第 4 章

测控系统网络技术

学 习 目 标

- 掌握网络与通信基本概念
- 掌握现场总线技术
- 熟悉工业以太网技术
- 熟悉无线通信相关技术

网络化测控系统是由各类工业控制网络构建，数据通信与测控网络技术是测控系统的基础。基于网络的测控系统将地域分散的功能单元，如智能传感器、测控模块、工控机等，通过各类网络互联，通过信息的传输和交换，构成网络化分布式测控系统，实现远距离测控、资源共享以及设备的远程诊断与维护，有利于降低测控系统的成本。

4.1 测控网络技术基础

4.1.1 网络与通信技术基础

1. 计算机网络概述

（1）计算机网络的组成。计算机网络是指将地理位置不同的、功能独立的各类计算机或其他数据终端设备，通过通信线路连接，以网络软件来实现资源共享和信息传递的系统。计算机网络的连接方式与结构具有多样性。计算机网络是由计算机系统、通信线路和设备、网络协议及网络软件四个部分组成。

计算机系统主要负责数据信息的收集、处理、存储和传播，提供共享资源和各种信息服务，包括各类计算机与其他数据终端设备，如终端服务器等。

通信线路和设备是连接计算机系统的桥梁，主要负责控制数据的发出、传送、接收或转发，包括信号转换、路径选择、编码与解码、差错校验、通信控制管理等。

网络协议为网络中各个主机之间或各节点之间通信双方事先约定和必须遵守的规则。网络协议规定了分层原则、层间关系、执行信息传递过程的方向、分解与重组等规则，网络协议的实现由相关硬件和软件完成。

网络软件是一种在网络环境下使用、运行或者控制和管理网络工作的计算机软件。网络软件根据软件功能可分为网络系统软件和网络应用软件两大类型。网络系统软件是控制和管理网络运行、提供网络通信、分配和管理共享资源的网络软件，包括网络操作系统、网络协议软件、通信控制软件和管理软件等。网络应用软件为用户提供访问网络的手段及网络服务，资源共享和信息传输的服务。

（2）计算机网络的类型。

1）按网络的覆盖范围分类。可分为局域网 LAN（Local Area Network）、城域网 MAN（Metropolitan Area Network）与广域网 WAN（Wide Area Network）。

局域网是最常见的计算机网络。局域网分布范围小，容易管理与配置，速度快，延迟小，是

实现有限区域内信息交换与共享的有效途径，应用于科研院所、企业与校园网等。城域网规模局限在一座城市的范围内，辐射的地理范围从几十公里至数百公里，是一个大型的局域网，通常使用与局域网相似的技术，但是在传输介质和布线结构方面牵涉范围较广，应用于政府城市范围、大型企业，以及社会服务部门的计算机联网需求。广域网也称远程网，其分布距离远，覆盖一个国家、地区，或横跨几个洲，形成国际性的远程网络。网络本身不具备规则的拓扑结构。速度慢，延迟大，需要采用网络设备负责管理工作。

2）按网络拓扑结构分类。星型结构由中央节点为中心与各节点连接组成，多节点与中央节点通过点到点的方式连接，中央节点相对复杂，拓扑结构如图 4-1（a）所示。星型结构结构简单，容易实现，新节点扩展方便，易于维护、管理及实现网络监控，某个节点与中央节点的链路故障不影响其他节点间的正常工作。

环型结构中各节点通过环路接口连在一条首尾相连的闭合环形通信线路中，拓扑结构如图 4-1（b）所示。环型网络在网络中沿固定方向流动，两个节点间仅有唯一的通路，简化了路径选择的控制；某个节点发生故障时，可以自动旁路，可靠性较高；由于信息是串行穿过多个节点环路接口，当节点过多时，使网络响应时间变长。但当网络确定时，其延时固定，实时性强。

总线型结构是一条公用总线连接若干个节点所形成的网络，拓扑结构如图 4-1（c）所示。总线型网络结构简单灵活，便于扩充，容易建造。由于多个节点共用一条传输信道，故信道利用率高，但容易产生访问冲突，可靠性不高。

树型网络结构可以看做是星型结构的扩展，是一种分层结构，具有根节点和各分支节点，如图 4-1（d）所示。除了叶节点之外，所有根节点和子节点都具有转发功能，其结构比星型结构复杂，数据在传输的过程中需要经过多条链路，延迟较大，适用于分级管理和控制的网络系统，是一种广域网或规模较大的快速以太网常用的拓扑结构。

网状型结构。由分布在不同地点、各自独立的节点经链路连接而成，每一个节点至少有一条链路与其他节点相连，每两个节点间的通信链路可能不止一条，需进行路由选择，如图 4-1（e）所示。

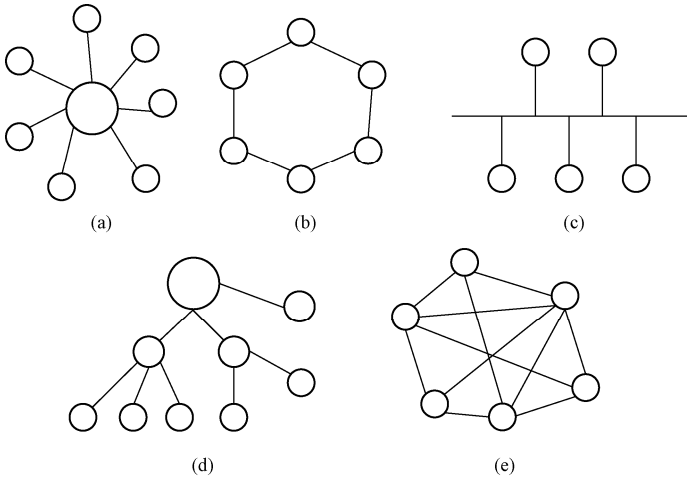

图4-1　常见的计算机网络拓扑结构

（a）星型拓扑；（b）环型拓扑；（c）总线型拓扑；（d）树型拓扑；（e）网状型拓扑

3）按网络传输技术分类。可分为广播式网络与点对点式网络。

广播式网络中所有联网计算机都共享一个公共通信信道。当某计算机利用共享通信信道发送

数据时，其他计算机都能收到相关数据，该网络存在信道访问冲突问题。典型的广播式网络有总线网、局域网、微波、卫星通信网。

在点对点式网络中，每条物理线路连接一对计算机。每两台主机、两台节点交换机之间或主机与节点交换机之间都存在一条物理信道，从某信道发送的数据只有信道另一端的设备能收到，该网络没有信道竞争。绝大多数广域网都采用点到点的拓扑结构，网状形网络是典型的点到点拓扑。点对点式网络还被用于星型结构、树型结构，以及某些环网。

4）其他分类方式。按网络传输信息采用的物理信道来分类，可划分为有线网络和无线网络。

按通信速率的不同来分类，可划分为低速、中速与高速网络。低速网络数据传输速率在 1.5Mb/s 以下，中速网络数据传输速率在 50Mb/s 以下，高速网络数据传输速率在 50Mb/s 以上。

按使用范围的大小分类，可分为公用网和专用网。其中专用网络根据网络环境又可细分为部门网络、企业网络、校园网络等。

按数据交换方式分类，可分为线路交换网络、报文交换网络、分组交换网络。

按传输的信号分类，可分为数字网和模拟网。

2. 网络体系结构与协议

（1）网络协议。在计算机网络中，为使各计算机之间或计算机与终端之间能正确地交换数据和控制信息，必须在有关信息传输顺序、信息格式和信息内容等方面给出一组约定或规则，规定所交换数据的格式和时序。这些为网络数据交换而定制的规则、约定和标准被称为网络协议。网络协议实质上是实体间通信时所使用的一种语言，主要由语义、语法、规则三个要素组成。

语义是对构成协议的协议元素含义的解释。不同类型的协议元素规定了通信双方所要表达的不同内容。即需要发出何种控制信息，以及要完成的动作与做出的响应。语法是用户数据与控制信息的结构与格式。即指用于规定将若干个协议元素组合在一起表达一个更完整的内容时所应遵循的格式。规则规定了事件的执行顺序。

（2）分层结构。计算机网络采用层次结构，各层之间相互独立，每层通过层间接口提供服务，各层实现技术的改变不影响其他层，层次结构使得复杂系统的实现和维护变得易于实现和维护。计算机网络体系结构是网络层次结构模型与各层协议的集合，网络体系结构是抽象的，其实现通过具体的软件和硬件完成。

（3）开放系统互连参考模型。国际标准化组织 ISO 于 1981 年制定了开放系统互连参考模型 OSI/RM（Open System Interconnection/Reference Model），OSI/RM 并不是一个具体的网络，它只给出了一些原则性的说明，任何两个遵守 OSI/RM 的系统都可以进行互连，当一个系统能按 OSI/RM 与另一个系统进行通信时，就称该系统为开放系统。OSI 网络系统结构参考模型如图 4-2 所示。该模型把网络通信的工作分为 7 层，由低层至高层分别为物理层、数据链路层、网络层、运输层、会话层、表示层和应用层。

1）物理层（Physical Layer）。物理层提供网络通信接口的机械、电气、功能和规程的特性，物理层的下面是具体的物理媒体，如双绞线、同轴电缆等。物理层的任务就是为数据链路层提供一个物理连接，以便在数据链路实体之间建立、维护和拆除物理连接。物理层通过物理连接在数据链路实体之间提供透明的位流传输。在物理层上所传数据的单位是比特。

2）数据链路层（Data Link Layer）。数据链路层负责在两个相邻节点间的链路上，无差错地传送以帧为单位的数据。帧是数据的逻辑单位，每一帧包括一定数量的数据和一些必要的控制信息。与物理层相似，数据链路层要负责建立、维持和释放数据链路的连接。在传送数据时，若接收节点检测到所传数据中有差错，要通知发方重发该帧，直到该帧正确无误地到达接收节点

为止。在每帧所包括的控制信息中，有同步信息、地址信息、差错控制，以及流量控制信息等。

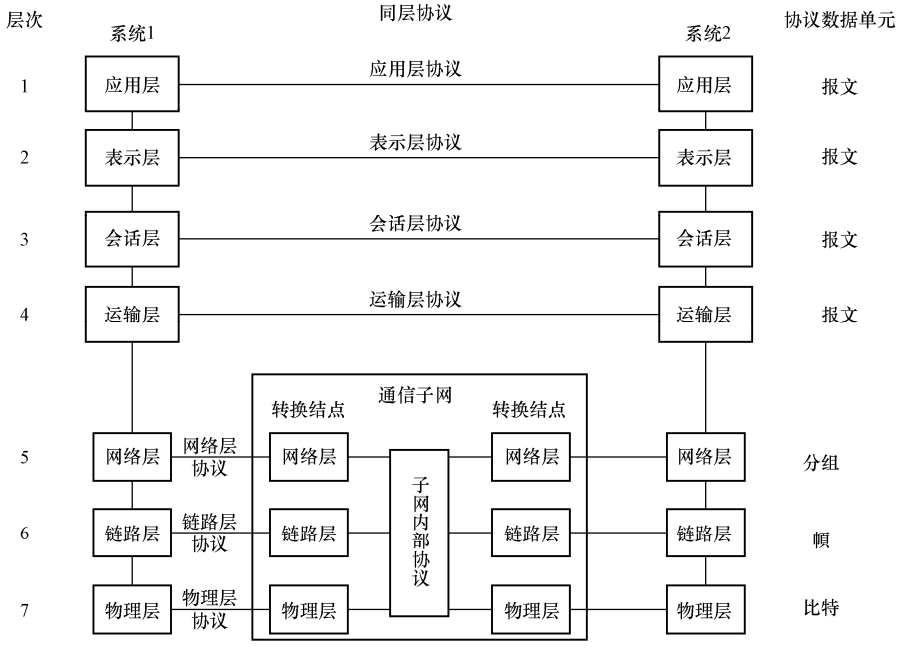

图 4-2　OSI 网络系统结构参考模型

3）网络层（Network Layer）。在计算机网络中进行通信的两个计算机之间可能要经过许多个节点和链路，也可能还要经过好几个通信子网。在网络层，数据的传送单位是分组或包。网络层的任务就是要选择合适的路由和交换节点，透明地向目的节点交付发送节点所发送的分组，并交付给目的站的传输层，这里“透明”表示网络的存在并不会使所传送的分组丢失、重复或甚至使分组的顺序出现错误，而好像收发两端是直接连通的。

4）传输层（Transport Layer）。在传输层，信息的传送单位是报文（message）。当报文较长时，先要把它分割成好几个分组，然后交给网络层进行传输。

传输层的任务是根据通信子网的特性最佳地利用网络资源，并以可靠和经济的方式，为两个端系统的会话层之间建主一条传输连接，透明地传送报文。或者说，传输层向会话层提供一个可靠的端到端的服务。在通信子网中没有传输层。传输层只能存在于端系统（即主机）之中。传输层以上的各层就不再管信息传输的问题。因此，传输层就成为计算机网络体系结构中最为关键的一层。

5）会话层（Session Layer）。该层也称对话层。在会话层及以上的更高层次中，数据传送的单位一般都称为报文。

会话层虽然不参与具体的数据传输，但它却对数据传输进行管理。会话层在两个互相通信的应用进程之间，建立、组织和协调其交互。例如，确定是双工还是半双工工作。当发生意外时，如已建立的连接突然断开，要确定在重新恢复会话时应从何处开始。

6）表示层（Presentation Layer）。表示层主要解决用户信息的语法表示问题。表示层将欲交换的数据从适合于某一用户的抽象语法，变换为适合于 OSI 系统内部使用的传送语法。有了表示层，用户就可以把精力集中在所要交谈的问题本身，而不必更多地考虑对方的某些特性。

对传送信息进行加密也是表示层的任务之一，解密则由通信的另一端的表示层来进行。由于数据的安全与保密问题比较复杂，7 层中的其他一些层次也与这一问题有关。

7）应用层（Application Layer）。应用层是 OSI 参考模型中的最高层。它确定进程之间通信的性质以满足用户的需要，这反映在用户所产生的服务请求，负责用户信息的语义表示，并在两个通信者之间进行语义匹配。应用层不仅要提供应用进程所需要的信息交换和远程操作，而且作为互相作用的应用进程的用户代理，来完成一些语义上有意义的信息交换所必需的功能。

3. 数据通信概念

（1）通信系统的组成。数据通信是通信技术和计算机技术相结合的一种通信方式，一个简单的通信系统如图 4-3 所示。数据通信系统包括信源/信宿、通信信道和收发设备。收发设备包含收发器与通信控制器。

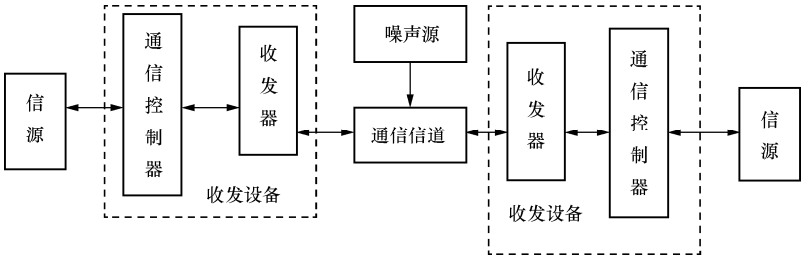

图 4-3　通信系统的组成

1）信源。信源指信息的来源或发送者，信宿指信息的归宿或接收者。在计算机网络中，信源和信宿可以是计算机或终端等设备。

2）通信信道。传输信号的通路，由传输线路及相应的附属设备组成。信道分有线信道（有形的电路作为传输介质）和无线信道（以电磁波在空间传输方式传送信息的信道），可以是模拟的，也可以是数字方式的。用以传输模拟信号的信道称为模拟信道，用以传输数字信号的信道称为数字信道。同一条传输线路上可以有多个信道。

3）收发器。它在信源或信宿与信道之间进行信号的变换。把通信控制器提供的数据转换成适合通信信道要求的信号形式，或把信道中传来的信号转换成可供数据终端设备使用的数据，最大限度地保证传输质量。

4）通信控制器。控制数据传输的设备，它的功能除进行通信状态的连接、监控和拆除等操作外，还可接收来自多个数据终端设备的信息，并转换信息格式。

5）噪声。在通信过程中，信道上不可避免地存在噪声，它是所有干扰信号的总称。噪声会影响原有信号的状态，干扰有效信号的传输，造成有效信号变形或失真。在计算机网络通信中应尽可能降低噪声对信号传输质量的影响。

（2）基本概念。

1）信息、数据和信号。信息是人脑对客观物质的反映，可以是对物质的形态、大小、结构、性能等特性的描述，也可以是物质与外部的联系。信息的具体表现形式可以是数据、文字、图形、声音、图像和动画等。

数据是描述物体概念、情况、形势的事实、数字、字母和符号，是信息的载体与表示方式。在计算机网络系统中，数据可以是数字、字母、符号、声音和图像等形式，从广义上可理解为在网络中存储、处理和传输的二进制数字编码。

信号是数据在传输过程中的表示形式，是用于传输的电子、光或电磁编码。信号有模拟信号

和数字信号之分。模拟信号是随时间连续变化的电流、电压或电磁波。用模拟信号表示要传输的数据，是指利用其某个参量（如幅度、频率或相位等）的变化来表示数据。数字信号是一系列离散的电脉冲，为离散信号。用数字信号表示要传输的数据，是指利用其某一瞬间的状态来表示数据。

由此可见，数据是信息的载体，信息是数据的内容和解释，而信号是数据的编码。

2）模拟通信和数字通信。数据通信是指发送方将要发送的数据转换成信号，并通过物理信道传送到接收方的过程。信号可以是模拟信号，也可以是数字信号，传输信道也被分为模拟数据信道和数字数据信道，数据通信又分为模拟通信和数字通信。模拟通信是指在模拟信道以模拟信号的形式来传输数据，数字通信是指在数字信道以数字信号的形式来传输数据。

3）数据通信方式。按照字节使用的信道数，数据通信分为并行通信与串行通信两种方式。

并行通信中数据以成组的方式在多个并行信道上同时进行传输。常用的方式是将构成 1 个字符代码的几位二进制比特分别通过几个并行的信道同时传输。并行通信的优点是速度快，但收发两端之间有多条线路，费用高，适合于近距离和高速率的通信。并行通信被广泛应用在计算机内部总线以及并行口通信中。

串行通信中数据以串行方式在一条信道上传输。由于计算机内部都采用并行通信，数据在发送之前，要将计算机中的字符进行并/串变换，在接收端再通过串/并变换，还原成计算机的字符结构实现串行通信。串行通信收发双方只需要一条通信信道，易于实现，成本低，但速度比较低。串行通信被广泛应用在计算机通串行口及远程通信中。

根据通信双方信息的传送方向，串行通信进一步分为单工、半双工和全双工三种。信息只能单向传送为单工；信息能双向传送但不能同时双向传送称为半双工，其通信线路简单，有两条通信线就行了，应用广泛；信息能够同时双向传送则称为全双工，全双工通信的效率最高，通信线至少三条（其中一条为信号地线），相对复杂，系统造价也较高。

（3）数据通信系统的技术指标。

1）波特率。每秒钟传送的码元数，单位为 Baud/s，又称为码元速率 R_B。在数字通信系统中，数字信号是用离散值表示的，每一个离散值就是一个码元，一个码元可携带多个比特。

2）比特率。每秒钟传送的信息量，单位为 b/s，又称为信息速率 R_b。对于一个用二进制表示的信号，每个码元包含 1 比特信息，其信息速率与码元速率相等；对于采用 M 进制信号传输信号时，信息速率和码元速率之间的关系是：$R_b=R_B\lg 2^M$。

3）误码率。衡量数据在规定时间内数据传输精确性的指标。误码率是指码元在传输过程中，错误码元占总传输码元的概率。在二进制传输中，误码率也称为误比特率。计算机通信的平均误码率要求低于 10^{-9}，普通通信信道如不采取差错控制技术是不能满足计算机通信要求的。

4）信道带宽。信道带宽是指信道中传输的信号在不失真的情况下所占用的频率范围，通常称为信道的通频带，单位用 Hz 表示。信道带宽是由信道的物理特性所决定的。例如，电话线路的频率范围为 300～3400Hz，它的带宽范围为 300～3400Hz。

5）信道容量。信道容量即信道的最大数据传输速率，即信道传输数据能力的极限。信道容量是衡量一个信道传输数字信号的重要参数。信道容量是指单位时间内信道上所能传输的最大比特数，用 bit/s 表示。当传输速率超过信道的最大信号速率时就会产生失真。信道的最大传输速率是与信道带宽有直接联系的。信道容量和信道带宽具有正比的关系，带宽越大，容量越高，要提高信号的传输率，信道就要有足够的带宽。

4. 数据传输

（1）数据的传输方式。

1）基带传输。基带传输是最基本的数据传输方式，即按数据波的原样，不包含任何调制，在数字通信的信道上直接传输数字信号。传输媒体整个带宽都被基带信号占用，双向地传输信息。就数字信号而言，它是一个离散的矩形波，这种矩形波固有的频带称为基带，基带实际上就是数字信号所占用的基本频带。

基带传输不适于传输语言、图像等信息。目前大部分局域网都是采用基带传输方式的基带网。基带网的信号按位流形式传输，整个系统不用调制解调器，传输介质较宽带网便宜，可以达到较高的数据传输速率（一般为 10～100Mb/s），其传输距离一般不超过 25km，传输距离越长，质量越低，基带网中线路工作方式只能为半双工方式或单工方式。基带传输时，通常对数字信号进行一定的编码。

2）频带传输。频带传输是一种采用调制、解调技术的传输形式。在发送端，采用调制手段，对数字信号进行某种变换，将代表数据的二进制数变换成具有一定频带范围的模拟信号，以适应在模拟信道上传输；在接收端，通过解调手段进行相反变换，把模拟的调制信号复原为二进制数。当采用频带传输方式时，要求发送端和接收端都要安装调制解调器。

3）宽带传输。将信道分成多个子信道，分别传送音频、视频和数字信号，称为宽带传输。宽带是比音频带宽更宽的频带，它包括大部分电磁波频谱。宽带传输系统通过借助频带传输，可以将链路容量分解成两个或更多的信道，每个信道可以携带不同的信号。宽带传输中的所有信道可以同时发送信号，实现多路复用，信道的容量大大增加，如 CATV、ISDN 等。

（2）数据传输的同步方式。通信过程中收发双方需要高度的协同动作，在时间上保持一致，一方面码元之间要保持同步，另一方面由码元组成的字符或数据之间在起止时间上也要同步。即传输数据的速率、持续时间和间隔都必须相同，否则，收发之间会产生误差，造成传输的数据出错。实现数据传输同步常用方法有同步传输和异步传输两种。

1）异步传输。异步传输方式，一次传输一个字符，每个字符由一位起始位引导，停止位结束，数据格式如图 4-4 所示。起始位为“0”，第 2～8 位为 7 位数据（字符），第 9 位为数据位的奇或偶校验位，停止位为 “1”，占用 1～2 位脉宽。一帧信息由 10 位、10.5 位或 11 位构成。

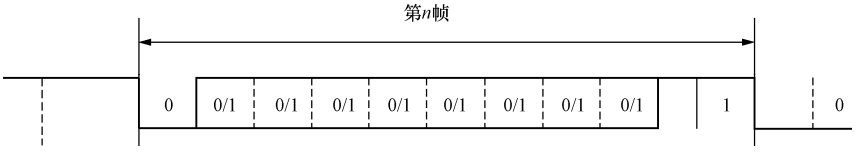

图 4-4　异步传输的数据格式

异步传输按照约定好的固定格式，一帧一帧地传送。在异步传输方式中，接收方根据起始位和停止位来判断一个新字符的开始和结束，从而起到通信双方的同步作用。异步方式的实现比较容易，但每传输一个字符都要用起始位和停止位作为字符开始和结束的标志，因而传送效率低，主要用于中、低速通信的场合。

