿环送到另一条链路上。这种链路可以是单向的, 也可以是双向的。数据以分组形式发送, 例如图中的 A 站希望发送一个报文到 C 站, 就先要把报文分成为若干个分组, 每个分组除了数据还要加上某些控制信息, 其中包括 C 站的地址。A 站依次把每个分组送到环上, 开始沿环传输, C 站识别到带有它自己地址的分组时, 便将其中的数据复制下来。由于多个设备连接在一个环上, 因此需要用分布式控制策略来进行控制。

环形拓扑的优点:

- (1) 电缆长度短。环形拓扑网络所需的电缆长度和总线拓扑网络相似, 但比星形拓扑网络要短得多。
- (2) 可使用光纤。光纤的传输速率很高, 十分适合于环形拓扑的单方向传输。
- (3) 所有计算机都能公平地访问网络的其它部分, 网络性能稳定。

环形拓扑的缺点:

- (1) 节点的故障会引起全网故障。这是因为环上的数据传输要通过接在环上的每一个节点, 一旦环中某一节点发生故障就会引起全网的故障, 故障检测困难。
- (2) 环节点的加入和撤出过程较复杂。
- (3) 环形拓扑结构的介质访问控制协议都采用令牌传递的方式, 在负载很轻时, 信道利用率相对来说就比较低。

4. 树形拓扑

树形拓扑可以看成是总线和星形拓扑的扩展, 形状像一棵倒置的树, 顶端是树根, 树根以下带分支, 每个分支还可再带子分支, 如图 1-4 (d) 所示。树根接收各站点发送的数据, 然后再用广播发送到全网。

树形拓扑的优点:

- (1) 易于扩展。这种结构可以延伸出很多分支和子分支, 这些新节点和新分支都能容易地加入网内。
- (2) 故障隔离较容易。如果某一分支的节点或线路发生故障, 很容易将故障分支与整个系统隔离开来。

树形拓扑的缺点是，各个节点对根的依赖性太大，如果根发生故障，则全网不能正常工作。从这一点来看，树形拓扑结构的可靠性有点类似于星形拓扑结构。

5. 混合形拓扑

将以上某两种单一拓扑结构混合起来，取两者的优点构成的拓扑称为混合形拓扑结构。如图 1-4 (e) 所示，一种是星形拓扑和环形拓扑混合成的“星—环”拓扑，另一种是星形拓扑和总线拓扑混合成的“星—总”拓扑。其实，这两种混合形拓扑在结构上有相似之处，若将总线结构的两个端点连在一起也就成了环形结构。这种拓扑的配置由一批接入环中或总线的集中器组成，由集中器再按星形结构连至每个用户站。

混合形拓扑的优点：

(1) 故障诊断和隔离较为方便。一旦网络发生故障，只要诊断出哪个集中器有故障，将该集中器和全网隔离即可。

(2) 易于扩展。要扩展用户时，可以加入新的集中器，也可在设计时，在每个集中器留出一些备用的可插入新的站点的连接口。

(3) 安装方便。网络的主电缆只要连通这些集中器，这种安装和传统的电话系统电缆安装很相似。

混合形拓扑的缺点：

(1) 需要选用带智能的集中器。这是为了实现网络故障自动诊断和故障节点的隔离所必需的。

(2) 像星形拓扑结构一样，集中器到各个站点的电缆安装长度会增加。

6. 网形拓扑

网形拓扑如图 1-4 (f) 所示。这种结构在广域网中得到了广泛的应用，它的优点是不受瓶颈问题和失效问题的影响。由于节点之间有许多条路径相连，可以为数据流的传输选择适当的路由，从而绕过失效的部件或过忙的节点。这种结构虽然比较复杂，成本也比较高，提供上述功能的网络协议也较复杂，但由于它的可靠性高，仍然受到用户的欢迎。

1.3.2 按网络的交换方式分类

按交换方式来分类，计算机网络可以分为电路交换网、报文交换网和分组交换网三种。

电路交换 (Circuit Switching) 方式类似于传统的电话交换方式，用户开始通信前，必须申请建立一条从发送端到接收端的物理信道，并且在双方通信期间始终占用该信道。

报文交换 (Message Switching) 方式的数据单元是要发送的一个完整报文，其长度并无限制。报文交换采用存储—转发原理，这有点像古代的邮政通信，邮件由途中的驿站逐个存储转发一样。报文中含有目的地址，每个中间节点要为途径的报文选择适当的路径，使其能最终到达目的端。

分组交换 (Packet Switching) 方式也称包交换方式，1969 年首次在 ARPANET 上使用，现在人们都公认 ARPANET 是分组交换网之父，并将分组交换网的出现作为计算机网络新时代的开始。采用分组交换方式通信前，发送端先将数据划分为一个个等长的单位（即分

组), 这些分组逐个由各中间节点采用存储—转发方式进行传输, 最终到达目的端。由于分组长度有限, 可以在中间节点机的内存中进行存储处理, 其转发速度大大提高。

1.3.3 按网络的覆盖范围分类

按地理分布范围来分类, 计算机网络可以分为广域网、局域网和城域网三种。

广域网 WAN (Wide Area Network) 也称远程网, 其分布范围可达数百至数千公里, 可覆盖一个国家或几个洲, 形成国际性的远程网络。广域网的通信子网可以利用公用分组交换网、卫星通信网和无线分组交换网。局域网 LAN (Local Area Network) 是将小区域内的各种通信设备互连在一起的网络, 其分布范围局限在一个办公室、一幢大楼或一个校园内, 用于连接个人计算机、工作站和各类外围设备以实现资源共享和信息交换。其主要特点是: 覆盖有限的地理范围; 提供高数据传输速率、低误码率的高质量数据传输环境。城域网 MAN (Metropolitan Area Network) 是分布范围介于局域网和广域网之间的一种高速网络, 满足几十公里范围内的大量企业、机关、公司的多个局域网互连的需求。其目的是在一个较大的地理区域内提供数据、声音和图像的传输。

1.3.4 按网络传输技术分类

网络所采用的传输技术有两类: 广播方式和点对点方式。因此, 相应的计算机网络也可以分为两类: 广播式网络 (Broadcast Network) 和点对点式网络 (Point-to-point Network)。

在广播式网络中, 所有联网计算机都共享一个公共信道。当一台计算机利用共享信道发送报文分组时, 所有其它计算机都会“收听”到这个分组。由于发送的分组中带有目的地址和源地址, 如果接收到该分组的计算机的地址与该分组的地址相同, 则接收该分组, 否则丢弃该分组。因此在广播式网络中, 发送的报文分组的地址可以有 3 类: 单播地址、多播地址和广播地址。

在点对点式网络中, 每条物理线路连接一对计算机。如果源节点与目的节点之间没有直接连接的线路, 那么源节点发送的分组就要通过中间节点的接收、存储与转发, 直至传输到目的节点。因此从源节点到目的节点可能存在多条路径, 决定分组从通信子网的源节点到达目的节点的路由需要有路由选择算法。采用分组存储转发和路由选择机制是点对点式网络与广播式网络的重要区别之一。

除了以上分类方法外, 还可按所采用的传输介质分为双绞线网、同轴电缆网、光纤网、无线网; 按信道的带宽分为窄带网和宽带网; 按不同用途分为科研网、教育网、商业网、企业网等。

1.4 计算机网络的标准化

随着计算机通信、计算机网络和分布式处理系统的剧增, 协议和接口的不断进化, 迫切要求在不同公司制造的计算机之间以及计算机与通信设备之间方便地互连和相互通信。由

此, 接口、协议、计算机网络体系结构都应有公共遵循的标准。国际标准化组织 (ISO) 以及国际上一些著名标准制定机构专门从事这方面标准的研究和制定。

1.4.1 国际标准化组织 (ISO)

ISO 是一个自发的不缔约组织, 由各技术委员会 (TC) 组成, 其中的 TC97 技术委员会专门负责制定有关信息处理的标准。1977 年, ISO 决定在 TC97 下成立一个新的分技术委员会 SC16, 以“开放系统互连”为目标, 进行有关标准的研究和制定。现在 SC16 改为 SC21, 负责七层模型中高四层及整个参考模型的研究。另一个与计算机网络有关的分技术委员会为 SC6, 它负责低三层的标准及与数据通信有关的标准制定。中国从 1980 年开始也参加了 OSI 的标准工作。

1.4.2 其它标准化机构

(1) 国际电信联盟 (ITU)。国际电话电报咨询委员会 CCITT, 现已改名为国际电信联盟 ITU (International Telecommunication Union), 主要负责有关通信标准的研究和制定, 其中 ITU-T (国际电信联盟电信标准化局) 下设有 15 个工作组, 分别负责某一具体电信技术的标准制定。ITU 标准主要用于国与国之间互连, 而在各个国家内部则可以有自己的标准。

(2) 美国国家标准局 (NBS)。NBS 是美国商业部的一个部门, 其研究范围较广, 包括 ISO 和 ITU 的有关标准, 研究目标是力争与国际标准一致。NBS 在美国已颁布了许多与 ISO 和 ITU 兼容或稍有改动的标准。

(3) 美国国家标准学会 (ANSI)。ANSI 是由制造商、用户通信公司组成的非政府组织, 是美国的自发标准情报交换机构, 也是由美国指定的 ISO 投票成员。它的研究范围与 ISO 相对应, 例如电子工业协会 (EIA) 是电子工业的商界协会, 也是 ANSI 成员, 主要涉及 OSI 的物理层标准的制定; 又如电气和电子工程师学会 (IEEE) 也是 ANSI 成员, 主要研究最低两层和局域网的有关标准。

(4) 欧洲计算机制造商协会 (ECMA)。ECMA 由在欧洲经营的计算机厂商组成, 包括某些美国公司的欧洲分部, 专门致力于有关计算机技术标准的协同开发。ECMA 发布它自己的标准, 这些标准对 ISO 的工作有着重大影响。

1.4.3 Internet 的组织机构

因特网体系结构局 IAB (Internet Architecture Board) 负责 Internet 策略和标准的最后仲裁。IAB 下设特别任务组 (Task Force), 其中最著名的是因特网工程特别任务组 (Internet Engineering Task Force, IETF)。它为 Internet 工程和发展提供技术及其它支持。它的任务之一是简化现存的标准并开发一些新的标准, 并向 Internet 工程指导小组 (Internet Engineering Steering Group, IESG) 推荐标准。

IETF 主要的工作领域: 应用程序、Internet 服务管理、运行要求、路由、安全性、传输、用户服务与服务应用程序。

IETF 又分为若干工作组 (Working Group)。Internet 有关的许多被称为“请求评注”(Request For Comments, RFC) 的技术文件大都出自于工作组。因特网的标准都有一个 RFC 编号, 如著名的 IP 协议和 TCP 协议文件最早分别为 RFC791 和 RFC793。但是并不是每个 RFC 文件都是因特网的标准。有的 RFC 文件只是提出一些新的思想和建议, 也可以对原有一些老的 RFC 文件进行增补和修订。

习 题

1. 计算机网络的发展可划分为哪几个阶段? 每个阶段各有什么特点?
2. 计算机网络可分为哪两大子网? 它们各实现什么功能?
3. 简述各种网络拓扑类型的优缺点。
4. 广播式网络与点对点式网络有何区别?
5. 局域网、广域网与城域网的主要特征是什么?
6. 早期的计算机网络中, 哪些技术对日后的发展产生了深远的影响?
7. 简述计算机网络的功能。
8. 缩写名词解释: PSE、PAD、NCC、FEP、IMP、PSTN、ADSL、DDN、FR、ATM、ISDN、VOD、WAN、LAN、MAN、OSI、ITU、IETF。

第2章 计算机网络体系结构

计算机网络体系结构是现代计算机网络的核心。本章分节介绍计算机网络体系结构与开放系统互连基本参考模型（OSI/RM）、TCP/IP 协议以及 OSI/RM 和 TCP/IP 的比较。

2.1 网络的分层体系结构

2.1.1 协议的要素

通过通信信道和设备互连起来的多个不同地理位置的计算机系统，要使其能协同工作以实现信息交换和资源共享，它们之间必须具有共同的语言。交流什么、怎样交流及何时交流，都必须遵循某种互相都能接受的规则。这些为计算机网络中进行数据交换而建立的规则、标准或约定的集合就称为网络协议（Protocol）。网络协议主要由下列三个要素组成：

- (1) 语义（Semantics）。涉及用于协调与差错处理的控制信息。
- (2) 语法（Syntax）。涉及数据及控制信息的格式、编码及信号电平等。
- (3) 定时（Timing）：涉及速度匹配和排序等。

2.1.2 分层体系结构

计算机网络系统是一个十分复杂的系统。将一个复杂系统分解为若干个容易处理的子系统，然后“分而治之”逐个加以解决，这种结构化设计方法是工程设计中常用的手段。分层就是系统分解的最好方法之一。

在如图 2-1 所示的一般分层结构中， n 层是 $n-1$ 层的用户，又是 $n+1$ 层的服务提供者。 $n+1$ 层虽然只直接使用了 n 层提供的服务，实际上它通过 n 层还间接地使用了 $n-1$ 层以及以下所有各层的服务。

层次结构的好处在于使每一层实现一种相对独立的功能。每一层不必知道下面一层是如何实现的，只要知道下层通过层间接口提供的服务是什么及本层向上层提供什么样的服务，就能独立地设计。系统经分层后，每一层次的功能相对简单且易于实现和维

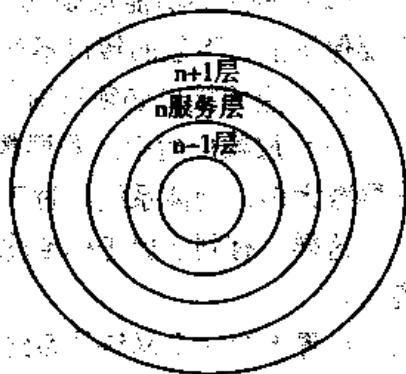


图 2-1 层次模型

护。此外，若某一层需要作改动或被替代时，只要不去改变它和上、下层的接口服务关系，则其它层次都不会受其影响，因此具有很大的灵活性。分层结构还有利于交流、理解和标准化。

计算机网络各层次结构模型及其协议的集合，称为网络的体系结构（Architecture）。体系结构是一个抽象的概念，它精确定义了网络及其部件所应实现的功能，但这些功能究竟用何种硬件或软件方法来实现则是一个具体实施的问题。换言之，网络的体系结构相当于网络的类型，而具体的网络结构则相当于网络的一个实例。

计算机网络都采用层次化的体系结构。由于计算机网络涉及多个实体间的通信，其层次结构一般以图 2-2 所示的垂直分层模型来表示。这种层次结构的要点可归纳如下：

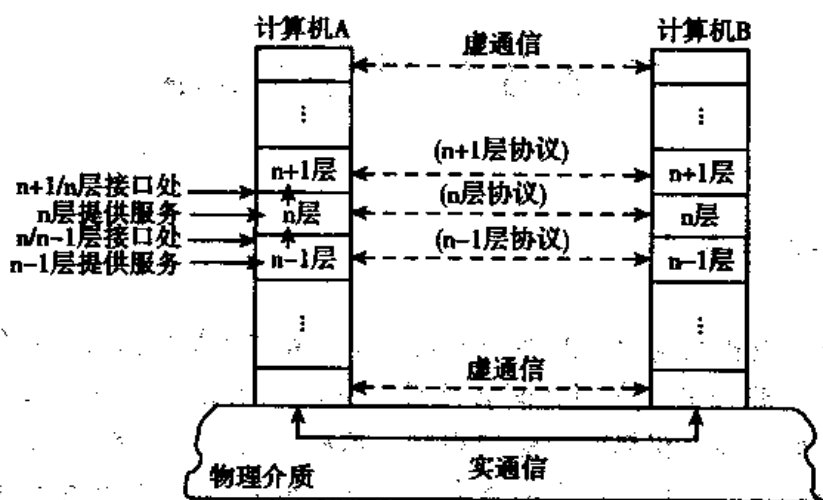


图 2-2 计算机网络的层次模型

- (1) 除了在物理介质上进行的是实通信之外，其余各对等实体间进行的都是虚通信。
- (2) 对等层的虚通信必须遵循该层的协议。
- (3) n 层的虚通信是通过 $n/n-1$ 层间接口处 $n-1$ 层提供的服务以及 $n-1$ 层的通信（通常也是虚通信）来实现的。

层次结构的划分，一般要遵循以下原则：

- (1) 每层的功能应是明确的，并且是相互独立的。当某一层的具体实现方法更新时，只要保持上、下层的接口不变，便不会对邻层产生影响。
- (2) 层间接口必须清晰，跨越接口的信息量应尽可能少。
- (3) 层数应适中。若层数太少，则多种功能混杂在一层中，造成每一层的协议太复杂；若层数太多，则体系结构过于复杂，使描述和实现各层功能变得困难。

这样，有利于促进标准化。这主要是因为每一层的功能和所提供的服务都已有了精确的说明。

世界上第一个网络体系结构是 IBM 公司于 1974 年提出的，命名为“系统网络体系结构 SNA”。在此之后，许多公司纷纷提出了各自的网络体系结构。这些网络体系结构共同之处在于它们都采用了分层技术，但层次的划分、功能的分配与采用的技术术语均不相同。随着信息技术的发展，各种计算机系统连网和各种计算机网络的互连成为人们迫切需要解决的课题。开放系统互连参考模型就是在这样一个背景下提出和研究的。

2.2 OSI/RM 开放系统互连参考模型

2.2.1 OSI/RM 简介

开放系统互连 (Open System Interconnection) 基本参考模型是由国际标准化组织 (ISO) 制定的标准化开放式计算机网络层次结构模型, 又称 ISO'S OSI 参考模型。“开放”这个词表示能使任何两个遵守参考模型和有关标准的系统进行互连。

OSI 包括了体系结构、服务定义和协议规范三级抽象。OSI 的体系结构定义了一个七层模型, 用以进行进程间的通信, 并作为一个框架来协调各层标准的制定; OSI 的服务定义描述了各层所提供的服务, 以及层与层之间的抽象接口和交互用的服务原语; OSI 各层的协议规范, 精确地定义了应当发送何种控制信息及用何种过程来解释该控制信息。需要强调的是, OSI 参考模型并非具体实现的描述, 它只是一个为制定标准而提供的概念性框架。在 OSI 中, 只有各种协议是可以实现的, 网络中的设备只有与 OSI 的有关协议相一致时才能互连。

2.2.2 OSI/RM 的结构

简而言之, OSI 参考模型将网络划分为七层, 如图 2-3 所示, OSI 七层模型从下到上分别为物理层 (Physical Layer, PH)、数据链路层 (Data Link Layer, DL)、网络层 (Network Layer, N)、传输层 (也称运输层) (Transport Layer, T)、会话层 (Session Layer, S)、表示层 (Presentation Layer, P) 和应用层 (Application Layer, A)。从图 2-3 中可见, 整个开放系统环境由作为信源和信宿的端开放系统及若干中继开放系统通过物理介质连接构成。这

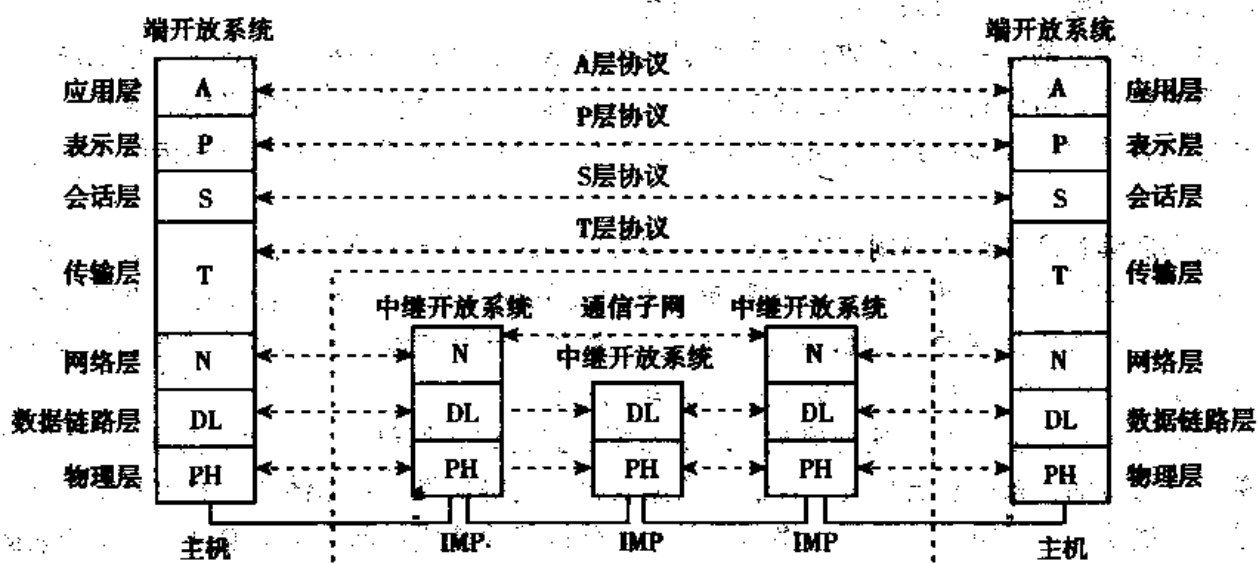


图 2-3 ISO'S OSI 参考模型

里的端开放系统和中继开放系统，都是国际标准 ISO 7498 中使用的术语。通俗地说，它们就相当于资源子网中的主机和通信子网中的节点机（IMP）。只有在主机中才可能需要包含所有七层的功能，而在通信子网中的 IMP 一般只需要最低三层甚至只要最低两层的功能就可以了。

层次结构模型中数据的实际传送过程如图 2-4 所示。图中发送进程发送给接收进程的数据，实际上是经过发送方各层从上到下传递到物理介质；通过物理介质传输到接收方后，再经过从下到上各层的传递，最后到达接收进程。

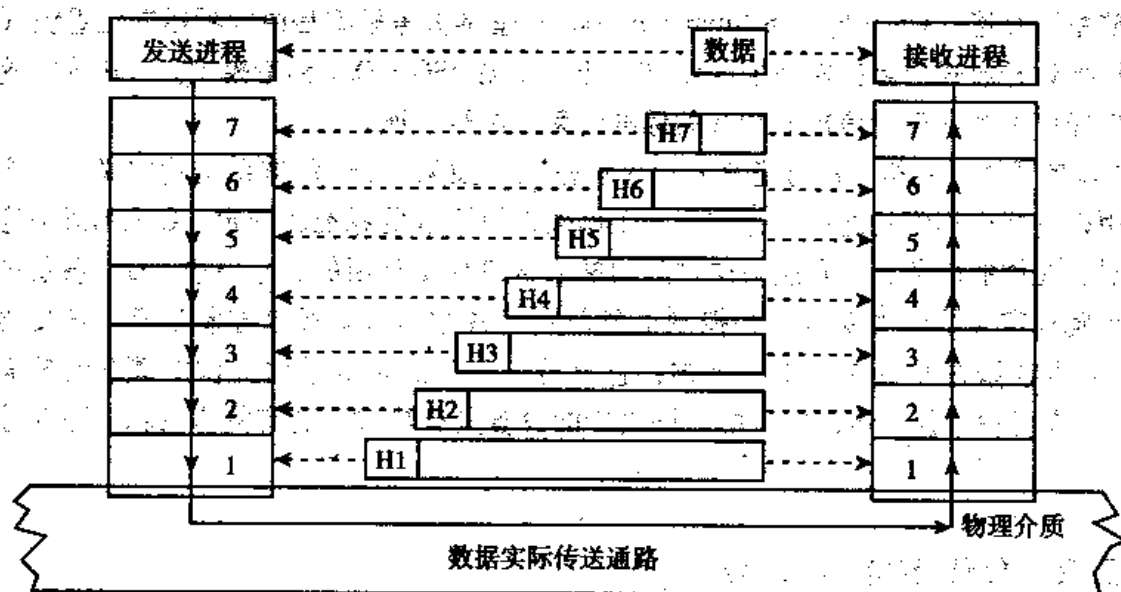


图 2-4 数据的实际传递过程

在发送方从上到下逐层传递的过程中，每层都要加上适当的控制信息，即图中的 H7、H6、……H1，它们统称为报头。到最底层成为由“0”或“1”组成的数据比特流，然后再转换为电信号在物理介质上传输至接收方。接收方在向上传递时过程正好相反，要逐层剥去发送方相应层加上的控制信息。这个过程，有点与邮政信件实际传递中要加信封、加邮袋、邮车等层层封装，再层层去掉封装的过程相类似。

由于接收方的某一层不会收到底下各层的控制信息，而高层的控制信息对于它来说又只是透明的数据，所以它只阅读和去除本层的控制信息，并进行相应的协议操作。这样，发送方和接收方的对等实体看到的信息是相同的，就好像这些信息通过虚通信直接传给了对方一样。

本书后续各章节将详细阐述网络各层要解决的问题，在此先简要介绍一下各层的功能：

(1) 物理层定义了为建立、维护和拆除物理链路所需的机械的、电气的、功能的和规程的特性，其作用是使原始的数据比特流能在物理介质上传输。具体涉及接插件的规格，“0”、“1”信号的电平表示，收发双方的协调等内容。

(2) 在数据链路层中，比特流被组织成数据链路协议数据单元（通常称为帧），并以其为单位进行传输，帧中包含地址、控制、数据及校验码等信息。数据链路层的主要作用是通过校验、确认和反馈重发等手段，将不可靠的物理链路改造成对网络层来说是无差错的数据链路。数据链路层还要协调收发双方的数据传输速率，即进行流量控制，以防止接收方因来不及处理发送方来的高速数据而导致缓冲器溢出及线路阻塞。

(3) 在网络层中, 数据以网络协议数据单元 (通常称为分组) 为单位进行传输。网络层关心的是通信子网的运行控制, 主要解决如何使数据分组跨越通信子网从源传送到目的地的问题。这就需要在通信子网中进行路由选择。另外, 为避免通信子网中出现过多的分组而造成网络阻塞, 需要对流入的分组数量进行控制。当分组要跨越多个通信子网才能到达目的地时, 还要解决网际互连的问题。

(4) 传输层是第一个端一端, 也即主机—主机的层次。传输层提供的端到端的透明数据传输服务, 使高层用户不必关心通信子网的存在, 由此用统一的传输原语书写的高层软件便可运行于任何通信子网上。传输层还要处理端到端的差错控制和流量控制问题。

(5) 会话层是进程—进程的层次, 其主要功能是组织和同步不同主机上各种进程间的通信 (也称为对话)。会话层负责在两个会话层实体之间进行对话连接的建立和拆除。在半双工情况下, 会话层提供一种数据权标来控制某一方何时有权发送数据。会话层还提供在数据流中插入同步点的机制, 使得数据传输因网络故障而中断后, 可以不必从头开始而仅重传最近一个同步点以后的数据。

(6) 表示层为上层用户提供共同的数据或信息语法表示变换。为了让采用不同编码方法的计算机在通信中能相互理解数据的内容, 可以采用抽象的标准方法来定义数据结构, 并采用标准的编码表示形式。表示层管理这些抽象的数据结构, 并将计算机内部的表示形式转换成网络通信中采用的标准表示形式。数据压缩/恢复和加密/解密也是表示层可提供的表示变换功能。

(7) 应用层是开放系统互连环境的最高层。不同的应用层为特定类型的网络应用提供访问 OSI 环境的手段。网络环境下不同主机间的文件传送访问和管理 (FTAM)、传送标准电子邮件的文电处理系统 (MHS)、使不同类型的终端和主机通过网络交互访问的虚拟终端 (VT) 协议等都属于应用层的范畴。

2.2.3 面向连接服务与无连接服务

1. 通信服务类型

通信服务可以分为两大类: 面向连接服务 (Connection-oriented Services) 和无连接服务 (Connectionless Services)。

面向连接服务和电话系统的工作模式相类似。其特点是: 数据传输过程前必须经过建立、连接、维护连接和释放连接的 3 个过程; 在数据传输过程中, 各分组不需要携带目的节点的地址。面向连接服务的传输连接类似于一个通信管道, 发送者在一端放入数据, 接收者从另一端取出数据。面向连接数据传输的收发数据顺序不变, 因此传输的可靠性好, 但需通信开始前的连接开销, 协议复杂, 通信效率不高。

无连接服务与邮政系统的信件投递过程相类似。其特点是: 每个分组都要携带完整的目的节点的地址, 各分组在通信子网中是独立传送的。因此, 无连接服务中的数据传输过程不需要经过建立连接、维护连接和释放连接的 3 个过程; 由于无连接服务中发送的不同分组可能选择不同路径到达目的节点, 先发送的不一定先到达, 因此无连接服务中的目的节点接收到的数据分组可能出现乱序、重复与丢失的现象。其可靠性不是很好, 但因其省去了建立连

接的开销和许多保证机制，因此通信协议相对简单，效率较高。

面向连接服务与无连接服务对实现服务的协议的复杂性与传输的可靠性有很大的影响。根据主机间数据传输的效率和可靠性要求不同，设计者可以选择面向连接服务与无连接服务的类型。网络的物理层、数据链路层、网络层和传输层都会涉及面向连接服务与无连接服务的问题。采用的服务类型不同，通信的可靠性与协议的复杂性也不相同。

2. 确认和重传机制

面向连接服务与无连接服务对数据传输可靠性有影响，但网络数据传输可靠性一般通过确认和重传机制保证。

确认是指数据分组接收节点在收到每个分组后，要求向发送节点回送正确接收分组的确认信息。在规定时间内，如果发送节点没有接收到接收节点返回的确认信息，就认为该数据分组发送失败，发送节点重传该数据分组。确认和重传机制可以提高数据传输的可靠性，但是它需要制定较为复杂的确认和重传协议，并且需要增加网络额外的通信开销，占用网络带宽。

当然，接收节点也可以不需要向发送节点发送接收数据分组的确认信息，发送节点也不需要重传协议。因此协议简单，不需要增加网络额外的通信开销，但是它是以降低传输的可靠性为代价的。

3. 服务类型和服务质量

面向连接服务可以同时要求采用确认和重传机制，提供最为可靠的服务；也可以不要求采用确认机制，这时数据传输服务的可靠性主要由面向连接服务来保证。同样，无连接服务也可以要求采用确认和重传机制，来提高数据传输的可靠性；无连接服务也可以采用不确认机制，但数据传输的可靠性较低。

在网络的各个层次的设计中，可以在面向连接与确认服务、面向连接与不确认服务、无连接与确认服务、无连接与不确认服务这4种情况中，根据不同的通信要求，决定选择不同的服务类型。

2.3 TCP/IP 参考模型

2.3.1 TCP/IP 简介

网络互连是目前网络技术研究的热点之一，并且已经取得了很大的进展。在诸多网络互连协议中，传输控制协议/互连网协议 TCP/IP (Transmission Control Protocol / Internet Protocol) 是一个使用非常普遍的网络互连标准协议。TCP/IP 协议是美国国防部高级计划研究局 DARPA 为实现 ARPANET (后来发展为 Internet) 互连网而开发的，也是很多大学及研究所经过多年的研究及商业化的结果。目前，众多的网络产品厂家都支持 TCP/IP 协议，TCP/IP 已成为一个事实上的工业标准。

Internet 上的 TCP/IP 协议之所以能迅速发展, 不仅仅是因为它是美国军方指定使用的协议, 更重要的是它恰恰适应了世界范围内数据通信的需要。TCP/IP 协议具有以下几个特点:

- (1) 开放的协议标准, 可以免费使用, 并且独立于特定的计算机硬件与操作系统。
- (2) 独立于特定的网络硬件, 可以运行在局域网、广域网, 更适用于互联网中。
- (3) 统一的网络地址分配方案, 使得整个 TCP/IP 设备在网中都具有惟一的地址。
- (4) 标准化的高层协议, 可以提供多种可靠的用户服务。

2.3.2 TCP/IP 的体系结构

协议分层模型包括两方面的内容: 一是层次结构, 二是各层功能的描述。在如何用分层模型来描述 TCP/IP 的问题上争论很多, 但共同的观点是 TCP/IP 的层次数比 OSI 参考模型的七层要少。图 2-5 给出了 TCP/IP 参考模型与 OSI 参考模型。

TCP/IP 参考模型可以分为 4 个层次: 应用层、传输层、互连层、主机—网络层。

其中, 应用层 (Application layer) 与 OSI 应用层相对应, 传输层 (Transport layer) 与 OSI 传输层相对应, 互连层 (Internet layer) 与 OSI 网络层相对应, 主机—网络层 (Host-to-Network layer) 与 OSI 数据链路层及物理层相对应。在 TCP/IP 参考模型中, 对 OSI 表示层、会话层没有对应的协议。

TCP/IP参考模型	OSI参考模型
应用层	应用层
	表示层
	会话层
传输层	传输层
互连层	网络层
主机—网络层	数据链路层
	物理层

图 2-5 TCP/IP 参考模型与 OSI 参考模型

TCP/IP 是一组协议的代名词, 它还包括许多别的协议, 组成了 TCP/IP 协议簇。一般来说, TCP 提供传输层服务, 而 IP 提供网络层服务。TCP/IP 的体系结构与 ISO 的 OSI 七层参考模型的对应关系如图 2-6 所示。

ISO'S OSI 参考模型	TCP/IP 协议簇				
5-7	TELNET	FTP	SMTP	DNS	其它
4	TCP		UDP		
3	IP	ICMP			
				ARP	RARP
2	Ethernet	ARPANET	PDN	其它	

图 2-6 TCP/IP 层次模型

在 TCP/IP 层次模型中, 主机—网络层是 TCP/IP 参考模型的最底层, 是 TCP/IP 的实现基础, 它包括 TCP/IP 赖以存在的各种通信网与 TCP/IP 之间的接口和物理网络协议, 这些

通信网络包括多种广域网如 ARPANET、MILNET 和 X.25 公用数据网, 以及各种局域网, 如 IEEE802.3 的 CSMA/CD、IEEE802.4 的 Token Bus 以及 IEEE 802.5 的 Token Ring 等。

在互连层中, IP 为互连网协议 (Internet Protocol)、ICMP 为互连网控制报文协议 (Internet Control Message Protocol)、ARP 为地址转换协议 (Address Resolution Protocol)、RARP 为反向地址转换协议 (Reverse ARP)。互连层的功能主要由 IP 来提供。除了提供端到端的分组分发功能外, IP 还提供了很多扩充功能。例如, 为了克服数据链路层对帧大小的限制, 网络层提供了数据分块和重组功能, 这使得很大的 IP 数据报能以较小的分组在网上传输。

互连层的另一个重要服务是在互相独立的局域网上建立互连网络, 即互连网。网间的报文分组来往根据它的目的 IP 地址通过路由器传到另一网络。

在传输层中, TCP 为传输控制协议、UDP 为用户数据报协议 (User Datagram Protocol)。这一层主要功能是负责应用进程之间的端一端通信; 它与 OSI 参考模型的传输层功能是相似的。TCP 提供可靠的字节流信道, UDP 提供不可靠的数据报传送信道。

在应用层中, SMTP 为简单邮件传送协议 (Simple Mail Transfer Protocol)、DNS 为域名服务 (Domain Name Service)、FTP 为文件传输协议 (File Transfer Protocol)、TELNET 为远程终端访问协议。

TCP/IP 协议本身的分层模型如图 2-7 所示。

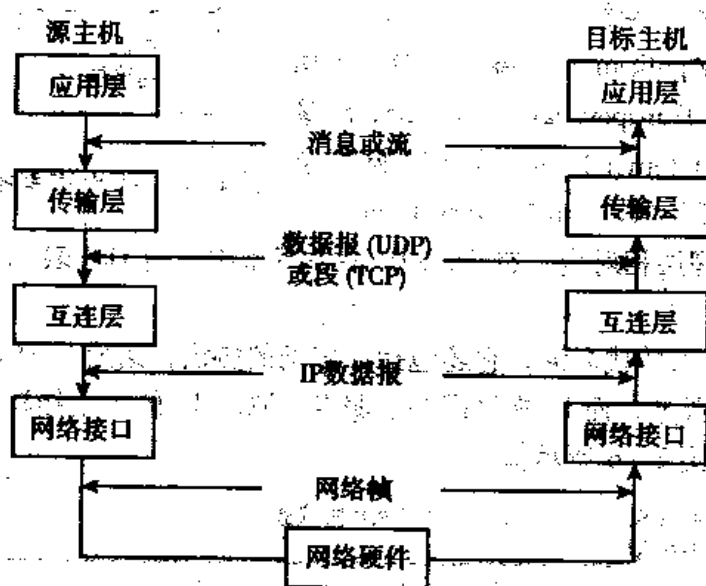


图 2-7 TCP/IP 协议层次

2.4 OSI/RM 与 TCP/IP 参考模型的比较

OSI 和 TCP/IP 参考模型有很多共同之处, 两者都以协议栈的概念为基础, 并且协议栈中的协议彼此相互独立, 而且两个模型中都采用了层次结构的概念, 各个层的功能也大体相似。例如, 在两个模型中, 传输层以及传输层以上的各层都为希望进行通信的进程提供了一种端到端的与网络无关的服务。除了这些基本的相似之处以外, 两个模型也有着许多不同的地方。

首先, OSI 模型有七层, 而 TCP/IP 只有四层, 它们都有网络层 (或者称互连网层)、传输层和应用层, 但其它的层并不相同。

其次, 在于无连接的和面向连接的通信范围有所不同。OSI 模型的网络层同时支持无连接和面向连接的通信, 但是传输层上只支持面向连接的通信。TCP/IP 模型的网络层只有一种模式即无连接通信, 但是在传输层上同时支持两种通信模式。

2.4.1 OSI 模型和协议的缺点

不管是 OSI 模型和协议, 还是 TCP/IP 模型及其协议, 都不是完美无缺的。对它们都有不少评论和批评意见。

OSI 参考模型和协议的设计者从工作的开始, 就试图建立一个全世界范围的计算机网络都要遵循的统一标准, 从技术角度希望追求一种完美的理想境界。在 20 世纪 80 年代末, 这个领域中的大多数专家都认为 OSI 模型及协议将会统领整个世界, 从而把所有其它的技术和标准都排除出局。但事实却与人们预想的相反, 这种情况并没有发生。

造成 OSI 协议不能流行的原因之一是模型和协议自身的缺陷。大多数人都认为 OSI 模型的层次数量与内容可能是最佳的选择, 其实并非如此, 其中的会话层和表示层这两层几乎是空的, 而另外的数据链路层和网络层包含内容太多, 有很多的子层插入, 每个子层都有不同的功能。OSI 模型以及相应的服务定义和协议都极其复杂, 它们很难实现, 有些功能, 例如编址、流控制和差错控制, 都会在每一层上重复出现, 这必然会降低系统的效率。

造成 OSI 协议不能流行的另一个原因是它的协议出现时机晚于 TCP/IP 协议。当 OSI 协议出现的时候, 与之竞争的 TCP/IP 协议已经被广泛地应用于大学和科研机构了。许多厂商已经在陆续地提供符合 TCP/IP 的相关产品, 这些厂商并不想再支持第二个协议栈。因此, OSI 模型和协议在它诞生之初, 就缺乏市场与商业动力, 也成为它没有能够达到预想目标的重要原因。

2.4.2 TCP/IP 模型和协议的缺点

TCP/IP 模型和协议也有自身的缺陷。首先, 该模型并没有清楚地区分哪些是规范、哪些是实现, TCP/IP 参考模型没有很好地做到这一点, 这使得在使用新技术来设计新网络的时候, TCP/IP 模型的指导意义显得不大, 而且 TCP/IP 模型不适合于其它非 TCP/IP 协议簇。

其次, TCP/IP 模型的主机—网络层并不是常规意义上的一层, 它是定义了网络层与数据链路层的接口。接口和层的区别是非常重要的, 而 TCP/IP 模型却没有将它们区分开来。

总体上, TCP/IP 协议在 20 世纪 70 年代诞生以来, 经实践检验其成功业绩已经赢得了大量的用户和投资。TCP/IP 协议的成功促进了 Internet 的蓬勃发展, Internet 的发展又进一步扩大了 TCP/IP 协议的影响。TCP/IP 不仅在学术界争取了一大批用户, 而且越来越受到计算机产业界的青睐。

相比之下, OSI 模型与协议显得有些曲高和寡。人们虽有良好的愿望, 指望网络标准化, 但 OSI 迟迟没有相对应的成熟产品推出, 也妨碍了第三方厂家开发相应的硬件和软件, 从而影响了 OSI 的发展。

习 题

1. 说明协议的基本含义，三要素的含义与关系。
2. 协议与服务有何区别？又有何关系？
3. 计算机网络采用层次结构模型的理由是什么？有何好处？
4. ISO 在制定 OSI/RM 时对层次划分所遵循的主要原则是什么？
5. 说明在 OSI/RM 中数据传输过程。
6. 请比较面向连接服务和无连接服务的异同点。
7. OSI/RM 的主要缺点是什么？
8. TCP/IP 协议的主要特点是什么？其主要缺点是什么？
9. 试比较 OSI/RM 与 TCP/IP 的异同点。

第3章 物理层

物理层位于 OSI 参考模型的最底层，它的主要功能是实现比特流的透明传输，为数据链路层提供数据传输服务。它直接面向实际承担数据传输的物理介质（即通信信道）。物理层的传输单位为比特（bit），即一个二进制位（“0”或“1”）。必须强调的是，物理层不是指具体的物理设备，也不是指信号传输的物理介质，而是指在物理介质之上为上一层（即数据链路层）提供一个传输原始比特流的物理连接。本章将介绍物理层接口与协议、传输介质、数据通信技术、数据编码以及数据交换技术。

3.1 物理层接口与协议

3.1.1 物理层接口

物理层上的协议有时也称为接口。物理层协议规定了与建立、维持及断开物理信道有关的特性，这些特性包括机械的、电气的、功能性的和规程性的四个方面。这些特性确保物理层能通过物理信道在相邻网络节点之间正确地收、发比特流信息，即确保比特流能送上物理信道，并且能在另一端取下它。物理层仅单纯关心比特流信息的传输，而不涉及比特流中各比特之间的关系（包括信息格式及其含义），对传输差错也不作任何控制。

ISO 对 OSI 模型的物理层所作的定义为：在物理信道实体之间合理地通过中间系统，为比特传输所需的物理连接的激活、保持和去除提供机械的、电气的、功能性和规程性的手段。比特流传输可以采用异步传输，也可以采用同步传输完成。

另外，ITU 在 X.25 建议书第一级（物理级）中也作了类似的定义：利用物理的、电气的、功能的和规程的特性在 DTE 和 DCE 之间实现对物理信道的建立、保持和拆除功能。这里的 DTE（Data Terminal Equipment）指的是数据终端设备，是对属于用户所有的连网设备或工作站的统称，它们是通信的信源或信宿，如计算机、终端等；DCE（Data Circuit-Terminating Equipment 或 Data Communications Equipment），指的是数据电路终接设备或数据通信设备，是对为用户提供入网连接点的网络设备的统称，如自动呼叫应答设备、调制解调器等。

DTE - DCE 的接口框图如图 3-1 所示，由图中可见物理层接口协议实际上是 DTE 和



图 3-1 DTE - DCE 接口框图

DCE 或其它通信设备之间的一组约定，主要解决网络节点与物理信道如何连接的问题。物理层协议规定了标准接口的机械连接特性、电气信号特性、信号的功能特性以及交换电路的规程特性，这样做的主要目的是为了便于不同的制造厂家能够根据公认的标准各自独立地制造设备，使各个厂家的产品都能相互兼容。

3.1.2 物理层的功能和提供的服务

1. 机械特性

DTE 与 DCE 之间的接口，首先涉及从机械上分界的问题。DTE 与 DCE 之间通过多根导线相互连系，DTE、DCE 作为两种分立的设备通常采用连接器实现机械上的互连，即一种设备的引出导线连接插头，另一种设备的引出导线连接插座，然后通过插头、插座将两种设备连接起来。为了使不同厂家生产的 DTE、DCE 设备便于连接，物理层的机械特性对插头和插座的几何尺寸、插针或插孔芯数及其排列方式、锁定装置形式等作了详细的规定。

图 3-2 列出了各类已被 ISO 标准化了的 DCE 连接器的几何尺寸及插孔芯数和排列方式。一般来说，DTE 的连接器常用插针形式，其几何尺寸与 DCE 连接器相配合，插针芯数和排列方式与 DCE 连接器成镜像对称。

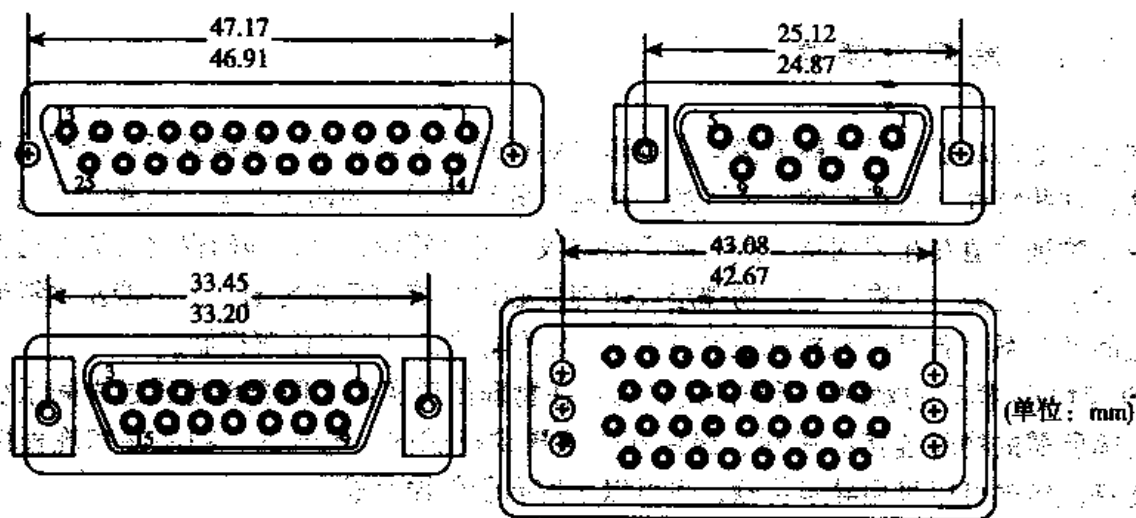


图 3-2 常用连接器机械特性

2. 电气特性

DTE 与 DCE 之间有多根导线相连，这些导线中除了地线以外，其它信号线均有方向性。物理层的电气特性规定了这组导线的电气连接及有关电路的特性，一般包括：接收器和发送器电路特性的说明，表示信号状态的电压/电流电平的识别、最大数据传输速率的说明，以及与互连电缆相关的规则等。

DTE 与 DCE 接口的各根导线（也称电路）的电气连接方式有非平衡方式、采用差动接收器的非平衡方式和平衡方式三种。

(1) 非平衡方式。采用分立元件技术设计的非平衡接口，每个电路使用一根导线，收

发两个方向共用一根信号地线，信号速率 ≤ 20 Kbps，传输距离 ≤ 15 米。由于使用共用信号地线，所以会产生比较大的串扰。ITU V. 28 建议采用这种电气连接方式，EIA RS-232C 标准基本与之兼容。

(2) 采用差动接收器的非平衡方式。这类采用集成电路技术设计的非平衡接口，与前一种方式相比，发送器仍使用非平衡式，但接收器使用差动接收器。每个电路使用一根导线，但每个方向都使用独立的信号地线，使串扰信号较小。这种方式的信号速率可达 300Kbps，传输距离为 10m (≤ 300 Kbps 时) ~ 1000m (≤ 3 Kbps 时)。ITU V. 10/X. 26 建议采用这种电气连接方式，EIA RS-423 标准与之兼容。

(3) 平衡方式。采用集成电路技术设计的平衡接口，使用平衡式发送器和差动式接收器，每个电路采用两根导线，构成各自完全独立的信号回路，使得串扰信号减至最小。这种方式的信号速率 ≤ 10 Mbps，传输距离为 10 米 (≤ 10 Mbps 时) ~ 1000 米 (≤ 100 Kbps 时)。ITU V. 11/X. 27 建议采用这种电气连接方式，EIA RS-422 标准与之兼容。

图 3-3 给出这三种电气连接方式的结构。

物理层的电气特性还规定了 DTE-DCE 接口线的信号电平、发送器的输出阻抗、接收器的输入阻抗等电气参数。

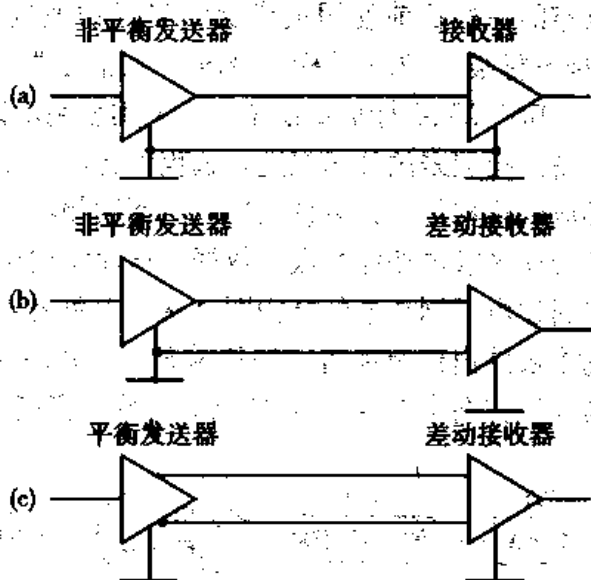


图 3-3 电气连接方式

3. 信号的功能特性

物理层的功能特性规定了接口信号的来源、作用以及与其它信号之间的关系。接口信号线按功能一般可分为数据信号线、控制信号线、定时信号线和接地线等四类。信号线的名称可以采用数字、字母组合或英文缩写三种方式来命名。

ITU V. 24 建议采用数字命名法，用于 DTE-DCE 接口时，信号线名称均为“1××”，故也称其为 100 系列接口信号线；用于 DTE-ACE (Automatic Calling Equipment, 自动呼叫设备) 接口时，信号线名称均为“2××”，故也称其为 200 系列接口信号线。EIA RS-232C 采用字母组合命名法，EIA RS-449 采用英文缩写命名法。

4. 规程特性

物理层的规程特性规定了使用交换电路进行数据交换的控制步骤，这些控制步骤的应用使得比特流传输得以完成。

目前由 ITU 建议在物理层使用的规程有 V. 24、V. 25、V. 54 等 V 系列标准，以及 X. 20、X. 20 bis、X. 21、X. 21 bis 等 X 系列标准，它们分别适用于各种不同交换电路中。物理层中较重要的新规程是 EIA RS-449 及 X. 21，然而经典的 EIA RS-232C 仍是目前最常用的计算机异步通信接口。

3.1.3 物理层协议举例

1. EIA RS-232C 接口标准

EIA RS-232C 是由美国电子工业协会 EIA (Electronic Industry Association) 在 1969 年颁布的一种目前使用最广泛的串行物理接口标准。RS (Recommended Standard) 的意思是“推荐标准”，232 是标识号码，而后缀“C”则表示该推荐标准已被修改过的次数。

RS-232C 标准提供了一个利用公用电话网络作为传输介质，并通过调制解调器将远程设备连接起来的技术规定。远程设备与电话网相连接时，通过调制解调器将数字数据转换成相应的模拟信号，以使其能与电话网相容；在通信线路的另一端，另一个调制解调器将模拟信号逆转换成相应的数字数据，从而实现比特流的传输。图 3-4 (a) 给出了两台远程计算机通过电话网相连的结构图。从图中可看出，DTE 实际上是数据的信源或信宿，而 DCE 则完成数据由信源到信宿的传输任务。RS-232C 标准接口只控制 DTE 与 DCE 之间的通信，与连接在两个 DCE 之间的电话网没有直接的关系。

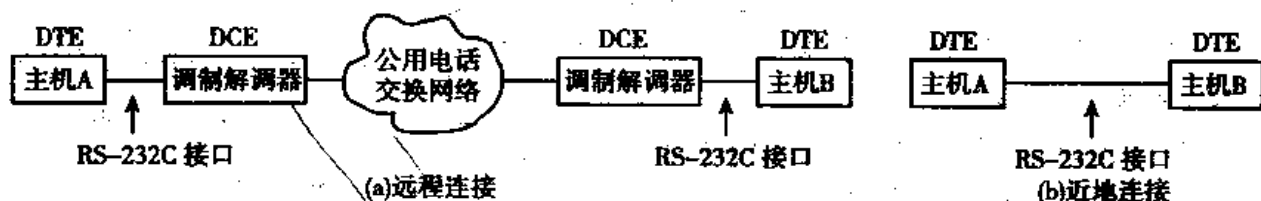


图 3-4 RS-232C 的远程连接和近地连接

RS-232C 标准接口也可如图 3-4 (b) 所示用于直接连接两台近地设备，此时既不使用电话网也不使用调制解调器。由于这两个设备必须分别以 DTE 和 DCE 方式成对出现才符合 RS-232C 标准接口的要求，所以在这种情况下要借助于一种采用交叉跳接信号线方法的连接电缆，使得连接在电缆两端的 DTE 通过电缆看对方都好像是 DCE 一样，从而满足 RS-232C 接口需要 DTE-DCE 成对使用的要求。这根连接电缆也称作零调制解调器 (Null Modem)。

RS-232C 的机械特性规定使用一个 25 芯的标准连接器，并对该连接器的尺寸及针或孔芯的排列位置等都作了详细说明。顺便提一下，实际的用户并不一定需要用到 RS-232C 标准的全集，这在个人计算机 (PC) 高速普及的今天尤为特殊，所以一些生产厂家为 RS-232C 标准的机械特性作了变通的简化，使用了一个 9 芯标准连接器将不常用的信号线舍弃。

RS-232C 的电气特性规定逻辑“1”的电平为 -15 至 -5 伏，逻辑“0”的电平为 +5 至 +15 伏，也即 RS-232C 采用 ± 15 伏的负逻辑电平， ± 5 伏之间为过渡区域不作定义。RS-232C 接口的电气特性见图 3-5，其电气信号表示见表 3-1。

RS-232C 电平高达 ± 15 伏，较之 0~5 伏的 TTL 电平来说具有更强的抗干扰能力。但是，即使使用这样高的电平，若两设备利用 RS-232C 接口直接相连（即不使用调制解调器），它们的最大距离也仅约 15 米，而且由于电平较高，通信速率反而受影响。RS-232C 接口的通信速率 $\leq 20\text{Kbps}$ （标准速率有 150、300、600、1200、2400、4800、9600、19200bps 等几档）。

表 3-1 RS-232C 电气信号表示

	负电平	正电平
逻辑状态	1	0
信号状态	传号	空号
功能状态	OFF (断)	ON (通)

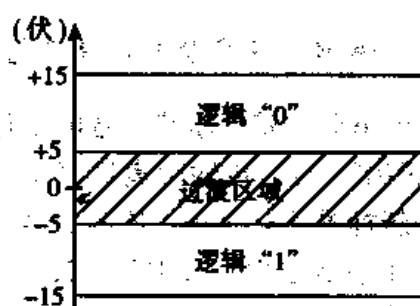


图 3-5 RS-232C 电气特性

RS-232C 的功能特性定义了 25 芯标准连接器中的 20 根信号线，其中 2 根地线、4 根数据线、11 根控制线、3 根定时信号线、剩下的 5 根线作备用或未定义。表 3-2 给出了其中最常用的 10 根信号线的功能特性。

表 3-2 RS-232C 功能特性

引脚编号	信号线名称	功能说明	信号线类型	连接方向
1	AA	保护地线 (GND)	地线	
2	BA	发送数据 (TD)	数据线	→DCE
3	BB	接收数据 (RD)	数据线	→DTE
4	CA	请求发送 (RTS)	控制线	→DCE
5	CB	清除发送 (CTS)	控制线	→DTE
6	CC	数据设备就绪 (DSR)	控制线	→DTE
7	AB	信号地线 (Sig. GND)	地线	
8	CF	载波检测 (CD)	控制线	→DTE
20	CD	数据终端就绪 (DTR)	控制线	→DCE
22	CE	振铃指示 (RI)	控制线	→DTE

RS-232C 的 DTE-DCE 连接如图 3-6 所示。

若两台 DTE 设备，如两台计算机在近距离直接连接，则可采用图 3-7 的方法，图中 (a) 为完整型连接，(b) 为简单型连接。

RS-232C 的工作过程是在各根控制信号线有序的“ON”（逻辑“0”）和“OFF”（逻辑“1”）状态的配合下进行的。在 DTE-DCE 连接的情况下，只有当 CD（数据终端就绪）和 CC（数据设备就绪）均为“ON”状态时，才具备操作的基本条件；此后，若 DTE 要发送数据，则须先将 CA（请求发送）置为“ON”状态，等待 CB（清除发送）应答信号为“ON”状态后，才能在 BA（发送数据）上发送数据。

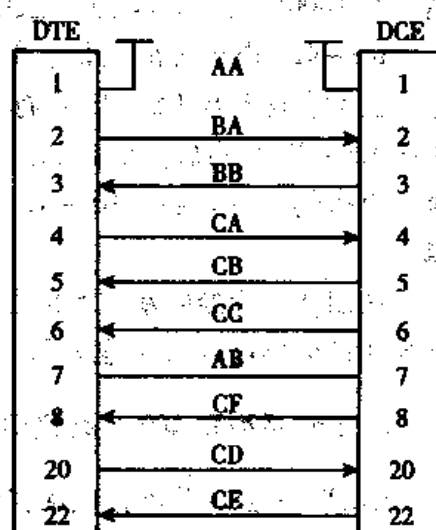


图 3-6 DTE-DCE 连接

2. EIA RS-449 及 RS-422 与 RS-423 接口标准

由于 RS-232C 标准信号电平过高, 采用非平衡发送和接收方式, 所以存在传输速率低 ($\leq 20\text{Kbps}$), 传输距离短 (≤ 15 米)、串扰信号较大等缺点。1977 年年底, EIA 颁布了一个新标准 RS-449, 次年, 这个接口标准的两个电气子标准: RS-423 (采用差动接收器的非平衡方式) 和 RS-422 (平衡方式) 也相继问世。这些标准在保持与 RS-232C 兼容的前提下, 重新定义了信号电平, 并改进了电路方式, 以达到较高的传输速率和较大的传输距离。

RS-449 对标准连接器作了详细的说明, 由于信号线较多, 使用了 37 芯和 9 芯连接器, 37 芯连接器定义了与 RS-449 有关的所有信号, 而辅信道的信号在 9 芯连接器中定义。

RS-449 标准的电气特性有两个子标准, 即平衡式的 RS-422 标准和非平衡式的 RS-423 标准。

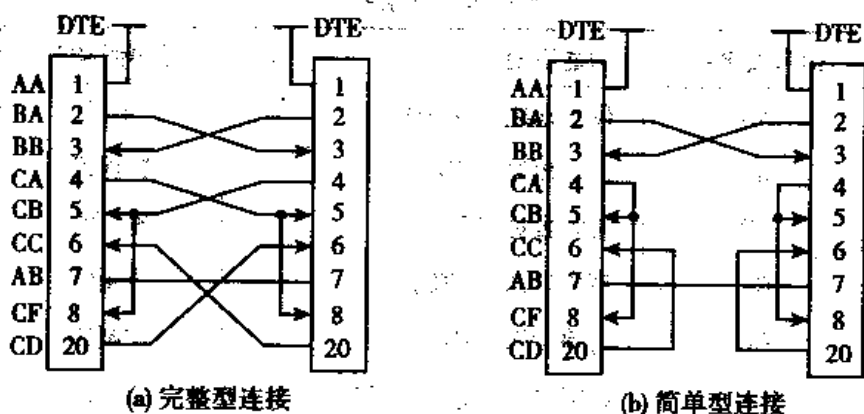


图 3-7 RS-232 的 DTE-DTE 连接

RS-422 电气标准是平衡方式标准, 它的发送器、接收器分别采用平衡发送器和差动接收器, 由于采用完全独立的双线平衡传输, 抗串扰能力大大增强。又由于信号电平定义为 ± 6 伏 (± 2 伏为过渡区域) 的负逻辑, 故当传输距离为 10m 时, 速率可达 10Mbps; 而距离增长至 1000m 时, 速率仍可达到 100Kbps, 性能远远优于 RS-232C 标准。

RS-423 电气标准是非平衡标准, 它采用单端发送器 (即非平衡发送器) 和差动接收器。虽然发送器与 RS-232C 标准相同, 但由于接收器采用差动方式, 所以传输距离和速率仍比 RS-232C 有较大的提高。当传输距离为 10m 时, 速率可达 100Kbps; 距离增至 100m 时, 速率仍有 10Kbps。RS-423 的信号电平定义为 ± 6 伏 (其中 ± 4 伏为过渡区域) 的负逻辑。

从旧技术标准向新技术标准的过渡, 需要花费巨大的代价和经过漫长的过程。RS-423 电气特性标准可以认为是从 RS-232C 向 RS-449 标准全面过渡过程中的一个台阶。

3. 100 系列和 200 系列接口标准

CCITT 是原国际电报电话咨询委员会的简称, 现已更名为国际电信联盟电信标准化局。该组织从事有关通信标准的研究和制定, 其标准一般都称作建议。

ITU V. 24 建议中有关 DTE-DCE 之间的接口标准有 100 系列、200 系列两种。100 系列

接口标准作为 DTE 与不带自动呼叫设备的 DCE (如调制解调器) 之间的接口。在设置自动呼叫设备的 DCE (如网络控制器) 中, 则由 200 系列接口标准完成 DTE 与自动呼叫设备的接口。若系统采用人工呼叫, 则无须设置 200 系列接口。

100 系列接口标准的机械特性采用两种规定, 当传输速率为 200bps ~ 9600bps 时, 采用 25 芯标准连接器; 传输速率达 48Kbps 时, 采用 34 芯标准连接器。200 系列接口标准则采用 25 芯标准连接器。

100 系列接口标准的电气特性采用 V. 28 和 V. 35 两种建议。当传输速率为 200bps ~ 9600bps 时, 采用 V. 28 建议; 当传输速率为 48Kbps 时, 100 系列中除控制信号仍使用 V. 28 建议外, 数据线与定时线均采用 V. 35 建议。200 系列标准接口的电气特性则采用 V. 28 建议。

4. X. 21 和 X. 21 bis 建议

ITU 对 DTE 与 DCE 的接口标准有 V 系列和 X 系列两大类建议。V 系列接口标准 (如前述的 V. 24 建议) 一般指数据终端设备与调制解调器或网络控制器之间的接口, 这类系列接口除了用于数据传输的信号线外, 还定义了一系列控制线, 是一种比较复杂的接口。X 系列接口标准是较晚制定的, 这类接口适用于公共数据网的室内电路终接设备和数据终端设备之间的接口, 定义的信号线很少, 因此是一种比较简单的接口。

X. 21 建议是 ITU 于 1976 年制定的一个用户计算机的 DTE 如何与数字化的 DCE 交换信号的数字接口标准。X. 21 建议的接口以相对来说比较简单的方式提供了点一点式的信息传输, 通过它能实现完全自动的过程操作, 并有助于消除传输差错。在数据传输过程中, 任何比特流 (包括数据与控制信号) 均可通过该接口进行传输。ISO 的 OSI 参考模型建议采用 X. 21 作为物理层规约的标准。

X. 21 的设计目标之一是要减少信号线的数目, 其机械特性采用 15 芯标准连接器代替熟悉的 25 芯连接器, 而且其中仅定义了 8 条接口线。

X. 21 的另外一个设计目标是允许接口在比 EIA RS-232C 更长的距离上进行更高速率的数据传输, 其电气特性类似于 EIA RS-422 的平衡接口, 支持最大的 DTE-DCE 电缆距离是 300m。X. 21 可以按同步传输的半双工或全双工方式运行, 传输速率最大可达 10Mbps。X. 21 接口适用于由数字线路 (而不是模拟线路) 访问公共数据网 (PDN) 的地区。欧洲网络大多使用 X. 21 接口。

若数字信道一直延伸到用户端, 用户的 DTE 当然就可以通过 X. 21 建议的接口进行远程通信。但目前实际连接用户端的大多数仍为模拟信道 (如电话线), 且大多数计算机和终端设备上也只具备 RS-232C 接口或以 V. 24 为基础的设备, 而不是 X. 21 接口。为了使从旧的网络技术转到新的 X. 21 接口更容易些, ITU 提出了用于公共数据网中的与 V 系列调制解调器接口的 X. 21 bis 建议。这里的 “bis” 是法语 “替换物” 的意思。

X. 21 bis 标准指定使用 V. 24/V. 28 接口, 它们与 EIA RS-232D 非常类似。美国的大多数公共数据网应用实际上都使用 EIA RS-232D (或更早的 RS-232C) 作为物理层接口。可以认为, X. 21 bis 是 X. 21 的一个暂时过渡版本, 它是对 X. 21 的补充并保持了 V. 24 的物理接口。X. 25 建议允许采用 X. 21 bis 作为其物理层的规程。

X. 21 和 X. 21 bis 为三种类型的服务定义了物理电路, 这三种服务是租用电路 (专用

线)服务、直接呼叫服务和设备地址呼叫服务。租用电路设计成在两个终端之间的连续连接;直接呼叫服务像“热线”电话,可使用户在任何时间直接连接指定的目标;设备地址呼叫则如“拨号”电话,每次连接需由用户呼叫指定目标。

3.2 传输介质

传输介质是通信网络中发送方和接收方之间的物理通路,计算机网络中采用的传输介质可分为有线和无线两大类。双绞线、同轴电缆和光纤是常用的三种有线传输介质;无线电通信、微波通信、红外通信以及激光通信的信息载体都属于无线传输介质。

传输介质的特性对网络数据通信质量有很大影响,这些特性是:

(1) 物理特性。说明传输介质的特征。

(2) 传输特性。包括信号形式、调制技术、传输速率及频带宽度等内容。

(3) 连通性。采用点到点连接还是多点连接。

(4) 地理范围。网上各点间的最大距离。

(5) 抗干扰性。防止噪音、电磁干扰对数据传输影响的能力。

(6) 相对价格。以元件、安装和维护的价格为基础。

下面分别介绍几种常用的传输介质的特性。

3.2.1 双绞线

由螺旋状扭在一起的两根、四根或八根绝缘导线组成,线对扭在一起可以减少相互间的辐射电磁干扰。双绞线是最常用的传输介质,早就用于电话通信中的模拟信号传输,也可用于数字信号的传输。

双绞线芯一般是铜质的,能提供良好的传导率。既可以用于传输模拟信号也可以用于传输数字信号。对于模拟信号来说,大约每5~6公里需要一个放大器;对于数字信号来说,每2~3公里使用一个中继器。双绞线分为两种:无屏蔽的和屏蔽的。无屏蔽双绞线(UTP, Unshielded Twist Pair)就像普通电话线一样,使用方便,价格便宜,但易受外部电磁场的干扰。屏蔽双绞线(STP, Shielded Twist Pair)是用铝箔将双绞线屏蔽起来,以减少受干扰,但价格贵于无屏蔽双绞线。电子工业协会 EIA 为无屏蔽双绞线订立了标准,3 类线(Category 3)能承载 16MHz,5 类线(Category 5)能承载 100MHz,随着千兆、10G 以太网网络设备的发展,6 类综合布线已经成为目前综合布线的主流。6 类和随后的 7 类,它们可承载更高的带宽信号。

3.2.2 同轴电缆

同轴电缆也像双绞线一样由一对导体组成,但它们是按“同轴”形式构成线对,其结构如图 3-8 所示。最里层是内芯,向外依次为绝缘层、屏蔽层,最外则是起保护作用的塑料外套,内芯和屏蔽层构成一对导体。

同轴电缆分为基带同轴电缆(阻抗 50Ω)和宽带同轴电缆(阻抗 75Ω)。基带同轴电缆

又可分为粗缆和细缆两种，都用于直接传输数字信号；宽带同轴电缆用于频分多路复用的模拟信号传输，也可用于不使用频分多路复用的高速数字信号和模拟信号传输。闭路电视所使用的 CATV 电缆就是宽带同轴电缆。

单根同轴电缆的直径约为 1.02~2.54 厘米，可在较宽的频率范围内工作。基带同轴电缆主要用于数字信号传输，并使用曼彻斯特编码，数据传输速率取决于传输距离，1km 距离时可达 10Mbps。宽带同轴电缆既可用于模拟信号传输又可用于数字信号传输，对于模拟信号，带宽最高可达 900MHz。一般，在 CATV 电缆上，每个电视通道分配 6MHz 带宽，每个广播通道需要的带宽要窄得多，因此在同轴电缆上使用频分多路复用技术可以支持大量的视频、音频通道。

同轴电缆适用于点到点和多点连接。基带 50Ω 电缆每段可支持几百台设备，在大系统中还可以用转接器将各段连接起来；宽带 75Ω 电缆可以支持数千台设备。

传输距离取决于传输的信号形式和传输的速率，典型基带电缆的最大距离限制在几公里，在同样数据速率条件下，粗缆的传输距离较细缆的长。宽带电缆的传输距离可达几十公里，同轴电缆的抗干扰性能比双绞线强。安装同轴电缆的费用比双绞线贵，但比光导纤维便宜。

3.2.3 光纤

光纤是光导纤维的简称，它由能传导光波的超细石英玻璃纤维外加保护层构成。多条光纤组成一束，就构成一条光缆。相对于金属导线来说具有重量轻、线径细的特点。

用光纤传输电信号时，在发送端先要将其转换成光信号，而在接收端又要由光检测器还原成电信号。光纤的电信号传送过程如图 3-9 所示。

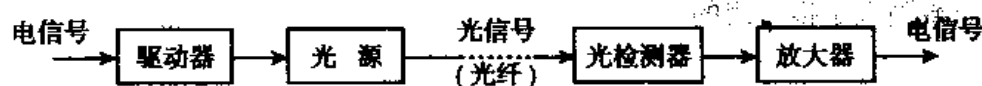


图 3-9 光纤的电信号传送过程

光源可以采用发光二极管 LED (Light Emitting Diode) 和注入型激光二极管 ILD (Injection Laser Diode)。发光二极管 LED 是一种价格较便宜的固态器件，电流通过时就产生可见光，但定向性较差，是通过在光纤石英玻璃介质内不断反射而向前传播的，这种光纤称为多模光纤 (Multimode Fiber)；注入型激光二极管 ILD 也是一种固态器件，它根据激光器原理进行工作，即以激励量子电子效应来产生一个窄带的超辐射光束，产生的是激光。由于激光的定向性好，它可沿着光导纤维直接传播，减少了折射和损耗，效率更高，也能传播更大的距离，而且可以保持很高的数据传输率，这种光纤称为单模光纤 (Single Mode Fiber)。

在接收端用来把光波转换为电能的检波器是一个光电二极管，目前常用的两种固态器件是 PIN 检波器和 APD 检波器。PIN 光电二极管是在二极管的 P 层和 N 层之间增加一小段纯

(I) 硅：雪崩光电二极管 (APD) 的外部特性和 PIN 类似，但是使用了较强的电场。PIN 的价格便宜，但是不如 APD 灵敏。

对光载波的调制属于移幅键控法 ASK，也称亮度调制 (Intensity Modulation)。典型的做法是在给定的频率下，以光的出现和消失来表示两个二进制数字。发光二极管 LED 和注入型激光二极管 ILD 的信号都可用这种方法调制，PIN 和 APD 检波器直接响应亮度调制。

在计算机网络中均采用两根光纤 (一来一去) 组成传输系统。按波长范围 (近红外范围内) 可分为三种： $0.85\mu\text{m}$ 波长区 ($0.8\sim0.9\mu\text{m}$)、 $1.3\mu\text{m}$ 波长区 ($1.25\sim1.35\mu\text{m}$) 和 $1.55\mu\text{m}$ 波长区 ($1.53\sim1.58\mu\text{m}$)。不同的波长范围光纤损耗特性也不同，其中 $0.85\mu\text{m}$ 波长区为多模光纤通信方式， $1.55\mu\text{m}$ 波长区为单模光纤通信方式， $1.3\mu\text{m}$ 波长区有多模和单模两种方式。

光纤通过内部的全反射来传输一束经过编码的光信号，内部的全反射可以在任何折射指数高于包层介质折射指数的透明介质中进行。实际上光纤作为频率范围从 $10^{14}\sim10^{15}\text{Hz}$ 的波导管，这一范围覆盖了可见光谱和部分红外光谱。光纤的数据传输率可达 Gbps 级，传输距离达数十公里。目前，除了一条光纤线路上只能传输一个载波的技术之外，还出现了采用一种波分技术，在一条光纤上复用多路传输，每路使用不同的波长，称为波分复用的技术 WDM (Wavelength Division Multiplexing)。

光纤普遍用于点到点的链路。总线拓扑结构的实验性多点系统已经建成，但是价格还太贵。原则上讲，由于光纤功率损失小、衰减少的特性以及有较大的带宽潜力，因此一段光纤能够支持的分接头数比双绞线或同轴电缆多得多。光纤适合于在几个建筑物之间通过点到点的链路连接局域网络。光纤具有不受电磁干扰或噪声影响的特征，适宜在长距离内保持高数据传输率，而且能够提供很好的安全性。

就每米的价格和所需部件 (发送器、接收器、连接器) 来说，光纤比双绞线和同轴电缆都要贵，但是双绞线和同轴电缆的价格不大可能再下降，而光纤的价格将随着工程技术的进步会大大下降，使它能与同轴电缆的价格相竞争。

由于光纤通信具有损耗低、频带宽、数据传输率高、抗电磁干扰强等特点，对高速率、距离较远的局域网也是很通用的。

3.2.4 无线传输介质

无线传输介质通过空间传输，不需要架设或铺埋电缆或光纤，目前常用的技术按照频率由低向高排列有：无线电波、微波、红外线和可见光。便携式计算机的出现，以及在军事、野外等特殊场合下移动式通信联网的需要，促进了数字化无线移动通信的发展，开始出现无线局域网产品。

美国的贝尔实验室最早在 1947 年就提出了蜂窝无线移动通信 (Cellular Radio Mobile Communication) 的概念，1958 年向美国联邦通信委员会 FCC 提出了建议，1977 年完成了可行性技术论证，1978 年完成了芝加哥先进移动电话系统 AMPS (Advanced Mobile Phone System) 的试验，并且在 1983 年正式投入运营。由于微电子学与 VLSI 技术的发展，促进了蜂窝移动通信的迅速发展。

早期的移动通信系统采用大区制的强覆盖区，即建立一个无线电台基站，架设很高的天

线塔（一般高于30米），使用很大的发射功率（一般在50W~200W），覆盖范围可以达到30km~50km。大区制的优点是结构简单，不需要交换，但频道数量较少，覆盖范围有限。为了提高覆盖区域的系统容量与充分利用频率资源，人们提出了小区制的概念。

如果将一个大区制覆盖的区域划分成多个小区，每个小区（Cell）中设立一个基站（BS），通过基站在用户的移动台（MS）之间建立通信。小区覆盖的半径较小，一般为1km~20km，因此可以用较小的发射功率实现双向通信。如果每个基站提供一到几个频道，可容纳的移动用户数就可以有几十到几百个。这样，由多个小区构成的通信系统的总容量将大大提高。由若干小区构成的覆盖区叫做区群。由于区群的结构酷似蜂窝，因此人们将小区制移动通信系统叫做蜂窝移动通信系统，其结构如图3-10所示。在每个小区设立一个（或多个）基站，它与若干个移动站建立无线通信链路。区群中各小区的基站之间可以通过电缆、光缆或微波链路与移动交换中心（MSC）连接。移动交换中心通过PCM电路与市话交换局连接，从而构成了一个完整的蜂窝移动通信的网络结构。

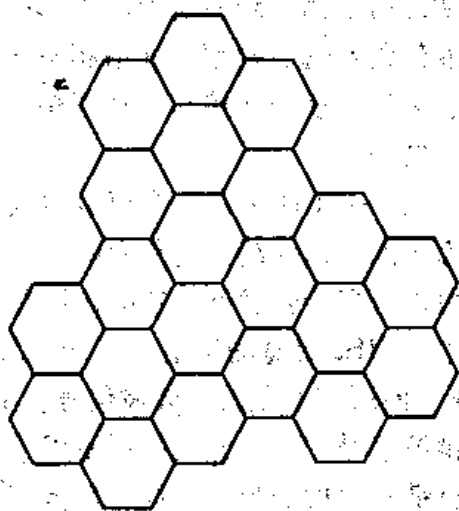


图3-10 蜂窝移动通信系统结构示意图

第一代蜂窝移动通信是模拟方式，这是指用户的语音信息的传输以模拟语音方式出现的。第二代蜂窝移动通信是数字方式。数字方式涉及语音信号的数字化与数字信息的处理、传输问题。目前人们正在研究和开发第三代移动通信产品。

在无线通信环境中的电磁波覆盖区内，如何建立用户的无线信道的连接，这就是多址连接问题。在无线通信网中，任一用户发送的信号均能被其它用户接收，所以网中用户如何能从接收的信号中识别出本地用户地址，就是多址接入问题。解决多址接入的方法称为多址接入技术。在蜂窝移动通信系统中，多址接入方法主要有3种：频分多址接入FDMA、时分多址接入TDMA与码分多址接入CDMA。蜂窝移动通信网的设计，涉及OSI参考模型的物理层、数据链路层与网络层。

微波通信的载波频率为100MHz~10GHz范围。因为频率很高，可同时传送大量信息，用来传输数字数据，速率可达数Mbps。微波通信的工作频率很高，与通常的无线电波不一样，是沿直线传播的。由于地球表面是曲面，微波在地面的传播距离有限。直接传播的距离与天线的高度有关，天线越高传播距离越远，超过一定距离后就要用中继站来接力。由于微波信号波长较短，因此利用机械尺寸相对较小的抛物面天线，就可以将微波信号能量集中在一个很小的波束内发送出去，这样就可以用很小的发射功率来进行远距离通信。红外通信和激光通信也像微波通信一样，有很强方向性，都是沿直线传播的。这三种技术都需要在发送方和接收方之间有一条视线（Line of Sight）通路，故它们统称为视线介质。所不同的是，红外通信和激光通信把要传输的信号分别转换为红外光信号和激光信号直接在空间传播。这三种视线介质由于都不需要铺设电缆，对于连接不同建筑物内的局域网特别有用。这三种技术对环境气候较为敏感，例如雨、雾和雷电。相对来说，微波对一般雨和雾的敏感度较低。

在1945年,英国人阿塞·C. 克拉克提出了利用卫星进行通信的设想。1957年,前苏联发射了第一颗人造地球卫星 Sputnik,使人们看到了实现卫星通信的希望。1962年,美国成功发射了第一颗通信卫星 Telsat,试验了横跨大西洋的电话和电视传输。由于卫星通信具有通信距离远、费用与通信距离无关、覆盖面积大、不受地理条件的限制、通信信道带宽宽、可进行多址通信与移动通信的优点,因此获得了迅速的发展,并成为现代主要的通信手段之一。

图3-11所示是一个简单的卫星通信原理示意图。图3-11(a)是通过卫星微波形成的点一点通信线路,它是由两个地球站(发送站、接收站)与一颗通信卫星组成的。卫星上可以有多个转发器,它的作用是接收、放大与发送信息。目前,一般是12个转发器拥有一个36MHz带宽的信道,不同的转发器使用不同的频率。地面发送站使用上行链路(Uplink)向通信卫星发射微波信号。卫星起到一个中继器的作用,它接收通过上行链路发送来的微波信号,经过放大后再使用下行链路(Downlink)发送回地面接收站。由于上行链路与下行链路使用的频率不同,因此可以将发送信号与接收信号明显区分出来。图3-11(b)是通过卫星形成的广播通信线路。

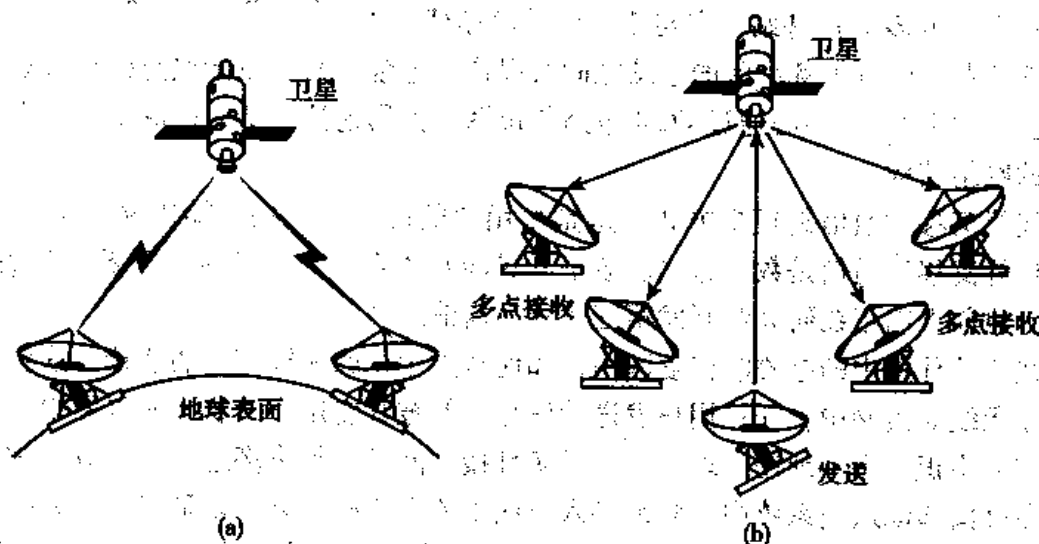


图3-11 卫星通信原理示意图

使用卫星通信时,需要注意到它的传输延时。由于发送站要通过卫星转发信号到接收站,如果从地面发送到卫星的信号传输时间为 Δt ,不考虑转发中处理时间,那么从信号发送到接收的延迟时间为 $2\Delta t$ 。 Δt 值取决于卫星距地面的高度,一般 Δt 值在250毫秒~300毫秒,典型值为270毫秒。这样的话,传输延迟的典型值为540毫秒,这个数值在设计卫星数据通信系统时是一个重要参数。

商用通信卫星一般被发射在赤道上方35900公里的同步轨道上。这就意味着,当地球自转时,地球同步轨道卫星(GEO, Geostationary Earth Orbit, 地球同步轨道)也以适当的速度沿地球自转方向绕轨道运行,地球与卫星之间可以保持相对的静止。三颗这样的卫星均匀沿轨道分开,就可以覆盖整个地球表面。

随着通信的急速增长,在20世纪80年代初发展起来一种新的低成本卫星通信系统,即甚小口径天线地球站 VSAT (Very Small Aperture Terminal),这是指采用小口径的卫星天线的地面接收系统。在C频段,下行链路4.0GHz,上行链路6.0GHz,天线口径可压缩至1米

以下：在 Ka 频段，下行链路 11GHz，上行链路 14GHz，天线口径可压缩到 2.4 米以下。VSAT 按其承担的服务类型可以分为两类：一类是以数据传输为主的小型数据地球站 (PES, Personal Earth Station)，另一类是以语音传输为主，并且兼容数据传输的小型电话地球站 (TES, Telephone Earth Station)。

由于小卫星技术的发展，出现了中、低轨道卫星移动通信的新方法。中、低轨道卫星不是同步卫星，它作为陆地移动通信系统的补充和扩展，与地面公用通信网有机地结合起来，才能实现全球个人移动通信。低轨道移动通信系统实现个人通信的优点是：卫星轨道高度低，使传输延迟缩短，多个卫星组成的星座可以真正覆盖全球。

典型的低轨道卫星系统是微软公司与麦考通信公司的卫星通信网络 Teledesic，其目标是遍布全球的、对带宽的需求非常大的 Internet 用户。提供上行链路可达 100Mbps、下行链路可达 720Mbps 的带宽。计划发射 840 ~ 924 颗卫星组成一个卫星通信网。每颗卫星是网中的一个交换节点，相邻的 8 颗卫星构成一个网状拓扑。这些卫星发射到距地球 700 公里的 21 个轨道上运行，覆盖地球表面 95% 的地区，采用 Ka (30GHz/20GHz) 频段通信链路，传输从电话到视频会议、交互式多媒体通信与实时双向数据等宽带业务。

另一个有代表性的使用低轨道 LEO (Low Earth Orbit, 低地球轨道) 卫星群实现全球卫星移动通信的方案是 Motorola 公司的 Iridium 系统，也叫做“铱卫星移动通信系统”。Iridium 系统最初的设计为 77 颗小型智能卫星均匀有序地分布在离地面 785km 上空的 7 个轨道平面上，通过微波链路形成全球连接网络。由于这种结构与元素周期表中铱原子的外层电子分布很相似，因此取名为铱系统。为了减少投资，简化结构，Motorola 公司将卫星数减少到 66 颗，轨道平面减为 6 个。每颗卫星可以提供 48 个点波束，每个波束平均包含 80 个信道，这样的话，每颗卫星可以提供 3840 个全双工通道。系统要求具有空间交换与路由选择功能。每颗卫星发射到地面的多个波束，在地球表面上形成 48 个蜂窝分组交换区，每个蜂窝区的直径约为 667 公里。蜂窝区随着地球自转而快速扫过地球表面，可以提供数字语音传输、数据传输、全球定位、全球寻呼与个人通信等通信业务。用户可以通过 Iridium 系统，实现全球通信。

卫星移动通信系统将形成一个空间的通信子网，它的通信功能将实现 OSI 参考模型中的物理层、数据链路层与网络层的功能。显然，全世界已经出台的十几个利用小卫星组成中、低轨道卫星移动通信系统的方案，将是实现 21 世纪个人通信与信息高速公路最有前途的通信手段之一，它也将对计算机网络技术的发展产生重要的影响。

3.2.5 传输介质的选择

传输介质的选择取决于以下诸因素：网络拓扑的结构、实际需要的通信容量、可靠性要求、能承受的价格范围。

双绞线的显著特点是价格便宜，但与同轴电缆相比，其带宽受到限制。对于单个建筑物内的低通信容量局域网来说，双绞线的性能价格比可能是最好的。

同轴电缆的价格要比双绞线贵一些，对于大多数的局域网来说，需要连接较多设备而且通信容量相当大时可以选择同轴电缆。

光纤作为传输介质，与同轴电缆和双绞线相比具有一系列优点：频带宽、速率高、体积

小、重量轻、衰减小、能电磁隔离、误码率低等，因此，在国际和国内长话传输中的地位日益提高，并已广泛用于高速数据通信网。随着光纤通信技术和成本的降低，光纤作为局域网的传输介质也得到了普遍采用，光纤分布数据接口 FDDI 就是一例。

目前，便携式计算机已经有了很大的发展和普及，由于可随身携带，对可移动的无线网的需求将日益增加。无线数字网类似于蜂窝电话网，人们随时随地可将计算机接入网络，发送和接收数据。移动无线数字网的发展前景将是十分美好的。

3.3 数据通信技术

3.3.1 通信信道

数据通信的任务是传输数据信息，希望达到传输速度快、出错率低、信息量大、可靠性高，并且既经济又便于使用维护。这些要求可以用下列技术指标加以描述。

1. 数据传输速率

所谓数据传输速率，是指每秒能传输的二进制信息位数，单位为位/秒 (Bit/Sec-ond)，记作 bps 或 b/s，它可由下式确定：

$$R = \frac{1}{T} \cdot \log_2 N \quad (\text{bps})$$

式中 T 为一个数字脉冲信号的宽度 (全宽码情况) 或重复周期 (归零码情况)，单位为秒。一个数字脉冲也称为一个码元， N 为一个码元所取的有效离散值个数，也称调制电平数， N 一般取 2 的整数次方值。若一个码元仅可取 0 和 1 两种离散值，则该码元只能携带一位 (Bit) 二进制信息；若一个码元可取 00、01、10 和 11 四种离散值，则该码元就能携带两位二进制信息。以此类推，若一个码元可取 N 种离散值，则该码元便能携带 $\log_2 N$ 位二进制信息。

当一个码元仅取两种离散值时， $R = (1/T)$ ，表示数据传输速率等于码元脉冲的重复频率。由此，可以引出另一个技术指标——信号传输速率，也称码元速率、调制速率或波特率，单位为波特 (Baud)。信号传输速率表示单位时间内通过信道传输的码元个数，也就是信号经调制后的传输速率。若信号码元的宽度为 T 秒，则码元速率定义为：

$$B = \frac{1}{T} \quad (\text{Baud})$$

在有些调幅和调频方式的调制解调器中，一个码元对应于一位二进制信息，即一个码元有两种有效离散值，此时调制速率和数据传输速率相等。但在调相的四相信号方式中，一个码元对应于两位二进制信息，即一个码元有四种有效离散值，此时调制速率只是数据传输速率的一半。由以上两式合并可得到调制速率和数据传输速率的对应关系式：

$$R = B \cdot \log_2 N \quad (\text{bps})$$

$$\text{或 } B = R / \log_2 N \quad (\text{Baud})$$

一般在二元调制方式中, R 和 B 都取同一值, 习惯上二者是通用的。但在多元调制的情况下, 必须将它们区别开来。例如采用四相调制方式, 即 $N=4$, 且 $T=833 \times 10^{-6}$ 秒, 则可求出数据传输速率为:

$$R = \frac{1}{T} \cdot \log_2 N = \frac{1}{833 \times 10^{-6}} \cdot \log_2 4 = 2400 \quad (\text{bps})$$

而调制速率为:

$$B = \frac{1}{T} = \frac{1}{833 \times 10^{-6}} = 1200 \quad (\text{Baud})$$

通过上例可见, 虽然数据传输速率和调制速率都是描述通信速度的指标, 但它们是完全不同的两个概念。打个比喻来说, 假如调制速率是公路上单位时间经过的卡车数, 那么数据传输速率便是单位时间里经过的卡车所装运的货物箱数。如果一车装一箱货物, 则单位时间经过的卡车数与单位时间里卡车所装运的货物箱数相等, 如果一车装多箱货物, 则单位时间经过的卡车数便小于单位时间里卡车所装运的货物箱数。

2. 信道容量

信道容量表征一个信道传输数据的能力, 单位也用位/秒 (bps)。信道容量与数据传输速率的区别在于, 前者表示信道的最大数据传输速率, 是信道传输数据能力的极限, 而后者则表示实际的数据传输速率。这就像公路上的最大限速值与汽车实际速度之间的关系一样, 它们虽然采用相同的单位, 但表征的是不同的含义。

奈奎斯特 (Nyquist) 首先给出了无噪声情况下码元速率的极限值 B 与信道带宽 H 的关系:

$$B = 2 \cdot H \quad (\text{Baud})$$

其中, H 是信道的带宽, 也称频率范围, 即信道能传输的上、下限频率的差值, 单位为 Hz。由此可推出表征信道数据传输能力的奈奎斯特公式:

$$C = 2 \cdot H \cdot \log_2 N \quad (\text{bps})$$

此处, N 仍然表示携带数据的码元可能取的离散值的个数, C 即是该信道最大的数据传输速率。

由以上两式可见, 对于特定的信道, 其码元速率不可能超过信道带宽的两倍, 但若能提高每个码元可能取的离散值的个数, 则数据传输速率便可成倍提高。例如, 普通电话线路的带宽约为 3KHz, 则其码元速率的极限值为 6KBaud。若每个码元可能取的离散值的个数为 16 (即 $N=16$), 则最大数据传输速率可达 $C=2 \times 3K \times \log_2 16 = 24Kbps$ 。

实际的信道总要受到各种噪声的干扰, 香农 (Shannon) 则进一步研究了受随机噪声干扰的信道的情况, 给出了计算信道容量的香农公式:

$$C = H \cdot \log_2 (1 + S/N) \quad (\text{bps})$$

其中, S 表示信号功率, N 为噪声功率, S/N 则为信噪比。由于实际使用的信道的信噪比都

要足够大，故常表示成 $10 \log_{10} (S/N)$ ，以分贝 (dB) 为单位来计量，在使用时要特别注意。例如，信噪比为 30dB，带宽为 3KHz 的信道的最大数据传输速率为：

$$C = 3K \times \log_2(1 + 10^{30/10}) = 3K \times \log_2(1 + 1001) \approx 30Kbps。$$

由此可见，只要提高信道的信噪比，便可提高信道的最大数据传输速率。

需要强调的是，上述两个公式计算得到的只是信道数据传输速率的极限值，实际使用时必须留有充足的余地。

3. 误码率

误码率是衡量数据通信系统在正常工作情况下的传输可靠性的指标，它定义为二进制数据位传输时出错的概率。设传输的二进制数据总数为 N 位，其中出错的位数为 N_e ，则误码率表示为：

$$P_e = N_e / N$$

计算机网络中，一般要求误码率低于 10^{-9} ，即平均每传输 10^9 位数据仅允许错一位。若误码率达不到这个指标，可以通过差错控制方法进行检错和纠错。

4. 通信方式

在计算机内部各部件之间、计算机与各种外部设备之间及计算机与计算机之间都是以通信的方式传递交换数据信息的。通信有两种基本方式，即串行方式和并行方式。通常情况下，并行方式用于近距离通信，串行方式用于距离较远的通信。在计算机网络中，串行通信方式更具有普遍意义。



图 3-12 并行数据传输

(1) 并行通信方式。在并行数据传输中有多数据位，例如 8 个数据位（如图 3-12 所示），同时在两个设备之间传输。

发送设备将 8 个数据位通过 8 条数据线传送给接收设备，还可附加一位数据校验位。接收设备可同时接收到这些数据，不需作任何变换就可直接使用。在计算机内部的数据通信通常以并行方式进行。并行的数据传送线也叫总线，如并行传送 8 位数据就叫 8 位总线，并行传送 16 位数据就叫 16 位总线。并行数据总线的物理形式有好几种，但功能都是一样的。例如：计算机内部直接用印刷电路板实现的数据总线、连接软/硬盘驱动器的扁平带状电缆、连接计算机外部设备的圆形多芯屏蔽电缆等。

(2) 串行通信方式。并行传输时，需要一根至少有 8 条数据线（因一个字节是 8 位）的电缆将两个通信设备连接起来。当进行近距离传输时，这种方法的优点是传输速度快，处理简单；但进行远距离数据传输时，这种方法的线路费用就难以容忍了。这种情况下，使用现成的电话线来进行数据传输就经济得多了。

用电话线进行通信，就必须使用串行数据传输技术。串行数据传输时，数据是一位一位

地在通信线上传输的，与同时可传输好几位数据的并行传输相比，串行数据传输的速度要比并行传输慢得多。但由于公用电话系统已形成了一个覆盖面极其广阔的网络，所以，使用现成的电话网以串行传输方式通信，对于计算机网络来说具有更大的现实意义。

如图 3-13 所示，串行数据传输时，先由具有 8 位总线的计算机内的发送设备，将 8 位并行数据经并—串转换硬件转换成串行方式，再逐位经传输线到达接收站的设备中，并在接收端将数据从串行方式重新转换成并行方式，以供接收方使用。

(3) 串行通信的方向性结构。串行数据通信的方向性结构有三种，即单工、半双工和全双工，如图 3-14 所示。

单工数据传输只支持数据在一个方向上传输；半双工数据传输允许数据在两个方向上传输，但是，在某一时刻，只允许数据在一个方向上传输，因而半双工通信实际上是一种可切换方向的单工通信；全双工数据传输允许数据同时在两个方向上传输，因此全双工通信是两个单工通信方式的结合，它要求发送设备和接收设备都有独立的接收和发送能力。

这里要特别指出的是移动通信中按照通话状态和频率使用的方法也可分三种方式：单工制、半双工制和双工制。因为在无线工作方式下有单频、双频之分，因而上述三种方式与计算机网络的串行通信三种工作方式的含义有所不同，这里不再赘述。

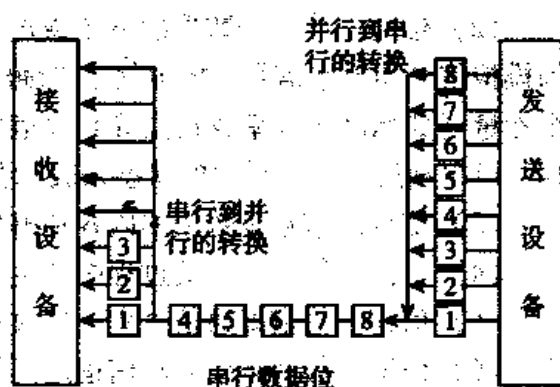


图 3-13 串行数据传输

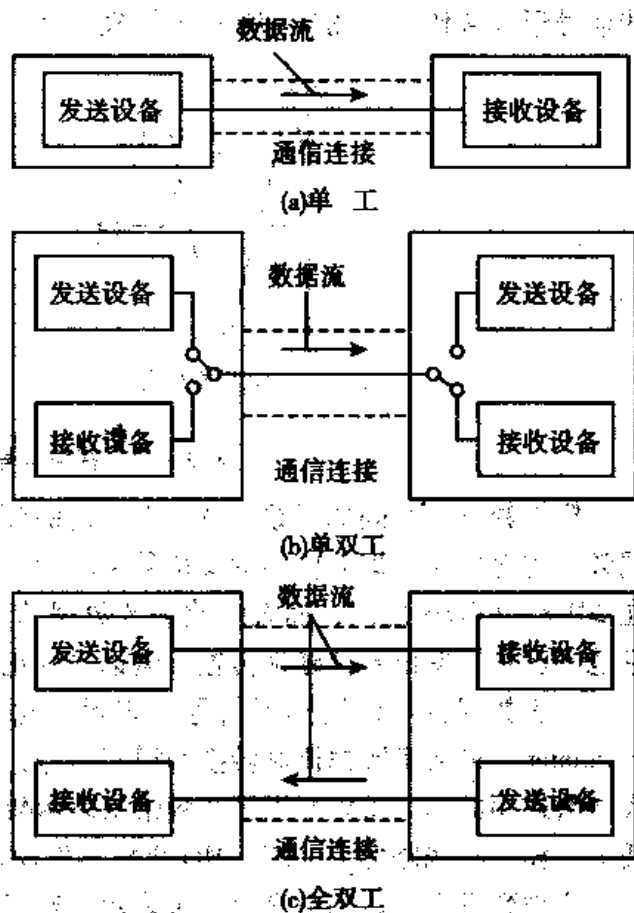


图 3-14 串行数据通信的方向性结构

3.3.2 模拟数据通信和数字数据通信

在介绍数据通信之前，先对几个基本术语作一下解释：

(1) 数据。数据可定义为有意义的实体，它涉及事物的存在形式。数据可分为模拟数据和数字数据两大类。模拟数据是在某个区间内连续变化的值，例如声音和视频都是幅度连续变化的波形，又如温度和压力也都是连续变化的值；数字数据是离散的值，例如文本信息和整数。

