北京郵電大學

计算机网络

第六章 局域网
LAN

网络空间安全学院

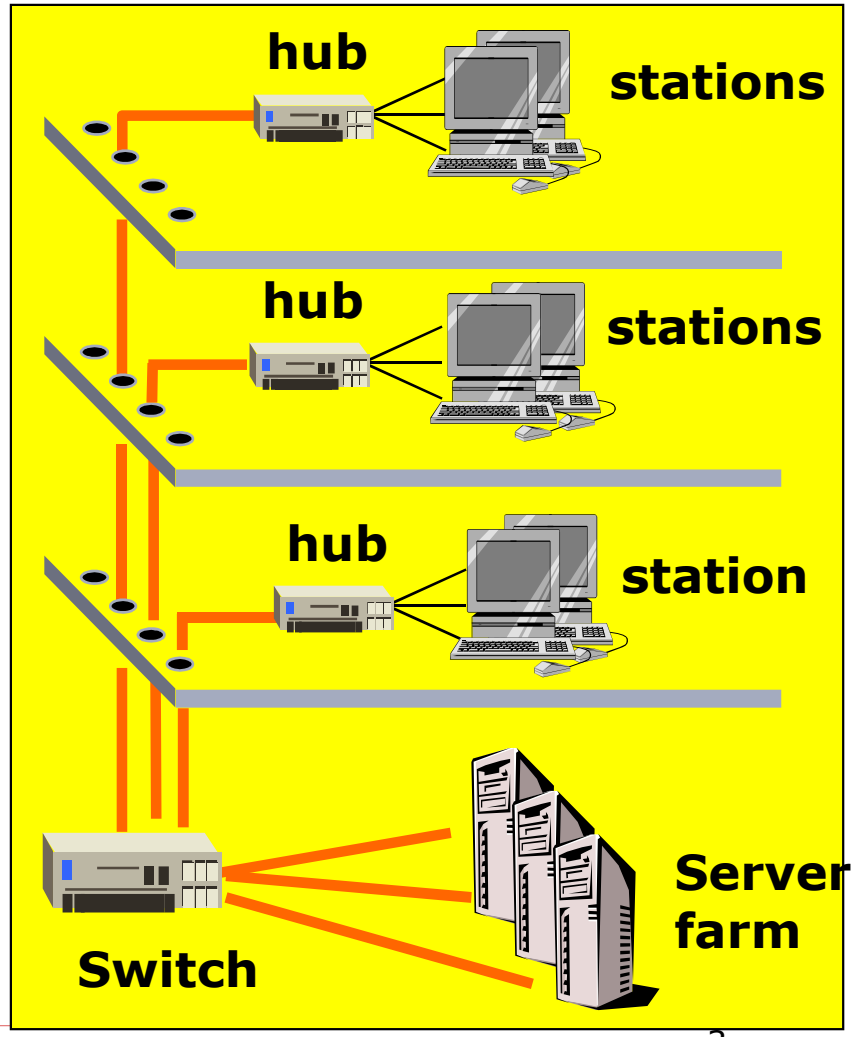
2019年12月

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

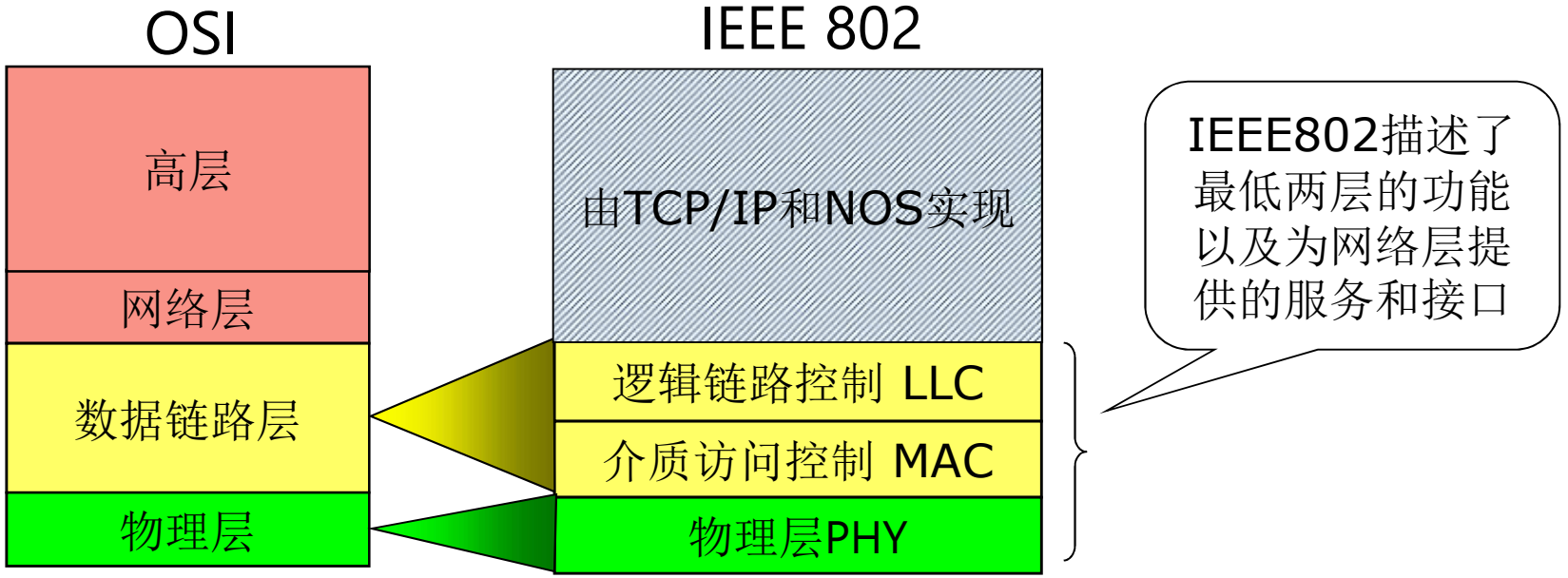
局域网（LAN）概述

- LAN的特点
  - 覆盖范围小
    - 房间、建筑物、园区范围
  - 高传输速率
    - 10Mbps～1000Mbps
  - 低误码率
    - 10^{-8} ～ 10^{-11}
  - 拓扑：总线型、星形、环形
  - 传输介质：双绞线、光纤、同轴电缆
  - 专用网络：自建、自管、自用



局域网参考模型

- 局域网的标准：IEEE802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



局域网的物理层

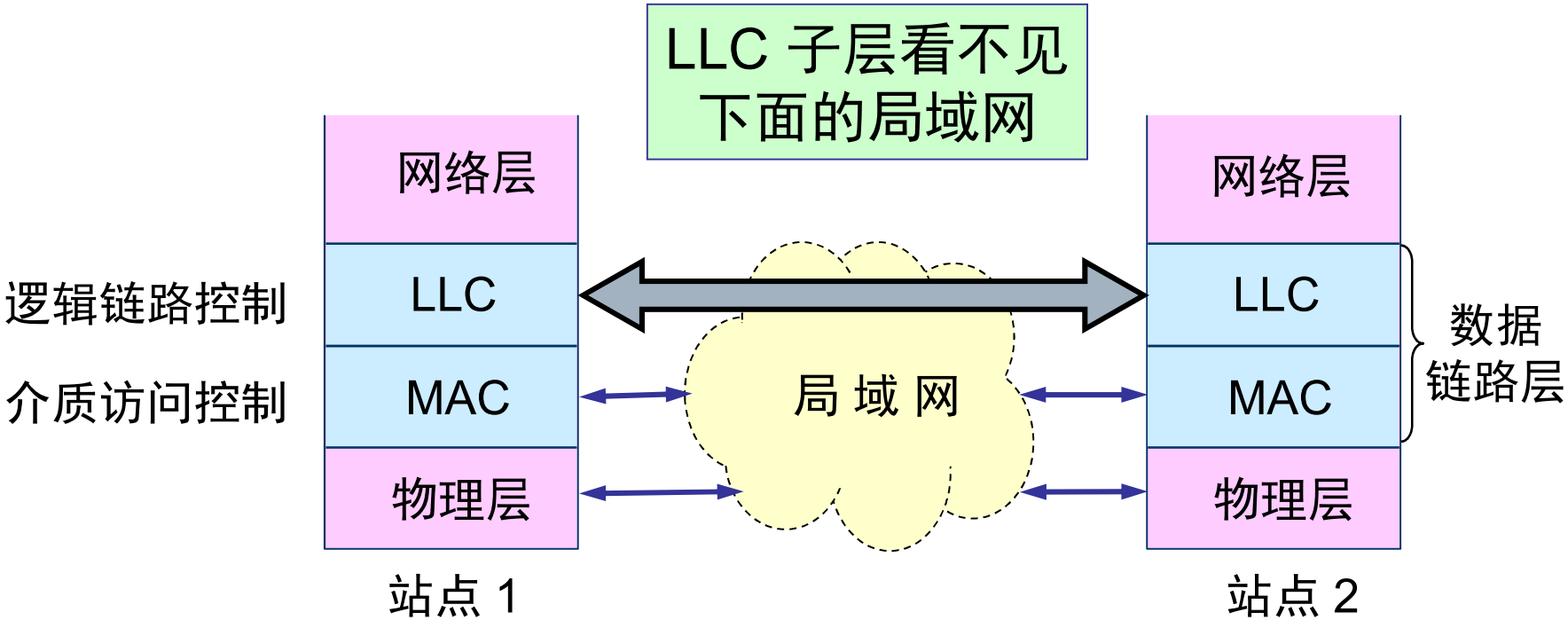
- 功能：
  - 位流（bit stream，位串）的传输与接收；
  - 同步前序码的产生与识别；
  - 确定与传输媒体接口的特性；
  - 信号编码和译码。
- IEEE802定义了多种物理层，以适应不同的网络介质和不同的介质访问控制方法。

局域网的数据链路层

- 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。*

局域网的数据链路层

- 局域网对 LLC 子层是透明的



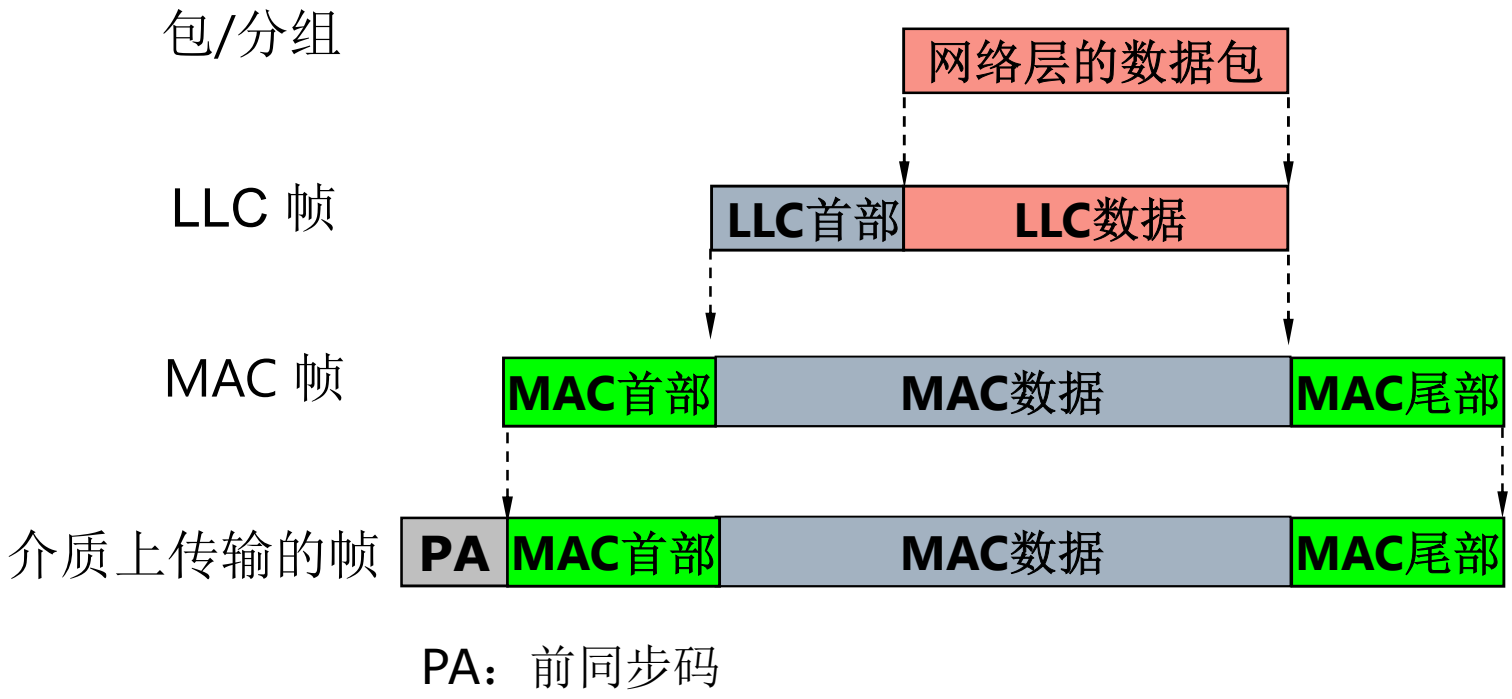
LLC子层的功能

- 向高层提供统一的链路访问形式
- 组帧/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
  - *对不同的LAN标准，它们的LLC子层都是一样的，区别仅在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

