



北京邮电大学

Beijing University of Posts and Telecommunications

计算机网络

第六章 局域网 LAN

网络空间安全学院

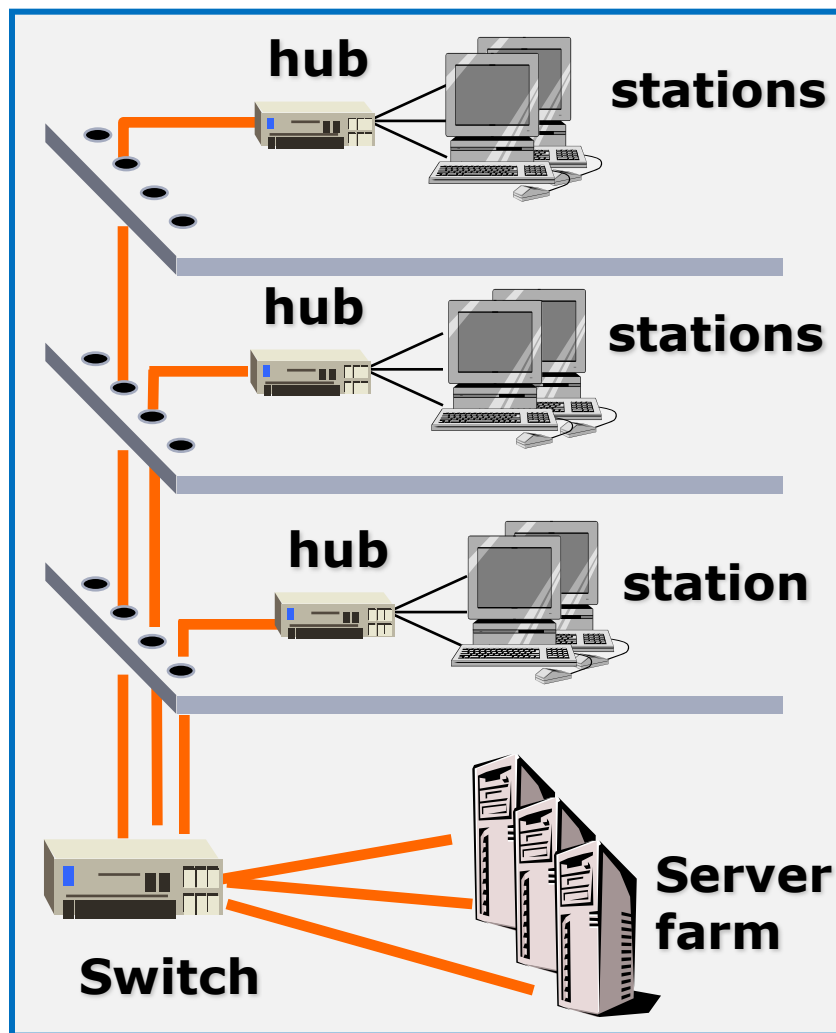
主要内容

- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

局域网（LAN）概述

■ LAN的特点

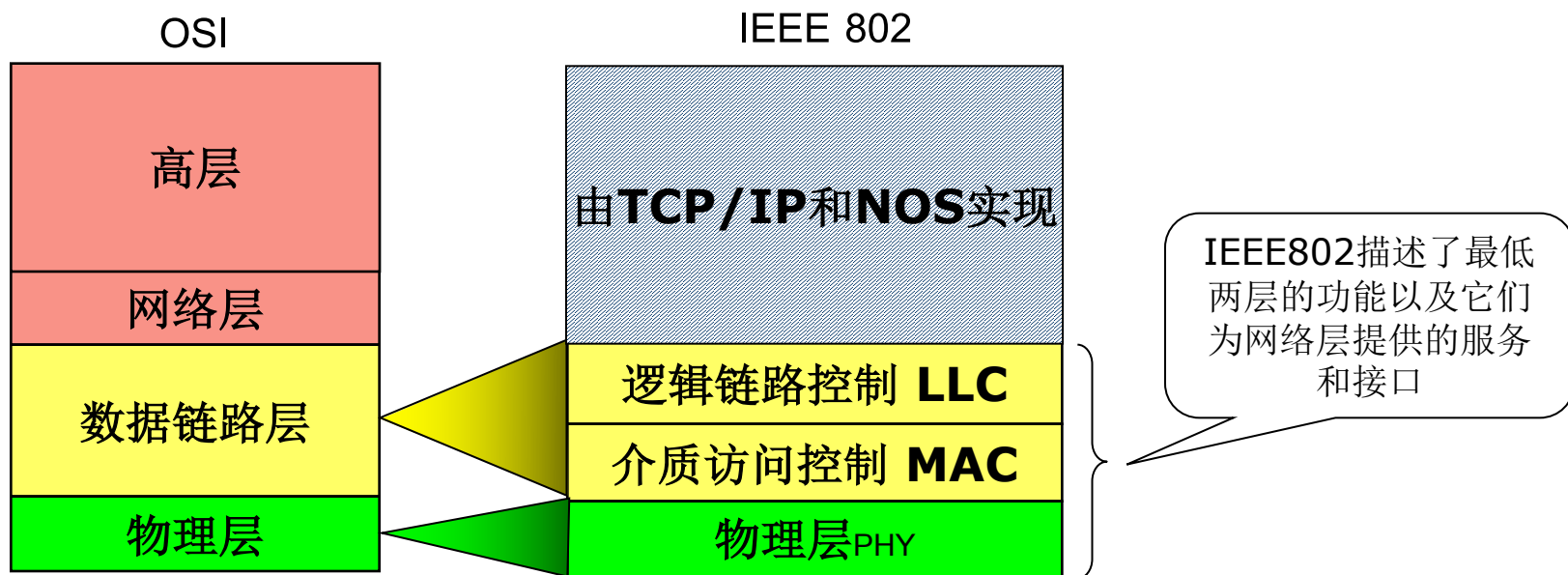
- 覆盖范围小
 - 房间、建筑物、园区范围
- 高传输速率
 - 10Mb/s ~ 400 Gb/s
- 低误码率
 - $10^{-8} \sim 10^{-11}$
- 拓扑：总线型、星形、环形
- 介质：UTP、Fiber、COAX
- 私有性：自建、自管、自用



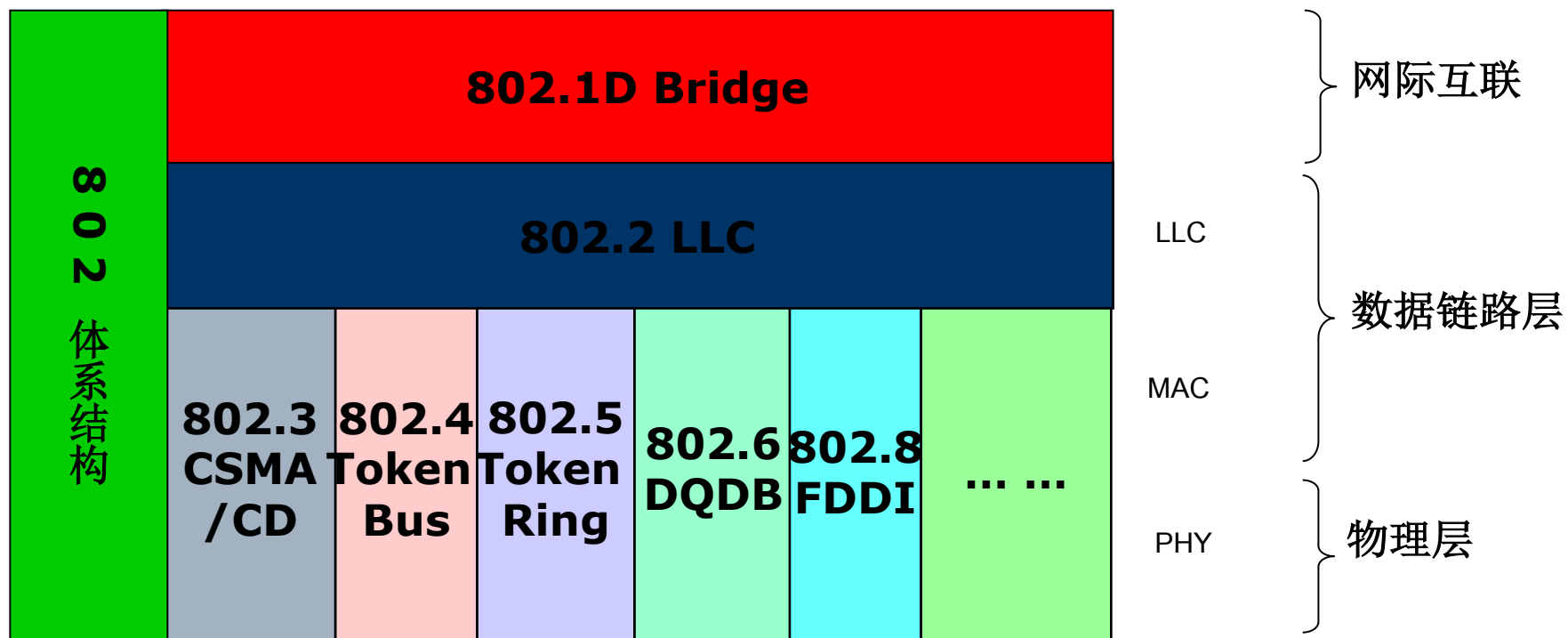
[来源于网络]

局域网参考模型

- 局域网的标准：IEEE802（ISO8802）
 - IEEE802是一个标准系列：IEEE802.1～IEEE802.20
- 其体系结构只包含了两个层次：数据链路层、物理层
 - 数据链路层又分为逻辑链路控制和介质访问控制两个子层



局域网参考模型



LAN：物理层

□ 功能：

- 位流的传输与接收；
- 同步前序码的产生与识别；
- 确定与传输媒体接口的特性；
- 信号编码和译码。

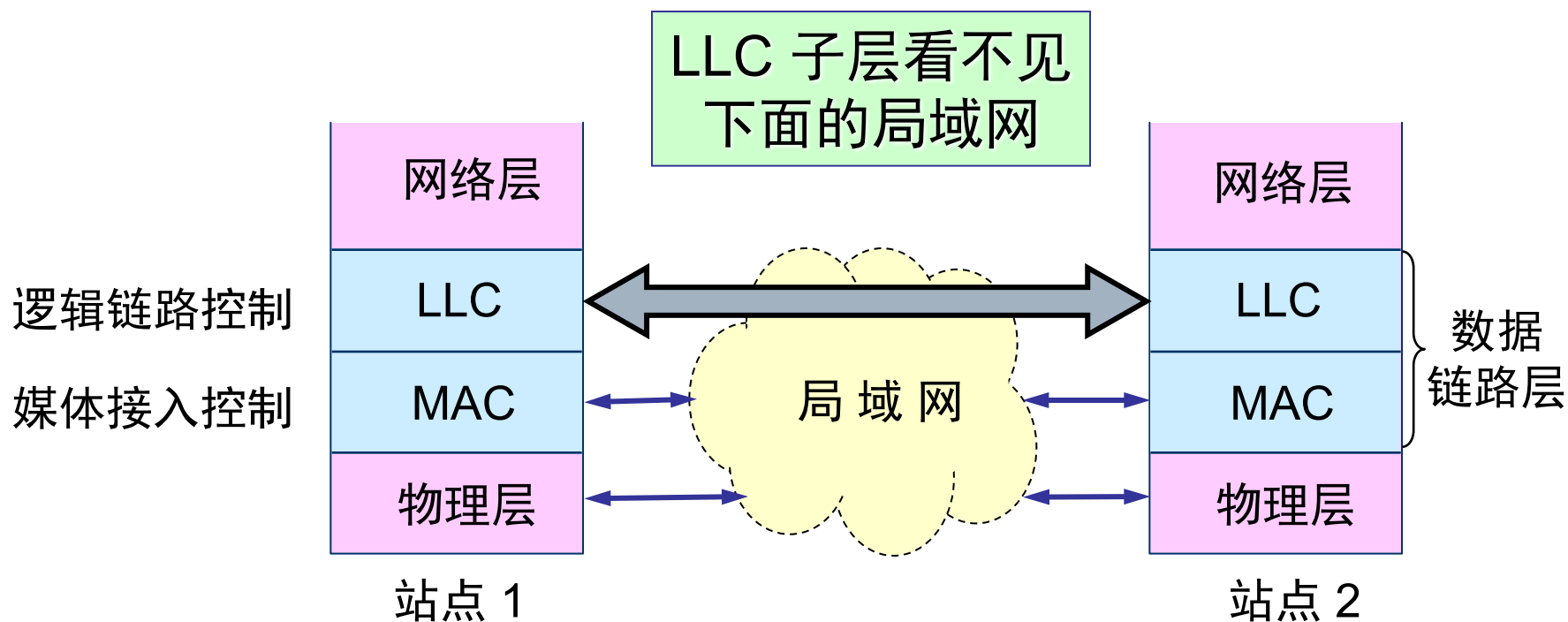
□ IEEE802定义了多种物理层，以适应不同的网络介质和不同的介质访问控制方法。

LAN：数据链路层

- 按功能划分为两个子层：LLC和MAC
 - 功能分解的目的：
 - 将功能中与硬件相关的部分和与硬件无关的部分分开，以适应不同的传输介质。
 - 解决共享信道(如总线)的介质访问控制问题，使帧的传输独立于传输介质和介质访问控制方法。
 - LLC：与介质、拓扑无关；
 - MAC：与介质、拓扑相关。
-

LAN：数据链路层

➤ 局域网对 LLC 子层是透明的



LLC子层的功能

- 遵循IEEE802.2标准
- 向高层提供统一的链路访问形式
- 成帧/拆帧
- 建立/释放逻辑连接
- 差错控制
- 帧序号处理
- 提供网络层接口
 - 不同的LAN标准, LLC子层都是一样的
 - 区别在于MAC子层和物理层

LLC提供的服务

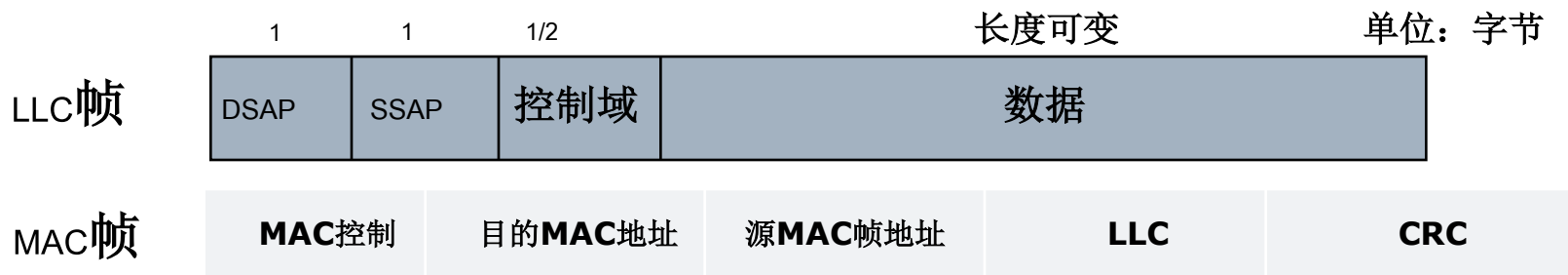
- ❑ LLC1：不确认的无连接服务，适用于广播、组播通信，周期性数据采集
 - ❑ LLC2：面向连接服务，适用于长文件传输，只支持单播
 - ❑ LLC3：带确认的无连接服务，适用于传送可靠性和实时性都要求的信息，如告警信息
 - ❑ LLC4：高速传送服务，适用于MAN
-