(2) 信号。信号是数据的电子或电磁编码。对应于模拟数据和数字数据，信号也可分为模拟信号和数字信号。模拟信号是随时间连续变化的电流、电压或电磁波，可以利用其某个参量（如幅度、频率或相位等）来表示要传输的数据；数字信号则是一系列离散的电脉冲，可以利用其某一瞬间的状态来表示要传输的数据。

(3) 信息。信息是数据的内容和解释。

(4) 信源。信源即通信过程中产生和发送信息的设备或计算机。

(5) 信宿。信宿即通信过程中接收和处理信息的设备或计算机。

(6) 信道。信道是信源和信宿之间的通信线路。

无论信源产生的是模拟数据还是数字数据，在传输过程中都要转换成适合于信道传输的某种信号形式。模拟数据和数字数据都可以用模拟信号或数字信号来表示，因而也可以用这些信号形式来传输。图 3-15 给出了模拟信号、数字信号的表示形式。

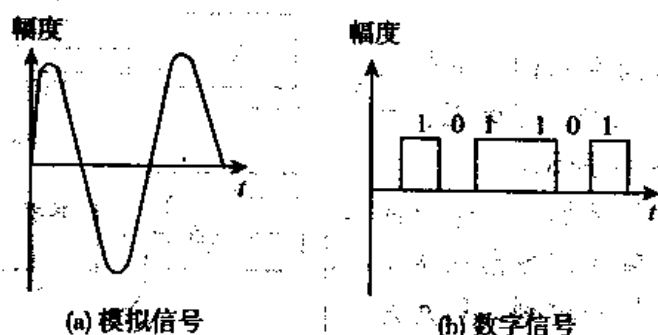


图 3-15 模拟信号和数字信号的表示

模拟数据是时间的函数，并占有一定的频率范围，即频带。这种数据可以直接用占有相同频带的电信号，即对应的模拟信号来表示。就人类的听觉能力而言，声音数据的频率范围在 $20\text{Hz} \sim 20\text{kHz}$ 之间，而大多数语音数据的可懂度频率范围仅为 $300\text{Hz} \sim 3400\text{Hz}$ ，这个频率范围已足够使语音清晰地传输，电话系统正是按这一标准运行的。

数字数据也可以用模拟信号来表示，此时要利用调制解调器 MODEM (Modulator Demodulator) 将数字数据调制转换为模拟信号，使之能在适合于此种模拟信号的介质上传输。大多数通用的 MODEM 都用语音频带来表示数字数据，因此能使数字数据在普通的音频电话线上传输；在线路的另一端，MODEM 再把模拟信号解调还原成原来的数字数据。

模拟数据也可以用数字信号来表示。对于声音数据来说，完成模拟数据和数字信号转换功能的设施是编码解码器 CODEC (Coder Decoder)。CODEC 将直接表示声音数据的模拟信号，编码转换成用二进制位流近似表示的数字信号；而线路另一端的 CODEC，则将二进制位流解码恢复成原来的模拟数据。

数字数据还可以直接用二进制形式的数字脉冲信号来表示，但为了改善其传播特性，一般先要对二进制数据进行编码。有关的编码技术将在本章稍后再详细介绍。

模拟信号和数字信号都可以在合适的传输介质上进行传输，即模拟传输和数字传输。模拟信号可以表示模拟数据（例如声音），也可以表示数字数据（例如通过 MODEM 发送的数据）。无论哪种情况，在传输一定距离之后，模拟信号都将衰减。为了实现长距离传输，模拟传输系统要用放大器来增强信号中的能量，但同时也会使噪音分量增强，以至于引起信号畸变。对于模拟数据来说，例如声音，即使存在一些畸变，内容仍然可以听懂理解；但对于

数字数据来说，畸变将会使数据传输产生错误。数字传输的衰减也会危及数据的完整性，数字信号只能在一个有限距离内传输，为了获得更大的传输距离，可以使用中继器。中继器接收衰减了的数字信号，把数字信号恢复为“0”、“1”的标准电平，然后重新传输这种新的信号，这样就有效地克服了衰减。

模拟数据、数字数据的模拟信号、数字信号传输的描述如图 3-16 所示。

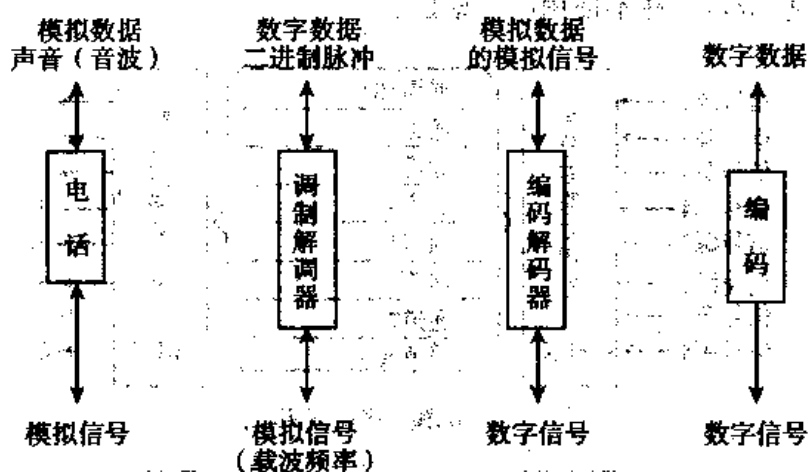


图 3-16 模拟数据、数字数据的模拟信号、数字信号传输的表示

数字传输无论在价格方面还是在质量方面，都比模拟传输优越。因此，数字传输是今后数据通信的发展方向。

数据通信是一种通过计算机或其它数据装置与通信线路，完成数据编码信号的传输、转接、存储和处理的通信技术。所以，数据通信系统也就是以计算机为中心、用通信线路连接分布在异地的数据终端设备，以实施数据传输的一种系统。

在局域网中，由于距离近以及数字电路器件价格的下降，采用数字传输技术更具优越性。

3.3.3 多路复用技术

在数据通信系统或计算机网络系统中，传输介质的带宽或容量往往超过传输单一信号的需求，为了有效地利用通信线路，希望一个信道同时传输多路信号，这就是所谓的多路复用技术（Multiplexing）。采用多路复用技术能把多个信号组合起来在一条物理信道上进行传输，在远距离传输时可大大节省电缆的安装和维护费用。

频分多路复用 FDM（Frequency Division Multiplexing）和时分多路复用 TDM（Time Division Multiplexing）是两种最常用的多路复用技术。

对于光纤信道，还使用频分多路复用的一个变种称为波分多路复用 WDM（Wavelength Division Multiplexing）。

1. 频分多路复用 FDM

在物理信道的可用带宽超过单个原始信号所需带宽情况下，可将该物理信道的总带宽分割成若干个与传输单个信号带宽相同（或略宽）的子信道，每个子信道传输一路信号，这

就是频分多路复用。多路原始信号在频分复用前，先要通过频谱搬移技术将各路信号的频谱搬移到物理信道频谱的不同段上，也即使信号的带宽不相互重叠，这可以通过采用不同的载波频率进行调制来实现。频分多路复用 FDM 的一个示例见图 3-17 (a)，其中 8 个信号源输入到一个多路复用器中，该多路复用器用不同的频率 ($f_1 \sim f_8$) 调制每一个信号，每个信号需要一个以它的载波频率为中心的一定带宽的通道。为了防止相互干扰，使用保护带来隔离每一个通道，保护带是一些不使用的频谱区。

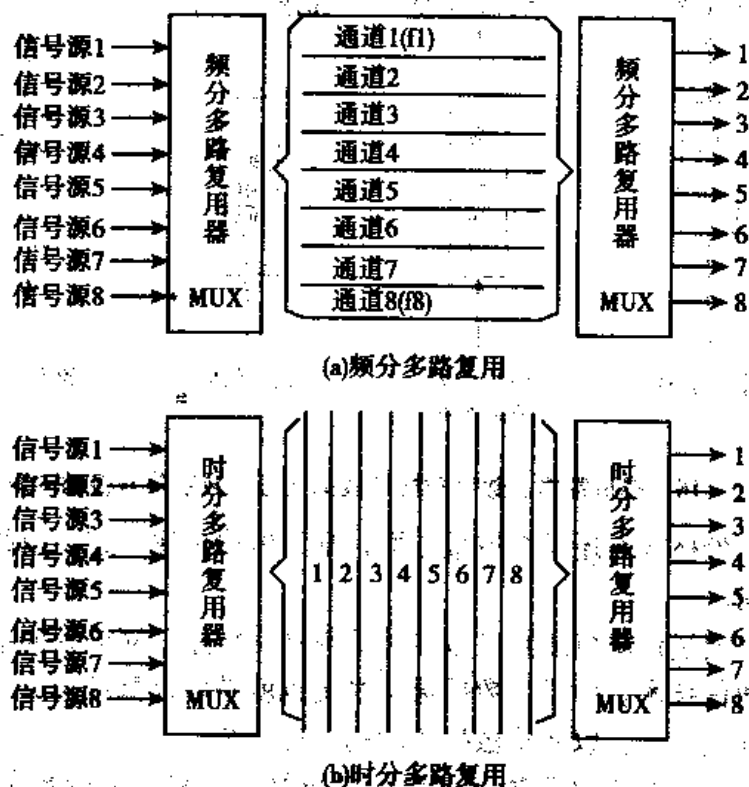


图 3-17 频分多路复用与时分多路复用

2. 时分多路复用 TDM

若介质能达到的位传输速率超过传输数据所需的数据传输速率，就可采用时分多路复用 TDM 技术，也即将一条物理信道按时间分成若干个时间片轮流地分配给多个信号使用。每一时间片由复用的一个信号占用，而不像 FDM 那样，同一时间同时发送多路信号。这样，利用每个信号在时间上的交叉，就可以在一条物理信道上传输多个数字信号。这种交叉可以是位一级的，也可以是由字节组成的块或更大的信息组进行交叉。如图 3-17 (b) 中的多路复用器有 8 个输入，每个输入的数据速率假设为 9.6Kbps，那么一条容量达 76.8Kbps 的线路就可容纳 8 个信号源。该图描述的时分多路复用 TDM 方案，也称同步 (Synchronous) 时分多路复用 TDM，它的时间片是预先分配好的，而且是固定不变的，因此各种信号源的传输定时是同步的。与此相反，异步时分多路复用 TDM 允许动态地分配传输介质的时间片。

时分多路复用 TDM 不仅仅局限于传输数字信号，也可以同时交叉传输模拟信号。另外，对于模拟信号，有时可以把时分多路复用和频分多路复用技术结合起来使用。一个传输系统，可以频分成许多条子通道，每条子通道再利用时分多路复用技术来细分。在宽带局域网

络中可以使用这种混合技术。

Bell 系统的 T1 载波利用脉码调制 PCM 和时分多路复用 TDM 技术, 使 24 路采样声音信号复用在一个通道, 其帧结构如图 3-18 所示。24 路信道各自轮流将编码后的 8 位数字信号组成帧, 其中 7 位是编码的数据, 第 8 位是控制信号。每帧除了 192 位 (24×8) 之外, 另加一位帧同步位。这样, 一帧中就包含 193 位, 每一帧用 $125\mu\text{s}$ 时间传送, 因此 T1 系统的数据传输速率为 1.544Mbps 。

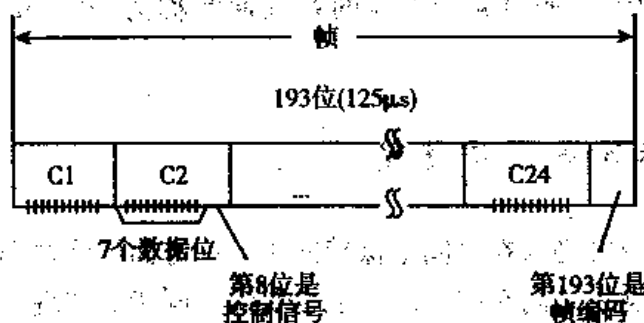


图 3-18 T1 载波帧结构

ITU 建议了一种 2.048Mbps 速率的 PCM 载波标准, 称为 E1 载波 (欧洲标准)。它的每一帧开始处有 8 位作同步用, 中间有 8 位用作信令, 再组织 30 路 8 位数据, 全帧含 256 位, 每一帧也用 $125\mu\text{s}$ 传送, 可计算出数据传输速率为 $256\text{位}/125\mu\text{s} = 2.048\text{Mbps}$ 。

3. 波分多路复用 WDM

光纤上 WDM 的基本原理如图 3-19 所示。发送端假定有 4 条光纤汇合到一个组合器 (Combiner) 中, 每条光纤的能量位于不同的波长处。四束光被组合到一条共享的光纤上, 传输到远端的目的地。在远端又被分离器分离到与发送端一样多的 4 条光纤上。每条光纤上的过滤器能够过滤出某一波长的光, 而其它波长被过滤掉, 这一结果信号可以再被路由到它们各自的目的地。

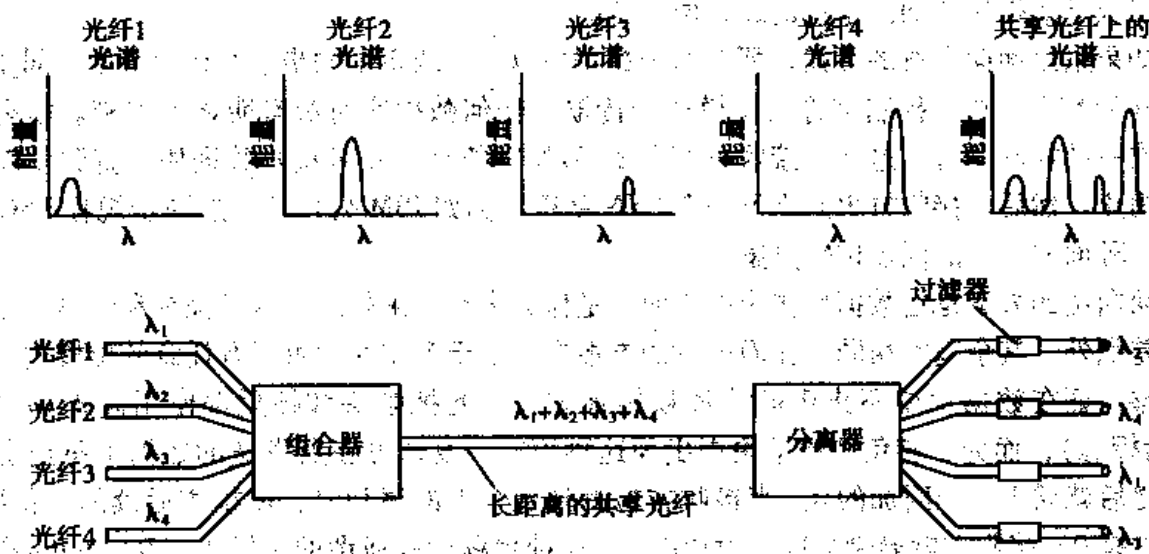


图 3-19 波分多路复用

上述的复用技术只不过是频分多路复用在极高频率上的应用而已。只要每条信道有它自己的频率（也就是波长）范围，并且所有的频率范围都是分开的，它们都可以被复用到长距离光纤上。

WDM 技术自 1990 年前后问世至今已发展到了让计算机技术望尘莫及的速度了。2001 年在市场上有了 96 条信道（每条信道的带宽为 10Gbps，总共 960Gbps）的产品。具有 200 条信道的系统也不久问世。当信道的数目很大，并且波长范围之间的间隔非常接近（例如：仅为 0.1 纳米）的时候，这样的系统通常称为 DWDM（Dense WDM，即密集波分多路复用）。

3.3.4 异步传输和同步传输

通信过程中收、发双方必须在时间上保持同步，一方面码元之间要保持同步，另一方面由码元组成的字符或数据块之间在起止时间上也要保持同步。实现字符或数据块之间在起止时间上同步的常用方法有异步传输和同步传输两种。

1. 异步传输

异步传输即前面介绍过的群同步传输。异步传输方式中，一次只传输一个字符（由 5~8 位数据组成）。每个字符用一位起始位引导、一位停止位结束。起始位为“0”，占一位时间；停止位为“1”，占 1 到 2 位的持续时间。在没有数据发送时，发送方可发送连续的停止位（称空闲位）。接收方根据“1”至“0”的跳变来判别一个新字符的开始，然后接收字符中的所有位。这种通信方式简单便宜，但每个字符有 2~3 位的额外开销。

2. 同步传输

同步传输时，为使接收方能判定数据块的开始和结束，还须在每个数据块的开始处和结束处各加一个帧头和一个帧尾，加有帧头、帧尾的数据称为一帧（Frame）。帧头和帧尾的特性取决于数据块是面向字符的还是面向位的。

如果采用面向字符的方案，那么每个数据块以一个或多个同步字符作为开始。同步字符通常称为 SYN，这一控制字符的位模式与传输的任何数据字符都有明显的差别。帧尾是另一个唯一的控制字符。这样，接收方判别到 SYN 字符后，就可接收数据块，直到发现帧尾字符为止。然后，接收方再判别下一个 SYN 字符。例如 IBM 公司的二进同步规程 BSC 就是这样一种面向字符的同步传输方案。

面向位的方案是把数据块作为位流而不是作为字符流来处理。除了帧头和帧尾的原理有一点差别外，其余基本相同。在面向位的方案中，由于数据块中可以有任意的位模式，因此不能够保证在数据块中不出现帧头和帧尾标志，为此把帧头和帧尾都使用模式 01111110（称为标志），而为了避免在数据块中出现这种模式，发送方在所发送的数据中每当出现五个 1 之后就插入一个附加的 0。当接收方检测到五个 1 的序列时，就检查后续的一位数据，若该位是 0，接收方就删除掉这个附加的 0，这种规程就是所谓的位插入（Bit Stuffing）。在国际标准化组织 ISO 所规定的高级数据链路控制规程 HDLC 和 IBM 公司所规定的同步数据链路控制规程 SDLC 中都采用这种技术。

3.4 数据编码

除了模拟数据的模拟信号直接传输外，数字数据的模拟信号传输、数字数据和模拟数据的数字信号传输都需要进行某种形式的数据表示或者称数据编码。

3.4.1 数据编码技术

1. 数字数据的数字信号编码

数字信号可以直接采用基带传输；所谓基带就是指表示二进制比特序列的矩形脉冲信号所占的固有频带，称为基本频带（简称基带）。基带传输就是在线路中直接传送数字信号的电脉冲，这是一种最简单的传输方式，近距离通信的局域网都采用基带传输。

基带传输时，需要解决数字数据的数字信号表示以及收发两端之间的信号同步问题。对于传输数字信号来说，最简单最常用的方法是用不同的电压电平来表示两个二进制数字，也即数字信号由矩形脉冲组成。下面介绍几种基本的数字信号脉冲编码方案（参见图3-20）。

单极性不归零码，无电压（也就是无电流）用来表示“0”，而恒定的正电压用来表示“1”。每一个码元时间的中间点是采样时间，判决门限为半幅度电平（即0.5）。也就是说接收信号的值在0.5与1.0之间，就判为“1”码，如果在0与0.5之间就判为“0”码。每秒钟发送的二进制码元数称为“码速”。

双极性不归零码，“1”码和“0”码都有电流，但是“1”码是正电流，“0”码是负电流，正和负的幅度相等，故称为双极性码。此时的判决门限为零电平，接收端使用零判决器或正负判决器，接收信号的值若在零电平以上为正，判为“1”

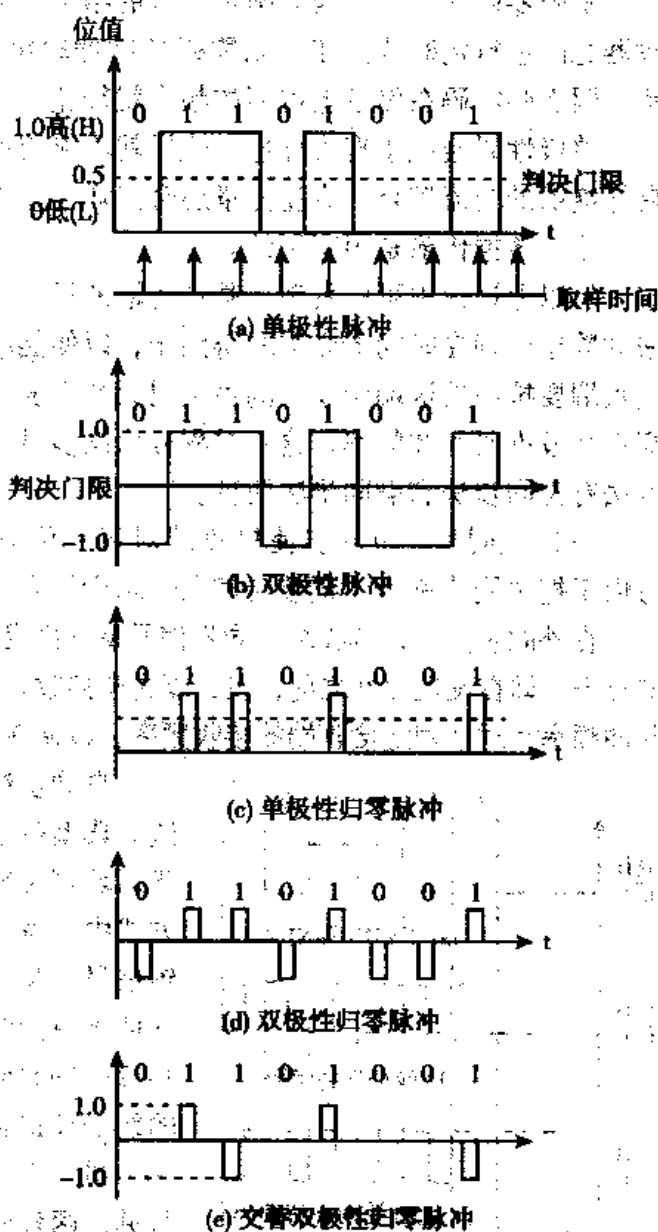


图3-20 基本脉冲编码方案

码；若在零电平以下为负，判为“0”码。

以上两种编码，都是在一个码元的全部时间内发出或不发出电流（单极性），和发出正电流或负电流（双极性）。每一位编码占用了全部码元的宽度，故这两种编码都属于全宽码，也称作不归零码 NRZ (Non Return to Zero)。如果重复发送“1”码，势必要连续发送正电流；如果重复发送“0”码，势必要连续不送电流或连续发送负电流，这样使某一位码元与其下一位码元之间没有间隙，不易区分识别。而归零码可以改善这种状况。

单极性归零码，当发“1”码时，发出正电流，但持续时间短于一个码元的时间宽度，即发出一个窄脉冲；当发“0”码时，仍然完全不发送电流，所以称这种码为单极性归零码。

双极性归零码，其中“1”码发正的窄脉冲，“0”码发负的窄脉冲，两个码元的间隔时间可以大于每一个窄脉冲的宽度，取样时间是对准脉冲的中心。

不归零码在传输中难以确定一位的结束和另一位开始，需要用某种方法使发送器和接收器之间进行定时或同步；归零码的脉冲较窄，根据脉冲宽度与传输频带宽度成反比的关系，因而归零码在信道上占用的频带就较宽。

单极性码会积累直流分量，这样就不能使用变压器在数据通信设备和所处环境之间提供良好绝缘的交流耦合，直流分量还会损坏连接点的表面电镀层；双极性码的直流分量大大减少，这对数据传输是很有利的。

从以上讨论中可以发现，基带传输的另一个重要问题就是同步问题。接收端和发送端发来的数据序列在时间上必须取得同步，以便能准确地区分和接收发来的每位数据。这就要求接收端要按照发送端所发送的每个码元的重复频率及起止时间来接收数据，在接收过程中还要不断校准时间和频率，这一过程称为同步过程。在计算机通信与网络中，广泛采用的同步方法有位同步法和群同步法两种。

(1) 位同步。位同步使接收端对每一位数据都要和发送端保持同步。在数据通信中，习惯于把位同步称为“同步传输”。实现位同步的方法可分为外同步法和自同步法两种。

在外同步法中，接收端的同步信号事先由发送端送来，而不是自己产生也不是从信号中提取出来。即在发送数据之前，发送端先向接收端发出一串同步时钟脉冲，接收端按照这一时钟脉冲频率和时序锁定接收端的接收频率，以便在接收数据的过程中始终与发送端保持同步。

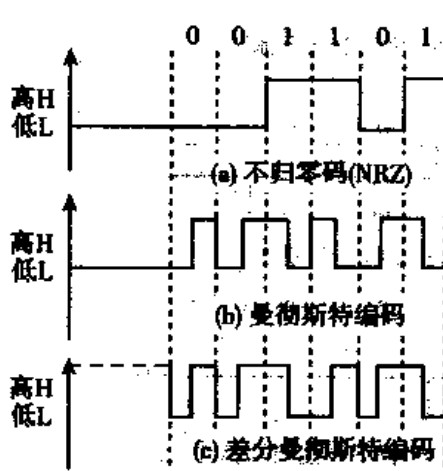


图 3-21 数字信号的同步编码

自同步法是指能从数据信号波形中提取同步信号的方法。典型例子就是著名的曼彻斯特编码，这种编码通常用于局域网传输。在如图 3-21 (b) 所示的曼彻斯特编码方式中，每一位的中间有一跳变，位中间的跳变既作为时钟信号，又作为数据信号；从高到低的跳变表示“1”，从低到高的跳变表示“0”。另外，还有一种如图 3-21 (c) 所示的差分曼彻斯特编码，这种编码每位中间的跳变仅提供时钟定时，而用每位开始时有无跳变表示“0”或“1”，有跳变表示“0”，无跳变表示“1”。由此可见，两种曼彻斯特编码方法都是将时钟和数据包含在信号流中，在传输代码信息的同时，也将时钟同步信号一起传输到对方，所以这种编码也称为自同步编码。

从曼彻斯特编码和差分曼彻斯特编码的脉冲波形中可以看出,这两种双极性编码的每一个码元都被调制成两个电平,所以数据传输速率只有调制速率的 $1/2$,也即对信道的带宽有更高的要求。但它们具有自同步能力和良好的抗干扰性能,在局域网中仍被广泛使用。

(2) 群同步。在群同步的通信系统中,传输的信息被分成若干“群”。所谓的“群”,一般是以字符为单位,在每个字符的前面冠以起始位、结束处加上终止位,从而组成一个字符序列。数据传输过程中,字符可顺序出现在比特流中,字符与字符间的间隔时间是任意的,即字符间采用异步定时,但字符中的各个比特用固定的时钟频率传输。在数据通信中,习惯于把群同步称为“异步传输”。字符间的异步定时和字符中比特之间的同步定时,是群同步即异步传输的特征。这种传输方式中,每个字符以起始位和停止位加以分隔,故也称“起一止”式传输。

群同步传输规程中的每个字符可由下列四部分组成:

- ① 1 位起始位,以逻辑“0”表示;
- ② 5~8 位数据位,即要传输的字符内容;
- ③ 1 位奇/偶校验位,用于检错,该部分可以不选;
- ④ 1~2 位停止位,以逻辑“1”表示,用作字符间的间隔。

群同步的字符格式见图 3-22。由图中可以看出,群同步是靠起始位(逻辑“0”)和停止位(逻辑“1”)来实现字符的定界及字符内比特的同步的。接收端靠检测链路上由空闲位或前一字符停止位(均为逻辑“1”)到该字符起始位的下降沿来获知一个字符的开始,然后按收、发双方约定的时钟频率对约定的字符比特数(5~8 位)进行逐位接收,最后以约定算法(奇/偶校验法)进行差错检测,完成一个字符的传输。发送器和接收器中近似于同一频率的两个约定时钟,在一段较短的时间内能够保持同步。在群同步传输中,起始位和停止位的作用是十分重要的。起始位指示字符的开始,并启动接收端对字符中比特的同步;而停止位则是作为字符之间的间隔位而设置的,没有停止位,紧跟其后的下一字符的起始位下降沿便可能丢失。

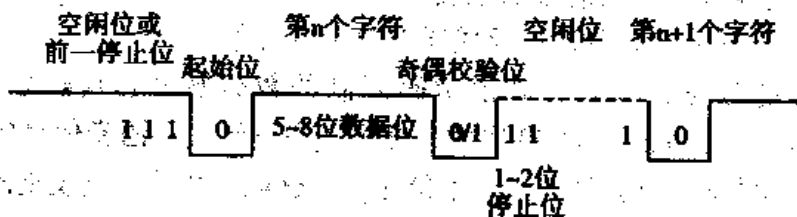


图 3-22 群同步的字符格式

群同步法只需保持每个字符的起始点同步,在群内则按约定的频率进行位的接收就可以了。这种方法实现简单,但需要添加诸如起始位、校验位和停止位等附加位,相对于同步传输来说,编码效率和信道利用率较低,一般用于低速数据传输的场合。

2. 模拟数据的数字信号编码

对模拟数据进行数字信号编码的最常用方法是脉码调制 PCM (Pulse Code Modulation),它常用于对声音信号进行编码。脉码调制是以采样定理为基础的,该定理从数学上证明:若对连续变化的模拟信号进行周期性采样,只要采样频率大于等于有效信号最高频率或其带宽的两

倍, 则采样值便可包含原始信号的全部信息, 利用低通滤波器可以从这些采样中重新构造出原始信号。设原始信号的最高频率为 $F_{\max}$, 采样频率为 F_s , 则采样定理可以下式表示:

$$F_s (=1/T_s) \geq 2F_{\max} \quad \text{或} \quad F_s \geq 2B_s$$

式中 T_s 为采样周期, $B_s (=F_{\max} - F_{\min})$ 为原始信号的带宽。

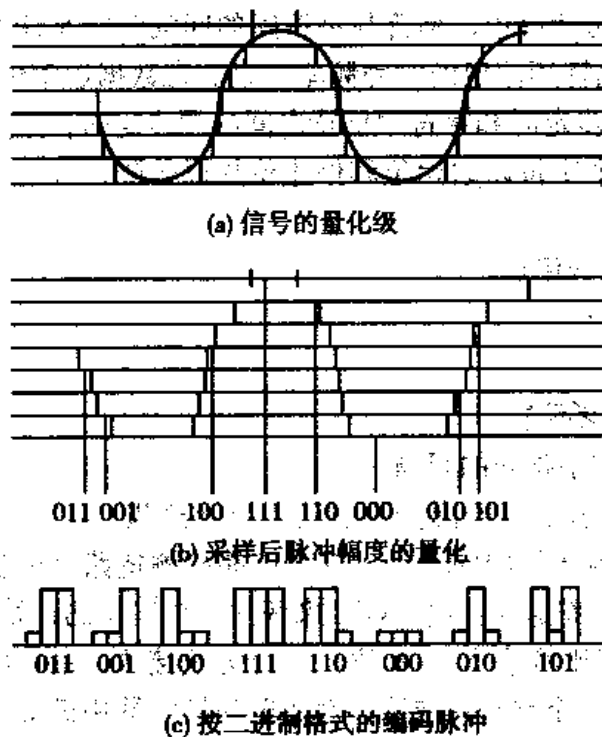


图 3-23 脉冲调制 (PCM) 原理

信号数字化的转换过程可包括采样、量化和编码三个步骤。图 3-23 说明了脉码调制的原理, 图中的波形按幅度被划分成 8 个量化级, 如要提高精度, 则可以分成更多的量化级。

第一步是采样, 以采样频率 F_s 把模拟信号的值采出; 第二步是量化, 使连续模拟信号变为时间轴上的离散值, 也就是分级的过程, 把采样的值按量级“取整”得到的是一个不连续的值; 第三步是编码, 将离散值编成一定位数的二进制数码。图中是 8 个量化级, 故取 3 位二进制编码就可以了。如果有 N 个量化级, 那么每次采样将需要 $\log_2 N$ 位二进制数码。目前在语音数字化脉码调制系统中, 通常分为 128 或 256 个量级, 即用 7 位或 8 位二进制数码来表示, 这样的二进制码组称为一个码字, 其位数称为字长。

在发送端经过这样的变换过程, 就可把模拟信号转换成二进制数码脉冲序列, 然后经过信道进行传输。在接收端, 先进行译码, 将二进制数码转换成代表原来模拟信号的幅度不等的量化脉冲, 然后再经过滤波 (如低通滤波器), 就可使幅度不同的量化脉冲还原成原来的模拟信号。

根据原始信号的频宽, 可以估算出脉码调制的数码脉冲速度。如果语音数据限于 4000Hz 以下的频率, 那么每秒钟 8000 次的采样可以完整地表示语音信号的特征。使用 7 位二进制表示每次采样的话, 就允许有 128 个量化级, 这就意味着, 仅仅是语音信号就需要有每秒钟 8000 次采样 $\times$ 每次采样 7 位 = 56000bps (即 56Kbps) 的数据传输速率。

模拟数据 (例如语音) 经过 PCM 编码转换成数字信号后, 就可以和计算机中的数字数据统一采用数字传输方式进行传输了。对于数字传输的数字电话、数字传真、数字电视等数字通信系统而言, 它具有下列两个显著的优点:

(1) 抗干扰性强。在模拟通信中, 当外部干扰和机内噪声叠加在有用的信号上时, 就很难完全将干扰和噪声去掉, 因而使输出信号的信噪比降低。而当数字信号在传输过程中出现上述情况时, 通过数字信号再生的方法, 可以容易地将干扰和噪声消除。当发送数字信号“1”时, 干扰噪声与有用信号叠加, 若这结果值不小于某一门限电平, 即仍可再生为“1”; 同样, 当发送“0”信号时, 干扰和噪声电平只要小于这一门限电平, 就仍能再生为“0”。

(2) 保密性好。信息被数字化后, 产生一个二进制数字编码序列 $I(t)$, 可以将 $I(t)$ 与

数字密码机产生的二进制密码序列 $C(t)$ 进行“模 2 加”运算，得到传送序列 $B(t)$ 。这样送到信道上传送的信号为 $B(t) = I(t) + C(t)$ ，（此处的“+”为模 2 加）。由于他人无法知道密码序列 $C(t)$ ，所以就无法破译原始信息 $I(t)$ 。密码序列 $C(t)$ 可以任意变换，这样就使通信系统的保密性大大提高。

当然，数字通信也有它的一些问题，例如模拟信号变成数字信号后占有较宽的频带、数字设备和联网技术较复杂、与现有的模拟通信设备之间也不免存在一些矛盾等等。

3.4.2 调制解调器

人们熟知的电话系统主要部分如图 3-24 所示，有本地回路、干线以及长途局和端局，这两种局都包含了用于切换电话的交换设备。从电话公司的端局到家庭或者小型业务部门的双线本地回路经常称为“最后一英里”（Last Mile），但实际上它的长度可以达到几英里。在过去，它一直传输模拟信号，因为转换为数字信号传输的成本相对比较高，当然这最后一段的模拟传输目前也正在发生变化。

当一台计算机希望通过模拟拨号线路发送数字数据的时候，这些数据首先必须转换成模拟的形式，才能通过本地回路进行传输。这个转换过程是通过一种称为调制解调器（MODEM）的设备来完成的。在电话公司的端局中，这些模拟数据又通过编解码器（CODEC）转换成数字形式，以便通过长途干线进行传输。

如果另一端也是一台带调制解调器的计算机，则必须再由编解码器进行相反的转换过程（从数字到模拟），以便通过目的地的一段本地回路。然后由目的地的调制解调器将模拟形式的数据反转换成计算机能接受的数字信号，这个过程如图 3-24 的右下角所示，图中的 ISP 1 (Internet Service Provider, Internet 服务供应商) 有一群调制解调器，每个调制解调器分别连接到不同的本地回路上。

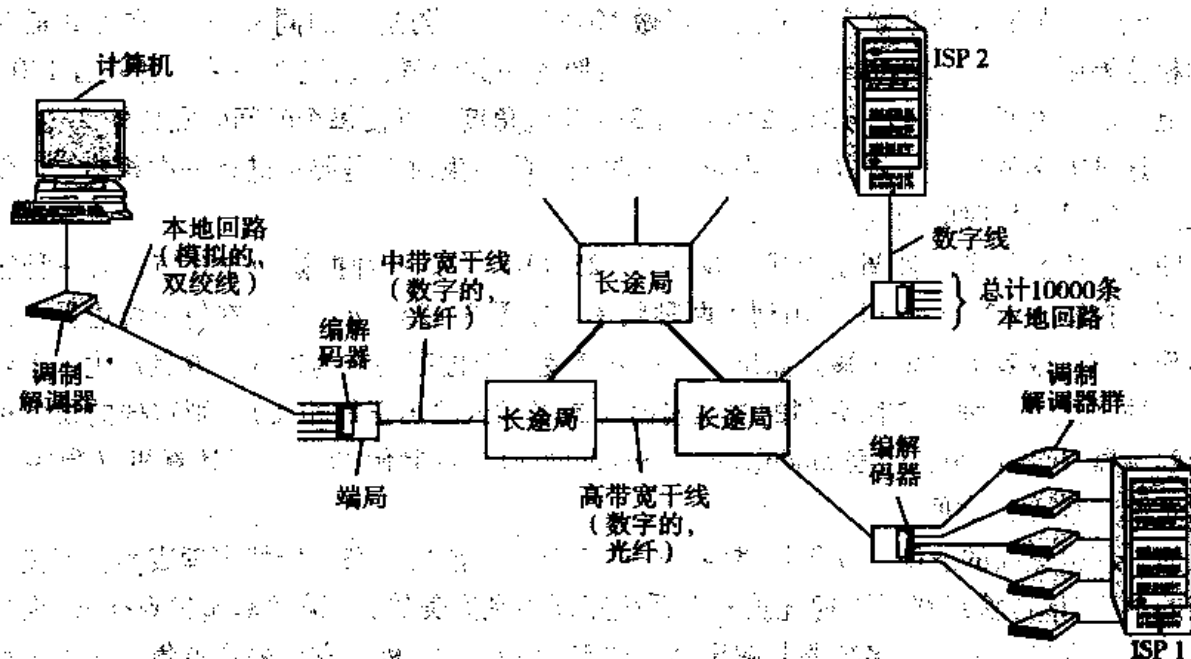


图 3-24 电话系统原理示意

模拟信号是由一个随时间变化的电压构成的。如果传输介质非常完美无缺的话，则接收方收到的信号与发送方送出的信号应该完全相同。然而，没有一种介质是完美无缺的，所以接收到的信号不可能与送出的信号完全一致。对于数字数据，信号之间的差异可能会导致错误。

传输线路存在三个主要的问题：衰减（Attenuation）、延迟畸变（Delay Distortion）和噪声（Noise）。衰减是指信号传播的过程中能量的损失。这种损失可以表示为每公里多少分贝。能量损失的数量跟频率有关。信号并非是一个简单的波形，而是傅立叶级数中的一些分量。每个分量被衰减的程度不同，因而导致了在接收方得到一个完全不同的傅立叶频谱。

更糟的是，不同的傅立叶分量在线路上的传播速度也不同。这种速度的差异会导致接收端信号的畸变。

另一个问题是噪声。热噪声是由线路中电子的随机运动而引起的，也是不可避免的。串音则是由于两根相距太近的线路的感应耦合而引起的。最后，还有脉冲噪声，这是由于尖峰干扰或者其它原因引起的。对于数字数据，脉冲噪声可能会淹没掉一位或者多位数据。

1. 模拟用户线路的调制解调器

由于上面讨论到的衰减和传播速度都是与信号频率有关的，不幸的是，在数字信号中用到的方波恰好有一个很宽的频谱，因而它的衰减和延迟畸变很严重。这种影响使得基带信号传输并不合适，除非是在低速和短距离的情况下使用。

为了绕过与基带信号相关的这些问题，特别是在电话线上使用的时候，采用了调制信号传输。首先引入 1000Hz ~ 2000Hz 范围内的一个连续波，称为正弦载波（Sine Wave Carrier）。它的振幅、频率或者相位被调制后可用来传输信息。在调幅（Amplitude Modulation）方法中，两种不同的振幅用来分别代表 0 和 1。在调频（Frequency Modulation，也称为 Frequency Shift Keying，移频键控）方法中，使用了两个（或多个）不同频率的连续波（这里术语 Keying（键控）在工业界也被广泛使用，当做 Modulation（调制）的同义词）。在形式最为简单的相位调制（Phase Modulation）中，载波按照统一的间隔，系统地平移 0 度或者 180 度。一种更好的方案是使用 45、135、225 或者 315 相位角度，以便每个时间间隔传输 2 位信息。而且，这种方案的另一个好处是，在每一个时间间隔结束时总是要求进行一次相移，这使得接收方很容易识别时间间隔的边界。

图 3-25 显示了三种调制形式。在图 3-25 (b) 中，一种振幅为非 0 值，另一种振幅为 0 值。在图 3-25 (c) 中，用到了两种频率。在图 3-25 (d) 中，在每个位边界上，或者出现相移，或者不出现相移。如果一个设备接受一个位序列作为输入，并且产生一个经过以上一种（或者多种）方法调制的载波输出（或者输入输出正好相反），则这样的设备称为调制解调器（MODEM，代表 Modulator - demodulator）。调制解调器位于计算机（数字）和电话系统（模拟）之间。

为了获得更高的速度，仅仅依靠增加采样率是不可能的。奈奎斯特定理表明，即使对于完美的 3000Hz 传输线路（更何况拨号电话线路还不是完美的），采样率超过 6000Hz 也是没有意义的。在实践中，大多数调制解调器采样率为 2400 次/秒，它们的焦点集中在每次采样如何表达更多的位信息。

每秒钟采样的次数可以用波特（Baud）来计量。在每一个波特中，发送一个码元

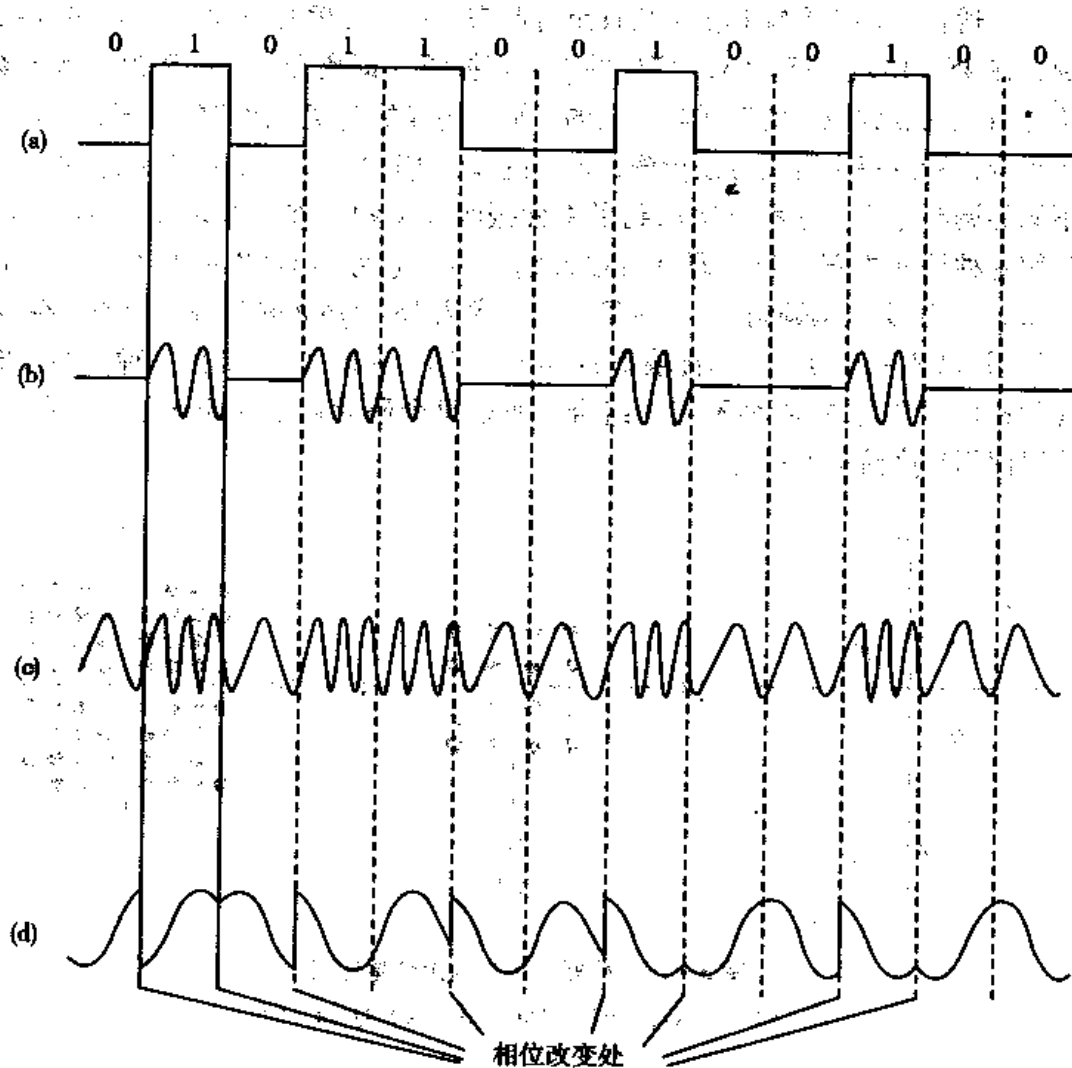


图 3-25 调制形式示意图

(a) 一个二进制信号; (b) 调幅; (c) 调频; (d) 相位调制

(Symbol)。因此，一条 n 波特的线路传输 n 码元/秒。例如，一条 2400 波特的线路大约每 $416.667 \mu s$ 发送一个码元。如果该码元用 0 伏电压代表逻辑 0，1 伏电压代表逻辑 1，则位传输率为 2400bps。然而，如果 0、1、2 和 3 伏电压都使用的话，则每个码元可以包含 2 位，因此，2400 波特的线路可以传输 2400 码元/秒，数据传输率为 4800bps。类似地，如果使用四种可能的相移的话，则每个码元也可以表达 2 位，所以同样地，位传输率为波特率的两倍。后一种技术已广泛使用，称为 QPSK (Quadrature Phase Shift Keying, 正交相移键控)。

带宽、波特、码元和位传输率的概念通常很容易混淆，所以，这里重新说明一次。一种介质的带宽是指在最小衰减的情况下能够通过这种介质的频率范围。它是介质的一种物理特性（通常从 0 到某一个最大的频率），度量单位为 Hz（赫兹）。波特率是指每秒钟的采样次数。每个采样发送一份信息，这份信息称为码元。因此，波特率和码元率是相同的。调制技术（比如 QPSK）决定了每个采样的位数。位传输率是指一条信道上发送的信息的数量，它等于每秒采样数乘以每个采样的位数。

实际应用中，高级的调制解调器都组合使用了几种调制技术，以便在每个波特中传输尽

可能多的位。通常，多个振幅和多个相移组合起来就可以传输几位/波特。在图 3-26 (a)，可以看到，在 45、135、225 和 315 度处的点，其振幅（即离开原点的距离）为常数。一个点的相移是由从该点到原点的直线与正向的 x 轴所构成的角度来决定的。图 3-26 (a) 有 4 种有效的组合，所以每个码元可以传输 2 位。这就是 QPSK。在图 3-26 (b) 中，可以看到另一种不同的调制方案。这种方案用到了 4 种振幅和 4 种相移，总共有 16 种不同的组合。因此，利用这种调制方案，每个码元可以传输 4 位。它称为 QAM-16 (Quadrature Amplitude Modulation, 正交振幅调制)。有时候也使用术语 16-QAM 来代替。例如，在 2400 波特线路上，利用 QAM-16 可以达到传输率 9600bps。图 3-26 (c) 是另一种调制方案，它也涉及振幅和相位。它允许 64 种不同的组合，所以每个码元可以传输 6 位。它称为 QAM-64。也可以使用更高阶的 QAM。

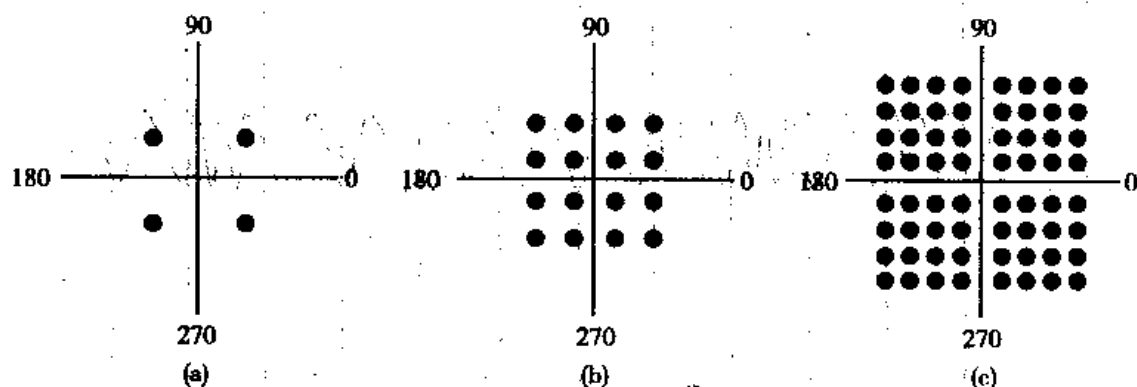


图 3-26 振幅和相位的组合星座图

(a) QPSK; (b) QAM-16; (c) QAM-64

图 3-26 中的三个图形分别显示了振幅和相位的几种合法组合，这些图形称为星座图 (Constellation Diagram)。每个高速调制解调器标准都有自己的星座模型，并且只能与使用了同样星座模型的调制解调器才可以通信（不过，大多数调制解调器都可以模拟所有低速的调制解调器）。

由于星座模型中有许多点，所以，在检测到的振幅和相位中，即使很小量的噪声也可能导致一个错误，而且这个错误又可能隐含着许多错误的位。为了降低出错的可能性，高速调制解调器的标准都有纠错机制，其做法是在每个采样中增加一些额外的位。这样的方案称为 TCM (Trellis Coded Modulation, 格子架编码调制)。举例来说，V.32 调制解调器标准使用了 32 个星座点，每个码元传输 4 个数据位和 1 个奇偶校验位，在 2400 波特上可以达到 9600bps (带纠错特性)。它的星座模型如图 3-27 (a) 所示。之所以绕着原点旋转 45 度，是出于工程的原因。旋转的和不旋转的星座模型具有同样的信息传输能力。

称为 V.32bis 的 14400bps 这个速度是这样得来的：在 2400 波特上，每个采样传输 6 个数据位和 1 个奇偶校验位。它的星座模型有 128 个点，如图 3-27 (b) 所示，它使用了 QAM-128。传真调制解调器就使用这种速度来传输扫描之后的页面位图 (Bit Map)。

V.34 的电话调制解调器它在 2400 波特上，每个采样传输 12 个数据位，因此，数据传输率为 28.8Kbps。在这个系列中，最后一种调制解调器是 V.34bis，它在 2400 波特上，每个采样传输 14 个数据位，所以可达到 33.6Kbps。

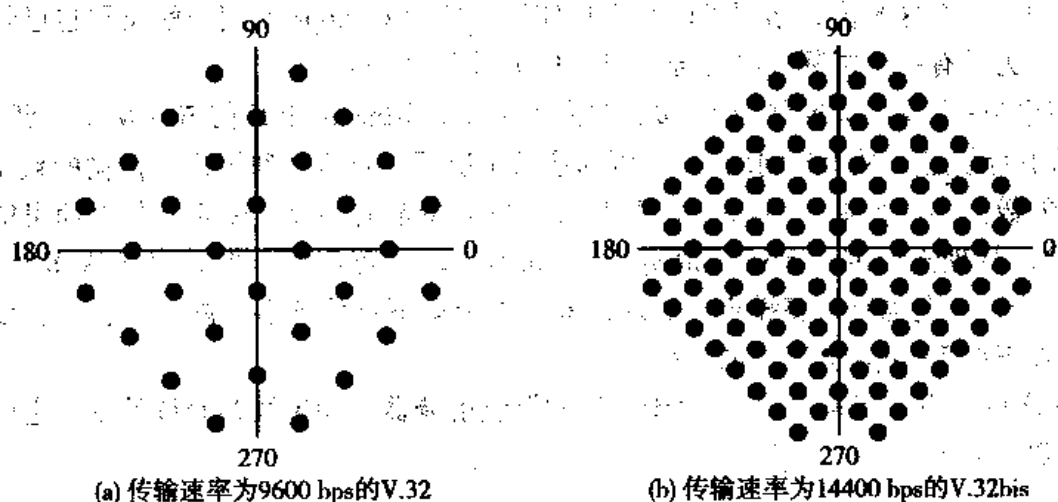


图 3-27 V.32 和 V.32bis 的星座图

为了进一步提高实际的数据传输率，许多调制解调器在传输数据之前，先对数据进行压缩，这样得到的有效数据传输率可以高于 33.6Kbps。另一方面，几乎所有的调制解调器在开始传输用户数据之前，先对线路进行测试，如果发现质量不好的话，则退回到低一点的速率上（低于标定的最大速率）。因此，用户观察到的有效速率可能会低于、等于，或者高于正式标定的速率。

所有的调制解调器都允许同时在两个方向上传输（做法是，在不同的方向上使用不同的频率）。允许在两个方向上同时进行数据传输的连接称为全双工的（Full Duplex）。一条双车道的公路是全双工的。如果一个连接允许任何一个方向的流量通过，但是同一时刻只有一个方向可以传输数据，则这个连接称为半双工的（Half Duplex）。单条铁路轨道是半双工的。如果一个连接只允许一个方向的数据通过，则称它为单工的（Simplex）。单向的马路是单工的。单工连接的另一个例子是：一根光纤的一头是激光源，另一头是一个光检测器。

标准调制解调器为什么在 33.6Kbps 这里停住了呢？其原因是，电话系统的香农定律限制大约是 35Kbps，所以，比 35Kbps 更快的速度会违反物理学（热力学部分）的法则。

但是，为什么会有 35Kbps 的理论限制呢？它与本地回路的平均长度，以及这些线路的质量有关系。35Kbps 是由本地回路的平均长度决定的。在图 3-24 中，发起于左侧计算机并终止于 ISP1 的呼叫要经过两个本地回路传输模拟信号，一个本地回路在源处，另一个本地回路在目的地。这两个本地回路都在信号中加入了噪声。如果可以从消除掉一个本地回路，则最大速率就可以增加一倍。

ISP2 正是这样的情形。它有一条纯的数字线路，直接到达最近的端局。在干线上使用的数字信号直接被传送给 ISP2，从而消除了它这一端的“编解码器、调制解调器和模拟传输”的过程。因此，当连接的一端是数字信号传输的时候（现在大多数 ISP 都是这样的），则最大数据传输率可以达到 70Kbps。如果两个家庭用户通过调制解调器和模拟线路来连接，则最大速率是 33.6Kbps。

为什么使用 56Kbps 调制解调器，其理由与奈奎斯特理论有关系。电话信道的带宽大约是 4000Hz（包括防护频段）。因此，每秒钟的最大独立采样次数为 8000。在美洲，每个采样的位数是 8，其中 1 位被用于控制的用途，因而每秒钟允许传输用户数据 56000 位。

在欧洲,所有这 8 位数据都可以给用户使用,所以 64Kbps 的调制解调器也已经在使用了,但是,为了有一个国际性的标准约定,故选择了 56000。

这种调制解调器的标准称为 V.90。它提供了 33.6Kbps 的上行信道(从用户到 ISP)和 56Kbps 的下行信道(从 ISP 到用户),因为通常情况下,从 ISP 到用户方传输的数据比另一个方向上的数据多(比如,请求一个 Web 页面只需少量的字节,而实际的页面可能有几兆字节数据)。从理论上讲,上行信道宽于 33.6Kbps 也是可能的,但是对于许多本地回路,即使在 33.6Kbps 上也有太多噪声,所以,最后决定给下行信道多分配一点带宽,以便增加下行信道真正在 56Kbps 上工作的几率。

V.90 之后的下一步是 V.92。对于这样的调制解调器,如果线路允许的话,它的上行信道可以达到 48Kbps。

2. 数字用户线路 (Digital Subscriber Lines)

当电话最后达到了 56Kbps 的时候,有线电视正在提供高达 10Mbps 的速度(在共享电缆上),卫星公司正在计划提供上行 50Mbps 的速度。Internet 访问已经成为日渐重要的一部分,这时,电话公司(LEC)开始意识到,需要一种更具竞争力的产品。利用本地回路提供新的数字服务。所提供的带宽比标准的电话服务要多得多,这样的服务称为宽带(Broadband)。

有许多相互重叠的服务都使用了 xDSL (Digital Subscriber Line, 数字用户线路)这样的名称,只是 x 不同而已。下面将讨论最为流行的服务: ADSL (Asymmetric DSL, 非对称数字用户线路)。

调制解调器之所以如此慢的原因是,电话的发明是为了承载人类的语音,而且整个电话系统也为了这个目的而进行了多次而仔细的优化。数据就好像不是自己亲生的子女,一直没有被认真地对待。每条本地回路都在端局那里被终止,就在这个终止的点上,有一个滤波器把所有 300Hz 以下、3400Hz 以上的频率都衰减。截止的地方并不尖锐——300Hz 和 3400Hz 都是 3 分贝点——所以,尽管两个 3 分贝点之间的距离是 3100Hz,但是,这一段带宽也常常被当做 4000Hz 来引用。因此,数据在过去很长一段时期内也被限制在这一窄窄的频段之中。

使 xDSL 工作的诀窍是,进来的线路被连接到另一种不同的交换机上,这种交换机上没有滤波器,因而可以充分发挥本地回路的全部承载能力。而不再是人工加入的滤波器所建立起来的 3100Hz 带宽限制。

但是,本地回路的能力依赖于几方面的因素,包括它的长度、粗细和综合质量。距离与潜在带宽之间的函数关系如图 3-28 所示。该图假设所有其它的因素都是最佳的(新的线路、捆扎得也不错,等等)。

该图对于电话公司来说意味着一个问题。当电话公司承诺提供某一个速度的传输率的时候,它同时也划定了一个以端局为中心的圆,超出了这个圆就无法提供这样的服务。公司选定的速度越低,则圆的半径越大,从而覆盖面越广。但是,速度越低,则这项服务的吸引力就越小,愿意付钱购买这项服务的人就越少。

所有的 xDSL 服务都有一些特定的设计目标。第一,这些服务必须在现有的 3 类双绞线本地回路上工作。第二,它们不能影响顾客原来的电话机和传真机。第三,它们必须比

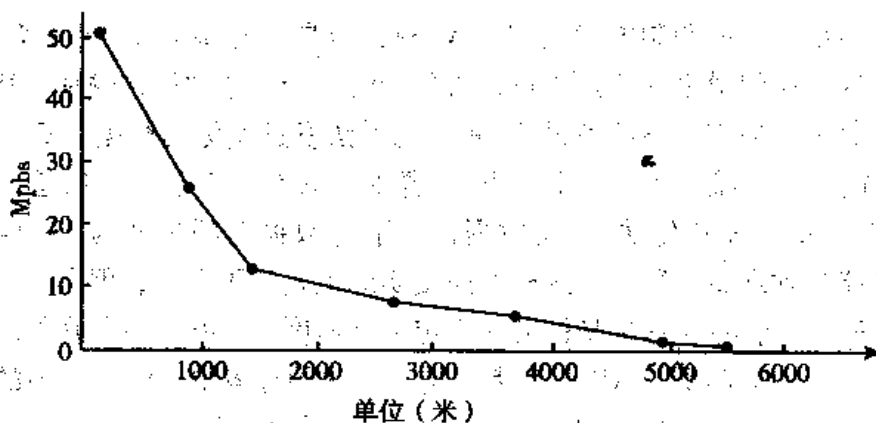


图 3-28 3 类 UTP 用于 DSL 时带宽与距离的关系

56Kbps 还要快。第四，这些服务应该总是可用的，并且按月租方式收费，而不是按每分钟收费。

最初的 ADSL 服务是 AT&T 公司提供的，它的工作原理是，将本地回路上可供使用的频谱（大约是 1.1MHz）分成三个频段：POTS（Plain Old Telephone Service，传统的简单电话服务）、上行数据流（从用户到端局）和下行数据流（从端局到用户）。使用多个频段范围的技术称为频分多路复用。

图 3-29 显示了一种称为 DMT（Discrete MultiTone，离散的多信道调制）的频段划分方法。它将本地回路上的 1.1MHz 频谱分成 256 条独立的信道，每条信道 4312.5Hz。信道 0 用于 POTS。信道 1~5 没有被使用，目的是让语音信号与数据信号避免相互干扰。在剩下的 250 条信道中，一条用于上行控制，另一条用于下行控制，其它的信道全部用于用户数据。

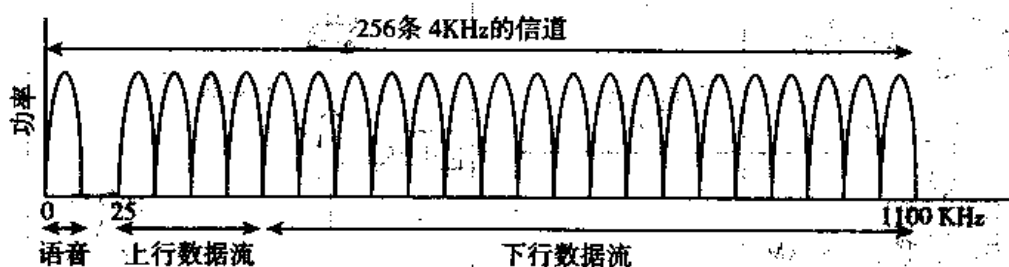


图 3-29 使用 DMT 的 ADSL 频谱划分方案

从原理上讲，剩下的每条信道都可以被用作全双工数据流，但是谐波、串音和其它的影响使得实际的系统性能大大低于理论限制。ADSL 供应商可以决定多少信道用于上行数据流，多少信道用于下行数据流。上行和下行各 50% 的做法在技术上是可行的，但是大多数供应商倾向于将 80%~90% 的带宽分配给下行信道，因为大多数用户的下载数据量超过上传数据量。这种选择正好表达了 ADSL 中的第一个字母“A”（非对称）的含义。一种常见的分法是，32 条信道用于上行数据流，其余的用于下行数据流。

ADSL 标准（ANSI T1.413 和 ITU G.992.1）允许的速度可以达到 8Mbps 下行速度和 1Mbps 上行速度。然而，很少有供应商提供这样的速度。通常情况下，供应商提供 512Kbps 下行速度和 64Kbps 上行速度（标准服务），以及 1Mbps 下行速度和 256Kbps 上行速度（高

级服务)。

每一条信道内部使用的调制方案类似于 V. 34，但是采样率为 4000 波特，并非 2400 波特。系统一直监视每条信道中的线路质量，必要的时候会调整数据传输率，所以不同的信道可能会有不同的数据传输率。系统通过 QAM 调制方法发送实际的数据，每个波特可以达到 15 位，所使用的星座图类似于图 3-26 (b)。譬如，共有 224 条下行信道，每条信道工作在 4000 波特，并且每个波特传输 15 位数据，则下行数据流的带宽为 13.44Mbps。在实践中，信噪比不可能非常理想，所以，这样的速度实际上是达不到的，但是，在较短的高质量回路上，8Mbps 是有可能的（这也是标准中指定下行速度为 8Mbps 的原因）。

图 3-30 显示了一个典型的 ADSL 部署结构。在这种方案中，电话公司的技术人员必须在用户的家里安装一个 NID (Network Interface Device, 网络接口设备)。在靠近 NID 的地方是一个分离器 (Splitter) (有时候，分离器也组合在 NID 中)，分离器是一个模拟滤波器，它将 POTS 使用的 0~4000Hz 频段与数据分离开。POTS 信号被路由到原来的电话机或者传真机，而数据信号则被路由到 ADSL 调制解调器中。ADSL 调制解调器实际上是一个数字信号处理器，相当于一组 25QAM 调制解调器，它们在不同的频率上并行地工作。由于当前大多数的 ADSL 调制解调器都是外置的，所以计算机与它必须通过高速方式连接起来。通常的做法是，在计算机中安装一块以太网卡，然后运行一个只包含两个节点（该计算机和 ADSL 调制解调器）的以太网。偶尔情况下，也可以使用 USB 端口来代替以太网。毫无疑问，在将来，内置的 ADSL 调制解调器也一定会出现。

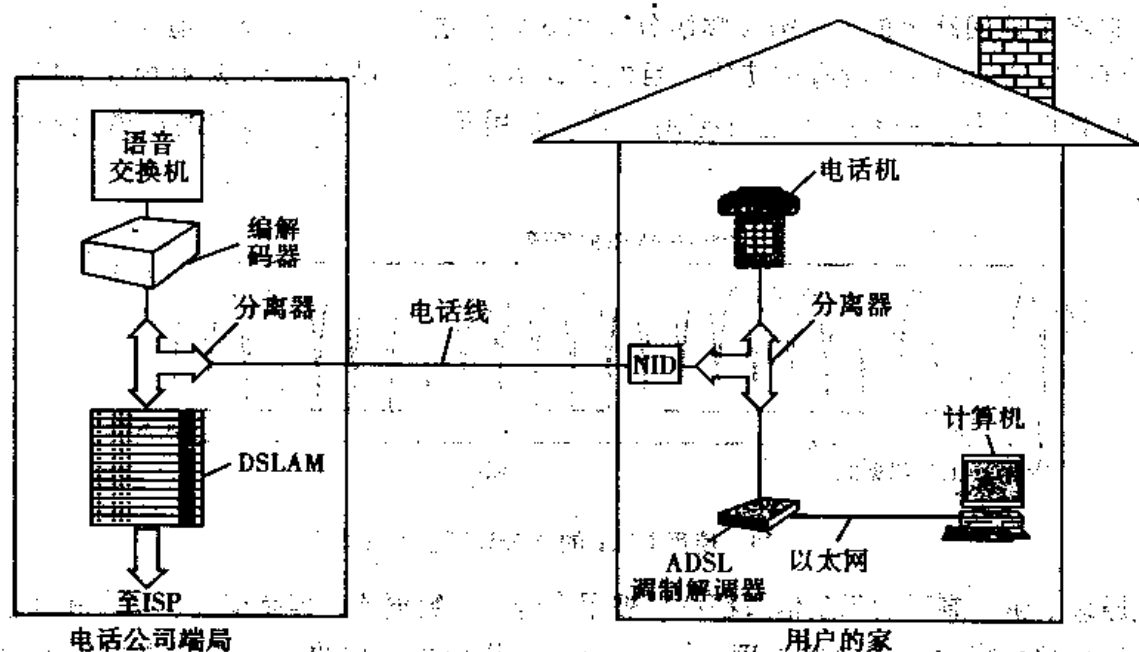


图 3-30 一个典型的 ADSL 设备配置图

在线路的另一头，即电话公司的端局，也要安装一个对应的分离器。信号的语音部分在这里被过滤出来，并送到语音交换机中。频率在 26KHz 以上的信号则被路由到一种新的称为 DSLAM (Digital Subscriber Line Access Multiplexer, 数字用户线路访问复用器) 的设备中，该设备也包含一个数字信号处理器，与 ADSL 调制解调器中的一样。一旦数字信号被恢复成一个位流，就可以重新构造出分组来，然后送给 ISP。

图3-30中的设计方案也有一个缺点，那就是，在用户的家里需要安装一个NID和分离器。这些设备只能由电话公司的技术人员来安装，因而就会招致昂贵的“流动服务”（即让技术人员上门提供服务）。因此，另外一种不需要分离器的设备也已经被标准化了。它的非正式名称为G.lite，而ITU的标准号为G.992.2。它的部署结构与图3-30一样，只不过没有分离器。现有的电话线直接可以使用。惟一的区别在于，在电话或者ADSL调制解调器与电话线的每个插孔中插入了一个微滤波器。电话的微滤波器是一个低通滤波器，它消除了3400Hz以上的频率成分；ADSL调制解调器的微滤波器是一个高通滤波器，它消除了26KHz以下的频率成分。然而，这个系统的可靠性不如带分离器的系统，所以G.lite用起来至多只能达到1.5Mbps（相比之下，带分离器的ADSL可以达到8Mbps）。

3.5 数据交换技术

数据经编码后在通信线路上进行传输的最简单形式，是在两个互连的设备之间直接进行数据通信。但是，网络中所有设备都直接两两相连是不现实的，通常要经过中间节点将数据从信源逐点传送到信宿，从而实现两个互连设备之间的通信。这些中间节点并不关心所传数据的内容，而是提供一种交换功能，使数据从一个节点传到另一个节点，直至到达目的地为止。通常将作为信源或信宿的一批设备称为网络站，而将提供中间通信的设备称为节点。这些节点以某种方式用传输链路相互连接起来，每个站都连接到一个节点上，这些节点的集合便称为通信网络。如果所连接的设备是计算机和终端的话，那么节点集加上一些站就构成计算机网络。图3-31所示为一个交换网络的拓扑结构。按所用的数据传送技术划分，交换网络又可分为电路交换网、报文交换网和分组交换网。

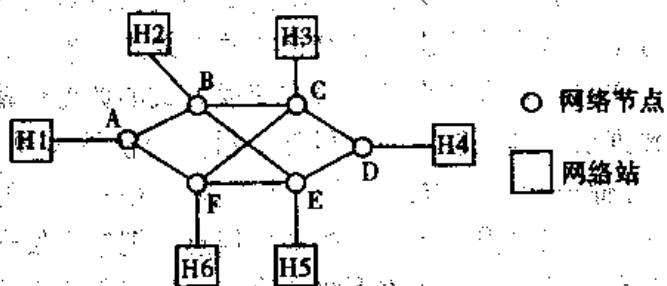


图3-31 交换网络的拓扑结构

3.5.1 电路交换 (Circuit Switching)

电话交换网是使用电路交换技术的典型例子。采用电路交换技术进行数据传输期间，在源节点与目的节点之间有一条利用中间节点构成的专用物理连接线路，直到数据传输结束。如果两个相邻节点之间的信道容量很大时，这两个相邻节点之间可以复用多条电路。用电路交换技术完成数据传输要经历以下电路建立、数据传输、电路拆除三个过程：

(1) 电路建立。如同打电话先要通过拨号在通话双方间建立起一条通路一样，在传输数据之前，也要先经过呼叫过程建立一条端到端（站到站）的电路。例如，H1站要与H3站建立一个连接，典型的做法是，H1站先向与之连接的A节点提出请求，然后A节点在通向C节点的路径中找到下一个支路。比如，根据路径信息，A节点选择经B节点的电路，在此电路上分配一个未用的通道（使用时分多路复用TDM或频分多路复用FDM），并告诉B它还要连接C节点；B再呼叫C，建立电路BC，最后，节点C完成到H3站的连接。这样

在 A 与 C 之间就有了一条专用电路 ABC，用于 H1 站与 H3 站之间的数据传输。其间，会有如下几种特殊情况发生：若 AB 电路的通信容量已经饱和或 B 出故障，则 A 呼叫 B 失败，此时 A 就要另辟途径呼叫 F，最后可能建立电路 AFC；若 B 呼叫 C 失败，则 B 可以去呼叫 E，再由 E 呼叫 C，建立 ABEC 电路；若由于暂时的阻塞或永久性的故障，所有途径都试过后仍不能建立连接，那么 A 到 C 就不能传送数据。

(2) 数据传输。电路 ABC 建立了以后，数据就可以从 A 发送到 B，再由 B 交换到 C；C 也可以经 B 向 A 发送数据。这种数据传输有最短的传播延迟，并且没有阻塞的问题，除非有意外的线路或节点故障而使电路中断。在整个数据传输过程中，所建立的电路必须始终保持连接状态。

(3) 电路拆除。数据传输结束后，由某一方（A 或 C）发出拆除请求，然后逐节拆除到对方节点。被拆除的信道空闲后，就可被其它通信使用。

电路交换方式的优点是数据传输可靠、迅速，数据不会丢失且保持原来的序列。缺点是在某些情况下，电路空闲时的信道容量被浪费；另外，当数据传输阶段的持续时间不长时，电路建立和拆除所用的时间就得不偿失。因此，它适用于系统间要求高质量的大量数据传输的情况。这种通信方式的计费方法一般按照预订的带宽、距离和时间来计算。

3.5.2 报文交换 (Message Switching)

在有些应用场合里，端点之间交换的数据是随机性和突发性的。如果此时采用电路交换方法，就会暴露出电路交换方法的缺点，即导致信道容量和有效时间的浪费。一种更直接的传送方式是报文交换。报文交换方式的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。报文交换不需要在两个站之间建立专用通路，传送方式采用“存储—转发”方式。当一个站要发送一个报文时，它先将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。每个节点在收下整个报文并检查无错误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无须先通过呼叫建立连接。

在电路交换的网络中，每个节点是一个电子的或者是机电结合的交换设备，这种设备发送二进制位与接收二进制位一样快。而报文交换节点通常是一台小型计算机，它具有足够的存储容量来缓存进入的报文。一个报文在每个节点的延迟时间，等于接收报文所需的时间加上向下一个节点转发所需的排队延迟时间之和。再用图 3-31 来考察一个从 H1 站到 H3 站的报文交换：H1 站把 H3 站的地址附加在报文上，然后把它发送到 A 节点；A 节点存储该报文并且决定下一个路径的支路（假定到节点 B）；A 节点为了在 AB 线路上传送这个报文，要进行报文排队；当链路可用时，就把报文发送到 B 节点，B 节点再继续将报文转送到 C 节点，并且最后到达 H3 站。

与电路交换比较，报文交换有如下优点：

(1) 电路利用效率高。由于许多报文可以分时共享两节点之间的通道，所以对于同样的通信量来说，对电路的传输能力要求较低。

(2) 在电路交换网络上，当通信量变得很大时，就不能接受新的呼叫。而在报文交换

网络上,通信量大时仍然可以接收报文,不过传送延迟会增加。

(3) 报文交换系统可以把一个报文发送到多个目的地,而电路交换网络很难做到这一点。

(4) 报文交换网络可以进行速度和代码的转换。因为每个站可以用它特有的数据传输率连接到其它节点,所以两个不同传输速率的站也可以相互连接;报文交换网络还能转换数据的格式(例如从 ASCII 码转换成 EBCDIC 码),这些特点在电路交换系统中往往很难做到。

报文交换的主要缺点是,它不能满足实时或交互式的通信要求,报文经过网络的延迟时间长且不定。因此,这种方式不能用于语音连接,也不适合于交互式终端到计算机的连接。有时节点收到过多的数据而无空间存储或不能及时转发时,就不得不丢弃报文,而且发出的报文不按顺序到达目的地。其计费一般是根据通信的流量和时间来计算。报文交换也已不再使用。

3.5.3 分组交换(Packet Switching)

为了更好地利用信道容量,并降低节点中数据量的突发性,可以将报文交换改进为分组交换,即将一个报文分成若干个分组,每个分组的长度有一个上限,典型的最大长度是数千位。

还以图 3-31 为例,考察 H1 站到 H3 站的一个分组传输过程:分组中包括数据和目的站地址,H1 站发送这个分组到 A 节点,A 节点暂存这个分组,然后把它发送到 B 节点,B 节点再把它发送到 C 节点,最后送到 H3 站。

从表面上看,分组交换与报文交换相比没有什么特殊的优点。但值得注意的是,有限长度的分组使每个节点所需要的存储能力降低了,分组可以存储在内存中,而不是硬盘上,提高了交换速度。分组交换适用于交互式通信,如终端与主机通信。分组交换的具体过程又可分为虚电路分组交换和数据报分组交换两种。

1. 虚电路方式

在虚电路(Virtual Circuit)方式中,为进行数据传输,网络的源节点和目的节点之间先要建立一条逻辑通路。在图 3-31 中,假设 H1 站有一个或多个报文要发送到 H3 站去,那么它首先要发送一个呼叫请求分组到 A 节点,请求建立一条到 H3 站的连接。A 节点决定到 B 节点的路径,B 节点再决定到 C 节点的路径,C 节点最终把呼叫请求分组传送到 H3 站。如果 H3 站允许接受这个连接,就发送一个呼叫接受分组到 C 节点,这个分组通过 B 和 A 返回到 H1 站。至此,H1 站和 H3 站就可以在已建立的逻辑连接上或者说在虚电路上交换数据了。每个分组除了包含数据之外还得包含一个虚电路标识符。在预先建立好的路径上的每个节点都知道把这些分组引导到哪里去,不再需要路由选择判定。于是来自 H1 站的每一个数据分组都通过节点 A、B 和 C;来自 H3 站的每个数据分组都经过节点 C、B 和 A。最后,由某一个站用清除请求分组来结束这次连接。

无论何时,一个站都能和任何站建立多个虚电路,也能与多个站建立虚电路。这种传输数据的逻辑通路就是虚电路,它之所以是“虚”的,是因为这条电路不是专用的。每条虚

电路支持特定的两个端点之间的数据传输，两个端点之间也可以有多条虚电路为不同的进程服务，这些虚电路的实际路由可能相同，也可能不同。

虚电路技术的主要特点是：在数据传送之前先建立站与站之间的一条路径。需要注意的是，这样做并不是说它像电路交换那样有一条专用通路，分组在每个节点上仍然需要缓冲，并在线路上进行排队等待输出。

2. 数据报方式

在数据报方式中，每个分组的传送是被单独处理的，就像报文交换中的报文一样。每个分组被称为一个数据报，每个数据报自身携带足够的地址信息。一个节点接收到一个数据报后，根据数据报中的地址信息和节点所储存的路由信息，找出一个合适的出路，把数据报原样地发送到下一节点。因此，当某一站点要发送一个报文时，先把报文拆成若干个带有序号和地址信息的数据报，依次发送到网络节点上。此后，各数据报所走的路径就可能不再相同，因为各个节点随时根据网络流量、故障等情况选择路由，因此不能保证各个数据报按顺序到达目的地，有的数据报甚至会在途中丢失。整个过程中，没有虚电路建立，但要为每个数据报作路由选择。

例如在图 3-31 中，若 H1 站要将由 3 个数据报分组组成的报文发送到 H3 站，它先按顺序依次将分组发送到 A 节点，A 节点再对每个数据报做出路由选择。当数据报 1 进入时，假设 A 节点检测到去 B 节点的队列比去 F 节点的队列短，便选择去 B 节点的路径，数据报 2 也同样处理；但是对于数据报 3，可能节点 A 发现去 F 节点的队列最短，因此把数据报 3 发送到 F 节点。这样，具有相同目的地址的数据报就不一定遵循相同的路径，数据报 3 有可能正好抢在数据报 2 之前到达节点 C。于是这三个数据报可能不按发送顺序到达 H3 站，也就是说要对到达 H3 站的数据报重新按原来顺序进行排序。

可以对虚电路和数据报这两种操作方式作一比较。虚电路分组交换适用于两端之间的长时间数据交换，尤其是在交互式会话中每次传送的数据很短的情况下，可免去每个分组要有地址信息的额外开销。它提供了更可靠的通信功能，保证每个分组正确到达，且保持原来顺序。还可对两个数据端点的流量进行控制，接收方在来不及接收数据时，可以通知发送方暂缓发送分组。但虚电路有一个弱点，当某个节点或某条链路出现故障而彻底失效时，则所有经过故障点的虚电路将立即破坏。数据报分组交换省去了呼叫建立阶段，它传输少量分组时比虚电路方式简便灵活。在数据报方式中，分组可以绕开故障区而到达目的地，因此故障的影响面要比虚电路方式小得多。但数据报不保证分组的按序到达，数据的丢失也不会立即知晓。

3.5.4 高速交换

随着光传输技术的发展，带宽已不再是网络的瓶颈。技术的进步使得原本分组交换的优势和电路交换的缺陷不再有意义。结合分组交换和电路交换的优势，并与光传输技术融合是高速交换的趋势。

从传统的观点看，电路交换技术因为其资源利用率低，不适用于数字业务网络；分组交换技术通过统计复用方式，提高了资源利用率，而且当出现线路故障时，分组交换技术可通

过重新选路重传,提高了可靠性,是当今因特网技术的主流。但是现状是:许多线路资源由于缺少交换能力而未被使用,使用的线路资源利用率往往不到10%,路由器平均一年的宕机时间不到5s,发生故障的概率很小。因此资源利用率和可靠性对于当今选择交换技术没有意义。另一方面,当分组交换选择面向非连接的工作方式时,对于一些实时性业务有着先天的缺陷,虽然有资源预留等一系列缓解之道,但并不是以解决根本问题,因此这些业务的QoS问题较为复杂。而电路交换技术是面向连接的,很适用于实时业务。与分组交换技术相比,电路交换技术实现简单,价格低廉,易于用硬件高速实现,且由于其不需要缓冲区,因此它易于与光技术融合。如果能很好地解决电路交换技术的用户与WDM(波分复用)之间的流量力度不匹配问题,因特网可能会完全采用电路交换技术。

当前因特网的主干线路采用的是SONET(同步光纤)或是SDH(同步数字系列),就其本质应属于电路交换技术。而本地网接入则采用的是IP路由器,属于分组交换技术。所以当今的因特网采用的应是电路交换技术和分组交换技术结合,而且在主干线中,电路交换技术的用户与WDM(波分复用)之间的流量力度不匹配问题也不存在。电路交换技术与光交换技术在本质上极为相似,因此随着速率的增长,自然而然引入了光传输技术,通过光电转换技术,实现了高速交换,极大地扩展了带宽。

长期以来,高速全光网的梦想一直受到交换问题的困扰。因为传统的交换技术需要将数据转换成电信号进行交换,然后再转换为光信号传输。虽然传统的交换技术与光技术结合,在带宽和速度上有十分积极的意义,但是其中的光电转换设备体积过于庞大且费用昂贵,因此自然地呼唤光交换技术。目前光交换技术发展主要有以下几种:

1. 微电子机械系统(MEMS)的光交换机

基于MEMS的光交换机在入口光纤和出口光纤之间使用微镜阵列,阵列中的镜元可以在光纤之间任意改变角度来改变光束传输方向,达到实时对光信号进行重新选路的目的。当一路波长光信号照到镜面时,镜面倾斜以便将其导引到某一特定出口光纤中,从而实现光路倒换的目的。

2. 无交换式光路由器

它使用具有波长发射和控制功能的交换功能模块取代了传统的外围光开关交换网络。其关键模块是一种自由空间色差校正凹面光栅,通过它将入射光线阵列中的波长信道进行发散后,再聚集到出射光纤阵列中相互独立的单路光纤上,就可实现 91×91 的波长路由器功能。

3. 阵列波导光栅路由器

构成阵列波导光栅的是许多长度按 L 线性递增(即各路光波的相位差恒定)的光臂,可实现波分复用与解复用以及静态波长路由功能,并具备双向传输的特性。WDM信号从一端口输入,经一入射波导到达聚集平面波导,被衍射耦合到各阵列波导中,各路光经不同的相位延迟后在出射波导端合成不同波长的光波。如果输入端只有单路的多波长信号,则构成 $1 \times N$ 的解复用器,如果输入端为 M 路多波长信号,则构成 $M \times N$ 的路由器。

光交换的优点在于光信号通过光交换单元时,无须经过光电/电光转换,因此它不受监

测器和调制器等光电器件响应速度的限制，它对比特率和调制方式透明，可以大大提高交换单元的吞吐量，因此，光交换必将成为高速网络交换技术的中坚力量。光交换技术费用不受接入端口带宽的影响，因为它在进行光交换时并不区分带宽，而且不受光波传输数据速率的影响，因此在传统的交换技术费用随带宽增加而大幅提高的情况下，光交换更具吸引力。随着光技术的进一步发展，光交换一定会在交换领域占据越来越重要的地位。

3.5.5 交换技术的比较

图3-32描述了几种交换技术的工作时序，从图中可以看出这几种交换方法在时间关系上的特点。

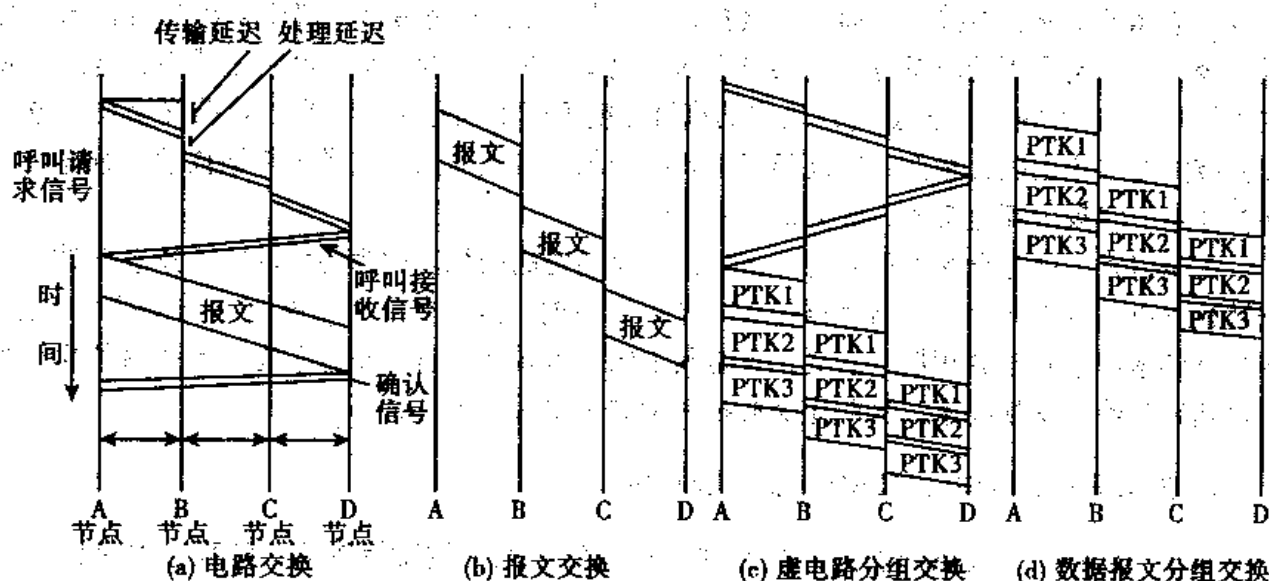


图3-32 几种交换方法的时序图

不同的交换技术适用于不同的场合：对于交互式通信来说，报文交换肯定是不适合的；对于较轻和间歇式负载来说，电路交换是最合适的，可以通过电话拨号线路来实行通信；对于较重和持续的负载来说，使用租用的线路以电路交换方式实行通信是合适的；对于必须交换中等到大量数据的情况，可用分组交换方法。

下面再简单小结一下三种交换技术的主要特点：

(1) 电路交换。在数据传送开始之前必须先设置一条专用的通路。在线路释放之前，该通路由一对用户完全占用。对于猝发式的通信，电路交换效率不高。

(2) 报文交换。报文从源点传送到目的地采用“存储—转发”的方式，在传送报文时，一个时刻仅占用一段通道。在交换节点中需要缓冲存储，报文需要排队，故报文交换不能满足实时通信的要求。

(3) 分组交换。交换方式和报文交换方式类似，但报文被分成分组传送，并规定了最大的分组长度。在数据报分组交换中，目的地需要重新组装报文；在虚电路分组交换中，数据传送之前必须通过虚呼叫设置一条虚电路。分组交换技术是计算机网络中使用最广泛的一种交换技术。

表3-3总结了电路交换和分组交换的一些区别。

表 3-3

电路交换和分组交换的比较

项 目	电路交换	分组交换
建立呼叫连接	要求	不要求
专门的物理路径	是	否
每个分组沿着同样的路由路径	是	否
电文或分组按序到达	是	否
一台交换机崩溃是否有严重影响	是	否
可用带宽	固定	动态
可能拥塞的时间点	建立呼叫连接的时候	每个分组传送的时候
可能有浪费的带宽	是	否
存储—转发传输机制	否	是
透明性	是	否
收费	每分钟	每个分组

公用数据网较多采用分组交换技术,例如我国的 CNPAC,美国的 TELENET,以及很多国家建立的公用数据网都属于这一类型。目前广泛采用的 X.25 协议就是由 ITU 制定的分组交换协议。

习 题

1. 物理层协议包括哪些内容?
2. 比较 RS-232C 与 RS-449 的电气特性。
3. 请说明和比较双绞线、同轴电缆与光纤 3 种常用传输介质的特点。
4. 控制字符 SYN 的 ASCII 码编码为 0010110,请画出 SYN 的 FSK、NRZ、曼彻斯特编码与差分曼彻斯特编码等四种编码方法的信号波形。
5. 对于脉冲编码调制 PCM 来说,如果要对频率为 600Hz 的某种语音信号进行采样,传送 PCM 信号的信道带宽为 3KHz,那么采样频率 f 取什么值时,采样的样本就可以包含足够重构原语音信号的所有信息。
6. 请说明调制解调器的基本工作原理。
7. 多路复用技术有哪几种?它们各有什么特点?
8. 广域网采用的数据交换技术有哪几种?它们各有什么特点?
9. 考虑一条长度为 50km 的点到点链路,对一个 100 字节的分组,带宽为多大时其传播延迟(速度为 $2 \times 10^8 \text{ m/s}$)等于发送延迟?对于 512 字节的分组,情况又如何?
10. 计算下列情况的时延(从第一个比特发送到最后一个比特接收):
 - (a) 1 Gbps 以太网,其路径上有一个存储转发交换机,分组长度为 5000 比特。假定每条链路的传播延迟为 $10 \mu\text{s}$,并且交换机在接收完分组后立即开始转发该分组。
 - (b) 同 (a),但是要经过三个交换机。
 - (c) 同 (b),但是,假定交换机实现“直通式”转发:就是在收到分组的头(128 比特)后立即开始转发该分组。
11. 假设在地球和一个火星探测器之间架设了一条 128Kbps 的点到点链路。从火星到地球的距离(当

它们离得最近时) 大约是 55gm, 而且数据在链路上以光速传播, 即 $3 \times 10^8 \text{ m/s}$ 。

(a) 计算链路上的传播延迟。

(b) 探测车上的一部照相机拍摄周围的照片, 并发送回地球。计算从拍完一幅图像到这幅图像到达地球上的控制中心所用的时间。假设每幅图像的大小为 5MB。

12. 下列情况下, 假定不对数据进行压缩, 对于 (a) ~ (d), 计算实时传输所需要的带宽:

(a) HDTV 高清晰度视频, 分辨率为 1920×1080 , 24 位/像素, 30 帧/秒。

(b) 8 比特 POTS (普通的电话服务) 语音频率, 采样频率为 8 KHz。

(c) 260 比特 GSM 移动语音音频, 采样频率为 50Hz。

(d) 24 比特 HDCD 高保真音频, 采样频率为 88.2 KHz。

第4章 数据链路层

本章将介绍数据链路层的功能、差错控制、基本数据链路协议、协议描述与验证、链路控制规程以及因特网的数据链路层协议。

数据链路层是 OSI 参考模型中的第二层，介乎于物理层和网络层之间，它在物理层提供服务的基础上向网络层提供服务。数据链路层的作用是对物理层传输原始比特流的功能的加强，将物理层提供的可能出错的物理连接改造成为逻辑上无差错的数据链路，即使之对网络层表现为一条无差错的链路。数据链路层的基本功能是向网络层提供透明的和可靠的数据传送服务。透明性是指该层上传输的数据的内容、格式及编码没有限制，也没有必要解释信息结构的意义；可靠的传输使用户免去对丢失信息、干扰信息及顺序不正确等的担心。

4.1 数据链路层的功能

数据链路层最基本的服务是将源机网络层来的数据可靠地传输到相邻节点的目标机网络层。为达到这一目的，数据链路层必须具备一系列相应的功能，它们主要有：如何将数据组合成数据块，在数据链路层中将这种数据块称为帧（Frame），帧是数据链路层的传送单位；如何控制帧在物理信道上的传输，包括如何处理传输差错，如何调节发送速率以使之与接收方相匹配；在两个网络实体之间提供数据链路通路的建立、维持和释放管理。

4.1.1 帧同步功能

为了使传输中发生差错后只将出错的有限数据进行重发，数据链路层将比特流组织成以帧为单位传送。帧的组织结构必须设计成使接收方能够明确地从物理层收到的比特流中对其进行识别，也即能从比特流中区分出帧的起始与终止，这就是帧同步要解决的问题。由于网络传输中很难保证计时的正确和一致，所以不能采用依靠时间间隔关系来确定一帧的起始与终止的方法。下面介绍几种常用的帧同步方法。

1. 使用字符填充的首尾定界符法

该法用一些特定的字符来定界一帧的起始与终止，本节稍后要介绍的 BSC 规程便是典型例子。为了不使数据信息位中出现的与特定字符相同的字符被误判为帧的首尾定界符，可以在这种数据字符前填充一个转义控制字符（DLE）以示区别，从而达到数据的透明性。但这种方法使用起来比较麻烦，而且所用的特定字符依赖于所采用的字符编码集，兼容性比较差。

2. 使用比特填充的首尾标志法

该法以一组特定的比特模式（如 01111110）来标志一帧的起始与终止。本节稍后要详细介绍的 HDLC 规程即采用该法。为了不使信息位中出现的与该特定比特模式相似的比特串被误判为帧的首尾标志，可以采用比特填充的方法。比如，采用特定模式 01111110，则对信息位中的任何连续出现的五个“1”，发送方自动在其后插入一个“0”，而接收方则做该过程的逆操作，即每接收到连续五个“1”，则自动删去其后所跟的“0”，以此恢复原始信息，实现数据传输的透明性。比特填充很容易由硬件来实现，性能优于字符填充方法。

3. 违法编码法

该法在物理层采用特定的比特编码方法时采用。例如，曼彻斯特编码方法，是将数据比特“1”编码成“高—低”电平对，将数据比特“0”编码成“低—高”电平对。而“高—高”电平对和“低—低”电平对在数据比特中是违法的。可以借用这些违法编码序列来定义帧的起始与终止。局域网 IEEE 802 标准中就采用了这种方法。违法编码法不需要任何填充技术，便能实现数据的透明性，但它只适用于采用冗余编码的特殊编码环境。

4. 字节计数法

这种帧同步方法以一个特殊字符表征一帧的起始，并以一个专门字段来标明帧内的字节数。接收方可以通过对该特殊字符的识别从比特流中区分出帧的起始，并从专门字段中获知该帧中随后跟随的数据字节数，从而可确定出帧的终止位置。

面向字节计数的同步规程的典型实例是数字数据通信报文协议 DDCMP (Digital Data Communication Message Protocol)。DDCMP 采用的帧格式如下：

8	14	2	8	8	8	16	8 ~ 131064	16	(位)
SOH	Count	Flag	Ack	Seg	Addr	CRC ₁	Data	CRC ₂	

格式中控制字符 SOH 标志数据帧的起始。Count 字段共有 14 位，用以指示帧中数据段中数据的字节数，数据段最大长度为 $8 \times (2^{14} - 1) = 131064$ (位)，长度必须为字节（即 8 位）的整倍数，DDCMP 协议就是靠这个字节计数来确定帧的终止位置的。DDCMP 帧格式中的 Ack、Seg、Addr 及 Flag 中的第 2 位，它们的功能分别类似于本节稍后要详细介绍的 HDLC 中的 N(R)、N(S)、Addr 字段及 P/F 位。CRC₁、CRC₂ 分别对标题部分和数据部分进行双重校验，强调标题部分单独校验的原因是，一旦标题部分中的 Count 字段出错，即失去了帧边界划分的依据，将造成灾难性的后果。由于采用字符计数方法来确定帧的终止边界不会引起数据及其它信息的混淆，因而不必采用任何措施便可实现数据的透明性，即任何数据均可不受限制地传输。

由于字节计数法中 Count 字段的脆弱性（其值若有差错将导致灾难性后果）以及字符填充法实现上的复杂性和不兼容性，目前较普遍使用的帧同步法是比特填充法和违法编码法。

4.1.2 差错控制功能

通信系统必须具备发现（即检测）差错的能力，并采取措施纠正之，使差错控制在所允许的尽可能小的范围内，这就是差错控制过程，也是数据链路层的主要功能之一。

接收方通过对差错编码（如奇偶校验码或 CRC 码）的检查，可以判定一帧在传输过程中是否发生了差错。一旦发现差错，一般可以采用反馈重发的方法来纠正。这就要求接收方收完一帧后，向发送方反馈一个接收是否正确信息，使发送方据此做出是否需要重新发送的决定。发送方仅当收到接收方已正确接收的反馈信号后才能认为该帧已经正确发送完毕，否则需重发直至正确为止。