LAN的数据封装



PA：前同步码

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，大致格式如下

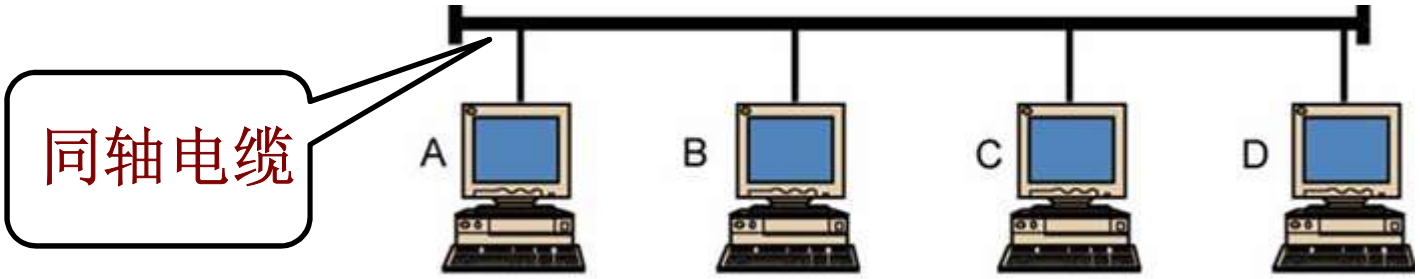
MAC控制	目的MAC地址	源MAC帧地址	LLC 帧	CRC

介质访问控制方法

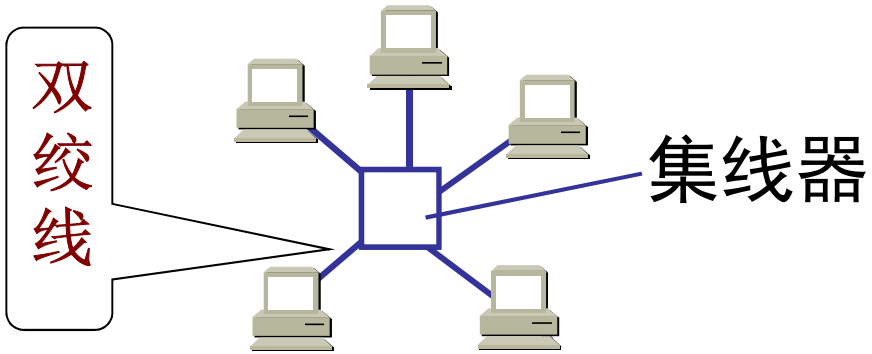
- 局域网使用广播信道（多点访问、随机访问），多个站点共享同一信道。
  - 各站点如何访问共享信道？
  - 如何解决同时访问造成的冲突（信道争用）？

    → 介质访问控制(MAC)
- 两类信道共享技术：
  - 静态分配（FDM、WDM、TDM、CDM）
    - 不适用于LAN
  - 动态分配（随机接入、受控接入）
    - CSMA/CD、集中控制（如轮询、传递令牌）

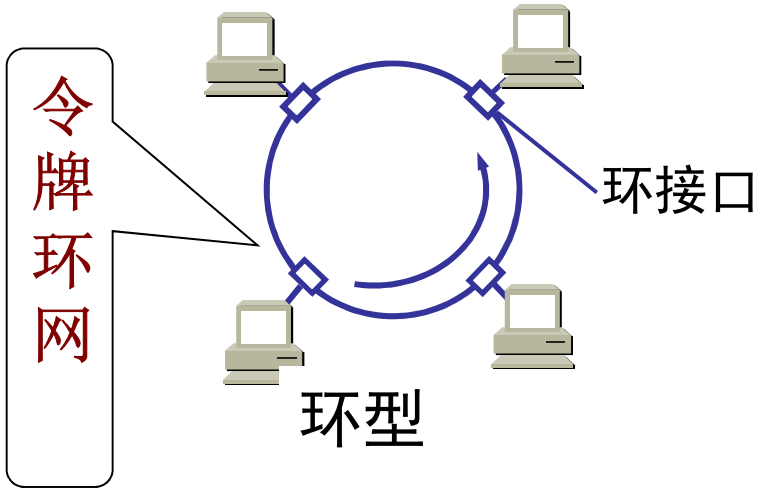
局域网的拓扑结构



总线型



星型



环型

主要内容

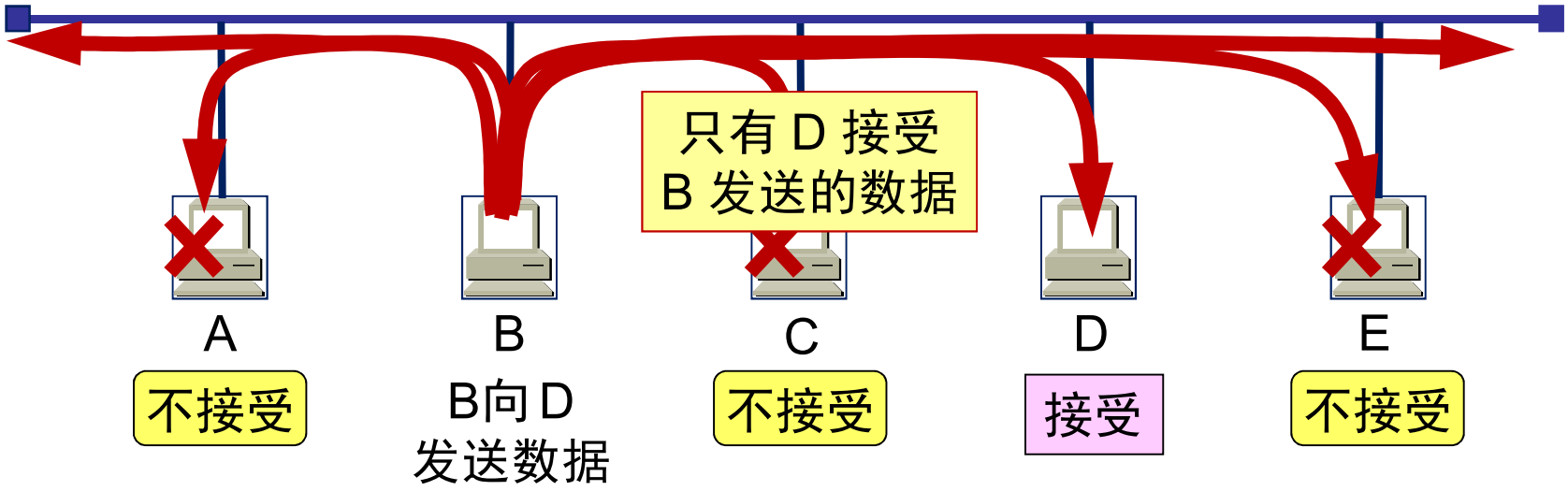
- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

以太网

- 20世纪70年代中期,由施乐公司（Bob Metcalfe）提出，数据率为2.94Mbps，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10Mbps标准（DIX Ethernet II标准）
- 1985年，IEEE 802.3标准发布，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
- 目前已发展到万兆以太网，仍在继续发展 …

以太网：CSMA/CD 协议

- 载波监听/冲突检测协议
- 传统以太网：总线拓扑，广播通信



CSMA/CD 协议

- 广播方式发送
  - ✓ 总线上每一个工作的计算机都能检测到 **B** 发送的数据信号
  - ✓ 在帧的首部写入目的地址，只有计算机 **D** 的地址与帧首的木器地址一致，因此只有 **D** 才接收这个数据帧
  - ✓ 其他的计算机（**A, C** 和 **E**）都检测到不是发送给它们的数据帧，就丢弃这个数据帧而不接收
  - ✓ 在具有广播特性的总线上实现了一对一通信

以太网协议要点：CDMA

- 多个站点如何安全地使用共享信道？
  - 载波监听：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？
      - 若有多个站点都在等待发送，必然冲突！
      - 解决：等待一段随机时间后再发（降低了冲突概率）
    - 若信道忙，如何处理？
      - 继续监听，等到信道空闲后立即发送

以太网协议要点：CD

- 一旦出现两个站点同时发送的情况，如何处理？
- 冲突检测：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

总结：CSMA/CD协议

- 用于**IEEE802.3**以太网
- 工作原理：
  - 发送前先监听信道是否空闲，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，仍需继续监听。若监听到冲突，则立即停止发送数据，然后发送冲突强化信号**Jam**
    - 发送**Jam**信号的目的是使所有的站点都能检测到冲突
  - 等待一段随机时间（称为退避）以后，再重新尝试。
- 归结为四句话：
  - 发前先听，空闲即发送，边发边听，冲突时退避。

CSMA/CD

载波监听多点接入/冲突检测

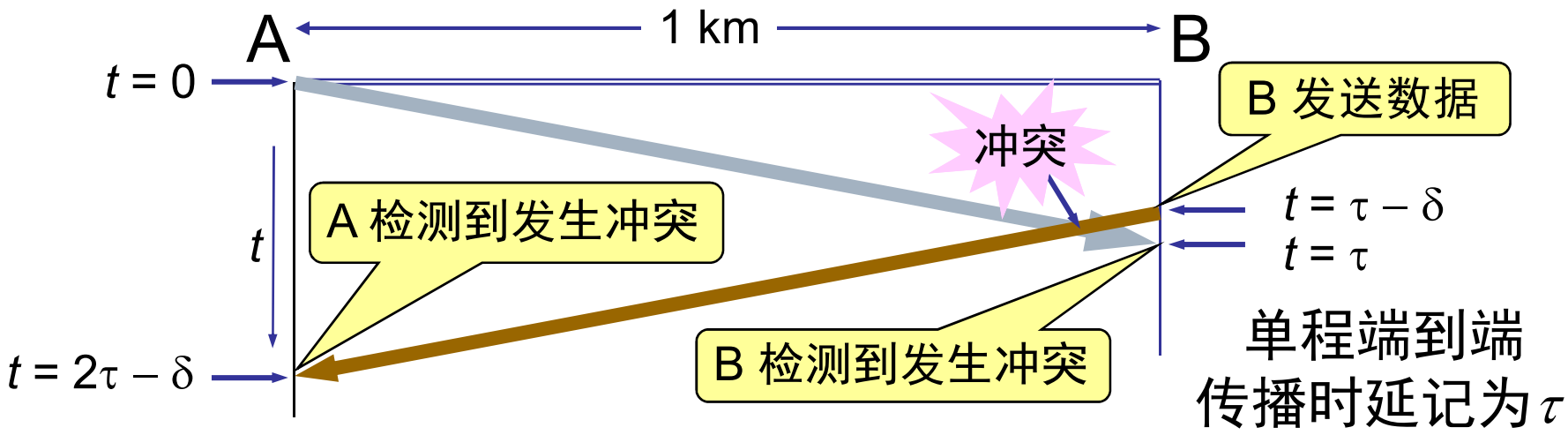
- “多点接入”表示许多计算机以多点接入的方式连接在一根总线上。
- “载波监听”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生冲突。
- “冲突检测”就是计算机边发送数据边检测信道上的信号电压大小。当信号电压摆动值超过一定的门限值时，认为总线上至少有两个站同时在发送数据，产生了冲突(碰撞)。立即停止发送，然后等待一段随机时间后再次发送。

