第 5 章　数据链路层

本章首先介绍数据链路层的功能，理解其差错控制和流量控制方法；然后着重介绍共享介质的多路访问控制协议，以及以太网和交换局域网等目前最流行的有线局域网技术。尽管无线局域网属于链路层范围，但本书将在第 8 章无线及移动通信中对其进行详细介绍。

5.1　数据链路层概述

数据链路层利用不可靠的物理链路向网络层提供可靠的数据链路，实现网络中两个相邻节点之间的无差错数据传输。

5.1.1　数据链路与帧

物理链路（物理线路）是由传输介质与设备组成的。原始的物理传输线路指没有采用高层差错控制的基本的物理传输介质与设备。数据链路（逻辑线路）构建在一条物理线路之上，通过一些规程或协议来控制这些数据的传输，以保证被传输数据的正确性。实现这些规程或协议的硬件和软件加到物理线路，就构成了数据链路，即从数据发送点到数据接收点所经过的传输途径。当采用复用技术时，一条物理链路上可以有多条数据链路。

运行链路层协议的设备称为节点（node），节点包括主机、路由器、交换机和 Wi-Fi 接入点。沿着通信路径连接相邻节点的通信信道称为链路（link）。数据链路层负责将数据报从一个节点通过链路传输到另一个物理连接的相邻节点。为了将一个数据报从源主机传输到目的主机，数据报必须通过沿端到端的路径来传输，一个路径由多条链路组成，此外还必须有控制规程（协议）来控制数据的传输。数据报可以在不同的链路传输，每段链路可以采用不同的链路层协议，例如，可以在第一段链路采用以太网技术，在中间链路采用帧中继技术，在最后一段链路采用 802.11 无线以太网技术。

图 5-1 所示网络中，移动终端 A 发送数据报到服务器 B，该数据报将经过 6 段链路：移动终端 A 到无线接入点之间的无线链路（Wi-Fi），无线接入点与交换机之间的以太网链路，交换机与路由器之间的链路，两台路由器之间的链路，路由器与第二层交换机之间的链路，交换机和服务器 B 之间的以太网链路。在通过特定的链路时，传输节点将数据报封装在链路层帧中，并将该帧传送到链路中。

数据链路层将数据报封装成帧，帧是数据链路层的传送单位，它将网络层的分组封装成帧，每一帧包括帧头、净荷（网络层的分组，IP 数据报）、帧尾，如图 5-2 所示。帧头包含 MAC 地址信息，以识别原主机和目标主机的 MAC 地址。

5.1.2　数据链路层功能

数据链路层是 OSI 参考模型中的第二层，介于物理层和网络层之间。数据链路层在物

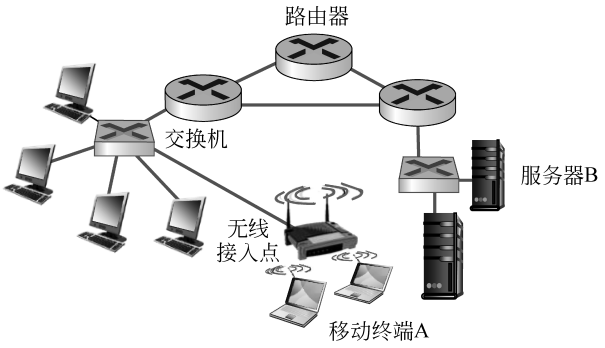


图 5-1　数据传输的不同数据链路

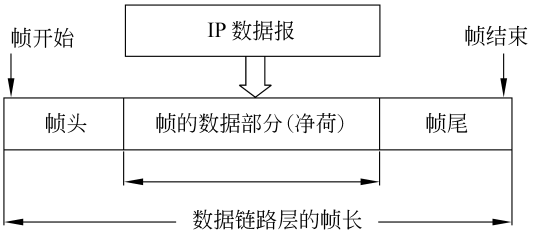


图 5-2　帧示意图

理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源自网络层的数据可靠地传输到相邻节点的目标主机网络层。其主要作用是加强物理层传输原始比特流的功能，将物理层提供的可能出错的物理连接改造成为逻辑上无差错的数据链路，使之对网络层表现为一条无差错的链路。

