第3章
数据链路层

张瑞
ruizhang@shu.edu.cn

第3章 数据链路层

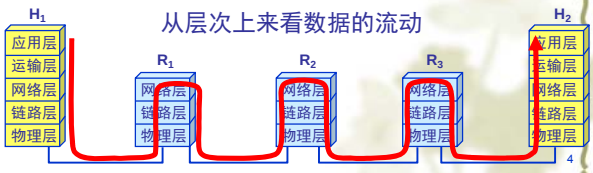
3.1 数据链路层的基本概念

- 链路(link)
  - 一条无源的点到点的物理线路段，中间没有任何其他的交换结点
- 数据链路(data link)
  - 除了物理线路外，还必须有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

数据链路层的简化模型

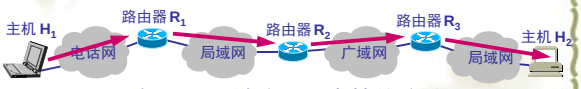
主机 H_1 向 H_2 发送数据

从层次上来看数据的流动

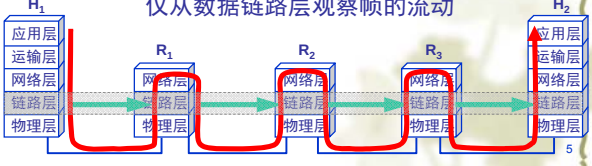


数据链路层的简化模型（续）

主机 H_1 向 H_2 发送数据



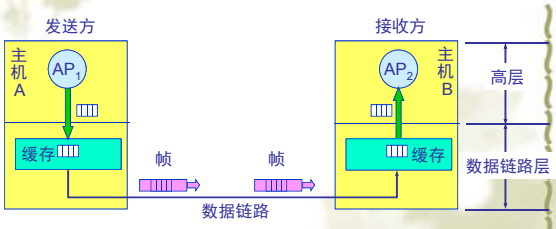
仅从数据链路层观察帧的流动



数据链路层的简化模型

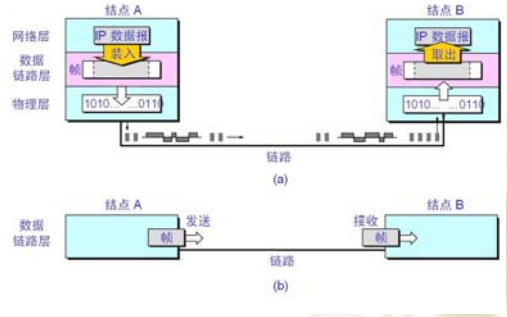
- 两个主机通信时，应用进程将数据从应用层往下传，经过物理层到达传输线路，到达接收端后，通信线路将数据传到物理层，最后由应用层交给应用进程。
- 为了分析链路层协议，采用简化的链路层模型
  - 数据链路层以上的各层用一个主机代替；
  - 物理层和通信线路等效成一条简单数据链路；

数据链路层的简化模型



7

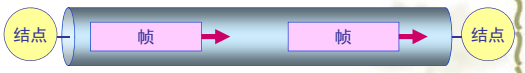
数据链路层传送的是帧



8

数据链路层像个数字管道

- 讨论链路层时，常常在两个对等的数据链路层之间画出一个数字管道，而在这条数字管道上传输的数据单位是帧。



- 物理层间传输的是比特流，物理媒体上传送的是电或光信号，而在链路层上传输的数据帧。

9

数据链路层的主要功能

- 基本功能
  - 向网络层提供可靠的、透明的数据传输服务，将源节点的网络层数据可靠地传送到相邻节点的网络层
- 主要功能描述
  - 链路管理

数据链路层，数据的传送以	每一帧都能送到正确的目的地；
纠错，通过编码技术，接收	收方也能知道发送方的地址
数据和控制信息在同一个帧	

含，设与

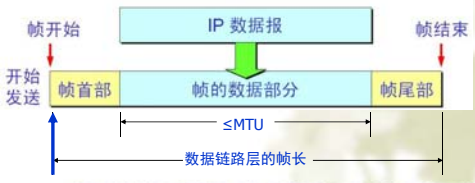
第3章 数据链路层

- 3.1 数据链路层的基本概念
- 3.2 组帧
- 3.3 差错控制
- 3.4 点对点协议PPP
- 3.5 使用广播信道的数据链路层
- 3.6 以太网的MAC层
- 3.7 扩展的以太网
- 3.8 虚拟局域网

11

3.2 组帧

- 组帧(framing)就是在一段数据的前后分别添加首部和尾部，这样就构成了一个帧。
- 目的：使接收方能准确识别帧的边界
- 首部和尾部的一个重要作用就是进行帧定界



12

帧定界（帧同步）的方法

- 1、字节计数法
- 2、使用字符填充的首尾定界法
- 3、使用比特填充的首尾定界法*
- 4、违法编码法

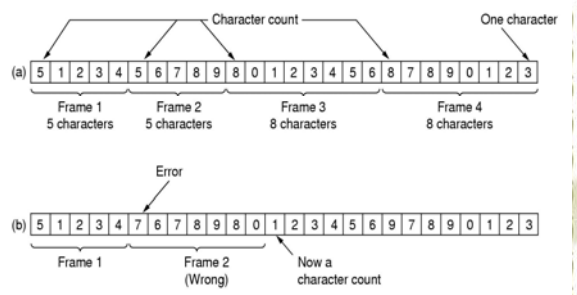
13

1、字节计数法

- 思想
  - 在帧头设置一个长度域，放置该帧的字节数，当收方收到帧后，通过帧的长度，确定帧的开始。
- 问题
  - 当帧的长度域出错，帧同步完全丢失；
  - 该方法很少单独使用。

14

字节计数法举例



15

2、字符填充法

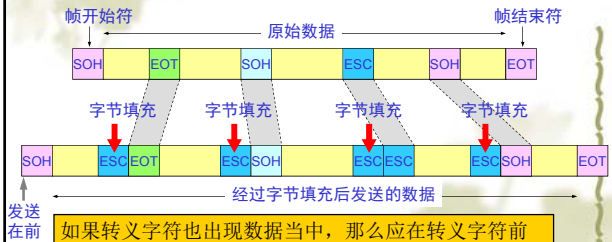
- 思想
  - 使用特殊的ASCII字符（不可打印的控制字符）作为帧的起始和终止定界符。
  - 例如：使用SOH作为开始符，EOT作为结束符。
- 问题：数据传输不透明
  - 当数据中出现定界符(SOH或EOT)时，如何加以区分是数据还是定界符？
  - 解决：字符填充

发送端的数据链路层在数据中出现控制字符“SOH”或“EOT”的前面插入一个转义字符“ESC”(其十六进制编码是 1B)。接收端的数据链路层在将数据送往网络层之前删除插入的转义字符。

误认为是一个帧

16

字符填充法举例



如果转义字符也出现数据当中，那么应在转义字符前面插入一个转义字符。当接收端收到连续的两个转义字符时，就删除其中前面的一个。

17

3、比特填充法

- 思想
  - 使用一个特殊的比特模式01111110作为帧的起始和结束标志。
  - 发送方边发送边检查数据，每连续发送5个“1”后在后面自动插入一个“0”。这样数据中只会连续出现5个“1”，而不会出现定界符。
  - 接收方在收到5个连续的“1”后将后面的“0”删掉而恢复出原始数据。
- 好处
  - 数据传输的基本单位是比特而不是字符，可用来传输任意长度的二进制比特串，通用性强。

18

零比特的填充与删除

数据中某一段比特组合恰好出现和 定界符一样的情况

0 1 0 0 1 1 1 1 1 1 0 0 0 1 0 1 0

会被误认为是定界符

发送端在 5 个连 1 之后填入 0 比特再发送出去

0 1 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0

填入 0 比特

在接收端将 5 个连 1 之后的 0 比特删除，恢复原样

0 1 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0

在此位置删除填入的 0 比特

19

比特填充法举例

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0

Stuffed bits

(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

20

4、违法编码法

- 前提
  - 物理介质上使用的信号编码有冗余码字时，使用这些冗余的码字来作为帧的定界。
- 举例
  - 如曼彻斯特编码或差分曼彻斯特编码中，有效电平是“低－高”或“高－低”，而“低－低”和“高－高”电平没有定义，这种违法编码可以作为帧的边界。

21

第3章 数据链路层

- 3.1 数据链路层的基本概念
- 3.2 组帧
- 3.3 差错控制
- 3.4 点对点协议PPP
- 3.5 使用广播信道的数据链路层
- 3.6 以太网的MAC层
- 3.7 扩展的以太网
- 3.8 虚拟局域网

22

3.3 差错控制

- 差错控制技术：由接收方来检查并纠正错误，传输错误如何处理？
  - 前向纠错
  - 自动重发请求（不能纠正，接收方反馈。若有错误则重发，否则给肯定应答）
  - 在发送端引入计时器，进行超时重发
    为了避免相同的帧收到多次，需要对帧进行编号
- 差错编码技术：如何发现差错？
  - 检错码（奇偶校验码、CRC）
  - 纠错码（海明码）

23

3.3.1 差错控制技术

- 前向纠错（FEC，Forward Error Correct）
  - 即发送方发送能使接收方检错并纠错的冗余位，纠错任务由接收方完成；常采用海明码。
  - 主要应用于没有反向信道或反向传输时间很长的场合
- 缺点：为纠错附加的冗余码较多，传输效率低
- 优点：实时性好。

24

差错控制技术（2）

- 自动重发请求（ARQ – Automatic Repeat reQuest）
  - 即发送方发送能使接收方检错的冗余位，若无差错，则接收方回送一个肯定应答(ACK)；若有差错，则接收方回送一个否定应答(NAK)，要求发送方重发。
- 缺点：信息传递连贯性差
- 优点：接收端设备简单，只要请求重发，无需纠正错误。

25

3.3.2 差错编码技术

- 差错编码
  - 差错编码：数据块中插入冗余信息的过程。
  - 思想：判断一个数据块中是否存在传输错误，发送端必须在数据块中插入一些冗余信息，使得数据块中的各个比特建立某种形式的关联，接收端通过验证这种关联关系来判断是否有传输错误。
- 差错编码策略
  - 检错码：能检测出错误，但不能纠正错误，如CRC
  - 纠错码：能知道错误，且知道错误的位置，如海明码

26

3.3.2.1检错码

- 检错码的构造
  - 检错码(码字、传输帧)＝信息位＋冗余校验位
  - 码字长n=K(信息位位数)＋r(校验位位数)
  - 编码效率R＝有效数据位K / 码字长n
- 信息字段和校验字段之间的对应关系
  - 校验字段越长，编码的检错能力越强，编码/解码越复杂；附加的冗余信息在整个编码中所占的比例越大，传输的有效成分越低，传输的效率下降。
  - 检错码一旦形成，整个检错码将作为一个整体被发往线路，通常的发送顺序是信息字段在前，校验字段在后。

27

奇偶校验码

包括信息位和校验位

- 奇校验：使码字中“1”的总个数为奇数。
- 偶校验：使码字中“1”的总个数为偶数。
- 奇/偶校验码：最常用的一种检错码，包括
  - 水平奇/偶校验码
  - 垂直奇/偶校验码
  - 水平垂直奇/偶校验码

