无线网络

林海

Lin.hai@whu.edu.cn

第 9 章　无线网络和移动网络

- 9.1　无线局域网 WLAN
- 9.2　无线个人区域网 WPAN
- 9.3　无线城域网 WMAN

9.1 无线局域网 WLAN

- 9.1.1 无线局域网的组成
- 9.1.2 802.11 局域网的物理层
- 9.1.3 802.11 局域网的 MAC 层协议
- 9.1.4 802.11 局域网的 MAC 帧

9.1.1 无线局域网的组成

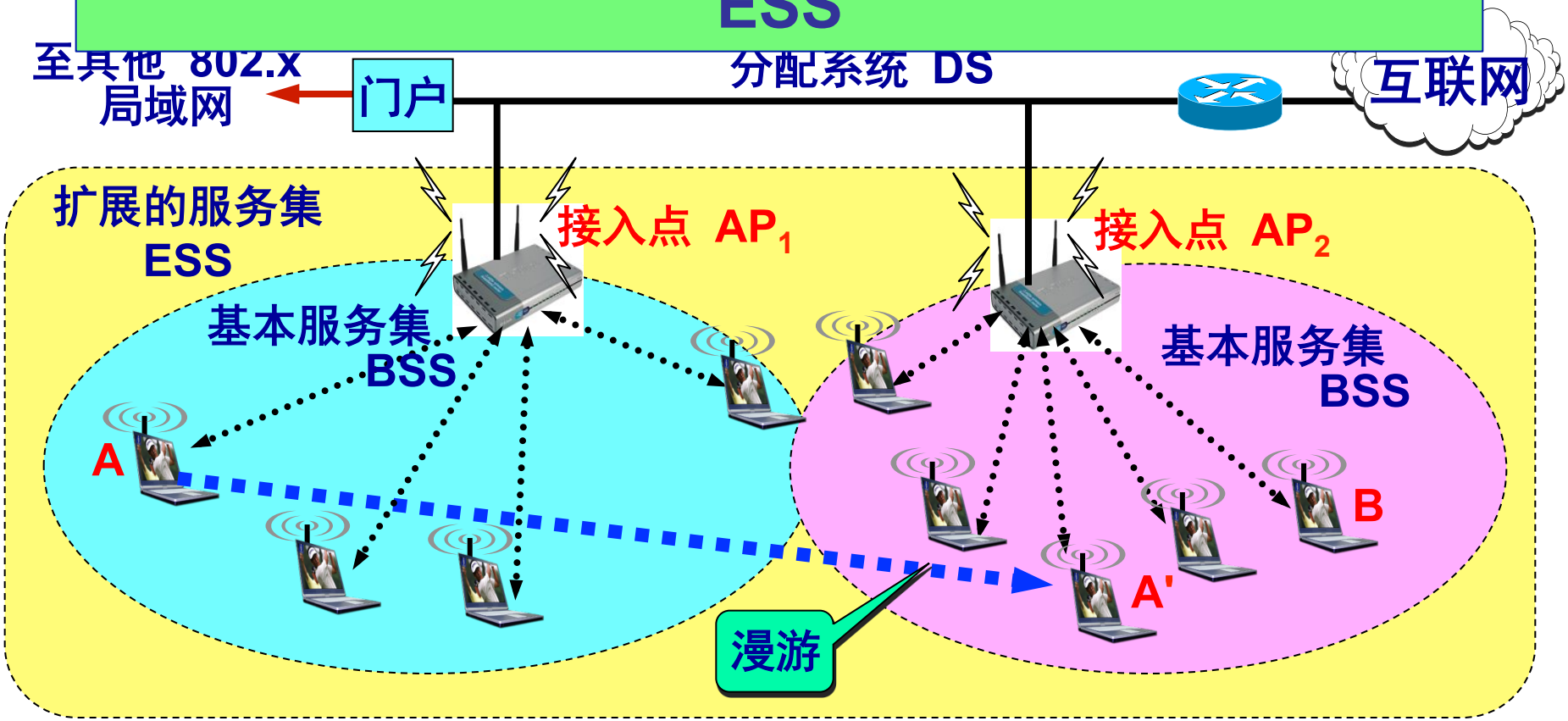
- 无线局域网 WLAN (Wireless Local Area Network) 可分为两大类：
  - 有固定基础设施的 WLAN
  - 无固定基础设施的 WLAN
- 所谓“固定基础设施”是指预先建立起来的、能够覆盖一定地理范围的一批固定基站。

