

§ 4. 介质访问控制子层

★ 与第三章的关系

第三章：点对点网络，单向/双向

第四章：广播网络，多方竞争使用权

§ 4. 介质访问控制子层

4. 1. 信道分配问题

4. 1. 1. 静态信道分配

★ 含义：把一个信道拆开，分给多个用户使用

- FDM：将频带分成若干逻辑子信道，用户在分配到一定的频带后，在通信过程中始终都占用这个频带
 - ◆ 同样的时间占用不同的频率带宽资源
 - ◆ 每个信源占用一个子信道
- TDM：将时间划分为一段段等长的时分复用帧，每个用户在每个TDM帧中占用固定序号的时隙，即将一条物理传输线路分成若干等长的时间片，轮换地被多个信源使用
 - ◆ 每个用户所占用的时隙是周期性地出现，其周期就是TDM帧的长度，因此所有用户在不同的时间占用同样的频带宽度

★ 存在的问题：静态信道分配适用于流量均衡且平稳的情况，而计算机系统中数据流量则表现为(每个用户的)极端突发性

- FDM：总存在信道浪费或不够用
- TDM：即使 $N=\text{用户数}$ 仍存在信道浪费和不够用

§ 4. 介质访问控制子层

4. 1. 信道分配问题

4. 1. 1. 静态信道分配

★ 存在的问题

- 以FDM为例进行定量分析, 假设:

容量为 C bps,

发送一帧的平均时延为 T ,

随机到达帧的平均到达率为 λ 帧/秒

帧长度可变, 均值为每帧 $1/\mu$ 位

则: 信道的服务率为 μC 帧/秒

由排队论可知, $T = \frac{1}{\mu C - \lambda}$ (泊松分布)

100Mbps

5000

10000

服务率 $\mu C = 100 * 1000 * 1000 * (1/10000) = 10000$
 $T = 1/(10000 - 5000) = 0.2\text{ms} = 200 \mu\text{s}$

假设: 将 C 分为 N 个独立子信道, 则每个子信道的容量为 C/N bps, 到达率为 λ/N

则: $T_{FDM} = \frac{1}{\mu(C/N) - \lambda/N} = \frac{N}{\mu C - \lambda} = NT$

- 每个用户的极端突发性与总体流量的动态均衡

例: 不同机场安检通道的人群引导

普通电话与IP电话

电信宽带与长城宽带(每人独享/多人共享)

§ 4. 介质访问控制子层

4. 1. 信道分配问题

4. 1. 2. 动态信道分配的假设

- ★ 流量独立：N个站，每个站仅一个进程产生待发帧，在时间 Δt 内产生帧的概率是 $\lambda \Delta t$
(λ 为新帧到达率)，生成后该站被阻塞直到帧被成功发送出去
- ★ 单信道假设：所有通信共用一个信道，N个站等概率
- ★ 冲突可观察：若两个以上的帧同时发送就产生冲突，所有站均能检测到冲突，冲突帧会被再次发送
- ★ 时间连续或分槽：下列两者任取其一
 - 连续时间假设：帧可在任何时刻发送
 - 时隙假设：帧总在时隙开始时发送，且一个时隙内至多1个帧可能发送成功
(空闲、一帧发送成功、多帧发送冲突)
- ★ 侦听假设：下列两者任取其一
 - 载波侦听：发送前先检测是否空闲，满足条件才发送
 - 非载波侦听：任意发送，通过接受端来检测发送是否成功

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.1. ALOHA

★ 纯ALOHA

- 采用连续时间的非载波侦听，竞争使用
- 由发送方侦听收到的数据来判断发送是否成功
- 若产生冲突(发送不成功)则发送方等待随机时间后再次发送(等待时间不能固定，否则永远冲突)
- 帧长度一般统一(比长度可变帧的吞吐量更大)

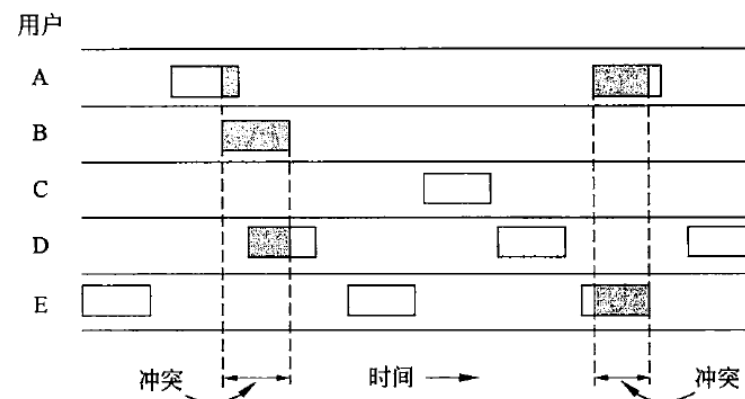


图 4-1 在纯 ALOHA 中帧的发送次序是任意的

★ 时隙ALOHA

- 协议机制：时间划分为若干时间槽，每个时间槽对应一帧，只有在时间槽开始的时候才允许发送，发送方式为非载波侦听，称为时隙非载波侦听
- 易损期比纯ALOHA缩小一半

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.1. ALOHA

★ 纯ALOHA的效率分析

- 帧时：发送标准长度帧所需时间(帧长/比特率)

- 假定无限多个用户按泊松分布规律产生新帧，

平均每帧时产生 N 个新帧，则：

$\left\{ \begin{array}{l} 0 < N < 1: \text{冲突小, 合理, 期望} \\ N > 1: \text{冲突大, 不合理} \end{array} \right.$

$\Rightarrow N$ 实际上是每帧时的吞吐率

\Rightarrow 每帧时内除新帧外，还有考虑旧帧重传

- 考虑重传帧：假设每帧时新旧帧总数为 G ($G \geq N$)，且 G 也服从泊松分布，则：

$\left\{ \begin{array}{l} G \approx N, \text{低负荷, 冲突少, 重传少} \\ G > N, \text{高负荷, 冲突多, 重传多} \end{array} \right.$

- 吞吐量 $S = GP_0$ ，其中， P_0 为一帧发送成功概率

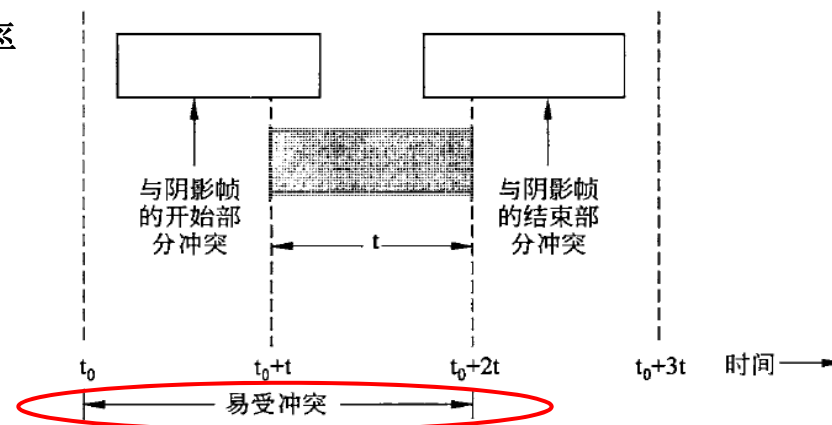


图 4-2 阴影帧的易受冲突周期

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.1. ALOHA

★ 纯ALOHA的效率分析

- 假设在任一给定“帧时”内，希望有G帧但生成k帧的概率服从Poisson分布，则： $P_r[k] = \frac{G^k e^{-G}}{k!}$
 - => 产生0帧的概率为 e^{-G}
 - => 在两个“帧时”内产生帧的平均数为2G
 - => 由上面两个条件得，在整个易受冲突期中一帧发送成功(无它帧产生)的概率 $P_0 = e^{-2G}$
 - => 令 $S = Ge^{-2G}$ 的一阶导数为0，可得 $G=0.5$
 - 则： $S = \frac{1}{2e} \approx 18.4\%$ (最大吞吐率)

★ 时隙ALOHA

- 最大吞吐率 纯ALOHA : $S = Ge^{-2G}$
时隙ALOHA: $S = Ge^{-G}$
 - => 令 $S = Ge^{-G}$ 的一阶导数为0，可得 $G=1$
 - 则： $S = \frac{1}{e} \approx 36.8\%$ (最大吞吐率)
 - => 时隙ALOHA的最好结果是空闲、成功和冲突时隙分别占37%、37%和26%

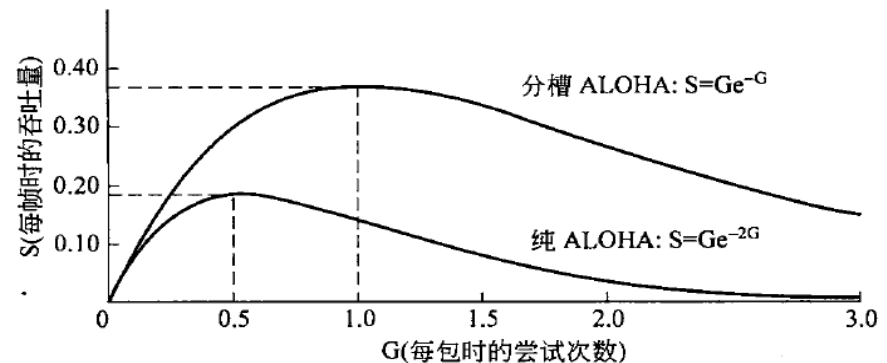


图 4-3 ALOHA 系统的吞吐量与负载的关系

- 一帧发送成功(无其它帧产生)的概率 $P_0 = e^{-G}$
则冲突概率为 $(1 - e^{-G})$
 - => 经k次尝试(前k-1次均失败)才能成功的概率

$$P_k = e^{-G} (1 - e^{-G})^{k-1}$$

- => 每帧传输成功次数的数学期望

$$E = \sum_{k=1}^{\infty} k P_k = e^G$$

结论：性能随负载的增长呈指数级下降

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.2. 载波侦听多路访问协议

★ 含义：发送站监听是否存在载波（是否有传输），并据此采取相应的动作，则这样的协议称为载波侦听协议(carrier sense protocol)

- “载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生碰撞
- 信道上实际并没有“载波”，只是用电子技术检测信道上有没有其他计算机发送的数据信号

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.2. 载波侦听多路访问协议

★ 坚持与非坚持CSMA (Carrier Sense Multiple Access)

● 1-坚持CSMA:

(1) 若信道空闲就发送

(2) 若信道忙则继续侦听，直到检测到信道空闲就发送

(3) 若冲突，则等待一随机时间后再重复(1)

=> 两站的随机时间相同仍可能冲突

=> 两站随机时间相差很小时（某站刚开始发送，信号尚未到达另一站时），也可能会产生冲突

=> 取决于信道的带宽-延迟积 (第3章)

● 非坚持CSMA:

(1) 若信道空闲就发送

(2) 若信道忙，则等待一随机时间后再重复(1)

● p-坚持CSMA:

(1) 若信道空闲就以概率 p 发送，或以 $(1-p)$ 等待一个时间单位

(2) 若信道忙则继续侦听，直到信道空闲重复(1)

(3) 若发送延迟一个时间单位，则重复(1)

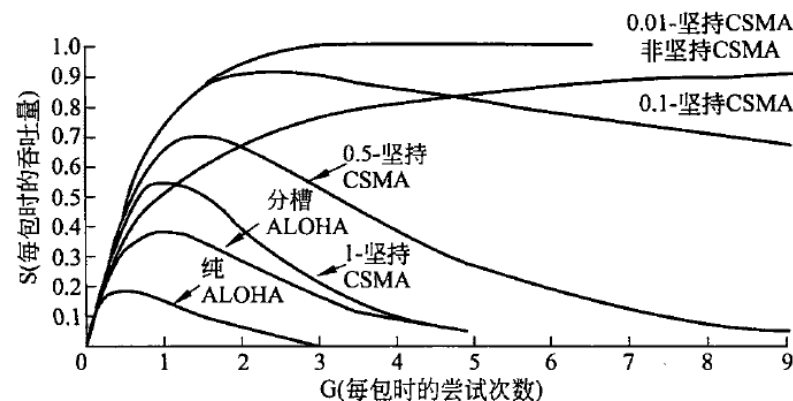


图 4-4 不同随机访问协议的信道使用率与负载比较

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.2. 载波侦听多路访问协议

★ 冲突检测：前述的多种CSMA，在发生冲突时均能检测出来，但是发生冲突后仍然会持续将本帧发送完成(后续发送实际无价值)，因此可以边发送边检测，发现冲突立即停止传输(节约时间和带宽)

- 计算机边发送数据边检测信道上的信号电压大小
- 当几个站同时在总线上发送数据时，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
- 所谓“碰撞”就是发生了冲突。因此“冲突检测”也称为“碰撞检测”

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.2. 载波侦听多路访问协议

★ 带冲突检测的CSMA (CSMA/CD = CSMA with Collision Detection)

- 由发送站读接受信号并检测
- 适用于有线信道，要求接受信号相比于发射信号不能相差太多
- 要求采用能被检测到冲突的调制解调技术

(例：电压正/负 - 1/0 => 可以)

电压正/0 - 1/0 => 不可以)

- 是经典以太网采用的方法，只能是半双工
- 概念模型存在三种状态：竞争周期、传输周期和空闲周期

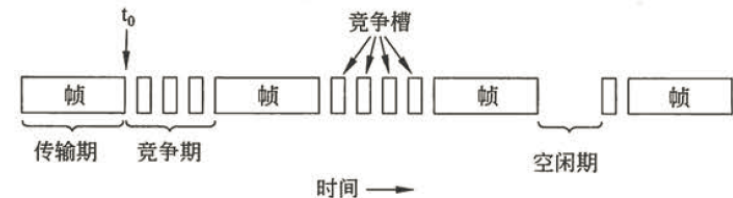


图 4-5 CSMA/CD 可能处于竞争、传输或空闲状态

问：假设 t_0 同时有两站开始发送数据，多少时间后能检测到发生冲突？（设信道上相距最远两站传输时间为 τ ）

答： τ ?

