



北京邮电大学

计算机网络

第六章 局域网 LAN

网络空间安全学院

主要内容

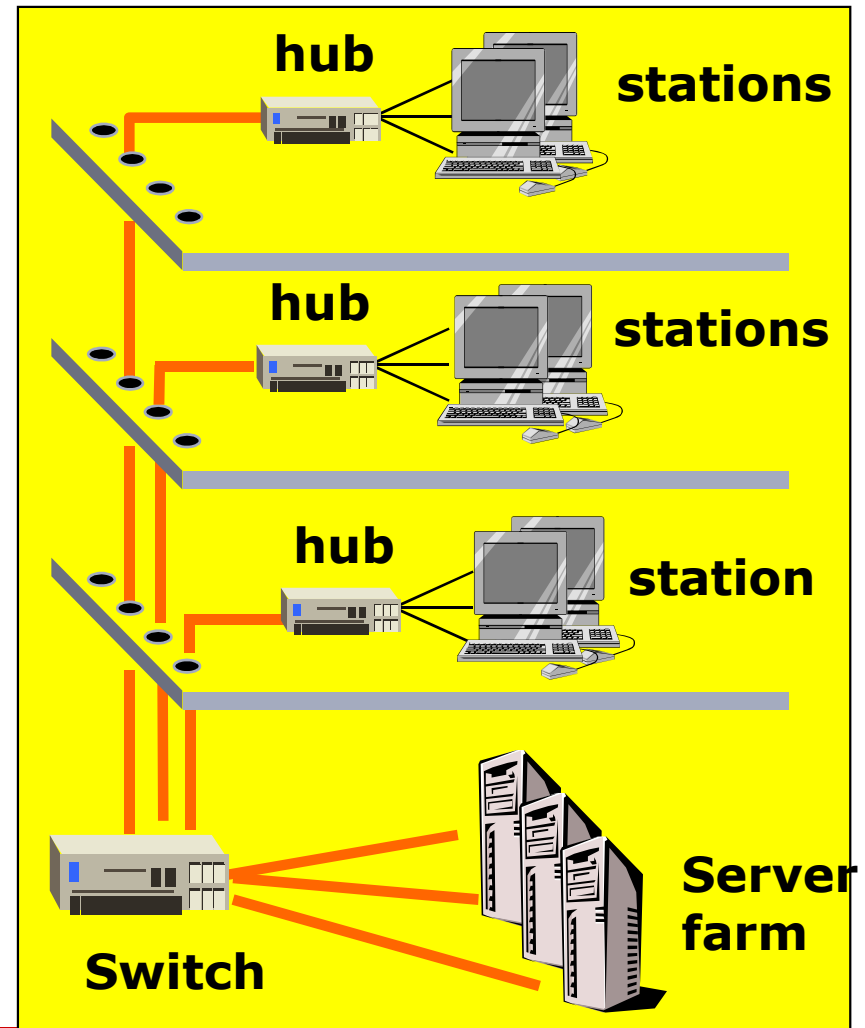
- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

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

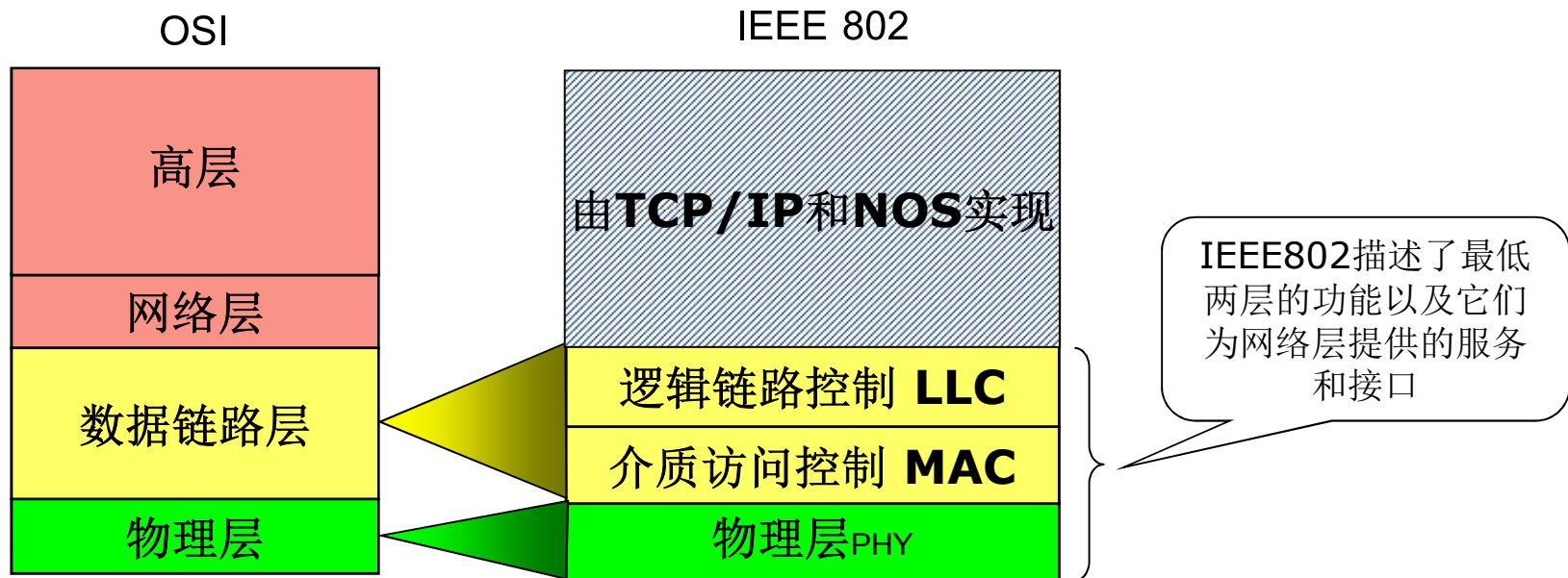
局域网（LAN）概述

- 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~1000Mb/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



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



局域网的物理层

□ 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。

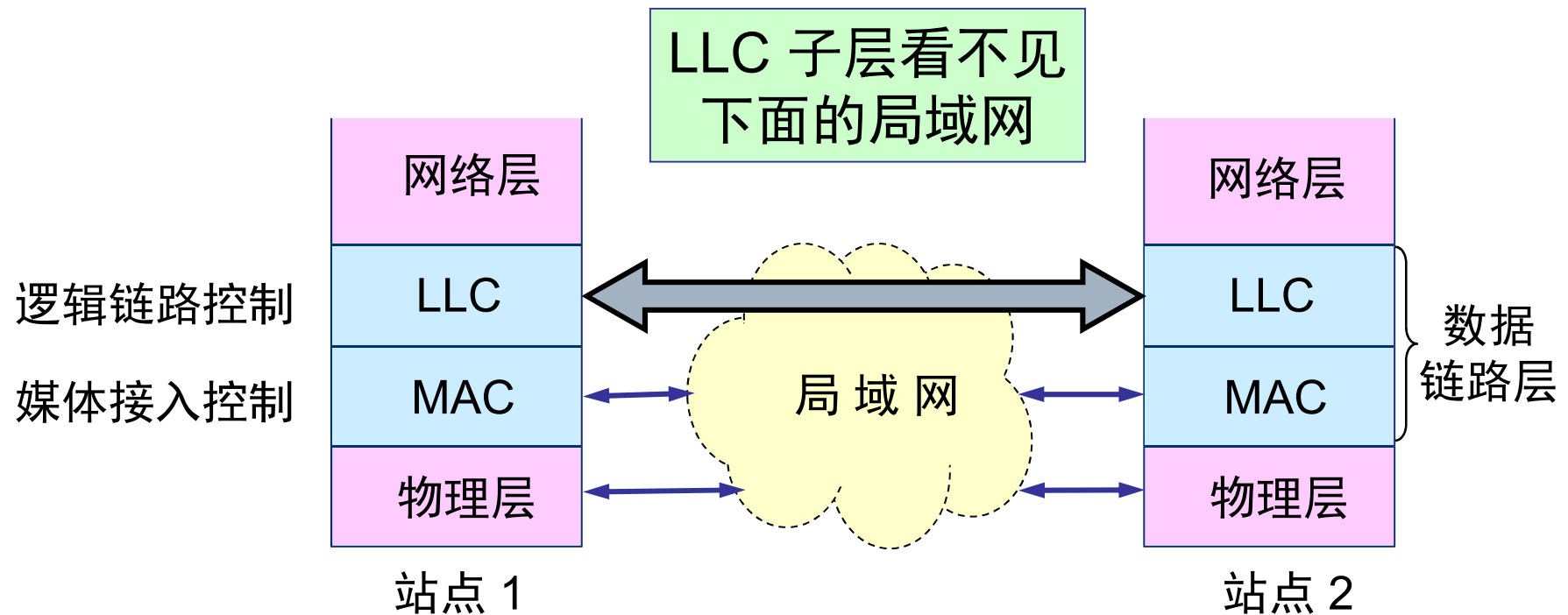
□ IEEE802定义了多种物理层，以适应不同的网络介质和不同的介质访问控制方法。

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。
-

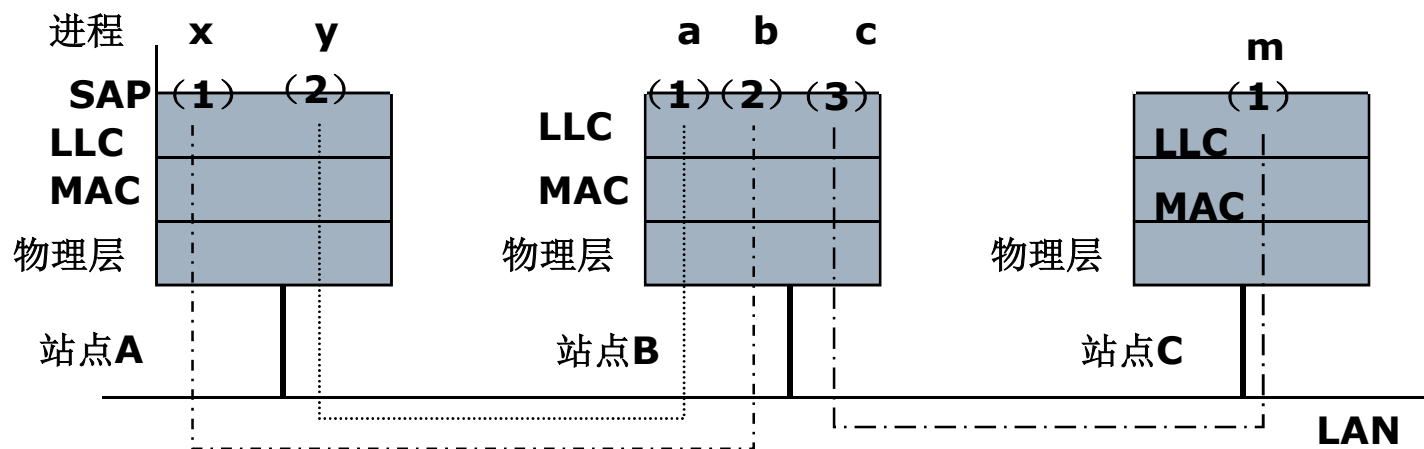
局域网的数据链路层

➤ 局域网对 LLC 子层是透明的



LLC子层的功能

➤ LLC SAP



一个主机中可能有多个进程在运行，它们可能同时与其它的一些进程进行通信。因此，在一个主机的LLC子层上设有多个服务访问点，以便向多个进程提供服务。

✱ 两种地址：A(1) B(2) C(1)

①MAC地址，DTE在网络中的物理地址（站地址），在MAC帧中传送

②SAP地址，进程在DTE中的逻辑地址，在LLC帧中传送

LLC子层的功能

□ LAN中的寻址分成两步：

- ① 根据MAC地址找到目的站点
- ② 根据SAP地址找到该DTE中的相应进程

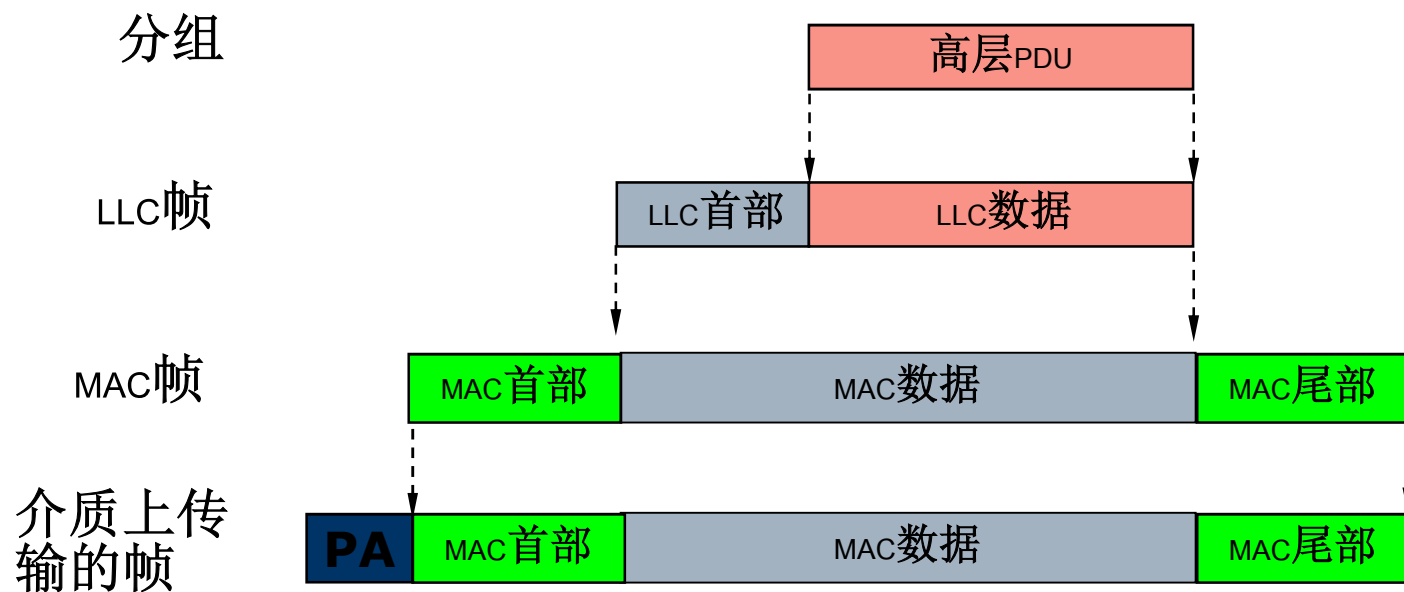
□ LLC子层功能：向高层提供统一的链路访问形式，组帧/拆帧、建立/释放逻辑连接，差错控制，帧序号处理，提供某些网络层功能。

- 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的帧结构



IEEE802 LAN的封装过程：



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	CRC
-------	---------	---------	-----	-----

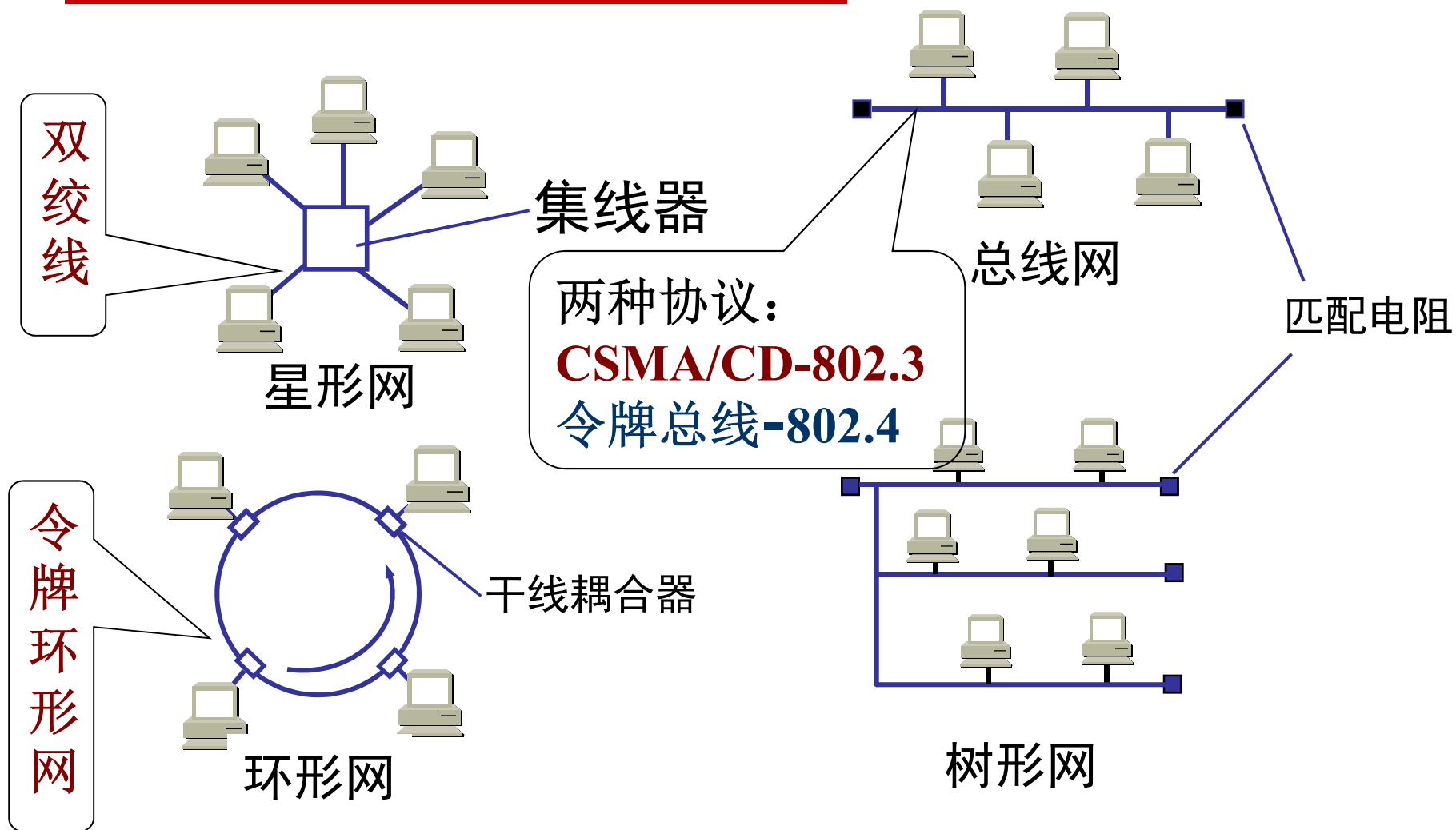
介质访问控制方法

- 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。问题：
 - 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）？
 - 解决以上问题的方法称为介质访问控制方法。
 - 两类介质共享技术：
 - 静态分配（**FDM、WDM、TDM、CDM**）
 - 不适用于局域网
 - 动态分配（随机接入、受控接入）
 - **CSMA/CD、Token-Passing**
-

局域网中的介质访问控制方法

- 常见的有两种：
 - 随机访问控制方式，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**
 - 令牌传递（**Token Passing**）
 - **Token Ring**
 - **Token Bus**
 - **FDDI**
 - 采用受控访问技术的分散控制型介质访问控制方法

局域网的拓扑



主要内容

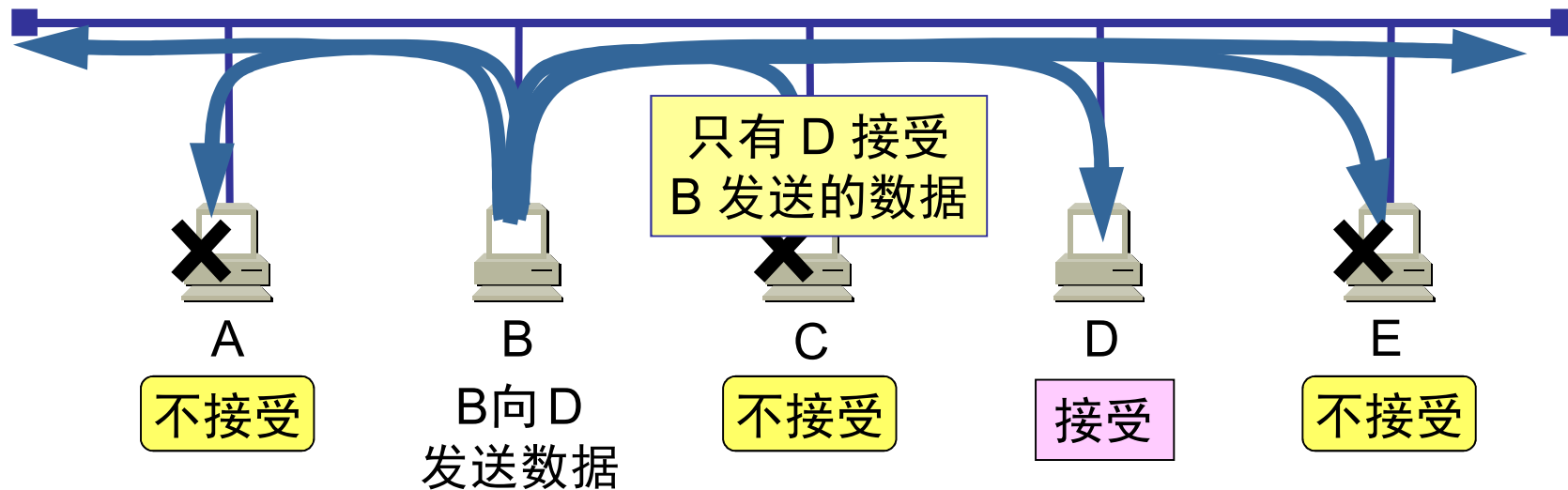
- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

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）
- 1985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
- 目前已发展到万兆以太网，仍在继续发展 …

CSMA/CD 协议

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



CSMA/CD 协议

➤ 以太网的广播方式发送

- ✓ 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** 的地址与数据帧首部写入的地址一致，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，就丢弃这个数据帧不收下来。
- ✓ 具有广播特性的总线上实现了一对一通信。

