第3章 数据链路层

【本章主要内容】

数据链路层是计算机网络体系结构中的第二层。本章讨论的内容局限于一个局域网，即在一个局域网中数据帧从一个设备转发到另一个设备，中间没有路由器。有路由器的网络，是一个广域网的概念，将在第4章网络层中讨论。

本章首先介绍数据链路层上的三个基本问题和常用的点对点协议(PPP)，然后用较大的篇幅讨论共享信道的局域网和有关的协议，最后简单介绍无线局域网。本章重要的内容如下：

(1) 数据链路层的点对点信道和广播信道的特点，以及这两种信道所使用的协议(PPP以及CSMA/CD协议)的特点。

(2) 数据链路层的三个基本问题：封装成帧、透明传输和差错检测。

(3) 以太网MAC层的硬件地址。

(4) 适配器、转发器、集线器、网桥、以太网交换机的作用以及使用场合。

(5) 无线网络特点及CSMA/CA协议的工作机制。

3.1 数据链路层概述

图3-1展示了主机 H_1 发送数据包给主机 H_2。可以看到中间经过了路由器 R_1、R_2 和 R_3。如第1章所述，真实的数据流动如图3-1(b)所示。主机 H_1 到主机 H_2 的路径上，由4段链路组成，即 $H_1 \rightarrow R_1$、$R_1 \rightarrow R_2$、$R_2 \rightarrow R_3$ 和 $R_3 \rightarrow H_2$。这4段链路可能使用不同的传输介质和数据链路层协议。我们在数据链路层上只讨论一段链路上的数据传输。

3.1.1 点对点信道与广播信道

数据链路层使用的信道主要有如下两种。

(1) **点对点信道**。这种信道使用一对一的点对点通信方式。

(2) **广播信道**。多个设备连接到一个共享信道上，任一结点发送数据，都会被其他结点收到，也就是广播信道的由来。这种信道上会有冲突的发生，因此必须设计特殊的信道使用协议来协调主机的数据发送，这个过程比较复杂，是本章的重点内容。

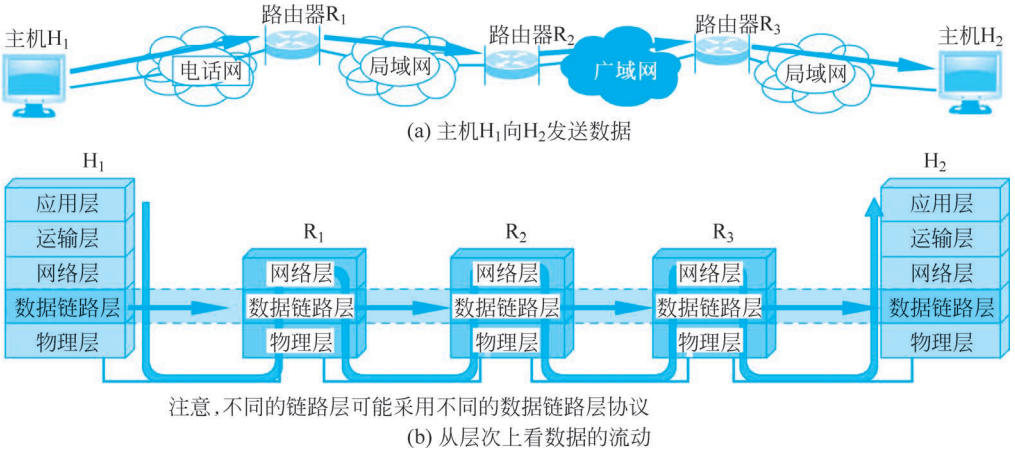

图 3-1 数据链路层的地位

3.1.2 数据链路和帧

首先介绍链路和数据链路的概念。

链路(link)就是从一个结点到相邻结点的一段物理线路,这可以是有线线路,也可以是无线线路,而且不经过任何其他的交换或转发结点。链路也称为物理链路。当信源和信宿之间距离比较远时,一般它们之间的路径由多个链路组成,如图 3-1 所示,H_1 和 H_2 之间的路径上有 4 段链路。

当在一条链路上传输数据时,仅有一条物理线路是不行的,还需要一些协议来控制数据的传输。物理线路可以看成硬件,而协议可以看成软件,硬件和软件就组成了数据链路。也就是把控制通信的协议加载到物理链路上,就组成了数据链路。网络适配器一般简称为网卡,它既包括硬件(看得见的硬件电路),也包括软件(驱动程序)。网络适配器既实现了物理层的功能,也实现了数据链路层的功能。数据链路也称为逻辑链路。

和物理层一样,数据链路层的协议也称为规程。

下面再介绍数据链路层的协议数据单元——帧。如图 3-2 所示,结点 A 的数据链路层把网络层交付下来的 IP 数据报加上帧的首部和尾部构成帧发送到链路上,结点 B 把接收到的帧的首部和尾部剔除并对数据进行校验,将 IP 数据报提取出来上交给网络层。

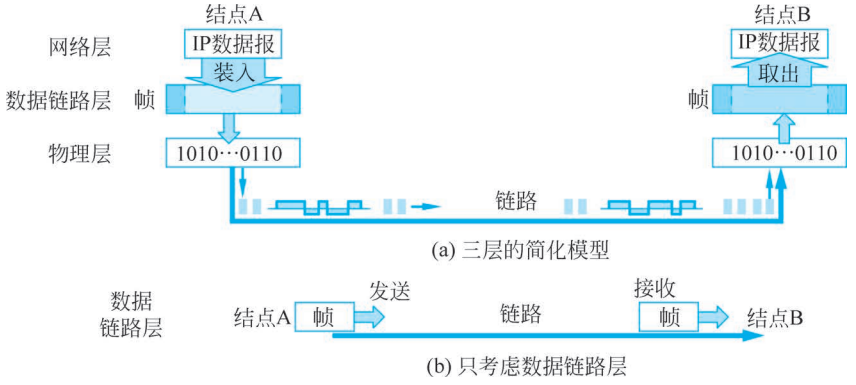

图 3-2 使用点对点信道的数据链路层

3.1.3　三个基本问题

数据链路层需要解决三个基本问题：**封装成帧、透明传输和差错检测**。下面分别讨论这三个基本问题。

1. 封装成帧

封装成帧就是给一段数据添加首部和尾部，形成一个帧。接收端在收到物理层交付的比特流后，可以根据首部和尾部的标记，从比特流中识别帧的开始和结束。一个帧的帧长度等于帧的数据部分长度加上帧首部和帧尾部的长度。很明显，首部和尾部的一个重要作用就是进行帧定界（即确定帧的开始和结束）。此外，一般首部和尾部还包括一些必要的控制信息，如校验、地址等。发送帧时，从帧首部开始发送。显然，为了尽可能地提高传输效率，帧的数据部分长度应尽可能地大于首部和尾部的长度。

各种数据链路层协议对帧首部和帧尾部的格式有明确的规定。同时，链路层协议规定了帧的数据部分长度上限——**最大传送单元**（Maximum Transfer Unit，MTU）。需要强调的是，MTU 是数据链路层的帧可以载荷的数据部分的最大长度，而不是帧的总长度。图 3-3 给出了帧的首部和尾部的位置，以及帧的数据部分与 MTU 的关系。

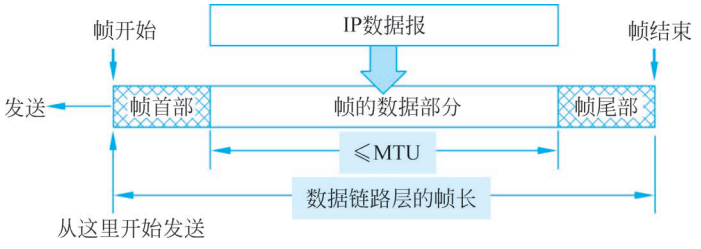

图 3-3　封装成帧

当数据部分由可打印的 ASCII 码组成时，帧的首部和尾部可以使用特殊的控制字符。如图 3-4 所示，控制字符 SOH（Start Of Header）放在一帧的最前面，表示帧的首部开始。另一个控制字符 EOT（End Of Transmission）表示帧的结束。注意，SOH 和 EOT 的十六进制编码分别是 0x01（二进制是 00000001）和 0x04（二进制是 00000100）。此外，与帧定界符无关的其他控制信息在图 3-4 中都省略了。

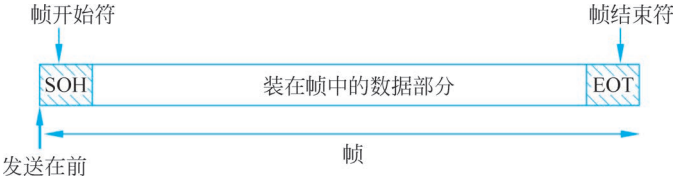

图 3-4　用控制字符进行帧定界

2. 透明传输

数据部分的字符如果是帧定界的控制字符，就会被误认为这是一个帧的开始或结束，从而就会出现帧定界错误。如图 3-5 所示，数据部分的 EOT 会被当作帧结束的标记。这就要求数据部分不能出现控制字符，而这并不符合“透明传输”的概念。所谓**透明传输**是指上层传下来的数据，不管是什么形式的比特组合都必须能够正确传输。

“透明”的意思指某一个实际存在的事物看起来好像不存在一样，例如玻璃是透明的。

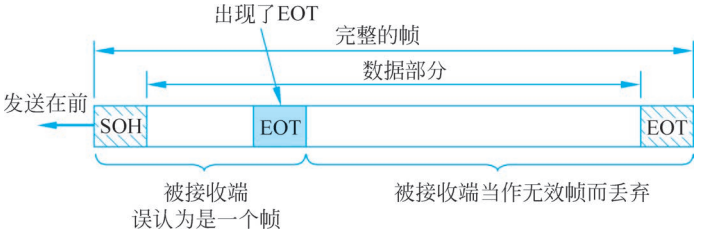

图 3-5 数据部分恰好出现与 EOT 一样的代码

“在数据链路层透明传送数据”的含义是无论什么样的数据，都能够按照原样没有差错地通过这个数据链路层，就好像这个数据链路不存在一样。

解决透明传输问题的关键是数据中的控制字符(SOH 和 EOT)不要被误认为用于帧定界的控制字符。如图 3-6 所示，可以利用字节填充法来解决透明传输的问题。发送端在数据中的控制字符 SOH 或 EOT 的前面插入一个转义字符 ESC(其编码是 0x1B)，如果数据中有转义字符 ESC，也在其前面插入一个转义字符，接收方则进行相反的动作。即在收到转义字符＋控制字符时就将转义字符剔除。这种方法称为**字节填充**或**字符填充**。

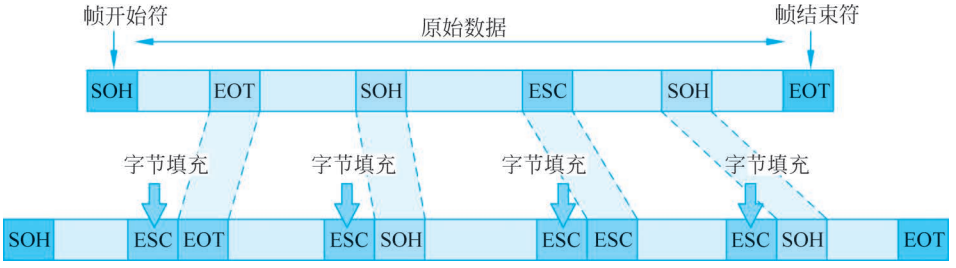

图 3-6 用字节填充法解决透明传输的问题

3. 差错检测

虽然随着技术的进步，出错的概率越来越低，但是现实的通信线路传输数据肯定会发生差错。错误比特数和总比特数的比值称为误码率(Bit Error Rate，BER)。例如，误码率为 10^{-10} 表示平均每传送 10^{10} 比特就会出现 1 比特错误。当然，可以通过技术手段使误码率降低。但实际信道绝非理想的信道，误码率不可能下降为 0。因此，在实际信道的数据传输中，必须采用各种差错检测措施，使用各种差错检测码，甚至在星际通信中使用纠错码。下面介绍广泛使用的**循环冗余校验**(Cyclic Redundancy Check，CRC)。

循环冗余校验中每 k 比特为一组，需要在这 k 比特数据后面加上 n 位冗余码，一起发送出去。一共需要发送 $k+n$ 位。可以看到多发送了 n 比特的数据，但是可以进行差错检测，当信道传输有可能发生差错时，这种代价还是值得的。

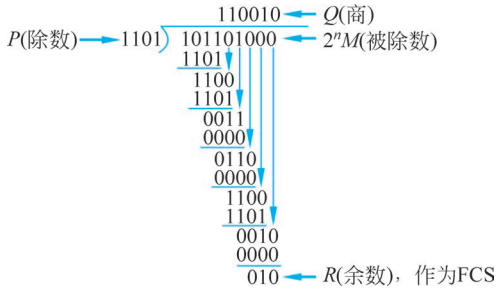

图 3-7 CRC 原理的例子

假设要传送的数据 $M=101101$，这时 $k=6$。下面是 n 位冗余码的获取方法。M 的后面增加 n 个 0，得到一个 $k+n$ 位的数。这个 $k+n$ 位的数用模 2 除法除以事先约定好的 $(n+1)$ 位的除数 P。得到结果商是 Q 而余数是 R(n 位，比 P 少一位，如果 R 的位数不足 n 位，则前面补 0 补足 n 位)。计算过程如图 3-7 所示。在这个例子中，$P=1101$，$n=3$，余数 $R=10$，前面补一个 0。

此时，$R=010$，刚好 3 位。R 就是冗余码。将 R 拼接在 M 的后面组成 101101010 发送出去。为了进行检错而添加的冗余码被称为**帧检验序列**(Frame Check Sequence，FCS)。注意，FCS 和 CRC 并不等同，FCS 可以用 CRC 获得，也可以利用其他方式获得。

接收端的检验过程如下：把收到的 $k+n$ 位的数据用模 2 除法除以 P，得到余数 R。若 R 等于 0，则很大概率数据传输过程中是没有差错的。若 R 不等于 0，则数据传输中一定发生了差错。发生差错后，余数 R 仍然是 0 的这种情况被称为漏检。精心设计的校验方案可以让漏检的概率很小。所以，实际上接收端检验最后的判断过程是，若 $R=0$，则判定没有差错，新收到的数据被接收。若 $R\neq0$，则判定发生了差错，将新收到的数据丢弃。

前面例子中除数 $P=1101$，也可以用多项式表示：$P(X)=1X^3+1X^2+0X^1+1X^0=X^3+X^2+1$。$P(X)$被称为生成多项式。另外，上述生成帧校验序列和检验过程都可以利用硬件完成，所以速度非常快。

数据链路层并不需要向网络层提供“可靠传输”的服务。这里的“可靠传输”是指数据链路层的发送端发送什么，在接收时就收到什么。

传输差错可分为两大类，前面描述的某些比特发生错误称为比特差错，是其中一类。而另一类传输差错则更复杂些，如收到的帧没有比特差错，而是**帧丢失**、**帧重复**或**帧失序**。例如，发送方顺序发送了三个帧：[＃1]，[＃2]，[＃3]。接收端对收到的每个帧进行校验，发现没有比特差错。第一种情况，接收方顺序收到[＃1]和[＃3]([＃2]丢失了)，这种情况就是帧丢失。第二种情况，接收方顺序收到[＃1]，[＃2]，[＃2]，[＃3](收到两个[＃2])，这种情况就是帧重复。第三种情况，接收方顺序收到[＃1]，[＃3]，[＃2]，可以看到后发送的帧反而先到达接收端，这种情况就是帧失序。可以看到，“无比特差错”与“无传输差错”并不是一个含义。在数据链路层使用 CRC 检验，能够实现无比特差错的传输，但数据链路层并没有提供可靠传输服务。

OSI 的观点是让数据链路层向上提供可靠传输。历史上，通信线路质量较差时，数据链路层在检错的基础上，增加了帧编号、确认和重传等机制，以提供可靠传输。关于可靠传输的工作原理，可以参考第 5 章。

现在有线传输线路一般通信质量较好，数据链路层协议不使用确认和重传机制，对比特差错的数据帧直接丢弃，这种效率反而比较高。这种情况下，可靠传输的任务由运输层负责。

3.2　PPP

在早期，由于通信线路质量较差，需要可靠传输协议，如高级数据链路控制(High-level DataLink Control，HDLC)。随着技术的进步，线路质量越来越好，出现差错的概率已经很低，这时传输效率是首要考虑因素，对于点对点的链路，简单的点对点协议(Point-to-Point Protocol，PPP)是目前使用得最广泛的数据链路层协议。一般情况下，用户通过连接某个 ISP 接入互联网。而 PPP 就是用户的计算机和 ISP 进行通信时所使用的数据链路层协议，如图 3-8 所示。

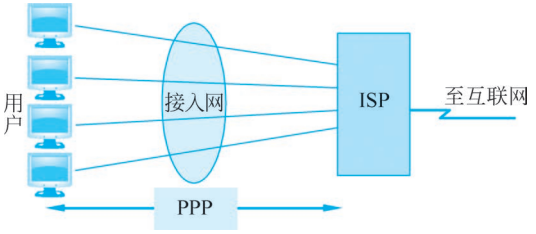

图 3-8　用户到 ISP 的链路使用 PPP

3.2.1 PPP 的特点

PPP 于 1994 年成为互联网的正式标准，其特点如下。

(1) **简单**。PPP 对数据链路层的帧，不需要纠错，不需要序号，也不需要流量控制。PPP 的实现非常简单：接收方每收到一个帧，就进行 CRC 检验。如果 CRC 检验正确，就收下这个帧；反之，就丢弃这个帧，其他什么也不做。简单的设计使得协议的稳定性很好。

