第1章 引 言

过去的三百年中，每一个世纪都有一种技术占据主要的地位。18世纪伴随着工业革命而来的是伟大的机械时代；19世纪是蒸汽机时代；20世纪的关键技术是信息的获取、存储、传送、处理和利用。计算机是20世纪人类最伟大的发明之一，它的产生标志着人类开始迈向一个崭新的信息社会。从工业革命到信息革命，一个根本的变革就是从劳动密集型社会转入到知识密集型社会。在20世纪的最后10年中，人们惊喜地发现：电话、电视及计算机正在迅速地融合；信息的获取、存储、传送和处理之间的孤岛现象随着计算机网络的发展而逐渐消失；曾经独立发展的电信网、电视网和计算机网将合而为一；新的信息产业正以强劲的势头迅速崛起。因此，在未来社会中，信息产业将成为社会经济中发展最快和最大的部门。为了提高信息社会的生产力，提供一种全社会的、经济的、快速的存取信息的手段是十分必要的，这种手段是由计算机网络来实现的。

1.1 计算机网络的产生和发展

世界上第一台电子计算机的诞生在当时是很大的创举，但是任何人都没有预测到五十年后的今天，计算机在社会各个领域的应用和影响是如此广泛和深远。当1969年12月世界上第一个数据包交换计算机网络ARPANET出现时，也不会有人预测到时隔二十多年，计算机网络在现代信息社会中扮演了如此重要的角色。ARPANET网络已从最初的四个结点发展为横跨全世界一百多个国家和地区、挂接有几万个网络、几百万台计算机、几亿用户的因特网（Internet）。Internet是当前世界上最大的国际性计算机互联网络，而且还在发展之中。

回顾计算机网络的发展历史，对预测这个行业的未来，会得到一些有益的启示。在电气时代到来之前，还不具备发展远程通信的先决条件，所以通信事业的发展十分缓慢。从19世纪40年代到20世纪30年代，电磁技术被广泛用于通信。1844年电报的发明以及1876年电话的出现，开始了近代电信事业，为人们迅速传递信息提供了方便。从20世纪30年代到60年代，电子技术被广泛用于通信领域。微波传输、大西洋电话电缆以及1960年美国海军首次使用命名为“月亮”的卫星进行远距离通信，标志着远程通信事业的开始。

纵观计算机网络的发展历史可以发现，它和其他事物的发展一样，也经历了从简单到复杂，从低级到高级的过程。在这一过程中，计算机技术与通信技术紧密结合，相互促进，共同发展，最终产生了计算机网络。

在1946年，世界上第一台数字计算机问世，但当时计算机的数量非常少，且非常昂贵。由于当时的计算机大都采用批处理方式，用户使用计算机首先要将程序和数据制成纸带或卡片，再送到计算中心进行处理。1954年，出现了一种被称作收发器（transceiver）的终端，人们使用这种终端首次实现了将穿孔卡片上的数据通过电话线路发送到远地的计算机。此后，电传打字机也作为远程终端和计算机相连，用户可以在远地的电传打字机上输入自己的程序，而计算机计算出来

的结果也可以传送到远地的电传打字机上并打印出来，计算机网络的基本原型就这样诞生了。

由于当初的计算机是为批处理而设计的，因此当计算机和远程终端相连时，必须在计算机上增加一个接口。显然，这个接口应当对计算机原来软件和硬件的影响尽可能小。这样就出现了如图1-1所示的线路控制器（line controller）。图中的调制解调器M是必须的，因为电话线路本来是为传送模拟话音而设计的。

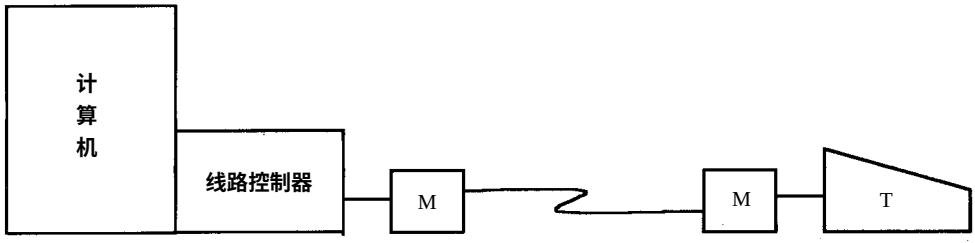


图1-1 计算机通过线路控制器与远程终端相连

随着远程终端数量的增加，为了避免一台计算机使用多个线路控制器，在 60年代初期，出现了多重线路控制器（multiple Line controlLev）。它可以和多个远程终端相连接，构成面向终端的计算机通信网，如图 1-2所示。有人将这种最简单的通信网称为第一代计算机网络。这里，计算机是网络的控制中心，终端围绕着中心分布在各处，而计算机的主要任务是进行批处理。同时考虑到为一个用户架设直达的通信线路是一种极大的浪费，因此在用户终端和计算机之间通过公用电话网进行通信。

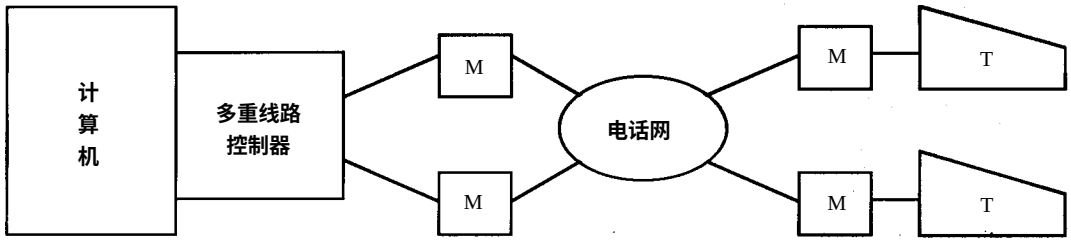


图1-2 第一代计算机网络：以主机为中心

在第一代计算机网络中，人们利用通信线路、集中器、多路复用器以及公用电话网等设备，将一台计算机与多台用户终端相连接，用户通过终端命令以交互的方式使用计算机系统，从而将单一计算机系统的各种资源分散到了每个用户手中。面向终端的计算机网络系统（分时系统）的成功，极大地刺激了用户使用计算机的热情，使计算机用户的数量迅速增加。但这种网络系统也存在着一些缺点：如果计算机的负荷较重，会导致系统响应时间过长；而且单机系统的可靠性一般较低，一旦计算机发生故障，将导致整个网络系统的瘫痪。

为了克服第一代计算机网络的缺点，提高网络的可靠性和可用性，人们开始研究将多台计算机相互连接的方法。

人们首先想到能否借鉴电话系统中所采用的电路交换（ circuit switching）思想？多年来，虽然电话交换机经过多次更新换代，从人工接续、步进制、纵横制直到现代的计算机程序控制，

但是其本质始终未变，都是采用电路交换技术。从资源分配角度来看，电路交换是预先分配线路带宽的。用户在开始通话之前，先要通过拨号申请建立一条从发送端到接收端的物理通路。只有在此物理通路建立之后，双方才能通话。在通话过程中，用户始终占有从发送端到接收端的固定传输带宽。

电路交换本来是为电话通信而设计的，对于计算机网络来说，建立通路的呼叫过程太长，必须寻找新的适合于计算机通信的交换技术。 1964年8月，巴兰（Baran）在美国兰德（Rand）公司“论分布式通信”的研究报告中提到了存储转发的概念。 1962-1965年，美国国防部高级研究计划署（Advanced Research Projects Agency，ARPA）和英国的国家物理实验室（National Physics Laboratory，NPL）都在对新型的计算机通信技术进行研究。英国NPL的戴维斯（David）于1966年首次提出了“分组”（packet）这一概念。到1969年12月，DARPA的计算机分组交换网ARPANET投入运行。ARPANET连接了美国加州大学洛杉机分校、加州大学圣巴巴拉分校、斯坦福大学和犹他大学四个结点的计算机。 ARPANET的成功，标志着计算机网络的发展进入了一个新纪元。

ARPANET的成功运行使计算机网络的概念发生了根本性的变化。早期的面向终端的计算机网络是以单个主机为中心的星型网，各终端通过电话网共享主机的硬件和软件资源。但分组交换网则以通信子网为中心，主机和终端都处在网络的边缘，如图 1-3所示。主机和终端构成了用户资源子网。用户不仅共享通信子网的资源，而且还可共享用户资源子网的丰富的硬件和软件资源。这种以资源子网为中心的计算机网络通常被称为第二代计算机网络。

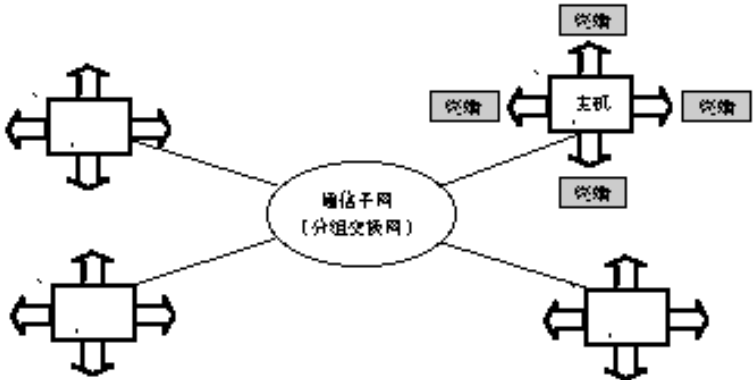


图1-3 第二代计算机网络：以通信子网为中心

在第二代计算机网络中，多台计算机通过通信子网构成一个有机的整体，既分散又统一，从而使整个系统性能大大提高；原来单一主机的负载可以分散到全网的各个机器上，使得网络系统的响应速度加快；而且在这种系统中，单机故障也不会导致整个网络系统的全面瘫痪。

在网络中，相互通信的计算机必须高度协调工作，而这种“协调”是相当复杂的。为了降低网络设计的复杂性，早在当初设计ARPANET时就有专家提出了层次模型。分层设计方法可以将庞大而复杂的问题转化为若干较小且易于处理的子问题。 1974年IBM公司宣布了它研制的系统网络体系结构SNA（System Network Architecture），它是按照分层的方法制定的。DEC公司也在七十年代末开发了自己的网络体系结构——数字网络体系结构（Digital Network Architecture，DNA）。

有了网络体系结构，使得一个公司所生产的各种机器和网络设备可以非常容易地被连接起来。但由于各个公司的网络体系结构是各不相同的，所以不同公司之间的网络不能互连互通。针对上述情况，国际标准化组织（International Standard Organization，ISO）于1977年设立专门的机构研究解决上述问题，并于不久后提出了一个使各种计算机能够互连的标准框架——开放式系统互连参考模型（Open System Interconnection / Reference Model，OSI/RM），简称OSI。OSI模型是一个开放体系结构，它规定将网络分为7层，并规定每层的功能，如图1-4所示。OSI参考模型的出现，意味着计算机网络发展到第三代。

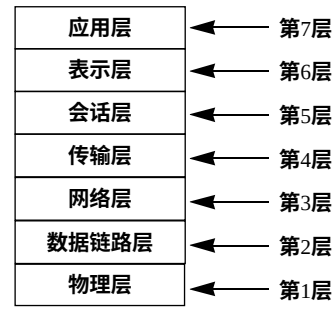


图1-4 第三代计算机网络：OSI参考模型

在OSI参考模型推出后，网络的发展道路一直走标准化道路，而网络标准化的最大体现就是Internet的飞速发展。现在Internet已成为世界上最大的国际性计算机互联网。Internet遵循TCP/IP参考模型，由于TCP/IP仍然使用分层模型，因此Internet仍属于第三代计算机网络。

计算机网络经过第一代、第二代和第三代的发展，表现出其巨大的使用价值和良好的应用前景。进入20世纪90年代以来，微电子技术、大规模集成电路技术、光通信技术和计算机技术不断发展，为网络技术的发展提供了有力的支持；而网络应用正迅速朝着高速化、实时化、智能化、集成化和多媒体化的方向不断深入，新型应用向计算机网络提出了挑战，新一代网络的出现已成必然。

计算机网络的发展既受到计算机科学技术和通信科学技术的支撑，又受到网络应用需求的推动。如今,计算机网络从体系结构到实用技术已逐步走向系统化、科学化和工程化。作为一门年轻的学科，它具有极强的理论性、综合性和依赖性，又具有自身特有的研究内容。它必须在一定的约束条件下研究如何合理、有效地管理和调度网络资源（如链路、带宽、信息等），提供适应不同应用需求的网络服务和拓展新的网络应用。图1-5给出了计算机网络体系结构演变的大致过程。

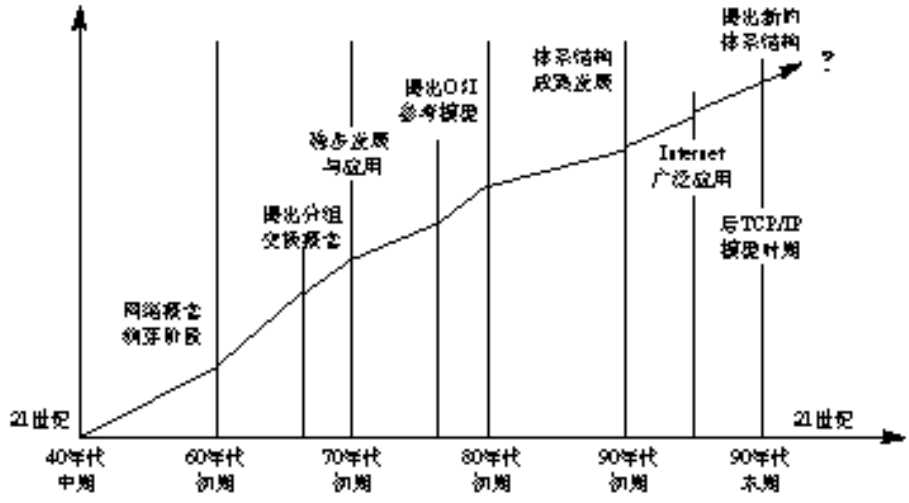


图1-5 网络体系结构的演变过程

1.2 计算机网络的功能

计算机网络自20世纪60年代末诞生以来，仅20多年时间即以异常迅猛的速度发展起来，被越来越广泛的应用于政治、经济、军事、生产及科学技术的各个领域。计算机网络的主要功能包括如下几个方面。

1. 数据通信

现代社会信息量激增，信息交换也日益增多，每年有几万吨信件要传递。利用计算机网络传递信件是一种全新的电子传递方式。电子邮件比现有的通信工具有更多的优点，它不像电话需要通话者同时在场，也不像广播系统只是单方向传递信息，在速度上比传统邮件快得多。另外，电子邮件还可以携带声音、图像和视频，实现多媒体通信。如果计算机网络覆盖的地域足够大，则可使各种信息通过电子邮件在全国乃至全球范围内快速传递和处理（如因特网上的电子邮件系统）。

除电子邮件以外，计算机网络给科学家和工程师们提供一个网络环境，在此基础上可以建立一种新型的合作方式——计算机支持协同工作（Computer Supported Co-operative Work，CSCW），它消除了地理上的距离限制。

2. 资源共享

在计算机网络中，有许多昂贵的资源，例如大型数据库、巨型计算机等，并非为每一用户所拥有，所以必须实行资源共享。资源共享包括硬件资源的共享，如打印机、大容量磁盘等；也包括软件资源的共享，如程序、数据等。资源共享的结果是避免重复投资和劳动，从而提高了资源的利用率，使系统的整体性能价格比得到改善。

3. 增加可靠性

在一个系统内，单个部件或计算机的暂时失效必须通过替换资源的办法来维持系统的继续运行。但在计算机网络中，每种资源（尤其程序和数据）可以存放在多个地点，而用户可以通过多种途径来访问网内的某个资源，从而避免了单点失效对用户产生的影响。

4. 提高系统处理能力

单机的处理能力是有限的，且由于种种原因（例如时差），计算机之间的忙闲程度是不均匀的。从理论上讲，在同一网内的多台计算机可通过协同操作和并行处理来提高整个系统的处理能力，并使网内各计算机负载均衡。

由于计算机网络具备上述功能，因此可以得到广泛的应用。在银行利用计算机网络进行业务处理时，可使用户在异地实现通存通兑，还可以利用地理位置的差异增加资金的流通速度。例如，地处美国的银行晚上停止营业后将资金通过网络转借给新加坡的银行，而此刻新加坡正是白天，新加坡银行就可在白天利用这些资金，到晚上再归还给美国的银行，从而提高了资金的利用率。

使用网络的另一个主要领域是访问远程数据库。也许要不了很长时间，许多人就能坐在家里向世界上任何地方预订飞机票、火车票、汽车票、轮船票，向饭店、餐馆和剧院订座，并且立即得到答复。

在军事指挥系统中的计算机网络，可以使遍布在十分辽阔地域范围内的各计算机协同工作，

对任何可疑的目标信息进行处理，及时发出警报，从而使最高决策机构采取有效措施。

在计算机网络的支持下，医生将可以联合看病：医疗设备技术人员、护士及各科医生同时给一个病人治疗；医务人员和医疗专家系统互为补充，以弥补医生在知识和医术方面的不足；各种电视会议可以使医生在遇到疑难病症时及时得到一个或更多医生的现场指导。伦敦的心脏病专家可以观察到旧金山进行的手术，并对正在进行手术的医生提出必要的建议。

在计算机网络的支持下，科学家们将组成各个领域的研究圈。现在科学家进行学术交流主要是通过国际会议和专业期刊，效率相对较低。预计在不久的将来，信息技术将使世界各地的科学家频繁、方便地参加电视会议，并在专用电子公告牌上发表最新的思想和研究成果。在更远的将来，信息技术将使异地的科学家们能够同时进行相同的课题研究并分担研究工作的各个部份。

目前，IP电话、网上寻呼、网络实时交谈和 E-mail已成为人们重要的通信手段。视频点播（VOD）、网络游戏、网上教学、网上书店、网上购物、网上订票、网上电视直播、网上医院、网上证券交易、虚拟现实以及电子商务正逐渐走进普通百姓的生活、学习和工作当中。

在未来，谁拥有“信息资源”，谁能有效使用“信息资源”，谁就能在各种竞争中占据主导地位。随着美国“信息高速公路”计划的提出和实施，计算机网络作为信息收集、存储、传输、处理和利用的整体系统，将在信息社会中得到更加广泛的应用。随着网络技术的不断发展，各种网络应用将层出不穷，并将逐渐深入到社会的各个领域及人们的日常生活当中，改变着人们的工作、学习和生活乃至思维方式。

1.3 计算机网络分类

计算机网络是指独立自治、相互连接的计算机集合。独立自治意味着每台连网的计算机是完整的计算机系统，可以独立运行用户的作业；相互连接意味着两台计算机之间能够相互交换信息。计算机之间的连接是物理的，由硬件实现。计算机连接所使用的介质可以是双绞线、同轴电缆或光纤等有线介质；也可以是无线电、激光、大地微波或卫星微波等无线介质。计算机之间的信息交换具有物理和逻辑上的双重含义。在计算机网络的最底层（通常为物理层），信息交换体现为直接相连的两台机器之间无结构的比特流传输；而在物理层之上的各层所交换的信息便有了一定的逻辑结构，越往上逻辑结构越复杂，也越接近用户真正需要的形式。信息交换在低层由硬件实现，而到了高层则由软件实现。在上述定义中之所以强调联网计算机的“独立自治”性，主要是为了将计算机网络与主机加终端构成的分时系统，以及与主机加从属计算机构成的主从式系统区分开。如果一台计算机带多台终端和打印机，这种系统通常被称为多用户系统，而不是计算机网络；而由一台主控机带多台从控机构成的系统，是主从式系统，也不是计算机网络。

计算机网络的分类标准很多，比如按拓扑结构、介质访问方式、交换方式以及数据传输率等，但这些分类标准只给出了网络某一方面的特征，并不能反映网络技术的本质。事实上，确实存在一种能反映网络技术本质的网络划分标准，那就是计算机网络的覆盖范围。按网络覆盖范围的大小，我们将计算机网络分为局域网（ LAN）、城域网（MAN）、广域网（WAN）和互联网，如表1-1所示。网络覆盖的地理范围是网络分类的一个非常重要的度量参数，因为不同规

模的网络将采用不同的技术。下面我们将简要介绍上述几种网络，最后讨论目前比较流行的无线网。

表1-1 计算机网络分类

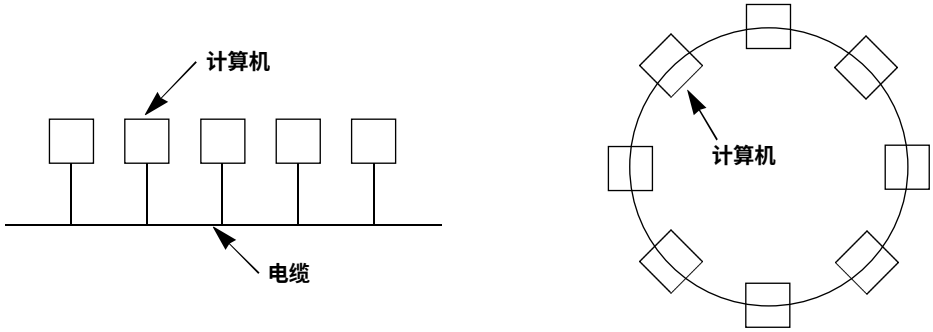
分布距离	覆盖范围	网络种类
10米	房间	
100米	建筑物	局域网
1公里	校园	
10公里	城市	城域网
100公里	国家	广域网
1000公里	洲或洲际	互联网

1.3.1 局域网

局域网（Loxal Area Network，LAN）是指范围在几百米到十几公里内办公楼群或校园内的计算机相互连接所构成的计算机网络。计算机局域网被广泛应用于连接校园、工厂以及机关的个人计算机或工作站，以利于个人计算机或工作站之间共享资源（如打印机）和数据通信。局域网区别于其他网络主要体现在下面3个方面：①网络所覆盖的物理范围；②网络所使用的传输技术；③网络的拓扑结构。

局域网中经常使用共享信道，即所有的机器都接在同一条电缆上。传统局域网具有高数据传输率（10 Mbps或100 Mbps）、低延迟和低误码率的特点。新型局域网的数据传输率可达每秒千兆位甚至更高。

局域网有不同的拓扑结构。图1-6给出了两种不同网络拓扑结构的示意图。在总线网络中，任何时刻只允许一台机器发送数据，而所有其他机器都处于接收状态。当有两台或多台机器想同时发送数据时必须进行仲裁，仲裁机制可以是集中式也可以是分布式的。例如IEEE 802.3，即以太网，它是基于共享总线采用分布控制机制、数据传输率为10 Mbps的局域网。以太网中的站点机器可以在任意时刻发送数据，当发生冲突时，每个站点机器立即停止发送数据并等待一个随机长的时间继续尝试数据发送。



a) 总线结构 b) 环状结构

图1-6 局域网的两种拓扑结构

局域网的第二种类型是环型网。在环型网中，数据沿着环不停地旋转。同样的道理，在环型网中必须有一种机制用于仲裁不同机器站点对环的同时访问。IEEE 802.5（即IBM令牌环）就是一种常用的数据传输率为4 Mbps或16 Mbps的环型局域网。

1.3.2 城域网

城域网（Metropolitan Area Network，MAN）所采用的技术基本上与局域网相类似，只是规模上要大一些。城域网既可以覆盖相距不远的几栋办公楼，也可以覆盖一个城市；既可以是私人网，也可以是公用网。城域网既可以支持数据和话音传输，也可以与有线电视相连。城域网一般只包含一到两根电缆，没有交换设备，因而其设计就比较简单。

将城域网作为一种网络类型的主要原因是其有标准而且已经实现，该标准的名称为分布式队列双总线（Distributed Queue Dual Bus，DQDB），它现在已经成为国际标准，编号为IEEE 802.6。DQDB的工作范围一般是160 km，数据传输率为44.736 Mbps。

DQDB采用两条单向总线，如图1-7所示，这两条平行的单向总线贯穿于整个城市，每个站点都同时与这两条总线相连。其中每条总线都有一个端接点，各自产生一个53字节的信元流。每个信元都从端接点沿着总线往下传，当它到达终点时，就从总线中消失。

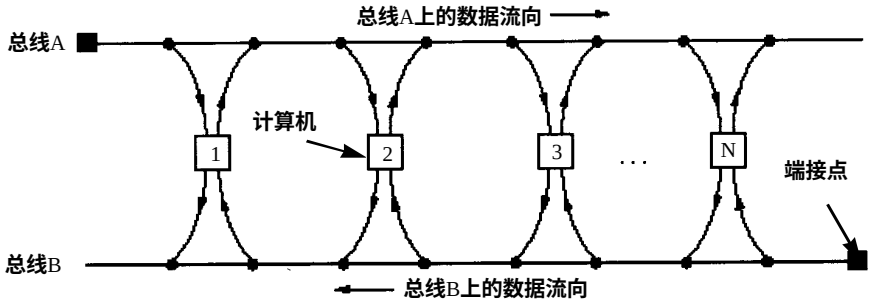


图1-7 DQDB城域网的结构

每个信元带有44字节的有效载荷，而且每个信元中带有两个标志位：“忙”（busy）位和“请求”（request）位。当“忙”标志位为1，表示该信元已被占用；当某站点想发出请求时，将信元的“请求”标志位置为1。

每个站点在发送信元之前必须知道目的站点是位于其左方还是右方。如果目的站点位于它的右方，发送站点使用总线A，否则使用总线B。在DQDB中，每个站点的数据是通过“线或”电路输入到相应的总线中，因此某个站点的失效不会造成整个网络的瘫痪。

在802.6标准中，站点是按照先进先出的原则进行排队发送数据。802.6采取的发送原则是每个站点必须有礼貌，即每个站点必须等到其下方的站点发送完后自己才能发送。这种礼貌的目的是为了防止下列情况的发生，即离端接点最近的站点将经过它的所有空闲信元全部捕获并填入内容，致使其后的站点被“饿死”。

1.3.3 广域网

广域网（Wido Area Network，WAN）通常跨接很大的物理范围，如一个国家。广域网包含

很多用来运行用户应用程序的机器集合，我们通常把这些机器叫做主机（ host）；把这些主机连接在一起的是通信子网（communication subnet)。通信子网的任务是在主机之间传送报文。将计算机网络中的纯通信部分的子网与应用部分的主机分离开来，可以大大简化网络的设计。广域网的物理结构如图1-8所示。

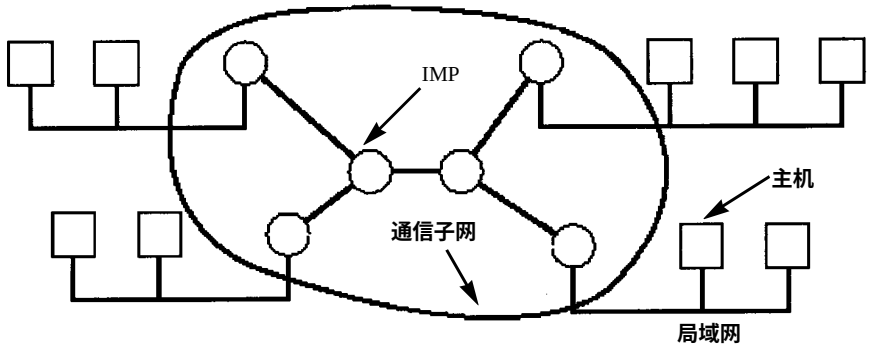


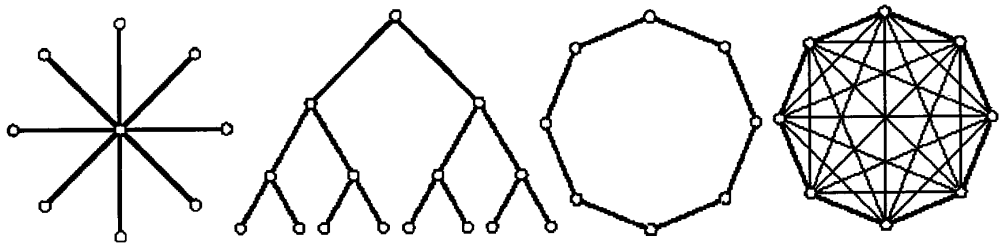
图1-8 广域网物理结构

在大多数广域网中，通信子网一般都包括两部份：传输信道和转接设备。传输信道用于在机器间传送数据。转接设备是专用计算机，用来连接两条或多条传输线。当数据从一条输入信道到达后，转接设备必须选择一条输出信道，把数据继续向前发送。在 ARPANET网中，转接设备叫做接口信息处理机 IMP。在图1-8所示模式中，每一台主机都至少连着一台 IMP。所有出入该主机的报文，都必须经过与该主机相连的 IMP。

绝大多数广域网中，通信子网包含大量租用线路或专用线路，每一条线路连着一对 IMP。当报文从源结点经过中间 IMP发往远方目的结点时，每个 IMP将输入的报文完整接收下来并贮存起来，然后选择一条空闲的输出线路，继续向前传送，因此这种子网又称为点到点（ point-to-point）子网、存储转发（store-and-forward）子网。除了那些使用卫星的广域网外，几乎所有的广域网都采用存储转发方式。

广域网最初只是为使物理上广泛分布的计算机能够进行简单的数据传输。主要用于交互终端与主机的连接、计算机之间文件或批处理作业传输以及电子邮件传输等。

在广域网中，一个重要的设计问题是 IMP互连的拓扑结构应是什么形式。图 1-9展示了几种可能的网络拓扑结构。



a) 星型 b) 树型 c) 环型 d) 全互连

图1-9 广域网拓扑结构

广域网的第二种可能的组网方式是卫星或地面无线电网。每个中间转接站点都通过天线接收和发送数据。所有的中间站点都能接收到来自卫星的信息，并能同时听到其相邻站点发往卫星的信息。

1.3.4 互联网

目前世界上有许多网络，而不同网络的物理结构、协议和所采用的标准是各不相同的。如果连接到不同网络的用户需要进行相互通信，就需要将这些不兼容的网络通过称为网关（gateway）的机器设备连接起来，并由网关完成相应的转换功能。多个网络相互连接构成的集合称为互联网（internetworking）。互联网的最常见形式是多个局域网通过广域网连接起来。实际上，在图1-8中，我们只要将“通信子网”改为“广域网”，就可得到互联网的结构图。如何判断一个网络是广域网还是通信子网取决于网络中是否含有主机。如果一个网络只含有中间转接站点，即IMP，则该网络仅仅是一个通信子网；反之，如果网络中既包含 IMP，又包含用户可以运行作业的主机，则该网络是一个广域网。

通信子网、网络和互联网这三个概念经常混淆。通信子网作为广域网的一个重要组成部分，通常是由IMP和通信线路所组成。举个例子，电话系统包括用高速线路连接的局间交换机和连到用户端的低速线路，这些线路和设备就构成电话系统的通信子网，它的所有权属于电话公司并由它们经营管理，而用户的电话机则不是子网的一部分。通信子网和主机相结合构成计算机网络（对于局域网来说，它是由电缆和主机构成的，没有通信子网）。而互联网一般是不同网络的相互连接，如局域网和广域网的连接、两个局域网的相互连接或多个局域网通过广域网连接起来。

1.3.5 无线网

随着笔记本电脑（Cnotebook compnter）和个人数字助理（Personal Digital Assistant，PDA）等便携式计算机的日益普及和发展，人们经常要在路途中接听电话、发送传真和电子邮件阅读网上信息以及登录到远程机器等。然而在汽车或飞机上是不可能通过有线介质与单位的网络相连接的，这时候可能会对无线网感兴趣了。

虽然无线网与移动通信经常是联系在一起的，但这两个概念并不完全相同。表 1-2给出了它们之间的对比。例如当便携式计算机通过 PCMCIA卡接入电话插口，它就变成有线网的一部分。另一方面，有些通过无线网连接起来的计算机的位置可能又是固定不变的，如在不便于通过有线电缆连接的大楼之间就可以通过无线网将两栋大楼内的计算机连接在一起。

表1-2 无线网与移动通信的对比

无线的	移动的	应用场所
No	No	办公室内固定计算机联网
No	Yes	在宾馆中使用的便携式计算机联网
Yes	No	没有布线的办公大楼内的计算机联网
Yes	Yes	移动办公室或PDA

无线网特别是无线局域网有很多优点，如易于安装和使用。但无线局域网也有许多不足之处：如它的数据传输率一般比较低，远低于有线局域网；另外无线局域网的误码率也比较高，而且站点之间相互干扰比较厉害。

用户无线网的实现有不同的方法。国外的某些大学在它们的校园内安装许多天线，允许学生们坐在树底下查看图书馆的资料。这种情况是通过两个计算机之间直接通过无线局域网以数字方式进行通信实现的。另一种可能的方式是利用传统的模拟调制解调器通过蜂窝电话系统进行通信。目前在国外的许多城市已能提供蜂窝式数字信息分组数据（Cellular Digital Packet Data，CDPD）的业务，因而可以通过CDPD系统直接建立无线局域网。

无线网络是当前国内外的研究热点，无线网络的研究是由巨大的市场需求驱动的。无线网的特点是使用户可以在任何时间、任何地点接入计算机网络，而这一特性使其具有强大的应用前景。当前已经出现了许多基于无线网络的产品，如个人通信系统（ Personal Communication System，PCS）电话、无线数据终端、便携式可视电话、个人数字助理（ PDA）等。

无线网络的发展依赖于无线通信技术的支持。目前无线通信系统主要有：低功率的无绳电话系统、模拟蜂窝系统、数字蜂窝系统、移动卫星系统、无线 LAN和无线WAN等。

1.4 网络体系结构

要想让两台计算机进行通信，必须使它们采用相同的信息交换规则。我们把在计算机网络中用于规定信息的格式以及如何发送和接收信息的一套规则称为网络协议（ network protocol）或通信协议（communication protocol）。

为了减少网络协议设计的复杂性，网络设计者并不是设计一个单一、巨大的协议来为所有形式的通信规定完整的细节，而是采用把通信问题划分为许多个小问题，然后为每个小问题设计一个单独的协议的方法。这样做使得每个协议的设计、分析、编码和测试都比较容易。

分层模型（layering model）是一种用于开发网络协议的设计方法。本质上，分层模型描述了把通信问题分为几个小问题（称为层次）的方法，每个小问题对应于一层。

1.4.1 协议分层

为了减少网络设计的复杂性，绝大多数网络采用分层设计方法。所谓分层设计方法，就是按照信息的流动过程将网络的整体功能分解为一个个的功能层，不同机器上的同等功能层之间采用相同的协议，同一机器上的相邻功能层之间通过接口进行信息传递。

为了便于理解接口和协议的概念，我们首先以邮政通信系统为例进行说明。人们平常写信时，都有个约定，这就是信件的格式和内容。首先，我们写信时必须采用双方都懂的语言文字和文体，开头是对方称谓，最后是落款等。这样，对方收到信后，才可以看懂信中的内容，知道是谁写的，什么时候写的等。当然还可以有其他的一些特殊约定，如书信的编号、间谍的密写等。信写好之后，必须将信封装并交由邮局寄发，这样寄信人和邮局之间也要有约定，这就是规定信封写法并贴邮票。在中国寄信必须先写收信人地址、姓名，然后才写寄信人的地址和姓名。邮局收到信后，首先进行信件的分拣和分类，然后交付有关运输部门进行运输，如航空信交民航，平信交铁路或公路运输部门等。这时，邮局和运输部门也有约定，如到站地点、时

间、包裹形式等等。信件运送到目的地后进行相反的过程，最终将信件送到收信人手中，收信人依照约定的格式才能读懂信件。如图 1-10所示，在整个过程中，主要涉及到了三个子系统、即用户子系统，邮政子系统和运输子系统。

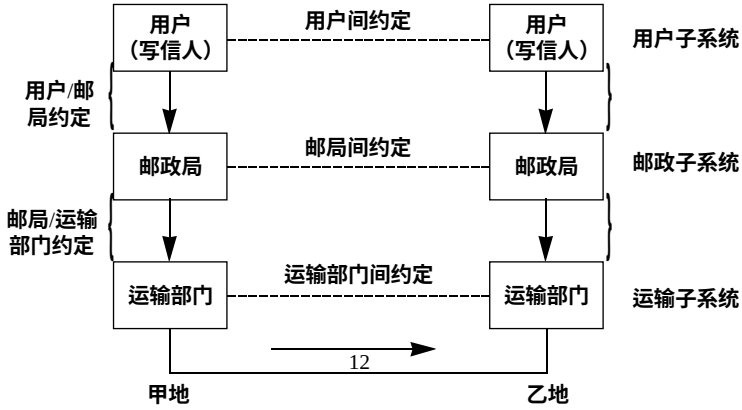


图1-10 邮政系统分层模型

从上例可以看出，各种约定都是为了达到将信件从一个源点送到某一个目的点这个目标而设计的，这就是说，它们是因信息的流动而产生的。可以将这些约定分为同等机构间的约定，如用户之间的约定、邮政局之间的约定和运输部门之间的约定，以及不同机构间的约定，如用户与邮政局之间的约定、邮政局与运输部门之间的约定。

