

# 第一章 计算机网络概述

1997 年，在美国拉斯维加斯的全球计算机技术博览会上，微软公司总裁比尔盖茨先生发表了著名的演说。在演说中，“网络才是计算机”的精辟论点充分体现出信息社会中计算机网络的重要基础地位。计算机网络技术的发展越来越成为当今世界高新技术发展的核心之一。

所谓计算机网络，是指把地理上分散的自主计算机，通过数据通信系统连接起来，以达到资源共享为目的的一种计算机系统。所谓自主计算机，是指具有独立处理能力的计算机。对计算机网络的一种更为简洁的定义是指一些互连的自主计算机系统的集合。可见，计算机网络是在计算机技术和通信技术高度发展的基础上，两者相互结合的产物。一方面，通信系统为计算机之间的数据传送，提供最重要的支持；另一方面，由于计算机技术渗透到通信领域中，又极大地提高了通信网络的性能。

## 1.1 计算机网络的发展历史

计算机网络的发展经历了一个从简单到复杂，计算机网络的发展经历了四个阶段：面向终端的计算机网络；分组交换网络；开放式标准化网络；Internet 的产生与发展。

### 1.1.1 面向终端的计算机网络

1954 年，收发器终端出现，实现了将穿孔卡片上的数据从电话线上发送到远地的计算机。用户可在远地的电传打字机上键入自己的程序，计算机计算出来的结果从计算机传送到远地的电传打字机上打印出来。计算机网络的概念也就这样产生了，常称为联机系统，如图 1-1 所示。面向终端的计算机通信网中，计算机是网络的中心和控制者，终端围绕中心计算机分布在各处，呈分层星型结构，而计算机的任务是进行成批处理。面向终端的计算机网络采用了多路复用器（MUX）、线路集中器、前端控制器等通信控制设备连接多个中断，使昂贵的通信线路为若干个分布在同一远程地点的相近用户分时共享使用。

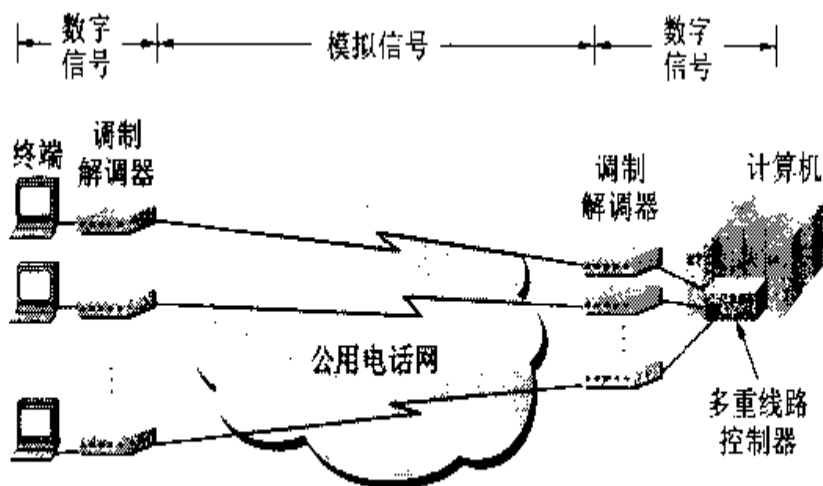


图 1-1 计算机通过多重线路控制器与远程终端相连

以单个计算机为中心的远程联机系统，构成面向终端的计算机网络。用一台中央主机连接大量的地理上处于分散位置的终端。如 20 世纪 60 年代初，美国建成了全国性航空飞机订票系统，用一台中央计算机联结 2000 多个遍布全国各地的终端，用户通过终端进行操作。这些应用系统的建立，构成了计算机网络的雏形。

为减轻中心计算机的负载，在通信线路和计算机之间设置了一个前端处理机 FEP 或通信控制器 CCU 专门负责与终端之间的通信控制，使数据处理和通信控制分工。在终端机较集中的地区，采用了集中管理器（集中器或多路复用器）用低速线路把附近群集的终端连起来，通过 MODEM 及高速线路与远程中心计算机的前端机相连（图 1-2）。这样的远程联机系统既提高了线路的利用率，又节约了远程线路的投资。

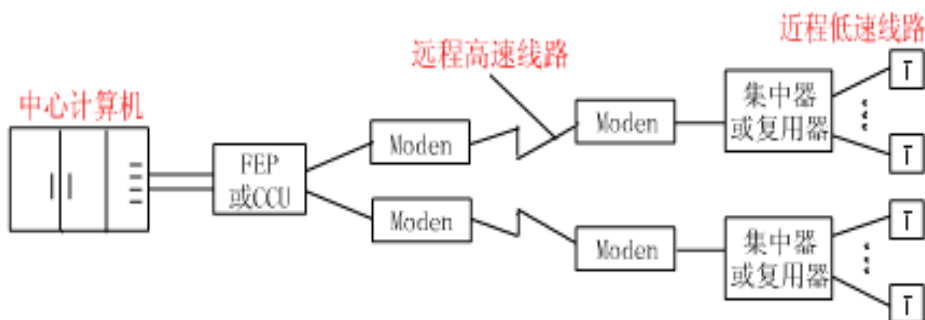


图 1-2 单计算机为中心的远程联机系统

### 1.1.2 分组交换网络

第二阶段计算机网络的典型代表是 ARPA 网络。ARPA 网络的建成标志着现代计算机网络的诞生。ARPA 网络的试验成功是计算机网络的概念发生了根本性的变化，很多有关计算机网络的基本概念都与 APRA 网的研究成果有关，如分组交换、网络协议、资源共享等。

存储转发的概念最初是在 1964 年 8 月巴兰在美国兰德公司的“论分布式通信”的研究报告中提出的。在 1962 年到 1965 年，美国国防部远景规划局和英国的国家物理实验室都在对新型的计算机通信网进行讲究。1966 年 6 月，英国的国家物理实验室的戴维斯首次提出“分组”这个名词。1969 年 12 月，美国的分组交换网 ARPANET（当时仅 4 个结点）投入运行。从此，计算机网络的发展就进入了一个崭新的纪元。1973 年英国的国家物理实验室也开通了分组交换试验网。现在大家都公认 ARPANET 为分组交换网之父，并将分组交换网的出现作为现代电信时代的开始。

按数据传送技术划分，交换网络又可分为电路交换网、报文交换网和分组交换网。图 1-3 为交换网络的拓扑结构图。分组交换也称为包交换，它是现代计算机网络的技术基础。

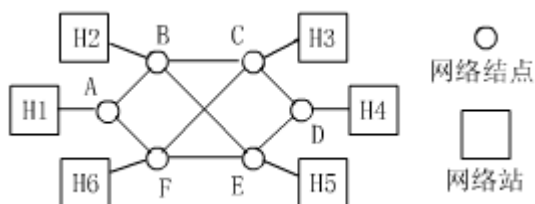


图 1-3 交换网络的拓扑结构

#### 1、电路交换的工作原理

##### 1) 电路交换的三个过程

（1）电路建立：在传输任何数据之前，要先经过呼叫过程建立一条端到端的电路。如图 1-3 所示，若 H1 站要与 H3 站连接，典型的做法是，H1 站先向与其相连的 A 节点提出请求，然后 A 节点在通向 C 节点的路径中找到下一个支路。比如 A 节点选择经 B 节点的电路，在此电路上分配一个未

---

用的通道，并告诉 B 它还要连接 C 节点；B 再呼叫 C，建立电路 BC，最后，节点 C 完成到 H3 站的连接。这样 A 与 C 之间就有一条专用电路 ABC，用于 H1 站与 H3 站之间的数据传输。

(2) 数据传输：电路 ABC 建立以后，数据就可以从 A 发送到 B，再由 B 交换到 C；C 也可以经 B 向 A 发送数据。在整个数据传输过程中，所建立的电路必须始终保持连接状态。

(3) 电路拆除：数据传输结束后，由某一方（A 或 C）发出拆除请求，然后逐节拆除到对方节点。

## 2) 电路交换技术的优缺点及其特点

(1) 优点：数据传输可靠、迅速，数据不会丢失且保持原来的序列。

(2) 缺点：在某些情况下，电路空闲时的信道容易被浪费：在短时间数据传输时电路建立和拆除所用的时间得不偿失。因此，它适用于系统间要求高质量的大量数据传输的情况。

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

## 2、 报文交换的工作原理

当端点间交换的数据具有随机性和突发性时，采用电路交换方法的缺点是信道容量和有效时间的浪费。采用报文交换则不存在这种问题。

### 1) 报文交换原理

报文交换方式的数据传输单位是报文，报文就是站点一次性要发送的数据块，其长度不限且可变。当一个站要发送报文时，它将一个目的地址附加到报文上，网络节点根据报文上的目的地址信息，把报文发送到下一个节点，一直逐个节点地转送到目的节点。

每个节点在收到整个报文并检查无误后，就暂存这个报文，然后利用路由信息找出下一个节点的地址，再把整个报文传送给下一个节点。因此，端与端之间无需先通过呼叫建立连接。

一个报文在每个节点的延迟时间，等于接收报文所需的时间加上向下一个节点转发所需的排队延迟时间之和。

### 2) 报文交换的特点

(1) 报文从源点传送到目的地采用“存储—转发”方式，在传送报文时，一个时刻仅占用一段通道。

(2) 在交换节点中需要缓冲存储，报文需要排队，故报文交换不能满足实时通信的要求。

### 3) 报文交换的优点

(1) 电路利用率高。由于许多报文可以分时共享两个节点之间的通道，所以对于同样的通信量来说，对电路的传输能力要求较低。

(2) 在电路交换网络上，当通信量变得很大时，就不能接受新的呼叫。而在报文交换网络上，通信量大时仍然可以接收报文，不过传送延迟会增加。

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

(4) 报文交换网络可以进行速度和代码的转换。

### 4) 报文交换的缺点

(1) 不能满足实时或交互式的通信要求，报文经过网络的延迟时间长且不定。

(2) 有时节点收到过多的数据而无空间存储或不能及时转发时，就不得不丢弃报文，而且发出的报文不按顺序到达目的地。

## 3、 分组交换的工作原理

分组交换是报文交换的一种改进，它将报文分成若干个分组，每个分组的长度有一个上限，有限长度的分组使得每个节点所需的存储能力降低了，分组可以存储到内存中，提高了交换速度。它适用于交互式通信，如终端与主机通信。分组交换有虚电路分组交换和数据报分组交换两种。它是

计算机网络中使用最广泛的一种交换技术。

通常我们将发送的整块数据称为一个报文。在发送报文之前，先将较长的报文划分成为一个个较小的等长数据块（如图 1-4），例如，每个数据块为 1024 比特。在每一个数据块的前面，加上首部后，就构成了一个分组。分组又称为“包”，而分组的首部也可称为“包头”。分组中的首部是非常重要的，因为正是分组的首部才包含了诸如目的地址和源地址等重要控制信息，而分组交换网只有从分组的首部才能获知应将此分组发往何处。

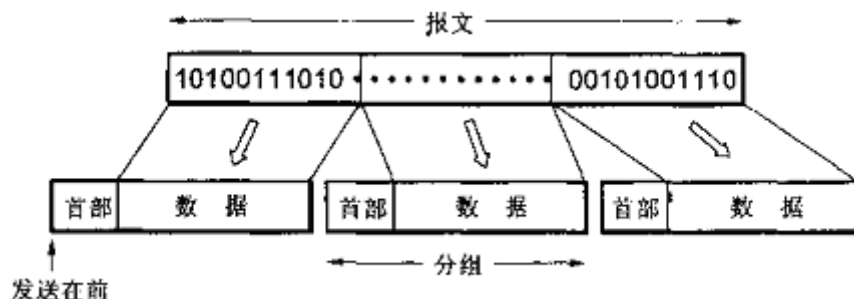


图 1-4 分组的概念

#### 1) 虚电路分组交换原理与特点

在虚电路分组交换中，为了进行数据传输，网络的源节点和目的节点之间要先建一条逻辑通路。每个分组除了包含数据之外还包含一个虚电路标识符。在预先建好的路径上的每个节点都知道把这些分组引导到哪里去，不再需要路由选择判定。最后，由某一个站用清除请求分组来结束这次连接。它之所以是“虚”的，是因为这条电路不是专用的。

虚电路分组交换的主要特点是：在数据传送之前必须通过虚呼叫设置一条虚电路。但并不像电路交换那样有一条专用通路，分组在每个节点上仍然需要缓冲，并在线路上进行排队等待输出。

#### 2) 数据报分组交换原理与特点

在数据报分组交换中，每个分组的传送是被单独处理的。每个分组称为一个数据报，每个数据报自身携带足够的地址信息。一个节点收到一个数据报后，根据数据报中的地址信息和节点所储存的路由信息，找出一个合适的出路，把数据报原样地发送到下一节点。由于各数据报所走的路径不一定相同，因此不能保证各个数据报按顺序到达目的地，有的数据报甚至会中途丢失。整个过程中，没有虚电路建立，但要为每个数据报做路由选择。

### 4、各种数据交换技术的性能比较

1) 电路交换：在数据传输之前必须先设置一条完全的通路。在线路拆除(释放)之前，该通路由一对用户完全占用。电路交换效率不高，适合于较轻和间接式负载使用租用的线路进行通信。

2) 报文交换：报文从源点传送到目的地采用存储转发的方式，报文需要排队。因此报文交换不适合于交互式通信，不能满足实时通信的要求。

3) 分组交换：分组交换方式和报文交换方式类似，但报文被分成分组传送，并规定了最大长度。分组交换技术是在数据网中最广泛使用的一种交换技术，适用于交换中等或大量数据的情况。采用存储转发的分组交换，实质上是采用了在数据通信的过程中断续(或动态)分配传输带宽的策略。这对传送突发式的计算机数据非常合适，使得通信线路的利用率大大提高了。为了提高分组交换的可靠性，常采用网状拓扑结构，使得当发生网络拥塞或少数结点、链路出现故障时，可灵活地改变路由而不致引起通信的中断或全网的瘫痪。此外，通信网络的主干线路往往由一些高速链路构成，这样就能迅速地传送大量的计算机数据。

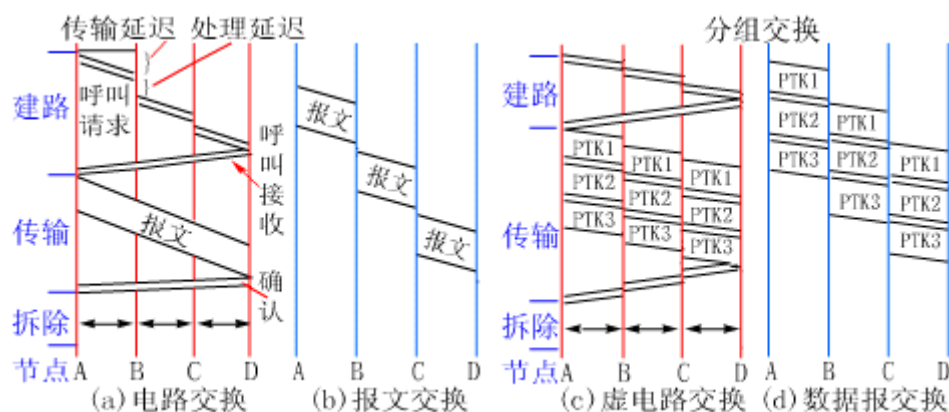


图 1- 5 几种交换方法的时序图

### 1.1.3 开放式标准化网络

20 世纪 70 年代以后,局域网得到了迅速发展。美国 XEROX、DEC 和 INTEL 三公司推出了以 CSMA/CD 介质访问技术为基础的以太网 (ETHERNET) 产品。其他大公司也纷纷推出自己的产品。但各家网络产品在技术、结构等方面存在着很大差异,没有统一的标准,因而给用户带来了很大的不便。

1974 年 IBM 公司宣布了按分层方法研制的网络标准——系统网络体系结构 SNA (System Network Architecture),它是世界上使用得较为广泛的一种网络体系结构。不久后,其他一些公司相继推出本公司的网络体系结构。网络体系结构的出现,使得一个公司所生产各种网络产品都能够很容易的互连成网,而不通公司生产的产品,由于网络体系结构不同,则很难相互连通。

为了使不同体系结构的计算机网络都能互连,国际标准化组织 ISO 于 1977 年成立了专门机构研究该问题。1984 年,ISO 正式颁布了一个使各种计算机互连成网的标准框架——开放系统互连参考模型 (Open System Interconnection Reference Model: 简称 OSI/RM 或 OSI)。80 年代中期,ISO 等机构以 OSI 模型为参考,开发制定了一些列协议标准,形成了一个庞大的 OSI 基本协议集。OSI 标准确保了各厂家生产的计算机和网络产品之间的互联,推动了网络技术的应用和发展,形成了第三代计算机网络。

计算机网络体系结构的出现,用户可以把计算机网络看作一个大的计算机系统,用户不必了解这个网络是由哪些子系统构成,可以用极简单的方式访问被授权的资源,真正实现透明的资源共享。Internet 的出现,使这种共享达到了至善至美的境界。

### 1.1.4 Internet 的产生与发展

20 世纪 80 年代是计算机网络快速发展的年代。1983 年美国加利福尼亚大学伯克莱分校把 TCP/IP 软件集成到该校研制的 BSD UNIX 中,使计算机的操作系统具有了 TCP/IP 网络通信功能,不需要什么额外的投资,运行 BSD UNIX 的计算机就可以方便地互连起来,诞生了真正的 Internet,ARPANT 成了 Internet 的骨干网。80 年代中期,美国国家科学基金会 (NSF) 意识到 Internet 对科学研究的重要性,决定资助 Internet 的发展和 TCP/IP 技术,开始建设使用 TCP/IP 协议的 NSFNET。由于美国国家科学资金的资助和鼓励,很多大学、政府科研机构甚至私营的科研机构都纷纷将自己的局域网并入 NSFNET 网,最终 NSFNET 取代了 ARPANT 成为 Internet 骨干网。随着用户数的飞速地增加,NSFNET 的通讯能力很快地饱和。因此,NSFNET 不得不再次考虑采用更新地网络技术来适应发展的需要。

1989 年,连接 13 个地点地 T1 级主干网开始运行。T1 级主干网能以 1.544 Mbps 的速度传输数据。

---

现在看来 NSFNET 是非常成功的，它不仅向科研人员提供了可获得无限资源的通信网络，并在不断完善、提高的过程中，构造现代美国 Internet 网络结构。

这一时期 Internet 以百分之百的速度迅速向世界各国发展，法国、欧洲、日本相继建成自己的网络。在中国，中国科学院等一些单位通过长途电话拨号方式进行国际联机，进行数据库检索，这是我国 Internet 的开始。

90 年代初期，Internet 已形成一个“网中之网”，各个子网分别负责各自的架设和运作费用，而这些子网又与国家出资资助的主干网 NSFNET 互联起来。由国家出资的 NSFNET 主干网，只允许用于科研和教育的目的，明确规定不准用于商业目的。可是人们在使用中发现加入 Internet，不只是共享 NSFNET 网上巨型计算机的资源，还能相互间进行通讯，这种新通讯方式对商家产生巨大的吸引力。试想这种通讯方式不正是一种很好的商业广告宣传形式吗？到 1991 年底，NSFNET 的主干网已升级 T3 级，速度达到 45Mbps。

随着 Internet 的迅速发展，美国的私人企业开始建立自己的网络，在一定程度上绕开了美国国家科学资金出资的 Internet 骨干网 NSFNET，向用户提供 Internet 商业的联网服务。91 年这些企业组成了“商用 Internet 协会”，纷纷宣布自己开发的子网可用于各种商业用途。

商界的介入，进一步发挥了 Internet 在通讯、资料检索、客户服务等方面的巨大潜力，世界各地无数的企业和个人纷纷涌入 Internet，给 Internet 带来了一个新的飞跃。

到 94 年底为止，Internet 已联通了世界上的 150 多个国家和地区，联接 Internet 的子网有三万多个、320 多万台计算机主机。它的发展如此迅速，以致目前已无法说清楚网上究竟有多少用户。

那么谁是 Internet 的主管？没有！没有人组织可以对 Internet 具有控制权！当前联接到 Internet 的几万个网络都是自愿加入的，它是一个相互协作，共同遵守通讯协议的集合体，所以有人说“Internet 是一个虚拟网络”。在网络中的每个子网作为一个成员，只负责本网络的管理和费用，各子网间相互协作共享资源，互相发送各种信息和数据，共同遵守网络间的通讯协议。如果有谁不恰当地使用 Internet，而损害了网络上其它用户的正常工作，那么其它用户就会切断与其联系。这种网络同行的压力才是保障 Internet 可靠运行的重要条件。

目前是 Internet 发展的一个重要阶段，Internet 原来是专门为教育科研服务的网络。近年开始向商业应用发展，1994 年被人们称为 Internet 的商业年，1997 年则被人们称为网络年。许多公司已在 Internet 上开始了联机商业服务。但 Internet 还是在教育科研领域的应用上从原来的信息查询走向更加广阔的领域，应用的层次也从原来的大专院校发展到中小学。而在我国 Internet 是由中科院高能物理研究所在 1993 年接入的，在促进国内外联络和学术交流起到了很好地作用。直到 1995 年中科院实施了“百所联网”工程，建立中科院 CASNET。

今天，Internet 成为一种通过服务器将较小网络连接起来的错综复杂的网络结构。大部分情况下，服务器通过专门进行 Internet 通讯的线路来传送数据。个人计算机则通过直接线路，或者通过电话线和调制解调器连接到这些服务器上。直接线路一般是高速的电讯线路，专门用于在建筑物之间或组织之间传送数据。而标准的电话线路，或者被称为 ISDN 线路的特殊数字线路（这种情况目前正在增多），则通常用于连接个人计算机。

## 1.2 计算机网络的定义和分类

### 1.2.1 计算机网络的定义

关于什么是计算机网络？到目前为止，尚不能说有一个精确的标准定义。人们看待问题的观点不同，给计算机网络下的定义也不同，通常情况，从资源共享的角度定义计算机网络能够比较全面



---

反映计算机网络的特征。将分散的多台计算机、终端和外部设备用通信线路互连起来，实现彼此间通信，并且计算机的软件、硬件和数据资源大家都可以共同使用，这样一个实现了资源共享的系统叫做计算机网络。

一个计算机网络必须具备三个要素：

- (1) 计算机：至少有两台具有独立操作系统的计算机，且相互间有共享的资源；
- (2) 通信介质：两台（或多台）计算机之间要有通信手段将其互连，如用双绞线、电话线、同轴电缆或光纤等有线通信，也可以使用微波、卫星等无线媒体把它们连接起来；
- (3) 协议：这是关键的要素，由于不同厂家生产的不同类型的计算机，其操作系统、信息表示方法等都存在差异，它们的通信就需要遵循共同的规则和约定，如同讲不同的语言的人类进行对话需要一种标准语言才能沟通。在计算机网络中需要共同遵守的规则和约定被称为网络协议，由它解释、协调和管理计算机之间的通信和相互间的操作。

计算机网络的特征：

- (1) 网络上各计算机系统相互独立。每台计算机可以运行各自的操作系统，如 UNIX、DOS、Windows。
- (2) 各计算机地位平等。广域网上绝对平等，局域网上基本平等，不互相干预。
- (3) 数据交换（通信）是网络的最基本的功能。各种网络资源共享都是建立在数据交换的基础上。
- (4) 资源共享是网络的最终目标。资源共享指网络中计算机软、硬件资源及数据资源的共享。此外，数据交换的必要前提是：用通信设备和通信介质完成计算机的互联。

## 1.2.2 计算机网络的分类

由于计算机网络的广泛使用，目前在世界上已出现了多种形式的计算机网络，可以从不同的角度对它们进行分类，如根据其地理覆盖范围的大小，可将计算机网络分成广域网、城域网、局域网；根据网络拓扑结构的不同，又可将网络分成星型网络、树型网络、总线型网络、环型网络和网状型网络等，还可从交换方式或控制方式等方面进行分类。

### （一）按网络的覆盖范围分类

计算机网络的地理范围分类法是按照网络覆盖地理范围的大小而划分的，可以分为局域网、城域网和广域网。

#### （1）局域网

局域网（Local Area Network, LAN）的作用范围一般限于几公里，用于将较小范围的（如一个实验室，一栋大楼，整个校园等）的各种计算机及外部设备互连成网。局域网的作用范围小，入网设备便宜，网络管理简单，再加上微机的日益普及，局域网成为发展最迅猛，应用最广泛的一种廉价网，是计算机网络中最活跃的领域之一。它有自己独特的一套网络标准和体系结构。

#### （2）城域网

城域网（Metropolitan Area Network, MAN），又称为城市地区网。即它的覆盖范围一般是一个城市，是介于广域网与局域网之间的一种大范围的高速网络。城域网设计的主要目标是满足几十公里范围内的计算机连网需求，实现大量用户，多种信息（数据、声音、图像等）传输的综合性信息网络。城域网目前还处于研究阶段，已经制定出完备的网络标准和技术规范，主要包括分布式队列总线、光纤分布式数据接口及交换多兆位数据服务。其中，光纤分布式数据接口已得到大量应用，而其余两种还未得到广泛普及。

#### （3）广域网

广域网（Wide Area Network, WAN）也称远程网，它所覆盖的地理范围从几十公里到几千甚至

几万公里，覆盖一个地区、国家，甚至延伸至全世界。计算机网络出现的初期，就是以广域网的面目出现的，局域网和城域网都是在广域网技术已经成熟后才出现的。因此大量的网络标准及技术规范都是针对广域网的，像 ISO 的 OSI/RM, X. 25, TCP/IP 等。

网络覆盖的地理范围不同，它所采用的技术就不同，因此形成了不同的网络技术特点与网络服务功能。当然，覆盖的地理范围越大，采用的技术越复杂，管理就越难，造价也就越高。

## （二）按网络的拓扑结构分类

计算机网络的布线方式常常抽象成规则的几何图形（如图 1-6），即通常所说的拓扑结构，一般分为以下几类：

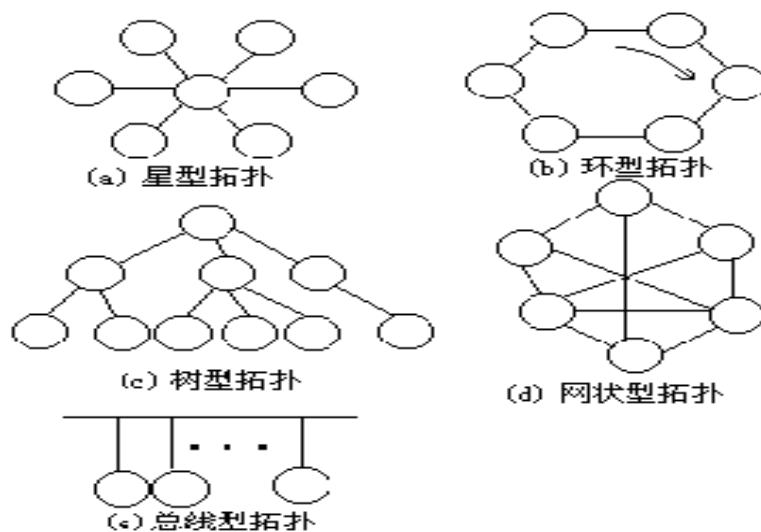


图1-6 常见网络拓扑

### （1）星型网络

必须有一个中心结点，通过中心结点向四面发射，所有结点间通信都要通过中心结点。星型网络的特点：

- 1) 功能高度集中：整个网络的处理和控制功能，都集中在中心结点上，结构简单，易于实现，但不可靠。一个结点或一个信道故障不影响其它部分，但一旦中心结点故障，全网停止工作。
- 2) 单信息流路径：每个结点只有一条路径到中心结点，不存在路径选择。
- 3) 线路利用率低：因为每条通信线路只连接一个远程结点，该线路利用低。
- 4) 可扩充性差：由于受硬件接口和软件功能限制，使其可扩充性差。

星型网络的常用场合：

- 1) 数据传输主要在中心结点和从结点之间，从结点之间数据传输量较少。
- 2) 采用专用自动交换机（PABX）或计算机交换机（CBX）的电话网。

### （2）树型网络

在实际建造一个较大型的网络时，往往采用多级星型网络。而将多级星型网络按层次方式进行排列，即形成树型网络。网络的最高层是中央处理机，最低层是终端，其他各层可以是多路转换器、集中器或部门计算机。树型网络的特点：

- 1) 众多终端共享一条通信线路，线路利用率高。
- 2) 网络分布处理能力增强，改善了星型网的可扩充性、可靠性。；
- 3) 通信费用（合理组网）低于星型网。
- 4) 结构比星型复杂，链路多，时延大。



---

树型网络适用场合：分级管理和控制系统。

### **(3) 总线型网络**

由一条高速公用总线通过相应的硬件接口连接若干个结点所形成，其中一个结点是网络服务器，由它提供网络通信及资源共享服务，其它结点是网络工作站。由于多个结点连接到一条公用总线上，因此必须采取某种介质访问控制规程来分配信道，以保证在一段时间内，只允许一个结点传送信息，是总线型网络的关键问题。如：以太网采用 CSMA/CD 协议，以太网是总线网，反之不然。采用 CSMA/CD 协议的总线网是以太网。总线型网络特点：

- 1) 广播通信方式，即一个结点发送消息，可被网络上所有结点接收。
  - 2) 信道利用率高，因为多个结点共用一条传输信道。
  - 3) 地理覆盖范围小，公用总线长度受限 $<2.5$  公里，限于一个单位，超过一定范围，要加中继器来放大信号。
  - 4) 建网容易，结点连到总线即可，易于控制。
  - 5) 结点数增多，难以维护，主干任何一处出故障，难排除。
- 总线型网络适用场合：局域网，且结点很少时。

### **(4) 环型网络**

在环型网络中，每台入网的计算机都先连接到一个转发器上，再将所有的转发器通过高速点对点信道，这成一环形。网络中的信息是单向流动的，从任一源转发器所送出的信息，经环路传送一周后又都返回到源转发器。环型网络的特点：

- 1) 广播通信方式，由信源站点发出的信息，沿单方向经环路一周返回，故可实现广播通信。
- 2) 传输时延确定，源站发出信息在确定的时间内到达目的站点。
- 3) 引入优先机制，可使某结点具有较高优先级，先发信息。
- 4) 可靠性差，从结构上看，一旦一个站点断环，都会造成网络的瘫痪。
- 5) 灵活性差：不论是增加或减少网络结点都需要断开原环，造成网络中断。

环型网络的适应场合：局域网。单向传输，点到点方式，非常适于光纤连接。

### **(5) 网状型网络**

在网状型网络中，每个结点至少有两条链路与其它结点相连，任何一条线路出故障时，数据可经其它链路传输、可靠性较高。因为没有自然的中心，数据流向也没有固定方向，这种网络的控制往往是分布式的，所以又叫分布式网络。网状型网络的特点：

- 1) 两级网络形式，有通信子网和资源子网组成。
- 2) 网络可靠性高，在任何结点之间，存在多条传输路径，所以网络的稳定性比较好。
- 3) 可扩充性好，凡需入网的计算机只要连接到接口信息处理机上，各计算机之间通过通信子网进行通信。

网状型网络的适应场合：一般用在 WAN 中，是大型网络的基本部分。

## **(三) 按网络控制方式分类：集中式计算机网络、分布式计算机网络**

### **(1) 集中式计算机网络**

集中式计算机网络的处理和控制中心都高度集中在一个或少数几个结点上，所有的信息流都必须经过这些结点之一，因此，这些结点是网络的控制中心，而其余的大多数结点则有较少的处理和控制中心功能。前面所介绍的星型网络和树型网络都是典型的集中式网络。集中式计算机网络的优点是：实现简单，其网络操作系统很容易从传统的分时操作系统经适当地扩充和改造而成。集中式计算机网络的缺点：实时性差、可靠性低、缺乏较好的可扩充性和灵活性。

## （2）分布式计算机网络

在分布式计算机网络中，不存在一个处理和控制中心。网络中的任一结点都至少和另外两个结点相连接，信息从一个结点到达另一结点时，可能有多条路径。同时，网络中的各个结点均以平等地位相互协调工作和交换信息，并可共同完成一个大型任务。前述的分组交换网、网状型网络都属于分布式网络。集中式计算机网络具有信息处理的分布性、可靠性高、可扩充性及灵活性好的优点。