(2) **封装成帧**。这是数据链路层必须实现的功能。PPP 规定特殊的字符作为帧定界符，以便使接收端从收到的比特流中能准确地找出帧的开始符和结束符。

(3) **透明性**。PPP 保证数据传输的透明性，也就是用户想传什么数据都可以。

(4) **多种网络层协议**。PPP 同时支持多种网络层协议(如 IP 和 IPX 等)。当点对点链路所连接的是局域网或路由器时，PPP 必须同时支持在链路所连接的局域网或路由器上运行的各种网络层协议。

(5) **多种类型链路**。PPP 能够在多种类型的链路上运行。例如，串行的或并行的、同步的或异步的、低速的或高速的、电的或光的、交换的或非交换的链路。

1999 年公布的在以太网上运行的 PPP，即 PPP over Ethernet，简称 PPPoE。PPPoE 是为宽带上网的主机使用的链路层协议。这个协议把 PPP 再封装在以太网帧中(当然还要增加一些能够识别各用户的功能)。宽带上网时由于数据传输速率较高，因此可以让多个连接在以太网上的用户共享一条到 ISP 的宽带链路。

(6) **差错检测**。PPP 具备差错检测的功能，对出错的数据帧，立即丢弃。

(7) **检测连接状态**。PPP 能够检测对端设备是否处于正常状态、有没有突然死机。

(8) **最大传送单元**。PPP 可以协商并设置最大传送单元(MTU)。如果要发送的分组过长并超过 MTU 的限制，PPP 就要丢弃这样的帧，并返回差错。

(9) **网络层地址协商**。PPP 需要提供一种机制使通信的两个网络层的实体能够通过协商或配置彼此的网络层地址。该机制应尽可能简单且有效。

(10) **数据压缩协商**。PPP 需要提供一种机制来协商使用数据压缩算法。

PPP 不需纠错，不需要编号，也不需流量控制。PPP 不支持多点线路，而只支持点对点的链路通信。PPP 只支持全双工链路。

3.2.2 PPP 的组成

PPP 由如下三部分组成。

(1) 一个将上层数据报封装到串行链路的方法。PPP 既支持异步链路，也支持面向比特的同步链路。

(2) 一个用来建立、配置和测试数据链路连接的**链路控制协议**(Link Control Protocol，LCP)。通信的双方可协商一些选项。

(3) 一套**网络控制协议**(Network Control Protocol，NCP)，其中的每个协议都支持不同的网络层协议，如 IP、OSI 的网络层、DECnet 和 AppleTalk 等。

3.2.3 PPP 的帧格式

PPP 的帧格式如图 3-9 所示。PPP 帧的首部和尾部分别为 4 个字段(5 字节)和 2 个字

段(3 字节)。第一个字段和最后一个字段都是标志字段 F(flag),规定为 0x7E,表示一个帧的开始或结束。连续两帧之间只需要用一个标志字段。如果出现连续两个标志字段,就表示这是一个空帧,应当丢弃。地址字段 A 规定为 0xFF,控制字段 C 规定为 0x03。PPP 最初设计时,打算以后对这两个字段进行定义,但一直没有后续定义。

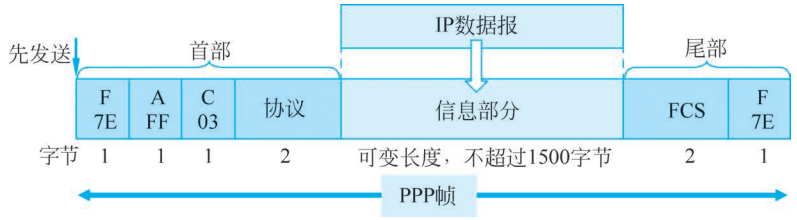

图 3-9　PPP 的帧格式

协议字段的长度为 2 字节,表示数据部分的内容。当协议字段为 0x0021 时,PPP 的数据部分就是 IP 数据报。若为 0xC021 时,则数据部分是 PPP 链路控制协议的数据,而 0x8021 表示这是网络层的控制数据。数据部分的长度是可变的,但不超过 1500 字节。尾部中 FCS 的长度为 2 字节,使用 CRC。

3.2.4　PPP 的字节填充与零比特填充

1. 字节填充

PPP 异步传输时,使用转义字符 0x7D,通过字节填充从而实现透明传输。具体方法如下:

(1) 数据部分的 0x7E(标志字段)转变成为 2 字节数据(0x7D,0x5E)。

(2) 数据部分的 0x7D(即出现了转义字符)转变成为 2 字节数据(0x7D,0x5D)。

(3) 在数据部分的 ASCII 码控制字符(即小于 0x20 的字符)前面插入一个 0x7D,同时将该字符的编码加以改变。例如,出现 0x03(“传输结束”ETX)就要把它转变为 2 字节序列(0x7D,0x23)。

2. 零比特填充

PPP 在 SONET/SDH 链路上,使用同步传输。在同步传输时,PPP 采用**零比特填充**方法来实现透明传输。如图 3-10 所示,发送端扫描整个数据部分,只要发现有 5 个连续 1,则立即填入一个 0。经过上面的填充处理,数据部分肯定不会出现 6 个连续 1。接收端在收到一个帧时,连续的 6 个 1 肯定是标志字段 F。在数据部分,发现 5 个连续 1 时,就把 5 个连续 1 后的一个 0 删除。这样就保证了透明传输。

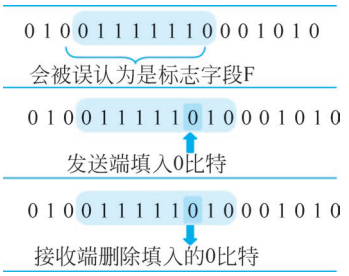

图 3-10　零比特的填充与删除

3.2.5　PPP 的工作状态

PPP 的工作过程如图 3-11 所示。“链路静止”状态是 PPP 链路的起始和终止状态,这表示计算机和 ISP 的路由器之间还没有物理层的连接。当计算机通过调制解调器向路由器拨号时,路由器就可以检测到调制解调器发出的载波信号。

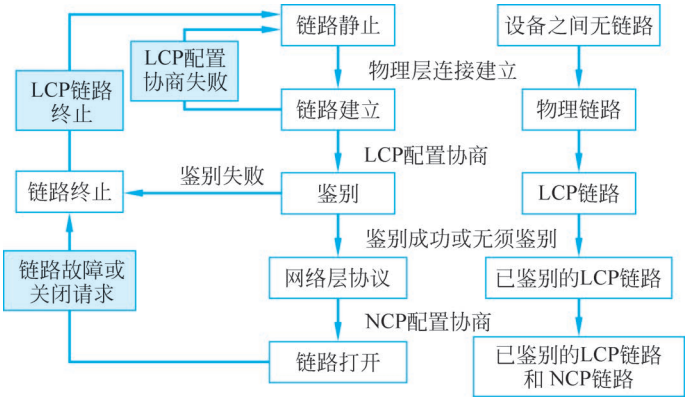

图 3-11　PPP 的工作过程

在双方建立了物理层连接后，PPP 就进入“链路建立”状态。下面进行 LCP 配置协商，即发送 LCP 的配置请求帧。配置请求信息被封装在配置请求帧中。LCP 配置选项包括链路上的最大帧长、鉴别协议，以及不使用 PPP 帧中的地址和控制字段。

协商结束后双方建立 LCP 链路，就进入“鉴别”状态。在这一状态下，只允许传送 LCP 的分组、鉴别协议的分组以及监测链路质量的分组。若使用口令鉴别协议（PAP），则需要通信发起方提供身份标识符和口令。系统可允许用户重试若干次。如果需要更高级别的安全，则可使用更加复杂的挑战握手认证协议（CHAP）。若鉴别身份失败，则转到“链路终止”状态。若鉴别成功，则进入“网络层协议”状态。

在“网络层协议”状态，链路两端的网络控制协议（NCP）根据不同的网络层协议互相交换网络层特定的网络控制分组。PPP 链路两端的网络层可以运行不同的网络层协议，可使用同一个 PPP 进行通信。如果在 PPP 链路上运行的是 IP，需要对 PPP 链路的每一端配置 IP 模块。在低速链路上运行时，双方还可以协商使用压缩的 TCP 和 IP 首部，以减少在链路上发送的比特数。

当网络层配置完毕后，链路就进入可进行数据通信的“链路打开”状态。链路的两个 PPP 端点可以彼此向对方发送分组。两个 PPP 端点还可发送回送请求 LCP 分组和回送回答 LCP 分组，以检查链路的状态。

数据传输结束后，链路任一端发出终止请求 LCP 分组请求终止链路连接，在收到对方发来的终止确认 LCP 分组后，转到“链路终止”状态。如果链路出现故障，则也会从“链路打开”状态转到“链路终止”状态。当调制解调器的载波停止后，则回到“链路静止”状态。

图 3-11 右侧方框给出了对 PPP 几个状态的说明。从设备之间无链路开始到先建立物理链路，再建立链路控制协议 LCP 链路。经过鉴别后再建立网络控制协议链路，然后才能交换数据。由此可见，PPP 已不是纯数据链路层的协议，它还包含了物理层和网络层的内容。

3.3　使用广播信道的数据链路层

局域网是在 20 世纪 70 年代末发展起来的。早期的局域网使用的是广播信道。广播信道可以进行一对多的通信。局域网技术在计算机网络中占有非常重要的地位。

3.3.1　局域网的数据链路层

局域网一般为一个单位所拥有，覆盖范围有限，站点数目比较少。一般具有较高的数据速率、较低的时延和较低的误码率。如图 3-12 所示，局域网按网络拓扑有**星形**、**环形**和**总线型**。早期的局域网是总线型和环形。随着网络技术的演进，集线器和交换机的出现，星形网获得了广泛的应用。

图 3-12　局域网的拓扑

局域网的传输媒体可以是同轴电缆、双绞线和光纤，也可以是无线电。早期多使用同轴电缆，现在双绞线占主导地位，如果要求速率更高，则可以使用光纤。实际上局域网的内容涵盖物理层和数据链路层。

局域网使用广播信道，也就是共享信道。因此，一个非常重要的问题是协调局域网中结点访问共享信道而不发生冲突。一般有如下两种方法。

(1) **静态划分信道**。利用频分复用、时分复用、波分复用和码分复用等技术静态地为用户划分信道。用户分配了信道后，就不会和其他用户发生冲突，但代价较高，不适合于局域网。

(2) **动态媒体接入控制**，也就是信道并非固定地分配给每个用户，而是动态分配。这又分为如下两类。

① **受控接入**。受控接入的特点是用户需要在一定的控制规则下发送数据。例如令牌环局域网和集中控制的多点线路探询(也称为轮询)。令牌环局域网中有一个令牌，令牌绕环网传递，想要发送数据的结点截获令牌从而发送数据帧。发送的数据绕环一周，回到发送结点，发送结点再把令牌释放到环上。轮询则有一个控制机器，循环地询问其他结点有没有发送数据帧的需求。如果有结点有发送数据帧的需求，则在被询问时发送数据帧。受控接入因为比较简单且在局域网中使用较少，后文不再讨论。

② **随机接入**。随机接入的特点是所有用户可以随机地发送信息。但如果有两个或两个以上的站点在同一时刻发送数据，就会发生冲突(碰撞)，导致这些站点的发送都失败。随机接入是本章的重点内容。

10Mb/s 速率的以太网一般被称为传统以太网，采用广播信道实现数据的传输。下面结合传统以太网讨论广播信道的数据链路层涉及的几个问题。

1. 以太网的两个主要标准

1980 年 9 月，DEC 公司、英特尔(Intel)公司和施乐(Xerox)公司联合提出了 10Mb/s 以太网规约的第一个版本 DIX Ethernet V1(DIX 是这三个公司名称首字母组合)。1982 年又修改为第二版，即 **DIX Ethernet V2，其成为世界上第一个局域网产品的规约**。

在此基础上，IEEE (Institute of Electrical and Electronics Engineers) 802 委员会的

802.3 工作组于 1983 年制定了**第一个 IEEE 的以太网标准 IEEE 802.3**，数据速率为 10Mb/s。IEEE 802.3 工作组对以太网标准的帧格式做了很小的改动，允许基于这两种标准的硬件实现可以在同一个局域网上互操作。以太网的两个标准 DIX Ethernet V2 与 IEEE 802.3 标准只有很小的差别。严格来讲，“以太网”应当是指符合 DIX Ethernet V2 标准的局域网，在不严格的情况下，IEEE 802.3 局域网也可以称为“以太网”。

实际上，IEEE 802 委员会并没有制定一个统一的局域网标准，而是制定了多个局域网标准，如 802.4 工作组制定的令牌总线网、802.5 工作组制定的令牌环网等。为了多个局域网标准互容，IEEE 802 委员会把局域网的数据链路层拆分成两个子层，即**逻辑链路控制**（Logical Link Control，LLC）子层和**媒体接入控制**（Medium Access Control，MAC）子层。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。不管采用何种传输媒体和 MAC 子层的局域网，对 LLC 子层来说都是透明的，如图 3-13 所示。

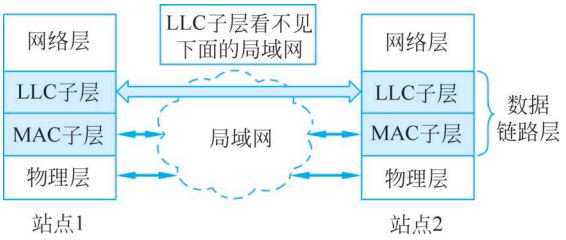

图 3-13　局域网对 LLC 子层是透明的

随着技术的演进，以太网占据了主导地位，目前使用最多的局域网只剩下 DIX Ethernet V2，而不是 IEEE 802 委员会制定的几种局域网。IEEE 802 委员会制定的逻辑链路控制子层（即 IEEE 802.2 标准）的作用已经消失了，很多厂商生产的适配器上就仅装有 MAC 协议，而没有 LLC 协议。

2. 网络适配器

计算机通过网络适配器与外界局域网连接，其也被称为**网卡**。网卡是在主机箱内插入的一块网络接口板，现在很多计算机的网卡集成在主板上。计算机内部数据以并行方式传输，适配器和外部通信采用串行传输的方式进行。所以，适配器要进行数据串并转换。另外，为了适配网络和总线上的数据速率，适配器还要有对数据缓存的功能。适配器的驱动程序安装在操作系统中。适配器还要能够实现以太网协议。

网络适配器完成了数据链路层和物理层两个层次的功能，实际上，因为现在芯片的集成度很高，很难将适配器的数据链路层和物理层的功能划分开。

适配器和计算机的 CPU 并行工作。当适配器收到帧时自动进行地址匹配，自动进行校验，如果出现差错，则直接丢弃差错帧；适配器收到正确的帧时，利用中断的方式通知计算机，并交付给网络层。适配器在接收和发送数据帧时，不需要使用计算机的 CPU。当网络层要发送数据时，将数据报交付给适配器，适配器封装成帧，发送出去。在计算机网络中，会用到两个地址：一个是硬件地址，其存储在适配器的 ROM 中；另一个是 IP 地址，其存储在计算机的存储器中，如图 3-14 所示。


视频讲解

3.3.2　CSMA/CD 协议

最早的以太网是总线型网，多台计算机连接到共享总线上。总线天然具有广播特性。

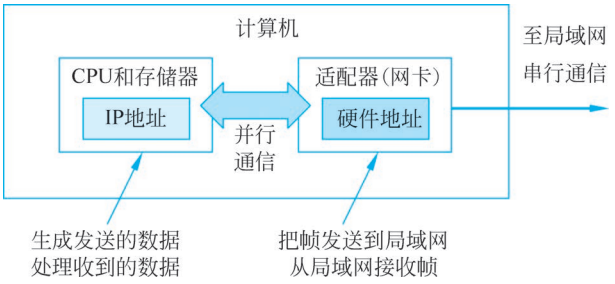

图 3-14　网络适配器

在总线上怎么实现一对一通信呢？每个计算机的网络适配器都有一个独一无二的硬件地址，每个站点仅仅接收目的地址是自己的帧，而对其他帧则丢弃。这个接收动作是由硬件（网络适配器）自动完成的。这样就可以在总线上实现一对一的通信。需要注意，在总线型网上，同一时刻只能允许一台计算机发送数据，否则各计算机发送的数据之间就会互相干扰，使得所发送数据被破坏。

为了简便，以太网使用了如下两种措施。

第一，通信采用无连接的工作方式，即不必先建立连接。对发送的帧不编号，也不要求对方确认。以太网提供的是尽最大努力的交付，也就是不可靠的交付。当收到的数据帧校验有差错时，就把帧丢弃，其他什么也不做。对丢弃的数据帧是否需要重传则由高层来决定，例如，由 TCP 负责。

第二，以太网发送的数据使用曼彻斯特编码。曼彻斯特编码带有自同步信号。但曼彻斯特编码所占的频带宽度比原始的基带信号增加了一倍。

以太网协议的工作非常类似于大家在一个教室里面讨论问题。在这个讨论中没有老师或者管理者，想发言的人都可以随时发言。但是有两个要求：如果想发言时，别人正在发言，则需要等待，这个可以被称为“先听后说”；如果碰巧有两个甚至更多的人同时发言，那么大家意识到这问题后，就停止发言，这个可以被称为“边说边听”。

