

计算机网络

■ 主讲：肖林





内容

- ④ 第1章 概述
- ④ 第2章 物理层
- ④ 第3章 数据链路层
- ④ **第4章 介质访问控制子层**
- ④ 第5章 网络层
- ④ 第6章 传输层
- ④ 第7章 应用层

第4章 介质访问控制子层



- ④ 局域网与信道分配
- ④ 多路访问协议
- ④ 以太网
- ④ 无线LAN
- ④ 蓝牙
- ④ DOCSIS
- ④ 数据链路层交换

4.1 局域网与信道分配



- 局域网概述
- 静态信道分配
- 动态信道分配的假设

局域网概述



■ 网络链路分类

- 点到点链路：广域网
- 广播信道：局域网

■ 定义

- 局域网是一种将小区域内的各种通信设备互连在一起的通信网络

■ 主要特点

- 网络为一个单位所拥有，且地理范围和站点数目均有限

局域网概述(2)



■ 局域网的基本特点

- 高数据传输率 (10 ~ 1000 Mbps)
- 短距离 (0.1 ~ 10 km)
- 低出错率 (10^{-8} ~ 10^{-11})

■ 局域网具有如下的一些主要优点

- 能方便地共享昂贵的外部设备、主机以及软件、数据。提高了系统的可靠性、可用性
- 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

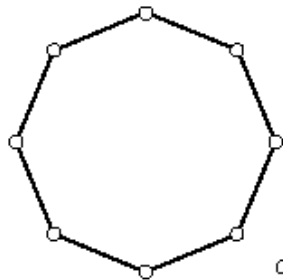
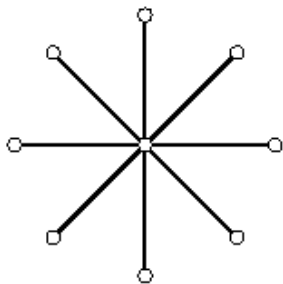
■ 局域网发展趋势

- 高速：10G Ethernet
- 移动：无线局域网 IEEE 802.11

局域网概述(3)

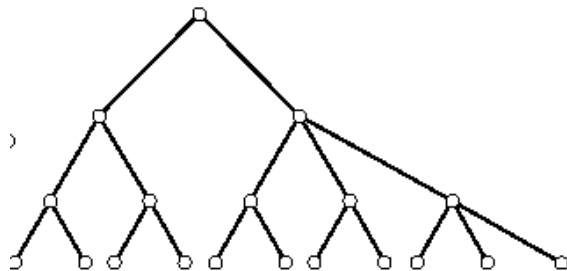
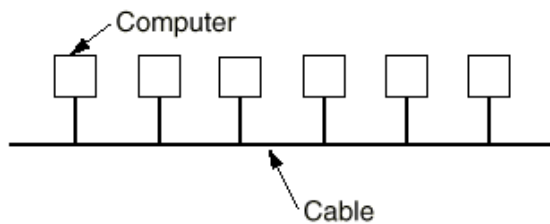
■ 局域网拓扑结构

- 星型结构
- 环型结构
- 总线型结构
- 树型结构

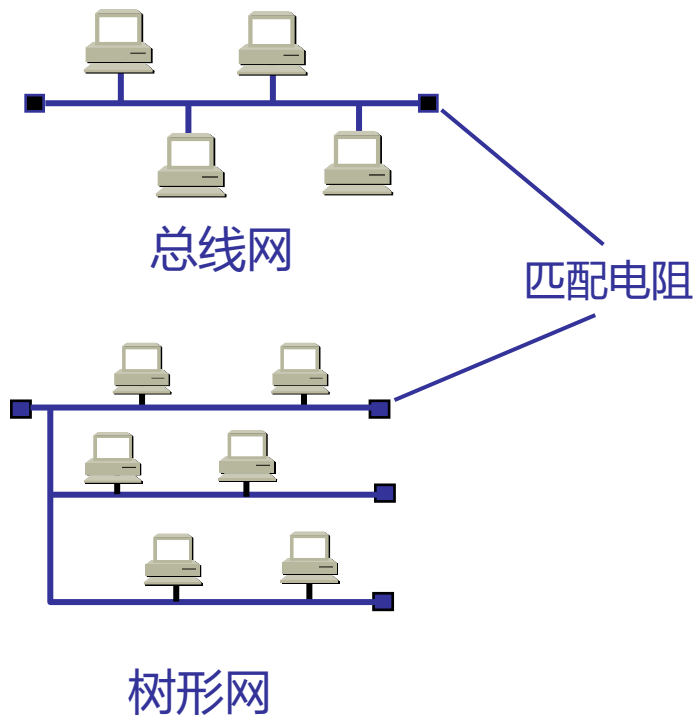
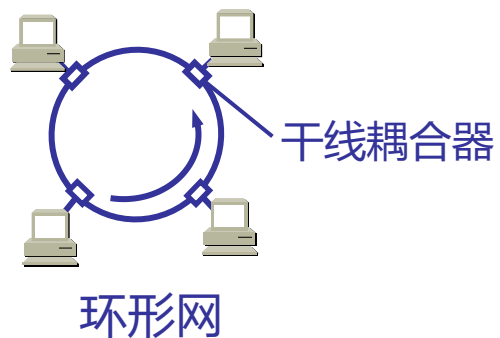
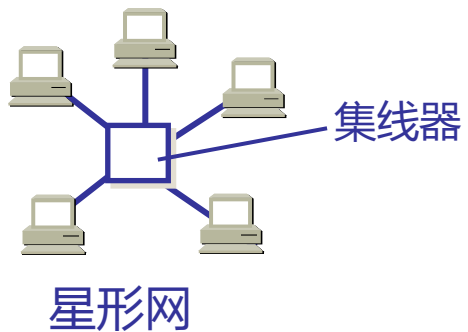


■ 传输介质

- 双绞线
- 基带同轴电缆
- 光纤
- 无线



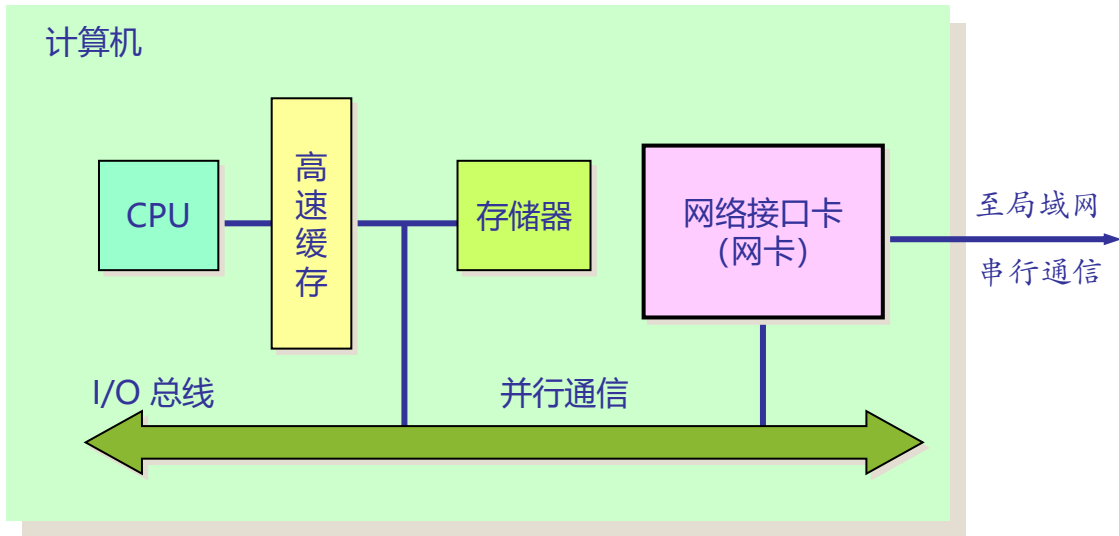
拓扑结构说明





网卡的作用

- 网卡又称为通信适配器(adapter)或网络接口卡 NIC (Network Interface Card)
- 网卡的重要功能：
 - 进行串行/并行转换
 - 对数据进行缓存
 - 安装设备驱动程序
 - 实现以太网协议



局域网技术

■ 广播信道

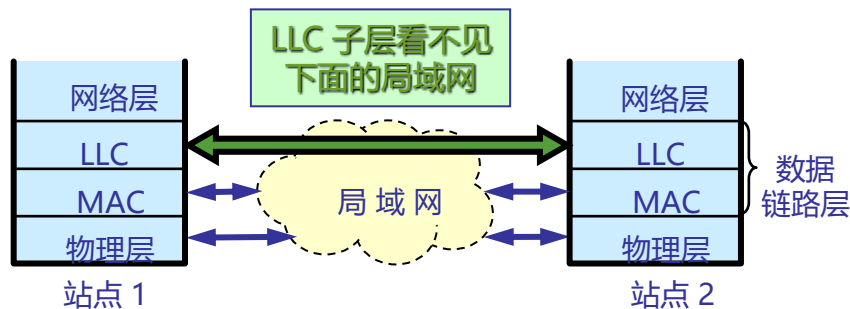
- 多路访问信道，随机访问信道
- 关键问题：如何解决对信道争用

■ 数据链路层的两个子层

- 逻辑链路控制 LLC (Logical Link Control)子层
- 介质访问控制MAC (Medium Access Control)子层：解决信道争用的协议

■ 信道分配方法

- 静态分配
- 动态分配



静态信道分配



■ 频分多路复用 FDM (波分复用WDM)

- 原理：将频带平均分配给每个要参与通信的用户
- 优点：适合于用户较少，数目基本固定，各用户的通信量都较大的情况
- 缺点：无法灵活地适应站点数及其通信量的变化

■ 时分多路复用 TDM

- 原理：每个用户拥有固定的信道传送时槽
- 优点：适合于用户较少，数目基本固定，各用户的通信量都较大的情况
- 缺点：无法灵活地适应站点数及其通信量的变化

子队列的效率



■ 队列平均延时

- 容量C b/s, 数据到达率 λ 帧/秒, 平均帧长 $1/\mu$ 比特/帧

$$T = 1 / (\mu C - \lambda)$$

- 例子: 100M bps, 5000 帧/秒, 10 000 比特/帧

$$T = 1 / (100\,000\,000 / 10\,000 - 5000) = 1 / 5000 \text{ (s)} = 200 \text{ (}\mu\text{s)}$$

■ N个子队列平均延时

- 子队列容量C/N b/s, 子队列数据到达率 λ/N 帧/秒, 平均帧长 $1/\mu$ 比特/帧

$$T_N = 1 / (\mu(C/N) - \lambda/N) = N / (\mu C - \lambda) = NT$$

- 例子: 100Mbps用10个10Mbps代替, 平均延时是多少?

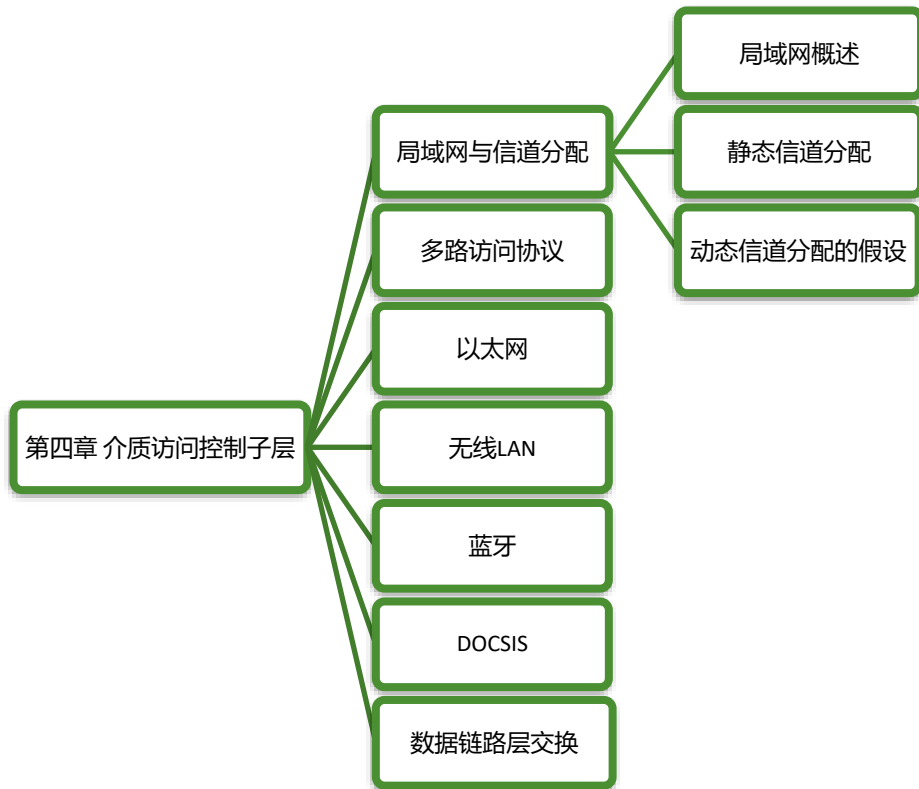
动态信道分配的假设



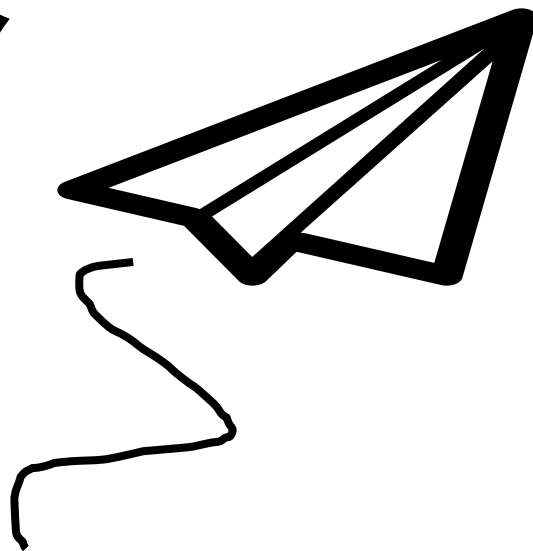
■ 信道分配方案的5个假设

- 流量独立：站模型，每个站点是独立的，并以统计固定的速率产生帧，一帧产生后到被发送走之前，站点被封锁
- 单信道：所有的通信都是通过单一的信道来完成的，各个站点都可以从信道上收发信息
- 冲突可观察：若两帧同时发出，会相互重叠，结果使信号无法辨认，称为冲突。所有的站点都能检测到冲突，冲突帧必须重发
- 连续时间或时隙：任意时间传输或时间分槽
- 载波侦听或非载波侦听：使用信道之前检查是否占用，或直接盲目发送

本章导航与要点



本节课程结束



4.2 多路访问协议



- ALOHA
- 载波侦听多路访问协议CSMA
- 无冲突的协议
- 有限竞争协议
- 无线局域网协议

ALOHA



■ ALOHA协议

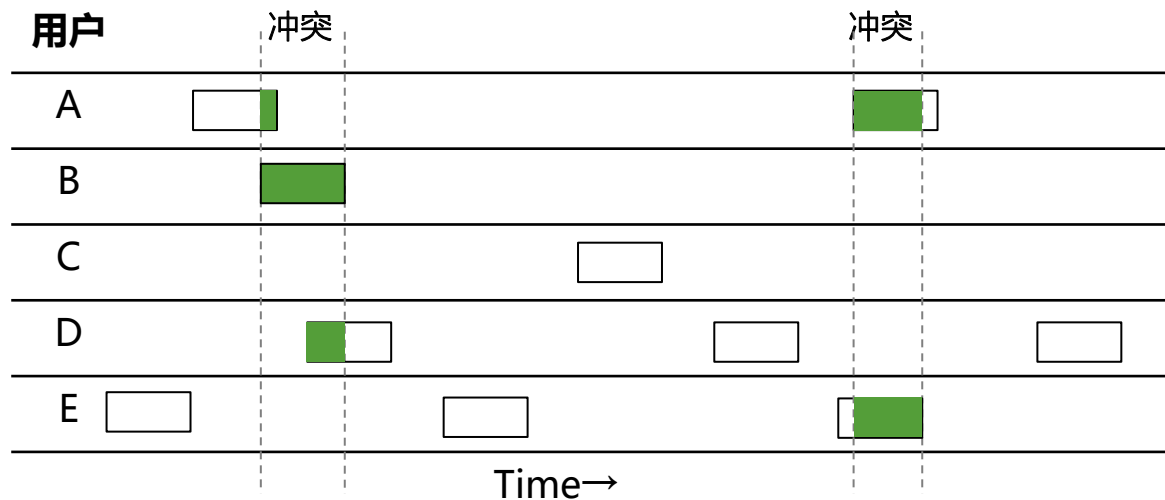
- 目的：解决信道的动态分配，基本思想可用于任何无协调关系的用户，争用单一共享信道使用权的系统
- 夏威夷大学早期研制的系统称为ALOHA，是Additive Link On-line HAwaii system的缩写，而ALOHA恰好又是夏威夷方言的“你好”

■ 协议分类

- 纯ALOHA协议：任意时间任意发送
- 分槽ALOHA协议：指定分段开始时间任意发送

纯ALOHA协议

- 基本思想：用户有数据要发送时，可以直接发至信道；然后监听信道看是否产生冲突，若产生冲突，则等待一段随机的时间重发
- 多用户共享单一信道，并由此产生冲突，这样的系统称为竞争系统



两个归一化参数



■ 吞吐量 S ，又称为吞吐率

- 它等于在帧的发送时间 t (也称为帧时frame time) 内成功发送的平均帧数
- 显然, $0 \leq S \leq 1$, 而 $S = 1$ 是极限情况

■ 网络负载(offered load) G

- 从网络的角度看, G 等于在 t 内总共发送的平均帧数
- 在稳定状态下, 吞吐量 S 与网络负载 G 的关系为

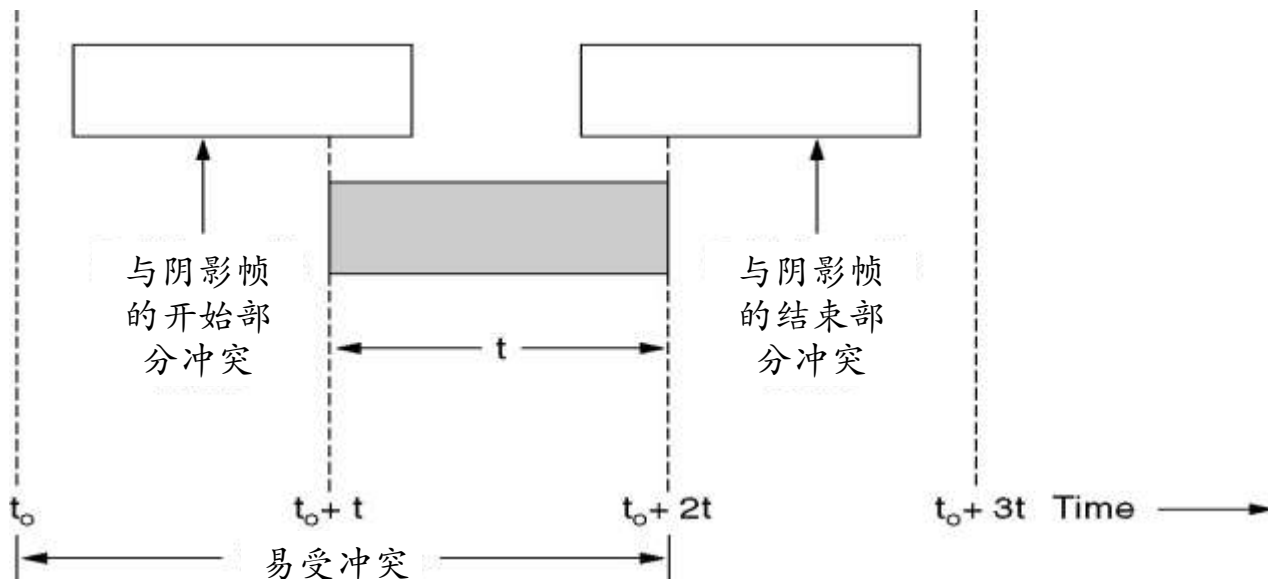
$$S = G \cdot P[\text{发送成功}]$$

- 这里 $P[\text{发送成功}]$ 是一个帧发送成功的概率, 表示为 P_0 , 它实际是发送成功的帧, 在所发送的帧的总数中所占的比例

冲突危险周期

■ 阴影帧的冲突危险周期

$(t_0, t_0 + 2t)$



信道效率



■ 假设：帧长固定，无限个用户，按泊松分布产生新帧

- 平均每个帧时产生 N 帧 ($0 < N < 1$) ; 发生冲突重传，新旧帧共传 k 次，遵从泊松分布，平均每个帧时生成 G 帧

- 吞吐率 $S = GP_0$, P_0 为发送一帧不受冲突影响的概率

- 冲突危险区，见前图

- 一个帧时内产生 k 帧的概率 $\Pr[k] = G^k e^{-G} / k!$

两个帧时平均产生 $2G$ 个帧，在冲突危险区内无其它帧产生的概率为：

$$P_0 = e^{-2G}, \text{ 所以 } S = Ge^{-2G};$$

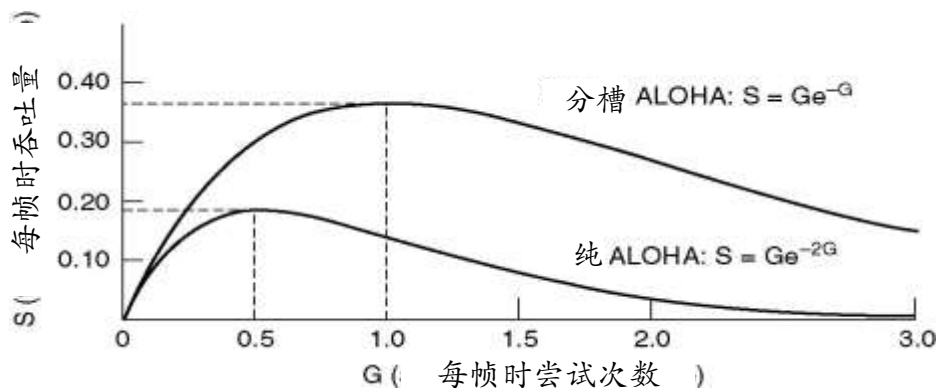
- 效率：最高在 $G=0.5$ 时，信道利用率最高只有18.4%.