MAC子层的功能

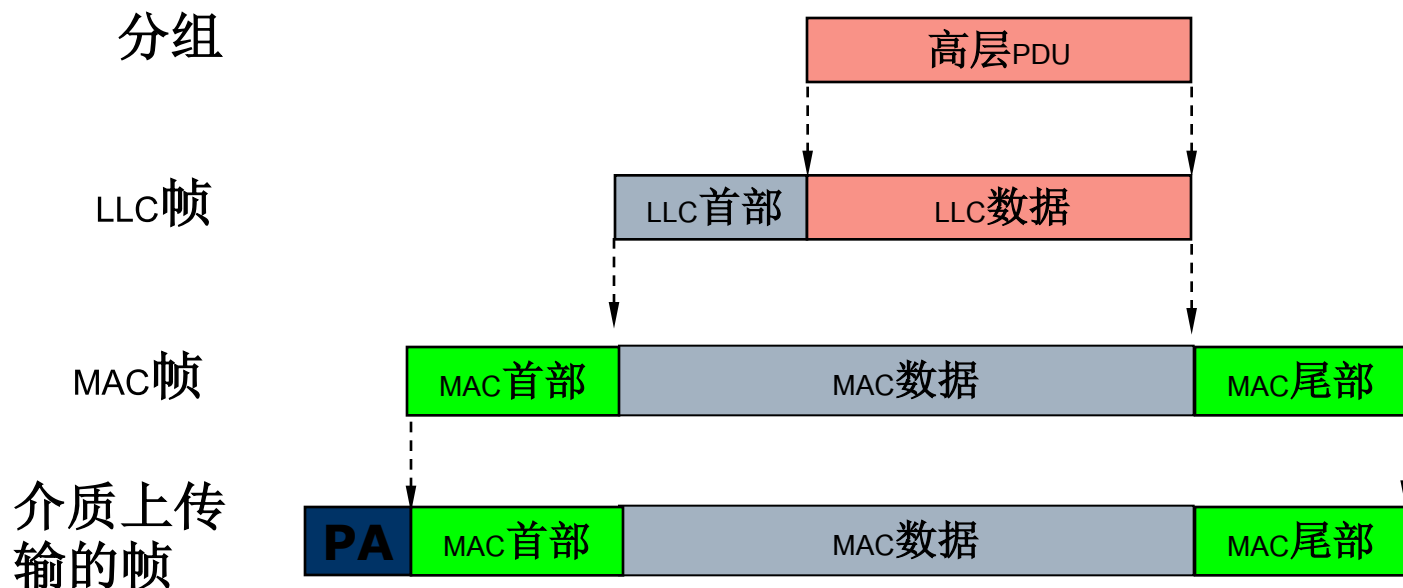
- ❑ 发送信息时负责把LLC帧组装成带有地址和差错校验段的MAC帧，接收数据时对MAC帧进行拆卸，执行地址识别和差错校验；
- ❑ 实现和维护MAC协议
- ❑ 由于采用不同的MAC协议，MAC帧的确切定义不一样。但是所有的MAC帧的格式大致类似：

MAC控制	目的MAC地址	源MAC帧地址	LLC 帧	CRC
-------	---------	---------	-------	-----

LAN的封装过程



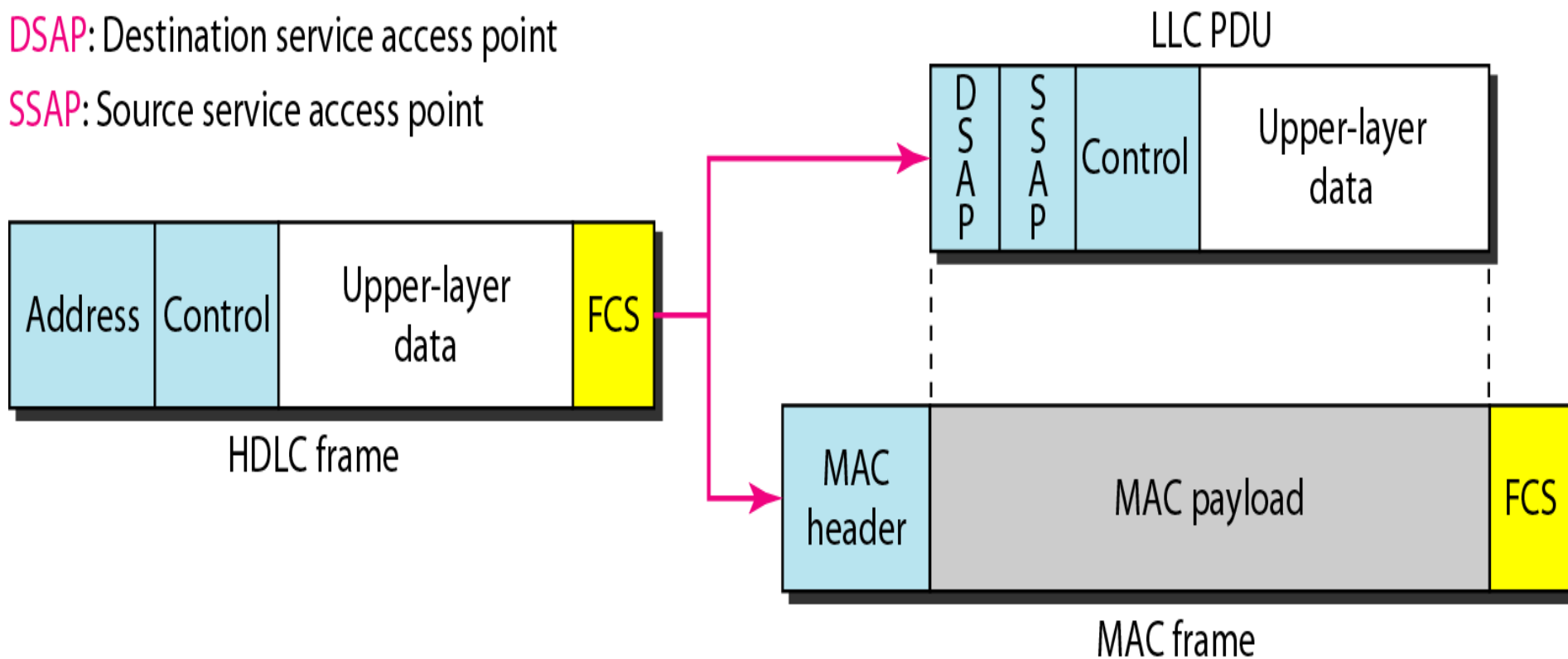
IEEE802 LAN的封装过程：



HDLC帧 vs. LLC帧和MAC帧

DSAP: Destination service access point

SSAP: Source service access point



- 成帧、差错检测由**MAC**子层负责
- 差错恢复、流量控制由**LLC**子层负责

介质访问控制方法

□ 广播信道：多个站点共享同一信道

- 各站点如何访问共享信道？
- 如何解决同时访问造成的冲突（信道争用）？
 - ✓ 介质（媒体）访问控制(MAC)

□ 信道共享技术：

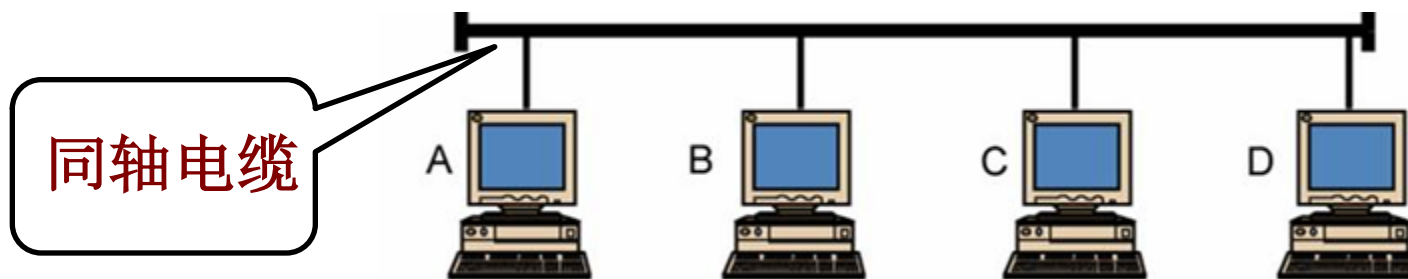
- 静态分配（FDM、WDM、TDM、CDM）
 - ✓ 无法灵活适应站点数及通信量变化，不适用于LAN
 - 动态分配（随机接入、受控接入）
 - ✓ ALOHA、CSMA/CD、预约、集中控制（如轮询、传递令牌）
-

介质访问控制方法

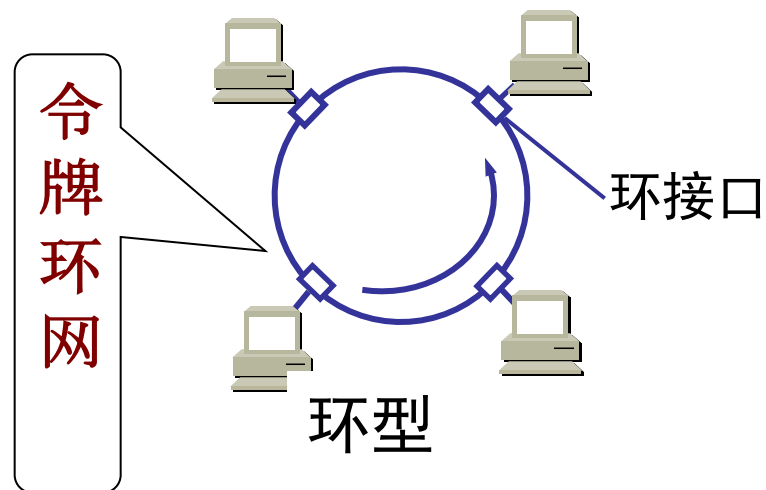
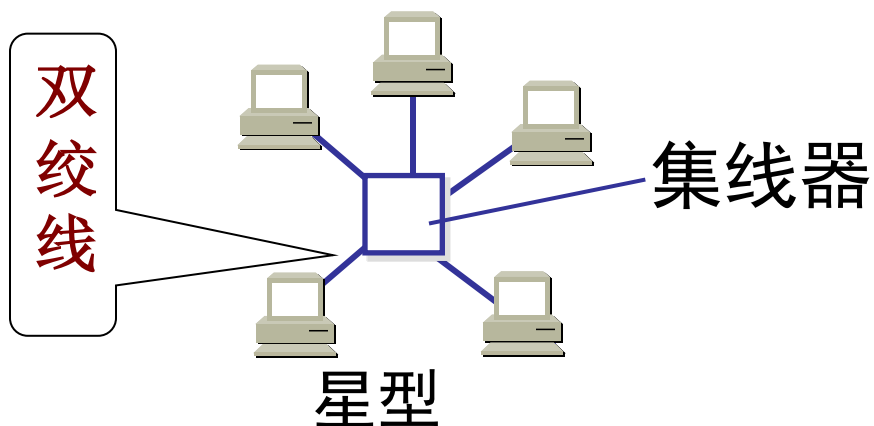
□ 动态分配常见的有两种：

- 随机接入方式，采用随机访问技术的竞争型介质访问控制方法
 - ✓ 不预先规定发送时间和发送顺序，各站点都是随机和平等的
 - ✓ ALOHA、CSMA、CSMA/CD
- 受控接入方式，采用受控访问技术的分散控制型介质访问控制方法
 - ✓ 需要服从一定的控制
 - ✓ Token Ring、Token Bus、FDDI

局域网的拓扑结构



总线型



主要内容

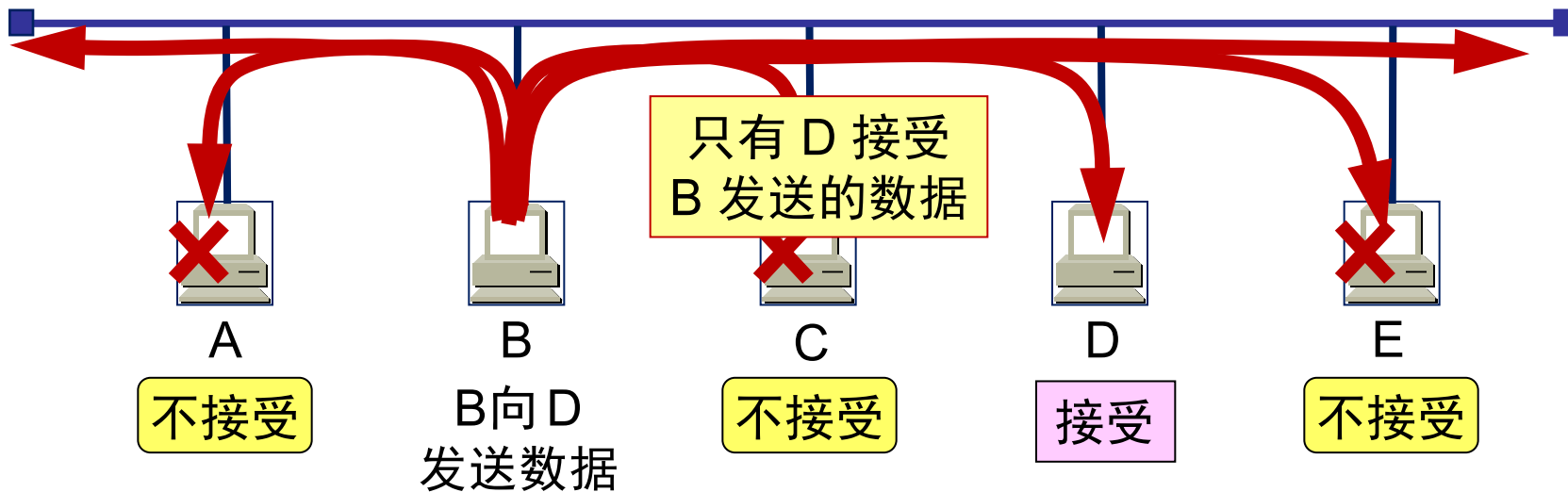
- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