以太网使用的协议是 CSMA/CD，意思是带碰撞检测的载波监听多路访问（Carrier Sense Multiple Access with Collision Detection）。“**多路访问**”表示这是总线型网络，多个站点共同连接到一个共享总线上。“**载波监听**”就是“边发送边监听”。载波监听发送数据前或发送数据中，每个站需要不断地检测信道，以便发现有没有其他站点也在发送数据。“**碰撞检测**”的具体操作是边发送数据边检测信道上信号电压的情况。当两个或多于两个站点同时发送数据时，总线上的信号电压变化幅度将会增大。当信号电压变化幅度超过门限值时，就认为这时至少有两个站点在同时发送数据，发生了碰撞。所谓“碰撞”就是发生了冲突，因此“碰撞检测”也称为“冲突检测”。

每个站点检测到信道空闲后发送数据，也会发生碰撞。这非常类似于会议讨论中，一旦会场安静，偶尔也会发生几个人同时抢着发言而产生冲突的情况。

让我们看图 3-15 所示的例子。图 3-15 中的局域网两端的站点 A 和 B 的距离为 s。电磁波在电缆中的传播时延为 $\tau=s/v$，v 为电信号在电缆中的传播速度。

在 $t=0$ 时，A 有数据发送，检测信道，信道空闲，开始发送数据。

在 $t=\tau-\delta$（这里 $\tau>\delta>0$）时，A 发送的数据还没有传播到 B，B 也有数据要发送，B 检测到信道是空闲的，因此 B 发送数据。

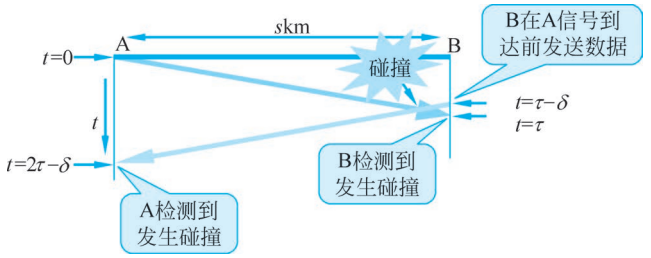

图 3-15 传播时延对载波监听的影响

经过时间 $\delta/2$ 后，即在 $t=\tau-\delta/2$ 时，A 发送的数据和 B 发送的数据发生了碰撞，但这时 A 和 B 都不知道发生了碰撞。

在 $t=\tau$ 时，A 发送的数据传播到 B，B 检测到发生了碰撞，于是停止发送数据。

在 $t=2\tau-\delta$ 时，A 也检测到发生了碰撞，因而也停止发送数据。

A 和 B 发送数据均失败，都要推迟一段时间再重新发送。

可以看到 A 发出的数据，在 τ 时间后才能传播到 B。如果 B 在 A 的数据到达 B 之前发送自己的帧（这时 B 的载波监听是检测不到 A 所发送的信息），则必然发生碰撞。碰撞的结果是两个帧都变得无用。所以，发送数据的站点经过 2τ 的时间才知道有没有发生碰撞。经过 2τ 的时间，数据才可以传播到最远的站点。**由于局域网上任意两个站点之间的传播时延有长有短，因此按最坏情况设计，即取总线两端的两个站点之间的传播时延（这两个站点之间的距离最大）为端到端传播时延**。

另外，在图 3-15 中，如果站点 A 在 $2\tau-\delta$ 时间点已经完成了数据帧的发送，这时，站点 A 是检测不到冲突的。站点 A 会误认为这次数据发送成功。所以，站点 A 不能在 $2\tau-\delta$ 时间点前完成数据帧的发送，其中 δ 可以认为是一个无穷小量。也就是，站点 A 不能在 2τ 时间点前完成数据帧的发送。假设数据帧长为 L，以太网的数据速率为 C，则有

$$\frac{L}{C} \geqslant 2\tau \tag{3-1}$$

显然，在使用 CSMA/CD 协议时，一个站点不可能同时进行发送和接收（但必须边发送边监听信道）。因此，使用 CSMA/CD 协议的以太网不可能进行全双工通信而只能进行双向交替通信（半双工通信）。

可以看到，即使检测到信道空闲，也有可能发生冲突。同时，以太网也不能保证在检测到信道空闲后的某一时间内，一定能够把自己的数据成功地发送出去。以太网的这一特点称为发送的不确定性。如果希望在以太网上发生碰撞的机会很小，则必须使整个以太网的平均通信量远小于以太网的最高数据速率。

以太网的端到端往返时间 2τ 称为**争用期**，它是一个很重要的参数。争用期又称为**碰撞窗口**。这是因为一个站点在发送数据时，只有通过争用期的“考验”，即经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞。这时，就可以放心把这一数据顺利发送完毕。

以太网使用**截断二进制指数退避**（truncated binary exponential back off）算法来确定碰撞后重传的时机。截断二进制指数退避算法让发生碰撞的站点不是等待信道空闲后就立即再发送数据，而是退避一个随机的时间。立即再发送会导致冲突的多个站点再次发生碰撞。

截断二进制指数退避算法尽可能降低重传时再次发生冲突的概率，可以很好地解决这个问题。

退避算法的规定如下。

(1) 基本退避时间为争用期 2τ。对于 10Mb/s 以太网，具体的争用期时间是 51.2μs，在争用期内可发送 512 比特，即 64 字节。也可以说争用期是 512 比特时间。1 比特时间就是发送 1 比特所需的时间。所以，这种时间单位与数据速率密切相关。为了方便，也可以直接使用比特作为争用期的单位。争用期是 512 比特，即争用期是发送 512 比特所需的时间。

(2) 从离散的整数集合[0，1，…，(2^k-1)]中随机选取一个数，记为 r。重传应推后的时间就是 r 倍的争用期。参数 k 按式(3-2)计算：

$$k=\min(\text{重传次数},10) \tag{3-2}$$

可见，当重传次数不超过 10 时，参数 k 等于重传次数；但当重传次数超过 10 时，k 就不再增大而一直等于 10。

(3) 当重传达 16 次仍不能成功时，则丢弃该帧，并向高层报告。

例如，在第 1 次重传时，$k=1$，随机数 r 从整数{0，1}中选一个数。因此，重传的站点可选择的重传推迟时间是 0 或 2τ，在这两个时间中随机选择一个。若再发生碰撞，则在第 2 次重传时，$k=2$，随机数 r 就从整数{0，1，2，3}中选一个数。因此，重传推迟的时间是在 0、2τ、4τ 和 6τ 这 4 个时间中随机地选取一个。同样，若再发生碰撞，则重传时 $k=3$，随机数 r 就从整数{0，1，2，3，4，5，6，7}中选一个数。以此类推。

若多次发生冲突，就表明网络比较拥挤。使用上述退避算法可使重传推迟时间加大，从而降低发生碰撞的概率。适配器对过去发生过的碰撞并无记忆功能。这种退避算法有可能使得后到的数据帧先被发送。例如，当好几个适配器正在执行指数退避算法时，很可能有某一个适配器发送的新帧能够碰巧立即成功地插入信道中，得到了发送权，而已经推迟好几次发送的站点，有可能很不巧，还要继续执行退避算法，继续等待。

式(3-1)中，$L\geqslant 2\tau\times C=51.2\mu s\times 10Mb/s=512b=64B$。所以，**以太网中一个帧的长度最短为 64 字节，即 512 比特。如果帧长少于 64 字节，那么必须加入一些填充字节，使帧长不小于 64 字节。对于 10Mb/s 以太网，发送 512 比特的时间需要 51.2μs，也就是上面提到的争用期。**

以太网在发送数据时，如果在争用期(对应前面 64 字节)没有发生碰撞，那么后续发送的数据就一定不会发生冲突。换句话说，如果发生碰撞，就一定是在发送的前 64 字节之内。由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节，因此凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。只要收到了这种无效帧，就应当立即将其丢弃。

信号在以太网上传播 1km 大约需要 5μs。以太网上最大的端到端时延必须小于争用期的一半(即 25.6μs)，这相当于以太网的最大端到端长度约为 5km。实际上的以太网覆盖范围远远没有这样大。因此，实际的以太网都能在争用期 51.2μs 内检测到可能发生的碰撞。

下面介绍强化碰撞的概念。当发送数据的站点一旦发现了碰撞时，除了立即停止发送数据，还要再继续发送 32 比特或 48 比特的人为干扰信号(jamming signal)，以便让所有用户都知道现在已经发生了碰撞，如图 3-16 所示。对于 10Mb/s 以太网，发送 32(或 48)比特只需要 3.2(或 4.8)μs。

以太网还规定了帧间最小间隔为 9.6μs，相当于 96 比特时间。这样做是为了使刚刚收

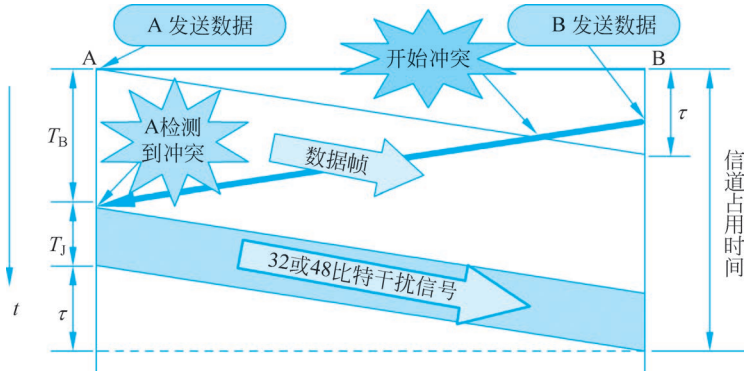

图 3-16　人为干扰信号的加入

到数据帧的站点的接收缓存来得及清理，做好接收下一帧的准备。

CSMA/CD 协议的要点归纳如下。

（1）准备发送：网络适配器从网络层获得一个分组，加上以太网的首部和尾部，组成以太网帧，放入适配器的缓存中，然后先检测信道。

（2）若检测到信道忙，则继续不停地检测，一直等待信道转为空闲。此时若在 96 比特时间内信道保持空闲（保证了帧间最小间隔），就发送这个帧。

（3）在发送过程中仍不停地检测信道，即网络适配器要边发送边监听。这里有两种可能：

① 如果一直未检测到碰撞，就认为发送成功，回到（1）。

② 检测到碰撞，这时立即停止发送，并发送人为干扰信号。适配器执行指数退避算法，等待 r 倍 512 比特时间后，返回到步骤（2），继续检测信道。若重传达 16 次仍不能成功，则停止重传而向上层报错。

3.3.3　10Base-T 双绞线以太网

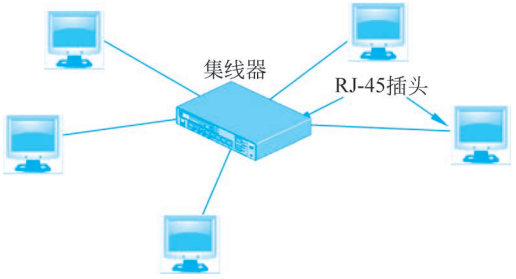

图 3-17　使用集线器的双绞线以太网

以太网的传输介质从最初的粗同轴电缆，到细同轴电缆，再到最后双绞线，价格越来越便宜、可靠性越来越高。双绞线以太网是一种星形拓扑的以太网，在星形的中心的设备叫作**集线器**（hub），如图 3-17 所示。每个计算机使用两对无屏蔽双绞线，用于发送和接收数据。双绞线的两端使用 RJ-45 插头。1990 年，IEEE 制定出星形以太网 10Base-T 的标准 802.3i。其中，“10”代表 10Mb/s 的数据速率，Base 表示基带传输，T 代表双绞线。

10Base-T 以太网每个站点到集线器的距离不超过 100m。10Base-T 双绞线以太网的出现，是局域网发展史上一个非常重要的里程碑。以太网的拓扑从总线型变为更加方便的星形网络，而以太网也就在局域网中占据了统治地位。粗缆和细缆以太网现在都已成为历史，并已从市场上消失了。

集线器的特点如下。

（1）使用集线器的以太网，表面上看是一个星形网，在逻辑上是一个总线型网，各站点共享逻辑上的总线，使用的还是 CSMA/CD 协议。网络中的各站点竞争对传输媒体的使用，并且在同一时刻至多只允许一个站点发送数据。

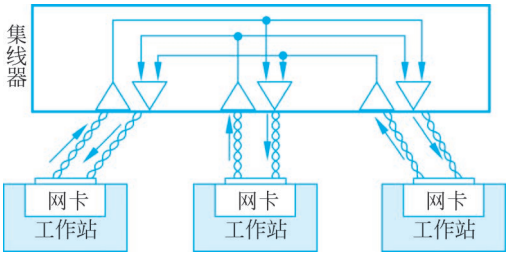

图 3-18　具有三个端口的集线器

（2）一个集线器有很多端口（见图 3-18），例如，8～16 个，每个端口通过 RJ-45 插头和计算机互连。因此，一个集线器实际上是一个多端口的转发器。

（3）集线器工作在物理层，它的每个端口仅仅简单地接收和转发，接收什么数据就转发什么数据，并不进行碰撞检测。

（4）集线器采用了专门的芯片，进行自适应串音回波抵消。集线器的性能非常可靠。另外，现在可以使用 4～8 个堆叠式集线器堆叠起来一起使用。有些集线器具有少量的容错能力和网络管理功能。

IEEE 802.3 标准还可使用光纤作为传输媒体，相应的标准是 10Base-F 系列，F 代表光纤。

3.3.4　以太网的信道利用率

假定一个以太网上有 10 个站点，直观上每个站点分得的平均速率应该是总数据速率的 1/10。实际上，远没有这么大。以太网的实际速率一般比标称的速率低很多，每个站点分得的速率会更低。出现这样结果的原因是，以太网随机接入的方式会导致碰撞。碰撞发生时，信道资源实际上被浪费掉了。以太网上站点数目越多，这种碰撞发生的概率就越大。

图 3-19 是以太网的信道被占用的情况。一个站点监听到信道空闲，开始发送帧。但是前面 2τ（τ 是单程端到端传播时延）的时间是争用期，争用期内可能发生碰撞。如图 3-19 所示，经过一个争用期，发生了碰撞，又经过一个争用期，又发生了碰撞。经过若干争用期，终于有一个站点争得发送数据的权利，并发送成功。图 3-19 中 T_0 表示数据帧的传输时间。

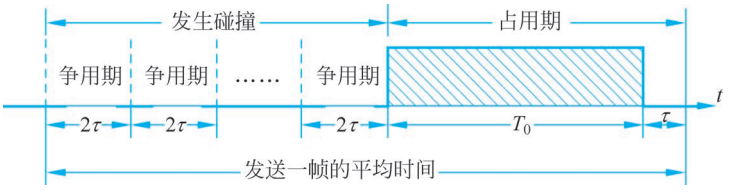

图 3-19　以太网的信道被占用的情况

注意，成功发送一个帧后还有 τ 的时间信道是被占用的，这是因为站点发送完最后一个比特后，这个比特还需要 τ 的时间在以太网上传播。因此，必须在经过时间 $T_0+\tau$ 后信道才能完全进入空闲状态。图 3-19 展示了发送一个帧的情况，可以看到要提高以太网的信道利用率，就必须减小 τ 与 T_0 的比值。该比值在以太网中被定义为参数 a。

$$a=\frac{\tau}{T_0} \tag{3-3}$$

当 a 很小趋近于 0 时，表示碰撞发生后可以立即检测出来，然后站点停止发送，因而信

道资源的浪费就非常少。反之，若 a 比较大，表示争用期所占的比例就比较大，在这种情况下，只要发生碰撞就浪费比较多的信道资源，从而使信道利用率不高。因此，参数 a 应当尽可能小些。参数 a 比较小，就表示 τ 比较小，然后就表示结点之间的距离比较小。另外，参数 a 比较小，就表示 T_0 不能太小，也就是以太网的帧长不能太短。

假设网络不发生碰撞，且网络一有空闲就有站点发送数据，这时可以得到极限信道利用率 S_{max} 为

$$S_{max}=\frac{T_0}{T_0+\tau}=\frac{1}{1+a} \tag{3-4}$$

式(3-4)也表明 a 的值越小越好。

实际上，随机控制的以太网的信道利用率非常低。当以太网的利用率达到 30%时就已经处于重载的情况。

3.3.5 MAC 地址

IEEE 802 标准为局域网规定了一种 48 位的全球地址，其被固化在适配器的 ROM 中。该地址称为硬件地址，又称为物理地址或 MAC 地址。如果连接在局域网上的主机或路由器有多个网络适配器，那么这个主机或路由器就有多个“地址”。实际上，这种 48 位“地址”应当是某个接口的标识符。

IEEE 802 标准规定 MAC 地址字段可采用 6 字节(48 位)或 2 字节(16 位)这两种中的一种。6 字节地址字段对局部范围内使用的局域网的确是太长了，但是由于 6 字节的地址字段可使全世界所有的网络适配器都具有不相同的地址，因此现在的局域网适配器实际上使用的都是 6 字节 MAC 地址。