分槽ALOHA协议

- 基本思想：把信道时间分成离散的时间槽，槽长为一个帧所需的发送时间
 - 每个站点只能在时槽开始时才允许发送。其他过程与纯ALOHA协议相同

- 信道效率

- 冲突危险区是纯ALOHA的一半，所以 $P_0 = e^{-G}$ ， $S = Ge^{-G}$
- 与纯ALOHA协议相比，降低了产生冲突的概率，信道利用率最高为34.8%



载波侦听多路访问协议CSMA



- 载波监听多路访问协议 (Carrier Sense Multiple Access protocols)
 - 载波监听：站点在为发送帧而访问传输信道之前，首先监听信道有无载波，若有载波，说明已有用户在使用信道，则不发送帧以避免冲突
 - 多路访问：多个用户共用一条线路
- 持续和非持续CSMA
 - 1-持续CSMA、非持续CSMA、p-持续CSMA
- 带冲突检测的CSMA
 - 有冲突则停止发送，CSMA/CD——以太网MAC子层

1-持续CSMA



■ 原理

- 若站点有数据发送，先监听信道
- 若站点发现信道空闲，则发送
- 若信道忙，则继续监听直至发现信道空闲，然后完成发送
- 若产生冲突，等待一随机时间，然后重新开始发送过程

■ 优点：减少了信道空闲时间

■ 缺点：增加了发生冲突的概率

■ 广播延迟对协议性能的影响：广播延迟越大，发生冲突的可能性越大，协议性能越差

非持续CSMA



■ 原理

- 若站点有数据发送，先监听信道
- 若站点发现信道空闲，则发送
- 若信道忙，等待一随机时间，然后重新开始发送过程
- 若产生冲突，等待一随机时间，然后重新开始发送过程

■ 优点：减少了冲突的概率

■ 缺点：增加了信道空闲时间，数据发送延迟增大

■ 信道效率比 1-持续CSMA高，传输延迟比 1-持续CSMA大

p-持续CSMA



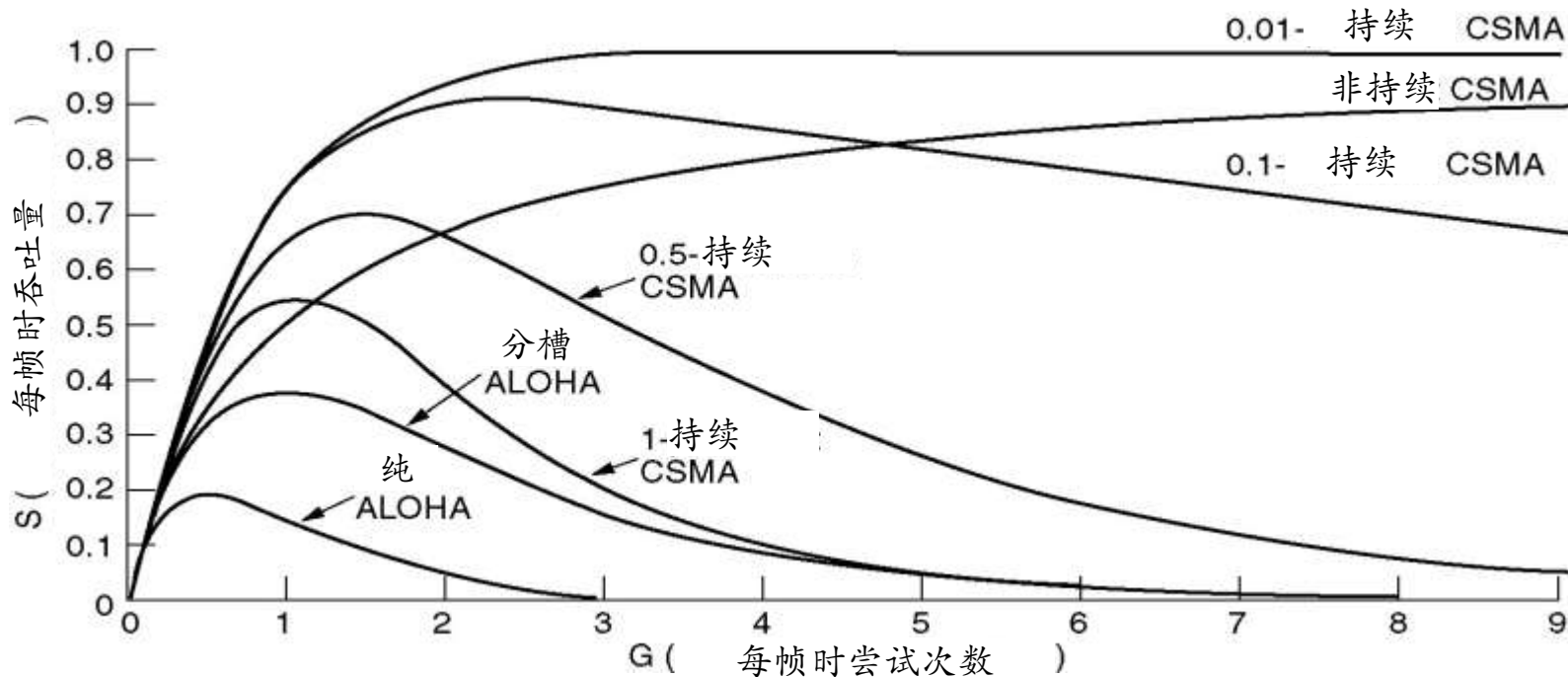
■ 适用于分槽信道

■ 原理

- 若站点有数据发送，先监听信道
- 若站点发现信道空闲，则以概率 p 发送数据，以概率 $q = 1 - p$ 延迟至下一个时槽发送。若下一个时槽仍空闲，重复此过程，直至数据发出或时槽被其他站点所占用
- 若信道忙，则等待下一个时槽，重新开始发送
- 若产生冲突，等待一随机时间，然后重新开始发送

五种多路访问协议性能比较

■ 各随机访问协议的信道利用率与负载之间的比较



带冲突检测的CSMA



- 带冲突检测的载波监听多路访问协议CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- 引入原因：当两个帧发生冲突时，两个被损坏帧继续传送毫无意义，而且信道无法被其他站点使用，对于有限的信道来讲，这是很大的浪费。如果站点边发送边监听，并在监听到冲突之后立即停止发送，可以提高信道的利用率，因此产生了CSMA/CD
- 原理
 - 站点使用CSMA协议进行数据发送
 - 在发送期间如果检测到冲突，立即终止发送，并发出一个瞬间干扰信号，使所有的站点都知道发生了冲突
 - 在发出干扰信号后，等待一段随机时间，再重复上述过程

CSMA/CD说明



- “多路访问”、“载波监听”：前面已有解释（见P20）
 - 总线上并没有什么“载波”，因此“载波监听”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
- “冲突检测”就是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“碰撞检测”也称为“冲突检测”

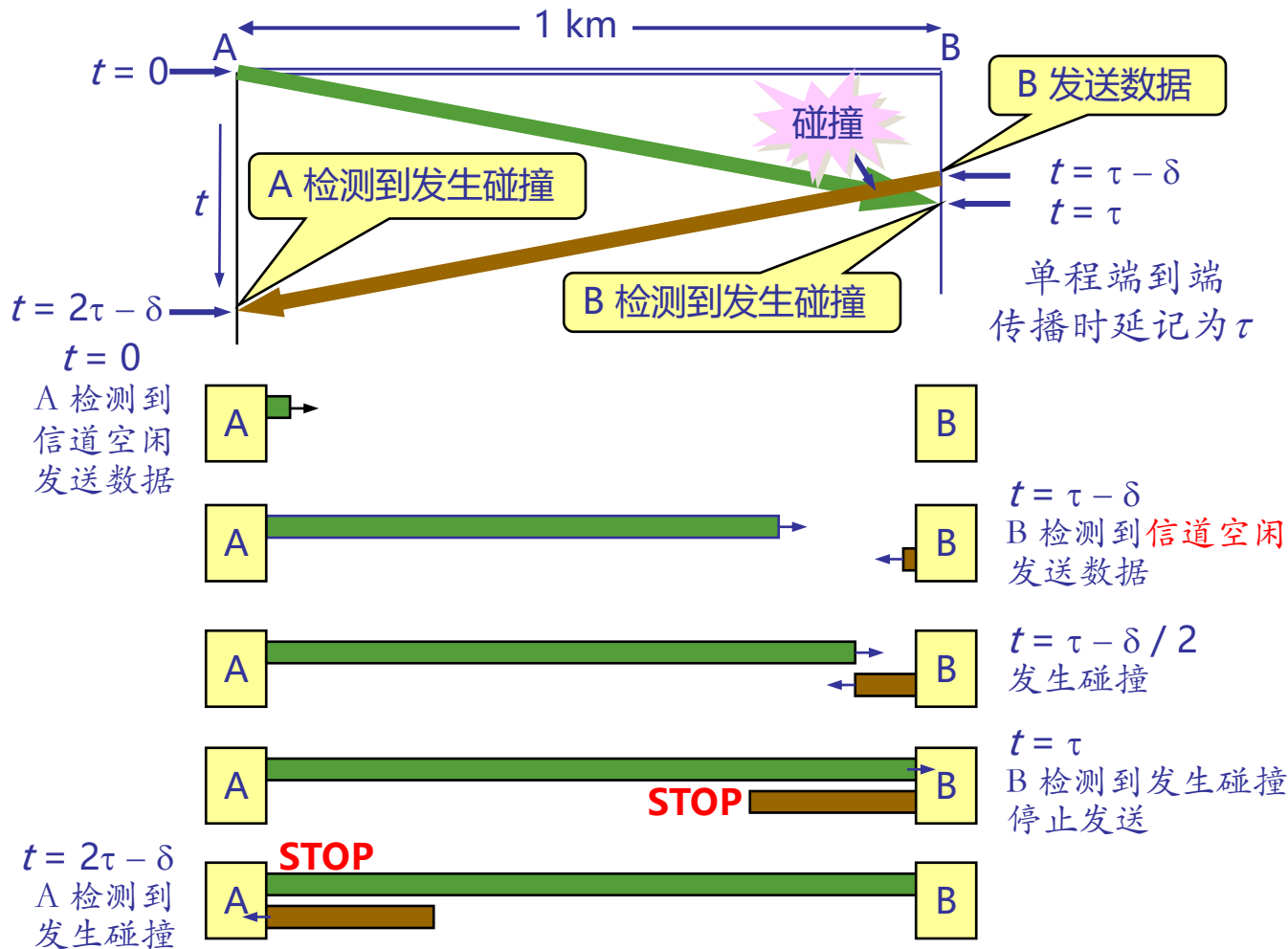
碰撞



- 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
 - 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

- 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
 - 碰撞的结果使两个帧都变得无用

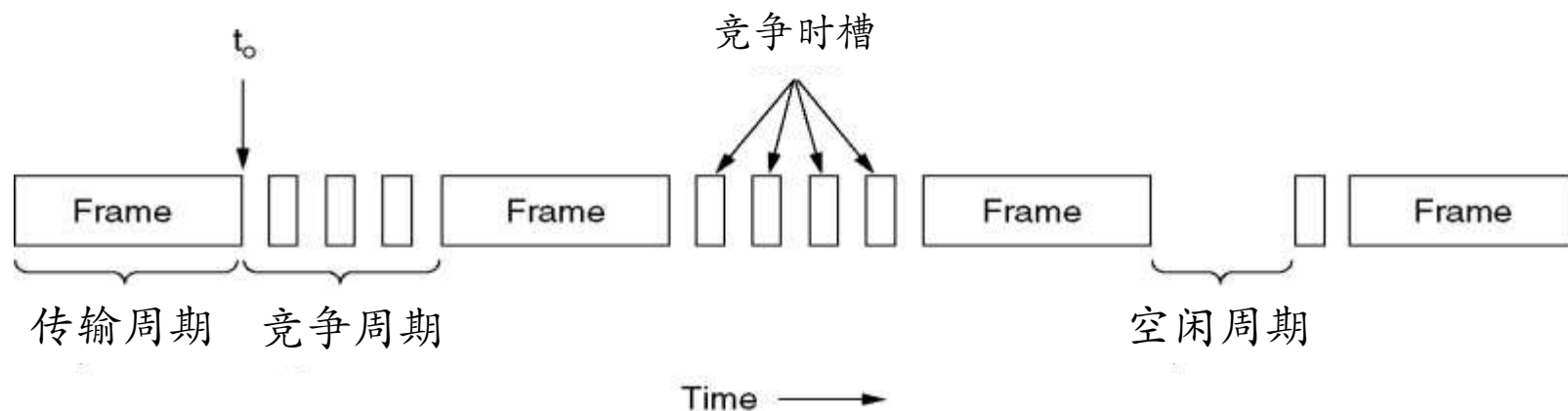
碰撞图解



CSMA/CD分析



- CSMA/CD的三种状态：传输、竞争和空闲



- 问题：一个站点确定发生冲突要花多少时间

CSMA/CD分析(2)



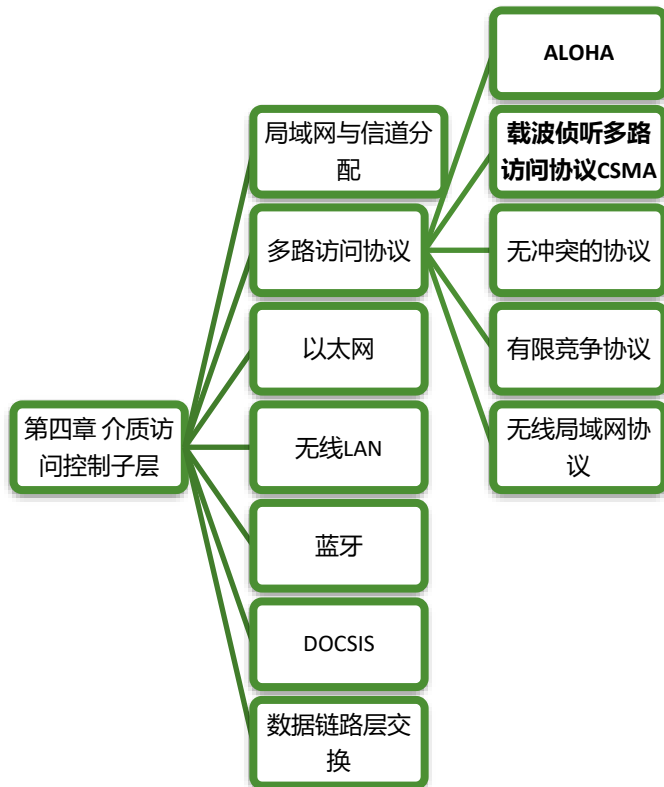
■ 重要特性

- 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
- 这种发送的不确定性，使整个以太网的平均通信量远小于以太网的最高数据率

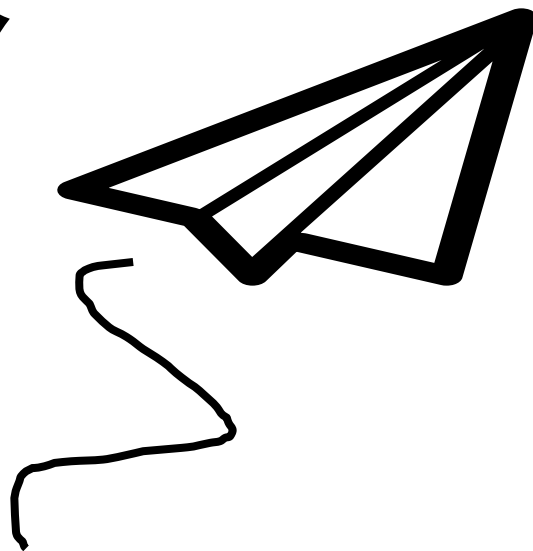
■ 争用期

- 最先发送数据帧的站，在发送数据帧后至多经过时间 2τ （两倍的端到端传播时延）就可知道发送的数据帧是否遭受了碰撞
- 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

本章导航与要点



本节课程结束



无冲突的协议



- 基本位图协议
 - 预定协议
- 二进制倒数计数法
 - 站号仲裁，高序号优先
 - 变种：动态站号

基本位图协议 (A Bit-Map Protocol)



■ 工作原理

- 共享信道上有多N个站，竞争周期分为N个时槽，如果一个站有帧发送，则在对应的时槽内发送比特1
- N个时槽之后，每个站都知道哪个站要发送帧，这时按站序号顺序发送



基本位图协议(2)



- 象这样在实际发送信息前先广播发送请求的协议称为预定(reservation)协议
- 效率
 - 轻负载下, 效率为 $d / (N + d)$, 数据帧由d个时间单位组成
 - 重负载下, 效率为 $d / (d + 1)$
- 缺点
 - 与站序号有关的不平等性, 序号大的站得到的服务好
 - 每个站都有 1 比特的开销

二进制倒数计数法(Binary Countdown)

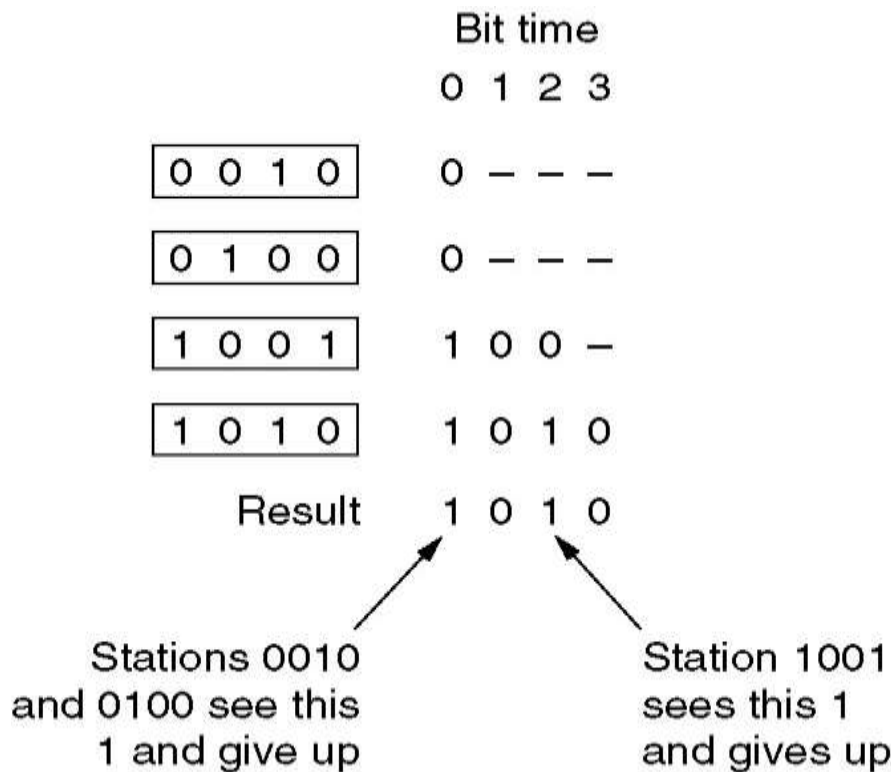


■ 工作原理

- 所有站的地址用等长二进制位串表示，若要占用信道，则广播该位串
- 不同站发的地址中的位做“或”操作，一旦某站了解到比本站地址高位更高的位置被置为“1”，便放弃发送请求

■ 效率

$$d / (d + \log_2 N)$$



有限竞争协议



■ 占用信道的策略

● 竞争方法

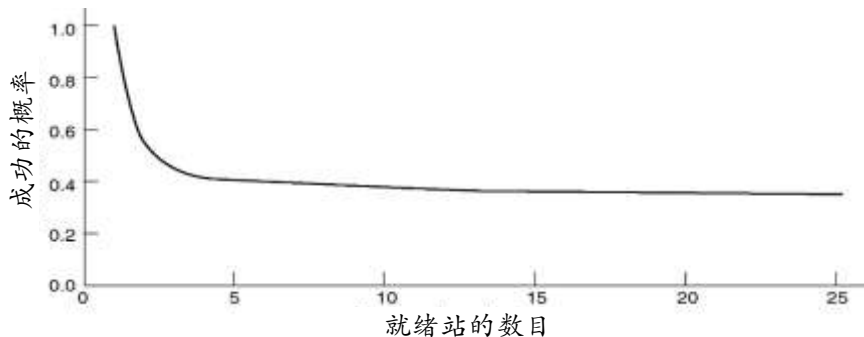
- ◆ 例，CSMA。轻负载下，发送延迟小；重负载下，信道效率低

● 无冲突方法

- ◆ 例，基本位图协议。轻负载下，发送延迟大；重负载下，信道效率高

● 有限竞争方法

- ◆ 结合以上两种方法，轻负载下使用竞争，重负载下使用无冲突方法
- ◆ 减少竞争的站的数目可以增加获取信道的概率
- ◆ 基本思路：将站分组，组内竞争
- ◆ 问题：如何分组？

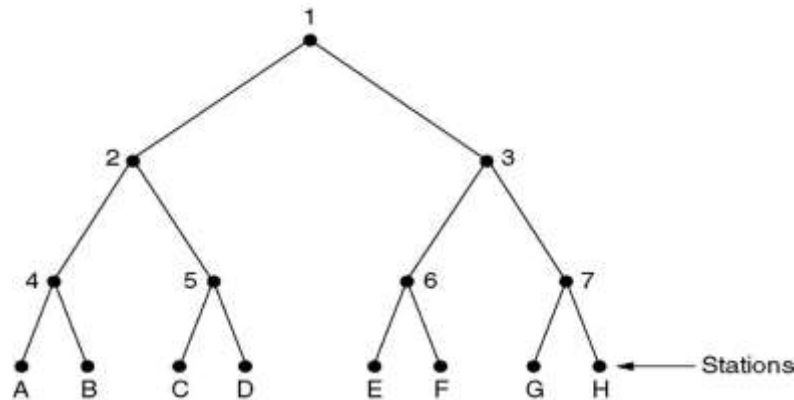


自适应树遍历协议



■ 工作原理

- 站点组织成二叉树
- 一次成功传输之后，第0槽全部站可竞争信道，只有一个站要使用信道则发送；有冲突则在第1槽内半数站（2以下站）参与竞争。如其中之一获得信道，本帧后的时槽留给3以下的站；如发生冲突，继续折半搜索