## 1.3 计算机网络系统的组成

### 1.3.1 计算机广域网的组成

从网络拓扑结构来看，计算机广域网是由一些网络节点和连接这些网络节点的通信链路构成。从逻辑功能上讲，广域网是由通信子网和资源子网组成（图 1-7 所示）。通信子网是计算机广域网中负责数据通信的部分，主要完成计算机之间数据的传输、交换以及通信控制，它由网络节点、通信链路组成；资源子网提供访问网络和处理数据的能力，是由主机系统、终端控制器和终端组成，主机系统负责本地或全网的数据处理，运行各种应用程序或大型数据库，向网络用户提供各种软硬件资源和网络服务，终端控制器把一组终端连入通信子网，并负责对终端的控制及终端信息的接收和发送。通信双方必须共同遵守的规则和约定就称为通信协议，它的存在与否是计算机网络与一般计算机互连系统的根本区别。

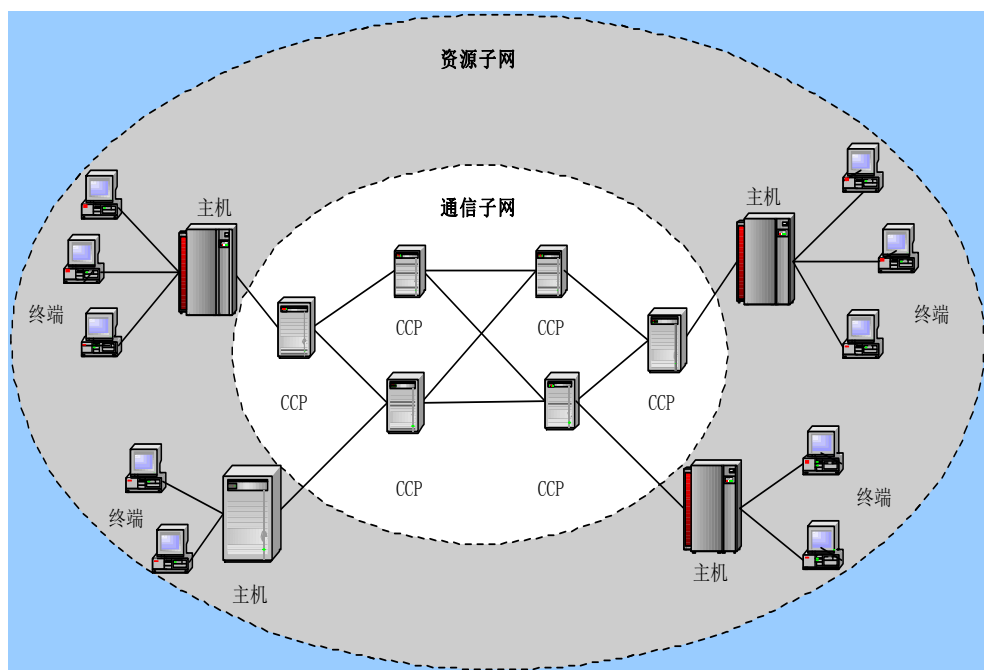


图 1-7 计算机网络的组成

网络软件系统和网络硬件系统是计算机广域网系统赖以存在的基础。在广域网中，硬件对网络的选择起着决定性作用，而网络软件则是挖掘网络潜力的工具。

#### 一、网络软件

在广域网中，网络上的每个用户，都可享有系统中的各种资源，系统必须对用户进行控制。否则，就会造成系统混乱、信息数据的破坏和丢失。为了协调系统资源，系统需要通过软件工具对网络资源进行全面的、管理和分配，并采取一系列的安全保密措施，防止用户不合理的对数据和信息的访问，以防数据和信息的破坏与丢失。网络软件是实现网络功能不可缺少的软件环境。

通常网络软件包括：

网络协议和协议软件：它是通过协议程序实现网络协议功能。

网络通信软件：通过网络通信软件实现网络工作站之间的通信。

---

网络操作系统：网络操作系统是用以实现系统资源共享、管理用户对不同资源访问的应用程序，它是最主要的网络软件。

网络管理及网络应用软件：网络管理软件是用来对网络资源进行管理和对网络进行维护的软件。网络应用软件是为网络用户提供服务并为网络用户解决实际问题的软件。

网络软件最重要的特征是：网络管理软件所研究的重点不是在网络中互连的各个独立的计算机本身的功能，而是在如何实现网络特有的功能。

## 二、网络硬件

网络硬件是计算机网络系统的物质基础。要构成一个计算机网络系统，首先要将计算机及其附属硬件设备与网络中的其它计算机系统连接起来。不同的计算机网络系统，在硬件方面是有差别的。随着计算机技术和网络技术的发展，网络硬件日趋多样化，功能更加强大，更加复杂。

- (1) 线路控制器：是主计算机或终端设备与线路上调制解调器的接口设备。
- (2) 通信控制器：是用以对数据信息各个阶段进行控制的设备。
- (3) 通信处理机：是作为数据交换的开关，负责通信处理工作。
- (4) 前端处理机：是负责通信处理工作的设备。
- (5) 集中器、多路选择器：是通过通信线路分别和多个远程终端相连接的设备。
- (6) 主机和终端。

随着计算机网络技术的发展和网络应用的普及，网络结点设备会越来越多，功能也更加强大，设计也更加复杂。

### 1.3.2 计算机局域网的组成

组成计算机局域网的部件，根据其作用不同，可分为网络服务器、客户工作站、网络接口卡、传输介质和网络软件系统等。

#### 一、网络服务器

目前流行的各种局域网，其访问控制方式均是集中控制型，其控制核心部件称为网络服务器，一般是一个高档微机或一个以大容量硬盘为主的专用服务器。微机局域网操作系统也都是运行在网络服务器上，通常网络中至少有一个服务器，其运行效率直接影响着整个局域网的效率，如何选择和配置网络服务器是组建网络时非常重要的问题。

##### 1 网络服务器的作用

(1) 运行网络操作系统：这是服务器的最主要功能。通过网络操作系统控制和协调网络各工作站的运行，处理和响应各工作站同时发来的各种网络操作要求。

(2) 存储和管理网络中的共享资源：网络中共享的数据库、文件、应用程序等软件资源；大容量硬盘、打印机、绘图仪及其他贵重设备等硬件资源均存放在网络服务器中，由网络操作系统对这些资源进行分配管理，使各工作站得以共享这些资源。

(3) 网络管理员在网络服务器上对各工作站的活动进行监视控制及调整。

(4) 在 Client/Server(客户/服务器)体系结构中，网络服务器不仅充当文件服务器，还应具有为各网络工作站的应用程序服务的功能。

##### 2 网络服务器的分类

按网络服务器的应用可分为：文件服务器、应用程序服务器、通信服务器等，通常一个网络至少有一个文件服务器，网络操作系统及其实用程序和共享硬件资源都安装在文件服务器上。早期微机局域网只有文件服务器概念。文件服务器只为网络提供硬盘共享、文件共享、打印机共享等功能，工作站需要共享数据时，便从文件服务器中去取过来，文件服务器只负责共享信息的管理、接收和发送，而丝毫不帮助工作站对所要求的信息进行处理。随着分布式网络操作系统和分布式数据库管理系统的出现，要求网络服务器不仅要具有文件服务器功能，而且要能够处理用户提交的任务。简单地说就是当某一网络工作站要对共享数据进行操作时，具体控制该操作的不仅是工作站上的处理

---

器，还应有网络服务器上的处理器，即网络中有多个处理器为一个事务进行处理，具有这种能执行用户应用程序功能的服务器叫应用程序服务器。人们所说的一般微机局域网中的工作站并不共享网络服务器的 CPU 资源，如果有了应用程序服务器就可以实现了。若应用程序是一个数据库管理系统，则有时也称之为数据库服务器。

## 二、客户工作站

工作站是网络各用户的工作场所，通常是一台带有硬盘的微机，也可以是不配有磁盘驱动器的“无盘工作站”。工作站通过插在其中的网络接口板（网卡）经传输介质与网络服务器相连，用户通过工作站向局域网请求服务和访问共享资源。它通过网络从服务器中取出程序和数据后，用自己的 CPU 和内存进行运算处理，处理结果可以再存到服务器中去。工作站可有自己的单独工作的操作系统，独立工作，但与网络相连时，需要将网络操作系统的一部分，即“工作站连接软件”安装在工作站上，形成一个专门的引导程序，访问服务器；在无盘工作站中必须在网络接口板上加插一片专用的启动芯片（远程复位 EPROM），用作从服务器上来引导本地系统。

## 三、网络接口卡

为了将服务器、工作站（通称智能设备）连到网络中去，需要在网络通信介质和智能设备之间用网络接口设备进行物理连接，局域网中由一块网络接口板（网卡）完成这一功能。

网卡基本功能包括：基本数据转换（例如并行到串行或串行到并行）、信息包的装配和拆装、网络存取控制、数据缓存、生成网络信号等。一方面，网卡要和计算机 RAM 交换数据；另一方面还必须以网络物理数据路径或介质的速度和格式传送或接收数据。在网络中数据是串行按位传送。如果网络与主机 CPU 之间速率不匹配，就需要缓存以防数据丢失。由于网卡处理数据包的速度比网络传送数据的速度慢，也比主机向网卡发送数据的速率慢，经常会现速率不匹配，成为网络与主机之间的瓶颈。

## 四、网络软件系统

网络软件是计算机网络系统不可缺少的重要资源。网络软件所涉及到和解决的问题要比单机系统中的各类软件都复杂。其复杂性主要表现在以下几个方面：

### 1、软件系统结构

虽然网络软件也同单机系统中软件系统一样，是一种层次结构，但由于各类网络软件之间联系密切，相互渗透，所以对网络软件来说没有明显的分层结构，层与层之间没有明显的界线，也就是说对许多网络软件来说，很难把它划分在某一确定的层次上。

### 2、软件功能

软件所要解决的问题多而复杂，并且涉及的范围广，内容丰富。

### 3、软件类型

软件的类型多种多样，难于标准化，这是由于网络体系的多样化、网络硬件的多样化和复杂化而造成的。根据网络软件在网络系统中所起的作用不同，可以将其分为：协议软件、通信软件、管理软件、网络操作系统和网络应用软件等。

## 1.4 计算机网络的功能和服务

### 1.4.1 计算机网络的功能

计算机网络是以资源共享为主要目标，它具备下述几个方面的功能：

#### （1）数据通信

该功能实现计算机与终端、计算机与计算机间的数据传输，这是计算机网络的基本功能。

#### （2）资源共享

网络上的计算机彼此之间可以实现资源共享，包括硬件、软件和数据。信息时代的到来，资源

---

的共享具有重大的意义。首先，从投资考虑，网络上的用户可以共享使用网上的打印机、存储设备等，这样就节省了资金。其次，现代的信息量越来越大，单一的计算机已经不能将其储存，只有分布在不同的计算机上，网络用户可以共享这些信息资源。再次，现在计算机软件层出不穷，在这些浩如烟海的软件中，不少是免费共享的，这是网络上的宝贵财富。任何连入网络的用户，都有权利使用它们。资源共享为用户使用网络提供了方便。

#### (2) 远程传输

计算机应用的发展，已经从科学计算到数据处理，从单机到网络。分布在远程的用户可以互相传输数据信息，互相交流，协同工作。

#### (3) 集中管理

计算机网络技术的发展和运用，已使得现代的办公手段、经营管理等发生了变化。目前，已经有了许多 MIS 系统、OA 系统等，通过这些系统可以实现日常工作的集中管理，提高工作效率，增加经济效益。

#### (4) 实现分布式处理

网络技术的发展，使得分布式计算成为可能。对于大型的课题，可以分解为许多的子课题，由不同的计算机分别完成，然后再集中起来，解决问题。

#### (5) 负荷均衡

负荷均衡是指工作被均匀的分配给网络上的各台计算机系统。网络控制中心负责分配和检测，当某台计算机负荷过重时，系统会自动转移负荷到较轻的计算机系统去处理。

由此可见，计算机网络可以大大扩展计算机系统的功能，扩大其应用范围，提高可靠性，为用户提供方便，同时也减少了费用，提高了性能价格比。

综上所述，计算机网络首先是计算机的一个群体，是由多台计算机组成的，每台计算机的工作是独立的，任何一台计算机都不能干预其他计算机的工作，例如启动、关机和控制其运行等；其次，这些计算机是通过一定的通信媒体互连在一起，计算机间的互连是指它们彼此间能够交换信息。网络上的设备包括微机、小型机、大型机、终端、打印机，以及绘图仪、光驱等设备。用户可以通过网络共享设备资源和信息资源。网络处理的电子信息除一般文字信息外，还可以包括声音和视频信息等。

### 1.4.2 计算机网络的服务

为了方便用户，计算机网络在其基本功能的基础上，又提供了许多非常有效的服务。不论是广域网还是局域网，通常都提供下述几种网络服务：(1) 电子邮件服务，(2) 文件传输服务，(3) 远程登录服务等。

#### (1) 电子邮件服务

电子邮件，也就是我们通常所说的 E-mail，是指借助电脑网络的连接，彼此传递信息的通信方式。它的通信方式与我们日常信件的交流方式十分相似，故称之为电子邮件。和普通信件一样，电子邮件也有它的通信地址，可以分为两个部分：前面是注册的用户名，后面是用户信箱所在的邮件服务器的域名，中间用“@”相连。比如：leejone@163.net。知道一个人的 Email 地址，我们就可以给他写信了，同样，如果你拥有一个 Email 信箱，也会收到别人的来信。

电子邮件之所以得到迅速的发展，主要是它与传统的通讯手段相比电子邮件比具有速度快、价格便宜、功能多等特点和优势。

#### (2) 文件传输服务

文件传输(FTP)是 Internet 提供的基本服务，它向所有的 Internet 用户提供了在 Internet 上传输任何类型的文件：文本文件、二进制文件、图像文件、声音文件、数据压缩文件等。

FTP 服务可以分为两种类型：普通 FTP 服务和匿名 Anonymous FTP 服务。普通 FTP 在 FTP 服务器向用户提供文件传输功能，而匿名 FTP 可向任何 Internet 用户提供文件传输功能。当用户不希

---

望在远程联机的情况下浏览存放在 Internet 联网的某一台计算机上的文件时，可能先将这些文件取回到用户自己在本地的联网计算机中，这样不但能为用户节省实时联机的长时间通信费用，还让用户认真阅读和处理这些取来的文件。Internet 提供的文件传输服务 FTP 正好能满足用户的这一需求。

### **(3) 远程登录服务**

指某台用户计算机通过该网络服务，暂时成为另一台远程主机的仿真终端。用户要使用远程服务时，应先在指定的远程主机上进行登录，以成为该主机的合法用户。登录成功后，用户便可在自己的仿真终端上实时地使用远程主机上对外开放的全部资源，比如访问该主机数据库中的数据。

### **(4) 共享硬盘服务**

在 LAN 中广泛提供共享硬盘服务。该服务允许连接在 LAN 上的多个工作站共享服务器上的硬盘，即将指定文件或数据部分或全部地存储在服务器的硬盘上，这样，工作站上便可不配置硬盘和软盘而形成无盘工作站，或者将另一部分可供全网用户使用的文件和数据存储在服务器的硬盘上，以便实现文件和数据共享。

### **(5) 共享打印机服务**

在 LAN 中，通常以共享硬盘为基础，又提供了共享打印机服务。该服务允许网上各工作站共享连接在服务器上的打印机，亦即当工作站需要打印数据时，可将要打印的数据送服务器，由服务器上的共享打印机进行(排队)打印。LAN 提供了该服务后，便不需再在所有的工作站上配置打印机。

## **1.5 中国计算机网络的发展**

我国的网络发展也是由来已久的。早在 60 年代初，计算机技术与通信技术相结合的研究课题便开始提上日程，也就有了网络的早期研究与应用。1960 年—1964 年中科院计算所、自动化所和七机部一院研制成功飞行器缓变参数遥测数据自动收集与处理系统（计算机与无线通信结合的系统）。60 年代中、后期建立了卫星地面测控系统（计算机与电话网专线结合的系统）。70 年代，计算机通信系统的应用扩展到国民经济领域。80 年代以后，局域网开始在国内应用，金融、气象、石化等部门开始率先建设专用广域计算机网，包括各种管理信息系统、办公自动化系统和金融电子化等专用业务网。

80 年代中到 1993 年是中国计算机互联网发展的重要时期，主要由高等院校和研究所的一些学者倡导和推动，为中国计算机互联网的形成和发展，在技术、人才方面准备了条件。如 1987 年，清华大学校园网建成为我国第一个用 TCP/IP 协议的校园网；次年，清华校园网通过中国公用数据网 CNPAC，开通了 Internet 电子邮件。1991 年，中科院高能物理研究所，采用 DECNET 协议，以 X.25 方式连入美国斯坦福大学的 LIVEMORE 实验室，开通了电子邮件。1989 年，中关村地区教育科研示范网（NCFC）立项，由中科院主持、联合北大、清华，在中关村地区建设了连接三个院校网的高速互联网络。

1993 年后，世界各国政府纷纷规划建设国家信息基础设施 NII，我国政府也着手规划建设中国国家信息基础设施。1993 年 12 月，国家经济信息化联席会议成立，1996 年 1 月，改为国务院信息化工作领导小组。1997 年 4 月，召开全国信息化工作会议，通过了“国家信息化九五规划和 2000 年远景目标”，将中国互联网列入国家信息基础设施建设，并提出建立国家互联网信息中心和互联网交换中心。1994 年 4 月 20 日，NCFC 网通过 64K 专线接入 Internet，这是国内第一个直接接入 Internet 的互联网。在此前后，1990 年 10 月，注册登记我国顶级域名 CN。1993 年制定了我国的域名体系。1994 年 5 月完成中国国家顶级域名 CN 服务器设置。

1994 年，中国四大互联网开始空前发展。1994 年 9 月，中国公用计算机互联网建设开始启动；1995 年 1 月，中国电信分别在北京、上海通过 64K 专线接入美国；1995 年 5 月，开始筹建中国公用计算机互联网全国骨干网，于 1996 年 1 月建成，1998 年 7 月，骨干网二期工程启动，带宽扩至 155M。1994 年 10 月，中国教育和科研计算机网工程建设启动，1995 年 7 月，连入美国的 128K 国际专线开通，1995 年 12 月，一期工程提前一年完成；1994 年春天，曙光 BBS 正式开通，成为中国

---

大陆第一个 Internet 上的 BBS。1995 年 4 月，中国科技网工程启动，同年 12 月，中科院百所连网工程完成。1996 年 9 月，中国金桥信息网连入美国的 256K 专线正式开通，并提供上网服务。1997 年，上述四大网实现互连互通。1997 年 6 月组建中国互联网信息中心（CNNIC）。

近年来，中国互联网的规模和应用有了很大发展，互联网用户数每半年增加一倍。中国互联网的发展还带动了国内各种专用计算机网络向 Intranet、Extranet 发展。并且，我国已进行了下一代高速信息网络的规划，1999 年 10 月至 2000 年 9 月，国家自然科学基金委资助建设了“中国高速互联研究试验网 NSFCnet”，并与美国 Internet2 实现互连；1999 年到 2000 年，863-300 项目建立了“中国高速信息示范网”（CAINONET）；中国网通公司于 2000 年开始建设高速 CNCnet。

### 1.5.1 中国的国家信息化

中国没有国家信息基础设施的提法，代之的是国家信息化的构想。中国的国家信息化是在国家统一规划和组织下，在农业、工业、科学技术、国防及社会生活各个方面应用现代信息技术，深入开发、广泛利用信息资源，加速国家实现现代化的进程。

国家信息化建设的目标是：到 2000 年，初步形成一定规模和比较完整的国家信息化体系；到 2010 年，将建立起健全的、具有相当规模的、先进的国家信息化体系。国家信息化体系由下列六个要素组成，即信息资源、国家信息网络、信息技术应用、信息技术与产业、信息化人才、信息化政策法规和标准。

可以看出，我国的信息化与外国的信息高速公路和国家信息基础设施有所不同。我国强调信息化体系六个要素之间的紧密关系，将信息资源开发利用放在核心地位。近年来，中国信息产业发展速度超过了国民经济的增长速度，电子工业年平均递增 30%，电信业平均递增 40% 以上。中国通信网基本上实现了数字化和程控化。全国已经初步建成以光缆为主，以数字微波和卫星通信为辅，多种手段并用的网络。

1993 年底国家有关部门决定兴建“金桥”、“金卡”、“金关”工程，简称“三金”工程。“金桥”工程是以卫星综合数字网为基础，以光纤、微波、无线移动等方式，形成空地一体的网络结构，是一个连接国务院、各部委专用网，与各省、市、大中型企业以及国家重点工程联结的国家公用经济信息通信网，可传输数据、语音、图像等，以电子邮件、电子数据交换（EDI）为信息交换平台，为各类信息的流通提供物理通道。金桥工程已在北京、天津、沈阳、大连、长春、哈尔滨、上海等全国 24 个中心城市利用卫星通信建立了一个以 VSAT 技术为主体，光纤为辅的卫星综合信息网络。

“金卡”，工程即电子货币工程。它的目标是用 10 年多的时间，在 3 亿城市人口推广普及金融交易卡、信用卡。“金关”工程是用 EDI 实现国际贸易信息化，进一步与国际贸易接轨。

### 1.5.2 中国公用分组交换数据网(ChinaPAC)

中国公用分组交换数据网(ChinaPAC)于 1993 年 9 月开通，1996 年底已经覆盖全国县以上城市 and 一部分发达地区的乡镇，与世界 23 个国家和地区的 44 个数据网互联。

#### 1 网络状况

分组交换网是邮电部门建设和发展最早的基础数据通信网络。分组交换网以 CITTX.25 建议为基础，可以满足不同速率、不同型号终端与计算机、计算机与计算机间以及计算机局域网之间的通信。分组交换网是一种基础的数据通信网络，在其网络平台上可以构架各种增值业务，如：电子信箱、电子数据交换、传真存储转发等。

ChinaPAC 由国家骨干网和各省（市、区）的省内网组成。目前骨干网之间覆盖所有省会城市，省内网覆盖到有业务要求的所有城市和发达乡镇。通过和电话网的互连，ChinaPAC 可以覆盖到电话网通达到的所有地区。ChinaPAC 设有一级交换中心和二级交换中心，一级交换中心之间采用不完全网状结构，一级交换中心到所属二级交换中心之间采用星状结构；ChinaPAC 在北京和上海设有国际出



---

入口，广州设有到港澳地区的出入口，以完成与国际数据的联网。

## 2 网络特点及业务功能

分组交换网的突出优点是可以在一条物理电路上同时开放多条虚电路，为多个用户同时使用；网络具有动态路由功能和复杂完备的误码纠错功能。X.25 协议是在物理链路传输质量很差的情况下开发出来的，为了保证数据传输的可靠性，她在每一段链路上都要执行差错检验和出错重传。这种复杂的差错校验机制虽然使它的传输效率受到了限制，但确实为用户数据的安全传输提供了很好的保障。ChinaPAC 提供的业务如下：

### (1) 本业务功能

基本业务功能是指向任一数字终端设备 (DTE) 提供的基本业务功能。它能满足用户对通信的基本要求。有两类基本业务：交换型虚电路 (SVC) 和永久型虚电路 (PVC)。

### (2) 任选业务功能

用户任选业务功能是为了满足用户的特殊需要，向用户提供的特殊业务功能，如入呼叫封阻、出呼叫封阻、单向入逻辑信道、单向出逻辑信道等。

### (3) 其他业务功能

ChinaPAC 还提供其他费 ITU-T 建议的业务功能，如虚拟专用网 (VPN)、TCP/IP、分组多址广播、呼叫改向等。

## 1.5.3 中国公用数字数据网 (ChinaDDN)

数字通信网 (DDN) 是利用数字通道提供永久性、半永久性连接线路，以传输数据信号为主的数字传输网络。它可以提供各种灵活的数据接口，为传送数据信号服务。由于它协议简单，速率较高，在我国得到迅速发展。

DDN 由数字通道、DDN 节点、网管系统和用户环路组成，它主要提供点到点和点到多点的数字专用线路业务，也可以提供帧中继和压缩语音/G3 传真业务。

### 1 DDN 的主要特点

(1) 传输质量高：由于目前 DDN 大量采用光纤传输通道，使得传输质量大大提高；

(2) 传输速率高：速率介于 2400BPS 到 2MBPS 之间；

(3) 协议简单：由于 DDN 主要采用时分复用和交叉连接技术，对用户信息进行全透明传输，对用户的技术要求较少，应用灵活；

(4) 在 DDN 网中，采用了先进的网管技术，线路调度、故障监控可以实现集中管理，线路遇故障时还可以自动路由迂回，提高了用户线路的利用率。

### 2 DDN 的业务应用

DDN 主要提供点到点的数字专用线路业务。广泛应用于银行、证券、气象、文化教育等领域，使用于 LAN 与 WAN 的互联、WAN 与 WAN 的互联等。例如，一个公司的总部和分部位于不同的地点，两点之间的通信又很频繁，不仅要保持电话联系，还有进行计算机联网通信。如果租用一条 DDN 专线，两端加上复用设备，把分布两地的电话系统和计算机系统连接起来，就可以在两地间方便地通信。这样既节省了两地之间的长途电话费用，又能实现计算机系统的互联互通。

DDN 还提供多点业务，主要指广播多点业务、双向多点业务 (轮询) 和会议电视业务。广播多点业务特点是：数据信息流可以从一点传送到多点，使多点同时获得同一信息。多点广播业务适用于信息颁布 (股票、新闻、气象预报等)。双向多点业务主要指一个主站在一个时刻可以和一个从站进行双向通信，主站定期访问一个从站，与从站交换信息。双向多点通信业务适用于集中监视、信用卡验证、数据服务、预定系统等领域。

### 3 ChinaDDN 的历史、现状及发展

公用数据网是邮电部门经营的、在全国范围内向用户提供服务的计算机网络。90 年代初，首先在城市发展起来，1994 年开始组建 CHINADDN 一级干线网。目前一级干线网已通达所有省会城

---

市，各省、直辖市、自治区都在积极建设经营 DDN 网，至 1996 年底，CHINADDN 已经覆盖到 2100 个县以上城市，发达地区已覆盖到乡镇，端口总数达 18 万个。目前，能为用户提供全国范围内的虚拟专用网 (VPN) 业务。

CHINADDN 按照网络的建设、经营、管理和维护的责任地理区域，划分为一级干线网、二级干线网和本地网三级。一级干线网由设置在各省、自治区和直辖市的节点组成，主要提供跨省长途 DDN 业务的转接，目前已通达除台湾外的所有省会城市。二级干线网由设置在省内的节点组成，它提供本省内长途和出入省的 DDN 业务。本地网是指城市范围内的网络，主要为用户提供本地和长途 DDN 业务。

目前，CHINDDN 已经成为邮电部门其他网络的支撑网。大量的 CHINDDN，CHINAFAX，CHINANET 的中继线路都开在 CHINADDN 上。CHINADDN 作为电话七号信令网一期工程的一个传输平面，将在电话网的建设中发挥重要的作用。部网管中心与各省网管中心联网的 DCN 工程也选择 CHINADDN 作为其传输通道，移动电话信令漫游、多媒体网都依靠 CHINADDN 来传送信息，CHINADDN 正日益成为电信各种业务的重要支撑。

另外社会各界也纷纷租用 CHINADDN 专线来开展自己的业务，各专业银行、证券公司、教育科研部门都是 CHINADDN 的用户群。

#### 1.5.4 中国公用帧中继网 (ChinaFRN)

中国公用帧中继宽带业务骨干网 (CHINAFRN) 是我国第一个向公众提供服务的宽带数据通信网络，其建成投产后对我国的国民经济信息化产生了积极的影响，成为我国信息高速公路的重要组成部分。

CHINAFRN 主要提供 64K 以上的中高速数据通信服务。业务类型既可以是突发性的，也可以是实时性的。

CHINAFRN 还可为其他数据通信网络提供高速中继传输，使得各网络的性能得以增强，同时提高线路的使用效率。

中国公用帧中继宽带业务骨干网的一个主要特点就是采用 ATM 技术平台，同时提供帧中继和信元中继等业务。CHINAFRN 主要技术特点：

- (1) 设备单机先进，网络整体性好，骨干枢纽采取全网状连接。
- (2) 网络业务种类齐全，提供帧中继 PVC、ATMPVC 和 SVC 等基本业务。
- (3) 端口种类齐全，速率范围广。对于帧中继业务，网络所提供的接口类型包括 v35、x.21、E1、信道化 E1、ISDNPRI、E3 等。对于 ATM 业务，网络所提供的接口类型有 E1、E3、STM-1 等。
- (4) 用户接入方式灵活。支持帧中继或 ATM 协议的终端设备可以直接接入；局域网可通过路由器、局域网交换机直接接入；其他协议终端可通过 FRAD 设备进行接入。此外，由于网络端口本身内置 FRAD 功能，支持 HDLC、SDLC 和 PPP 协议的终端也可直接接入。
- (5) 支持帧中继、ATM 互通功能。

#### 1.5.5 中国科学技术网 (CSTNet)

中国科学技术网络经历了四个不同的工程发展阶段，NCFC，CASNET，CERNET，CSTNET。

##### 1 NCFC

NCFC (THE NATIONAL COMPUTING AND NETWORKING FACILITY OF CHINA) 是中国国家计算与网络设施的英文缩写，是世界银行贷款“重点学科发展项目”中的一个高技术基础设施项目。该项目由中国科学院主持，联合北京大学、清华大学共同完成。项目总经费约七千万元，主要来自世界银行贷款及国家计委的配套资金，部分来自国家自然科学基金委、国家科委、以及三个院校的自筹资金。

NCFC 网络由四级组成，广域网，城域网 (主干网)，院校网，局域网。

---

局域网是最基层的网络设施，安装在中国科学院中关村地区的近四十个研究所、两所大学的各教学楼里，每个所、系可有一至几个局域网，取决于该所、系的建筑物分布情况。局域网采用以太网(IEEE 802.3)结构，提供所有计算机入网的接入点。

院校网是利用光缆、网桥、路由器、FDDI 集中器、程控交换机等设备将院校内所有以太网互连而成的网络。三个院校网分别称为 CASNET-BEIJING(中国科学院院网北京部分)、PUNET(北京大学校园网)、TUNET(清华大学校园网)。

城域网即 NCFC 主干网，由光缆及路由器、网桥等设备组成。NCFC 主干网将三个院校网的网络中心用单模和多模光缆互连成一个三角型，早期通信速率为 10MBPS，后来改为 100MBPS 的 FDDI 连接。NCFC 主干网在中科院计算机网络信息中心设立了全网的网络中心，设置了网络监控、网络服务、科学数据库服务、网络超级计算能力、国际出入口等各种设施。

广域网即 NCFC 主干网向北京市及全国各地的扩展。主要的连接手段为 DDN 专线、CHINAPAC 公用分组交换网、电话网、微波等。卫星、帧中继等通信技术，也正在逐步引入。到 1994 年 5 月，NCFC 工程基本完成时，已连接了 150 多个以太网，3000 多台计算机，其中工作站以上的机器 800 多台，每天有数千名科研、教育人员使用。每天从国外进来的信息量 300-400MB，出国的信息量 250-300MB。

## 2 CASnet

CASNET 是中国科学院的全国性网络建设工程。该工程分为两部分，部分为分院区域网络工程，另一部分是用远程信道将各分院区域网络及另星分布在其他城市的研究所互连到 NCFC 网络中心的广域网工程。

分院区域网络 中国科学院除北京的总部及 50 多个研究所外，有 12 个分院，分布在上海、南京、合肥、武汉、广州、成都、兰州、西安、沈阳、长春、昆明、乌鲁木齐等城市。还有一批另星研究所分布在青岛、大连、哈尔滨、太原、石家庄、长沙、贵阳、西宁、福州等城市。在建设 NCFC 的同时，中国科学院从 1992 年开始，陆续安排建设分院区域网络。

广域网 1995 年底，CASNET 完成了将 12 个分院区域网及其他城市的研究所连到北京的广域网工程，连接了 24 个城市。作为第一步，1995 以前，连接通过 CHINAPAC 实现，速率为 9.6KBPS-64KBPS 不等。不久，各分院的网络改用 DDN 专线或帧中继(FR)，有的研究所仍暂时沿用 CHINAPAC 信道。