物理信道的突发噪声可能完全“淹没”一帧，即使得整个数据帧或反馈信息帧丢失，这将导致发送方永远收不到接收方发来的反馈信息，从而使传输过程停滞。为了避免出现这种情况，通常引入计时器（Timer）来限定接收方发回反馈信息的时间间隔，当发送方发送一帧的同时也启动计时器，若在限定时间间隔内未能收到接收方的反馈信息，即计时器超时（Timeout），则可认为传出的帧已出错或丢失，就要重新发送。

由于同一帧数据可能被重复发送多次，就可能引起接收方多次收到同一帧并将其递交给网络层的危险。为了防止发生这种危险，可以采用对发送的帧编号的方法，即赋予每帧一个序号，从而使接收方能从该序号来区分是新发送来的帧还是已经接收但又重新发送来的帧，以此来确定要不要将接收到的帧递交给网络层。数据链路层通过使用计数器和序号来保证每帧最终都能被正确地递交给目标网络层一次。

有关差错控制的详细内容，将在本节稍后再作介绍。

4.1.3 流量控制功能

首先需要说明一下，流量控制并不是数据链路层特有的功能，许多高层协议中也提供流量控制功能，只不过流量控制的对象不同而已。比如，对于数据链路层来说，控制的是相邻两节点之间数据链路上的流量，而对于传输层来说，控制的则是从源到最终目的之间端对端的流量。

由于收发双方各自使用的设备工作速率和缓冲存储空间的差异，可能出现发送方发送能力大于接收方接收能力的现象，若此时不对发送方的发送速率（也即链路上的信息流量）作适当的限制，前面来不及接收的帧将被后面不断发送来的帧“淹没”，从而造成帧的丢失而出错。由此可见，流量控制实际上是对发送方数据流量的控制，使其发送速率不致超过接收方所能承受的能力。这个过程需要通过某种反馈机制使发送方知道接收方是否能跟得上发送方的速率。也即需要有一些规则使得发送方知道在什么情况下可以接着发送下一帧，而在什么情况下必须暂停发送，以等待收到某种反馈信息后再继续发送。

下面介绍两种最常用的流量控制方案：停止等待方案和滑动窗口机制。

1. 停止等待方案

增加缓冲存储空间在某种程度上可以缓解收、发双方在传输速率上的差异，但这是一种

被动、消极的方法。因为，一方面系统不允许开设过大的缓冲空间，另一方面对于速率显著失配并且又传送大量数据的场合，仍会出现缓冲存储空间不够的现象。停止等待流量控制方案则是一种相比之下更主动、更积极的流量控制方法。其工作原理是：发送方发出一帧，玉后等待应答信号到达后再发送下一帧；接收方每收到一帧后送回一个应答信号，表示愿意接收下一帧，如果接收方不送回应答，则发送方必须一直等待。

2. 滑动窗口机制

为了提高信道的有效利用率，如前所述采用了发送方不等待确认帧返回就连续发送若干帧的方案。由于允许连续发送多个未被确认的帧，帧号就须采用多位二进制数才能加以区分。因为凡被发送出去但尚未被确认的帧都可能出错或丢失而要求重发，因而这些帧都要保留下来。这就要求发送方有较大的发送缓冲区保留可能要求重发的未被确认的帧。

但是缓冲区容量总是有限的，如果接收方不能以发送方的发送速率处理接收到的帧，则还是可能用完缓冲容量而暂时过载。为此，在收到一确定帧之前，对发送方可发送的帧的数目加以限制。这是由发送方调整保留在重发表中的待确认帧的数目来实现的。如果接收方来不及对收到的帧进行处理，则接收方便停发确认信息，此时发送方的重发表就会增长，当达到重发表限度时，发送方就不再发送新帧，直至再次收到确认信息为止。

为了实现此方案，发送方存放待确认帧的重发表中，应设置待确认帧数目的最大限度，这一限度被称为链路的发送窗口。显然，如果窗口设置为1，即发送方缓冲能力仅为一个帧，此时传输效率很低。故窗口限度应选为使接收方尽量能处理或接受收到的所有帧。当然选择时还必须考虑诸如帧的最大长度、可使用的缓冲存储空间以及传输速率等因素。

重发表是一个连续序号的列表，对应发送方已发送但尚未确认的那些帧。这些帧的序号有一个最大值，这个最大值即发送窗口的限度。所谓发送窗口就是指示发送方已发送但尚未确认的帧序号队列的界，其上、下界分别称为发送窗口的上、下沿，上、下沿的间距称为窗口尺寸。接收方类似地也有接收窗口，它指示允许接收的帧的序号。

发送方每次发送一帧后，待确认帧的数目便增1，每收到一个确认信息后，待确认帧的数目便减1。“窗口”随着数据传送过程的发展而向前滑动，因而称为滑动窗口流量控制。当重发表长度计数值，即待确认帧的数目等于发送窗口尺寸时，便停止发送新的帧。

4.1.4 链路管理功能

链路管理功能主要用于面向连接的服务。在链路两端的节点要进行通信前，必须首先确认对方已处于就绪状态，并交换一些必要的信息以对帧序号初始化，然后才能建立连接。在传输过程中则要维持该连接。如果出现差错，需要重新初始化，重新自动建立连接。传输完毕后则要释放连接。数据链路层连接的建立、维持和释放就称作链路管理。

在多个站点共享同一物理信道的情况下（例如在局域网中），如何在要求通信的站点间分配和管理信道也属于数据链路层链路管理的范畴。

4.2 差错控制

4.2.1 差错检测

差错控制是指在数据通信过程中能发现或纠正差错，把差错限制在尽可能小的允许范围内的技术和方法。

信号在物理信道中传输时，线路本身电气特性造成的随机噪声、信号幅度的衰减、频率和相位的畸变、电气信号在线路上产生反射造成的回音效应、相邻线路间的串扰以及各种外界因素（如大气中的闪电、开关的跳火、外界强电流磁场的变化、电源的波动等）都会造成信号的失真。在数据通信中，将会使接收端收到的二进制数位和发送端实际发送的二进制数位不一致，从而造成由“0”变成“1”或由“1”变成“0”的差错。

一般来说，传输中的差错都是由噪声引起的。噪声有两大类：一类是信道固有的、持续存在的随机热噪声；另一类是由外界特定的短暂原因所造成的冲击噪声。

热噪声引起的差错称为随机错，所引起的某位码元的差错是孤立的，与前后码元没有关系。由于物理信道在设计时，总要保证达到相当大的信噪比，以尽可能减少热噪声的影响，因而由它导致的随机错通常较少。

冲击噪声呈突发状，由其引起的差错称为突发错。冲击噪声幅度可能相当大，无法靠提高信号幅度来避免冲击噪声造成的差错，它是传输中产生差错的主要原因。冲击噪声虽然持续时间很短，但在一定的数据速率条件下，仍然会影响到一串码元。例如，一个冲击噪声（如一次电火花）持续时间为10毫秒，但对于4800bps的数据速率来说，就可能对连续48位数据造成影响，使它们发生差错。从突发错误发生的第一个码元到有错的最后一个码元间所有码元的个数，称为该突发错的突发长度。

数据通信中不加任何差错控制措施，直接用信道来传输数据是不可靠的。而且，无线通信正在普及，它的错误率比光纤干线要高出几个数量级，因而必须要知道如何处理传输错误。差错控制的首要任务就是如何进行差错检测。差错检测应包含两个任务：即差错控制编码和差错校验。数据信息位在向信道发送之前，先按照某种关系附加上一定的冗余位，构成一个码字后再发送，这个过程称为差错控制编码过程。接收端收到该码字后，检查信息位和附加的冗余位之间的关系，以检查传输过程中是否有差错发生，这个过程称为差错校验过程。

4.2.2 差错控制方法

利用差错控制编码来进行差错控制的方法基本上有两类：一类是自动请求重发 ARQ (Automatic Repeat reQuest)，另一类是前向纠错 FEC (Forward Error Correction)。在 ARQ 方式中，接收端检测出有差错时，就设法通知发送端重发，直到正确的码字收到为止。在 FEC 方式中，接收端不但能发现差错，而且能确定二进制码元发生错误的位置，从而加以纠正。因此，差错控制编码又可分为检错码和纠错码。检错码是指能自动发现差错的编码，纠错码

是指不仅能发现差错而且能自动纠正差错的编码。

ARQ 方式只使用检错码,但必须有双向信道才可能将差错信息反馈至发送端。同时,发送方要设置数据缓冲区,用以存放已发出去的数据,以便知道出差错后可以调出数据缓冲区的内容重新发送。FEC 方式必须用纠错码,但它可以不需要反向信道来传递请求重发的信息,发送端也不需要存放以备重发的数据缓冲区。虽然 FEC 有上述优点,但由于纠错码一般说来要比检错码使用更多的冗余位,也就是说编码效率低,而且纠错设备也比检错设备复杂得多,因而除非在单向传输或实时要求特别高(FEC 由于不需要重发,实时性较好)等场合外,数据通信中使用更多的还是 ARQ 差错控制方式。有些场合也可以将上述两者混合使用,即当码字中的差错个数在纠正能力以内时,直接进行纠正;当码字中的差错个数超出纠正能力时,则检出差错,使用重发方式来纠正差错。

衡量编码性能好坏的一个重要参数是编码效率 R ,它是码字中信息位所占的比例。若码字中信息位为 k 位,编码时外加冗余位为 r 位,则编码后得到的码字长度为 $n = k + r$ 位,由此编码效率 R 可表示为:

$$R = k/n = k/(k + r)$$

显然,编码效率越高,即 R 越大,信道中用来传送信息码元的有效利用率就越高。

奇偶校验码、循环冗余码和海明码是几种最常用的差错控制编码方法。

4.2.3 奇偶校验码和循环冗余码

1. 奇偶校验码

奇偶校验码是一种通过增加冗余位使得码字中“1”的个数恒为奇数或偶数的编码方法,它是一种检错码。在实际使用时又可分为垂直奇偶校验、水平奇偶校验和水平垂直奇偶校验等几种。

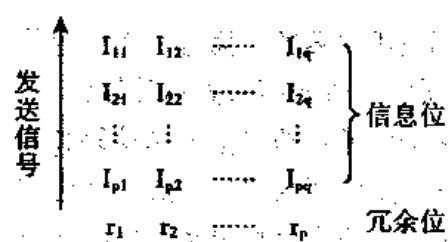


图 4-1 垂直奇偶校验

(1) 垂直奇偶校验。垂直奇偶校验又称为纵向奇偶校验,它是将要发送的整个信息块分为定长 p 位的若干段(比如说 q 段),每段后面按“1”的个数为奇数或偶数的规律加上一位奇偶位(如图 4-1 所示)。 pq 位信息 ($I_{11}, I_{21}, \dots, I_{p1}, I_{12}, \dots, I_{pq}$) 中,每 p 位构成一段(即图中的一列),共有 q 段(即共有 q 列)。每段加上一位奇偶校验冗余位,即图中的 r_i 。编码规则为

偶校验: $r_i = I_{1i} + I_{2i} + \dots + I_{pi} \quad (i = 1, 2, \dots, q)$

奇校验: $r_i = I_{1i} + I_{2i} + \dots + I_{pi} + 1 \quad (i = 1, 2, \dots, q)$

注意:此间的“+”指的是模二加,也即异或运算。

图中箭头给出了串行发送的顺序,即逐位先后次序为 $I_{11}, I_{21}, \dots, I_{p1}, r_1, I_{12}, \dots, I_{p2}, r_2, \dots, I_{1q}, \dots, I_{pq}, r_q$ 。在编码和校验过程中,用硬件方法或软件方法很容易实现上述连续半加运算,而且可以边发送边产生冗余位;同样,在接收端也可边接收边进行校验后去掉校验位。

垂直奇偶校验方法的编码效率为 $R = p/(p+1)$ 。通常, 取一个字符的代码为一个信息段, 这种垂直奇偶校验有时也称为字符奇偶校验。例如, 在 8 位字符代码 (即用 8 位二进制数位表示一个字符) 中, $p=8$, 编码效率便为 $8/9$ 。

垂直奇偶校验方法能检测出每列中的所有奇数位错, 但检测不出偶数位的错。对于突发错误来说, 奇数位错与偶数位错的发生概率接近于相等, 因而对差错的漏检率接近于 $1/2$ 。



图 4-2 水平奇偶校验

(2) 水平奇偶校验。为了降低对突发错误的漏检率, 可以采用水平奇偶校验方法。水平奇偶校验又称为横向奇偶校验, 它是对各个信息段的相应位横向进行编码, 产生一个奇偶校验冗余位 (如图 4-2 所示), 编码规则为

偶校验: $r_i = I_{i1} + I_{i2} + \dots + I_{iq} \quad (i = 1, 2, \dots, p)$

奇校验: $r_i = I_{i1} + I_{i2} + \dots + I_{iq} + 1 \quad (i = 1, 2, \dots, p)$

若每个信息段就是一个字符的话, 这里的 q 就是发送的信息块中的字符数。

水平奇偶校验的编码效率为 $R = q/(q+1)$ 。

水平奇偶校验不但可以检测出各段同一位上的奇数位错, 而且还能检测出突发长度 $\leq p$ 的所有突发错误。因为按发送顺序从图 4-2 中可见, 突发长度 $\leq p$ 的突发错误必然分布在不同的行中, 且每行一位, 所以可以检出差错, 它的漏检率要比垂直奇偶校验方法低。但是实现水平奇偶校验时, 不论采用硬件方法还是软件方法, 都不能在发送过程中边产生奇偶校验冗余位边插入发送, 而必须等待要发送的全部信息块到齐后, 才能计算冗余位, 也就是一定要使用数据缓冲器, 因此它的编码和检测实现起来都要复杂一些。

(3) 水平垂直奇偶校验。同时进行水平奇偶校验和垂直奇偶校验就构成水平垂直奇偶校验, 也称为纵横奇偶校验 (如图 4-3 所示)。若水平垂直都采用偶校验, 则



图 4-3 水平垂直奇偶校验

$$r_{i,q+1} = I_{i1} + I_{i2} + \dots + I_{iq} \quad (i = 1, 2, \dots, p)$$

$$r_{p+1,j} = I_{1j} + I_{2j} + \dots + I_{pj} \quad (j = 1, 2, \dots, q)$$

$$\begin{aligned} r_{p+1,q+1} &= r_{p+1,1} + r_{p+1,2} + \dots + r_{p+1,q} \\ &= r_{1,q+1} + r_{2,q+1} + \dots + r_{p,q+1} \end{aligned}$$

水平垂直奇偶校验的编码效率为 $R = pq/[(p+1)(q+1)]$ 。

水平垂直奇偶校验能检测出所有 3 位或 3 位以下的错误 (因为此时至少在某一列或某一行上有一位错)、奇数位错、突发长度 $\leq p+1$ 的突发错以及很大一部分偶数位错。测量表明, 这种方式的编码可使误码率降至原误码率的百分之一到万分之一。

水平垂直奇偶校验不仅可检错, 还可用来纠正部分差错。例如数据块中仅存在 1 位错时, 便能确定错码的位置就在某行和某列的交叉处, 从而可以纠正它。

2. 循环冗余码

奇偶校验码作为一种检错码虽然简单, 但是漏检率太高。在计算机网络和数据通信中用

得最广泛的检错码，是一种漏检率低得多也便于实现的循环冗余码 CRC (Cyclic Redundancy Code)，CRC 码又称为多项式码。

任何一个由二进制数位串组成的代码，都可以惟一地与一个只含有 0 和 1 两个系数的多项式建立一一对应的关系。例如，代码 1010111 对应的多项式为 $X^6 + X^4 + X^2 + X + 1$ ，同样多项式 $X^3 + X^2 + X + 1$ 对应的代码为 10111。

CRC 码在发送端编码和接收端校验时，都可以利用事先约定的生成多项式 $G(X)$ 来得到。 k 位要发送的信息位可对应于一个 $(k-1)$ 次多项式 $K(X)$ ， r 位冗余位则对应于一个 $(r-1)$ 次多项式 $R(X)$ ，由 k 位信息位后面加上 r 位冗余位组成的 $n = k+r$ 位码字则对应于一个 $(n-1)$ 次多项式 $T(X) = X^r \cdot K(X) + R(X)$ 。例如

信息位：1011001 $\rightarrow K(X) = X^6 + X^4 + X^3 + 1$

冗余位：1010 $\rightarrow R(X) = X^3 + X$

码字：10110011010 $\rightarrow T(X) = X^4 \cdot K(X) + R(X)$
 $= X^{10} + X^8 + X^7 + X^4 + X^3 + X$

由信息位产生冗余位的编码过程，就是已知 $K(X)$ 求 $R(X)$ 的过程。在 CRC 码中可以通过找到一个特定的 r 次多项式 $G(X)$ （其最高项 X^r 的系数恒为 1），然后用 $X^r \cdot K(X)$ 去除以 $G(X)$ ，得到的余式就是 $R(X)$ 。特别要强调的是，这些多项式中的“+”都是模 2 加（也即异或运算）；此外，这里的除法用的也是模 2 除法，即除法过程中用到的减法是模 2 减法，它和模 2 加法的运算规则一样，都是异或运算，这是一种不考虑加法进位和减法借位的运算，即

$0+0=0, 0+1=1, 1+0=1, 1+1=0$
 $0-0=0, 0-1=1, 1-0=1, 1-1=0$

在进行基于模 2 运算的多项式除法时，只要部分余数首位为 1，便可上商 1，否则上商 0。然后按模 2 减法求得余数，该余数不计最高位。当被除数逐位除完时，最后得到比除数少一位的余数。此余数即为冗余位，将其添加在信息位后便构成 CRC 码字。

仍以上例中 $K(X) = X^6 + X^4 + X^3 + 1$ 为例（即信息位为 1011001），若 $G(X) = X^4 + X^3 + 1$ （对应代码 11001），取 $r = 4$ ，则 $X^4 \cdot K(X) = X^{10} + X^8 + X^7 + X^4$ （对应代码为 10110010000），其由模 2 除法求余式 $R(X)$ 的过程所示如下：

```

      1 1 0 1 0 1 0
1 1 0 0 1 ) 1 0 1 1 0 0 1 0 0 0 0
            1 1 0 0 1
            1 1 1 1 0
            1 1 0 0 1
            1 1 1 1 0
            1 1 0 0 1
            1 1 1 0 0
            1 1 0 0 1
            1 1 1 0 0
            1 1 0 0 1
            1 0 1 0
    
```

得到的最后余数为 1010，这就是冗余位，对应 $R(X) = X^3 + X$ 。

由于 $R(X)$ 是 $X^r \cdot K(X)$ 除以 $G(X)$ 的余式，那么下列关系式必然满足

$X^r \cdot K(X) = G(X)Q(X) + R(X)$

其中 $Q(X)$ 为商式。根据模 2 运算规则 $R(X) + R(X) = 0$ 的特点, 可将上式改记为

$$[X^r \cdot K(X) + R(X)] / G(X) = Q(X)$$

$$\text{即 } T(X) / G(X) = Q(X)$$

由此可见, 信道上发送的码字多项式 $T(X) = X^r \cdot K(X) + R(X)$, 若传输过程无错, 则接收方收到的码字也对应于此多项式, 也即接收到的码字多项式能被 $G(X)$ 整除。因而接收端的校验过程就是将接收到的码字多项式除以 $G(X)$ 的过程。若余式为零则认为传输无差错; 若余式不为零则传输有差错。

例如, 前述例子中若码字 10110011010 经传输后由于受噪声的干扰, 在接收端变成为 10110011100, 则求余式的除法如下:

$$\begin{array}{r}
 \overline{1101010} \\
 11001 \overline{) 10110011100} \\
 \underline{11001} \\
 11110 \\
 \underline{11001} \\
 11111 \\
 \underline{11001} \\
 11010 \\
 \underline{11001} \\
 0110
 \end{array}$$

求得的余式不为零, 相当于在码字上面半加上了差错模式 00000000110。差错模式对应的多项式记为 $E(X)$, 上例中 $E(X) = X^2 + X$ 。有差错时, 接收端收到的不再是 $T(X)$, 而是 $T(X)$ 与 $E(X)$ 之模 2 加, 即

$$[T(X) + E(X)] / G(X) = T(X) / G(X) + E(X) / G(X)$$

若 $E(X) / G(X) \neq 0$, 则这种差错就能检测出来; 若 $E(X) / G(X) = 0$, 那么由于接收到的码字多项式仍然可被 $G(X)$ 整除, 错误就检测不出来, 也即发生了漏检。

理论上可以证明循环冗余校验码的检错能力有以下特点:

- (1) 可检测出所有奇数位错。
- (2) 可检测出所有双比特的错。
- (3) 可检测出所有小于、等于校验位长度的突发错。

CRC 码是由 $X^r \cdot K(X)$ 除以某个选定的多项式后产生的, 所以该多项式称生成多项式。一般来说, 生成多项式位数越多校验能力越强。但并不是任何一个 $r + 1$ 位的二进制数都可以作生成多项式。目前广泛使用的生成多项式主要有以下四种:

- (1) $\text{CRC12} = X^{12} + X^{11} + X^3 + X^2 + 1$
- (2) $\text{CRC16} = X^{16} + X^{15} + X^2 + 1$ (IBM 公司)
- (3) $\text{CRC16} = X^{16} + X^{13} + X^5 + 1$ (ITU)
- (4) $\text{CRC32} = X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

4.3 基本数据链路协议

4.3.1 停等协议

差错控制方法中的自动重发请求法即 ARQ 法有几种实现方案, 空闲重发请求 (Idle RQ) 和连续重发请求 (Continuous RQ) 是最基本的两种方案。

空闲重发请求方案也称停等 (Stop and Wait) 法, 该方案规定发送方每发送一帧后就要停下来等待接收方的确认返回, 仅当接收方确认正确接收后再继续发送下一帧。停等协议的实现过程如下:

- (1) 发送方每次仅将当前信息帧作为待确认帧保留在缓冲存储器中;
- (2) 当发送方开始发送信息帧时, 赋予该信息帧一个帧序号, 随即启动计时器;
- (3) 当接收方收到无差错的信息帧后, 即向发送方返回一个与该帧序号相同序号的 ACK 确认帧;
- (4) 当接收方检测到一个含有差错的信息帧时, 便舍弃该帧;
- (5) 若发送方在规定时间内收到 ACK 确认帧, 即将计时器清零, 继而开始下一帧的发送;
- (6) 若发送方在规定时间内未收到 ACK 确认帧 (即计时器超时), 则应重发存于缓冲器中的待确认信息帧。

从以上过程可以看出, 停等协议的接收、发送双方仅需设置一个帧的缓冲存储空间和帧序号只取 0 或 1 的两个状态标志位, 便可有效地实现数据重发并确保接收方接收的数据不会重份。该方案最主要的优点就是所需的缓冲存储空间最小, 因此在链路端使用简单终端的环境中广泛采用。它的最大缺点是: 发送方要停下来等待 ACK 帧返回后再继续发送而造成的信道浪费。

4.3.2 顺序接收管道协议

连续重发请求方案就是指顺序接收管道协议。为了提高信道的有效利用率, 就要允许发送方可以连续发送一系列信息帧, 即不用等前一帧被确认便可发送下一帧。发送过程就像一条连续的流水线, 故称为管道 (Pipelining) 技术。凡是被发送出去尚未被确认的帧, 都可能出错或丢失而要求重发, 因而都要保留下来。这就需要在发送方设置一个较大的缓冲存储空间 (称作重发表), 用以存放若干待确认的信息帧。当发送方收到对某信息帧的确认帧后, 便可从重发表中将该信息帧删除。所以, 连续 RQ 方案的链路传输效率大大提高, 但相应地需要更大的缓冲存储空间。由于允许连续发出多个未被确认的帧, 帧号就不能仅采用一位 (只有 0 和 1 两种帧号), 而要采用多位帧号才能区分。该协议的实现过程如下:

- (1) 发送方连续发送信息帧而不必等待确认帧的返回;
- (2) 发送方在重发表中保存所发送的每个帧的备份;

- (3) 重发表按先进先出 (FIFO) 队列规则操作;
- (4) 接收方对每一个正确收到的信息帧返回一个确认帧;
- (5) 每一个确认帧包含一个惟一的序号, 随相应的确认帧返回;
- (6) 接收方保存一个接收次序表, 它包含最后正确收到的信息帧的序号;
- (7) 当发送方收到相应信息帧的确认帧后, 从重发表中删除该信息帧的备份;

(8) 接收方因某一帧出错, 则对后面再发送来的帧均不接收而丢弃。换句话说, 接收方只允许顺序接收。而发送方发现前面帧未收到确认信息, 计时器已超时, 不得不退回重发最后确认序号以后的帧。这种方法又称之为“回退 N”(Go-back-N) 策略的重发请求法。

Go-back-N 策略的基本原理是, 当接收方检测出失序的信息帧后, 要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧; 或者当发送方发送了 n 个帧后, 若发现该 n 帧的前一帧在计时器超时区间内仍未返回其确认信息, 则该帧被判定为出错或丢失, 此时发送方就不得不重新发送该出错帧及其后的 n 帧。这就是 Go-back-N (退回 N) 法名称的由来。因为, 对接收方来说, 由于这一帧出错, 就不能以正确的序号向它的高层递交数据, 对其后发送来的 n 帧也可能都不能接收而丢弃。Go-back-N 法操作过程如图 4-4 所示。图中假定发送完 8 号帧后, 发现 2 号帧的确认返回在计时器超时后还未收到, 则发送方只能退回从 2 号帧开始重发。

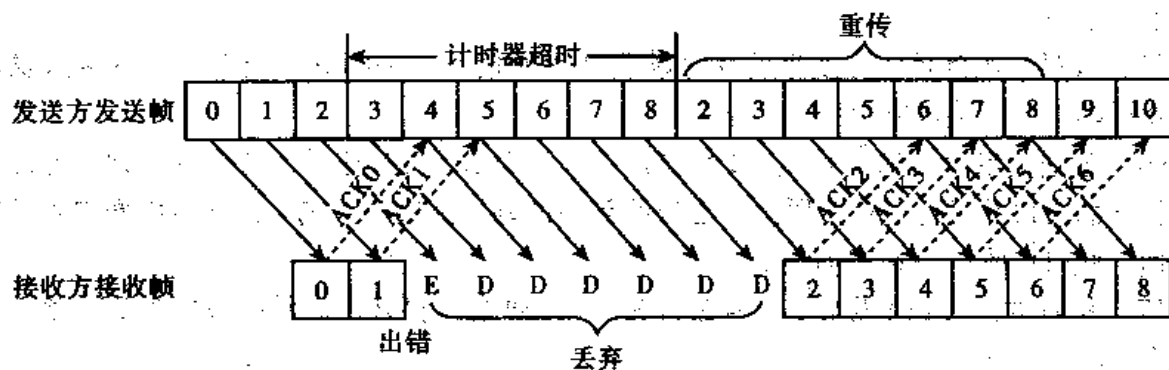


图 4-4 Go-back-N 法举例

为了提高信道的有效利用率, 如前所述采用了发送方不等待确认帧返回就连续发送若干帧的方案。显然, 允许已发送有待于确认的帧越多, 可能要退回来重发的帧也越多。另外, 为了控制发送方的发送速度, 并考虑到受发送缓冲区大小的制约因素, 要求对发送方已发出但尚未确认的帧的数目加以限制。此时可以采用基于窗口机制的流量控制方法来限制发送方已发出而未被确认的帧数目。发送方的发送窗口指示已发送但尚未确认的帧序号。接收方类似地也有接收窗口, 它指示允许接收的帧的序号。

一般帧序号只取有限位二进制数, 到一定时间后就反复循环。若帧号配 3 位二进制数, 则帧号在 0~7 间循环。如果发送窗口尺寸取值为 2, 则发送过程如图 4-5 所示。图中发送方阴影部分表示打开的发送窗口, 接收方阴影部分则表示打开的接收窗口。当传送过程进行时, 打开的窗口位置一直在滑动, 所以也称为滑动窗口 (Sliding Window), 或简称为滑窗。

图中的滑动窗口状态变化过程可叙述如下 (假设发送窗口尺寸为 2, 接收窗口尺寸为 1):

- (1) 初始态, 发送方没有帧发出, 发送窗口前后沿相重合。接收方 0 号窗口打开, 表示等待接收 0 号帧;

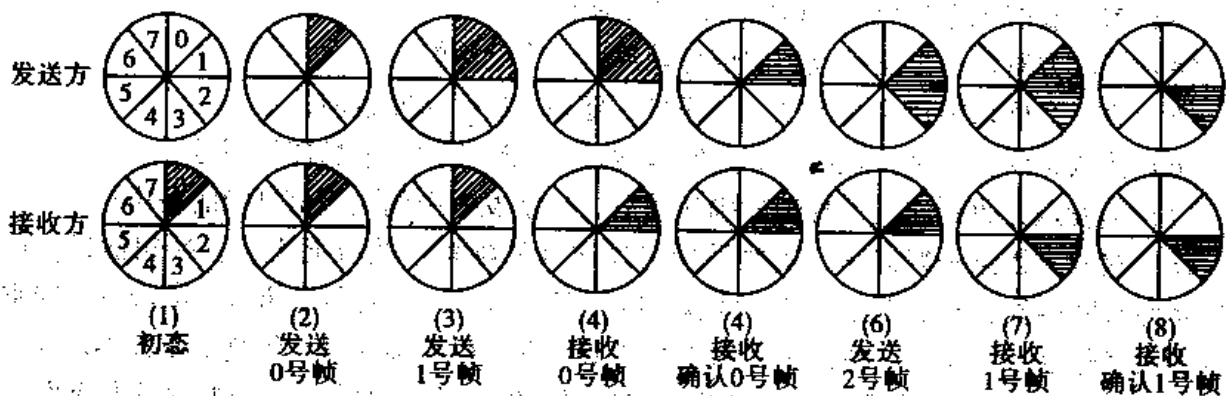


图 4-5 滑动窗口状态变化过程

(2) 发送方已发送 0 号帧，此时发送方打开 0 号窗口，表示已发出 0 号帧但尚未收到确认返回信息。此时接收窗口状态同前，仍等待接收 0 号帧；

(3) 发送方在未收到 0 号帧的确认返回信息前，继续发送 1 号帧。此时，1 号窗口打开，表示 1 号帧也属等待确认之列。至此，发送方打开的窗口数已达规定限度，在未收到新的确认返回帧之前，发送方将暂停发送新的数据帧。接收窗口此时状态仍未变；

(4) 接收方已收到 0 号帧，0 号窗口关闭，1 号窗口打开，表示准备接收 1 号帧。此时发送窗口状态不变；

(5) 发送方收到接收方发来的 0 号帧确认返回信息，关闭 0 号窗口，表示从重发表中删除 0 号帧。此时接收窗口状态仍不变；

(6) 发送方继续发送 2 号帧，2 号窗口打开，表示 2 号帧也纳入待确认之列。至此，发送方打开的窗口数又已达规定限度，在未收到新的确认返回帧之前，发送方将暂停发送新的数据帧。此时接收窗口状态仍不变；

(7) 接收方已收到 1 号帧，1 号窗口关闭，2 号窗口打开，表示准备接收 2 号帧。此时发送窗口状态不变；

(8) 发送方收到接收方发来的 1 号帧收毕的确认信息，关闭 1 号窗口，表示从重发表中删除 1 号帧。此时接收窗口状态仍不变。

停等协议可以看成是发送窗口、接收窗口等于 1；Go-back-N 是发送窗口大于 1、接收窗口等于 1 的一个特例。

4.3.3 选择重传协议

Go-back-N 可能将已正确传送到目的方的帧再重传一遍，这显然是一种浪费。另一种效率更高的策略是当接收方发现某帧出错后，其后继续送来的正确的帧虽然不能立即递交给接收方的高层，但接收方仍可收下来，存放在一个缓冲区中，同时要求发送方重新传送给出错的那一帧。一旦收到重新传来的帧后，就可与原已存于缓冲区中的其余帧一并按正确的顺序递交高层。这种方法称为选择重传 (Selective Repeat)，其工作过程如图 4-6 所示。图中 2 号帧的否认返回信息 NAK_2 要求发送方选择重发 2 号帧。发送方得此信息后不用等待计时器超时就可重新发送 2 号帧了。显然，选择重传协议在某帧出错时减少了后面所有帧都要重传的浪费，但要求接收方有足够大的缓冲区空间来暂存未按顺序正确接收到的帧。一般来说，凡

是在一定范围内到达的帧，即使它们不按顺序，接收方也要接收下来。若把这个范围看成是接收窗口的话，则接收窗口的大小也应该是大于1的。若帧序号采用3位二进制编码，则最大序号为 $S_{max} = 2^3 - 1 = 7$ 。对于有序接收方式，发送窗口最大尺寸选为 S_{max} ；对于无序接收方式，发送窗口最大尺寸至多是序号范围的一半。发送方管理超时控制的计时器数应等于缓冲器数，而不是序号空间的大小。

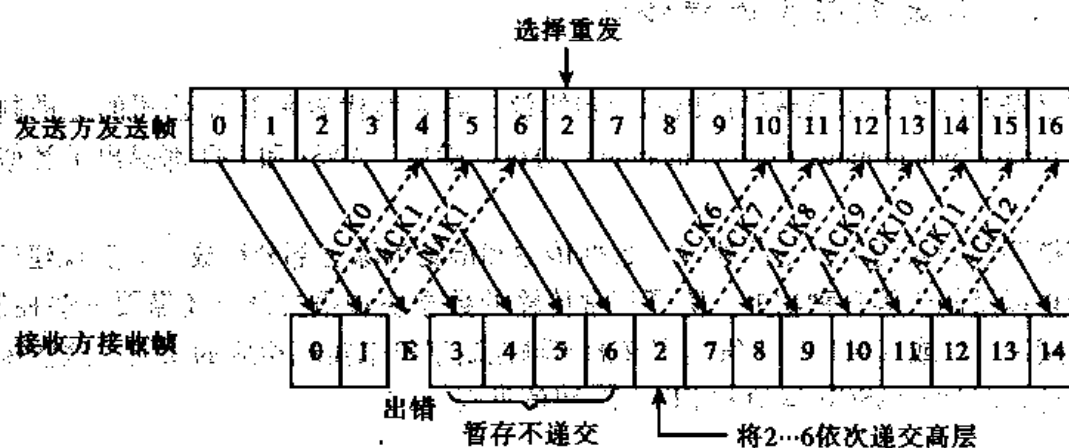


图4-6 选择重发法举例

选择重传协议也可以看成一种滑动窗口协议，只不过其发送窗口和接收窗口都大于1。若从滑动窗口的观点来统一看待停等、Go-back-N及选择重传三种协议，它们的差别仅在于各自窗口尺寸的大小不同而已：

停等：发送窗口 = 1，接收窗口 = 1；

Go-back-N：发送窗口 > 1，接收窗口 = 1；

选择重传：发送窗口 > 1，接收窗口 > 1。

4.4 链路控制规程

数据链路控制协议也称链路通信规程，也就是 OSI 参考模型中的数据链路层协议。链路控制协议可分为异步协议和同步协议两大类。

异步协议以字符为独立的信息传输单位，在每个字符的起始处开始对字符内的比特实现同步，但字符与字符之间的间隔时间是不固定的（即字符之间是异步的）。由于发送器和接收器中近似于同一频率的两个约定时钟，能够在一段较短的时间内保持同步，所以可以用字符起始处同步的时钟来采样该字符中的各比特，而不需要每个比特再用其它方法同步。前面介绍过的“起—止”式通信规程便是异步协议的典型，它是靠起始位（逻辑0）和停止位（逻辑1）来实现字符的定界及字符内比特的同步的。异步协议中由于每个传输字符都要添加诸如起始位、校验位、停止位等冗余位，故信道利用率很低，一般用于数据速率较低场合。

同步协议是以许多字符或许多比特组织成的数据块——帧为传输单位，在帧的起始处同步，使帧内维持固定的时钟。由于采用帧为传输单位，所以同步协议能更有效地利用信道，

也便于实现差错控制、流量控制等功能。

同步协议又可分为面向字符的同步协议、面向比特的同步协议及面向字节计数的同步协议三种类型。其中面向字节计数的同步协议在本节前面的帧同步功能中已作了较详细的介绍, 下面介绍另外两种同步协议。

4.4.1 二进制同步通信协议

面向字符的同步协议是最早提出的同步协议, 其典型代表是 IBM 公司的二进制同步通信 BSC (Binary Synchronous Communication) 协议。随后, ANSI 和 ISO 都提出了类似的相应标准。

任何链路层协议均可由链路建立、数据传输和链路拆除三部分组成。为实现建链、拆链等链路管理以及同步等各种功能, 除了正常传输的数据块和报文外, 还需要一些控制字符。BSC 协议用 ASCII 或 EBCDIC 字符集定义的传输控制字符来实现相应的功能。这些传输控制字符的标记、名称及 ASCII 码值和 EBCDIC 码值见表 4-1。

表 4-1

传输控制字符

标记	名称	ASCII 码值	EBCDIC 码值
SOH	序始	01H	01H
STX	文始	02H	02H
ETX	文终	03H	03H
EOT	送毕	04H	37H
ENQ	询问	05H	2DH
ACK	确认	06H	2EH
DLE	转义	10H	10H
NAK	否认	15H	3DH
SYN	同步	16H	32H
ETB	块终	17H	26H

各传输控制字符的功能如下:

SOH (Start of Head): 序始, 用于表示报文的标题信息或报头的开始。

STX (Start of Text): 文始, 标志标题信息的结束和报文文本的开始。

ETX (End of Text): 文终, 标志报文文本的结束。

EOT (End of Transmission): 送毕, 用以表示一个或多个文本块的结束, 并拆除链路。

ENQ (Enquire): 询问, 用以请求远程站给出响应, 响应可能包括站的身份或状态。

ACK (Acknowledge): 确认, 由接收方发出的作为对正确接收到报文的响应。

DLE (Data Link Escape): 转义, 用以修改紧跟其后的有限个字符的意义。在 BSC 中实现透明方式的数据传输, 或者当 10 个传输控制字符不够用时提供新的转义传输控制字符。

NAK (Negative Acknowledge): 否认, 由接收方发出的作为对未正确接收的报文的响应。

SYN (Synchronous): 同步字符, 在同步协议中, 用以实现节点之间的字符同步, 或用于在无数据传输时保持该同步。

ETB (End of Transmission Block): 块终或组终, 用以表示当报文分成多个数据块时, 一个数据块的结束。

BSC 协议将在链路上传输的信息分为数据报文和监控报文两类。监控报文又可分为正向监控和反向监控两种。每一种报文中至少包含一个传输控制字符, 用以确定报文中信息的性质或实现某种控制作用。

数据报文一般由报头和文本组成。文本是要传送的有效数据信息, 而报头是与文本传送及处理有关的辅助信息, 报头有时也可不用。对于不超过长度限制的报文可只用一个数据块发送, 对较长的报文则分作多块发送, 每一个数据块作为一个传输单位。接收方对于每一个收到的数据块都要给以确认, 发送方收到返回的确认后, 才能发送下一个数据块。

BSC 协议的数据块有如下四种格式:

(1) 不带报头的单块报文或分块传输中的最后一块报文:

SYN	SYN	STX	报文	ETX	BCC
-----	-----	-----	----	-----	-----

(2) 带报头的单块报文:

SYN	SYN	SOH	报头	STX	报文	ETX	BCC
-----	-----	-----	----	-----	----	-----	-----

(3) 分块传输中的第一块报文:

SYN	SYN	SOH	报头	STX	报文	ETB	BCC
-----	-----	-----	----	-----	----	-----	-----

(4) 分块传输中的中间报文:

SYN	SYN	STX	报文	ETB	BCC
-----	-----	-----	----	-----	-----

BSC 协议中所有发送的数据均跟在至少两个 SYN 字符之后, 以使接收方能实现字符同步。报头字段用以说明数据报文字段的包识别符 (序号) 及地址。所有数据块在块终限定符 (ETX 或 ETB) 之后还有块校验字符 BCC (Block Check Character), BCC 可以是垂直奇偶校验或 16 位 CRC, 校验范围从 STX 开始到 ETX 或 ETB 为止。

当发送的报文是二进制数据而不是字符串时, 二进制数据中形同传输控制字符的比特串将会引起传输混乱。为使二进制数据中允许出现与传输控制字符相同的数据 (即数据的透明性), 可在各帧中真正的传输控制字符 (SYN 除外) 前加上 DLE 转义字符, 在发送时, 若文本中也出现与 DLE 字符相同的二进制比特串, 则可插入一个外加的 DLE 字符加以标记。在接收端则进行同样的检测, 若发现单个的 DLE 字符, 则可知其后为传输控制字符; 若发现连续两个 DLE 字符, 则知其后的 DLE 为数据, 在进一步处理前将其中一个删去。

正、反向监控报文有如下四种格式:

(1) 肯定确认和选择响应:

SYN	SYN	ACK
-----	-----	-----

(2) 否定确认和选择响应:

SYN	SYN	NAK
-----	-----	-----

(3) 轮询/选择请求:

SYN	SYN	P/S 前缀	站地址	ENQ
-----	-----	--------	-----	-----

(4) 拆链:

SYN	SYN	EOT
-----	-----	-----

监控报文一般由单个传输控制字符或由若干个其它字符引导的单个传输控制字符组成。引导字符统称为前缀,它包含识别符(序号)、地址信息、状态信息以及其它所需的信息。ACK 和 NAK 监控报文的作用,首先是作为对先前所发数据块是否正确接收的响应,因而包含识别符(序号);其次,用作对选择监控信息的响应,以 ACK 表示所选站能接收数据块,而 NAK 表示不能接收。ENQ 用作轮询和选择监控报文,在多站结构中,轮询或选择的站地址在 ENQ 字符前。EOT 监控报文用以标志报文交换的结束,并在两站点间拆除逻辑链路。

由于 BSC 协议与特定的字符编码集关系过于密切,故兼容性较差。为满足数据透明性而采用的字符填充法,实现起来也比较麻烦,且也依赖于所采用的字符编码集。另外,由于 BSC 是一个半双工协议,它的链路传输效率很低。不过,由于 BSC 协议需要的缓冲存储空间较小,因而在面向终端的网络系统中仍然被广泛使用。

4.4.2 高级数据链路控制协议

这里以 ISO 的高级数据链路控制规程 HDLC (High-level Data Link Control) 协议为例,来讨论面向比特的同步控制协议的一般原理与操作过程。作为面向比特的数据链路控制协议的典型,HDLC 具有如下特点:协议不依赖于任何一种字符编码集;数据报文可透明传输,用于实现透明传输的“0 比特插入法”易于硬件实现;全双工通信,不必等待确认便可连续发送数据,有较高的数据链路传输效率;所有帧均采用 CRC 校验,对信息帧进行顺序编号,可防止漏收或重份,传输可靠性高;传输控制功能与处理功能分离,具有较大灵活性。由于以上特点,目前网络设计普遍使用 HDLC 作为数据链路控制协议。

1. HDLC 的操作方式

HDLC 是通用的数据链路控制协议,在开始建立数据链路时,允许选用特定的操作方式。所谓操作方式,通俗地讲就是某站点是以主站方式操作还是以从站方式操作,或者是二者兼备。

链路上用于控制目的的站称为主站,其它的受主站控制的站称为从站。主站负责对数据流进行组织,并且对链路上的差错实施恢复。由主站发往从站的帧称为命令帧,而由从站返回主站的帧称响应帧。连有多个站点的链路通常使用轮询技术,轮询其它站的站称为主站,

而在点对点链路中每个站均可为主站。主站需要比从站有更多的逻辑功能，所以当终端与主机相连时，主机一般总是主站。在一个站连接多条链路的情况下，该站对于一些链路而言可能是主站，而对另外一些链路而言又可能是从站。有些站可兼备主站和从站的功能，这种站称为组合站。用于组合站之间信息传输的协议是对称的，即在链路上主、从站具有同样的传输控制功能，这又被称作平衡操作。相对的，那种操作时有主站、从站之分的，且各自功能不同的操作，称为非平衡操作。

HDLC 中常用的操作方式有以下三种：

(1) 正常响应方式 NRM (Normal Responses Mode)。这是一种非平衡数据链路操作方式，有时也称非平衡正常响应方式。该操作方式适用于面向终端的点对点或一点与多点的链路。在这种操作方式中，传输过程由主站启动，从站只有收到主站某个命令帧后，才能作为响应向主站传输信息。响应信息可以由一个或多个帧组成，若信息由多个帧组成，则应指出哪一个是一帧。主站负责管理整个链路，且具有轮询、选择从站及向从站发送命令的权利，同时也负责对超时、重发及各类恢复操作的控制。

(2) 异步响应方式 ARM (Asynchronous Responses Mode)。这也是一种非平衡数据链路操作方式，与 NRM 不同的是，ARM 下的传输过程由从站启动。从站主动发送给主站的一个或一组帧中可包含有信息，也可以是仅以控制为目的而发的帧。在这种操作方式下，由从站来控制超时和重发。该方式对采用轮询方式的多站链路来说是必不可少的。

(3) 异步平衡方式 ABM (Asynchronous Balanced Mode)。这是一种允许任何节点来启动传输的操作方式。为了提高链路传输效率，节点之间在两个方向上都需要有较高的信息传输量。在这种操作方式下，任何时候任何站点都能启动传输操作，每个站点既可作为主站又可作为从站，即每个站都是组合站。各站都有相同的一组协议，任何站点都可以发送或接收命令，也可以给出应答，并且各站对差错恢复过程都负有相同的责任。

2. HDLC 的帧格式

在 HDLC 中，数据和控制报文均以帧的标准格式传送。HDLC 中的帧类似于 BSC 的字符块，但 BSC 协议中的数据报文和控制报文是独立传输的，而 HDLC 中的命令和响应以统一的格式按帧传输。完整的 HDLC 帧由标志字段 (F)、地址字段 (A)、控制字段 (C)、信息字段 (I)、帧校验序列字段 (FCS) 等组成，其格式如下：

标志	地址	控制	信息	帧校验序列	标志
F	A	C	I	FCS	F
01111110	8 位	8 位	N 位	16 位	01111110

图 4-7

(1) 标志字段 (F)：标志字段为 01111110 的比特模式，用以标志帧的起始和前一帧的终止。通常，在不进行帧传送的时刻，信道仍处于激活状态，标志字段也可以作为帧与帧之间的填充字符。在这种状态下，发送方不断地发送标志字段，而接收方则检测每一个收到的标志字段，一旦发现某个标志字段后面不再是一个标志字段，便可认为一个新的帧传送已经开始。采用“0 比特插入法”可以实现数据的透明传输，该法在发送端检测除标志码以外的所有字段，若发现连续 5 个“1”出现时，便在其后添插 1 个“0”，然后继续发送后面的比

特流，在接收端同样检测除标志码以外的所有字段，若发现连续5个“1”后是“0”，则将其删除以恢复比特流的原貌。

(2) 地址字段 (A)：地址字段的内容取决于所采用的操作方式。在操作方式中，有主站、从站、组合站之分，每一个从站和组合站都被分配一个惟一的地址。命令帧中的地址字段携带的是对方站的地址，而响应帧中的地址字段所携带的地址是本站的地址。某一地址也可分配给不止一个站，这种地址称为组地址，利用一个组地址传输的帧能被组内所有拥有该组地址的站接收，但当一个从站或组合站发送响应时，它仍应当用它惟一的地址。还可用全“1”地址来表示包含所有站的地址，这种地址称为广播地址，含有广播地址的帧传送给链路上所有的站。另外，还规定全“0”地址为无站地址，这种地址不分配给任何站，仅用作测试。

(3) 控制字段 (C)：控制字段用于构成各种命令和响应，以便对链路进行监视和控制。发送方主站或组合站利用控制字段来通知被寻址的从站或组合站执行约定的操作；相反，从站用该字段作为对命令的响应，报告已完成的操作或状态的变化。该字段是 HDLC 的关键，下面还将详细介绍。

(4) 信息字段 (I)：信息字段可以是任意的二进制比特串。比特串长度未作严格限定，其上限由 FCS 字段或站点的缓冲器容量来确定，目前用得较多的是 1000 ~ 2000 比特；而下限可以为 0，即无信息字段。但是，监控帧 (S 帧) 中规定不可有信息字段。

(5) 帧校验序列字段 (FCS)：帧校验序列字段可以使用 16 位 CRC，对两个标志字段之间的整个帧的内容进行校验。FCS 的生成多项式由 ITU V.41 建议规定为 $X^{16} + X^{12} + X^5 + 1$ 。

3. HDLC 的帧类型

HDLC 有信息帧 (I 帧)、监控帧 (S 帧) 和无编号帧 (U 帧) 三种不同类型的帧，各类帧中控制字段的格式及比特定义如下：

表 4-2

控制字段位	1	2	3	4	5	6	7	8
I 格式	0	N(S)			P	N(R)		
S 格式	1	0	S_1	S_2	P/F	N(R)		
U 格式	1	1	M_1	M_2	P/F	M_3	M_4	M_5

控制字段中的第 1 位或第 1、第 2 位表示传送帧的类型。第 5 位是 P/F 位，即轮询/终止 (Poll/Final) 位。当 P/F 位用于命令帧 (由主站发出) 时，起轮询的作用，即当该位为“1”时，要求被轮询的从站给出响应，所以此时 P/F 位可称轮询位 (或 P 位)；当 P/F 位用于响应帧 (由从站发出) 时，称为终止位 (或 F 位)，当其为“1”时，表示接收方确认的结束。为了进行连续传输，需要对帧进行编号，所以控制字段中还包括了帧的编号。

(1) 信息帧 (I 帧)：信息帧用于传送有效信息或数据，通常简称 I 帧。I 帧以控制字段第 1 位为“0”来标志。信息帧控制字段中的 N(S) 用于存放发送帧序号，以使发送方不必等待确认而连续发送多帧。N(R) 是一个捎带的确认，用于存放接收方下一个预期要接收

的帧的序号, 如 $N(R) = 5$, 即表示接收方下一帧要接收 5 号帧, 换言之, 5 号帧前的各帧接收方都已正确接收到。 $N(S)$ 和 $N(R)$ 均为 3 位二进制编码, 可取值 0~7。

(2) 监控帧 (S 帧): 监控帧用于差错控制和流量控制, 通常简称 S 帧。S 帧以控制字段第 1、2 位为 “10” 来标志。S 帧不带信息字段, 帧长只有 6 个字节即 48 个比特。S 帧的控制字段的第 3、4 位为 S 帧类型编码, 共有四种不同组合, 分别表示:

“00” — 接收就绪 (RR), 由主站或从站发送。主站可以使用 RR 型 S 帧来轮询从站, 即希望从站传输编号为 $N(R)$ 的 I 帧, 若存在这样的帧, 便进行传输; 从站也可用 RR 型 S 帧来作响应, 表示从站期望接收的下一帧的编号是 $N(R)$ 。

“01” — 拒绝 (REJ), 由主站或从站发送, 用以要求发送方对从编号为 $N(R)$ 开始的帧及其以后所有的帧进行重发, 这也暗示 $N(R)$ 以前的 I 帧已被正确接收。

“10” — 接收未就绪 (RNR), 表示编号小于 $N(R)$ 的 I 帧已被收到, 但目前正处于忙状态, 尚未准备好接收编号为 $N(R)$ 的 I 帧, 这可用来对链路流量进行控制。

“11” — 选择拒绝 (SREJ), 它要求发送方发送编号为 $N(R)$ 的单个 I 帧, 并暗示其它编号的 I 帧已全部确认。

可以看出, 接收就绪 RR 型 S 帧和接收未就绪 RNR 型 S 帧有两个主要功能: 首先, 这两种类型的 S 帧用来表示从站已准备好或未准备好接收信息; 其次, 确认编号小于 $N(R)$ 的所有接收到的 I 帧。拒绝 REJ 和选择拒绝 SREJ 型 S 帧, 用于向对方站指出发生了差错。REJ 帧对应 Go-back-N 策略, 用以请求重发 $N(R)$ 起始的所有帧, 而 $N(R)$ 以前的帧已被确认, 当收到一个 $N(S)$ 等于 REJ 型 S 帧的 $N(R)$ 的 I 帧后, REJ 状态即可清除。SREJ 帧对应选择重发策略, 当收到一个 $N(S)$ 等于 SREJ 帧的 $N(R)$ 的 I 帧时, SREJ 状态即应清除。

(3) 无编号帧 (U 帧): 无编号帧因其控制字段中不包含编号 $N(S)$ 和 $N(R)$ 而得名, 简称 U 帧。U 帧用于提供对链路的建立、拆除以及多种控制功能, 这些控制功能用 5 个 M 位 ($M_1 \sim M_5$, 也称修正位) 来定义, 可以定义 32 种附加的命令或应答功能。但并不是所有的 32 种可能都用到了。用到的命令例如 DISC (DISConnect) 表示要拆除连接。例如 FRMR (FraMe Reject) 表示帧拒绝。

4.5 因特网的数据链路层协议

在因特网上有两个被广泛使用的链路层协议, 它们是串行线路 IP 协议 (Serial Line IP, SLIP) 和点到点协议 (Point-to-Point Protocol, PPP)。

4.5.1 SLIP 协议

SLIP 提供在串行通信线路上封装 IP 分组的简单方法, 用以使远程用户通过电话线和 MODEM 能方便地接入 TCP/IP 网络。

SLIP 是一种简单的组帧方式, 使用时还存在一些问题。首先, SLIP 不支持在连接过程中的动态 IP 地址分配, 通信双方必须事先告知对方 IP 地址, 这给没有固定 IP 地址的个人用

户上 Internet 网带来了很大的不便；其次，SLIP 帧中无协议类型字段，因此它只能支持 IP 协议；再有，SLIP 帧中无校验字段，因此链路层上无法检测出传输差错，必须由上层实体或具有纠错能力的 MODEM 来解决传输差错问题。

4.5.2 PPP 协议

为了解决 SLIP 存在的问题，在串行通信应用中又开发了 PPP 点到点协议，RFC 1661 定义了该协议，PPP 具有处理错误检测、支持多个协议、允许在连接时刻协商 IP 地址、允许身份认证等功能，还有其它特性。PPP 提供了 3 类功能：

(1) 成帧：它可以毫无歧义地分割出一帧的起始和结束。其帧格式支持错误检测。

(2) 链路控制：有一个称为 LCP (Link Control Protocol) 的链路控制协议，支持同步和异步线路，也支持面向字节的和面向位的编码方法，可用于启动线路、测试线路、协商参数，以及关闭线路。

(3) 网络控制：具有协商网络层选项的方法，并且协商方法与使用的网络层协议独立。所选择的方法对于每一种支持的网络层都有一个不同的 NCP (Network Control Protocol) 网络控制协议。

一个家庭用户呼叫一个 Internet 服务供应商首先是 PC 机通过调制解调器呼叫供应商的路由器，当路由器的调制解调器回答了用户的呼叫，并建立起一个物理连接之后，PC 机给路由器发送一系列 LCP 分组，它们被包含在一个或多个 PPP 帧的净荷中。这些分组以及它们的应答信息将选定所使用的 PPP 参数。

一旦双方对 PPP 参数达成一致之后，又会发送一系列 NCP 分组，用于配置网络层。通常情况下，PC 机希望运行一个 TCP/IP 协议栈，所以需要有一个 IP 地址。针对 IP 协议的 NCP 负责动态分配 IP 地址。

此时，PC 机已经成为一台 Internet 的主机，它可以发送和接收 IP 分组，当用户完成了工作后，NCP 断开网络层连接，并释放 IP 地址。然后 NCP 停掉数据链路层连接。最后，计算机通知调制解调器挂断电话，释放物理层连接。

PPP 选择的帧格式与 HDLC 的帧格式非常相似。PPP 与 HDLC 之间最主要的区别是：PPP 是面向字符的，HDLC 是面向位的。特别是，PPP 在拨号调制解调器线路上使用了字节填充技术，所以，所有的帧都是整数个字节。图 4-8 表示了 PPP 帧的格式。

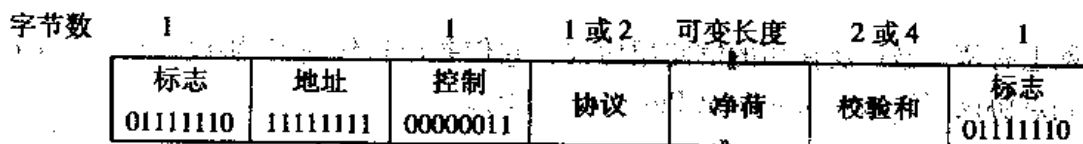


图 4-8 PPP 帧格式

PPP 帧都以一个标准的 HDLC 标志字节 (01111110) 作为开始，如果它正好出现在净荷域中，都需要进行字节填充。地址域总是被设置成二进制值 11111111，以表示所有的站都可以接受该帧。使用这样的值可以避免“必须分配数据链路层地址”的问题。

控制域的默认值是 00000011。此值表示了这是一个无序号帧。换言之，在默认方式下，PPP 并没有采用序列号和确认来实现可靠传输。

由于在默认配置下,地址和控制域总是常量,所以 LCP 提供了必要的机制,允许双方协商一个选项,该选项的目的仅仅是省略这两个域,因而每一帧可以节约 2 个字节。

协议域的任务是指明净荷域中是哪一种分组。已定义了代码的协议为: LCP、NCP、IP、IPX、AppleTalk 和其它协议。以 0 位作为开始的协议是网络层协议,例如 IP、IPX、OSI CLNP、XNS。以 1 位作为开始的协议被用于协商其它的协议,这包括 LCP 以及每一个支持的网络层协议都有一个不同的 NCP。协议域的默认大小为 2 字节,但通过 LCP 可以将它协商为 1 个字节。

净荷域是变长的,最多可达到某一个商定的最大值。如果在线路建立过程中,没有通过 LCP 协商该长度,则使用默认长度 1500 字节。如果有需要的话,在净荷域之后可以添加一些填充字节。

校验和域通常为 2 个字节,但通过协商也可以是 4 个字节。因而 PPP 在链路层上具有差错检测的功能。

总之,PPP 是一种多协议成帧机制,它适合于调制解调器、HDLC 位序列线路、SONET 和其它的物理层上使用。它支持错误检测、选项协商、头部压缩以及使用 HDLC 类型帧格式(可选)的可靠传输。

习 题

1. 数据链路层的主要功能包括哪几个方面的内容?
2. 试比较四种帧定界方法的特点。
3. 传输差错的主要原因是哪些? 差错类型有哪两种? 都有什么特点?
4. 检错码与纠错码的主要区别是什么? 常用的检错码有哪些?
5. 若发送窗口尺寸为 4,在发送 3 号帧并收到 2 号帧的确认帧后,发送方还可发几帧? 请给出可发帧的序号。
6. 若窗口序号位数为 3,发送窗口尺寸为 2,采用 Go-back-N 法,请画出由初始态出发相继下列事件发生时的发送及接收窗口图: 发送帧 0、发送帧 1、接收帧 0、接收确认帧 0、发送帧 2、帧 1 接收出错、帧 1 确认超时、重发帧 1、接收帧 1、发送帧 2、接收确认 1。
7. 若 BSC 帧数据段中出现下列字符串:
"A <DLE> <STX> BC <DLE> <DLE> DE <DLE> <ETB>"
问字符填充后的输出是什么?
8. 若 HDLC 帧数据段中出现下列比特串:
"0 1 0 0 0 0 0 1 1 1 1 1 1 0 1 0 1 1 1 1 1 0"
问比特填充后的输出是什么?
9. 用 BSC 规程传输一批汉字(双字节),若已知采用不带报头的分块传输,且最大报文块长为 129 字节,共传输了 5 帧,其中最后一块报文长为 101 字节。问每个报文最多能传多少汉字? 该批数据共有多少汉字?(假设采用单字节的块校验字符。)
10. 用 HDLC 传输 12 个汉字(双字节)时,帧中的信息字段占多少字节? 总的帧长占多少字节?
11. 简述 HDLC 帧中控制字段各分段的作用。
12. 试比较 BSC 和 HDLC 协议的特点。
13. 假设一条链路上到达的比特序列为 011010111110101001111111011001111110,给出去掉填充比特之后的帧,指出可能引入帧中的任何差错。

14. 假设要传输消息 1011001001001011, 并用 CRC 多项式 $X^8 + X^2 + X + 1$ 防止它出错。

(a) 使用多项式除法确定应传输的信息 (原始信息加系数)。

(b) 假设由于传输链路上的噪音使得消息最左端的比特发生反转。接收方 CRC 的计算结果是什么? 接收方如何知道发生了一个差错?

15. 试说明 PPP 协议的应用范围、帧结构的特点。

第5章 网络层

网络层是 OSI 参考模型中的第三层，介于传输层和数据链路层之间。它在数据链路层提供的两个相邻端点之间的数据帧的传送功能上，进一步管理网络中的数据通信，将数据设法从源端经过若干个中间节点传送到目的端，从而向传输层提供最基本的端到端的数据传送服务。网络层关系到通信子网的运行控制，体现了网络应用环境中资源子网访问通信子网的方式，是 OSI 模型中面向数据通信的第三层（也即通信子网）中最为复杂、关键的一层。

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括路由选择、拥塞控制和网际互连等。本章重点介绍网络层的原理、功能及其实现。

5.1 通信子网的操作方式和网络层提供的服务

端点之间的通信是依靠通信子网中的节点间的通信来实现的，在 OSI 模型中，网络层是网络节点中的最高层，所以网络层将体现通信子网向端系统所提供的网络服务。在分组交换方式中，通信子网向端系统提供虚电路（Virtual Circuit）和数据报（Datagram）两种网络服务，而通信子网内部的操作也有虚电路和数据报两种方式。

5.1.1 虚电路操作方式

在虚电路操作方式中，为了进行数据传输，网络的源节点和目的节点之间先要建立一条逻辑通路，因为这条逻辑通路不是专用的，所以称之为“虚”电路。每个节点到其它任一节点之间可能有若干条虚电路支持特定的两个端系统之间的数据传输，两个端系统之间也可以有多条虚电路为不同的进程服务，这些虚电路的实际路径可能相同也可能不同。

节点间的物理信道在逻辑上均可看作由多条逻辑信道组成，这些逻辑信道实际上由节点内部的分组缓冲器来实现。所谓占用某条逻辑信道，实质上是指占用了该段物理信道上节点分配的分组缓冲器。不同的逻辑信道在节点内部通过逻辑信道号加以区分，各条逻辑信道异步地分时复用同一条物理信道。

一条虚电路可能要经过多个中间节点，在节点间的各段物理信道上都要占用一条逻辑信道用以传送分组。由于各节点均独立地为通过的虚电路分配逻辑信道，也即同一条虚电路通过各段信道所获取的逻辑信道号可能是不相同的，所以各节点内部必须建立一张虚电路表，用以记录经过该点的各条虚电路所占用的各个逻辑信道号。

为使节点能区分一个分组属于哪条虚电路，每个分组必须携带一个逻辑信道号；同样，同一条虚电路的分组在各段逻辑信道上的逻辑信道号可能也不相同。传输中，当一个分组到

达节点时，节点根据其携带的逻辑信道号查找虚电路表，以确定该分组应发往的下一个节点及其下一段信道上所占用的逻辑信道号，用该逻辑信道号替换分组中原先的逻辑信道号后，再将该分组发往下一个节点。

各节点的虚电路表是在虚电路建立过程中建立的。比如，与 A 节点相连的源端系统要经中间节点 B、C 跟与 D 节点相连的目的端系统建立一条虚电路，源端系统可发出一个呼叫请求分组，该分组除了包含目的地址外，还包含源端系统所选取的还没被使用的最小逻辑信道号 N 。A 节点收到请求分组后在 A 节点与下一节点 B 间所有已使用的逻辑信道号之外选取一个最小编号 N_A ，并将请求分组中的逻辑信道号 N 替换成该逻辑信道号 N_A ，再将分组发送给节点 B。此后的各节点依次逐个根据自身实际情况选取新的逻辑信道号（如 N_B 、 N_C 、 N_D 等）来替换收到的分组中的逻辑信道号。最后，目的节点 D 将请求分组传送给连接它的端系统。在此过程中，每个节点的虚电路表中要记录两个逻辑信道号：前一个节点所选取的逻辑信道号和本节点所选取的逻辑信道号。这样便使得虚电路所跨越的每一段连接上的逻辑信道号都是惟一的。

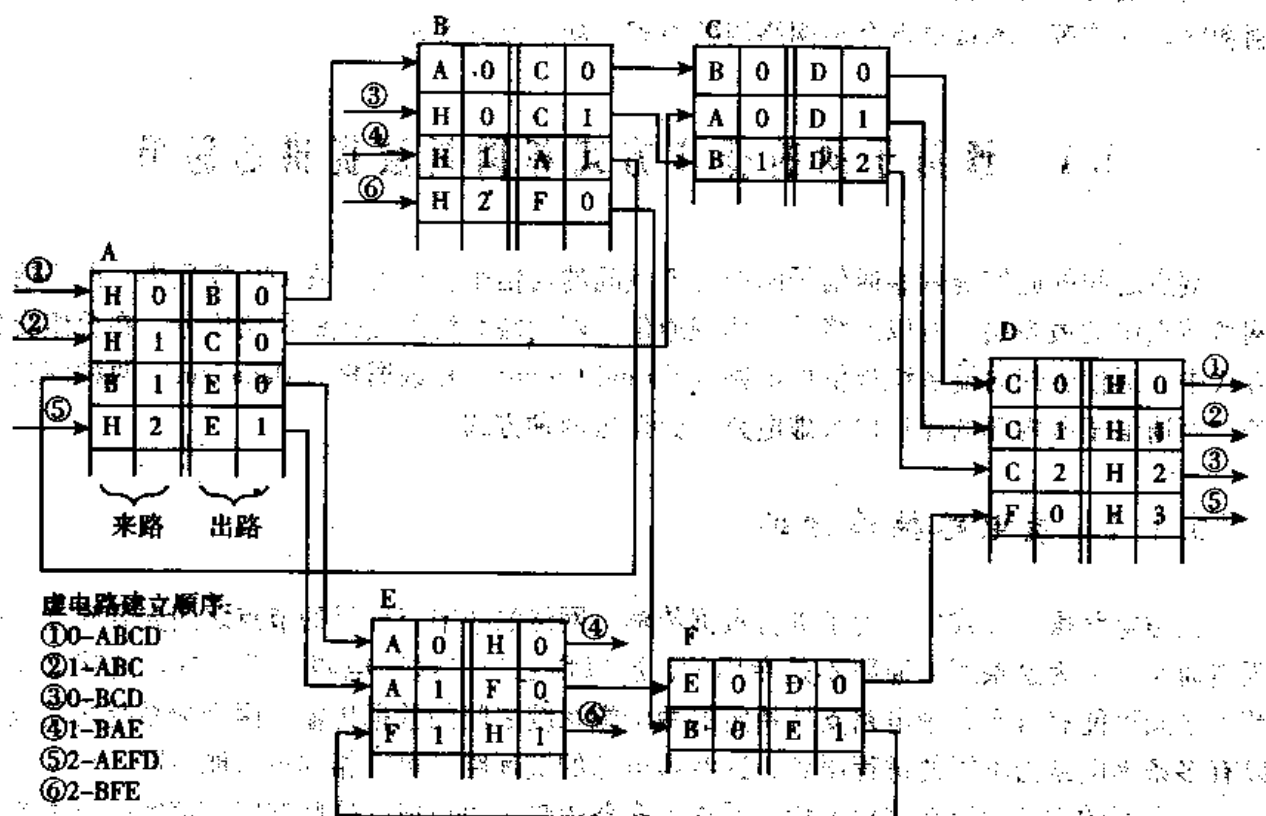


图 5-1 虚电路建立示例

图 5-1 给出了一个虚电路表建立的示例，这里假设建立了 6 条虚电路。由于虚电路上的数据是双向传输的，为保证两节点之间正、反两个方向的虚电路不相混淆，在一个节点选取逻辑信道号来替换其前一节点使用的逻辑信道号时，不仅要考虑与下一节点之间的逻辑信道号不相同，还要考虑与下一节点作为另一条反向虚电路的上一节点时所选取的逻辑信道号相区别。例如，在建立虚电路 1-BAE 时（这里 1-BAE 表示源节点为 B，建立虚电路时选取 1 为逻辑信道号，并经 A 传送到 E），在节点 B 中，尽管 A 节点是第一次作为 B 节点的下一节点，但由于虚电路 0-ABCD 中 A 到 B 间已使用了逻辑信道号 0，因此在出路一栏应选

B到A间的逻辑信道号为1。这样,当从节点A发来一个分组时,若它所携带的逻辑信道号为0,则说明是虚电路ABCD上的正向分组;若为1,则说明是虚电路BAE上的反向分组。对于虚电路2-BFE的建立也是同样情况。

各节点的虚电路表空间和逻辑信道号都是网络资源,当虚电路拆除时必须回收。这可通过某端系统发出一个拆链请求分组,告知虚电路中各节点删除虚电路表中有关表项来实现。

5.1.2 数据报操作方式

在数据报操作方式中,每个分组被称为一个数据报,若干个数据报构成一次要传送的报文或数据块。每个数据报自身携带有足够的信息,它的传送是被单独处理的。一个节点接收到一个数据报后,根据数据报中的地址信息和节点所存储的路由信息,找出一个合适的出路,把数据报原样地发送到下一个节点。

当端系统要发送一个报文时,将报文拆成若干个带有序号和地址信息的数据报,依次发给网络节点。此后,各个数据报所走的路径就可能不同了,因为各个节点在随时根据网络的流量、故障等情况选择路由。由于各行其道,各数据报不能保证按顺序到达目的节点,有些数据报甚至还可能在途中丢失。在整个数据报传送过程中,不需要建立虚电路,但网络节点要为每个数据报作路由选择。

5.1.3 虚电路服务

虚电路服务是网络层向传输层提供的一种使所有分组按顺序到达目的端系统的可靠的数据传送方式。进行数据交换的两个端系统之间存在着一条为它们服务的虚电路。

为了建立端系统之间的虚电路,源端系统的传输层首先向网络层发出连接请求,网络层则通过虚电路网络访问协议向网络节点发出呼叫分组;在目的端,网络节点向端系统的网络层传送呼叫分组,网络层再向传输层发出连接指示;最后,接收方传输层向发起方发回连接响应,从而使虚电路建立起来。此后,两个端系统之间就可以传送数据。数据由网络层拆成若干个分组送给通信子网,由通信子网将分组传送到数据接收方。

上述虚电路的服务是网络层向传输层提供的服务,也是通信子网向端系统提供的网络服务。但是,提供这种虚电路服务的通信子网内部的实际操作既可以是虚电路方式的,也可以是数据报方式的。以虚电路方式操作的网络,一般总是提供虚电路服务。OSI中面向连接的网络服务就是虚电路服务。在虚电路操作方式中,端系统的网络层同通信子网节点的操作是一致的。SNA就是采用这种虚电路操作支持虚电路服务方式的实例。

以数据报方式操作的网络,也可以提供虚电路服务,即通信子网内部节点按数据报方式交换数据,而与端系统相连的网络节点则向端系统提供虚电路服务。对于端系统来说,它的网络层与网络节点间的通信仍像虚电路操作方式的网络节点间一样,先建立虚电路,再交换数据分组,最后拆除电路。但实际上,每个分组被网络节点分成若干个数据报,附加上地址、序号、逻辑信道号等信息分送到目的节点。目的节点再将数据报进行排序,拼成原来的分组,送给目的端系统。因此,源端系统和源网络节点之间、目的

节点和目的端系统之间的网络层按虚电路操作方式交换分组，而目的节点和源节点之间则按数据报方式完成分组的交换。尽管通信子网的数据报交换是不可靠的，但是两端的网络节点做了许多诸如排序、重发等额外工作，从而满足了虚电路服务的要求。例如，在 ARPANET 中，其内部使用数据报操作方式，但可以向端系统提供数据报和虚电路两种服务。

5.1.4 数据报服务

数据报服务一般仅由数据报交换网来提供。端系统的网络层同网络节点中的网络层之间，一致地按照数据报操作方式交换数据。当端系统要发送数据时，网络层给该数据附上地址、序号等信息，然后作为数据报发送给网络节点；目的端系统收到的数据报可能是不按序到达的，也可能有数据报的丢失。例如，在 ARPANET、DNA 等网络中，就提供了数据报服务。数据报服务与 OSI 的无连接网络服务类似。

由虚电路交换网提供数据报服务的组合方式并不常见。可以想像有这么一种特殊情况：一个端系统的网络层已经构造好了用于处理数据报的服务，而当它要接入以虚电路方式操作的网路时，网络节点就需要做一些转换工作。当端系统向网络节点发送一个携带有完整地址信息的数据报时，若发向同一地址的数据报数量足够大，则网络节点可以为这些数据报同目的节点间建立一条虚电路，所有相同地址的数据报均在这条虚电路上传送。过一段时间后，当没有这类相同的地址的数据报要发送时，这条虚电路便可拆除。所以，这种数据报服务具有了虚电路服务的通信质量，但这样做既不经济，效率也低。

5.1.5 虚电路子网和数据报子网的比较

虚电路和数据报都有各自的支持者和反对者。这里试图从多个角度对两者作一下总结。表 5-1 中列出了最主要的比较项目。在子网内部，虚电路和数据报之间存在几个折衷。一个是路由器的内存空间和带宽之间的平衡。虚电路机制使得分组只要包含电路号即可，而不用包含完整的目标地址。使用数据报如果每个分组都很短，那么每个分组中的完整目标地址可能需要消耗相当多的开销，因而会浪费带宽。而使用虚电路付出的代价是路由器内部的表空间。根据通信电路和路由器之间的相对价格情况，来选择虚电路或数据报孰更合算。

另一个平衡点是建立虚电路所需要的时间和地址解析的时间。在使用虚电路的时候，它要求有一个建立阶段，这个阶段既要花费时间，也要消耗资源。然而，在一个虚电路子网中处理一个数据分组的方法却非常简单：路由器只要使用电路号作为索引，在内部表中找到该分组的目标去向即可。在一个数据报子网中，路由器需要执行一个相对复杂的查找过程，以便定位到该目标的表项。

还有一个需要考虑的问题是在路由器内存中所要求的表空间的数量。在数据报子网中，针对每一个可能的目标地址都要求有一个表项，而在虚电路子网中，只要为每一个虚电路提供一个表项即可。然而，这种优势并非绝对，因为建立连接的分组也需要被路由，它们也使用目标地址，如同数据报子网的做法一样。

表5-1

数据报和虚电路子网的比较

比较项目	数据报子网	虚电路子网
建立电路	不需要	需要
地址信息	每个分组包含完整的源地址和目标地址	每个分组包含一个很短的虚电路号
状态信息	路由器不保留任何有关连接的状态信息	每个虚电路都要求路由器为每个连接建立表项
路由	每个分组被独立地路由	当虚电路建立的时候选择路径，所有的分组都沿着这条路径
路由器失效的影响	没有，除非在崩溃过程中分组丢失	所有经过此失效路由器的虚电路都将终止
服务质量	很难实现	如果有足够的资源可以提前分配给每一个虚电路，则很容易实现
拥塞控制	很难实现	如果有足够的资源可以提前分配给每一个虚电路，则很容易实现

从保证服务质量，在子网内部避免拥塞的角度来讲，虚电路有一些优势，因为当建立连接的时候，虚电路子网可以提前预留资源（例如缓冲区空间、带宽和CPU周期）。当分组开始陆续到来之后，所需要的带宽和路由器CPU资源都已经准备就绪了。而对于数据报子网，要想避免拥塞是非常困难的。

对于事务处理系统，用于建立和消除虚电路所需的开销有可能会妨碍虚电路的使用。如果系统中大量的流量都是这种类型，那么在子网内部使用虚电路就毫无意义了。永久虚电路，即手工建立起来并且会持续几个月或者几年的虚电路，有可能在这里会很有意义。

虚电路也有脆弱性的问题。如果一台路由器崩溃了，或者内存中的数据丢失了，那么，即使它一秒钟之后又重新启动了，所有从它这里经过的虚电路都将不得不被中断。相反，如果一台数据报路由器停止了，则只有当时还有分组尚留在路由器队列中的用户会受到影响，甚至这些用户也不全都受到影响，这取决于这些分组是否都已经被确认了。一条通信线路的失败对于使用了该线路的虚电路来说是致命的，但如果使用了数据报，则这种失败很容易得到补偿。对于数据报子网，路由器可以平衡通信流量，因为在传输一个很长的分组序列过程中，路由器可以在半途改变传输路径。

5.2 路由选择

通信子网为网络源节点和目的节点提供了多条传输路径的可能性。网络节点在收到一个分组后，要确定向下一节点传送的路径，这就是路由选择，路由选择是网络层要实现的基本功能。在数据报方式中，网络节点要为每个分组路由做出选择；而在虚电路方式中，只需在连接建立时确定路由。路由选择包括两个基本操作，即最佳路径的判定和网间信息包的传送

(交换)。两者之间, 路径的判定相对复杂。确定路由选择的策略称路由选择算法 (Routing Algorithm)。

路由选择的核心是路由选择算法, 设计路由算法时要考虑诸多技术要素。首先, 考虑是选择最短路由还是选择最佳路由; 其次, 要考虑通信子网是采用虚电路的还是数据报的操作方式; 其三, 是采用分布式路由算法, 即每节点均为到达的分组选择下一步的路由, 还是采用集中式路由算法, 即由中央节点或始发节点来决定整个路由; 其四, 要考虑关于网络拓扑、流量和延迟等网络信息的来源; 最后, 确定是采用静态路由选择策略, 还是动态路由选择策略。路由选择算法以及它们使用的数据结构是网络层设计的一个重要研究领域。

5.2.1 最优化原则

所谓最优化原则 (Optimality Principle) 是指: 如果路由器 J 在从路由器 I 到 K 的最佳路由上, 那么从 J 到 K 的最佳线路就会在同一路由之中。

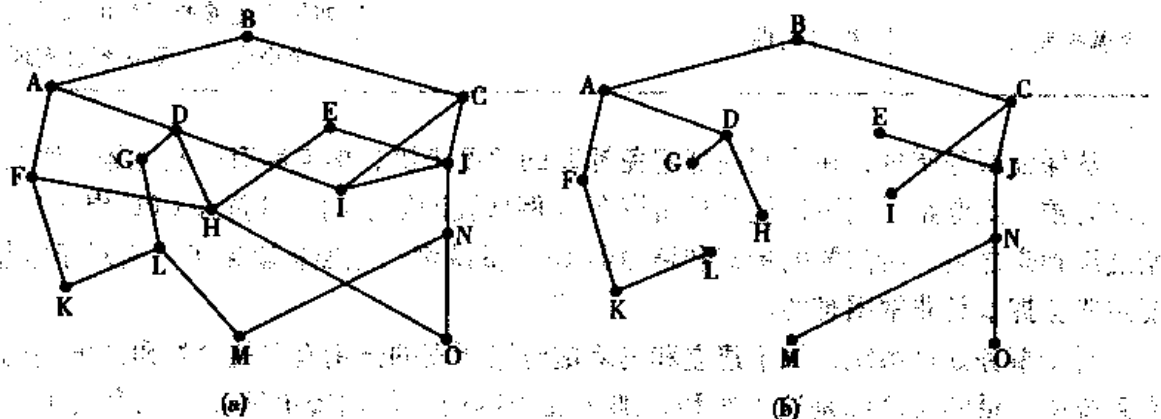


图 5-2 (a) 一个子网; (b) 路由器 B 的汇集树

作为最优化原则的一个直接结果, 可知从所有源端到目的端的最佳路由集合, 形成了以目的地为根的树。这样的一棵树称为汇集树 (Sink Tree), 如图 5-2 所示, 其中距离度量单位是站数。需要指出的是汇集树并不惟一。所有路由选择算法的目的就是为所有路由器找出并使用汇集树。

由于汇集树是一棵树, 它不包含任何循环, 因此沿汇集树传送分组不仅路由最优, 而且每个分组均可以在有限次数的步骤内送达。但实际情况并非如此简单, 因为在操作过程中链路和路由器可能经常会断开或停止工作, 然后又恢复工作, 所以不同的路由器对当前的拓扑结构可能会有不同的理解; 而且路由器获取子网及其汇集树信息的方法也可能不同。但不管怎样, 最优化原则和汇集树为路由选择算法提供了一种衡量标准。

5.2.2 静态路由选择算法

静态路由选择算法是一类不用测量也不需要利用网络信息, 而按某种固定规则进行路由

选择的算法。静态路由选择算法严格来说并不是一种算法，而是由网络管理员在路由选择前就已手工建立了映射表。20 世纪 90 年代以来，大多数优秀路由选择算法都是动态的，通过分析接收的路由修正消息来适应网络环境的变化。但静态路由选择算法也可以弥补动态路由选择算法的某些不足，如可以指定一些无法选择路由的数据包转发到某个指定的路由器，以保证所有数据包都得到处理。下面介绍三种静态路由选择算法：最短路由选择算法、扩散法和基于流量的路由选择算法。

1. 最短路由选择算法

最短路由选择 (Shortest Routing) 算法是一种简单易懂而应用广泛的技术。它的基本思想是：建立一个子网图，图中的每个节点代表一台路由器，每条弧线代表一条通信线路 (链路)，弧上的数字代表该线路的权重。为了在一对给定的路由器之间选择一条路由路径，路由算法只需在图中找到这对节点之间的最短路径即可。对于路径长度的测量有多种方法。一种方法是计算站点数量，另外也可以计算距离、信道带宽、平均通信量、通信开销、队列长度、传播时延等。

计算图中两个节点之间的最短距离有多种算法，其中最著名的算法是 Dijkstra 在 1959 年提出的 Dijkstra 算法。该算法要求每个节点用从源节点沿已知最佳路径到本节点的距离来标注。开始时由于一条路径也不知道，故所有的节点都标注为无穷大。随着算法的进行和不断找到的路径，标注随之改变，使之反映出较好的路径。一个标注可以是暂时性的，也可以是永久性的。但最初所有标注都是暂时性的。当发现标注代表了从源节点到该节点的最短可能路径时，就使之成为永久性的，不再进行修改。

为了说明加标注算法是怎样工作的，请参考图 5-3 (a) 所示的加权无向图，其中权值表示距离。要找出从 A 至 D 的最短距离，首先标注 A 为永久性的 (用实心圆点来表示) 作为开始，然后依次考察与 A 相邻的每个节点，用它们各自到 A 的距离重新标注这些点。每当重新标注一个节点时，也标注了此试探所对应的源节点，以便在以后重建最终路径时，检查完与 A 相邻的每一个节点后，再来检查整个图中所有暂时性的标注节点，并使标注最小的节点成为永久性节点，如图 5-3 (b) 所示。这个节点就变成了新工作节点。接下来从新工作节点 B 开始，检查与 B 相邻的所有节点。如果 B 的标注与从 B 到所有检查的节点距离之和小于此节点的标注，就重新标注这个节点。检查完所有与工作节点相邻节点以后，如果可能，则已修改了暂时性标注，在整个图中查找具有最小值的临时加标注节点。然后使此节点成为永久性的，并成为下一轮检查的工作节点。图 5-3 描述了此算法的前五步。

为了更好地理解该算法的工作原理，请看图 5-3 (c)。在这个点上，我们刚把 E 变成永久性节点。假设存在一条比 ABE 还要短的路径，比如说 AXYZE，则有两种可能性：节点 Z 已经是永久性的，或者它还没有变成永久性节点。如果 Z 是永久性的，则已经被探查过了 (当 Z 变成永久性节点之后的下一轮会探查 Z 的相邻节点)，所以路径 AXYZE 不会逃脱我们的搜索范围，因而它不可能是一条最短路径。现在考虑 Z 仍然是暂时性标注的情形。如果节点 Z 上的标注大于或者等于 E 上的标注，则 AXYZE 不可能是一条比 ABE 更短的路径；如果 Z 上的标注小于 E 上的标注，则应该首先是 Z 而不是 E 变成永久性节点，然后再从 Z 探查 E。

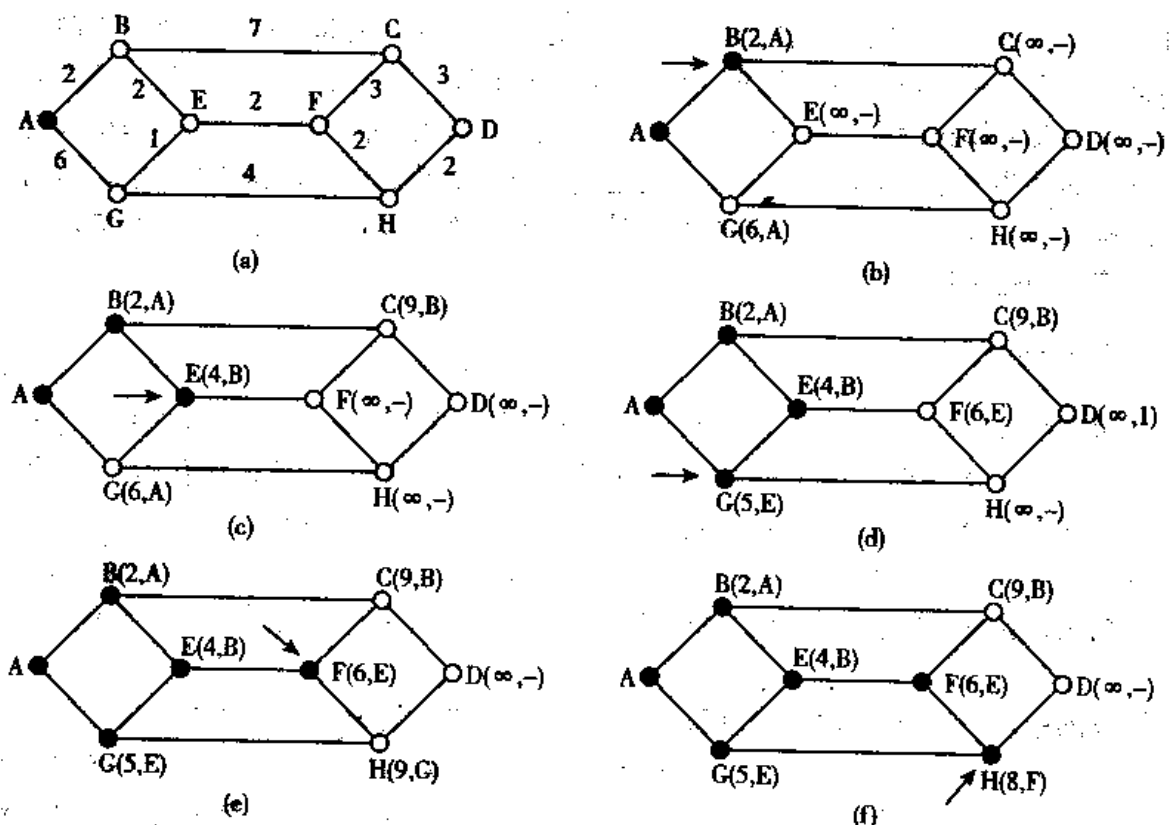


图 5-3 计算从 A 到 D 最短路径的前 5 步 (箭头指示工作节点)

2. 扩散法

另一种静态算法是扩散法 (Flooding)。这是一种最简单的路由算法, 又叫泛射路由选择法。一个网络节点从某条线路收到一个分组后, 再向除该条线路外的所有线路发送收到的分组。结果, 最先到达目的节点的一个或若干个分组肯定经过了最短的路径, 而且所有可能的路径都被尝试过。这种方法在一般系统中很少被实际采用, 但是可用于诸如军事网络等强壮性要求很高的场合, 即使有的网络节点遭到破坏, 只要源节点、目的节点之间有一条信道存在, 则泛射路由选择法仍能保证数据的可靠传送。另外, 这种方法也可用于将一个分组从数据源传送到所有其它节点的广播式数据交换中, 例如在分布式数据库应用中, 可同时更新所有的数据库。它还可被用来进行网络的最短路径及最短传输延迟的测试。在无线网络中, 一个站送出的消息可以被位于该站的无线范围内的所有站接收到, 这实际上正是扩散法。

显然这种方法会产生大量的重复分组, 甚至可能产生无穷多个分组。解决这个问题方法之一是让每个分组头包含站计数器, 每经过一个站点计数器减 1, 当计数器值为 0 时就扔掉分组。理想的情况是计数器设置初值为从源端到目的端的路径长度。如果发送者不知道路径长度, 它可以按最糟的情况把子网直径设置成计数器的初值。另一种方法是记录下分组扩散的路径, 防止它第二次再扩散到已扩散的路径中, 让源端路由器在所接收的来自主机的每一个分组中设置一个序号, 路由器收到分组后就将分组序号记录在相应源端对应的表项中, 以此来区分是否是一个分组的重复出现。同时, 为了防止记录分组序号的表无限地增长, 每个表应加一个计数器 k 作为参数, 表示直到 k 的序号都已看到。当一个分组进入时就查表, 如果是重复分组就将其扔掉。

扩散法的一个稍微实际的变种是选择性扩散法 (Selective Flooding)。在这种算法中, 路由器并不将每一个进来的分组从一条输出线上输出, 而是仅发送到与正确方向接近的那些线路上。

3. 基于流量的路由选择

前面介绍的算法只考虑到了拓扑结构, 而没有考虑到网络负载。在一些网络中, 每对节点间平均数据流量是相对稳定和可预测的。因此, 完全有条件在进行静态路由选择时把负载因素考虑进去。基于流量的路由选择 (Flow-based Routing) 正是这样一种既考虑拓扑结构又兼顾网络负载的静态路由算法。这种算法在预先知道的平均通信量的条件下对流量进行数学分析, 以优化路由选择。

这种分析的基本思想为: 对某一给定的线路, 如果已知负载与平均流量, 那么可以根据排队论计算出该线路上的平均分组延迟。由所有的线路平均延迟可直接计算出流量的加权平均值, 从而得到整个网络的平均分组延迟, 这样路由选择问题就归结为如何找出产生网络最小平均延迟的路由选择算法。

要采用这种方法, 有些信息必须是已知的。首先, 网络的拓扑结构已知; 其次必须给出通信量矩阵和线路容量矩阵; 最后, 必须选定一种路由算法。

5.2.3 动态路由选择算法

因为静态算法不考虑网络的当前负载情况, 现代的计算机网络通常使用动态的路由算法, 而不是上面介绍的静态路由算法。节点的路由选择要依靠网络当前的状态信息来决定的策略, 称动态路由选择策略, 也称为自适应路由选择算法。这种策略能较好地适应网络流量、拓扑结构的变化, 有利于改善网络的性能。但由于算法复杂, 会增加网络的负担, 开销也比较大。其中有两个动态路由选择算法最为常见, 即距离矢量路由算法和链路状态路由算法。

1. 距离矢量路由 (Distance Vector Routing) 算法

距离矢量路由算法是这样工作的: 每个路由器维护一张路由表 (即一个矢量), 它以子网中的每个路由器为索引, 表中列出了当前已知的路由器到每个目标路由器的最佳距离, 以及所使用的线路。通过在邻居之间相互交换信息, 路由器不断地更新它们内部的路由表。

举例来说, 假定使用延迟作为“距离”的度量标准, 并且该路由器知道它到每一个邻居路由器的延迟。每隔 T 毫秒每个路由器向它的每一个邻居路由器发送一个列表, 其中包含了它到每一个目标路由器的延迟估计值; 同时, 它也从每一个邻居路由器接收到一个类似的列表。假设一个路由器接收到来自邻居 X 的一个列表, 其中 X_i 表示 X 估计的到达路由器 i 所需要的时间。如果该路由器知道它到 X 的延迟为 m 毫秒, 那么它也知道在 $X_i + m$ 毫秒之内经过 X 可以到达路由器 i 。每个路由器针对每一个邻居都执行这样的计算, 就可以发现最佳的估计值, 然后新的路由表中使用这个最佳的估计值以及对应的输出线路。

这个更新过程如图 5-4 所示。其中 (a) 显示一个子网, (b) 的左 4 列显示了 J 路由器从邻居路由器接收到的列表。A 路由器声称它到 B 有 12 毫秒的延迟, 到 C 有 25 毫秒的延

迟, 到 D 有 40 毫秒的延迟, 等等。假定 J 已经测量和估计了它到邻居 A、I、H 和 K 的延迟分别为 8、10、12 和 6 毫秒。

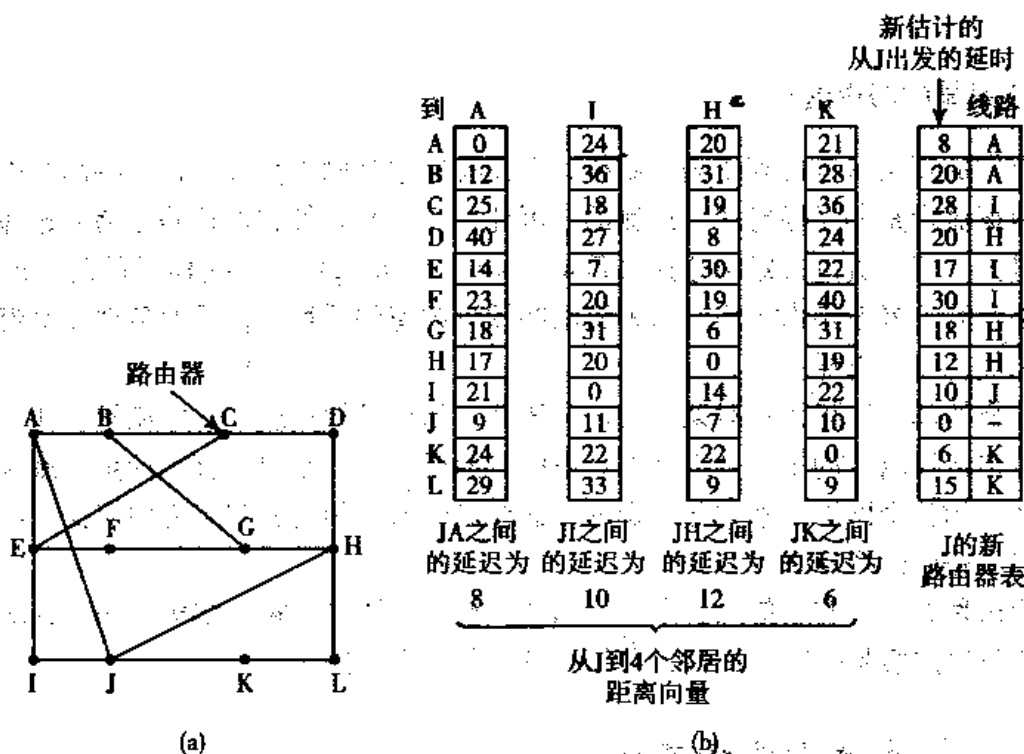


图 5-4 (a) 子网; (b) 来自 A、I、H、K 的列表以及 J 的新路由表

现在考虑 J 如何计算它到路由器 G 的新路径。它知道在 8 毫秒之内可以到达 A, 并且 A 声称可以在 18 毫秒内到达 G, 所以 J 知道, 如果它将那些目标地址为 G 的分组转发给 A 的话, 那么它到达 G 的延迟为 26 毫秒。类似地, 它计算出经 I、H 和 K 到达 G 的延迟分别为 41 ($31 + 10$)、18 ($6 + 12$) 和 37 ($31 + 6$) 毫秒。在这些值中, 最好的结果是 18, 所以在 J 的路由表中, 对应于 G 的表项中的延迟值为 18 毫秒, 所用的路径经过 H。对于所有其它的目标也执行同样的计算过程, 最后得到的新路由表如图中的最右一列。

距离矢量路由算法最初是 ARPANET 使用的路由算法, 也被用于 INTERNET 的 RIP (Routing Information Protocol) 路由信息协议。

2. 链路状态路由 (Link State Routing) 算法

在 1979 年以前, ARPANET 一直使用距离矢量路由算法, 而在此后, 则被替换为链路状态路由算法。该算法可以用以下 5 个部分加以描述。每一个路由器必须完成以下的工作:

- (1) 发现它的邻居节点, 并知道其网络地址;
- (2) 测量到各邻居节点的延迟或者开销;
- (3) 构造一个分组, 分组中包含所有它刚刚知道的信息;
- (4) 将这个分组发送给所有其它的路由器;
- (5) 计算出到每一个其它路由器的最短路径。

下面对每一个步骤稍作解释。

第一步: 发现邻居节点。

为了实现这个目标, 只需在每一条点到点线路上发送一个特殊的 HELLO 分组即可。线

路另一端的路由器应回送一个应答来说明它是谁？这些名字必须是全局惟一的。

第二步：测量线路开销。

链路状态路由算法要求每一个路由器知道它到各个邻居节点之间的延迟，最直接的方法是在这条线路上发送一个特殊的 ECHO 分组，另一端必须立即回送一个应答。这样可以计算出往返时间，再除以 2，则发送方路由器就可以得到合理的延迟估计值。

第三步：创建链路状态分组。

该分组的内容首先是发送方的标识，接着是一个序列号 (Seq) 和年龄 (Age)，以及一个邻居列表。对于每个邻居，同时也要给出这个路由器到每个邻居的延迟。图 5-5 (a) 所示的是一个通信子网的示例，每条线路上标出了延迟信息。共有六个路由器，所对应的链路状态分组如图 5-5 (b) 所示。

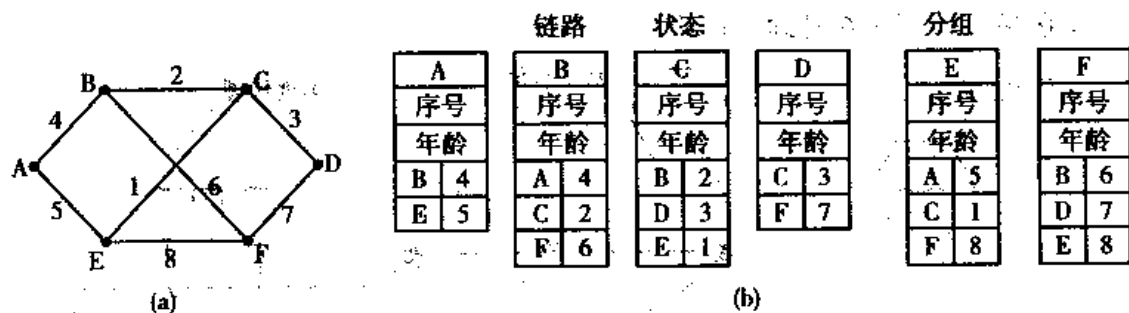


图 5-5 (a) 子网；(b) 链路状态分组

第四步：发布链路状态分组。

这一步骤首先是使用扩散（泛射）法来发布链路状态分组。为了控制扩散过程，每个分组都包含一个序列号，序列号随着每一个新的分组而递增。每个路由器记录下它所看到的所有（源路由器、序列号）对。当一个新的链路状态分组进来的时候，路由器在已经看到的分组列表中检查这个新进来的分组，如果它是一个重复分组，则将它丢弃。如果一个分组的序列号小于当前所看到过的来自该源路由器的最大序列号，则它将被当作过时分组而拒绝，因为该路由器已经有了更新的数据。

第五步：计算新的路由。

一旦一个路由器已经获得了全部的链路状态分组之后，它就可以构造出完整的子网图了，因为每条链路都已经被表示出来了。然后在路由器本地运行寻找最短路径的算法（例如：Dijkstra 算法），将该算法的结果安装在路由表中，然后恢复正常的操作。

链路状态路由算法被广泛应用于实际的网络中，在因特网中被广泛使用的 OSPF (Open Shortest Path First) 开放的最短路径优先协议，就用到了链路状态路由算法。

5.2.4 移动主机的路由选择

永远不会移动的主机称为固定主机，它们通过铜线或者光纤连接到网络中。另外还有两类主机，一种是迁移主机，它们基本上也是固定的，但是经常会从一个固定的站点移动到另一个固定的站点，并且只有当它们物理上连接到网络的时候才使用网络。另一种是漫游主机，是在移动过程中执行计算，它们希望在移动的时候还能保持与网络的连接，我们使用术语移动主机 (Mobile Host) 来代表这类主机，也就是说，移动主机是指那些离开了原始站点

(Home) 还想继续连接网络的主机。假设所有的主机都有一个永远不变的主场所, 主机也有一个永久性的主地址, 在包含移动主机的系统中, 路由算法的目标是, 能够做到用移动主机地址给它们发送分组, 而不管这些主机在哪里, 这些分组都能够被递交给它们。

如今, 成千上万的人拥有便携式计算机, 人们希望在任何地方都能够阅读自己的电子邮件, 访问他们日常使用的文件系统。移动式主机的出现增加了计算机网络的复杂性: 为了将一个分组路由到一台移动主机上, 网络首先要找得到这台主机, 也就是说如何把移动主机连入网络。这个问题的解决可采用如图 5-6 的方案, 它是一个由路由器和主机构成的 WAN, 与 WAN 相连的是若干个 LAN、MAN 及无线蜂窝单元。在这个模型里, 空间被划分成许多小单元, 称之为区域, 每个区域常常是一个 LAN 或无线蜂窝单元。每个区域有一个或多个外地代理, 用来管理所有来到当地的移动用户。另外, 每个区域还有一个主代理, 用来管理原本属于本区域, 但当时在外地的用户。

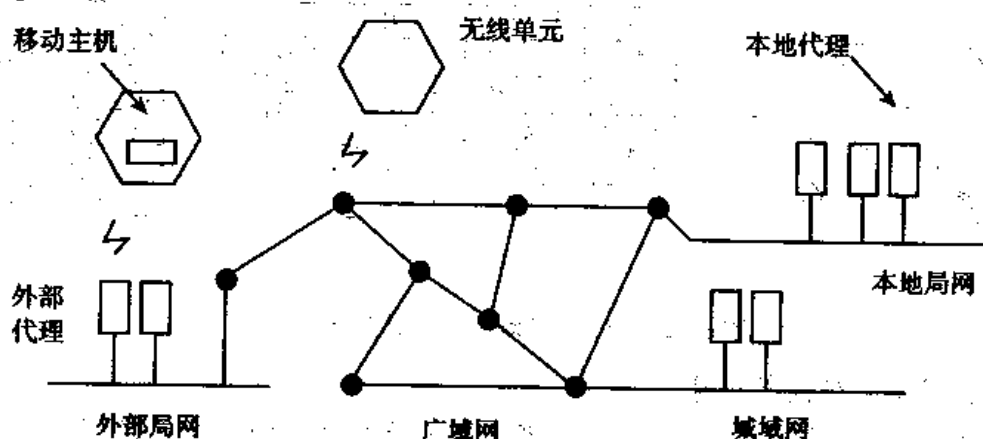


图 5-6 一个连着多个 LAN、多个 MAN 和无线单元的 WAN

当一个新用户进入某区域通过与当地网络相连, 或者进入该无线单元时必须将自己登录到当地的外地代理。典型的登录工作过程如下:

(1) 外地代理定期广播一个分组, 宣布自己的存在及其地址。一个新来的移动主机可以等待这类消息。移动主机可以广播一个分组问: 这里有没有外地代理?