■ 效率

- 当系统负载很重时，从根结点开始竞争发生冲突的概率非常大
- 为提高效率，可以从中间结点开始竞争
- 问题：遍历应该从树的哪一级开始？

无线局域网协议



■ 无线局域网产生背景

- 笔记本电脑的普及促进了无线局域网的发展
- portable \neq mobile
- 要做到真正的移动，需要使用无线信号进行通信

■ 无线局域网的特点

- 基于蜂窝 (cell) 的通信
- 每个蜂窝内只有一个信道 (与蜂窝电话不同)
- 一个站点发送的信号，只能被它周围一定范围内的站点接收到
- 短距离传输

无线局域网的不同

■ 基站、移动站

- 隐藏站点问题(侦听不到)



- 暴露站点问题(侦听无关通讯)



无线局域网的不同(2)



■ 隐藏站点问题 (hidden station problem)

- 由于站点距离竞争者太远，从而不能发现潜在介质竞争者的问题称为隐藏站点问题
- A向B发送数据的过程中，C由于收不到A的数据，也可以向B发送数据，导致B接收发生冲突

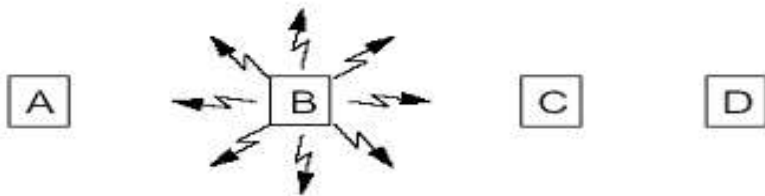


无线局域网的不同(3)



■ 暴露站点问题 (exposed station problem)

- 由于非竞争者距离发送站点太近，从而导致介质非竞争者不能发送数据的问题称为暴露站点问题
- B向A发送数据，被C监听到，导致C不能向D发送数据



无线局域网的不同(4)



■ CSMA

- 在电缆上，信号传播给所有站点
- CSMA只判断本发送站点周围是否有活跃发送站点
- 冲突被发送站点发现
- 某一时刻，信道上只能有一个有效数据帧

■ 无线局域网

- 信号只能被发送站点周围一定范围内的站点接收
- MAC子层协议需要尽量保证接收站点周围一定范围内只有一个发送站点。
- 冲突被接收站点发现
- 某一时刻，信道上可以有多个有效数据帧

MACA冲突避免多路访问



■ 冲突避免多路访问 (Multiple Access with Collision Avoidance)

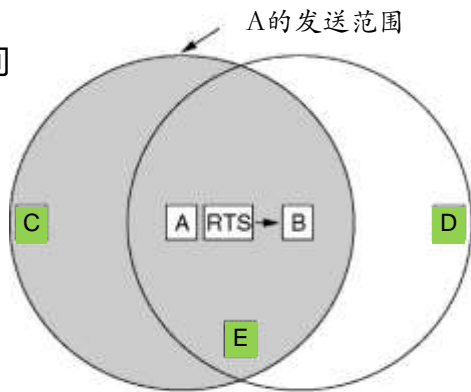
● IEEE 802.11无线局域网标准的基础，基本过程：

- ◆ A向B发送RTS(Request To Send)帧，A周围的站点在一定时间内不发送数据，以保证CTS帧返回给A
- ◆ B向A回答CTS(Clear To Send)帧，B周围的站点在一定时间内不发送数据，以保证B接收完数据
- ◆ A开始发送
- ◆ 若发生冲突，等待随机时间

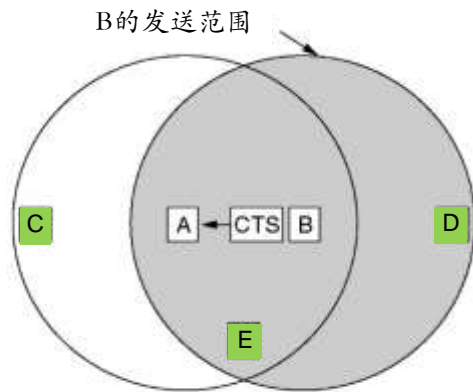
C: 能听到A的RTS，静默一段时间，确保A收到CTS；听不到B的CTS，之后可以发送信息

D: 听不到A的RTS，能听到B的CTS，根据CTS确定静默时间

E: 两条信息都能听到，处理与D相同



(a) A给B发送一个RTS



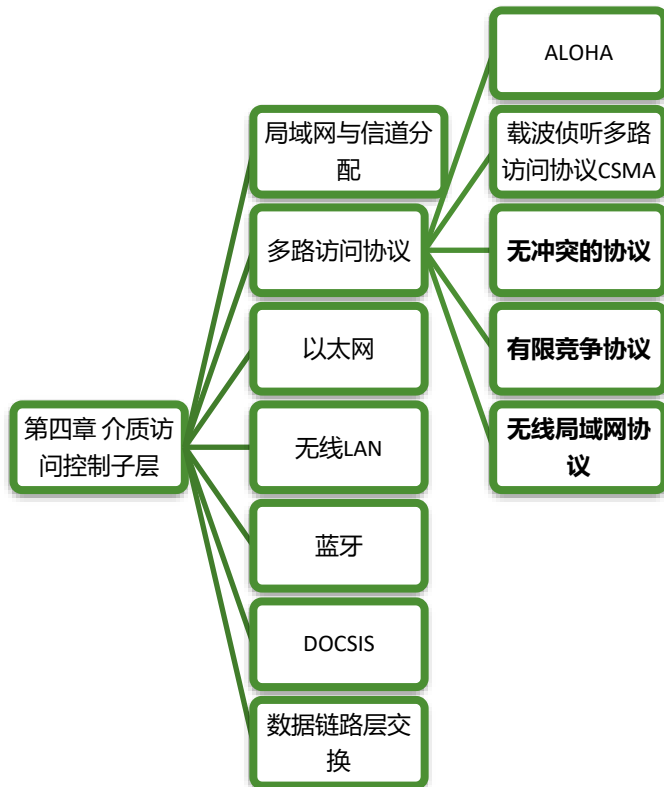
(b) B给A返回一个CTS

本节小节

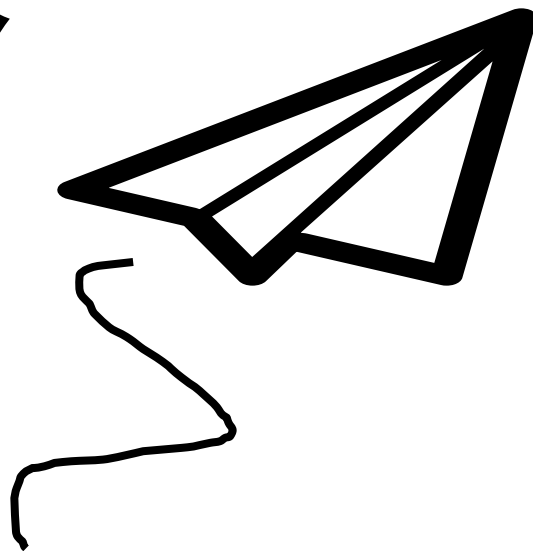


- 关键问题：在MAC子层，如何解决多个站点争用共享信道？
- 信道分配方式：静态(FDM、WDM、TDM)，动态
- 多路访问协议
 - ALOHA：纯ALOHA、分槽ALOHA，（冲突危险周期）
 - CSMA：1-坚持型CSMA、非坚持型CSMA、p-坚持型，（分槽协议）
 - CSMA/CD
- 无冲突协议、有限竞争协议
- 无线局域网协议

本章导航与要点



本节课程结束



4.3 以太网



- 以太网标准
- 经典以太网物理层
- 经典以太网MAC子层
- 交换式以太网
- 快速以太网
- 高速以太网

以太网标准



- IEEE802标准
- 802标准在网络体系结构中的位置
- 局域网的参考模型

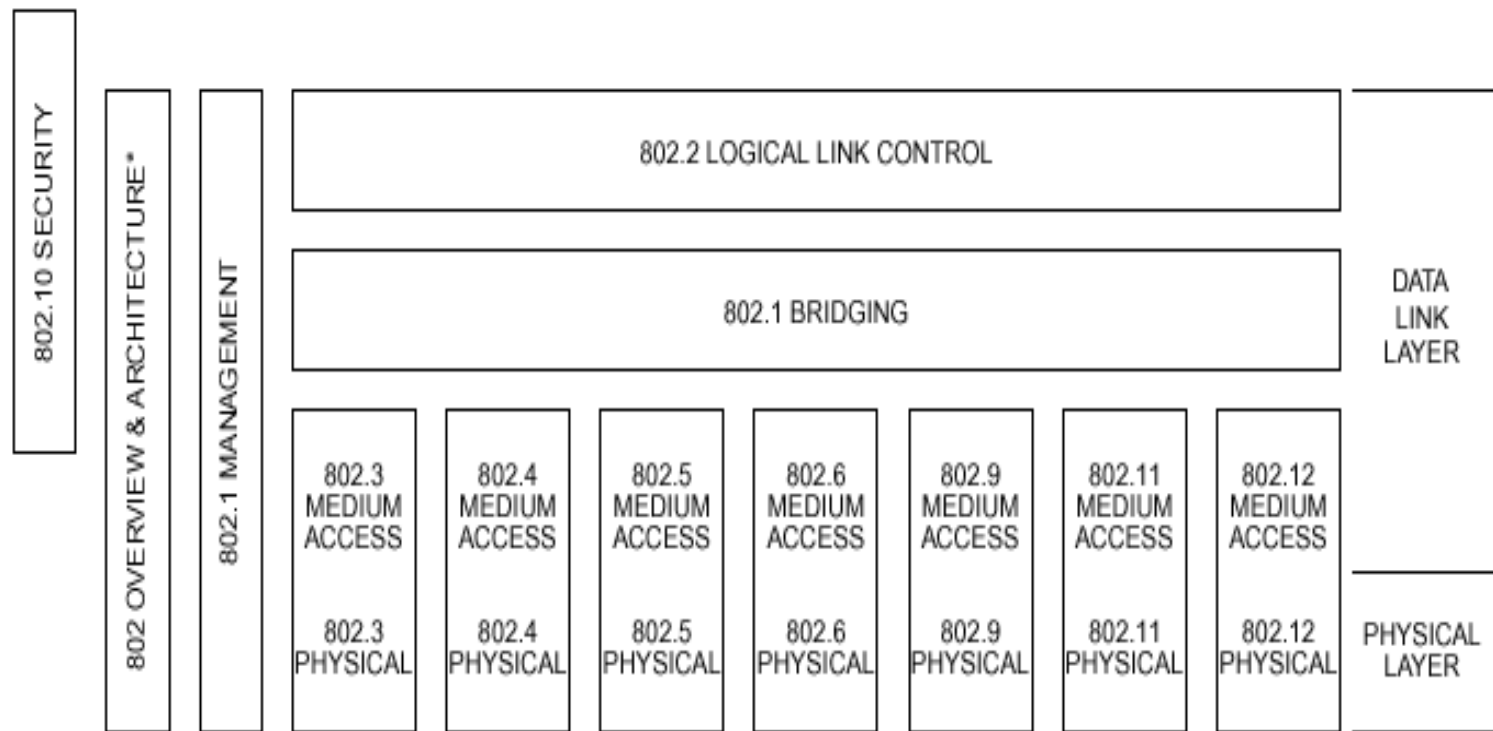
IEEE802标准



- IEEE802.1标准: 总体介绍, 定义接口原语
- IEEE802.2标准: 逻辑链路控制(LLC)
- IEEE802.3标准: CSMA/CD(以太网)
- IEEE802.4标准: 令牌总线
- IEEE802.5标准: 令牌环
- IEEE802.6标准: 城域网MAN,分布队列双路总线
- IEEE802.7标准: 宽带技术
- IEEE802.8标准: 光纤技术
- IEEE802.9标准: 综合话音数据局域网
- IEEE802.10标准: 可互操作的局域网的安全
- IEEE802.11标准: 无线局域网
- IEEE802.12标准: 优先级高速局域网(100Mb/s)
- IEEE802.14标准: 有线电视(Cable-TV)
- IEEE802.15标准: 蓝牙
- IEEE802.16标准: 无线MAN



802标准在网络体系结构中的位置



* Formerly IEEE Std 802.1A.



局域网的参考模型

■ 逻辑链路控制子层 LLC (Logical Link Control)

- 引入LLC子层的原因
 - ◆ MAC子层只提供尽力而为的数据报服务，不提供确认机制和流量控制（滑动窗口），有些情况下，这种服务足够，如支持IP协议；当需要确认和流控的时候，这种服务就不能满足，需要LLC
- LLC子层提供确认机制和流量控制
- LLC隐藏了不同802MAC子层的差异，为网络层提供单一的格式和接口
- LLC提供三种服务选项
 - ◆ 不可靠数据报服务
 - ◆ 有确认数据报服务
 - ◆ 可靠的面相连接的服务
- LLC帧首部基于HDLC协议



局域网的参考模型(2)

■ 介质访问控制子层 MAC (Medium Access Control)

- 数据封装 (发送和接收)
 - ◆ 成帧 (帧定界、帧同步)
 - ◆ 寻址 (源和目的地址处理)
 - ◆ 差错检测
- 介质访问管理
 - ◆ 介质分配 (冲突避免)
 - ◆ 冲突解决 (处理冲突)

■ 分成两个子层的原因

- 管理多点访问信道的逻辑不同于传统的数据链路控制
- 对于同一个LLC, 可以提供多个MAC选择

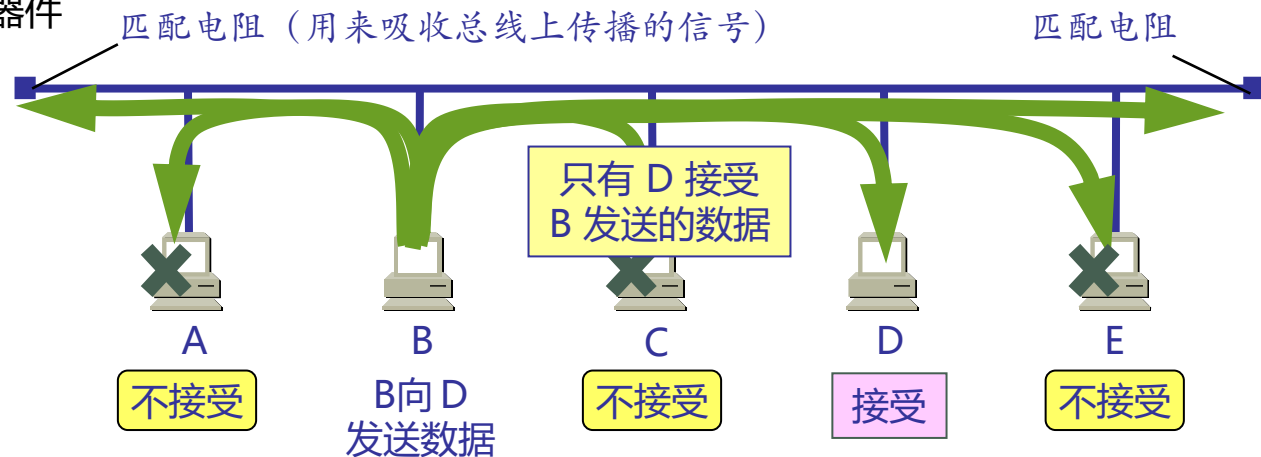
经典以太网物理层



- 早期的以太网
- 早期以太网的连接方式
- 星形以太网与集线器
- 以太网的最大作用距离

早期的以太网

- 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



- 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
- 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
- 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
- 具有广播特性的总线上实现了一对一的通信



以太网提供的服务

■ 简化措施

- 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很小

■ 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确定
- 如果高层发现丢失了一些数据而进行重传，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

早期以太网的连接方法

- 传统以太网可使用的传输介质有四种：

802.3采用的电缆标准

- 铜缆（粗缆或细缆）

- 铜线（双绞线）

- 光缆

名 称	电 缆	最大区间长度	节点数/段	优 点
10Base5	粗同轴电缆	500m	100	早期用于主干
10Base2	细同轴电缆	185m	30	不需要集线器
10Base-T	双绞线	100m	1024	易于维护
10Base-F	光纤	2000m	1024	最适于楼宇间

- 这样，以太网就有四种不同的物理层。

以太网介质访问控制 MAC

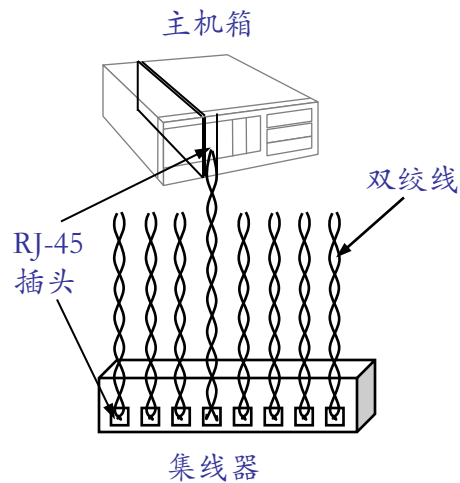
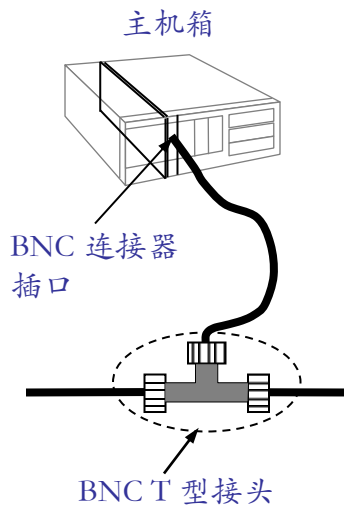
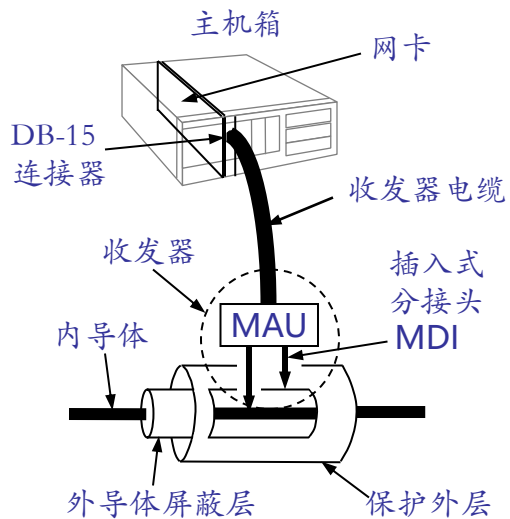
10BASE5
粗缆

10BASE2
细缆

10BASE-T
双绞线

10BASE-F
光缆

铜缆或铜线连接到以太网的示意图



以太网的最大作用距离



■ 粗缆为例

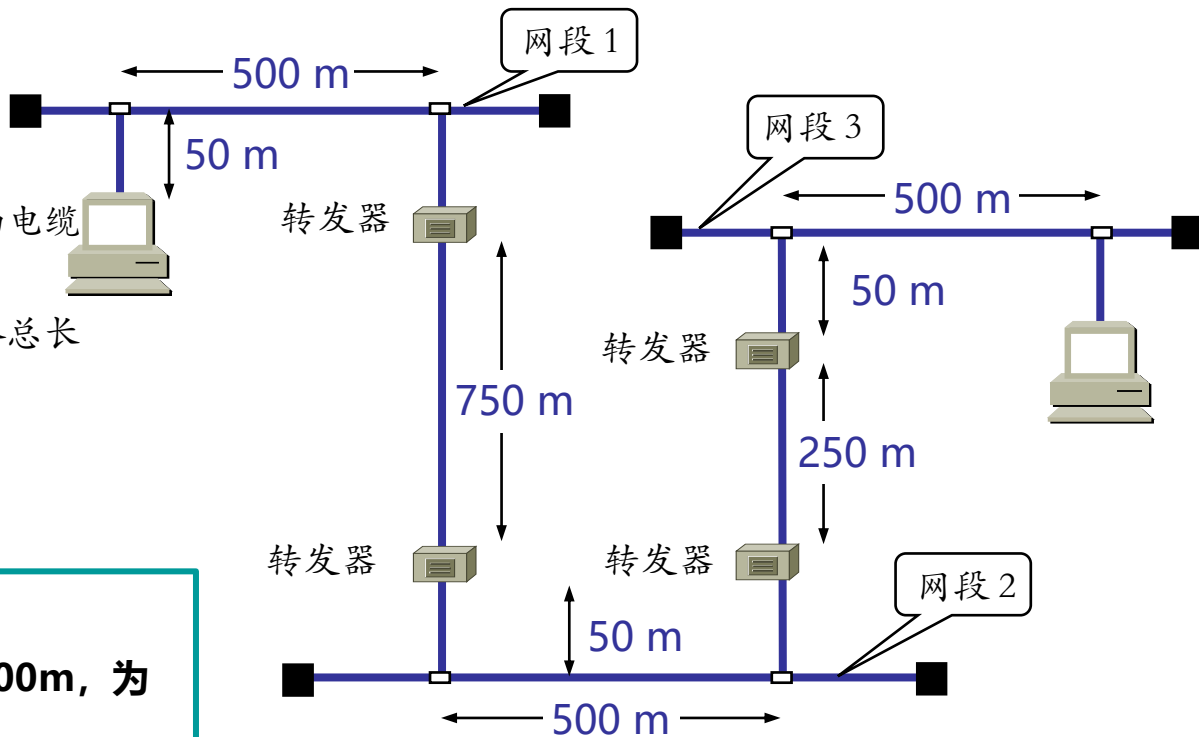
802.3规定:

- 任意两站间最多三个铜轴电缆段，最多四个转发器
- 接到转发器的点到点链路总长不超过1000m
- 网上最大站点数1024

以太网最大长度2500m

思考题 4.3-1:

以太网规定最大长度为2500m，为什么？



星形以太网与集线器



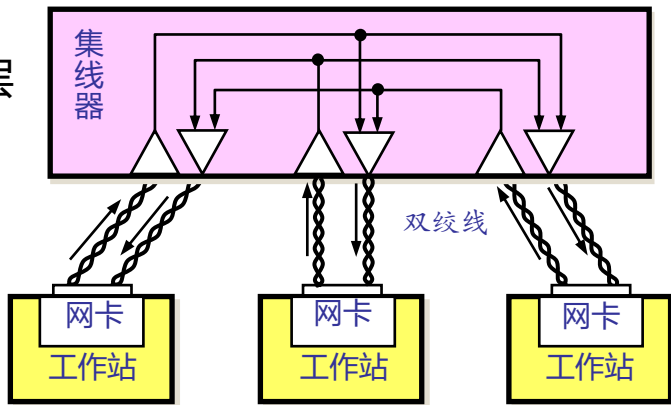
- 不用电缆而使用无屏蔽双绞线。每个站需要用两对双绞线，分别用于发送和接收
- 在星形网的中心则增加了一种可靠性非常高的设备，叫做集线器(hub)
 - 集线器使用了大规模集成电路芯片，因此这样的硬件设备的可靠性已大大提高了
- 10BASE-T的地位
 - 10BASE-T 的通信距离稍短，每个站到集线器的距离不超过 100m
 - 这种 10 Mb/s 速率的无屏蔽双绞线星形网的出现，既降低了成本，又提高了可靠性
 - 10BASE-T 双绞线以太网的出现，是局域网发展史上的一个非常重要的里程碑，它为以太网在局域网中的统治地位奠定了牢固的基础

集线器的一些特点

■ 特点

- 集线器是使用电子器件来模拟实际电缆线的工作，因此整个系统仍然像一个传统的以太网那样运行
- 使用集线器的以太网在逻辑上仍是一个总线网，各工作站使用的还是CSMA/CD 协议，并共享逻辑上的总线
- 集线器很像一个多端口的中继器，工作在物理层

■ 具有三个端口的集线器



经典以太网MAC子层

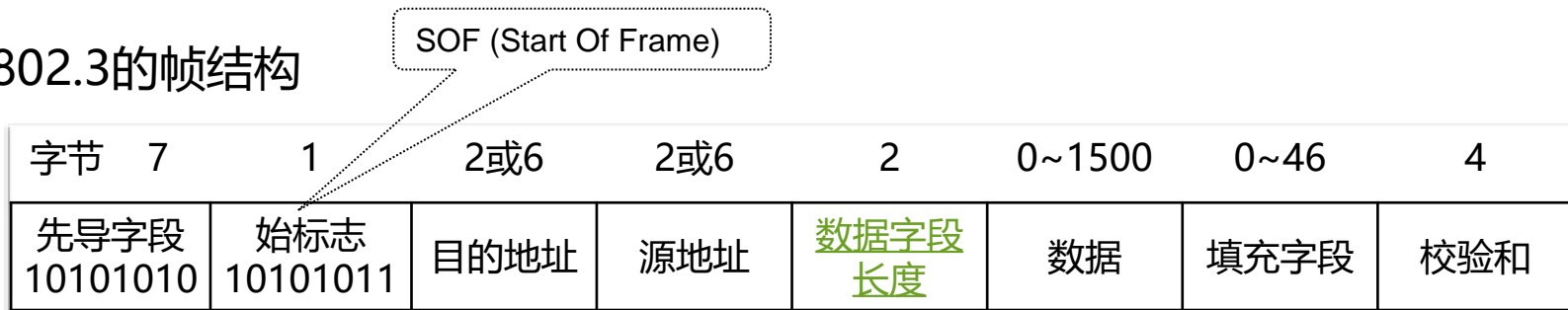


- MAC帧结构
- MAC地址
- 冲突检测时间
- 二进制指数后退算法
- 以太网性能

MAC帧结构



■ 802.3的帧结构

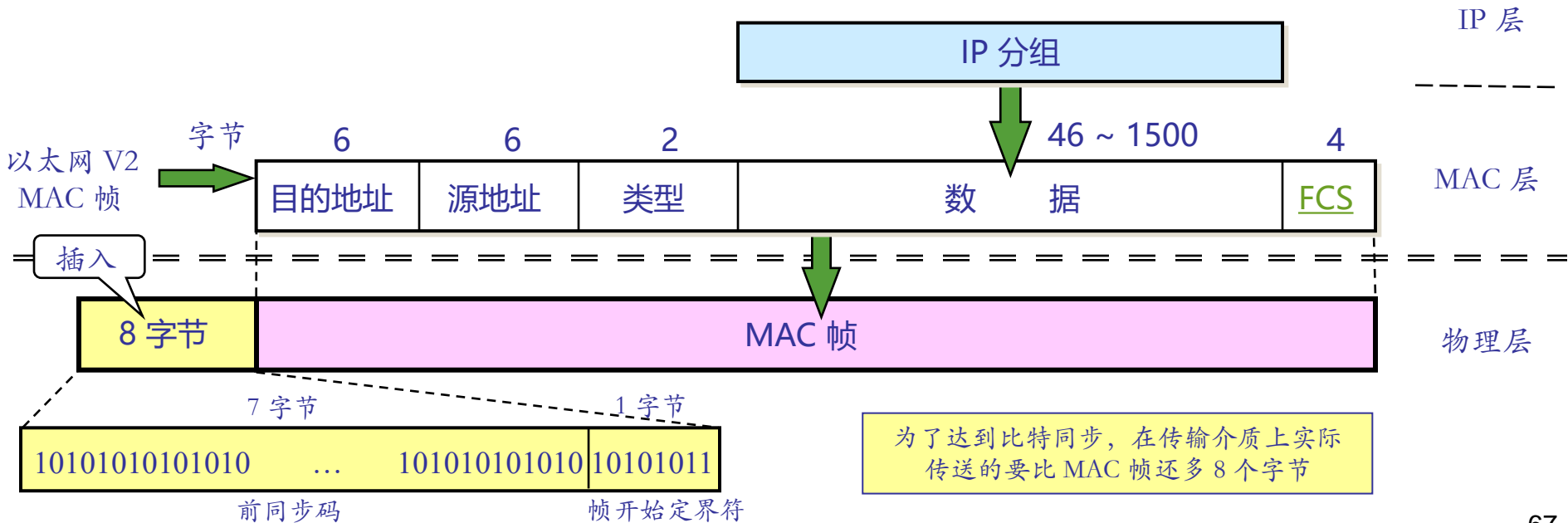


- 地址 (以太网为6个字节)
 - ◆ 目标地址第一位(I/G, Individual/Group): 0表示单播地址, 1表示组播地址; 广播发送(目的地址全1)
 - ◆ 第二位(G/L, Global/Local): 0表示局部地址, 1表示全局地址; (以太网基本不用)
- 数据字段长度: 0~1500
- 填充字段: 数据少于46字节则填充
- 校验和(CRC)



MAC帧结构(2)

■ 以太网V2 (DIX Ethernet II) 的帧结构



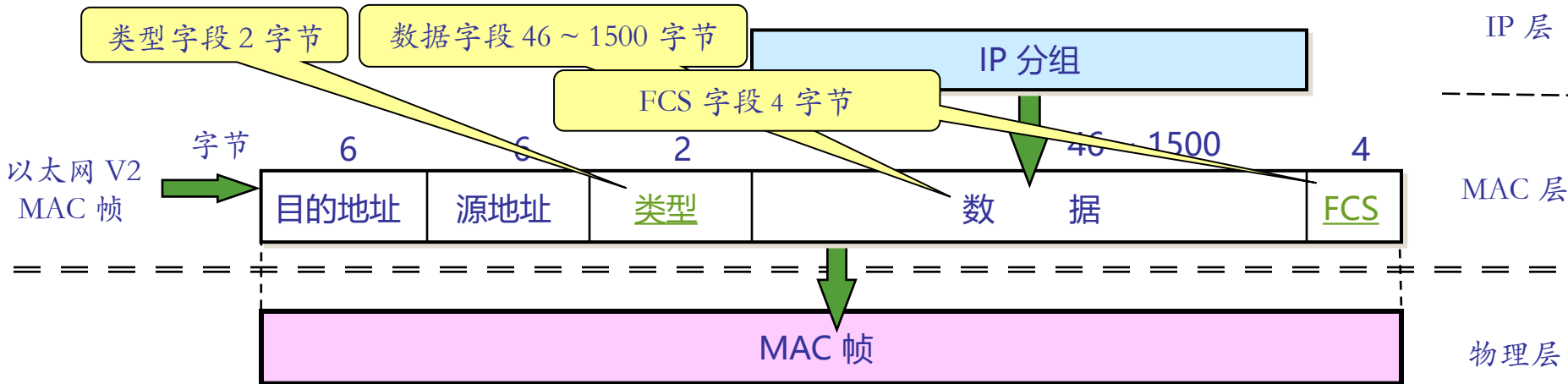
MAC帧结构(3)

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 (DIX Ethernet II) 的帧结构

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

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



所幸的是，IEEE802.3的帧定义的有效长度值，
与Ethernet II帧定义的有效类型值无一相同，
这样就容易区分两种帧格式了

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

类型字段还是长度字段



- 除了吉比特以太网之外的所有以太网版本，如果传输数据少于46个字节，应将数据字段填充至46字节
(注意，填充字符的个数不包括在长度字段值中)
- 同时支持以太网和IEEE 802.3帧格式的网络接口卡，通过这一字段的值区分这两种帧（已解决二者的不兼容）
 - 也就是说，因为数据字段的最大长度为1500字节，所以超过十六进制数05DC的值说明它不是长度字段（IEEE802.3），而是类型字段（Ethernet II）
(例如：0x0800代表IP协议帧，0x8137代表IPX和SPX协议帧)

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

MAC地址

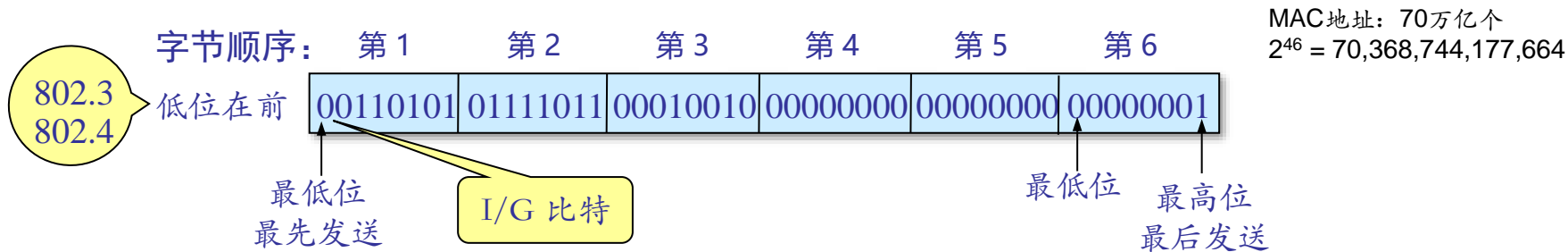
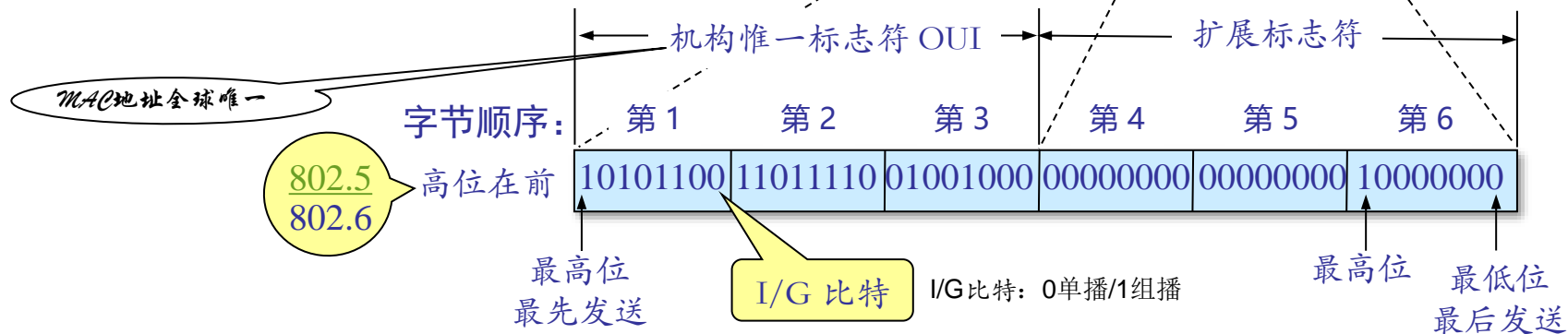
十六进制表示的 EUI-48 地址:

AC-DE-48-00-00-80

第 1 字节

第 6 字节

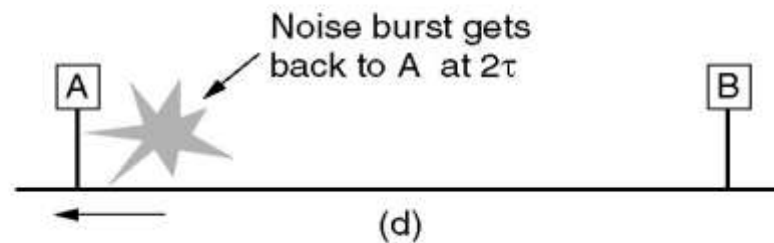
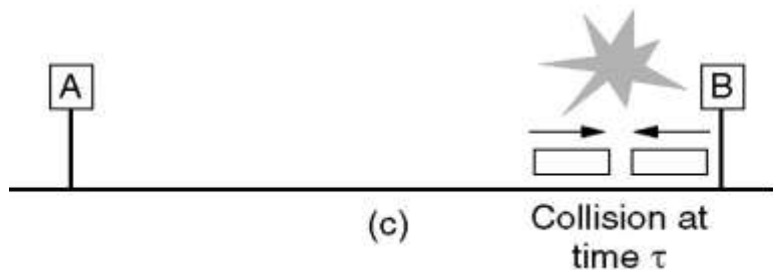
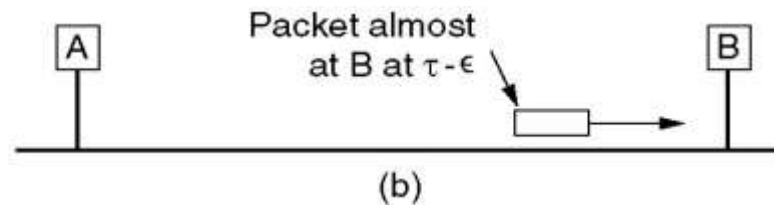
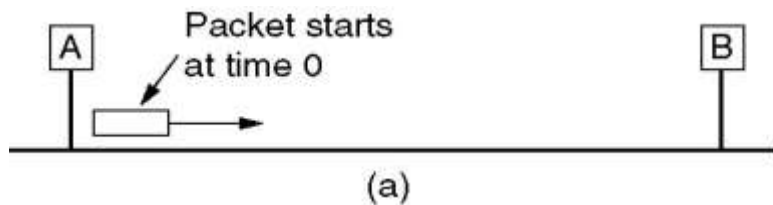
二进制表示的 EUI-48 地址:



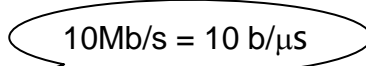
冲突检测时间

■ 最短帧长

- 避免帧的第一个比特到达电缆的远端前帧已经发完，帧发送时间应该大于 2τ



争用期的长度


$$10\text{Mb/s} = 10\text{ b}/\mu\text{s}$$

■ 以太网取 $51.2\ \mu\text{s}$ 为争用期的长度

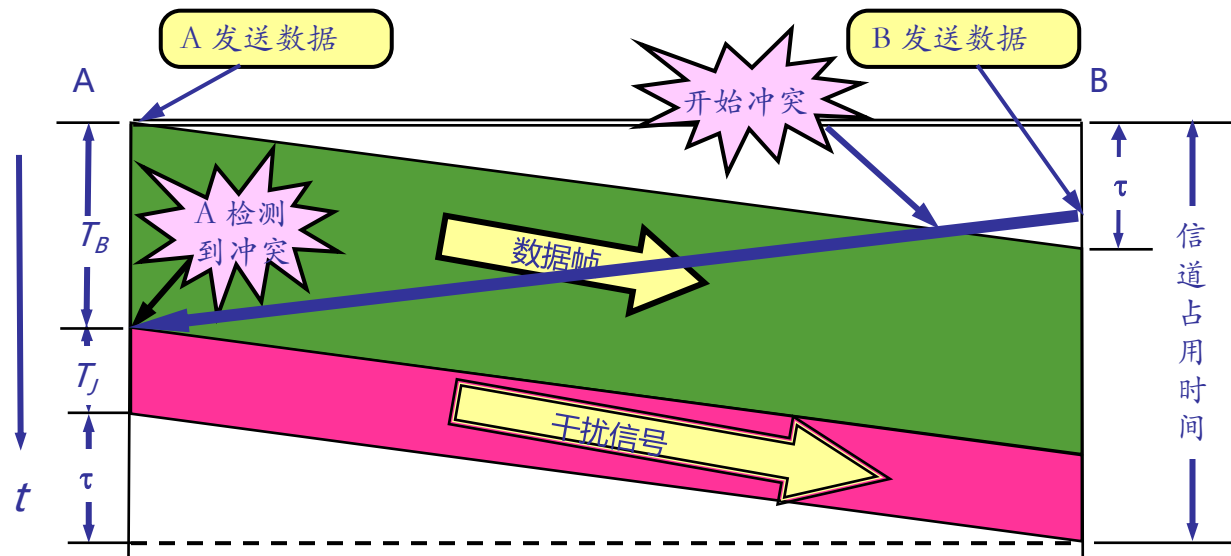
- 对于 10 Mb/s 以太网，在争用期内可发送 512 bit ，即 64 字节
- 以太网在发送数据时，若前 64 字节 没有发生冲突，则后续的数据就不会发生冲突，即若发生冲突，一定是在发送的前 64 字节 之内
- 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节
- 以太网规定了最短有效帧长为 64 字节 ，凡长度小于 64 字节 的帧都是由于冲突而异常中止的无效帧

■ 网络速度提高，最短帧长也应该增大或者站点间的距离要减小

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

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。



二进制指数后退算法



■ 发生碰撞的站，在停止发送数据后，要推迟（退避）

一个随机时间才能再发送数据

- 确定基本退避时间，一般是取为争用期 2τ

- 定义重传次数 i ， $i \leq 10$ ，即

- $i = \text{Min}[\text{重传次数}, 10]$

- 从整数集合 $[0, 1, \dots, (2^i - 1)]$ 中随机地取出一个数，记为 r

- 重传所需的推迟时间就是 r 倍的基本退避时间

- 当重传达 16 次仍不能成功时，即丢弃该帧，并向高层报告

- 时隙 (2τ) : $51.2\mu\text{s}$,
 $64\text{B}=512\text{b}$ 时间

- 第一次， $0 \sim 1$

- 第二次， $0 \sim 3$

-

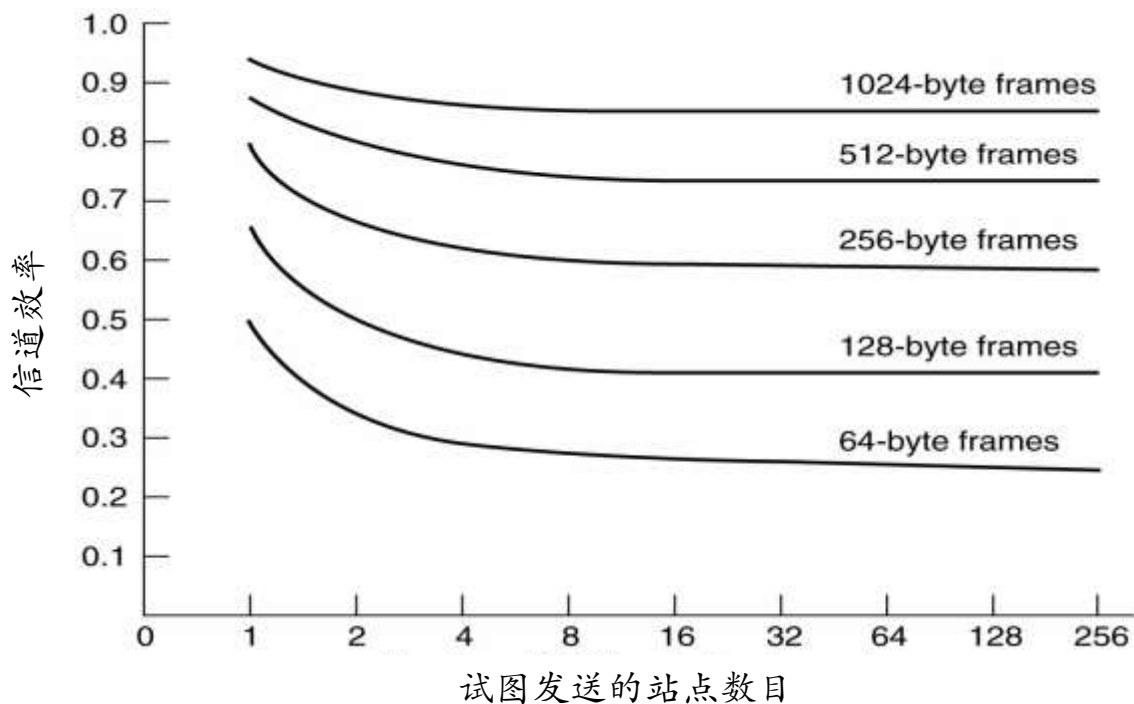
- 第 i 次， $0 \sim 2^i - 1$

- $i > 10$ ， $0 \sim 1023$

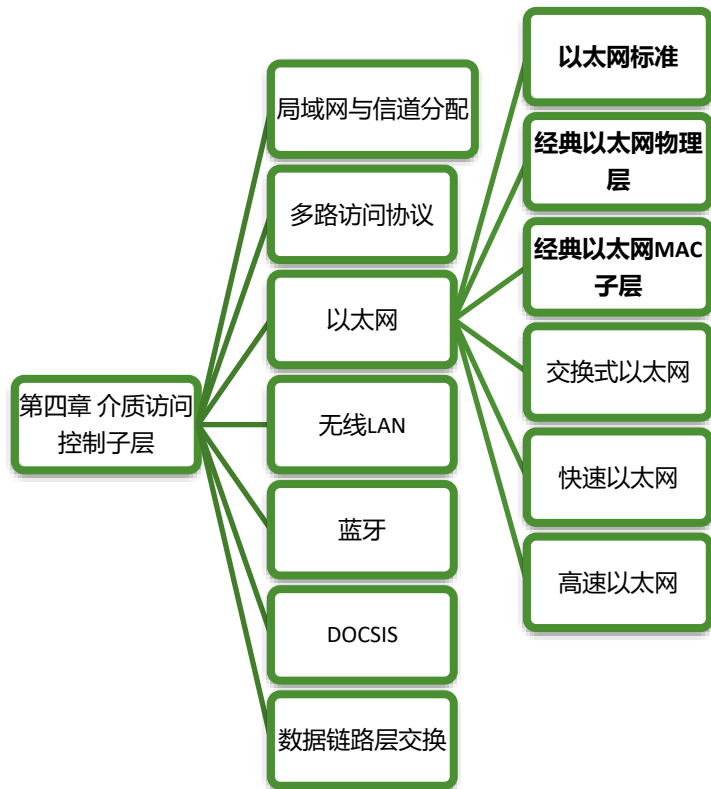
- $i > 16$ ，失败

以太网性能

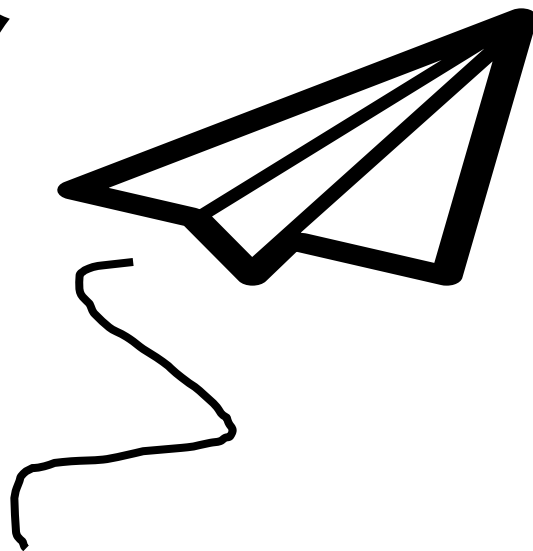
■ 具有512位时隙的10Mbps以太网效率



本章导航与要点



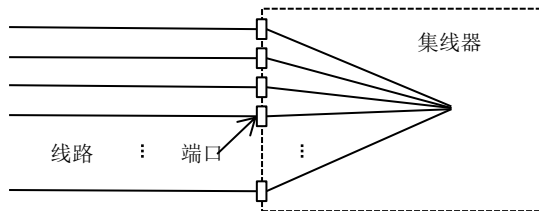
本节课程结束



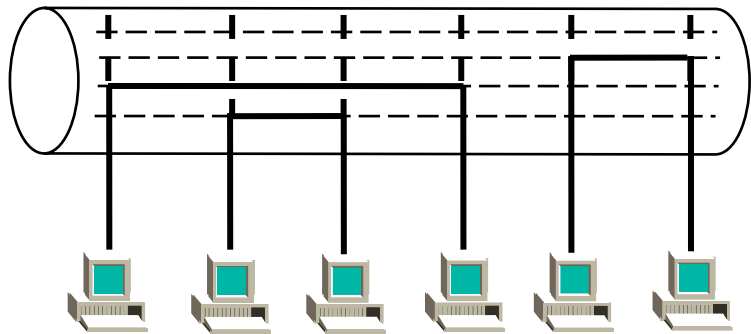
交换式以太网



- 集线器 (802.3) :
- 交换目的: 减少冲突



交换背板矩阵 (多网段)