1. IEEE 802.11

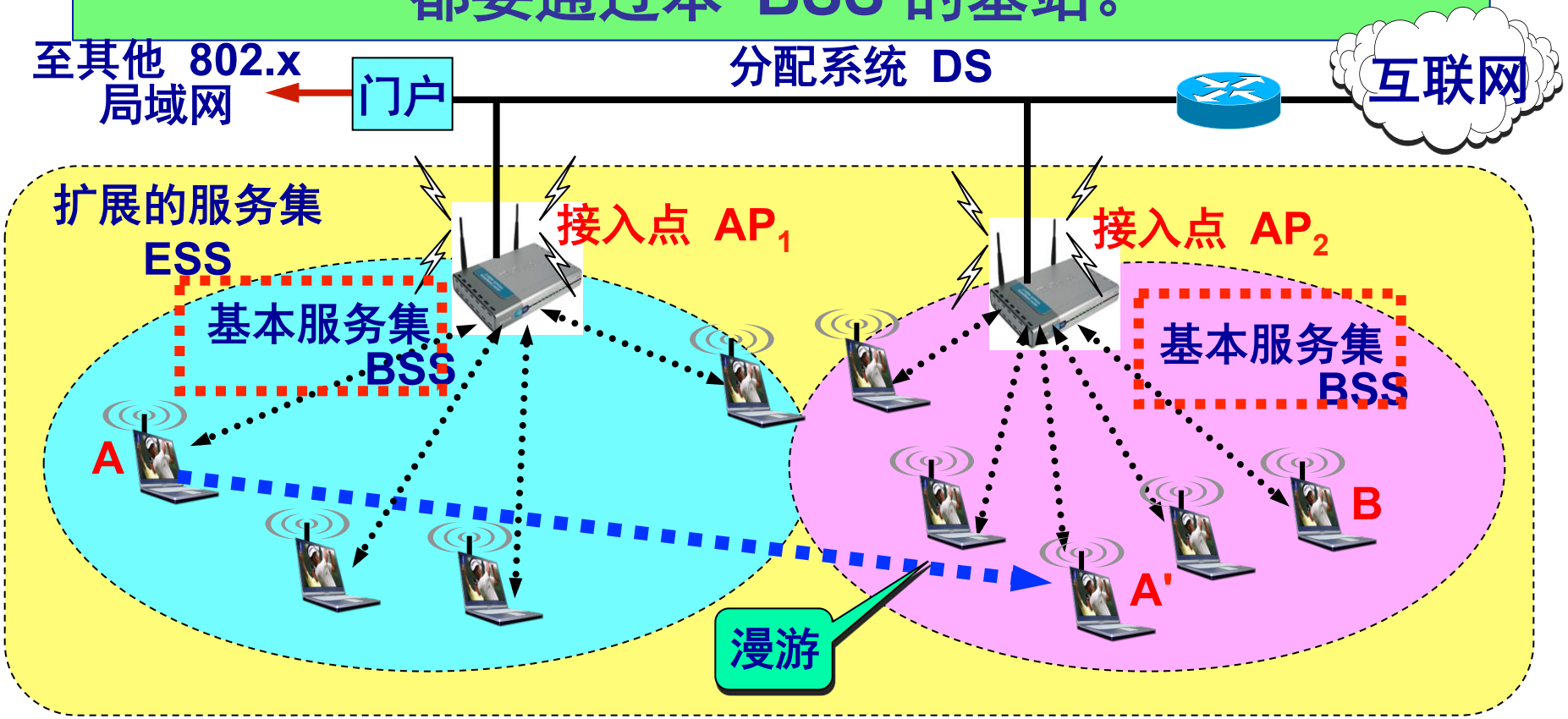
- IEEE 802.11 是一个有固定基础设施的无线局域网的国际标准。
- IEEE 802.11 是个相当复杂的标准。但简单地说，802.11 就是无线以太网的标准：
  - 它使用星形拓扑，其中心叫做接入点 AP (Access Point)
  - 在MAC层使用 CSMA/CA 协议
- 凡使用 802.11 系列协议的局域网又称为 Wi-Fi (Wireless-Fidelity，意思是“无线保真度”。