(2) 移动主机登录到外地代理, 并给出其原来所在地的地址, 当前数据链路层地址, 以及一些安全性信息。

(3) 外地代理与移动主机的主代理联系, 核实移动主机是否真的在那。

(4) 主代理检查安全性信息 (由外地代理核实时发来), 如果核实通过, 则通知外地代理继续。

(5) 当外地代理从主代理处得到确认后, 在它的表中加入一个表项, 并通知移动主机, 登录成功。

在理想的情况下, 当用户离开某区域时, 也应该宣布自己的离开请求, 以便让外地代理注销自己, 但是许多用户离开时只是突然关掉计算机。

当一个分组被发往移动用户时, 它先路由到用户的主 LAN, 因为那里才是该用户的有效地址。发往主 LAN 的移动用户的分组被主代理收到, 接着主代理查找移动用户的新方位, 并找出管理移动用户的外地代理。然后主代理做两件事情: 其一, 将发给移动用户的分组装入一个外地分组的有效载荷字段中, 再将该外地分组发给外地代理; 其二, 告诉发送者, 将

分组装进有效载荷字段后，直接发往外地代理所在的地址，再由外地代理发送给移动主机，这样随后的分组就可以绕过主代理直接通过外地代理路由到移动主机。

5.2.5 广播路由选择

在有些应用中，主机需要给其它多个主机发送消息。例如，用于发布天气预报的服务，它的最佳工作方式是将消息广播给所有的机器，然后让那些感兴趣的机器读取数据。同时给所有的目标发送一个分组，这称为广播 (Broadcasting)；为了实现广播，已经提出了各种各样的方法。

一种不要求子网具有任何特殊特性的广播方法是，让源机器简单地给每一个目标单独发送一个分组。这种方法不仅浪费带宽，而且也要求源机器拥有所有目标机器的完整地址列表。

扩散法是另一种很显然的候选方法。尽管扩散法并不适合于普通的点到点通信，但是对于广播而言，它可能很值得考虑，尤其当下面所介绍的方法都不能适用的时候。用扩散法来实现广播所涉及的问题，与用扩散法作为点到点路由算法的问题是一样的：扩散过程产生了太多的分组，从而消耗太多的带宽。

第三种算法是多目标路由 (Multi-destination Routing)。使用这种方法，每个分组或者包含一组目标，或者包含一个位图，由该位图来指定所期望的目标。当一个分组到达一个路由器的时候，路由器检查所有的目标，以确定哪些输出线路是必要的（只要一条输出线路是到达至少一个目标的最佳路径，那么它就是必要的）。路由器为每一条需要用到的输出线路生成一份新的副本，在这份副本中只包含那些使用这条线路的目标。实际上，原来的目标集合被分散到这些输出线路上。在经过了足够多的跳数之后，每个分组只包含一个目标，因此可以被当做普通分组来对待。多目标路由方法就如同单个地址的分组一样，只不过当多个分组必须沿着同样的路径被转发的时候，其中一个分组承担全部的费用，而其它的分组都是免费搭乘的。

第四种广播算法显式地使用了以发起广播的路由器为根的汇集树 (Sink Tree)，或者也可以使用任何其它适当的生成树 (Spanning Tree)。生成树是子网的一个子集，它包含所有的路由器，但是不包含任何环。如果每个路由器都知道它的哪些线路属于一棵生成树，那么，它就可以将一个进来的广播分组复制到除了该分组到来的那条线路之外的所有生成树线路上。这种方法可以最佳地使用带宽，并且所生成的分组也绝对是完成这项任务所需的最少数量的分组。但存在的问题是，每个路由器必须都知道某一棵生成树才可以使用这种方法。有时候这样的信息是可以得到的（比如采用了链路状态路由算法的时候），但是有的时候无法获得这样的消息（比如采用了距离矢量路由算法的时候）。

最后一种广播算法是，即使当路由器根本不知道任何关于生成树的信息的时候，也要试图达到前一种方法的近似效果。其基本的想法称为逆向路径转发 (Reverse Path Forwarding)，当一个广播分组到达一个路由器的时候，该路由器对它进行检查，看它到来的那条线路是否是通常用来给广播源发送分组的那条线路。如果是的话，那就很有可能该广播分组是沿着最佳路径被转发过来的，因而是到达当前路由器的第一份副本。如果是这种情况，则路由器将该分组转发到除了到来的那条线路之外的所有其它线路上。然而如果广播分组是从其它任何一条并非首选的到达广播源的线路上到来的话，该分组被当作一个可能的重复分组而丢弃。

逆向路径转发算法的一个例子如图 5-7 所示。(a) 部分显示了一个子网，(b) 部分显

示了该子网中路由器 I 的一棵汇集树；(c) 部分显示了逆向路径算法是如何工作的。在第一跳的时候，I 发送分组给 F、H、J 和 N，如汇集树中的第二行所示。这些分组中的每一个都是在通向 I 的首选路径（假定首选的路径都沿着汇集树）上到来的，在图 (c) 中字母外面加一个圆圈就表示这样的分组。在第二跳的时候，共产生了 8 个分组，其中，在第一跳接收到分组的路由器各产生 2 个分组。结果是这 8 个分组都到达了以前没有访问过的路由器。其中 5 个是沿着首选线路到来的。在第三跳所产生的 6 个分组中，只有 3 个是在首选路径（在 C、E 和 K）上到来的，其它的都是重复分组。在经过第 5 跳和 24 个分组以后，广播过程终止了。相比之下，如果完全沿着汇集树的话，只需要 4 跳和 14 个分组。

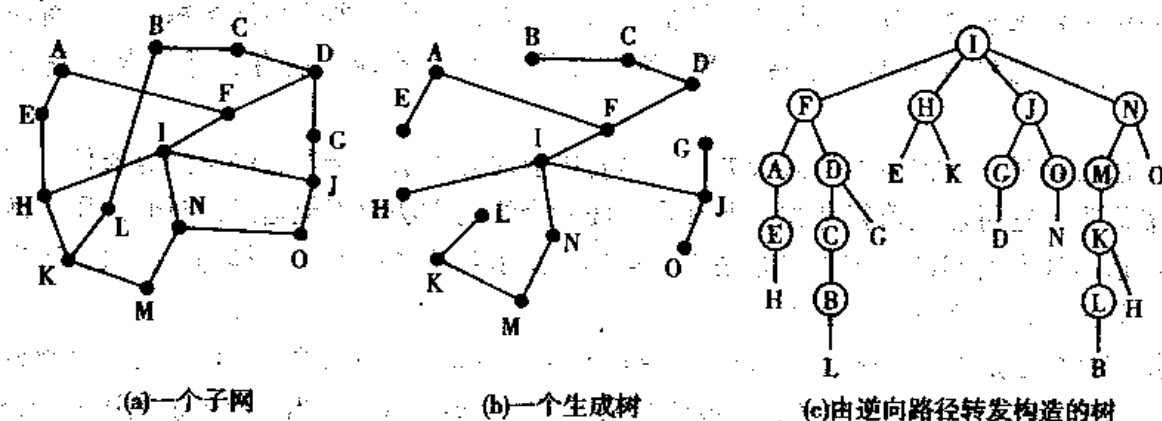


图 5-7 逆向路径转发

逆向路径转发的优点是：它的效率相对合理，而且容易实现。它并不要求路由器都知道生成树，也不像多目标路由方法那样要求每个分组中包含目标列表或者位图的开销。而且，它也不像扩散法那样要求特殊的机制来终止广播或扩散过程（在扩散法中，一种终止扩散的机制是，要求在每个分组中包含一个跳计数器，并且还需要提前知道子网的直径信息；另一种方法是，每个路由器为每个源维护一个看到过的分组的列表）。

5.2.6 多播路由选择

有些应用会有这样的要求：一些分布在各处的进程需要以组的方式协同工作，组中的进程通常要给其它所有的成员发送信息。如果组的规模比较小，那么它只要以点对点的方式给每一个其它的成员发送消息即可。如果组的规模比较大，那么这种策略的代价就会非常昂贵。有时也可以使用广播机制来实现这一点，但是在一个有上百万个节点的网络中使用广播机制来通知 1000 台机器会显得非常低效。因为大多数接收者对于这样的消息并没有兴趣（甚至更糟糕的是，他们虽然有兴趣，但实际上他们不应该看到这些消息）。因此，需要有一种方法能够给一些有明确定义的组发送消息，这些组的成员数量虽然很多，但是与整个网络规模相比却很小。给这样一个组发送消息称为多点播送（Multicasting），简称多播，又称组播，它的路由算法称为多播路由选择（Multicast Routing）。

多播传输需要对组进行管理。首先需要有一种方法来创建和销毁组，并且允许进程加入或者离开组。但路由算法关心的是，当一个进程加入组的时候，它需要把这个事实告诉它的主机。对于路由器来说，它们的哪些主机属于哪些组是非常重要的。当主机与组之间的从属

关系发生变化的时候，主机必须将这些变化告诉路由器，或者路由器定期地询问它们的主机。无论采用哪一种方式，路由器必须知道它们的哪些主机属于哪些组。路由器再告诉它的邻居，所以，主机与组的从属信息在整个子网中传播开来。

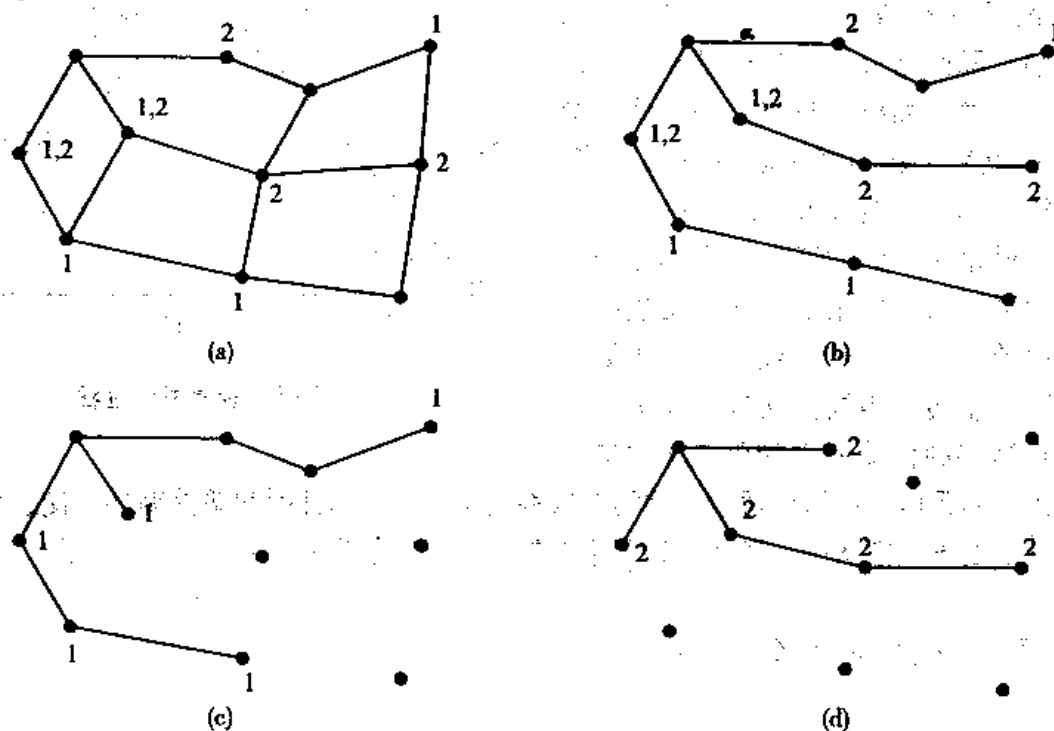


图 5-8 (a) 一个子网; (b) 最左边路由器的生成树;
(c) 小组 1 的多点播送树; (d) 小组 2 的多点播送树。

为了实现多播路由，每个路由器计算一棵生成树，该生成树覆盖所有其它的路由器。例如，在图 5-8 (a) 中，我们有两个组：1 和 2。有的路由器上连接了一些属于一个或者两个组的主机，如图 5-8 中所标出的那样。针对最左边路由器的一棵生成树如图 (b) 所示。当一个进程给一个分组发送多播分组的时候，第一个路由器检查它的生成树，并对该树进行修剪，去掉那些并不通向该组成员主机的所有线路。在我们的例子中，图 (c) 显示了针对组剪枝之后的生成树。类似地，图 (d) 显示了针对组剪枝之后的生成树。多播分组只沿着正确的生成树被转发。

修剪生成树有很多种可能的方法。最简单的修剪方法用于那些采用了链路状态路由算法的网络，这时候每个路由器都知道完整的拓扑结构，包括哪些主机属于哪些组。然后，修剪工作从每条路径的末端开始，逐步向根路由器前行，同时去掉所有不属于相应组的路由器。

5.3 拥塞控制

拥塞现象是指到达通信子网中某一部分的分组数量过多，使得该部分网络来不及处理，以致引起这部分乃至整个网络性能下降的现象，严重时甚至会导致网络通信业务陷入停顿，即出现死锁现象。这种现象跟公路网中习常所见的交通拥挤一样，当节假日公路网中车辆大量增加时，各种走向的车流相互干扰，使每辆车到达目的地的时间都相对增加（即延迟增

加), 甚至有时在某段公路上车辆因堵塞而无法开动 (即发生局部死锁)。

网络的吞吐量与通信子网负荷 (即通信子网中正在传输的分组数) 有着密切的关系。当通信子网负荷比较小时, 网络的吞吐量 (分组数/秒) 随网络负荷 (每个节点中分组的平均数) 的增加而线性增加。当网络负荷增加到某一值后, 若网络吞吐量反而下降, 则表征网络中出现了拥塞现象。在一个出现阻塞现象的网络中, 到达某个节点的分组将会遇到无缓冲区可用的情况, 从而使这些分组不得不由前一节点重传, 或者需要由源节点或源端系统重传。当拥塞比较严重时, 通信子网中相当多的传输能力和节点缓冲器都

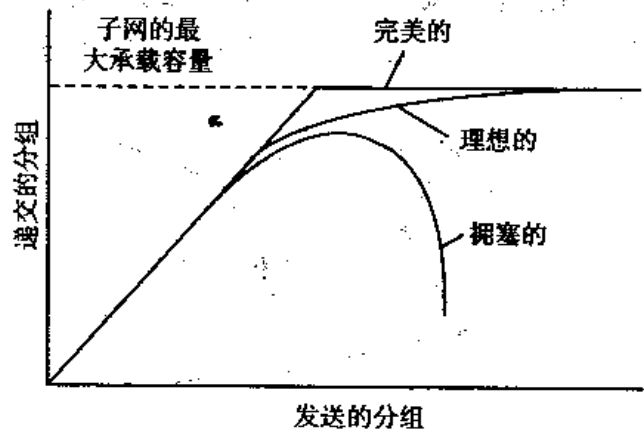


图 5-9 拥塞发生过程

用于这种无谓的重传, 从而使通信子网的有效吞吐量下降。由此引起恶性循环, 使通信子网的局部甚至全部处于死锁状态, 最终导致网络有效吞吐量接近为零 (如图 5-9 所示)。

5.3.1 拥塞发生的原因

(1) 多条流入线路有分组到达, 并需要同一输出线路, 此时, 如果路由器没有足够的内存来存放所有这些分组, 那么有的分组就会丢失。

(2) 路由器的慢速处理器的缘故, 以至于难以完成必要的处理工作 (如缓冲区排队、更新路由表等)。那么, 即使有多余的线路容量, 分组也需要进入到队列之中。

这里要指出的是拥塞控制和流控制之间的差异。拥塞控制的任务是确保子网能够承载所到达的流量。这是一个全局性的问题, 涉及各方面的行为, 包括所有的主机、所有的路由器、路由器内部的存储—转发处理过程, 以及所有可能会削弱子网承载容量的其它因素。与此相反, 流控制只与特定的发送方和特定的接收方之间的点到点流量有关。它的任务是, 确保一个快速的发送方不会持续地以超过接收方吸收能力的速率传输数据。流控制通常涉及的做法是接收方向发送方提供某种直接的反馈, 以便告诉发送方另一端的情形到底怎么样。

5.3.2 拥塞控制的通用原则

拥塞控制问题可以从控制论角度来看待, 解决的方案可以分成两类: 开环的和闭环的。

完成开环控制的手段有: 确定何时接受新的流量、确定何时丢弃分组及丢弃哪些分组, 以及在网络的不同点上执行调度决策。所有这些手段的共同之处是, 它们在做出决定的时候不考虑网络的当前状态。

开环算法可以分成在源端采取动作还是在目的端采取动作两类算法。

闭环方案则建立在反馈回路的概念基础之上, 当这种方法用于拥塞控制的时候, 它有三个部分:

(1) 监视系统, 检测到何时何地发生了拥塞。监视拥塞情况时可以使用多种度量标准,

其中最主要的度量包括：由于缺少缓冲区空间而丢弃的分组所占的百分比、平均队列长度、超时和重传分组的数量、平均分组延迟以及分组延迟的标准方差。对于所有这些度量值，数值越大，表示拥塞的可能性也越大。

(2) 将该信息传递到能够采取行动的地方。一种很显然的方法是，检测到拥塞的路由器给流量源（可能有多个源）发送一个分组。还有一种方法是，在每一个分组中可以保留一位或者一个域，当拥塞度量超过某一个阈值的时候，由路由器来填充入该位或者该域，以警告它的邻居。第三种方法是，让主机或者路由器周期性地向外发送探测分组，显式地询问有关拥塞的情况。然后，在有问题的区域中，可以利用这些信息来采取措施。

(3) 调整系统的运行，以改正问题。在闭环算法中可以分成显式反馈和隐式反馈两类。在显式反馈算法中，从拥塞点向源端发送分组以警告源端。在隐式反馈算法中，源端利用本地观察到的现象，比如确认分组送回来所需要的时间，来推断出是否存在拥塞。

一旦出现了拥塞，马上会想到两种解决方案：增加资源（带宽），或者降低负载。然而有时增加系统的资源或者容量是不可能的，或者说系统已达到了极限。此时，解决拥塞问题的惟一办法就是降低系统的负载。降低负载的措施包括：拒绝为某些用户提供服务，给某些用户或者全部用户降低服务等级以及让用户以一种更有预见性的方式来安排他们的需求。

5.3.3 拥塞预防策略

为预防拥塞在网络各个层次上可以采取的策略如表 5-2 所示。

表 5-2

影响拥塞的策略

层	策略
传输层	• 重传策略
	• 乱序缓存策略
	• 确认策略
	• 流控制策略
	• 确定超时策略
网络层	• 子网内部的虚电路与数据报策略
	• 分组排队和服务策略
	• 分组丢弃策略
	• 路由算法
	• 分组生存管理
数据链路层	• 重传策略
	• 乱序缓存策略
	• 确认策略
	• 流控制策略

我们首先从数据链路层开始，重传策略涉及一个发送方发送分组之后多久会超时，以及超时之后重传什么。一种是用回退 N 步的技术来重传所有未确认的分组，它给系统带来的负载要比使用选择性重传策略多得多。与此紧密相关的是缓存策略，如果接收方只是机械性地丢弃所有的乱序分组，那么，这些分组将不得不被重传，从而带来了额外的负载。从拥塞控制的角度而言，选择性重传比回退 N 步重传的策略明显要好得多。确认策略也会影响到拥塞。然而，如果确认消息被保存起来以便在反向流量中捎带回去，那么有可能会造成额外的超时和重传。一个紧凑的流控制方案（例如：一个小的窗口）将降低数据传输率，因此有助于缓解拥塞。

在网络层上，选择使用虚电路还是使用数据报，这也会影响到拥塞的情况，因为许多拥塞控制算法只能与虚电路子网一起工作。分组排队和服务策略关系到路由器是否为每一条输入线路使用一个队列，是否为每条输出线路使用一个队列，或者为两者各使用一个队列。它也关系到分组的处理顺序。丢弃策略是指当没有空间的时候，指明该丢弃哪个分组的规则。好的路由算法有助于避免拥塞，它可以将流量分配到所有的线路上，而一个不好的路由算法则会将大量的流量分配到本身已经拥塞的线路上。最后，分组生存期管理策略负责处理一个分组在被丢弃之前应该生存多长时间。如果生存期太长的话，则丢弃的分组可能会长时间地妨碍工作，但是，如果生存期太短的时候，则分组在到达目的地之前就有可能超时，从而导致重传。

在传输层中，如同数据链路层的情况一样，同样的问题也会发生，但是除此之外，在传输层上确定超时间隔更加困难，因为跨越一个网络的传输时间，要比两台路由器之间线路上的传输时间更加难以预测。如果超时间隔太短的话，则会发送不必要的额外负担，如果太长的话，则拥塞会缓解，但是一旦分组丢失，则响应时间将会增加。

5.3.4 虚电路子网中的拥塞控制

在这一小节中，将介绍用于虚电路子网的动态拥塞控制方法。

(1) 防止已经拥塞的子网进一步恶化的技术是准入控制 (Admission Control)。其思路较简单：一旦出现拥塞的信号，则不再创建任何虚电路，直到问题排除为止。这种方法非常简单，而且也易于实现。在电话系统中，当一台交换机超过负载的时候，它也会采用准入控制的方法，不再送出拨号音。

(2) 虽然允许建立新的虚电路，但要谨慎地选择路由，使所有新的虚电路都避开有问题的区域。例如，在图 5-10 (a) 的子网中，两台路由器已经损坏了。

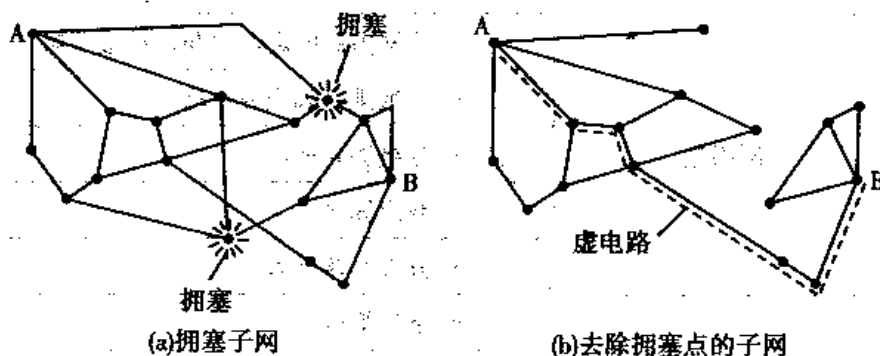


图 5-10

假设一台连接到路由器 A 的主机想要与另一台

连接到路由器 B 的主机建立一个连接。通常情况下，这个连接将会经过其中一台拥塞的路由器。为了避免这种情形，可以重构子网拓扑，如图 5-10 (b) 所示，省略掉拥塞的路由器和它们所有的线路。图中的虚线显示了一条可能的虚电路路径，它避开了拥塞的路由器。

(3) 进行资源预留：当建立虚电路的时候，在主机和子网之间进行协商，以达成一致的约定。约定的内容包括了流量的形状、所要求的服务质量和其它参数。为了保证约定的有效性，在建立虚电路的时候，子网往往会在沿途预留资源。资源可以是路由器中的表空间和缓冲空间，也可以是线路上的带宽。由于所有需要的资源得到了保证，因而新的虚电路上不可能发生拥塞。

5.3.5 数据报子网中的拥塞控制

每台路由器很容易就可以监视到它的输出线路和其它资源使用情况。例如：它可以给每条线路关联一个实变量 u ，其取值在 0.0 和 1.0 之间，它代表了这条线路最近的利用率。为了使 u 值尽可能地反映实际的情况，路由器需要定期地对线路的瞬时利用率 f (0 或者 1) 进行采样，然后，根据下面的公式更新 u 值：

$$u(\text{新}) = a \times u(\text{旧}) + (1-a) \times f$$

其中常数 a 代表了路由器忘记最近的历史情况有多快。

每当 u 超过了特定的阈值的时候，该输出线路进入到一种“警告”状态。路由器对每个新到来的分组都要进行检查，看它的输出线路是否处于警告状态。如果是的话，就需要采取以下各种措施。

(1) 警告位。在分组的头部设置一个特殊的位来指示警告状态；在帧中继 (Frame Relay) 网络中就是如此。当分组到达它的目标端的时候，传输实体将这一位复制到下一个确认分组中，所以，这一位也被送回到源主机。然后，源主机就可以削减流量。

只要路由器处于警告状态之中，它就会不停地设置警告位，这意味着源主机也会不停地得到这样的设置了警告位的确认分组。源主机可以监视这种设置了警告位的确认分组的比例，然后相应地调整它的传输速率。只要警告位仍然在源源不断地回来，则源主机就不停地减慢它的传输速率。当警告位确认分组减到极少量的时候，源主机增加它的传输速率。

(2) 抑制分组 (Chock Packet)。路由器给源主机送回一个抑制分组，并在抑制分组中指明原分组的的目标地址。同时，原来的分组被加上一个标记 (设置头部中的一位)，因而它在前行的路径上不会再产生更多的抑制分组。

当源主机收到抑制分组的时候，按照要求，它发送给指定目标的流量必须减少某一个百分比。由于发送给同一目标的其它分组可能已经在路上了，并且它们也将会产生更多的抑制分组，所以，在一段固定的时间间隔内，该主机应该忽略掉所有指向此目标的抑制分组。过了这一段时间间隔后，该主机继续监听下一段时间间隔内的抑制分组。如果又收到了抑制分组的话，则说明线路仍然拥塞，所以该主机进一步减少流量，并再次忽略掉一段时间间隔内的抑制分组。如果在监听周期内没有收到抑制分组的话，该主机可能会再次增加流量。该协议中暗含的反馈信息有助于防止拥塞同时又不影响正常的分组流。

主机通过调整策略参数 (比如窗口大小) 可以减慢流量。通常情况下，第一个抑制分组使得数据率减少到原来的 0.50，第二个抑制分组使得数据率减少到 0.25，以此类推。增长数据率的幅度要小得多，这样可以避免很快又发生拥塞。

(3) 逐跳 (Hop-by-hop) 抑制分组。当网络速度很高或者路由器离源主机的距离很远的时候，给源主机发送抑制分组并不能很好地起作用，因为反应太慢。例如：如图 5-11 (a)

所示，路由器 A 所连的一台主机正在给路由器 D 所连的一台主机发送数据，速度为 155Mbps。如果 D 主机现在用完了缓冲空间，那么抑制分组的传播过程如图 5-11 (a) 中的第 2、3、4 步所示。假如在三步的 30 毫秒期间内，A 又给 D 发送了 4.6Mb 的数据，即使 A 路由器的主机立刻停机，但沿途路径上的 4.6Mb 数据还在继续不断传输过来，并且必须要对它进行处理。只有在图 5-11 (a) 的第 7 步，D 路由器才会注意到分组减慢了。

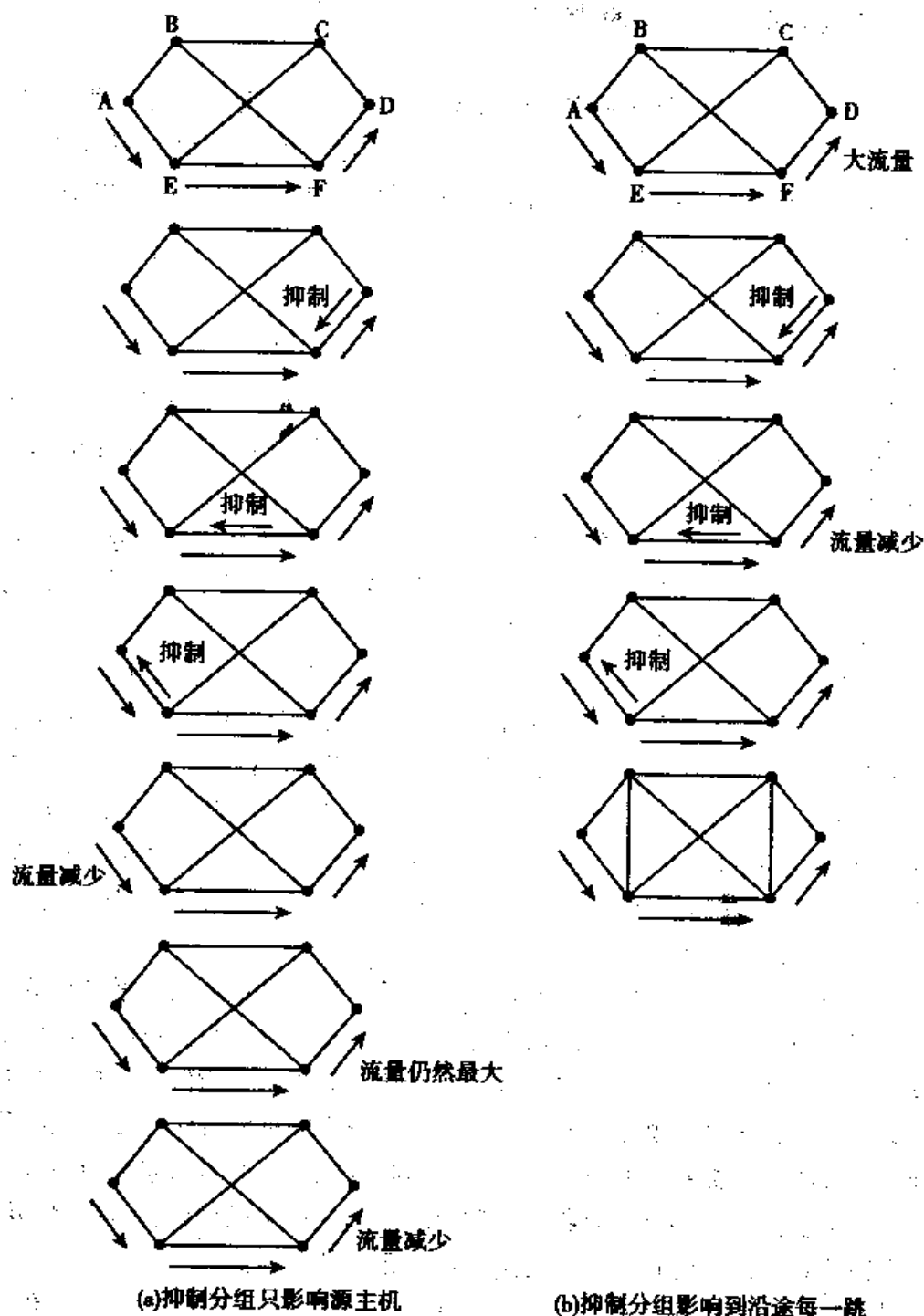


图 5-11

改进的方法是让抑制分组影响到沿途的每一跳，如图 5-11 (b) 所示。只要抑制分组到达了 F，则 F 必须按照要求减慢向 D 的分组流。为了做到这一点，要求 F 为 D 的分组流

分配更多的缓冲区，因为源主机仍然在全速发送数据，但是 F 这么做却让 D 立刻缓解了。在下一步中，抑制分组到达 E，它告诉 E 要减慢向 F 的分组流。这样也同样增加了 E 的缓冲区需求，但是却让 F 立即缓解了。最后，抑制分组到达 A，分组流才真正地减慢下来。

这种逐跳方案的实际效果是，在拥塞点上的拥塞现象很快得到了缓解，但其代价是上游路径上需要消耗更多的缓冲区空间。使用这种方法可以将拥塞消灭在萌芽状态，同时又不会丢失任何分组。

5.3.6 负载丢弃

当以上任何一种方法都不能消除拥塞的时候，路由器只有亮出最后的杀手锏了，即实施负载脱落 (Load Shedding)。它是指当路由器因为来不及处理分组而被淹没的时候，只要将这些分组丢弃即可。此想法可以与电力供应相比拟，在炎热的夏日里，当电力需求超过了供电能力时，为了避免电力系统崩溃，而有意实施“拉闸”。

到底应该丢弃哪些分组，这取决于所运行的应用的类型。对于文件传输而言，老的分组比新的分组更有价值，因为丢掉分组 6 而保留分组 7~10 将使得在接收方出现一个空隙，有可能导致重传分组 6~10 (如果接收方的习惯是丢弃乱序分组的话)。如果一个文件总共只有 12 个分组，那么，丢弃分组 6 可能意味着要重传分组 7~12，而丢弃分组 10 可能只要求重传 10~12。相反，对于流媒体应用，一个新的分组比老的分组更加重要。因此前一种策略 (即旧的分组比新的分组更好) 通常称为葡萄酒 (Wine) 策略，而后一种策略 (即新的分组比旧的分组更好) 通常称为牛奶 (Milk) 策略。

为了实现一种智能的丢弃策略，应用程序必须在它们的分组中标明优先级，以指明这些分组的重要性。如果它们做到了这一点，那么当路由器必须要丢掉分组的时候，它们可以首先丢掉最低优先级的分组，然后丢掉次低级的分组，以此类推。

当一开始检测到拥塞的时候，就采取措施，比等到拥塞严重影响了工作之后再采取措施显然要有效得多。因而产生一种新的流行算法：在实际耗尽所有的缓冲区空间之前就开始丢弃分组，这就是 RED (Random Early Detection) 随机的早期预测算法。

为了确定该什么时候开始丢弃分组，路由器维护了其队列最近的平均长度值。当某一条线路上的队列平均长度超过一定阈值的时候，该线路被认定是拥塞的，从而对它采取措施。由于路由器可能无法判断哪一个源是引起拥塞的罪魁祸首，所以，它能够做到的也就是随机地从拥塞的队列中选取分组。那么，路由器用什么方法来告知源主机有关的问题呢？一种办法就是如前所述，给源主机发送一个抑制分组，但这种做法会在已经拥塞的网络上引入更多的负载。另一种不同的策略是，只是将选取出来的分组丢弃，而不向源主机报告。源主机最终会感觉到缺少了确认，并采取相应的措施。由于源主机知道缺失分组往往是因为拥塞并丢弃分组造成的，所以它只能用减慢发送速度作为正确对策，而不是更加费力地发送更多的分组。这种隐式的反馈机制只有当源主机使用减慢传输速率作为分组丢失的响应对策时才起作用。

5.3.7 抖动控制

对于像音频流和视频流这样的应用，只要传输时间是恒定的，那么它就不会介意到底需

要 20 毫秒还是 30 毫秒才能将分组递交给目标主机。分组到达时间的变化量（即标准偏差）被称为抖动（Jitter）。比如，在高抖动的情况下，有的分组需要 20 毫秒到达，而其它的分组需要 30 毫秒到达，这将使得声音或者电影的质量很不稳定。图 5-12 显示了抖动的情况。与此相反，如果 99% 的分组都在 24.5 毫秒 ~ 25.5 毫秒的延迟范围内被递交给目标主机的话，则当然是可以接受的。

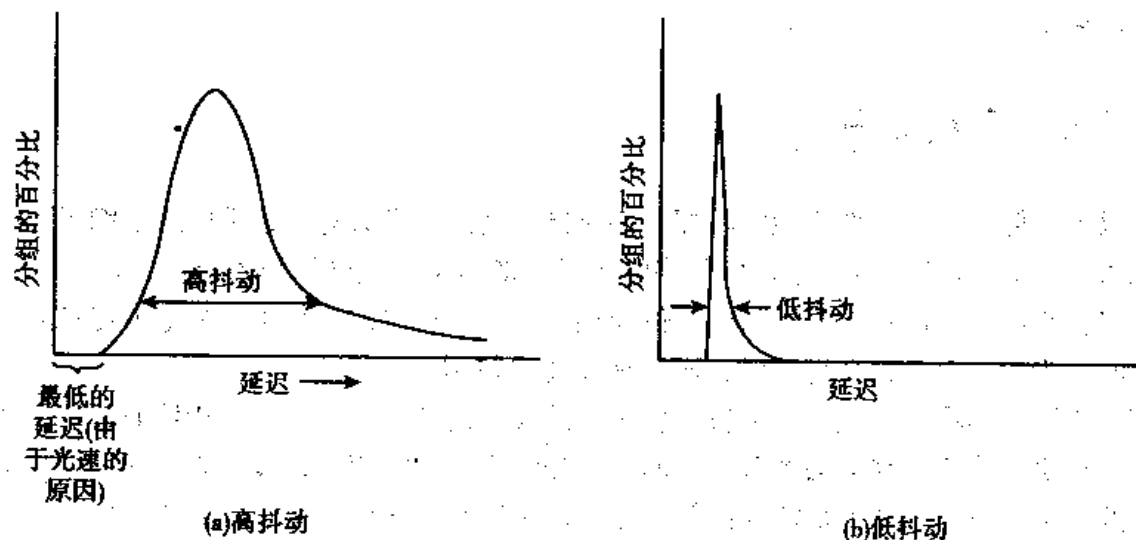


图 5-12

通过计算，得出沿途每一跳的期望传输时间，就可以对抖动加以控制。当一个分组到达一台路由器的时候，该路由器对它进行检查，看这个分组比预定的时间来早了，还是来晚了。这些信息被保存在分组之中，每一跳都相应地更新。如果一个分组提前到达的话，那么它尽可能多停留一段时间，以便回到预定的时间点。如果一个分组比预定的时间到达得晚的话，则路由器尽可能快地将它转发出去。

对于多个正在竞争同一条输出线路的分组，路由器接下去该转发哪一个分组呢？实际上，它所使用的算法总是可以选择偏离预定时间最远的那个分组。按照这种方法，比预定时间提前到达的分组将会减慢下来，而落后于预定时间的分组则会逐渐加速，无论哪一种情形，都可以减缓抖动的程度。

在有些应用场合中，例如视频点播（Video on Demand），也可以通过这样的方法来消除抖动：接收方将分组缓存起来，然后从缓冲区中获取数据并输出到显示器上，而不是实时地从网络上获取数据。然而，对于其它应用，特别是那些要求人与人之间进行实时交互的应用，例如因特网电话和视频会议，因缓存带来的延迟是不可接受的。

5.4 服务质量

从一个源到一个目标的分组流（Stream）称为一个流（Flow）。在面向连接的网络中，属于同一个流的所有分组将会走同样的路由路径；而在无连接的网络中，它们可能会走不同的路径。我们可以用 4 个基本的参数来描述每个流的需求特征：可靠性、延迟、抖动和带宽。这 4 个特征合起来决定了一个流所要求的服务质量（Quality of Service, QoS）。表 5-3

列出了一些常见的应用，以及它们的需求的严格程度。

表 5-3 服务质量需求的严格程度

应用	可靠性	延迟	抖动	带宽
电子邮件	高	低	低	低
文件传输	高	低	低	中
Web 访问	高	中	低	中
远程登录	高	中	中	低
音频点播	低	低	高	中
视频点播	低	低	高	高
电话	低	高	高	低
视频会议	低	高	高	高

前 4 种应用对于可靠性有很严格的要求。任何一位都不允许被错误递交。为了实现这个目标，通常的做法是，发送方计算每一个分组的校验和，接收方验证此校验和。如果一个分组在传输过程中被损坏了，那么它不会被确认，最终发送方重传该分组。这种策略可以带来很高的可靠性。后面 4 种应用可以容忍错误，所以，它们不需要计算或者验证校验和。

文件传输应用，包括电子邮件和视频，它们对于延迟并不敏感。如果所有的分组都统一延迟了几秒钟，则不会有任何影响。然而，一些交互应用，比如 Web 浏览和远程登录，则对于延迟比较敏感。另外，一些实时应用，比如视频会议和电话，它们有非常严格的延迟要求。

总之，不同的应用对于性能的需求各不相同。那么，如何实现这样的需求呢？没有一项技术能够以最优的方法提供高效的、可靠的 QoS，研究人员提出了许多技术，而且一些实际的解决方案通常将多种技术结合起来使用。例如：过度提供资源、流量整形、资源预留、准入控制、分组调度等。

5.4.1 集成服务和区分服务

从 1995 到 1997 年之间，IETF 作了很大的努力来设计流式多媒体的体系结构。此项工作的一般叫法为基于流的算法（Flow-based Algorithm）或者集成服务（Integrated Service）。这些算法同时针对单播和多播应用，下面我们主要将注意力集中在多播上，因为单播可以看做是多播的一个特例。

在集成服务体系结构中，主要的 IETF 协议是资源预留协议（Resource Reservation Protocol, RSVP）。利用该协议可以完成资源预留工作；若要发送数据则还需要使用其它的协议。RSVP 允许多个发送方给多个接收组传送数据，也允许接收方单独自由地切换信道，并且在优化使用带宽的同时消除阻塞的发生。在进行资源预留的时候，接收方可以（有选择地）指定一个或者多个期望的数据源。它也可以指定在预留期间这些选择是否固定

不变，或者指定它是否希望以后还可以改变数据源。路由器利用这些信息来优化带宽的使用计划。尤其是，如果两个接收方都同意以后不再改变数据源的话，那么它们只需共享一条路径即可。

基于流的算法有能力为一个或者多个流提供非常好的服务质量，因为它们在路由路径上预留了必要的资源。然而，这些算法也有一个缺点，要求提前一步建立每一个流。当应用中存在几千几万个流的时候，这种做法的扩展性很差。RSVP 几乎没有具体的实现，甚至类似于 RSVP 的实现也很少。

由于这些原因，IETF 设计了另外一个更加简单的服务质量方法，该方法不要求提前建立流，它主要由每台路由器在局部范围内实现，而不牵涉到整条路径。这种方法叫做基于类别 (Class-based) 的服务质量。IETF 已经对这种方法的体系结构进行了标准化，称为区分服务 (Differentiated Service)。

下面通过一个 Internet 电话的例子来理解基于流的服务质量和基于类别的服务质量之间的差异。如果使用基于流的方案，则每个电话呼叫都有专用的资源，从而服务质量可以保证。如果使用基于类别的方案，则所有的电话呼叫合起来共享同一份资源，即预留给电话类别的那份资源。其它类别的分组，比如文件传输中的分组，不可能夺走电话类别的资源，但是，任何一个电话呼叫都没有单独预留给它的私有资源。

5.4.2 标签交换和 MPLS

当 IETF 完成了集成服务和区分服务的时候，有些路由器厂商还在努力提出更好的转发方法。其工作思路是：在每个分组的前端增加一个标签，然后根据这个标签而不是根据目标地址进行路由。将这个标签作为内部表中的一个索引值，就可以把“找到正确的输出线路”这件事情变成简单的表格查询，利用这样的技术，路由过程可以很快地完成，而且沿途预留必要的资源也很容易做到。

显然，标记分组流的做法非常接近于虚电路的思想。X.25、ATM、帧中继，以及所有其它包含虚电路子网的网络也会在每个分组中放上一个标签（即虚电路标识符），也会在内部表中查询，并且根据查到的表项进行路由。然而，Internet 构造路由路径的处理方法与面向连接的网络构造路由路径的方法有本质的不同，所以，这里的标签技术肯定不是传统的电路交换。

这种“新的”交换思想有几个不同的名字，其中包括 Label Switching 和 Tag Switching（中文都翻译成标签交换）。最终 IETF 开始对这种思想进行标准化，它所用的名字是多协议标签交换协议 (Multi Protocol Label Switching, MPLS)。RFC 3031 和其它许多 RFC 文档描述了 MPLS。尽管 MPLS 背后的思想非常直截了当，但是它的细节却异常复杂，并且它有许多变种和优化。

MPLS 是实现 QoS 保证的关键技术。其目的是提高网络设备的性能价格比，提高网络设备的转发能力。所谓多协议是指不但支持 IPv4，还支持多种网络协议，如 IPv6、IPX、Appletalk 和 DECnet 等。它最初是由 Cisco 等网络设备公司提出的。在技术上是把第二层交换机的交换速度引入到路由器，使路由器在做出转发决定时，以一种简单的标签为参照，不再根据目标 MAC 地址和对应的 IP 地址做复杂的寻由查找。随着 MPLS 的完善，目前它已经成

为流量工程 (Traffic Engineering) 和 VPN 的重要手段。

MPLS 技术结合 IP 技术信令简单和 ATM 交换引擎高效的优点。在目前的通信网络中, 存在两种通信节点。一种是 ATM 交换机, 它是面向连接的异步传输模式, 传输的是固定长度的 53 字节信元。另一种是路由器, 它采用无连接的传输模式, 传输的是长度可变的 IP 分组。由于因特网爆炸式的增长, 基于 IP 的业务量以指数式飞速发展, 不但要求通信网具有高速数据通信能力、良好的可扩展性和完善的服务质量保证, 而且实现 IP 业务在 ATM 上的有效传输也成为迫切问题。按当前网络设备的发展趋势来看, 可以把具有 MPLS 功能的 IP 路由器和具有 MPLS 功能的 ATM 交换机结合起来, 组建新的集成业务通信网。其简单原理是, IP 分组通过路由器进入 ATM 骨干网, 既可以利用 ATM 交换机又可以避免在 ATM 网络中形成过多的虚通道。人们希望新的网络实现 IPOA (IP Over ATM), 即通过 ATM 网络来传输 IP 分组, MPLS 正是实现这一技术的最佳途径。MPLS 可以把二层交换和三层路由与网络业务组合在一起, 利用标签识别的简单性以大大减少寻由的复杂性。

5.5 网络互连

5.5.1 网络互连原理

网际互连的目的是使一个网络上的用户能访问其它网络上的资源, 使不同网络上的用户互相通信和交换信息。这不仅有利于资源共享, 也可以从整体上提高网络的可靠性。

要实现网际互连, 必须:

- (1) 在网络之间至少提供一条物理上连接的链路, 并具有对这条链路的控制规程;
- (2) 在不同网络的进程之间提供合适的路由实现数据交换;
- (3) 有一个始终记录不同网络使用情况并维护该状态信息的统一的计费服务;
- (4) 在提供以上服务时, 尽可能不对互连在一起的网络的体系结构作任何修改。

互连的网络在体系结构、层次协议及网络服务等方面或多或少存在着差异, 对于异构网来说 (例如各种类型的局域网) 差异就更大。这种差异可能表现在寻址方式、路由选择、最大分组长度、网络接入机制、用户接入控制、超时控制、差错恢复方法、状态报告方法、服务 (面向连接服务还是无连接服务)、管理方式等诸方面的不同。要实现网际互连, 就必须消除网络间的差异, 这些都是网际互连要解决的问题。

局域网 (LAN)、广域网 (WAN) 的网际互连有 “LAN—LAN”、“LAN—WAN”、“WAN—WAN” 和 “LAN—WAN—LAN” 四种形式。由于非 OSI 系统要与 OSI 系统互连, 非 OSI 系统之间也要互连, 所以, 网际互连并不单纯指不同的通信子网在网络层上互连。实际上, 两个网络之间要互连时, 它们之间的差异可以表现在 OSI 七层模型中的任何一层上。用于网络之间互连的中继设备称为网间连接器, 按它们对不同层次进行的协议和功能转换, 可以分为以下几类:

- (1) 转发器 (Repeater), 是一种低层次设备, 实现网络物理层的连接, 它对网段上的

衰减的信号进行放大整形或再生。转发器只能起到扩展网段距离的作用，所以使用转发器互连的网络在逻辑上仍属于同一网络。

(2) 网桥 (Bridge)，提供数据链路层上的协议转换，在不同或相同的局域网之间存储和转发帧。

(3) 路由器 (Router)，作用于网络层，提供网络层上的协议转换，在不同的网络之间存储和转发分组。路由器从一条输入线路上接收分组，然后再向另一条输出线路转发，这两条线路可能属于不同的网络，采用的协议也可能不同。

(4) 网关 (Gateway)，提供传输层及传输层以上各层间的协议转换，又称协议转换器。

注意，由于术语的不统一性，有些文献中将上述的网桥、路由器和网关一起统称为“网关”，此时它可能指的是在数据链路层及其以上各层之间进行协议转换的网间连接器。另外，还有一种称为桥路器 (Brouter) 的产品，兼有网桥和路由器两者的功能。

5.5.2 网桥技术

网桥 (Bridge) 最早是为把那些具有相同物理层和介质访问控制子层的局域网互连起来而设计的。后来网桥也用于具有不同 MAC 协议的局域网的互连。网桥工作在 OSI 模型的第二层，进行相似网络间帧的转发。

IEEE802.1 定义了网桥的协议结构。图 5-13 给出了一种使用一个网桥把两个局域网互连起来的情况。由图 5-13 可以看出网桥转发数据分组的过程是：首先数据由用户提交给 LLC。LLC 实体附加了一个头部后先把它递交给 MAC 实体，MAC 层再附加一个头部和尾部从而形成一个 MAC 帧。根据帧中的地址所包含的目的 MAC 地址，桥把这个包接收下来。桥并不把 MAC 字段分割，而是原封不动的转发给目的 LAN。因此该帧最后被注入目的 LAN，并由目的站点接收。

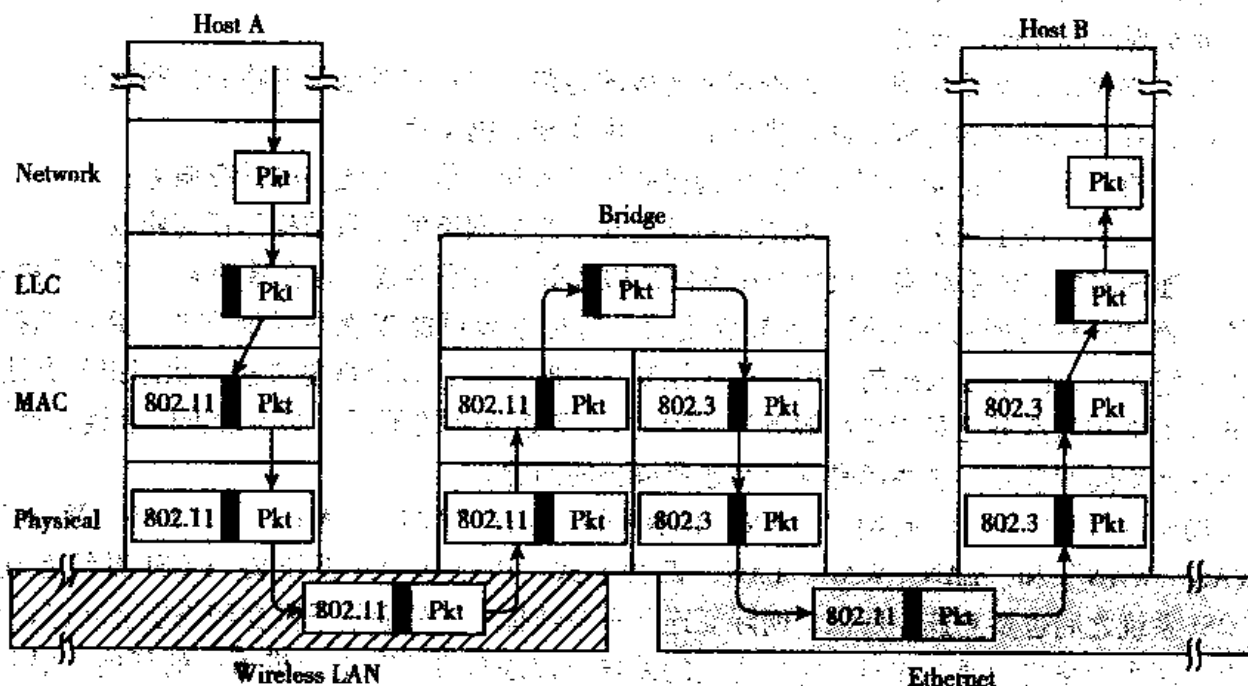


图 5-13 无线局域网到以太网的网桥

网桥除了发送跨网段传输的数据帧之外，还接收控制帧、目的地址为桥的帧等所有帧。

在网桥设计中,由于在一段时间内 MAC 帧到网桥的速率可能过快,网桥应该有足够的缓冲区。并且采取某种控制机制来防止拥塞。如果缓冲区接近饱和状态,网桥应该给那些已经经过多个网桥转发的帧以更高的优先权,这样不至于浪费已经花费在转发该帧上的带宽。

一个网桥可能连接多个局域网,连接多个局域网的网桥有相应的多个不同的 MAC 子层和物理层。网桥应该有寻址功能,它为了转发 MAC 帧必须知道该帧是属于它所连接的哪个局域网。在一个互连的局域网中也可能有多个网桥,因此该网桥应该有路由功能。

网桥的作用是通过过滤和转发功能实现的。当网桥收到一个 MAC 帧时,它检查该帧的源地址和目的地址,如果目的站点和源站点属于同一网络,则不进行转发,从而起到过滤作用并能正确地对网络进行隔离;否则,根据它所保留的路由表选择正确的网络进行转发。

1. 透明网桥

IEEE 802.1 委员会制订了一个称为透明网桥 (Transparent Bridge) 的标准,该标准的主页特征是:它的设计不仅仅是为了同种 MAC 协议的 LAN 间互连,同时也支持不同类型 LAN 之间互连。它的设计目标是把几个局域网连接在网桥上之后立即就可以运行,不需要进行硬件的配置,不用装入路由表参数。现有 LAN 不受网桥的影响。透明网桥的路由机制采用一种叫做生成树算法的技术。

透明网桥以混杂方式工作。接收连接到该网桥的局域网上传递的所有帧。每个网桥维护一个基于 MAC 地址的过滤数据库。数据库中列出了每个可能的目的地 (目前的 MAC 地址),以及它属于哪一条输出线路 (一个端口号,即表示转发给哪个 LAN),同时每个表项还有一个超时。网桥根据这个数据库把接收到的帧向相应的局域网中转发。假设一个桥在端口 x 上接收一个 MAC 帧时,则操作过程如下:

(1) 过滤数据库,确定该目的 MAC 地址是否在除端口 x 外的其它端口中。

(2) 如果目的 MAC 地址没有列到 x 以外的其它端口中,则将该帧送往 x 端口以外的所有端口进行扩散。

(3) 如果目的 MAC 地址在过滤数据库的某个端口 y ($y \neq x$),则确定端口 y 是否处在阻塞或转发状态。如果端口 y 是非阻塞的,就把该帧通过端口 y 转发到它所连接的 LAN 中。

当网桥初始化时,过滤数据库为空。为了能够了解到所有目的地的位置,透明网桥有一个自动学习的机制。该学习机制采用逆向学习法,从收到帧的源地址确定端口连接的 LAN 位置。

当一个帧到达一个特定端口时,网桥知道它来自于哪个 LAN,因而可以更新那个 MAC 地址对应的过滤数据库的有关信息。当计算机和网桥加电、断电或者移动时,网络的拓扑结构都会随之改变,因此过滤数据库中每一项都有一个防止过时的计时器。

在互连网络中,每个 LAN 对应一个图的节点,连接任意两个 LAN 的网桥对应着一条边。在透明网桥中,使用一个简单算法通过互连网络中网桥之间交换足够的信息,自动生成一棵生成树。该算法是动态的,当拓扑结构改变时,网桥应该能够发现,并自动生成一棵新的生成树。为了建造生成树,首先必须选出一个网桥作为生成树的根,实现的方法是每个网桥广播其序列号,序列号最小的网桥作为根,接着按根到每个网桥的最短路径来构造生成树。

2. 源路由选择网桥

透明网桥的优点是易于安装，只需要插进电缆即大功告成。但是从另一方面来讲，这种网桥并没有最佳地利用网络带宽，因为它们只用到了拓扑结构的一个子集（生成树）。一般支持总线网的人喜欢选择透明网桥。而令牌环的支持者则偏爱一种称为源路由选择网桥（Source Routing Bridge）。

源路由选择的核心思想是假定每个帧的发送者都知道接收者是否在同一 LAN 上。当发送一个帧到另外的 LAN 时，源机器将目的地址的高位设置成 1 作为标记。另外它还在帧头加进此帧应走的实际路径。

路径的构造过程如下：每个 LAN 有惟一的 12 位编号，每个网桥有一个在它的 LAN 中惟一标识自己的 4 位编号。因此，相距甚远的两个网桥可能会有相同的编号。但在同一 LAN 中两个网桥的编号必须不同。路径是网桥、LAN、网桥、LAN 等的编号序列。

源路由选择网桥只关心那些目的地高位是 1 的帧。当见到这样的帧时，它扫描帧头中的路由，寻找发来此帧的那个 LAN 的编号。如果发来此帧的那个 LAN 编号后跟的是本网桥的编号，则就将此帧转发到路由表中自己后面的那个 LAN。如果该 LAN 编号后跟的不是本网桥，则不转发此帧。

源路由选择的前提是互连网中的每台机器都知道所有其它机器的最佳路径。如何得到这些路由是源路由选择算法的重要部分。获取路由算法的基本思想是：如果不知道目的地地址的位置，源机器就发一广播帧，询问它在哪里。每个网桥都转发此帧，这样查找帧就可以到达互连网中的每一个 LAN。当应答回来时，途经的网桥将它们自己的标识记录在应答帧中，于是广播帧的发送者就可得到确切的路由，并从中选取最佳者。

5.5.3 网络互连协议

由于现在 Internet 使用非常广泛并且正在迅速发展，因此以下主要介绍在 Internet 中广泛使用的一些网络互连协议。

1. 路由信息协议

路由信息协议（Routing Information Protocol, RIP）实际上是一个简单的距离向量路由协议。RIP 可以在主机或路由器中实现。因此 RIP 协议被分为两种不同类型的操作方式。主机中实现的 RIP 工作在被动（Passive）状态，它不会传递自己路由表中的信息给别的路由器，它只是接收其它 RIP 路由器广播的路由信息，并且根据收到的路由信息更新自己的路由表。路由器中实现的 RIP 工作在主动（Active）状态，它定期把路由器信息传递给其它 RIP 路由器。并且根据收到的 RIP 消息来更新自己的路由表。这也就是说，被动 RIP 只接收，而主动 RIP 则发送和接收 RIP 消息。下面将主要讨论主动型 RIP 路由器的操作，被动 RIP 的操作相对来说要简单、直接得多。

每个 RIP 路由器都保存了一张路由表，每一项对应着一个目的地，其中，每项包括了目的地的 IP 地址、到目的地的路径距离的度量（Metric）、到目的地的路径的下一个路由表的 IP 地址（如果目的地是直接连接的，则不需要这个子段）、路由改变标志（指示这个路由信

息是否最近被改变过)以及和这条路由有关的一些计时器。RIP 采用的距离度量是一种非常简单的到目的地距离的测量方式: 站点计数度量, 路由器把到它直接连接的网络的距离定义为 1, 如果距离为 n , 表示它到达目的地途中要经过 n 个路由器, 即距离给出了该路由要经过的路由器个数。

每个 RIP 路由器每隔 30 秒广播一个路由消息。RIP 路由器也可能通过发送 Request 消息来询问别的路由器有关某些路由或者所有路由的信息, 比如, 当一个主机启动后, 可能要求相邻的 RIP 路由器传递路由表中的所有信息。当 RIP 路由器 R 从路由器 G 收到一个路由消息时, 它会检查该消息中包含的每一条到目的地 D 的路由, 其中距离为 $\text{cost}(G, D)$, 并把该路由与自己路由表中到同一目的地 D 的路由相比较。如果路由表中不存在到目的地 D 的路由, 就在路由表中增加一条路由: 到目的地 D 的下一个路由器跳段的地址为 G, 距离为 $\text{cost}(R, G) + \text{cost}(G, D)$, 其中 $\text{cost}(R, G)$ 为本地网络的花费 (经常为 1)。如果路由表中的路由把 G 作为下一个跳段, 则更新该路由的距离为 $\text{cost}(R, G) + \text{cost}(G, D)$ 。否则, 比较是否路由消息中指出的到目的地 D 的路由的距离更短:

$$\text{cost}(R, G) + \text{cost}(G, D) < \text{cost}(R, D)$$

其中 $\text{cost}(R, D)$ 为路由表中原有到目的地 D 的路由。如果满足这个式子, 说明找到一条更短的路由, 从而更新路由表中那条到目的地 D 的路由: 下一个跳段路由器为 G, 距离为 $\text{cost}(R, G) + \text{cost}(G, D)$ 。注意, 如果路由消息中新通知的路由和原来的路由的距离是一样的, RIP 仍然选择使用老的路由, 这有助于保持路由的稳定。但是, 如果某个路由器崩溃或者某一网络连接出现了故障, 这条路由就不会继续存在。因此, RIP 在路由表中对每条路由都有一个计时器, 当收到新的有关这条路由的消息时, 该计时器被重新设置, 如果计时器超时 (超过 180 秒), 这条路由就被宣告为非法, 即目的地不可达。注意, 它并不是马上从路由表中删去, 因为这条失效的路由还应该向邻居路由器报告, 经过一段超时 (被称为 Garbage Collection Timer) 后, 该路由最终从路由器中被去掉。这种机制实际上是一种 n 中取 k ($k = \text{out-of-}n$) 机制。每个路由器接收定期广播的路由信息, 只有每 6 次广播 ($6 \times 30 = 180$ 秒) 中至少收到一个消息时才会认为该路由合法, 这样在一定程度上防止了由于路由消息的丢失而带来的不可靠性。

2. 开放最短路径优先协议

当网络规模很大时, RIP 协议的运作并不令人满意, 并且 RIP 还受到无穷计数问题的困扰。在这种情况下, 一种新的内部网关协议被提出来, 这就是开放最短路径优先 (Open Shortest Path First, OSPF) 协议, 它已成为目前最主要的内部网关协议。

OSPF 是一种链路状态路由协议。在链路状态路由协议中, 每个路由器通过维护它自己的本地链路状态信息 (即路由器到子网的链路状态和可以到达的邻居路由器), 并通过扩散的方法把更新了的本地链路状态信息广播给自治系统中的每个路由器。这样每个路由器都知道自治系统内部的拓扑结构和链路状态信息。路由器根据这个链路状态库计算出到每个目的地的最短路径 (路由)。所有路由器都采用相同的算法来计算最短路由, 而且这个计算是在路由器本地进行的。

OSPF 是一种动态的路由算法, 能够自动而快速地适应拓扑结构的变化。每次收到一个

链路状态消息，并且这个链路状态消息改变了整个自治系统的拓扑或链路状态时，都要重新计算到每个目的地的最短路由。OSPF 支持负载平衡功能，当同时有几条到目的地的最短路径时，可以将负载分流到这些路由之上。因为链路状态信息的描述非常小，并且很少需要进行传输，所以链路状态算法所要使用的带宽也非常小。

(1) 链路拓扑。OSPF 支持 3 种类型的连接和网络：

- 点到点网络，即连接一对路由器的网络，比如一个 56Kb/s 的串行线路。
- 广播网络，该网络支持广播功能，并且至少有两个以上的路由器连接在上面，比如 Ethernet。
- 非广播方式的网络，该网络有多个（大于两个）路由器连接在上面，但是不支持广播功能，比如 X.25 分组交换网。OSPF 把非广播方式的网络进一步分为两种方式：第一种称为非广播多路访问（Non-Broadcast Multi-Access, NBMA）网络，连在这个网络上的路由器可以直接通信，它和广播方式的 OSPF 运作类似；第二种是点到多点（Point-to-Multi-Point）网络，这种方式把非广播网络看成多个点到点链路。

(2) OSPF 协议过程。在正常情况下，每个路由器要定期扩散链路状态更新信息，为了保证运行这个链路状态路由算法的所有路由器都能收到这个消息，路由器之间应建立一个逻辑连接，并沿这个逻辑连接传递链路状态信息。路由器收到一个消息时，如果该消息是重复的，则丢弃它，否则除了到来连接外，在它的所有逻辑连接上传播该消息的一个拷贝。扩散消息被确认（Link State ACK），以保证可靠性。

路由器之间的逻辑连接被称为一个邻接（Adjacency）。在大多数情况下，邻接是在邻居路由器之间的连接，比如一条连接两个邻居路由器的点到点链路。但是并不是所有邻居路由器都是邻接路由器。假设所有的邻居路由器都是邻接路由器，考虑一个 Ethernet，如果有 N 个路由器连在上面，则总共可能有 $N(N-1)/2$ 条邻接，每当其中一个路由器收到一个消息时，它将发送一个同样的消息给每个邻接路由器。在最坏情况下，每个邻接路由器将立即把收到的消息扩散给其它邻接路由器，因此这个消息在被检测到重复之前可能被传递给大多数邻接路由器两次。这样，大概有消息的 N^2 个拷贝在该网络上传递，而实际上只要 N 个拷贝就足够了。为了防止这种情况，OSPF 引入了选取路由器（Designated Router）的概念，即对广播网络或者前面提到的 NBMA 非广播网络，连在上面的所有路由器选举一个选取路由器作为代表，它被认为与所有邻居路由器邻接，而其它邻居路由器之间没有邻接。只有邻接的路由器之间才能交换路由信息。选取路由器负责把它所连接的网络的链路状态信息传递给其它路由器。除了选取路由器外，一般还有个备份选取路由器，在选取路由器出现故障时使用。

为了发现邻居路由器以及维护相应的邻接关系，OSPF 使用 Hello 协议来定期交换消息。对于点到点物理连接来说，只要在链路上发送 Hello 消息就可以了。而在广播方式网络中是通过多点广播来交换消息的，对于非广播网络，则可能需要网络管理人员进行配置以发现邻居路由器。

在通常情况下，每个路由器会定期扩散链路状态更新（Link State Update）消息到其邻接路由器，该消息给出了链路的状态，邻接关系及路径花费。当链路的状态、邻接关系或者路径花费有变化时，路由器也会马上发送链路状态更新消息。

数据库描述（Database Description）消息给出了发送者所拥有的所有链路状态的当前顺

序号。接收者通过比较这个序号，就可以知道谁的数据最新，这个消息是在路由器刚加入进来时使用，以便能够拥有最新的链路状态信息。

一个路由器在和邻接路由器交换数据库描述消息后，可能发现自己的某部分数据已经过时了。路由器可以发送链路状态请求（Link State Request）消息来要求邻接路由器传递最新的信息。表5-4给出了 OSPF 所使用的 5 种消息。

表 5-4

OSPF 的消息类型

消息类型	描述
Hello	用于发现谁是邻居
Link State Update	为邻居提供发送者的链路状态更新
Link State ACK	确认链路状态更新
Database Description	通知发送者有哪些更新
Link State Request	向对方请求信息

综上所述，路由器通过扩散把自己的链路状态信息告诉它所在区域的其它路由器。这种每个路由器都建立一个它所在区域的有向图，并计算出最短路径。主干区域中的路由器也执行相同的过程，另外主干区域还从区域边界路由器获取信息，计算出从主干到每个非主干区域的最短路径，这个信息再分发给区域边界路由器，由该路由器在它的区域中广播该消息。通过这个消息，路由器在转发跨区域分组时可以选择到主干区域的最合适出口（区域边界路由器）。

5.5.4 网络互连设备

1. 网桥

网桥是一种存储转发设备，用来连接类型相似的局域网。从互连网络的结构看，网桥属于 DCE 级的端到端的连接；从协议层次看，网桥属于链路层范畴，在该层对数据帧进行存储转发。它既不同于只作单纯信号增强的转接器，也不同于进行网络层转换的网间连接器。但网桥仍然是一种网络连接的方法，因为局域网本身没有网络层，只有在主机站点上才有网络层或提供网络层服务的功能。

网桥接收帧并送到数据链路层进行差错校验，然后送到物理层再经物理传输介质送到另一个子网。在转发帧以前，网桥对帧的内容和格式不作修改或仅作很少的修改。网桥应该有足够的缓冲空间，以便能满足高峰负荷时的要求。另外，网桥必须具备寻址和路由选择的逻辑功能。

局域网的逻辑功能自下向上可分为物理层、介质访问控制层（MAC）及逻辑链路控制层（LLC）三层，异构局域网的差异主要体现在物理层及介质访问控制层中。图 5-14 给出了一个网桥的工作原理图，图中的两个局域网 802.X 和 802.Y 分别为 802.3、802.4 和 802.5 MAC 标准中的一种。网络中发送的数据由 802.X 的 MAC 控制信息 X、LLC 控制信息

L 和网络协议数据单元（即分组）组成。当网桥收到数据后，在 MAC 子层去掉 MAC 控制信息 X，然后交给 LLC 子层。若网桥的 LLC 子层发现数据是要发向 802. Y 局域网中某个站的，则将数据通过 MAC 子层加上相应控制信息 Y 送到 802. Y 局域网中，再由对方主机接收。此时，在 802. Y 局域网中，数据由 802. Y 的 MAC 控制信息 Y、LLC 控制信息 L 和网络协议数据单元组成。在上述过程中，由于各种局域网有其不同的物理特性和数据格式，所以传输过程中还要进行转换。

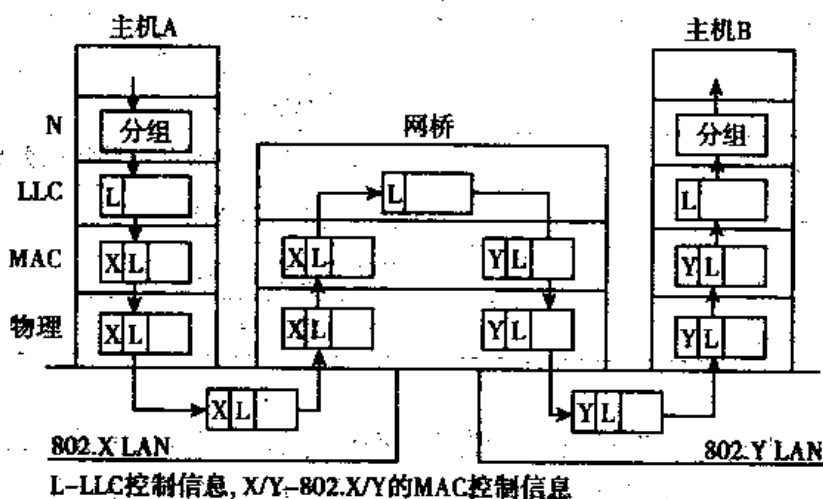


图 5-14 网桥工作原理

2. 路由器

(1) 路由器和网桥的区别。路由器和网桥都是实现多个网络互连的设备。路由器和网桥的不同点表现在：

① 网桥工作在数据链路层，而路由器工作在网络层。网桥利用物理地址（MAC 地址）来确定是否转发数据帧，而路由器则根据目的 IP 地址来确定是否转发该分组。

② 如果使用网桥去连接两个局域网，那么两个局域网的物理层与数据链路层协议可以是不同的，但数据链路层以上的高层要采用相同的协议。如果使用路由器去连接两个局域网，那么两个局域网的物理层、数据链路层与网络层协议可以是不同的，但网络层以上的高层要采用相同的协议。

③ 网桥工作在数据链路层，由于传统局域网采取的是广播方式，因此容易产生“广播风暴”问题，而路由器可以有效地将多个局域网的广播通信量相互隔离开来，使得互连的每一个局域网都是独立的子网。

(2) 路由器的主要服务功能。

① 建立并维护路由表。为了实现分组转发功能，路由器内部有一个路由表数据库与一个网络路由状态数据库。在路由表数据库中，保存着路由器每个端口对应连接的节点地址，以及其它路由器的地址信息。路由器通过定期与其它路由器和网络节点交换地址信息来自动更新路由表。路由器之间还需要定期地交换网络通信量、网络结构与网络链路状态等信息，这些信息保存在网络路由状态数据库中。

② 提供网络间的分组转发功能。每当一个分组进入路由器时，路由器检查报文分组的源 IP 地址与目的 IP 地址，然后根据路由表数据库的相关信息，决定该分组往下应该传送给

哪一个路由器或主机。

(3) 路由器的基本工作原理。

① 互连网络的协议结构。图 5-15 给出了用路由器互连的网络系统层次结构与数据流示意图。其中，图 5-15 (a) 给出了一个使用两个路由器，将两个局域网通过一个广域网互连的结构。

图中的两个局域网中，局域网 1 是总线形以太网，局域网 2 是令牌环网。广域网 (WAN) 是一个 X.25 分组交换网。主机 A 连接在局域网 1 的 Ethernet 上，主机 B 连接在局域网 2 的 Token Ring 网上。图 5-15 (b) 给出了对应的主机、路由器的层次结构。图 5-15 (c) 给出了在互连网络中不同位置分组的格式。

其中，连接在局域网 1 的主机 A 的传输层与网络层使用的是 TCP/IP 协议，逻辑链路控制 (LLC) 子层采用 802.2 协议标准，MAC 子层与物理层采用 802.3 标准的 Ethernet 协议。连接在局域网 2 的主机 B 的传输层与网络层同样也使用了 TCP/IP 协议，LLC 子层采用 802.2 协议标准，MAC 子层与物理层采用 802.5 标准的 Token Ring 协议。

路由器 1 要分别连入局域网 1 的 Ethernet 与广域网 X.25 分组交换网。那么从它的内部协议层次结构看，与局域网 1 连接的端口 1 的 LLC 子层采用 802.2 协议标准，MAC 子层与物理层采用 802.3 标准的 Ethernet 协议，与局域网 1 保持一致，与 WAN 连接的端口 2 的网络层、数据链路层与物理层采用 X.25 分组交换网的协议标准。

路由器 2 要分别连入广域网与局域网 2 的 Token Ring。那么从它的内部协议层次结构看，与 WAN 连接的端口 1 的网络层、数据链路层与物理层采用 X.25 分组交换网的协议标准，与局域网 2 连接的端口 2 的 LLC 子层采用 802.2 协议标准，MAC 子层与物理层采用 802.5 标准的 Token Ring 协议。

② 用路由器互连的网络系统中数据的传输过程。可以通过图 5-15 (b) 中主机 A 向主机 B 发送数据的传输过程，来说明用路由器互连的网络的基本工作原理。

当主机 A 要向主机 B 发送数据时，主机 A 的应用层数据 (Data) 传送给传输层；传输层在 Data 前面加上 TCP 的报头 TCP 头部后，将 (TCP 头部 + Data) 传送给网络层；网络层在它的前面再加上 IP 报头 IP 头部后，将 (IP 头部 + TCP 头部 + Data) 传送给 LLC 子层，依照以上的规律，通过局域网 1 发送的帧的内容为 (MAC 头部 + LLC 头部 + IP 头部 + TCP 头部 + Data)。

当路由器 1 接收到该帧时，由于路由器 1 端口 1 的 LLC、MAC 子层与物理层采用 802.3 标准的 Ethernet 协议，与局域网 1 保持一致，因此它可以通过 MAC、LLC 子层的顺序，将 (IP 头部 + TCP 头部 + Data) 整体作为高层数据送到路由器 1 的网络层。网络层根据 IP 报头 IP 头部中的源 IP 地址与目的 IP 地址，通过路由表查找输出路径。如果路由表表明了该分组应该通过路由器 1 的端口 2 发送到 X.25 网，那么路由器 1 通过端口 2 的 X.25 分组交换网的网络层、数据链路层，逐级在 (IP 头部 + TCP 头部 + Data) 之前加上 X.25-3 分组头与 X.25-2 帧头 (即链路头)、帧尾 (即链路尾)，再由物理层，通过 X.25 分组交换网，传输到远程的路由器 2。

当路由器 2 的端口 1 接收到该分组之后，它将按照 X.25 分组交换网的数据链路层、网络层的顺序，逐级除去 X.25-3 分组头 X.25-2 帧头、帧尾，将 (IP 头部 + TCP 头部 + Data) 交给路由器 2 的路由处理软件。路由器 2 的路由处理软件发现分组的目的主机就在

端口2连接的局域网2上,那么它就会将(IP头部+TCP头部+Data)作为网络层的高层数据,通过端口2对应的LLC、MAC子层的顺序,按照802.2、802.5Token Ring协议标准,逐级加上帧头,再由Token Ring的物理层传输到主机B。

主机B在接收到该帧之后,按照MAC、LLC子层顺序,逐级除去802.5帧头,将(IP头部+TCP头部+Data)分组交主机B的网络层。主机B的网络层根据目的IP地址判断是它应该接收的分组后,除去IP协议头IP头部,将正确的(TCP头部+Data)送交主机B的传输层。

图5-15(c)给出了互连网络中不同位置的分组和帧结构,它是以上关于路由器对数据处理过程的总结。数字分别表示主机与路由器的相邻层接口,对应的是通过该接口的分组或帧的结构。

从以上讨论中可以看出,通过路由器连接两个网络,它们的物理层、数据链路层与网络层协议可以是不同的,这是因为路由器在不同的端口根据连接的网络类型的不同,已经考虑了端口的各层的协议一致性问题。但是,网络层以上的高层要采用相同的协议。

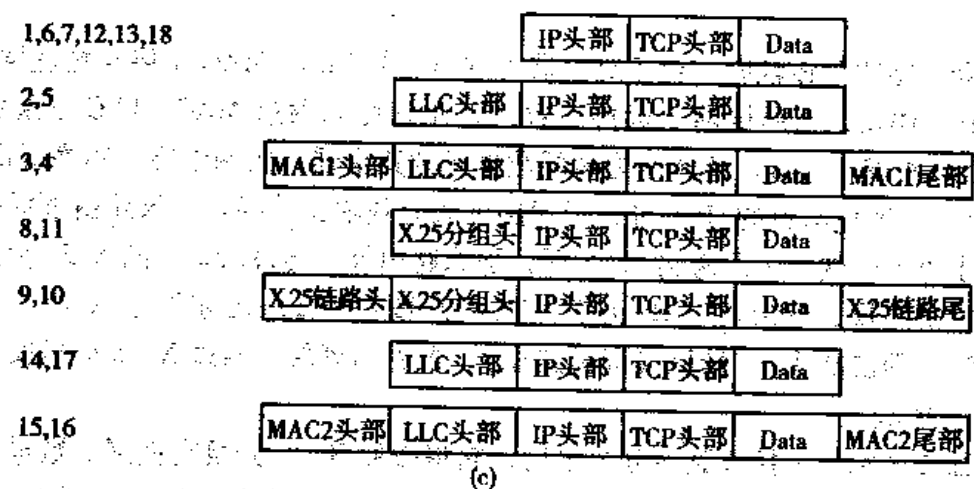
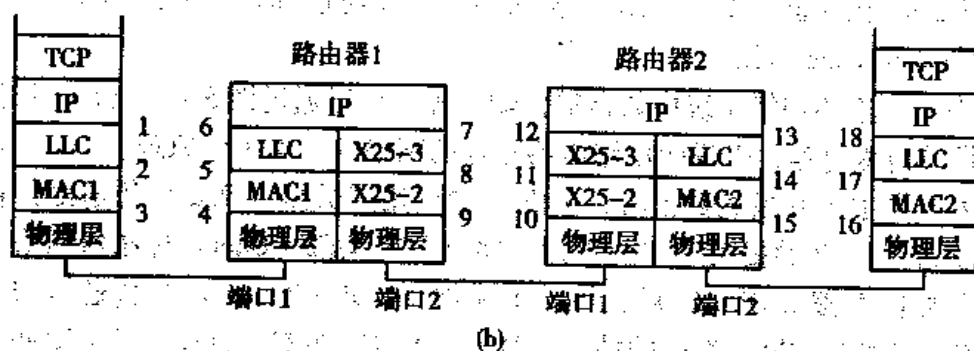
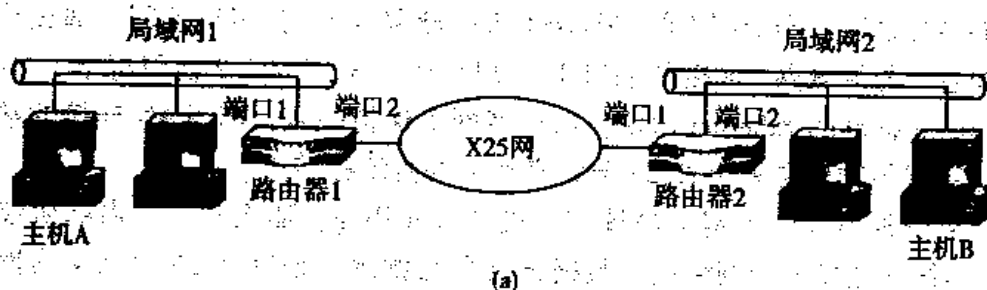


图5-15 路由网互连的层次结构与数据流示意图

3. 网关

网关也称为协议转换器，用于高层协议的转换，对传输层到应用层均能支持。

若两互连网络的主机高层中仅传输层协议不同，则可以利用网关的功能在传输层间作协议转换，内容包括数据格式的重新装配、长数据的分段、地址格式的转换及操作规程的适配等。在高层协议转换的实际实现中，并不一定要分层进行，例如，从传输层到应用层的协议转换可以一起进行。

5.6 因特网的互连层协议

在网络层，因特网可以被看做一组互相连接的子网或自治系统（AS）。在因特网中，实现这些子网或 AS 互连的就是互连层协议，IP 协议就是为了实现网络互连而设计的。IP 协议是 TCP/IP 协议族的核心，它提供一种不可靠的、无连接的 IP 报文服务，传输层上的数据信息都以 IP 报文的形式传输，它提供一种从源端到目的端传输 IP 报文的最佳尝试方法，而不管这些机器是否在同一网络中，或者传输是否还要经过其它网络。

在互连层中有四个重要的协议：互连网协议（Internet Protocol, IP）、互连网控制报文协议（Internet Control Message Protocol, ICMP）、地址转换协议（Address Resolution Protocol, ARP）和反向地址转换协议（Reverse Address Resolution Protocol, RARP）。

5.6.1 IP 协议

互连网协议 IP（Internet Protocol）是互连层最重要的协议，它将多个网络连成一个互连网，可以把高层的数据以多个数据报的形式通过互连网分发出去。互连层的功能主要由 IP 来提供，主要用于负责 IP 寻址、路由选择和 IP 数据包的分割和组装。

IP 的基本任务是通过互连网传送数据报，各个 IP 数据报之间是相互独立的。主机上的 IP 层向传输层提供服务。IP 从源传输实体取得数据，通过它传给目的主机的 IP 层。IP 不保证服务的可靠性，在主机资源不足的情况下，它可能丢弃某些数据报，同时 IP 也不检查被丢弃的报文。

在传送时，高层协议将数据传给 IP，IP 再将数据封装为互连网数据报，并交给主机—网络层协议通过局域网传送。若目的主机直接连在本网中，IP 可直接通过网络将数据报传给目的主机；若目的主机在远地网络中，则 IP 路由器传送数据报，而路由器则依次通过下一网络将数据报传送到目的主机或再下一个路由器。也即一个 IP 数据报是通过互连网络，从一个 IP 模块传到另一个 IP 模块，直到终点为止。

IP 协议提供了不可靠的、无连接的数据报传输机制。TCP/IP 是为了适应物理网络的多样性而设计的，而这种适应性主要是通过 IP 层来体现的。由于物理网络的多样性，各种物理网络的数据帧格式、地址格式之间的差异很大。为了将这些底层的细节屏蔽起来，使得采用不同物理网络的网络之间进行通讯，TCP/IP 分别采用了 IP 数据报和 IP 地址作为物理数据帧与物理地址的统一描述形式。这样 IP 向上层提供统一的 IP 数据报和统一的 IP 地址，使得各种物理帧及物理地址的差异性对上层协议不复存在。

1. IP 数据报头

一个 IP 数据报由一个头部和数据部分构成。头部包括一个 20 字节的固定长度部分和一个可选任意长度部分。头部格式如图 5-16 所示, 各部分介绍如下。

(1) 版本: 4 位。记录了数据报对应的协议版本号。当前的 IP 协议有两个版本: IPV4 和 IPV6。

(2) IHL: 4 位。代表头部的总长度, 以 32 位字节为一个单位。

(3) 服务类型: 8 位。使主机可以告诉子网它想要什么样的服务。

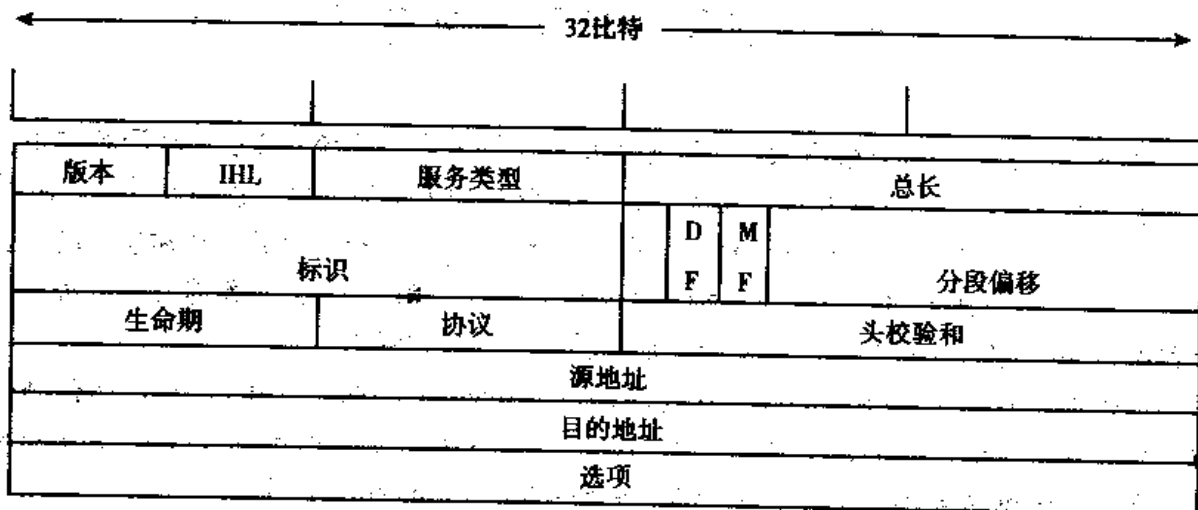


图 5-16 IP 头结构图

(4) 总长: 16 位。指头部和数据的总长。最大长度是 65535 个字节。

(5) 标识: 16 位。通过它使目的主机判断新来的分段属于哪个分组, 所有属于同一分组的分段包含同样的标识值。

(6) DF: 代表不要分段。它命令路由器不要将数据报分段, 因为目的端不能重组分段。

(7) MF: 代表还有进一步的分段, 用它来标志是否所有的分段都已到达。除了最后一个分段的所有分段都设置了这一位。

(8) 分段偏移: 13 位。标明分段在当前数据报的什么位置。

(9) 生命期: 8 位。用来限制分组生命周期的计数器。它在每个节点中都递减, 而且当在一个路由器中排队时可以倍数递减。

(10) 协议: 8 位。说明将分组发送给那个传输进程, 如 TCR、VDP 等。

(11) 头校验和: 16 位。仅用来校验头部。

(12) 源地址: 32 位。产生 IP 数据报的源主机 IP 地址。

(13) 目的地址: 32 位。IP 数据报的目的主机的 IP 地址。

(14) 选项: 是变长的。每个可选项用一个字节标明内容。有些可选项还跟有一字节的可选项长度字段, 其后是一个或多个数据字节。现在已定义了安全性、严格的源路由选择、宽松的源路由选择、记录路由和时间标记五个可选项。但不是所有的路由器都支持全部 5 个可选项。

安全性选项说明了信息的安全程度。

严格的源路由选择选项以一系列的 IP 地址方式, 给出了从源到目的地的完整路径。数

据报必须严格地从这条路径传送。当路由选择表崩溃，系统管理员发送紧急分组时，或作时间测量时，此字段很有用。

宽松的源路由选择选项要求分组遍及所列的路由器，但它可以在其间穿过其它的路由器。

记录路由选项让沿途的路由器都将其 IP 地址加到可选字段之后，这使系统管理者可以跟踪路由选择算法的错误。

时间标记选项像记录路由选项一样，除了记录 32 位的 IP 地址外，每个路由器还要记录一个 32 位的时间标记。同样地，这一选择可用来为路由选择算法查错。

2. IP 数据报的分段与重组

IP 数据报是通过封装为物理帧来传输的。由于因特网是通过各种不同物理网络技术互连起来的，在因特网的不同部分，物理帧的大小（最大传输单元 MTU）可能各不相同。为了最大程度的利用物理网络的能力，IP 模块以所在的物理网络的 MTU 作为依据，来确定 IP 数据报的大小。当 IP 数据报在两个不同 MTU 的网络之间传输时，就可能出现 IP 数据报的分段与重组操作。

在 IP 头中控制分段和重组的 IP 头域有三个：标识域、标志域、分段偏移域。标识是源主机赋予 IP 数据报的标识符。目的主机根据标识域来判断收到的 IP 数据报分段属于哪一个数据报，以进行 IP 数据报重组。标志域中的 DF 位标识该 IP 数据报是否允许分段。当需要对 IP 数据报进行分段时，如果 DF 位置 1，网关将会抛弃该 IP 数据报，并向源主机发送出错信息。标志域中的 MF 位标识该 IP 数据报分段是否是最后一个分段。分段偏移域记录了该 IP 数据报分段在原 IP 数据报中的偏移量。偏移量是 8 字节的整数倍。分段偏移域被用来确定该 IP 数据报分段在 IP 数据报重组时的顺序。

IP 数据报在被传输过程中，一旦被分段，各段就作为独立的 IP 数据报进行传输，在到达目的主机之前有可能会被再次或多次分段。但是 IP 数据报分段的重组都只在目的主机进行。

3. IP 对输入数据报的处理

IP 对输入数据报的处理分为两种：一种是主机对数据报的处理；另一种是网关对数据报的处理。

当 IP 数据报到达主机时，如果 IP 数据报的目的地址与主机地址匹配，IP 接收该数据报并将它传给高级协议软件处理；否则抛弃该 IP 数据报。

网关则不同，当 IP 数据报到达网关 IP 层后，网关首先判断本机是否是数据报到达的目的主机。如果是，网关将接收到的 IP 数据报上传给高级协议软件处理。如果不是，网关将对接收到的 IP 数据报进行寻径，并随后将其转发出去。

4. IP 对输出数据报的处理

IP 对输出数据报的处理也分为两种：一种是主机对数据报的处理；另一种是网关对数据报的处理。

对于网关来说，IP 接收到 IP 数据报后，经过寻径，找到该 IP 数据报的传输路径。该路径实际上是全路径中的下一个网关的 IP 地址。然后，该网关将该 IP 数据报和寻径到的下一个网关的地址交给网络接口软件。网络接口软件收到 IP 数据报和下一个网关地址后，首先调用 ARP 完成下一个网关 IP 地址到物理地址的映射，然后将 IP 数据报封装成帧，最后由子

网完成数据报的物理传输。

通常我们所说的 IP 地址可以理解为符合 IP 协议的地址。目前,我们常用的 IP 协议是 IP 协议的第四版本,即 IPv4,是互联网中最基础的协议,于 1981 年在 RFC 791 中定义。IPv4 使用了 32 位地址,通常使用圆点分隔的 4 个十进制数字表示,比如 192.168.0.1。目前,IPv4 最多支持 2^{32} (2 的 32 次方) 个地址连接到 Internet。随着互联网的迅猛发展,IP 地址的需求越来越大,在未来几年有被用完的危机。

5.6.2 ARP 协议与 RARP 协议

1. 地址转换协议 ARP

在 TCP/IP 网络环境下,每个主机都分配了一个 32 位的 IP 地址,这种互联网地址是在网际范围标识主机的一种逻辑地址。为了让报文在物理网上传送,必须知道彼此的物理地址。这样就存在把互联网地址变换为物理地址的地址转换问题。以以太网 (Ethernet) 环境为例,为了正确地向目的站传送报文,必须把目的站的 32 位 IP 地址转换成 48 位以太网目的地址 DA。这就需要在互连层有一组服务将 IP 地址转换为相应物理网络地址,这组协议即是 ARP。

在进行报文发送时,如果源互连层所给的报文只有 IP 地址,而没有对应的以太网地址,则互连层广播 ARP 请求以获取目的站信息,而目的站必须回答该 ARP 请求。这样源站点可以收到以太网 48 位地址,并将地址放入相应的高速缓存 (Cache)。下一次源站点对同一目的站点的地址转换可直接引用高速缓存中的地址内容。地址转换协议 ARP 使主机可以找出同一物理网络中任一物理主机的物理地址,只需给出目的主机的 IP 地址即可。这样,网络的物理编址可以对网络层服务透明。

在互联网环境下,为了将报文送到另一个网络的主机,数据报先定向到发送方所在网络的 IP 路由器。因此,发送主机首先必须确定路由器的物理地址,然后依次将数据报发往接收端。除基本 ARP 机制外,有时还须在路由器上设置代理 ARP,其目的是由 IP 路由器代替目的站对发送方 ARP 请求做出响应。

2. 反向地址转换协议 RARP

反向地址转换协议用于一种特殊情况,如果站点初始化以后,只有自己的物理网络地址而没有 IP 地址,则它可以通过 RARP 协议,发出广播请求,征求自己的 IP 地址,而 RARP 服务器则负责回答。这样,无 IP 地址的站点可以通过 RARP 协议取得自己的 IP 地址,这个地址在下次系统重新开始以前都有效,不用连续广播请求。RARP 广泛用于获取无盘工作站的 IP 地址。

5.6.3 ICMP 协议

互联网控制报文协议 ICMP。从 IP 互联网协议的功能,可以知道 IP 提供的是一种不可靠的无连接报文分组传送服务。若路由器或主机故障使网络阻塞,就需要通知发送主机采取

相应措施。

为了使互联网能报告差错,或提供有关意外情况的信息,在 IP 层加入了一类特殊用途的报文机制,即互联网控制报文协议 ICMP。

分组接收方利用 ICMP 来通知 IP 模块发送方某些方面所需的修改。ICMP 通常是由发现别的站发来的报文有问题的站产生的,例如可由目的主机或中继路由器来发现问题并产生有关的 ICMP。如果一个分组不能传送,ICMP 便可以被用来警告分组源,说明有网络、主机或端口不可达。ICMP 也可以用来报告网络阻塞。ICMP 是 IP 正式协议的一部分,ICMP 数据报通过 IP 送出,因此它在功能上属于网络第三层,但实际上它是像第四层协议一样被编码的。

5.6.4 IGMP 协议

通常的 IP 通信是在一个发送方和一个接受方之间进行的,称为单播 (Unicast)。局域网中可以实现对所有网络节点的广播 (Broadcast)。但对于有些应用,需要同时向大量接受者发送信息,比如说应答的更新复制、分布式数据库、为所有经纪人传递股票交易信息,以及多会场的视频会议等。这些应用的共同特点就是一个发送方对应多个接受方,接受方可能不是网络中的所有主机,也可能没有位于同一子网。这种通信方式介于单播和广播之间,被称为组播或多播 (Multicast)。

IP 采用 D 类地址来支持多播,每个 D 类地址代表一组主机。共有 28 位可用来标识主机组 (Host Group),因此可以同时有多达 2 亿 5 千万个多播组。当一个进程向一个 D 类地址发送报文时,就是同时向该组中的每个主机发送同样的数据,但网络只是尽最大的努力将报文传送给每个主机,并不能保证全部送达,有些组内主机可能收不到这个报文。

因特网支持两类组地址:永久组地址和临时组地址。

(1) 永久组不必创建而且总是存在的,每个永久组有一个永久组地址。例如:224.0.0.1 代表局域网中所有的系统;224.0.0.2 代表局域网中所有的路由器;224.0.0.5 代表局域网中所有的 OSPF 路由器。

(2) 临时组在使用前必须先创建,一个进程可以要求其所在的主机加入或退出某个特定的组。当主机上的最后一个进程脱离某个组后,该组就不再在这台主机中出现。每个主机都要记录它的进程当前属于哪个组。

多播需要特殊的多播路由器支持,多播路由器可以兼有普通路由器的功能。因为组内主机的关系是动态的,因此本地的多播路由器要周期性地对本地网络中的主机进行轮询(发送一个目的地址为 224.0.0.1 的多播报文),要求网内主机报告其进程当前所属的组,各主机会将其感兴趣的 D 类地址返回,多播路由器以此决定哪些主机留在哪个组内。若经过几次轮询在一个组内已经没有主机是其中的成员,多播路由器就认为该网络中已经没有主机属于该组,以后就不再向其它的多播路由器通告组内成员的状况。

多播路由器和主机间的询问和响应过程使用因特网组管理协议 (Internet Group Management Protocol, IGMP) 进行通信。IGMP 类似于 ICMP,但只有两种报文:询问和响应,都有一个简单的固定格式,其中数据字段中的第一个字段是一些控制信息,第二个字段是一个 D 类地址。IGMP 使用 IP 报文传递其报文,具体做法是 IGMP 报文加上 IP 报文头部构成 IP 报文进行传输,但 IGMP 也向 IP 提供服务。通常不把 IGMP 看作一个单独的协议,而是看做整

个互连网络协议 IP 的一个组成部分。

为了适应交互式音频和视频信息的多播, Internet 上从 1992 年开始试验虚拟的多播主干网 (Multicast Backbone On the Internet, MBONE)。MBONE 可以将报文传播给不在一起但属于一个组的许多个主机。在 MBONE 中具有多播功能的路由器称为多播路由器 (Multicast Router, MRouter), 多播路由器既可以是一个单独的路由器, 也可以是运行多播软件的普通路由器。

尽管 TCP/IP 中的多播已经成为标准, 但在多播路由器中路由信息的传播尚未标准化。目前正在进行实验的是距离向量多播路由协议 (Distance Vector Multicast Routing Protocol, DVMRP)。DVMRP 的路由选择是通过生成树实现的, 每个多播路由器采用修改过的距离矢量协议与相邻的多播路由器交换信息, 以便每个路由器为每个多播组构造一个覆盖所有组成员的生成树。在修剪生成树及删除无关路由器和网络时, 用到了很多优化方法。

若多播报文在传输过程中遇到不支持多播的路由器或网络, 就要用隧道 (Tunneling) 技术来解决, 即将多播报文再次封装为普通报文进行单播传输, 在到达另外一个支持多播的路由器后再解除封装恢复为多播报文继续传输。

5.6.5 IPv6

IP 协议是因特网中的关键协议。现在广泛使用的 Ipv4 是在 20 世纪 70 年代末期设计的, 无论从计算机技术的发展还是从因特网的规律和网络的传输速率来看, Ipv4 都已经不适用了。其中最主要的问题就是 32 比特的 IP 地址空间已经无法满足迅速膨胀的因特网规模。为此, IETF 在 1992 年 6 月就提出要制订下一代的 IP (IP Next Generation, IPNG)。由于此前已经推出 Ipv5, 但未获广泛认同和应用, 因此 Ipv6 最后正式定名为 Ipv6。

Ipv6 的主要目标包括:

- 扩大 IP 地址空间, 即使地址利用率不高, 也能支持上百亿台主机。
- 减小路由选择表的长度, 提供路由选择速度。
- 简化协议, 使路由器处理分组更迅速。
- 提供更好的安全性。
- 增加对服务类型的支持, 特别是实时的多媒体数据。
- 通过定义范围来支持多点播送的实现。
- 主机可以在不改变其 IP 地址的情况下实现漫游。
- 协议保留未来发展的余地。
- 允许新旧协议共同存在一个时期。

1995 年以后 IETF 陆续公布了一系列有关 Ipv6 的协议、编址方法、路由选择以及安全等问题的 RFC 文档。Ipv6 所引进的主要变化如下:

- Ipv6 把 IP 地址长度增加到 128 比特, 使地址空间增大了 2^{96} 倍。它可以为地球上每平方米的面积分配一千多个 IP 地址, 这个近似无限的地址空间可以保证 IP 地址的分配不会再出现过去的窘迫局面。

- 灵活的 IP 报文头部格式。Ipv6 采用一种全新的报文格式, 使用一系列固定格式的扩展头部取代了 Ipv4 中可变长度的选项字段。Ipv6 中选项部分的出现方式也有所变化, 使路

由器可以简单跳过选项而不做任何处理,加快了报文处理速度。

- 简化协议,加快报文转发。Ipv6 简化了报文头部格式,将字段从 Ipv4 的 13 个减少到 7 个,报文分段也只是在源主机进行,这些简化使路由器可以更快地完成对报文的处理和转发,提高了吞吐量。

- 提高安全性。鉴于 Ipv4 中出现的种种安全问题,Ipv6 全面考虑和支持协议的安全功能。身份认证和隐私权是 Ipv6 的关键特性。

- 支持更多的服务类型。如支持对网络资源的预分配,以实现实时视频传输等要求保证一定带宽和时延的应用。

- 允许协议继续演变,增加新的功能,使之适应未来技术的发展。

习 题

1. 网络层实现的功能主要有哪些?