极端情况： $t_0 + \tau - \xi$ 时刻另一站开始发送，则：

新发送站： ξ 后立即检测到

原发送站： $2\tau - \xi$ 才检测到

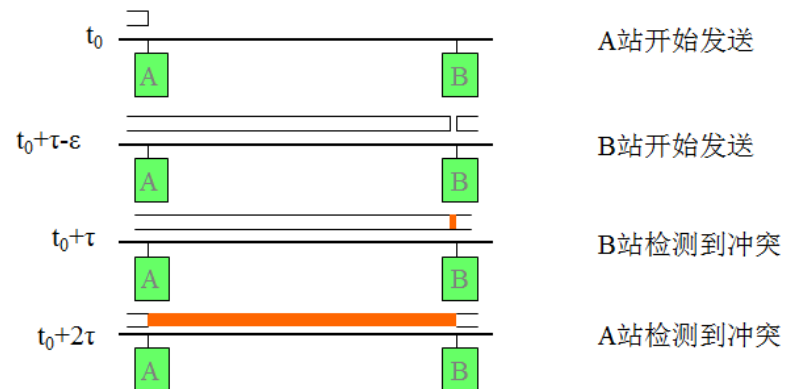
正确答案： 2τ

=> CSMA/CD 可看做时间槽宽度为 2τ 的分槽ALOHA

两者区别：

分槽ALOHA：到时间槽开始则直接发送

CSMA/CD：到时间槽开始要检测碰撞后发送



§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.3. 无冲突协议

★ 协议描述

- 假定N个站，地址0~N-1
- 假定传播时延可忽略不计

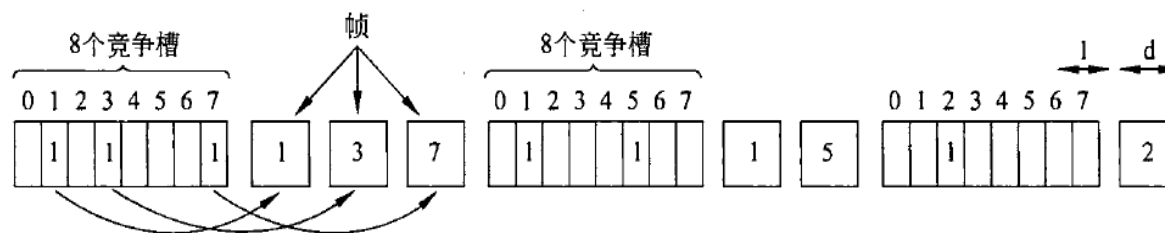


图 4-6 基本位图协议

★ 位图协议

- 工作过程：基本位图法，每个竞争期正好N个槽，在一个竞争期内，所有想发送的站在对应位置位，然后依次发送；全部发送完成后再次重复上述操作
- 性能分析：以位图作为测量时间的基本单位，每个数据帧由d个时间单位组成，时间槽不断轮询，某时间点第i槽有数据发送

◆ 低负荷情况

=> 小序号平均等待 $1.5N$ ，大序号平均等待 $0.5N$

=> 效率为 $d/(N+d)$ **N位额外开销，d位数据长度**

◆ 高负荷情况

假定所有站均为待发站，则每帧的额外开销为1bit，其效率为 $d/(d+1)$

=> 一帧平均延迟时间=站内排队时间+ $(N-1)d+N$

(其它所有站轮流发送一帧+一个位图时间)

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.3. 无冲突协议

★ 令牌传递

- 工作过程：系统定义一个特定的短帧，当做令牌，按照某个特定的预定义顺序在各站间依次传输，持有令牌者才能发送数据，若持有令牌者本次无数据发送，则直接传递给下一站
- 性能分析：类似于位图协议(略)

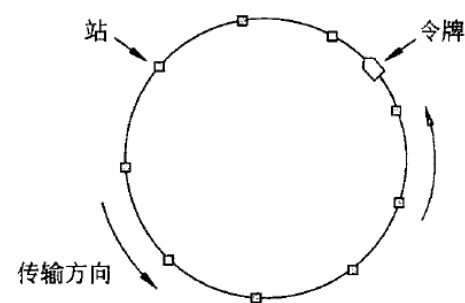
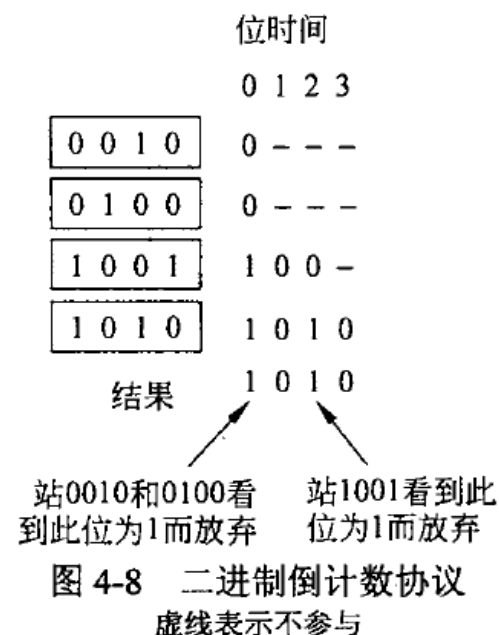


图 4-7 令牌环

★ 二进制倒数计数

- 工作过程：假设所有地址长度相等，各待发站将二进制位串地址进行广播，然后从高到低逐位比较；各地址的相同位进行按位OR操作，如果发现自身对应0的位为1则退出竞争，否则继续参与竞争直到获得发送权(低地址放弃，最高地址站获得发送权)
- 性能分析：信道效率为 $d/(d+\log_2 N)$
 - ◆ 适当调整帧结构，可节省 $\log_2 N$ (利用率100%)
 - ◆ 高地址拥有高优先级，可以变换为采用动态优先级方式，每站成功发送后变更其优先级为最低



§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.4. 有限竞争协议

★ 有限竞争协议的引入

- 有竞争(多种CSMA、CSMA/CD):
 - 负载较轻时: 延迟短、冲突少 (选)
 - 负载较重时: 冲突多, 不断重发
- 无竞争(位图、令牌、二进制倒计数):

负载较轻时: 延迟相对较高

负载较重时: 额外开销相对固定使信道的利用率高 (选)

=> 能否使二者的优势结合 (轻负载时良好的延迟特性, 重负载时较高的信道利用率)

=> 有限竞争协议

★ 有限竞争协议的基本思想

- 对节点进行分组, 每个时隙内只允许一个组的节点竞争信道 (目的是通过减少同一时隙内的竞争节点数来提高发送成功的概率)
- 组内节点数随系统负载的变化动态调整, 负载轻则节点数较多, 负载重则节点数少 (各自走向极端, 就是竞争协议和无冲突协议)
- 协议的关键在于如何根据系统负载自适应调整组的划分, 将时隙分配给节点

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.4. 有限竞争协议

★ 对称协议性能分析

对称协议：每个站均以概率 p 申请使用信道

设有 k 个站竞争，每个站在每个时隙中发送概率为 p ，在一给定时隙内某站获取信道的概率为 $P_r[p] = kp(1-p)^{k-1}$

令 $P_r[p]$ 的一阶导数为0，则当 $p=1/k$ 时， P_r 有最佳值，即 $P_r[p = \frac{1}{k} \text{ (最佳值) 的成功率}] = (\frac{k-1}{k})^{k-1}$

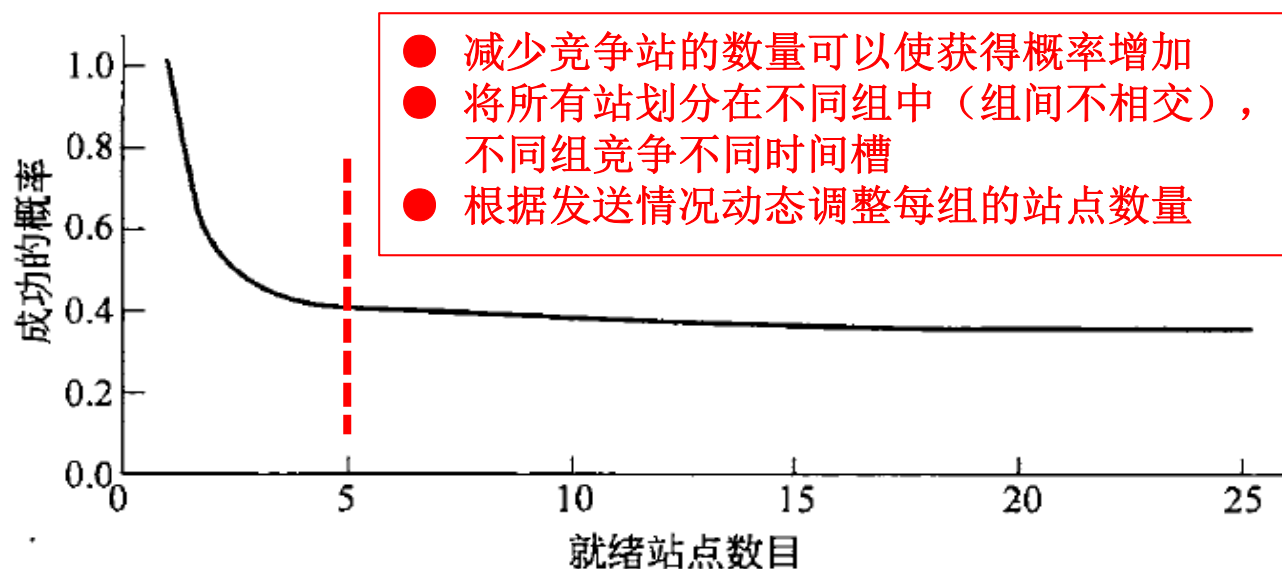


图 4-9 对称竞争信道的获得概率

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.4. 有限竞争协议

★ 自适应树遍历协议(Adaptive Tree Walk Protocol)

- 各站作为二叉树的叶子节点，按先序遍历的顺序依次分配各时隙（第0/1/2...时隙）
- 每个非叶节点下面的全部叶子节点(站)共同竞争该非叶节点的时隙，叶子节点独享该时隙
- 若某个时隙无冲突，则要么无站需发送，要么仅有一个站需发送（发送成功），此时其下层所有节点的对应时隙全部被跳过，将后续时隙分配给序列中的后续节点
- 若某个时隙有冲突，则继续下一时隙的发送判断

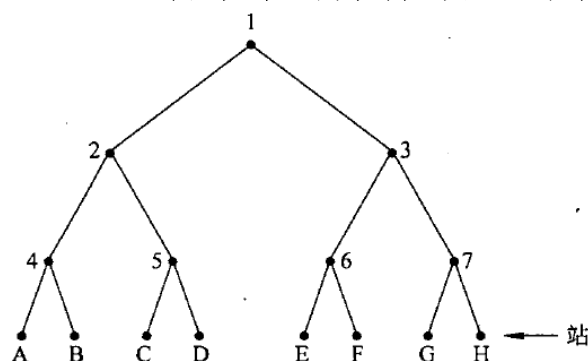


图 4-10 包含 8 个站的树

例：A-H 八个站点，形成
如果所示自适应树

问：假设 CF 需发送
需要几个时隙？

答：共 3 个时隙

第 0 时隙：节点 1 - CF

第 1 时隙：节点 2 - C 发送

4AB5CD - 被跳过

第 2 时隙：节点 3 - F 发送

6EF7GH - 被跳过

例：A-H 八个站点，形成
如果所示自适应树

问：假设 AEFG 四站需发送
需要几个时隙？

答：共 7 个时隙

第 0 时隙：节点 1 - AEFG

第 1 时隙：节点 2 - A 发送

4AB5CD - 被跳过

第 2 时隙：节点 3 - EFG

第 3 时隙：节点 6 - EF

第 4 时隙：节点 E 发送

第 5 时隙：节点 F 发送

第 6 时隙：节点 7 - G 发送

GH - 被跳过

例：A-H 八个站点，形成
如果所示自适应树

问：若 CD 需发送
需要几个时隙？

答：共 7 个时隙

第 0 时隙：节点 1 - CD

第 1 时隙：节点 2 - CD

第 2 时隙：节点 4 - 空

AB - 被跳过

第 3 时隙：节点 5 - CD

第 4 时隙：节点 C 发送

第 5 时隙：节点 D 发送

第 6 时隙：节点 3 - 空

6EF7GH - 被跳过

例：A-H 八个站点，形成
如果所示自适应树

问：若 A-H 全部需发送
需要几个时隙？

答：共 15 个时隙

例：A-H 八个站点，形成
如果所示自适应树

问：若 D 需发送
需要几个时隙？

答：共 1 个时隙

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.4. 有限竞争协议

★ 自适应树遍历协议

- 改进：从树的那层开始搜索效率更高？

假定N个站中有q个站准备好发送，且分布均匀，则最优搜索起始级应是每时隙参与竞争的平均站数为1的那一级，即 $2^{-i}q=1$ ，可得 $i=\log_2 q$

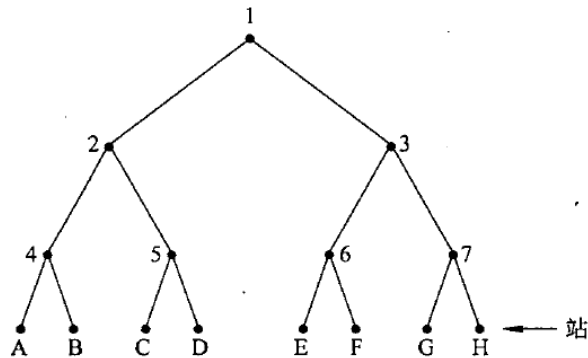


图 4-10 包含 8 个站的树

例：ACEG四个站准备发送
=> 从4（第2层）开始
第0时隙：节点4 - A发送
第1时隙：节点5 - C发送
第2时隙：节点6 - E发送
第3时隙：节点7 - G发送
不改进：七个时隙，分别节点
1245367

例：CF两个站准备发送
=> 从2（第1层）开始
第0时隙：节点2 - C发送
第1时隙：节点3 - F发送
不改进：三个时隙，分别节点123

例：C站准备发送
=> 从1（第0层）开始
第0时隙：节点1 - C发送
不改进：同样一个时隙

- 继续改进：跳过必冲突节点

例：GH两个站准备发送
=> 从2（第1层）开始
第0时隙：节点2 - 空
第1时隙：节点3 - GH
第2时隙：节点6 - 空
第3时隙：节点7 - GH
第4时隙：节点G发送
第5时隙：节点H发送

例：GH两个站准备发送
=> 从2（第1层）开始
第0时隙：节点2 - 空
则同级3必冲突，跳过
第1时隙：节点6 - 空
则同级7必冲突，跳过
第2时隙：节点G发送
第3时隙：节点H发送

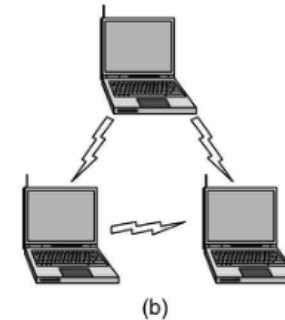
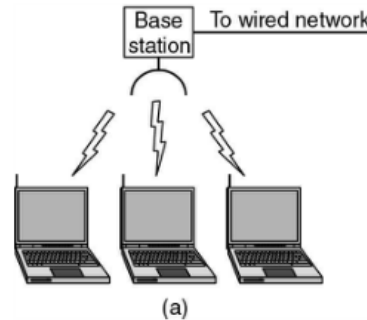
§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.5. 无线局域网协议

★ 无线LAN的两种模式

- 基站方式 (Infrastructure mode)
- 自组织方式 (Ad-hoc mode)

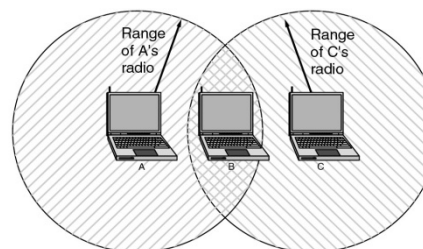
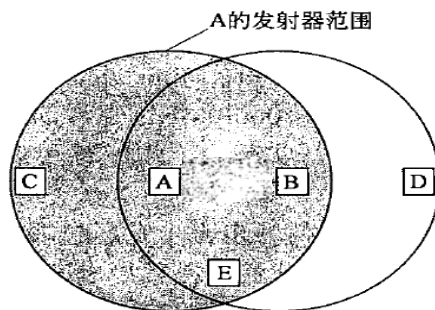


★ 无线LAN的基本特征

- 一个基站仅一个信道
- 目前带宽为11Mbps ~ 1.3Gbps
- 基站方式 (Infrastructure mode) 下，每个设备与一个接入点 (AP=Access Point) 关联，收发数据包都通过AP，设备相互不直接收发信息，因此只要保证每个设备与AP可通信即可
- 自组织方式 (Ad-hoc mode)，设备间直接收发信息，但一个站发送的信息无法保证所有站均能收到 (冲突与盲区的存在)

=> ad hoc 也称为多跳无线网络

=> 如果两站同时发送，则处于信号重叠部分的接收站会导致接收错误



§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.5. 无线局域网协议

★ 是否能在WLAN中使用CSMA

- 可能无法在发送方判断发出的数据是否有冲突 (接收信号弱)，只能采用确认机制

- 隐蔽站与暴露站问题

=> 在WLAN中，发送站应侦听接收站周围有无其它发送活动 (若其它发送站在该发送站范围外则无法实现)

=> 对于多个发送站，若各自的接收站不同，且各接收站彼此在接收范围之外，便可同时发送 (只影响两个发送站的信号重叠部分)