CSMA/CD协议

- 多个站点如何安全地使用共享信道？
 - 最简单的思路：发送前先检测一下其它站点是否正在发送（即信道忙否）。
 - 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
 - 等到信道空闲后等待随机时间后再发送
 - 等待一段随机时间后再重新检测信道
 - 一旦出现两个站点同时发送的情况，如何处理？
 - 以上方法均无法处理！

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 协议

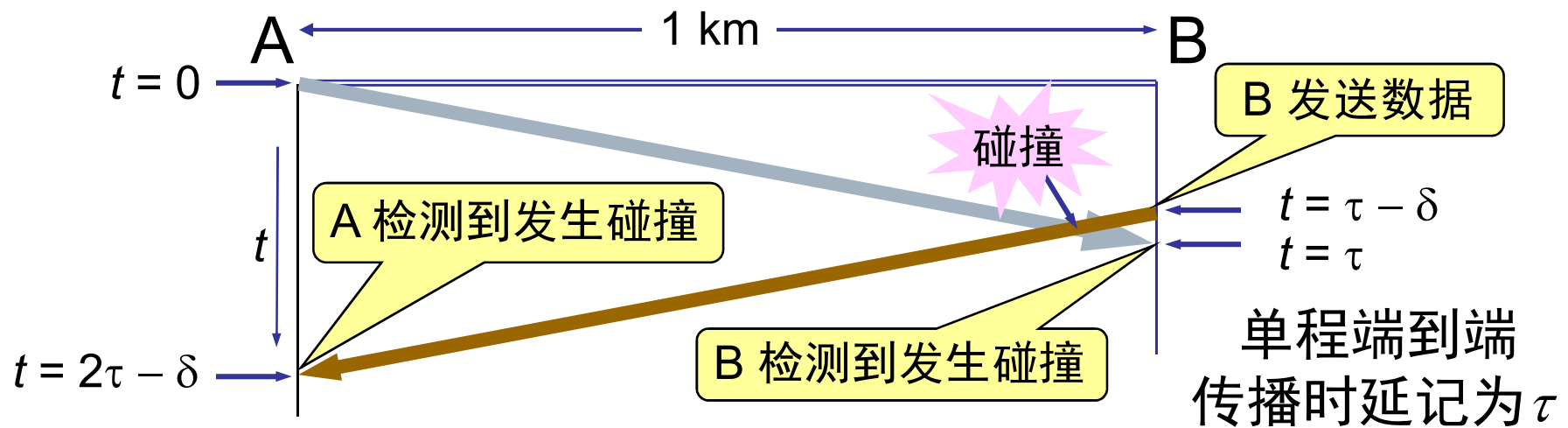
- 载波监听多点接入/碰撞检测 CSMA/CD
 - ✓ “**多点接入**”表示许多计算机以多点接入的方式连接在一根总线上。
 - ✓ “**载波监听**”是指每一个站在发送数据之前先要检测一下总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生碰撞。
 - ✓ “**碰撞检测**”就是计算机边发送数据边检测信道上的信号电压大小。当信号电压摆动值超过一定的门限值时，认为总线上至少有两个站同时在发送数据，产生了碰撞(冲突)。立即停止发送，然后等待一段随机时间后再次发送。

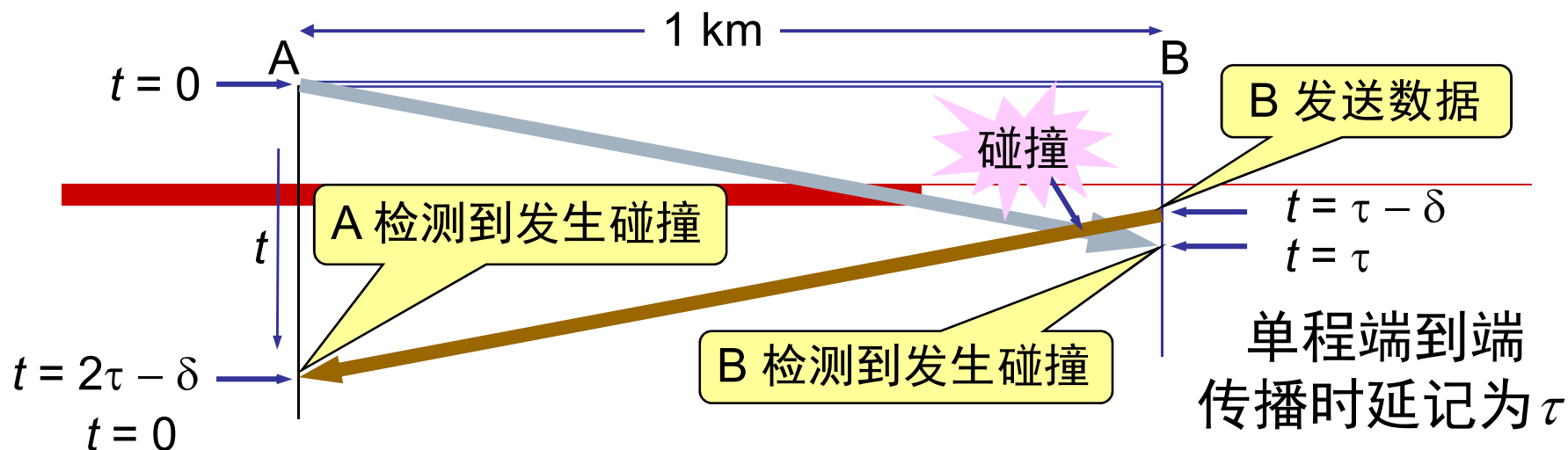
CSMA/CD 协议

- 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 发送的帧发生碰撞。
 - ✓ 碰撞的结果是两个帧都变得无用。

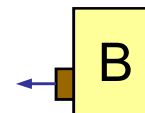
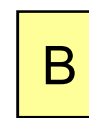
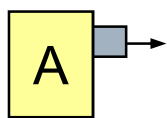
CSMA/CD 协议

➤ 传播时延对载波监听的影响





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

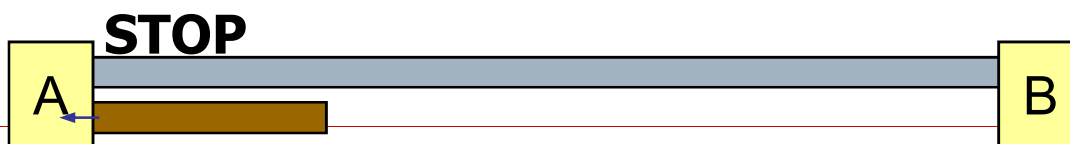


$t = \tau - \delta / 2$
发生碰撞



$t = \tau$
B 检测到发生碰撞
停止发送

$t = 2\tau - \delta$
A 检测到
发生碰撞



CSMA/CD 协议争用期

- 载波监听多点接入/碰撞检测 CSMA/CD
 - ✓ 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。

截断二进制指数退避算法

✓ 截断二进制指数退避算法 (truncated binary exponential backoff)

- ✓ 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，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 $[0, 1, \dots, (2^k - 1)]$ 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 ， $k \leq 10$ ，即 $k = \text{Min}[\text{重传次数}, 10]$
 - (3) 重传 16 次仍不能成功时丢弃该帧，向高层报告。

截断二进制指数退避算法

- ✓ **截断二进制指数退避算法 (truncated binary exponential backoff)**
 - ✓ 以太网取 $51.2\ \mu\text{s}$ 为基本退避时间
 - ✓ 对于 $10\ \text{Mb/s}$ 以太网，在争用期内可发送 $512\ \text{bit}$ ，即 64 字节。
 - ✓ 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。

CSMA/CD 协议

➤ 最短有效帧长为64字节

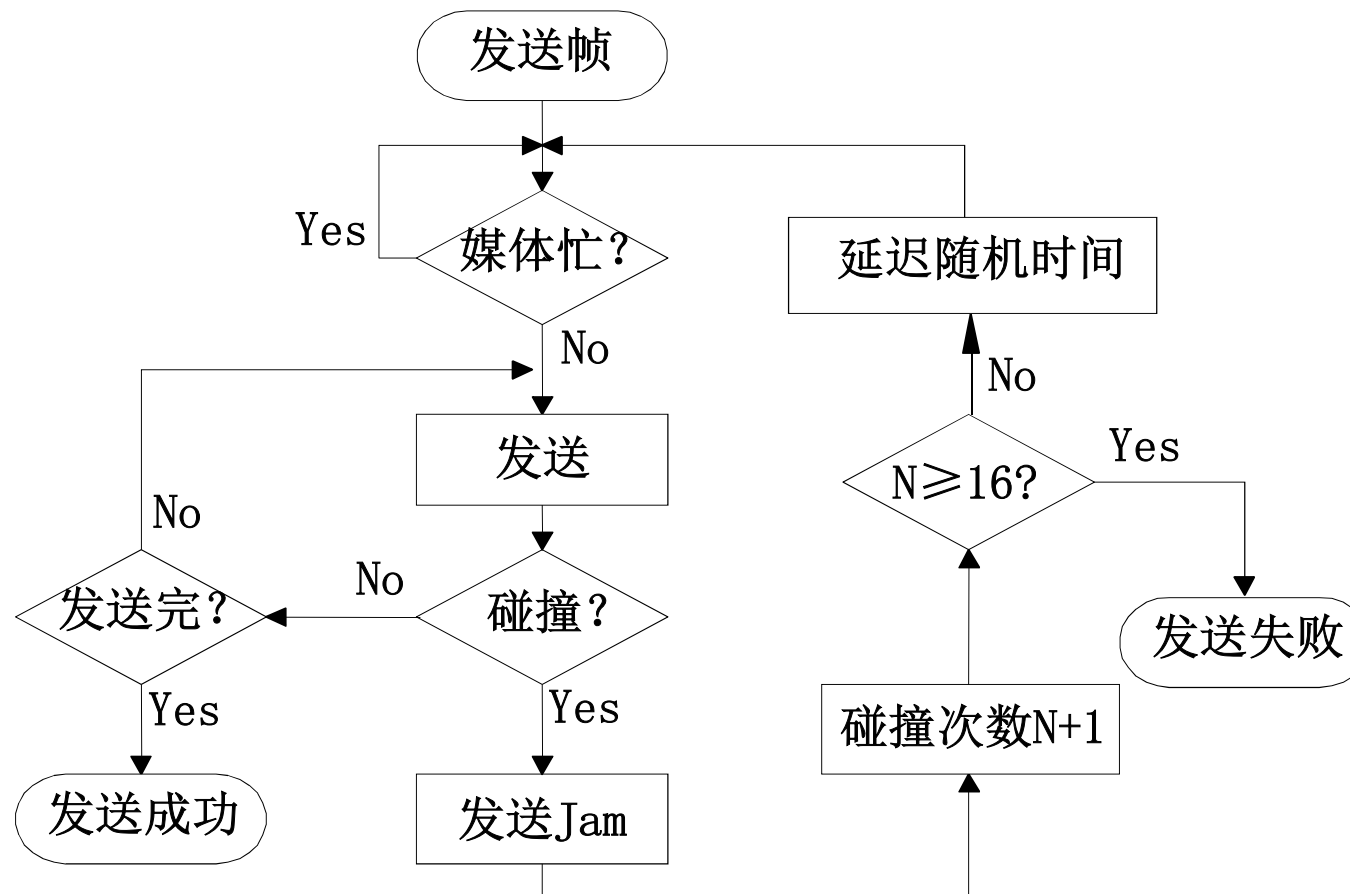
- ✓ 如果发生冲突，就一定是在发送的前64字节之内。
- ✓ 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于64字节。
- ✓ 以太网规定了最短有效帧长为64字节，凡长度小于64字节的帧都是由于冲突而异常中止的无效帧。

CSMA/CD 协议

➤ 载波监听多点接入/碰撞检测 CSMA/CD 协议要点:

- ① 适配器从网络层获得一个分组，加上以太网的首部和尾部，组成帧，放入适配器缓冲区，准备发送。
- ② 若适配器检测到信道空闲，就发送。
- ③ 在发送过程中继续检测信道，若发生碰撞，中止数据发送，并发送人为干扰信号。
- ④ 在中止发送后，执行指数退避算法，等待 r 倍的512比特时间后，返回②。