如图 5-3 所示，节点 A 的数据链路层把网络层传送来的 IP 数据报封装成帧，添加帧头和帧尾信息，然后将其传送给物理层的数据单元。帧头包括地址和其他控制信息，这一级的地址指的是网络中接收帧的相邻节点的物理地址。这些地址随着帧在从源节点到目的节点的路由上所经过不同的节点而发生变化。到达目的节点后，若节点 B 的数据链路层收到的帧无差错，则从收到的帧中提取出 IP 数据报交给网络层，否则丢弃这一帧。数据链路层不必考虑物理层如何实现比特传输的细节，甚至可以更简单地设想好像是沿着两个数据链路层之间的水平方向把帧直接发送给对方。

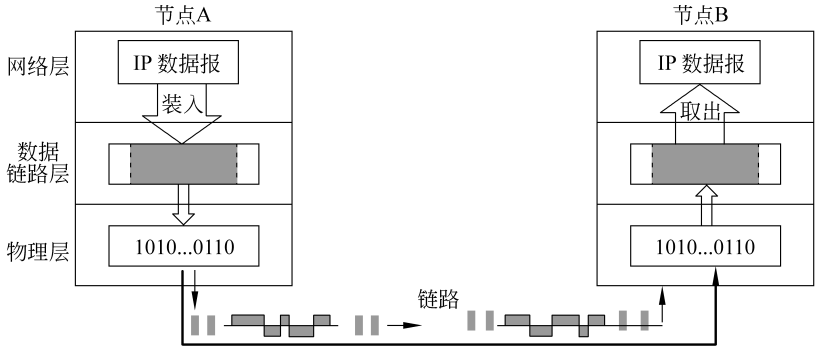


图 5-3　数据链路层帧的传输

数据链路层的功能如下。

(1) 链路管理。

链路层对数据报传输提供了不同级别的服务,从无连接、无确认服务到可靠的面向连接服务。链路管理负责数据链路的建立、维持和释放,主要用于面向连接的服务,为网络层提供链路服务。通信前,必须首先确认对方已处于就绪状态(如发送一个询问帧),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,传输完毕后则要释放连接。

(2) 封装成帧与帧同步。

数据链路层将数据报封装为数据帧,增加头部和尾部信息,然后以帧为单位发送、接收和校验数据。此外,为了能在接收方收到的比特流中明确区分出一帧,发送方必须建立和区分帧的边界(起始和终止),保证发送方与接收方帧同步。

(3) 差错控制。

数据链路层中通过检错与纠错实现对物理层传输原始比特流的功能加强,在链路层实现数据可靠传输。当接收到数据帧后,接收数据的一方对其进行检验,如果发现错误,则通知发送方重传。

(4) 流量控制。

根据接收站的接收情况,发送数据的一方实时地进行传输速率控制,避免发送数据过快,接收方来不及处理,使缓冲区溢出而丢失数据。

5.1.3 数据链路层协议

数据链路层服务和规范是按基于各种技术的多种标准和各协议所应用的介质定义的。数据链路层中的工作协议和服务是由工程组织(如 IEEE、ANSI 和 ITU)和通信公司描述的。工程组织设置公共开放式标准和协议,通信公司可能设置和使用私有协议以利用新的技术进步和市场占有。数据链路层进程将在软件和硬件中执行。该层中的各协议的实施位置为连接设备和物理网络的网络适配器电子元件。