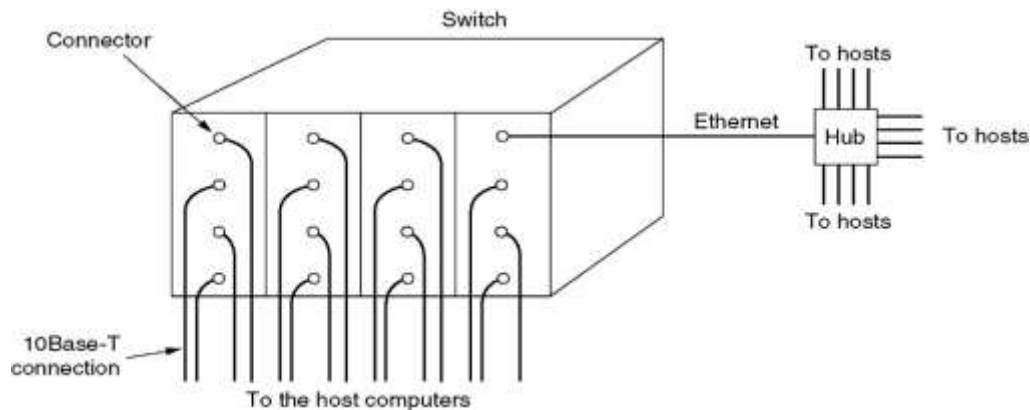


- 两种实现方法
 - 一个卡内是一个802.3LAN, 构成自己的冲突域, 卡间并行
 - 使用端口缓存, 无冲突发生

交换背板

■ 冲突域

- 插板：插板为局域网CSMA/CD
- 端口：插板（为单位）采用缓存



以太网交换机



■ 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介质那样，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，其交换速率较高

■ 以太网交换机的带宽（10 Mb/s）

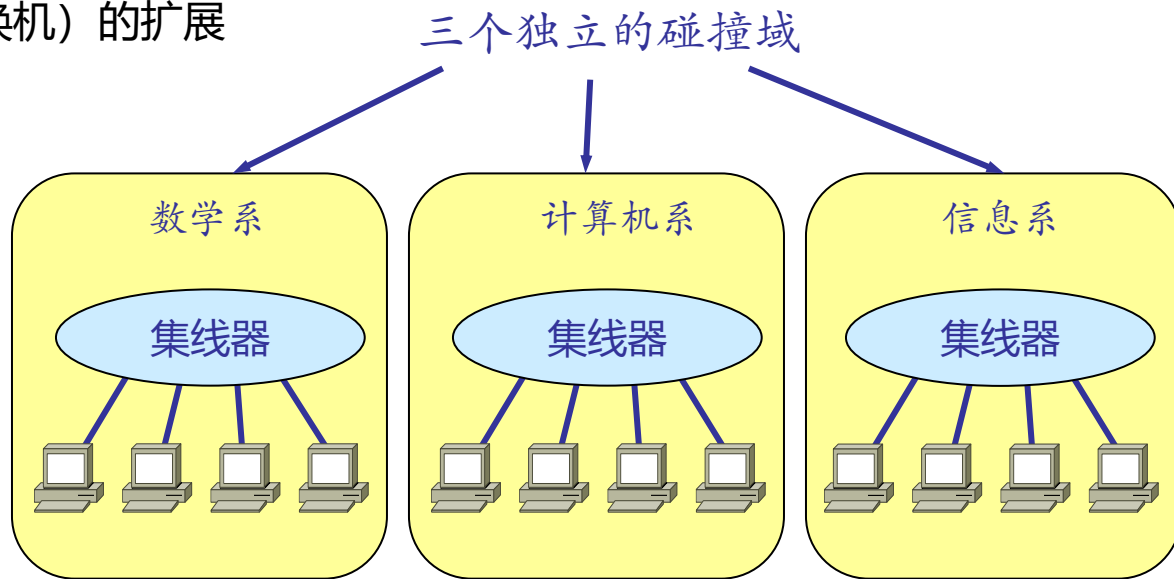
- 对于共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽的 N 分之一
- 使用以太网交换机时，虽然在每个端口的带宽还是 10 Mb/s，但由于一个用户在通信时是独占而不是和其他网络用户共享传输介质的带宽，因此对于拥有 N 对端口的交换机的总容量为 $N \times 10 \text{ Mb/s}$

局域网的扩展



■ 用多个集线器可连成更大的局域网

- 物理层（集线器）的扩展
- 数据链路层（交换机）的扩展





在物理层扩展

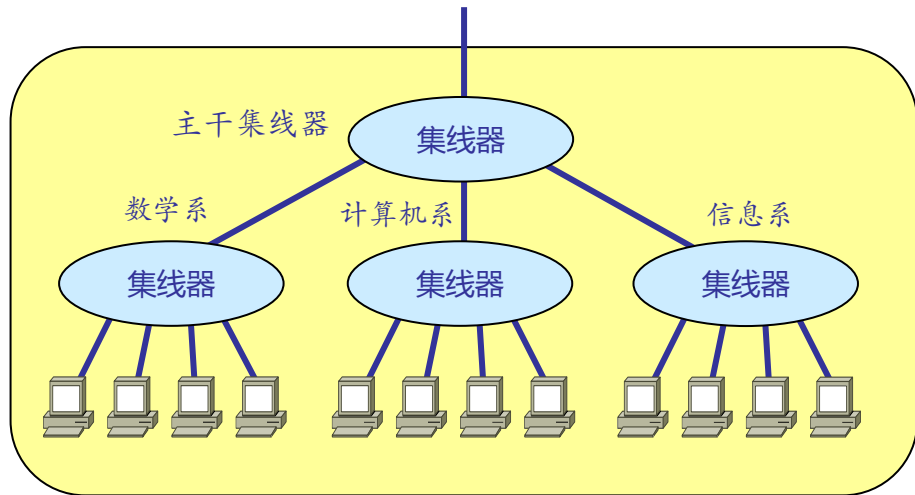
■ 用多个集线器可连成更大的局域网

■ 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

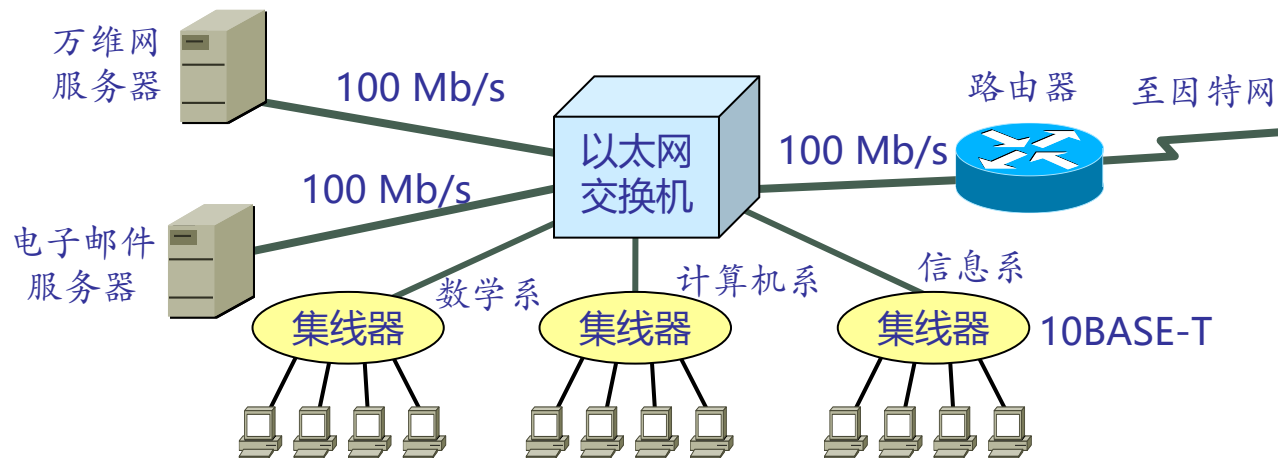


在数据链路层扩展



- 在数据链路层扩展局域网是使用网桥
- 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

用以太网交换机扩展



快速以太网



■ 对10 Mbps 802.3 LAN的改进

- 一种方法是改进10Base-5或10Base-2，采用CSMA/CD，最大电缆长度减为1/10，未采纳
- 另一种方法是改进10Base-T，使用HUB，被采纳

■ 标准

- 1995年，IEEE通过802.3u标准，实际上是802.3的一个补充
- 原有的帧格式、接口、规程不变，只是将比特时间从100ns缩短为10ns

■ 冲突域

- 半双工：集线器HUB，一个冲突域，采用CSMA/CD算法
- 全双工：交换机，输入帧被缓存，一个端口构成一个冲突域
- 争用期长度：最小帧长64B(512b)不变（争用期长度为 $5.12 \mu\text{s}$ ），最大线缆长度减为1/10

三种不同的物理层标准



■ 100Base-TX

- 全双工2对5类双绞线，使用125 MHz的信号
- 编码方案：4B/5B编码，5个时钟周期发送4个比特，比特率为： $125 * 4/5 = 100 \text{ Mbps}$
- 100Base-T4 和100Base-TX 统称100Base-T，又称为快速以太网(Fast Ethernet)

名称	线缆	最大分段长度	优点
100Base-T4	UTP	100m	可用3类UTP(4对双绞线)
100Base-TX	UTP	100m	全双工100Mb/s(5类UTP)
100Base-F	光缆	2000m	全双工100Mb/s，长距离

■ 100Base-FX

- 使用2根多模光纤，全双工

更高速的以太网

■ 千兆以太网

- 标准

- ◆ 802.3z

- ◆ 802.3ab

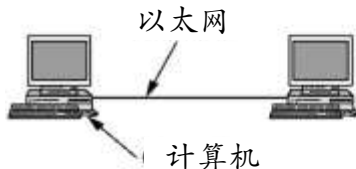
- 载波扩充

- ◆ 由硬件在普通帧后增加填充位，帧长扩充至512字节，接收方硬件删除，软件无须改变

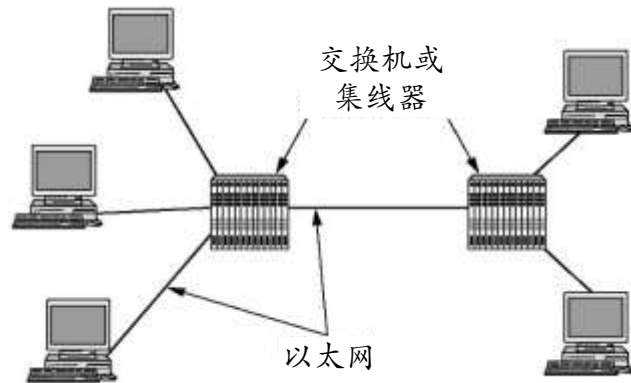
- 帧突发

- ◆ 多个待发帧级连一起发送，长度不够再填充

■ 万兆以太网：802.3an



(a) 包含两个站的以太网



(b) 包含多个站的以太网

千兆以太网



■ 千兆以太网线缆

- 允许全双工或半双工，后者使用标准的CSMA/CD（采用载波扩充或帧突发）

名称	电缆	最大分段长度	优点
1000Base-SX	光纤	550m	多模光纤(50、62.5微米)
1000Base-LX	光纤	5000m	单模光纤(10微米)或多模光纤
1000Base-CX	4对STP	25m	屏蔽双绞线
1000Base-T	4对UTP	100m	标准5类UTP（或超5类）

■ 编码方案：8B/10B，8个数据位编码为10比特码字

- 1000Base-T：使用5类UTP（125M波特），每对同时双向传输，接口采用串扰消除技术
- 1000Base-Tx：使用6类UTP（250M波特），2对发送、2对接收，接口处理较简单

万兆以太网



■ 万兆以太网线缆

- 仅支持全双工，没有CSMA/CD

名称	电缆	最大分段长度	优点
10GBase-SR	光纤	<=300m	多模光纤(波长0.85微米)
10GBase-LR	光纤	10km	单模光纤(波长1.3微米)
10GBase-ER	光纤	40km	单模光纤(波长1.5微米)
10GBase-CX	4对双轴	15m	双轴铜缆
10GBase-T	4对UTP	100m	6a类UTP

■ 编码方案：64B/66B

- 四对同时双向传输，每对速率2500Mbps（800M波特，编码为16个电压等级）

40Gbps和100Gbps以太网



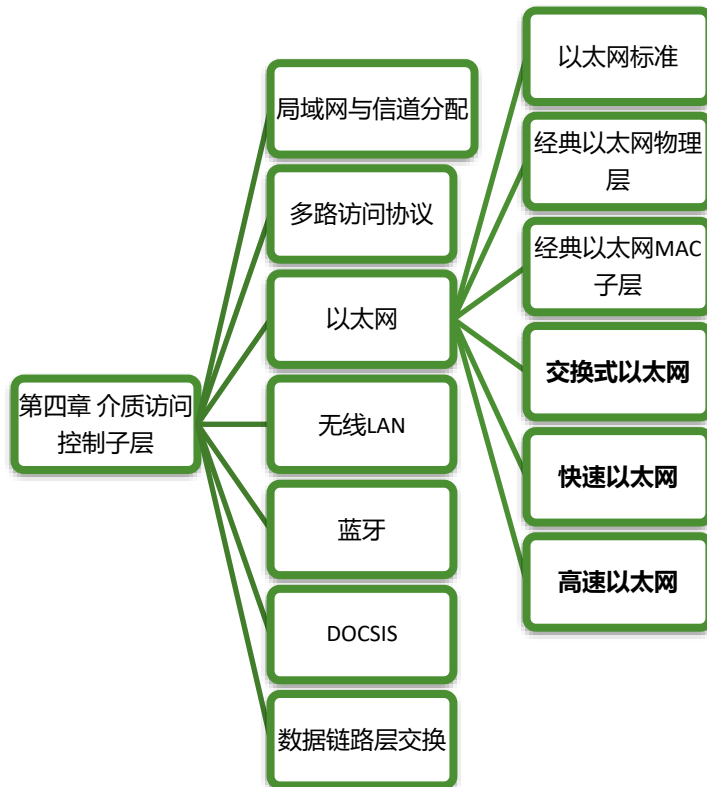
■ 40Gbps和100Gbps以太网标准

IEEE 802.3ba(2010), 802.3bj(2014), 802.3cd(2018)

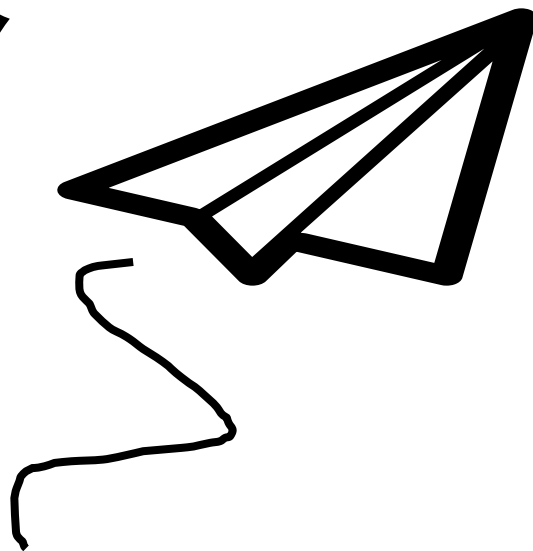
- 兼容1Gbps
- 允许最小和最大帧尺寸保持相同
- 处理 10^{-12} 或更低的比特错误率
- 在光纤网络上很好地工作
- 数据速率为40Gbps或100Gbps
- 允许使用单模或多模光纤以及专用背板

■ 2018之后, 802.3cd(ck,cm,cn)支持400GbE

本章导航与要点



本节课程结束



4.4 无线LAN

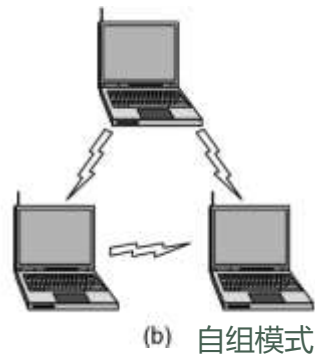
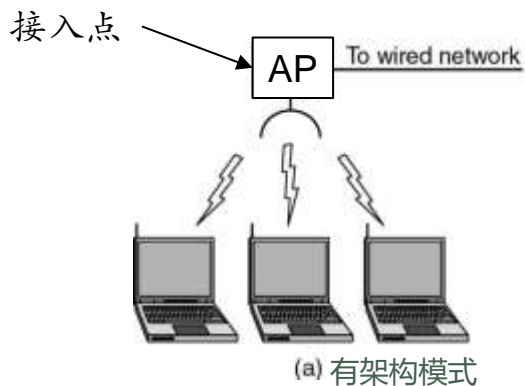