虽然两个用户、两个邮政局、两个运输部门分处甲、乙两地，但它们都分别对应同等机构，同属一个子系统；而同处一地的不同机构则不在一个子系统内，而且它们之间的关系是服务与被服务的关系。很显然，这两种约定是不同的，前者为部门内部的约定，而后者是不同部门之间的约定。

在计算机网络环境中，两台计算机中两个进程之间进行通信的过程与邮政通信的过程十分相似。用户进程对应于用户，计算机中进行通信的进程（也可以是专门的通信处理机）对应于邮局，通信设施对应于运输部门。

为了减少计算机网络设计的复杂性，人们往往按功能将计算机网络划分为多个不同的功能层。网络中同等层之间的通信规则就是该层使用的协议，如有关第 N层的通信规则的集合，就是第N层的协议。而同一计算机的不同功能层之间的通信规则称为接口（ interface），在第N层和第（N+1）层之间的接口称为N /（N+1）层接口。总的来说，协议是不同机器同等层之间的通信约定，而接口是同一机器相邻层之间的通信约定。不同的网络，分层数量、各层的名称和功能以及协议都各不相同。然而，在所有的网络中，每一层的目的都是向它的上一层提供一定的服务。

协议层次化不同于程序设计中模块化的概念。在程序设计中，各模块可以相互独立，任意拼装或者并行，而层次则一定有上下之分，它是依数据流的流动而产生的。组成不同计算机同等层的实体称为对等进程（peer process）。对等进程不一定非是相同的程序，但其功能必须完全一致，且采用相同的协议。

分层设计方法将整个网络通信功能划分为垂直的层次集合后，在通信过程中下层将向上层

隐蔽下层的实现细节。但层次的划分应首先确定层次的集合及每层应完成的任务。划分时应按逻辑组合功能，并具有足够的层次，以使每层小到易于处理。同时层次也不能太多，以免产生难以负担的处理开销。

计算机网络体系结构是网络中分层模型以及各层功能的精确定义。对网络体系结构的描述必须包括足够的信息，使实现者可以为每一功能层进行硬件设计或编写程序，并使之符合相关协议。但我们要注意的是，网络协议实现的细节不属于网络体系结构的内容，因为它们隐含在机器内部，对外部说来是不可见的。

现在我们来考查一个具体的例子：在图 1-11所示的5层网络中如何向其最上层提供通信。在第5层运行的某应用进程产生了消息 M，并把它交给第 4层进行发送。第 4层在消息M前加上一个信息头（header），信息头主要包括控制信息（如序号）以便目标机器上的第 4层在低层不能保持消息顺序时，把乱序的消息按原序装配好。在有些层中，信息头还包括长度、时间和其他控制字段。

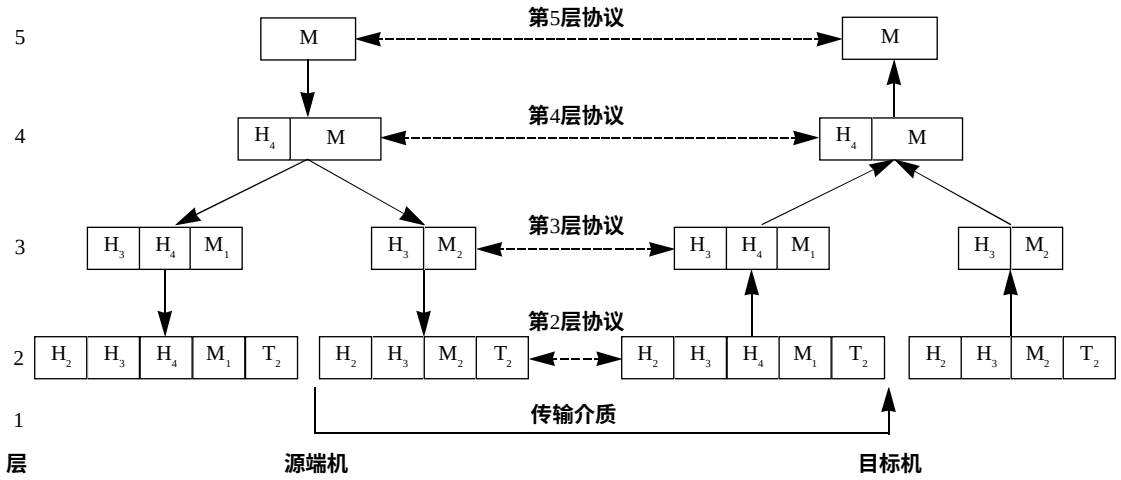


图1-11 支持第5层虚拟通信的例子

在很多网络中，第 4层对接收的消息长度没有限制，但在第 3层通常存在一个限度。因此，第3层必须将接收的入境消息分成较小的单元如报文分组（ packet），并在每个报文分组前加上一个报头。在本实例中，消息M被分成两部分：M1和M2。

第3层确定使用哪一条输出线路，并将报文传给第 2层。第2层不仅给每段消息加上头部信息，而且还要加上尾部信息，构成新的数据单元，通常称为帧（ frame），然后将其传给第 1层进行物理传输。在接收方，报文每向上递交一层，该层的报头就被剥掉，决不可能出现带有 *N*层以下报头的报文交给接收方第 *N*层实体的情况。

要理解图1-11示意图，关键要理解虚拟通信与物理通信之间的关系，以及协议与接口之间的区别。比如，第4层的对等进程，在概念上认为它们的通信是水平方向地应用第四层协议。每一方都好像有一个叫做“ 发送到另一方去 ”的过程和一个叫做“ 从另一方接收 ”的过程，尽管实际上这些过程是跨过3/4层接口与下层通信而不是直接同另一方通信。

抽象出对等进程这一概念，对网络设计是至关重要的。有了这种抽象技术，网络设计者就

可以把设计完整的网络这种难以处理的大问题，划分成设计几个较小的且易于处理的问题，即分别设计各层。

1.4.2 服务类型

服务（service）这个极普通的术语在计算机网络中无疑是一个极重要的概念。在网络体系结构中，服务就是网络中各层向其相邻上层提供的一组操作，是相邻两层之间的界面。

由于网络分层结构中的单向依赖关系，使得网络中相邻层之间的界面也是单向性的：下层是服务提供者，上层是服务用户。而服务的表现形式是原语（ primitive），比如库函数或系统调用。为了更好地讨论网络服务，我们先解释几个术语。

在网络中，每一层中至少有一个实体（ entity）。实体既可以是软件实体（比如一个进程），也可以是硬件实体（比如一块网卡）。在不同机器上同一层内的实体叫做对等实体（ peer entity）。*N*层实体实现的服务为*N*+1层所利用，而*N*层则要利用*N*-1层所提供的服务。*N*层实体可能向*N*＋1层提供几类服务，如快速而昂贵的通信或慢速而便宜的通信。

N＋1层实体是通过*N*层的服务访问点（Service Access Point，SAP）来使用*N*层所提供的服务。*N*层SAP就是*N*+1层可以访问*N*层服务的地方。每一个SAP都有一个唯一地址。为了使读者更清楚，我们可以把电话系统中的SAP看成标准电话插孔，而SAP地址是这些插孔的电话号码。要想和他人通话，必须知道他的 SAP地址（电话号码）。在伯克利版本的 Unix系统中， SAP是“ Socket ”，SAP地址是Socket号。

邻层间通过接口要交换信息。*N*+1层实体通过SAP把一个接口数据单元（Interface Data Unit，IDU）传递给*N*层实体，如图1-12所示。IDU由服务数据单元（Service Data Unit，SDU）和一些控制信息组成。

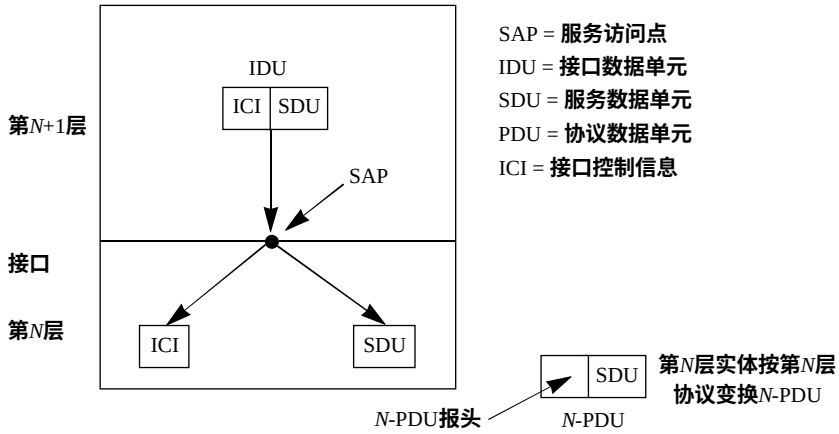


图1-12 相邻层在接口的关系

为了传送SDU，*N*层实体可以将SDU分成几段，每一段加上一个报头后作为独立的协议数据单元（Protocol Data Unit，PDU）送出，如“ 分组 ”就是 PDU。PDU报头被同层实体用来执行它们的同层协议，用于辨别哪些 PDU包含数据，哪些包含控制信息，并提供序号和计数值等。

在网络中，下层向上层提供的服务分为两大类：面向连接服务（ connection-oriented service）

和无连接服务（connectionless service）。

面向连接服务是电话系统服务模式的抽象。每一次完整的数据传输都必须经过建立连接、数据传输和终止连接三个过程。在数据传输过程中，各数据包地址不需要携带目的地址，而是使用连接号。连接本质上类似于一个管道，发送者在管道的一端放入数据，接收者在另一端取出数据。其特点是接收到的数据与发送方发出的数据在内容和顺序上是一致的。

无连接服务是邮政系统服务模式的抽象。其中每个报文带有完整的目的地址，每个报文在系统中独立传送。无连接服务不能保证报文到达的先后顺序，原因是不同的报文可能经不同的路径去往目的地，所以先发送的报文不一定先到。无连接服务一般也不对出错报文进行恢复和重传。换句话说，无连接服务不保证报文传输的可靠性。

在计算机网络中，可靠性一般通过确认和重传（acknowledgement and retransmission）机制实现。大多数面向连接服务都支持确认重传机制，但确认和重传将带来额外的延迟。有些对可靠性要求不高的面向连接服务（如数字电话网）不支持重传；因为电话用户宁可听到带有杂音的通话，也不喜欢等待确认所造成的延迟。大多数无连接服务不支持确认重传机制，所以无连接传输服务往往可靠性不高。

1.4.3 服务原语

“服务”在形式上是用一组原语来描述的，这些原语供用户实体访问该服务或向用户实体报告某事件的发生。服务原语可以划分为如表1-3所示的4类。

表1-3 4类服务原语

原 语	意 义
请求（Request）	用户实体要求服务做某项工作
指示（Indication）	用户实体被告知某事件发生
响应（Response）	用户实体表示对某事件的响应
确认（Confirm）	用户实体收到关于它的请求的答复

第1类原语是“请求”（request）原语，服务用户用它促成某项工作，如请求建立连接和发送数据。服务提供者执行这一请求后，将用“指示”（indication）原语通知接收方的用户实体。例如，发出“连接请求”（CONNECT_request）原语之后，该原语地址段内所指向的接收方的对等实体会得到一个“连接指示”（CONNECT_indication）原语，通知它有人想要与它建立连接。接收到“连接指示”原语的实体使用“连接响应”（CONNECT_response）原语表示它是否愿意接受建立连接的建议。但无论接收方是否接受该请求，请求建立连接的一方都可以通过接收“连接确认”（CONNECT_confirm）原语而获知接收方的态度（事实上传输层以及其他层的服务用户要拒绝建立连接请求不是采用CONNECT_response原语而是采用DISCONNECT_request原语）。

原语可以带参数，而且大多数原语都带有参数。“连接请求”原语的参数可能指明它要与哪台机器连接、需要的服务类别和拟在该连接上使用的最大报文长度。“连接指示”原语的参数可能包含呼叫者的标志、需要的服务类别和建议的最大报文长度。如果被呼叫的实体不同意呼叫实体建立的最大报文长度，它可能在“连接响应”原语中提出一个新的建议，呼叫方会从“连

接确认”原语中获知。这一协商过程的细节属于协议的内容。例如，在两个关于最大报文长度的建议不一致的情况下，协议可能规定选择较小的值。

服务有“有确认”和“无确认”之分。有确认服务，包括“请求”、“指示”、“响应”和“确认”4个原语。无确认服务只有“请求”和“指示”两个原语。建立连接的服务总是有确认服务，可用“连接响应”作肯定应答，表示同意建立连接；或者用“断连请求”（DISCONNECT_request）表示拒绝，作否定应答。数据传送既可以是有确认的也可是无确认的，这取决于发送方是否需要确认。

为了使服务原语的概念更具体化一些，我们将考查一个简单的面向连接服务的例子。它使用了下述8个服务原语：

1) 连接请求：服务用户请求建立一个连接。
2) 连接指示：服务提供者向被呼叫方示意有人请求建立连接。
3) 连接响应：被呼叫方用来表示接受建立连接的请求。
4) 连接确认：服务提供者通知呼叫方建立连接的请求已被接受。
5) 数据请求：请求服务提供者把数据传至对方。
6) 数据指示：表示数据的到达。
7) 断连请求：请求释放连接。
8) 断连指示：将释放连接请求通知对等端。

在本例中，连接是有确认服务（需要一个明确的答复），而断连是无确认的（不需要应答）。与电话系统作一比较，也许有助于理解这些原语是如何应用的。请考虑一下打电话邀请你的姑姑到家来喝茶的步骤：

1) 连接请求：拨姑姑家的电话号码。
2) 连接指示：她家的电话铃响了。
3) 连接响应：她拿起电话。
4) 连接确认：你听到响铃停止。
5) 数据请求：你邀请她来喝茶。
6) 数据指示：她听到了你的邀请。
7) 数据请求：她说她很高兴来。
8) 数据指示：你听到她接受邀请。
9) 断连请求：你挂断电话。
10) 断连指示：她听到了，也挂断电话。

图1-13用一系列服务原语来表示上述各步。每一步都涉及其中一台计算机内两层之间的信息交换。每一个“请求”或“响应”稍后都在对方产生一个“指示”或“确认”动作。本例中服务用户（你和姑姑）在N+1层，服务提供者（电话系统）在N层。

服务和协议常常被混淆，而实际上二者是迥然不同的两个概念。为此我们再强调一下两者的区别。服务是网络体系结构中各层向它的上层提供的一组原语（操作）。尽管服务定义了该层能够代表它的用户完成的操作，但丝毫也未涉及这些操作是如何实现的。服务描述两层之间的接口，下层是服务提供者，上层是服务用户。而协议是定义同层对等实体间交换帧、数据包的

格式和意义的一组规则。网络各层实体利用协议来实现它们的服务。只要不改变提供给用户的服务和接口，实体可以随意地改变它们所使用的协议。这样，服务和协议就完全被分离开来。在OSI参考模型之前的很多网络并没有把服务从协议中分离出来，造成网络设计的困难，现在人们已经普遍承认这样的设计是一种重大失策。

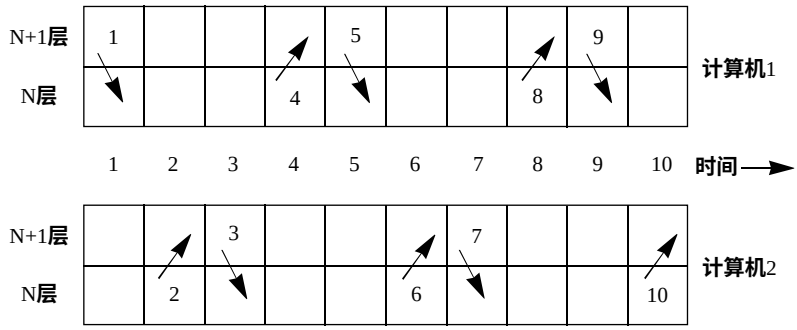


图1-13 计算机1与计算机2进行通信

1.5 ISO/OSI参考模型

我们已经一般性地讨论了协议分层和网络体系结构。下面我们将分析和讨论一些具体的网络体系结构。在下面的内容中，我们将主要讨论一个重要的网络体系结构，即 OSI参考模型。

1.5.1 参考模型

在网络发展的初期，许多研究机构、计算机厂商和公司都大力发展计算机网络。从ARPANET出现至今，已经推出了许多商品化的网络系统。这种自行发展的网络，在体系结构上差异很大，以至于它们之间互不相容，难于相互连接以构成更大的网络系统。为此，许多标准化机构积极开展了网络体系结构标准化方面的工作，其中最为著名的就是国际标准化组织 ISO提出的开放系统互连参考模型 OSI/RM。OSI参考模型是研究如何把开放式系统（即为了与其他系统通信而相互开放的系统）连接起来的标准。

OSI参考模型将计算机网络分为 7层，如图1-14所示。我们将从最底层开始，依次讨论模型的各层所要完成的功能。

1. 物理层

物理层（physical layer）的主要功能是完成相邻结点之间原始比特流的传输。物理层协议关心的典型问题是使用什么样的物理信号来表示数据“ 1”和“ 0”；一位持续的时间多长；数据传输是否可同时在两个方向上进行；最初的连接如何建立和完成通信后连接如何终止；物理接口（插头和插座）有多少针以及各针的用处。物理层的设计主要涉及物理层接口的机械、电气、功能和过程特性，以及物理层接口连接的传输介质等问题。物理层的设计还涉及到通信工程领域内的一些问题。

2. 数据链路层

数据链路层（data link layer）的主要功能是如何在不可靠的物理线路上进行数据的可靠传

输。数据链路层完成的是网络中相邻结点之间可靠的数据通信。为了保证数据的可靠传输，发送方把用户数据封装成帧（frame），并按顺序传送各帧。由于物理线路的不可靠，因此发送方发出的数据帧有可能在线路上发生出错或丢失（所谓丢失实际上是数据帧的帧头或帧尾出错），从而导致接收方不能正确接收到数据帧。为了保证能让接收方对接收到的数据进行正确性判断，发送方为每个数据块计算出 CRC（循环冗余检验）并加入到帧中，这样接收方就可以通过重新计算CRC来判断数据接收的正确性。一旦接收方发现接收到的数据有错，则发送方必须重传这一帧数据。然而，相同帧的多次传送也可能使接收方收到重复帧。比如，接收方给发送方的确认帧被破坏后，发送方也会重传上一帧，此时接收方就可能接收到重复帧。数据链路层必需解决由于帧的损坏、丢失和重复所带来的问题。

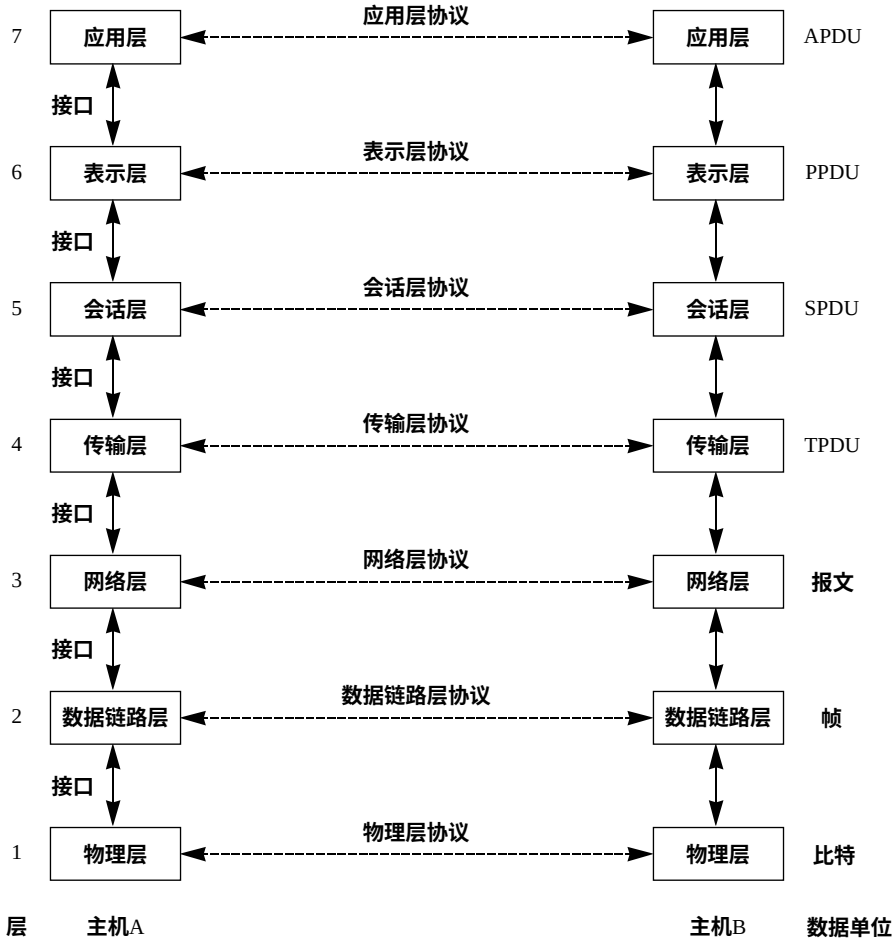


图1-14 ISO/OSI参考模型

数据链路层要解决的另一个问题是防止高速发送方的数据把低速接收方“淹没”。因此需要某种信息流量控制机制使发送方得知接收方当前还有多少缓存空间。为了控制的方便，流量控制常常和差错处理一同实现。

在广域网中，数据链路层负责主机- IMP、IMP-IMP之间数据的可靠传送；而在局域网中，数据链路层负责主机之间数据的可靠传输。

3. 网络层

网络层（network layer）的主要功能是完成网络中主机间的报文传输，其关键问题之一是使用数据链路层的服务将每个报文从源端传输到目的端。在广域网中，这包括产生从源端到目的端的路由，并要求这条路径经过尽可能少的 IMP。如果在子网中同时出现过多的报文，子网可能形成拥塞，必须加以避免，此类控制也属于网络层的内容。

当报文不得不跨越两个或多个网络时，又会产生很多新问题。例如第二个网络的寻址方法可能不同于第一个网络；第二个网络也可能因为第一个网络的报文太长而无法接收；两个网络使用的协议也可能不同，等等。网络层必须解决这些问题，使异构网络能够互连。

在单个局域网中，网络层是冗余的，因为报文是直接从一台计算机传送到另一台计算机的，因此网络层所要做的工作很少。

4. 传输层

传输层（transport layer）的主要功能是完成网络中不同主机上的用户进程之间可靠的数据通信。

传输层要决定对会话层用户，最终对网络用户，提供什么样的服务。最好的传输连接是一条无差错的、按顺序传送数据的管道，即传输层连接是真正端到端的。换言之，源端机上的某进程，利用报文头和控制报文与目标机上的对等进程进行对话。在传输层下面的各层中，协议是每台机器与它的直接相邻机器之间（主机- IMP、IMP-IMP）的协议，而不是最终的源端机和目标机之间（主机-主机）的协议。在它们中间，可能还隔着多个 IMP。即1至3层的协议是点到点的协议，而4至7层的协议是端到端的协议。

由于绝大多数主机都支持多用户操作，因而机器上有多道程序，这意味着多条连接将进出于这些主机，因此需要以某种方式区别报文属于哪条连接。识别这些连接的信息可以放入传输层的报文头中。除了将几个报文流多路复用到一条通道上，传输层还必须管理跨网连接的建立和拆除。这就需要某种命名机制，使机器内的进程能够讲明它希望交谈的对象。另外，还需要有一种机制来调节信息流，使高速主机不会过快地向低速主机传送数据。尽管主机之间的流量控制与IMP之间的流量控制不尽相同，但是稍后我们将看到类似的原理对二者都适用。

5. 会话层

会话层（session layer）允许不同机器上的用户之间建立会话关系。会话层允许进行类似传输层的普通数据的传送，在某些场合还提供了一些有用的增强型服务。允许用户利用一次会话在远端的分时系统上登录，或者在两台机器间传递文件。

会话层提供的服务之一是管理对话控制。会话层允许信息同时双向传输，或任一时刻只能单向传输。如果属于后者，类似于物理信道上的半双工模式，会话层将记录此时该轮到哪一方。一种与对话控制有关的服务是令牌管理（ token management）。有些协议保证双方不能同时进行同样的操作，这一点很重要。为了管理这些活动，会话层提供了令牌，令牌可以在会话双方之间移动，只有持有令牌的一方可以执行某种关键性操作。另一种会话层服务是同步。如果在平均每小时出现一次大故障的网络上，两台机器间要进行一次两小时的文件传输，想想会出现什

么样的问题？每一次传输中途失败后，都不得不重新传送这个文件。当网络再次出现大故障时，可能又会半途而废。为了解决这个问题，会话层提供了一种方法，即在数据中插入同步点。每次网络出现故障后，仅仅重传最后一个同步点以后的数据。

6. 表示层

表示层（presentation layer）完成某些特定的功能，对这些功能人们常常希望找到普遍的解决办法，而不必由每个用户自己来实现。值得一提的是，表示层以下各层只关心从源端机到目标机可靠地传送比特，而表示层关心的是所传送的信息的语法和语义。表示层服务的一个典型例子是用一种大家一致选定的标准方法对数据进行编码。大多数用户程序之间并非交换随机的比特，而是交换诸如人名、日期、货币数量和发票之类的信息。这些对象是用字符串、整型数、浮点数的形式，以及由几种简单类型组成的数据结构来表示。

网络上计算机可能采用不同的数据表示，所以需要在数据传输时进行数据格式的转换。例如在不同的机器上常用不同的代码来表示字符串（ ASCII和EBCDIC）、整型数（二进制反码或补码）以及机器字的不同字节顺序等。为了让采用不同数据表示法的计算机之间能够相互通信并交换数据，我们在通信过程中使用抽象的数据结构（如抽象语法表示 ASN.1）来表示传送的数据，而在机器内部仍然采用各自的标准编码。管理这些抽象数据结构，并在发送方将机器的内部编码转换为适合网上传输的传送语法以及在接收方做相反的转换等工作都是由表示层来完成的。

另外，表示层还涉及数据压缩和解压、数据加密和解密等工作。

7. 应用层

连网的目的在于支持运行于不同计算机的进程进行通信，而这些进程则是为用户完成不同任务而设计的。可能的应用是多方面的，不受网络结构的限制。应用层（ application layer）包含大量人们普遍需要的协议。虽然，对于需要通信的不同应用来说，应用层的协议都是必须的。

例如，PC机用户使用仿真终端软件通过网络仿真某个远程主机的终端并使用该远程主机的资源。这个仿真终端程序使用虚拟终端协议将键盘输入的数据传送到主机的操作系统，并接收显示于屏幕的数据。

再比如，当某个用户想要获得远程计算机上的一个文件拷贝时，他要向本机的文件传输软件发出请求，这个软件与远程计算机上的文件传输进程通过文件传输协议进行通信，这个协议主要处理文件名、用户许可状态和其他请求细节的通信。远程计算机上的文件传输进程使用其他特征来传输文件内容。

由于每个应用有不同的要求，应用层的协议集在 ISO/OSI模型中并没有定义，但是，有些确定的应用层协议，包括虚拟终端、文件传输、和电子邮件等都可作为标准化的候选。

1.5.2 模型评价

值得注意的是，OSI模型本身不是网络体系结构的全部内容，这是因为它并未确切地描述用于各层的协议和实现方法，而仅仅告诉我们每一层应该完成的功能。不过， ISO已经为各层制定了相应的标准，但这些标准并不是模型的一部分，它们是作为独立的国际标准而被发布的。

在OSI参考模型中，有三个基本概念：服务、接口和协议。也许 OSI模型的最重要的贡献是

将这三个概念区分清楚了。

OSI参考模型是在其协议开发之前设计出来的。这意味着 OSI模型不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着 OSI模型在协议实现方面存在某些不足。实际上，OSI协议过于复杂，这也是OSI从未真正流行开来的原因所在。

虽然OSI模型和协议并未获得巨大的成功，但是 OSI参考模型在计算机网络的发展过程中仍然起到了非常重要的指导作用，作为一种参考模型和完整体系，它仍对今后计算机网络技术朝标准化、规范化方向发展具有指导意义。

1.6 本书的结构

本书从内容上可分为五个部分。第一部分介绍数据通信知识，涉及数据通信基本概念和基础理论、传输介质、多路复用技术、数据交换技术、调制解调技术以及物理层接口技术等内容。这一部分内容包括书中的第2、3章。

第二部分讨论各种底层网络技术，涉及各种广域网、局域网和高速局域网技术。这一部分内容包括书中的第4～6章。

第三部分讨论网络互联技术及其相关协议，涉及网络互联、 TCP/IP参考模型、IP、ARP和ICMP、IP路由协议以及TCP和UDP等内容。这一部分内容包括第7～11章。

第四部分讨论网络应用程序相互作用模式以及各种具体的网络应用，涉及客户 /服务器模型、套接字编程接口、域名系统（DNS）、远程登录（Telnet）、文件传输和访问、电子邮件以及万维网。这一部分内容包括书中第12～17章。

第五部分讨论网络安全和管理，内容包括书中第18、19章。

本章是本书的第1章，简单介绍计算机网络的产生和发展、主要功能、分类以及网络体系结构和ISO/OSI参考模型。

本书的最后一章第20章，简单介绍了网络技术的未来发展。

第一部分　数 据 通 信

第2章　数据通信基础知识

数据通信是计算机网络的基础，没有数据通信技术的发展，就没有计算机网络的今天。写这一章的目的是想本书能够由浅入深，使只有少量甚至没有数据通信背景的读者也可以很好地阅读下去。

本章首先简单介绍数据通信的基本概念和基础理论，然后介绍各种传输介质、多路复用技术、数据交换技术以及调制解调技术。

2.1　基本概念

自古以来人们都在用自己的智慧来解决远距离、快速通信的问题，而衡量人类历史进步的尺度之一是人与人之间传递信息的能力，尤其是远距离传递消息的能力。例如古代的烽火台、金鼓、旌旗；近代的灯光、旗语；现代的电话、电报、传真和电视等都是传递消息的手段。通信技术的发展使社会产生了深远的变革，为人类社会带来了巨大的利益。

在当今和未来的信息社会中，通信是人们获取、传递和交换信息的重要手段。随着大规模集成电路技术、激光技术、空间技术等新型技术的不断发展以及计算机技术的广泛应用，现代通信技术日新月异。近二三十年来出现的数字通信、卫星通信、光纤通信是现代通信中具有代表性的新领域。而在这些新领域中，数字通信尤为重要，它是现代通信系统的基础。特别是数字通信技术和计算机技术的紧密结合可以说是通信发展史上的一次飞跃。本节我们将简单介绍数字通信的一些基本概念。

2.1.1　信号与通信

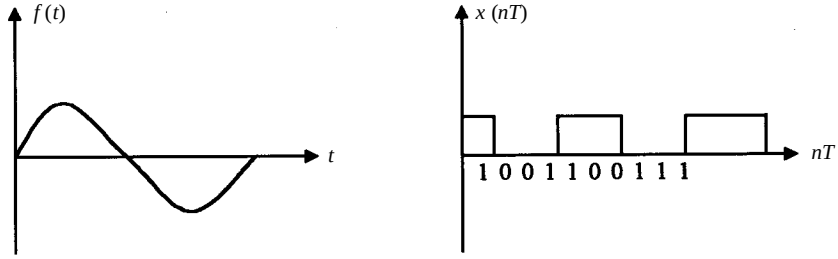
消息一般是用数据来表示的，而表示消息的数据通常要把它转变为信号进行传递。信号是消息（或数据）的一种电磁编码，信号中包含了所要传递的消息。

信号一般以时间为自变量，以表示消息（或数据）的某个参量（振幅、频率或相位）为因变量。信号按其因变量的取值是否连续可分为模拟信号和数字信号。

模拟信号是指信号的因变量完全随连续消息的变化而变化的信号。模拟信号的自变量可以是连续的，也可以是离散的；但其因变量一定是连续的，如图 2-1a所示。电视图像信号、语音信号、温度压力传感器的输出信号以及许多遥感遥测信号都是模拟信号；脉冲振幅调制信号（PAM）、脉冲相位调制信号（PPM）以及脉冲宽度调制信号（PWM）等也属于模拟信号。

数字信号是指表示消息的因变量是离散的，自变量时间的取值也是离散的信号，如图 2-1b所

示，通常表示为$x(nT)$，数字信号的因变量的状态是有限的。计算机数据、数字电话和数字电视等都是数字信号。



a) 模拟信号　　b) 数字信号

图2-1　模拟信号和数字信号

虽然模拟信号与数字信号有着明显的差别，但二者之间并没有存在不可逾越的鸿沟，在一定条件下它们是可以相互转化的。模拟信号可以通过采样、编码等步骤变成数字信号，而数字信号也可以通过解码、平滑等步骤恢复为模拟信号。

通信的任务是将表示消息的信号从发送方（信源）传递到接收方（信宿）。既然信号可分为模拟信号和数字信号，与之相对应的，通信也可分为模拟通信和数字通信。模拟通信通常是利用模拟信号来传递消息：而数字通信则是利用数字信号来传递消息。按传送模拟信号而设计的通信系统称为模拟通信系统，按传送数字信号而设计的通信系统称为数字通信系统。

2.1.2　模拟通信

利用模拟信号来传递消息称为模拟通信，普通的电话、广播、电视等都属于模拟通信。模拟通信系统的模型如图2-2所示。

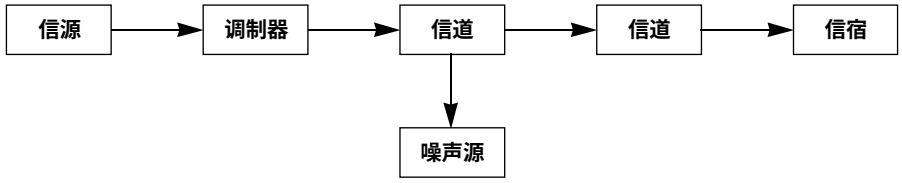


图2-2　模拟通信系统模型

模拟通信系统通常由信源、调制器、信道、解调器、信宿以及噪声源组成。信源所产生的原始模拟信号一般都要经过调制再通过信道传输（距离很近的有线通信也可以不调制，如市内电话）。调制器是用发送的消息对载波的某个参数进行调制的设备。解调器是实现上述过程逆变换的设备。

信道是用来传输表示消息的电信号的介质或通路。它可以是双绞线、同轴电缆、光缆、微波以及卫星链路等，有时我们将传输介质两端的设备也看作是信道的一部分。

模拟通信系统中的噪声源包括了影响该系统的所有噪声，如脉冲噪声（天电噪声、工业噪声等）和随机噪声（信道噪声、发送设备噪声、接收设备噪声等）。

在模拟通信系统中，信道上所传输的信号是模拟信号。例如对载波进行了连续的振幅调制（AM）、频率调制（FM）或相位调制（PM）而得到的调幅波、调频波或调相波都是模拟信号。对脉冲进行了连续的振幅调制、相位调制或宽度调制而得到的脉冲调幅波（ PAM）、脉冲调相波（PPM）或脉冲调宽波（PWM）也都属于模拟信号。

2.1.3 数字通信

利用数字信号来传递消息称为数字通信，计算机通信、数字电话以及数字电视都属于数字通信。数字通信系统模型如图 2-3所示。数字通信系统由信源、信源编码器、信道编码器、调制器、信道、解调器、信道译码器、信源译码器、信宿、噪声源以及发送端和接收端时钟同步组成。

