计算机网络技术讲义

第 1 章　计算机网络概论

前言：人类社会已进入信息时代；世界各国积极建设信息高速公路；计算机网络是信息高速公路的基础；　Internet 最终改变我们的生活方式，人类进入网络文化时代。

1.1 计算机网络的定义、演变和发展

1.1.1 计算机网络的定义

计算机网络：就是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式、网络操作系统等）实现网络中资源共享和信息传递的系统。

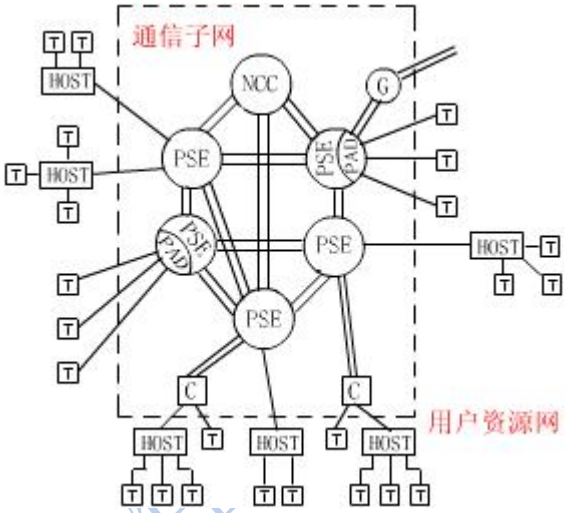


图 1.1 一个典型的计算机网络示例

计算机网络：资源子网＋通信子网
资源子网：主机 Host＋终端 Terminal
通信子网：通信链路组成
网络节点：分组交换设备 PSE、分组装 / 卸设备 PAD、集中器 C、网络控制中心 NCC、网间连接器 G。统称为接口住处处理机 IMP。

1.1.2 计算机网络的演变和发展

网络发展三阶段：面向终端的网络；计算机－计算机网络；开放式标准化网络。

1.面向终端的计算机网络

以单个计算机为中心的远程联机系统，构成面向终端的计算机网络。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 50 年代初美国的 SAGE 系统。

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。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。

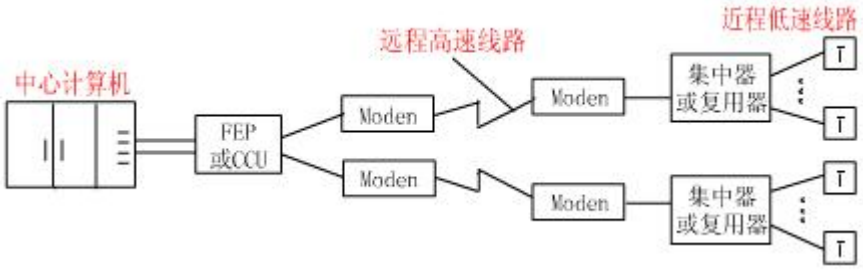


图 1.2 单计算机为中心的远程联机系统

2.计算机－计算机网络

60 年代中期，出现了多台计算机互连的系统，开创了“计算机－计算机”通信时代，并存多处理中心，实现资源共享。美国的 ARPA 网，IBM 的 SNA 网，DEC 的 DNA 网都是成功的典例。这个时期的网络产品是相对独立的，未有统一标准。

3.开放式标准化网络

由于相对独立的网络产品难以实现互连，国际标准化组织 ISO(Internation Standards Organization)于 1984 年颁布了一个称为“开放系统互连基本参考模型”的国际标准 ISO 7498，简称 OSI/RM。即著名的 OSI 七层模型。从此，网络产品有了统一标准，促进了企业的竞争，大大加速了计算机网络的发展。

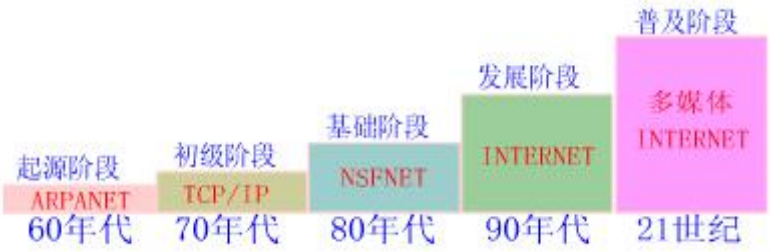
1.1.3 计算机网络实例简介

1.因特网(Internet)

1969 年--ARPANET，ARM 模型，早于 OSI 模型，低三层接近 OSI，采用 TCP/IP 协议。

1988 年--NSFNET ，OSI 模型，采用标准的 TCP/IP 协议，成为 Internet 的主干网。

两种服务公司：进入因特网产品服务公司 ISP，因特网信息服务公司 ICP。



2.公用数据网 PDN(Public Data Network)

计算机网络中负责完成节点间通信任务的通信子网称为公用数据网。如英国的 PSS、法国的 TRANSPAC、加拿大的 DATAPAC、美国的 TELENET、欧共体的 EURONET、日本的 DDX-P 等都是公用数据网。我国的公用数据网 CHINAPAC(CNPAC)于 1989 年开通服务。

这些公用数据网对于外部用户提供的界面大都采用了国际标准，即国际电报电话咨询委员会 CCITT 制定的 X.25 建议。规定了用分组方式工作和公用数据网连接的数据终端设备 DTE 和数据电路终接设备 DCE 之间的接口。在计算机接入公用数据网的场合下，DTE 就是指计算机，而公用数据网中的分组交换节点就是 DCE。

X.25 是为同一个网络上用户进行相互通信而设计的。而现在的 X.75 是为各种网络上用户进行相互通信而设计的。X.75 取代了 X.25。

3.SNA(System Network Architecture)

SNA 是 IBM 公司的计算机网络产品设计规范。1974 年 SNA 适用于面向终端的计算机网络；1976 年 SNA 适用于树型(带树根)的计算机网络；1979 年 SNA 适用于分布式(不带根)的网络；

1985 年 SNA 可支持与局域网组成的任意拓扑结构的网络。

SNA 虽早于 OSI,但底层却很相似。

1.2 计算机网络的功能与应用

1.2.1 计算机网络的功能

1.硬件资源共享
2.软件资源共享
3.用户间信息交换

1.2.2 计算机网络的分类

1.按网络的分布范围分类:广域网 WAN、局域网 LAN、城域网 MAN
2.按网络的交换方式分类:电路交换、报文交换、分组交换
3.按网络的拓扑结构分类:星形、总线、环形、树形、网形
4.按网络的传输媒体分类:双绞线、同轴电缆、光纤、无线
5.按网络的信道分类:窄带、宽带
6.按网络的用途分类:教育、科研、商业、企业

1.2.3 计算机网络的应用

1.办公自动化 OA(Office Automation)
2.电子数据交换 EDI(Electronic Data Interchange)
3.远程交换(Telecommuting)
4.远程教育(Distance Education)
5.电子银行
6.电子公告板系统 BBS(Bulletin Board System)
7.证券及期货交易
8.广播分组交换
9.校园网(Campus Network)
10.信息高速公路
11.企业网
12.智能大厦和结构化综合布线系统

1.2.4 计算机网络的标准制定机构

1.国际标准化组织(ISO)
2.国际电报电话咨询委员会(CCITT)
3.美国国家标准局(NBS)
4.美国国家标准学会(ANSI)
5.欧洲计算机制造商协会(ECMA)

第 2 章　计算机网络基础知识

2.1 数据通信技术

2.1.1 模拟数据通信和数字数据通信

1.几个术语的解释

1)数据－定义为有意义的实体。数据可分为模拟数据和数字数据。模拟数据是在某区间内连续变化的值；数字数据是离散的值。

2)信号－是数据的电子或电磁编码。信号可分为模拟信号和数字信号。模拟信号是随时间连续变化的电流、电压或电磁波；数字信号则是一系列离散的电脉冲。可选择适当的参量

来表示要传输的数据。

3)信息－是数据的内容和解释。

4)信源－通信过程中产生和发送信息的设备或计算机。

5)信宿－通信过程中接收和处理信息的设备或计算机。

6)信道－信源和信宿之间的通信线路。

2. 模拟信号和数字信号的表示

模拟信号和数字信号可通过参量(幅度)来表示：

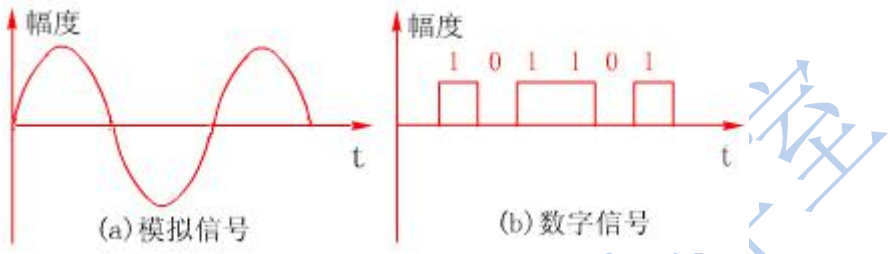


图 2.1 模拟信号、数字信号的表示

3. 模拟数据和数字数据的表示

模拟数据和数字数据都可以用模拟信号或数字信号来表示，因而无论信源产生的是模拟数据还是数字数据，在传输过程中都可以用适合于信道传输的某种信号形式来传输。

1)模拟数据可以用模拟信号来表示。模拟数据是时间的函数，并占有一定的频率范围，即频带。这种数据可以直接用占有相同频带的电信号，即对应的模拟信号来表示。模拟电话通信是它的一个应用模型。

2)数字数据可以用模拟信号来表示。如 Modem 可以把数字数据调制成模拟信号；也可以把模拟信号解调成数字数据。用 Modem 拨号上网是它的一个应用模型。

3)模拟数据也可以用数字信号来表示。对于声音数据来说，完成模拟数据和数字信号转换功能的设施是编码解码器 CODEC。它将直接表示声音数据的模拟信号，编码转换成二进制流近似表示的数字信号;而在线路另一端的 CODEC,则将二进制流码恢复成原来的模拟数据。数字电话通信是它的一个应用模型。

4)数字数据可以用数字信号来表示。数字数据可直接用二进制数字脉冲信号来表示，但为了改善其传播特性，一般先要对二进制数据进行编码。数字数据专线网 DDN 网络通信是它的一个应用模型。

4. 数据通信的长距离传输及信号衰减的克服

1)模拟信号和数字信号都可以在合适的传输媒体上进行传输(如图 2.2)；

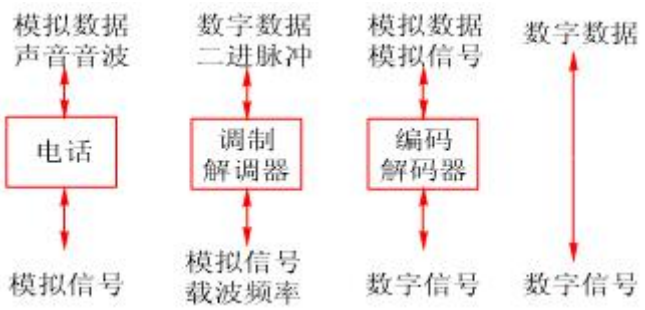


图 2.2 模拟数据、数字数据的模拟信号、数字信号的传输表示

2)模拟信号无论表示模拟数据还是数字数据,在传输一定距离后都会衰减。克服的办法是用放大器来增强信号的能量，但噪音分量也会增强，以至引起信号畸变。

3)数字信号长距离传输也会衰减，克服的办法是使用中继器，把数字信号恢复为"0、1"的标准电平后继续传输。

2.1.2 数据通信中的主要技术指标

1.数据传输速率

1)**数据传输速率**--每秒传输二进制信息的位数，单位为位/秒，记作 bps 或 b/s。

计算公式：$S=1/T*\log_2 N$(bps)　.....(1)

式中 T 为一个数字脉冲信号的宽度(全宽码)或重复周期(归零码)单位为秒；

N 为一个码元所取的离散值个数。

通常 $N=2^K$，K 为二进制信息的位数，$K=\log_2 N$。

N=2 时，S=1/T，表示数据传输速率等于码元脉冲的重复频率。

2)**信号传输速率**--单位时间内通过信道传输的码元数，单位为波特，记作 Baud。

计算公式：$B=1/T$ (Baud)　.....(2)

式中 T 为信号码元的宽度，单位为秒.

信号传输速率,也称码元速率、调制速率或波特率。

由(1)、(2)式得：　$S=B*\log_2 N$ (bps)　.....(3)

或　$B=S/\log_2 N$ (Baud)　.....(4)

[例 1]采用四相调制方式，即 N=4，且 $T=833x10^{-6}$ 秒，则

$S=1/T*\log_2 N=1/(833x10^{-6})*\log_2 4=2400$ (bps)

$B=1/T=1/(833x10^{-6})=1200$ (Baud)

2.信道容量

1)信道容量表示一个信道的最大数据传输速率，单位：位/秒(bps)

信道容量与数据传输速率的区别是，前者表示信道的最大数据传输速率，是信道传输数据能力的极限，而后者是实际的数据传输速率。像公路上的最大限速与汽车实际速度的关系一样。

2)离散的信道容量

奈奎斯特(Nyquist)无噪声下的码元速率极限值 B 与信道带宽 H 的关系：

$B=2*H$ (Baud)　.....(5)

奈奎斯特公式--无噪信道传输能力公式：

$C=2*H*\log_2 N$ (bps)　.....(6)

式中 H 为信道的带宽，即信道传输上、下限频率的差值，单位为 Hz；

N 为一个码元所取的离散值个数。

[例 2]普通电话线路带宽约 3kHz，则码元速率极限值 B=2*H=2*3k=6kBaud ；

若码元的离散值个数 N=16，则最大数据传输速率 $C=2*3k*\log_2 16=24$kbps。

3)连续的信道容量

香农公式--带噪信道容量公式：

$C=H*\log_2(1+S/N)$ (bps)　.....(7)

式中 S 为信号功率，

N 为噪声功率，

S/N 为信噪比，通常把**信噪比**表示成 **10lg(S/N)分贝**(dB)。

[例 3]已知信噪比为 30dB，带宽为 3kHz，求信道的最大数据传输速率。

∵ $10\lg(S/N)=30$　∴ $S/N=10^{30/10}=1000$

∴ $C=3k\log_2(1+1000)\approx 30k$ bps

3. 误码率--二进制数据位传输时出错的概率。

它是衡量数据通信系统在正常工作情况下的传输可靠性的指标。在计算机网络中，一般要求误码率低于 10^{-6}，若误码率达不到这个指标，可通过差错控制方法检错和纠错。

误码率公式：

$$Pe=Ne/N \qquad \ldots\ldots(8)$$

式中 Ne 为其中出错的位数；

N 为传输的数据总数。

2.1.3 通信方式

1. 并行通信方式

并行通信传输中有多个数据位，同时在两个设备之间传输。发送设备将这些数据位通过对应的数据线传送给接收设备，还可附加一位数据校验位。接收设备可同时接收到这些数据，不需要做任何变换就可直接使用。并行方式主要用于近距离通信。计算机内的总线结构就是并行通信的例子。这种方法的优点是传输速度快，处理简单。

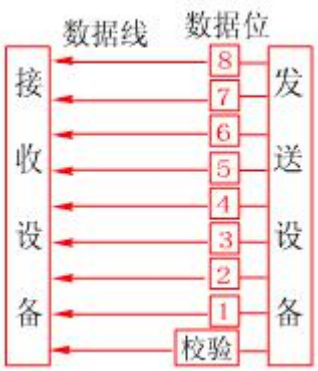


图 2.3　并行数据传输

2. 串行通信方式

串行数据传输时，数据是一位一位地在通信线上传输的，先由具有几位总线的计算机内的发送设备，将几位并行数据经并--串转换硬件转换成串行方式，再逐位经传输线到达接收站的设备中，并在接收端将数据从串行方式重新转换成并行方式，以供接收方使用。串行数据传输的速度要比并行传输慢得多，但对于覆盖面极其广阔的公用电话系统来说具有更大的现实意义。

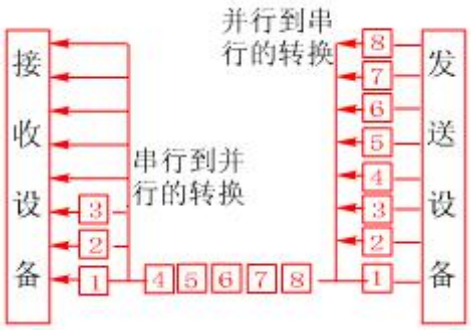


图 2.4　串行数据传输

3. 串行通信的方向性结构

串行数据通信的方向性结构有三种，即单工、半双工和全双工。

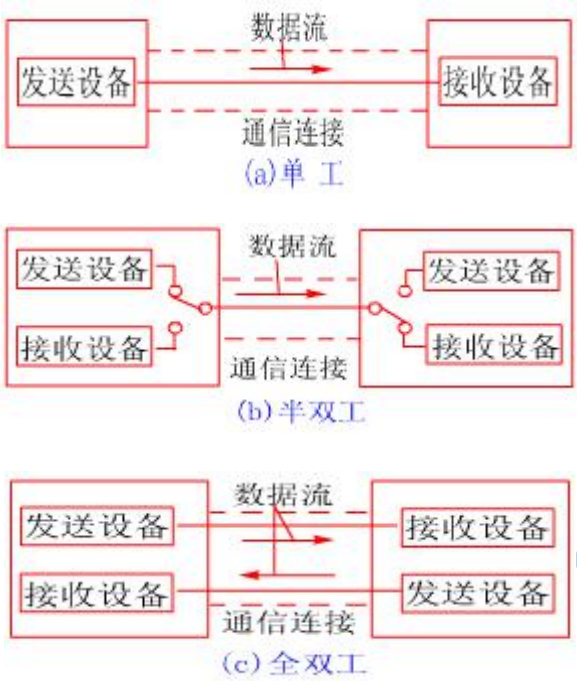


图 2.5　单工、半双工、全双工

单工数据传输只支持数据在一个方向上传输；

半双工数据传输允许数据在两个方向上传输，但是，在某一时刻，只允许数据在一个方向上传输，它实际上是一种切换方向的单工通信；

全双工数据通信允许数据同时在两个方向上传输，因此，全双工通信是两个单工通信方式的结合，它要求发送设备和接收设备都有独立的接收和发送能力。

2.2 数据编码技术和时钟同步

2.2.1 数字数据的模拟信号编码

为了利用廉价的公共电话交换网实现计算机之间的远程通信，必须将发送端的数字信号变换成能够在公共电话网上传输的音频信号，经传输后再在接收端将音频信号逆变换成对应的数字信号。实现数字信号与模拟信号互换的设备称作调制解调器(Modem)。

图 2.6　远程系统中的调制解调器

模拟信号传输的基础是载波，载波具有三大要素：幅度、频率和相位，数字数据可以针对载波的不同要素或它们的组合进行调制。

1. 数字调制的基本形式

数字调制的三种基本形式：移幅键控法 ASK、移频键控法 FSK、移相键控法 PSK。

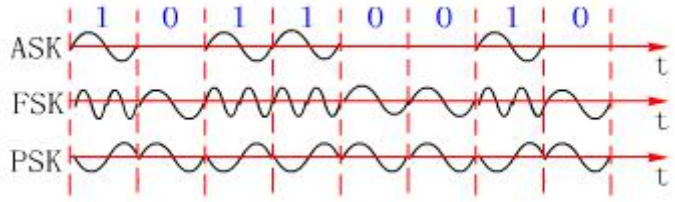


图 2.7　数字调制的三种基本形式

在 ASK 方式下，用载波的两种不同幅度来表示二进制的两种状态。ASK 方式容易受增益变化的影响，是一种低效的调制技术。在电话线路上，通常只能达到 1200bps 的速率。

在 FSK 方式下，用载波频率附近的两种不同频率来表示二进制的两种状态。在电话线路上，使用 FSK 可以实现全双工操作，通常可达到 1200bps 的速率。

在 PSK 方式下，用载波信号相位移动来表示数据。PSK 可以使用二相或多于二相的相移，利用这种技术，可以对传输速率起到加倍的作用。

由 PSK 和 ASK 结合的相位幅度调制 PAM，是解决相移数已达到上限但还要提高传输速率的有效方法。

2. 公共电话交换网中使用调制解调器的必要性

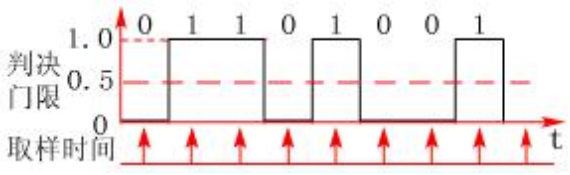
公共电话交换网是一种频带模拟信道，音频信号频带为 300Hz～3400Hz，而数字信号频宽为 0Hz～几千兆 Hz。若不加任何措施利用模拟信道来传输数字信号，必定出现极大的失真和差错。所以，要在公共电话网上传输数字数据，必须将数字信号变换成电话网所允许的音频频带范围 300Hz～3400Hz。

2.2.2 数字数据的数字信号编码

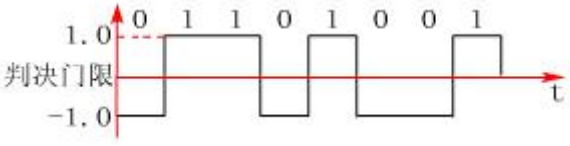
数字信号可以直接采用基带传输。基带传输就是在线路中直接传送数字信号的电脉冲，它是一种最简单的传输方式，近距离通信的局域网都采用基带传输。基带传输时，需要解决的问题是数字数据的数字信号表示及收发两端之间的信号同步两个方面。

1. 数字数据的数字信号表示

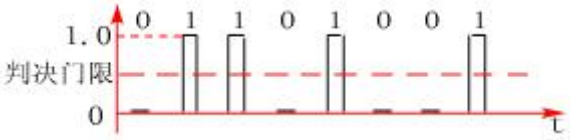
对于传输数字信号来说，最常用的方法是用不同的电压电平来表示两个二进制数字，即数字信号由矩形脉冲组成。



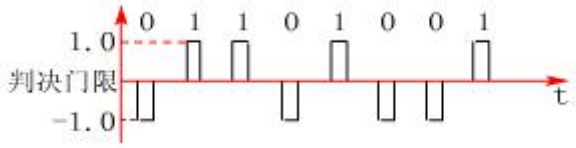
a) 单极性脉冲



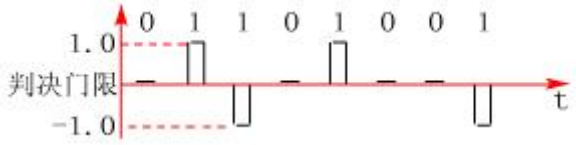
b) 双极性脉冲



c) 单极性归零脉冲



d) 双极性归零脉冲



e) 交替双极性归零脉冲

图 2.8　基脉冲编码方案

a) 单极性不归零码，无电压表示"0"，恒定正电压表示"1"，每个码元时间的中间点是采样时间，判决门限为半幅电平。

b) 双极性不归零码，"1"码和"0"码都有电流，"1"为正电流，"0"为负电流，正和负的幅度相等，判决门限为零电平。

c) 单极性归零码，当发"1"码时，发出正电流，但持续时间短于一个码元的时间宽度，即发出一个窄脉冲；当发"0"码时，仍然不发送电流。

d) 双极性归零码，其中"1"码发正的窄脉冲，"0"码发负的窄脉冲，两个码元的时间间隔可以大于每一个窄脉冲的宽度，取样时间是对准脉冲的中心。

2. 归零码和不归零码、单极性码和双极性码的特点

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

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

3. 同步过程

1) 位同步

位同步又称同步传输，它是使接收端对每一位数据都要和发送端保持同步。实现位同步的方法可分为外同步法和自同步法两种。

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

自同步法是指能从数据信号波形中提取同步信号的方法。典型例子就是著名的曼彻斯特编码，常用于局域网传输。在曼彻斯特编码中，每一位的中间有一跳变，位中间的跳变既作时钟信号，又作数据信号；从高到低跳变表示"1"，从低到高跳变表示"0"。还有一种是差分曼彻斯特编码，每位中间的跳变仅提供时钟定时，而用每位开始时有无跳变表示"0"或"1"，有跳变为"0"，无跳变为"1"。

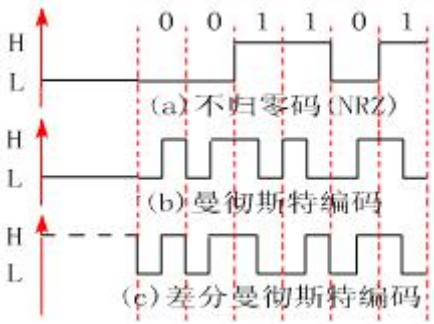


图 2.9　数字信号的同步编码

两种曼彻斯特编码是将时钟和数据包含在数据流中，在传输代码信息的同时，也将时钟同步信号一起传输到对方，每位编码中有一跳变，不存在直流分量，因此具有自同步能力和良好的抗干扰性能。但每一个码元都被调成两个电平，所以数据传输速率只有调制速率的1/2。

2)群同步

在数据通信中，群同步又称异步传输。是指传输的信息被分成若干“群”。数据传输过程中，字符可顺序出现在比特流中，字符间的间隔时间是任意的，但字符内各个比特用固定的时钟频率传输。字符间的异步定时与字符内各个比特间的同步定时，是群同步即异步传输的特征。

群同步是靠起始和停止位来实现字符定界及字符内比特同步的。起始位指示字符的开始，并启动接收端对字符中比特的同步；而停止位则是作为字符间的间隔位设置的，没有停止位，下一字符的起始位下降沿便可能丢失。

群同步传输每个字符由四部组成：

1)1 位起始位，以逻辑"0"表示；

2)5～8 位数据位，即要传输的字符内容；

3)1 位奇偶校验位，用于检错；

4)1～2 位停止位，以逻辑"1"表示,用作字符间的间隔。

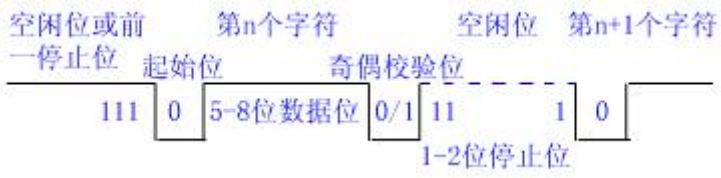


图 2.10 群同步的字符格式

2.2.3 模拟数据的数字信号编码

1.脉码调制 PCM。

脉码调制是以采样定理为基础，对连续变化的模拟信号进行周期性采样，利用≥有效信号最高频率或其带宽 2 倍的采样频率，通过低通滤波器从这些采样中重新构造出原始信号。

采样定理表达公式：

$$Fs(=1/Ts) \geq 2Fmax \text{ 或 } Fs \geq 2Bs$$

式中　Ts 为采样周期

Fs 为采样频率

Fmax 为原始信号的最高频率

Bs(=Fmax-Fmin)为原始信号的带宽

2. 模拟信号数字化的三步骤

1)采样，以采样频率 Fs 把模拟信号的值采出；

2)量化，使连续模拟信号变为时间轴上的离散值；

3)编码，将离散值变成一定位数的二进制数码。

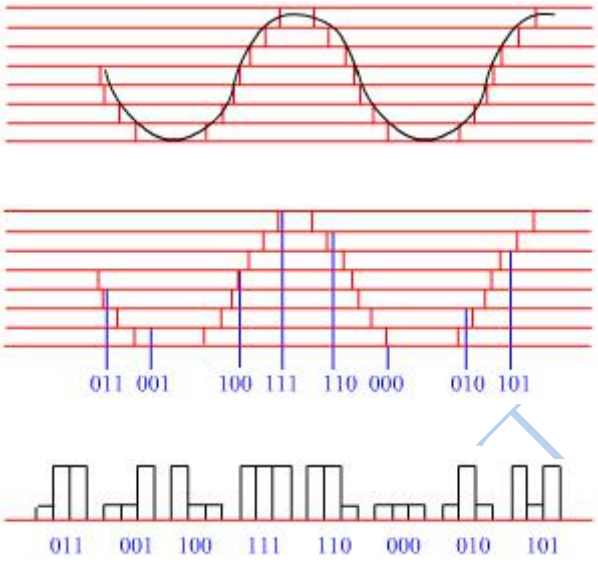


图 2.11　脉码调制(PCM)原理

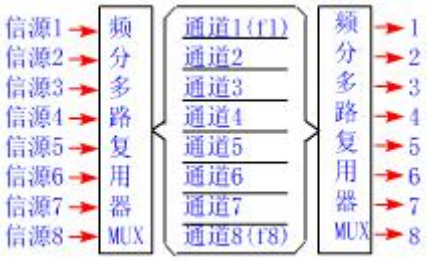
2.2.4 多路复用技术

多路复用技术就是把许多个单个信号在一个信道上同时传输的技术。频分多路复用 FDM 和时分多路复用 TDM 是两种最常用的多路复用技术。

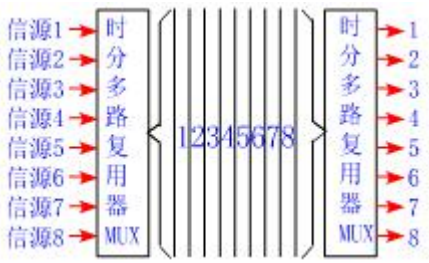
1. 频分多路复用 FDM 技术原理

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

多路原始信号在步分复用前，先要通过频谱搬移技术将各路信号的频谱搬移到物理信道频谱的不同段上，使各信号的带宽不相互重叠，然后用不同的频率调制每一个信号，每个信号要一个样以它的载波频率为中心的一定带宽的通道。为了防止互相干扰，使用保护带来隔离每一个通道。



(a)频分多路复用



(b)时分多路复用

图 2.12　频分多路复用与时分多路复用

2.时分多路复用 TDM 技术原理

若媒体能达到的位传输速率超过传输数据所需的数据传输速率，可采用时分多路复用 TDM 技术，即将一条物理信道按时间分成若干个时间片轮流地分配给多个信号使用。每一时间片由复用的一个信号占用，这样，利用每个信号在时间上的交叉，就可以在一条物理信道上传输多个数字信号。

时分多路复用 TDM 不仅局限于传输数字信号，也可同时交叉传输模拟信号。

3.T1 载波与 E1 载波的帧结构

1)T1 载波

Bell 系统的 T1 载波利用脉码调制 PCM 和时分 TDM 技术，使 24 路采样声音信号复用一个通道。每一个帧包含 193 位，每一帧用 125us 时间传送。T1 系统的数据传输速率为 1.544Mbps。

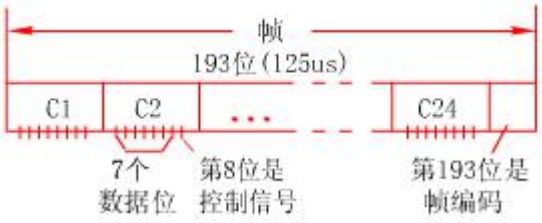


图 2.13　T1 载波帧结构

2)E1 载波

CCITT 建议了一种 2.048Mbps 速率的 PCM 载波标准，称为 E1 载波(欧洲标准)。它每一帧开始处有 8 位同步作用，中间有 8 位作用信令，在组织 30 路 8 位数据，全帧包括 256 位，每一帧用 125us 时间传送。可计算出 E1 系统的数据传输速率为 256 位/125us=2.048Mbps。

2.2.5 异步传输和同步传输

1.异步传输方式中，一次只传输一个字符。每个字符用一位起始位引导、一位停止位结束。在没有数据发送时，发送方可发送连续的停止位。接收方根据"1"至"0"的跳变来判断一个新字符的开始,然后接收字符中的所有位。

2.同步传输时，为使接收双方能判别数据块的开始和结束，还需要在每个数据块的开始处和结束处各加一个帧头和一个帧尾，加有帧头、帧尾的数据称为一帧。帧头和

2.3 数据交换技术

数据经编码后在通信线路上进行传输，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 2.14 为一个交换网络的拓扑结构

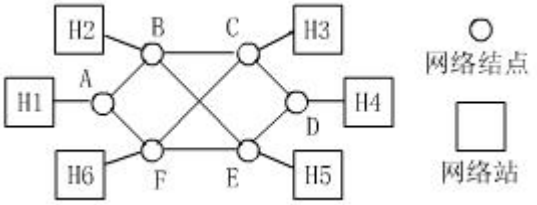


图 2.14 交换网络的拓扑结构

2.3.1 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 2.14 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。

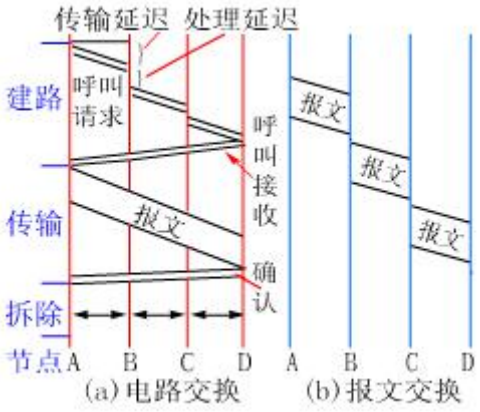
3)电路拆除：数据传输结束后，由某一方（A 或 C）发出拆除请求，然后逐节拆除到对方节点。

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。对于猝发式的通信，电路交换效率不高。



2.3.2 报文交换的工作原理

问题的提出：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。

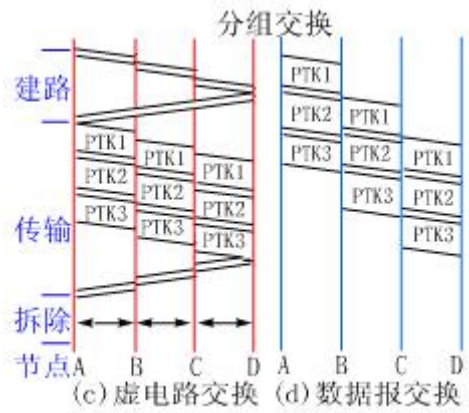
4. 报文交换的缺点

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。

2.3.3 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。



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。

2.3.4 各种数据交换技术的性能比较

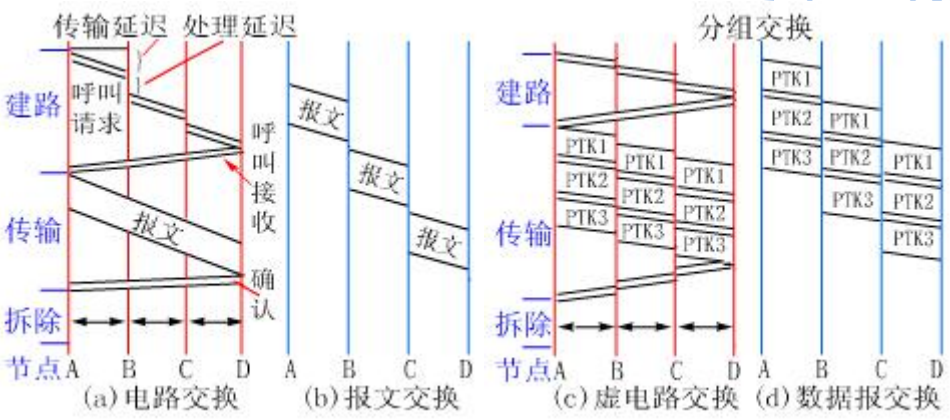


图 2.15 几种交换方法的时序图

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。

2.4 拓扑结构与传输媒体

2.4.1 拓扑结构

网络拓扑是指网络形状，或者是它在物理上的连通性。网络的拓扑结构主要有：星形拓扑、总线拓扑、环形拓扑、树形拓扑、混合拓扑及网形拓扑。

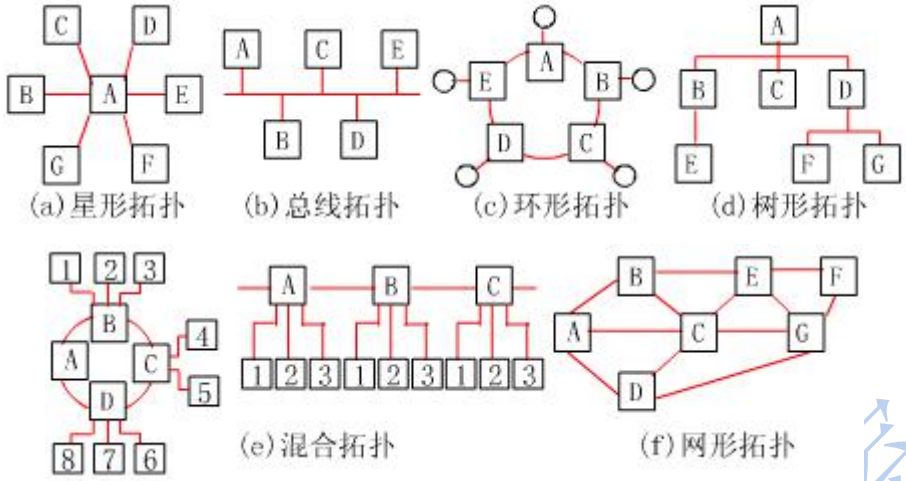


图 2.16 各种网络拓扑

拓扑结构的选择往往与传输媒体的选择及媒体访问控制方法的确定紧密相关。在选择网络拓扑结构时，应考虑的因素有下列几点：

1)可靠性。

2)费用。

3)灵活性。

4)响应时间和吞吐量。

1. 星形拓扑的特点及优缺点

优点：1)控制简单；2)故障诊断和隔离容易；3)方便服务；

缺点：1)电缆长度和安装工作量可观；2)中央节点负担较重，形成瓶颈；3)各站点的分布处理能力较低。

2. 总线拓扑的特点及优缺点

优点：1)总线结构所需电缆数量少；2)结构简单又是无源工作，有较高的可靠性；3)易于扩充，增减用户方便。

缺点：1)传输距离有限，通信范围受到限制；2)故障诊断和隔离困难；3)分布式协议不保证信息及时传送，不具实时功能。站点必须是智能的，要有媒体访问控制功能，增加站点软件和硬件的开销。

3. 环形拓扑的特点及优缺点

优点：1)电缆长度短；2)增减工作站时只需简单连接；3)可用光纤。

缺点：1)节点故障会引起全网的故障；2)故障难检测；3)媒体访问协议都用令牌传递方式，在负载很轻时，信道利用率较低。

4. 树形拓扑的定义及优缺点

树形拓扑：从总线拓扑演变而来，像一棵倒置的树，顶端是树根，树根以下带分支，每个分支还可带子分支。树根接收各站点发送的数据，然后再广播发送到全网。

优点：1)易于扩展；2)故障隔离较容易。

缺点：1)节点对根依赖性太大，若根发生故障，则全网不能正常工作。

5. 混合形拓扑的定义及优缺点

混合形拓扑：将两种单一拓扑结构混合起来，取两者的优点构成的拓扑。

优点：1)故障诊断和隔离方便；2)易于扩展；3)安装方便；

缺点：1)需用带智能的集中器；2)集中器到各站点的电缆长度会增加。

6. 网形拓扑的特点及优缺点

优点：1)应用广泛；2)不受瓶颈问题和失效问题的影响。

缺点：1)结构较复杂，网络协议也复杂，建设成本高。

2.4.2 传输媒体

传输媒体是通信网络中发送方和接收方之间的物理通路，计算机网络中采用的传输媒体分有线和无线两大类。

传输媒体的特性对网络数据通信的质量有很大影响，这些特征是：

⑴物理特性：说明传输媒体的特性。

⑵传输特性：包括是使用模拟信号发送还是使用数字信号发送、调制技术、传输容量及传输频率范围。

⑶连通性：采用点到点连接还是多点连接。

⑷地理范围：在不用中间设备并将失真限制在允许范围内的情况下，整个网络所允许的最大距离。

⑸抗干扰性：防止噪音、电磁干扰对传输数据影响的能力。

⑹相对价格：包括元件、安装和维护等价格。

1.有线传输媒体

1)双绞线(TP)--由螺旋状扭在一起的两根绝缘导线组成。双绞线一般分为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)。计算机网络中最常用的是第三类和第五类非屏蔽双绞线。

⑴物理特性：铜质线芯，传导性能良好。

⑵传输特性：可用于传输模拟信号和数字信号，对于模拟信号，约 5--6 公里需要一个放大器；对于数字信号，约 2--3 公里需要一个中继器。双绞线的带宽达 268kHz。

对于模拟信号，可用频分多路复用技术把它分成 24 路来传输音频模拟信号，根据目前的 Modem 技术，若使用移相键控法 PSK，每路可达 9600bps 以上，这样，在一条 24 路的双绞线上，总传输率可达 230kbps。

对于数字信号，使用 T1 线路总传输率可达 1.544Mbps。达到更高传输率也是可能的，但与距离有关。

对于局域网(10BASE-T 和 100BASE-T 总线)，传输速率可达 10Mbps-100Mbps。常用的 3 类双绞线和 5 类双绞线电缆均由 4 对双绞线组成，3 类双绞线传输速率可达 10Mbps，5 类双绞线传输速率可达 100Mbps。但与距离有关。

⑶连通性：可用于点到点连接或多点连接。

⑷地理范围：对于局域网，速率 100Kbps,可传输 1 公里；速率 10Mbps--100Mbps,可传输 100 米。

⑸抗干扰性：低频(10kHz 以下)抗干扰性能强于同轴电缆，高频(10-100kHz)抗干扰性能弱于同轴电缆。

⑹相对价格：比同轴电缆和光纤便宜得多。

2)同轴电缆--由绕同一轴线的两个导体所组成，被广泛用于局域网中。为保持同轴电缆的正确电气特性，电缆必须接地，同时两头要有端接器来削弱信号反射作用。

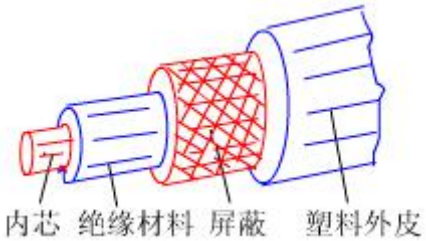


图 2.17 同轴电缆

⑴物理特性：单根同轴电缆直径约为 1.02-2.54cm，可在较宽频范围工作。

⑵传输特性：基带同轴电缆仅用于数字传输，阻抗为 50Ω，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 75Ω，对于模拟信号，带宽可达 300-450MHz。在 CATV 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。基带 50

⑶连通性：可用于点到点连接或多点连接。

⑷地理范围：基带同轴电缆的最大距离限制在几公里；宽带电缆的最大距离可以达几十公里。。

⑸抗干扰性：能力比双绞线强。

⑹相对价格：比同轴电缆贵，比光纤便宜。

3)光纤--由能传导光波的石英玻璃纤维外加保护层构成的。光纤具有宽带、数据传输率高、抗干扰能力强、传输距离远等优点。按使用的波长区的不同分为单模和多模光纤通信方式。

图 2.18 光纤的电信号传送过程

⑴物理特性：在计算机网络中均采用两根光纤(一来一去)组成传输系统。按波长范围可分为三种：0.85um 波长(0.8-0.9um)、1.3um 波长(1.25-1.35um)和 1.55um 波长区(1.53-1.58um)。不同的波长范围光纤损耗特性也不同，其中 0.85um 波长区为多模光纤通信方式，1.55um 波长区为单模光纤通信方式，1.3um 波长区有多模和单模两种方式。

⑵传输特性：光纤通过内部的全反射来传输一束经过编码的光信号，内部的全反射可以在任何折射指数高于包层媒体折射指数的透明媒体中进行。实际上光纤作为频率范围从 10^{14}-10^{15}Hz 的波导管，这一范围覆盖了可见光谱和部分红外光谱。光纤的数据传输率可达 Gbps 级，传输距离达数十公里。目前，一条光纤线路上只能传输一个载波，随着技术进一步发展，会出现实用的多路复用光纤。

⑶连通性：采用点到点连接还是多点连接。

⑷地理范围：可以在 6-8 公里的距离内不用中继器传输，因此光纤适合于在几个建筑物之间通过点到点的链路连接局域网。

⑸抗干扰性：不受噪声或电磁影响，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。

⑹)相对价格：目前价格比同轴电缆和双绞线都贵。

2.无线传输媒体

1)微波通信：载波频率为 2GHZ 至 40GHZ。频率高，可同时传送大量信息；由于微波是沿直线传播的，故在地面的传播距离有限。

2)卫星通信：是利用地球同步卫星作为中继来转发微波信号的一种特殊微波通信形式。卫星通信可以克服地面微波通信距离的限制，三个同步卫星可以覆盖地球上全部通信区域。

3)红外通信和激光通信：和微波通信一样，有很强的方向性，都是沿直线传播的。但红外通信和激光通信要把传输的信号分别转换为红外光信号和激光信号后才能直接在空间沿直线传播。

微波、红外线和激光都需要在发送方和接收方之间有一条视线通路，故它们统称为视线媒体。

3.传输媒体的选择

取决于以下诸因素；网络拓扑的结构、实际需要的通信容量、可靠性要求、能承受的价格范围。

4.基带同轴电缆与宽带同轴电缆

基带同轴电缆用于直接传输数字信号，阻抗为50Ω，基带同轴电缆的最大距离限制在几公里；宽带同轴电缆既可传输数字信号也可传输模拟信号，阻抗为75Ω，宽带电缆的最大距离可以达几十公里。

2.5 差错控制方法

2.5.1 差错的产生原因及其控制方法

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

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

1.热噪声和冲击噪声

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

热噪声引起的差错称为随机差错所引起的某位码元的差错是孤立的，与前后码元没有关系。它导致的随机错通常较少。

冲击噪声呈突发状，由其引起的差错称为突发错。冲击噪声幅度可能相当大，无法靠提高幅度来避免冲击噪声造成的差错，它是传输中产生差错的主要原因。冲击噪声虽然持续时间较短，但在一定的数据速率条件下，仍然会影响到一串码元。

2.差错的控制方法

最常用的差错控制方法是差错控制编码。数据信息位在向信道发送之前，先按照某种关系附加上一定的冗余位，构成一个码字后再发送，这个过程称为差错控制编码过程。接收端收到该码字后，检查信息位和附加的冗余位之间的关系，以检查传输过程中是否有差错发生，这个过程称为检验过程。

