第3章 数据链路层

[本章主要内容]

1. 理解数据链路层的地位及功能。
2. 详细介绍数据链路层的成帧、透明传输、CRC 差错检测。
3. 掌握点到点信道的数据链路及 PPP 协议。
4. 详细介绍广播信道的数据链路，重点掌握以太网基本工作原理及 CSMA/CD 协议。
5. 掌握数据链路层设备网桥和以太网交换机的工作原理。
6. 掌握高速以太网的基本工作原理。
7. 掌握 VLAN 的原理及划分。
8. 理解无线局域网的基本概念及 CSMA/CA 协议。

数据链路层属于计算机网络的低层，数据链路层使用的信道主要有以下两种类型：

(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：这种信道使用一对多的广播通信方式，因此过程比较复杂。局域网就是使用广播信道的网络。

数据链路层也常简称为链路层，链路层要解决的三个基本问题：封装成帧、透明传输和差错控制。

两种类型的数据链路层，点到点信道的数据链路层和广播信道的数据链路层。这两种数据链路层通信机制不一样，帧格式与使用的协议也都不一样，点到点信道使用 PPP (Point to Point Protocol) 协议，广播信道的有线局域网使用带冲突检测的载波监听多路访问协议(CSMA/CD 协议)，而广播信道的无线局域网则使用冲突避免的载波监听多路访问协议(CSMA/CA)。

3.1 数据链路层概述

3.1.1 数据链路层的地位

在 OSI/RM 网络体系结构中，数据链路层位于第 2 层，在物理层之上，网络层之下。

划分数据链路层的必要性可以从以下两个方面来说明。

1. 物理层传输产生的误码率

物理线路由传输介质与通信设备组成。在物理线路上传输数据信号是存在差错的，误码率是指二进制比特在数据传输过程中被传错的概率。电话线路的传输速率在300～2400bps时，平均误码率在10^{-6}～10^{-4}；传输速率在4800～9600bps时，平均误码率在10^{-4}～10^{-2}。由于计算机网络对数据通信的要求是平均误码率必须低于10^{-9}，因此普通电话线路不采取差错控制措施不能满足计算机网络的要求。

2. 差错检测与控制

设计数据链路层的主要目的是在有差错的物理线路的基础上采取差错检测、差错控制与流量控制等方法，将有差错的物理线路改进成无差错的数据链路，向网络层提供高质量的数据传输服务。

3.1.2 数据链路层的基本概念

链路(Link)与数据线路的含义是不同的。在通信技术中，链路是指一条无源的点对点的物理线路段(有线或无线)，中间没有其他任何的交换结点。通常，两台计算机进行数据通信，其信道是由许多链路串接而成的，因而一条链路只是一条通路的一个组成部分。

数据链路(Data Link)则是另一个概念，这是因为在一条链路上传输数据时，除物理线路外，还必须具有控制数据传输的规程。链路加上实现这些规程的软硬件构成了数据链路，只有在这样的数据链路上才能进行数据通信。因此，也将链路称为物理链路，而将数据链路称为逻辑链路。

3.1.3 数据链路层与网络层、物理层的关系

1. 数据链路层与网络层的关系

数据链路层在OSI参考模型中处于网络层与物理层之间。数据链路层是在物理层比特流传输功能的基础上为网络层提供服务。

(1) 网络层路由选择算法找出的传输路径一般都是由多段链路组成。

网络层的主要功能是基于一定的路由算法，为源主机和目的主机之间的通信寻找一条最佳的传输路径，这条传输路径可能要经过多个路由器才能够到达目的主机，一般传输路径是由多段链路组成。

数据链路层解决的是相邻两个结点之间的通信规则，如果数据链路层能够保证数据传输路径中的每一段链路传输时都不会出现差错，那么网络层数据经过的多段链路传输也就不会出错。

(2) 由于数据链路层的存在，网络层不需要知道物理层具体采用了哪种传输介质与通信设备。只要接口关系与功能不变，物理层所采用的传输介质与通信设备的变化对网络层不会产生影响。

2. 数据链路层与物理层的关系

数据链路连接建立在物理线路连接基础上。在物理层完成物理线路连接并提供比特流传输能力的基础上,数据链路层才能传输数据链路层协议数据单元——帧。数据链路层协议软件控制数据链路的建立、帧传输与释放过程。同时通过流量控制与差错控制功能来保证数据在数据链路上的正确传输,为其上一层即网络层提供服务。

3.1.4 数据链路层的功能

数据链路层解决的是相邻两个结点之间的通信规则,数据链路层在物理层提供服务的基础上向网络层提供服务。

发送端的数据链路层把网络层交下来的数据封装成帧发送到链路上,而接收端的数据链路层把接收到的帧中的数据取出,检测帧在传输过程中是否产生差错,如果无差错将会把数据上交给网络层,如果有差错则丢弃。数据链路层简化模型如图 3-1 所示。

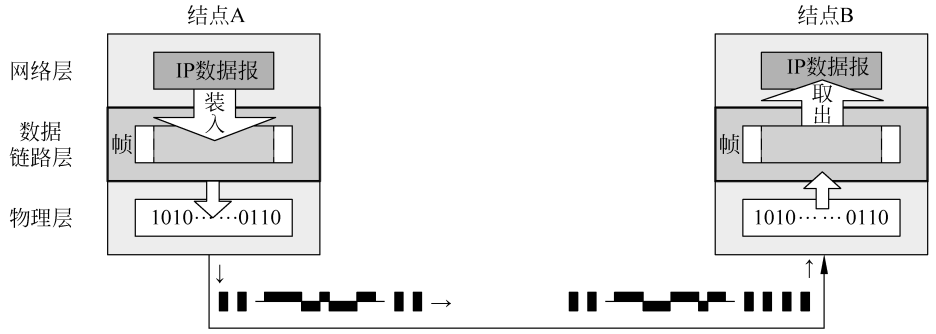


图 3-1 数据链路层简化模型

尽管任一链路层的基本服务都是将数据报通过单一通信链路从一个结点移动到相邻结点,但所提供的服务细节能够随着链路层协议的不同而变化。链路层协议能够提供的可能服务包括:

(1) 链路管理

数据链路层连接的建立、维持和释放过程就称作链路管理,它主要用于面向连接的服务。当链路两端的结点要进行通信前,必须首先确认对方已处于就绪状态,并交换一些必要的信息以对帧序号初始化,然后才能建立连接,在传输过程中则要能维持连接,而在传输完毕后则要释放该连接。在多个站点共享同一物理信道的情况下(如局域网中)如何在要求通信的站点间分配和管理信道也属于数据链路层管理的范畴。

(2) 成帧、帧同步

两个工作站之间传输信息时,必须将网络层的分组封装成帧,以帧的格式进行传送。将一段数据的前后分别添加首部和尾部,就构成了帧。首部和尾部中含有很多控制信息,它们的一个重要作用是确定帧的界限,即帧定界。帧的结构由链路层协议规定,在本章的后面部分研究具体的链路层协议时,将看到几种不同的帧格式。

数据在链路层以帧为单位传输。帧同步是指按接收方应该能够从收到的比特流中正确

地判断出一帧的开始位与结束位。

(3) 透明传输

当传输的数据中出现控制字符时,就必须采取适当的措施,使接收方不至于将数据误认为是控制信息。如在 HDLC 通信规程中,用标识位 01111110 来标识帧的开始和结束。通信过程中,当检测到帧标识 01111110 即认为是帧的开始,然后一旦检测到帧标识即表示帧的结束。如果数据中恰好出现与帧定界符相同的比特组合(会误认为"传输结束"而丢弃后面的数据),就要采取有效的措施解决这个问题,即透明传输。

(4) 差错控制

由于信道噪声等各种原因,帧在传输过程中可能会出现错误。用以使发送方确定接收方是否正确收到了由它发送的数据的方法称为差错控制。差错控制技术要使接收方能够发现与纠正传输错误,数据链路层协议必须能实现差错控制功能。

由于过去端结点功能较弱,必须在通信的数据链路层实现可靠传输。因此在差错检测的基础上,增加了帧编号、确认和重传机制。收到正确的帧就要向发送方发送确认。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,因而就进行重传,直到收到对方的确认为止。这种方法在历史上曾经起到很好的作用。但现在的端结点有足够的智能功能,而且通信线路的质量也已经大大提高了,由通信链路质量不好引起差错的概率已经大大降低。因此,现在互联网采取了区别对待的方法:

对通信质量良好的有线传输链路,数据链路层协议不使用确认和重传机制,即不要求数据链路层向上提供可靠传输的服务。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,那么改正差错的任务就由高层协议(例如传输层的 TCP 协议)来完成。

对于通信质量较差的无线传输链路,数据链路层协议使用确认和重传机制,数据链路层向上层提供可靠传输的服务。

(5) 为网络层提供的服务

当链路层协议提供可靠交付服务时,它保证无差错地经链路层传输每个网络层数据报。在 TCP/IP 网络体系结构中,传输层的 TCP 协议也提供可靠交付服务。与运输层可靠交付服务类似,链路层的可靠交付通常是通过确认和重传取得的。链路层可靠交付服务通常用于易于产生高差错率的链路,例如无线链路,其目的是本地(也就是在差错产生的链路上)纠正一个差错,而不是通过运输层或应用层协议迫使进行端到端的数据重传。然而,对于低比特差错的链路,包括光纤、同轴电缆和许多双绞铜线链路,链路层可靠交付可能会被认为是一种不必要的开销。由于这个原因,许多有线的链路层协议不提供可靠交付服务。

3.2　成帧与透明传输

数据链路层之所以要把比特组合成帧为单位传输,是为了在出错时只重发出错的帧,而不必重发全部数据,从而提高了效率。

封装成帧,就是将网络层的 IP 数据报的前后添加首部和尾部,这样就构成了一个帧,如图 3-2 所示。

为了使接收方能正确地接收并检查所传输的帧,发送方必须依据一定的规则把网络层递交的 IP 数据报封装成帧(称为成帧)。不同的数据链路层协议的帧的首部和尾部包含的

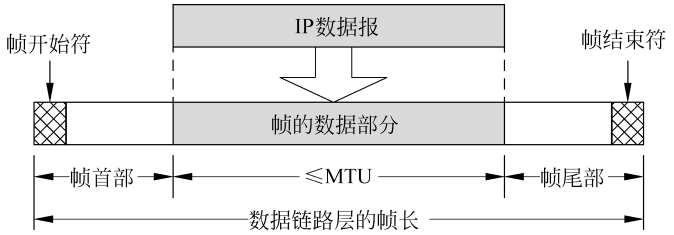


图 3-2 帧首部和帧尾部封装成帧

信息有明确的规定。

为了提高数据链路层传输效率,应当使帧的数据部分尽可能大于首部和尾部的长度。但是每一种数据链路层协议都规定了所能传送帧的数据部分长度的上限,即最大传输单元(Maximum Transfer Unit,MTU),以太网的 MTU 为 1500 个字节,如图 3-2 所示,MTU 指的是数据部分长度。

成帧的过程中也要解决透明传输的问题,当传输的数据帧数据字段中出现某些特定的控制字符的二进制代码时,成帧必须采取适当的措施,使接收端不至于将数据中的系统代码误认为是控制字符。数据链路层必须保证帧数据字段可以传输任意的二进制比特序列,即需要保证帧传输的“透明性”问题。

成帧主要解决帧定界、帧同步、透明传输等问题。通常成帧的方法是:字节填充的首尾定界符法、比特填充的首尾标志法、违规编码法等。

1. 字节填充的首尾定界符法

字符填充法使用一些特殊的字节作为开始和结束,考虑到了出错之后的重新同步问题。这些特殊字节通常都相同,称为标志字节(Flag Byte),作为帧的起始和结束分界符。两个连续的标志字节代表了一帧的结束和下一帧的开始。因此,如果接收方丢失了同步,它只需搜索两个标志字节就能找到当前帧的结束和下一帧的开始位置。

为了使信息位中出现的特殊字符不被误判为帧的首尾定界符,可以在特殊字符前面填充一个转义字节(ESC)来加以区分,以实现数据的透明传输。接收方收到转义字符后,就知道其后面紧跟的是数据信息,而不是控制信息。

图 3-3(a)所示的是由标志字节分界的帧。若帧的数据段中出现 ESC 转义字节,发送方在每个 ESC 前再插入一个 ESC 字节(见图 3-3(b)),在接收方,第一个转义字节 ESC 被删除,留下紧跟在它后面的数据字节(或许是另一个转义字节或者标志字节),结果仍得到原来的数据,图 3-3(b)给出了一些例子。

2. 比特填充的首尾标志法

比特填充的成帧方法考虑了字节填充的缺点,即只能使用 8 比特的字节。帧的划分可以在比特级完成,比特填充法允许数据帧包含任意个数的比特(而不是只能以 8 比特为单元),也允许每个字符的编码包含任意个数的比特。每个帧的开始和结束由一个特殊的比特模式,即 01111110 或十六进制 0x7E 标记,来标志一帧的开始和结束。为了不使信息位中出现的比特流 01111110 被误判为帧的首尾标志,发送方的数据链路层在信息位中遇到 5 个

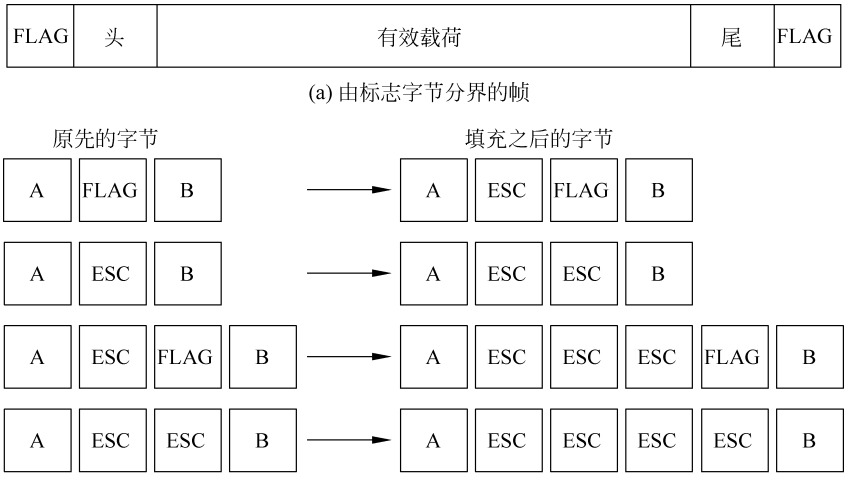


图 3-3　字节填充法

连续的“1”时，将自动在其后插入一个“0”；而接收方做该过程的逆操作，即每收到 5 个连续的“1”时，则自动删除后面紧跟的“0”，以恢复原信息。比特填充的过程如图 3-4 所示。

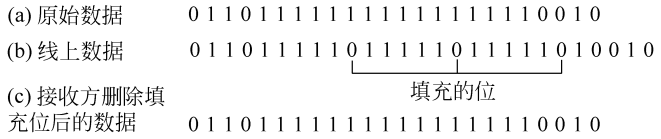


图 3-4　比特填充法

比特填充很容易用硬件来实现，性能优于字节填充方法。

3. 违规编码法

在物理层比特编码时通常采用违规编码法。例如，曼彻斯特编码方法，将数据比特“1”编码成“高—低”电平对，将数据比特“0”编码成“低—高”电平对。而“高—高”电平对和“低—低”电平对在数据比特中是违规的(没有采用)，可以借用这些违规编码序列来定界帧的起始和终止。局域网 IEEE 802 标准就采用了这种方法。

违规编码法不需要采用任何填充技术便能实现数据传输的透明性，但它只适用于采用冗余编码的特殊编码环境。

由于字节填充法实现上的复杂性与不兼容性，目前较常用的组帧方法是比特填充法和违规编码法。

3.3　差错控制

概括地说，传输中的差错都是由于噪声引起的。噪声有两大类：一类是信道所固有的、持续存在的随机热噪声；另一类是由于外界特定的短暂原因所造成的冲击噪声。前者可以

通过提高信噪比来减少或避免干扰,而后者不可能靠提高信号幅度来避免干扰造成的差错,是产生差错的重要原因。

检错编码都是采用冗余编码技术。其核心思想是在有效数据(信息位)被发送前,先按某种关系附加上一定的冗余位,构成一个符合某一规则的码字后再发送。当要发送的有效数据变化时,相应的冗余位也随之变化,使得码字遵从不变的规则。接收端根据收到码字是否仍符合原规则,从而判断是否出错。

常见的检错编码有奇偶校验码和循环冗余校验码。

1. 奇偶校验码

奇偶校验码是奇校验码和偶校验码的统称,是一种最基本的检错码。其校验规则是:在原数据上附加一个校验位,其值为 0 或 1,使附加该位后的整个数据码中 1 的个数称为奇数(奇校验)或偶数(偶校验),如 Y 的 ASCII 码为 1011001,其中 1 的个数为 4,偶校验为 0,奇校验位为 1,如图 3-5 所示。接收方通过计算接收到的码中 1 的个数来确定传输的正确性。它又分为垂直奇偶校验、水平奇偶校验和水平垂直奇偶校验。

校验方式	校验位	ASCII代码位							字符
	8	7	6	5	4	3	2	1	
偶校验	0	1	0	1	1	0	0	1	Y
奇校验	1	1	0	1	1	0	0	1	Y