CSMA/CD操作的流程图



以太网的 MAC 层

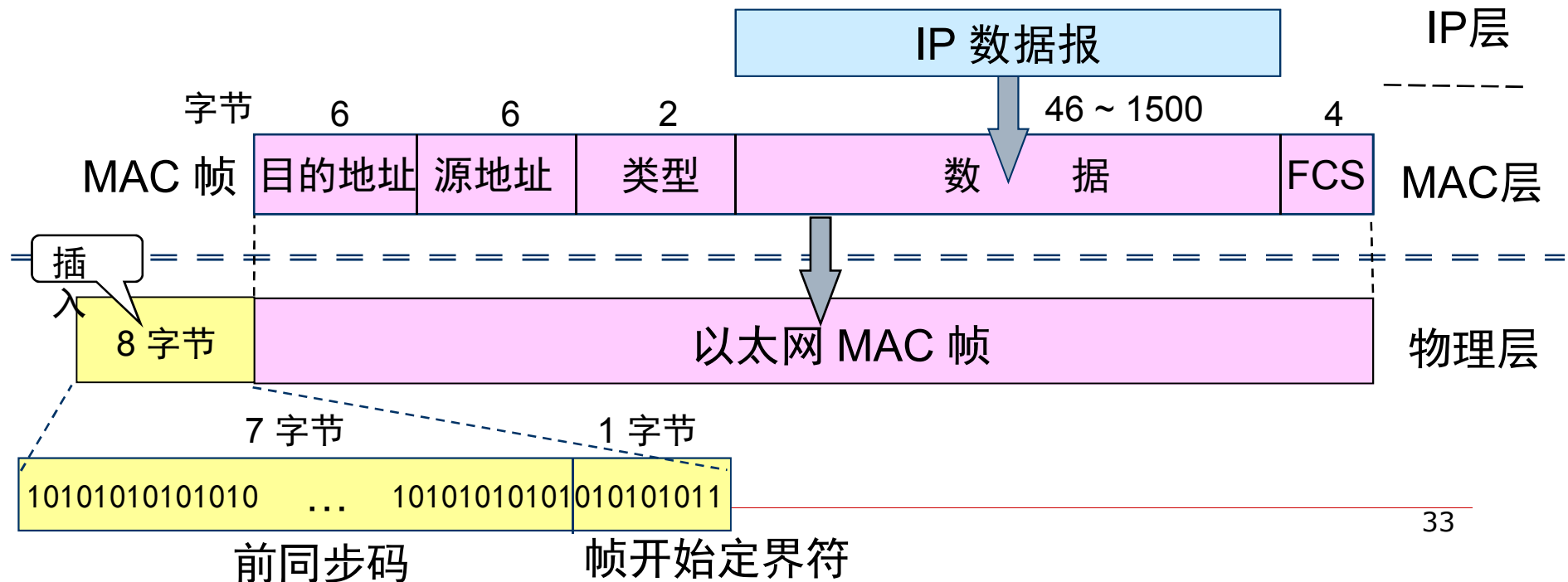
➤ MAC 帧的格式

最常用

✓ 常用的以太网MAC帧格式有两种标准：

◆ DIX Ethernet V2 标准

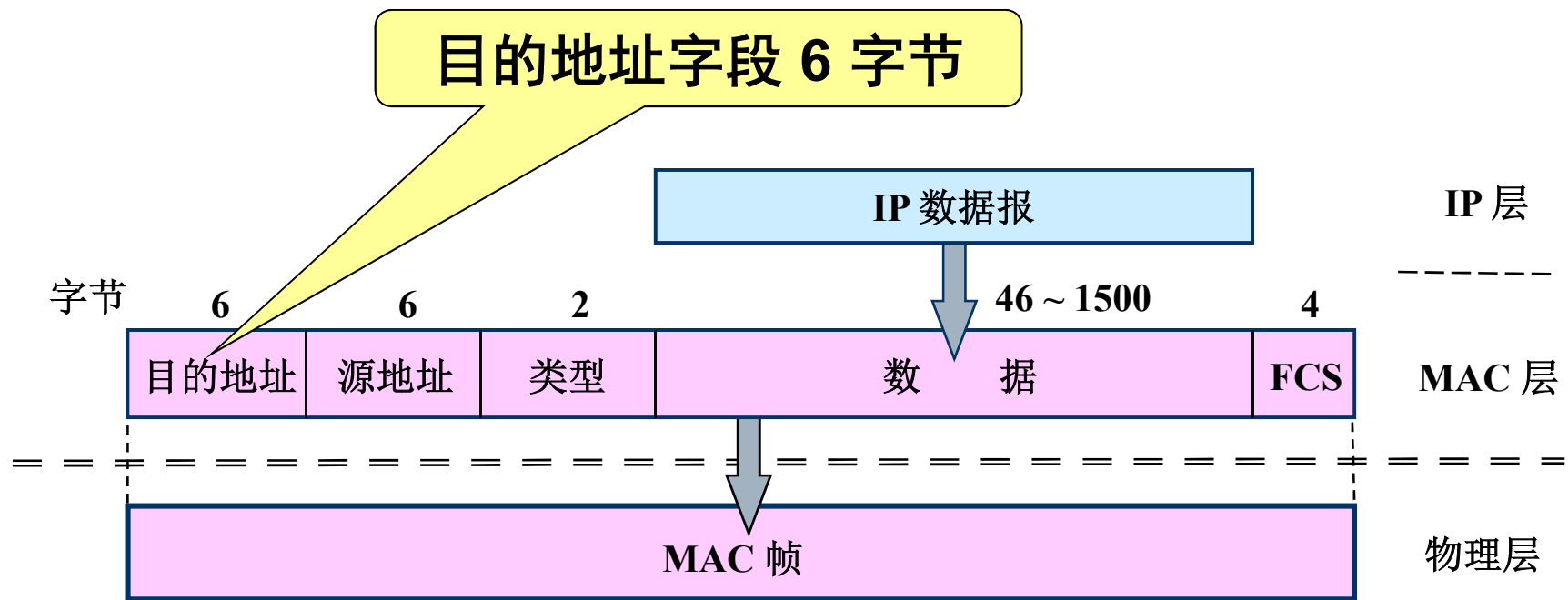
◆ IEEE 的 802.3 标准



以太网的 MAC 层

➤ MAC 帧的格式

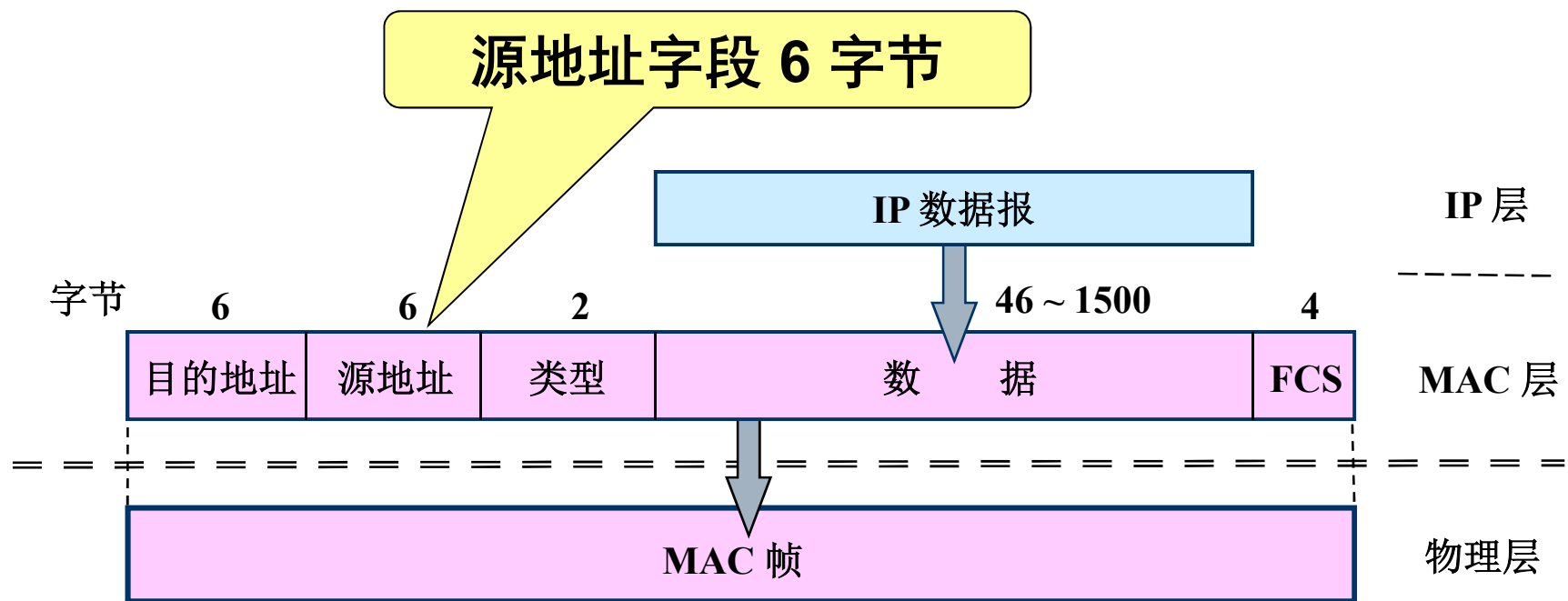
✓ 以太网 **DIX Ethernet V2** MAC 帧格式



以太网的 MAC 层

➤ MAC 帧的格式

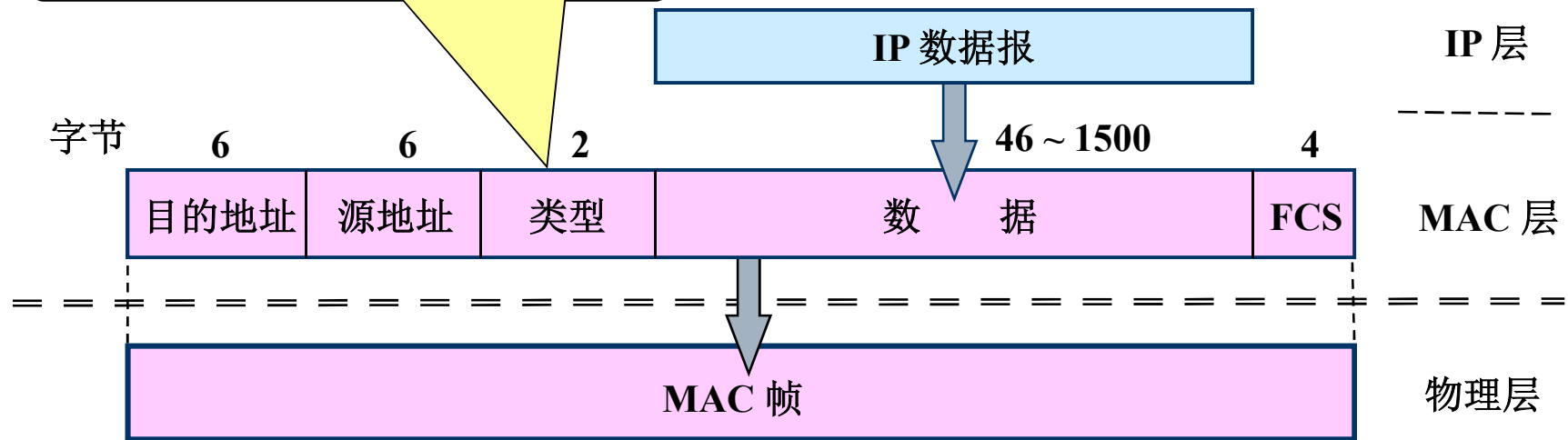
✓ 以太网DIX Ethernet V2 MAC帧格式



以太网的 MAC 层

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。
值为0x0800时，表示上一层使用IP数据报

类型字段 2 字节

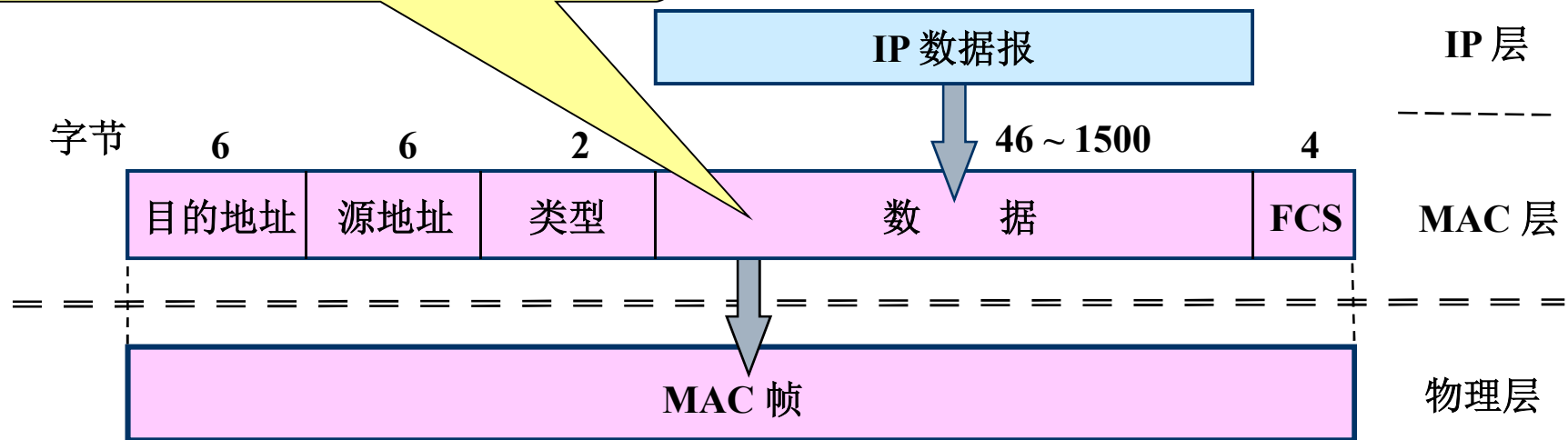


➤ 数据字段的正式名称是 **MAC 客户数据字段**

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

➤ 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**。

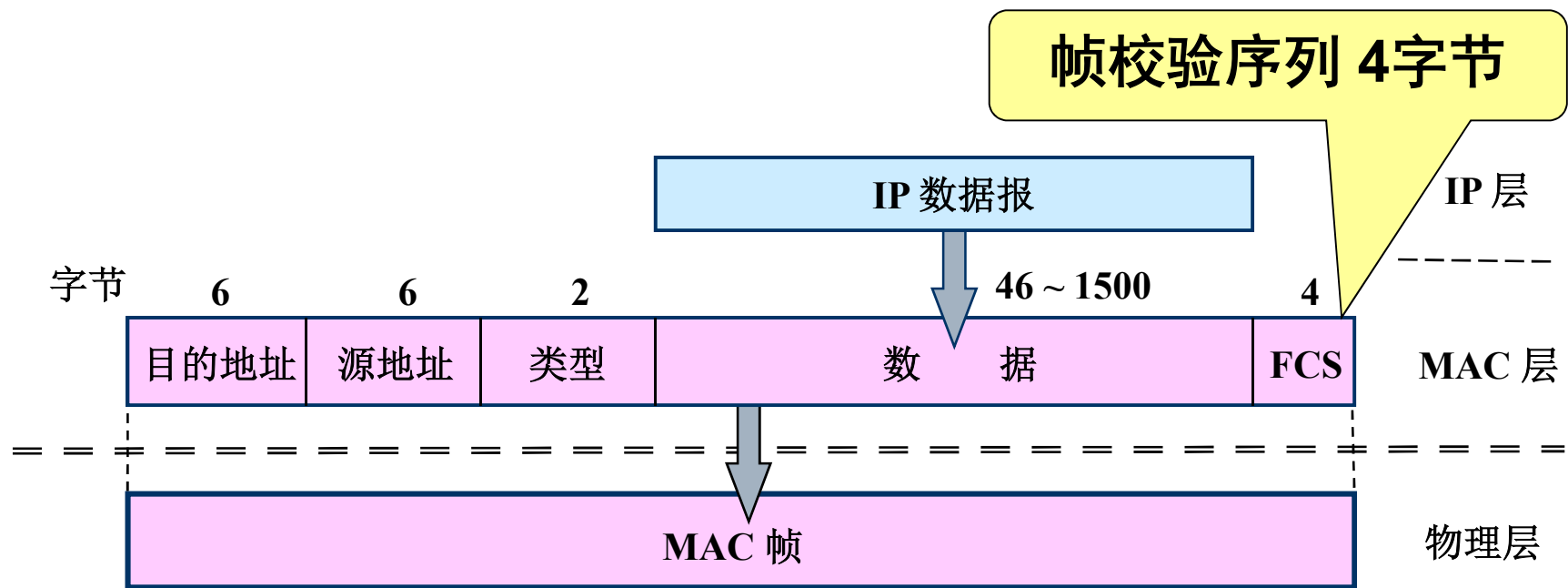
数据字段46 ~1500 字节



以太网的 MAC 层

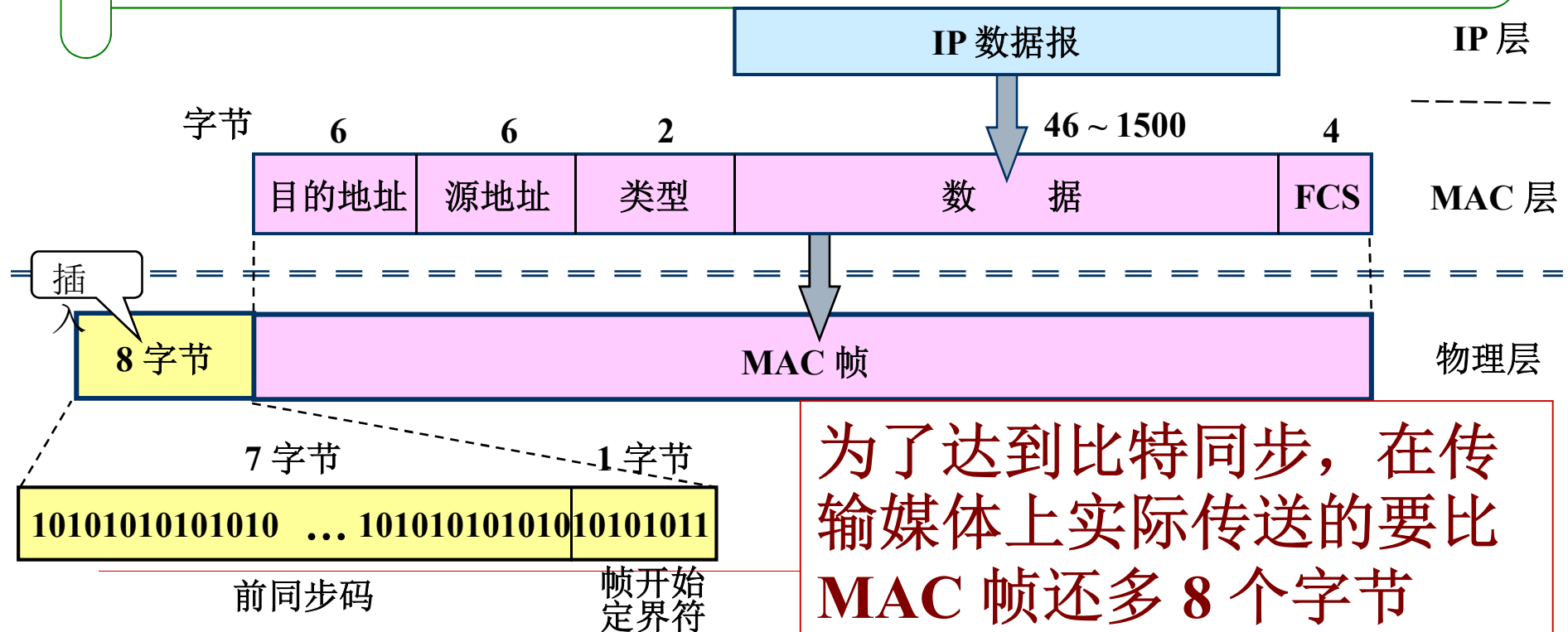
➤ MAC 帧的格式

✓ 以太网 DIX Ethernet V2 MAC 帧格式



以太网的 MAC 层

在帧的前面插入的 8 字节中的第一个字段共 7 个字节，是前同步码，用来迅速实现 MAC 帧的比特同步。第二个字段是帧开始定界符，表示后面的信息就是 MAC 帧。



以太网的 MAC 层

➤ MAC 帧的格式

✓ 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 帧长度为 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

➤ MAC 帧的格式

✓ 帧间最小间隔

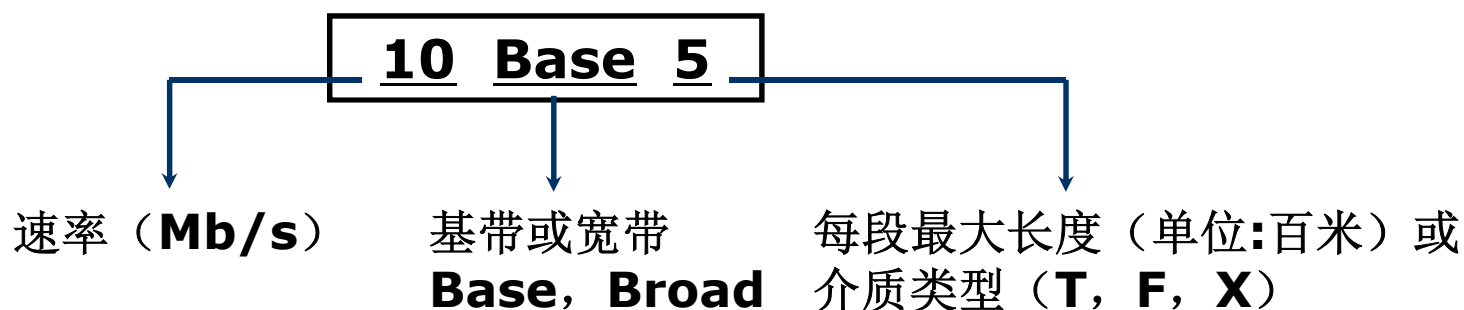
- ◆ 帧间最小间隔为 $9.6\ \mu\text{s}$ ，相当于 96 bit 的发送时间。
- ◆ 一个站在检测到总线开始空闲后，还要等待 $9.6\ \mu\text{s}$ 才能再次发送数据。
- ◆ 这样做是为了使刚刚收到数据帧的站的接收缓存来得及清理，做好接收下一帧的准备。

IEEE 802.3 以太网标准 (主要的)

- 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
 - 802.3j —— 光纤
- 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

以太网的物理层选项与标识方法

- 速率、信号方式、介质类型

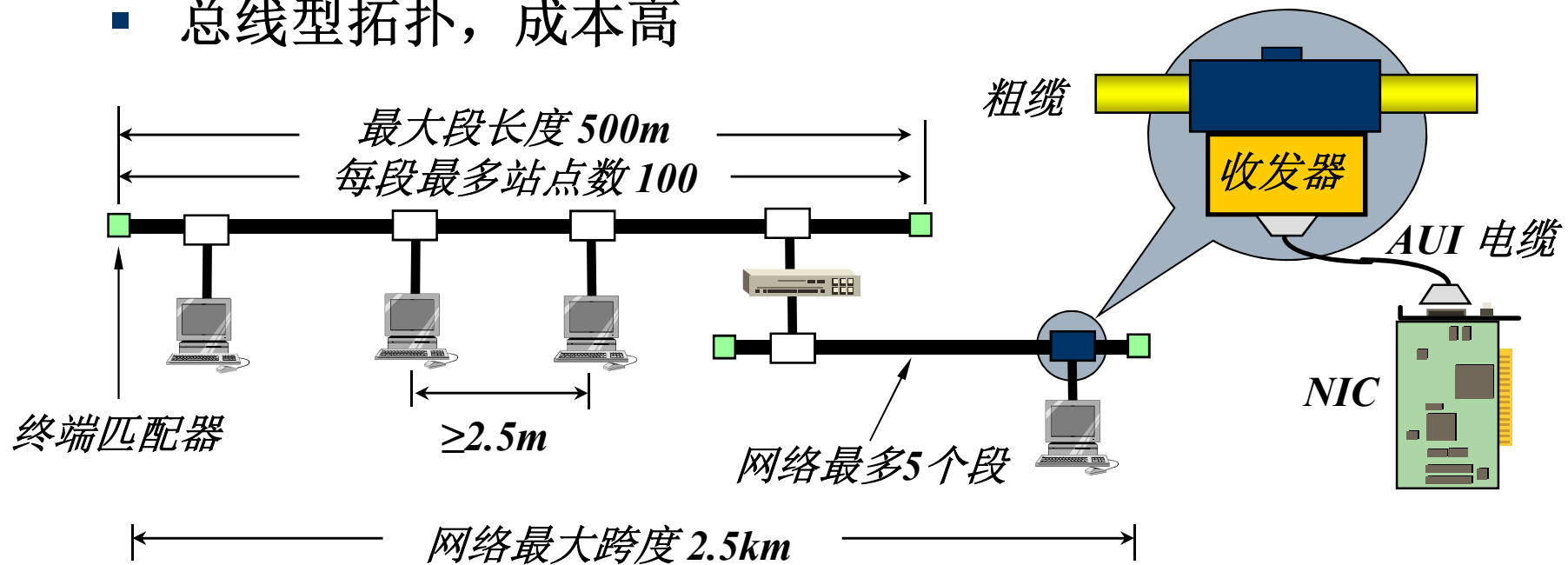


传统以太网		快速以太网和千兆以太网	
• 10Base5	粗同轴	• 100Base-T	UTP
• 10Base2	细同轴	• 100Base-F	MMF/SMF
• 10Base-T	UTP	• 1000Base-X	STP/MMF/SMF
• 10Base-F	MMF	• 1000Base-T	UTP

同轴电缆以太网

粗缆以太网（10BASE5）

- 粗同轴电缆，直径为**1.27**厘米，可靠性好，抗干扰能力强。扮演网络主干的角色，用来连接由细缆所结成的网络
- 收发器：发送/接收，冲突检测，电气隔离
- 总线型拓扑，成本高

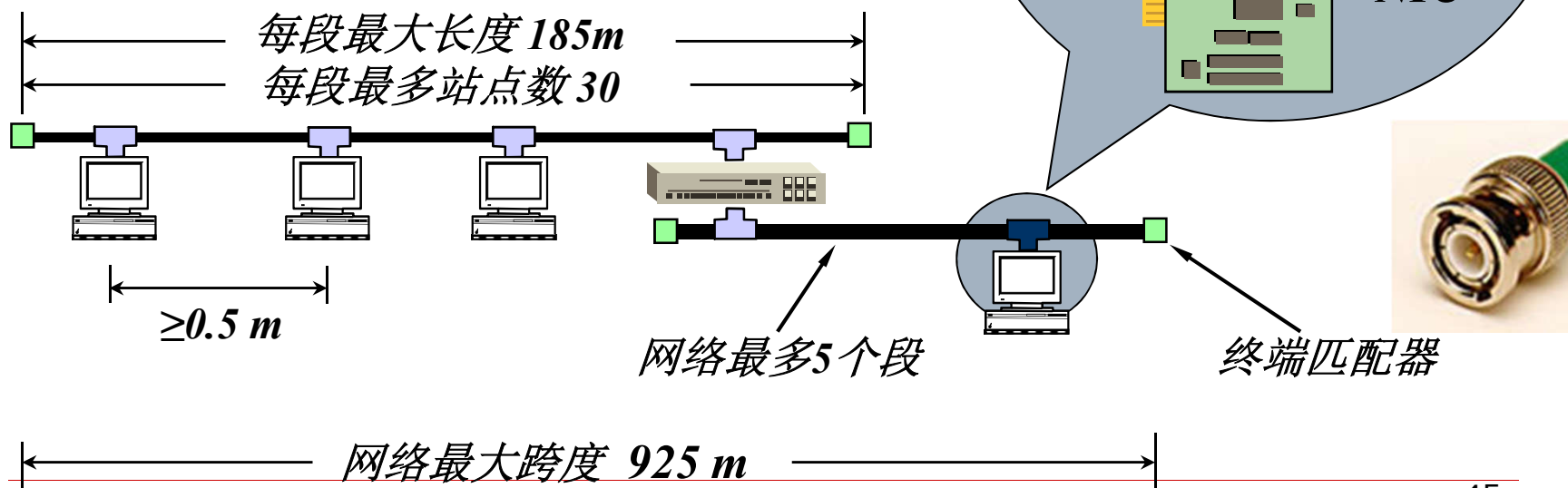


同轴电缆以太网



细缆以太网（**10Base2**）

- 细同轴电缆，**0.26厘米**，可靠性稍差
- 无外置收发器
- 轻便、灵活、成本较低
- 总线型拓扑，小型网络

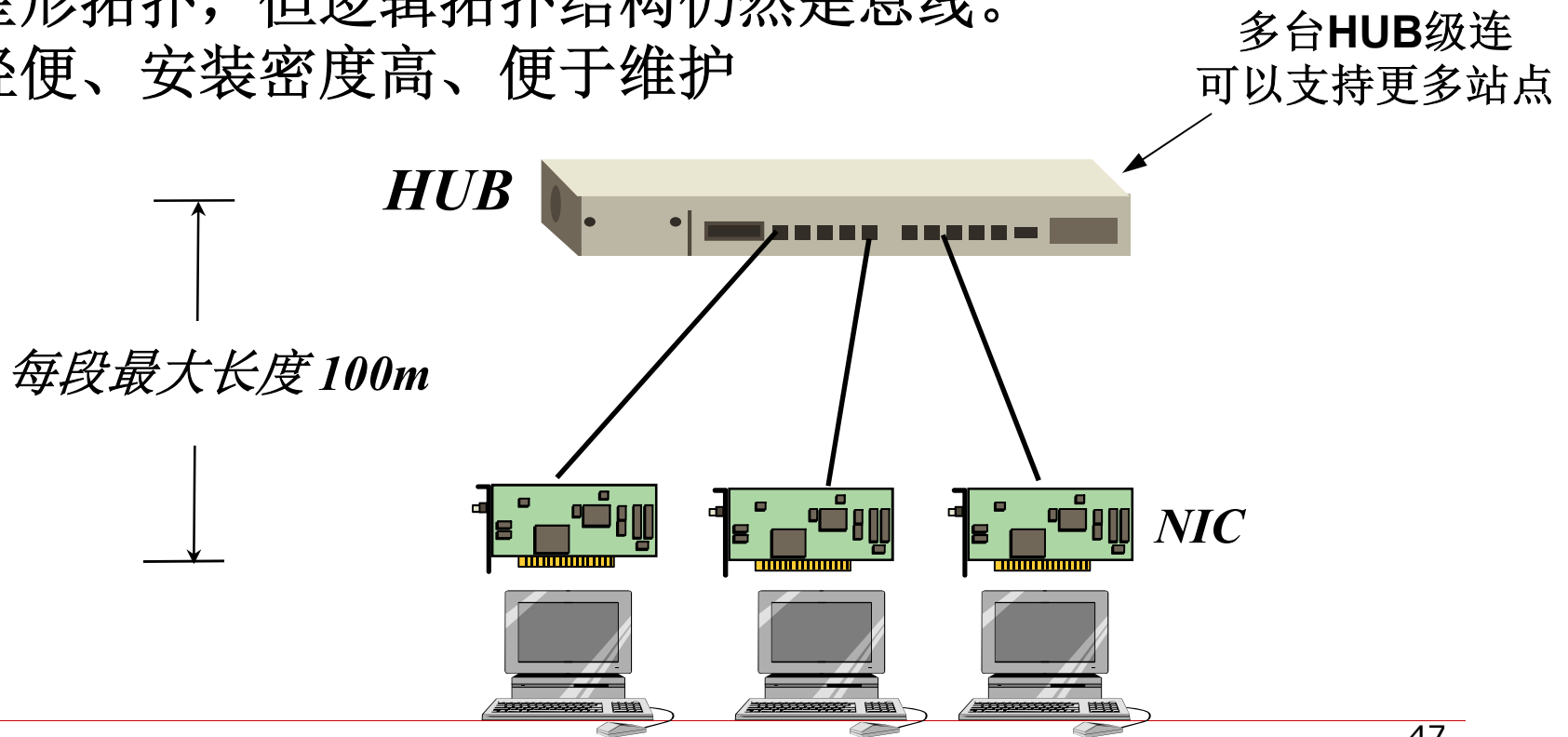


同轴电缆以太网

- 优点：可以在相对长的无中继器的线路上支持高带宽通信
- 缺点：
 - 一是体积大，要占用电缆管道的大量空间；
 - 二是不能承受缠结、压力和严重的弯曲，这些都会损坏电缆结构，阻止信号的传输；
 - 三是成本高，
- 而所有这些缺点正是双绞线能克服的，因此在现在的局域网环境中，基本已被基于双绞线的以太网物理层规范所取代。