2）同步方式。同步传输要求发送方和接收方时钟始终保持同步，即每比特位必须在收发两端始终保持同步，中间没有间断时间。通常，同步传输方式的信息格式是由一组字符或一个二进制位组成的数据块（帧）。对这些数据，不需要附加起始位和停止位，而是在发送一组

字符或数据块之前先发送一个同步字符 SYN（以 01101000 表示）或一个同步字节（01111110），用于接收方进行同步检测，从而使收发双方进入同步状态。在同步字符或字节之后，可以连续发送任意多个字符或数据块，发送数据完毕后，再使用同步字符或字节来标识整个发送过程的结束。

同步传输中发送方和接收方将整个字符组作为一个单位传送，且附加位少，从而提高了数据传输的效率，该方法一般用在高速传输数据的系统，如计算机之间的数据通信。同步传输又可分为面向字符的同步和面向位的同步，如图 4-5 所示。

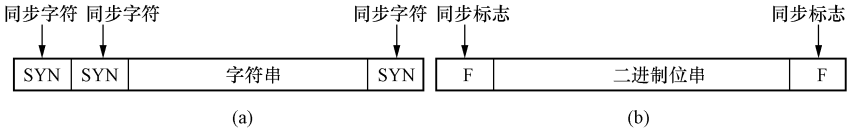

图 4-5　同步传输方式

（a）面向字符的同步；（b）面向位的同步

面向字符的同步在传送一组字符之前加入 1 个（8bit）或 2 个（16bit）同步字符 SYN 使收发双方进入同步。同步字符之后可以连续地发送多个字符，每个字符不再需要任何附加位。接收方接收到同步字符时就开始接收数据，直到又收到同步字符时停止接收。

面向位的同步每次发送一个二进制序列，用某个特殊的 8 位二进制串（如 01111110）作为同步标志来表示发送的开始和结束。

（3）数据的编码和调制技术。计算机中的数据是以离散的二进制“0”、“1”比特序列方式来表示的。计算机数据在传输过程中的数据编码类型主要取决于它采用的通信信道所支持的数据通信类型。网络中的通信信道分为模拟信道和数字信道，信道传输的数据也分为模拟数据与数字数据。数据的编码方法包括数字数据的编码与调制和模拟数据的编码与调制，如图 4-6 所示。

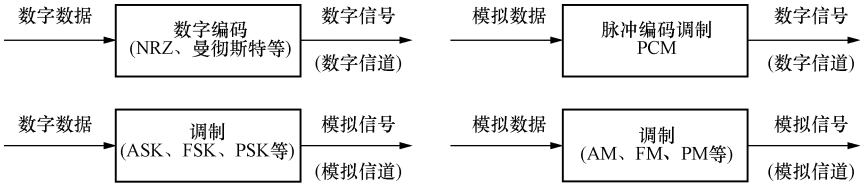

图 4-6　数据的编码和调制技术

1）数字数据的编码。利用数字通信信道直接传输数字数据信号的方法，称为数字信号的基带传输。而数字数据在传输之前需要进行数字编码。数字数据的编码，就是解决数字数据的数字信号表示问题，即通过对数字信号进行编码来表示数据。常用的编码方法有不归零编码 NRZ（Non-return to Zero）、曼彻斯特编码（Manchester）、差分曼彻斯特编码（Difference Manchester）三种，图 4-7 为数字数据信号的编码方法。

- 不归零编码。NRZ 编码可以用正电平表示逻辑“1”，用负电平表示逻辑“0”，反之亦然。NRZ 编码的缺点是发送方和接收方不能保持同步，需采用其他方法才能保持收发同步。
- 曼彻斯特编码。该编码是目前应用最广泛的编码方法之一。其特点是每一位二进制信号的中间都有跳变，若从低电平跳变到高电平，就表示数字信号“1”；若从高电平跳变到低电平，就表示数字信号“0”。曼彻斯特编码将每比特的中间分为前 T/2 和后 T/2，其原则是前 T/2 取反码，后 T/2 取原码。

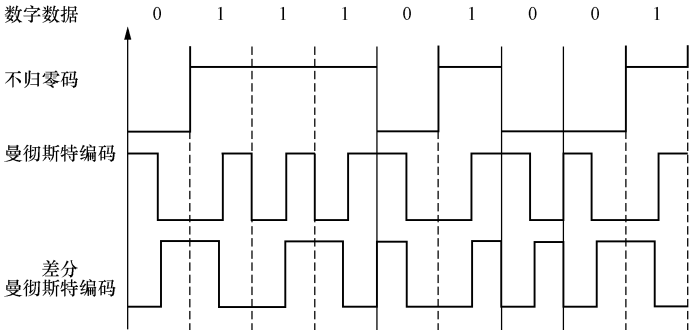

图 4-7　数字数据信号的编码方法

曼彻斯特编码的优点是每一比特中间的跳变可以作为接收端的时钟信号，以保持接收端和发送端之间的同步。

- 差分曼彻斯特编码。差分曼彻斯特编码是对曼彻斯特编码的改进，其特点是每位二进制信号的跳变依然提供收、发端之间的同步，但每位二进制数据的取值，必须要根据其开始边界是否发生跳变来决定，若一比特开始处存在跳变则表示“0”，无跳变则表示“1”。

2）数字数据的调制。典型的模拟通信信道是电话通信信道，传统的电话通信信道是为传输语音信号设计的，用于传输音频 300～3400Hz 的模拟信号，不能直接传输数字数据。为了利用模拟语音通信的电话交换网实现计算机的数字数据的传输，必须对数字数据进行调制。在发送端将数字数据信号变换成模拟信号的过程称为调制（Modulation），调制设备就称为调制器（Modulator），在接收端将模拟数据信号还原成数字数据信号的过程称为解调（Demodulation），解调设备就称为解调器（Demodulator）。若进行数据通信的发送端和接收端以双工方式进行通信时，就需要一个同时具备调制和解调功能的设备，称为调制解调器（Modem）。

模拟信号可以用 $A\cos(2\pi ft+\varphi)$ 表示，其中 A 表示波形的幅度，f 代表波形的频率，φ 代表波形的相位。根据这三个不同参数的变化，就可以表示特定的数字信号 0 或 1，实现调制的过程。数字数据的调制方法如图 4-8 所示。相应的调制方式分别称为幅移键控 ASK（Amplitude Shift Keying）、频移键控 FSK（Frequency Shift Keying）和相移键控 PSK（Phase Shift Keying）。

- 幅移键控。ASK 是通过改变载波信号的幅度值来表示数字信号“1”、“0”的，以载波幅度 A_1 表示数字信号“1”，用载波幅度 A_2 表示数字信号“0”，而载波信号的参数 f 和 φ 恒定。
- 频移键控。FSK 是通过改变载波信号频率的方法来表示数字信号“1”、“0”的，用 f_1 表示数字信号“1”，用 f_2 表示数字信号“0”，而载波信号的 A 和 φ 不变。
- 相移键控。PSK 是通过改变载波信号的相位值 ϕ 来表示数字信号“1”、“0”的，而载波信号的 A 和 f 不变。PSK 包括绝对调相和相对调相两种类型。绝对调相。使用相位的绝对值，ϕ 为 0 表示数字信号“1”，ϕ 为 π 表示数字信号“0”。相对调相。相对调相使用相位的偏移值，当数字数据为 0 时，相位不变化，而数字数据为 1 时，相位要偏移 π。

3）模拟数据的编码。由于数字信号传输具有失真小、误码率低、价格低和传输速率高等特点，所以常把模拟数据转换为数字信号来传输。脉冲编码调制 PCM（Pulse Code Modulation）是模拟数据数字化的主要方法，它包括采样、量化和编码 3 个步骤。

PCM 的理论基础是奈奎斯特（Nyquist）采样定理：若对连续变化的模拟信号进行周期性采样，只要采样频率大于等于有效信号最高频率或其带宽的两倍，则采样值便可包含原始信号的全

部信息，可以从这些采样中重新构造出原始信号。

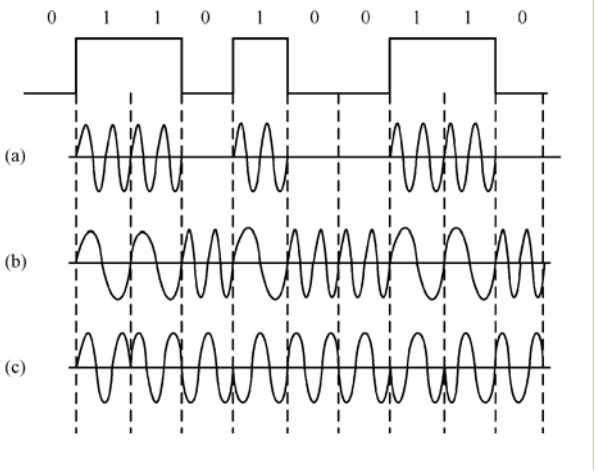

图 4-8　数字数据的调制方法

（a）ASK；（b）FSK；（c）PSK

- 采样：根据采样频率，隔一定的时间间隔采集模拟信号的值，得到一系列模拟值。
- 量化：将采样得到的模拟值按一定的量化级进行“取整”，得到一系列离散值。
- 编码：将量化后的离散值数字化，得到一系列二进制值；然后将二进制值进行编码，得到数字信号。

PCM 技术的典型应用是语音数字化。语音可以用模拟信号的形式通过电话线路传输，但是在网络中将语音与计算机产生的数字、文字、图形、图像同时传输，就必须首先将语音信号数字化。在发送端通过 PCM 编码器变换为数字化语音数据，通过通信信道传送到接收方，接收方再通过 PCM 解码器还原成模拟语音信号。数字化语音数据传输速率高、失真小，可以存储在计算机中，进行必要的处理。

4）模拟数据的调制。在模拟数据通信系统中，信源的信息经过转换形成电信号，可以直接在模拟信道上传输，由于天线尺寸和抗干扰等诸多问题，一般也需要进行调制，其输出信号是一种带有输入数据的、频率极高的模拟信号。其调制技术有调幅、调频和调相三种，最常用的是调幅和调频，如调频广播。

幅度调制是指载波的幅度会随着原始模拟数据的幅度变化而变化的技术。载波的幅度会在整个调制过程中变化，而载波的频率是相同的。频率调制是一种使高频载波的频率随着原始模拟数据的幅度变化而变化的技术。载波的频率会在整个调制过程中波动，而载波的幅度是相同的。

（4）多路复用技术。多路复用（Multiplexing）是在一条物理线路上传输多路信号来充分利用信道资源。信道复用的目的是让不同的计算机连接到相同的系统上，以共享信道资源。在长途通信中，一些高容量的同轴电缆、地面微波、卫星设施以及光缆可传输的频率带宽很宽，为了高效地利用资源，通常采用多路复用技术，使多路数据信号共同使用一条电路进行传输，即利用一个物理信道同时传输多个信号。多路复用原理示意图如图 4-9 所示。

计算机网络中的信道连接方式一般有点到点和信道复用两种。复用技术采用多路复用器（Multiplexer）将来自多个输入电路的数据组合调制成一路复用数据，并将此数据信号送上高容量

的数据链路；多路解复器接收复用的数据流，依照信道分离还原为多路数据，并将它们送到适当的输出电路上，用一对多路复用器和一条通信线路来代替多套发送、接收设备与多条通信线路。

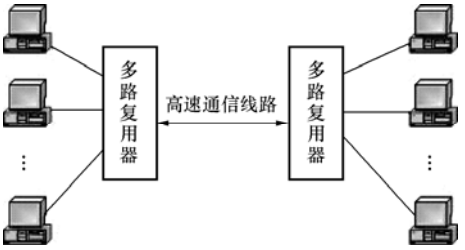

图 4-9　多路复用原理示意图

信道复用方式主要有 4 种类型，即频分多路复用 FDM（Frequency Division Multiplexing）、时分多路复用 TDM（Time Division Multiplexing）、WDM 波分多路复用（Wave-length Division Multiplexing）和码分多路复用 CDMA（Coding Division Multiplexing Access）。

1）频分多路复用 FDM。FDM 把信道的可用频带分成多个互不交叠的频段，每个信号占其中一个频段。接收时用适当的滤波器分离出不同信号，分别进行解调接收。

频分多路复用是把电路或空间的频带资源分成多个频带，并将其分别配给多个用户，每个用户终端的数据通过分配给它的子通路传输，其主要用于电话和电缆电视（CATV）系统。在 FDM 频分复用中，各个频带都有一定的带宽，称为逻辑信道，有时简称为信道。

2）时分多路复用 TDM。TDM 是按传输信号的时间进行分割的。它使不同的信号在不同时间内传送，即将整个传输时间分为许多时间间隔（Slot time），每个时间段被一路信号占用。TDM 就是通过在时间上交叉发送每一路信号的一部分来实现一条电路传送多路信号的。电路上的每一短暂时刻只有一路信号存在，而频分多路复用是同时传送若干路不同频率的信号。因为数字信号是有限个离散值，所以时分多路复用技术广泛应用于包括计算机网络在内的数字通信系统，而模拟通信系统的传输一般采用频分多路复用。

3）波分多路复用 WDM。WDM 主要用于全光纤网组成的通信系统。波分复用就是光的频分复用，人们借用传统的载波电话的频分复用的概念，可以做到使用一根光纤来同时传输与多个频率都很接近的光载波信号，这样就使光纤的传输能力成倍地提高。由于光载波的频率很高，而习惯上是用波长而不用频率来表示所使用的光载波，因而称其为波分复用。最初，只能在一根光纤上复用两路光载波信号，但随着技术的发展，在一根光纤上复用的路数越来越多。

4）码分多路复用 CDMA。码分多路复用又称为码分多址，它也是一种共享信道的方法，每个用户可在同一时间使用同样的频带进行通信，但使用的是基于码型的分割信道的方法，即每个用户分配一个地址码，各个码型互不重叠，通信各方之间不会相互干扰，且抗干扰能力强。码分复用技术主要用于无线通信系统，特别是移动通信系统。它不仅可以提高通信的语音质量、数据传输的可靠性和减小干扰对通信的影响，而且增大了通信系统的容量。

5. 数据交换技术

数据经编码后在通信线路上进行传输的最简单形式，是在两个互连的设备之间直接进行数据通信。但是网络中所有设备都直接两两相连，显然不经济，当通信设备相隔很远时更不合适。

数据传输通常要经过中间节点将数据从信源逐点传送到信宿，实现两个互连设备之间的通信。这些中间节点并不关心数据内容，其目的只是提供一个交换设备，把数据从一个节点传送到另一个节点，直至到达目的地。通常将数据在各节点间的数据传输过程称为数据交换。数据交换技术主要是指网络中间节点所提供的数据交换功能。

在网络系统中，主要使用三种交换技术：电路交换（Circuit Exchanging）、报文交换（Message Switching）和分组交换（Packet Switching），如图 4-10 所示。

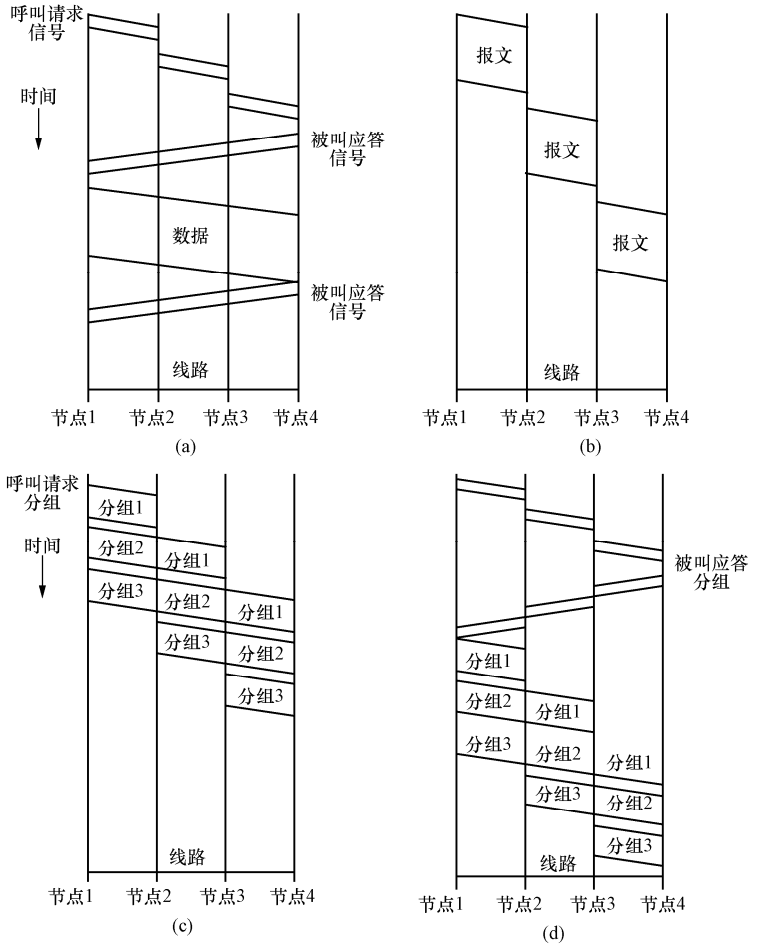

图 4-10　数据交换方式

（a）电路交换；（b）报文交换；（c）数据报交换；（d）虚电路交换

（1）电路交换。也称线路交换，在两台计算机通过通信网络进行数据交换之前，首先要在通信网中建立一条实际的物理线路连接。在电路交换方式中，一次数据通信过程要经历电路建立、数据传输与电路拆除三个阶段。电路建立是构建一条利用中间节点构成的端到端的专用物理连接线路，数据传输是沿着已建好的线路传输数据，电路拆除是在数据传送结束后，拆除物理连接，释放该连接所占用的专用资源。

电路交换的特点如下：

1）线路建立后，所有数据直接传输。因此数据传输可靠、迅速、有序。

2）电路接通后即为专用信道，因此线路利用率低。例如线路空闲时，信道容量被浪费。

3）线路建立时间较长，造成有效时间的浪费。例如只有少量数据要传送时，也要花不少时间用于建立和拆除电路。

4）电路交换适用于高负荷的持续通信和实时性要求较强的场合，如会话式通信，不适合突发性通信。

（2）报文交换。报文交换是以报文为单位进行存储转发交换的技术。在发送数据时不需要事先建立一条专用通道，而是把要发送的数据作为整体交给网络节点，网络节点通常为一台专用计算机，备有足够的外存来缓存报文，每个中间节点接收一个报文之后，报文暂存在外存中，等待

输出线路空闲时再根据报文中所指的目的地址转发到下一个合适的网络节点，直到报文到达目的节点。

报文交换方式与电路交换方式相比，具有如下优点：

1）没有建立和拆除连接所需的等待时间，节点之间的信道共享，在同一线路容量条件下，可以承载更大的网络流量，线路利用率高。

2）收发端无需同步工作，当接收端忙碌时，中间节点可将报文暂时存储，等到接收端空闲时再传送。

3）当流量增大时，电路交换网络可导致一些呼叫请求被阻塞；在报文交换网络中，报文仍然可以接收，但会增加传输延时。

4）报文交换系统可同时向多个目的端发送同一报文，实现多播（Multicast）功能，电路交换系统难以实现。

5）报头中设置报文优先级，中间节点可根据报文优先级的高低提供不同质量的转发服务。

6）网络上分段实施差错控制和纠错处理功能。

7）提供传输速率和数据格式的转换，不同传输速率和数据格式的端点之间能够相互通信。

（3）分组交换。它是以分组为单位进行存储转发交换的技术。它不是以整个报文为单位进行交换的，而是以更短的、标准化的分组为单位进行交换的。分组交换中，将大的报文分成若干个小的分组，每个分组通过交换网络中的节点进行存储转发。由于分组长度较小，可以用内存来缓冲分组，因而减少了中间节点的转发延迟，也降低了差错率。

分组交换可以分成数据报交换和虚电路交换两种方式。

数据报交换与报文交换相类似，在数据传输时不需要预先建立连接，当发送端有一个较长的报文要发送时，首先将报文分解成若干个较小的数据单元，每个数据单元都要附加一个分组头并封装成分组，然后将各个分组发送出去。每个分组都被独立地传输，中间节点可能为每个分组选择不同的路由，这些分组到达目的端的顺序可能与发送的顺序不同，因此目的端必须重新排序分组，组装成一个完整的原始报文。

虚电路（Virtual Circuit）交换与电路交换相类似，数据传输是面向连接的，在数据传输时必须预先建立一个连接，但这种连接是基于共享线路的，而不像电路交换中的连接需要独占线路。虚电路交换也分成三个阶段：建立连接、数据传输和拆除连接。

1）建立连接。发送端在发送数据分组之前，首先使用一个特定的建立连接请求分组建立一条逻辑连接，网络中间节点将根据该请求在发送端和目的端之间预先选择一条传输路径。由于该路径上的各段线路是共享的，并非独占的。因此，这种逻辑连接称为虚电路。

2）数据传输。当虚电路建立起来后，发送端和目的端之间便可以在这条虚电路上交换数据，并且每个数据分组中都必须包含一个虚电路标识符，用于标识这个虚电路。由于虚电路的传输路径是预先选择好的。因此，每个中间节点只要根据虚电路标识符就能查找到相应的路径来传输这些数据分组，无需重新选择路由。

3）拆除连接。当数据传输完毕后，任一个端点都可以发出一个拆除连接请求分组，终止这个虚电路，释放该虚电路所占用的系统资源。

可见，虚电路是一种面向连接的数据交换方式，它既不像电路交换那样需要独占线路，而是采用共享线路方式来建立连接，通过存储—转发方法实现数据交换；它又不同于数据报方式，只是在建立虚电路时选择一次路由，后续的各个分组只要使用该路由传送即可，而无需重新选择路由。

6. 差错控制技术

根据数据通信系统的组成，当数据从信源端发出后，经过通信信道传输时，由于信道存在着

一定的噪声，当数据到达信宿端后，接收的信号实际上是数据信号和噪声信号的叠加。如果噪声对信号的影响非常大时，就会造成数据的传输错误。

通信信道中的噪声分为热噪声和冲击噪声。热噪声是由传输媒体的电子热运动产生，冲击噪声是由外界电磁干扰引起的。在数据通信过程中，为了保证将数据的传输差错控制在允许的范围内，就必须采用差错控制方法。

（1）差错编码。差错控制常采用冗余编码方案来检测和纠正信息传输中产生的错误。冗余编码是指在发送端把要发送的有效数据，按照所使用的某种差错编码规则加上控制码（冗余码），当信息到达接收端后，再按照相应的校验规则检验收到的信息是否正确。常用的检错编码有奇偶校验码、循环冗余码 CRC（Cycle Redundancy Check）等。

1）奇偶校验码。奇偶校验码是一种简单的检错码。其原理是通过增加冗余位来使得码字中“1”的个数保持为奇数（奇校验）或偶数（偶校验）。

采用奇偶校验码时，在每个字符的数据位传输之前，先检测并计算出数据位中“1”的个数，并根据使用的是奇检验还是偶检验来确定奇偶校验位，然后将其附加在数据位之后进行传输。当接收端接收到数据后，重新计算数据位中包含“1”的个数，再通过奇偶检验就可以判断出数据是否出错。奇偶校验可分为垂直奇偶校验、水平奇偶校验与水平垂直奇偶校验三种方式。

奇偶检验码被广泛地应用于异步通信中。奇偶校验码只能检测单比特出错的情况，对于两个或两个以上的比特出错无能为力。

2）循环冗余码 CRC。它先将要发送的信息数据与一个通信双方共同约定的数据进行除法运算，并根据余数得出一个校验码，然后将这个校验码附加在信息数据帧之后发送出去。接收端在接收数据后，将包括校验码在内的数据帧再与约定的数据进行除法运算，若余数为“0”，则表示接收的数据正确，若余数不为“0”，则表明数据在传输的过程中出现错误。

CRC 在数据通信中用得最广泛的检错码，是一种较为复杂的检验方法，CRC 码检错能力强，不仅能够检测出全部单个错误和全部随机的两位错误，同时也能检测出全部奇数个错误和全部长度小于或等于校验位的突发性错误。