最典型的数据链路层协议是 IEEE(Institute of Electrical and Electronics Engineers,美国电气和电子工程师协会)开发的 802 系列规范,IEEE 802 LAN/MAN 标准专用于以太网局域网、无线局域网 (WLAN)、无线个人区域网 (WPAN) 和其他类型的局域网和城域网。为了使数据链路层能更好地适应多种局域网标准,IEEE 802 系列规范将数据链路层拆成两个子层:逻辑链路控制层(Logic Link Control,LLC)和介质访问控制层(Media Access Control,MAC)。与接入传输媒体有关的内容都放在 MAC 子层,而 LLC 子层则与传输媒体无关,不管局域网采用何种协议,对 LLC 子层来说都是透明的。

LLC 子层负责建立和维护两台通信设备之间的逻辑通信链路;用户的数据链路服务通过 LLC 子层为网络层提供统一的接口。LLC 子层获取网络协议数据(通常是 IPv4 或 IPv6 数据包)并加入第二层控制信息,帮助将数据包传送到目的节点。

MAC 子层控制多个信息通道复用一个物理介质,负责数据封装和介质访问控制。它提供数据链路层寻址,并与各种物理层技术集成。最常用的方法是使用适配器(即网卡)来实现数据链路协议。MAC 子层提供对网卡的共享访问与网卡的直接通信。网卡在出厂前会被分配唯一的由 12 位十六进制数表示的 MAC 地址(物理地址),MAC 地址可提供给高

层，以在同一个局域网中的两台设备之间建立逻辑链路。

IEEE 802 参考模型已成为局域网的标准，以太网已经成为局域网的主流技术，在局域网市场中已取得了垄断地位，由于因特网发展很快而 TCP/IP 体系中经常使用的局域网只有 DIX Ethernet V2(世界上第一个局域网产品——以太网规范)，因此现在 802 委员会制定的逻辑链路控制子层 LLC(即 802.2 标准)的作用已经不大了，很多厂商生产的适配器上仅装有 MAC 协议而没有 LLC 协议。在 DIX Ethernet V2 基础上，IEEE 制定了 802.3 标准，DIX Ethernet V2 标准与 IEEE 的 802.3 标准只有很小的差别，因此可以将 802.3 局域网简称为以太网。

IEEE 802 委员会公布了许多标准，目前主要协议如下。

(1) 802.1：802 协议概论，其中 802.1A 规定了局域网体系结构，802.1B 规定了寻址、网络互联与网络管理。

(2) 802.2：LLC 协议。

(3) 802.3：以太网的 CSMA/CD(Carrier Sense Multiple Access/Collision Detect，载波监听多路访问/冲突检测) 协议，其中 802.3i 规定了 10Base-T 访问控制方法与物理层规范，802.3u 规定了 100Base-T 访问控制方法与物理层规范，802.3ab 规定了 1000Base-T 访问控制方法与物理层规范，802.3z 规定了 1000Base-SX 和 1000Base-LX 访问控制方法与物理层规范。

(4) 802.4：令牌总线(TokenBus)访问控制方法与物理层规范。

(5) 802.5：令牌环访问控制方法。

(6) 802.6：城域网访问控制方法与物理层规范。

(7) 802.7：宽带局域网访问控制方法与物理层规范。

(8) 802.8：FDDI 访问控制方法与物理层规范。

(9) 802.9：局域网上的语音/数据集成规范。

(10) 802.10：局域网安全互操作标准。

(11) 802.11：无线局域网(WLAN)标准协议。

(12) 802.12：100VG-Any 局域网访问控制方法与物理层规范。

(13) 802.14：协调混合光纤同轴网络的前端和用户站点间数据通信的协议。

(14) 802.15：无线个人网技术标准，其代表技术是蓝牙技术。

(15) 802.16：无线 MAN 空中接口规范。

5.2 差错控制和流量控制

实际通信中，差错的产生主要是由于线路本身电气特性所产生的随机噪声(热噪声)、信号振幅、频率和相位的衰减或畸变、电信号在传输介质上的反射回音效应、相邻线路的串扰、外界的电磁干扰和设备故障等因素造成的。为保证无差错通信，需要通信系统提供一种发现错误和纠正错误的机制。