需要对信息按行、列分组然后

方阵校验（在水平校验的基础上，增加垂直校验）

28

水平奇/偶校验

- 其信息字段以字符为单位，校验字段仅含一个比特称为校验比特或校验位。
- 例如：使用七单位的ASCII码来构造成八单位的检错码时若采用奇/偶校验，校验位的取值应使整个码字包括校验位，1的比特个数为奇数或偶数。

29

水平奇/偶校验

- 例：信息字段　奇校验码　偶校验码
- 0110001　01100010　01100011

信息位 3个1　校验位

0 1 1 0 0 0 1　奇 0

偶 1

- 编码效率：Q/(Q+1)（信息字段占Q个比特）
- 应用：通常在异步传输方式中采用偶校验，同步传输方式中采取奇校验。

30

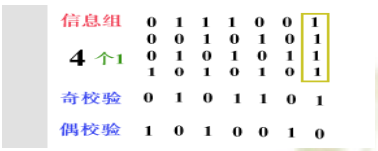
垂直奇/偶校验

- 做法：
  - 被传输的信息进行分组，并排列为若干行和若干列。组中每行的相同列进行奇/偶校验，最终产生由校验位形成的校验字符（校验行），并附加在信息分组之后传输。
- 举例：
  - 4个字符（4行）组成一信息组，求垂直奇/偶校验码

31

垂直奇/偶校验

- 例：4个字符（4行）组成一信息组，其垂直奇/偶校验码为：



  - 发往线路顺序（垂直奇校验）
    - 0111001|0010101|0101011|1010101|0101101
  - 编码效率：
    - PQ/P(Q+1) （假设信息分组占Q行P列）

32

水平垂直奇/偶校验

- 水平垂直奇/偶校验码(方阵校验)
  - 在水平校验的基础上实施垂直校验。
- 例：4行7列信息组的水平垂直偶校验码为：

33

水平垂直奇/偶校验

- **发往线路顺序(偶校验字符)：**
  01110010|00101011|01010110|10101010|10100101
- **第1字符 | 第2字符 |第3字符 | 第4字符 |垂直偶校验字符**
- **编码效率：**
  - **PQ/(P+1)(Q+1) （假设被传信息分组占Q行P列）**

34

3.3.2.2 循环冗余码

- 循环冗余码（Cyclic Redundancy Check，CRC）
  - 计算机和数据通信中使用最广泛的检错码，漏检率低，可用简单的电路实现。
- CRC编码的一般操作
  - 给定一个k比特的帧或报文，发送方生成n比特的序列（也称为帧检验序列FCS，Frame Check Sequence），形成（k+n）的码字，该码字能被某个事先确定的数整除。接收方用相同的数去除收到的帧，如果无余数，则认为数据帧无差错

35

CRC也称多项式编码

- 任意一个由二进制位串组成的代码都可以和一个系数仅为‘0’和‘1’取值的多项式一一对应。
- 多项式表示：即将k比特的数据用k项多项式表示，它的各项为$X^{k-1}...X^0$，它的系数为数据中对应位的0或1。
- 例如：
  - 代码1010111对应的多项式为$x^6+x^4+x^2+x+1$
  - 多项式为$x^5+x^3+x^2+x+1$对应的代码101111

36

冗余码的计算

- 假设待传送的数据 M = 1010001101（共k bit）。我们在M的后面再添加供差错检测用的 n bit 冗余码一起发送。
- 计算方法
  - 用二进制的模 2 运算进行 2^n 乘 M 的运算，这相当于在 M 后面添加 n 个 0。
  - 得到的 (k + n) bit 的数除以事先选定好的长度为 (n + 1) bit 的数 P，得出商是 Q 而余数是 R，余数 R 比除数 P 少1 个比特。
  - 核心问题：P如何选定？P若选定，则n就确定了。

生成多项式

37

二进制模2运算

- 模2运算
  - 用模2运算进行加法时不进位。
  - 减法和加法一样，按加法规则进行运算。
- 举例
  - 1111＋1010＝？
  - 答案为0101

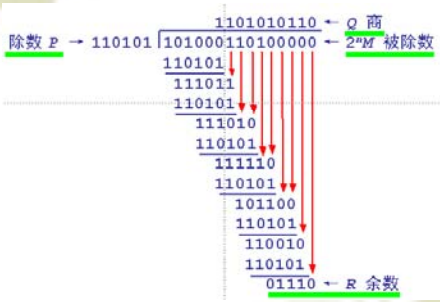
38

冗余码计算举例

- 设 M = 1010001101，P = 110101，n = 5，模 2 运算的结果2^nM除以P得出：
  - 商 Q = 1101010110
  - 余数R = 01110
- 将余数 R 作为冗余码添加在数据 M 的后面发送出去，即发送的数据是101000110101110，或 2^nM + R。

39

循环冗余检验的原理说明



40

生成多项式P

- 发送方和接收方有一事先约定的生成多项式P
  - 例如上例中的P＝110101，即P＝$X^5+X^4+X^2+1$（P为5阶多项式）；
  - 生成多项式的最高位和最低位都必须为1；
  - P的用途：发送方用它生成冗余位；⇨ 发送方用P生成R
  - P的用途：接收方用它判断是否有错；
  - 实现：不同的P有不同的编码电路，用简单的移位寄存器电路硬件实现；
  - 实现：发送方通过编码电路产生冗余位，接收方用相似电路检测错误；
  - 若P为r阶，将产生r位冗余位；
    - 有（r+1）位比特

41

发送方用P生成冗余位

- P(X)--------生成多项式
- M(X)--------信息多项式
- R(X)--------冗余多项式
- T(X)--------传输帧多项式
- 发送方用P(X)产生冗余位
  - 2^n•M(x)/P(x)产生冗余多项式R(x)附加到M(x)后形成T(x)变成带校验位的传输帧多项式

42

接收方用P进行校验

- T(X)/P(X)
  - ≠0(除不尽)，则有错（1）
  - =0(除尽)，则无错或漏检（2）
- 有错分析：
  - 只要得出的余数R不为0，就表示检测到了差错。即用收到的比特流(2^nM+R)除以P，看得出的余数是否为0。
  - 但这种检测方法并不能确定究竟是哪一个或哪几个比特出现了差错。
  - 一旦检测出差错，就丢弃这个出现差错的帧。

43

接收方用P进行校验（漏检）

- 漏检分析
  - 收到：T(X)+E(X)；其中E(X)为出错多项式
  - 漏检,即: [T(X)+E(X)]/P(X)=0
  - ∵T(X)/P(X)=0（T(X)为正确的部分）
  - ∴E(X)/P(X)=0
  - 即若P(X)是E(X)的因子,将可能漏检.
  - 选取合适的P(x),使P(x)不成为E(X)的因子,则可避免漏检.

44

CRC漏检

- CRC不能保证检测出所有的传输错误，但是只要选择位数足够的P，可以使得差错的概率足够小。
- 例如：CRC-16和CRC-CCITT可以检测出所有1、2、奇数个、突发长度小于等于16比特错。17比特突发错的99.997%，18比特或更长比特突发错的99.998%。

45

P的确定方法

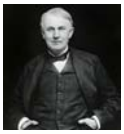
- **P为生成多项式，已有的国际标准。**
  - **CRC-12=$X^{12}+X^{11}+X^3+X^2+X+1$**
  - **CRC-16=$X^{16}+X^{15}+X^2+1$**
  - **CRC-CCITT=$X^{16}+X^{12}+X^5+1$**
    - **HDLC和X.25采用**
  - **CRC32=**
    $X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$
    - **CSMA/CD LAN采用**

46

CRC算法思路

- 已知：信息多项式M(X)，生成多项式P(X)
- 求：传送的信息序列
  - 多项式与二进制代码的对应关系
  - 求出余数
    - 根据P(X)得到n
    - 二进制除法
- 求某个比特出错时，接收方能否检验出来
  - 用接收到的序列/生成多项式，看余数是否为0

47



汉明　同事　香农　远亲　爱迪生

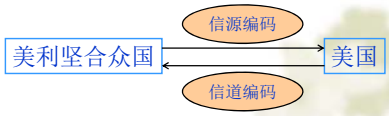
1950年提出汉明码

1968年 图灵奖

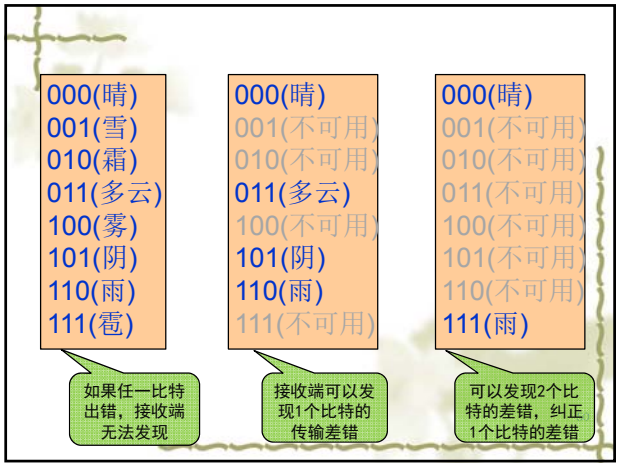
48

信源编码与信道编码

- 信源编码：无失真的压缩信息
- 信道编码：通过插入冗余信息，使得在有差错的信道中实现无差错的传输
- 汉明码属于信道编码，是纠错码



49



3.3.2.3 汉明码

- 码距（汉明距离Hamming Distance）
  - 一个编码系统中任意两个合法编码（码字）之间不同的二进位（bit）数叫这两个码字的码距。
  - 例如，10001001 与10110001它们的汉明距离为3
  - 而整个编码系统中任意两个码字的的最小距离就是该编码系统的码距。

51

两个结论

- 如果要检测出d个比特的错，则编码集的汉明距离至少为d+1。
  例如：数据后加奇偶校验位，编码后的汉明距离为2，能检测1比特错。
- 如果要纠正d个比特的错，则编码集的汉明距离至少应为2d+1。
  例如有4个有效码字：它们是000000，000111，111000，111111，汉明距离为3，能纠正1比特错

52

汉明码的基本思想

- 汉明码是R.Hamming在1959年提出的，基本思想是：
  - 在k比特信息后附加r比特冗余信息（校验比特），构成n=k+r比特的码字，其中每个校验比特和某几个特定的信息比特构成偶校验关系。
  - 接收端对这r个奇偶校验关系进行校验，即将每个校验比特和与它关联的信息比特进行相加（异或），相加的结果为校正因子。
    - 如果没有错，则r个校正因子都为0；
    - 若校正因子不全为0，根据校正因子的取值，确定错误发生的位置。

53

汉明码：主要介绍内容

- 主要介绍单比特纠错汉明码
  - 纠正单比特错误
  - 发送方冗余位产生与接收方纠错过程

54

发送方冗余位计算

- A、根据信息位长度(如每帧K位)，计算出所需冗余位位数r：
  - 若需纠正一位错，需满足：$2^r \geq K+r+1$
  - 原理：求汉明码时的一项基本考虑是确定所需最少的校验位数r。*考虑长度为K位的信息，若附加了r个校验位，则所发送的总长度为K+r。*在接收端中要进行r个奇偶检查，每个检查结果或是真或是伪。*这个奇偶检查的结果可以表示成一个r位的二进制数，它可以确定最多2^r种不同状态。*这些状态中必有一个其所有奇偶测试都是真的，它便是判定信息正确的条件。*于是剩下的（2^r-1）种状态，可以用来判定误码的位置。*则导出下一关系：
    - $2^r-1 \geq K+r$
  - 例如：如果K＝4，则r=3，则n=K+r=7