（2）差错控制技术。

1）前向差错控制。也称为前向纠错（Forward Error Correction，FEC）。接收端通过所接收到的数据中的差错编码进行检测，判断数据是否出错。若使用了差错纠错编码，当判断数据存在差错后，还可以确定差错的具体位置，并自动加以纠正。当然，差错纠错编码也只能解决部分出错的数据，对于不能纠正的错误，就只能使用自动重传请求（Automatic Repeat-reQuest，ARQ）的方法予以解决。

2）自动重传请求。接收端检测到接收信息有错后，通过反馈信道要求发送端重发原信息，直到接收端认可为止，从而达到纠正错误的目的。自动重传请求包括停止等待 ARQ 和连续 ARQ 方式。

7. 传输介质

传输介质分有线传输介质与无线传输介质两大类。有线传输介质包括双绞线、同轴电缆和光缆等介质，普通双绞线可以传输低频与中频信号，同轴电缆可以传输低频到特高频信号，光缆可以传输可见光信号。无线传输介质包括无线电、微波、卫星、移动通信等各种通信介质。

（1）有线传输介质。

1）双绞线。双绞线是一种最广泛的传输介质，由绞合在一起的两根绝缘导线组成，可以减少电磁干扰，提高传输质量。双绞线既可用于传输模拟信号，也可用于传输数字信号，信号传输速率取决于双绞线的芯线材料、传输距离、驱动器与接收器能力等诸多因素。

双绞线有多种类型，不同类型的双绞线所提供的带宽各不相同。局域网中所使用的双绞线有无屏蔽双绞线 UTP（Unshielded Twisted Pair）和屏蔽双绞线 STP（Shielded Twisted Pair）两类。

非屏蔽双绞线 UTP 用一层绝缘胶皮包裹，传输距离一般为 100m，价格相对便宜，使用广泛。非屏蔽双绞线有 1、2、3、4、5 五类，常用的是 3 类线和 5 类线，5 类线既可支持 100Mb/s 的快速以太网连接，又可支持到 150Mbps 的 ATM 数据传输，是连接桌面设备的首选传输介质。

屏蔽双绞线 STP 外面由一层金属材料包裹，可以减小辐射，抗干扰性好，数据传输速率较快，用于远程中继线时，最大距离可以达到十几千米，但成本较高。

2）同轴电缆。同轴电缆由绕在同一轴线的两个导体所组成的，即内导体（铜芯导线）和外导体（屏蔽层），外导体的作用是屏蔽电磁干扰和辐射，两导体之间用绝缘材料隔离。

常用的同轴电缆有两大类：基带同轴电缆与宽带同轴电缆。基带同轴电缆用于局域网传输数字信号的 50Ω 的粗缆和 50Ω 的细缆，最大距离限制在几公里范围内。宽带同轴电缆用于宽带传输模拟信号的 75Ω 电缆，最大距离可达几十千米左右，同轴电缆抗干扰能力较强，基带同轴电缆的误码率低于 10^{-7}，宽带同轴电缆的误码率低于 10^{-9}。

3）光缆。光缆是光纤电缆的简称，是传送光信号的介质，它由纤芯、包层和外部增强强度的保护层构成。纤芯是采用二氧化硅掺以锗、磷等材料制成，呈圆柱形。外面包层用纯二氧化硅制成，它将光信号折射到纤芯中。光纤分单模和多模两种，单模只提供一条光通路，在无中继的条件下，传输距离可达几十千米，多模有多条光通路，在无中继的情况下，传输距离可达几千米。单模光纤容量大，传输距离比多模远，价格较贵。光纤只能做单向传输，如需双向通信，需要成对使用。

光缆是目前计算机网络中最有发展前途的传输介质，具有传输距离远、速度快的显著特点，它的传输速率可高达 1000Mb/s，误码率低，衰减小，传播延时很小，并有很强的抗干扰能力。大规模应用于骨干网络的远距离数据传输，在局域网中应用也非常广泛。

（2）无线传输介质。电磁波按照频率由高到低排列可分为无线电波、微波、红外线、可见光、紫外线、X 射线和 γ 射线。目前用于通信的主要有无线电波、微波、红外线、可见光。

对于无线媒体，发送和接收都是通过天线实现的。在发送时，天线将电磁能量发射到媒体（通常是空气）中；接收时，天线从周围的媒体中获取电磁波。

1）无线通信。无线通信所使用的无线电波频段覆盖从低频到特高频。例如，调幅无线电使用中波（中频）MF（300kHz～3MHz），短波无线电使用高频 HF（3～30MHz），调频无线电广播使用甚高频 VHF（30～300MHz），电视广播使用甚高频到特高频 UHF（30MHz～3GHz）。

扩频（Spread Spectrum）无线电是一种新的无线通信技术，不需要许可证，它采用 900 MHz 或 2.4 GHz 的无线电频段作为传输信道，通过先进的直序扩展频谱或跳频方式发射信号，属于宽带调制发射，具有传输速率高、发射功率小、抗干扰能力强以及保密性好等特点。

目前，802.11 系列无线局域网使用无线电波作为传输介质，主要使用 2.4GHz 的无线电波频段。应用于无线上网的蓝牙（Bluetooth）技术也使用无线电波中的 2.4GHz 频段。

2）微波通信。微波通信系统有两种形式：地面系统和卫星系统。微波通信频率在 100MHz 到 10GHz 的微波信号进行通信。微波天线最常见的类型是抛物面天线，固定使用，将电磁波聚集成细波束，从而在可视区内发送给接收天线。

微波在空间是直线传播，传播距离受限，一般只有 50km 左右。为实现远距离通信，必须在一条微波信道的两个端点之间建立若干个中继站，地面微波接力通信。微波通信主要用于不适合铺设有线传输介质的情况，而且只能用于点到点的通信，速率也不高，一般为几百比特率。

3）移动通信。早期的移动通信系统采用大区制的强覆盖区，即建立一个无线电台基站，架设很高的天线塔（高于 30m），使用很大的发射功率，覆盖范围可以达到 30～50km。

目前的移动通信系统将一个大区制覆盖的区域划分成多个小区，每个小区制的覆盖区域设立一个基站，通过基站在用户的移动站之间建立通信。小区覆盖的半径较小，一般为 1～10km，因此可用较小的发射功率实现双向通信。这样，由多个小区构成的通信系统的总容量将大大提高。由若干小区构成的覆盖区叫做区群。由于区群的结构酷似蜂窝，因此将小区制移动通信系统叫做蜂窝移动通信系统。

在无线通信环境中的电磁波覆盖区内，如何建立用户的无线信道的连接就是多址连接问题，解决多址接入的方法称为多址接入技术。在蜂窝移动通信系统中，多址接入方法主要有 3 种：频分多址接入 FDMA、时分多址接入 TDMA 和码分多址接入 CDMA，其技术核心是多路复用。

4）卫星通信。卫星通信是指利用人造卫星进行中转的通信方式。卫星通信系统是通过卫星微波形成的点到点通信线路，是由两个地球站（发送站、接收站）与一颗通信卫星组成的。地面发送站使用上行链路向通信卫星发射微波信号。卫星起到一个中继器的作用，它接收通过上行链路发送来的微波信号，经过放大后使用下行链路发送回地面接收站。

卫星通信系统也是微波通信的一种，只不过其中继站设在卫星上。卫星通信可以克服地面微波通信距离的限制。一个同步卫星可以覆盖地球的三分之一表面，三个这样的卫星就可以覆盖地球上全部通信区域，实现地球上的各个地面站之间的互相通信。卫星通信优点是容量大、距离远，具有广播能力、多站可以同时接收一组信息，但是存在传输延迟。

5）红外通信。红外（Infrared）通信是指利用红外线进行的通信。红外线的方向性很强，不易受电磁波干扰。在视野范围内的两个互相对准的红外线收发器之间通过将电信号调制成非相干红外线而形成通信链路，可以准确地进行数据通信。红外通信无须申请频率，被广泛应用于短距离的通信，如电视机、空调的遥控器。

4.1.2 局域网技术

1. 局域网概述

局域网是将有限的地理范围内的各种数据通信设备连接在一起，实现数据传输和资源共享的计算机网络。连到局域网的数据通信设备必须加上高层协议和网络软件才能组成计算机网络。

（1）局域网的特点。

1）覆盖范围小。局域网中各节点分布的地理范围较小，通常在几米到几十千米之间，如一个学校、企事业单位。

2）传输速率高。由于通信线路较短，故可选用高性能的介质做通信线路，使线路有较宽的频带，提高了通信速率。共享式局域网的传输速率通常为 1～100Mb/s，交换式局域网技术的传输速率为 10～100Mb/s，目前已达到 1Gb/s。

3）传输延时小。一般在几毫秒到几十毫秒之间。

4）误码率低，可靠性高。局域网通信线路短，出现差错的机会少，噪声和其他干扰因素影响小，局域网的误码率可达 10^{-8}～10^{-11}。

5）介质适应性强。在局域网中可采用价格低廉的双绞线、同轴电缆或价格昂贵的光纤，也可采用微波信道。

6）结构简单，成本低，易于实现。

（2）局域网的基本组成。建立局域网时，必须将计算机与网络设备连接起来，根据不同的局域网连网技术，使用的网络设备不尽相同。局域网包括网络硬件和网络软件两大部分，网络硬件用于实现局域网的物理连接，为连接在局域网上的各计算机之间的通信提供一条物理通道，网络

软件用来控制并具体实现通信双方的信息传递和网络资源的分配与共享。

网络硬件由计算机系统和通信系统组成，局域网硬件主要包括网络服务器、网络工作站、网络接口卡、网络设备、传输介质及介质连接部件，以及各种适配器等。网络软件分为网络系统软件和网络应用软件。网络系统软件主要包括网络操作系统（NOS）、网络协议软件和网络通信软件等。常用的网络操作系统有 Windows NT、Windows 2000 Server、Unix 和 Netware，网络协议软件有 TCP/IP 和 SPX/IPX，通信软件有各种类型的网卡驱动程序等。常用的网络应用软件有网络管理监控程序、网络安全软件、分布式数据库、管理信息系统、Internet 信息服务、远程教学等。图 4-11 所示为局域网基本组成示意图。

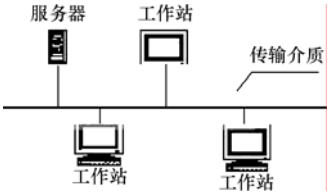

图 4-11　局域网基本组成示意图

2. 局域网介质访问控制方式

局域网介质访问控制是局域网的基本任务，对局域网体系结构、工作过程和网络性能产生决定性的影响。局域网介质访问控制方式主要解决介质使用权问题，实现对网络传输信道的合理分配，用于确定网络节点将数据发送到介质上去的时刻和解决如何对公用传输介质访问和利用并加以控制。传统的局域网介质访问控制方式有三种：带有冲突碰撞检测的载波监听多路访问（CSMA/CD）、令牌环（Token Ring）、令牌总线（Token Bus）。

（1）载波监听多路访问/冲突检测（CSMA/CD）。CSMA/CD（Carrier Sense Multiple Access with Collision Detection）是一种适用于总线结构的分布式介质访问控制方法，CSMA/CD 发送时的工作过程分为载波监听总线和总线冲突检测两部分。

1）载波监听总线，即先听后发。使用 CSMA/CD 方式时，总线上各节点都在监听总线，即检测总线上是否有别的节点发送数据。如果发现总线空闲，没有检测到有信号正在传送，则可立即发送数据。如果监听到总线忙，即检测到总线上有数据正在传送，这时节点要持续等待直到监听到总线空闲时才能将数据发送出去，或等待一个随机时间，再重新监听总线，一直到总线空闲再发送数据。

2）总线冲突检测，即边发边听。当两个或两个以上节点同时监听到总线空闲，开始发送数据时，会发会碰撞，产生冲突。另外，传输延迟可能会使第一个节点发送的数据未到达目的节点，另一个要发送数据的节点就已监听到总线空闲，并开始发送数据，这也会导致冲突的产生。发生冲突时，两个传输的数据都会被破坏，使数据无法到达正确的目的节点。为确保数据的正确传输，每一节点在发送数据时要边发送边检测冲突。当检测到总线上发生冲突时，就立即取消传输数据，随后发送一个短的干扰信号，以加强冲突信号，保证网络上所有节点都知道总线上已经发生了。在阻塞信号发送后，等待一个随机时间，然后再将要发送的数据发送一次。如果还有冲突发生，则重复监听、等待和重传的操作。图 4-12 显示了采用 CSMA/CD 方法的流程图。

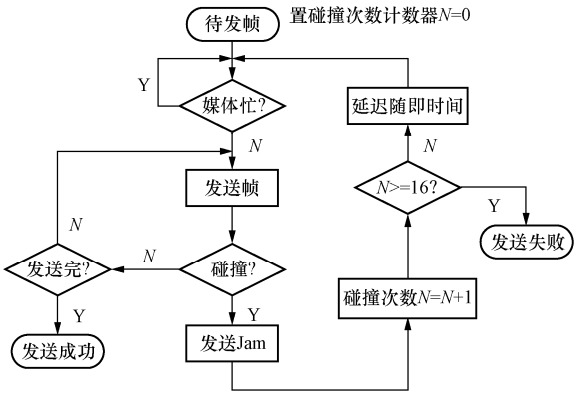

图 4-12　CSMA/CD 流程图

CSMA/CD 是一种争用协议，采用用户访问总线时间不确定的随机竞争总线的方法，每一节点处于平等地位去传输介质，算法较简单，技术上易实现。但它不能提供优先级控制，即不能提供急需数据的优先处理能力。

此外，不确定的等待时间和延迟难以满足远程控制所需要的确定延时和绝对可靠性的要求。为克服 CSMA/CD 的不足，产生了许多 CSMA/CD 的改进方式，如带优先权的 CSMA/CD。CSMA/CD 适用于办公自动化等对数据传输实时性要求不严格和通信负荷较轻的应用环境中。

（2）令牌环访问控制（Token-Ring）。令牌环访问控制是流行的环形网络访问技术，该技术的基础是令牌。令牌是一种特殊的帧，用于控制网络节点的发送权，只有持有令牌的节点才能发送数据。由于只有一个令牌，一次只能有一个站点发送，发送节点在获得发送权后就将令牌删除，在环路上不会再有令牌出现，其他节点也不可能再得到令牌，保证环路上某一时刻只有一个节点发送数据，令牌环技术不存在争用现象，它是一种无争用型介质访问控制方式。

当令牌环正常工作时，令牌总是沿着物理环路单向逐节点传送，传送顺序与节点在环路中的排列顺序相同。当某一个节点要发送数据时，必须等待空闲令牌的到来。它获得空令牌后，将令牌置“忙”，并以帧为单位发送数据。如果下一节点是目的节点，则将帧复制到接收缓冲区，在帧中标志出帧已被正确接收和复制，同时将帧送回环上，否则只是简单地将帧送回环上。帧绕行一周后到达源节点后，源节点回收已发送的帧，并将令牌置“闲”状态，再将令牌向下一个节点传送。图 4-13 给出了令牌环的基本工作过程。

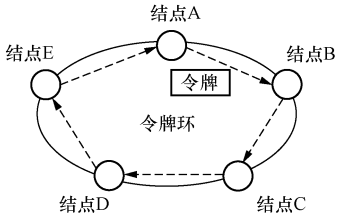

图 4-13　令牌环的工作过程

当令牌在环路上绕行时，可能会产生令牌的丢失，此时，应在环路中插入一个空令牌。令牌的丢失将降低环路的利用率，而令牌的重复也会破坏网络的正常运行，因此必须设置一个监控节点，以保证环路中只有一个令牌绕行。当令牌丢失，则插入一个空闲令牌。当令牌重复时，则删除多余的令牌。

令牌环的主要优点在于其访问方式具有可调整性和确定性，每个节点具有同等的介质访问权，还提供优先权服务，具有很强的适用性。其主要缺点是令牌环维护复杂，实现较困难。

（3）令牌总线访问控制（Token-Bus）。令牌总线访问控制综合了 CSMA/CD 与令牌环两种介质访问方式的特点。图 4-14 给出了令牌总线的工作过程。令牌总线主要适用于总线型或树型网络。采用此种方式时，各节点共享的传输介质是总线型的，每一节点都有一个本站地址，并知道上一个节点地址和下一个节点地址，令牌传递规定由高地址向低地址，最后由最低地址向最高地址依次循环传递，从而在一个物理总线上形成一个逻辑环。环中令牌传递顺序与节点在总线上的物理位置无关。

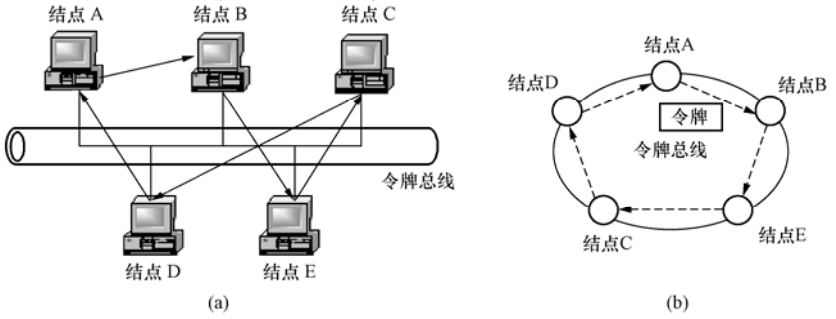

图 4-14　令牌总线的工作过程

（a）令牌总线物理结构；（b）令牌总线逻辑结构

与令牌环一致，令牌总线只有获得令牌的节点才能发送数据。在正常工作时，当节点完成数据帧的发送后，将令牌传送给下一个节点。从逻辑上看，令牌是按地址的递减顺序传给下一个节

点的，从物理上看，带有地址字段的令牌帧广播到总线上的所有节点，只有节点地址和令牌帧的目的地址相符的节点才有权获得令牌。

获得令牌的节点，如果有数据要发送，则可立即传送数据帧，完成发送后再将令牌传送给下一个节点；如果没有数据要发送，则应立即将令牌传送给下一个节点。由于总线上每一节点接收令牌的过程是按顺序依次进行的，因此所有节点都有访问权。为了使节点等待令牌的时间是确定的，需要限制每一节点发送数据帧的最大长度。令牌总线还提供了不同的优先级机制。优先级机制的功能是将待发送的帧分成不同的访问类别，赋予不同的优先级，并把网络带宽分配给优先级较高的帧，而当有足够的带宽时，才发送优先级较低的帧。

令牌总线具有确定性、可调整性及较好的吞吐能力特点，适用于对数据传输实时性要求较高或通信负荷较重的应用环境中，如生产过程控制领域。但是令牌总线相对复杂、时间开销较大，节点可能要等待多次无效的令牌传送后才能获得令牌。

3. 局域网参考模型和 IEEE 802 标准

（1）局域网参考模型。国际上通用的局域网标准由 IEEE 802 委员会制定。IEEE 802 委员会根据局域网适用的传输媒体、网络拓扑结构、性能及实现难易等因素，为局域网制定了一系列标准，称为 IEEE 802 标准，已被 ISO 采纳为国际标准。局域网的体系结构一般仅包含 OSI 参考模型的最低两层：物理层和数据链路层，如图 4-15 所示。

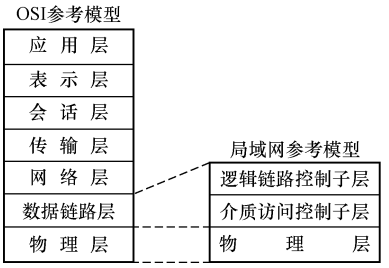

图 4-15　局域网参考模型

1）物理层。物理层用来建立物理连接，确保通信信道的正确传输。物理层要实现电气、机械、功能和规程特性的匹配，提供的发送和接收信号的能力，包括对宽带的频带分配和对基带信号的调制。

2）数据链路层。数据链路层负责把数据从一个节点可靠地传输到相邻的节点。数据链路层把数据转换成帧来传输，并实现帧的顺序控制、差错控制及流量控制等功能，使不可靠的链路变成可靠的链路，数据链路层分为 MAC 子层和 LLC 子层，使数据链路的功能中与硬件有关和无关的部分分开。

LLC 子层向高层提供一个或多个逻辑接口（具有帧发和帧收功能）。发送时把要发送的数据加上地址和 CRC 检验字段构成帧，介质访问时把帧拆开，执行地址识别和 CRC 校验功能，并具有帧顺序控制和流量控制等功能。LLC 子层还包括某些网络层功能，如虚拟控制和多路复用等。

MAC 子层支持数据链路功能，并为 LLC 子层提供服务。它将上层交下来的数据封装成帧进行发送（接收时将帧拆卸）、实现和维护 MAC 协议、比特差错检验和寻址等。

（2）IEEE 802 标准。IEEE 802 局域网标准委员会为局域网制定了不同的标准，统称为 IEEE 802 标准，适用于不同的网络环境。IEEE 802 部分标准之间的关系如图 4-16 所示。

IEEE 802 标准包括：

1）IEEE 802.1 标准，定义了局域网体系结构、网络互连，以及网络管理和性能测试。

2）IEEE 802.2 标准，定义了逻辑链路控制 LLC 子层功能与服务。

3）IEEE 802.3 标准，定义了 CSMA/CD 总线介质访问控制子层与物理层规范。

4）IEEE 802.4 标准，定义了令牌总线（Token Bus）介质访问控制子层与物理层规范。

5）IEEE 802.5 标准，定义了令牌环（Token Ring）介质访问控制子层与物理层规范。

6）IEEE 802.6 标准，定义了城域网 MAN 介质访问控制子层与物理层规范。

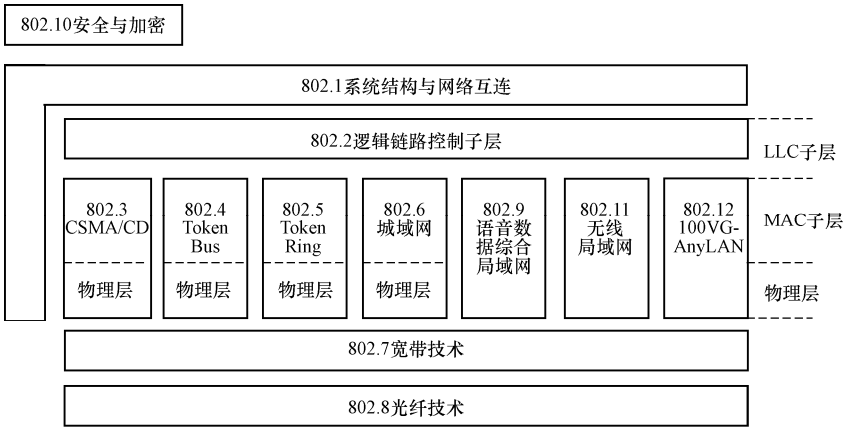

图 4-16　IEEE 802 标准之间的关系

7）IEEE 802.7 标准，定义了宽带网络技术。

8）IEEE 802.8 标准，定义了光纤传输技术。

9）IEEE 802.9 标准，定义了综合语音与数据局域网（IVD LAN）技术。

10）IEEE 802.10 标准，定义了可互操作的局域网安全性规范（SILS）。

11）IEEE 802.11 标准，定义了无线局域网技术。主要包括有：① IEEE 802.11a，工作在 5GHz 频段，传输速率为 54Mb/s 的无线局域网标准；② IEEE 802.11b，工作在 2.4GHz 频段，传输速率为 11Mb/s 的无线局域网标准；③ IEEE 802.11g，工作在 2.4GHz 频段，传输速率为 54Mb/s 的无线局域网标准。

12）IEEE 802.12 标准，定义了优先度要求的访问控制方法。

13）IEEE 802.13 标准，未使用。

14）IEEE 802.14 标准，定义了交互式电视网。

15）IEEE 802.15 标准，定义了无线个人局域网（WPAN）的 MAC 子层和物理层规范。

16）IEEE 802.16 标准，定义了宽带无线访问网络。

17）IEEE 802.17 标准，定义了弹性分组环（RPR）标准。

18）IEEE 802.18 标准，定义了宽带无线局域网标准规范。

4.1.3　企业信息网络

1. 企业信息网概述

企业信息网络简称企业网，是在一个企业范围内将各类测控设备、网络、计算、存储等资源连接在一起，提供企业内的通信和信息共享以及企业外部的信息访问，用于经营、管理、调度、监测与控制的全局通信网络，提供面向客户的企业信息查询及信息交流等功能的计算机网络。