5.2.1 差错检测方法

数据链路层差错检测和纠正技术主要针对的是比特差错(比特在传输过程中可能会产生差错：1可能会变成0,而0也可能变成1)。对一个节点发送到一个相邻节点的帧,检测是否出现比特差错并纠正。

数据链路层使用差错校验码来检测数据在传输过程中是否产生了比特差错。

在发送节点,将待发送数据附加若干比特的差错校验码,一起发送到链路。这里的数据包括网络层传来的数据报,以及链路级寻址信息、序列号和其他字段,保护范围包括数据的所有字段。

在接收节点,接收包含数据和差错校验码的比特序列。如果发生传输比特差错,收到数据和差错校验码可能与发送的数据和差错校验码不同。接收方根据收到的数据和差错校验码,判断收到的数据是否和初始的数据位相同,以判断数据的传输是否正确。若正确则解封取出数据报,交给网络层;若出错则进行差错处理。接收方利用收到的数据位按照规则来计算差错校验码,判断计算的差错校验码是否与收到的差错校验码相同,相同则无错误,不相同则有错误。

常见的差错检测技术包括奇偶校验方法、校验和方法,以及循环冗余校验。

(1) 奇偶校验。在待发送的数据后面添加1位奇偶校验位,使整个数据(包括所添加的校验位在内)中1的个数为奇数(奇校验)或偶数(偶校验)。

如果系统有奇数位发生误码,则奇偶性发生变化,可以检查出误码;如果有偶数位发生误码,则奇偶性不发生变化,不能检查出误码,产生漏检。

因此,奇偶校验仅能检测奇数个的错误,漏检率比较高,仅适用于异步的数据传输,计算机网络的数据链路层一般不采用这种检测方法。

(2) 校验和。校验和是在数据通信领域和数据处理的过程中,用来进行校验的一组数据项的总和。校验和差错检测基本思想是求数据的总和,将数据总和作为校验码发送到网络接收端。

在发送方,将数据的每2字节当作一个16位的整数,可分成若干整数;对所有16位的整数求和;对得到的和逐位取反,作为检查和,放在报文段首部,一起发送。

在接收方,对接收到的信息(包括校验和项)按与发送方相同的方法求和。如果结果全为1,则收到的数据无差错;如果结果中有0,则收到的数据出现差错。

校验和位数比较少,分组开销小,但是差错检测能力弱,适用于对所传数据的准确性要求不是特别高的情况,因此,校验和方法更适用于传输层(差错检测用软件实现,该方法简单、快速)。

(3) 循环冗余校验(Cyclic Redundancy Check,CRC)。CRC是一种检错能力很强的检错方法,漏检率极低,在数据通信中利用广泛,可以任意选定校验字段和信息字段的长度。CRC校验的原理是在数据码之后拼接校验码,并将原信息与校验码一同发送到接收端。

上面三种差错检测方法中,奇偶校验能力最弱,通常用于简单的串口通信;校验和通常用于网络层及其之上的层次,要求简单快速的软件实现方式;CRC校验能力最强,通常用于

数据链路层的差错检测，一般由适配器硬件实现。

5.2.2 CRC 原理

CRC 编码也称为多项式编码，把要发送的比特序列看作系数是 0 或 1 的一个多项式，对比特序列的操作看作多项式运算。在代数编码理论中，为了便于计算，把码组中各码元当作一个多项式的系数，即把$(a^{n-1},a^{n-2},\cdots,a^1,a^0)$长度为 n 的码组表示成

$$T(x)=a^{n-1}X^{n-1}+a^{n-2}X^{n-2}+a^1X+a^0$$

例如，101011 这个比特序列，如果用多项式表示，每个比特作为多项式的系数，则为 $X^5+X^3+X^1+1$。

CRC 差错检测的基本思想为：收发双方约定一个生成多项式 $G(x)$（其最高阶和最低阶系数必须为 1），发送方基于待发送的数据和生成多项式计算出差错检测码，在待传输数据帧的末尾加上校验位一起传输，使带校验位的帧的多项式能被 $G(x)$整除；接收方收到后，用生成多项式 $G(x)$除以带校验位的帧，若有余数，则产生了误码。