## 3 CERNET

在建设 NCFC 与 CASNET 的同时，中国科学院于八十年代后期启动了两个重大的项目，一个是“中国生态研究网”(CER-CHINESE ECOSYSTEM RESEARCH NETWORK)，另一个是“生物多样性研究与信息管理”(BRIM-BIODIVERSITY RESEARCH AND INFORMATION MANAGEMENT)。两个项目的总投资达两亿元。由世界银行贷款 1550 万美元，国家计委拨款，中国科学院筹集部分资金。其中生物多样性项目，也将以 CERNET 作为通信平台。CERN 分成三层结构，最高层是一个综合中心；中间层为四个分中心(土壤分中心、大气分中心、生物分中心、水分中心)；下层为一批遍布全国的生态系统台站。网络的核心是高速的 FDDI 光纤环，三个分中心在北京，以高速信道互联，一个分中心在南京，经 CHINAPAC 和帧中继连接，生态台站的连接主要靠 CHINAPAC、电话专线、拨号、无线通信、卫星线路等。CERN 与 CASNET 以高速光缆互连，速率为 100MBPS，由于它也属中国科学院，从网络结构看，它可被看作是 CASNET 的一部分。

## 4 CSTNET

CSTNET 是以 NCFC 及 CASNET 为基础，连接了中国科学院以外的一批中国科技单位而构成的网络。CSTNET 为非盈利网络，为科技用户、科技管理部门及与科技有关的政府部门服务。目前的 64KBPS 将升级到 E1(2.048MBPS)，并与高能所的国际出口互为备份，统一管理。

接入 CSTNET 的单位有农业、林业、医学、电力、地震、气象、铁道、电子、航空航天、环境保护等近二十个科研部门及国家自然科学基金委、国家专利局等科技管理部门。国家科技网络将

---

从两个方面发展扩大网络规模，加强网络服务能力。

### 1.5.7 中国教育和科研网(CERNet)

“中国教育和科研计算机网”的总体建设目标，是利用先进实用的计算机技术和网络通信技术，把全国大部分高等学校连接起来，推动这些学校校园网和信息资源的建设交流，与现存的国际性学术计算机网络互连，使其成为中国高等学校进入世界科学技术领域快捷方便的入口。同时成为培养面向世界、面向未来高层次人才，提高教学质量和科研水平的最重要的基础设施。在条件成熟时，为其它部门提供服务，并与国内其它计算机网络相互连接，逐步形成覆盖全国的计算机网络。

“中国教育和科研计算机网 CERNET”是一个包括全国主干网，地区网和校园网在内的三级层次结构的网络。建设内容包括，连接八个地区网络的全国主干网和国际连网；全国网络中心；八个地区网络中心和若干地区网点；功能齐备的网络管理系统，保证网络高效可靠地运行；提供较丰富的网络应用资源和便利的资源访问手段。“中国教育和科研计算机网”的网络中心建在清华大学，地区网络中心分别设在北东、上海、南京、西安、广州、武汉、成都、沈阳等八个城市的一所著名大学。

CERN 采用三层网络管理结构，即国家主干网，地区网和校园网。

主干网拓扑结构：以北京为中心的三环拓扑结构。

主干网通信线路：DDN 专线，最高传输速率可达 64Kbps 至 2.048Mbps。用 X.25 作为后备线路。

国际联网：在北京设置国际出口，开通到美国的 INTERNET 国际信道，速率为 128Kbps 至 2Mbps。另外，还开通到香港 HARNET 和德国 DFN 的国际信道。

中国教育和科研计算机网具有全国性的覆盖范围，而且与国际计算机网络互连，因此采用 Internet 的 TCP/IP 网络体系结构。中国教育和科研计算机网络将充分利用国家已有的公共通信传输设施。租用数字数据网 DDN 的光缆线路组建其主干网，并根据使用情况逐步提高其传输速率。

中国教育和科研计算机网主干网结点位置的选择考虑到了中国高校及大学生分布情况、通信基础设施建设的具体情况和地理位置等因素。北京、上海、沈阳、广州、武汉、成都、南京、西安八大城市，既是中国 DDN 骨干网的枢纽局和我国公用分组交换网及长途电话网的汇接结点，又是高等院校和科研院所相对较为集中的地区中心，具有较好的通信基础条件和较强的科研能力、水平。因此将主干网结点设置在这些城市，并以这些城市为中心，构筑地区网络，对于将 CERNET 建设成为覆盖全国的教育和科研网是有利的。

中国教育和科研计算机网的网络中心设在清华大学，通过网络中心，与国际性学术计算机网络 Internet 连网。网络中心的主要职能包括，网络运行中心 NOC；网络信息中心 NIC；高性能计算中心 HPCC 和教育培训中心等。中国教育和科研计算机网的地区网络中心的主要职能是负责本地区网络建设的有关事宜。地区网点是各地区高校连网的中心，负责这些高校的连网，并提供技术支持和服务，也是网络管理和各种网络应用及服务的分中心。

## 第二章 计算机网络的体系结构

要想让计算机之间进行通信，必须使它们采用相同的信息交换规则。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规则称为网络协议或通信协议。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巨大的协议来为所有形式的通信的细节，而是采用把通信问题划分为许多个子问题，然后为每个子问题设计一个单独的协议的方法。这样可以使得每个协议的设计、分析、编码和测试都比较容易。分层技术是一种用于开发网络协议的设计方法。

### 2.1 计算机网络体系结构概述

#### 2.1.1 计算机网络体系结构的定义

**计算机网络体系结构**是关于**计算机网络应设置哪几层，每层应提供哪些功能的精确定义**。功能如何实现，则不属于网络体系结构部分。网络体系结构只是从功能上描述计算机网络的结构，而不涉及每层硬件和软件的组成，也不涉及这些硬件或软件的实现问题。因此，计算机网络体系结构是抽象的。定义和描述一组用于计算机之间互连的标准和规范的集合，遵循这组规范可以很方便地实现计算机之间的通信。将计算机网络的层次及其各层协议的集合，称为计算机网络体系结构。计算机网络体系结构是抽象的，而实现则是具体的，是真正在运行的计算机硬件和软件。

1974 年，美国 IBM 公司首先公布了世界上第一个计算机网络体系结构（SNA，System Network Architecture），叫**系统网络体系结构 SNA**。凡是遵循 SNA 的网络设备都可以很方便地进行互连，凡是遵循 SNA 的设备叫 SNA 设备。在此以后，各公司纷纷推出自己的网络体系结构，像 DNA，TCP/IP 等。这些网络结构均采用了层次技术，但层次的划分、功能的分配及采用的方法均不相同，以适合本公司生产的计算机组成网络。随着信息技术的发展，不同结构的计算机网络互连已成为人们迫切需要解决的问题。于是，国际标准化组织于 1977 年提出了开放系统互连参考模型 OSI。

#### 2.1.2 网络协议

大多数的计算机网络都采用层次式结构，即将一个计算机网络分为若干层次，处在高层次的系统仅是利用较低层次的系统提供的接口和功能，不需了解低层实现该功能所采用的算法和协议；较低层次也仅是使用从高层系统传送来的参数，这就是层次间的无关性。因为有了这种无关性，层次间的每个模块可以用一个新的模块取代，只要新的模块与旧的模块具有相同的功能和接口，即使它们使用的算法和协议都不一样。当任何一层发生技术上的变化，只要层间接口关系保持不变，则在这层以上或以下各层均不受影响。此外，对某一层提供的服务还可进行修改。当某层提供的服务不再需要时，甚至可以将这层取消。

**网络中的计算机与计算机间要能够正确的传送信息和数据，必须在数据传输的顺序、数据的格式及内容等方面有一个约定或规则**，这种约定或规则称**网络协议**。网络协议主要有三个组成部分：

**语法**：将若干个协议元素和数据组合在一起用来表达一个完整的内容所应遵循的格式，也就是**对信息的数据结构做一种规定**。例如用户数据与控制信息的结构与格式等。

**语义**：**是对协议元素的含义进行解释**，不同类型的协议元素所规定的语义是不同的。

**规则**：**对事件实现顺序的详细说明**。例如在双方进行通信时，发送点发出一个数据报文，如果目标点正确收到，则回答源节点接收正确；若接收到错误的信息，则要求源节点重发一次。

由此可以看出，协议实质上是网络通信时所使用的一种语言，是计算机网络的不可缺少的组成部分。

### 2.1.3 层次模型及其划分原则

#### 1、层次模型

计算机网络系统是一个十分复杂的系统。将一个复杂系统分解为若干个容易处理的子系统，然后“分而治之”，这种结构化设计方法是工程设计中常见的手段。分层就是系统分解的最好方法之一。在(图 2-1)所示的一般分层结构中， $n$  层是  $n-1$  层的用户，又是  $n+1$  层的服务提供者。 $n+1$  层虽然只直接使用了  $n$  层提供的服务，实际上它通过  $n$  层间接地使用了  $n-1$  层以及以下所有各层的服务。

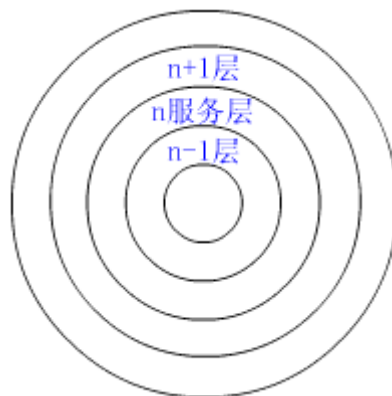


图 2-1 层次模型

层次结构的优点在于使每一层实现一种相对独立的功能。分层结构还有利于交流、理解和标准化。计算机网络的层次结构一般以垂直分层模型来表示(图 2-2)。

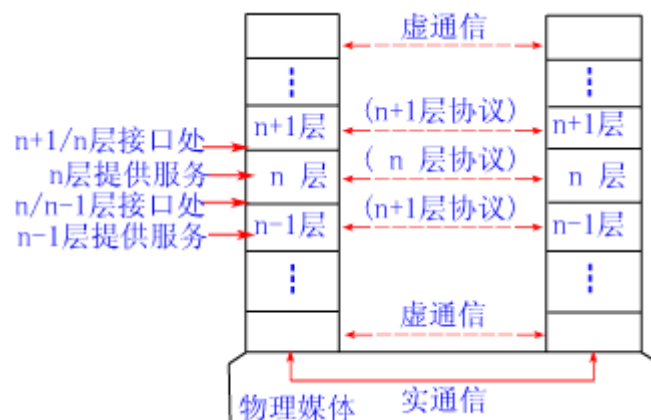


图 2-2 计算机网络的层次模型

#### 2、层次结构的特点

把功能作为划分层次的基础，第  $n$  层的实体在实现自身定义的功能时，只能使用第  $n-1$  层提供的服务，第  $n$  层在向第  $n+1$  层提供的服务时，此服务不仅包含第  $n$  层本身的功能，还包含由下层服务提供的功能，仅在相邻层间有接口，且所提供服务的实现细节对上一层完全屏蔽。因此，层次结构的主要特点：

- 1) 除了在物理媒体上进行的是实通信之外，其余各对等实体间进行的都是虚通信。
- 2) 对等层的虚通信必须遵循该层的协议。

3)  $n$  层的虚通信是通过  $n/n-1$  层间接口处  $n-1$  层提供的服务以及  $n-1$  层的通信（通常也是虚通信）来实现的。

### 3、层次结构划分的原则

分层时应注意使每一层的功能非常明确。当层次数太少，就会使每一层的协议太复杂。层次数太多又会在描述和综合各层功能的系统工程任务时遇到较多的困难。层次结构划分层次的原则：

1) 每层的功能应是明确的，并且是相互独立的。当某一层的具体实现方法更新时，只要保持上、下层的接口不变，便不会对邻居产生影响。

2) 层间接口必须清晰，跨越接口的信息量应尽可能少。

3) 层数应适中。

## 2.2 网络标准化组织

所谓标准即是推动某一特定产品或服务应如何被设计或实施的技术规范。通过标准，不同的生产厂商可以确保产品、生产过程以及服务适合他们的目的。由于计算机工业发展迅速，许多不同的组织都开发自己的标准。如，ANSI 和 ITU 均负责 ISDN (综合业务数字网) 通信标准，而 ANSI 制定接收一个 ISDN 连接所需要的硬件种类，ITU 判定如何使 ISDN 链接的数据以正确序列到达用户。管理和建立计算机网络的所有标准是几个重要组织，这些组织，将负责建立网络的未来。

### 2.2.1 ANSI

ANSI (美国国家标准协会) 是由 1000 多名来自工业界和政府的代表组成的组织，负责制定电子工业的标准，此外也制定其他行业的标准，如化学和核工程、健康和安全以及建筑行业。ANSI 也代表美国制定国际标准。ANSI 并不命令生产厂商服从它的标准，而是请它们自愿遵守其标准。当然，生产厂商和开发者也通过遵从标准获得潜在客户。遵从标准，其系统将会是可靠的，可与既存基础设施集成。新的电子设备和方法必须通过严格测试才可获得 ANSI 的认可。ANSI 标准的一个例子即是 ANSI T1.240 - 1998, “电信—操作、管理、维护、供应—操作系统和网络部件之间接口的通用网络系统信息模型”。可以通过 ANSI 网站 ([www.ansi.org](http://www.ansi.org)) 在线购买 ANSI 标准文档，也可通过一个大学或公共图书馆找到它们。要想成为一个合格的网络专业人士，无需阅读全部 ANSI 标准，但你应理解 ANSI 影响的范围之广，意义之大。

### 2.2.2 EIA

EIA (电子工业联盟) 是一个商业组织，其代表来自全美各电子制造公司。1924 年 EIA 作为 RMA (无线电生产厂商协会) 产生，时至今日，它已涉及到电视机、半导体、计算机以及网络设备。该组织不仅为自己的成员设定标准，还帮助制定 ANSI 标准，并进行游说促使建立更有利于计算机和电子工业发展的立法。EIA 包括几个下属组织：电信工业协会 (TIA)；用户电子生产商协会 (CEMA)；电子部件、组装、设备与供应协会 (ECA)；联合电子设备工程委员会 (JEDEC)；固态技术协会；政府处以及电子信息组 (EIG)。除了促使立法及制定标准，每个特定组根据自身的研究领域，还负责承办会议、展览及研讨会。从网站 <http://www.eia.org>，你可获得更多的 E I A 信息。

### 2.2.3 IEEE

IEEE (电气与电子工程师学或称为 I3E)，是一个由工程专业人士组成的国际社团，其目的在于促进电气工程和计算机科学领域的发展和教育。IEEE 主办大量的研讨会、会议和本地分会议，发行刊物以培养技术先进的成员。同时，IEEE 有自己的标准委员会，为电子和计算机工业制定自己的标准，并对其他标准制定组织如 ANSI 的工作提供帮助。IEEE 技术论文和标准在网络专业受到高度重视。尤其你在网络接口卡手册中经常可发现对 IEEE 标准的引用。它目前已被广泛使用的



标准已有几百项，可通过 IEEE 的网站 <http://www.ieee.org> 在线订购这些文档，或在大学或公共图书馆找到它们。

#### 2.2.4 ISO

ISO（国际标准化组织）是一个代表了 130 个国家的标准组织的集体，它的总部设在瑞士的日内瓦。ISO 的目标是制定国际技术标准以促进全球信息交换和无障碍贸易。你可能认为该组织应被简称为“IOS”，但“ISO”并不意味着是一个首字母缩略字。实际上，在希腊语中，“ISO”意味着“平等”。通过这个词汇表达了组织对标准的贡献。ISO 的权威性不仅限于信息处理和通信工业，它还适用于纺织业、包装业、货物分发、能源生产和利用、造船业，以及银行业务和金融服务。关于螺纹、银行信用卡，甚至货币名称的通用协议都是 ISO 的工作产物。事实上，在 ISO 的大约 12000 标准中，仅有大约 500 个应用于计算机相关的产品和功能中。国际电子与电气工程标准是由一个相似的国际标准组织 IEC（国际电子技术协会）单独制定的。ISO 所有的信息技术标准设计与 IEC 相一致。可通过 ISO 的网站 <http://www.iso.ch> 获得更多 ISO 的信息。

#### 2.2.5 ITU

ITU（国际电信同盟）是联合国特有的管理国际电信的机构，它管理无线电和电视频率、卫星和电话的规范、网络基础设施、全球通信所使用的关税税率。它为发展中国家提供技术专家和设备以提高其技术基础。ITU 于 1865 年成立于巴黎，1947 年成为联合国的一部分，并迁址瑞士的日内瓦。ITU 的成员来自于 188 个国家，所发行的详细政策和标准可从网址 <http://www.itu.ch> 上找到。通常 ITU 文档中有关全球电信问题的内容比工业技术规范多。ITU 关于全球电信问题文档的例子有“农村和边远地区的通信”、“电信对环境保护的支持”、“国际频率列表”。

## 2.3 OSI/RM 参考模型

### 2.3.1 开放系统互连参考模型

虽然网络体系结构在 20 世纪 70 年代后期得到了蓬勃发展，但这些网络结构都是以自己公司的产品为对象，不具备与其它公司网络结构的兼容性。随着网络的不断发展，需要有一个国际标准。在这种形势下，开放系统互连参考模型应运而生。

开放系统互连参考模型即 OSI/RM (Open System Interconnection / Reference Model)，它是在两大国际组织 ISO 和 CCITT 的共同努力下制定出来的。ISO 主要负责工业产品的标准化。CCITT 主要从事与电报、电话、数据通信有关的协议和标准化。起初 ISO 主要关心信息的处理，CCITT 则从通信的角度考虑制定标准。随着科学技术的发展，通信与信息处理的角度变得比较模糊。于是，通信与信息处理就都成为 ISO 和 CCITT 共同关心的领域。因此在制定 OSI / RM 标准上，两家一直在协手并进，共同制定。

现在大家都用简称 OSI 来表示开放系统互连 (Open System Interconnection)。所谓“开放”，就是指：只要遵循 OSI 标准，一个系统就可以和世界上任何地方的、也遵循这同一标准的其他任何系统进行通信。SNA 不是开放系统。

**“系统”**是指按一定关系或规则工作在一起的一组物体或一组部件。**“实系统”**表示在现实世界中能够进行信息处理的自治整体，可以是一台计算机或者多台计算机以及和这些计算机相关的软件、外部设备、终端、操作员、信息交换方式的集合。如果这些实系统通信时遵守 OSI 标准，则这个实系统称为**“开放实系统”**。一个开放实系统的各部分功能不一定都与互连有关。开放实系统中与互连有关的部分称为**“开放系统”**。

分层是制定网络体系结构时常采用的方法，分层技术是一种处理复杂问题的好技术，但分层

是影响计算机网络体系结构性能的主要因素。目前还没有一种理想的分层方法，OSI / RM 遵循以下规则：

- 1、结构的层次不能太多，以免造成系统结构的繁杂；结构的层次太少会使每层协议过于复杂。
- 2、当必须区分不同类型功能群时，应设置一层。
- 3、每一层只与它相邻的上、下层发生关系，且层与层边界的选取应使通过边界的信息量尽可能少。
- 4、每层功能应非常明确。

依据这些原则，经反复研究讨论，OSI 参考模型采用了 7 个层次的体系结构（图 2-3）。

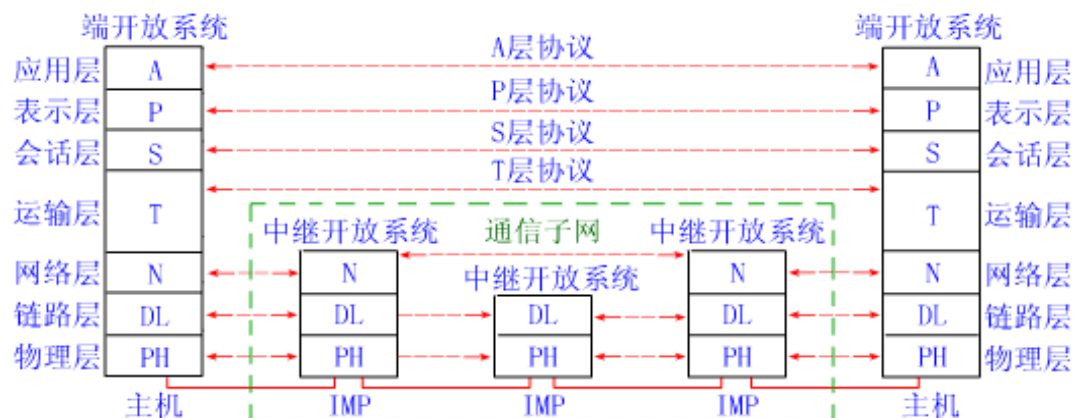


图 2-3 OSI 参考模型体系结构

### 2.3.2 OSI 参考模型各层的主要功能

OSI/RM 的概念比较抽象，它并没有规定具体的实现方法和措施，更未对网络的性能提出具体的要求，它只是一个为制定标准用的概念性框架。OSI/RM 七层协议模型上、下大，中间小，这是因为最高层要为各种类型的应用进程提供接口，而最低层要提供各种类型的网络接口，因此上、下两头标准特别多，而中间几层标准就稍简单些。有些层的任务过于繁重，如数据链路层和网络层，有些层的任务又太轻，如会话层和表示层。

#### 1 物理层

物理层在物理信道实体之间合理地通过中间系统，为比特传输所需的物理连接的激活、保持和去除提供机械的、电气的、功能性和规程性的手段。比特流传输可以采用异步传输，也可以采用同步传输完成。物理层是 OSI 参考模型的最低层，也是在同级层之间直接进行信息交换的唯一一层。物理层负责传输二进制位流，它的任务就是为上层(数据链路层)提供一个物理连接，以便在相邻节点之间传送二进制位流。物理层要定义的是多大的电压代表‘1’，多大的电压代表‘0’，连接电缆的插头尺寸多大等。

#### 2 数据链路层

数据链路层的主要作用是通过一些数据链路层协议和链路控制规程，在不太可靠的物理链路上实现可靠的数据传输。“线路 (Line)”、“链路 (Link)”和“数据链路”是不同的概念。线路中间没有任何交换节点，而链路是一条无源的端到端的物理线路段，在进行数据通信时，两台计算机之间的通信链路往往是由许多线路串接而成。把实现控制数据传输的一些规程的硬件和软件加到链路上就构成了像数据管道一样的数据链路。链路称为物理链路，而数据链路称为逻辑链路，在物理链路加上必要的通信规程就是数据链路。

数据链路层的作用是将物理层提供的可能出错的物理链路改造成为逻辑上无差错的数据链路，即使之对网络层表现为一条无差错的链路。数据链路层的基本功能是向网络层提供透明的和可靠的数据传送服务。

### 3 网络层

网络层是在数据链路层提供的两个相邻结点之间的数据帧的传送功能上，进一步管理网络中的数据通信，将数据设法从源端经过若干个中间节点传送到目的端，从而向运输层提供最基本的端到端的数据传送服务。网络层关系到通信子网的运行控制，体现了网络应用环境中资源子网访问通信子网的方式，是 OSI 模型中面向数据通信的低三层中最为复杂、关键的一层。网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括路由选择、阻塞控制和网际互连等。

### 4 传输层

传输层的任务是在端到端之间提供可靠的报文传输，向会话层提供一个可靠的端到端服务，使会话层以上看不见传输层以下的通信细节，传输层以上各层不再管数据传输的问题了。传输层是 OSI/RM 模型中负责数据通信的最高层，也是面向网络通信的低三层和面向信息处理的高三层之间的中间层。传输层位于网络层之上、会话层之下，它利用网络层提供给它的服务开发本层的功能，并实现本层对会话层的服务。正因为如此，传输层是计算机网络体系结构中最重要的一层，传输层协议也是最复杂的协议，其复杂程度取决于网络层所提供的服务类型及上层对传输层的要求。传输层协议通常由网络操作系统的一部分来完成。

### 5 会话层

会话层是建立在传输层之上，由于利用传输层提供的服务，使得两个会话实体之间不考虑它们之间相隔多远、使用了什么样的通信子网等网络通信细节，进行透明的、可靠的数据传输。会话层在两个相互通信的实体之间，建立、组织、协调其交互。两个应用进程进行相互通信时，希望有个第三方的进程能管理它们的通话，协调它们之间的数据流，以便使应用进程专注于信息交互。会话层就是为了达到这个目的，因此，会话层是在传输层的基础上进行增值服务，向会话的应用进程之间提供会话管理和同步服务，对数据的传输提供控制和管理，以达到协调会话过程，为表示层实体提供更好的服务。

### 6 表示层

表示层位于 OSI 参考模型的第六层。它的低五层用于将数据从源主机传送到目的主机，而表示层则要保证所传输的数据经传输后其意义不改变。因此，表示层要解决的是处理两个应用实体之间进行数据交换的语法问题，解决数据交换中存在的格式不一致以及数据表示方法不相同等问题，如何描述数据结构并使之与机器无关。表示层还必须提供数据压缩、数据加密解密等服务。

### 7 应用层

应用层是用户应用程序访问网络服务的接口，它为用户的应用进程访问 OSI 环境提供服务。OSI/RM 模型中应用层包含的协议最多。

#### 2.3.3 虚拟通信与实际信息流向

在 OSI/RM 中，通信在对等层的实体之间进行。实际上，除物理层外，同等层之间并没有直接的物理通信。尽管第 N 层协议是不同机器上两个 N 层实体之间的通信规则，但这个通信是虚的。因此对等层之间的通信为虚拟通信。实际的通信在相邻层之间通过层间接口进行。实际的信息流如下图 2-4 所示。

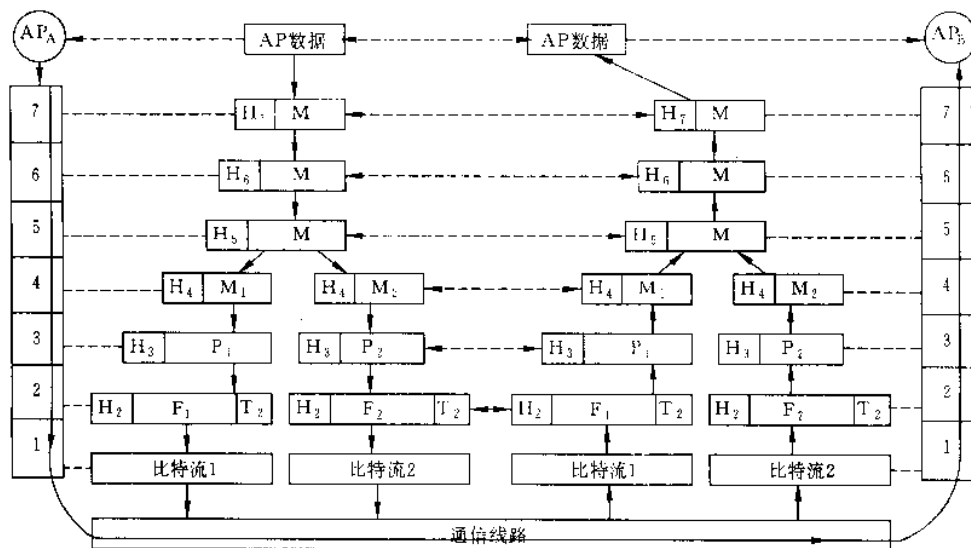


图 1-10 开放系统互连环境中的信息流

图 2-4 OSI/RM 的信息流

应用进程 A 先将其数据交给第 7 层，第 7 层在这个报文 (MESSAGE) 上加上若干比特的控制信息，这些控制信息称为报头 (Header)，成为下一层的数据单元。第 6 层收到这个报文后，加上该层的报头传送给第 5 层。第 5 层对收到的报文加上第 5 层的报头传到第 4 层。假定因报文过长第 4 层对收到的报文作一些处理，把 M 分成两个分组 P1 和 P2。每个分组分别加上第 4 层的控制信息发送到第 3 层。第 3 层把第 4 层传来的报文分组及报头看成是高层数据单元，再加上第 3 层的报头发往第 2 层。第 2 层加上自己的头部和尾部构成第 2 层的数据单元“帧”，传送给第 1 层，第 1 层 (物理层) 由于是比特流的传送，所以不再加控制信息。当比特流经网络的传输介质送到目的站时，就从第 1 层依次上升到最高层，每层根据控制信息进行必要的操作。然后将控制信息丢弃，将剩下的数据单元交给相邻上层，最后把应用进程 APa 发送的数据交给目的应用进程 APb。由此可见，除物理层外，信息交换是在同一系统中纵向进行的，并没有在不同系统的同级层之间进行。但对每一实体来讲，由于这些复杂的过程都交给通信处理软件去处理，对进行通信的实体来讲是“透明”的，所以从进行通信的同等层实体来看，好像信息是直接传递给对方。对等层之间的通信，即虚拟通信。

对等层实体之间虚拟通信的概念是非常重要的，只有在理解它的基础上才能正确理解网络体系结构的分层思想 (图 2-5)。

#### 2.3.4 协议、服务、服务访问点

研究开放系统中进行交换信息时，发送或接收信息的究竟是一个进程、是一个文件还是一个终端，都没有实质上的影响。为此，可以用实体这一名词表示任何可发送或接收信息的硬件或软件进程。在许多情况下，实体就是一个特定的软件模块。

**协议**是控制两个对等实体进行通信规则的集合，协议的语法方面的规则定义了所交换信息的

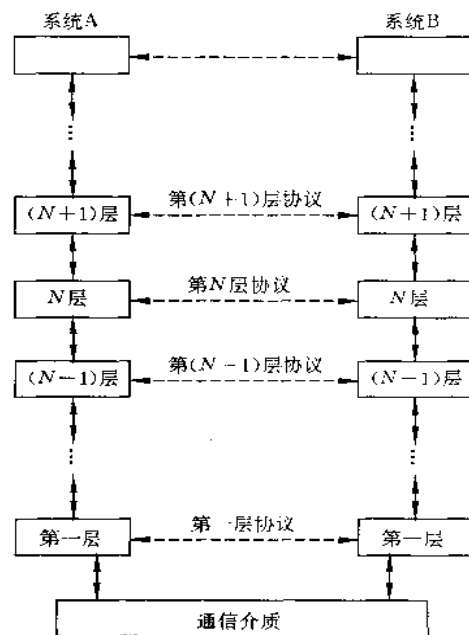


图 1-8 计算机网络的层次结构

图 2-5 计算机网络的层次结构

格式，而协议的语义方面的规则就定义了发送者或接收者所要完成的操作。在协议的控制下，两个对等实体间的通信使得本层能够向上一层提供服务。要实现本层协议，还需要使用下面一层所提供的服务。协议和服务在概念是有区别的。第一，协议的实现保证了能够向上一层提供服务。本层的服务用户只能看见服务而无法看见下面的协议，下面的协议对上面的服务用户是透明的。第二，协议是控制对等实体之间通信的规则，是实现虚通信的；而服务是由下层向上层通过层间接口提供的，实现的实通信。并非在一个层内完成的全部功能都称为服务，只有那些能够被高一层看得见的功能才能称之为“服务”。上层使用下层所提供的服务必须通过与下层交换一些命令，这些命令在 OSI 中称为服务原语。

在同一系统中相邻两层的实体进行交互(即交换信息)的地方服务访问点。服务访问点 SAP 是一个抽象的概念，是相邻两层实体的逻辑接口（图 2-6 所示）。在一个系统的两层之间可以允许有多个服务访问点，每个 SAP 都有一个唯一的地址码，供服务用户间建立连接之用。

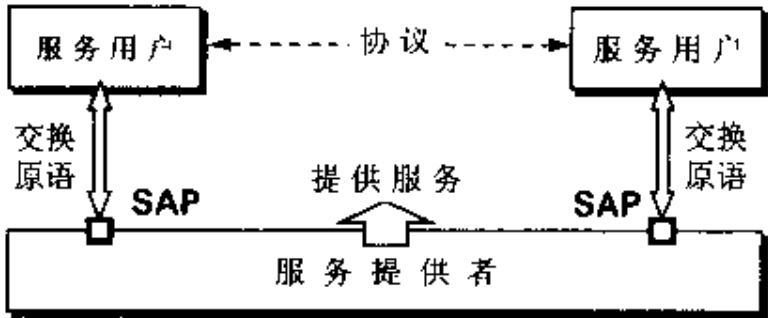


图 1-14 相邻两层之间的关系

图 2-6 相邻两层之间的关系

### 2.3.5 信息传送单元

OSI 参考模型中，信息传递的数据单元共分 3 种。

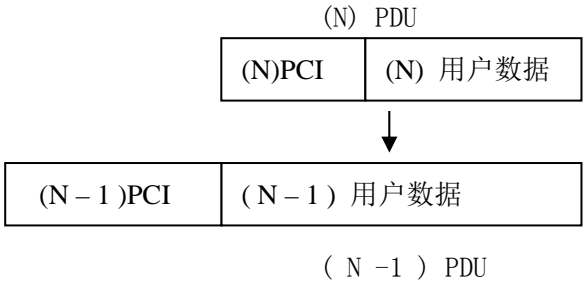
#### 1 协议数据单元 (PDU)