早期的企业网主要用于信息系统和办公自动化系统，以信息管理和服务为主，生产过程的检测和控制基本上独立于企业信息网之外。现场总线技术的发展实现了生产过程现场级设备之间以及车间级设备之间的联系，使得测量与控制成为企业信息网的一个组成部分，将信息网络与自动化控制网络融为一体，实现上层管理与底层控制的信息直接联系，形成了一体化的工业企业网。信息网络处于企业中上层，用于处理企业管理、高层次调度与决策信息，处理的信息量大、多样且多变，具有高速、综合的特征。控制网络处理企业现场实时测控信息，处于企业中下层，处理实时的、现场的信息，具有协议简单、容错性强、安全可靠、成本低廉等特征。

美国著名的 IT 分析公司 GartnerGroup 根据企业发展和企业对供应链管理的需求提出了企业

资源规划 ERP 的概念。ERP 将供应商和企业内部的采购、生产、销售以及客户紧密联系起来，集成了企业内部的其他管理功能，如人力资源、质量管理、决策支持等，可对供应链上的所有环节进行有效管理，并支持 Internet、企业信息网和电子商务 E-Business 等，实现对企业的动态控制以及多种资源的集成与优化，达到企业资源合理、高效利用的目的。

ERP 系统涉及复杂的软件技术和网络技术，企业在建立 ERP 系统时，既要根据经济现状、企业内外部环境和自身经营状况，选择合适的 ERP 模式，同时又要考虑企业网建设。企业信息网的设计是以实现企业建设和发展的战略目标为原则。企业网作为 ERP 的主要支撑系统，其设计、规划与实现应当反映企业现代化、信息化的发展方向。控制网络的应用能为 ERP 的实施提供来自企业底层的实时信息和生产过程的状态数据，为企业实现 ERP 战略奠定了基础。

2. 企业网网络结构

（1）Intranet、Extranet 与 Internet。企业网常用的网络有 Intranet、Extranet、Internet 三种结构，企业应根据各自信息化的不同需要而有针对性地进行选择实施。Extranet、Intranet、Internet 的关系示意如图 4-17 所示。

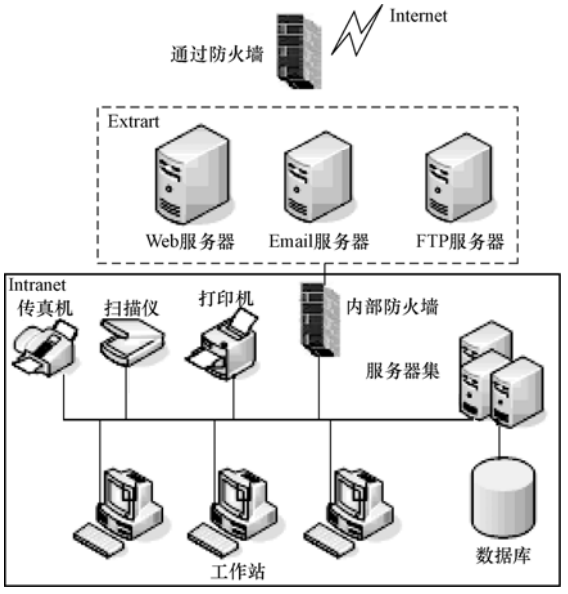

图 4-17　Intranet、Extranet、Internet 关系示意图

1）Internet。Internet 是一个计算机交互网络，也称因特网或国际互联网，其前身是 APRANET。因特网是一组全球信息资源的总汇，它由那些使用公用语言互相通信的计算机连接而成的全球网络。Internet 以相互交流信息资源为目的，基于一些共同的协议，并通过许多路由器和公共互联网而成，它是一个信息资源和资源共享的集合。为了保证计算机之间的信息交流，制定了 TCP/IP，使各种不同位置、不同型号的计算机可以在 TCP/IP 的基础上实现信息交流。

2）Intranet。Intranet 是企业内部网或企业内联网，目的是实现企业内部的信息交流和共享，包括获取信息和提供信息，还可与数据库服务器连接，支持企业的决策支持系统。它在企业各部门现有网络上增加一些特定的软件，使企业已有网络连接起来，服务于企业的内部机构和人员，还提供局域网与 Internet 的互连接口，使企业和广阔的外部信息世界连通，获取所需要的信息，促进企业组织结构的优化和管理。

相比 Internet，Intranet 的网络规模有限，管理权限集中，可以有效地进行用户身份鉴别，安全性好，易于配置管理、内部信息管理等。Intranet 可以看成是 Internet、局域网等技术的集成物，可连接到 Internet 上，利用 Internet 提供的丰富信息资源和各种服务。在不需要的情况下，也可以与 Internet 断开，成为相对独立的网络。

通常 Intranet 提供的服务包括：Web 服务、文件传送服务 FTP、远程登录服务 Telnet、电子邮件服务、数据库查询服务、打印共享管理、用户管理、视频会议、视频点播和网络管理等，支持企业内部办公业务的自动化、电子化和网络化管理。

Intranet 的特点：采用基于 Internet 技术和基于 Web 的应用系统，容易集成各种已有信息系统，易与 LAN/WAN 结合；可从传统企业网发展到 Intranet，继续利用原有资源；建设 Intranet 周

期短，规模有伸缩性；采用防火墙等强有力的安全措施，防范来自 Internet 的非法入侵；支持多媒体应用。

3）Extranet。Extranet 是企业外延网或企业外联网，是一种与外部世界有相对隔离的内部网络，Extranet 使用 Internet/Intranet 技术使企业与其客户和其他相关企业相连，完成共同目标的交互式合作网络。

Extranet 是 Intranet 向外部的延伸，用于有关联企业之间的联结和信息沟通，为企业间合作的纽带。服务对象既不限于企业内部的机构和人员，也不像 Internet 那样，完全对外开放服务，而是有选择地扩大到与本企业相关联的供应商、代理商和客户等。

企业往往通过 Internet 等公共互联网络与分支机构或其他公司建立 Extranet，进行安全的通信。需要解决 Intranet 与这些远程节点连接所用的公共传输网的安全、费用和方便性的问题。目前最常用且有效的技术是虚拟专用网 VPN（Virtual Private Network）。

Extranet 的特点：采用 Internet 技术和基于 Web 的应用系统；在保证企业核心数据安全的前提下，扩大对网络的访问范围，让商业伙伴甚至客户访问，制定特定的应用策略，可以让外部用户访问优先权高于内部；设置防火墙确保网络安全。

（2）企业信息网层次结构。企业信息网综合了信息网与控制网络。典型的企业信息网层次结构为三层网络结构，从低到次依次为现场设备层、监控调度层和信息管理层，如图 4-18 所示。

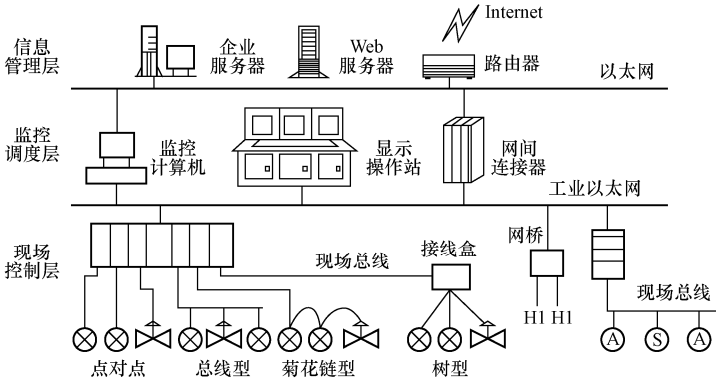

图 4-18　企业信息网层次结构示意图

1）现场控制层。低层的现场控制层，由现场设备和控制网段组成，通过现场总线将智能仪器、控制设备、工控机或者 PLC 设备的远程 I/O 点连接在一起，实现现场级的通信。按照 IEC 标准，现场总线支持多种类型的网络拓扑结构，现场设备以网络节点的形式挂接在现场总线网络上，由带有功能块的现场总线设备完成对生产过程的控制。

在同时使用多种总线时，可在不同网络协议的现场总线之间加入协议转换器（网关），识别并解释不同格式的数据包，在不同的网络之间转发。

2）监控调度层。中间层的监控调度主要用于监控、优化与调度，将 PLC、工控机以及操作员界面连接在一起，在企业信息网络中起到承上启下的作用。在进行企业综合自动化时要充分的重视。

监控调度层由高速以太网以及连接在总线上的担任监控任务的工作站或显示操作站组成，对应车间级通信。现场控制层通过现场总线接口与监控层相连，监控站可以完成对控制系统的组态设计和下载，执行对现场控制系统的监视、操作、趋势分析、报警、维护及各种人机交互功能。

此外，监控层还为实现先进控制和过程操作优化提供支撑环境。

3）信息管理层。上层的信息管理层是企业信息管理层，主要用于企业的计划、销售、库存、财务、人事及企业的经营、管理及决策等。

信息管理层网络由各种服务器和客户机组成，对应整个企业的管理。其主要目的是在分布式网络环境下，集成企业的各种信息，实现与 Internet 的连接。首先要将监控层实时数据库中的信息转入上层的关系数据库中，管理层用户能随时查询网络运行状态以及现场设备工况，对生产过程进行实时远程监控。赋予一定权限后，还可以在线修改各种设备参数和运行参数，从而在企业网范围内实现底层测控信息的实时传递。

3. 企业网互连与设备

（1）企业网互连。网络互连是通过相应的技术将分布在不同地理位置的网络或网络与远程工作站之间进行物理和逻辑上的连接，以组成更大规模的计算机网络系统，实现更大范围的资源的高度共享和文件传输。

企业网络一般包括处理企业管理与决策信息的信息网络和处理企业现场实时测控信息的控制网络两部分。控制网络和信息网络融合是为了实现网络间的信息与资源的共享，将底层的实时信息传送到信息网络，为企业的管理决策提供重要的信息。控制网络与信息网络的集成技术主要有：

1）互联技术。一般来说控制网络与信息网络是两类具有不同功能、不同结构和不同形式的网络。通常采用网关和路由器实现网络互联，网络的扩展采用网桥和中继器实现。通常采用的网络扩展方法有网桥和中继器。Web 技术在控制网络与信息网络的互联中已得到实际控制网络与信息网络集成的远程通信技术。

2）远程通信技术。当控制网络与信息网络地理上相距较远时，远程通信技术是实现网络集成的有效方法之一。远程通信技术有利用调制解调器的远程通信、基于 TCP/IP 的远程通信。

3）动态数据交换技术。当控制网络与信息网络有一共享工作站或通信处理机时，可通过动态数据交换技术实现控制网络中实时的数据与信息网络中数据库数据的动态交换，从而实现控制网络与信息网络的集成。

4）数据库访问技术。信息网络一般采用开放的数据库系统，通过数据库访问技术可实现控制网络与信息网络的集成。信息网络的浏览器接入控制网络，基于 Web 技术，通过浏览器可与信息网络数据库进行动态的、交互式的信息交换，实现控制网络与信息网络的集成。

控制网络与信息网络集成的最终目标是实现管理与控制一体化的、统一的、集成的企业网络，为企业实现高效益、高效率、高柔性提供强有力的支持。相比其他控制网络而言，工业以太网在与信息网络集成方面具有得天独厚的优势。

（2）网络互连设备。

1）中继器（Repeater）。中继器是工作于 OSI 物理层的网络连接设备，要求每个网络在数据链路层以上具有相同的协议。由于所使用的传输介质的限制，信号传输到一定距离后因衰减导致接收设备无法识别该信号，使用中继器可扩大网上的所有信号，并将其放大、再生发送，从而扩展网络信号的传输距离。中继器虽然延伸了网络，但从网络层看仍然是一个网络，常被看成是网段的连接设备而不是网络互连设备。

2）网桥（Bridge）。网桥又被称为桥接器，工作在 OSI 参考模型的数据链路层，要求每个网络在网络层以上各层中采用相同或兼容协议。网桥一般用于互连两个运行同类型的 LAN，而网络的拓扑结构、通信介质和通信协议可以不同。

网桥以接收、存储、地址过滤与转发的方式实现两个互连网络之间的通信，并实现大范围局

域网的互连。网桥可以分隔两个网络之间的通信量，有利于改善互连网络的性能。若是同网络内的信息传递，则网桥不进行复制和转发，否则转发。当两个 LAN 之间采用两个或两个以上的网桥互连时，由于网桥转发广播数据包，易产生广播风暴。

3）交换机（Switch）。交换机是一种用于电信号转发的网络设备，属于数据链路层，还能够解析出 MAC 地址信息。交换机的所有端口都共享同一指定的带宽，这种方式比网桥的性价比要高。交换机的每一个端口都扮演一个网桥的角色，交换机可以把每一个共享信道分成几个信道。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。

4）路由器（Router）。路由器是一种能连通不同的网络或网段的互连设备，工作在 OSI 模型的网络层。通常用来互连局域网和广域网，是目前用来构建 Internet 骨干网的核心互连设备。

路由器的功能主要包括网络互连、数据处理与网络管理。路由器支持各种局域网和广域网接口，主要用于互连局域网和广域网，实现不同类型网络互相通信。在数据处理上，提供数据包的过滤、数据包的寻址和转发、优先级、复用、加密、压缩和防火墙等功能。在网络管理上，路由器提供包括配置管理、性能管理、容错管理和流量控制等功能。

5）网关（Gateway）。网关又称网间协议变换器，用于连接采用不同通信协议的网络，实现网络间的数据传输的网络互连设备。交换机、网桥和路由器主要用于网络层以下有差异的子网的互连，互连后的网络仍然属于通信子网的范畴。采用网桥或者路由器连接两个或者两个以上的网络时，都要求互相通信的用户节点具有相同的高层通信协议。如果两个网络完全遵循不同的体系结构，则无论是网桥还是路由器都无法保证不同网络的用户之间的有效通信。

网关是传输层及其以上层次的互连设备。执行网络层以上高层协议的转换，或者实现不同体系结构的网络协议转换的互连，主要用于不同体系结构网络的互连。

4.2 现场总线技术

4.2.1 现场总线概述

1. 现场总线标准

现场总线是一种工业数据总线，是自动化领域中底层数据通信网络。随着网络技术的发展和市场需求的变化，工业设备实现网络化管理控制已经成为一种必然趋势，满足改善工业测控系统需要，在不同生产设备之间实现高效、可靠、标准化的互连。国际电工委员会（International Electrotechnical Commission，IEC）制定的国际标准 IEC 61158 对现场总线的定义是：安装在制造或过程区域的现场装置与控制室内的自动控制装置之间的数字式、串行、多点通信的数据总线称为现场总线。

2000 年 1 月 IEC TC65（负责工业测量和控制的第 65 标准化技术委员会）通过了 8 种类型的现场总线作为新的 IEC 61158 国际标准，分别是：type1 IEC 技术报告（即 FF 的 H1）；type2 ControlNet（美国 Rockwell 公司支持）；type3 Profibus（德国 Siemens 公司支持）；type4 P-Net（丹麦 Process Data 公司支持）；type5 FF HSE（即原 FF 的 H2，Fisher-Rosemount 等公司支持）；type6 Swift Net（美国波音公司支持）；type7 World FIP（法国 Alstom 公司支持）；type8 Interbus（德国 Phoenix Conact 公司支持）。

为了进一步完善 IEC 61158 标准，IEC/SC65C 成立了 MT9 现场总线修订小组，继续这方面的工作。MT9 工作组在原来 8 种类型现场总线的基础上不断完善扩充，于 2001 年 8 月制定出

由 10 种类型现场总线组成的第三版现场总线标准，分别是：Type1 TS61158 现场总线、Type2 ControlNet 和 Ethernet/IP 现场总线、Type3 Profibus 现场总线、Type4 P-NET 现场总线、Type5 FF HSE 现场总线、Type6 Swift-Net 现场总线、Type7 WorldFIP 现场总线、Type8 INTERBUS 现场总线、Type9 FF H1 现场总线和 Type10 PROFInet 现场总线，该标准于 2003 年 4 月成为正式国际标准。

加上 IEC TC17B（负责低压开关设备和控制设备）通过的 3 种现场总线国际标准，即 SDS（Smart Distributed System）、ASI（Actuator Sensor Interface）和 DeviceNet，ISO 还有一个 ISO 11898 的 CAN（Control Area Network），现场总线标准有 12 种之多。此外，一些国家还有其国家的标准，如英国的 ERA、挪威的 FINT 等，一些国际著名公司也推出自己的标准，如三菱公司的 CC-Link、施耐德公司的 Modbus 等。

2. 现场总线技术特征

（1）现场设备已成为以微处理器为核心的数字化设备，彼此通过传输媒体（双绞线、同轴电缆或光纤）相连。

（2）网络数据通信采用基带传输，数据传输速率高，实时性好，抗干扰能力强。

（3）废弃了集散控制系统 DCS 中的 I/O 控制站，将这一级功能分配给通信网络完成。

（4）分散的功能模块，便于系统维护、管理与扩展，提高了可靠性。

（5）开放式互连结构，既可与同层网络相连，也可通过网络互连设备与控制级网络或管理信息级网络相连。

（6）互操作性，在遵守同一通信协议的前提下，可将不同厂家的现场设备产品统一组态，构成所需要的网络。

3. 现场总线通信模型

现场总线的体系结构基本遵照 ISO/OSI 参考模型建立，主要使用了 ISO/OSI 七层参考模型的三层，即物理层、数据链路层、应用层，由于现场总线通常只包括一个网段，因此不需要 3～6 层，即省去了 ISO/OSI 参考模型中的网络层、传输层、会话层与表示层。不过它又在原有 ISO/OSI 参考模型第 7 层之上增加了用户层，可将通信模型视为四层。

（1）物理层。IEC61158 规定了数据的物理信号表达形式、传输媒体、传输速率，以及可使用的网络拓扑结构等。为了满足工业通信要求，IEC 提出高速总线接口标准，使其传输速率分别 Mb/s 级，典型的响应时间可达 32μs，总线段最大长度缩短为 750m，能够连接 127 个现场设备，目前，高速总线标准正在向高速以太网标准倾斜。

（2）数据链路层。现场总线的实时通信主要由数据链路层提供。数据链路层规定如何在设备之间共享网络和进行调度通信；为了满足实时性要求，IEC 61158 数据链路层标准中采用了不同于 IEEE 802 标准的全新的数据链路层服务定义和数据链路层规范。现场总线在其媒体访问控制协议中充分利用了令牌传送的灵活性和调度访问的实时性，数据传输具有很高的确定性。另外，IEC 数据链路层还可以为实体间数据交换提供连接服务和无连接服务。

现场总线的数据链路层与 ISO/OSI 参考模型的数据链路层在功能上相类似，都涉及帧在节点之间的传输问题，但现场总线的帧传输不涉及中间交换节点，信道是共享的，不同于传统的链路，现场总线的链路支持多重访问，支持成组地址与广播式的帧传输，支持媒体访问控制子层的链路访问控制功能；提供某些网络层功能。

LLC 子层向高层提供一个或多个逻辑接口或称为服务访问点（Service Access Point，SAP），负责控制节点间帧的发送和接收，同时检验传输差错。发送时把要发送的数据加上地址和 CRC 字段等构成帧。接收时，把帧拆开，执行地址识别和 CRC 检验功能，并具有帧顺序以及差错控

制等功能。这一层还包括某种网络层功能，如虚电路、多路复用等。

MAC 子层主要实现对共享总线媒体的交通管理，并检测传输线路的异常情况。IEC 为现场总线设定了三种媒体访问控制方式：令牌传送、立即响应和授权令牌。令牌传送方式中，一个节点必须持有令牌才能使用总线，完成信息传输后，立即将令牌交还给链路活动调度器（Link Active Scheduler，LAS），LAS 则根据预先的组态或调度算法将令牌交给下一个令牌申请者。立即响应，即主节点给某个节点一个机会来应答一次信息。授权令牌方式是指一个节点在做出应答时，若加了一个申请令牌的代码，LAS 侦听到这一申请后，如果调度时间允许，即把令牌授权给这个申请节点。

在数据链路层，LAS 是一条总线段的调度中心，拥有总线段上所有设备的清单及链路活动调度表。总线段上的设备只有得到 LAS 许可，才能向总线上传输数据。LAS 是有效利用总线，并进行报文实时传输的保证。

（3）应用层。应用层则规定了在设备间交换数据、命令、事件信息以及请求应答中的信息格式，为用户层提供访问现场总线通信环境的手段。应用层分为总线报文规范子层（FMS）和总线访问子层（FAS）两个子层。总线报文规范子层针对分布式测控系统的构成、运行和改变，提供对象字典服务、变量访问服务和事件服务；总线访问子层则针对 FMS、功能块、应用管理和系统管理，提供发布/预订接收者、客户/服务器和报告分发三种服务。

IEC 现场总线网络中，设备之间的信息传递是通过预先组态好的通信通道进行的。这种现场设备应用进程之间的通信通道，是一种逻辑上的连接，或者可以看做一种软连接，IEC 将这种在现场总线网络的各应用进程之间的通信通道称为虚拟通信关系（Virtual Communication Relationship，VCR）。

（4）用户层。用户层用于组成用户所需要的应用程序，如规定标准的功能块、设备描述，实现网络管理、系统管理。现场总线系统可以看做协同工作的应用进程（AP）的集合，IEC 把实现控制系统所需要的各种功能划分为功能模块，使其公共特征标准化，规定它们各自的输入、输出、算法、事件、参数与块控制图，并把它们组成为可在某个现场设备中执行的功能块应用进程（FBAP），便于实现不同制造商产品的混合组态与调用。功能块应用进程能够使用应用层接口访问应用层通信实体，IEC 规定通过这个接口既可以单独访问 FMS 子层或 FAS 子层，也可以同时访问两者。功能块的通用结构是实现开放结构框架的基础，也是实现各种网络功能与自动化功能的基础。

4.2.2 几种流行的现场总线

1. Profibus 总线

（1）Profibus 概述。Profibus（Process Fieldbus）是国际化、开放、不依赖于生产商的现场总线标准。广泛用于制造业、过程自动化和楼宇、交通、电力等其他自动化领域。Profibus 技术的发展经历为：1987 年，德国 SIEMENS 等 18 家企业和研究机构联合开发；1989 年，德国工业标准 DIN19245；1996 年，欧洲标准 EN50170V.2（PROFIBUS-FMS-DP）；1998 年，PROFIBUS-PA 被纳入 EN50170V.2；1999 年，国际标准 IEC 61158 的组成部分（TYPE3）；2001 年，中国的机械行业标准 JB/T 10308-3-2001。

Profibus 由三个兼容部分组成，即 Profibus－DP（Decentralized Periphery）分散外围设备、Profibus—PA（Process Automation）过程自动化、Profibus-FMS（Fieldbus Message Specification）现场总线报文规范。

Profibus—DP 用于分散外设间的高速传输，主要用于加工自动化领域的应用。传输速率可达 12Mb/s，一般构成单主站系统，主站、从站间采用循环数据传送方式工作。

Profibus—PA 用于安全性要求较高的场合，它具有本质安全特性，是 Profibus 的过程自动化解决方案，将自动化系统和过程控制系统与现场设备，如压力、温度和液位变送器等连接起来，代替了 4～20mA 模拟信号传输技术。

Profibus-FMS 用于车间和厂级智能主站间通用的通信，它提供了大量的通信服务，用以完成以中等传输速度进行的循环和非循环的通信任务。主要考虑系统功能而非响应时间，通常要求随机信息交换（如改变设定参数等）。可用于大范围和复杂的通信系统。