1. IEEE 802.11

IEEE 802.11 的基本服务集 BSS 和扩展服务集 ESS

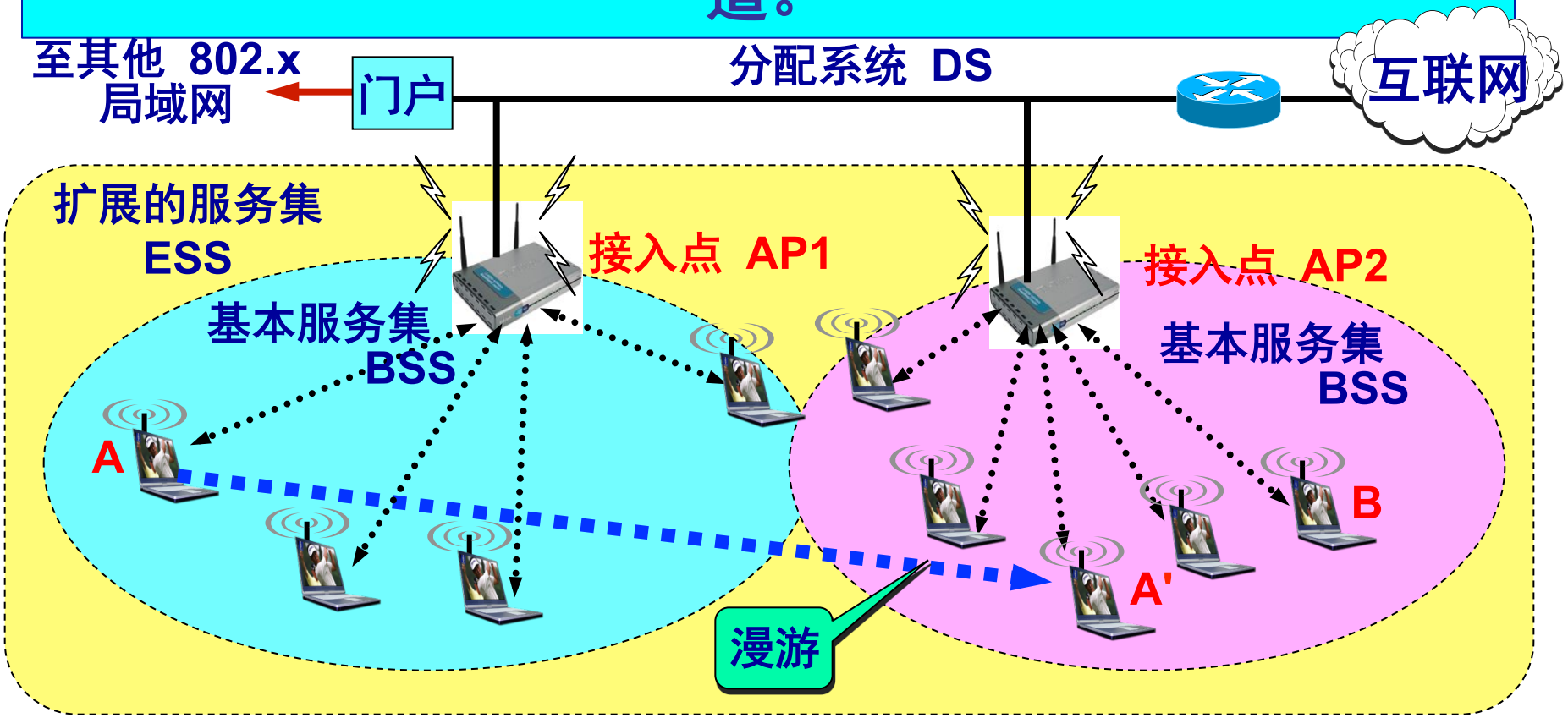


一个基本服务集 BSS 包括一个基站和若干个移动站，
所有的站在本 BSS 以内都可以直接通信，
但在和本 BSS 以外的站通信时 ，
都要通过本 BSS 的基站。