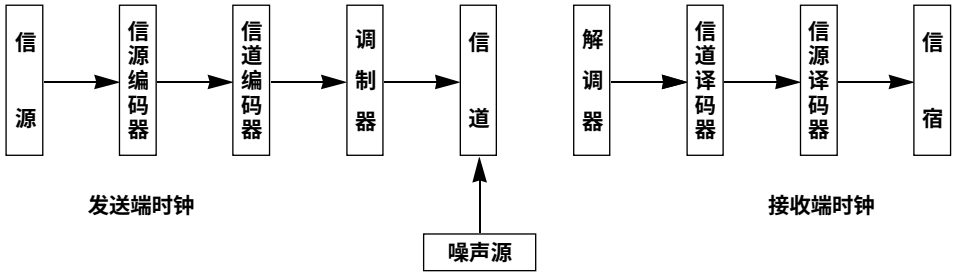


图2-3 数字通信系统模型

在数字通信系统中，如果信源发出的是模拟信号，就要经过信源编码器对模拟信号进行采样、量化及编码，将其变换为数字信号。信源编码有两个主要作用：一个是实现数 /模转换；另一个是降低信号的误码率。而信源译码则是信源编码的逆过程。

由于信道通常会遭受各种噪声的干扰（自然的和人为的）以及通信终端设备本身的噪声干扰，有可能导致接收端接收信号产生错误，即误码。为了能够自动地检测出错误或纠正错误，可采用检错编码或纠错编码，这就是信道编码；信道译码则是信道编码的逆变换。

从信道编码器输出的数码序列还是属于基带信号。除某些近距离的数字通信可以采用基带传输外，通常为了与采用的信道相匹配，都要将基带信号经过调制变换成频带信号再传输，这就是调制器所要完成的工作；而解调则是调制的逆过程。

时钟同步也是数字通信系统的一个重要的不可或缺的部分。由于数字通信系统传递的信号是数字信号，所以发送端和接收端必须有各自的发送和接收时钟系统。而为了保证接收端正确接收数字信号，接收端的接收时钟必须与发送端的发送时钟保持同步。

近年来，数字通信无论在理论上还是技术上都有了突飞猛进的发展。数字通信和模拟通信相比，具有抗干扰能力强、可以再生中继、便于加密、易于集成化等一系列优点。另外，各种通信业务，无论是话音、电报，还是数据、图像等信号，经过数字化后都可以在数字通信网中传输、交换并进行处理，这就更显示出数字通信的优越性。下面我们将讨论数字通信系统的主要特点：

(1) 抗干扰能力强

模拟通信系统传输的是模拟信号。模拟信号在传输过程中，噪声将叠加在有用的模拟信号上，接收端很难将信号和噪声分开，因而模拟通信系统的抗干扰能力比较差。相反，数字通信系统传输的是二进制信号，消息是寓于数字脉冲波形的两种状态之中。在数字通信的接收端对每一个接收信号进行采样并与某个门槛电平进行比较，只要采样时刻的信号电平不超过门槛电平，接收端就不会形成错判，可以正确接收数据，而不受噪声的影响。因此数字通信系统比模拟通信系统的抗干扰能力强。此外，数字通信系统还可以采用许多具有检错或纠错能力的编码技术，从而进一步提高了系统的抗干扰能力。

(2) 可实现高质量的远距离通信

对于模拟通信，噪声是叠加在有用的模拟信号上的。而模拟通信系统中的模拟放大器无法将有用的信号与噪声分开，只好将有用信号和噪声同时放大。随着传输距离的增加以及模拟放大器的增多，噪声也会越来越大，因此模拟通信系统中的噪声是有积累的，对远距离通信的质量造成很大的影响。而数字通信系统则是采用再生中继器的方法。即，传输过程中信号所受到的噪声干扰经过中继器时就已经被消除，然后再生器恢复出与原始信号相同的数字信号，因而克服了模拟通信系统中噪声叠加的问题，因此数字通信系统可以实现高质量的远距离通信。现代数字电话的通话质量要比传统模拟电话的通话质量好得多。

(3) 能适应各种通信业务

在数字通信系统中，各种消息（电报、电话、图像和数据等）都可以被变换为统一的二进制数字信号进行传输，所以数字通信系统能灵活地适应各种通信业务。通常我们把能够同时传输和处理各种不同业务的数字通信网叫做综合业务数字网（Intergated Services Digital Network，ISDN）。随着高速光纤传输技术、高速数字交换技术以及高性能处理技术的不断发展， ISDN将会在21世纪得到更广泛的应用。

(4) 能实现高保密通信

由于数字通信系统中传输的是数字信号，因而在传输过程中，可以对信号进行各种数字处理：如存储、转发、复制、加密、检错纠错等。这些处理在模拟通信系统中是不可能实现的。正因为在数字通信系统中可以对信号进行各种处理，因而也就可以在数字通信系统中采用复杂的、非线性的的长周期的密码序列对数字信号进行加密，从而使数字通信具有高度的保密性，能适用于很多对保密性要求非常高的场合，如军事应用领域。而模拟通信要实现高度加密是比较困难的。

(5) 通信设备的集成化和微型化

数字通信设备大都是由数字电路构成，数字电路比模拟电路更容易集成化。数字信号处理技术和大规模集成电路技术的发展为数字通信设备的微型化和集成化提供了良好的条件。而随着数字处理器件和大规模集成电路芯片价格的不断下降，数字传输设备以及相关的交换和处理设备都将比模拟传输设备便宜得多。

当然，与模拟通信相比，数字通信也有其缺点。数字通信的最大缺点是占用的频带宽。可以说数字通信的许多优点是以牺牲信道带宽为代价而换来的。以电话为例，一路模拟电话占用4 KHz信道带宽，而一路数字电话所需要的数据传输率是 64 Kbps，所需占用的带宽要远远大于4 KHz。数字通信的这一缺点限制了它在某些信道带宽不够大的场合的使用。

总之，数字通信的优点是主要的。特别是随着微波、卫星、光纤等高带宽信道的广泛使用，数字通信的缺点也越来越不明显，数字通信将是现代通信系统的一个重要发展方向。

2.2 数据通信基础理论

这一节的主要目的是讨论数据通信涉及的理论基础，主要内容包括信号的频谱与带宽、信道的截止频率与带宽以及信道所能支持的最大数据传输率。

2.2.1 信号的频谱与带宽

信号是数据的电磁编码，信号中包含了所要传递的数据。信号一般以时间为自变量，以表示消息（或数据）的某个参量（振幅、频率或相位）为因变量。信号按其自变量时间的取值是否连续，可分为连续信号和离散信号；按其因变量的取值是否连续，又可分为模拟信号和数字信号。

信号具有时域和频域两种最基本的表现形式和特性。时域特性反映信号随时间变化的情况。频域特性不仅含有信号时域中相同的信息量，而且通过对信号的频谱分析，还可以清楚地了解该信号的频谱分布情况及所占有的频带宽度。为了得到所传输的信号对接收设备及信道的要求，只了解信号的时域特性是不够的，还必须知道信号的频谱分布情况。信号的时域特性表示出信号随时间变化的情况。如正弦信号就可以表示为：

$$f(t) = A\ \mathrm{Sin}\ (2\pi ft + \theta)$$

这个正弦信号的振幅为 A，频率为 f，初始相位为 θ。幅度、频率以及相位是周期信号 $f(t)$ 的3个重要特性。信号的频域特性表示出了信号包含的各个频率分量和它们的幅度相位的关系，即信号随频率变化的情况。法国伟大的数学家吉·傅立叶已经证明：任何一个周期为 T 的函数 $f(t)$ 都是由无穷多个正弦函数和余弦函数合成：

$$f(t) = C/2 + \sum_{n=1}^{\infty}(a_n \mathrm{Sin}2\pi nft + b_n \mathrm{Cos}2\pi nft) = \sum_{n=0}^{\infty} A_n \mathrm{Cos}(2\pi nft + \theta_n)$$

其中：

$$a_n = \frac{2}{T}\int_0^T f(t)Sin(2\pi nftdt)$$

$$a_n = \frac{2}{T}\int_0^T f(t)Cos(2\pi nftdt)$$

$$C = \int_0^T f(t)\mathrm{d}t$$

$$A_n = \sqrt{a_n^2 + b_n^2}$$

$$\theta_n = arctg(b_n / a_n)$$

此处 $f = 1/T$ 是基频，a_n 和 b_n 是 n 次正弦谐波和余弦谐波的振幅。

在分析信号 $f(t)$ 的频谱时，只要求出 A_n、θ_n 之值便可确定 $f(t)$ 所对应的频率分量的幅度和相位。我们常把 $f(t)$ 各次谐波的振幅 A_n 按照频率高低依次排列起来所形成的谱状图形称为信号 f(t)的频谱，而信号频谱所覆盖的频率范围称为信号的绝对带宽（bandwidth）。由于信号中的大部分能量

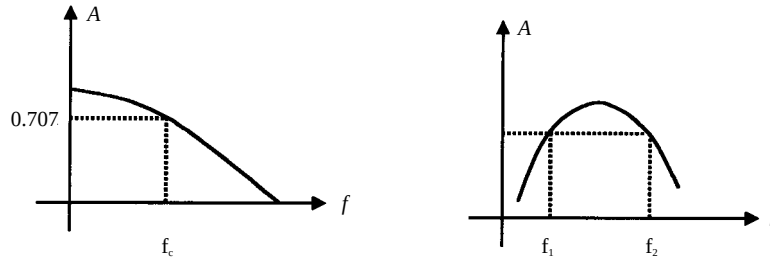
都集中在一个相对较窄的频带范围之内，因此我们将信号大部分能量集中的那段频带称为有效带宽，简称带宽。任何信号都有带宽。一般来说，信号的带宽越大，利用这种信号传送数据的速率就越高，要求传输介质的带宽也越大。下面我们将简单介绍常见信号的频谱和带宽。

声音信号的频谱大致在20 Hz～2000 kHz的范围（低于20 Hz的信号为次声波，高于2000 KHz的信号为超声波），但用一个窄得多的带宽就能产生可接受话音的重现，因而话音信号的标准频谱为300 Hz～3400 Hz，其带宽为3 kHz。电视信号的频谱为0～4 MHz，因此其带宽为4 MHz。作为一个特殊的例子，单稳脉冲信号的带宽为无穷大。而对于二进制信号，其带宽一般依赖于信号波形的确切形状以及0、1的次序。信号的带宽越大，它就越忠实地表示着数字序列。

2.2.2 信道的截止频率与带宽

根据傅立叶级数我们知道，如果一个信号的所有频率分量都能完全不变地通过信道传输到接收端，那么在接收端由这些频率分量叠加起来而形成的信号则和发送端的信号是完全一样的，即接收端完全恢复了发送端发出的信号。但现实世界上，没有任何信道能毫无损耗地通过所有频率分量。如果所有的傅立叶分量都被等量衰减，那么接收端接收到的信号虽然在振幅上有所衰减，但并没有发生畸变。然而所有的传输信道和设备对不同的频率分量的衰减程度是不同的，有些频率分量几乎没有衰减，而有些频率分量被衰减了一些，这就是说，信道也具有一定的振幅频率特性，因而导致输出信号发生畸变。通常情况是频率为 0到fc赫兹范围内的谐波在信道传输过程中不发生衰减（或其衰减是一个非常小的常量），而在此fc频率之上的所有谐波在传输过程中衰减很大，我们把信号在信道传输过程中某个分量的振幅衰减到原来的 0.707（即输出信号的功率降低了一半）时所对应的那个频率称为信道的截止频率（ cut-off frequency）。

截止频率反映了传输介质本身所固有的物理特性。另一些情况下，则是因为人们有意地在线路中安装了滤波器以限制每个用户使用的带宽，如图 2-4a所示。有些时候，由于在信道中加入双通滤波器，因而信道对应着两个截止频率 f1和f2，它们分别被称为下截止频率和上截止频率。而这两个截止频率之差 f2-f1被称作信道的带宽，如图 2-4b所示。



a) 单通滤波器　　b) 双通滤波器

图2-4 信道截止频率

如果输入信号的带宽小于信道的带宽，则输入信号的全部频率分量都能通过信道，因而信道输出端得到的输出波形将是不失真的。但如果输入信号的带宽大于信道的带宽，则信号中某些频率分量就不能通过信道，这样输出得到的信号将与发送端发送的信号有些不同，即产生了失真。为了保证数据传输的正确性，必须限制信号的带宽。

2.2.3 信道的最大数据传输率

单位时间内能传输的二进制位数称为数据传输率。数据传输率的提高意味着每一位所占用的时间的减小，即二进制数字脉冲序列的周期时间会减小，当然脉冲宽度也会减小。

前一节里我们已经知道，即使二进制数字脉冲信号通过带宽有限的理想信道时也会产生波形失真，而且当输入信号的带宽一定时，信道的带宽越小，输出的波形失真就会越大。换个角度说，当信道的带宽一定时，输入信号的带宽越大，输出信号的失真就越大，因此当数据传输率提高到一定程度时（信号带宽增大到一定程度），在信道输出端上的信号接收器根本无法从已失真的输出信号中恢复出所发送的数字序列。这就是说，即使对于理想信道，有限的带宽也限制了信道数据传输率。

早在1924年，H. Nyquist（奈奎斯特）就认识到这个基本限制的存在，并推导出表示无噪声有限带宽信道的最大数据传输率的公式。在1948年，C. Shannon（香农）把奈奎斯特的工作进一步扩展到了信道受到随机噪声干扰的情况。这里我们不加证明地简述这些现在视为经典的结果。

Nyquist证明，任意连续信号$f(t)$通过一个无噪声的带宽为B的信道后，其输出信号为一个带宽为B的时间连续信号$g(t)$。如果要输出数字信号，还必须以一定的速率对$g(t)$进行等间隔的抽样。抽样速度高于每秒$2B$次是无意义的，因为信号中高于信道带宽B以外的高频分量已被信道衰减掉。如果$g(t)$由V个离散化的电平组成，即每次抽样的可能结果为V个离散化电平之一，则该信道的最大的数据传输率R_{max}为：

$$R\max = 2B\log_2 V \text{（比特/秒）}$$

例如，一个无噪声带宽为3000 Hz的信道不能传送速率超过6000比特/秒的二进制数字信号。

前面我们仅仅考虑了无噪声的理想信道。对于有噪声的信道，情况将会迅速变坏。信道中热噪声用信号功率与噪声功率之比来度量，信号功率与噪声功率的比值称为信噪比（Signal-to-Noise Ratio）。如果我们用S表示信号功率，用N表示噪声功率，则信噪比应被表示为S/N。但人们通常不使用信噪比的绝对值，而是使用$10\log_{10}S/N$来表示，单位是分贝（dB）。对于S/N等于10的信道，则称其信噪比为10dB；同样的道理，如果信道的S/N等于100，则称其信噪比为20dB；以此类推。Shannon关于有噪声信道最大数据传输率的结论是：对于带宽为BHz，信噪比为S/N的信道，其最大数据传输率$R\max$为：

$$R\max = B\log_2(1 + S/N) \text{（比特/秒）}$$

例如，对于一个带宽为3 kHz，信噪比为30 dB的信道，无论其使用多少个量化电平，也不管采样速度多快，其数据传输率不可能大于30 000比特/秒。Shannon的结论是根据信息论推导出来的，适用的范围非常广，要想超越这一结论就好比想要发明永动机一样，几乎是不可能的。值得注意的是，Shannon的结论仅仅给出了一个理论极限，而实际上，要接近这个极限也是相当困难的。

2.3 传输介质

传输介质通常分为有线介质（或有界介质）和无线介质（或无界介质）。有线介质将信号约束在一个物理导体之内，如双绞线、同轴电缆和光纤等；而无线介质则不能将信号约束在某个

空间范围之内。

2.3.1 双绞线

双绞线TP（Twisted Pair）是目前使用最广，价格相对便宜的一种传输介质。它是由两条相互绝缘的铜导线组成。其中导线的典型直径为 1mm（在0.4mm至1.4mm之间）。这两条线扭绞在一起，可以减少对邻近线对的电气干扰，因为两条平行的金属线可以构成一个简单的天线，而双绞线则不会。

由若干对双绞线构成的电缆被称为双绞线电缆。双绞线对可以并排放在保护套中。目前双绞线电缆广泛应用于电话系统。几乎所有的电话机都是通过双绞线接到电话局的。在双绞线中传输的信号在几公里的范围内不需放大，但传输距离比较远时就必须使用放大器。

双绞线既可以传输模拟信号，又能传输数字信号。用双绞线传输数字信号时，其数据传输率与电缆的长度有关。距离短时，数据传输率可以高一些。在几公里的范围内，双绞线的数据传输率可达10Mbps，甚至100Mbps，因而可以采用双绞线来构成价格便宜的计算机局域网。

对于双绞线的定义有两个主要来源。一个是 EIA（电子工业协会）的 TIA（远程通信工业分会），即通常所说的EIA/TIA；另一个是IBM。EIA负责“ Cat ”（即“ Category ”）系列非屏蔽双绞线（Unshielded Twisted Pair，UTP）标准。IBM负责“ Type ”系列屏蔽双绞线标准，如IBM：Type 1、Type 2等。严格地说，电缆标准本身并未规定连接双绞线电缆的连接器类型，然而 EIA和IBM都定义了双绞线的专用连接器。对于 Cat3、Cat4和Cat5来说，使用RJ-45（4对8芯），遵循EIA-568标准；而对于Type 1电缆来说，则使用DB9连接器。大多数以太网在安装时使用基于EIA标准的电缆，而大多数 IBM及令牌环网则倾向于使用符合 IBM标准的电缆。下面为 EIA/TIA电缆规格说明：

Cat 1：适用于电话和低速数据通信；

Cat 2：适用于ISDN及T1/E1、支持高达16MHz的数据通信；

Cat 3：适用于10Base-T或100Mbps的100Base-T4、支持高达20MHz的数据通信；

Cat 5：适用于100Mbps的100Base-TX和100Base-T4支持高达100MHz的数据通信。

双绞线的技术和标准都是比较成熟的，价格也比较低廉，而且双绞线电缆的安装也相对容易。但双绞线电缆的最大缺点是对电磁干扰比较敏感；另外，双绞线电缆不能支持非常高速的数据传输。

2.3.2 同轴电缆

另一种常用的传输介质是同轴电缆（Coaxial Cable）。同轴电缆中的材料是共轴的，如图 2-5所示，故同轴之名由此而来。外导体是一个由金属丝编织而成的圆形空管，内导体是圆形的金属芯线。内外导体之间填充着绝缘介质。同轴电缆内芯线的直径一般为 1.2mm至5mm，外管的直径一般为4.4mm至18mm。内芯线和外导体一般都采用铜质材料。同轴电缆可以是单芯的，也可以将多条同轴电缆安排在一起形成同轴电缆。

广泛使用的同轴电缆有两种。一种是阻抗为 50欧姆的基带同轴电缆，另一种是阻抗为 75欧姆的宽带同轴电缆。

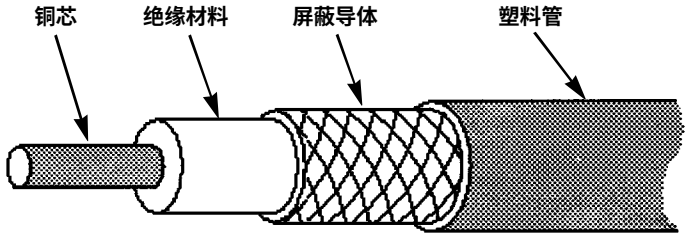


图2-5 同轴电缆

基带同轴电缆主要用于传输数字信号，可以作为计算机局域网的传输介质。基带同轴电缆的带宽取决于电缆长度。1公里电缆可达到10Mbps的数据传输率。电缆增长，其数据传输率将会下降；短电缆可获得较高的数据传输率。

宽带同轴电缆用于传输模拟信号。“宽带”这个词来源于电话业，指比4kHz宽的频带。宽带电缆技术使用标准的闭路电视技术，可以使用的频带高达900MHz；由于使用模拟信号，可传输近100公里，对信号的要求也远没有像对数字信号那样高。

同轴电缆的低频串音及抗干扰性不如双绞线电缆，但当频率升高时，外导体的屏蔽作用加强，同轴电缆所受的外界干扰以及同轴电缆间的串音都将随频率的升高而减小，因而特别适用于高频传输。一般情况下，同轴电缆的上限工作频率为300MHz，有些质量高的同轴电缆其工作频率可达900MHz，因此同轴电缆具有很宽的工作频率范围。当它被用来传输数据时，其数据传输率可达每秒几百兆位。由于同轴电缆具有寿命长、频带宽、质量稳定、外界干扰小、可靠性高、维护便利、技术成熟等优点，而且其费用又介于双绞线与光纤之间，在光纤通信没有大量应用之前，同轴电缆在闭路电视传输系统中一直占主导地位。

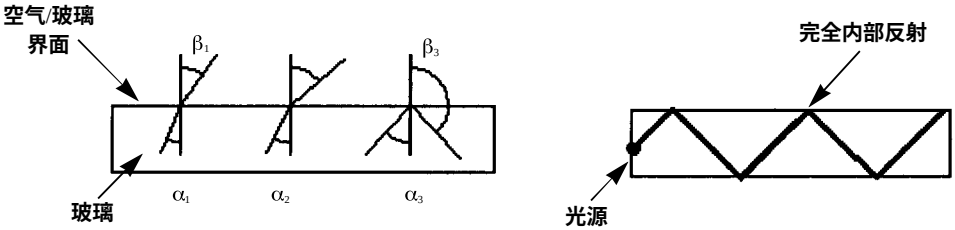
2.3.3 光纤

随着光通信技术的飞速发展，现在人们已经可以利用光导纤维来传输数据。人们用光脉冲的出现表示“1”，不出现表示“0”。由于可见光所处的频段为10^8MHz左右，因而光纤传输系统可以使用的带宽范围极大。事实上，目前为止的光纤传输技术使得人们可以获得超过50 000GHz的带宽，而且今后还可能更高。当前实际使用的10Gbps限制是因为光/电以及电/光信号转换的速度跟不上。在实验室里，短距离可以获得100Gbps的带宽甚至更高。今后将有可能实现完全的光交叉和光互连，即构成全光网络，到那时网络的速度将成千上万倍地增加。

光传输系统由三个部分组成：光纤传输介质、光源和检测器。光纤传输介质是超细玻璃或熔硅纤维。光源是发光二极管（Light Emitting Diode，LED）或激光二极管。这两种二极管在通电时都发出光脉冲。检测器是光电二极管，遇光时，它产生一个电脉冲。在光纤的一端安装一个LED或激光二极管，另一端安装一个光电二极管，我们就有了一个单向的数据传输系统。

实际上，如果不是利用一个有趣的物理原理，光传输系统会由于光纤的漏光而变得没有实际价值。当光线从一种介质穿过另一种介质时，如从玻璃到空气，光线会发生折射，如图2-6a所示。当光线在玻璃上的入射角为α_1时，则在空气中的折射角为β_1。折射量取决于两种介质的折射率。当光线在玻璃上的入射角大于某一临界值时，光线将完全反射回玻璃，而不会漏入空气，

这样，光线将被完全限制在光纤中，而几乎无损耗地传播，如图 2-6b所示。

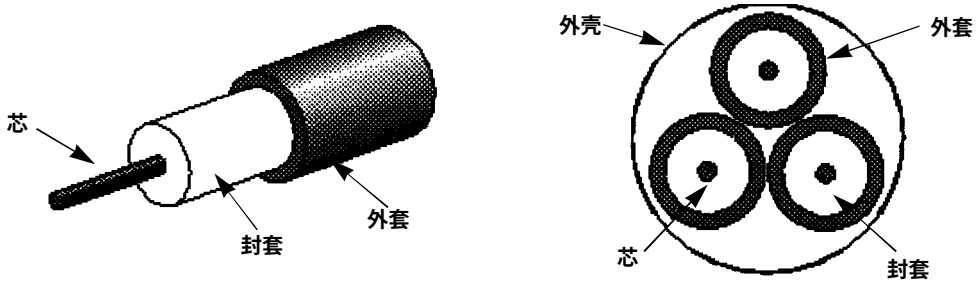


a) 光线以不同的角度从玻璃射入空气　　b) 光线在玻璃内全反射的情况

图2-6　光折射原理

在图2-6b中仅给出了一束光在玻璃内部全反射传播的情况。实际上，任何以大于临界值角度入射的光线，在介质边界都将按全反射的方式在介质内传播，而且不同的光线在介质内部将以不同的反射角传播，我们可以认为每一束光线都有不同的模式。如果纤芯的直径较粗，则光纤中可能有许多种沿不同途径同时传播的模式，我们将具有这种特性的光纤称为多模光纤（ Multi-mode Fiber）；如果将光纤纤芯直径减小到光波波长大小的时候，则光纤如同一个波导，光在光纤中的传播没有反射，而沿直线传播，这样的光纤称为单模光纤（ Single-mode Fiber)。

光纤结构是圆柱形，包含有纤芯和包层，如图 2-7所示。纤芯直径约5~75μm ，包层的外直径约为100～150μm ，最外层的是塑料，对纤芯起保护作用。纤芯材料是二氧化硅掺以锗和磷，包层材料是纯二氧化硅。纤芯的折射率比包层的折射率高 1（左右，这使得光局限在纤芯与包层的界面以内向前传播。



a) 1根光纤的侧面图　　b) 1根光缆(含3根光纤)的剖面图

图2-7　光导纤维

光纤的主要传播特性为损耗和色散。损耗是光信号在光纤中传输时单位长度的衰减，其单位为dB/km。色散是到达接收端的时延差，即脉冲宽度，其单位是 μs/km 。光纤的损耗会影响传输的中继距离，色散会影响数据传输率，两者都很重要。自 1976年以来，人们发现 1.3μm 和 1.55μm 波长的光纤可以获得0.5dB/km至0.2dB/km的衰减率，0.85μm 波长的光纤的衰减为3dB/km，多模光纤能使0.85μm 波长的光纤的色散从 400μm/km 减至10μm/km 以下。在1.3μm 的波长中，单模光纤的色散近于零，所以单模光纤在使用时，可以同时兼得低损耗和低色散两项优点，无中继的距离可达50～100km，数据传输率可达2Gbps以上。

单模光纤很昂贵，且需要激光光源，但其传输距离非常远，且能获得非常高的数据传输率。

目前在实际中用到的光纤系统能以2.4Gbps的速率传输100km，而且不需要中继。而在实验室里，则可以获得更高的数据传输率。而多模光纤相对来说传播距离要短些，而且数据传输率要小于单模光纤；但多模光纤的优点在于价格便宜，并且可以用发光二极管作为光源。单模光纤与多模光纤的比较如表2-1所示。

光纤支持的十分高的带宽，因为它们仅仅受光的高频光子特性的限制，而不受电信号的低频特性限制。光纤通信的优点是频带宽、传输容量大、重量轻、尺寸小、不受电磁干扰和静电干扰、无串音干扰、保密性强、原料丰富、生产成本低。因而，由多条光纤构成的光缆已成为当前主要发展的传输介质。

表2-1 单模光纤与多模光纤的比较

项 目	单模光纤	多模光纤
距离	长	短
数据传输率	高	低
光源	激光	发光二极管
信号衰减	小	大
端接	较难	较易
造价	高	低

2.3.4 无线介质

信息时代的人们对信息的需求是无止境的。很多人需要随时与社会或单位保持在线连接，对于这些移动用户，双绞线、同轴电缆和光纤都无法满足他们的要求。他们需要利用笔记本计算机、掌上型计算机随时随地获取信息，而无线介质可以帮助解决上述问题。

无线介质是指信号通过空气传输，信号不能被约束在一个物理导体内。无线介质实际上就是无线传输系统，主要包括无线电、微波和卫星通信等。

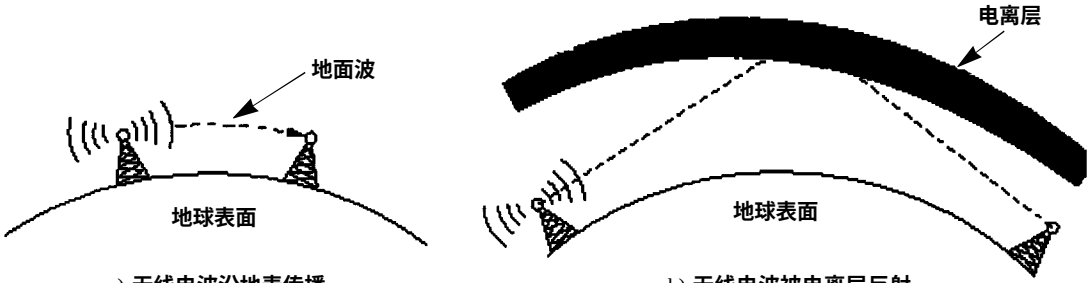
大气中的电离层是具有离子和自由电子的导电层，无线通信就是利用地面发射的无线电波通过电离层的反射，或电离层与地面的多次反射而到达接收端的一种远距离通信方式，如图2-8所示。无线通信使用的频率一般在3MHz至1GHz。电离层的高度在地面以上数十公里至百公里，可分为各种不同的层次，并随季节、昼夜以及太阳活动的情况而发生变化。由于电离层的不稳定性，因而无线通信与其他通信方式相比，在质量上存在不稳定性。

无线电波被广泛应用于通信的原因是它传播距离可以很远，也很容易穿过建筑物。而且无线电波是全方向传播的，因此无线电波的发射和接收装置不必要求精确对准。

无线电波的传播特性与频率有关。在低频上，无线电波能轻易地绕过一般障碍物，但其能量随着传播距离的增大而急剧递减。在高频上，无线电波趋于直线传播并易受障碍物的阻挡，还会被雨水吸收。而对于所有频率的无线电波，都很容易受到其他电子设备的各种电磁干扰。

中、低频无线电波（频率在1MHz以下）沿着地球表面传播，如图2-8a所示。在这些波段上的无线电波很容易穿过一般建筑物。用中、低频无线电波进行数据通信的主要问题是它们的通信带宽较低。

高频和甚高频（频率在1MHz～1GHz之间）无线电波将被地球表面吸收，但是到达离地球表面大约100km～500km高度的带电粒子层的无线电波将被反射回地球表面，如图2-8b所示。我们可以利用无线电波的这种特性来进行数据通信。



a) 无线电波沿地表传播　　b) 无线电波被电离层反射

图2-8　无线电波的传播

对于频率在100MHz以上的无线电波，其能量将集中于一点并沿直线传播，这就是微波。我们可以通过抛物状天线将微波的能量集中于一小束，从而获得极高的信噪比。微波通信是利用无线电波在对流层的视距范围内进行信息传输的一种通信方式。它使用的频率范围一般在1 GHz至20GHz左右。在长途线路上，其典型的工作频率为2 GHz、4 GHz、8 GHz和12 GHz。

由于微波只能沿直线传播，所以微波的发射天线和接收天线必须精确对准。而且如果两个微波塔相距太远，一方面地球表面就会挡住去路，另一方面，微波长距离传送会发生衰减，因此每隔一段距离就需要一个中继站。中继站之间的距离与微波塔的高度成正比例。由于受地形和天线高度的限制，两个中继的之间的距离一般为30km～50km。而对于100m高的微波塔，中继站之间的距离可以达到80km。

微波通信按所提供的传输信道可分为模拟和数字两种类型，分别简称为“模拟微波”与“数字微波”。目前，模拟微波通信主要采用频分多路复用技术和频移键控调制方式，其传输容量可达30～6000个电话信道。数字微波通信发展较晚，目前大都采用时分多路复用技术和相移键控调制方式。和数字电话一样，数字微波的每个话路的数据传输率为64kbps，基群速率为2.048Mbps，二次群的速率为8.448Mbps，三次群的速率为34.368Mbps等。无论是对于模拟微波还是数字微波，都可以利用其中的一个话路或一个群路来传输数字信号，利用模拟微波的一个话路来传输数字信号时，其数据传输率可达9600bps；而利用数字微波的一个话路传输数字信号时，其数据传输率为64Kbps。若利用数字微波的一个群路来传输数字信号时，我们可以得到更高的数据传输率。

微波通信在传输质量上比较稳定。但微波在雨雪天气时会被吸收，从而造成损耗。与同轴电缆相比，由于微波通信的中继站数目比同轴电缆的增音站数目（在同轴电缆系统中，增音站间距为几公里）少得多，而且不需要铺设电缆，所以其成本低得多，在当前的长途通信方面是一种十分重要的手段。微波通信的缺点是保密性不如电缆和光缆好，对于保密性要求比较高的应用场合需要另外采取加密措施。目前数字微波通信被大量运用于计算机之间的数据通信。

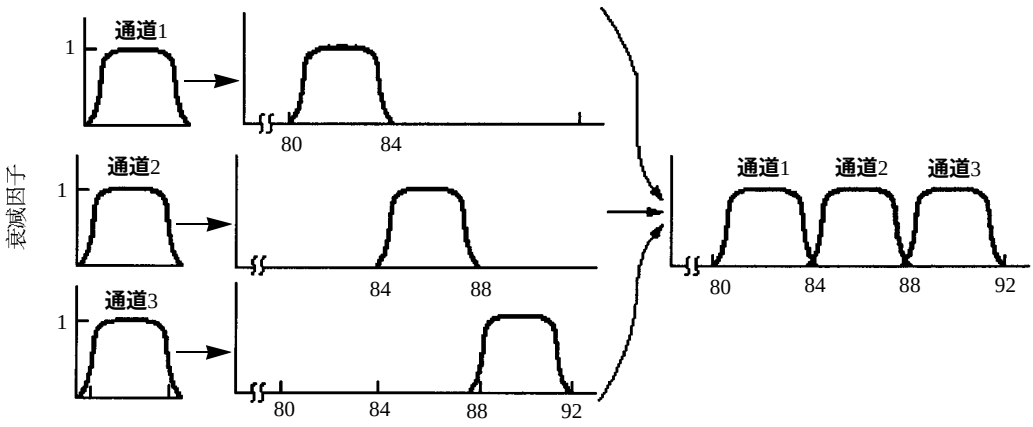
2.4 多路复用

在同一介质上，同时传输多个有限带宽信号的方法，被称为多路复用（Multiplexing）。当前主要采用的多路复用方式有两种：频分多路复用（Frequency Division Multiplexing，FDM）和时分多路复用（Time Division Multiplexing，TDM），下面我们分别加以阐述。

2.4.1 频分多路复用

任何信号只占据一个宽度有限的频率，而信道可以被利用的频率比一个信号的频率宽得多，因而可以利用频率分隔的方式来实现多路复用。

频分多路复用是利用频率变换或调制的方法，将若干路信号搬移到频谱的不同位置，相邻两路的频谱之间留有一定的频率间隔，这样排列起来的信号就形成了一个频分多路复用信号。它将被发送设备发送出去，传输到接收端以后，利用接收滤波器再把各路信号区分开来。这种方法起源于电话系统，我们就利用电话系统这个例子来说明频分多路复用的原理。现在一路电话的标准频带是0.3KHz至3.4KHz，高于3.4KHz和低于0.3KHz的频率分量都将被衰减掉（这对于语音清晰度和自然度的影响都很小，不会令人不满意）。所有电话信号的频带本来都是一样的，即0.3~3.4KHz。若在一对导线上传输若干路这样的电话信号，接收端将无法把它们分开。若利用频率变换，将三路电话信号搬到频段的不同位置，如图 2-9所示这样，就形成了一个带宽为



a) 调频前　　b) 调频后　　c) 多路复用后

图2-9 频分多路复用的电话系统

12KHz的频分多路复用信号。图中一路电话信号共占有 4KHz的带宽。由于每路电话信号占有不同的频带。到达接收端后，就可以将各路电话信号用滤波器区分开。由此可见，信道的带宽越大，容纳的电话路数就会越多。随着通信信道质量的提高，在一个信道上同时传送的电话路数会越来越多。目前，在一根同轴电缆上已实现了上千路电话信号的传输。多路频分复用系统又称为多路载波系统。按照 CCITT的建议，每 12个电话话路构成一个基群（ Group），占用60~108KHz的频带；每5个基群在一起构成一个 60路的超群（Super-Group），占用312~552KHz

的频带；5个超群构成一个300路的主群（Master-Group），占用812～2044KHz的频带；3个主群构成一个900路的超主群（Super-Mastergroup ），占用8516～12 388KHz的频带；4个超主群构成一个3600路的巨群（Giant-Group），占用42612～59 684KHz的频带。在实现多路载波系统时，需逐级实现频率升高，由低次群组成高次群。

在目前的有线或无线模拟通信网中，使用了大量频分多路复用载波系统，因此频分模拟话路也是当前主要的长距离数据传输信道，每个话路最高数据传输率可达 56Kbps。

2.4.2 波分多路复用

在光纤信道上使用的频分多路复用的一个变种就是波分多路复用（ Wave-length Division Multiplexing，WDM）。图2-10即是一种在光纤上获得WDM的简单方法。在这种方法中，两根光纤连到一个棱柱或衍射光栅，每根光纤里的光波处于不同的波段上，这样两束光通过棱柱或衍射光栅合到一根共享的光纤上，到达目的地后，再将两束光分解开来。