设发送节点要把数据 D（m 比特）发送给接收节点。校验位计算算法如下。

(1) 发送方和接收方先共同选定一个生成多项式 $G(x)$（$r+1$ 比特），最高有效位（最左边）是 1。设 $G(x)$为 r 阶，则在数据帧的末尾加 r 个 0，即 $D\times 2^r$，使帧为 $m+r$ 位，相应多项式为 $x^rM(x)$。

(2) 按模 2 除法，用生成多项式 $G(x)$的各项系数构成的位串作为除数，去除对应于 $x^rM(x)$的位串，余数为 $R(x)$。（注：模 2 除法，加法没有进位，减法没有借位。加法和减法都等同于异或运算。）

(3) 将对应于 $x^rM(x)$的位串与余数 $R(x)$进行异或运算，结果就是要传送的带校验和的多项式 $T(x)$，$T(x)=x^rM(x)+R(x)$，亦即发送方传送带校验位的帧为 $D\times 2^r$ xor R（D 为待传输数据，R 是由 $D\times 2^r$ 除以 $G(x)$位串的余数）。

在接收方，用生成多项式 $G(x)$去除接收到的 $T(x)$（$m+r$ 比特），如果余数不为 0，则传输发生差错；如果余数为 0，则传输正确，去掉尾部 r 位，得到所需数据 D。

CRC 编码可以用软件实现，但通常用硬件实现 CRC 的编码、译码和判错。

数学分析表明，当 $G(x)$具有某些特点时，才能检测出各种不同错误。为了能对不同场合下的各种错误模式进行校验，已经研究出了几种 CRC 生成多项式的国际标准，常见的有 8 位、16 位、32 位生成多项式 G；8 位 CRC（CRC-8）用于 ATM 信元首部的保护；32 位 CRC（CRC-32）用于大量链路层 IEEE 协议。

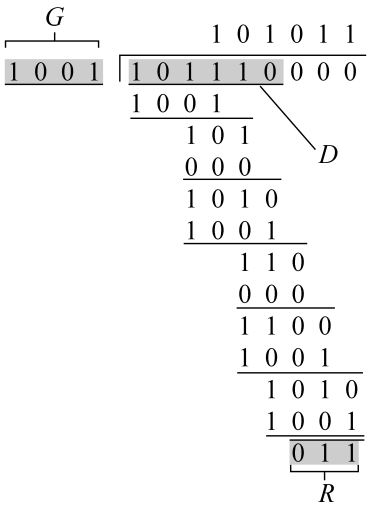
CRC-8 生成多项式为 $G(X)=X^8+X^5+X^4+1$。

CRC-16 生成多项式为 $G(X)=X^{16}+X^{12}+X^5+1$。

CRC-32 生成多项式为 $G(X)=X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$。

【例 5-1】 考虑 CRC 算法。假设生成多项式 $G(X)=X^3+1$（$r=3$），数据有效负载（D）是 101110，则与该数据有效载荷相关的 CRC 位如何计算？实际发送的帧是什么？

解 $G(x)$为 3 阶，首先取 D 值 101110，乘以 2^3，即在帧的低位端加上 3 个 0，则帧为 9 位，101110000。然后，用模 2 算法将这个数字除以生成多项式位串 $G=1001$。除法后的最后余数 R 是 CRC 位，则实际发送的帧 $T(x)$为 101110011。计算结果如下。