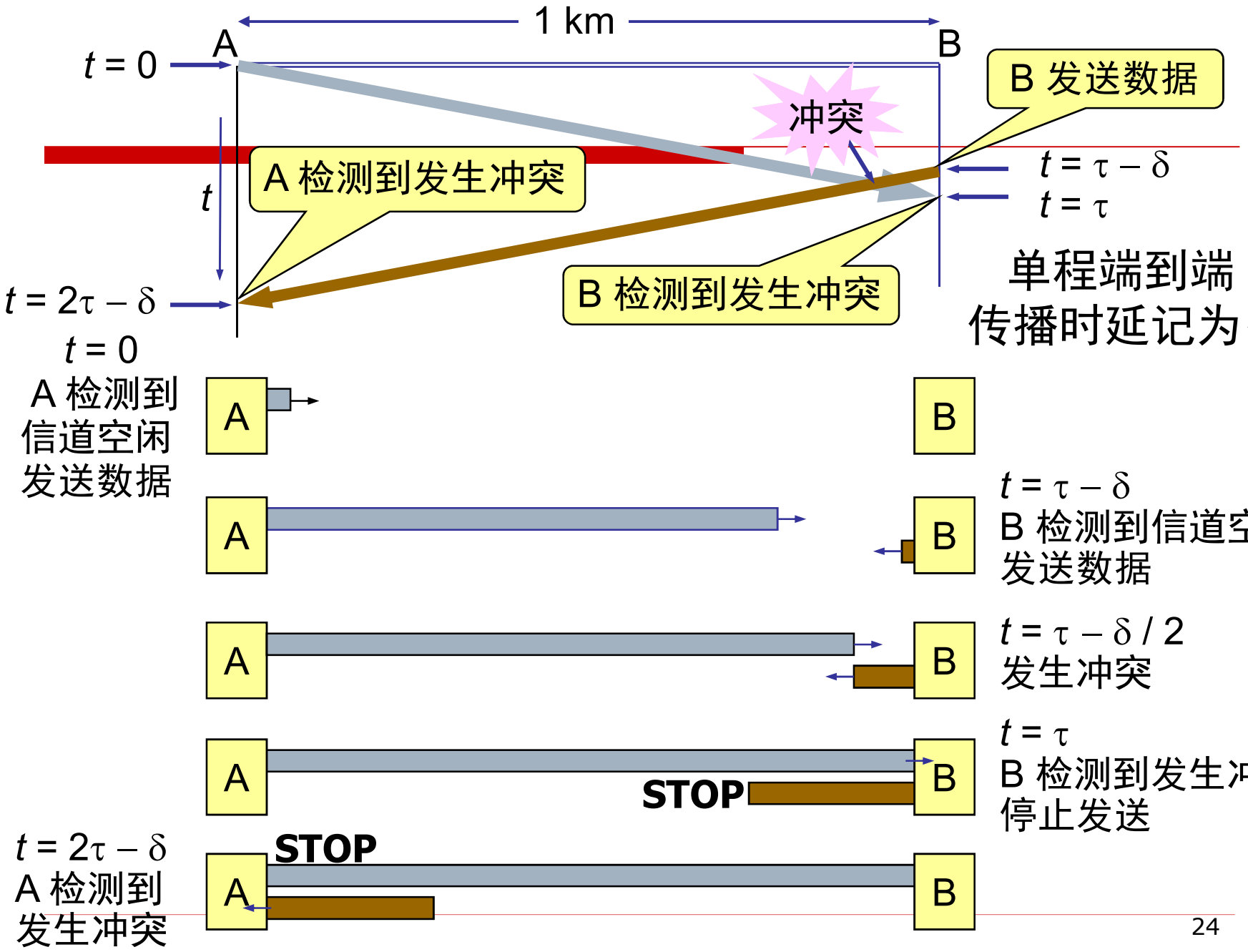
为什么会冲突？

- 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，因为电磁波以有限速率传播
  - ✓ **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，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。

传播时延与冲突

- 传播时延对载波监听的影响




1 km
A
B
t = 0
B 发送数据
冲突
A 检测到发生冲突
t
t = τ – δ
t = τ
B 检测到发生冲突
t = 2τ – δ
单程端到端
传播时延记为τ
t = 0
A 检测到
信道空闲
发送数据
A
B
t = τ – δ
B 检测到信道空闲
发送数据
t = τ – δ / 2
发生冲突
STOP
t = τ
B 检测到发生冲突
停止发送
STOP
t = 2τ – δ
A 检测到
发生冲突

CSMA/CD 协议的争用期

- 最先发送数据帧的站，在发送数据帧后至多经过时间 2τ (两倍的端到端往返时延)就可知道发送的数据帧是否遭受了冲突
- 以太网的端到端往返时延 2τ 称为争用期，或冲突窗口
- 经过争用期这段时间还没有检测到冲突，才能肯定这次发送不会发生冲突

截断二进制指数退避算法

- 发生冲突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，减小再次发生冲突的概率

  (1) 基本退避时间，一般是取为争用期 2τ

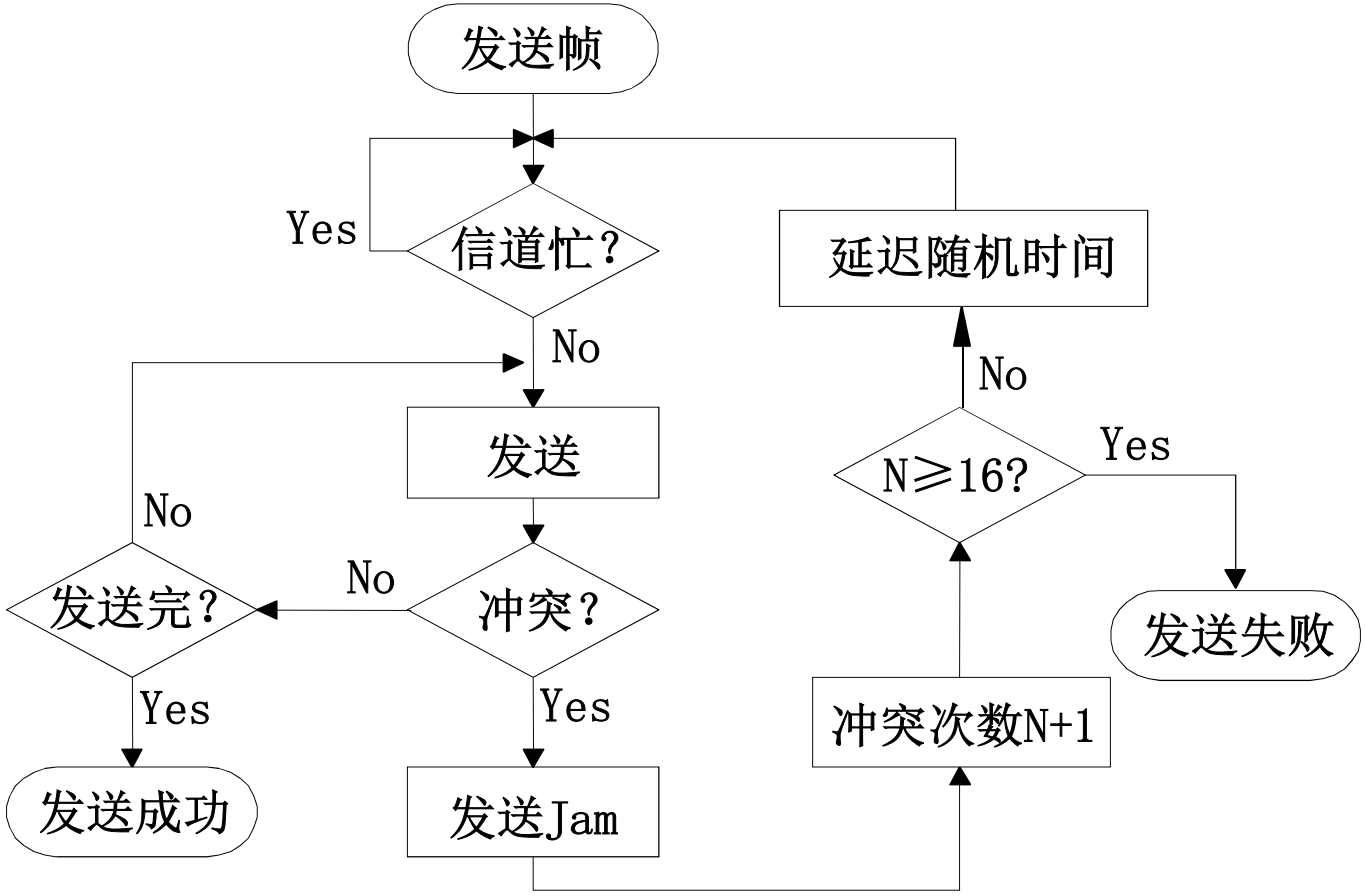
  (2) 从整数集合[0,1,…, (2^k-1)]中随机地取出一个数，记为 r。重传所需的时延就是 r 倍的基本退避时间，定义重传次数 k，$k \le 10$，即k = Min[重传次数, 10]

  (3) 重传 16 次仍不能成功时丢弃该帧，向高层报告。

CSMA/CD 协议：最短帧长

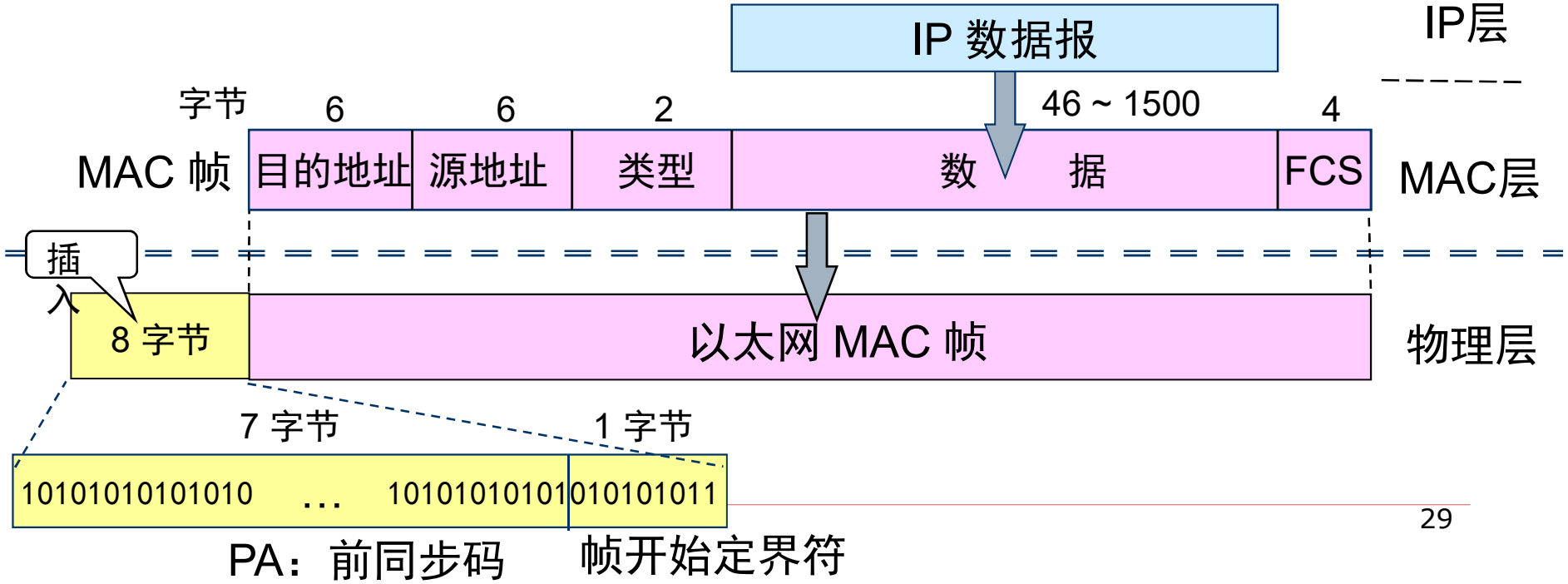
- **64字节**
  - 以太网取 51.2 μs 为基本退避时间（争用期）
  - 对于 传统以太网（10 Mbps），在争用期内可发送512 bit，即 64 字节
  - 如果发生冲突，一定是在发送的前 64 字节之内
  - 由于一检测到冲突就立即中止发送，已经发送的数据一定小于 64 字节
  - 因此以太网规定最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧

CSMA/CD操作的流程图



以太网的 MAC子 层

- **MAC 帧的格式**
  - ✓ 常用的以太网**MAC**帧格式有两种标准：
    - **DIX Ethernet V2 标准（更常用）**
    - **IEEE 的 802.3 标准**



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
- 对于检查出的无效 MAC 帧就丢弃。以太网不负责重传丢弃的帧

以太网的 MAC 层：帧间最小间隔

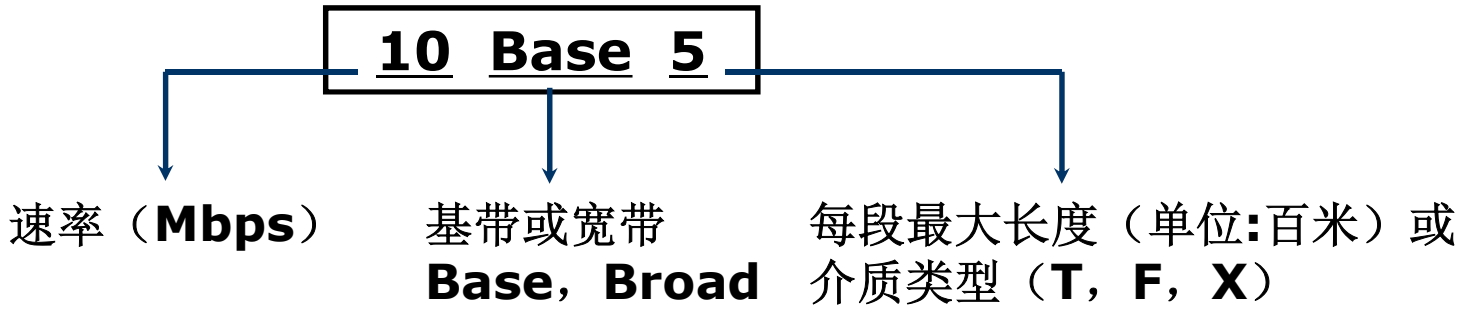
- 帧间最小间隔为 9.6 μs，相当于 96 bit 的发送时间
- 一个站在检测到总线开始空闲后，还要等待 9.6 μs 才能再次发送数据
- 目的：使其他站点（尤其是刚发送的站点和刚接收的站点）做好接收帧的准备