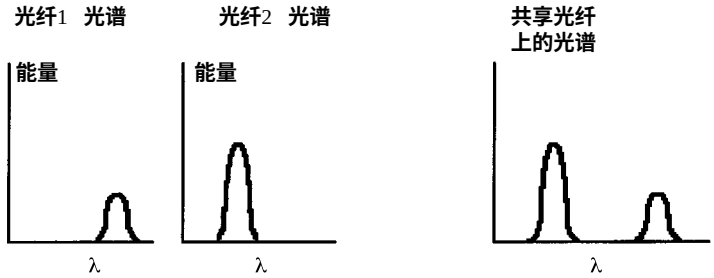


图2-10 波分多路复用

波分多路复用技术并没有什么新鲜的东西。与 FDM的唯一区别就是：在WDM中使用的衍射光栅是无源的，因此可靠性非常高。

由于受到目前电/光和光/电转换的速度的限制，因此对于带宽可达 25 000GHz的光纤来说，目前一般可以利用的数据传输率可达 10Gbps。如采用波分多路复用技术，在一根光纤上可以发送8个波长的光波，假设每个波长可以支持 10Gbps的数据传输率，则一根光纤所能支持的最大数据传输率将达到80Gbps。目前，这样的波分复用系统已经在实际组网中得到应用。

2.4.3 时分多路复用

我们知道，对于一个带宽为 B的模拟信号，只需每秒等间隔地传输 $2B$个采样点，接收方就可以根据接收到的数字信号完全恢复出原始的模拟信号。当传输某路模拟信号的采样数据时，整个信道的频带都将被该路信号所占用。如果信道的带宽很宽，则该信道所能支持的数据传输率就可以很高。在采样间隔时间里，传输一个采样数据的时间仅占采样间隔时间的一部分。则其他时间可以被用来传输其他模拟信号的采样数据，或传输其他低速数据。这就是时分多路复用的基本原理。时分复用是利用时间分隔方式来实现多路复用的，对于数字通信系统主干网的复用都采用时分多路复用技术。

我们以电话系统作为例子来说明时分多路复用的工作原理。对于带宽为 4kHz的电话信号，

每秒采样8000次就可以完全不失真地恢复出话音信号。这种技术被称为脉冲编码调制（ Pulse Code Modulation，PCM）。假设每个采样点的值用8位二进制数来表示，因此一路电话所需要的数据传输率为8×8000＝64Kbps。如果有24路电话，即在每个采样周期（125微秒）中要传输24个采样值。首先是第1路电话的8位采样值，然后是第2路电话的8位采样值…直至第24路电话的8位采样值，最后加上1位用于区分或同步每一次的采样间隔，这样在一个采样周期中主干线路要传输193位二进制数据，即要求主干线路的数据传输率达到 193bits/125μs=1.544Mbps 。因此我们可以利用了一条数据传输率为 1.544Mbps的信道同时传输24路电话，如图2-11所示，这种24路电话复用一条1.544Mbps主干线路被称为T1标准。

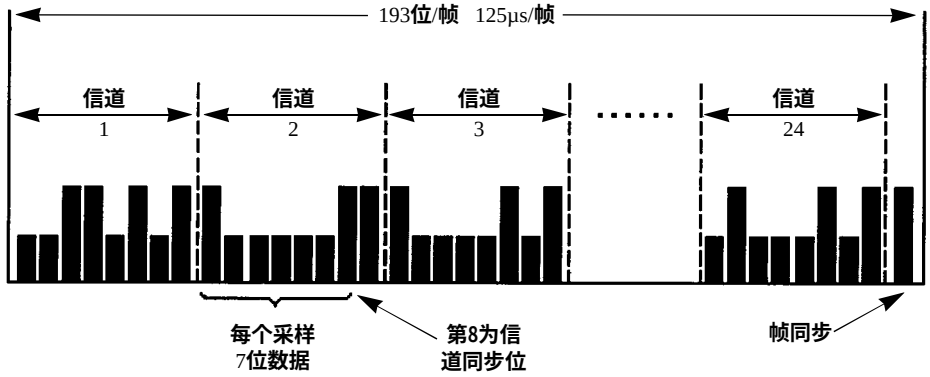


图2-11 数字电话系统的基群采样周期（下线路）

时分多路复用允许多个T1线路复用到更高级的线路上，如图 2-12所示。在图2-12中，4个T1信道被复用到T2线路上。在T2及更高级的线路上的多路复用是按比特进行的，而不是构成 T1帧的24个话音信道的字节。 4个1.544Mbps的T1信道按理应复用成6.176Mbps的速率，而T2线路的实际速率是6.312Mbps。额外的比特主要是用于帧定界和时钟同步。同理， 6个T2流按比特复用成T3线路；而7个T3流复用成T4线路。每一次向上的复用都要附带一些开销用于帧定界和时钟同步。

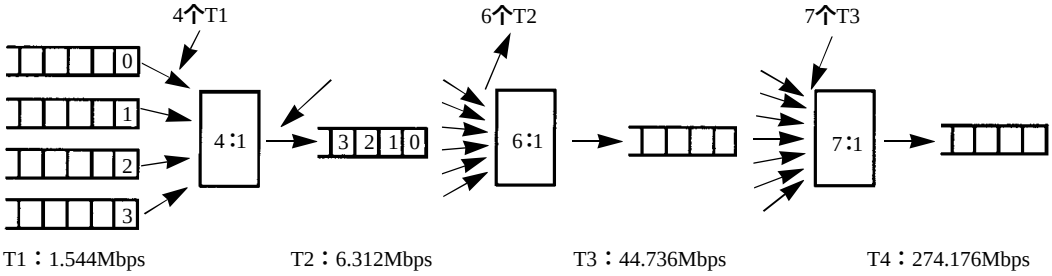


图2-12 在更高级的线路上多路复用的T1流

正如美国和其他国家在基本传输线路上不一致一样，在美国使用的时分多路复用标准是 E1，即30路电话复用一条2.048Mbps的E1线路。在E1标准中，以30路PCM电话为一个基群（即E1，数据传输率为2.048Mbps），4个基群组成120路的二次群（即E2，数据传输率为8.448Mbps），4

个二次群汇成480路的三次群（即E3，数据传输率为34.368Mbps），4个三次群又组成1920路的四次群（即E4，数据传输率为139.246Mbps）。

时分复用数字通信系统和频分复用多路载波系统相比，存在着许多优越性，这些优越性都是由于数字通信的特点所带来的。

2.5 数据交换技术

对于广域网一般都采用点到点信道，而点到点信道使用存储转发的方式传送数据，也就是说从源结点到目的结点的数据通信需要经过若干个中间结点的转接。这涉及到数据交换技术。数据交换技术主要有三种类型：电路交换、报文交换和分组交换。

2.5.1 电路交换

交换的概念最早来自于电话系统。当用户进行拨号时，电话系统中的交换机（telephone switch）在呼叫者的电话与接收者的电话之间建立了一条实际的物理线路（这条物理线路可能包括双绞线、同轴电缆、光纤或无线电在内的各种介质，或是经过多路复用得到的带宽），通话便建立起来，此后两端的电话拥有该专用线路，直到通话结束。这里所谓的交换体现在电话交换机内部。当交换机从一条输入线上接到呼叫请求时，它首先根据被呼叫者的电话号码寻找一条合适的输出线，然后通过硬件开关（比如继电器）将二者连通。假如一次电话呼叫要经过若干交换机，则所有的交换机都要完成同样的工作。电话系统的交换方式叫做电路交换（circuit switching）技术。在电路交换网中，一旦一次通话建立，在两部电话之间就有一条物理通路存在，直到这次通话结束，然后拆除物理通路。

电路交换技术有两大优点，第一是传输延迟小，唯一的延迟是物理信号的传播延迟；第二是一旦线路建立，便不会发生冲突。第一个优点得益于一旦建立物理连接，便不再需要交换开销；第二个优点来自于独享物理线路。

电路交换的缺点首先是建立物理线路所需的时间比较长。在数据开始传输之前，呼叫信号必须经过若干个交换机，得到各交换机的认可，并最终传到被呼叫方。这个过程常常需要10秒甚至更长的时间（呼叫市内电话、国内长途和国际长途，需要的时间是不同的）。对于许多应用（如商店信用卡确认）来说，过长的电路建立时间是不合适的。

在电路交换系统中，物理线路的带宽是预先分配好的。对于已经预先分配好的线路，即使通信双方都没有数据要交换，线路带宽也不能为其他用户所使用，从而造成带宽的浪费。当然，这种浪费也有好处，对于占用信道的用户来说，其可靠性和实时响应能力都得到保证。

2.5.2 报文交换

报文交换（message switching）又称为包交换。报文交换不事先建立物理电路，当发送方有数据要发送时，它将把要发送的数据当做一个整体交给中间交换设备，中间交换设备先将报文存储起来，然后选择一条合适的空闲输出线将数据转发给下一个交换设备，如此循环往复直至将数据发送到目的结点。采用这种技术的网络就是存储转发网络，正如第1章中所提到的那样。电报系统使用的是报文交换技术。

在报文交换中，一般不限制报文的大小，这就要求各个中间结点必须使用磁盘等外设来缓存较大的数据块。同时某一块数据可能会长时间占用线路，导致报文在中间结点的延迟非常大（一个报文在每个结点的延迟时间等于接收整个报文的时间加上报文在结点等待输出线路所需的排队延迟时间），这使得报文交换不适合交互式数据通信。为了解决上述问题又引入了分组交换技术。

2.5.3　分组交换

分组交换（packet switching）技术是报文交换技术的改进。在分组交换网中，用户的数据被划分成一个个分组（packet），而且分组的大小有严格的上限，这样使得分组可以被缓存在交换设备的内存而不是磁盘中。同时由于分组交换网能够保证任何用户都不能长时间独占某传输线路，因而它非常适合于交互式通信。电路交换技术、报文交换技术和分组交换技术的比较如图2-13所示。

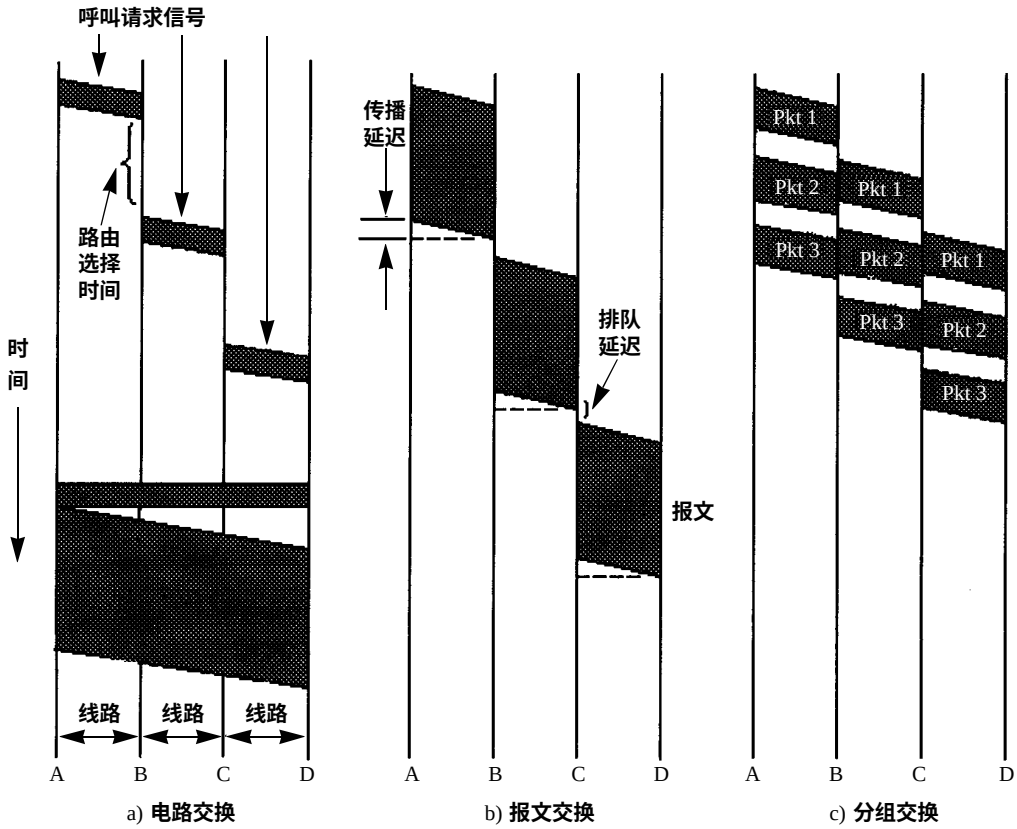


图2-13　电路交换、报文交换和分组交换比较

图2-13说明了分组交换比报文交换优越的情况：在具有多个分组的报文中，中间交换机在接收第二个分组之前，就可以转发已经接收到的第一个分组，即各个分组可以同时在各个结点对之间传送，这样减少了传输延迟，提高了网络的吞吐量。

分组交换除吞吐量较高外，还提供一定程度的差错检测和代码转换能力。由于这些原因，计算机网络常常使用分组交换技术，偶尔才使用电路交换技术，但决不会使用报文交换技术。当然分组交换也有许多问题，比如拥塞、报文分片和重组等。对这些问题的不同处理方法将导致分组交换的两种不同实现，对此我们将在后面的章节作深入讨论。

电路交换和分组交换技术有许多不同之处。关键之处在于电路交换中信道带宽是静态分配的，而分组交换中信道带宽是动态分配和释放的。在电路交换中已分配的信道带宽未使用时都被浪费掉。而在分组交换中，这些未使用的信道带宽可以被其他分组所利用，因为信道不是为某对结点所专用的，从而使信道的利用率非常高（相对来说每个用户信道的费用就可以降低）。但是，正是因为信道不是专用的，突发的输入数据可能会耗尽交换设备的存储空间，造成分组丢失。

另一个不同之处是电路交换是完全透明的。发送方和接收方可以使用任何速率（当然是在物理线路支持的范围内）、任意帧格式来进行数据通信。而在分组交换中，发送方和接收方必须按一定的数据速率和帧格式进行通信。

电路交换和分组交换的最后一个区别是计费方法的不同。它们所采用的技术决定了它们的计费方法是不同的。在电路交换中，通信费用取决于通话时间和距离，而与通话量无关，原因是在电路交换中，通信双方是独占信道带宽的。而在分组交换中，通信费用主要按通信流量（如字节数）来计算，适当考虑通话时间和距离。因特网电话（Internet phone）就是使用分组交换技术的一种新型电话，它的通话费远远低于传统电话，原因就在这里。

2.6 调制解调器

早在计算机网络出现之前，采用模拟传输技术的电话网就已经工作了近一个世纪。尽管我们都知道数字传输技术优于模拟传输技术，而且也意识到数字通信网是今后的发展方向，但谁也不会轻易丢弃现有的规模庞大且仍能继续工作的模拟通信网。下面我们将讨论如何在传统的模拟电话网上传输计算机的二进制数据。

因为基带信号含有大量的低频信号，甚至还含有直流分量，所以它往往不通过电话线路传输（话音通路频带范围一般为 300～3400Hz）。因此要利用电话线路传输数字信号，必须采取措施把数据信号调制到电话线路的频带范围内。

数字信号的调制实际上是用基带信号对载波波形的三个参数进行控制，使这些参数随基带脉冲信号的变化而变化。完成上述功能的设备就称为调制解调器 Modem。

2.6.1 调制方式

根据调制参数的不同，其调制方式可分为幅移键控法（Amplitude-Shift Keying，ASK）、频移键控法（Frequency-Shift Keying，FSK）和相移键控法（Phase-Shift Keying，PSK）三类，我们经常把它们简称为调幅（Amplitude Modulation，AM）、调频（Frequency Modulation，FM）和调相（Phase Modulation，PM）。

所谓调幅方式就是用基带信号来控制载波的振幅变化。同样的道理，调频方式就是用用基带信号来控制载波的频率变化；调相就是用基带信号来控制载波的相位变化，如图 2-14所示。

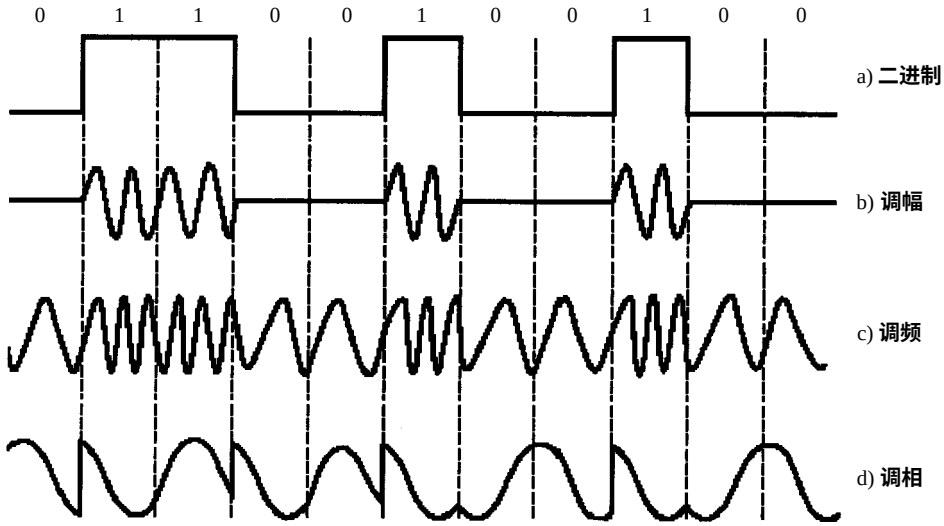


图2-14 Modem的调制方式

在图2-14中，一个载波只能调制一位二进制数，因此 Modem所能支持的数据传输率与其载波的波特率是一样的，也就是说，对于载波频率为 2400波特的Modem，其所能支持的最大数据传输率为2400bps。

为了让Modem支持更高的数据传输率，必须采用新的调制方式。其中最常用的方法是让每波特的载波携带多位二进制数，也就是说，用多位二进制编码来控制改变 Modem载波的多个参量，例如同时改变载波的振幅和相位。我们将这种调制方式称为正交幅度调制（ Quadrature Amplitude Modulation，QAM）。

每种调制解调器有各自不同的调制方式，以支持不同的数据传输率。 Modem的调制方式和数据传输率大多数由国际电信联盟（ ITU）进行标准化，如ITU V.32标准支持9.6Kbps数据传输率。支持14.4Kbps数据传输率的调制解调器的标准为 V.32bis，即V.32规范的扩展形式。 V.32bis规范后面是数据传输率为 28.8Kbps的V.34标准以及支持33.6Kbps的V.42标准。上述这些 Modem标准都是通过在 2400波特的电话线路上每波特传输多位二进制数来实现的。而支持 56Kbps的V.90标准的实现机制则完全不一样，有兴趣的读者可以参考其他资料。

2.6.2 Modem标准

Modem标准规定了Modem所采用的调制方式以及所支持的数据传输率，如前面提到的 V.32、V.32bis、V.34以及V.90等。

另外，为了提高Modem的传输速度和有效数据传输率，目前许多 Modem都采用数据压缩和差错控制技术。数据压缩指的是发送端的 Modem在发送数据以前先将数据进行压缩，而接收端的Modem收到数据后再把数据还原，从而提高了 Modem的有效传输速率。通常使用的压缩技术有两种，CCITT规范和Microcom网络协议（Microcom Networking Protocol，MNP）。CCITT规范，即CCITT V.42bis规范，使用Huffman（霍夫曼）编码技术，将传输数据中频繁出现的字符

用4位表示，很少出现的字符用11位表示，从而达到压缩目的。Huffman压缩技术非常适合于压缩文本数据文件。MNP有几种压缩编码方式。MNP 5级使用运行长度编码，它利用回车、换行和空格等非打印字符在内的一串重复字符容易识别这一特点，在一行中发现有3个以上相同字符时则发送该字符及重复个数，从而达到压缩目的。对于图表文件，使用这种协议达到的压缩比很高。MNP 7级又根据字符对的频率编码字符，进一步提高压缩能力。MNP 5级可以实现2：1的压缩比，MNP 7级的压缩比可以达到3：1。

然而对于高速Modem，线路中的瞬间噪声可使Modem产生多位错误。因此必须采用差错控制技术，制定相应的标准。常用的差错控制标准有两种。其中使用最广泛的标准是Microcom的网络协议MNP。MNP是一组独立的差错控制和数据压缩标准。前面提到的MNP 5级和MNP 7级定义数据压缩技术。MNP1～4级以及MNP 10级描述差错控制技术。使用MNP 4级差错控制标准的Modem已得到广泛应用，并且成为2400bps调制解调器的工业标准。MNP 10级是功能非常齐全的差错控制协议，可用于像蜂窝电话这样的噪声环境。另一种差错控制标准是CCITT的V.42。V.42把MNP 4级作为选项。如果某个Modem应答时不支持V.42标准，则可用MNP 4级方式，从而做到兼容。使用CCITT V.42和MNP 4级协议的Modem可以协商传输速率。如果通信线路在某个速率条件下连续出错次数超过一个设定值，则通信双方的Modem降低速度，直到可以正常传输数据为止。

2.6.3 Modem分类

Modem有各种各样的分类方法，下面我们简单讨论其中几种有代表性的分类方法。

如按通信设备对Modem进行分类，可将Modem分为拨号Modem和专线Modem。拨号Modem主要用于公用电话网上传输数据。拨号Modem具有在性能指标较低的环境中进行有效操作的特殊性能。多数拨号Modem具备自动拨号、自动应答、自动建立连接和自动拆线等功能。专线Modem主要用在专用线路或租用线路上，它不必带有自动应答和自动拆线功能。专线Modem的数据传输率比拨号Modem要高。

如按数据传输方式进行分类，可将Modem分为同步Modem和异步Modem。同步Modem能够按同步方式进行数据算术，它的速率较高；一般用在主机到主机的通信上。同步Modem需要同步电路，故设备复杂、造价昂贵。异步Modem是指能随机地以突发方式进行数据传输的Modem，它所传输的数据以字符为单位，用起始位和停止位表示一个字符的起止。异步Modem主要用于终端到主机或其他低速通信的场合，故它的电路简单、造价低廉。目前市场上的许多Modem支持两种数据传输方式。

如按通信方式对Modem进行分类，可分为单工、半双工和全双工三种。单工Modem只能接收或发送数据。半双工Modem可收可发，但不能同时接收和发送数据。全双工Modem则可同时接收和发送数据。在这三类Modem中，只支持单工方式的Modem很少，而大多数Modem都支持半双工和全双工方式。全双工工作方式比半双工工作方式的优越之处在于，它不需要线路换向时间，因此响应速度快、延迟小。全双工的缺点是双向传输数据时需要占用共享线路的带宽，故设备复杂、价格昂贵；相对来说，支持半双工方式的Modem具有设备简单、造价低的优点。

对于某些应用来说，半双工可能比全双工更合适。目前市场上的许多 Modem既支持半双工传输又支持全双工传输。

另外，按传输速率进行分类，可将 Modem分为低速、中速和高速。最后，按 Modem支持的物理接口的不同，又可将其分为支持 RS-232-C接口、RS-449接口、RS-530接口、V.35接口以及X.21接口等物理接口。

2.6.4 工作模式

调制解调器有两种工作模式，一是命令模式，一是数据模式。正常工作时， Modem总处于这两种模式之一。命令模式（ command mode），也称本地模式（ local mode）或终端模式（terminal mode）。在命令模式中运行的Modem，对用户送到Modem上的任何信息都作为命令来解释。数据模式（data mode），也称联机模式（online mode）。在这种模式中运行的Modem，对用户给它的任何信息都作为数据来解释。从数据模式切换到命令模式，使用转义序列“ +++ ”，从命令模式切换到数据模式时，使用“ AT0 ”命令。

2.7 小结

信号是消息（或数据）的一种电磁编码，信号中包含了所要传递的消息。信号按其因变量的取值是否连续，可分为模拟信号和数字信号，相应的也可将通信分为模拟通信和数字通信。

傅立叶已经证明：任何信号（不管是模拟信号还是数字信号）都是由各种不同频率的谐波组成的，任何信号都有相应的带宽。而且任何信道在传输信号时都会对信号产生衰减，因此，任何信道在传输信号时都存在一个数据传输率的限制，这就是奎 Nyquist（奈奎斯特）定理和Shannon（香农）定理所要告诉我们的结论。

传输介质是计算机网络与通信的最基本的组成部分，它在整个计算机网络的成本中占有很大的比重。为了提高传输介质的利用率，我们可以使用多路复用技术。多路复用技术有频分多路复用、波分多路复用和时分多路复用三种，它们用在不同的场合。

数据交换技术包括电路交换、报文交换和分组交换三种，它们各自有优缺点。

Modem是用于在模拟电话网上传输计算机的二进制数据的设备。 Modem的调制方式有调幅、调频、调相以及正交幅度调制，而且 Modem还支持数据压缩和差错控制。

习题

1. 请简单比较一下模拟通信系统和数字通信系统和组成和特点。
2. 数字通信系统具有哪些优点？它的主要缺点是什么？
3. 对于带宽为6MHz的电视信道，如果使用量化等级为 4的数字信号传输，则其数据传输率是多少？假设信道是无噪声的。
4. 对于带宽为3kHz、信噪比为20dB的信道，当其用于发送二进制信号时，它的最大数据传输率是多少？
5. 一个每秒钟采样一次的4kHz无噪声信道的最大数据传输率是多少？

6. 比较一下各种传输介质的优缺点。
7. 在50kHz的线路上要传输T1载波（1.544Mbps）需要多大的信噪比？
8. 为什么PCM采样时间为125μs ？
9. 对于无噪声的4kHz信道，比较使用下列方案所能达到的最大数据传输率：
   (1) 每次采样2比特；
   (2) T1 PCM系统。
10. 比较频分多路复用和时分多路复用的异同点。
11. 比较电路交换、报文交换和分组交换三种交换技术的工作原理和性能特点。
12. Modem的功能是什么？它有哪几种调制方式？

第3章　物理层接口

物理层接口主要涉及各种传输介质或传输设备的接口。由于传输介质和传输设备的种类繁多，因此物理层接口的标准也非常多。本章主要介绍 RS-232-C、RS-449等物理层接口。

3.1　RS-232-C接口

RS-232-C是美国电子工业协会（Electrical Industrial Association，EIA）于1973年提出的串行通信接口标准，主要用于模拟信道传输数字信号的场合。　RS-232-C是用于数字终端设备（Data Terminal Equipment，DTE）与数字电路端接设备（Data Circuit-terminating Equipment，DCE）之间的接口标准。RS-232-C与CCITT 的V.28建议很相近。RS-232-C接口标准所定义的内容属于国际标准化组织ISO所制订的开放式系统互联（OSI）7层参考模型中的最低层 —— 物理层所定义的内容。RS-232-C接口规范的内容包括机械特性、电气特性、功能特性和过程特性四个方面。现分别介绍如下：

3.1.1　机械特性

RS-232-C接口规范并没有对机械接口作出严格规定。RS-232-C的机械接口一般有9针、15针和25针3种类型。标准的RS-232-C接口使用25针的DB连接器（插头、插座）。RS-232-C在DTE设备上用作接口时一般采用 DB25M插头（针式）结构，插头两个螺钉中心距离为 47.040.13mm；而在DCE（如Modem）设备上用作接口时采用 DB25F插座（孔式）结构。特别要注意的是，在针式结构和孔式结构的插头插座中引脚号的排列顺序（顶视）是不同的，使用时要务必小心。

3.1.2　电气特性

DTE/DCE接口标准的电气特性主要规定了发送端驱动器与接收端驱动器的信号电平、负载容限、传输速率及传输距离。RS-232-C接口使用负逻辑，即逻辑“ 1 ”用负电平（范围为-5～-15V）表示，逻辑“ 0 ”用正电平（范围为+5～+15V）表示，-3～+3V为过渡区，逻辑状态不确定（实际上这一区域电平在应用中是禁止使用的），如图3-1所示。RS-232-C的噪声容限是2V。

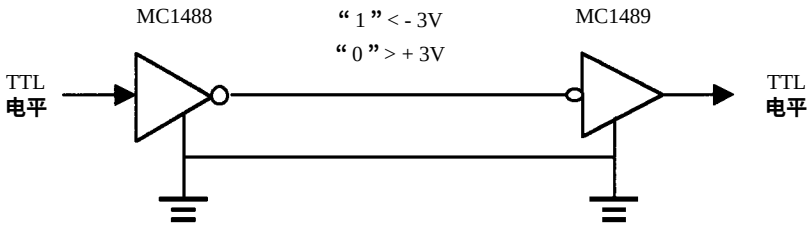


图3-1　RS-232-C接口电路

根据RS-232-C的电气特性可知，RS-232-C接口电平与TTL电平（TTL电平的逻辑“ 1 ”是

2.4V，逻辑“0”是0.4V）不兼容，所以要外加电路实现电平转换。目前可用已有的集成电路电平转换器来进行电平转换。MC1488发送器输入TTL电平，产生RS-232-C输出电平，它的电源一般取12V，输出为9V左右。MC1489接收器使用标准5V电源，输入为RS-232-C电平，输出为TTL电平，该接收器具有1V噪声保护功能。

RS-232-C的电气特性有一些不足之处，首先是参考地（信号地）问题。发送端和接收端是对信号地测量的，信号地与逻辑地连接在一起，但发送端和接收端的逻辑地可能不一致，使信号地中有地电流。而导线是有电阻的，所以导线的两端存在电压降，当发送器对接口电路施加电压时，这个电压降会使接收器收到的电压与没有电位差时收到的电压不同。为尽量减少地电位对信号的影响，RS-232-C接口使用较高的传送电压。

另一个电气问题是电缆电容。EIA标准规定在数据传输率为20kbps时，被驱动电路的电容（包括所连电缆电容）必须小于2500pf。对于一个多芯电缆来说，每英尺40～50pf电容是很平常的，所以满足电容特性的电缆长度为50英尺（15.24m）。因此RS-232-C标准中规定在数据传输率为20Kbps时，RS-232-C传输电缆的长度不能超过50英尺（15.24m）。实际上可以正常工作的电缆长度远远大于给出的限制，但由于电缆电容、时钟频率变化、噪声干扰和地电位差的影响，会使工作不可靠，所以电缆长度只能限制为不能超过50英尺。当数据传输率较低时，可以适当增加电缆长度。如数据传输率为1200bps时，电缆长度可达3000英尺[⊖]；当数据传输率为9600bps时，传输电缆长度为200英尺。

CCITT V.24接口的电气特性由CCITT V.28给出，V.24的电气特性和RS-232-C的相同。

3.1.3 功能特性

RS-232-C接口连线的功能特性，主要是对接口各引脚的功能和连接关系作出定义。RS-232-C接口规定了21条信号线和25芯的连接器，其中最常用的是引脚号为1～8、20这9条信号线。表3-1列出了接口电路的名称和方向。在表的左侧还标出了25芯连接器的脚号，其中9、10脚为测试保留，11、25脚未指定。RS-232-C接口在不同的应用场合所用到的信号线是不同的。例如，在异步传输时，不需要定时信号线；在非交换应用中则不需要某些控制信号；在不使用备用信道操作时，则可省去5个反向信号线。

表3-1 RS-232-C接口电路

25芯连接器引脚号	接口电路名称	信号方向DTE DCE		数据	控制	定时	地线
1	屏蔽地	PG	——				√
7	信号地	GND	——				√
2	发送数据	TxD	→	√			
3	接收数据	RxD	←	√			
4	请求发送	RTS	→		√		
5	允许发送	CTS	←		√		
6	数据设备就绪	DSR	←		√		
20	数据终端就绪	DTR	→		√		

⊖ 1英尺（ft）= 0.3048米（m）

（续）

25芯连接器引脚号	接口电路名称		信号方向DTE DCE	数据	控制	定时	地线
8	载波检测	CD	←		√		
22	振铃指示	RI	←				
24	发送信号码元定时（DTE）	TxC	→			√	
15	发送信号码元定时（DCE）	TxC	←			√	
17	接收信号码元定时（DCE）	RxC	←			√	
21	信号质量检查	SQD	←		√		
23	数据信号速率选择（DTE）		→		√		
18	数据信号速率选择（DCE）		←		√		
14	备用信道发送数据		→	√			
16	备用信道接收数据		←	√			
19	备用信道请求发送		→		√		
13	备用信道允许发送		←		√		
12	备用信道载波检测		←		√		

3.1.4 过程特性

为了更好地说明RS-232-C物理接口的过程特性，我们将以两台计算机通过公用电话网进行数据交换的工作过程来阐述 RS-232-C各个信号线的动作，即 RS-232-C物理层接口的过程特性。计算机通过公用电话网进行通信的连接方式如图 3-2所示。在计算机与 Modem之间的物理层接口是RS-232-C。

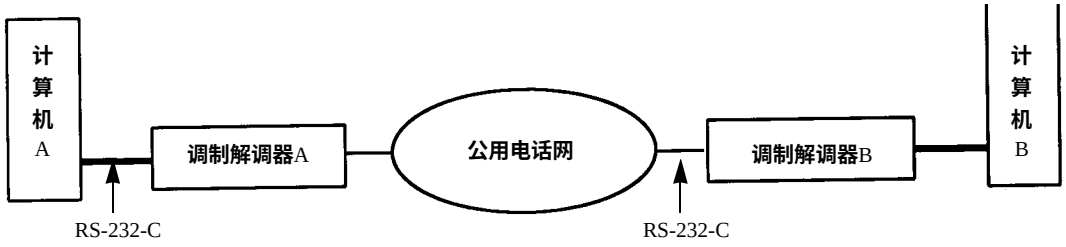


图3-2 计算机通过公用电话网的通信过程

第一步，将计算机和 Modem分别加电，计算机将“数据终端就绪”（Data Terminal Ready，DTR）信号线（第20针）置为“ON”状态，而Modem则将“数据设备就绪”（Data Set Ready，DSR）信号线(第6针)置为“ON”状态，此时Modem处于命令方式(空闲状态)。

第二步，计算机 A通过“发送数据”（Transmit Data，TxD）信号线(第2针)发出拨号命令给Modem A，通知Modem A摘机并拨号。

第三步，Modem B检测到振铃信号后，通过“振铃指示”（Ring Indicator，RI）信号线(第22针)通知计算机B对呼叫进行应答。而计算机 B通过“数据终端就绪”（DTR）信号线(第20针)允许Modem B自动应答Modem A的拨号呼叫，即Modem B发出摘机信号(音频信号)。

第四步，当Modem A收到Modem B返回的应答音频信号后，随即向 Modem B发送载波，而

Modem B收到载波后，通过“载波检测”（Carrier Detection，CD）信号线（第8针）通知计算机B线路接通，同时回应以自身的载波给Modem A。而当Modem B检测到Modem A发出的载波后，它也通过载波检测CD（Carrier Detection）信号线（第8针）通知计算机A线路接通。此时计算机A和计算机B接通，Modem进入联机状态（即数据方式），通信双方可以进入数据通信。

第五步，计算机A通过“发送数据”（TxD）信号线（第2针）将数据发送给Modem A，Modem A将该二进制数据调制成一串不同频率的音频信号通过公用电话网发送给Modem B，Modem B则从音频信号中解调出原始数据并通过“接收数据”（Receive Data，RxD）信号线（第3针）将数据送给计算机B上。而计算机B向计算机A发送数据的过程与此相同。计算机在发送数据过程中，要求“请求发送”（Request To Send，RTS）信号线（第4针）为“ON”状态；而在接收数据过程中，要求“载波检测”（CD）信号线（第8针）为“ON”状态。

第六步，计算机A通过将“请求发送”（RTS）信号线置为”OFF”状态以通知Modem A数据发送结束。Modem A检测到RTS信号为“OFF”状态后，停止发送载波，并置“允许发送”（CTS）信号线为“OFF”状态以响应计算机A。而Modem B检测不到载波后自动恢复到待机状态，并置“载波检测”（CD）信号线（第8针）为“OFF”状态，通知计算机B不能接收数据。

第七步，计算机A置DTR信号线（第20针）为“OFF”状态，通知Modem A拆线。Modem A收到DTR的“OFF”信号后撤除与电话线的连接，并将DSR信号线置为“OFF”状态作为回答。