现在 IEEE 的注册管理机构 RA 是局域网全球地址的法定管理机构，它负责分配地址字段的 6 字节中的前 3 字节(即高位 24 位)。世界上凡要生产网络适配器的厂家都必须向 IEEE 购买由这前 3 字节构成的地址块。这前 3 字节的正式名称是组织唯一标识符(OUI)，通常也叫作公司标识符。现实的情况是，一个公司可能购买多个 OUI，也可能几个小公司合起来购买一个 OUI，所以，24 位的 OUI 不能够单独用来标志一个公司。地址字段中的后 3 字节(即低位 24 位)则可由厂家自行指派，称为扩展标识符，要保证生产出的适配器没有重复地址。购买了一个 OUI，就可以生成 2^{24} 个不同的 6 字节(48 位)MAC 地址，这种地址又称为 EUI-48，这里 EUI 表示扩展的唯一标识符。在生产适配器时，这种 6 字节的 MAC 地址已被固化在适配器的 ROM 中。因此，MAC 地址也叫作硬件地址(hardware address)或物理地址。

IEEE 规定地址字段的第一字节的最低有效位为 I/G 位。I/G 表示 individual/group。当 I/G 位为 0 时，地址字段表示单个站点地址。当 I/G 位为 1 时表示组地址，用来进行多播。IEEE 还考虑可能有人并不愿意向 IEEE 的 RA 购买 OUI。为此，IEEE 把地址字段第一字节的最低第二位规定为 G/L 位，表示 global/local。当 G/L 位为 0 时是全球管理(保证在全球没有相同的地址)，厂商向 IEEE 购买的 OUI 都属于全球管理。当地址字段的 G/L 位为 1 时是本地管理，这时用户可任意分配网络上的地址。采用 2 字节地址字段时全都是本地管理。但应当指出，以太网几乎不理会这个 G/L 位。这样，在全球管理时，实际上 MAC 地址可用 46 位的二进制数字来表示(其最低位和最低第二位均固定为 0)。这 46 位

组成的地址空间可有 2^{46} 个地址，可保证世界上的每一个适配器都有一个唯一的地址。

当计算机通过适配器连接到局域网时，适配器上的硬件地址就用来标志该计算机的这个接口。如果路由器连接到两个网络上，它就需要两个适配器和两个硬件地址。

适配器具有过滤功能。适配器每收到一个 MAC 帧就先用硬件检查 MAC 帧中的目的地址。如果是发往本站点的帧则收下，然后进行其他处理。这里“发往本站点的帧”包括以下三种帧。

（1）**单播（unicast）帧（一对一）**，即收到帧的目的 MAC 地址与本站点的 MAC 地址相同。

（2）**广播（broadcast）帧（一对全体）**，即发送给本局域网上所有站点的帧（MAC 地址为全 1）。

（3）**多播（multicast）帧（一对多）**，即发送给本局域网上多个站点的帧。

所有的适配器都能够识别前两种帧，即识别单播和广播地址。有的适配器可以用软件编程的方法识别多播地址。显然，广播地址和多播地址是不可以作为源地址使用的。

以太网适配器还可设置在**混杂模式**。工作在混杂模式的适配器会把所有的帧都收下来。网络黑客可以利用混杂模式窃听其他站点发送的数据帧。因此，以太网上非常不希望有适配器工作在混杂模式。但混杂模式也有正面的用途。例如，网络维护和管理人员可以利用这种方式来监视和分析以太网上的流量。

3.3.6　以太网帧格式

常用的以太网帧格式有两种标准：一种是 DIX Ethernet V2 标准（即以太网 V2 标准）；另一种是 IEEE 802.3 标准。下面介绍以太网 V2 的帧格式，如图 3-20 所示。

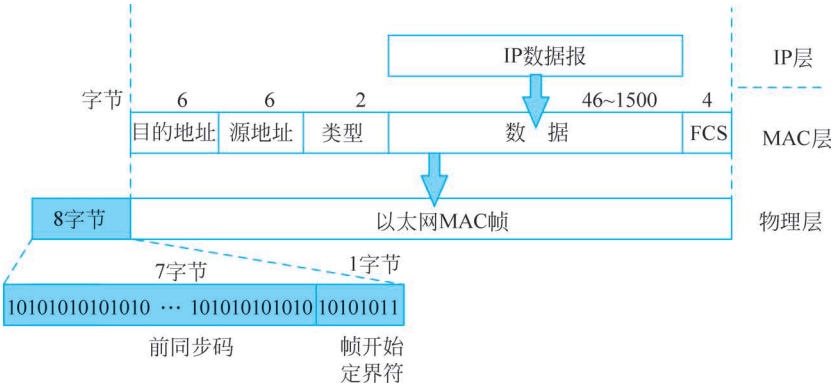

图 3-20　以太网 V2 的帧格式

以太网 V2 的帧由 5 个字段组成，依次是目的地址（6 字节）、源地址（6 字节）、类型（2 字节）、数据部分（长度视情况而定）和帧校验序列 FCS（4 字节）。目的地址和源地址字段写入目的站点和源站点的 MAC 地址。类型字段用来表示数据部分使用的是什么协议，以便把收到的数据上交给这个协议。例如，该值是 0x0800 时表示数据部分是 IP 数据报。数据字段的长度为 46～1500 字节（以太网帧的最小长度为 64 字节，减去 18 字节的首部和尾部可以得到数据字段的最小长度为 46 字节）。帧检验序列（FCS）使用 CRC 检验，检验的范围是 5 个字段，不包括 8 字节的前同步码和帧开始定界符。当误码率为 1×10^{-8} 时，未检测到的

差错概率小于 1×10^{-14}。

特别指出，以太网 V2 的帧格式中，并没有一个长度（或数据长度）字段。这可以利用曼彻斯特编码的特性来获取帧的结束。曼彻斯特编码在每个码元的中间位置都有一次电压跳变，而如果没有数据，则没有电压跳变。当检测到没有跳变时，就获取了数据帧的尾部，从而可以确定数据帧的长度。另外，上层交付下来的数据少于 46 字节时，MAC 子层就会在数据字段的后面加入一个整数字节的填充字段，以保证以太网的 MAC 帧长不小于 64 字节。一般地，填充后保证帧长等于 64 字节。具体处理时，接收端会把数据和填充一起交付给网络层。IP 数据报首部有长度字段，从而网络层根据长度字段将填充数据丢弃。

为了使得接收端和到达的比特流同步，帧的前面还有硬件生成的 8 字节，其包括两个字段。第一个字段是 7 字节的前同步码（10 重复出现），使接收端的适配器调整其时钟频率以便和发送端的时钟同步，也就是“实现位同步”。第二个字段是帧开始定界符，定义为 10101011。其前 6 位和前同步码一样，最后的两个连续的 1 提醒接收端适配器帧的信息马上开始。FCS 字段的检验范围不包括前同步码和帧开始定界符。使用 SONET/SDH 进行同步传输时则不需要前同步码，因为在同步传输时收发双方的位同步总是一直保持着的。

出现下列情况之一的，即为无效的 MAC 帧。

（1）帧的长度不是整数字节。

（2）FCS 校验有差错。

（3）数据字段的长度不是 46～1500 字节的帧。相应地，帧长度不是 64～1518 字节的帧。

对于无效 MAC 帧就简单地丢弃，以太网不负责重传。

IEEE 802.3 标准的帧格式与以太网 V2 帧格式总体上是相同的，区别在于以下三点。

第一，IEEE 802.3 帧第三个字段是“长度/类型”。当这个字段的值大于 0x0600（十进制数 1536）时，这个字段就是“类型”。这时，IEEE 802.3 的帧格式和以太网 V2 帧格式一样。当这个字段值小于 0x0600 时表示“长度”，即帧的数据部分长度。需要注意，编码采用了曼彻斯特编码，长度字段并无实际意义。

第二，当“长度/类型”字段值小于 0x0600 时，数据部分必须是 LLC 子层的 LLC 帧。

第三，IEEE 802.3 标准文档中规定的帧格式包括 8 字节的前同步码和帧开始定界符。

3.4 扩展的以太网

在一些工作场景下，希望把以太网的覆盖范围进行扩展。本节将讨论在物理层和数据链路层扩展以太网。

3.4.1 在物理层扩展以太网

以太网上主机之间的距离是受到限制的（注意，这个距离不是物理距离，而是连接两个主机之间的线路的长度），不能太远（如 10Base-T 以太网上这个限制是不超过 200m）。早期，工作在物理层的转发器被用来扩展以太网的覆盖范围。两个网段可以用一个转发器连接起来。IEEE 802.3 标准还规定，任意两个站点之间最多可以经过三个网段。随着技术的进步、双绞线以太网的普及，目前转发器已经很少使用了。扩展主机和集线器之间的连接可

以由光纤和一对光纤调制解调器组成，如图 3-21 所示。光纤的时延小，带宽很大，使用这种方法可以很容易地使主机和几千米以外的集线器相连接。

图 3-21　主机使用光纤和一对光纤调制解调器连接到集线器

现在常用的做法是使用多个集线器把星形以太网连接起来扩展成覆盖范围更大的多级星形结构的以太网。例如，一个单位内部三个部门各有一个 10Base-T 以太网，利用一个主干集线器把它们的以太网连接起来，成为一个更大的以太网，如图 3-22 所示。

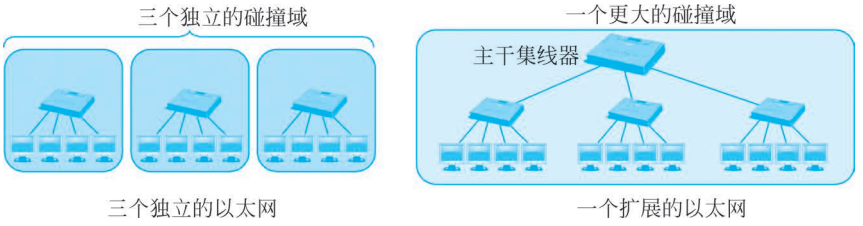

图 3-22　集线器连成更大的以太网

可以看到，第一，原来不能互通的计算机现在可以通信了。第二，扩大了以太网覆盖的范围。例如，每个部门的网络没有互联前，两台主机之间的最大距离是 200m。互联后，不同部门的主机之间的距离就可扩展了，因为集线器之间的距离可以是 100m。

利用集线器扩展以太网也存在一些问题。

（1）互联起来的网络组成了一个更大的碰撞域，碰撞的概率增加，每个结点分得的带宽减少了。原来是 4 个站点共用 10Mb/s 的带宽，互联后是 12 个站点共用 10Mb/s 的带宽。

（2）利用集线器互联的网络必须是同种类型的局域网且数据速率相同。集线器只能转发而不具有缓存的功能。

3.4.2　在数据链路层扩展以太网

更多的时候，人们在数据链路层扩展局域网，使用的设备包括网桥和交换机。网桥是比较老的设备，现在多数使用交换机。这两个设备比物理层的集线器具有更智能的功能，它们可以对收到的帧根据目的地址进行转发和过滤。当网桥（交换机）收到一个帧时，并不是向所有的端口转发此帧，而是根据此帧的目的 MAC 地址，查找网桥（交换机）中的地址表（交换表），然后确定将该帧转发到哪一个端口，或者是把它丢弃（即过滤）。

1990 年诞生了交换式集线器（switching hub），其也被称为以太网交换机（switch）或第二层交换机（简称交换机）。这里说明，现在出现了三层交换机和四层交换机，强调该交换机的协议最高层次分别是网络层和运输层。一般出现在计算机网络书籍中的交换机特指二层交换机，也就是工作在数据链路层。

下面简单介绍以太网交换机的特点。交换机实际上是一个多端口的网桥，后文介绍的交换机的特性，一般网桥也具有。

1. 以太网交换机的特点

交换机通常都有十几个或更多的端口。交换机的每个端口可以连接一个主机，也可以连接一个交换机，这个交换机又连接多个主机。交换机的每个端口一般都工作在全双工方式。以太网交换机端口之间一般具有并行性，即能同时让多对端口间通信。主机都独占传输媒体，无碰撞地传输数据。也就是每一个端口和连接到该端口的设备构成了一个碰撞域。这样，具有 N 个端口的交换机就有 N 个碰撞域。

以太网交换机的端口有存储器，可以在输出端口繁忙时把到来的帧进行缓存。交换机是一种即插即用设备。交换机有一个交换表，交换机根据交换表来转发或过滤数据包。交换表（又称为地址表）是通过自学习算法自动地建立起来的。交换机内部使用了专用的交换结构，用硬件转发，其转发速率要比使用软件转发的网桥快很多。

现实生活中交换机的性能远远超过集线器，而价格并没有高很多。所以，实际生活中交换机用得比较多。用集线器互联的以太网被称为共享式以太网，而交换机互联的以太网被称为交换式以太网。从共享式以太网升级到交换式以太网时，所有设备的软件和硬件、适配器等都不需要做任何改动。对 10Mb/s 共享式以太网，所有用户共享带宽 10Mb/s。而对于 10Mb/s 交换式以太网，每个端口的用户独占带宽 10Mb/s。

交换机的端口一般是自适应端口，例如 10/100Mb/s 自适应端口，可以根据网络设备自适应选择通信速率。

交换机对收到的帧可以采用存储转发的方式进行转发，有一些交换机采用转发效率更高的直通交换方式。直通交换方式不需要把整个数据帧都收到后再进行转发，其在收到帧的目的地址字段就转发。使用直通交换方式，转发时延非常小。但直通交换方式不进行差错检验就进行转发，有可能将一些无效帧转发出去。

2. 交换机（网桥）的自学习机制

交换机（网桥）使用转发表来转发数据帧。转发表是利用**自学习**机制建立的。图 3-23 中的以太网交换机有 3 个端口，各连接一个站点，其 MAC 地址分别是 A、B 和 C，分别连接到端口 1～3 上。交换表中最重要的就是两个条目：目的 MAC 地址和转发接口。交换机刚启动时，交换表是空的。

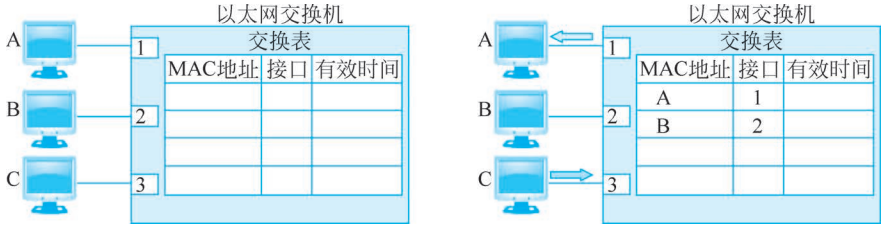

图 3-23　以太网交换机的交换表及自学习

站点 A 向站点 B 发送了一帧，从端口 1 进入交换机。交换机收到该帧后，先查找交换表。交换表是空的，交换机不知道站点 B 连接在哪个端口上。所以交换机向除端口 1 以外的所有端口广播这个帧。另外，虽然交换机不知道站点 B 连接到哪个端口上，但交换机知道站点 A 连接到端口 1 上，因为源地址是 A 的数据帧从端口 1 进入交换机。交换机将学习到的地址 A 和端口 1 写入交换表中。这就是自学习过程。站点 B 收到广播的数据帧。另外，站点 C 也收到该数据帧，因为 MAC 地址不匹配，丢弃该帧，这被称为过滤。

以后，假设站点 B 向站点 A 发送一个数据帧，交换机将查找交换表，知道该帧应该转发到端口 1。同时，学习到站点 B 连接到端口 2 上，将学习到的信息更新到交换表中。

经过一段时间的学习，交换机得到了所有结点连接的端口信息。

另外，从图 3-23 可以看到，交换表中还有“有效时间”。当交换表中写入一个项目时就记录下当时的时间。每一个项目只要超过预定的时间（例如 300s），该项目被删除。用这样的方法去除旧的网络信息，来应对站点从一个端口移动到另一个端口或者站点更换适配器或者站点关机等情况。

交换机的这种自学习机制使得交换机具有即插即用的功能，不必人工进行配置，因此非常方便。

图 3-24 展示了一种糟糕的情况，即自学习的过程可能导致以太网帧在网络的某个环路中无限制地兜圈子。假设交换表刚开始是空的。站点 A 向站点 B 发送了一个帧。交换机 S1 收到该帧后会广播。该数据帧通过交换机 S2 的 5 号端口进入交换机 S2。同样，交换机 S2 也会广播该数据帧，该帧又通过交换机 S1 的 6 号端口进入交换机 S1。这样的发送过程会一直重复下去，交换机 S1 端口 5→交换机 S2 端口 5→交换机 S2 端口 6→交换机 S1 端口 6，白白消耗了网络资源。

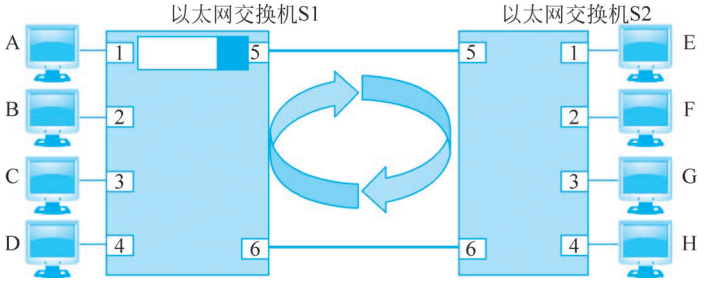

图 3-24　在两个交换机之间兜圈子的帧

出现上述问题的原因是网络中存在环路。为了解决该问题，IEEE 802.1D 标准制定了一个生成树协议（Spanning Tree Protocol，STP）。其核心要点就是不改变网络的实际拓扑，但让一些端口不工作，在逻辑上切断某些链路，网络中没有环路，形成一个树状结构，从而消除了兜圈子现象。