主要的IEEE 802.3 以太网标准（主要的）

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

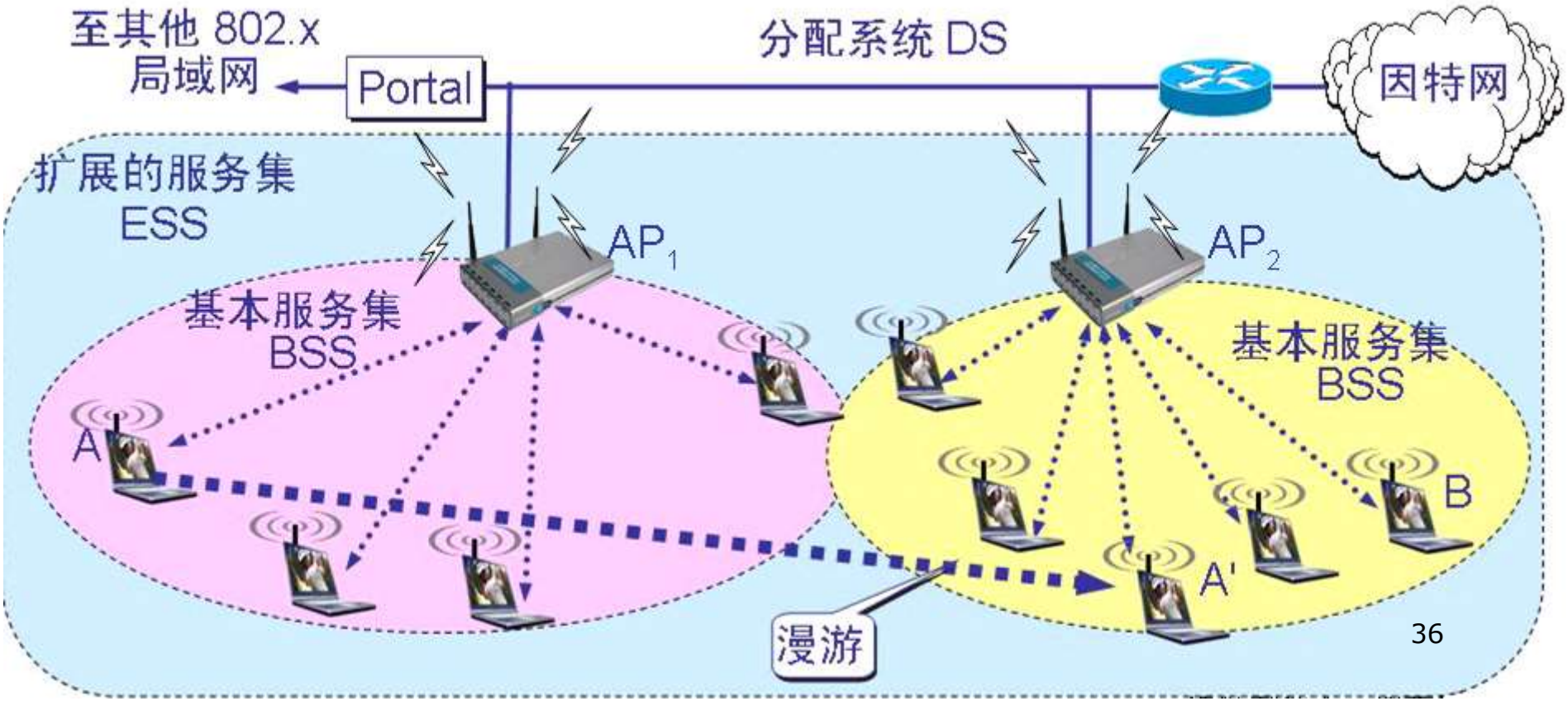
无线网络

- 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
  - 无线网络可以很好地解决以上问题，利用电磁波在空中发送和接收数据，是对有线网络的一种补充和扩展。

无线局域网(WLAN)的组成

1. 有固定基础设施的WLAN

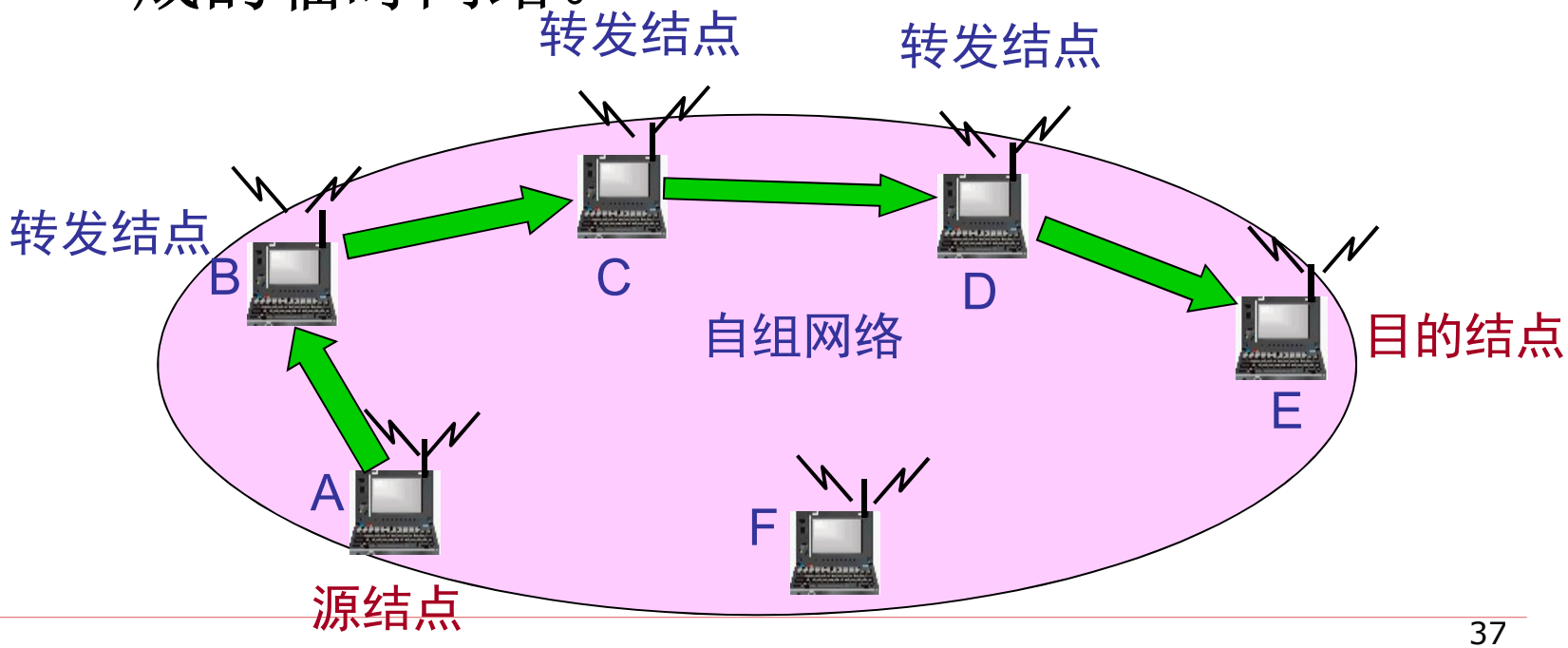
- 预先建立起来的、能够覆盖一定范围的一批固定基站



无线局域网的组成

2. 移动自组织网络(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。

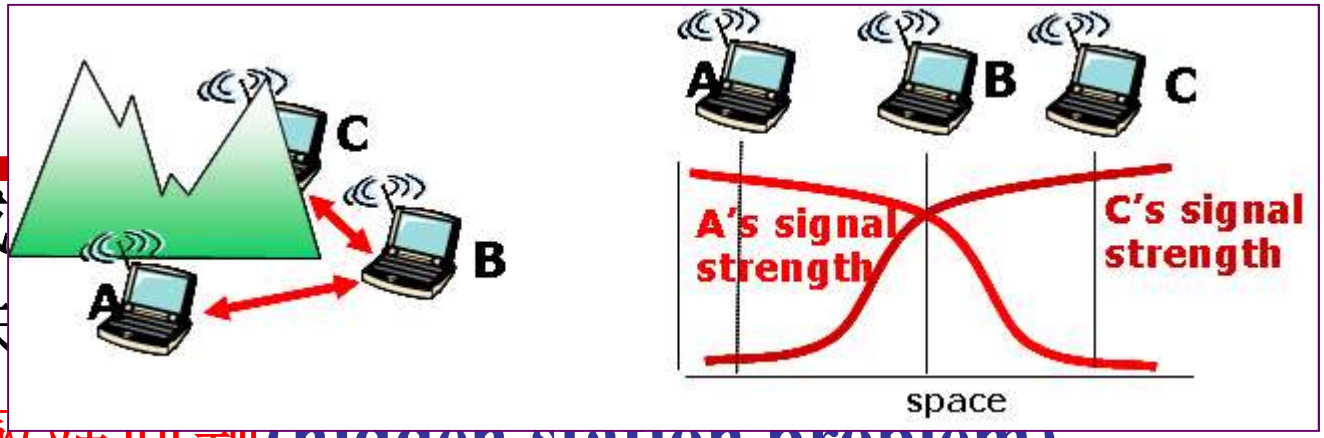


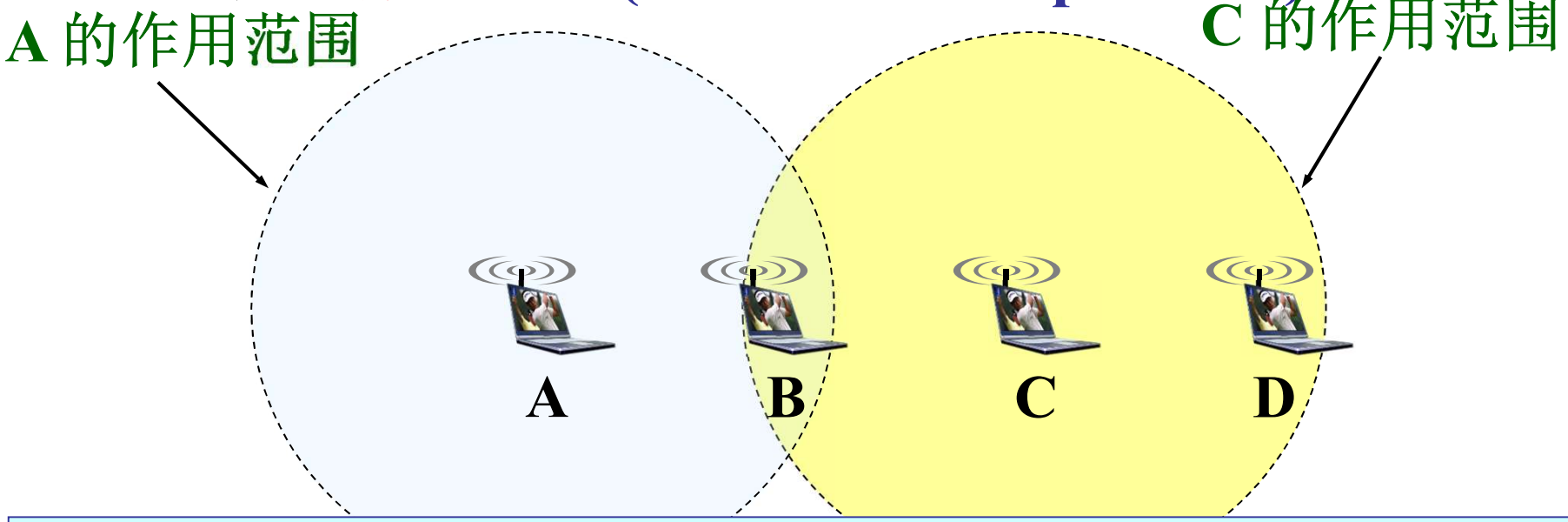
802.11 WLAN的MAC 子层协议

- 与802.3协议的MAC非常相似，都在共享媒体上支持多个用户共享资源，由发送者在发送数据前先进行网络的可用性检测。但照搬 CSMA/CD
  - 在无线局域网的适配器上，接收信号的强度往往会远小于发送信号的强度，因此若要实现冲突检测，在硬件上需要的花费就会过大
  - 在无线局域网中，并非所有的站点都能听见对方，而所有站点都能听见对方是实现CSMA/CD协议必须的基础