2. 虚电路中的“虚”是什么含义?如何区分一个网络节点所处理的多个虚电路?

3. 简述虚电路操作与数据报操作的特点、虚电路服务与数据报服务的特点。

4. 考虑下面虚电路服务实现涉及的设计问题。如果虚电路用在子网内部,每个数据报文必须有一个 3 字节的报文;每个路由器必须留有 8 字节的空间来标识虚电路。如果内部使用数据报,则需要使用一个 15 字节的分组头。假定每站段传输带宽的费用为每 10^6 字节 1 元人民币;路由器存储器的价格为每字节 0.1 元人民币,并且在未来两年会下降。平均每次会话长度为 1000 秒,传输 200 分组;分组平均需传 4 个站段。试问子网内部采用虚电路或数据报哪个更便宜?便宜多少?

5. 考虑图 5-5 (a) 中的子网。该子网使用了距离矢量路由算法,下面的矢量刚刚到达路由器 C,来自 B 的矢量为 (5, 0, 8, 12, 6, 2);来自 D 的矢量为 (16, 12, 6, 0, 9, 10);来自 E 的矢量为 (7, 6, 3, 9, 0, 4) 经测量,到 B、D 和 E 的延迟分别为 6、3 和 5。请问 C 的新路由表将会怎么样?请给出将使用的输出线路以及期望(预计)的延迟。

6. 假定所有的路由器和主机都正常工作,路由器和主机的软件都没有错误。问:有没有可能(无论可能性多小)把一个分组递交到错误的目的地?

7. 考虑图 5-2 (a) 中的子网,采用:(1) 反向路径转发;(2) 汇集树。从 B 广播,分别可形成多少个分组?

8. 计算如图 5-8 (a) 所示子网中路由器的一个多点播送生成树。

9. 什么叫拥塞?造成拥塞的原因是什么?

10. 简述防止拥塞的几种方法。

11. 网络互连设备按其工作的层次可分为几类?它们分别是什么?网际互连的意义是什么?请列出各种网络互连设备及它们工作的 OSI 协议层。

12. 简述透明网桥的工作原理。

13. 比较透明网桥和源端路由网桥各自的优缺点。

14. 一台主机的 RIP 协议可以是主动方式的吗?说明理由。

15. 简述 ARP 协议和 RARP 协议的要点。

16. 多播和广播有何异同?若要路由器支持多播,还需要添加哪些功能?

17. 与 IPv4 相比,IPv6 有哪些改进?

18. IPv6 有哪些特点?下一代网络为什么要使用 IPv6?

第6章 传输层

传输层是整个协议层次结构的核心，其功能是从源主机到目的主机提供可靠的、价格低廉的数据传输，而与当前网络或使用的网关无关。本章首先介绍传输层的基本概念，包括：传输层提供给高层的服务、传输层的两种连接方式、特别应明确传输层的寻址与网络层的寻址的区别；然后着重介绍因特网的两种传输协议 TCP 和 UDP，详述了针对上述两种传输层协议的两种连接管理——面向连接和无连接的概念；另外介绍了传输层对拥塞的控制。

6.1 传输层基本概念

第五章介绍的网路层的主要功能之一是路由的选择，网络中传输的数据经过网络层可以做到从源主机到目的主机。那么，传输层在寻址这一功能中又起到什么作用呢？传输层的最终目标是向用户或者说是向应用程序的进程，提供有效、可靠且最佳的服务。要了解传输层的功能首先要清楚传输层及应用层之间的关系。

6.1.1 传输服务

传输层位于网络层与应用层之间，传输层利用网络层提供的服务，向应用层提供服务。

1. 传输实体

传输层中完成向应用层提供服务的硬件和（或）软件称为传输实体（Transport Entity）。传输实体可能存在于下列软、硬件环境中：

- 操作系统的内核中。
- 一个单独的用户进程内。
- 网络应用的程序库中。
- 网络接口卡上。

2. 传输层提供给应用层的服务

传输层的最终目标是向其用户（或是指应用层的进程）提供有效、可靠且价格合理的服务。为了达到这一目标，传输层利用网络层提供的服务。

（1）网络层、传输层和应用层的逻辑关系。网络层、传输层和应用层的逻辑关系如图 6-1 所示。图中的 TPDU（Transport Protocol Data Unit）是传输协议数据单元。

网络层是通信子网的最高层，无法保证通信子网或路由器提供的面向连接的服务可靠，

而用户一般不能直接对通信子网加以控制，因此在网络层之上，加一层传输层以改善传输质量。有了传输层后，应用于各种网络的应用程序就能够通过采用一个标准的原语集来编写，而不必担心不同的子网接口和不可靠的数据传输。传输层起着将通信子网的技术、设计和各种缺欠与上层相隔离的关键作用。

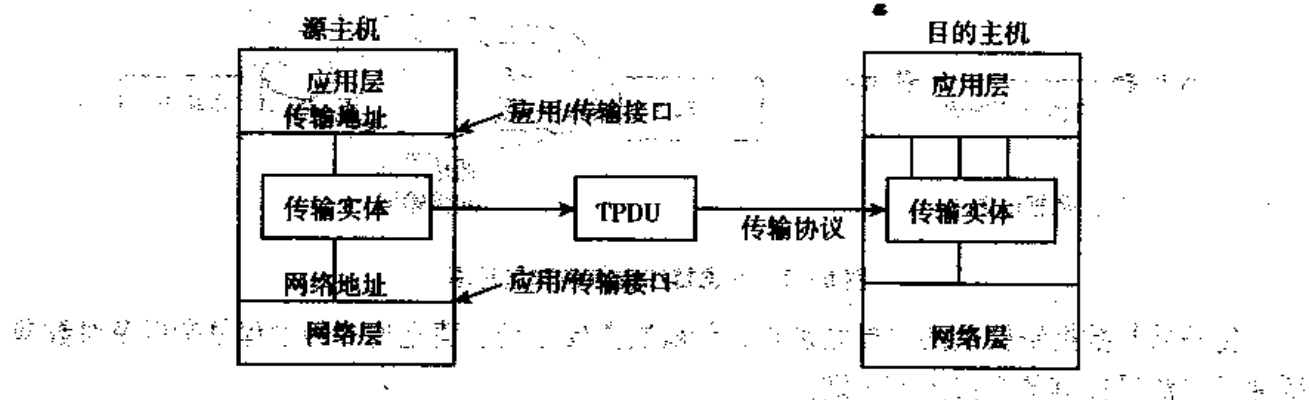


图 6-1 网络层、传输层和应用层的逻辑关系

(2) 网络地址与传输地址的关系。通过图 6-2 可以进一步理解网络地址与传输地址的关系。

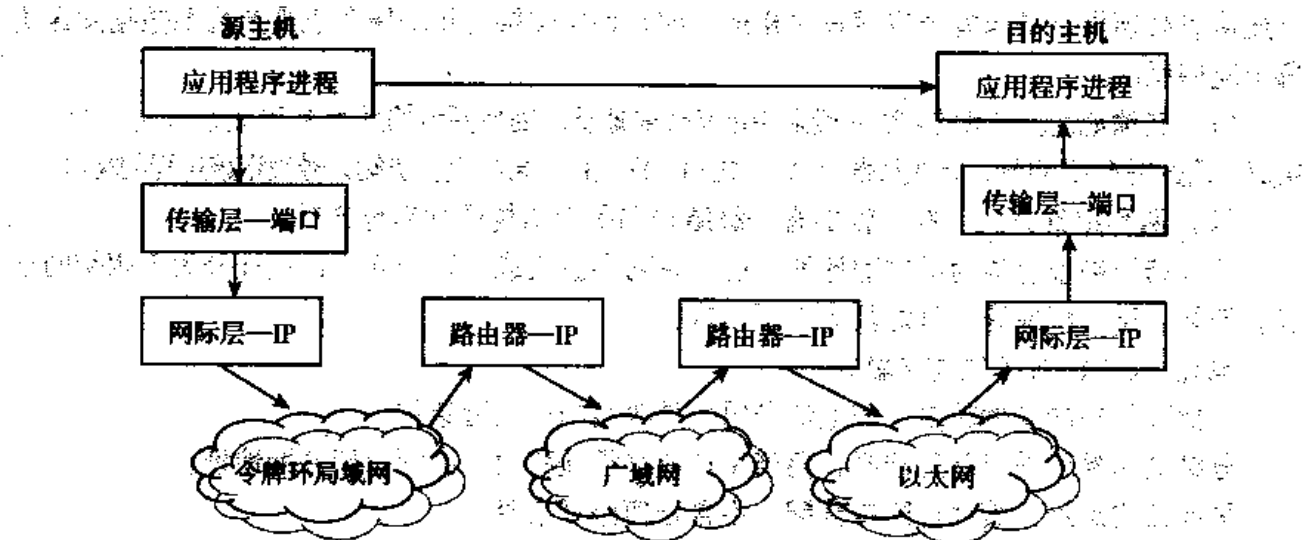


图 6-2 传输层与网际层地址比较

从图 6-2 可以看出，网际层地址是 IP 地址，即可以到达主机的地址；而传输层地址是主机上的某个进程使用的端口的地址。

关于端口的规定，在后面介绍传输层协议时详细介绍。

(3) 两种传输服务。传输层的传输服务根据不同的协议分为面向连接与非连接的两种类型。所谓面向连接是发送方与接收方传输服务需要经过建立连接，然后再传输数据，最后释放连接 3 个过程。而对于非连接的传输服务，发送方无须事先建立连接，只要有数据需要发送，就直接发送。

6.1.2 传输协议的要素

传输服务是通过建立连接的两个传输实体之间所采用的传输协议来实现的。在某些方面，传

传输层协议与数据链路层协议有相似的地方。表现在两者都必须解决差错控制、分组顺序、流量控制及其它问题。而两者最大的差异是两层的协议所运行的环境不同，由此而带来的不同。数据链路层是两个相邻节点间数据的传输，传输层的传输双方是通过通信子网进行数据的传输，这一环境的差异对协议产生了很多重要影响。数据链路层与传输层传输环境如图 6-3 所示。



图 6-3 数据链路层与传输层环境

传输层与数据链路层的主要区别是：传输层需要寻址、建立连接的过程复杂以及对数据缓冲区与流量控制的方法上的区别。

1. 寻址

当一个应用程序希望与另一个应用程序传输数据时，如果是面向连接的传输服务，在建立连接时必须指定是与哪个应用程序相连，如果是非连接的传输服务也需要指明数据发送给哪个应用程序。

(1) 传输地址。寻址的方法一般采用定义传输地址。因特网传输地址由 IP 地址和主机端口号组成。通过图 6-2 可知，首先按照 IP 地址找到目标主机，再根据主机端口号确定该进程的端口。

(2) 两种编址方式。在传输层有分级结构和平面结构两种编址方式。

分级结构编址也称为层次型地址，由一系列字段组成，这些字段将地址分为不相交的分区。例如，层次型地址有可能具有以下结构：

地址 = 国家/网络/主机/端口

层次型结构的实例较多，如电话号码就是典型的层次型结构。

分级结构易于进行路径选择，但当用户或进程迁移时，必须重新分配地址。

平面结构编址，其地址随机分配，不含任何路径信息。

2. 建立连接

要保证建立起可靠的连接并非是一件容易的事，问题的复杂性体现在如何确认可靠的连接已经建立起来了。在实际的网络应用中，采用一种称为三次握手的算法，并增加某些条件来解决最后确认问题。

增加的条件是所发送的报文都要有递增的序列号；对每个报文都设立一个计时器，设定一个最大时延，对那些超过最大时延仍没有收到确认信息的报文就认为已经丢失。

三次握手算法的工作原理是：发送方向接收方发送建立连接的请求报文，接收方向发送方回应一个对建立连接请求报文的确认报文，发送方再向接收方发送一个对确认报文的确认报文。

在三次握手算法的基础上，加上增加的条件，就可以建立可靠的连接了。

3. 释放连接

释放连接仍然采用和建立连接相类似的三次握手的方法。但释放连接有对称释放和非对

称释放两种方式。

(1) 对称释放方式。对称释放方式在两个方向上分别释放连接，一方释放连接后，只是不能发送数据，可以继续接收数据。这种方式适合于每个进程有固定数量的数据需要发送并确切知道何时发送完毕的情况。

(2) 非对称释放方式。非对称释放方式是当一方释放连接时，两个方向的连接都会被释放。如电话系统，当一方挂机后，连接即被中断。非对称释放很突然，可能会导致数据丢失，不适于在传输层使用。

6.1.3 传输层在 OSI 中的地位和作用

OSI 七层模型中的物理层、数据链路层和网络层是面向网络通信的低三层协议，为网络环境中的主机提供点对点通信服务。传输层提供应用进程端到端的进程通信服务，既是七层模型中负责数据通信的最高层，又是面向网络通信的低三层和面向信息处理的高三层之间的中间层。传输层位于网络层之上、会话层之下，在网络分层结构中起着承上启下的作用。它利用网络层子系统提供给它的服务去开发本层的功能，并实现本层对会话层的服务。

传输层是 OSI 七层模型中最重要最关键的一层，是惟一负责总体数据传输和控制的一层。传输层的两个主要目的是：第一，提供可靠的端到端的通信；第二，向会话层提供独立于网络的传输服务。

在讨论为实现这两个目标所应具有的功能之前，先考察一下传输层所处的地位。首先，传输层之上的会话层、表示层及应用层均不包含任何数据传输的功能，而网络层又不一定需要保证发送站的数据可靠地送至目的站；其次，会话层不必考虑实际网络的结构、属性、连接方式等实现的细节。

根据传输层在七层模型中的地位，它的主要功能是：对一个进行的对话或连接提供可靠的传输服务，在通向网络的单一物理连接上实现该连接的复用，在单一连接上提供端到端的序号与流量控制、端到端的差错控制及恢复等服务。

传输层反映并扩展了网络层子系统的服务功能，并通过传输层地址提供给高层用户传输数据的通信端口，使系统间高层资源的共享不必考虑数据通信方面的问题。

6.2 传输控制协议

传输控制协议 TCP 是用于在不可靠的因特网上提供可靠的、端到端的字节流通信的协议。

6.2.1 TCP 服务模型

TCP 提供的服务具有以下主要特征：

- (1) 面向连接的传输，传输数据前需要先建立连接，数据传输完毕要释放连接。
- (2) 端到端通信，不支持广播通信。

(3) 高可靠性, 确保传输数据的正确性, 不出现丢失或乱序。

(4) 全双工方式传输。

(5) 采用字节流方式, 即以字节为单位传输字节序列。如果字节流太长, 将其分段。

(6) 提供紧急数据传送功能, 即当有紧急数据需要发送时, 发送进程会立即发送, 接收方收到后会暂停当前工作, 读取紧急数据并做相应处理。

6.2.2 TCP 数据传输机制

1. TCP 的段结构

因为 TCP 是应用于大数据量传输的情况, 所以需要将长的数据流分段, TCP 的段结构如图 6-4 所示。

TCP 地址与 IP 地址不同, IP 地址是字节地址, 一个节点可以运行多个应用, TCP 的地址是节点的某个应用的地址, 这种应用在计算机内部是进程。多个进程的数据传递通过不同的端口完成, 因此在 TCP 段结构中, 是以“端口”表示地址的。

源端口		目标端口	
序列号			
确认号			
头长度		标志	窗口
校验和		紧急数据指针	
选项（可变长度）			
数据			

图 6-4 TCP 的段结构

(1) 源端口: 16 比特, 源节点进程端口。

(2) 目标端口: 16 比特, 目标节点端口。

(3) 序列号: 32 比特, TCP 对字节流中的每个字节都编号。假设每个数据段包含 1000 个数据字节, 第一个字节的编号为 X , 则对于字节流中各段的第一个字节的序列号分别为: X , $X+1000$, $X+2000$ 等。

(4) 确认号: 32 比特, 为准备接收的字节序列号, 即意味着该字节序列号前的字节都已正确接收。

(5) 头长度: 4 比特, 随可变长度选项的改变而改变, 接收方可根据该数据确定 TCP 的数据的起始位置。

(6) 标志: 6 比特, 该字段包含对其它字段的说明或对控制功能的标志。具体的设置如下。

ACK——说明确认字段中的数据有意义。

URG——说明紧急数据指针字段中的数据有意义。

FIN——标志是最后的 TCP 数据段, FIN 也称为“完成”。

PSH——指出接收方不必等待一定量的数据再向应用提供数据 (一般情况是等待一定量再提供), 而是立即提供该数据段, PSH 也称为“推”。

RST——在有异常情况发生时, 发送方通知接收方暂时终止连接, 释放与连接有关的缓冲区, 中断 TCP 传输, RST 也称为“复位”。

SYN——在建立初始连接时, 允许双方共同确定初始序列号, SYN 也称为“同步”。

(7) 窗口: 16 比特, 通知接收方还可以发送的数据字节数 (因为是全双工通信), 接

收方可以根据该值改变其发送窗口的大小。

(8) 校验和: 16 比特, 进行传输层的差错校验, 具体算法是将 TCP 段的内容转换成一系列的 16 比特的整数, 并相加。

(9) 紧急数据指针: 16 比特, 当标志字段中的值为 URG 时, 表示有紧急数据, 紧急数据位于段的开始, 紧急数据指针指向紧挨着紧急数据后的第一个字节, 以区分紧急数据和非紧急数据。对于紧急数据接收方必须尽快送给高层应用。

(10) 选项: 可变长度, 选项一般包含两个内容, 一是在通信双方容量相差很大时, 必须在初始建立连接时, 确定可接收的段的最大尺寸; 另一个是在使用高带宽线路传输大型文件时, 允许用 16 比特来代替 32 比特的窗口字段。需要注意的是, 利用填充选项字段, 以保证 TCP 段的头尺寸是 4 字节的整数倍。

(11) 数据: 可变大小, 用户提供的数据。

2. TCP 端口号

TCP 段结构中端口地址是 16 比特, 可以有在 0 ~ 65535 范围内的端口号。对于这 65536 个端口号有以下的使用规定。

(1) 端口号小于 256 的定义为常用端口, 服务器一般都是通过常用端口号来识别的。任何 TCP/IP 实现所提供的服务都用 1 ~ 1023 之间的端口号。这些端口号由 Internet 端口号分配机构 (Internet Assigned Numbers Authority, IANA) 来管理。

(2) 客户端通常对他所使用的端口号并不关心, 只需保证该端口号在本机上是惟一的就可以了。客户端端口号因存在时间很短暂又称作临时端口号。

(3) 大多数 TCP/IP 实现给临时端口分配 1024 ~ 5000 之间的端口号。大于 5000 的端口号是为其它服务器预留的 (Internet 上并不常用的服务)。

常用的 TCP 协议所使用的端口如表 6-1 所示。

表 6-1 常用的 TCP 协议所使用的端口

协议名称	协议内容	所使用的端口号
FTP (控制)	文件传输服务	21
FTP (数据)		20
TELNET	远程登录	23
HTTP	超文本传送协议	80
Gopher	菜单驱动信息检索	70
SMTP	简单邮件传送协议	25
POP3	接收邮件 (与 SMTP 对应)	110

6.2.3 TCP 连接管理

TCP 传输控制协议是面向连接的控制协议, 即在传输数据前要先建立逻辑连接, 数据传输结束还要释放连接。这种建立、维护和释放连接的过程, 就是连接管理。

1. 连接建立

TCP 连接的建立采用三次握手协议。三次握手的具体过程是：第一方向另一方发送连接请求段，另一方回应对连接请求的确认段，第一方再发送对对方确认段的确认。这个过程可以用图 6-5 表示。

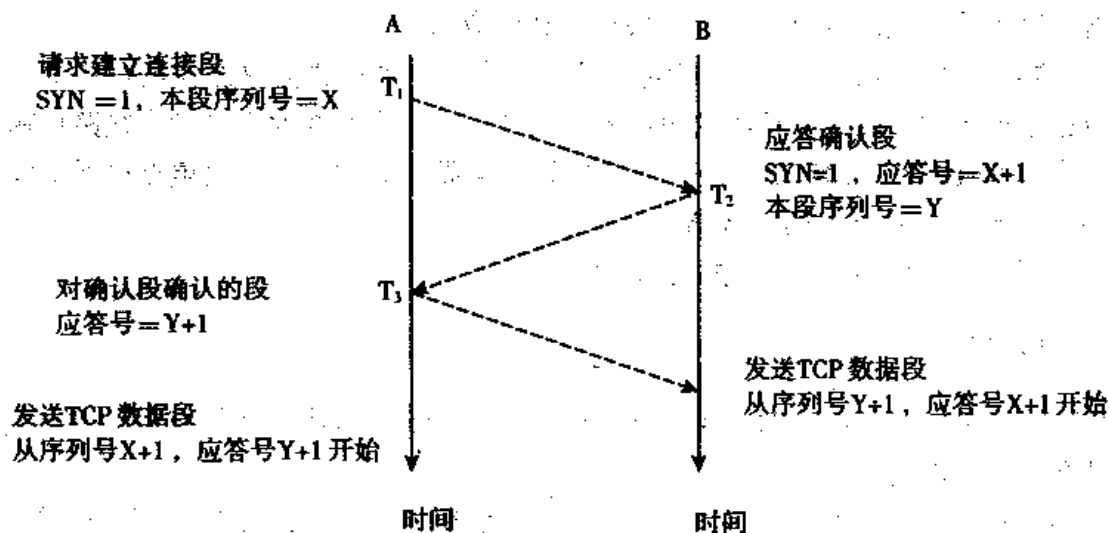


图 6-5 TCP 建立连接的过程

图 6-5 中，SYN 为请求建立连接的标志，三次握手过程如下：

在 T_1 时刻，A 向 B 发送请求建立连接段，序列号为 X 。

在 T_2 时刻，B 发送应答 A 的 X 序列号的请求建立连接的段，该应答段的序列号为 Y 。

在 T_3 时刻，A 发送对 B 的应答段的应答，应答号为 $Y+1$ ，表明应答号为 Y 的段已接收。

至此，连接建立成功，A、B 分别发送数据段，序列号分别是 $X+1$ 、 $Y+1$ ，应答号分别是 $Y+1$ 、 $X+1$ 。

2. 连接释放

因为是双工通信，一方的数据段发送完毕要终止连接时，另一方不一定也发送完数据段。因此，TCP 连接释放采用对称释放方式。连接释放的过程同样采取三次握手的协议。连接释放的三次握手的示意图如图 6-6 所示。

在图 6-6 中，FIN 为终止标志，释放连接的过程如下：

- A 在 T_1 时刻收到应用层的终止请求，发送释放连接段。
- B 在 T_2 时刻收到 A 发送的释放连接段，发送应答段，确认已经收到该段，并通知应用层 A 已经无数据发送，请求释放连接。
- 此后 B 仍然可以发送数据，但在 T_3 时刻收到无数据传输的通知，向 A 发送释放连接段。
- A 在 T_4 时刻收到 B 的释放连接段，A 向 B 发送应答段，确认已经收到该段，并中断连接。
- 在 T_5 时刻 B 收到 A 的确认，也中断连接。

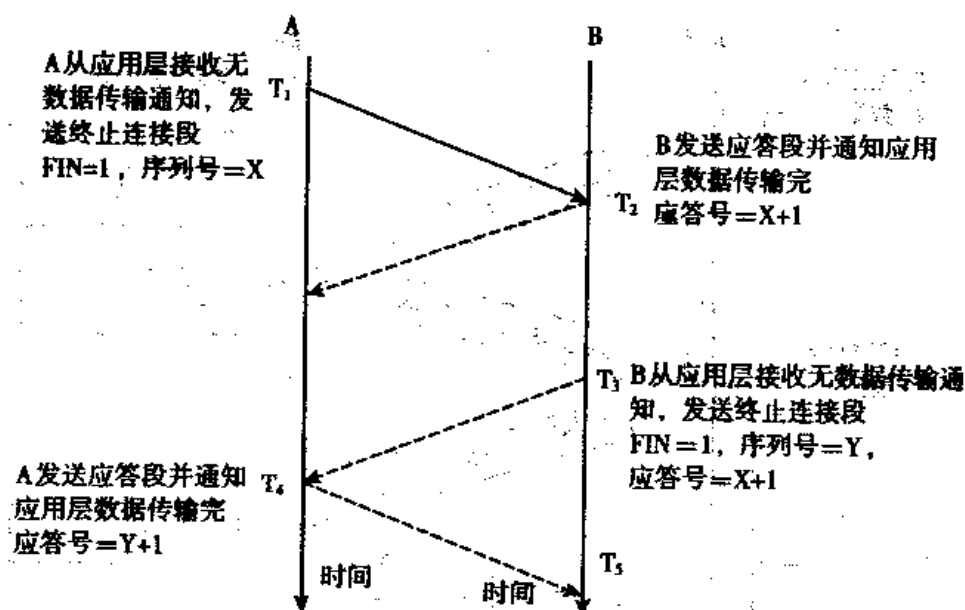


图 6-6 TCP 释放连接的过程

6.2.4 TCP 滑动窗口控制

TCP 中的滑动窗口管理并不直接受制于确认信息。发送方不需要从应用层的数据一到就马上发送, 可以等数据达到一定数量后一起发送。接受方也不用一接收到数据立即发送确认, 可以等待接受的数据达到一定数量后一起发送确认。

TCP 的滑动窗口协议中的接受窗口的大小是随着已经接受的数据量变化的。TCP 滑动窗口的管理如图 6-7 所示。

在图 6-7 所示例中, 假定接受方有 4096 字节的缓冲区。ACK 为将要确认的字节号, 即在此前的字节已经被正确接受; WIN 为可以接收的窗口大小; SEQ 为定序器, 即发送数据段的起始字节号。该例的运行步骤如下:

- 在 T_1 时刻, 发送方的应用写入 2048 字节的数据, 发送数据段的起始字节号为 0。
- 在 T_2 时刻, 接受方接收到发送方的数据段后, 在没有交给应用层前, 缓冲区被占用 2K, 还剩下 2K, 接收方向发送方发确认段, $ACK=2048$, $WIN=2048$ 。
- 在 T_3 时刻, 发送方收到应用层写入的 3K 字节的数据, 但因接受方的缓冲区只剩下 2K, 因此发送 2K 的数据段, $SEQ=2048$ 。
- 在 T_4 时刻, 接受方接收到发送方的数据段后, 在没有交给应用层前, 缓冲区又被占用 2K, 缓冲区满, 接受方向发送方发确认段, $ACK=4096$, $WIN=0$, 此时发送方被阻塞。
- 在 T_5 时刻, 接受方向应用层上传一个数据段, 缓冲区被释放 2K 字节, 接受方向发送方发送确认段, 通知发送方有 2048 字节缓冲区, 即 $WIN=2048$ 。
- 在 T_6 时刻, 发送方发送余下的 1K 字节数据段, $SEQ=4096$, 此时, 接受方缓冲区还剩下 1K。

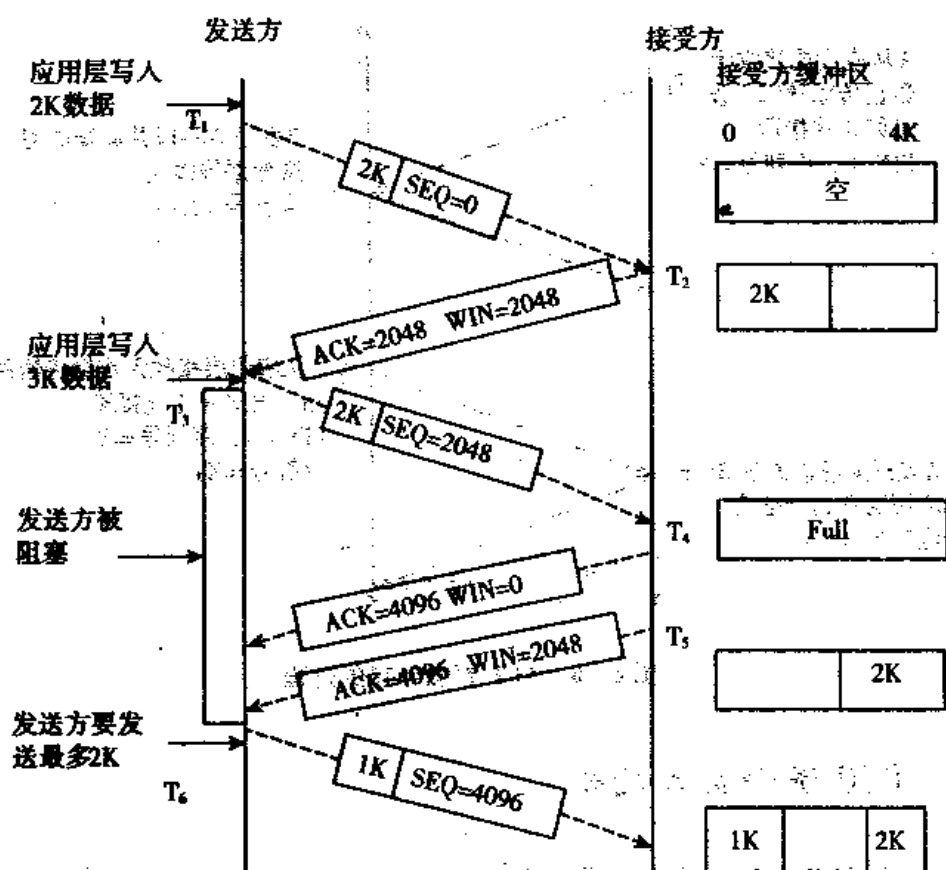


图 6-7 TCP 滑动窗口协议

6.2.5 TCP 重传策略

TCP 协议用于控制数据段是否需要重传的依据是设立重发定时器。在发送一个数据段的同时启动一个重发定时器，如果在定时器超时前收到确认，就关闭该定时器，如果定时器超时前没有收到确认，则重传该数据段。

这种重传策略的关键是对定时器初值的设定。目前采用较多的算法是 Jacobson 于 1988 年提出的一种不断调整超时时间间隔的动态算法。其工作原理是：对每条连接 TCP 都保持一个变量 RTT，用于存放当前到目的端往返所需时间最接近的估计值。当发送一个数据段时，同时启动连接的定时器，如果在定时器超时前确认到达，则记录所需的时间 (M)，并修正 RTT 的值，如果定时器超时前没有收到确认，则将 RTT 的值增加 1 倍。

6.2.6 TCP 拥塞控制

因特网中，对拥塞的控制大部分是由 TCP 来完成，对拥塞控制的最有效的方法是降低数据传输速率。要进行拥塞控制首先要检测到拥塞的发生，由于传输线路质量的提高，由传输错误造成的数据丢失的情况越来越少，因此，因特网上的传输超时大部分是因拥塞造成的。这样，就可以明确地认为，如果出现传输超时就意味着出现了拥塞。

造成拥塞出现，是由网络容量与接受方容量两个方面的问题引起的，需要分别处理。为

此, 发送方除前面讲到的接受方承认的发送窗口外, 增加一个拥塞窗口。每个窗口都反应出发送方能够传输的字节数, 发送方取两个窗口中的最小值作为发送的字节数。

关于发送窗口, 前面已经进行了讲述, 在此不再赘述。下面着重讲述如何确定拥塞窗口的大小。

在刚建立连接时, 将拥塞窗口的大小初始化为该连接所需的最大数据段的长度值, 并发送一个最大长度的数据段 (当然必须是接收窗口允许的)。如果在定时器超时前, 得到确认, 将拥塞窗口的大小增加一个数据段的字节数, 并发送两个数据段, 如果每个数据段在定时器超时前都得到确认, 就再在原基础上增加一倍, 即为 4 个数据段的大小, 如此反复, 每次都在前一次的基础上加倍。当定时器超时或达到发送窗口设定的值时, 停止拥塞窗口尺寸的增加。这种反复称为慢速启动, 所有的 TCP 协议都支持这种方法。

6.3 用户数据报传输协议

用户数据报传输协议 UDP 提供了无连接的数据报服务。

6.3.1 UDP 服务模型

UDP 提供的服务具有以下主要特征:

(1) 传输数据前无须建立连接, 一个应用进程如果有数据报要发送就直接发送, 属于一种无连接的数据传输服务。

(2) 不对数据报进行检查与修改。

(3) 无须等待对方的应答。

(4) 正因为以上的特征, 使其具有较好的实时性, 效率高。

会出现分组丢失、重复、乱序, 应用程序需要负责传输可靠性方面的所有工作。它适用于无须应答并且通常一次只传送少量数据的情况。对于只有一个响应的情况, 采用 UDP 可以避免建立和释放连接段麻烦。

6.3.2 UDP 数据传输机制

1. UDP 的段结构

UDP 功能简单, 它的段结构也简单。UDP 的段结构如图 6-8 所示。

图 6-8 中 UDP 各字段的含义如下:

(1) 源端口——16 比特, 标明发送端地址。

(2) 目的端口——16 比特, 标明接收端地址。

(3) 长度——16 比特, 指明包括 UDP 的头在内的数据段的总长度。

(4) 校验和——16 比特, 该字段是可选项, 当不用时置为全 0。

源端口	目标端口
长度	校验和
数据	

图 6-8 UDP 的段结构

比较图 6-8 与图 6-4, 可以看出 UDP 的段结构比 TCP 的段结构简单, 因此网络开销也小。

2. UDP 的端口号

UDP 的端口号的规定与 TCP 相同, 用于 UDP 的常用端口号如表 6-2 所示。

表 6-2 常用的 UDP 协议的端口号

协议名称	协议内容	所使用的端口号
DNS	域名解析服务	53
SNMP	简单网络管理协议	161
QICQ	聊天软件	8000
TFTP	简单文件传输协议	69

6.3.3 UDP 协议的应用

UDP 协议从问世至今已经被使用了很多年, 虽然其最初的光彩已经被一些类似协议所掩盖, 但是即使是在今天, UDP 仍然不失为一项非常实用和可行的网络传输层协议。

由于 UDP 协议在数据传输过程中无须建立逻辑连接, 对数据包也不进行检查, 因此在优良的网络环境中, 其工作的效率较 TCP 协议要高, 具有 TCP 所望尘莫及的速度优势。这使得在有些情况下, UDP 协议可能会变得非常有用, 仍然继续在主流应用中发挥着作用。包括视频电话会议系统在内的众多的客户/服务器模式的网络应用都需要使用 UDP 协议, 许多应用都证明了 UDP 协议的存在价值。因为相对于可靠性来说, 这些应用更加注重实际性能, 所以为了获得更好的使用效果 (例如, 更高的画面帧刷新速率) 往往可以牺牲一定的可靠性 (例如, 画面质量)。这就是 UDP 和 TCP 两种协议的权衡之处。

传输层介于网络层与高层之间, 它使用网络层的服务并为应用层提供服务。传输层协议的复杂程度取决于网络传输质量和网络层服务的水平, 针对不同的网络质量, 传输层协议分为 0~4 类。传输层功能的实质是最终完成端到端的可靠连接, 在此, 要特别明确“端”是指用户应用程序的“端口”, 即传输层的“地址”要落实到端口号。

习 题

1. 什么是传输服务?
2. 传输协议的要素有哪些?
3. 简述传输层向应用层提供的服务内容。
4. 试述 UDP 的传输过程、端口号分配原则以及应用场合。
5. 试述 TCP 的主要特点、端口号分配、Socket 地址概念以及应用场合。
6. TCP 的连接建立与释放分别采用几次握手? 为何要这样的步骤?
7. TCP 的重传策略是什么?
8. TCP 与 UDP 有什么不同之处?
9. 简述 TCP 与 UDP 的服务模型。
10. TCP 与 UDP 对于端口号的使用有什么规定?

第7章 应用层

应用层包括各种满足用户需要的应用程序，某些应用的适用范围十分广泛，有关国际标准化组织已经进行了标准化，如文件传输等，它们都属于 OSI 应用层的范畴。应用层协议是网络和用户之间的接口，即网络用户是通过不同的应用协议来使用网络的。应用层协议向用户提供各种实际的网络应用服务，使得上网者更方便地使用网络上的资源，随着网络技术的发展，应用层服务的功能还在不断改进和增加。

本章主要介绍几个目前在因特网上使用最广泛的应用层协议：超文本传输协议、文件传输协议、远程登录协议 Telnet、电子邮件协议 SMTP 和 POP3、域名系统 DNS 等。

7.1 域名系统

7.1.1 IP 地址与域名

1. 主机 IP 地址

为了确保通信时能相互识别，在 Internet 上的每台主机都必须有一个惟一的标识，即主机的 IP 地址。IP 协议就是根据 IP 地址实现信息传递的。

IP 地址由 32 位（即 4 字节）二进制数组成，为书写方便起见，常将每个字节作为一段并以十进制数来表示，每段间用“.”分隔。例如，202.96.209.5 就是一个合法的 IP 地址。

IP 地址由网络标识和主机标识两部分组成。常用的 IP 地址有 A、B、C 三类，每类均规定了网络标识和主机标识在 32 位中所占的位数。这三类 IP 地址的格式如图 7-1 所示，它们的表示范围分别为：

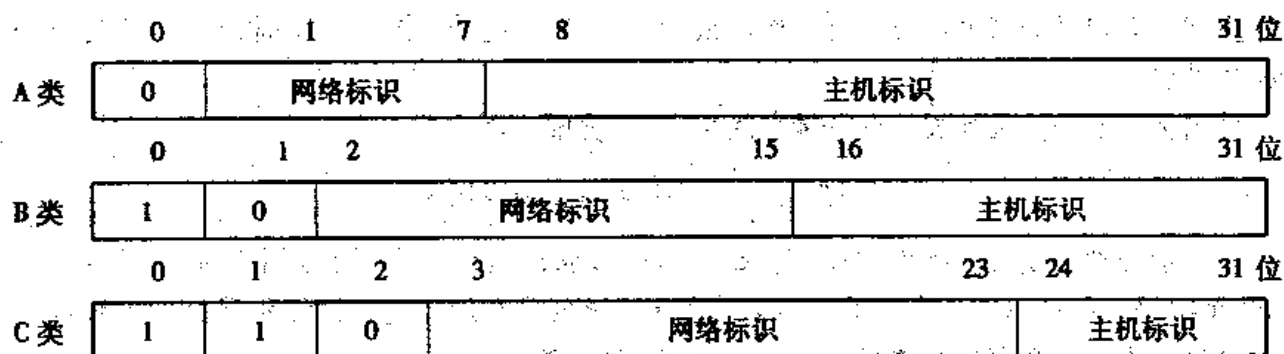


图 7-1 三类 IP 地址格式

A 类地址: 0. 0. 0. 0 ~ 127. 255. 255. 255

B 类地址: 128. 0. 0. 0 ~ 191. 255. 255. 255

C 类地址: 192. 0. 0. 0 ~ 223. 255. 255. 255

A 类地址一般分配给具有大量主机的网络使用, B 类地址通常分配给规模中等的网络使用, C 类地址通常分配给小型局域网使用。为了确保惟一性, IP 地址由世界各大地区的权威机构 Inter NIC (Internet Network Information Center) 管理和分配。

在 IP 地址的某个网络标识中, 可以包含大量的主机 (如 A 类地址的主机标识域为 24 位、B 类地址的主机标识域为 16 位), 而在实际应用中不可能将这么多的主机连接到单一的网络中, 这将给网络寻址和管理带来不便。为解决这个问题, 可以在网络中引入“子网”的概念。注意, 这里的“子网”与前面所说的通信子网是两个完全不同的概念。

将主机标识域进一步划分为子网标识和子网主机标识, 通过灵活定义子网标识域的位数, 可以控制每个子网的规模。将一个大型网络划分为若干个既相对独立又相互联系的子网后, 网络内部各子网便可独立寻址和管理, 各子网间通过跨子网的路由器连接, 这样也提高了网络的安全性。

利用子网掩码可以判断两台主机是否在同一子网中。子网掩码与 IP 地址一样也是 32 位二进制数, 不同的是它的子网主机标识部分为全“0”。若两台主机的 IP 地址分别与它们的子网掩码相“与”后的结果相同, 则说明这两台主机在同一子网中。

2. 域名

32 位二进制数的 IP 地址对计算机来说十分有效, 但用户使用和记忆都很不方便。为此, Internet 引进了字符形式的 IP 地址, 即域名 (Domain Name)。但是因特网通信仍然要使用 IP 地址来标识主机, 因此必须提供一种映射机制来实现域名和 IP 地址之间的转换, 这就是域名系统所要解决的问题。域名采用层次结构的基于“域”的命名方案, 任何一个连在因特网上的主机或路由器, 都有一个惟一的层次结构的名称, 即域名。域名只是一个逻辑概念, 并不反映出计算机所在的物理地点。

7.1.2 域名系统的概念

Internet 上的域名由域名系统 DNS (Domain Name System) 统一管理。DNS 是一个分布式数据库系统, 由域名空间、域名服务器和地址转换请求程序三部分组成。有了 DNS, 凡域名空间中有定义的域名都可以有效地转换为对应的 IP 地址, 同样, IP 地址也可通过 DNS 转换成域名。

域名由若干个分量组成, 各分量之间用“.”分隔, 其格式为:

n 级域名 二级域名 . 顶级域名

各分量分别代表不同级别的域名。每一级的域名都由英文字母和数字组成 (长度不超过 63 个字符, 并且不区分大小写), 级别最低的域名写在最左边, 而级别最高的顶级域名则写在最右边。一个完整的域名长度不超过 255 个字符。

现在顶级域名有 3 类:

- 国家顶级域名, 如 `cn` (中国)、`us` (美国)、`uk` (英国) 等。有一些地区也有顶级域名, 如 `hk` (香港)、`tw` (台湾)。
- 国际顶级域名, 采用 `int`, 国际性的组织可在 `int` 下注册。
- 通用顶级域名, 如 `com` (公司企业)、`net` (网络服务)、`edu` (教育机构) 等。

在国家顶级域名下注册的二级域名均由该国家自行确定。我国则将二级域名划分为类别域名和行政区域域名两大类。其中类别域名 6 个, 分别为: `ac` (科研机构)、`com` (商业企业)、`edu` (教育机构)、`gov` (政府部门)、`net` (网络服务商) 和 `org` (非盈利组织)。行政区域名 34 个, 用于我国的各省、自治区、直辖市, 如 `bj` (北京)、`sh` (上海) 等。

因特网的域名空间是一种层次型的树状结构。一级是最高级的顶级域名节点, 在顶级域节点下面的是二级域节点……最下面的就是接入因特网的主机。域名分为两种, 一种是网络域名, 它只用来表示是一个网络域; 另一种则是主机域名, 它用来表示一台具体的主机。如 `ecust.edu.cn` 是一个网络域名, 表示华东理工大学这个子域, 而 `www.ecust.edu.cn` 则是一个主机域名, 表示在 `ecust.edu.cn` 域中主机名为 `www` 的一台主机。在因特网的域名空间中, 非叶节点都是网络域名, 而叶节点则是主机域名。

同一子域中的主机拥有相同的网络域名, 但是不能有相同的主机名; 在不同子域中的主机可以使用相同的主机名, 但是其网络域名又不相同。因此, 因特网中不存在域名完全相同的两台主机。最后强调两点: 一是因特网的名字空间是按照机构的组织来划分的, 与物理的网络无关, 同 IP 地址空间中的子网也没有关系; 二是允许一台主机拥有多个不同的域名, 即允许多个不同的域名映射到同一个 IP 地址。

7.1.3 域名解析原理

域名到 IP 地址的映射是由若干个域名服务器程序组成的。域名服务器程序在专设的节点上运行, 而人们也常把运行该程序的计算机称为域名服务器。

当应用进程需要将一个主机域名映射为 IP 地址时, 就调用域名解析函数 (Resolve), 解析函数将待转换的域名放在 DNS 请求中, 以 UDP 报文方式发给本地域名服务器 (使用 UDP 是为了减少开销)。本地的域名服务器在查找域名后, 将对应的 IP 地址放在应答报文中返回。应用进程获得目的主机的 IP 地址后即可进行通信。若域名服务器不能回答该请求, 则此域名服务器就暂时成为 DNS 中的另一个客户, 直到找到能回答该请求的域名服务器为止。

每一个域名服务器都管理着一个 DNS 数据库, 保存着一些域名到 IP 地址的映射关系。同时域名服务器还必须具有连向其它域名服务器 (通常是其上级域名服务器) 的信息, 这样当遇到本地不能进行解析的域名时, 就会向其它服务器转发该解析请求。

因特网上的域名服务器系统也是按照域名的层次来安排的。每一个域名服务器都只对域名体系中的一部分进行管辖。共有以下 3 种不同类型的域名服务器。

(1) 本地域名服务器 (Local Name Server)。在因特网域名空间的任何一个子域都可以拥有一个本地域名服务器, 本地域名服务器中通常只保存属于本子域的域名——IP 地址对。一个子域中的主机一般都将本地域名服务器配置为默认域名服务器。

当一个主机发出域名解析请求时, 这个请求首先被送往默认的域名服务器。本地域名服

务器通常距离用户比较近，一般不超过几个路由的距离。当所要解析的域名属于同一个本地子域时，本地域名服务器立即就能将解析到的 IP 地址返回给请求的主机，而不需要再去查询其它的域名服务器。

(2) 根域名服务器 (Root Name Server)。目前在因特网上有十几个根域名服务器，大部分在北美。当一个本地域名服务器不能基于本地 DNS 数据库响应某个主机的解析请求查询时，它就以 DNS 客户的身份向某一根域名服务器查询。若根域名服务器有被查询主机的信息，就发送 DNS 应答报文给本地域名服务器，然后本地域名服务器再应答发出解析请求的主机。

可能根域名服务器中也没有所查询的域名信息，但它一定知道某个保存有被查询主机名字映射的授权域名服务器的 IP 地址。通常根域名服务器用来管辖顶级域，它并不直接对顶级域下面所属的所要域名进行转换，但它一定能够找到下面的所有二级域名的域名服务器，这样以此类推，一直向下解析，直到查询到所请求的域名。

(3) 授权域名服务器 (Authoritative Name Server)。每一个主机都必须在授权域名服务器处登记，通常一个主机的授权域名服务器就是它所在子域的一个本地域名服务器。为了更可靠地工作，一个主机应该有至少两个授权域名服务器。许多域名服务器同时充当本地域名服务器和授权域名服务器。授权域名服务器总是能够将其管辖的主机名转换为该主机的 IP 地址。

因特网允许各个单位根据单位的具体情况将本单位的域名划分为若干个域名服务器管辖区 (Zone)，而一般就在各管辖区中设置相应的授权域名服务器，管辖区是域的子集。

7.2 电子邮件

E-mail 是 Internet 上使用最广泛的一种服务。用户只要能与 Internet 连接，具有能收发电子邮件的程序及个人的 E-mail 地址，就可以与 Internet 上具有 E-mail 地址的所有用户方便、快速、经济地交换电子邮件。电子邮件可以在两个用户间交换，也可以向多个用户发送同一封邮件，或将收到的邮件转发给其它用户。电子邮件中除文本外，还可包含声音、图像、应用程序等各类计算机文件。此外，用户还可以邮件方式在网上订阅电子杂志、获取所需文件、参与有关的公告和讨论组，甚至还可浏览 WWW 资源。

7.2.1 电子邮件的基本概念

用户 E-mail 地址的格式为：用户名@主机域名。其中用户名是用户在邮件服务器上的信箱名，通常为用户的注册名、姓名或其它代号，主机域名则是邮件服务器的域名。用户名和主机域名之间用“@”分隔。例如，chang@online.sh.cn 即表示域名为“online.sh.cn”的邮件服务器上的用户“chang”的 E-mail 地址。

由于主机域名在 Internet 上的惟一性，所以，只要 E-mail 地址中的用户名在该邮件服务器中是惟一的，则这个 E-mail 地址在整个 Internet 上也是惟一的。

收发电子邮件必须有相应的软件支持。常用的收发电子邮件的软件有 Exchange、Outlook Express 等，这些软件提供邮件的接收、编辑、发送及管理功能。大多数 Internet 浏览器也都包含收发电子邮件的功能，如 Internet Explorer 和 Navigator / Communicator。

邮件服务器使用的协议有简单邮件传输协议 SMTP (Simple Mail Transfer Protocol)、邮局协议 POP (Post Office Protocol) 和因特网邮件存取协议 IMAP (Internet Mail Access Protocol)。POP 服务须由一个邮件服务器来提供，用户必须在该邮件服务器上取得账号才可使用这种服务。目前使用得较普遍的 POP 协议为第 3 版，故又称为 POP3 协议。

7.2.2 简单邮件传输协议 SMTP

简单邮件传输协议 SMTP 是一个简单的基于文本的电子邮件传输协议，是在因特网上用于在邮件服务器之间交换邮件的协议。SMTP 作为应用层的服务，可以适应于各种网络系统。

1. SMTP 命令

SMTP 是个请求/响应协议，在 SMTP 协议 25 号端口监听连接请求。SMTP 命令和响应都是基于 ASCII 文本、以命令行为单位，换行符为 CR/LF。响应信息一般只有一行，由一个 3 位数字的代码开始，后面可以附上很简短的文字说明，也可以不附。

2. SMTP 连接和发送过程

使用 SMTP 要经过建立连接、传送邮件和释放连接 3 个阶段，其中主要包括以下一些具体步骤：

- (1) 建立 TCP 连接。
- (2) 客户端向服务器发送 HELLO 命令以标识发件人自己的身份，然后客户端发送 MAIL 命令。
- (3) 服务器端以 OK 作为响应，表明准备接受。
- (4) 客户端发送 RCPT 命令（标识单个的邮件接收人，常在 MAIL 命令后面），以标识该电子邮件的计划接收人，可以有多个 RCPT 行。
- (5) 服务器端则表示是否愿意为收件人接受邮件。
- (6) 协商结束，发送邮件；用命令 DATA（在单个或多个 RCPT 命令后，表示所有的邮件接收人已标识，并初始化数据传输，以“.”结束）发送输入内容。
- (7) 结束此次发送，用 QUIT（结束会话）命令退出。

3. 邮件路由过程

SMTP 服务器基于 DNS 中的邮件交换 (Mail Exchanger, MX) 记录来路由电子邮件。MX 记录注册了域名或相关的 SMTP 主机，属于该域的电子邮件都应向该主机发送。电子邮件系统发邮件时是根据收信人的地址后缀来定位邮件服务器的。

SMTP 通过用户代理程序和邮件传输代理程序实现邮件的传输。其中用户代理程序 (User Agent, UA) 完成邮件的编辑、收取、阅读等功能；邮件传输代理程序 (Mail Transfer

Agent, MTA) 则负责将邮件传送到目的地。在应用中, 用户代理程序和邮件传输代理程序实际是被整合在一起的。一些常用的邮件软件, 如 Outlook Express 和 Netscape 等, 都可以完成邮件的编辑和发送功能, 避免用户和设置的麻烦。

7.2.3 邮局协议 POP

电子邮件的收信人使用邮局协议 (Post Office Protocol, POP) 从邮件服务器自己的邮箱中取出邮件。POP 有两种版本, 即 POP2 和 POP3, 都具有简单的电子邮件存储转发功能。POP2 与 POP3 本质上类似, 都属于离线式工作协议, 但是由于使用了不同的协议端口, 两者并不兼容。POP3 是目前与 SMTP 协议相结合最常用的电子邮件服务协议。目前大多数邮件服务器都支持 POP3。POP3 为邮件系统提供了一种接收邮件的方式, 使用户可以直接将邮件下载到本地计算机, 在自己的客户端阅读邮件。如果电子邮件系统不支持 POP3, 用户则必须通过远程登录, 到邮件服务器上查阅邮件。

1. POP3 命令

POP3 命令行有 1 个命令和一些参数组成。所有命令行以一个 CRLF 对结束。命令和参数由可打印的 ASCII 字符组成, 它们之间由空格间隔。命令一般是 3~4 个字母, 每个参数却可达 40 个字符长。

2. POP3 收发邮件的过程

用户使用 POP3 收发邮件的过程如下:

- (1) 通过 POP3 客户程序登录到支持 POP3 协议的邮件服务器, 用户可以发送邮件及附件。
- (2) 邮件服务器将为该用户收存的邮件传送给 POP3 的客户群, 使用户收到这些邮件, 并将这些邮件从服务器上删除。
- (3) 邮件服务器再将用户提交的发送邮件, 转发到运行 SMTP 协议的计算机中, 通过它实现邮件的最终发送。

在为用户从邮件服务器收取邮件时, POP3 是以该用户当前存储在服务器上全部邮件为对象进行操作的, 并一次性将它们下载到用户端计算机中。一旦客户的邮件下载完毕, 邮件服务器对这些邮件的暂存即告完成。使用 POP3, 用户不能对他们储存在邮件服务器上的邮件进行部分传输。离线工作方式适合那些从固定计算机上收发邮件的用户使用。

3. POP3 的连接过程

POP3 操作开始时, 服务器通过侦听 TCP 端口 110 开始服务。当客户主机需要使用服务时, 它将与服务器主机建立连接。当 TCP 连接建立后, POP3 发送确认消息。客户和 POP3 服务器相互 (分别) 交换命令和响应, 这一过程一直要持续到连接终止。

POP3 遵循存储转发机制。用户可按需要在客户级与保存邮件的服务器之间建立连接。用户通过客户机上的客户邮件程序或邮件用户代理 (Mail User Agent, MUA) 程序将邮件服务器上的待处理的邮件取回到客户机上, 同时删除服务器上已取走的邮件, 并断开客户机与

服务器的连接。然后,在本地客户机上进行阅读、删除、编辑或回复等脱机邮件处理。对新编辑的待发送和回复的邮件,可通过选择发送操作,再次建立客户机与服务器的连接来实现。

由以上可知,POP3 协议是用户计算机与邮件服务器之间的传输协议,SMTP 协议是邮件服务器之间的传输协议。

7.2.4 Internet 消息访问协议 IMAP

Internet 消息访问协议 (IMAP) 被定义在 RFC2060 中,是一个功能更强大的电子邮件协议,常用的是版本 4。IMAP4 改进了 POP3 的不足,用户可以通过浏览信件头来决定是否要下载、删除或检索信件的特定部分,还可以在服务器上创建或更改文件夹或邮箱。它除支持 POP3 协议的脱机操作模式外,还支持联机操作和断连接操作。它为用户提供了有选择地从邮件服务器接收邮件的功能、基于服务器的信息处理功能和共享信箱功能。IMAP4 提供离线、在线和断开连接 3 种工作方式。

(1) 离线工作方式。离线工作方式与 POP3 提供的服务类似,用户在所用的计算机与邮件服务器保持连接的状态下读取邮件。用户的电子邮件从服务器全部下载到用户计算机。

(2) 在线工作方式。选择在线工作方式时,用户无论进行怎样的操作,其电子邮件都被保留在服务器一端。所有邮件都始终存储在可共享的邮件服务器中,并可利用客户机上的邮件程序,对邮件服务器上的邮件进行远程的编辑、删除和回复等联机操作和管理。在客户邮件程序对邮件服务器的邮件进行处理过程中,始终保持与该服务器的连接。在这种操作方式中,客户机对邮件服务器的操作是透明的,操作的结果作用在邮件服务器上,而操作过程显示于本地客户机上。

(3) 断连接方式。断连接方式是一种脱机与联机操作的混合模式。在这种方式中,客户机先与邮件服务器建立连接,客户邮件程序选取相关的邮件,在本地客户机上生成一种高速缓存。与此同时,所选邮件的主拷贝仍保存在邮件服务器上,然后断掉与邮件服务器的连接,对客户机高速缓存的邮件进行“脱机”处理,以后客户机与邮件服务器再连接时,进行再同步处理使邮件状态相一致。在断连接操作中,联机和断连接操作相互补充,彼此交替进行。

断连接操作中的“脱机”处理不同于脱机操作模式,因为脱机操作模式会从邮件服务器中删除被取走的邮件,断连接操作在邮件服务器仍保存被移出邮件的拷贝。在断开连接工作方式下,用户的一部分邮件被保留在服务器一端,另一部分下载到用户计算机之后,如果用户还需要下载其它信件,可以将用户计算机再次与服务器建立连接,下载指定的信件;在用户计算机显示下载的信件复本。

选择使用 IMAP4 协议提供邮件服务的代价是要提供大量的邮件存储空间。受磁盘容量的限制,管理员要定期删除无用的邮件。为了用户邮件的安全,管理员还要定期进行操作。这样,即使用户计算机中的邮件被删除,也不至于造成邮件丢失。IMAP4 服务为那些希望灵活进行邮件处理的用户带来了很大方便,但是用户登录浏览邮件的联机会话时间将增加。

与 POP3 协议类似,IMAP4 协议仅提供面向用户的邮件收发服务,邮件在 Internet 上的收发是借助运行 SMTP 协议的计算机完成的。有时可以把 IMAP4 看成是一个远程文件服务

器，把 POP3 看成是一个存储转发服务。

7.3 万维网

7.3.1 WWW 的工作原理

WWW 是 World Wide Web 的英文缩写，有时也可简称 Web，中文译名为“万维网”，其含义是指通过 HTTP 协议链接起来的无数 Web 服务器中的网页资源。它是因特网上使用效率很高的一种消息发布和访问模式。

WWW 采用的是客户机/服务器 (Client/Server) 的工作模式。具体的工作流程如下：

- (1) 在客户端，建立连接，用户使用浏览器向 Web 服务器发送浏览信息请求。
- (2) Web 服务器接收到请求，并向浏览器返回所请求的信息。
- (3) 关闭连接。

在这里，客户机应用程序是用户与 Web 服务器进行信息传输的界面。首先，用户通过客户端程序与服务器进行连接，然后，用户通过客户端的浏览器向 Web 服务器发出查询请求，服务器接收到请求后，解析该请求并进行相应的操作，如打开数据库进行查询，调用 HTML 文件及 CGI 可执行程序等，以得到客户所需的信息，并将查询结果返回客户机，最后，当一次通信完成后，服务器关闭与客户机的连接。

7.3.2 超文本传输协议 HTTP

Internet 上 Web 服务器上存放的信息都是超文本信息。所谓超文本是指带超链接的文本。即超文本中除了文本信息外，还提供了一些超链接的功能，超链接的出现使得用户可以根据自己的兴趣有选择地阅读信息，而不是按照作者编排的顺序阅读文本信息。超文本文档中存在大量的链接，每一个链接都是将某些单词或图像以某些特殊的方式显示出来，往往是以特殊的颜色，加下划线或高亮度。WWW 中称这些链接为超链接 (Hyperlink)。

HTTP 是客户端浏览器和 Web 服务器之间的应用层通信协议，也即浏览器访问 Web 服务器上的超文本信息时使用的协议。HTTP 协议是 TCP/IP 组的应用层协议之一，它不仅需要保证超文本文档在主机间的正确传输，还能确定传输文档中的哪一部分，以及传输哪部分内容等。通过安装在客户计算机中的浏览器程序来观察页面，浏览器取来所需的页面，解释它所包含的文本和格式化命令，并以适当的形式在屏幕上显示该页面。每个网站服务器有有关服务监听端口 TCP 80 端口，看是否有从客户端浏览器来的连接请求。在连接建立起来后，每当客户发出一个请求，服务器就发回一个应答，然后释放连接。定义合法的请求与应答的协议就是 HTTP 协议。

HTTP 是一种通用协议，除了 Web 访问外，也可以广泛应用于域名系统服务器和企业信息管理信息系统；还可以用于用户软件、网关或其它因特网/内联网应用系统之间的通信，从而可以实现各类应用资源超媒体访问的集成。资源标识是 HTTP 的核心问题，在 HTTP 中通过

统一资源定位器 URL 来标识被操作的资源。URL 可以是 Web 服务器的 IP 地址或域名。

7.3.3 统一资源定位器 URL

URL 是为了能够使客户端程序查询不同的信息资源时有统一的访问方法而定义的一种地址标识方法。Internet 上所有资源都有了一个 URL (Union Resource Locator) 地址, 并且是独一无二的。只要知道某网页的 URL, 便可直接打开该网页。例如, 在 Internet 浏览器的 URL 输入框输入:

`http://www.online.sh.cn`

按回车后即可进入中国上海热线的主页。

URL 的完整格式如下:

协议://主机名或 IP 地址:端口号/路径名/文件名

协议又称为信息服务类型, 是客户端浏览器服务各种服务器资源的方法, 它定义了浏览器与服务器之间使用何种方式检索或传输信息。浏览器的地址栏或状态栏中 URL 的开始部分, 表明了使用什么协议访问 Internet。

URL 栏中的协议有很多种, 常用的有:

http: 提供了访问超文本信息的方法, 是目前因特网上主要的信息服务方式。

ftp: 文件传输协议, 提供在因特网上传输文件的服务。

telnet: 远程登录协议, 是客户机远程登录 Telnet 服务器的方法。

gopher: 使用 Gopher 协议访问 Gopher 服务器。

news: 代表访问网络新闻服务器。

waits: 广域信息服务 (Wide Area Information Service), 提供广域网的信息服务检索。

file: 访问本地文件的协议。

7.4 其它服务

7.4.1 文件传输 FTP

FTP (File Transfer Protocol) 协议是 Internet 上文件传输的基础, 通常所说的 FTP 是基于该协议的一种服务。FTP 文件传输服务允许 Internet 上的用户将一台计算机上的文件传输到另一台上, 几乎所有类型的文件, 包括文本文件、二进制可执行文件、声音文件、图像文件、数据压缩文件等, 都可以用 FTP 传送。

FTP 实际上是一套文件传输服务软件, 它以文件传输为界面, 使用简单的 get 或 put 命令进行文件的下载或上传, 如同在 Internet 上执行文件复制命令一样。大多数 FTP 服务器主机都采用 Unix 操作系统, 但普通用户通过 Windows 也能方便地使用 FTP。

FTP 最大的特点是用户可以使用 Internet 上众多的匿名 FTP 服务器。所谓匿名服务器, 指的是不需要专门的用户名和口令就可进入的系统。用户连接匿名 FTP 服务器时, 都可

以用“anonymous”（匿名）作为用户名、以自己的 E-mail 地址作为口令登录。登录成功后，用户便可从匿名服务器上下载文件。匿名服务器的标准目录为 pub，用户通常可以访问该目录下所有子目录中的文件。考虑到安全问题，大多数匿名服务器不允许用户上传文件。

7.4.2 远程登录 Telnet

Telnet 是 Internet 远程登录服务的一个协议，该协议定义了远程登录用户与服务器交互的方式。Telnet 允许用户在一台联网的计算机上登录到一个远程分时系统中，然后像使用自己的计算机一样使用该远程系统。

要使用远程登录服务，必须在本地计算机上启动一个客户应用程序，指定远程计算机的名字，并通过 Internet 与之建立连接。一旦连接成功，本地计算机就像通常的终端一样，直接访问远程计算机系统的资源。远程登录软件允许用户直接与远程计算机交互，通过键盘或鼠标操作，客户应用程序将有关的信息发送给远程计算机，再由服务器将输出结果返回给用户。用户退出远程登录后，用户的键盘、显示控制权又回到本地计算机。一般用户可以通过 Windows 的 Telnet 客户程序进行远程登录。

7.4.3 电子公告板系统 BBS

在日常生活中大家可能都曾经见过各种形式的公告牌，电子公告板系统 BBS (Bulletin Board System) 就是一种完全开放的、电子形式的公告牌系统。BBS 系统允许 Internet 用户注册进入系统（商业系统要收取一定的费用），一般说来，它们大都提供了一些共同的基本的服务，如允许用户把自己的观点或看法张贴于各讨论组的公告牌以供其它用户传阅，浏览各讨论组的内容，与其它用户谈话、闲聊等；有的 BBS 系统还向用户提供交换软件及其它网络服务，如发送电子邮件及参加小组讨论等。

从用户的观点来看，BBS 几乎可以提供我们日常生活所需的各种服务。用户在这里可以找到志同道合的朋友，向各方面的专家咨询各类问题，发布广告以推销产品，寻求生活上和工作上的帮助和指导，以及进行休闲娱乐。

从技术角度看，Internet 用户利用远程登录方式进入 BBS 站点，阅读其中分门别类的文章，在某些 BBS 站点上，用户不仅可以寻求信息，而且能得到 Talk、Chat、文件传输、Gopher、News 等其它 Internet 服务。

目前，基于 WWW 服务的 BBS 系统非常流行，它实际上是一种继承了 BBS 讨论方式的信息服务。前面我们讲过，BBS 最主要的功能就是讨论区。而基于 WWW 服务的 BBS 系统在实现了这个功能的同时，还在服务上提供了更多的优点。首先，它以环球网站点或主页的形式提供，这就使得它们更容易连接，不需要专门的 Telnet 软件，使用浏览器就可以访问；其次，它们是由 CGI 程序、Java 程序或 ASP 程序编写的，以主页的形式提供，用户可以在讨论过程中使用 HTML 命令，这样就可以在讨论的文章中使用不同的字体字号并嵌入图形，进一步丰富了讨论的表达形式。由于这些优点，使得这些 BBS 系统受到互联网用户的格外青睐，并在很短的时间内，在环球网上迅速普及开来。

习 题

1. 目前在 Internet 上有哪些使用比较广泛的应用?
2. 简述 HTML、HTTP 和 URL 的含义及其作用。
3. 简要说明 WWW 的工作过程。
4. Internet 的域名结构是怎样的? 与电话网的号码结构有何异同之处?
5. 说明域名解析的过程。
6. 简要说明电子邮件系统的工作过程。
7. 简述 SMTP 的工作过程。
8. 简单说明 POP3 的工作原理。
9. 说明 IMAP4 的特点。
10. POP 协议与 IMAP 协议有何区别?
11. 说明文件传输协议的原理。
12. 访问一个 FTP 服务器, 下载软件或文献。
13. 什么是域名服务?
14. 目前有哪些国际通用域名?
15. 如何实现域名注册?

第8章 局域网技术

局域网 (Local Area Network, LAN) 是在一个较小的范围内将各种通信设备和计算机互连起来以实现资源共享和消息交换的计算机网络。局域网具有覆盖范围小、传输速率高、通信延迟小、误码率低的特点。本章将对局域网的介质访问控制子层、IEEE802 标准、高速局域网、无线局域网、移动 Ad Hoc 网络以及局域网操作系统作详细介绍。

8.1 介质访问控制子层

从传输技术上, 计算机网络分为广播网和点到点网两大类。点到点网中, 两个网络节点间存在直接的通信信道才能进行数据通信, 信道的访问控制容易实现。如果是全双工信道, 则两个网络节点可以各自占用一个信道, 同时向对方发送数据; 如果是半双工信道, 则可以利用通信协议来保证在任何时刻都只有一个网络节点在使用网络。在广播网中, 所有网络节点共享同一个通信信道, 每个节点发出的消息都可以被所有其它的节点接收。但在广播网中存在信道争用的问题, 如果有两个或多个网络节点同时发送数据, 则数据信号会在信道中发生碰撞, 导致数据发送失败, 这个过程被称为冲突 (Collision)。信道争用产生的碰撞会导致数据传输失败, 信道利用率降低, 严重的情况下将无法进行通信。因此在所有的广播网中都必须面对和解决的一个关键问题就是: 当信道的使用存在竞争时, 如何分配信道的使用权。

广播信道有时被称为多路访问信道 (Multiaccess Channel) 或随机访问信道 (Random Channel), 通信信道又称介质, 网络节点使用信道进行通信称为介质访问, 协调各网络节点的行为, 决定广播信道使用权的协议就称为介质访问控制协议。广播网中, 不同的传输介质、不同的网络拓扑结构, 所采用的介质访问控制协议也不尽相同。为此, 在数据链路层专门设计了一个介质访问控制 (Medium Access Control, MAC) 子层, 用来实现广播网中的信道分配, 解决信道争用问题。点到点网中没有 MAC 子层的概念。

几乎所有的局域网都以广播信道作为通信的基础, 而广域网中除卫星网以外, 都采用点到点连接, 所以介质访问控制子层对于局域网技术来说尤为重要。

8.1.1 信道分配策略

广播信道的分配策略主要包括静态分配策略和动态分配策略两大类。

1. 静态分配策略

静态分配策略包括频分多路复用和同步时分多路复用, 这种分配策略是预先将频带或时隙固定地分配给各个网络节点, 各节点都有自己专用的频带或时隙, 彼此之间不会产生干扰。静态分配策略适用于网络节点数目少而固定, 且每个节点都有大量数据要发送的场合。此时采用静态分配策略不仅控制协议简单, 而且信道利用率较高。

但对于大部分计算机网络来说, 节点数量多而且不固定, 随时可能会有节点加入或退出网络, 同时网络节点间的数据传输也具有突发性的特点。如果采用静态分配策略进行信道分配既不容易实现, 信道的利用率也比较低, 这时应采用动态分配策略。

2. 动态分配策略

动态分配策略包括随机访问和控制访问, 本质上属于异步时分多路复用。各站点当有数据需要发送时, 才占用信道进行数据传输。

随机访问又称争用, 各个网络节点在发送前不需要申请信道的使用权, 有数据就发送, 发生碰撞之后再采取措施解决。随机访问适用于负载较轻的网络, 其信道的利用率一般不高, 但网络延迟时间较短。

控制访问有两种方法: 轮转和预约。轮转是使每个网络节点轮流获得信道的使用权, 没有数据要发送的节点将使用权传给下一节点。预约是各个网络节点首先声明自己有数据要发送, 然后根据声明的顺序依次获得信道的使用权来发送数据。无论是轮转还是预约, 都是使发送节点首先获得信道的使用权, 然后再发送数据, 因而不会出现碰撞和冲突。当网络负载较重时, 采用控制访问, 可以获得很高的信道利用率。

8.1.2 介质访问控制协议

目前已有多种广为人知的介质访问控制协议, 根据其工作原理和采用的广播信道使用权的分配算法的不同, 可划分为 3 类: 争用协议 (Contention Protocol)、无冲突协议 (Collision-Free Protocol) 和有限争用协议 (Limited-Contention Protocol)。

1. 争用协议

最早采用争用协议的计算机网络是 20 世纪 70 年代美国夏威夷大学的 Norman Abramson 设计的 ALOHA 系统, 该系统通过无线信道将各分校的远程终端连接到校本部的主机上。尽管 ALOHA 系统使用基于地面的无线广播信道, 但其基本思想适用于任何无协调关系的多用户竞争使用单一信道的系统。

ALOHA 系统有两种版本: 纯 ALOHA (Pure ALOHA, P-ALOHA) 和时分 ALOHA (Slotted ALOHA, S-ALOHA)。两者的区别在于是否将时间分为离散的时隙 (slot)。纯 ALOHA 系统中时间是连续的, 不需要全局时间同步; 而时分 ALOHA 系统中时间是离散的, 必须进行时间同步。

(1) 纯 ALOHA。纯 ALOHA 系统的基本思想是: 任何用户有数据需要发送就可以发送; 用户通过监听信道来获得是否产生冲突、数据传输是否成功; 若发现有冲突发生导致数据传

输失败，在等待一段随机时间后，再重新发送。

因为用户在发送数据前不需要取得信道的使用权，有数据就可以发送，所以存在产生冲突而导致数据帧被破坏的可能。但是，由于广播的反馈性，发送方只需要监听信道就可以得知它发出的帧是否被破坏。对于局域网，反馈消息很快就可以得到，对于卫星网，发送方在延迟 270ms 后才可以确认发送成功与否。如果监听到冲突，发送方等待一段随机时间后重发该帧。等待时间必须是随机的，否则有可能因为连续的冲突而导致系统死锁。

需要说明的是，任何时候，主要有两个网络节点同时使用信道发送数据就会产生冲突，并破坏所发送数据帧的内容。即使两个数据帧只有一个二进制位相重叠，两帧也会发生破坏，都必须事后重发。

图 8-1 给出一个包括 4 个网络节点的纯 ALOHA 系统的工作过程。在纯 ALOHA 系统中，用户可以在任何时刻发送数据。在站 1 发送帧 1 的过程中，其它站都没有发送数据，所以帧 1 被成功发送（这里不考虑信道产生的误码）。随后站 2 和站 3 发送的帧 2 和帧 3 在时间上有重叠，产生了冲突，其结果就是冲突的双方（有时可能是多方）发送的数据都出现差错，因此必须进行重发。但是发送冲突的各节点不能马上进行重发，因为这样必然会继续产生冲突，则需再等待一段随机的时间，直到重发成功为止。图中帧 4 发送成功，帧 5 和帧 6 发生冲突，帧 7 发送成功。

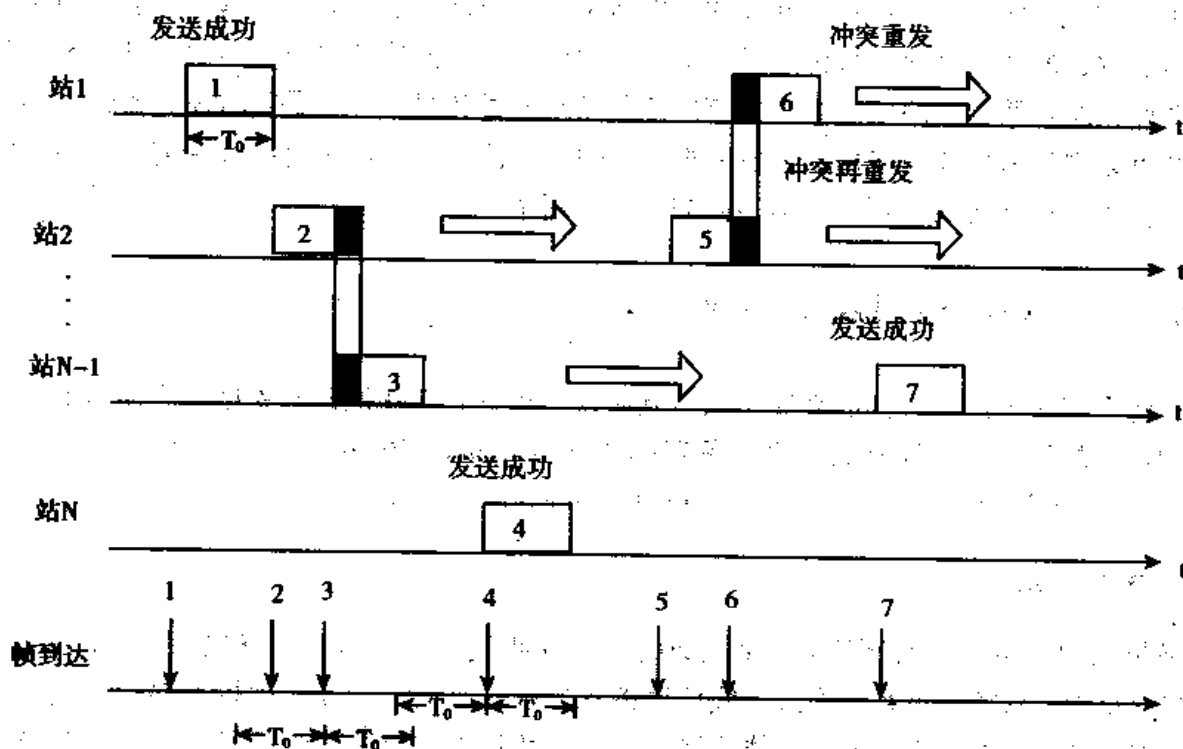


图 8-1 纯 ALOHA 系统的工作过程

研究发现，采用定长帧的 ALOHA 系统可以获得最大的吞吐量。图 8-1 的系统中各节点发送的帧长都是相同的。引入帧时 (Frame Time) 的概念来表示发送一个标准长度的帧所需要的时间。帧时是指一个标准长度的帧从发送开始，到发送成功所要的时间。

在 ALOHA 系统中，一方面不断有新产生的数据帧发送；另一方面由于冲突的发生，那些被破坏的数据帧也需要重发。为了分析 ALOHA 系统的性能，引入两个归一化参数：

① 吞吐量 S ：又称吞吐率，指在单位帧时内系统成功发送新产生的数据帧的平均数量。显然有 $0 \leq S \leq 1$ 。 $S=1$ 是最好的情况，此时帧一个接一个地发送出去，帧与帧之间没有空隙，信道利用最为充分。但在各系统用户无序争用、帧随机产生的情况下这个极值是不可能达到的。但可以利用 S 接近 1 的程度来衡量信道的利用率是否充分。

② 网络负载 G ：指在单位帧时内系统发送的所有数据帧的平均数量，包括成功发送的帧和因冲突而重发的帧。显然有 $G \geq S$ 。只有在不发生冲突的情况下，才有 $G=S$ 。当系统的负载很小时，几乎不发生冲突，这时可以认为 $S \approx G$ 。当系统负载增大而有冲突发生时，显然有 $G > S$ 。

对于一个实际运行的系统，在稳定状态下，吞吐量 S 和网络负载 G 的关系为：

$$S = GP$$

其中 P 为系统中一个帧成功发送的概率，实际上就是发送成功的帧在所有发送的帧的总数中所占的比例。

进一步分析帧发送成功的概率 P 。假设系统发送一帧所需时间为 t ，即系统帧时为 t 。如图 8-2 所示，在时间区间 $[t_0, t_0+t]$ 内开始发送的帧，其尾部必然与阴影帧的头部发生碰撞；在时间区间 $[t_0+t, t_0+2t]$ 内开始发送的帧，其头部必然与阴影帧的尾部发生碰撞。也就是说在时间区间 $[t_0, t_0+2t]$ 内，除阴影帧外只要有其它数据帧开始发送，就必然会导致冲突，这个时间区间称为阴影帧的易破坏区。由图 8-2 可知，纯 ALOHA 系统的易破坏区长度为 $2t$ 。

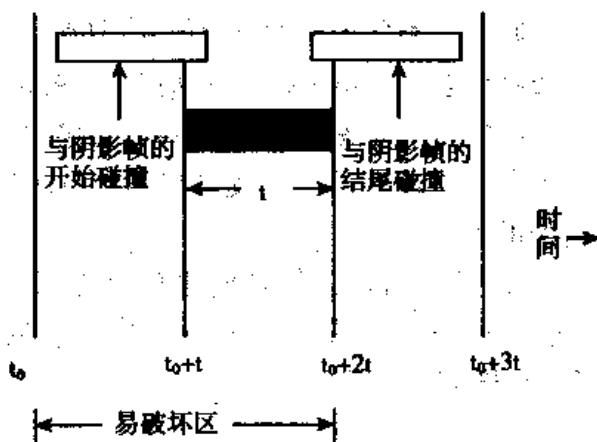


图 8-2 纯 ALOHA 系统中阴影帧的易破坏区

经过数学公式推导（过程略），在纯 ALOHA 系统中， $2t$ 时间内只有一个数据帧的概率，即帧成功发送的概率：

$$P = e^{-2G}$$

因此系统的吞吐量：

$$S = G e^{-2G}$$

当 $G=0.5$ 时， $S_{\max} = 1/2e \approx 0.184$ 。也就是说，纯 ALOHA 系统信道利用率的理论最大值只有 18.4%。实际应用中为了安全起见，纯 ALOHA 系统的吞吐量 S 一般不超过 10%。尽管如此，在很多情况下，当需要进行突发式的交换性数据通信时，纯 ALOHA 系统依然是一

种既简单又经济的通信方式。

(2) 时分 ALOHA。针对纯 ALOHA 系统信道利用率低下的问题, Roberts 于 1972 年提出一种对纯 ALOHA 系统的改进方法; 时分 ALOHA 系统。

时分 ALOHA 系统的基本思想是: 将时间分成等长的间隙, 每个间隙可以用来发送一个帧; 用户有数据帧要发送时, 不论帧在何时产生, 都必须到下一个间隙开始时才能发送; 用户通过监听信道来获知是否产生冲突、数据传输是否成功; 若发现有冲突发生导致数据传输失败, 则在随机等待若干个间隙后, 再重新发送。

时分 ALOHA 系统必须具有某种同步机制, 以保证每个网络节点都确切知道每个间隙的开始。通常的实现方法是设置一个特殊的网络节点在每个间隙的开始发送一个信号。

图 8-3 给出一个包含两个网络节点的时分 ALOHA 系统的工作过程。

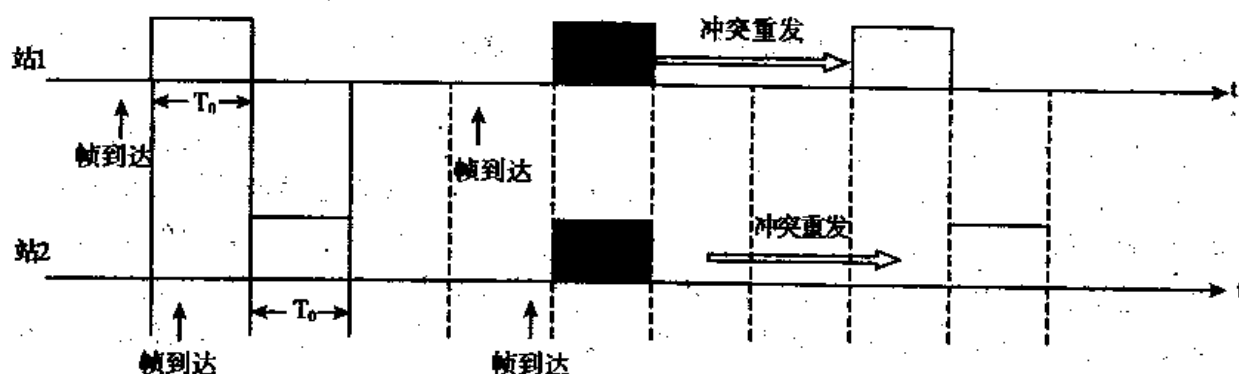


图 8-3 时分 ALOHA 系统的工作过程

图中向上的垂直箭头代表帧的到达。每个帧在到达后, 一般都要在缓冲区中等待一段时间 (等待时间小于时隙 T_0), 然后才能发送出去。当在一个时隙内有两个或两个以上的帧到达时, 则在下一个时隙将产生冲突。冲突后对重发策略与纯 ALOHA 系统的情况是相似的, 但随机等待的时间长度为时隙的整数倍。

在时分 ALOHA 系统中限制每个用户只能在时隙的开始发送数据, 这样, 连续的纯 ALOHA 就变成了离散的时分 ALOHA。如图 8-4 所示, 由于发生碰撞的可能减小了一半, 时分 ALOHA 系统的易破坏区长度缩小为 t 。

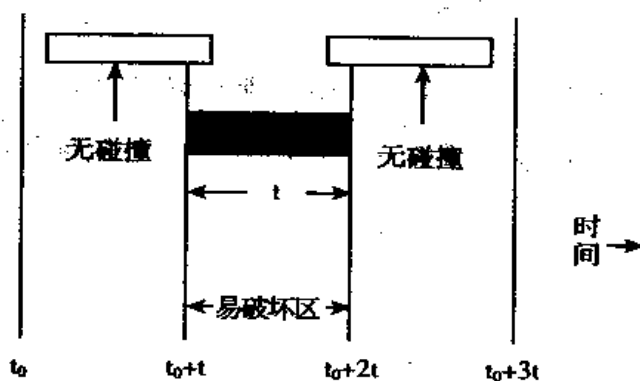


图 8-4 时分 ALOHA 系统中阴影帧的易破坏区

同样经过数学公式推导, 在时分 ALOHA 系统中, t 时间内只有一个数据帧的概率, 即帧成功发送的概率:

$$P = e^{-G}$$

因此系统的吞吐量:

$$S = G e^{-G}$$

当 $G=1$ 时, $S_{\max} = 1/e \approx 0.368$ 。也就是说, 时分 ALOHA 系统信道利用率的理论最大值为 36.8%。时分 ALOHA 系统与纯 ALOHA 系统的吞吐量曲线如图 8-5 所示。

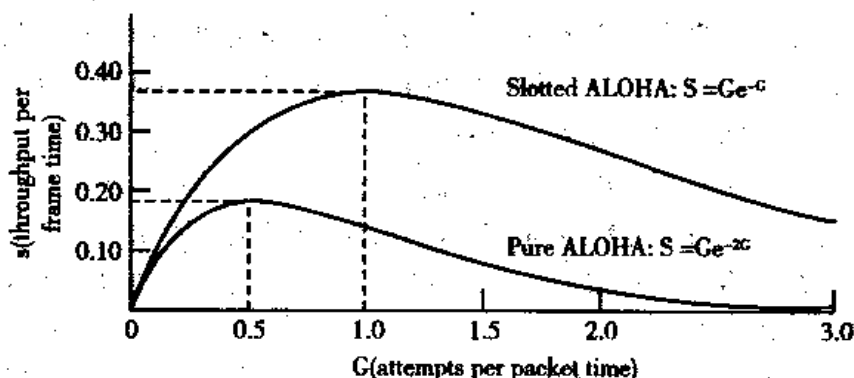


图 8-5 时分 ALOHA 系统与纯 ALOHA 系统的吞吐量曲线

(3) 载波监听多路访问 (Carrier Sense Multiple Access, CSMA) 协议。尽管时分 ALOHA 系统的效率是纯 ALOHA 系统的两倍, 但仍然是比较低的, 因为每个网络节点都是随心所欲地发送数据, 即使别的站正在发送也照发不误, 因此发生碰撞的概率很大。CSMA 协议是在 ALOHA 协议的基础上提出的一种改进协议, 与 ALOHA 协议的主要区别就是多了一个载波监听装置。

在采用 CSMA 协议的网络系统中, 每个节点在发送数据前先监听信道是否有载波存在 (即是否有数据在传输), 再根据监听的结果决定如何动作。由于采用了附加的硬件装置, 每个网络节点都可以在发送数据前监听信道上是否有其它节点在发送数据, 若有, 则该节点就暂不发送数据, 这就减少了发送冲突的可能, 从而提高了系统的吞吐量。

根据监听的方式以及监听到信道忙后的反应方式的不同, 有多种不同的 CSMA 协议, 下面介绍其中的 4 种。

① 1-坚持 CSMA。1-坚持 CSMA (1-persistent CSMA) 的基本思想是: 当一个节点要发送数据时, 首先监听信道; 如果信道空闲就立即发送数据; 如果信道忙则等待, 同时继续监听直至信道空闲; 如果发生冲突, 则随机等待一段时间后, 再重新开始监听信道。

“1-坚持”的含义是指当监听到信道忙后, 继续坚持监听信道; 当监听到信道空闲后, 其发送数据的概率为 1, 即立即发送数据。

信号传输延迟对 1-坚持 CSMA 协议的性能影响很大。概率虽小但仍然可能出现这样一种情况, 当节点 A 开始发送数据时, 节点 B 也正好有数据要发送, 但这时节点 A 发出的数据传输信号还未到达节点 B, 节点 B 监听信道, 发现信道空闲, 于是立即发送数据, 结果必然导致冲突。信号传输延迟越大, 这种情况发生的可能就越大, 协议的性能就越差。

即使不考虑传输延迟, 1-坚持 CSMA 协议也可能产生冲突。比如当节点 A 正在发送数据的时候, 节点 B 和节点 C 也都准备好要发送数据, 它们监听信道时发现信道忙, 于是都坚持监听, 结果当节点 A 一发送完, 节点 B 和节点 C 都会立即发送数据, 同样导致冲突。

尽管也存在冲突的可能,但 1-坚持 CSMA 协议的性能要好于 ALOHA 系统,因为有节点在发送数据时,其它节点检测到信道忙后就不会再发送数据了。

② 非坚持 CSMA。非坚持 CSMA (Nonpersistent CSMA) 的基本思想是:当一个节点要发送数据时,首先监听信道;如果信道空闲就立即发送数据;如果信道忙则放弃监听、随机等待一段时间,再开始监听信道。

与 1-坚持 CSMA 的“贪婪”不同,非坚持 CSMA 比较“理智”,在监听到信道忙后将放弃监听,这样就减少了多个节点等待信道空闲后同时发送数据导致冲突的概率。因为各节点在监听到信道忙时,都放弃监听,各自随机等待一段时间后再监听,这就有可能将各节点重新试图发送数据的时间错开,避免了冲突的发生。

但与此同时,非坚持 CSMA 也使得数据在网络中的平均延迟时间增加了。因为当某个节点发完数据后,由于非坚持的随机等待,其它节点没有连续监听信道,也就不可能紧接着立即发送,造成数据在网络中的平均延迟时间增加。可见,信道利用率的提高是以数据在网络中的延迟时间增加为代价的。

③ p-坚持 CSMA。p-坚持 CSMA (p-persistent CSMA) 用于时分信道 (Slotted Channel),其基本思想是,当一个节点要发送数据时,首先监听信道;如果信道忙则坚持监听到下一个时隙;如果信道空闲,便以概率 p 发送数据,以概率 $1-p$ 推迟到下一个时隙;如果下一个时隙信道仍然空闲,则仍以概率 p 发送数据,以概率 $1-p$ 推迟到下一个时隙;这样过程一直持续下去,直到数据被发送出去,或因其它节点发送而检测到信道忙为止,若是后者,则等待一段随机的时间后重新开始监听。

P-坚持 CSMA 在检测到信道空闲后,以概率 p 发送数据,以概率 $1-p$ 推迟到下一个时隙,其目的是试图降低 1-坚持 CSMA 协议中多个节点检测到信道空闲后同时发送的冲突概率;采用“坚持”监听,是试图克服非坚持 CSMA 协议中由于随机等待造成延迟时间较长的缺点。

p-坚持 CSMA 的性能依赖于概率 p 的选取。假设任一时刻平均有 N 个节点准备好要发送,则在当前数据发送完后的下一个时隙里,平均有 Np 个节点要发送数据。如果 p 选择得过大,使 $Np > 1$,则冲突的概率很大,所以应使 $Np < 1$;但如果 p 选择得过小,数据在网络中的延迟时间将变得很长,会降低信道的利用率;一般 P 的选取应令 Np 略小于 1。

概率 p 可以用随机发生器来产生,假设该随机数发生器产生 $(0, 1)$ 之间的一个随机数 r ,当 r 在 $(0, p)$ 范围内时,发送数据;当 r 在 $[p, 1]$ 范围内时,推迟到下一个时隙发送。