值得注意的是，在数据链路层若仅使用循环冗余校验 CRC 差错检测技术，则只能做到对帧的比特进行差错检验，并不能保证数据链路层向网络层提供“可靠传输”的服务。通常传输差错除了比特差错外，可能收到的帧并没有出现比特差错，但却出现了帧丢失、帧重复或帧失序。OSI 要求数据链路层做到可靠传输，在 CRC 检错的基础上，增加了帧按序编号、确认和重传机制。收到正确的帧就要向发送端发送确认。发送端在一定的期限内若没有收到对方的确认，就认为出现了差错，需要进行重传，直到收到对方的确认为止。这种方法在早期的数据链路层协议中曾经起到很好的作用。但现在通信线路的质量已经大大提高了，由通信链路质量问题引起差错的概率已经大大降低。因此，因特网广泛使用的数据链路层协议都不使用确认和重传机制。如果在数据链路层传输数据时出现了差错并且需要进行改正，则由上层协议（传输层的 TCP）来完成纠错任务。

5.2.3 流量控制

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，如若此时不对发送方的发送速率（即链路上的信息流量）作适当的限制，前面来不及接收的帧将被后面不断发送来的帧“淹没”，造成帧的丢失，从而出错。因此，流量控制实际上是对发送方数据流量的控制，使其发送速率不超过接收方能够处理的能力。流量控制并不是数据链路层所特有的功能，许多高层协议中也提供流量控制功能，数据链路层的流量控制是点对点的，控制的是相邻两节点之间数据链路上的流量；而传输层的流量控制是端到端的，控制的是从源主机到目的主机之间端的流量。

流量控制需要通过某种反馈机制使发送方知道接收方是否能跟上发送方，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，在什么情况下必须暂停发送，要等待收到某种反馈信息后继续发送。常用的流量控制方法是停止等待（stop and wait）和滑动窗口（sliding window）等机制。

停止等待机制指每发送完一个帧就停止发送，等待对方的确认，在收到确认后再发送下一个帧，传输效率较低。

滑动窗口机制是发送方在收到确认帧前可以发送若干帧。发送方允许连续发送的帧的序号，称为发送窗口，用来对发送方进行流量控制，发送窗口的大小代表在还未收到对方确认信息的情况下发送方最多还可以发送多少个数据帧；接收方允许接收帧的序号，称为接收窗口，用于控制可以接收哪些数据帧。只有收到的数据帧的序号在接收窗口内时，才允许将该数据帧收下，否则将其丢弃。窗口在数据传输过程中根据控制向前滑动，只有接收窗口向前滑动，同时接收方发送了确认帧时，发送方收到确认帧后，发送窗口才有可能向前滑动，从而控制数据传输过程，并对发送方在收到接收方的确认之前能够传输的帧数目进行了限制。

5.3 介质访问控制协议

目前网络中的链路可分为两类：一类是点对点链路，即链路两端各一个节点，一个发送数据、另一个接收数据，如点对点协议 PPP；另一类是广播链路，即多个节点连接到一个共享的广播信道，广播信道中的每个节点都可能发送和接收数据帧，如果多个节点同时向共享信道发送数据，会导致信道中的信号相互干扰，使数据帧不能正确接收，因此，需要解决如何协调多个发送和接收节点对共享广播信道的访问，即多路访问控制问题，相关技术称为多路访问协议。广播链路常用于局域网中，如早期的以太网和无线局域网。数据链路层中介质访问控制（MAC）子层，用于实现广播链路中的信道分配，解决信道争用问题。

5.3.1 MAC 协议

理想的 MAC 协议是给定速率为 R bps 的广播信道，期望当只有一个节点传输数据时，它可以以速率 R 发送；当有 M 个节点期望发送数据时，每个节点发送数据的平均速率是 R/M。介质访问实现完全分散控制，无须特定节点协调。

目前已有的 MAC 协议有三种类型，分别是信道划分 MAC 协议、随机访问 MAC 协议和轮转 MAC 协议。

1. 信道划分 MAC 协议

采用多路复用技术把信道划分为小片（时隙），给节点分配专用的小片。目前主要的信道划分协议包括时分多路接入（TDMA）、频分多路接入（FDMA）、码分多路接入（CDMA）等。