图 3-5 奇偶校验举例

2. 水平垂直奇偶校验码

同时采用了水平方向的奇偶校验和垂直方向的奇偶校验,既对每个字符做校验,同时也对整个字符块的各位(包括字符的校验位)做校验,则检验能力可以明显提高,这种奇偶校验方式称为水平垂直奇偶校验,也称为纵横奇偶校验。如发送“NETWORK”字符串时,先对每个字符各位进行偶校验,再对所有字符的每一位进行偶校验,如图 3-6 所示。

字符	N 字符$_1$	E 字符$_2$	T 字符$_3$	W 字符$_4$	O 字符$_5$	R 字符$_6$	K 字符$_7$	LRC 字符 (偶)
位1	1	1	1	1	1	1	1	1
位2	0	0	0	0	0	0	0	0
位3	0	0	1	1	0	1	0	1
位4	1	0	0	0	1	0	1	1
位5	1	1	1	1	1	0	0	1
位6	1	0	0	1	1	1	1	1
位7	0	1	0	1	1	0	1	0
校验位 (偶)	0	1	1	1	1	1	0	1

图 3-6 水平垂直偶校验

3. 循环冗余校验码

循环冗余校验(Cyclic Redundancy Check,CRC)码又称为多项式编码,任何一个由二进制数位串组成的代码都可以和一个只含有 0 和 1 两个系数的多项式建立一一对应关系。一个 k 位帧可以看成是从 X^{k-1} 到 X^0 的 k 次多项式的系数序列,这个多项式的阶数为 $k-1$,高位是 X^{k-1} 项的系数,下一位是 X^{k-2} 的系数,以此类推。例如:1110011 有 7 位,表示成多项式是 $X^6+X^{5+}X^{4+}X+1$,而多项式 $X^5+X^4+X^2+X$ 对应的位串是 110110。

给定一个 m bit 的帧或报文,发送器生成一个 r bit 的序列,称为帧检验序列(Frame Check Sequence,FCS)。这样所形成的帧将由($m+r$)比特组成。发送方和接收方事先商定一个多项式 $G(x)$(最高位和最低位必须为 1),使这个带检验码的帧刚好能被这个预先确定的多项式 $G(x)$整除。

接收方用相同的多项式去除收到的帧,如果无余数,则认为无差错。

目前,常见的生成多项式 $G(x)$国际标准有以下几种:

CRC-16　　$G(x)=x^{16}+x^{15}+x^2+1$

CRC-CCITT　　$G(x)=x^{16}+x^{12}+x^5+1$

CRC-32　　$G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

1) 计算 CRC 码的算法

假设要发送的数据帧有 m 位,使用的与接收方事先商定好的除数多项式为 $G(x)$,则计算冗余码的步骤如下:

(1) 加 0。假设 $G(x)$的阶为 r,在帧的低位端加上 r 个 0。

(2) 模 2 除。利用模 2 除法,用 $G(x)$对应的数据串去除(1)中计算出的数据串,得到的余数即为冗余码(共 r 位,前面的 0 不可省略)。

多项式以 2 为模运算。按照模 2 运算规则,加法不进位,减法不借位,它刚好是异或操作。乘除法类似于二进制的运算,只是在做加减法时按模 2 规则进行。

循环冗余校验码的计算举例。

【例 3.1】 要发送的数据帧为 110101,假设使用的生成多项式为 $G(x)=x^4+x^3+1$,计算应发送数据帧的比特序列。

解析:多项式为 $G(x)=x^4+x^3+1$ 对应的二进制数为 $G(x)=11001$(即 $r=4$),待传送数据 $M=110101$(即 $m=6$),具体计算过程如图 3-7 所示。

```
                  100101
G(x)→ 11001 ) 1101010000
              11001
              -----
                11100
                11001
                -----
                  10100
                  11001
                  -----
                   1101 ←S(x) (余数)
```

图 3-7　循环冗余码的运算过程

经模 2 除法运算后的结果是:商 $Q=100101$(这个商没什么用),余数 $R=1101$。所以

发送出去的数据为 1101011101(即 2^rM+FCS),共有 $m+r$ 位。

2) CRC 码的校验过程

在接收方,将收到的数据用约定的多项式 $G(x)$ 去除,如果余数为 0 则传输无误;如有某一位出错,则余数不为 0,且不同数位出错余数不同。

CRC 码的检错能力很强,并且实现起来容易,是目前应用最广的检错码编码方法之一。

【例 3.2】 已知:接收码字为 1101011101,使用的生成多项式为 $G(x)=x^4+x^3+1$,即生成码为 11001($r=4$)。问接收是否正确?若正确,指出冗余码和原信息码。

解:用接收的码字除以生成码,过程如图 3-8 所示。

```
                    100101
G(x) ──► 11001 ) 1101011101
                 11001
                   11111
                   11001
                     11001
                     11001
                         0
```

图 3-8 接收方进行的校验计算

计算结果余数为 0,所以接收正确。

因 $r=4$,从接收码中除去右边的 4 位 1101,原信息码是:110101。

注意,在数据链路层若使用 CRC 检验,能够实现无比特差错的传输,但这还不是可靠传输。CRC 差错检测技术,只能做到对帧的无差错接收,因为接收端收到有差错的帧就丢弃,即没有被接收,凡是接收端数据链路层接收的帧均为无差错的帧。

3.4 点对点协议(PPP)

点到点信道是指一条链路上就一个发送端和一个接收端的信道,通常用在广域网链路。例如两个路由器通过串口(广域网口)相连,如图 3-9 所示。或家庭用户使用调制解调器通过电话线拨号连接 ISP,如图 3-10 所示,这都是点到点信道。

图 3-9 广域网点到点链路

实现数据链路层的功能就需要制定相应的数据链路层协议。在通信线路质量较差的年代,在数据链路层使用可靠传输协议,即高级数据链路控制(High-level Data Link Control,HDLC),不过随着通信线路质量的不断提高,现在 HDLC 已很少使用了。对于点对点的链路,目前使用最广泛的是点对点协议(Point-to-Point Protocol,PPP)。

PPP 协议广泛应用于广域网环境中主机—路由器、路由器—路由器连接以及家庭用户接入 Internet 之中,成为点—点线路中应用最多的数据链路层协议。

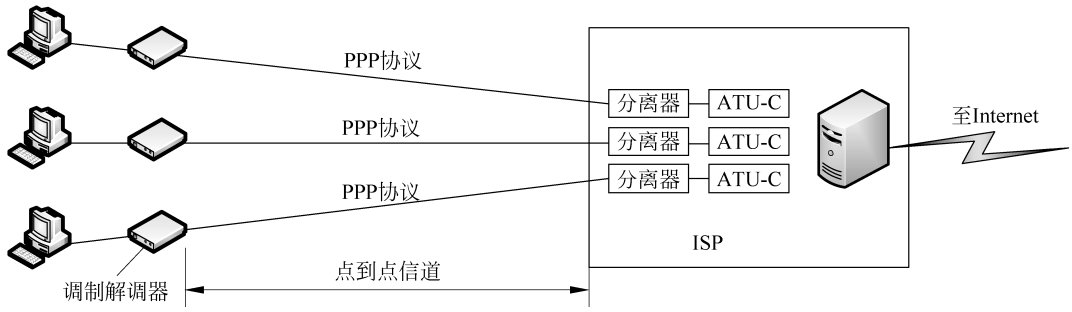


图 3-10　　用户电话连接 ISP 链路

1. PPP 协议的特点

1994 年公布的 RFC1661，以及 RFC1662、RFC1663 对 PPP 的帧结构、差错处理、IP 地址动态分配与身份认证等功能进行了详细的说明。

PPP 既可以在异步线路上传输，也可在同步线路上使用；不仅用于 Modem 链路，也用于租用的路由器到路由器的线路。

PPP 协议比较简单，不负责可靠传输、纠错和流量控制，也不需要给帧编号，接收端收到帧后，就进行 CRC 校验，如果 CRC 校验正确，就收下该帧，反之，直接丢弃。

PPP 有三个组成部分：

(1) 链路控制协议(Link Control Protocol，LCP)，用于建立、配置、测试和管理数据链路。

(2) 网络控制协议(Network Control Protocol，NCP)，PPP 允许同时采用多种网络层协议，每个不同的网络层协议要用一个相应的 NCP 来配置，为网络层协议建立和配置逻辑连接。

(3) 一个将 IP 数据报封装到串行链路的方法。IP 数据报在 PPP 帧中就是其信息部分。这个信息部分的长度受最大传送单元 MTU 的限制。

2. PPP 协议的帧格式

PPP 帧的格式如图 3-11 所示。PPP 帧的前 3 个字段和最后两个字段与 HDLC 帧是一样的，PPP 是面向字节的，因而所有 PPP 帧的长度都是整数个字节。

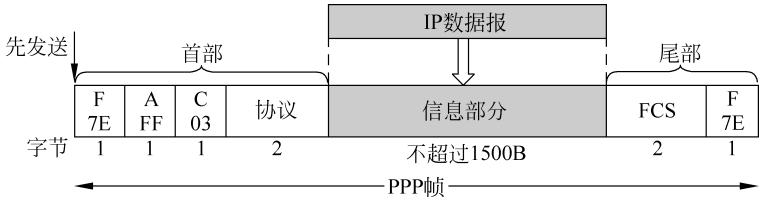


图 3-11　PPP 帧的格式

(1) 首部的第一个字段和尾部的第二个字段都是标志字段 F(Flag)，规定为 0x7E，十六进制的 7E 的二进制表示为 01111110。标志字段表示一个帧的开始或结束。因此标志字段

就是 PPP 帧的定界符。连续两帧之间需要一个标志字段。如果出现连续的两个标志字段，则表示这是一个空帧，应该丢弃。

(2) 首部中的地址字段 A 规定为 0xFF(11111111)，控制字段 C 规定为 0x03(00000011)。最初曾考虑以后再对这两个字段的值进行其他定义，但至今也没有给出。可见这两个字段实际上并没有携带 PPP 帧的信息。

(3) PPP 首部的第 4 个字段是 2 字节的协议字段。

- 当协议字段为 0x0021H 时，PPP 帧的信息字段就是 IP 数据报。
- 当协议字段为 0xC021H 时，PPP 帧的信息字段是链路控制协议 LCP 的数据。
- 当协议字段为 0x8021H 时，PPP 帧的信息字段是网络控制协议 NCP 的数据。

信息字段的长度是可变的，但不允许超过 1500 字节。

(4) 尾部中的第一个字段(2 字节)是使用 CRC 的帧检验序列 FCS。

3. PPP 协议中的透明传输

PPP 协议可以用于异步通信，也可以用于同步通信。

(1) PPP 协议用于异步通信

当 PPP 协议用于异步通信时，使用一种特殊的字节填充法。为了实现透明传输，当信息字段中出现和标志字段一样的比特(0x7E)组合时，就必须采取一些措施使这种与标志字段形式上一样的比特组合不出现在信息字段中。

RFC1662 规定 PPP 使用 0x7D 作为转义字符，并使用字节填充，具体做法如下。

① 在信息字段中出现的每一个 0x7E 字节，要转换成为 2 字节序列(0x7D,0x5E)。

② 若信息字段中出现的每一个 0x7D 的字节(即出现了和转义字符一样的比特组合)，则把 0x7D 转变成为 2 字节序列(0x7D,0X5D)。

③ 若信息字段中出现 ASCII 码的控制字符(即数值小于 0x20)，则在该控制符前加一个 0x7D 字节，同时将该字符的编码加以改变。例如，0x03(在控制字符中是“传输结束”ETX)就要变为 2 字节序列(0x7D,0x23)。这样做的目的是防止这些表面上的 ASCII 码控制符(在被传输的数据中当然已不是控制符了)被错误地解释为控制符。

④ 由于在发送端进行了字节填充，因此接收端需要检测并删除填充字节，还原成发送的值。

(2) PPP 协议用于同步通信

当 PPP 用在同步通信时(如在 SONET/SDH 链路上使用)，采用零比特插入/删除方法，协议规定采用硬件来完成比特填充(和 HDLC 的做法一样)。

4. PPP 协议的工作状态

PPP 链路建立、使用、撤销所经历的状态如图 3-12 所示。当线路处于静止状态时，不存在物理层连接。当线路检测到有载波信号时，建立物理连接，线路变为建立状态。此时，LCP 开始选项商定。商定成功后就进入身份验证状态。通信双发身份验证通过后，进入网络状态。这时，采用 NCP 配置网络层，配置成功后，进入打开状态，然后就可以进行数据传输了。当数据传输完成后，线路转为终止状态。载波停止后则回到静止状态。

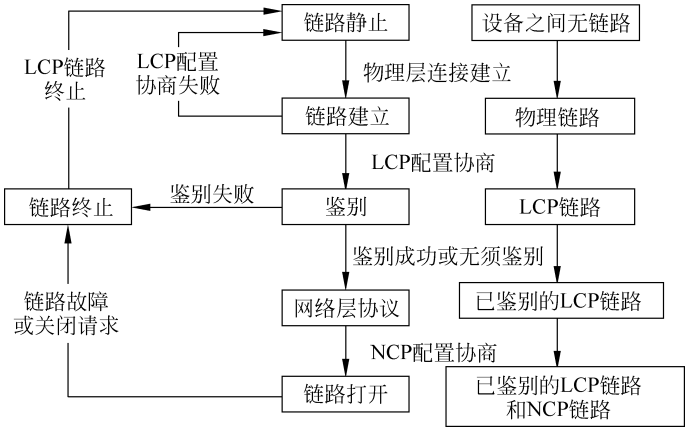


图 3-12　PPP 协议的状态图

注意：

(1) PPP 提供差错检测但不提供纠错功能，只保证无差错接收(通过硬件进行 CRC 校验)。它是不可靠的传输协议，因此也不使用序号和确认机制。

(2) 它仅仅支持点对点的链路通信，不支持多点线路。

(3) PPP 只支持全双工链路。

(4) PPP 的两端可以运行不同的网络层协议，但仍然可使用同一个 PPP 进行通信。

(5) PPP 是面向字节的，当信息字段出现和标志字段一致的比特组合时，PPP 有两种不同处理方法：如果 PPP 用在异步线路(默认)时，采用字节填充法；如果 PPP 用在 SONET/SDH 等同步线路时，协议规定采用硬件来完成比特填充。

3.5　局域网

3.5.1　局域网的基本概念和体系结构

局域网(Local Area Network，LAN)是在一个较小的地理范围(一般在几十米至 1km 左右)内将各种计算机、外部设备和数据库等互相连接起来组成的计算机通信网络。

局域网技术在计算机网络技术的发展过程中，是发展最快、最为活跃和流行的技术之一。由于局域网的传输速度高、组网简单灵活，因而得到了广泛的应用。

1. 局域网的主要特点

(1) 为一个单位所拥有，且地理范围和站点数目均有限。

(2) 所有的站共享较高的总带宽(即较高的数据传输速率)。

(3) 较低的时延和较低的误码率。

(4) 各站为平等关系而不是主从关系。

(5) 能进行广播和组播。

2. 决定局域网特性的三种主要技术

(1) 网络的拓扑结构

局域网的拓扑结构是指在进行局域网设计时所采用的物理和逻辑的结构。局域网按网络拓扑结构可分类为：总线型网、星型网、环型网、树型网。但在实际应用中，以树型网居多。有关局域网拓扑图的内容在本书第 1 章有详细的说明。

(2) 用来传输数据的传输介质

局域网的传输媒体：与网络拓扑相结合，局域网可以使用双绞线、铜缆和光纤等多种传输介质，其中双绞线为主流传输介质。目前在局域网中使用的传输介质主要有 5 类以上的双绞线和光纤，其中早期的总线型网络中还使用基带同轴电缆。无线局域网的传输介质为电磁波。

(3) 介质访问控制方法

局域网的介质访问控制方法主要有：CSMA/CD、令牌总线和令牌环。其中前两种方法主要用于总线型局域网，令牌环主要用于环型局域网。

这三种技术在很大程度上决定了传输数据的类型、网络的响应、吞吐量和效率，以及网络的应用等各种网络特性。其中最重要的是介质访问控制方法，它对网络特性起着十分重要的影响。

3. 局域网的体系结构

由于局域网大多采用共享信道，当通信局限于一个局域网内部时，任意两个结点之间都连接的链路，即网络层的功能可由链路层来完成，所以局域网中不单独设立网络层，它和 OSI 参考模型有较大差别。

随着局域网的出现和广泛使用，局域网产品也日益增多，其标准化的工作也显得越来越重要。电气和电子工程师协会 IEEE 于 1980 年 2 月专门成立了 IEEE 802 委员会，从事局域网参考模型和标准化工作的研究与制定，即著名的 IEEE 802 参考模型，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 LAN 制定了一系列标准，称为 IEEE 802 标准，许多 IEEE 802 标准已成为 ISO 的国际标准，称为 ISO 标准。