3.4.3　虚拟局域网

以太网交换机的出现，加速了以太网的普及应用，确立了以太网的重要地位。以太网交换机可以使用级联和堆叠的方式，组成更大的以太网。但当一个以太网包含的站点太多时，往往会带来两个缺点。

首先，若干交换机互联组成的以太网是一个广播域。在一个主机数量很大的以太网上传播广播帧会造成网络资源的浪费，并有可能形成“广播风暴”，甚至使整个网络瘫痪。

其次，一个单位的以太网连接众多员工的计算机，这些员工分属不同的部门。但有些部门的信息是敏感且需要保密的（例如，财务部门或人事部门）。许多部门共享一个局域网对信息安全极为不利。

为了克服上述问题，可以在以太网交换机上建立虚拟局域网（Virtual LAN，VLAN），把一个较大的局域网分割成一些较小的局域网，而每一个较小的局域网是一个广播域。虚拟

局域网是交换机提供给用户的一种服务，而并不是一种新型局域网。在同一个虚拟局域网上的主机，看起来好像物理上组成了一个局域网。而不在同一个虚拟局域网上的主机，看起来好像是物理上隔离开的。

1988 年，IEEE 批准了 802.3ac 标准，这个标准定义了以太网的帧格式的扩展，以便支持虚拟局域网。虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符（见图 3-25），称为 VLAN 标签（tag），用来指明发送该帧的计算机属于哪一个虚拟局域网。插入 VLAN 标签的帧称为 802.1Q 帧。

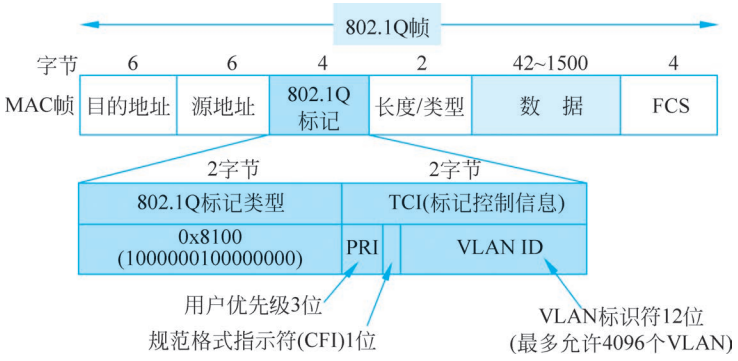

图 3-25 插入 VLAN 标签后变成了 802.1Q 帧

VLAN 标签字段的长度是 4 字节，插入在以太网 MAC 帧的源地址字段和类型字段之间。VLAN 标签的前 2 字节总是设置为 0x8100，称为 IEEE 802.1Q 标签类型。VLAN 标签的后 2 字节中，前面 4 位实际上并没用，后面的 12 位是该虚拟局域网标识符 VID（VLAN ID），它唯一地标志了 802.1Q 帧属于哪一个 VLAN。12 位的 VID 可区分 4096 个不同的 VLAN。插入 VLAN 标签后，FCS 必须重新计算。

当数据链路层检测到 MAC 帧的源地址字段后面的 2 字节的值是 0x8100 时，就知道现在插入了 4 字节的 VLAN 标签。由于用于 VLAN 的以太网帧的首部增加了 4 字节，因此以太网的最大帧长从原来的 1518 字节变为 1522 字节。

每台计算机都是通过接入链路（access link）连接到以太网交换机的。管理人员划分虚拟局域网的方法有多种。例如，按交换机的端口划分，或按 MAC 地址划分。每台主机并不知道自己的 VID 值（但交换机必须知道这些信息）。这些主机通过接入链路发送到交换机的帧都是标准的以太网帧。连接两个交换机端口之间的链路称为汇聚链路（trunk link）或干线链路。汇聚链路上的数据帧需要插入 VLAN 标签，以表明该数据帧属于哪个 VLAN。图 3-26 中计算机 1 和计算机 2 属于 VLAN 10，而计算机 3 和计算机 4 属于 VLAN 20。当计算机 1 向计算机 2 发送数据帧时，计算机 1 向交换机 1 发送标准的以太网帧，交换机 1 发现计算机 2 在另一个交换机 2 上，就向交换机 2 转发该数据帧，在转发前，插入 802.1Q 标记。交换机 2 收到该标记，知道属于 VLAN 10，将该标记去除，并转发标准以太网帧给计算机 2。如果计算机 1 向计算机 3 发送数据帧，因为它们分属于不同的虚拟局域网，需要网络层（例如路由器）的支持。另外，有的交换机中嵌入了一个由专用芯片构成的转发模块，用来在不同的 VLAN 之间转发帧。这样就可以不必再使用另外的路由器，而就在交换机中实现了第 3 层的转发功能。这种转发功能被称为第 3 层交换，而这种交换机常被称为 L3/L2 交换机。

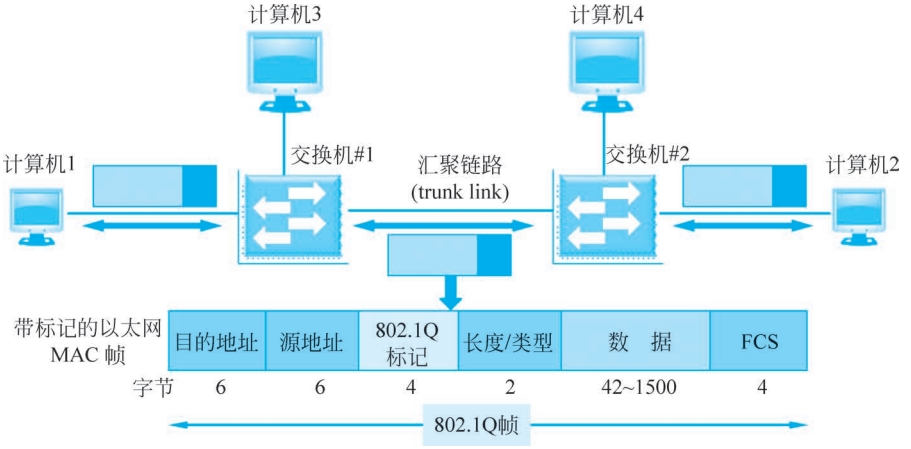

图 3-26　利用以太网交换机构成虚拟局域网

3.5　高速以太网

随着技术的进步，以太网的速率得到持续改进，从 10Mb/s、100Mb/s 以太网一直发展到 1Gb/s 的吉比特以太网，甚至更快的以太网。

3.5.1　100Base-T 以太网

100Base-T 以太网也被称为快速以太网，其传输介质仍然是双绞线，数据速率提升到 100Mb/s，是一种星形拓扑的以太网，依然采用 IEEE 802.3 的 CSMA/CD 协议。用户只要更换 100Mb/s 的网络适配器以及 100Mb/s 的集线器或者交换机，就能非常容易地升级到 100Mb/s，而无须对网络的拓扑结构做出改变。现有的 100Base-T 的适配器一般具有很强的自适应能力，能够自行识别 10Mb/s 和 100Mb/s 并调整自己的数据速率。100Base-T 快速以太网的标准为 IEEE 802.3u。

100Base-T 以太网可在全双工方式下工作而无冲突发生，这时并不使用 CSMA/CD 协议。100Base-T 的 MAC 格式仍然是 IEEE 802.3 标准规定的帧格式。IEEE 802.3u 的标准未包括对同轴电缆的支持。现在 10Mb/s、100Mb/s 以太网都使用无屏蔽双绞线。

当帧长不变时，若数据速率提高 10 倍，网络电缆长度应该减小到原来的 1/10。在 100Mb/s 的以太网中采用的方法是保持最短帧长不变，对于铜缆 100Mb/s 以太网一个网段的最大长度是 100m，其最短帧长仍为 64 字节，即 512 比特。因此，100Mb/s 以太网的争用期是 5.12μs，帧间最小间隔现在是 0.96s，是 10Mb/s 以太网的 1/10。

表 3-1 是 100Mb/s 以太网的物理层标准。

表 3-1　100Mb/s 以太网的物理层标准

名　　称	媒　　体	网段最大长度/m	特　　点
100Base-TX	铜缆	100	2 对 UTP 5 类线或屏蔽双绞线
100Base-T4	铜缆	100	4 对 UTP 3 类线或 5 类线
100Base-FX	光缆	2000	两根光纤，发送和接收各 1 根

3.5.2 吉比特以太网

IEEE 在 1997 年通过了吉比特以太网的标准 802.3z，其在 1998 年成为正式标准。吉比特以太网可用作主干网，也可在高带宽的应用场合中用来连接计算机和服务器。

吉比特以太网的标准 IEEE 802.3z 有以下几个特点。

(1) 沿用 IEEE 802.3 的帧格式。

(2) 允许全双工和半双工两种方式工作，在半双工方式下使用 CSMA/CD 协议，而在全双工方式下不使用 CSMA/CD 协议。

(3) 与 10Base-T 和 100Base-T 技术向后兼容。

表 3-2 是吉比特以太网的物理层标准。

表 3-2 吉比特以太网的物理层标准

名　　称	媒　　体	网段最大长度/m	特　　点
1000Base-SX	光缆	550	多模光纤
1000Base-LX	光缆	5000	单模光纤多模光纤
1000Base-CX	铜缆	25	使用 2 对屏蔽双绞线电缆 STP
1000Base-T	铜缆	100	使用 4 对 UTP 5 类线

表 3-2 中的前三项的标准是 IEEE 802.3z，而 1000Base-T 的标准是 IEEE 802.3ab。

当吉比特以太网工作在半双工方式时，由于数据速率提高到 10 倍，因此只有减小最大电缆长度为原来的 1/10 或增大帧的最小长度为原来的 10 倍。若最大电缆长度减小到 10m，那么网络的覆盖就非常有限。而若最短帧长提高到 640 字节，则发送短数据时额外开销又太大。吉比特以太网仍然保持一个网段的最大长度为 100m。采用了“**载波延伸**”(carrier extension)的办法，使最短帧长仍为 64 字节，同时将争用期增大为 512 字节。凡帧长不足 512 字节时，就使用一些特殊字符填充在帧的后面，使 MAC 帧的长度增大到 512 字节。接收端在收到这样的帧后，把所填充的特殊字符删除后才向高层交付。很明显，填充部分越多，额外的开销就越大。

吉比特以太网还增加了**分组突发**(packet bursting)的功能。当很多短帧要发送时，第一个短帧要采用载波延伸的方法进行填充。但随后的一些短帧则可以一个接着一个地发送，这些短帧之间只需留有必要的帧间最小间隔即可。这样就形成一串分组的突发，直到达到 1500 字节或稍多一些为止。当吉比特以太网工作在全双工方式时，不使用载波延伸和分组突发。

3.5.3 10 吉比特以太网和更快的以太网

10 吉比特以太网(10GbE)的帧格式与 10Mb/s、100Mb/s 和 1Gb/s 以太网的帧格式完全相同，并保留了 IEEE 802.3 标准规定的以太网最小帧长和最大帧长。这就使得 10GbE 和原有以太网能够很好地兼容。10GbE 只工作在全双工方式，因此不存在争用问题，当然也不使用 CSMA/CD 协议。这使得 10GbE 的传输距离大大提高了。

表 3-3 是 10GbE 的物理层标准。前三项的标准是 IEEE 802.3ac，第四项的标准是 IEEE 802.3ak，最后一项的标准是 IEEE 802.3an。

表 3-3 10GbE 的物理层标准

名 称	媒 体	网段最大长度/m	特 点
10GBase-SR	光缆	300	多模光纤
10GBase-LR	光缆	10 000	单模光纤
10GBase-ER	光缆	40 000	单模光纤
10GBase-CX4	铜缆	15	使用 4 对双芯同轴电缆
10GBase-T	铜缆	100	使用 4 对 6A 类 UTP 双绞线

在 10GbE 之后又制定了 40GbE/100GbE(即 40 吉比特以太网和 100 吉比特以太网)的标准 IEEE 802.3ba—2010 和 IEEE 802.3bm—2015。40GbE/100GbE 以太网只工作在全双工的传输方式,不使用 CSMA/CD 协议,并且仍然保持了以太网的帧格式以及 IEEE 802.3 标准规定的以太网最小和最大帧长。100GbE 在使用单模光纤传输时,仍然可以达到 40km 的传输距离,但这需要波分复用(使用 4 个波长复用一根光纤,每一个波长的有效传输速率是 25Gb/s)。

2017 年 12 月,更高速率的以太网标准 IEEE 802.3bs 标准颁布,其共有两种速率,即 200GbE(速率为 200Gb/s)和 400GbE(速率为 400Gb/s),全部用光纤传输(单模和多模)。根据传输方式的不同,传输距离从 100m 至 10km 不等。

3.5.4 使用以太网进行宽带接入

现在人们可以使用以太网进行宽带接入互联网。以太网接入可以提供双向的宽带通信,并且可以根据用户对带宽的需求灵活地进行带宽升级。当城域网和广域网都采用吉比特以太网或 10GbE 以太网时,采用以太网接入可以实现端到端的以太网传输,中间不需要再进行帧格式的转换。这就提高了数据的传输效率且降低了传输的成本。

以太网的帧格式标准中,并没有用户名字段,也没有让用户输入密码来鉴别用户身份的过程。现在人们把数据链路层的两个协议结合起来,即把 PPP 中的 PPP 帧再封装到以太网中来传输。这就是 1999 年公布的 **PPPoE**。现在的光纤宽带接入 FTTx 都要使用 PPPoE 的方式进行接入。

例如,光纤到大楼方案中,在每个大楼的楼口安装一个光网络单元(ONU),然后根据用户所申请的带宽,用 5 类线接到用户家中。如果用户很多,还可以在每一个楼层再安装一个 100Mb/s 的以太网交换机。各大楼的以太网交换机通过光缆汇接到光汇接点(光汇接点一般通过城域网连接到互联网的主干网)。在这种方式下,不再需要使调制解调器,只要 RJ-45 的插口即可。用户把个人计算机通过 5 类网线连接到墙上的 RJ-45 插口中,然后在 PPPoE 弹出的窗口中输入用户名和密码,进行验证后就可以进行宽带上网了。

3.6 无线局域网

近几十年来,无线通信网络得到了飞速发展。本节介绍无线局域网,其重点是无线局域网 MAC 层协议——带冲突避免的载波监听多路访问(CSMA/CA)的原理。无线局域网的简写为 WLAN(Wireless Local Area Network)。

3.6.1 无线局域网的组成

无线局域网可分为两大类：第一类是有基础设施的无线局域网；第二类是无基础设施的无线局域网。

1. 有基础设施的无线局域网

1997 年，IEEE 制定出**无线局域网协议 802.11 系列标准**适用于第一类有基础设施的无线局域网。IEEE 802.11 是一系列无线局域网的标准，它使用星形拓扑。在这种无线局域网中，需要事先部署好基础设施，其一般被称为接入点（Access Point，AP），是一个链路层的设备。AP 一般通过有线的方式连接到互联网上。现在家用的无线局域网的 AP 一般集成 IP 层的路由功能，所以被称为无线路由器。**802.11 无线局域网的 MAC 层使用 CSMA/CA 协议**。

无线局域网的最小构件是基本服务集（Basic Service Set，BSS）。一个基本服务集包括一个接入点和若干移动站。一个站点在和本 BSS 内的站点通信，或者与本 BSS 外的站点通信，都必须通过本 BSS 的接入点。每个 AP 都会分配一个不超过 32 字节的服务集标识符（Service Set IDentifier，SSID）和一个通信信道。SSID 就是指使用该 AP 的无线局域网的名字。一个 BSS 所覆盖的地理区域叫作一个基本服务区（Basic Service Area，BSA）。一个 BSA 的直径一般不超过 100m。接入点 AP 在出厂时就分配了一个唯一的 48b 的 MAC 地址，其正式名称是基本服务集标识符（BSSID）。

无线局域网使用 ISM 频段，通常使用的频段是 2.4GHz 和 5GHz。每一个频段又再划分为若干信道。例如，在 2.4GHz 频段中有大约 85MHz 的带宽可用。802.11b 标准定义了 11 个部分重叠的信道集。相邻信道的中心频率相差 5MHz，而每个信道的带宽约为 22MHz。因此，仅当两个信道由 4 个或更多信道隔开时它们彼此才无重叠。其中，信道 1、6 和 11 的集合是唯一的 3 个非重叠信道的集合。

多个基本服务集可以通过分配系统（Distribution System，DS）连接起来，构成了一个扩展服务集（Extended Service Set，ESS）。ESS 也有个标识符，被称为扩展服务集标识符（ESSID），它是不超过 32 字符的字符串名字。分配系统使 ESS 像一个 BSS 一样。分配系统可以使用以太网（这是最常用的）、点对点链路或其他无线网络。ESS 还可以通过叫作门户（poral）的设备来连接到其他 802.x 局域网。门户的作用相当于一个网桥。在一个 ESS 内几个不同的 BSS 也可能有重合的部分，如图 3-27 中，A_1 所在的区域。图 3-27 中，站点 A 和 C 通信，数据包的路径是 A→AP→C；站点 A 和 B 通信，数据包的路径是 A→AP_1→AP_2→B。