55

某公司笔试题

- 实验室里有1000个一模一样的瓶子，但是其中的一瓶有毒。可以用实验室的小白鼠来测试哪一瓶是毒药。如果小白鼠喝掉毒药的话，会在一个星期的时候死去，其他瓶子里的药水没有任何副作用。请问最少用多少只小白鼠可以在一个星期以内查出哪瓶是毒药？

  a. 9 b. 10 c. 32 d. 999 e. 以上都不对

  请给出正确答案，并解释原因。

56

汉明码计算

- B、确定校验比特和信息比特的位置
  - 理论上校验比特可在任何位置，但习惯都是将校验比特放在1、2、4、8、16…位置上。
  - 通常是将2^k位置上，放r_k (K>=0)，其余位置放I_i (K>=1)。
  - 例如7比特的汉明码的构造为：

I_4	I_3	I_2	R_2	I_1	R_1	R_0
7	6	5	4	3	2	1

57

汉明码的计算

恰好是校验位所在位置

- 将每个信息比特的位置写成2的次幂之和的形式有：
  - I_4：$7=2^2+2^1+2^0$（说明I_4参与R_2、R_1和R_0的生成）
  - I_3：$6=2^2+2^1$（说明I_3参与R_2、R_1的生成）
  - I_2：$5=2^2+2^0$（说明I_2参与R_2、和R_0的生成）
  - I_1：$3=2^1+2^0$（说明I_1参与R_1和R_0的生成）

目的：计算每一个信息位与哪些校验位有关联

I_4	I_3	I_2	R_2	I_1	R_1	R_0
7	6	5	4	3	2	1

58

汉明码计算

- 从另一个方面说：
  - R_2参与校验I_4、I_3、I_2，即R_2和I_4、I_3、I_2构成偶校验关系
  - R_1参与校验I_4、I_3、I_1，即R_1和I_4、I_3、I_1构成偶校验关系
  - 同理R_0和信息比特I_4、I_2、I_1构成偶校验
  - 这样可以写成如下比特计算公式（XOR运算）：
    - $R_2=I_4 \oplus I_3 \oplus I_2$
    - $R_1=I_4 \oplus I_3 \oplus I_1$
    - $R_0=I_4 \oplus I_2 \oplus I_1$
  - 例如：一段信息1000，按以上校验比特的生成方法，则$R_2=1$，$R_1=1$，$R_0=1$.那么发送码字为1001011

59

接收方验证

- 接收端利用相应的偶关系进行验证：
  - $S_2=R_2 \oplus I_4 \oplus I_3 \oplus I_2$
  - $S_1=R_1 \oplus I_4 \oplus I_3 \oplus I_1$
  - $S_0=R_0 \oplus I_4 \oplus I_2 \oplus I_1$
- 这里S_2、S_1、S_0为校正因子，若校正因子全0,无错；
- 校正因子不全为0，有错，错误位置为$S=S_2S_1S_0$处，将该比特取反。
- 例如：若S＝101＝5，则将位置5的比特取反，最后去掉校验比特即可得到正确的信息。

60

汉明码计算小结

- **单比特纠错汉明码**的编码方法如下：

11	10	9	8	7	6	5	4	3	2	1
D_6	D_5	D_4	R_3	D_3	D_2	D_1	R_2	D_0	R_1	R_0

1、确定校验位和信息位的位置

- 校验位R_3、R_2、R_1、R_0的计算如下：
  - $R_3=D_6\oplus D_5\oplus D_4$
  - $R_2=D_3\oplus D_2\oplus D_1$
  - $R_1=D_6\oplus D_5\oplus D_3\oplus D_2\oplus D_0$
  - $R_0=D_6\oplus D_4\oplus D_3\oplus D_1\oplus D_0$

2、确定每一个校验位与哪些信息位形成偶校验关系

- 校正因子S_3、S_2、S_1、S_0的计算如下：
  - $S_3=R_3\oplus D_6\oplus D_5\oplus D_4$
  - $S_2=R_2\oplus D_3\oplus D_2\oplus D_1$
  - $S_1=R_1\oplus D_6\oplus D_5\oplus D_3\oplus D_2\oplus D_0$
  - $S_0=R_0\oplus D_6\oplus D_4\oplus D_3\oplus D_1\oplus D_0$

3、计算校正因子

- **$S_3S_2S_1S_0$的值即指出差错的位置**

4、指出出错位置

61

第3章 数据链路层

- 3.1 数据链路层的基本概念
- 3.2 组帧
- 3.3 差错控制
- 3.4 点对点协议PPP
- 3.5 使用广播信道的数据链路层
- 3.6 以太网的MAC层
- 3.7 扩展的以太网
- 3.8 虚拟局域网

62

数据链路层使用的信道类型

- 数据链路层使用的信道主要有以下两种类型：
  - 点对点信道：这种信道使用一对一的点对点通信方式。
  - 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。广播信道上连接的主机很多，因此必须使用专用的共享信道协议来协调这些主机的数据发送。

63

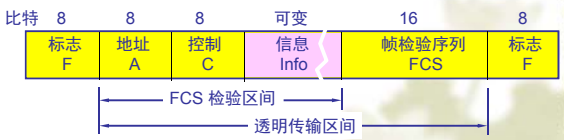
面向比特的协议HDLC

- 高级数据链路控制（High-Level Data Link Control）是由国际标准化组织制定的面向比特的有序链路层协议。
- 是为非平衡的链路级操作而研制的，采用主从结构，链路上一个主站控制多个从站，主站向从站发命令，从站向主站返回响应。
- 在通信线路质量较差的年代，能实现可靠传输的HDLC协议成为当时比较流行的数据链路层协议，但目前已经很少使用。

64

HDLC 的帧格式

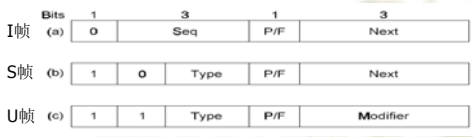
- 标志字段、地址字段、控制字段、信息字段和帧校验序列组成。



65

HDLC帧的分类

- 根据控制字段前两个比特的取值分类
  - 信息帧(I：Information)：用来实现信息的传送，含有信息字段
  - 监控帧(S：Supervision)：帧中不包含信息字段，具有监控链路的作用，并能对收到的帧进行确认。
  - 无编号帧(U：Unnumbered)：对数据链路进行附加控制。



66

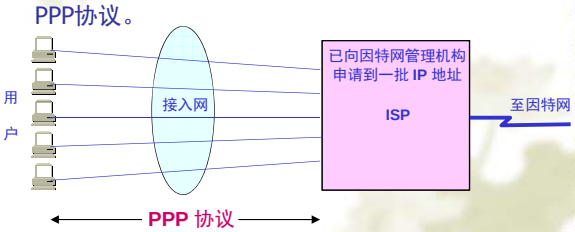
PPP协议

- 现在全世界使用得最多的数据链路层协议是点对点协议 PPP (Point-to-Point Protocol)。
- 1992年制订了 PPP 协议。经过 1993 年和 1994 年的修订，现在的 PPP 协议已成为因特网的正式标准[RFC1661]。
- PPP协议的改进
  - 处理错误检测
  - 支持多种协议
  - 连接时允许商议IP地址
  - 允许身份验证

67

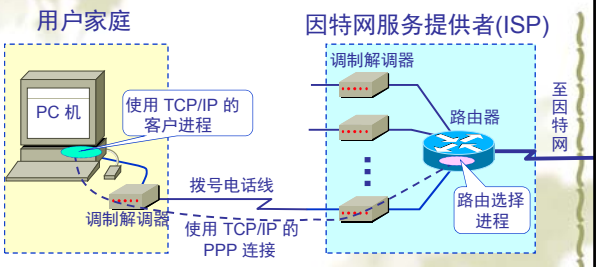
用户到ISP的链路使用PPP协议

- 用户使用拨号电话线接入因特网时，一般都是使用PPP协议。



68

用户拨号上网示意图



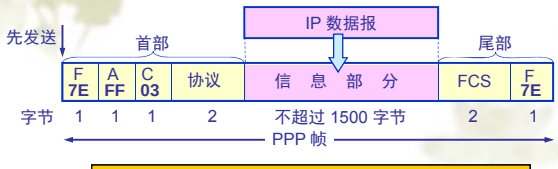
69

PPP协议的组成

- PPP协议有三个组成部分：
  - 提供一个将IP数据报封装到串行链路的方法。
  - 一个链路控制协议LCP (Link Control Protocol)：建立、配置和测试数据链路的协议。
  - 一套网络控制协议NCP (Network Control Protocol)：如为IP协议分配临时IP地址，支持多个网络层协议。

70

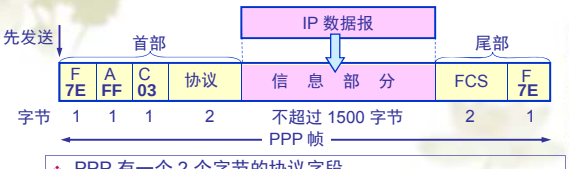
PPP协议的帧格式



PPP 是面向字节的，
所有的 PPP 帧的长度都是整数字节

71

PPP协议的帧格式



- PPP 有一个 2 个字节的协议字段。
  - 当协议字段为 0x0021 时，PPP 帧的信息字段就是IP 数据报。
  - 若为 0xC021, 则信息字段是PPP链路控制数据LCP分组
  - 若为 0x8021，则表示这是网络控制数据NCP分组
- 帧校验字段：采用循环冗余码CRC校验。

72

透明传输问题

- 异步传输：字符填充法
  - 将信息字段中出现的每一个 0x7E 字节转变成为 2 字节序列(0x7D, 0x5E)。
  - 若信息字段中出现一个 0x7D 的字节, 则将其转变成为 2 字节序列(0x7D, 0x5D)。
  - 若信息字段中出现 ASCII 码的控制字符（即数值小于 0x20 的字符），则在该字符前面要加入一个 0x7D 字节, 同时将该字符的编码加以改变。
- 同步传输：比特填充法
  - 在5个连续 1 的后面插入0

73

不提供使用序号和确认的可靠传输

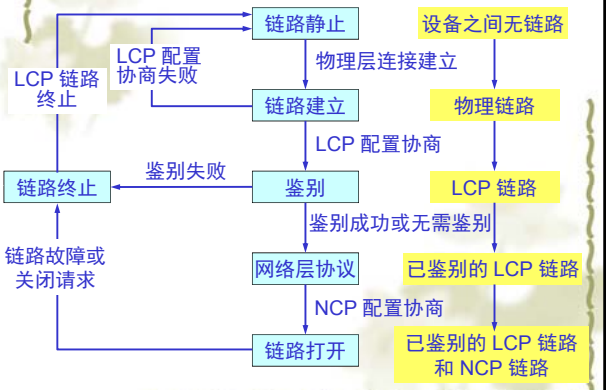
- PPP 协议之所以不使用序号和确认机制是出于以下的考虑：
  - 在数据链路层出现差错的概率不大时，使用比较简单的 PPP 协议较为合理。
  - 在因特网环境下，PPP 的信息字段放入的数据是 IP 数据报。数据链路层的可靠传输并不能够保证网络层的传输也是可靠的。
  - 帧检验序列 FCS 字段可保证无差错接受。