IEEE 802 标准的内容：

IEEE 802 委员会制定了一系列局域网标准，ISO 也将其作为国际标准，主要包括：

IEEE 802.1 基本介绍和接口原语定义；概述、体系结构和网络互连，以及网络管理和性能测量。

IEEE 802.2 定义了 LLC 子层协议。

IEEE 802.3 定义了总线型网络的介质访问控制协议 CSMA/CD 及物理层技术规范。

IEEE 802.4 定义了令牌总线(Token Bus)网络 MAC 子层协议及物理层技术规范。

IEEE 802.5 定义了令牌环(Token Ring)网络 MAC 子层协议及物理层技术规范。

IEEE 802.6 定义了城域网(MAN)的 MAC 子层协议及物理层技术规范。

IEEE 802.7 定义了宽带网络技术，为其他分委员会提供宽带网络技术建议。

IEEE 802.8 定义了光纤网络技术，为其他分委员会提供光纤网络技术建议。

IEEE 802.9 定义了语音及数据综合局域网(IVD LAN)的 MAC 子层协议及物理层技术规范。

IEEE 802.10 定义了局域网安全技术规范。

IEEE 802.11 定义了无线局域网技术的 MAC 子层协议及物理层技术规范。

IEEE 802.12 定义了 100VG-Any LAN 局域网的 MAC 子层协议。

在这些标准中，IEEE 802.3 标准最为常用。

在 OSI 参考模型中，局域网的相关标准和规范由最低两层（物理层和数据链路层）来定义。由于局域网内部采用的是共享信道技术，其拓扑结构比较简单，一般不需要中间转接，所以，在局域网中不需要网络层的路由功能，在 IEEE 802 标准中网络层简化成了上层协议的服务访问点（Service Access Point，SAP）。另外，由于局域网使用多种传输介质，而每一种介质访问协议又与传输介质和拓扑结构相关。为了简化局域网中数据链路层的功能划分，所以 IEEE 802 标准把数据链路层划分为介质访问控制（Media Access Control，MAC）子层和逻辑链路控制（Logical Link Control，LLC）子层，与接入到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，不管采用何种协议的局域网对 LLC 子层来说都是透明的，LLC 隐藏了不同 IEEE 802 MAC 子层的差异，为网络层提供单一的格式和接口，同时 SAP 则位于 LLC 子层与高层的交界面上。

与 OSI 参考模型相比，局域网的参考模型只相当于 OSI 的最低两层。图 3-13 所示的是局域网的协议层次与 OSI 的对比。

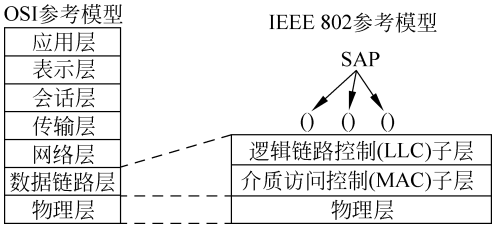


图 3-13　OSI 参考模型与 IEEE 802 参考模型之间的对应关系

由于 TCP/IP 体系经常使用的局域网是 DIX Ethernet V2 而不是 IEEE 802.3 标准中的几种局域网，因此现在 IEEE 802 委员会制定的逻辑链路控制子层 LLC（即 IEEE 802.2 标准）的作用已经不大了。故现在许多网卡仅装有 MAC 协议而没有 LLC 协议。

3.5.2　以太网与 IEEE 802.3

以太网（Ethernet）是在 20 世纪 70 年代中期由 Xerox（施乐）公司 Palo Alto 研究中心推出的。由于相关介质技术的发展，Xerox 可以将许多机器相互连接。这就是以太网的原型。将这项技术命名为“Ethernet”（以太网），源于当时“电磁辐射可以通过以太来传播”的想法。

后来，Xerox 公司推出了带宽为 2Mbps 的以太网，又与 Intel 和 DEC 公司合作推出了带宽为 10Mbps 的以太网，这就是通常所称的以太网 Ⅱ 或以太网 DIX（Digital，Intel 和 Xerox），有时也写成 DIX Ethernet V2。

IEEE 成立后，制定了以太网介质的标准。其中，IEEE 802.3 与 DIX Ethernet V2 非常相似，两者都使用 CSMA/CD 协议，但两者之间略有不同。

严格来说，以太网应当是指符合 DIX Ethernet V2 标准的局域网。但 DIX Ethernet V2 标准与 IEEE 802.3 标准只有很小的差别，因此通常将 802.3 局域网简称为以太网。

以太网逻辑上采用总线型拓扑结构,以太网中所有计算机共享同一条总线,信息以广播方式发送。为了保证数据通信的方便性和可靠性,以太网简化了通信流程并且使用了CSMA/CD方式对总线进行访问控制。

以太网采用两项措施简化通信:采用无连接的工作方式;不对发送的数据帧编号,也不要求接收方发送确认。即以太网尽最大努力交付数据,提供的是不可靠服务,对于差错的纠正则由高层完成。

20世纪80年代以来,随着网络技术的发展,以太网的产品及其标准不断更新和扩展,以太网在网络拓扑、传输速率和相应传输介质上都与原来的标准有了很大的变化,表3-1中显示的是以太网标准的主要进展情况。

表3-1 以太网标准的进展情况

时间/年	技术描述	IEEE标准	网络介质
1982	10Base-5	802.3	粗同轴电缆
1985	10Base-2	802.3a	细同轴电缆
1990	10Base-T	802.3i	双绞线
1993	10Base-F	802.3j	光纤
1995	100Base-T	802.3u	双绞线、光纤
1997	100Base-T2	802.3x	双绞线、光纤
1998	100Base-X	802.3z	光纤、屏蔽铜缆
1999	1000Base-T	802.3ab	双绞线
2002	10GBase-X/R/W	802.3ae	光纤

1. 以太网的传输介质与网卡

以太网常用的传输介质有4种:同轴电缆(粗缆和细缆)、双绞线和光纤。

传统以太网是指IEEE 802.3中最早的以太网产品,主要有10Base-5、10Base-2、10Base-T、10Base-F,这样,以太网就有4种不同的物理层,如图3-14所示。

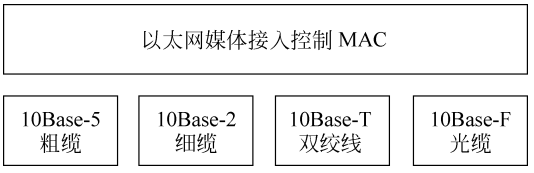


图3-14 传统以太网物理层标准

各种介质的适应情况如表3-2所示。

表3-2 以太网各种传输介质的适应情况

参数	10Base-5	10Base-2	10Base-T	10Base-FL
传输媒体	基带同轴电缆(粗缆)	基带同轴电缆(细缆)	非屏蔽双绞线	光纤
编码	曼彻斯特编码	曼彻斯特编码	曼彻斯特编码	曼彻斯特编码
拓扑结构	总线	总线	星形	点对点
最大段长/m	500	185	100	2000

由于以太网的物理层介质和配置方式有多种，为了准确地表达它们所构成的以太网产品，对于它们名字的命名有一套规定，即由以下三部分组成：

<数据传输率(Mbps)> <信号方式> <最大段长度(百米)或介质类型>

下面介绍传统以太网的几个标准。

10Base-5：速率为 10Mbps，基带信号传输，一条电缆的最大长度为 500m。它是原始的以太网 802.3 标准，又称为粗缆以太网，粗缆是粗同轴电缆的简称。

10Base-5 粗缆以太网的特点：总线一般为粗同轴电缆；抗干扰性好；收发器可以防止信号衰减；布线不方便，价格也比较高。

10Base-2：速率为 10Mbps，基带信号传输，网络的每个段最长为 185m，因此这种细缆局域网就简记为 10Base-2(2 表示距离约为 200m，实际上是 185m)。它是在 10Base-5 的基础上产生的，工作方式与粗缆相似，它对应 IEEE 802.3a 标准。

10Base-2 细缆以太网的特点：总线一般为细同轴电缆；布线方便，价格低廉。但网络的可靠性差，总线连接故障很难查找，不利于维护。

10Base-T：速率为 10Mbps，基带信号传输，采用双绞线和星型结构。它是采用非屏蔽双绞线电缆作为传输介质的以太网。1990 年形成 10Base-T，对应的标准为 IEEE 802.3i。

在 10Base-T 中，组网的设备为集线器，工作站与集线器之间的双绞线最大距离为 100m。

10Base-T 以太网的特点：采用双绞线和星型结构；全部集成到网卡；布线更方便；结构化布线。

注意：10Base-T 非屏蔽双绞线以太网拓扑结构为星型网。星型网中心为集线器，但使用集线器的以太网在逻辑上仍然是一个总线网，属于一个冲突域。

10Base-F：是在 10Base-T 的基础上，用光纤替代双绞线连接站点和集线器，增加网络段长度和覆盖范围的一种以太网。

10Base-F 系列又分为以下三个标准：

(1) 10Base-FP：P 表示无源(Passive)，用于无源星型拓扑，表示连接点(站点或转发器)之间连接的每段链路最大距离不超过 1km。10Base-FP 最多可支持 33 个站点。

(2) 10Base-FL：L 表示链路(Link)，表示连接点(站点或转发器)之间的最大距离不超过 2km。

(3) 10Base-FB：B 表示主干(Backbone)，表示连接转发器之间的链路的最大距离不超过 2km。

计算机与外界局域网的连接是通过主机箱内插入一块网络接口板，又称为网络适配器(Adapter)或网络接口卡(Network Interface Card，NIC)，或“网卡”。网卡是局域网中连接计算机和传输介质的接口，具有物理层的电气等特性，能实现与局域网的物理连接和电信号匹配。网卡也完成数据链路层的功能，负责处理接收和传输数据帧。

网卡和计算机之间的通信则是通过计算机主板上的 I/O 总线以并行传输方式进行的，如图 3-15 所示。

网卡的主要功能：

(1) 数据的封装与解封：发送时将网络层传下来的数据加上首部和尾部，成为以太网的帧。接收时将以太网的帧剥去首部和尾部，然后传送至上一层，进行串行/并行转换。

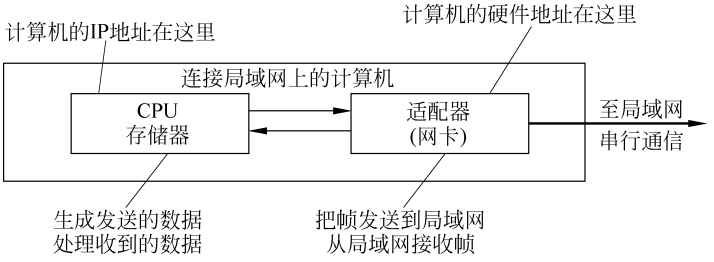


图 3-15 计算机通过适配器和局域网进行通信

(2) 进行串行/并行转换：网卡和局域网之间的通信是通过电缆或双绞线以串行传输方式进行的，而网卡和计算机之间的通信则是通过计算机主板上的 I/O 总线以并行传输方式进行的。因此，网卡的一个重要功能就是要进行数据串行和并行传输的转换。

(3) 对数据进行缓存：由于网络上的数据率和计算机总线上的数据率并不相同，因此在网卡中必须装有进行缓存的存储芯片。

(4) 链路管理：主要是 CSMA/CD 协议的实现。

全世界的每块网卡在出厂时都有一个唯一的代码，称为介质访问控制(MAC)地址，这个地址用于控制主机在网络上的数据通信。数据链路层设备(网桥、交换机等)都使用各个网卡的 MAC 地址。另外，网卡控制着主机对介质的访问，因此网卡也工作在物理层，因为它只关注比特，而不关注任何地址信息和高层协议信息。

2. MAC 地址

每一块网络适配器(网卡)有一个地址，称为 MAC 地址。IEEE 802 标准为局域网规定了一种 48 位的 MAC 地址。在生产网卡时，这种 6 字节的 MAC 地址已被固化在网卡的 ROM 中。因此，MAC 地址也叫作硬件地址(Hardware Address)或物理地址。MAC 地址长 6 字节，一般用由连字符(或冒号)分隔的 6 个十六进制数表示，如 02-60-8C-2E—6E-1B，如图 3-16 所示。

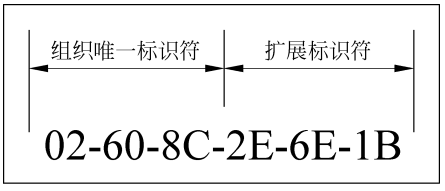


图 3-16 MAC 地址

如何确保各网卡生产厂家的网卡 MAC 地址全球唯一呢？这就要有一个组织对这些网卡生产厂家分配地址块。IEEE 的注册管理机构(Registration Authority，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 个字节中的前三个字节(即高 24 位)。世界上凡是生产局域网适配器的厂家都必须向 IEEE 购买由这三个字节构成的号码(即地址块)，号码的正式名称是组织唯一标识符(Organizationally Unique Identifier，OUI)，通常也叫作公司标识符(Company_id)。

连接在以太网上的路由器和计算机网卡一样，也有 MAC 地址。当路由器通过适配器

连接到局域网时，适配器上的硬件地址就用来标志路由器的某个接口。路由器如果同时连接到两个网络上，那么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。适配器从网络上每收到一个 MAC 帧就先用硬件检查 MAC 帧中的目的地址。如果是发往本站的帧则收下，然后再进行其他的处理；否则就将此帧丢弃，不再进行其他的处理。这样做不浪费主机的处理机和内存资源。这里“发往本站的帧”包括以下 3 种帧：

(1) 单播(Unicast)帧(一对一)，即收到帧的 MAC 地址与本站的硬件地址相同。

(2) 广播(Broadcast)帧(一对全体)，即发送给本局域网上所有站点的帧(全 1 地址)。

(3) 多播(Multicast)帧(一对多)，即发送给本局域网上一部分站点的帧。

所有的适配器都至少应当能够识别前两种帧，即能够识别单播地址和广播地址。有的适配器可用编程方式识别多播地址。当操作系统启动时，它就把适配器初始化，使适配器能够识别某些多播地址。显然，只有目的地址才能使用广播地址和多播地址。

以太网适配器还可以设置为一种特殊的工作方式，即混杂方式(Promiscuous Mode)。工作在混杂模式方式的适配器只要“听到”有帧在以太网上传输就都悄悄地接收下来，而不管这些帧是发往哪个站。这样做实际上是“窃听”其他站点的通信而并不中断其他站点的通信。网络上的黑客常利用这种方法非法获取用户的信息。但混杂方式有时却非常有用。例如，网络维护和管理人员需要用这种方式来监视和分析以太网上的流量，以便找出提高网络性能的具体措施。因此，混杂模式就像一把双刃剑，是利是弊看你怎样使用它。

如何查看网卡的 MAC 地址呢？在 Windows 系统的命令提示符中输入“ipconfig /all”可以查看网卡的 MAC 地址，如图 3-17 所示。

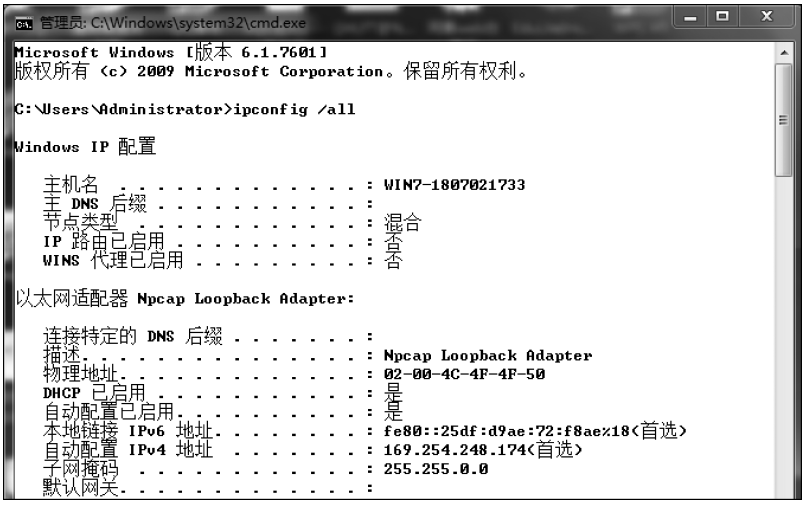


图 3-17　查看计算机网卡的 MAC 地址

3. 以太网的 MAC 帧

由于总线上使用的是广播通信，因此网卡从网络上每收到一个 MAC 帧，首先要用硬件检查 MAC 帧中的 MAC 地址。如果是发往本站的帧就收下，否则丢弃。

常用的以太网 MAC 帧格式有两种标准：

(1) DIX V2 标准的帧。

(2) IEEE 802.3 标准的帧。

最常用的 MAC 帧是 DIX V2 的格式。DIX V2 标准的帧格式如图 3-18 所示。

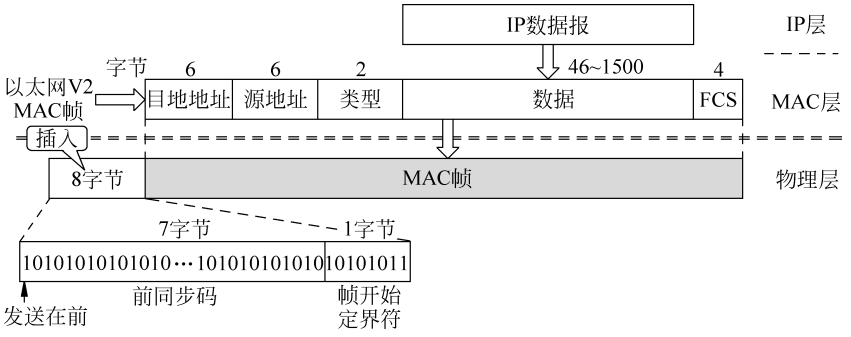


图 3-18 以太网 V2 标准的 MAC 帧格式

(1) 前导码：在帧的前面插入的 8 字节，使接收端与发送端时钟同步，可再分为两字段：第一个字段共 7 字节，是前同步码，用来迅速实现 MAC 帧的比特同步；第二个字段是帧开始定界符，表示后面的信息就是 MAC 帧。