差错控制编码可分为检错码和纠错码。

①检错码——能自动发现差错的编码；

②纠错码——不仅能发现差错而且能自动纠正差错的编码。

差错控制方法分两类，一类是自动请求重发ARQ，另一类是前向纠错FEC。

在ARQ方式中，当接收端发现差错时，就设法通知发送端重发，直到收到正确的码字为止。ARQ方式只使用检错码。

在FEC方式中，接收端不但能发现差错，而且能确定二进制码元发生错误的位置，从而加以纠正。FEC方式必须使用纠错码。

3.编码效率

衡量编码性能好坏的一个重要参数是编码效率R，它是码字中信息位所占的比例。编码效率越高，即R越大，信道中用来传送信息码元的有效利用率就越高。编码效率计算公式为：

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

式中 k为码字中的信息位位数

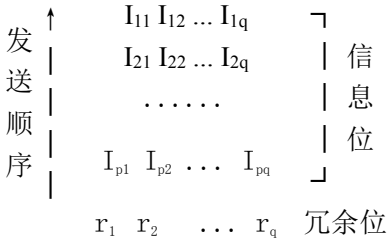
r为编码时外加冗余位位数

n 为编码后的码字长度

2.5.2　奇偶校验码

奇偶校验码是一种通过增加冗余位使得码字中“ 1 ”的个数为奇数或偶数的编码方法，它是一种检错码。

1. 垂直奇偶校验的特点及编码规则



1)编码规则：

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

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

式中 p 为码字的定长位数

q 为码字的个数

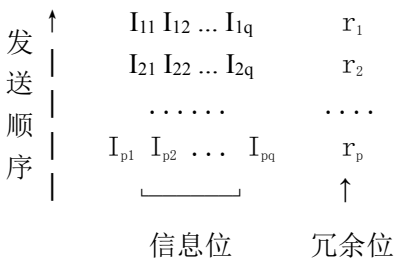
垂直奇偶校验的编码效率为 R=p/(p+1)。

2)特点：垂直奇偶校验又称纵向奇偶校验，它能检测出每列中所有奇数个错，但检测不出偶数个的错。因而对差错的漏检率接近 1/2。

位\数字		0 1 2 3 4 5 6 7 8 9
C_1		0 1 0 1 0 1 0 1 0 1
C_2		0 0 1 1 0 0 1 1 0 0
C_3		0 0 0 0 1 1 1 1 0 0
C_4		0 0 0 0 0 0 0 0 1 1
C_5		1 1 1 1 1 1 1 1 1 1
C_6		1 1 1 1 1 1 1 1 1 1
C_7		0 0 0 0 0 0 0 0 0 0
偶	C_0	0 1 1 0 1 0 0 1 1 0
奇		1 0 0 1 0 1 1 0 0 1

2. 水平奇偶校验的特点及编码规则

1)编码规则：



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

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

式中 p 为码字的定长位数

q 为码字的个数

水平奇偶校验的编码效率为 R=q/(q+1)。

2)特点：水平奇偶校验又称横向奇偶校验，它不但能检测出各段同一位上的奇数个错，而且还能检测出突发长度<=p 的所有突发错误。其漏检率要比垂直奇偶校验方法低，但实现水平奇偶校验时，一定要使用数据缓冲器。

位\数字	0 1 2 3 4 5 6 7 8 9	偶校验
C_1	0 1 0 1 0 1 0 1 0 1	1
C_2	0 0 1 1 0 0 1 1 0 0	0
C_3	0 0 0 0 1 1 1 1 0 0	0
C_4	0 0 0 0 0 0 0 0 1 1	0
C_5	1 1 1 1 1 1 1 1 1 1	1
C_6	1 1 1 1 1 1 1 1 1 1	1
C_7	0 0 0 0 0 0 0 0 0 0	0

3. 水平垂直奇偶校验的特点及编码规则

1)编码规则：

发送顺序 ↑

$$\begin{array}{cccccc} I_{11} & I_{12} & \ldots & I_{1q} & r_{1,q+1} \\ I_{21} & I_{22} & \ldots & I_{2q} & r_{2,q+1} \\ \ldots\ldots & & & & \ldots \\ I_{p1} & I_{p2} & \ldots & I_{pq} & r_{p,q+1} \\ r_{p+1,1} & r_{p+1,2} & \ldots & r_{p+1,q} & r_{p+1,q+1} \end{array}$$

若水平垂直都用偶校验，则

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

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

$r_{p+1,q+1}=r_{p+1,1}+r_{p+1,2}+\ldots+r_{p+1,q}$

$=r_{1,q+1}+r_{2,q+1}+\ldots+r_{p,q+1}$

水平垂直奇偶校验的编码效率为 R=pq/[(p+1)(q+1)]。

2)特点：水平垂直奇偶校验又称纵横奇偶校验。它能检测出所有 3 位或 3 位以下的错误、奇数个错、大部分偶数个错以及突发长度<=p+1 的突发错。可使误码率降至原误码率的百分之一到万分之一。还可以用来纠正部分差错。有部分偶数个错不能测出。适用于中、低速传输系统和反馈重传系统。

位\数字	0 1 2 3 4 5 6 7 8 9	校验码字
C_1	0 1 0 1 0 1 0 1 0 1	1
C_2	0 0 1 1 0 0 1 1 0 0	0
C_3	0 0 0 0 1 1 1 1 0 0	0
C_4	0 0 0 0 0 0 0 0 1 1	0

C_5	1 1 1 1 1 1 1 1 1 1	1
C_6	1 1 1 1 1 1 1 1 1 1	1
C_7	0 0 0 0 0 0 0 0 0 0	0
C_8	0 1 1 0 1 0 0 1 1 0	1

2.5.3　循环冗余码（CRC）

1. CRC 的工作方法

在发送端产生一个循环冗余码，附加在信息位后面一起发送到接收端，接收端收到的信息按发送端形成循环冗余码同样的算法进行校验，若有错，需重发。

2. 循环冗余码的产生与码字正确性检验例子。

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

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

求：循环冗余码和码字。

解：1) $(X^5+X^4+X+1)*X^4$ 的积是 $X^9+X^8+X^5+X^4$ 对应的码是 1100110000。

2)积 / G(X)(按模二算法)。

由计算结果知冗余码是 1001，码字就是 1100111001。

```
                  1 0 0 0 0 1←Q(X)
G(x)→1 1 0 0 1 )1 1 0 0 1 1 0 0 0 0←F(X)*X^r
                1 1 0 0 1
                  1 0 0 0 0
                  1 1 0 0 1
                  1 0 0 1←R(X)(冗余码)
```

例 2. 已知：接收码字:1100111001　多项式:$T(X)=X^9+X^8+X^5+X^4+X^3+1$

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

求：码字的正确性。若正确，则指出冗余码和信息码。

解：1)用字码除以生成码，余数为 0，所以码字正确。

```
                  1 0 0 0 0 1←Q(X)
G(x)→1 1 0 0 1 )1 1 0 0 1 1 1 0 0 1←F(X)*X^r+R(x)
                1 1 0 0 1
                  1 1 0 0 1
                  1 1 0 0 1
                        0←S(X)(余数)
```

2)因 r=4，所以冗余码是：11001，信息码是:110011

3. 循环冗余码的工作原理

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

4. 循环冗余校验码的特点

1)可检测出所有奇数位错；

2)可检测出所有双比特的错；

3)可检测出所有小于、等于校验位长度的突发错。

5.4 种生成码(P44)

2.5.4 海明码

1.海明码的概念

海明码是一种可以纠正一位差错的编码。它是利用在信息位为 k 位，增加 r 位冗余位，构成一个 n=k+r 位的码字，然后用 r 个监督关系式产生的 r 个校正因子来区分无错和在码字中的 n 个不同位置的一位错。它必需满足以下关系式：

$$2^r>=n+1 \quad 或 \quad 2^r>=k+r+1$$

海明码的编码效率为：

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

式中 k 为信息位位数

r 为增加冗余位位数

2.海明码的生成与接收

方法一：（按教科书）

1)海明码的生成。

例 1.已知：信息码为："0010"。海明码的监督关系式为：

$$S_2=a_2+a_4+a_5+a_6$$

$$S_1=a_1+a_3+a_5+a_6$$

$$S_0=a_0+a_3+a_4+a_6$$

求：海明码码字。

解：1)由监督关系式知冗余码为 $a_2a_1a_0$。

2)冗余码与信息码合成的海明码是："$0010a_2a_1a_0$"。

设 $S_2=S_1=S_0=0$，由监督关系式得：

$$a_2=a_4+a_5+a_6=1$$

$$a_1=a_3+a_5+a_6=0$$

$$a_0=a_3+a_4+a_6=1$$

因此，海明码码字为："0010101"

2)海明码的接收。

例 2.已知：海明码的监督关系式为：

$$S_2=a_2+a_4+a_5+a_6$$

$$S_1=a_1+a_3+a_5+a_6$$

$$S_0=a_0+a_3+a_4+a_6$$

接收码字为："0011101"(n=7)

求：发送端的信息码。

解：1)由海明码的监督关系式计算得 $S_2S_1S_0=011$。

2)由监督关系式可构造出下面错码位置关系表：

$S_2S_1S_0$	000	001	010	100	011	101	110	111
错码位置	无错	a_0	a_1	a_2	a_3	a_4	a_5	a_6

3)由 $S_2S_1S_0=011$ 查表得知错码位置是 a_3。

4)纠错--对码字的 a_3 位取反得正确码字："0 0 1 0 1 0 1"

5)把冗余码 $a_2a_1a_0$ 删除得发送端的信息码："0010"

方法二：（不用查表，方便编程）

1)海明码的生成（顺序生成法）。

例 3.已知：信息码为：″ 1 1 0 0 1 1 0 0 ″ (k=8)

求：海明码码字。

解：1)把冗余码 A、B、C、…，顺序插入信息码中，得海明码

码字:″ A B 1 C 1 0 0 D 1 1 0 0 ″

码位： 1 2 3 4 5 6 7 8 9 10 11 12

其中 A,B,C,D 分别插于 2^k 位(k=0,1,2,3)。码位分别为 1,2,4,8。

2)冗余码 A,B,C,D 的线性码位是：(相当于监督关系式)

A->1,3,5,7,9,11;

B->2,3,6,7,10,11;

C->4,5,6,7,12; (注 5=4+1; 6=4+2; 7=4+2+1; 12=8+4)

D->8,9,10,11,12。

3)把线性码位的值的偶校验作为冗余码的值(设冗余码初值为 0):

A=∑(0,1,1,0,1,0)=1

B=∑(0,1,0,0,1,0)=0

C=∑(0,1,0,0,0) =1

D=∑(0,1,1,0,0) =0

4)海明码为:″1 0 1 1 1 0 0 0 1 1 0 0″

2)海明码的接收。

例 4.已知：接收的码字为：″1 0 0 1 1 0 0 0 1 1 0 0″(k=8)

求：发送端的信息码。

解：1)设错误累加器(err)初值=0

2)求出冗余码的偶校验和，并按码位累加到 err 中：

A=∑(1,0,1,0,1,0)=1 err=err+2^0=1

B=∑(0,0,0,0,1,0)=1 err=err+2^1=3

C=∑(1,1,0,0,0) =0 err=err+0 =3

D=∑(0,1,1,0,0) =0 err=err+0 =3

由 err≠0 可知接收码字有错，

3)码字的错误位置就是错误累加器(err)的值 3。

4)纠错--对码字的第 3 位值取反得正确码字：

″1 0 1 1 1 0 0 0 1 1 0 0″

5)把位于 2^k 位的冗余码删除得信息码：″1 1 0 0 1 1 0 0″

第 3 章　计算机网络体系结构及协议

3.1 网络体系结构及 OSI 基本参考模型

3.1.1　协议及体系结构

通过通信信道和设备互连起来的多个不同地理位置的计算机系统，要使其能协同工作实现信息交换和资源共享，它们之间必须具有共同的语言。交流什么、怎样交流及何时交流，都必须遵循某种互相都能接受的规则。

1.网络协议(Protocol)

为进行计算机网络中的数据交换而建立的规则、标准或约定的集合。协议总是指某一层协议，准确地说，它是对同等实体之间的通信制定的有关通信规则约定的集合。

网络协议的三个要素：

1)语义（Semantics)。涉及用于协调与差错处理的控制信息。

2)语法（Syntax)。涉及数据及控制信息的格式、编码及信号电平等。

3)定时（Timing)。涉及速度匹配和排序等。

2.网络的体系结构及其划分所遵循的原则

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

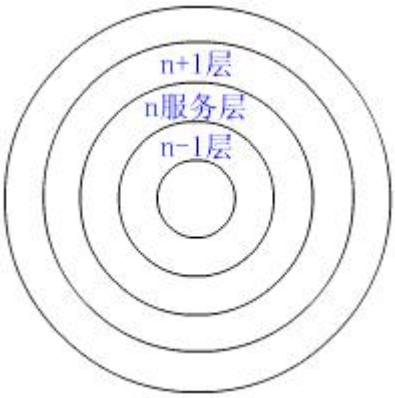


图 3.1 层次模型

层次结构的好处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。

所谓网络的体系结构(Architecture)就是计算机网络各层次及其协议的集合。层次结构一般以垂直分层模型来表示(图 3.2)。

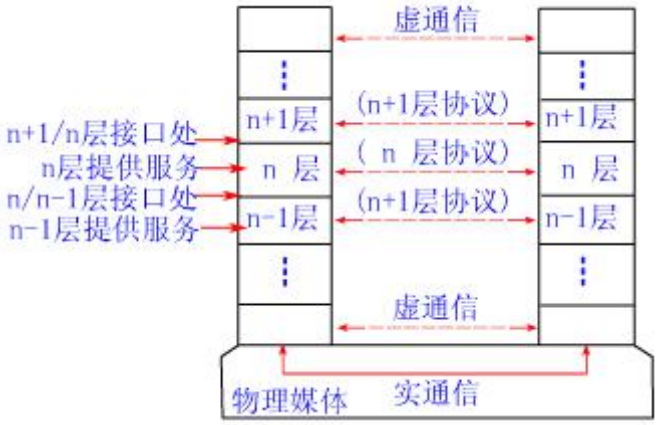


图 3.2 计算机网络的层次模型

层次结构的要点：

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。

层次结构划分的原则：

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。若层数太少，则造成每一层的协议太复杂；若层数太多，则体系结构过于复杂，使描述和实现各层功能变得困难。

网络的体系结构的特点是：

1)以功能作为划分层次的基础。

2)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。

3)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。

4)仅在相邻层间有接口，且所提供服务的具体实现细节对上一层完全屏蔽。

3.1.2　OSI 基本参考模型

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

OSI 包括了体系结构、服务定义和协议规范三级抽象。OSI 的体系结构定义了一个七层模型，用以进行进程间的通信，并作为一个框架来协调各层标准的制定；OSI 的服务定义描述了各层所提供的服务，以及层与层之间的抽象接口和交互用的服务原语；OSI 各层的协议规范，精确地定义了应当发送何种控制信息及何种过程来解释该控制信息。

需要强调的是，OSI 参考模型并非具体实现的描述，它只是一个为制定标准机而提供的概念性框架。在 OSI 中，只有各种协议是可以实现的，网络中的设备只有与 OSI 和有关协议相一致时才能互连。

如图形 3.3 所示,OSI 七层模型从下到上分别为物理层(Physical Layer,PH)、数据链路层(Data Link Layer,DL)、网络层(Network Layer,N)、运输层(Transport Layer,T)、会话层(Session Layer,S)、表示层(Presentation Layer,P)和应用层(Application Layer,A)。

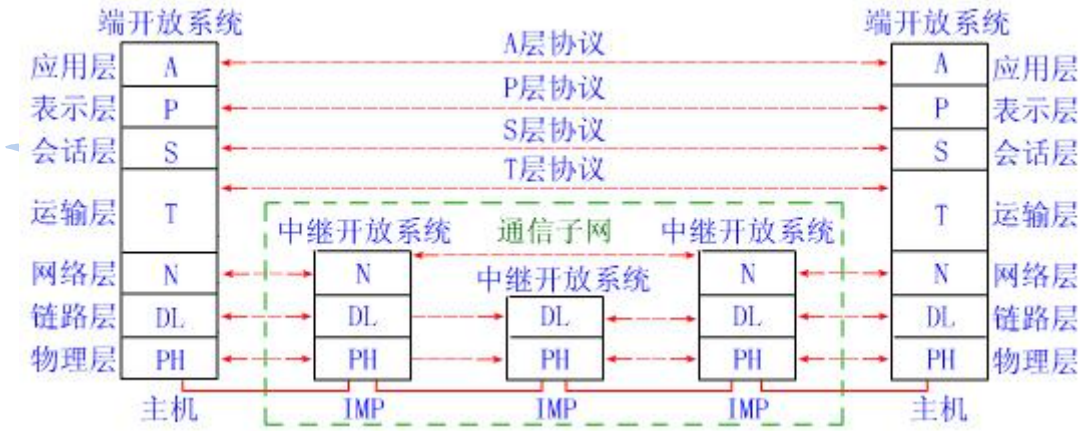


图 3.3 ISO’s OSI 参考模型

从图中可见,整个开放系统环境由作为信源和信宿的端开放系统及若干中继开放系统通过物理媒体连接构成。这里的端开放系统和中继开放系统，都是国际标准 OSI7498 中使用的术语。通俗地说，它们变相当于资源子网中的主机和通信子网中的节点机(IMP)。只有在主

机中才可能需要包含所有七层的功能，而在通信子网中的 IMP 一般只需要最低三层甚至只要最低两层的功能就可以了。

2.层次结构模型中数据的实际传送过程如图 3.4 所示。图中发送进程送给接收进程和数据，实际上是经过发送方各层从上到下传递到物理媒体；通过物理媒体传输到接收方后，再经过从下到上各层的传递，最后到达接收进程。

在发送方从上到下逐层传递的过程中，每层都要加上适当的控制信息，即图中和 H7、H6、...、H1，统称为报头。到最底层成为由“0”或“1”组成和数据比特流，然后再转换为电信号在物理媒体上传输至接收方。接收方在向上传递时过程正好相反，要逐层剥去发送方相应层加上的控制信息。

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

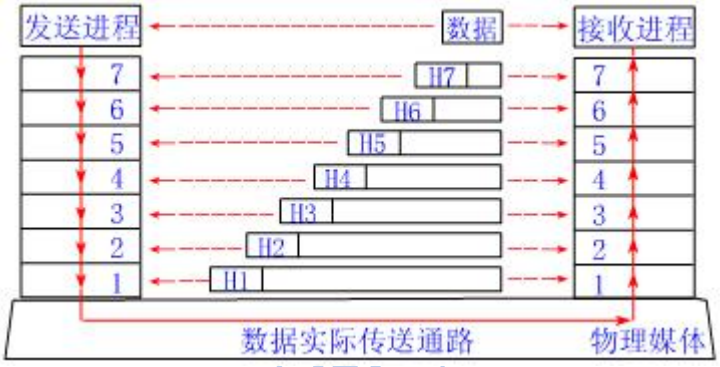


图 3.4 数据的实际传递过程

各层功能简要介绍：

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

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

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

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

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

传最近一个同步点以后的数据。

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

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

3.2 物理层

3.2.1 物理层接口与协议

物理层位于 OSI 参与模型的最低层，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、维持及断开物理信道所需的机械的、电气的、功能性的和规和程性的特性。其作用是确保比特流能在物理信道上传输。

图 3.5 DTE-DCE 接口框图

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

另外，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(Date Terminal Equipment)指的是数据终端设备，是对属于用户所有的连网设备或工作站的统称，它们是通信的信源或信宿，如计算机、终端等；DCE(Date Circuit Terminating Equipment 或 Date Communications Equipment)，指的是数据电路终接设备或数据通信设备，是对为用户提供入接点的网络设备的统称，如自动呼叫应答设备、调制解调器等。

DTE-DCE 的接口框如图 3.5 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。

1.机械特性：

规定了物理连接时对插头和插座的几何尺寸、插针或插孔芯数及排列方式、锁定装置形式等。

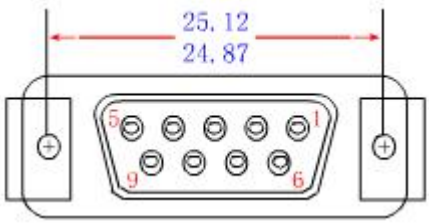


图 3.6 常用连接机械特性

图形 3.6 列出了各类已被 ISO 标准化了的 DCE 连接器的几何尺寸及插孔芯数和排列方式。一般来说，DTE 的连接器常用插针形式，其几何尺寸与 DCE 连接器相配合，插针芯数和排列方式与 DCE 连接器成镜像对称。

2.电气特性：

规定了在物理连接上导线的电气连接及有关的电咱路的特性，一般包括：接收器和发送器电路特性的说明、表示信号状态的电压/电流电平的识别、最大传输速率的说明、以及与互连电缆相关的规则等。

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

(a)非平衡发送器 接收器 (b)非平衡发送器 差动接收器 (c)平衡发送器 差动接收器

图 3.7 电器连接方式

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

1)非平衡方式。 采用分立元件技术设计的非平衡接口，每个电路使用一根导线，收发两个方向共用一根信号地线，信号速率《20kbps，传输距离《15。由于使用共用信号地线，所以会产生比较大的串扰。CCITTV.28 建议采用这种电气连接方式，EIA RS-232C 标准基本与之兼容。

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

3)平衡方式。采用集成集成电路技术设计的平衡接口，使用平衡式发送器和差动式接收器，每个电路采用两根导线，构成各自完全独立的信号回路，使得串扰信号减至最小。这种方式的信号速率<=10Mbps，传输距离为 10m（10Mbps 时）-1000m(<=100kbps 时）。CCITT V.11/X.27 建议采用这种电气连接方式，EAI RS-423 标准与之兼容。

图 3.7 给出这三种电气连接方式的结构。

3.功能特性：

规定了接口信号的来源、作用以及其它信号之间的关系。

4.规程特性：

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

3.2.2 物理层协议举例

1. EIA RS-232C 接口标准

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

RS-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 3.8(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 3.8 RS-232C 的远程连接和近地连接

RS-232C 标准接口也可以如图 3.8(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象是 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。顺便提一下，实际的用户并不一定需要用到 RS-232C 标准的全集，这在个人计算机(PC)高速普及的今天尤为突出，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 3.9，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 等几档)。

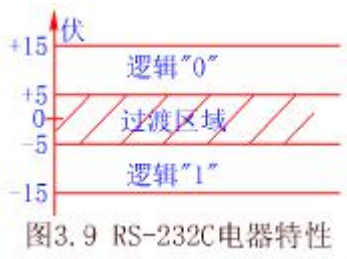


图3.9 RS-232C电器特性

表3.1 RS-232C电器信号表示

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

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 给出了其中最学用的 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 3.10。

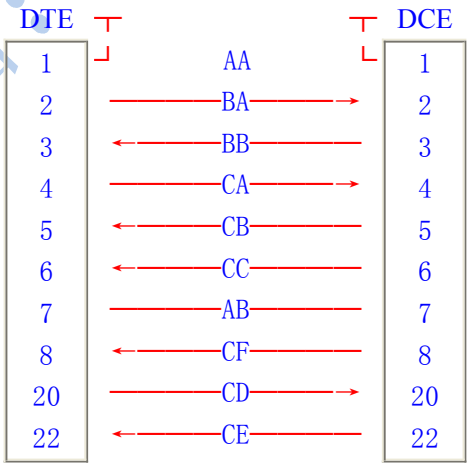


图 3.10 RS-232C 的 DTE-DCE 连接

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 3.11 的方法，图中(a)为完整型连接，(b)为简单型连接。

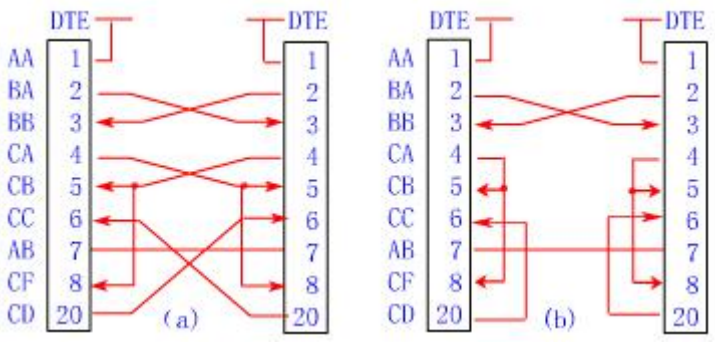


图 3.11 RS-232C 的 DTE-DTE 连接

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。

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(≤20Kbpc)、传输距离短(《15m)、串扰信号较大等缺点。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-499 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，抗串扰能力大大增强。又由于信号电平定义为±6 伏(±2V 为过度区域)的负逻辑，故当传输距离为 10M 时，速率可达 10Mbps；而距离增长至 1000m 时，速率可达到 100Kbps 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 10M 时，速度可达成 100KBPS；距离增至 100M 时，速度仍有 10KBPS。RS-423 的信号最平定义为±6 伏(其中±4 伏为过渡区域)的负逻辑。

从旧技术标准向新技术标准的过渡，需要花费巨大的代价主经过漫长的过程。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. 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，其标准一般都称做建议。

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 200bps～9600bps 时，采用

25 芯标准连接器；传输速率达 48Kbps 时，采用 34 芯标准连接器。200 系列接口标准则采用 25 芯标准连接器。

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

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形式提供了点--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 作为物理层载规约的标准.

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略多于,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.这时的“bis”是法语“替换物”的意思.

X.21 bis 标准指定使用 V.24/V.28 接口,它们与 EIA RS-232D 非常类似.美国的大多数公共数据网应用实际上都使用 EIA RS-232D(或更早的 RS-232C)作为物理层接口.可以认为,X.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。

3.2.3 串行通信编程方法

利用 RS-232C 标准接口可实现两台 PC 之间的异步串行通信。下面分别就 PC 机的 DOS 级和 BIOS 级异步串行通信编程方法做一简单介绍。

1.DOS 级的 PC 通信

PC 机通常配备有两个异步通信端口，分别称作为 COM1 和 COM2，它们都符合 RS-232C 标准。在 DOS 操作系统中，COM1、COM2 被作为 I/O 设备进行管理，COM1、COM2 便是它们的逻辑设备名。据此，DOS 便可通过对 COM1、COM2 的操作来实现 PC 之间的异步串行通信。

DOS 的 MODE 命令可用以设置异步串行端口的参数，DOS 的 COPY 命令允许将异步串行端

口作为一个特殊的“文件”，以对其进行数据传输。下面举一个利用 DOS 的 MODE、COPY 命令，进行双机键盘输入字符传输的例子。

MODE 命令的格式为：

MODE 端口名：数据速率，校验方式，数据位数，停止位位数

其中端口名为 COM1 或 COM2；数据速率可选 150、300、600、1200、2400、4800 或 9600bps；校验方式为 E(偶校验)、O(奇校验)或(无校验)；数据位数为 7 或 8 位；停止位位数为 1 或 2 位。通信双方设置的参数应一致，如双方都键入如下命令

MODE COM1：1200，E，7，1 〈Enter〉

则表示双方以 COM1 为异步通信端口、速率 1200bps、偶校、7 位数据位、1 位停止位的设置参数据进行通信。

DOS 中有一个名为 CON 的标准控制台设备，作为输入时 CON 指的就是键盘，作为输出时 CON 指的就是显示器。准备发送的 PC 机执行如下命令：

COPY CON ：COM1： 〈Enter〉

表示将从键盘收到的信息通过 COM1 串行口发送出去。准备接收的 PC 机执行如下命令：

COPY COM1：CON： 〈Enter〉

则表示将接收来自 COM1 串行口的信息，并在显示器上加以显示。

两台 PC 机分别执行完上述命令后，在发送方键盘上输入的字符便会在接收方显示器上显示出来。

上面介绍的是用 DOS 的 MODE，COPY 命令实现的最简单的 PC 通信。在 MS-DOS 的高版本中(例如 MS-DOSV6.0)还提供了一条 INTERLNK 命令，实际上它是一个通信程序。使用 INTERLNK 命令和一根连接两台 PC 机串行端口的电缆，可以使一台 PC 机从另一台 PC 机的磁盘驱动器中存取数据并运行程序，无需再使用软盘去复制文件。

用以键入命令的 PC 机叫客户机(Client)，与客户机相连的 PC 机叫服务器(Server)。客户机使用服务器的驱动器和打印机，服务器显示两台 PC 机的连机状态。

当两台 PC 机被 INTERLNK 连接以后，服务器上的驱动器便以扩展驱动器的形式映象到客户机上，若两台 PC 机原来均有 A，B，C 三个驱动器，则连接后客户机除了自身的三个驱动器外，又多了 E,F,G(服务器驱动器映象)三个扩展驱动器，客户可以象使用自己的驱动器一样使用这些扩展驱动器。

使用 INTERLNK 时，每台 PC 机上至少要有一个空闲的串行口，还要一根 3 导线或 7 导线的零调制调解器(Null MODEM)串行电缆线，客户机上至少有 16K 空闲内存，服务器上至少有 130K 空闲内存。

在客户机的系统配置文件 CONFIG.SYS 中添加如下命令：

DEVICE=C：\DOS\INTERLNK.EXE/DRIVES:5

再重新启动客户机，便可装入 INTERLNK。这里假设 INTERLNK.EXE 已存在于客户机 C 驱动器的 DOS 目录中，/DRIVERS:5 参数用于映象 5 个服务器驱动器，缺省情况下为 3 个驱动器。

服务器上启动 INTERLNK 不需对其 CONFIG.SYS 作任何改动，只需在 DOS 命令提示符下键入 INTERLNK 即可。此时，屏幕底下出现一行状态信息，显示出 INTERLNK 的连接状态。

关于 DOS 级通信命令的详细使用方法，可参阅有关 DOS 手册。

2.BIOS 级的 PC 通信

PC 级的基本输入输出系统(BIOS)总的中断 14H 提供了异步串行端口的四种通信服务功能，通过之种功能，可以访问串行通信端口，实现连机通信。INT 14H 的串行端口通信功能为：

功能号 功能

00 通信端口初始化

01 向通信端口写一个字符

02 从通信端口读一个字符

03 返回通信端口状态

INT 14H 的一般汇编语言调用顺序如下:

```
MOV AH, <功能号>
MOV DX, <端口号>
```

(在相应寄存器中装入与功能有关的参数)

```
INT 14H
```

(1)初始化通讯端口

调用: AH = 00H

AL = 初始化参数

DX = 端口号(COM1 为 0, COM2 为 1)

返回: AH = 通信端口状态

AL = 调制解调器状态

初始化参数为 8 为二进制数,其中各位的含义如图 3.12 所示。

图 3.12(P61)

若置 COM1 为 9600bps,8 位数据位,1 位停止位,无奇偶校验,指初始化参数为 11100011B,即 0E3H。程序调用如下:

```
MOV AH, 0
MOV AL, 0E3H
MOV DX, 0
INT 14H
```

(2)向通信端口输出字符。

用以向指定端口输出一个字符。

调用: AH = 01H

AL = 所要输出的字符

DX = 端口号

返回: 调用后若 AH 的第 7 位为 0, 表示输出成功, AL 内容不变; 若 AH 的第 7 位为 1, 表示输出失败, 此时 AL 的 0~6 位给出端口状态。

```
MOV AH, 01H
MOV DX, 0
MOV AL, '*'
INT 14H
```

(3)从通信端口输入字符

用以从指定端口输入一个字符。

调用: AH = 02H

DX = 端口号

返回: 若 AH 的第 7 位为 0, 表示输入成功, AL 中为输入的字符; 若 AH 的第 7 位为 1, 表示输入失败, AH 的 0~6 位给出端口状态。

若从 COM1 中输入一个字符,假设以有字符从对方发送到本地 PC,只可调用如下程序段:

```
MOV AH, 02H
MOV DX, 0
INT 14H
```

(4)读取通信端口状态

用以读取指定端口的状态

调用：AH = 03H
DX = 端口号
返回：AH = 端口状态
AL = 调制解调器状态
若要读取 COM1 端口状态，只可调用如下程序段：

```
MOV AH，02H
MOV DX，0
INT 14H
```

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 Atention(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记存器设置为缺省的参数值，以便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伙同编编程手段经通信端口发向调制解调器。

3.3 数据链路层

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

3.3.1 数据链路层功能

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

1.帧同步功能

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

(1)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。

面向字节计数的同步规程的典型实例是DEC公司的数字数据通信报协议DDCMP(Digital DataCommunications Message Protocol)。DDCMP采用的帧格式如下：

8	14	2	8	8	8	16	8-131064	16(位)
SOH	Count	Flag	Ack	Seg	Addr	CRC1	Data	CRC2

格式中控制字符SOH标志数据帧的起始。Count字段共有14位，用以指示帧中数据段中数据的字节数，数据段最大长度为8×(214-1)=131064位，长度必须为字节(即8位)的整倍数，DDCMP协议就是靠这个字节计数来确定帧的终止位置的。DDCMP帧格式中的Ask、Seg、Addr及Flag中的第2位。它们的功能分别类似于本节稍后要详细介绍的HDLC中的N(S)、N(S)、Addr字段及P/F位。CRC1、CRC2分别对标题部分和数据部分进行双重校验，强调标题部分单独校验的原因是,一旦标题部分中的Count字段出错,即失却了帧边界划分的依据,将造成灾难性的后果。

由于采用字段计数方法来确定帧的终止边界不会引起数据及其它信息的混淆,因而不必采用任何措施便可实现数据的透明性，即任何数据均可不受限制地传输。

(2)使用字符填充的首尾定界符法。该法用一些特定的字符来定界一帧的起始与终止，本节稍后要介绍的BSC规程便是典型例子。为了不使数据信息位中出现的与特定字符相同的字符被误判为帧的首尾定界符，可以在这种数据字符前填充一个转义控制字符(DLE)以示区别，从而达到数据的透明性。

(3)使用比特填充的首尾定界符法。该法以一组特定的比特模式(如01111110)来标志一帧的起始与终止。本节稍后要详细介绍的HDLC规程即采用该法。为了不使信息位中出现的与该特定模式相似的比特串被误判为帧的首尾标志，可以采用比特填充的方法。比如，采用特定模式01111110，则对信息位中的任何连续出现的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。该法在物理层采用特定的比特编码方法时采用。例如，曼彻斯特编码方法，是将数据比特“1”编码成“高-低”电平对，将数据比特“0”编码成“低-高”电平对。而“高-高”电平对和“低-低”电平对在数据比特中是违法的。可以借用这些违法编码序列来定界帧的起始与终止。局域网IEEE 802标准中就采用了这种方法。违法编码法不需要任何填充技术，便能实现数据的透明性，但它只适用采用冗余编码的特殊编码环境。

由于字节计数法中Count字段的脆弱性(其值若有差错将导致灾难性后果)以及字符填充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。

2.差错控制功能

通信系统必须具备发现(即检测)差错的能力，并采取措施纠正之，使差错控制在所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，向发送方反柜一个接收是否正确的信息，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)来限定接收方发回方反柜消息的时间间隔，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柜信息，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标网络层一次。

有关差错控制的详细内容，将在本节稍后再做介绍。

3.流量控制功能

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

由于收发双方各自使用的设备工作速率和缓冲存储空间的差异，可能出现发送方发送能力大于接收方接收能力的现象，若此时不对发送方的发送速率（也即链路上的信息流量）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。本节稍后将要介绍的 XON/XOFF 方案和窗口机制就是两种常用的流量控制方法。

4.链路管理功能

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

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

3.3.2 差错控制

用以使发送方确认接收方是否正确收到了由它发送的数据信息的方法称为反馈差错控制。通常采用反馈检测和自动重发请求(ARQ)两种基本方法来实现。

1.反馈检测法

反馈检测法也称回送校检法或“回声”法，主要用于面向字符的异步传输中，如终端与远程计算机间的通信。这是一种无须使用任何特殊代码的差错检测法。双方进行数据传输时，

接收方将接收到的数据（可以是一个字符，也可以是一帧）重新发回发送方，由发送方检查是否与原始数据完全相符。若不相符，则发送方发送一个控制字符（如 DEL）通知接收方删去出错的数据，并重新发送该数据；若相符，则发送下一个数据。

反馈检测法原理简单，实现容易，也有较高的可靠性。但每个数据均被传输两次，信道利用率很低。这种差错控制方法一般用于面向字符的异步传输中，因为这种场合下信道效率并不是主要矛盾。

2.自动重发请求法(ARQ 法)

实用的差错控制方法，既要传达室输可靠性高，又要信道利用率高。为此可使发送方将要发送的数据帧附加一定的冗余检错码一并发送，接收方则根据检错码对数据帧进行差错检测，若发现错误，就返回请求重发的应答，发送方收到请求重发的应答后，便重新传送该数据帧。这种差错控制方法就称为自动重发请求法(Automatic Repeat reQuest)，简称 ARQ 法。

ARQ 法仅需返回少量控制信息，便可有效地确认所发数据帧是否正确被接收。ARQ 法有几种实现方案，空闲重发请求(Idle RQ)和连续重发请求(Continuous RQ)是其中最基本的两种方案。

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

①发送方每次仅将当前信息帧作为待确认帧保留在缓冲存储器中；

②当发送方开始发送信息帧时，随即启动计时器；

③当接收方收到无差错信息帧后，即向发送方返回一个确认帧；

④当接收方检测到一个含有差错的信息帧时，便舍弃该帧；

⑤若发送方在规定时间内收到确认帧，即将计时器清零，继而开始下一帧的发送；

⑥若发送方在规定时间内未收到确认帧，(即计时器超时)，则应重发存于缓冲器中的待确认信息帧。

从以上过程可以看出，空闲 RQ 方案的收、发送方仅需设置一个帧的缓冲存储空间，便可有效地实现数据重发并确保接收方接收的数据不会重份。空闲 RQ 方案最主要的优点就是所需的缓冲存储空间最小，因此在链路端使用简单终端的环境中被广泛采用。

(2)连续重发请求(Continuous RQ)。连续重发请求方案是指发送方可以连续发送一系列信息帧，即不用等前一帧被确认便可发送下一帧。这就需要在发送方设置一个较大的缓冲存储空间(称作重发表)，用以存放若干待确认的信息帧。当发送方到对某信息帧的确认帧后便可从重发表中将该信息帧删除。所以，连续 RQ 方案的链路传输效率大大提高，但相应地需要更大的缓冲存储空间。连续 RQ 方案的实现过程如下：

①发送方连续发送信息帧而不必等待确认帧的返回；

②发送方在重发表中保存所发送的每个帧的备份；

③重发表按先进先出(FIFO)队列规则操作；

④接收方对每一个正确收到的信息帧返回一个确认帧；

⑤每一个确认帧包含一个惟一的序号，随相应的确认帧返回；

⑥接收方保存一个接收次序表，它包含最后正确收到的信息帧的序号；

⑦当发送方收到相应信息帧的确认后，从重发表中删除该信息帧的备份；

⑧当发送方检测出失序的确认帧(即第 N 号信息帧和第 N+2 号信息帧的确认帧已返回，而 N+1 号的确认帧未返回)后，便重发未被确认的信息帧。

上面连续 RQ 过程是假定在不发生传输差错的情况下描述的，如果差错出现，如何进一步处理还可以有两种策略，即 GO-DACK-N 策略和选择重发策略。

GO-DACK-N 策略的基本原理是，当接收方检测出失序的信息帧后，要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧；或者当发送方发送了 N 个帧后，若发现该 N 帧的前一个帧在计时器超时后仍未返回其确认信息，则该帧被判为出错或丢失，此时发送方就不得不重新发送出错帧及其后的 N 帧。这就是 GO-DACK-N(退回 N)法名称的由来。因为，对接收方来说，由于这一帧出错，就不能以正常的序号向它的高层递交数据，对其后发送来的 N 帧也可能都不能接收而丢弃。GO-DACK-N 法操作过程如图 3.13 所示。图中假定发送完 8 号帧后，发现 2 号帧的确认返回在计时器超时后还未收到，则发送方只能退回从 2 号帧开始重发。

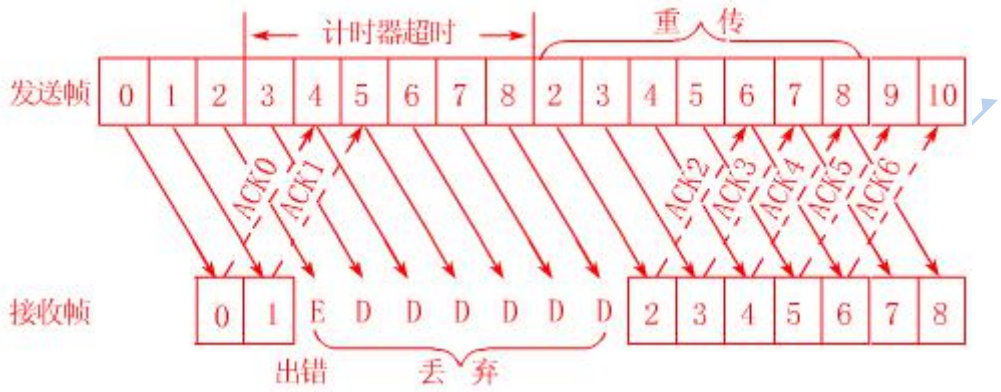


图 3.13 Go-back-N 法举例

GO-DACK-N 可能将已正确传送到目的方的帧再重传一遍，这显然是一种浪费。另一种效率更高的策略是当接收方发现某帧出错后，其后继续送来的正确的帧虽然不能立即递交给接收方的高层，但接收方仍可收下来，存放在一个缓冲区中，同时要求发送方重新传送出错的那一帧。一旦收到重新传来的帧后，就可以原已存于缓冲区中的其余帧一并按正确的顺序递交高层。这种方法称为选择重发(SELECTICE REPEAT)，其工作过程如图 3.14 所示。图中 2 号帧的否认返回信息 NAK2 要求发送方选择重发 2 号帧。显然，选择重发减少了浪费，但要求接收方有足够大的缓冲区空间。

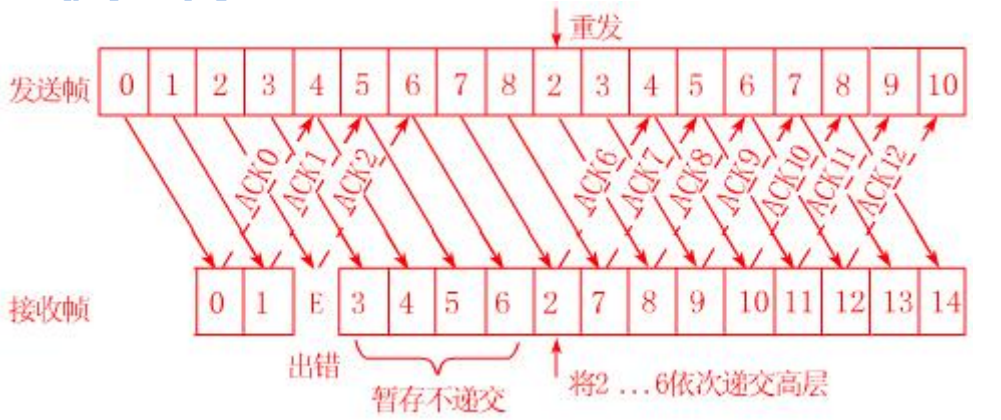


图 3.14 选择重发举例法

3.3.3 流量控制

流量控制涉及链路上字符或帧的发送速率的控制，以使接收方在接收前的足够的缓冲存储空间来接收每一个字符或帧。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 方案和窗口机制。

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 方案方案则是一种相比之下更主动、更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。

2.窗口机制

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

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

不了实现此方案，发送方存放待确认帧的重发表中，应设置待确认帧数目的最大限度，这一限度被称为链路的发送窗口。显然，如果窗口设置为 1，即发送方缓冲能力仅为一个帧，则传输控制方案就回到了空闲 RQ 方案，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、可使用的缓冲存空间以及传输速率等因素。

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

发送方每次发送一帧后，待确认帧的数目便增 1，每收到一个确认信息后，待确认帧的数目便减 1。当重发表长度计数值，即待确认帧的数目等于发送窗口尺寸时，便停止发送新的帧。

一般帧号只取有限位二进制数，到一定时间后就又反复循环。若帧号配 3 位二进制数，则帧号在 0~7 间循环。如果发送窗口尺寸取值为 2。则发送如图 3.15 所示。图中发送方阴

影部分表示打开的发送窗口，接收方阴影部分则表示打开的接收窗口。当传送过程进行时，打开的窗口位置一直在滑动，所以也称为滑动窗口(Slidding Window)，或简称为滑窗。

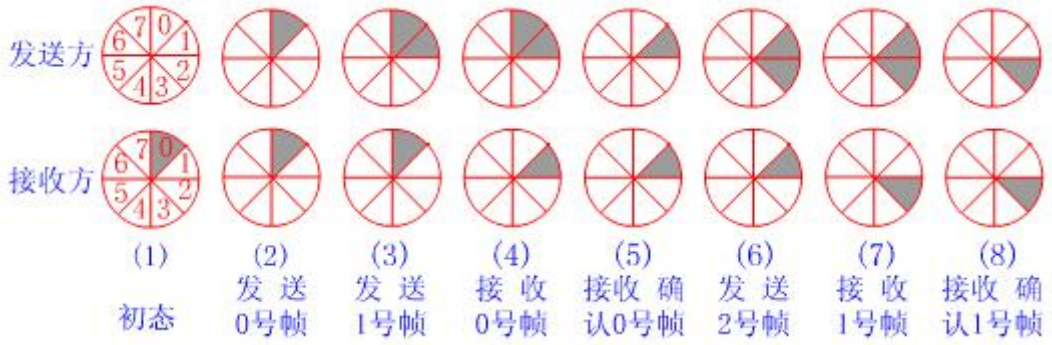


图 3.15 滑动窗口状态变化过程

图3.15中的滑动窗口变化过程可叙述如下(假设发送窗口尺寸为2,接收窗口尺寸为1)：

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

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

③发送方在未收到 0 号帧的确认返器信息前，继续发送 1 号帧。此时，1 号窗口打开，表示 1 号帧也属等待确认之列。至昆，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，在未收到新的确认返回帧之前，发送方将暂停发送新的数据帧，此时接收窗口状态仍不变；

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

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

一般来说，凡是在一定范围内到达的帧，即使它们不按顺序，接收方也要接收下来。若把这个范围看成是接收窗口的话，由接收窗口的大小也应该是大于 1 的。而 Go-back-N 正是接收窗口等于 1 的一个特例，选择重发也可以看做是一种滑动窗口协议，只不过其发送窗口和接收窗口都大于 1。若从滑动窗口的观点来统一看待空闲 RQ、Go-back-N 及选择重发三种协议，它们的差别仅在于各自窗口尺寸的大小不同而已：