74

PPP协议的工作状态

- 当用户拨号接入 ISP 时，路由器的调制解调器对拨号做出确认，并建立一条物理连接。
- PC 机向路由器发送一系列的 LCP 分组（封装成多个 PPP 帧）。
- 这些分组及其响应选择一些 PPP 参数，和进行网络层配置，NCP 给新接入的 PC机分配一个临时的 IP 地址，使 PC 机成为因特网上的一个主机。
- 通信完毕时，NCP 释放网络层连接，收回原来分配出去的 IP 地址。接着，LCP 释放数据链路层连接。最后释放的是物理层的连接。

75



PPP协议的特点

- PPP帧中增加了校验字段，PPP在链路层具有差错检测功能；
- PPP的LCP协议提供通信双方进行参数协商的手段；
  - 协商参数有：数据帧的最大载荷、身份认证、NCP协议、数据压缩方式等。
- PPP帧中增加了协议字段，使得PPP可以支持多种网络层协议，有IP、IPX、OSI、CLNP等。
- 支持IP的NCP可以在建立连接时动态分配IP地址，解决了家庭用户拨号上网的问题。

77

第3章 数据链路层

- 3.1 数据链路层的基本概念
- 3.2 组帧
- 3.3 差错控制
- 3.4 点对点协议PPP
- 3.5 使用广播信道的数据链路层
- 3.6 以太网的MAC层
- 3.7 扩展的以太网
- 3.8 虚拟局域网

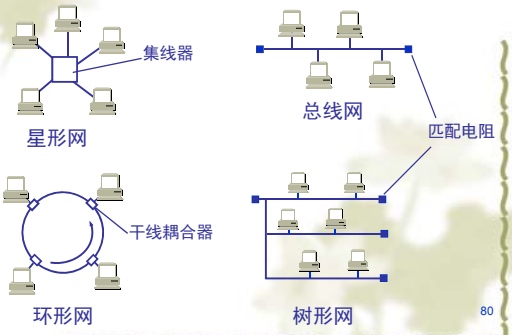
78

局域网的数据链路层

- 局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限
- 局域网具有如下的一些主要优点：
  - 具有广播功能，从一个站点可很方便地访问全网。局域网上的主机可共享连接在局域网上的各种硬件和软件资源。
  - 便于系统的扩展和逐渐地演变，各设备的位置可灵活调整和改变。
  - 提高了系统的可靠性、可用性和生存性。

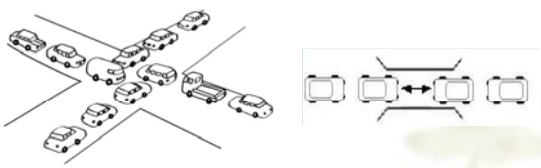
79

局域网的拓扑



80

冲突的产生



单一车道上同时有两个方向的车行驶时，如果要让两个方向的车通过，就必须是不同时刻经过。

81

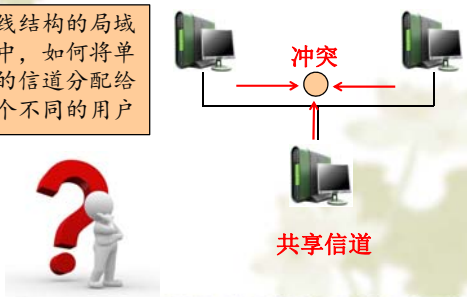
局域网信道分配策略

- 广播网中所有站点共享同一个信道，任一站点发送的信息能被所有其他站点接收到。
- 问题
  - 若有两个或两个以上的站点同时发送数据，则信号在信道中发生碰撞，数据发送失败，为冲突。
- 解决
  - 广播网中，如何将单一的信道分配各各个不同的用户，是个重要的问题。
- 用户使用的信道称为媒体，决定由谁来使用信道的协议为“媒体访问控制协议”。
- 绝大多数的局域网使用广播信道。因此，解决局域网中如何使众多用户能够合理而方便地共享通信媒体是个重要问题。

82

总线型局域网的特性

总线结构的局域网中，如何将单一的信道分配给各个不同的用户



83

信道分配策略—静态划分信道

- 静态划分信道
  - 频分复用、时分复用、波分复用和码分复用
  - 将频带或时间片固定分配给各个站点，各个站点有自己的频带或时间片，不会产生冲突
- 静态分配的特点
  - 站点数目少且固定，且每个站点有大量数据发送，控制协议简单且传输的效率高。
  - 对于大部分计算机网络，站点数目多且不固定，数据传输有突发性，信道的利用率低。
  - 代价较高，不适合于局域网使用

84

信道分配策略—动态分配

- 动态媒体接入控制（多点接入）
  - 信道不是在用户通信时固定分配给用户。
  - 如异步时分多路复用STDM，各站点仅当有数据发送时，才占用信道发送数据。
- 动态接入控制类型
  - 随机接入
  - 控制接入

85

随机接入和受控接入

- 随机接入
  - 又称为争用，各站点发送前不需要取得发送权，有数据就发送，发生冲突后采取措施解决冲突
  - 适合负载较轻的网络，信道的利用率一般不高，但网络延迟较短
  - 例如：以太网和卫星通信
- 受控接入
  - 都是使发送站点首先获得发送权，再发送数据，不会产生冲突
  - 当网络负载较重时，可以获得较高的信道利用率
  - 主要有轮询(round-robin)和预约(reservation)两种方式
  - 例如：光纤分布式数据接口FDDI网络

86

代表性的媒体访问控制方法

- 争用协议
  - ALOHA协议
  - CSMA/CD协议
- 无冲突协议（略）
  - 比特映像媒体访问控制协议（先预约然后传输）
  - 小时间片轮换优先权媒体访问控制协议
  - 二进制地址相加协议
- 有限争用协议（略）
  - 思想：网络轻负载时使用竞争策略，重负载时使用无冲突策略
  - 自适应步进树协议

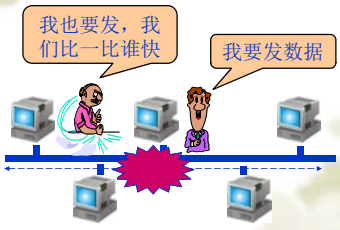
87

争用协议

- 争用协议的特性
  - 随机访问：意味着对任何站都无法预计其发送的时刻；
  - 竞争发送：是指所有发送的站自由竞争信道的使用权。
  - ALOHA系统和它的后继者CSMA/CD都是争用协议的代表。

88

争用协议



89

争用协议的发展

- 想发就发，冲突重发 ⇨ ALOHA
- ALOHA+划分时隙 ⇨ 时隙ALOHA
- ALOHA+载波检测 ⇨ CSMA
  - 载波检测：发送前，先监听信道，信道空才发
- CSMA+冲突检测 ⇨ CSMA/CD
  - 冲突检测：发送时，边发边测

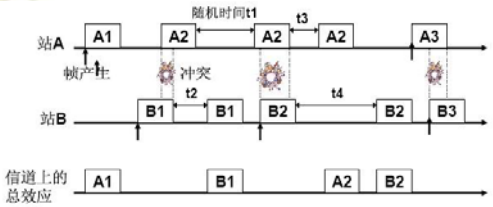
90

ALOHA系统

- 争用协议最早起源于20世纪70年代夏威夷大学的ALOHA系统，该网络通过无线信道将各个分校的终端连接到本部的主机上。
- 基本思想是如何实现多个用户竞争使用单一信道的系统
- ALOHA系统的思想
  - 任何用户有数据发送就可以发送（会带来冲突）；
  - 每个用户通过监听信道来获知数据传输是否成功；
  - 发现数据传输失败后，各自等待一段随机时间，再重新发送。

91

ALOHA系统的工作原理



92

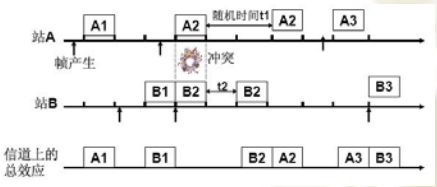
ALOHA系统信道分析

- 竞争系统中，一方面不断有新的数据帧发送，另一方面冲突帧需要重发，系统的吞吐量是一个重要的指标
- 系统的吞吐量：单位时间内系统能够成功发送的新的数据帧的平均数量。
- 结论：
  - ALOHA系统最大的信道利用率为18.4%
  - ALOHA系统的信道利用率是非常低的。原因主要是各个站自由发送数据，碰撞概率增大

93

时隙ALOHA系统

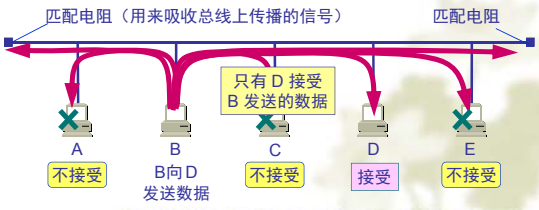
- 时隙ALOHA系统（Slotted ALOHA）：将信道时间分为离散的时间片，每个时间片可以用来发送一个数据帧。一个站点有数据发送时，必须等到下个时间片的开始才能发送。
- 时隙ALOHA系统的最大信道利用率为36.8%



94

CSMA/CD 协议

- 最初的以太网是将许多计算机都连接到一根总线上。当初认为这样的连接方法既简单又可靠，因为总线上没有有源器件。



95

以太网的广播方式发送

- 总线上的每一个工作的计算机都能检测到 B 发送的数据信号。
- 由于只有计算机 D 的地址与数据帧首部写入的地址一致，因此只有 D 才接收这个数据帧。
- 其他所有的计算机（A, C 和 E）都检测到不是发送给它们的数据帧，因此就丢弃这个数据帧而不能够收下来。
- 具有广播特性的总线上实现了一对一的通信。

96

为了通信的简便
以太网采取了两种重要的措施

- 采用较为灵活的无连接的工作方式，即不必先建立连接就可以直接发送数据。
- 以太网对发送的数据帧不进行编号，也不要求对方发回确认。
  - 这样做的理由是局域网信道的质量很好，因信道质量产生差错的概率是很小的。

97

以太网提供的服务

- 以太网提供的服务是不可靠的交付，即尽最大努力的交付。
- 当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做。差错的纠正由高层来决定。
- 如果高层发现丢失了一些数据而进行重传，但以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送。

98

载波监听多点接入/碰撞检测
CSMA/CD

Carrier Sense Multiple Access with Collision Detection

载波监听　　多点接入　　碰撞检测（也叫冲突检测）

先听后讲　　总线型网络　　边讲边听

总线上并没有什么“载波”，“载波监听”本质上就是用电子技术检测总线上有没有其他计算机发送的数据信号

当几个站同时发送数据时，总线上的信号电压摆动值将会增大（互相叠加）。当一个站检测到的信号电压摆动值超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。