以太网

- 20世纪70年代中期由施乐公司（Bob Metcalfe）提出，数据率为2.94Mb/s，称为Ethernet（以太网）
 - 最初人们认为电磁波是通过“[以太](#)”来传播的
- 经DEC, Intel和Xerox公司改进为10Mb/s标准（DIX Ethernet II标准）
- 1983年被采纳为IEEE 802.3，支持多种传输媒体。
 - “带有冲突检测的载波监听多路访问方法和物理层技术规范”
- Ethernet II和IEEE 802.3二者区别很小
- 目前已发展到400Gbps，仍在继续发展 …

以太网

□ 传统以太网(10Mbps)：总线拓扑，广播通信



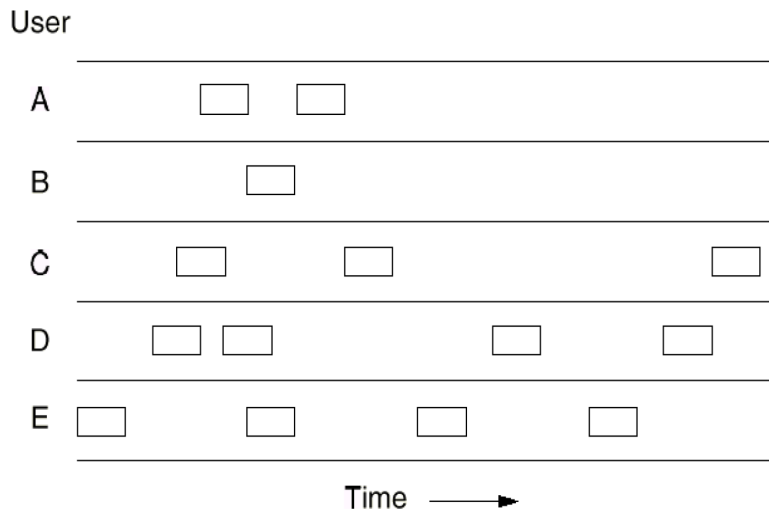
早期信道动态分配：ALOHA协议

□ 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。

□ 时隙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。



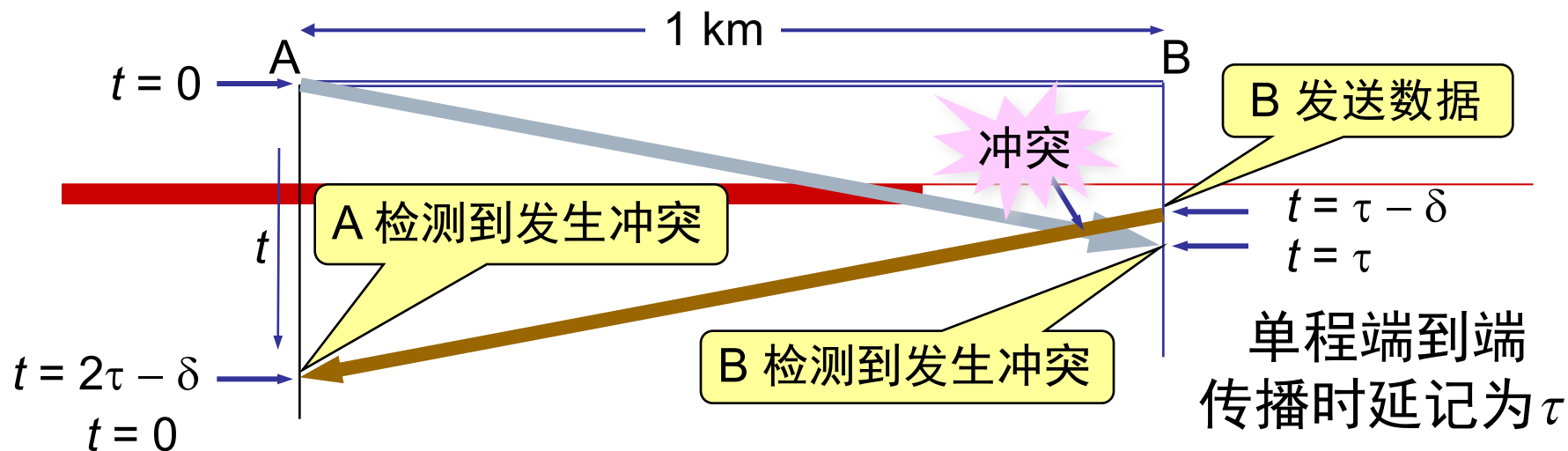
CSMA/CD协议

- 载波监听多点接入/冲突检测协议
- 多个站点如何安全地使用共享信道？
 - **载波监听（CSMA）**：发送前先检测一下其它站点是否正在发送（即信道是否忙）
 - 若信道空闲，是否可以立即发送？
 - ✓ 立即发送（**1坚持的CSMA**）
 - 若信道忙，如何处理？
 - ✓ 继续监听，等到信道空闲后立即发送
 - **冲突检测（CD）**：边发送边检测是否有冲突
 - 若不冲突，持续发送，直到发完
 - 若冲突，停止发送

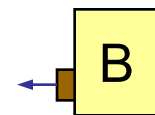
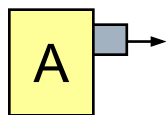
为什么会冲突？

□ 既然发送之前已经监听信道为“空闲”，为什么还会出现冲突？

- 当某个站监听到总线是空闲时，总线并非真正是空闲的，因为电磁波有传播时延
- A 发出的信号，要经过一定时间后才能传送到 B
- B 若在 A 发送的信息到达 B 之前发送自己的帧，则必然要在某个时间和 A 发送的帧发生冲突
- 结果是两个帧都变得无用



A 检测到
信道空闲
发送数据



$t = \tau - \delta$
B 检测到信道空闲
发送数据

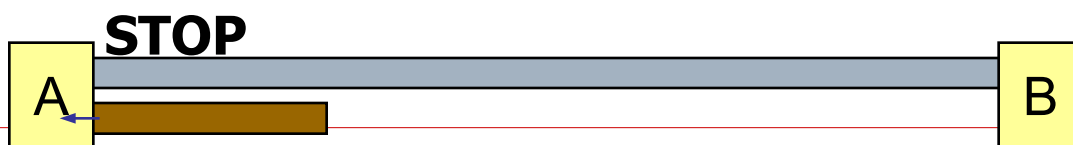


$t = \tau - \delta / 2$
发生冲突



$t = \tau$
B 检测到发生冲突
停止发送

$t = 2\tau - \delta$
A 检测到
发生冲突



CSMA/CD 协议争用期

- 发送数据帧的站点，在发送后最多经过 2τ (端到端的往返传播时延) 可以知道是否有冲突
- 以太网的争用期 (冲突窗口) : 2τ
- 经过争用期之后还没有检测到冲突，即没有冲突
- 以太网的最短帧长 : 64字节
 - ◆ 传统10Mbps以太网的争用期为 $51.2\mu\text{s}$ ，这段时间可发送512 bit，即 64 字节
 - ◆ 如果帧长小于64字节，则争用期内已经发送完毕，发送站点可能检测不到冲突
 - ◆ 因此规定最短有效帧长为 64 字节，长度小于 64 字节的帧都是由于冲突而异常中止的无效帧

退避算法：截断二进制指数退避算法

- 发生冲突的站点在停止发送后，要推迟(退避)一个随机时间才能再发送数据，减小再次发生冲突的概率
 - 基本退避时间，一般取 2τ
 - 从整数集合 $[0, 1, \dots, (2^k - 1)]$ 中随机地取出一个数 r ，重传需退避的时间= $r \times 2\tau$ ，其中 $k = \text{Min}[\text{重传次数}, 10]$
 - 重传 16 次仍失败，则丢弃该帧，向高层报告

总结：CSMA/CD协议

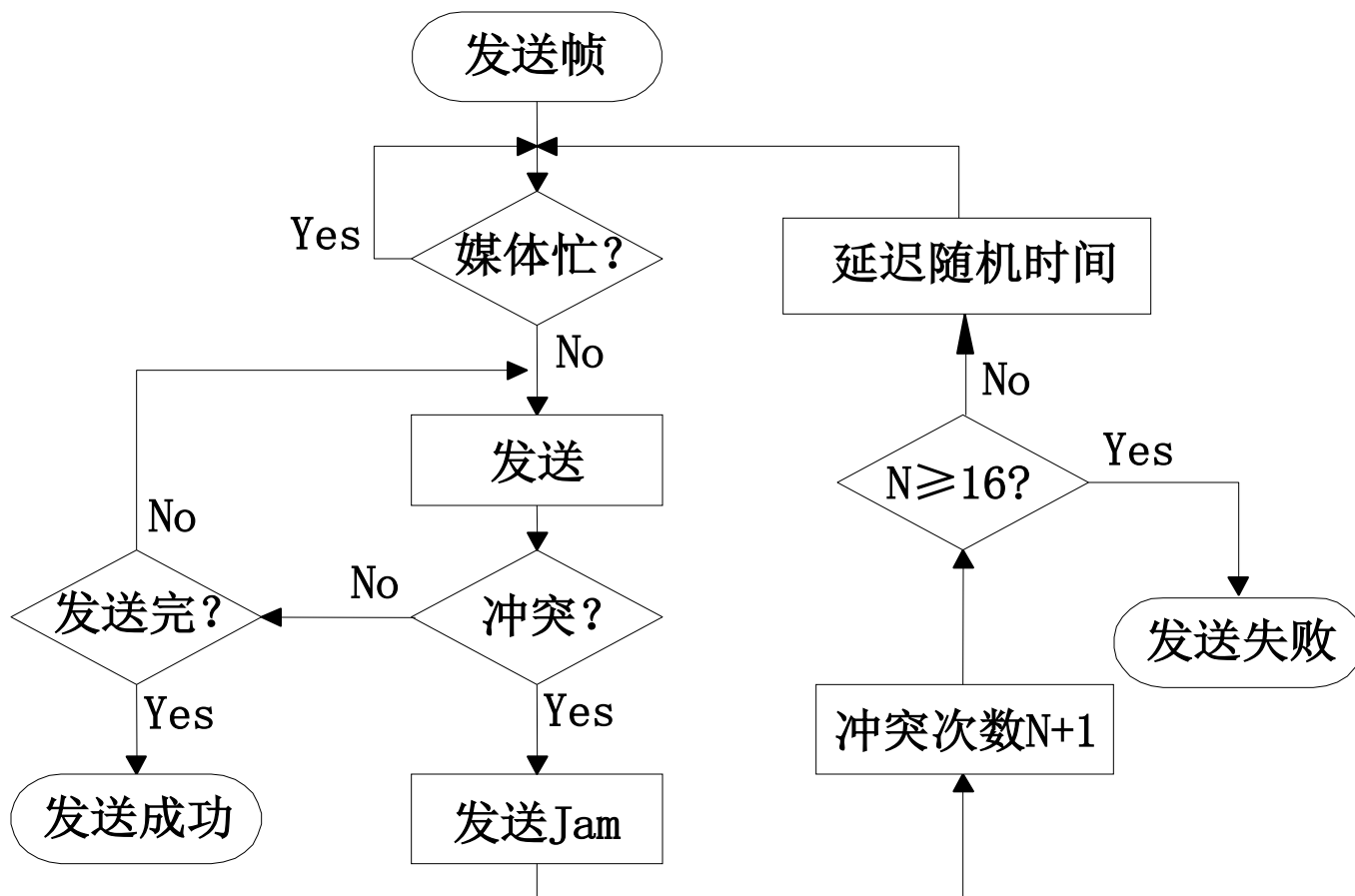
□ 用于IEEE802.3以太网

□ 工作原理：

- 发送前先监听信道，若空闲则立即发送；
- 如果信道忙，则继续监听，一旦空闲就立即发送；
- 在发送过程中，监听是否冲突。若冲突，则立即停止发送数据，并发送冲突强化信号Jam
 - 目的是使所有的站点都能检测到冲突
- 等待一段随机时间（退避）以后，再重新尝试

● 总结：发前先听，空闲即发送，边发边听，冲突时退避

1 坚持的CSMA/CD协议的操作流程

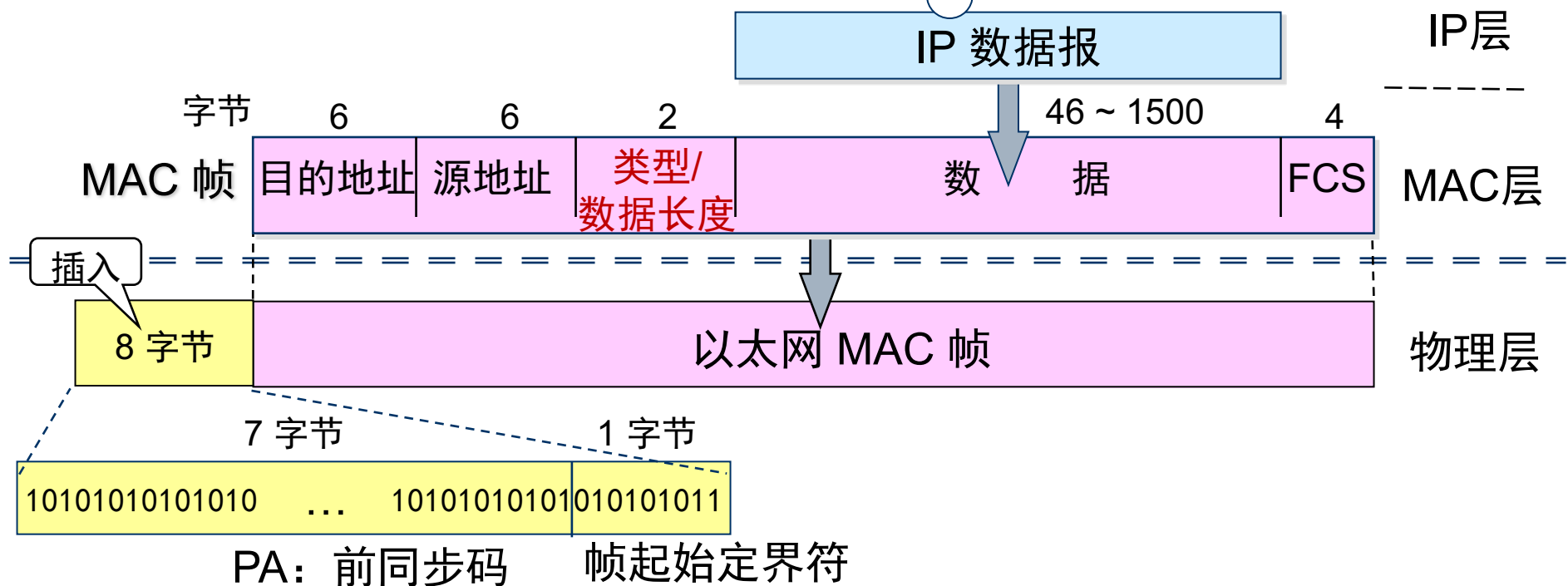


以太网的帧格式

两种标准：

- ◆ DIX Ethernet 标准（更常用）
- ◆ IEEE 802.3 标准

当数据字段长度小于 46 字节时，应进行填充，以保证 MAC 帧长不小于 64 字节。



无效的MAC帧

- ❑ 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 MAC 帧长度不在 64 ~ 1518 字节之间
- ❑ 以太网丢弃无效 MAC 帧，不负责重传