=> 通过CSMA，只能知道发送站周围是否有节点在发送，但真正影响此次通信的是接收节点周围是否有其它节点在发送

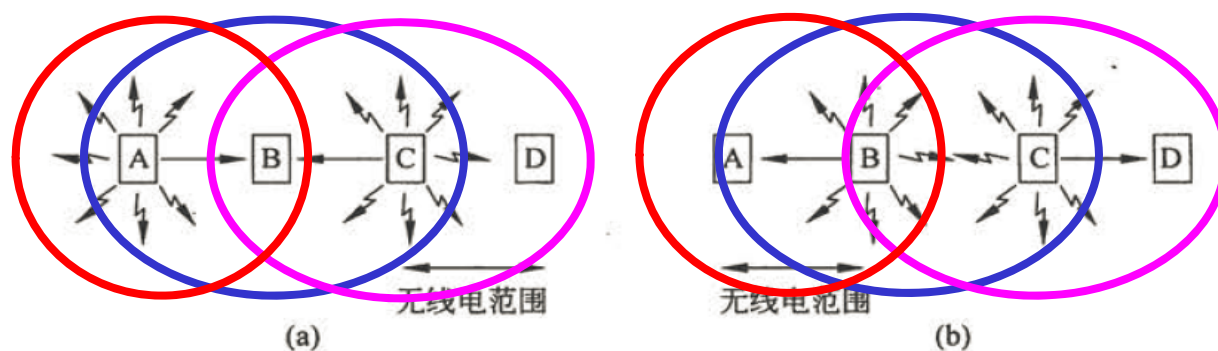


图 4-11 一个无线 LAN

(a) 在给 B 传输时 A 和 C 是隐藏终端；(b) 在给 A 和 D 传输时 B 和 C 是暴露终端

假设：A (红) 覆盖B，不覆盖C/D
B (蓝) 覆盖A/C，不覆盖D
C (粉) 覆盖B/D，不覆盖A

情况(1) A和C向B发送

=> 采用CSMA，

=> A/C互不覆盖，均认为可发送

=> B接收错误

隐蔽站问题

情况(2) B向A / C向D 同时发送

=> 采用CSMA

=> BC相互覆盖，均认为冲突

=> 不发送 (A/D不在BC的共同区域)

暴露站问题

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.5. 无线局域网协议

★ 冲突避免多路访问协议 (MACA = Multiple Access With Collision Avoidance)

- IEEE 802.11 无线LAN标准的基础

- 基本思想:

- (1) 发送方向接收方发送RTS(Request To Send)短帧, 包含了要发送帧的长度
- (2) 接收方若空闲/接收正确, 则向发送方回送CTS(Clear To Send)短帧, 同样包含要发送帧的长度
- (3) 发送方开始发送数据帧
- (4) 如果在预定时间内发送方未收到CTS, 则静默一段随机时间后再次重复(1)
- C** (5) 其它站若收到RTS, 则在一定时间内静默, 以保证发送站能收到CTS(静默时间超过CTS的返回时间即可), 之后可以向其它站(肯定与接收站互不干扰)发送信息
- D** (6) 其它站若收到CTS, 则在一定时间内静默, 直到数据发送完毕(静默时间由CTS中的帧长算出)
- E** (7) 其他站如果能先后收到RTS和CTS, 则直到数据帧发送完毕都应该保持静默
(静默时间=等待CTS返回时间+传输时间)

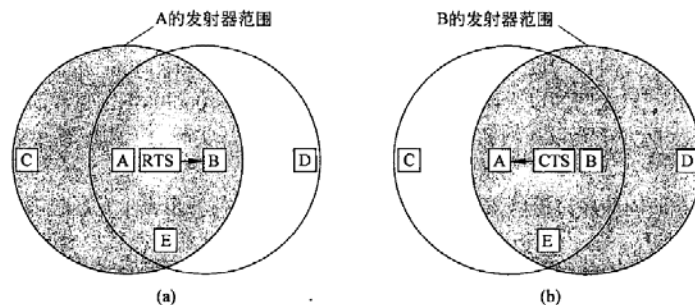


图 4-12 MACA 协议
(a) A 给 B 发送一个 RTS; (b) B 作为响应给 A 返回一个 CTS

§ 4. 介质访问控制子层

4.2. 多路访问协议

4.2.5. 无线局域网协议

★ MACAW对MACA的改进(MACA for Wireless)

- 接收站对成功收到的帧发ACK帧
- 发送站在发送RTS前，采用CSMA侦听，避免多个发送站同时向同一个接收站发送RTS
- 对每个数据流采用后退（backoff）算法
- 增加站间交换拥塞信息的机制

§ 4. 介质访问控制子层

4.3. 以太网

4.3.0. 概述

★ 以太网的发展及两个标准

- 1976年, Xerox Ethernet, 3Mbps速率
- 1978年, DIX Ethernet, 10Mbps速率 (DIX = DEC Intel Xerox)
- 1981年, DIX Ethernet V2, 是世界上第一个局域网产品 (以太网) 的标准
- 1983年, DIX Ethernet V2 => IEEE 802.3, DIX Ethernet V2 标准与IEEE 的802.3 标准只有很小的差别 (具体见后), 因此可将 802.3局域网简称为“以太网” (严格来说“以太网”应当是指符合 DIX Ethernet V2 标准的局域网)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.0. 概述

★ IEEE 802简介

- IEEE于1980年2月成立局域网标准化委员会，形成的一系列标准统称为IEEE 802标准
- IEEE 802标准于1984年3月被ISO采纳，作为局域网的国际标准，称为ISO 8802标准。
- IEEE 802标准主要涉及物理层、数据链路层、网络层的一部分；数据链路层又进一步分为介质访问控制（MAC）子层和逻辑链路控制（LLC）子层（LLC即802.2标准，已处于冬眠状态，基本不用，很多网卡都已不支持）

编号	主题
802.1	LAN概述与体系结构
802.2 ↓	逻辑链路控制
802.3 *	以太网 ←
802.4 ↓	令牌总线（主要被用在制造业）
802.5	令牌环（IBM的LAN技术）
802.6 ↓	双队列双总线（早期城域网）
802.7 ↓	宽带技术的技术咨询组
802.8 ↑	光纤技术的技术咨询组
802.9 ↓	同步LAN（实时应用）
802.10 ↓	虚拟LAN和安全
802.11 *	无线LAN（WiFi） ←
802.12 ↓	优先级需求（HP的AnyLAN）
802.13	不吉利的数字；没人愿意使用
802.14 ↓	线缆调制解调器（已消失：行业协会首先使用的）
802.15 *	个域网（蓝牙，Zigbee） ←
802.16 *	宽带无线（WiMAX） ←
802.17	弹性数据包环
802.18	无线电规范问题的技术咨询组
802.19	所有标准并存的技术咨询组
802.20	移动宽带无线（类似于802.16e）
802.21	介质独立切换（在不同技术间漫游）
802.22	无线区域网

书：第1章 P.63

图 1-38 802 工作组

最重要的用 * 标注；标注为 ↓ 的处于冬眠；标注 ↑ 的为放弃已经解散

§ 4. 介质访问控制子层

4.3. 以太网

4.3.0. 概述

★ 两种常用的以太网

- 共享式以太网(经典以太网): 采用广播通信方式, 所有用户共享一个信道, 但该信道每次只能在一对用户间进行通信, 因此每个用户的实际可用带宽随用户数的增加而递减, 且因为无法分割冲突域, 会因为碰撞冲突导致性能降低
- 交换式以太网: 节点通过交换机连接, 采用交换技术分割冲突域, 交换技术的作用便是根据所传递信息包的目的地地址, 将每一信息包独立地从发送端口送至目的端口, 避免了与其它端口发生碰撞, 提高了网络的实际吞吐量

★ 集线器(hub)与交换机(switch)

- 集线器: 把所有网络节点集中在以它为中心的节点上, 主要功能是对接收到的信号进行**整形再生放大**, 使被衰减的信号再生(恢复)到发送时的状态, 以扩大网络传输距离。集线器**工作于“物理层”**, 每个接口简单的收发比特并采用**广播式发送**向其它端口转发, 不进行碰撞检测, 不具备信号的定向传送能力
- 交换机: 为接入交换机的任意两个网络节点提供**独享**的电信号通路, 与其它节点不冲突。交换机**工作于“物理链路层”**(一般称为二层交换机, 此外还有工作于网络层的三层交换机), **拥有“智能记忆”和“学习”能力**, 除非两个源端口企图将信息同时发往同一目的端口, 否则各个源端口与各自的目的端口之间可同时进行通信而不发生冲突

§ 4. 介质访问控制子层

4.3. 以太网

4.3.1. 经典以太网物理层

★ 组网方式

名称	线缆类型	线缆最大长度限制	结点数量	拓扑结构
10Base-5	粗基带同轴电缆	500m	100	总线型
10Base-2	细基带同轴电缆	185m	30	总线型
10Base-T	3类双绞线+集线器	100m	1024	物理上星形逻辑上总线型
10Base-F	多模光纤	2000m	1024	星形

- 10Base-T是最流行的RJ-45+双绞线组合

★ 特性

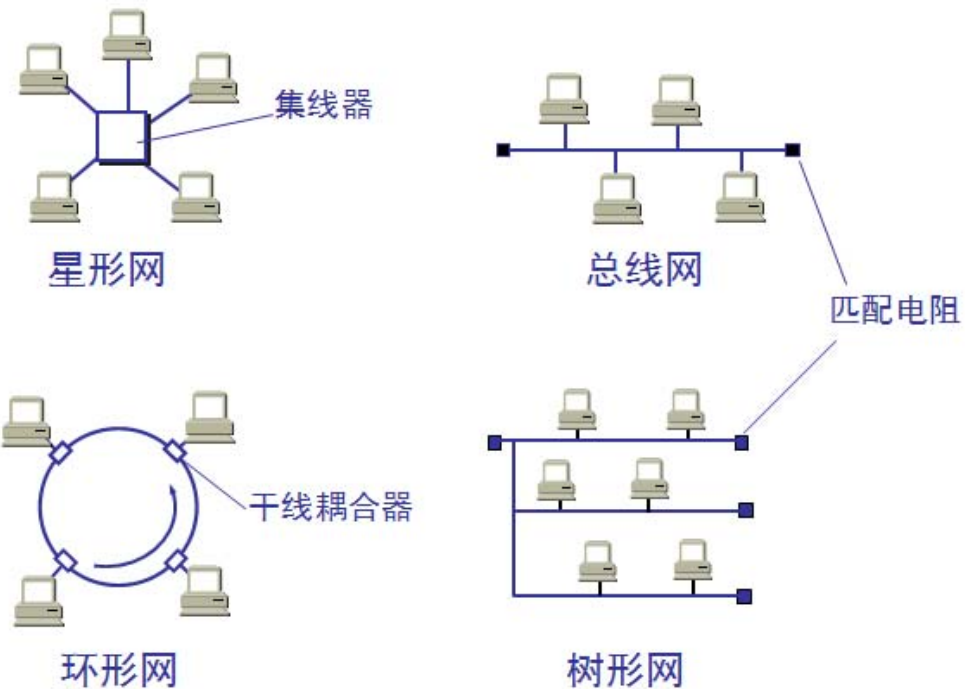
- 最大传输速率为10Mbps，半双工
- 编码方式为曼彻斯特编码
- 超出线缆最大长度则需要使用中继器 (repeater)，中继器用于将物理层信号放大，允许多个，但任意两结点间距离 $\leq 2500\text{m}$ ，中继器 ≤ 4 个
- 采用CSMA/CD解决多路访问的冲突
- 采用无连接工作方式，即不必先建立连接就可以直接发送数据
- 以太网对发送的数据帧不进行编号，提供的服务是不可靠的交付（即尽最大努力的交付）
- 当目的站收到有差错的数据帧时就丢弃此帧，其他什么也不做（差错的纠正由高层来做）
- 即使高层发现丢失数据而进行重传，以太网并不知道这是一个重传的帧，而是当作一个新的数据帧来发送，也不要求对方发回确认

§ 4. 介质访问控制子层

4.3. 以太网

4.3.1. 经典以太网物理层

★ 常见拓扑结构（除星形外，其它基本已淘汰）



★ 实际应用中已淘汰，但基本理论仍然延续了下来

§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 以太网的帧格式



图 4-14 帧格式

(a) 以太网 (DIX); (b) IEEE 802.3

- 前导码为8字节的10101010 (DIX)
7字节的10101010 + 10101011 (802.3)
- 802.3的 **10101011** 称为SOF (Start of Frame)
- 前导码是由曼彻斯特编码产生的10MHz方波发送，持续6.4us，作用是使接收方与发送方时钟同步，准备开始发送数据 (发送时由硬件自动填充)
- 校验和为4字节，采用CRC32 (发送时由硬件自动填充)
- 前导码/校验和在Wireshark等抓包工具中无法抓到，可捕获的以太网帧从目标地址到填充字节 (部分抓包工具还会自动去除填充字节)

1. 10Mbps的速率
=> 10MHz方波
=> 每个时钟周期传1bit
问: 为达到10M bps速率,
信号速率 (波特率)
要达到 20M baud,
为什么?

2. 10Mbps的速率
=> 每秒传输10000000bit
=> 每传输1bit需0.1us
=> 传输8字节 (64bit) 需
6.4us

§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 以太网的帧格式



图 4-14 帧格式

(a) 以太网 (DIX) ; (b) IEEE 802.3

- 目标地址和源地址均为6字节，称为MAC地址

- ◆ MAC地址也称为物理地址、硬件地址

- ◆ 常见表示方法为“E8-2A-EA-D7-88-72” / “E8:2A:EA:D7:88:72” / “E82A:EAD7:8872”

- ◆ 每一个网络适配器(网卡)均固定分配一个

- ◆ 前三个字节由IEEE分配给网络设备制造商，后三字节制造商内部分配，保证全球唯一，设备出厂前固化，不可改变(软件可模拟改)

- ◆ 从左到右依次编号为47 - 0，则 BBBB BB.XX.XX.XX.XX

第40bit位：0 - 单播地址 / 1 - 组播地址 (网卡MAC地址的最高字节必定偶数)

第41bit位：0 - 全局地址(IEEE分配) / 1 - 本地地址(自行分配)

48bit 全1 - 广播地址

- ◆ 源地址只能是单机地址，目的地址可以是单机/组播/广播地址

- ◆ 网卡的MAC地址虽然固定，但是仍可以监听到任何发送到它连接的网线上的数据，正常情况下网卡忽略目的地址非本机/组播/广播的数据包，不向上层传输；但可以将网卡设置为混杂模式(Promiscuous Mode)，此时则将所有收到的数据包均向上层传输

(Wireshark等抓包软件/路由器网卡均需此模式)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 以太网的帧格式



图 4-14 帧格式

(a) 以太网 (DIX); (b) IEEE 802.3

- 类型/Length字段为2字节，在 $\leq 0x0600$ 时，表示后面数据+填充的长度 ($0x0600=1536$)，否则表示帧的类型，**最常用的有两种**
 - 0x0800: IPv4
 - 0x0806: ARP, 完成IP地址到MAC地址的映射
- 数据+填充字段: 46-1500字节之间，如果数据的长度小于46，则需要填充字节(一般填0)来保证数据总长度 ≥ 46 (**以太网帧总长度 ≥ 60 ，不含CRC**)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 以太网的帧格式

● 问题：为什么要限制帧的最小长度？

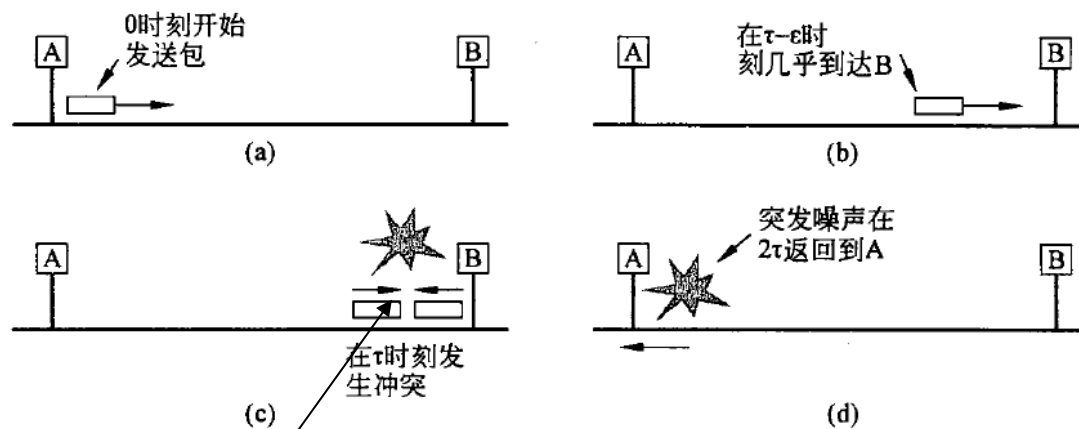


图 4-15 冲突检测只需要 2τ 时间

B检测到发生冲突后
发送48bit突发噪声
来阻塞以太网

在两站最长距离2500m,
有4个中继器的最差情况

=> 来回时延 $2\tau = 50\mu s$

(实验数据)