（2）Profibus 网络结构。一个典型的工厂自动化系统采用三级网络结构。基于现场总线 Profibus—DP/PA 控制系统位于工厂自动化系统中的底层，即现场级与车间级。现场总线 Profibus 是面向现场级与车间级的数字化通信网络，结构如图 4-19 所示。

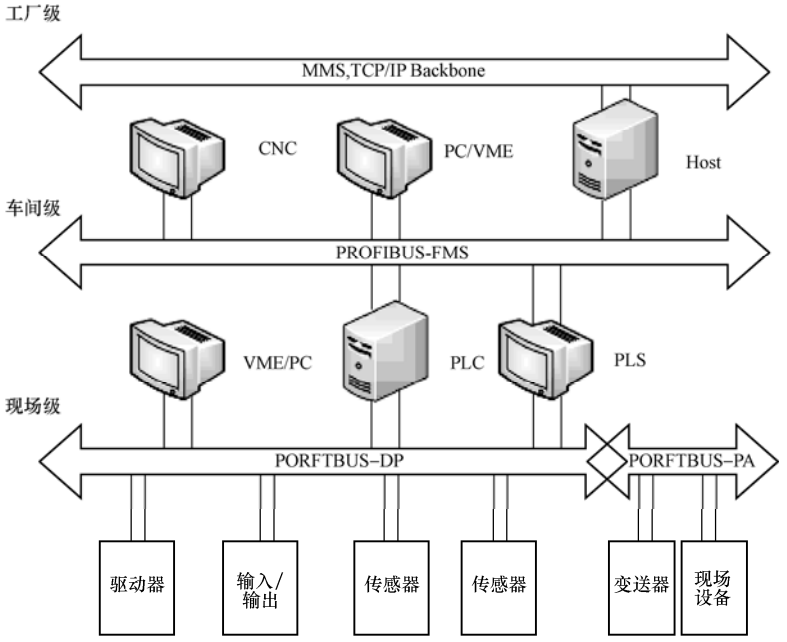

图 4-19　Profibus 网络结构

现场控制级由现场智能设备、现场智能仪表、远程 I/O 和网络设备构成，完成现场设备控制及设备间连锁控制。主站（PLC、PC 机或其他控制器）负责总线通信管理及所有从站的通信。现场控制涉及 Profibus 协议 Profibus—DP 和 Profibus—PA 两个部分。

车间监控级由执行监控任务的工作站或显示操作站、工程师站、控制器组成。用来完成车间生产设备之间的连接，完成生产设备状态在线监控、设备故障报警及维护等。还具有生产统计、生产调度等车间级生产管理功能。车间级监控网络可采用 Profibus—FMS，它是一个多主网，这一级数据传输速度不是最重要的，而是要能够传送大容量信息。

工厂管理级由各种服务器和客户机组成，主要由 SIS、MIS 和 ERP 系统构成。车间操作员工作站可通过交换机与车间办公管理网连接，将车间生产数据送到车间管理层。车间管理网作为工厂主网的一个子网。子网通过交换机、网桥或路由等连接到厂区骨干网，将车间数据集成到工厂管理层。

（3）Profibus 通信模型。Profibus 协议结构是根据 ISO7498 国际标准，以开放式系统互联网络作为参考模型。Profibus 协议结构如图 4-20 所示。Profibus 采用 OSI 的 1、2、7 层（FMS），即

物理层、数据链路层和应用层。

<table>
<tr><td rowspan="3">用户层</td><td>DP设备行规</td><td rowspan="2">FMS设备行规</td><td>PA设备行规</td></tr>
<tr><td>基本功能
扩展功能</td><td>基本功能
扩展功能</td></tr>
<tr><td>DP用户接口
直接数据链路映象程序
（DDLM）</td><td>应用层接口
（ALI）</td><td>DP用户接口
直接数据链路映象程序
（DDLM）</td></tr>
<tr><td rowspan="2">第7层
（应用层）</td><td rowspan="2">未使用</td><td>应用层
现场总线报文规范（FMS）</td><td rowspan="2">未使用</td></tr>
<tr><td>低层接口（LLI）</td></tr>
<tr><td>第3～6层</td><td colspan="3"></td></tr>
<tr><td>第2层
（数据链路层）</td><td>数据链路层
现场总线数据链路（FDL）</td><td>数据链路层
现场总线数据链路（FDL）</td><td>IEC接口</td></tr>
<tr><td>第1层
（物理层）</td><td>物理层
（RS485/光纤）</td><td>物理层
（RS485/光纤）</td><td>IEC61158-2</td></tr>
</table>

图 4-20　Profibus 协议结构

1）物理层。Profibus—DP 和 Profibus—FMS 的 RS485 传输采用屏蔽双绞铜线，传输速率为 9.6kb/s～12Mb/s，每分段不带中继可有 32 个站，带中继可多到 127 个站。Profibus—PA 的 IEC1158-2 传输支持本征安全和总线供电，IEC 1158-2 采用两线技术进行供电和数据传输。光纤传输采用专用总线插头转换 RS-485 信号和光纤信号。

2）数据链路层。数据链路层规定总线存取控制、数据安全性以及传输协议和报文的处理。在 Profibus 中，数据链路层称为 FDL 层。

3）应用层。Profibus 的应用层由 FMS 接口（现场总线报文规范）和 LLI 接口（低层接口）组成。在不同的应用中，功能范围必须与具体应用相适应，这些适应性定义称为行规。行规提供了设备的可互换性，保证不同厂商生产的设备具有相同的通信功能。

Profibus—DP 物理层与 ISO/OSI 参考模型的第一层相同，采用 EIA—RS485 协议，根据数据传输速率的不同，可选用双绞线和光纤两种传输媒体。

Profibus—DP 数据链路层协议媒体访问控制采用受控访问的令牌总线（Token Bus）和主从方式。其中令牌总线与局域网 IEEE 802.4 协议一致，令牌在总线上的各主站间传递，持有令牌的主站获得总线控制权，该主站依照关系表与从站或与其他主站进行通信。主从方式的数据链路协议与局域网标准不同，它符合 HDLC 中的非平衡正常响应模式（NRM）。该模式的工作特点是：总线上一个主站控制着多个从站，主站与每一个从站建立一条逻辑链路，主站发出命令，从站给出响应；从站可以连续发送多个帧，直到无信息发送、达到发送数量或被主站停止为止。

Profibus—FMS 定义了第一、二、七层，应用层包括现场总线信息规范和低层接口。FMS 包括了应用协议并向用户提供了可广泛选用的通信服务。协调不同的通信关系并提供不依赖设备的第二层访问接口。

Profibus—PA 的数据传输采用扩展的 Profibus—DP 协议。传输技术遵从 IEC 1158-2 标准，可实现总线供电与本质安全防爆。PA 还描述了现场设备行为的 PA 行规。根据 IEC 1158-2 标准，PA 的传输技术可确保其安全性，而且可通过总线给现场设备供电。使用连接器可在 DP 上扩展 PA 网络。

Profibus 的 DP、FMS、PA 的数据链路层相同，支持主-从系统、纯主站系统、多主多从混合系统等传输方式。主站之间采用令牌传送方式，主站与从站之间采用主从传送方式。

2. CAN 总线技术

（1）CAN 总线概述。

1）CAN 总线技术特点。CAN（Controller Area Network）即控制器局域网络，是国际上应用最广泛的现场总线之一，是 ISO 国际标准化的串行通信协议，它是一种有效支持分布式控制或实时控制的串行通信网络。1986 年德国 Bosch 公司推出面向汽车的 CAN 通信协议，用于汽车内部测量与执行部件之间的数据通信。此后，CAN 通过 ISO11898 及 ISO11519 进行了标准化，成为汽车网络的标准协议。世界上一些著名的汽车制造厂商，如奔驰（Benz）、宝马（BMW）、大众（Volkswagen）等都采用了 CAN 总线，实现汽车内部控制系统与各检测和执行机构间的数据通信。

最初，CAN 被设计作为汽车环境中的微控制器通信，在车载各电子控制装置 ECU 之间交换信息，形成汽车电子控制网络。比如：发动机管理系统、变速箱控制器、仪表装备、电子主干系统中，均嵌入 CAN 控制装置。CAN 总线的数据通信具有突出的可靠性、实时性和灵活性，其应用范围已不再局限于汽车行业，已经被广泛应用在航空航天、航海、过程工业、机械工业、纺织机械、农用机械、机器人、数控机床、医疗器械及传感器等领域。

CAN 总线具有以下主要技术特性：

- CAN 遵从 ISO/OSI 模型，采用了其中的物理层、数据链路层与应用层。采用双绞线，通信传输速率最高达到 1Mb/s，直接传输距离最远可达 10km（5kb/s），最多可挂接 110 个设备。
- CAN 的信号传输采用短帧结构，每一帧有效字节数为 8 个。因而传输时间短，受干扰的概率低。当节点发生严重错误时，具有自动关闭的功能，切断该节点与总线的联系，使总线上其他节点不受影响，具有很强的抗干扰能力。
- CAN 支持多主工作方式，网络上任一节点均可在任何时候主动向其他节点发送信息，支持点对点，一点对多点和全局广播方式接收/发送数据，而优先级低的节点则主动停止发送，从而避免了总线冲突。
- 采用非破坏性的总线仲裁技术，多点同时发送信息时，按优先级顺序通信，节省总线冲突仲裁时间，避免网络瘫痪。
- 远程数据请求。CAN 总线可以通过发送“远程帧”，请求其他节点的数据。

现有 Intel、Motorola 及 Philips 等公司生产符合 CAN 协议的通信芯片，还有基于 PC 总线的 CAN 接口卡，CAN 总线网络具有接口简单、编程方便、开发系统价格便宜。

2）CAN 总线与 RS-485 总线比较。与通常应用的 RS-485 方式相比，现场总线 CAN-bus 具有更多方面的优势，可以完全取代 RS-485 网络，从而组建一个具有高可靠性、远距离、多节点、多主方式的设备通信网络。同时，现场总线 CAN-bus 可以直接采用 RS-485 方式相同的传输电缆、拓扑结构。CAN-bus 总线与 RS-485 通信方式的特性比较如表 4-1 所示。

表 4-1　　CAN-bus 总线与 RS-485 通信的特性比较

特　性	RS-485 方 式	CAN-bus 总 线
拓扑结构	直线拓扑	直线拓扑
传输介质	双绞线	双绞线

续表

特　性	RS-485 方 式	CAN-bus 总 线
硬件成本	很低	每个节点成本有所增加
总线利用率	低	高
网络特性	单主结构	多主结构
数据传输率	低	最高可达 1Mb/s
容错机制	无	由硬件完成错误处理和检错机制
通讯失败率	很高	极低
节点错误的影响	导致整个网络瘫痪	故障节点对整个网络无影响
通讯距离	<1.5km	可达 10km（5kb/s）
网络调试	困难	非常容易
开发难度	标准 Mod-bus 协议	标准 CAN-bus 协议
后期维护成本	较高	很低

3）CAN 总线的电平与传输距离。总线上的信号使用差分电压传送，两条信号线被称为 CAN_H 和 CAN_L，如图 4-21 所示。CAN 总线上用显性（Dominant）和隐性（Recessive）表示 0 和 1。在隐性状态即逻辑 1 时，CAN_H 和 CAN_L 被固定在平均电压电平（2.5V 左右）附近，V_{diff} 近似于 0。在显性状态即逻辑 0 时，CAN_H 比 CAN_L 高，此时通常电压值为 CAN_H = 3.5V 和 CAN_L= 1.5V。在总线空闲或隐性位期间，发送隐性位。当在总线上出现同时发送显性位和隐性位时，总线上数值将出现显性。

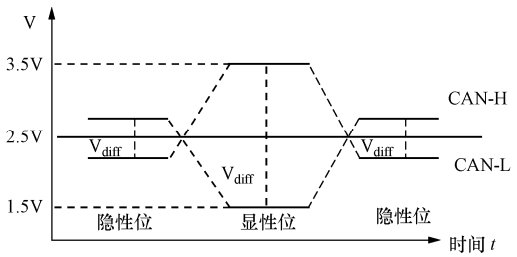

图 4-21　CAN 总线位的数值表示

CAN 总线上任意两个单元之间的最大传输距离与位速率有关，表 4-2 列出了距离与位速率的相关数据。这里的最大距离是指不接中继器的两个单元之间的距离。

表 4-2　　CAN 总线系统任意两节点之间的最大距离

位速率（kb/s）	1000	500	250	125	100	50	20	10	5
最大距离（m）	40	130	270	530	620	1300	3300	6700	10000

4）CAN 的基本术语与概念。

- 报文（Message）。总线上的信息以不同格式的报文发送，但长度有限。当总线开放时，任何连接的单元均可开始发送一个新报文。
- 信息路由（Information Routing）。在 CAN 系统中，一个 CAN 节点不使用有关系统配置的任何信息（例如站地址）。CAN 废除了站地址编码方式，代之以对通信数据进行编码。

- 位速率（Bit Rate）。CAN 的数据传输速率在不同系统中是不同的。然而，在一个给定系统中，位速率是唯一的，并且是固定的。
- 优先权（Priorities）。在总线访问期间，报文的标识符定义了一个静态的报文优先权。在 CAN 总线上发送的每一个报文都具有唯一的一个 11 位或 29 位的标识符，总线状态取决于二进制数 0 而不是 1，标识符越小，则该报文拥有越高的优先权，因此一个为全 0 标志符的报文具有总线上的最高级优先权。当有两个节点同时进行发送时，必须通过逐位仲裁方法使有最高优先权的报文优先发送。
- 远程数据请求（Remote Data Request）。通过发送一个远程帧，一个需要数据的节点可以请求另一个节点发送一个相应的数据帧，该数据帧和相应的远程帧以相同的标识符 ID 命名。
- 多主机（Multimaster）。当总线开放时，任何单元均可开始发送一个报文。具有要发送的最高优先权报文的单元赢得总线访问权。
- 仲裁（Arbitration）。总线开放时，任何单元均可发送报文，若有 2 个或更多的单元同时开始发送报文，总线访问冲突借助标识符 ID 逐位仲裁来解决。这种仲裁机制可以使信息和时间均无损失。若具有相同标识符 ID 的一个数据帧和一个远程帧同时启动，数据帧优先于远程帧。仲裁期间，每一个发送器都将发送的位电平与在总线上监视到的电平进行比较。若相同，则该单元可以继续发送。当发送一个“隐性”电平，而监视到一个“显性”电平时，该单元退出仲裁，并不再发送后续位。
- 错误标定和恢复时间（Error Signaling and Recovery Time）。任何检测到错误的单元会标志出已被损坏的报文。此报文会失效并将自动重传。如果不再出现错误，则从检测到错误到下一报文的传送开始，恢复时间最多为 31 个位的时间。
- 故障界定（Fault Confinement）。CAN 单元能够把永久故障和短暂的干扰区别开来，故障单元会被关闭。
- 连接（Connection）。CAN 通信链路是一条可连接多单元的总线。理论上，总线上单元数目是无限制的，实际上，单元数受限于延迟时间和总线的电气负载能力。例如，当使用 Philips P82C250 作为 CAN 收发器时，同一网络中一般最多允许挂接 110 个节点。
- 单通道（Single Channel）。CAN 总线由单一通道组成，借助数据的同步实现信息传输。CAN 技术规范中没有规定该通道的实现方法，可以是单线（加地线）、双绞线、光纤等，通常使用双绞线。
- 应答（Acknowledgment）。所有接收器对接收到的报文进行一致性（Consistency）检查。对于一致的报文，接收器给予应答；对于不一致的报文，接收器做出标志。
- 睡眠方式/唤醒（Sleep Mode/Wake-up）。为降低系统功耗，CAN 器件可被置于无任何内部活动的睡眠方式。借助于任何总线活动或者系统的内部条件均可唤醒 CAN 器件。为唤醒系统内仍处于睡眠状态的其他节点，可使用专用标识符的特殊唤醒报文。

（2）CANbus 技术协议规范。CAN 协议有 2.0A 和 2.0B 版本，CAN 协议的 2.0A 版本采用 CAN 标准报文格式，规定 CAN 控制器必须有一个 11 位的标志符，2.0B 版本为 CAN 标准报文格式和扩展报文格式，规定 CAN 控制器的标志符长度可以是 11 位或 29 位。

1）CAN 协议的分层结构。CAN 协议是建立在国际标准组织的开放系统互联模型基础之上的。CAN 的规范定义了 OSI 模型的最下面两层：数据链路层和物理层。CAN 结构层次少，数据结构简单，有利于系统中实时控制信号的传送。CAN 的 ISO/OSI 参考模型层结构如图 4-22

所示。

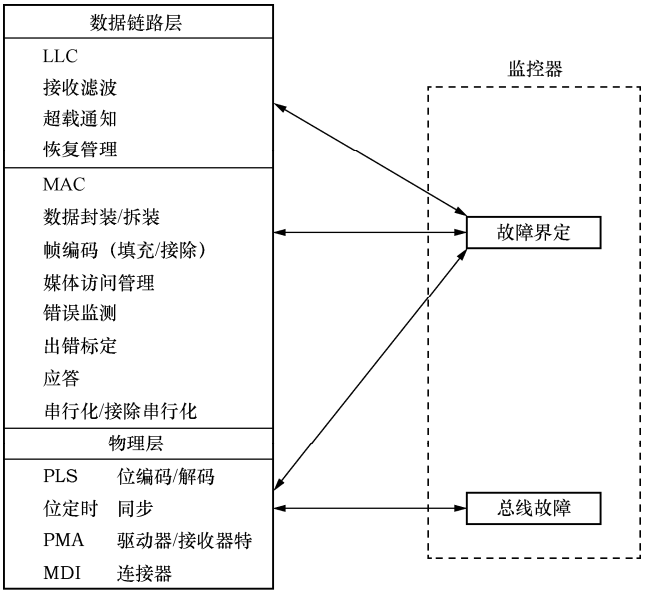

图 4-22　CAN 的分层结构和功能

物理层的范围是有关全部电气特性的不同节点间的位的实际传送。在一个网络内，物理层所有节点必须是相同的。然而，在选择物理层时存在很大的灵活性。物理层定义信号怎样进行发送，涉及位定时、位编码和同步的描述。该部分未定义物理层的驱动器/接收器特性，以便根据它们的应用，对发送媒体和信号电平进行优化。

数据链路层的 LLC 子层的主要功能是：为数据传送和远程数据请求提供服务，确认由 MAC 子层接收的报文实际已被接收和为恢复管理和通知超载提供信息。MAC 子层的功能主要是：传送协议，亦即控制成帧、执行仲裁、错误检测、错误标注和故障界定。MAC 子层是 CAN 协议的核心。它把接收到的报文呈现给 LLC，并接收来自 LLC 的报文以便发送。

2）报文传送与帧结构。CAN 以报文为单位进行信息传送，在进行数据传送时，发出一个报文的节点称为该报文的发送器，并且保持该身份直到总线空闲或丢失仲裁。若一个单元不是某个报文的发送器，并且总线不处于空闲状态，则称该节点为该报文的接收器。

CAN 总线报文中包含标识符 ID，它也标志了报文的优先权。该标识符 ID 并不指出报文的目的地址，而是描述数据的含义。网络中所有节点都可由 ID 来自动决定是否接收该报文。每个节点都有 ID 寄存器和屏蔽寄存器，接收到的报文只有与该屏蔽寄存器中的内容相同时，该节点才接收报文。

构成一帧的帧起始、仲裁场、控制场、数据场和 CRC 序列均借助位填充规则进行编码。无论何时，当发送器在将被发送的位流中检测到数值相同的 5 个连续位时，会自动地在实际的发送位流中插入一个补码位。数据帧或远程帧的其余位场（CRC 界定符，应答场和帧结束）具有固定格式，不进行填充。错误帧和超载帧同样具有固定格式，并且不用位填充规则编码。如位流 100000abc，填充后位流 1000001abc。报文中的位流按照非归零码规则编码，在一个完整的位时间内，产生的位电平要么是“显性”，要么是“隐性”。

CAN 总线中报文传输由 4 个不同的帧类型表示和控制。数据帧将数据从发送器传输到接收器。远程帧通过总线单元发出，以请求发送具有同一标识符的数据帧。错误帧由任何单元检测到总线

错误单元发出，超载帧用于在先行和后续数据帧（或远程帧）之间提供一附加的延时。数据帧和远程帧既可使用标准帧，也可使用扩展帧。

- 数据帧。数据帧由 7 个不同的位场组成：帧起始、仲裁场、控制场、数据场、CRC 场、应答场、帧结束。数据帧组成如图 4-23 所示。

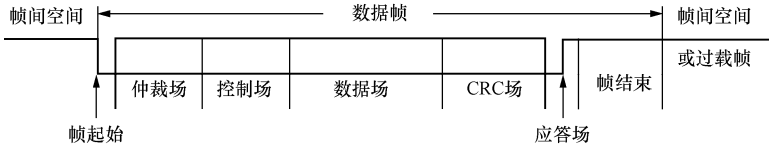

图 4-23　数据帧组成

帧起始（标准格式和扩展格式）：标志数据帧和远程帧的起始，仅由一个“显性”位组成。只有在总线空闲时，才允许总线上的通信节点开始发送报文。所有的节点必须同步于首先开始发送信息的节点的帧起始前沿。

仲裁场：在 CAN2.0B 中存在两种不同的帧格式，其主要区别在于标识符的长度，具有 11 位标识符的帧称为标准帧，而包括 29 位标识符的帧称为扩展帧。标准格式帧与扩展格式帧的仲裁场格式是不同的。

标准格式中，仲裁场由 11 位标识符和远程发送请求位（RTR）组成，标识符位由 ID28……ID18 组成。如图 4-24 所示。

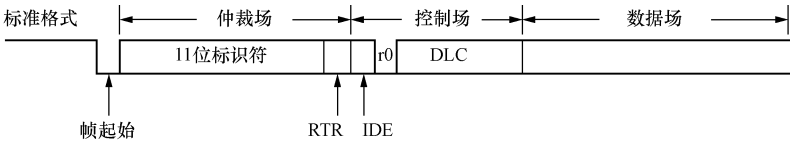

图 4-24　数据帧标准格式中的仲裁场结构

扩展格式中，仲裁场包括 29 位标识符、SRR、IDE、RTR 位。其标识符为 ID28……ID0。如图 4-25 所示。

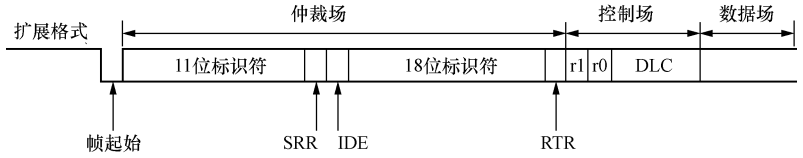

图 4-25　数据帧扩展格式中的仲裁场结构

在标准格式中，标识符的长度为 11 位。这些位的发送顺序是从 ID10 到 ID0。最低位是 ID0。最高的 7 位（ID10 到 ID4）不能全是隐性。而扩展格式的标识符长为 29 位，包括 11 位基本 ID 和 18 位扩展 ID 帧，基本 ID 定义了扩展帧的基本优先权。

RTR 位为“远程请求发送位”，在数据帧里为显性，在远程帧里为隐性。

SRR 位为“替代远程请求位”，属扩展格式，它是在扩展帧的标准帧 RTR 位的位置，因而替代标准帧的 RTR 位。当标准帧与扩展帧发生冲突且扩展帧的基本 ID 同标准帧的标识符一样时，标准帧优先于扩展帧。

IDE 位是“标识符扩展位”，属扩展格式的仲裁场和标准格式的控制场，在标准格式中 IDE

为显性，而扩展格式中 IDE 为隐性。

控制场：由 6 个位组成。标准格式的控制场格式和扩展格式不同。标准格式中的帧包括数据长度代码、IDE 位（为显性）、保留位 r0。扩展格式包括数据长度代码和两个必须为显性的保留位 r1 和 r0。但接收器接收由显性和隐性位组合。