以上 3 种 CSMA 协议以及纯 ALOHA 和时分 ALOHA 的性能比较见图 8-6 所示。

④ 带有冲突检测的 CSMA。带有冲突检测的 CSMA (CSMA with Collision Detection, CSMA/CD) 广泛应用于局域网的 MAC 子层中,其基本思想是:当一个节点要发送数据时,首先监听信道;如果信道空闲就发送数据,并继续监听;如果在数据发送过程中监听到了冲突,则立刻停止数据发送,等待一段随机的时间后,重新开始尝试发送数据。

CSMA 只在发送前监听信道,以保证信道忙时不会有新的节点发送数据;但在数据发送过程中检测到冲突时,仍要将剩余的数据发送完,既浪费时间又浪费带宽。CSMA/CD 对此进行的改进就是网络节点边发送边监听,一旦监听到冲突就立刻停止发送。这样信道很快就会空闲下来,提高了信道利用率。

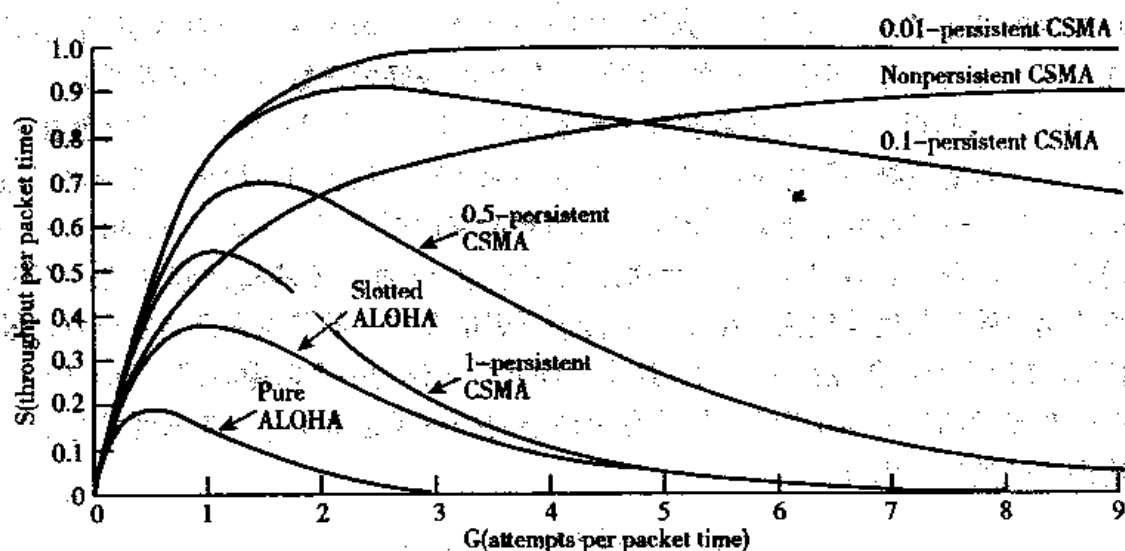


图 8-6 各种争用协议的 S-G 性能曲线

CSMA/CD 的工作过程如图 8-7 所示。在时刻 t_0 一个节点完成数据发送，信道变为空闲，此时其它节点有数据要发送的话都可以发送；当多个节点同时发送时产生冲突，各节点检测到冲突后立即停止发送，于是形成了一个较短的时隙，这种时隙称为争用时隙；各节点停止发送后，各自随机等待一段时间再监听信道，发现信道空闲又发送数据；当争用信道的节点比较多时，可能会接连发送冲突，结果形成一系列的争用时隙，经过几轮竞争后，有一个节点发送数据获得成功；随后，有数据要发送的节点又开始新一轮的争用。因此，CSMA/CD 的工作过程就是传输周期、争用周期和空闲周期周而复始、交替出现的一个过程。

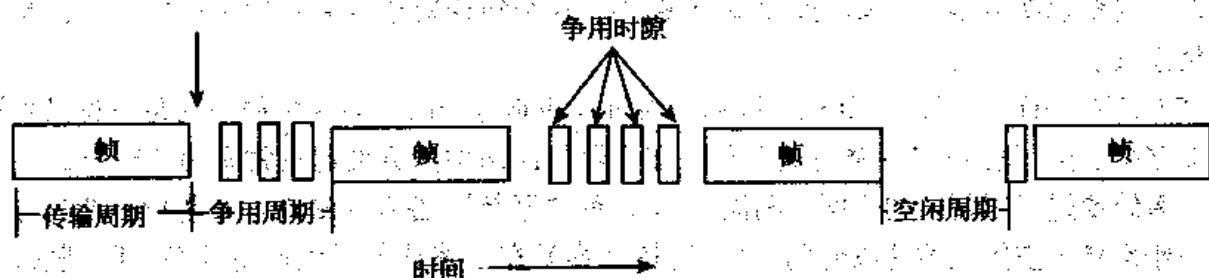


图 8-7 CSMA/CD 的工作过程

冲突检测的方法很多，通常以硬件技术实现。最简单的方法是比较接收到的信号的电压大小。在基带传输系统中，当两个帧的信号迭加在信道上时，电压的摆动值要比正常值大一倍。因此只要接收到的信号的电压摆动值超过某一门限值，就可以认为发生了冲突。当若两个节点距离很远，以致信号在信道上传播时衰减很多，则有可能使冲突迭加信号的电压摆动值不超过门限值，这就无法判断是否出现了冲突。因此，采用这种基于模拟技术的冲突检测方法，对站间的最大距离有一定的限制。另一种可行的方法是在发送帧的同时进行接收，将收到的信号逐比特地与发送的信号相比较，如果有不符合的，就说明出现了冲突。

CSMA/CD 中，在每个节点发送数据刚刚开始的一个很短的时间内，由于电磁波在网络上传播需要时间，因此冲突仍有可能发生。那么一个节点在开始发送后，经过多长时间的监听才能确信数据传输成功（仅指不发生冲突）呢？考虑最为极端的一种情况。A 和 B 是网

网络中相距最远的两个节点，信号从 A 到 B 的传播时间为 τ 。假设在 t_0 时刻 A 开始发送数据，而恰好在 $t_0 + \tau - \varepsilon$ (ε 为一个任意小的正数) 时刻 B 准备好发送数据。B 监听信道，发现信道空闲（由于传播延迟，A 发出的数据尚未到达 B），于是立即发送数据，冲突就在 B 的附近发生了。B 立即就检测到了冲突，但 A 这时还一无所知，只有当被损坏的信号再经过时间 τ 传到 A 时，A 才知道发生了冲突，所以 A 检测到冲突的时刻是 $t_0 + 2\tau - \varepsilon$ 。由于 ε 是一个任意小的正数，因此可以说 A 在开始发送后最多经过 2τ 时间才能检测到冲突。不失一般性，可将争用时隙的长度确定为网络中最大传播延迟的 2 倍，即节点在开始发送后，最多经过 2τ 时间就能确定此次传输是否成功。这个时间通常被作为一个时隙时间 (Slot Time)。设网络中两个节点间的最大间距为 S ，信号在物理层的处理延迟为 t_{PHY} ，考虑到发送、接收均需经过物理层的处理，则有：

$$\text{Slot Time} \approx 2S/0.7C + 2t_{PHY}$$

其中 C 为光速， $0.7C$ 是电信号在介质上的传播速率。

时隙时间决定了在网络中传输的数据帧的最小帧长 L_{min} ，因为要想在时隙时间内检测到碰撞，就有：

$$\text{Slot Time} = L_{min}/R$$

因此，数据帧的最小帧长：

$$L_{min} = \text{Slot Time} \times R \approx (2S/0.7C + 2t_{PHY}) \times R$$

因为光速 C 和物理层延迟 t_{PHY} 均为常数，因此公式中的 3 个参数 L_{min} 、 S 和 R 有正、反比关系。当传输速率 R 固定时，最小帧长 L_{min} 与网络跨距 S 成正比；而当最小帧长 L_{min} 不变时，传输速率 R 越高，则网络跨距 S 越小。这个结论对于今后对网络性能的讨论具有指导性意义。

和 CSMA 一样，CSMA/CD 也可以划分为时分和非时分的，而这两种中的每一种又可再分为非坚持、p-坚持和 1-坚持这 3 种。在实际的网络中为方便起见常采用非时分的（因为时分系统要进行很复杂的全网时间同步）。3 种“坚持”各有优缺点。非坚持不能充分利用信道刚刚转入空闲期的这段时间。1-坚持又容易在上述这段时间产生冲突。P-坚持可以在一定程度上克服这些缺点，但却很难选择一个能用于各种通信强度的 p 值。在实用网络中常选择 1-坚持。1-坚持比 p-坚持在实现上要简单一些。

由于单向传输的原因，对于宽带总线而言，冲突检测时间等于任意两个站之间最大传播时延的 4 倍。所以，对于宽带 CSMA/CD 来说，要求数据帧的传输时延至少 4 倍于传播时延。

在 CSMA/CD 算法中，一旦检测到冲突并发完阻塞信号后，为了降低再次发生冲突的概率，需要等待一个随机时间，然后再使用 CSMA 方法试图传输。为了保证这种退避操作维持稳定，采用了一种称为二进制指数退避的算法，其规则如下：

- (1) 对每个数据帧，当第一次发生冲突时，设置一个参量 $L=2$ ；
- (2) 退避间隔取 1 到 L 个时间片中的一个随机数，1 个时间片等于两站点之间的最大传播时延的两倍；
- (3) 当数据帧再次发生冲突，则将参量 L 加倍；

(4) 设置一个最大重传次数, 超过该次数, 则不再重传, 并报告出错。

二进制指数退避算法是按后进先出 LIFO (Last In First Out) 的次序控制的, 即未发生冲突或很少发生冲突的数据帧, 具有优先发送的概率; 而发生多次冲突的数据帧, 发送成功的概率就更小。

IEEE 802.3 就是采用二进制指数退避和 1-坚持算法的 CSMA/CD 介质访问控制方法。这种方法在低负荷时, 如介质空闲时, 要发送数据帧的站点能立即发送; 在重负荷时, 仍能保证系统的稳定性。由于在介质上传播的信号会衰减, 为确保能检测出冲突信号, CSMA/CD 总线网限制一段无分支电缆的最大长度为 500 米。

2. 无冲突协议

在争用协议中由于冲突的存在, 影响了系统的性能。下面介绍一些无冲突地解决信道争用问题的协议, 即无冲突协议。

(1) 位图协议。假设网络中有 N 个节点, 每个节点都拥有一个惟一的序号 ($0 \sim N-1$)。位图协议 (Bit-Map Protocol) 的基本思想是: 将数据传输过程分成一系列的预约周期和传输周期; 每个预约周期由 N 个争用时段组成, 每个时段对应一个节点, 节点 i 可以在时段 i 发出一个比特“1”来声明它有一个数据帧要发送, 以此预约对信道的使用权; 预约周期过后, 每个节点都知道了究竟有哪些节点要发送数据, 接下来进入传输周期, 各预约信道的节点按照序号大小顺序依次发送数据; 待最后一个节点结束数据发送后, 开始新一轮预约。由于预约周期的 N 个争用时段就像是 N 个比特的位图, 因此协议被称为位图协议。

图 8-8 是 8 个节点的例子。第一轮预约中, 节点 1、3、7 对信道的使用权进行了预约, 在接下来的传输周期中这 3 个节点各成功发送了一个数据帧。因为每一个节点都知道下一个该谁发送, 所以根本就不可能发生冲突。第二轮中, 节点 1、5 的数据帧发送同样也不可能发生冲突。如果某个节点在其争用时段过后才做好发送准备, 那它必须保持沉默, 直到新一轮预约周期自己的争用时段到来。这种在实际发送之前首先声明的协议又被称为预定协议 (Reservation Protocol)。

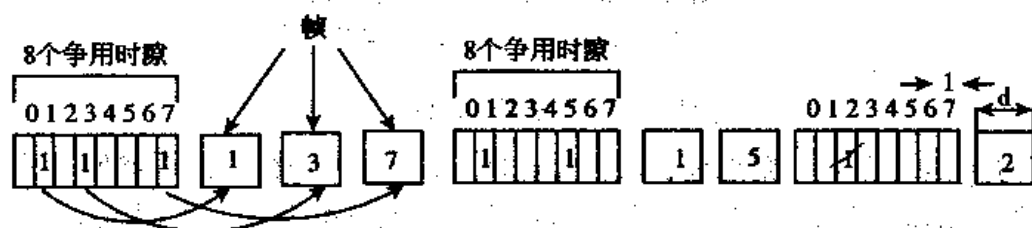


图 8-8 位图协议

下面简单分析一下位图协议的性能。为方便起见, 以争用时段作为时间的基准单位, 假设每个数据帧由 d 个时间单位组成。

在系统负载较重的情况下, 每个节点都有数据要发送, 那么 N 个争用时段的预约周期后, 每个节点轮流发送一个数据帧, 共 N 个帧, 平均起来每帧产生了一个时段的额外开销。因此协议效率为 $d/(d+1)$ 。

位图协议在较轻负载时是不公平的, 而且节点必须等待预约周期结束后才能传输数据,

增加了数据的等待时间。为此提出一种改进的位图协议，原有的位图协议又被称为基本位图协议。改进的位图协议有一点变化：节点在自己的争用间隙声明预约后立即开始发送数据，发送之后是下一个节点的争用间隙。

改进的位图协议在系统负载较轻的情况下每个节点的平均等待时间都为 $0.5N$ 个间隙，性能优于基本位图协议；但在协议负载较重的情况下，二者相差无几。

(2) 二进制倒计数协议。二进制倒计数协议 (Binary Countdown Protocol) 的基本思想是：每个节点的地址用二进制数来表示，并假设所有地址长度相等；想要发送数据的节点，首先将其地址以二进制位串的形式按照由高到低的次序进行广播；所有广播出来的地址要进行对应二进制位的逻辑或运算；节点在发送地址的同时监听信道，当发现自己的地址中的某个“0”在发送出去后变为“1”时，就退出信道的争用；最后参与争用的地址最高的节点获得信道的使用权发送一个数据帧；数据发送结束后，开始新一轮争用。

图 8-9 给出了 4 个节点争用信道的例子。4 个节点的地址分别为 0010、0100、1001 和 1010，它们都有数据要发送。在第 1 个位时，各节点分别发送了 0、0、1 和 1，它们进行逻辑或运算后的结果为 1。节点 0010 和 0100 一监听到 1，就会知道有地址更高的节点在参与信道争用，于是它们就会退出信道争用，而站点 1001 和 1010 仍将继续。在第 2 位时，两节点发出的都是 0，逻辑或运算的结果也为 0，因此站点 1001 和 1010 仍然继续。在第 3 位时，两节点分别发出 0 和 1，逻辑或运算的结果为 1，于是站点 1001 放弃，最后获得胜利的是站点 1010，因为其地址最高。

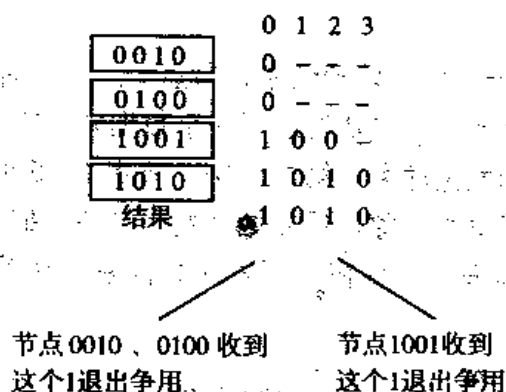


图 8-9 二进制倒计数协议

如果系统有 N 个节点，则地址长度为 $\log_2 N$ ，每个帧为获得信道而增加的额外开销为 $\log_2 N$ 。如果数据帧长为 d ，则二进制倒计数协议的信道效率为 $d / (d + \log_2 N)$ 。但是，如果数据帧格式选择适当，帧中第一个字段就是发送方地址的话，协议效率将达到 100%。

显然，二进制倒计数协议对不同地址的节点是不公平的，高地址节点优先级高，低地址节点优先级低，为此提出一种改进方案：使用虚拟地址且地址可变，当节点成功发送出一个数据帧后将其地址变为 0，使之排在最后，原来排在其后的节点地址递增 1，形成优先级轮换。改进方案使长时间沉默的节点获得较高的优先权。例如，节点 C、H、D、A、G、B、E、F 的发送优先级分别为 7、6、5、4、3、2、1、0。如果此时节点 D 成功发送一个数据帧，则优先级顺利变为 C、H、A、G、B、E、F、D，优先级分别为 7、6、5、4、3、2、1、0。

3. 有限争用协议

每种信道分配策略的性能都可以根据两项指标加以评定：轻负载下的时间延迟以及重负载下的信道利用率。争用协议和无冲突协议在这两方面各有利弊。系统负载较轻时，争用协议由于其时延短而性能较优。但随着系统负载的增加，信道分配的开销越来越大，争用协议的性能也就越来越差。无冲突协议恰好相反，系统负载较轻时，其时延较长，但随着系统负载的增加，信道利用率不仅没有下降，反而有所改善。

有限争用协议就是综合争用协议和无冲突协议的优点而产生的一种新的协议，该协议在轻负载时采用争用协议的信道分配策略，使时间延迟较短，而在重负载时采用无冲突协议的信道分配策略，使信道利用率较高。

有限争用协议的基本思想是：将系统中的网络节点分组，每个争用时隙只允许一个分组争用信道。协议的关键是如何分配时隙，只要节点分组合理，就可以减少在每个时隙内的竞争，从而提高争用的成功率。分组有两种极端的情况：第一种情况是每组只有一个成员，这样每个时隙最多只有一个站点参与竞争，此时是无冲突协议；第二种情况是所有节点在一个组中，这样每个时隙都是有所有节点参与竞争，此时是争用协议。有限争用协议就是要根据当前网络的分组情况，对节点进行动态分组，当网络分组较轻时，每组的节点数量就多一些，当网络分组较重时，每组的节点数量就少一些。

有限争用协议的典型例子是适应树步行协议 (Adaptive Tree Walk Protocol)。该协议把网络节点看做二叉树的叶节点，如图 8-10 所示。在一次成功传送之后，在第一个争用时隙 (即 0 时隙) 内，所有节点都可以尝试获取信道。如果只有一个节点申请使用信道，它会立即获得信道。假如有多个节点同时申请，便会产生冲突，那么在 1 时隙内，只允许树中位于节点 2 以下的节点参与争用。如果它们其中之一获得了信道，那么下一时隙内将由节点 3 以下的各站来争用信道。但如果节点 2 下有多个站都想发送，那么在时隙 1 内就会产生冲突，于是下一时隙 (即时隙 2) 内将由节点 4 以下各节点来争用信道。

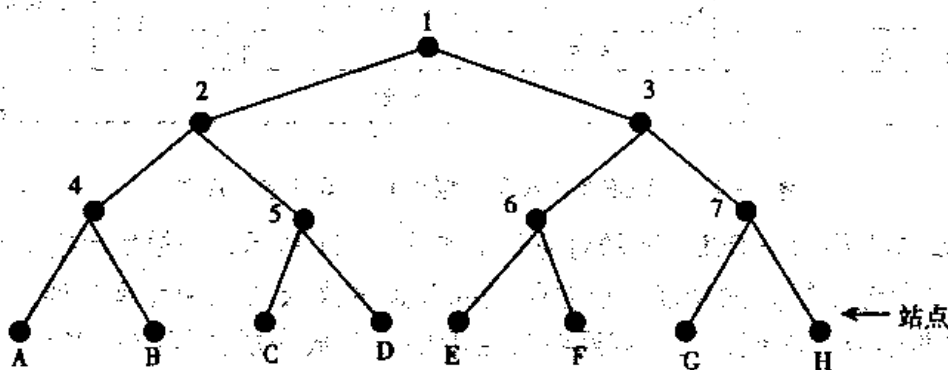


图 8-10 有限争用协议

显然，系统负载越重，搜索开始的层次就应该越低。一般而言，如果当前有 q 个节点准备发送数据，则应该从第 $\log_2 q$ 层开始搜索。

8.2 IEEE 802 标准与局域网

局域网的标准化工作，能使不同生产厂家的局域网产品之间有更好的兼容性，以适应各种不同型号计算机的组网需求，并有利于产品成本的降低。国际上从事局域网标准化工作的机构主要有国际标准化组织 ISO、美国电气电子工程师学会 IEEE 的 802 委员会、欧洲计算机制造商协会 ECMA、美国国家标准局 NBS、美国电子工业协会 EIA、美国国家标准化协会 ANSI 等。IEEE 于 1980 年 2 月成立了一个局域网标准化委员会——IEEE 802 委员会来统一制定局域网的有关标准，这些标准统称 IEEE 802 标准。IEEE 802 标准已被 ANSI 接受为美国国家标准，随后又被 ISO 采纳，作为局域网的国际标准系列，称为 ISO 8802 标准。

8.2.1 IEEE 802 标准概述

局域网是一个通信网络，只涉及相当于 OSI/RM 通信子网的功能。由于内部大多采用共享信道的技术，所以局域网通常不单独设立网络层。局域网的高层功能则由具体的局域网操作系统来实现。

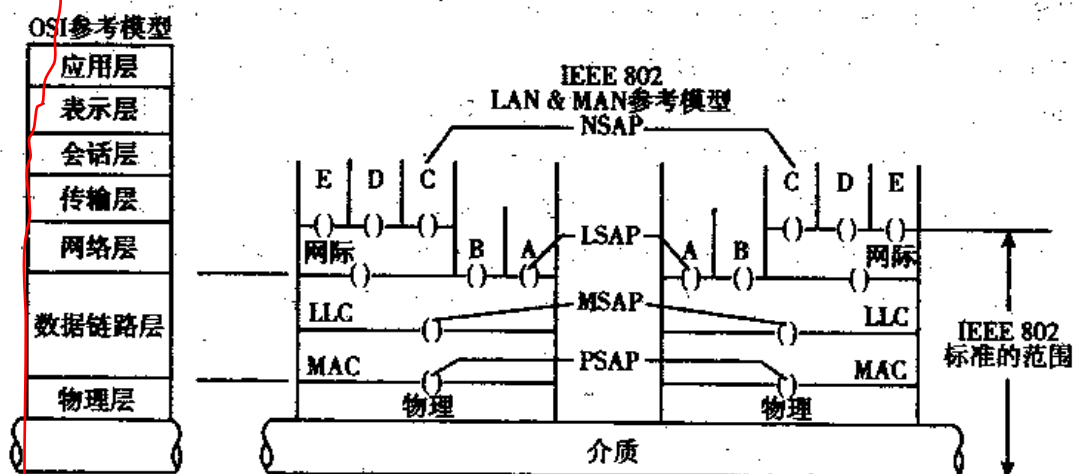


图 8-11 IEEE 802 参考模型与 OSI/RM 的对应关系

IEEE 802 参考模型与 OSI/RM 的对应关系如图 8-11 所示，该模型包括了 OSI/RM 最低两层（物理层和链路层）的功能，也包括网间互连的高层功能和管理功能。从图中可见，OSI/RM 的数据链路层功能，在局域网参考模型中被分成介质访问控制 MAC (Medium Access Control) 和逻辑链路控制 LLC (Logical Link Control) 两个子层。

在 ISO/RM 中，物理层、数据链路层和网络层使计算机网络具有报文分组转接的功能。对于局域网来说，物理层是必需的，它负责体现机械、电气和过程方面的特性，以建立、维持和拆除物理链路；数据链路层也是必需的，它负责把不可靠的传输信道转换成可靠的传输信道，传送带有校验的数据帧，采用差错控制和帧确认技术。

但是，局域网中的多个设备一般共享公共传输介质，在设备之间传输数据时，首先要解决由哪些设备占有介质的问题。所以局域网的数据链路层必须设置介质访问控制功能。由于

局域网采用的介质有多种，对应的介质访问控制方法也有多种，为了使数据帧的传送独立于所采用的物理介质和介质访问控制方法，IEEE 802 标准特意把 LLC 独立出来形成一个单独子层，使 LLC 子层与介质无关，仅让 MAC 子层依赖于物理介质。由于设立了 MAC 子层，IEEE 802 标准就具有了可扩充性，有利于接纳新的介质和介质访问控制方法。

由于穿越局域网的链路只有一条，不需要设立路由选择和流量控制功能，如网络层中的分组寻址、排序、流量控制、差错控制等功能都可以放在数据链路层中实现。因此，局域网中可以不单独设置网络层。当局限于一个局域网时，物理层和链路层就能完成报文分组转接的功能。但当涉及网络互连时，报文分组就必须经过多条链路才能到达目的地，此时就必须专门设置一个层次来完成网络层的功能，在 IEEE 802 标准中这一层被称为网际层。

在参考模型中，每个实体和另一个系统的同等实体按协议进行通信；而一个系统中上下层之间的通信，则通过接口进行，并用服务访问点 SAP (Service Access Point) 来定义接口。为了对多个高层实体提供支持，在 LLC 层的顶部有多个 LLC 服务访问点 (LSAP)，为图中的实体 A 和 B 提供接口端；在网际层的顶部有多个网间服务访问点 (NSAP)，为实体 C、D 和 E 提供接口端；介质访问控制服务访问点 (MSAP) 向 LLC 实体提供单个接口端，物理服务访问点 (PSAP) 也向 MAC 实体提供单个接口端。

LLC 子层中规定了无确认无连接、有确认无连接和面向连接三种类型的链路服务。无确认无连接服务是一种数据报服务，信息帧在 LLC 实体间交换时，无须在同等层实体间事先建立逻辑链路，对这种 LLC 帧既不确认，也无任何流量控制或差错恢复；有确认无连接服务除了对 LLC 帧进行确认外，其它类似于无确认无连接服务；面向连接服务提供服务访问点之间的虚电路服务，在任何信息帧交换前，一对 LLC 实体之间必须建立逻辑链路，在数据传送过程中，信息帧依次发送，并提供差错恢复和流量控制功能。

MAC 子层在支持 LLC 子层完成介质访问控制功能时，可以提供多个可供选择的介质访问控制方式。使用 MSAP 支持 LLC 子层时，MAC 子层实现帧的寻址和识别。MAC 到 MAC 的操作通过同等层协议来进行，MAC 还产生帧检验序列和完成帧检验等功能。

将数据链路层分成两个子层，只要设计合理，使得 MAC 子层向上提供统一的服务接口，就能将底层的实现细节完全屏蔽掉，局域网对于 LLC 子层来说是透明的，只有到 MAC 子层才能看到所连接的是采用什么标准的局域网。也就是说，对于不同的物理网络，其 LLC 子层是相同的，数据帧的传送完全独立于所采用的物理介质和介质访问控制方法，网络层以上的协议可以运行于任何一种 IEEE 802 标准的局域网上。这种分层方法也使得 IEEE 802 标准具有良好的可扩充性，可以很方便地接纳新的传输介质以及介质控制方法。

IEEE 802 委员会下设若干工作组，每个工作组负责一个标准。这些标准中，根据局域网的多种类型，规定了各自的拓扑结构、介质访问控制方法、帧的格式和操作等内容。目前主要的 IEEE 802 标准包括：

IEEE 802.1 是局域网的体系结构、网络管理和网际互连协议。IEEE 802.2 集中了数据链路层中与介质无关的 LLC 协议。涉及与介质访问有关的协议，则根据具体网络的介质访问控制方法分别处理，其中主要的 MAC 协议有：IEEE 802.3 载波监听多路访问/冲突检测 CSMA/CD 访问方法和物理层协议、IEEE 802.4 令牌总线 (Token Bus) 访问方法和物理层协议、IEEE 802.5 令牌环 (Token Ring) 访问方法和物理层协议，IEEE 802.6 关于城域网

的分布式队列双总线 DQDB (Distributed Queue Dual Bus) 的标准等。IEEE 802 标准系列中各个子标准之间的关系如图 8-12 所示。

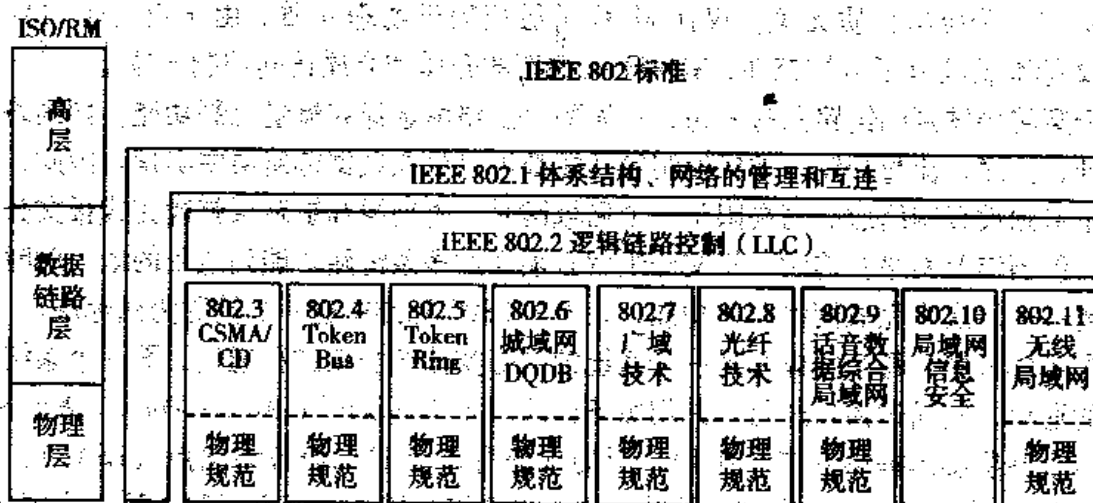


图 8-12 IEEE 802 标准系列

8.2.2 IEEE 802.2: 逻辑链路控制子层

局域网的底层只提供尽力的数据报业务，不保证数据的可靠传输，尽管这对有些系统来说已经足够了，但仍有系统希望底层网络能提供更好的服务。为此，IEEE 802 委员会定义了运行在介质访问控制 (MAC) 子层之上的逻辑链路控制 (LLC) 子层。

LLC 子层负责处理诸如差错控制、流量控制等问题，保证数据的可靠传输；同时向上提供统一的数据链路层接口，从而屏蔽各种物理网络的实现细节。LLC 可提供 3 种服务：不确认的无连接服务，确认的无连接服务和确认的面向连接的服务。

不确认的无连接服务，在数据传输前双方不需要建立连接，接收方收到数据后也不要求进行应答，因而链路层不保证数据的正确传送。这种服务形式可用于如下场合：物理网络可靠性极高，不需要在链路层上专门进行差错控制；网络层本身提供不确认无连接服务，因而对链路层提供的服务要求不高；某些实时通信系统允许数据单元的偶然丢失，但要求数据及时传递，如数字话音传输、实时数据采集等。

确认的无连接服务，在数据传输前双方不需要建立连接，但接收方对收到的每一帧数据都要给出应答，因而链路层保证数据的正确传送。这种服务形式可用于如下场合：每次发送的数据量少，不值得专门为此建立连接，但要求数据可靠传送；有些实时系统要求迅速可靠地传送数据，来不及预先建立连接；在广播网络中不需要建立连接，但要求数据可靠传输。

确认的面向连接服务，在数据传输前双方需建立连接，接收方必须对收到的帧进行检错、排序和应答，发送方对出错的帧要进行重发，因而链路层保证全部数据正确有序地传送。这种服务形式可用于如下场合：物理网络可靠性差，在链路层上提供较好的服务可以减轻网络层的负担；需要进行长数据交换（如文件传输），在链路层上保证各个帧正确有序地传送可以减轻较高层上组装的难点和工作量。

8.2.3 IEEE 802.3: CSMA/CD

IEEE 802.3 是为采用二进制指数退避和 1-坚持 CSMA/CD 协议的基带总线局域网制定的标准。在低负荷时,如介质空闲时,要发送数据帧的站点能立即发送;在重负荷时,仍能保证系统的稳定性。

世界上第一个 CSMA/CD 局域网是由美国 Xerox 公司于 1975 年成功研制,采用无源总线电缆作为传输介质,被称为以太网 (Ethernet)。以太 (Ether) 在历史上是指一种可以传播电磁波的介质。此后, Xerox 公司与 DEC 公司、Intel 公司合作,提出了以太网产品规范,并成为 IEEE 802 标准系列中第一个局域网标准。

以太网所采用的介质访问控制方法就是后来成为 IEEE 802.3 标准的载波监听多路访问/冲突检测 (CSMA/CD), 所以 IEEE 802.3 标准与以太网标准有很多相似之处。但正式发布的 IEEE 802.3 标准和以太网标准并不完全相同,因此把“以太网”同“IEEE 802.3 局域网”或“CSMA/CD”等同起来就不太严格了,不过在不涉及网络协议的细节时,也把 IEEE 802.3 局域网简称为以太网。

1. IEEE 802.3 物理层规范

IEEE 802.3 委员会在定义可选的物理配置方面表现了极大的多样性和灵活性。为了区分各种可选用的实现方案,该委员会给出了一种简明的表示方法:

(数据传输速率 (Mbps)) (信号方式) (最大段长度 (百米))

如 10BASE5、10BASE2、10BROAD36。但 10BASE-T 和 10BASE-F 有些例外,其中的 T 表示双绞线、F 表示光纤。IEEE 802.3 的 10 Mbps 可选方案见表 8-1。

(1) 10BASE5 和 10BASE2。与 10BASE5 一样, 10BASE2 也使用 50 Ω 同轴电缆和曼彻斯特编码,数据速率为 10Mbps。两者的区别在于 10BASE5 使用粗缆 ($\Phi 10\text{mm}$), 10BASE2 使用细缆 ($\Phi 5\text{mm}$)。由于两者数据速率相同,所以可以使 10BASE5 电缆段和 10BASE2 电缆段共存于一个网络中。

表 8-1

IEEE 802.3 的 10 Mbps 可选方案

	10BASE5	10BASE2	10BASE-T	10BROAD36	10BASE-F
传输介质	基带同轴电缆	基带同轴电缆	非屏蔽双绞线	宽带同轴电缆	850nm 光纤对
编码技术	曼彻斯特码	曼彻斯特码	曼彻斯特码	差分 PSK 码	曼彻斯特码
拓扑结构	总线	总线	星形	总线/树形	星形
最大段长	500m	185m	100m	1800m	500m
每段节点	100	30	—	—	33

(2) 10BASE-T。10BASE-T 定义了一个物理上的星形拓扑网,其中央节点是一个集线器,每个节点通过一对双绞线与集线器相连。集线器的作用类似于一个转发器,它接收来

自一条线上的信号并向其它的所有线转发。由于任意一个站点发出的信号都能被其它所有站点接收，若有两个站点同时要求传输，冲突就必然发生。所以，尽管这种策略在物理上是一个星形结构，但从逻辑上看与 CSMA/CD 总线拓扑的功能是一样的。

(3) 10BROAD36。10BROAD36 是 802.3 中惟一针对宽带系统的规范，它采用双电缆带宽或中分带宽的 75ΩCATV 同轴电缆。从端出发的段的最大长度为 1800 米，由于是单向传输，所以最大的端一端距离为 3600 米。

(4) 10BASE-F。10BASE-F 是 802.3 中关于以光纤作为介质的系统的规范。该规范中，每条传输线路均使用一对光纤，每条光纤采用曼彻斯特编码传输一个方向上的信号。每一位数据经编码后，转换为一对光信号元素（有光表示高、无光表示低），所以，一个 10Mbps 的数据流实际上需要 20Mbaud 的信号流。

2. CSMA/CD 总线的实现模型

IEEE 802.3 是一个使用 CSMA/CD 介质访问控制方法的局域网标准。CSMA/CD 总线的实现模型如图 8-13 所示，它对应于 ISO/RM 的最低两层。从逻辑上可以将其划分为两大部分：一部分由 LLC 子层和 MAC 子层组成，实现 OSI/RM 的数据链路层功能；另一部分实现物理层功能。

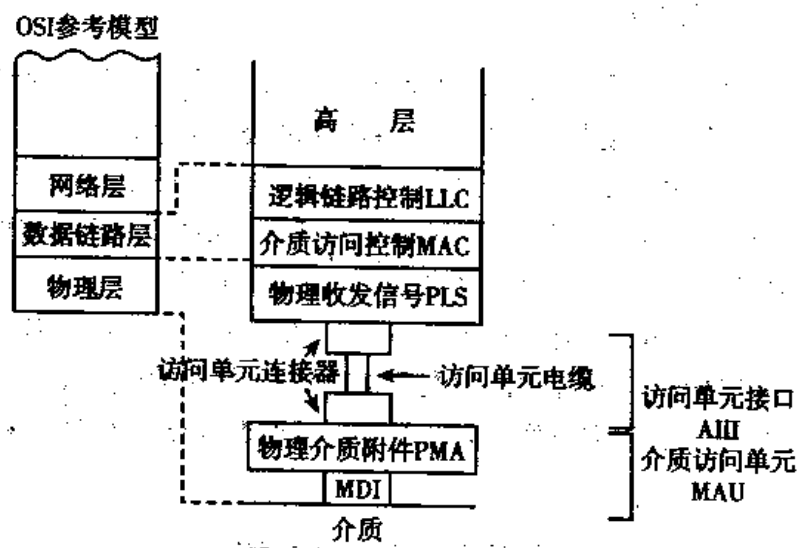


图 8-13 CSMA/CD 总线的实现模型

把依赖于介质的特性从物理层中分离出来的目的，是要使得 LLC 子层和 MAC 子层能适用于各类不同的介质。

物理层内定义了两个兼容接口：依赖于介质的介质相关接口 MDI 和访问单元接口 AUI。MDI 是一个同轴电缆接口，所有站点都必须遵循 IEEE 802.3 定义的物理介质信号的技术规范，与这个物理介质接口完全兼容。由于大多站点都设在离电缆连接处有一段距离的地方，在与电缆靠近的 MAC 中只有少量电路，而大部分硬件和全部的软件都在站点中，AUI 的存在为 MAC 和站点的配合使用带来了极大的灵活性。

MAC 子层和 LLC 子层之间的接口提供每个操作的状态信息，以供高一层差错恢复规程所用。MAC 子层和物理层之间的接口，提供包括成帧、载波监听、启动传输和解决争用、在两层间传送串行比特流的设施及用于定时等待等的功能。

3. IEEE 802.3 MAC 帧格式

MAC 帧是在 MAC 子层实体间交换的协议数据单元。IEEE 802.3 MAC 帧的格式如图 8-14 所示。

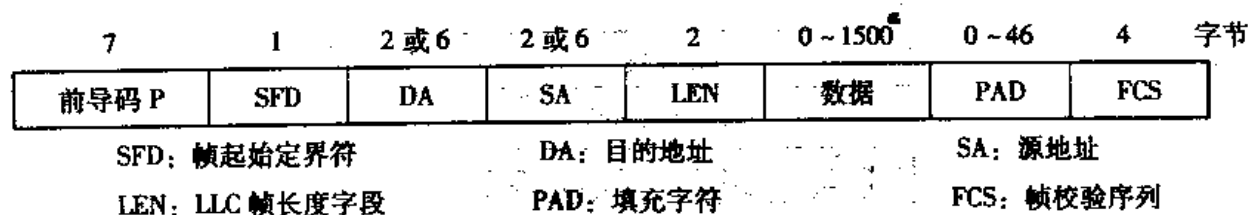


图 8-14 IEEE 802.3 MAC 帧格式

IEEE 802.3 MAC 帧中包括前导码 P、帧起始定界符 SFD、目的地址 DA、源地址 SA、表示数据字段字节数长度的字段 LEN、要发送的数据字段、填充字段 PAD 和帧校验序列 FCS 等 8 个字段。这 8 个字段中除了数据字段和填充字段外，其余的长度都是固定的。

前导码字段 P 占 7 个字节，每个字节的比特模式为“10101010”，用于实现收发双方的时钟同步。帧起始定界符字段 SFD 占 1 个字节，其比特模式为“10101011”，它紧跟在前导码后，用于指示一帧的开始。前导码的作用是使接收端能根据“1”、“0”交变的比特模式迅速实现比特同步，当检测到连续两位“1”（即读到帧起始定界符字段 SFD 最末两位）时，便将后续的信息递交给 MAC 子层。

地址字段包括目的地址字段 DA 和源地址字段 SA。目的地址字段占 2 个或 6 个字节，用于标识接收站点的地址，它可以是单个的地址，也可以是组地址或广播地址。DA 字段最高位为“0”表示单个地址，该地址仅指定网络上某个特定站点；DA 字段最高位为“1”、其余位不为全“1”表示组地址，该地址指定网络上给定的多个站点；DA 字段为全“1”，则表示广播地址，该地址指定网络上所有的站点。源地址字段也占 2 个或 6 个字节，但其长度必须与目的地址字段的长度相同，它用于标识发送站点的地址。在 6 字节地址字段中，可以利用其 48 位中的次高位来区分是局部地址还是全局地址。局部地址是由网络管理员分配，且只在本网中有效的地址；全局地址则是由 IEEE 统一分配的，采用全局地址的网卡出厂时被赋予惟一的 IEEE 地址，使用这种网卡的站点也就具有了全球独一无二的物理地址。

长度字段 LEN 占两个字节，其值表示数据字段的字节数长度。数据字段的内容即为 LLC 子层递交的 LLC 帧序列，其长度为 0~1500 个字节。

为使 CSMA/CD 协议正常操作，需要维持一个最短帧长度，必要时可在数据字段之后、帧校验序列 FCS 之前以字节为单位添加填充字符。这是因为正在发送时产生冲突而中断的帧都是很短的帧，为了能方便地区分出这些无效帧，IEEE 802.3 规定了合法的 MAC 帧的最短帧长。对于 10 Mbps 的基带 CSMA/CD 网，MAC 帧的总长度为 64~1518 字节。由于除了数据字段和填充字段外，其余字段的总长度为 18 个字节，所以当数据字段长度为 0 时，填充字段必须有 46 个字节。

帧校验序列 FCS 字段是 32 位（即 4 个字节）的循环冗余码（CRC），其校验范围不包括前导码字段 P 及帧起始定界符字段 SFD。

4. IEEE 802.3 MAC 子层的功能

IEEE 802.3 标准提供了 MAC 子层的功能说明，内容主要有数据封装和介质访问管理两个方面。MAC 功能模块如图 8-15 所示。

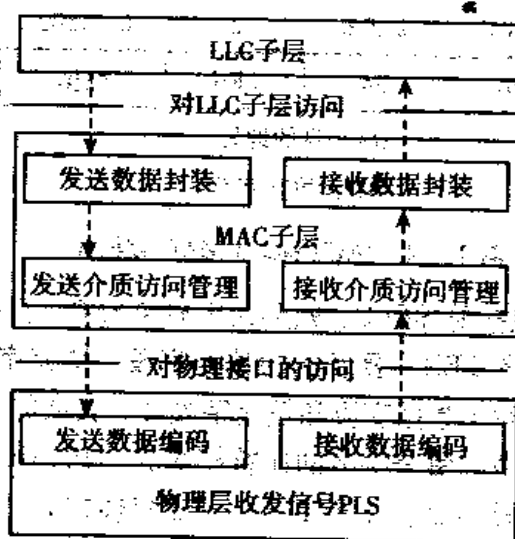


图 8-15 MAC 功能模块

数据封装（发送和接收数据封装）包括成帧（帧定界和帧同步）、编址（源地址及目的地址的处理）和差错检测（物理介质传输差错的检测）等；介质访问管理包括介质分配和竞争处理。

当 LLC 子层请求发送一数据帧时，MAC 子层的发送数据封装部分便按 MAC 子层的数据帧格式组帧。首先将一个前导码 P 和一个帧起始定界符 SFD 附加到帧的开头部分，填上目的地址和源地址，计算出 LLC 数据帧的字节数，填入数据长度计数字段 LEN。必要时还要将填充字符 PAD 附加到 LLC 数据帧后，以确保传送帧的长度满足最短帧长的要求。最后求出 CRC 校验码附加到帧校验序列 FCS 中。完成数据封装后的 MAC 帧，便可递交 MAC 子层的发送介质访问管理部分以供发送。

借助于监视物理层收发信号（PLS）部分提供的载波监听信号，发送介质访问管理设法避免发送信号与介质上其它信息发生冲突。在介质空闲时，经短暂的帧间延迟（提供给介质恢复时间）之后，就启动帧发送。然后，MAC 子层将串行位流送给 PLS 接口以供发送。PLS 完成产生介质上电信号的任务，同时监视介质和产生冲突检测信号。在没有争用的情况下，即可完成发送。发送完成后，MAC 子层通过 LLC 与 MAC 间的接口通知 LLC 子层，等待下一个发送请求。假如产生冲突，PLS 接通冲突检测信号，接着发送介质访问管理开始处理冲突。首先，它发送一串称为阻塞（Jam）码的位序列来强制冲突，由此保证有足够的冲突持续时间，以使其它与冲突有关的发送站点都得到通知。在阻塞信号结束时，发送介质访问管理就暂停发送，等待一个随机选择的时间间隔后再进行重发尝试。发送介质访问管理用二进制指数退避算法调整介质负载。最后，或者重发成功，或者在介质故障、过载的情况下，放弃重发尝试。

接收介质访问管理部分的功能是，首先由 PLS 检测到达帧，使接收时钟与前导码同步，并接通载波监听信号。接收介质访问管理部件要检测到达的帧是否错误，帧长是否超过最大长度，是否为 8 位的整倍数。还要过滤因冲突产生的碎片信号（即小于最短长度的帧）。

接收数据解封部分的功能，用于检验帧的目的地址字段，以确定本站点是否应该接收该

帧。如地址符合，将其送到 LLC 子层，并进行差错检验。

8.2.4 IEEE 802.4：令牌总线

符合 IEEE 802.3 标准的网络产品广泛应用于办公自动化系统，却无法应用到实时性很强的工厂自动化系统中，主要有两个原因：一是 IEEE 802.3 采用无序竞争机制，且采用二进制指数退避算法解决冲突，无法预知一个帧要经过多长时间才能发送出去；二是 IEEE 802.3 没有优先级，无法保证重要信息的优先传送。

环网中每个站点轮流发送数据，还可以限定每个站每次发送的帧数或时间，可以预知一个帧最多经过多长时间能够发送出去；另外环网中数据帧和令牌都带有优先级，只有优先级不低于令牌优先级的帧才能获准发送，这就可以保证重要信息的优先传送。但从网络的可靠性来看，由于环接口是有源器件，其可靠性不如总线网高；另外环形也不适用于大多数装配生产线的线性拓扑结构。

为此设想将总线网和环网的优点集中起来，物理上采用总线结构以获得较高的物理可靠性，但在逻辑上采用令牌环的工作原理，使各站轮流获得发送权，这就是 IEEE 802.4 标准定义的令牌总线网（Token Bus）。

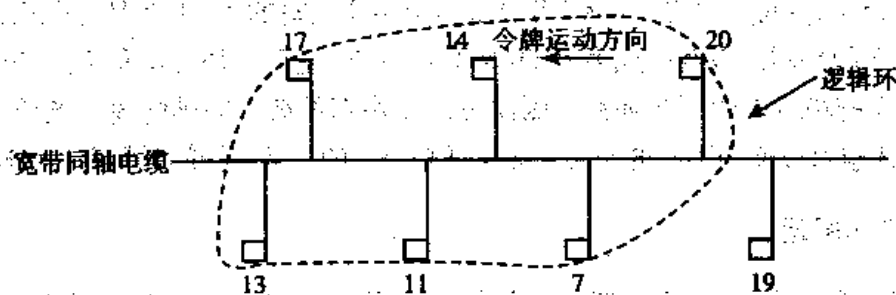


图 8-16 令牌总线

1. 工作原理

如图 8-16 所示，在物理上，令牌总线是一根线形或树形的电缆，在其上连接着若干站点。但在逻辑上，所有工作的站点都组织在一根逻辑环里面（虚线所示的环），且被按照地址从高到低的顺序进行排列，最低地址后面紧接着最高地址，环中每个站点只知道它的直接前驱和直接后继的地址。

令牌是按地址从高到低的顺序进行传递的，当一个站点发完数据后，在令牌中填入其后继站的地址，并传给后继站；后继站有数据就可以发送，没有数据则立即将令牌往下传；因此，令牌在逻辑环中循环流动，各站轮流发送，没有冲突。令牌总线中的令牌需要携带地址。因为总线本质上是一个广播信道，事实上所有的站都收到了总线上的数据，只是将地址与自身地址不相符的帧丢掉而已。同样，令牌也能被所有的站点收到，但只有地址相符的站才允许获得令牌。因此在令牌总线中，站的物理位置并不重要，在环上相邻的站，在物理连接上并不需要是相邻的。

令牌总线的控制比较复杂。在系统启动时，逻辑环并不存在，需要进行环初始化，使得有且仅有一个站点获得令牌加入环中；同时逻辑环是一个动态的环，不断地有新的站点要求

加入, 同时也不断地有站点因为关机或故障从环中删除, 因此还要实现站的动态插入和删除; 另外, 网络出现故障如令牌丢失、地址重复、重复令牌时, 必须能做出相应的处理。

2. 故障处理

(1) 逻辑环中断。逻辑环中断, 一般是由于环上某些站故障、关机或总线断开, 致使令牌无法按照原有的顺序传递。这种故障令牌传递算法即可解决, 当最后逻辑环重建失败时, 需要检查电缆或设备硬件是否有问题。

(2) 令牌丢失。当令牌持有站出现故障时, 就会造成令牌丢失, 其表现是总线上没有站点发送数据。每个站点利用不活动计时器来计算总线空闲的时间, 每当总线上出现信号时即复位计时器, 而当计时器超时, 即发送一个“Claim Token”控制帧, 进行环初始化。

(3) 重复令牌。当某个持有令牌的站发现其它站正在发送数据时, 即丢弃自己的令牌。这样, 如环上有多个令牌, 则经过一段时间后, 最后只剩下一个令牌; 如果不幸令牌全部丢失, 那么总线空闲一段时间后, 就会有站点发送“Claim Token”帧, 进行环初始化。

8.2.5 IEEE 802.5: 令牌环

令牌环网 (Token Ring) 最早于 1969 年在美国贝尔实验室的 Newhall 环上采用, 1985 年 IBM 公司推出了 IBM 令牌环网, 该网络成为 IEEE 802.5 标准的基础。环并不是真正的广播介质, 而是由一系列点一点链路组成的闭合环路, 因而可以使用双绞线、同轴电缆、光纤等多种传输介质, 甚至环的各段也可以使用不同的介质, 而且环是公平的, 信道访问时间有一个确定的上限。

1. 令牌环工作原理

(1) 环长的比特度量。环的长度往往折算成比特数来度量, 以比特度量的环长反映了环上能容纳的比特数量。假如某站点从开始发送数据帧到该帧发送完毕所经历的时间, 等于该帧从开始发送经循环返回到发送站点所经历的时间, 则数据帧的所有比特正好布满整个环路。换言之, 当数据帧的传输时延等于信号在环路上的传播时延时, 该数据帧的比特数就是以比特度量的环路长度。

所谓一个比特的物理长度是指 1 比特在环上占有的长度。如果环的数据速率是 $R \text{ Mb/s}$, 则每 $1/R_{\mu\text{s}}$ 发送 1 比特, 同轴电缆上典型的信号传播速度为 $200 \text{ m}/\mu\text{s}$, 则 1 比特在环上占据的物理长度即为 $200/R$ 米。对于一个速率为 1 Mb/s 的环网, 每比特物理长度为 200 米, 如果环周长为 1000 米, 不考虑环接口上的延迟, 则环上同时只能容纳 5 比特, 即环的比特长度为 5。

在令牌环网中, 发送站可以一边发送数据, 一边将返回的数据取消, 因此对帧的最大长度没有限制, 但对环的最小长度却是有限制的, 因为环的长度至少要能容纳下整个令牌在其上轮转。

实际操作过程中, 环路上的每个接口都会引入延迟。接口延迟时间的存在, 相当于增加了环路上的信号传播时延, 也即等效于增加了环路的比特长度。所以, 接口引入的延迟同样也可以用比特来度量。一般, 环路上每个接口相当于增加 1 位延迟。环接口处的延迟也计入环的长度中, 如环上共有 10 个站点, 每个站的环接口处引入 1 比特延迟, 则整个环可同时容纳 $5 + 10 = 15$ 比特。环的比特长度就是指环上能同时容纳的比特数, 上述 1 Mb/s 的环的比特长度即为 15 比特。由此, 可给出以比特度量的环长计算式:

$$\begin{aligned}\text{环的比特长度} &= \text{信号传播时延} \times \text{数据传输速率} + \text{接口延迟位数} \\ &= \text{环路介质长度} \times 5(\mu\text{s}/\text{km}) \times \text{数据传输速率} + \text{接口延迟位数}\end{aligned}$$

式中 $5\mu\text{s}/\text{km}$ 即信号传播速度 $200\text{m}/\mu\text{s}$ 的倒数。例如, 某令牌环介质长度为 10Km , 数据传输速率为 4Mbps , 环路上共有 50 个站点, 每个站点的接口引入 1 位延迟, 则可计算得:

$$\begin{aligned}\text{环的比特长度} &= 10(\text{km}) \times 5(\mu\text{s}/\text{km}) \times 4(\text{Mbps}) + 1(\text{bit}) \times 50 \\ &= 10 \times 5 \times 10^{-6} \times 4 \times 10^6 + 1 \times 50 \\ &= 200 + 50 = 250(\text{bit})\end{aligned}$$

如果由于环路介质长度太短或站点数太少, 以至于环路的比特长度不能满足数据帧长度的要求, 则可以在每个环接口引入额外的延迟, 如使用移位寄存器等。

(2) 环形网络。如图 8-17 所示, 令牌环在物理上是一个由一系列环接口和这些接口间的点一点链路构成的闭合环路, 各站点通过环接口连到网上。对介质具有访问权的某个发送站点, 通过环接口出径链路将数据帧串行发送到环上; 其余各站点边从各自的环境接口入径链路逐位接收数据帧, 同时通过环接口出径链路再生、转发出去, 使数据帧在环上从一个站点至下一个站地环行, 所寻址的目的站点在数据帧经过时读取其中的信息; 最后, 数据帧绕环一周返回发送站点, 并由其从环上撤除所发的数据帧。

由点一点链路构成的环路虽然不是真正意义上的广播介质, 但环上运行的数据帧仍能被所有的站点接收到, 而且任何时刻仅允许一个站点发送数据, 因此同样存在发送权竞争问题。为了解决竞争, 可以使用一个称为令牌 (Token) 的特殊比特模式, 使其沿着环路循环。规定只有获得令牌的站点才有权发送数据帧, 完成数据发送后立即释放令牌以供其它站点使用。由于环路中只有一个令牌, 因此任何时刻至多只有一个站点发送数据, 不会产生冲突。而且, 令牌环上各站点均有相同的机会公平地获取令牌。

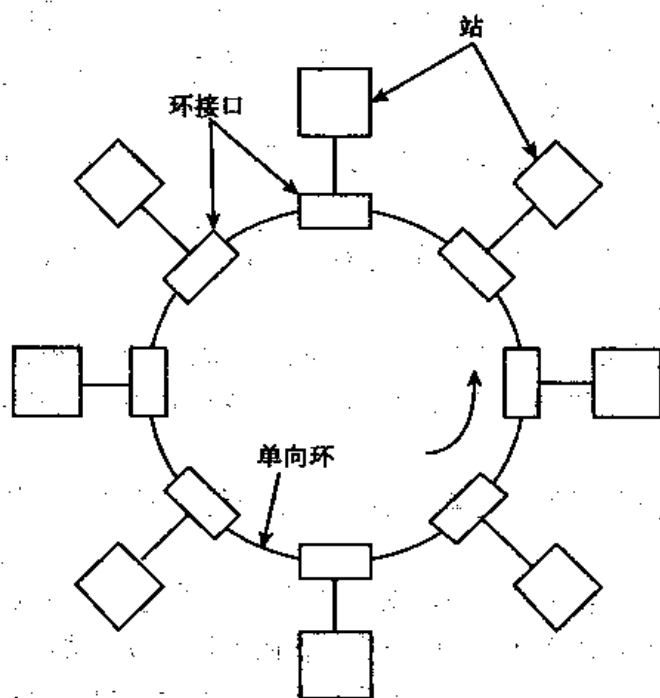


图 8-17 令牌环结构

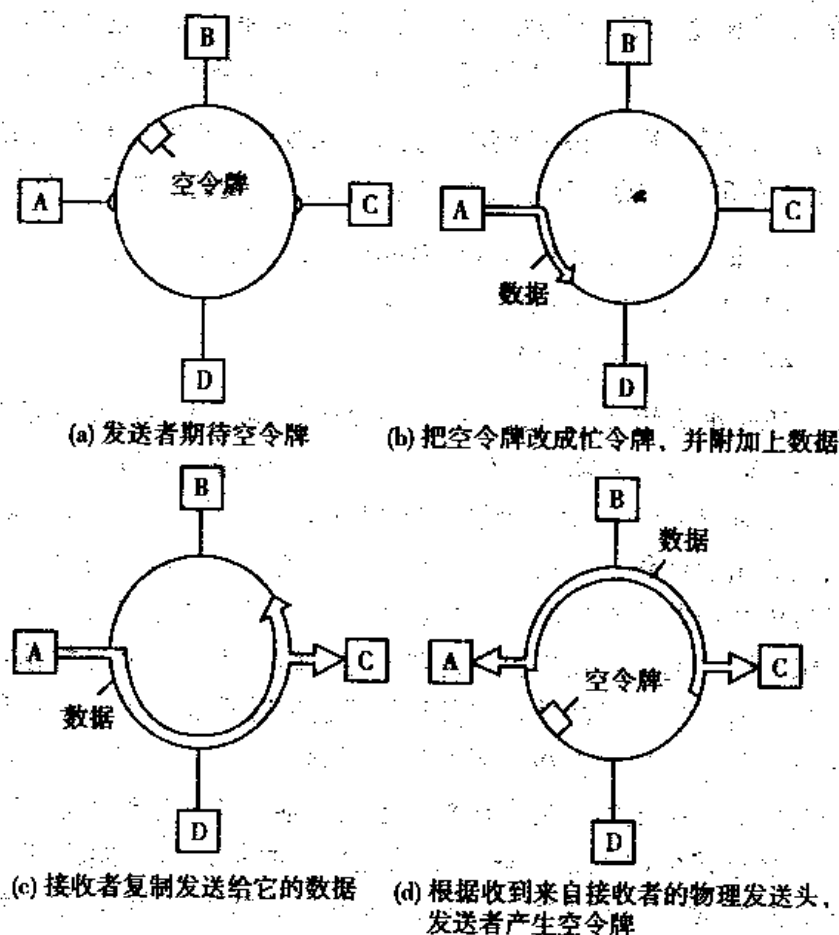


图 8-18 令牌环的操作过程

令牌环的操作过程如图 8-18 所示。

① 网络空闲时，只有一个令牌在环路上绕行。令牌是一个特殊的比特模式，其中包含一位“令牌/数据帧”标志位，标志位为“0”表示该令牌为可用的空令牌，标志位为“1”表示有站点正占用令牌在发送数据帧。

② 当一个站点要发送数据时，必须等待并获得一个令牌，将令牌的标志位置为“1”，随后便可发送数据。

③ 环路中的每个站点边转发数据，边检查数据帧中的目的地址，若为本站点的地址，便读取其中所携带的数据。

④ 数据帧绕环一周返回时，发送站将其从环路上撤销。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧，否则释放缓冲区中的待确认帧。

⑤ 发送站点完成数据发送后，重新产生一个令牌传至下一个站点，以使其它站点获得发送数据帧的许可权。

(3) 令牌环的维护。令牌环的故障处理功能主要体现在对令牌和数据帧的维护上。令牌本身就是比特串，绕环传递过程中也可能受干扰而出错，以致造成环路上无令牌循环的差错；另外，当某站点发送数据帧后，由于故障而无法将所发的数据帧从网上撤销时，又会造成网上数据帧持续循环的差错。令牌丢失和数据帧无法撤销，是环网上最严重的两种差错，可以通过在环路上指定一个站点作为主动令牌管理站，以此来解决这些问题。

主动令牌管理站通过一种超时机制来检测令牌丢失的情况，该超时值比最长的帧为完全遍历环路所需的时间还要长一些。如果在该时段内没有检测到令牌，便认为令牌已经丢失，管理站将清除环路上的数据碎片，并发出一个令牌。

为了检测到一个持续循环的数据帧，管理站在经过的任何一个数据帧上置其监控位为1，如果管理站检测到一个经过的数据帧的监控位已经置为1，便知道有某个站未能清除自己发出的数据帧，管理站将清除环路上的残余数据，并发出一个令牌。

(4) 令牌环的特点。令牌环网在轻负荷时，由于存在等待令牌的时间，故效率较低；但在重负荷时，对各站公平访问且效率高。

考虑到帧内数据的比特模式可能会与帧的首尾定界符形式相同，可在数据段采用比特插入法或违法码法，以确保数据的透明传输。

采用发送站点从环上收回帧的策略，具有对发送站点自动应答的功能；同时这种策略还具有广播特性，即可有多个站点接收同一数据帧。

令牌环的通信量可以加以调节，一种方法是通过允许各站点在其收到令牌时传输不同量的数据；另一种方法是通过设定优先权使具有较高优先权的站点先得到令牌。

2. IEEE 802.5 令牌环

IEEE 802.5 标准规定了令牌环的介质访问控制子层和物理层所使用的协议数据单元格式和协议，规定了相邻实体间的服务及连接令牌环物理介质的方法。

(1) IEEE 802.5 MAC 帧格式。IEEE 802.5 令牌环的 MAC 帧有两种基本格式：令牌帧和数据帧（如图 8-19 所示）。

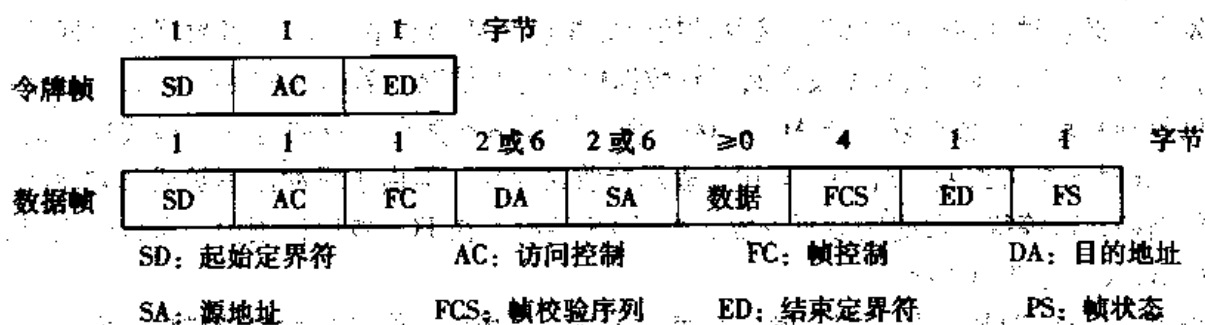
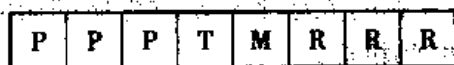


图 8-19 IEEE 802.5 MAC 帧格式

令牌帧只有 3 个字节长，数据帧则可能很长。这两种帧都有一对起始定界符 SD 和结束定界符 ED 用于确定帧的边界，它们中各有 4 位采用曼彻斯特编码中不使用的违法码（“高一高”电平对和“低—低”电平对），以实现数据的透明传输。

访问控制字段 AC 的格式如下：



其中 T 为令牌/数据帧标志位，该位为“0”表示令牌，为“1”表示数据帧。当某个站点要发送数据并获得了一个令牌后，将 AC 字段中的 T 位置“1”。此时，SD、AC 字段就作为数

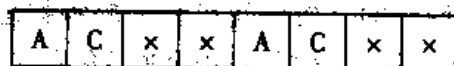
据帧的头部，随后便可发送数据帧的其余部分。M 为监控位，用于检测环路上是否存在持续循环的数据帧。PPP (3 比特) 为优先级编码，当某站点要发送一个优先级为 n 的数据帧时，必须获得一个 PPP 编码值 $\leq n$ 的令牌才可发送。RRR (3 比特) 为预约编码，当某站点要发送数据帧而信道又不空时，可以在转发其它站点的数据帧时将自己的优先级编码填入 RRR 中，待该数据帧发送完毕，产生的令牌便具有了预约的优先级。若 RRR 已被其它站点预约了更高的优先级，则不可再预约。将令牌的优先级提升了的站点，在数据帧发送完毕后，还要负责将令牌的优先级降下来，这样就使优先级较低的站点也有发送数据帧的机会。

帧控制字段 FC 中的前两位标志帧的类型。“01”表示为一般信息帧，即其中的数据字段为上层提交的 LLC 帧；“00”表示为 MAC 控制帧，此时其后的 6 位用以区分控制帧的类型。信息帧只发送给地址字段所指示的目的站点，控制帧则发送给所有站点。控制帧中不含数据字段。

数据字段的长度没有下限，但其上限受站点令牌持有时间的限制。令牌持有时间的缺省值为 10 毫秒，数据帧必须在该时段内发送完，超过令牌持有时间，必须释放令牌。

32 位的帧校验序列 FCS 的作用范围自帧控制字段 FC 起至 FCS 止，其中不包括帧首 (SD、AC 字段) 和帧尾 (ED、FS 字段)。

帧状态字段 FS 的格式如下：



字段中设置了两位 A 和两位 C，其余 4 位未定义。A 位为地址识别位，发送站发送数据帧时将该位置“0”，接收站确认目的地址与本站相符后将该位置“1”。C 为帧复制位，发送站发送数据帧时将该位置“0”，接收站接收数据帧后将该位置“1”。当数据帧返回发送站时，A、C 位作为应答信号使发送站了解数据帧发送的情况。若返回的 AC = 11，表示接收站已收到并复制了数据帧；若 AC = 00，表示接收站不存在（目的地址有错或接收站未工作），此时不必再重发；若 AC = 10，表示接收站存在，但由于缓冲区不够或其它原因未接收数据帧，可等待一段时间后再重发。由于 FS 字段不在 FCS 校验范围内，所以使用两套重复的 A、C 以提高可靠性。

结束定界符 ED 除了用于指示帧的结束边界外，其最后一位 E 还用作差错位，发送站发送数据帧时将该位置“0”。此后，任何一个站点在转发该数据帧时，通过 FCS 校验一旦发现错误，都可以将 E 位置“1”。这样，当数据帧返回时，发送站便可了解数据帧的传输情况。

(2) IEEE 802.5 的介质访问控制功能。令牌环局域网协议标准包括四个部分：逻辑链路控制 (LLC)、介质访问控制 (MAC)、物理层 (PHY) 和传输介质；IEEE 802.5 规定了后面三个部分的标准。令牌环的介质访问控制功能如下：

① 帧发送：采用沿环传递令牌的方法来实现对介质的访问控制，取得令牌的站点具有发送一个数据帧或一系列数据帧的机会。

② 令牌发送：发送站完成数据帧发送后，等待数据帧的返回。在等待期间，继续发送填充字符。一旦源地址与本站相符的数据帧返回后，即发送令牌。令牌发送之后，该站仍保持在发送状态，直到该站发送的所有数据帧从环路上撤销为止。

③ 帧接收：若接收到的帧为信息帧，则将 FC、DA、SA、Data 及 FS 字段复制到接收缓冲池中，并随后将其转至适当的子层。

④ 优先权操作：访问控制字段中的优先权位和预约位配合工作，使环路服务优先权与环上准备发送的 PDU 最高优先级匹配。

(3) IEEE 802.3、IEEE 802.4 与 IEEE 802.5 的比较。IEEE 802.3、IEEE 802.4 和 IEEE 802.5 这 3 种局域网标准采用了大致相同的技术并且具有大致相似的性能。

IEEE 802.3 总线网由于结构简单、安装容易、协议简单及总线可靠性高而成为应用最为广泛的局域网，在轻负载时可以获得很好的延迟特性，甚至可以达到零延迟。

但 IEEE 802.3 总线网在网络负载增加时，大量的冲突会引起网络性能下降；随机争用和退避等待机制无法预知数据传输的最大延迟，也不提供优先级支持，因此不适用实时系统；大量使用模拟器件和模拟技术（如用于载波监听及冲突检测的收发器），增加了设备的复杂性及不可靠性；为了进行冲突检测必须限制帧的最小长度，处理短帧时需要添加一定的填充字符，增加了额外开销；电缆长度被限制在 2.5 公里以内，网络规模不易扩充。

IEEE 802.4 令牌总线网使用可靠性较高的宽带同轴电缆，可以同时支持多个通道；使用令牌轮换发送权以避免冲突，在重载下可以获得很高的传输效率；采用公平的优先级机制，保证各种优先级的数据都能占有一定的带宽发送，并可预知数据传输的最大延迟，适用于实时系统；不需限制帧的最小长度，但对最大帧长有限制。

但 IEEE 802.4 令牌总线网也使用了大量的模拟设备和技术（如调制解调器、宽带放大器等），设备复杂而且代价昂贵；即使低负载时也必须等待令牌才能发送，延迟特性较差；采用分布式的控制策略，协议相当复杂；这种网络用户使用得比较少。

IEEE 802.5 令牌环网使用点一点连接，可以使用多种传输介质，而且可以采用全数字技术；使用线路中心的令牌环网是唯一可以自动检测和隔离网络故障的局域网；支持优先级，支持短帧，最大帧长只受令牌持有时间限制，在重载下可以获得很高的传输效率。

但 IEEE 802.5 令牌环网在低负载下时延较大，这与令牌总线网相同；它的优先级策略对低优先级不公平；采用集中式控制，对监控站的可靠性要求较高，监控站成为网络中最为脆弱的部分。

因此，单纯从性能角度比较这三种局域网技术的优劣是没有意义的，对局域网技术的选择往往要从网络性能、网络用途、网络规模及网络代价等多方面来综合考虑。在很重的负载下 IEEE 802.3 总线网彻底不能用，而基于令牌的 IEEE 802.4 总线网或 IEEE 802.5 环网却可以达到接近于 100% 的效率；若负载范围是从轻到中等，则 3 种局域网都可以胜任。

8.2.6 IEEE 802.6：分布队列双总线

由于城域网的覆盖范围远远超出局域网的覆盖范围，无法使用前面介绍的局域网技术来构建城域网，IEEE 为都市建网定义了一种城域网标准，即 IEEE 802.6 标准的分布队列双总线（Distributed-Queue Dual Bus, DQDB）。

DQDB 的基本结构如图 8-20 所示。两条平行的单向总线穿绕于整个城市，每个站点同时连接到两条总线上。每条总线都有一个首端，它能产生一个稳定的 53 字节的信元流。每个信元从首端沿着总线往下传，当它到达终点时，就从总线上消失。

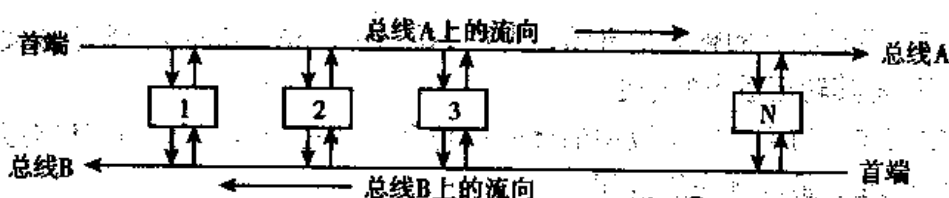


图 8-20 DQDB 的基本结构

每个信元带有 44 字节的有效载荷。每个信元中带有两个协议位：Busy（繁忙），其值为 1 表示该信元已被占用；Request（请求），当站点想发请求时可将其置为 1。

在发送信元之前，站点必须知道目的站点位于其左方还是右方。如果目的站点位于右方，发送站点就使用总线 A，否则就使用总线 B。数据通过硬件或运算电路输入到相应的总线中，因此，一个站点失效不会影响整个网络的正常运行。

与所有其它 IEEE 802 局域网标准不同，IEEE 802.6 并不贪婪。在其它的网络中，如果站点获得机会发送，它就发送。而在 IEEE 802.6 中，站点按照准备好发送的顺序进行排队，并按照先进先出（FIFO）的原则进行发送。因此，最为关键的问题就是在没有集中排队的情况下，如何实现先进先出。

DQDB 采取的基本原则是站点必须有礼貌：在其下方的站点完全发送完后自己才发送，这是为了防止下列情况的发生：离首端最近的站点把经过它的所有空信元全部捕获并填入内容，致使其后的站点处于饥饿状态。因为两条总线的工作机制完全相同，为了简单起见，这里只讨论总线 A 上的传送。

为了模拟 FIFO 队列，每个站点均保持有两个计数器：请求计数器（Request Counter, RC）和倒计时计数器（Countdown Counter, CD）。RC 对本站下方未响应的请求进行计数，直到本站有数据要发送为止。在停止计数的同时，将 RC 的值复制到 CD 中，然后 RC 置为 0，并对此后下方的请求进行计数。例如，若站点 K 中 $CD=3$ 、 $RC=2$ ，站点 K 先放过 3 个空信元给其下方的站点，此时 K 可以发送，然后再放过 2 个或更多的信元。为了简化问题，假定任一时刻站点只能有 1 个信元进行发送。

在发送信元之前，站点必须通过设置相反总线上某个信元的请求（Request）位来进行预约（即总线 A 上的传送必须先在线 B 中设置 Request 位）。当该信元沿着相反总线传播时，一路上经过的所有站点都会看到从而将本地的 RC 值加 1。

图 8-21 用一个例子来说明 DQDB 的工作过程。最初，所有站点的 RC 值均为 0，并且也无信元进行排队，如图（a）所示。后来站点 D 发出一个请求，使站点 C、B、A 的 RC 均加 1，如图（b）所示。紧接着，B 发出一个请求，将其 RC 当前值拷贝到 CD 中，各站点的状态如图（c）所示。

此时总线 A 的首端产生一个空信元。当经过 B 时，B 注意到其 $CD > 0$ ，所以它不能使用这个空信元（当某个站点有信元进行排队时，其 CD 值代表了该信元在队列中的位置，值为 0 时表示它位于队列的首端），于是将其 CD 值减 1。当该空信元经过 D 时，D 注意到其 $CD=0$ ，即它已在队列的首端，于是它将数据以或运算的形式输出到该空信元中，并将其 Busy 位置 1。空信元经过 $RC > 1$ 的站点时将 RC 值减 1。发送结束后的情况如图（d）所示。

当下一个空信元产生后经过 B 时，B 注意到它已位于队列的首端，于是便抓住信元进行

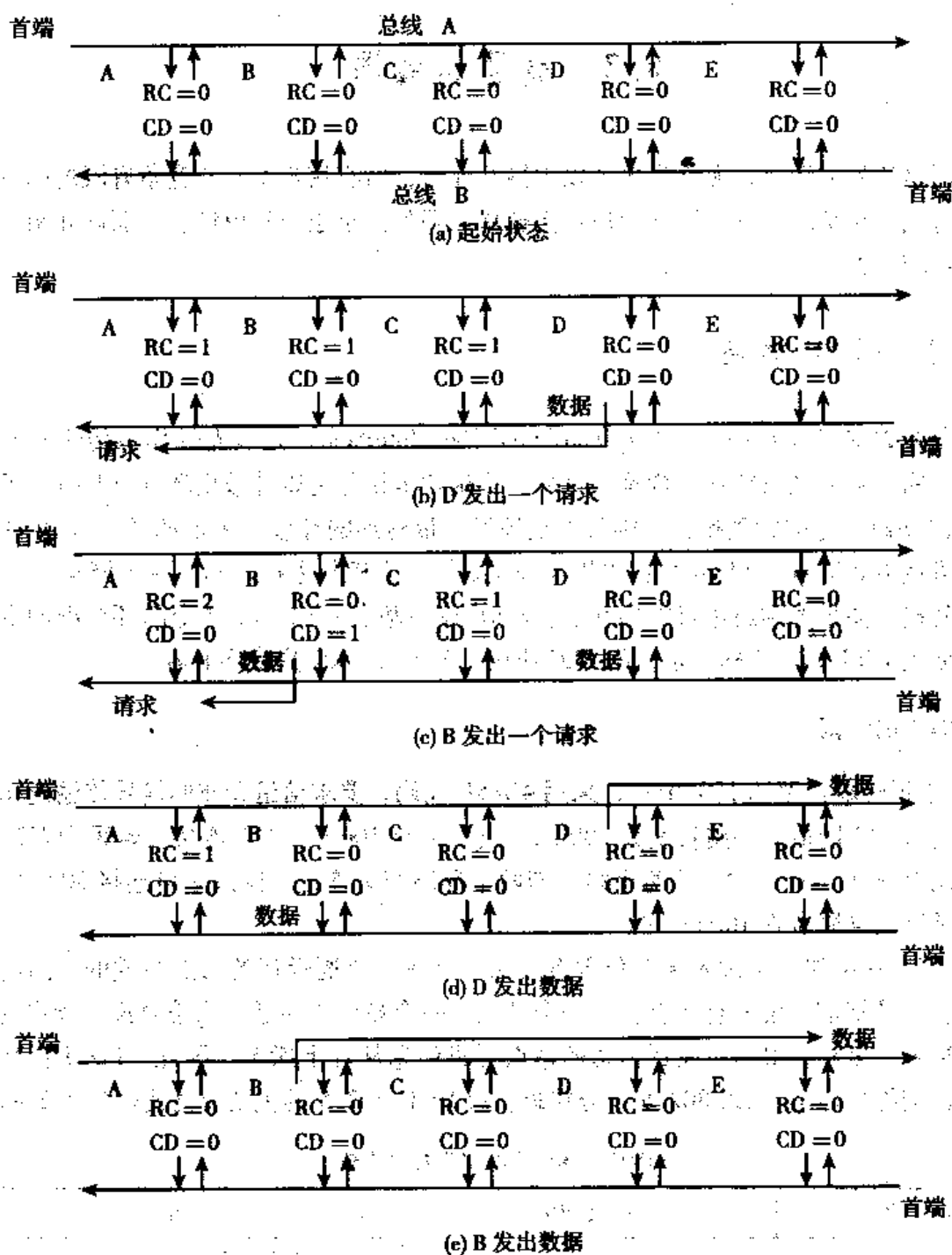


图 8-21 DQDB 的工作过程

发送 (将 Busy 位置 1), 如图 (e) 所示。在这种形式下, 站点排队依次发送, 而无须集中的队列管理器。

现在已经有很多城市中安装了 DQDB 城域网。典型的 DQDB 的覆盖范围是 160km, 数据传输速率为 44.736Mb/s (T3)。

8.3 高速局域网

由于网络流量的激增, 尤其当多个以太网互连时, 所有用户都参与竞争有限的同一个网络带宽, 造成网络负载加重, 因此用户对高速局域网的需求也与日俱增。下面就介绍一些典型的高速局域网技术。

8.3.1 FDDI 环网

光纤分布数据接口 FDDI (Fiber Distributed Data Interface) 是以光纤作为传输介质的高性能令牌环网, 它的逻辑拓扑结构是一个环, 更确切地说是逻辑计数循环环 (Logical Counter Rotating Ring), 它的物理拓扑结构可以是环形、带树形的环或带星形的环。FDDI 的数据传输速率可达 100 Mbps。FDDI 可在主机与外设之间、主机与主机之间、主干网与 IEEE 802 低速网之间提供高带宽和通用目的的互连。FDDI 使用基于 IEEE 802.5 令牌环标准的令牌传递协议, 使用 IEEE 802.2 标准定义的 LLC 协议, 与 IEEE 802 局域网兼容。

1. FDDI 的性能

FDDI 数据传输速率达 100 Mbps, 采用 4B/5B 编码, 要求信道介质的信号传输速率达到 125 Mbaud。FDDI 网最大环路长度为 200km, 最多可有 1000 个物理连接。若采用双环结构时, 站点间距离在 2km 以内, 且每个站点与两个环路都有连接, 则最多可连接 500 个站点, 其中每个单环长度限制在 100km 内。

FDDI 网络是由许多通过光传送介质连接成一个或多个逻辑环的站点组成的, 因此与令牌环类似, 也是把信息发送至环上, 从一个站到下一个站依次传递, 当信息经过指定的目的站时就被接收、复制, 最后, 发送信息的站点再将信息从环上撤销。因此, FDDI 标准和令牌环介质访问控制标准 IEEE 802.5 十分接近。FDDI 和 802.5 的主要特性比较见表 8-2。

表 8-2

FDDI 和 802.5 的主要特性比较

特 性	FDDI	802.5
介质类型	光纤	屏蔽双绞线
数据速率	100Mbps	4Mbps
可靠性措施	可靠性规范	无可靠性规范
数据编码	4B/5B 编码	差分曼彻斯特编码
编码效率	50%	80%
时钟同步	分布式时钟	集中式时钟
信道分配	定时令牌循环时间	优先级位
令牌发送	发送后产生新令牌	接收完后产生新令牌
环上帧数	可多个	最多一个

2. 数据编码

FDDI 规定了一种很特殊的定时和同步方法。在网络中使用的代码最好是那种信号状态变化频繁的代码, 这些状态变化使得接收器能够持续地与输入信号相适应, 这样就保证了发送设备和接收设备之间的同步。在 IEEE 802.3 标准中使用的曼彻斯特编码只有 50% 的效率, 因为每一比特都要求线路上有 2 次状态变化 (即 2 Baud)。如果采用曼彻斯特编码, 那么 100 Mbps 传输速率就要求 200 MBaud 的调制速率, 也即 200 MHz 的带宽。换言之, 曼彻斯特编码需要发送数据的 2 倍带宽。

考虑到生产 200 MHz 的接口和时钟设备会大大增加成本, ANSI 设计了一种称为 4B/5B 的代码。在这种编码技术中, 每次对 4 位数据进行编码, 每 4 位数据编码成 5 位符号, 用光的存在和不存在表示 5 位符号中每一位是 1 还是 0。这样, 对于 100 Mbps 的光纤网只需 125 MHz 的元件就可实现, 使效率提高到 80%。

为了得到信号同步, 可以采用二级编码的方法。即先按 4B/5B 编码, 然后再利用一种称为倒相的不归零制 NRZI 编码。该编码确保无论 4 比特符号为何种组合 (包括全“0”), 其对应的 5 比特编码中至少有 2 位“1”, 从而保证在光纤中传输的光信号至少发生两次跳变, 以利于接收端的时钟提取。这个原理类似于第 3 章中介绍过的差分编码。

5 比特编码的 32 种组合中, 实际只使用了 24 种, 其中的 16 种用作数据符号, 其余 8 种用作控制符号 (如帧的起始和结束符号等)。表 8-3 列出 4B/5B 编码的数据符号部分, 所有 16 个 4 位数据符号, 经编码后的 5 位码中“1”码至少为 2 位, 按 NRZI 编码原理, 信号中就至少有两次跳变, 因此接收端可得到足够的同步信息。

表 8-3

4B/5B 编码 (数据部分)

符号	4 位二进制数	4B/5B 代码	符号	4 位二进制数	4B/5B 代码
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	10	1010	10110
3	0011	10101	11	1011	10111
4	0100	01010	12	1100	11010
5	0101	01001	13	1101	11011
6	0110	01110	14	1110	11100
7	0111	01111	15	1111	11101

3. 时钟偏移问题

在一般的环形网中, 采用只有一个主时钟的集中式时钟方案, 在绕环运行时, 时钟信号会偏移。每个站点产生的偏移, 积累起来还是很可观的。为了消除这种时钟偏移现象, 采用一种称为弹性缓冲器来消除这种偏移。但即使采用了这种措施, 由于偏移积累的缘故, 限制

了环网的规模。

这种集中式时钟方案，对 100 Mbps 高速率的光纤网来说是不适用的。100 Mbps 光纤网中每一位的时间为 10 ns（而在 4 Mbps 环网中，1 位的时间为 250 ns）。因此，时钟偏移的影响更严重，如采用集中式时钟方案，就需在每一个站点配置锁相电路，成本会很高。

因此，FDDI 标准规定使用分布式时钟方案，即在每个站点都配有独立的时钟和弹性缓冲器。进入站点缓冲器的数据时钟是按照输入信号的时钟确定的，而从缓冲器输出的信号时钟则根据站点的时钟确定，这种方案使环路中中继器的数目不受时钟偏移因素的限制。

4. FDDI MAC 帧格式

FDDI 标准以 MAC 实体间交换的 MAC 符号来表示帧结构，每个 MAC 符号对应 4 个比特，这是因为在 FDDI 物理层中，数据是以 4 位为单位来传输的。FDDI 的令牌帧和数据帧的格式如图 8-22 所示。

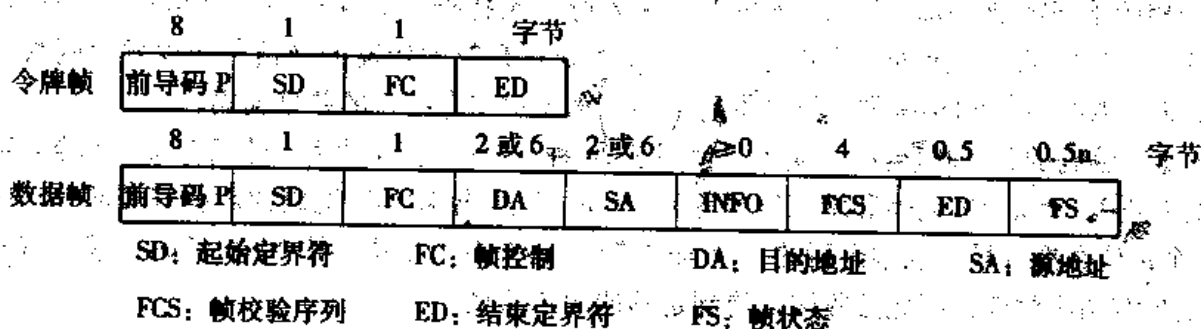
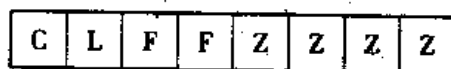


图 8-22 FDDI MAC 帧格式

前导码 P 用以在收发双方实现时钟同步。发送站点以 16 个 4 位空闲符号（64 个比特）作为前导码。

起始定界符 SD 占一个字节，由两个 4 比特 MAC 非数据符号组成。

帧控制字段 FC 占一个字节，其格式为：



其中 C 表示是同步帧还是异步帧，L 表示是使用 2 字节（16 位）地址还是 6 字节（48 位）地址，FF 表示是 LLC 数据帧还是 MAC 控制帧，若为 MAC 控制帧，则用最后 4 位 ZZZZ 来表示控制帧的类型。

目的地址字段 DA 和源地址字段 SA 可以是 2 字节或 6 字节地址。

数据字段用于装载 LLC 数据或与控制操作有关的信息。FDDI 标准规定最大帧长为 4500 字节。

帧检验序列 FCS 为 4 个字节（32 比特）长。

结束定界符 ED，对令牌来说占 2 个 MAC 控制符号（共 8 比特）；其它帧则只占一个 MAC 控制符号（即 4 比特），用于与非偶数个 4 比特 MAC 控制符号的帧状态字段 FS 配合，以确保帧的长度为 8 比特的整数倍。

帧状态字段 FS 用于返回地址识别、数据差错及数据复制等状态，每种状态用一个 4 比特 MAC 控制符号来表示。

由上可见，FDDI MAC 帧与 802.5 的 MAC 帧十分相似，不同之处是 FDDI 帧含有前导码，这对高数据速率下的时钟同步十分重要；允许在网内使用 16 位和 48 位地址，比 802.5 更灵活；令牌帧也有不同，没有优先位和预约位，而用别的方法分配信道使用权。

虽然 FDDI 和 802.5 都采用令牌传递的协议，但两者还是存在着一个重要差别，即 FDDI 协议规定发送站发送完帧后，可立即发送新的令牌帧，而 802.5 规定当发送出去的帧的前沿回送至发送站时，才发送新的令牌帧。因此，FDDI 协议具有较高利用率的特点，特别在大的环网中显得更为明显。

8.3.2 快速以太网

传统以太网是 10 Mbps 的基带总线局域网，采用 10BASE5、10BASE2 或 10BASE-T 作为传输介质，各站点共享共用信道，任何一个站点所发送的数据均沿着介质以广播方式传输，总线上其它所有站点均可以接收到。由于协议简单、安装方便而得到了广泛应用，但其有限的带宽成为系统的“瓶颈”。

为了提高传统以太网系统的带宽，制定了 IEEE802.3u 标准作为对 IEEE802.3 标准的追加。符合 IEEE802.3u 标准的以太网产品被称为快速以太网（Fast Ethernet）。

1. 介质访问控制方法

IEEE 于 1995 年通过了 100 Mbps 快速以太网的 100BASE-T 标准，并正式命名为 IEEE 802.3u 标准，作为对 IEEE 802.3 标准的补充。100BASE-T 标准不但在最大程度上保持了 IEEE 802.3 标准的完整性，而且保留了核心以太网的细节规范。

虽然 100BASE-T 仍采用常规 10 Mbps 以太网的 CSMA/CD 介质访问控制方法，但其性能是 10BASE-T 的 10 倍，而价格仅为其一半。100BASE-T 的 MAC 与 10BASE-T 的 MAC 相比，除了帧间隙缩短到原来的 1/10 外，两者的帧格式及参数完全相同。100BASE-T 的 MAC 也可以运行于不同的速率，并能与不同的物理层接口。这样，原先 10 Mbps 以太网上运行的软件不加任何修改即可在快速以太网上运行，原先的协议分析和管理工具也可轻易地被继承。

为了能成功地进行冲突检测，100BASE-T 也必须满足“最短帧长 = 冲突检测时间 × 数据传输速率”的关系。其中的冲突检测时间等于网络中最大传播时延的 2 倍。100BASE-T 与 10BASE-T 的 MAC 帧相同，两者的最短帧长均为 64 字节（512 比特），但由于 100BASE-T 的数据速率提高了 10 倍，故相应的冲突检测时间缩短为 10BASE-T 的 1/10，由此整个网络的直径（任何两站点间的最大距离）也减小到 10BASE-T 的 1/10。

2. 物理层

100BASE-T 和 10BASE-T 的区别在物理层标准和网络设计方面。100BASE-T 的物理层包含三种介质选项：100BASE-TX、100BASE-FX 和 100BASE-T4（见表 8-4）。

表 8-4

100BASE-T 物理层介质选项

	100BASE-TX	100BASE-FX	100BASE-T4
传输介质	2 对 STP 或 5 类 UTP	2 对光纤	4 对 3、4 或 5 类 UTP
传输信号	4B/5B NRZI	4B/5B NRZI	8B/6T NRZ
数据速率	100Mbps	100Mbps	100Mbps
每段长度	100 m	100 m	100 m
物理范围	200 m	400 m	200 m

注：STP—屏蔽双绞线、UTP—非屏蔽双绞线、NRZ—不归零制编码、NRZI—差分不归零制编码

(1) 100BASE-TX 和 100BASE-FX。100BASE-TX 和 100BASE-FX 均采用两对链路，其中一对用于发送、另一对用于接收，每对链路实现单方向的 100Mbps 数据速率。100BASE-TX 使用屏蔽双绞线或 5 类非屏蔽双绞线，100BASE-FX 则使用光纤。

100BASE-TX 和 100BASE-FX 都使用高效的 4B/5B NRZI 编码。NRZI 为差分不归零制编码，这种编码与常规的不归零制 (NRZ) 编码的区别在于每个“1”码开始处都有跳变，每个“0”码开始处没有跳变。在 NRZI 编码中的，信号通过相邻码元极性的跳变来解码，而不是简单地以绝对电平为准，由此可获得更高的抗干扰能力。

(2) 100BASE-T4。100BASE-T4 是为在低质量要求的 3 类非屏蔽双绞线上实现 100Mbps 数据速率而设计的，该规范也可使用 4 类或 5 类非屏蔽双绞线。

要想直接用一对 3 类非屏蔽双绞线获取 100Mbps 的数据速率几乎是不可能的。因此，100BASE-T4 采用一种称为 8B/6T 的编码方案。该方案将原始数据流分为 3 股子数据流，经 4 对子信道 D1~D4 传输，每个子信道的数据速率为 33.3Mbps。其中 D1、D3、D4 用于发送，D2、D3、D4 用于接收。因此，D3、D4 被配置为双向传输。另外，D2 既用于接收，又用于冲突检测。每个子信道中，将每 8 位数据为单位映射成一个 6 位的信号码组，这样，子信道的信号传输速率便为 $33.3 \times (6/8) = 25\text{Mbaud}$ 。

8.3.3 千兆位以太网

随着多媒体技术、网络分布计算、桌面视频会议等应用的不断发展，用户对局域网的带宽提出了更高的要求；同时，100M 快速以太网也要求主干网、服务器一级有更高的带宽。另外，由于以太网的简单、实用、廉价及应用的广泛性，人们又迫切要求高速网技术与现有的以太网保持最大的兼容性。千兆以太网技术就是在这种需求背景下开始酝酿的。1996 年 3 月成立的 IEEE802.3Z 工作组，专门负责千兆以太网的研究，并制定相应标准。

千兆以太网使用原有以太网的帧结构、帧长及 CSMA/CD 协议，只是在低层将数据速率提高到了 1Gbps。因此，它与标准以太网 (10Mbps) 及快速以太网 (100Mbps) 兼容。用户能在保留原有操作系统、协议结构、应用程序及网络管理平台与工具的同时，通过简单的修改，使现有的网络工作站廉价地升级到千兆位速率。

1. 千兆以太网的物理层协议

千兆以太网的物理层协议包括 1000BASE-SX、1000BASE-LX、1000BASE-CX 和

1000BASE-T 等标准。

(1) 1000BASE-SX。使用芯径为 $50\mu\text{m}$ 及 $62.5\mu\text{m}$ 、工作波长为 850nm 的多模光纤, 采用 8B/10B 编码方式, 传输距离分别为 260m 和 525m , 适用于建筑物中同一层的短距离主干网。

(2) 1000BASE-LX。使用芯径为 $50\mu\text{m}$ 及 $62.5\mu\text{m}$ 的多模、单模光纤, 工作波长为 1300nm , 采用 8B/10B 编码方式, 传输距离分别为 525m 、 550m 和 3000m , 主要用于校园主干网。

(3) 1000BASE-CX。使用 150Ω 平衡屏蔽双绞线 (STP), 采用 8B/10B 编码方式, 传输速率为 1.25Gbps , 传输距离为 25m , 主要用于集群设备的连接, 如一个交换机房内的设备互连。

(4) 1000BASE-T。使用 4 对 5 类非平衡屏蔽双绞线 (UTP), 传输距离为 100m , 主要用于结构化布线中同一层建筑的通信, 从而可以利用以太网或快速以太网已铺设的 UTP 电缆。

2. 千兆以太网的 MAC 子层

MAC 子层的主要功能包括数据帧的封装/卸装、帧的寻址与识别、帧的接收与发送、链路的管理、帧的差错控制及 MAC 协议的维护。

千兆以太网的帧结构与标准以太网的帧结构相同, 其最大帧长为 1518 字节, 最小帧长为 46 字节。

千兆以太网对介质的访问采用全双工和半双工两种方式。全双工方式适用于交换机到交换机或交换机到站点之间的点一点连接, 两点间可同时进行发送与接收, 不存在共享信道的争用问题, 所以不需采用 CSMA/CD 协议。半双工方式则适用于共享介质的连接方式, 仍采用 CSMA/CD 协议解决信道的争用问题。

千兆以太网的数据速率为快速以太网的 10 倍, 若要保持两者最小帧长的一致性, 势必大大缩小千兆以太网的网络直径; 若要保持网络直径为 200m , 则最小帧长要 512 字节。为了确保最小帧长为 64 字节, 同时维持网络直径为 200m , 千兆以太网采用了载波扩展和数据包分组两种技术。

载波扩展技术用于半双工的 CSMA/CD 方式, 实现方法是对小于 512 字节的帧进行载波扩展, 使这种帧所占有的时间等同于长度为 512 字节的帧所占用的时间。虽然载波扩展信号不携带数据, 但由于它的存在保证了 200m 的网络直径。对于 ≥ 512 字节的帧, 不必添加载波扩展信号。若大多数帧短于 512 字节, 则载波扩展技术会使带宽利用率下降。

数据包分组技术允许站点每次发送多帧, 而不是一次发送一帧。若多个连续的数据帧短于 512 字节, 仅其中的第一帧需要添加载波扩展信号。一旦第一帧发送成功, 则说明发送信道已打通, 其后续帧就可不加载波扩展连续发送, 只需帧间保持 12 字节的间隙即可。

由于全双工方式不存在冲突问题, 所以不需任何处理即可传输 64 字节的最小数据帧。

3. 千兆以太网的特点

一方面为了保持从标准以太网、快速以太网到千兆以太网的平滑过渡; 另一方面又要兼顾新的应用和新的数据类型, 在千兆以太网的研究过程中应注意以下特点:

(1) 简易性: 千兆以太网应保持经典以太网的技术原理、安装实施和管理维护的简易性, 这是千兆以太网成功的基础之一。

(2) 技术过渡的平滑性: 千兆以太网保持了经典以太网的主要技术特征, 采用 CSMA/CD 介质管理协议, 采用相同的帧格式及帧的大小, 支持全双工、半双工工作方式, 以确保平滑过渡。