在 OSI 参考模型中，每一层都将建立协议数据单元 (PDU)。PDU 包含来自上层的信息，以及本层的控制信息。然后，这个 PDU 被传送到下一较低的层。接收端自下而上传送这些 PDU，在每一层分离出 PDU 中的相关信息。重要的一点是，每一层附加到 PDU 上的信息，是指定给另一个系统的同等层的。因此，协议数据单元就是在不同站点的各层对等实体之间，为实现该层协议所交换的信息单元。PDU 在不同的层有不同的叫法。在物理层称作比特流，在数据链路层称作数据帧，在传输层中称为数据段或报文段，在应用层中称作报文等。

第 N 层协议数据单元记为：(N)PDU

(N)PDU 包含二个部分：本层的用户数据和本层的协议控制信息（图 2-7）。

(N)PDU = (N) 用户数据 + (N) PCI



( N - 1 ) PDU

图 2-7 PDU 的组成

## 2 接口数据单元 (IDU)

相邻层通过接口通信交换的数据单元称为接口数据单元 (IDU)。IDU由接口控制信息ICI和服务数据单元SDU组成。相邻层间的服务是通过其接口界面上的服务访问点SAP进行的，n层的SAP是n+1 层可以访问n 层的访问点。

## 3 服务数据单元 (SDU)

实体为了完成服务用户所请求的功能所需要的数据单元。服务数据单元是层与层之间交换的数据单位。协议数据单元、(PDU) 接口数据单元 (IDU)、服务数据单元 (SDU) 三者关系见图2-8。

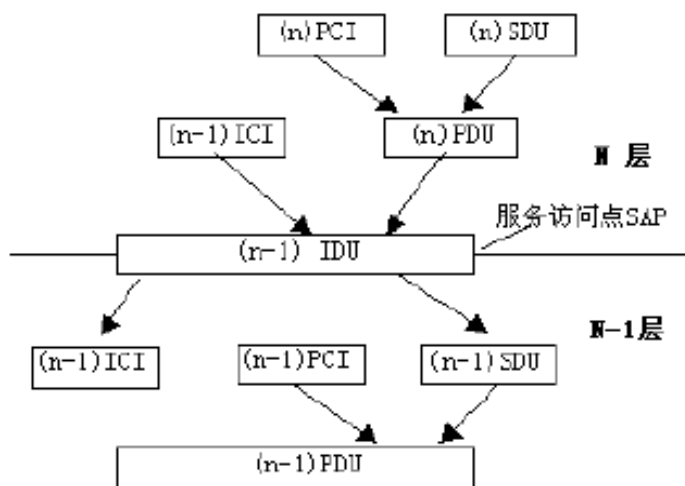


图2-8 PDU、IDU和SDU的关系

### 2.3.6 服务方式

OSI 参考模型中服务方式有二种：面向连接服务与无连接服务。

#### 1 面向连接服务

连接是两个对等实体为进行数据通信而进行的一种结合。面向连接服务是在数据交换之前，必须建立连接。数据交换结束后，则终止这个连接。因此，面向连接服务在网络层中又称为虚电路服务，虽然在两个服务用户的通信过程中并没有自始至终专用一条端到端的完整物理电路，但却好像一直占用了一条这样的电路。面向连接服务比较适合于在一定期间内要向同一目的地发送许多报文的情况。

面向连接服务具有连接建立、数据传输和连接释放这三个阶段。在传送数据时是按序传送的，是可靠的服务，可提供流量控制、差错控制和序列控制。

面向连接服务的特点：

- (1) 在连接建立时，需要给出双方地址，连接成功后，在数据传输时，仅仅使用连接符。
- (2) 报文能够按顺序发送，质量好，不会丢失。
- (3) 通信的两个实体必须同时是活跃的。

#### 2 无连接服务

在无连接服务的情况下，两个实体之间的通信不需要先建立好一个连接，传输数据过程中每个分组都必须携带完整的目标地址和源地址，各分组在系统中独立传送。无连接服务不能保证接收发送数据的顺序一致。无连接服务适合传送少量零星的数据。

无连接服务的特点是：

- (1) 灵活方便，但不能防止报文的丢失。
- (2) 每个报文都需要提供双方地址，网络传输的开销大。



- (3) 不需要通信的两个实体同时处于激活状态。发送端实体或者接收端实体在发送或者接收时，它才必须是活跃的。

## 2.4 其他著名体系结构简介

### 2.4.1 TCP/IP 体系结构

TCP 协议最早由斯坦福大学的两名研究人员于 1973 年提出。1983 年，TCP/IP 被 Unix 4.2BSD 系统采用。随着 Unix 的成功，TCP/IP 逐步成为 Unix 机器的标准网络协议。Internet 的前身 ARPANET 最初使用 NCP(Network Control Protocol)协议，由于 TCP/IP 协议具有跨平台特性，ARPANET 的实验人员在经过对 TCP/IP 的改进以后，规定连入 ARPANET 的计算机都必须采用 TCP/IP 协议。随着 ARPANET 逐渐发展成为 Internet，TCP/IP 协议就成为 Internet 的标准连接协议。到 90 年代 TCP/IP 已发展成为计算机之间最常应用的组网形式。

TCP/IP 是一组不同层次上的多个协议的组合。TCP/IP 通常被认为是一个四层协议系统，如图 2-9 所示。每一层负责不同的功能：

**1 链路层**，有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。

**2 网络层**，有时也称作互联网层，处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（网际协议），ICMP 协议

（Internet 互联网控制报文协议），以及 IGMP 协议

（Internet 组管理协议）。不同的物理网络技术有不同的

的编址方式。不同物理网络中的主机，有不同的物理网络地址。互联网技术是将不同物理网络技术统一起来的高层软件技术。互联网技术采用一种全局通用的地址格式，为全网的每一网络和每一主机都分配一个网间网地址，以此屏蔽物理网络地址的差异。IP 协议提供一种全互联网通用的地址格式，并在统一管理下进行地址分配，保证一个地址对应一台互联网主机，这样物理地址的差异被 IP 层所屏蔽。IP 提供的是无连接服务。

**3 运输层**，主要为两台主机上的应用程序提供端到端的通信。从通信和信息处理的角度看，运输层属于面向通信部分的最高层。但从网络功能或用户功能来划分，则运输层又属于用户功能中的最低层。运输层向高层用户屏蔽了下面通信子网的细节，使用户看不到实现通信功能的物理链路是什么，看不见数据链路采用的是什么协议。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（传输控制协议）和 UDP（用户数据报协议）。TCP 为两台主机提供高可靠性的数据通信。它所做的工作包括把应用程序交给它的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。TCP 协议提供的是面向连接服务，是在不可靠的网络服务上提供端到端的可靠字节流。UDP 则应用层提供一种非常简单的服务。它只是把称作数据报的分组从一台主机发送到另一台主机，但并不保证该数据报能到达另一端，任何必需的可靠性必须由应用层来提供。这两种运输层协议分别在不同的应用程序中有不同的用途。

**4 应用层**，负责处理特定的应用程序细节。应用层协议并不是解决用户各种具体运用的协议，而是规定应用进程在通信时所遵循的协议。TCP/IP 体系结构中常用的应用层协议有：

(1) 文件传送协议 FTP、TFTP

FTP 是 Internet 上使用最广泛的文件传送协议，它屏蔽了各计算机系统的字节，因而适合于异构网络中任意计算机之间传送文件，它支持许多不同文件类型和文件组织形式。FTP 是基于 TCP 协议。TFTP 是 FTP 功能的一个子集，简化了 FTP 实现的复杂性，TFTP 使用的是 UDP 数据报，因此

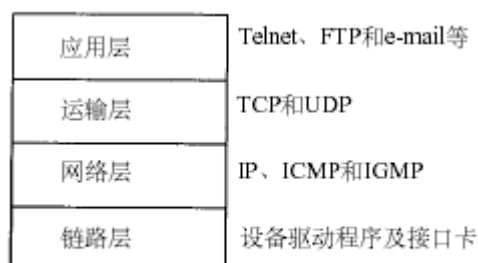


图1-1 TCP/IP协议族的四个层次



TFTP 要有自己的差错纠正措施。TFTP 只支持文件传输，而不支持交互，因此没有庞大的命令集。

(2) 简单邮件传输协议 SMTP

SMTP 就是在两个报文传送代理之间的通信协议。SMTP 规定了十四条命令和二十一种应答信息。SMTP 通信的三个主要阶段是连接建立、邮件传送、连接释放。

(3) 远程登录 TELNET

TELNET 是一个简单的终端协议。用户用 TELNET 就可以在其所在地通过 TCP 连接注册到远地的另一个主机上。TELNET 能把用户的击键传到远地主机，同时也能把远地主机的输出通过 TCP 连接返回到用户屏幕。这种服务是透明的，因为用户感觉到好像键盘和显示器是直接连在远地主机上。

(4) SNMP简单网络管理协议

SNMP 是简单网络管理协议，它是由 Internet 工程任务组织的研究小组为了解决 Internet 上的路由器管理问题而提出的，提供了一种从网络上的设备中收集网络管理信息的方法，也为设备向网络管理中心报告问题和错误提供了一种方法。具有远程管理能力的 SNMP 使管理人员可以对整个子网进行管理，而不是对整个子网内的设备进行管理。SNMP 是一个标准的用于管理 IP 网络上结点的协议。SNMP 协议提供了用于定义网络信息、框架和用于交换信息的协议标准。SNMP 模型引入了管理器和代理的概念，管理器指的是以人类管理员身份负责所有网络的软件。代理指的被管理设备中的软件，它用以完成管理器所需要进行的局部管理和应急通知管理的功能。

图2-10示意了 TCP/IP体系结构与OSI 参考模型之间的对应关系。

OSI		TCP/IP协议集
应用层	应用层	Telnet, FTP, SMTP, DNS, HTTP 以及其他应用协议
表示层		
会话层		
传输层	传输层	TCP, UDP
网络层	网络层	IP, ARP, RARP, ICMP
数据链路层	网络接口	各种通信网络接口（以太网等） （物理网络）
物理层		

图2-10 TCP/IP体系结构与OSI模型的对应

2.4.2 SNA 体系结构

SNA 是 IBM 公司于 1974 年公布的一个网络体系结构。IBM 用户利用它可将分布在各地的计算机系统和终端联成一个整体。从描述的内容来看，SNA 是指经过通信系统传输信息的逻辑结构、格式、协议和操作顺序的总称。相应地，对于服从 SNA 结构的设备就称为 SNA 设备。

SNA 早于 OSI 出现，它就不像 OSI 那样严格按照层次的关系来构成。SNA 注意于同一公司产品的互连，是一种集中控制的体系结构。图 2-11 示意了 IBM SNA 与 OSI 参考模型之间的对应关系。

1、SNA 路径控制层(NCP)：类似 OSI 网络层，提供分组装拆、路由选择、流量控制和拥塞处理等功能。

2、SNA 传输控制层：类似 OSI 运输层，并增加了 OSI 表示层的部分能力，在提供端到端数据

可靠和有序传输的同时，可以增加加密/解密的功能。

APPN(高级对等网络)：提供对等通信的能力，提供路由选择、目录服务和窗口流量控制的服务。

VTAM( 虚拟远程通信访问机制)：控制 SNA 网络中的通信和数据流量，提供单域、多域及互连的能力。

3、SNA 数据流控制层；类似 OSI 会话层，控制请求和应答的时序，确定数据的流向，并提供必要的的数据差错校正，保证数据传输的完整性。

4、网络可寻址部件服务(NAU)层：类似 OSI 表示层，执行数据的转换、以及数据的压缩，提高传输效率；同时还支持应用进程与网络地址的映射，保证应用进程的寻址能力，以及协调资源共享和同步操作等。

APPC（高级程序间通信）：允许结点之间的对等通信，支持定义的服务实现，提供系列通信平台，提供编程接口。

CICS（客户信息控制系统）：支持事务处理应用，提供终端到应用的通信。

5、SNA 事务服务层：包括为实现用户需求而开发的应用进程，以程序的方式提供用户使用。例如：SNADS（SNA 分布式服务）可向用户提供分布式处理服务。

OSI	SNA 体系结构		
应用层	事务服务层	DIA, SNADS, DDM, 用户应用	
表示层	网络可寻址部件 (NAU) 服务层	APPC, CICS, IMS, TSO, DB2	
会话层	数据流控制层 传输控制层	APPN, VTAM	
传输层			
网络层	路径控制层	NCP	
数据链路层	数据链路控制层	令牌环	SDLC X.25
物理层	物理控制层		V.24 RS-232

图 2-11 SNA 与 OSI 模型的对应

2.4.3 DNA 体系结构

DNA 是由数字设备公司（Digital Equipment Corporation）推出并支持的一组协议集合。目前市面上的 DNA 有多种版本。最初的 DNA 支持两台直接相连的小型机之间的通信。后来推出的版本在原 DNA 功能基础上另外提供了对附加所有者和标准协议的支持。当前使用较为广泛的两种 DNA 版本分别为：DNA IV 和 DNA V。DNA 是一种基于数字网络体系结构（DNA: Digital Network Architecture）的较为全面的分层网络体系结构，它支持大量的标准协议。DECnet 网络是 DNA 的一个具体实现。DECnet 在我国有一定的市场。DECnet 网络从 I 型到 V 型的发展过程：

I 型 DECnet 于 1974 产生：在 PDP-11 计算机上用，点到点通信，OS 为：RSX-11

II 型 DECnet 于 1976 产生，实现了对远程资源的管理和操作，可以在实时、分时和多任务操作系统上运行，但仍然是点到点通信。

III 型 DECnet 于 1980 产生，实现了多点通信、自适应选择路由、分布式的网络管理等功能，网络节点数增加到 255 个，并实现了与 X.25、SNA 的互连。

IV 型 DECnet 于 1982 产生，1984 年交付使用，可以与 LAN 相连，节点数达 6 万个，使用了 16 位的地址。由于 IV 型 DECnet 产生时，OSI 还没有完全制定出来，所以在层次划分上区别比较大。DNA 类似于 OSI 体系结构，同样采用了分层结构，只是它被分为八层。DECnet IV DNA 规定了上面四层提供用户交互服务、网络管理能力、文件传输和会话管理等功能。上面四层分别为：

用户层(user layer)、网络管理层(network management layer)、网络应用层(network application layer) 以及会话控制层 (session control layer)。IV 型 DECnet 的体系结构 DNA 共分 8 层，见图 2-12：

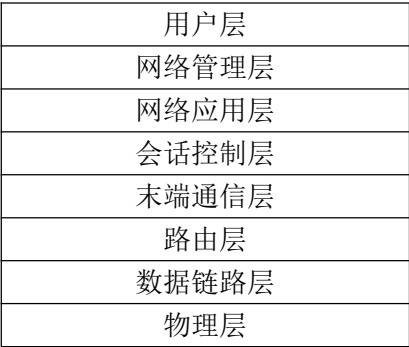


图 2-12 DNA 体系结构

V 型 DECnet 于 1987 产生，1991 年进入市场。DECnet V（可以表示为 DECnet Plus 或 DECnet/OSI）的分层模式可以实现三种协议组：OSI、DECnet 和 TCP/IP。DECnet plus 遵循七层 OSI 参考模型并支持众多的标准 OSI 协议，提供了与 DECnet IV 的反向兼容性。此外 DECnet plus 还支持应用层、表示层及会话层各功能，它支持低层 TCP/IP 协议，并能够实现在 TCP 传输协议上的 DECnet 流量传输。DECnet V 实现了下列目标：

- 1、地址长度为 20 字节，可支持非常大的网络，节点数可以超过 1 百万个。
- 2、在体系结构上要过渡到 ISO 标准。
- 3、定义了新的网络管理模型。
- 4、与 IV 型 DECnet 相容。

V 型 DECnet 的 DNA 体系结构如图 2-13。

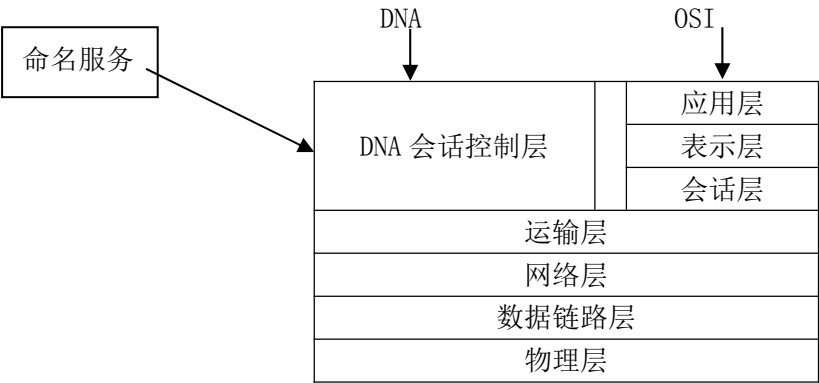


图 2-13 V 型 DECnet 的体系结构

2.4.4 Netware 体系结构

Netware 是 Novell 公司推出的局域网（Novell）操作系统，其产品曾经创下占据 60% 局域网市场份额的记录。Netware 主要面向 PC 机市场，以客户机/服务器（C/S）方式工作。作为一个独立的网络，Novell Netware 具有自己的网络体系结构。图 2-14 示意了 Netware 体系结构与 ISO OSI 参考模型之间的对应关系。

OSI		Netware 体系结构			
应用层	应用层	NETWARE 实 用 程 序			
表示层		SHELL	NFS	SAP	.....
会话层	会话层	NETBIOS			
传输层	运输	NETWARE STREAM			
网络层	协议层	SPX / IPX	MCP/IPX	TCP / IP	
数据链路层	链路支持层 (LSL)	开 放 式 数 据 链 路 接 口 (ODI)			
物理层		网 卡 驱 动 程 序 ( 以 太 网 , 令 牌 环 网 , ARCnet , FDDI . . . )			

图 2-14 Netware 体系结构与 OSI 模型的对应

#### 2.4.5 Windows NT 体系结构

Windows NT 是微软 (Microsoft) 公司开发的网络操作系统, 完全采用 Windows (视窗) 界面, 增加了“即插即用”的功能, 系统能够自动检测硬件配置, 具有用户使用方便和直观的特点, 被认为是新一代的网络操作系统。

Windows NT 网络可以支持各种网络适配卡, 不同的适配卡采用不同的网卡驱动程序。Windows NT 采用网络驱动程序接口规范 (NDIS) 来屏蔽不同的网卡, 并支持不同的高层协议 (如 TCP/IP、SPX/IPX, NetBEUI、Data Link Control-DCL 等)。图 2-15 示意了 Windows NT 的体系结构与 ISO OSI 参考模型之间的对应关系。

OSI		Windows NT 体系结构		
应用层	应用层	Windows NT 应用服务		
表示层		Windows NT 内核		
会话层				
传输层	传输层	NWLink SPX/IPX	TCP/IP	NetBEUI
网络层	网络层	网络驱动程序接口规范 (NDIS) 网卡驱动程序 (以太网, 令牌环网, FDDI ...)		
数据链路层	数据链路层			
物理层	物理层			

图 2-15 Windows NT 体系结构与 OSI 模型的对应

#### 2.4.6 MAP/TOP 体系结构

MAP/TOP 实质上包括两个协议集，分别用于制造自动化和办公自动化。约在 70 年代末期，美国波音公司着手研究用于办公自动化的网络开放系统体系结构。并作为研究成果，公布了基于 ISO OSI 基本参考模型的办公自动化局域网协议-技术和办公协议（TOP）。在 80 年代初期，美国通用汽车公司（GM）为了实现制造系统，开始着手制造自动化方面有关计算机通信的研究，并提出了制造自动化协议（MAP），同时成立 MAP 指导委员会，负责 MAP 的推广和应用。1984 年，通用汽车公司和波音公司双方达成协议，将波音公司开发的计算机网络体系扩充为 MAP 的办公室技术版本，于是，出现了 MAP 和 TOP 的结合，形成了一套即可支持生产、又可支持办公的完整的网络体系结构（称为 MAP/TOP 体系结构），并被广泛地应用于各种不同类型的企业，也被选为支持企业 CIMS 过程的计算机网络标准。

MAP 和 TOP 均遵从 OSI 参考模型，MAP/TOP 是 OSI 相关标准的实现。由于各自的侧重点不同，MAP 和 TOP 在支撑环节和应用服务方面略有不同。由于 OSI 模型的固有的不足（层次过多，影响效率），MAP 协议被分为三类：全 MAP 结构、最小 MAP 结构和增强形 MAP 结构。

全 MAP 结构（Full-MAP）包括 OSI 的七个层次，是 MAP 协议的全面实现。最小 MAP 结构（Mini-MAP）仅含 OSI 的三个层次（第一、二和七层），是 MAP 协议的一种简化实现，以强调实时性为网络设计的主要目的。增强型 MAP 结构（MAP/EPA）是互连 Full-MAP 和 Mini-MAP 的相关技术实现，它同时包含了 Full-MAP 和 Mini-MAP 结构的两种实现。

TOP 网络支持办公自动化应用，例如，人事、财务和市场决策等系统的运作。MAP 网络支持生产自动化应用，全 MAP 网络支持车间和部门之间的生产调度等，最小 MAP 网络支持生产与单元控制器之间的指令和响应的交换，增强型 MAP 结点实现全 MAP 网络和最小 MAP 网络之间的互连操作。

根据 MAP/TOP 有关的标准，MAP/TOP 网络主要由三种局域网技术所支持：CSMA/CD 总线、令牌总线和令牌环，并且前两种技术最为常用。由于 CSMA/CD 总线方式的应用十分普及，CSMA/CD 技术支持 MAP 的实例经常出现。使用时应当切记 CSMA/CD 方式的性能会由于负载的增加而降低。

## 第三章 物理层

物理层是网络体系结构中的最低层。它是网络体系结构上层各功能实现的基础，它向网络提供最基本的信号传输服务。物理层负责点到点的数据信号传输，为设备之间的数据通信提供传输媒体及互连设备，为数据传输提供可靠的环境。

### 3.1 物理层的概念

物理层需要解决的是怎样在连接各种计算机的传输媒体上传输数据的比特流。物理层设计时主要考虑的是如何在连接开放系统的传输介质上传输各种数据的比特流。由于计算机网络中可以利用的物理传输介质与传输设备存在着很大的差异，设计物理层的主要目的是向数据链路层屏蔽通信技术的差异性。数据链路层实体通过与物理层的接口，将数据传送给物理层，通过物理层按比特流的顺序，将信号传输到另一个数据链路层实体。物理层的协议通常称物理层规程。

#### 3.1.1 物理层的任务

物理层的任务就是为数据链路层提供一个物理连接，以便透明地传送比特流。物理连接可以通过中继系统，允许进行全双工或半双工的二进制比特流的传输。物理层的数据服务单元是比特，它可以通过同步或异步的方式进行传输。物理层就是将比特流送到物理媒体上传送。要设计用多大电压表示“1”，用多大电压为表示“0”。可以将物理层的主要任务定义为确定与传输媒体之间的接口特性，即：

1、**机械特性**：主要定义物理连接的即接插装置。规定物理连接时所采用的规格、引脚的数量和排列情况。常用的标准接口：1) ISO 2110, 25 芯连接器, EIA RS-232-C, EIA RS-366-A ;2) ISO 2593, 34 芯连接器, V. 35 宽带 MODEM;3) ISO 4902, 37 芯和 9 芯连接器, EIA RS-449;4) ISO 4903, 15 芯连接器, X. 20、X. 21、X. 22。

2、**电气特性**：规定传输二进制位时，线路上信号的电压高低、阻抗匹配、传输速率和距离限制等。说明在接口电线上电压范围，用什么样的电压表示 1 或 0。常用的 CCITT 标准化的电气特性标准：1) CCITT V. 10/X. 26：新的非平衡型电气特性, EIA RS-423-A; 2) CCITT V. 11/X. 27：新的平衡型电气特性, EIA RS-422-A; 3) CCITT V. 28：非平衡型电气特性, EIA RS-232-C; 4) CCITT X. 21/EIA RS-449。

3、**功能特性**：主要定义各条物理线路的功能。说明线路上出现的某电压表示何种意义。物理线路的功能分为四大类：数据功能、控制功能、定时功能、接地功能。

4、**规程特性**：主要定义各条物理线路的工作规程和时序关系，说明不同功能的各种可能事件的出现顺序。

物理层位于 OSI 参考模型的最低层，它直接面向实际承担数据传输的物理媒体(即信道)。物理层的传输单位为比特。物理层是指在物理媒体之上为数据链路层提供一个原始比特流的物理连接。物理层协议规定了与建立、维持、断开物理信道所需的机械的、电气的、功能性的和规程性的特性。其作用是确保比特流能在物理信道上传输。



图 3-1 DTE-DCE 接口框图

---

OSI 参考模型的物理层的定义：在物理信道实体之间合理地通过中间系统，为比特传输所需的物理连接的激活、保持和去除提供机械的、电气的、功能性和规程性的手段。比特流传输可以采用异步传输，也可以采用同步传输完成。另外，CCITT 在 X.25 建议书第一级（物理级）中也做了类似的定义：利用物理的、电气的、功能的和规程的特性在 DTE 和 DCE 之间实现对物理信道的建立、保持和拆除功能。这里的 DTE (Data Terminal Equipment) 指的是数据终端设备，是对属于用户所有的连网设备或工作站的统称，它们是通信的源接点或目的接点，如计算机、终端等；DCE (Data Circuit Terminating Equipment 或 Data Communications Equipment)，指的是数据电路终接设备或数据通信设备，是为用户提供接入接点的网络设备的统称，如自动呼叫应答设备、调制解调器等。

DTE-DCE 的接口如图 3-1 所示，物理层接口协议实际上是 DTE 和 DCE 或其它通信设备之间的一组约定，主要解决网络节点与物理信道如何连接的问题。物理层协议规定了标准接口的机械连接特性、电气信号特性、信号功能特性以及交换电路的规程特性，这样做的主要目的，是为了便于不同的制造厂家能够根据公认的标准各自独立地制造设备。使各个厂家的产品都能够相互兼容。

### 3.1.2 物理层提供的服务

物理层是 OSI 参考模型的最低层，它向数据链路层提供的主要服务就是网络的物理连接、物理服务数据单元传输、发送与接收双方比特顺序保持一致。物理层所提供的服务如下：

#### 1 物理连接

数据电路是一条通信路径。该路径是由两个物理实体之间的物理介质和用于传输比特流必需的设施以及物理层中的中继设备、互连数据电路而构成。

物理连接分为两类：

- (1) 点到点连接：它连接两个数据链路实体；
- (2) 多点连接：一个数据链路实体与多个数据链路实体连接。

当物理层一旦完成数据链路互连后，其中间的物理实体在物理层以上是不可见的，数据链路层所能感知的只是两个物理连接端点(点到点连接)，或多个物理连接端点(多点连接)，物理连接可以是永久性连接(专线)，也可以是动态连接(交换网)。

#### 2 物理服务数据单元

物理层提供两类物理服务数据单元：

- (1) 串行传输方式物理服务数据单元 1 个比特；
- (2) 并行传输方式物理服务数据单元，它由若干个比特组成。

#### 3 顺序化

物理层接收物理实体收到的比特顺序，与发送物理实体所发送的比特顺序相同。

另外，物理层提供唯一能标识两相邻系统之间数据电路的标识符。当物理层中传输出现差错时，应向数据链路层实体报告物理层中所检测到的故障和差错。物理连接服务的质量大部分由数据电路本身确定，其质量指标含误码率、服务可用性数据传输速率和传输时延。

### 3.1.3 物理层提供的功能

为了实现数据链路层实体之间比特流的透明传输，物理层应具有下述功能：

#### 1 物理连接的建立与拆除

为数据端设备提供传送数据的通路，数据通路可以是一个物理媒体，也可以是多个物理媒体连接而成。一次完整的数据传输，包括激活物理连接、传送数据、终止物理连接过程。当数据链路层请求在两个数据链路层实体之间建立物理连接时，物理层立即为它们建立相应的物理连接。若两个数据链路层实体之间要经过若干中继数据链路层实体时，物理层应对这些中继数据链路层实体进行互连，



以建立起一条所需的物理连接。当物理连接不再需要时，由物理层立即拆除。

## 2 传输数据

物理层要形成适合数据传输需要的数据单元，为数据传送服务。一是要保证数据能在其上正确通过，二是要提供足够的带宽(带宽是指每秒钟内能通过的比特(BIT)数)，以减少信道上的拥塞。传输数据的方式能满足点到点、一点到多点、串行或并行、半双工或全双工、同步或异步传输的需要。

## 3 物理层管理

物理层要涉及到本层的某些管理事务，如功能的激活(何时发送和接收、异常情况处理等)、差错控制(传输中出现的奇偶错和格式错等)。

# 3.2 物理层协议举例

## 3.2.1 EIA RS-232C 接口标准

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

RS-232 标准提供了一个利用公用电话网络作为传输媒体，并通过调制解调器将远程设备连接起来的技术规定。远程电话网相连接时，通过调制解调器将数字转换成相应的模拟信号，以使其能与电话网相容；在通信线路的另一端，另一个调制解调器将模拟信号逆转换成相应的数字数据，从而实现比特流的传输。图 3-2 (a)给出了两台远程计算机通过电话网相连的结构图。从图中可看出，DTE 实际上是数据的信源或信宿，而 DCE 则完成数据由信源到信宿的传输任务。RS-232C 标准接口只控制 DTE 与 DCE 之间的通信，与连接在两个 DCE 之间的电话网没有直接的关系。

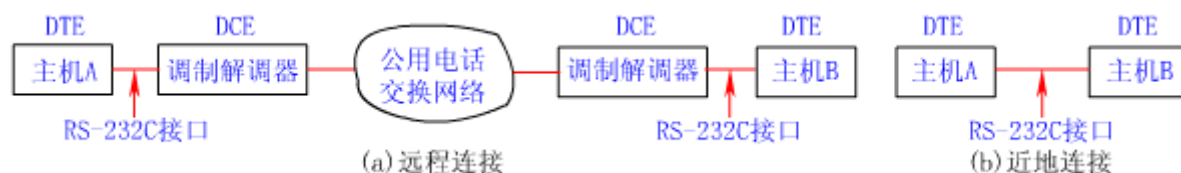


图 3-2 RS-232C 的远程连接和近地连接

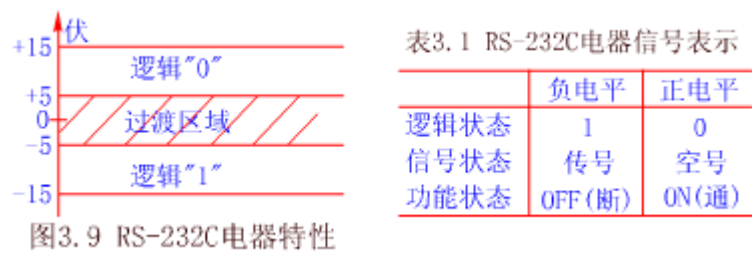
RS-232C 标准接口也可以如图 3-2 (b) 所示用于直接连接两台近地设备，此时既不使用电话网也不使用调制解调器。由于这两种设备必须分别以 DTE 和 DCE 方式成对出现才符合 RS-232C 标准接口的要求，所以在这种情况下要借助于一种采用交叉跳接信号线方法的连接电缆，使得连接在电缆两端的 DTE 通过电缆看对方都好像是 DCE 一样，从而满足 RS-232C 接口需要 DTE-DCE 成对使用的要求。这根连接电缆也称作零调制解调器(Null Modem)。

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

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

RS-232C 电平高达+15 伏和-15 伏，较之 0~5 伏的电平来说具有更强的抗干扰能力。但是，即使用这样的电平，若两设备利用 RS-232C 接口直接相连(即不使用调制解调器)，它们的最大距离

也仅约 15m，而且由于电平较高、通信速率反而能受影响。RS-232C 接口的通信速率<20KBPS (标准速率有 150、300、600、1200、2400、4800、9600、19200BPS 等)。



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

表 3-2 RS-232C 功能特性				
引脚号	信号线	功能说明	信号线型	连接方向
1	AA	保护地线 (GND)	地线	
2	BA	发送数据 (TD)	数据线	→DCE
3	BB	接收数据 (RD)	数据线	→DTE
4	CA	请求发送 (RTS)	控制线	→DCE
5	CB	清除发送 (CTS)	控制线	→DTE
6	BB	数据设备就绪 (DSR)	控制线	→DTE
7	AB	信号地线 (Sig. GND)	地线	
8	CF	载波检测 (CD)	控制线	→DTE
20	CD	数据终端就绪 (DTR)	控制线	→DCE
22	CE	振铃指示 (RI)	控制线	→DTE