空闲 RQ：　　发送窗口=1，接收窗口=1；

Go-back-N：　发窗口>1，接收窗口>1；

选择重发：　发送窗口>1,接收窗口>1。

若帧序号采用 3 位二进制编码，由最大序号为 Smax=2^3-1=7。对于有序接收方式，发送窗口最大尺寸选为 Smax；对于无序接收方式，发送窗口最大尺寸至多是序号范围的一半。发送方管理超时控制的计时器数应等于缓冲器数，而不是序号空间的大小。

3.3.4 数据链路控制协议举例

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

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

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

同步协议又可分为面向字符的同步协议、面向比特的同步协议及面向字节计数的同步协议三种类型。其中面向字节计数的同步协议在本节前面的帧同步功能中已做了较详细的介绍，下面介绍另两种同步协议。

1. 面向字符的同步控制协议

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

任何链路层协议均可由链路建立、数据传输和链路拆除三部分组成。位实现建链、拆链等链路管理以及同步等各种功能，除了正常传输的数据块和报文外，还需要一些控制字符。BSC 协议用 ASCII 和 EBCDIC 字符集定义的传输控制字符来实现相应的功能。这些传输控制字符的标记、名字及 ASCII 码值和 EBCDIC 码值见表 3.3。

表 3.3　　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 test):文始，标志标题信息的结束和报关文本的开始。

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。

BSC 协议将在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，发送方收到反回的确认后，才能发送下一个数据块。

BSC 协议的数据块有如下四种格式：

(1)不带报头的单块报文或分块传输中的最后一块报文：

SYN	SYN	STX	报文	ETX	BCC

(2)带报头的单块报文：

SYN	SYN	SOH	报头	STX	报文	ETX	BCC

(3)分块传输中的第一块报文：

SYN	SYN	SOH	报头	STX	报文	ETB	BCC

(4)分块传输中的中间报文：

SYN	SYN	STX	报文	ETB	BCC

BSC 协议中所有发送的数据均跟在至少两个 SYN 字符之后，发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库而不是字符串时，二进制数据中形同传输控制字符的比特串将会引起传输混乱。为使二进制数据中允许出现与传输控制字符相同的数据(即数据的透明性)，可在各帧中真正的传输控制字符(SYN 除外)前加上 DLE 转义字符，在发送时，若文本中也出现与 DLE 字符相同的二进制比特串，则可插入一个外加以标记。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，用做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，它的链路伟传输效率很低。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。

2、面向比特的同步协议

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

(1)HDLC 的操作方式。HDLC 是通用的数据链路控制协议，在开始建立数据链路时，允许选用特定的操作方式。所谓操作方式，通俗地讲就是某站点是以主站点方式操作还是以从站方式操作，或者是二者兼备。 链路上用于控制目的的站称为主站，其它的受主站控制的站称为从站。主站对数据流进行组织，并且对链路上的差错实施恢复。由主站发往从站的帧称为命令帧，而从从站返回主站的帧称为响应帧。连有多个站点的链路通常使用轮询技术，轮询其它站的站称为主站，而在点-点链路中每个站均可为主站。主站需要比从站有更多的逻辑功能，所以当终端与主机相连时，主机一般总是主站。在一个站连接多个链路的情况下，该站对于一些链路而言可能是主站，而对于一些链路而言又可能是从站。有些站可兼备主站和从站的功能，这种站称为组合站，用于组合站之间信息传输的协议是对称的，即在链路上主、从站具有同样的传输控制功能，这又称作平衡操作。相对的，那种操作时有主站、从站之分的，且各自功能不同的操作，称为非平衡操作。

HDLC 中常有的操作方式有以下三种：

①正常响应方式 NRM(Norma Responses Model) 。这是一非平衡数据链路方式，有时也称非平衡正常响应方式。该操作方式适用于面向终端的点—点或一点与多点的链路。在这种操作方式中，传输过程由主站启动，从站只有收到主站某个命令帧后，才能作出响应向主站传输信息。响应信息可以由一个或多个帧组成，若信息由多个帧组成，则应指出哪一个是最后一帧 。主站负责整个链路，且具有轮询、选择从站及向从站发送命令的权利，同时也负责对超时、重发及各类恢复操作的控制。

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

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

(2)HDLC 的帧格式。在 HDLC 中，数据和控制报文均以帧的标准格式传送。HDLC 中的帧类似于 BSC 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，其格式如下：

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

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

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

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

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

⑤帧校验序列字段(FCS)：帧校验序列字段可以使用 16 位 CRC，对两个标志字段之间的整个帧的内容进行校验。FCS 的生成多项式由 CCITT V.41 建议规定为 X16+X12+X5+1。

(3)HDLC 的帧类型。HDLC 有信息帧(I 帧)、监控帧(S 帧)和无编号帧(U 帧)三种不同类型的帧，各类帧中控制字段的格式及比特定义如下表 3.4:

控制字段位	1	2	3	4	5	6	7	8
I 格式	0	N(S)			P	N(R)		
S 格式	1	0	S1	S2	P/F	N(R)		
U 格式	1	1	M1	M2	P/F	M3	M4	M5

控制字段中的第 1 位或第 1、第 2 位表示传送帧的类型。第七位是 P/K 位，即轮询/终止(Poll/Final)位。当 P/F 位用于命令帧(由主站发出)时，起轮询的作用，即当该位为“1”时，要求被轮询的从站给出响应，所以此时 P/F 位可称轮询位(或 P)；当 P/F 位用于响应帧(由从站发出)时，称为终止位(或 F 位)，当其为“1”时，表示接收方确认的结束。为了进行连续传输，需要对帧进行编号，所以控制字段中严寒包括了帧的编号。

①信息帧(I 帧)：信息帧用于传送有效信息或数据，通常简称 I 帧。I 帧以控制字段第三者位为“0”来标志。信息帧控制字段宫的 N(S)用于存放发送帧序号，以使发送方不必等待确认而连续发送多帧。N(R)用于存放接收方下一个预期要接收的帧的序号，如 N(R)=5，即表示接收方下一帧要接收 5 号帧，换言之，5 号帧前的各帧接收方都已正确接收到。N(S)和 N(R)均为 3 位二进制编码，可取值 0~7。

②临控帧(S 帧)：监控帧 用于差错控制和流量控制，通常简称 S 帧。S 帧以控制字段第 1、2 位为“10”来标志。S 帧不带信息字段，帧长只有 6 个字节即使 8 个比特。S 帧的控 制字段的第 3、4 位为 S 帧类型编码，共有四种不同组合，分别表示：

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

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

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

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

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

③无编号帧(U 帧)：无编号帧因其控制字段中不包含编号 N(S)和 N(R)而得名，简称 U 帧。U 帧用于提供对链路的建立、拆除以及多种控制功能，这些控制功能用于个 M 位(M1~M5，也称修正位)来定义，可以定义气 32 种附加的命令或应答功能。

3.4 网络层

网络层是 OSI 参考模型中的第三层,介于运输层和数据链中路层之间。它在数据路层提供的两个相邻端点之间的数据帧的传送功能上，进一步管理网络中的数据通信，将数据设法从源端经过若干个中间节点传送到目的端,从而向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(也即通信子网)中最为复杂、关键的一层。

网络层的目的是实现两个端系统之间的数据透明传送，具体功能包括路由选择、阻塞控制和网际互连等。

3.4.1 通信子网的操作方式和网络层提供的服务

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

虚电路的数据报两种方式。

1.虚电路操作方式

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

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

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

为使节点能区分一个分组属于哪条虚电路，每个分组必须携带一个逻辑信道；同样，同一条虚电路的分组在各段逻辑信道上的逻辑信道可能也不相同。传输中，当一个分组到达节点时，节点根据其携带的逻辑信道号查找虚电路表，以确定该分组应发往的下一个节点及其下一段信道上所占用的逻辑信道号，有该逻辑信道号替换分组中原先的逻辑信道号后，再将该分组发往下一个节点。

各节点的虚电路表是在虚电路建立过程中建立的。比如，与 A 节点相连的源端系统要经中间节点 B、C 跟与 D 节点相连的目的端系统建立一条虚电路，源端系统可发出一个呼叫请求分组，该分组除了包含目的地址外，还包含源端系统所选取的不用的最小逻辑信道号 N。A 节点收到请求分组后在 A 节点与下一节点 B 间所有已使用的逻辑信道号之外选取一个最小编号 NA，并将请求分组中的逻辑信道 N 替换成该逻辑信道号 NA，再将分组成发送给节点 B。此后的各节点依次逐个根据自身实际情况选取新的逻辑信道号(如 NB、NC、ND 等)来替换收到的分组中的逻辑信道号。最后，目的节点 D 将请求分组传送给连接它的端系统。在此过程中，每个节点的虚电路表中要记录两个逻辑信道：前一个节点所选取的逻辑信道号和本节点所选取的逻辑信道号。这样便使得虚电路所跨越的每一段连接上的逻辑信道号都是唯一的。

图 3.16 给出一个虚电路表建立的示例，这里假设建立了 6 条虚电路。由于虚电路上的数据是双向传输的，为保证两节点之间正、反两个方向的虚电路不相混淆，在一个节点选取逻辑信道号来替换其前一节点的逻辑信道号时，不仅要考虑与下一节点之间的逻辑信道号不相同，还在考虑与下一节点作为另一个条反向虚电路的上一节点头时所选取的逻辑信道号相区别。例如，在建立虚电路 1-BAE 时(这里 1-BAE 表示源节点为 B，建立虚电路时选取 1 为逻辑信道号，并经 A 传送到 E)，在节点 B 中，尽管 A 节点是第一次作为 B 节点的下一节点，但由于虚电路 0-ABCD 中 A 到 B 间已使用了逻辑信道号 0，因此在出路一栏选 B 到 A 间的逻辑信道号为 1。这样，当从节点 A 发来一个分组时，若它所携带的逻辑信道号为 0，刚说明是虚电路 ABCD 上的正向分组；若为 1，则说明虚电路 BAE 上的反向分组。对于虚电路 2-BFE 的建立也是同样情况。

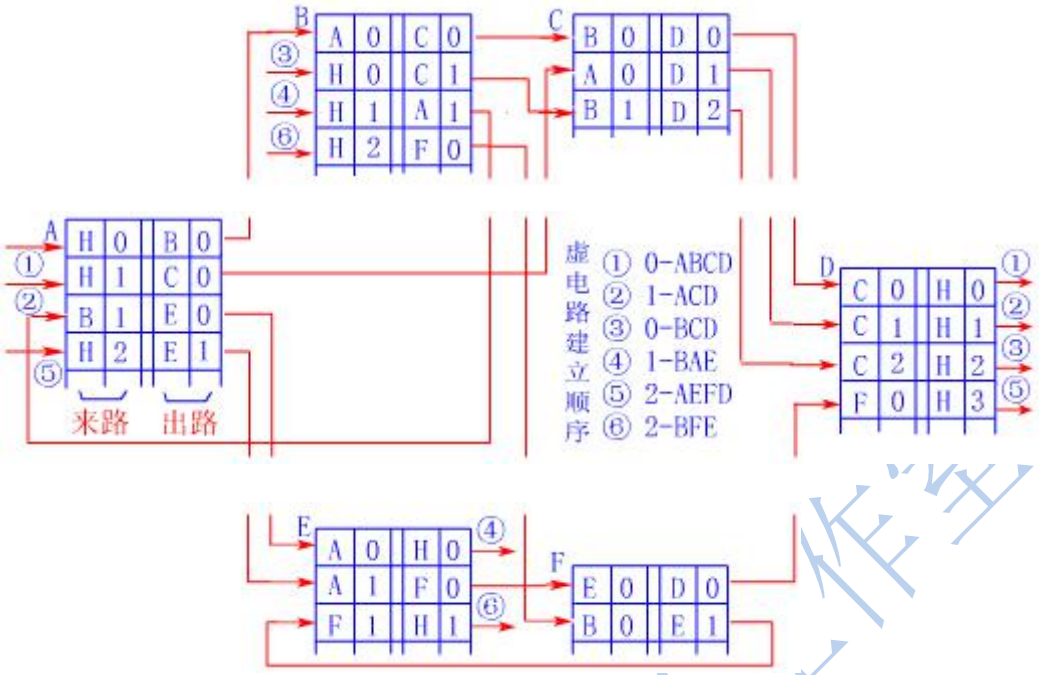


图 3.16 虚电路建立示例

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

2.数据报操作方式

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

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

3.虚电路服务

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

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

上述虚电路的服务是网络层向运输层提供的服务，也是通信子网端向系统提供的网络服务。但是，提供这种虚电路服务的通信子网内部的实际操作既可是虚电路方式的，也可以是数据报方式的。以虚电路操作方式的网络，一般总是提供虚电路服务。OSI 中面向连接的网络服务就是虚电路服务。在虚电路操作方式，端系统的网络层同通信子网节点的操作是一致

的。SNA 就是采用这种虚电路操作支持虚电路服务方式的实例。

以数据报方式操作的网络,也可以提供虚电路服务,即通信子网内部节点按数据报方式交换数据,而与端系统相连的网络节点则向端系统提供虚电路报务.对于端系统来说,它的网络层与节点间通信仍像虚电路操作方式的网络节点间一样,先建立虚电路,再交换数据分组,最后拆除电路.但实际上,每个分组被网络节点分成若干个数据报,附加上地址、序号、逻辑信道等信息分送到目的节点。目的节点再将数据报进行排序，拼成原来的分组，送给目的端系统。因此，源端系统和源网络节点之间、目的节点和目的端系统之间的网络层按虚电路操作方式交换分组，而目的节点和源节点之间则按数据报交方式完成分组的交换。尽管通信子网的数据报交换是不可靠的，但是两端原网络节点做了许多诸如排序、重发等额外工作，从而满足了虚电路服务的要求。例如，在 ARPANET 中，其内部使用数据报操作方式，但可以向端系统提供数据报和虚电路两种服务。

4.数据报服务

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

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

3.4.2 路由选择

通信子网为网络源节点和目的节点提供了多条传输路径的可能性。网络节点在收到一个分组后后，要确定向下一节点传送的路径，这就是路由选择。在数据报方式中，网络节点要为每个分组路由做出选择；而在虚电路方式中，只需在连接建立时确定路由。确定路由选择的策略称路由算法。

设计路由算法时要考虑诸多技术要素。首先，考虑是选择最短路由还是选择最佳路由；其次，要考虑通信子网是采用虚电路的还是采用数据报的操作方式；其三，是采用分布式路由算法，即每节点均为到达的分组选择下一步的路由，还是采用集中式路由算法，即由中央节点或始发节点来决定整个路由；其四，要考虑关于网络拓朴、流量和延迟等网络信息的来源；最后，确定是采用静态路由选择策略，还是动态路由选择策略。

1.静态路由选择策略

静态路由选择策略不用测量也不需利用网络信息,这种策略按某种固定规则进行路由选择，其中还可分为泛射路由选择、固定路由选择和随机路由选择三种算法。

(1)泛射路由选择法。这是一种最简单的路由算法。一个网络节点从某条线路收到一个分组后，再向除该线路外的所有线路重复发送收到分组。结果，最先到达目的的节点的一个或若干个分组肯定经过了最短的路径，而且所有可能的路径都被尝试过。这种方法用于诸如军事网络等强壮性要求很高的场合。即使有的网络节点遭到破坏，只要源、目间有一条信道存在，则泛射路由选择仍能保证数据的可靠传送。另外，这种方法也可用于将一个分组数据源传送到所有其它节点的广播式数据交换中。它还可被用来进行网络的最短路径及最短传输延迟的测试。

(2)固定路由选择。这是一种使用较多的简单算法。每个网络节点存储一张表格，表格中每一项记录着对应某个目的节点的下一节点或链路。当一个分组到达某节点时，该节点只要根据分组上的的地址信息，便可从固定的路由表中查出对应的目的节点及所应选择的下一节点。一般，网络中都有一个网络控制中心，由它按照最佳路由算法求出每对源、目节点的最佳路由，然后为每一节点构造一个固定路由表并分发给各个节点。固定路由选择法的优点是简便易行，在负载稳定，拓扑结构变化不大的网络中运行效果很好。它的缺点是灵活性差，无法应付网络中发生的阻塞和故障。

(3)随机路由选择。在这种方法中，收到分组的节点，在所有与之相邻的节点中为分组随机选择出一个节点。方法虽然简单，但实际路由不是最佳路由，这会增加不必要的的负担，而且分组传输延迟也不可预测，故此法应用不广。

2.动态路由选择策略

节点的路由选择要依靠网络当前的状态信息来决定的策略，称动态路由选择策略。这种策略能较好地适应网络流量、拓扑结构的变化，有利于改善网络的性能。但由于算法复杂，会增加网络的负担。独立路由选择、集中路由选择和分布路由选择是三种动态路由选择策略的具体算法。

(1)独立路由选择。在这类路由算法中，节点不仅根据自己搜集到的有关信息做出路由选择的决定，与其它节点不交换路由选择信息。这种算法虽然不能正确确定距离本节点较远的路由选择，但还是能较好地适应网络流量和拓扑结构的变化。一种简单的独立路由选择算法是 Baran 在 1964 年提出的热土豆(Hot Potato)算法：当一个分组到来时，节点必须尽快脱手，将其放入输出队列最短的方向上排队，而不管该方向通向何方。

(2)集中路由选择。集中路由选择也像固定路由选择一样，在每个节点上存储一张路由表。不同的是，固定路由选择算法中的节点路由表由人工制作，而在集中路由选择算法中的节点路由表由路由控制中心 RCC(Routing Control Center)定时根据网络状态计算、生成并分送到各相应节点。由于 RCC 利用了整个网络的信息，所以得到的路由选择是完美的，同时也减轻了各节点计算路由选择的负担。

(3)分布路由选择。在采用分布路由选择算法的网络中，所有节点定期地与其每个相邻节点交换路由选择信息。每个节点均存储一张以网络中其它节点为索引的路由选择表，，网络中每个节点占用表中一项。每一项又分为两个部分，一部分是所希望使用的到目的节点的输出线，另一部分是估计到目的的节点所需要的延迟或距离。度量标准可以是毫秒或链路段数、等待的分组数、剩余的线路和容量等。

3.4.3 阻塞控制

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

网络的吞吐量与通信子网负荷(即通信子网中正在传输的分组数)有着密切的关系。当通信子网负荷比较小时，网络的吞吐量(分组数/秒)随网络负荷(每个节点中分组的平均数)的增加而线性增加。当网络负荷增加到某一值后，若网络吞吐量反而下降，则表征网络中出现了阻塞现象。在一个出现阻塞现象的网络中，到达某个节点的分组将会遇到无缓冲区可用的情况，从而使这些分组不得不由前一节点重传，或者需要由源节点或源端系统重传，从而使通信子网的有效吞吐量下降。由此引起恶性循环，使通信子网的局部甚至全部处于死锁状态，最终导致网络有效吞吐量接近为零。

1.阻塞控制方法

(1)缓冲区预分配方法。该法用于虚电路分组交换网中。在建立虚电路时，让呼叫请求分组的途经的节点为虚电路预先分配一个或多个数据缓冲区。若某个节点缓冲器已被占满，则呼叫请求分组另择路由，或者返回一个“忙”信号给呼叫者。这样，通过途经的各个节点为每条虚电路开设的永久性缓冲区(直到虚电路拆除)，就总能有空间来接纳并转送经过的分组。此时的分组交换跟电路交换很相似。当节点收到一个分组并将它转发出去之后，该节点向发送节点返回一个确认信息。该确认一方面表示接收节点已正确收到分组，另一方面告诉发送节点，该节点已空出缓冲区以备接收下一个分组。上面是“等一等”协议下的情况，若节点之间的协议允许多个未处理的分组存在，则为了完全消除阻塞的可能性，每个节点要为每条虚电路保留等价于窗口大小数量的缓冲区。这种方法不管有没有通信量，都有可观的资源(线路容量或存储空间)被某个连接占有，因此网络资源的有效利用率不高。这种控制方法主要用于要求高带宽和低延迟的场合，例如传送数字化语音信息的虚电路。

(2)分组丢弃法。该法不必预先保留缓冲区，当缓冲区占满时，将到来的分组丢弃。若通信子网提供的是数据报服务，则用分组丢弃法来防止阻塞发生不会会引起大的影响。但若通信子网提供的是虚电路服务，则必须在某处保存被丢弃分组的备份，以便阻塞解决后能重新传送。有两种解决被丢弃分组重发的方法，一种是让发送被丢弃分组的节点超时，并重新发送分组直至分组被收到；另一种是让发送被丢弃分组的节点在一定次数后放弃发送，并迫使数据源节点超时而重新开始发送。但是不加分辨地随意丢弃分组也不妥，因为一个包含确认信息的分组可以释放节点的缓冲区，若因节点无空余缓冲区来接收含确认信息的分组，这便使节点缓冲区失去了次释放的机会。解决这个问题的方法可以为每条输入链路永久地保留一块缓冲区，以用于接纳并检测所有进入的分组，对于捎带确认信息的分组，在利用了所捎带的确认释放缓冲区后，再将该分组丢弃或将该捎带好消息的分组保存在刚空出的缓冲区中。

(3)定额控制法。这种方法在通信子网中设置适当数量的称做“许可证”的特殊信息，一部分许可证在通信子网开始工作前预先以某种策略分配给各个源节点，另一部分则在子网开始工作后在网中四处环游。当源节点要发送来自源端系统的分组时，它必须首先拥有许可证，并且每发送一个分组注销一张许可证。目的节点方则每收到一个分组并将其递交给目的端系统后，便生成一张许可证。这样便可确保子网中分组数不会超过许可证的数量，从而防止了阻塞的发生。

2.死锁及其防止

阻塞的极端后是死锁。死锁是网络中最容易发生的故障之一，即使在网络负荷不很重时也会发生.死锁发生时,一组节点由于没有空闲缓冲区而无法接收和转发分组,节点之间相互等待,既不能接收分组也不能转发分组,并一直保持这一僵局,严重时 至导致整个网络的瘫痪.此时,只能靠人工干预来重新启动网络,解除死锁.但重新启动后并未消除引起死锁的隐患,所以可能再次发生死锁.死锁是由于控制技术方面的某些缺陷所引起的,起因通常难以捉摸、难以发现，即使发现，也常常不能立即修复。因此，在各层协议中都必须考 如何避免死锁问题。

(1)存储转发死锁及其防止。最常见的死锁是发生在两个节点之间的直接存储转发死锁。例如，A 节点的所有缓冲区装满了等待输出到 B 节点的分组，而 B 节点的所有缓冲区也全部装满了等待输出到 A 节点的分组；此时，A 节点不能从 B 节点接收分组，B 节点也不能从 A 节点接收分组，从而造成两节点间的死锁。这种情况也可能发生在一组节点之间，例如，A 节点企图向 B 节点发送分组、B 节点企图向 C 节点发送分组，这种情形称做间接存储转发死锁。当一个节点处于死锁状态时，所有与之相连的链路将完全被阻塞。

一种防止存储处于死锁的方法是，每个节点设置 M+1 个缓冲区，并以 0 到 M 编号。M 为

通信子网的直径，即从任一源节点到任一目的节点间的最大链路段数。每个源节点仅当其为0号缓冲区时才能接收源端系统来的分组，而此分组仅能转发给1号缓冲区空闲的相邻节点，再由该节点将分组转发给它的2号缓冲区空闲的相邻节点.....最后，该公组或者顺利到达目的节点并被递交给目的端系统，或者到了某个节点编号为M 的缓冲区中再也转发不下去，此时一定发生了循环，应该将该分组丢弃。由于每个分组都是接照编号递增规则分配缓冲区，所以节点之间不会相互等待空闲缓冲区而发生死锁现象。这种方法的不足之处在于，当某节点虽然有空闲缓冲区，但正巧没有所需要的特性编号的缓冲区时，分组仍要等待，从而造成了缓冲区和链路的浪费。

另一种防止存储转发死锁的方法是，使每个分组上都携带一个全局性的惟一的“时间戳”，每个节点要为每条链路保留一个特殊的接收缓冲区，而其它缓冲区均可用于存放中转分组。在每条输出链路的队列上分组时间戳顺序排队。例如，节点A要将分组送到节点B，若B节点没有空闲缓冲区，但正巧有要送到A节点的分组，此时A、B节点可通过特殊的接收缓冲区交换分组；若B节点既没有空闲缓冲区，也没有要送到A节点的分组，B节只好强行将一个出路方向大致与A节点方向相同的分组与A节点互相交换分组，但此时A节点中的分组必须比B节点中的分组具有更早的时间戳，这样才能保证子网中某个最早的分组不受阻挡地转发到目的地。由此可见，每个分组最终总会成为最早的分组，并总能一步一步地发送到目的节点，从而避免了死锁现象的发生。

(2)重装死锁及其防止。死锁中比较严重的情况是重装死锁。假设发给一个端系统的报文很长，被源节点拆成若干个分组发送，目的节点要将所有具有相同编号的分组重新装配成报文递交给目的端系统，若目的节点用于重装报文的缓冲区空间有限，而且它无法知道正在接收的报文究竟被拆成多少个分组，此时，就可能发生严重的问题：为了接收更多的分组，该目的节点用完了它的缓冲空间，但它又不能将尚未拼装完整的报文递送给目的端系统，而邻节点仍在不断地向它传送分组，但它却无法接收。这样，经过多次尝试后，邻节点就会绕道从其它途径再向该目的节点传送分组，但该目的节点已被死锁，其周边区域也由此发生了阻塞。下面几种方法可用以避免重装死锁的发生：

①允许目的节点将不完整的报文递交给目的端系统；

②一个不能完整重装的报文能被检测出来，并要求发送该报文的源端系统重新传送；

③每个节点配备一个缓冲空间，用以暂存不完整的报文。

①、②两种方法不能很满意地解决重装死锁，因为它们使端系统中的协议复杂化了。一般的设计中，网络层应该对端系统透明，也即端系统不该考虑诸如报文拆、装只类的事。(3)方法虽然不涉及端系统，但使每个节点增加了开销。

3.4.4 X.25 协议

CCITT提出的X.25协议描述了主机(DTE)与分机交换网(PSN)之间的接口标准，使主机不必关心网络内部的操作就能方便地实现对各种不同网络的访问。X。25实际上是DTE与PSN之间接口的一组协议，它包括物理层、数据链路层和分组层三个层次。X。25的分组级相当与OSI参考模型中的网络层，其主要功能是向主机提供多信道的虚电路服务。

1.X.25 分组级的功能

X.25分组级的主要功能是将链路层所提供的连接DTE-DCE的一条或多条物理链路复用成数条逻辑信道，并且对每一条逻辑信道所建立的虚电路执行与链路层单链路协议类似的链路建立、数据传输、流量控制、顺序和差错检测、链路的拆除等操作。利用X。25分组级协议，可向网络层的用户提供多个虚电路连接，使用户可以同时与公用数据网中若干个其它X。25数据终端有用户(DTE)通信。

X.25提供虚呼叫和永久虚电路两种虚电路服务，虚呼叫即需要呼叫建立与拆除过程的虚电路服务，永久虚电路即在接入是由协商指定的不需要呼叫建立与拆除过程的虚电路服

务。每条虚电路都要赋予一个虚电路号，X.25 中的虚电路号由逻辑信道组号(0～15)和逻辑信道号(0～255)组成。用于虚呼叫的虚电路号范围和永久虚电路的虚电路号应在签定服务时与管理部门协商确定与分配。

公用数据网有虚电路和数据报两种操作方式，尽管有些网络体系结构(如 Ethernet)仍在使用数据报技术，但数据报服务已在 1980 年的修订中被从 X。25 标准中删去，取而代之的是一个称做快速(Fast Select)的可选扩充服务。

X.25 所规定的虚电路服务属于面向连接的 OSI 服务方式，这正好符合 OSI 参考模型中的网络层服务标准定义，这就为公用数据网与 OSI 结合提供了可能性。OSI 网络层的功能是提供独立于运输层的中继和路由选择以及其它以之相关的功能。在面向连接的网络层服务中，要进行通信的网络层实体必须首先建立连接，这在 X.25 中即为相应的建立虚电路的呼叫建立规程。

2. X.25 分组级分组格式

在分组级上，所有的信息都以分组为基本单位进行传输和处理，无论是 DTE 之间所要传输的数据，还是交换网所用的控制信息，都以分组形式来表示，并按照链路协议穿越 DTE-DCE 界面进行传输。因此在链路层上传输时，分组应嵌入到信息帧(I 帧)的信息字段中，即表示成如下的格式：

标记字段 F	地址字段	控制字段	(分组)	帧校验序列 FCS	标记字段 F

每个分组均由分组头和数据信息两部分组成，其一般格式如图 3.17 所示。

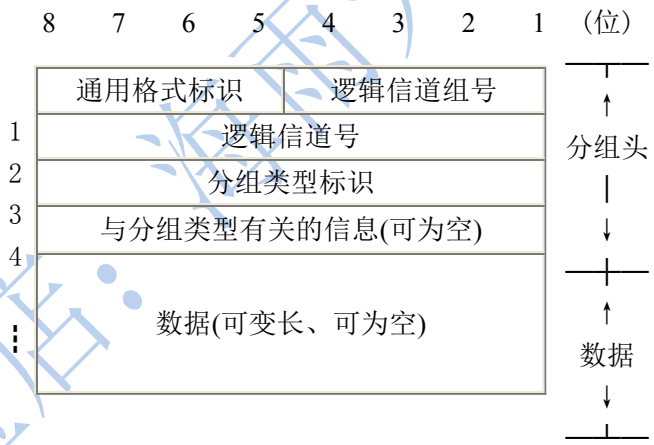


图 3.17 X.25 分组的一般格式

分组格式中的数据部分(可以为空)通常被递交给高层协议或用户程序去处理，所以分组协议中不对它做进一步规定。分组头用于网络控制，主要包括 DTE-DCE 的局部控制信息，其长度随分组类型不同有所不同，但至少要包含前三个字节作为通用格式标识、逻辑信道标识和分组类型标识，它们的含义如下：

(1)通用格式标识(GFI)。由分组中第一个字节的前四位组成，用于标志分组头中其余部分的格式。第一位(b8)称作 Q 位或限定位，只用于数据分组中。这是为了对分组中的数据进行特殊处理而设置的，可用于区分数据正常数据，还是控制信息。对于其它类型的分组，该位恒置为“0”。第二位(b7)称 D 位或传送确认位，设置该位的目的是用来指出 DTE 是否希望用分组接收序号 P(R)来对它所接收的数据做端一端确认。在呼叫建立时，DTE 之间可通过 D 位来商定虚呼叫期间是否将使用 D 位来商定虚呼叫期间是否将使用 D 位规程。第三、四位

(b6、b5)用以指示数据分组的序号是用 3 位即模 8(B5 置“1”)还是 7 位即模 128(b6 置“1”)，这两位或者取“10”，或者取“10”，或者取“01”，一旦选定，相应的分组格式也有所变化。

(2)逻辑信道标识。由第一个字节中和剩余四位(b4、b3、b2、b1)所做的逻辑信道组号(LCGN)和
第二个字节所做的逻辑信道号(LCN)两部分组成，用以标识逻辑信道。

(3)分组类型标识。由第三个字节组成，用于区分分组的类型和功能。若该字节的最后一位(B1)为
“0”，则表示分组为数据分组成；若该位为“1”，则表示分组为控制分组，可以用做呼叫请求或指示分组、释放请求或指示分组。若该字节末三位(b3、b2、b1)为全“1”，则表示该分组是某个确认或接受分组。

第四个字节及其后诸字节将依据分组类型的不同而有不同的定义。

X.25 分组级协议规定了多种类型的分组。由于 DTE 与 DCE 的不对称性，所以具有相同类型编码的同类型分组，因其传输方向的不同的含义和解释，具体实现时也有所不同。为此，分组协议从本地 DTE 的角度出发，为它们取了不同的名称以示区别。一般来说，从 DTE 到 DCE 的分组表示本地 DTE 经 DCE 向远地 DTE 发送的命令请求或应答响应；反之，从 DCE 到 DTE 的分组表示 DCE 代表远地 DTE 向本地 DTE 发送的命令或应答响应。表 3.5 列出了这些分组的名称、分组类型编号及参数。表中的分组类型可归纳为图 3.18 所示的六种格式。

表 3.5　　X.25 分组级分组类型

	分组类型名称		分组类型编号(位)	格式编号
	DTE->DCE	DTE->DCE	8 7 6 5 4 3 2 1	
呼叫建立和清除	呼叫请求	呼叫指示	0 0 0 0 1 0 1 1	①
	呼叫接受	呼叫接通	0 0 0 0 1 1 1 1	⑥
	释放请求	释放指示	0 0 0 1 0 0 1 1	④
	DTE 释放确认	DCE 释放确认	0 0 0 1 0 1 1 1	⑥
数据和中断	DTE 数据	DCE 数据	P(R)　M　P(S) 0	②
	DTE 中断请求	DCE 中断请求	0 0 1 0 0 0 1 1	④
	DTE 中断确认	DCE 中断确认	0 0 1 0 0 1 1 1	⑥
流量控制和复位	DTE RR	DCE RR	P(R)　0 0 0 0 1	③
	DTE RNR	DCE RNR	P(R)　0 0 1 0 1	③
	复位请求	复位请求	0 0 0 1 1 0 1 1	⑤
	DTE 复位确认	DCE 复位确认	0 0 0 1 1 1 1 1	⑥
重启动	重启动请求	重启动指示	1 1 1 1 1 0 1 1	④
	DTE 重启动确认	DCE 重启动确认	1 1 1 1 1 1 1 1	⑥
任选	DTE REJ	DCE REJ	P(R)　0 1 0 0 1	③

①呼叫请求、呼叫指示

0	0	0	1	逻辑信道组号
逻辑信道号				
分组类型				1
主叫地址长度		被叫地址长度		

②数据分组

0	0	0	0	逻辑信道组号
逻辑信道号				
P(R)	M	P(S)		0
数据部分				

DTE 地址				
		0	0	0	0
0	0	补充业务字段长度			
补充业务(0～63 字节)				
呼叫用户数据(0～16/128 字节)				

③流量控制分组

0	0	0	0	逻辑信道组号
逻辑信道号				
P(R)		分类类型		1

④请求、指示分组

0	0	0	1	逻辑信道组号
逻辑信道号				
分组类型				1
原 因				

⑤复位分组

0	0	0	0	逻辑信道组号
逻辑信道号				
分组类型				0
原 因				
诊断码				

⑥确认分组

0	0	0	1	逻辑信道组号
逻辑信道号				
分组类型				0

图 3.18 X.25 分组格式

数据分组中的数据类型编码部分，除了用 M 位代替 I 帧中的 P/F 位外，其它内容与数据链路级的 HDLC 帧格式中的控制字段 C 非常类似，最末位的“0”是数据类型分组的特征位。M(More data)位置“1”，代表还有后续的数据，即当前数据分组中的数据将以同一逻辑信道上的下一数据分组中的数据作为逻辑继续。P(S)P(R)分别称为分组发送顺序号和接收顺序号，它们的作用大致与帧格式中的 N(S)和 N(R)相当。但是，它们的主要作用是控制每条逻辑道上向分组交换网发送或从交换网接收的数据流，而不只为站点子÷之间提供确认手段。其目的是为了调节每个逻辑信道上的流量，以防止对分组交换网的压力过重。实际上，P(S)或 P(R)的值用以确定一个给定的逻辑信道上的“窗口”，表示信道上的允许传送多少个未被响应的分组。能传输未响应分组的最大值称为窗口尺寸，每条虚电路的窗口尺寸是在立户或呼叫建立时分配的，但序号采用 3 位时最大能超过 7 个分组，序号采用 7 位时最大不能超过 127 个分组。

与数据链路级帧格式一样，分组级也包括 RR、RNR 和 REJ 三种分组，它们被称为流量控制分组，这些分组中的类型字段只包括接收顺序号 P(R)，而无发送顺序号 P(S)。RR 用于告知对方本方正在准备从给定逻辑信道上接收顺序号为 P(S)的分组；RNR 用于向对方表示本方目前不能在给定的逻辑信道上接收数据分组。RNR 可以通过同一方向上发送的 RR 分组加以清除。

另外，分组级也包括一些无编号的分组。如是中断请求分组，它不需要等待事先已发送的其它分组而能立即向外发送，甚至在对方不能接收数据时也能发送。中断请求分组只能携带一个字节的用户数据，放在原因字段中用以向对方传送中断信息或原因。

X.25 中还定义了很多其它类型的分组，包括释放请求/指示、复位请求/指示、重启动请求/指示等。其中除复位请求/指示分组多下个诊断代码外，其它均与中断请求分组格式相同。这些分组都包括一个“原因”字段，用以存入引入相应动作的原因。需要说明一下复位与重启动之间的差别。复位请求是为了在数据传输状态中对虚电路进行重初始准备而设置的；而重启动则为同时释放 DTE-DCE 界面上所有虚呼叫以及复位所有永久虚电路而设置的。

各类确认分组仅包含三个字节，它们分别用做对呼叫、释放、中断、复位及重启动的请求或指示的确认。

3.4.5 网际互连

1.网际互连原理

网际互连的目的是使一个网络上的用户能访问其它网络上的资源，使不同网络上的用户互相通信和交换信息。这不仅有利于资源共享，也可以从整体上提高网络的可靠性。

要实现网际互连，必须：

(1)在网络之间至少提供一条物理上连接的链路，并具有对这条链的控制规程；

(2)在不同网络的进程之间提供合适的路由实现数据交换；

(3)有一个始终记录不同网络使用情况并维护该状态信息的统一的记费服务；

(4)在提供以上服务时，尽可能不对互连在一起的网络的体系结构做任何修改。

互连的网络在体系结构、层次协议及服务等方面或多或少存在着差异，对于异构网来说(例如各种类型的局域网)差异就更大。这种差异可能表现在寻址方式、路由选择、最大长度、网络接入机制、用户接入控制、超时控制、差错恢复方法、服务、管理方式等诸方面的不同。要实现网际互连，就必须消除差异。要事现网际互连，就必须消除网络间的差异，这些都是网际互连要解决的问题。

局域网(LAN)、广域网(WAN)的网际互连有“LAN-LAN”，“LAN-WAN”、“WAN-WAN”和“LAN-WAN-LAN”等四种型式。由于非 OSI 系统要与 OSI 系统互连，非 OSI 系统之间要互连，所以，网际互连并不单纯指不同的通信子网在网络层上互连。实际上，两个网络之间要互连时，它们之间的差异可以表现在 OSI 七层模型中的任一层上。用于网络之间互连的中继设备称为网间连接器，按它们对不同层次的协议和功能转换，可以分为以下几类：

(1)转发器(Repeater)，在物理层间实现透明的二进制比特复制，以补偿信号衰减；

(2)网桥(Bridge) ，提供链路层间的协议转换，在局域网之间存储和转发帧；

(3)路由器(Router)，提供链路层间的协议转换，在不同的网络之间存储和转发分组；

(4)网关(Gateway)，提供运输层及运输以上各层间的协议转换。

注意，由于术语的不统一性，有些文献中将上述的网桥、路由器和网关一起统称为“网关”，此时它可能指的网之间进行协议转换的网间连接器，另外，还有一种称为桥路器(Router)的产品，兼有网桥和路由器两者的功能。

2.网桥

网桥是一种存储转发设备，用来连接类型相似的局域网。从互连网络的结构看，网桥属于 DCE 级的端到端的连接；从协议层次看，网桥属于链路层范畴，存该层对数据帧进行存储转发。它既不同于只作单纯信号增强的转接器，也不同于进行网络层转换的网间连接器。但网桥仍然是一种网络连接的方法，因为局域网本身没有网络层，只有在主机站点上才有网络层或提供网络层服务的功能。

网桥接收帧并送到数据链路层进行差错校验，然后送到物理层再经物理传输媒体送到另一个子网。在转发帧以前，网桥对帧的内容和格式不做修改或仅做很少的修改。 网桥应该有足够的缓冲空间，以便能满足高峰负荷时的要求。另外，必须具备寻址和路由选择的；逻辑功能。

局域网贩逻辑功能自下向上可分为物理层、媒体访问控制层(MAC)及逻辑路控制层(LLC)三层，异构局域的差异主要体现在物理及媒体访问控制层中，图 3.19 给出了一个假想的网桥的工作原理图，图中的两个局域网 802.X 和 802.Y 分别为 802.3、802.4 和 802.5MAC 标准中的一种.网络中发送的数据由 802.X 的 MAC 控制信息 X、LLC 控制控制信息 X，然后交给 LLC 子层加上相应控制信息 Y 送到 802.Y 局域网中，再由对方主机接收。此时，在 802.Y 局域网中，数据由 802.Y 的 MAC 控制信息 Y、LLC 控制信息 L 各网络协议数据单元组成。在上述过程中，由于各种局域网有其不同的物理和数据格式，所以传输过程中还要进行转换。

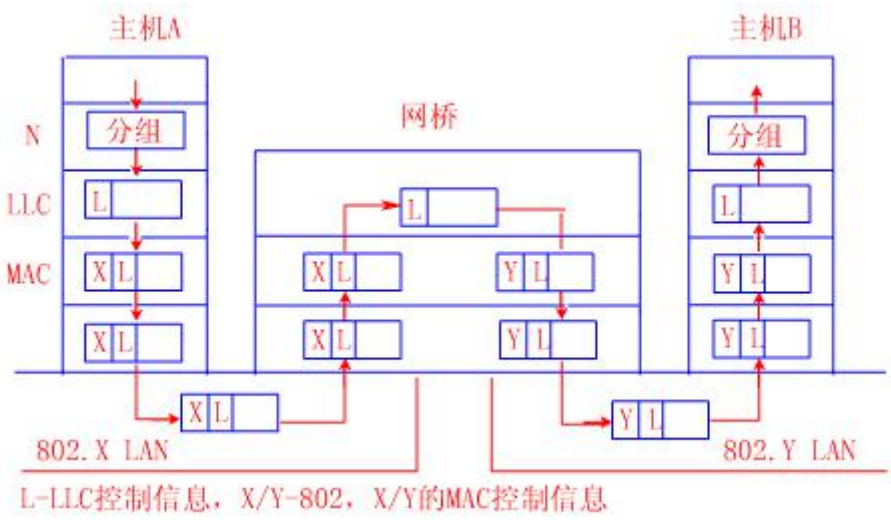


图 3.19 网桥工作原理

3. 路由器

路由器工作网络层,用以实现不同网络间的地址翻译、协议转换和数据式转换等功能，一般用于广域网之间的连接或广域网与局域网之间的连接。常用的路由器有用于面向连接的路由器和用于无连接的路由器两种。

面向连接的路由器用于连接两个提供虚电路服务的广域网。一种采用 CCITT X.75 协议的路由器，可用于连接两个提供 X.25 访问的网络。

无连接的路由器用于提供数据报服务的网际互连模型中，使若干个局域网通过广域网互连。这样，一个局域网上的主机就可以通过广域网与远程局域网上的主机相互通信，局域网上的主机也可以与广域网上的主机以数据报方式通信。IP 协议网际互连方式便是这种模型的实例。

4. 网关

网关也称为协议转换器，用于高层协议的转换，对运输层到应用层均能支持。

若两互连网络的主机高层中仅运输层协议不同，则可以利用网关的功能在运输层间做协议转换，内容包括数据格式的重新装配、长数据的分段、地址格式的转换及操作规程的适配等。在高层协议转换的实际实现中，并不一定要分层进行，例如，从运输层到应用层的协议转换可以一起进行。

3.5 高层协议介绍

3.5.1 运输层(又称传输层)

1. 运输层在 OSI 中的地位和作用

OSI 七层模型中的物理层、数据链路层和网络层是面向网络通信的低三层协议。运输层负责端到端的通信，既是七层模型中负责数据通信的最高层，又是面向网络通信的低三层和面向信息处里的高三层之间的中间层。运输层位于网络层之上、会话层之下，它利用网络层子系统提供给它的服务区开发本层的功能，并实现本层对会话层的服务。

运输层是 OSI 七层模型中最重要、最关键的一层，是唯一负责总体数据传输和控制的一层。运输层的两个主要目的是：第一，提供可靠的端到端的通信；第二，向会话层提供独立于网络的运输服务。

在讨论为实现这两个目标所应具有的功能之前，先考察一下运输层所处的地位。首先，运输层之上的会话层、表示层及应用层局部包含任何数据传输的功能，而网络层又不一定需

要保证发送站的数据可靠地送至目的站会话层不必考虑实际网络的结构属性连接方式等实现的细节。

根据运输层在七层模型中的目的和单位，它的主要功能是：对一个进行的对话或连接提供可靠的运输服务，在通向网络的单一物理连接上实现该连接的复用，在单一连接上提供端到端的序号与流量控制端到端的差错控制及恢复等服务。

运输层反映并扩展了网络层子系统的服务功能，并通过运输层地址提供给高层用户传输数据的通信端口，是系统间高层资源的共享不必考虑数据通信方面的问题。

2.运输服务

运输层的服务包括的内容有：服务的类型、服务的等级、数据的传输、用户的接口、连接管理、快速数据传输、状态报告、安全保密等。

(1)服务类型。 运输服务有两大类，即面向连接的服务和面向无连接服务。面向连接的服务提供运输服务用户之间逻辑连接的建立、维持和拆除，是可靠的服务，可提供流量控制、差错控制和序列控制。无连接服务，只能提供不可靠的服务。

需要说明的是，面向连接的运输服务与面向连接的网络层服务十分相似，两者都向用户提供连接的建立、维持和拆除，而无连接的运输服务与无连接的网络层服务业十分相似。那么，既然运输层服务与网络层服务如此相似，又为什么要将它们划分为两个层次呢？前面章节已经介绍过，网络层是通信子网的一个组成部分，网络服务质量并不可靠，如会频繁的丢失分组、网络层系统可能崩溃或不断的进行网络复位。对于这种情况，用户将束手无策，因为用户不能对通信子网加以控制，因而无法采用更优的通信处理机来解决网络服务质量低劣的问题，更不能通过改进数据链路层纠错能力来改善它。解决这个问题的唯一可能办法就是在网路层上增加一层运输层。运输层的存在，使运输服务比网络服务更可靠，分组的丢失、残缺、甚至网络的复位均可被运输层检测出来，并采取相应的补救错施。而且，因为运输服务独立于网络服务，可以采用一种标准的原预计作为运输服务，而网络服务则随不同的网络可能有很大的不同。因为运输服务是标准的，用运输服务原语编写的应用程序能广泛适应于各种网络，因而不必担心不同的通信子网所提供的不同的服务及服务质量。