(3) 网络可靠性: 保持经典以太网的安装、维护方法, 采用中央集线器和交换机的星形结构和结构化布线方法, 以确保千兆以太网的可靠性。

(4) 可管理性与可维护性: 采用简易网络管理协议 (SNMP) 及经典以太网的故障查找与排除工具, 以确保千兆以太网的可管理性与可维护性。

(5) 经济性: 网络成本包括设备成本、通信成本、管理成本、维护成本及故障排除成本。由于继承了经典以太网的技术, 使千兆以太网的整体成本下降。

(6) 支持新应用与新数据类型: 计算机技术和应用的发展, 出现了许多新的应用模式, 对网络提出了更高的要求。为此, 千兆以太网必须具有支持新应用与新数据类型的能力。

8.3.4 万兆以太网

万兆以太网技术与千兆以太网类似, 仍然保留了以太网帧结构。通过不同的编码方式或波分复用提供 10Gbit/s 传输速度。所以就其本质而言, 10G 以太网仍是以太网的一种类型。

10G 以太网于 2002 年 6 月在 IEEE 通过。10G 以太网包括 10GBASE-X、10GBASE-R 和 10GBASE-W。10GBASE-X 使用一种特紧凑包装, 含有 1 个较简单的 WDM 器件、4 个接收器和 4 个在 1300nm 波长附近以大约 25nm 为间隔工作的激光器, 每一对发送器/接收器在 3.125Gbit/s 速度 (数据流速度为 2.5Gbit/s) 下工作。10GBASE-R 是一种使用 64B/66B 编码 (不是在千兆以太网中所用的 8B/10B) 的串行接口, 数据流为 10.000Gbit/s, 因而产生的时钟速率为 10.3Gbit/s。10GBASE-W 是广域网接口, 与 SONET OC-192 兼容, 其时钟为 9.953Gbit/s、数据流为 9.585Gbit/s。

万兆以太网的特性如下:

(1) 万兆以太网不再支持半双工数据传输, 所有数据传输都以全双工方式进行, 这不仅极大地扩展了网络的覆盖区域 (交换网络的传输距离只受光纤所能到达距离的限制), 而且使标准得以大大简化。

(2) 为使万兆以太网不但能以更优的性能为企业骨干网服务, 更重要的是, 还要从根本上对广域网以及其它长距离网络应用提供最佳支持, 尤其是还要与现存的大量 SONET 网络兼容。该标准对物理层进行了重新定义。新标准的物理层分为两部分, 分别为 LAN 物理层和 WAN 物理层。LAN 物理层提供了现在正广泛应用的以太网接口, 传输速率为 10G; WAN 物理层则提供了与 OC-192c 和 SDH VC-4-64c 相兼容的接口, 传输速率为 9.58G。与 SONET 不同的是, 运行在 SONET 上的万兆以太网依然以异步方式工作。WIS (WAN 接口子层) 将万兆以太网流量映射到 SONET 的 STS-192c 帧中, 通过调整数据包间的间距, 使 OC-192c 的略低的数据传输率与万兆以太网相匹配。

(3) 万兆以太网有 5 种物理接口。千兆以太网的物理层每发送 8 比特的数据要用 10 个比特组成编码数据段, 网络带宽的利用率只有 80%; 万兆以太网则每发送 64 比特只用 66

个比特组成编码数据段，比特利用率达 97%。虽然这是牺牲了纠错位和恢复位而换取的，但万兆以太网采用了更先进的纠错和恢复技术，确保数据传输的可靠性。

新标准的物理层可进一步细分为 5 种具体的接口，分别为 1550 纳米 LAN 接口、1310 纳米宽频波分复用 (WDM) LAN 接口、850 纳米 LAN 接口、1550 纳米 WAN 接口和 1310 纳米 WAN 接口。每种接口都有其对应的最适宜的传输介质。850 纳米 LAN 接口适于用在 50/125 微米多模光纤上，最大传输距离为 65 米。50/125 微米多模光纤现在已用得不多，但由于这种光纤制造容易，价格便宜，所以用来连接服务器比较划算。1310 纳米宽频波分复用 (WDM) LAN 接口适于用在 62.5/125 微米的多模光纤上，传输距离为 300 米。62.5/125 微米的多模光纤又叫 FDDI 光纤，是目前企业使用得最广泛的多模光纤，从 20 世纪 80 年代末 90 年代初开始在网络界大行其道。1550 纳米 WAN 接口和 1310 纳米 WAN 接口适于在单模光纤上进行长距离的城域网和广域网数据传输，1310 纳米 WAN 接口支持的传输距离为 10 公里，1550 纳米 WAN 接口支持的传输距离为 40 公里。

8.3.5 交换型以太网

计算机技术与通信技术的结合促进了计算机局域网的飞速发展，从 20 世纪 60 年代末 ALOHA 的出现到 90 年代中期 1000Mbps 交换型以太网的登台亮相，短短的 30 年间经过了从单工到双工，从共享到交换，从低速到高速，从简单到复杂，从昂贵到普及的飞跃。

20 世纪 80 年代中后期，由于通信量的急剧增加，促进了技术的发展，使局域网的性能越来越高。最早的 1Mbps 的速率已广泛地被今天的 100BASE-T 替代。但是，传统的介质访问方法都局限于使大量的站点共享对一个公共传输介质的访问，即 CSMA/CD 模式。

90 年代初，随着计算机性能的提高及通信量的剧增，传统局域网已经愈来愈超出了自身的负荷，交换型以太网技术应运而生，大大提高了局域网的性能。交换技术的加入，就可以建立地理位置相对分散的网络，使局域网交换机的每个端口可平行、安全、同时互相传输信息，而且使局域网可以高度扩容。

局域网交换技术的发展要追溯到两端口网桥。桥是一种存储转发设备，用来连接相似的局域网。从互连网络的结构看，桥是属于 DCE 级的端到端的连接；从协议层次看，桥是在逻辑链路层对数据帧进行存储转发，桥与中继器在第一层、路由器在第三层的功能相似。两端口网桥几乎是和以太网同时发展的。

以太网交换技术 (Switch) 是在多端口网桥的基础上于 20 世纪 90 年代初发展起来的，实现 OSI 模型的下两层协议，与网桥有着千丝万缕的关系，甚至被业界人士称为“许多联系在一起的网桥”，因此现在的交换式技术并不是什么新的标准而是现有技术的新应用而已，是一种改进了的局域网桥。与传统的网桥相比，它能提供更多的端口、更好的性能、更强的管理功能以及更便宜的价格。现在有的以太网交换机实现了 OSI 参考模型的第三层协议，实现路由选择功能。以太网交换机又与电话交换机相似，除了提供存储转发 (Store-and-forward) 方式外还提供其它桥接技术，如直通方式 (Cutthrough)。

8.4 无线局域网技术

一般局域网的传输介质大多采用双绞线、同轴电缆或光纤,这些有线传输介质往往存在敷设费用高、施工周期长、改动不方便、维护成本高、覆盖范围小等问题。日趋成熟的无线技术给人们带来了享受无线移动联网的高效接入和自由沟通的便利。无线局域网(Wireless LAN, WLAN)是局域网技术与无线通信技术相结合的产物。目前,常用的无线接入技术主要有 IEEE 802.11 无线局域网技术、红外(Infrared rays, Ir)端口技术和蓝牙(Blue Tooth)技术等。

8.4.1 无线局域网概述

无线局域网与有线局域网相比有以下诸多优点:

(1) 安装便捷:无线局域网的最大优势是免去或减少了网络布线的工作量,一般仅需安装一个或数个接入点(Access Point, AP)设备,便可实现无线局域网的有效覆盖。

(2) 使用灵活:在无线局域网的有效信号覆盖范围内,站点可以在任何位置接入网络,而不必受网络设备安放位置的限制。

(3) 经济节约:有线局域网必须为预设大量实际使用率低下接入点花费不小的开支,而当用户数量和位置发生变更时又要花费较大的开支进行网络改造。无线局域网可以避免或减少这种问题的出现。

(4) 易于扩展:无线局域网提供了多种配置方式供用户灵活选择,用户可以组成仅有几个站点的小型局域网,也可以组成拥有上千站点的大型局域网,并且能获得有线网络无法提供的“漫游”等功能。

无线局域网的不足之处是,数据传输速率相对较低、有时会有通信盲点等。

无线局域网必须支持高速、突发的数据业务,在室内使用还要解决多径衰落以及相邻子网间串扰等问题。具体来说,无线局域网必须实现以下技术要求:

(1) 可靠性:实验数据表明,为保证通信系统的可靠性和稳定性、提高网络的有效吞吐量,无线局域网的系统分组丢失率应低于 10^{-5} 、误码率应低于 10^{-8} 。

(2) 兼容性:对于室内使用的无线局域网,应尽可能使其跟现有有线局域网在网络操作系统和网络软件上相互兼容。

(3) 数据速率:为了能满足局域网业务量的需要,无线局域网的数据传输速率应该至少在 1 Mbps 以上。

(4) 通信保密:由于数据通过无线介质在空中传播,无线局域网必须在不同层次采取有效措施以提高通信保密和数据安全性能。

(5) 移动性:支持全移动网络或半移动网络。全移动网络中的站点可在网络覆盖范围内以移动状态与网络通信;半移动网络中的站点可在网络覆盖范围内移动,但与网络通信时以静止状态进行。

(6) 节能管理:由于大多数用户一般都使用笔记本电脑连接无线局域网,所以无线局

域网应具备节能管理功能,当无数据收发时使站点机处于休眠状态,当有数据收发时再使其处于激活状态,从而达到节省笔记本电脑内电池消耗的目的。

(7) 小型化、低价格:这是无线局域网得以实用并普及的关键所在。

(8) 电磁环境:无线局域网应考虑电磁波对人体和周边环境的影响问题。

无线局域网的硬件设备有:

(1) 无线网卡。无线网卡的作用和以太网中网卡的作用基本相同,它作为无线局域网的接口,能够实现无线局域网各客户机之间的连接与通信。

(2) 无线 AP。AP 是 Access Point 的简称,无线 AP 就是无线局域网中接入点、无线网关,它的作用类似于有线网络中的集线器。

(3) 无线天线。当无线网络中各网络设备相距较远时,随着信号的减弱,传输速率会明显下降以致无法实现无线网络的正常通信,此时就要借助于无线天线对所接收或发送的信号进行增强。

无线局域网协议主要分为两大阵营:IEEE 802.11 系列标准和欧洲的 HiperLAN。其中 IEEE 802.11 协议、蓝牙标准和 HomeRF 工业标准等是无线局域网所有标准中最主要的协议标准。

8.4.2 IEEE 802.11 协议

IEEE802.11 是美国电气和电子工程师协会 IEEE 在 1997 年 6 月颁布的无线网络标准。IEEE802.11 规定了无线局域网在 2.4GHz 波段进行操作,这一波段全球无线电法规组织定义为扩频使用波段。标准的 802.11 主要用于解决办公室局域网和园区网中用户与用户终端的无线接入,速率最高只能达到 2Mbit/s。

1. IEEE802.11 物理层实现方式

IEEE802.11 是早期无线局域网标准之一。该标准定义了物理层和介质访问控制 MAC 协议的规范,允许无线局域网及无线设备制造商在一定范围内建立互操作网络设备。

与 802.3 相比,IEEE802.11 有如下新特点:在物理层定义了数据传输的信号特征和调制方法,定义了 2 个射频传输技术和 1 个红外传输规范共 3 种不同的物理层实现方式。RF 传输标准是直接序列扩频 DSSS (Direct Sequence Spread Spectrum) 和跳频扩频 FHSS (Frequency Hopping Spread Spectrum)。红外 (Infrared, IR) 传输规范则是利用红外线实现无线通信的规范。接入速率有 1Mbit/s 和 2Mbit/s 两种。

2. MAC 结构及服务内容

802.11 的 MAC 子层负责解决客户端工作站和访问接入点之间的连接。当一个 802.11 客户端进入一个或者多个接入点的覆盖范围时,它会根据信号的强弱以及包错误率自动选择一个接入点进行连接。

无线局域网 MAC 提供的服务有:安全服务、MAC 服务数据单元 (MSDU) 重新排序服务和数据服务。802.11 MAC 子层还提供了 CRC 校验和包分片功能。对于上层协议这个分片的过程是完全透明的。

3. CSMA/CA 协议

802.11 的 MAC 和 802.3 协议的 MAC 非常相似, 都是在一个共享介质上支持多个用户共享资源, 发送方在发送数据前先进行网络的可用性检测。802.3 协议采用 CSMA/CD 介质访问控制方法。然而, 在无线系统中设备不能够一边接收数据信号一边传送数据信号。

无线局域网中采用了一种与 CSMA/CD 相类似的载波监听多路访问/冲突防止协议 (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) 实现介质资源共享。CSMA/CA 利用确认信号来避免冲突的发生, 也就是说, 只有当客户端接收到网络上返回的确认信号才确认送出的数据已经到达目的地。CSMA/CA 通过这种方式来提供无线的共享访问, 这种方式在处理无线问题时非常有效。以 CSMA/CA 的方式共享无线介质将时间域的划分与帧格式紧密联系起来, 保证某一时刻只有 1 个站点发送, 实现了网络系统的集中控制。

因传输介质不同, CSMA/CD 与 CSMA/AC 的检测方式也不同。CSMA/CD 通过电缆中电压的变化来检测, 当数据发生碰撞时, 电缆中的电压就会随着发生变化; 而 CSMA/CA 采用能量检测 (ED)、载波检测 (CS) 和能量载波混合检测 3 种检测信道空闲的方式。

8.4.3 IEEE 802.11 系列标准

最早的 IEEE 802.11 标准是在 1997 年提出的, 接着在 1999 年 9 月又提出了 IEEE 802.11a 和 IEEE 802.11b 两个标准, 新近又提出了 IEEE 802.11g 标准。IEEE 802.11 标准集见表 8-5。

表 8-5

IEEE 802.11 标准集

	802.11	802.11b	802.11b +	802.11a	802.11g
频率	2.4GHz	2.4GHz	5GHz	2.4GHz	2.4GHz
带宽	2/1Mbps	11/5.5/2/1Mbps	22/11/5.5/2/1Mbps	可达 54Mbps	可达 54Mbps
距离	100m	100m ~ 300m	100m ~ 300m	5km ~ 10km	5km ~ 10km
业务	数据	数据 图像	数据 图像	语音 数据 图像	语音 数据 图像

1. IEEE 802.11b

802.11b 工作于 2.4GHz 频带, 其物理层支持 5.5Mbps 和 11Mbps 的传输速率, 传输速率可根据环境干扰或传输距离的不同在 11Mbps、5.5Mbps、2Mbps、1Mbps 之间切换, 而且在以 2Mbps 和 1Mbps 速率传输时与 802.11 兼容。802.11b 使用 Direct Sequence (直接序列) DSSS 作为协议, 提供数据加密, 最高使用 128bit 的 WEP。相对于其它标准, 802.11b 价格比较低廉, 并且能够达到 11Mbps 的传输速率, 因此, 802.11b 产品已经广泛地投入市场, 在许多实际场所运行, 但 802.11b 和工作在 5GHz 的 802.11a 标准不兼容。

2. IEEE 802.11a

802.11a 工作于 5GHz 频带, 其物理层速率可达 54Mbps, 传输层可达 25Mbps。它采用正交频分复用 (OFDM) 的独特技术, 可提供 25Mbps 的无线 ATM 接口和 10Mbps 的以太网无线帧结构接口, 以及 TDD/TDMA 的空中接口, 一个扇区可接入多个用户, 每个用户可带多个用户终端, 它的数据加密可达 152bit WEP。但 802.11a 芯片价格昂贵、空中接力不好、点对点连接很不经济。不过由于其传输速率和有效传输距离均远远高于 802.11b, 所以在带宽要求较高的场所, 或者是传输距离较远的地方, 如楼宇中间的无线连接等, 802.11a 仍是用户的首选。

3. IEEE 802.11g

802.11g 是 IEEE 于 2002 年 11 月 15 日批准的一种试验性新标准。802.11g 和 802.11b 一样也工作于 2.4GHz 频带, 所以可以完全兼容 802.11b, 但速度却比 802.11b 快 5 倍, 能达到 802.11a 的水平。

4. IEEE 802.11b+

802.11b+ 是一个非正式的标准, 称为增强型 802.11b。802.11b+ 与 802.11b 完全兼容, 只是采用了 Packet Binary Convolutional Coding (PBCC) 数据调制技术, 所以能够实现高达 22Mbps 的传输速率。

此外, 一些公司还推出了同时兼容 802.11b 和 802.11a 的接入点产品和网卡产品, 提供双频接入, 从而支持 802.11a、802.11b 或者同时支持两种方式, 使得网络中所有无线用户既能同时实现与有线网络的连接, 又能实现彼此之间的连接, 有效解决了标准之间不兼容问题, 保护了用户的投资。

5. IEEE 802.16

IEEE802.16 是宽带无线协议。802.16 工作组成立于 1999 年, 其主要使命是推动固定宽带无线接入系统的发展与应用。IEEE802.16 工作组负责对无线本地环路的无线接口及其相关功能制定标准, 它包括 3 个项目组, 每个项目组负责不同的方面: 802.16.1 负责制定频率为 10~60GHz 的无线接口标准; 802.16.2 负责制定宽带无线接入系统共存方面的标准; 802.16.3 负责制定频率范围在 2~10GHz 之间并获得频率使用许可的无线接口标准。2001 年 12 月, IEEE 批准通过了 802.16 标准, 802.16 也被称为 “Wireless-MAN”。

802.16 协议标准是按照 3 层结构体系组织的。

(1) 物理层。物理层协议主要是关于频率带宽、调制模式、纠错技术以及发射机同接收机之间的同步、数据传输率和时分复用结构等方面的。对于从用户到基站的通信, 该标准使用的是 “按需分配多路寻址” (DAMA—TDMA) 技术。按需分配多路寻址 (Demand Assigned Multiple Access, DAMA) 技术是一种根据多个站点之间的容量需要的不同而动态地分配信道容量的技术。时分多路技术可以根据每个站点的需要为其在每个帧中分配一定数量的时隙来组成每个站点的逻辑信道。通过 DAMA—TDMA 技术, 每个信道的时隙分配可以动态

地改变。

(2) 数据链路层。在该层上 IEEE802.16 规定的主要是为用户提供服务所需的各种功能。这些功能都包括在介质访问控制 MAC 层中,主要负责将数据组成帧格式来传输和对用户如何接入到共享的无线介质中进行控制。MAC 协议规定基站或用户在什么时候采用何种方式来初始化信道,并分配无线信道容量。位于多个 TDMA 帧中的一系列时隙为用户组成一个逻辑上的信道,而 MAC 帧则通过这个逻辑信道来传输。IEEE 802.16.1 规定每个单独信道的数据传输率范围是从 2Mbit/s 到 155Mbit/s。

(3) 会聚层。在 MAC 层之上是会聚层,该层根据提供服务的不同而提供不同的功能。对于 IEEE802.16.1 来说,能提供的服务包括数字音频/视频广播、数字电话、异步传输模式 ATM、因特网接入、电话网络中无线中继和帧中继。

8.4.4 蓝牙技术

具体说来,蓝牙 (Blue Tooth) 是一种短距离的无线连接技术标准的代称,蓝牙的实质内容就是要建立通用的无线电空中接口及其控制软件的公开标准。

“蓝牙”计划主要面向网络中各类数据及语音设备,如 PC 机、笔记本电脑、打印机、传真机、数码相机、移动电话、家电设备等,使用无线微波的方式将它们连成一个微微网,多个微微网之间也可以互连,从而方便快速地实现各类设备之间的通信。

蓝牙采用分散式网络结构以及快跳频和短包技术,支持点对点及点对多点通信,工作在全球通用的 2.4GHz ISM (即工业、科学、医学) 频段。其数据速率为 1Mbps,采用时分双工传输方案实现全双工传输。

蓝牙 1.0 标准由两个文件组成。一个是核心部分 (Foundation Core),它规定的是设计标准;另一个叫协议子集部分 (Foundation Profile),它规定的是运作性准则。

蓝牙协议可以分为 4 层,即核心协议层、电缆替代协议层、电话控制协议层和采纳的其它协议层。由于篇幅的限制,这里只介绍核心协议。

蓝牙的核心协议包括基带 (Baseband)、链路管理 (LMP)、逻辑链路控制与适应协议 (SDP) 四部分。

链路管理 (LMP) 负责蓝牙组件间连接的建立。通过连接的发起、交换、核实,进行身份鉴权和加密等安全方面的任务;通过协商确定基带数据分组大小;它还控制无线单元的电源模式和工作周期,以及微微网内蓝牙组件的连接状态。

逻辑链路控制与适应协议 (L2CAP) 位于基带协议层之上,属于数据链路层,是一个为高层传输和应用层协议屏蔽基带协议的适配协议。其完成数据的拆装、基带与高层间的适配,并通过协议复用、分用及重组操作为高层提供数据业务和分类提取,它允许高层协议和应用接收或发送长过 64K 字节的 L2CAP 数据包。

业务搜寻协议 (SDP) 是极其重要的部分,它是所使用模式的基础。通过 SDP,可以查询设备信息、业务及业务特征,并在查询之后建立两个或多个蓝牙设备间的连接。SDP 支持 3 种查询方式:按业务类别搜寻、按业务属性搜寻和业务浏览 (Browsing)。

蓝牙作为一个全球公开的无线应用标准,通过把各种语音和数据设备用无线链路连接起来,使人们能随时随地进行数据信息的交换与传输。无疑,它将在人们的日常生活和工作中

扮演重要的角色,其市场潜力巨大,正成为 21 世纪的投资热点。

8.4.5 IrDA 和 HomeRF 技术

1. IrDA

红外线数据标准协会 (Infrared Data Association, IrDA) 成立于 1993 年。IrDA 数据传输技术是一种利用红外线进行点对点通信的技术。

基于红外线的传输技术最近几年有了很大发展。目前广泛使用的家电遥控器几乎都是采用的红外线传输技术。作为无线局域网的传输方式,红外线方式的最大优点是不受无线电干扰,且它的使用不受国家无线电管理委员会的限制。但是,红外线对非透明物体的透过性较差,导致传输距离受限制。

红外线是波长在 $750\text{nm} \sim 1\text{mm}$ 之间的电磁波,它的频率高于微波而低于可见光,是一种人的眼睛看不到的光线。红外通信一般采用红外波段内的近红外线,波长在 $0.75\mu\text{m} \sim 25\mu\text{m}$ 之间。红外数据协会 (IrDA) 成立后,为了保证不同厂商的红外产品能够获得最佳的通信效果,红外通信协议将红外数据通信所采用的光波波长的范围限定在 $850\text{nm} \sim 900\text{nm}$ 之内。

IrDA 标准包括三个基本的规范和协议:物理层规范 (Physical Layer Link Specification)、链接建立协议 (Link Access Protocol, IrLAP) 和链接管理协议 (Link Management Protocol, IrLMP)。物理层规范制定了红外通信硬件设计上的目标和要求, IrLAP 和 IrLMP 为两个软件层,负责对链接进行设置、管理和维护。在 IrLAP 和 IrLMP 基础上,针对一些特定的红外通信应用领域, IrDA 还陆续发布了一些更高级别的红外协议,如 TinyTP、IrOBEX、IrCOMM、IrLAN、IrTran-P 和 IrBus 等。

2. HomeRF

HomeRF 是由 HomeRF 工作组开发的,适合家庭区域范围内在 PC 和用户电子设备之间实现无线数字通信的开发性工业标准。

HomeRF 工作在 2.4GHz 频段,采用数字跳频扩频技术,速率为 50 跳/秒,并有 75 个带宽为 1MHz 跳频信道。调制方式为 2FSK 与 4FSK。数据的传输速率在 2FSK 方式下为 1Mbit/s ,在 4FSK 方式下为 2Mbit/s 。在新版 HomeRF2.x 中采用了宽带频率群 (Wide Band Frequency Hopping, WBFH) 技术把跳频带宽增加到了 3MHz 和 5MHz ,跳频速率也加到 75 跳/秒,数据传输速率达到了 10Mbit/s 。

HomeRF 工作组制定了共享无线访问协议 (SWAP) 无线通信规范,定义了一个新的通用空中接口,此接口支持家庭范围内语音、数据的无线通信。用户使用符合 SWAP 规范的电子产品可实现在 PC 的外设、无线电话等设备之间建立一个无线网络,以共享语音和数据;在家庭区域范围内的任何地方,可以利用便携式微型显示设备浏览因特网;在 PC 和其它外设备之间共享一个 ISP 连接等多项共享功能。

8.4.6 无线应用协议 WAP

1997 年包括摩托罗拉、诺基亚、爱立信和美国的软件公司的一些跨国通信技术公司共同制定了新一代无线应用协议 (Wireless Application Protocol, WAP)。WAP 是一种使用在无线通信设备 (包括手机、便携计算机、掌上电脑 PDA 等) 上的新的移动通信技术, 其功能类似于因特网上的 HTTP 协议。它定义了一系列将因特网内容过滤和转化为适用移动通信的标准, 使内容可以更容易地在移动终端上显示, 使得利用手机就可以接入因特网并使用因特网上的各种应用。

WAP 定义了一个开放的标准化的结构以及一系列的标准以实现因特网的无线接入访问, WAP 主要包括 3 部分: 客户、网关和 WWW 服务器。其中 WWW 服务器就是目前常用的 WWW 服务器。网关与服务器之间通过 HTTP 协议进行通信, 这就意味着服务的提供者几乎可以不改动信息的内容, 只要增加网关设备, 就可以向移动用户提供信息。

1. 无线标记语言 (WML)

WAP 移动终端上的浏览器所识别的描述语言不再是 HTML 或 JavaScript, 而是无线标记语言 (Wireless Markup Language, WML) 和无线标记语言脚本 WMLScript。WML 是一种符合 XML 标准的描述语言, 在 WML 中使用的标记数量比 HTML 使用的要少很多, 这主要是为了易于在终端设备中实现。这些移动设备的存储容量不大, 不可能放置很大的系统和复杂的应用程序。HTML 文档是平面型的, 而 WML 的文档由一系列精心定义的用户交互单元组成, 一个交互单元成为一个卡 (Card), 用户可以在一个或多个 WML 文档的 Card 之间进行浏览。

2. WDP 协议

众所周知, HTTP 所采用的是 TCP/IP 协议, 而 WAP 所采用的通信协议则是无线数据报协议 (Wireless Datagram Protocol, WDP)。WDP 是属于无线网络传输层的协议, 其作用是为了使 WAP 能使用 TCP/IP 访问因特网。

3. WAP 网关

WAP 网关用标准的 HTTP1.1 协议从 WWW 服务器上获取信息, 然后将其转换为 WML 格式的文档, 并提供给移动终端。这样只需要增加网关设备就可以将现有的 WWW 服务器上的内容发送给移动用户, 而不需要专门开发相关的信息内容。WAP 规范使用标准的 Web 代理技术来将无线网络与 Web 连接起来。通过将处理功能集中在 WAP 网关中, WAP 结构大大减少了手机上的操作负载。此外, 网关还要完成 DNS 的功能。这样, 终端只需要输入 URL 就可以得到相应的信息, 减少了终端设备上浏览器的负担, 使之既简单又廉价。网关的另一个功能是尽可能地减少用户浏览网络的时延, 它可以通过与其它信息服务器之间的高速连接, 减少信息获取的时间。

4. 轻量级协议栈

WAP 协议栈将无线手机访问因特网的带宽需求降到最低,保证了各种无线网络都可以使用 WAP 规范。通过使用 WAP 协议栈可以节省大量的无线带宽。要完成同样一个访问操作,使用 WAP 协议栈涉及的包数量不到使用全标准的 HTTP/TCP/IP 协议栈的一半,这对于带宽严重受限的无线网络来讲无疑是十分有益的。

8.5 移动 Ad Hoc 网络

Ad Hoc 网络又称移动自组网、多跳网络,是一种特殊的在不借助中心管理的情况下,在有限的范围内实现多个移动终端的临时互连,它为局域网内的移动通信网络提供了一种灵活的互连方式。

8.5.1 Ad Hoc 网络的发展和特点

1. 移动 Ad Hoc 网络的发展

一般认为,没有基础设施的网络出现在 20 世纪 70 年代,在最初开发报文交换技术(后来发展成因特网)不久,美国国防部高级研究规划署(DARPA)资助了一项特别的研究一分组无线网络(Packet Radio Network),即让报文交换技术在不受固定或有线的基础设施限制的环境下运行。最初的动机之一就是满足战场生存的军事需求。在战场恶劣的环境下,通信设备不可能依赖已经敷设的通信基础设施,一方面,这些设施可能根本不存在,另一方面,这些设施会随时遭到破坏。因此,能快速装备、自组织的移动基础设施是这种网络区别于其它商业蜂窝系统的基本要素。在结构上,这种网络是由一系列移动节点组成,是一种自组织的网络,它不依赖于任何已有的网络基础设施。网络中的节点动态且任意分布,节点之间通过无线方式互连,它将分组交换网络的概念引申到广播网络的范畴。这项工作开辟了移动自组网(Mobile AdHoc Network,简称 Ad Hoc 网络或 MANET)研发的先河。20 世纪 90 年代中期,随着一些技术的公开,Ad Hoc 网络开始成为移动通信领域一个公开的研究热点。目前 Ad Hoc 网络尚未达到完全实用阶段,大部分工作仍处在仿真和实验阶段,仿真规模在数百至数千节点,实验规模在几十个节点左右。

2. 移动 Ad Hoc 网络的特点

由于移动 Ad Hoc 网络是一种移动、多跳、自律式系统,它是移动通信和计算机网络相结合的网络,网络中的每个节点都兼有路由器和主机两种功能。移动 Ad Hoc 网络的特点主要体现在以下四方面:

(1) 网络的独立性。Ad Hoc 网络相对常规通信网络而言,最大的区别就是可以在任何时刻、任何地点不需要硬件基础网络设施的支持,快速构建起一个移动通信网络。它的建立不依赖于现有的网络通信设施,具有一定的独立性。

(2) 动态变化的网络拓扑结构。在 Ad Hoc 网络中, 移动主机可以在网中随意移动。主机的移动会导致主机之间的链路增加或消失, 主机之间的关系不断发生变化。另外, 主机可能同时还是路由器, 因此, 移动会使网络拓扑结构不断发生变化, 而且变化的方式和速度都是不可预测的。加上无线发射装置发送功率的变化、环境的影响以及信号之间的互相干扰等因素, 都会造成网络拓扑结构的动态变化。对于常规网络而言, 网络拓扑结构则相对较为稳定。

(3) 有限的无线通信带宽。在 Ad Hoc 网络中没有有线基础设施的支持, 因此, 主机之间的通信均通过无线传输来完成。由于无线信道本身的物理特性, 它提供的网络带宽相对有线信道要低得多。除此以外, 考虑到竞争共享无线信道产生的碰撞、信号衰减、噪音干扰等多种因素, 移动终端可得到的实际带宽远远小于理论中的最大带宽值。

(4) 有限的主机能源。在 Ad Hoc 网络中, 主机均是一些移动设备, 如 PDA、便携计算机或掌上电脑。由于主机可能处在不停的移动状态下, 主机的能源主要由电池提供, 因此 Ad Hoc 网络有能源有限的特点, 在进行系统设计时节能就成为一个非常重要的指标。

(5) 网络的分布式特性。在 Ad Hoc 网络中没有中心控制节点, 主机通过分布式协议互连。一旦网络的某个或某些节点发生故障, 其余的节点仍然能够正常工作。

(6) 生存周期短。Ad Hoc 网络主要用于临时的通信需求, 相对于有线网络, 它的生存时间一般比较短。

(7) 有限的物理安全。

3. 移动 Ad Hoc 网络的应用需求

Ad Hoc 网络的应用范围很广, 总体上来说, 它可以用于以下场合:

- (1) 没有有线通信设施的地方, 如没有建立硬件通信设施或有线通信设施遭受破坏。
- (2) 需要分布式特性的网络通信环境。
- (3) 现有有线通信设施不足, 需要临时快速建立一个通信网络的环境。
- (4) 作为生存性较强的后备网络。

8.5.2 Ad Hoc 网络的结构

Ad Hoc 无线网络的拓扑结构可分为两种: 对等式平面结构和分级结构。在对等式平面结构中, 所有网络节点地位平等。

而在分级结构的 Ad Hoc 无线网络拓扑结构中, 整个网络是以簇为子网组成, 每个簇由一个簇头和多个簇成员组成, 簇头形成高级网络, 高级网络又可分簇形成更高级网络。每一个簇中的簇头和簇成员是动态变化、自动组网。分级结构根据硬件的不同配置, 又可以分为单频分级结构和多频分级结构。单频分级结构使用单一频率通信, 所有节点使用同一频率; 而在多频分级结构中, 若存在两级网络, 则低级网络通信范围小, 高级网络通信范围大, 簇成员用一个频率通信, 簇头节点用一个频率与簇成员通信, 用另一个频率来维持与簇头之间的通信。

对等式平面结构和分级结构使用时各存在优缺点: 对等式平面结构网络结构简单, 各节点地位平等, 源节点与目的节点通信时存在多条路径, 不存在网络“瓶颈”, 而且网络相对

比较安全,但最大的缺点是网络规模受到限制,当网络规模扩大时路由维护的开销指数增长而消耗掉有限的带宽;分级结构网络规模不受限制,可扩充性好,而且由于分簇,路由开销相对小一些,虽然分级结构中需要复杂的簇头选择算法,但由于分级网络结构具有较高的系统吞吐量,节点定位简单,目前 Ad Hoc 网络正逐渐呈现分级化的趋势,许多网络路由算法都是基于分级结构网络模式提出的。

8.5.3 Ad Hoc 网络的路由协议

1. Ad Hoc 网络路由协议的设计要求

Ad Hoc 网络设计中的一个关键问题是开发能够在两个节点之间提供高质量、高效率通信的路由协议。网络节点的移动性使得网络拓扑结构不断变化,传统的基于因特网的路由协议无法适应这些特性,因此,应用于 Ad Hoc 网络的路由协议必须满足以下的条件:

- (1) 必须对网络拓扑结构动态变化具有快速应变的能力,并且尽量避免路由环路的发生,提供方便简单的网络节点定位法。
- (2) 必须高效地利用有限的带宽资源,尽可能压缩不必要的开销。
- (3) 实施多跳通信的中间转接次数也是有限的,一般不要超过 3 次。
- (4) 必须尽可能减少发射时间和发射的数据量,节约有限的工作能源。
- (5) 在可能的条件下,使设计的路由协议具有安全性,降低遭受攻击的可能性。

2. Ad Hoc 网络的路由协议分析

根据 Ad Hoc 网络路由协议的特殊性,近年来提出了多种 Ad hoc 网络路由协议。IETF 的 MANET 工作小组目前正专注于 Ad Hoc 网络路由协议的研究,提出了许多协议草案,如 DSR、AODV、ZRP 等路由协议;另外,专业研究人员也发表了大量关于 Ad Hoc 网络路由协议的相关文章,提出了许多关于 Ad Hoc 的网络路由协议,如 DSDV、WRP 等。根据路由触发原理,目前的路由协议大致可以分为先验式路由协议、反应式路由协议和混合式路由协议 3 种。

(1) 先验式路由协议。先验式路由协议又称表驱动路由协议,每个节点维护一张包含到达节点的路由信息的路由表,并根据网络拓扑的变化随时更新路由表,所以路由表可以准确地反映网络的拓扑结构;源节点一旦要发送报文,可以立即获得到达目的节点的路由,这类的路由协议通常是通过修改现有的有线路由协议来适应 Ad Hoc 无线网络要求,如通过修改路由信息协议(RIP)得到的目的节点序列距离矢量协议(DSDV)。因此,这种路由协议的时延较小,但是协议需要大量的路由控制报文路由,协议的开销较大。常用的先验式路由协议有 DSDV、HSR、GSR、WRP 等。

DSDV 协议通过给每个路由设定序列号避免了路由环路的产生,采用时间驱动和事件驱动技术控制路由表的传送,即每个移动节点在本地都保留一张路由表,其中包括所有有效信宿点、路由跳数、信宿路由序列号等信息,信宿路由序列号用于区别新旧路由以避免环路的产生。每个节点周期性地将本地路由表传送给邻近节点,或者当其路由表发生变化时,也会将其路由信息传给邻近点,当无节点移动时使用间隔较长的大数据包(包括多个数据单元)

进行路由更新；邻近节点收到包含修改的路由表信息后，先比较信源 K 信宿路由序列号的大小，信宿路由序列号大的路由将被采用，而信宿路由序列号小的路由则被淘汰，若相同，则采用最佳制式的路由（如最短路径）。

HSR (Hierarchical State Routing) 是一种用于分级网络的路由协议，高级节点保存它所有子孙节点的位置信息，沿从最高级的根节点到最低级的叶节点的路径为节点分配逻辑序列地址，可以用序列地址进行节点寻址。

GSR 称为全局状态路由协议，其工作原理与 DSDV 协议类似，采用链路状态路由算法，但避免了路由报文的泛滥，它包括一个邻近节点表、网络拓扑表、下一跳路由表和距离表。

无线路由协议 WRP 是一种距离——矢量路由协议，每个节点都维持一个距离表、路由表、链路开销表和报文重传表，通过其邻近节点的最短路径生成数 SST (Short path Spanning Tree) 生成自己的 SST 后，再向邻节点传递更新信息。当网络路由表没有任何变化时，接收节点需回传一个空闲报文以示连接，否则，修改距离表，寻找更优路径。这种算法的特点是当检测到任意相邻节点变化时，则检查所有相邻节点的坚固性以消除回路，具有较快的收敛性。

(2) 反应式路由协议。反应式路由协议又称随选路由或者按需路由，是一种当需要时才查找路由的路由选择方式。节点不需要维护及时准确的路由信息，当需要发送数据时才发起路由查找过程。与先验式路由协议相比，反应式路由协议的开销小，但是数据报传送的时延较大，不适合于实时性的应用。常用的反应式路由协议有 AODVR、DSR、TORA 等。AODVR (Ad hoc On demand Distance Vector Routing) 协议：源节点发送数据前先广播一个路由请求消息，附近节点收到后再次广播，直到请求消息到达目的节点或到达知道目的节点路由的中间节点，目的节点或中间节点沿原来路径返回响应消息，源节点收到响应后就知道到达目的节点的路由。

DSR 协议称为动态源路由协议，是一种源路由协议，每个分组的分组头中包含了源一目的整条路由信息。它采用路由缓存技术，用于存储源路由信息，当学习到新的路由时则修改路由缓存内容，该协议包含两个方面：路由发现和路由维护。

TORA 协议称为临时预定路由算法，是一种源初始化按需路由选择协议，它采用链路反转的分布式算法，具有高度自适应、高效率和较好的扩充性，比较适合高度动态移动、多跳的无线网络，其主要特点是控制报文定位在最靠近拓扑变化的一小部分节点处，因此节点只保留邻近点的路由信息。该算法中路由不一定是最优的，常常使用次优路由以减少发现路由的开销。TORA 协议包括 3 个基本模块：路由的创建、路由的维护和路由的删除。

(3) 混合式路由协议。Ad hoc 网络中单纯采用先验式或反应式路由协议都不能完全解决路由问题，因此，许多学者提出了结合先验式和反应式路由协议优点的混合式路由协议，如 ZRP 协议。ZRP 协议是一个先验式和反应式路由协议的组合，网络内的所有节点都有一个以自己为中心的虚拟区，区内的节点数与设定的区半径有关，因此区是重叠的，这是与分群路由的区别；在区内使用先验式路由算法，中心节点使用区内路由协议 IARP 维持一个到区内其它成员的路由表，对区外节点的路由使用按需路由，利用区间路由协议 IERP 建立临时的路由。但是，实施混合式路由也面临着很多困难，如簇的选择和维护、先验式和反应式路由协议的合理选择以及网络工作的大流量等问题。

8.5.4 与其它移动通信系统的比较

蜂窝系统、集群系统、卫星通信系统等传统的移动通信系统都需要有线网络通信基础设施的支持,如基站、交换机、卫星等。这些设施的建立和运转需要大量的人力和物力,因此成本比较高,同时建设的周期也长。Ad Hoc 网络不需要基站的支持,由主机自己组网,因此,网络建立的成本低,同时时间短,一般只要几秒钟或几分钟。上述通信系统中,移动终端之间并不直接通信,并且移动终端只具备收发功能,不具备转发功能。而 Ad Hoc 网络由移动主机构成,移动主机之间可以直接通信,而移动主机不仅收发数据,同时还转发数据。此外目前的移动通信系统主要为用户提供语音通信功能,通常采用电路交换,拓扑结构比较稳定。而 Ad Hoc 网络使用分组转发技术,主要为用户提供数据通信服务,拓扑结构易于变化。

Ad Hoc 网络组网灵活、快捷,不受有线网络的影响,可广泛应用于军事通信、发生地震或水灾后的营救等无法或不便预先敷设网络设施的场合,具有广阔的发展前景。

8.6 局域网操作系统

8.6.1 局域网操作系统概述

1. 局域网操作系统的演变过程

局域网操作系统的定义是:在局域网低层所提供的数据传输能力的基础上,为高层网络用户提供共享资源管理和其它网络服务功能的局域网系统软件。

操作系统是计算机系统中的重要组成部分,它是计算机与用户之间的接口。单机操作系统必须具备以下两个基本功能:

- (1) 为用户提供各种简便有效的访问本机资源的手段。
- (2) 合理地组织系统工作流程,有效地管理系统。

为实现上述功能,需要在操作系统中建立各种进程,编制不同的功能模块,按层次结构将功能模块有机地组织起来,以完成处理器管理、存储系统管理、文件系统管理、设备管理和作业控制等功能。

单机操作系统只能为本地用户使用本机资源提供服务,不能满足开放网络环境的要求。对于联网的计算机系统,它们不仅要为本地用户使用本地资源和网络资源提供服务,也要为远地网络用户使用资源提供服务。局域网操作系统的基本任务就是为用户提供各种基本网络服务功能,完成网络共享系统资源的管理,并提供网络系统的安全性服务。

局域网操作系统可以分为两类:面向任务型局域网操作系统和通用型局域网操作系统。面向任务型局域网操作系统是为某一种特殊网络应用要求而设计的;通用型局域网操作系统能提供基本的网络服务功能,以支持各个领域应用的需求。

通用型局域网操作系统又可以分为变形系统和基础级系统两类。变形系统是以原单机操作系统为基础，通过增加网络服务功能构成的局域网操作系统；基础级系统则是以计算机裸机的硬件为基础，根据网络服务的特殊要求，直接利用计算机硬件和少量软件资源进行设计的局域网操作系统。

纵观十多年来的发展，局域网操作系统经历了从对等结构向非对等结构演变的过程（如图 8-23 所示）。

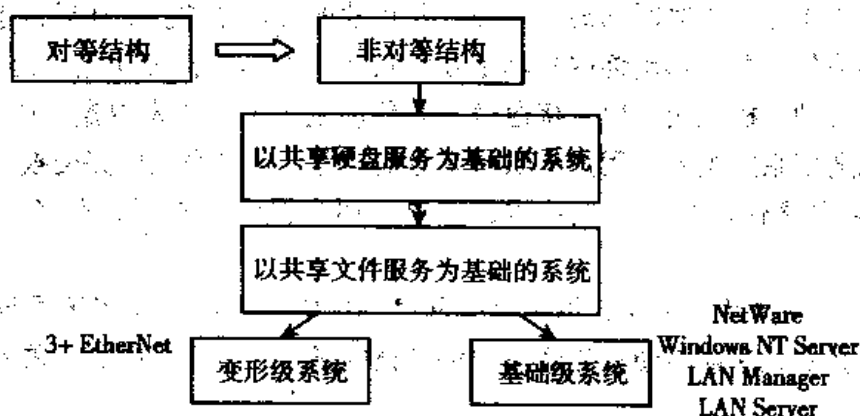


图 8-23 局域网操作系统的演变过程

(1) 对等结构局域网操作系统。对等结构的局域网操作系统具有以下特点：联网节点地位平等、每个网络节点上安装的局域网操作系统软件均相同、联网计算机的资源原则上均可相互共享。各联网计算机均以以前后台方式工作，前台为本地用户提供服务，后台为其它节点的网络用户提供服务。对等结构的局域网操作系统可以提供共享硬盘、共享打印机、共享 CPU、共享屏幕、电子邮件等服务。

对等结构局域网操作系统的优点是：结构简单，网络中任意两个节点间均可直接通信；而其缺点是：每台联网计算机既是服务器又是工作站，节点要承担较重的通信管理、网络资源管理和网络服务管理等工作。对于早期资源较少、处理能力有限的微机来说，要同时承担多项管理任务，势必降低性能指标。因此，对等结构局域网操作系统支持的网络系统一般规模均较小。

(2) 非对等结构局域网操作系统。非对等结构局域网操作系统的设计思想是将节点计算机分为网络服务器（Server）和网络工作站（Work Station，简称 WS）两类。网络服务器采用高配置、高性能计算机，以集中方式管理局域网的共享资源，为网络工作站提供服务；网络工作站一般为配置较低的 PC 机，用以为本地用户访问本地资源和网络资源提供服务。

非对等结构局域网操作系统的软件也分为两部分：一部分运行在服务器上；另一部分运行在工作站上。安装运行在服务器上的软件，是局域网操作系统的核心部分，其性能直接决定网络服务功能的强弱。

早期的非对等结构局域网操作系统以共享硬盘服务器为基础，向网络工作站用户提供共享硬盘、共享打印机、电子邮件、通信等基本服务功能。这种系统效率低、安全性差，使用也不方便。为了克服这些缺点，提出了基于文件服务器的局域网操作系统的设计思想。

基于文件服务器的局域网操作系统软件由文件服务器软件和工作站软件两部分组成。文件服务器具有分时系统文件管理的全部功能，向网络用户提供完善的数据、文件和目录

服务。

初期开发的基于文件服务器的局域网操作系统属于变形级系统，其典型实例是 3 + 网操作系统。在变形级系统中，作为文件服务器的计算机安装了基于 DOS 的文件服务器软件。由于对硬盘的存取控制仍通过 DOS 的 BIOS 进行，因此在服务器大量读/写操作时会造成网络性能的下降。

后期开发的局域网操作系统均属于基础级系统，它们具有优越的网络性能，能提供很强的网络服务功能，目前大多数局域网的操作系统都采用这种方式。其典型实例有 Novell NetWare、Microsoft Windows NT Server、Microsoft LAN Manager 及 IBM LAN Server 等。

2. 局域网操作系统的基本服务功能

(1) 文件服务 (File Service)。文件服务是局域网操作系统中最重要、最基本的网络服务功能。文件服务器以集中方式管理共享文件，为网络工作站提供完整的数据、文件、目录服务。用户可以根据所规定的权限对文件进行建立、打开、关闭、删除、读写等操作。

(2) 打印服务 (Print Service)。打印服务也是局域网操作系统提供的基本网络服务功能。共享打印服务可以通过设置专门的打印服务器来实现，打印服务器也可由文件服务器或工作站兼任。局域网中可以设置一台或多台共享打印机，向网络用户提供远程共享打印服务。打印服务实现对用户打印请求的接收、打印格式的说明、打印机的配置、打印队列的管理等功能。

(3) 数据库服务 (Database Service)。随着局域网应用的深入，用户对网络数据库服务的需求也日益增加。Client/Server 工作模式以数据库管理系统为后盾，将数据库操作与应用程序分离开来，分别由服务器端数据库和客户端工作站来执行。用户可以使用结构化查询语言 SQL 向数据库服务器发出查询请求，由数据库服务器完成查询后再将结果传送给用户。Client/Server 工作模式优化了局域网操作系统的协同操作性能，有效地增强了局域网操作系统的服务功能。

(4) 通信服务 (Communication Service)。局域网操作系统提供的通信服务主要有工作站与工作站之间的对等通信、工作站与主机之间的通信服务等功能。

(5) 信息服务 (Message Service)。局域网可以存储—转发方式或对等的点—点通信方式向用户提供电子邮件服务，也可提供文本文件、二进制数据文件的传输服务以及图像、视频、语音等数据的同步传输服务。

(6) 分布式服务 (Distributed Service)。局域网操作系统的分布式服务功能，将不同地理位置的互联局域网中的资源组织在一个全局性的、可复制的分布式数据库中，网络中的多个服务器均有该数据库的副本。用户在一个工作站上注册，便可与多个服务器连接。服务器资源的存放位置对于用户来说是透明的，用户可以通过简单的操作访问大型互联局域网中的所有资源。

网络安全对用户来说十分重要，它包括用户口令、目录权限、文件和目录属性以及对用户登录工作站点及时间的限制。网络为目录提供了多种权限设置，如读权、写权、打开权、创建权、删除权、授权权、列目权和修改权。目录除了有权限还有属性，目录的属性有正常、隐含、系统和专用 4 种。对文件也可以设置属性，它们是只可执行、只可读、可读写、允许共享、不可共享、不可共享但可读写、隐文件、索引、上次备份后又已修改、系统文件

及允许事务跟踪等属性。

局域网的可靠性在很大程度上取决于对服务器硬件故障的检错和纠错能力。对文件服务器的共享硬盘一般都采取了较多的可靠性措施，具体又分为以下几个级别。

第一级是对硬盘目录和文件分配表（FAT）的保护。在硬盘的不同区域保存双份的目录和文件分配表，如果一处损坏，系统会自动转向另一处，并在硬盘中另找一处安排副本；

第二级是对硬盘表面损坏时的数据保护。为了防止将数据写入磁盘的不可靠块，采用了热调整（Hot Fix）及写后读验证这两个互补技术进行数据保护；

第三级是采用磁盘镜像的方法实现对硬盘驱动器损坏的保护。所谓磁盘镜像，即在一个磁盘通道上有两个成对的磁盘驱动器，同一数据分别写在两台硬盘上，如果一台硬盘驱动器损坏，另一台硬盘能单独运行，不会造成数据丢失和系统停止；

第四级是采用磁盘双工，对磁盘通道或硬盘驱动器损坏起到保护作用。磁盘双工是采用两个磁盘通道，每个磁盘通道接磁盘镜像对中的一个硬盘；

第五级是一个称为事务跟踪系统 TTS（Transaction Tracking System）的附加容错功能，用以防止当数据在写到数据库时，因系统故障而造成的数据库损坏。TTS 起作用时，将数据库变更的整个过程看做是单个事务，仅当所有文件正确更正之后，事务才算整个完成。如果在一个事务执行期间发生系统故障，TTS 便放弃这一事务已做的所有修改，并返回到数据库的原始状态。

8.6.2 典型局域网操作系统简介

1. NetWare

Novell 公司开发的 Novell NetWare 网络操作系统是一个可使 PC 机网络取代小型机系统的多任务网络操作系统，它开创了工作站/服务器的结构，在一个 Novell 网络中允许有多个文件服务器，每个服务器可适用于不同类型的网卡。NetWare 具有十分灵活的拓扑结构，如总线、星形、环形和混合型的拓扑结构，并可以和其它网络（如 3 + 网、TCP/IP 网）在同一网络下工作，Novell 网还提供了不同种类的网间连接器。

Novell NetWare 由文件服务器软件、工作站软件、网桥软件等组成。其中文件服务器软件和工作站软件是建网不可缺少的软件，安装时需根据硬件的配置生成。由于 Novell NetWare 是直接对微处理器编程的，因而它总是可以和最新的微处理器一起发展，并能充分利用微处理器的高性能，形成高效的网络操作系统。Novell NetWare 操作系统有多种版本。

Novell NetWare 是在局域网的基础上建立的网络操作系统，因此它不同于一般网络协议所需的完整的协议和通信传输功能，它具有所有操作系统的职能，如任务管理、缓冲区管理、文件管理、磁盘及打印机等外设管理，因而结构相当复杂。它是一个围绕核心调度的多用户共享资源的操作系统，它包括磁盘处理、打印机处理、控制台命令处理及网络通信处理等面向用户的处理程序和一个多用户分时核心调度程序，它们之间的关系如图 8-24 所示。

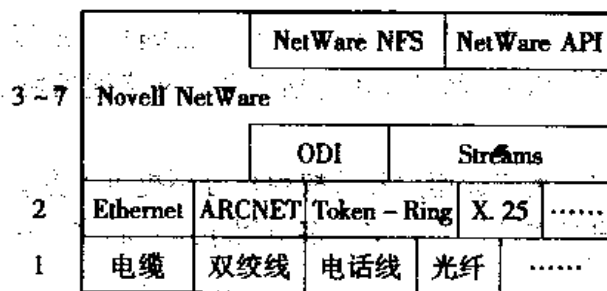


图 8-24 Novell NetWare 网络层次结构

从网络层次结构的第 3~7 层来看, NetWare 与标准网络协议有较大差别。因为 NetWare 是一个基于服务器的网络操作系统, 因而 NetWare 的侧重点在于基于服务器的网络文件系统以及网络管理功能。这与以数据通信为主要目的的网络软件有很大区别。

Novell NetWare 的主要特点:

- (1) Novell 网络为用户使用提供完善的安全措施。
- (2) 具有系统容错 (SFT) 的可靠性措施。
- (3) 开放的网络软件开发环境。开放数据链路接口 ODI (Open Data-link Interface) 是 Novell NetWare 的一项重要网络互连技术。它的实现方法是以 NetWare 作为开放式服务器, 支持多种通信协议和多种设备驱动程序, 以构成异构的计算机网络。ODI 允许在 NetWare 工作站上不必增加网络接口卡, 就可使用多种网络协议 (如 IPX/SPX、TCP/IP 等) 来扩展网络。

NetWare Streams 流提供了操作系统和网络通信协议 (如 IPX/SPX、TCP/IP、SNA、OSI 等) 之间的通用接口, 它允许在单个文件服务器上存放和使用多种网络协议。

NetWare 的有关网络功能的 C 语言应用函数库, 为用户灵活使用网络资源提供了高级语言接口。用户可以在自己的应用环境中, 使用 NetWare 的网络功能, 建立自身的网络开发环境。NetWare 开放系统结构给用户使用和扩充自己的网络功能提供了极大方便。

2. UNIX

自 20 世纪 70 年代中期间世后, UNIX 操作系统便赢得了计算机界的普遍认可, 并得到了广泛传播和迅速发展。作为工业标准的 UNIX 操作系统被广泛应用于大型机、中型机、小型机、工作站及微型机中, 尤其在工作站中几乎全部采用了 UNIX 操作系统。

目前, 常用的 UNIX 版本有 AT&T 和 SCO 公司的 Unix SVR3.2、Unix SVR4.0 以及 Unix 的 Unix SVR4.2 等。新推出的各种 UNIX 版本都将网络功能放在了首位。在 Unix SVR3.2 版本时, TCP/IP 协议已经以模块形式运行于 UNIX 中; 自 Unix SVR4.0 开始, TCP/IP 协议更成了 UNIX 的核心组成, 从而构成了 UNIX 网络操作系统。

UNIX 网络操作系统的主要特点有:

- (1) 良好的用户界面。UNIX 是较早提供图形用户界面的操作系统。
- (2) 统一的处理方法。文件、目录及设备采用统一的处理方法。
- (3) 强大的核外程序功能。UNIX 的内核程序短小精悍, 可以常驻于内存中, 其余可分离部分均作为核外系统程序。这部分核外系统程序内容丰富、功能强大, 可供用户自由选

择、灵活搭配。

(4) 良好的可移植性。由于目前的 UNIX 用 C 语言编写, 所以非常便于移植。

(5) 良好的网络环境。UNIX 网络环境包括齐全的网络通信协议、方便的网络通信工具及灵活的网络编程接口。

(6) 完善的安全机制。为普通用户和特权用户分别提供了完善的多级安全保密机制。

(7) 多任务、多用户操作性。同时支持多道程序运行和多个用户登录。

3. Windows NT

Microsoft 公司将其成熟的 Windows 3.1 技术与 LAN Manager 局域网操作系统技术集成, 于 1993 年成功发布了 Windows NT 3.1, 随后又于 1996 年年底推出了著名的 Windows NT 4.0 版本, 从此打破了网络操作系统由 NetWare 一统天下的局面。

Windows NT 4.0 是一个以客户/服务器模式工作于网络环境中的操作系统, 它包括 Windows NT Server 4.0 和 Windows NT Workstation 4.0 两个产品, 前者是一个基于服务器的功能强大的网络操作系统, 后者是一个高级个人计算机多任务桌面操作平台。

由于 Windows NT Server 4.0 具有与广大用户所熟悉的 Windows 95/98/2000 等相似的用户界面和操作方式, 从而为用户的学习、理解、掌握和运用提供了极大的便利, 使其迅速成为普及的网络操作系统之一。

Windows NT Server 4.0 主要技术特点:

(1) 内存与任务管理。为操作系统和应用程序分配独立的内存空间, 以防两者之间发生冲突; 采用线程 (Thread) 及占先式 (Preemptive) 管理多任务, 使应用程序能更高效地运行。

(2) 开放的体系结构。支持网络驱动接口 (NDIS) 标准和传输驱动接口 (TDI) 标准, 内置 TCP/IP、Microsoft MW Link、Net BIOS 的扩展用户接口 Net BEUI 和数据链路控制 4 种标准网络协议。

(3) 内置管理。通过内部安全保密机制, 使网络管理可以为每个文件设置不同的访问权限、规定用户对服务器的操作权限及用户审计。

(4) 集中式管理。利用域 (Domain) 与域信任关系实现对大型网络的管理。

(5) 用户工作站管理。通过用户描述文件对工作站用户的优先级、网络连接、程序组及用户的注册进行管理。

习 题

1. 在局域网体系结构中, 为什么要将数据链路层分为介质访问控制 (MAC) 子层和逻辑链路控制 (LLC) 子层?

2. IEEE 802 局域网参考模型与 ISO/OSI 参考模型有何异同?

3. 局域网的信道分配策略有哪些? 各有什么特点?

4. 纯 ALOHA 和时分 ALOHA 相比较, 哪一个时延更小? 为什么?

5. 1 万个站点正在竞争使用一时分 ALOHA 信道, 信道时隙为 $125\mu\text{s}$ 。如果每个站点平均每小时发出 18 次请求, 试计算总的信道载荷 G 。

6. N 个站点共享 56Kbps 纯 ALOHA 信道, 各站点平均每 100 秒送出一个长度为 1000 比特的数据帧, 而不管前一个数据帧是否已经发送出去 (假设站点有发送缓冲区)。试计算 N 的最大值。

7. 某个局域网采用二进制倒数计数法的信道分配策略, 在某一时刻, 10 个站点的虚站号为 8、2、4、5、1、7、3、6、9、0。接下来要进行数据发送的是 4、3、9 三个站点。当三个站点全部完成发送后, 各站点的新的虚站号是什么?

8. 2^N 个站点采用碰撞树搜索协议来仲裁对一条共享信道的访问。在某一时刻, 其中两个站点准备发送。设 $2^N \geq 1$, 试分别计算搜索该树的最小、最大和平均时隙。

9. 一栋 7 层的办公楼, 每层有 15 间办公室, 每间办公室的墙上设有一个终端插座, 所有的插座在一个垂直面上构成一个正方形栅格, 相邻插座间的垂直和水平距离均为 4 米。假定任意两个插座间都允许连上电缆 (垂直、水平、斜线连接均可)。试计算在下面 3 种情况下连接所有插座所需的电缆总长度: (1) 采用集线器的星形网; (2) 采用总线以太网; (3) 采用令牌环网 (不设线路中心)。

10. 标准 10Mbps 802.3 LAN 的波特率是多少?

11. 一个 1km 长的 10Mbps 的 CSMA/CD 局域网 (不是 IEEE 802.3), 其信号传播速度为 $200\text{m}/\mu\text{s}$ 。数据帧长度为 256 比特, 其中包括 32 比特首部、校验和以及其它开销。传输成功后的第一个时隙被留给接收方, 用来使接收方捕获信道并发送一个 32 比特的确认帧。假定没有冲突, 试计算该局域网的有效数据传输速率 (不包括开销)。

12. 为什么 CSMA/CD 有最短帧长度的要求?

13. 简述非坚持、1-坚持及 P-坚持算法的特点。

14. 长 1km、10Mbps 的基带总线 LAN, 信号传播速度为 $200\text{m}/\mu\text{s}$, 计算一个 1000 比特的帧从发送开始到接收结束的最大时间是多少? 若两相距最远的站点在同一时刻发送数据, 则经过多长时间两站发现冲突。

15. 100 个站点的时槽环, 任意两站间的平均距离为 10m, 数据传输速率为 10Mbps, 信号传播速度为 $200\text{m}/\mu\text{s}$, 若每个站引入 1 位延迟, 试计算: (1) 两站点间链路的位长度为多少位? (2) 整个环路的有效位长度为多少位? (3) 此环上最多允许有几个 37 位长的时槽?

16. 当数据传输速率为 5 Mbps、传播速度为 $200\text{m}/\mu\text{s}$ 时, 令牌环接口中的一个比特时延等价于多少米的电缆?

17. 长 1km、10Mbps、50 个站点的令牌环, 每个站引入 1 位延迟, 信号传播速度为 $200\text{m}/\mu\text{s}$, 令牌长 8 位, 数据帧长度为 256 位 (包括 32 位开销), 确认在数据帧捎带, 问该环不包括开销的有效数据速率为多少?

18. 长 10km、16Mbps、100 个站点的令牌环, 每个站引入 1 位延迟, 信号传播速度为 $200\text{m}/\mu\text{s}$ 。问: (1) 该环上 1 位的延迟相当于多少米长度的电缆? (2) 该环的有效位长度为多少位?

19. 长 1km、4Mbps、50 个站点的令牌环, 每个站引入 1 位延迟, 信号传播速度为 $200\text{m}/\mu\text{s}$, 设数据帧最大长度为 100 字节。问该环上检查令牌丢失的超时计数器的值至少要设置为多少微秒?

20. 一个 10Mbps 的令牌环, 其令牌保持计数器的设置值为 $10\mu\text{s}$, 在此环上可发送的最长帧为多少位?

21. 简述 802.3 LAN、802.4 LAN 及 802.5 LAN 的特点。

22. 在令牌总线中, 如果某一个站点在接到令牌后随即崩溃, 将会出现什么问题? 应如何解决所出现的问题?

23. 在图 8-21 所示的 DQDB 系统中, 从起始状态开始, 假设节点 C、A、B 要发送数据, 3 个节点以此顺序发送向上的请求且在此之前没有数据传送, 写出每一次请求和每一次数据传输后每个节点 RC 和 CD 的变化情况。

24. 简述 FDDI 与 Token Ring 的异同点。

25. FDDI 采用何种编码技术? 该编码技术有何特点?

26. 10Mbps 的传统以太网升级到 100Mbps、1Gbps 甚至 10Gbps 时, 需要解决哪些技术问题? 试说明 10Mbps、100Mbps、1Gbps 和 10Gbps 以太网的异同。

27. 简述局域网操作系统的发展演变过程。

28. 简述网络操作系统提供的 5 级可靠性措施的特点。

第9章 实用网络技术

前面的章节介绍了计算机网络的基本原理、局域网技术,本章介绍一些曾被广泛关注和应用的实用网络技术,包括分组交换技术、异步传输模式、第三层交换技术、虚拟局域网技术等。

9.1 分组交换技术

广域网的构建由于受各种因素的制约,必须借助公共传输网络。设计广域网的前提在于掌握各种公共传输网络的特性、公共传输网络 and 用户网络之间的互连技术。公共传输网络基本可以分成两大类:一类是电路交换网络;另一类是分组交换网络。公共交换电话网(PSTN)和综合业务数字网(ISDN)都是采用电路交换技术的通信网络。X.25、帧中继及ATM等都是采用分组交换技术的广域网。

分组交换方式也是广域网上经常使用的交换技术。由于采用复用技术,所以分组交换方式线路利用率高,但实时性较差。分组交换网络提供虚电路和数据报两种服务。

虚电路和电路交换的最大区别在于:虚电路只给出了两个远程端点之间的传输通路,并没有把通路上的带宽固定分配给通路两端的用户,其它用户的信息流仍可以共享传输通路上物理链路的带宽。虚电路又可分为永久虚电路和交换虚电路两种。永久虚电路由公共传输网络提供者设置,这种虚电路一经设置便长期存在。交换虚电路需要两个远程端点通过呼叫控制协议建立,在完成当前数据传输后再拆除。当然,呼叫控制协议在建立虚电路时,也必须根据用户设备地址来确定传输通路的两个端点。

数据报服务不需要经过虚电路建立过程就可实现报文传送,由于没有在报文的发送端和接收端之间建立传输通路,报文中必须携带源和目的端点地址,公共传输网络的中间节点必须能够根据报文的目的端点地址选择合适的路径转发报文。

9.1.1 X.25 协议

X.25 是使用最早的分组交换协议标准,多年来一直作为用户网和分组交换网络之间的接口标准。分组交换网络动态地对用户传输的信息流分配带宽,有效地解决了突发性、大信息流的传输问题。分组交换网络同时可以对传输的信息进行加密和有效的差错控制。虽然各种错误检测和相互之间的确认应答浪费了一些带宽、增加了报文传输延迟,但对早期可靠性较差的物理传输线路来说,X.25 不失为一种提高报文传输可靠性的有效手段。但随着光纤越来越普遍地作为传输介质,传输出错的概率越来越小,在这种情况下,重复地在链路层和

网络层实施差错控制,不仅显得冗余,而且浪费带宽、增加报文传输延迟。由于 X.25 分组交换网络是在早期低速、高出错率的物理链路基础上发展起来的,其特性已不适应目前高速远程连接的要求,因此目前 X.25 一般只在传输费用要求少、远程传输速率要求不高的广域网环境使用。

ITU 提出的 X.25 协议描述了主机 (DTE) 与分组交换网 (PSN) 之间的接口标准,使主机不必关心网络内部的操作就能方便地实现对各种不同网络的访问。X.25 实际上是 DTE 与 PSN 之间接口的一组协议,它包括物理层、数据链路层和分组层三个层次。X.25 的分组级相当于 OSI 参考模型中的网络层,其主要功能是向主机提供多信道的虚电路服务。

1. X.25 分组级的功能

X.25 分组级的主要功能是将链路层所提供的连接 DTE—DCE 的一条或多条物理链路复用成数条逻辑信道,并且对每一条逻辑信道所建立的虚电路执行与链路层单链路协议类似的链路建立、数据传输、流量控制、顺序和差错检测、链路的拆除等操作。利用 X.25 分组级协议,可向网络层的用户提供多个虚电路连接,使用户可以同时与公用数据网中若干个其它 X.25 数据终端用户 (DTE) 通信。

X.25 提供虚呼叫和永久虚电路两种虚电路服务,虚呼叫即需要呼叫建立与拆除过程的虚电路服务,永久虚电路即在接入时由协商指定的不需要呼叫建立与拆除过程的虚电路服务。每条虚电路都要赋予一个虚电路号,X.25 中的虚电路号由逻辑信道组号 (0~15) 和逻辑信道号 (0~255) 组成。用于虚呼叫的虚电路号范围和永久虚电路的虚电路号应在签订服务时与管理部门协商确定与分配。

公用数据网有虚电路和数据报两种操作方式,尽管有些网络体系结构 (如 Ethernet) 仍在使用数据报技术,但数据报服务已在 1980 年的修订中被从 X.25 标准中删去,取而代之的是一个称为快速选择 (Fast Select) 的可选扩充服务。

X.25 所规定的虚电路服务属于面向连接的 OSI 服务方式,这正好符合 OSI 参考模型中的网络层服务标准定义,这就为公用数据网与 OSI 结合提供了可能性。OSI 网络层的功能是提供独立于传输层的中继和路由选择以及其它与之相关的功能。在面向连接的网络层服务中,要进行通信的网络层实体必须首先建立连接,这在 X.25 中即为相应的建立虚电路的呼叫建立规程。

2. X.25 分组级分组格式

在分组级上,所有的信息都以分组为基本单位进行传输和处理,无论是 DTE 之间所要传输的数据,还是交换网所用的控制信息,都以分组形式来表示,并按照链路协议穿越 DTE—DCE 界面进行传输。因此在链路层上传输时,分组应嵌入到信息帧 (I 帧) 的信息字段中,即表示成如下的格式:

标记字段 F	地址字段 A	控制字段 C	(分组)	帧校验序列 FCS	标记字段 F
--------	--------	--------	------	-----------	--------

每个分组均由分组头和数据信息两部分组成,其一般格式如图 9-1 所示。

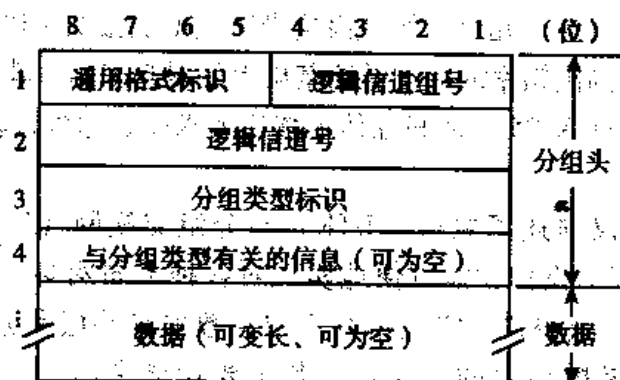


图 9-1 X.25 分组的一般格式

分组格式中的数据部分 (可以为空) 通常被递交给高层协议或用户程序去处理, 所以分组协议中不对它作进一步规定。分组头用于网络控制, 主要包括 DTE—DCE 的局部控制信息, 其长度随分组类型不同有所不同, 但至少要包含前三个字节作为通用格式标识、逻辑信道标识和分组类型标识, 它们的含义如下:

(1) 通用格式标识 (GFI)。由分组中第一个字节的前 4 位组成, 用于标志分组头中其余部分的格式。第一位 (b8) 称作 Q 位或限定位, 只用于数据分组中。这是为了对分组中的数据进行特殊处理而设置的, 可用于区分数据是正常数据, 还是控制信息。对于其它类型的分组, 该位恒置为“0”。第二位 (b7) 称 D 位或传送确认位, 设置该位的目的是用来指出 DTE 是否希望用分组接收序号 P(R) 来对它所接收的数据作端—端确认。在呼叫建立时, DTE 之间可通过 D 位来商定虚呼叫期间是否将使用 D 位规程。第三、四位 (b6、b5) 用以指示数据分组的序号是用 3 位即模 8 (b5 置“1”) 还是 7 位即模 128 (b6 置“1”), 这两位或者取“10”, 或者取“01”, 一旦选定, 相应的分组格式也有所变化。

(2) 逻辑信道标识。由第一个字节中的剩余四位 (b4、b3、b2、b1) 所作的逻辑信道组号 (LCGN) 和第二个字节所作的逻辑信道号 (LCN) 两部分组成, 用以标识逻辑信道。

(3) 分组类型标识。由第三个字节组成, 用于区分分组的类型和功能。若该字节的最后一位 (b1) 为“0”, 则表示分组为数据分组; 若该位为“1”, 则表示分组为控制分组, 可以用作呼叫请求或指示分组、释放请求或指示分组。若该字节末三位 (b3、b2、b1) 为全“1”, 则表示该分组是某个确认或接受分组。

第四个字节及其后诸字节将依据分组类型的不同而有不同的定义。

X.25 分组级协议规定了多种类型的分组。由于 DTE 与 DCE 的不对称性, 所以具有相同类型编码的同类型分组, 因其传输方向的不同有不同的含义和解释, 具体实现时也有所不同。为此, 分组协议从本地 DTE 的角度出发, 为它们取了不同的名称以示区别。一般来说, 从 DTE 到 DCE 的分组表示本地 DTE 经 DCE 向远地 DTE 发送的命令请求或应答响应; 反之, 从 DCE 到 DTE 的分组表示 DCE 代表远地 DTE 向本地 DTE 发送的命令或应答响应。表 9-1 列出了这些分组的名称、分组类型编号及参数。表中的分组类型可归纳为图 9-2 所示的六种格式。

表 9-1

X.25 分组级分组类型

	分组类型名称		分组类型编号 (位)								格式编号
	DTE→DCE	DCE→DTE	8	7	6	5	4	3	2	1	
呼叫建立 和清除	呼叫请求	呼叫指示	0	0	0	0	1	0	1	1	①
	呼叫接受	呼叫接通	0	0	0	0	1	1	1	1	⑥
	释放请求	释放指示	0	0	0	1	0	0	1	1	④
	DTE 释放确认	DCE 释放确认	0	0	0	1	0	1	1	1	⑥
数据和 中断	DTE 数据	DCE 数据	P(R)		M		P(S)		0		②
	DTE 中断请求	DCE 中断请求	0	0	1	0	0	0	1	1	④
	DTE 中断确认	DCE 中断确认	0	0	1	0	0	1	1	1	⑥
流量控制 和复位	DTE RR	DCE RR	P(R)		0	0	0	0	0	1	③
	DTE RNR	DCE RNR	P(R)		0	0	1	0	0	1	③
	复位请求	复位指示	0	0	0	1	1	0	1	1	⑤
	DTE 复位确认	DCE 复位确认	0	0	0	1	1	1	1	1	⑥
重启动	重启动请求	重启动指示	1	1	1	1	1	0	1	1	④
	DTE 重启动确认	DCE 重启动确认	1	1	1	1	1	1	1	1	⑥
任选	DTE REJ	DCE REJ	P(R)		0	1	0	0	0	1	③

数据分组中的数据类型编码部分，除了用 M 位代替 I 帧中的 P/F 位外，其它内容与数据链路级的 HDLC 帧格式中的控制字段 C 非常类似，最末位的“0”是数据类型分组的特征位。M (More Data) 位置“1”，表示还有后续的数据，即当前数据分组中的数据将以同一逻辑信道上的下一数据分组中的数据作为逻辑继续。P(S)、P(R) 分别称为分组发送顺序号和接收顺序号，它们的作用大致与帧格式中的 N(S) 和 N(R) 相当。但是，它们的主要作用是控制每条逻辑信道上向分组交换网发送或从交换网接收的数据流，而不只为站点之间提供确认手段。其目的是为了调节每个逻辑信道上的流量，以防止对分组交换网的压力过重。实际上，P(S) 或 P(R) 的值用以确定一个给定的逻辑信道上的“窗口”，表示信道上允许传送多少个未被响应的分组。能传输未响应分组的最大值称为窗口尺寸，每条虚电路的窗口尺寸是在立户或呼叫建立时分配的，但序号采用 3 位时最大不能超过 7 个分组，序号采用 7 位时最大不能超过 127 个分组。

与数据链路级帧格式一样，分组级也包括 RR、RNR 和 REJ 三种分组，它们被称为流量控制分组，这些分组中的类型字段只包括接收顺序号 P(R)，而无发送顺序号 P(S)。RR 用于告知对方本方正准备从给定逻辑信道上接收顺序号为 P(R) 的分组；RNR 用于向对方表示本方目前不能在给定逻辑信道上接收数据分组。RNR 可以通过同一方向上发送的 RR 分组加以清除。

另外，分组级也包括一些无编号的分组。如中断请求分组，它不需要等待事先已发送的其它分组，而能立即向外发送，甚至在对方不能接收数据时也能发送。中断请求分组只能携带一个字节的用户数据，放在原因字段中用以向对方传送中断信息或原因。

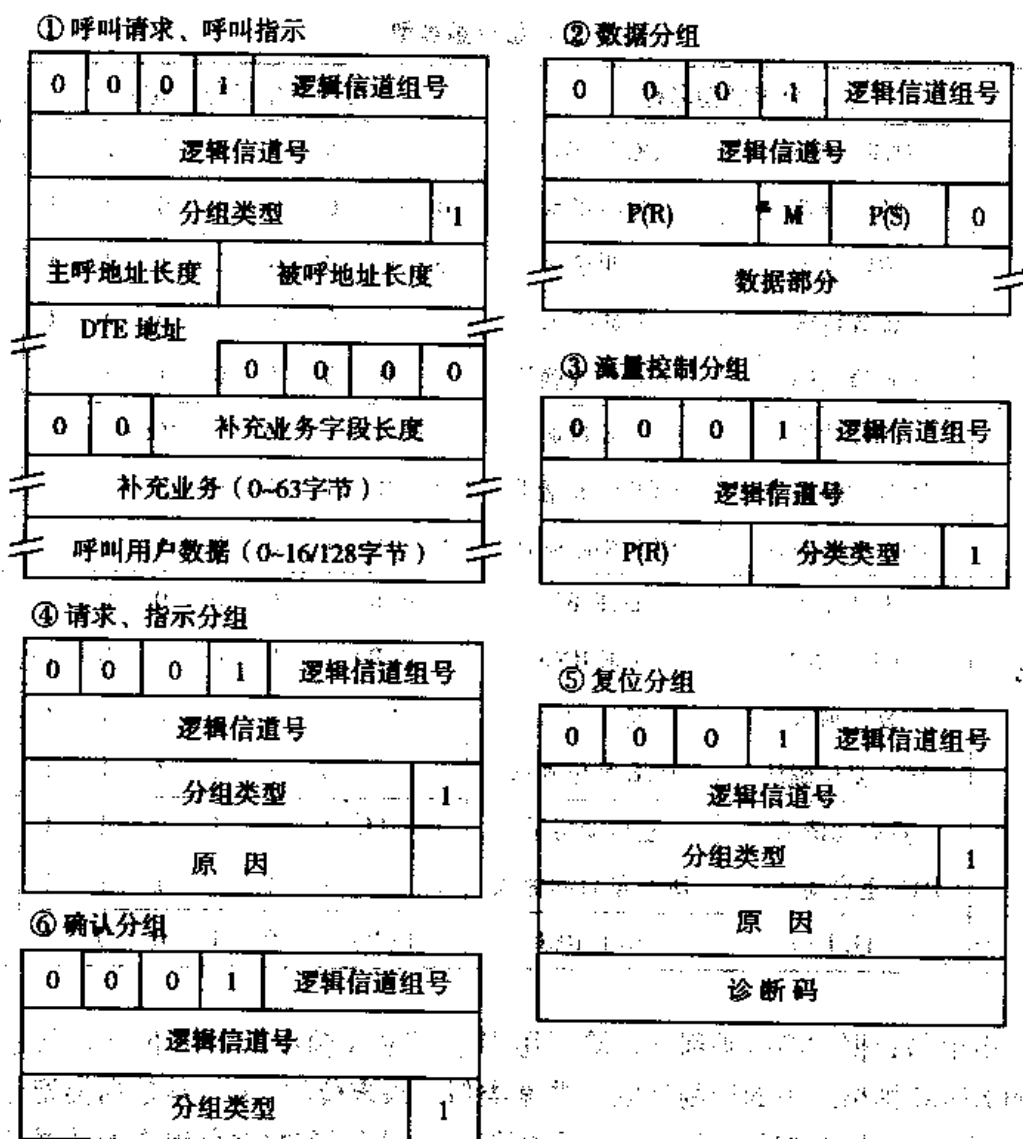


图 9-2 X.25 分组格式

X.25 中还定义了很多其它类型的分组，包括释放请求/指示、复位请求/指示、重启动请求/指示等。其中除复位请求/指示分组多一个诊断代码外，其它均与中断请求分组格式相同。这些分组都包括一个“原因”字段，用以存入引起相应动作的原因。需要说明一下复位与重启动之间的差别。复位请求是为了在数据传输状态中对虚呼叫或永久虚电路进行重新初始准备而设置的；而重启动则为同时释放 DTE—DCE 界面上所有虚呼叫以及复位所有永久虚电路而设置的。

各类确认分组仅包含三个字节，它们分别用作对呼叫、释放、中断、复位及重启动的请求或指示的确认。

9.1.2 帧中继

1984 年，ITU 开始了分组交换技术的“改造工程”，并提出了一种新的分组交换技术——帧中继 (Frame Relay) 技术，对应的标准为 ITU Q.922。

1. 帧中继的基本原理

帧中继技术首先是淡化了交换设备上的层次概念，将数据链路层和网络层进行了融合。融合的目的—方面减少了层次之间的接口处理；另一方面，也可以通过对融合的功能进行分析，发现冗余项，并进行简化。“优化”交换设备性能的另一—方面是简化流量控制的功能。上述的优化使得帧中继成为一种极为精简的协议，仅仅需要提供组帧、路由选择和高速传输的功能，从而可以获得较高的性能和有效性。

帧中继是继 X.25 后发展起来的数据通信方式。从原理上看，帧中继与 X.25 及 ATM 都同属分组交换—类。但由于 X.25 带宽较窄，而帧中继和 ATM 带宽较宽，所以常将帧中继和 ATM 称为快速分组交换。

帧中继保留了 X.25 链路层的 HDLC 帧格式，但不采用 HDLC 的平衡链路接入规程 LAPB (Link Access Procedure-Balanced)，而采用 D 通道链路接入规程 LAPD (Link Access Procedure on the D-Channel)。LAPD 规程能在链路层实现链路的复用和转接，而 X.25 只能在网络层实现该功能。由于帧中继可以不用网络层而只使用链路层来实现复用和转接，所以帧中继的层次结构中只有物理层和链路层。

与 X.25 相比，帧中继在操作处理上做了大量的简化。帧中继不考虑传输差错问题，其中间节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量控制均交由高层端系统完成，所以大大缩短了节点的时延，提高了网内数据的传输速率。

帧中继网络具有以下特点：

- FR 支持 OSI 下两层服务并提供部分的网络层功能；
- FR 采用光纤作为传输介质，传输误码率低；
- 将分组重发、流量控制、纠正错误、防止拥塞（正向拥塞通知，反向拥塞通知，丢失指示等）等处理过程由端系统去实现；简化了节点的处理过程，缩短了处理时间，降低了网络时延；
- 具有灵活可靠的组网方式，可采用永久虚电路（或交换虚电路）的方式，—条物理连接能够提供多个逻辑连接，用户所需的进网端口数减少；
- FR 具有按需分配带宽的特点，用户支付了一定的费用购买“承诺信息速率”，当突发性数据发生时，在网络允许的范围内，可以使用更高的速率；
- 使用 FR，用户接入费用相应减少。

2. 帧中继的帧格式

帧中继的帧结构如图 9-3 所示，它类似于 HDLC 的帧格式，不过没有控制字段。

帧中继的帧格式中，标志字段 F 和帧校验序列 FCS 的作用与 HDLC 中的类似。F 字段用以标志帧的起始和结束，其比特模式为 01111110，可采用 0 比特插入法实现数据的透明传输。FCS 字段用于帧的检错，若传输中出错，则由接收端将之丢弃并通知发送端重发。

帧格式中的地址字段的主要作用是路由寻址，也兼管拥塞控制。地址字段—般由 2 个字节组成，在需要时也可扩展到 3 或 4 个字节。地址字段的组成如下（参见图 9-3）。

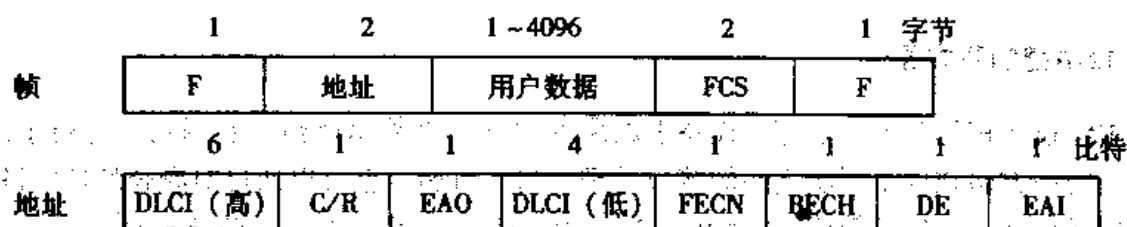


图 9-3 帧中继的帧格式

数据链路连接标识符 DLCI 由高、低两部分共 10 比特组成，用于惟一标识一个虚连接。命令/响应位 C/R 与高层应用有关，帧中继本身并不使用。

扩展地址位 EA 为“0”表示下一字节仍为地址，为“1”表示地址结束，用于对地址字段进行扩展。对于 2 字节地址，其 EAO 为“0”、EAI 为“1”。

发送方将前向显示拥塞通知位 FECN 置“1”，用于通知接收方网络出现拥塞；接收方将反向显示拥塞通知位 BECN 置“1”，用于通知发送方网络出现拥塞。

可丢弃位 DE 由用户设置，若置“1”，表示当网络发生拥塞时，该帧可被优先丢弃。

3. 帧中继的应用

帧中继既可作为公用网络的接口，也可作为专用网络的接口。专用网络接口的典型实现方式是，为所有的数据设备安装带有帧中继网络接口的 T1 多路选择器，而其它如语音传输、电话会议等应用则仅需安装非帧中继的接口。这两类网络中，连接用户设备和网络装置的电缆可以用不同速率传输数据，一般速率在 56Kbps 到 E1 速率 (2.048Mbps) 间。

帧中继的常见应用简介如下：

(1) 局域网的互连。由于帧中继具有支持不同数据速率的能力，使其非常适于处理局域网—局域网的突发数据流量。传统的局域网互连，每增加一条端—端线路，就要在用户的路由器上增加一个端口。基于帧中继的局域网互连，只要局域网内每个用户至网络间有一条带宽足够的线路，则既不用增加物理线路也不占用物理端口，就可增加端—端线路，而不致对用户性能产生影响。

(2) 语音传输。帧中继不仅适用于对时延不敏感的局域网的应用，还可以进行对时延要求较高的低档语音（质量优于长途电话）的应用。

(3) 文件传输。帧中继既可保证用户所需的带宽，又有较满意的传输时延，非常适合大流量文件的传输。

9.2 异步传输模式

9.2.1 ATM 交换

1. ATM 的定义与功能

ITU 在 I 系列建议中给 ATM 下了这样的定义：ATM 是一种转换模式（即前面所说的传

输方式)，在这一模式中信息被组织成信元（Cell），包含一段信息的信元并不需要周期性地出现在信道上，从这个意义上来说，这种转换模式是异步的。

ATM 的特点是进一步简化了网络功能。ATM 网络不参与任何数据链路层功能，将差错控制与流量控制工作都交给终端去做。

图 9-4 是分组交换、帧中继和 ATM 交换三种方式的功能比较。可以看出，分组交换网的交换节点参与了 OSI 第 1 到第 3 层的全部功能；帧中继节点只参与第 2 层功能的核心部分（2a），也即数据链路层中的帧定界、0 比特插入和 CRC 检验功能，第 2 层的其它功能，即差错控制和流量控制，以及第 3 层功能则由终端处理；ATM 网络则更为简单，除了第 1 层的功能之外，交换节点不参与任何工作。从功能分布的情况来看，ATM 网和电路交换网有点相似，可以说 ATM 网是综合了分组交换和电路交换的优点而形成的一种网络。

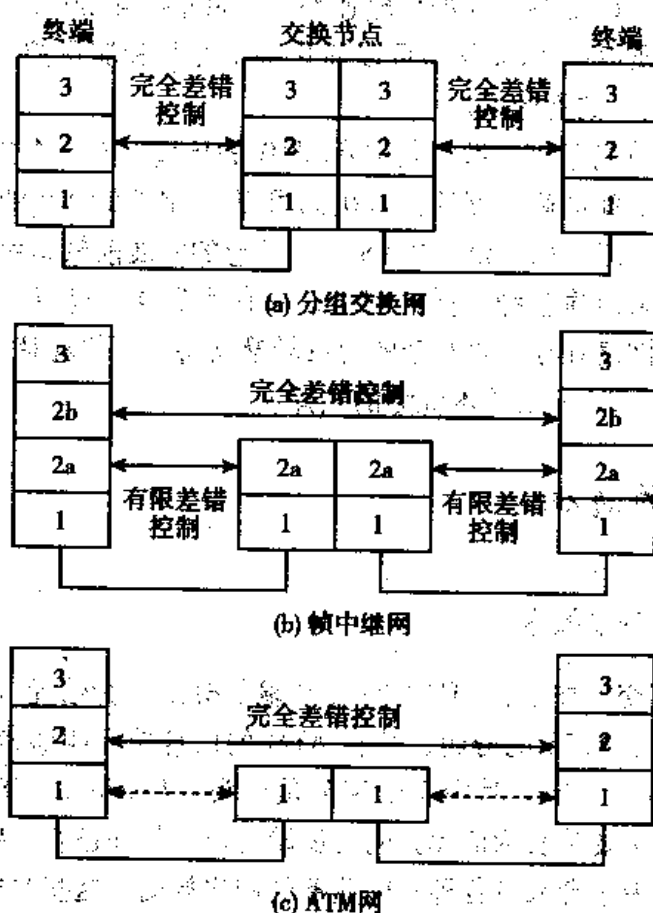


图 9-4 分组交换网、帧中继网和 ATM 网的功能比较

ATM 克服了其它传送方式的缺点，能够适应任何类型的业务，不论其速度高低、突发性大小、实时性要求和质量要求如何，都能提供满意的服务。

已有的各种高速网技术在支持对数据传输要求大容量、高实时性的应用时，总是存在这种或那种不足。例如：高速以太网（100Mbps）采用 CSMA/CD 访问控制技术，高负载时的实时传输能力难以预计；FDDI（100Mbps）基于令牌传递的工作方式，令牌的处理和传递占用了宝贵的时间，统计延时为 10~200ms。因此，迫切需要一种新的网络技术来支持多媒体应用，包括支持 B-ISDN 的应用，这就是异步传输模式（ATM）。ATM 被认为是为满足多媒体传输的要求而出现的一种新型通信技术。

ATM 标准主要由 ITU 制定, ITU 于 1985 年成立第 18 工作组, 制定支持宽带综合业务数字网 (B-ISDN) 的标准, 并将 ATM 作为支持 B-ISDN 传输的基础, 当异步传输模式 (ATM) 技术引入交换机时, 出现了 ATM 交换技术, ATM 交换机根据输入端口的各个信元的信元头中的信息将信元“交换”到指定的输出端口。由于使用了按需分配时间片的策略, 信道的利用率得到提高; 同时, 使用优先级机制, 使得具有实时性要求的信息可以尽快传输。采用 ATM 交换技术构造的网络称为 ATM 网络。

2. ATM 交换的优点

ATM 网络使用固定长度的信元作为传输的基本单元, 固定长度的信元头部可以简化 ATM 交换机的处理; ATM 网络允许混合使用多种高质量的传输介质 (双绞线、同轴电缆和单模/多模光纤), 并且可以支持不同的传输速率 (25Mbps、45Mbps、155Mbps、625Mbps); 同时, 高质量的传输介质使得 ATM 网络可以简化差错控制和流量控制的处理, 从而, 提高网络 (或者 ATM 交换机) 的吞吐量。

ATM 网络可以同时支持数据、数字化语音/图像的传输, 支持多媒体传输的应用, 不同的应用需求具有不同的处理策略, 资源预留机制可以支持高实时性的应用要求; ATM 技术可用于组建各种规模的网络, 如 LAN、WAN 等。理想的发展前景是用 ATM 交换技术来替代现有的各种交换技术, 来组建各种各样的网络, 只有达到这一境界, ATM 的优点才能得到充分的体现, 否则多种网络并存需要复杂的协议转换支持, 不仅耗费宝贵的资源, 而且由于其它网络的性能影响了 ATM 交换技术优势的发挥。

9.2.2 ATM 的特征

1. 基于信元的分组交换技术

ATM 仍然采用分组交换技术, ATM 网络中传输的分组称为信元 (Cell)。信元实际上就是分组, 只是为了区别于 X.25 的分组, 才将 ATM 的信息单元叫做信元。ATM 的信元具有固定的长度, 即总是 53 个字节。其中 5 个字节是信头 (Header), 48 个字节是信息段。信头包含各种控制信息, 主要是表示信元去向的逻辑地址, 另外还有一些维护信息、优先级及信头的纠错码。信息段中包含来自各种不同业务的用户数据, 这些数据透明地穿越网络。信元的格式与业务类型无关, 任何业务的信息都同样被切割封装成统一格式的信元。

2. 快速交换技术

ATM 将电路交换与分组交换二者结合起来, 类似于电路交换, 端用户之间的信息传输之前必须事先分配逻辑信道, 建立虚拟连接, 并且 ATM 交换机的内部实现输入端口的信元直接交换到输出端口。交换机本身不执行差错控制和流量控制, 减少节点处理延时, 使得传输速率可达 Gbps 的数量级。由于简化了信元交换的过程, 并采用硬件予以支持, 使得 ATM 交换成为一种快速交换, 减少了交换延时, 使得信元在 ATM 交换机中“逗留”的时间不会超过 100us。交换机的输入/输出速率高, 一般为 155.252Mbps、622.080Mbps 等, 以 155.252Mbps 为例, 每个信元服务时间为 2.73us, 即使排队信元高达 36 个, 排队时间也不

超过 100us。

3. ATM 网络环境

ATM 网络环境由两部分组成：ATM 网络和 ATM 终端用户。

ATM 网络由 ATM 交换机和传输介质组成，其中传输介质可以是双绞线、同轴电缆和光纤。更进一步，ATM 网络又被分为专用 ATM 网络和通用 ATM 网络两类，专用 ATM 网络是指为完成某种特定的应用而开发的 ATM 网络，通常由某个部门组建；通用 ATM 网络则由电信部门主管，可以支持多种服务，收取一定的费用。

ATM 终端用户包括 ATM 网络的用户设备，可以是主机（工作站、服务器等）、互连设备（如路由器等），这些设备通过 ATM 适配卡接入 ATM 网络。

4. 面向连接的信元交换

ATM 网络支持面向连接的信元交换，数据信元交换之前必须建立虚拟连接。

为了支持多个用户同时访问 ATM 网络，采用了复用/解复用技术。物理链路逻辑上被分为多条虚拟路径（VP - Virtual Path），VP 又被划分为多条虚拟通道（VC - Virtual Channel），每个 VP 和 VC 都由标识符予以标识（VPI 和 VCI），VPI 和 VCI 的组合（VPI/VCI）唯一地标识了一条 VC，支持一对用户之间的信息单向交换。为了支持部分用于控制和管理的信元的交换，部分 VPI/VCI 被预先设定。

为了提高效率，信元交换（输入 VPI/VCI 和输出 VPI/VCI 的映射）可以通过硬件予以实现。目前常用的实现方法有两种：时分交换结构和空分交换结构。

采用时分交换结构的交换机内部可被理解为一个可为各个端口共享的高速时间片环，交换机端口类似于环上的节点，并且具有环路的吞吐量大于或者等于所有各个端口的传输能力总和的特点，从而保证交换的及时性。

空分交换结构也称多级矩阵交换结构，要求在输入和输出端口之间具有一条或者多条“通路”。空分交换结构的特点是具有内部硬件实现的电路交换，并且采用多级交换结构。

5. 预约带宽

为了支持不同的应用，ATM 允许根据应用的需求，可以进行带宽预约，确保规定的时间内完成数据信元的传输。带宽预约的过程发生在 VC 建立时。同时，不同的用户数据分配不同的优先级别，当交换机内部出现信元排队时，高优先级的数据可以优先交换。当 ATM 网络出现拥塞时，低优先级的数据信元可以被“优先”丢弃。

9.2.3 ATM 的层次结构

原理上说，ATM 包含了 OSI 低三层的功能；但是类似于帧中继的实现，ATM 交换也融合和简化了 OSI 低三层的功能。由于网络层的流量控制功能被简化（也可以认为是忽略），而路由选择又隐含在 ATM 交换的过程中，因此，从数据流的角度出发，ATM 网络主要含物理层和数据链路层。ATM 物理层被进一步划分为两个子层：物理介质子层（PM）和传输汇聚子层（TC）；数据链路层又被划分为两个子层：ATM 适配子层（AAL）和 ATM 子层。

1. ATM 子层

ATM 子层是 ATM 数据链路层的子层, 主要定义信元头的结构, 以及使用物理链路的方法。ATM 的信头有两种格式, 分别对应用户—网络接口 UNI 和网络节点接口 NNI。UNI 信头的格式如图 9-5 所示, 其中各字段的含义及功能如下:

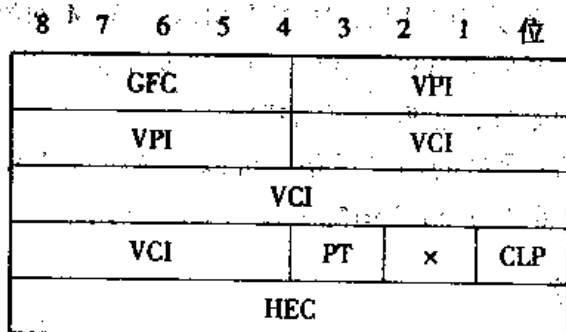


图 9-5 ATM 的信头

GFC (Generic Flow Control): 一般流量控制字段, 又称接入控制字段, 当多个信元等待传输时, 用以确定发送顺序的优先级。

VPI (Virtual Path Identifier) / VCI (Virtual Channel Identifier): 虚路径标识字段/虚通道标识字段, 用作路由选择。

PT (Payload Type): 负荷类型字段, 用以标识信元数据字段所携带的数据的类型。

CLP (Cell Loss Priority): 信元丢失优先级字段, 用于拥塞控制, 若网络出现拥塞时, 首先丢弃 CLP 值小的信元。

HEC (Head Error Control): 信头差错控制字段, 用以检测信头中的差错, 并可纠其中的 1 比特错。HEC 的功能在物理层实现。

ATM 子层的功能:

(1) 信元的汇集和分检: 负责将多个输入端口的信元分检到不同的输出端口;

(2) VPI/VCI 的管理: 根据 VPI/VCI 映射表, 将输入端口来的信元中的 VPI/VCI 映射成输出端口对应的 VPI/VCI, 并填充进信元头;

(3) 信元头的增删: ATM 子层实体接收来自于 AAL 子层的信元体, 并增加信元头, 形成信元; 接收方 ATM 子层实体执行相反的动作, 完成删除信元头的任务;