RS-232C 的连接见图 3-4。

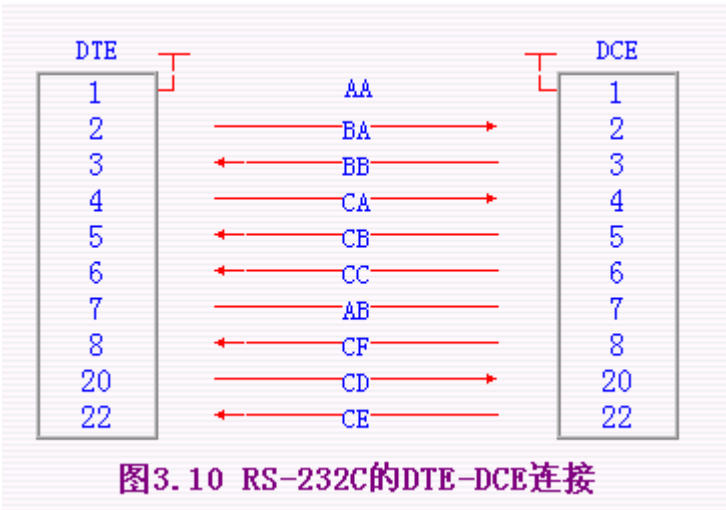


图 3-4 RS-232C 的 DTE-DCE 连接

若两台 DTE 设备，如两台计算机在近距离直接连接，则可采用图 3-4 的方法，图中 (a) 为完整型连接，(b) 为简单型连接。

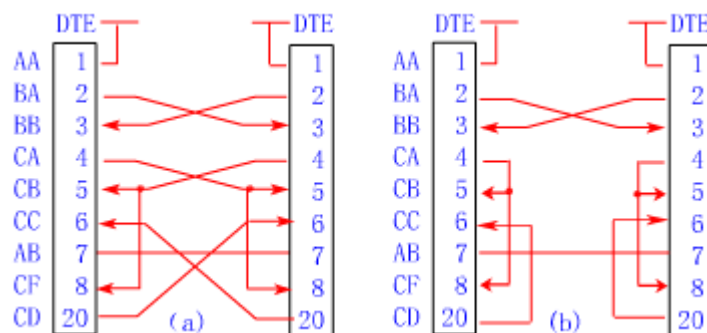


图 3-5 RS-232C 的 DTE-DTE 连接

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

### 3.2.2 EIA RS-449 及 RS-422 与 RS-423 接口标准

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

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

RS-449 标准的电器特性有两个标准，即平衡式的 RS-422 标准和非平衡式的 RS-423 标准。

RS-422 电气标准是平衡方式标准，它的发送器、接收器分别采用平衡发送器和差动接收器，由于采用完全独立的双线平衡传输，抗干扰能力大大增强。又由于信号电平定义为  $\pm 6\text{V}$ （ $\pm 2\text{V}$  为过度区域）的负逻辑，故当传输距离为  $10\text{M}$  时，速率可达  $10\text{MBPS}$ ；而距离增长至  $1000\text{m}$  时，速率可达到  $100\text{KBPS}$  时，性能远远优于 RS-232C 标准。

RS-423 电气标准是非平衡标准，它采用单端发送器（即非平衡发送器）和差动接收器。虽然发送器与 RS-232C 标准相同，但由于接收器采用差动方式，所以传输距离和速度仍比 RS-232C 有较大的提高。当传输距离为  $10\text{M}$  时，速度可达成  $100\text{KBPS}$ ；距离增至  $100\text{M}$  时，速度仍有  $10\text{KBPS}$ 。RS-423 的信号最平定义为  $\pm 6\text{V}$ （其中  $\pm 4\text{V}$  为过渡区域）的负逻辑。

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

### 3.2.3 100 系列和 200 系列接口标准

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

CCITT V. 24 建议中有关 DTE-DCE 之间的接口标准有 100 系列、200 系列两种。100 系列接口标准作为 DTE 与不带自动呼叫设备的 DCE（如调制解调器）之间的接口。在调置自动呼叫设备的 DCE（如网络控制器）中，则由 200 系列接口标准完成 DTE 与自动呼叫设备的接口。若系统采用人工呼叫，则无需设置 200 系列接口。

100 系列接口标准的机械特性采用两种规定，当传输速率为  $200\text{BPS} \sim 9600\text{BPS}$  时，采用 25 芯标准连接器；传输速率达  $48\text{KBPS}$  时，采用 34 芯标准连接器。200 系列接口标准则采用 25 芯标

---

准连接器。

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

### 3.2.4 X. 21 和 X. 21bis 建议

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

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

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

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

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

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

X. 21 和 X. 21 bis 为三种类型的服务定义了物理电路, 这三种电路是租用电路(专用线)服务、直接呼叫服务和设备地址呼叫服务。租用电路设计成在两个终端之间的连续连接; 直接呼叫服务像“热线”电话, 可使用户在任何时间直接连接指定的目标; 设备地址呼叫则如“拨号”电话, 每次联接需由用户呼叫指定目标。

## 3.3 传输介质特性

物理层的目的是将原始的比特流从一台机器传输到另一台机器。有多种物理介质可用于实际传输, 每一种物理介质在带宽、延迟、成本和安装维护难度上都不相同。当需要决定使用哪一种传输介质时, 必须将连网需求与介质特性进行匹配。通常说来, 选择数据传输介质时必须考虑 5 种特性: 吞吐量和带宽、成本、尺寸和可扩展性、连接器、抗噪性。当然, 每种连网情况都是不同的, 对一个单位至关重要的特性对另一个单位来说可能是无关重要的, 需要判断哪一方面对单位是最重要的。

### 3.3.1 吞吐量和带宽

在选择一个传输介质时所要考虑的最重要的因素可能是吞吐量。吞吐量是在一给定时间段内介质能传输的数据量，它通常用每秒兆位或 Mbps 进行表示。吞吐量也被称为容量，每种传输介质的物理性质决定了它的潜在吞吐量。例如，物理规律限制了电沿着铜线传输的速度，如果试图将超过它处理能力的数据量沿着一根铜线传输，结果将是数据丢失或出错。与传输介质相关的噪声和设备能进一步限制吞吐量，充满噪声的电路将花费更多的时间补偿噪声，因而只有更少的资源可用于传输数据。

带宽这个术语常常与吞吐量交换使用。严格地说，带宽是对一个介质能传输的最高频率和最低频率之间的差异进行度量；频率通常用 Hz 表示，它的范围直接与吞吐量相关。例如，若 FCC 通知你能够在 870 - 880 MHz 之间传输无线信号，那么分配给你的带宽将是 10MHz。带宽越高，吞吐量就越高，如图 3-6 所示。图 3-6 中的情形是由于在一给定的时间段内，较高的频率能比较低频率传输更多的数据。

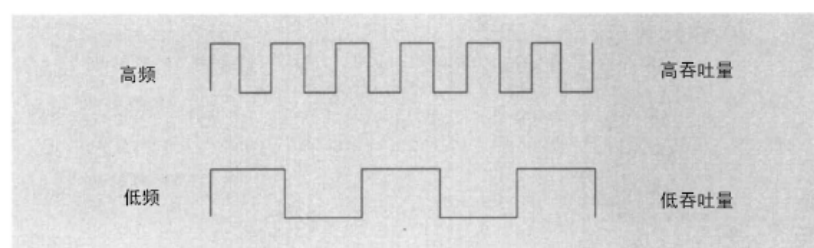


图 3-6 两个数字频率的比较

### 3.3.2 成本

不同种类的传输介质牵涉的成本是难以准确描述的。它们不仅与环境中现存的硬件有关，而且还与你所处的场所有关。下面的变量都可能影响采用某种类型介质的最后成本。

1 安装成本：你能自己安装介质吗？或你必须雇佣承包商做这件事吗？你是否需要折墙或修建新的管道或机柜？你是否需要从一个服务提供商处租借线路。

2 新的基础结构相对于复用已有基础结构的成本：你是否能使用已有的电线？在某些情况下安装所有新的 5 类 UTP；如果你能使用已有的 5 类 UTP，电线将可以不用付费。假如仅仅替换基础结构的一部分，它是否能轻易地与已有介质集成。

3 维护和支持成本：假如复用已有介质基础结构常常需要修理或改进，复用并不省任何钱。同时，假如使用了一种不熟悉的介质类型，可能需要花费更多却雇佣一个工程师维护它。你是否能自己维护介质，或你是否必须雇佣承包商维护它？

4 因低传输速率而影响生产效率所付出的代价：如果你通过复用已有的低速的线路来省钱，你是否可能因为降低了生产率而遭受损失？换言之，你是否使你的员工在进行保存和打印报告或发送邮件时等待更长的时间？

5 更换过时介质的成本：你是否选择了要被逐渐淘汰或需迅速替换的介质？你是否能发现某种价格合理的连接硬件与你几年前选择的介质相兼容？

### 3.3.3 尺寸和可扩展性

三种规格决定了网络传输介质的尺寸和可扩展性：每段的最大节点数、最大段长度、以及最大网络长度。在进行布线时，这些规格中的每一个都是基于介质的物理特性的。每段最大节点数与衰减有关，即通过一给定距离信号损失的量有关。对一个网络段每增加一个设备都将略微增加信号的衰减。为了保证一个清晰的强信号，必须限制一个网络段中的节点数。

---

网络段的长度也应因衰减受到限制。在传输一定的距离之后，一个信号可能因损失得太多以至于无法被正确解释。在这种损失发生之前，网络上的中继器必须重发和放大信号。一个信号能够传输并仍能被正确解释的最大距离即为最大段长度。若超过这个长度，更易于发生数据损失。类似于每段最大节点数，最大段长度也因不同介质类型而不同。

在一种理想的环境中，网络可以在发送方和接收方之间实时传输数据，不论两者之间相隔多远。不幸的是我们没有生活在一个理想的环境中。一个信号从它的发送到它的最后接收之间存在一个延迟。每个网络都受这个延迟的支配。例如，当你在计算机上敲一个键将一个文件保存到网络上时，文件的数据在它到达服务器的硬盘时必须通过网络接口卡、网络中的一个集线器或也可能是一个交换机或路由器、更多的电缆以及服务器的网络接口卡。虽然电子传输迅速，它们仍然不得经过传输这一过程。这个过程在你敲键的那一刻和服务器接收数据的那一刻之间必然存在一个短暂的延迟，这种延迟被称时延。

如同存在一个连通设备，如一路由器，接入设备的转换时间将影响时延，所使用的电缆的长度也将影响时延。但是，仅仅当一个接收节点正期望接收某种类型的数据时，如它已开始接收的数据流的剩余部分，时延的影响将可能成为问题。假如该接收节点未能接收数据流的剩余部分，它将认为没有更多的数据输入，这将导致网络上的传输错误。同时，当连接多个网络段时，也将增加网络上的时延。为了限制时延并避免相关的错误，每种类型的介质都标定一个最大连接段数。

### 3.3.4 连接器

连接器是连接电缆与网络设备的硬件。网络设备可以是一个文件服务器、工作站、交换机或打印机。每种网络介质都对应一种特定类型的连接器。所使用的连接器的种类将影响网络安装和维护的成本、网络增加段和节点的容易度，以及维护网络所需的专业技术知识，用于 UTP 电缆的连接器（HUB）在接入和替换时比用于同轴电缆的连接器的插入和替换要简单得多，UTP 电缆连接器同时也更廉价并可用于许多不同的介质设计。

### 3.3.5 抗噪性

噪声能使数据信号变形，噪声影响一个信号的程度与传输介质有一定关系。某些类型的介质比其他介质更易于受噪声影响。无论是何种介质，都有两种类型的噪声会影响它们的数据传输：电磁干扰（EMI）和射频干扰（RFI）。EMI 和 RFI 都是从电子设备或传输介质发出的波。发动机、电源、电视机、复制机、荧光灯以及其他的电源都能产生 EMI 和 RFI。RFI 也可由来自广播电台或电视塔的强大广播信号产生。对任何一种噪声，你都能够采取措施限制它对网络的干扰。例如，可以远离强大的电磁源进行布线。如果环境仍然使网络易受影响，应选择一种能限制影响信号的噪声量的传输。

电缆可以通过屏蔽、加厚、或抗噪声算法获得抗噪性。假如屏蔽的介质仍然不能避免干扰，你可以使用金属管道或管线以抑制噪声并进一步保护电缆。

## 3.4 有线传输介质

在组建计算机网络过程中，需要传输介质来进行数据传递。常用的网络传输介质可分为两类：一类是有线传输介质；一类是无线传输介质。有线传输介质主要有同轴电缆、双绞线和光纤；无线传输介质主要有无线电波和红外线。

### 3.4.1 双绞线



在目前的计算机网络中，双绞线是应用最为广泛的传输介质。不管广域网，还是局域网，都离不开双绞线。

### 1、物理特性

双绞线是现在最普通的传输介质，它由两条相互绝缘的铜线组成，典型直径为 1 毫米。把两根绝缘的铜导线按一定密度互相绞在一起，可降低信号干扰的程度，每一根导线在传输中辐射的电波会被另一根线上发出的电波抵消。双绞线中每根铜导线的绝缘层上分别涂有不同的颜色，以示区别。把一对或多对双绞线放在一个绝缘套管中便成了双绞线电缆，不同线对具有不同的扭绞长度。与其他传输介质相比，双绞线在传输距离、信道宽度和数据传输速度等方面均受到一定限制，但价格较为低廉。双绞线接头为具有国际标准的 RJ-45 插头和插座。

局域网中所使用的双绞线分为两类：

- 1) 屏蔽双绞线(STP)
- 2) 非屏蔽双绞线(UTP)

屏蔽双绞线由外部保护层、屏蔽层与多对双绞线组成。非屏蔽双绞线由外部保护层与多对双绞线组成。屏蔽双绞线与非屏蔽双绞线的结构如图 3-7 所示。

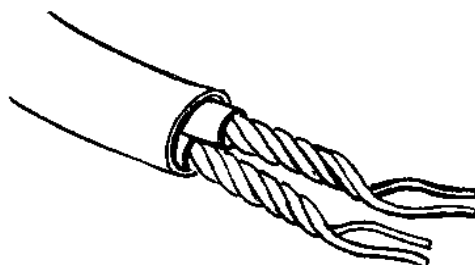


图 3-7 双绞线结构图

### 2、传输特性

双绞线主要是用来传输模拟声音信息的，但同样适用于数字信号的传输，特别适用于较短距离的信息传输。在传输期间，信号的衰减比较大，并且产生波形畸变。采用双绞线的局域网的带宽取决于所用导线的质量、长度及传输技术。只要精心选择和安装双绞线，就可以在有限距离内达到每秒几百万位的可靠传输率。当距离很短，并且采用特殊的电子传输技术时，传输率可达 100~155Mbps。网络中常用的双绞线根据传输特性可以分为 5 类。在典型的以太网中，常用第三类、第四类与第五类非屏蔽双绞线，通常简称为三类线、四类线与五类线。其中，三类线带宽为 10MB，适用于语音及 10MBPS 以下的数据传输；五类线带宽为 100MB，适用于语音及 100MBPS 的高速数据传输，甚至可以支持 155MBPS 的 ATM 数据传输。

常用的双绞线根据传输特性可以分为五类：

- 1 类：主要用于传输语音，不用于数据传输。
- 2 类：传输频率为 1MHz，用于语音传输和最高传输速率 4MBPS 的数据传输。
- 3 类：传输频率为 16MHz，用于语音传输及最高传输速率为 10MBPS 的数据传输。
- 4 类：传输频率为 20MHz，用于语音传输和最高传输速率 16MBPS 的数据传输。
- 5 类：该双绞线增加了绕线密度，外套一种高质量的绝缘材料，传输频率为 100MHz，用于语音传输和最高传输速率为 100MBPS 的数据传输。

为了适应网络速度的不断提高，出现了超 5 类和 6 类双绞线。局域网最常使用是 5 类非屏蔽的双绞线。

### 3、连通性

双绞线既可用于点到点连接，也可用于多点连接。

### 4、地理范围



双绞线用做远程中继线时，最大距离可达 15 公里；用于局域网时，与集线器(或者交换机)的距离最大为 100 米。

#### 5、抗干扰性

双绞线的抗干扰性取决于一束线中相邻线对的扭曲长度及适当的屏蔽。

#### 6、价格

双绞线的价格低于其它传输介质，并且安装、维护方便。

### 3.4.2 同轴电缆

同轴电缆是网络中常用的传输介质之一。

#### 1、物理特性

同轴电缆以硬铜线为芯，外包一层绝缘材料。这层绝缘材料用密织的网状导体环绕，网外又覆盖一层保护性材料。内、外导体同轴心。同轴电缆的结构如图 3-8 所示。同轴介质的特性参数由内、外导体及绝缘层的电参数与机械尺寸决定。目前，有两种广泛使用的同轴电缆。一种是 50 欧姆电缆，只适用于传输数字信号，由于多用于基带传输，也叫基带同轴电缆。另一种是 75 欧姆电缆，用于传输频分多路(FDM)方式产生的模拟信号(宽带信号)，又称宽带同轴电缆。同轴电缆直径约为 1.02-2.54cm，可在较宽频范围工作。

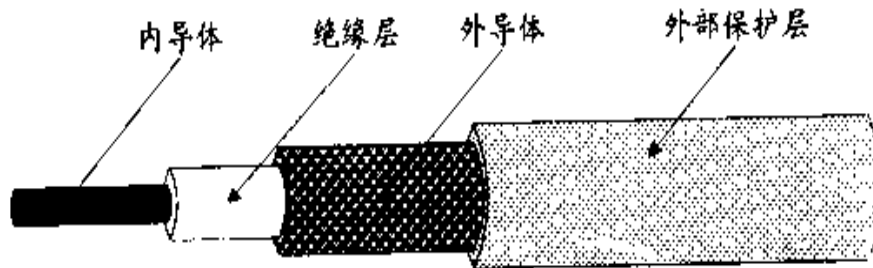


图 3-8 同轴电缆的结构图

#### 2、传输特性

基带同轴电缆仅用于数字传输，阻抗为  $50\Omega$ ，并使用曼彻斯特编码，数据传输速率最高可达 10Mbps。宽带同轴电缆可用于模拟信号和数字信号传输，阻抗为  $75\Omega$ ，使用 MODEM，通过频分多路技术的调制调器方式传输模拟信号，对于模拟信号，带宽可达 300-450MHz。在 CATV 用的  $75\Omega$  电缆上，每个电视通道分配 6MHz 带宽，而广播通道的带宽要窄得多，因此，在同轴电缆上使用频分多路复用技术可以支持大量的视音频通道。同轴电缆具有良好的电气性能，非常适合于传输高频信号。同轴电缆的电磁辐射较小、信号损耗低、抗外界电磁干扰强。

#### 3、连通性

同轴电缆可用于点到点及多点的链路结构。每段  $50\Omega$  基带同轴电缆可支持上百台设备工作，而且还可以通过中继器将各段链接在一起。 $75\Omega$  宽带同轴电缆理论上可以支持上千台设备工作。

#### 4、地理范围

$50\Omega$  同轴电缆传输的最远距离只有几公里； $75\Omega$  同轴电缆传输距离可达数十公里。

#### 5、抗干扰性

同轴电缆的抗干扰能力比双绞线强。同轴电缆的抗噪声性取决于具体的应用环境。在低频段，它的抗噪声性能与双绞线相近，甚至还略差一些；而在高频段时，却优于双绞线。为了使信号能远距离传送，需将待传输信号调制到较高的频率载波后再在同轴电缆上传输。

#### 6、价格

使用同轴电缆组建局域网的费用略微高于双绞线、低于光缆组建局域网的费用。

### 3.4.3 光纤电缆

光纤即光导纤维，是一种细小、柔韧并能传输光信号的介质，一根光缆中包含有多条光纤。20 世纪 80 年代中期，光缆开始进入计算机网络。因为光纤不会向外界辐射电子信号，所以使用光纤介质的网络无论是在安全性、可靠性，还是网络性能方面都有了很大的提高。对于快速网络，光纤是最好的选择。。

### 1、物理特性

光纤是由许多细如发丝的塑胶或玻璃纤维外加绝缘护套组成，如图 3-9 所示。利用光纤连接网络，每端必须连接光/电转换器，另外还需要一些其它辅助设备。光纤电缆是由两层折射率不同的材料所构成，是一种能通过光线的细小而柔韧的传输介质。其内层是具有较高折射率的玻璃或塑料单根纤维线，外层是折射率较低的材料。在多模光纤中，光纤芯的直径是 15-50 $\mu\text{m}$ ，大致与人的头发粗细相当。在单模光纤中，光纤芯的直径为 8-10 $\mu\text{m}$ 。光纤芯通常是由石英玻璃制成的横截面积很小的双层同心圆柱体，它质地脆，易断裂，需要外加一保护层。

### 2、传输特性

光纤电缆是利用全反射的原理来传输被调制好的光信号。只要外部物质的光折射率低于传输光纤的折射率，则产生内部全反射。带有信息编码的光束在光纤电缆中不断地全反射，最终将信息从发出端传输到接受端。

光纤通信过程中，由光发送机产生光束，将表示数字代码的电信号转变成光信号，并将光信号导入光纤，光信号在光纤中传播，在另一端由光接收机负责接收光纤上传出的光信号，并进一步将其还原成为发送前的电信号。实际应用中，光缆的两端都应安装有光纤收发器，光纤收发器集成了光发送机和光接收机的功能，既负责光的发送也负责光的接收。

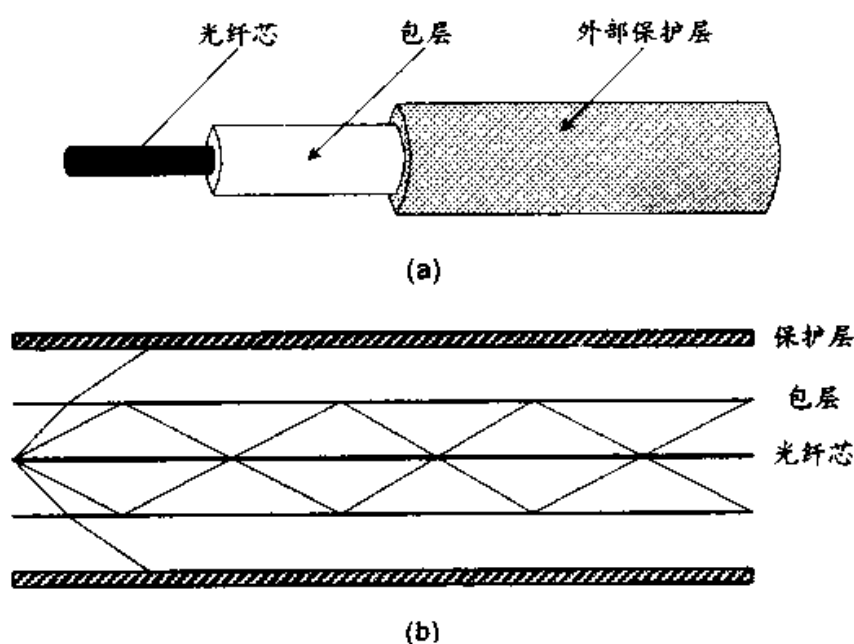


图 2-9 光缆结构与传输方式

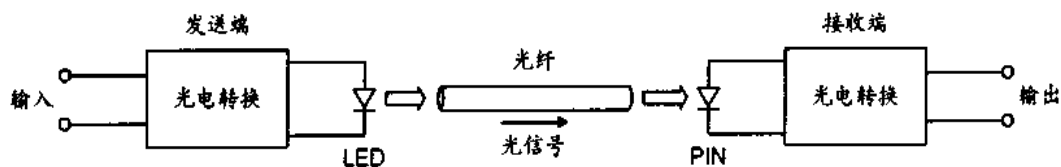


图 2-10 光缆传输系统结构示意图

光纤分为单模光纤和多模光纤两种(“模”是指以一定角度进入光纤的一束光)。包层较纤芯有较低的折射率。当光线从高折射率的媒体射向低折射率的媒体时，其折射角将大于入射角。因此，如果入射角足够大，就会出现全反射。只要射到光纤表面的光线的入射角大于一个临界角度，就可以产生全反射。因此，可以存在许多条不同角度入射的光线在一条光纤中传输。这种光纤就称为多模光纤。但是，若光纤的直径减小到只有一个光的波长，则光纤就像根波导那样，它可使光线一直向前传播，称为单模光纤。单模光纤采用激光二极管作为光源，而多模光纤采用发光二极管为光源。多模光纤的芯线粗，传输速率低、距离短，整体的传输性能差，但成本低，一般用于建筑物内或地理位置相邻的环境中。单模光纤的纤芯相应较细，传输频带宽、容量大、传输距离长，但需激光源，成本较高，通常在建筑物之间或地域分散的环境中使用。

### 3、链接方法

光纤电缆主要运应用于点到点的链路。

### 4、距离范围

光纤电缆可以在 6~10KM 距离内不使用中继器就能进行有关信息的传输。因而，光纤电缆较适合于在几个建筑物之间通过点到点链路实现局域网。

### 5、抗干扰性

光纤电缆不受电磁波的干扰或噪声的影响，适宜在长距离内保持高数据传输率，而且能够提供良好的安全性、保密性，损耗及误码率都较低。

### 6、相对价格

按光纤电缆及其所需设备如：发光器、接收器、连接器、中继器等计算，光纤局域网比双绞线及同轴电缆局域网的费用要高得多。

#### 3.4.4 几种传输介质的性能及其比较

通过以上对双绞线、同轴电缆及光纤电缆为传输介质所组成网络的个分析，可以得出以下特性比较。几种常用传输介质性能比较见表 3-3：

表 3-3：常用传输介质性能比较

项目 \ 类型	双绞线	基带	宽带	光缆
传输信息	数字或模拟	数字	数字或模拟	模拟
最大带宽	100~1MHZ	10M~50MHZ	300M~400MHZ	不受限制
互连复杂性	简单	较简单	较复杂	复杂
可使用部件	广泛	受限制	广泛	很受限制
介质价格	低	较低	较高	高
多站适用性	较好	好	很好	差
端点个数	10	10~100	100	2
信号噪声比	低	中	中	高
最大距离	100M	数公里	数十公里	6~10 公里
传输速率	1~2MBPS	10MBPS	50MBPS	10MBPS
技术状态	成熟	较成熟	较成熟	成熟

## 3.5 无线传输介质

无线传输介质并不利用导体。确切地说，信号完全通过空间从发射器发射到接收器。无线传输介质有时被称为无线电波系统。由于发射器和接收器之间有空气、干扰，无线传输会产生信号减弱及失真。目前最常用的无线信道有微波、红外线和激光信道。

### 3.5.1 微波信道和卫星信道

#### 1、微波信道

所谓微波是指频率大过于 1GHz 的电波。目前所用微波的频率范围为 1—20GHz。如果应用较小的发射功率（约 1 瓦）配合定向高增益微波天线，再于每隔 16 公里~80 公里的距离设置一个中继站就可以架构起微波通信系统。微波传播主要采用自由空间传播，也就是在收发二地之间没有任何阻隔，也没有任何其它的影响（包括反射、折射、绕射、散射或吸收）下传播，这种环境在现实生活中很少会出现。自由空间传播是假设微波传输的两点之间没有物体阻挡，而且除了两点间直线上不能有阻碍物体外，直线附近的某一个范围内也必须避免物体存在才行，因为微波天线虽具有良好的方向性，但它所发射的信号路径不是一条单纯的直线，它所发射的波面是会逐渐扩大的，若这些散逸的电波遇到物体阻挡，就会变成经由反射路径达到接发点，反射路径与直线路径因为长度不等，所以到达接收点的相位自然有差，这就是“干扰”的形成，这种干扰偶尔会对传播有利，但通常它都是有害的，所以电波传播路径的直线周围必须预留相当大的空间。

微波是计算机网络中最早使用的无线信道类型。美国的 ARPA 网络中用于连接美国本土和夏威夷的信道即是微波信道。它既可传输模拟信号，又可传输数字信号。由于微波能穿透电离层而不反射到地面，故只能使微波沿地球表面由源向目标直接发射。又因微波被地表吸收致使其传输损耗很大，故每隔几十公里便需进行中继（图 3-11）。微波对环境干扰虽然不敏感，但却易于受障碍物的影响，故微波的收发器必须安装在建筑物的外面。虽然微波具有很强的方向性，但仍存在保密和安全性问题。

因此，微波信道主要特点是：

- 1) 微波波段频率很高，其频段范围也很宽，因此其通信信道的容量很大；
- 2) 因为工业干扰和天电干扰的主要频谱成分比微波频率低得多，对微波通信的危害比对短波通信小得多，因而微波传输质量较高；
- 3) 与相同容量和长度的电缆载波通信比较，微波接力通信建设投资少，见效快。
- 4) 相邻站之间必须直视，不能有障碍物，有时一个天线发射出的信号也会分成几条略有差别的路径到达接收天线，因而造成失真；
- 5) 微波的传播有时也会受到恶劣气候的影响；
- 6) 与电缆通信系统比较，微波通信的隐蔽性和保密性较差；
- 7) 对大量中继站的使用和维护要耗费一定的人力和物力。

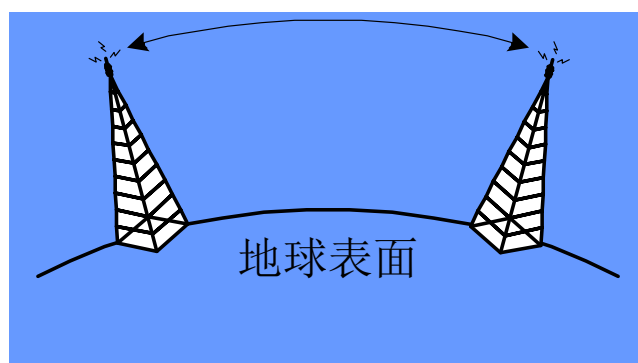


图 3-11 微波信道传输

## 2、卫星信道

卫星其实就是非地面微波，有时与地面系统工作在同一频率范围内。最常见的卫星系统就是同步地球轨道卫星，始终处在赤道正上方的位置上，高度大约为 22300 英里。在这样的位置及高度，卫星与地球表面总是保持相对位置。为了增加微波的传输距离，应提高微波收发器或中继站的高度。当将微波中继站放在人造卫星上时，便形成了卫星通信系统，可见，卫星通信是一种特殊的微波中继系统。用卫星上的中继站接收从地面发来的信号后，加以放大整形后再发回地面（图 3-12）。卫星通信可能是推动社会各个领域发生变化的介质。为有助于把网络迅速延伸到人迹罕至和偏远地点，除传统的地面链路、光纤链路外，卫星通信将起着举足轻重的作用。卫星具有诸多优点，包括覆盖区域广泛。由于处在如此高的高度，它们所能发射及接收信号的范围很大。一个同步卫星可以覆盖地球三分之一以上的地表，这样，利用三个相距 120 度的卫星便可覆盖整个地球上的全部通信区域。因此，卫星在一点对多点和广播应用具有很大优势。然而与所有微波系统一样，卫星的性能随天气的变化而有所不同。卫星通信的最大特点是通信距离远，且通信费用与通信距离无关。卫星通信的另一特点就是具有较大的传播时延。

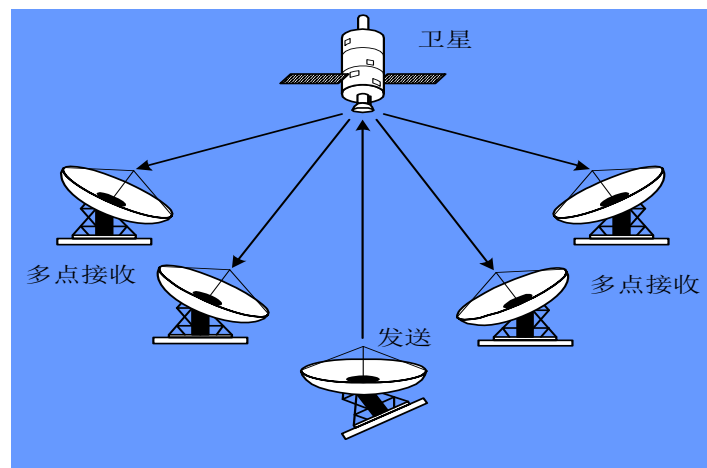


图 3-12 卫星信道传输

### 3.5.2 红外线信道和激光信道

#### 1、红外线信道

电视和立体声系统所使用的遥控器是用红外线进行通信。红外线一般局限于一个很小的区域（例如，在一个房间内）并且通常要求发送器直接指向接收器。红外硬件与采用其他机制的设备比较相对便宜，且不需要天线。计算机网络可以使用红外技术进行数据通信。例如，为一个大房间配备一套红外连接以使该房间内的所有计算机在房间内移动时仍能和网络保持连接。红外网络对小型的便携计算机尤为方便。因为红外技术提供了无需天线的无绳连接。这样，使用红外技术的便携计算机可将所有的通信硬件放在机内。