(2).服务等级。运输协议实体应该允许运输层用户能选择运输层所提供的服务等级，以利于更有效的利用所提供的链路际互连网络资源。可提供的服务包括差错和丢失数据的程度、允许的平均延迟和最大延迟、允许的平均吞吐率和最小吞吐率以及优先级水平等。更具这些要求，可将运输层协议服务等级细分为以下四类：

①.可靠的面向连接的协议；

②.不可靠的无连接协议；

③.需要定序和定时传输的话音传输协议；

④.需要快速和高可靠的实时协议。

(3).数据传输。数据传输的任务是在两个运输实体之间传输用户数据和控制数据。一般采用全双工服务，来别也可采用半双工服务。数据可分为正常的服务数据分组和快递服务数据分组两种，对快速服务数据分组的传输可暂时中止当前的数据传输，在接收短用中短方式优先接收。

(4).用户接口。用户接口机制可以有多种方式，包括采用过程调用、通过邮箱传输数据和参数、用 DMA 方式在主机与具有运输层实体的前端处理机之间传输等。

(5).连接管理。面向连接的协议需要提供建立和终止连接的功能。一般总是提供对称的功能，即两个对话的实体豆油连接管理的功能，对简单的应用也有仅对一方提供连接管理功能的情况。连接的终止可以采用立即终止传输，或等待全部数据传输完再终止连接。

(7).安全保密。包括对发送者和接收者的确认、数据的加密以及通过保密的链路和节点的路由选择等安全保密服务。

3.服务质量

服务质量 QOS（Quallity of Service）是指在运输两节点之间看到的某些运输连接的特征，是运输层性能的度量，反映了传输质量及服务的可用性。

服务质量可用一些参数来描述，如连接建立延迟、连接建立失败、吞吐量、输送延迟、残留差错率、连接拆除延迟、连接拆除失败概率、连接会弹率传输失败率等等。用户可以在连接建立是指明所期望的、可以接受的或不接受的 QOS 参数值。通常，用户使用连接建立源于在用户与运输服务提供者之间协商 QOS，协商过的 QOS 适用于整个运输连接的生存期。但主呼用户请求的 QOS 可能被运输服务者提供者降低，也可能被被呼用户降低。

根据用户要求和差错性质，网络服务按质量可分为以下三种类型：

⑴.A 型网络服务,具有了接受的残留差错率和故障通知率；

⑵.B 型网络服务,具有可接受的残留差错率和不可接受的故障通知率；

⑶.C 型网络服务,具有不可接受的残留差错率。

可见,网络服务质量的划分是以用户要求为依据的.若用户要求比较高,则一个网络可能归于 C 型；反之，则一个网络可能归于 B 型甚至 A 型。例如，对于某个电子邮件系统来说，每周丢失一个分组的网络也许可算做 A 型;而同一个网络对银行系统来说则只能算作 C 行了。三种类型的网络服务中,A 型服务质量最高,B 型网络服务质量次之,C 型网络服务质量最差。

4.运输层协议等级

运输层的功能是要弥补从网络层获得的服务和拟向运输服务用户提供的服务之间的差距,它所担心的是提高服务质量,包括优化成本。

运输层的功能按级别划分，OSI 定义了五种协议级别，即级别 0（简单级）、级别 1（基本差错恢复级）、级别 2（多路复用级）、级别 3（差错恢复和多路复用级）和级别 4（差错检测和恢复级）。服务质量划分的较高的网络，仅需药较简单的协议级别；反之，服务质量划分的较低的网络，仅需要较复杂的协议级别。

5.运输服务原语

服务在形式上是一组原语（Primitive）来描述的。原语被用来统治服务提供者采取某些行动，或报告某同层尸体已经采取的行动。在 OSI 参考模型中，服务原语划分为四种类型：

⑴.请求(Request)。用户利用它要求服务提供者提供某些服务，如建立连接或发送数据等；

⑵.指示(Indication)。服务提供者执行一个请求以后，用指示原语通知收方的用户实体，告知有人想要与之建立连接或发送数据等；

⑶.响应(Response)。收到指示原语后，利用响应原语向对方作出反应，；例如同意或不同意建立连接等；

⑷.确认(Confirm)。请求对方可以通过接收确认原语来获悉对方是否同意接受请求。原语可以携带参数，如连接请求原语的参数肯恩公之命他摇匀阿台机器连接，需要什么服务类别等。连接指示原语的参数肯恩公包含呼叫者的表示、需要服务的类别等。被呼叫实体可以在响应原语中的参数里表示同意或不同意连接,若同意,则肯恩公对某些参数给出协商制,比如最大数据吞吐量等。ISO 定义的运输服务包括了 4 种类型共 10 个运输服务原语。

3.5.2 会话层

会话层在运输层提供的服务上，加强了会话管理、同步和活动管理等功能。

1.实现会话连接到运输连接的映射

会话层的主要功能是提供建立连接并有序传输数据的一种方法，这种连接就叫作绘画(Session)。会话可以使一个远程终端登录到远地的计算机，进行文件传输或进行其它的应用。

会话连接建立的基础是建立运输连接，只有当运输连接建立好之后，会话连接才能依赖

于它而建立。会话与运输层的连接有三种对应关系。一种是一对一的关系，即在会话层建立会话时，必须建立一个运输连接，当会话结束时，这个运输连接也被释放。另一种是多对一的关系，例如在多顾客系统中，一个客户所建立的一次会话结束后，又有另一顾客要求建立另一个会话，此时运载这些会话的运输连接没有必要不停的建立和释放，但在同一时刻，一个运输连接只能对应一个会话连接。第三种是一对多的关系，若运输连接建立后中途失效，此时会话层可以重新建立一个运输连接而不用废弃原有的会话，当新的运输连接建立后，原来的会话可以继续下去。

2.会话连接的释放

会话连接的释放不同于运输连接的释放，它采用有序释放方式，也即使用完全的握手，包括请求、指示、响应和确认原语，只有双方同意，会话菜终止。这种释放方式不会丢失数据。对于异常原因，会话层也可以不经协商立即释放，但这样可能会丢失数据。

3.会话层管理

与其它各层一样，两个会话实体之间的交互活动都需要协调、管理和控制。会话服务的获得是执行会话层协议的结果，会话层协议支持并管理同等对接会话实体之间的数据交换。由于会话层往往是由一系列交互对话组成的，所以对话的次序、对化的进展情况必须加以控制和管理。在会话层管理中考虑了令牌与对话管理、活动与活动单元以及同步与重新同步等措施。

⑴.令牌和对话管理。从原理上说，所有 OSI 的连接都是全双工的。但在许多情况下高层软件为方便起见往往设计成半双工交互式通信。例如,远程终端访问一个数据库管理系统，往往是发出一个查询，然后等待回答，要么轮到用户发送，要么轮到数据库发送，保持这种轮换并强制实行的过程就叫作对话管理。实现对话管理的方法是使用数据令牌(DataToken)，令牌是会话连接的一个属性，它表示了会话服务用户对某种服务的独占使用权，只有我有令牌的用户可以发送数据，另一方必须保持沉默。令牌是一种非共享的 OSI 资源。

⑵.活动与对话单元。会话服务用户之间的合作可以划分为不同的逻辑单位，每一个逻辑单位成为一个活动(Activity)，每个活动的内容具有相对的完整性和独立性。在任一时刻，一个会话连接只能为一个活动所使用，但允许某个活动跨越多个会话连接。另外，可以允许有多个活动顺序的使用一个会话连接，但在世上不允许重叠。活动与会话连接的关系可以用电话用户线路的连接关系说明，一对拨通的电话相当于一个会话连接，使用者对电话线通话的用户进行的对话相当于活动显然一个电话人一时刻只能供一个人使用，即支持一个活动。然而，当一对用户通完话后可不挂断电话，让后续需要统一电话线路连接的人接着使用，这就相当于一个会话连接顺序的工多个活动使用。若在通话过程中线路出现故障引起中断，则需要重新再接电话继续对话，这就相当于一个活动跨越了多个连接。

对化单元是一个活动中数据的基本交换单元，通常代表逻辑上重要的工作部分。在活动中，存在一系列的交互通话，每个单项的连接通信动作所传输的数据就构成一个对化单元。

⑶同步与重新同步。会话层的另一个服务是同步。所谓同步就是使会话服务用户对会话的进展情况有一致的了解,在会话被中断后可以从中断处继续下去,而不必从头恢复会话，这种会话进程的了解是通过设置同步点来获得的。会话层允许会话用户在传输的数据中自由设置同步点，并对每个同步点与同步序号，用以识别和管理同步点，这些同步点是插在用户数据流中一起传送给对方的。当接收方通知发送方它收到一个同步点时，发送方就可确定接收方已将此同步点之前发送的数据流全部收妥。

会话层定义了两个两类同步点。主同步点用于在同步的数据流中划分出对话单元，一个主同步点是一个对话单元的结束和下一个对话单元的开始;次同步点用于在一个对话单元内部实现数据结构化。主同步点与次同步点有一些不同，在重新同步时只可能回到最近的主同步点；每一个插入数据流中的主同步点都被明确地确认，而次同步点不被确认。

4.OSI 会话服务

会话层可以向用户提供许多服务，为使两个会话服务用户在会话建立阶段能协商所需的服务，将服务分成若干个单元。通用的功能单元包括：

(1) 核心功能单元，提供连接管理和全双工数据传输的基本功能。

(2) 协商释放功能单元，提供有次序的释放服务。

(3) 同步功能单元，在会话连接期间提供同步或重新同步。，

(4) 活动管理功能单元，提供对话活动的识别、开始、结束、暂停和 新开始等。

(5) 异常报告功能单元，在会话连接期间提供异常情况报告。

上述所有功能的执行均有相应的用户服务原语，每一种语类型都可能具有请求、指示、响应和确认四种形式。

5.OSI 会话协议

OSI 的会话层协议填补了运输层所提供的服务与会话用户所要求的服务之间的缝隙。会话服务提供了各种与数据交换的管理和构造有关的服务。

会话协议含有 34 种会话协议数据单元的类型，会话协议数据单元与会话服务原语之间具有相对应的映象关系，大多数服务原语导致会话协议实体产生并发送一个相应的会话协议数据单元。

3.5.3 表示层

1.表示层的特点及功能

OSI 环境的低五层提供透明的数据传输，应用层负责处理语义，而表示层则负责处理语法，由于各种计算机都可能有各自的数据描述方法，所以不同类型计算机之间交换的数据，一般需经过格式转换才能保证其意义不变。表示层要解决的问题是如何描述数据结构并使之与具体的机器无关，其作用是对原站内部的数据结构进行编码，使之形成适合于传输的比特流，到了目的站再进行解码，转换成用户所要求的格式。

为使各个系统间交换的信息具有相同的语义，应用层采用了相互承认的抽象语法。抽象是对数据一般结构的描述。表示实体实现抽象语法与传输语法间的转换，传输语法是同等表示实体之间通信时对用户信息的描述，是对抽象语法比特流进行编码得到的。抽象语法与传输语法之间的对应关系称为上下关系。

表示层的主要功能为：

（1）语法转换。将抽象语法转换成传输语法，并在对方实现相反的转换。涉及的内容有代码转换、字符转换、数据格式的修改，以及对数据结构操作的适应、数据压缩、加密等。

（2）语法协商。根据应用层的要求协商选用合适的上下文，即确定传输语法并传送。

（3）连接管理。包括利用会话层服务建立表示连接，管理在这个连接之上的数据传输和同步控制，以及正常或异常地终止这个连接。

2. 语法转换

（1）数据表示。不同厂家生产的计算机具有不同的内部数据表示。如 IBM 公司的主机广泛使用 EBCDIC 码，而大多数其它厂商的计算机则使用 ASCII 码；Intel 公司的 80X86 芯片从右到左计数字节，而 Motorola 公司的 68020 和 68030 芯片则从左到右计数；大多数微型机用 16 位或 32 位整数的补码运算，而 CDC 的 Cyber 机用 60 位的反码。由于表示方法的不同，即使所有的位模式都正确接收，也不能保证数据含义的不变。人们要的是保留含义，而不是位模式。为了解决此类问题，必须进行数据表示方式的转换。可以在发送方转换，也可以在接收方转换，或者双方都向一种标准格式转换。

（2）数据压缩。强调数据压缩的必要性是基于以下几个原因。首先，随着多媒体技术的发展，数字化/音频数据的吞吐、传输和存储问题日益凸现。具有中等分辩率（640×480）的彩色（24bit/像素）数字视频图像的数据量约 7.37Mbit/帧，若按 25 帧/秒的动画要求，

则视频数据的传输速率大约为 184Mbps。由此可见，高效实时地数据压缩对于缓解网络带宽和取得适宜的传输速率是非常必要的。其次，网络的费用依赖于传输的数据量，在传输之前对数据进行压缩可减少传输费用。

实现数据压缩的可能性是基于以下原因。首先，是原始信源数据（视/音频）存在着很大的冗余度，比如电视图像帧内邻近像素之间空域相关性及前后之间的时域相关性都很大，信息有冗余。其次，是有可能利用人的视觉对于边缘急剧变化不敏感（视觉掩盖效应）各眼睛对图像的亮度信息敏感、对颜色分辨力弱的特点以及听觉的生理特性实现高压缩比，而使由压缩数据恢复的图像及声音数据仍有满意的主观质量。第三，利用数据本身的特征也可实现压缩。

(3)网络安全和保密。随着计算机网络应用的普及，计算机网络的安全和保密问题就变得越来越重要了。为保护网络的安全，最常见的方法是采用加密措施。从理论上讲，加密可以在任何一层上实现，但实际应用中常常在物理层、运输层和表示层三层实现加密。在物理层加密的方案叫做链路加密，它的特点是可以对整个报文进行加密；在运输层实现加密可以提高有效性，因为表示层可以对数据事先进行压缩处理；而在表示层可以有选择地对数据实现加密。

3.OSI 表示服务原语

表示层大部分服务原语与会话层的相类似。在实施中，几乎所有的表示服务原语只是穿过表示层到会话层。有些表示服务原语可不加改变直接映射成相应的会话服务原语，即无需产生一个表示协议数据单元。通常与这些原语有关的参数在会话服务原语的用户数据字段中传输。

4.抽象语法标记 ASN.1

表示编码、 传输和解码数据结构的关键,是要有一种足够灵活的 、适应各种类型应用的标准数据描写方法.为此,OSI 中提出了一种标记法,叫做抽象语法标记 1,简称为 ASN.1.发送时将 ASN.1 数据结构编码成位流,这种位流的格式叫做抽象语法.

在 ASN.1 中为每个应用所需的所有数据结构类型下了定义，并将它们组成库。当一个应用想发送一个数据结构时,可以将数据结构与其对应的 ASN.1 标识一起传给表示层。以 ASN.1 定义作为索引，表示层便知道数据结构的域的类型及大小，从而对它们编码 传输；在另一端，接收表示层查看此数据结构的 ASN.1 标识，从而了解数据结构的域的类型及大小。这样，表示层便就可以实现从通信线路上所用的外部数据格式到接收计算机所用的内部数据格式的转换。

数据类型的 ASN.1 描述称为抽象语法,同等表示实体之间通信时对用户信息的描述称为传输语法。为抽象语法指定一种编码规则，便构成一种传输语法。在表示层中，可用这种方法定义多种传输语法。传输语法与抽象语法之间是多一多对应关系，即一种传输语法可用于多种抽象 语法 的数据传输，而一种抽象语法的数据 值可用多传输语法来传输。

每个应用层协议中的抽象语法与一个能对其进行编码的传输语法的组合,就构成一个表示上下文(Presentation Context).表示上下文表示连接建立时协商确定，也可以在通信过程 中重新定义。表示层提供定义表示上下文的设施。

3.5.4 应用层

应用层也称为应用实体(AE),它由若干个特定应用服务元素(SASE)和一个或多个公用服务元素（CASE）组成 。每个 SASE 提供特定的应用服务，例如文件传输访问和管理（FTAM）电子文电处理系统（MHS） 虚拟终端协议(VIP)等。CASE 提供一组公用的应用服务，例如联系控制服务元素（ACSE）可靠传输服务元素（RTSE）和远程操作服务元素(ROSE)等。

1.文件传输 访问和管理（FTAM）功能

FTAM 是一个用于传输、访问和管理开放系统工程中文件的一个信息标准化。FTAM 服务

使用户即使不了解所使用的实际文件系统的实现细节，也能对该文件系统进行操作，或对数据的描述进行维护。

一个具有通用目的的文件传输协议必须考虑异种机的环境，因为不同的系统可能有不同的文件夹格式和结构。对于 M 种本地文件结构和 N 种输入文件夹结构来说，为了避免 M*N 种可能的不同文件夹结构之间的映射 转换问题，可以采用一种虚拟文件夹的方案。该方案制定了一个通用的虚拟文件结构，使文件传输系统中交换的只是虚拟文件，而在端系统则对虚拟文件格式和本地文件格式实施一种局部的转换。

虚拟文件可以组成一个虚拟文件库，虚拟文件库模型是 FTAM 的基础。FTAM 定义了一系列用户服务原语，用以实现文件的有关操作。

2.电子邮件功能

电子邮件是允许终端用户编辑文电的一种设施。这种服务是邮政发展的主要方向，是一种新的分布式综合文电处理系统，它可分为单系统电子邮件和网络电子邮件两类。
向单系统电了邮件中，允许一个共享计算机系统上的所有用户交换文电。每个用户在系统上登记，并有惟一的标识符，与每个用户相联系的是一个邮箱。用户可以调用电子邮箱设施，准备文电，并把它给此系统上的任何其它用户。邮箱实际上只是由文件管理系统维护的一个文件目录，每个邮箱有一个用户与之相联。任何输入信件只是简单地作为文件存放于用户邮箱目录之下，用户可以取出并阅读这个文电。

在单系统电子邮件设施中，文电只能在特定系统的用户之间交换。若希望通过网络系统在更广泛的范畴内交换文电，就需要包括 OSI 模型的 1-6 层的服务，并在应用层制订一个标准化的文电传输协议，这就是网络电子邮件。

CCITT 发表了一个关于文电处理系统 MHS（Message Handling System）的 X.400 建议。MHS 包含了网络电子邮件的需要，规定了通过网络发送文电所用的服务，为构筑用户接口提供了基础。1988 年 CCITT 又发表了经过修订的 MHS 建议，该版本对早期版本进行了功能扩充，并使用新的抽象模型来描述服务和协议，从而使 MHS 与 OSI 参考模型统一在一起来。MHS（88）是 CCITT 与 ISOR 联合版本，ISO 称其为面向文电的正文交换系统 MOTIS（Message Oriented Text Interchange Systems).

文电处理系统具有以下几个特点：

（1）文电以存储--转发的方式进行传输；

（2）文电的递交和交付可以不同时进行，即发送者可以在适当的时候将文电递交给系统，而接收者也可以在以后的某个时间里接收交付的文电，在此期间文电保存在邮箱中；

（3）同一份文电可以交付给多个接收者（多地址交付）；

（4）文电的内容形式、编码类型可以由系统自动进行转换，以适应接收终端的要求；

（5）交付时间的控制可由发送方规定，经过若干时间后系统才可将文电交付给接收方；

（6）系统可以将文电交付与否的结果通知给发送方。

在 X.400 中定义了 MHS 模型，这个模型为所有其它的建议提供了一个框架。它定义了三种类型的实体：用户代理 UA（User Agent）、文电传输代理 MTA（Message Transfer Agent）和温点存储 MS（Message Store）。次处还有访问单元 AU 以及物理投递访问单元 PDAU，分别与其它的通信及投递服务接口。
用户代理 AU 代表用户进行操作，为用户与文电处理系统交换文电起桥梁作用。它直接与用户有关，执行文电准备、整理、回复、检索和转发等功能。

文电传输代理 MTA 为文电传输提供存储－转发服务，接受从 UA 来的文电并把它投递给其它 UA。MTA 的集合构成文电传输系统 MTS。MTA 必须为文电进行路径选择和转发，使文电通过一系列 MTA 经存储转发到达目的地。使用存储转发的方法，消除了对所有的 UA 和 MTA 必须连续工作的需要。

文电存储器 MS 作为 UA 和 MTA 之间的中介体，它是 MHS 的一个可选功能，其主要功能是存储和检索被投递的文电。MS 可以与 UA 或 MTA 共存于一个系统中，也可以独立设置。

3.虚拟终端协议 VTP

鉴于终端标准化工作进展迟缓，ISO 提出了虚拟终端的概念。虚拟终端方法就是对终端访问中的公共功能引进一个抽象模型，然后用该模型来定义一组通信服务以支持分布式的终端服务。这就需要在虚拟终端服务与本地终端访问方式之间建立映射，使实终端可在 OSI 环境中以虚拟终端方式进行通信。ISO 将虚拟终端标准列入应用层，归属于特定应用服务元素。

虚拟终端是对各种实终端具有的功能进行一般化、标准化之后得到的通用模型。但由于目前现有的实终端种类太多，具有的功能也不利于终端功能的扩充。

VTP 的根本目的是将实终端的特性变换成标准化的形式，即虚拟终端。

VTP 有两种模型：非对称模型和对称模型。在非对称模型中，虚拟终端可以看成是实际终端和本地映象功能的结合；在对称模型中，两边都使用了一种代表虚拟终端状态的共享表示单元，这个表示单元可以看做是一种数据结构，两边都可对称地进行读、写。对称模型即允许终端－主机对话，也允许终端－终端及主机－主机间的对话。

4.其它应用功能

其它许多应用已经或正在标准化，如：

(1)目录服务：类似于电子电话本，它提供了在网络上找人或查询的可用服务地址的方法；

(2)远程作业录入：允许用户将作业提交到另一台计算机去执行；

(3)图形：具有发送工程图至远地显示、标绘的功能；

(4)信息通信：用于办公室和家庭的公用信息服务。

3.6 TCP/TP 协议簇

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

3.6.1 TCP/IP 的体系结构和功能

TCP/IP 是一组协议的代名词，它还包括许多别的协议，组成了 TCP/IP 协议簇。一般来说，TCP 提供运输层服务，而 IP 提供网络层服务。TCP/IP 的体系结构与 ISO 的 OSI 七层参考模型的对应关系如图 3.20 所示。

在 TCP/IP 层次模型中，第二层为 TCP/IP 的实现基础，其中可包含 MILNET，IEEE802.3 的 CSMA/CD、IEEE802.5 的 TokenRing。

在第三层网络中，IP 为网际协议(Internet Protocol)、ICMP 为网际控制报文协议(Internet Control Message Protocol)、ARP 为地址转换协议(Address Resolution Protocol)、RARP 为反向地址转换协议(Reverse ARP)。

第四层为运输层，TCP 为传输控制协议、UDP 为用户数据报协议(User Datagram Protocol)。

第五－七层中，SMTP 为简单邮件传送协议(Simple Mail Transfer Protocol)、DNS 为域名服务(Domain Name Service)、FTP 为文件传输协议(File Transfer Protocol)、TELNET 为远程终端访问协议。

TCP/IP 协议本身的分层模型如图 3.21 所示。以下各节侧重从体系结构的角度分层介绍 TCP/IP 的协议组。

3.6.2 TCP/IP 的数据路层

数据链路层不是 TCP/IP 协议的一部分，但它是 TCP/IP 赖以存在的各种通信网和 TCP/IP 之间的接口，这些通信网包括多种广域网如 ARPANFT、MILNET 和 X.25 公用数据网，以及各种局域网，如 Ethernet、IEEE 的各种标准局域网等。IP 层提供了专门的功能，解决与各种网络物理地址的转换。

一般情况下、各物理网络可以使用自己的数据链路层协议和物理层协议，不需要在数据链路层上设置专门的 TCP/IP 协议。但是，当使用串行线路连接主机与网络，或连接网络与网络时，例如用户使用电话线和 MODEM 接入或两个相距较远的网络通过数据专线互连时，则需要在数据链路层运行专门的 SLIP(serial Line IP)协议的 PPP(Point to Point Protocal)协议。

1.SLIP 协议

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

SLIP 是一种简单的组帧方式，使用时还存在一些问题。首先，SLIP 不支持在连接过程中的动态 IP 地址分配，通信双方必须事先告知对方 IP 地址，这给没有固定 IP 地址的个人用户上 Internet 网带来了很大的不便：其次，SLIP 帧中无协议类型字段，因此它只能支持 IP 协议；再有，SLIP 帧中列校验字段，因此链路层上无法检测出传输差错，必须由上层实体或具有纠错能力的 MODEM 来解决传输差错问题。

2.PPP 协议

为了解决 SLIP 存在的问题，在串行通信应用中又开发了 PPP 协议。PPP 协议是一种有效的点一点通信协议，它，由串行通信线路上的组帧方式，用于建立、配制、测试和拆除数据链路的链路控制协议 LCP 及一组用以支持不同网络层协议的网络控制协议 NCPs 三部分组成。

由于 PPP 帧中设置了校验字段，因而 PPP 在链路层上具有差错检验的功能。PPP 中的 LCP 协议提供了通信双方进行参数协商的手段，并且提供了一组 NCPs 协议，使得 PPP 可以支持多种网络层协议，如 IP、IPX、OSI 等。另外，支持 IP 的 NCP 提供了在建立连接时动态分配 IP 地址的功能，解决了个人用户上 Internet 网的问题。

3.6.3 TCP/IP 网络层

网络层中含中有四个重要的协议：互连网协议 IP、互连网控制报文协议 ICMP、地址转换协议 ARP 和反向地址转换协议 RARP。

网络层的功能主要由 IP 来提供。除了提供端到端的分组分发功能外，IP 还提供了很多扩充功能。例如，为了克服数据链路层对帧大小的限制，网络层提供了数据分块和重组功能，这使得很大的 IP 数据报能以较小的分组在网上传输。

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

1.互连网协议 IP(Internet Protocol)

网络层最重要的协议是 IP，它将多个网络联成一个互连网，可以把高层的数据以多个数据报的形式通过互连网分发出去。

IP 的基本任务是通过互连网传送数据报，各个 IP 数据报之间是相互独立的。主机上的 IP 层向运输层提供服务。IP 从源运输实体取得数据，通过它的数据链路层服务传给目的主机的 IP 层。IP 不保证服务的可靠性，在主机资源不足的情况下，它可能丢弃某些数据报，同时 IP 也不检查被数据链路层丢弃的报文。

在传送时，高层协议将数据传 IP，IP 再将数据封装为互连网数据报，并交给数据链路层协议通过局域网传送。若目的主机直接连在本网中，IP 可直接通过网络将数据报传给目的主机；若目的主机在远在网络中，则 IP 路由器传送数据报，而路由器则依次通过下一网络将数据报传送到目的主机或再下一个路由器。也即一个 IP 数据报是通过互连网络，从一个 IP 模块传到另一人个 IP 模块，直到终点为止。

需要连接独立管理的网络的路由器，可以选择它所需的任何协议，这样的协议称为内部网间连接器协议 IGP(Interior Geteway PROTOCOL)。在 IP 环境中，一个独立管理的系统称为自治系统。

跨越不同的管理域的路由器(如从专用网到 PDN)所使用的协议，称为外部网间连接器协议 EGP(Exterior Gateway Protocol),EGP 是一组简单的定义完备的正式协议。

2.互连网控制报文协议 ICMP

从 IP 互连网协议的功能,可以知道 IP 提供的是一种不可靠的无法接报文分组传送服务。若路由器或麻风故障使网络阻塞，就需要通知发送主机采取相应措施。

为了使互连网能报告差错，或提供有关意外情况的信息，在 IP 层加入了一类特殊用途的报文机制，即互连网控制报文协议 ICMP。

分组接收方利用 ICMP 来通知 IP 模块发送方某些方面所需的修改。ICMP 通常是由发现别的站发来的报文有问题的站产生的,例如可由目的主机或中继路由器来发现问题并产生有关的 ICMP。如果一个分组不能传送，ICMP 便可以被用来警告分组源，说明有网络、主机或端口不可达。ICMP 也可以用来报千网络阻塞。ICMP 是 IP 正式协议的一部分，ICMP 数据报通过 IP 送出，因此它在功能上属于网络第三层，但实际上它是像第四层协议一被编码的。

3.地址转换协议 ARP

在 TCP/IP 网络环境下，每个主机都分配了一个 32 位的 IP 地址，这种互连网地址是在国际范围标识主机的一种逻辑地址。为了让报文在物理网上传送,必须知道彼此的物理地址。这样就存在把互连网地址变换为物理地址的地址转换问题。以以太网(Ethernet)环境为例，为了正确地向目的站传送报文，必须把目的站的 32 位 IP 地址转换成 48 位以太网目的地址 DA。这就需要在网络层有一组服务将 IP 地址转换为相应物理网络地址，这组协议即是 ARP。

在进行报文发送时，如果源网络层给的报文只有 IP 地址，而没有对应的以太网地址，则网络层广播 ARP 请求以获取目的站信息，而目的站必须回答该 ARP 请求。这样源站点可以收到以太网 48 位地址，并将地址放入相应的高速缓存(cache)。下一次源站点对同一目的站点的地址转换可直接引用高速缓存中的地址内容。地址转换协议 ARP 使主机可以找出同一物理网络中任一个物理主机的物理地址，只需给出目的主机的 IP 地址即可。这样，网络的物理编址可以对网络层服务透明。

在互联网环境下，为了将报文送到另一个网络的主机，数据报先定向发送方所在网络 IP 路由器。因此，发送主机首先必须确定路由器的物理地址，然后依次将数据发往接收端。除基本 ARP 机制外，有时还需在路由器上设置代理 ARP，其目的是由 IP 路由器代替目的站对发送方 ARP 请求做出响应。

4.反向地址转换协议 RARP

反向地址转换协议用于一种特殊情况，如果站点初始化以后，只有自己的物理地址而没有 IP 地址，则它可以通过 RARP 协议，发出广播请求，征求自己的 IP 地址，而 RARP 服务器则负责回答。这样，无 IP 地址的站点可以通过 RARP 协议取得自己的 IP 地址，这个地址在下一次系统重新开始以前都有效，不用连续广播请求。RARP 广泛用于获取无盘工作站的 IP 地址。

3.6.4 TCP/IP 的运输层

TCP/IP 在这一层提供了两个主要的协议：传输控制协议(TCP)和用户数据协议(UDP)，另外还有一些别的协议，例如用于传送数字化语音的 NVP 协议。

1.传输控制协议 TCP

TCP 提供的是一种可靠的数据流服务。当传送受差错干扰的数据，或基础网络故障，或网络负荷太重而使网际基本传输系统(无连接报文递交系统)不能正常工作时，就需要通过其它协议来保证通信的可靠。TCP 就是这样的协议，它对应于 OSI 模型的运输层，它在 IP 协议的基础上，提供端到端的面向连接的可靠传输。

TCP 采用“带重传的肯定确认”技术来实现传输的可靠性。简单的“带重传的肯定确认”是指与发送方通信的接收者，每接收一次数据，就送回一个确认报文，发送者对每个发出去的报文都留一份记录，等到收到确认之后再发出下一报文分组。发送者发出一个报文分组时，启动一个计时器，若计时器计数完毕，确认还未到达，则发送者重新送该报文分组。

简单的确认重传严重浪费带宽，TCP 还采用一种称之为“滑动窗口”的流量控制机制来提高网络的吞吐量，窗口的范围决定了发送方发送的但未被接收方确认的数据报的数量。每当接收方正确收到一则报文时，窗口便向前滑动，这种机制使网络中未被确认的数据报数量增加，提高了网络的吞吐量。

TCP 通信建立在面向连接的基础上，实现了一种“虚电路”的概念。双方通信之前，先建立一条连接，然后双方就可以在其上发送数据流。这种数据交换方式能提高效率，但事先建立连接和事后拆除连接需要开销。TCP 连接的建立采用三次握手的过程，整个过程由发送方请求连接、接收方再发送一则关于确认的确认三个过程组成。

2.用户数据报协议 UDP

用户数据报协议是对 IP 协议组的扩充，它增加了一种机制，发送方使用这种机制可以区分一台计算机上的多个接收者。每个 UDP 报文除了包含某用户进程发送数据外，还有报文目的端口的编号和报文源端口的编号，从而使 UDP 的这种扩充，使得在两个用户进程之间的递送数据报成为可能。

UDP 是依靠 IP 协议来传送报文的，因而它的服务和 IP 一样是不可靠的。这种服务不用确认、不对报文排序、也不进行流量控制，UDP 报文右能会出现丢失、重复、失序等现象。

3.6.5 TCP/IP 的会话层至应用层

TCP/IP 的上三层与 OSI 参考模型有较大区别，也没有非常明确的层次划分。其中 FTP、TELNET、SMTP、DNS 是几个在各种不同机型上广泛实现的协议，TCP/IP 中还定义了许多别的高层协议。

1.文件传输协议 FTP

文件传输协议是网际提供的用于访问远程机器的一个协议，它使用户可以在本地机与远程机之间进行有关文件的操作。FTP 工作时建立两条 TCP 连接，一条用于传送文件，另一条用于传送控制。

FTP 采用客户/服务器模式，它包含客户 FTP 和服务器 FTP。客户 FTP 启动传送过程，而服务器对其做出应答。客户 FTP 大多有一个交互式界面，使用权客户可以灵活地向远地传文件或从远地取文件。

2.远程终端访问 TELNET

TELNET 的连接是一个 TCP 连接，用于传送具有 TELNET 控制信息的数据。它提供了与终端设备或终端进程交互的标准方法，支持终端到终端的连接及进程到进程分布式计算的通信。

3.域名服务 DNS

DNS 是一个域名服务的协议，提供域名到 IP 地址的转换，允许对域名资源进行分散管理。DNS 最初设计的目的是使邮件发送方知道邮件接收主机及邮件发送主机的 IP 地址，后

来发展成为右服务于其它许多目标的协议。

4.简单邮件传送协议 SMTP

互连网标准中的电子邮件是一个单间的基于文件的协议，用于可靠、有效的数据传输。SMTP 作为应用层的服务，并不关心它下面采用的是何种传输服务，它可能过网络在 TCP 连接上传送邮件，或者简单地在同一机器的进程之间通过进程通信的通道来传送邮件。这样，邮件传输就独立于传输子系统，可在 TCP/IP 环境、OSI 运输层或 X.25 协议环境中传输邮件。

邮件发送之前必须协商好发送者、接收者。SMTP 服务进程同意为基本个接收方发送邮件时，它将邮件直接交给接收方用户或将邮件逐个经过网络连接器，直到邮件交给接收方用户。在邮件传输过程中，所经过的路由被记录下来。这样，当邮件不能正常传输时可按原路由找到发送者。

在当前的 UNIX 版本中，已将 TCP/IP 协议融入其中，使之成为 UNIX 操作系统的一个部分。DOS 上也推出了相应的 TCP/IP 软件产品。SUN 公司则将 TCP/IP 广泛推向商务系统，它在所在的工作站系统中都预先安装了 TCP/IP 网络软件及网络硬件，使网络和计算机成为一体，同时也使 TCP/IP 网络软件及其客户/服务器的工作方式 为广大用户所接受。

第四章 局域网

局域网 LAN(Local Area Network),是一种在有限的地理范围内将大量 PC 机及各种设备互连一起实现数据传输和资源共享的计算机网络。社会对信息资源的广泛需求及计算机技术的广泛普及，促进了局域网技术的迅猛发展。在当今的计算机网络技术中，局域网技术已经占据了十分重要的地位。本章从介绍局域网的体系结构、协议标准及拓扑结构入手,详细讨论 CSMA/CD 总域网、令牌环网及令牌总线网的媒体访问控制方法，最后不定期要介绍光纤分布数据接口 FDDI 和局域网的操作系统。

4.1 局域网的主要技术

4.1.1 局域网的特点

区别于一般的广域网(WAN),局域网(LAN)具有以下特点：

(1)地理分布范较小,一般为数百米至数公里。可覆盖一幢大楼、一所校园或一个企业。

(2)数据传输速率高，一般为 0.1-100Mbps，目前已出现速率高达 1000Mbps 的局域网。可交换各类数字和非数字(如语音、图象、视频等)信息。

(3)误码率低，一般在 10^{-11}-10^{-8} 以下。这是因为局域网通常采用短距离基带传输，可以使用高质量的传输媒体，从而提高了数据传输质量。

(4)以 PC 机为主体，包括终端及各种外设，网中一般不设中央主机系统。

(5)一般包含 OSI 参考模型中的低三层功能，即涉及通信子网的内容。

(6)协议简单、结构灵活、建网成本低、周期短、便于管理和扩充。

局域网可分成三大类；一类是平时常说的局域网 LAN;另一类是采用电路交换技术的局域网,称计算机交换机 CBX(Computer Branch eXchange)或 PBX(Private Branch eXchange)；还有一类是新发展的高速局域网 HSLN(High Speed Local Network)。

在 LAN 和 WAN 之间的是城市区域网 MAN(Metropolitan Area Network)简称城域网。MAN 是一个覆盖整个城市的网络，但它使用 LAN 的技术。

局域网的特性主要涉及拓扑结构、传输媒体和媒体访问控制(Medium Access Control,MAC)等三项技术问题，其中最重要的是媒体访问控制方法。局域网的技术特性见表 4.1。

4.1.2 局域网的拓扑结构

网络的拓扑结构对网络性能是有很大的影响。选择网络拓扑结构，首先要考虑采用何种媒体访问控制方法，因为特定的媒体访问控制方法一般仅适用于特定的网络拓扑结构；其次要考虑性能、可靠性、成本、扩充灵活性、实现的难易程度及传输媒体的长度等因素。局域网常用的拓扑结构有总线、环形、星形三种。有关网络拓扑结构的概念已在第二章中做了介绍，这里再针对局域网的拓扑适用范围做一些说明。

总线网一般采用分布式媒体访问控制方法。总线网可靠性高、扩充性能好、通信电缆长度短、成本低，是用来实现局域网的最通用的拓扑结构，著名的以太网的 CSMA/CD;另一种是总线拓扑网与令牌环相结合的变形，其在物理连接上是总线拓扑结构，而在逻辑结构上则采用令牌环，兼有了总线结构和令牌环的优点。总线网的缺点是若主干电缆某处发生故障，整个网络将瘫痪；另外，当网上站点较多时，会因数据冲突增多而使效率降低。

环形网也采用分布式媒体访问控制方法。环形网控制简单、信道利用率高、通信电缆长度短、不存在数据冲突问题,在局域网中应用较广泛，典型实例有 IBM 令牌环(Token Ring)网和剑桥环(Cambrige Ring)网。另外还有一种 FDDI 结构,它是采用光纤作为传输媒体的高速通用令牌环网，常用于高速局域网 HSLN 和城域网 MAN 中。环形网的缺点是对节点接口和传输线的要求较高，一旦接口发生故障可能导致整个网络不能正常工作。

星形网往往采用集中式媒体访问控制方法。星形网结构简单、实现容易、信息延迟确定。其缺点是通信电缆总长度长、传输媒体不能共享。星形网的典型实例是计算机交换机 CBX。

4.1.3 局域网的传输媒体

LAN 中使用的传输方式有基带和宽带两种。基带用于数字信号传输,常用的传输媒体有双绞线或同轴电缆。宽带用于无线电频率范围内的模拟信号的传输,常用同轴电缆。表 4.2 给出了这两种传输方式的比较。

表 4.2　　基带、宽带传输方式比较

基　　带	宽　　带
数字信号传输	模拟信号的传输(需用 MODEM)
全部带宽用于单路信道传输	使用 FDM 技术，多路信道复用
双向传输	单向传输
总线拓扑	总线或树形拓扑
距离达数公里	距离达数十公里

1.基带系统

使用数字信号传输的 LAN 定义为基带 LAN。数字信号通常采用曼彻斯特编码传输，媒体的整个带宽用于单信道的信号传输，不采用频分多路复用技术。数字信号传输要求用总线形拓扑，因为数字信号不易通过树形拓扑所要求的分裂器和连接器。基带系统只能延伸数公里的距离，这是由于信号的衰减会引起脉冲减弱和模糊，以致无法实现更大距离上的通信。基带传输是双向的，媒体上任意一点加入的信号沿两个方向传输到两端的端接器(即终端接收阻抗器)，并在那里被吸收，如图 4.1 所示。

图 4.1 双向基带系统

总线 LAN 常采用 50Ω 的基带同轴电缆。对于数字信号来说，50Ω 电缆受到来自接头插入容抗的反射不那么强，而且对低频电磁噪声有较好的抗干扰性。最简单的基带同轴电缆 LAN 由一段无分枝的同轴电缆构成，两端接有防反射的端接器，推荐的最大长度为 500 米。站点通过接头接入主电缆，任何两接头间的距离为 2.5 米的整倍数，这是为了保证来自相邻接头的反射在相位上不致于叠加。推荐的最多接头数目为 100 个，每个接头包括一个收发器，其中包含发送和接收用的电子线路。

为了延伸网络的长度，可以采用中继器。中继器由组合在一起的两个收发器组成，连到不同的两段同轴电缆上。中继器在两段电缆间向两个方向传送数字信号，在信号通过时将信号放大和复原。因而，中继器对于系统的其余部分来说是透明的。由于中继器不做缓冲存贮操作，所以并没有将两段电缆隔开，因此如果不同段上的两个站同时发送的话，它们的分组将互相干扰(冲突)。为了避免多路径的干扰，在任何两个站之间只允许有一条包含分段和中继器的路径。802 标准中，在任何两个站之间的路径中最多只允许有 4 个中继器，这就将有效的电缆长度延伸到 2.5 公里。图 4.2 是一个具有 3 个分段和两个分段和两个中继器的基带系统例子。

双绞线基带 LAN 用于低成本、低性能要求的场合，比绞线安装容易，但往往限制在 1 公里以内，数据速率为 1Mbps-10Mbps。

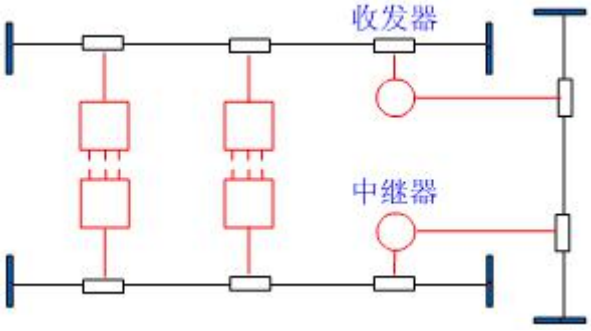


图 4.2 带中继器的基带系统

2、宽带系统

在 LAN 范围内，宽带一般用于传输模拟信号，这些模拟载波信号工作在高频范围(通常为 10～400MHz)，因而可用 FDM 技术把宽带电缆的带宽分成功经验多个信道或频段。宽带系统采用总线/树形拓扑结构，可以达到比基带大得多的传输距离(达数十公里)，这是因为携带数字数据的模拟信号，在噪声和和衰减损失数据之前，可以传播较长的距离。

宽带同基带一样，系统中的站点是通过搠头接入电缆的。但是，与基带不同的是宽带本质上是一种单方向传输的媒体，加到媒体上的信号只能沿一个方向传播。这种单向性质，意

味着只有处于发送站“下游”的站点才能疏到发送站的信号。因此需有两条数据路径，这些路径在网络的端头处接在一起。对于总线拓扑，端头就是总线的一端；对于树形拓扑，端头具有分枝的树根。所有站沿一条路径(入径)向端头传输，在端头接疏到的信号,再沿另一条数据路径(出径)离开端头传输，所有的站点都在出径上接收。

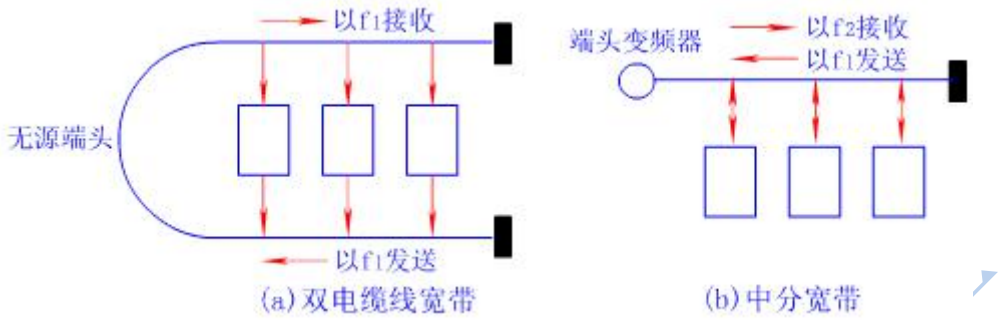


图 4.3 双向宽带系统

在物理上，可用双电缆和中分(Midsplit)两种不同的结构来实现输入和输出的通路，如图 4.3 所示。在双电费结构中，入径和出径是分开的两根电缆,两者间的端头只是一个无源联接装置，每个站点以相同的频率发送和接收。在中分构造中,入径和出径是同一电缆上的不同频率，双向放大器传送较低频率(5～116MHz)的入径和较高频率(168～300MHz)的出径。端头饱含一个称为频率转换器的装置，将入径频率转换为出径频率。频率转换器可以是模拟装置也可以是数字装置，模拟装置只要把信号转换成一个新的频率并重发就可以了，而数字装置则先要在端头恢复数字数据，然后再在新的频率上重发净化了的数据。

4.1.4 局域网的媒体访问控制方法

环形或总线拓扑中，由于只有一条物理传输通道连接所有的设备，因此，连到网络上的所有设备必须遵循一定的规则，才能确保传输媒体的正常访问和使用。常用的媒体访问控制方法有：具有冲突检测的载波监听多路访问 CSMA/CD(Carrier Sense Multiple Access/Collision Detection)、控制令牌(Control Token)及时槽环(Slotted Ring)三种技术。

1、具有冲突检测的载波监听多路访问 CSMA/CD

具有冲突检测的载波监听多路访问 CSMA/CD 采用随机访问和竞争技术，这种技术只用于总线拓扑结构网络。CSMA/CD 结构将所有的设备都直接连到同一条物理信道上,该信道负责任何两个设备之间的全部数据传送，因此称信道是以“多路访问”方式进行操作的。站点以帧的形式发送数据，帧的头部含有目的和源点的地址。帧在信道上以广播方式传输，所有连接在信道上的设备随时都能检测到该帧。当目的地站点检测到目的地址为本站地址的帧时，就接收帧中所携带的数据，并按规定的链路协议给源站点返回一个响应。