隐蔽站

- 无线局域
  - 这种未
  - 叫做隐蔽站问题(hidden station problem)

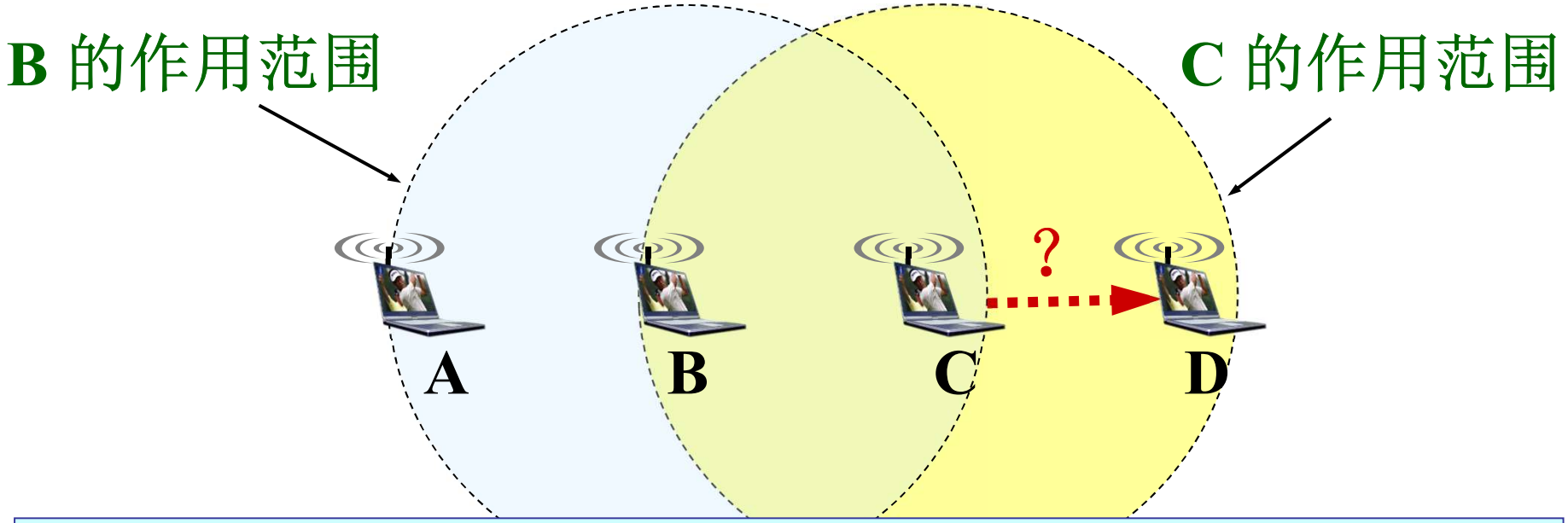




- 当 A 和 C 检测不到无线信号时，都以为 B 是空闲的，因而都向 B 发送数据，结果发生冲突。

暴露站问题

➢其实 B 向 A 发送数据并不影响 C 向 D 发送数据，这就是暴露站问题(exposed station problem)



➢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。

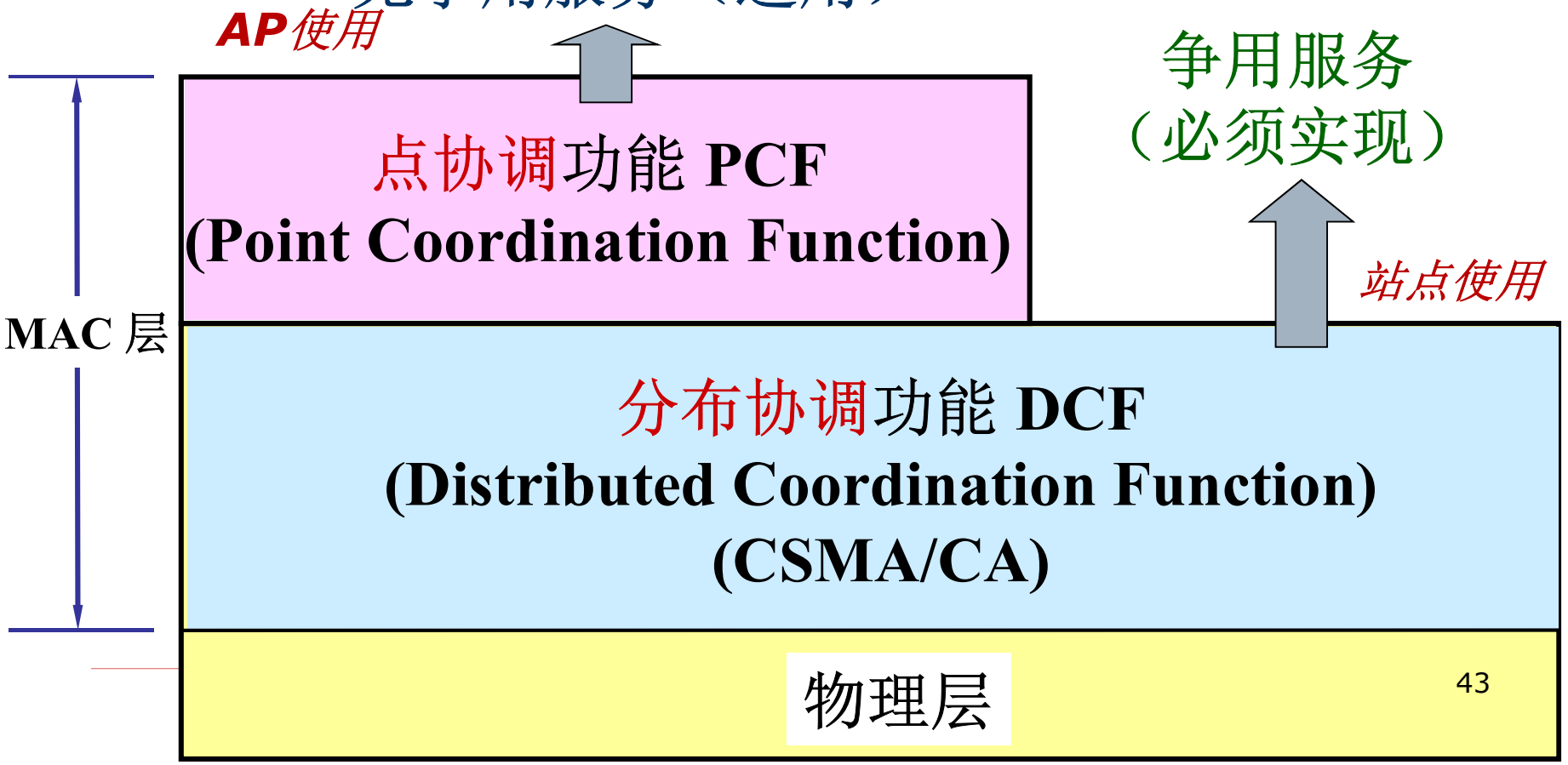
802.11 WLAN的MAC 层协议

- 无线局域网不能使用 CSMA/CD，而只能使用改进的 CSMA 协议。
- 改进的办法是把 CSMA 增加一个冲突避免(Collision Avoidance)功能，尽量减少冲突的概率。
  - 不是在发送过程中去监听是否发生了冲突，而是发送前设法避免冲突的发生
  - “冲突避免”采用了三种机制来实现：预约信道、正向确认和RTS/CTS

- 预约信道
  - 发送站点向所有其他无线站点通告本站点将要占用信道多长时间，让其它站在这段时间内不要发送数据，避免冲突
- 正向确认
  - 接收站点正确收到数据帧时，就向发送站点发送一个ACK帧作为接收成功的肯定回答，否则将不采取任何动作。发送站点根据是否收到ACK帧决定重发与否。
  - 用于冲突的恢复。
- **RTS/CTS**
  - 通过RTS/CTS帧预约信道，以避免隐蔽站冲突问题。

PCF与DCF

➢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。



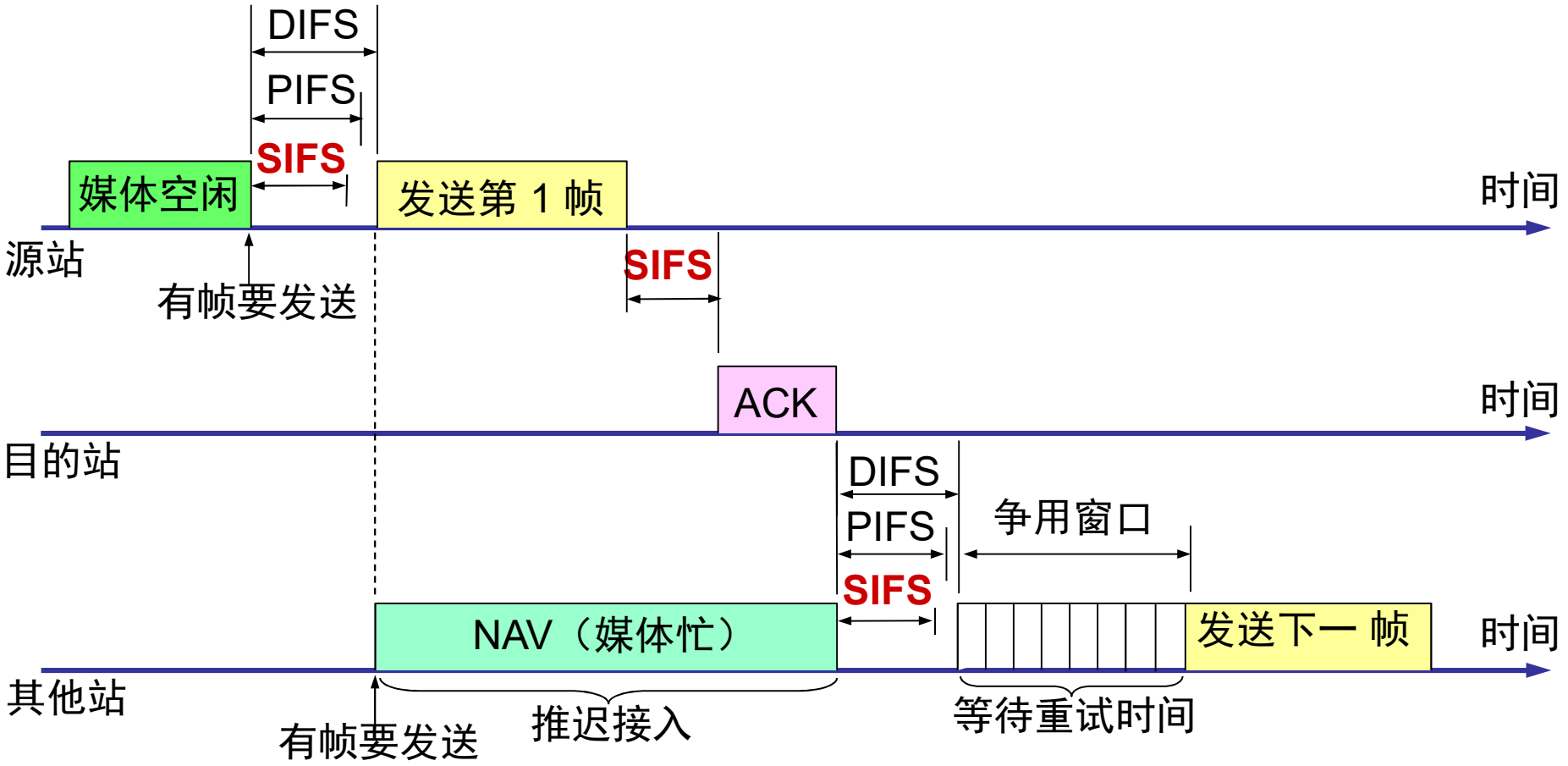
帧间间隔 IFS (InterFrame Space)

- 为了尽量避免冲突，所有的站在完成发送后，必须再等待一段很短的时间(继续监听)才能发送下一帧→ 帧间间隔 IFS 。
- 帧间间隔长度取决于该站欲发送的帧的类型