利用红外线来传输信号，其传输方式类似于家用电器的红外线遥控，在发送端设有红外线发送器，接收端有红外线接收器。发送器和接收器可任意安装在室内或室外，但需使它们之间处于视线范围内，即发送器和接收器彼此都看到对方，中间不允许有障碍物。红外线信道具有一定的带宽，当传输速率为 100KBPS 时，其通信距离可大于 16 公里，当传输速率为 1.5MBPS 时，通信距离为 1.6 公里。此外，因红外线具有极强的方向性，故对于这类系统很难窃听、插入数据和进行干扰；但环境干扰都会影响红外线的传输。

#### 2、激光信道

光纤可把光用于通信中，光也能用于在空中传输数据。和微波通信系统一样，采用光的通信连接通常由两个站点组成，每个站点都拥有发送器和接收器，设备安装在一个固定的位置，也同样需使它们处在视线范围内，以便一个站点的发送器将光束直接传输至另一站点的接收器。因为激光能在很长距离内保持聚焦，所以发送器可以使用激光器产生光束。激光通信与红外线通信一样是全数字的，不能传输模拟信号。和微波传输一样，激光器发出的光束走的也是直线，并且不能被遮挡。激光具有方向性，难以窃听、插入数据及进行干扰，易受环境的影响。

## 3.6 调制解调器

### 3.6.1 调制解调器

为了能利用现有的电话系统传输数字信号，必须先将数字信号变换成模拟信号。调制器的基本职能是把从终端设备和计算机送出的数字信号变换为适合于在模拟信道上传输的模拟信号；解调器的基本职能是把模拟信号恢复成数字信号。常说的 Modem，其实是 Modulator（调制器）与 Demodulator（解调器）的简称，通常都把调制器和解调器做在一起而称之为调制解调。有人根据 Modem 的谐音，亲昵地称之为“猫”。图 3-13 描述了使用调制解调器通过电话交换网连接二台远程计算机的连接方式。

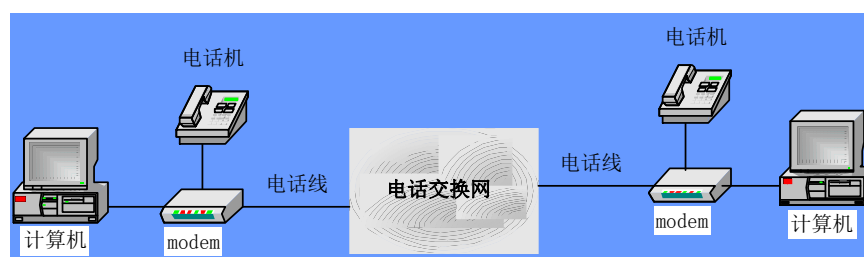


图 3-13 调制解调器连接

### 3.6.2 调制解调器的分类与协议

#### 1、调制解调器分类

一般来说，根据 Modem 的形态和安装方式，可以大致可以分为以下四类：

##### 1) 外置式 Modem

外置式 Modem 放置于机箱外，通过串行通讯口与主机连接。这种 Modem 方便灵巧、易于安装，闪烁的指示灯便于监视 Modem 的工作状况。但外置式 Modem 需要使用额外的电源与电缆。

##### 2) 内置式 Modem

内置式 Modem 在安装时需要拆开机箱，并且要对中断和 COM 口进行设置，安装较为繁琐。这种 Modem 要占用主板上的扩展槽，但无需额外的电源与电缆，且价格比外置式 Modem 要便宜一些。

##### 3) PCMCIA 插卡式 Modem

插卡式 Modem 主要用于笔记本电脑，体积纤巧。配合移动电话，可方便地实现移动办公。

##### 4) 机架式 Modem

机架式 Modem 相当于把一组 Modem 集中于一个箱体或外壳里，并由统一的电源进行供电。机架式 Modem 主要用于 Internet/Intranet、电信局、校园网、金融机构等网络的中心机房。

除以上四种常见的 Modem 外，现在还有 ISDN 调制解调器和一种称为 Cable Modem 的调制解调器，另外还有一种 ADSL 调制解调器。Cable Modem 利用有线电视的电缆进行信号传送，不但具有调制解调功能，还集路由器、集线器、桥接器于一身，理论传输速度更可达 10Mbps 以上。通过 Cable Modem 上网，每个用户都有独立的 IP 地址，相当于拥有了一条个人专线。

#### 2、调制解调器传输协议



---

Modem 的传输协议包括调制协议 (Modulation Protocols)、差错控制协议 (Error Control Protocols)、数据压缩协议 (Data Compression Protocols) 和文件传输协议。

#### 1) 调制协议

计算机内的信息是由“0”和“1”组成数字信号，而在电话线上传递的却只能是模拟电信号。于是，当两台计算机要通过电话线进行数据传输时，就需要一个设备负责数模的转换。计算机在发送数据时，先由 Modem 把数字信号转换为相应的模拟信号，这个过程称为“调制”。经过调制的信号通过电话载波传送到另一台计算机之前，也要经由接收方的 Modem 负责把模拟信号还原为计算机能识别的数字信号，这个过程称为“解调”。正是通过这样一个“调制”与“解调”的数模转换过程，从而实现了两台计算机之间的远程通讯。

#### 2) 差错控制协议

随着 Modem 的传输速率不断提高，电话线路上的噪声、电流的异常突变等，都会造成数据传输的出错。差错控制协议要解决的就是如何在高速传输中保证数据的准确率。目前的差错控制协议存在着两个工业标准：MNP4 和 V4.2。其中 MNP (Microcom Network Protocols) 是 Microcom 公司制定的传输协议，包括了 MNP1 - MNP10。由于商业原因，Microcom 目前只公布了 MNP1 - MNP5，其中 MNP4 是目前被广泛使用的差错控制协议之一。而 V4.2 则是国际电信联盟制定的 MNP4 改良版，它包含了 MNP4 和 LAP-M 两种控制算法。因此，一个使用 V4.2 协议的 Modem 可以和一个只支持 MNP4 协议的 Modem 建立无差错控制连接，而反之则不能。所以我们在购买 Modem 时，最好选择支持 V4.2 协议的 Modem。

#### 3) 数据压缩协议

为了提高数据的传输量，缩短传输时间，现时大多数 Modem 在传输时都会先对数据进行压缩。与差错控制协议相似，数据压缩协议也存在两个工业标准：MNP5 和 V4.2bis。MNP5 采用了 Rnu-Length 编码和 Huffman 编码两种压缩算法，最大压缩比为 2:1。而 V4.2bis 采用了 Lempel-Ziv 压缩技术，最大压缩比可达 4:1。这就是为什么说 V4.2bis 比 MNP5 要快的原因。要注意的是，数据压缩协议是建立在差错控制协议的基础上，MNP5 需要 MNP4 的支持，V4.2bis 也需要 V4.2 的支持。并且，虽然 V4.2 包含了 MNP4，但 V4.2bis 却不包含 MNP5。

#### 4) 文件传输协议

文件传输是数据交换的主要形式。在进行文件传输时，为使文件能被正确识别和传送，需要在两台计算机之间建立统一的传输协议。这个协议包括了文件的识别、传送的起止时间、错误的判断与纠正等内容。常见的传输协议有以下几种：

ASCII：这是最快的传输协议，但只能传送文本文件。

Xmodem：这种古老的传输协议速度较慢，但由于使用了 CRC 错误侦测方法，传输的准确率可高达 99.6%。

Ymodem：这是 Xmodem 的改良版，使用了 1024 位区段传送，速度比 Xmodem 要快。

Zmodem：Zmodem 采用了串流式 (streaming) 传输方式，传输速度较快，而且还具有自动改变区段大小和断点续传、快速错误侦测等功能。这是目前最流行的文件传输协议。

### 3.6.3 调制解调器的编程命令

Hayes 公司生产的调制解调器目前几乎成了公认的调制解调器标准，其它厂家生产的调制解调器一般都与之兼容。Hayes 公司推出了一套用于对调制解调器进行编程的命令，这些命令都以 AT 打头，故也称作 AT 命令集。AT 是 Attention(注意)的开头两个字母，意为引起调制解调器的注意。跟在 AT 后面的字符串用以通知调制解调器干什么。下面介绍几种常用的 AT 命令。

(1) 拨号命令。ATD 命令用于电话拨号。拨号分脉冲拨号和音频拨号两种，因此拨号时应告诉调制解调器采用何种信号进行拨号。ATDP 用于脉冲拨号，ATDT 用于音频拨号，两者均后续要拨的电话号码。例如：ATDT12345678 表示用音频拨号呼叫 12345678。若在分机拨出，则先要拨外线，



---

然后稍停顿后再拨对方号码，其间插入逗号稍作停顿，一个逗号相当于停顿 2 秒。例如 ADTP0, 12345678 则表示先拨 0，请求接外线后停顿 2 秒，再拨外线 12345678。

(2) 应答命令。ATA 命令用于使用调制解调器立即应答电话。调制解调器自动应答功能是通过对其 S0 寄存器的设置来实现的，ATS0=0 表示取消调制解调器的自动应答功能，ATS0=N(N 为非零的整数)表示调制解调器振铃达到 N 次后，才应答电话。

(3) 摘机和挂机命令。输入的 ATH1 使电话摘机，就像拿起听筒一样；输入 ATH0 或 ATH 是电话挂机，就像放下电话一样。执行拨号命令时，调制解调器会自动进入摘机状态，若在联机状态时载波信号调时，调制解调器会自动断开连接或挂机。

(4) 调制解调器缺省设置恢复命令。输入 ATZ 命令可以将调制解调器内部寄存器设置为缺省的参数值，以使用户重新调用其数值。

还用许多其他的 AT 命令，提供了对调制解调器的各种操作功能，这些都可以在相应的手册上查阅到。需要说明的是，AT 命令不是 DOS 命令，它必须通过通信软件经通信端口发向调制解调器。

# 第四章 数据链路层

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

数据链路层的许多概念都属于计算机网络的基本概念。本章在介绍数据链路层的基本概念后，就详细地讨论两个重要的协议：停止等待协议和连续 ARQ 协议，包括滑动窗口的概念；接着阐明面向比特的链路控制规程 HDLC；最后介绍 Internet 中的数据链路层协议。

## 4.1 数据链路层概述

### 4.1.1 数据链路层的作用

在计算机网络中，“链路”和“数据链路”是两个不同的概念。所谓链路就是一条无源的点到点的物理线路段，中间没有任何其它的交换结点。在进行通信时，两个计算机之间的通路往往是由许多的链路串接而成的。可见一条链路只是一条通路的一个组成部分。当需要在一条链路上传送数据时，除了必须有一条物理线路外，还必须有一些必要的规程来控制这些数据的传输。把实现这些规程的硬件和软件加到链路上，就构成了数据链路。数据链路就像一个数字管道，可以在它上面进行数据通信。当采用复用技术时，一条链路上可以有多条数据链路。

人们经常将链路分为物理链路和逻辑链路。物理链路就是上面所说链路，而逻辑链路就是上面的数据链路，是物理链路加上必要的通信规程。这两种划分方法实质上是一样的。

数据链路层最重要的作用就是：通过数据链路层协议(即链路控制规程)，在不太可靠的物理链路上实现可靠的数据传输。

### 4.1.2 数据链路层的功能

数据链路层从物理层获得的服务是原始的比特流传输服务，而比特流在传输过程中会出错，因此检测和纠正这些错误使得网络层可以不用关心传输错误，成为数据链路层的一项重要工作；其次，较高的发送速度和较低的接收能力的不匹配，也是造成传输出错的一个原因，因此流量控制也是数据链路层的一项重要工作；另外，不同的应用或者传输环境可能要求不同的数据链路层服务，因此数据链路层应该有多种服务供上层选择，且每种服务有定义良好的接口供上层调用。

数据链路层的主要功能归纳如下：

#### 1) 链路管理

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

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

## 2) 帧同步

为了使传输中发生差错后只将出错的有限数据进行重发，数据链路层将比特流组织成以帧为单位传送。帧的结构必须设计成使接收方能够明确的从物理层收到的比特流中对其进行识别，即能从比特流中区分出帧的开始和结束，这就是帧同步要解决的问题。由于网络传输中很难保证计时的正确和一致，所以不能采用依靠时间间隔关系来确定一帧的开始和结束。

下面介绍几种常用的帧同步方法。

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

(2) 使用字符填充的首尾定界符法。该方法用一些特定的字符来定界一帧的开始和结束。为了不使数据信息中出现的与特定字符相同的字符被误判为帧的首尾定界符，可以在这种数据字符前填充一个转义控制字符以示区别，从而达到数据的透明性。

(3) 使用比特填充的首尾定界符法。该方法以一组特定的比特模式(如 01111110)来标志一帧的开始和结束。为了不使数据信息中出现的与该特定模式相似的比特串被误判为帧的首尾标志，可以采用比特填充的方法。比如，采用特定模式 01111110，则对数据信息中的任何连续出现的 5 个“1”，发送方自动在其后插入一个“0”，而接受方则做该过程的逆操作，即每收到连续 5 个“1”，则自动删去其后所跟的“0”，以此恢复原始信息，实现数据传输的透明性。比特填充很容易由硬件来实现，性能优于字符填充方法。

(4) 违法编码法。该方法在物理层采用特定的比特编码方法。例如，曼彻斯特编码方法是将数据比特“1”编码成“高-低”电平对，将数据比特“0”编码成“低-高”电平对。而“高-高”电平对和“低-低”电平对在数据比特中是违法的。可以借用这些违法编码序列来定界帧的开始和结束。局域网 IEEE 802 标准中就采用了这种方法。违法编码法不需要任何填充技术，便能实现数据的透明性，但它只适用采用冗余编码的特殊编码环境。

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

## 3) 流量控制

流量控制并不是数据链路层特有的功能，许多高层协议中也提供流量控制功能，只不过流量控制的对象不同而已。比如，对于数据链路层来说，控制的是相邻两节点这间数据链路上的流量，而对于传输层来说，控制的则是从源端到最终目的端之间的端对端的流量。

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

## 4) 差错控制

在计算机通信中，一般都要求有极低的比特差错率。一个实用的通信系统必须具备发现(即检测)差错的能力，并采取某种措施纠正之，使差错被控制在所能允许的尽可能小的范围内，这就是差错控制过程，也是数据链路层的主要功能。为此，广泛地采用了编码技术。编码技术有两大类。一类是前向纠错，即接收方收到有差错的数据帧时，能够自动将差错改正过来。这种方法的开销较大，不适合于计算机通信。另一类是检错重发，即接收方可以检测出收到的帧中有差错(但并不知道是哪几个比特错了)。于是就让发送方重复发送这一帧，直到接收方正确收到这一帧为止。这种方法在计算机通信中是最常用的，也是数据链路层的主要功能之一。

接收方通过对差错编码(奇偶校验码或 CRC 码)的检查，可以判定一帧在传输过程中是否发

生了差错。一旦发现差错，一般可以采用反馈重发的方法来纠正。这就要求接受方收完一帧后，向发送方反馈一个接收是否正确信息，使发送方据此做出是否需要重新发送的决定。发送方仅当收到接收方以正确接收的反馈信号后才能认为该帧已经正确发送完毕，否则需要重发直至正确为止。

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

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

### 5) 透明传输

所谓透明传输就是不管所传数据是什么样的比特组合，都应当能够在链路上传送。当所传数据中的比特组合恰巧出现了与某一个控制信息完全一样时，必须采取适当的措施，使接收方不会将这样的数据误认为是某种控制信息。这样才能保证数据链路层的传输的透明的。

### 6) 寻址

在多点连接的情况下，必须保证每一帧都能送到正确的目的站。接收方也应当知道发送方是哪一个站。

## 4.1.3 数据链路层提供的服务

数据链路层提供多种不同的服务，但大多提供以下三种服务：

### 1 无确认的无连接服务

源端向目的端发送独立的帧，传输前不需要建立逻辑连接，传输后也不要求目的端进行确认，也就是说不能保证每个帧能被正确接收。目的端可能会将出错的帧丢弃，但不会通知源端，也不会试图发现是否有帧丢失，传输错误的恢复依靠高层协议去完成。这类服务适用于误码率非常低的传输环境及一些实时业务，大多数局域网使用这一类服务。

### 2 有确认的无连接服务

传输前不需要建立逻辑连接，但目的端对于收到的每个帧都必须单独向源端发送确认或者否认信息，出错或丢失的帧需要重发，直到目的端正确接收为止。这类服务适用于误码率较高的传输环境，如无线传输环境。

### 3 有确认的面向连接的服务

传输前需要建立逻辑连接，为每个发送的帧建立帧编号并按序发送，目的端对收到的帧进行检错和确认，出错或丢失的帧需要重发直至目的端正确接收为止，目的端的数据链路层保证向其网络层递交正确有序的数据流。

当 OSI 确定了应当有一个数据链路层后，又出现了许多种新的网络，如局域网等。这些网络的数据链路层种类繁多，无法使用一种统一的数据链路层协议。于是数据链路层就分解为两个子层(这在局域网中讨论)。本章讨论最基本的数据链路层协议，这里所涉及的许多概念对学习计算机网络整个课程都是很重要的。

## 4.2 基本的数据链路层协议

停止等待协议是最简单但也最基本的数据链路层协议。为了便于说明，我们采用一个简化的模型(图 4-1 所示)，把数据链路层以上的各层用一个主机来代替，物理层和传输介质则等效成一条简单的链路。在发送方和接收方的数据链路层分别有一个发送缓冲区和接收缓冲区。若进行双工通信，则在每一方要同时设有发送缓冲区和接收缓冲区。缓冲区是必不可少的，因为在通信线路上数据是以比特流的形式串行传输的，但在计算机内部数据的传输则是以字节为单位进行并行传输。因此，必须在计算机的内存中设置一定容量的缓冲区，以便解决数据传输速率不一致的问题。

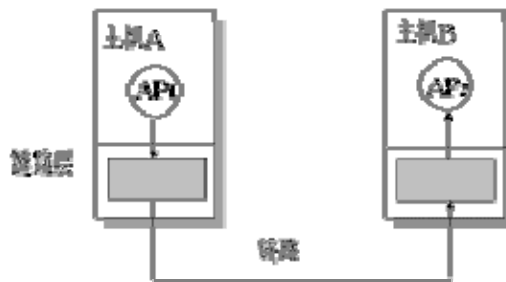


图 4-1 两台计算机通信的简化模型

### 4.2.1 停止等待协议

停止等待协议是工作在数据链路层，一种具有基本流量控制和差错检测校验的基本协议。是当今网络中常用的具有流量控制功能的数据链路层协议的基础，大部分的数据链路层协议，如，ARQ, HDLC 及 PPP 等协议都是在停等协议的基础上发展起来。

设计实用的数据链路层协议应考虑到：传输数据的信道不是可靠的（即不能保证所传的数据不产生差错），并且还需要对数据的发送方进行流量控制。

#### 1) 正常情况。

数据在传输过程中不出差错的情况下，接收方 B 在接收到一个正确的数据帧后，立即交付给主机进行上层协议的进一步处理，同时向主机 A（发送方）发送一个确认帧 ACK。当主机 A 收到确认帧 ACK 后才能发送一个新的数据帧。

#### 2) 数据帧出错。

如果主机 A 发送的数据在传输过程中出错，接收方 B 进行差错检测（CRC 检测）后，会给主机 A 发送一个否认帧 NAK。这种情况下，发送方需要重发出错的数据。

#### 3) 数据帧丢失。

如果主机 A 发送的数据在传输过程中丢失，接收方 B 没法接收到数据。此时，B 即不会发送确认帧 ACK，也不会发送否认帧 NAK。因此，A 在无法接收应答帧的情况下，不会进行任何处理，出现了死锁现象。为了避免此种情况出现，在发送方 A 发送完一个数据帧时，需要同时启动一个定时器（timer）。若到了超过定时器所设置的重传时间而仍接收不到应答帧，主机 A 就会重发数据。此过程称为超时重传。

4) 应答帧丢失。超时重传的缺点是若丢失的数据帧是接收方发出的回应帧，发送方 A 同样会在超时后重发数据，此时接收方 B 就会接到两个同样的数据帧，出现了重复帧情况。为了解决重复帧问题，必须给每个数据帧编号。在对比编号后，只有编号相同时才正常接收，否则丢弃。

任何一个编号系统的序号所占用的比特数一定是有限的。因此，经过一段时间后，发送序号就会重复。例如，当发送序号占用 3 个比特时，就可组成共有 8 个不同的发送序号，从 000 到 111。当数据帧的发送序号为 111 时，下一个发送序号就又是 000。因此，要进行编号就要考虑序号到底要占用多少个比特。序号占用的比特数越少，数据传输的额外开销就越小。对于停止等待协议，由于每发送一个数据帧就停止等待，因此用一个比特来编号就够了。一个比特可以有 0 和 1 两种不同的序号。这样，数据帧中的发送序号(以后记为  $N(S)$ ， $S$  表示发送)就以 0 和 1 交替的方式出现在数据帧中。每发一个新的数据帧，发送序号就和上次发送的不一样。用这样的方法就可以使接收方能够区分开新的数据帧和重发的数据帧了。

#### 4.2.2 停止等待协议的算法

为了对上面所述的停止等待协议有一个完整而准确的理解，图 4-2 给出此协议的算法。

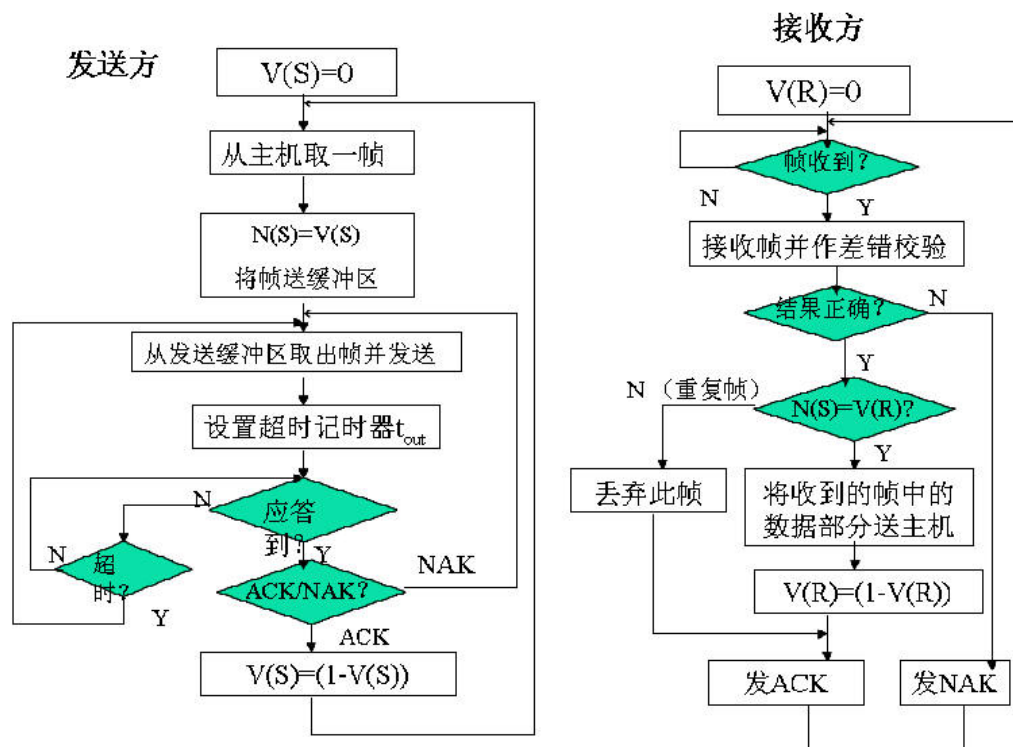


图 4-2 停止等待协议的算法

发送方：

- (1) 发送一个帧；启动定时器；等待应答；转(2)
- (2) 定时器未到：收到应答
  - 1) 肯定应答，转(1)，发下一帧；
  - 2) 否定应答，转(3)，重传该帧；
 或  
 定时器已到：未收到应答  
 转(3)，重传该帧；
- (3) 若重传次数<设定值，重传该帧；  
 否则，信道故障，通讯终止。

接收方：

- (1) 收到数据帧；

(2) 帧正确性判断

不正确, 发 NAK;

正确, 转(3);

(3) 重复帧判断

重复, 丢弃, 发 ACK 应答;

不重复, 接受, 发 ACK 应答。

由于发送端对出错的数据帧进行重发是自动进行的, 所以这种差错控制体制常简称为 ARQ(Automatic Repeat reQuest), 即自动请求重发。

### 4.2.3 连续 ARQ 协议

ARQ 协议的工作要点就是在发送完一个数据帧后, 不是停下来等待应答帧, 而是可以连续再发送若干个数据帧。如果这时收到了接收端发来的确认帧, 那么还可以接着发送数据帧。由于减少了等待时间, 整个通信的吞吐量就提高了。

如图 4-3 所示, 结点 A 向结点 B 发送数据帧。当结点 A 发完 0 号帧后, 不是停止等待, 而是继续发送后续的 1 号帧、2 号帧等。由于连续发送了许多帧, 所以应答帧不仅要说明是对哪一帧进行确认或否认, 而且应答帧本身也必须编号。

结点 B 正确地收到了 0 号帧和 1 号帧, 并送交其主机。现在设 2 号帧出了差错, 于是结点 B 就将有差错的 2 号帧丢弃。结点 B 运行的协议可以有两种选择: 一种是在出现差错时就向结点 A 发送否认帧, 另一种则是在出现差错时不做任何响应。我们现在假定采用后一种协议, 这种协议比较简单, 使用得较多。

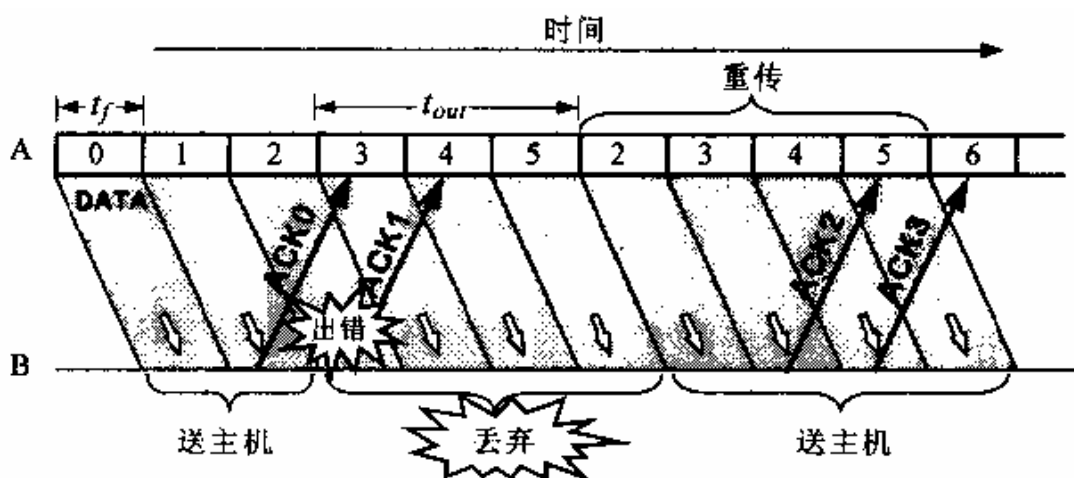


图 4-3 连续 ARQ 协议的工作原理: 数据帧出错

因此, 连续 ARQ 协议是指发送方可以连续发送一系列数据帧, 即不用等前一帧被确认便可发送下一帧。这就需要在发送方设置一个较大的缓冲存储空间(称作重发表), 用以存放若干待确认的数据帧。发送方收到对某数据帧的确认帧后便可从重发表中将该数据帧删除。所以, 连续 ARQ 方案的链路传输效率大大提高, 但相应地需要更大的缓冲存储空间。连续 ARQ 方案的实现过程如下:

- (1) 发送方连续发送数据帧而不必等待确认帧的返回;
- (2) 发送方在重发表中保存所发送的每个帧的备份;
- (3) 重发表按先进先出(FIFO)队列规则操作;
- (4) 接收方对每一个正确收到的数据帧返回一个确认帧; 对每一个出错的数据帧返回一个否



认帧；

- (5) 每一个确认帧（否认帧）包含一个唯一的序号，随相应的确认帧返回；
- (6) 接收方保存一个接收次序表，它包含最后正确收到的数据帧的序号；
- (7) 当发送方收到相应数据帧的确认帧后，从重发表中删除该数据帧的备份；
- (8) 当发送方收到第 N 号数据帧的否认帧或者在  $T_{out}$  时间内没有收到第 N 号数据帧的确认帧或否认帧，便从第 N 号数据帧开始重发。

这里要注意两点：

(1) 接收端只按序接收数据帧。虽然在有差错的 2 号帧之后接着又收到了正确的 3 个数据帧，但都必须将它们丢弃，因为这些帧的发送序号都不是所需的 2 号。

(2) 结点 A 在每发送完一个数据帧时都要设置超时定时器。只要在所设置的超时时间  $T_{out}$  到而仍未收到确认帧，就要重发相应的数据帧。在等不到 2 号帧的确认而重发 2 号数据帧时，虽然结点 A 已经发完了 5 号帧，但仍必须向回走，将 2 号帧及其以后的各帧全部进行重传。

正因如此，连续 ARQ 又称为 Go-back-N ARQ，意思是当出现差错必须重传时，要向回走 N 个帧，然后再开始重传。

从这里不难看出，连续 AREQ 协议一方面因连续发送数据帧而提高了效率，但另一方面，在重传时又必须把原来已正确传送过的数据帧进行重传（仅因这些数据帧之前有一个数据帧出了错），这种做法又使传送效率降低。由此可见，若传输信道的传输质量很差因而误码率较大时，连续 ARQ 协议不一定优于停止等待协议。

如果 2 号数据帧不是出现差错而是彻底丢失了，那么情况也是类似的。

#### 4.2.4 选择重传 ARQ 协议

为了进一步提高信道的利用率，可以设法只重传出现差错的数据帧或者是定时器超时的数据帧。此时必须加大接收方的缓冲存储空间，以便先收下发序号不连续但仍处在有效状态的那些数据帧。等到所缺序号的数据帧收到之后再一并送交主机。这就是选择重传 ARQ 协议。

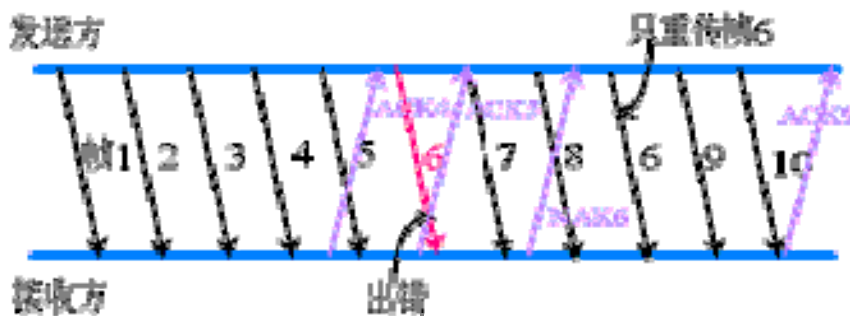


图 4-4 选择重传 ARQ 协议的工作原理

图 4-4 是选择重传 ARQ 协议的示意图。假定 6 号数据帧在传送时丢失，按照选择重传 ARQ 协议，接着传送的 7-8 号数据帧在接收端不是被丢弃，而是先暂存一下。等到 6 号数据帧由于超时定时器时间到而重传并到达接收端时，接收端再按数据帧的序号顺序交付给主机。这样做可避免重复传送那些本来已经正确到达接收端的数据帧。但我们付出的代价是在接收端要设置具有一定容量的缓存空间，这在很多情况下是不够经济的。正因如此，选择重传 ARQ 协议在目前还远没有连续 ARQ 协议使用的那么广泛。今后随着存储器芯片价格的下降，选择重传 ARQ 协议还是有可能得到重视的。