- CSMA/CD可以完全避免冲突吗？　不能
- 冲突是怎么发生的
- 如何检测到冲突
- 检测到冲突后怎么办
- 冲突后如何选择重发的时间

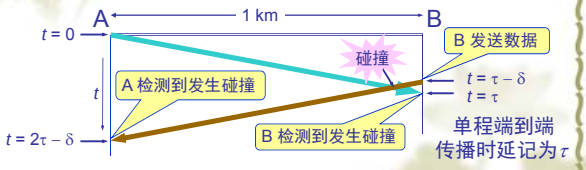
100

电磁波在总线上的
有限传播速率的影响

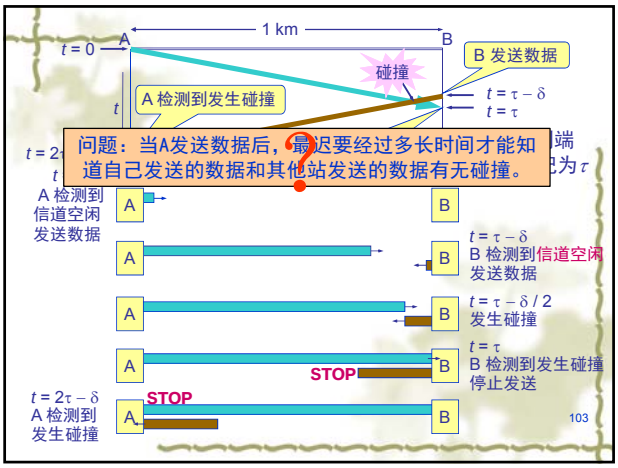
- 当某个站监听到总线是空闲时，也可能总线并非真正是空闲的。
- A 向 B 发出的信息，要经过一定的时间后才能传送到 B。
- B 若在 A 发送的信息到达 B 之前发送自己的帧(因为这时 B 的载波监听检测不到 A 所发送的信息)，则必然要在某个时间和 A 发送的帧发生碰撞。碰撞的结果是两个帧都变得无用。
- 因此，碰撞的根本原因是电磁波在媒体上的传播速度总是有限的。
- 例如：电磁波在1km电缆上的传播时延约为5us。

101

传播时延对载波监听的影响



102



争用期（碰撞窗口）

- 网上任一站点在开始发送后，最多经过2τ时间就能确认此次传输是否成功。
- 将以太网的端到端往返时延2τ称为争用期，或碰撞窗口。
- 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。
- 作用：可以用来确定最短有效帧长，即最短有效帧长为（2τ ×带宽）。
- 以太网取 51.2 μs 为争用期的长度。

问题： 10 Mb/s以太网的最短有效帧长是多少字节？

104

争用期的长度

- 对于 10 Mb/s以太网，在争用期内可发送512bit，即64字节。
- 以太网在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。即如果发生冲突，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，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中止的无效帧。

105

检测到碰撞后

- 在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息来
- 每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送

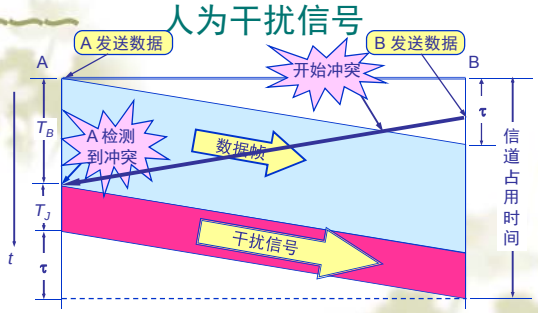
106

强化碰撞

- 当发送数据的站一旦发现发生了碰撞时，除了立即停止发送数据外，还要再继续发送若干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。
- 原因：假设冲突点离A很远，离B很近(例如40米，即B发送2bit后冲突，4bit后停发），4bit的叠加数据远距离传到A，可能被A忽略。A继续发送，浪费时间。
- 强化冲突的违规码长度介于32-64比特之间，不易被忽略。

107

人为干扰信号



B 也能够检测到冲突，并立即停止发送数据帧，接着就发送干扰信号。这里为了简单起见，只画出 A 发送干扰信号的情况。

108

二进制指数退避算法(truncated binary exponential backoff)

- 算法如下：
  - 1. 令基本退避时间T=2τ （即争用期）；
  - 2. k=min[重传次数，10]；
  - 3. r=在 [0, 1, …, (2^k-1)] 中随机取一个数；
  - 4. 退避时间=rT。
- 限定最大重传次数＝16，若发送16次仍不成功，则发送失败。

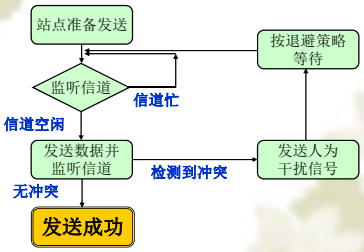
109

CSMA/CD的重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信而只能进行双向交替通信（半双工通信）。
- 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性，称为发送的不确定性。
- 要使碰撞的概率减小，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率。

110

CSMA/CD工作流程图



111

CSMA/CD 小结（1）

- 采用CSMA/CD，即“具有冲突检测的载波侦听多路访问”的介质访问控制方法。其要点如下：
  - a) 先听后讲
    - 发送前先侦听介质，若介质空闲，则立即发送；若介质忙，则继续侦听，直到介质空闲。
  - b) 边讲边听
    - 在发送过程中进行冲突检测。
  - c) 冲突停止
    - 若发送过程中检测到冲突，则立即停止发送。
  - d) 随机等待
    - 停止发送后，须等待一段随机时间后再侦听介质

112

CSMA/CD 小结（2）

- 每次冲突后，随机延迟的平均值加倍（二进制指数退避算法），即使较少发生冲突的帧具有较优先发送的概率。
- CSMA/CD访问方法可减少争用型总线上的冲突。

113

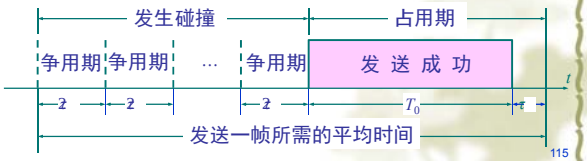
以太网的信道利用率

- 以太网的信道被占用的情况：
- 争用期长度为 2τ，即端到端传播时延的两倍。检测到碰撞后不发送干扰信号。
- 帧长为 L (bit)，数据发送速率为 C (b/s)，因而帧的发送时间为 $L/C = T_0$ (s)。

114

以太网的信道被占用的情况

- 一个帧从开始发送，经可能发生的碰撞后，将再重传数次，到发送成功且信道转为空闲(即再经过时间 τ 使得信道上无信号在传播)时为止，是发送一帧所需的平均时间。



参数 a

- 要提高以太网的信道利用率，就必须减小 τ 与 T_0 之比。在以太网中定义了参数 a，它是以太网单程端到端时延 τ 与帧的发送时间 T_0 之比：

$$a = \frac{\tau}{T_0}$$

- a→0表示一发生碰撞就立即可以检测出来，并立即停止发送，因而信道利用率很高。
- a越大，表明争用期所占的比例增大，每发生一次碰撞就浪费许多信道资源，使得信道利用率明显降低。

对以太网参数的要求

- 当数据率一定时，以太网的连线的长度受到限制，否则 τ 的数值会太大。
- 以太网的帧长不能太短，否则 T_0 的值会太小，使 a 值太大。

信道利用率的最大值 S_{max}

- 在理想化的情况下，以太网上的各站发送数据都不会产生碰撞（这显然已经不是 CSMA/CD，而是需要使用一种特殊的调度方法），即总线一旦空闲就有某一个站立即发送数据。
- 发送一帧占用线路的时间是 $T_0 + \tau$，而帧本身的发送时间是 T_0。于是我们可计算出理想情况下的极限信道利用率 S_{max}为：

$$S_{max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + a}$$

第3章 数据链路层

以太网标准

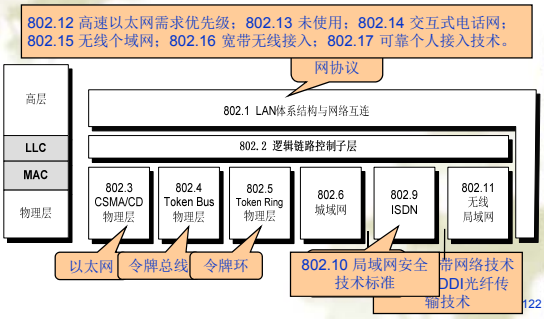
- 以太网是美国施乐(Xerox)公司于1975年研制成功的。
- 以太网用无源电缆作为总线来传送数据帧，并用历史上表示传播电磁波的以太(Ether)来命名。
- 两个标准
  - 1980年DEC、Intel、Xerox公司联合提出10Mb/s的以太网规约。DIX Ethernet V2 是世界上第一个局域网产品（以太网）的规约。
  - 1983年IEEE的802委员会制定以太网的 802.3 标准
  - DIX Ethernet V2 标准与IEEE的 802.3 标准只有很小的差别，因此人们常将 802.3 局域网简称为“以太网”

IEEE 802标准

- 80年代局域网迅速发展，各种标准层出不穷，为了使得不同厂家生产的局域网能够通信，IEEE于1980年2月成立一个局域网标准委员会，形成一系列的标准为IEEE802标准。
- IEEE802标准已被ANSI接收为美国国家标准，并于84年3月被ISO采纳为局域网的国际标准。
- 厂商的竞争，IEEE没有制定一个统一的局域网的标准，而是制定不同的局域网标准。

121

IEEE 802标准间的关系



122

以太网的层次结构

- IEEE 802委员会是局域网标准的主要制定者，它提出的局域网参考模型主要定义了物理层和数据链路层的规范，即相当于OSI模型的下两层。
  - 物理层：与OSI模型中类似，物理层负责与传输介质的连接，并在传输介质上传输比特流，因此，它描述和规定了与传输介质接口的特性。
  - 数据链路层：OSI模型中数据链路层的功能在IEEE 802模型中分成了两个子层(MAC和LLC)。

123

数据链路层的两个子层

- 为了使数据链路层能更好地适应多种局域网标准，802 委员会就把局域网的数据链路层拆成两个子层：
  - 逻辑链路控制LLC(Logical Link Control)子层
    - 逻辑链路控制子层的主要功能是屏蔽对各种不同物理网络的访问方法的差异，向上提供数据传输服务的统一的逻辑接口
  - 媒体接入控制MAC(Medium Access Control)子层
    - 媒体接入控制子层的主要功能是控制对传输介质的访问，并在物理层的基础上实现无差错通信。该子层随不同的物理网络差异较大

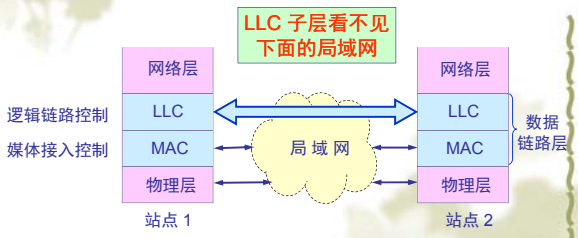
124

数据链路层的两个子层

- 以太网数据链路层拆分成MAC子层与LLC子层的好处：
  - 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。

125

局域网对LLC子层是透明的



126

TCP/IP一般不考虑 LLC 子层

- 由于TCP/IP 体系经常使用的局域网是 DIX Ethernet V2 而不是 802.3 标准中的几种局域网，因此现在 802 委员会制定的逻辑链路控制子层 LLC（即 802.2 标准）的作用已经不大了。
- 很多厂商生产的网卡上就仅装有 MAC 协议而没有 LLC 协议。