=> 最短帧要保证在 $50\mu s$
内不能发送完成

速率为10Mbps

=> 传输1bit需要 $0.1\mu s$

=> 最短帧至少500bit

=> 加安全余量 = 512bit
(64字节)

=> 去CRC后最短帧60字节

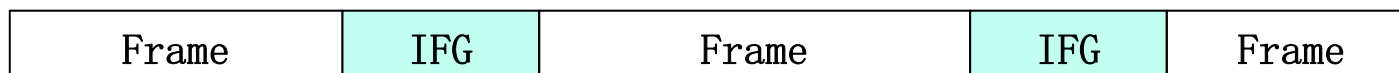
§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 以太网的帧间距 (IFG = Interframe Gap)

- 以太网的发送以帧方式进行，每帧长度不等，因此两帧之间要有间隙，网络设备在接收一帧后，需要一段时间来恢复并为接收下一帧做准备



- IFG是时间，不是距离，最小值为96个bit时间 (10Mbps下就是9.6us，不同速率下不同)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.2. 经典以太网的MAC子层协议

★ 二进制指数后退的CSMA/CD

- 1) 发送站的适配器从网络层获取一个数据报，构造Ethernet帧，存入适配器缓存
 - 2) 适配器采用1-坚持CSMA/CD算法监听信道，发现空闲时间超过96bit时间则开始发送
 - 3) 在发送过程中，适配器监视来自其它适配器的信号能量。若传输完成且无其它适配器信号能量则完成该帧传输；如在传输过程中发现其它适配器信号能量，则中止传输(冲突发生)，改为发送48bit的阻塞信号
 - 4) 第1次冲突发生后，令 $i=1$ ，等待 $0 \sim 2^{i-1}$ 个时间槽(因为最短帧512bit，对应发送时间为51.2us，因此时间槽的划分也是51.2us)后发送站的适配器再次重复(2)
 - 5) 以后每发生一次冲突，则 i 加倍，等待 $0 \sim 2^i-1$ 个时间槽后发送站的适配器再次重试
 - 6) 若 $10 < i \leq 16$ ，则最大时隙固定为 $2^{10}-1 = 1023$ ，若 $i > 16$ 仍冲突，则向上层报告出错
- 少量站发生冲突，则可保证较低的延迟
 - 大量站发生冲突，则降低冲突再次发生的概率
 - 最大时间槽1023则避免了延迟增长太大
 - 超时16次则报错避免了陷于无限循环中

§ 4. 介质访问控制子层

例：站点A和B同在一个10Mbps的以太网上。两个站点间传播时延为225bit时间。现假定A开始发送最短帧，并且在A发送结束之前B也发送一帧

问：(1) A在检测到和B发生碰撞前能否把自己的数据发送完毕？

(2) 若A在发送完毕之前并没有检测到碰撞，那么能否肯定A所发送的帧不会和B所发送的帧发生碰撞？

答： 设 $t=0$ 时A开始发送，

=> 在 $t=(64+8)*8=576\text{bit}$ 时间后发送完毕

=> 在 $t=225\text{bit}$ 时间，B就检测出A的信号

=> B在 $t=224\text{bit}$ 时间之前发送数据，则A在发送完毕前($t \leq 449\text{bit}$ 时间)一定检测到碰撞

=> 检测到碰撞前A不能发送完 (问题1)

=> B在 $t=225\text{bit}$ 之后不会发送数据

=> 若A在发送完毕之前并没有检测到碰撞

=> 肯定A所发送的帧不会和B发送的帧发生碰撞 (问题2)

§ 4. 介质访问控制子层

例：同上例条件(AB相距225bit时间)，假设站点A和B在 $t=0$ 时同时发送了数据帧。则当 $t=225\text{bit}$ 时间时，AB同时检测到碰撞，并且在 $t=225+48=273\text{bit}$ 时间完成了干扰信号的传输。现在AB在CSMA/CD算法中选择不同的 r 值退避，假定 $r_A=0$ 和 $r_B=1$

- 问：(1) A和B各在什么时间开始重传其数据帧？
(2) A重传的数据帧在什么时间到达B？
(3) A重传的数据帧会不会和B重传的数据再次发生碰撞？
(4) B会不会在预定的重传时间停止发送数据？

答： $t=0$ 时，A和B开始发送数据

$t_1=225\text{bit}$ 时间，A和B都检测到碰撞

$t_2=273\text{bit}$ 时间，A和B结束干扰信号的传输(也收完)

$\Rightarrow r_A=0$ ，A在273bit时间立即再次检测信道，

\Rightarrow 在 $273 + 225 = 498\text{bit}$ 时间信道开始空闲

\Rightarrow 再过 96 bit时间 ($498+96=594\text{bit}$ 时间)后A开始重传(问题1)

\Rightarrow A的重传数据在 $594+225=819\text{bit}$ 时间到达B(问题2)

$\Rightarrow r_B=1$ ，B在 $273+1*512=785\text{bit}$ 时间再次检测信道

\Rightarrow 若785bit时间信道空闲

\Rightarrow 在 $785+96=881\text{bit}$ 时间B开始再次传输(问题1)，否则再退避

\Rightarrow A的重传数据在819bit时间到达B， $819 \leq 881$ ，应再次退避(问题3)

\Rightarrow B在预定时间会再次停止(问题4)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.3. 以太网性能

★ 平均竞争时隙

在稳定重负荷条件下，有k个待发站，假定每个时隙内重传概率为一常数；若每个站在竞争时隙内发送的概率为p，则在该时隙内某站获得信道的概率A为

$$A = kp(1-p)^{k-1}$$

=> 当 $p=1/k$ 时，A有最大值，当 $k \rightarrow \infty$ 时， $A=1/e$ 。

=> 竞争时间为j个时隙的概率为 $A(1-A)^{j-1}$

=> 每次竞争的平均时隙数
$$\sum_{j=0}^{\infty} jA(1-A)^{j-1} = A \cdot \frac{1}{[1-(1-A)]^2} = \frac{1}{A}$$

=> 每个时隙持续时间 2τ

=> 平均竞争时间 $w = \frac{2\tau}{A}$

=> 假定最佳概率为p，即竞争时隙的平均值永小于e，

所以w最大为 $2\tau e \approx 5.4\tau$

§ 4. 介质访问控制子层

4.3. 以太网

4.3.3. 以太网性能

★ 信道效率

若每帧发送时间为P秒，当有多个待发站时，则 信道效率 = $\frac{P}{P + \frac{2\tau}{A}}$

设：帧长F，带宽B，电缆长度L，信号传播速率C，
每帧有e个竞争时隙时，则 信道效率 = $\frac{\frac{F}{B}}{\frac{F}{B} + \frac{2(L/C)}{1/e}} = \frac{1}{1 + 2BLE/(CF)}$

- 经典以太网适合在轻负载下工作，一般而言，信道利用率超过30%就认为是重负载了

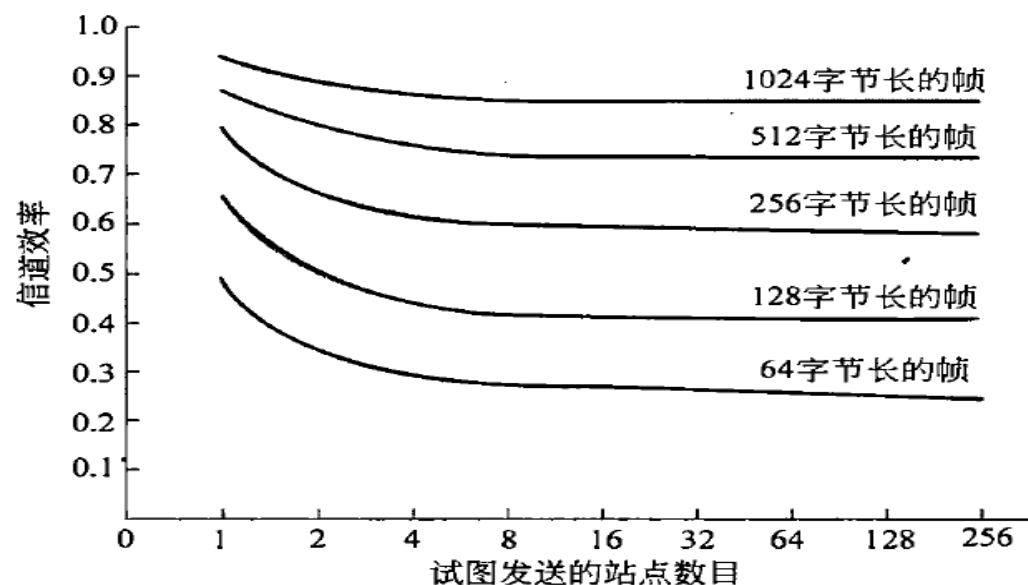


图 4-16 具有 512 位时间槽的 10Mbps 以太网效率

§ 4. 介质访问控制子层

4.3. 以太网

4.3.4. 交换式以太网

★ 共享式以太网的问题

- 在N个节点的系统中，每个节点平均只能获得总带宽的 $1/N$
- 当N较大时，由于冲突增加，导致网络性能下降

★ 解决网络规模与网络性能之间矛盾的几种方法

- 提高网络速度：不能从根本上解决冲突增加问题
- 网络分段：增加设备代价，管理困难
- 交换技术：将冲突域中的节点数减少到一个，避免冲突的发生

(从根本上改变了共享式以太网的结构)

★ 集线器与交换机 (概念4.3.0已介绍)

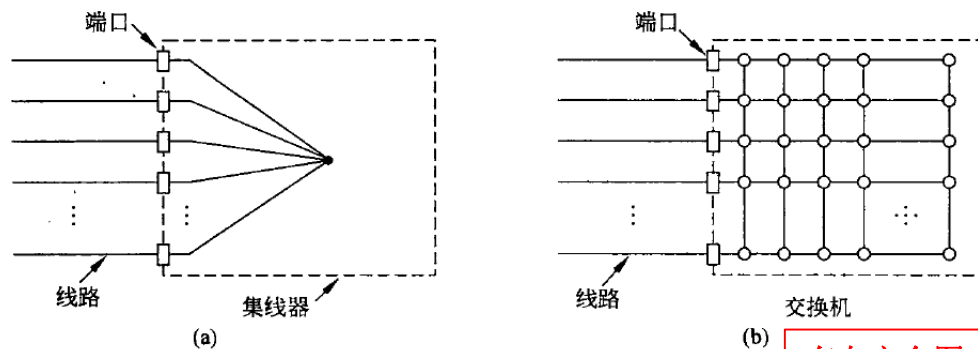


图 4-17
(a) 集线器; (b) 交换机

有向完全图
更容易理解

- 集线器与交换机工作原理的具体差别见4.8

§ 4. 介质访问控制子层

4.3. 以太网

4.3.4. 交换式以太网

★ 交换式以太网的基本概念

- 交换机是交换式以太网的核心，由一个高速交换背板和若干端口组成，每个端口可连接一台主机或另一台交换机/集线器
- 如果交换式以太网和集线器一起组网，则通过集线器的部分仍然要使用CSMA/CD算法，只能用**半双工**的方式实现**有碰撞**的数据传输
- 交换式以太网将“共享”变为“独享”，交换机为每个端口提供专用的带宽，连接在两个端口上的一对主机独占一对信道，因此可以进行**全双工**的**无碰撞**数据传输，网络的总带宽为各个交换端口带宽之和
- 数据帧通过背板在不同端口间交换，每个端口有一个输入缓存，可以将输入的帧排入队列，直到被传输到输出端口，随着用户(端口)的增多，网络总带宽不断增加，但即使网络负载很重也不会导致网络性能下降，因此从**根本上解决**了网络规模与网络性能的矛盾问题
- 交换式以太网不再使用CSMA/CD协议，理论上说，不再需要限制帧的最小长度；但为了向后兼容，帧的最小长度仍为64字节(**协议软件不需要做任何改动**)
- 由于交换式以太网不再使用CSMA/CD协议，传输介质的长度只和信号强度及介质传输能力有关，与信号的最大往返时间无关
- 交换机的定向转发机制具体见 4.8

§ 4. 介质访问控制子层

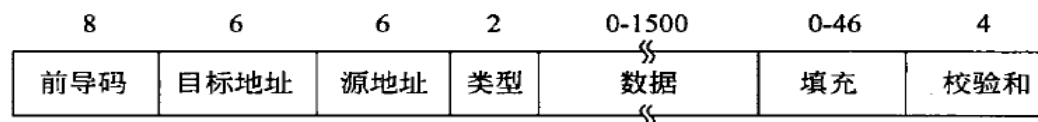
4.3. 以太网

4.3.4. 交换式以太网

★ 交换式以太网的流量控制

- 当出现多个端口向同一个端口发送数据等情况时，需要采用流量控制机制来保证不丢弃帧，流量控制可以有效的防止由于网络中瞬间的大量数据对网络带来的冲击，保证网络高效而稳定的运行
- 在半双工方式下通过反向压力（backpressure），即我们通常说的背压计数实现的，这种计数是通过向发送源发送干扰信号（人为制造干扰）或者使用载波“延期”机制（发送先导符，好像信道忙）使得信息源降低发送速度
- 在全双工方式不使用CSMA/CD，因此不判断干扰，因此采用IEEE 802.3x标准，由交换机向信息源发送“PAUSE”帧令其暂停发送

● “PAUSE”帧的格式



目的地址：专用组播地址（01-80-c2-00-00-01）

类型：0x8808

数据：0x0001 + 2字节停止时间（单位是当前传输速率传512bit的时间）

填充：42字节

● “PAUSE”帧的工作原理（实现流控的简单“停启”）

当一设备希望暂停进入帧时，发送带有时间范围的PAUSE帧。收到PAUSE帧的设备在给定时间内暂停发送数据帧。暂停周期结束后恢复发送

可以发送零时间的PAUSE帧中止暂停周期，或发送非零时间帧延长暂停周期

§ 4. 介质访问控制子层

4.3. 以太网

4.3.5. 快速以太网

★ 定义了三种新的物理层标准（组网方案）

名称	线缆	最大长度	优点
100Base-T4	双绞线	100 米	可用3类UTP 基本已淘汰
100Base-TX	双绞线	100 米	全双工速率100 Mbps(5类UTP)
100Base-FX	光纤	2000 米	全双工速率100 Mbps, 距离长

图 4-19 最初的快速以太网线缆

- 100Base-T4: 四对3类双绞线，一对发送，一对接收，另两对可以收发切换，保持发送方有3对线同时发送，使用25MHz 的信令速度，用三种电压传送三元数字，将三对双绞线视为一体，则信号状态共有27种，每种状态携带4比特数据

{ 发送方向: $25\text{M Baud} \times 4 = 100\text{Mbps}$ (三对)
接收方向: $100\text{Mbps} \times 1/3 = 33.3\text{M bps}$ (一对)

(使用四对3类双绞线，半双工100MB，基本淘汰)

- 100Base-TX: 每对双绞线使用125 MHz的信令速度，在不超过100米的距离内，采用4B/5B编码可获得100Mbps的数据速率

{ 发送方向: $125\text{M Baud} \times 4/5 = 100\text{Mbps}$
接收方向: $125\text{M Baud} \times 4/5 = 100\text{Mbps}$

(使用两对5类双绞线，全双工100MB)

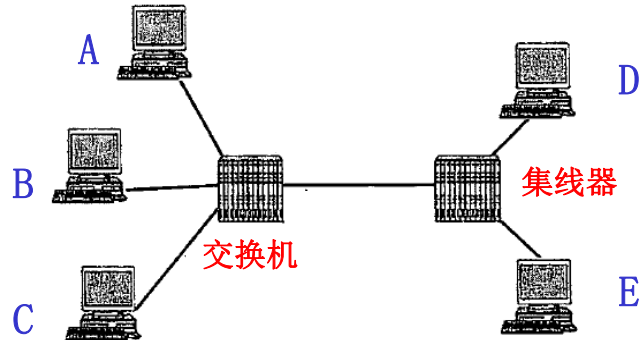
- 100Base-FX: 两条多模光纤分别用于发送/接收，采用4B/5B编码，每条光纤均提供100Mbps的数据速率(使用两条MMF光纤，全双工100M)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.5. 快速以太网