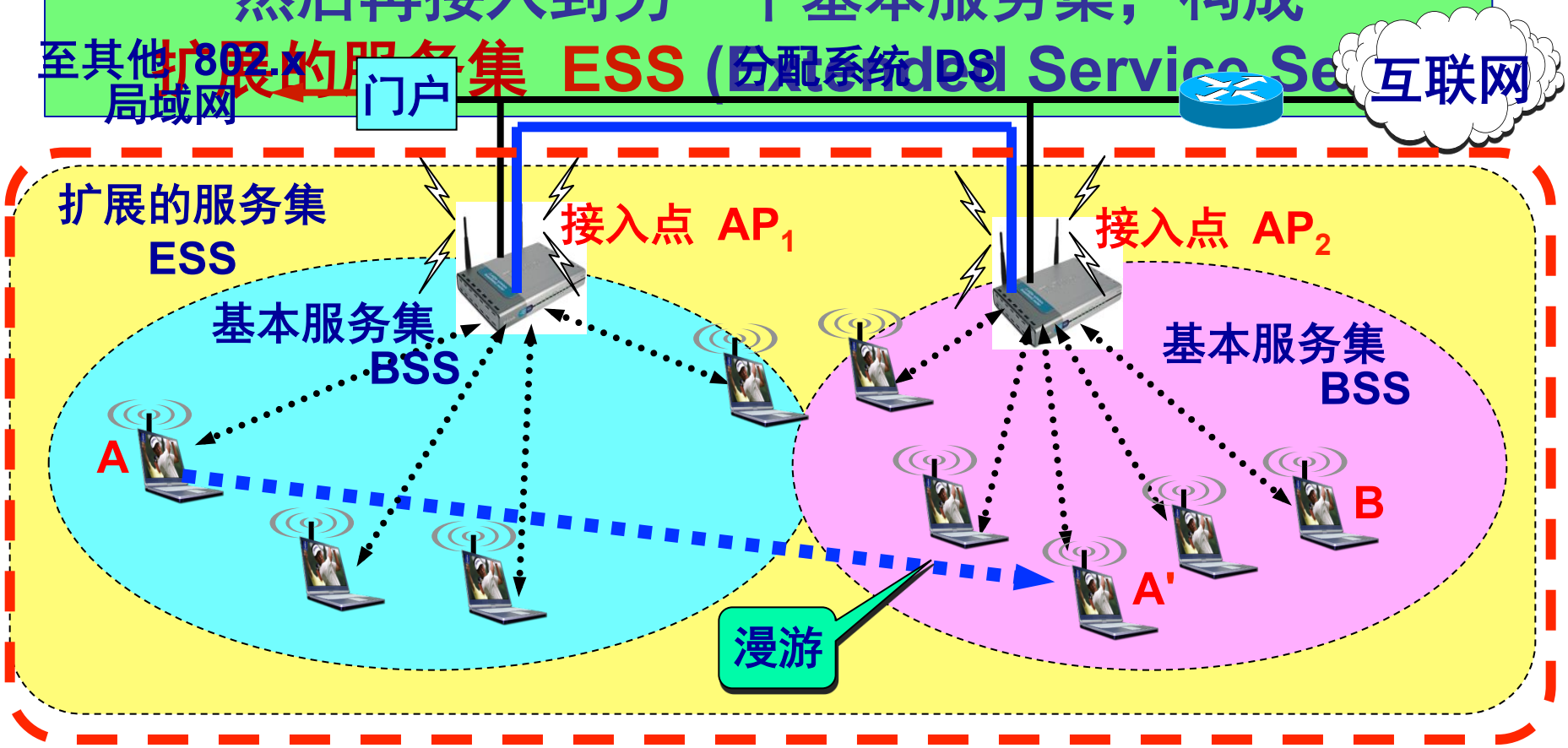


基本服务集内的基站叫做接入点 AP (Access Point)