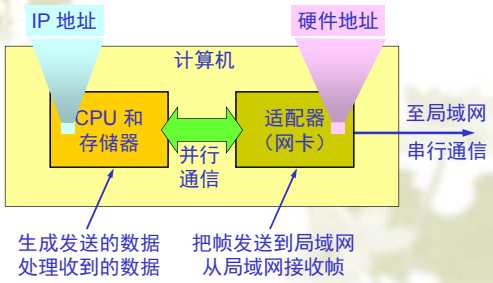
127

适配器的作用

- 计算机要连接到局域网需要依靠网卡。
- 网卡
  - 网络接口板又称为通信适配器(adapter)或网络接口卡 NIC (Network Interface Card)，或“网卡”。
  - 网卡的主要功能：
    - 进行串行/并行转换。
    - 对数据进行缓存。
    - 实现以太网协议。
    - 在计算机的操作系统安装设备驱动程序。

128

计算机通过网卡和局域网通信



129

MAC层的硬件地址

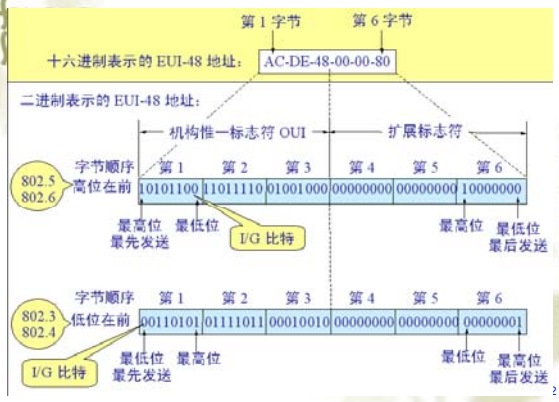
- 在局域网中，硬件地址又称为物理地址，或 MAC 地址
- 802标准为局域网规定一个48位的全球地址，是指固化在网卡ROM中的地址。
- 802 标准所说的“地址”严格地讲应当是每一个站的“名字”或标识符。
- 经典定义：
  - “名字是指我们要寻找的那个资源，地址指出资源在何处，路由告诉我们如何到达该处”。

130

MAC地址分配与描述

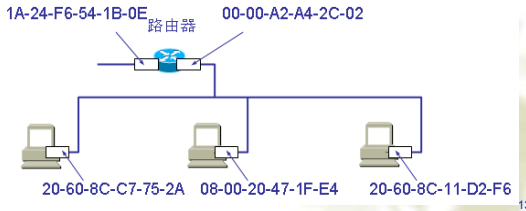
- IEEE的注册管理机构RA(Registration Authority)是局域网法定的全球管理机构。负责分配地址字段6个字节中的前3个字节(即高位24位)。
- 生产局域网网卡的厂家必须向IEEE购买由这3个字节构成的一个号(机构唯一标识符OUI)。
- 后三个字节(即低位24位)由厂家自行指派，称为扩展的唯一标识符EUI。
- 网卡地址或网卡标识符常写为：EUI-48
- IEEE规定地址第一字段第一字节为I/G比特；
  - “0”表示单站地址；“1”表示组地址。

131



网卡上的硬件地址

路由器由于同时连接到两个网络上，
因此它有两块网卡和两个硬件地址。



133

网卡检查MAC地址

- 网卡从网络上每收到一个 MAC 帧就首先用硬件检查 MAC 帧中的 MAC 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。
- “发往本站的帧”包括以下三种帧：
  - 单播(unicast)帧（一对一）
  - 广播(broadcast)帧（一对全体）
  - 多播(multicast)帧（一对多）

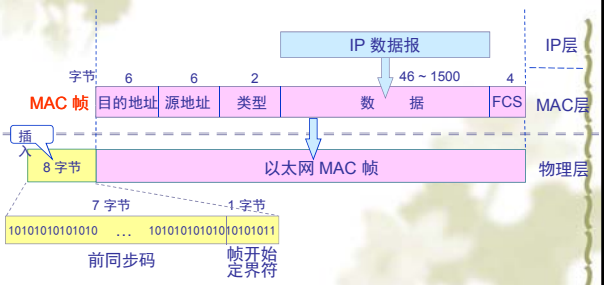
134

MAC帧格式

- 常用的以太网MAC帧格式有两种标准：
  - DIX Ethernet V2 标准
  - IEEE 的 802.3 标准
- 最常用的 MAC 帧是以太网 V2 的格式。

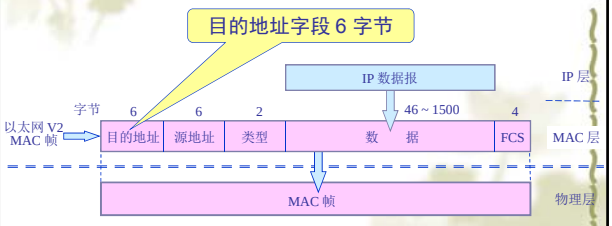
135

以太网的 MAC 帧格式



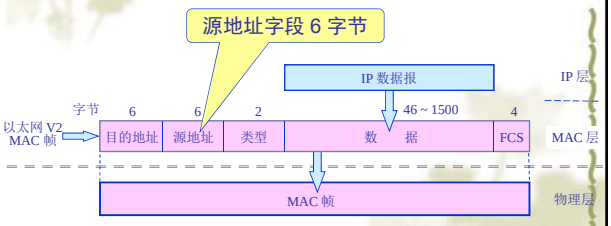
136

以太网 V2 的 MAC 帧格式



137

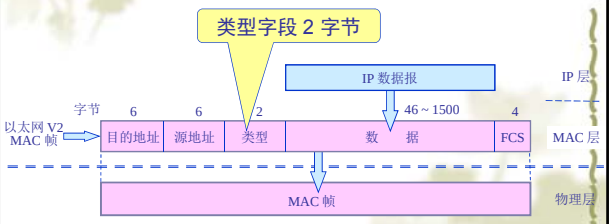
以太网 V2 的 MAC 帧格式



138

以太网 V2 的 MAC 帧格式

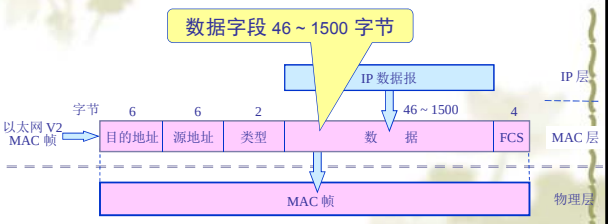
类型字段用来标志上一层使用的是什么协议，
以便把收到的 MAC 帧的数据上交给上一层的这个协议。



Xerox公司负责类型字段的代码分配：
类型字段为0x0800表示上层使用IP数据报
类型字段为0x8137表示上层使用Novell IPX数据报

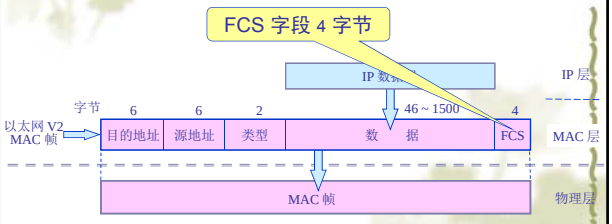
以太网 V2 的 MAC 帧格式

数据字段的正式名称是 MAC 客户数据字段
最小长度 64 字节 – 18 字节的首部和尾部 = 数据字段的最小长度



以太网 V2 的 MAC 帧格式

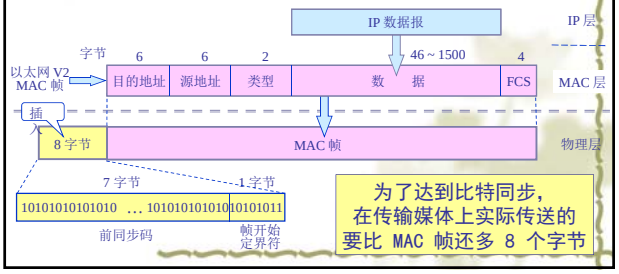
当传输媒体的误码率为 1×10^{-8} 时，
MAC 子层可使未检测到的差错小于 1×10^{-14}。



当数据字段的长度小于 46 字节时，
应在数据字段的后面加入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。

以太网 V2 的 MAC 帧格式

因为当一个站开始接收MAC帧时，没有与到达的比特流同步，
因此MAC帧的开始若干比特无法接收，这样使得整个帧无效。
这样需要插入同步码。



为了达到比特同步，
在传输媒体上实际传送的
要比 MAC 帧还多 8 个字节

无效的MAC帧

- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；
- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 ~ 1500 字节之间。
- 有效的 MAC 帧长度为 64 ~ 1518 字节之间。
- 对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

帧间最小间隔

- MAC子层标准还规定帧间最小间隔为 9.6 μs，相当于 96 bit 的发送时间。
- 一个站在检测到总线开始空闲后，还要等待 9.6 μs 才能再次发送数据。
- 这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理，做好接收下一帧的准备。

例题

- 右图示出了以太网V2的MAC帧格式，请参照这一格式完成下列关于局域网的问题。

(1) 前缀由二进制序列10101010重复7次组成，帧起始定界符则是固定的二进制序列_____。
10101011

例题

(2) 如果帧长按图中所示范围计算，那么允许的最小帧长是___64___字节，允许的最大帧长等于__1518__字节。

(3) 如果一个帧的数据单元段长度是40字节，那么该帧中填充字段的长度应该是___6___字节。

第3章 数据链路层

- 3.1 数据链路层的基本概念
- 3.2 组帧
- 3.3 差错控制
- 3.4 点对点协议PPP
- 3.5 使用广播信道的数据链路层
- 3.6 以太网的MAC层
- 3.7 扩展的以太网
- 3.8 虚拟局域网

局域网互联与互联设备

- 为什么要进行局域网互联？
  - (1) 局域网覆盖的距离有限
    - 单个局域网覆盖的距离往往不能满足应用的需要。
  - (2) 局域网能支持的连网计算机数目有限
    - 单个局域网所能连接的计算机数目往往不能满足应用的需要。
  - (3) 局域网上能传输的通信量有限
    - 单个局域网所容许的通信量往往不能满足应用的需要。

局域网互联设备

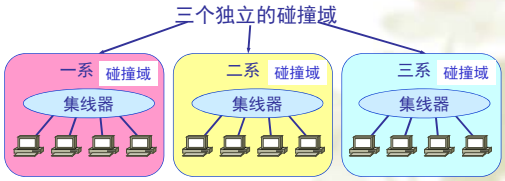
- 互联的本质
  - 由于网络是分层次实现的，而局域网又各有不同的标准，因此网络互联的本质就是在不同的协议层次上实现协议的彼此转换。
- 互联设备
  - 转发器（Repeater，重发器，中继器）
  - 集线器（Hub）
  - 网桥（Bridge）
  - 交换机（Switch）
  - 路由器（Router）
  - 网关（Gateway）

中继器

- 重发器又称中继器，它用于在物理层上实现两个同构型局域网之间的互连。
- 重发器的功能
  - 常用于连接两个同轴电缆以太网，将信号放大整形后，以延伸网络的传输距离。
  - 不具有信号通路的选择功能

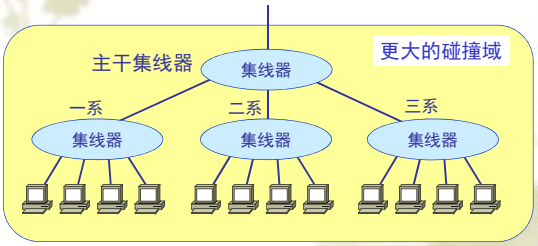
集线器

- 冲突域（碰撞域）
  - 任一时刻每个系中只能有一个站发送数据。
  - 若每个局域网的最大吞吐量为10Mb/s，则整个系统为30Mb/s的最大吞吐量。



151

集线器扩展局域网



152

集线器扩展局域网优缺点

- 优点
  - 使原来属于不同碰撞域的局域网上的计算机能够进行跨碰撞域的通信。
  - 扩大了局域网覆盖的地理范围。
- 缺点
  - 碰撞域增大了，但总的吞吐量并未提高。
  - 如果不同的碰撞域使用不同的数据率，那么就不能用集线器将它们互连起来。
  - 不具备自动转发和自动寻址能力，即不具备交换功能