- ★ 标准为802.3u，除了数据速率提高到100Mbps以外，完全保留了802.3的MAC层(帧格式、接口及处理规程) => 64bit的前导码、96bit时间的帧间距等均相同只是发送1bit的时间更快
- ★ 物理层上只使用集线器和交换机进行组网，且传输介质只使用双绞线和光纤
- ★ 100BaseFx只能连接交换机，100Base-T4/Tx则允许连接集线器或交换机
 - 如果使用集线器，则通过集线器的部分仍然要使用CSMA/CD算法，为了保持最小帧长与最大线缆长度的关系(经典以太网是64字节/2500米)，在保持最小帧长64字节不变的情况下，选择降低最大线缆长度(一般 ≤ 100 米)



A/B/C \leftrightarrow A/B/C 之间: 全双工, 不使用CSMA/CD
D \leftrightarrow E 之间: 半双工, 使用CSMA/CD
A/B/C \leftrightarrow D/E 之间: 半双工, 使用CSMA/CD

- 为保持向后兼容，快速以太网提供自动协商机制，允许两站自动协商速度(100MB/10MB)和工作模式(全/半双工)
 - => 两台主机通过集线器，可10/100MB，只能半双工
 - => 两台主机通过交换机，可10/100MB，可以全双工

§ 4. 介质访问控制子层

4.3. 以太网

4.3.6. 千兆以太网

- ★ 标准是802.3z/802.3ab，除数据速率提高到1Gbps以外，仍与已有的以太网标准相兼容，包括帧格式、最小和最大帧长限制等
- ★ 支持两种不同的操作模式
 - 全双工模式：不采用CSMA/CD机制，交换机到计算机之间的传输距离取决于信号强度
 - 半双工模式：采用CSMA/CD机制，交换机到计算机间的最大传输距离为25m (2500m/100=25m)

问：如何扩充25m的最大传输距离 (一般可达到 $\leq 200\text{m}$)

答：方法一：波扩展，链路层上仍使用64字节的最小帧长，由发送硬件在发送时填充至512字节，接收硬件会自动去除

方法二：帧突发传输，发送端可将多个帧放在一起一次发送出去 (若合并后长度小于512则继续填充，应优于方法一)

- ★ 可以连接集线器或交换机，仍支持自动协商机制 (10/100/1000Mbps，全/半双工)
- ★ 千兆以太网引入了巨型帧 (>1500)，但不能向后兼容，即只有纯千兆以太网才可能支持 (还需要厂家的设备支持)

§ 4. 介质访问控制子层

4.3. 以太网

4.3.6. 千兆以太网

★ 有以下几种组网方式 (P. 228图有错, 4对UTP)

名称	线缆	最大长度	优点
1000Base-SX	光纤	550 米	多模光纤(50、62.5 微米)
1000Base-LX	光纤	5000 米	单模光纤(10 微米)或多模光纤(50、62.5微米)
1000Base-CX	2对STP	25 米	屏蔽双绞线
1000Base-T	2对UTP	100 米	标准5类UTP

- 1000Base-SX/LX: 以激光作为光源, 激光的波长有 $0.85\mu\text{m}$ (多模光纤)和 $1.3\mu\text{m}$ (单模光纤)两种; 光纤有 $10\mu\text{m}$ (单模)和 $50\mu\text{m}/62.5\mu\text{m}$ (多模)两种, 传输距离可以达到5公里甚至更长; 采用125M Baud信号, 使用8B/10B编码, 传输速率 $1250\text{M} \times 8/10 = 1000\text{Mbps}$
- 1000Base-CX: 由于距离太近, 很少使用
- 1000Base-T: 使用4对5类双绞线, 最大长度100米, 每对运行在125MBaud, 采用PAM5编码, 5个电平等级, 其中四种电平用于编码数据, 一种电平用于控制, 因此每个信号携带2比特数据, 4对双绞线总共获得的数据速率 $= 2 \times 4 \times 125\text{M} = 1000\text{Mbps}$, 每对双绞线都可以双向传输, 因此可全双工地获得 1000Mbps 数据速率

§ 4. 介质访问控制子层

4.3. 以太网

4.3.7. 万兆以太网

- ★ 标准是802.3ae，除数据速率提高到10Gbps以外，仍与已有的以太网标准相兼容，包括帧格式、最小和最大帧长限制等
- ★ 10Gbps以太网只工作在全双工方式，不允许连接集线器，因此没有争用问题，也不使用CSMA/CD协议
- ★ 目前新的40Gbps/100Gbps的以太网已经投入使用，这些超高速以太网统称为**电信级以太网**
(家用无意义)

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 0. 无线局域网的基本概念

- ★ 通信双方通过无线方式进行通信，通信之前需要建立连接(有线网络不需要)
- ★ 通信方式是半双工(有线网络可以是全双工)
- ★ 通信时在网络层以下出错的概率非常高，所以帧的重传概率很大，需要在网络层之下的协议添加重传的机制，而不能只依赖上层TCP/IP的延时等待重传等机制(有线网络出错概率非常小，下层无需此机制)
- ★ 数据在无线环境下传输，非常容易被抓包，存在安全隐患
- ★ 收发无线信号的功耗较大，吞吐量低(相对有线网络)
- ★ 频率范围(Band)：指无线信号使用的频率范围段，WLAN一般是5GHz / 2.4GHz(公共频段)
(非公共频段需要申请才能获得)
- ★ 信道(Channel)：对频段的进一步划分，将频段范围再划分为几个小的频段，每个频段称作一个信道，处于相同传输信道上面的数据，如果信道覆盖范围没有重叠，那么不会相互干扰
- ★ 信道宽度(Channel Width)：每个信道的带宽

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 0. 无线局域网的基本概念

★ 无线网络的安全性(Wireless Security)

- ┌ WEP (Wired Equivalent Privacy): 采用RC4算法
- ├ WPA (Wi-Fi Protected Access): 采用TKIP算法
- └ WPA2(WPA V2): 采用CCMP算法

- WEP只支持802.11b/g模式，802.11n后不再支持，如果设置WEP方式，则路由器性能会降低
- 实用中，CCMP在某些路由器会表示为AES等
- WPA2+AES是安全性最强的
- 某些路由器中WPA-PSK/WPA2-PSK(pre share key)，表示不使用专门的验证服务器(家用/SOH0)
- 使用中，某些路由器可能没有严格按照这些约定来设置(例：WPA方式，选择AES)

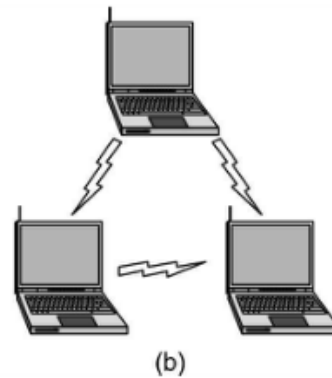
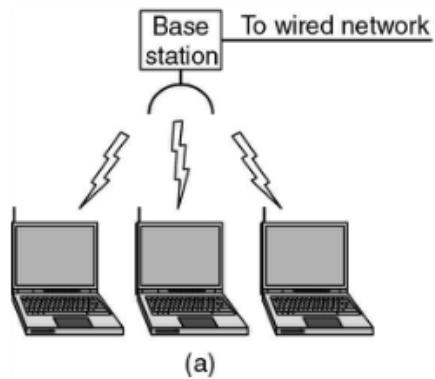
§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 1. 802. 11 体系结构和协议栈

★ 两种模式 (4. 2. 5讲过)

- 基站方式 (Infrastructure mode)
- 自组织方式 (Ad-hoc mode)



§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 1. 802. 11 体系结构和协议栈

★ 基站方式

- 一个AP和连接到其上的若干个移动站构成一个基本服务集 BSS (Basic Service Set)
- AP的标识符称为SSID(Service Set Identification)一般由字母+数字+符号形式组成, 方便人的识别, BSS的标识符称为BSSID, 其格式和MAC地址一样, 是48位的地址格式 (通常用AP的MAC地址表示)

(SSID - 人 BSSID - 机器)

- AP周期性发送信标 (beacon), 含SSID+MAC地址, 移动站与其中一个AP建立关联 (associate)
- 移动站如果希望连接到AP, 首先必须发现AP, 发现方式有被动扫描 (passive scan) 和主动扫描 (active scan), 被动方式是监听AP周期性发出的信标 (beacon), 主动方式是移动站主动发出探查请求帧 (Probe Response)

(若移动站采用主动扫描, 则可以隐藏AP的SSID)

- 移动站可同时收到多个AP信号, 称为Wi-Fi丛林, 不同AP在信号重叠范围内使用相同频率信号则会产生干扰, 因此每个AP都支持多个频率的信道, 移动站与AP连接时自动协商信道
- 移动站如果发现多个AP具有相同的SSID, 则会根据信号强度和质量自动选择最佳的AP连接, 而且在移动过程中会支持在多个相同SSID间漫游

(一个AP也可以有多个不同的SSID, 方便不同性质的用户接入)

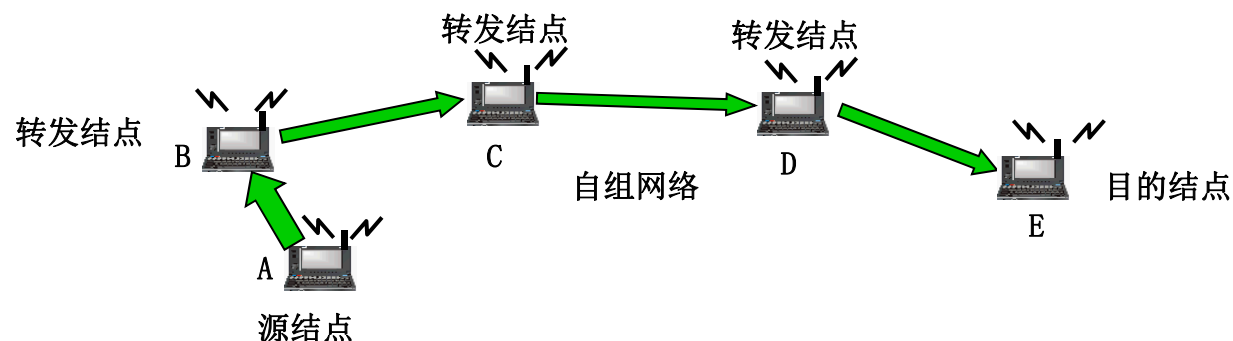
§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 1. 802. 11 体系结构和协议栈

★ 自组织方式

- 处于同一个Ad hoc下的多个移动站也构成一个基本服务集 BSS (Basic Service Set)
- 如果两个移动站的信号无法直接覆盖，则通过其他移动站转发(基站方式只能由AP转发)



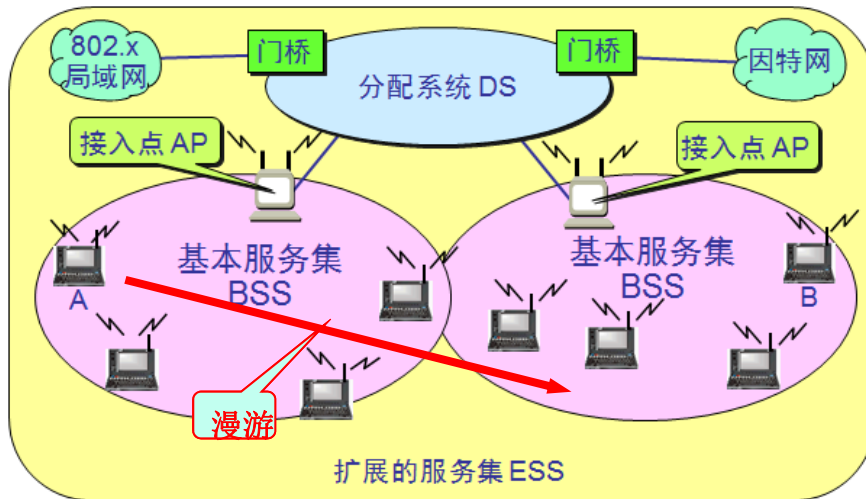
- 在军事领域中，Ad hoc适合在战场上快速建立移动自组网络并进行通信
- 当出现自然灾害时，在抢险救灾时利用移动自组网络进行及时的通信往往很有效的

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 1. 802. 11 体系结构和协议栈

★ 有固定设施的无线局域网的拓扑结构 (补: 校园网)



- 一个BSS可以是孤立的，也可通过AP连接到主干分配系统 DS (Distribution System)，然后再接入到另一个BSS，构成扩展的服务集ESS (Extended Service Set)
- ESS 还可通过门桥(portal)为无线用户提供到非 802.11 无线局域网（例如，到有线连接的因特网）的接入
- 移动站 A 从某一个BSS漫游到另一个BSS，仍然可保持与另一个移动站 B 进行通信。

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 1. 802. 11 体系结构和协议栈

★ 802. 11协议栈

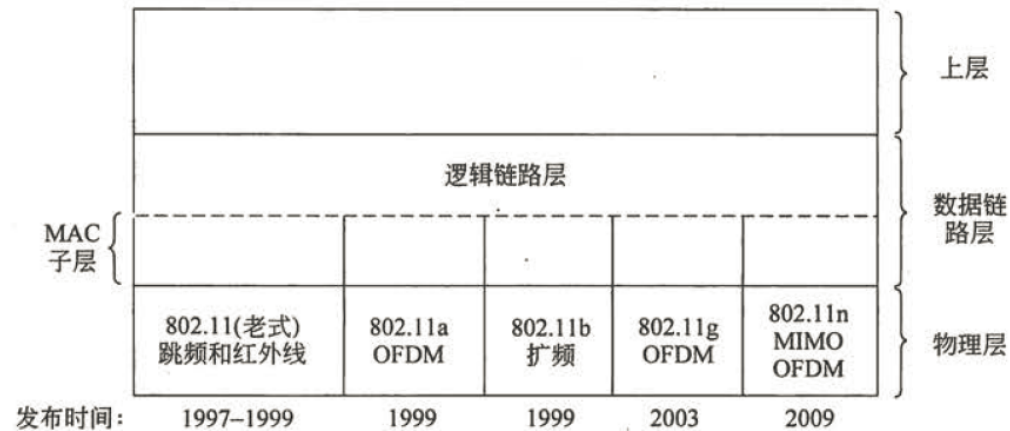


图 4-24 802.11 协议栈的组成部分 2012 802.11ac

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 2. 802. 11 物理层

★ 802. 11(老式)跳频和红外线

- 802. 11 infrared: 红外通信, 1 Mbps和2 Mbps 两种速率。优点是各个房间的通信系统互不干扰, 缺点是带宽太低
- 802. 11 FHSS: 跳频扩频, 工作在2. 4GHz频带, 1 Mbps和2 Mbps两种速率。优点是安全性好, 抗干扰强, 常用于建筑物之间的通信, 缺点是带宽太低
- 802. 11 DSSS: 直序扩频, 1Mbps和2Mbps两种速率

★ 802. 11a: 采用OFDM(正交频分多路复用), 工作于5GHz频带, 最高速率54Mbps。优点是抗窄带干扰强, 并能够使用非连续信道

★ 802. 11b: 采用 HR-DSSS(高速直序扩频), 工作于2. 4GHz频带, 有1, 2, 5. 5和11Mbps四种速率, 通信范围是802. 11a 的7倍

★ 802. 11g: 采用OFDM, 工作在2. 4GHz频带, 理论上可以达到54Mbps

★ 802. 11n: 采用MIMO(Multiple Input Multiple Output) + OFDM技术, 工作在2. 4GHz和5GHz两个频段, 理论速度600Mbps

(实际中某些产品因为成本问题只有2. 4G)