一个站点若要加入某一基本服务集，就必须先与该服务集的 AP 建立关联。建立关联就表示这个站点加入了选定的 AP 所属的子网，并和这个接入点 AP 创建了一个虚拟线路。只有已关联的 AP 才向这个站点发送数据帧，而这个站点也只有通过关联的 AP 才能向其他站点发送数据帧。

站点与 AP 建立关联的方法有两种。一种是被动扫描（见图 3-28（a）），其过程如下。

① AP 周期性发出信标帧（beacon frame），信标帧中包含有若干系统参数（如服务集标识符以及支持的速率等）。

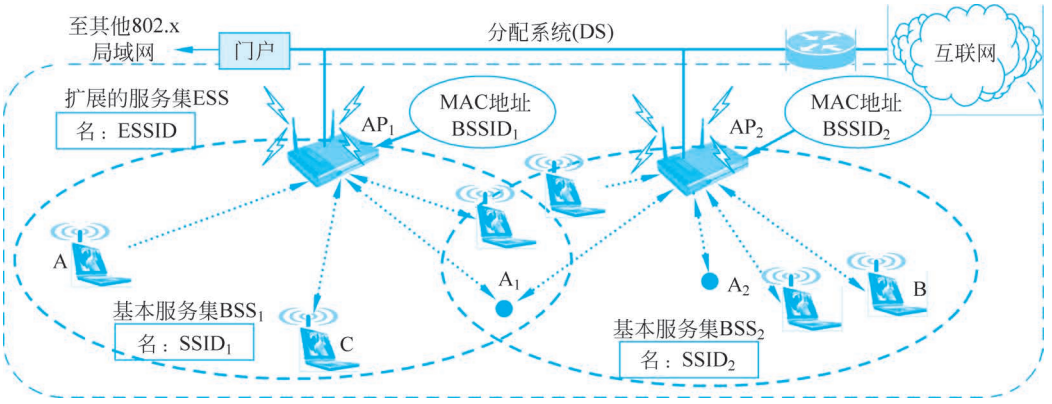

图 3-27　IEEE 802.11 的基本服务集和扩展服务集

② 站点 A 收到多个接入点发出的信标帧，站点 A 选择其中一个加入。图 3-28 中，站点 A 收到 2 个信标帧，然后向 AP_2 发出关联请求帧(association request frame)。

③ 接入点 AP_2 同意站点 A 发来的关联请求，向站点 A 发送关联响应帧(association response frame)。

这样，站点 A 和接入点 AP_2 的关联就建立了。

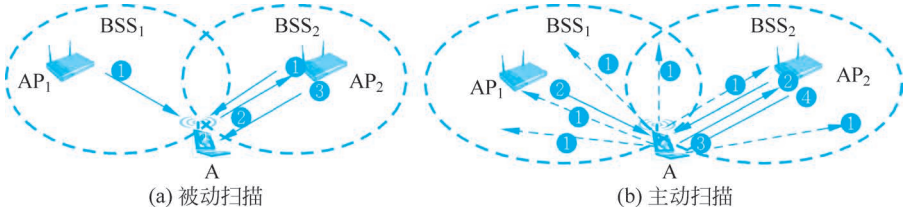

图 3-28　被动扫描和主动扫描

另一种建立关联的方法是主动扫描(见图 3-28(b))，其步骤如下。

① 站点 A 以广播的方式发出探测请求帧(probe request frame)，让站点 A 通信范围内的所有接入点知道有站点要求建立关联(见图 3-28(b)中的多个虚线箭头)。

② 收到探测请求帧的接入点发送探测响应帧(probe response frame)。

③ 站点 A 收到多个接入点发出的探测响应帧，站点 A 选择其中一个加入。图 3-28(b)中，站点 A 向 AP_2 发出关联请求帧。

④ 接入点 AP_2 向站点 A 发送关联响应帧，与站点 A 建立了关联。

若站点使用重建关联服务，就可把这种关联转移到另一个接入点。当使用分离服务时，就可终止这种关联。

无线局域网用户在和附近的 AP 建立关联时，一般还要输入口令。输入正确后，才能和该 AP 建立关联。在无线局域网发展初期，这种接入加密方案称为 WEP(Wired Equivalent Privacy，有线等效的保密)。然而 WEP 的加密方案有安全漏洞，因此现在的无线局域网普遍采用了保密性更好的加密方案(WiFi Protected Access，WPA，无线局域网受保护的接入)或其第二个版本 WPA2。现在 WPA2 是 802.11n 中强制执行的加密方案。

2. 无固定基础设施的无线局域网

另一类无线局域网是无固定基础设施(AP)的无线局域网，又被称为自组网络(ad hoc

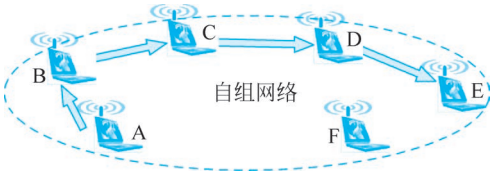

图 3-29　自组网络

network)，是由一些地位对等的站点组成的临时网络。如图 3-29 所示，站点 A 和站点 E 通信时，数据包的路径是 A→B、B→C、C→D 和 D→E。可以看到，在上述通信中结点 B、C、D 相当于路由器，实现的是路由层的功能。所以，**自组网络中的每个结点既充当路由器又是端结点**。

自组网络的服务范围一般是受限的，且自组网络一般独立组网，不和外部其他网络互连。自组网络在军用和民用领域都有很好的应用前景。在军事领域中，移动自组网络可以应用到地面车辆群和坦克群，以及海上的舰艇群、空中的机群。在民用领域，自然灾害后组建临时通信网络用于抢险救灾。

3.6.2　无线局域网的 MAC 层协议

1. CSMA/CA 协议

虽然 CSMA/CD 协议已成功地应用于有线局域网，但无线局域网的特点决定了不能使用 CSMA/CD 协议。

CSMA/CD 协议要求一边发送数据一边检测信道，一旦检测到碰撞，就停止发送。无线网络中实现一边发送数据一边检测的代价比较高，且检测的结果不准确。图 3-30 所示的例子被称为无线局域网的**隐蔽站问题**(hidden station problem)，说明了无线网络中对信道的检测结果不准确。

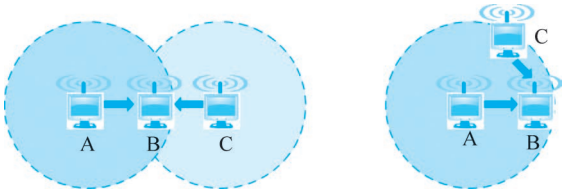

图 3-30　隐藏站问题

假定每个移动站的无线电信号覆盖都是以发送站为圆心的一个圆形。站点 A 和站点 C 都想向站点 B 发送数据。但站点 A 和站点 C 的距离较远，彼此都检测不到对方发送的信号。当站点 A 和站点 C 同时检测到信道空闲，就都向站点 B 发送数据，结果发生了碰撞，并且无法检测出这种碰撞。发生碰撞的原因是站点 B 在站点 A 和站点 C 的共同无线信号覆盖区域，站点 B 收到的信号是站点 A 和站点 C 发送信号的叠加。这种情况就是隐蔽站问题。当两个移动站距离比较近但有障碍物阻挡时也有可能出现上述情况。

CSMA/CD 协议可以很方便地检测到碰撞。如果有碰撞，冲突的站点可以立即停止，从而减少信道资源的浪费。而无线网络无法使用碰撞检测，一旦开始发送数据，就要把整个帧完全发送完，这样，一旦发生碰撞，浪费的信道资源就比较严重。所以，802.11 局域网使用 CSMA/CA 协议。**这里 CA 表示 Collision Avoidance(碰撞避免)**。协议设计的初衷就是要尽可能降低碰撞发生的概率。同时因为无线信道的通信质量远不如有线信道，CSMA/CA 使用了停止等待协议。无线站点每发送完一帧后，要等到收到对方的确认帧后才能继续发送下一帧。这就是数据链路层确认。没有确认的数据帧，需要重传。

先看一下图 3-31 所示的 IEEE 802.11 的 MAC 层，它通过协调功能（coordination function）来决定移动站在什么时间能发送数据。IEEE 802.11 的 MAC 层在物理层的上面，它包括两个子层。

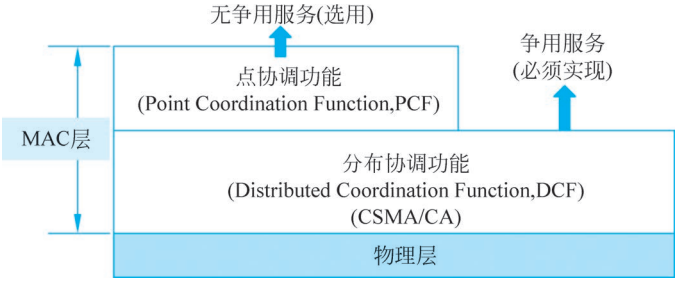

图 3-31　IEEE 802.11 的 MAC 层

（1）**分布协调功能**（Distributed Coordination Function，DCF）。DCF 不采用任何中心控制，而是分布式接入算法，让每个站点通过争用信道来获取发送数据权。因此，DCF 向上提供争用服务。IEEE 802.11 标准规定，DCF 是必须实现的功能。为此，定义了两个非常重要的时间间隔，即短帧间间隔（Short Inter-Frame Spacing，SIFS）和分布协调功能帧间间隔（DCF IFS，DIFS）。

（2）**点协调功能**（Point Coordination Function，PCF）。PCF 是可选功能，是一种集中控制，让接入点集中控制整个 BSS 内站点的活动。自组网络是没有 PCF 子层的。PCF 使用集中控制的接入算法，避免了碰撞的产生。对于时间敏感的业务，如分组话音，就应使用提供无争用服务的点协调功能（PCF）。目前大量的无线局域网都是使用上述的分布协调功能（DCF）。

CSMA/CA 协议比较复杂。下面介绍 CSMA/CA 协议的要点。

（1）站点若想发送数据必须先监听信道。若信道在时间间隔 DIFS 内一直为空闲，则发送整个数据帧。否则，进行（2）。

（2）站点选择一个随机数，设置退避计时器。计时器的运行规则是：若信道忙，则冻结退避计时器，继续等待，直至信道变为空闲（这叫作推迟接入）；若信道空闲，并在时间间隔 DIFS 内均为空闲，则退避计时器进行倒计时。当退避计时器的时间减到零时（显然这只能发生在信道空闲时），站点就发送数据帧，且把整个数据帧发送完。

（3）站点若收到接收方发来的确认帧，且无后续帧发送，则结束。若收到确认，且还有后续帧要发送，就转到（2）。若在设定时间内未收到确认，则准备重传，并转到（2），但会在更大的范围内选择一个随机数。

2. 虚拟载波监听

图 3-32 展示了站点 A 向站点 B 发送数据的全部过程。站点 A 有数据要发送，先监听信道。若信道在 DIFS 时间间隔内一直都是空闲的，站点 A 就可以发送数据帧 DATA。站点 B 收到后立即确认。因为站点 B 要进行校验等操作，所以站点 B 收到数据到发送 ACK 之间有一个 SIFS 时间间隔。DIFS 和 SIFS 值在 IEEE 802.11 标准中有规定。因此从站点 A 开始发送数据帧 DATA 开始，到收到确认 ACK 为止的这段时间（DATA＋SIFS＋ACK），必须不能有其他站点发送数据，这样才不会发生碰撞。

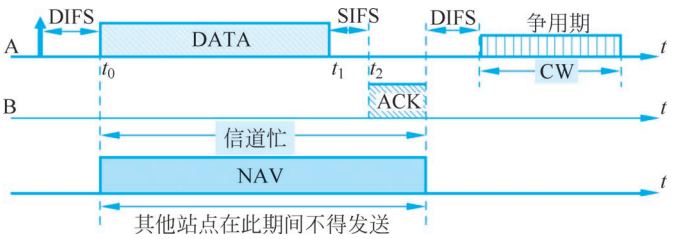

图 3-32 站点 A 向站点 B 发送数据，站点 B 发回确认

为此，IEEE 802.11 标准规定以下两个方法。

第一个方法是用软件实现的**虚拟载波监听**的机制。发送数据的源站点 A 把需要占用信道的时间（DATA＋SIFS＋ACK，以微秒为单位）写入其数据帧 DATA 的首部。在站点 A 的通信范围内的其他各站点都能收到这一信息，并创建自己的网络分配向量（Network Allocation Vector，NAV）。NAV 指出了信道忙的持续时间，意思是“这段时间有其他站点使用信道发送数据，我不可以在这个时间段发送数据”。

第二个方法是在物理层用硬件实现载波监听。每个站点根据收到的信号强度是否超过一个门限数值，用此来判断是否有其他站点正在发送数据。任何站点要发送数据之前，必须监听信道。只要监听到信道忙，就不能发送数据。

从图 3-32 可以看出，DATA 和 ACK 中间有一段 SIFS 时间，信道是空闲的。我们知道，凡是想发送数据的站点，必须等待 DIFS 的空闲时间才能发送。而 IEEE 802.11 规定，SIFS 是小于 DIFS 的。这就保证了确认帧 ACK 优先发送，而不会被其他站点抢走信道占用权。这个方法使得在这段时间（DATA＋SIFS＋ACK），其他站点暂时都不能发送数据。

3. 退避算法

如图 3-33 所示，我们看一下在站点 A 和站点 B 通信的过程中，站点 C 和站点 D 也要发送数据的情况。站点 C 和站点 D 检测到信道忙，必须推迟接入，以免发生碰撞（因为这时站点 A 和站点 B 正在占用信道）。很明显，信道空闲后，等待的站点如果经过相同的时间间隔 DIFS 后同时发送数据，一定会发生碰撞。所以，所有推迟接入的站点不能等待相同的时间，而是使用下面介绍的退避算法公平地争用信道。

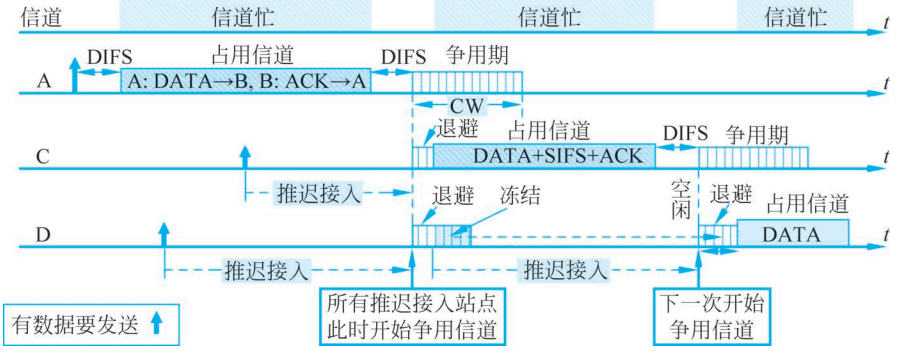

图 3-33 在争用期根据退避算法公平竞争

图 3-33 中的争用期叫作争用窗口（Contention Window，CW）。争用窗口由许多时隙组成。例如，CW＝15 表示窗口大小是 15 个时隙。时隙的长短在不同 IEEE 802.11 标准中可

以有不同数值。例如，IEEE 802.11g 规定一个时隙时间为 9μs，SIFS＝10μs，而 DIFS 应比 SIFS 的长度多两个时隙，因此 DIFS＝28μs。

退避算法规定，站点在进入争用期时，应在 0～CW 个时隙中随机选择一个退避时隙数，并设置退避计时器。当若干站点同时争用信道时，计时器最先降为零的站点就首先接入媒体，发送数据帧。这时信道转为忙，而其他正在退避的站点则冻结其计时器，保留计时器的数值不变，推迟到在下次争用信道时接着倒计时。这样的规定对所有的站点是公平的。

例如，图 3-33 中的站点 C 的退避时隙数为 3，而站点 D 的退避时隙数为 9。当信道空闲后，经过 3 个退避时隙，站点 C 获得了发送权，立即发送数据，信道转为忙状态。这时站点 D 冻结其计时器（这时其计时器为 6 个时隙），等待下一次争用信道时间的到来。下一个争用期到来后，如果没有其他站点要发送数据，那么经过剩余的 6 个退避时隙，站点 D 就可以发送数据了。

注意“推迟接入”和“退避”（backoff）的区别。推迟接入发生在信道处于忙的状态，为的是等待争用期的到来，以便执行退避算法来争用信道。这时退避计时器处于冻结状态。而退避是争用期各站点执行的算法，退避计时器进行倒计时。这时信道是空闲的，并且总是出现在时间间隔 DIFS 的后面（见图 3-33）。

IEEE 802.11 标准并未规定 CW 的初始值，但建议 CW 最小值取为 15，最大值为 1023。CSMA/CA 规定，如果未收到确认帧，则必须重传。但每重传一次，CW 的数值就加倍增大。例如，假定选择初始 CW＝$2^4-1=15$，那么首次争用信道时，随机退避时隙数应在 0～15 生成。在进行重传时，第 i 次重传的 CW＝$2^{4+i}-1$。

第 1 次重传时，随机退避的时隙数应在 0～31 生成。

第 2 次重传时，随机退避的时隙数应在 0～63 生成。

第 3 次重传时，随机退避的时隙数应在 0～127 生成。

第 4 次重传时，随机退避的时隙数应在 0～511 生成。

第 5 次以及 5 次以上重传时，随机退避的时隙数应在 0～1023 生成，CW 不再增大了。

采用上面这些措施，几个站点同时发送数据的概率可以大大降低。

以下是发送数据必须经过争用期公平竞争的几种情况：①要发送数据时检测到信道忙；②已发出的数据帧未收到确认，重传数据帧；③接着发送后续的数据帧。第③种情况是为了防止一个站点长期使用信道。若一站点要连续发送若干数据帧，则不管有无其他站点争用信道，都必须进入争用期，见图 3-34。