双绞线以太网（10Base-T）

- 双绞线（**UTP**），两头压接**RJ45**连接器；
- 所有站点都与**HUB**（集线器）相连接；
 - **HUB**的作用：信号放大与整形
- 星形拓扑，但逻辑拓扑结构仍然是总线。
- 轻便、安装密度高、便于维护



光纤以太网

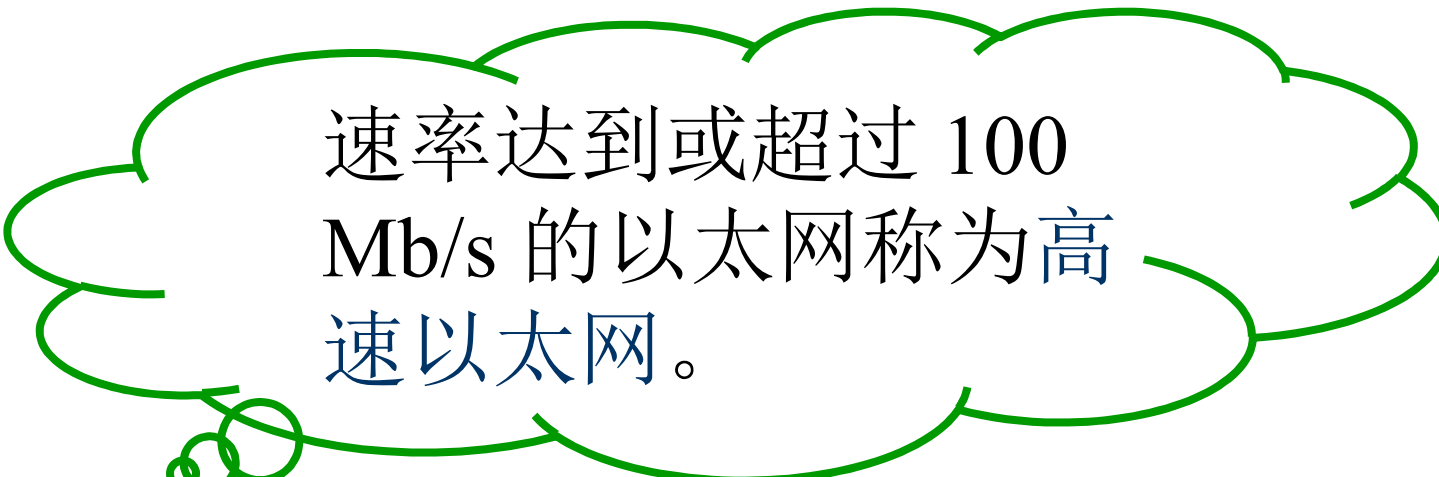
- 使用光纤介质；
 - 两根**62.5/125 μ m**多模光纤，收发各一根
- 星形拓扑结构；
- 通常用于远距离网络连接，可达**2000m**；
- 光纤与其他介质可使用介质转换器进行转换
 - 介质转换器是可连接不同介质的中继器

高速以太网

100BASE-T 以太网

吉比特以太网

10 吉比特以太网



速率达到或超过 100
Mb/s 的以太网称为高
速以太网。

100BASE-T 以太网

- 1992年9月100 Mb/s以太网的设想提出后13个月100 Mb/s以太网的产品就问世了。
- 在双绞线上传送 100 Mb/s 基带信号的星型拓扑以太网，仍使用 IEEE 802.3 的 CSMA/CD 协议。从10BASE-T升级到100BASE-T只需更换适配器和集线器。
- 100BASE-T 以太网又称为快速以太网 (Fast Ethernet)。

100BASE-T 以太网

➤ 100BASE-T 以太网特点

- ✓ 采用集线器或交换机组网，不再采用总线组网方式。
- ✓ MAC 帧格式仍然是 802.3 标准规定的。
- ✓ 保持最短帧长不变，但将一个网段的最大电缆长度减小到 100 m。
- ✓ 帧间时间间隔从原来的 9.6 μs 改为现在的 0.96 μs 。

吉比特以太网

- 千兆以太网，1996年产品问世，1997年通过了IEEE802.3z
- 在 1 Gb/s 下全双工和半双工两种方式工作。
- 使用 802.3 协议规定的帧格式。
- 在半双工方式下使用 CSMA/CD 协议。
- 在全双工方式时(即通信双方可同时进行发送和接收数据)，不用载波延伸和分组突发。
- 与 10BASE-T 和 100BASE-T 技术向后兼容。

10吉比特以太网

- 2002年6月，10GE万兆以太网标准完成。
- 与 10 Mb/s，100 Mb/s 和 1 Gb/s 以太网的帧格式完全相同。
- 保留了 802.3 标准规定的以太网最小和最大帧长，便于升级。
- 不再使用铜线而只使用光纤作为传输媒体。
- 工作在全双工方式，因此没有争用问题，也不使用 CSMA/CD 协议。

10吉比特以太网

- 10 吉比特以太网的出现，以太网的工作范围已经从局域网（校园网、企业网）扩大到城域网和广域网，从而实现了端到端的以太网传输。
- 从 10 Mb/s 到10 Gb/s 的演进证明了以太网：
 - ✓ 可扩展的（从 10 Mb/s 到 10 Gb/s）。
 - ✓ 灵活的（多种传输媒体、全/半双工、共享/交换）。
 - ✓ 易于安装。
 - ✓ 稳健性好。

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。

无线网络的类型

□ 无线个人区域网WPAN

- 小范围内相互连接数个装置所形成的无线网，10m左右
- 蓝牙、ZigBee

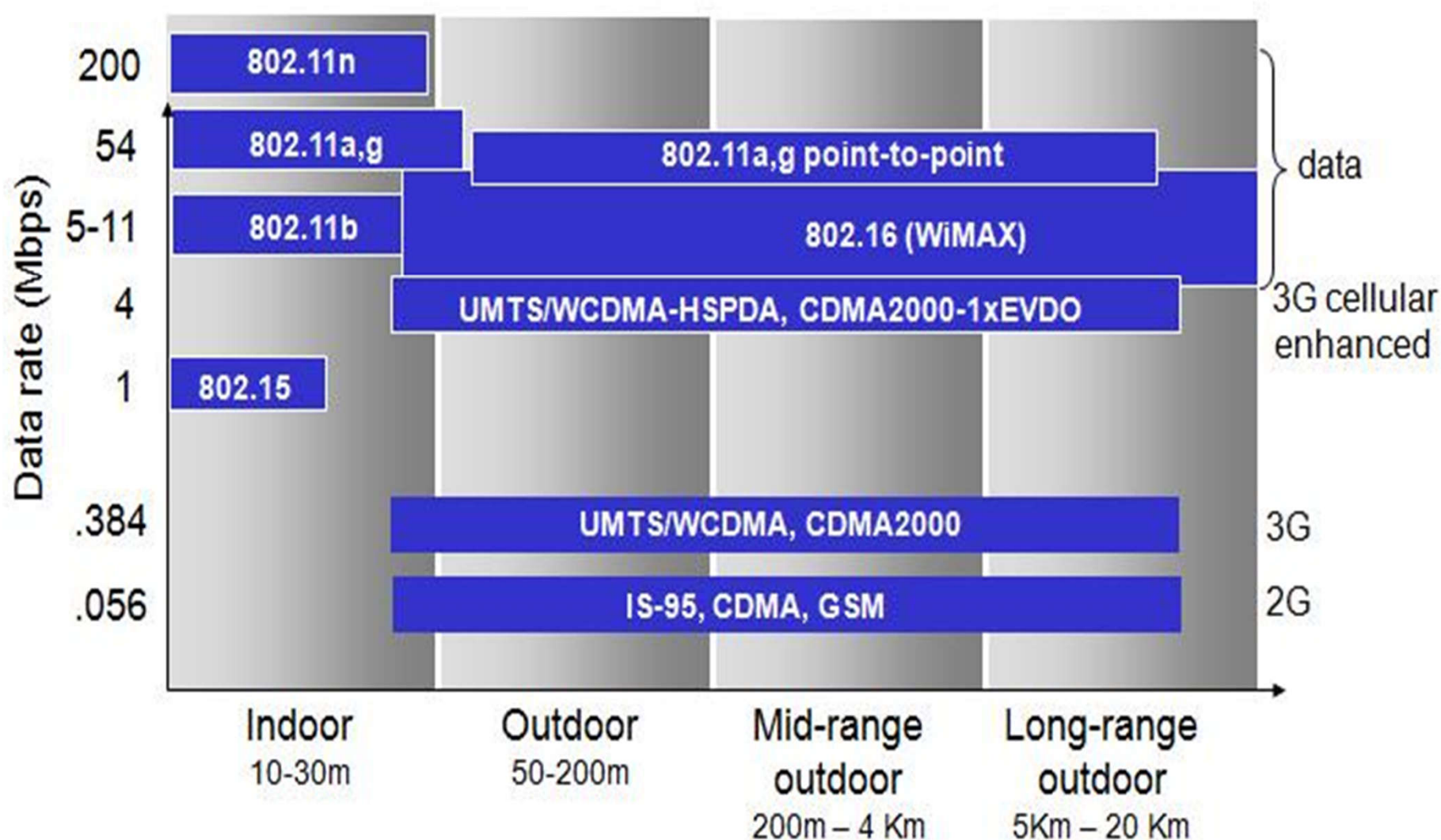
□ 无线局域网WLAN

- 采用无线通信技术构成的局域网
- Wifi

□ 无线城域网WMAN

- 无线方式构成的城域网，提供面向互联网的高速连接，50km。
- WiMAX

无线网络



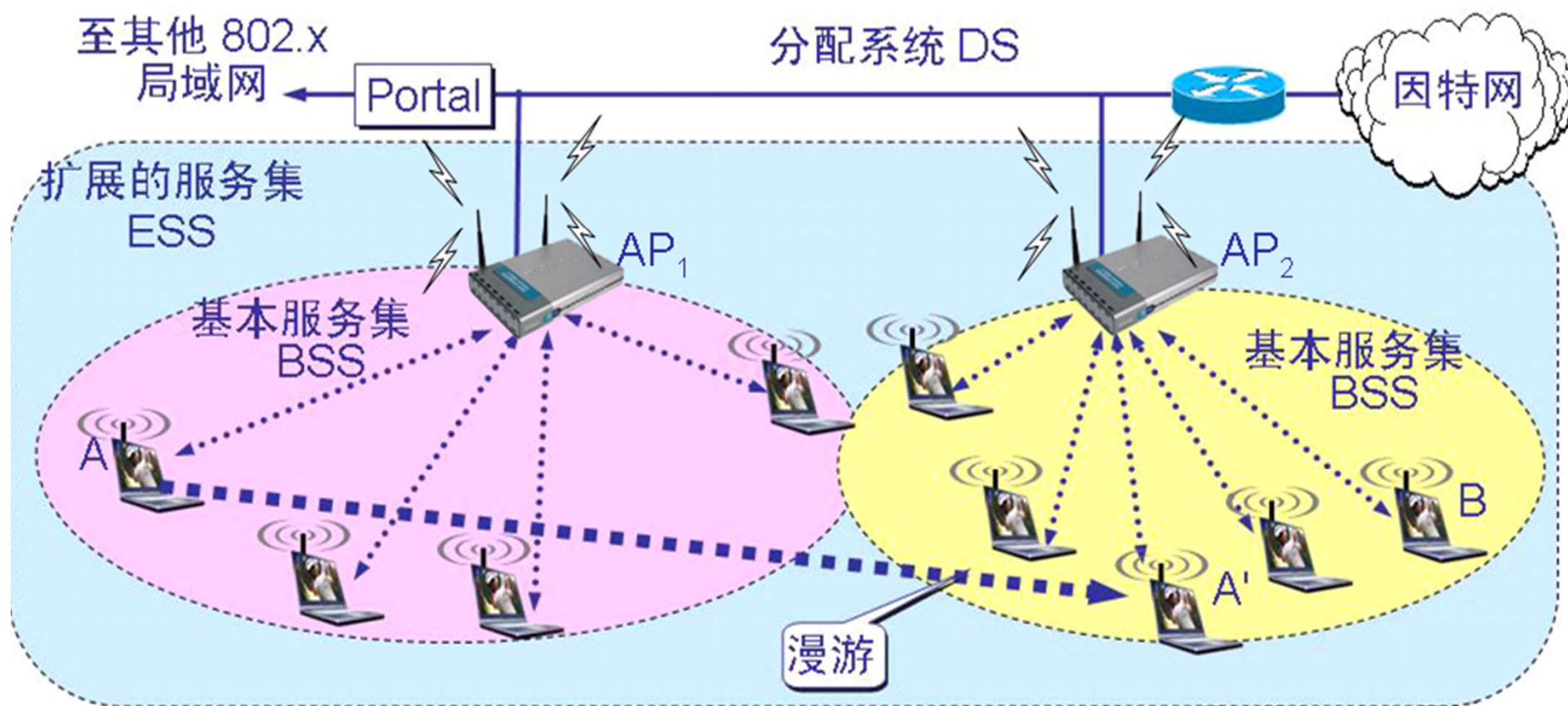
无线局域网标准

- WLAN，采用无线传输技术的局域网
- IEEE802.11标准，1997年发布
 - 工作频带2.4GHz，最大传输速率2Mb/s
- 1999年9月，802.11a和802.11b
 - 802.11a：工作频带5.8GHz，最大传输速率54Mb/s
 - 802.11b：工作频带2.4GHz，最大传输速率11Mb/s
- 2003年6月，802.11g
 - 工作频带2.4GHz，最大传输速率54Mb/s
- 2007年3月，802.11n（草案2.0版本）
 - 工作频带2.4GHz/5GHz，最大传输速率约为300Mb/s

无线局域网的组成

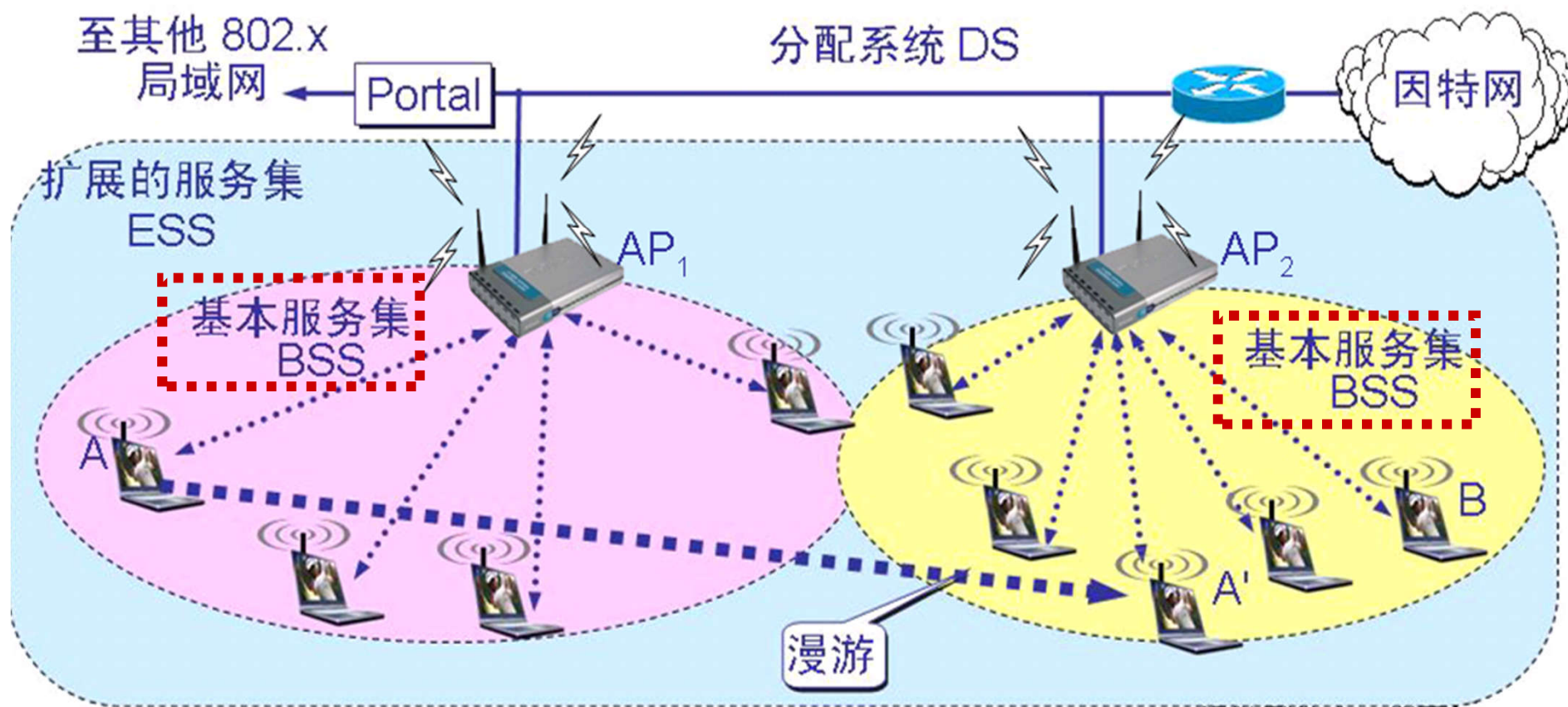
□ 1、有固定基础设施的无线局域网

- 预先建立起来的、能够覆盖一定范围的一批固定基站



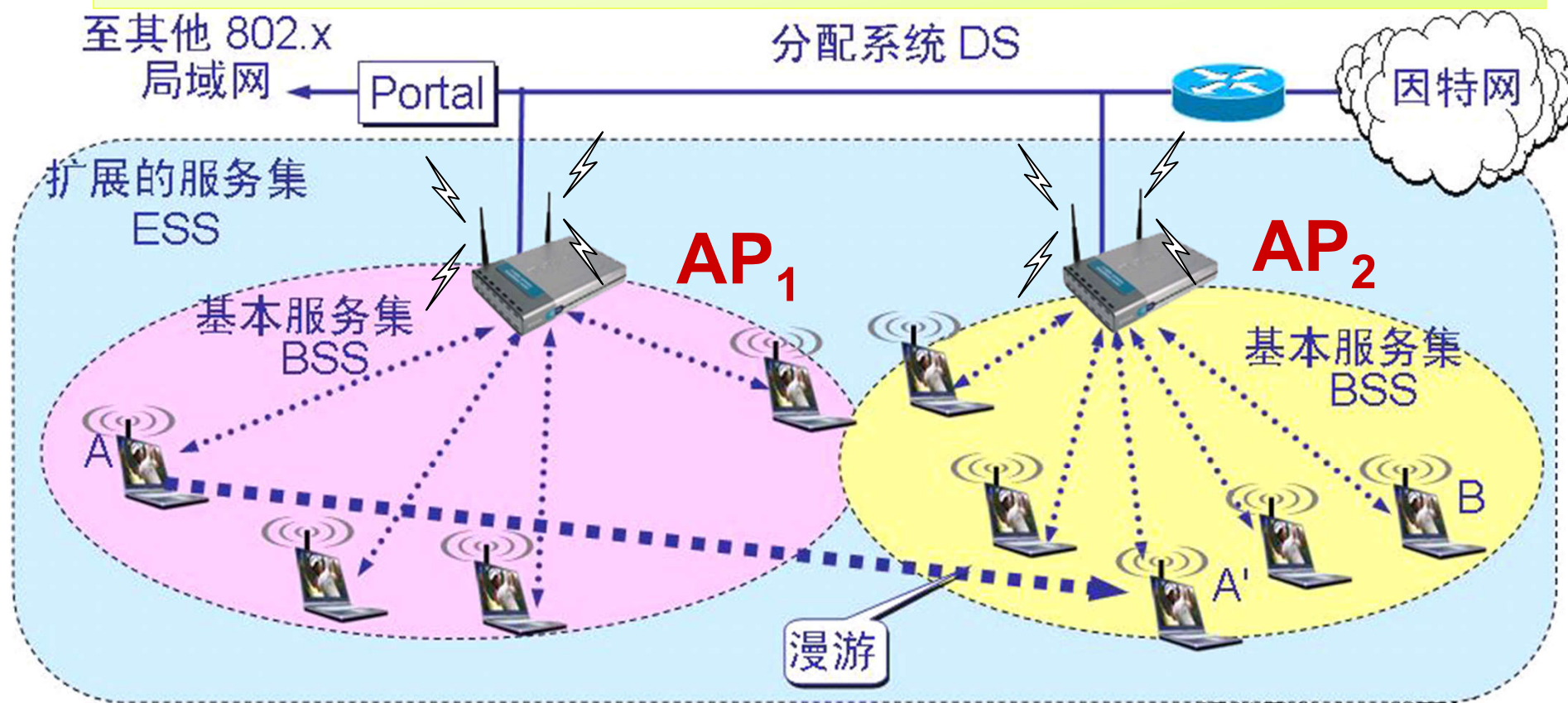
无线局域网的组成

➤ 一个**基本服务集 BSS** 包括一个基站和若干个移动站，所有的站在本 BSS 以内都可以直接通信，但在和本 BSS 以外的站通信时，都要通过本 BSS 的基站