高优先级帧需要等待的时间较短，因此可优先获得发送权。

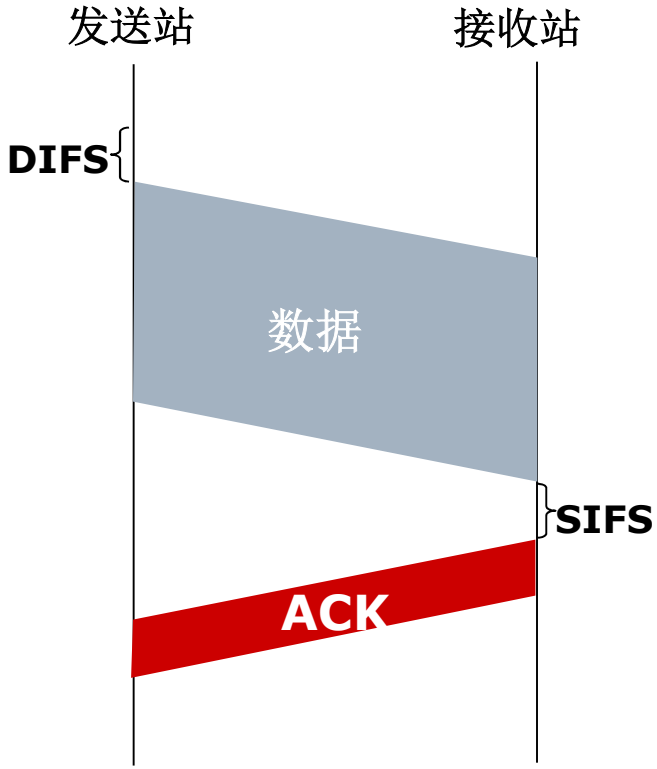
- 若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态因而低优先级帧就只能再推迟发送，因此减少冲突

三种帧间隔


DIFS
PIFS
SIFS
媒体空闲
发送第 1 帧
时间
源站
有帧要发送
SIFS
ACK
时间
目的站
DIFS
PIFS
争用窗口
SIFS
NAV（媒体忙）
发送下一 帧
时间
其他站
有帧要发送
推迟接入
等待重试时间

CAMA/CA协议

- *发送站点*
  - 如果监听到信道空闲时间达到DIFS，则发送数据帧
  - 如果信道忙，则开始退避，退避时间到时发送数据帧
  - 如果ACK超时，则增加退避时间
- *接收站点*
  - 如果收到数据帧，则在SIFS时间段之后发送ACK
- *其他站点*
  - 设置网络分配向量NAV



为什么信道空闲还要再等待？

- 可能有其他的站有高优先级的帧要发送。
- 如有，就要让高优先级帧先发送。

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

虚拟载波监听

- 目的：减少冲突，
- 让源站将它要占用信道的时间(包括目的站发回确认帧所需的时间)通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据
- 源站在其 MAC 帧首部中的第二个字段“持续时间”中填入了在本帧结束后还要占用信道多少时间(以微秒为单位)
- “虚拟载波监听”是表示其他站并没有监听信道，而是由于其他站收到了“源站的通知”才不发送数据。

NAV

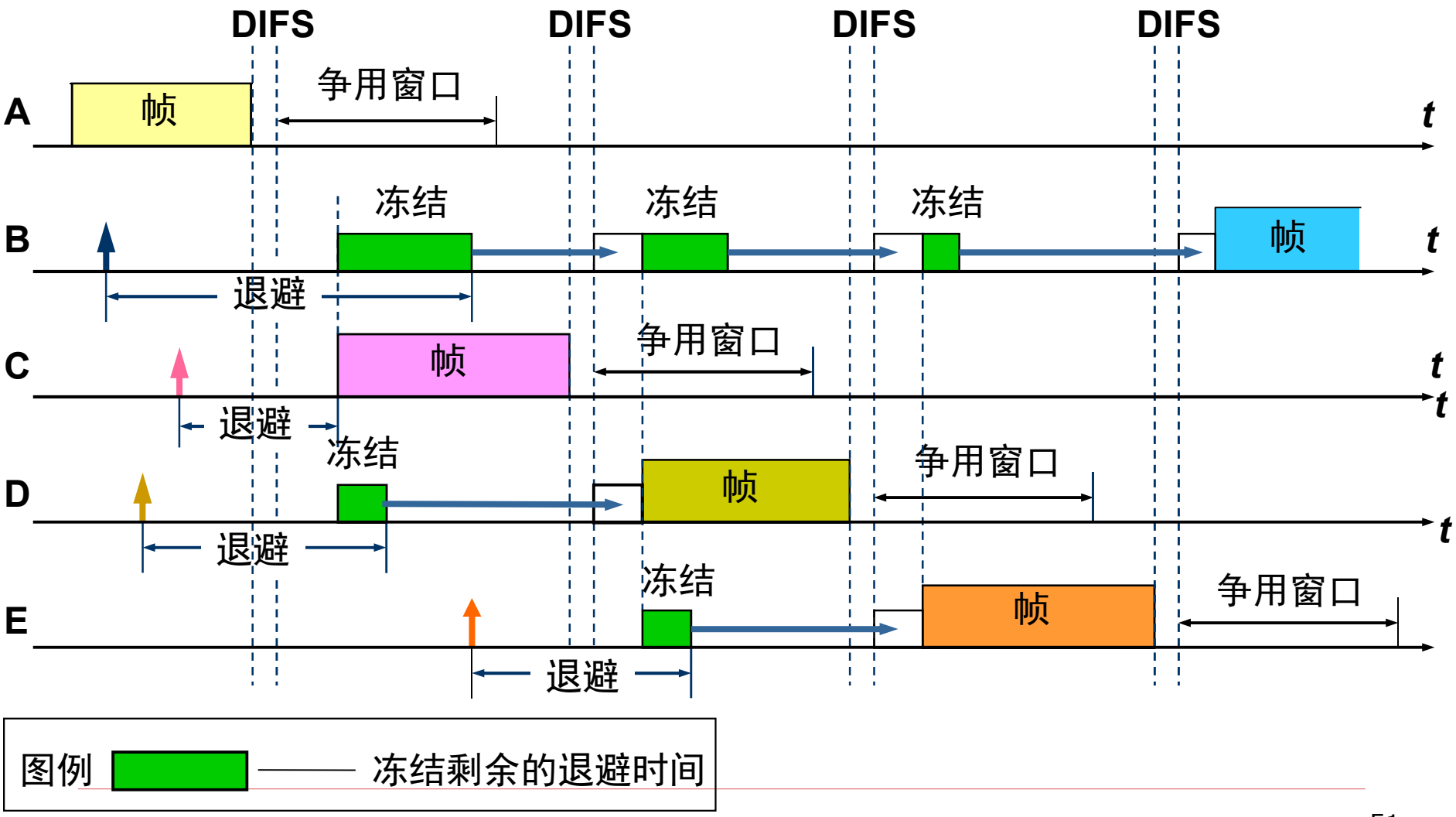
- 网络分配向量NAV (Network Allocation Vector)
  - 当一个站检测到正在信道中传送的MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 。
  - NAV 指出了必须经过多少时间才能完成数据帧的这次传输，才能使信道转入到空闲状态。

争用窗口与退避

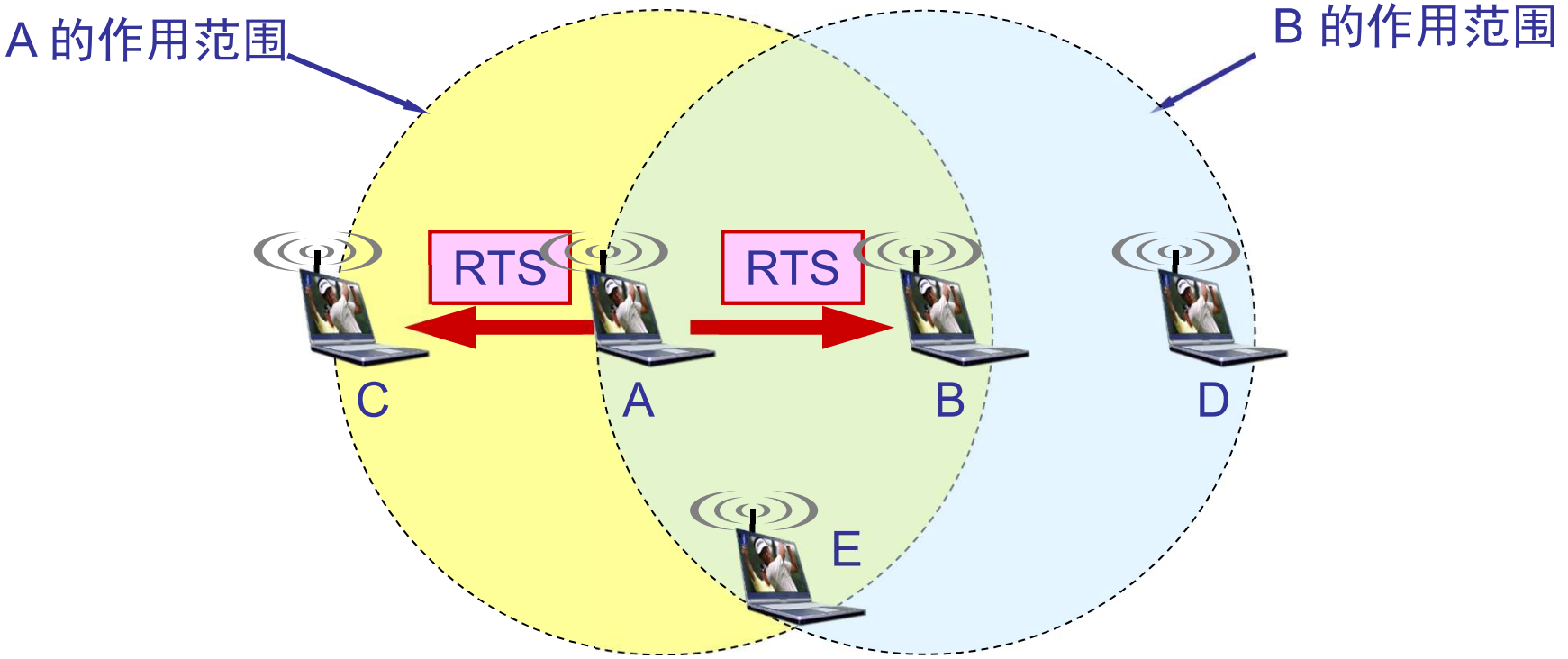
争用窗口

- 信道从忙态变为空闲时，任何一个站要发送数据帧时，不仅都必须等待一个 DIFS 的间隔，而且还要进入争用窗口，并计算随机退避时间以便再次重新试图接入到信道
- 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
- 802.11 使用二进制指数退避算法 （略）
  - 扩展退避的时间范围，使得不同站点选择相同退避时间的概率减少