帧间最小间隔 (IFG)

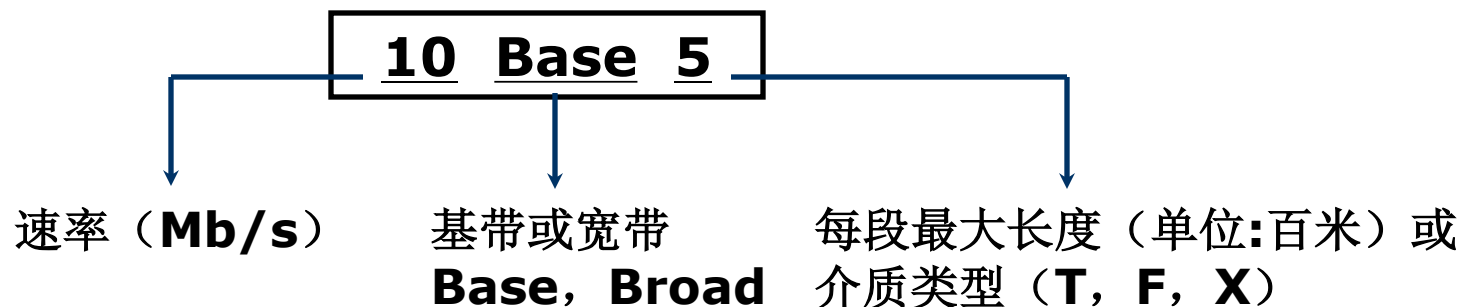
- ❑ 帧间最小间隔为 $9.6\ \mu\text{s}$ ，相当于 96 bit 发送时间
- ❑ 一个站在检测到总线开始空闲后，还要等待 $9.6\ \mu\text{s}$ 才能再次发送数据
- ❑ 目的：使其他站点（尤其是刚发送的站点和刚接收的站点）做好接收帧的准备

IEEE 802.3 以太网的主要标准

- 传统以太网：10Mb/s
 - 802.3 —— 粗同轴电缆
 - 802.3a —— 细同轴电缆
 - 802.3i —— 双绞线
- 快速以太网（FE）：100Mb/s
 - 802.3u —— 双绞线，光纤
- 千兆以太网（GbE）：1000Mb/s（1Gb/s）
 - 802.3z —— 屏蔽短双绞线、光纤
 - 802.3ab —— 双绞线
- 万兆以太网：10Gb/s
 - 802.3ae —— 光纤
- 更高速以太网：100Gb/s
 - 802.3bs —— 光纤

以太网的物理层选项与标识方法

- 速率、信号方式、介质类型



传统以太网		快速以太网和千兆以太网	
• 10Base5	粗同轴	• 100Base-T	UTP
• 10Base2	细同轴	• 100Base-F	MMF/SMF
• 10Base-T	UTP	• 1000Base-X	STP/MMF/SMF
• 10Base-F	MMF	• 1000Base-T	UTP

主要内容

- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

无线网络

□ 为什么需要无线网络？

■ 有线网络的缺点

□ 临时组网不方便

- 如军事演习、自然灾害

□ 网络互联要跨越公共场合时布线很麻烦

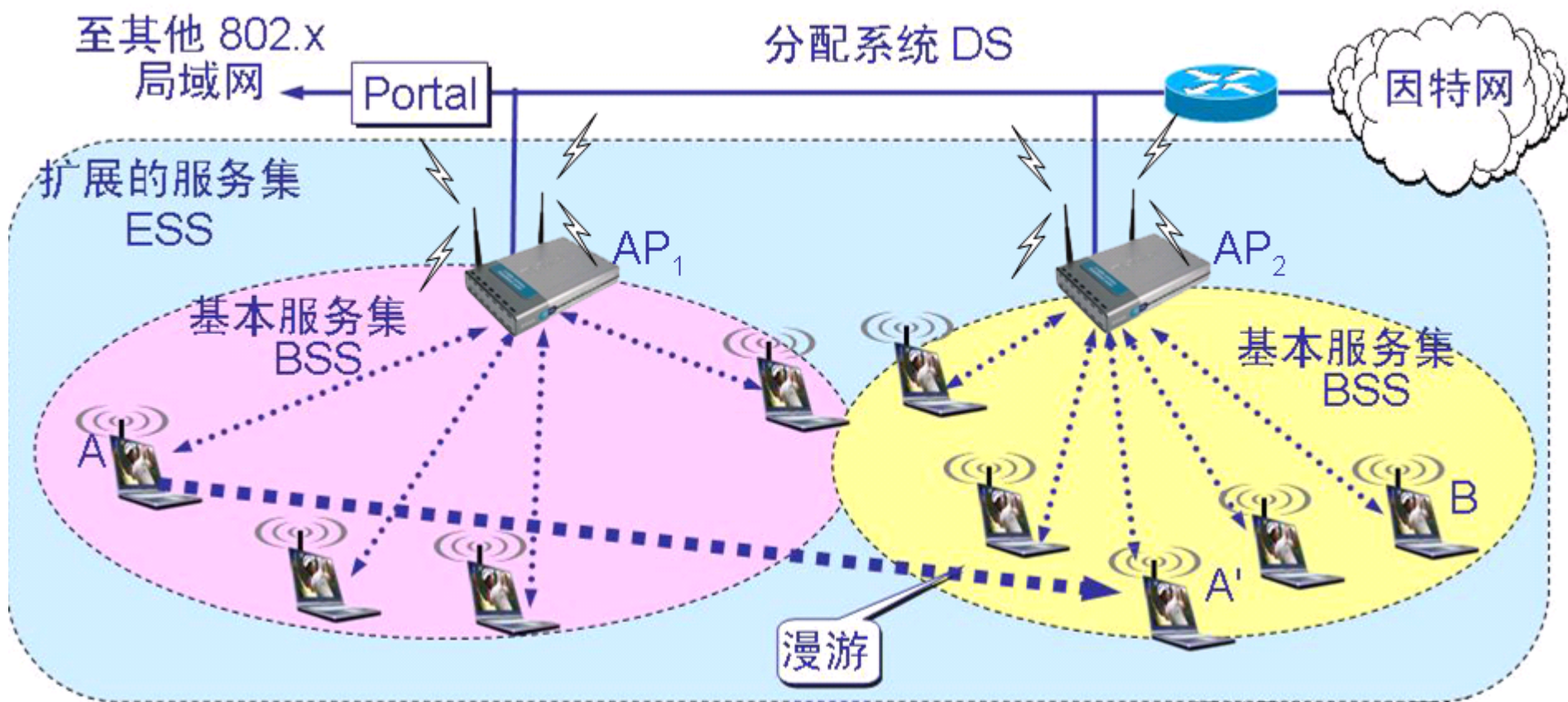
□ 难于解决移动站点问题

■ 无线网络利用电磁波在空中发送和接收数据，是对有线网络的补充和扩展

无线局域网的组成

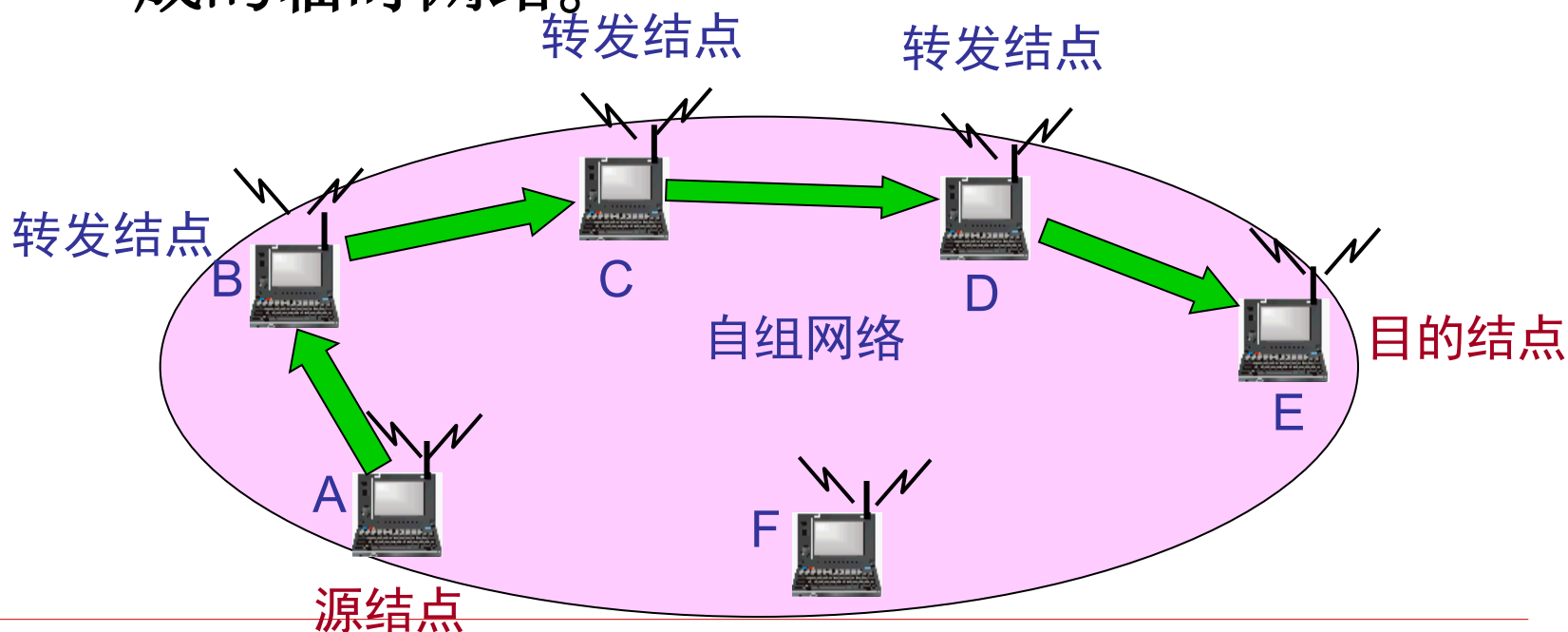
□ 1、有固定基础设施的无线局域网

- 预先建立起来的、能够覆盖一定范围的一批固定基站



无线局域网的组成

- 2. 移动自组网络, 又称**自组网络**(ad hoc network)
 - 没有**固定基础设施**(没有 AP)的无线局域网。
 - 由一些处于平等状态的移动站之间相互通信组成的临时网络。



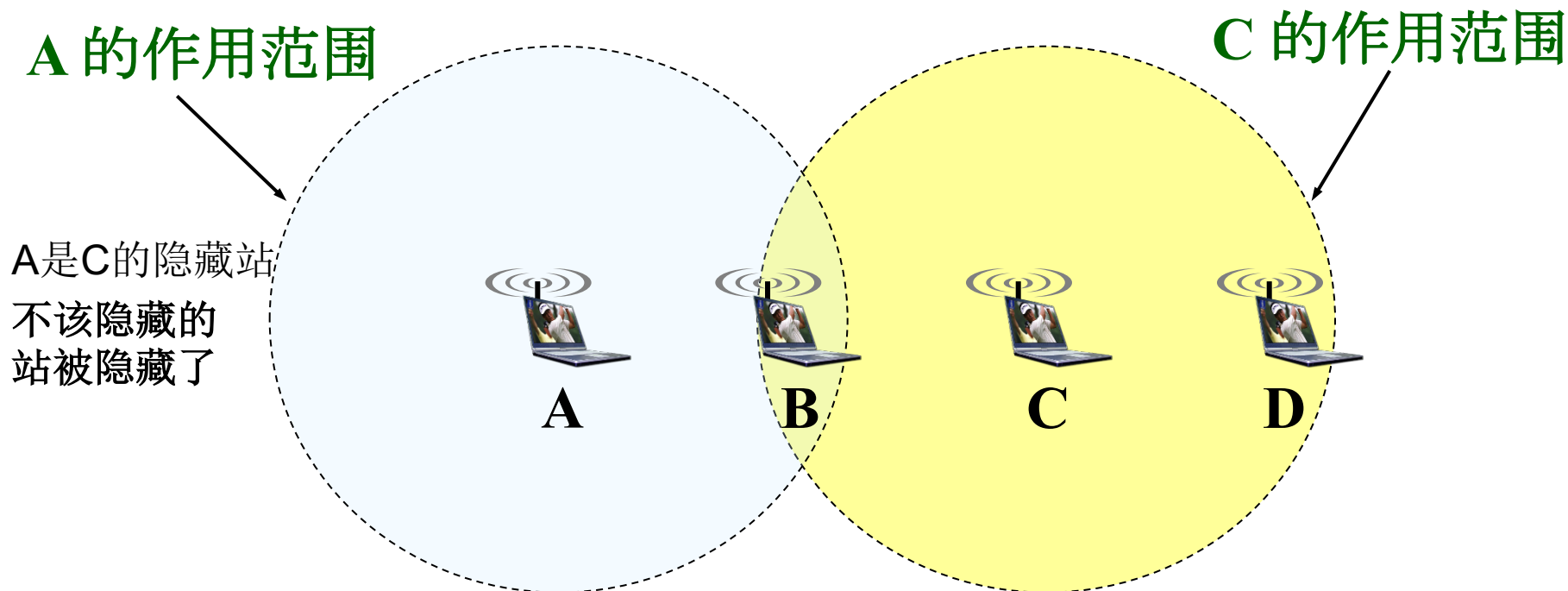
无线局域网的特殊性

- 共享介质：多个用户（站点）共享同一条公共信道
 - 发送站点先检测信道是否空闲（CSMA）
 - CSMA/CD是否适用？
 - 在WLAN的适配器上，接收信号的强度往往远小于发送信号的强度，要实现冲突检测，硬件上成本过高
 - 在WLAN中，并非所有的站点都能听见对方
-