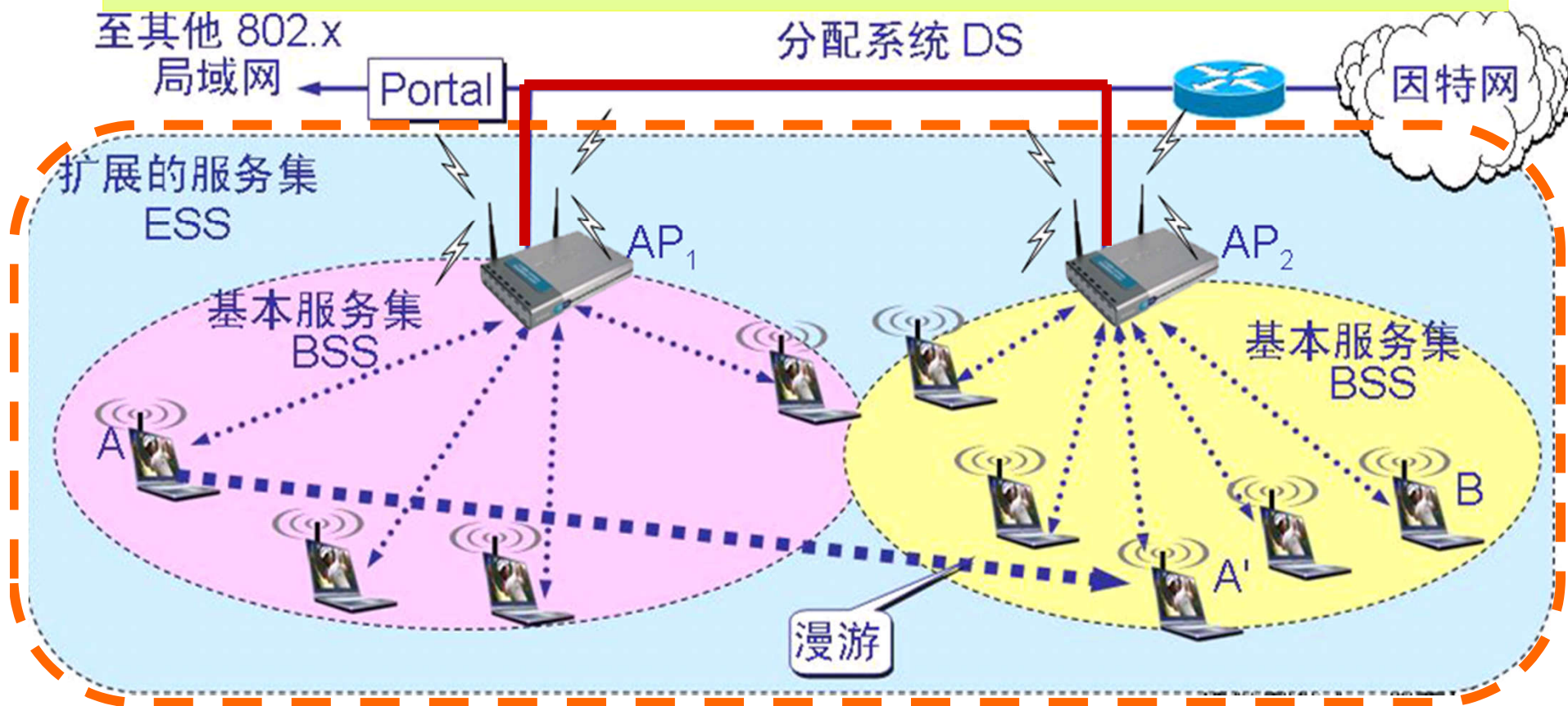
无线局域网的组成

- 基本服务集内的基站叫做**接入点 AP (Access Point)**, 其作用和**网桥**相似。
- 当网络管理员安装 AP 时, 必须为该 AP 分配一个不超过 32 字节的服务集标识符 **SSID** 和一个**信道**。



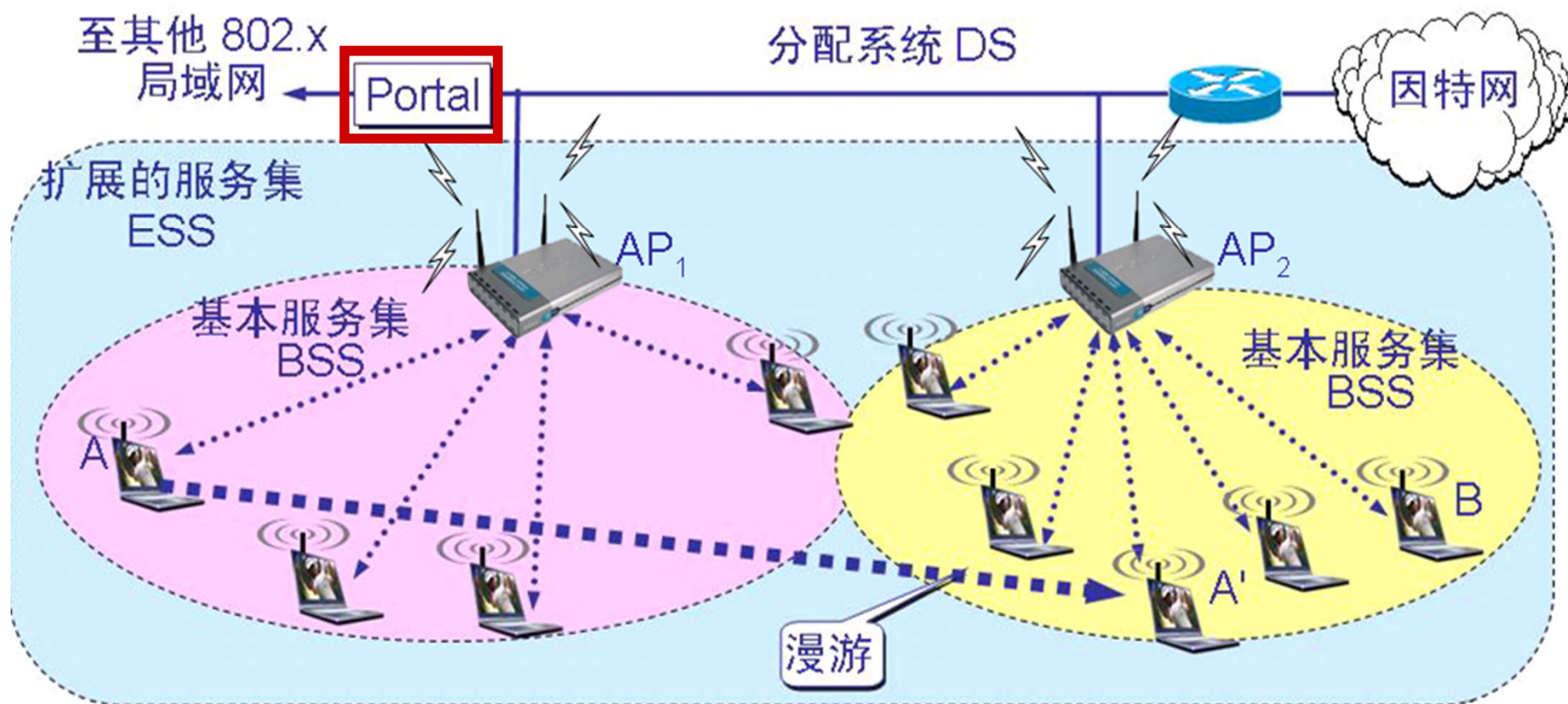
无线局域网的组成

➤ 一个基本服务集可以是孤立的，也可通过接入点 AP 连接到一个主干分配系统 DS (Distribution System)，然后再接入到另一个基本服务集，构成扩展的服务集 ESS (Extended Service Set)。



无线局域网的组成

➤ ESS 还可通过**门户 (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。**门户**的作用就相当于一个**网桥**。



无线局域网的组成

- 与接入点 AP 建立**关联**(association)
 - 一个移动站若要加入到一个基本服务集BSS,就必须先选择一个接入点 AP, 并与此接入点**建立关联**。
 - 建立关联就表示这个移动站加入了选定的 AP 所属的子网, 并和这个 AP 之间创建了一个**虚拟线路**。
 - 只有关联的 AP 才向这个移动站发送数据帧, 而这个移动站也只有通过关联的 AP 才能向其他站点发送数据帧。
-

无线局域网的组成

- 移动站与 AP 建立关联的方法
 - **被动扫描**，移动站等待接收接入站周期性发出的**信标帧**(beacon frame)。
 - 信标帧中包含有若干系统参数(如服务集标识符 **SSID** 以及支持的速率等)。
 - **主动扫描**，移动站主动发出**探测请求帧**(probe request frame)，然后等待从 AP 发回的**探测响应帧**(probe response frame)。
-

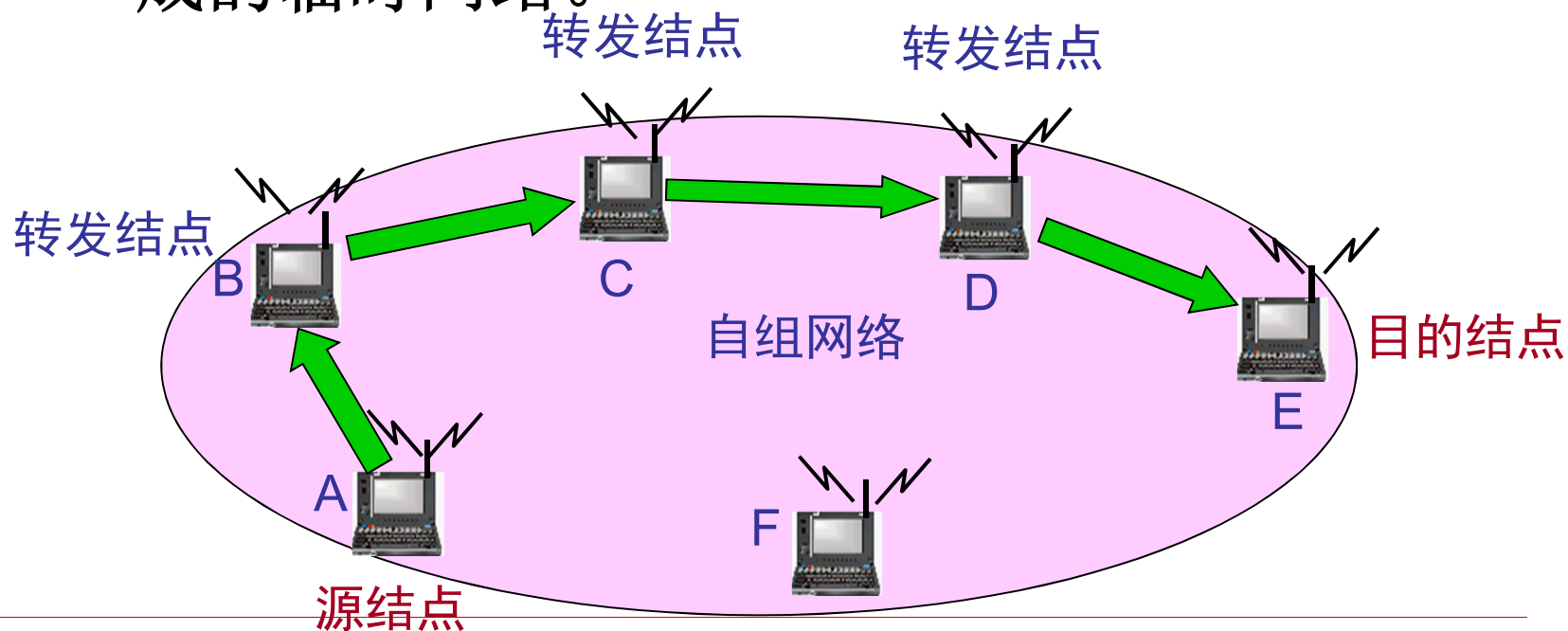
无线局域网的组成

□ 热点(hot spot)

- 现在许多地方，如办公室、机场、快餐店、旅馆、购物中心等都能够向公众提供有偿或无偿接入 **Wi-Fi** 的服务。这样的地点就叫做**热点**。
 - 由许多热点和 **AP** 连接起来的区域叫做**热区** (**hot zone**)。热点也就是公众无线入网点。
 - 现在也出现了**无线因特网服务提供商 WISP** (**Wireless Internet Service Provider**)这一名词。用户可以通过无线信道接入到 **WISP**，然后再经过无线信道接入到因特网。
-

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。



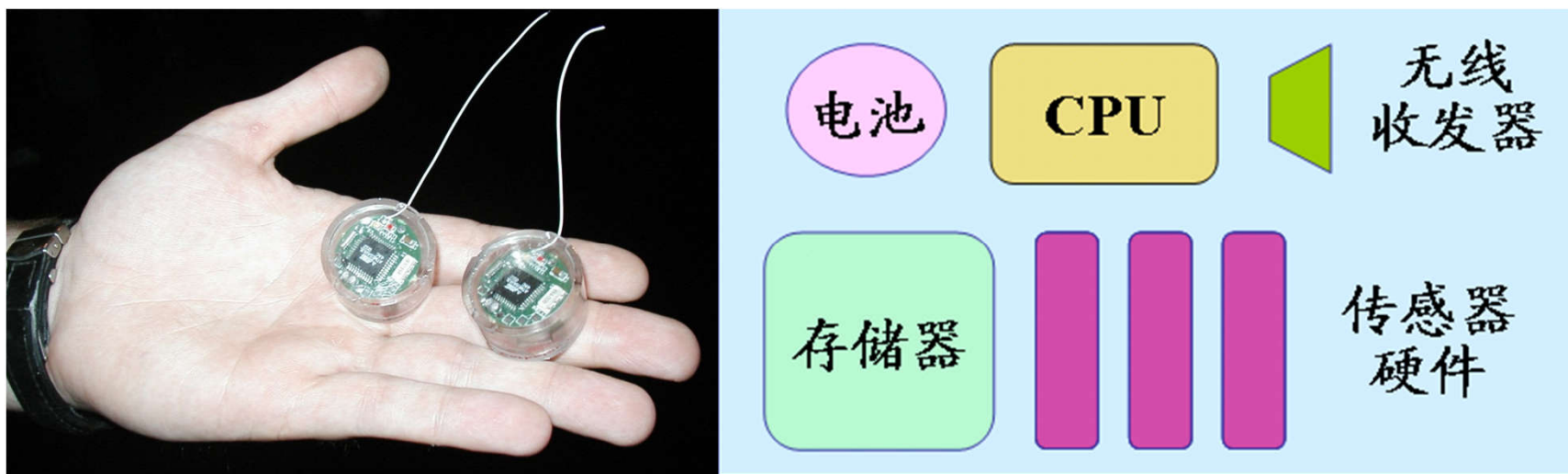
无线局域网的组成

□ 移动自组网络的应用前景

- 在军事领域中，携带了移动站的战士可利用临时建立的移动自组网络进行通信。
 - 这种组网方式也能够应用到作战的地面车辆群和坦克群，以及海上的舰艇群、空中的机群。
 - 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。
-

无线局域网的组成

- ❑ 无线传感器网络 WSN (Wireless Sensor Network)
 - 由大量**传感器**结点通过无线通信技术构成的自组网络。
 - 应用在各种数据的采集、处理和传输，一般并不需要很高的带宽，但是在大部分时间必



802.11 局域网的MAC 层协议

- 802.11的MAC和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。但无线局域网不能简单地搬用 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，因此若要实现碰撞检测，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
-

802.11 局域网的MAC 层协议

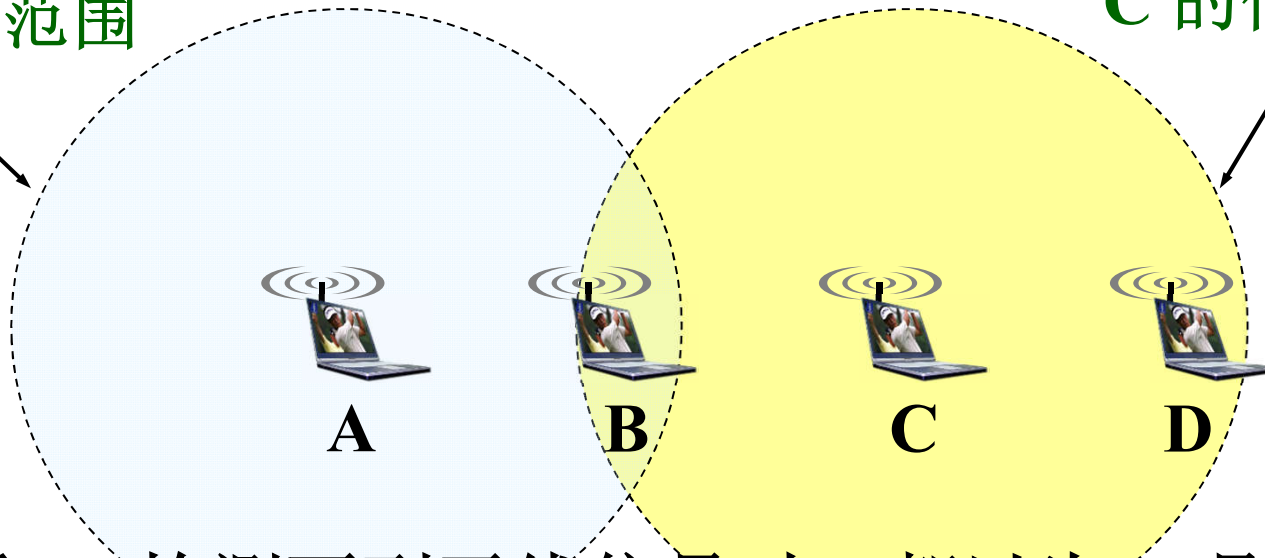
□ 无线局域网的特殊问题

➤ 这种未能检测出媒体上已存在的信号的问题

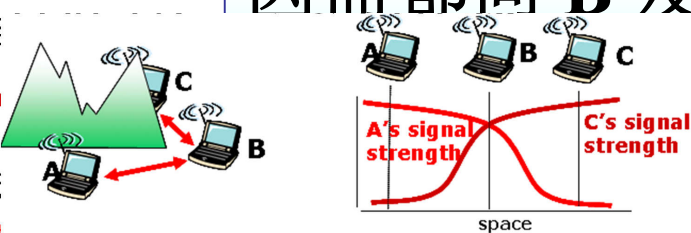
叫做**隐蔽站问题**(hidden station problem)

A 的作用范围

C 的作用范围



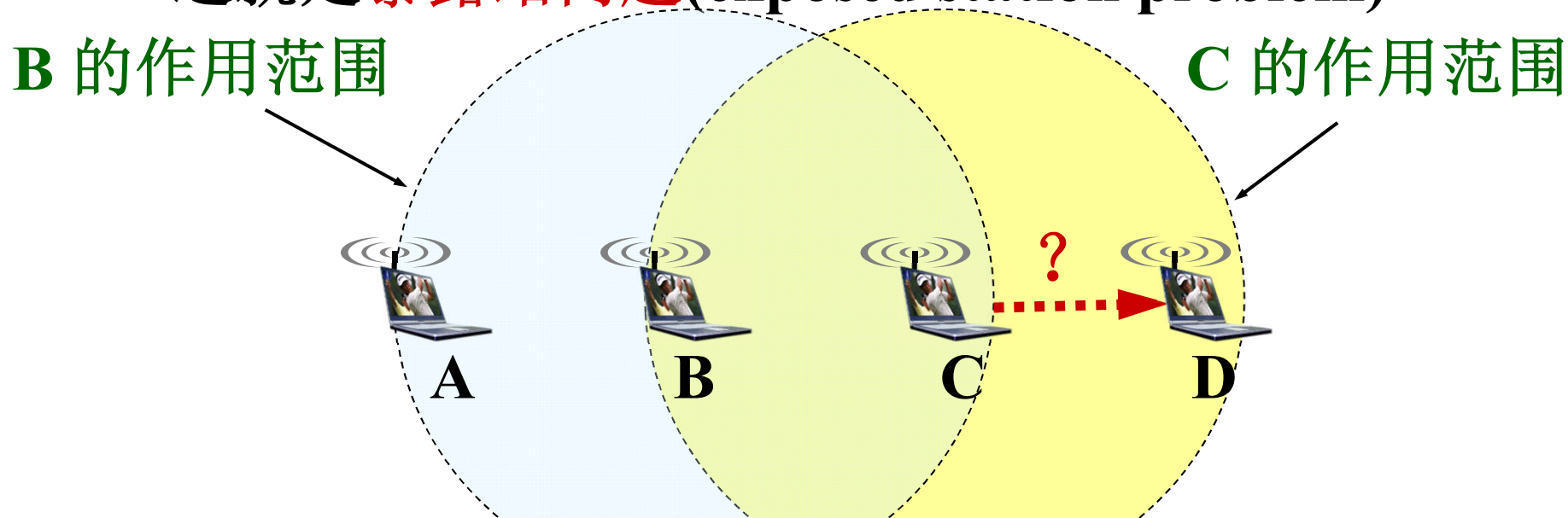
➤ 当 A 和 C 检测不到无线信号时，都以为 B 是空闲的，因而都向 B 发送数据，结果发生碰撞。



802.11 局域网的MAC 层协议

❑ 无线局域网的特殊问题

- 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 局域网的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**碰撞避免**(Collision Avoidance)功能，尽量减少碰撞的概率。
 - 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（Acknowledgement）和 RTS/CTS
-

802.11 局域网的MAC 层协议

□ 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，以便让其它站在这段时间内不要发送数据，起到了避免冲突的效果。