## 4.3 流量控制

在使用连续 ARQ 协议时，如果发送方一直没有收到对方的确认信息。那么实际上发送方并不能无限制地发送其数据帧。这是因为：

(1) 当未被确认的数据帧的数目太多时，只要有一帧出了差错，就可能要有很多的数据帧需要重传，这必然就要白白花费较多的时间，因而增大开销。

(2) 为了对所发送出去的大量数据帧进行编号，每个数据帧的发送序号也要占用较多的比特数，这样又增加了一些不必要开销。

因此，在连续 ARQ 协议中，应当将已发送出去但未被确认的数据帧的数目加以限制，这就是流量控制所要研究的内容。

流量控制是数据链路上数据帧的发送速率的控制，以使接收方在接收前有足够的缓冲存储空间来接收每一个数据帧。例如，在面向字符的终端—计算机链路中，若远程计算机为许多台终端服务，它就有可能因不能在高峰时按预定速率传输全部字符而暂时过载。同样，在面向数据帧的自动重发请求系统中，当待确认帧数量增加时，有可能超出缓冲器存储空间，也会造成过载。下面介绍两种常用的流量控制方案：XON/XOFF 方案和滑动窗口机制。

### 4.3.1 XON/XOFF 方案

增加缓冲存储空间在某种程度上可以缓解收、发双方在传输速率上的差异，但这是一种被动、消极的方法。因为，一方面系统不允许开设过大的缓冲空间，另一方面对于速率显著失配并且又传送大量数据的场合，仍会出现缓冲空间不够的现象。XON/XOFF 方案则是一种比较主动和积极的流量控制方法。

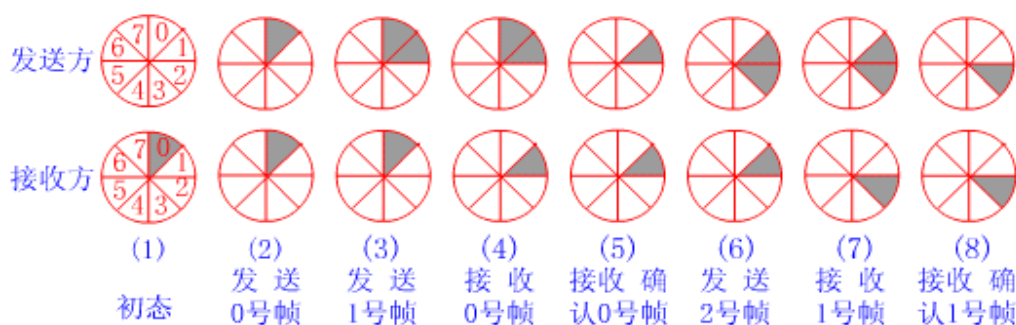
XON/XOFF 方案中使用一对控制字符来实现流量控制，其中 XON 采用 ASCII 字符集中的控制字符 DC1，XOFF 采用 ASCII 字符集中的控制字符 DC3。当通信路上的接收方发生过载时，便向发送方发送一个 XOFF 字符，发送方接收 XOFF 字符后便暂停发送数据；等接收方处理完缓冲器中的数据，过载恢复后，再向发送方发送一个 XON 字符，以通知发送方恢复数据发送。在一次数据传输过程中，XOFF、XON 的周期可重复多次，但这些操作对用户来说是透明的。

许多异步数据通信软件包均支持 XON/XOFF 协议。这种方案也可用于计算机向打印机或其它终端设备发送字符，在这种情况下，打印机或终端设备中的控制部件用以控制字符流量。

### 4.3.2 滑动窗口机制

滑动窗口机制的基本原理就是在任意时刻，发送方都维持了一个连续的允许发送的帧的序号，称为发送窗口；同时，接收方也维持了一个连续的允许接收的帧的序号，称为接收窗口。发送窗口和接收窗口的序号的上下界不一定要一样，甚至大小也可以不同。

发送方窗口内的序列号代表了那些已经被发送，但是还没有被确认的帧，或者是那些可以被发送的帧。例如图 4-5 所示（假设发送窗口尺寸为 2，接收窗口尺寸为 1）：



分析：

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

2) 发送方打开 0 号窗口, 表示已发出 0 帧但尚确认返回信息。此时接收窗口状态不变;

3) 发送方打开 0、1 号窗口, 表示 0、1 号帧均在等待确认之列。至此, 发送方打开的窗口数已达规定限度, 在未收到新的确认返回帧之前, 发送方将暂停发送新的数据帧。接收窗口此时状态仍未变;

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

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

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

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

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

显然, 如果窗口设置为 1, 即发送方缓冲能力仅为一个帧, 则传输控制方案就回到了 ARQ 协议, 此时传输效率很低。故窗口限度应选为使接收方尽量能处理或接受收到的所有帧。当然选择时还必须考虑诸如帧的最大长度、可使用的缓冲存储空间以及传输速率等因素。

当数据帧的发送序号所占用的比特数一定时, 发送窗口的最大值是多少。初看起来, 这个问题好像很简单。例如, 用 3 个比特可编出 8 个不同的序号, 因而发送窗口的最大值似乎应当是 8。但实际上, 这将使协议在某些情况下无法工作。现在我们就来说明这点。

现在设发送窗口  $W_t=8$ 。设发送方发送完 0 - 7 号共 8 个数据帧。因发送窗口已满, 发送暂停。假定这 8 个数据帧均已正确到达接收端, 并且对每一个数据帧, 接收端都发送出确认帧。下面考虑两种不同的情况。

第一种情况是: 所有的确认帧都正确到达了发送方, 因而发送方接着又发送 8 个新的数据帧, 其编号应当是 0 - 7。

第二种情况是: 所有的确认帧都丢失了。经过一段时间后, 发送方重发 8 个旧的数据帧。其编号仍为 0 - 7。问题已经十分明显了, 接收端第二次收到编号为 0 - 7 的 8 个数据帧时, 无法判定; 这是 8 个新的数据帧, 或这是 8 个旧的重发的数据帧。

因此, 将发送窗口设置为 8 显然是不行的。可以证明, 当用  $n$  个比特进行编号时, 若接收窗口的大小为 1, 则只有在发送窗口的大小  $W_t \leq 2^n - 1$  时, 连续 ARQ 协议才能正确运行。这就是说, 当采用 3 比特编码时, 发送窗口的最大值是 7 而不是 8。这对一般的陆地链路已足够大了。但对于卫星链路, 由于其传播时延很大, 发送窗口也必须适当增大才能使信道利用率不会太低。这时常用 7 位编码, 因而发送窗口的大小可达 127。在这种情况下, 所有已发送出去的但尚未被确认的数据帧都必须保存在发送方的缓冲区中, 以便在出差错时进行重发。当然, 这就要占用相当大的内存空间。相反, 对于停止等待协议, 发送窗口  $W_t=1$ , 发送方只要花费 1 个数据帧的内存空间即可。

当采用  $n$  个比特进行编码时, 由于选择重传 ARQ 协议, 发送窗口  $W_t$  与接收窗口  $W_r$  之和必须满足下式:

$$W_t + W_r \leq 2^n$$

因为接收窗口不应大于发送窗口, 所以在选择重传 ARQ 协议中, 接收窗口的最大值受下式

的约束：

$$W_r \leq 2^{n-1}$$

当接收窗口  $W_r$  为最大值时， $W_r = W_t = 2^{n-1}$ 。当  $n=3$  时，可以算出  $W_r = W_t = 4$ 。

## 4.4 面向字符的数据链路控制规程

### 4.4.1 数据链路控制协议的分类

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

异步协议以字符为独立的信息传输单位，在每个字符的起始处开始对字符内的比特实现同步，但字符与字符之间的间隔时间是不固定的(即字符之间是异步的)。由于发送器和接收器中近似于同一频率的两个约定时钟，能够在一段较短的时间内保持同步，所以可以用字符起始处同步的时钟来采样该字符中的各比特，而不需要每个比特再用其他方法同步。异步协议中由于每个传输字符都要添加诸如起始位、校验位、停止位等冗余位，故信道利用率很低，一般用于数据速率较低的场合。

同步协议是以许多字符或许多比特组成的数据帧为传输单位，在帧的起始处同步，使帧内维持固定的时钟。由于采用帧为传输单位，所以同步协议能更有效地利用信道，也便于实现差错控制、流量控制等功能。

同步协议又分为面向字符的同步协议、面向比特的同步协议二种类型。本节主要讨论面向字符的同步协议。

### 4.4.2 面向字符的同步控制协议—BSC

面向字符的同步协议是最早提出的数据链路层协议，其典型代表是 IBM 的二进制同步通信 BSC(Binary Synchronous Communication)协议。ANSI 和 ISO 也提出了类似的相应标准。所谓面向字符就是说的在链路上所传送的数据必须是由规定字符集(例如 ASCII 码)中的字符所组成。不仅如此，在链路上所传送的控制信息也必须由同一个字符集中的若干指定的控制字符构成。

任何链路层协议均可由链路建立、数据传输和链路拆除三部分组成。为了实现链路建立、链路拆除等链路管理以及同步等各种功能，除了正常传输的数据块和报文外，还需要一些控制字符。BSC 协议用 ASCII 和 EBCDIC 字符集定义的传输控制字符来实现相应的功能。

#### 1. 控制字符

BSC 协议的传输控制字符的标记、名字及 ASCII 码值和 EBCDIC 码值见表 4-1。

表 4-1 传输控制字符

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

各传输控制字符的功能如下：

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

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

ETX(End of Text)：文终，标志报文文本的结束。

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

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

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

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

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

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

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

## 2. 报文格式

BSC 协议将在数据链路上传输的信息分为数据和监控报文两类。监控报文又可分为正向监控和反向监控两种。每一种报文中至少包括一个传输控制字符, 用以确定报文中信息的性质或实现某种控制作用。

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

BSC 协议的数据块有如下四种格式:

- (1) 不带报头的单块报文或分块传输中的最后一块报文:

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

- (2) 带报头的单块报文:

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

- (3) 分块传输中的第一块报文:

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

- (4) 分块传输中的中间报文:

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

说明: BCC 是校验字段。

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

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

正、反向监控报文有如下四种:

- (1) 肯定确认和选择响应:

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

- (2) 否定确认和选择响应:

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

- (3) 轮询/选择请求:

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

- (4) 拆链:

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

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

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

### 3. 数据帧的交换过程

因为 BSC 是使用停等流控的半双工协议，发送和确认帧的处理就简化了。图 4-9 说明了一个典型的事件流。站 A（主站）发送一个 ENQ 控制帧给 B。因为 ENQ 帧请求一个回答，站 B 就发回一个确认信号。A 接收到确认信号后，A 和 B 就交换一系列的数据帧和确认信号。如果 B 正确地接收了一帧，它就发回一个包含 ACK 控制字符的控制帧。当 A 接收到这个控制帧，ACK 字符就表明前一帧已经被接收了。因此，A 发送下一帧。只要 A 有帧发送，这种交换就继续下去。当 A 没有数据可发送时，它就发送一个 EOT 帧。作为回答，B 就发送它自己的 EOT 帧。当 A 接收到这一帧时，这两者之间的连接就终止了。

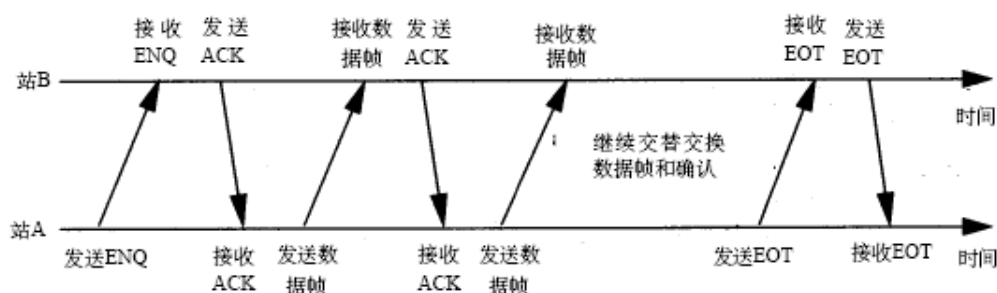


图 4-7 数据帧的交换过程

## 4.5 面向比特的链路控制规程—HDLC

### 4.5.1 HDLC 的产生背景

在计算机通信的早期人们就已经发现，对于经常产生误码的实际链路，只要加上合适的控制规程，就可以使通信变为比较可靠的。那时 ARPANET 和 IBM 公司分别使用了各自的控制规程，它们分别是：IMP-IMP 协议和 BSC 规程。这些规程都是数据链路层的协议。这种面向字符的链路控制规程在计算机网络的发展过程中曾起了重要的作用。但随着计算机通信的发展，这种面向字符的链路控制规程就逐渐暴露出其弱点。就以著名的 BSC 规程来说，其主要限制是：

- (1) 通信线路的利用率低，因为它采用的是停止等待协议。收发双方交替地工作。
- (2) 所有通信的设备必须使用同样字符代码，而不同版本的 BSC 规程要求使用不同的代码。
- (3) 只对数据部分进行差错控制，若控制部分出错就无法控制，因而可靠性较差。

(4) 不易扩展。每增加一种功能就需要设定一个新的控制字符。

此外，它还存在其他一些缺点。由此可见，需要设计出一种新的链路控制规程来代替旧的面向字符的链路规程。

1974年，IBM公司推出了著名的体系结构SNA。在SNA的数据链路层规程采用了面向比特的规程SDLC。后来IBM将此规程提交美国国家标准协会ANSI和国际标准化组织ISO，建议能成为国家和国际标准。ANSI把SDLC修改为ADCCP作为美国国家标准，而ISO把SDLC修改后称为HDLC，译为高级数据链路控制，作为国际标准ISO3309。我国的相应国家标准是GB7496。CCITT则将HDLC再修改后称为链路接入规程LAP，并作为X.25建议书的一部分(即有关数据链路层协议的部分)。不久，HDLC的新版本又把LAP修改为LAPB，“B”表示平衡型(Balanced)，所以LAPB叫做平衡型链路接入规程。

上述这几个面向比特的链路规程均大同小异。ADCCP与HDLC没有多少区别。SDLC虽然最早提出，但它实际上是HDLC的一个子集。本节主要介绍HDLC控制规程的要点。

#### 4.5.2 HDLC 基本概念

HDLC涉及三种类型的站，即主站、从站和复合站。

主站的主要功能是发送命令(包括数据信息)帧、接收响应帧，并负责对整个链路的控制系统的初启、流程的控制、差错检测或恢复等。

从站的主要功能是接收由主站发来的命令帧，向主站发送响应帧，并且配合主站参与差错恢复等链路控制。

复合站的主要功能是既能发送，又能接收命令帧和响应帧，并且负责整个链路的控制。

在HDLC中，对主站、从站和复合站定义了三种链路结构，如图4-8所示。

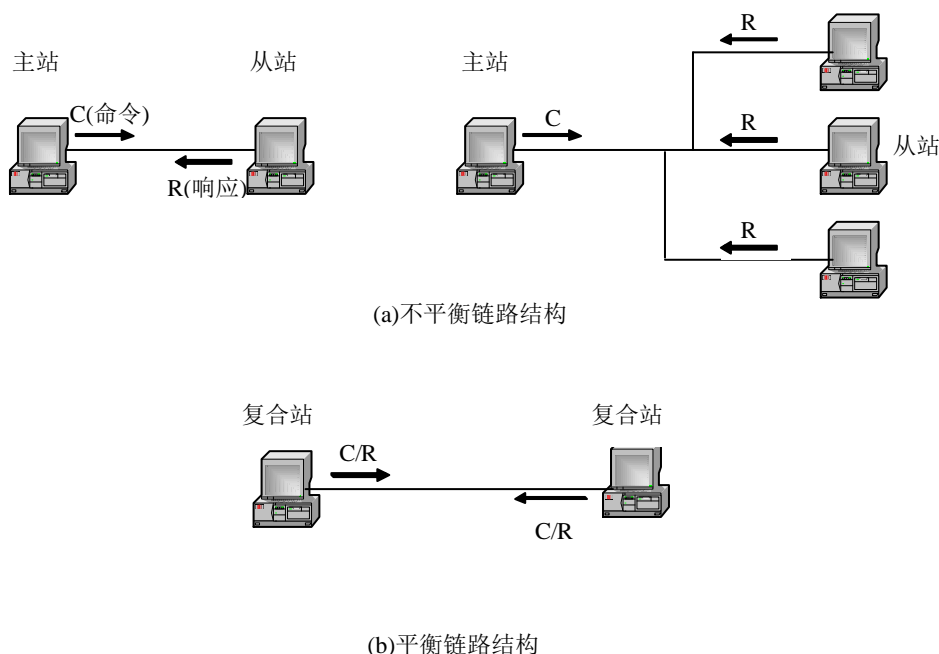


图 4-8 HDLC 链路结构类型

根据通信双方的链路结构和传输响应类型，HDLC 提供了三种操作方式：正常响应方式、异步响应方式和异步平衡方式。

- 正常响应方式（NRM）

正常响应方式（NRM）适用于不平衡链路结构，即用于点-点和点-多点的链路结构中，特



别是点-多点链路。这种方式中，由主站控制整个链路的操作，负责链路的初始化、数据流控制和链路复位等。从站的功能很简单，它只有在收到主站的明确允许后，才能发出响应。

● 异步响应方式（ARM）

异步响应方式（ARM）也适用于不平衡链路结构。它与 NRM 不同的是：在 ARM 方式中，从站可以不必得到主站的允许就可以开始数据传输。显然它的传输效率比 NRM 有所提高。

● 异步平衡方式（ABM）

异步平衡方式（ABM）适用于平衡链路结构。链路两端的复合站具有同等的能力，不管哪个复合站均可在任意时间发送命令帧，并且不需要收到对方复合站发出的命令帧就可以发送响应帧。ITU-T X.25 建议的数据链路层就采用这种方式。

除三种基本操作方式，还有三种扩充方式，即扩充正常响应方式（SNRM）、扩充异步响应方式（SARM）、扩充异步平衡方式（SABM）它们分别与基本方式相对应。

4.5.3 HDLC 的帧结构

在 HDLC 中，数据和控制报文均以帧的标准格式传送。HDLC 中的帧类似于 BSC 字符块，但 BSC 协议中的数据报文和控制报文是独立传输的，而 HDLC 中命令和响应以统一的格式按帧传输。完整的 HDLC 帧由标志字段 (F)、地址字段 (A)、控制字段 (C)、信息字段 (I)、帧校验序列字段 (FCS) 等组成，其格式如图 4-9 所示。

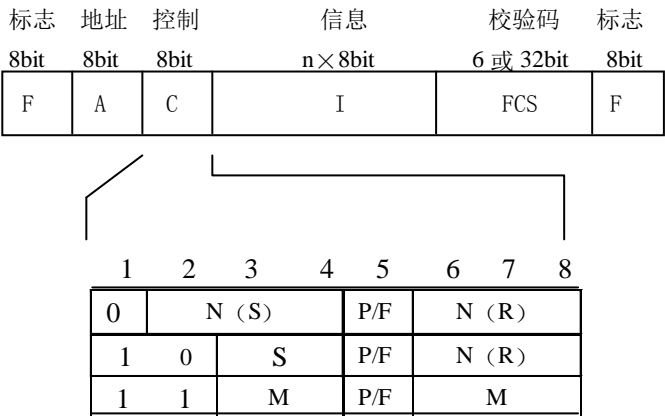


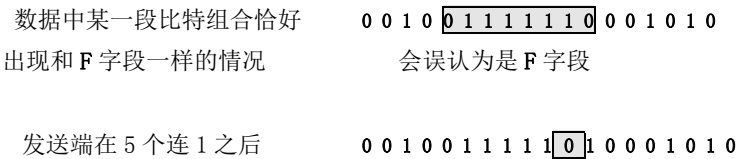
图 4-9 HDLC 的帧结构

1 各字段的意义

● 标志序列（F）

HDLC 指定采用 01111110 为标志序列，称为 F 标志。要求所有的帧必须以 F 标志开始和结束。接收设备不断地搜寻 F 标志，以实现帧同步，从而保证接收部分对后续字段的正确识别。另外，在帧与帧的空载期间，可以连续发送 F，用来作时间填充。

在一串数据比特中，有可能产生与标志字段的码型相同的比特组合。为了防止这种情况产生，保证对数据的透明传输，采取了比特填充技术。当采用比特填充技术时，在信码中连续 5 个“1”以后插入一个“0”；而在接收端，则去除 5 个“1”以后的“0”，恢复原来的数据序列，如图 4-10 所示。比特填充技术的采用排除了在信息流中出现的标志字段的可能性，保证了对数据信息的透明传输。



填入 0 比特再发送出去

填入 0 比特

在接收端将 5 个连 1 之后      0010 **01111110** 001010

图 4-10 比特填充

当连续传输两帧时，前一个帧的结束标志字段 F 可以兼作后一个帧的起始标志字段。当暂时没有信息传送时，可以连续发送标志字段，使接收端可以一直保持与发送端同步。

#### ● 地址字段 (A)

地址字段表示链路上站的地址。在使用不平衡方式传送数据时（采用 NRM 和 ARM），地址字段总是写入从站的地址；在使用平衡方式时（采用 ABM），地址字段总是写入应答站的地址。

地址字段的长度一般为 8bit，最多可以表示 256 个站的地址。在许多系统中规定，地址字段为“11111111”时，定义为全站地址，即通知所有的接收站接收有关的命令帧并按其动作；全“0”比特为无站地址，用于测试数据链路的状态。因此有效地址共有 254 个之多，这对一般的多点链路是足够的。但考虑在某些情况下，例如使用分组无线网，用户可能很多，可使用扩充地址字段，以字节为单位扩充。在扩充时，每个地址字段的第 1 位用作扩充指示，即当第 1 位为“0”时，后续字节为扩充地址字段；当第 1 位为“1”时，后续字节不是扩充地址字段，地址字段到此为止。

#### ● 信息字段 (I)

信息字段内包含了用户的数据信息和来自上层的各种控制信息。在 I 帧和某些 U 帧中，具有该字段，它可以是任意长度的比特序列。在实际应用中，其长度由收发站的缓冲器的大小和线路的差错情况决定，但必须是 8bit 的整数倍。

#### ● 帧校验序列字段 (FCS)

帧校验序列 FCS 字段共占 16 位。它采用的生成多项式是  $X^{16}+X^{12}+X^5+1$ ，即 CRC-CCITT。所校验的范围是从地址字段的第 1 个比特起，到信息字段的最末 1 个比特为止。图 4-11 标识出了这个校验范围。下面简单介绍 CRC 的工作原理，关于 FCS 具体的运算方法见有关通信教材。

利用 CRC 进行检错的过程可简单描述为：在发送端根据要传送的  $m$  位二进制码序列，以一定的规则产生一个校验用的  $k$  位监督码 (CRC 码)，附在原始信息后边，构成一个新的二进制码序列数共  $m+k$  位，然后发送出去。在接收端，根据信息码和 CRC 码之间所遵循的规则进行检验，以确定传送中是否出错。这个规则在差错控制理论中称为“生成多项式”。

设编码前的原始信息多项式为  $f(x)$ ，生成多项式为  $G(x)$ ， $G(x)$  的最高幂次等于  $k$ ，CRC 多项式为  $R(x)$ ；编码后的带 CRC 的信息多项式为  $T(x)$ 。发送方编码方法：将  $f(x)$  乘以  $x^k$  (即对应的二进制码序列左移  $k$  位)，再除以  $G(x)$ ，所得余式即为  $R(x)$ 。用公式表示为：

$$T(x) = x^k f(x) + R(x)$$

$G(x)$  为生成多项式； $R(x)$  为 CRC 多项式，存入 FCS 字段，由信息字段和 FCS 字段组成  $T(x)$ 。

接收方解码方法：将收到的  $T(x)$  除以  $G(x)$ ，如果余数为 0，则说明传输中无错误发生，否则说明传输有误。

举例来说，设信息码为 1100，生成多项式为 1011，即  $f(x)=x^3+x^2$ ， $G(x)=x^3+x+1$ ，计算 CRC 的过程为：

$$\begin{array}{r} x^3 f(x) \quad x^3(x^3+x^2) \quad x^6+x^5 \quad x \\ \hline G(x) \quad x^3+x+1 \quad x^3+x+1 \quad x^3+x+1 \end{array} = (x^3+x^2+x) + \frac{x}{x^3+x+1}$$

即  $R(x) = x$ 。注意到  $G(x)$  最高幂次  $k = 3$ ，得出 CRC 为 010

循环冗余码的产生与正确性检验例子。

已知：信息码：110011    信息多项式： $f(X) = X^5 + X^4 + X + 1$

生成码：11001    生成多项式： $G(X) = X^4 + X^3 + 1$  ( $k = 4$ )

解: 1) 发送端,  $x^k f(x) = (X^5 + X^4 + X + 1) * X^4$  的积是  $X^9 + X^8 + X^5 + X^4$  对应的码是 1100110000。  
2)  $x^k f(x) / G(X)$  (按模二算法)。

[illegible]

$$T(x) = x^k f(x) + R(x) = X^4 * (X^5 + X^4 + X + 1) + 1001 = 1100111001$$

3) 接收端, 接收码字: 1100111001, 即多项式:  $T(X) = X^9 + X^8 + X^5 + X^4 + X^3 + 1$   
用字码除以生成码, 余数为 0, 所以码字正确。

[illegible]

● 控制字段 (C)

控制字段 C 共 8Bit, 是最复杂的字段。HDLC 的许多重要功能都要靠控制字段来实现。从图 4-9 可见, 由于 C 字段的构成不同, 可以把 HDLC 帧分为三种类型: 信息帧、监控帧、无编号帧, 分别简称 I 帧(Information)、S 帧(Supervisory)、U 帧(Unnumbered)。

下面分别介绍这三种帧的特点。

## 2 信息帧

若控制字段的第 1 比特为 0, 则该帧为信息帧。I 帧用于数据传送, 它包含信息字段。在 I 帧控制字段中 b1~b3 比特为 N(S), b5~b7 比特为 N(R)。由于是全双工通信, 所以通信每一方都各有一个 N(S) 和 N(R)。这里要特别强调指出: N(R) 带有确认的意思, 它表示序号为 N(R)-1 以及在这以前的各帧都已经正确无误地收妥了。

为了保证 HDLC 的正常工作，在收发双方都设置两个状态变量  $V(S)$  和  $V(R)$ 。 $V(S)$  是发送状态变量，为发送 I 帧的数据站所保持，其值指示待发的一帧的编号； $V(R)$  是接收状态变量，其值为期望所收到的下一个 I 帧的编号。可见这两个状态变量的值确定发送序号  $N(S)$  和接收序号  $N(R)$ 。

在发送站, 每发送一个 I 帧,  $V(S) \rightarrow N(S)$ , 然后  $V(S)+1 \rightarrow V(S)$ 。在接收站, 把收到的  $N(S)$  与保留的  $V(R)$  作比较, 如果这个 I 帧可以接收, 则  $V(R)+1 \rightarrow N(R)$ , 回送到发送站, 用于对前面所收到的 I 帧的确认。  $N(R)$  除了可以用 I 帧回送之外, 还可以用 S 帧回送, 这一点从图 5-11 中可以看出, 在 I 帧和 S 帧的控制字段中具有  $N(R)$ 。

V(S)、V(R)和 N(S)、N(R)都各占 3bit，即序号采用模 8 运算，使用 0~7 八个编号。在有些场合，如卫星通信模 8 已经不能满足要求了，这时可以把控制字段扩展为两个字节，N(S)、N(R)和 V(S)、V(R)都用 7bit 来表示，即增加到模 128。

### 3 监控帧

若控制字段的第1~2比特为10，则对应的帧即为监督帧S。监控帧用于监视和控制数据链路，完成信息帧的接收确认、重发请求、暂停发送请求等功能。监控帧不具有信息字段。监控帧共有4种，表4-2是这4种监控帧的代码、名称和功能。

表 4-2 监控帧的名称和功能

记忆符	名 称	比特		功 能
		b <sub>2</sub>	b <sub>3</sub>	
RR	接收准备好	0	0	确认，且准备接受下一帧，已收妥 N(R) 以前的各帧
RNR	接收未准备好	1	0	确认，暂停接收下一帧，N(R) 含义同上
REJ	拒绝接收	0	1	否认，否认 N(R) 起的各帧，但 N(R) 以前的帧已收妥
SREJ	选择拒绝接收	1	1	否认，只否认序号为 N(R) 的帧

上面四种监控帧中，前三种用在返回 N 连续 ARQ 方法中，最后一种只用于选择重发 ARQ 方式中。

S 帧中没有包含用户的数据信息字段，它只有 48bit 长，显然不需要 N(S)，但 S 帧中 N(R) 特别有用，它具体含义随不同的 S 帧类型而不同。其中 RR 帧和 RNR 帧相当于确认信息 ACK，REJ 帧相当于否认信息 NAK。同时应当注意到，RR 帧和 RNR 帧还具有流量控制的作用，RR 帧表示已经作好表示接收帧的准备，希望对方继续发送，而 RNR 帧则表示希望对方停止发送（这可能是由于来不及处理到达的帧或缓冲器已存满）。

### 4 无编号帧

若控制字段的第1~2比特都是1时，这个帧就是无编号帧U。无编号帧用于数据链路的控制，它本身不带编号，可以在任何需要的时刻发出，而不影响带编号的信息帧的交换顺序。它可以分为命令帧和响应帧。用5个比特位（即 M<sub>1</sub>、M<sub>2</sub>）来表示不同功能的无编号帧。HDLC 所定义的无编号帧名称和代码见表 4-3。

表 4-3 无编号帧的名称和代码

记忆符	名 称	类型		M <sub>1</sub>	M <sub>2</sub>
		命令	响应	b <sub>3</sub> b <sub>4</sub>	b <sub>6</sub> b <sub>7</sub> b <sub>8</sub>
SNRM	置正常响应模式	C		0 0	0 0 1
SARM/DM	置异步响应模式/断开方式	C	R	1 1	0 0 0
SABM	置异步平衡模式	C		1 1	1 0 0
SNRME	置扩充正常响应模式	C		1 1	0 1 1
SARME	置扩充异步响应模式	C		1 1	0 1 0
SABME	置扩充异步平衡模式	C		1 1	1 1 0
DISC/RD	断链/请求断链	C	R	0 0	0 1 0
SIM/RIM	置初始化方式/请求初始化方式	C		1 0	0 0 0
UP	无编号探询	C		0 0	1 0 0
UI	无编号信息	C		0 0	0 0 0
XID	交换识别	C	R	1 1	1 0 1
RESET	复位	C		1 1	0 0 1
FRMR	帧拒绝		R	1 0	0 0 1
UA	无编号确认		R	0 0	

下面介绍几种最常用的无编号帧的用途。

在主站 A 与次站 B 和 C 交换信息之前必须有一个建立数据链路的阶段，而在数据传送完毕后，必须有一个数据链路释放阶段，或称为数据链路拆除阶段。在图 4-11 画出了这两个阶段所用的无编号帧的情况。

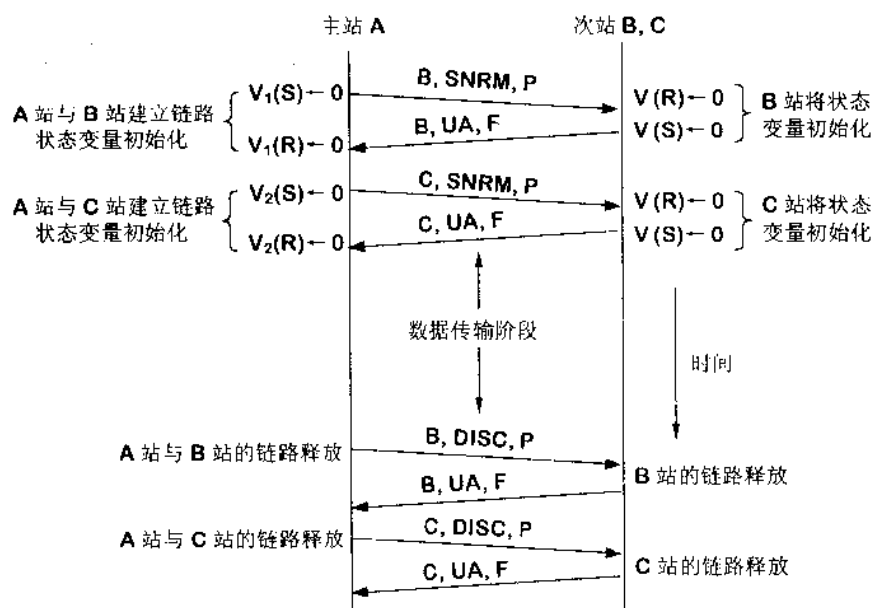


图 3-17 多点链路的建立和释放

图 4-11 多点链路的建立和释放

主站 A 先向次站 B 发出置正常响应方式 SNRM(setNRM)的命令，并将 P 置 1，要求 B 站做出响应。B 站同意建立链路后，发送无编号确认 UA(Unnumbered Acknowledgment)的响应，将 F 置 1。A 站和 B 站在将其状态变量  $V(S)$  和  $V(R)$  进行初始化(通常就是置 0)后，就完成了数据链路的建立。