无线局域网的特殊性

□ 隐蔽站问题

- 不能检测出介质上已存在的信号

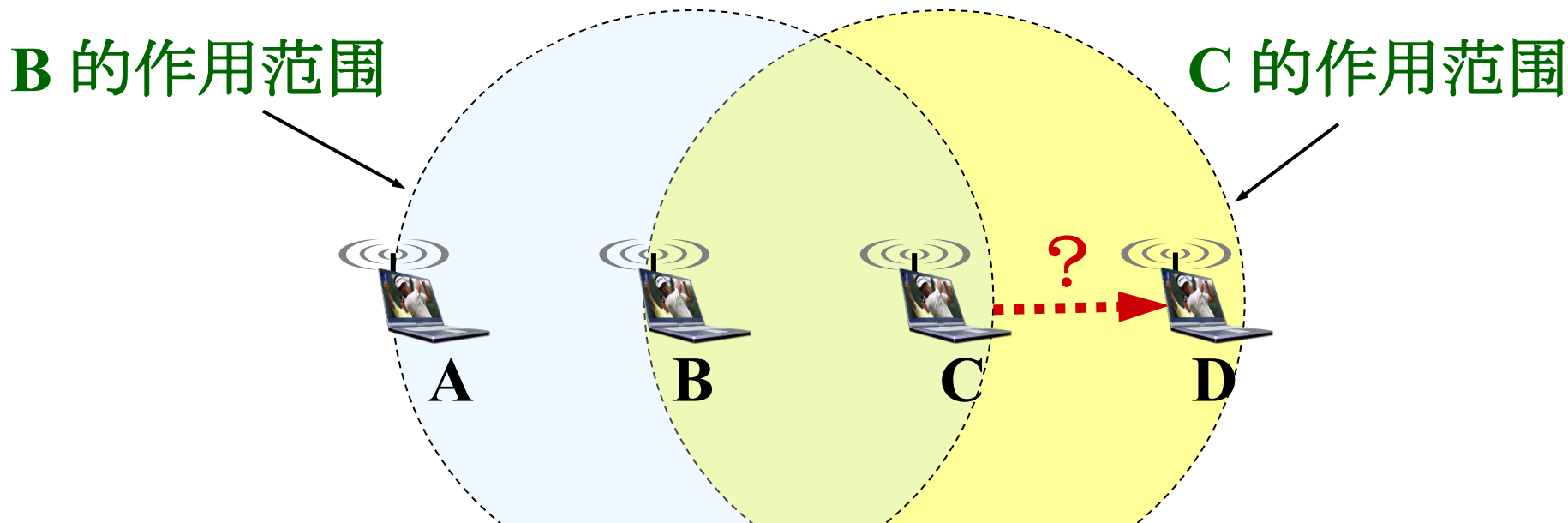


- 当 A 和 C 检测不到无线信号时，都以为 B 是空闲的，因而都向 B 发送数据，结果发生冲突。

无线局域网的特殊性

❑ 暴露站问题

- CSMA误判冲突：B 向 A 发送数据并不影响 C 向 D 发送数据



- B 向 A 发送数据，而 C 又想和 D 通信。
- C 检测到媒体上有信号，于是就不敢向 D 发送数据。

CSMA/CA协议

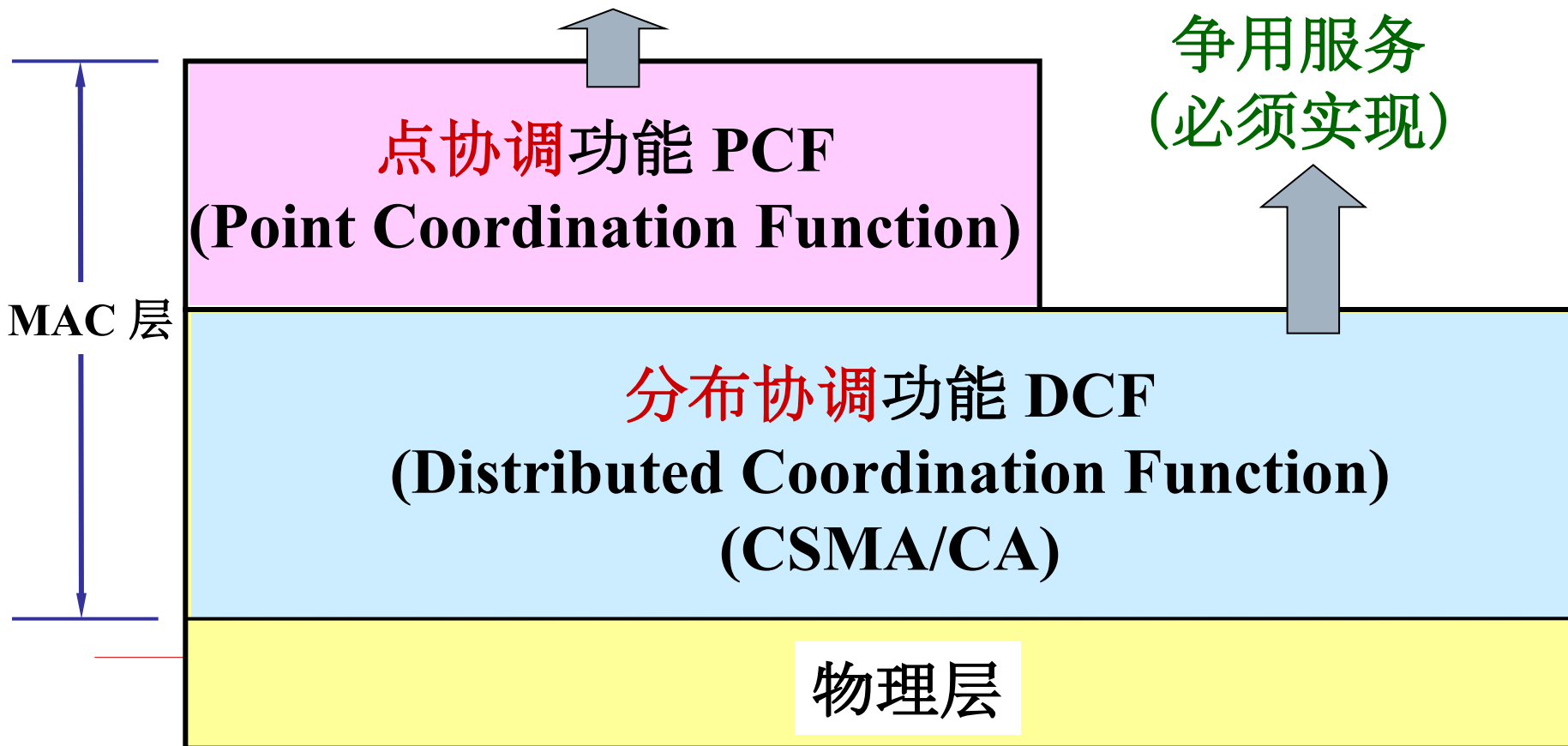
- CSMA/CD不适用
 - 改进：增加冲突避免(Collision Avoidance), 尽量减少冲突概率 → CSMA/CA
 - 发送前设法避免冲突的发生
 - “冲突避免”采用了三种机制
 - 预约信道：发送站点向其他站点通告本站点将要占用信道的的时间，其他站点将设置为“信道忙”
 - ACK：接收站点的确认
 - 握手：RTS/CTS，解决隐蔽站问题
-

CSMA/CA协议

➤ MAC 层通过**协调**功能来确定在基本服务集 BSS 中的移动站在什么时间能**发送数据**或**接收数据**。

无争用服务（选用）

争用服务
(必须实现)

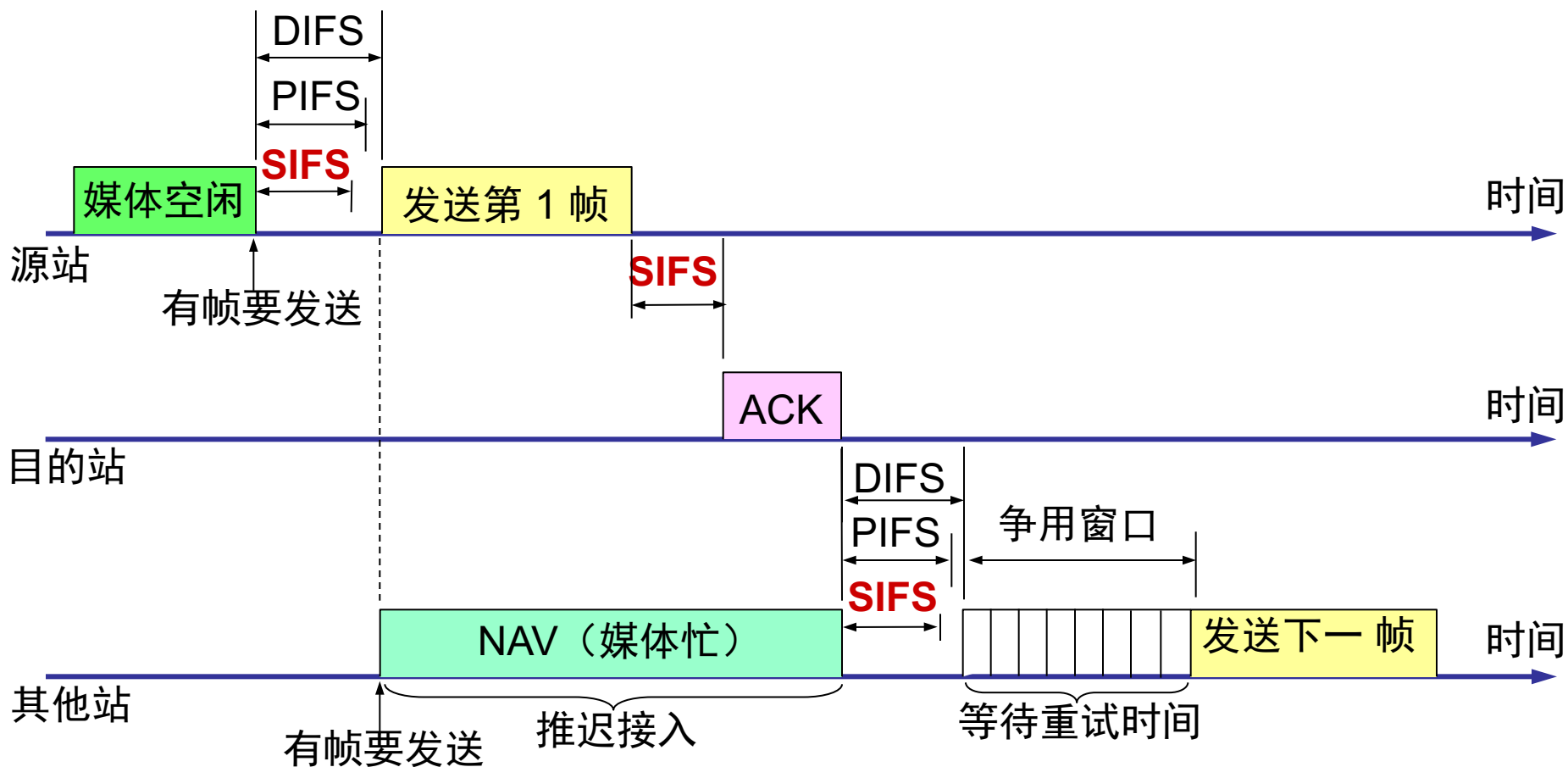


CSMA/CA协议

- 为避免冲突，站点在完成发送后，必须再等待一段很短的时间(持续监听)才能发送下一帧→
帧间间隔 IFS (InterFrame Space)
 - 帧间间隔长度取决于帧的优先级
 - **高优先级**帧IFS较短，优先发送
 - **低优先级**帧IFS较长；且在发送之前若其他站的高优先级帧已到达，则信道变为忙，低优先级帧只能再推迟发送
-

三种帧间间隔

$SIFS < PIFS < DIFS$



CSMA/CA协议

□ 发送站点

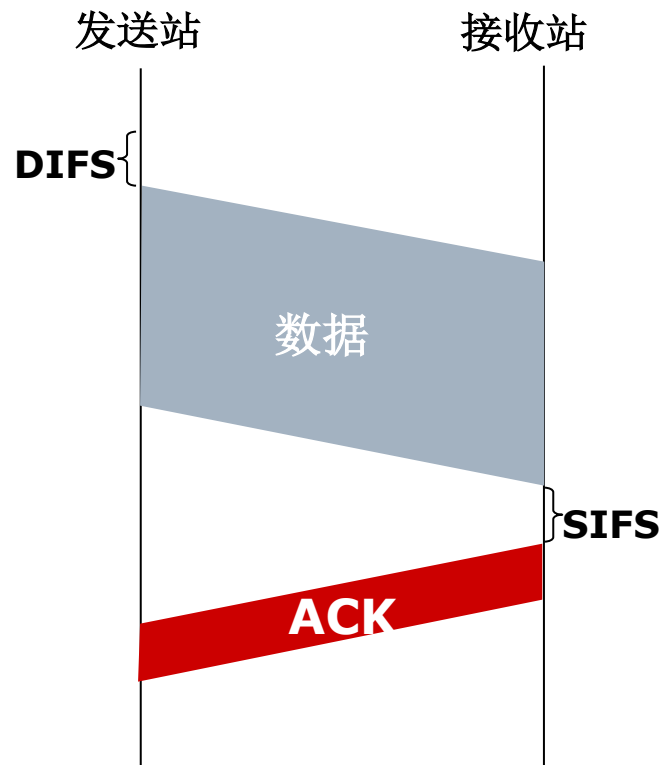
- 若监听到信道空闲时间达到**DIFS**，则发送
- 若信道忙，则开始退避，退避时间到则发送
- 若ACK超时，则增加退避时间