采用这种操作方法时，在信道上可能有两个或更多的设备在同一瞬间都会发送帧，从而在信道上千万帧的重叠而出现并有差错，这种现象称为冲突。为减少这种冲突，源站点在发送帧之前，首先要监听信道上是否有其它站点发送的载波信号(即进行“载波监听”)，若监听到信道上有载波信号则推迟发送，直到信道恢复到安静(空闲)为止。另外，还要采用边发送边监听的技术(即“冲突检测”)，若监听到干扰信号，就表示检测到冲突，于是就要立即停止发送。为了确保冲突的其它站点知道发生了冲突，首先在短时间里持续发送一串阻塞(Jam)码,卷入冲突的站点则等待一随机时间，然后准备重发受到冲突影响的帧。这种技术对发生冲突的传输能迅速发现并立即停止发送,因此能明显减少冲突次数和冲突时间。CMSA/CD 媒体访问控制的具体实现，将在本章第 4.3 节中再详细介绍。

2、控制令牌

控制令牌是另一种传输媒体访问控制方法。它是按照所有站点共同理解和遵守的规则，从一个站点到另一个站点传递控制令牌，一个站点只有当它占有令牌时，才能发送数据端帧，发完帧后，即把令牌传递下一个站点。其操作次序如下：

⑴首先建立一个逻辑环，将所有站点同物理媒体相连，然后产生一个控制令牌。

⑵控制令牌由一个站点沿着逻辑环顺序向下一个站点传递。

⑶等待发送帧的站点接收到控制令牌后，把要发送的帧利用物理媒体发送出去，然后再将控制令牌沿逻辑环传递给下一站点。

控制令牌方法除了用于环形网拓扑结构(即令牌环)之外，也可以用于总线网拓扑结构(即令牌总线)，这两类结构建立的逻辑环分别如图 4.4(a)、(b)所示。

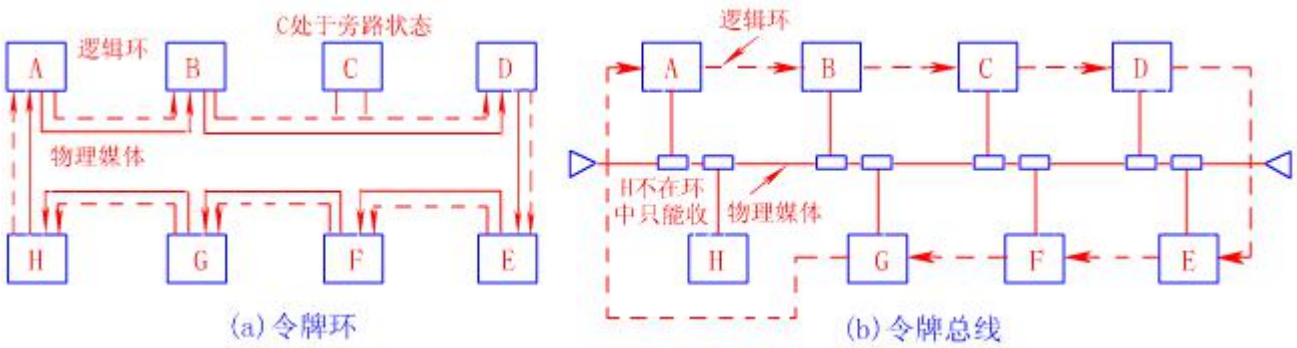


图 4.4 控制令牌媒体访问控制

对于一个物理环，令牌传递的逻辑结构和物理环的结构是相同的，令牌传递的次序和站点连接的物理次序也是一致的；百对于总线网，逻辑环次序则不必和电缆上的站点连接次序相对应，所有站点没有必要抱着按逻辑环连接。例如图 4.4(b)中,H 站并不是逻辑环的一总部分，这意味着 H 站永远拿不到令牌,因此只能以接收方式工作。令牌访问方式的具体的控制方法将在本章第 4.4 节、4.5 节详细介绍。

3、时槽环

时槽环只用于环形网的媒体控制访问,这种方法对每个节点预先安排一个特定的时间内段(即时槽段)，每个节点只能在时槽内传输数据。若数据较长，可用多个时槽来传输。

时槽环采用集中控制方式，这种方法首先由环中被称为监控的站的特定节点起动环，并产生若干个固定长度的比特串，这种比特串即称为时槽。时槽子不停地绕环从一个站点传递到另一个站点。当一个站点收到时槽子时，由该站点的接口阅读后再将其转发到下一个站点，如此一直循环下去。监控站确保总有一个固定数目的时槽绕环传送，而不考虑组成环的站点数目。每个时槽能携带一个固定尺寸的停息帧，时槽帧的格式如图 4.5(a)所示。

时槽环初始化时，由监控站将每个时槽开头的满/空位置为空状态。某个站点要发送数据前，首先要得到一个空时槽，然后将该时槽的满/空位置为空状态，将数据的内容插入时槽中，同时在帧的头部未填入目的地地址和源地址，并将帧尾部的两个响应位全置为 1,然后发送该时槽，使它绕物理环从一个站点至另一个站点传送。

环中每个站对任何置满的时槽头部的目的地址进行检测，如果检测到是自己的地址，便从时槽中阅读所携带的数据内容，并修改时槽尾部的一对响应位，然后通过环再将它转发也去。如果目的地站点忙或者拒收，则响应位做相应的标记或保留不做改变。

源站点在起动一个帧发送之后，要等到该帧绕环一周。由于每个站均知道环上时槽的总数，由环接口对时槽转发计数可知道所发时槽的到来。此后，源站点将所用时槽重新标记为

空状态，并阅读时槽尾部的响应位，以确定是否应舍弃已被发送的该帧备份，或者重发该帧。由于采用了响应位，就不需要设置独立的响应帧。

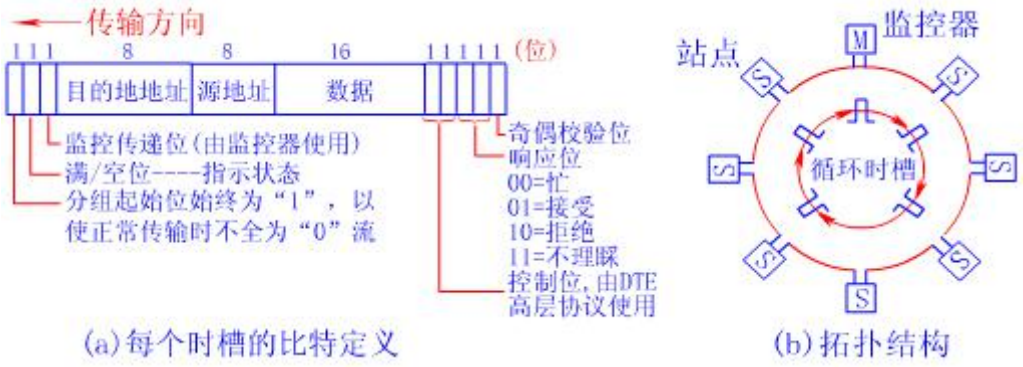


图 4.5 时槽环原理

监控站传递位由监控站用于监测各个站点发送的帧是否有差错或站点有无故障，该位由源站点在发送帧时置“0”。当满时槽在环接口上转发时，由监控站对每一个满时槽的该位置“1”。如果监控站在其转发某个满时槽时，测得监控站传递位已被置为 1，就认为源站点有故障，便可将该帧的满/空位置为空，并释放空时槽。时槽尾部的两个控制位是提供给 DTE 高层协议使用的，在媒体访问控制层中没有意义。

需要特别指出的是，在时槽环媒体访问控制方法中，每个站点每次只能传送一个帧，若想要传送另一个帧，则首先必须释放传输前一帧所用的时槽。这种对环的访问方法体现了公平性，并被各个互连的站点所共享。

时槽环的优点是结构简单，节点间相互干扰少、可靠性高。但是，时槽环为保持基本环结构需要一个特定的监控站节点；由于绕环一周时间内，每个站点只能占用一个时槽，若某站点发送的数据较长要占用多个时槽，而此时环上只有该站有数据要发送，则许多时槽都是空循环；另外，每个 40 位长的时槽只能携带 16 位有效数据，开销大、效率低。相比之下，令牌环中的某个站点得到控制令牌后，就可将包括多个字节的信息帧作为一个整体进行发送，所以效率比时槽环高。

4.2 局域网的参考模型与协议标准

局域网的标准化工作，能使不同生产厂家的局域网产品之间有更好的兼容性，以适应各种不同型号计算机的组网需求，并有利于产品成本的降低。国际上从事局域网标准化工作的机构主要有国际标准化组织 ISO、美国电气与电子工程师学会 IEEE 的 802 委员会、欧洲计算机制造商协会 ECMA、美国国家标准局 NBS、美国电子工业协会 EIA、美国国家标准化协会 ANSI 等。

4.2.1 局域网的参考模型

局域网是一个通信网，只涉及到相当于 OSI/RM 通信子网的功能。由于内部大多采用共享信道的技术，所以局域网通常不单独设立网络层。局域网的高层功能由具体的局域网操作系统来实现。

IEEE 802 标准的局域网参考模型与 OSI/RM 的对应关系如图 4.6 所示，该模型包括了 OSI/RM 最低两层（物理层和链路层）的功能，也包括网间互连的高层功能和管理功能。从图中可见，OSI/RM 的数据链路层功能，在局域网参考模型中被分成媒体访问控制 MAC(Medium Access Control)和逻辑链路控制 LLC（Logical Link Control)两个子层。

在 OSI/RM 中，物理层、数据链路层和网络层使计算机网络具有报文分组转接的功能。对于局域网来说，物理层是必需的，它负责体现机械、电气和过程方面的特性，以建立、维持和拆除物理链路；数据链路层也是必需的，它负责把不可靠的传输信道转换成可靠的传输信道，传送带有校验的数据帧，采用差错控制和帧确认技术。

但是，局域网中的多个设备一般共享公共传输媒体，在设备之间传输数据时，首先要解决由哪些设备占有媒体的问题。所以局域网的数据链路层必须设置媒体访问控制功能。由于局域网采用的媒体有多种，对应的媒体访问控制方法也有多种，为了使数据帧的传送独立于所采用的物理媒体和媒体访问控制方法，IEEE 802 标准特意把 LLC 独立出来形成一具单独子层，使用权 LLC 子层与媒体无关，仅让 MAC 子层依赖于物理媒体和媒体访问控制方法。

由于穿越局域网的链路只有一条，不需要设立路由器选择和流量控制功能，如网络层中的分级寻址、排序、流量控制、差错控制功能都可以放在数据链路层中实现。因此，局域网中可以不单独设置网络层。当局限于一个局域网时，物理层和链路层就能完成报文分组转接的功能。但当涉及网络互连时，报文分组就必须经过多条链路才能到达目的地，此时就必须专门设置一个层次来完成网络层的功能，在职 IEEE 802 标准中灾一层被称为网际层。

在参考模型中，每个实体和另一个系统和同等实体按协议进行通信；而一个系统中上下层之间的通信，则通过接口进行，并用服务访问点 SAP（Server Access Point）来定义接口。为了对多个高层实体提供支持，在 LLC 层的顶部有多个 LLC 服务访问点（LSAP），为图中的实体 A 和 B 提供接口端；在网际层的顶部有多个网间服务访问点（NSAP），为实体 C、D 和 E 提供接口端；媒体访问控制服务访问点（MSAP）向 LLC 实体提供单个接口端。

LLC 子层中规定了无确认无连接、有确认无连接和面向连接三种类型的链路服务。无确认城无连接服务是一促数据报服务，信息帧在 LLC 实体间交换时，无需在同等层实体间事先建立逻辑链路，对这种 LLC 帧进行确认外，其它类似于无确认无连接服务；面向连接服务提供访问点之间的虚电路服务，在任何住处帧交换前，一对 LLC 实体之间必须建立逻辑路，在数据传送过程中，信息帧依次发送，并提供差错恢复和流量控制功能。

MAC 子层在支持 LLC 层完成毁灭体访问控制功能时，可以提供多个可供选择的毁灭体访问控制方式。使用 MSAP 支持 LLC 子层悍，MAC 子层实现帧的寻址和识别。MAC 到 MAC 的操作通过同等层协议来进行 MAC 还产生帧检验序列和完成帧检验等功能。

4.2.2 IEEE 802 标准

IEEE 在 1980 年 2 月成立了局域网标准化委员会（简称 IEEE 802 委员会），专门从事局域网的协议制订，形成了一毓的标准，称为 IEEE 802 标准。亥标准已被国际标准化组织 ISO 采纳，作为局域网的国际标准系列，称为 ISO 8802 标准。要这些标准中，根据局域网的多种类型，规定了各自的拓朴结构、媒体访问控制方法、帧和格式和听任等内容。IEEE 802 标准系列中各个子标准之间的关系如图 4.7 所示。

IEEE 802.1 是局域网的体系结构、网络管理和网际互连协议。IEEE 802.2 集中了数据链路层中与媒体无亲的 LLC 协议。涉及与媒体访问有关的协议，则根据具体网络的媒体访问控制访问分别处理，其中主要的 MAC 协议有：IEEE 802.3 载波监听多路访问/冲突检测 CSMA/CD 访问方法和物理层协议、IEEE 802.4 令牌总线（Token Bus)访问方法和物理层的协议、IEEE 802.5 令牌环（Token Ring)访问方法和物理层协议，IEEE 802.6 关于城域网的分布式他列总线 DQDB（Distributed Queue Dual Bus)的标准等。

IEEE 802 标准定义了 LLC 子层和 MAC 子层的帧格式。数据传输过程中，LLC 子层将高层递交的报文分组作为 LLC 的信息字段，再加上 LLC 子层目的服务访问点（DSAP）、源服务访问点（SSAP）及相应的控制信息以构成 LLC 帧。LLC 帧格式及其控制字段定义见图 4.8。

LLC 的链路只有异步平衡方式（ABM），而不用政党响应方式（NRM）和异步响应（ARM）。也即节点均为组合站，它们既可作为主站发送命令，也可作为从站响应命令。IEEE 802.2

标准定义的 LLC 帧格式与 HDLC 的帧格式有点类似，其控制字段的格式和功能完全效仿 HDLC 的平衡方式制定。LLC 帧也分为信息帧、监控帧和无编号帧三类。信息帧主要用于信息数据传输，监控帧主要用于流量控制，无编号帧用于 LLC 子层传输控制信号以对逻辑链路进行建立与释放。LLC 帧的类型取决于控制字段的第 1 、 2 位，信息帧和监控帧的控制字段均为 2 字长，无编号帧的控制字段为 1 字节。监控帧控制字段中的第 5 ～ 8 位为保留位，一般设置为 0 。控制字段中的其它位含义与 HDLC 控制字段中的含义相同。

4.3 CSMA/CD 媒体访问控制

CSMA/CD 是一种常用争用的方法来决定对媒体访问权的协议，这种争用协议只适用于逻辑上属于总线拓扑结构的网络。在总线网络中，每个站点都能独立地决定帧的发送，若两个或多个站同时发送帧，就会产生冲突，导致所发送的帧都出错。因此，一个用户发送信息成功与否，在很大程度上取决于监测总线是否空闲的算法，以及当两个不同节点同时发送的分组发生冲突后所使用的中断传输的方法。总线争用技术可分为载波监听多路访问 CSMA 和具有冲突检测的载波监听多路访问 CSMA/CD 两大类。

4.3.1 载波监听多路访问 CSMA

载波监听多路访问 CSMA 的技术，也称做无听后说 LBT(Listem Before Talk)。要传输数据的站点首先对媒体上有无载波进行监听，以确定是否有别的站点在传输数据。如果媒体空闲，该站点便可传输数据；否则，该站点将避让一段时间后再做尝试。这就需要有一种退避算法来决定避让的时间，常用的退避算法有非坚持、1－坚持、P－坚持三种。

1、非坚持算法

算法规则为：

⑴如果媒本是空闲的，则可以立即发送。

⑵如果媒体是忙的，则等待一个由概率分布决定的随机重发延迟后，再重复前一步骤。采用随机的重发延迟时间可以减少冲突发生的可能性。非坚持算法的缺点是：即使有几个着眼点为都有数据要发送，但由于大家都在延迟等待过程中，致使媒体仍可能处于空闲状态，使用率降低。

2、1-坚持算法

算法规则：

⑴如果媒体空闲的，则可以立即发送。

⑵如果媒体是忙的，则继续监听，直至检测到媒体是空闲，立即发送。

⑶如果有冲突(在一段时间内未收到肯定的回复)，则等待一随机量的时间，重复步骤⑴～⑵。

这种算法的优点是：只要媒体空闲，站点就立即可发送，避免了媒体利用率的损失；其缺点是：假若有两个或两个以上的站点有数据要发送，冲突就不可避免。

3、P-坚持算法

算法规则：

⑴监听总线，如果媒体是空闲的，则以 P 的概率发送，而以(1-P)的概率延迟一个时间单位。一个时间单位通常等于最大传播时延的 2 倍。

⑵延迟一个时间单位后，再重复步骤⑴。

⑶如果媒体是忙的，继续监听直至媒体空闲并重复步骤⑴。

P-坚持算法是一种既能像非坚持算法那样减少冲突，又能像 1-坚持算法那样减少媒体空闲时间的折中方案。问题在于如何选择 P 的有值，这要考虑到避免重负载下系统处于的不稳定状态。假如媒体是忙时，有 N 个站有数据等待发送，一旦当前的发送完成时，将要试图

传输的站的总期望数为 NP。如果选择 P 过大，使 NP＞1，表明有多个站点试图发送，冲突就不可避免。最坏的情况是，随着冲突概率的不断增大，而使吞吐量降低到零。所以必须选择适当 P 值使 NP＜1。当然 P 值选得过小，则媒体利用率又会大大降低。

4.3.2 具有冲突检测的载波监听多路访问 CSMA/CD

在 CSMA 中，由于信道传播时延的存在，即使总线上两个站点没有监听到载波信号而发送帧时，仍可能会发生冲突。由于 CSMA 算法没有冲突检测功能，即使冲突已发和，仍然将已破坏的帧发送完，使总线的利用率降低。

一种 CSMA 的改进方案是使发送站点传输过程中仍继续监听媒体，以检测是否存在冲突。如果发生冲突，信道上可以检测到超过发送站点本身发送的载波信号的幅度，由此判断出冲突的存在。一于检测到冲突，就立即停止发送，并向总线上发一串阻塞信号，用以通知总线上其它各有关站点。这样，通道容量就不致因白白传送已受损的帧而浪费，可以提高总线的利用率。这种方案称做载波监听多路访问/冲突检测协议，简写为 CSMA/CD，这种协议已广泛应用于局域网中。

CSMA/CD 的代价是用于检测冲突所花费的时间。对于基带总线而言，最坏情况下用于检测一个冲突的时间等于任意两个站之间传播时延的两倍。从一个站点开始发送数据到另一个站点开始接收数据，也即载波信号从一端传播到另一端所需的时间，称为信号传播时延。信号传播时延(μs)=两站点的距离(m)/信号传播速度(200m/μs)。如图 4.9 所示，假定 A、B 两个站点位于总线两端，两站点之间的最大传播时延为 tp。当 A 站点发送数据后，经过接近于最大传播时延 tp 时，B 站点正好也发送数据，此时冲突便发生。发生冲突后，B 站点立即可检测到该冲突，而 A 站点需再经过一份最大传播时延 tp 后，才能检测出冲突。也即最坏情况下，对于基带 CSMA/CD 来说，检测出一个冲突的时间等于任意两个站之间最大传播时延的两倍(2tp)。

数据帧从一个站点开始发送，到该数据帧发送完毕所需的时间和为数据传输时延；同理，数据传输时延也表示一个接收站点开始接收数据帧，到该数据帧接收完毕所需的时间。数据传输时延(s)=数据帧长度(bit)/数据传输速率(bps)。若不考虑中继器引入的延迟，数据帧从一个站点开始发送，到该数据帧被另一个站点全部接收所需的总时间，等于数据传输时延与信号传播时延之和。

由上述分析可知，为了确保发送数据站点在传输时能检测到可能存在的冲突，数据帧的传输时延至少要两倍于传播时延。换句话说，要求分组的长度不短于某个值，否则在检测出冲突之前传输已经结束，但实际上分组已被冲突所破坏。由此引出了 CSMA/CD 总线网络中最短帧长的计算关系式：

最短数据帧长(bit)	任意两站点间的最大距离(m)
数据传输速率(Mbps)	200m/us

计算时要注意单位统一。

由于单向传输的原因，对于宽带总线而言，冲突检测时间等于任意两个站之间最大传播时延的 4 倍。所以，

对于宽带 CSMA/CD 来说，要求数据帧的传输时延至少 4 倍于传播时延。

在 CSMA/CD 算法中，一旦检测到冲突并发完阻塞信号后，为了降低再次冲突的概率，需要等待一个随机时间，然后再使用 CSMA 方法试图传输。为了保证这种退避操作维持稳定采用了一种称为二进制指数退避和算法，其规则如下：

(1)对每个数据帧，当第一次发生冲突时，设置一个参量 L=2；

(2)退避间隔取 1 到 L 个时间片中的一个随机数，1 个小时片等于两站之间的最大传播时延的两倍；

(3)当数据帧再次发生冲突，由将参量 L 加倍；

(4)设置一个最大重传次数，超过该次数，则不再重传，并报告出错。

二进制指数退避算法是按后进先出 LIFO(List In First Out)的次序控制的，即未发生冲突或很少发生冲突的数据帧，具有优先发送的概率；而发生过多次冲突的数据帧，发送成功的概率就更少。

IEEE 802.3 就是采用二进制指数退避和 1-坚持算法的 CSMA/CD 媒体访问控制方法。这种方法在低负荷时，如媒体空闲时，要发送数据帧的站点能立即发送；在重负荷时，仍能保证系统的稳定性。由于在媒体上传播的信号会衰减，为确保能检测出冲突信号，CSMA/CD 总线网限制一段无分支电缆的最大长度为 500 米。

4.3.3 IEEE 802.3 媒体访问控制协议

1.CSMA/CD 总线的实现模型

IEEE 802.3 是一个使用 CSMA/CD 媒体访问控制方法的局域网标准。CSMA/CD 总线的实现模型如图 4.10 所示，它对应于 OSI/RM 的最低两层。从逻辑上可以将其划分为两大部分：一部分由 LLC 子层和 MAC 子层组成，实现 OSI/RM 的数据链路层功能，另一部分实现物理层功能。

把依赖于媒体的特性从物理层中分离出来的目的，是要使得 LLC 子层和 MAC 子层能适应于各类不同的媒体。

物理层内定义了两个兼容接口：依赖于媒体的媒体相关接口 MDI 和访问单元接口 AUI。MDI 是一个同轴电缆接口，所有站点都必须遵循 IEEE 802.3 定义的物理媒体信号的技术规范，与这个物理媒体接口完全兼容。由于大多站点都设在离电缆连接处有一段距离的地方，在与电缆靠近的 MAC 中只有少量电路，而大部分硬件和全部的软件都在站点中，AUI 的存在为 MAC 和站点的配合使用带来了极大的灵活性。

MAC 子层和 LLC 子层之间和接口提供每个操作的状态信息，以供高一层差错恢复规程所用。MAC 子层和物理层之间的接口，提供包括成帧、载波监听、启动传输和解决争用、在两层间传送串行比特流的设施及用于定时等待等功能。

2.IEEE 802.3 MAC 帧格式

MAC 帧是在 MAC 子层实体间交换的协议数据单元,IEEE 802.3 MAC 帧的格式如图 4.11 所示.

IEEE 802.3 MAC 帧中包括前导码 P、帧起始定界符 SFD、目的地址 DA、源地址 SA、表示数据字段字节数长度的字段 LEN、要发送的数据字段、填充字段 PAD 和帧校验序列 FCS 等 8 个字段。这 8 个字段中除了数据字段和填充字段外，其余的长度都是固定的。

前导码字段 P 占 7 个字节，每个字节的比特模式为“10101010”，用于实现收发双方的时钟同步。帧起始定界符字段 SFD 占 1 个字节，其比特模式为“10101011”，它紧跟在前导码后，用于指示一帧的开始。前导码的作用是使接收端能根据“1”、“0”交变的比特模式迅速实现比特同步，当检测到连续两位“1”(即读到帧起始定界符字段 SFD 最末两位)时，便将后续的信息递交给 MAC 子层。

地址字段包括目的地址字段 DA 和源地址字段 SA。目的地址字段占 2 个或 6 个字节，用于标识接收站点的地址，它可以是单个的地址，也可以是组地址或广播地址。DA 字段最高位为“0”表示单个的地址，该地址仅指定网络上某个特定站点；DA 字段最高位为“1”、其余位不为全“1”表示组地址，该地址指定网络上给定的多个站点；DA 字段为全“1”，则表示广播地址，该地址指定网络上所有的站点。源地址字段也占 2 个或 6 个字节，但其长度必须与目的地址字段的长度相同，宁用于标识发送站点的址。在 6 字节地址字段中，可以利用其 48 位中的次高位来区分是局问部地坦还是全局地址。局部地址是由网络管理员分配，且只在本网中有效的地址；全局地址则是由 IEEE 统一分配的，采用全局地址的网卡出厂时被赋予惟一的 IEEE 地址，使用这种网卡的站点也就具有了全球独一无二的物理地址。

长度字段 LEN 占两个字节,其值表示数据字段的内容即为 LLC 子层递交的 LLC 帧序列,其长度为 0～1500 个字节。

为使 CSMA/CD 协议正常操作，需要维持一个最短帧长度，必要时可在数据字段之后、帧校验序列 FCS 之前以字节为单位添加填充字符。这是因为正在发送时产生冲突而中断的帧都是很短的帧，为了能方便地区分出这些无效帧，IEEE 802.3 规定了合法的 MAC 帧的最短帧长。对于 10Mbps 的基带 CSMA/CD 网，MAC 帧的总长度为 64～1518 字节。由于除了数据字段和填充字段外，其余字段的总长度为 18 个字节，所以当数据字段长度为 0 时，填充字段必须有 46 年字节。

帧校验序列 FCS 字段是 32 位(即 4 个字节)的循环冗余码(CRC),其校验范围不包括前导字段 P 及帧起始定界符字段 SFD。

3. IEEE 802.3 MAC 子层的功能

IEEE802.3 标准提供了 MAC 子层的功能说明,内容主要有数据封装和媒体访问管理两个方面。数据封装(发送和接收数据封装)包括成帧(帧定界和帧同步)、编址(源地址脏乱目的地址的处理)和差错检测(物理媒体传输差错的检测)等；媒体访问管理包括媒体分配和竞争处理。MAC 功能模块如图 4.12 所示。

当 LLC 子层请求发送一数据帧时，MAC 子层的发送数据封装部分便按 MAC 子层的数据帧格式组帧。首先将一个前导 P 和一个帧起始定界符 SFD 附加到帧的开阔部分，填上目的地址和源地址，计算出 LLC 数据帧的字节数，填入数据长度计数字段 LEN。必要时还要将填充字符 PAD 附加到 LLC 数据帧后，以确保传送帧的长度满足最短帧长的要求。最后求出 CRC 校验附加到帧校验列 FCS 中。守成数据封装后的 MAC 帧，便可递交 MAC 子层的发送媒体访问管理部分以供发送。

借助于监视物理层收发信号(PLS)部分提供的载波监听信号，发送媒体访问管理设法避免发送信号与媒体上其它信息发生冲突。在媒体空闲时，经短暂的帧间延迟(提供给媒体恢复时间)之后，就启动帧发送。然后，MAC 子层将串行位流送给 PLS 接口以供发送。PLA 完成产生媒体上电信号的任务，同时监视媒体和产生冲突检测信号。在没有争用的情况下，即可完成发送。发送完成后，MAC 子层通过 LLC 与 MAC 间的接口通知 LLC 子层，等待下一个发送请求。假如产生冲突，PLS 接通冲突检测信号，接着发送媒体访问管理开始处理冲突。道德它发送一串称为阻塞(JAM)码的位诎列来强制冲突，由此食品保证有足够的冲突持续时间，以使其它与冲突有关的发送站点都得到通知。在阻塞信号结束时，发送媒体访问管理就暂停发送，等待一个随机选择的时间间隔后再进行重发尝试。发送媒体访问管理用二进制指数退避算法调整媒体负载。最后，或者重发成功或者在媒体故障、过载的情况下，放弃重发尝试。

接收媒体访问管理部分的功能是，首先由 PLS 检测到达帧，使接收时钟与前导码同步，并接通载波监听信号。接收媒体访问管理部件要检测到达的帧是否错误，帧长是否超过最大长度，是否为 8 位的整倍数。还要过滤因冲突产生的碎片信号(即小于最短长度的帧)。

接收数据解封部分的功能，用于检验帧的目的地址字段，以确定本站点是否应该接收该帧。如地址符合，将其送到 LLC 子层，并进行差错检验。

4.3.4 IEEE 802.3 物理层规范

IEEEE 802.3 委员会在定义可选的物理配置方面表现了极大的多样性和灵活性。为了区分各种可选用的实现方案，该委员会给出了一种简明的表示方法：

〈数据传输率(Mpbs)〉〈信号方式〉〈最大段长度(百米)〉

如 10BASE5、10BASE2、10BROAD36。但 10BASE-F 有些例外，其中的 T 表示双绞线、光纤。IEEE 802.3 的 10Mbps 可选方案见表 4.3。

(1)10BASE5 和 10BASE2。前面介绍 IEEEE 802.3 时所涉及的物理范围，实际上所说的就是基于以太网的 10BASE5。

与 10BASE5 一样，10BASE2 也使用 50 欧姆同轴电缆和曼切斯特编码. 数据速率为 10Mbps. 两者的区别在于 10BASE5 使用粗缆(50mm)，10BASE2 使用细缆(5mm). 由于两者数据传输率相同，所以可以使用 10BASE2 电缆段和 10BASE5 电缆段共存于一个网络中.

(2) 10BASE-T。10BASE-T 定义了一个物理上的星形拓扑网，其中央节点是一个集线器，每个节点通过一对双绞线与集线器相连. 集线器的作用类似于一个转发器，它接收来自一条线上的信号并向其他的所有线转发. 由于任意一个站点发出的信号都能被其他所有站点接收，若有两个站点同时要求传输，冲突就必然发生. 所以，尽管这种策略在物理上是一个星形结构，但从逻辑上看与 CSMA/CD 总线拓扑的功能是一样的。

(3) 10BROAD36。10BROAD36 是 802.3 中为一针对宽带系统的规范，它采用双电缆带宽或中分带宽的 75 欧姆 CATV 同轴电缆。从端出发的段的最大长度为 1800cm，由于是但向传输，所以最大的端－端距离为 3600m。

(4) 10BASE-F。10BASE-F 是 802.3 中关于以光纤作为媒体的系统的规范。该规范中，每条传输线路均使用一条光纤，每条光纤采用曼切斯特编码传输一个方向上的信号。每一位数据经编码后，转换为一对光信号元素(有光表示高、无光表示低)，所以，一个 10bps 的数据流实际上需要 20Mbps 的信号流。

4.4 令牌环媒体访问控制

4.4.1 令牌环工作原理

1. 令牌环的结构

如图 4.13 所示，令牌环在物理上是一个由一系列环接口和这些接口间的点—点链路构成的闭合环路，各站点通过环接口连到网上。对媒体具有访问权的某个发送站点，通过环接口出径链路将数据帧串行到环上；其余各站点边从各自的环接口入径链路逐位接收数据帧，同时通过环接口出径链路再生、转发出去，使数据帧在环上从一个站点至下一个站地环行，所寻址的目的站点在数据帧经过时读取其中的信息；最后，数据帧绕环一周返回发送站点，并由其从上撤除所发的数据帧。

由点—点链路构成的环路虽然不是真正意义上的广播媒体，但环上运行的数据帧仍能被所有的站点接收到，而且任何时刻仅允许一个站点发送数据，因此同样存在发送权竞争问题。为了解决竞争，可以使用一个称为令牌（Token）的特殊比特模式，使其沿着环路循环。规定只有获得令牌的站点才有权发送数据帧，完成数据发送后立即释放令牌以供其它站点使用。由于环路中只有一个令牌，因此任何时刻至多只有一个站点发送数据，不会产生冲突。而且，令牌环上各站点均有相同的机会公平地获取令牌。

2. 令牌环的操作过程

令牌环的操作过程如图 4.14 所示。

（1）网络空闲时，只有一个令牌在环路上绕行。令牌是一个特殊的比特模式，其中包含一位“令牌/数据帧”标志位，标志位为“0”表示该令牌为可用的空令牌，标志位为“1”表示有站点正占用令牌在发送数据帧。

（2）当一个站点要发送数据时，必须等待并获得一个令牌，将令牌的标志位置为“1”，随后便可发送数据。

（3）环路中的每个站点边转发数据，边检查数据帧中的目的地址，若为本站点的地址，便读取其中所携带的数据。

（4）数据帧绕环一周返回时，发送站将其从环路上撤消。同时根据返回的有关信息确定所传数据有无出错。若有错则重发存于缓冲区中的待确认帧，否则释放缓冲区中的待确认帧。

（5）发送站点完成数据发送后，重新产生一个令牌传至下一个站点，以使其它站点获得发送数据帧的许可权。

3.环长的比特度量

环的长度往往折算成比特数来度量，以比特度量的环长反映了环上能容纳的比特数量。假如某站点从开始发送数据帧到该帧发送完毕所经历的时间，等于该帧从开始发送经循环返回到发送站点所经历的时间，则数据帧的所有比特正好布满整个环路。换言之，当数据帧的传输时延等于信号在环路上传播时延时，该数据帧的比特数就是以比特度量的环路长度。

实际操作过程中，环路上的每个接口都会引入延迟。接口延迟时间的存在，相当于增加了环路上的信号传播时延，也即等效于增加了环路的比特长度。所以，接口引入的延迟同样也可以用比特来度量。一般，环路上每个接口相当于增加 1 位延迟。由此，可给出以比特度量的环长计算式：

环的比特长度=信号传播时延×数据传输速率＋接口延迟位数

=环路媒体长度×5(μs/Km)×数据传输速率＋接口延迟位数

式中 5μs/Km 即信号传播速度 200m/μs 的倒数。例如，某令牌环媒体长度为 10Km，数据传输速率为 4Mbps,环路上共有 50 个站点，每个站点的接口引入 1 位延迟，则可计算得：

环的比特长度=10(Km)×5(μs/Km)×4(Mbps)＋1(bit)×50

=10×5×10

如果由于环路媒体长度太短或站点数太少，以至于环路的比特长度不能满足数据帧长度的要求，则可以在每个环接口引入额外的延迟，如使用移位寄存器等。

4.令牌环的维护

令牌环的故障处理功能主要体现在对令牌和数据帧的维护上。令牌本身就是比特串，绕环传递过程中也可能受干扰而出错，以至造成环路上无令牌循环的差错；另外，当某站点发送数据帧后，由于故障而无法将所发的数据帧从网上撤消时，又会造成网上数据帧持续循环的差错。令牌丢失和数据帧无法撤消，是环网上最严重的两种差错，可以通过在环路上指定一个站点作为主动令牌管理站，以此来解决这些问题。

主动令牌管理站通过一种超过机制来检测令牌丢失的情况，该超时值比最长的帧为完全遍历环路所需的时间还要长一些。如果在该时段内没有检测到令牌，便认为令牌已经丢失，管理站将清除环路上的数据碎片，并发出一个令牌。

为了检测到一个持续循环的数据帧，管理站在经过的任何一个数据帧上置其监控位为 1，如果管理站检测到一个经过的数据帧的监控拉的已经置为 1，便知道有某个站未能清除自己发出的数据帧，管理站将清除环路的残余数据，并发出一个令牌。

5.令牌环的特点

令牌环网在轻负荷时，由于存在等待令牌的时间，故效率较低；但在重负荷时，对各站公平访问且效率高。

考虑到帧内数据的比特模式可能会与帧的首尾定界符形式相同，可在数据段采用比特插入法或违法码法，以确保数据的透明传输。

采用发送站点从环上收回帧的策略，具有对发送站点自动应答的功能；同时这种策略还具有广播特性，即可有多个站点接收同一数据帧。

令牌环的通信量可以加以调节，一种方法是通过允许各站点在其收到令牌时传输不同量的数据，另一种方法是通过设定优先权使具有较高优先权的站点先得到令牌。

4.4.2 令牌环媒体访问控制协议

IEEE 802.5 标准规定了令牌环的媒体访问控制子层和物理层所使用的协议数据单元格式和协议，规定了相邻实体间的

的服务及连接令牌环物理媒体的方法。

1. IEEE 802.5 MAC 帧格式

IEEE 802.5 令牌环的 MAC 帧有两种基本格式：令牌帧和数据帧，如图 4.15 所示。

令牌帧只有 3 个字节长，数据帧则可能很长。这两种帧都有一对起始定界符 SD 和结束定界符 ED 用于确定帧的边界，它们中各有 4 位采用曼彻斯特编码中不使用的违法码（“高—高”电平对和“低—低”电平对），以实现数据的透明传输。

访问控制字段 AC 的格式如下：

其中 T 为令牌/数据帧标志位，该位为“0”表示令牌，为“1”表示数据帧。当某个站点要发送数据并获得了一个令牌后，将 AC 字段中的 T 位置“1”。此时，SD、AC 字段就作为数据帧的头部，随后便可发送数据帧的其余部分。M 为监控位，用于检测环路上是否存在持续循环的数据帧。PPP（3 比特）为优先编码，当某站点要发送一个优先级为 n 的数据帧时。必须获得一个 PPP 编码值≤n 的令牌才可发送。RRR（3 比特）为预约编码，当某站点要发送数据帧而信道又不空发时，可以在转发其它站点的数据帧时将自己的优先级编码填入 RRR 中，待该数据帧发送完毕，产生的令牌便有了预约的优先级。若 RRR 已被其它的站点预约了更高的优先级，则不可再预约。将令牌的优先级提升了的站点，在数据帧发送完毕后，还要负责将令牌的优先级较低的站点也有发送数据帧的机会。

帧控制字段 FC 中的前两位标志帧的类型。“01”表示为一般信息帧，即其中的数据字段为上层提交的 LLC 帧；“00”表示为 MAC 控制帧，此时其后的 6 位用以区分控制帧的类型。信息帧只发送给地址字段所指的目的站点，控制帧则发送给所有站点。控制帧中不含数据字段。

数据字段的长度没有下限，但其上限受站点令牌持有时间的限制。令牌持有时间的缺省值为 10 毫秒，数据帧必须在该时段内发送完，超过令牌持有时间，必须释放令牌。

32 位的帧校验序列 FCS 的作用范围自控制字段 FC 起 FC 至 FCS 止，其中不包括帧首（SD、AC 字段）和帧尾（ED、FS 字段）。

帧状态字段 FS 的格式如下：

字段中设置了两位 A 和两位 C，其中 4 位未定义。A 位为地址识别位，发送站发送数据帧时将该位置“0”，接收站确认目的地址与本站相符后将该位置“1”。C 为帧复制位，发送站发送数据帧时将该位置“0”，接收站接收数据帧后将该位置“1”。当数据帧返回发送站时，A、C 位作为应答信号使发送站了解数据帧发送的情况。若返回的 AC=11，表示接收站已收到并复制了数据帧；若 AC=00，表示接收站不存在，但由于缓冲区不够或其它原因未接收数据帧，右等待一段时间后再重发。由于 FS 字段不在 FCS 校验范围内，所以使用两套重复的 A、C 以提高可靠性。

结束定界符 ED 除了用于指示帧的结束边界外，其最后一位还用做差错位，发送站发送数据帧时将该位置“0”。此后，任何一个站点要转发该数据帧时，通时 FCS 校验一旦发现有错，都可以将 E 位置“1”。这样，当数据帧返回时，发送站便可了解数据帧的传输情况。

2. IEEE 802.5 的媒体访问控制功能

令牌环局域协议标准包括四个部分：逻辑链路控制（LLC）、媒体访问控制（MAC）、物理层（PHY）和传输媒体，IEEE802.5 规定了后面三个部分的标准。令牌环的媒体访问控制功能如下：

（1）帧发送。采用沿环传递令牌的方法来实现对媒体的访问控制，取得令牌的站点具有发送一个数据帧或一系列数据帧的机会。

（2）令牌发送。发送站完成数据帧发送后，等待数据帧的返回。在等待期间，继续发送填充字符。一旦源地址与本站相符的数据帧返回后，即发送令牌。令牌发送之后，该站仍保持在发送状态，直到该站点发送的所有数据帧从环路上撤消为止。

（3）帧接收。若接收到的帧为信息帧，则将 FC、DA、Data 及字段复制到接收缓冲区中，

并随后将其转至适当的子层。

（4）优先权操作。访问控制字段中的优先权和预约位配合工作，使环路服务优先权与环上准备发送的 PDU 最高优先级匹配。

4.5 令牌总线媒体访问控制

前面介绍过的 CSMA/CD 媒体访问控制采用总线争用方式，具有结构简单、在轻负载下延迟小等优点，但随着负载的增加，冲突概率增加，性能将明显下降。采用令牌环媒体访问控制具有重负载下利用率高、网络性能对距离不敏感以及具有公平访问等优越性能,但环形网结构复杂，存在检错和可靠性等问题。令牌总线媒体访问控制是在综合了以上两种媒体访问控制优点的基础上形成的一种媒体访问控制方法，IEEE802.4 提出的就是令牌总线媒体访问控制方法的标准。

4.5.1 令牌总线工作原理

令牌总线媒体访问控制访问是将局域网物理总线的站点构成一个逻辑环,每一个站点都在一个有序的序列中被指定一个逻辑位置，序列中最后一个站点的后面又跟着第一个站点。每个站点都知道在它之前的前趋站和在它之后的的后继站垢标识，如图 4.16 所示。

从图中可以看出，在物理结构上它是一个总线结构局域网，但是在逻辑结构上，又成了一种环形结构的局域网。和令牌环一样，站点只有取得令牌，才能发送帧，而令牌在逻辑环上依次(A->D->C->A)循环传递。

在正常运行时，当站点做完该做的工作或者时间终了时，它将令牌传递给逻辑序列中的下一个站点。从逻辑上看，令牌是按地址的递减顺序传送至下一个站点的，但从物理上看，带有目的的令牌帧广播到总线上所有的站点的，但从物理上看，带有目的地址的令牌帧广播总线上所有的站点，当目的站点识别出符号它的地址，即把该令牌帧接收。应该指出，总线上站点的实际顺序与逻辑顺序并无对应关系。

只有收到令牌帧的站点才能将信息帧送到总线上，这就不像 CSMA/CD 访问方式那样，令牌总线不可能产生冲突。由于不可能产生冲突，令牌总线的信息帧长度只需根据要传送的信息长度来确定，就没有最短帧的要求。而对于 CSMA/CD 访问控制，为了使最远距离的站点也能检测到冲突，需要在实际的信息长度后添加填充位，以满足最短帧长度的要求。

令牌总线控制的另一个特点是站点间有公平的访问权。因为取得令牌的站点有报文要发送则可发送，随后，将令牌传递给下一个站点；如果取得令牌的站点没有报文要发送，则立刻把令牌传递到下一站点。由于站点接收到令牌的过程是顺序依次进行的，因此对所有站点都有公平的访问权。

令牌总线控制的优越之处,还体现在每个站点传输之前必须等待的时间总量总是"确定"的，这是因为每个站点发送发送帧的最大长度可以加以限制。当所有站点都有报文要发送，最坏的情况下，等待取得令牌和发送报文的时间，等于全部令牌和报文传送时间的总和；如果只有一个站点有报文要发送，则最坏情况下等待时间只是便部令牌传递时间的总和。对于应用于控制过程的局域网，这个等待访问时间是一个很关键的参数。可以根据需求，选定网中的站点数及最大的报文长度，从而保证在限定的时间内，任一站点都可以取得令牌。

令牌总线访问控制还提供了不同的服务级别，即不同的优先级。

令牌总线的主要操作如下：

(1)环初始化，即生成一个顺序访问的次序。网络开始启动时，或由于某种原因，在运行中所有站点不活动的时间超过规定的时间，都需要进行逻辑环的初始化。初始化的过程是一个争用的过程，角用结果只有一个站能取得令牌，其它的站台点用站插入的算法插入。

(2)令牌传递算法。逻辑环按递减的站地址次序组成，刚发完帧的站点将令牌传递给后

继站，后继站应立即发送数据或令牌帧，原先释放令牌的站监听到总线上的信号，便可确认后继站已获得令牌。

(3)站插队入环算法。必须周期性地给未加入环的站点以机会，将它们插入到逻辑环的适当位置中。如果同时有几个站要插入时，可采用带有响应窗口的争用处理算法。

(4)站退出环算法。可以通过将其前趋站和后继站连到一起的办法，使不活动的站退出逻辑环，并修正逻辑环递减的站地址次序。

(5)故障处理。网络可能出现错误，这包括令牌丢失引起断环，重复地址、产生鑫个令牌等。网络需对这些故障做出相应的处理。

4.5.2 令牌总线媒体访问控制协议

1. IEEE 802.4 MAC 帧格式

IEEE 802.4 标准规定了令牌总线媒体访问控制(MAC)子层、物理层(PHY)所使用的格式和协议，以及连接令牌总线物理媒体的方法，媒体访问协调所有连接的站点对其享媒体的使用。令牌总线的 MAC 帧具有如图 4.17 所示的一般格式。

帧校验序列 FCS 使用 32 位 CRC 码，校验范围为 SD 与 ED 之间的帧内容。数据字段有三类，即 LLC 协议数据单元，MAC 管理数据和用于 MAC 控制帧的数据。在 SD 和 ED 之间的字节数应少于 8191。另外还有异常终止序列格式，仅由 SD 和 ED 两个字节组成。

2.IEEE 802.4 的媒体访问控制功能

逻辑环上的每个站点由三个地址决定它的位置，即本站地址 Ts、前趋地址 Ps 和后继地址 Ns。前趋地址 Ps 和后继地址 Ns 可以动态地设置和保持。

(1)令牌传递算法。逻辑环按递减的站地址次序组成，刚发完帧的 Ts 站点将令牌传递给后继 Ns 站应立即发送数据或令牌帧，Ts 站监将令牌传递给后继 Ns 站，后继 Ns 站应立即了送数据或令牌帧，Ts 站监听到总线上的信号，便可确认后继站已获得令牌.