802.11WLAN的退避机制

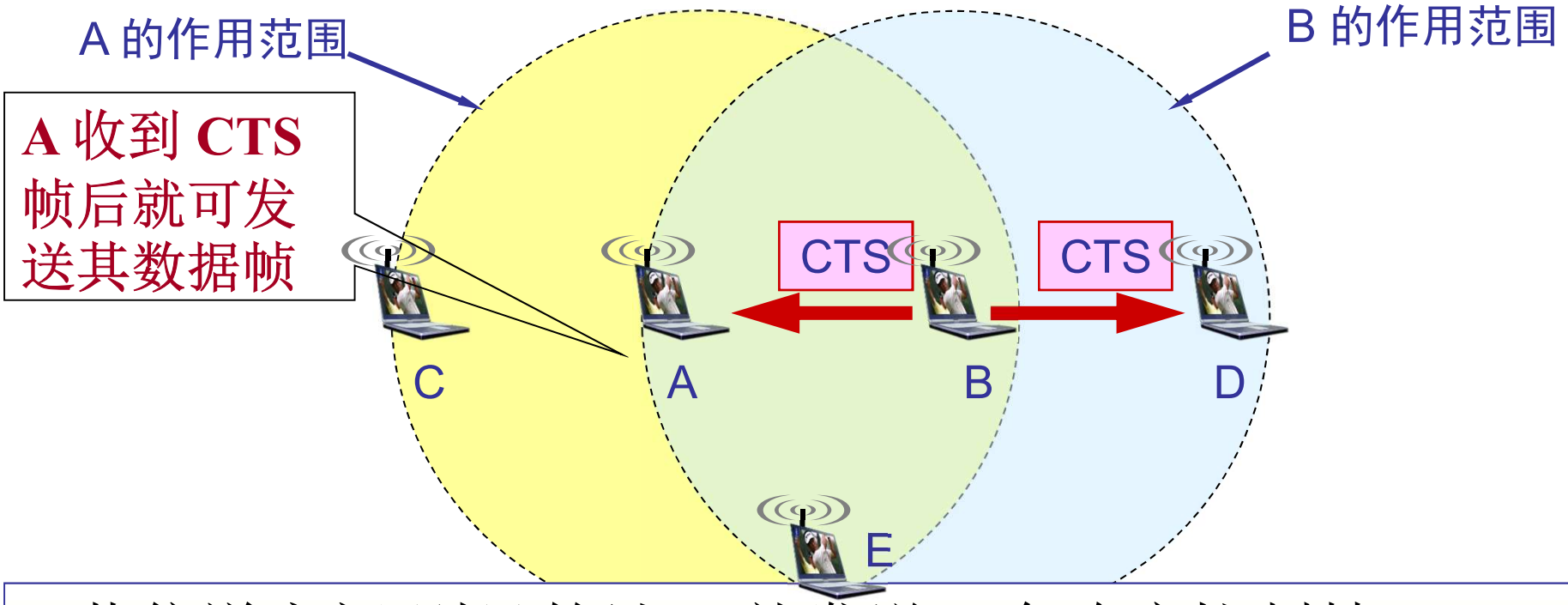


802.11 WLAN的信道预约机制



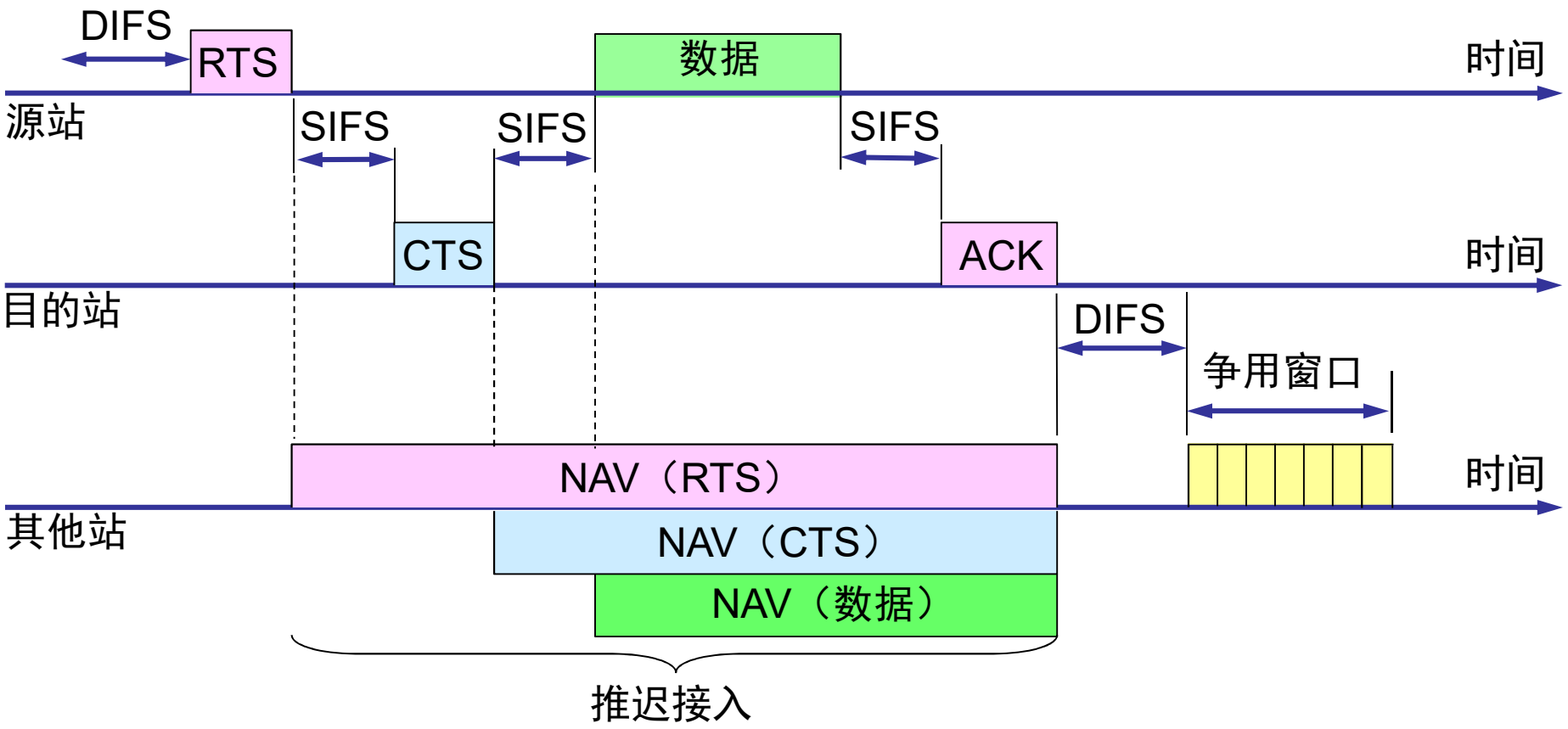
➢源站 A 在发送数据帧之前先发送一个短控制帧 RTS (Request To Send)，它包括源地址、目的地址和这次通信(包括相应的确认帧)所需的持续时间

预约机制

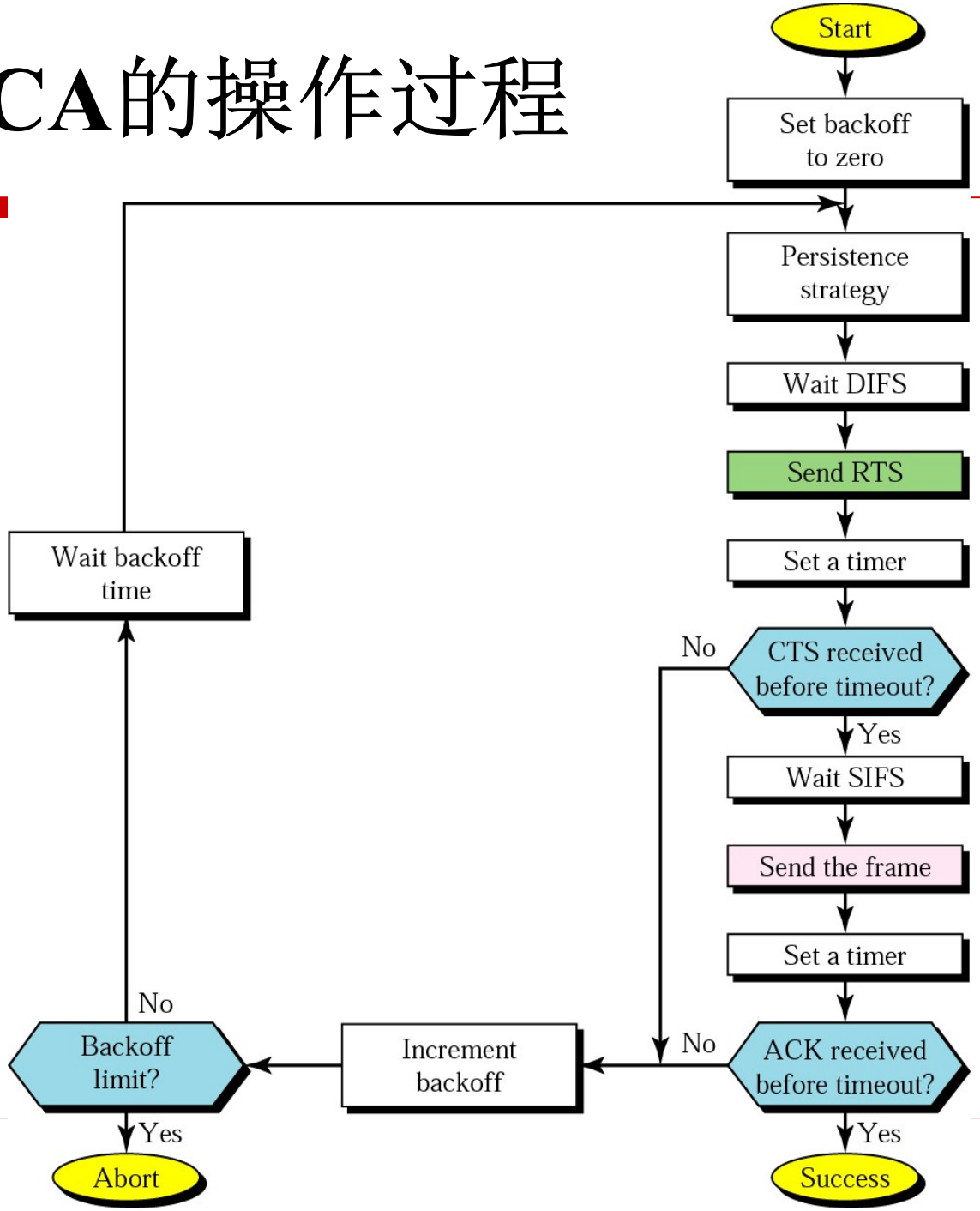


➢若信道空闲,则目的站 B 就发送一个响应控制帧 CTS (Clear To Send)，包括这次通信所需的持续时间(从 RTS 帧中将此持续时间复制到 CTS 帧中)。

RTS/CTS与NAV


DIFS
RTS
数据
时间
源站
SIFS
SIFS
SIFS
CTS
ACK
时间
目的站
DIFS
争用窗口
NAV（RTS）
时间
其他站
NAV（CTS）
NAV（数据）
推迟接入