★ 802. 11ac: 在802. 11n的基础上采用更宽的带宽, 更多的MIMO空间流以及更高阶的调制, 工作在5GHz频段, 理论速度>1Gbps (6. 9G)

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 3. 802. 11 MAC子层协议

★ 带有冲突避免的CSMA协议

(CSMA/CA = CSMA with Collision Avoidance)-无线

(CSMA/CD = CSMA with Collision Detection)-有线

- CSMA/CD通过电缆中电压的变化来检测碰撞，当数据发生碰撞时，电缆中的电压就会随着发生变化
- CSMA/CA采取了三种检测信道空闲的方式
 - 能量检测(ED)：接收端对接收到的信号进行能量大小的判断，当功率大于某一确定值时，表示有用户在占用信道，否则信道为空
 - 载波检测(CS)：接收端将接收到的信号与本机的伪随机码(PN码)进行运算比较，如果其值超过某一极限，表示有用户在占用信道，否则认为信道为空
 - 能量载波混台检测：两者结合

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 3. 802. 11 MAC子层协议

★ 带有冲突避免的CSMA协议

- 1) 有帧待发送时，监听到信道空闲，则等待一个DIFS（分布式帧间隔）时间后发送该帧
 - 2) 否则，选一随机回退计数值，在监听到信道空闲时递减该值，在信道忙时该值不变
 - 3) 当计数值为0，则发送整个帧，等待确认；接收方接收成功后，在短帧间隔（SIFS）发送确认帧
 - 4) 收到确认，还有另一帧，则从第2步开始，若未收到确认，则从第2步回退阶段选择更大范围随机回退值
- 发送方无法检测冲突，因此一旦发送就要完成
 - 利用确认帧来检测冲突

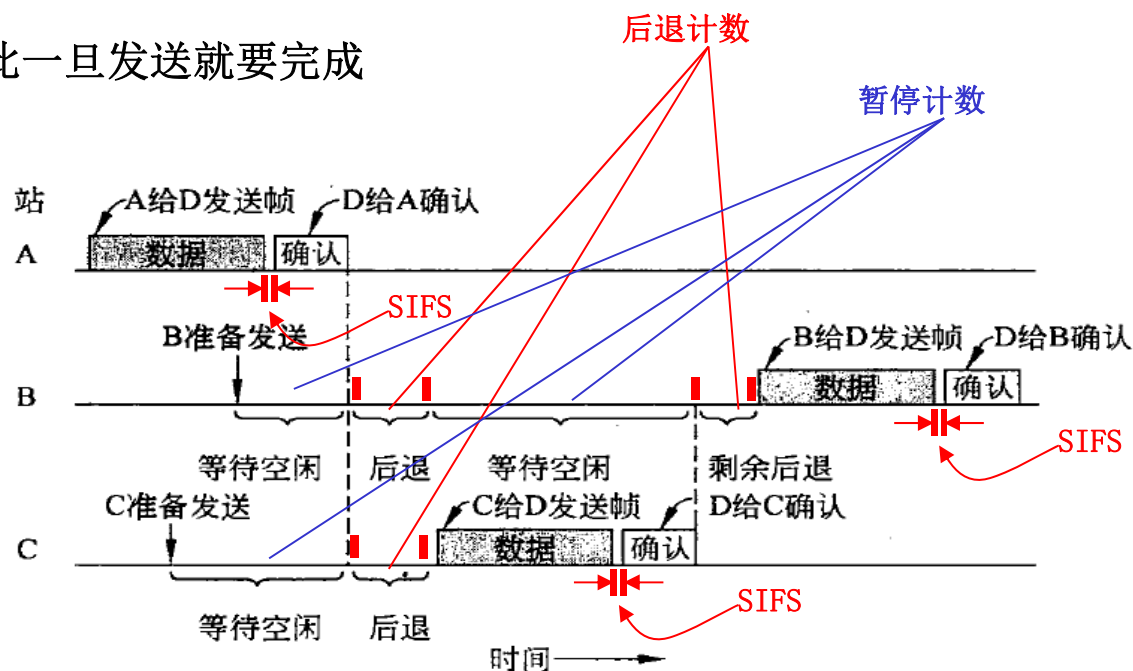


图 4-25 在 CSMA/CA 机制下发送帧

§ 4. 介质访问控制子层

4.4. 无线局域网

4.4.3. 802.11 MAC子层协议

★ 分布式协调功能（DCF）与点协调功能（PCF）

● DCF (Distributed Coordination Function)

所有节点(包括AP)使用CSMA/CA协议竞争信道，适用于基站和自组织两种方式（必须支持）

● PCF (Point Coordination Function)

只能用于基站方式，由AP控制覆盖范围内的所有通信活动（可选功能）

- ◆ 轮询：基站依次询问单元中的节点，被询问到的节点可发送它的帧，不会有冲突发生
- ◆ 新节点注册：新加入节点可注册一个恒定速率的轮询服务，声明自己希望得到的带宽
- ◆ 电源管理：基站可以指示某些节点进入睡眠状态，当有数据发给这些节点时唤醒它们

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 3. 802. 11 MAC子层协议

★ CSMA/CA支持两种机制

- 无信道预约的机制 (无法解决隐藏站/暴露站问题)
- 信道预约机制: 基于MACAW并使用虚信道侦听, 在发送RTS和CTS帧时携带要发送数据的长度, 第三方侦听到后, 更新自己的网络分配向量

(NAV = Network Allocation Vector, NAV指出了必须经过多少时间才能完成数据帧的传输并使信道转入空闲状态), 通过NAV可知道虚信道忙 (不管此时实际信道能否被侦听、是否忙), 从而避免冲突

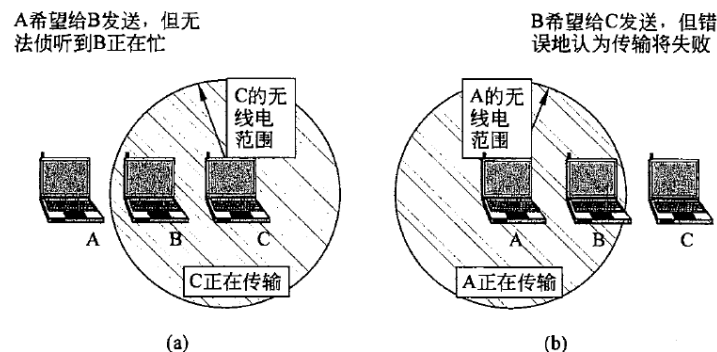


图 4-26
(a) 隐藏终端问题; (b) 暴露终端问题

例: A向B发送数据, 信号相互覆盖关系如下图

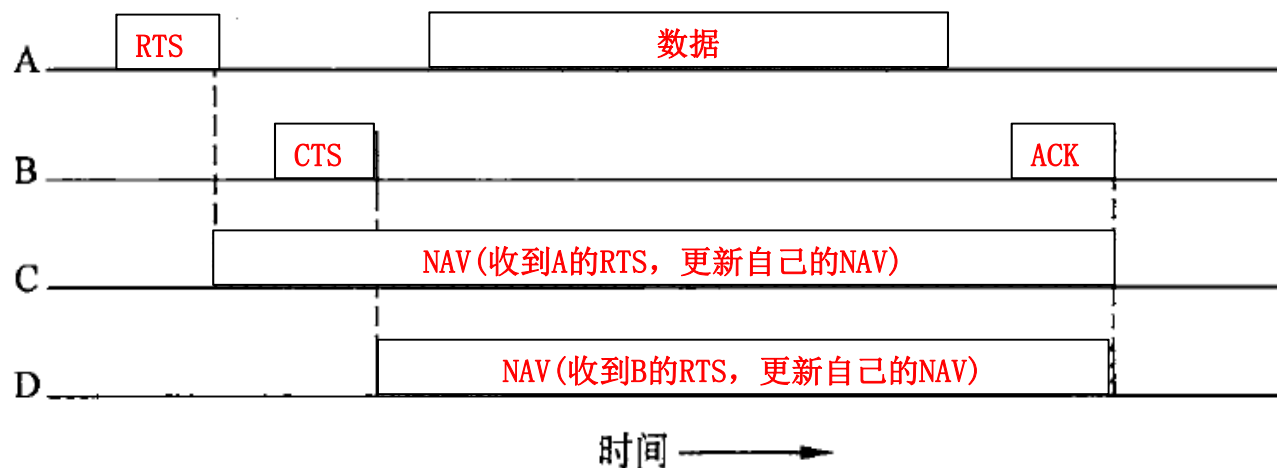
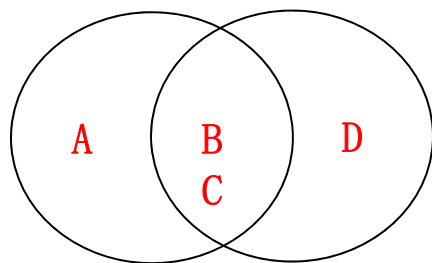


图 4-27 使用 CSMA/CA 的虚拟信道侦听

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 3. 802. 11 MAC子层协议

★ 为提高传输成功率所做的改进 - 短帧

- 假设任何一位传输出错的概率为 p ，帧长为 n 位，则整帧被正确接受概率为 $(1-p)^n$
 - => 无线 $p=10^{-4}$ ，以太网帧： $1518*8=12144$ bit
 - => 被完整接收的概率 = 29.69 %
 - => 一帧分解为三帧（帧长=4048 bit）
 - => 被完整接收的概率 = 66.71 %
 - 802. 11允许发送站将帧分成较小的段传输以减小出错重发的通信量
 - 每个段单独编号，采用停-等协议传输
 - 节点在获取信道后可以连续地将一个帧的所有段全部发完

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 3. 802. 11 MAC子层协议

★ 802. 11的帧间间隔

- 最短帧间隔（SIFS）：在SIFS之后，允许简单对话，包括接收方发送CTS响应RTS，对帧分段或全数据帧的ACK，允许发送站在无需重发RTS条件下分段集中发送
- PCF帧间隔（PIFS）：在PIFS之后，基站发送信标帧，进行轮询各站（选）
- DCF帧间隔（DISF）：在DCF之后，移动站可试图获得信道。此时用争用原则和二进制指数退避算法解决争用发生
- 仲裁帧间隔（AIFS）：用于控制不同优先级帧的发送间隔(语音：高 背景：低)，高优先级比DISF短，低优先级比DISF长
- 扩展帧间隔（EISF）：在EISF之后仅用于发现坏帧和不认识的帧

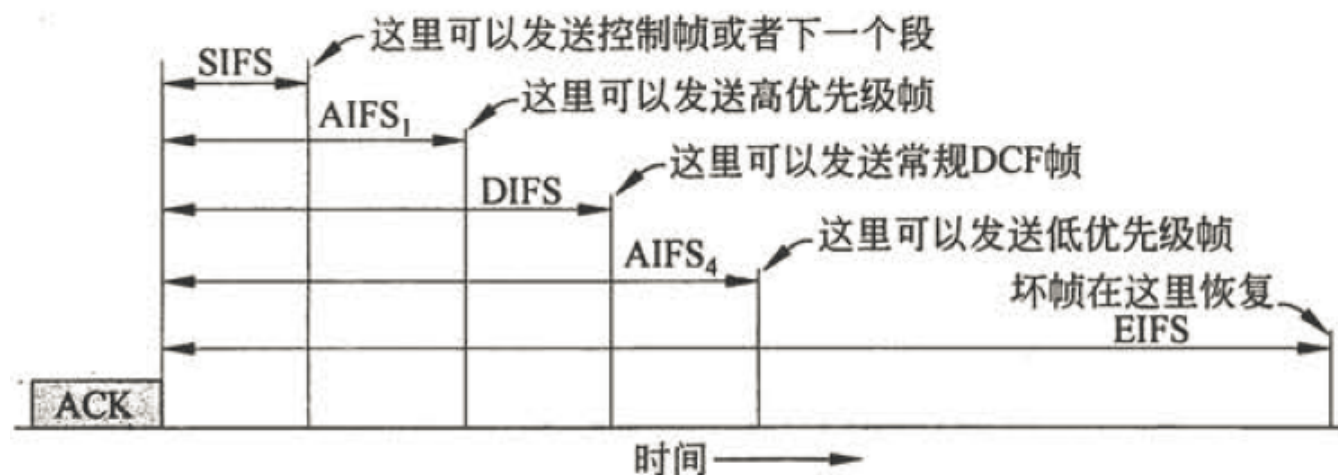


图 4-28 802.11 中的帧间间隔

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 4. 802. 11 帧结构

§ 4. 介质访问控制子层

4. 4. 无线局域网

4. 4. 4. 802. 11 帧结构

★ 帧类型：数据帧、控制帧和管理帧

★ 每种帧都有一个被MAC层使用的头，此外还有一些被物理层使用的头

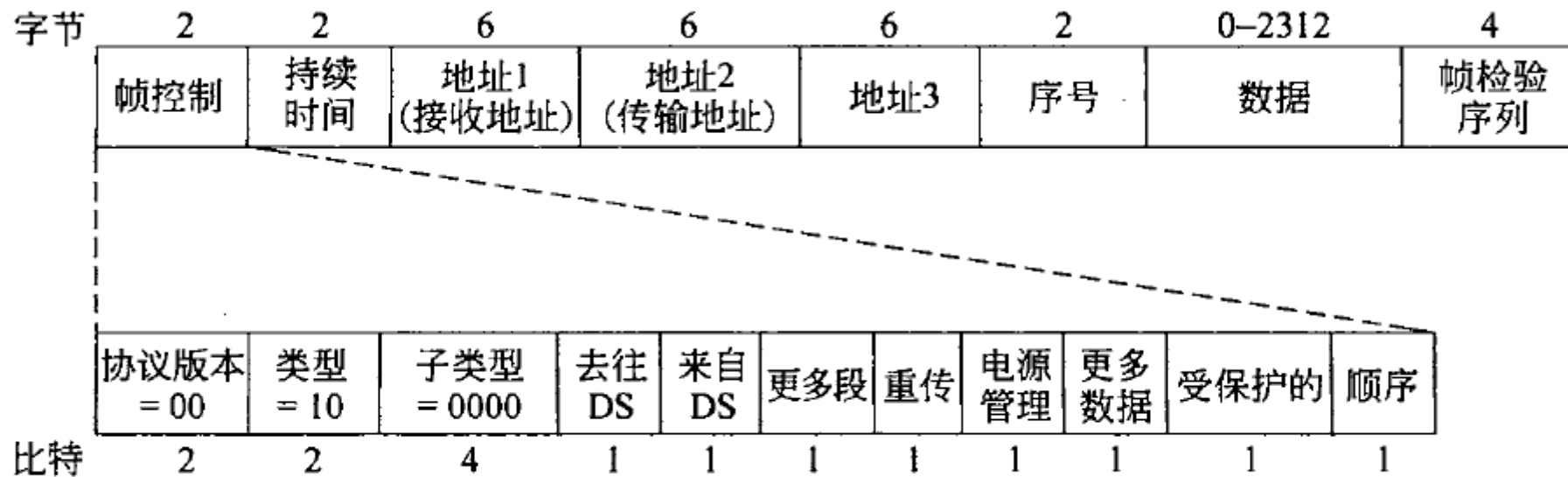


图 4-29 802.11 数据帧的格式

★ Windows 下的Wireshark无法抓到802.11帧（附件）

§ 4. 介质访问控制子层

4.4. 无线局域网

4.4.5. 服务

★ 分布式服务：由基站提供，处理站的移动性

- 接入（association）：移动站进入一基站射频范围，完成与基站的连接。包括宣布移动站的标识和能力，以及认证等

- 脱离（disassociation）

- 重接入（reassociation）：移动站在移动中从一个射频区域到另一个时所用服务

- 分发（distribution）：帧路由选择服务

- 集成（integration）：与非802.11网络集成

★ 站服务：在单一射频区域内发生接入服务后的服务

- 认证（authentication）：由基站发送特定的质疑帧，盘问移动站

- 退出认证（deauthentication）：在离开该射频区域时调用

- 加密：对敏感信息加密与解密

- 数据传输

★ 漫游：保持传输层连接的无缝移动

★ 速率适应：能自适应选择不同数据传输速率

- 遇连续两个帧未受到ACK，则降一级速率，并启动计时器

- 连续10个帧收到ACK，或计时器超时，则提高一级速率

★ 功率管理

- 节点向AP指示，其将进入睡眠

- 此后AP缓存发往该节点数据帧

- 待该节点被唤醒时（接收AP的信标），接收缓存的数据帧

§ 4. 介质访问控制子层

4. 5. 宽带无线(仅与802. 11做简单对比, 其余略)