接着，A 站开始建立与 C 站的链路连接。因此，A 站还需要再设置与 C 通信的状态变量  $V_2(S)$  和  $V_2(R)$ 。同理，C 站也要将自己的状态变量初始化。待双方的状态变量都初始化完毕后，轮询将就可开始。

当数据通信完毕后，A 站应分别向 B 站和 C 站发出断连命令 DISC(DISConnect)。当 B 站和 C 站用无编号确认帧 UA 响应后，数据链路的断连阶段即告结束。请注意，“断连”是指将逻辑链路而不是将物理链路断开。

图 4-12 为点对点链路中两个站都是复合站(即每个站都包括一个主站和一个次站)的情况。复合站中的一个站先发出置异步平衡方式 SABM(setABM)的命令。待对方回答一个无编号响应帧 UA 后，即完成链路的建立阶段。由于现在两个站平等，所以任何一个站均可在数据传送完毕后提出断连的要求(即发出 Disc 命令)。在对方用无编号确认帧 UA 回答后，链路的断连阶段就结束了。应注意到，现在是 B 站发出断链命令，要 A 站做出响应，因此这时在 B 站发出的断链命令的地址字段中应写入 A 站的地址。

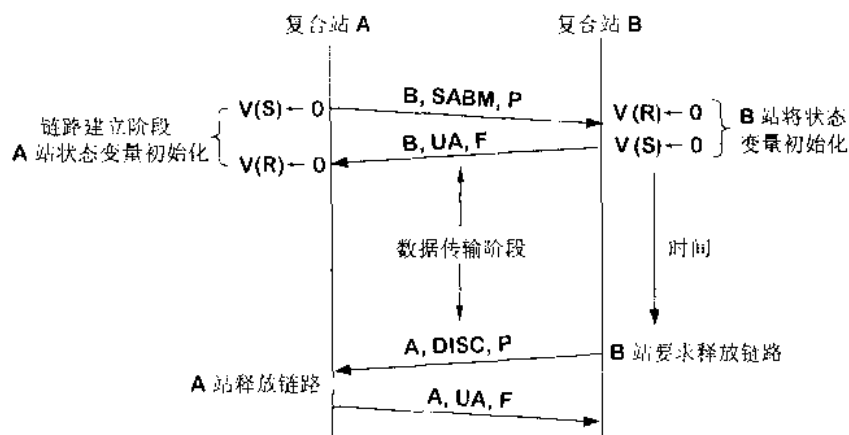


图 3-18 复合站的链路建立和断连

图 4-12 复合站链路的建立和释放

无编号帧中的控制字段没有扩展方式。也就是说，无编号帧的控制字段都是 8 位长。但是无编号帧却有三个帧与扩展方式有关：这三个帧与置正常响应方式 SNRM，置异步平衡方式 SABM 以及置异步响应方式 SARM 这三个无编号帧相对应，即置扩展的正常响应方式 SNRME、置扩展的异步平衡方式 SABME 和置扩展的异步响应方式 SARME。但是，最后一个命令用得不多。

还有一个无编号帧很有用，叫帧拒绝 FRMR (FRAME REJECT)。FRMR 是个响应帧，用来表示通过重发同一个帧仍不能纠正的差错 (注意：这时所收到的帧的循环冗余校验还是正确的)。例如，收到了没有指明的或实现不了的命令、收到了无效的控制字段、数据字段过长、收到了无效的 N(R) (即此 N(R) 所确认的帧对方尚未发出)、收到了长度有错误的监督帧或无编号帧等等。无编号帧 FRMR 有 3 或 5 个字节的信息字段，用以说明发送此帧的原因。

还有一些其他的无编号帧，这里不再一一进行介绍了。

最后要指出，一般的应用极少需要使用 HDLC 的全集。因此，HDLC 按照数据的三种不同传送方式，给出了相应的三种基本的命令响应子集和 14 个扩展的功能选项，供不同的用户选择。当使用某一家厂商的 HDLC 时，一定要弄清该厂商所选用的子集是什么。

## 5 P / F 比特

信息帧、监督帧、无编号帧的第 5 比特都是 P / F 比特。若 P / F 值为零，则 P / F 比特并没有什么意义，只有当 P / F 比特的值为 1 时才具有意义。但需要注意：在不同的数据传送方式中，P / F 比特的用法是不一样的。在说明帧的传送过程中，为了更清楚地表示 P / F 比特的作用，往往将它写为 P 比特或 F 比特。下面简单说明其作用。

在非平衡配置的正常响应方式 NRM 中，次站不能主动向主站发送消息。次站只有收到主站发出的 P 比特为 1 的命令帧 (S 帧或 I 帧) 以后才能发送响应帧。若次站有数据发送，则在最后一个数据帧中将 F 比特置 1。若无数据发送，则应在回答的 S 帧中将 F 比特置 1。

在非平衡配置的异步响应方式 NRM 或在平衡配置的异步平衡方式 ABM 中，任何一个站都可以在主动发送的 S 帧和 I 帧中将 P 比特置 1。对方站收到 P=1 的帧后，应尽早地回答本站的状态并将 F 比特置 1，不过此时并不表示数据已发完和不再发送数据了。

下面结合图 4-13 的例子具体说明 P / F 比特的使用方法。在图中主站 A 与次站 B 和 C 连成多点链路。我们将所传送的帧的一些主要参数按照“地址，帧名和序号，P / F”的先后顺序标注在图中。这里的“地址”是指地址字段中应填入的站地址，“帧名”是指帧的名称，如 RR 或 I，而序号则是指监督帧中的 N(R) 或信息帧中的 N(S)N(R)。P / F 是在当 P / F 为 1 时才写上 P 或 F，表明此时控制字段的第 5 比特为 1。

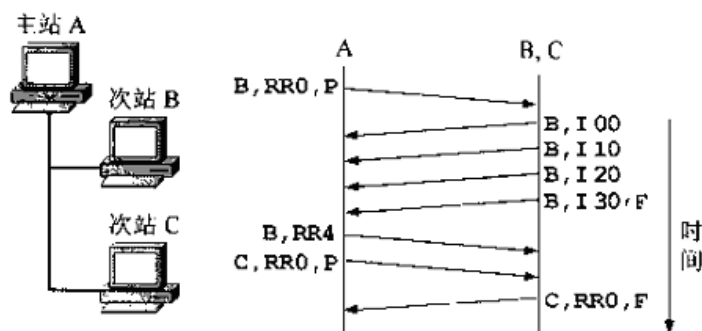


图 4-13 非平衡配置中 P/F 比特的使用方法

主站 A 先询问 B 站：“B 站，若有信息，请即发送。”这时 A 站发送的帧是 RR 监督帧，并将  $N(R)$  置 0，表示期望收到对方的 0 号帧。因此在图 4-17 中将这样的帧记为“B, RR0, P”。对主站的这一命令，B 站响应以连续 4 个信息帧，其序号  $N(S)$  从 0 到 3。最后在第 4 个信息帧中将 P / F 置为 1，表示“我要发送的信息已发完。”这个帧在图 4-17 中记为“B、130、F”。在图中的某一帧标注的参数最后出现 P 或 F 时，就表示在实际传送的帧中都是控制字段中的第 5 比特为 1。

应注意到， $P=1$  表示的“询问”带有强制性质，即对方（在复合站通信的情况下对方不一定是次站）必须立即回答。如在图 3-17 中，A 站收到 B 站发来的 4 个信息帧后，发回确认帧 RR4（这时  $N(R)=4$ ）。我们注意到这时 P / F 比特并未置 1，所以 B 站收到 RR4 后不必应答。相反，接下去 A 轮询 C 站， $P=1$ 。虽然这时 C 站没有数据发送，但也必须立即应答。C 站应答也是 RR 帧，表示目前没有信息帧发送， $F=1$  表明这是回答对方命令的一个响应。

有了 P / F 比特，使 HDLC 规程使用起来更加灵活。在两个复合站全双工通信时，任何一方都可随时使  $P=1$ 。这时对方就要立即回答 RR 帧，并置  $F=1$ 。这样做可以更早地收到对方的确认。如果不使用 P / F 比特，则接收方不一定马上发出确认帧。接收方可以在发送自己的信息帧时，在某一个信息帧中捎带把确认信息发出（利用  $N(R)$ ）。为了更好地理解信息帧和监督帧中控制字段的作用，在图 4-14 中画出了两个复合站进行全双工通信的例子。注意搞清每一帧旁边所标符号的意思。

A 站发第 1 个信息帧中  $N(S)N(R)=00$ ，因此我们记为 I00。后面加上 P 表示这时将 P 置 1，其目的是想尽快了解链路的通信状况。A 站发送的信息帧都是命令帧，因此地址填的是接收站的地址。A 站将此帧和下一帧 I10 发完时，还没有收到 B 站发来的头一个信息帧，因此 A 站发的第 3 帧 ( $N(S)=2$ ) 中的  $N(R)$  仍为 0。B 站发送的 2 号帧 122 传丢了，超时再重发时变成了 I26，这是因为在收到 A 站的  $N(S)=5$  的信息帧后将接收状态变量的值更新了。

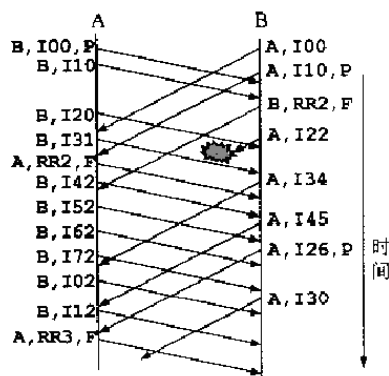


图 4-14 两个复合站全双工通信



## 4.6 Internet 的数据链路层协议 — PPP

### 4.6.1 PPP协议概述

在提及 PPP 协议时，不可不提及它的老祖宗 SLIP (Serial Line Internet Protocol) 协议。虽然它已被淡忘在历史的长河中，但毕竟有过辉煌的日子。它曾经主载了 Internet 半边江山，人们不仅可以通过在计算机上安装该协议实现浏览 Internet 的梦想，而且还可以互连许多网络设备（如路由器与路由器的互连、路由器与主机的互连和主机与主机的互连）。随着网络技术的不断日新月异，特别是计算机技术的发展，人们开始渐渐认识到使用 SLIP 协议已不能满足日益增长的网络需求，如何在串行点对点的链路上封装 IPX、AppleTalk 等网络层的协议呢？这就给网络专家提出了新的挑战，也为 PPP 协议的出现提供了契机，PPP 由于自身的诸多的优点已成为目前被广泛使用的数据链路层协议。

#### 1 SLIP 协议的基本概念

SLIP 协议出现在 80 年代中期，并被使用在 BSD UNIX 主机和 SUN 的工作站上，因为 SLIP 简单好用，所以后来被大量使用在线路速率从 1200Bps 到 19.2KBps 的专用线路和拨号线路上互连主机和路由器，到目前为止仍有大部分 UNIX 主机保留对该协议的支持。在 80 年代末 90 年代初期，被广泛用于家庭中每台有 RS232 串口的计算机和调制解调器连接到 Internet。SLIP 是一种在点对点的串行链路上封装 IP 数据报的简单协议，它并非是 Internet 的标准协议。

#### 2 SLIP 协议的封装格式

SLIP 协议的封装格式必需遵循以下几条原则：

1) 通过在被发送 IP 数据报的尾部增加特殊的 END 字符 (0xC0) 从而形成一个简单的 SLIP 的数据帧，而后该帧会被传送到物理层进行发送。为了防止线路噪声被当成数据报的内容在线路上传输，通常发送端在被传送数据报的开始处也传一个 END 字符。如果线路上的确存在噪声，则该数据报起始位置的 END 字符将结束这份错误的报文，这样当前正确的数据报文就能正确的传送了，而前一个含有无意义报文的数据帧会在对方的高层被丢弃。

2) 当被传送的 IP 数据报文中含有 END 字符时，则需要对该字符进行转义（就是使用其它字符来表示），可使用连续传输的两个字节来代替它（如 0xdb 和 0xdc）。如果当被转义后的字符也包含在数据报中，则也需要对其进行同样的操作，直至不出现歧义为止。图 4-15 为 SLIP 数据帧的封装格式。

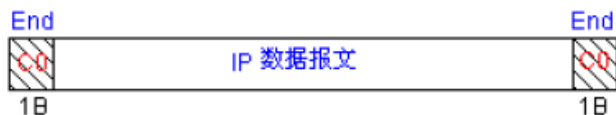


图 4-15 SLIP 数据帧的封装格式

SLIP 简单封装方式的缺陷：从上图 4-15 可以看出 SLIP 帧的封装格式非常简单，通信双方无需在数据报发送前协商任何配置参数选项（在 PPP 协议中需协商配置参数选项），所以双方 IP 层通信前必需先获知对方的 IP 地址，才能进行网络层的通信，否则数据链路层发送的数据帧在被送到对方网络层时将无法进行转发；由于数据帧中也没有类似于 HDLC 和 PPP 数据链路层协议中定义的协议域字段，因此 SLIP 仅支持一种网络层协议（IP 协议）同一时刻在串行链路上发送；SLIP 协议没有在数据帧的尾部加上 CRC 校验和，如果由于线路噪声的干扰影响传送数据包的内容是无法在对方的数据链路层中发现的，必须交由上层的应用软件来处理。正是由于这些缺点，导致了 SLIP 很快的被 PPP 协议所替代。

### 3 PPP 协议简介

PPP 提供了一种在点对点的链路上封装多协议数据报（IP、IPX 和 AppleTalk）的标准方法。它不仅能支持 IP 地址的动态分配和管理、同步（面向位的同步数据块的传送）或异步（起始位+数据位+奇偶校验位+停止位）物理层的传输、网络层协议的复用、链路的配置、检测和纠错，而且还支持多种配置参数选项的协商。PPP 协议主要包括三部分：LCP（Link Control Protocol）链路控制协议、NCP（Network Control Protocol）和 PPP 的扩展协议。随着网络技术的不断发展，网络带宽已不再是瓶颈，所以 PPP 扩展协议的应用也就越来越少，因此往往人们在叙述 PPP 协议时经常会忘记它的存在。而且大部分教材上将 PPP 的认证也作为 PPP 协议的一个主要部分，实际上这是一个错误概念的引导。PPP 协议默认是不进行认证配置参数选项的协商，它只作为一个可选的参数，当点对点线路的两端需要进行认证时才需配置。当然在实际应用中这个过程是不可忽略的，例如我们使用计算机上网时，需要通过 PPP 协议与 NAS 设备互连，在整个协议的协商过程中，我们需要输入用户名和密码。因此当别人说 PPP 协议主要包括 LCP、认证和 NCP 协议三个部分时，你不要认为他的说法有误，而只是不够准确罢了。

#### 4.6.2 PPP协议的封装格式

ISO 参考模型共分七层，自下而上分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。通常依据协议所完成的功能将它与这七层进行对照，PPP 协议就属于数据链路层协议。PPP 协议的封装方式都是基于 HDLC 的封装格式的，采用了 HDLC 的定界帧格式。图 4-16 为 PPP 数据帧的封装格式。

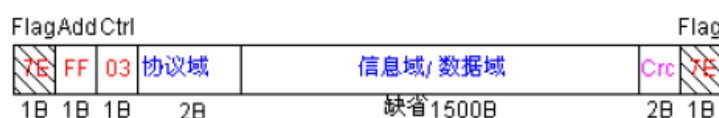


图 4-16 PPP 数据帧的格式

对PPP数据帧封装格式作以下几点说明：

每一个 PPP 数据帧均是以一个标志字节起始和结束的，该字节为 0x7E。

紧接在起始标志字节后的一个字节是地址域，该字节为 0xFF。我们熟知网络是分层的，且对等层之间进行相互通信，而下层为上层提供服务。当对等层进行通信时首先需获知对方的地址，而对不同的网络，在数据链路层则表现为需要知道对方的 MAC 地址、X.121 地址、ATM 地址等；在网络层则表现为需要知道对方的 IP 地址、IPX 地址等；而在传输层则需要知道对方的协议端口号。例如如果两个以太网上的主机希望能够通信的话，首先发送端需获知对端的 MAC 地址。但由于 PPP 协议是被应用在点对点的链路上的特殊性，它不像广播或多点访问的网络一样，因为点对点的链路就可以唯一表示对方，因此使用 PPP 协议互连的通信设备的两端无须知道对方的数据链路层地址，所以该字节已无任何意义，按照协议的规定将该字节填充为全 1 的广播地址。

同地址域一样，PPP 数据帧的控制域也没有实际意义，按照协议的规定通信双方将该字节的内容填充为 0x03。

对 PPP 协议本身而言，最关心的内容应该是它的协议域和信息域。协议域可用来区分 PPP 数据帧中信息域所承载的数据报文的内容。协议域的内容必须依据 ISO 3309 的地址扩展机制所给出的规定。该机制规定协议域所填充的内容必须为奇数，也即是要求低字节的最低位为“1”，高字节的最低位为“0”。如果当发送端发送的 PPP 数据帧的协议域字段不符合上述规定，则接收端认为此数据帧是不可识别的，那么接收端向发送端发送一个 Protocol-Reject 报文，在该报文尾部将完整地填充被拒绝的报文。协议域的具体取值如表 4-4 所示。

表 4-4 PPP 数据帧的协议域取值含义：

	协议域类型	说明
<b>ISO 标 准</b>	0x0*** - 0x3***	信息域中承载的是网络层的数据报文
	0x4*** - 0x7***	信息域中承载的是与NCP无关的低整流量
	0x8*** - 0xb***	信息域中承载的是网络控制协议（NCP）的数据报文
	0xc*** - 0xf***	信息域中承载的是链路控制协议（LCP）的数据报文
<b>最典 型的 几种 取值</b>	0xc021	信息域中承载的是链路控制协议（LCP）的数据报文
	0xc023	信息域中承载的是PAP协议的认证报文
	0xc223	信息域中承载的是CHAP协议的认证报文
	0x8021	信息域中承载的是网络控制协议（NCP）的数据报文
	0x0021	信息域中承载的是IP数据报文

说明：协议域类型中的\*号表示可从（0-F）中任意取值。

信息域缺省时最大长度不能超过1500字节，其中包括填充域的内容（在图4-20中并未表示，因为它属于信息域的一部分），1500字节大小等于PPP协议中配置参数选项MRU（Maximum Receive Unit）的缺省值，在实际应用当中可根据实际需要进行信息域最大封装长度选项的协商。信息域如果不足1500字节时可被填充，但不是必须的，如果填充则需通信双方的两端能辨认出有用与无用的信息方可正常通信。通常在通信设备的配置过程中，遇到最多的也是MTU（Maximum Transmit Unit）。对于一个设备而言，它网络的层次均使用MTU和MRU两个值，一般情况下设备的MRU会比MTU稍大几个字节，但这需根据各厂商的设备而定。

CRC校验域主要是对PPP数据帧传输的正确性进行检测。

### 4.6.3 LCP协议数据报文的封装格式

LCP数据报文是在链路建立阶段被交换的，它作为PPP的净载被封装在PPP数据帧的信息域中，此时PPP数据帧的协议域固定填充0xC021，但在链路建立阶段的整个过程中信息域的内容是在变化的，它包括很多种类型的报文，所以这些报文也要通过相应的字段来区分。LCP数据报文的一般封装格式如下图4-17所示。

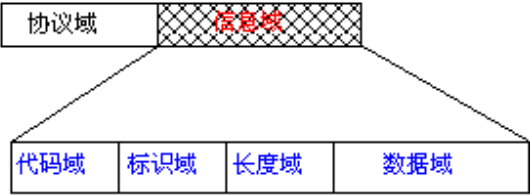


图 4-17 LCP 数据报文的格式

代码域的长度为一个字节，主要是用来标识LCP数据报文的类型的。在链路建立阶段时，接收方收到LCP数据报文的代码域无法识别时，就会向对端发送一个LCP的代码拒绝报文（Code-Reject报文）。根据RFC的规定，LCP共包括表4-5所示几种类型的数据报文：

表4-5 LCP数据报文类型表

代码值	报文类型	代码	报文类型
0x01	Config-Request	0x07	Code-Reject
0x02	Config-Ack	0x08	Protocol-Reject
0x03	Config-Nak	0x09	Echo-Request
0x04	Config-Reject	0x0A	Echo-Reply
0x05	Terminate-Request	0x0B	Discard-Request
0x06	Terminate-Ack	0x0C	Reserved

标识域也是一个字节，其目的是用来匹配请求和响应报文。一般而言在进入链路建立阶段时，通信双方无论哪一端都会连续发送几个配置请求报文（Config-Request报文），而这几个请求报文的数据域可能是完全一样的，仅仅是它们的标志域不同罢了。通常一个配置请求报文的ID是从0x01开始逐步加1的，当对端接收到该配置请求报文后，无论使用何种报文（回应报文可能是Config-Ack、Config-Nak和Config-Reject三种报文中的一种）来回应对方，但必须要求回应报文中的ID要与接收报文中的ID一致，当通信设备收到回应后就可以将该回应与发送时的报文进行比较来决定下一步的操作。例如：假设点对点通信的一端发送了一个Config-Request报文，报文内容如下：“7E FF 03 C0 21 01 01 00 17 02 06 00 0A 00 00 05 06 00 0B 42 CB 07 02 08 02 0D 03 06 7E”，从报文中可以看出这个配置请求报文包括5个配置参数选项。当对端正确接收到了该报文后，应该回应一个Config-Ack报文，报文内容如下：“7E FF 03 C0 21 02 01 00 17 02 06 00 0A 00 00 05 06 00 0B 42 CB 07 02 08 02 0D 03 06 7E”，该报文中唯一修改的内容就是代码域（02表示是Config-Ack报文），标识域与原报文中的一样。

长度域的内容 = 总字节数据（代码域+标志域+长度域+数据域）。长度域所指示字节数之外的字节将被当作填充字节而忽略掉，而且该域的内容不能超过MRU的值。

数据域的内容依据不同LCP数据报文的内容也是不一样的。

#### 4.6.4 NCP协议

NCP协议的数据报文是在网络层协议阶段被交换的，在这个阶段所需的一些配置参数选项协商完后，就可以进行网络层的通信，也即是在点对点的链路上可以开始传送网络层的数据报文了。NCP协议主要包括IPCP、IPXCP等，在实际中最常用IPCP协议，如果对IPXCP网络控制协议有兴趣，则可参见RFC1552。

IPCP控制协议主要是负责完成IP网络层协议通信所需配置参数的选项协商的。IPCP在运行的过程当中，主要是完成点对点通信设备的两端动态的协商IP地址。依据两端设备的配置选项可将IPCP的协商过程分为“静态”和“动态”。何为静态，何为动态，这是一个相对的概念。IPCP的数据的报文与LCP的数据报文非常类似，只不过一个是在网络层协议阶段协商配置参数选项，而LCP协议则是在链路建立阶段协商配置参数选项的。除此之外是两者在所使用报文上的相似之处，我们知道LCP共包括十几种报文，而IPCP也包括多种报文，但它的报文类型只是LCP数据报文的一个子集（只有LCP代码域从1到7这七种报文），而且实际的数据报文交换过程中也仅涉及以下几种：Config-Request、Config-Ack、Config-Nak和Config-Reject（代码域从1到4，而链路终止报文一般而言是不在网络协议阶段使用的，而且也是不需要的）。以下具体介绍一下IPCP控制协议的静态和动态的两个过程，实际上两者的区分是在于互连设备IP地址的获取过程。

**静态协商**，也即是不协商。点对点的通信设备两端在PPP协商之前已配置好了IP地址，所以就无须在网络层协议阶段协商IP地址，而双方唯一要做的就是告诉对方自身的IP地址。在IPCP控制协议完成整个配置的过程时，理想的情况将会看到如图4-18所示的四种报文，而无其它报文再被发送。

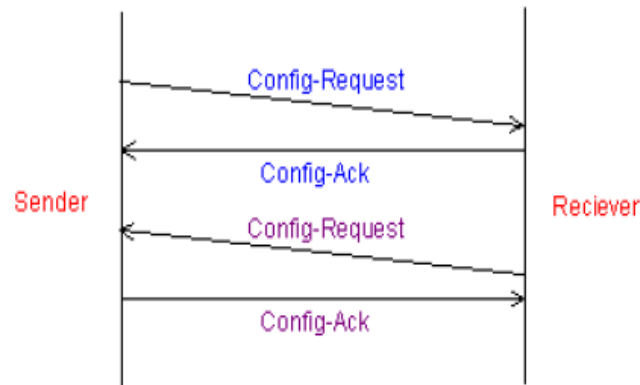


图4-18 静态协商

在静态协商时，如果IPCP的Config-Request报文中只含有地址配置参数选项时（实际中可能还会附带其它配置参数选项，这些配置参数选项的协商与LCP阶段的一样，而这里只提到了IP地址配置参数选项），无论是发送方还是接收方都同时发送Config-Request报文，其中配置选项中只含有各自的IP地址。当对端收到该报文后，会发送一个Config-Ack报文，这个目的是告诉对端已经知道了你的IP地址，对路由器而言会增加一条到对端接口的主机路由。刚进入网络层协议阶段时，IPCP的状态机是initial的，但当完成了上述的整个过程后，IPCP的状态机改变为Opened，双方也就可以开始网络层数据网的传送了。IPCP协议中并未规定，当一端接收到Config-Request报文后，它从报文的配置参数选项中可获知对端的IP地址，但并不与本端的IP地址进行比较。我们也知道，一般而言点对点的两端应该是在一个网段。但如果双方的地址不在一个网段，就不给对方回应Config-Ack报文，而是无条件的回送一个回应报文。因此说点对点通信的两端如果是手动设置每一端的IP地址时，无须双方地址在同一网段。

例如：假设IPCP在网络层协议阶段开始协商配置参数选项（这里只举协商IP地址的配置参数选项地的过程），发送方设置IP地址为192.168.0.1，接收方设置IP地址为192.168.0.2，发送方发送给Config-Request报文内容如下：

7E FF 03 80 21 01 01 00 0A 03 06 C0 A8 00 01 7E

在这个例子中我们能看见明显的改变之处再于PPP协议域字段由原先的0xC021改变为0x8021，下划线的部分表示本端的IP地址。

当对端正确接收到了该报文后，应该回应一个Config-Ack报文，报文内容如下：

7E FF 03 80 21 02 01 00 0A 03 06 C0 A8 00 01 7E

同样的接收方给发送方也发送一个Config-Request报文内容如下，但此时报文中IP地址配置参数选项的值为本端的IP地址（192.168.0.2）：

7E FF 03 80 21 01 01 00 0A 03 06 C0 A8 00 02 7E

发送方回应一个Config-Ack报文给接收方，报文内容如下：

7E FF 03 80 21 02 01 00 0A 03 06 C0 A8 00 02 7E

**动态协商**，也即是一端配置为动态获取IP地址，另一端通过手动方式配置IP地址，且允许给对端分配IP地址，这个过程实际上可与窄带拨号上网的过程相一致，计算机中的拨号网络适配器是采用动态获取IP地址的方式。



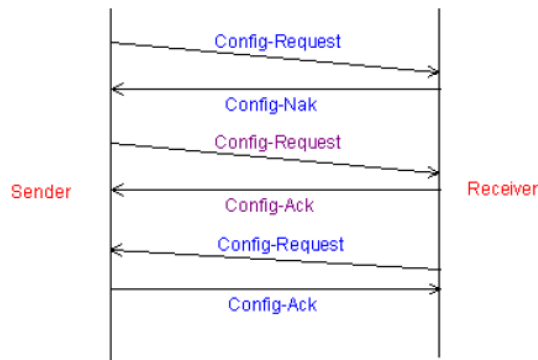


图4-19 动态协商

图4-19中可以看出发送方连续发送了两次Config-Request报文，才能完成发送方的协商过程。而接收方仍然只需要发送一次Config-Request即可完成本端的协商过程。由于发送方没有配置IP地址（而是动态获取IP地址），所以在IPCP的Config-Request报文的IP地址配置参数配置选项中的IP地址填充全0（也即是0.0.0.0），这样当对端收到这个Config-Request报文时，当接收方收到该配置请求报文后会检测IP地址的内容，如果发送为全0，则认为对端的这个IP地址不是所希望的值，这样就回应一个Config-Nak报文，并将希望分配给对方的IP地址填充到Config-Nak报文内。这时当接收方收到Config-Nak报文后，就会重新发送一个Config-Request报文，这个报文中的IP地址配置选项为对方在Nak报文中所提供的。接收方IP地址的配置过程与静态时的一样，只需发送一个Config-Request报文即可，当收到发送方的Config-Ack报文，就表示接收方的IP地址配置完成。

例如：假设IPCP在网络层协议阶段开始协商配置参数选项（这里只举协商IP地址的配置参数选项地的过程），发送方没有配置IP地址，而接收方配置了IP地址为192.168.0.2，接收方可给发送方分配IP地址（192.168.0.1），发送方发送给接收方的Config-Request报文内容如下：

7E FF 03 80 21 01 01 00 0A 03 06 00 00 00 00 7E

有下划线的部分表示本端的IP地址。

当对端正确接收到了该报文后，应该回应一个Config-Nak报文，报文内容如下：

7E FF 03 80 21 03 01 00 0A 03 06 C0 A8 00 01 7E

当接收方收到该报文后，重新发送一个Config-Request报文，报文内容如下：

7E FF 03 80 21 01 02 00 0A 03 06 C0 A8 00 01 7E

接收方再次收到发送方的一个Config-Request报文，此时将回应一个Config-Ack报文，报文内容如下：

7E FF 03 80 21 02 02 00 0A 03 06 C0 A8 00 01 7E

仔细观察一下这些报文在交互过程中，PPP数据帧内的数据报文的类型域和报文ID。

同样的接收方给发送方也发送一个Config-Request报文，报文内容如下：

7E FF 03 80 21 01 01 00 0A 03 06 C0 A8 00 02 7E

发送方应回送一个Config-Ack给接收方，报文内容如下：

7E FF 03 80 21 02 01 00 0A 03 06 C0 A8 00 02 7E

本节只是将IPCP配置参数选项配置过程中最关键的部分做了一些说明，如果想深入了解IPCP或IPXCP，可参见相关的RFC文档。

#### 4.6.5 PPP扩展协议

ISDN可以在两个系统之间提供2B+D和30B+D多通道捆绑能力，为用户能够提供更多可用的带宽。许多链路捆绑功能需要软件和硬件的协同工作，更多的基于硬件来实现的。然而我们

是否考虑过仅仅通过软件的实现来完成链路捆绑的功能，同时还考虑到很多实际链路的情况，对于软件在实现过程中还要能对不同速率的链路进行捆绑。我们可以通过在发送数据之前增加一定数据的字节头，其中含有为重组数据而所需的一些字段。

随着PPP的广泛应用，Multilink Protocol (MP) 作为PPP功能扩展协议应运而生。它可为用户提供更大的带宽，实现数据的快速转发。同时，还可实现对链路资源进行动态分配，有效的利用宝贵的资源。但随着网络技术的发展，网络的带宽已不再是瓶颈，所以对于使用PPP扩展协议已没有实际意义，本节中简单做一下介绍，如果想进一步了解该协议，可参考相应的RFC1717。

Multilink Protocol的协商较为特殊。MP配置参数选项的协商是在LCP协商过程中完成的，协商MP配置参数选项的目的完成以下几个过程：

- 1 表明系统是否支持将多个物理链路捆绑成一个逻辑链路。
- 2 系统在多链路上接收到了对端发送的数据单元后，能够通过附加在这些数据之前的重组字段对这些分段的数据单元进行重组。
- 3 逻辑链路为了能够提高传输的效率，可以不使用单一PPP物理链路上的最大接收单元，可以重新协商新的逻辑链路上使用的最大接收单元进行数据报文的发送和接收。

MP协议可以用来灵活的调整点对点系统之间的多条独立物理链路，它可为整个系统提供一个虚拟链路，虚拟链路的带宽是N个链路的捆绑之和（ $N \geq 1$ ）。