另外，在计算机发送数据到Modem的过程中，如果Modem的接收速度太慢，则Modem可以通过降下CTS信号通知计算机暂停发送数据。而且两个Modem建立载波连接后将继续保持载波连接，当载波消失或中断几十分之一秒后，连接被终止。

必须注意的一点是，两个Modem在进行真正数据传输之前，必须首先交换如何向对方发送数据的信息，这一过程叫做交接过程。两个Modem必须就以下事项协调一致：传输速度、组成数据包的位数、包的起始位/停止位、奇偶校验以及半双工/全双工等。

3.1.5 空Modem电缆

RS-232-C接口电路在实际系统中应用广泛。除了作为DTE与DCE之间的连接标准外，常用于设备之间的直接连接。例如，个人计算机与个人计算机的直接通信，计算机与CRT终端以及打印机的通信等。这种直接通过RS-232-C接口将两个DTE连接起来的方法称为空Modem（null modem）连接方式。

两台计算机或终端通过Modem远程连接时，计算机或终端都被作为DTE使用，用标准接口电缆和DCE（如Modem）相连。当两台计算机仍想采用RS-232-C标准接口直接互连时就会产生问题（Windows 98操作系统中两台计算机通过串口直接连接的电缆就是RS-232-C空Modem电缆）。RS-232-C标准接口使用的连接器是DB25的插头和插座（DTE端为DB25M连接器，即插头；DCE端为DB25F连接器，即插座），其中第2脚为“发送数据”线、第3脚为“接收数据”线。若将两台计算机用RS-232-C标准接口电缆直接连接（RS-232-C标准接口电缆一头为DB25M插头连接器，接DCE端；另一头为DB25F插座连接器，接DTE端），不仅因为两台计算机（DTE）的连接器都是插头而无法用RS-232-C标准接口电缆连接，而且还有接线脚的连接问题。例如，两台计算机都使用第2脚来发送数据，使用第3脚来接收数据，结果出现“顶牛”现象。

为了解决这些问题，通常采用空 Modem电缆连接方式。简单型空 Modem电缆，如图3-3a所示，保持两台计算机作为 DTE的接口不做任何改变，只是将两台计算机的 RS-232-C接口的“发送数据”线和“接收数据”线交叉连接，而地线直接对接即可。这样两台计算机就可以通过 RS-232-C标准接口直接进行通信。

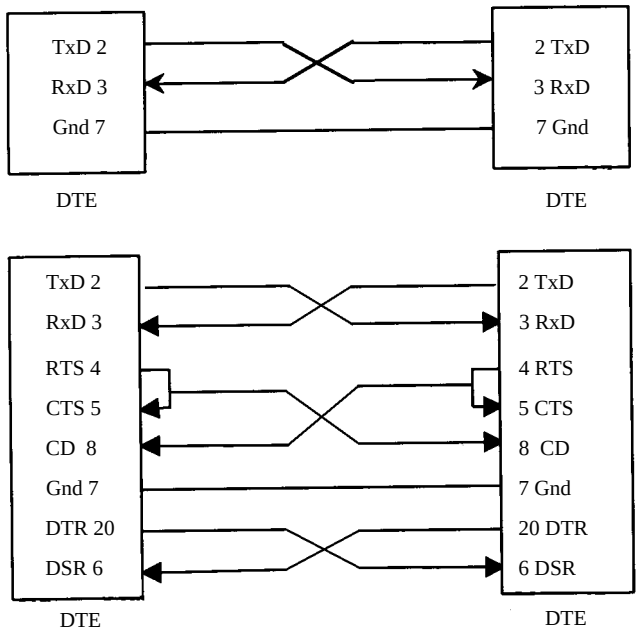


图3-3 异步传输时的RS-232-C空Modem电缆

复杂型空Modem电缆可用于多根接口线连接的情况，其接线情况如图 3-3b所示。“发送数据”（TxD）线和“接收数据”（RxD）线是交叉连接的，这样就保证了数据的正确收发。由于使用空 Modem电缆直接连接时也支持全双工特性， RTS和CTS不再具有与 Modem连接时那样的功能，为了让发送请求总是许可的，将 RTS信号返回作为CTS信号，同时把RTS信号直接接到另一端的 CD信号，这是因为 RTS信号的出现在功能上类似于通信信道中的载波检测。 DSR信号线和DTR 信号线也是交叉连接的。另外，有时我们也可以将 DTR信号线交叉连到CI信号线上，表示当一个DTE设备给出DTR信号时，就可以表示另一端收到了 CI信号。

前面所讲的用空 Modem电缆直接连接的方式都是基于异步传输的。同步传输时，就要涉及定时电路。由于有的 Modem既提供发送时钟又提供接收时钟；而有的 Modem只提供接收时钟，不提供发送时钟，因此这时需要 DTE提供定时信息，且 DTE必须具有发送时钟源。 RS-232-C接口标准中，“接收码元定时”信号由 Modem的锁相环提供，加到DB25连接器的第 17脚上。“发送码元定时”信号是由 Modem还是由DTE提供，与使用的Modem有关。当由Modem提供时，这个信号加到DB25连接器的第 15脚上。当由 DTE提供时，这个信号加到 DB25连接器的第 24脚上。如果不使用 Modem，把两个同步传输的 DTE连到一起时，在定时方面就会遇到困难。因此，在使用空Modem电缆连接两个设备时，应保证至少有一个设备带有时钟信号源。对于 Modem，这种时钟可以称为外部时钟，即可理解为是“非 Modem”时钟。

如果只有一个设备带有时钟源时，含有外部时钟的设备通常在第 24脚（有些设备是在第 15脚）上输出时钟信号。我们通过空 Modem电缆将两个DTE设备的第15脚和第17脚与第24脚的时钟信号线连接起来，如图 3-4所示。这样两个同步的DTE设备在没有Modem的情况下就可进行直接通信。但这种单端提供时钟信号的连接方式，因为 1个时钟信号驱动器要驱动 4个接收器，所以负载较重。

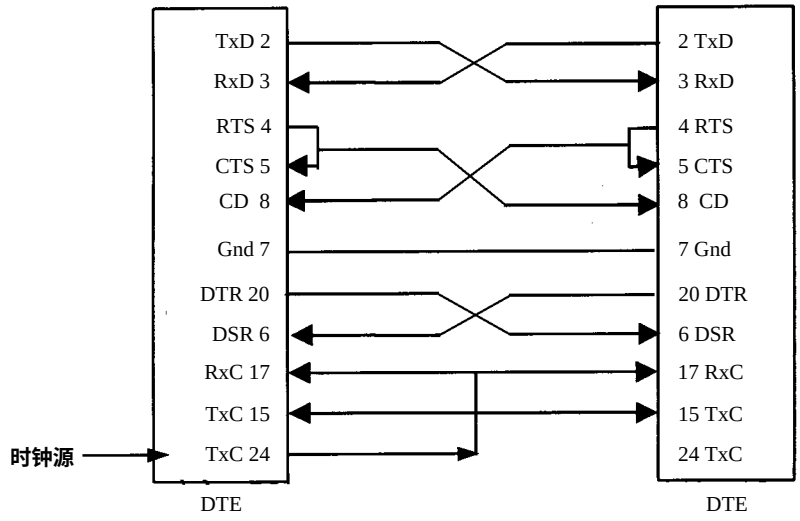


图3-4 只有一个DTE具有时钟源时的连接

如果两个同步 DTE设备各自都带有时钟源，假设它们都分别从 24脚输出时钟。则我们可以通过空Modem电缆分别将一设备的第 24脚与同一设备的第 15脚和另一设备的第 17脚连接，如图 3-5所示（同步传输方式下的空 Modem电缆的其他连线情况与前面讲述异步传输空 Modem电缆的连线情况是相同的，只是增加了同步传输时所必需的时钟线的对接）。

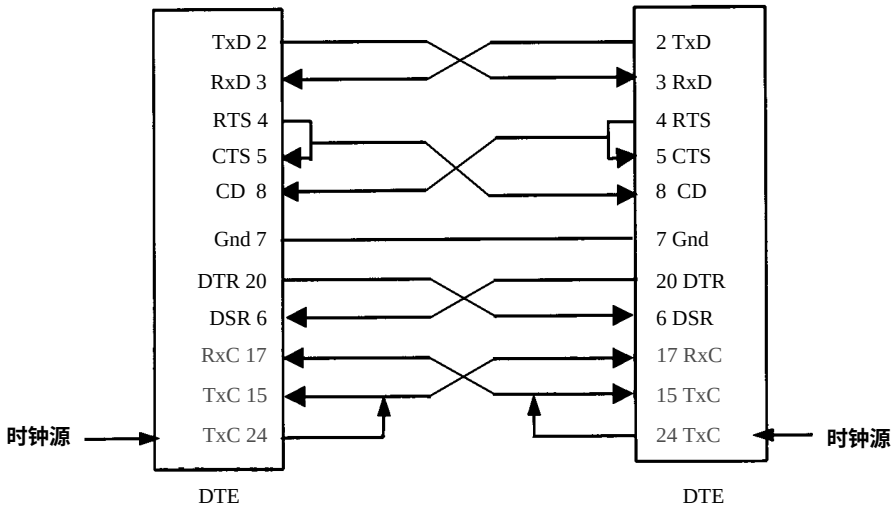


图3-5 两个DTE具有时钟源时的连接

请读者注意，空Modem电缆不同于一般标准RS-232-C连接电缆，标准RS-232-C电缆由于两端的连接器不同，因而它有方向性。而空 Modem电缆没有方向性，其任一端均可与计算机或终端等DTE设备相连，而计算机或终端的接口均和原来与 Modem连接时的接口相同。

3.2 其他接口

除了EIA RS-232-C/CCITT V.24接口标准外，还有其他一些接口标准，下面将简单介绍这些接口标准。如果读者想要更详细地了解这些接口，可以查找相应的接口标准文本。

3.2.1 RS-449接口

如前所述，由于RS-232-C接口标准具有某些不足，如不能进行远距离传输驱动，因此为了改善RS-232-C的电气性能，美国电子工业协会（ EIA）提出了一个新型接口标准，即 EIA RS-449。该标准包含三个部分： RS-449、RS-422-A和RS-423-A。RS-449规定了接口的机械特性、功能特性以及过程特性。而接口的电气特性由 EIA RS-422-A（即CCITT V.10/X.26标准）和EIA RS-423-A（即CCITT V.11/X.27标准） 标准予以规定。

RS-423-A是为了解决RS-232-C的信号地电位差问题而对 RS-232-C的电气特性作了一些改进而提出的标准。 RS-423-A是一种不平衡接口电路，它采用差分接收器，接收器的一个输入端接发送方的信号地，如图3-6所示。RS-423-A的输入电平与TTL兼容，输出电平与CMOS兼容。

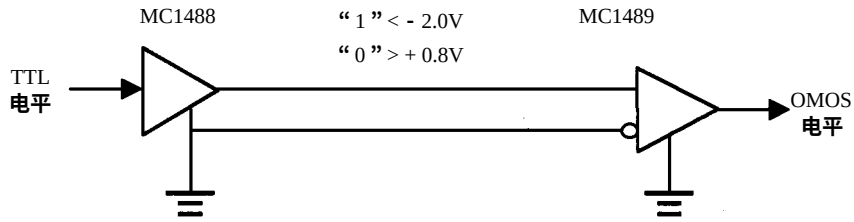


图3-6 RS-423-A接口电路

RS-423-A接口标准中，传输电缆的最大长度与数据传输率有关。当数据传输速率为 3kbps时，电缆长度可达1km；当传输速率超过3kbps时，电缆长度相应缩短；当电缆长度为 10m时，数据传输率可达300kbps。

RS-422-A则更进一步采用平衡驱动和差分接收的方法，从根本上消除了信号地电位差的影响。平衡驱动器相当于两个单端驱动器，它们输入的是同一个信号，而一个驱动器的输出正好与另一个反相，如图 3-7所示。当干扰信号作为共模信号出现时，接收器则接收差分输入电压。只要接收器具有足够的抗共摸电压的范围，它就能识别这两种信号并正确接收所传送的数据，因此RS-422-A接口具有非常好的抗干扰性。 RS-422-A的输入电平与 TTL兼容，输出电平与CMOS兼容。

RS-422-A接口标准中，传输电缆的最大长度与数据传输率有关。当传输速率为 100kbps时，电缆长度可达1000m；当传输速率为2Mbps时，电缆长度只能为60m；当传输速率为10Mbps时，电缆距离仅为10m。

在机械特性上，为了适应信号线数目的增加， RS-449标准采用37针和9针连接器。正常情况

下只需要37针连接器，当要使用备用信道时，必须加上 9针连接器。另外在功能特性上， RS-449采用与RS-232-C不同的信号线命名符。

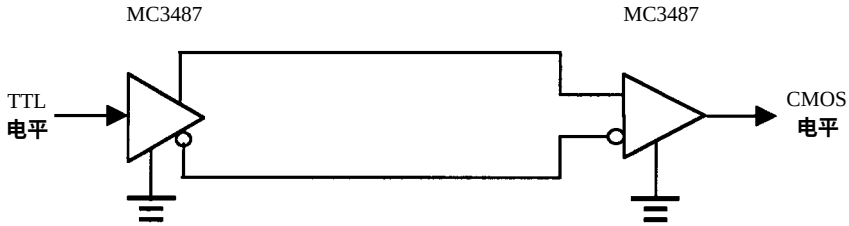


图3-7 RS-422-A接口电路

RS-449标准保留了在RS-232-C中定义的基本交换电路的功能。除了在电气特性及机械特性方面与RS-232-C标准不同之外，RS-449标准与RS-232-C标准的主要不同点有：

(1) RS-449新定义了10个接口电路，包括3个用于测试状态的电路； 2个用于控制DCE在备用信道传输的电路； 1个在DTE控制下提供终止使用功能的接口电路； 1个提供新信号功能的电路和1个对DCE进行频率选择的电路。 RS-449还定义了2个为每个方向传输提供公共参考的接口电路。

(2) 有3个RS-232-C的接口电路在RS-449中没有定义。它们是保护地和两个留作测试用的电路（RS-232-C中的第9脚和第10脚）。

(3) 对电路功能的有些定义作了改变。例如，将 RS-232-C中的DSR电路的名字改为数据方式DM，相应的功能也发生了改变。

(4) 为了防止和RS-232-C电路的记忆名混淆， RS-449标准中的所有电路记忆名都和 RS-232-C的电路记忆名不同。

RS-449标准的接口电路可分为5类：地或公用电路、数据电路、控制电路、定时电路和备用信道电路。

3.2.2 RS-530接口

EIA RS-530接口标准是1987年颁布的，作为对 RS-449标准的改进建议。它是 RS-232-C、RS-422-A和RS-423-A的结合物。它支持的数据传输率的范围从 20kbps～2Mbps，因此不能取代RS-232-C。EIA RS-530包含下面几个特性。

(1) 机械特性

EIA RS-530使用标准的DB25连接器。

(2) 电气特性

EIA RS-530的电气特性遵循RS-422-A标准，但有些细微的差别；其诊断电路则遵循 RS-423-A标准。

(3) 功能特性

包括RS-232-C中的所有重要电路，如TxD、RxD、DTR、DSR、RTS、CTS、CD以及3个时钟电路。EIA RS-232-C中的诊断电路也包括在内。

EIA RS-530的过程特性与RS-232-C基本类似，在此不再多述。

3.3 小结

物理层接口是物理层协议标准的具体体现。一个物理层接口包含机械特性、电气特性、功能特性和过程特性四个方面。RS-232-C是最常用的物理层接口标准，RS-449、RS-530是RS-232-C接口标准的改进。

习题

1. 物理层接口标准包含哪方面的特性？每种特性的具体含义是什么？
2. 请说明RS-232-C接口中主要信号线的功能。
3. 请解释物理层接口的电气特性与其支持的数据传输率和传输距离的关系。
4. 什么是空Modem电缆？它有什么作用？
5. 简述两台计算机通过公用电话交换网进行通信的工作过程。
6. RS-232-C、RS-423-A和RS-422-A的电气特性各有什么不同？

第5章　局域网

计算机局域网一般采用共享介质，这样可以节约局域网的造价。对于共享介质，关键问题是当多个站点要同时访问介质时，如何进行控制，这就涉及到局域网的介质访问控制（ Medium Access Control，MAC）协议。本章我们首先介绍局域网中的介质访问控制协议，然后介绍常用的两种局域网：以太网和令牌环网，最后介绍局域网互连设备，即网桥。

5.1　介质访问控制

正如我们在第2章所介绍的那样，对于单个信道的访问控制可以采用传统的频分多路复用技术。如果网络中有 N个用户，则可以将信道按频率划分成 N个逻辑子信道，每个用户分配一个频段。由于每个用户都有各自的频段，所以相互之间不会产生干扰。

频分多路复用（FOM）的技术在用户数目固定且每个用户通信量都较大时是一种比较简单且有效的信道访问控制策略。然而对于用户数目经常变化且用户通信量也经常发生变化的局域网来说，FDM存在一些问题。例如，对于前面提到的将信道划分为 N个频段的情况，如果网络中当前希望通信的用户数目少于 N时，许多宝贵的频段资源就会被浪费；而如果有超过 N个以上的用户希望通信时，则其中的某些用户会因为没有分配到频段而不能进行通信，即使这时已分配到频段的用户并没有通信需求，这些频段资源也不能被其他用户使用。

如果我们设法将网络用户的数目维持在 N个左右，是否就可以使用静态FDM分配策略呢？答案是否定的。下面我们通过一个简单的排队论计算来阐述这个问题。

假设信道的容量是 C位/秒，其数据到达率为λ帧/秒，每帧长度服从指数分布，且帧的平均长度为1 / μ比特帧，则信道传输一帧的平均时间 T应为：

$$T = \frac{1}{\mu C - \lambda}$$

如果将单个信道划分为 N个独立的子信道后，其中每个子信道的容量应为 C/N位/秒，每个子信道的数据到达率为 λ/N帧/秒，帧的平均长度仍为1/μ比特/帧，则此时传输一帧所需的时间 T_{FDM}为：

$$T_{\mathrm{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT$$

由此可以看出，采用FDM分配策略将会导致传输一帧所需的时间为单个信道时的 N倍。

同样的道理，对于时分多路复用（ TDM）技术也会产生同样的问题。在 TDM中，设信道的使用时间被均匀分为 N个时隙，每个用户静态地占用一个时隙。假如用户在规定的时隙内没有通信，也将造成资源的浪费。

由此可见，传统的多路复用技术并不能有效地处理局域网中用户通信的突发性，因此我们必须采用新的介质访问控制协议。

5.1.1 ALOHA协议

ALOHA协议是20世纪70年代在夏威夷大学由Norman Abramson及其同事发明的，目的是为了解决地面无线电广播信道的争用问题。ALOHA协议分为纯ALOHA和分槽ALOHA两种。

1. 纯ALOHA

ALOHA协议的思想很简单，只要用户有数据要发送，就尽管让他们发送。当然，这样会产生冲突从而造成帧的破坏。但是，由于广播信道具有反馈性，因此发送方可以在发送数据的过程中进行冲突检测，将接收到的数据与缓冲区的数据进行比较，就可以知道数据帧是否遭到破坏。同样的道理，其他用户也是按照此过程工作。如果发送方知道数据帧遭到破坏（即检测到冲突），那么它可以等待一段随机长的时间后重发该帧。对于局域网LAN，反馈信息很快就可以得到；而对于卫星网，发送方要在270ms后才能确认数据发送是否成功。通过研究证明，纯ALOHA协议的信道利用率最大不超过18%（1/2e）。

2. 分槽ALOHA

1972年，Roberts发明了一种能把信道利用率提高一倍的信道分配策略，即分槽ALOHA协议。他的思想是用时钟来统一用户的数据发送。办法是将时间分为离散的时间片，用户每次必须等到下一个时间片才能开始发送数据，从而避免了用户发送数据的随意性，减少了数据产生冲突的可能性，提高了信道的利用率。在分槽ALOHA系统中，计算机并不是在用户按下回车键后就立即发送数据，而是要等到下一个时间片开始时才发送。这样，连续的纯ALOHA就变成离散的分槽ALOHA。由于冲突的危险区平均减少为纯ALOHA的一半，因此分槽ALOHA的信道利用率可以达到36%（1/e），是纯ALOHA协议的两倍。但对于分槽ALOHA，用户数据的平均传输时间要高于纯ALOHA系统。

5.1.2 CSMA协议

分槽ALOHA协议的最大信道利用率仅为1/e，而纯ALOHA协议的信道利用率为1/2e，这一点并不奇怪。原因是上述的ALOHA协议中，各站点在发送数据时从不考虑其他站点是否已经在发送数据，这样当然会引起许多冲突。由于在局域网中，一个站点可以检测到其他站点在干什么，从而也就可以相应地调整自己的动作，这样的协议可以大大提高信道的利用率。

对于站点在发送数据前进行载波侦听，然后再采取相应动作的协议，人们称其为载波侦听多路访问（Carrier Sense Multiple Access，CSMA）协议。CSMA协议有几种类型，我们将分别进行讨论。

1. 1-坚持CSMA（1-persistent CSMA）

1-坚持CSMA协议的工作过程是：某站点要发送数据时，它首先侦听信道，看看是否有其他站点正在发送数据。如果信道空闲，该站点立即发送数据；如果信道忙，该站点继续侦听信道直到信道变为空闲，然后发送数据；之所以称其为1-坚持CSMA，是因为站点一旦发现信道空闲，将以概率1发送数据。

2. 非坚持CSMA（nonpersistent CSMA）

对于非坚持CSMA协议，站点比较“理智”，不像1-坚持CSMA协议那样“贪婪”。同样的道

理，站点在发送数据之前要侦听信道。如果信道空闲，立即发送数据；如果信道忙，站点不再继续侦听信道，而是等待一个随机长的时间后，再重复上述过程。定性分析一下，就可以知道非坚持CSMA协议的信道利用率会比1-坚持CSMA好一些，但数据传输时间可能会长一些。

3. *p*-坚持CSMA（p-persistent CSMA）

p-坚持CSMA主要是用于分槽ALOHA。其基本工作原理是，一个站点在发送数据之前，首先侦听信道。如果信道空闲，便以概率 *p*发送数据，以概率 1-*p*把数据发送推迟到下一个时间片；如果下一个时间片信道仍然空闲，便再次以概率 *p*发送数据，以概率1-*p*将其推迟到下下一个时间片。此过程一直重复，直到将数据发送出去或是其他站点开始发送数据。如果该站点一开始侦听信道就发现信道忙，那么它就等到下一个时间片继续侦听信道，然后重复上述过程。

在上述三个协议中，都要求站点在发送数据之前侦听信道，并且只有在信道空闲时才有可能发送数据。但即便如此，仍然存在发生冲突的可能。考虑下面的例子：假设某站点已经在发送数据，但由于信道的传播延迟，它的数据信号还未到达另外一个站点，而另外一个站点此时正好要发送数据，则它侦听到信道处于空闲状态，也开始发送数据从而导致冲突。一般来说，信道的传播延迟越长，协议的性能越差。

5.1.3 CSMA/CD协议

1-坚持和非坚持CSMA协议都是对ALOHA协议的改进，CSMA协议要求站点在发送数据之前先侦听信道。如果信道空闲，站点就可以发送数据；如果信道忙，站点则不能发送数据。我们还可以对CSMA协议作进一步的改进，要求站点在发送数据过程中进行冲突检测，而一旦检测到冲突立即停止发送数据。这样的协议被称为带冲突检测的载波侦听多路访问协议，即CSMA/CD（Carrier Sense Multiple Access with Collision Detection）协议。

CSMA/CD协议的工作原理是：某站点想要发送数据，必须首先侦听信道。如果信道空闲，立即发送数据并进行冲突检测；如果信道忙，继续侦听信道，直到信道变为空闲，才继续发送数据并进行冲突检测。如果站点在发送数据过程中检测到冲突，它将立即停止发送数据并等待一个随机长的时间，重复上述过程。

下面仔细研究一下CSMA/CD协议。假设某个站点正好同时在t0处开始发送数据，那么站点需要多长时间后才能发现冲突？检测到冲突的最短时间应该是信号从一个站点传输到另一个站点所需的时间。

基于上述推理，读者可能会认为，假设某站点从开始发送数据起的整个电缆传输时间内未检测到冲突，就可以确认自己“抓住”了电缆。所谓“抓住”指的是其他站点知道该站点在使用电缆，因而不会干扰该站点的数据传输。实际上这个推断是错误的。考虑图 5-1所给出的一种最坏的情况。

在图5-1中，A、B两个站点的传播延迟是τ。假设在0时刻，站点A开始发送数据，经过τ-ε后（即信号快到达最远站点B之前），由于A站点发送的数据信号还未到达B站点，因此B站点侦听信道时认为信道是空闲的，B也发送数据。当然，B站点很快检测到冲突而取消数据发送，而站点A则要等到2τ 时刻后才能检测到冲突。也就是说，对于该模型中的站点，必须在经过 2τ 时间内都没有检测到冲突时，才能确定该站点“抓住”信道。我们一般把 2τ 称为“冲突窗口”。

CSMA/CD是个很重要的协议，我们将在IEEE 802.3国际标准中加以重点讨论。其他的多路访问协议如令牌传递机制，我们将在后面介绍具体的局域网技术时加以介绍。

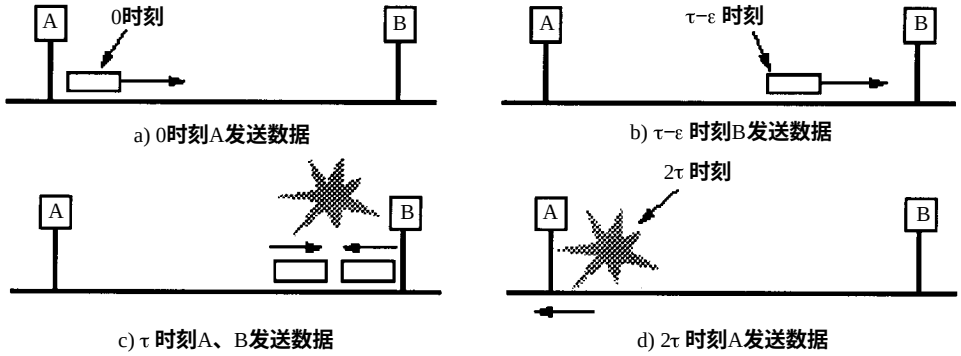


图5-1 冲突检测时间

为了便于下面内容的学习，我们先简单介绍一下IEEE 802系列标准。随着局域网的广泛使用和各种局域网产品的增加，标准化问题愈加显得重要。国际电工电气委员会IEEE下设的802委员会在局域网LAN的标准制定方面做了卓有成效的工作，它们制定了IEEE 802标准，有时也称为局域网参考模型。其中包括CSMA/CD、令牌总线和令牌环网等底层网络协议。这些标准在物理层和MAC层上有所不同，但在数据链路层上是兼容的，如图5-2所示。

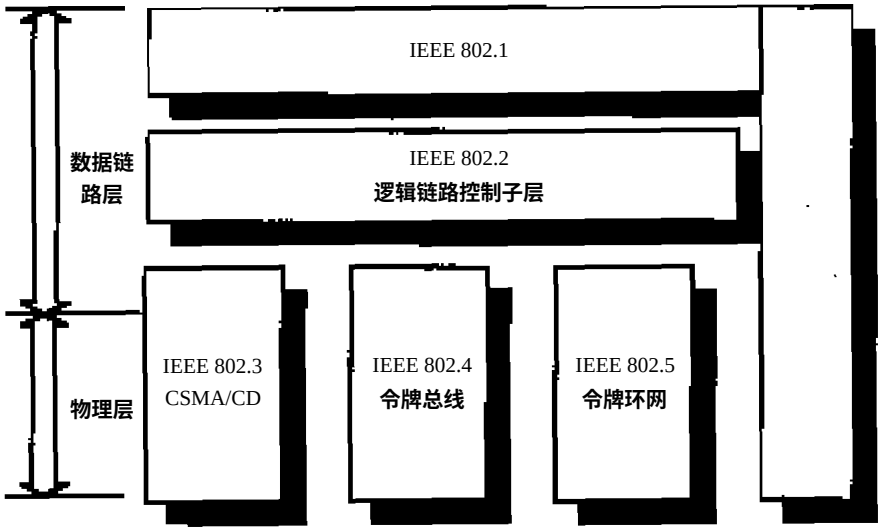


图5-2 IEEE 802局域网参考模型

IEEE 802标准已经被ISO接收为国际标准，编号为ISO 8802。IEEE 802标准分成几个部分：802.1主要介绍局域网体系结构、局域网互联和管理；802.2描述了数据链路层的上部，它使用逻辑链路控制（Logical Link Control，LLC）协议；802.3、802.4和802.5分别描述了3种局域网标准（以太网、令牌总线和令牌环网）。下面我们将介绍其中最重要的两种。

5.2 以太网和IEEE 802.3

以太网（Ethernet）是一种总线式局域网，以基带同轴电缆作为传输介质，采用 CSMA/CD 协议，如图5-3所示。

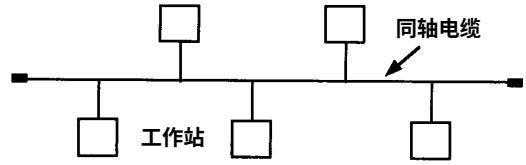


图5-3 以太网拓扑结构

以太网最早来源于 Xerox公司著名的 PARC（Palo Alto Research Center）研究中心于1973年建造的第1个2.94Mbps的CSMA/CD系统，该系统可以在14米的电缆上连接100多个个人工作站。

Xerox公司建造的以太网是如此的成功，于是Xerox、DEC和Intel公司于1980年联合起草了以太网标准，并于 1982年发表了第2版本的以太网标准。1985年，IEEE802委员会吸收以太网为IEEE802.3标准，并对其进行了修改。以太网标准和IEEE802.3标准的主要区别是：以太网标准只描述了使用 50Ω同轴电缆、数据传输率为10Mbps的的总线局域网，而且以太网标准包括 ISO数据链路层和物理层的全部内容；而IEEE802.3标准描述了运行在各种介质上的、数据传输率从 1Mbps～10Mbps的所有采用CSMA/CD协议的局域网，而且IEEE802.3标准只定义了ISO参考模型中的数据链路层的一个子层（即介质访问控制MAC子层）和物理层，而数据链路层的逻辑链路控制 LLC子层由IEEE802.2描述。另外，以太网和 IEEE802.3在帧格式上有所不同，我们将在介绍 IEEE802.3帧格式时加以说明。下面我们主要是针对IEEE802.3标准展开讨论。

5.2.1 物理层标准

IEEE802.3支持不同的物理层标准，而这些不同的物理层标准意味着 IEEE802.3可以使用不同的物理介质和物理层接口。IEEE802.3的不同物理层标准如表5-1所示。

表5-1 IEEE802.3物理层标准

名 称	介 质	最大长度/段	工作站数目/段	特 点
10Base5	粗同轴电缆	500m	100	适合于主干
10Base2	细同轴电缆	200m	30	低廉的网络
10Base-T	双绞线	100m	1024	易于安装和维护
10Base-F	光纤	2000m	1024	远程工作站连接

第1种电缆是10Base5，我们俗称为“粗以太电缆”。10Base电缆类似于一个黄色的花园用水管，每隔2.5米有一个标记，标明是分接头插入处。工作站通过收发器电缆和收发器上的分接头连入粗以太电缆。收发器牢牢地夹在电缆上，使得触针能够接触到电缆的内芯。收发器内部有电子线路用于载波侦听和冲突检测。当检测到冲突时，收发器就在电缆上产生一个特殊的无效信号，确保其他收发器也能尽快知道产生了冲突。

收发器电缆将收发器与网络接口板连起来。收发器电缆的最大长度为 50m，电缆内有4对屏蔽双绞线，其中2对分别用于数据的输入和输出， 1对用于冲突指示，另 1对用于向收发器供电。设置冲突指示线对是为了能在收发器中识别冲突，因为网络接口板从输入数据线中检测冲突较为困难。以太网收发器电缆连接器的引脚分配如表 5-2所示。

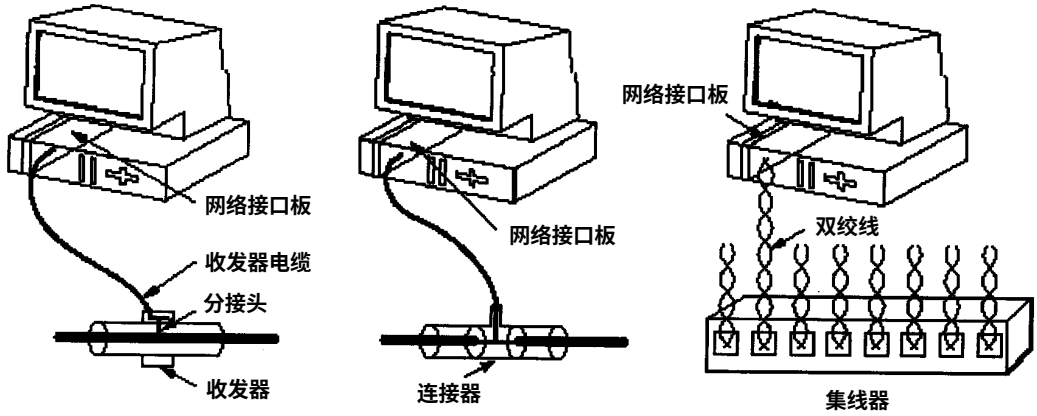
表5-2 收发器电缆连接器引脚分配

引 脚	信 号	引 脚	信 号	引 脚	信 号
1	屏蔽地	6	电源地	11	保留
2	冲突指示＋	7	保留	12	接收数据－
3	发送数据＋	8	保留	13	电源
4	保留	9	冲突指示－	14	保留
5	接收数据＋	10	发送数据－	15	保留

第2种电缆是10Base2，或称之为“细以太电缆”。细以太电缆采用工业标准的BNC连接器组成T型接头，因而比较灵活、可靠。细以太电缆价格低廉、安装方便，但是它覆盖的范围只有200m，而且每段电缆内只能连接30台机器。网络接口板通过一个无源的BNC T型头与电缆直接相连，不需要收发器电缆，收发控制电路在网络接口板上。

对于上述两种电缆，都存在电缆断裂、插入式分接头损坏或插接头松动的潜在隐患。我们可以采用一种称为时域反射测量（time domain reflectometry）的技术，其基本工作原理是：首先向电缆输入一个已知形状的脉冲，如果它受到阻碍或达到电缆尽头，就会返回一个回波，仔细测量发送脉冲和回波到达之间的间隔，就可以确定回波的发源处。

为了更好地解决电缆故障的问题，现在广泛采用一种新的接线方式，即将所有的站点通过双绞线连接到中心集线器（Hub）上，构成星型结构，这种方式被称作10Base-T。10Base-T的结构使得网络结点的加入和移去都变得十分简单，对电缆故障的检测也非常容易。 10Base-T的缺点是它的电缆长度为距离集线器100m。尽管如此，由于10Base-T易于维护，它的应用越来越广。图5-4给出了上述3种连接方式的图解。IEEE802.3的第4种电缆连接方式是10Base-F，它采用光纤介质。10Base-F具有很好的抗干扰性，常常用于远程办公室或工作站的连接，但10Base-F的的连接器和终端匹配器价格比较昂贵。

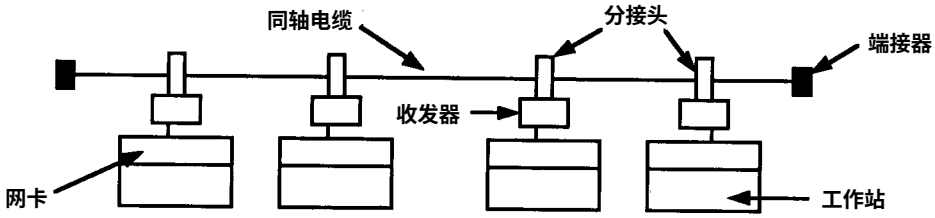


a) 10Base5 b) 10Base2 c) 10Base-T

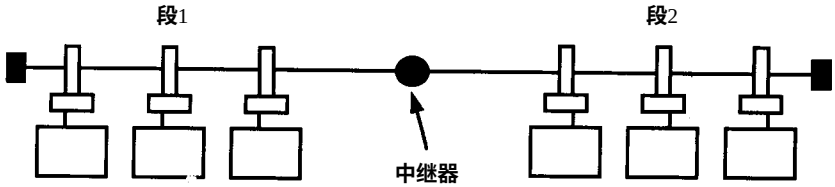
图5-4 IEEE802.3 的三种接线方式

图5-5给出了10Base5网络的一个连接示意图，其中图5-5a表示电缆长度小于500m的情形；图5-5b表示当网络覆盖的距离超过500m时可以用中继器（repeator）加以扩充。中继器是一个物