(2) 目的地址：6 个字节，是帧发往的站点物理地址。

(3) 源地址：6 个字节，是发送帧的站点物理地址。

(4) 类型：指出数据域中携带的数据应交给哪个协议实体处理。

(5) 数据：46～1500 字节，包含高层的协议消息。由于 CSMA/CD 算法的限制，以太网帧必须满足最小长度要求 64 字节，当数据较少时必须加以填充(0～46 字节)。

(6) FCS：4 字节，校验范围从目的地址段到数据段的末尾，算法采用 32 位 CRC。MAC 帧的 FCS 字段的检验范围不包括前同步码和帧开始定界符。

802.3 帧格式与 DIX V2 帧格式的不同之处：

长度域：替代了 DIX 帧中的类型域，指出数据域的长度。

在实践中，前述长度/类型两种机制可以并存，由于 IEEE 802.3 数据段的最大字节数是 1500，所以长度段的最大值是 1500，因此从 1501 到 65 535 的值可用于类型段标识符。

DIX V2 帧没有帧结束定界符，那么接收端如何断定帧结束呢？

以太网使用曼彻斯特编码，这种编码的一个重要特点就是：在曼彻斯特编码的每一个码元(不管码元是 1 或 0)的正中间一定有一次电压的转换(从高到低或从低到高)。当发送端把一个以太网帧发送完毕后，就不再发送其他码元了(既不发送 1，也不发送 0)。因此，发送端网络适配器的接口上的电压也就不再变化了，这样，接收端就可以很容易地找到以太网帧的结束位置。从这个位置往前数 4 字节(FCS 长度是 4 字节)，就能确定数据字段的结束位置。

由于以太网帧必须满足最小长度要求 64 字节，所以当数据较少时必须加以填充(0～46 字节)数据字段。接收端还必须能够将添加的字节去掉。现在的问题是，MAC 帧的首部并没有指出数据字段的长度是多少，接收端的数据链路层在剥去首部和尾部后就把数据字段和填充字段一起交给上层协议，上层协议如何知道填充字段的长度呢？

这就要求网络层丢弃没有用处的填充字段。上层协议必须具有识别有效的数据字段长

度的功能。在后面网络层章节中会讲到网络层首部有一个“总长度”地段，用来指明网络数据包的长度，根据网络层首部标注的数据包总长度，会去掉数据链路层提交的填充字段字节。

3.5.3 共享信道的介质访问控制方法

介质访问控制方法通过解决传输介质使用权问题，实现对网络传输介质的合理分配。IEEE 802 标准规定了局域网中几种常用的介质访问控制方法：CSMA/CD、令牌环访问控制和令牌总线访问控制，后两种已经不再使用，本书也不再介绍，所以，本节主要介绍 CSMA/CD 的原理。

带冲突检测的载波侦听多路访问（Carrier Sense Multiple Access with Collision Detection，CSMA/CD），它广泛应用于局域网的 MAC 子层，是一种适合总线结构的采用随机访问技术的竞争型（有冲突的）介质访问控制方法。

CSMA/CD 的工作原理如下：

（1）每个站点在发送数据前，先监听信道，以确定介质上是否有其他站点发送的信号在传送。

（2）若介质处于空闲状态，则发送数据帧。

（3）若介质忙，则继续临听，直到介质空闲，然后立即发送。

（4）边发送帧边进行冲突检测，如果发生冲突，则立即停止发送，并向总线上发出一串阻塞信号（连续几个字节全是“1”）来强化冲突，以保证总线上所有站点都知道冲突已发生。

（5）各站点等待一段随机时间，重新进入侦听发送阶段。

其工作原理可以概括为：先听后发，边发边听，冲突停止，延迟再发。

使用 CSMA/CD 协议，一个站点不能同时进行发送和接收（全双工通信），只能双向交替通信（半双工通信）。

因为电磁波在总线上总是以有限的速率传播的。因此当某个站监听到总线是空闲时，也可能总线并非是空闲的。

每个站点在发送数据之后的一小段不确定时间内，存在着遭遇碰撞的可能性，冲突产生过程如图 3-19 所示。

最先发送数据帧的站点，在接收到碰撞信息时才可知道发送的数据帧是否遭受了碰撞。发送的数据帧在可能收到碰撞信息前不应提前结束，否则发送的计算机认为数据已正确发送，会清除缓冲寄存器中的数据，当收到碰撞信息后就无法再重发此数据帧了。

检测到冲突所用的时间，最长为以太网的端到端往返时延 $2r$，这段时间称为争用期或碰撞窗口。若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。以太网取 51.2μs 为争用期的长度。

对于 10Mbps 以太网，在争用期内可发送 512bit，即 64 字节。

一个站点在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。因此，以太网规定了最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常终止的无效帧。

如果数据帧太长就会出现有的工作站长时间不能发送数据，而且可能超出接收端的缓冲区大小，造成缓冲溢出。所以以太网的帧长度规定为 64～1518 字节。

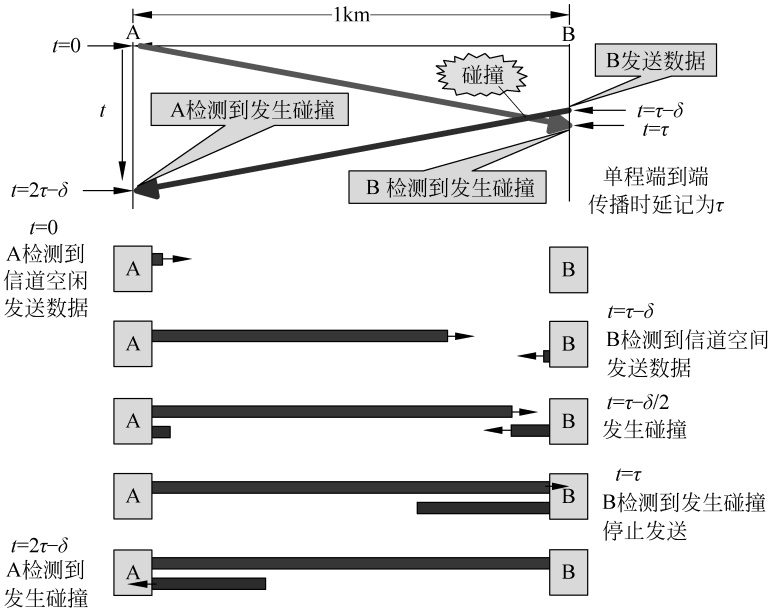


图 3-19 冲突产生示意图

二进制指数退避算法：

当站点发现冲突后便会发送一个干扰信号，然后后退(退避)一段时间再重新发送。后退时间的多少对网络的稳定性起着十分重要的作用，这时可以使用二进制指数退避算法来决定后退时间(重传数据的时延)。

在由于检测到碰撞而停止发送后，一个站必须等待一个随机时间段才能重新尝试发送。这一随机等待时间是为了减少再次发生碰撞的可能性。通常，人们把这种等待一段随机时间再重传的处理方法称为退避处理，把计算随机时间的方法称为退避算法。

IEEE 802.3 所使用的是截断的二进制指数退避算法，其基本工作原理为：先确定基本退避时间(如 2τ)，再定义 $k=\text{Min}[\text{重传次数},10]$，然后从正整数集合$[0,1,2,\cdots,2^k-1]$中随机取出一个数，记为 r。重传所需的后退时延就是 r 倍的基本退避时间。具体来说：如果一个站发生了第 2 次冲突，则 $k=2$，r 可随机从$[0,1,2,3]$中取得，然后在 r 倍的基本退避时间后再重试，以此类推。

标准中允许的最大尝试发送的次数是 16，超过 16 次以后，就放弃这一帧，并向高层报告。

退避算法的一个缺点是它具有一种后进先出的效应，即无碰撞或少碰撞的站比起等待时间较长的站来讲可获得优先的发送机会。

3.6 局域网扩展

由于以太网的物理限制，一个局域网网段覆盖的范围是有限的，每个网段的最大距离、最大站点数也都有一定的限制。但在许多情况下，一个单位往往拥有许多个局域网，因而需要实现局域网之间的通信。这就需要使用一些中间设备将这些局域网连接起来。本节要讨

论的是在物理层或数据链路层将局域网进行扩展。这种扩展的局域网在网络层看来仍然是一个网络。下面介绍集线器、网桥、交换机等局域网的扩展设备。

3.6.1　集线器扩展局域网

集线器(多端口中继器)又称 Hub,工作在物理层,是以太网中的中心连接设备,它是对“共享介质”总线型局域网结构的一种改进。所有的结点通过非屏蔽双绞线与集线器连接,这样的以太网物理结构看似是星型结构,但在逻辑上仍然是总线型结构。当集线器接收到某个结点发送的帧时,它立即将数据帧通过广播方式转发到其他的连接端口。

集线器的一些特点如下:

(1) 集线器是使用电子器件模拟实际电缆线的工作,因此整个系统仍然像一个传统以太网那样运行。10Base-T 以太网又称为星型总线或盒中总线。

(2) 一个集线器有许多端口。

(3) 集线器和转发器都是工作在物理层,它的每个端口都具有发送和接收数据的功能。

(4) 集线器采用了专门的芯片,进行自适应串音回波抵消。

在结点竞争共享介质的过程中,冲突是不可避免的。在网络中,冲突发生的范围称为冲突域。冲突会造成发送结点随机延迟和重发,进而浪费网络带宽。随着网络中结点数的增加,冲突和碰撞必然增加,相应的带宽浪费也会越大。

集线器组建的网络处于一个冲突域中,站点越多,冲突的可能性越大,如图 3-20 所示。

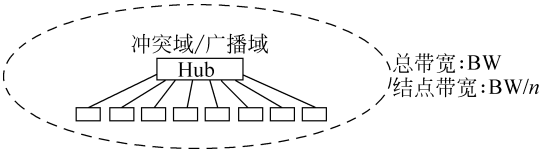


图 3-20　集线器组建的网络处于一个冲突域中

减小网络冲突的解决方法是将网络分段,减少每个网段中站点的数量,使冲突的概率减小,从而增加网络的总体带宽。实现网络分段的设备包括网桥、变换机和路由器,网桥和交换机可以隔离冲突域,如图 3-21 所示。

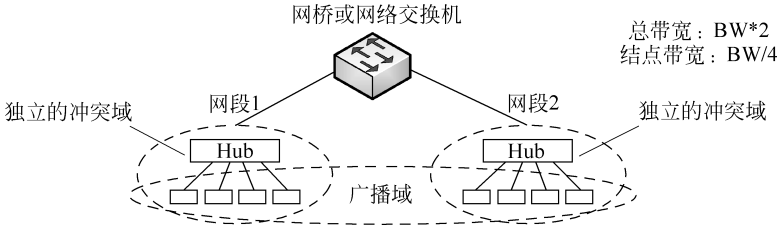


图 3-21　利用网桥或交换机分隔冲突域

3.6.2　网桥

网桥(Bridge)也称网络桥接器,它工作于数据链路层,网桥能将两个局域网连接起来,并对网络的数据流进行管理。网桥不但能扩展网络的距离和范围,还可以在不同介质之间

转发信号以及隔离不同网段之间的通信。

1. 网桥的基本功能

(1) 过滤通信量。网桥具有帧过滤的功能,可以按目的地址过滤、源地址过滤和协议过滤,可以阻止某些帧通过网桥,使局域网各网段成为隔离开的碰撞域。

(2) 扩大了物理范围。因而也增加了整个局域网上工作站的最大数目。

(3) 提高了可靠性。当隔离开的碰撞域出现故障时,一般只影响个别网段。

(4) 可互连不同物理层、不同 MAC 子层和不同速率(如 10Mbps 和 100Mbps 以太网)的局域网。

由于网桥对接收的帧要先存储和查找站表,然后才转发,这就增加了时延。

前面提到网桥的最主要功能是在不同局域网之间进行互联。由于不同局域网在帧格式、数据传输率、CRC 校验等方面都不相同。这些方面都涉及帧的分段和重组,帧的分段和重组工作必须快速完成,否则会降低网桥的性能。

另外,网桥还必须具有一定的管理功能,以便对扩展网络进行有效管理。例如,可对网桥转发及丢弃的帧进行统计,及时修改网桥地址映象表,某些类型的网桥还可以通过生成树算法动态调整扩展网络的拓扑结构以适应网络的变化。

网桥的缺点:①增加时延;②MAC 子层没有流量控制功能;③不同 MAC 子层的网段桥接在一起时,帧格式的转换速率降低;④网桥只适合于用户数不多和通信量不太大的局域网,否则有时还会因传播过多的广播信息而产生网络拥塞,这就是所谓的广播风暴。

2. 网桥的工作原理

下面我们主要讨论两种最常见的网桥:透明网桥和源路由网桥。

1) 透明网桥

透明网桥(Transparent Bridge)是由 DEC 公司针对以太网提出的桥接技术。所谓"透明"是指 LAN 上的每个站并不知道所发送的帧将经过哪几个网桥,而网桥对各站来说是看不见的。

透明网桥的基本思想是:网桥自动了解每个端口所接同段的物理地址(MAC 地址),形成一个地址映像表,网桥每次转发帧时,先查地址映像表,如查到,则向相应端口转发;如查不到,则向除接收端口之外的所有端口转发或扩散。

对于到来帧的处理取决于它来自哪个 LAN 以及目的地属于哪个 LAN:

(1) 学习:当接收到一个数据帧时,将源 MAC 地址与接收的端口号写入地址映射表。

(2) 过滤:如果源和目的地 LAN 相同,则丢弃此帧。

(3) 转发:若目的地址在地址映射表中存在并和源地址在不同端口,则由此端口转发。

(4) 泛洪:若目的地址不在映射表中,则向除源端口外的所有端口转发该帧。

在上述过程中,网桥在站表中登记三个信息:

(1) 站地址:收到的帧的源 MAC 地址。

(2) 端口:收到的帧进入该网桥的端口号。

(3) 时间:收到的帧进入该网桥的时间。超时或过期时移除此条目。

网桥站表的形成基于这样的原理:若网桥现在能从端口 x 收到从源地址 A 发来的帧,

则以后就可以从端口 x 将一个帧转发到目的地址 A。

透明网桥是通过逆向学习算法(Backward Learning)来填写地址映像表的。当网桥刚接入时,其地址映像表是空的,此时,网桥采用扩散技术将接收的帧转发到桥的所有端口上(接收帧的端口除外)。透明网桥通过查看转发帧的源地址就可以知道通过哪个 LAN 访问某个站点。

为了说明透明网桥的工作原理,我们先看图 3-22 的例子。

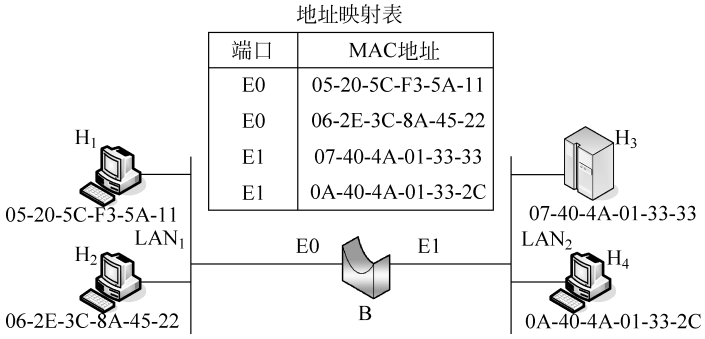


图 3-22　透明网桥的工作原理示意图

在图 3-22 中,网桥 B 连接 LAN_1 和 LAN_2,主机 H_1、H_2 接在 B 的 E0 端口上,主机 H_3、H_4 接在 B 的 E1 端口上。

若 H_1 向 H_2 发送数据:

(1) 取目的地址:网桥 B 取出帧中的目的地址 06-2E-3C-8A-45-22。

(2) 查地址映射表:表中目的地址 06-2E-3C-8A-45-22 对应的端口为 E0。

(3) 比较:发送端口与目的端口一致。

(4) 过滤:丢弃该帧。

若 H_1 向 H_3 发送数据帧:

(1) 取目的地址:网桥 B 取出帧中的目的地址 07-40-4A-01-33-33。

(2) 查地址映射表:表中目的地址 07-40-4A-01-33-33 对应的端口为 E1。

(3) 比较:发送端口 E0 与目的端口 E1 不相同。

(4) 转发:经 E1 端口转发该数据帧至 LAN_2。

下面举例说明 MAC 地址表构建过程,如图 3-23 所示,网桥 1 和网桥 2 刚刚接入以太网,MAC 地址表是空的。

(1) 计算机 A 给计算机 B 发送一个帧,源 MAC 地址为 MA,目标 MAC 地址为 MB。网桥 1 的 E0 接口收到该帧,查看该帧的源 MAC 地址是 MA,就可以断定 E0 接口连着 MA,于是在 MAC 地址表记录一条对应关系 MA 和 E0,这就意味着以后要有到达 MA 的帧需要转发给 E0。