153

网桥

- 在数据链路层扩展局域网使用网桥：
  - 网桥工作在数据链路层；
  - 网桥根据 MAC 帧的目的地址对收到的帧进行转发。
  - 网桥具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的端口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定将该帧转发到哪一个端口，或者把它丢弃（即过滤）。

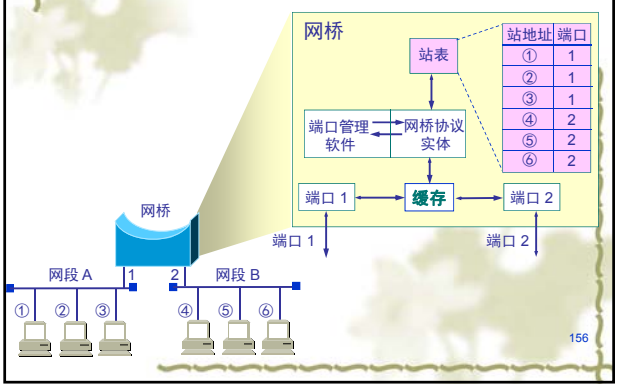
154

网桥的工作原理

- 网桥从端口接收网段上传送的各种帧，每当收到一个帧时，先暂存在缓存中。
  - 若此帧出错，则丢弃该帧。
  - 若此帧未出错，
    - 且欲发送的目的站的MAC地址属于另外一个网段，则通过查找“转发表”，将收到的帧送往对应的端口转发。
    - 同一个网段内的帧，不会被网桥转发，不会增加网络负担。
    - 如果网桥不知道目的地址属于哪个网段，则向其他所有网段广播。

155

网桥的内部结构



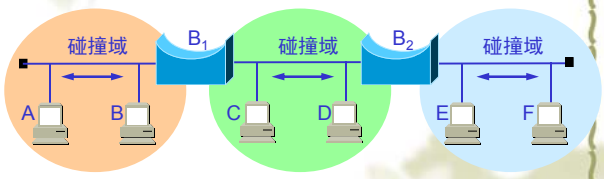
156

使用网桥带来的好处

- 过滤通信量，增大吞吐量。
- 扩大了物理范围。
- 提高了可靠性。
- 可互连不同物理层、不同 MAC 子层和不同速率（如10 Mb/s 和 100 Mb/s 以太网）的局域网。

157

网桥使各网段成为隔离开的碰撞域

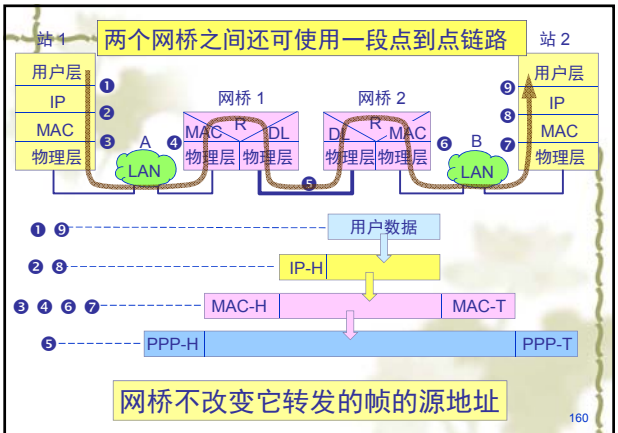


158

使用网桥带来的缺点

- 存储转发增加了时延。
- 在MAC 子层并没有流量控制功能。
- 具有不同 MAC 子层的网段桥接在一起时时延更大。
- 网桥只适合于用户数不太多(不超过几百个)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。

159



160

网桥和集线器(或转发器)的不同

- 集线器在转发帧时，不对传输媒体进行检测。
- 网桥在转发帧之前必须执行 CSMA/CD 算法。
  - 若在发送过程中出现碰撞，就必须停止发送和进行退避。
  - 在这一点上网桥的接口很像一个网卡。但网桥却没有网卡。
- 由于网桥没有网卡，因此网桥并不改变它转发的帧的源地址。

161

网桥的类型

- 网桥的特点
  - 用于在数据链路层上实现在数据链路层以上使用相同协议的局域网的互连
  - 负责完成物理层和数据链路层协议的转换
  - 具有路由选择功能，可提高网络的整体效率
- 依据不同路由确定方法
  - 固定路由网桥
  - 透明网桥
  - 源路由网桥

162

固定路由网桥

- 根据网络的互连环境，人工为每个网桥针对它所连接的每个局域网分别建立一张路由表。当一个帧到达时，网桥就根据预先设计好的路由表来决定如何进行转发。
- 缺点：不能适应动态改变的网络互连环境，路由表的维护困难。

163

透明网桥

- 能生成和修改自己路由表的网桥。
- 目前使用得最多的网桥是透明网桥(transparent bridge)。
- “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。
- 透明网桥是一种即插即用设备，其标准是IEEE 802.1D。

164

透明网桥

- 透明网桥的做法
  - 任何时候当网桥接收到一个帧时，根据其源地址就可获得发送该帧的站点所在的局域网，从而为路由表建立相应的条目；
  - 同时，为未知路由的帧使用扩散算法(Flooding Algorithm)来进行转发（即向它所连接的每个局域网发送该帧，该帧来自的那个局域网除外）。
- 特点：
  - 容易安装，能适应动态改变的网络环境
  - 确定路由的负担在网桥
  - 网络资源的利用不充分

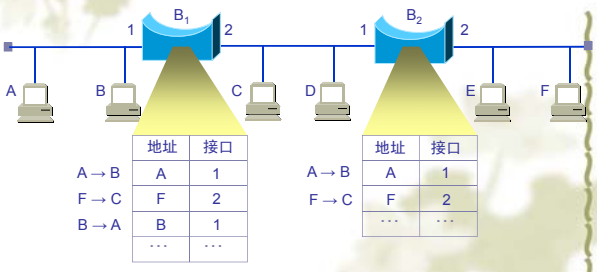
165

网桥在转发表中登记的信息

- 登记三项信息
  - 站地址：登记收到的帧的源 MAC 地址。
  - 端口：登记收到的帧进入该网桥的端口号。
  - 时间：登记收到的帧进入该网桥的时间。
- 站地址问题
  - 转发表中的 MAC 地址是根据源 MAC 地址写入的，但在进行转发时是将此 MAC 地址当作目的地址。
  - 例如：如果网桥现在能够从端口 x 收到从源地址 A 发来的帧，那么以后就可以从端口 x 将帧转发到目的地址 A。

166

转发表的建立过程举例



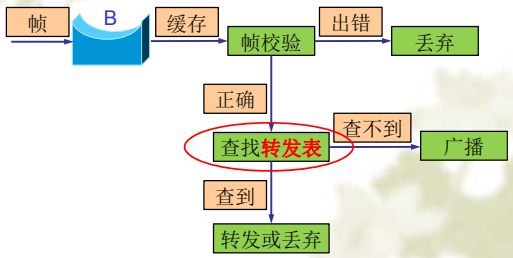
167

转发表中的计时器

- 为了使转发表反映最新的局域网拓扑
  - 局域网的拓扑结构经常变化，为了使转发表能反映整个局域网的最新拓扑，所以要记录下每个帧到达到达网桥的时间。
- 具体做法：
  - 网桥中的端口管理软件周期性地扫描转发表中的项目。将一定时间（如几分钟）之前登记的项目删除。

168

透明网桥的工作原理

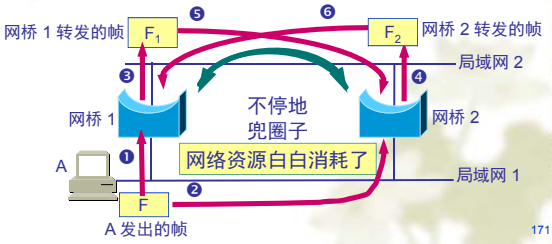


网桥自学习和转发帧的步骤归纳

- 网桥收到一帧后先进行自学习。查找转发表中与收到帧的源地址有无相匹配的项目。
  - 如没有，就在转发表中增加一个项目（源地址、进入的端口和时间）。
  - 如有，则把原有的项目进行更新。
- 转发帧。查找转发表中与收到帧的目的地址有无相匹配的项目。
  - 如没有，则通过所有其他端口（但进入网桥的端口除外）进行转发。
  - 如有，则按转发表中给出的端口进行转发。
  - 若转发表中给出的端口就是该帧进入网桥的端口，则应丢弃这个帧（因为这时不需要经过网桥进行转发）。

透明网桥使用了生成树算法

- 这是为了避免产生转发的帧在网络中不断地兜圈子



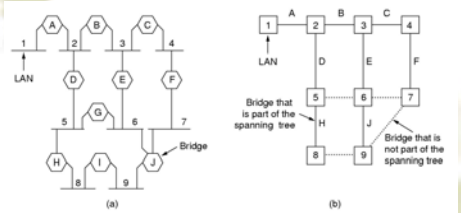
生成树的得出

- 互连在一起的网桥在进行彼此通信后，就能找出原来的网络拓扑的一个子集。在这个子集里，整个连通的网络中不存在回路，即在任何两个站之间只有一条路径。

为了避免产生转发的帧在网络中不断地兜圈子

- 为了得出能够反映网络拓扑发生变化时的生成树，在生成树上的根网桥每隔一段时间还要对生成树的拓扑进行更新。

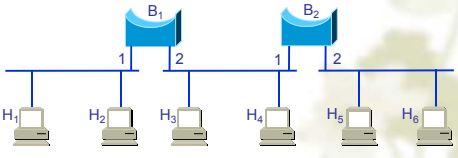
生成树算法

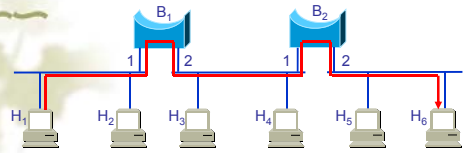


基本原理：选择一个网桥作为生成树的根，然后以最短路径为依据，找到树上的每一个结点

例题

- 现有六个站分别连接在三个局域网上，并且用两个透明网桥B_1和B_2连接起来，如下图所示。每一个网桥的两个端口号都标明在图上。在一开始，两个网桥中的转发表都是空的。按下表中发送帧的顺序将有关数据填写在表中（其中MACn表示该机的站地址即MAC地址）





发送的帧	网桥1的转发表		网桥2的转发表		B_1的处理（转发?丢弃?登记?）	B_2的处理（转发?丢弃?登记?）
	站地址	端口	站地址	端口		
$H_1 \rightarrow H_6$	MAC_1	1	MAC_1	1	转发，登记	转发，登记
$H_3 \rightarrow H_2$	MAC_3	2	MAC_3	1	转发，登记	转发，登记
$H_5 \rightarrow H_3$	MAC_5	2	MAC_5	2	登记，丢弃	转发，登记
$H_2 \rightarrow H_1$	MAC_2	1			登记，丢弃	接收不到这个帧