- ★ 协议为802. 16系列, 称为WiMAX (Worldwide Interoperability for Microwave Access)
其中802. 16m与LTE(含TD-LTE/FDD-LTE)同为4G标准
- ★ 802. 11主要为个人移动用户提供因特网接入服务; 802. 16主要为公众移动用户提供包括话音、视频、因特网接入在内的综合服务
- ★ 802. 11是覆盖范围很小的专用网络; 802. 16是覆盖范围较大的公用通信网络, 因此802. 16的安全性要求比802. 11高
- ★ 802. 16的用户数及带宽高于802. 11
- ★ 802. 16要求更好的服务质量

§ 4. 介质访问控制子层

4.6. 蓝牙

(略)

§ 4. 介质访问控制子层

4. 7. RFID

(略)

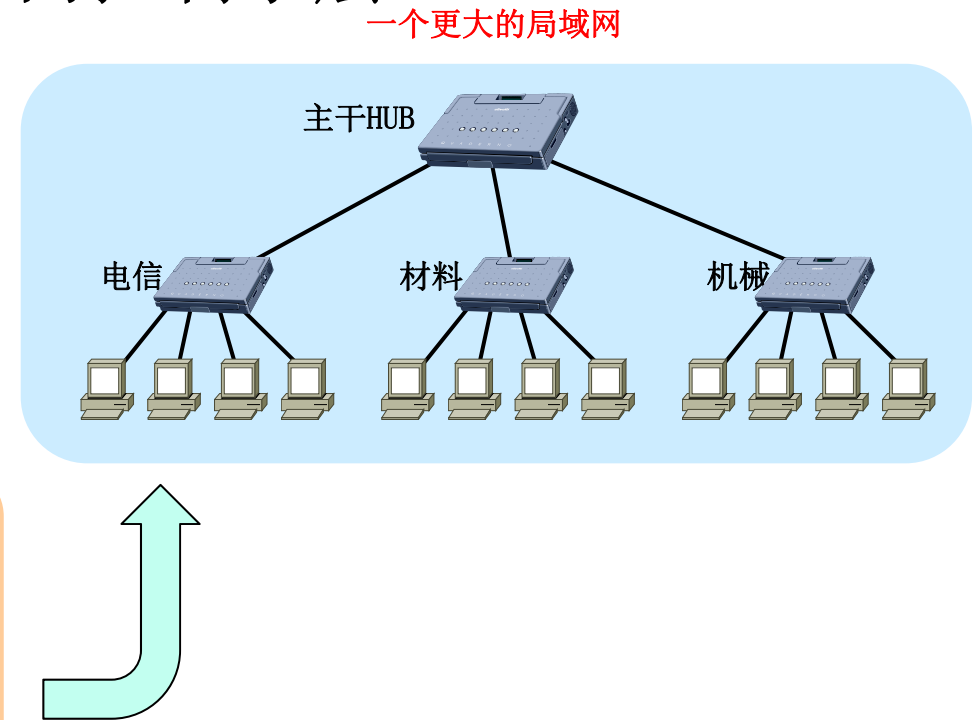
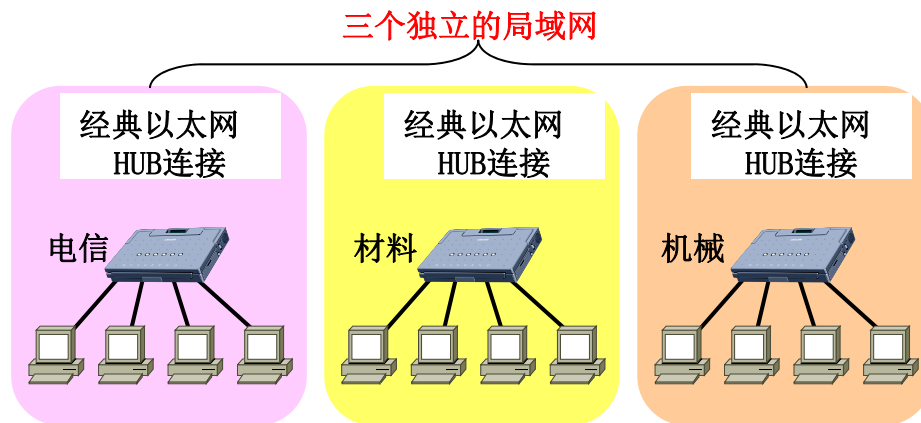
§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.1. 网桥的使用

★ 局域网的扩展方法

- 在物理层使用集线器(HUB)扩展



优点:

- ◆ 使原来属于不同局域网上的计算机能够进行通信, 扩大了局域网的覆盖范围

缺点:

- ◆ 碰撞域增大, 总的吞吐量并未提高(甚至下降)
- ◆ 本质上是一个局域网, 因此传输距离、节点数量等要受局域网的限制(HUB的特性决定)
- ◆ 如果不同的局域网使用不同的数据率, 则无法使用HUB互联(HUB的特性决定)
- ◆ 无法连接异种网络(例: 802.3 / 802.11)

§ 4. 介质访问控制子层

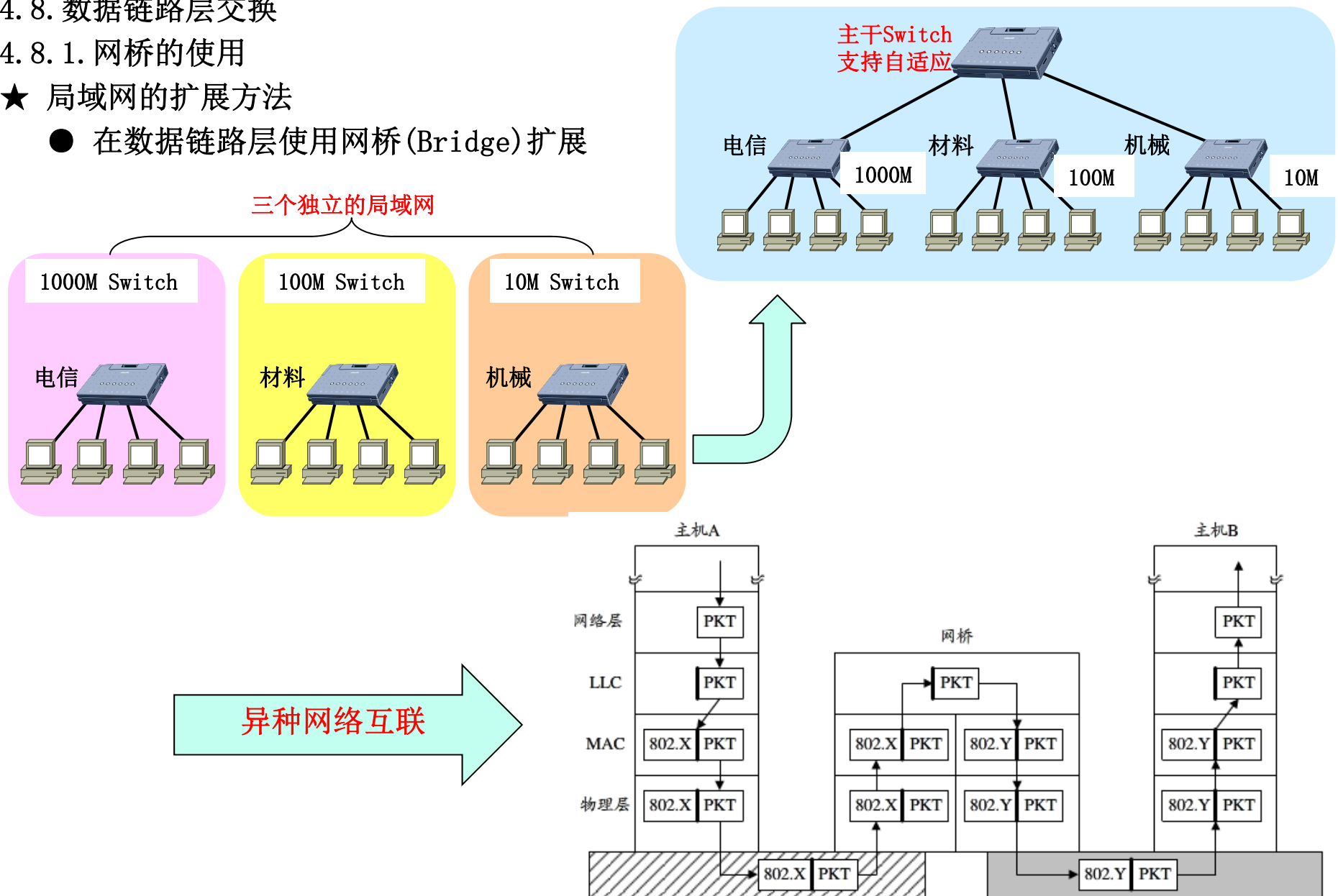
三个局域网互联

4.8. 数据链路层交换

4.8.1. 网桥的使用

★ 局域网的扩展方法

- 在数据链路层使用网桥(Bridge)扩展



§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.1. 网桥的使用

★ 局域网的扩展方法

- 在数据链路层使用网桥(Bridge)扩展

- ◆ 以太网交换机是网桥的一种
- ◆ 网桥的作用是多个LAN之间互联，方便扩展LAN的节点数和物理覆盖距离，提高可靠性
- ◆ 网桥工作在数据链路层，它根据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，并不是向所有的接口转发此帧，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接口
- ◆ 异种网络互联时，要求网络层采用相同协议

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.1. 网桥的使用

★ 使用网桥连接不同局域网时应考虑的问题

- 不同的速率：不同LAN的速率不相同，要求网桥能够缓存大量的帧，但仍有可能因内存不够而丢失帧
- 不同的帧长：最大帧长不同，数据链路层不能处理帧的分片与重组，超过目的网络最大帧长的帧只能被丢弃
- 不同的帧格式：异种网络互联时，802.x和802.y的帧格式不同，需要重新组帧和重新计算校验和
- 不同的QoS要求：异种网络互联时，某些网络支持优先级（例：令牌传递网络），某些网络不支持（例：以太网）
- 不同的安全措施：异种网络互联时，某些网络支持加密（例：802.11），某些网络不支持（例：以太网）

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.1. 网桥的使用

★ 理想网桥的特点

- 即插即用，只需将网桥与各个欲通过它互联的局域网连接起来，整个系统就能够正常工作，不需要做任何硬件或软件上的设置，增删节点非常容易
- 网桥的插入不会中断现有网络的运行
- 网桥的存在对网络用户是透明的（透明网桥）
- “透明”是指局域网上的站点不知道所发送的帧将经过哪几个网桥，即网桥对各站来说是看不见的
- 透明网桥的标准是 IEEE 802.1D

★ 透明网桥的学习算法

- 向后学习算法(backward learning)
- 生成树算法(spanning tree)

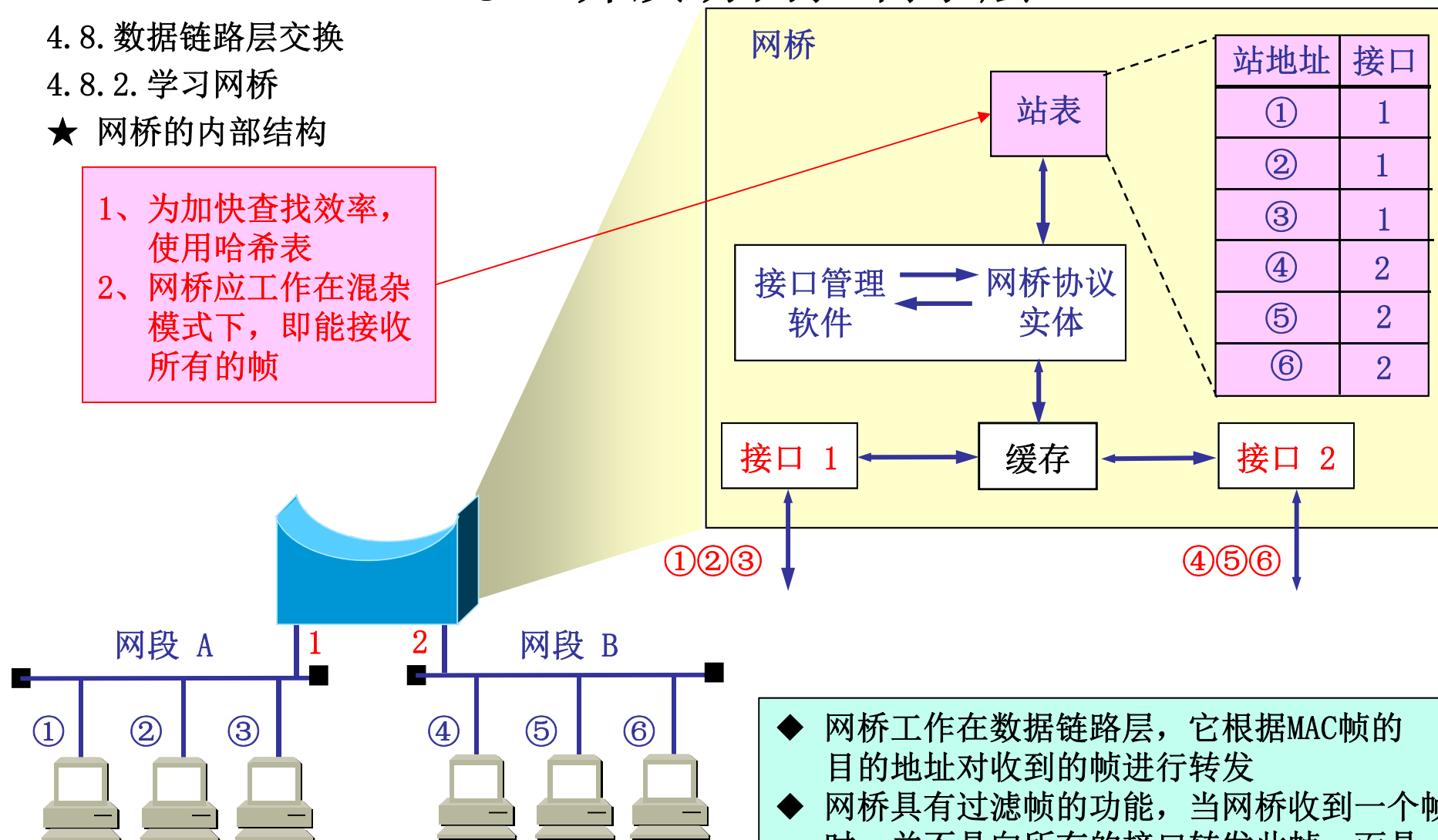
§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.2. 学习网桥