□ 接收站点

- 若收到数据帧，则在**SIFS**时间之后发送ACK

□ 其他站点

- 设置网络分配向量**NAV**



冲突避免措施：虚拟载波监听

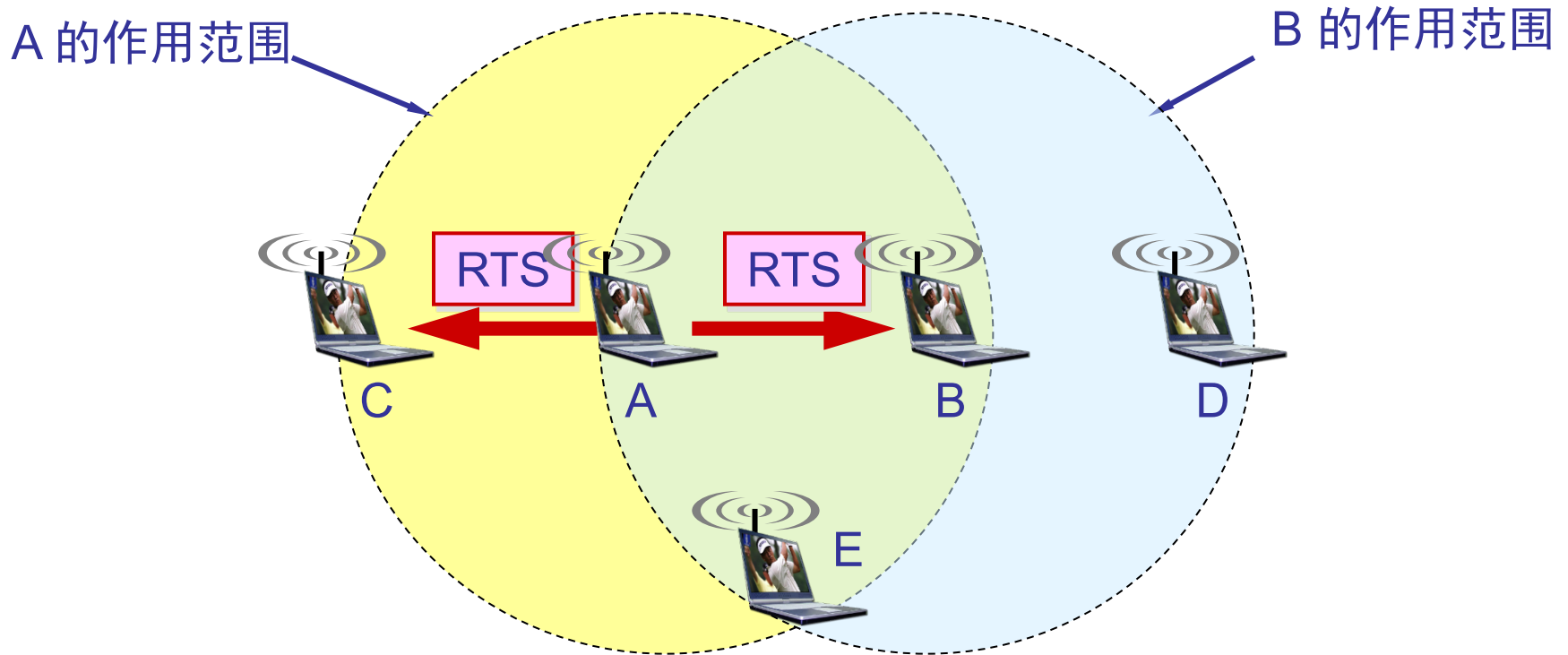
- 目的：发送站预约信道，以减少冲突，
- 原理：源站将要占用信道的时间(包括目的站发回确认帧所需的时间)通知给所有其他站，以使其他所有站在这一段时间都停止发送
 - 方法：源站在 **MAC 帧头** 中的“**持续时间**”字段中填入发送之后要占用信道的时间(μs)；其他站点根据收到的 MAC 帧头的“持续时间”字段来设置自己的网络分配向量NAV（信道持续忙的时间）
- “**虚拟**载波监听”：站点并没有监听信道，而是由于收到“源站的通知”才不发送数据

冲突避免措施：争用窗口与退避

- 信道从忙态变为空闲时，任何一个站要发送数据帧，不仅必须等待 DIFS，而且还要进入争用窗口，根据退避时间确定能否发送
- 争用窗口：各站点争用信道的时间段，其时间取决于站点最短的剩余退避时间
 - 在信道从忙态转为空闲时，各站就要执行退避算法，减少了发生冲突的概率
 - 二进制指数退避算法（略）
 - 扩展退避的时间范围，减少不同站点选择相同退避时间的概率

冲突避免措施：握手预约（可选）

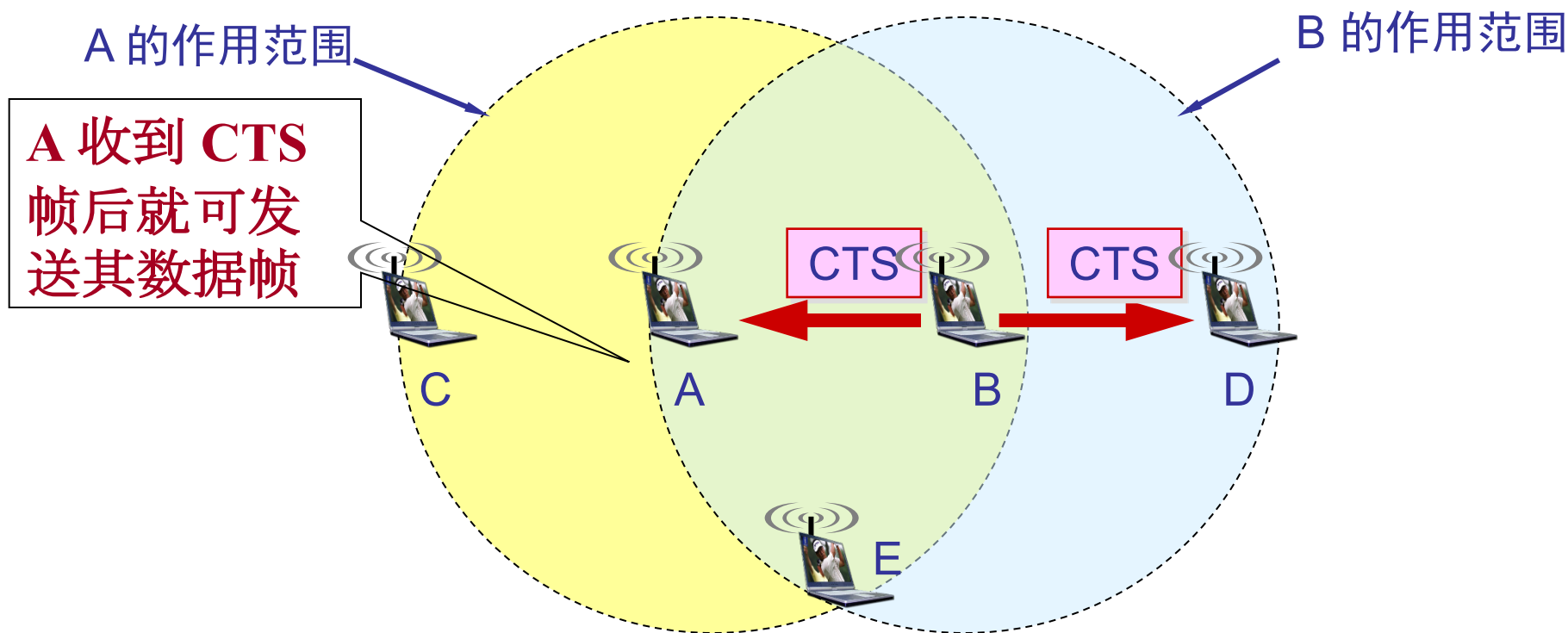
——源站发RTS



- 源站 A 发送一个 **RTS** (Request To Send)
- 帧中包括源地址、目的地址和这次通信所需的时间

冲突避免措施：握手预约（可选）

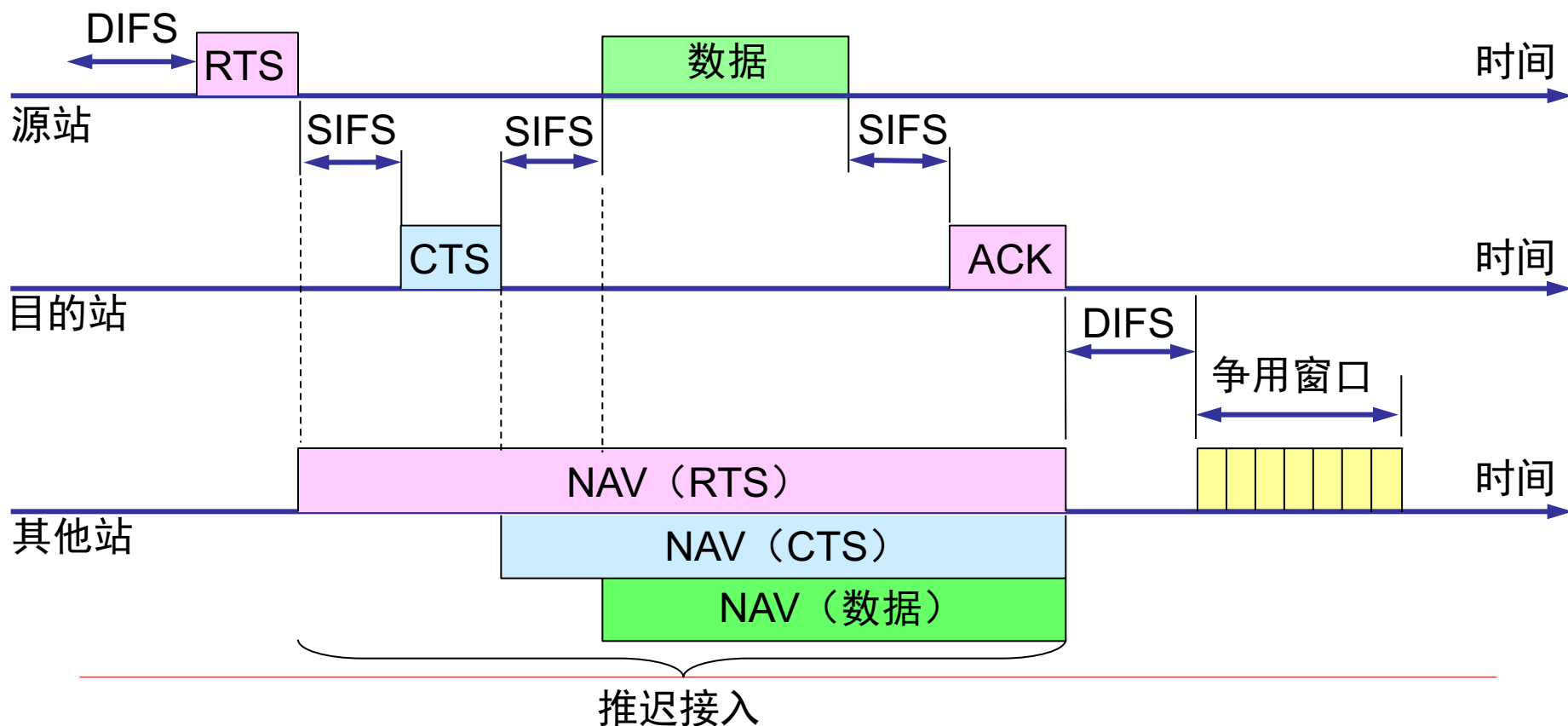
——目的站发CTS



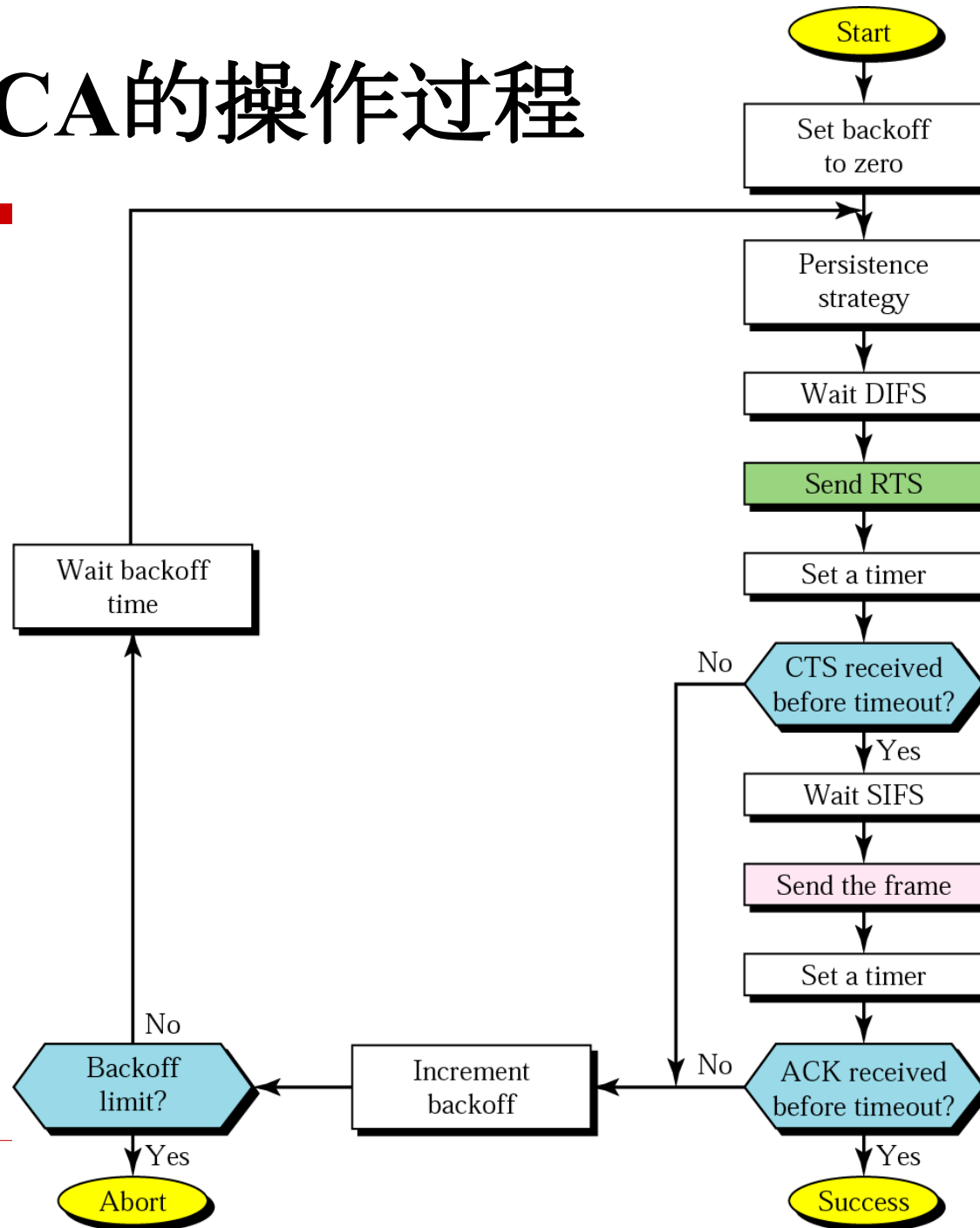
- 目的站 B 发送 **CTS** (Clear To Send)
- 帧中包括这次通信所需的时间(从 RTS 帧中复制)