□ 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。

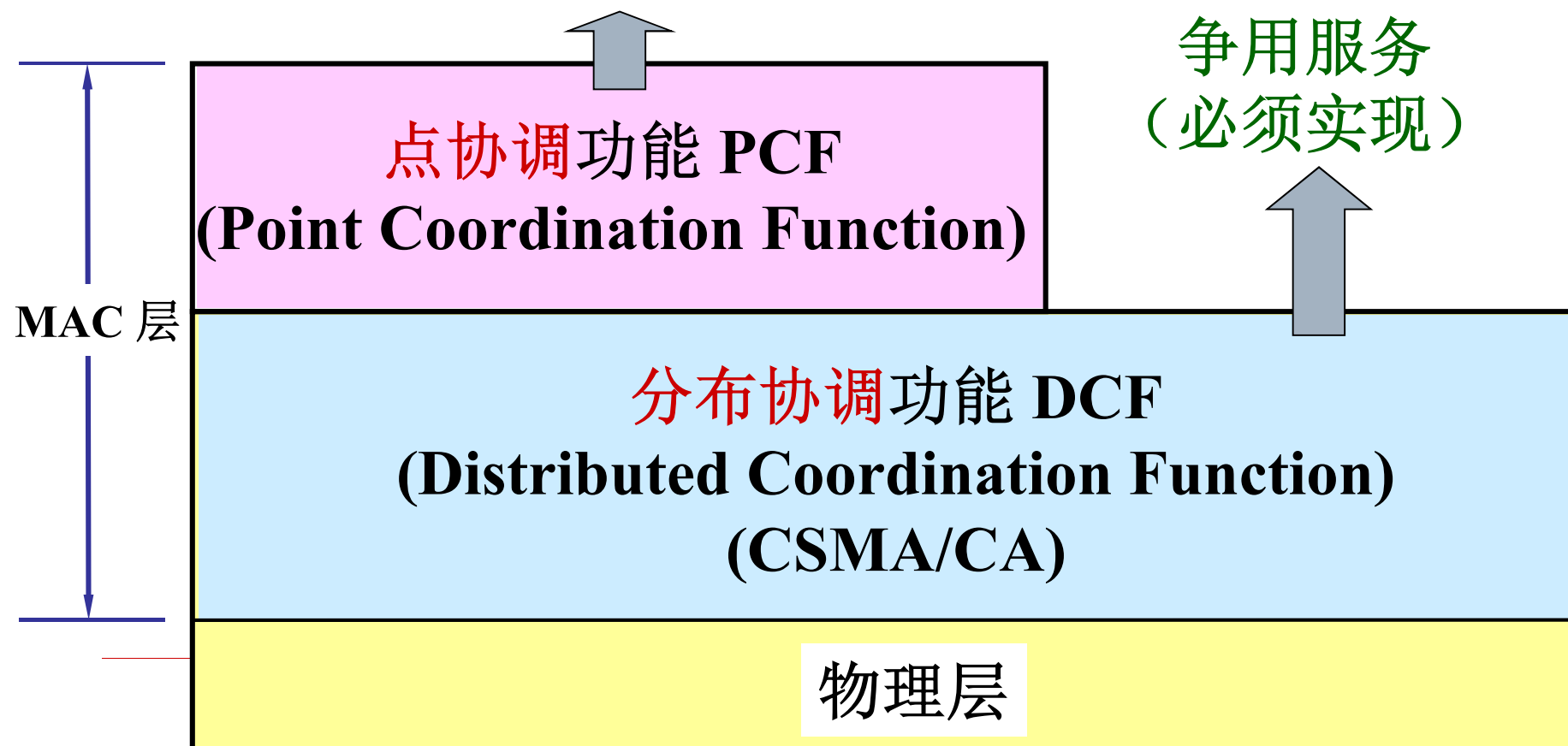
□ **RTS/CTS**

- 通过RTS/CTS帧预约信道，以避免隐蔽站冲突问题。
-

802.11 局域网的MAC 层协议

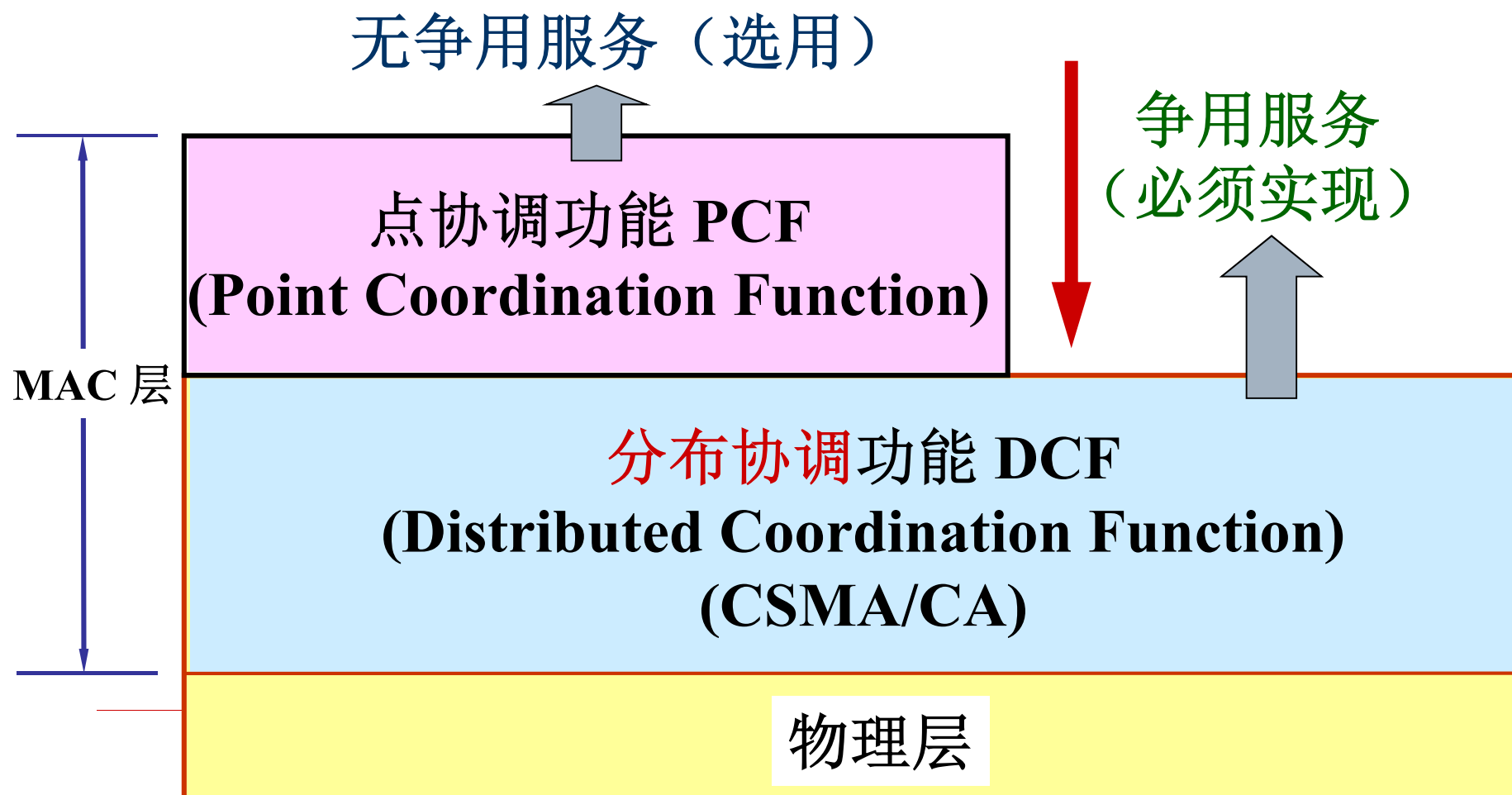
➤MAC 层通过**协调**功能来确定在基本服务集 BSS 中的移动站在什么时间能**发送数据**或**接收数据**。

无争用服务（选用）



802.11 局域网的MAC 层协议

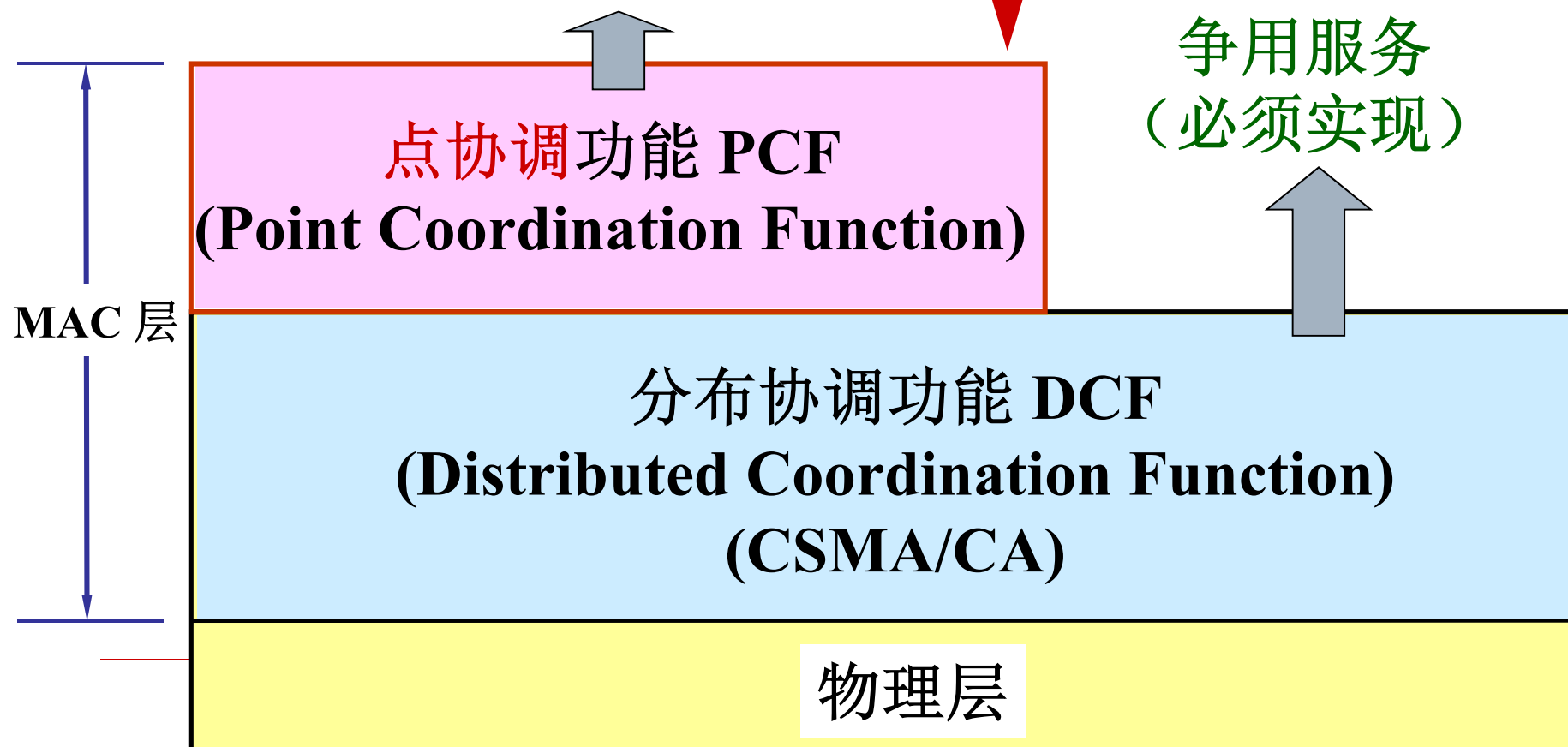
➤ 每个节点使用CSMA 机制的分布式接入算法,让各站通过争用信道获取发送权,向上提供争用服务。



802.11 局域网的MAC 层协议

➤使用AP集中控制的接入算法把发送数据权轮流交给各个站从而避免了碰撞的产生。自组网没有PCF。

无争用服务（选用）



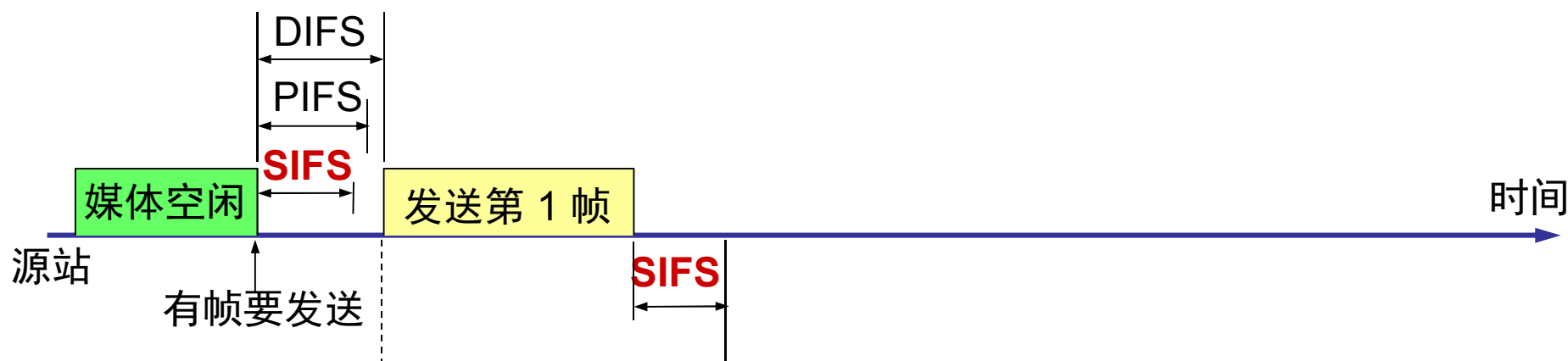
802.11 局域网的MAC 层协议

□ 帧间间隔 IFS (InterFrame Space)

- 为了尽量避免碰撞，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。这段时间的通称是**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了。这样就减少了发生碰撞的机会。
-

802.11 局域网的MAC 层协议

□三种帧间间隔



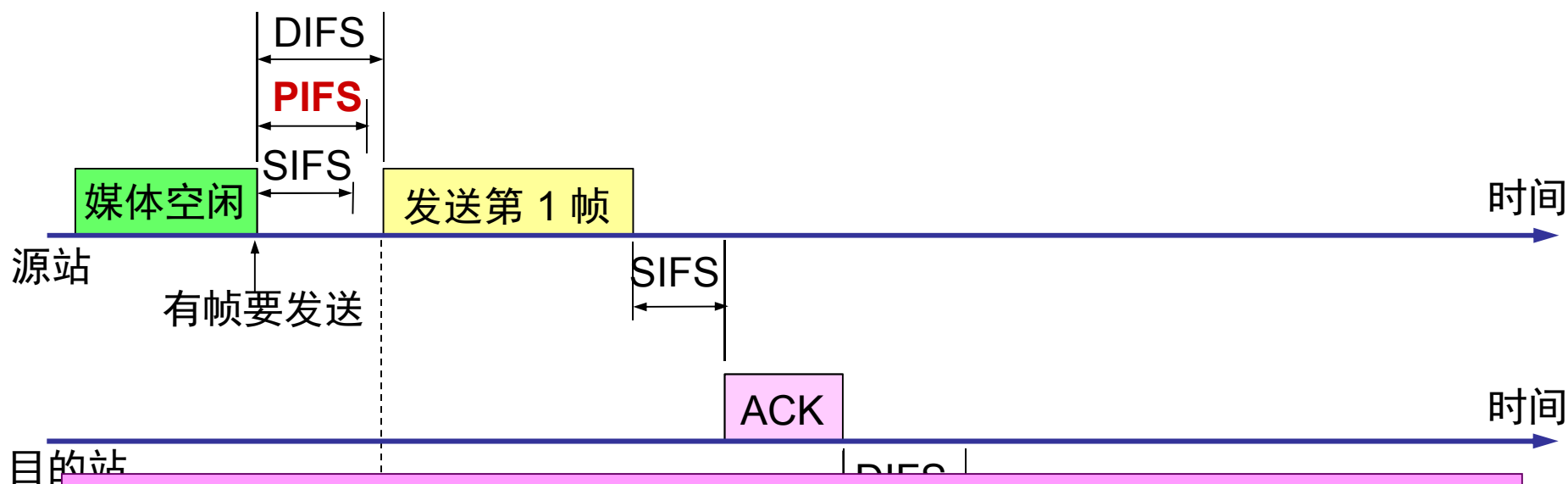
□SIFS，即短(Short)帧间间隔，是最短的帧间间隔，用来分隔开属于一次对话的各帧。

□一个站应当能够在这段时间内从发送方式切换到接收方式。

□使用 SIFS 的帧类型有：ACK 帧、CTS 帧、由过长的 MAC 帧分片后的数据帧，以及所有回答 AP 探测的帧和在 PCF 方式中接入点 AP 发送出的任何帧。

802.11 局域网的MAC 层协议

□ 三种帧间间隔



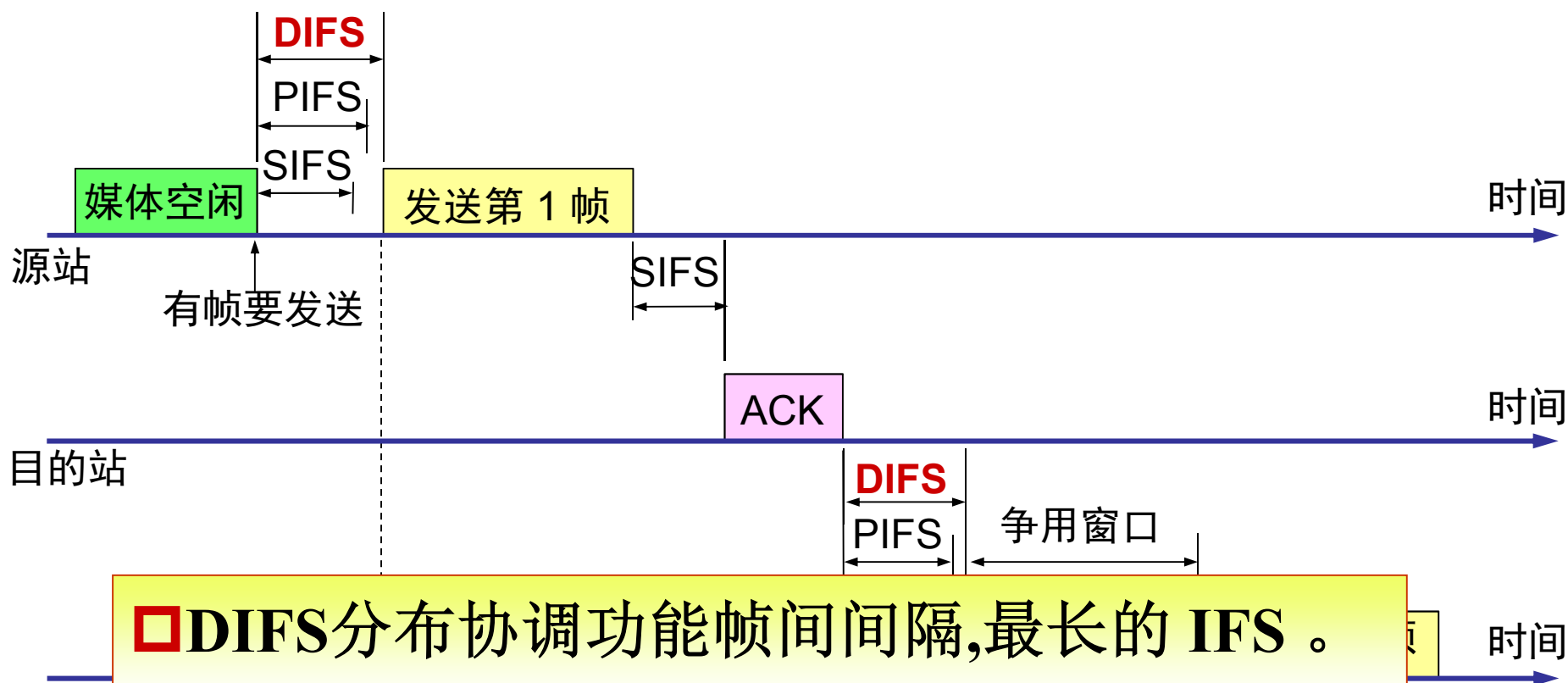
□ PIFS点协调功能帧间间隔，比 SIFS 长

□ 用于AP发送信标帧或者关联响应帧。

□ 表明AP比一般的无线站点有更高的优先级访问无线信道，同时表明无线站点处于PCF工作模式。

802.11 局域网的MAC 层协议

□ 三种帧间间隔



□ DIFS 分布协调功能帧间间隔,最长的 IFS。

□ 在 DCF 方式中用来发送数据帧和管理帧。
通过 CSMA/CA 协议竞争访问信道。

802.11 局域网的MAC 层协议

□ CSMA/CA 协议的原理

□ 发送站点

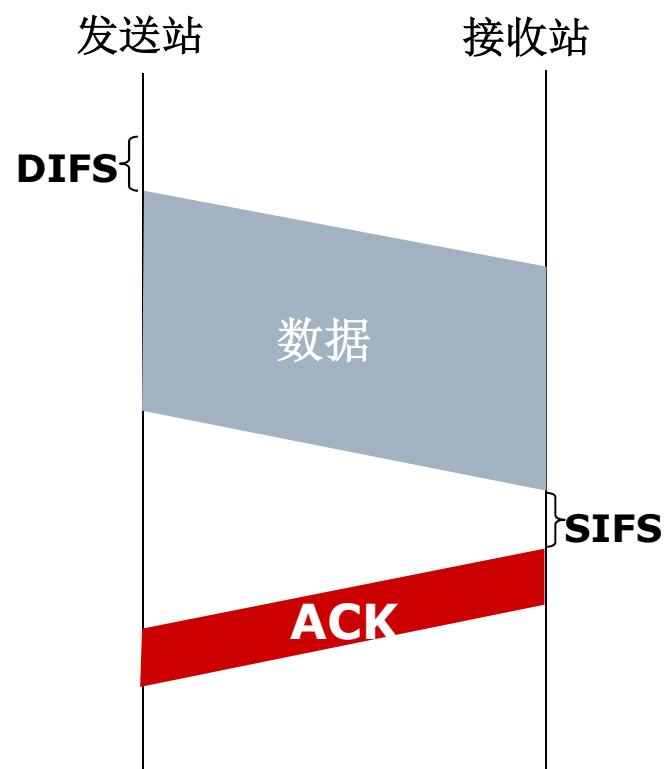
- 如果监听到信道空闲时间达到DIFS，则发送数据帧
- 如果信道忙，则开始退避，退避时间到时发送数据帧
- 如果ACK超时，则增加退避时间