理层设备，它能够双向接收并放大信号。对于 CSMA/CD协议来说，用中继器连接起来的一系列电缆段同单根电缆并无区别（除了中继器产生一些延迟外）。一个IEEE802.3 系统可以同时有多个电缆段和多个中继器。但 10Base5规定，任意两个收发器的距离不能超过 2.5km，即任意两个收发器之间中继器的个数不能超过 4个。



a) 单段电缆的10Base 5



b) 有中继器的10Base 5

图5-5 IEEE802.3 10Base5连接示意图

IEEE802.3在电缆上传输的信号采用曼彻斯特编码。其编码规则为，每个数据单元分割为等宽的两部分：电平由低到高时表示“ 1 ”，由高到低时表示“ 0 ”。曼彻斯特编码将时钟与数据组合在一起，接收方可以从接收到的数据中提取时钟信号以取得与发送方时钟的同步。另外，曼彻斯特编码保证每个数据单元至少有一个跳变，可以用它来区分电缆的工作状态和空闲状态，便于实现载波侦听。同样的道理，曼彻斯特编码也能适合冲突检测。

5.2.2 MAC协议

IEEE802.3 MAC子层协议包括帧格式和 CSMA/CD协议两部分，下面我们主要介绍IEEE802.3帧格式并对CSMA/CD协议的某些内容加以讨论。

1. 帧格式

IEEE802.3的帧格式如图 5-6所示。802.3的帧由八部分组成：前导符、起始符、目的地址、源地址、长度、数据、 PAD和CRC校验码。其发送顺序是从前导符开始发送，每个字节从最低开始发送。

7	1	6	6	2	0～1500	0～46	4	字节
前导符	起始符	目的地址	源地址	长度	数据	PAD	CRC	

图5-6 IEEE802.3帧格式

前导符是7个字节的10101010。前导符字段的曼彻斯特编码会产生 10MHz、持续5.6μs 的方波，便于接收方的接收时钟与发送方的发送时钟进行同步。

起始符为10101011，标志着一帧的开始。

目的地址共 48位，指示接收站点。最高位为“ 0 ”时表示唯一地址或单播地址（ unicast address）；最高位为“ 1 ”时表示组地址或组播地址（ multicast address）；全“ 1 ”时为广播地址（broadcast address）。

802.3采用长地址是出于所谓“ 全球唯一地址 ”的编址策略，即所有 802.3网络中的工作站网卡的物理地址都互不相同（共有 247 ，即超过一百万亿个地址），从而使得工作站在不同网络之间移动时无需改变地址。另外，在网络互连后，唯一地址还有利于跨网寻址。在 Xerox公司设有一个专门负责分配这一百万亿个地址的机构。

802.3的源地址也是48位，它必须是一个唯一地址，也就是说源地址的最高位必须为“ 0 ”。

长度字段用于指明数据段中的字节数，其值为 0~1500。数据段是用户要发送的数据。 0字节数据是合法的，但这会引起麻烦。如前所述， CSMA/CD协议有一个冲突窗口，如果发送方在发送时间达到冲突窗口宽度后仍然没有检测到冲突，则认为它已经“ 抓住 ”了信道，可以无冲突地将数据发送完毕。但若一个完整帧的发送时间小于冲突窗口宽度，则发送方由于没有数据发送将无法检测到是否有冲突（ CSMA/CD要求边发送边进行冲突检测）。其结果是，产生冲突的数据帧不能被CSMA/CD协议检测到并重新发送，而要靠高层软件加以处理，这将极大地延长发送时间。另一方面，限制最小帧长度后，若接收方接收到一个短于最小帧长度的帧，即可判定其是冲突碎片，无须再去判定其 CRC，直接将其丢弃。

对于IEEE802.3，两个站点的最远距离不超过 2500m，由4个中继器连接而成，其冲突窗口为 51.2μs （2倍电缆传播延迟加上 4个中继器的双向延迟）.对于 10Mbps的IEEE802.3来说，这个时间等于发送64字节，即512位的时间，64字节就是由此而来的。

随着网络速度的提高，相应地必须增大最小帧长度或缩小电缆最大长度。当 802.3网络的速度提高到100Mbps时，如果最大的电缆长度仍然为 2500m，则最小帧长度必须为 640字节，如果要维持最小帧长度不变（与 10Mbps的802.3相兼容），则必须限制两个站点的最大电缆长度为 250m。当网络速度提高到1Gbps时，既维持站点之间的最大距离为 2500m，又要求最小帧长度应达到6400字节，或既维持 64字节的最小帧长度，又限制两个站点之间的最大距离为 25m，都将使网络不堪忍受。实际情况是，在千兆位以太网中，做了一些处理，一方面使之与 10Mbps和100Mbps的以太网兼容，同时又使网络中站点之间的最大距离仍保持在 250m的可用范围之内。

PAD字段用于数据填充。当用户数据不足 46字节时，要求将用户数据凑足 46字节，以保证IEEE802.3的帧长度不小于64字节（14字节帧头+46字节数据+4字节CRC）。

IEEE802.3的最大帧长度是1518字节（14字节帧头+1500字节数据+4字节CRC）。为应用方便，一般不限制最大帧长度。将用户报文一次性发送完，既节省软件开销，又可提高网络利用率。特别是像802.3这样的竞争型网络，帧越短，为发送一次数据所需的竞争次数越多，冲突碎片所占用的网络带宽也就越大。理论分析与实际测量结果都表明，数据帧越长，网络的有效利用率就越高。然而帧长度还受另外两个因素限制：一是网络平均响应时间，帧越长，一次占用信道的时间越长，其他结点等待发送所需要的时间也就越长；二是缓冲区的限制，考虑到典型环境

下报文长度多在500～2000字节之间，故802.3标准选取最大帧长度为1518字节（其中1500字节为用户数据）。

最后一个字段是32位的CRC校验码，其生成多项式为：$G(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X+1$。CRC码的校验范围为：目的地址、源地址、长度、数据和PAD。目的地址的最高位为生成多项式最高次项的系数。 CRC码由高位到低位顺序发送。较之16位CRC，32位CRC的检错能力更强。

2. CSMA/CD协议

CSMA/CD协议在前一节已经介绍过了，这里只是针对某些内容加以重点讨论。首先我们来看一下，当站点检测到冲突时，随机等待时间是如何产生的？

当冲突产生后，时间被分割成离散的时间片，时间片的大小即为“冲突窗口”的大小。对于802.3，时间片为51.2μs。

第一次冲突产生后，站点等待0或1个时间片后重新尝试发送。如果有两个站点等待的时间片相同，它将再次冲突。第二次冲突后，站点将从0、1、2和3中随机选择一个并等待相应的时间片。如果产生第三次冲突，那么站点将在$0\sim2^{3}-1$之间随机选出等待的时间片数。

以此类推，如果站点第i次发生冲突后，等待的时间片数就将从0到$2^{i}-1$中随机选出。但是，发生10次冲突后，随机等待的最大时间片数就固定在1023。发生16次冲突后，一般情况下，表明有硬件故障，CSMA/CD协议控制器将不再采取任何动作，而是通过向主机发中断报告错误，进一步的恢复留待高层软件或网络管理员完成。

这种算法被称为二进制指数后退（binary exponential backoff）算法。其核心思想是，站点冲突次数越多，平均等待时间也越长。从单个站点的角度来看，好象是不公平的，但从整个网络来看，站点冲突次数的增加，意味着网络的负载较大，因而要求站点的平均等待时间增大，这样可以更快地解决站点的冲突问题。

5.2.3 性能分析

为了对802.3进行性能分析，我们首先定义一些在以太网性能分析中常用的参数。吞吐量S表示通过网络所传输的数据量，利用率U表示网络吞吐量与总容量的比值。

分析802.3协议的性能时，电缆传播延迟τ和网络数据传输率R是两个重要的参数。τ反映了传输介质的长度，R与τ的乘积决定以太网性能。假设有两个以太网，一个以太网数据传输率为500Mbps，电缆长度为1km；另一个以太网数据传输率为10Mbps，电缆长度为10km。因其$R\tau$相等，则这两个以太网的性能相差无几。$R\tau$乘积的物理意义是传输介质等价的比特长度，即传输介质能够容纳的比特数。因为信号在介质上的传播速度是个常数，约等于2×10^{8}米/秒（光速的2/3），所以对于一个数据传输率为10Mbps的以太网来说，500m长的电缆等价于25比特。

若假设R为以太网的数据传输率，d为任意两个站点间的最大距离，V为信号在介质上的传播速度，L为帧的平均数据长度，那么在802.3网络中，传播延迟（propagation delay）与发送时间（transmission time）之比α等于：

$$a=\frac{d/V}{L/R}=\frac{Rd}{LV}$$

参数α 决定了以太网的利用率。若在没有冲突的理想情况下，一个站发送完数据之后，另一个站接着发送数据，并且假定不考虑协议开销，那么 802.3网络的利用率U等于：

$$U = \frac{L/R}{d/V + L/R} = \frac{1}{1+a}$$

从上面的公式可以知道，U和α 成反比，随着α 的增大，802.3网络的利用率U将下降。为了提高吞吐率和利用率U，应尽量减小α，这可以通过适当增加帧的长度来实现。 U对α的关系曲线如图5-7所示。

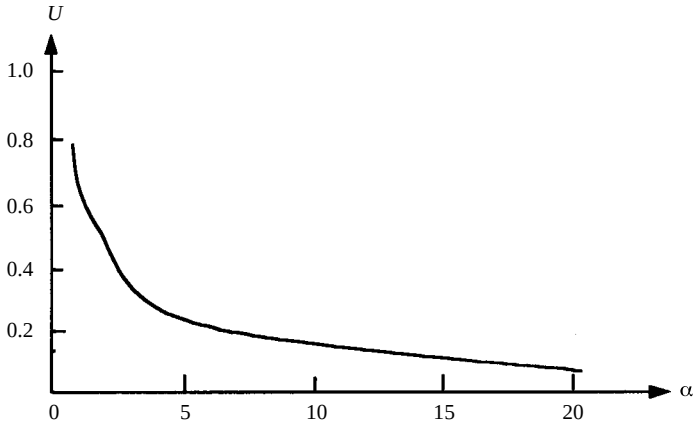


图5-7 U对α 关系曲线

5.3 令牌环网和IEEE802.5

环型网的研究已有多年的历史，但是比起其他局域网技术，环型网的研究进展要缓慢得多。值得一提的是，环型网并不是真正的广播介质，而是单个的点到点线路的集合所形成的一个环，如图5-8a所示。点到点线路涉及的技术已为人们透彻了解，它可以使用双绞线、同轴电缆和光纤等物理介质。环型网在工程实现上几乎全部采用数字技术，不像以太网为了解决冲突检测采用了一部分模拟器件。环型网中站点对环的访问是公平的，站点对环的访问在时间上有一个确定的上限。基于这个原因， IBM选择环型网作为它的局域网。 IEEE在802中定义了环型网的标准，编号为IEEE802.5。

像前面提到的那样，环实际上是许多环接口通过点到点线路连接起来的。每个比特到达环接口后，先复制到接口缓冲区，然后再输出到环上。在输出到环上之前，比特在缓冲区可能被检查或修改，这样必须在环接口处至少引入 1比特的延迟。

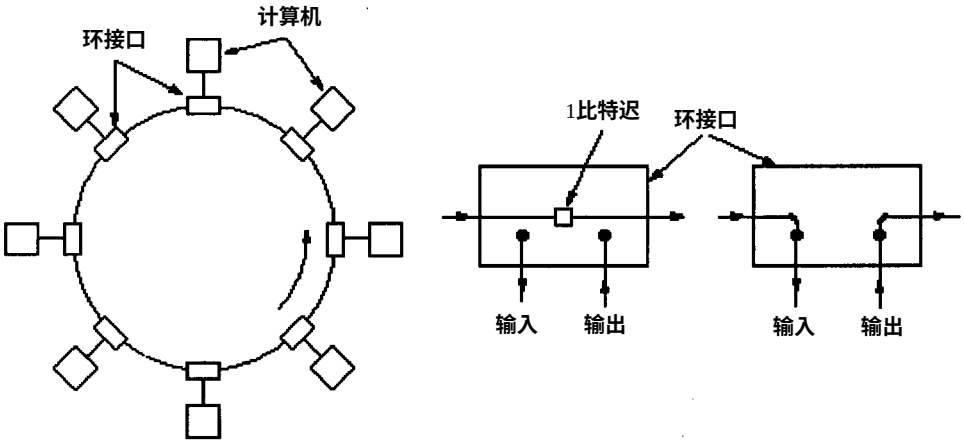
环型网设计和分析的一个关键问题是一个“ 比特 ”的等效“ 物理长度 ”。 假设环的数据传输率是RMbps，则每1/Rμs发送一个比特。信号在环上的典型传播速度为 200m/μs ，则环中一个比特的等效物理长度为 200/R米。这意味着，假设环型网的数据传输率为 1Mbps，环的物理长度为 1km，则同一时刻，环上最多只能存放 5比特数据。

令牌环网是环型网的一种。令牌环网的原理是使用一个称为令牌的特殊比特组合模式，当

环上所有的站点都处于空闲时，令牌沿着环不停旋转。当某一站点想发送数据时必须等待，直至检测到经过该站点的令牌为止。这时，该站点可以用改变令牌中特定位的值的方式将令牌抓住，并将令牌转变成数据帧的一部分，同时，该站点将自己要发送的数据附带上去发送。由于网上只有一个令牌，因此一次只能有一个站点发送。发送站点负责将数据从环中删去。发送站点在下列两个条件都符合时将在环上插入一个新的令牌：

(1) 该站已完成其帧的发送；

(2) 该站所发送的帧的前沿已绕环一周回到发送站。



a) 环网　　b) 侦听模式　　c) 发送模式

图5-8　令牌环网和IEEE802.5的拓扑结构

如果环的等效比特长度小于帧的长度，则第一项条件将隐含着第二项条件。反之，一个站在完成发送后，从理论上讲是可以释放一个令牌的，因而第二项条件并不是必要的。但是，只满足第一条件有可能导致多个帧同时在环上，使令牌环网的差错恢复问题更加复杂化。这样在任何情况，使用令牌机制可以保证在某个时刻只有一个站正在发送数据。

当某站释放一个新的令牌时，它下游的第一站若有数据要发送，将能够抓住这个令牌并进行数据发送。

令牌环设计隐含着这样一个问题，即当环中所有站点都空闲时，环本身必须有足够的时延来容纳一个完整的令牌在环内不停地旋转。这个时延由每个站点引入的 1比特时延和信号在环上的传播时延两部分组成。对于所有的环，设计者必须考虑到各站点关机时所导致的 1比特时延的损失。这意味着，对于短环，当有站点从环中移出时，需要自动向环中插入时延以保证环足够容纳一个完整的令牌。

环接口有侦听和发送两种模式，如图 5-8(b)和(c)所示。在侦听模式时，数据在环接口经过 1比特延迟后输出到环上。只有当站点抓住令牌时才可以进入发送模式。在发送模式下，接口截断输入输出连接，并将自己的数据放到环上。当数据帧在环上旋转一周又回到发送站点时，发送站点将其从环中移走。发送站点或将其保存起来与发送前的数据进行比较以检测环的可靠性，或将其丢弃。当数据帧的最后一位返回发送站点时，环接口必须立即切换到侦听模式，并重新

产生令牌。

当环的通信量很小时，令牌在大部分时间内都在环内空转。然而当通信量很大时，每个站点都有大量数据要发送时，一旦某个站点发送完毕释放令牌，它的下一个站点就会立即抓住这个令牌并发送数据，这样相当于令牌轮流在每个站点之间传递。在网络负载相当重的情况下，网络的效率将近100%。

令牌网最早是由IBM公司开发的，它支持4Mbps和16Mbps两种数据传输率。后来，IEEE将其吸收为国际标准，编号为802.5。下面我们的讨论是按照IEEE802.5标准来进行的。

IEEE802.5标准在物理层上要求使用屏蔽双绞线，数据传输率可以为1Mbps或4Mbps。物理层的信号编码采用差分曼彻斯特编码。在通常的情况下，差分曼彻斯特编码在每位数据中间信号肯定有变化（高到低或低到高）。这样可以在帧的起始标识符和结束标识符中引入高-高和低-低电平这两个无效字符J和K，以便将其与正常数据区分开来。

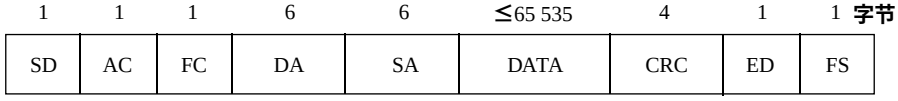
5.3.1 MAC协议

802.5 MAC协议的工作过程比较简单：当环上的站点没有数据要发送时，令牌一直在环上旋转，等待某个有数据要发送的站点将其抓获。该站点把令牌中的某个特定的位由0变为1，将其从令牌变为数据帧的一部分，然后站点输出正常数据帧的其余部分，如图5-9所示。

在令牌环网中，站点抓住令牌后是否可以无限制地发送数据呢？实际上，环型网中的每个站点都有一个令牌保持时间定时器（Token Holding Timer，THT），由THT控制站点拥有令牌的时间。THT的时间一般为10ms，环型网也可以在初始化时设置其他值。由于数据帧的第1位将会遍历整个环，并在整个帧发送完之前就回到发送站点，因此发送站点在发送新帧之前，必须把环中的内容吸空。在发送网第1帧后，若余下的时间可以发送更多的帧，站点可以进行相应的数据发送。当待传帧发送完毕或者在发送另外一帧将超过令牌保持时间时，站点要释放令牌以便下一个站点可以发送数据。

IEEE802.5有令牌和数据/命令帧两种帧格式，如图5-9所示。令牌占用3个字节，有一位用于标记令牌忙闲。当令牌为闲时，表明环上没有站发送数据。当它为忙时，就变成一帧的帧首序列，其后面跟着一个数据/命令帧的其余部分。

a) 令牌格式



b) 数据/命令帧格式

图5-9 IEEE802.5帧格式

IEEE 802.5中帧的发送顺序也是从最左边的起始界符开始，但每个字节的传输是从最高位开始发送的，这与前面介绍的IEEE802.3正好相反，IEEE802.3帧中每个字节的发送顺序是从最低

位开始发送的。这一点对于两种不同局域网互连时要特别注意。

下面我们分别讨论令牌和数据/命令帧中各个字段的含义。

起始界符SD由无效数据位J、K和二进制0与1组成，SD字段中每一位的含义如图5-10所示。

J	K	0	J	K	0	0	0

图5-10 起始定界符SD的格式

如前所述，802.5物理层标准规定数据用差分曼彻斯特编码表示，由每位信号开始的极性来区分1和0，但在每位数据的中间要变换一次极性。无效数据 J和前面符号的极性相同，而无效数据K则和前面符号的极性相反，且J和K符号的中间极性都不变。

结束界符ED格式如图5-11所示。

J	K	1	J	K	1	1	E

图5-11 结束界符ED的格式

J、K的含义与SD中的一样。中间帧位I指示是传送最后一帧或单帧（I=0），还是传送多帧时的中间某帧（I=1），如同文件结束标志一样。 E位用来指示令牌或数据/命令帧是否有错误，一旦环接口检测到错误就将它置1。

访问控制字段AC提供访问介质所必需的信息，其格式如图 5-12所示。

P	P	P	T	M	R	R	R

图5-12 访问控制字段AC的格式

T位是令牌标志位。当 T=0时，表示该帧是令牌；当 T=1时，表示该帧为数据/命令帧。 PPP表示令牌的优先级。只有当某站点的优先级大于或等于令牌的优先级时，该站点才可以捕获此令牌并发送数据。令牌和站点共有8个优先级，从000到111。站点的优先级在环初始化时就确定，而令牌的优先级则由站点申请而确定。环上的站点可以通过 RRR字段预约下一个令牌的优先级。M位是供监控站使用的，监控站使用 M位来检测环是否正常运行，以防止令牌或数据 /命令帧在环上不停地旋转。有关如何通过 M位来检测环是否正常运行的详细过程将在 5.3.2节展开讨论。帧控制字段FC的格式如图5-13所示。

F	F	Z	Z	Z	Z	Z	Z

图5-13 帧控制字段FC的格式

其中FF用于表示是数据帧还是命令帧。 FF=00时，表示是命令帧，即 MAC帧。命令帧主要用于环的管理和维护，表 5-3给出了常用的命令帧的控制字段格式及它的功能介绍。 FF=01时，表示是数据帧，也称为 LLC帧，它用于携带高层的数据（ LLC层的数据）。FF=10或11两种状态暂时没有使用。对于数据帧， ZZZZZZ被设计成rrrYYY形式，rrr暂设置成000，作为备用，YYY则指示数据帧（LLC帧）的优先级。

表5-3 IEEE802.5命令帧

控制字段（ZZZZZZ）	名 称	功 能
000000	重复地址测试帧	重复MAC地址测试
000010	报警帧	确定环断点
000011	声明帧	申请成为监控站
000100	环初始化帧	重新初始化
000101	监控站广播帧	被监控站周期性调用
000110	潜在监控站广播帧	广播潜在监控站存在

802.5帧格式中的目的地址、源地址与802.3是一样的。目的地址也分唯一地址、组播地址、广播地址，而源地址都是唯一地址。

从环结构和协议本身来说，令牌环网对数据字段的长度没有限制。数据长度的限制主要来自于令牌保持时间定时器THT以及环接口的缓存器的大小。一般情况下，环中的数据长度缺省值为5000字节，足够应付高层协议的传送需求。

CRC校验码的含义与IEEE802.3是一样的，在此不再讨论。

在802.5 MAC帧格式中设有一个帧状态字段FS，它主要包括A和C两个标志位。当数据或命令帧到达目的站点的环接口时，环接口将对A和C进行置位。发送站点通过检查A和C位就可以知道刚才发送出去的数据帧是否被目的站点正确接收。如果A=0且C=0，则表示目的站点不存在或目的站点存在但未加电；如果A=1但C=0，则表示目的站点存在但数据/命令帧未被接收（帧出错）；如果A=1且C=1，则意味着目的站点存在且目的站点正确接收到数据或命令帧。

在802.5中引入FS字段，为发送站每发送一帧提供了自动确认机制，这点要优于802.3。因为在802.3中，应答帧是要接收站点额外发送的，而且它也要竞争信道，如果不加特殊处理，会使应答帧的延迟不确定。在FS字段中，A和C位均出现两次，这是由于FS字段没有被CRC码所保护。为了保证A和C的可靠性，A和C都重复地出现在FS字段中，FS字段的格式如图5-14所示。

A	C	r	r	A	C	r	r

图5-14 帧状态字段FS的格式

5.3.2 管理与维护

对于IEEE802.5环型网来说，管理和维护显得尤为重要。其原因是环容易出现物理故障导致环的中断或令牌的丢失；不管什么情况，都会导致环的不正常工作。

令牌环网采用分布式的管理方法。为了便于环型网的管理和维护，在协议中就提供了支持，增加了许多用于环管理和维护的命令或控制帧。同时令牌环网还引入了监控站（monitor station），由它来负责整个环的正常工作。

在环型网中，每个站点都可能成为监控站，监控站是通过竞争产生的。在环刚启动或重新初始化时，所有站点都发送声明帧，试图声明自己为监控站。竞争监控站的过程是：环中任意一个站点在接收到其上游站点发送或转发的声明帧时，将本站地址与声明帧中的源地址进行比较。如果本站地址大于声明帧中的源地址，则停止发送本站的声明帧，转发接收到的声明帧；

否则，继续发送本站的声明帧（地址最小的站点可以成为监控站）。如果某个站点接收到自己发出的声明帧，它就成为监控站。

监控站的职责是：确保令牌不丢失；在环断开时采取行动；当环中出现破损帧时清除掉；以及查看是否有无主帧出现。产生无主帧的的情况是：某站点将一短帧发送到环上，然而在该帧被取走之前，站点发生故障（如掉电）。如果不对无主帧采取措施，它将会在环上不停地旋转下去。

为了检查令牌是否丢失，监控站有一个定时器，它设置为最长无令牌时间。每个站点只能在令牌保持时间内发送数据；如果超过该时间，监控站将取走环内的帧，并产生一个新的令牌。

当环中出现破损帧时，监控站可以从其无效格式或校验码中检测到，然后监控站断开环取走破损帧，并产生一个新的令牌。

监控站对无主帧的检测是通过在访问控制字段 AC中设置监控位来实现的。若监控站发现某帧中的监控位已被置成“ 1 ”，则意味着同一帧经过监控站两次而未被取走，说明该帧可能是无主帧，所以监控站将帧从环中取走。

监控站的最后一项功能涉及环的长度。 802.5中的令牌长度是24位，这就意味着环必须至少能容纳24位。如果所有站点引入1位延迟，再加上电缆长度的延迟所得的和还小于 24位的话，监控站就插入额外的延迟，使令牌能够绕环工作。

监控站唯一不能解决的问题是：确定环断点的位置。也就是说，环型网中的监控站可以发现环断开了，但它不能具体确定断点的物理位置，而必须由管理员拿着所有机房门的钥匙打开机房逐段进行检查。为了解决上述问题，在令牌环中引入了报警机制。当一个站点发现其邻近站点好像失效时（包括线路），便发出一个报警帧并给出假定失效站的地址。同样的道理，其他站点也会发现环出现了故障因而也发出各自的报警帧。如果某个站点接收到其上游站点发送或转发的报警帧，则停止发送自己的报警帧。这样经过一段时间后，环上只存在某个站点发出的报警。此时只要打开任何一台机器检查一下其中的报警帧，就可以确定环断点的位置（发出报警帧站点的上游）。

上面我们介绍了报警过程。虽然报警过程可以确定环断点的位置，但环故障的恢复仍然需要人工干预。为了解决故障的自动恢复问题，可以采用类似于 802.3中集线器的设备，即每个站点通过有源集线器连在一起。

这种结构在逻辑上仍保持环状，而物理结构上每个站点通过两对双绞线电缆与线路中心相连，一对用于输入，一对用于输出。这种结构通常被称为星型环（ star-shaped ring）。在线路中心设有旁路开关，它由各个站点供电。如果线路或站点发生故障，旁路开关将自动将该站点隔离出去，以维持环的正常工作。

5.3.3 性能分析

令牌环网的工作过程可以用一个排队服务模型来描述，所有活跃站点构成一个发送队列。环中各站依次抓住令牌并发送数据。假设两个站点之间的传播延迟为 τ 。由于数据要沿环旋转一周返回到发送站点，因此目的站在环上的位置对分析令牌环网的性能没有影响。影响令牌环网性能的主要参数是数据传输率、电缆长度、令牌保持时间以及帧长度。

同样的道理，在对IEEE802.5令牌环进行性能分析之前，我们也需要定义一组参数，这些参数与IEEE802.3网络是一样的。延迟D用于表示一个站点从准备好发送数据到发送完数据所用的时间，吞吐量S表示通过网络所传输的数据量，利用率U表示网络吞吐量与总容量的比值。

同时我们仍然假定R为局域网的数据传输率，d为任意两个站点间的最大距离，V为信号在介质上的传播速度，L为帧的平均数据长度，那么根据前面的计算结果可知，在理想的情况下，802.5网络的的利用率U为：

$$U = \frac{1}{1+a}$$

其中α是网络传播延迟与数据发送时间之比，其值为：

$$a = \frac{d/V}{L/R} = \frac{Rd}{LV}$$

同样的道理，α值对令牌环网的性能有影响，随着α的增大，网络的吞吐率将下降。为了提高信道的利用率和网络的吞吐率，应尽量减小α。另外，令牌环网中，站点数目的增加也可以增加网络的吞吐率，这是由于站点数目的增加将减少传送令牌的时间，从而提高802.5协议的效率。

5.4 网桥

网桥（bridge）也称桥接器，是连接两个局域网的一种设备。网桥还可以用于扩展网络的距离、在不同介质之间转发数据信号以及隔离不同网段之间的通信。一般情况下，被连接的局域网具有相同的逻辑链路控制规程LLC，但在介质访问控制协议MAC上可以不同。网桥是为各种局域网之间存储转发数据而设计的，它对末端站点的用户是透明的。

网桥在相互连接的两个局域网之间起到帧转发的作用，它允许每个LAN上的站点与其他站点进行通信，看起来就像在一个扩展的局域网上一样。为了有效地转发数据帧，网桥自动存储接收进来的帧，通过查找地址映像表完成寻址，并将接收帧的格式转换成目的局域网的格式，然后将转换后的帧转发到网桥对应的端口上。

网桥除了具有存储转发功能外，还具有帧过滤的功能。帧过滤功能是阻止某些帧通过网桥。帧过滤有3种类型：目的地址过滤、源地址过滤和协议过滤。目的地址过滤指的是当网桥接收到一个帧后，首先确定其源地址和目的地址，如果源地址和目的地址处在同一个局域网中，就简单地将其丢弃，否则就将其转发到另一个局域网上。目的地址过滤是任何网桥的最基本的功能。源地址过滤是指网桥拒绝某一特定地址（站点）发出的帧，这个特定地址无法从网桥的地址映像表中得到，但可以由网络管理模块提供。而协议过滤是指网桥能用帧中的协议信息来决定是转发还是滤掉该帧。协议过滤通常用于流量控制和网络安全控制。并非每一种网桥都提供源地址过滤和协议过滤功能。

前面提到网桥的最主要功能是在不同局域网之间进行互连。由于不同局域网在帧格式、数据传输率、CRC校验等方面都不相同。例如，FDDI（将在下一章介绍）网络中允许的最大帧长度是4500字节，而802.3以太网的最大帧长度是1518字节。这样网桥在从FDDI向以太网转发数据帧时，就必须将FDDI长达4500字节的帧分割成几个1518字节长度的IEEE802.3帧，然后再将这

些帧转发到以太网上；反之，在从以太网向 FDDI转发数据帧时，必须将只有 1518字节的以太网帧组合成FDDI格式的帧，并以FDDI格式传输。以上这些过程都涉及到帧的分段和重组，帧的分段和重组工作必须快速完成，否则会降低网桥的性能。

另外，网桥还必须具有一定的管理管理，以便对扩展网络进行有效管理。例如，可对网桥转发及丢弃的帧进行统计，及时修改网桥地址数据库，某些类型的网桥还可以通过生成树算法动态调整扩展网络的拓扑结构以适应网络的变化。

网桥可分为封装式网桥（encapsulation bridge）和转换式网桥（translation bridge）、本地网桥（local bridge）和远程网桥（remote bridge）等。

封装式网桥是将某局域网的数据帧封装在另一种局域网的帧格式中，是一种“管道”技术。以FDDI-以太网封装式网桥为例，封装式网桥接收以太网上的帧，然后用专用协议技术来封装该以太网帧（接收站点的地址也被封装在 FDDI帧中）并转发到FDDI网络上；接收端的封装式网桥使用同样的专用协议技术拆封 FDDI帧并将已被拆封的帧转发到以太网上，由目的站点进行接收，如图5-15所示。

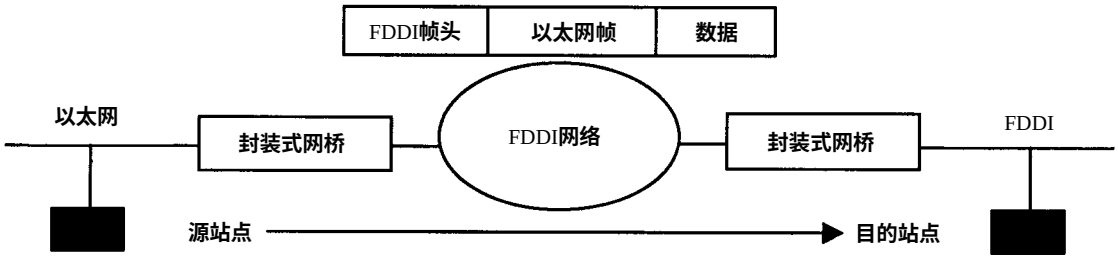


图5-15 FDDI-以太网封装式网桥

由于目的地址被封装在FDDI帧中，因此封装式网桥只能采用广播方式发送 FDDI帧，这无疑会降低FDDI网络带宽的利用率。另外封装式网桥必须成对出现；同时，由于在封装式网桥中使用了专用的协议，使得由不同厂商生产的封装式网桥之间存在互操作问题，因此成对使用的封装式网桥必须是一个厂商生产的。最后，在使用封装式网桥的扩展网络中，不同网络之间的站点不能通信。如在图 5-15中，以太网中的工作站不能与 FDDI网络中的服务器进行通信，只能是FDDI网络中的主机可以通信，两个以太网网中的主机可以经过 FDDI网络进行通信。

转换式网桥需要在不同的局域网之间进行帧格式的转换，它克服了封装式网桥的弊病。将图5-15中的封装式FDDI-以太网网桥改为转换式网桥后，以太网网上的工作站就可以访问 FDDI网上的高性能服务器了。

本地网桥是指在传输介质允许范围内完成局域网之间的互联。远程网桥是指两个局域网之间的距离超过一定范围需要用点到点线路或广域网进行连接的网桥，远程网桥必须成对使用。

下面我们主要讨论两种最常见的网桥：透明网桥和源选径网桥。

5.4.1 透明网桥

透明网桥是由DEC公司针对以太网提出的桥接技术。透明网桥的基本思想是：网桥自动了解每个端口所接网段的机器地址（MAC地址），形成一个地址映像表，网桥每次转发帧时，先查

地址映像表，如查到，则向相应端口转发，如查不到，则向除接收端口之外的所有端口转发或扩散（flood）。

为了说明透明桥的工作原理，我们先看图 5-16的例子。

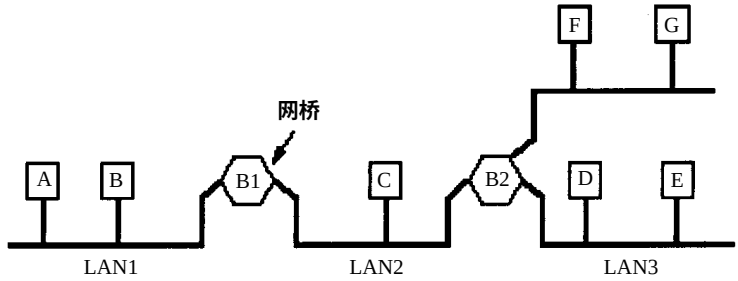


图5-16 4个局域网和2个网桥的配置

图5-16中，网桥B1连接LAN1和LAN2，网桥B2连接LAN2、LAN3和LAN4。LAN1中站点发出的帧到达网桥B1且目的地址为A的帧可立即被丢弃，这是因为A在LAN1上；而目的站点为C、E或F 的帧则必须经过B1桥转发。

当桥接收到一帧后，必须决定是转发还是丢弃该帧。如果需要转发，则必须决定发往桥的哪个端口。这需要通过查阅桥中地址映像表来确定，该地址映像表可列出每个可能的目的站点地址，以及它将通过桥的哪个端口。对于上述例子， B2桥的地址映像表中列出 A要经过LAN2（意味着桥B2接收到目的地址为A的帧时，将发往连接LAN2的端口），因为桥B2只需知道把目的地址为A的帧发往LAN2即可。

透明网桥是通过逆向学习算法（ backward learning）来填写地址映像表的。当桥刚接入时，其地址映像表是空的，此时，网桥采用扩散技术将接收的帧转发到桥的所有端口上（接收端口除外）。透明网桥通过查看转发帧的源地址就可以知道通过哪个 LAN可以访问某个站点。在图5-16中，桥B1从LAN2上接收到来自C的帧，那么它就可以得出结论：经过 LAN2肯定能到达C。于是，桥B1就在其地址映像表中添上一项，注明发往站点 C的帧应经过LAN2。如果以后桥B1收到来自LAN1且目的地址为C的帧，它就按照该路径转发；如果收到来自 LAN2且其目的地址为C的帧，则将此帧丢弃。