(2) 网桥 1 在 MAC 地址表中没有找到关于 MB 和接口的对应关系,就会将该帧转发到 E1。

(3) 网桥 2 的 E2 接口收到该帧,查看该帧的源 MAC 地址,就会在 MAC 地址表中记录一条 MA 和 E2 的对应关系。

(4) 这时,计算机 F 给计算机 C 发送一个帧,会在网桥 2 的 MAC 地址表添加一条 MF

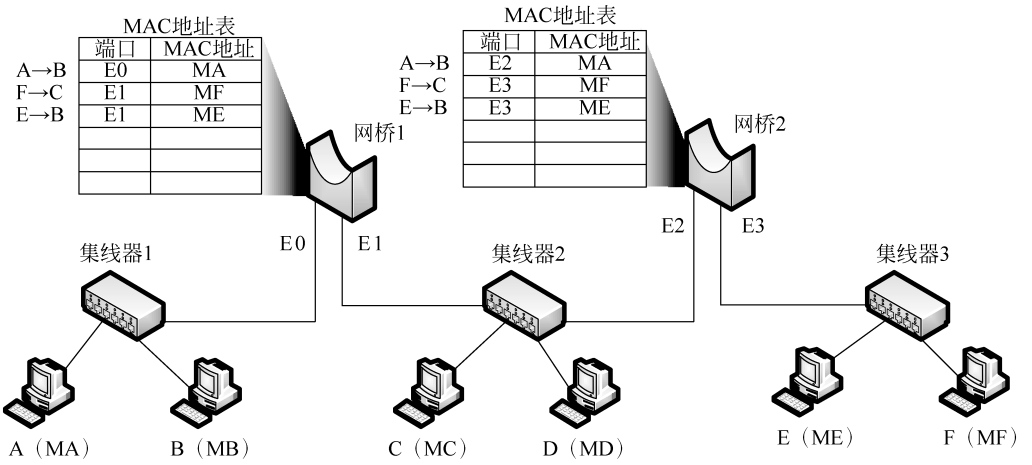


图 3-23 MAC 地址表构建过程

和 E3 的对应关系。由于网桥 2 的 MAC 地址表没有 MC 和接口的对应关系，该帧会被发送到 E2 接口。

(5) 网桥 1 的 E1 接口收到该帧，会在 MAC 地址表添加一条 MF 和 E1 的对应关系，同时将该帧发送到 E0 接口。

(6) 同样，计算机 E 给计算机 B 发送一个帧，会在网桥 1 的 MAC 地址表添加 ME 和 E1 的对应关系，在网桥 2 的 MAC 地址表添加 ME 和 E3 的对应关系。

只要网桥接收到的帧的目标 MAC 地址能够在 MAC 地址表中找到和接口的对应关系，就会将该帧转发到指定接口。

网桥 MAC 地址表中 MAC 地址和接口的对应关系只是临时的，这是为了适应网络中的计算机发生的调整，例如连接在集线器 1 上的计算机 A 连接到了集线器 2，或者计算机 F 从网络中移除了，网桥中的 MAC 地址表中的条目就不能一成不变。而且接口和 MAC 地址的对应关系有时间限制，如果过了几分钟没有使用该对应关系转发帧，该条目将会从 MAC 地址表中删除。

一般在一对 LAN 之间可以使用多个这种桥接器来连接，以增加可靠性。多条路由的存在意味着有一个闭合的环。为了避免转发的帧在网络中不断地“兜圈子”，产生帧传送的回路，透明网桥还使用了一个生成树(Spanning Tree)算法来覆盖实际的拓扑结构，使得从每一个源到每个目的地只有唯一的通路。生成树使得整个扩展局域网在逻辑上形成树型结构，所以工作起来逻辑上没有环路，但生成树一般不是最佳路由。

IEEE 802.3 以太网选用的是透明网桥方案。透明网桥的优点是安装容易，它犹如一个黑盒子，对网上主机完全透明。其缺点是不能选择最佳路径，无法利用冗余网桥来分担负载。

当互连局域网的数目非常大时，支撑树的算法可能要花费很多的时间。

2) 源路由网桥

源路由网桥(Source-Route Bridge，SRB)即源选径网桥，其核心思想是发送方知道目的站点的位置，并将路径中间所经过的网桥地址包含在帧头中一并发出，路径中的网桥依照帧头中的下一站网桥地址将帧一一转发，直到将帧传送到目的地。

确定路由：

(1) 源站以广播的方式向欲通信的目的站发送一个发现帧，作为探测之用；

(2) 发现帧在整个扩展的 LAN 中沿所有可能的路由传送，在传送过程中，每个发现帧都记录它所经过的路由；

(3) 发现帧到达目的站后，再沿原路返回源站；

(4) 源站得到这些路由后，从所有可能的路由中选择一个最佳的路径，以后凡从这个源站向该目的站发送的帧的首部都携带源站所确定的这一路由信息。

为了说明源路由网桥的工作原理，我们先来考察图 3-24 的例子。

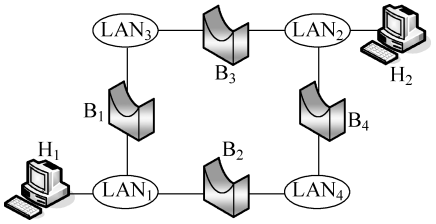


图 3-24　4 个源选径网桥和 4 个局域网的配置

对于图 3-24 的例子，H_1 想向 H_2 发送数据帧，则 H_1 首先发送一个测试帧以检测 H_2 是否与 H_1 在同一网段上；如果测试后发现 H_2 与 H_1 不在同一网段上，则 H_1 将进行下列动作：

第一步，H_1 发出一个探测帧，探测 H_2 的所在位置。

第二步，网桥 B_1 和 B_2 都收到 H_1 发出的探测帧，它们分别在探测帧中加进路由信息，然后将探测帧分别转发到 LAN_3 和 LAN_4。

第三步，网桥 B_3 和 B_4 也收到 H_1 发出的探测帧，它们也分别在探测帧中加进自己的路由信息，然后继续将探测帧转发到 LAN_2。

第四步，H_2 收到两个探测帧，H_2 检查探测帧中累积的路由信息，然后分别沿着探测帧来的路径发响应帧。

第五步，H_1 收到 H_2 发来的两个响应帧，从而得知有两条路径可以到达 H_2，分别为：$LAN_1 \rightarrow B_1 \rightarrow LAN_3 \rightarrow B_3 \rightarrow LAN_2$ 和 $LAN_1 \rightarrow B_2 \rightarrow LAN_4 \rightarrow B_4 \rightarrow LAN_2$。

最后，H1 选择其中一条路径，将路由信息加到数据帧中发给 H_2。

需要注意的是，源路由网桥必须对 IEEE 802.5 的帧格式进行扩充。如果 IEEE 802.5 帧格式中的源地址字段最高位为“1”，则表明源地址字段之后还有一个路由信息字段(Route Information Field，RIF)，该字段包含了如何到达目的结点的路径信息；并将 IEEE 802.5 帧格式中的源地址字段最高位称为路由信息标识符(Route Information Indicator，RII)。

源路由网桥只关心源地址字段中 RIF 位为“1”的帧。对于这些帧，网桥扫描 RIF 字段并根据 RIF 中的路由信息进行帧的转发。

源路由算法能寻找最佳路径，因而可以充分利用冗余的网桥来分担负载，其缺点是存在帧爆发现象。特别当互联网络规模很大时，包含很多网桥和局域网，广播帧的数目在网内剧增，会产生拥挤现象。

3) 两种网桥的比较

使用源路由网桥可以利用最佳路由。若在两个以太网之间使用并联的源路由网桥,还可使通信量较平均地分配给每一个网桥。用透明网桥则只能使用生成树,而使用生成树一般并不能保证所使用的路由是最佳的,也不能在不同的链路中进行负载均衡。

3.6.3 局域网交换机

1. 局域网交换机

桥接器的主要限制是在任一时刻通常只能执行一个帧的转发操作,于是就出现了局域网交换机,又称以太网交换机。从本质上说,以太网交换机就是一个多端口的网桥,工作在数据链路层。交换机能将网络分成小的冲突域,为每个工作站提供更高的带宽。

以太网交换机对工作站是透明的,这样管理开销低廉,简化了网络结点的增加、移动和网络变化的操作。利用以太网交换机还可以很方便地实现虚拟局域网 VLAN,VLAN 不仅可以隔离冲突域,也可以隔离广播域。

2. 交换机工作原理

在介绍交换机的工作原理之前,我们先来比较一下集线器与交换机的特点。

(1) 从工作现象看,它们都是通过多端口连接以太网的设备,可以将多个用户通过网络以星型结构连接起来,共享资源或交换数据。

(2) 从外观上看,交换机跟集线器差不多,但端口的数目可能比集线器多(一般情况下是 24 个或更多)。

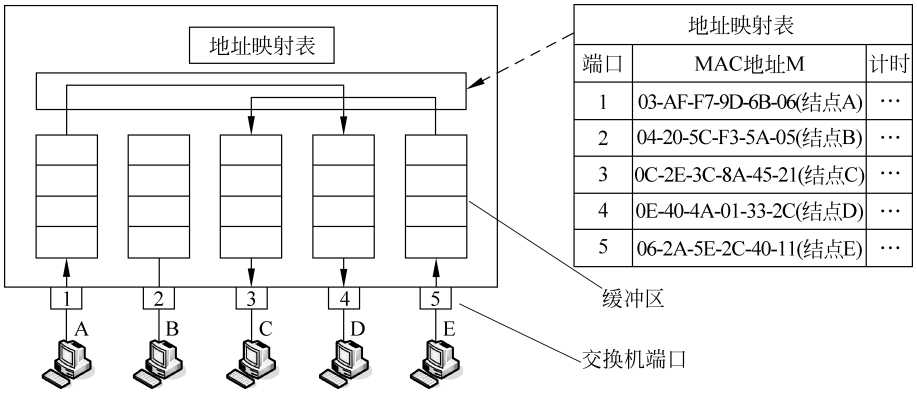
(3) 设备结构、工作原理不同。集线器是一种"盒中总线"的结构,采用的是共享带宽的工作方式,同一时间只能有一个端口转发数据;交换机采用专用的交换结构芯片,是一个独享带宽的通道,它能确保每个端口使用的带宽,如百兆的交换机,它能确保每个端口都有百兆的带宽。

(4) 转发方式不同。交换机跟集线器的最大区别就是转发方式不同,交换机能做到接口到接口的转发。例如接收到一个数据帧以后,交换机会根据数据帧头中的目的 MAC 地址发送到适当的端口;而集线器则不然,它把接收到的数据帧向所有端口转发。交换机之所以能做到根据 MAC 地址进行选择端口,完全依赖于内部的一个重要的数据结构:地址映射表。

集线器是工作在物理层的设备;以太网交换机是工作在数据链路层的设备。

(5) 集线器所有端口是一个广播域,所有端口是一个冲突域;而以太网交换机所有端口是一个广播域,但每个端口是一个独立的冲突域。例如,对于 4 端口的集线器:广播域是 1,冲突域也是 1;对于 12 端口的交换机:广播域是 1,冲突域是 12。

交换机的工作原理:它检测从以太网端口来的数据帧的源 MAC 地址和目的 MAC 地址,然后与系统内部的地址映射表进行比较(地址映射表的建立过程可参考网桥的工作原理),若数据帧的源 MAC 地址不在表中,则将该地址加入地址映射表中,并将数据帧发送给相应的目的端口,交换机的工作原理与网桥相同。交换机的内部结构与工作原理如图 3-25 所示。



地址映射表		
端口	MAC地址M	计时
1	03-AF-F7-9D-6B-06(结点A)	…
2	04-20-5C-F3-5A-05(结点B)	…
3	0C-2E-3C-8A-45-21(结点C)	…
4	0E-40-4A-01-33-2C(结点D)	…
5	06-2A-5E-2C-40-11(结点E)	…

图 3-25　交换机的结构与工作原理

3. 交换机的特点

以太网交换机的特点如下：

(1) 每个端口都直接与单个主机相连(普通网桥的端口往往是连接到以太网的一个网段)，并且一般都工作在全双工方式。

(2) 它能同时连通许多对的端口，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。

(3) 它也是一种即插即用设备(和透明网桥一样)，其内部的帧的地址映射表也是通过自学习算法自动地逐渐建立起来的。

(4) 由于使用了专用的交换结构芯片，其交换速率较高。

(5) 独占传输媒体的带宽。

对于普通 10Mbps 的共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽(10Mbps)的 N 分之一。在使用以太网交换机时，虽然在每个端口到主机的带宽还是 10Mbps，但由于一个用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此对于拥有 N 对端口的交换机的总容量为 $N\times10$Mbps。这正是交换机的最大优点。

以太网交换机一般都具有多种速率的端口，例如，可以具有 10Mbps、100Mbps 和 1Gbps 的端口的各种组合，这就大大方便了各种不同情况的用户。

4. 以太网交换技术

以太网交换机的交换方式分为静态方式和动态方式。静态方式的特点是端口间的通道由人工事先配置，两个端口间的连接类似于硬件连接，端口按固定的连接方式交换帧。

动态交换方式又分为：存储转发(Store Forward)；直通；自由分段(帧碎片丢弃)。下面分别予以介绍。

(1) 存储转发方式

当交换机运行存储转发模式时，在转发数据帧之前必须接收整个帧，交换机接收到完整的数据帧以后，检查其源地址和目标地址，并对整个帧进行 CRC(循环冗余校验)。如果交换机没有发现错误，它将继续转发这个帧；如果交换机发现数据帧中存在错误，它将丢弃这

个帧。

(2) 直通转发方式

直通转发方式(也称为直通式)允许交换机在检查到数据帧中的目标地址时就开始转发数据帧。目标地址在数据帧中占用 6Byte(这 6Byte 正是目标设备的 MAC 地址),所以直通式的延迟很小。

(3) 自由分段方式

自由分段方式有效地结合了直通式和存储转发模式的优点。当交换机工作在自由分段模式时,它只检查数据帧的前 64Byte,如果前 64Byte 没有出现错误,交换机就转发该帧。反之,如果检测到前 64Byte 出错,交换机就丢弃该帧。

交换机的每种工作方式都有各自的优点和缺点。其主要体现在两个方面:错误检测和延迟。

存储转发工作方式:检查整个数据帧,如果发现错误,则丢弃该帧。延迟随数据帧的长度而变化,不固定,延迟最大。

直通式工作方式:不进行帧的错误检查,收到前 6Byte 直接转发。延迟是固定的,属于低延迟。

自由分段工作方式:检查前 64Byte,如果发现错误,则丢弃该帧。延迟是固定的,比直通式稍大。

3.7 高速以太网

1995 年,IEEE 公布了 100Mbps 以太网标准 IEEE 802.3u,命名为 100Base-T,100Mbps 以太网以它的价格低廉和与传统以太网相兼容的优势迅速占领了整个局域网市场,速率达到或超过 100Mbps 的以太网称为快速以太网。

3.7.1 100Base-T 以太网

100Base-T 是在 10Mbps 系列 IEEE 802.3 传统以太网的基础上开发出来的,为了与传统以太网兼容,提供了 10M/100Mbps 双速自适应功能,具有协商功能,也被用来判定双方设备室采用半双工还是全双工方式工作。该以太网既支持全双工又支持半双式方式,可在全双工方式下工作而无冲突发生。因此,在全双工方式下不使用 CSMA/CD 协议。

1. 100Base-T 以太网的特点

(1) MAC 帧格式仍然是 802.3 标准规定的。

(2) 保持最短帧长 64Byte 不变,但将一个网段的最大电缆长度减小到 100m。

(3) 帧间间隔从原来的 9.6μs 改为现在的 0.96μs。

(4) 使用新的编码方式取代低效的曼彻斯特编码。

100Base-T 不再支持同轴电缆介质和总线型拓扑,100Base-T 中所有的电缆连接都是点对点的星型拓扑。

2. 100Base-T 以太网的物理层标准

IEEE 802.3u 标准定义了不同的物理层规范以支持不同的物理介质。

(1) 100Base-TX：使用 5 类以上的 UTP 或 STP，通信中使用两对双绞线，其中一对用于发送，另一对用于接收。在传输中使用 4B/5B 编码方式，支持半双工/全双工系统。

(2) 100Base-FX：使用两根独立的多模光纤作为传输介质，其中一根用于发送，另一根用于接收，光纤的最大长度为 412m。信号的编码采用 4B/5B-NRZ1 编码，100Base-FX 允许工作在全双工方式下，这时其跨距可增加到 2km。

(3) 100Base-T4：使用 4 对 3 类以上的 UTP，它是为已使用 3 类 UTP 的大量用户而设计的。信号的编码采用 8B6T-NRZ(不归零)的编码方法。100Base-T4 使用 3 对线同时传送数据，使每一对线的传输速率达到 33.3Mbps，将另一对线作为冲突检测的接收信道。

快速以太网支持结构化布线，包括 3 类、4 类、5 类无屏蔽双绞线、150Ω 屏蔽双绞线(STP)以及光纤，这些介质都是当前流行的，且各类介质可混合使用，通过中继器或交换器连接起来。

3.7.2 吉比特以太网

1996 年，IEEE 成立了千兆以太网(Gigabit Ethernet，GE)工作组来制定千兆以太网的标准，1998 年 6 月，IEEE 制定了第一个使用光纤线缆和短程铜线线缆的千兆以太网标准 IEEE 802.3z。1999 年公布了使用双绞线的 IEEE 802.3ab。吉比特以太网迅速占领了市场，成为以太网的主流产品。