图 3-34　站点 A 连续发送多个数据帧

注意，即使使用了上述措施，碰撞仍有可能发生，例如两个站点选择了相同的退避时隙数，上述措施只是降低了发生碰撞的可能性。

4. 预约机制

为了进一步降低碰撞的概率，IEEE 802.11 提供了一个预约机制。在图 3-35 中，站点

A 要和站点 B 通过 AP 的转发进行通信。站点 C 距离站点 A 和站点 B 都比较远，站点 C 接收不到站点 A 和站点 B 发来的信号，站点 C 发送的信号也传播不到远处的站点 A 或站点 B。

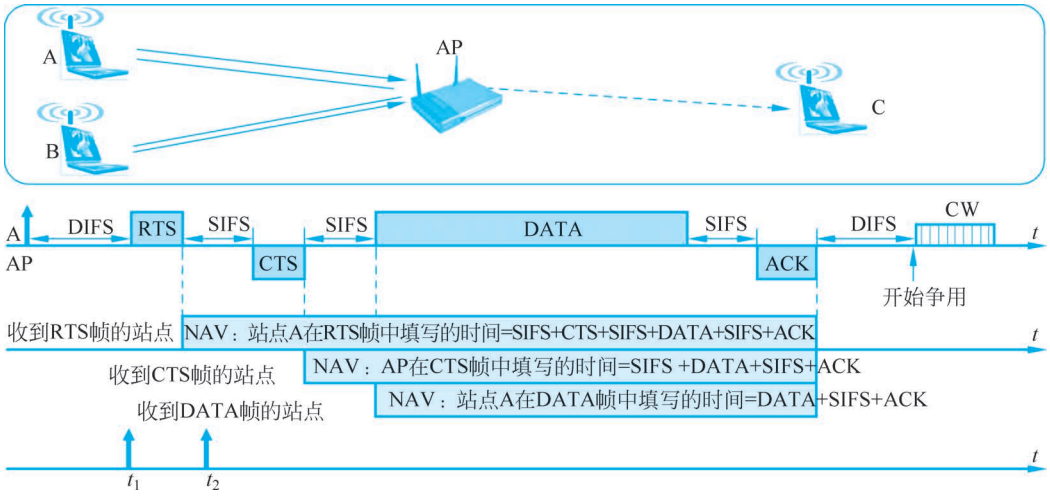

图 3-35　预约机制

在站点 A 向 AP 发送数据帧 DATA 之前，可以进行预约。预约的流程如下。站点 A 先发送一个叫作请求发送(Request To Send，RTS)的控制帧，这个帧比较短，所有收到该信息的站点都知道站点 A 要占用信道一段时间：SIFS＋CTS＋SIFS＋DATA＋SIFS＋ACK。这个时长写在 RTS 帧的首部中。可以看到，站点 A 发送的 RTS 帧，站点 B 能收到，但站点 C 收不到。

AP 收到 RTS 帧，经过 SIFS 后，向站点 A 发送一个叫作允许发送(Clear To Send，CTS)的控制帧，告诉站点 A：“你可以发送数据了”。同时，其他收到该 CTS 控制帧的站点也知道：“站点 A 和 AP 通信，要占用信道一段时间：SIFS＋DATA＋SIFS＋ ACK”。这个时长写在 CTS 的首部中。AP 发送的 CTS 帧，站点 A 和站点 B 以及站点 C 都能够收到。

站点 A 收到 CTS 后，经过一个 SIFS，就发送 DATA 帧，其首部也写入了时间(DATA＋SIFS＋ACK)，表示需要占用信道的时长。如果有的站点没有收到 RTS 和 CTS，那么收到 DATA 后，也根据该时长设置其 NAV。站点 C 知道站点 A 和 AP 之间的通信占用信道的情况，会保持静默，不去争抢信道。

以上预约机制使得站点 A 和 AP 的通信过程中发生碰撞的概率大大降低，特别是减少了隐蔽站点的干扰问题。

显然，RTS 帧和 CTS 帧的使用浪费了一点时间，浪费的时间为 RTS＋SIFS＋CTS＋SIFS。但这两种控制帧都很短，其长度分别为 20 字节和 14 字节，与数据帧(最长可达 2346 字节)相比开销小很多。相反，若不使用预约机制，一旦发生碰撞会导致数据帧重发，浪费的时间就更多了。信道预约不是强制性规定。各站点可以自己决定使用或不使用信道预约。只有当数据帧的长度超过某一数值时，使用预约才比较合适。

另外，预约机制只是使碰撞的概率降低了，并不能完全消除碰撞。例如，图 3-35 中若有的站点在时间 t_1 或 t_2 发送数据(这些站点可能是没有收到 RTS 帧、CTS 帧)，结果必定与

RTS 帧或 CTS 帧发生碰撞，从而导致站点 A 的数据帧发送的推迟。但是，预约机制下，即使发生了碰撞，信道资源的浪费也是很小的。

3.6.3　IEEE 802.11 局域网的 MAC 帧

图 3-36 展示了 IEEE 802.11 局域网的帧格式，其共有三种类型，即控制帧、数据帧和管理帧。

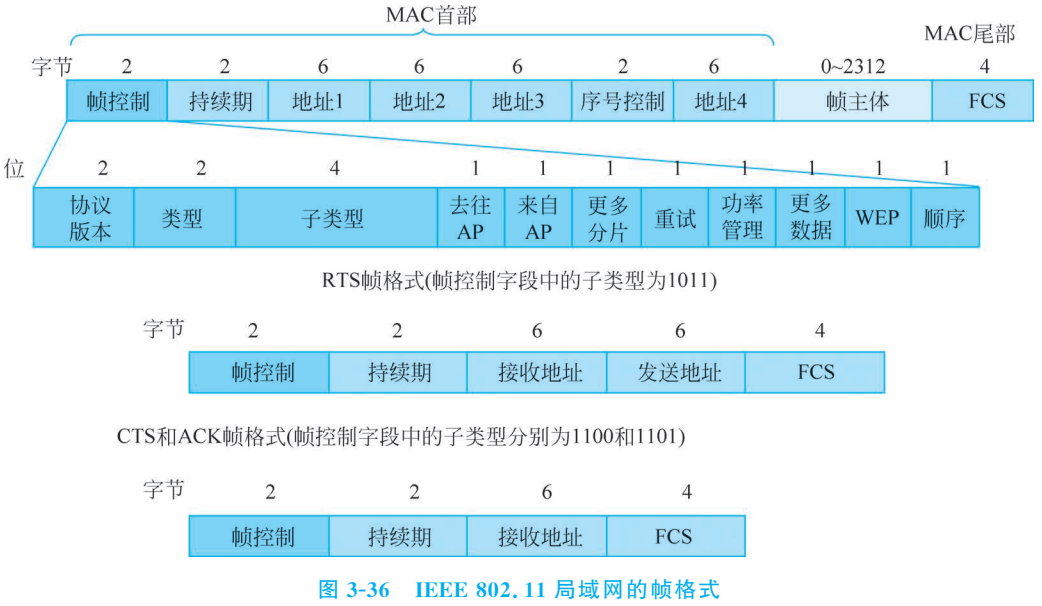

图 3-36　IEEE 802.11 局域网的帧格式

802.11 数据帧由以下三大部分组成。

(1) MAC 首部，共 30 字节。

(2) 帧主体，也就是帧的数据部分，不超过 2312 字节。这个数值比以太网的最大长度长。不过，通常 802.11 数据帧的长度都小于 1500 字节。

(3) FCS 是 MAC 尾部，共 4 字节。

1. 关于 802.11 数据帧的地址

802.11 数据帧有 4 个地址字段，而这几个地址又与控制字段中的“去往 AP”和“来自 AP”这两个子字段的数值有关。很明显“去往 AP”和“来自 AP”字段只能一个是 1，另一个是 0。

地址 1 永远是接收地址(即直接接收数据帧的结点地址)。

地址 2 永远是发送地址(即实际发送数据的结点地址)。

地址 3 取决于数据帧中的“来自 AP”和“去往 AP”这两个字段的数值。当“来自 AP”和“去往 AP”分别是 1 和 0 时，地址 3 是数据帧的源地址。当“来自 AP”和“去往 AP”分别是 0 和 1 时，地址 3 是数据帧的目的地址。

地址 4 仅仅在移动自组网中使用。

这里要再强调一下，上述地址都是 MAC 地址，即硬件地址，而 AP 的 MAC 地址就是 BSSID。

表 3-4 给出了 802.11 帧的地址字段常见的两种情况。现假定在一个基本服务集中的站点 A 通过 AP 向站点 B 发送数据。

表 3-4 802.11 帧的地址字段常见的两种情况

去往 AP	来自 AP	地址 1	地址 2	地址 3	地址 4
1	0	接收地址＝AP 地址	发送地址＝源地址	目的地址	—
0	1	接收地址＝目的地址	发送地址＝AP 地址	源地址	—

在站点 A 发往 AP 的数据帧的帧控制字段中，“去往 AP”＝1 而“来自 AP”＝0。地址 1 是 AP 的地址 BSSID，地址 2 是站点 A 的 MAC 地址，地址 3 是站点 B 的 MAC 地址。

AP 收到数据帧后，转发给站点 B，在数据的控制字段中，“去往 AP”＝0 而“来自 AP”＝1。地址 1 是站点 B 的 MAC 地址，地址 2 是接入点 AP 的地址 BSSID，而地址 3 是站点 A 的 MAC 地址。

另一种更复杂的情况如图 3-37 所示，位于两个子网的站点 A 向站点 B 发送数据。这个数据传输过程需要封装成 4 个数据链路层的帧，每个帧的地址字段介绍如下。

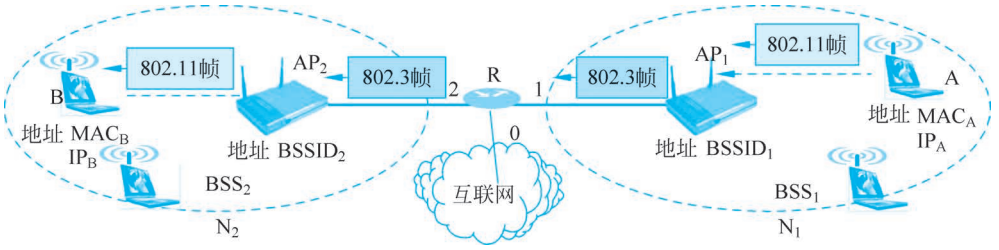

图 3-37 链路上的 802.11 帧和 802.3 帧

第一个数据帧 A→AP_1：站点 A 发送的 802.11 帧的控制字段中，“去往 AP”＝1 而“来自 AP”＝0。地址 1 是 AP_1 的地址 $BSSID_1$；地址 2 是站点 A 的地址 MAC_A；地址 3 是本子网中路由器 R 接口 1 的地址 MAC_{R-1}。

第二个数据帧 AP_1→R：当接入点 AP_1 收到 802.11 帧后，就转换为 802.3 帧，其目的地址是 MAC_{R-1}，而源地址是 MAC_A。

第三个数据帧 R→AP_2：这也是一个 802.3 帧，目的地址是 MAC_B，源地址是路由器 R 接口 2 的地址 MAC_{R-2}。

第四个数据帧 AP_2→B：802.3 的帧被转换为 802.11 帧，其控制字段中，“去往 AP”＝0 而“来自 AP”＝1。地址 1 是站点 B 的地址 MAC_B；地址 2 是 AP_2 的地址 $BSSID_2$；地址 3 是路由器 R 接口 2 的地址 MAC_{R-2}。

2. 序号控制字段、持续期字段和帧控制字段

(1) 序号控制字段占 16 位。其中序号子字段占 12 位(从 0 开始，每发送一个新帧就加 1，到 4095 后再回到 0)，分片子字段占 4 位(不分片则为 0。如分片，则序号子字段保持不变，而分片子字段从 0 开始，每个分片加 1，最多到 15)。重传的帧序号和分片子字段的值都不变。序号控制的作用是使接收方能够区分开是新传送的帧还是因出现差错而重传的帧。

(2) 持续期字段占 16 位。这个就是“对信道进行预约”中预约信道的一段时间。只有最高位为 0 时才表示持续期。这样，持续期不能超过 $2^{15}-1=32\ 767$，单位是微秒。

(3) 帧控制字段共分为 11 个子字段。下面介绍其中较为重要的几个字段。

协议版本字段现在是 0。

类型字段和子类型字段用来区分帧的功能。802.11 帧共分为三种类型：控制帧、数据

帧和管理帧，而每一种帧又分为若干子类型。例如，控制帧有 RTS、CTS 和 ACK 等几种不同的子类型。

更多分片字段置为 1 时表明这个帧属于一个帧的多个分片之一。无线信道的通信质量是较差的，为了提高传输成功的概率，需要把一个较长的帧划分为许多较短的分片。这时可以在一次使用 RTS 和 CTS 预约信道后连续发送这些分片。当然这仍然要使用停止等待协议，即发送一个分片，等收到确认后再发送下一个分片，不过后面的分片都不需要用 RTS 和 CTS 帧重新预约信道。该过程如图 3-38 所示。

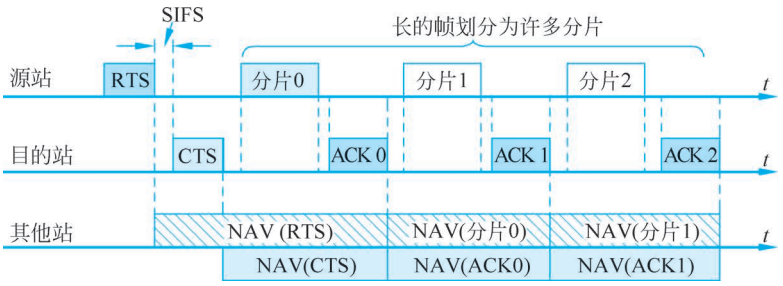

图 3-38　分片的发送

功率管理字段只有 1 位，用来指示移动站的功率管理模式。移动站有三种状态，分别是活跃状态、关机状态和待机状态。待机状态时移动站不进行任何实质性操作，屏幕也处于断电状态，但并未断开与 AP 的关联，因此这种状态非常省电。若一个移动站在发送给 AP 的 MAC 帧中的功率管理字段置为 0，就表示这个移动站处于活跃状态。但若把功率管理字段置为 1 则表示在成功发送完这一帧后，即进入待机状态。由于 AP 总是处在活跃状态，因此 AP 发送的 MAC 帧的功率管理字段总是置为 0。AP 将处于待机状态的移动站保存起来。AP 将发送给待机状态的移动站的帧都暂存起来不发送，而是等到唤醒待机状态的移动站后再发送。通过这种方式，大大地减少了电池功率的消耗。

WEP 字段占 1 位。若 WEP＝1，就表明对 MAC 帧的主体字段采用了加密算法。

3.7　本章重要概念

链路是一段物理线路，而数据链路则是在物理线路的基础上增加了一些协议。数据链路层的信道主要有点对点信道和广播信道两种。

数据链路层的协议数据单元是帧。封装成帧、透明传输和差错检测是数据链路层的三个基本问题。循环冗余检验是一种常用的高效实现帧检验序列(FCS)的方法。

点对点协议(PPP)是数据链路层广泛使用的一种协议，简单是其最重要的特点。

使用广播信道的局域网最重要的问题是协调各站点实现对共享信道的访问。共享广播信道的方法有：一是静态划分信道；二是动态媒体接入控制(又称为多点接入、随机接入或受控接入)。

IEEE 802 委员会把局域网的数据链路层分成两个子层，即逻辑链路控制(LLC)子层(与传输媒体无关)和媒体接入控制(MAC)子层(与传输媒体有关)。现在 LLC 子层的功能已弱化。

网络适配器又称为网络接口卡或网卡，是计算机与外界通信的接口。数据链路层使用的硬件地址(MAC 地址)就存储在网卡的 ROM 中。硬件地址 48 位长。以太网的适配器有过滤功能，它只接收发往本站点的单播帧、广播帧或本站点所在多播组的多播帧。

以太网采用无连接的工作方式，对发送的数据帧不进行编号，也不要求对方发回确认。目的站点收到有差错帧就把它丢弃，其他什么也不做。

以太网使用的协议是带冲突检测的载波监听多路访问(CSMA/CD)。发送数据前先监听，边发送边监听，一旦发现了碰撞，就立即停止发送。然后按照退避算法等待一段随机时间后再次尝试发送。每一个站点在自己开始发送数据之后的 512 比特时间内，存在碰撞的可能。各站点按照 CSMA/CD 协议平等地争用信道。

以太网中参数 a 是一个重要的指标，a 越小，网络效率越高。实际上，传统以太网的信道利用率很低。

双绞线以太网使用了集线器，这种网络在物理上是星形网，但在逻辑上是总线型网。集线器工作在物理层，它的每个端口仅仅简单地转发比特，不进行碰撞检测。使用集线器可以在物理层扩展以太网。

交换式集线器常称为以太网交换机或第二层交换机(工作在数据链路层)。它就是一个多端口的网桥，工作在全双工方式。以太网交换机能同时连通许多对端口，使每一对相互通信的主机都能像独占通信媒体那样，无碰撞地传输数据。