为了提高扩展局域网的可靠性，我们可以在 LAN之间设置并行的两个或多个网桥，如图 5-17所示。但是，这样配置引起了另外一些问题，因为在拓扑结构中产生了回路。

通过观察上图如何处理目的地址不明确的帧 F，就可以简单地了解这些问题。按照前面提到的算法。对于目的地址不明确的帧，每个网桥都要进行扩散。在本例中，即只是将其复制到LAN2中。紧接着，桥B1看见目的地不明确的帧F2，将其复制转发到LAN1，产生一个新帧，如F3（图中未画出）；类似地，桥 B2也将F1复制转发到LAN1，产生F4。随后，桥B1又复制转发F4，而桥B2则复制转发F3，无限循环下去。

解决这个难题的方法是让桥相互通信，并用一棵覆盖到每个 LAN的生成树（spanning tree）覆盖实际的拓扑结构。生成树网桥是 DEC公司针对透明网桥中存在的环路问题而提出的， IEEE将其标准定义为802.1d。

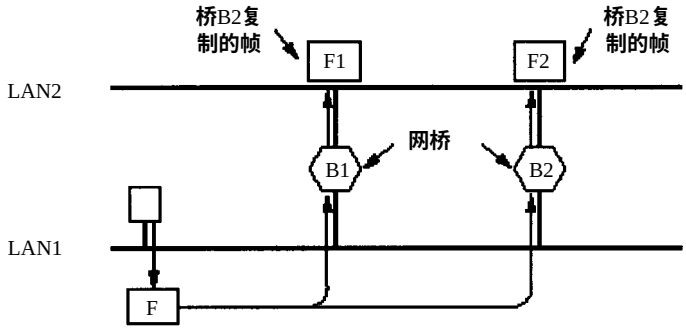


图5-17 两个并行的透明网桥

我们知道，任何一个由多个网段经网桥连接在一起构成的扩展局域网都可看作是一个无向图。在这个无向图中，每个网段和每个网桥相当于一个结点（ node），网段与网桥之间的连接相当于一条边（edge）。

图论中的结论是：“ 对于任何一个由多个结点和连接一对结点的边构成的连接图，都存在一棵部分边组成的生成树，既可保持图中各结点的连通性，同时又不存在环路 ”。 一旦得到覆盖所有LAN的生成树，就能保证任意两个LAN之间只存在唯一的路径，故不会构成环路。

下面我们通过图5-18的例子，来说明如何构造扩展局域网的生成树。

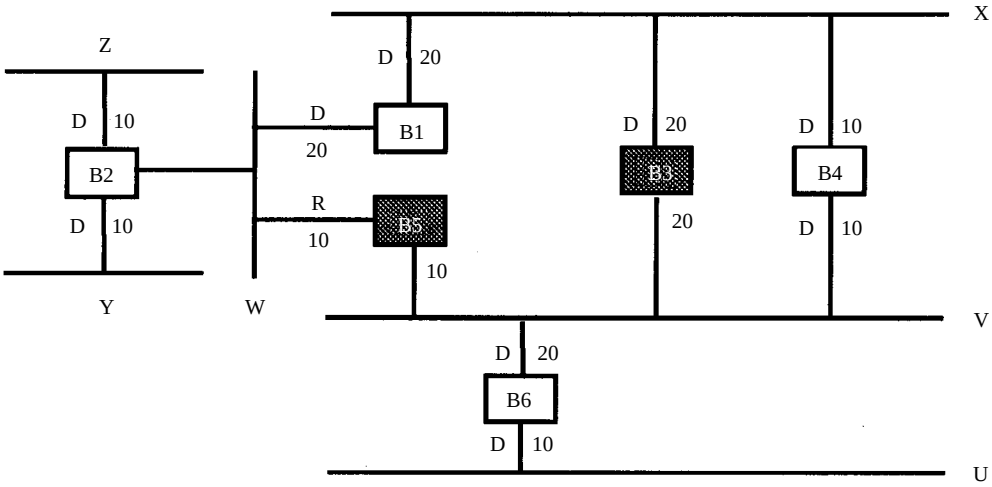


图5-18 扩展局域网的拓扑结构

假定每个桥有一个唯一的标识（该标识由厂商设置并保证全球唯一，例如可以是桥某一端口的MAC地址），桥到每个LAN的连接有一个代价（cost）。则生成树的构造算法为：

(1) 选择标识号最小的桥为生成树的根（图 5-18中为B1）。

(2) 确定除根之外的其他网桥的 Root 端口（Root Port），它是该桥到根代价最小的端口。

(3) 确定每个LAN上的指定桥（Designated Bridge）。指定桥是提供每个网段到根代价最小的桥（图5-18，网段Z的指定桥为B2，Y为B2，V为B4，U为B6，W为B1，X为B1）。如果有多个

桥到根的代价相同，则选标识号最小的桥作为该网段的指定桥。只有指定桥才可以在网段间转发帧。

(4) 确定每个网段的指定端口（Designated Port）。每个网段与其指定桥相连的端口叫指定端口。

(5) 最后每个网桥将非根端口和非指定端口置为阻塞状态，即该端口不转发帧。

此算法的结果是建立起从每一个LAN到根的唯一路径，从而它也是到每个其他LAN的唯一路径。虽然此树横跨全部的LAN，但这并不是说所有的桥必须在此树之中。当生成树建立以后，此算法还要继续工作，以便自动地检查拓扑结构的变化及更新该树。图 5-17经过生成树算法后的结果如图5-19所示。在执行生成树算法过程中各网桥之间需要不断交换各自的信息，交换的信息有一定的格式，在此不再展开讨论，有兴趣的读者可以查看IEEE802.1d文档。

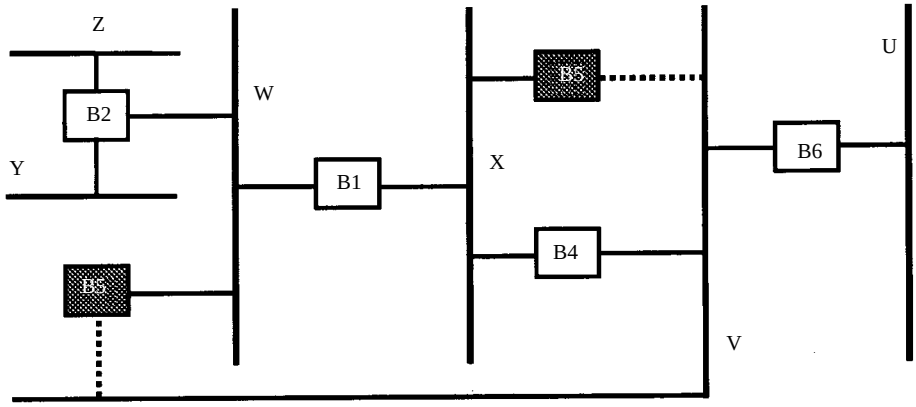


图5-19 覆盖所有LAN的生成树，虚线不是生成树的一部分

5.4.2 源选径网桥

源选径网桥（Source-Route Bridge，SRB）是由IBM公司针对其802.5令牌环网提出的一种网桥技术，属于IEEE802.5的一部分。其核心思想是发送方知道目的机的位置，并将路径中间所经过的网桥地址包含在帧头中一并发出，路径中的网桥依照帧头中的下一站网桥地址将帧一一转发，直到将帧传送到目的地。

为了说明源路径网桥的工作原理，我们先来考察图5-20的例子。

对于图5-20的例子，H1想向H2发送数据帧，则H1首先发送一个测试帧以检测H2是否与H1在同一网段上；如果测试后发现H2与H1不在同一网段上；则H1将进行下列动作：

第一步，H1发出一个探测帧，探测H2的所在位置。

第二步，桥B1和B2都收到H1发出的探测帧，它们分别在探测帧中加进路由信息，然后将探测帧分别转发到LAN3和LAN4。

第三步，桥B3和B4也收到H1发出的探测帧，它们也分别在探测帧中加进自己的路由信息，然后继续将探测帧转发到LAN2。

第四步：H2收到两个探测帧，H2检查探测帧中累积的路由信息，然后分别沿着探测帧来的

路径发响应帧。

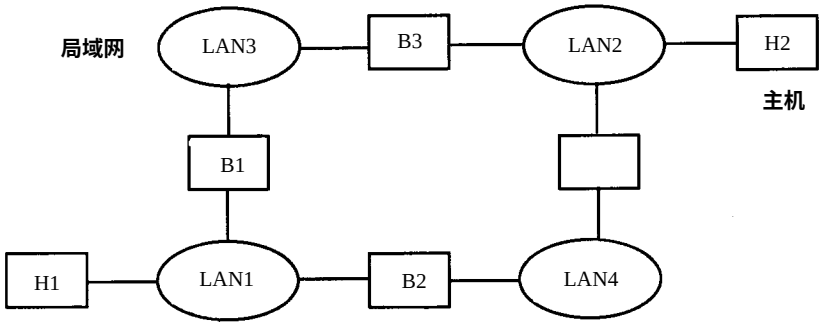


图5-20 4个源路径网桥和4个局域网的配置

第五步：H1收到两个H2发来的两个响应帧，从而得知有两条路径可以到达 H2，分别为：LAN1→B1→LAN3→B3→LAN2和LAN1→B2→LAN4→B4→LAN2

最后H1选择其中一条路径，将路由信息加到数据帧中发给 H2。

需要注意的是，源路径网桥必须对 802.5的帧格式进行扩充。如果 802.5帧格式中的源地址字段最高位为“ 1 ”，则表明源地址字段之后还有一个路由信息字段 RIF （Route Information Field），该字段包含了如何到达目的结点的路径信息；并将 802.5帧格式中的源地址字段最高位称为路由信息标识符（Route Information Indicator，RII）。

源选径网桥只关心源地址字段中 RII位为“ 1 ”的帧。对于这些帧，网桥扫描 RIF字段并根据RIF中的路由信息进行帧的转发。

5.5 小结

局域网一般使用广播式信道。在广播式信道中，关键的问题是如何协调控制多个站点对共享信道的同时访问，这就涉及到信道分配策略。不同的分配策略将导致网络具有不同的性能。

传统的局域网主要有以太网、令牌环网。这两种网络在数据传输率、物理层编码、帧格式、网络的管理与维护以及性能方面都有很大的差异，适合不同的使用环境。

当某个单位构建的网络中要使用多种不同的局域网技术时，必须引入网桥设备，以使不同局域网上的用户能够相互通信。网桥主要分为透明网桥和源选径网桥两种。

习题

1. 纯ALOHA的延迟和分槽ALOHA的延迟相比，哪一个更小？请说明原因。

2. 标准10Mbps的IEEE 802.3 LAN的波特率是多少？

3. 长度为1km，数据传输率为10Mbps的以太网，电信号在网上的传播速度是 200m/（s。数据帧的长度为256比特，包括32比特帧头、校验和及其他开销。数据帧发送成功后的第一个时间片保留给接收方用于发送一个 32比特的的应答帧。假设网络负载非常轻（即没有冲突），问该网络的有效数据传输率是多少？

4. 数据传输率为5Mbps的令牌环接口中的1比特延迟的等效物理长度是多少？电信号的传播

速度是200m/（s。

5. 令牌上的环绕时延必须能够容纳整个令牌。如果电缆长度不够，必须人为地增加时延。请解释一下，为什么在时延只有16比特、而令牌为24比特的环型网上，必须额外地增加时延。

6. 在一个4Mbps的令牌环中，站点的令牌保持时间为 10ms。问在此环上可以发送的最大帧的长度是多少？

7. 长度为1km，数据传输率为 10Mbps、重负载的令牌环网，电信号在网上的传播速度是200m/μs 。在环上有50个等距离的站点。数据帧的长度为 256比特，包括32比特帧头、校验和及其他开销。应答帧附带在数据帧中，令牌为 8比特。问该环型网的有效数据传输率是多少？比10Mbps的CSMA/CD网的有效数据传输率相比，这个数据传输率是高还是低？

8. 什么是封装式网桥，它有什么优缺点？

9. 请说明透明网桥中生成树的作用及其构造过程。

10. 请描述源选径网桥的工作过程。

第6章　高速局域网

上一章主要介绍传统的局域网：以太网和令牌环网。随着通信技术的发展以及用户对网络带宽需求的增加，迫切需要建立高速的局域网。下面我们介绍几种常见的高速局域网。

6.1　FDDI网络

光纤分布式数据接口（Fiber Distributed Data Interface，FDDI）是世界上第一个高速局域网标准。

20世纪80年代初，正当以太网和令牌环网技术如日中天之时，大多数人都还沉浸在新的网络技术带来的10Mbps高传输速率的喜悦之中，就有一些有远见的网络工作者已看到其中的不足，断定在不远的将来网络传输业务的需求将超过现有网络带宽，网络带宽将会成为未来信息业发展的瓶颈。

首先他们注意到了光纤通信技术的最新成果。光纤通信技术以其巨大的信息容量、很低的信号衰减和高度的可靠性著称于世。这项始于 20世纪70年代的新兴通信技术，以其无比的优越性和蓬勃的生命力受到了广大网络设计者的青睐，一举成为新一代网络技术的首选传输介质，并以此为基础形成了FDDI光纤网络技术。

设计人员以业已成熟的IEEE 802.5令牌环网技术为基础，开发出一种称之为反向双环的技术。它以增加一条光纤链路为代价，提高了网络系统的可靠性；用改进的定时令牌技术，能够同时进行多数据帧的传输，扩大了带宽利用率，达到了大容量数据传输的目的。

经过ANSI的ASC X3T9.5委员会长达近十年的不懈努力，这项技术终于被国际标准化组织ISO正式接纳为国际标准。

为适应日新月异的市场需求，设计人员以 FDDI作为一个基本协议集，又先后开发出了铜缆标准CDDI，为多媒体而设计的FDDI-Ⅱ，以及最新的大容量网络系统 —— FFOL局域网改进标准（FDDI Follow On LAN，FFOL），FFOL的传输速率最高可达2.4Gbps。

6.1.1　FDDI与OSI的关系

FDDI标准主要由四个部分组成，按其完成时间顺序依次为：介质访问控制（ Medium Access Contro，MAC）子层，物理（PHYsical，PHY）子层，物理介质相关（Physical Medium Dependent，PMD）子层，站管理（Station ManagemenT，SMT）。它们实现了OSI参考模型的物理层和数据链路层的功能。图6-1给出了两者之间的相互关系。

FDDI将OSI的物理层分成PHY子层和PMD子层两部分。其中最低的子层是 PMD，这是整个网络中唯一真正与物理介质打交道的层次，它定义了光纤和连接器的规格型号以及光传输的接口特性要求等内容。较高的子层是 PHY，它规定了线路的状态、时钟处理和编码技术等方面的细节。而FDDI数据链路层的功能也由两个子层来实现，即是 MAC和LLC。其中较低的子层是

MAC，主要完成令牌管理、差错检测、寻址、介质访问和数据帧结构定义等功能。较高的子层是IEEE 802.2逻辑链路控制LLC子层。该子层不属于FDDI标准的范围。FDDI的站管理SMT的作用是实现对上述几个层次的有效控制，加强网络管理能力。 FDDI提供了专门的站管理功能，包括连接管理、结点配置、故障恢复等内容。

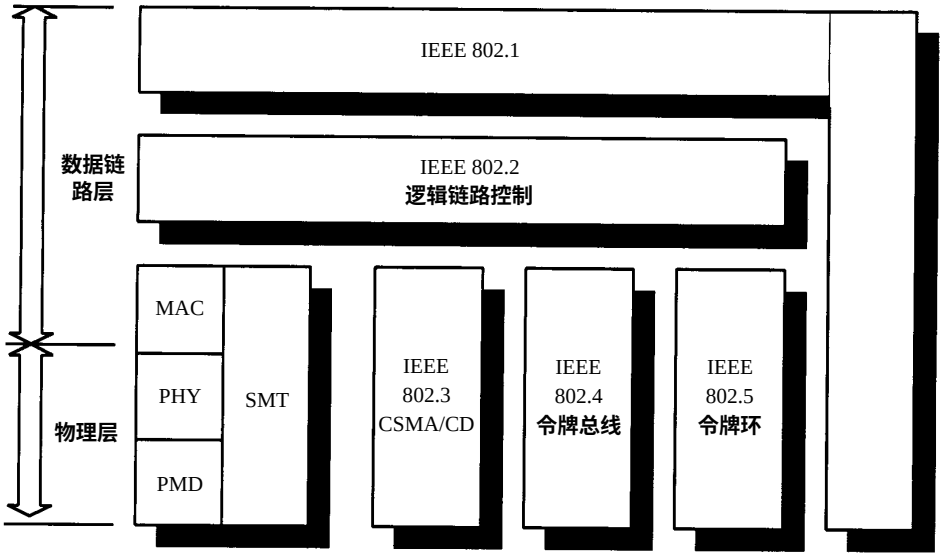


图6-1 FDDI与OSI参考模型关系图

6.1.2 帧格式

与IEEE 802.5令牌环协议相似，FDDI中的MAC子层协议也定义了令牌和数据/命令帧两种帧格式。

FDDI的帧由若干个字段组成，这些字段分别为帧起始符、帧控制、源地址、目的地址、数据、帧校验序列、帧结束符以及帧状态符。

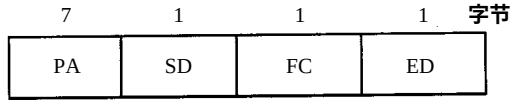
令牌包括MAC帧，数据/命令帧包括SMT帧和LLC帧。MAC帧主要用于传送控制信息，包括声明帧和报警帧。声明帧用于产生新的监控站，报警帧确定环的断点位置。而 SMT帧用于传送FDDI环的控制、操作和管理信息。只有LLC帧是用来传送用户数据的。

令牌是FDDI环上各站点传送信息的“通行证”。根据FDDI MAC子层的规定，任何站点要传送数据时，首先必须捕获到令牌。数据传送结束或站点的令牌保持时间定时器超时后，站点将重新产生令牌并将其发送到FDDI环上，供其他站点使用。

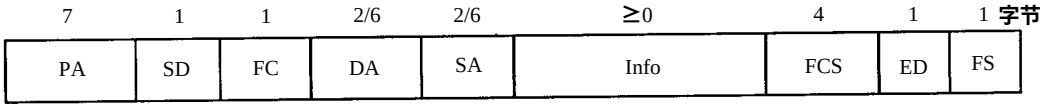
在FDDI网络中，令牌是一个特殊的帧，它也由若干个字段组成。 FDDI的令牌分为受限令牌和非受限令牌两种类型。

无论哪一种FDDI帧，都有一个通用的帧格式。图6-2描述了FDDI帧和令牌的格式。

FDDI令牌和帧格式中各个字段的的含义与IEEE802.5令牌和帧格式中各个字段的含义非常类似。下面我们将简单讨论FDDI帧中各字段的含义。



a) 令牌格式



b) 帧格式

图6-2 FDDI令牌和帧的格式

前导符PA用于接收站点的时钟同步。起始符SD指示一个帧的开始。帧控制FC字段用来指明帧的类型、寻址方式等。FC字段的长度为8位，其格式为CLFFZZZZ，其中C指明是同步帧还是异步帧，L指明是使用16位地址还是48位地址，FF指明是MAC帧、LLC帧还是SMT帧。表6-1描述了FDDI帧结构中FC字段的各种取值及其相应含义。

表6-1 帧结构中FC字段的取值及其含义

FC字段取值（CLFF ZZZZ）	帧 类 型	含 义 说 明
0X00 0000	无效帧	逻辑上不是一个帧
1000 0000	非受限令牌帧	用于同步传输和不受限制的异步传输
1100 0000	受限令牌帧	用于同步传输和受限制的异步传输
1L00 0001~1111	MAC服务帧	MAC与LLC的服务关系
1L00 0010	MAC报警帧	指明环路出现了故障
1L00 0011	MAC声明帧	用于环路的初始化
0L00 0001~1111	SMT管理帧	包含站管理控制信息
0L00 1111	SMT地址帧	用于站管理
CL00 r000~r111	LLC数据帧	包含用户数据
0L01 rPPP	LLC同步帧	具有优先级PPP的同步传输
1L01 rrrr	LLC异步帧	用于异步传输
CL10 r000~r111	为系统保留	与系统的实现有关
CL11 rrrr	为标准化保留	用于将来的标准化定义

目的地址DA字段用于指明该帧的目的站点。从地址长度来看，它可以是16位地址或48位地址；从地址类型来看，它可以是唯一地址或单播地址、组播地址或广播地址。源地址SA字段用于指明产生该帧的站点地址。信息Info字段是用户数据。帧检验序列FCS字段是32位的CRC校验码，它覆盖的范围包括FC、DA、SA、Info 4个字段。帧结束符ED表示该帧结束。帧状态FS字段描述了该帧在传输过程中的状态，它包含差错检测位E、地址识别位A、拷贝位C等。

6.1.3 MAC协议

在这小节中，我们将讨论FDDI网络的定时令牌协议以及FDDI的介质访问控制MAC协议方式，并将它与IEEE802.5 MAC协议进行比较。

1. 定时令牌协议

FDDI 的MAC子层采用定时令牌循环协议（Timer Token Rotation Protocol，TTRP）来控制站点对环的访问。

定时令牌协议规定每个站点都设有三个定时器：目标令牌循环时间（ Target Token Rotation Time，TTRT）定时器、令牌循环时间（ Token Rotation Time，TRT）定时器和令牌保持时间（Token Holding Time，THT）定时器。目标令牌循环时间（TTRT）是指一个站点连续两次获得令牌的时间间隔，TTRT的值在环初始化时进行设置。令牌循环时间（ TRT）是指一个站点发送完数据到下次获得令牌的时间间隔，TRT的大小反映了网络当前的负载状况。令牌保持时间 THT是指站点在抓住令牌后可以发送数据的时间。当 THT时间片到，站点必须立即释放令牌。它们三者之间的关系是THT等于TTRT减去TRT。

定时令牌协议规定获取令牌的站点在发送完数据后，便可立即产生一个新的令牌发送到环上，而不必等到吸收完本站发送的数据。

定时令牌协议支持帧的成批同步传输，也支持突发异步传输及混合传输方式；另外 FDDI的定时令牌协议还允许两个站点独占整个信道，支持站点之间的多帧对话。

2. 介质访问控制

FDDI的介质访问控制涉及到三个方面的问题：帧的发送、帧的接收和帧的删除。

根据FDDI的定时令牌协议，当所有站点都没有数据要发送时，令牌就绕环不停地循环。需要发送数据的站点必须等到令牌经过它并将令牌吸收后，才能开始发送数据。当发送完数据或令牌保持时间定时器超时后，站点立即产生一个新的令牌并将其发送到环上。环上的其他站点根据帧的目的地址判别是否接收该帧。数据帧绕环旋转一周后，由发送站点负责将该帧移去。

FDDI介质访问控制方式与IEEE 802.5相比有两个新的特点。第一，FDDI站点捕获令牌不是通过改变令牌的某一个位来实现，而是把令牌“吸收”掉。 FDDI的令牌不再与数据帧一起发送到环上。第二，FDDI站点一旦完成其数据帧的发送，立即生成新的令牌发送到环上。因此，在FDDI网络中，可能有多个站点发送的数据帧在环上绕行。

6.1.4 工作原理

FDDI的工作原理主要体现在FDDI的三个主要过程中，这三个主要过程是站点物理连接建立、环初始化和数据传输。

1. 站点物理连接建立

FDDI网络在正常运行时，站管理 SMT一直监视着环的运行状况并管理着所有站点的活动。站管理SMT中的连接管理模块负责在站点的每对 PHY/PMD之间的双向光缆上建立起端到端的物理连接。站点通过传送与接收某些特定的线路状态序列来与其相邻站点交换端口类型和连接规则等信息，并对物理连接的质量进行测试。在测试过程中，一旦检测到故障，就用跟踪诊断的方法来确定故障原因，对故障进行隔离，并对网络进行重新配置。

2. 环初始化

在完成站点的物理连接后，接下去的工作便是对环进行初始化。在进行环的初始化工作之前，首先要确定系统的目标令牌循环时间 TTRT。各个站点都可借助声明帧提出各自的 TTRT值。

系统按照既定的竞争规则来确定 TTRT的值，由被选中 TTRT值的那个站点来完成环的初始化工作。确定TTRT值的过程通常叫做声明过程。

声明过程是用来确定TTRT值的。当某个站点或多个站点的 MAC实体发出声明请求时，环进入声明过程。在声明过程中，每个站点连续不断地发送声明帧。声明帧包含站点源地址和目标令牌循环时间TTRT。环上其他站点接收到某个声明帧后，将声明帧中的 TTRT值与本站的TTRT值进行比较。如果前者大于后者，站点就转发声明帧，同时停止发送自己的声明帧；如果前者小于后者，该站点就删除此声明帧，并发送自己的声明帧。声明帧中包含本站建议的 TTRT值。当某个站点接收到自己发出的声明帧，该站就赢得了对环进行初始化的权力。如果两个或更多的站点使用的TTRT值相同，那么地址值最大的站点将优先赢得对环进行初始化的权力。

赢得初始化环权力的站点通过发送一个令牌来初始化环，这个令牌将不会被环上的其他站点捕获而通过环。环上的其他站点在接收到该令牌后，将重新设置自己的工作参数，使本站点从初始化状态转为正常工作状态。当该令牌回到源站点时，环初始化工作宣告结束，环路进入稳定操作状态，各站点便可以进行正常的数据传送。

3. 数据传输

FDDI数据传输包括数据发送、接收和删除三个过程。

在FDDI环网中，想要发送数据的站点必须等待令牌到达该站点并将令牌捕获后，才能发送一个或多个数据帧，直到所有数据发送完或直到 THT超时为止。最后，站点释放一个新令牌到环。

FDDI环上的每一个站点随时都在监听经过本站点的帧，站点通过比较帧中的目的地址来决定是否接收该帧。如果该帧的目的地址与站点地址匹配，站点接收该帧，同时将此帧 FS字段的“A”标志位置“1”，表示目的站点存在；在接收该帧的同时，站点还对该帧进行差错校验。如果没有发现错误，则站点将帧中的数据字段复制下来，并在该帧 FS字段的“C”标志位置“1”，表示该帧已被目的站点接收；如果发现 CRC错，则在该帧FS字段的“E”标志位置“1”。请注意，在FDDI环网中，站点在接收帧的同时，还要把该帧转发到下一站点。

发送站点在发送完数据后将继续监听经过站点的帧。当发送站点检测到某数据帧的源地址与本站点的地址相同时，立即停止转发该帧并将其置为无效帧，使已转发到环上的部分帧信息在到达下一站点时被当做帧碎片而丢弃，以免这些帧碎片在环上继续绕行。然后发送站点负责将该帧剩余部分从环上删除，并同时检查帧中的 FS字段。如果FS字段中“A”和“C”标志位都为“1”，则说明该帧已被目的站点成功接收；如果只有“ A”标志位为“1”则说明目的站点存在但没有接收该帧，这说明帧在传输过程中发生了错误；如果“ A”和“C”标志位都为“0”，则说明帧中的目的地址有错。

6.1.5 拓扑结构

FDDI一般采用反向双环的拓扑结构。在FDDI双环中，一个环称为主环，另一个环称为辅环，两个环的数据传输方向相反。正常情况下，只有主环工作，而辅环作为备份。一旦网络发生故障，无论是线路故障还是站点故障， FDDI网络都会通过卷绕自动将双环重构为一个单环，从而保证网络不会中断，这是FDDI区别于其他局域网的一个重要特点。

FDDI网络支持两种类型的工作站：双连接站（Dual Attachment Station，DAS）和单连接站（Single Attachment Station，SAS）。DAS工作站包含两套物理层器件（PMD和PHY）以及一个或两个MAC实体，它可直接连在FDDI双环主干网上。当DAS工作站发生故障时，可以通过卷绕或光旁路开关将该站点隔离出去。而SAS工作站只包含一套物理层器件和一个MAC实体，它必须通过一个称为集中器的设备才能连入FDDI网络。

在FDDI环上还有两种类型的设备：双连接集中器（Dual Attachment Concentrator，DAC）和单连接集中器（Single Attachment Concentrator，SAC）。这两种设备用于将工作站连入FDDI环上。DAC可以直接连在FDDI双环主干网上，它本身可以与多个SAS、SAC、DAS以及其他DAC相连。而SAC主要用于将多个SAS连在一起，而SAC本身必须通过DAC才能连入FDDI双环主干网。

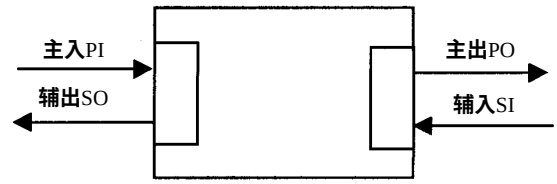


图6-3 FDDI DAS和DAC的A、B端口

DAS和DAC至少有两个物理接口，分别称为A端口和B端口，A端口和B端口用于将DAS和DAC连入FDDI双环主干网上。A端口包含主环输入（Primary Input，PI）和辅环输出（Secondary Output，SO），B端口包含主环输出（Primary Output，PO）和辅环输入（Secondary Input，SI），如图6-3所示。SAS工作站的物理接口称为S端口，集中器上的物理接口称为M端口。

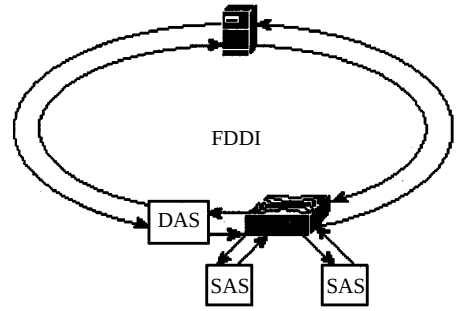


图6-4 FDDI网络物理结构连接示意图

FDDI网络在逻辑上是双环结构。但在物理上，FDDI网络可以有各种类型的拓扑结构。星型结构是由一台FDDI集中器连接多台计算机构成；环型结构是由多个双连接站DAS首尾相接构成；而树型拓扑则由星型和环型混合而成。图6-4给出了FDDI网络树型拓扑结构连接示意图。

6.1.6 网络容错

FDDI的一个重要特点是具备网络容错功能。FDDI的双环拓扑结构保证了网络在出现单个故障情况下还能正常工作，这就需要FDDI网络具有故障隔离和网络重构的功能。。

图6-5给出各种故障情况下网络如何进行重构。若FDDI网络出现单个故障，包括单个线路故障和单个站点故障，FDDI将把双环结构重构为一个单环网络，如图6-5b和图6-5c所示；而当网络上出现两个或多个故障（包括线路和站点故障），FDDI将把网络分成多个相互独立的子网段，如图6-5d所示。

除了上面提到的环重构的容错方法外，FDDI网络还提供另外一种容错方法。这种方法是在FDDI站点中引入可配置的光旁路开关。当FDDI工作站出现故障时，光旁路开关被启动，进行重新配置以切断站点与光纤环的连接，让光信号从上游站点通过光旁路开关直接连到下游站点，

绕过有故障的站点，从而将故障隔离，如图 6-6所示。

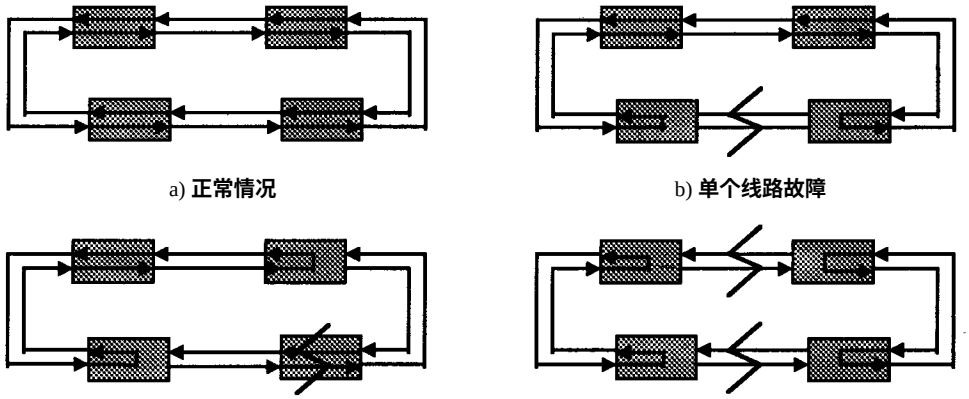


图6-5 FDDI网络重构的各种情况

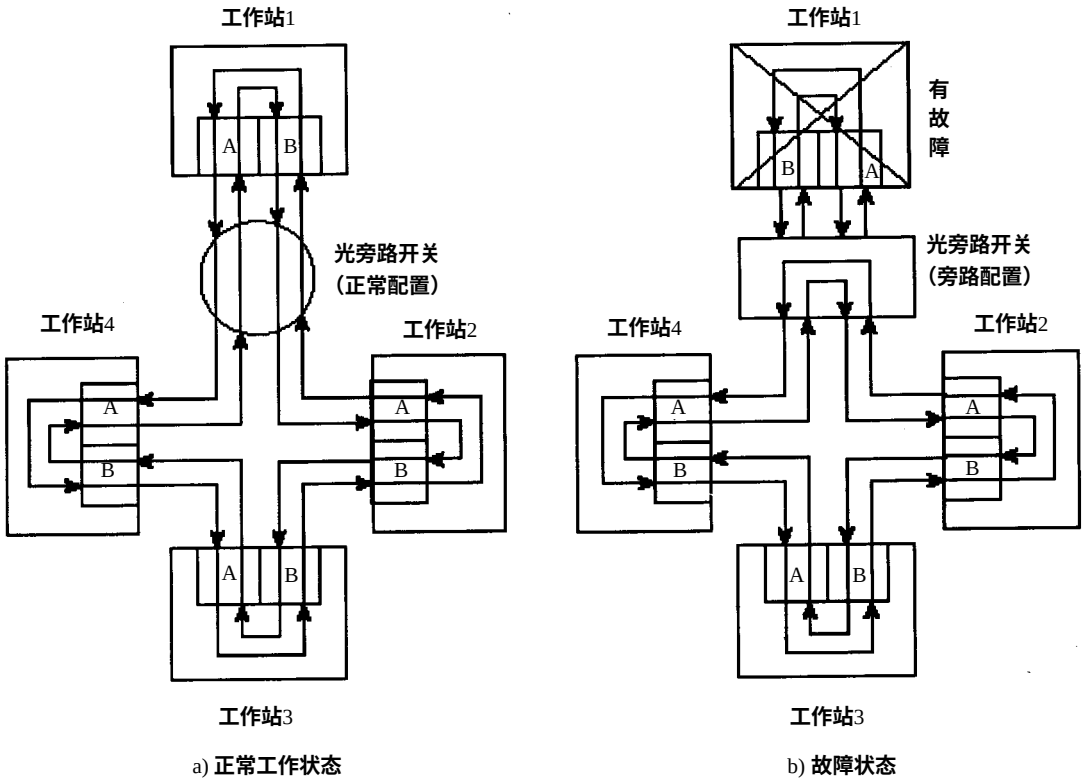


图6-6 光旁路开关

在FDDI网络中，双环冗余和光旁路开关两种容错措施都是为了解决环或站点故障，但这两种措施对于集中器发生故障的情况就无能为力了。在许多高可靠性的场合，要求服务器或路由

器等关键设备与网络的连接必须非常稳定、可靠。为此FDDI网络还提供了另外一种容错措施，即双归宿（dual homing）技术，简称双归。双归技术就是将服务器或路由器分别连到两个集中器上。正常情况下，服务器或路由器通过其中一个集中器与FDDI网络相连，而当此集中器出现故障时，将自动切换到另一个集中器，以保证服务器和路由器等关键设备与网络的连通性。FDDI网络的双归接法如图6-7所示。

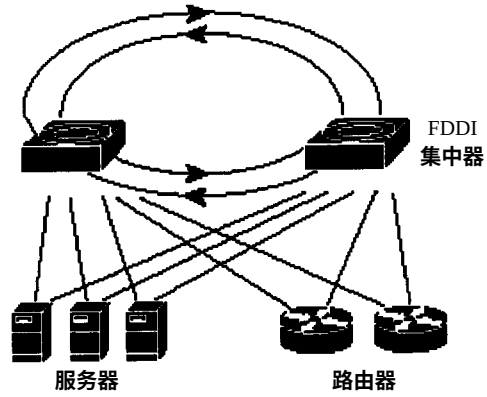


图6-7 FDDI双归连接示意图

6.1.7 技术指标

FDDI由于采用了光纤作为传输介质，同时又增加了容错处理能力，从而使其具有独特的优越性，概括起来主要有如下几点：

(1) 高带宽

FDDI充分利用了光纤通信技术带来的高带宽，以125MHz的时钟频率实现100Mbps的数据传输速率，比传统的局域网提高了10倍的数据传输能力。

(2) 大容量

在100Mbps传输速率的基础上，FDDI还采用了多数据帧的处理方式，大大提高了网络带宽的利用率，真正做到了大容量的数据传输。

(3) 长距离

光纤介质传输损耗非常低，因而使得光纤介质的不间断传输距离可以很长。多模光纤的不中继传输距离为2公里，而单模光纤的传输距离则可达40~100公里。

(4) 高可靠性

由于在FDDI网络的拓扑结构设计中采用了独特的双归冗余技术，使得FDDI网络的可靠性大大提高。FDDI网络在各种故障情况下都能正常运行。

(5) 安全性好

光纤介质是通过光信号传输数据的，因而它不产生任何电磁辐射，也不受各种电磁干扰的影响。因此FDDI可在强电流和强干扰等恶劣环境下使用，并能保持数据传输的高度可靠和安全。表6-2给出了FDDI网络的一些技术指标。