- 802.11体系结构与协议栈
- 802.11 MAC 子层协议
- 802.11 帧结构与服务

802.11体系结构与协议栈

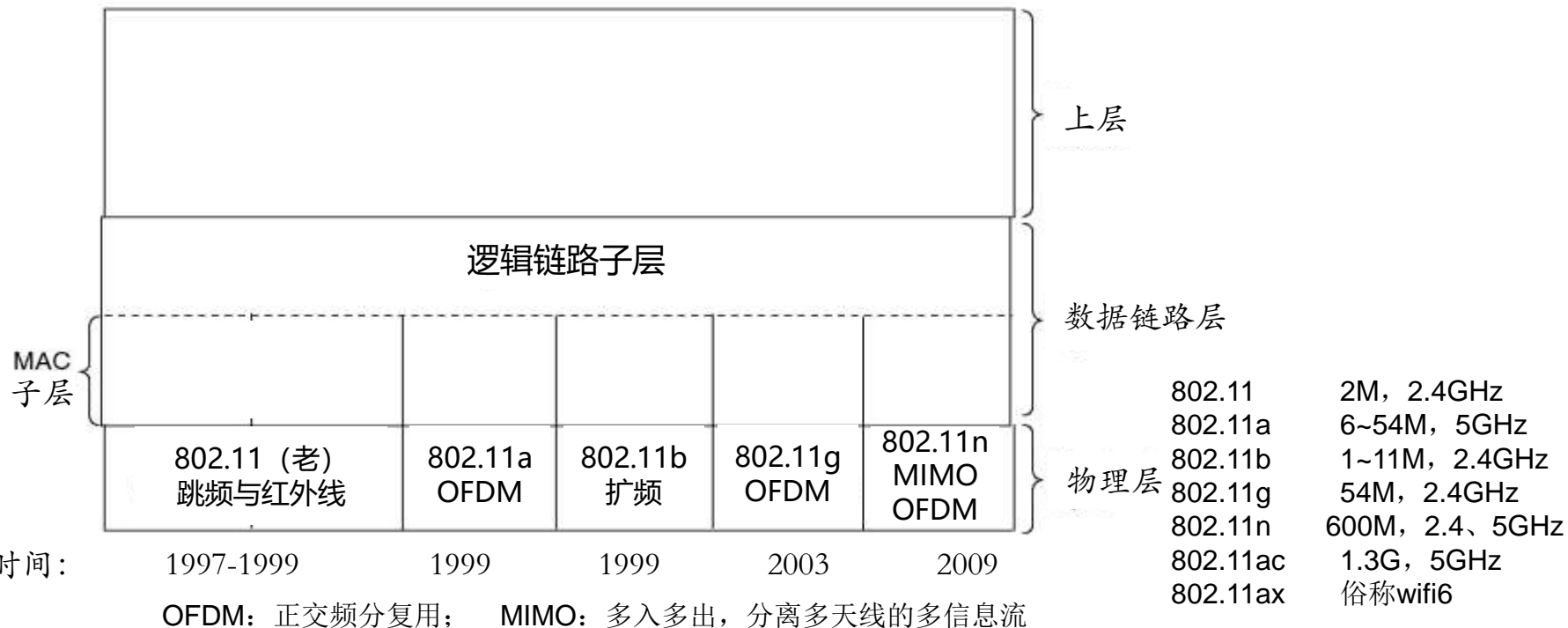


■ 802.11的体系结构



802.11协议栈

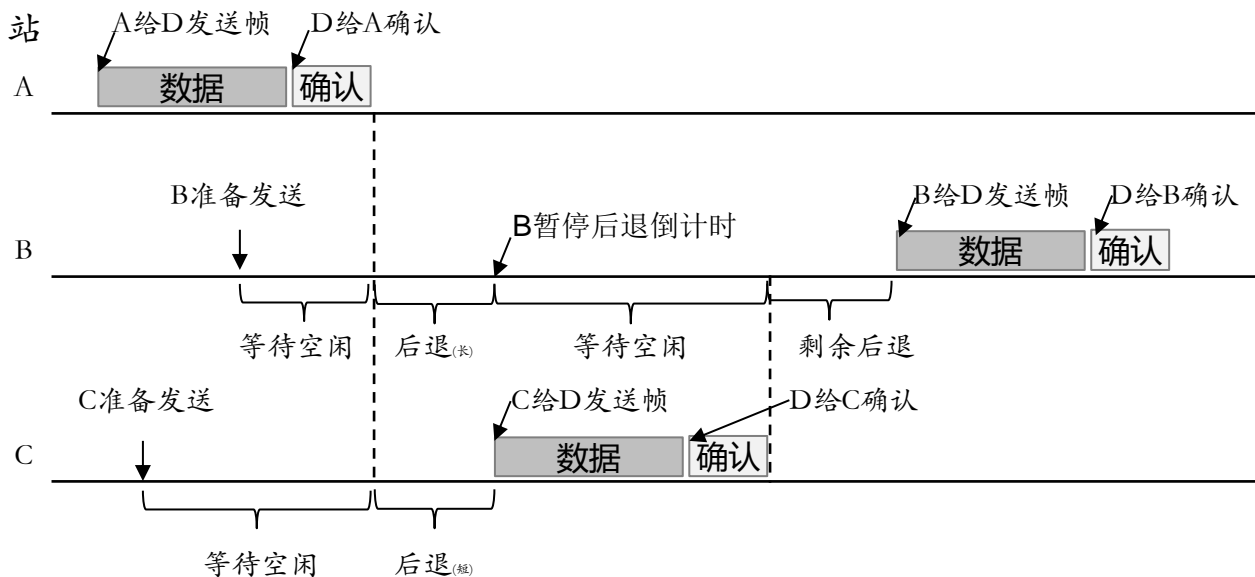
■ 部分802.11协议栈



802.11 MAC 子层协议



- 无线通信的特点：总是半双工；冲突无法检测
- 带有冲突避免的CSMA (CSMA/CA)
 - 在CSMA/CA机制下发送帧：起始后退（随机时长）可以避免冲突，确认可以推测冲突



与802.3的区别



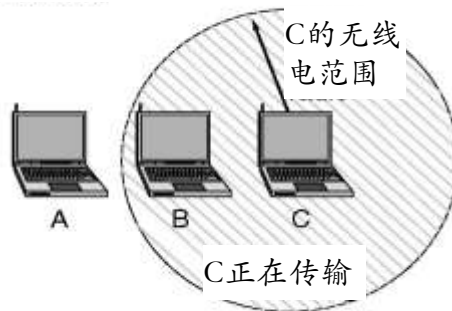
■ 避免冲突的模式

- 分布式协调功能 (DCF, Distributed Coordination Function) : 后退, 确认
- 可选——点协调功能 (PCF, Point Coordination Function) : AP控制覆盖范围内活动
(无法阻止临近网络其他站竞争, 很少使用)

■ 隐藏站点与暴露站点问题

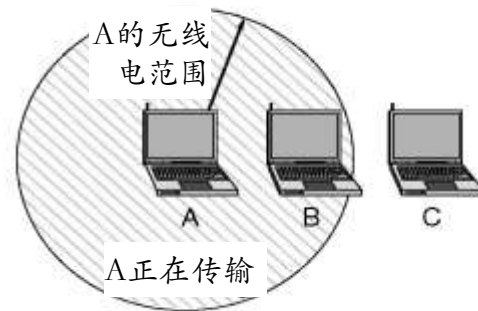
引入信道侦听

A准备发送给B, 却无法
侦听到B正接收数据



(a) 隐藏站点问题

B准备发送给C, 却错误认为会
造成冲突 (A正发送给D)



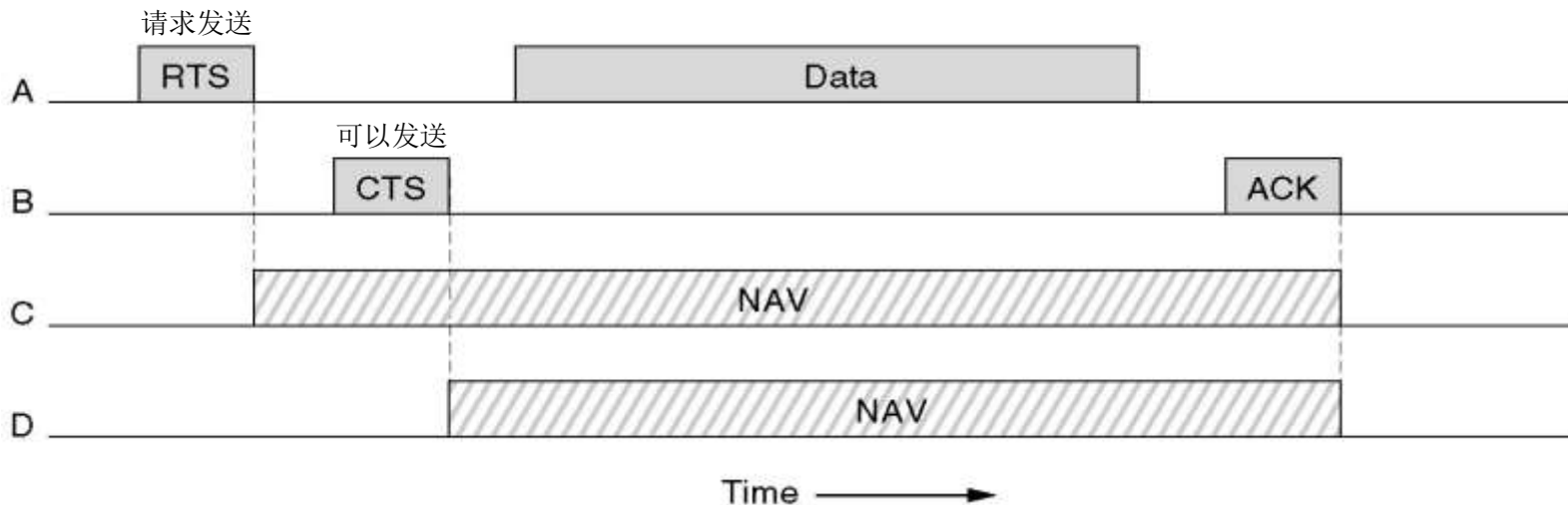
(b) 暴露站点问题

信道侦听



- 物理侦听：直接检查介质
- 虚拟侦听：网络分配向量 (NAV, Network Allocation Vector)
 - 使用CSMA/CA的虚拟信道侦听，帧中的NVA字段说明后续信道繁忙的时间段

无用设计之一：①对短帧和接入（热）点无用；②解决不了暴露站点，只能解决隐藏站点（极少）



802.11协议优化



■ 增加帧成功传输概率

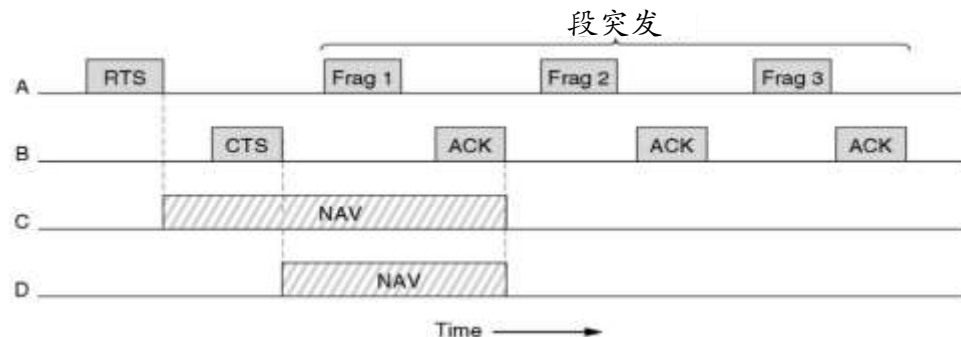
- 调整传输率：出错时降低传输率，无差错时尝试较高传输率
- 发送短帧：一位出错概率为 p ， n 位帧正确接收概率为 $(1-p)^n$

◆ 分段

若 $P=10^{-4}$

帧长12144b，正确率30%

帧长4048b，正确率66%



- 节省电源：入境流量缓存，在信标帧（接入点定时发送）之间或要发送数据为止
- 服务质量：建立不同帧之间的优先级

服务质量

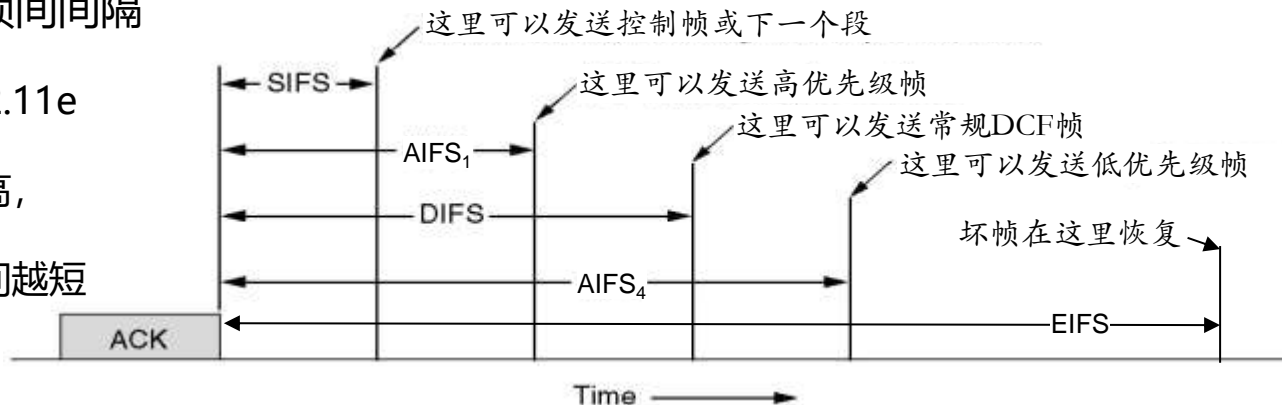


■ 802.11中的帧间间隔

- 标准：802.11e

优先级越高，

帧间隔时间越短



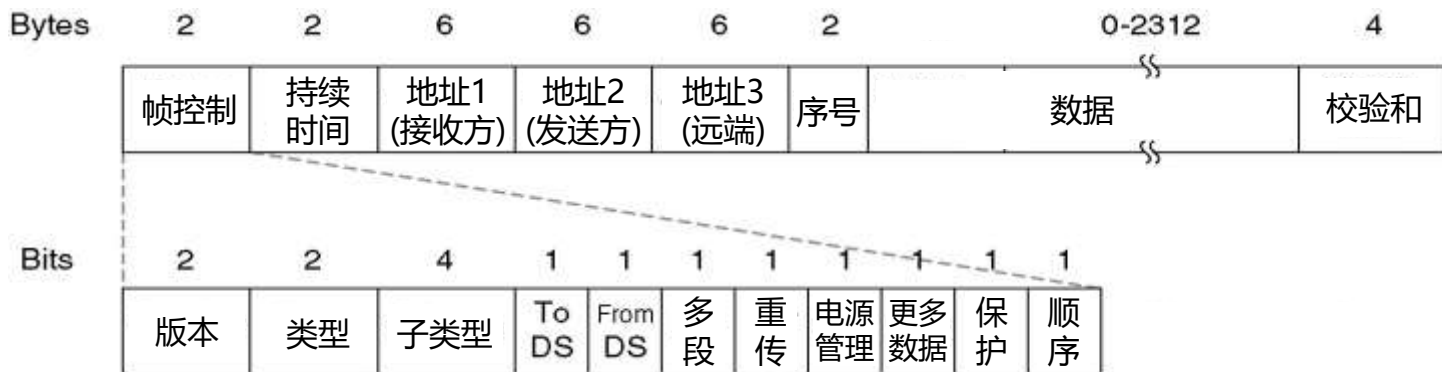
- 短帧间隔 (SIFS, Short InterFrame Spacing) , 可阻止段间被其他站横插一帧
- 仲裁帧间隔 (AIFS, Arbitration InterFrame Spacing) , 高为语音; 低为背景流量等
- DCF帧间隔 (DIFS, DCF InterFrame Spacing) , 常规数据帧之间的间隔
- 扩展帧间隔 (EIFS, Extended InterFrame Spacing) , 仅用于报告问题

802.11 帧结构与服务



■ 帧类型：数据、控制、管理

● 802.11 数据帧



■ 帧控制

- 类型（数据、控制、管理），子类型（RTS、CTS），DS（发送到或来自于分布式系统）
- 电源管理（发送方进入节能模式），保护（帧体已加密）

服务

■ 关联

- 进入AP无线电覆盖范围时，移动站使用该服务连接AP

■ 重新关联

- 允许移动站改变首选AP，以便连接到另一个AP

■ 认证

- 无加密
- WEP (Wired Equivalent Privacy, 有线等效保密)
- WPA (WiFi Protected Access)
- WPA2: 建议采用，算法选用高级加密标准AES (Advanced Encryption Standard)

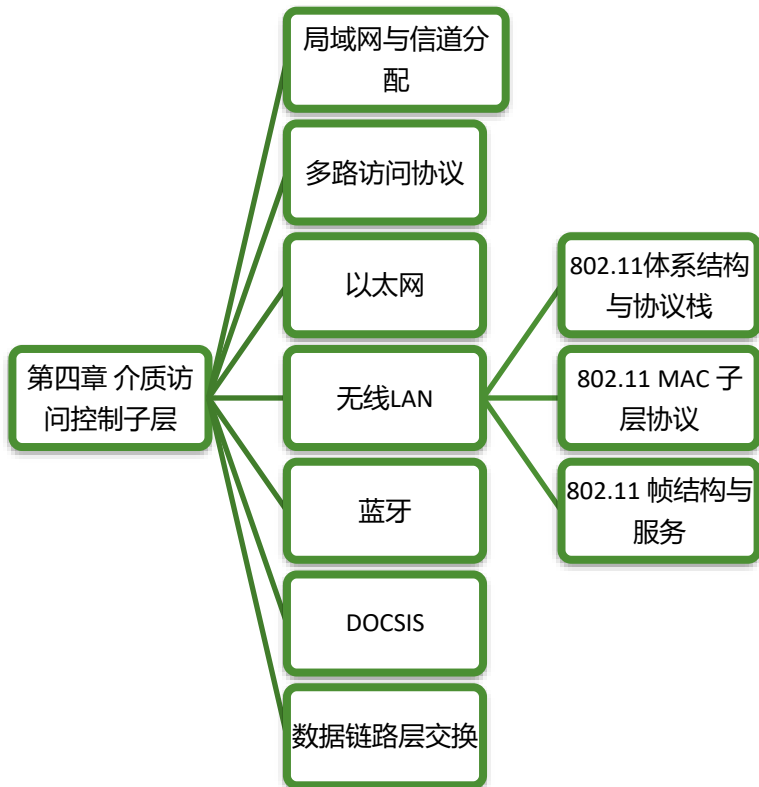
加密配置

安全模式:

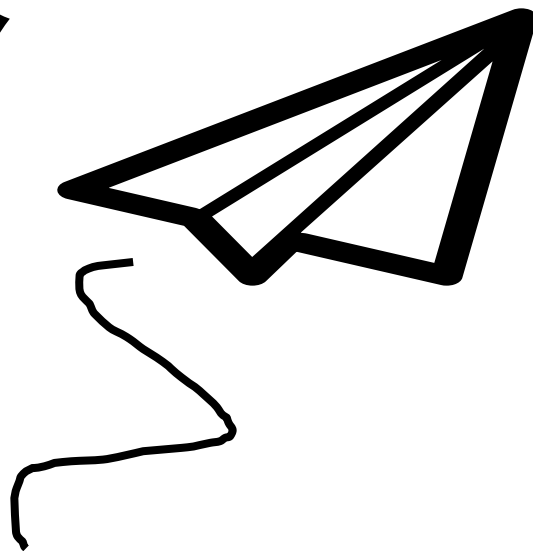
WPA 加密模式:

WPA预共享密钥:

本章导航与要点



本节课程结束



4.5 蓝牙技术



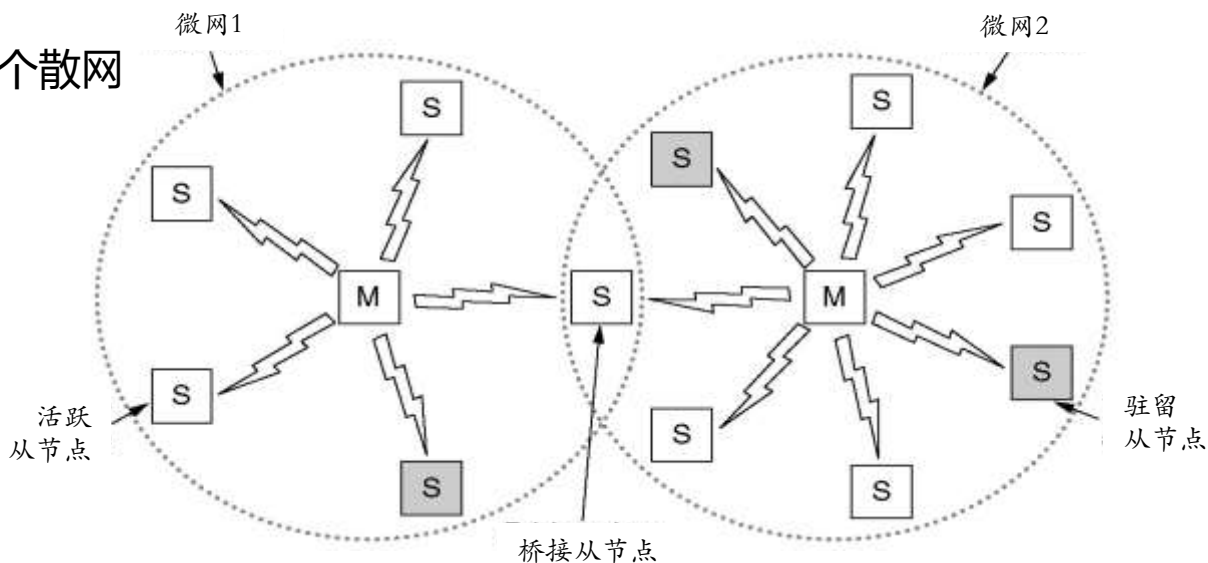
- 蓝牙的体系结构
- 蓝牙应用与蓝牙协议栈
- 蓝牙无线层与蓝牙链路层
- 蓝牙的帧结构

蓝牙的体系结构

■ 微网

- 1个主节点，7个活跃从节点，255个驻留从节点
- 集中式TDM

■ 两个微网连接成一个散网



蓝牙应用与蓝牙协议栈

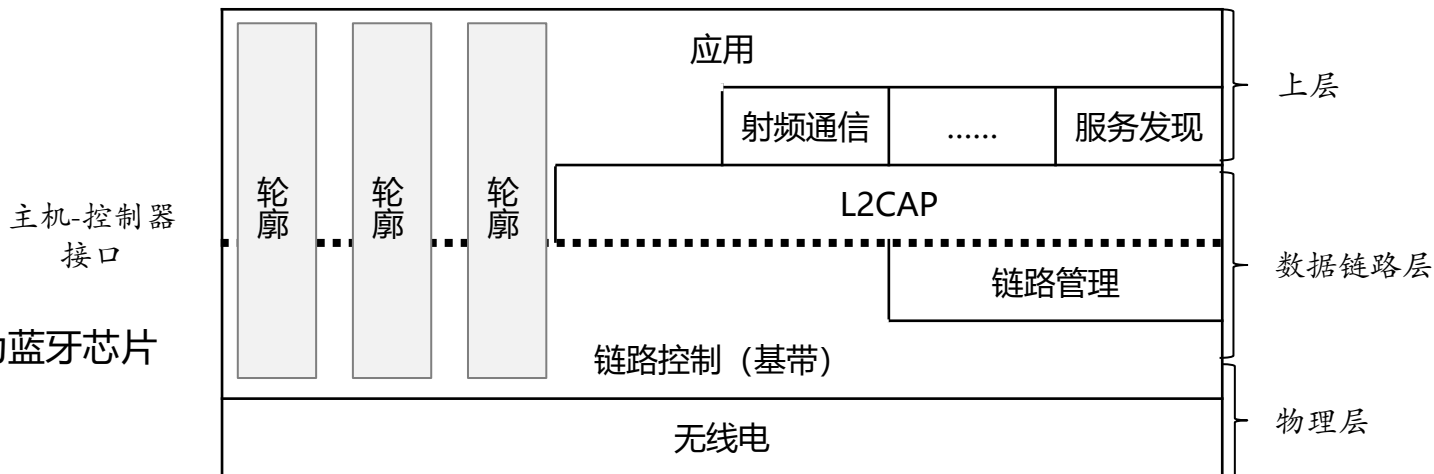


■ 蓝牙应用轮廓

- 通用访问应用、内部通信、头戴式设备、人机接口、局域网访问、通用对象交换

■ 蓝牙协议栈

- 逻辑链路控制适配协议(L2CAP, Logical Link Control Adaptation Protocol)