数据长度代码指示了数据场中字节数量。数据长度代码为 4 位，在控制场中被发送。数据长度码中数据字节数据编码如表 4-3 所示。其中，d 表示显性位，r 表示隐性位，数据字节的数目个数只能在 0～8。

表 4-3　　数据长度码中数据字节数目个数编码表

数据字节数目	数 据 长 度 码			
	DLC3	DLC2	DLC1	DLC0
0	d	d	d	d
1	d	d	d	r
2	d	d	r	d
3	d	d	r	r
4	d	r	d	d
5	d	r	d	r
6	d	r	r	d
7	d	r	r	r
8	r	d	d	d

数据场（标准格式以及扩展格式）：数据场由数据帧里的发送数据组成。它可以为 0～8 字节，每字节包含了 8 位，按字节大端顺序发送。

CRC 场（标准格式以及扩展格式）：CRC 场包括 CRC 序列（CRC SEQUENCE），其后是 CRC 界定符（CRC DELIMITER）。

应答场（标准格式以及扩展格式）：应答场长度为 2 位，包含应答间隙（ACK SLOT）和应答界定符（ACK DELIMITER）。在应答场里，发送器发送两个“隐性”位。当接收器正确地接收到有效的报文，接收器就会在应答间隙期间发送 ACK 信号，向发送器发送一“显性”位以示应答。应答界定符是应答场的第二个位，并且是一个“隐性”位。因此，应答间隙被两个“隐性”的位所包围，也就是 CRC 界定符和应答界定符。

帧结束（标准格式以及扩展格式）：每个数据帧和远程帧均由一标志序列定界。这个标志序列由 7 个“隐性”的位组成。

- 远程帧。作为数据接收站，可以借助于发送远程帧启动其资源节点传送数据。远程帧也有标准格式和扩展格式，而且都由 6 个不同的位场组成：帧起始、仲裁场、控制场、CRC 场、应答场、帧结尾。远程帧的组成如图 4-26 所示。

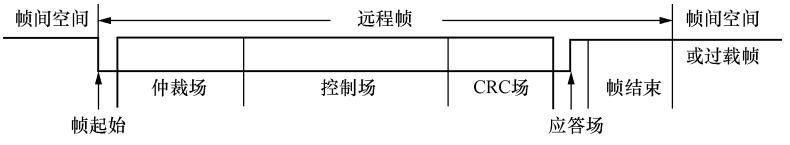

图 4-26　远程帧的组成

与数据帧相反，远程帧的 RTR 位是“隐性”的。它没有数据场。

RTR 位的极性表示了所发送的帧是数据帧（RTR 位“显性”）还是远程帧（RTR 位“隐性”）。

- 错误帧。错误帧由两个不同的场组成。第一个场是由不同站提供的错误标志（ERROR FLAG）的叠加；第二个场是错误界定符。错误帧的组成如图 4-27 所示。

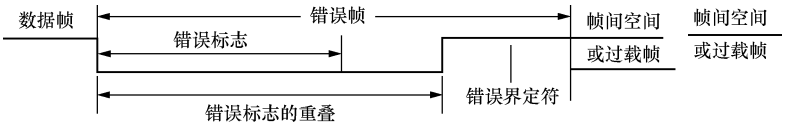

图 4-27　错误帧的组成

错误标志有两种形式：主动错误标志和被动错误标志。主动错误标志由 6 个连续的显性位组成，而被动错误标志由 6 个连续的隐性位组成，除非被其他节点的显性位重写。

- 超载帧。超载帧包括两个位场：超载标志和超载界定符，如图 4-28 所示。

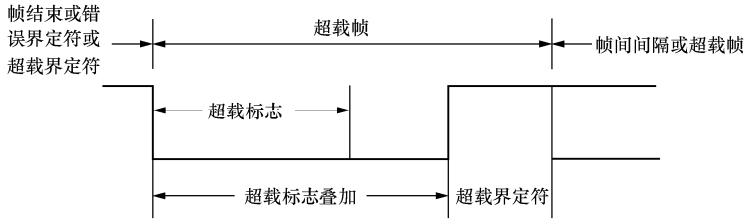

图 4-28　超载帧格式

存在两种导致发送超载标志的超载条件：一是要求延迟下一数据帧或远程帧的接收器的内部条件；另一是在间歇场检测到显性位。前一超载条件引起的超载帧起点，仅允许在期望间歇场第一时间开始，后一条件引起的超载帧在检测到显性位的后位开始，大多情况下，为延迟下一数据帧或远程帧，两种超载帧均可产生。

超载标志由 6 个显性位组成，全部形式对应于活动错误标志形式。超载界定符由 8 个隐性位组成，超载界定符与钜误界定符具有相同的形式。

- 帧间空间。数据帧和远程帧与其前面的帧相同，不管是何种帧（数据帧、远程帧、错误帧或超载帧）均以帧间空间（Interframe Space）的位场分隔开。在超载帧和错误帧前面没有帧间空间，并且多个超载帧也不被帧间空间分隔。

帧间空间包括间歇场和总线空闲场，对于已经发送先前报文的“错误认可”节点还有暂停发送场。对于非“错误认可”或已经完成前面报文的接收器，其帧空间如图 4-29（a）所示，对于已经完成前面报文发送的“错误认可”站，其帧空间如图 4-29（b）所示。

间歇场由 3 个“隐性”位组成。间歇场期间，不允许任何站启动发送数据帧或远程帧。唯一的作用是标注超载条件。

总线空闲场持续时间可为任意长度。此时，总线是开放的，因而任何需要发送的节点均可访问总线。

在其他报文发送期间，待发送的报文，在间歇场后的第一位开始发送。检测到总线上的一个“显性”位将被理解为帧起始。

暂停发送场是指错误认可节点发完一个报文后，在开始下一次报文发送或认可总线空闲之前，

它紧随间歇场后送出 8 个“隐性”位。如果在此期间其他节点开始一次发送，该节点将变为报文接收器。

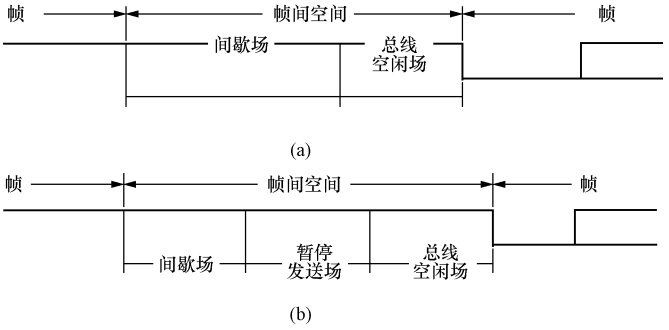

图 4-29　帧间空间构成

（a）非“错误认可”或已接收先前报文的站的帧间空间；（b）已发送先前报文的“错误认可”站的帧间空间

3）错误类型和界定。

- 错误类型。在 CAN 总线中存在位错误、填充错误、CRC 错误、形式错误和应答错误 5 种错误类型。

位错误（Bit Error）：向总线送出一位的某个单元同时也在监视总线。当监视到的总线位数值与送出的位数值不同时，则在该位时刻检出一个位错误。例外情况是在仲裁场的填充位流期间或应答期间送出隐性位而检测到显性位时。

填充错误（Stuff Error）：在使用位填充方法进行编码的报文中，出现了第 6 个连续相同的位电平时，将检出一个填充错误。

CRC 错误（CRC Error）：CRC 序列是由发送器完成的 CRC 计算结果组成的。接收器以与发送器相同的方法计算 CRC。如果计算结果与接收到的 CRC 序列不相同，则检出一个 CRC 错误。

形式错误（Form Error）：当固定形式的位场中出现一个或更多非法位时，则检出一个形式错误。

应答错误（Acknowledgement Error）：在应答间隙期间，发送器未检测到“显性”位，则由它检出一个应答错误。

- 错误信号的发出。检测到错误条件的节点通过发送错误标志指示错误。对于“错误激活”的节点，错误信息为“激活错误”标志；对于“错误认可”的节点，错误信息为“认可错误”标志。节点检测到无论是位错误、填充错误、形式错误，还是应答错误，这个节点会在下一位时发出错误标志信息。

如果检测到的错误的条件是 CRC 错误，则错误标志的发送开始于 ACK 界定符之后的位，除非其他错误条件引起的错误标志已经开始。

- 故障界定。在 CAN 总线中，就故障界定而言，一个节点可能处于三种状态。

错误激活（Error Active）：“错误激活”的节点可以正常地参与总线通信，并在错误被检测到时发出“激活错误”标志。

错误认可（Error Passive）：“错误认可”节点不允许发送“激活错误”标志。当“错误认可”节点参与总线通信时，在错误被检测到时只发出“认可错误”标志。而且，发送之后，“错误认可”节点将在启动下一个发送之前处于等待状态。

总线关闭（Bus Off）：“总线关闭”的节点不允许对总线产生任何的影响，例如关闭输出驱动器。

为了界定故障，在每一总线节点中都设有两种计数，包括发送错误计数和接收错误计数。这些计数按照下列规则进行，在给定的报文发送期间，可能要用到的规则不止一个。

接收器检出错误时，接收错误计数加 1。接收器在送出错误标志后的第一位检出一个“显性”位时，接收错误计数加 8。发送器送出一个错误标志时，发送错误计数加 8。有两种例外情况，发送错误计数不改变。

一个是如果发送器为“错误认可”，由于未检测到“显性”应答而检测到一个应答错误，并且在送出其认可错误标志时，未检测到“显性”位。另一个是如果由于仲裁期间发生的填充错误，则发送器送出一个错误标志，本应是“隐性”的，而且确实发送的是“隐性”的，但监视到的为“显性”的。

如果发送器送出一个激活错误标志或超载标志时，发送器检测到位错误，则发送错误计数加 8。如果接收器送出一个激活错误标志或超载标志时，接收器检测到位错误，则接收错误计数加 8。

在送出激活错误标志、认可错误标志或超载标志后，任何节点都允许多至 7 个连续的“显性”位。在检测到第 11 个连续的“显性”位后，或紧随认可错误标志检测到第 8 个连续的“显性”位后，以及附加的 8 个连续的“显性”位的每个序列后，每个发送器的发送错误计数都加 8，并且每个接收器的接收错误计数也都加 8。

报文成功发送后，则发送错误计数减 1，若它已经为 0，则仍保持为 0。

报文成功接收后，如果它处于 1 和 127 之间，则接收错误计数减 1，若接收错误计数为 0，则仍保留 0，若它大于 127，则将其置值为 119 和 127 之间的某个数值。

发送错误计数等于或大于 128 或接收错误计数等于或大于 128 时，节点为“错误认可”。导致节点变为“错误认可”的错误状态使节点送出一个激活错误标志。

发送错误计数大于或等于 256 时，节点为“总线脱离”。发送错误计数和接收错误计数两者均小于或等于 127 时，“错误认可”节点再次变为“错误激活”节点。

在检测到总线上 11 个连续的“隐性”位发生 128 次后，“总线脱离”节点将变为其两个错误计数器均置为 0 的“错误激活”节点。

当错误计数值大于 96 时，说明总线被严重干扰。它提供测试此状态的一种手段。

若系统启动期间，仅有一个节点在线，此节点发送报文后，将得不到应答，检出错误并重复该报文。它可以变为“错误认可”，但不会因此变或“总线脱离”。

4）位定时要求。

- 正常位速率（Nominal Bit Rate）。在非重同步情况下，借助理想发送器每秒发送的位数。
- 正常位时间（Nominal Bit Time）。正常位速率的倒数。

正常位时间可划分为几个互不重叠的时间段，如图 4-30 所示。这些时间段包括：

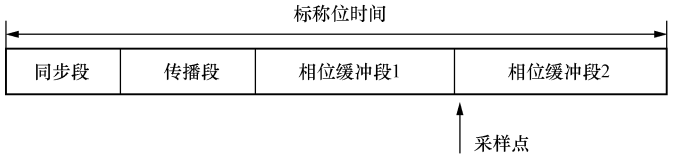

图 4-30　正常位时间的划分

① 同步段（SYNC-SEG）：用于使总线上的各个节点同步。期望有一个跳变沿位于此段内。

② 传播段（PROP-SEG）：用于补偿网络内的物理延时。它是信号在总线上传播时间的两倍与输入比较器延时和输出驱动器延时之和。

③ 相位缓冲段 1（PHASE-SEG1）和相位缓冲段 2（PHASE-SEG2）：用于补偿沿的相位误差，使总线上的各个节点同步。通过重同步，这两个时间段可被延长或缩短。

④ 采样点（Sample Point）：在此时刻上，总线电平被读，并被理解为其自身位的数值。它位于相位缓冲段 1 的终点。

- 信息处理时间。由采样点开始、为计算后续位电平而保留的时间段。
- 时间份额（Time Quantum）。由振荡器周期派生出的一个固定时间单元。时间份额的总数必须被编程为至少由 8～25。正常位时间中各时间段长度：SYNC-SEG 为 1 个时间份额；PROP-SEG 长度可编程为 1，2，…，8 个时间份额；PHASE-SEG1 长度可编程为 1，2，…，8 个时间份额； PHASE-SEG2 长度为 PHASE-SEG1 和信息处理时间的最大值；信息处理时间长度小于或等于 2 个时间份额。
- 硬同步（Hard Synchronization）。硬同步后，内部位时间从 SYNC-SEG 重新开始。硬同步强迫引起硬同步的沿处于重新开始的位时间同步段之内。
- 重同步（Resynchronization）。当引起重同步的沿的相位误差数值小于或等于重同步跳转宽度编程值时，重同步的作用与硬同步的作用相同。当相位误差数值大于重同步跳转宽度，且相位误差为正时，则 PHASE-SEG1 延长数值等于重同步跳转宽度。当相位误差数值大于重同步跳转宽度，且相位误差为负时，则 PHASE-SEG2 缩短数值等于重同步跳转宽度。
- 重同步跳转宽度（Resynchronization Jump Width）。作为重同步的结果， PHASE-SEG1 可被延长或 PHASE-SEG2 可被缩短。这两个相位缓冲段的延长或缩短的数值有一个由重同步跳转宽度给定的上限。重同步跳转宽度应编程为 1 和 4（PHASE-SEG1）之间。时钟信息可由一位数值到另一位数值的跳变取得。具有相同数值的连续位的最大个数是唯一而固定的，这一特性提供了在帧期间总线单元重同步于位流的可能性。可被用于重同步的两个跳变之间的最大长度是 29 个位时间。
- 沿相位误差（Phase Error of an Edge）。沿相位误差由沿相对于 SYNC-SEG 的位置给定，以时间份额量度。相位误差的符号定义如下：若沿处于 SYNC-SEG 之内，则 $e = 0$；若沿处于采样点之前，则 $e > 0$；若沿处于前一位采样点之后，则 $e < 0$。
- 同步规则（Synchronization Rules）。在一个位时间内仅允许一种同步。只要在先前采样点上检测到的数值与一个沿过后立即得到的总线数值不同，则该沿将被用于同步。在总线空闲期间，无论何时当存在一个“隐性”至“显性”的跳变沿，则执行一次硬同步。

（3）CAN 总线应用层协议。应用层协议内容提供一组服务和规范，通信规范提供配置设备的方法和通信数据，定义设备之间的数据通信方式。CAN 现场总线只对物理层和数据链路层做了描述和规定，而没有规定应用层，其本身并不完整，在 CAN 总线的分布式测控系统中，有些功能需要一个高层协议来实现，例如通过应用层通信协议规定 CAN 报文中的 11/29 位标识符和 8 字节数据的使用，如何响应或者确定报文的传送，网络的启动及监控，网络中 CAN 节点故障的识别和标识等问题。

不同的应用出现了不同的应用层协议，为了使不同厂商的产品能够相互兼容，需要在 CAN 网络中实现统一的通信模式，执行网络管理，提供设备功能描述方式。CAN 应用层协议有

DevceNet、CANopen、CAL、SDS、CANKingdom、SAE J1939 协议，也可以自行制定一个应用层协议。目前广泛使用的两个应用层协议是 CANopen 协议与 DeviceNet 协议。

1）CANopen。CANopen 由 CiA（CAN in Aoutmation）成员编制，是在 CAL（CAN Application Layer）基础上开发的，它在通信和系统服务以及网络管理方面使用了 CAL 通信和服务协议子集，设备建模是借助于对象目录而基于设备功能性的描述，标准设备以设备子协议的形式规定。CANopen 协议主要用于汽车、工业控制、自动化仪表等领域，CANopen 标准由 CIA 负责管理和维护。

2）DeviceNet。DeviceNet 是 20 世纪 90 年代中期发展起来的一种基于 CAN 技术的开放型、符合全球工业标准的低成本、高性能的通信网络。DeviceNet 不仅可以作为设备级的网络，还可以作为控制级的网络，通过 DeviceNet 提供的服务还可以实现以太网上的实时控制。较之其他的一些现场总线，DeviceNet 不仅可以接入更多、更复杂的设备，还可以为上层提供更多的信息和服务。

DeviceNet 最初由 Rockwell 公司设计，目前由 ODVA（Open DeviceNet Vendors Association）致力于支持 DeviceNet 产品和规范的进一步开发。此外，Rockwell、 GE、ABB、Hitachi、Omron 等公司也致力于 DeviceNet 的推广。

3. 其他典型现场总线

（1）基金会现场总线。基金会现场总线 FF（FoudationFieldbus），在过程自动化领域得到广泛支持，具有良好的发展前景。以美国 Fisher-Rousemount 公司为首，联合 Foxboro、横河、ABB、西门子等 80 家公司制订了 ISP，以 Honeywell 公司为首，联合欧洲等地的 150 家公司制订了 WordFIP，1994 年 9 月这两大集团合并，成立了现场总线基金会，致力于开发国际上统一的现场总线协议。它以 ISO/OSI 开放系统互连模型为基础，取物理层、数据链路层、应用层为 FF 通信模型的相应层次，并在应用层上增加了用户层。

基金会现场总线分低速 H1 和高速 H2 两种通信速率。H1 的传输速率为 3125kb/s，通信距离可达 1900m（可加中继器延长），支持总线供电与本质安全防爆环境。H2 的传输速率为 1Mb/s 和 2.5Mb/s 两种，其通信距离为 750m 和 500m。物理传输介质支持双绞线、光缆和无线发射，协议符合 IEC1158-2 标准。

（2）LonWorks。LonWorks 是由美国 Ecelon 公司推出，并与摩托罗拉、东芝公司共同倡导，于 1990 年正式公布而形成。它采用了 ISO/OSI 模型的全部七层通信协议，采用了面向对象的设计方法，通过网络变量把网络通信设计简化为参数设置，其通信速率从 300b/s 至 15Mb/s 不等，直接通信距离可达到 2700m（78kb/s，双绞线），支持双绞线、同轴电缆、光纤、射频、红外线、电源线等多种通信介质，并开发了相应的本安防爆产品。

LonWorks 是符合 ISO/ OSI 全部 7 层参考模型的现场总线，实行开放结构，节点应用程序编写简易，具备良好的互操作性。另外网关可方便构成局域网，甚至与 Internet 相连。

（3）HART。HART（Highway Addressable Remote Transduer）最早由 Rosemout 公司开发并得到 80 多家著名仪表公司的支持，于 1993 年成立了 HART 通信基金会。该开放通信协议是在现有模拟信号传输线上实现数字通信，属于模拟系统向数字系统转变过程中的过渡产品。

HART 通信模型由物理层、数据链路层和应用层 3 层组成。物理层采用 FSK 技术，数据传输速率为 1200b/s，逻辑“0”的信号频率为 2200Hz，逻辑“1”的信号传输频率为 1200Hz。

（4）CC-Link。CC-Link（Control&Communication Link）是三菱电机于 1996 年推出的开放式现场总线，应用于控制与通信链路系统，其数据容量大，通信速度多级可选择，它是一个复合的、开放的、适应性强的网络系统，能够适应于较高的管理层网络到较低的传感器层网络的不同范围。

CC-Link 是一个以设备层为主的网络，一般情况下，CC-Link 整个一层网络可由 1 个主站和 64 个从站组成。网络中的主站由 PLC 担当，从站可以是远程 I/O 模块、特殊功能模块、带有 CPU 和 PLC 本地站、人机界面、变频器及各种测量仪表、阀门等现场仪表设备。

4.3 工业以太网技术

4.3.1 以太网与 TCP/IP

1. 以太网

802.3 局域网最早源于美国施乐公司 Xerox 、DEC 与 Intel 三家公司合作研究 10Mb/s 的 Ethernet 实验系统，于 1980 年第一次公布了 Ethernet 的物理层、数据链路层规范，1981 年 11 月公布了 Ethernet V2.0，随后该标准成为 IEEE802.3 的基础。

（1）以太网技术特性。

1）以太网是基带网，采用基带传输技术，在同一时间只能有一个设备占用信道发送数据，基带网上的设备能够使用全部有效带宽，对信道不进行多路复用。

2）以太网的标准是 IEEE802.3，它使用 CSMA/CD 介质访问控制方法，对单一信道的访问进行控制、分配介质的访问权，以保证同一时间只有一对网络站点使用信道，避免发生冲突。

3）以太网是一种共享型网络，网络上的所有站点共享传输媒体和带宽，是广播式网络，它具有广播式网络的全部特点。

4）采用曼彻斯特编码。

5）以太网所支持的传输介质类型有同轴电缆、非屏蔽双绞线和光纤。

6）以太网所构成的拓扑结构主要是总线型和星型。

7）有多种以太网标准，支持不同的传输速率（10Mb/s、100Mb/s 和 1000Mb/s），最高可达 1Gb/s。

（2）以太网体系结构。按 IEEE802.3 标准规定，以太网具有图 4-31 所示的体系结构。

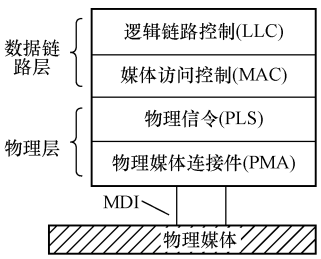

图 4-31 以太网体系结构

1）物理层。在 IEEE802.3 标准中，将物理层分为两个子层，分别是物理信令（PLS）子层和物理媒体连接件（PMA）子层。PLS 子层向 MAC 子层提供服务，并负责比特流的曼彻斯特编码与译码和载波监听功能。PMA 子层向 PLS 子层提供服务，完成冲突检测、超长控制以及发送和接收串行比特流的功能。媒体相关接口（MDI）与传输媒体的形式有关，它定义了连接器以及电缆两端的终端负载的特性，是设备与总线的接口部件。

2）数据链路层。MAC 子层与硬件相关，与 LLC 子层之间通过 MAC 服务访问点相连接。MAC 子层的核心协议是 CSMA/CD，它的帧结构如图 4-32 所示。

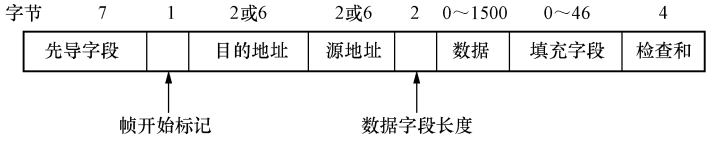

图 4-32 IEEE 802.3 帧结构

其中，7 字节的先导字段是接收方与发送方时钟同步用的，它的每字节的内容都是 10101010。一字节的帧开始标志，表示一个帧的开始，内容为 10101011。后面为两个地址段，即源地址和目的地址，目的地址可以是单个物理地址，也可以是一组地址（多点广播），当地址的最高位为 0 时，是普通地址，为 1 时，是组地址。2 字节的数据字段长度标志数据段中的字节数。数据字段就是 LLC 数据帧，如果帧的数据部分少于 46 字节，则用填充字段，使之达到要求的最短长度。

（3）传统以太网。

1）10Base-5。IEEE802.3 中最早定义的以太网标准，也叫粗缆以太网。10Base-5 的拓扑结构为总线型，采用基带传输，无中继器的情况下最远的传输距离可以达到 500m。