①Ts 站在发送完整数帧后，发出带有地址 DA=Ns 的令牌传递给下一个站，DA 这目的地址。Ts 站监听总线，若监测到的信息为有效帧，则传递令牌成功。

②若 Ts 站未监测到总线上的有效帧，且已超时，则重复前一步骤。

③此后若 Ts 站仍未监测到有效帧，即第二次令牌传递仍然失败，则原发送站判定后继站有故障，就发送"Who Follows"MAC 控制帧，并将它的后继地址 Ns 放在数据字段中。所有站与该地址相比较，若某站的前趋站是发送站的后继站，则该站发送一个"Set Successor"MAC 控制帧来响应"Who Follows"帧，在"Set Successor"帧中带有该站的地址，于是该站点取得令牌。如此，便将故障的站点排除在逻辑环之外，建立了一个新的连环次序。然后返回第①步。

④如 Ts 站未监听到响应"Who Follows"控制帧的"Set Successor"帧，则重复第③步，再发"Who Follows"帧。

⑤如果第二次"Who Follows"帧发出后，仍得不到响应，则该站就尝试另一策略来重建逻辑环，即再发送请求后继站"Solicit Sucessor 2"MAC 控制帧，并将本站地址作为 DA 和 SA 放入控制帧内，询问环中哪一个站要响应它。收到该询问请求后就会有站点响应。然后，使用响应窗口处理算法来重新建立逻辑环。最后返回第①步。

⑥如果发送"Solicit Successor 2"控制帧后仍无响应，则断定发生发故障。此时，就需要维护逻辑环，使其重新正常工作。

(2)插入环算法。逻辑环上的每个站点应周期性地使新的站点有机会插入环中。当同时有几个站点要插入时，可以采用带有响应窗口的争用处理算法。

(3)退出环算法。方案一：要退出环的 Ts 站接收到令牌后，发送给一个设置后继"Set Successor"MAC 控制帧给 Ps 站，设置后继站为 Ns，并将令牌传递给 Ns 站。

方案二：要退出环的 Ts 站拒绝接收 ps 站发出的"Who Follows"MAC 控制帧，而让 Ns 站

去响应。

(4)逻辑环的初始化操作。初始化操作实质上是增加新站的一特例,其操作过程如下:每个站设置一个环不活动计时器。当某个站点的不活动计时器超时，则发一个请求令牌"Claim Token" MAC 控制帧，控制帧带有一个数据字段，其长度取决于站地址高二位。类似于站插入环的操作，当多个同时试图进行初始化操作时，用基于地址的争用算法，争用结果只能允许一个站点获得令牌。

4.6 光纤分布数据接口 FDDI

光纤由于其众多的越性，在数据通信中得到了日益广泛的应用。用光纤作为媒体的局域网技术主要是光纤分布数据接口 FDDI(Fiber Distributed Data Interface)。FDDI 以光纤作为传输媒体,它的逻辑拓朴结构是一个环,更确切地说是逻辑计数循环环(Logical Counter Rotating Ring),它的物理拓朴结构可以是环形.带树形或带星形的环。FDDI 的数据传输速率可达 100Mbps, 覆盖的范围可达几公里.FDDI 可在主机与外设之间、主机与主机之间、主干网与 IEEE802 低速网之间提供高带宽和通用目的的互连.FDDI 采用了 IEEE802 的体系结构,其数据链层中的 MAC 子层可以在 IEEE802 标准定义的 LLC 下操作。

4.6.1 FDDI 工作原理

1.FDDI 的性能

FDDI 数据传输速率达 100Mbps,采用 4B/5B 编码,要求信道媒体的信号传输率达到 125Mbaud。FDDI 网最大环路长度为 200Km，最多可有 1000 个物理连接。若采用双环节结构时，站点间距离在 2Km 以内，且每个站点与两个环路都有连接，则最多可连接 500 个站点，其中每个单环长度限制在 100Km 内。

FDDI 网络是由许多通过光传送媒体连接成一个或多个逻辑环的站点组成的，因此与令牌环类似，也是把信息发送至环上，从一个站到下一个站依次传递，当信息经过指定的目的站时就被接收、复制，最后，发送信息的站点再将信息从环上撤消。因此 FDDI 标准和令牌环媒体访问控制标准 IEEE802.5 十分接近。FDDI 和 802.5 的主要特性比较见表 4.4

2.数据编码

FDDI 规定了一种很特殊的定时和同步方法。在网络中使用的代码最好是那种信号状态变化频繁的代码,这些状态变化使得接收器能够持续地与输入信号相适应,这样就保证了发送设备和接收设备之间的同步。IEEE802.3 标准中使用的曼彻斯特码只有 50%的效率,因为每一比特都要求线路上有 2 次状态变化(即 2Baud)。如果采用曼彻斯特码,那么 100Mbps 传输速率就要求 200M Baud 的调制速率,也即 200MHz。换言之,曼彻斯特码需要发送数据的 2 倍宽带。

考虑到生产 200MHz 的接口和时钟设备会大大增加成本,ANSI 设计了一种称为 4B/5B 的代码。在这种编码技术中,每次对 4 位数据进行编码,每 4 位数据编码成 5 位符号,用光的存在和不存在表示 5 位符号中每一位是 1 还是 0。这样，对于 100Mbps 的光纤网只需 125NHz 的元件就可实现，使效率提高到 80%。

为了得到信号同步，可以采用二级编码的方法。即先按 4B/5B 编码，然后再利用一种称为倒相的不归零制 NRZI 编码。应该编码确保无论 4 比特符号为何种组合(包括全“0”)，其对应的 5 比特编码中至少有 2 位“1”，从而保证在光纤中传输的信号至少发生两次跳变，以利于接收端的时钟提取。这个原理类似于第 2 章中介绍过的差分编码。

5 比特编码的 32 种组合中，实际只使用了 24 种，其中的 16 种用做数据符合，其余 8 种用做控制符号(如帧的起始和结束符号等)。表 4.5 列出 4B/5B 编码的数据符号部分,所有 16 个 4 位数据符号,经编码后的 5 位码中"1"码至少为 2 位,按 NRZI 编码原理,信号中就至少有两次跳变,因此接收端可得到足够的同步信息.

3.时钟偏移问题

在一般的环形网中，采用只有一个主时钟的集中式时钟方案，在绕环运行时，时钟信号会偏移。每个站点产生的偏移，积累起来还是很可观的。为了消除这种时钟偏移现象，采用一种弹性缓冲器来消除这种偏移。但即使采用了这种措施，由于偏移积累的缘故，也限制了环网的规模。

这种集中式时钟方案，对 100Mbps 高速率的光纤网来说是不适用的。100Mbps 光纤网中每一位的时间为 10ns(而在 4Mbps 环网中，1 位的时间为 250ns)。因此，时钟偏移的影响更严重，如采用集中式时钟方案，就需要每一个站点配置锁相电路，成本会很高。

因此 FDDI 标准规定使用分布式时钟方案，即在每个站点都配有独立的时钟和弹性缓冲器。进入站点缓冲器数据时钟是按照输入信号的时钟确定的，而从缓冲器输出的信号时钟则根据站点的时钟确定，这种方案使环路中中继器的数目不受时钟偏移因素的限制。

4.FDDI MAC 帧格式

FDDI 标准以 MAC 实体间交换的 MAC 符号来表示帧结构,每个 MAC 符号对应 4 个比特,这是因为在 FDDI 物理层中,数据是以 4 位为单位来传输的.FDDI 的令牌帧和数据帧的格式如图 4.18 所示.

前导码 P 用以在收发双方实现时钟同步.发送站点以 16 个 4 位空闲符号(64 个比特)作为前导码.

起始定界符 SD 占一个字节,由两个 4 比特 MAC 非数据符号组成.

帧控制字段 FC 占一个字节,其格式为:

其中 C 表示是同步帧还是异步帧,L 表示是使用 2 字节(16 位)地址还是 6 字节(48 位)地址,FF 表示是 LLC 数据帧还是 MAC 控制帧,若为 MAC 控制帧,则用最后 4 位 ZZZZ 来表示控制帧的类型.

目的地址字段 DA 和源地址字段 SA 可以是 2 字节或 6 字节地址.

数据字段用于装载 LLC 数据或与控制操作有关的停息.FDDI 标准规定最大帧长为 4500 字节.

帧检验序列 FCS 为 4 个字节(32 比特)长.

结束定界符 ED,对令牌来说占 2 个 MAC 控制符号(共 8 比特);其它帧则只占一个 MAC 控制符号(即 4 比特),用于与非偶数个 4 比特 MAC 控制符号的帧状态字段 FS 配合,以确保帧的长度 8 比特的整倍数.

帧状态字段 FS 用于返回地址识别、数据差错及数据复制等状态，每种状态用一个 4 比特 MAC 控制符号来表示。

由上可见，FDDI MAC 帧与 802.5 的 MAC 帧十分相似，不同之处是 FDDI 帧所含有前导码，这对高数据速率下的时钟同步十分重要；允许有网内使用 16 位和 48 位地址，比 802.5 更灵活；令牌帧也不同，没有优先位和预约位，而用别的方法分配信道使用权。

虽然 FDDI 和 802.5 都采用令牌传递的协议，但两者还是存在着一个重要差别，即 FDDI 协议规定发送站发送完帧后，可立即发送新的令牌帧，而 802.5 规定当发送出去的帧的前沿回送至发送站时，才发送新的令牌帧。因此，FDDI 协议具有较高利用率的特点，特别在大的环网中显得更为明显。

4.6.2 FDDI 组成

1982 年 ANSI 的 X3T9.5 委员会提出并在以后陆续制订了由物理层(PHY)、物理层媒体依赖(PMD)和媒体访问控制(MAC)三部分组成的基本 FDDI，1990 年 ISO 也发布了 ISO9314-1(PHY)、ISO9314-2(MAC)和 ISO9314-3(PMD)的国际标准。

FDDI 的基本组成如图 4.19 所示。FDDI 的站点管理 SMI(Station Management)，提供在

节点级上管理各种 FDDI 层次中正在进行的进程所必需的控制，以使节点可以在环上协调地工作。

1.FDDI 的物理层

FDDI 的物理层被分为两个子层：

(1)物理媒体依赖 PMD,它在 FDDI 网络的节点之间提供点--点的数字基带通信。早先的 PMD 标准规定了多模光纤的连接，现在已有关于单模光纤连接的 SMF--PMD,并正在开发与同步光纤网连接的 PMD 子层标准。

(2)物理层协议 PHY，它提供 PMD 与数据链路层之间的连接。

2.FDDI 的数据链路层

FDDI 的数据链路层被分为多个子层：

(1)可选的混合型环控制 HRC(Hybrid Ring Control)，它在共享的 FDDI 媒体上提供分组数据和电路交换数据的多路访问。HRC 由混合多路器(H-MUX)和等时 MAC(I-MUX)两部分组成。

(2)媒体访问控制 MAC，它提供对于媒体的公平和确定性访问、识别地址、产生和验证帧校验序列。

(3)可选的逻辑链路控制 LLC，它提供 MAC 与网络层之间所要求的分组数据适应服务的公共协议。

(4)可选的电路交换多路器(CS-MUX)。

4.7 Novell NetWare 局域网操作系统

4.7.1 局域网操作系统概述

1.局域网操作系统的演变过程

局域网操作系统的定义是：在局域网低层所提供的数据传输能力的基础上，为高层网络用户提供共享资源管理和其它网络服务功能的局域网系统软件。

操作系统是计算机系统中的重要组成部分，它是计算机用户之间的接口。单机操作系统必须具备以下两个基本功能：

(1)为用户提供各种简便有效的访问本机资源的手段。

(2)合理地组织系统工程流程，有效地管理系统。

为实现上述功能，需要在操作系统中建立各种进程，编制不同的功能模块，按层次结构将功能模块有机地组织起来，以完成处理器管理、文件系统管理、设备管理和作业控制等功能。

单机操作系统只能为本地用户使用本机资源提供服务，不能满足开放网络环境的要求。对于连网的计算机系统，它们不仅要为使用本地资源和网络资源提供服务，也要为远地网络用户资源提供服务。局域网操作系统的基本任务就是为用户提供各种基本网络服务功能，完成网络共享系统的安全性服务。

局域网操作系统可以分为两类：面向任务型局域网操作系统和通用型局域网操作系统。面向任务型局域网操作系统是为某一种特殊网络应用要求而设计的;通用型局域网操作系统能提供基本的网络服务功能，以支持各
个领域的需求。

通用型局域网操作系统又可以分为变形系统和基础系统两类。变形系统是以原单机操作系统为基础，通过增加网络服务功能构成的局域网操作系统，基础级系统则是以计算机裸机的硬件为基础,根据网络服务的特殊要求直接利用计算机硬件和少量软件资源进行设计的局域网操作系统。

纵观十多年来的发展，局域网操作系统经历了对等结构向非对等结构演变的过程如图

4.20 所示。

(1)对等结构局域网操作系统。对等结构的局域网操作系统具有以下特点：连网节点地位平等、每个网络
节点上安装的局域网操作系统软件均相同、连网计算机的资源原则上均可相互共享。各连网计算机均可以前后
台方式工作，前台为本地用户提供服务，后台为其它节点的网络用户提供服务。以等结构的对等结构的局域网操作系统可以提供共享硬盘、共享打印机、共享 CPU、共享屏幕、电子邮件等服务。

对等结构局域网操作系统的优点是：结构简单，网络中任意两个节点均可直接通信；而其缺点是：每台连网计算机既是服务器又是工作站，节点要承担较重的通信管理、网络资源管理和网络服务管理等工作。对于早期资源较少、处理能力有限的微机来说，要同时承担多项管理任务，势必降低性能指标。因此，对等结构局域网操作系统支持的网络系统一般规模均较小。

(2)非对等结构局域网操作系统。对等结构局域网操作系统的设计思想是将节点计算机分为网络服务器(SERVER)和网络工作站(WORK STATION，简称 WS)两类。网络服务器采有记配置、高性能计算机，以集中方式管理局域网的共享资源，为网络工作站提供服务；网络工作自欺欺人一般为配置较低的 PC 机，用以为本地资源和网络资源提供服务。

非对等结构局域网操作系统的软件也分为两部分；一部分运行在服务器上；另一部分运行在工作站上。安装运行在服务器上的软件，是局域网操作系统的核心部分，其性能直接决定网络服务功能的强弱。

早期的非对等结构局域网操作系统以共享硬盘服务器为基础，向网络工件作站用户提供共享硬盘、共享打印机、电子邮件、通信等基本服务功能。这种系统效率低、安全性差，使用也不方便。为了克服这些缺点，提出了基于文件服务器的局域网操作系统的设计思想。

基于文件服务器的局域网操作系统操作软件由文件服务器软件和工作站软件两部分组成。文件服务器具有分时系统文件管理的全部功能，向网络作用户提供完善的数据、文件和目录服务。

初期开发的基于文件服务器的局域网操作系统属于变形级系统，其典型实例是 3+网操作系统。在变形级系统中，作为文件服务器的计算机安装了基于 DOS 的文件服务器软件。由于对硬盘的存取控制仍通过 DOS 的 BIOS 进行，因此在服务器大量读/写操作时会造成网络性能的下降。

后期开发的局域网操作系统操作均属于基础级系统，它们具有优越的网络性能，能提供很强的网络服务功能，目前大多数局域网操作系统操作都采用这种方式。其典型实例有 NOVELL NETWARE、MICROSOFT WINDOW NT SERVER、MICROFT LAN MANAGER 及 IBM LAN SERVER 等。

2、局域网操作系统操作系统的基本服务功能

(1)文件服务(FILE SERVER)。文件服务昌局域网操作系统操作中最重要、最基本的网络服务。文件服务器以集中方式管理共享文件，为网络提供完整的数据、文件、目录服务。用户可以根据所规定的权限对文件进行建立、打开、删除、读写等操作。

(2)打印服务(PRINT SERVICE)。打印服务也是局域网操作系统操作提供的基本网络服务功能。共享打印服务可以通过设置专门的打印服务器来实现，打印服务器也可由文件服务器或工作站兼任。局域网中可以设置一台或多台共享打印机，向网络用户提供远程共享打印服务。打印服务实现对用户打印请求的接收、打印格式的说明、打印机的配置、打印队列的管理等功能。

(3)数据库服务(DATABASE SERVICE)。随着局域网应用的深入，用户对网络数据库服务

的需求也日益增加。CLIENT/SERVER 工作模式以数据库管理系统为后援，将数据库操作与应用程序分离开来，分别由服务器端数据库和客户端工作站来执行。用户可以使用结构化查询语言 SQL 向数据库服务器发出查询请求，由数据库服务器完成查询后再将结果传送给用户。CLIENT/SERVER 工作模式优化了局域网操作系统的协同操作性能，有效地增强了局域网操作系统的服务功能。

(4)通信服务(COMMUNICATION SERVICE)。局域网操作系统提供的通信服务主要有工作站与工作站之间的对等通信、工作站与主机之间的通信服务等功能。

(5)信息服务(MESSAGE SERVICE)。局域网可以存储一转方式或对等的点一点通信方式向用户提供电子服务邮件，也可提供文本文件、二进制数据文件的传输服务以及图象、视频、语音等数据的同步传输服务。

(6)分布式服务(DISTRBUTED SERVICE)。局域网操作系统的分布式服务功能，将不同的地理位置的互局域网中的资源组织在一个全局性的、可复制的分布式数据库中，网络中的多个服务器均有该数据库的副本。用户在一个工作站上注册，便可与多个服务器连接。服务器资源的存放位置对于用户来说是透明的，用户可以通过简单的操作访问大型互连局域网中的所有资源。

4.7.2 NOVELL NETQAER 的体系结构

NOVELL 公司开发的 NOVELL NETWARE 网络操作系统是一个可使 PC 机网络取代小型机系统的多任务网络操作系统，它开创了工作站/服务器的结构，在一个 NOVELL 网络中允许有多个文件服务器可适用于不同的网络接口卡(NIA)。NETWARE 具有十分灵活的拓扑结构，如总线、星形、环形和混合形的拓扑结构，并可以和其它网络(如 3+网、TCP/IP 网)在同一网络下工作，NOVELL 网还提供了不同种类的网间连接器。

NOVELL NETWARE 由文件服务器软件、工作站软件、网桥软件等组成。其中文件服务器软件的工作站软件是建网不可缺少的软件，安装时需根据硬件的配置生成。

由于 NOVELL NETWARE 是直接对微处理器编程的，因而它总是可以和最新的微处理器一起发展，并能充分利用微处理器的高性能，形成高效的网络操作系统。

NOVELL NETWARE 操作系统有多种版本，归纳起来可分为 NETWARE86、NETWARE86、NETWARE286 和 NETWARE386 四个阶段。其中 NETWARE386 的性能指标如下：

服务器中桥接网卡最大数：16 块 同时登陆的最大用户数：250 个

推荐的最小服务器 RAM 容量：4MB 服务器可同时打一的文件数：100000 个

每个服务器的文卷最大数：32 个 每个文件最大物理驱动器数：32 个

每个服务器最大物理驱动器数：1024 个 最大文卷容量：32TB

最大的文件占用盘容量：4GB 最大的 RAM 物理地址：4GB

最大总的磁盘容量：32TB 支持共享打印机数：16 台

1、NETWARE 的核心结构

NOVELL NETWARE 是在局域网有基础上建立的网络操作系统，因此它不同于一艉网络协议所需的完整的协议和通信传输功能，它具有所有操作系统的职能，如任务管理、缓冲区管理、文件管理、磁盘及打印等外设管理，因此结构相当复杂。它是一个围绕核心调度的多用户共享资源的操作系统，包括磁盘处理、打印机处理、控制台命令处理及网络通信处理等面向用户的处理程序和一个用户分时核心调度程序，它们之间的关系如图 421 所示。

2、NETWARE 网络层次结构

若将 NETWARE 和标准的网络层次模式作比较，其层次结构的相应关系如图 422 所示。

从物理数据链路层来看，NETWARE 可支持多种网络接口卡，它包括 NOVELL 公司自己的各种网卡的、3COM 公司及别的厂家的网卡。其中有基于总路线的，也有基于令牌环的，还有支持星形网络的 ARCNET 网卡。

NOVELL 网不仅可以使用协议的网络接口卡，也可以使用不同协议的网络接口卡。将使用相同协议的网络接口卡分别连成网，然后将这几个风用网桥连接起来，就形成了更大的 NOVELL 网络。

NOVELL 的网桥可用于完全不同的通信协议，在桥接网络上的用户可以跨桥访问另一网络的文件服务器，无需知道网络的具体配置和通信协议。NOVELL 的网桥可分为内桥、外桥和远程桥几类。

从网络层次结构的第三至七层来看，NETWARE 与标准网络协议有较大差别。因为 NETWARE 是一个基于服务器的网络操作系统，因而 NETWARE 的侧重点在于基于服务器的网络文件系统以及网络管理功能。这与以数据通信为主要目的的网络软件有很大区别。

3、NOVELL NETWARE 的主要特点

(1)NOVELL 网络为用户使用提供完善的安全措施，网络安全对用户来说十分重要，它包括用户口令、目录权限、文件和目录属性以及对用户登陆工作站点及时间的限制。

用户要在文件服务器登陆必须提供“用户名”和相应的口令。用户名是文件服务器识别用户的标志，设置口令的目的则是为了防止冒名顶替者进网。为了网络的安全，管理员可以对网上的某些用户做出登陆限制，包括登陆时间和登陆站点的限制。

用户文件服务器共享磁盘中的目录，由于各用户的身份不同，它们对目录的使用权限也不同。因此，对各用户就有个授权的问题。此外，目录本身也有个权限问题。NOVELL 网络为目录提供了 8 种权限设置，它们是读权、写权、打开权、建立权、删除权、授权权、列目权和修改权。一般来说，共享目录的创建和授权是由管理用户执行的，这样有利于网络的统一管理和安全。一盘用户在共享磁盘的个人目录中，可以创建子目录和其它用户授权。

目录除了有权限还有属性，目录的属性有正常、隐含、系统和专用等 4 种。NOVELL 网针对文件也可以设置属性，它们是只可执行、只可读、可读写、允许共享、不可共享但可读[与、隐文件、索引、上次备份后双已修改、系统文件及允许事务跟踪等属性。

(2)具有系统容错(SFT)的可靠性措施。局域网的可靠性在很大程度上取决于对服务器硬件故障检错和纠错能力。Novell 对文件服务器的共享硬盘采取了较多的可靠性措施。，具体又分为以下几个级别。

第一级是对硬盘目录和文件分配表(FAT)的保护，NetWared 在硬盘的不同区域保存双份的目录和文件分配表，如果一处损坏，系统会自动转向另一处，并在硬盘中另外找一处安排副本。每次启动文件服务器都要例行检查目录和文件分配表的副本，以确认其一致性，目录和文件分配表的复制均由系统自动完成。

第二级是对硬盘表面损坏时的数据保护。为了防止将数据写入磁盘的不可靠块，采用了热调整(Hot Fix)及写后读验证这两个互补技术进行数据保护。热调整技术首先在磁盘上划出一小部分区域(默认值为硬盘容量的 2%)作为热调整重定向区，用于存放因硬盘上的主数据存贮区损坏而被重定向的数据块。

第三级是采用磁盘镜像的方法实现对硬盘驱动器损坏的保护。所谓磁盘镜像，即在一个磁盘通道上有两个成对的磁盘驱动器，同一数据分别写在两台硬盘上，如果一台硬盘驱动器损坏，另一台硬盘能单独运行，不会造成数据丢失和系统停止。磁盘镜像仅用于对硬盘驱动器损坏的保护，磁盘通道控制板的损坏不能得到保护。

第四级是采用磁盘双工，对磁盘通道或硬盘驱动器损坏起到保护作用。磁盘双工是采用两个磁盘通道，每个磁盘通道接磁盘镜像对中的一个硬盘。这样，不仅在通道发生损坏时有保护功能，而且传送数据速度也比单纯的磁盘镜像快得多。

第五是 NetWare 的一个称为事务跟踪系统 TTS(Transaction Teacking Syatem)的附加容错功能，用以防止当数据在写到数据库时，因系统故障而造成的数据库损坏。TTS 起作用时，NetWare 将数据库变更的整个过程看做是单个事务，仅当所有文件正更正之后，事务才

算整个完成。如果在一个事务执行期间发生系统故障，TTS 便放弃这一事务已做的所有修改，并返回到数据库的原始状态。

(3)开放的网络软件开发环境。开放数据链路接口 ODI(Open Data-Link Interface)是 Novell NetWare 的一项重要网络互联技术，它的实现方法是以 NetWare 作为开放式服务器，支持多种通信协议和多种设备驱动程序，以构成异构的计算机网络。ODI 允许在 NetWare 工作站上不必增加网络接口卡,就可使用多种网络协议(IPX/SPX、TCP/IP 等)来扩展网络。

NetWare Streams 流提供了操作系统和网络通信协议(如 IPX/SPX、TCP/IP、SNA、OSI 等)之间的通信接口，它允许在单个文件服务器上存放和使用多种网络协议。

NetWare 的有关网络功能的 C 语言应用函数库，为用户灵活使用函数资源提供了高级语言接口。用户可以在自己的应用环境中，使用 NetWare 的网络功能，建立自身的网络开发环境。NetWare 开放系统结构给用户使用和扩充自己的网络功能提供了极大方便。

4.7.3 Novell 网的硬件配置

经典的 PC 机可分为三类：一类是使用标准结构总线(AT 总线)的 PC 机，大部分网卡都是按 AT 总线设计的：第二类 PC 机使用微通道接口，这样的 PC 机连网时要使用微通道网卡，如 Novell 公司的 NE/2 和 3COM 公司的 3C523 网卡；第三类使用 EISA 总线的 PC 机，需使用 EISA 总线的网卡，如 Novell 公司的 NE3200 网卡。一般 EISA 总线 PC 机都可使用标准的 AT 总线插件，故也可以用总线的网卡。

1.最小配置

(1)服务器：NetWare386 网络的文件服务器需要使用以 80386 或许 86 为主处理器的 PC 机，建议有 4MB 以上内存。文件服务器的内存可以作为磁盘文件的高速缓冲区，如果条件允许应尽量配置多一些，以改善文件用器的响应速度。

(2)工作站：作为工作站的 PC 机的内存建议配置足 640KB，在其中要安装 DOS、中文操作系统以及 NetWare 的 Shell 软件,在此工期基础上再运行用户的应用程序。

(3)外部网桥：应使用 286 以上的微机并具有 1MB 以上内存。

2.网卡参数设置

需要设置的网卡参数有：中断号(IRQ)、I/O 地址、DMA 号以及内存地址。

每块网卡都要有 RAM 作为数据缓冲器，有一些网卡的缓冲器与内存统一编址，使用 640K 至 1MB 的 DOS 保留区，可以直接快速访问，因此事先要设置缓冲器与内存缓冲器的 RAM 地址

每块网卡的参数在出厂时都有已设置好，称之为默认设置。网卡的默认设置有可能和 PC 机内其它设备的设置相冲突。因此。使用前必须根据实际情况重新设置网卡参数。当 PC 机作为网桥需要安装多块网卡时，为使这些网卡上的中断号、I/O 地址、DMA 号及 RAM 地址，如 3C501、3C505、DE-100 网卡都采用这种方法;另一种是用软件设置,如 3C503 网卡。NetWare 软件在安装时设置了多种参数组合以供用户选择。

3、站点地址

每块网卡都有一个网卡地址，这个地址将作为工作站点地址。以太网的地址是 12 位 16 进制的数(即 6 个字节 48 比特)，这个地址在国际上有统一的分配，不会重复。ARCnet 网卡地址范围为 0~255,可通过 8 位拔动开关进行设置。要求设置的占地址在同一个网上不重复，因为网络上的工作站是以网络地址作为惟一标识的。

4.7.4 Novell 网的安装

Novell 网络的安装包括网络硬件和软件的安装。硬件安装包括对硬件的选择、设置和连接，软件安装包括文件服务软件、工作站软件、网桥软件及加值程序的安装。

1、NetWare386 文件服务器软件安装

在安装 Novell NetWare386 V3.1 的文件服务器软件之前，先开辟一个至少 3MB 已格式化的活动 DOS 分区，并使剩余的磁盘区域为空，即无 DOS、NetWare 或其它操作系统使用的

磁盘分区。

(1)复制 SYSTEM-1 盘片的所有文件到 C 盘。

(2)键入的 SERVER(ENTER)。然后按提示键入文件服务器名(由 2~47 个字符组成，不能有句点，也不能有空格)和内部网络号(由 1~8 个 16 进制数字组成)。

(3)在文件服务器上装入磁盘驱动程序。键入命令：

LOAD ISADISK <ENTER>

这里假定是用 AT 兼容机的内部磁盘。

(4)安装 INSTALL 程序。INSTALL 是一个菜单化的程序，它能格式化磁盘和组合磁盘镜像对，形成新的 NetWare 分区、文卷和文件服务器的自举文件，装入 SYSRTEM 和 PUBLIC 文件。在文件服务器上键入命令：

LOAD INSTALL <Enter>

根据菜单提示可进行的操作。

(5)安装网卡、驱动程序和其它要装入模块。先装入 NMAGENT 文件，在文件服务器上键入命令：

LOAD NMAGENT<Enter>

再装入网卡驱动程序，在文件服务器是键入命令：

LOAD<网卡驱动程序> <Enter>

网卡驱动程序与具体支持网络的线缆系统和网卡有关。例如，3c503 网卡的驱动程序为 3C503.LAN,NE3200 网卡的驱动程序为 NE3200LAN。根据提示键入每块网卡的地址和中断号，然后安装其它可装入模块。

(6)将指定的核心协议连接到网卡驱动程序上。NetWare386 不仅支持 IPX 协议，还可支持其它网络协议。想要使某种协议运行于网络之下，就应该将协议模块与网卡驱动程序相连接。用以连接协议与网卡驱动程序的 BIND 命令格式为：

BIND <协议模块> to<网卡驱动程序>

假定要在服务器上运行 IPX 协议，且网卡为 NE2000，则执行如下命令：

BIND IPX to NE2000<Enter>

执行 BIND 命令后，还需为每一个 LNA 驱动程序指派一个可识别其所连接网络的网络编号。根据提示在文件服务器上键入网络号(由 1 ～ 8 个 1 6 进制数组组成)。此网络号的值应与内部网络号的值不同。如果要缺下协议，则应执行 UNBIND 命令：

UNDIND〈协议模块〉from〈网卡驱动程序〉

例如： UNDIND IPX from NE2000 <Enter>

(7)创建文件服务器启动文件(AUTOEXEC.NCT)。在启动文件服务器时，各文件执行顺序是先执行 SERVER.EXE，然后是 STARTUP.NCF，再让系统执行 AUTOEXEC.NCF 完成服务器的启动过程。其中 AUTOEXEC.NCF 保存于 SYS：SYSTEM 目录下，并从中调出执行，其中包含大多数启动命令(磁盘驱动程序装载和名字空间支持命令除外)。

(8)建交 STARTUP.NCF 文件。该文件包含了安装磁盘驱动程序的命令，必要时还可以在其中设置空间支持命令。该文件建立之后将被保存于用以启动 服务器的磁盘上(启动软盘或硬盘 DOS 分区)。

以上几个步骤就是 NetWare386 文件服务器的安装、配置过程。安装了文件服务器之后，每次启动时，系统即通过执行 SERVER.EXE、STARTUP.NCF 和 AUTOEXEC.NCF 文件完成启动过程，进入服务器主控台方式。

2.工作站安装及工作站软件生成

NetWare386 系统不仅可以支持普通的 DOS 工作站,还可以支持 DOS ODI 工作站。ODI(Open Datalink Interface)是基于 Novell 的互连策略的开放数据链接口，它通过支持多重协议和

驱动程序功能和加入到 NetWare 网络系统之中。本节仅对 DOS 工作站的安装做一简要介绍。

工作站软件中最主要的有两个文件：一个是运行 IPX/SPX 协议的 IPX.COM，它管理网络站点之间的通信；另一个是用以进行信息重要定向的文件，即工作站外壳 Shell。它们支持工作站与工作站、工作站与文件服务器之间的会话，也可将它们通称为工作站外壳 Shell 文件。

常规内存的工作站上进行信息重定向的文件夹是 NETX.COM，其中 X 与 DOS 版本号相对应(例如 DOS3.0 以上版本启动工作站,则应使用 NET3.COM)。扩充内存(EMS)和扩展内存(XMS)的工作站，由需分别选用 EMSNETX.EXE、和 XMSNETX.EXE 信息重定向 Shell。

NetWare 工作站 Shell 的作用是对来自工作站应用程序的请求进行解释，它判断这些请求是本地请求还是网络请求。如果是本地请求(比如读写本地硬盘)，则将请求传给 DOS 进行常规处理；如果是网络请求，由将其转换成网络请求格式，并通过网卡将其重向定向到服务器。

(1)准备工作站及安装、设置网卡。PC 及其兼容机等都可作为网络式作站，但至少需要 80KB 内存用以装载 NetWare 工作站文件。安装网卡之前，应正确设置网卡参数。以常用的 3C503 网卡为例，其中 I/O 地址和内存地址可用网卡上的跳线来设置，中断可通过网卡所配置的软件来设置。

(2)运行 SHGEN 生成工作站文件 IPX.COM。SHGEN 存放于 NetWare386 工作站生成盘 SHGEN-1 上。运行 SHGEN,EXE，根据屏幕提示进行相关的操作，即可在软盘或硬盘是生成 IPX.ECOM。

(3)建立工作站启动盘。将生成的特定的 IPX.COM 文件连同系统已提供的其它的 Shell 文件置于同一个可自举的软盘或硬盘中，必要时建立适当的批文件，供启动特定的工作站之用。以建立 DOS3.x 工作站启动软盘为例，具体步骤如下：

①用带”/S“参数的 FORMAT 命令格式化一张 DOS3.x 系统盘。

②将 IPX.COMt 复制到该软盘中，再根据常规内存、扩充内存划扩展内存工作站的不同需要，复制 NET3.COM、EMSNET3.EXE 或 XMSNET3.EXE 该软盘。

③对于特定的应用程序，可能要求 NETBIOS.EXE 和 INT2F.COM 两个文件复制到软盘中。

④建立必要的 AUTOEXEC.BAT 文件以及其它的辅助文件。例如：AUTOEXEC.BAT 的文件内容可为：

```
IPX
NET3 或 EMSNET3 或 XMSNET3
F:
LOGIN
```

完成以上操作后，即生成了工作站启动软盘，运行盘上的批文件就可启动工作站，进而登录入网。

3.网桥及其安装

网桥(Bridge)是用以连接局域网的软件和硬件,经由网桥互连的两个网络通常应使用相同的通信协议、传输介质及寻址方式。NetWare 网桥分为内部网桥和外部网桥两类。内部网桥简称内桥，它存在于文件服务中；外部网桥简称外桥，它建立在一个工作站上。不同子网之间的通信与信息共享是由内桥来实现的，外桥则用以提供路由服务。实际应用中又会涉及与远程网络或工作站的通信，所以又有远程外部网桥及远程工作站的问题。

外部网桥可分为专用外桥和非专用外桥。专用网桥是指这台机器只运行网桥软件，不能再做普通工作站；而非专用网桥可同时用做网桥和工作站。为使网桥更为安全、可靠和高效，建议使用专用网桥。

以外桥互连的目标之间的距离来划分，又可分为本地外桥和远程外桥。本地网桥是指在电缆线允许的长度范围内互连网络的网桥。如果互连网之间的距离超过了电缆线所允许的最

大长度限制，就必须借助其它传输介质(电话线等)来互连,此时用来连接远程网络或远程工作站的网桥就是远程网桥。

一个本地网桥可互连两个本地网络，如图 4.23 所示。若要将一个本地网络与一个远程网络相连，则需要在互连的两端各安装一个远程网桥。若要将本地网络与一个远程工作站相连，则只需在本地网络端安装一个远程网桥，通过该网桥再与远程工作站连接。在连接远程网络或远程工作站时，除需要借助电话线外，在互连两端还分别要使用调制解调器(Modem)。

安装外部网桥的工作主要包括生成网桥软件、配置网桥软件(用于远程连接)和硬件安装三部分。用于生成网桥软件的工具是 BRGEN 程序，生成后的网桥软件需用 ARCONFIG 进行配置。

4.7.5 MetWare 基本命令简介

Novell 网提供两种基本类型的实用程序:菜单实用程序和命令行实用程序。使用菜单实用程序或命令行实用程序都能完成同样的任务。下面简要介绍一些最基本的操作命令。

1.用户操作

用户操作是用户使用网络资源和实现站点间报文传输的命令。

(1)用户登录上网和退网。在 Novell 网文件服务器软件安装成功以后，已自动生成了管理员(SUPERVISOR)和客户(GUEST)两个用户及一个全体成员(EVERYONE)分组。管理员用户可以创建用户，用户一旦被创建，就可以在网络工作站上登录上网。用户登录上网的步骤如下：

①用 DOS 引导工作站 PC 机。

②运行 Shell 软件：

A>IPX<Enter>

A>NET3<Enter>(对应 DOS3.X 版本)。

③登录上网：

A>F:<Enter>

F>LOGIN<Enter>

根据提示键入用户名、口令，即可登录上网。用户退网可使用 LOGOUT 命令。

(2)驱动器映射。网络用户在工作站录进网后，最多可以拥有 26 个磁盘驱动器。一般前 5 个盘符 A：--E：分配给本地驱动器，从 F：--Z：共 21 个盘符可定义为逻辑磁盘驱动器。用户的逻辑磁盘驱动器一旦与文件服务器共享磁盘某文卷上的目录建立了映象关系,便可使用这些目录中的文件，使用方法与单机 DOS 磁盘目录类似。建立映像可使用 MAP 命令。

(3)目录和权限。目录的创建和授权主要是管理员(Supervisor)的工作,对目录权限的操作有设置目录的最大访问权限、授权、撤消权限、查看实际权限等命令。但用户可以用 DOS 命令创建、更名和删除用户目录下的子目录。用户对自己创建的子目录拥有全部权限。

(4)文件的属性。文件的属性主要有三个方面：一是确定该文件是只读文件还是可读写文件；二是确定文件可共享还是不可共享；三是该文件是否允许事务跟踪。要查看或修改文件的属性，可使用 FLAG 命令；查看和修改子目录属性，可使用 FLAGDIR 命令。

(5)发送和接收即时报文。Novell 网络的一个重要功能是发送和接收即时报文。发送报文的命令 SEND，报文长度加上发送方用户名的字符数不得多于 45 个字符，中文则要减半。用户接收报文无需运行其它软件，因为运行 NET3EXE 文件就有接收即时报文的功能。用户若为避免干扰想阻止来自其它站点的报文，可使用 CASTOFF 命令；此后使用 CASTON 命令可恢复报文接收。

(6)网络共享打印。在网络上安装的打印机称为网络共享打印，可供工作站上的用户共享使用。NetWare 386 系统中的共享打印机不论是连接在文件服务器上还是连在用户工作站上，都可以为网上的用户所共享。网络共享打印机的管理核心是打印机队列和假脱机(Spooling)技术。

用户请求在共享打印机上打印的一个任务称为一个打印作业，用户请求的打印被放在打印队列中排队。打印队列实际上是 NetWare 在磁盘上开辟的空间，这个空间用以存放用户请求打印的文件。每个打印队列都有一个队列名，打印队列名是打印队列的标识。

打印队列到打印机的分配关系称为打印机映像。为了不致使打印作业等待时间太长，允许将一个队列指派给两台以上的打印机；同样，服务器上的每一个打印机也可以被指派给两个以上的打印机队列。打印作业的优先次序取决于打印队列的优先级和打印作用在队列中的位置，可以通过控制台命令改变原有打印作业顺序。

假脱机映像是把假脱机号与打印队列联系起来，使用户申请的打印作业进入所分配的打印队列，以便让与假脱机号对应的假脱机程序为该打印队列服务。控制台有专门的命令实现假脱机映像。

(7)查看网络情况。Novell 网向用户提供了一系列作以查看网络情况的命令，它们是：SLIST(查看服务器)、USERLIST(查看已登录用户)、WHOAMI(查看本用户)、CHKVOL(查看文卷)、LISTIME(查看子目录)、NDIR(查看指定目录中文件)、NVER(查看网络软件版本)和 SYSTIME(查看网上时间)等。

(8)设置用户口令。使用命令 SETPASS 或菜单 SYSCON，可以对用户口令进行设置。管理员在创建用户时，可以规定用户口令周期性改变的时间，口令到期后允许用户以老口令继续登录的次数，以及允许在规定时间内打入不正确口令的次数等。用户可以设置或更改自己的口令。

(9)自动执行登录批文件。每个用户可以建立自己的登录批文 AUTOEXEC.BAT，其中可以包括 Shell 命令、登录命令以及逻辑驱动器与目录映像等命令。在登录时，首先执行系统登录文件，然后自动执行用户登录批文件。

(10)SHELL.CFG 文件。该文件是工作站上使用的 Sheel 软件的配置文件，它为 Shell 软件配置任选项，其中有些任选项供 NetBIOS.COM 程序作用。SHELL.CFG 对 Shell 软件的作用，类似于 CONFIG.SYS 对 DOS 的作用。SHELL.CFG 是在工作站上设置 NetWare 所用的参数，应和 IPX.COM 和 NET3.COM 文件放在同一个目录中，以便运行 IPX.COM 和 NET3.COM 时使用 SHELL.CFG 中的选项。NetWare 为 SHELL.CFG 中的大部分选项设置了默认值，因此在工作站上不一定要有 SHELL.CFG 文件。

2.管理员操作

管理员(Suppervisor)是一个特殊的用户，它负责对共享磁盘目录和网络用户的管理。

(1)创建和管理目录结构。一般情况下，在安装好文件服务器软件后，已经在共享盘上建立了系统文卷 SYS:，并在 SYS：文卷中建立 SYSTEM 目录和 PUBLIC 目录。SYSTEM 目录主要供给管理员使用，而 PUBLIC 目录则提供给所有网络用户使用。管理员负责管理共享目录，只有管理员才有权在文卷的根目录下创建目录，而用户创建目录的仅限制在该用户自己的目录中。

(2)创建用户与用户的管理。使用 SYSCON 菜单能够很容易地加入新用户或删除老用户。管理员可以创建用户分组，将一些已创建的用户分在一个组中以便管理。管理员可设定用户的口令与登录安全性，包括对用户口令、用户使用站点、用户使用时间等限定。

(3)网络收费和用户账户.管理员可对网络用户使用网络资源安装记帐服务,进行收费标准设置、账户余额修改、账户限定情况修改等操作.

(4)系统登陆批文件.网络用户在登录时,先执行系统登录批文工团件,然后执行各用户自己的登录批文件.因此,系统登录批文件对网络上的所有用户起作用.只有管理员级的用户才能改变系统登录批文件.要建立或修改系统登录批文件,可使用 SYSCON 菜单编辑登录批文件.

(5)打印机设定.PQINTDEF 可用于创建关于打印机设备的操作方式和打印格式的数据库,

网络管理员负责管理和维护这个数据库.

(6)虚拟控制台操作员.FCONSOLE 是一个虚拟控制台实用程序,它用于管理文件服务器.FCONSOLE 菜单包括广播控制台报文、变更当前文件服务器、连接信息、关闭文件服务器、文件状态、版本信息等项内容。一般网络用户仅能使用 FCONSOLE 菜单中的有限几项子菜单，真正能使用 FCONSOLE 功能的用户是具有虚拟控制台操作员身份的用户。管理员是当然的虚拟控制台操作用户，同时它可以指定富有经验的网络用户作为虚拟控制台操作员用户。

(7)管理员命令。管理员除了使用一般用户使用的所有命令外，主要是使用菜单对网络进行管理操作。此外，NetWare 操作系统还为管理员提供了专用的命令实用程序。管理员命令行实用程序(MAKEUSER 除外)在安装文件服务器软件时已装入文件服务器的 SYS：SYSTEM 目录。管理员专用的命令有 ATOTAL(查看网络上记帐服务汇总表)、BINDFIX(修复组装文件)、BINDREST(将组装文件恢复原样)、HIEFILE(隐含某一文件)、PAUDIT(查看系统记帐记录)、MAKEUSER(建交或删除用户)、SECURITY(检查组装文件中可能有的安全漏洞)、SHOWFILE(把由 HIDEFILE 隐含的文件恢复为不隐含)等。

3.控制台操作员操作

控制台操作员操作的职责是开启和关闭服务器，对网络工作进行监视和控制。控制台操作员可以在文件服务器控制台键入控制台命令，用这些命令来管理网络打印机和打印队列，监视文件服务器的使用，以及控制工作站使用文件服务器资源等。

(1)启动和关闭文件服务器。开启文件服务器的电源即可自举 NetWare 操作系统，此时该机的控制台即为网络操作员控制台。文件服务器下电前必须由控制台操作员关闭文件服务器，在关闭文件服务器之前，控制台操作员必须使用控制台命令 BROADCAST 通知各工作站上的用户退网，同时可使用 DISABLE LODGIN 命令阻止新的用户登录进网.控制台操作还可使用 MONITOR 命令查看是否所有用户已经退网.若有工作站未注销(可能该工作站发生问题无法注销),可使用 CLEAR STATION 命令将该站点清除.当确认所有工作站均已注销后,再使用 DOWN 命关闭文件服务器.此后,作为文件服务器的主机便可以安全关机.

(2)打印管理.控制台命令中有一系列有关打印的命令,使用这些命令可以对打印机和打印队进行管理,能够启、停与文件服务器相接的打印机,创建和删除打印队列,改变打印队列的优先级,观察打印机和打印队列以及打印队列中打印作业的情况等.

(3)其它控制台命令.在控制台中还有 CONFIG(显示网络的硬件配置)、DISK(监视网络磁盘驱动器状态)、MOUNT(使可卸文卷投入服务)、UNMIRROR(关闭驱动器及镜像功能)、SET TIME(设置文件服务器日期和时间)等命令。

(4)锁定控制台键盘。为保证文件服务器的安全，防止控制台为他人误操作，NetWare 提供了 LOCK.VAP 程序。为锁定控制台键盘，在文件服务器控制台键入 LOCK，输入正确的口令，控制台键盘便被锁定。只有再输入口令，才能开放键盘。

(5)远程控制台。远程控制台功能允许控制台操作人员在网上任何地点的工作站上招待网络管理任务。实现远程控制台的先决条件是在文件服务器上装入 REMOTE 和 RSPX 模块，然后在准备作为远程控制台的工站上以 SUPERVISOR 的身份登录上网，此后便可执行远程控制台操作。

5.1 综合业务数字网(ISDN)及异步传输模式(ATM)

产生于 80 年代的综合业务数字网(ISDN),是基于单一通信网络的能提供包括语音、文字、数据、图像等综合业务的数学网.在此之前,各类不同的公众网同时并存,分别提供不同的业务,造成相对独立的割裂状态.例如,电话网提供语音业务、用户电报网提供文字通信业

务、电路交换和分组交换网提供数据传输业务等.ISDN 的目的就是应用单一网络向公众提供不同的业务.