虚拟局域网是交换机提供给用户的一种服务。在同一个虚拟局域网上的主机，看起来好像物理上组成了一个独立的局域网。

高速以太网有 100Mb/s 的快速以太网、吉比特以太网和 10Gb/s 的 10 吉比特以太网。最近还发展到 400 吉比特以太网。在宽带接入技术中，也常使用高速以太网进行接入。PPPoE 是为宽带上网的主机使用的链路层协议。

无线局域网可分为两大类：第一类是有基础设施的无线局域网；第二类是无基础设施的无线局域网。无线局域网的 MAC 层协议是带冲突避免的载波监听多路访问(CSMA/CA)。IEEE 802.11 的 MAC 层包括两个子层：分布协调功能(DCF)和点协调功能(PCF)。

3.8 本章知识图谱

3.9 习题

习题答案

1. 在局域网参考模型中，与媒体无关，从而实现数据帧的独立传输的是(　　)。

A. 物理层　　B. MAC 子层　　C. LLC 子层　　D. 网际层

2. 就交换技术而言，局域网中的以太网采用的是(　　)。

A. 分组交换技术　　B. 电路交换技术

C. 报文交换技术　　D. 分组交换与电路交换结合技术

3. 以太网的访问方法和物理层技术规范由(　　)描述。

A. IEEE 802.3　　B. IEEE 802.4　　C. IEEE 802.5　　D. IEEE 802.6

4. 一个采用 CSMA/CD 技术的局域网,其速率为 10Mb/s,电缆的长度为 500m,无中继器,信号在电缆中的传播速度为 200 000km/s,由此可知 MAC 帧的最小长度不得少于(　　)位。

A. 10　　B. 50　　C. 100　　D. 500

5. IEEE 802.3 标准规定,若采用同轴电缆作为传输介质,在无中继的情况下,传输介质的最大长度不能超过(　　)。

A. 500m　　B. 200m　　C. 100m　　D. 50m

6. 以太网交换机根据(　　)转发数据包。

A. IP 地址　　B. MAC 地址　　C. LLC 地址　　D. PORT 地址

7. 以太网可以采用的传输介质有(　　)。

A. 光纤　　B. 双绞线　　C. 同轴电缆　　D. 以上均可以

8. 目前,最流行的以太网组网的拓扑结构是(　　)。

A. 总线型结构　　B. 环形结构　　C. 星形结构　　D. 网状结构

9. 对于基带 CSMA/CD 而言,为了确保发送站点在传输时能检测到可能存在的冲突,数据帧的传输时延至少要等于信号传播时延的(　　)。

A. 1 倍　　B. 2 倍　　C. 4 倍　　D. 2.5 倍

10. 下列选项中(　　)不是以太网的特点。

A. 采用碰撞检测的载波监听多路访问机制

B. 采用二进制指数退避算法以减少再次竞争时冲突的概率

C. 采用确认、重发机制以保证数据传输的可靠性

D. 采用可携带时钟的曼彻斯特编码

11. 10Base-T 采用的是(　　)的物理连接结构。

A. 总线型　　B. 环形　　C. 星形　　D. 网状

12. 10Base-T 以太网中,以下说法不正确的是(　　)。

A. 10 指的是传输速率为 10Mb/s　　B. Base 指的是基带传输

C. T 指的是以太网　　D. 10Base-T 是以太网的一种配置

13. CSMA/CD 是 IEEE 802.3 所定义的协议标准,它适用于(　　)。

A. 标记环网　　B. 标记总线网　　C. 以太网　　D. 城域网

14. CSMA/CD 相对 CSMA 所做的改进在于(　　)。

A. 控制策略　　B. 延迟算法　　C. 等待时间　　D. 冲突检测

15. 在基带传输系统中,为了延伸网络长度,可以采用转发器。IEEE 802.3 的标准以太网中,在任何两站点之间的路径中最多只允许(　　),这就将有效的电缆长度延伸到 2.5km。

A. 三个转发器　　B. 四个转发器　　C. 二个转发器　　D. 五个转发器

16. 用中继器进行信号转发时,其传输单位是(　　)。

A. 一个完整的帧频　　B. 一个完整的分组

C. 一个完整的报文　　D. 比特

17. 在以太网中,当一台主机发送数据时,总线上所有计算机都能检测到这个数据信

号，只有数据帧中的目的地址与某主机的地址一致时，该主机才接收这个数据帧。这里所提到的地址是(　　)。

A. 端口　　B. IP 地址　　C. MAC 地址　　D. 地理位置

18. 对于以太网，如果一个网络适配器发现刚刚收到的一个帧中的地址是另一个网络适配器的，那么(　　)。

A. 它发送一个 NACK 给发送这个帧的主机

B. 它把这个帧交给网络层，让网络层决定如何处理

C. 它丢弃这个帧，并且向网络层发送错误消息

D. 它丢弃这个帧，不向网络层发送错误消息

19. CSMA/CD 是一种(　　)工作方式。

A. 全双工　　B. 半双工　　C. 单工　　D. 其他方式

20. 网桥是在以下(　　)上实现不同网络互联的设备。

A. 数据链路层　　B. 网络层　　C. 会话层　　D. 物理层

21. 各种网络在物理层互联时要求(　　)。

A. 数据传输率和链路协议都相同　　B. 数据传输率相同，链路协议可不同

C. 数据传输率可不同，链路协议相同　　D. 数据传输率和链路协议都可不同

22. MAC 地址通常存储在计算机的(　　)。

A. 内存中　　B. 网卡上　　C. 硬盘上　　D. 高速缓冲区

23. 以太网交换机中的端口/MAC 地址映射表(　　)。

A. 是由交换机的生产厂商建立的

B. 是交换机在数据转发过程中通过学习动态建立的

C. 是由网络管理员建立的

D. 是由网络用户利用特殊的命令建立的

24. 在下列网间连接器中，(　　)在数据链路层实现网络互连。

A. 中继器　　B. 网桥　　C. 路由器　　D. 网关

25. 数据链路层使用的信道主要有(　　)信道和(　　)信道两种类型。

26. 一般的网络适配器包括(　　)和(　　)这两层的功能。

27. 数据链路层协议解决的三个基本问题是(　　)、(　　)和(　　)。

28. PPP 是点对点信道上的数据链路层协议之一，使用异步传输模式时，采用(　　)方法解决透明传输问题，而使用同步传输时，采用(　　)方法解决透明传输问题。

29. 为了使数据链路层能够更好地适应多种局域网标准，IEEE 802 委员会将局域网的数据链路层拆成两个子层：(　　)子层与(　　)子层，其中，(　　)子层与硬件无关。

30. 传统以太网采用(　　)协议解决媒体共享问题。

31. 以太网物理层协议 100Base-T 表示其传输速率为(　　)，传输介质为(　　)，物理上采用(　　)形拓扑结构连接。

32. (　　)双绞线以太网的出现，是局域网发展史上一个非常重要的里程碑。

33. 硬件地址又称为物理地址或(　　)。

34. 计算机的硬件地址在适配器的(　　)中，而计算机的软件地址(IP 地址)则在计算机的(　　)中。

35. 以太网某个站点收到的帧可能是(　　)帧、(　　)帧和(　　)帧中的一种。

36. 在以太网 V2 的 MAC 帧格式中,(　　)字段用来标志上一层使用的是什么协议。

37. 以太网帧中的数据字段的长度在(　　)字节到(　　)字节。

38. 以太网 V2 的 MAC 帧格式中的 FCS 字段使用(　　)方法检查收到的帧是否有差错。

39. 快速以太网是指速度在(　　)的以太网,采用的是(　　)标准。

40. 100Base-T 是在双绞线上传送 100Mb/s 基带信号的(　　)拓扑以太网,仍使用 IEEE 802.3 的(　　)协议,又称为快速以太网。

41. 吉比特以太网仍然保持一个网段的最大长度为 100m,但采用了(　　)的技术,使最短帧长仍为(　　)字节,同时将争用期增大为 512 字节。

42. 10 吉比特以太网采用的是(　　)标准,不再使用铜线而只使用光纤作为传输媒体,只工作在(　　)方式,不使用 CSMA/CD 协议。

3.10　考研真题

1. (2023 年)若甲向乙发送数据时采用 CRC 校验,生成多项式 $G(x)=x^4+x+1$($G(x)=10011$),则乙接收到下列比特串时,可以断定其在传输过程中未发生错误的是(　　)。

A. 101110000　　B. 101110100　　C. 101111000　　D. 101111100

2. (2013 年)HDLC 协议(零比特填充)对 0111110001111110 组帧后对应的比特串为(　　)。

A. 011111000011111010　　B. 01111100011111010011111110

C. 01111100011111010　　D. 01111100011111001111101

3. (2013 年)下列介质访问控制方法中,可能发生冲突的是(　　)。

A. CDMA　　B. CSMA　　C. TDMA　　D. FDMA

4. (2013 年)10Base-T 网卡接收到如图 3-39 所示的信号波形,则该网卡收到的比特串是(　　)。

A. 00110110　　B. 10101101　　C. 01010010　　D. 11000101

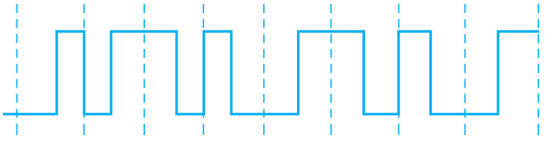

图 3-39　信号波形

5. (2012 年)以太网的 MAC 协议提供的是(　　)。

A. 无连接不可靠服务　　B. 无连接可靠服务

C. 有连接不可靠服务　　D. 有连接可靠服务

6. (2023 年)已知 10Base-T 以太网的争用时间片为 51.2μs。若网卡在发送某帧时发生了连续 4 次冲突,则基于二进制指数退避算法确定的再次尝试重发该帧前等待的最长时间是(　　)。

A. 51.2μs　　B. 204.8μs　　C. 768μs　　D. 819.2μs

7. (2009 年)在一个采用 CSMA/CD 协议的网络中,传输介质是一根完整的电缆,传输

速率为1Gb/s，电缆中的信号传输速度为200 000km/s。若最小数据帧长度减少800b，则最远的两个站点之间的距离至少需要(　　)。

A. 增加160m　　B. 增加80m　　C. 减少160m　　D. 减少80m

8.（2019年）假设一个采用CSMA/CD协议的100Mb/s局域网，最小帧长是128B，则在一个冲突域内两个站点之间的单向传播延时最多是(　　)。

A. 2.56μs　　B. 5.12μs　　C. 10.24μs　　D. 20.48μs

9.（2016年）如图3-40所示，若Hub再生比特流过程中，会产生1.535μs延时，信号传输速度为200m/μs，不考虑以太网的前导码，则H3与H4之间理论上可以相距的最远距离是(　　)。

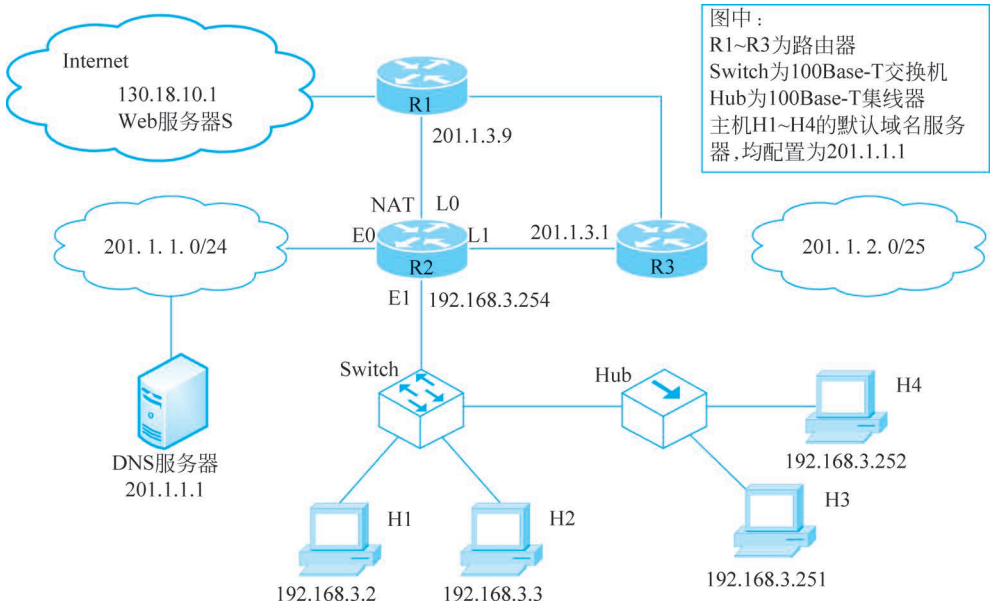

图3-40　信号传输

A. 200m　　B. 205m　　C. 359m　　D. 512m

10.（2016年）如图3-40所示，若主机H2向主机H4发送1个数据帧，主机H4向主机H2立即发送一个确认帧，则除了H4，从物理层上能够收到该确认帧的主机还有(　　)。

A. 仅H2　　B. 仅H3　　C. 仅H1，H2　　D. 仅H2，H3

11.（2015年）关于CSMA/CD协议的叙述中，错误的是(　　)。

A. 边发送数据帧，边检测是否发生冲突

B. 适用于无线网络，以实现无线链路共享

C. 需要根据跨距和数据传输速率限定最小帧长

D. 当信号传播延迟趋近0时，信道利用率趋近100%

12.（2013年）对于100Mb/s的以太网交换机，当输出端口无排队，以直通交换转发一个以太网帧(不包括前导码)，引入的转发延迟至少是(　　)。

A. 0μs　　B. 0.48μs　　C. 5.12μs　　D. 121.44μs

13.（2009 年）以太网交换机进行转发决策时使用的 PDU 地址是（　　）。

A. 目的物理地址　B. 目的 IP 地址　C. 源物理地址　D. 源 IP 地址

14.（2014 年）某以太网拓扑及交换机当前转发表如图 3-41 所示，主机 a1 向主机 c1 发送一个数据帧，主机 c1 收到该帧后，向主机 a1 发送一个确认帧，交换机对这两个帧的转发端口分别是（　　）。

A.｛3｝和｛1｝　B.｛2,3｝和｛1｝　C.｛2,3｝和｛1,2｝　D.｛1,2,3｝和｛1｝

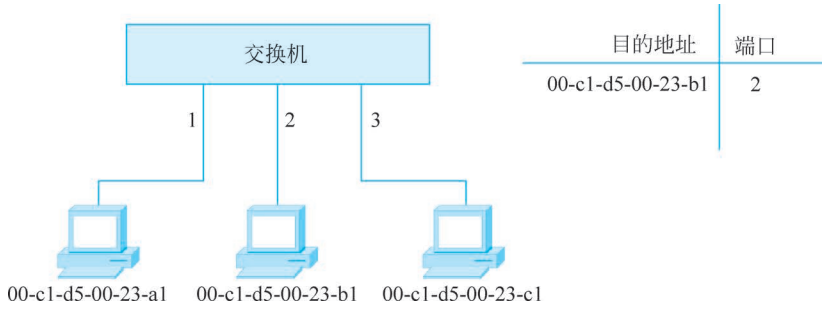

图 3-41　某以太网拓扑及交换机当前转发表

15.（2015 年）下列关于交换机的叙述中，正确的是（　　）。

A. 以太网交换机本质上是一种多端口网桥

B. 通过交换机互连的一组工作站构成一个冲突域

C. 交换机每个端口所连网络构成一个独立的广播域

D. 以太网交换机可实现采用不同网络层协议的网络互联

16.（2020 年）图 3-42 中，冲突域和广播域的个数分别是（　　）。

A. 2,2　B. 2,4　C. 4,2　D. 4,4

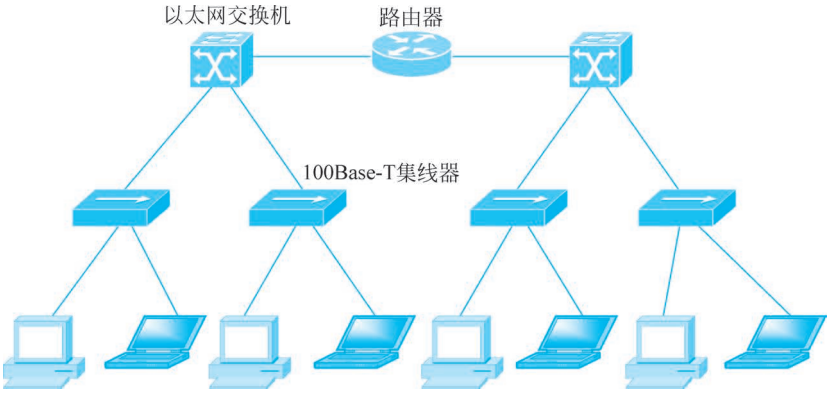

图 3-42　某以太网拓扑

17.（2010 年）下列网络设备中，能够抑制广播风暴的是（　　）。

Ⅰ. 中继器　Ⅱ. 集线器　Ⅲ. 网桥　Ⅳ. 路由器

A. Ⅰ,Ⅱ　B. Ⅲ　C. Ⅲ,Ⅳ　D. Ⅳ

18.（2019 年）100Base-T 快速以太网使用的导向传输介质是（　　）。

A. 双绞线　B. 单模光纤　C. 多模光纤　D. 同轴电缆