(4) 信元速率调整: 不同的链路需要不同的信元速率, 例如: SDH STM-1 链路 (线路速率为 155.520Mbps, 数据速率为 150.336Mbps) 每秒应传输 35000 多个信元; 如果输入的实际信元不够时, ATM 层必须生成空信元填充信道。

2. ATM 适配层

AAL 的主要目的是将高层的信息转换成适合 ATM 网络传输要求的格式。

(1) ITU 的通信业务分类。ITU 将 ATM 网络可以支持的业务分为四大种类:

CLASS A: 支持源/宿之间具有实时要求的恒定位速率 (CBR) 业务。CBR 业务采用面向连接的工作方式;

CLASS B: 支持源/宿之间具有实时性要求的可变位速率 (VBR) 业务, VBR 业务采用

面向连接的工作方式；

CLASS C：支持源/宿之间无实时性要求的可变位速率（VBR）业务；

CLASS D：支持面向无连接的数据传输服务。

(2) AAL 协议类型。为了支持上述 4 种类别的业务，ITU 定义了 4 种类型的 AAL 协议。AAL 层又可进一步划分为两个子层：汇聚子层（CS）和分段/组装子层（SAR）。CS 子层面向不同应用要求，为高层的信息分段进行准备工作；SAR 将高层数据分段成信元负载域的格式，或者将多个信元负载域中的信息组装成高层数据。4 种 AAL 协议及其服务类型见表 9-2。

表 9-2

4 种 AAL 协议及其服务类型

	AAL1	AAL2	AAL3/4	AAL5
连接模式	面向连接	面向连接	面向无连接	面向连接
端到端定时	要求	要求	不要求	不要求
位速率	恒定	可变	可变	可变
业务类型	CLASS A	CLASS B	CLASS C/D	CLASS C/D

(3) AAL5 的工作过程。发方 AAL 的 CS 子层实体接到高层发出的用户数据，组成 CS-PDU。CS-PDU 的格式见图 9-6。

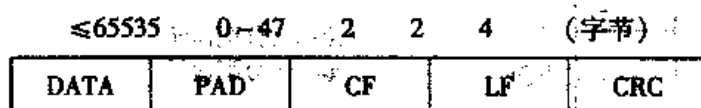


图 9-6 CS-PDU 的格式

基于 AAL5 的 ATM 各层实体的工作过程如图 9-7 所示。

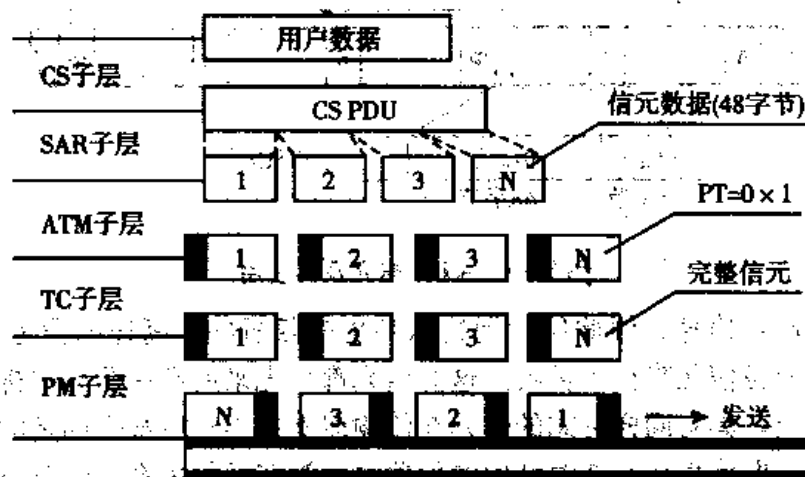


图 9-7 ATM 各层实体的工作过程

发方 SAR 子层实体接到 CS-PDU，执行拆卸工作，将 CS-PDU 拆卸成若干信元数据（长度为 48 字节），并依次提交物理层增加信元头和传输；由于 PAD 字段的增加，使得这种拆卸可以完整地进行。

为了保证收方 SAR 实体可以正确地组装 CS-PDU, AAL5 利用信元头的 PT (信元负载类型) 中的第 2 位来指明本信元在整个 CS-PDU 对应的信元流中的位置 (b_2 为 1 表示本信元为整个 CS-PDU 信元流中的最后一个信元);

收方 SAR 实体接到 PT (b_1, b_2, b_3) = 0x1 的信元时, 组装 CS-PDU, 并上交给收方 CS 子层实体;

收方 CS 子层实体计算 CRC, 并与 CS-PDU 中的 CRC 比较: 如果一致 (正确), 根据 CS-PDU 尾部的 LF, 截取用户数据并投递给其用户; 如果错误, 并且无法恢复, 根据用户需要, 确定是否将有错的用户数据投递给用户。

9.2.4 ATM 的工作方式

ATM 采用如图 9-8 所示的异步时分复用方式工作, 来自不同信息源的信元汇集到一起, 在一个缓冲器内排队, 队列中的信元逐个输出到传输线路, 在传输线路上形成首尾相接的信元流。信元的信头中写有信息的标志 (如 A 和 B), 说明该信元去往的地址; 网络根据信头中的标志来转移信元。

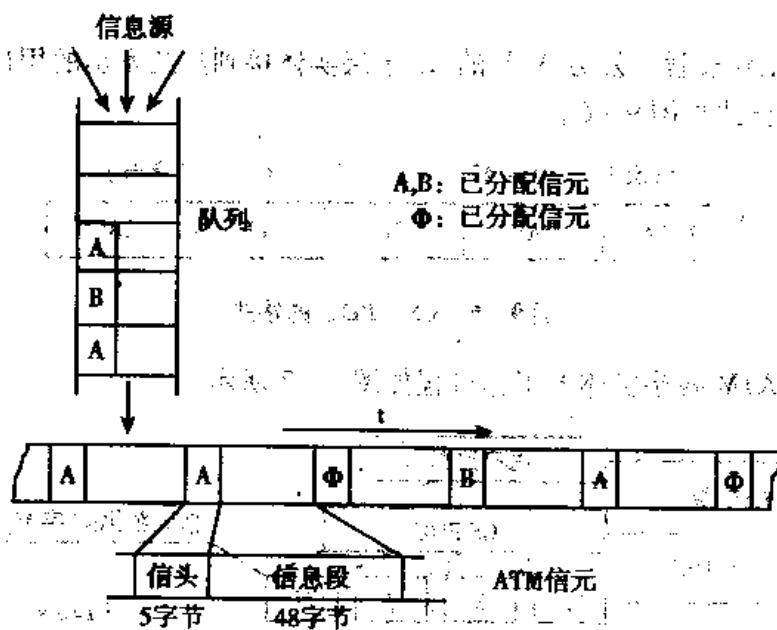


图 9-8 ATM 信元及其复用

信息源随机地产生信息, 因此信元到达队列也是随机的。高速的业务信元来得十分频繁、集中, 低速的业务信元来得很稀疏。这些信元都按先来后到在队列中排队, 然后按输出次序复用到传输线上。具有同样标志的信元在传输线上并不对应某个固定的时间间隙, 也不是按周期出现的, 也即信息和它在时域中的位置之间没有任何关系, 信息只是按信头中的标志来区分的。这种复用方式称为异步时分复用 (Asynchronous Time Division Multiplex), 又称统计复用 (Statistic Multiplex)。而在同步时分复用方式 (如 PCM 复用方式) 中, 信息以它在一帧中的时间位置 (时隙) 来区分, 一个时隙对应着一条信道, 不需要另外的信息头来标志信息的身份。

异步时分复用方式使 ATM 具有很大的灵活性, 任何业务都可按实际需要来占用资源。

对于特定的业务，传送速率可随信息到达的速率而变化，因此网络资源得到了最大限度的利用。ATM 网络可以适用于任何业务，不论其特性如何（速率高低、突发性大小、质量和实时性要求等），网络都按同样的模式来处理，真正做到了完全的业务综合。

若某个时刻队列中没有等待发送的信元，此时线路上就出现未分配信元（信头中含有标志 Φ ）；反之，若某个时刻传输线路上找不到可以传递信元的机会（信元都已排满），而队列已经充满缓冲区，此时为了尽量减少对业务质量的影响，将优先级别低的信元丢弃。缓冲区的容量必须根据信息流量来计算，以使信元丢失率在 10^{-9} 以下。

为了提高处理速度和降低延迟，ATM 以面向连接的方式工作。网络的处理工作十分简单：通信开始时建立虚电路，以后用户将虚电路标志写入信头（即地址信息），网络根据虚电路标志将信元送往目的地。

经过 ATM 复用后，信元流速率取决于传输线路的速率，如果采用单模光纤，速率可高达数 Gbps。每条虚电路的速率与属于该虚电路的信元出现的频率有关。

ATM 网络中的节点提供信元的交换。其实，ATM 网络的节点完成的只是虚电路的交换，因为同一虚电路上的所有信元都选择同样的路由，经过同样的通路到达目的地。在接收端，这些信元到达的次序总是和发送次序相同。

ATM 交换节点的工作比 X.25 分组交换网中的节点要简单得多。ATM 节点只做信头的 CRC 检验，对于信息段的传输差错根本不过问。ATM 节点不做差错控制（信头中根本没有信元的编号），也不参与流量控制，这些工作都留给终端去做。ATM 节点的主要工作就是读信头，并根据信头的内容快速地将信元送往要去的地方。这件工作在很大程度上依靠硬件来完成，所以 ATM 交换的速度非常快，可以和光纤的传输速度相匹配。

9.3 第三层交换技术

第三层交换技术是一种新兴的网络互连技术，它综合第二层交换和第三层路由的优点，在第三层提供交换能力。

9.3.1 第三层交换的引入

1. 传统的网络互连设备的局限性

传统的网络互连设备包括网桥、路由器、交换机等，虽然都能提供一定的网络互连功能，但又都存在不可克服的缺点。

网桥工作在数据链路层，既可以被用来分割网段，提高网络带宽，也可以作为网络互连设备来扩展网络覆盖范围。其优点是操作简单，速度快且与其它层次的协议无关；网桥没有路由功能，属简单的网络设备，易于维护且价格低廉。

但网桥无法实现流量控制，广播包的转发容易导致广播风暴，使整个网络瘫痪。而且网桥容易成为系统“瓶颈”，某些情况下，因网桥拥塞而丢失帧，使得网络不稳定、不可靠。

路由器工作在网络层，是一种智能化程度高、功能强大而复杂的网络互连设备。路由器

的功能主要包括：网络分段，将不同的 LAN 进行互连；路由选择，为跨越不同 LAN 的流量在网络上选择最适宜的路径；隔离广播，避免广播风暴的形成；安全管理与防火墙功能；广域网连接等。

但现在的网络应用越来越复杂，传输的信息量也迅猛增长，作为网络主干设备的路由器对网络性能形成了很大限制；路由器的功能主要是通过软件来实现的，处理延迟过高，容易成为网络“瓶颈”；当流经路由器的流量超过其吞吐量能力时，会使流经路由器的数据包丢失。路由器的这些限制给网络应用带来极大的麻烦。另外，路由器的复杂性还对网络的维护工作造成了沉重的负担。

交换机工作在数据链路层，可以看做是对多端口网桥的扩展。交换机可以用来分割 LAN，连接不同的 LAN，或扩展 LAN 的覆盖范围。交换机通常采用全硬件结构来实现，转发速度快，可以为每一个节点提供全部网络带宽，有效提供了网络带宽。但是由于交换机也只是工作在数据链路层的设备，因此同网桥一样，它也不具有隔离广播包的能力。

2. 第三层交换技术的引入

既然交换技术可以克服网络带宽的局限，并提供灵活的网络配置，而路由技术在目前的情况下又必不可少，于是人们就将这两种不同的技术结合起来，扬长避短，发挥它们各自的优点，从而推出一种新的网络互连技术，这就是第三层交换技术（Layer 3 Switching），简称 L3 交换。如果仅考虑 IP 网，则可称为 IP 交换技术（IP Switching）。

日益增长的数据报文流量要求能够以接近线路速度并且经济实用的方式来降低传统的路由器对数据报文依次处理带来的智能处理；如果应用于 MAN 和 LAN 的话，还必须考虑和已有 WAN 的端到端无缝互连；最后，这种新的技术必须继承传统的路由和转发可以实现的一些功能，例如广播和多播、网络安全、路由和管理策略控制等，同时这种新的技术所能提供的价格必须和现在已有的技术价格接近，不能太高。一种成功的解决方案将决定下一代网络互连和设备的操作方式和未来的拓扑结构乃至整个网络的体系结构。

目前已提出的 L3 交换解决方案分为两类：一类基于核心模型；另一类基于边缘多层混合交换模型。

9.3.2 局域网 L3 交换技术

1. Fast IP 技术

Fast IP 技术是一种典型的基于边缘多层混合交换模型的 L3 交换解决方案，它采用了“路由一次，随后交换”的技术。下一跳解析协议（Next Hop Resolution Protocol, NHRP）是 Fast IP 的主要技术基础。NHRP 协议用于 IPOA 中的非广播多路访问（NBMA）网络（如 ATM），它并不是一个路由协议，而只是一个逻辑 IP 子网 LIS 的地址解析协议。

Fast IP 实现了局域网环境中主机到主机模式的 NHRP 协议，从而可以减少中间的路由环节，提高网络性能。Fast IP 技术应用的正是“一次路由，随后交换”的思想。Fast IP 技术的基本思想是设法在数据交换过程中避开第三层路由器，即把基于 IP 的地址路由表的路由功能转换成基于端口—MAC 地址表的转发功能，从而实现完全的端到端高速交换通信，

使网络的性能获得提高。本质上, Fast IP 并不是要替代路由, 而是把交换和路由很好地结合在一起, 或者说在路由是既成事实的情况下, 设法对路由进行补充。

Fast IP 支持 ATM 和吉比特以太网环境, Fast IP 可以把网络的吞吐量提高 4~5 倍, 在 802.1p/Q 标准支持下还可以提高强大的服务质量保证。Fast IP 还可以和 WAN 互连。

但是, Fast IP 技术受到拓扑结构的限制, 这是因为 NHRP 响应是基于交换路径的。在源主机和目的主机之间必须存在交换路径, 否则无法应用 Fast IP 技术提高网络性能。

2. Net Flow 技术

Net Flow 技术是典型的基于核心模型的 L3 交换方案, 其目的是提高网络核心节点即路由器的性能。Net Flow 可以在路由器上进行软件升级, 使之对每一个数据报文不再采用传统的处理方法, 因而可以提高路由/转发能力。路由器的 CPU 可能会因为路由和转发方式的改进减轻一些负担, 但是 Net Flow 也会使 CPU 要处理的任務更多、更复杂, 需要提高 CPU 进行实时处理的能力。

在 Net Flow 技术中, 每一个数据报文仍然采用一般的第三层路由/交换方式, 处理之后路由器把第一个数据报文的信息记录在 Net Flow 高速缓存中, 后继的数据报文到达之后首先的高速缓存中进行匹配查找, 如果命中就使用高速缓存中的路由信息(例如下一个主机/中继路由器的 MAC 地址或本路由器的输出端口号)直接进行交换转发, 否则再进行通常的路由转发。

Net Flow 仍然工作在第三层, 而不是第二层。Cisco 总是反复强调路由器中“路由”和“转发”功能的区别, 并且习惯使用“交换”这个概念来描述路由器的“转发”功能, 可见 Net Flow 实现的交换并不是第二层上的直通(Cut Through)交换路径。

本质上, Net Flow 技术是一种传统路由和转发的改进方法, 即使用高速缓存的一个变种, 并在技术上做了一些改进。

和其它第三层交换技术不同, Net Flow 并没有建立连接源和目的主机系统的第二层交换路径, 它单独地在路由器上完成。在这里, 数据报文被“交换”只有局部意义, 与通常意义上的交换完全不同。

9.3.3 广域网 L3 交换技术

Tag Switching 技术是一种典型的基于核心模型的 L3 交换解决方案, 其基本思想是增强广域网核心路由器的路由/转发能力。Tag Switching 技术支持 ATM 和第三层路由的集成, 从而可以提高 Internet 的扩展性, 并克服 ATM LANE、IPOA 和 MPOA 效率低下的缺点。

支持 Tag Switching 技术的路由器被称为标记交换路由器(Tag Switching Router, TSR)。相邻的 TSR 之间的路由信息的交互都是基于网络层的路由协议, 如 OSPF、BGP 等。当路由表收敛后, 每个 TSR 为每条路径指定在本地生成的标记(Tag)。所谓标记是一个很短的长度固定的标号, 路由表根据标记进行路由表查找, 而不是根据传统的子网前缀, 显然前者比后者要快得多。每个标记可以标识一条或多条路径的聚集, 标记的分配是借助标记分配协议(Tag Distribution Protocol, TDP)来完成的。

每个 TSR 都要实现两个基本的功能: 基于标记的转发/交换功能, 以及对互连 TSR 的合

法标记集的管理功能。这两个功能也不是单纯靠软件来实现的，Cisco 使用硬件来实现第一个功能，即基于标记的转发/交换功能以提高效率。

当一个数据报文到达 TSR 之后，TSR 检查其标记域，并把它作为标记信息数据库（Tag Information dataBase，TIB）的索引进行查找。TIB 中的每一项都包括了输入标记和与之相关的转发信息。对于单目的数据通信来说，转发信息包括输出标记、输出端口、输出所需的帧信息（例如下行路由器的 MAC 地址）；对于多播而言，转发信息则包括了多组这样的信息。由于转发算法是基于标记进行查找匹配，比传统的最长子网前缀匹配要快得多，并且标记本身长度固定，这些特点使得 Tag Switching 技术非常易于使用专用硬件集成电路（Application Specific Integrated Circuit，ASIC）来实现。

9.4 虚拟局域网技术

虚拟局域网（Virtual LAN，VLAN）是通过路由和交换设备在网络的物理拓扑结构基础上建立的逻辑网络。一个 VLAN 可以看做是一组网络节点的集合，这些节点不必位于同一个物理网络中，但可以不受地理位置的限制而像在同一个局域网中那样进行数据通信。一般认为，VLAN 等价于一个第二层广播域或者等价于一个第三层网络。

VLAN 代表着一种不用路由器实现对广播数据进行抑制的解决方案。在 VLAN 中，对广播数据的抑制由交换机完成。此时每一个物理网段可以仅包含一个用户，而一个广播域中则可以具有多达 1000 个以上的用户。另外，VLAN 还可以跟踪各个网络节点物理位置的变化，使之在移动位置后不需要对其网络地址重新进行手工配置。

9.4.1 虚拟局域网的交换技术

建立虚拟局域网的交换技术包括端口交换（Port Switch）、帧交换（Frame Switch）和信元交换（Cell Switch）3 种方式。

（1）端口交换。端口交换又称配置交换，最初的方式是把端口经过手工配置到一个或若干个通过背板连接的共享集线器上，可以形成若干个独立的由端口组合的共享传输介质段，每一个连接到端口上的用户被分配到其中一个段上。近年来发展成为由一个或几个通过背板连接的端口交换机，通过软、硬件的控制和管理，把交换机上的端口划分成若干个共享式的互相独立的 VLAN。

由于端口交换形成的 VLAN 还是共享介质段，因此使用这种方式形成的 VLAN，端口用户以及整个 VLAN 的带宽受到限制。对需要高带宽的端口用户或者规模较大、对带宽要求高的 VLAN 来说，选用全交换的网络设备是必需的。

（2）帧交换。在帧交换中，局域网交换机在每一个端口上提供一个独立的共享介质端口，在此端口上可以接共享集线器也可以接单独的一个网络节点。在一个端口上接收到的帧被正确地转发到输出端口上，在寻路和转发时帧是不会被破坏的。对于广播帧来说，可以转发到交换机上的所有端口。

帧交换方式的特点是比端口交换增加了有效的带宽，LAN 交换机上每个端口用户具有

独占带宽的性能,交换机间互连的速率可达数百兆甚至千兆位的数据传输率。服务器和高速客户站可以直接连到交换机端口上。

目前,绝大多数厂家的局域网交换机均按帧交换方式来实现 VLAN 的交换,以太网交换机与端口交换机组合应用,使用户加入 VLAN 更灵活。

(3) 信元交换。信元交换在 ATM 交换机上实现。一个或者多个互连的 ATM 交换机组成网络的核心系统,类似于帧交换,所不同的是从 ATM 交换机端口上接收到信元后,正确地转发到输出端口。ATM 允许网络节点加入多个 VLAN,允许一条物理信道上实现多个逻辑连接。ATM 上目前常采用 ATM LANE 技术实现 VLAN。

9.4.2 虚拟局域网的划分方法

划分 VLAN 的方法有很多种,常用的方法包括按交换端口号、按 MAC 地址或者按第三层协议来划分 VLAN。

(1) 按交换端口号划分 VLAN。通常将交换设备端口进行分组来划分 VLAN。例如,将交换机的 1、3、5、7 端口划分为 VLAN1,而将 2、4、6、8 端口划分为 VLAN2。

时至今日,按端口号划分 VLAN 仍然是构造 VLAN 的一个最常用的方法。而且此种方法也确实比较简单并且非常有效。但仅靠端口号来分组定义 VLAN 将无法实现同一个物理分段(或交换端口)同时参与到多个 VLAN 中,而且更要紧的是当一个网络节点从一个端口移至另一个端口时,网管人员将不得不对 VLAN 成员进行重新配置。

(2) 按 MAC 地址划分 VLAN。由网管人员指定属于同一个 VLAN 的各网络节点的 MAC 地址。由于 MAC 地址是固化在网卡中的,故移至网络中另外一个地方时他将仍保持其原先的 VLAN 成员身份而无须网管人员对之进行重新的配置,另外在此种方式中,同一个 MAC 地址处于多个 VLAN 中是不成问题的。

但这种方法也有许多不足之处,首先所有的用户在最初都必须将网络节点手工配置到至少一个 VLAN 中,只有在经过手工配置之后方可实现对 VLAN 成员的自动跟踪。但在大型的网络中完成初始的配置并不是一件容易的事。

(3) 按第三层协议划分 VLAN。基于第三层协议的 VLAN 划分决定 VLAN 成员身份时主要是考虑协议类型(支持多协议的情况下)或网络层地址(如 TCP/IP 网络的子网地址)。此种类型的 VLAN 划分需要将子网地址映射到 VLAN,交换设备则根据子网地址而将各机器的 MAC 地址同一个 VLAN 联系起来。交换设备将决定不同网络端口上连接的机器是否属于同一个 VLAN。

按第三层协议划分 VLAN 有许多优点。首先可以根据协议类型进行 VLAN 划分,这对那些基于服务或基于应用 VLAN 策略的网管人员无疑是极具吸引力的。其次,用户可以自由地移动他们的机器而无须对网络地址进行重新配置,并且不再需要提交标识,从而可以消除因在交换设备之间传递 VLAN 成员信息而花费的开销。

按第三层协议划分 VLAN 的主要缺点是其性能问题。对报文中的网络地址进行检查将比对帧中的 MAC 地址进行检查开销更大。正是由于这个原因,使用第三层协议信息进行 VLAN 划分的交换设备一般都比使用第二层信息的交换设备要慢。

9.4.3 虚拟局域网的互连方式

一般情况下网络环境中的 VLAN 实现了网络流量的分割,但 VLAN 之间互连和数据传输仍要借助于路由手段来实现,而对于无法进行路由选择的协议则借助于交换功能来实现。目前基本上有 4 种不同的 VLAN 路由模式:边界路由、“独臂”路由器、MPOA 路由、第三层交换。

(1) 边界路由。边界路由指的是将路由功能包含在位于主干网络边界的每一个 LAN 交换设备中,此时 VLAN 间的报文将由交换设备内在的路由能力进行处理,从而无须再将其传送到某个外部的路由器上,数据的转发延迟因而也将得以降低。

使用这种路由方式的主要优点在于不像集中式路由那样会因中央路由站点的崩溃而导致主干网络的瘫痪。主要缺点在于:相对统一路由功能的集中式管理而言,边界路由需要对多个物理设备进行管理,另外这种方式可能比由一个集中式路由器和多个较便宜的边界路由器组成的集中式方案在价格上要贵一些。

(2) “独臂”路由器。采用“独臂”路由器的网络方案能消除主干网上集中式处理和高延迟的路由功能。这种路由器一般接在主干网的一个交换设备上,以使得网络中的大部分报文在通过主干网时无须通过路由器进行处理,而且配置和管理起来也比较方便。

同一个 VLAN 内的报文将用不着通过路由器而直接在交换设备之间进行高速传输。显然此种路由方式只是在大部分报文都无须经过路由器进行处理时效果才能比较理想。为此在规划 VLAN 解决方案时应尽可能地减少 VLAN 之间的数据传输量。但这种路由方式的不足之处在于它仍然是一种集中式的路由策略,因此在主干网上一般均设置有多余的“独臂”路由器,但如果网络中 VLAN 之间的数据传输量比较大,那么在路由器处将形成“瓶颈”。

(3) MPOA 路由。MPOA 的目的是给可能属于不同路由子网的多个用 ATM 网络连接的设备提供直接的虚拟连接,也就是说, MPOA 将使得多个属于不同 ELAN 的站点通过 ATM 网络直接进行通信,而用不着经过一个中间的路由器。其中 ELAN 就可以看成是一种形式的 VLAN,它是在 ATM 网络环境下用 LANE 标准建立起来的。

MPOA 实际上可以看成是将路由功能集成到 LAN—ATM 边界交换设备中,这样一来在 VLAN 之间的通信中将不再需要外部路由器,从而降低网络传输的延迟。

(4) 第三层交换。在上一节中,已经详细地介绍了各种第三层交换技术的原理和特点,有的技术方案本身就是一个带有路由功能的交换机。特别是具有智能可编程 ASIC 的第三层交换机(如 3Com 与 Bay 公司的产品),它既包括了第二层和第三层的交换功能,而且还具备路由寻址功能。因此可以利用它来作为网络的主干交换机,既可以根据多种方法来定义 VLAN 成员,随后配置 VLAN,又能不附加其它路由设备来实现 VLAN 之间的通信。不论从网络结构还是降低网络传输延迟来说,采用第三层交换技术都不失是一个很好的选择。

9.5 虚拟专用网 VPN

9.5.1 何谓 VPN

顾名思义,虚拟专用网 VPN (Virtual Private Network) 并不是真正的专用网络,但却能实现专用网络的功能。虚拟专用网指的是依靠 ISP (Internet 服务提供商) 和其它 NSP (网络服务提供商),在公用网络中建立专用的数据通信网络的技术。在虚拟专用网中,任意两个节点之间的连接并没有传统专网所需的端到端的物理链路,而是利用某种公众网的资源动态组成的。所谓虚拟,是指用户不再需要拥有实际的长途数据线路,而是使用 Internet 公众数据网络的长途数据线路;所谓专用网络,是指用户可以为自己制定一个最符合自己需求的网络。

虚拟专用网一般指的是构建在 Internet 上能够自我管理的专用网络,而不是 Frame Relay 或 ATM 等提供虚拟固定线路 (PVC - Permanent Virtual Circuit) 服务的网络。以 IP 为主要通信协议的 VPN,也可称之为 IP - VPN。

由于 VPN 是在 Internet 上临时建立的安全专用虚拟网络,用户就节省了租用专线的费用,在运行的资金支出上,除了购买 VPN 设备外,企业所付出的仅仅是向企业所在地的 ISP 支付一定的上网费用,也节省了长途电话费。这就是 VPN 价格低廉的原因。

9.5.2 VPN 的特点

(1) 安全保障。VPN 的实现技术和方式很多,但所有的 VPN 均应保证通过公用网络平台传输数据的专用性和安全性。在非面向连接的公用 IP 网络上建立一个逻辑的、点对点的连接,称之为建立一个隧道,可以利用加密技术对经过隧道传输的数据进行加密,以保证数据仅被指定的发送者和接收者了解,从而保证了数据的私有性和安全性。在安全性方面,由于 VPN 直接构建在公用网上,实现简单、方便、灵活,但同时其安全问题也更为突出。企业必须确保其 VPN 上传送的数据不被攻击者窥视和篡改,并且要防止非法用户对网络资源或私有信息的访问。ExtranetVPN 将企业网扩展到合作伙伴和客户,对安全性提出了更高的要求。

(2) 服务质量保证 (QoS)。VPN 网应当为企业数据提供不同等级的服务质量保证。不同的用户和业务对服务质量保证的要求差别较大。如移动办公用户,提供广泛的连接和覆盖性是保证 VPN 服务的一个主要因素;而对于拥有众多分支机构专线 VPN 网络,交互式的内部企业网应用则要求网络能提供良好的稳定性;对于其它应用 (如视频等) 则对网络提出了更明确的要求,如网络时延及误码率等。所有以上网络应用均要求网络根据需要提供不同等级的服务质量。在网络优化方面,构建 VPN 的另一重要需求是充分有效地利用有限的广域网资源,为重要数据提供可靠的带宽。广域网流量的不确定性使其带宽的利用率很低,在流量高峰时引起网络阻塞,产生网络“瓶颈”,使实时性要求高的数据得不到及时发送;

而在流量低谷时又造成大量的网络带宽空闲。QoS 通过流量预测与流量控制策略, 可以按照优先级分配带宽资源, 实现带宽管理, 使得各类数据能够被合理地先后发送, 并预防阻塞的发生。

(3) 可扩充性和灵活性。VPN 必须能够支持通过 Intranet 和 Extranet 的任何类型的数据流, 方便增加新的节点, 支持多种类型的传输介质, 可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

(4) 可管理性。从用户角度和运营商角度应可方便地进行管理、维护。在 VPN 管理方面, VPN 要求企业将其网络管理功能从局域网无缝地延伸到公用网, 甚至是客户和合作伙伴。虽然可以将一些次要的网络管理任务交给服务提供商去完成, 企业自己仍需要完成许多网络管理任务。所以, 一个完善的 VPN 管理系统是必不可少的。VPN 管理的目标为: 减小网络风险、具有高扩展性、经济性、高可靠性等优点。VPN 管理主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS 管理等内容。

9.5.3 VPN 的安全技术

目前 VPN 主要采用如下四项技术来保证安全: 隧道技术 (Tunneling)、加解密技术 (Encryption & Decryption)、密钥管理技术 (Key Management)、使用者与设备身份认证技术 (Authentication)。

(1) 隧道技术。隧道技术是 VPN 的基本技术, 类似于点对点连接技术, 它在公用网建立一条数据通道 (隧道), 让数据包通过这条隧道传输。隧道是由隧道协议形成的, 分为第二、三层隧道协议。第二层隧道协议是先把各种网络协议封装到 PPP 中, 再把整个数据包装入隧道协议中, 这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有 L2F、PPTP、L2TP 等; 第三层隧道协议是把各种网络协议直接装入隧道协议中, 形成的数据包依靠第三层协议进行传输。第三层隧道协议有 VTP、IPSec 等。

(2) 加解密技术。加解密技术是数据通信中一项较成熟的技术, VPN 可直接利用现有技术实现加解密。

(3) 密钥管理技术。密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为 SKIP 与 ISAKMP/OAKLEY 两种。SKIP 主要是利用 Diffie-Hellman 的演算法则, 在网络上传输密钥; 在 ISAKMP 中, 双方都有两把密钥, 分别用于公用、私用。

(4) 使用者与设备身份认证技术。使用者与设备身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

9.5.4 VPN 的发展趋势

Internet 已成为全社会的信息基础设施, 企业端应用也大都基于 IP, 在 Internet 上构筑应用系统已成为必然趋势。因此基于 IP 的 VPN 业务获得了极大的增长空间。

以前无论因特网的远程接入还是专线接入, 以及骨干传输的带宽都很小, QoS 更是无法保障, 造成企业用户宁愿花费大量的金钱去投资自己的专线网络或是宁愿花费巨额的长途话

费来提供远程接入。现在随着 ADSL、DWDM、MPLS 等新技术的大规模应用和推广, 上述问题将得到根本改善和解决。目前大多企业用户可以享受到 10Mbps 乃至 100Mbps 的 Internet 专线接入, 而骨干网发展到上百乃至上千个 Gbps 已不是技术问题。随着互联网技术的发展, VPN 的应用必将得到迅速普及。

VPN 技术将成为当前广域网建设的最佳解决方案之一, 它不仅大大节省了广域网的建设和运行维护费用, 而且增强了网络的可靠性和安全性。同时, VPN 将加快企业网的建设步伐, 使得集团公司不仅仅只是建设内部局域网, 而且能够很快地把全国各地分公司的局域网连起来, 从而真正发挥整个网络的作用。VPN 对推动整个电子商务、电子贸易也将起到不可低估的作用。

9.6 计算机网络管理与安全

计算机网络管理是计算机网络发展中的关键技术, 对网络的正常运行起着极其重要的作用。网络管理的目的是协调、保持网络系统的高效、可靠运行, 当网络出现故障时, 能及时报告和处理。计算机网络的安全问题随着 Internet 的发展越来越被人们所重视。由于计算机网络所具有的开放性、互连性等特征, 致使网络容易受到各种攻击和破坏, 无论是在局域网还是广域网中, 都存在着自然和人为等诸多因素形成的潜在安全威胁。大量在网络中存储和传输的数据需要被保护, 这些数据在网络中存储和传输的过程中, 都有可能被盗用、暴露或篡改。

9.6.1 网络管理基本功能

ISO 建议网络管理应包含以下基本功能: 故障管理、计费管理、配置管理、性能管理和安全管理。

(1) 故障管理 (Fault Management)。故障管理是网络管理中最基本的功能之一。当网络发生故障时, ①必须尽可能快地找出故障发生的确切位置; ②将网络其它部分与故障部分隔离, 以确保网络其它部分能不受干扰继续运行; ③重新配置或重组网络, 尽可能降低由于隔离故障后给网络带来的影响; ④修复或替换故障部分, 将网络恢复为初始状态。对网络组成部件状态的监测是网络故障检测的依据。不严重的简单故障或偶然出现的错误通常被记录在错误日志中, 一般需作特别处理; 而严重一些的故障则需要通知网络管理器, 即发出报警。因此网络管理器必须具备快速和可靠的故障监测、诊断和恢复功能。

(2) 计费管理 (Accounting Management)。在商业性有偿使用的网络上, 计费管理功能统计哪些用户、使用何信道、传输多少数据、访问什么资源等信息; 另一方面, 计费管理功能还可以统计不同线路和各类资源的利用情况。由此可见, 计费管理的根本依据是网络用户资源的情况, 例如, 信息传输量、占用线路的时间等统计量。一个网络管理系统必须记录这些信息, 并制定一种用户可接受的计费方法。商业性网络中的计费系统还要包含诸如每次通信的开始和结束时间、通信中使用的服务等级以及通信中的另一方等更详细的计费信息, 并让用户能够随时查询这些信息。

(3) 配置管理 (Configuration Management)。配置管理也是网络管理的基本功能。计算机网络由各种物理结构和逻辑结构组成, 这些结构中还有许多参数、状态等信息需要设置并协调。另外, 网络运行在多变的环境中, 系统本身也经常要随着用户的增、减或设备的维修而调整配置。网络管理系统必须具有足够的手段支持这些调整的变化, 使网络更有效地工作。这些手段构成了网络管理的配置管理功能。配置管理功能至少应包括识别被管理网络的拓扑结构、标识网络中的各种现象、自动修改指定设备的配置、动态维护网络配置数据库等内容。

(4) 性能管理 (Performance Management)。性能管理的目的是在使用最少的网络资源和具有最小延迟的前提下, 确保网络能提供可靠、连续的通信能力, 并使网络资源的使用达到最优化的程度。网络的性能管理有监测和控制两大功能, 监测功能实现对网络中的活动进行跟踪, 控制功能实施相应调整来提高网络性能。性能管理的具体内容包括: 从被管对象中收集与网络性能有关的数据, 分析和统计历史数据, 建立性能分析的模型, 预测网络性能的长期趋势, 并根据分析和预测的结果, 对网络拓扑结构、某些对象的配置和参数做出调整, 逐步达到最佳运行状态。如果需要做出的调整较大时, 还要考虑扩充或重建网络。

(5) 安全管理 (Security Management)。安全管理的目的是确保网络资源不被非法使用, 防止网络资源由于入侵者攻击而遭受破坏。其主要内容包括: 与安全措施有关的信息分发 (如密钥的分发和访问权设置等), 与安全有关的通知 (如网络有非法入侵、无权用户对特定信息的访问企图等), 安全服务措施的创建、控制和删除, 与安全有关的网络操作事件的记录、维护和查询日志管理工作等。一个完善的计算机网络管理系统必须制定网络管理的安全策略, 并根据这一策略设计实现网络安全管理系统。

目前最有影响的网络管理协议有两个: 一个是简单网络管理协议 SNMP (Simple Network Management Protocol); 另一个是公共管理信息服务和公共管理信息协议 CMIS/CMIP (Common Management Information Service/Common Management Information Protocol)。

ISO 早在提出 OSI/RM 的同时, 就提出了网络管理标准的框架, 并制定了基于开放系统互连参考模型的 CMIS/CMIP。然而由于种种原因, 符合 OSI 网络管理标准的可供实用的产品几乎没有。与此同时, Internet 组织在长期运行因特网的实践中, 提出了一个基于 TCP/IP 协议簇的网络管理标准协议 SNMP, 并得到了众多网络产品生产厂家的广泛支持, 使之成为事实上的网络管理工业标准。

计算机网络安全包括物理安全和信息安全。物理安全是指网络设备、程序、线路等方面的安全; 信息安全则是防止在网络中存储或传送的信息受到破坏。

9.6.2 网络安全

1. 网络安全的概念

从广义上讲, 术语“网络安全” (Network Security) 和“信息安全” (Information Security) 是指确保网络上的信息和资源不被非授权用户所使用, 通常把为了保护数据及反黑客而设计的工具的集合成为计算机安全 (Computer Security)。

网络安全是为了在数据传输期间保护这些数据并且保证数据的传输是可信的, 它强调的

是网络中信息或数据的完整性 (Integrity)、可用性 (Availability) 以及保密性 (Confidentiality and Privacy)。所谓完整性, 是指保护信息不被非授权用户修改或破坏; 可用性是指避免拒绝授权访问或拒绝服务; 保密性是指保护信息不被泄露给非授权用户。

2. 网络安全攻击

正常情况下, 信息从信源传向信宿, 如图 9-9(a) 所示。通常的网络安全攻击有以下四种形式: 中断是以可用性作为攻击目标, 它毁坏系统资源 (如硬件), 切断通信线路, 或使文件系统变得不可用, 如图 9-9(b) 所示; 截获是以保密性作为攻击目标, 非授权用户通过某种手段获得对系统资源的访问, 如搭线窃听、非法拷贝等, 如图 9-9(c) 所示; 修改是以完整性作为攻击目标, 非授权用户不仅获得对系统资源的访问, 而且对文件进行篡改, 如改变文件中的数据或者修改网上传输的信息等, 如图 9-9(d) 所示; 伪造是以完整性作为攻击目标, 非授权用户将伪造的数据插入到正常系统中, 如在网络上散布一些虚假信息等, 如图 9-9(e) 所示。

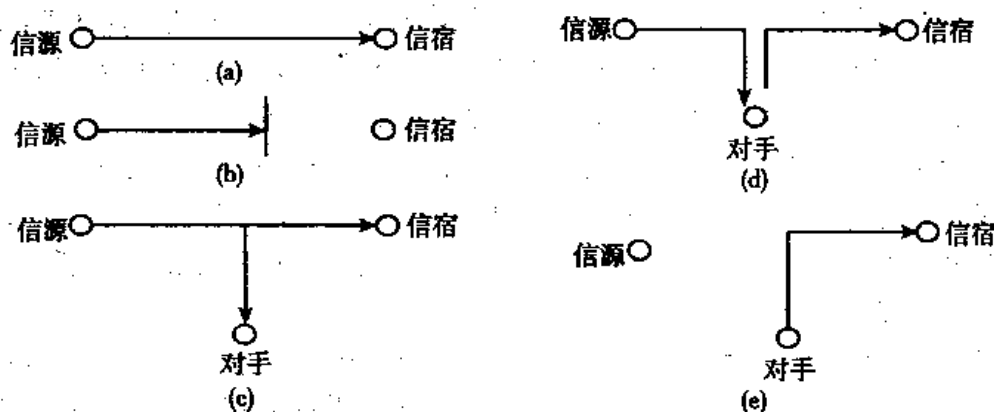


图 9-9 网络安全攻击的几种形式

网络安全攻击又可分为主动攻击和被动攻击。被动攻击的主要目的是窃听和监视信息的传输并存储, 攻击者只是想获得被传送的信息。被动攻击通常很难被检测出来, 因为它不改变数据, 但预防这种攻击的发生是可能的。因此, 对被动攻击通常是采取预防手段而不是检测恢复手段。主动攻击通常修改数据流或创建一些虚假数据流。对于主动攻击, 要绝对预防是非常困难的, 因为这需要在所有时间内对所有通信设施或路径实行物理安全保护。但是主动攻击通常可以采取有效的监测和恢复手段进行保护。

3. 网络安全机制

安全策略 (Security Policy) 是描述保护数据或信息的规则, 但不需要规定具体的技术实现。网络安全机制是网络安全策略的实施手段。一种安全策略可以由一种或多种安全机制实现, 一种安全机制也可以支持多种安全策略。安全机制的种类繁多, 如加密机制、认证机制、数字签名机制以及检测机制 (如病毒检测和入侵检测) 等。

(1) 传统的加密机制。数据加密技术由来已久, 随着数字技术、信息技术、网络技术的发展, 数据加密技术也不断发展。加密技术历史悠久, 随着算法、计算机技术的发展, 其功能也越来越强大。所谓加密就是将明文 (原信息) 经过处理转换成密文 (与原信息不同

的、不易理解的信息)的过程,解密是加密的逆过程,即将密文翻译成明文的过程。加密/解密必须遵循明文与密文的相互交换是惟一的、无误差的可逆变换的规则。

根据数据加密的密钥的情况,可以将加密技术分为对称数据加密技术和非对称数据加密技术。对称数据加密技术的加密和解密过程采用同一把密钥,即加密密钥和解密密钥相同。非对称数据加密技术的加密和解密过程采用不同的密钥,即加密密钥和解密密钥不同。发送方只知道加密密钥,而解密密钥只有接收方自己知道。

这里所述的传统加密也称为对称加密或单密钥加密,是在20世纪70年代出现公开密钥加密之前存在的惟一一种加密机制。传统的加密机制由五部分组成。

明文:原始的报文或数据,作为输入被送入算法。

加密算法:对明文执行各种替代和替换的算法。

密钥:是加密算法的输入,加密算法执行什么样的替代和转换则取决于密钥。

密文:经过加密算法和密钥替代和转换后形成的混乱的报文。

解密算法:是加密算法的逆行运行,它接受密文和密钥;并还原出原始的明文。

传统的加密技术是发送方和接收方必须使用相同的密钥,而且密钥必须保密,这种加密方法称为秘密密钥加密。它的原理是:发送方用该密钥对待发数据进行加密,然后加密数据传送到接收方,接收方再用相同的密钥对收到的加密数据进行解密。

(2) 公开密钥加密。公开密钥加密技术是给每个用户分配两把密钥:一个是保密的私有密钥;另一个是公开密钥。该方法的加密函数必须具备如下数学特性:用公开密钥加密的数据除了使用相应的私有密钥外很难被解密;同样,使用私有密钥加密的数据除了使用相应的公开密钥外也很难被解密。

这种方法是安全的,因为加密和解密的函数具有单向性质。也就是说,仅知道了公开密钥并不能伪造由相应私有密钥加密过的数据。可以证明,公开密钥加密法能够保证保密性。只要发送方使用接收方的公开密钥来加密待发数据,那么就只有接收方能够解密该加密数据,因为解密必须要知道接收方的私有密钥。

(3) 加密算法。最常用的传统加密算法是分组密码(Block Ciphers),它将明文输入变成固定长度的数据块,并生成与明文大小相同的密文块。两种最重要的传统算法是DES和TDEA,它们都属于分组密码。DES(Data Encryption Standard)是美国国家标准与技术研究院于1977年采纳的标准定义。DES明文长度是64bit,而密钥的长度为56bit。1985年,三重DES(TDEA, Triple DES)在ANSI X9.17中第一次被标准化,用于金融应用。三重DES使用了三个密钥,并执行了三次DES算法,这个函数的执行顺序是加密—解密—加密,在第二个阶段中使用的解密不具有密码的含义,它的惟一作用就是让三重DES的用户能够解密以前单次DES用户加密的数据。使用三个不同的密钥,TDEA的有效密钥长度为168bit。

(4) 认证(Authentication)。加密可以保护数据不受被动攻击(窃听),而要保护数据不受主动攻击(数据的伪造和变动)则有不同的要求。防止此类攻击的保护措施称为报文认证。

报文的认证过程使通信各方能够证实接收到的报文是可信的。有两个重要的内容需要证实,一方面是报文的内容没有被改变,另一方面报文的来源是可信的。

报文的认证方式有以下四种:

① 使用传统加密方式的认证,假设发送方和接收方共享一个密钥,只有真正的发送方

才能成功地加密发往对方的报文。

② 没有报文加密的报文认证，这是不依靠加密的报文认证方式。在这种方式中，需要生成一个认证标签，并将其附加在每个报文上进行传输。报文本身并没有经过加密，并且可以由目的端读取，读取过程与目的端的认证函数无关。

③ 使用密钥的报文认证码方式，它是使用密钥来生成一小块数据，被附加在报文上。这种技术假设通信双方共享一个公共的密钥 K_{AB} (AB 是发送方和接收方)。当 A 有报文要发送到 B 时， A 通过计算得到报文认证码，这个报文认证码是报文与密钥的一个函数。报文再加上一个编码被一起传输到接收方。接收方根据接收到的报文，并使用相同的密钥来执行相同的计算，以生成一个新的报文认证码，将接收到的编码与计算得到的编码进行比较。

④ 使用单向散列函数的认证。单向散列函数是一种报文认证码的变形。散列函数接收变长的报文 M 作为输入，并产生固定尺寸的标签 $H(M)$ 作为输出。与报文认证码不同的是，散列函数不用密钥作为输入。为了证实一个报文，报文摘要要与报文一起发送，并且被认证是报文摘要。认证报文摘要要有散列方法，即传统加密方法、公开密钥加密和保密的值。

(5) 数字签名。所谓数字签名 (Digital Signature)，就是附加在数据单元上的一些数据，或是对数据单元作的密码变换，也就是信息的发送者使用公开密钥算法的主要技术产生的别人无法伪造的一段数字串。发送者用自己的私有密钥将数据加密后传送给接收者，接收者用发送者的公钥解开数据后，就可确定消息来自于谁，这也是对发送者发送的信息真实性的一个证明，发送者对所发信息不能反悔。

之所以使用数字签名，是因为对文件进行加密只解决了传送信息的保密问题，而防止他人对传输的文件进行破坏，以及如何确定发信人的身份还需要采取其它的手段，而这一手段就是数字签名。在电子商务安全保密系统中，数字签名技术有着特别重要的地位，在电子商务安全服务中的源认证、完整性服务、不可否认服务中都要用到数字签名技术。

目前的数字签名是建立在公共密钥体制基础上的，它是公共密钥加密技术的另一类应用。它的主要方式是，报文发送方从报文文本中生成一个 128 位的散列值 (或报文摘要)。发送方用自己的私人密钥对这个散列值进行加密来形成发送方的数字签名。然后，这个数字签名将作为报文的附件和报文一起发送给报文的接收方。接收方首先从接收到的原始报文中计算出 128 位的散列值 (或报文摘要)，接着再用发送方的公用密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

数字签名与书面文件签名有相同之处，采用数字签名也能确认以下两点：第一，信息是由签名者发送的；第二，信息自签发后到收到为止曾作过任何修改。这样数字签名就可用来防止电子信息被修改 (窜改)，或冒用他人名义发送信息 (伪造)，或发出 (收到) 信件后又加以否认等情况发生。

应用广泛的数字签名方法主要有三种，即 RSA 签名、DSS 签名、Hash 签名。这三种算法可单独使用，也可综合在一起使用。

用 RSA 或其它公开密钥密码算法的最大方便是没有密钥分配问题，因为公开密钥加密使用两个不同的密钥，其中有一个是公开的，另一个是保密的。RSA 算法中数字签名技术实际上是通过一个哈希函数来实现的。数字签名的特点是它代表了文件的特征，如果文件发生改变，则数字签名的值也将发生变化。不同的文件将得到不同的数字签名。一个最简单的

哈希函数是把文件的二进制编码相累加，取最后的若干位。哈希函数对发送数据的双方都是公开的。

DSS 数字签名是由美国国家标准化研究院和国家安全局共同开发的。由于它是美国政府颁布实施的，主要用于与美国政府做生意的公司，其它公司则较少使用，它只是一个签名系统，而且美国政府不提倡使用任何削弱政府窃听能力的加密软件，认为这才符合美国的国家利益。

Hash 签名是最主要的数字签名方法，也称之为数字摘要法 (Digital Digest) 或数字指纹法 (Digital Finger Print)。它与 RSA 数字签名不同，该数字签名方法是将数字签名与要发送的信息紧密联系在一起，它更适合于电子商务活动。将一个商务合同的内容与签名结合在一起传播，比合同和签名分开传输增加了可信度和安全性。数字摘要加密方法称安全 Hash 编码法 (Secure Hash Algorithm, SHA) 或 MD5 (Standard For Message Digest)，由 Ron River 所设计。该编码法采用单向 Hash 函数将需加密的明文“摘要”成一串 128b 的密文，这一串密文亦称为数字指纹 (Finger Print)，它有固定的长度，且不同的明文摘要必定一致。这样这串摘要便可成为验证明文是否是“真身”的“指纹”了。

只有加入数字签名及验证才能真正实现在公开网络上的安全传输。加入数字签名和验证的文件传输过程如下：

① 首先发送方用哈希函数从原文得到数字签名，然后采用公开密钥体系用发送方的私有密钥对数字签名进行加密，并把加密后的数字签名附加在要发送的原文后面。

② 发送方选择一个秘密密钥对文件进行加密，并把加密后的文件通过网络传输到接收方。

③ 发送方用接收方的公开密钥对秘密密钥进行加密，并通过网络把加密后的秘密密钥传输到接收方。

④ 接收方使用自己的私有密钥对密钥信息进行解密，得到秘密密钥的明文。

⑤ 接收方用秘密密钥对文件进行解密，得到经过加密的数字签名。

⑥ 接收方用发送方的公开密钥对数字签名进行解密，得到数字签名的明文。

⑦ 接收方用得到的明文和哈希函数重新计算数字签名，并与解密后的数字签名进行对比。如果两个数字签名是相同的，则说明文件在传输过程中没有被破坏。

如果第三方冒充发送方发出了一个文件，因为接收方在对数字签名进行解密时使用的是发送方的公开密钥，只要第三方不知道发送方的私有密钥，则解密出来的数字签名和经过计算的数字签名必然是不相同的。这就提供了一个安全的确认发送方身份的方法。

数字签名的加密解密过程和私有密钥的加密解密过程虽然都使用公开的密钥体系，但实现的过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密，这是一个一对多的关系：任何拥有发送方公开密钥的人都可以验证数字签名的正确性。私有密钥的加密解密则使用的是接收方的密钥对，这是多对一的关系：任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有惟一拥有接收方私有密钥的人才能对信息解密。在实用过程中，通常一个用户拥有两个密钥对，一个密钥对用来对数字签名进行加密解密，一个密钥对用来对私有密钥进行加密解密。这种方式提供了更高的安全性。

习 题

1. 简述 X.25 各类分组的格式及其功能。
2. 在 X.25 分组级中,理论上最多允许存在多少条虚电路?若已知分配的虚电路号为 536,试计算其二进制逻辑信道组号及逻辑信道号。
3. 帧中继与 X.25 相比较,帧中继有什么优缺点?应用如何?
4. 简述帧中继的工作原理。为什么帧中继的层次结构中只有物理层和数据链路层?
5. 简述 ATM 的工作原理及其信元的结构。并说明信元头部各字段的作用和意义。
6. 简要说明 ATM 传输过程。
7. 传统的网络互连设备如网桥、路由器和交换机存在什么样的局限性?
8. 什么是第三层交换?第三层交换有哪些解决方案?
9. 简述 Fast IP 技术的基本原理和工作过程。
10. 简述 Net Flow 技术的基本原理和工作过程。
11. 简述 Tag Switching 技术的基本原理和工作过程。
12. 什么是虚拟局域网?引入虚拟局域网的意义何在?
13. 建立虚拟局域网的交换技术有哪些?
14. 简要说明划分虚拟局域网的方法。
15. 简述虚拟局域网的互连方式。
16. 什么叫 VPN?它有哪些特点?如何保证安全?在哪些场合应用?
17. 网络管理包含哪些基本功能?
18. 简述网络安全的概念。
19. 简述对称数据加密技术和非对称数据加密技术的工作原理。
20. 简述认证和数字签名的工作原理和应用。

计算机网络原理自学考试大纲

全国高等教育自学考试指导委员会制定

出版前言

为了适应社会主义现代化建设事业对培养人才的需要,我国在20世纪80年代初建立了高等教育自学考试制度。高等教育自学考试是个人自学、社会助学和国家考试相结合的一种高等教育形式,是我国高等教育体系的重要组成部分。实行高等教育自学考试制度,是落实宪法规定的“鼓励自学成才”的重要措施,是提高中华民族思想道德和科学文化素质的需要,也是培养和选拔人才的一种途径。自学考试应考者通过规定的专业课程考试并经思想品德鉴定达到毕业要求的,可以获得毕业证书,国家承认学历,并按照规定享有与普通高等学校毕业生同等的有关待遇。经过20多年的发展,高等教育自学考试已成为我国高等教育基本制度之一,为国家培养造就了大批专门人才。

高等教育自学考试是标准参照性考试。为科学、合理地制定高等教育自学考试的考试标准,保证教育质量,全国高等教育自学考试指导委员会(以下简称“全国考委”)按照国务院发布的《高等教育自学考试暂行条例》的规定,组织各方面的专家,根据自学考试发展的实际情况,对高等教育自学考试专业设置进行了研究,逐步调整、统一了专业设置标准,并陆续制定了相应的专业考试计划。在此基础上,全国考委各专业委员会按照专业考试计划的要求,从培养和选拔人才的需要出发,组织编写了相应专业的课程自学考试大纲,进一步规定了课程学习和考试的内容与范围,使考试标准更加规范、具体和明确,以利于社会助学和个人自学。

为更好地贯彻十六大和全国考委五届二次会议精神,适应社会经济发展的需要,反映自学考试专业建设和学科内容的发展变化,全国考委电子电工及信息类专业委员会参照普通高等学校相关课程的教学基本要求,结合自学考试计算机及应用专业考试工作的实践,组织修订了《计算机网络原理自学考试大纲》,现经教育部批准,颁发施行。

《计算机网络原理自学考试大纲》是该课程编写及修订教材和自学辅导材料的依据,也是个人自学、社会助学和国家考试的依据,各地教育部门、考试机构应认真贯彻执行。

全国高等教育自学考试指导委员会

2007年2月

一、课程性质与设置目的

(一) 课程性质和特点

“计算机网络原理”是全国高等教育自学考试计算机及应用专业独立本科段的一门专业课程。计算机网络是计算机技术和通信技术相互渗透、密切结合的一门交叉科学，在信息社会中得到了极其广泛的应用。计算机网络化是计算机进入到第四个时代的重要标志，“计算机网络原理”已成为计算机专业及其相关专业的学生必须掌握的一门重要核心课程，它是进行网络设计和开发的基础。

计算机网络涉及数据通信、网络理论、各类网络标准协议及众多相关技术，为便于学生全面了解和掌握计算机网络知识，本课程对计算机网络的基本原理、局域网技术、因特网技术、实用网络技术以及网络安全等内容做了比较系统全面的介绍。

本课程在内容安排上以基础性和实用性为重点，不仅包括了计算机网络的基本原理和技术，还介绍了目前比较成熟的网络实用新技术，对网络发展前沿的内容也有所涉及。通过这些内容的学习，使学生掌握计算机网络的工作原理，理解计算机网络的一系列标准和协议，了解计算机网络的新技术，为开展和从事计算机网络的应用打下扎实的基础。

(二) 本课程的基本要求

通过本课程的学习，要求学生达到如下几点：

1. 系统地学习和掌握计算机网络的主要基础知识，了解计算机网络的产生与发展和未来发展趋势、网络功能、网络分类、网络应用，理解计算机网络的概念、网络的拓扑结构、计算机网络组成等知识。
2. 理解计算机网络协议与分层的体系结构的知识，理解面向连接服务与无连接服务的机制，理解 OSI 参考模型和 TCP/IP 参考模型各层的功能、协议、基本工作原理。了解 OSI 和 TCP/IP 的相同点与不同点。
3. 理解数据通信的有关概念，了解各类传输介质的性能和应用场合，理解和掌握信道最大数据传输速率、数据编码原理、调制解调器、ADSL、多路复用技术、异步传输和同步传输、电路交换与分组交换的工作原理，了解物理层的功能和协议。
4. 理解和掌握数据链路层成帧、差错控制、流量控制等功能，理解链路层的基本协议的功能，掌握典型的数据链路层协议—HDLC 和因特网的数据链路层协议 PPP。
5. 深入理解网络层的功能、为传输层提供的服务、虚电路子网和数据报子网的概念，理解路由选择算法、拥塞的概念和拥塞预防策略，理解 Internet 的 IP、ARP、RARP 和 IPv6

协议,了解 ICMP 和 IGMP 协议、理解 Internet 使用的路由协议,理解网络互连基本原理,掌握互连设备、互连协议,理解网桥和路由器的概念与功能、适用范围和工作原理。

6. 理解传输层提供给高层的服务、服务质量和传输服务原语,理解 Internet 上的传输协议 (TCP, UDP),理解和掌握寻址、建立连接、释放连接、流量控制和缓冲策略。

7. 理解和掌握应用层的域名系统、电子邮件协议、文件传输协议、万维网的原理等。

8. 理解局域网的参考模型与协议标准,掌握几种典型的介质访问控制 (MAC) 即 CS-MA/CD、Token Ring 的工作原理和协议规范,掌握以太网 (包括交换以太网、快速以太网、千兆网以及万兆网) 以及无线局域网的工作原理。了解移动 Ad Hoc 网络的基本概念、特点、结构、路由协议和应用,了解与其它移动通信系统的区别点。了解局域网操作系统的基本概念。

9. 了解分组交换技术 (X.25 和帧中继)、异步传输模式 (ATM)、第三层交换技术、虚拟局域网技术、VPN、计算机网络管理与安全等实用技术的概念和基本原理。

(三) 本课程与相关课程的联系

计算机网络作为一门综合性的交叉科学,它综合运用了多个学科的知识,形成了自身比较完整的体系。学习计算机网络的基本原理课程之前,应很好地掌握计算机组成原理、接口与通信、计算机操作系统、高级语言程序设计等知识。对于计算机及应用专业,本课程的前修课程为模拟电路与数字电路、计算机组成原理,相关课程为操作系统概论。

二、课程内容与考核目标

第1章 计算机网络概述

(一) 学习目的与要求

本章介绍计算机网络的演变发展阶段和未来网络发展趋势, 计算机网络的基本概念、定义、组成和它的功能及应用, 计算机网络的分类, 计算机网络标准的制定。

要求了解计算机网络的几个发展阶段和未来网络发展趋势; 了解三大网络的基本知识, 理解计算机网络的定义和两大组成部分; 了解计算机网络的功能、分类及应用; 理解星形、总线形、环形等网络拓扑结构的特征、性能指标和优、缺点, 并了解树形、混合形和网形等网络拓扑结构的特征; 了解 ISO、ITU 以及 IETF 等标准制定和管理机构。

(二) 课程内容与考核知识点

1. 计算机网络的发展

(1) 计算机网络的四个发展阶段。

(2) 三大网络: 计算机网、电信业务网、广播电视网络。

(3) 网络发展趋势: 宽带网络、全光网络、多媒体网络、移动网络、下一代网络。

2. 计算机网络的基本概念

(1) 计算机网络的定义。

(2) 计算机网络的两大组成部分。

(3) 网络的功能: 硬/软件共享、信息交换。

(4) 计算机网络的典型应用。

3. 计算机网络的分类

(1) 按拓扑类型分类: 总线形、环形、星形、树形、网形、混合形。

(2) 按网络交换方式分类: 电路交换网、报文交换网和分组交换网。

(3) 按网络的覆盖范围分类: 广域网、局域网和城域网。

(4) 按网络传输技术分类: 广播方式、点对点方式。

4. 计算机网络的标准化

- (1) 国际标准化组织。
- (2) 其它标准化机构。
- (3) Internet 的组织机构。

(三) 考核要求

1. 计算机网络的发展

识记：计算机网络的四个发展阶段，计算机网络、电信业务网及广播电视网络三大网络的基本知识，宽带网络、全光网络、多媒体网络、移动网络以及下一代网络的未来发展趋势。

2. 计算机网络的基本概念

- (1) 识记：计算机网络的功能：硬/软件共享、信息交换，计算机网络的典型应用。
- (2) 领会：计算机网络的定义，计算机网络的两大组成部分。

3. 计算机网络的分类

(1) 识记：按拓扑结构分类：总线形、环形、星形、树形、网形、混合形，各种网络拓扑结构的特征；按网络交换方式分类：电路交换网、报文交换网和分组交换网；按网络的覆盖范围分类：广域网、局域网和城域网；按网络传输技术分类：广播方式、点对点方式。

(2) 领会：星形、总线形、环形拓扑结构的特征、性能指标和优、缺点。

4. 计算机网络的标准化

识记：计算机网络的主要标准制定机构：ISO、ITU、IETF。

第2章 计算机网络体系结构

(一) 学习目的与要求

本章介绍计算机网络体系结构的概念、网络的分层体系结构、网络的参考模型、面向连接的服务和无连接的服务，开放系统互连参考模型（OSI/RM）及其各层概述，TCP/IP 网络体系结构及其各层概述。OSI 和 TCP/IP 的相同点与不同点。

要求理解计算机网络分层的目的，理解协议的要素、服务、协议与服务的区别、协议数据单元，理解面向连接的服务和无连接的服务的概念，理解 OSI 基本参考模型与各层的功能，理解 TCP/IP 参考模型与各层的功能，了解两个参考模型的相同点与不同点。

(二) 课程内容与考核知识点

1. 网络的分层体系结构

- (1) 计算机网络体系结构的定义和发展。

(2) 计算机网络分层体系结构及分层原理。
(3) 计算机网络通信协议的概念, 网络通信协议三要素。

2. OSI/RM 开放系统互连参考模型

(1) OSI/RM 对等实体的通信。

(2) OSI/RM 各层的功能。

(3) 面向连接的服务和无连接的服务

3. TCP/IP 参考模型

(1) TCP/IP 的体系结构。

(2) TCP/IP 各层的功能。

4. OSI/RM 与 TCP/IP 参考模型的比较

(1) 两者相似之处: 基于协议栈的概念, 分层体系结构。

(2) 两者不同之处: 层的数目不同; 面向连接的和无连接的通信。

(三) 考核要求

1. 网络的分层体系结构

领会: 网络分层体系结构的概念和计算机网络体系结构, 协议的概念, 网络通信协议三要素: 语义、语法、时序关系。

2. OSI/RM 开放系统互连参考模型

领会: OSI 参考模型及每层的功能。OSI/RM 对等实体的通信。

3. TCP/IP 参考模型

领会: TCP/IP 参考模型及每层的功能; TCP/IP 协议簇内容。

4. OSI/RM 与 TCP/IP 参考模型的比较

(1) 识记: 两者相似之处: 基于协议栈的概念, 分层体系结构; 两者不同之处: 层的数目不同; 面向连接的和无连接的通信。

(2) 领会: 面向连接的和无连接的服务机制。

第3章 物理层

本章主要介绍物理层的功能、物理层接口与协议、传输介质、数据通信技术、数据编码技术和时钟同步、调制解调器、ADSL 和数据交换技术。

本章主要介绍物理层的功能、物理层接口与协议、传输介质、数据通信技术、数据编码技术和时钟同步、调制解调器、ADSL 和数据交换技术。

本章主要介绍物理层的功能、物理层接口与协议、传输介质、数据通信技术、数据编码技术和时钟同步、调制解调器、ADSL 和数据交换技术。

(一) 学习目的与要求

本章主要介绍物理层的功能、物理层接口与协议、传输介质、数据通信技术、数据编码技术和时钟同步、调制解调器、ADSL 和数据交换技术。

本章物理层是计算机网络体系结构中的最底层, 其功能是为数据链路层提供比特流传输服务, 物理层与数据通信系统有着直接的联系, 主要介绍物理层接口与协议、传输介质、数据通信技术、数据编码技术和时钟同步、调制解调器、ADSL 和数据交换技术。

要求了解物理层提供的为建立、维持和拆除物理链路所需的机械的、电气的、功能的和规程的特性; 理解 EIA RS-232C 和 EIA RS-449 接口标准; 了解计算机网络中所采用的双

绞线、同轴电缆、光导纤维、无线通信等传输介质的传输特性,理解数据传输速率、误码率、信道容量等主要指标的定义并掌握它们的计算方法;理解各种通信方式、编码方法、时钟同步方法、多路复用技术、异步传输和同步传输方法的工作原理和特点;理解调制解调器和 ADSL 的工作原理及性能,理解电路交换、报文交换和分组交换技术的概念、工作原理和各自的特点。

(二) 课程内容与考核知识点

1. 物理层接口与协议

- (1) 物理层的定义和功能, DTE、DCE 的定义。
- (2) 常用的 25 芯、9 芯连接器标准。
- (3) 非平衡方式、采用差动接收器的非平衡方式及平衡方式三种电气连接方式。
- (4) 数据、控制、定时及接地四类接口信号线。
- (5) 规程特性。
- (6) EIA RS-232C 接口标准。
- (7) EIA RS-449 及 RS-422 与 RS-423 接口标准。
- (8) 100 系列和 200 系列接口标准, X.21、X.21 bis 建议。

2. 传输介质

- (1) 双绞线。
- (2) 同轴电缆:基带同轴电缆和宽带同轴电缆。
- (3) 光纤:多模光纤和单模光纤。
- (4) 无线传输介质:无线电波、微波、红外线和激光,卫星通信。
- (5) 传输介质的选择。

3. 数据通信技术

- (1) 数据和信号的定义,模拟数据或数字数据用模拟信号或数字信号表示的概念,MODEM 和 CODEC 作用,放大器和中继器的作用,数据通信的定义。
- (2) 数据传输速率及其单位 bps、信号调制速率及其单位波特的定义,数据传输速率与信号调制速率的关系。
- (3) 误码率的定义。
- (4) 计算信道容量的两个经典公式:奈奎斯特公式和香农公式,带宽、信号状态数和信噪比的含义。
- (5) 并行和串行通信方式,串行通信的单工、半双工和全双工方式。
- (6) 频分多路复用技术、时分多路复用技术和波分多路复用技术的实现条件及工作原理, T1 载波和 E1 载波的帧结构。
- (7) 同步传输和异步传输的工作原理和特征。

4. 数据编码

- (1) 数字数据的模拟信号编码,调幅、调频和调相三种基本调制方式及各种正交振幅调制(QAM)的工作原理。
- (2) 数字数据的数字信号编码,归零码和不归零码、单极性码和双极性码的特点,位

同步法的工作原理,曼彻斯特码的编码原理,群同步(起一止式同步法)的工作原理。

(3) 模拟数据的数字信号编码,采样定律及采样、量化、编码三过程。

(4) ADSL 的工作原理和特点。

5. 数据交换技术

(1) 电路交换技术的工作原理和特点。

(2) 报文交换技术的工作原理和特点。

(3) 分组交换技术(虚电路分组交换和数据报分组交换)的工作原理和特点。

(4) 各种数据交换技术的性能比较。

(5) 高速交换技术的工作原理和特点。

(三) 考核要求

1. 物理层接口与协议

(1) 识记:物理层的定义和功能,DTE、DCE 的定义,常用的 25 芯、9 芯连接器标准,数据、控制、定时及接地四类接口信号线,规程特性,100 系列和 200 系列接口标准,X.21、X.21 bis 建议。

(2) 领会:非平衡方式、采用差动接收器的非平衡方式及平衡方式三种电气连接方式,EIA RS-232C 接口标准,EIA RS-449 及 RS-422 与 RS-423 接口标准。

2. 传输介质

(1) 识记:多模光纤和单模光纤,无线传输介质:无线电波、微波、红外线和激光,卫星通信。

(2) 领会:有线传输介质:双绞线、同轴电缆和光纤,基带同轴电缆和宽带同轴电缆。

3. 数据通信技术

(1) 识记:数据和信号的定义,放大器和中继器的作用,数据通信的定义,误码率的定义。

(2) 领会:模拟数据或数字数据用模拟信号或数字信号表示的概念,MODEM 和 CODEC 作用,带宽、信号状态数和信噪比的含义,并行和串行通信方式,串行通信的单工、半双工和全双工方式。频分多路复用技术、时分多路复用技术和波分多路复用技术的实现条件及工作原理,同步传输和异步传输的工作原理和特征。

(3) 简单应用:数据传输速率及其单位 bps、信号调制速率及其单位波特的定义,数据传输速率与信号调制速率的关系。

(4) 综合应用:计算信道容量的两个经典公式:奈奎斯特公式和香农公式。

4. 数据编码

(1) 识记:调幅、调频和调相的工作原理,归零码和不归零码、单极性码和双极性码。

(2) 领会:数字数据的模拟信号编码,各种正交振幅调制(QAM)的工作原理和性能,ADSL 工作原理、性能和特点,数字数据的数字信号编码,位同步法的工作原理,群同步(起一止式同步法)的工作原理,模拟数据的数字信号编码。

(3) 简单应用:曼彻斯特码的编码原理,采样定律及采样、量化、编码三过程及量化级与编码位数的关系,T1 载波和 E1 载波的帧结构。

5. 数据交换技术

(1) 识记：高速交换技术的工作原理和特点。

(2) 领会：电路交换技术的工作原理和特点，报文交换技术的工作原理和特点，分组交换技术（虚电路分组交换和数据报分组交换）的工作原理和特点，各种数据交换技术的性能比较。

第4章 数据链路层

(一) 学习目的与要求

本章介绍数据链路层功能与协议，其功能是将物理层提供的传输原始比特流连接造成逻辑上无差错的数据传输链路，以向网络层提供透明、可靠的数据传输服务。介绍差错控制方法和编码，介绍因特网数据链路层的协议。

要求理解数据链路层的基本概念，理解数据链路层的帧同步、差错控制、流量控制的功能，理解流量控制的概念和基本协议，理解数据传输过程中差错产生的原因与性质，理解线路、链路、数据链路的概念，理解误码率的定义与差错控制方法。理解基本数据链路协议。了解面向字符型数据链路层协议实例——BSC，掌握面向比特型数据链路层协议实例——HDLC，理解 Internet 中的数据链路层协议。

(二) 课程内容与考核知识点

1. 数据链路层的功能

(1) 帧同步功能：字符填充法、比特填充法、违法编码法和字节计数法。

(2) 差错控制功能：反馈重发、超时计时器以及帧编号的原理。

(3) 流量控制功能：停止等待方案、滑动窗口机制。

(4) 链路管理功能。

2. 差错控制

(1) 随机热噪声引起的随机错和冲击噪声引起的突发错。

(2) 奇偶校验码（包括水平垂直奇偶校验码）的算法、检错能力和编码效率。

(3) 循环冗余码的算法、检错能力和编码效率，生成多项式、模 2 除的概念和应用，冗余位的求算。

3. 基本数据链路协议

(1) 停等协议。

(2) 顺序接收管道协议。

(3) 选择重传协议。

4. 链路控制规程

- (1) 面向字符的同步控制协议 BSC: 10 个传输控制字符、两类报文格式。
- (2) 面向比特的同步控制协议 HDLC: 帧格式、三种帧类型。

5. 因特网的数据链路层协议

- (1) SLIP 协议。
- (2) PPP 协议。

(三) 考核要求

1. 数据链路层的功能

- (1) 识记: 数据链路层的功能: 帧同步功能、差错控制、流量控制、链路管理功能。
- (2) 领会: 帧同步功能: 字符填充法、比特填充法、违法编码法和字节计数法; 差错控制: 反馈重发、超时计时器以及帧编号的原理; 流量控制: 停止等待方案、滑动窗口机制。

2. 差错控制

- (1) 识记: 随机热噪声引起的随机错和冲击噪声引起的突发错。
- (2) 简单应用: 奇偶校验码(包括水平垂直奇偶校验码)的算法、检错能力和编码效率, 循环冗余码的算法、检错能力和编码效率, 生成多项式、模 2 除的概念和应用, 冗余位的求算。

3. 基本数据链路协议

简单应用: 停等协议, 顺序接收管道协议, 选择重传协议。

4. 链路控制规程

- (1) 简单应用: 面向字符的同步控制协议 BSC: 10 个传输控制字符、两类报文格式。
- (2) 简单应用: 面向比特的同步控制协议 HDLC: 帧格式、三种帧类型。

5. 因特网的数据链路层协议

- (1) 识记: SLIP 协议。
- (2) 领会: PPP 协议。

第 5 章 网络层

(一) 学习目的与要求

本章介绍网络层的内容, 网络层涉及的是将源端发出的分组经各种途径传送到目的端, 在数据链路层提供的两个相邻节点之间的数据帧的传送功能上, 进一步管理网络中的数据通信, 将数据从源端经过若干中间节点传送到目的端。网络层是 OSI 模型中面向数据通信的底层中最为复杂、关键的一层。

网络层实现的主要功能包括路由选择、拥塞控制和网络互连等，本章着重介绍网络层的原理、功能及实现。要求了解网络层的功能，理解网络层两种操作方式的特点，理解路由选择算法和拥塞控制方法，了解服务质量，理解网络互连设备和互连协议，理解网桥、交换机和路由器的工作原理与功能，适用范围，理解因特网互连层的协议标准。

(二) 课程内容与考核知识点

1. 通信子网的操作方式和网络层提供的服务

- (1) 网络层的功能。
- (2) 通信子网的两种操作方式：虚电路和数据报，两种操作所提供的两种服务。
- (3) 虚电路子网和数据报子网的比较。

2. 路由选择

- (1) 最优化原则的定义。
- (2) 静态路由选择策略：最短路由选择算法，泛射路由选择算法。
- (3) 动态路由选择策略：距离矢量路由算法和 RIP 路由信息协议，链路状态路由算法和 OSPF 开放的最短路径优先协议。
- (4) 移动主机的路由选择。
- (5) 广播路由选择。
- (6) 多播路由选择。

3. 拥塞控制

- (1) 拥塞现象发生的原因，流量控制和拥塞控制的差异。拥塞控制的必要性。
- (2) 拥塞控制的基本原理。
- (3) 拥塞控制方法：虚电路子网中的拥塞控制，数据报子网中的拥塞控制，负载丢弃，抖动控制。

4. 服务质量

- (1) 集成服务和区分服务。
- (2) 标签交换和 MPLS 的概念。

5. 网络互连

- (1) 网络互连的基本原理，网桥技术。
- (2) RIP 和 OSPF。
- (3) 网桥、路由器和网关等网络互连设备。

6. 因特网的互连层协议

- (1) IP 协议。
- (2) ARP 协议与 RARP 协议。

(3) ICMP 协议。

(4) IGMP 协议。

(5) IPv6。

(三) 考核要求

1. 通信子网的操作方式和网络层提供的服务

(1) 领会：网络层的功能。

(2) 领会：通信子网的两种操作方式：虚电路和数据报，两种操作所提供的两种服务，两种子网的比较。

2. 路由选择

(1) 识记：最优化原则的定义。

(2) 领会：静态路由选择策略：泛射路由选择算法。动态路由选择策略：链路状态路由算法。移动主机的路由选择。广播路由选择。多播路由选择。

(3) 简单应用：最短路由选择算法，距离矢量路由算法。

3. 拥塞控制

(1) 识记：拥塞现象的原因，流量控制和拥塞控制的差异。拥塞控制的必要性。

(2) 领会：拥塞控制的基本原理，拥塞控制方法。

4. 服务质量

识记：集成服务和区分服务，标签交换和 MPLS 的概念。

5. 网络互连

(1) 识记：网络互连的基本原理，网桥技术。

(2) 领会：RIP 和 OSPF，网桥、路由器和网关等网际互连所使用的中继设备及其对应的 OSI 层次，网桥、交换机、路由器的基本工作原理。

(3) 综合应用：网络互连的概念，网络互连模型，网络互连设备。

6. 因特网的互连层协议

(1) 识记：ICMP 协议，IGMP 协议。

(2) 领会：IP 协议，ARP 协议与 RARP 协议，IPv6。

第 6 章 传输层

(一) 学习目的与要求

本章介绍传输层的内容，传输层是整个协议层次结构的核心，其任务是为从源端到目的端提供可靠的、合理的数据传输，而与使用的网络无关。

要求了解传输层的功能，理解传输层和数据链路层的区别，了解传输协议，理解 UDP、TCP 两个协议的作用和特点。

(二) 课程内容与考核知识点

1. 传输层的功能

(1) 传输层的功能和作用。

(2) 两种传输服务。

2. 传输协议

(1) 传输连接建立的方法。

(2) 传输层的服务。

3. 传输控制协议

(1) 报文格式, TCP 的段结构, 常用 TCP 协议所使用的端口号。

(2) TCP 连接管理。

(3) TCP 滑动窗口控制。

(4) TCP 重传策略。

(5) TCP 拥塞控制。

4. 用户数据报协议

(1) 报文格式, UDP 的段结构, 常用 UDP 协议所使用的端口号。

(2) UDP 协议的应用。

(三) 考核要求

1. 传输层的功能

识记: 传输层的功能和作用。

2. 传输协议

(1) 识记: 传输连接建立的方法。

(2) 领会: 传输协议的要素。传输层的服务

(3) 简单应用: 寻址和端口, 建立和释放连接。

3. 传输控制协议

(1) 识记: TCP 的滑动窗口控制、重传策略和拥塞控制。

(2) 领会: 协议的内容和功能, 报文格式。连接管理机制。

4. 用户数据报协议

领会: 协议的内容和功能, 报文格式。

第7章 应用层

(一) 学习目的与要求

本章介绍应用层的内容,应用层包含用户程序,实现计算机实际的工作。应用层具有文件传输、文件管理、文件访问、电子邮件等功能,其最终目标是为用户提供相应的服务。本章对应用层的协议、功能及服务进行介绍。

要求了解组成 OSI 参考模型高层结构的应用层的主要功能、特点和协议规范,理解域名系统、电子邮件协议和 WWW 的工作原理,了解应用层提供的其它服务。

(二) 课程内容与考核知识点

1. 应用层的概念

应用层的地位和作用。

2. 域名系统

(1) IP 地址与域名。

(2) 域名解析原理。

3. 电子邮件

(1) 电子邮件的格式。

(2) 电子邮件的协议:SMTP、POP3、IMAP。

4. 万维网

(1) WWW 的工作原理。

(2) 超文本传输协议 HTTP。

(3) 同一资源定位器 URL。

5. 其它服务

(1) 文件传输协议 FTP。

(2) 远程登录 Telnet。

(3) 电子公告板系统 BBS。

(三) 考核要求

1. 应用层的概念

识记:应用层的地位和作用。

2. 域名系统

(1) 识记:域名系统。

(2) 领会: IP 地址与域名, 域名解析原理。

3. 电子邮件

(1) 识记: 电子邮件的格式。

(2) 领会: 电子邮件的协议: SMTP、POP3、IMAP 的特点。

4. 万维网

(1) 识记: HTML, 浏览器, 超文本传输协议 HTTP 和统一资源定位器 URL。

(2) 领会: WWW 的工作原理。

5. 其它服务

(1) 识记: 远程登录 Telnet, 电子公告板系统 BBS。

(2) 领会: 文件传输协议 FTP。

第8章 局域网技术

(一) 学习目的与要求

本章介绍局域网技术, 局域网是在一个较小的区域范围内将各种通信设备和计算机互连起来以实现资源共享和信息交换的计算机网络, 局域网技术飞速发展并在计算机网络技术中占有越来越重要的地位。

要求理解介质访问控制技术、局域网的概念, 理解局域网的主要技术特点, 理解 IEEE 802 参考模型与协议的基本概念, 理解逻辑链路控制 (LLC) 协议层的服务和操作, 理解 Ethernet 局域网的基本工作原理, 深刻理解 CSMA/CD 总线网、Token Ring 令牌环的主要组成部分和操作系统, 了解 FDDI 的基本工作原理, 理解以太网包括交换以太网、快速以太网、千兆网以及万兆网的体系结构、特点及其实现技术, 了解高速局域网、无线局域网与移动 Ad Hoc 网络的基本工作原理, 了解无线局域网的特点、硬件设备组成、连接方案以及相应标准。了解局域网操作系统的特点、分类及其基本功能。

(二) 课程内容与考核知识点

1. 介质访问控制子层

(1) 信道访问权的分配: 静态分配, 动态分配。

(2) 局域网的介质访问控制协议: 争用协议, 无冲突协议, 有限争用协议。

(3) 纯 ALOHA 系统、时分 ALOHA 系统。

(4) 载波监听多路访问 CSMA 及非坚持、1-坚持、P-坚持退避算法, 载波监听多路访问/冲突检测 CSMA/CD, 二进制倒数计数协议。

(5) 介质访问控制 (CSMA/CD), 传播延时和传输延时的关系, 冲突检测时间和最短帧长的计算。

2. IEEE 802 标准与局域网

(1) 局域网的参考模型。

(2) IEEE 802 标准。

(3) IEEE 802.2: 逻辑链路控制子层。

(4) IEEE 802.3: IEEE 802.3 协议、帧格式、MAC 功能以及物理层规范。

(5) IEEE 802.4: 令牌总线。

(6) IEEE 802.5: 令牌环; 令牌环工作原理、环结构以及操作过程, 以比特度量的环长的计算, 令牌环的特点, 令牌环 MAC 帧格式。

(7) IEEE 802.3、IEEE 802.4 和 IEEE 802.5 的比较。

(8) IEEE 802.6: 分布队列双总线。

3. 高速局域网

(1) FDDI 环网, FDDI 工作原理、性能、编码、时钟偏移、帧格式, FDDI 组成。

(2) 以太网标准、帧格式、物理层规范, 快速以太网的介质访问控制方法、物理层规范, 交换型以太网技术特点, 千兆位以太网的介质访问控制方法、物理层规范, 万兆位以太网特性。

4. 无线局域网技术

(1) 无线局域网的特点、技术要求。

(2) 无线局域网的硬件设备。

(3) 无线局域网的连接方案。

(4) 无线局域网标准: IEEE 802.11 协议, 蓝牙技术, IrDA 和 HomeRF 技术, IEEE 802.16 协议。

(5) 无线应用协议 WAP。

5. 移动 Ad Hoc 网络

(1) 移动 Ad Hoc 网络的特点和应用。

(2) 移动 Ad Hoc 网络的结构和路由协议。

(3) 移动 Ad Hoc 网络与其它移动通信系统的比较。

6. 局域网操作系统

(1) 局域网操作系统的演变过程。

(2) 局域网操作系统的基本功能。

(3) 典型局域网操作系统简介。

(三) 考核要求

1. 介质访问控制子层

(1) 识记: 信道访问权的分配: 静态分配, 动态分配。

(2) 领会: 局域网的介质访问控制协议: 争用协议, 无冲突协议, 有限争用协议。

(3) 领会: 介质访问控制 (CSMA/CD), 载波监听多路访问 CSMA 及非坚持、1-坚持、P-坚持退避算法, 载波监听多路访问/冲突检测 CSMA/CD 及二进制倒数计数协议, 传播延时和传输延时的关系。

(4) 简单应用: CSMA 及非坚持、1-坚持、P-坚持退避算法; 冲突检测时间和最短帧

长的计算。

2. IEEE 802 标准与局域网

- (1) 识记: IEEE 802 标准系列。
- (2) 领会: 局域网的参考模型。
- (3) 领会: IEEE 802.2 逻辑链路控制子层。
- (4) 领会: IEEE 802.3: 协议、帧格式、MAC 功能以及物理层规范。
- (5) 识记: IEEE 802.4 令牌总线。
- (6) 识记: IEEE 802.5: 令牌环, 令牌环工作原理、环结构以及操作过程, 以比特度量的环长的计算, 令牌环的特点。
- (7) 领会: 以比特度量的环长的计算。
- (8) 领会: IEEE 802.3、IEEE 802.4 和 IEEE 802.5 的比较, IEEE 802.6: 分布队列双总线。
- (9) 综合应用: CSMA/CD, 以太网, 快速、高速局域网, 网桥与局域网互连, 交换机和交换式局域网。

3. 高速局域网

- (1) 识记: 光纤分布数据接口 FDDI 性能、编码、时钟偏移。
- (2) 识记: FDDI 工作原理、帧格式, FDDI 组成。
- (3) 识记: 以太网、100Mbps、1Gbps、10Gbps 以太网的体系结构。
- (4) 领会: 以太网、100Mbps、1Gbps、10Gbps 以太网的物理层规范, MAC 方法。

4. 无线局域网技术

- (1) 识记: 无线局域网的特点、技术要求、硬件组成。
- (2) 领会: 无线局域网的连接方案以及标准, 无线应用协议 WAP。
- (3) 领会: 无线局域网标准 IEEE 802.11 协议系列, 蓝牙技术, IrDA 和 HomeRF 技术, IEEE 802.16 协议。

5. 移动 Ad Hoc 网络

- (1) 识记: 移动 Ad Hoc 网络的特点和应用。
- (2) 识记: 移动 Ad Hoc 网络的结构和路由协议。
- (3) 识记: 移动 Ad Hoc 网络与其它移动通信系统的比较。

6. 局域网操作系统

识记: 局域网操作系统的演变过程, 局域网操作系统的基本功能, 典型局域网操作系统简介。

第9章 实用网络技术

(一) 学习目的与要求

前面的章节介绍了计算机网络的基本原理和局域网技术, 本章介绍一些广泛关注和应用

的实用网络技术,包括分组交换技术、异步传输模式、第三层交换技术、虚拟局域网技术、虚拟专用网和计算机网络安全等内容。

要求理解分组交换技术,理解 X.25 协议标准,理解帧中继(Frame Relay)网的工作原理以及主要特点,理解异步传输模式(ATM)的工作原理以及主要特点,理解第三层交换技术的概念和原理,了解虚拟局域网技术,了解虚拟专用网、网络管理基础与网络安全知识。

(二) 课程内容与考核知识点

1. 分组交换技术

- (1) X.25 协议:协议层次、分组格式、分组类型。
- (2) 帧中继(Frame Relay)的基本原理、帧格式、应用和发展。

2. 异步传输模式(ATM)

- (1) ATM 交换、定义及功能。
- (2) ATM 的特征及信元交换技术。
- (3) ATM 的层次结构、ATM 子层和 ATM 适配层。
- (4) ATM 的工作方式:异步时分复用。

3. 第三层交换技术

- (1) 第三层交换技术的引入。
- (2) 局域网第三层交换技术。
- (3) 广域网第三层交换技术。

4. 虚拟局域网技术

- (1) 虚拟局域网的概念。
- (2) 建立虚拟局域网的交换技术:端口交换、帧交换、信元交换。
- (3) 划分虚拟局域网的方法。

5. 虚拟专用网 VPN

- (1) VPN 的概念。
- (2) VPN 的特点。
- (3) VPN 的安全技术。
- (4) VPN 的应用。

6. 计算机网络安全

- (1) 网络管理五大基本功能及主要协议。
- (2) 网络安全概念,网络攻击的几种形式,网络安全机制,加密解密,数字签名。

(三) 考核要求

1. 分组交换技术

- (1) 识记:帧中继工作原理及应用。X.25 协议:协议层次、分组格式、分组类型。
- (2) 领会:帧中继帧格式。

2. 异步传输模式

识记：定义、工作方法、功能。ATM 特征，基于 Cell 的分组交换技术，信元格式、适配层功能。

3. 第三层交换技术

(1) 识记：第三层交换技术的引入。

(2) 领会：局域网第三层交换技术，广域网第三层交换技术。

4. 虚拟局域网技术

(1) 识记：虚拟局域网的概念。

(2) 领会：建立虚拟局域网的交换技术：端口交换、帧交换、信元交换，划分虚拟局域网的方法。

5. 虚拟专用网 VPN

识记：VPN 的特点，VPN 安全技术。

6. 计算机网络安全

(1) 识记：网络管理的五大基本功能及主要协议，网络安全的概念。

(2) 领会：常规加密解密方法，认证和数字签名。

三、关于大纲的说明与考核实施要求

(一) 关于“课程内容与考核目标”中有关提法的说明

在大纲的考核要求中,提出了“识记”、“领会”、“简单应用”和“综合应用”等四个能力层次,它们之间是递进等级关系,后者必须建立在前者的基础上,它们的含义是:

识记:要求考生能够识别和记忆本课程中规定的有关知识点的主要内容(如定义、定理、定律、表达式、公式、原则、重要结论、方法、步骤及特征、特点等),并能根据考核的不同要求,做出正确的表述、选择和判断。

领会:要求考生能够领悟和理解本课程中规定的有关知识点的内涵与外延,熟悉其内容要点和它们之间的区别与联系,并能根据考核的不同要求,做出正确的解释、说明和论述。

简单应用:要求考生能够运用本课程中规定的少量知识点,分析和解决一般应用问题,如简单的计算、绘图和分析、论证等。

综合应用:要求考生能够运用本课程中规定的多个知识点,分析和解决较复杂的应用问题,如计算、绘图、简单设计、编程和分析、论证等。

(二) 关于自学教材

《计算机网络原理》,全国高等教育自学考试指导委员会组编,杨明福主编,经济科学出版社2007年版。

(三) 自学方法的指导

本课程作为一门专业课程,内容多、难度大,自学者在自学过程中应注意以下几点:

1. 在学习前,应仔细阅读课程大纲的第一部分,了解课程的性质、地位和任务,熟知课程的基本要求以及本课程与有关课程的联系,使以后的学习能紧紧围绕课程的基本要求。

2. 在阅读某一章教材内容前,应先查阅考试大纲中关于该章的考核知识点、自学要求和考核要求,注意对各知识点的能力层次要求,以便在阅读教材时做到心中有数,有的放矢。

3. 阅读教材时,要逐段细读,逐句推敲,集中精力,吃透每个知识点,对基本概念必须深刻理解,对基本理论必须彻底弄清,对基本方法和基本技术必须牢固掌握,在阅读中遇有个别细节问题不清楚,在不影响学习新内容的情况下,可暂时搁置。

4. 在学完教材的每一节内容后,应认真做好教材中的有关习题和思考题,这是帮助考

生理解、消化和巩固所学知识、培养分析问题、解决问题能力的重要环节，必须引起极大的注意。

本课程共4学分。

(四) 对社会助学的要求

1. 应熟知考试大纲对课程所提出的总的要求和各章的知识点。
2. 应掌握各知识点要求达到的层次，并深刻理解对各知识点的考核要求。
3. 辅导时应以指定的教材为基础、考试大纲为依据，不要随意增删内容，以免与考试大纲脱节。
4. 辅导时应对学生进行学习方法的指导，提倡学生“认真阅读教材，刻苦钻研教材，主动提出问题，依靠自己学通”的学习方法。
5. 辅导时要注意基础、突出重点，要帮助考生对课程内容建立一个整体的概念，对考生提出的问题，应以启发引导为主。
6. 注意对考生能力的培养，特别是自学能力的培养，要引导考生逐步学会独立学习，在自学过程中善于提出问题、分析问题、做出判断和解决问题。同时要注意培养考生实验操作的能力。
7. 要使考生了解试题难易与能力层次高低两者不完全是一回事，在各个能力层次中都存在着不同难度的试题。

(五) 关于命题和考试的若干规定

1. 本大纲各章所提到的考核要求中，各条细目都是考试的内容，试题覆盖到章，适当突出重点章节，加大重点内容的覆盖密度。
2. 试卷中对不同能力层次要求的试题所占的比例大致是：“识记”为15%；“领会”为35%；“简单应用”为30%；“综合应用”为20%。
3. 试题难易程度要合理，可分为四档：易、较易、较难和难，这四档在各份试卷中所占的比例约为2:3:3:2。
4. 试题主要题型有：填空题、选择题、简答题、计算题及应用题等五种类型（见附录）。
5. 本课程考试方式为闭卷、笔试，考试时间为150分钟。试题分量应以中等水平的考生在规定时间内答完全部试题为度。评分采用百分制，60分为及格。

附录：题型举例

一、单项选择题（在每小题列出的四个备选答案中只有一个正确的答案，将其字母号码填在题后的括号内）

1. 帧头和帧尾都使用 01111110 标志，数据块作为位流来处理，这种传输方案称为（ ）。

- A. 面向位的同步传输 B. 异步传输
C. 面向字符的同步传输 D. 起止式传输

2. TCP 通信建立在面向连接的基础上，TCP 连接的建立采用（ ）次握手的过程。

- A. 1 B. 2
C. 4 D. 3

二、填空题

1. 同步数据链路控制协议主要分为面向字符的同步控制协议、面向_____的同步控制协议和面向_____的同步控制协议。

2. Ethernet 网采用_____的 CSMA 算法进行载波监听，采用_____算法来决定冲突后的避让时间。

三、简答题

1. 试比较 SLIP 与 PPP 协议的主要区别。
2. 简述分组交换技术的主要优点。

四、计算题

1. 长度 1km 的基带以太网，速率达 1Gbps，为保证冲突的可靠检测，需保证最起码的帧长度为多少位？（设传播时延为 $5\mu\text{s}/\text{km}$ ）
2. 一个 16M bps 的令牌环，其令牌保持计数器的设置值为 $10\mu\text{s}$ ，在此环上可发送的最长帧为多少位？

五、应用题

1. E1 载波的效率是多少？开销是多少？
2. 试用图来说明，为什么在基带总线的情况下，数据帧的传输时延至少要两倍于传播时延？

更多优质自考资料尽在百度贴吧自考乐园俱乐部
(<http://tieba.baidu.com/club/5346389>)
欢迎加入...欢迎交流...止不住的惊喜等着你.....

☆自考乐园---心境随缘, 诚与天下自考人共勉!!!
☆自考乐园---分享快乐, 你的快乐老家!!!
☆自考乐园---引领成功, 你的精神乐园!!!

后 记

自考乐园俱乐部, 专注于自考, 致力于成为全国最全,
最优的自考学习交流, 资料共享平台.....

本大纲是根据全国高等教育自学考试指导委员会电子电工与信息类专业委员会制定的“高等教育自学考试计算机及应用专业(独立本科段)”考试计划和全国高等教育自学考试指导委员会《关于修订高等教育自学考试课程自学考试大纲的几点意见》的精神制定的。

在大纲提出初稿后, 曾聘请专家通审, 并由电子电工与信息类专业委员会在上海组织召开审稿会进行审稿, 根据审稿会意见作了修改。最后由电子电工与信息类专业委员会定稿。

本大纲由杨明福教授(华东理工大学)负责编写和修改。参加审稿并提出修改意见的有马跃教授(北京邮电大学, 主审)、章坚武教授(杭州电子科技大学, 参审)、高传善教授(复旦大学, 参审)。

对参加本大纲编写和审稿的教授表示感谢。

全国高等教育自学考试指导委员会

电子电工与信息类专业委员会

2006年11月

俱乐部名称: 自考乐园

俱乐部id: 5346389 (请牢记它哦~在百度贴吧的搜索框中输入俱乐部id,
可以直接进入俱乐部)

俱乐部url地址: <http://tieba.baidu.com/club/5346389>

(您也可以通过此url进入俱乐部。)

俱乐部简介①自考乐园俱乐部, 专注于自考, 致力于成为全国最全,
最优的自考学习交流, 资料共享平台.....

②本人自考计算机网络独立本科已过8科, 真诚欢迎报考此科目的朋友进来一起交流,
进步, 提高.....欢迎加入自考乐园俱乐部, 如有需要自考资料, 请留言,
我们会尽力帮助大家的...祝大家自考快乐.....

③自考乐园诚与天下自考人共勉!!!

欢迎加入自考乐园俱乐部.....

更多优质自考资料尽在百度贴吧自考乐园俱乐部
(<http://tieba.baidu.com/club/5346389>)
欢迎加入...欢迎交流...止不住的惊喜等着你.....

☆☆☆与千万自考生同行，你准备好了吗？

你希望在自考的征途中，有一群和你志同道合的人同行吗？

你愿意在漫长的自考岁月中，有一群人和你分享快乐，分担忧愁吗？

你渴望在一个人奋斗时，有一群人在背后默默支持你吗？

你是否也一直在苦苦寻找这样一个平台，一群志同道合的人，一片积极向上的心，
一个共同的追求，一个诚挚的鼓励，一个坚实的支持.....
对！！！！就是这里！！！！这里有你想要的一切.....

与志者同行，你也将成为志者！！！！

与成功者同行，你也将获得成功！！！！

与千万自考生同行，你准备好了吗？？？

与千万自考生同行，你做好了准备吗？？？

今天我们诚挚的发出邀请，真诚的欢迎广大自考的朋友（尤其是和我报考相同专业的朋友）
加入本俱乐部，一起交流，进步，提高.....我们正寻找特别的你亲情加入.....

最后预祝所有的朋友：

自考快乐

天天有份好心情！！！！-----杨尚杰于2010.4.19

封面设计/寻木

ISBN 978-7-5058-6360-6



9 787505 863606

定价：26.00元