1. 吉比特以太网的特点

(1) 允许以 1000Mbps 的速度进行半双工或全双工操作。

(2) 保持 IEEE 802.3 以太网帧格式不变。

(3) 帧间间隔改为 0.096μs。

(4) 在半双工方式下继续使用 CSMA/CD 协议。

(5) 与 10Base-T 和 100Base-T 技术向后兼容。

2. 吉比特以太网的物理层标准

(1) 1000Base-X(IEEE 802.3z 标准)

1000Base-LX：可支持单模光纤，采用 8B/10B 编码，传输距离一般可达 5km 以上；也可支持多模光纤，一般为 550km(50μm 多模)，它主要应用在园区网络的骨干连接。

1000Base-SX：可支持多模光纤，采用 8B/10B 编码，传输距离依据不同的光纤标准为 220～550m，它主要应用在建筑物内的网络骨干连接。

1000Base-CX：用于屏蔽双绞线电缆 STP，传输距离为 25m，采用 8B/10B 编码。它主要应用在高速存储设备之间的低成本高速互连。

(2) 1000Base-T(IEEE 802.3ab 标准)

1000Base-T：定义在传统的 5 类双绞线上将传输距离提高到 100m，可应用于高速服务器和工作站的网络接入，也可作为建筑物内的 1000Mbps 骨干连接。

IEEE 802.3z 和 IEEE 802.3ab 都能实现 1Gbps 的数据传输,不同的是它们定义了不同传输介质的技术规范。IEEE 802.3z 主要定义基于光缆和短距离同轴电缆的 1000Base-X,它采用了 8B/10B 编码技术,信道信号速率达 1.25Gbps。IEEE 802.3ab 定义了基于 5 类非屏蔽双绞线的 1000Base-T 规范,它的最终目的是在 5 类非屏蔽双绞线上实现最长距离达 100m 的 1000Mbps 的以太网数据传输速率。

当吉比特以太网工作在半双工方式时,就必须进行碰撞检测。

由于数据率提高了,因此只有减小最大电缆长度或增大帧的最小长度,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"载波扩展"的办法,使最短帧长仍为 64 字节(这样可以保持兼容性),同时将争用时间增大为 512 字节。凡发送的 MAC 帧长不足 512 字节时,就用一些特殊字符填充在帧的后面,使 MAC 帧的发送长度增大到 512 字节,这对有效载荷并无影响,如图 3-26 所示。

图 3-26 带有扩展的千兆以太网帧格式

使用载波扩展技术,当网络中短帧较多时,网络性能会大大降低,为了解决这个问题,吉比特以太网还增加一种功能称为帧突发(Frame Bursting)技术,用来提高半双工方式下吉比特以太网的性能,就是当很多短帧要发送时,第一个短帧要采用上面所说的载波延伸的方法进行填充。但随后的一些短帧则可一个接一个地发送,它们之间只需留有必要的帧间最小间隔即可。

这样就形成了一串分组的突发,直到达到 1500 字节或稍多一些为止,如图 3-27 所示。

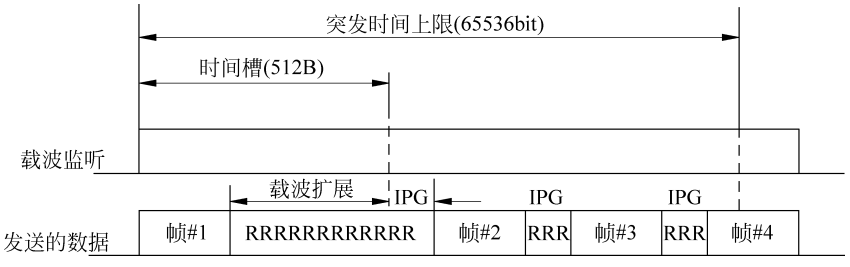


图 3-27 帧突发示意图

当吉比特以太网工作在全双工方式时(即通信双方可同时进行发送和接收数据),不采用 CSMA/CD 协议,因此不需要载波延伸和帧突发。

3.7.3 10吉比特以太网

10吉比特以太网也称为万兆网，10吉比特以太网并非将吉比特以太网的速率简单地提高到10倍。万兆以太网技术的研究始于1999年年底，当时成立了IEEE 802.3ae工作组，并于2002年6月正式发布IEEE 802.3ae 10GE标准。

1. 万兆位以太网的特点

(1) 把数据速率提升到10Gbps。
(2) 跟标准的、快速的、千兆位的以太网兼容。
(3) 只工作在全双工方式，不再使用CSMA/CD协议。
(4) 使用同样的帧格式。
(5) 保持同样的最小和最大帧长度。
(6) 只使用光纤作为传输介质。

IEEE为万兆位以太网建立了IEEE 802.3ae标准。万兆位以太网仅仅以全双工的方式运行，不需要竞争，不使用在千兆位以太网中还使用的CSMA/CD。

2. 万兆网的物理层

万兆位以太网的物理层的设计使用长距离的光纤。3种最普遍的实现方式如下：
(1) 10GBase-S：多模，短波长850nm，300m距离；
(2) 10GBase-L：单模，长波长1310nm，10km距离；
(3) 10GBase-E：单模，扩展波长1550nm，40km距离。

在数据链路层IEEE 802.3ae继承了IEEE 802.3以太网的帧格式和帧长度，支持多层星型连接、点到点连接及其组合，充分兼容已有应用，且不影响上层应用，进而降低了升级风险。

万兆以太网的应用领域主要是用于大型网络的主干网连接。

3.8 虚拟局域网(VLAN)

虚拟局域网(Virtual Local Area Network，VLAN)是指在交换式局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。IEEE于1999年颁布了用以标准化VLAN实现方案的IEEE 802.1Q协议标准草案。

VLAN技术的出现，主要是为了解决交换机在进行局域网互联时无法限制广播的问题。这种技术可以把一个LAN划分成多个逻辑的LAN—VLAN，每个VLAN都是一个广播域，VLAN内的主机间通信就像在一个VLAN内一样，而不同VLAN间则不能直接互通。

用集线器、网桥和未划分VLAN的交换机组建的传统网络中存在下列问题：
(1) 全网属于一个广播域，每一次广播的数据帧无论是否需要，都会到达网络中的所有设备，这就必然造成带宽资源的极大浪费。

(2) 全网属于一个广播域,很容易引起广播风暴等问题。

(3) 网络的安全性不高。在这种网络结构中,所有用户都可以监听到服务器以及其他设备端口发出的数据包,所以很不安全。

VLAN 允许一组不同物理位置的用户群共享一个独立的广播域,可以在一个物理网络中划分多个 VLAN,使得不同的用户群属于不同的广播域。

VLAN 在网络管理中具有以下三个优点:

(1) 控制广播风暴。

(2) 提高网络整体安全性。

(3) 方便的网络管理。

图 3-28 是没有划分 VLAN 的传统局域网,它有三个局域网,分别为 LAN1、LAN2 和 LAN3,分别是三个不同的广播域。由于网络的物理结构隔断了相同部门之间的资源共享,给业务处理带来了很多不便。

采用如图 3-29 所示的 VLAN 技术,根据业务关系将它们重新进行划分,组成三个 VLAN:VLAN1(教务处)、VLAN2(学生处)和 VLAN3(财务处),根据业务需求重新划分了广播域,使得相同部门的业务可以直接广播信息。

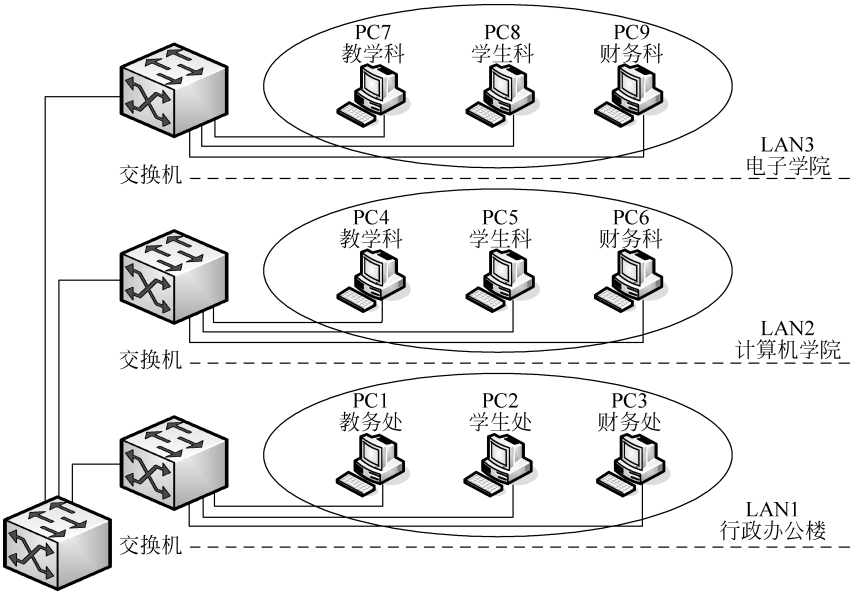


图 3-28 交换机将以太网分段

VLAN 的实现方式:VLAN 划分的方式分为静态 VLAN 和动态 VLAN。

1. 静态 VLAN

静态 VLAN 是基于端口的 VLAN,它是将端口强制性地分配给 VLAN。这是一种最经常使用的配置方式。静态 VLAN 容易实现和监控,而且比较安全。

这是一种最简单的 VLAN。划分静态 VLAN 时,既可以把同一交换机的不同端口划分为同一 VLAN,如图 3-30 所示,也可以把不同交换机的端口划分为同一 VLAN,如图 3-31 所示,可以把位于不同物理位置、连接在不同交换机上的用户按照一定的逻辑功能

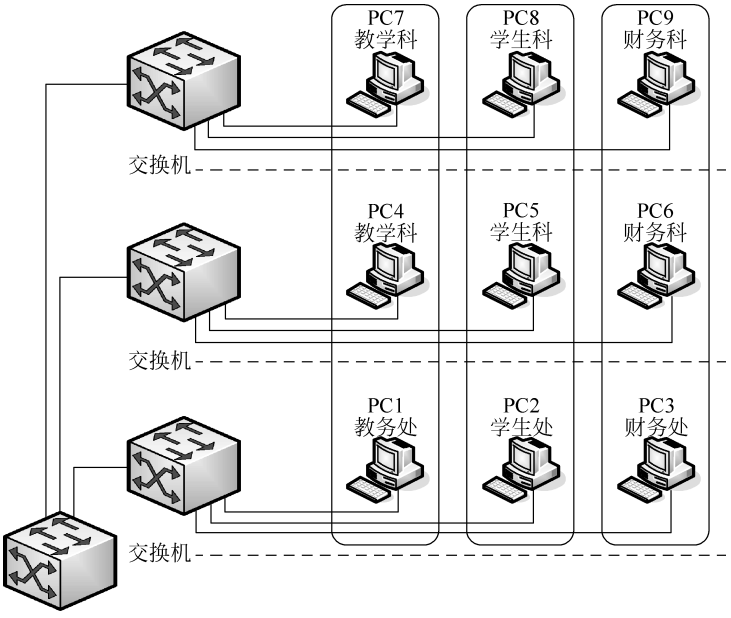


图 3-29　VLAN 分段

和安全策略进行分组，根据需要将其划分为同一或不同的 VLAN。静态 VLAN 通常使用网络管理软件来配置和维护端口。若需要改变端口的属性，必须手动重新配置，所以具有很好的安全性。

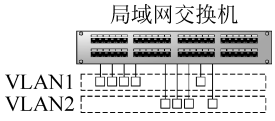


图 3-30　同一交换机的不同端口划分为同一 VLAN

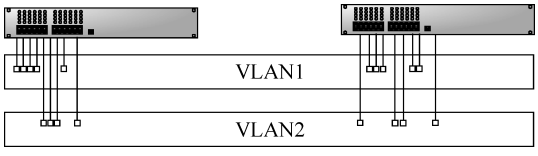


图 3-31　不同交换机的端口划分为同一 VLAN

2. 动态 VLAN

动态 VLAN 是一种较为复杂的划分方法。它可以通过基于硬件的 MAC 地址、IP 地址等条件划分。

(1) 基于 MAC 地址的 VLAN 划分

动态划分 VLAN 的方法是根据每个主机的 MAC 地址来划分。在这种实现方式中，我们必须先建立一个较复杂的数据库，数据库中包含了要连接的网络设备的 MAC 地址及相应的 VLAN 号。这样当网络设备接到交换机端口时，交换机会自动把这个网络设备分配给相应的 VLAN。

基于 MAC 地址的 VLAN 在把网络上的工作站移动到网络上的不同物理位置时，无须

重新配置 VLAN。但当更换网卡或增加工作站时,需要重新配置数据库,而且需要手动建立 MAC 地址的数据库。

(2) 基于 IP 地址的 VLAN 划分

在基于 IP 地址的 VLAN 中,新站点在入网时无须进行太多配置,交换机则根据各站点网络地址自动将其划分成不同的 VLAN。可以按传输协议划分网段,用户可以在网络内部自由移动而不用重新配置自己的工作站。

由于检查 IP 地址比检查 MAC 地址要花费更多的时间,因此用 IP 地址划分 VLAN 的速度比较慢。

3.9 无线局域网

前面讨论的都是有线局域网,其传输介质主要依赖铜缆或光缆。但有线网络在某些场合受到布线的限制:布线、改线工程量大;线路容易损坏;网中的各结点不可移动。对正在迅速扩大的连网需求形成了严重的瓶颈阻塞。

无线局域网(Wireless Local Area Network,WLAN)是指以无线信道作传输介质的计算机局域网,无须布线即可实现计算机之间互连的网络。无线网络的适用范围非常广泛,它不但能够替代传统的物理布线,而且在传统布线无法解决的环境或行业中都能够方便地组建无线网络。同时,在许多方面,无线网络比传统的有线网络具有明显的优势。

1998 年,IEEE 制定出无线局域网的协议标准 IEEE 802.11,802.11 使用星型拓扑,其中心叫作接入点 AP(Access Point),在 MAC 层使用 CSMA/CA 协议,凡使用 802.11 系列协议的局域网又称为 Wi-Fi(Wireless-Fidelity,意思是"无线保真度")。因此,Wi-Fi 几乎成了无线局域网 WLAN 的同义词。

3.9.1 无线局域网基本结构模型

无线局域网可分为两大类:第一类是有中心结构(Infrastucture 模式),第二类是无中心结构(Ad hoc 模式)。

Infrastucture 模式和无线移动通信的蜂窝小区相似。在无线局域网中,Infrastucture 模式的范围可以有几十米的直径,如图 3-32 所示。

Ad hoc 模式的无线局域网,又叫作自组网络(Ad hoc network)。这种自组网络没有上述中心接入点,而是由一些处于平等状态的移动站之间相互通信组成的临时网络,如图 3-33 所示。移动自组网络也就是移动分组无线电网络。

自组网络通常是这样构成的:一些可移动的设备发现在它们附近还有其他的可移动设备,并且要求和其他移动设备进行通信。便携式计算机的大量普及,自组网络的组网方式已受到人们的广泛关注。由于在自组网络中的每一个移动站都要参与到网络中的其他移动站的路由的发现和维护,同时由移动站构成的网络拓扑有可能随时间变化得很快,因此在固定网络之中行之有效的一些路由选择协议对移动自组网络已不适用,这样,路由选择协议在自组网络中就引起了特别的关注。另一个重要问题是多播,在移动自组网络中往往需要将某个重要信息同时向多个移动站传送。这种多播比固定结点网络的多播要复杂得多,需要

有实时性好而效率又高的多播协议。在移动自组网络中，安全问题也是一个更为突出的问题。

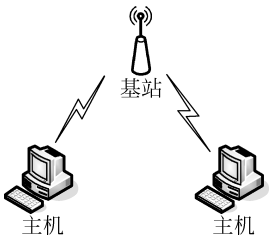


图 3-32　有中心结构

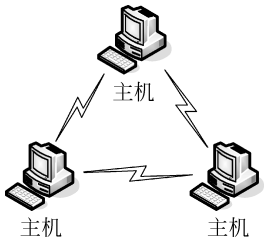


图 3-33　Ad hoc 网络结构

移动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，由于战场上往往没有预先建好固定接入点，但携带了移动站的战士就可以利用临时建立的移动自组网络进行通信。这种组网方式也能够应用到作战的地面车辆群和坦克群，以及海上的舰艇群，空中的机群。由于每一个移动设备都具有路由器的转发分组的功能，因此分布式的移动自组网络的生存性非常好。在民用领域，开会时持有笔记本电脑的人可以利用这种移动自组网络方便交换信息，而不受笔记本电脑附近没有电话线插头的限制。当出现自然灾害时，在抢险救灾时利用自组网络进行及时的通信往往也是很有效的，因为这时事先已建好的固定网络基础设施（基站）可能已经都被破坏了。

下面我们对有固定基础设施的无线局域网进行更加细致的讨论。

3.9.2　IEEE 802.11 物理介质规范

IEEE 802.11 标准的物理层有以下三种实现方法。

（1）跳频扩频（Frequency Hopping Spread Spectrum，FHSS）是扩频技术中常用的一种。它使用 2.4GHz 的 ISM 频段（即 2.4000～2.4835GHz），共有 79 个信道可供跳频使用。第一个频道的中心频率为 2.402GHz，以后每隔 1MHz 一个信道。因此每个信道可使用的带宽为 1MHz。当使用二元高斯移频键控 GFSK 时，基本接入速率为 1Mbps。当使用四元 GFSK 时，接入速率为 2Mbps。