CSMA/CA的操作过程



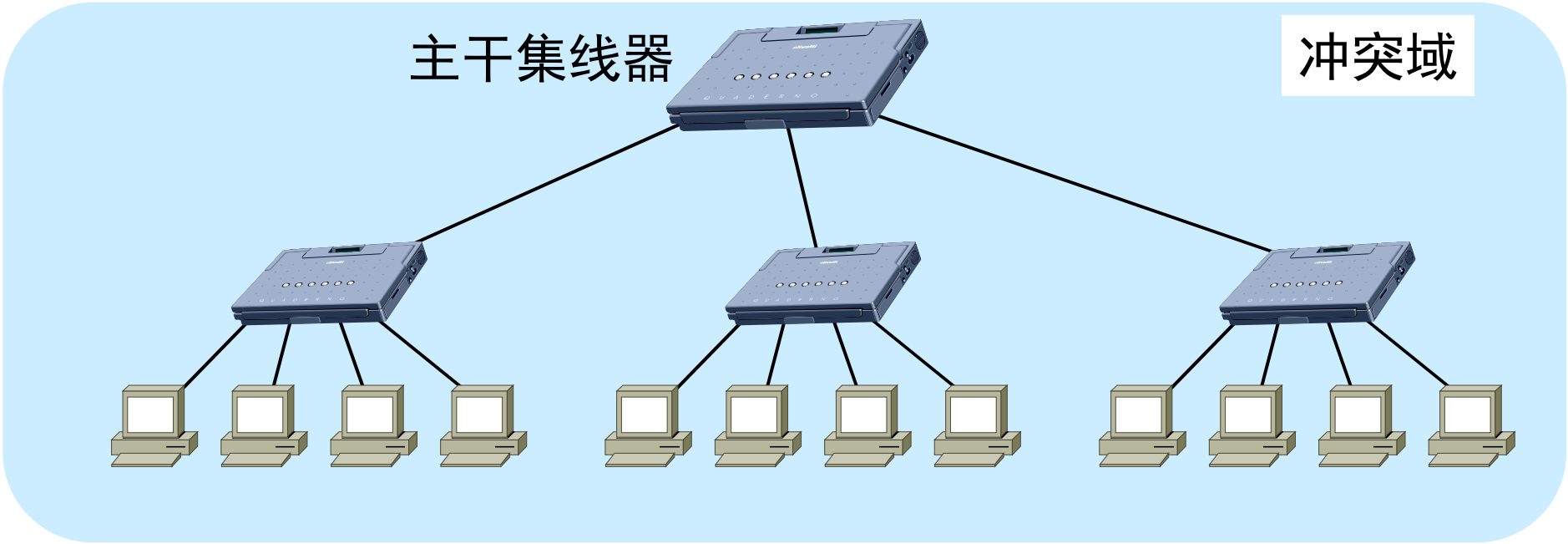
主要内容

- 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

在物理层扩展以太网

- 扩展以太网的地理覆盖范围
- 设备：中继器、集线器（HUB）
- 特点：复制信号，再生放大；

  一个冲突域（共享以太网）

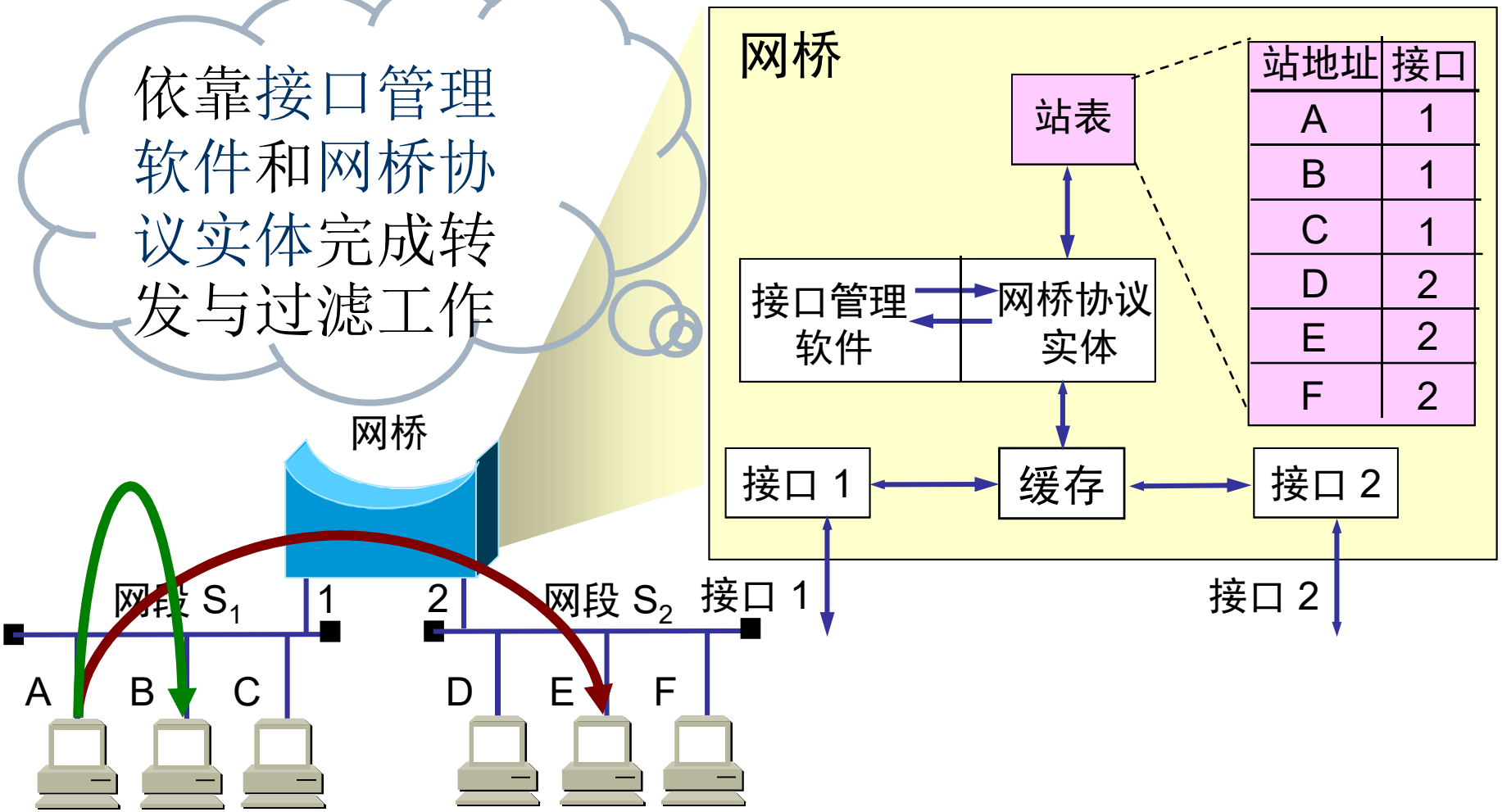


在数据链路层扩展局域网：网桥

- 网桥(bridge)根据 MAC 帧的目的地址对收到的帧进行转发
- 网桥具有过滤帧的功能：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，然后再根据站表确定将该帧转发到哪一个接口，或者把它过滤

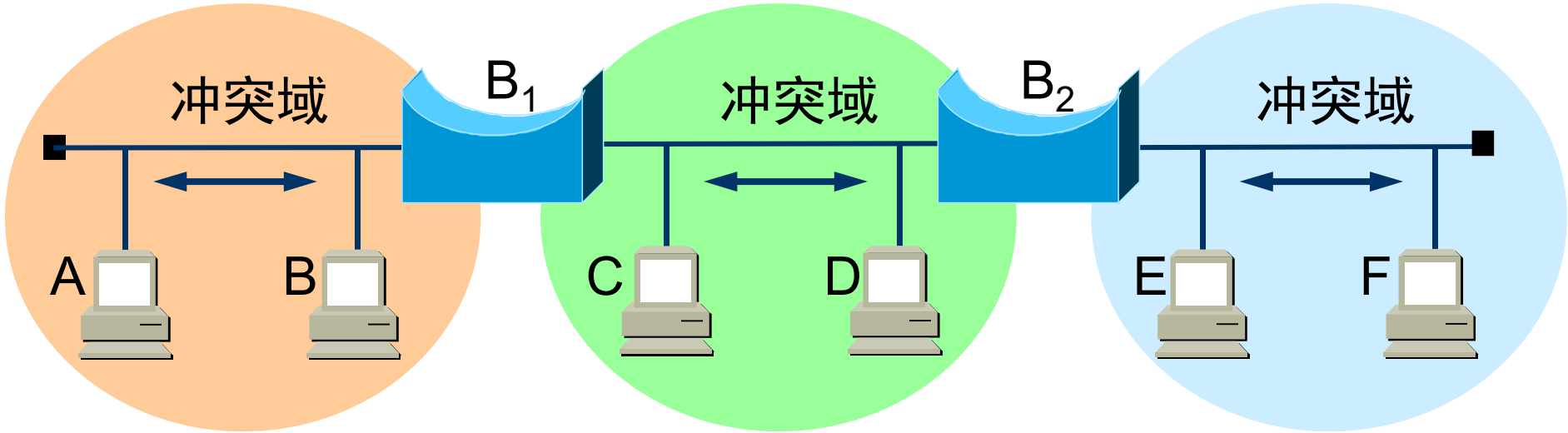
网桥的内部结构

依靠接口管理软件和网桥协议实体完成转发与过滤工作



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
- 可互连不同物理层、不同 MAC 子层和不同速率(10 Mbps ,100 Mbps)的局域网。



网桥的缺点

- 要先存储和查找站表（转发表），转发前必须执行CSMA/CD算法，增加了时延
- 在MAC 子层并没有流量控制功能，当负荷重时，缓存不足会产生帧丢失
- 对于目的地址为全1的广播帧，网桥将进行洪泛转发，会因传播过多的广播信息而产生网络拥塞→ 广播风暴

常用的网桥：透明王琦

- 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
- 即插即用设备，其标准是 IEEE 802.1D
  - 自动配置：只要 把网桥接入网络即可，不需人工配置转发表

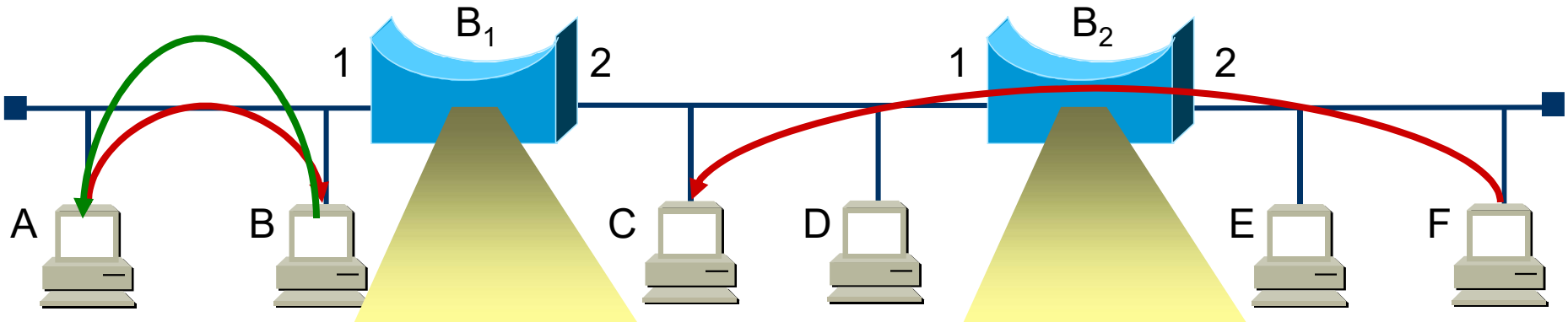
建立转发表：逆向学习

- 自学习算法

  若从 A 发出的帧从接口 x 进入了某网桥，那么从这个接口出发沿相反方向一定可把一个帧传送到 A

- ✓ 每收到一个帧，就记下其源地址和进入网桥的接口，作为转发表中的一项
- ✓ 在建立转发表时是把帧首部中的源地址写在“地址”这一栏的下面
- ✓ 在转发帧时，根据收到的帧首部中的目的地址来转发的。这时把在“地址”栏下面已经记下的源地址当作目的地址，而把记下的进入接口当作转发接口。

转发表的建立过程示例



A → B
F → C
B → A

地址	接口
A	1
F	2
B	1
…	…

A → B
F → C

地址	接口
A	1
F	2
…	…

网桥的工作过程

- 网桥收到一帧后，先进行自学习，查找转发表中与收到帧的源地址有无匹配项
  - 如没有，就在转发表中增加一个项目（源地址、进入的接口和时间）
  - 如有，则把原有的项目进行更新
- 然后转发帧：查找转发表中与收到帧的目的地址有无匹配项
  - 如没有，则洪泛转发，即转发到所有其他接口
  - 如有，则转发到表中的对应接口
  - 若转发表中的接口就是该帧进入网桥的接口，则丢弃这个帧

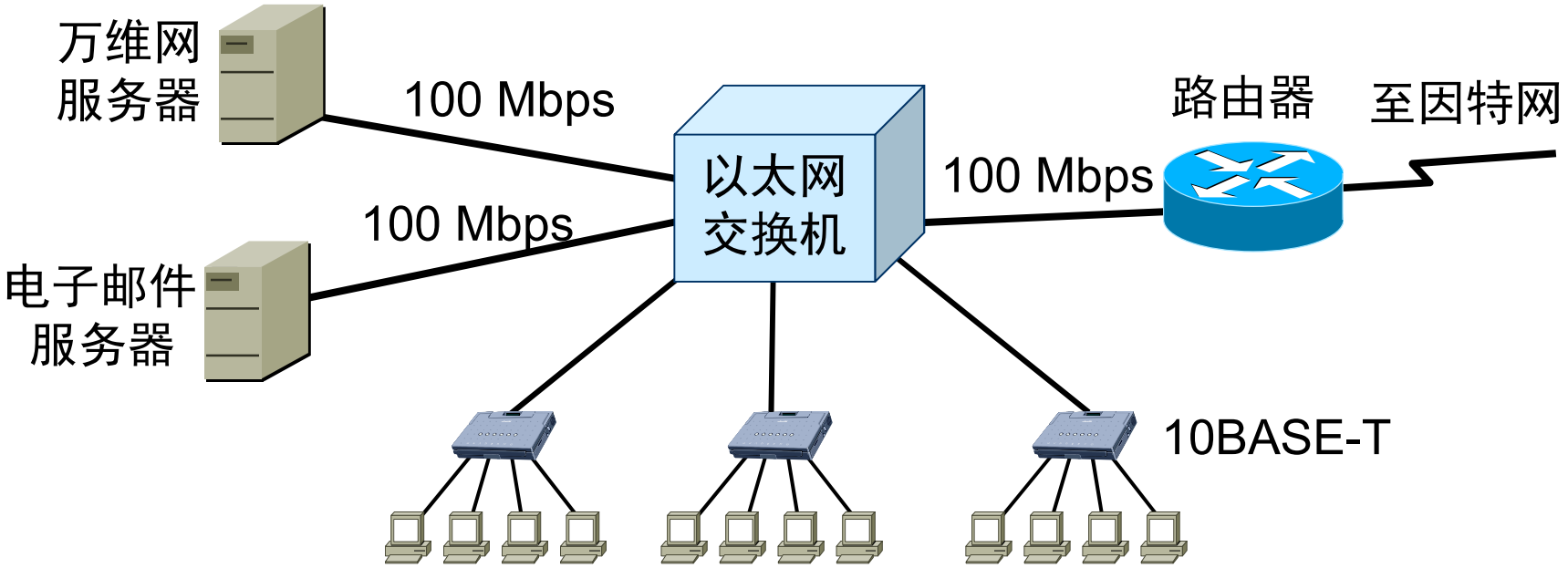
多接口网桥：以太网交换机

- 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，实质上多接口的网桥
- 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
- 主机需要通信时，交换机能同时连通多对接口，使每一对相互通信的主机都能像独占通信媒体那样，无冲突地传输数据
- 对于拥有 N 对接口的交换机的总容量为 N×10 Mbps
- 即插即用设备，帧转发表也需要通过自学习算法建立
- 使用了专用的交换结构芯片，交换速率较高

用交换机扩展LAN


万维网
服务器
100 Mbps
以太网
交换机
路由器
至因特网
100 Mbps
100 Mbps
电子邮件
服务器
10BASE-T

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

- 局域网的体系结构：物理层和数据链路层(及两个子层)
- 局域网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
- 局域网的扩展：在不同层次上实现的优缺点？网桥、逆向学习及转发
- 无线局域网：CSMA/CA、隐蔽站/暴露站

作业：6-7，6-10+补充题

下图中，网桥B1和B2均为透明网桥，其初始转发表均为空；主机按照下列次序发送数据。请填写出每一步，B1、B2对帧的处理（转发、丢弃等），并画出B1和B2的最终转发表（站点地址、LAN号）。

1) A发一帧给C
2) E发一帧给A
3) D发一帧给E
4) C发一帧给A
5) B发一帧给C