（1）时分多路接入的基本思想是将时间划分为时间帧，每个时间帧再划分为 N 个时隙（长度＝分组传输时间），分别分配给 N 个节点。每个节点只在固定分配的时隙中传输，周期性接入信道。TDMA 的特点是能避免冲突，将链路资源进行公平分配，每个节点专用速率 R/N bps；但是节点速率有限（R/N bps），当其他节点没有数据要传输时，需要发送数据的节点也不能充分利用链路资源。因此，TDMA 的效率不高，节点必须等待其传输时隙到来时才能发送数据。

（2）频分多路接入的基本思想是将总信道带宽划分为若干频带（带宽为 R/N），分别分配给 N 个节点，每个站点分配一个固定的频带，无空闲传输频带。FDMA 的特点是可以避免冲突，实现链路资源的公平分配；但是，每个节点可以占用的带宽有限（R/N），效率不高。

（3）码分多路接入（CDMA）的基本思想如下：每个节点分配一个唯一的编码，每个节点用其唯一的编码对发送的数据进行编码，允许多个节点“共存”，信号可叠加，即可以同时

传输数据。

2. 随机访问 MAC 协议

随机访问协议的基本思想是信道不划分。当节点要发送分组时，利用信道全部数据速率 R 发送分组。发送数据前，节点间没有协调，两个或多个节点同时传输会产生冲突。在发生冲突时，采用冲突恢复机制，冲突的每个节点分别等待一个随机时间，再重发，直到帧（分组）发送成功。

随机访问 MAC 协议需要定义如何检测冲突，以及如何从冲突中恢复。目前典型随机访问协议有 ALOHA 协议、载波监听多路访问协议（Carrier Sense Multiple Access，CSMA）、带冲突检测的载波监听多路访问协议（CSMA with Collision Detection，CSMA/CD）、冲突避免的载波监听多路访问协议（CSMA with Collision Avoidance，CSMA/CA）。

ALOHA 是夏威夷大学研制的一个无线电广播通信网，采用星型拓扑结构，使地理上分散的用户通过无线电来使用中心主机。中心主机通过下行信道向其他主机广播分组；非中心主机通过上行信道向中心主机发送分组（可能会冲突，无线电信道是一个公用信道）。

目前以太网广泛使用的是 CSMA/CD 协议，无线以太网 802.11 中采用的协议是 CSMA/CA，将在 5.3.2 节和 5.3.3 节详细介绍。

3. 轮转 MAC 协议

轮转链路访问控制协议的基本思想是让节点轮流使用信道，包括轮询协议和令牌传递协议两种。

（1）轮询方法是主节点轮流“邀请”从属节点发送数据。轮询协议要求首先从连入共享信道的节点中选择一个作为主节点，其余节点为从节点。主节点以循环的方式轮询每个节点。例如主节点首先向节点 1 发送一个报文，告诉它（节点 1）最大能够传输多少帧。如果节点 1 有数据要发送，则最多可发送允许的最大帧数；然后主节点会继续询问节点 2、节点 3。轮询的优点是消除了随机访问的碰撞问题；其缺点是引入了额外的开销，如果主节点有故障，整个信道都不能工作。

（2）令牌传递协议的基本思想是控制令牌依次从一个节点传递到下一个节点，只有获得令牌的节点才能够发送数据。令牌是一个小的特殊帧，在节点之间以某种固定的次序进行传递。当一个节点收到令牌时，如果有数据帧要传输，则发送允许的最大帧数，然后把令牌转发给下一个节点；如果没有数据帧要传输，则立即向下一个节点转发该令牌。令牌传递协议的缺点是存在令牌开销和等待延迟，以及单节点故障可能会使整个信道崩溃等问题。