（2）直接序列扩频（Direct Sequence Spread Spectrum，DSSS）是另一种重要的扩频技术。它也使用 2.4GHz 的 ISM 频段。当使用二元相对移相键控时，基本接入速率为 1Mbps。当使用四元相对移相键控时，接入速率为 2Mbps。

（3）红外线（Infra Red，IR）的波长为 850～950nm，可用于室内传送数据，接入速率为 1～2Mbps。

3.9.3　IEEE 802.3 介质访问控制

1. CSMA/CD 协议在无线网中的不足

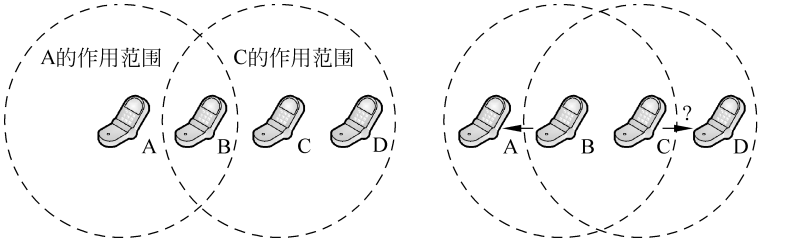
虽然 CSMA/CD 协议已成功地应用于使用有线连接的局域网，但无线局域网不能简单地搬用 CSMA/CD 协议。这里主要有两个原因：

第一，CSMA/CD 协议要求一个站点在发送本站数据的同时还必须不断地检测信道，以

便发现是否有其他的站也在发送,这样才能实现“碰撞检测”的功能。但在无线局域网的设备中要实现这种功能就不太容易。

第二,更重要的是,即使我们能够实现碰撞检测的功能,并且当发送数据时检测到信道是空闲的,在接收端仍然有可能发生碰撞。这就表明,碰撞检测对无线局域网没有什么用处。

产生这种结果是由无线信道本身特点决定的。具体地说,这是由于无线电波能够向所有的方向传播,且传播距离受限。当电磁波在传播过程中遇到障碍物时,其传播距离就更加受到限制。图 3-34 的例子表示了无线局域网的特殊问题。图中画有 4 个无线移动站,并假定无线电信号传播的范围是以发送站为圆心的一个圆形面积。



(a) A和C同时向B发送信号,发生碰撞　　(b) B向A发送信号,影响C向D发送数据

图 3-34　无线局域网的问题

图 3-34(a)表示站 A 和 C 都想和 B 通信,但 A 和 C 相距较远,彼此都接收不到对方发送的信号。当 A 和 C 检测不到无线信号时,就都以为 B 是空闲的,因而都向 B 发送自己的数据。结果 B 同时收到 A 和 C 发来的数据,发生了碰撞。可见在无线局域网中,在发送数据前未检测到媒体上有信号还不能保证在接收端能够成功地接收到数据。这种未能检测出媒体上已存在的信号的问题叫作隐蔽站问题(Hidden Station Problem)。

当移动站之间有障碍物时也有可能出现上述问题。例如,三个站 A、B 和 C 彼此距离都差不多,但 A 和 C 之间有一座山,因此 A 和 C 都不能检测到对方发出的信号。若 A 和 C 同时向 B 发送数据就会发生碰撞(但 A 和 C 并不知道),则 B 无法正常接收。

图 3-34(b)给出了另一种情况。站 B 向 A 发送数据,而 C 又想和 D 通信,但 C 检测到媒体上有信号,于是就不敢向 D 发送数据。其实 B 向 A 发送数据并不影响 C 向 D 发送数据,这就是暴露站问题(Exposed Station Problem)。在无线局域网中,在不发生干扰的情况下,可允许同时多个移动站进行通信。这点与总线式局域网有很大的差别。

除以上两个原因外,无线信道还由于传输条件特殊,造成信号强度的动态范围非常大,致使发送站无法使用碰撞检测的方法来确定是否发生了碰撞。

因此,无线局域网不能使用 CSMA/CD,而只能使用改进的 CSMA 协议。

改进的办法是将 CSMA 增加一个碰撞避免(Collision Avoidance)功能。于是 IEEE 802.11 就使用 CSMA/CA 协议,而在使用 CSMA/CA 的同时还增加使用确认机制。

2. IEEE 802.11 的介质访问控制机制

下面在讨论 CSMA/CA 协议之前,我们先介绍 IEEE 802.11 的 MAC 层。

1）IEEE 802.11 的 MAC 层

IEEE 802.11 标准设计了独特的 MAC 层，如图 3-35 所示。

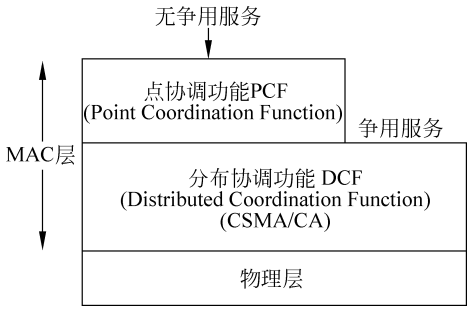


图 3-35　IEEE 802.11 标准中的 MAC 层

它通过协调功能(Coordination Function)确定基本服务集 BSS 中的移动站在什么时间能发送数据或接收数据。IEEE 802.11 的 MAC 层在物理层的上面，它包括两个子层。在下面的一个子层是分布协调功能(Distributed Coordination Function，DCF)。DCF 在每一个结点使用 CSMA 机制的分布式接入算法，让各个站通过争用信道来获取发送权。因此 DCF 向上提供争用服务。另一个子层叫作点协调功能(Point Coordination Function，PCF)。PCF 是选项，自组网络就没有 PCF 子层。PCF 使用集中控制的接入算法(一般在接入点 AP 实现集中控制)，用类似于探询的方法将发送数据权轮流交给各个站，从而避免了碰撞的产生。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。

2）帧间间隔

为了尽量避免碰撞，IEEE 802.11 规定，所有的站在完成发送后，必须再等待一段很短的时间(继续监听)才能发送下一帧。这段时间通称是帧间间隔(InterFrame Space，IFS)。帧间间隔的长短取决于该站打算发送的帧的类型。高优先级帧需要等待的时间较短，因此可优先获得发送权，但低优先级帧就必须等待较长时间。若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变化为忙态，因而低优先级帧就只能再推迟发送了。这样就减少了发生碰撞的机会。常用的三种帧间间隔如图 3-36 所示。

(1) SIFS，即短(Short)帧间间隔，长度为 28μs。SIFS 是最短的帧间间隔，用来分隔属于一次对话的各帧。一个站应当能够在这段时间内从发送方式切换到接收方式。使用 SIFS 的帧类型有：ACK 帧，CTS 帧(在后面第 4 小节中讲)，由过长的 MAC 帧分片后的数据帧，以及所有回答 AP 探询的帧和在 PCF 方式中接入点 AP 发送出的任何帧。

(2) PIFS，即点协调功能帧间间隔(比 SIFS 长)，是为了在开始使用 PCF 方式时(在 PCF 方式下使用，没有争用)优先获得接入到媒体中。PIFS 的长度是 SIFS 加一个时隙(Slot)长度(其长度为 50μs)，即 78μs。时隙的长度是这样确定的：在一个基本服务集 BSS 内，当某个站在一个时隙开始时接入到媒体时，那么在下一个时隙开始时，其他站就能检测出信道已转变为忙态。

(3) DIFS，即分布协调功能帧间间隔(最长的 IFS)，在 DCF 方式中用来发送数据帧和管理帧。DIFS 的长度比 PIFS 再多一个时隙长度，因此 DIFS 的长度为 128μs。

3) CSMA/CA 协议原理

CSMA/CA 协议的原理可用图 3-36 来说明。

欲发送数据的站先检测信道。在 IEEE 802.11 标准规定了在物理层的空中接口进行物理层的载波监听。通过收到的信号强度是否超过一定的门限数值就可以判定是否由其他的移动站在信道上发送数据。当源站发送它的第一个 MAC 帧时,若检测到信道空闲,则在等待一段时间 DIFS 后就可发送。

为什么信道空闲还要再等待呢?就是考虑到可能有其他的站有高优先级的帧要发送。如有,就要让高优先级帧先发送。

现在假定没有高优先级帧要发送,因而源站发送了自己的数据帧。目的站若正确收到此帧,则经过时间间隔 SIFS 后,向源站发送确认帧 ACK。若源站在规定时间内没有收到确认帧 ACK(由重传计时器控制这段时间),就必须重传此帧,直到收到确认为止,或者经过若干次的重传失败后放弃发送。

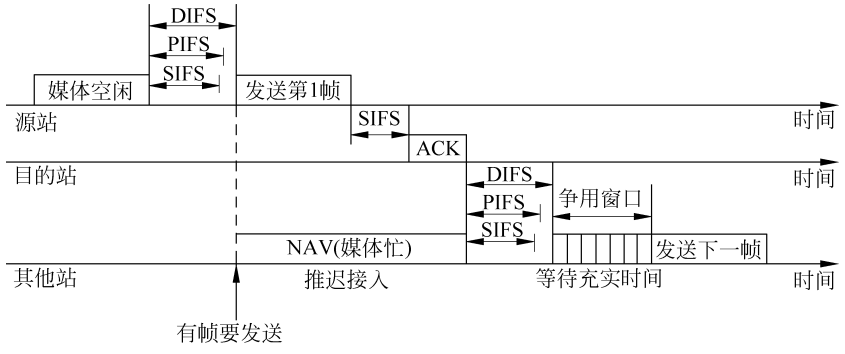


图 3-36 CSMA/CA 协议的工作原理

IEEE 802.11 标准还采用了一种叫作虚拟载波监听(Virtual Carrier Sense)的机制,这就是让源站将它要占用信道的时间(包括目的站发回确认帧所需的时间)通知给所有其他站,以便使其他所有站在这一段时间都停止发送数据,这样就大大减少了碰撞的机会。“虚拟载波监听”是表示其他站并没有监听信道。所谓“源站的通知”就是源站在其 MAC 帧首部中的第二个字段“持续时间”中填入了在本帧结束后还要占用信道多少时间(以微秒为单位),包括目的站发送确认帧所需的时间。

当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时,就调整自己的网络分配向量(Network Allocation Vector,NAV)。NAV 指出了必须经过多少时间才能完成数据帧的这次传输,才能使信道转入到空闲状态。因此,信道处于忙态,或者是由于物理层的载波监听检测到信道忙,或者是由于 MAC 层的虚拟载波监听机制指出了信道忙。

图 3-36 指出,当信道从忙态变为空闲,任何一个站要发送数据时,不仅都必须等待一个 DIFS 的间隔,而且还要进入争用窗口,并计算随机退避时间以便再次重新试图接入到信道。请读者注意,在以太网的 CSMA/CD 协议中,碰撞的每个站执行退避算法是在发生了碰撞之后。但在 802.11 的 CSMA/CA 协议中,因为没有像以太网那样的碰撞检测机制,因此在信道从忙态转为空闲时,各站就要执行退避算法。这样就减少了发生碰撞的概率(当多个站都打算占用信道)。802.11 也是使用二进制指数退避算法,但具体做法稍有不同。这就是,第 i 次退避就在 $22+i$ 个时隙中随机地选择一个,即第 1 次退避是在 8 个时隙(而不是 2

个)中随机选择一个,而第 2 次退避是在 16 个时隙(而不是 4 个)中随机选择一个。

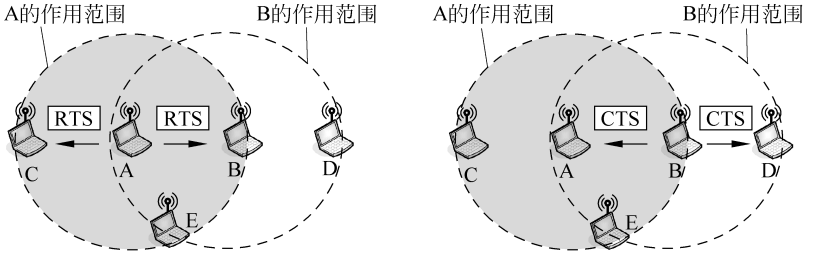
当某个想发送数据的站使用退避算法选择了争用窗口中的某个时隙后,就根据该时隙的位置设置一个退避计时器(Backoff Timer)。当退避计时器的时间减小到零时,就开始发送数据。也可能当退避计时器的时间还未减小到零时而信道又转变为忙态,这时就冻结退避计时器的数值,重新等待信道变为空闲,再经过时间 DIFS 后,继续启动退避计时器(从剩下的时间开始)。这种规定有利于继续启动退避计时器的站更早地接入到信道中。

应当指出,当一个站要发送数据帧时,仅在下面的情况下才不使用退避算法:检测到信道是空闲的,并且这个数据帧是它想发送的第一个数据帧。除此之外的所有情况,都必须使用退避算法。具体来说就是:

- 在发送它的第一个帧之前检测到信道处于忙态。
- 在每一次的重传后。
- 在每一次的成功发送后。

4) 对信道进行预约

为了更好地解决隐蔽站带来的碰撞问题,IEEE 802.11 允许要发送数据的站对信道进行预约。具体的做法是:如图 3-37(a)所示,源站 A 在发送数据帧之前先发送一个短的控制帧,叫作请求发送(Request To Send,RTS),它包括源地址、目的地址和这次通信(包括相应的确认帧)所需的持续时间。若媒体空闲,则目的站 B 就发送一个响应和这次控制帧,叫作允许发送(Clear To Send,CTS),如图 3-37(b)所示,它也包括这次通信所需的持续时间(从 RTS 帧中将此持续时间复制到 CTS 帧中)。A 收到 CTS 帧后就可发送其数据帧。下面讨论在 A 和 B 两个站附近的一些站将做出什么反应。



(a) A发送RTS帧　　(b) B响应CTS帧,D在一段时间内不发送数据

图 3-37　CSMA/CA 协议中的 RTS 和 CTS 帧

C 处于 A 的传输范围内,但不在 B 的传输范围内。因此,C 能够收到 A 发送的 RTS,但经过一小段时间后,C 不会收到 B 发送的 CTS 帧。这样,在 A 向 B 发送数据时,C 也可以发送自己的数据给其他的站而不会干扰 B。请读者注意,C 收不到 B 的信号表明 B 也收不到 C 的信号。

再观察 D,D 收不到 A 发送的 RTS 帧,但能收到 B 发送的 CTS 帧。D 知道 B 将要和 A 通信,D 在 A 和 B 通信的一段时间内不能发送数据,因而不会干扰 B 接收 A 发来的数据。

至于站 E,它能收到 RTS 和 CTS,因此 E 和 D 一样,在 A 发送数据帧和 B 发送确认帧的整个过程中都不能发送数据。

可见这种协议实际上就是在发送数据帧之前先对信道进行预约一段时间。

使用 RTS 和 CTS 帧会使整个网络的效率有所下降。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)相比开销不算大。相反,若不使用这种控制帧,则一旦发生碰撞而导致数据帧重发,则浪费的时间就更多。虽然如此,协议还是设有三种情况供用户选择:一种是使用 RTS 和 CTS 帧;另一种是只有当数据帧的长度超过某一数值时才使用 RTS 和 CTS 帧(显然,当数据帧本身就很短时,再使用 RTS 和 CTS 帧只能增加开销);第三种是不使用 RTS 和 CTS 帧。

虽然协议经过精心设计,但碰撞仍然会发生。例如,B 和 C 同时向 A 发送 RTS 帧。这两个 RTS 帧发生碰撞后,使得 A 收不到正确的 RTS 帧,因而 A 就不会发送后续的 CTS 帧。这时,B 和 C 像以太网发生碰撞那样,各自随机地推迟一段时间后重新发送 RTS 帧。推迟时间的算法也是使用二进制指数退避。

图 3-38 给出了 RTS 和 CTS 帧以及数据帧和 ACK 帧的传输时间关系。在除源站和目的站以外的其他站中,有的在收到 RTS 帧后就设置网络分配向量 NAV,有的则在收到 CTS 帧或数据帧后才设置 NAV,图中画出了几种不同的 NAV 的设置。

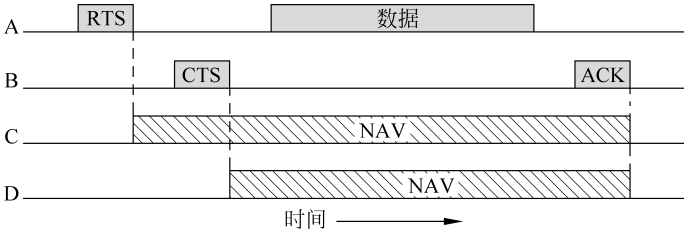


图 3-38 RTS 和 CTS 帧以及数据帧和 ACK 帧的传输时间关系

3.10 本章经典习题与解析

1. “链路”和“数据链路”有何区别?“电路接通了”与“数据链路接通了”有何区别?