5.1.1 ISDN 的定义及特性

1.ISDN 的定义

ISDN 从字面上解释是 Integrated Services Digital Network 的缩写,译作综合业务数字网.现代社会需要一种社会的、经济的、快速存取信息的手段,ISDN 正是在这种需求的背景下,以及计算机技术、通信技术、VLSI 技术飞速发展的前提下产生的。ISDN 的目标是提供经济有效的端的数字连接标准,就可在很大的区域范围,甚至全球范围内存取网络的信息。目前,窄带 ISDN(N-ISDN)技术在很多发达国家已进入实用阶段.我国也自 1995 年起,开始在一些主要城市实现了 N-ISDN 的商业应用。

2.ISDN 的特性

从上述 ISDN 的定义中,可以看其所具有的三个基本特性:端到的数字连接综合的业务和标准的入网接口。

(1)端到端的数字连接。ISDN 是一个数字网，网上所有的信息均以数字形成进行传输和交换，无论是语音、文字、数据还是图像，事先都是终端设备中被换成数字信号，经和交换。无论是语音、文字,数据,还是图像,事先都在终端设备中被转换成数字信号,经 ISDN 网的数字信息传输到接收方的终端设备后,再还原成原来的语言,文字,数据或图像.

(2)综合的业务.从理论上说,任何形式的原始数据,只要能转换成数字信号,都可以通过 ISDN 进行传输和交换.其典型业务有语音电话,电路交换数据\分组交换数据\信息检索\电子信箱\电子邮箱\智能电报,可视电话,电视会议\传真\监视等.数据传输速率不超过 N*64Kbps(N 为 1-30)的业务,可以采用窄带 ISDN(N-ISDN);对于需要更高数据传输速率的业务,则应采用宽带 ISDN(B-ISDN).

(3)标准的入网接口.ISDN 向用户提供一组标准的多用途网络接口,所谓"多用途",是指入网接口对各类业务都是通用的,也即不同的终端可以经过同一个接口接入网络.

3.ISDN 的技术基础

ISDN 是在数据网技术的基础上发展起来的,数字网的基本上发展起来的,数字网的基本技术包括数字传输,数字交换\网同步和公共信令.

(1)数字传输.数字传输技术可以采用脉码调制(PCM),差分脉码调制(DPCM),自适应差分脉调制(ADPCM),增量调制(M)等多种方式.其中最常用的是 8 比特的 PCM 技术.PCM 是时分多路通信中的主要技术,它的操作包括采样,量化,编码三个过程.数字传输系统可以采用大规模集成电路实现,使设备小型化,而且经济可靠.长距离传输时,可以使用中继消除噪声的积累作用.

(2)数字交换.数字交换系统由硬件共同组成.硬件包括控制系统,话路系统,输入/输出系统等处理机系统;软件包括操作系统;软件包括操作系统,应用程序,用户数据及控制数据.交换网主要由时分交换和空分交换构成.

(3)公共信令.公共信令利用一个公共信道传输多个其它信息的信令.公共信道信令系统除了具有呼叫监视,选择和动行功能外,还具有在交换局之间及交换与各类服务中心之间控制各种信息交换的功能.

(4)同步网技术.同步网向网内所有数字交换设备提供时钟同步控制信号,使它们的时钟频率保持相同的速度.

5.1.2 ISDN 的接口及配置

1.ISDN 的用户－网络接口

ISDN 系统结构主要讨论用户和网络之间的接口，该接口也称为数字位管道。用户－网络接口是用户和 ISDN 交换系统之间通过比特流的“管道”，无论数字位来自数字电话、数

字终端、数字传真还是任何其设备 ，它们都能通过接口双向传输。

用户网络接口用比特流的时分和复用技术多个独立的通道。在接口规范中定义了比特流的确切格式及比特流的复用。CCITT 定义了两种用户－网络接口的标准，它们是基本速率接口 BRI(Basic Rate ISDN)和一次群(基群)束率接口 PRI(Primary Rate ISDN)。

基本速率接口 BRI 是将现有电话网的普通用户线作为 ISDN 用户线而规定的接口，是最常用的 ISDN 用户—网络口。BRI 接口提供了两路 64kbps 的 B(载荷)和一路 16kbps 的 D(信令)通道，即 2B+D，用户能利用的最高传输速率为 64×2+6=144kpbs.B 信道用于传输语音和数据，可以与任何电话线一样连接。D 信道用于发送 B 信道使用的窑信号(即信令)或用于低速的分组数据传输。BRI 一般用于较低速率的系统中。

一次群速率接口 PRI 有两种：一种 PRI 接口提供 30 路 64kbps 的 B 信道和一路 64kbps 的 D 信道，即 30B+D，其传输速率与 2.048Mbps 的脉码调制(PCM)的基群相对应；另一种 PRI 接口提供 23 路 64kbps 的 B 信道和一路 64kbps 的 D 信道，即 23B+D，其传输速率与 1.544Mbps 的 PCM 基群相对应。同样，B 信道用于传输语音和数据。D 信道用于发送 B 信道使用的控制信号或用于用户分组数据传输。PRI 一般用于需要更高速率的系统中。

图 5.1(a)是用于家庭或小型企事业单位的配置，在用户设备和 ISDN 交换系统之间设置一个网络终端设备 NT1。NT1 设置在靠近用户设备一边，利用电话线与数公里外的 ISDN 交换系统相连。NT1 装有一个边接器，无源总线电缆可插入连接器，最多可接 8 个 ISDN 电话、终端或其它设备，连接方法与接入总线局域网的方法相同。NT1 上的连接器是用户和网络的界面。NT1 不仅起连接器的作用，它还包括网络管理、测试、维护和性能监视等功能。在无源总线上的每个设备有一个唯一的地址，NT1 还要解决争用问题，即几个设备同时访问总线时，NT1 来决定哪个设备获得总线访问权。从 OSI 参考模型来看，NT1 是一个物理设备。

对于大的企事业单位，因为要同时进行很多电话对话，总线无法及时处理，所以需要用如图 5.1(b)的配置。在这种配置中有一个网络终端设备 NT2（实际上 NT2 和 NT1 就是前面介绍过的 CBX），NT2 与 NT1 连接，并对各种电话、终端以及其它设备提供真正的接口。NT2 与 ISDN 交换系统没有本质上的差别，只是规模比较小。在单位内部通电话或数字通信只需拨 4 位数字的分机号码，与 ISDN 交换系统无关。CBX 专门分配一个通道与数字位管道连接，拨一个“9”，就能和外线相连。

CCITT 定义了 R、S、T 和 U 四个参考点（见图 5.1）。U 参考点连接 ISDN 交换系统和 NT1，可采用双绞线或光纤；T 参考点是 NT1 上提供给用户扫连接器；S 参考点是 ISDN 的 CBX 与 ISDN 终端的接口；R 参考点利用多个不同的接口连接终端适配器和非 ISDN 终端。

5.1.3 宽带 ISDN(B-ISDN)及其信息传送方式

当今人们对通信的要求越来越高，除原有的语音、数据、传真业务外，不要求综合传输高清晰度电视、广播电视、高速数据传真等宽带业务。计算机技术、微电子技术、宽带通信技术和光纤传输的发展，为满足这些迅猛增长的通信需求提供了基础。

早在 1985 年 1 月，CCITT 第 18 研究组就成立了专门小组着手研究宽带 ISDN，并提出了关于 B-ISDN 的建设性框架。此后，就采用同步时分方式 STM（Synchromous Transfer Mode）还是异步传输模式 ATM（Asynchronous Transfer Mode）进行了多年讨论，到 1989 年，由于解决了 ATM 存在的许多问题，才一致同意采用 ATM 方式，并要求 CCITT 加速制定 ATM 标准，以促进 B-ISDN 的发展。由此在 1990 年 11 月召开的第 18 研究组全体会议上通过了关于 B-ISDN 的 I-系列建议草案。

由窄带 ISDN 向宽带 ISDN 的发展，可分为三个阶段。

第一阶段是进一步实现话音、数据和图象等业务的综合。它由如图 5.2(a)所示的三个独立的网构成初步综合的 B-ISDN。由 ATM 构成的宽带交换网实现话音、高速数据和活动图象的综合传输。

第二阶段的主要特征是 B-ISDN 和用户--网络接口已经标准化，光纤已进入家庭，光交换技术已广泛应用，因此它能提供包括具有多频道的高清晰度电视 HDTV（High Definition Televition）在内的宽带业务，其结构如图 5.2(b)。

第三阶段的主要特征是在宽带 ISDN 中引入了智能管理网，其结构如图 5.2(c)所示,由智能网控制中心来管理三个基本网。智能网也可称做智能宽带 ISDN，其中可能引入智能电话、智能交换机及用于工程设计或故障检测与诊断的各种智能专家系统。

目前 B-ISDN 采用的传输模式主要有高速分组交换、高速电路交换、异步传输模式 ATM 和光交换方式四种。

高速分组交换是利用分组交换的基本技术，简化了 X.25 协议，采用面向连接的服务，在链路上无流量控制、无差错控制，集中了分组交换和同步时分交换的优点，已有多个试验网已投入运行。

高速电路交换主要采用多速时分交换方式（TDSM），这种方式允许信道按时间分配，其带宽可为基本速率的整数倍。由于这是快速电路交换，其信道的管理和控制十分复杂，尚有许多问题需要继续研究。

光交换技术的主要设备是光交换机，它将光技术引入传输回路，实现数字信号的高速传输和交换。

关于异步传输模式 ATM，将在下一小节做较详细介绍。

5.1.4 ATM 原理

1.ATM 的定义与功能

CCITT 在 I 系列建议中给 ATM 下了这样的定义：ATM 是一种转换模式（即前面所说的传输方式），在这一模式中信息被组织成信元（Cell），包含一段信息的信元并不需要周期性地出现在信道上，从这个意义上说，这种传输是异步的。

ATM 的特点是进一步简化了网络功能。ATM 网络不参与任何数据链路层功能，将差错控制与流量控制工作都交给终端去做。

图 5.3 是分组交换、帧中计和 ATM 交换三种方式的功能比较。可以看出，分组交换网的交换折点参与了 OSI 第 1 层到第 3 层的全部功能;帧中继节点只参与第 2 层功能的核心部分(2a)，也即数据链路层中的帧定界、0 比特插入和 CRC 检验功能，第 2 层的其它功能，即差错控制和流量控制，以及第 3 层功能则由终端处理；ATM 网络则更简单，除了第 1 层的功能之外，交换节点不参与任何工作。从功能分布的情况来看，ATM 网和电路交换网有点相似，可以说 ATM 网是综合了分组交换和电路交换的优点而形成的一种网络。

TAM 克服了其它传送方式的缺点，能够适应任何类型的业务，不论其速度高低、突发性大小、实时性要求和质量要求如何，都能提供满意的服务。

2.ATM 的信元

新元实际上就是分组，只是为了区别于 X.25 的分组，才将 ATM 的信息单元叫作单元。ATM 的信元具有固定的长度，即总是 53 个字节。其中 5 个字节是信头(Header),48 个字节是信息段。信头包含各种控制信息，主要是表示信元去向的逻辑地址，另外还有一些维护信息、优先级及信头的纠错码。信息段中包含来自各种不同业务的用户数据，这些数据透明地穿越网络。新元的格式与业务类型无关，任何业务的信息都同样被切割封装成统一格式的单元。

ATM 的信头有两种格式，分别对应用户－网络接口 UNI 和网络节点接口 NNI。UNI 信头的格式如图 5.4 所示，其中个字段的含义及功能如下：

(1)一般流量控制字段 GPC(Generic Flow Control),又称接入控制字段。当多个信元等待传输时，用以确定发送顺序的优先级。

(2)虚通道标识字段 VPI(Virtual Path Identifier)和虚通路标识字段 VCI(Virtual Channel Identifier)用做路由选择。

(3)负荷类型字段 PT(Payload Type)用以标识信元数据字段所携带的数据的类型。

(4)信元丢失优先级字段 CLP(Cell Loss Priority)用于阻塞控制，若网络出现阻塞时，首先丢弃 CLP 置位的信元。

(5)信头差错控制字段 HEC(Head Error Control)用以检测信头中的差错，并可纠其中的 1 比特错。HEC 的功能在物理层实现。

3、ATM 的工作方式

ATM 采用如图 5。5 所示的异步时分复用方式工作，来自不同信息源的信元汇集到一起，在一个缓冲器内排队，队列中的信元著个输出到传输线路，在传输线路上形成首尾相接的信元流。信元的信头中写有信息的标志(如 A 和 B)，说明该信元去往的地址，网络根据信头中的标志来转移信元。

信息源随机地产生信息，因为信元到达队列也是随机的。高速的业务信元来得十分频繁、集中，低速的业务信元来得很稀疏。这些信元都按先来后到在队列中排队，然后按输出次序复用到传输线上。具有同样标志的信元在传输线上并不对应某个固定的时间间隙，也不是按周期出现的，也即信息和它在时域的位置之间没有关系，信息只是按信头中的标志来区分的。这种复用方式称为异步时分复用(Asynchronous Time Division Multiolex)，又称统计复用(Statistic Multiptx)。而在同步时分复用方式(如 PCM 复用方式)中，信息以它在一帧中的时间位置(时隙)来区分，一个时隙对应着一条信道，不需要另外的信息头来标识信息的身份。

异步时分复用方式使 ATM 具有很大的灵活性，任何业务也都可按实际需要来占用资源。对于特定的业务，传送速率可随信息到达的速率而变化，因此网络资源得到了最大限度的利用。ATM 网络可以适用于任何业务，不论其特性如何(速率高低、突发性大小、质量和实时性要求等)，网络都按同时的模式来处理，真正做到了完全的业务综合。

若某个时刻队列中没有等待发送的信元，此时线路上就出现未分配信元(信头中含有标志 φ)；反之，若某个时刻传输线路上找不到可以传送新元的机会(信云啊都已排满)，而队列已经充满缓冲区，此时为了尽量减少对业务质量的影响，将优先级别低的信元丢弃。缓冲区的容量必须根据信息流量来计算，以使信元丢弃率在 10-9 以下。

为了提高处理速度和降低延迟，ATM 以面向连接器的方式工作。网络的处理工作十分简单：通信开始时建立虚电路，以后用户将虚电路标志写入信头(即地址信息)，网络根据虚电路标志将信元送往目的地。

经过 ATM 网络中的节点提供信元的交换。其实，ATM 网络的节点完成的只是虚电路的交换，因为同一虚电路上的所有信元都选择同样的路由，经过同样的通路到达目的地。在接收段，这些信元到达的次序总是和发送次序相同。

ATM 交换节点的工作比 X.25 分组交换网中的节点要简单得多。ATM 节点只做信头的 CRC 检验，对于信息的传输差错根本不过问。ATM 节点不做差错控制(信头中根本你没有信元的编号)，也不参与流量控制，这些工作都留给终端去做。ATM 节点的主要工作就是读信头，并根据信头的内容快速的将信元送往要去的地方，这件工作在很大的程度上依靠硬件来完成，所以 ATM 交换的速度非常快，可以和光纤的传输速度相匹配。

5.2 帧中继（Frame Relay）

5.2.1 帧中继的基本原理

帧中继是继 X.25 后发展起来的数据通信方式。从原理上看，帧中继与 X.25 及 ATM 都同属分组交换一类。但由于 X.25 带宽较窄，而帧中继和 ATM 带宽较宽，所以常将帧中继和 ATM 称为快速分组交换。

帧中继保留了 X.25 链路层的 HDLC 帧格式但不采用 HDLC 的平衡链路接入规程 LAPB(Link Access Procedure－Balanced)，而采用 D 通道链路接入规程 LAPD（Link Access Procedure

on the D-Channel）。LAPD 规程能在链路层实现链路的复用和转接，所以帧中继的层次结构中只有物理层和链路层。

与 X.25 相比，帧中继在操作处理上做了大量的简化。帧中继不考虑传输差错问题，其中节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量控制均交由高层端系统完成，所以大大缩短了节点的时延，提高了网内数据的传输速率。

5.2.2 帧中继的帧格式

帧中继的帧结构如图 5.6 所示，它类似与 HDLC 的帧格式，不过没有控制字段。

帧中继的帧格式中，标志字段 F 和帧校验序列 FCS 的作用与 HDLC 中的类似。F 字段用以标志帧的起始和结束，其比特模式为 01111110，可采用 0 比特插入法实现数据的透明传输。FCS 字段用于帧的验错，若传输中出错，则有接收端将之丢弃并通知发送端重发。

帧格式中的地址字段的主要作用是路由寻址，也兼管阻塞控制。地址字段一般由 2 个字节组成，在需要时也可扩展到 3 或 4 个字节。地址字段的组成如下（参见图 5.6）：

数据链路连接标识符 DLCI 由高、低两部分共 10 比特组成，用于唯一表示一个虚连接。

命令 / 相应位 C/R 与高层应用有关，帧中继本身并使用。

扩展地址位 EA 为“0”表示下一字节仍为地址，为“1” 表示地址结束，用于对地址字段进行扩展。对于 2 字节地址，其 EA0 为“0”、EA1 为“1”。

发送方将前向显示阻塞通知位 FECN 置为"1"，用于通知接收方网络出现阻塞；接收方将反向显示阻塞通知位 PECN 置"1"，用于通知发送方网络出现阻塞。

可丢弃位 DE 由用户设置，若置“1”，表示当网络发生阻塞时，该帧可被伏先丢弃。

5.2.3 帧中继的应用

帧中继既可作为公用网络的接口，也可作为专用网络的接口。专用网络接口的典型实现方式是，为所有的数据设备安装带有帧中继网络接口的 T1 多路选择器，而其它如语音传输、电话会议等应用则仅需安装非帧中继的接口。这两类网络中，连接用户设备和网络装置的电缆可以用不同速率传输数据，一般速率在 56Kbps 到 E1 速率（2.048Mbps）间。

帧中继的常见应用简介如下：

（1）局域网的互连。由于帧中继具有支持不同数据速率的能力，使其非常适于处理局域网-局域网的突发数据流量。传统的局域网互连，每凿一条端-端线路，就要在用户的路由器上增加一个端口。基于帧中继的局域网互连，只要局域网内每个用户至网络间有一条带宽足够的线路，则既不用增加物理线路也不占用物理端口，就可增加端-端线路，而不致对用户性能产生影响。

（2）语音传输。帧中继不仅适用于对时延不敏感的局域网的应用，还可以进行对时延要求较高的低档语音（质量伏于长途电话）的应用。

（3）文件传输。帧中继既可保证用户所需的带宽，又有实满意的传输时延，非常适合大流量文件的传输。

5.3 快速/高速局域网

5.3.1 快速成以太网

1.100BASE-T 媒体访问控制方法

IEEE 于 1995 年通过了 100Mbps 快速以太网的 100 BASE-T 标准，并正式命名为 IEEE802.3u 标准，作为对 IEEE802.3 标准的补充。100BASE-T 标准不但在最大程度上保持了 IEEE802.3 标准的完整性，而且保留了核心以太网的细节规范。

虽然 100BASE-T 仍采用常规 10Mbps 以太网的 CSMA/CD 媒体访问控制方法，但其性能是 10BADE-T 的 10 倍，而价格仅为其一半。100BASE-T 的 MAC 与 10BASE-T 的 MAC 相比，除了帧际间隙缩短到原来的 1/10 外，两者的帧格式及参数完全相同。100BADE-T 的 MAC 出可以运

行于不同的速率，并能与不同的物理层接口。这样，原先 10Mbps 以太网上运行的软件不加任何修改即可在快速以太网上运行，原先的协议分析和管理工具也可轻易地被继承。

为了能成功地进行冲突检测，100BASE-T 也必须满足“最短帧长冲突检测时间*数据传输速率”的关系。其中的冲突检测时间等于网络中最大传播时延的 2 位。100BASE-T 与 10BASE-T 的 MAC 帧相同，两者的最短帧长均为 64 字节（512 比特），但由于 100BASE-T 的数据速率提高了 10 位，故相应的冲突检测时间缩短为 10BASE-T 的 1/10，由此整个网络的直径（任何两站点间的最大跳）也减小到 10BASE-T 的 1/10。

2.100BASE-T 的物理层

100BASE-T 和 10BADE-T 的区别在物理层标准和网络设计方面。100BASE-T 的物理层包含三种媒体选项：100BASE-TX、100BASE-FX 和 100BADE-T4，见表 5.1。

（1）100BASE-TX 和 100BASE-FX。100BADE-TX 和 100BASE-FX 均采用两对链路，其中一对用于发送，另一对用于接收，每对链路实现单方向的 100MBPS 数据速率。100BASE-TX 使用屏蔽双绞线或 5 类非屏蔽双绞线，100BASE-FX 则使用光纤。

100BASE-TX 和 100BASE-FX 都使用高效 4B/5B NRXI 编码。NRZI 为差分不归零制编码，这种编码与常规的不归零制（NRZ）编码的区别在于每个“1”码开始处都有跳变、每个“0”码开始处没有跳变。在 NRZI 编码中的，信号通过相邻码元极性的跳变来解码，而不是简单地绝对电平为准，由此可获得更高的抗干扰能力。

（2）100BASE-TT4。10BASE-T4 是为在低质量要求的 3 类非屏蔽双绞线上实现 100MBPS 数据速率而设计的，该规范也可使用 4 类或 5 类非屏蔽双绞线。

要想直接用一对 3 类非屏蔽双绞线获取 100MBPS 的数据速率几乎是不可能的。因此，100BASE-T4 采用一种称为 8B/6T 的编码方案。该方案将原始数据流分为 3 股子数据流，经 4 对子信道 D1--D4 传输，每个子信道的数据速率为 33.3MBPS。其中 D1、D3、D4 用于发送，D2，D3,D4 用于接收。因此，D3\D4 被配置为双向传输。另外，D2 既用于接收，有用于冲突检测。每个子信道中，将每 8 为数据为单位影谢成一个 6 位的信号码组，这样，子信道的信号传输速率便为 33.3×（6/8)=25Mbaud。

5.3.2 千兆以太网

随着多媒体技术,网络分布计算,桌面视频会议等应用的不断发展,用户对局域网的带宽提出了更高的要求.同时,100M 快速以太网也要求主干网,服务器一级有更高的带宽.另外,由于以太网的简单,使用,廉价及应用 的广泛应用性,人们有迫切要求高网速技术与现有的以太网保持最大的兼容性.千兆以太网技术就是在这种需求背景下开始酝酿的.1996 年 3 月成立的 IEEE802.3Z 工作组，专门负责千兆以太网的研究，并制定相应标准。

千兆以太网使用原有以太网的帧结构、帧长及 CSMA/CD 协议，只是在低层将数据速率提高到了 1Gbps。因此，它与标准以太网（10Mbps）及快速以太网（100Mbps）兼容。用户能在保留原有操作系统、协议结构、应用程序及网络管理平台与工具的同时、通过简单的修改，使现有的网络工作站廉价地升级到千兆位速率。

1、千兆以太网的物理层协议

千兆以太网的物理层协议包括 1000BASE－SX、1000BASE-LX、1000BASE-CE、和 1000BASE-T 等标准。

(1)1000BASE-SX。使用芯径为50及6.2微米,工作波长为850nm的多模光纤,采用8B/10B编码方式,传输距离分别为 525m、和 260m，适用于建筑物中同一层的短距离主干网。

（2）1000BASE－LX。使用芯径为 50 及 62.5 微米的多模、单模光纤，工作波长为 1300m,采用 8B / 1B 编码方式，传输距离分别是 525m、550m、和 3000m，主要用于校园主干网。

（3）1000BASE-CE。使用 15 欧姆平衡屏蔽双绞线（STP)，采用 8B/10B 编码方式，传输速率为 1.25Gbps，传输距离为 25m,主要用于集群设备的连接,如一个交换机房的设备互联。

（4）1000BASE-T。使用 4 对 5 类非平衡屏蔽双绞线（UTP），传输距离为 100m,主要用于结构化布线中同一层建筑的通信，从而可以利用以太网或快速以太网已铺设的 UTP 电缆。

2.千兆以太网的 MAC 子层

MAC 子层的主要功能包括数据帧的封装 / 御载、帧的寻址与识别,帧的解收与发送,链路的管理、帧帧的差错控制及 MAC 协议的维护。

千兆以太网的帧结构与标准以太网的帧结构相同，其最大帧长为 1518 字节，最小帧长为 46 字节。

千兆以太网对媒体的访问采用全双工和半双工两种方式。全双工方式适用于交换机到交换机或交换机到站点之间点－点连接，两点间可以同时进行发送与接收，不存在共享信道的争用问题，所与不需采用 CSMA/CD 协议。半双工协议则适用于共享媒体的连接方式，仍采用 CSMA/CD 协议解决信道的争用问题。

千兆以太网的诗句传输率为快速以太网的 10 倍，若要保持两者最小帧长的一致性，势必大大缩小千兆以太网的网络直径；若要维持网络直径为 200m,则最小帧长要 512 字节。为了确保最小帧长为 64 字节，同时维持网络直径为 200M，千兆以太网采用了载波扩展和数据报分组两种技术。

载波扩展技术用于半双工的 CSMA/CD 方式,实现方法是对小于 512 字节的帧进行载波扩展，使这种帧所占用的时间等同与长度为 512 字节的帧所占用的时间。虽然载波扩展信号不携带数据，但由于他的存在保证了 200M 的网络直径。对于≥512 字节的帧，不必添加载波扩展信号。若大多数帧短于 512 字节，则载波扩展技术会使带宽利用率下降。

数据包分组技术允许站点每次发送多帧，而不是一次发送一帧。若多个连续的数据帧短于 512 字节，仅其中的第一帧需要添加载波扩展信号。一旦第一帧发送成功，则说明发送信道已打通，其后续帧就可不加载波扩展连续发送，只需帧间保持 12 字节的间期即可。

由于全双工方式不存在冲突问题,所以不需要任何处理机可传输 64 字节的最小数据帧。

3.千兆以太网的特点

一方面为了保持从标准以太网、快速以太网到千兆以太网的平滑过渡，另一方面又要兼顾新的应用核心的数据类型，在千兆以太网的研究过程中注意以下特点：

⑴.简易性：千兆以太网保持了经典以太网的技术原理、安装实施和管理维护的简易性，这是千兆以太网成功的基础之一。

⑵.技术过渡的平滑性：千兆以太网保持了经典以太网的主要技术特征，采用 CSMA/CD 媒体管理协议，采用相同的帧格式及帧的大小，支持全双工、半双工工作方式，以确保平滑过渡。

⑶.网络可靠性：保持经典以太网的安装、维护方法，采用中央集线器和交换机的星形结构和结构化布线方法，以确保千兆以太网的可靠性。

⑷.可管理性和可维护性：采用简易网络管理协议(SNMP)即经典以太网的故障查找和排除工具，以确保千兆以太网的可管理性和可维护性。

⑸.网络成本包括设备成本、通信成本、管理成本、维护成本及故障排除成本。由于继承了经典以太网的技术，使千兆以太网的整体成本下降。

⑹.支持新应用与新数据类型：计算机技术和应用的发展，出现了许多新的应用模式，对网络提出了更高的要求。为此，千兆以太网必须具有支持新应用与新数据类型的能力。第

5.4 因特网（Internet）

因特网是一个建立在网络互联基础上的罪的、开放的全球性网络。Internet 拥有数千

万台计算机和上亿个用户，是全球信息资源的超大型集合体。所有采用 TCP/IP 协议的计算机都可加入 Internet,实现信息共享和相互通信。与传统的书籍、报刊、广播、电视等传播媒体相比，Internet 使用方便，查阅更快捷，内容更丰富。今天，Internet 已在世界范围内得到了广泛的普及与应用，并正在迅速的改变人们的工作方式和生活方式。

Internet 的萌芽期起源于 20 世纪 60 年代中期由美国国防部高级研究计划局(ARPA)资助的 ARPANET,此后提出的 TCP/IP 协议为 Internet 的发展奠定了基础。1986 年美国国家科学基金会(NSF)的 NSFNET 加入了 Internet 主干网，由此推动了 Internet 的发展。但是，Internet 的真正飞跃发展应该归功于 20 世纪 90 年代的商业化应用。此后，世界各地无数的企业和个人纷纷加入，终于发展演变成今天成熟的 Internet。

5.4.1 Internet 的结构及其接入方式

1.Internet 的结构特点

Internet 采用了目前最流行的客户机 / 服务器工作模式，凡是使用 TCP/IP 协议，并能与 Internet 的任意主机进行通信的计算机，无论是何种类型、采用何种操作系统，均可看成是 Internet 的一部分。

严格的说，用户并不是将自己的计算机直接链接到 Internet 上，而是连接到其中的某个网络上，再由该网络通过网络干线与其它网络相连。网络干线之间通过路由器互连，使得各个网络上的计算机都能相互进行数据和信息传输。例如，用户的计算机通过拨号上网，连接到本地的某个 Internet 服务提供商（ISP）的主机上。而 ISP 的主机由通过高速干线与本国及世界各国各地区的无数主机相连，这样，用户仅通过一阶 ISP 的主机，便可遍访 Internet。由此也可以说，Internet 是分布在全球的 ISP 通过高速通信干线连接而成的网络。

Internet 的这样结构形式，使其具有如下的众多特点：

⑴ 灵活多样的入网方式。这是由于 TCP/IP 成功的解决了不同的硬件平台、网络产品、操作系统之间的兼容性问题。

⑵ 采用了分布网络中最为流行的客户机 / 服务器模式，大大提高了网络信息服务的灵活性。

⑶ 将网络技术、多媒体技术融为一体，体现了现代多种信息技术互相融合的发展趋势。

⑷ 方便易行。任何地方仅需通过电话线、普通计算机即可接入 Internet。

⑸ 向用户提供极其丰富的信息资源，包括大量免费使用的资源。

⑹ 具有完善的服务功能和友好的用户界面，操作简便，无须用户掌握更多的专业计算机知识。

2.ISP 接入方式

⑴ 帧中继方式。帧中继的主要特点是特点是：低网络时延、高传输速率以及在星形和网状网上的高可靠性连接。这些特点是帧中继特别适用于 Internet 的不可预知的、大容量的和突发性数据业务，如 E-mail、客户机 / 服务器等系统。但是，帧中继还不适用于传送大量的大容量(100MB)文件、多媒体部件或连续型业务量的应用。

⑵ 专线(DDN)方式。DDN(Digital Data Network)是通过数字信道为用户提供语音、数据、图像信号传输的数据网。DDN 可为公共数据交换网及各种专用网络提供用户数据信道，为帧中继、局域网及各类不同网络的互联提供网间连接。DDN 具有速度快、质量高的特点，但使用上不及模拟方式灵活，且投资成本较大。

⑶ ISDN 方式。ISDN 是数字技术和电信业务结合的产物，可用于取代租用线路实现域网间的互连。在这种连接方式中，ISDN 可以为用户提供高速、可靠的数字连接，并是主机或网络端口分享多个远程设备的接入。从窄带 ISDN（N-ISDN）发展而来的宽带 ISDN（B-ISDN），还能支持不同类型、不同速率的业务，不但包括连续性宽带业务，也包括突发型宽带业务。

3.用户接入方式

⑴ 仿真终端方式。终端可以通过电话线与远程主机相连，普通计算机安装相应的仿真软件后，也能像真正的终端一样实现与 ISP 主机的连接。这种接入方式简单、经济，且对用户计算机无特殊要求。但存在的缺点是用户端没有 IP 地址，无法运行高级接口软件，创诶用户的各类文件和电子邮件均存放在 ISP 主机上，影响了上网速度和时间。

⑵ 拨号 IP 方式。拨号 IP 方式也称 SLIP/PPP 方式，该方式采用串行网间协议 SLIP(Serial Line Internet Protocol)或点一点协议 PPP(Point to Point Protocol)，通过电话线拨号将用户计算机与 ISP 主机连接起来。拨号 IP 方式的优点是用户端有独立的 IP 地址，用户可以使用自己的环境和用户界面（如 Windows、Unix、Macintosh 等）进行连网操作，各类文件和电子邮件均可直接传送到用户计算机上。目前，大多数个人用户都采用这种方式上网。由于用户计算机上要运行大量接口软件，所以计算机的要求相对比较高。

⑶ 局域网连接方式。有两种方式可以实现局域网与 Internet 主机的连接。一种方法是通过局域网的服务器，使用高速 MODEM 经电话线路与 Internet 主机连接。在这种方法中，所有的工作站共享服务器的一个 IP 地址。另一种方法是通过路由器将局域网与 Inerter 主机相连，是整个将局域网加入到 Internet 中成为一个开放式局域网。在这种方法中，局域网中的所有工作站都可以有自己的 IP 地址。

5.4.2 Internet 的关键技术

1.TCP/IP 技术

有关 TCP/IP 的原理在第三章中已经作过介绍。TCP/IP 是 Internet 的核心，利用 TCP/IP 协议可以方便的实现多个网络的无缝连接。通常所谓某台主机在 Internet 上，Internet 地址（即 IP 地址），并运行 TCP/IP 协议，可以向 Internet 上的所有其他主机发送 IP 分组。

TCP/IP 的层次模型分为四层，其最高层相当于 OSI 的 5～7 层，该层中包括了所有的高层协议，如常见的文件传输协议 FTP、电子邮件 SMTP、域名系统 DNS、网络管理协议 SNMP、访问 WWW 的超文本传输协议 HTTP 等。

TCP/IP 的次高层相当于 OSI 的运输层，该层负责在源主机和目的主机之间提供端～端的数据传输服务。这一层上主要定义了两个协议：面向连接的传输控制协议 TCP 和无连接的用户数据报协议 UDP。

TCP/IP 的第二层相当于 OSI 的网络层，该层负责将分组独立地从信源传送到信宿，主要解决路由选择、阻塞控制级网际互联问题。这一层上定义了互连网协议 IP、地址转换协议 ARP、反向地址转换协议 RARP 和互连网控制报文协议 ICMP 等协议。

TCP/IP 的最低层为网络接口层，该层负责将 IP 分组封装成适合在物理网络上传输的帧格式并发送出去，或将从物理网络接收到的帧卸装并取于 IP 分组递交給高层。这一层与物理网络的具体实现有关，自身并无专用的协议。事实上，任何能传输 IP 分组的协议都可以运行。虽然该层一般不需要专门的 TCP/IP 协议，各物理网络可使用自己的数据链路层协议和物理层协议，但使用串行线路进行连接时仍需要运行 SLIP 或 PPP 协议。

2.标识技术

（1）主机 IP 地址。为了确保通信时能相互识别，在 Internet 上的每台主机都必须有一个惟一的标识，即主机的 IP 地址。IP 协议就是根据 IP 地址实现信息传递的。

IP 地址由 32 位（即 4 字节）二进制数组成，为书写方便起见，常将每的个字节作为一段并以十进制数来表示，每段间用“.”分隔。例如，202.96.209.5 就是一个合法的 IP 地址。

IP 地址由网络标识和主机标识两部分组成。常用的 IP 地址有 A、B、C 三类，每类均规定了网络标识和主机标识在 32 位中所占的位数。这三类 IP 地址的格式如图 5.7 所示，它们的表示范围分别为：

A 类地址：0.0.0.0～127.255.255.255

B 类地址：128.0.0.0～191.255.255.255

C 类地址：192.0.0.0～233.255.255.255

A 类地址一般分配具有大量主机的网络使用，B 类地址通常分配给规模中等的网络使用，C 类地址通常分配给小型局域网使用。为了确保惟一性，IP 地址由世界各大地区的权威机构 Inter NIC(Internet Network Information Center)管理和分配。

在 IP 地址的某个网络标识中，可以包含大量的主机（如 A 类地址的主机标识域为 24 位、B 类地址的主机标识域为 16 位），而在实际应用中不可能将这么多的主机连接到单一的网络中，这将给网络寻址和管理带来不便。为解决这个问题，可以在网络中引入“子网”的概念。注意，这里的“子网”与前面所说的通信子网是两个完全不同的概念。

将主机标识域进一步划分为子网标识和子网主机标识，通过灵活定义子网标识域的位数，可以控制每个子网的规模。将一个大型网络划分为若干个既相对独立又相互联系的子网后，网络内部各子网便可独立寻址和管理，各子网间通过跨子网的路由器连接，这样也提高了网络的安全性。

利用子网掩码可以产判断两台主机是否在同一子网中。子网掩码与 IP 地址一样也是 32 位二进制数，不同的是它的子网主机标识部分为全"0"。若两台主机的 IP 地址分别与它们的子网掩码相“与”后的结果相同，则说明这两台主机在同一网中。

（2）域名系统和统一资源定位器。32 位二进制数的 IP 地址对计算机来说十分有效，但用户使用和记忆都很不方便。为此，Internet 引进了字符形式的 IP 地址，即域名。域名采用层次结构的基于“域”的命名方案，每一层由一个子域名间用“.”分隔，其格式为：

机器名.网络名.机构名.最高域名

Internet 上的域名由域名系统 DNS(Domain Name System)统一管理。DNS 是一个分布式数据库系统，由域名空间、域名服务器和地址转换请求程序三部分组成。有了 DNS，凡域名空间中有定义的域名可以有效地转换为对应的 IP 地址，同样，IP 地址也可通过 DNS 转换成域名。

WWW 上的每一个网页(Home Page)都有一个独立的地址，这些地址称为统一资源定位器(URL)，只要知道某网页的 URL，便可直接打开该网页。例如，在 Internet 浏览器的 URL 输入框输入：

http://www.online.sh.cn

按回车后即可进入中国上海热线的主页。

（3）用户 E-mail 地址。用户 E-mail 地址的格式为：用户名@主机域名。其中用户名是用户在邮件服务器上的信箱名，通常为用户的注册名、姓名或其它代号，主机域名则是邮件服务器的域名。用户名和主机域名之间用“@”分隔。例如，hmchang@online.sh.cn 即表示域名为“online.sh.cn”的邮件服务器上的用户“hmchang”的 E-mail 地址。

由于主机域名在 Internet 上的惟一性，所以，只要 E-mail 地址中用户名在该邮件服务器中是惟一的，则这个 E-mail 地址在整个 Internet 上也是惟一的。

5.4.3 Internet 的应用

1.万维网 WWW

万维网(World Wide Web,简称 WWW)是 Internet 上集文本、声音、图像、视频等多媒体信息于一身的全球信息资源网络，是 Internet 上的重要组成部分。浏览器(Browser)是用户通向 WWW 的桥梁和获取 WWW 信息的窗口，通过浏览器，用户可以在浩瀚的 Internet 海洋中漫游，搜索和浏览自己感兴趣的所有信息。

WWW 的网页文件是超文件标记语言 HTML(Hyper Text Markup Language)编写，并在超文

件传输协议 HTTP(Hype Text Transmission Protocol)支持下运行的。超文本中不仅含有文本信息，还包括图形、声音、图像、视频等多媒体信息（故超文本又称超媒体），更重要的是超文本中隐含着指向其它超文本的链接，这种链接称为超链（Hyper Links）。利用超文本，用户能轻松地从一个网页链接到其它相关内容的网页上，而不必关心这些网页分散在何处的主机中。

HTML 并不是一种一般意义上的程序设计语言，它将专用的标记嵌入文档中，对一段文本的语义进行描述，经解释后产生多媒体效果，并可提供文本的超链。

WWW 浏览器是一个客户端的程序，其主要功能是使用户获取 Internet 上的各种资源。常用的浏览器 Microsoft 的 Internet Explorer(IE)和 Netvigator/Communicator。SUN 公司也开发了一个用 Java 编写的浏览器 HotJava。Java 是一种新型的、独立于各种操作系统和平台的动态解释性语言，Java 使浏览器具有了动画效果，为连机用户提供了实时交互功能。目前常用的浏览器均支持 Java。

2.电子邮件 E-mail

E-mail 是 Internet 上使用最广泛的一种服务。用户只要能与 Internet 连接，具有能收发电子邮件的程序及个人的 E-mail 地址，就可以与 Internet 上具有 E-mail 所有用户方便、快速、经济地交换电子邮件可以在两个用户间交换，也可以向多个用户发送同一封邮件，或将收到的邮件转发给其它用户。电子邮件中除文本外，还可包含声音、图像、应用程序等各类计算机文件。此外，用户还可以邮件方式在网上订阅电子杂志、获取所需文件、参与有关的公告和讨论组，甚至还可浏览 WWW 资源。

收发电子邮件必须有相应的软件支持。常用的收发电子邮件的软件有 Exchange、Outlook Express 等，这些软件提供邮件的接收、编辑、发送及管理功能。大多数 Internet 浏览器也都包含收发电子邮件的功能，如 Internet Explorer 和 Navigator/Communicator。

邮件服务器使用的协议有简单邮件转输协议 SMTP(Simple Mail Transfer Protocol)、电子邮件扩充协议 MIME(Multipurpose Internet Mail Extensions)和邮局协议 POP(Post Office Protocol)。POP 服务需由一个邮件服务器来提供，用户必须在该邮件服务器上取得账号才可能使用这种服务。目前使用得较普遍的 POP 协议为第 3 版，故又称为 POP3 协议。

3.专门讨论 Usenet

Usenet 是一个由众多趣味相投的用户共同组织起来的各种专题讨论组的集合。通常也将之称为全球性的电子公告板系统(BBS)。Usenet 用于发布公告、新闻、评论及各种文章供网上用户使用和讨论。讨论内容按不同的专题分类组织，每一类为一个专题组，称为新闻组，其内部还可以分出更多的子专题。

Usenet 的每个新闻都由一个区分类型的标记引导，每个新闻组围绕一个主题，如 comp.（计算机方面的内容）、news.（Usenet 本身的新闻与信息）、rec.（体育、艺术及娱乐活动）、sci.（科学技术）、soc.（社会问题）、talk.（讨论交流）、misc.（其它杂项话题）、biz.（商业方面问题）等。

用户除了可以选择参加感兴趣的专题小组外，也可以自己开设新的专题组。只要有人参加，该专题组就可一直存在下去；若一段时间无人参加，则这个专题组便会被自动删除。

4.文件传输 FTP

FTP（File Transfer Protocol）协议是 Internet 上文件传输的基础，通常所说的 FTP 是基于该协议的一种服务。FTP 文件传输服务允许 Internet 上的用户将一台计算机上的文件传输到另一台上，几乎所有类型的文件，包括文本文件、二进制可执行文件、声音文件、图像文件、数据压缩文件等，都可以用 FTP 传送。

FTP 实际上是一套文件传输服务软件，它以文件传输为界面，使用简单的 get 或 put 命令进行文件的下载或上传，如同在 Internet 上执行文件复制命令一样。大多数 FTP 服务器

主机都采用 Unix 操作系统，但普通用户通过 Windows95 或 Windows98 也能方便地使用 FTP。

FTP 最大的特点是用户可以使用 Internet 上众多的匿名 FTP 服务器。所谓匿名服务器，指的是不需要专门的用户名和口令就可进入的系统。用户连接匿名 FTP 服务器时，都可以用“anonymous”（匿名）作为用户名、以自己的 E-mail 地址作为口令登录。登录成功后，用户便可以从匿名服务器上下载文件。匿名服务器的标准目录为 pub，用户通常可以访问该目录下所有子目录中的文件。考虑到安全问题，大多数匿名服务器不允许用户上传文件。

5.远程登陆 Telnet

Telnet 是 Internet 远程登陆服务的一个协议，该协议定义了远程登录用户与服务器交互的方式。Telnet 允许用户在一台连网的计算机上登录到一个远程分时系统中，然后像使用自己的计算机一样使用该远程系统。

要使用远程登录服务，必须在本地计算机上启动一个客户应用程序，指定远程计算机的名字，并通过 Internet 与之建立连接。一旦连接成功，本地计算机就像通常的终端一样，直接访问远程计算机系统的资源。远程登录软件允许用户直接与远程计算机交互，通过键盘或鼠标操作，客户应用程序将有关的信息发送给远程计算机，再由服务器将输出结果返回给用户。用户退出远程登录后，用户的键盘、显示控制权又回到本地计算机。一般用户可以通过 Window 98 的 Telnet 客户程序进行远程登录。

5.4.4 Internet 的连接与设置

本节对 Window 98 环境下 Internet 的连接与设置操作做一简要介绍。

1.Internet 连接

连入 Internet 的用户可以分为两大部分：占绝大多数的是最终用户，他们使用 Internet 上提供的各类信息服务，如浏览 WWW、用 E-mail 进行电子邮件的收发、用 FTP 进行文件传输等；另一部分是 Internet 服务提供商(ISP)，他们通过租用高速通信线路建立服务器和路由器等设备，向用户提供 Internet 连接服务。连入 Internet 的方法有专线入网和拨号网络入网两种，目前国内的最终用户使用得最多的是拨号网络入网。使用“拨号网络”连接 Internet 需要进行如下准备工作：

(1)选择合适的 ISP，通过 ISP 获取 Internet 账号。

(2)准备一个调制解调器和一条能拨通 ISP 的电话线。

(3)安装“拨号网络”。

(4)安装 TCP/IP 协议并将其绑定到“拨号网络适配器”。

(5)输入 TCP/IP 信息。

(6)用“拨号网络”建立与 ISP 的连接。

其中 Internet 账号可能包括用户名、用户密码、ISP 的电话号码、ISP 所用域名服务器(DNS)的 IP 地址、用户电子邮件地址、电子邮件服务器名称等信息。

Internet 使用 TCP/IP 作为通信协议，所以必须安装 TCP/IP 协议并将其绑定到“拨号网络适配器”。如果已经安装了 TCP/IP 协议，则打开“控制面板”中的“网络”图标，进入“网络”对话框，在“配置”选项卡的“已安装组件栏”中，可以找到“TCP/IP---拨号网络适配器”信息。如果还没有安装 TCP/IP 协议，则可在“配置”选项卡中点击“添加”按钮，进入“请选择网络组件类型”对话框，选择“协议”，点击“添加”按钮，再在“选择网络协议”对话框中的“厂商”栏内选“Microsoft”，在“网络协议”栏内选“TCP/IP”，点击“确定”按钮即可。