□ 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



802.11 局域网的MAC 层协议

□ 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。
-

802.11 局域网的MAC 层协议

- ❑ 为了减少碰撞，采用了虚拟载波监听(Virtual Carrier Sense)的机制，是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段时间都停止发送数据。
 - ❑ 这样就大大减少了碰撞的机会。
 - ❑ “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。
-

802.11 局域网的MAC 层协议

□ 虚拟载波监听的效果

- 这种效果好像是其他站都监听了信道。
 - 所谓“源站的通知”就是源站在其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), 包括目的站发送确认帧所需的时间。
-

802.11 局域网的MAC 层协议

□ 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。
-

802.11 局域网的MAC 层协议

□ 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。这样做就减少了发生碰撞的概率。
 - **802.11** 使用二进制指数退避算法。
-

802.11 局域网的MAC 层协议

□ 二进制指数退避算法

- 第 i 次退避就在 2^{2+i} 个时隙中随机地选择一个，即：第 i 次退避是在时隙 $\{0, 1, \dots, 2^{2+i}-1\}$ 中随机地选择一个。
 - 第 1 次退避是在 8 个时隙（而不是 2 个）中随机选择一个。
 - 第 2 次退避是在 16 个时隙（而不是 4 个）中随机选择一个。
 - 到第 6 次就不再增加了
-

802.11 局域网的MAC 层协议

- 退避时间确定后，就相当于设置了一个退避计时器(**backoff timer**)

站点每经历一个时隙的时间就检测一次信道，可能发生两种情况。

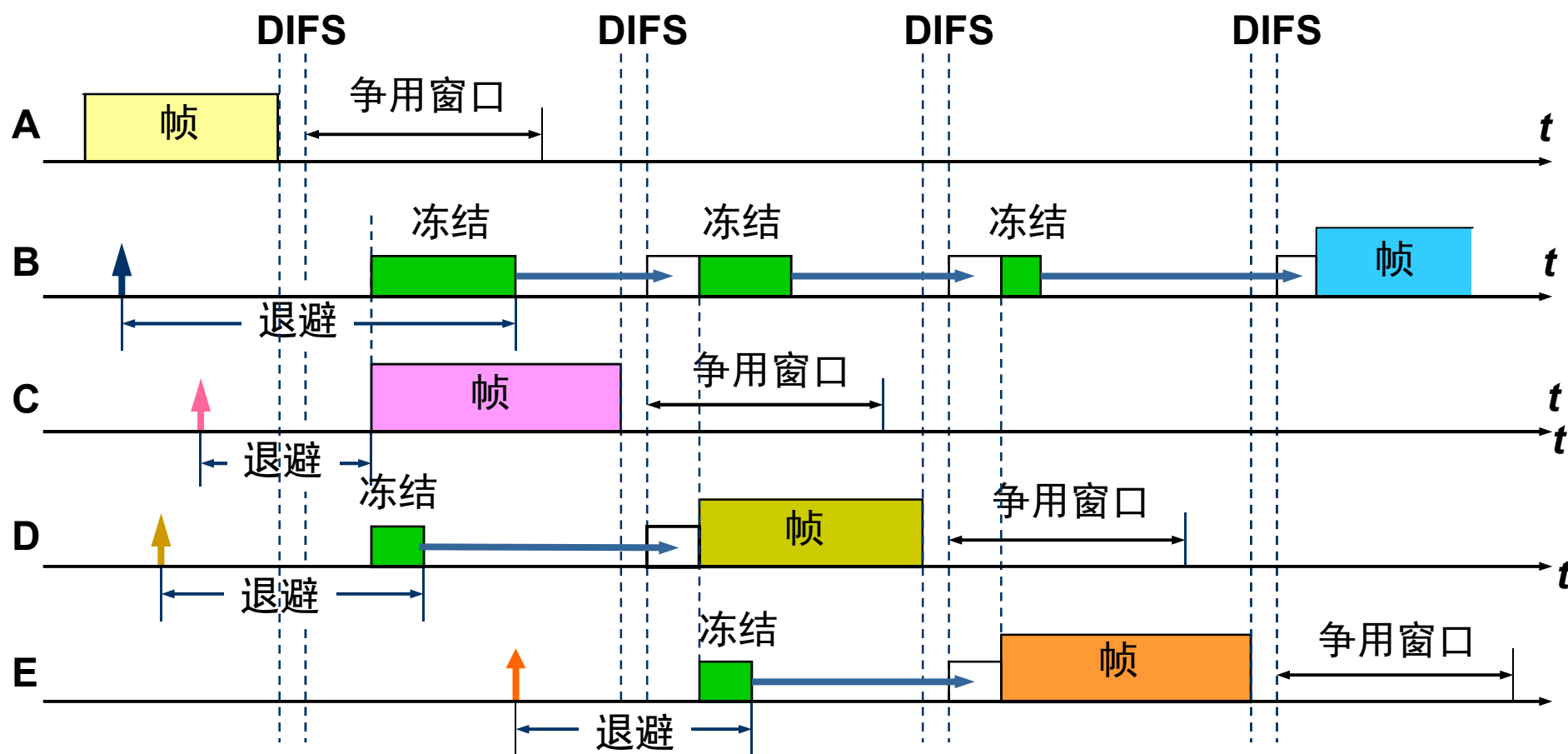
- 若检测到信道空闲，退避计时器继续倒计时。
 - 若检测到信道忙，就冻结退避计时器的剩余时间，重新等待信道变为空闲并再经过时间 **DIFS** 后，从剩余时间开始继续倒计时。如果退避计时器的时间减小到零时，就开始发送整个数据帧。
-

802.11 局域网的MAC 层协议

- 仅在下面的情况下才不使用退避算法：检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧。
 - 除此以外的所有情况，都必须使用退避算法。
即：
 - 在发送第一个帧之前检测到信道处于忙态。
 - 在每一次的重传后。
 - 在每一次的成功发送后再发送下一帧。
-

802.11 局域网的MAC 层协议

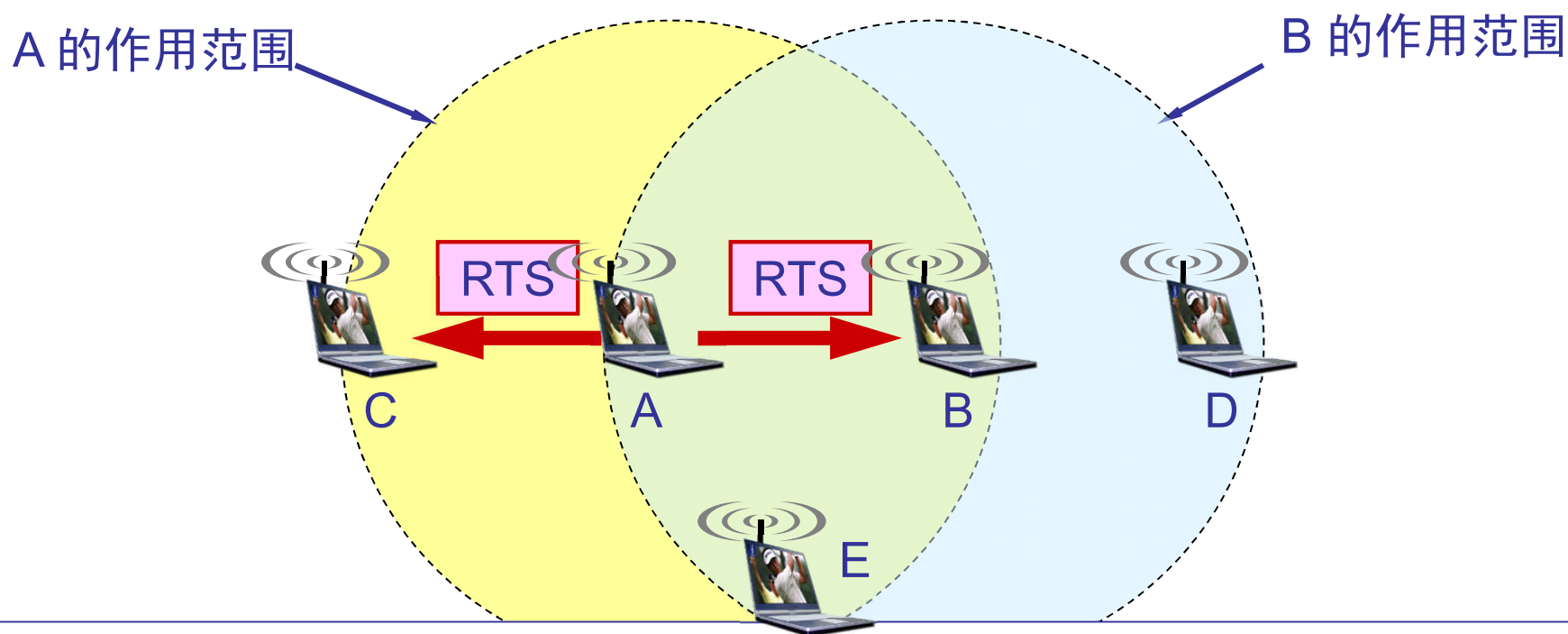
□ 802.11 的退避机制



图例 ——— 冻结剩余的退避时间

802.11 局域网的MAC 层协议

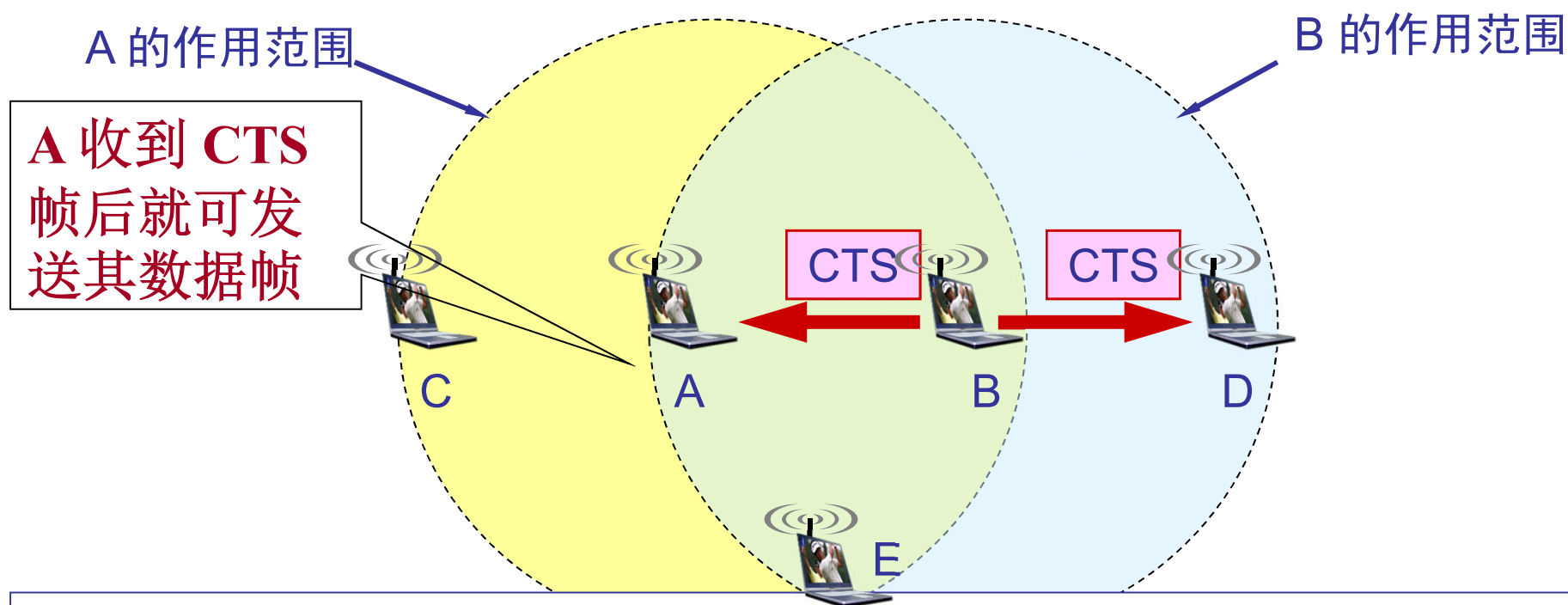
- 2、允许要发送数据的站对信道进行预约。



➤源站 A 在发送数据帧之前先发送一个短的控制帧，叫做请求发送 **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。

802.11 局域网的MAC 层协议

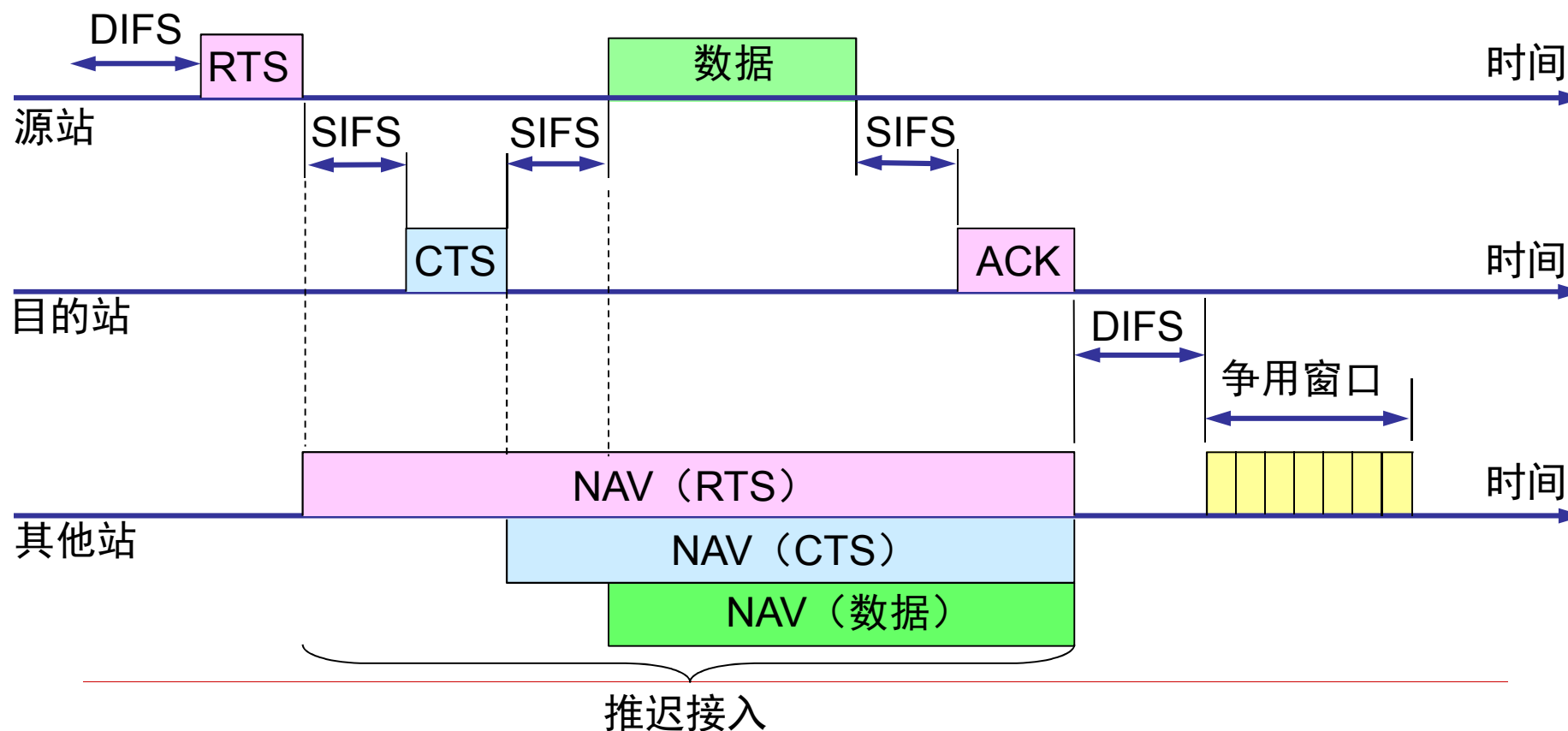
□ 2、允许要发送数据的站对信道进行预约。



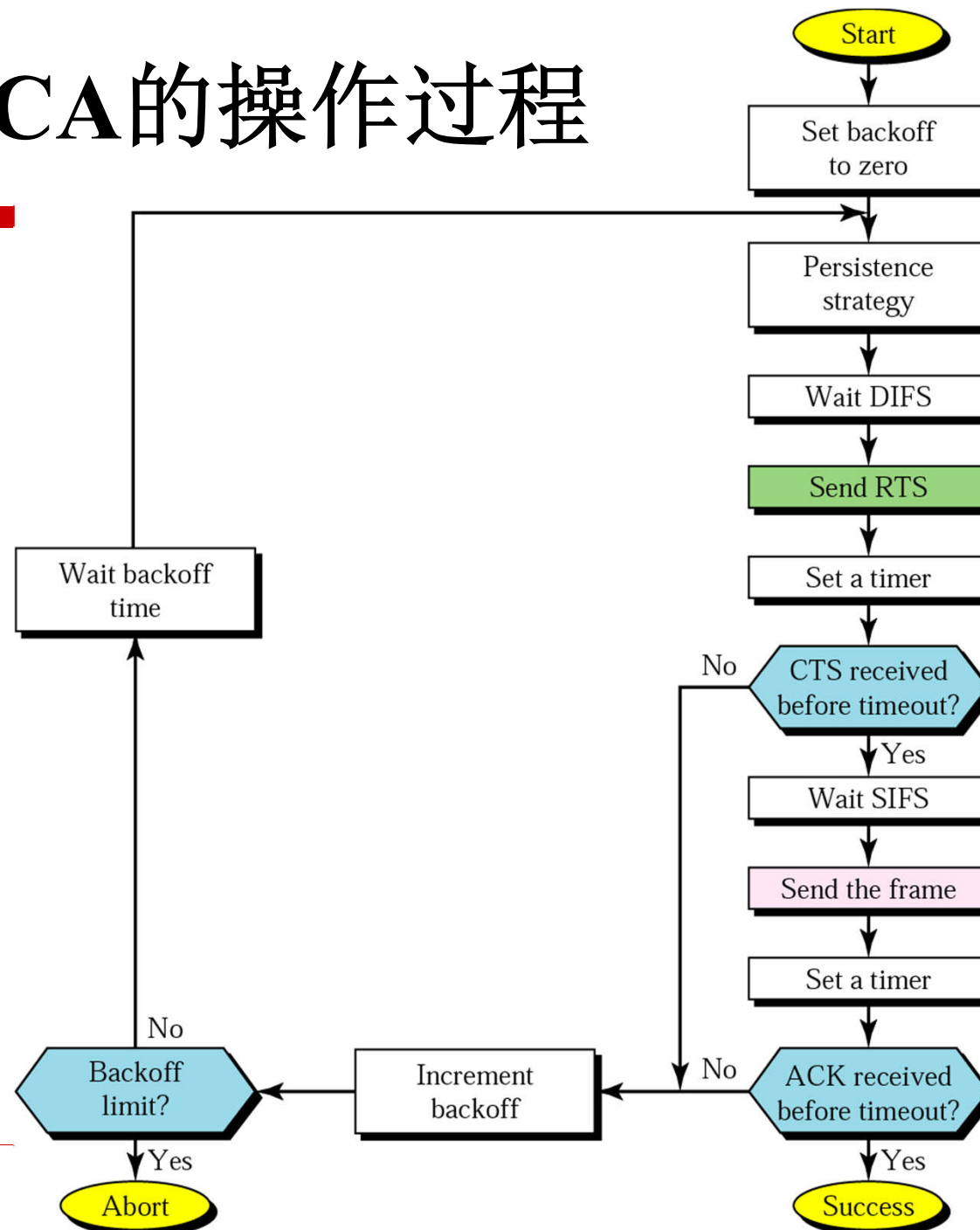
➤ 若媒体空闲,则目的站 **B** 就发送一个响应控制帧,叫做允许发送 **CTS (Clear To Send)**, 包括这次通信所需的持续时间(从 **RTS** 帧中将此持续时间复制到 **CTS** 帧中)。

802.11 局域网的MAC 层协议

➤ 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

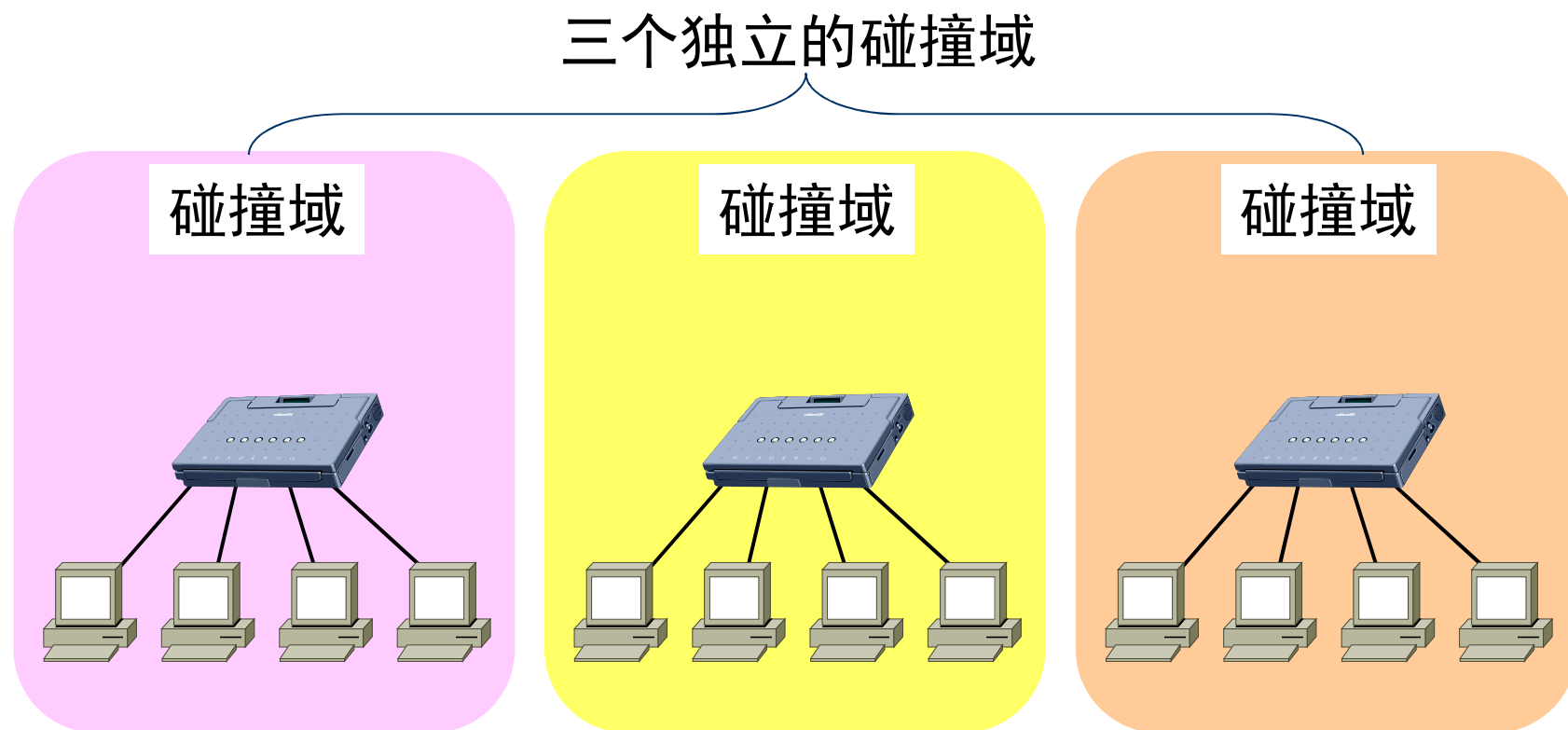
- 6.1 局域网参考模型
- 6.2 以太网
- 6.3 无线局域网
- 6.4 数据链路层互连设备