- 下面为蓝牙芯片

蓝牙无线电层与蓝牙链路层



■ 蓝牙无线电层

- 低功耗系统，距离范围10米
- 使用2.4~2.485GHz的ISM频段，分为79个信道，每信道1MHz，采用跳频扩展技术

■ 蓝牙链路控制层

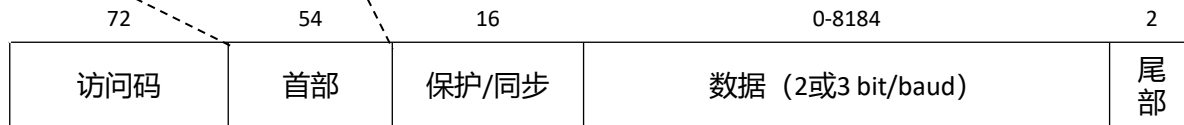
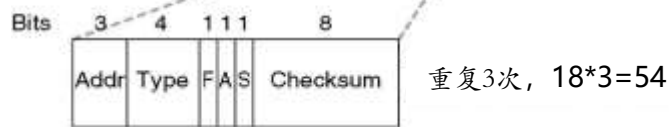
- 链路控制（基带）层最接近MAC子层，将比特流转换成帧
- 链路管理协议负责建立逻辑信道，即链路
 - ◆ 同步有连接链路，用于实时数据，如电话连接
 - ◆ 异步无连接链路，数据包方式交换数据，称为尽力而为投递

蓝牙的帧结构



基本型

- F流控制位
- A确认标志
- S序号



5*675毫秒时槽

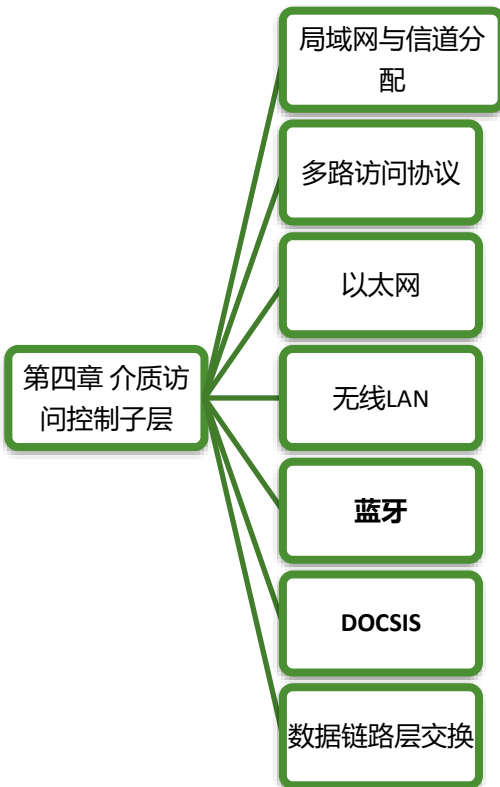
增强型

4.6 DOCSIS有线电视数据服务接口规范

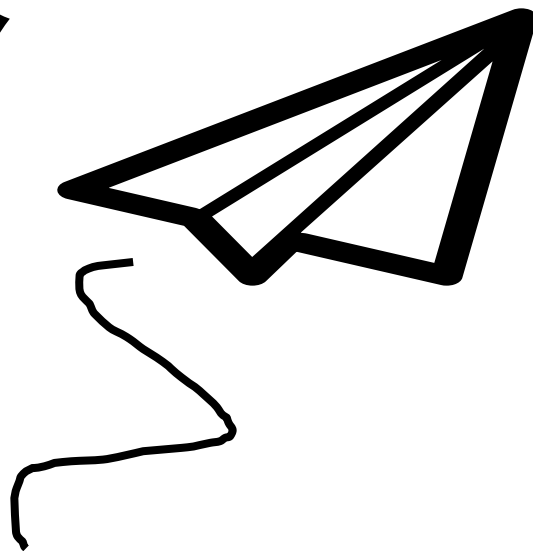


- DOCSIS(Data Over Cable Service Interface Specifications)
 - Cable Modem, MAC帧格式 (包括帧长度、校验和、扩展头)
- 测距
 - 测距请求帧周期性调整传输参数, 如时序、频率和功率
- 信道带宽分配
 - 服务流: MAC层提供管理上行流和下行流的服务质量的方法

本章导航与要点



本节课程结束



4.6 数据链路层交换



- 网桥的使用
- 学习网桥
- 生成树网桥
- 各层网络设备
- 虚拟局域网

网桥的使用



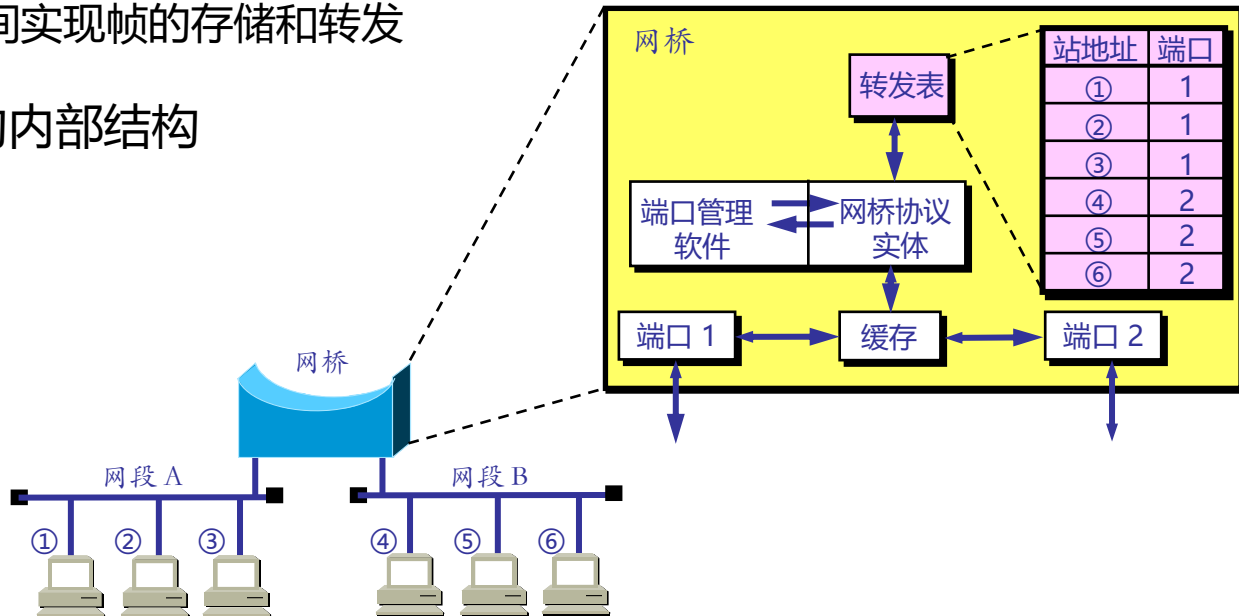
- 网桥技术
- 为何使用网桥
- 网桥与集线器的不同
- 网桥的优缺点

网桥技术

■ 定义

- 网桥 (bridge) 是工作在数据链路层的一种网络互连设备，它在互连的LAN之间实现帧的存储和转发

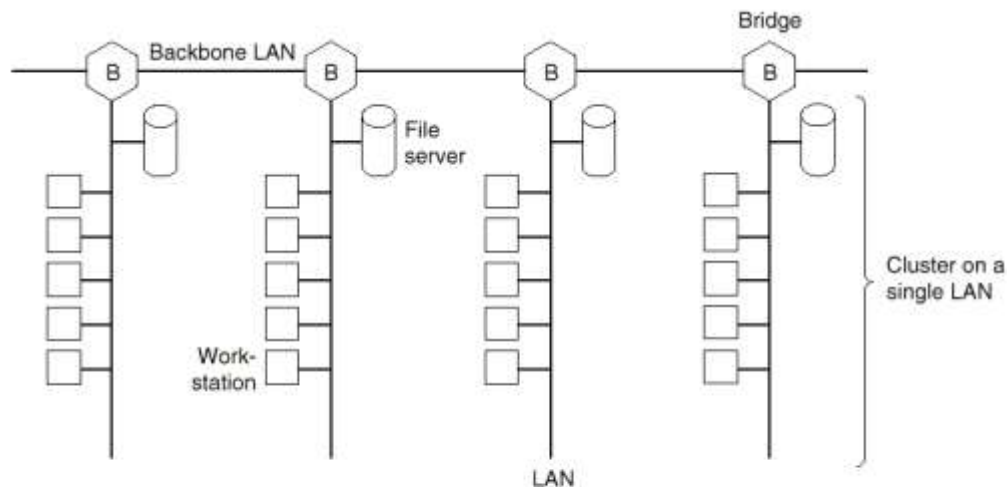
■ 网桥的内部结构



为何使用网桥

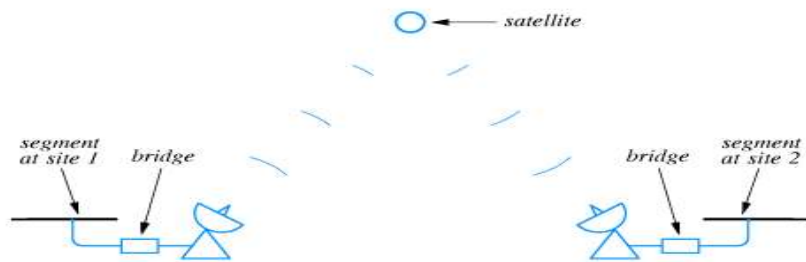


- 将一个负载很重的大LAN分隔成使用网桥互连的几个LAN以减轻负担



为何使用网桥 (2)

- LAN上的两台机器其距离超过2500米，必须使用网桥将这个 LAN 分隔以保证网络的正常工作



- 网桥可以互连不同类型的LAN
- 网桥可以隔离负载，防止出故障的站点损害全网
- 网桥可以有助于安全保密

网桥与集线器的不同



- 集线器（中继器或转发器）在转发帧时，不对传输介质进行检测
- 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

使用网桥的优缺点



■ 优点

- 过滤通信量
- 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

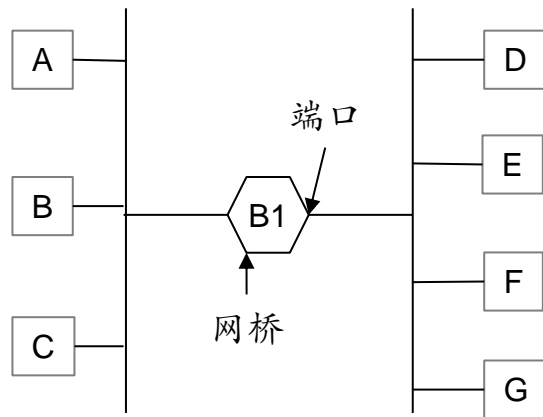
■ 缺点

- 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

学习网桥

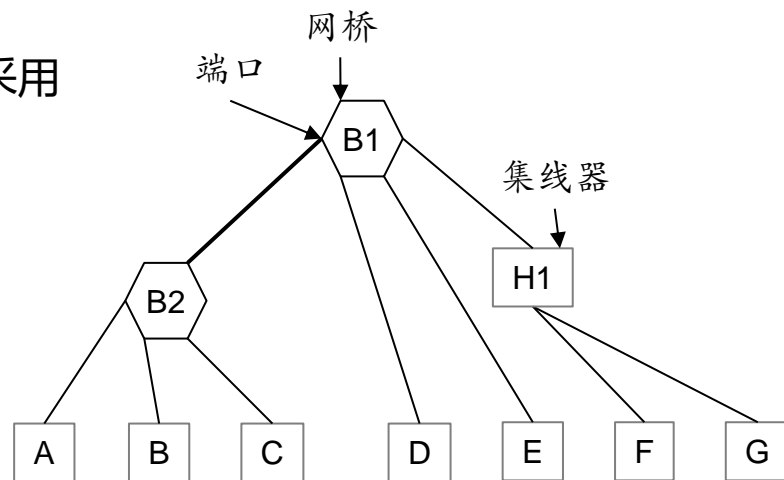


- 透明网桥
- 源路由网桥
- 网桥协议栈处理
- 网桥的工作原理
- 多端口网桥



透明网桥

- 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
- 以太网 (802.3)、令牌总线 (802.4) 采用





帧处理与转发表建立算法

- (1) 从端口 x 收到无差错的帧（如有差错即丢弃），在转发表中查找目的站 MAC 地址
- (2) 如有，则查找出到此 MAC 地址应当走的端口 d ，然后进行(4)
- (3) 向网桥除 x 以外的所有端口转发此帧（泛洪算法，这样做可保证找到目的站），转到(5)
- (4) 如果 $d = x$ ，则丢弃此帧（因为这表示不需要经过网桥进行转发）；
 否则从端口 d 转发此帧
- (5) 如源站在转发表中，更新计时器。然后转到(7)
- (6) 将源站 MAC 地址加入到转发表，登记该帧进入网桥的端口号 x ，设置计时器
- (7) 等待新的数据帧。转到(1)

网桥的转发表



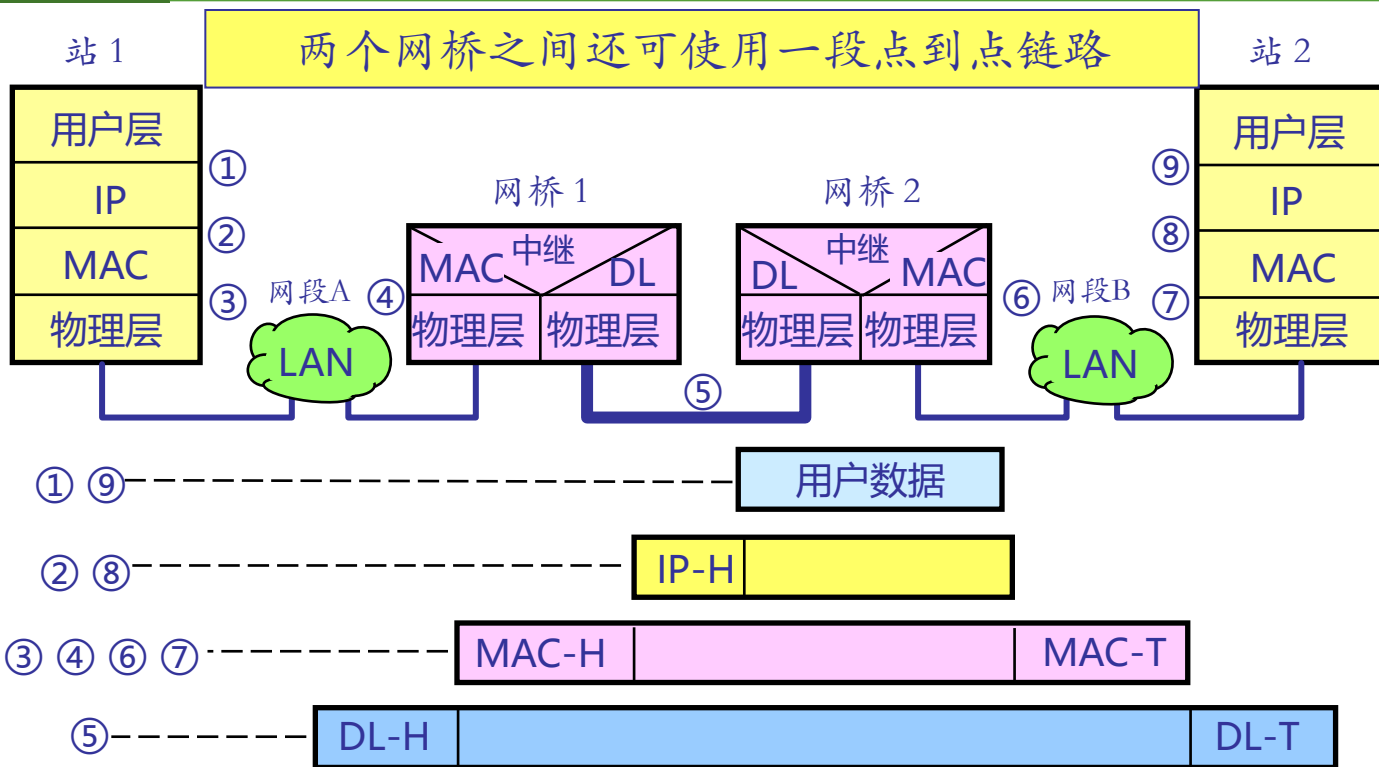
■ 转发表

- 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
- 转发表中 MAC 地址根据源 MAC 地址写入，但在转发时是将此 MAC 地址当作目的地址
 - ◆ 如果网桥能够从端口 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

■ 直通交换

- 转发算法可采用大规模集成电路芯片完成
- 在收到完整帧之前，只要收到MAC地址，就开始转发

网桥的协议栈处理

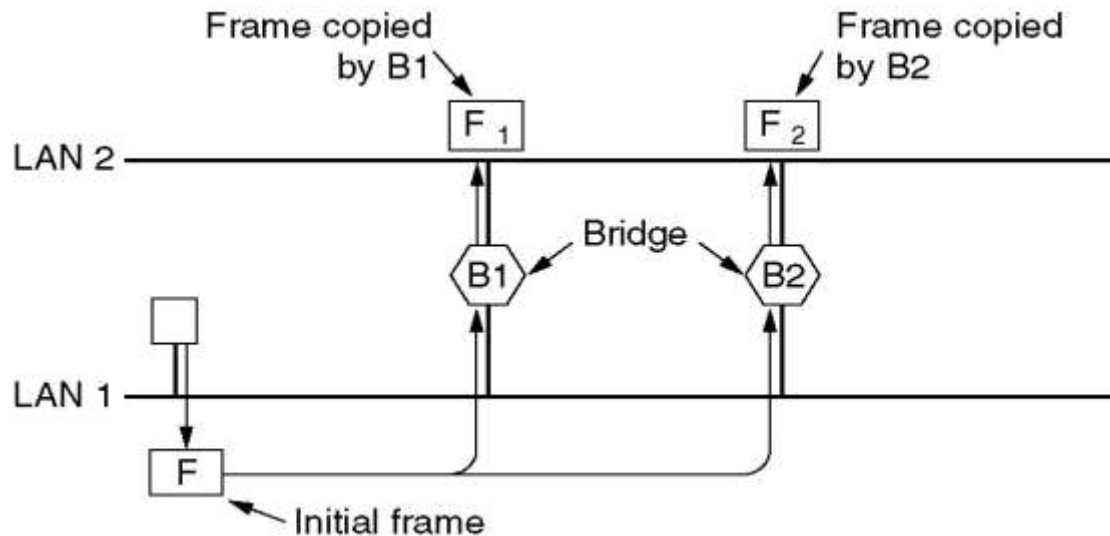


- 连接k个不同LAN的网桥具有k个MAC子层和k个物理层

生成树网桥



- 为提高可靠性，采用冗余的两个并行的透明网桥



- 使用生成树网桥可避免回路

解决多网桥产生回路问题



■ 思想

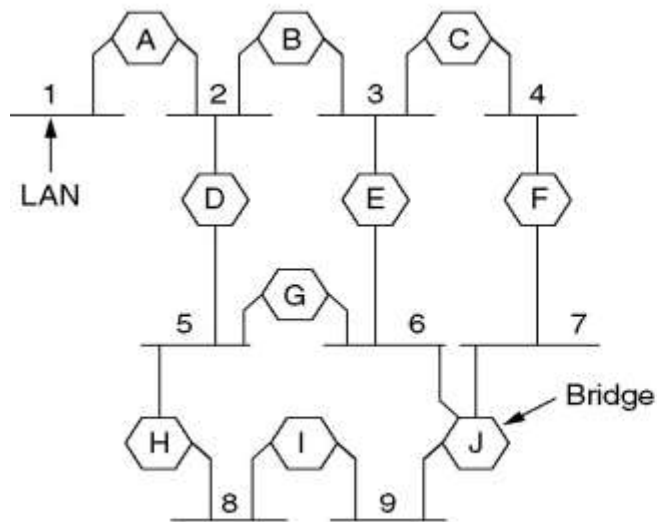
- 让网桥之间互相通信，用一棵连接每个LAN的生成树（Spanning Tree）覆盖实际的拓扑结构

■ 构造生成树

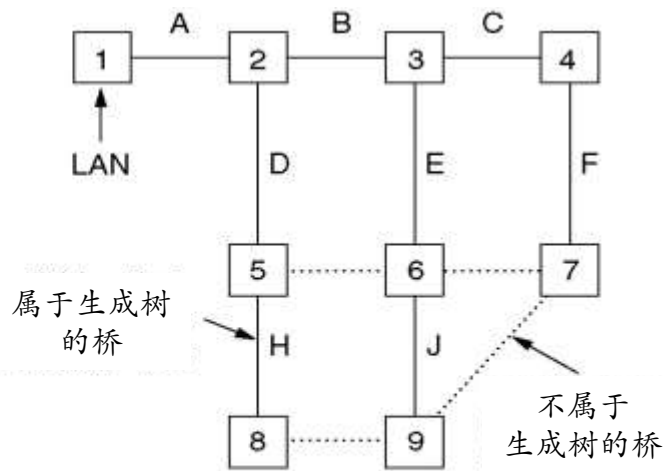
- 每个桥广播自己的桥编号，号最小的桥称为生成树的根
- 每个网桥计算自己到根的最短路径，构造出生成树，使得每个LAN和桥到根的路径最短
- 当某个LAN或网桥发生故障时，要重新计算生成树
- 生成树构造完后，算法继续执行以便自动发现拓扑结构变化，更新生成树

构造生成树

- (a) 互连的局域网
- (b) 一棵连接每个LAN的生成树



(a)



(b)