2.Internet 连接向导

Window 98 提供的“Internet 连接向导”，可以帮助用户快速建立与 Internet 的连接，而不必用手工方式分别安装调制解调器、设置网络参数和拨号网络。

以拨号连接 Internet 的用户为例，使用“Internet 连接向导”建立连接的操作步骤如

下：

(1)点击“开始”菜单，指向“程序”、“Internet Explorer”，点击“连接向导”进入“Internet 连接向导”
的欢迎对话框。该对话框中有 3 项选项，拨号连网用户应选择第 2 项：“我已经通过电话线或局域网(LAN)建立了 Internet
账号。只需帮助我设置计算机使其连到该 Internet 账号”，然后点击“下一步”。

(2)在“Internet 连接向导”对话框中，选择第 1 项“如果您正在通过 Internet 服务提供商或局域网(LAN)访问 Internet
请选定该选项”，然后点击“下一步”。

(3)在连接向导的“建立 Internet 连接”对话框中，选择第 1 项“通过本地电话线连接”，然后点击“下一步”。

(4)在连接向导的“拨号连接”对话框中，选择第 1 项“创建新的拨号连接”，然后点击“下一步”

(5)在连接向导的“电话号码”对话框中，输入 ISP 的区号、电话号码和国家(地区)代码，若 ISP 为本地电话，则应使“使
用区代码和国家代码拨号”选项无效，然后点击“下一步”。

(6)在连接向导的“用户名和密码”对话框中，输入用户登录到 ISP 的用户和密码，然后点击“下一步”

(7)连接向导的“高级设置”对话框，提示用户是否需要修改连接的高级设置，内容包括连接类型、登录过程、IP 地址及
DNS 服务器地址等。一般国内的 ISP 都要求拨号连网用户设置这些参数，选择“是”，然后点击“下一步”，进入高级设置操作
过程：

①在“连接类型”对话框中，选择“PPP”(点对点协议)，点击“下一步”；

②在“登录过程”对话框中，选择“需要手工输入信息”，点击“下一步”；

③在“IP 地址”对话框中，选择由“Internet 服务提供商自动分配”，点击“下一步”；

④在“DNS 服务器地址”对话框中,选择“始终使用以下地址”,并输入 ISP 提供的 DNS 服务器地址，点击“下一步”。

(8)至此，Internet 账号等信息已被置于“拨号连接”组中，连接向导要求用户在“拨号连接名”对话框中输入所建连接的
名称，用户可任意定义连接的名称，但一般常用 ISP 的名称作为连接的名称，然后点击“下一步”

(9)在“设置 Internet Mail 账号”对话框中，连接向导提示用户是否设置 Internet Mail 账号，若用户选择“是”，则点击“
下一步”后连接向导进入电子邮件设置操作：

①在“Internet Mail 账号”对话框中，选择“创建新的 Internet Mail 账号”，点击“下一步”；

②在“姓名”对话框中,输入用户的姓名。当用户发送电子邮件时,该姓名便出现在“发信人”栏中。输入用户姓名后，点击“下一步”；

③在“Internet 电子邮件地址”对话框中， 输入用户的电子邮件地址。电子邮件地址是其它人向用户发送电子邮件时使用的地址，该地址由 ISP 与用户协商后提供。电子邮件地址由两部分组成,如 nullman@ecust.edu.cn,其中“nullman”为用户名，“ecust.edu.cn”为邮件服务器地址，两者之间用“@”连接。输入电子邮件地址后，点击“下一步”；

④在“电子邮件服务器名”对话框的邮件服务器类型栏中，一般选择“POP3”类型，然后在“邮件接收服务器名”和“发送邮件的服务器”栏中填入服务器名，一般这两个服务器名是相同的，也即用户电子邮件地址后半部分的邮件服务器地址。输入电子邮件服务器名后，点击“下一步”；

⑤在“Internet Mail 登录”对话框中，选择“登录方式”选项，并在“POP 账号名”和“密码”栏中分别填入用户名和密码，然后点击“下一步”；

⑥在“友好名称”对话框中，连接向导要求用户为其账号起个友好的名称，以作为该账号的标识。此名称在发送邮件时并非必有的设置，用户可以随意选取，缺省时，系统使用邮件服务器的名称作为该账号的名称。设置完毕后，点击“下一步”；

(10)在“设置 Internet News 账号”对话框中，连接向导提示用户是否设置 InternetNews 账号，若用户选择“是”，则点击“下一步”后连接向导进入新闻组设置操作：

①在“姓名”对话框中，输入用户的姓名。当用户向新闻组投递文章或发送电子邮件时，该姓名便出现在“发件人”栏中。输入用户姓名后，点击“下一步”；

②在“Internet News 电子邮件地址”对话框中，输入用户的电子邮件地址，然后点击“下一步”；

③在“Internet News 服务器名称”对话框中，填入由 ISP 提供的 Internet News 服务器名称，然后点击“下一步”；

④在“友好名称”对话框中，连接向导要求用户为其账号起个友好的名称，以作为该账号的标识。此名称可以随意选取，缺省时，系统使用服务器名称作为该账号的名称。设置完毕后，点击“下一步”。

(11)在“建立 Internet 目录服务”对话框中，连接向导提示用户是否设置 Internet 目录服务账号，若用户选择“是”，则点击“下一步”后连接向导进入目录服务设置操作：

①在“Internet 目录服务”对话框中，用户可以创建新的目录服务，也可以选择或修改现有的目录服务。若选择“修改现有的目录服务”，则在列表栏内选择某个目录服务，然后点击“下一步”；

②在“确认导入设置”对话框中，连接向导提示测试到的目录服务器账号名等设置情况，若用户认可，则选择“接受设置”并点击“下一步”。

(12)在“完成配置”对话框中，点击“完成”按钮，Internet 连接设置便告结束。

5.4.5 Internet Explorer 浏览器

Windows98 内置了 Microsoft Internet Explorer 4.0(简称 IE 4.0)，并支持 Web 风格的桌面布局和文件夹窗口。完成 Windows98 安装后，可以在“Internet Explorer”程序组中找到 Windows98 提供的一系列 Internet 工具，它们包括：Internet Explorer 浏览器、Outlook Express 电子邮件和新闻系统，Microsoft NetMeeting 网络会议系统，FrontPage Express 网页编辑器等。

1.浏览 WWW

完成拨号连接后，指向并点桌面上的"Internet Explorer"图标，便可打开 IE4.0 浏览器。

第一个 Web 页面，包括主页都有一个惟一的地址，称为统一资源定位器 URL(Universal Resource Locator)。要进入某一网页，可在浏览器的“地址”栏中输入该页的地址，例如输入的网页地址为：http://www.sohoo.com.cn/,便可进入中文搜索引擎“搜狐”的主页，见图 5.8。

IE4.0 具有自动地址补全功能，如果用户以前访问过 http://www.sohoo.com.cn/, 再输入该网页地址时，只要键入“W”，IE4.0 便会将入补全成“WWW”，键入“S”，便会补全

成“sohoo”，按下鼠标右键，可以确认补全的内容。

在浏览器所显示的网页中，可以看到一些带下划线的文字或图标，它们被称为“超链”，用于帮助用户寻找相关内容的其它网页资源。当鼠标移到某个“超链”时，鼠标指针会变为手形，此时点击左键，便可激活并打开另一网页。这种链接的技术，可以使用户以任意的次序、突破空间的疆域来组织和浏览自己感兴趣的网页，这就是超文本的概念。

浏览器的主要访问功能，都可以通过点击工具栏的按钮来实现。如果浏览器窗口中未显示工具栏，可以在菜单栏中点击“查看”、指向“工具栏”，选中“标准按钮”选项。工具栏中每项工具下的文本标签、浏览器窗口中的地址栏和链接栏的显示或消隐，也可同此操作。

使用浏览器窗口的滚动条，可以上下左右翻滚窗口；点击“后退”或“前进”按钮，可以返回前一页或进入下一页，对已经看过的网页进行快速的切换；在“后退”和“前进”按钮右侧，各有一个下拉按钮下拉菜单中列出了所有已经查阅过的网页名，点击某个网页名，便可直接进入该网页；点击“停止”按钮，可以终止当前显示页的传输；点击“刷新”按钮，可以更新当前显示页；点击“主页”按按，则返回浏览器预定的起始页。

Internet 上的信息，数量巨大、种类繁多，且每时每刻都有新的信息产生，老信息也在不断更新。如果用户漫无目的地在 Internet 上搜寻，将既耗费通讯费用，又难以找到价值的信息。Intenet 上有许多搜索站点，这些站点的数据库中保存着各类信息网页的地址，可以根据用户提交的主题词，帮助用户快速搜寻到所需的网页。“YAHOO”、“Infoseek”、“LYCOS”、“excite”等都是 Internet 上著名的搜索引擎，IE4.0 浏览器已将它们集成到自己的搜索功能中，用户点击工具栏中的“搜索”按钮，即可激活窗口。用户在搜索窗口的文本框内，输入所要寻找的信息的主题词，再选择一个搜索站点，然后点击“搜索”按钮，即可获取有关站点的地址。以上这上这些搜索站点大多为西文站点，而前面提到过的“搜狐”(www.sohooo.com.cn)，则是一个非常出色的中文搜索站点。

IE4.0 浏览器的收藏夹可以帮助用户保存自己喜欢的站点的地址，在需要时，打开收藏夹便可快速连接到所要的网页。收藏夹是一个专用的文件夹，网页地址以快捷文件方式保存在其中。当用户在 Internet 上找到某个喜欢的网页时，若要将它添加到收藏夹中，只要在菜单栏的“收藏”项中点击“添加到收藏夹”，在对话框的“名称”栏中，给出了该网页的标题，用户可以将之改成自己喜欢的任何名称，然后点击“确定”按钮即可。使用时，只要点击“收藏”项中点击“添加到收藏夹”，在对话框的“名称”栏中，给出了该网页的标题，用户可以将之改成自己喜欢的任何名称，然后点击“确定”按钮即可，使用时，只要点击“收藏”菜单项或工具项，打开收藏夹，再点击需浏览的网页名称即可打开有关网页。

用户曾经访问过的网页地址，均被保存在历史记录文件中。点击工具栏中的“历史”按钮，浏览器窗口 左侧便显示所有保存的历史记录，用户借此可以脱机浏览曾经访问过的网页。

2. 设置浏览器选项

IE4.0 提供了丰富的属性选项，使用户可以根据需要和习惯来配置浏览器。在浏览器窗口的“查看”菜单项中点击“Internet 选项”，即可打开“Internet 选项”对话框；点击“控制面板”中的“Internet 属性”图标，也可打开“Internet 选项”对话框如图 5.9 所示，其中包括“常规”、“安全”、“内容”、“连接”、“程序”及“高级”共 6 个选项卡。

(1)“常规”选项设置。“常规”选项卡用于进行 Internet 常规属性的设置，用户可借此建立自己喜欢的浏览器风格。其中包括“主页”栏、“Internet 临时文件”栏、“历史记录”栏、“颜色”按钮、“字体”按钮、“访问选项”按钮等内容。

“主页”栏用于更改主页。所谓“主页”，是指浏览器启动时进入的起始网页，也即在浏览过程中点击工具栏“主页”按钮所返回到的网页。大部分的用户希望将自己喜欢和常用

的网页作为主页，此时只要将所选网页的 URL 地址填入该区的“地址”栏即可。

“Internet 临时文件”栏用于管理 Internet 临时文件夹。浏览器将用户看过的网页内容保存在本地硬盘的 Internet 临时文件夹中，用户需要回溯已查过的网页时，只要在硬盘中调用而不必再从网上传输，这样就可大大提高浏览速度。点击“设置”按钮，进入“Internet”临时文件设置对话框。在该对话框中，用户可以确定所存网页内容的更新方式。选中“每次访问此页时检查”项，当每次回溯查看网页时，浏览器都将检查该页是否已经更新，该方式以降低浏览速度为代价来确保网页内容的时效性；选中“每次启动 Internet Exploer 时检查“项，浏览器仅在启动时检查回溯查看网页的更新情况，其它时间查看该页时不再检查，该方式兼顾了时效性和查看速度；选中”不检查”项，可以获得最大的回溯浏览速度，但损失了内容的时效性。无论选定了何种网页更新方式，用户均可在浏览过程中按工具栏的“刷新”钮，更新网页内容。拉动对话框中的“可用的磁盘空间”滑块，可以控制分配给临时文件夹的硬盘空间大小。用户可以根据自己的硬盘剩余空间情况来确定临时文件夹的大小，一般在 50MB 左右较适中。

“历史记录”栏用于设定“历史记录”列表中已访问过的网页保留的天数，保留天数与磁盘空间的大小有关，默认值为 20 天。点击“清除历史记录”按钮，将清除保存在“历史记录”文件夹中已访问过的网页的快捷方式连接。

“颜色”按钮用于设置网页的文字和背景颜色，“字体”按钮用于浏览器字体设置，“访问选项”按钮用于确定否使用网页指定的颜色、字体和大小。

（2）“安全”选项设置。在“安全”选项卡对话框的“区域”下拉列表框中列出了 4 种不同的区域：“本地企业网上的所有着站点；”可信站点区域“，包含用户确认不会损坏计算机或数据的站点；”Internet 区域”，包含未列其它区域中的所有站点；“受限站点区域”，饮食可能会损坏计算机或数据的站点。用户选定一个区域后，便可为该区域指定安全级别，然后将 Web 站点添加到具到有所需安全级别的区域中。

安全级别有如下 4 种：“高（安全）”，当站点有潜在安全总是时警告用户，用户不可下载和查看有潜在安全问题的站点的内容；“中（比较安全）”，当站点有潜在安全问题时警告用户，但用户可以选择是否下载和查看有潜在安全总是的站点的内容；“低”，当站点有潜在安全问题时不警告用户，站点内容的下载无需用户确认；“自定义”（高级用户）“，用户自己定义安全设置，选定该级别后，点击”设置按钮可进入“安全设置”对话框，用以分别对 ActiveX、Java、JavaScript 和其它内容设置安全级别。

（3）“内容”选项设置。“内容”选项卡中包括“分级审查”、“证书”和“个人信息”三栏内容。“分级审查”栏用以控制从 Internet 上收看的内容，以防止儿童接触 Internet 上不适合的内容。“证书”栏用以确认用户个人、发证机构和发行商。“个人信息”栏用于管理用户姓名、地址和其它信息。

（4）“连接”选项设置。“连接”选项卡包括“连接”、“代理服务器”和“自动配置”三栏内容。

点击“连接”按钮，即可进入“Internet 连接向导“，内容与前述相同。也可选择”使用调制解调器连接到 Internet“或”通过局域网连接到 Internet“选项后，点击”设置“，直接进行设置更改。

“代理服务器”栏用于确定是否通过代理服务器连接到 Internet。代理服务器有两种应用情况：一种情况是本企业利用仅有的一个 IP 地址建立代理服务器，使企业内其它计算机能通过代理服务器连接到 Internet；另一种情况是 Internet 上存在免费的代理服务器，进入 Internet 的用户可以选择合适的代理服务器作为中转站，用以加快伟输速度或访问某些从本地网无法访问到的站点。如果选择“通过代理服务器访问”，则需在“地址”和“端口”栏内输入代理服务器的地址和端口号。点击“高级”按钮，将打开“代理服务器”设置

对话框，用于设置不同协议型的代理服务器的地址和端口号。

点击“自动配置”栏中的“配置”按钮，可进入“自动配置”对话框，在“URL”栏内输入服务器站点地址后，便可使用服务器提供的配置文件自动配置用户的浏览器。

（5）“程序”选项设置。“程序”先项卡中包括“通讯信息“栏、”个人信息“栏和”检查 Internet Explorer 是否为默认的浏览器“复选框等项内容。

“通讯信息”栏中的“邮件”、“新闻”、“Internet 呼叫”项分别用于指定浏览器所使用的电子邮件、新闻阅读、Internet 会议等功能程序的名称，默认什给出的“Outlook Express“、”Microsoft NetMeeting“是与 Internet Explorer 捆绑使用的电子邮件、新闻阅读、Internet 会议功能程序。如果安装了其它的相关功能程序，用户可以通过下拉式选择框加以选择。

“个人信息”栏中的“日历”项用以指定 Internet Explorer 使用的 Internet 日历程序，“联系人列表”项用以指定 Internet Explorer 使用的 Internt 联系人或通讯簿。

“检查 Internet Explorer 是否为默认的浏览器”复选框用以确定是否将 Internet Explorer 作为默认的浏览器，选中此复选框后，每次 Internet Explorer 将询问是否将 Internet Explorer 还原为默认的浏览器。

（6）“高级”选项设置。“高级”选项卡的对话框由许多复选项组成，用以指定浏览器的各项深层次的细节问题，内容包括辅助选项、浏览、多媒体、安全、JavaVM（Java 虚拟机）、打印、搜索、工具栏、HTTP1.1 设置等。对于一般用户来说，所有复选项均可彩其默认设置。其中的“多媒体”项用以控制图片、动画、视频、声音的显示和播放，在默认情况下，网页中所有的多媒体信息均下载，若用户仅需浏览网页的文字内容，则可取消相关的复选项，以加快网页的传输速度。

3、预定 Web 页

用户可以预定自己喜爱的站点，并要求在指定时间（例如每天、每周或每月一次）自动下载更新内容。一旦预定后，浏览器可以在用户忙于计算机上的其它工作甚至休息时，在后台下载已更新的 Web 页或整个站点，供用户在以后联机时或以脱机方式浏览这些内容。

需要说明的是，在预定传输时间内，计算机必须处于与 Internet 的连接状态。这对于全天侯不停机连续运行的转线上网用户来说，预定网页是一种高效、省时的信息获取方式。但对于拨号上网的用户来说，保持长时间不间断的 Internet 连接将耗费大量的通信费。除非将来电话通信费实际上限封顶收费，到那时，一般用户也可以全天侯连续上网了。

要预定某一网页，首先必须连接到该网页，使浏览器能获取有效的网页连接地址。然后点击浏览器菜单栏“收藏”菜单项、点击“添加到收藏夹”，打开“添加到收藏夹”对话框。用户可以根据需要在“是：仅在该网页更新时通知我”和“是：更新时通知我并下载该页以便脱机阅读”两项中确定更新方案，选定后点击“确定”按钮即可。

点击浏览器菜单栏“收藏”菜单项、点击“管理预定内容”，可以打开预定文件夹窗口。窗口内给出了每个预定网页的名称、上次更新时间、状态、下次更新时间、位置、计划、大小、优先级等详细信息。用户若要更改已预定网页的属性，可在窗口中选中某个网页项后点击鼠标右键，再在快捷菜单中点击“属性”，便可进入指定预定网页的属性对话框。属性对话框包括“预定”、“接收”及“计划”三个选项卡。

预定网页属性的“预定”选项卡对话框给出了预定网页的名称、网址及属性摘要。用户若要取消指定网页的预定，可点击“取消预定”按钮。其它属性的更改需在“接受”和“计划”两个选项卡中进行。

“接受”选项卡中的“预定类型”栏用以更改网页内容更新后的通知方式。如果用户选择“在更新时通知我并下载内容以便脱机阅读”项，则还可以通过点击“高级”按钮进入“高级下载选项”对话框，用以指定下载的内容、项目及最大下载量。不管选择何种通知方

式，当浏览器发现网页内容更新时，均会以闪烁的图标来提醒用户。用户也可以要求当网页内容更新时向用户发送电子邮件通知书，此时需在“通知”栏内选中“向以下地址发送电子邮件”，若电子邮件地址需更改，可点击“更改地址”按钮。有些付费站点在下载所选预定内容时需要用户登录，此时可点击“登录”按钮，在弹出的“登录选项”对话框中输入用户名和密码。

预定网页属性的“计划”选项卡对话框提供用户设置预定网页的下载计划。用户若选中“按预定计划”项，则可指定选择何时、按何种频度（如每天几点钟、每周星期几、每月几号），将预定网页下载到用户的硬盘上，要设置新的计划，可点击“新建”按钮；要更新现有的设置，可点击“编辑”按钮。用户若选中“手工”项，则点击“立即更新”按钮，即可将预定网页内容更新。

5.5 内联网（Intranet）

5.5.1 Intranet 概述

1. Intranet 的定义

Intranet 的浪潮冲击着人们生活的每一个环节，从此人类社会进入了网络时代。同样，Intranet 的浪潮也冲击着企业的计算机应用。人们发现 TCP/IP、HTML 及 Web 等技术也可以用于企业内部信息网的建设，由此便引发了 Intranet 应用的高潮。

Intranet 按字面直译就是“内部网”的意思，为了与互联网 Internet 对应，通常将之译成“内联网”，表示这是一组在特定机构范围内使用的互联网络。这个机构的范围，大可到一个跨国企业集团，小可到一个部门或小组，它们的地理分布不一定集中或只限定在特定的区域内。所谓“内部”，只是就机构职能而言的一个逻辑概念。

由于采用的是 Internet 上早已成熟的标准技术，Intranet 使得机构内涉及多种平台的网络应用开发不必再拘泥于传统的客户/服务器技术，从而使开发工作变得 十分简单。而且，用户端只需要配置一个一般用户都熟悉的浏览器软件，这样就使开发投资和培训费用也大大降低了。

Intranet 技术一问世就受到了各类机构组织和企业的极大欢迎，近年来推广速率与 Intranet 相比有过之无不及。现在全球几乎 80%的 Web 服务器都与 Intranet 应用有关，可以说
Intranet 已成为当前机构和企业计算机网络的新热点。

2. Intranet 的结构

Intranet 通常是指一组沿用 Intranet 协议的、采用客户/服务器结构的内部网络。服务器端是一组 Web 服务器，用以存放 Intranet 上共享的 HTML 标准格式信息以及应用；客户端
则为配置浏览器的工作站，用户通过浏览器以 HTTP 协议提出存取请求，Web 服务器则将结果回送到原始客户。

Intranet 通常是指可包含多个 Web 服务器，一个大型国际企业集团的 Intranet 常常会有多达数百个 Web 服务器及数千个客户工作站。这些服务器有的与机构组织的全局信息及应用
有关，有的仅与某个具体部门有关，这些分布组织方式不仅有利于降低系统的复杂度，也便于开发和维护管理。由于 Intranet 采用标准的 Intranet 协议，某些内部使用的信息必要时能随时方便地发布到公共的 Intranet 上去。

考虑到安全性，可以使用防火墙将 Intranet 与 Internet 隔离开来。这样，既可提供对公共 Internet 的访问，有又可防止机构内部机密的泄露。

5.5.2 Intranet 的特点

1.开放性和可扩展性

由于采用了 Intranet 的 TCP/IP、FTP、HTML、Java 等一系列标准，Intranet 具有良好的开放性，可以支持不同计算机、不同操作系统、不同数据库、不同网络的互连。在这些相异的平台上，各类应用可以相互移植、相互操作，使它们有机地集成为一个整体。在此基础上，应用的规模也可以增量式扩展，先从关键的小的应用着手，在小范围内实施取得效益和经验后，再加以推广和扩展。

Intranet 的开放性和可扩展性使之成为构筑记过组织级信息公路的主流。对内方面，Intranet 可将机构内部各自封闭的局域网信息孤岛联成一体，实现机构组织的信息交流、资源共享和业务运作；对外方面，可方便地接入 Intranet 成为全球信息网的成员，实现世界及信息交流和电子商务。

2.通用性

Intarnet 的通用性表现在它的多媒体集成和多应用集成两个方面。在 Intranet 上，用户可以利用图、文、声、像等各类信息，实现机构组织所需的各种业务管理和信息交流。

Intranet 从客户终端、应用逻辑和信息存储三个层次上支持多媒体集成。在客户端，Web 浏览器允许在一个程序里展现文本、声音、图像、视频等多媒体信息；在应用逻辑层，Java 提供交互的、三位的虚拟现实界面；在信息存储层，面向对象数据库为多媒体的存储和管理提供了有效的手段。

利用 TCP/IP、Web、Java 和分布式面向对象等开放性技术，Intranet 能支持不同内容应用在不同平台上的集成，这些应用可运行在同一机构组织的不同部门，也可运行在不同机构组织之间。

3.简易性和经济性

Intranet 的性能价格比远高于其碳诶不通信方式，这主要体现在其网络基础设施的费用投入较少。由于采用开放的协议和技术标准，大部分机构组织的现存平台，包括网络和计算机，均可继续利用。

作为 Intranet 的基本组成，Web 服务器和浏览器不仅价格较低，而且安装配置简易。作为开发语言，HTML 和 Java 等容易掌握和利用，使开发周期缩短。另外，Intranet 可扩展性不仅支持新系统的增量式构造，从而降低开发风险，而且支持与现存系统的接口和平滑过渡，可充分利用已有资源。

超文本的界面统一标准，操作简易友善，超链使用户只要简单的操纵鼠标就可浏览和存取所需的信息。由此，对用户的培训可以大大地简化。

Intranet 的简易性和经济性不仅表现在开发和使用上，而且也表现在管理和维护上。由于 Intranet 采用瘦客户机方式，其客户端部存在程序代码，所以维护更新和管理可以方便地在服务器上进行。另外，由于 Intranet 开发和维护技术要求简单，可以让更多部门甚至个人参与开发，从而降低了 IT 人员的负荷和数量。

4.安全性

Intranet 的安全性是它区别于 Internet 的最大特征之一。Intranet 的实现基于 Internet 技术，两个地理位置不同的部门或子机构也可能利用 Internet 相互联接。由于 Intranet 通常主要险韵诶不适用，所以在与 Internet 互联时，必须加密数据，设置防火墙，控制职员随意接入 Internet，以防止内部数据泄密、篡改和黑客入侵。

5.Intranet 存在的问题

虽然 Intranet 具有传统 MIS 系统和 LAN 无可比拟的优点，但由于 Intranet 的发展仍处于初级阶段，不少方面尚未成熟，其存在的问题主要表现在以下几个方面：

(1)规划不足的问题。由于 Intranet 的简易性和经济性，诱使各类机构和企业在无慎密规划的情况下纷纷仓促上马，以致造成失控状态。为避免混乱，Intranet 实施前应该根据本机构的特点和现状进行统一规划，并制定相应的详细实施步骤。

(2)安全风险问题。只要有接入 Internet 的可能，Intranet 的风险总是存在的。但是，如果能谨慎地设计安全系统，并充分利用如防火墙，公有密钥和私有密钥等成熟的安全性技术，风险是可以大大降低的。

(3)信息管理的重要问题。Intranet 的优点之一是其信息可以让机构内的所有成员共享，但由此也引发了越权访问、信息泄漏及垃圾数据上网的问题。为此，必须加强对信息管理的重视。

(4)开发方法和策略缺少问题。目前尚无成熟的方法和策略可用于 Intranet 的规划、设计和实施，大多开发工作只能借助于旧有的方法和策略，这样不利用于系统开发的质量和效益。

5.5.3 Intranet 的应用

在短短几年里，Intranet 的应用发生了两次跨时代的飞跃，从第一代的信息共享与通信应用，发展到第二代的数据库与工作流应用，节日进入以业务流程为中心的第三代 Intranet 应用。

1.信息共享与通信

第一代 Intranet 将 Internet 的应用搬到机构组织内部，实现信息共享和快捷通信。

信息共享将机构内部的信息网转换成了全球性的信息网，实现了高效、无纸的信息传输。信息共享应用不仅将大量的文件、手册转换成了电子形式，从而减少了印刷、分发成本和传播周期，而且也营造了开放的企业文化。通过 Intranet，领导可以直接与员工交流，及时了解和掌握企业运作和市场营销情况。

通常，信息共享应用是一组采用 HTML 编制的静态 Web 页面，其中包含丰富的多媒体信息，页面之间通过超链实现透明的浏览和切换。这些信息可以根据用户的身份和需要动态的产生或定制。与传统的媒体相比，Intranet 的信息共享应用不仅范围广、价格便宜、更新及时，更重要的是媒体丰富和按需点播。

初期 Intranet 应用的另一个内容是通信。通信应用可分为共同工作和独立工作两种方式。共同工作方式不管参与者是否在同一地点，他们必须在同一时间一起工作，这类应用的目的在于增强合作和交流的效率，常见的共同工作通信方式有：日程安排、电话会议、视频会议、电子系统、白板系统及交谈（Char）系统。独立工作方式则不关心参与者在何时何地进行工作，这类应用的旷日持久是取消必须同时参与的会议。常见的独立工作通信方式有：电子邮件、讨论组、支持小组工作的文档编辑工具等。

2.数据库与工作流应用

随着 Intranet 应用的深入，静态的信息共享已不能满足用户需求，于是开始尝试将传统的 MIS 系统向 Intranet 上搬迁，这就是以数据库应用和工作流为主的第二代 Intranet 应用。

这一代 Intranet 应用的技术特点是 Wed 和数据库的结合。在传统的 MIS 系统中，数据库的存取一般需要专门的用户端软件，检索所得的结果难以为大多数用户所接受。通过通用网关接口 CGI(Common Gateway InterFace)将 WWW 与数据库结合起来后便使无论存取本身和结果都变得更加容易。WWW 提供的友善、统一和易用的界面，使更多的用户乐意去访问数据库。由于用户使用的是统一的 WWW 浏览器界面，而不是各种各样的用户端软件，所以数据库的管理和支持人员可以集中精力的数据库建设上，而不用过多关心对用户端的支持。这样，

对于一个机构来说，原来不同部门之间不同应用与数据库的互联、转换、培训和使用等问题也就迎刃而解了。

3.以业务流程为中心的应用

Intranet 技术虽然给机构的信息化建设带来了巨大的活力，但仍然不能使现代企事业摆脱这样的尴尬 ：一方面单位对 IT 的投资越来越大，另一方面预期的效益总不能兑现。导致 IT 技术不能发挥其潜在效能的主要原因是，传统 MIS 系统仅使人工作业自动化，但并未改、变原有的工作和管理方式。简单地对现有流程自动化，无论采用何种技术，都只会加剧混乱的程度。

解决这个问题的惟一途径是将新的管理理念和先进的 Intranet 技术有机结合盐业，对现有业务流程进行重新分析、重组、优化和管理，以顾客为中心将流程中和每一项工作综合成一个整体，使之顺畅化和高效化，以协调内部业务关系和活动，提高对外界变化的反应能力，改善服务质量，降低经营和管理成本。这就是第三代以业务流程为中心和 Intranet 应用。

所谓业务流程，是指与顾客共同创造价值的相互衔接的一系列活动，也称为价值流。业务流程几乎包含了企事业单位所有运行操作，按内容可分为客户关系管理、供应链、知识及决策管理等。业务流程具有时间、成本、柔性、客户满意度等可测量和分析的指标，因此，单位的业绩可由业务流程的指标来体现。无论是分析流程还是重新设计，均可对流程的指标进行测量和评价。这些指标的定义、测量、收集和分析是控制业务流程的关键技术。

以业务流程为是中心的第三代 Intranet 集成了多种先进的 IT 技术，例如：基于 WED 的多层客户/服务器技术、数据库（DW）、计算机电话集成技术（CTI）、分布对象技术(DOT)、安全和保密术等。

5.6 网络管理基础与网络安全

随着网络的规模不断扩大,复杂性不断增加，为确保向用户提供满意的服务，迫切需要一个高效的网络管理系统对整个网络进行自动化的管理工作。网络管理是计算机网络发展中的关键技术，对网络的正常运行起着极其重要的作用。

1.网络管理的基本功能

网络管理的目的协调、保持网络系统的高效、可靠运行，当网络出现故障时，能及时报告和处理。ISO 建议网络管理应包含以下基本功能：故障管理、计费管理、配置管理、性能管理和安全管理。

(1)故障管理(Fault Management)。故障管理是网络管理中最基本的功能之一。当网络发生故障时，①必须尽可能快地找出故障发生的确切位置；②将网络其它部分与故障部分隔离，以确保网络其它部分能不受干扰继续运行；③重新配置或重组网络,尽可能降低由于隔离故障后对网络带来的影响;④修复或替换故障部分,将网络恢复为初始状态.对网络组成问部件状态的临测是网络故障检测的依据。不严重的简单故障或偶然出现的错误通常被记录在错误日志中，一般需做特别处理；而严重一些的故障则需要通知网络管理器，即发出报警。因此网络管理器必具备快速和可靠故障临测、诊断和恢复功能。

(2)计费管理(Accounting Management)。在商业有偿使用的网络上，计贯管理功能统计哪些用户、使用何信道、传输多少数据、访问什么资源等信息；另一方面，计费管理功能还可以统计不同线路和各类资源的利用情况。因此可见，计费管理的根本依据是网络用这些信息，并制定一种用户可接受的计费方法。商业性网络中的计费系统还要包含诸如每次通信的开始和结束时间、通信中使用的服务等级以及通信中的另一方等更详细的计费信息，并使用能够随时查询这些信息。

(3)配置管理(Configuration Management)。配置管理也是网络管理的基本功能。计算

机网络由各种物理结构
和逻辑结构组成，这些结构中有许多参数、状态等信息需要设置并协调。另外，网络运行在多变的环境中，系统本身也经常要随着用户的增、减或设备的维修而调整配置。网络管理系统必须具有足够的手段支持这些调整的变化，使网络更有效地工作。这些手段构成了网络管理的配置管理功能。配置管理功能至少应包括识别被管理网络的拓朴结构、标识网络中的各种现象、自动修改指定设备的配置、动态维护网络配置数据库等内容。

(4)性能管理(Performance Management)。性能管理的目的是在使用最少的网络资源和具有最小延迟的前提下，确保网络能提供可靠、连接的通信能力，并使网络资源的使用达到最优化的程度。网络的性能管理有监测和控制两大功能，监测能实现对网络中的活动进行跟踪，控制功能实施相应调整来提高网络性能。性能管理的具体内容包括：从被管对象中收集与网络性能有关的数据，分析和统计历史数据，建立性能分析的模型，预测网络性能的长期趋势，并根据分析和预测的结果，对网络拓朴结构、某些对象的配置和参数做出调整，逐步达到最佳运行状态。如果需要做出的调整时、还要考虑扩充或重建网络。

(5)安全管理(Security Management)。安全管理的目的是确保网络资源不被非法使用，防止网络资源由于入侵者攻击而遭受破坏。其主要内容包括：与安全措施有关的信息分发(如密钥的分发和访问权设置等)，与安全的通知(如网络有非法侵入、无权用户对特定信息的访问个图等)，安全服务措施的创建、控制和删除，与安全有关的网络操作事件的记录、维护和查询日志管理工作等等。个完善的计算机网络管理系统必须制定网络管理的安全策略，并根据这一策略设计实现网络安全管理系统。

2.网络管理系统的构成

一个具体的网络管理系统不一定要完全包含上述的五大管理功能，不同的系统可以选取其中的几个功能加以
组合，但几乎每个网络管理系统都会包括故障管理功能。

现代计算机网络的管理系统模型主要由以下几部分组成：(1)多个被管代理(Managed Agents)，也称管理代理；(2)至少一个网络管理器(Network Manager)，也称管理工作站；(3)一个通用的网络管理协议(Network Management Protocol)；(4)一个或多个管理信息库(MIB-Management Information Base)。

所有被管理的网络设备，包括用户站点和网络互连设备等，统称为被管对象(Managed Object)。驻留在这些被管对象上配合网络管理的处理实体称为被管代理，而驻留在管理工作站上实施管理的处理褓称为管理器。管理器和被管代理通过交换管理进行工作，这种信息交换通过一种网络管理协议来实现，分别驻留在被管对象和管理工作站上的管理信息库(MIB)中。

任何王码电脑公司软件中心促可被管理的被管对象，例如主机、工作站、文件预备器、打印服务器、终端服务器路由器，网桥或中继器等都有一个被管代理，被管代理时刻监听和、响应来自网络管理器的查询或命令。

任一网络管理至少都应该有一个网络工作站，驻留在网络管理工作站上的网络管理器负责网络管理的全部监视和控制工作。网络通过与被管代理的住处交互(发送请求/接受响应)来完成管理工作。被管代理与网络管理器之间的信息交互的动作规则和数据格式等，则由网络管理协议来规定。网络管理协议与管理信息库一起协调工作，简化了网络管理的复杂过程。因为管理信息库中的管理信息描述了所有被管对象及其属性值，使得网络管理的全部工作就是对这些对象及属性值变量的读取(Get,对应于监视)或设置(Set，对应于控制)。

3.网络管理协议

目前最有影响的网络管理协议有两个：一个是简单网络管理协议 SNMP(Simple Net-work Management Protocol)；另一个是公共管理信息服务和公共管理信息协议

CMIS/CMIP(Coommon Management Information Sever/Common Maagement Information Protocol)。

ISO 早在提出 OSI/RM 的同时，就提出了网络管理标准的框架，并制定了基于开放系统互连参考模型的 CMIS/CMIP。然而由于种种原因，符合 OSI 网络管理标准的可供实用的产品几乎没有。与此同时，Internet 组织在长期运行因特网的实践中，提出了一个基于 TCP/IP 协议簇的网络管理标准协议 SNMP，并得到了众多网络产品生产厂家的广泛支持，使之成为事实上的网络管理工业标准。

与 CMIS/CMIP 相比，SNMP 流行更广、应用更多、获得的支持更广泛。SNMP 的最大的优点是简易性与可扩展性，它体现了网络管理系统的一个重要准则，即网络管理功能的实现不能影响网络的正常功能，不给网络附加过多的开销。下面将摘要介绍 SNMP 网络管理协议。

SNMP 设计为一种基于用户数据报协议 UDP（User Datagram Protocol）的应用层协议，它是 TCP/IP 协议簇的一部分。SNMP 的管理站根据管理需要产生三种类型的 SNMP 消息：所有这三种消息在代理方面均以 Get Next Request 和 Set Request，前两种实现 Get 功能，后一种实现 SET 功能。所有这三种消息在代理方面均以 GET RESPONSE 消息确认，并传递给管理应用。

因为管理站要管理相当多的代理，而每个代理维护的对象数量又非常大，在实现过程中，管理站不可能频繁定期轮询全部代理中所胡的对象的数据。为此，SNMP 采用了一种不完全的轮询协议，它允许某些未经询问不发送的信息，这种信息称为 Trap。其工作机制如下：在初始化阶段，或者每隔一段较长时间，管理站通过轮询所有代理来了解某些关键信息，一旦了解到了这些信息，管理站可以不再进行轮询；另一方面，每个代理负责向管理站通知可能出现的异常情事件，这些事件通过 SNMP TRAP 消息传递；一旦管理站得到一个意外事件的通知，它可能采取一些动作，如直接轮询报告该事件的代理或还轮询与该代理邻近的一些代理以便取得更多有关该意外事件的特定信息。由 Trap 导致的轮询有助于大理节省网络带宽和降低代理的响应时间，尤其是管理站不需要的管理信息不必通过网络传递，代理也可以不用频繁响应那些不感兴趣的请求。

使用 SNMP 前提是要求所有的代理和管理站都支持 UDP 和 IP，这就限制了对于某些设备的管理，例如某些不支持 TCP/IP 协议的网桥和调制调解器等设备只能被排除在网管范围之外。此外，可能有许多小系统（个人计算机、工作站、可编程控制器等）虽然支持 TCP/IP，但是它们不能承受由于增加了 SNMP、代理逻辑和 MIB 的维护而带来额外负担。为了管理那些没有实现 SNMP 的设备，可以引入委托，即 SNMP 代理代表了被委托的设备。管理站给它的委托代理发送关于该设备的查询，委托代理再把每个查询转换为该设备所使用的管理协议；反之，当代理收到对某个查询的响应时，它把响应递交给管理站。与此相似，如果来自于该设备的某些通知传给代理后，代理再以 TRAP 消息的形式发送给管理站。

网络管理技术仍在继续发展，，INTERNET 体系结构委员会的长期目标是研究和开发 OSI 的网络管理标准，并希望最终使这些协议同时适用于 TCP/IP 和 OSI 网络环境，即 CMOT(CMIP Over TCP/IP)

5.6.2 网络安全

1.网络上的不安全因素

随着全球信息化的飞速发展，大量建设的各种信息化系统已经成为国家和政府的关键基础设施，其中许多业务都是国际性的，诸如电信、电子商务、金隔网络等。网络信息安全已成为亟待解决、影响国家全局和长远利益的重大关键问题。

计算机犯罪是一种高技术型犯罪，由于其犯罪的隐蔽性，因此对计算机网络安全构成了很大的威胁。计算机犯罪已经引起全社会的普遍关注。随着 Internet 的广泛应用，采用浏

览器/服务器模式的 Intranet 纷纷建成，这使网络用户可以方便地访问和共享网络资源。但同时对企业的重要信息，如贸易秘密、产品开发计划、市场策略、财务资料等的安全无疑埋下了致命的威胁。必须认识到，对于大到整个 Internet，小到各 Intranet 及各校园网，都存在着来自网络内部与外部的威胁。对 Inetrnet 的构成威胁可分为两类：故意危害和无意危害。

故意危害 Internet 安全的主在有三种人：故意破坏者又称黑客（Hackers）、不遵守规则者(Vandals)和刺探秘密者(Crackers)。故意破坏者企图通过各种手段去破坏网络资源与信息，例如涂抹别人的主页、修改系统配置、造成系统瘫痪；不遵守规则者企图访问不允许访问的系统，这种人可能仅仅是到网中看看、找些资料，也可能想盗用别人的计算机资源（如 CPU 时间）；刺探秘密者的企图是通过非法手段侵入他人系统，以窃取重要秘密和个人资料。

除了泄露信息对企业网构成威胁之外，还有一种危险是有害信息的侵入。有人在网上传播一些不健康的图片、文字或散布不负责任的消息；另一种不遵守网络使用规则的用户可能通过玩一些电子游戏将病毒带入系统，轻则造成信息出误，严重时将会造成网络瘫痪。

2.防火墙（Firewall）技术

防火墙是有被保护的 Intranet 与 Internet 之间竖起的一道安全屏障，用于增强 Intranet 的安全性。Internet/Intranet 防火墙，用以确定哪些服务可以被 Interneth 上的用户访问，外部的哪些人可以访问内部的嗖服务以及外部服务可以被内部人员访问，目前的防火墙技术可以起到以下安全作用：

（1）集中的网络安全。防火墙允许网络管理员定义一个中心（阻塞点）来防止非法用户（如黑客、网络破坏者等）进入内部网络，禁止存在不安全因素的访问进出网络，并抗击来自各种线路的攻击。防火墙技术能够简化网络的安全管理、提高网络的安全性。

（2）安全警报。通过防火墙可以方便地监视网络的安全性，并产生报警信号。网络管理员必须审查并记录所有通过防火墙的重要信息。

（3）重新部署网络地址转换（NAT）。Internet 的迅速发展使得有效的未被申请的 IP 地址越来越少，这意味着想进入 Internet 的机构可能申请不到足够的 IP 地址来满足内部网络用户的需要。为了接入 Internet，可以通过网络地址转换 NAT(Network Address Translator)来完成内部私有地址到外部注册地址的映射。防火墙是部署 NAT 的理想位置。

（4）监视 INTERNET 的使用。防火墙也是审查和记录内部人员对 INTERNET 使用的一个最佳位置，可以在此对内部访问 INTERNET 的情况进行记录。

（5）向外发布信息。防火墙除了起到安全屏障作用外，也是部署 WWW 服务器和 FTP 服务器的理想位置。允许 INTERNET 访问上述服务器，而禁止对内部受保护的其它系统进行访问。

但是，防火墙也是自身的局限性，它无法防范来自防火墙以外的其它途径所进行的攻击。例如在一个被保护的的网络上有一个没有限制的拨号访问存在，这样就为从后门进行攻击留下了可能性；另外，防火墙也不能防止来自内部变节者或不经心的用户带来的威胁；同时防火墙也不能解决进入防火墙的数据带来的所有安全问题，如果用户抓来一个程序在本地运行，那个程序可能就包含一段恶意代码，可能会导致敏感信息泄露或遭到破坏。

典型的防火墙系统可以由一个或多个构件组成，其主要部分是：包过滤路由器也称分组过滤路由器、应用层网关，电路层网关。

包过滤路由器对 IP 地址，TCP 或 UDP 分组头信息进行检查与过滤，以确定是否与设备的过滤规则匹配继而决定此数据包按照由表中的信息被转发或被丢弃。包过滤方式的主要优点是仅一个关健位置设置一个包过滤路由器就可以保护整个网络，而且包过滤对用户是透明的，不必在用户机上再安装特定的软件。包过滤也有它的缺点和局限性，如包过滤规则配置比较复杂，而且几乎没有什么工具能对过滤规则的正确性进行测试；包过滤也没法查出具有

数据驱动攻击这一类潜在危险的数据包；另外，随着过滤数目的增加，路由器的吞吐量会下降，从而影响网络性能。

应用层网关也就是通常所说的代理服务器。代理服务器运行在 INTERNET 和 INTRANET 之间，当收到用户对某站点的访问请求后，会检查请求是否符合规则。若规则允许用户访问该站的话，代理服务器便会经客户身份去那个站点取回所需的信息再发回给客户。因此代理服务器会像一堵墙一样挡在内部用户和外界之间，从外部只能看到该代理服务器而无法获知任何内部资料，诸如用户的 IP 地址等。应用层网关比单一的包过滤更为可靠，而且会详细记录所有的访问状态但是应用层网关也存在一些不足之外，首先因为它不允许用户直接访问网络，会使访问速度变慢；而且应用层网关需要对每一个特定的 Internet 服务器安装相应的代理服务软件，用户不能使用未被服务器支持的服务，对每一类服务要使用特殊的客户端软件；更不幸的是，并不是所有的 Internet 应用软件都可以使用代理服务理。

电路层网关是一种特殊的功能，它也可以由应用层网关来完成。电路层网关只依赖于 TCP 连接，并不进行任何的包处理或过滤。在 Telnet 的连接中，电路层网关简单地进行了中继，并不做任何审查、过滤或协议管理。它只在内部连接和外部连接之间来回拷贝字节，但隐藏受保护网络的有关信息。电路层网关常用于对外连接，此时假设网络管理员对其内部用户是信任的。它的优点是主机可以被设置成混合网关，对于内连接它支持应用层或代理服务，而对于外连接煞费苦心支持的电路层功能。这样，使得防火墙系统对于要访问 Internet 服务的内部用户来说使用起来很方便，同时又能提供保护内部网络免于外部攻击的防火墙功能。