在物理层扩展以太网

- 使用工作在物理层的设备扩展以太网的地理覆盖范围。
- 设备：
 - 总线网：中继器（转发器）
 - 星形/环形网：集线器
- 特点：
 - 一个网段上的信号不加选择地被复制~~复制~~到另一个网段；

在物理层扩展以太网

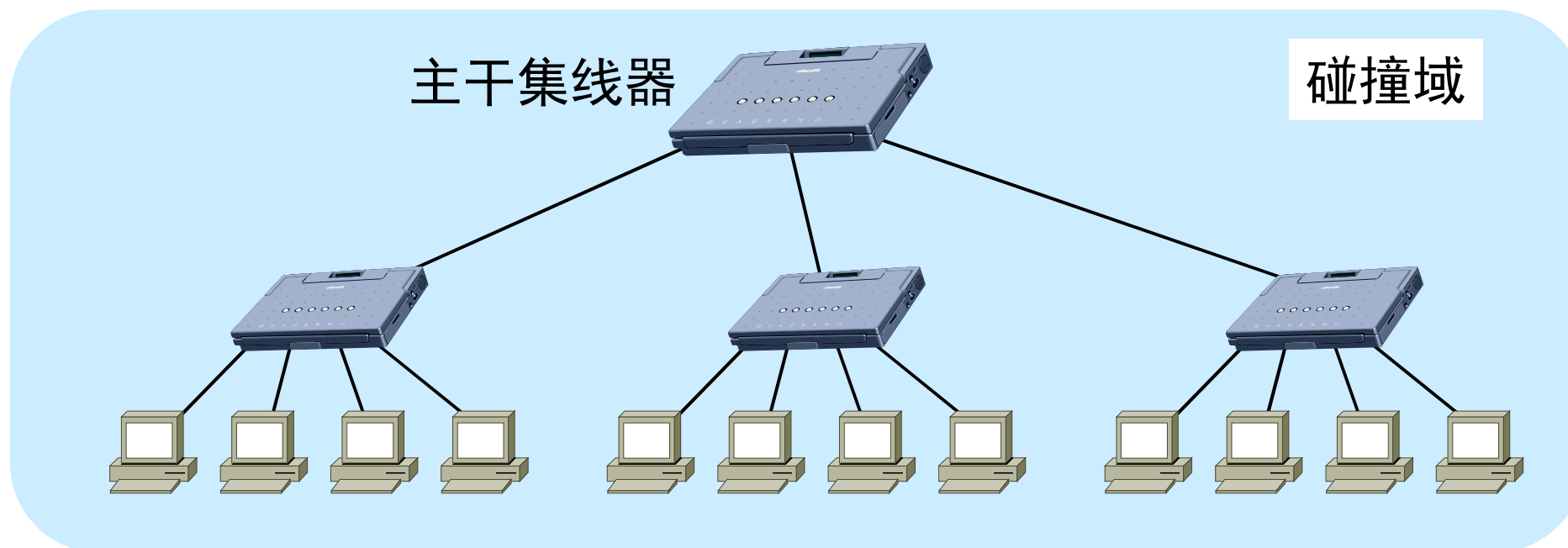
- 用多个集线器可连成更大的局域网



在物理层扩展以太网

- 用多个集线器可连成更大的局域网

一个更大的碰撞域



在物理层扩展以太网

➤ 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

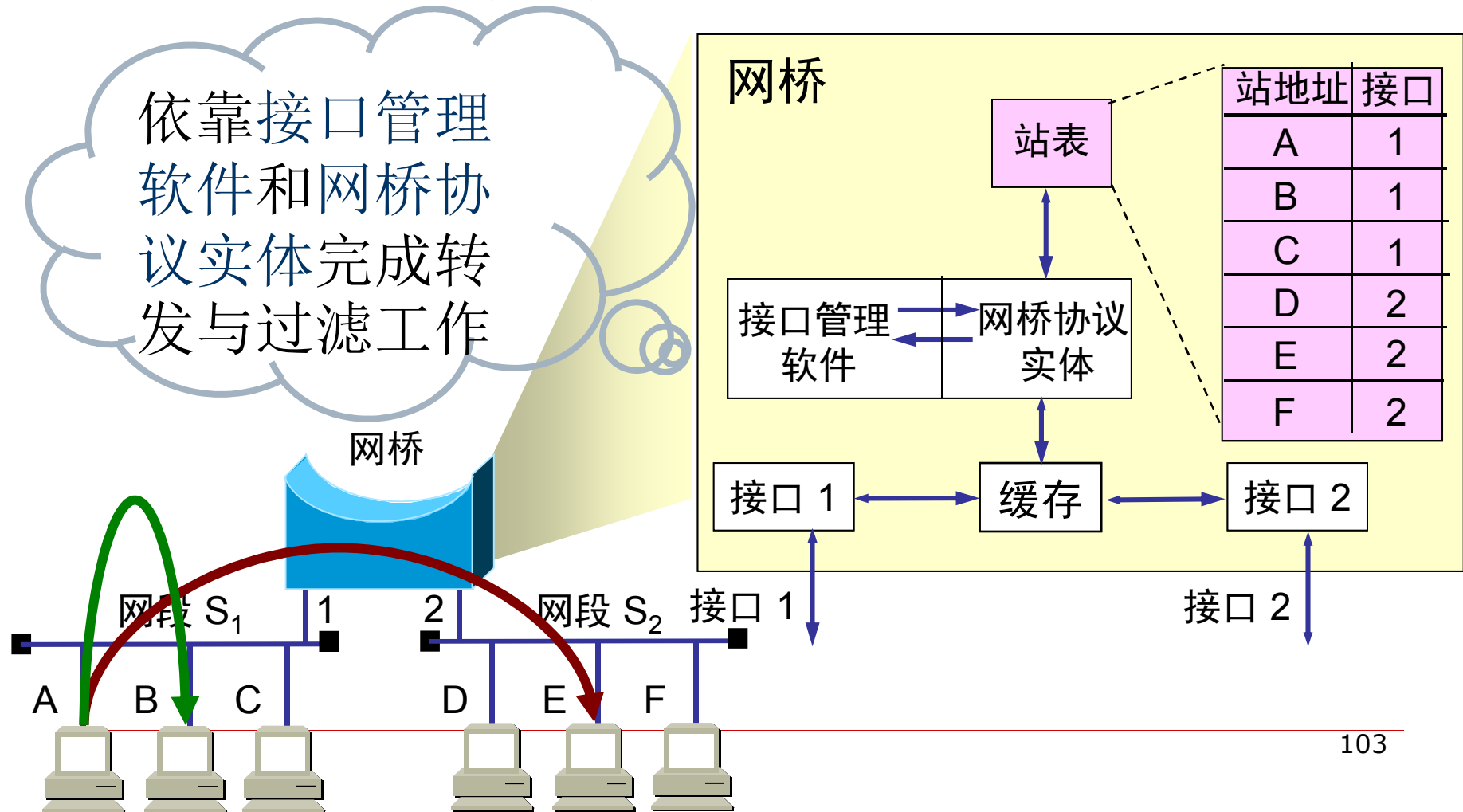
- ✓ 碰撞域增大了，总的吞吐量并未提高。
- ✓ 如果不同的碰撞域使用不同的数据率，就不能用集线器将它们互连起来。

在数据链路层扩展局域网

- 使用网桥在数据链路层扩展局域网
 - ✓ 网桥(bridge)根据 MAC 帧的目的地址对收到的帧进行转发和过滤。
 - ✓ 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，然后再确定将该帧转发到哪一个接口，或者把它过滤。

在数据链路层扩展局域网

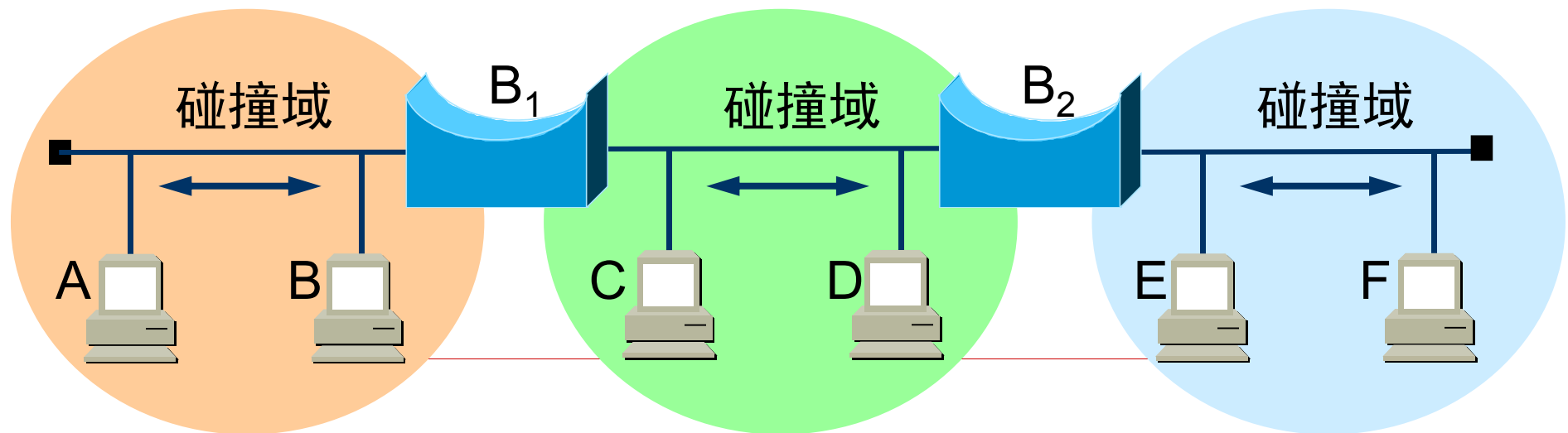
➤ 1. 网桥的内部结构



在数据链路层扩展局域网

➤ 使用网桥的好处

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



在数据链路层扩展局域网

➤ 使用网桥的缺点

- ✓ 要先存储和查找转发表，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。
- ✓ 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。

在数据链路层扩展局域网

- 网桥和集线器（或转发器）不同
 - ✓ 集线器在转发帧时，不对传输媒体进行检测。
 - ✓ 网桥在转发帧之前必须执行 **CSMA/CD** 算法。若在发送过程中出现碰撞，就必须停止发送和进行退避。

在数据链路层扩展局域网

➤ 2. 透明网桥(transparent bridge)

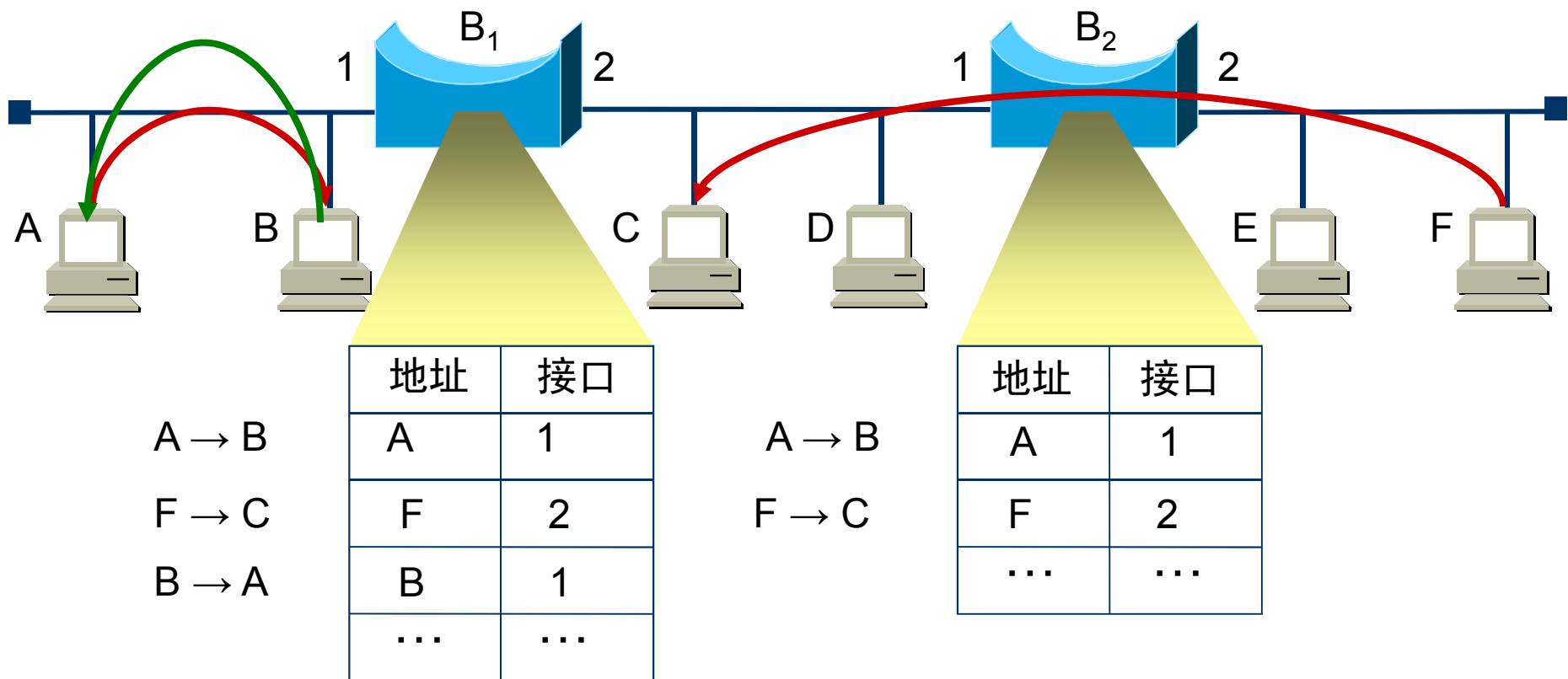
- ✓ “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。
- ✓ 透明网桥是一种即插即用设备，其标准是 **IEEE 802.1D**。
- ✓ 只要把网桥接入网络即可，不需人工配置转发表

在数据链路层扩展局域网

- 网桥处理收到的帧和建立转发表的自学习算法
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，作为转发表中的一个项目。
- ✓ 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。

在数据链路层扩展局域网

➤ 转发表的建立过程举例



在数据链路层扩展局域网

- 网桥在转发表中登记以下三个信息
 - ✓ 在转发表中写入的信息除了地址和接口外，还有帧进入该网桥的时间。
 - ✓ 因为以太网的拓扑可能会发生变化，站点也可能会更换适配器（这就改变了站点的地址）。
 - ✓ 记录帧到达网桥的时间，可以在转发表中只保留网络拓扑的最新状态信息。
 - ✓ 网桥会周期扫描转发表，只要是在一定时间前的都会删除

在数据链路层扩展局域网

➤ 网桥的自学习和转发帧的步骤归纳

- ✓ 网桥收到一帧后先进行自学习。查找转发表中与收到帧的源地址有无相匹配的项目。
 - ◆ 如没有，就在转发表中增加一个项目（源地址、进入的接口和时间）。
 - ◆ 如有，则把原有的项目进行更新。

在数据链路层扩展局域网

➤ 网桥的自学习和转发帧的步骤归纳

- ✓ 转发帧。查找转发表中与收到帧的目的地址有无相匹配的项目。
 - ◆ 如没有，则通过所有其他接口（进入接口除外）进行转发。
 - ◆ 如有，则按给出的接口进行转发。
 - ◆ 若转发表中给出的接口就是该帧进入网桥的接口，则丢弃这个帧。

在数据链路层扩展局域网

➤ 3.源路由(source route)网桥

- ✓ 透明网桥易安装，但网络资源利用不充分。
- ✓ 源路由网桥在发送帧时将详细的路由信息放在帧的首部中。
- ✓ 源站以广播方式向目的站发送一个发现帧，每个发现帧都记录所经过的路由。
- ✓ 发现帧到达目的站时沿各自的路由返回源站。源站在得知后，从所有可能的路由中选择一个最佳路由。凡从该源站向该目的站发送的帧的首部，都携带源站所确定的这一路由信息。

在数据链路层扩展局域网

➤ 4. 多接口网桥——以太网交换机

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

在数据链路层扩展局域网

➤ 以太网交换机的特点

- ✓ 以太网交换机的每个接口都直接与主机相连，并且一般都工作在全双工方式。
- ✓ 主机需要通信时，交换机能同时连通许多对的接口，使每一对相互通信的主机都能像独占通信媒体那样，进行无碰撞地传输数据。两个站通信完毕后即断开连接。
- ✓ 是即插即用设备，帧转发表也需要通过自学习算法建立。以太网交换机由于使用了专用的交换结构芯片，其交换速率就较高。

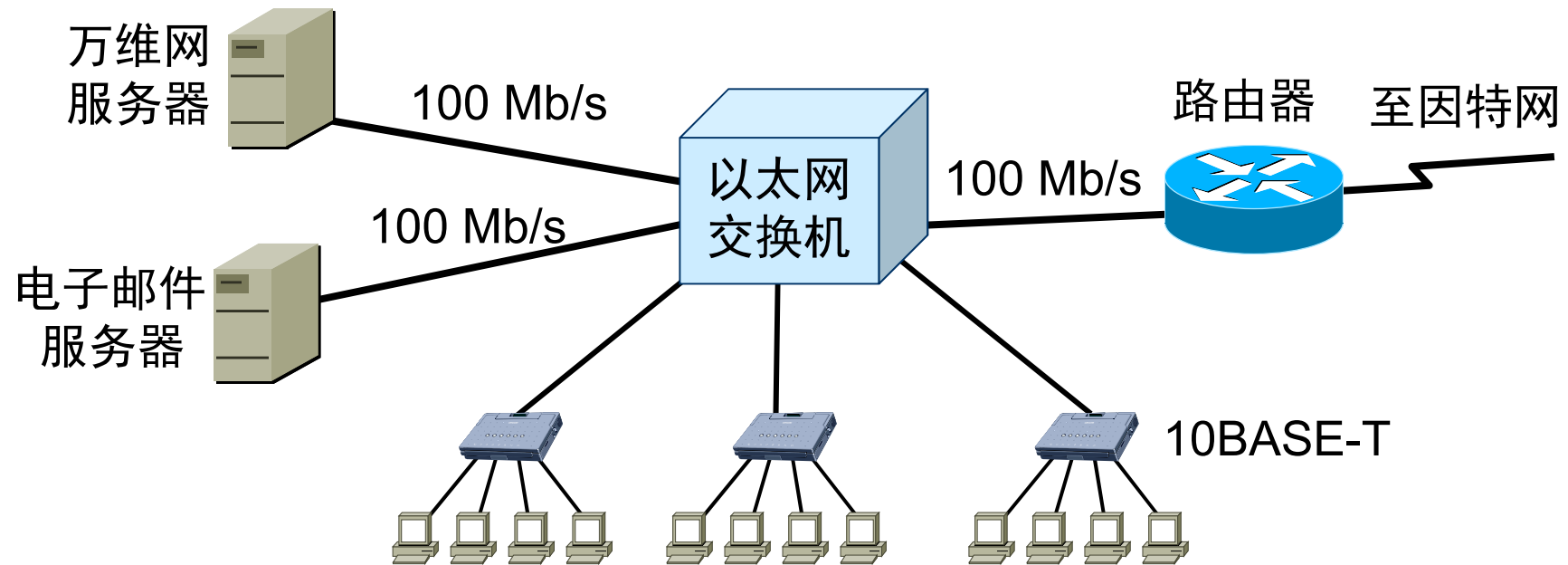
在数据链路层扩展局域网

➤ 独占传输媒体的带宽

- ✓ 对于普通 **10 Mb/s** 的共享式以太网，若共有 N 个用户，则每个用户占有的平均带宽只有总带宽(**10 Mb/s**)的 N 分之一。
- ✓ 使用以太网交换机时，虽然在每个接口到主机的带宽还是 **10 Mb/s**，但由于一个用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此对于拥有 N 对接口的交换机的总容量为 $N \times 10 \text{ Mb/s}$ 。这正是交换机的最大优点。

在数据链路层扩展局域网

➤ 用以太网交换机扩展局域网



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、转发表自学习算法
- 高速局域网技术：快速以太网、千兆/万兆以太网。
- 无线局域网： CSMA/CA、隐蔽站/暴漏站

补充作业

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