RTS/CTS与NAV

➤ RTS 和 CTS 帧以及数据帧和ACK 帧的传输时间关系



CSMA/CA的操作过程

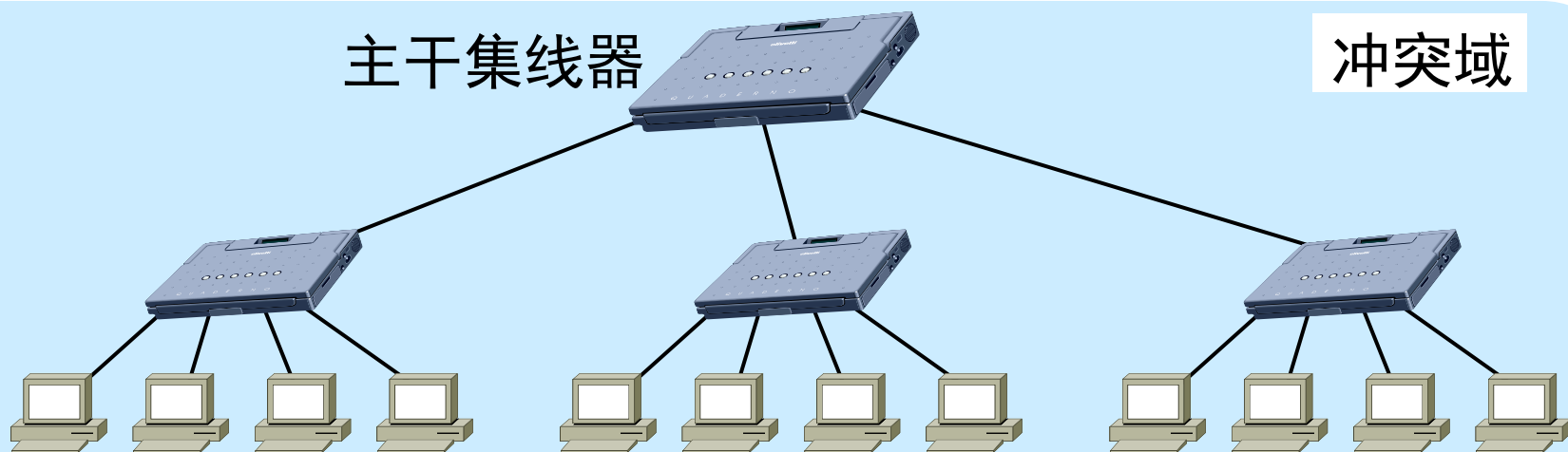


主要内容

- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

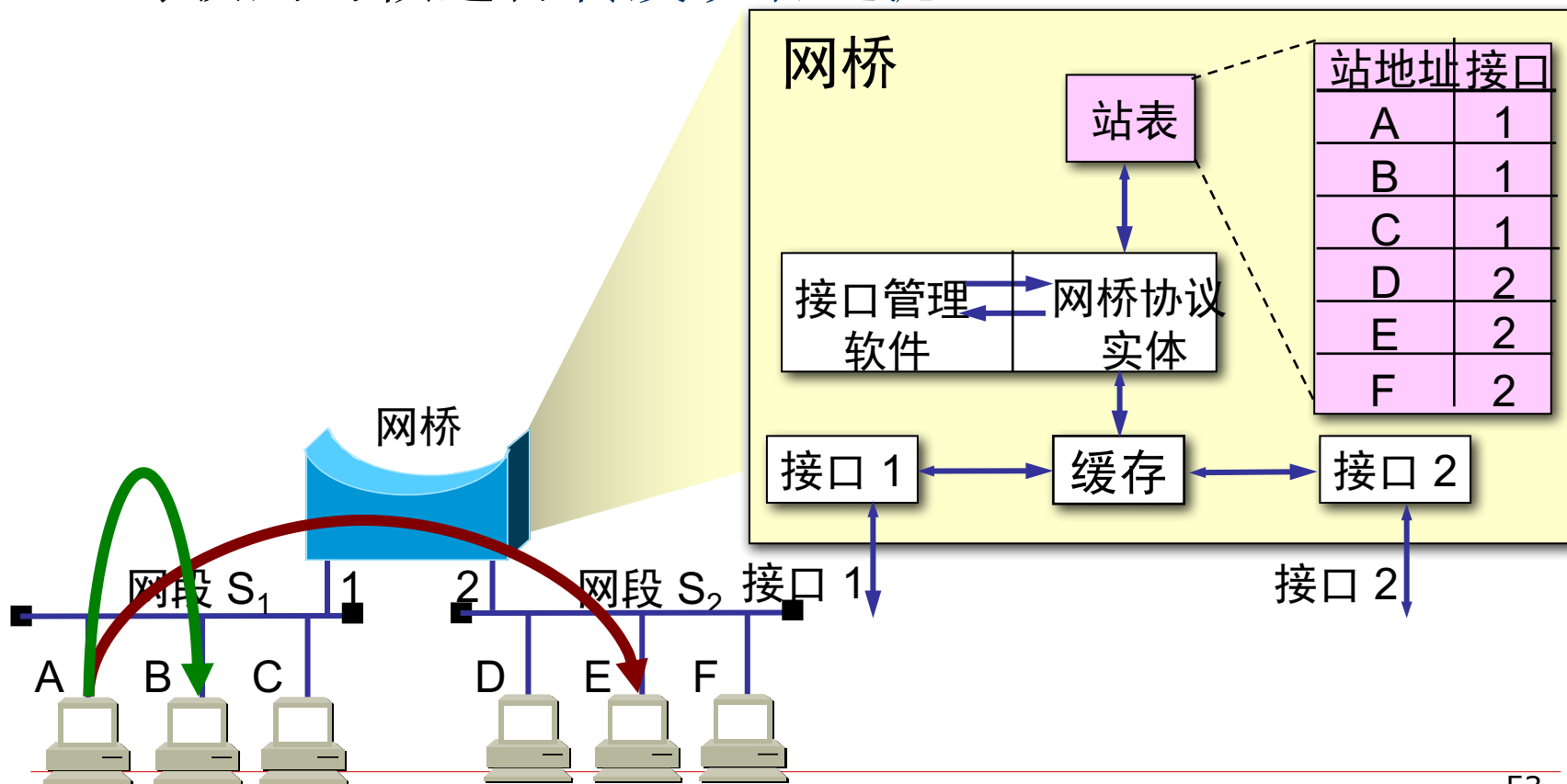
在物理层扩展LAN

- 功能：扩展LAN的地理覆盖范围
- 设备：中继器、集线器（HUB）
- 特点：**复制**信号，再生放大，转发到所有端口，连接后仍属于一个LAN，形成**一个更大冲突域**，**吞吐量没有提高**；
- 冲突域：可能发生数据帧冲突的网络范围，冲突域越大，冲突概率越高



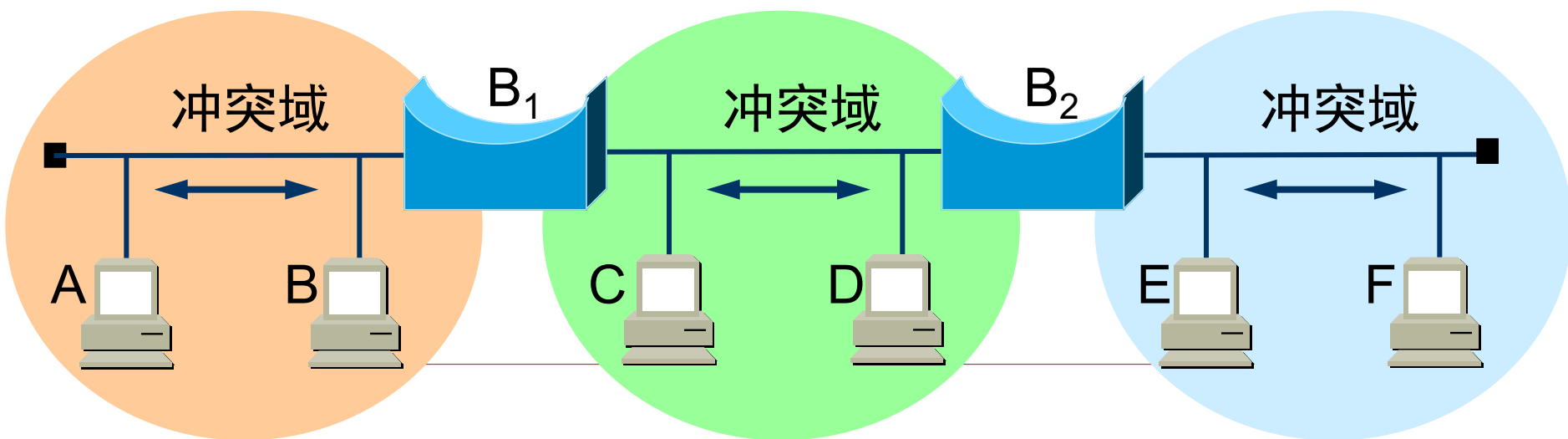
在数据链路层扩展局域网：网桥

- 网桥(bridge) 根据MAC 帧的目的地址查找站表确定对收到的帧进行转发或者过滤



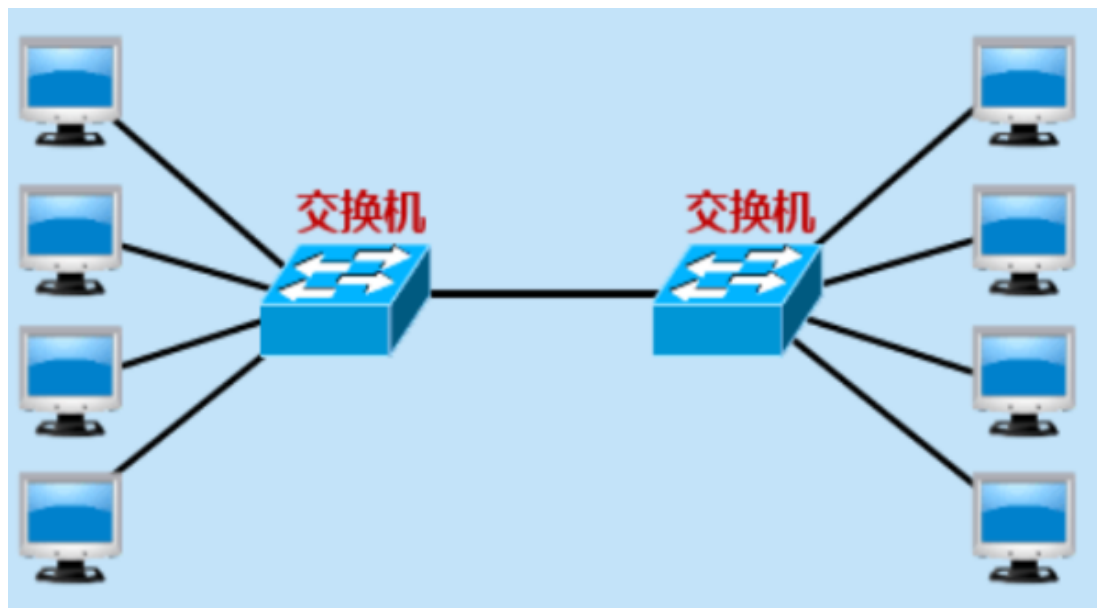
网桥的优点

- ❑ 过滤通信量，增大吞吐量；分隔冲突域；扩大了物理范围；提高了可靠性
- ❑ LAN互连：可互连不同物理层、不同MAC子层和不同速率(10 Mbps, 100 Mbps)的LAN



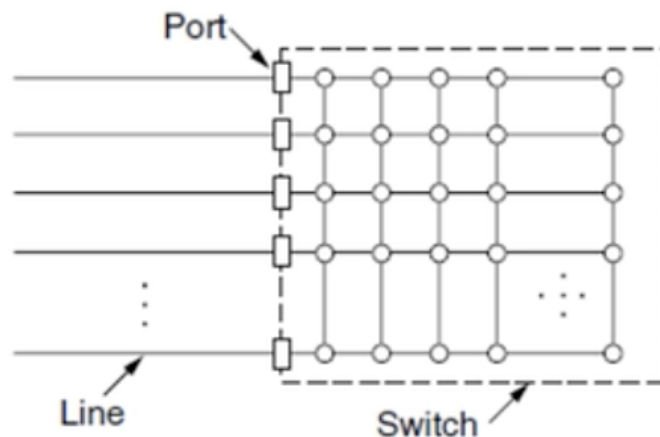
在数据链路层扩展局域网：交换机

- 交换式集线器(switching hub), 1990年问世
- 常称为以太网交换机(LAN Switch)或第二层交换机
- 通常有十几个接口, 实质上是多接口网桥
- 组成交换式以太网



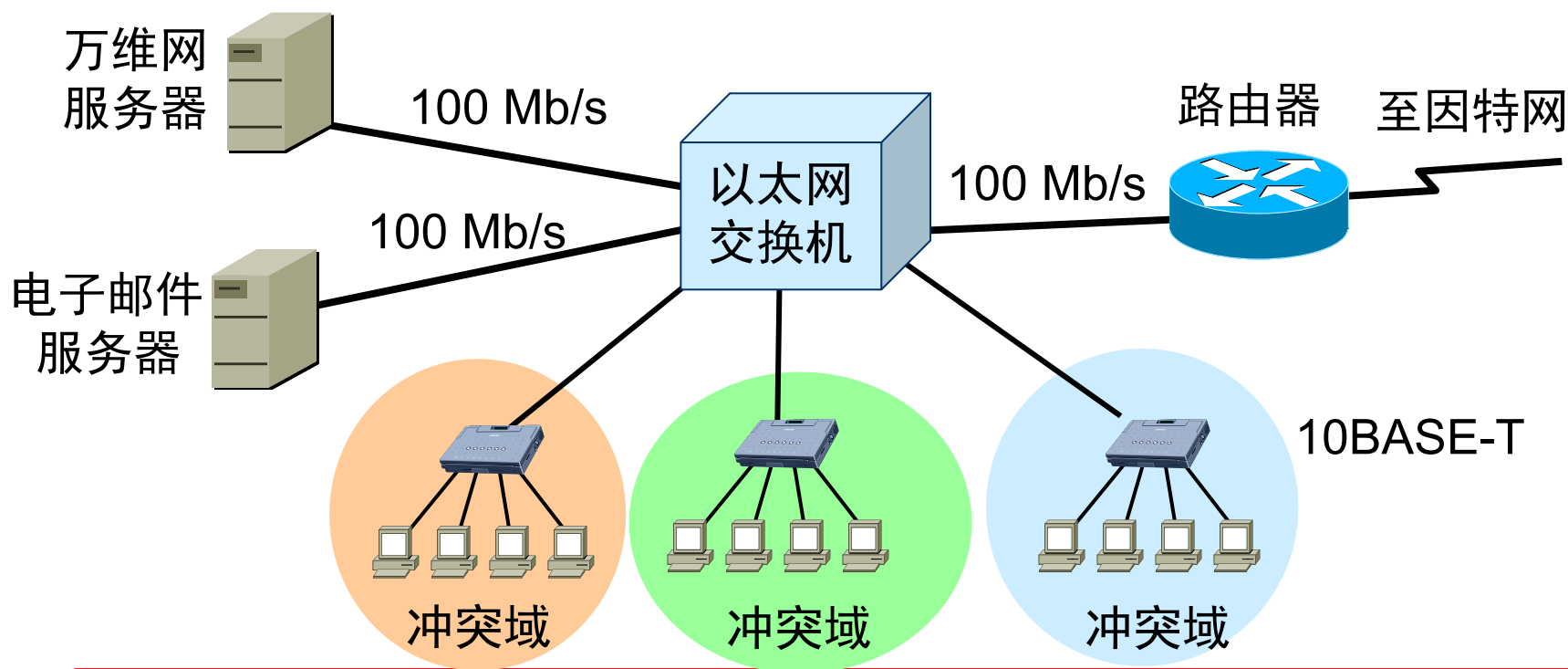
LAN交换机的特点

- 每个接口都直接与主机相连，并且工作在全双工方式，每个接口和连接到接口的主机形成了碰撞域。
- 交换机能同时连通多对接口，使每对相互通信的主机都能像独占通信介质那样，无冲突地传输数据（非CSMA/CD）
- 使用了专用的交换结构芯片，交换速率较高
- 即插即用设备，帧转发表通过逆向学习算法建立