★ 网桥的内部结构

- 1、为加快查找效率，使用哈希表
- 2、网桥应工作在混杂模式下，即能接收所有的帧



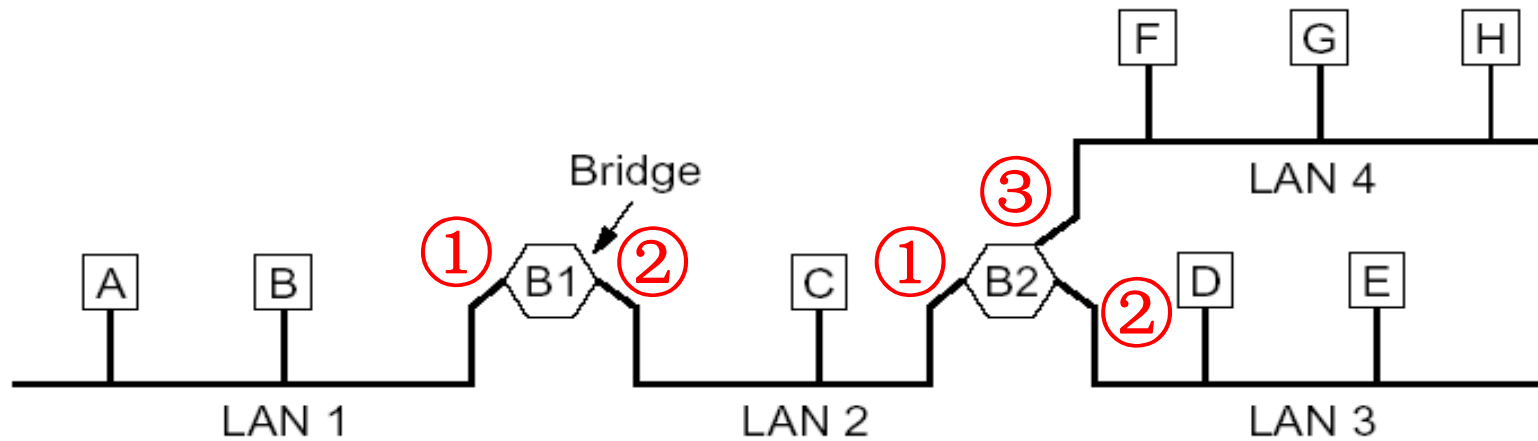
- ◆ 网桥工作在数据链路层，它根据MAC帧的目的地址对收到的帧进行转发
- ◆ 网桥具有过滤帧的功能，当网桥收到一个帧时，并不是向所有的接口转发此帧，而是先检查此帧的目的MAC地址，然后再确定将该帧转发到哪一个接口

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.2. 学习网桥

★ 网桥的内部结构



网桥B1中的转发表

MAC地址	端口
A	1
B	1
C	2
D	2
E	2
F	2
G	2
H	2

网桥B2中的转发表

MAC地址	端口
A	1
B	1
C	1
D	2
E	2
F	3
G	3
H	3

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.2. 学习网桥

★ 透明网桥的工作原理

- 问题1：网桥如何知道是否应当转发帧，以及应往哪个端口转发？
 - ◆ 网桥内部使用一张转发表，表中记录各个目的地址在网桥的哪个端口上
 - ◆ 网桥用帧的目的地址查找转发表，若目的地址所在端口与帧的输入端口相同，丢弃帧；否则从目的地址所在端口转发帧

- 问题2：如何生成网桥中的转发表？
 - ◆ 转发表初始为空，网桥通过**逆向学习**法获知各个目的地址所在端口，逐步建立转发表
 - ◆ **逆向学习**：网桥通过检查帧的源地址及输入端口来发现网络中的节点及所在的端口

- 问题3：若转发表尚未完全建立或出现了新节点，即帧的目的地址不在转发表中，网桥该如何转发？
 - ◆ 对于每个发向未知目的地址对应端口的帧，使用**泛洪算法**(flooding algorithm)转发到除源端口外的所有端口，学习成功后则不再泛洪而只转发到正确端口

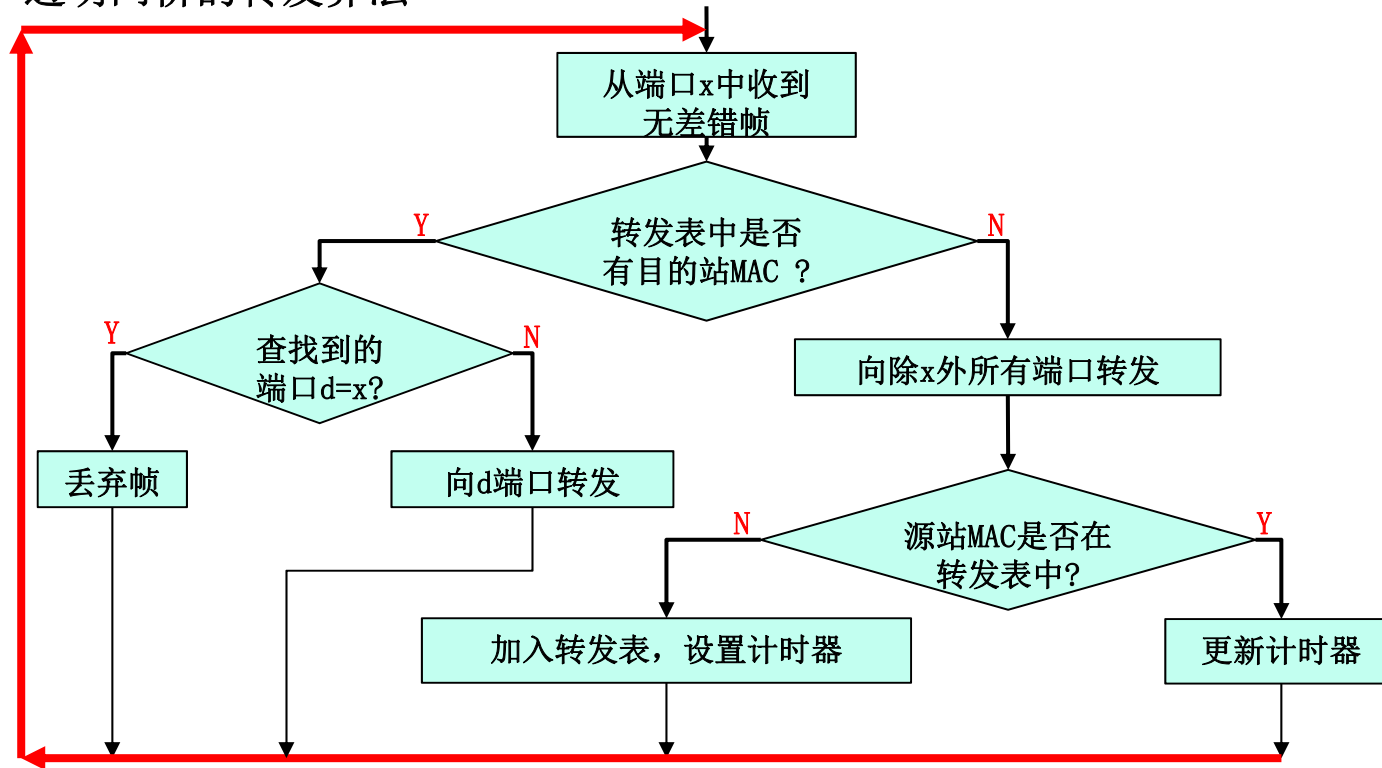
- 问题4：网桥学习到的知识过时了怎么办？
 - ◆ 给转发表的每个表项添加一个时间项，称为生存期，有转发则更新生存期为当前时间
 - ◆ 网桥定期扫描转发表，发现当前时间与生存期的差值超过设定值，则删去该表项

§ 4. 介质访问控制子层

4. 8. 数据链路层交换

4. 8. 2. 学习网桥

★ 透明网桥的转发算法



★ 另一个进程周期性扫描转发表并删除当前时间与计时器差值超过设定值的表项

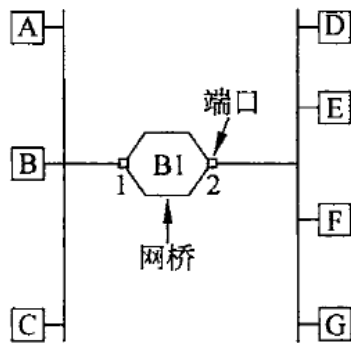
§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.2. 学习网桥

★ 透明网桥的转发算法

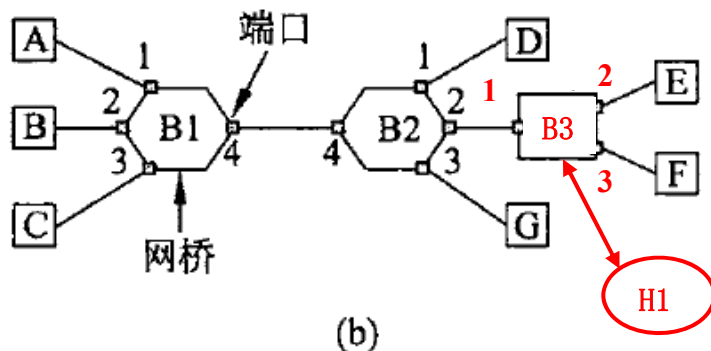
- 为提高转发效率，某些网桥（例：交换机）只要收到目的MAC地址就可以开始转发（此时帧还未接收完成），称为直通式交换/虫孔路由
- 网桥转发时，帧的格式可能重写，也可能不变，只要网络层协议相同即可
- 多个网桥级联时，每个网桥只维护自己的转发表，不会造成冲突



(a)

假设以太网，ABC通过HUB互联，
DEFG通过HUB互联，B1为交换机

- ◆ A/B/C ⇔ A/B/C
B1的1#口收到帧，丢弃
- ◆ D/E/F/G ⇔ D/E/F/G
B1的2#口收到帧，丢弃
- ◆ A/B/C ⇔ D/E/F/G
B1的1#/2#相互转发



(b)

假设以太网，B1/B2/B3为交换机

- ◆ A/B/C ⇔ A/B/C B1内转发
- ◆ D/G ⇔ D/G B2内转发
- ◆ E/F ⇔ E/F B3内转发
- B1/B2/B3间无转发

将B3替换为HUB H1

- ◆ E/F ⇔ E/F
H1广播式发送，因此B2的2#
收到E/F发来的信息，但丢弃

假设以太网，B1/B2/B3为交换机

- ◆ A/B/C ⇔ D/G
- A/B/C ⇔ E/F
- D/G ⇔ E/F
- B1的4#：有DGEF信息
- B2的2#：有EF信息
- 4#：有ABC信息
- B3的1#：有ABCDF信息
- B1/B2/B3相互转发

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.3. 生成树网桥

★ 引入

在透明网桥中，网桥间只有一条链路，导致可靠性不高，为了提高可靠性，可以采用冗余备份的方式

- 产生的问题：(第一次)目的地址未知的帧会循环冗余转发，目的地址已知的帧会重复发送

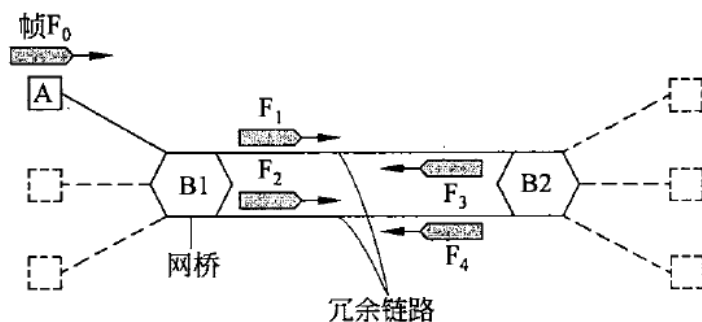


图 4-43 具有两条平行链路的网桥

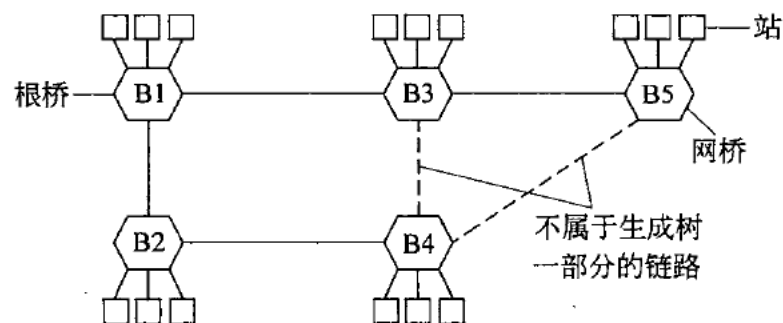


图 4-44 一棵连接 5 座网桥的生成树。虚线表示不属于生成树的链路

★ 解决循环冗余转发的方法

- 在有环的网络中，仅在网桥发生故障时才启用冗余链路，平时只使用没有环的拓扑转发帧
- 将网桥抽象成边，局域网抽象成顶点，形成网络拓扑图。求该图的一棵生成树 (spanning tree)，使得覆盖图中所有的顶点但没有环路
- 生成树构造完成后，只有位于生成树中的网桥能够在属于生成树的边上转发帧

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.3. 生成树网桥

★ 生成树的构造算法

- 选举根网桥：各个网桥广播自己的序列号，序列号最小的网桥成为生成树的根。根网桥可在所有的端口上转发帧
- 每个网桥计算自己到根的最短路径（跳数），记录自己的哪个端口在最短路径上，这个端口即为该网桥到根的优先路径
- 所有连接到同一个LAN上的网桥选一个指派网桥（designated bridge），指派网桥是这些网桥中离根最近的；若距离相等，则选序列号最小的
- 生成树的节点由根网桥和指派网桥组成，指派网桥到根网桥最短路径上的端口成为生成树上的边
- 生成树算法始终在每个网桥(包括非指派网桥)上运行，当某个网桥或局域网出现故障时，重新计算生成树

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.4. 中继器/集线器/网桥/交换机/路由器和网关

★ 名词解释

中继器 (repeater)：仅对电信号放大和整形

集线器 (hub)：所有端口一个碰撞域，不解析帧，广播式发送，每条线路速度必须相同

网桥 (bridge)：连接多个LAN，通过软件解析帧，每条线路是一个碰撞域，且速度可以不同

交换机 (switch)：每个端口是一个碰撞域，且都有缓冲区存放到达分组，通过硬件解析帧

路由器 (router)：在网络层转发数据，通过软件解析分组协议头，而不管帧头

网关 (gateway)：用于网络层以上的设备互联

传输网关：连接运行不同传输协议的网关

应用网关：在不同应用间进行格式转换

★ 工作在不同层次

应用层	应用网关
传输层	传输网关
网络层	路由器
数据链路层	网桥, 交换机
物理层	中继器, 集线器

(a)

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.5. 虚拟局域网

★ 多个LAN互连可能存在的问题

- 安全问题：希望各部门LAN独立
- 负载问题：各LAN负载不同
- 广播风暴

★ VLAN (Virtual LAN)

- VLAN是一个逻辑子网，按逻辑位置组织网络，而不是物理位置
- 每个VLAN是一个独立的广播域（隔离广播风暴）
- VLAN通过软件实现VLAN成员的增加、移动和改变（改变结构非常方便）
- 同一交换机的站点也可以属于不同的VLAN（要求交换机支持 VLAN 功能）
- 实际应用中通常用不同颜色来区分

§ 4. 介质访问控制子层

4.8. 数据链路层交换

4.8.5. 虚拟局域网

★ IEEE 802.1Q标准

● 在帧头中增加VLAN标志域

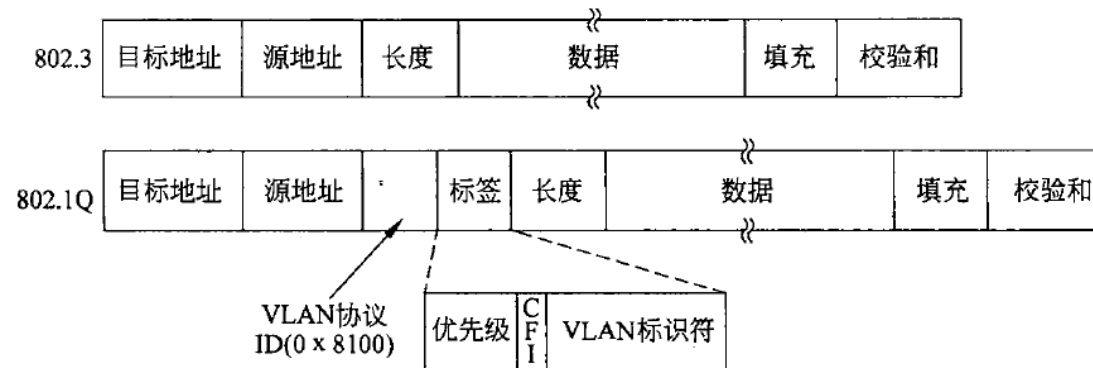


图 4-49 802.3 (传统的) 和 802.1Q 以太帧格式

增加4字节

协议 : 0x8100 (16 bit)
优先级 : 3 bit
CFI : 1 bit
VLAN标识: 12 bit (0-4095)

- 转发序列中所有交换机必须支持802.1Q
- 传输链路上第一台交换机加上VLAN标记, 最后一台去除VLAN标记 (对终端节点透明)