175

源路由网桥

- 源路由网桥(source route bridge)在发送帧时将详细的路由信息放在帧的首部中。
- 由发送站点确定到达目的地的路由，并将它存储在所发送的帧中；网桥接收帧后按其指示的路由将它转发到下一个局域网上。
- 特点
  - 能适应动态改变的网络环境
  - 确定路由的负担在站点

176

源路由网桥路由的确定

- 源站以广播方式向欲通信的目的站发送一个发现帧（discovery frame），每个发现帧都记录所经过的路由。
- 发现帧到达目的站时就沿各自的路由返回源站。源站在得知这些路由后，从所有可能的路由中选择出一个最佳路由。凡从该源站向该目的站发送的帧的首部，都必须携带源站所确定的这一路由信息。

177

多端口网桥—以太网交换机

- 1990 年问世的交换式集线器(switching hub)，可明显地提高局域网的性能。
- 交换式集线器常称为以太网交换机(switch)或第二层交换机（表明此交换机工作在数据链路层）。
- 以太网交换机通常都有十几个端口。因此，以太网交换机实质上就是一个多端口的网桥，可见交换机工作在数据链路层。

178

以太网交换机的特点

- 以太网交换机的每个端口都直接与主机相连，并且一般都工作在全双工方式。
- 交换机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，进行无碰撞地传输数据。
- 以太网交换机由于使用了专用的交换结构芯片，其交换速率就较高。

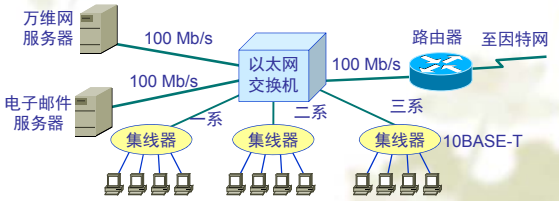
179

独占传输媒体的带宽

- 对于普通 10 Mb/s 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(10 Mb/s)的 N 分之一。
- 使用以太网交换机时，虽然在每个端口到主机的带宽还是 10 Mb/s，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×10 Mb/s。这正是交换机的最大优点。

180

用以太网交换机扩展局域网

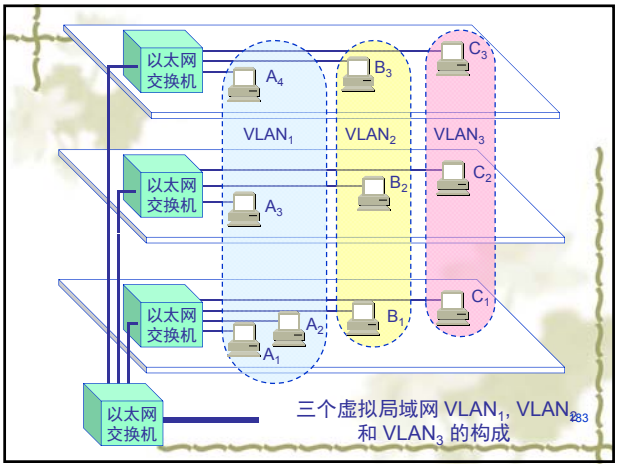


181

虚拟局域网

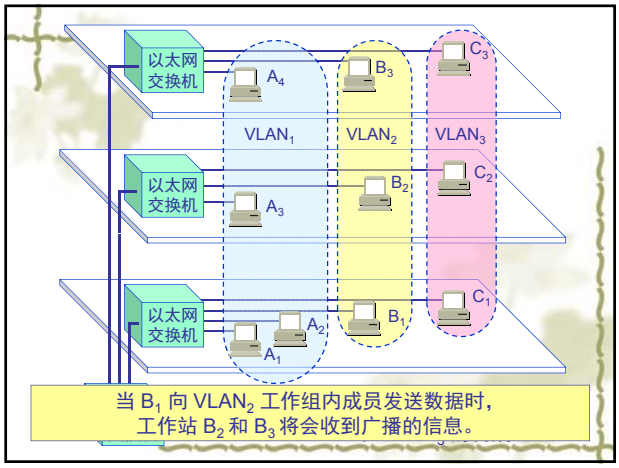
- 利用以太网交换机可以很方便地实现虚拟局域网
- 虚拟局域网 VLAN 是由一些局域网网段构成的与物理位置无关的逻辑组。
  - 这些网段具有某些共同的需求。
  - 每一个 VLAN 的帧都有一个明确的标识符，指明发送这个帧的工作站是属于哪一个 VLAN。
- 虚拟局域网其实只是局域网给用户提供的一种服务，而并不是一种新型局域网。

182

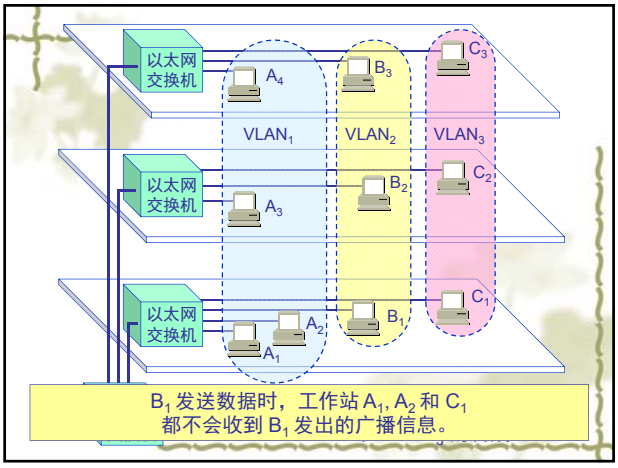


三个虚拟局域网 $VLAN_1$, $VLAN_2$ 和 $VLAN_3$ 的构成

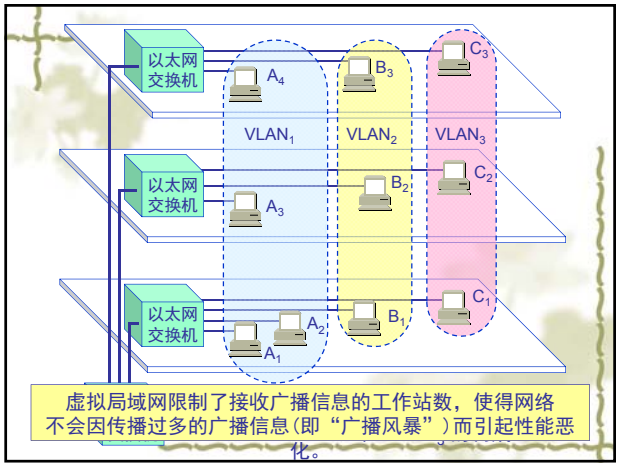
183



当 B_1 向 $VLAN_2$ 工作组内成员发送数据时，工作站 B_2 和 B_3 将会收到广播的信息。



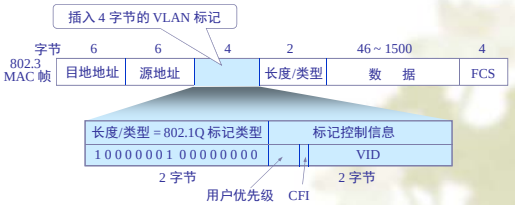
B_1 发送数据时，工作站 A_1, A_2 和 C_1 都不会收到 B_1 发出的广播信息。



虚拟局域网限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息(即“广播风暴”)而引起性能恶化。

虚拟局域网使用的以太帧格式

- 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，称为 VLAN 标记(tag)，用来指明发送该帧的工作站属于哪一个虚拟局域网。



虚拟局域网的优点

- 安全性好
  - 没有路由的情况下，不同虚拟局域网间不能相互通信。
- 网络分段
  - 可将物理网络逻辑分段，而不是按物理分段。可将不同地点、不同部门的计算机划分在一个虚拟局域网上。
- 提供较好的灵活性
  - 方便地将一个站点加入或从一个VLAN中删除。

第3章 数据链路层

100BASE-T 以太网

- 速率达到或超过 100 Mb/s 的以太网称为高速以太网。
- 在双绞线上传送 100 Mb/s 基带信号的星型拓扑以太网，仍使用 IEEE 802.3 的 CSMA/CD 协议。100BASE-T 以太网又称为快速以太网(Fast Ethernet)。

100BASE-T 以太网的特点

- 可在全双工方式下工作而无冲突发生。因此，不使用 CSMA/CD 协议。
- MAC 帧格式仍然是 802.3 标准规定的。
- 保持最短帧长不变，但将一个网段的最大电缆长度减小到 100 m。
- 帧间时间间隔从原来的 9.6 μs 改为现在的 0.96 μs。

三种不同的物理层标准

- 100BASE-TX
  - 使用 2 对 UTP 5 类线或屏蔽双绞线 STP。
- 100BASE-FX
  - 使用 2 根光纤。
- 100BASE-T4
  - 使用 4 对 UTP 3 类线或 5 类线。

吉比特以太网

- 允许在 1 Gb/s 下全双工和半双工两种方式工作。
- 使用 802.3 协议规定的帧格式。
- 在半双工方式下使用 CSMA/CD 协议（全双工方式不需要使用 CSMA/CD 协议）。
- 与 10BASE-T 和 100BASE-T 技术向后兼容。

193

吉比特以太网的物理层

- 1000BASE-X：基于光纤通道的物理层
  - 1000BASE-SX　SX表示短波长
  - 1000BASE-LX　LX表示长波长
  - 1000BASE-CX　CX表示铜线
- 1000BASE-T
  - 使用 4对 5 类线 UTP

194

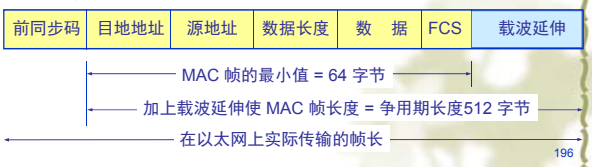
载波延伸(carrier extension)

- 吉比特以太网在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 100 m，但采用了“载波延伸”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。

195

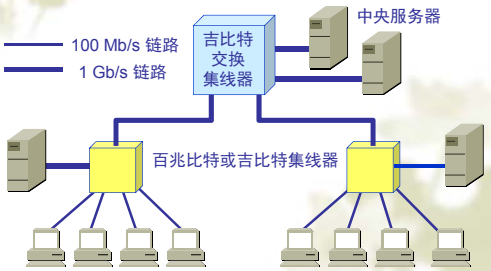
在短 MAC 帧后面加上载波延伸

- 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，但这对有效载荷并无影响。
- 接收端在收到以太网的 MAC 帧后，要将所填充的特殊字符删除后才向高层交付。



196

吉比特以太网的配置举例



197

10 吉比特以太网

- 10 吉比特以太网与 10 Mb/s，100 Mb/s 和 1 Gb/s 以太网的帧格式完全相同。
- 10 吉比特以太网还保留了 802.3 标准规定的以太网最小和最大帧长，便于升级。
- 10 吉比特以太网不再使用铜线而只使用光纤作为传输媒体。
- 10 吉比特以太网只工作在全双工方式，因此没有争用问题，也不使用 CSMA/CD 协议。

198

本章小结

- 熟悉数据链路层的基本功能，掌握常用的帧定界方法、检错码和数据链路层协议
- 掌握局域网的基本概念，重点掌握以太网的基本协议，媒体访问控制方法，熟悉网桥、交换机的工作原理
- 习题&作业

199