LAN交换机的特点

- 交换机的每个接口是一个冲突域
- 对于拥有 N 对接口的交换机的总容量为 $N \times 10 \text{ Mbps}$



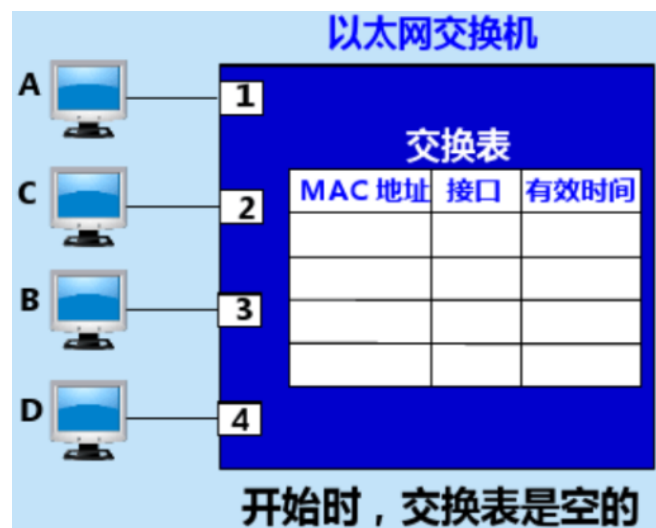
LAN交换机的自学习：逆向学习

□ 自学习算法：

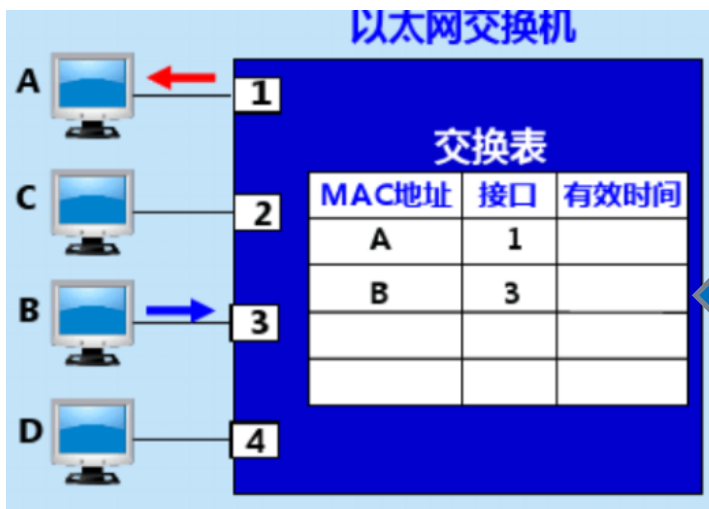
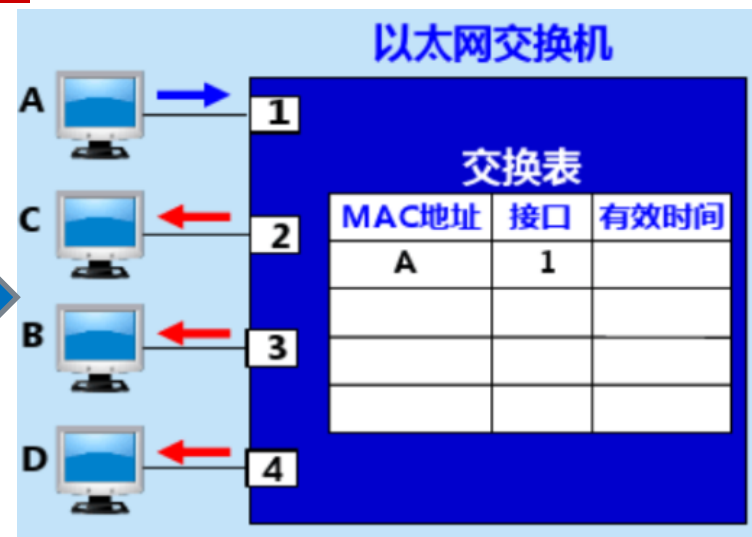
站点 A 发出的帧从端口 x 进入了交换机B，则交换机B可以把发送给站点A的帧转发到端口x，A一定能收到

- 交换机每收到一帧，就记录其源地址和进入交换机的端口，作为交换表中的一项
- 建立交换表时是把帧头的源地址写在“地址”这一栏的下面
- 转发帧时，根据收到的帧头的目的地址来转发（这时把之前记录的源地址当作目的地址，把记录的进入端口当作转发端口）

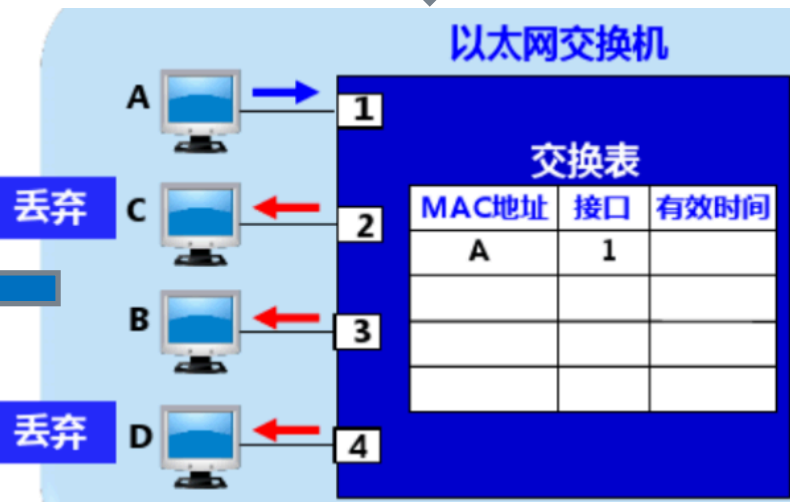
自学习示例



A发送B



B回应A



丢弃

丢弃

总结：交换机的工作过程

- 交换机收到一帧后，先进行**逆向学习**，查找交换表中是否有该帧的源地址
 - ◆ 若没有，就增加一个表项（源地址、进入端口和时间）
 - ◆ 若有，则更新原表项
- **转发帧**：查找交换表中是否有该帧的目的地址
 - ◆ 若没有，则**洪泛**转发，即转发到所有其他端口
 - ◆ 若有（且不是进入接口），则**转发到**表中的**对应端口**
 - ◆ 若有且等于进入接口，则丢弃这个帧（过滤）
- 自学习方法使得交换机能够即插即用

星形以太网

□ 总线以太网

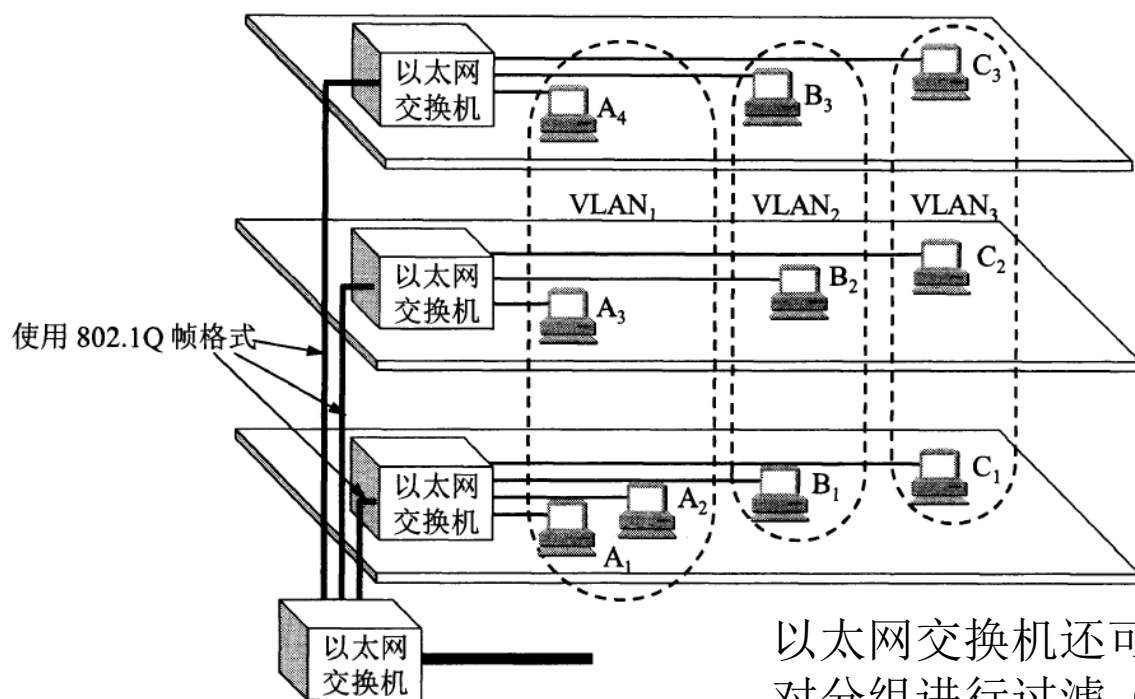
- 采用无源的总线结构
- 使用**CSMA / CD**协议，半双工方式

□ 星形以太网

- 以太网交换机为中心的星形结构
- 不使用共享总线，没有冲突问题，不使用**CSMA / CD**协议，全双工方式工作。但仍然采用以太网帧结构

虚拟局域网VLAN

- 定义：由一些局域网网段构成的与物理位置无关的逻辑组，而这些网段具有某些共同的需求。每个VLAN的帧都有一个明确的标识符，指明发送这个帧的计算机属于哪一个VLAN。（IEEE 802.1Q标准定义）
- 只是局域网给用户的一种服务，而不是一种新型局域网



虽然A4、B3、C3连在同一台交换机上，但B3、C3收不到A4在VLAN1中的消息

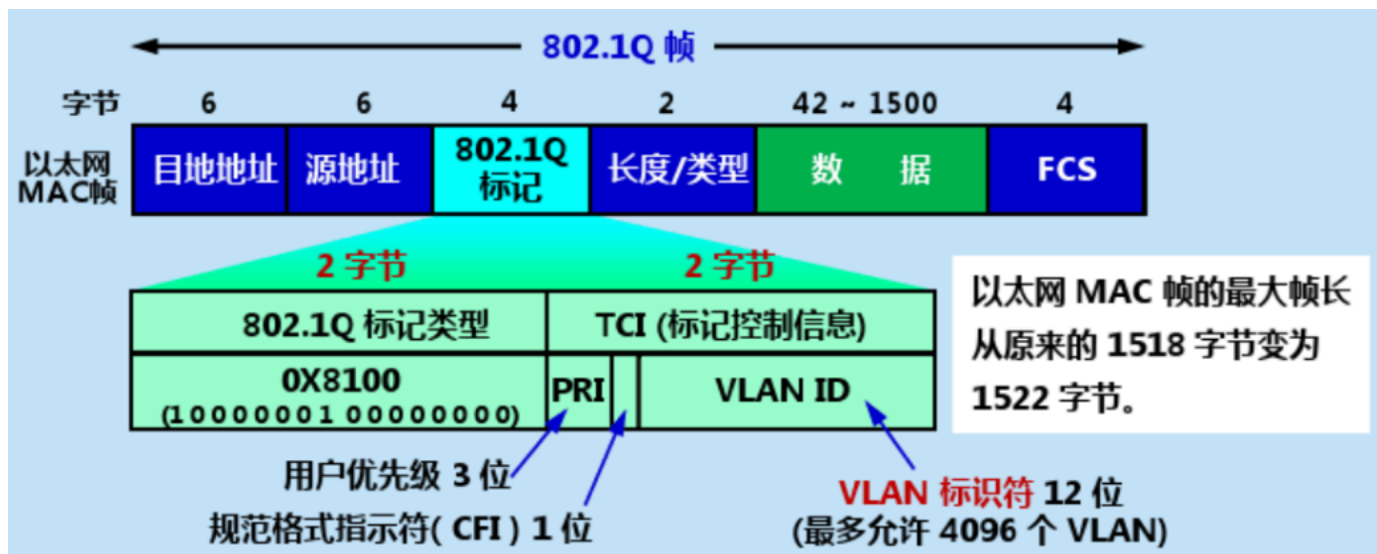
虽然A1、A2、A3、A4不在同一台交换机上，但A2、A3、A4能收到A1在VLAN1广播的消息

VLAN限制了接收广播消息的计算机数，抑制了广播风暴！

以太网交换机还可工作在第三层，依据IP地址对分组进行过滤（三层交换机）

虚拟局域网VLAN

- VLAN标记（802.3ac标准）：
- 允许在以太网帧格式中插入4字节标识符（VLAN tag），用来指明发送该帧的计算机属于哪一个VLAN。
- 插入VLAN tag的帧称为802.1Q帧
- 标记类型：2字节，0x8100
- 用户优先级3bit + 规范格式指示符(CFI) 1bit + VLAN标识符(VID) 12bit



对LAN交换机的安全威胁： MAC地址洪泛攻击

- ❑ 在LAN交换机中，交换机的端口与所连接设备的MAC地址的映射保存在CAM (Content Addressable Memory，内容寻址存储器)中
- ❑ 收到数据帧时，LAN根据CAM表确定转发的端口
- ❑ MAC地址泛洪攻击又称为CAM表溢出攻击
- ❑ 攻击者向交换机发送大量虚构的具有不同源MAC地址的数据帧，导致交换机的CAM表填满，交换机进入失效开放（fail open）模式，对收到的数据帧进行洪泛式转发
- ❑ 攻击者将截获来自所有其他主机的信息

本章小结

- LAN的体系结构：物理层和数据链路层(及两个子层)
- LAN的特点以及局域网具有的技术特征
- 以太网的工作原理，CSMA/CD、MAC地址
- WLAN：CSMA/CA、隐蔽站/暴露站问题
- 局域网的扩展：在不同层次上实现的优缺点？交换机、逆向学习及转发

版权说明

- 本讲义中有部分图片来源于下列教材所附讲义：
 - 谢希仁，计算机网络，第八版，电子工业出版社，2021年6月，引用时标记为[谢]；
 - Behrouz A. Forouzan, Data Communications and Networking, Fourth Edition, McGraw-Hill Higher Education, 2007年1月，引用时标记为[Forouzan]
 - James F. Kurose, Keith W. Ross著，陈鸣译，计算机网络：自顶向下方法，机械工业出版社，2009，引用时标记为[Kurose]；
 - 部分图片来源于网络，未找到确切来源，引用时标记为[来源于网络]。