解析:所谓链路(Link)就是从一个结点到相邻结点的一段物理线路,而中间没有其他任何的交换结点。在进行数据通信时,两个计算机之间的通信路径往往要经过许多段这样的链路。可见,链路只是一条路径的组成部分。

数据链路(Data Link)则是另一个概念。当要在一条线路上传送数据时,除了必须有一条物理线路外,还必须有一些通信协议来控制这些数据的传输。若把实现这些协议的硬件和软件加到链路上,就构成了数据链路。有时也把链路分为物理链路和逻辑链路。物理链路就是指上面所谓的链路,逻辑链路就是指上面所谓的数据链路。

“电路接通了”表示链路两端的结点交换机已经开机,物理连接已经能够传送比特流了,但是,数据传输并不可靠,在物理连接基础上,再建立数据链路连接,才是“数据链路接通了”。此后,由于数据链路连接具有检测、确认和重传功能,才使不太可靠的物理链路变成可靠的数据链路,进行可靠的数据传输。当数据链路断开连接时,物理电路连接不一定跟着断开连接。

2. 数据链路层使用 PPP 协议或 CSMA/CD 协议时,既然不保证可靠传输,那么为什么对所传输的帧进行差错检验呢?

解析:当数据链路层使用 PPP 协议或 CSMA/CD 协议时,在数据链路层的接收端对所

传输的帧进行差错检验是为了不将已经发现了有差错的帧(不管是什么原因造成的)收下来。如果在接收端不进行差错检测,那么接收端上交给主机的帧就可能包括在传输中出了差错的帧,而这样的帧对接收端主机是没有用处的。换言之,接收端进行差错检测的目的是:“上交主机的帧都是没有传输差错的,有差错的都已经丢弃了”。或者更加严格地说,应当是:“我们以很接近于 1 的概率认为,凡是上交主机的帧都是没有传输差错的”。

3. 为什么 PPP 协议不使用帧的编号和确认机制来实现可靠传输?

解析:PPP 不使用序号和确认机制是出于以下考虑:

若使用能够实现可靠传输的数据链路层协议(如 HDLC),开销就要增大。当数据链路层出现差错的概率不大时,使用比较简单的 PPP 较为合理。

在互联网环境下,PPP 的信息字段放入的数据是 IP 数据报。假定我们采用了能实现可靠传输但十分复杂的数据链路层协议,当数据帧在路由器中从数据链路层上升到网络层后,仍有可能因网络拥塞而被丢弃。因此,数据链路层的可靠传输并不能保证网络层的传输也是可靠的。

PPP 在帧格式中有帧校验序列 FCS 字段。对于每一个收到的帧,PPP 都要使用硬件进行 CRC 检验。若发现有差错,则丢弃该帧(一定不能把有差错的帧交给上一层)。端到端的差错控制最后由高层协议负责。因此,PPP 可以保证无差错接收。

4. IEEE 802 局域网参考模型与 OSI 参考模型有何异同之处?

解析:局域网的体系结构只有 OSI 的下两层(物理层和数据链路层),而没有第三层以上的层次。即使是下两层,由于局域网是共享广播信道,而且产品的种类繁多,涉及多种媒体访问方法,所以两者存在明显的差别。

在局域网中,与 OSI 参考模型的物理层相同的是:该层负责物理连接和在媒体上传输比特流,主要任务是描述传输媒体接口的一些特性。在局域网中,数据链路层的主要作用与 OSI 参考模型的数据链路层相同:都是通过一些数据链路层协议,在不可靠的传输信道上实现可靠的数据传输;负责帧的传送与控制,但在局域网中,由于各站共享网络公共信道,因此数据链路层必须具有媒体访问控制功能(如何分配信道,如何避免或解决信道争用)。又由于局域网采用的拓扑结构与传输媒体多种多样,相应的媒体访问控制方法也有多种,因此在数据链路功能中应该将与传输媒体有关的部分和无关的部分分开。这样,IEEE 802 局域网参考模型中的数据链路层划分为两个子层:媒体访问控制 MAC 子层和逻辑链路控制 LLC 子层。

与 OSI 参考模型不同的是:在 IEEE 802 局域网参考模型中没有网络层。局域网中,在任意两个结点之间只有唯一的一条链路,不需要进行路由选择和流量控制,所以在局域网中不单独设置网络层。

从上面的分析可知,局域网的参考模型只相当于 OSI 参考模型的最低两层,且两者的物理层和数据链路层之间也有很大差别,在 IEEE 802 系列标准中各个子标准的物理层和媒体访问控制 MAC 子层是有区别的,而逻辑链路控制 LLC 子层是相同的,也就是说,LLC 子层实际上是高层协议与任何一种 MAC 子层之间的标准接口。

5. 在 IEEE 802.3 标准以太网中,为什么说如果有冲突则一定发生在冲突窗口内,或者说一个帧如果在冲突窗口内没发生冲突,则该帧就不会再发生冲突?

解析:结点要发送数据时,先侦听信道是否有载波,如果有,表示信道忙,则继续侦听,

直至检测到空闲为止；当一个数据帧从结点 A 向最远的结点传输过程中，如果有其他结点也正在发送数据，此时就发生冲突，冲突后的信号需要经过冲突窗口时间后传回结点 A，结点 A 就会检测到冲突，所以说如果有冲突则一定发生在冲突窗口内，如果在冲突窗口内没有发生冲突，之后如果其他结点再发送数据，就会侦听到信道忙，而不会发送数据，从而不会再发生冲突。

6. 一个以太网速率从 10Mbps 升级到 100Mbps，满足 CSMA/CD 冲突条件，为使其正常工作，需做哪些调整？为什么？

解析：由于 10Base-T 证明比 10Base-2 和 10Base-5 具有更明显的优越性，因此所有的快速以太网系统都使用集线器(Hub)，而不使用同轴电缆，100Base-T MAC 与 10Mbps 的经典以太网 MAC 几乎一样，唯一不同的参数就是帧际间隙时间，10Mbps 以太网是 9.6μs(小值)，快速以太网(100Mbps)是 0.96μs(最小值)。另外，为了维持最小分组尺寸不变，需要减小最大冲突域直径。所有这些调整的主要原因是速率提高到了原来以太网的 10 倍。

7. 假定连接在透明网桥上的一台计算机把一个数据帧发给网络上不存在的一个设备，网桥将如何处理这个帧？

解析：网桥不知道网络上是否存在该设备，它只知道在其转发表中没有这个设备的 MAC 地址。因此，当网桥收到这个目的地址未知的帧时，它将扩散该帧，即把该帧发送到所连接的除输入网段以外的所有其他网段。

8. 与传统共享式局域网相比，使用局域网交换机的交换式局域网为什么能改善网络的性能和服务质量？

解析：传统共享式局域网的核心设备是集线器，而交换式局域网的核心是以太网交换机。在使用共享式集线器的传统局域网中，在任何一个时刻只能有一个结点能够通过共享通信信道发送数据；在使用交换机的交换式局域网中，交换机可以在它的多个端口之间建立多个并发连接，从而实现了结点之间数据的并发传输，有效地改善了网络性能和服务质量。

9. 试分析中继器、集线器、网桥和交换机这四种网络互联设备的区别和联系。

解析：这四种设备都是用于互联、扩展局域网的连接设备，但它们工作的层次和实现的功能不同。

中继器工作在物理层，用来连接两个速率相同且数据链路层协议也相同的网段，其功能是消除数字信号在基带传输中由于经过一长段电缆而造成的失真和衰减，使信号的波形和强度达到所需的要求。其原理是信号再生。

集线器也工作在物理层，相当于一个多接口的中继器，可以将多个结点连接成一个共享式的局域网，但任何时刻都只能有一个结点通过公共信道发送数据。

网桥工作在数据链路层，可以互连不同的物理层、不同的 MAC 子层以及不同速率的以太网。网桥具有过滤帧以及存储转发帧的功能，可以隔离冲突域，但不能隔离广播域。

交换机工作在数据链路层，相当于一个多端口的网桥，是交换式局域网的核心设备。它允许端口之间建立多个并发的连接，实现多个结点之间的并发传输。因此，交换机的每个端口结点所占用的带宽不会因为端口结点数目的增加而减少，且整个交换机的总带宽会随着端口结点的增加而增加。交换机一般工作在全双工方式，有的局域网交换机采用存储转发方式进行转发，也有的交换机采用直通交换方式(即在收到帧的同时立即按帧的目的 MAC

地址决定该帧的转发端口，而不必进行先缓存再进行处理）。另外，利用交换机可以实现虚拟局域网（VLAN），VLAN 不仅可以隔离冲突域，也可以隔离广播域。

10. 使用网桥分隔网络所带来的好处是什么？

解析：本题主要考查局域网使用网桥的概念。

早期的局域网使用集线器将计算机连接在一起。然而，随着所连接的结点数的增加，采用集线器连接的这种共享使局域网的负载增加，网络性能下降。这是因为所有连接到集线上的结点都共享同一个“冲突域”。另外，在这种结构的局域网中，一个结点发送的每一帧都能够被所有结点接收到，即所有结点共享同一个“广播域”。

为了结束“冲突域”问题，提高共享介质的利用率，人们利用网桥和交换机来分隔所互连的各网段中的通信量，建立多个分离的“冲突域”。但是，当网桥和交换机接收到一个未知转发信息的数据帧时，为了保证该数据帧能够被目的结点正确接收到，将该帧向所有的端口广播出去。这种方法虽然简单，但可能使网络中无用的通信量剧增，造成所谓的“广播风暴”。从上述的描述中可以看出，网桥和交换机的“冲突域”个数等于端口的个数，广播域都为 1。

为了解决“广播域”问题，人们引入了路由器，为互连网络之间的信息量提供路由。路由建立了分离的广播域，可以根据所接收的分组头部的地址决定是否转发分组。因此，路由器的“冲突域”和“广播域”的个数都等于端口的个数。网桥作为一种工作在数据链路层的互连设备，通过接收数据帧、地址过滤、存储与转发数据帧的方式，来实现多个局域网的互连。网桥可以根据数据帧中的源地址、目的地址以及网桥中存储的“端口—结点地址表”来决定是否转发帧。如果源地址与目的地址处于同一个网段，网桥不转发该数据帧；如果源地址与目的地址不属于同一个网段，网桥将根据“端口—结点地址表”把该数据帧转发到相应的端口；如果“端口—结点地址表”中没有相应的结点地址信息，网桥将该数据帧向所有的端口广播出去。

11. 如果一个“局域网有 11 台主机与 1 台服务器，使用一个 12 端口的集线器连接了主机与服务器，同时可以有多少条并发的连接？

解析：本题主要考查局域网中集线器的概念。

在使用共享式集线器的传统局域网中，当连接到集线器上的一个结点发送数据时，集线器将用广播方式将数据传送到集线器的每个端口。因此共享式以太网在每个时间片只能有一个结点占用公用通信信道发送数据，即任何一个时刻网络中只能有一条并发的连接。题中的 1 台服务器和 11 台主机共 12 台设备在任何一个时刻只能有一台设备通过总线发送数据。

12. 如果一个网络采用一个具有 24 个 10Mbps 端口的交换机作为连接设备，每个连接结点平均获得的带宽为多少？

解析：本题主要考查局域网中使用交换机时带宽的概念。

在采用交换机作为连接设备的交换式局域网中，交换机允许在端口之间建立多个并发的连接，即连接于一个端口的结点可以独占该端口的带宽。另外，交换机的端口可以设计成支持两种工作模式，即半双工与全双工。对于 100Mbps 的端口，半双工端口带宽为 10Mbps，而全双工端口的带宽为 20Mbps。

13. CSMA/CD 使用什么方法来解决多结点共享公用总线传输介质的问题？

解析：本题主要考查局域网中最主要的技术 CSMA/CD 的概念。

在采用 CSMA/CD 介质访问控制方法的局域网中,每个结点发送数据之前必须侦听信道的状态。如果信道空闲,立即发送数据,同时进行冲突检测;如果信道忙,站点继续侦听总线,直到信道变为空闲。如果在数据发送过程中检测到冲突,将立即停止发送数据并等待一段随机长的时间,然后重复上述过程。因此,不需要集中结点进行控制,而是让每个结点去争用总线以获得数据的发送权。

14. 虚拟局域网中逻辑工作组结点的组成不受地理位置的限制,逻辑工作组的划分与管理是通过什么方式实现的?

解析:本题主要考查构成虚拟局域网的主要技术的概念。

虚拟局域网 VLAN 是在交换式局域网的基础上形成的一种局域网,其技术基础是交换技术。VLAN 在功能、操作上与传统的局域网基本相同,其主要区别在于组网方法不同。在虚拟局域网中,处于不同物理网段的一组结点可以形成一个逻辑上的局域网。这样,虚拟局域网就不受网络用户的地理位置限制,而是根据用户需求进行网络的分段。根据虚拟局域网对成员的定义方法的不同,可以将虚拟局域网的组网方法分为 4 类:基于交换机端口号的 VLAN、基于 MAC 地址的 VLAN、基于网络层地址的 VLAN 以及 IP 多播组的 VLAN。虚拟局域网基于交换技术,因此其核心设备是局域网交换机,而不是共享式局域网的设备——集线器。

3.11 Wireshark 实验:数据链路层帧分析

基于 Wireshark 捕获的数据链路层以太网帧如图 3-39 所示。关于 Wireshark 软件的安装及使用说明见本书附录部分。

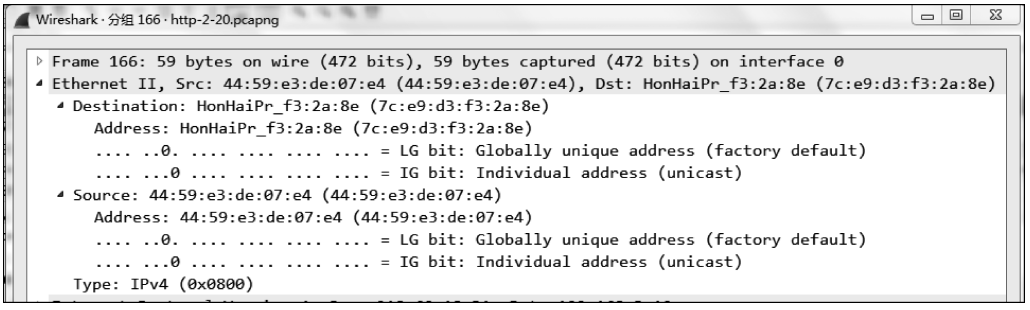


图 3-39 数据链路层的帧

以太网帧主要字段分析:

```
Ethernet II, Src: 44:59:e3:de:07:e4 (44:59:e3:de:07:e4), Dst: HonHaiPr_f3:2a:8e (7c:e9:d3:
f3:2a:8e)                              #以太网 源 MAC 地址   目的 MAC 地址
Destination: HonHaiPr_f3:2a:8e (7c:e9:d3:f3:2a:8e)                          #目的 MAC 地址
    Address: HonHaiPr_f3:2a:8e (7c:e9:d3:f3:2a:8e)                          #目的 MAC 地址
    ......0..... = LG bit: Globally unique address (factory default)  #全球唯一地址
    .......0 ..... = IG bit: Individual address (unicast)              #转播方式(0 位
                                                                          单播)
Source: 44:59:e3:de:07:e4 (44:59:e3:de:07:e4)                               #源 MAC 地址
    Address: 44:59:e3:de:07:e4 (44:59:e3:de:07:e4)                          #源 MAC 地址
    ......0..... = LG bit: Globally unique address (factory default)  #全球唯一地址
```

```
.......0 ..... = IG bit: Individual address (unicast)        #转播方式(0 位
                                                              单播)
Type: IPv4 (0x0800) # 0x0800 表示所携带上一层数据类型为 IPv4
```

习题 3

3-1 数据链路层提供的基本服务可以分为哪几类？试比较它们的区别。

3-2 物理线路与数据链路的区别是什么？

3-3 数据链路协议使用了下面的字符编码：

A：0100 0111 B：1110 0011 FLAG：0111 1110 ESC：1110 0000

为了传输一个包含 4 个字符的帧：A B ESC FLAG，试问使用下面的成帧方法时所发送的比特序列(用二进制表达)是什么？

(1) 字节填充的标志字节。(2)比特填充的首尾标志字节。

3-4 计算 CRC 校验码：要发送的数据为 101001，采用的生成多项式 $G(x)=X^3+X^2+1$，求应添加在数据后面的余数。

3-5 某个数据通信系统采用 CRC 校验方式，并且生成多项式 $G(x)$ 为 X^4+X^3+1，目的结点接收到的二进制比特序列为 110111001(含 CRC 校验码)。试判断传输过程中是否出现了差错？为什么？

3-6 简述 PPP 协议的组成及其功能。

3-7 说明局域网采用广播通信方式的特点。

3-8 什么是传统以太网？以太网有哪两个主要标准？

3-9 说明 10Base-5、10Base-2、10BASE-T 所代表的含义。

3-10 什么是 CSMA/CD，它是如何工作的？

3-11 简述网卡的主要功能。

3-12 简述 IEEE 802.3 标准规定的无效 MAC 帧。

3-13 考虑建立一个 CSMA/CD 网，电缆长 lkm，不使用重发器，运行速率为 lGbps，电缆中的信号速度是 200 000km/s，求最小帧长度是多少？

3-14 若构造一个 CSMA/CD 总线网，速率为 100Mbps，信号在电缆中的传播速度为 200 000km/s，数据帧的最小长度为 125 字节。试求总线电缆的最大长度(假设总线电缆中无中继器)。

3-15 什么是广播域？什么是冲突域？集线器、网桥、交换机如何划分广播域、冲突域？

3-16 高速以太网的特点有哪些？

3-17 什么是 VLAN？简述 VLAN 的原理。

3-18 以太网交换机如何划分 VLAN？

3-19 什么是 Wi-Fi？简述无线局域网的基本结构模型。

3-20 什么是隐蔽站和暴露站？

3-21 简述 CSMA/CA 的工作原理。