表6-2 FDDI的主要技术指标

项 目	指 标
拓扑结构	树型、双环、混合型
物理频宽	125MHz
数据传输率	100Mbps
介质访问方式	定时令牌协议
延时时间	10~200毫秒

（续）

项 目	指 标
有效负荷	99.5%
最大帧尺寸	4500字节
网上最大结点数	500个
最大站间距离	2公里（多模光纤），100公里（单模光纤）
最大环型网总长度	100公里

6.2 快速以太网

FDDI曾被认为是新一代的LAN，但是除了在主干网市场外，FDDI很少被使用。原因在于FDDI协议过于复杂，从而导致FDDI协议芯片复杂且价格昂贵。FDDI的昂贵价格使得它很难成为桌面用户的标准配置，从而影响了厂商的积极性，使得FDDI不能占据大块市场。人们从中得到的教训就是必须保证产品的简单和易用。

由于FDDI的不普及，为向10Mbps以上LAN发展留下了一个空间。正是在这种环境下，1992年IEEE重新召集了802.3委员会，指示他们制定一个快速的LAN协议。但在IEEE内部出现了两种截然不同的观点。一种观点是建议重新设计MAC协议和物理层协议，使用一种“请求优先级”的介质访问控制策略。它采用一种具有优先级、集中控制的介质访问控制方法，所以比我们熟悉的CSMA/CD控制方法更适合于多媒体信息的传输。支持这种观点的人组成自己的委员会，建立了他们自己的LAN标准，即IEEE802.12，常被称为100VG-AnyLAN。但由于它不兼容原先的以太网，所以后来的发展不大。另一种观点则建议保留原来以太网的CSMA/CD协议及帧格式，同时为了节省时间，在物理层没有重新设计新协议，而是“嫁接”了FDDI物理层协议。只是后来为了兼容原先10兆以太网的布线系统，又设计了可以使用3类非屏蔽双绞线的物理层协议。

802.3委员会之所以决定保持802.3原状，主要考虑到下面三个原因：①与现存成千上万个以太网相兼容；②担心制定新的协议可能会出现不可预见的困难；③不需要引入更多新技术便可完成这项工作。制定协议的工作进展非常顺利，1995年6月IEEE正式采纳了快速以太网（Fast Ethernet）标准，该标准被命名为802.3u。

快速以太网的基本思想是：保留802.3的帧格式和CSMA/CD协议，只是将数据传输率从10Mbps提高到100Mbps，相应的位时从100ns减小到10ns。从技术上讲，快速以太网可以完全照搬原来的10Base5和10Base2标准，只将最大电缆长度减少到原来的1/10并仍能检测到冲突。由于使用UTP的快速以太网标准10Base-T的优点如此突出，所以快速以太网是完全基于集线器的，不再使用带有插入式分接头或BNC接头的同轴电缆。

快速以太网标准支持3种不同的物理层标准，分别是100Base-T4、100Base-TX和100Base-FX。

100Base-T4需要4对3类双绞线：一对专用于发送，一对专用于接收，另两对则是双向的。将100Mbps的数据信号分配到3对电缆传输，从而降低了对电缆的要求。

100Base-TX需要2对高质量的双绞线：一对用于发送数据，另一对用于接收数据。这种电缆类型既可以是5类非屏蔽双绞线（Category 5），也可以是IBM 1类屏蔽双绞线（IBM Type 1 STP）。我们一般把100Base-TX和100Base-T4统称为100Base-T。100BASE-T站点与集线器的最大距离不

超过100米。

100Base-FX的标准电缆类型是内径为62.5μm、外经为125μm的多模光缆。光缆仅需一对光纤：一路用于发送，一路用于接收。100Base-FX可将站点与服务器的最大距离增加到185米，服务器和工作站之间（无集线器）的最大距离增加到约400米；而使用单模光纤时可达2公里。表6-3给出了快速以太网3种不同的物理层标准。

表6-3 快速以太网3种物理层标准

	100Base-TX	100Base-FX	100Base-T4
支持全双工	是	是	否
电缆对数	两对双绞线	一对光纤	四对双绞线
电缆类型	UTP Cat 5，STP Type 1	多模/单模光纤	UTP Cat 3
最大距离	100m	200m，2km	100m
接口类型	RJ-45或DB9	MIC，ST，SC	RJ-45

快速以太网集线器的工作方式类似于802.3集线器。它的所有端口也构成一个冲突域，在某一时刻只有一个站点可以发送数据。快速以太网支持Class I和Class II两种类型的集线器。Class I集线器延时比较大，该种类型的集线器首先将收到的电信号转换为数字信号，经过放大处理再将数字信号转换为电信号发往其他端口。Class I集线器支持各种介质类型的端口，但一个冲突域只能配置一个Class I集线器。Class II集线器的延时比Class I集线器小，它可直接转发电信号。Class II集线器只能支持100Base-T类型的端口，一个冲突域只能配置两个Class II集线器。

快速以太网也可以使用交换式集线器，即快速以太网交换机，它的工作原理也类似于802.3交换机，在此不再讨论。

最后需要指出的是，所有的快速以太网交换机均可同时支持10Mbps和100Mbps的端口。这是由于交换机一般都有缓冲存储器，可以在不同速率的端口之间进行速率匹配。

6.3 千兆位以太网

千兆位以太网是近期推出的高速局域网技术，以适应用户对网络带宽的需求。它在局域网组网技术上与ATM形成竞争格局。千兆位以太网是IEEE802.3以太网标准的扩展，编号为802.3z，其数据传输率为1000Mbps（即1Gbps，因此也称吉比特以太网）。千兆位以太网基本保留了原以太网MAC层CSMA/CD协议，但它对CSMA/CD协议进行了一些改动，增加了一些新的特性。为节省标准制定时间，千兆位以太网的物理层没有重新设计新协议，而是“嫁接”了ANSI X3T11的光纤通道（Fiber Channel，FC）的物理层协议（FC标准中关于物理介质和接口的FC-0和关于编码解码的FC-1这两部分）。传输介质可以采用：①阻抗为150欧姆的屏蔽双绞线（STP），其标准为1000Base-CX，传输距离为25m；②5类非屏蔽双绞线，其标准为1000Base-T，传输距离为100m；③使用短波长光源的1000Base-SX标准，该物理层标准支持62.5μm和50μm两种直径的多模光纤，传输距离分别为440m和550m；④使用长波长光源的1000Base-LX标准，该物理层标准支持62.5μm和50μm两种直径的多模光纤和直径为5μm的单模光纤，传输距离分别为250m、550m和3km。表6-4给出了千兆位以太网传输介质与距离的关系。

表6-4 千兆位以太网物理层接口标准

标 准	介质类型	光纤直径（μm）	最大传输距离
1000Base-CX	STP		25m
1000Base-T	5类UTP		100m
1000Base-SX	多模	62.5，50	440m，550m
1000Base-LX	多模，单模	62.5，50， 5	250m，550m，3km

千兆位以太网对上层用户的要求依旧是最小帧长度是 64字节，最大帧长度为 1518字节，以便与以太网和快速以太网兼容。为了在两个相距 200米的站点之间同时传输数据时能够检测到冲突，保证网络稳定可靠地运行，千兆位以太网引入了载波扩展（ carrier extension）和分组猝发（packet burst）传输技术。

所谓载波扩展就是适当增加帧的长度，即千兆位以太网对用户的最小帧长度要求仍然为 64字节时，实际传输的帧长度是 512字节，以保证在数据发送期间站点能够检测到冲突并采取相应的措施。但是载波扩展也耗费大量的带宽，为了弥补载波扩展之不足，又引入分组猝发传输技术，该技术可让载波扩展只用于猝发数据帧的第 1帧。单帧猝发限制在3K字节左右，以防止某个结点占据整个网络带宽。采用这两种技术就可以把千兆位以太网的冲突检测域扩展到 200m，而在传送大的数据帧时网络利用率可达 90%。

千兆位以太网与快速以太网相比，有其明显的优点。千兆位以太网的速度 10倍于快速以太网，但其价格只为快速以太网的 2~3倍。而且从现有的传统以太网与快速以太网可以平滑地过渡到千兆位以太网，并不需要掌握新的配置、管理与排除故障技术。千兆位以太网同样支持半双工和全双工两种工作方式。由于全双工是点到点专线连接，所以它不需要 CSMA/CD协议。

千兆位以太网最通用的办法是采用三层设计。最下面一层由 10Mbps以太网交换机加100Mbps上行链路组成；第二层由 100Mbps以太网交换机加1000Mbps上行链路组成；最高层由千兆位以太网交换机组成。在每一层，交换机逐步提高干线速率。这种设计的意图是一般由低廉的交换机完成10Mbps工作站的连接，昂贵的大容量交换机只用在最高层。在这一层由于交换的信息量大，价格相对高一些也合理。

随着千兆位以太网交换机的投入使用，有望解决长期困绕网络的主干拥挤问题。千兆位以太网可以将现有的10Mbps以太网和100Mbps快速以太网连接起来，现有的 100Mbps以太网可通过1000Mbps的链路与千兆位以太网交换机相连，从而组成更大容量的主干网，这种主干网可以支持大量的交换式和共享式的以太网段。用千兆位以太网取代 FDDI，将获得10倍于FDDI的带宽，同时可消除以太网和 FDDI之间的协议转化。千兆位以太网虽然在数据、话音、视频等实时业务方面还不能提供真正意义上的服务质量（ QoS）保证，但千兆位以太网的高带宽，能克服传统以太网的一些弱点，提供更高的服务性能。

6.4 局域网交换机

近年来，随着电视会议、远程教育和远程诊断等多媒体应用的不断发展，人们对网络带宽的要求越来越高，传统的共享式 LAN已不能满足多媒体应用对网络带宽的要求。在传统共享式10Mbps以太网或100Mbps的FDDI网络中，各站点去竞争和共享网络带宽。当用户增多时，分到

每个用户的带宽就会减少。根据一般常识，在一个共享的网段中，当用户数目超过 50个时，系统的响应速度会急剧下降。我们可以使用前面介绍的网桥设备将网段微化，以达到隔离网络、减小流量的目的。但过多的网段微化会带来设备投资的增加和管理上的难度，因此必须引入局域网交换机（LAN Switch）来解决上述问题。

交换式以太网的核心是一个以太网交换机。边个交换机有一个高速背板，此背板通常被划分成多个以太网段，每个网段由一个模块支持并构成一个冲突域（ collision domain)。

当某个站点发送的数据帧到达交换机时，交换机上的以太网模块首先检查该帧的目的地址所指向的站点是否在同一个以太网模块上。如果是，就复制该帧，并把它复制到对应的端口上；否则，就将该帧通过交换机的高速背板转发到另一个以太网模块上，而该以太网模块连接着目的站点。

如果同一个以太网模块上连接的两个站点同时发送数据，会发生什么情况？这取决于以太网模块的结构。一种方式是以太网模块上的所有端口连在一起形成一个以太网，其上的冲突检查和处理方式与共享CSMA/CD协议一样，也采用二进制指数后退算法进行重发。采用这种结构，任何时候每个以太网模块上只能有一个站可以发送数据，但不同以太网模块上的站点可以并行发送数据帧。我们称这种交换方式为模块交换。

另一种方案是，以太网模块采用缓存方法。当有数据帧到达时，它们首先被缓存在以太网模块上的RAM中。这种方案允许所有的输入端口并行地发送和接收数据。当以太网模块接收到数据帧时，首先检查该帧的目的地址所指向的站点是在该以太网模块的另一个端口，还是在其他以太网模块上。如果是在同一个以太网模块上，数据将被直接发送到目的端口；否则，数据帧必须先通过交换机的高速背板发送到正确的以太网模块上，然后再做相应的处理。在这种方案中，每个端口是一个独立的冲突域，端口之间不会发生冲突，我们称这种交换方式为端口交换。

从某种意义上说，局域网交换机就是交换速度更快（采用 ASIC芯片）、端口集成度更大（可达几十个）、地址缓存更多（可达上万个）的多端口网桥。但是局域网交换机与网桥相比还是有许多新特性，如提供全双工通信、流量控制和网络管理等功能。

从原理上看，交换机与网桥是一样的，都是工作在 OSI模型第2层的网络互连设备。它具有多个端口，每个端口都具有桥接功能，可以连接一个 LAN或一个高性能服务器。交换机能够为每个联网的机器提供专用的带宽。

由于交换机内部采用了专门设计的集成电路，使得交换机能够以线路速率在所有端口并行转发数据帧，提供比传统网桥高得多的操作性能。专用集成电路技术使得交换机在更多端口的情况下能够保持高性能运行，其端口造价低于传统网桥。另外在使用交换机的网络中，现有的线缆、中继器、集线器和网卡都不必升级；而且交换机对工作站是透明的，这样既降低了管理开销，又简化了因网络结点增加、移动和网络拓扑结构变化所引起的操作。

交换机在交换技术方面主要分为端口交换、帧交换以及信元交换三种。端口交换技术最早出现在插槽式集线器中，这类集线器的背板通常划分为多个以太网段，每个网段构成一个广播域。以太网模块插入后通常被分配到某个背板的网段上，而端口交换用于将以太网模块的端口在背板的多个网段之间进行负载分配和平衡。但端口交换还不是真正意义上的交换，它主要用

于端口容错。而帧交换是目前应用最为广泛的局域网交换技术，它对传统传输介质进行微分段，提供并行传送的机制，以减少冲突，获得较高的带宽。采用帧交换的交换机对帧的处理分为直通交换和存储转发两种方式。所谓直通交换是指交换机只取出数据帧的前 14个字节，然后根据帧的目的地址将帧转发到相应的端口上。这种方式的优点是交换速度非常快，可以提供线速处理能力；但缺点是缺乏对帧进行的差错控制，也无法支持不同速率的端口之间进行交换处理。而存储转发方式是指交换机将帧全部取出并缓存起来，然后根据帧的目的地址将其转发到相应的端口上。这种方式的交换速度相对来说比较慢，但它可以提供差错控制并支持不同速率的端口之间进行交换处理。有些厂商生产的交换机甚至对帧进行进一步分解，将帧分成固定大小的信元，信元的处理采用硬件实现，可以获得更高的处理速度，这就是信元交换，其最高速率可达Gbps的数量级。

局域网交换机根据使用的网络技术可以分为：以太网交换机、快速以太网交换机、千兆位以太网交换机、令牌网交换机、 FDDI交换机和ATM交换机，而实际情况是一台局域网交换机上可以同时支持多种局域网技术。如果按交换机应用领域来划分，可以分为台式交换机、工作组级交换机、主干交换机和企业级交换机。

局域网交换机是组成网络系统的核心设备。其最主要的指标是端口数量和类型、总交换能力、包交换速度、广域网连接、热切换和容错能力以及是否支持网络管理等。

6.5 小结

FDDI、快速以太网和千兆位以太网是目前比较流行的高速局域网。其中，快速以太网已大量使用在桌面系统，而 FDDI和千兆位以太网则被大量用于校园网、园区网或企业网的主干上，它们各有优缺点。随着网络规模的不断扩大以及用户对网络带宽的要求越来越高，传统的网桥也越来越多地被局域网交换机所取代，因为局域网交换机在互连规模、速度、性能 /价格比方面要远远高于网桥。

习题

1. 一个FDDI环型网有100个站点，令牌绕环一周的时间是 40ms，站点的令牌保持时间是10ms。问此环的最大速率是多少？
2. 比较FDDI与令牌环的介质访问控制协议的异同点。
3. 在FDDI网络中采用了哪几种容错技术？它们各自的工作原理是什么？
4. 为了保证与以太网兼容，快速以太网做了怎样的修改？
5. 千兆位以太网引入了什么技术以保证与以太网及快速以太网兼容？
6. 局域网交换机与网桥相比，主要的优点是什么？

第三部分　网 络 互 连

网络互联是指将各种不同的物理网络（如不同的局域网或广域网）连接在一起构成统一的网络，它是计算机网络中是一个非常重要的概念和技术。

TCP/IP技术是实现网络互联的重要手段，该部分将要讨论的内容包括： TCP/IP参考模型、IP、ARP和ICMP、IP路由协议以及TCP和UDP。

第7章　网络互连与TCP/IP

到目前为止，我们已经讨论了各种底层网络技术，如局域网、高速局域网和广域网。从本章开始，我们将讨论如何将上述各种物理网络连接成一个无缝的整体，以隐藏所有底层网络的技术，为用户提供一个统一、通用的服务界面，这就是网络互联技术，而 IP协议就是这一技术的体现。本章我们将讨论网络互联及IP。

7.1　网络互联层次

大家知道，网络互联要解决的是异构网的通信问题，目的是向高层隐藏底层物理网络技术的细节，为用户提供统一的通信服务。

为了完成网络互联以屏蔽底层网络的细节，我们可以在不同的层次上完成异构网络的互联。总体来说，有两种方式可实现网络互联：一种是利用应用程序，即应用级互联；另一种是利用操作系统，即网络级互联。

7.1.1　应用级互联

早期的异构网络互联是通过应用程序完成的。用协议转换的观点来说，在这种互联网中，除了应用层协议外，其他各层协议都不相同。应用程序必须了解本机与网络连接的所有内部细节，并直接通过网络与其他应用程序通信，换句话说，应用程序直接建立在物理网络上，无中间协议。

例如，OSI电子邮件系统中的每台机器都必须运行一个称为消息传输代理 MTA的应用程序，由它负责邮件的收发，而且每台中转邮件的机器也必须完整接收邮件，然后根据邮件地址将其转发到下一站。这就是一个典型的应用级互联的例子。

应用级互联是最容易想到也是最笨的办法。其缺点是：首先，在网络系统中增加新的功能意味着要为网络中的每台机器编写新的应用程序；第二，增加新的硬件意味着要修改旧的应用程序；第三，每个应用程序都必须处理本机与网络连接的细节，导致代码重复。上述这些问题的根源在于应用程序必须直接面对物理网络硬件。

应用级互联还有以下弊端：第一，当互联网络达到一定规模时，要为所有机器编写应用程序几乎是不可能的；第二，由于采用点到点的存储转发通信方式，当网络中的某个中间结点的应用程序出错时，发送方和接收方既无法不知道也无法控制。随着网络互联技术的发展，应用级互联技术已很少使用。

7.1.2 网络级互联

网络级互联提供一种机制，实时地把用户数据分组从源端发送到目的端。在网络级互联中，用户（应用程序）直接感受到的是互联网所提供的分组交换服务，而不是网络连接。也就是说，网络级互联通过分组交换机制将底层物理网络硬件细节隐藏起来，避免了应用级互联的种种弊端。与应用级互联相比，网络级互联必须在系统中增加某些中间层次（主要是网络层），使应用程序不直接处理物理网络连接，这样物理网络技术的特性及其变化就不会影响到应用程序，并且不同的应用程序还可以共享网络级互联所提供的分组交换服务，而不再产生重复代码。

网络级互联的优点在于：首先，这种互联技术直接映射到底层网络硬件，因此十分高效。第二，网络级互联把数据包传递功能从应用程序中分离出来，允许网络中的每台机器只需要处理与数据包传递有关的操作即可；第三，网络级互联使得整个互联网络的系统更加灵活；第四，网络互联模式允许网络管理人员通过修改或增加某些网络软件就能在互联网中加入新的网络技术，而对应用程序而言并不需要做任何改变。

网络级互联的关键思想归纳起来就形成 TCP/IP网络的基本概念。它是对各种不同的物理网络的一种高度抽象，它将通信问题从网络细节中解放出来，通过提供通用网络服务，使底层网络技术对用户或应用程序透明。

网络级互联的目标是建立一个统一、协作、提供统一服务的通信系统。具体方法就是在底层网络技术与应用程序之间增加一个中间层软件，以便抽象和屏蔽底层物理网络的硬件细节，向用户提供通用的网络服务。

7.2 TCP/IP参考模型

TCP/IP是20世纪70年代中期美国国防部为其研究性网络 ARPANET开发的网络体系结构。ARPANET最初是通过租用的电话线将美国的几百所大学和研究所连接起来。随着卫星通信技术和无线电技术的发展，这些技术也被应用到ARPANET网络中，而已有的协议已不能解决这些通信网络的互联问题，于是就提出了新的网络体系结构，用于将不同的通信网络无缝连接。这种网络体系结构后来被称为 TCP/IP（Transmission Control Protocol/Internet Protocol）参考模型。图7-1给出了TCP/IP参考模型。

图7-1 TCP/IP参考模型

TCP/IP参考模型是4层结构，下面我们分别讨论这4层的功能：

1. 网络接口层

这是TCP/IP模型的最低层，负责接收从IP层交来的IP数据报并将IP数据报通过低层物理网络发送出去，或者从低层物理网络上接收物理帧，抽出 IP数据报，交给IP层。

网络接口有两种类型。第一种是设备驱动程序，如局域网的网络接口；第二种是含自身数

据链路协议的复杂子系统，如X.25中的网络接口。

2. 互联网层

互联网层的主要功能是负责相邻结点之间的数据传送。它的主要功能包括三个方面。第一，处理来自传输层的分组发送请求：将分组装入IP数据报，填充报头，选择去往目的结点的路径，然后将数据报发往适当的网络接口。第二，处理输入数据报：首先检查数据报的合法性，然后进行路由选择，假如该数据报已到达目的结点（本机），则去掉报头，将IP报文的数据部分交给相应的传输层协议；假如该数据报尚未到达目的结点，则转发该数据报。第三，处理ICMP报文：即处理网络的路由选择、流量控制和拥塞控制等问题。TCP/IP网络模型的互联网层在功能上非常类似于OSI参考模型中的网络层。

3. 传输层

TCP/IP参考模型中传输层的作用与OSI参考模型中传输层的作用是一样的，即在源结点和目的结点的两个进程实体之间提供可靠的端到端的数据传输。为保证数据传输的可靠性，传输层协议规定接收端必须发回确认，并且假定分组丢失，必须重新发送。

传输层还要解决不同应用程序的标识问题，因为在一般的通用计算机中，常常是多个应用程序同时访问互联网。为区别各个应用程序，传输层在每一个分组中增加识别信源和信宿应用程序的标记。另外，传输层的每一个分组均附带校验和，以便接收结点检查接收到的分组的正确性。

TCP/IP模型提供了两个传输层协议：传输控制协议TCP和用户数据报协议UDP。TCP协议是一个可靠的面向连接的传输层协议，它将某结点的数据以字节流形式无差错投递到互联网的任何一台机器上。发送方的TCP将用户交来的字节流划分成独立的报文并交给互联网层进行发送，而接收方的TCP将接收的报文重新装配交给接收用户。TCP同时处理有关流量控制的问题，以防止快速的发送方淹没慢速的接收方。用户数据报协议UDP是一个不可靠的、无连接的传输层协议，UDP协议将可靠性问题交给应用程序解决。UDP协议主要面向请求/应答式的交易型应用，一次交易往往只有一来一回两次报文交换，假如为此而建立连接和撤销连接，开销是相当大的。这种情况下使用UDP就非常有效。另外，UDP协议也应用于那些对可靠性要求不高，但要求网络的延迟较小的场合，如话音和视频数据的传送。IP、TCP和UDP的关系如图7-2所示。

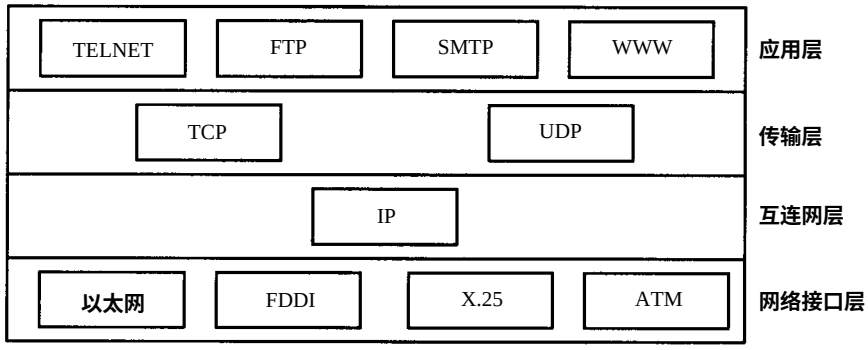


图7-2　TCP/IP模型各层使用的协议

4. 应用层

传输层的上一层是应用层，应用层包括所有的高层协议。早期的应用层有远程登录协议（Telnet）、文件传输协议（File Transfer Protocol，FTP）和简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）等协议。远程登录协议允许用户登录到远程系统并访问远程系统的资源，而且像远程机器的本地用户一样访问远程系统。文件传输协议提供在两台机器之间进行有效的数据传送的手段。简单邮件传输协议最初只是文件传输的一种类型，后来慢慢发展成为一种特定的应用协议。最近几年出现了一些新的应用层协议：如用于将网络中的主机的名字地址映射成网络地址的域名服务（ Domain Name Service，DNS）；用于传输网络新闻的（Network News Transfer Protocol，NNTP）和用于从WWW网上读取页面信息的超文本传输协议（Hyper Text Transfer Protocol，HTTP）协议。

7.3 TCP/IP参考模型的特点

TCP/IP是目前最成功、使用最频繁的互联协议。虽然现在已有许多协议都适用于互联网，但只有TCP/IP最突出，因为它在网络互联中用得最为广泛。下面我们介绍一下 TCP/IP的特点。

7.3.1 TCP/IP模型的两大边界

TCP/IP分层模型中有两大重要边界：一个是地址边界，它将 IP逻辑地址与底层网络的硬件地址分开；一个是操作系统边界，它将网络应用与协议软件分开，如图 7-3所示。

TCP/IP分层模型中，存在一个地址上的边界，它将底层网络的物理地址与互联网层的 IP地址分开。该边界出现在互联网层与网络接口层之间。互联网层和其上的各层均使用IP地址，网络接口层则使用各种物理网络的物理地址，即底层网络的硬件地址。 TCP/IP提供在两种地址之间进行映射的功能。划分地址边界的目的也是为了屏蔽底层物理网络的地址细节，以便使互联网软件在地址问题上显得简单而清晰，易于实现和理解。

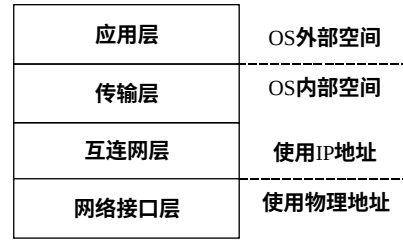


图7-3 TCP/IP 模型的两大边界

TCP/IP的不同实现，可能会导致 TCP/IP软件在操作系统内的位置有所不同，但大部分TCP/IP的实现都类似于图7-3所示的情况。影响操作系统边界划分的最重要因素是协议的效率问题，在操作系统内部实现的协议软件，其数据传递的效率明显要高。

7.3.2 IP层的地位

首先，IP层作为通信子网的最高层，提供无连接的数据报传输机制，但 IP协议并不能保证IP报文传递的可靠性。

其次，IP是点到点的。用IP进行通信的主机或路由器位于同一物理网络，对等机器（主机-路由器、路由器-路由器以及主机-主机）之间拥有直接的物理连接。

TCP/IP是为包容各种物理网络技术而设计的，这种包容性主要体现在 IP层中。通过前面的介绍，我们看到，各种物理网络技术（如各种局域网和广域网）在帧或报文格式、地址格式等

方面差别很大。TCP/IP的重要思想之一就是通过IP将各种底层网络技术统一起来，达到屏蔽底层细节，提供统一界面的目的，即统一的虚拟网。

IP向上层（主要是TCP层）提供统一的IP报文，使得各种网络帧或报文格式的差异性对高层协议不复存在。这种统一的意义不容小视，因为这是TCP/IP互联网首先希望实现的目标。IP层是TCP/IP实现异构网互联最关键的一层。

7.3.3　TCP/IP的可靠性思想

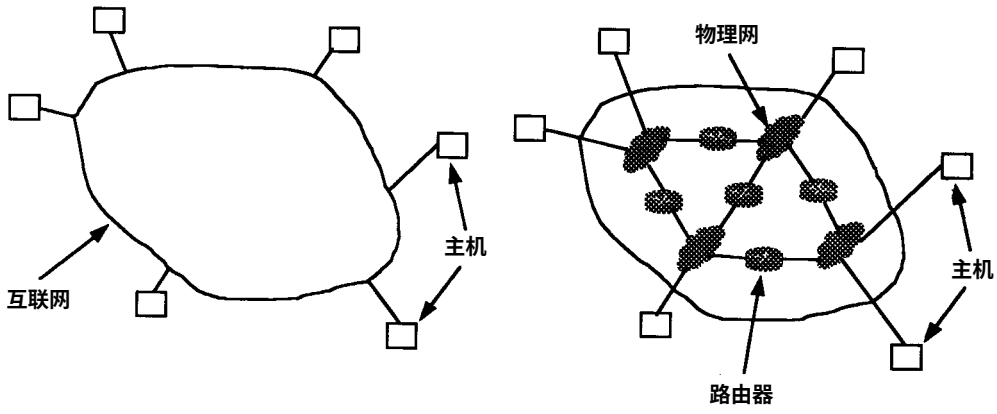
在TCP/IP网络中，IP采用无连接的数据报机制，对数据进行“尽力传递”，即只管将报文尽力传送到目的主机，无论传输正确与否，不做验证，不发确认，也不保证报文的顺序。

TCP/IP的可靠性体现在传输层，传输层协议之一的TCP协议提供面向连接的服务（传输层的另一个协议UDP是无连接的）。因为传输层是端到端的，所以TCP/IP的可靠性被称为端到端可靠性。

端到端可靠性思想有两个优点。第一，TCP/IP跟ISO/OSI协议相比，显得简洁清晰。面向连接协议的复杂性比无连接协议要高出许多。而TCP/IP只在TCP层提供面向连接的服务，比若干层同时的用户提供连接服务的协议族要显得简单。第二，TCP/IP的效率相当高。TCP/IP的IP协议是“尽力传递”方式，只有TCP层为保证传输可靠性而做必要的工作，不像ISO/OSI几乎每一层都要保证可靠传输。实践证明，TCP/IP的效率比ISO/OSI要高，尤其是当低层物理网络很可靠时，TCP/IP的效率更加可观。

7.3.4　TCP/IP模型的特点

TCP/IP将不同的底层物理网络、拓扑结构隐藏起来，向用户和应用程序提供通用的、统一的网络服务。这样，从用户的角度看，整个TCP/IP互联网就是一个统一的整体，它独立于具体的各种物理网络技术，能够向用户提供一个通用的网络服务，如图7-4所示。



a) TCP/IP互联网用户视图　　b) TCP/IP互联网用户视图

图7-4　TCP/IP互联网用户视图和内部结果

在某种意义上，可以把这个单一的网络看作一个虚拟网：在逻辑上它是独立的、统一的，在物理上它则是由不同的网络互联而成。将 TCP/IP互联网看作单一网络的观点，极大地简化了细节，使用户极容易建立起TCP/IP互联网的概念。

TCP/IP互联网还有一个基本思想：即任何一个能传输数据分组的通信系统，均可被看作是一个独立的物理网络，这些通信系统均受到互连网协议的平等对待。大到广域网、小到 LAN，甚至两台机器之间的点到点专线以及拨号电话线路都被当做网络，这就是互连网的网络对等性。网络对等性为协议设计者提供了极大的方便，大大简化了对异构网的处理。

可见，TCP/IP网络完全撇开了底层物理网络的特性，是一个高度抽象的概念，正是这一抽象的概念，为TCP/IP网络赋予了巨大的灵活性和通用性。

7.4 TCP/IP与ISO/OSI

通过前面的讨论，大家已经看到TCP/IP 模型和ISO/OSI模型有许多相似之处。例如，两种模型中都包含能提供可靠的进程之间端到端传输服务的传输层，而在传输层之上是面向用户应用的传输服务。

尽管ISO/OSI模型和TCP/IP模型基本类似，但是它们还是有许多不同之处。在这一节里，我们将讨论两种模型的不同之处。有一点需要特别指出：我们是比较两种参考模型的差异，并不对两个模型中所使用的协议进行比较。

在ISO/OSI参考模型中，有3个基本概念：服务、接口和协议。也许 ISO/OSI模型的最重要的贡献是将这3个概念区分清楚了。每一层都为其上层提供服务，服务的概念描述了该层所做的工作，并不涉及服务的实现以及上层实体如何访问的问题。

层间接口描述了高层实体如何访问低层实体提供的服务。接口定义了服务访问所需的参数和期望的结果。接口仍然不涉及到某层实体的内部机制，而只有不同机器同层实体使用的对等进程才涉及层实体的实现问题。只要能够完成它必须提供的功能，对等层之间可以采用任何协议。如果愿意，对等层实体可以任意更换协议而不影响高层软件。

上述思想也非常符合现代的面向对象的程序设计思想。一个对象（如模型中的某一层），有一组它的外部进程可以使用的操作。这些操作的语义定义了对象所能提供的服务的集合。对象的内部编码和协议对外是不可见的，也与对象的外部世界无关。

TCP/IP模型并不十分清晰地区分服务、接口和协议这些概念。相比 TCP/IP模型，ISO/OSI模型中的协议具有更好的隐蔽性并更容易被替换。

ISO/OSI参考模型是在其协议被开发之前设计出来的。这意味着 ISO/OSI模型并不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着 ISO/OSI模型在协议实现方面存在某些不足。

而TCP/IP模型正好相反。先有协议，模型只是现有协议的描述，因而协议与模型非常吻合。问题在于TCP/IP模型不适合其他协议栈。因此，它在描述其他非 TCP/IP网络时用处不大。

下面我们来看看两种模型的具体差异。其中显而易见的差异是两种模型的层数不一样：ISO/OSI模型有7层，而TCP/IP模型只有4层。两者都有网络层、传输层和应用层，但其他层是不同的。

两者的另外一个差别是有关服务类型方面。ISO/OSI模型的网络层提供面向连接和无连接两种服务，而传输层只提供面向连接服务。TCP/IP模型在网络层只提供无连接服务，但在传输层却提供两种服务。

综上所述，使用ISO/OSI模型（去掉会话层和表示层）可以很好地讨论计算机网络，但是OSI协议并未流行。TCP/IP模型正好相反，其模型本身实际上并不存在，只是对现存协议的一个归纳和总结，但TCP/IP协议却被广泛使用。在后面的章节中，我们主要讨论TCP/IP协议。

7.5 小结

网络互连的目是为了屏蔽底层物理网络的技术细节。网络互连可以在应用级完成，也可以在网络级完成。

TCP/IP参考模型将互连网分为4层，分别为网络接口层、互联网层、传输层以及应用层，而且它有两大边界。

IP层在TCP/IP参考模型中占有非常重要的地位。IP层作为通信子网的最高层，提供无连接的数据报传输机制，但它不能保证IP报文传递的可靠性，数据的可靠传输是由TCP完成的。

TCP/IP参考模型和ISO/OSI参考模型既有相同点，又有许多不同之处。ISO/OSI模型是在其协议被开发之前设计出来的，因此它更具有通用性。但另一方面，ISO/OSI模型在协议实现方面存在某些不足。而TCP/IP模型正好相反，先有协议，模型只是现有协议的描述，因而协议与模型非常吻合。问题在于TCP/IP模型不适合其他协议栈。因此，它在描述其他非TCP/IP网络时用处不大。

习题

1. 比较应用级互连与网络级互连的异同点。
2. TCP/IP参考模型包含几层，每一层主要完成的功能是什么？
3. TCP/IP参考模型的两大边界是什么？有何意义？
4. IP层的地位和特点是什么？
5. TCP/IP技术是如何对待互连网中的各个物理网络的？
6. 比较TCP/IP参考模型和ISO/OSI参考模型的异同点。