5.3.2 CSMA/CD 协议

多路访问协议的目的是协调多个节点在共享广播信道上的传输，避免多个节点同时使用信道，发生冲突（指两个以上的节点同时传输帧，使接收方收不到正确的帧），产生互相干扰。

载波监听多路访问（CSMA）协议的设计思想是：某个节点在发送帧之前，先监听信道。若信道空闲，则该节点开始传输数据帧；若信道忙，即有其他节点正向信道发送帧，则该节点推迟发送，随机等待一段时间，然后侦听信道。

在 CSMA 协议中，节点没有进行冲突检测，即使发生了冲突，节点仍继续传输帧。但该帧已经被破坏，是无用的帧，信道传输时间被浪费。因此，研究者进一步提出了带冲突检测

的 CSMA 机制，即 CSMA/CD 协议。该机制设计了“载波侦听”和“冲突检测”两个规则。

CSMA/CD 协议的基本原理是在传输数据帧的同时进行冲突检测，即节点传输数据同时侦听信道，如果检测到有其他节点正在传输帧，发生冲突，立即停止传输，并用某种方法来决定何时再重新传输。CSMA/CD 协议设计的目的是缩短无效传送时间，提高信道的利用率。CSMA/CD 协议的特点是控制原理简单，控制流程容易实现（代价小），但是当节点多时，碰撞频繁，信道利用率低，属竞争型、有冲突协议。

以太网通过分布式、随机争用型介质访问控制方法 CSMA/CD 来协调各节点数据传输有序地运行。

1. 数据发送流程

数据发送流程如图 5-4 所示。发送节点执行“载波侦听，冲突检测，冲突处理，延迟重发”的过程。

（1）载波侦听。

节点要通过总线发送数据时，先通过载波侦听来确定总线是否空闲。以太网物理层规定发送的数据采用曼彻斯特（Manchester）编码方式，Manchester 编码每一位的中间有一跳变，从低到高跳变表示 1，从高到低跳变表示 0，因此节点可通过判断总线电平是否跳变来确定总线的忙闲状态，总线上没有电平跳变则总线空闲，否则总线忙。节点要发送数据帧，并且此时总线处于空闲状态，则该节点可以启动发送。

（2）冲突检测。

节点发送数据的同时要进行冲突检测，从物理层看，冲突检测指总线上同时出现两个或以上发送信号，叠加后的信号波形将不等于任何一个节点发送的信号波形。常见的冲突检测方法有两种：一种是比较法，发送节点在发送帧的同时，将其发送信号波形与从总线上接收到的信号波形进行比较，若相同则说明没有发生冲突；另一种是编码违例判断法，两个按照 Manchester 编码的无关信号叠加后一般不会再符合其编码规则，因此节点可检查从总线上接收到的信号波形是否符合 Manchester 编码规则，从而判定是否产生冲突。

冲突窗口是以太网组网技术的重要参数之一。冲突窗口，也称为争用期，是节点发送数据后可以检测到冲突的最长时间，指从发送站发送数据到网络上最远的站之间两倍的信号传播时间 2τ，其中 $\tau=D/V$，D 为总线的最大长度，V 是电磁波在介质中的传播速度。如果超过时间 2τ 没有检测到冲突，就肯定没有发生冲突，因此定义 2τ 为冲突窗口。由于以太网的物理层协议对总线的最大长度作了规定，电磁波在介质中的传播速度也是确定的，因此冲突窗口值也是确定的。IEEE 802.3 协议给出 10Mbps 以太网的冲突窗口为 51.2μs。对于 10Mbps 以太网，在冲突窗口内可发送 512 比特，即 64 字节，也就是说在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。

（3）冲突处理。

当发现冲突时，继续发送若干比特的拥塞信号，使网络中所有节点都能检测出冲突并立即丢弃冲突帧，进入停止发送随机延迟重发流程。以太网协议规定一帧的最大重发数 16，如果小于 16，允许节点随机延迟再重发；如果超过 16，认为线路故障。也就是说，当冲突次数超过 16 时，表示发送失败，放弃该帧发送。

（4）延迟重发。

当允许节点随机延迟再重发时，为了公平解决信道争用问题，需要确定延迟发送时间。