各层网络设备



■ 网络设备的工作层次

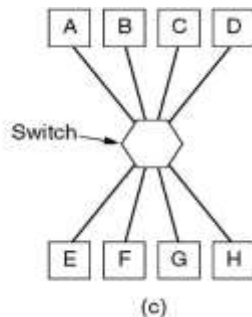
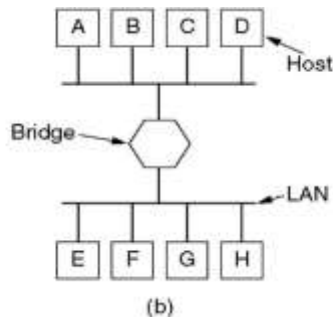
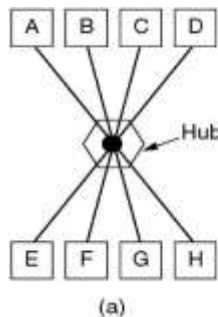
应用层：应用网关

传输层：传输网关

网络层：路由器

数据链路层：网桥(b)、交换机(c)

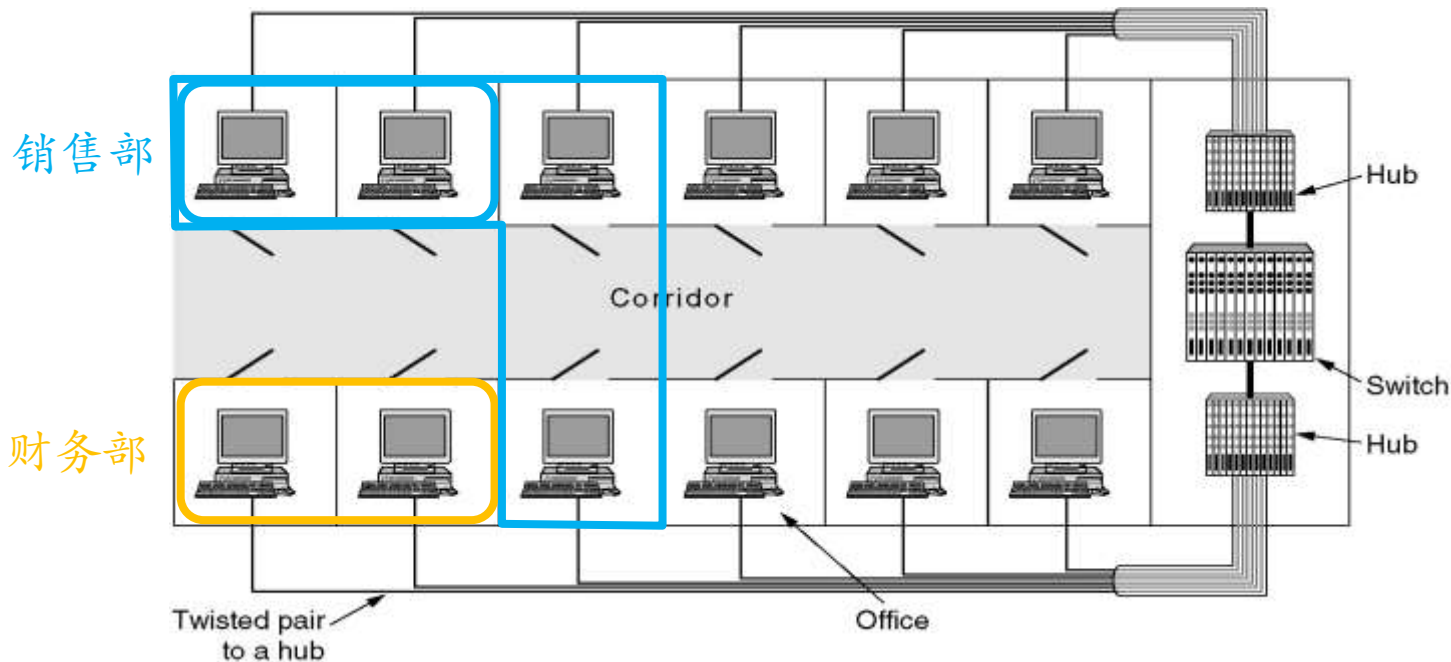
物理层：中继器、集线器(a)



虚拟局域网



- 大楼采用综合布线，使用交换机集中管理配置



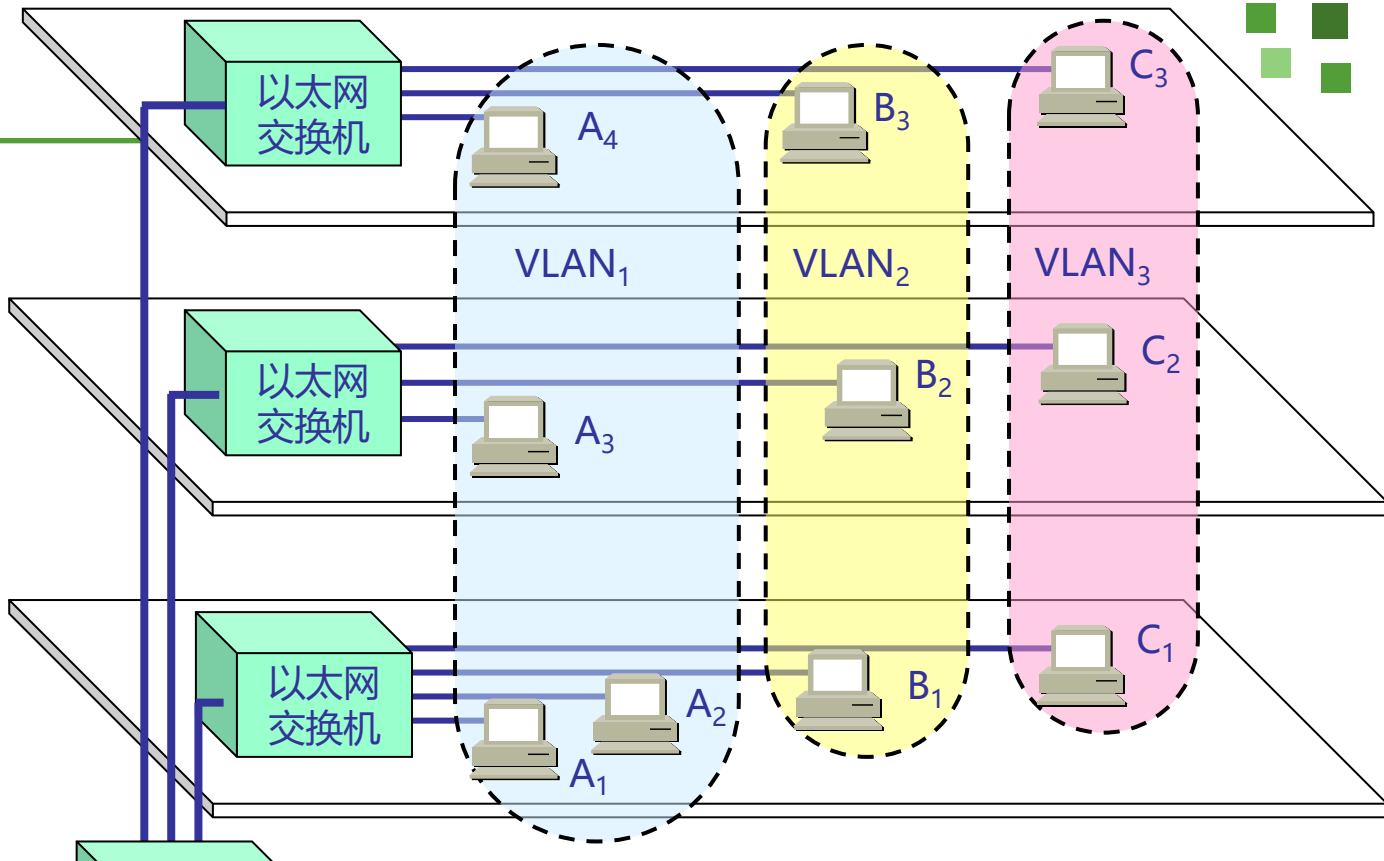
虚拟局域网概念



- 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服务的一种服务，而并不是一种新型局域网

VLAN示例

- 逻辑分组
- 安全性
- 负载优化
- 广播流量
- 管理维护



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。

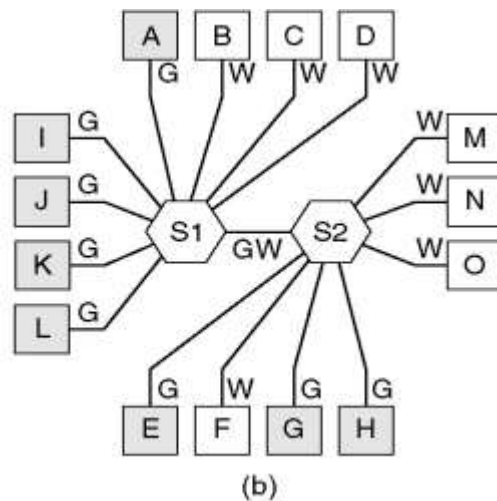
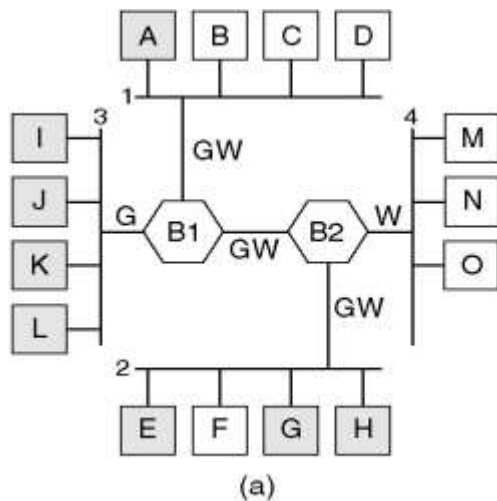
VLAN的物理与逻辑布局



■ 两个VLAN

(a) 四个物理的局域网，通过两个网桥重组为灰、白两个VLAN

(b) 15台电脑通过两台交换机组织成两个VLAN

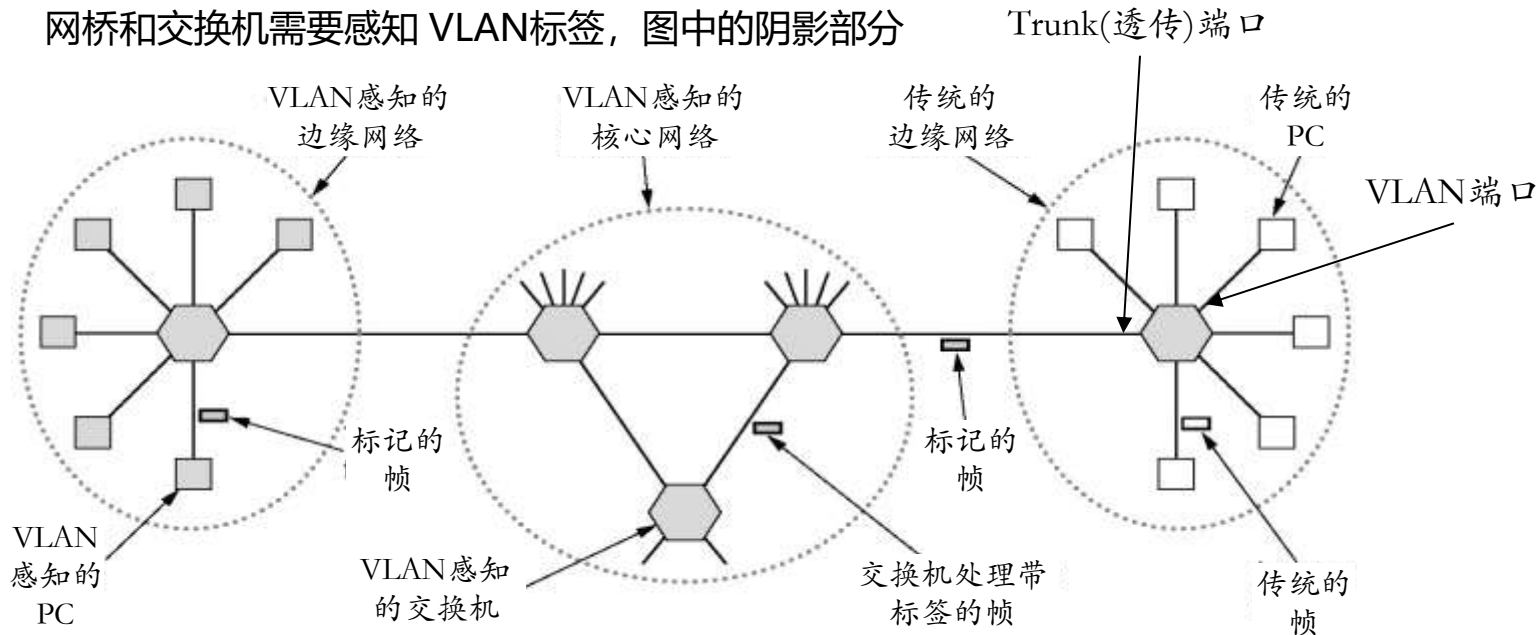


IEEE802.1Q



■ 增加VLAN标签

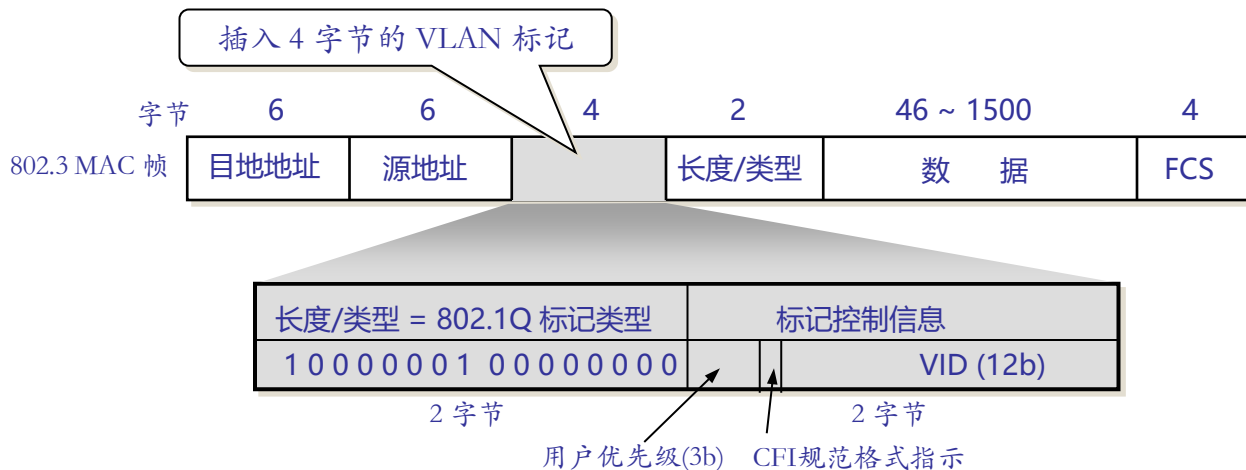
- 与以前的网络兼容，用户机器不需要感知，图中的白色部分
- 网桥和交换机需要感知 VLAN 标签，图中的阴影部分



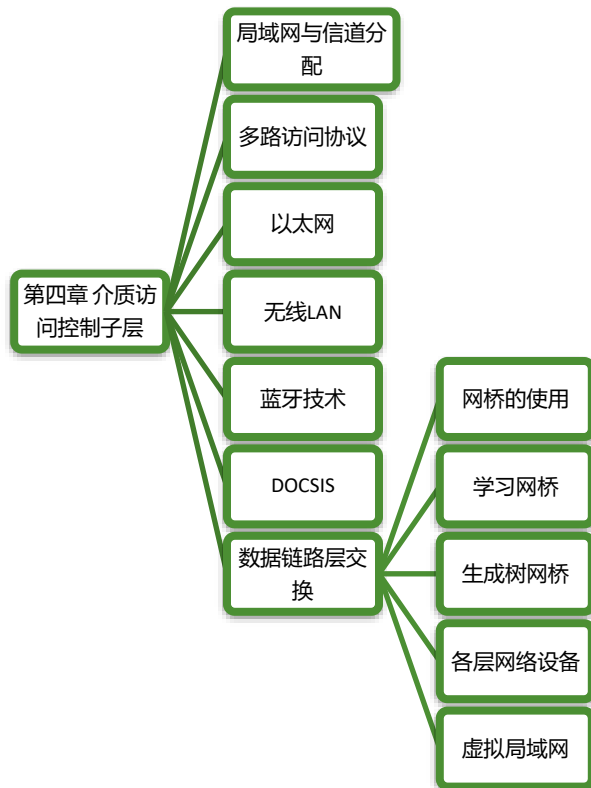
802.1Q 帧格式



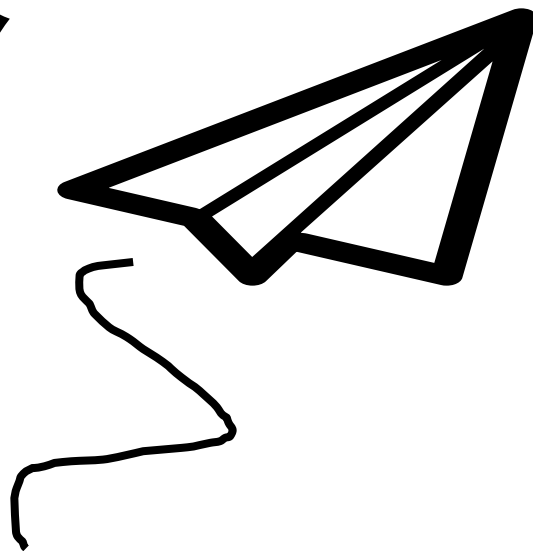
- 802.3 (传统)和802.1Q以太网帧格式
 - 虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符, 称为 VLAN 标记(tag), 用来指明发送该帧的工作站属于哪一个虚拟局域网, 最大帧长由1518B变为1522B



本章导航与要点



本章课程结束





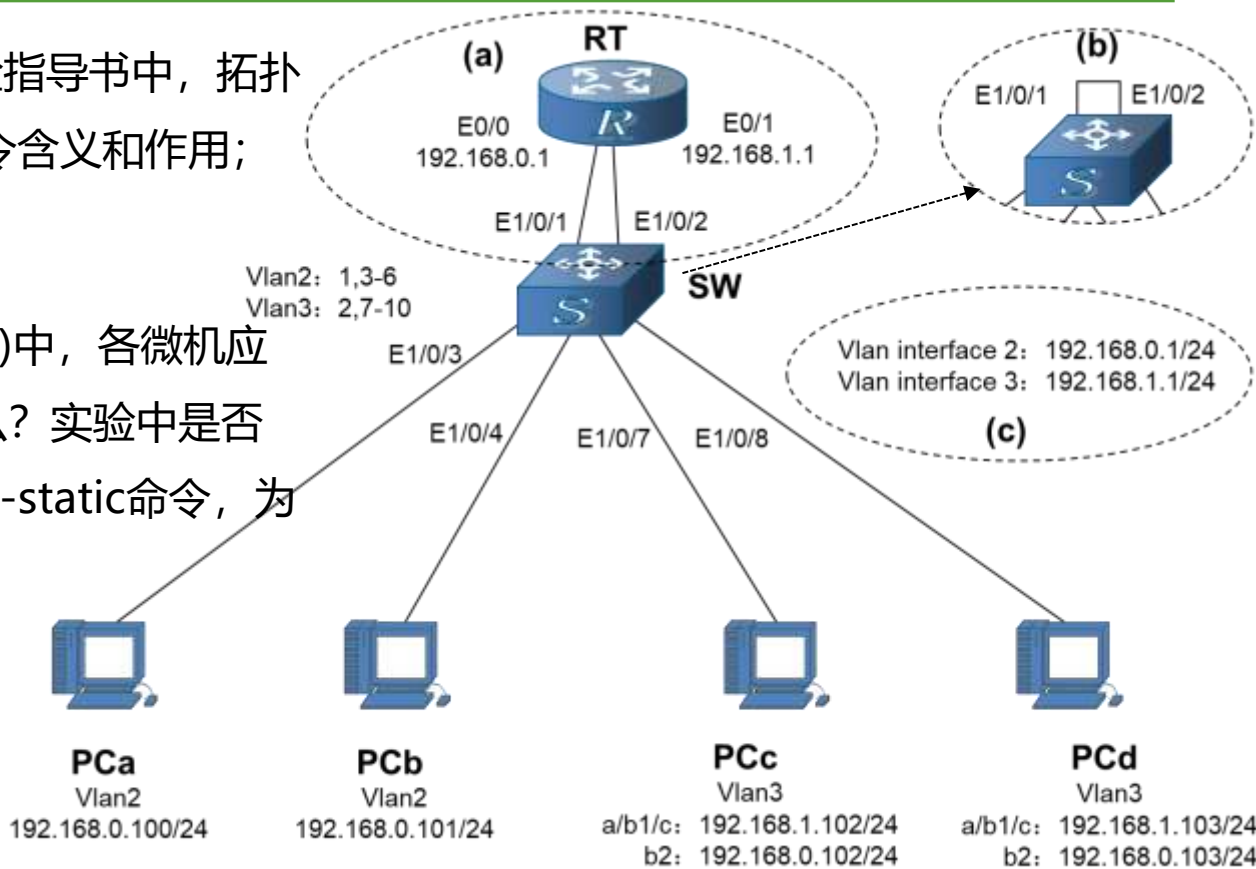
实验问题（实验12-1 路由表与静态路由）

- 题目1：解释实验指导书中各指令含义和作用；
- 题目2：写出实验结束后，各路由器的路由表；
- 题目3：如果PCa与 PCb无法 ping通，应如何检查故障？


实验问题（实验12-2 VLAN间路由）

- 题目4：简介实验指导书中，拓扑图(a)及之前各指令含义和作用；

- 题目5：拓扑图(a)中，各微机应配置的网关是什么？实验中是否需要使用ip route-static命令，为什么？



实验问题（实验12-2 VLAN间路由）



- 题目6：拓扑图(b)中，改变PCc、PCd的IP地址配置的目的是什么，不改变会出现什么情况？
- 题目7：拓扑图(c)中，是否可以使用ip route-static命令，为什么？
- 题目8：什么是静态路由，与动态路由的区别，什么情况下应该使用静态路由？本实验“路由表与静态路由”中，如果使用默认路由，应该如何配置？
- 题目9：为了加深对静态路由的理解，请在本实验的基础上，增加实验12-3，画出拓扑图，并写出实验目的和简单步骤。