2）10Base-2。10Base-2 是总线型细缆以太网，是以太网支持的第二类传输介质，10Base-2 使用 50Ω 细同轴电缆传输介质，组成总线型网。

3）10Base-T。该标准规定在非屏蔽双绞线（UTP）介质上提供 10Mb/s 的数据传输速率。每个网络站点都需要通过 UTP 连接到一个中心设备集线器（HUB）上，构成星型拓扑结构。10Base-T 双绞线以太网系统操作在二对 3 类 UTP 上，一对用于发送信号，另一对用于接收信号。为了改善信号的传输特性和信道的抗干扰能力，每一对线必须绞在一起。

4）10Base-F。10Base-F 是 10Mb/s 光纤以太网，它使用多模光纤传输介质，在介质上传输的是光信号而不是电信号。具有传输距离长、安全可靠、可避免电击的危险等特点。

（4）高速以太网。

1）快速以太网。快速以太网的传输速率比普通以太网快 10 倍，数据传输速率达到了 100Mb/s。快速以太网保留了传统以太网的所有特性，包括相同的数据帧格式、介质访问控制方式和组网方法，只是将每比特的发送时间由 100ns 降低到 10ns。快速以太网标准在 LLC 子层使用 IEEE 802.2 标准，在 MAC 子层使用 CSMA/CD 方法，在物理层做了一些调整，定义了新的物理层标准（100BASE-T）。100BASE-T 标准定义了介质专用接口，它将 MAC 子层和物理层分开，使得物理层在实现 100Mb/s 速率时所使用的传输介质和信号编码方式的变化不会影响 MAC 子层。100BASE-T 可以支持多种传输介质，目前制定了三种有关传输介质的标准：100BASE-TX、100BASE-T4、100BASE-FX。

2）千兆位以太网。千兆位以太网（GE-Gigabit Ethernet）是提供 1000Mb/s 数据传输速率的以太网。千兆位以太网与现有以太网完全兼容，其传输速率达到 1Gb/s。千兆位以太网支持全双工操作，最高速率可以达到 2Gb/s。

1996 年 IEEE802.3 工作组成立了 IEEE802.3z 千兆以太网工作组，并于 1998 年完成了 IEEE802.3z 标准。IEEE802.3z 千兆位以太网标准定义了三种介质标准，短波长激光光纤介质系统标准 1000Base-SX、长波长激光光纤介质系统标准 1000Base-LX、短铜线介质系统标准 1000Base-CX。有时也统称为 1000Base-X。

3）万兆位以太网。为了完善 IEEE802.3 协议，提高以太网带宽，1999 年 IEEE802.3 高速研究小组开始研究 IEEE802.3ae 万兆位以太网标准，将以太网应用扩展到城域网和广域网，并与原有以太网的网络操作和管理保持一致，2002 年正式公布了万兆位以太网标准。

万兆位以太网（10GE）是一种数据传输速率高达 10Gb/s、通信距离可延伸到 40km 的以太网。万兆位以太网本质上仍然是以太网，只是在速度和距离方面有了显著的提高。万兆位以太网继续使用 IEEE802.3 以太网协议，以及 IEEEE802.3 以太网的帧格式和帧大小。但由于万兆以位太网是一种只适用于全双工通信方式，并且只能使用光纤介质的技术，所以它不需要使用带冲突检测的载波监听多路访问协议 CSMA/CD。此外，万兆位以太网标准中包含了广域网的物理层协议，不

仅可以应用于局域网，也可以应用于城域网和广域网，使局域网与城域网和广域网实现无缝连接，其应用范围更为广泛。

4）光纤分布式数据接口。光纤分布式数据接口 FDDI（Fiber Distributed Data Interface）是一个使用光纤介质传输数据的高性能环型局域网，是在令牌环网的基础上发展起来的，它是一个技术规范，描述了一个以光纤为介质的高速（100Mb/s）令牌环网。FDDI 为各种网络提供高速连接，网络覆盖的最大距离可达 200km，最多可连接 1000 个站点。

FDDI 标准由 ANSI X3T9.5 标准委员会在 1980 年提出，具有高速、技术成熟、安全双环结构等特点。由于站点管理复杂，价格昂贵，主要用于主干网，在桌面局域网中，不如以太网应用广泛。

2. TCP/IP

（1）TCP/IP 参考模型。TCP/IP（Transmission Control/Internet Protocol）是指传输控制协议/网际协议，起源于美国 ARPAnet，由它的两个主要协议 TCP 和 IP 而得名。通常所讲的 TCP/IP 实际上包含了许多协议和应用，是由多个独力定义的协议组合在一起，确切地应称其为 TCP/IP 协议集。

TCP/IP 采用分层体系结构，每一层提供特定的功能，层与层间相对独立，改变某一层的功能不会影响其他层。分层技术简化了系统的设计和实现，提高了系统的可靠性及灵活性。

TCP/IP 分层体系结构共分四层，即网络接口层、网际层、传输层和应用层。与 OSI 七层模型相比，TCP/IP 没有表示层和会话层，这两层的功能由应用层提供，OSI 的物理层和数据链路层功能由网络接口层完成。OSI 模型在网络层支持无连接和面向连接的通信，在传输层仅有面向连接的通信。相对而言，TCP/IP 要简单些，ISO/OSI 协议在数量上要远多于 TCP/IP。TCP/IP 参考模型及协议集如图 4-33 所示。

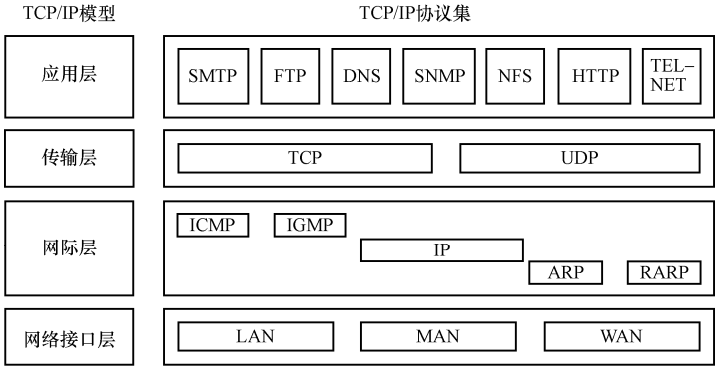

图 4-33　TCP/IP 参考模型及协议集

1）网络接口层。网络接口层也称为网络访问层，是 TCP/IP 参考模型的最低层，对应着 OSI 的物理层和数据链路层。TCP/IP 标准没有定义具体的网络接口协议，提供了灵活性，以适应各种网络类型，如 LAN、MAN 和 WAN，说明 TCP/IP 可以运行在多种网络之上。

2）网际层。网际层是 TCP/IP 参考模型的第二层。网际层主要功能是处理来自传输层的分组，将分组形成数据包（IP 数据包），为该数据包进行路径选择，最终将数据包从源主机发送到目的主机。在网际层中，最常用的协议是网际协议 IP，其他一些协议用来协助 IP 的操作。

3）传输层。传输层是 TCP/IP 参考模型的第三层，与 OSI 的传输层类似，主要负责主机到主机之间的端到端通信，该层使用了 TCP 和 UDP 两种协议来支持两种数据的传送，TCP/IP 参考模

型的传输层与 OSI 参考模型的传输层功能相似。

4）应用层。应用层是 TCP/IP 参考模型的最高层，它与 OSI 模型中的高三层的任务相同，它包括所有的高层协议，用于提供网络服务，例如文件传输、远程登录、域名服务和简单网络管理等等。

（2）TCP/IP 协议简介。TCP/IP 通过一系列协议来提供各层的功能服务，以实现网间的数据传送。

应用层包括了所有的高层协议，并不断有新的协议加入，该层中有许多协议，如远程登录协议（Telnet），本地主机作为仿真终端登录到远程主机上运行应用程序；超文本传输协议（HTTP），用于 Internet 中的客户机与 WWW 服务器之间的数据传输；文件传输协议（FTP），实现主机之间文件的传送；邮件传送协议（SMTP）实现主机之间电子邮件的传送等。

传输层使用两种不同的协议：一种是面向连接的传输控制协议 TCP（Transmission Control Protocol），另一种是无连接的用户数据报协议 UDP（User Data Protocol）。传输层传送的数据单位是报文（message）或数据流（stream）。

传输层下面是 TCP/IP 的网际层，其主要的协议是无连接的网络互连协议 IP（Internet Protocol）。该层传送的数据单位是分组（packet）。与 IP 配合使用的还有四个协议：Internet 控制报文协议 ICMP（ Internet Control Message Protocol）、Internet 组管理协议 IGMP（Internet Group Manage Protocal）、地址解析协议 ARP（Address Resolution Protocol）和逆地址解析协议 RARP（Reverse Address Resolution Protocol）。

最底层的网络接口层支持所有流行的物理网络协议，如 IEEE802 系列局域网协议、HDLC 等。部分 TCP/IP 协议介绍如下：

1）网际协议 IP。IP 的任务是对数据包进行相应的寻址和路由，并从一个网络转发到另一个网络。IP 在每个发送的数据包前加入一个控制信息，其中包含了源主机的 IP 地址和其他信息。IP 的另一项工作是分割和重编在传输层被分割的数据包。由于数据包要从一个网络转发到另一个网络，当两个网络所支持传输的数据包的大小不相同时，IP 就要在发送端将数据包分割，然后在分割的每一段前再加入控制信息进行传输。当接收端接收到数据包后，IP 协议将所有的片段重新组合形成原始的数据。

IP 是一个无连接的协议，主机之间不建立用于可靠通信的端到端连接，源主机将 IP 数据包发出可能会丢失、重复、延迟接收或者次序混乱，要实现数据包可靠传输，必须依靠高层的协议或应用程序，如传输层 TCP。

2）传输控制协议 TCP。TCP 是传输层的一种面向连接的通信协议，它提供可靠的数据传送。对于大量数据的传输，通常都要求可靠传送。TCP 将源主机应用层的数据分成多个分段，然后将每个分段传送到网际层，网际层将数据封装为 IP 数据包，并发送到目的主机。目的主机的网际层将 IP 数据包中的分段传送给传输层，再由传输层对这些分段进行重组，还原成原始数据，并传送给应用层。另外，TCP 还要完成流量控制和差错检验的任务，以保证可靠的数据传输。

3）用户数据报协议 UDP。UDP 是一种面向无连接的协议，它不能提供可靠的数据传输，而且 UDP 不进行差错检验，必须由应用层的应用程序来实现可靠性机制和差错控制，以保证端到端数据传输的正确性。虽然 UDP 与 TCP 相比显得不可靠，但在一些特定的环境下有其优势。例如，要发送的信息较短，不值得在主机之间建立一次连接。另外，面向连接的通信通常只能在两个主机之间进行，若要实现多个主机之间的一对多或多对多的数据传输，即广播或多播，就需要使用 UDP。

4.3.2 工业以太网概述

1. 传统以太网存在的问题

（1）不确定性。以太网采用 CSMA/CD 协议导致网络存在冲突，大量的冲突应用于控制网络，使得网间通信的不确定性大大增加，必然导致系统控制性能降低。

（2）非实时性。工业控制对数据传输实时性要求严格，数据更新通常在数十毫秒内完成。同样由于以太网的 CSMA/CD 机制，当发生冲突的时候，需要重发数据，增加了传输时间。如果出现掉线，还会造成安全事故。

（3）低可靠性。传统以太网以商业应用为目的，并非从工业网应用角度设计，不能满足工业现场各种工况的需要，可靠性低。

（4）安全性差。工业生产过程中，很多现场存在易燃、易爆或有毒气体等，要求设备采取一定的防爆措施来保证工业现场的安全生产。网络安全是以太网应用必须考虑的问题。企业采用传统的三层网络系统，网络之间集成，引入了一系列的网络安全向题，会受到非法操作、病毒感染、黑客入侵等网络安全威胁。

（5）总线供电问题。总线供电（或称总线馈电）是指连接到现场设备的线缆不仅传输数据信号，还能给现场设备提供工作电源。以太网设计没有考虑到该问题，而工业现场存在着大量的总线供电需求。

2. 工业以太网相关技术

传统以太网不适合直接用于工业现场控制，为了解决上述问题工业以太网便应运而生。工业以太网是将传统以太网应用于工业控制和管理的局域网技术，技术上与以太网 IEEE 802.3 标准兼容。产品设计时，在材质的选用、产品的强度、适用性以及实时性、可互操作性、抗干扰性和可靠性、总线供电和本质安全等方面能满足工业现场的需要，已采用多种方法来改善以太网的性能和品质，以满足工业领域的要求。

基于工业标准，工业以太网技术的发展得益于以太网技术发展。首先是通信速率的提高，其次由于采用星型网络拓扑结构和交换技术，使以太网交换机的各端口之间数据帧的输入和输出不再受 CSMA/CD 机制的制约，避免了冲突；再加上全双工通信方式使端口间两对双绞线（或光纤）上分别同时接收和发送数据，而不发生冲突。

（1）交换技术。为了改善以太网负载较重时的网络拥塞问题，使用以太网交换机（switch）。交换技术采用将共享的局域网进行有效的冲突域划分。各个冲突域之间用交换机连接，以减少 CSMA/CD 机制带来的冲突问题和错误传输，可以尽量避免冲突的发生，提高系统的确定性，但该方法成本较高，在分配和缓冲过程中存在一定的延时。

（2）高速以太网。当网络中的负载越大，发生冲突的概率也就越大。提高以太网的通信速度，可以有效降低网络的负荷。以太网已经出现数据传输速率达 100Mb/s，1Gb/s 的高速以太网，加上全面的设计及对系统中的网络节点的数量和通信流量进行控制，可以采用以太网技术作为工业网络。

（3）IEEE 1588 对时机制。IEEE 1588 定义了一个在测量和控制网络中，与网络交流、本地计算和分配对象有关的精确同步时钟的协议（PTP）。此协议特别适合于基于以太网的系统，精度可达微秒范围。它使用时间印章来同步本地时间的机制。即使在网络通信同步控制信号产生一定的波动时，它所达到的精度仍可满足要求。通过采用这种技术，以太网 TCP/IP 不需要大的改动就可以运行于高精度的网络控制系统之中。

4.3.3 工业以太网协议简介

对应于 ISO/OSI 通信参考模型，工业以太网协议在物理层和数据链路层均与商用以太网（即

IEEE 802.3 标准）兼容，在网络层和传输层则采用了 TCP/IP 协议，可以直接和局域网的计算机互连而不要额外的硬件设备，方便数据共享，采用 IE 浏览器进行终端数据访问。工业以太网除了完成数据传输之外，往往还需要依靠所传输的数据和指令，执行某些控制计算与操作功能，由多个网络节点协调完成控制任务，它需要在应用、用户等高层协议与规范上满足开放系统的要求，满足互操作条件。

由于不存在统一的应用层协议，以太网设备中的应用程序是专用的，而不是开放的，因此设备之间还不能实现透明互访。要解决这一问题，就必须在 Ethernet+TCP（UDP）/IP 之上，制定统一的、适用于工业现场控制的应用层技术规范。已经发布的工业以太网协议主要有以下几种：EtherCAT、Profinet、HSE、Modbus TCP、Ethernet Powerlink、Ethernet/IP 等。

1. HSE（High Speed Ethernet）

HSE 是基金会现场总线摒弃原有高速总线 H2 之后推出的基于以太网的协议，也是第一个成为国际标准的以太网协议。现场总线基金会明确将 HSE 定位于实现控制网络与 Internet 的集成。由 HSE 链接设备将 H1 网段信息传送到以太网的主干上，并进一步送到企业的 ERP 和管理系统。操作员在主控室可以直接使用网络浏览器查看现场运行情况。现场设备同样也可以从网络获得控制信息。

HSE 在低四层直接采用以太网和 TCP/IP，在应用层和用户层直接采用 FF H 1 的应用层服务和功能块应用进程规范，并通过链接设备将 H1 网络连接到 HSE 网段上。HSE 链接设备同时也具有网桥和网关的功能，其网桥功能可以连接多个 H1 总线网段，使不同 H1 网段上的 H1 设备之间能够进行对等通信而无需主机系统的干预。HSE 主机可以与所有的链接设备和链接设备上挂接的 H1 设备进行通信，使操作数据能传送到远程的现场设备，并接收来自现场设备的数据信息。

2. Profinet

国际组织 PNO（Profibus National Organization）于 2001 年提出了 Profinet 规范，Profinet 将工厂自动化和企业信息管理技术有机地集成为一体，同时又完全保留了 Profibus 的开放性。它主要包含基于通用对象模型（COM）的分布式自动化系统，规定了 Profibus 和标准以太网之间的开放、透明通信，提供了一个包括设备层和系统层、独立于制造商的系统模型。

Profinet 采用以太网+TCP/IP 通信模型加上应用层来完成节点之间的通信和网络寻址。它可以同时挂接传统 Profibus 系统和新型的智能现场设备。现有的 Profibus 网段可以通过一个代理设备连接到 Profinet 当中，使整套 Profibus 设备和协议能够原封不动地在 Profinet 中使用。传统的 Profibus 设备可通过代理与 Profinet 上面的 COM 对象进行通信，并通过 OLE 自动化接口实现 COM 对象之间的调用。

3. Ethernet/IP

标准工业以太网技术的解决方案 Ethernet/IP 由 Rockwell 公司推出。Ethernet/IP 使用所有传统的以太网协议，构建于标准以太网技术之上，这意味着 Ethernet/IP 可以和现在所有的标准以太网设备透明衔接工作。Ethernet/IP 的协议由 IEEE 802.3 物理层和数据链路层标准、TCP/IP 协议组和控制与信息协议 CIP（Control Information Protocol）等 3 个部分组成，Ethernet/IP 为了提高设备间的互操作性，采用了 ControlNet 和 DeviceNet 控制网络中相同的 CIP。不同于源/目的通信模式，Ethernet/IP 采用生产者/消费者（Producer/Consumer）的通信模式，允许网络上的不同节点同时存取同一个源的数据。

4. Modbus TCP/IP

Schneider 公司于 1999 年公布了 Modbus TCP/IP。Modbus TCP/IP 并没有对 Modbus 协议本身

进行修改，但是为了满足通信实时性需要，改变了数据的传输方法和通信速率。

Modbus TCP/IP 采用简单的方式将 Modbus 帧嵌入到 TCP 帧中。这是一种面向连接的方式，每一个请求都要求一个应答。这种请求/应答的机制与 Modbus 的主/从机制相互配合，使交换式以太网具有很高的确定性。利用 TCP/ IP，通过网页的形式可以使用户界面更加友好。利用网络浏览器就可以查看企业网内部的设备运行情况。

5. EtherCAT

EtherCAT 是开放的实时以太网络通信协议，最初由德国倍福自动化有限公司（Beckhoff Automation GmbH）研发。EtherCAT 是 IEC 规范（IEC/PAS 62407）。EtherCAT 为系统的实时性能和拓扑的灵活性树立了新的标准，同时，它还符合甚至降低了现场总线的使用成本。EtherCAT 的特点还包括高精度设备同步，可选线缆冗余和功能性安全协议。

4.4 无线通信技术

无线通信系统一般由无线基站、无线终端及应用管理服务器等组成，系统采用的无线通信技术有远距离无线接入技术与短距离无线接入技术两大类。远距离无线技术的代表为 GSM、GPRS、3G，短距离无线技术的代表有 Bluetooth、Wi-Fi、IrDA、ZigBee、UWB 等。

4.4.1 GSM/GPRS/CDMA 无线通信技术

无线通信系统主要技术平台如表 4-4 所示。GSM 和 CDMA 是极为成功的技术，GSM 系统支持国际漫游、短消息和网络层互操作，是用户最多的蜂窝移动通信系统。CDMA 技术提高了无线频谱效率，把手机的复杂性转移到低成本的基带信号处理电路中，在第二代中应用于 IS-95 系统，目前得到广泛支持的第三代蜂窝移动通信标准都使用 CDMA 技术。

表 4-4　　无线通信系统主要技术平台

发展阶段	系　　统	普　通　业　务
第 1 代/1G	AMPS、TACS、NMT	语音
第 2 代/2G	GSM、TDMA、CDMA	语音业务和短消息业务
过渡代/2.5G	CDMA、GPRS、EDGE	语音业务和新引入的分组数据业务
第 3 代/3G	CDMA2000、WCDMA、TD-SCDMA	为高速多媒体数据和语音设计的分组数据业务和语音业务

（1）GSM 无线通信技术。1982 年，欧洲邮电行政会议（CEPT）设立了“移动通信特别小组”，即 GSM（Group Special Mobile），以开发第二代移动通信系统为目标。随着设备的开发和数字蜂窝移动通信网的建立，专家们将 GSM 重新命名为 Global System for Mobile Communications，即全球移动通信系统。GSM 较其以前的标准最大的不同是其信令和语音信道是全数字的，让全球各地共同使用一个移动电话网络标准，一部手机就能行遍全球。20 世纪 90 年代初，我国引进采用此项技术标准，此前一直是采用蜂窝模拟移动技术，即第一代 GSM 技术。

无线移动通信包括高速电路交换数据、通用无线分组系统、基于 GSM 网络的数据增强型移动通信技术以及通用移动通信服务。GSM 系统包括 GSM 900：900MHz、GSM1800：1800MHz 和 GSM1900：1900MHz 等几个频段。

GSM 采用了高效调制器、信道编码、交织、均衡和语音编码技术，系统具有高频谱效率，系统的容量效率（每兆赫每小区的信道数）比 TACS（全向入网通信系统）提高 3～5 倍，在门限值以上时，话音质量达到相同水平而与无线传输质量无关。GSM 标准所提供的开放性接口，不仅限

于空中接口，而且包括网络之间以及网络中个设备实体之间，通过鉴权、加密和 TMSI 号码的使用，达到安全的目的，在 SIM 卡基础上实现漫游。GSM 系统网络容量大，手机号码资源丰富、防盗拷能力好、信息灵敏、稳定性强、手机耗电量低。

GSM 无线网络系统主要由一些功能实体组成，主要包括移动台 MS（Mobile Station）、基站子系统 BSS（Base Station Subsystem）、网络和交换子系统 NSS（Network Switching Subsystem）。

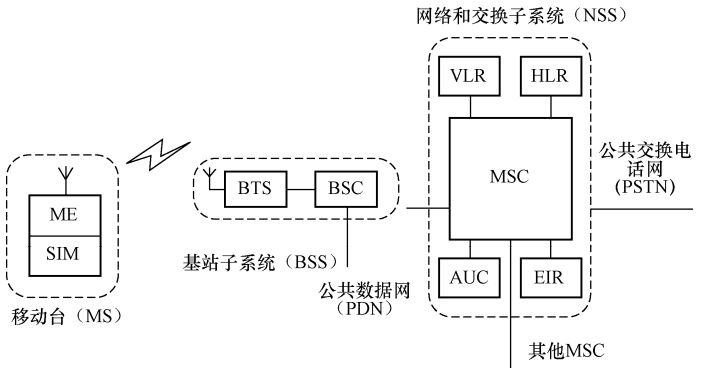

图 4-34　GSM 的参考体系结构

1）移动台 MS。MS 是用户直接使用、完成移动通信的设备。移动台由 SIM 卡与移动设备（ME）组成，两者是分离的。SIM 卡上包含所有与用户有关的无线接口的信息，也含有鉴权和加密实现的信息。移动设备可以是手持机、车载机或是由移动终端直接与终端设备相连而构成的设备。每个物理设备都有自己的识别码，即国际移动设备识别号 IMEI，由型号许可代码和厂家有关的产品号构成。每个移动用户有自己的国际移动用户识别号 IMSI，这个号码全球唯一，存储在用户的 SIM 卡上。

2）基站子系统 BSS。基站子系统 BSS 是 GSM 系统中与无线蜂窝方面关系最直接的基本组成部分，通过无线接口直接与移动台相连，负责无线发送接收和无线资源的管理，它与网络子系统 NSS 相连，实现移动用户间或移动用户与固定网路用户之间的通信连接，传送系统信息和用户信息等，在 GSM 网络的固定部分和无线部分之间提供中继。

BSS 包括基站收发信系统 BTS 和基站控制器 BSC。基站收发信系统 BTS 包括基带单元、载频单元和控制单元三部分，属于基站系统的无线部分，由 BSC 控制，服务于小区的无线收发信设备，完成 BSC 与无线信道之间的转换，实现 BTS 与 MS 之间通过空中接口的无线传输及相关的控制功能。基站控制器 BSC 是 BSS 的控制部分，在 BSS 中起交换作用。BSC 一端可与多个 BTS 相连，另一端与 MSC 和操作维护中心相连，BSC 面向无线网络，主要负责完成无线网络、无线资源管理及无线基站的监视管理，并能完成对基站子系统的操作维护功能。BSS 中的 BSC 所控制的 BTS 的数量随业务量的大小而改变。

3）网络子系统 NSS。网络子系统 NSS 主要包含有 GSM 系统的交换功能和用于用户数据与移动性管理、安全性管理所需要的数据库功能，它对 GSM 移动用户之间的通信和 GSM 移动用户与其他通信网用户之间通信起着管理作用。

网络子系统包括移动业务交换中心（MSC）、访问位置寄存器（VLR）、归属位置寄存器（HLR）、移动设备识别寄存器（EIR）和鉴权中心（AUC）。

- MSC。MSC 是网络的核心。它提供交换功能，把移动用户与固定网用户连接起来，或把

移动用户互相连接起来。MSC 从三种数据库即归属位置寄存器（HLR）、仿问位置寄存器（VLR）和鉴权中心（AUC）中取得处理用户呼叫请求所需的全部数据。反之，MSC 根据其最新数据更新数据库。

MSC 为用户提供一系列服务。电信业务，如电话、传真、紧急呼叫；承载业务，提供接入点 ISDN 协议中称为用户一网络间接口之间传输信号的能力；补充业务，如呼叫转移、呼叫限制、会议电话。

- 访问位置寄存器（VLR）。VLR 存储进入其覆盖区的移动用户的全部有关信息，使得 MSC 能够建立呼入/呼出呼叫，可以把它看做动态用户数据库。VLR 从移动用户的归属位置寄存器（HLR）处获取并存储必要的数据，一旦移动用户离开该 VLR 的控制区域，则重新在另一个 VLR 登记，原 VLR 将取消临时记录的该移动用户数据。VLR 通常与 MSC 设置在一起。
- 归属位置寄存器（HLR）。HLR 是 GSM 系统的中央数据库，存储着该 HLR 控制的所有存在移动用户的相关数据，一个 HLR 能够控制若干个移动交换区域或整个移动通信网。所有用户的重要的静态数据都存储在 HLR 中，包括移动用户识别号码、访问能力、用户类别和补充业务等数据。HLR 还存储且为 MSC 提供移动台实际漫游所在的 MSC 区域的信息（动态数据），这样就使任何入局呼叫立即按选择的路径送往被叫用户。
- 移动设备识别寄存器（EIR）。EIR 存储着移动设备的国际移动设备识别号（IMEI），通过核查白色清单、黑色清单、灰色清单这三种表格，分别列出准许使用、出现故障需监视、失窃不准使用的移动设备识别号（IMEI）。运营部门可据此确定被盗移动台的位置并将其阻断，对故障移动台能采取及时的防范措施。
- 鉴权中心（AUC）。AUC 属于 HLR 的一个功能单元部分，专用于 GSM 系统的安全性管理。鉴权中心（AUC）存储着鉴权信息与加密密钥，用来进行用户鉴权及对无线接口上的语音、数据、信令信号进行加密，防止无权用户接入，保证移动用户通信安全。

GSM 是一种多业务系统，可以依照用户的需要为用户提供各种形式的通信。电信业务的定义不仅仅取决于所传信息的特征，还涉及通信的其他特性，如传输结构、资费处理、用户的通信特点等。GSM 所提供的基本业务可分为承载业务和电信业务，这两种业务是独立的通信业务，其差别在于用户接入点的不同。

GSM 的承载业务使移动用户之间能完成数据通信，为移动用户与 PSTN 或 ISDN 用户之间提供数据通信服务，还能使 GSM 移动通信网与其他公用数据网（如公用分组数据网和公用电路数据网）实现互通。电信业务主要包括语音业务、数据业务及短消息业务 SMS（Short Message Service）等，GSM 还有各种补充业务。

（2）GPRS 无线通信技术。通用分组无线业务 GPRS（General Packet Radio Service）是在现有 GSM 系统基础上发展起来的一种移动分组数据业务。GPRS 通过在 GSM 数字移动通信网络中引入分组交换的功能实体，完成用分组方式进行数据传输。这种分组数据信道与电路交换的话音业务信道相似，在现有基站子系统基础上增加一些模块即可提供 GPRS 服务。GPRS 系统可以看作是对 GSM 电路交换系统的业务扩充，以支持移动用户利用分组数据移动终端接入 Internet 或其他分组数据网络的需求。

GSM 是一种电路交换系统，需要经过信道建立、数据传送和信道拆除 3 个过程，GPRS 是一个分组交换系统，采用存储转发的方式，可以充分利用信道资源。一个 GPRS 系统由两个子系统组成，即基站子系统和网络子系统两部分。其中，网络子系统（GPRS 骨干网）是整个系统的核心，它连接了移动网与分组业务数据网。基站子系统在原 GSM 网络中叠加一个 PCU 功能实体。

GPRS 系统结构原理图如图 4-35 所示。

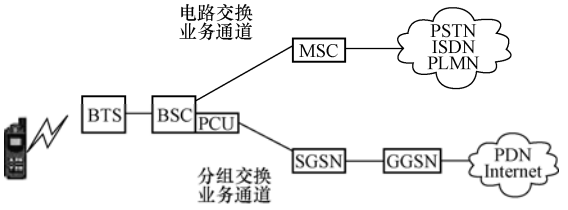

图 4-35　GPRS 系统结构原理图

分组控制单元 PCU（Packet Control Unit）是在 BSS 侧增加的一个处理单元，完成 BSS 侧的分组业务处理和分组无线信道资源的管理，PCU 一般在 BSC 和 SGSN 之间。

服务 GPRS 支持节点（Serving GPRS Support Node，SGSN）是 GPRS 网络的一个基本的组成网元，是为了提供 GPRS 业务而在 GSM 网络中引进的一个新的网元设备。其主要作用就是为本 SGSN 服务区域的 MS 进行移动性管理，并转发输入/输出的 IP 分组。SGSN 中还集成了类似于 GSM 网络中 VLR 的功能，当用户处于 GPRS 附着状态时，SGSN 中存储了同分组相关的用户信息和位置信息。同 VLR 相似，SGSN 中的大部分用户信息在位置更新过程中从 HLR 获取。

网关 GPRS 支持节点（Gateway GPRS Support Node，GGSN）也是为了在 GSM 网络中提供 GPRS 业务功能而引入的一个新的网元功能实体，提供数据包在 GPRS 网和外部数据网之间的网关接口功能。

GPRS 引入了分组交换的传输模式，用户只有在发送或接收数据期间才占用资源，这意味着多个用户可高效共享同一无线信道，从而提高了资源的利用率。GPRS 支持中、高速率数据传输，GPRS 用户能和 ISDN 用户一样快速地上网浏览。GPRS 网络接入速度快，能提供快速即时的连接，接入时间短。支持 IP 协议和 X.25 协议，可以和 IP 网、X.25 网互联互通。由于 GSM 网络覆盖面广，使得 GPRS 能提供 Internet 和其他分组网络的全球性无线接入。GPRS 的安全功能同现有的 GSM 安全功能一样。身份认证和加密功能由 SGSN 来执行。GPRS 移动设备（ME）可通过 SIM 访问 GPRS 业务，不管这个 SIM 是否具备 GPRS 功能。

GPRS 包含丰富的数据业务，如：PTP 点对点数据业务，PTM－M 点对多点广播数据业务、PTM－G 点对多点群呼数据业务、IP－M 广播业务。GPRS 可以实现基于数据流量、业务类型及服务质量等级（QoS）的计费功能，计费方式更加合理，用户使用更加方便。GPRS 被广泛应用于 Email 电子邮件、WWW 浏览、WAP 业务、电子商务、信息查询、远程监控等方面。

（3）CDMA 无线通信技术。CDMA（Code-Division Multiple Access）是码分多址的简称，是一种接入方法和空中接口的标准，是数字移动通信进程中出现的一种先进的无线扩频通信技术，它允许多个用户在相同的时间内使用相同的无线电信道或频段，每个用户都用其独有的码序列，从而与其他用户区别开来。

CDMA 最早由美国高通公司推出，CDMA 有 2 代、2.5 代和 3 代技术。在 2G 阶段，CDMA 增强型 IS95A 与 GSM 在技术体制上处于同一代产品，提供大致相同的业务，但 CDMA 技术有其独到之处，具有频谱利用率高、语音质量好、保密性强、掉话率低、电磁辐射小、容量大、覆盖广等特点。与 GPRS 技术相比，在 2.5G 阶段，CDMA 在传输速率上高于 GPRS，在新业务承载上比 GPRS 成熟，可提供更多的中、高速率的新业务。从 2.5G 向 3G 技术体制过渡上，CDMA 的过渡更为平滑。

CDMA 给每一用户分配唯一的码序列（扩频码），并用它对承载信息的信号进行编码。知道该码序列用户的接收机对收到的信号进行解码，并恢复出原始数据，用户码序列与其他用户码序列的互相关系很小。由于码序列的带宽远大于所承载信息的信号的带宽，编码过程扩展了信号的频谱，所以也称为扩频调制，所产生的信号也称为扩频信号。扩频是把频谱扩展到宽带中进行传

输的技术。由于扩频信号扩展了信号的频谱，通信系统具有抗干扰能力、抗多径能力、隐蔽性能、保密和多址能力。CDMA 按照其采用的扩频调制方式的不同，可以分为直接序列扩频（DS）、跳频扩频（FH）、跳时扩频（TH）和复合式扩频。

CDMA 被认为是第 3 代移动通信技术的首选，目前的标准有 WCDMA、CDMA2000、TD-SCDMA。W-CDMA，即 Wideband CDMA，也称为 CDMA Direct Spread，意为宽频分码多重存取，其支持者主要是以 GSM 系统为主的欧洲与日本公司，包括阿尔卡特、诺基亚以及日本的 NTT、富士通、夏普等厂商。CDMA2000 也称为 CDMA Multi-Carrier，由美国高通北美公司为主导提出，摩托罗拉、Lucent 和韩国三星都有参与，韩国现在成为该标准的主导者。TD-SCDMA 标准是由中国制定的 3G 标准。

3G 最大的优势是可以实现语音和视频的完美结合，并实现高速上网和数据传输。3G 的主导业务是数据通信。利用 3G 技术提供的高速数据传输能力，可以将工业现场图像、声音和测控信号等大量数据在无线网络上发布，让客户随时随地在移动终端上搜索和浏览所需的数据。3G 技术背景下的移动测控网络与现有固定网络、局部无线网络、2.5G 移动通信网络可实现无缝连接。

4.4.2 短距离无线通信技术

目前使用较广泛的短路距离无线通信技术均选择了 2.4GHz（2.4～2.483GHz）ISM 频段，该频段是国际规定的免费频段，无需向国际相关组织缴纳任何费用的。它们在传输速度、距离、耗电量的特殊要求方面、在功能的扩充性和特别应用需求方面以及在建立竞争技术的差异化方面各有其特点。

1. 蓝牙技术（bluetooth）

蓝牙技术诞生于 1994 年，Ericsson 开发了一种低功耗、低成本的无线接口，以建立手机及其附件间的通信，该技术还获得 PC 行业的支持。1998 年，蓝牙技术协议由 Ericsson、IBM、Intel、Nokia、Toshiba 等 5 家公司达成一致。蓝牙协议的标准版本为 802.15.1，由蓝牙小组（SIG）负责开发。802.15.1 的最初标准基于蓝牙 1.1 实现，后者已构建到现行很多蓝牙设备中。802.15.1a 基本等同于蓝牙 1.2 标准，具备一定的 QoS 特性，并完整保持后向兼容性。

蓝牙技术是一种无线数据与语音通信的开放性全球规范，它以低成本的短距离无线连接为基础，可为固定的或移动的终端设备提供廉价的接入服务。蓝牙技术实质是为固定设备或移动设备之间的通信环境建立通用的近距无线接口，将通信技术与计算机技术进一步结合，能在近距离范围内实现无线通信或操作，简化了移动通信终端设备之间、设备与 Internet 之间的通信，使得数据的传输变得更加迅速高效，为无线通信拓宽道路。蓝牙采用分散式网络结构以及快跳频和短包技术，支持点对点及点对多点通信，工作在全球通用的 2.4GHz ISM 频段，其数据速率为 1Mb/s，采用时分双工传输方案实现全双工传输。广泛应用于移动电话、PDA、无线耳机、笔记本电脑、相关外设等众多设备之间进行无线信息交换。

2. Wi-Fi 技术

Wi-Fi 速率最高可达 11Mb/s。虽然在数据安全性方面比蓝牙技术要差一些，但在电波的覆盖范围可达 100m 左右。Wi-Fi 是以太网的一种无线扩展。

最初的 IEEE802.11 规范是在 1997 年提出的，称为 802.11b，主要目的是提供 WLAN 接入，也是目前 WLAN 的主要技术标准，它的工作频率也是 2.4GHz，与无绳电话、蓝牙等许多不需频率使用许可证的无线设备共享同一频段。随着 Wi-Fi 协议如 802.11a 和 802.11g 的先后推出，Wi-Fi 的应用越来越广泛。速度更快的 802.11g 使用与 802.11b 相同的正交频分多路复用调制技术。它工作在 2.4GHz 频段，速率达 54Mb/s。

微软推出的桌面操作系统 Windows XP 和嵌入式操作系统 Windows CE，都包含了对 Wi-Fi 的支持。由于投资 802.11b 的费用低，许多厂商介入这一领域。Intel 采用 WLAN 技术的笔记本电脑芯片组，不用外接无线网卡，就可实现无线上网。

3. ZigBee 技术

ZigBee 是基于 IEEE802.15.4 标准的低功耗个域网协议。ZigBee 联盟成立于 2001 年 8 月。2002 年下半年，Invensys、Mitsubishi、Motorola 以及 Philips 半导体公司共同宣布加盟 ZigBee 联盟，以研发名为 ZigBee 的下一代无线通信标准，之后又有更多企业加入该联盟。

ZigBee 工作频段灵活。使用的频段分别为 2.4GHz、868MHz（欧洲）及 915MHz（美国），采用跳频技术。主要特点包括：数据传输速率低，只有 10～250kb/s，专注于低传输应用；功耗低，在低耗电待机模式下，两节普通 5 号干电池可使用 6 个月以上；成本低，协议简单，降低了成本；网络容量大，可支持 255 个设备，即每个 ZigBee 设备可以与另外 254 台设备相连接；有效范围小，有效覆盖范围 10～75m，具体依据实际发射功率的大小和各种不同的应用模式而定。

ZigBee 主要应用在短距离范围之内并且数据传输速率不高的设备之间。目前已在工业监控、传感器网络、家庭监控、安全系统等领域得到广泛应用。

4. IrDA 技术

IrDA 是一种利用红外线进行点对点通信的技术，是第一个实现无线个人局域网（PAN）的技术。最初 IrDA 标准的无线设备仅能在 1m 范围内以 115.2kb/s 速率传输数据，很快发展到 4Mb/s 以及 16Mb/s 的速率。IrDA 软硬件技术都很成熟，在小型移动设备，如 PDA、手机、笔记本电脑、打印机等产品上广泛使用。IrDA 通信成本低廉、体积小、功耗低、连接方便、传输上安全性高、简单易用。然而，IrDA 存在视距角度、传输距离短等问题，两个相互通信的设备之间必须对准，不适用于多台设备间的连接。

5. RFID 技术

RFID 又称电子标签、无线射频识别，是一种非接触式的自动识别技术，通过无线电信号识别特定目标并读/写相关数据，无须识别系统与特定目标之间建立机械或光学接触。通过射频信号识别目标对象并获取相关数据，识别工作无须人工干预。

雷达的改进和应用催生了 RFID 技术，1948 年哈里·斯托克曼发表的“利用反射功率的通讯”奠定了射频识别 RFID 的理论基础。RFID 系统至少包含电子标签和阅读器两部分。电子标签是射频识别系统的数据载体，电子标签由标签天线和标签专用芯片组成。依据电子标签供电方式的不同，电子标签可以分为有源电子标签、无源电子标签和半无源电子标签。有源电子标签内装有电池，无源射频标签没有内装电池，半无源电子标签部分依靠电池工作。

RFID 技术具有条形码所不具备的防水、防磁、耐高温、使用寿命长、读取距离大、标签上数据可以加密、存储数据容量更大、存储信息更改自如等优点，广泛应用于汽车、航空、军事、身份识别、医疗、制造业、物流、零售、交通、图书馆等多领域。

6. UWB 技术

超宽带 UWB 通过基带脉冲作用于天线的方式发送数据。3.1～10.6 脉冲采用脉位调制（Pulse PositionModulation，PPM）或二进制移相键控（BPSK）调制。UWB 被允许在 3.1～10.6GHz 的波段内工作。主要应用在小范围、高分辨率、能够穿透墙壁、地面和身体的雷达和图像系统中。此外，该技术适用于对速率要求非常高（大于 100 Mb/s）的 LAN 或无线个人局域网 PANs。

UWB 已在军用领域研究多年，并开发出了分辨率极高的雷达。直到 2002 年，美国联邦通信

委员会才准许该技术进入民用领域。例如，应用于汽车防撞系统中自动刹车系统的雷达及视频娱乐方面 PANs。

4.4.3 无线传感器网络

无线传感器网络（Wireless Sensor Network，WSN）是由大量的具有通信和计算能力的微小传感器节点，以无线的方式连接构成的自治测控网络。无线传感器网络是微机电系统、计算机、通信、自动控制、人工智能等多学科的综合性技术，被广泛应用于环境监测和预报、智能家居、建筑物状态监控、城市交通、大型车间和仓库管理、军事与空间探索等安全监测领域。

无线传感器网络的系统架构如下图 4-36 所示，一个典型的无线传感器网络的系统通常包括传感器节点（Sensor Node）、接收发送器汇聚节点（Sink Node）和任务管理节点。

无线传感器网络的工作原理是利用各种类型的敏感元件构成的传感器，分布于需要覆盖的领域内，组成传感器节点，用于收集数据，并且将数据路由送至信息收集节点，在传输过程中监测数据可能被多个节点处理，经过多跳后路由到汇聚节点，信息收集节点与信息处理节点通过广域网（如 Internet 或卫星网络）将数据送至地面监控中心进行统计分析和处理，并对监测结果进行综合评估。

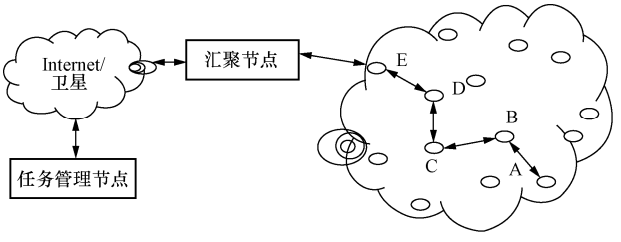

图 4-36　无线传感器网络的系统架构

无线传感器网络节点结构如图 4-37 所示，节点的基本组成包括 4 个基本单元：传感单元（由传感器和模数转换功能模块组成）、处理单元（包括 CPU、存储器、嵌入式操作系统等）、通信单元（由无线通信模块组成）以及电源。此外，可以选择的其他功能单元包括：节点定位系统、移动系统以及电源自供电系统等。

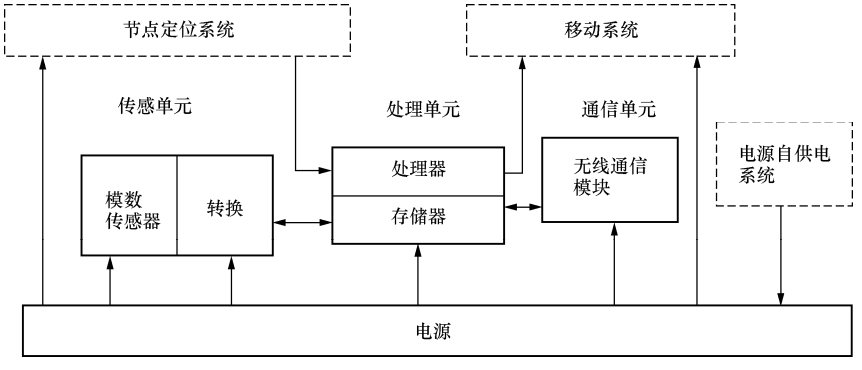

图 4-37　无线传感器网络节点

传感单元负责监测区域内信息的采集和数据转换，获取相关外界的信息；处理单元负责协调节点各部分的工作，如对传感单元获取的信息进行必要的处理、保存，控制传感单元和电源的工作模式等。通信单元负责与其他传感器节点进行无线通信，交换控制信息和收发采集数据；电源

为传感器提供正常工作所必需的能源。

无线传感器网络是当今信息领域研究的热点，研究涉及通信、组网、管理、分布式信息处理等多个方面，关键技术有路由协议、MAC 协议、拓扑控制、定位技术、时间同步、数据融合和能量管理等内容。不同于传统数据网络，无线传感器网络的设计与实现需要考虑以下几个方面问题。

（1）低能耗。传感器节点通常采用微型电池，一旦电能耗尽，节点就失去了工作能力。这要求无线传感器网络运行的过程中，每个节点都要最小化自身的能量消耗，无线传感器网络中的各项技术和协议的使用一般都以节能为前提。例如，设计采用低功耗器件，无通信任务时，切断射频部分电源，以保证获得最长工作时间。

（2）实时性。无线传感器网络应用大多有实时性的要求。例如，目标在进入监测区域之后，网络系统需要在一个很短的时间内对这一事件做出响应，以保证系统的性能。

（3）低成本。无线传感器网络的节点数量众多，在单个节点设计时，应从成本角度考虑计算、通信、数据的传递协作和存储能力，采用简单网络系统和通信协议，减少系统管理与维护的开销。

（4）安全和抗干扰。由于资源限制，针对可能产生严重的安全问题，应使用较少的能量完成数据加密、身份认证、入侵检测，保证受干扰或受损的情况下可靠完成任务。

4.5　小结

计算机网络与通信技术的发展促进了网络化测控系统的广泛应用。数据通信与测控网络技术是测控系统的基础，工业测控网络类型有很多。本章首先介绍了计算机网络与通信基本概念，对构建测控系统的信息网络、企业网络进行介绍，分别讲解了测控系统流行的现场总线技术、工业以太网技术以及无线通信技术，为后续章节网络化测控系统具体设计提供了理论基础。

思　考　题

1．简述计算机网络的基本组成。计算机网络的类型有哪些？
2．简述开放系统互连参考模型。为何计算机网络采用层次结构？
3．简述通信系统的基本组成，说明各部分的功能。
4．数字数据的编码方法有哪些？各有何特点？
5．简述局域网的基本组成与特点。
6．局域网介质访问控制方式有哪些？各有何特点？
7．简述 IEEE 802 标准基本内容。
8．简述 Intranet、Extranet 与 Internet 的区别与联系。
9．控制网络与信息网络有哪些主要集成技术？
10．什么是现场总线？现场总线技术有哪些特征？
11．CAN 总线技术有何特点？比较 CAN 总线与 RS-485 通信特性。
12．简述以太网技术特性与体系结构。
13．什么是 TCP/IP？简介 TCP/IP 参考模型及协议集。
14．传统以太网应用于工业场合存在哪些问题？
15．已经发布的工业以太网协议有哪些？

16．简述无线测控系统的分类和应用范围。
17．简要介绍 GSM 业务。说明 GSM 的参考体系结构组成。
18．GPRS 的特点有哪些？
19．近距离无线通信技术有哪些？
20．简述无线传感器网络的系统组或。画出无线传感器网络节点的组成示意图。
21．无线传感器网络的设计需要考虑哪些方面内容？