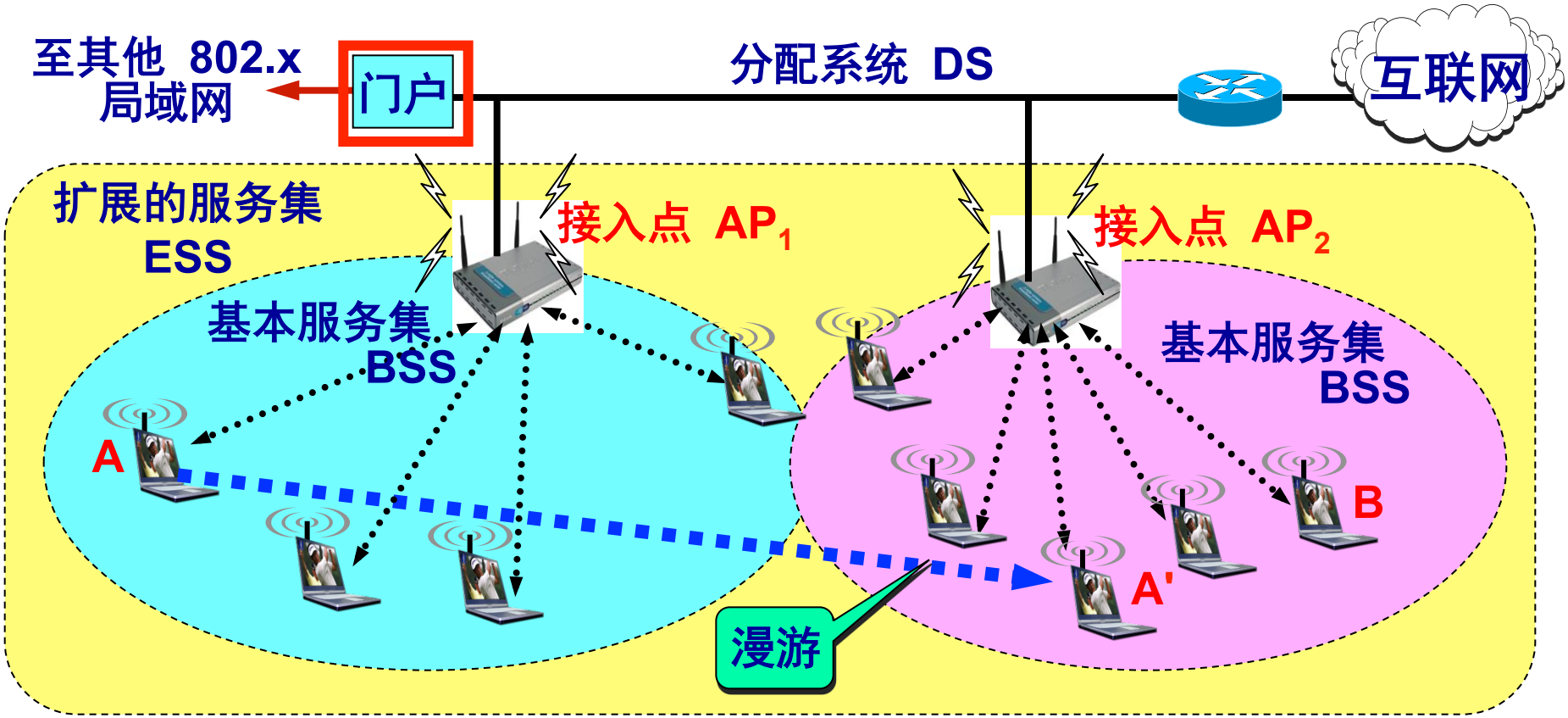
当网络管理员安装 AP 时，必须为该 AP 分配一个不超过 32 字节的服务集标识符 SSID 和一个信道。



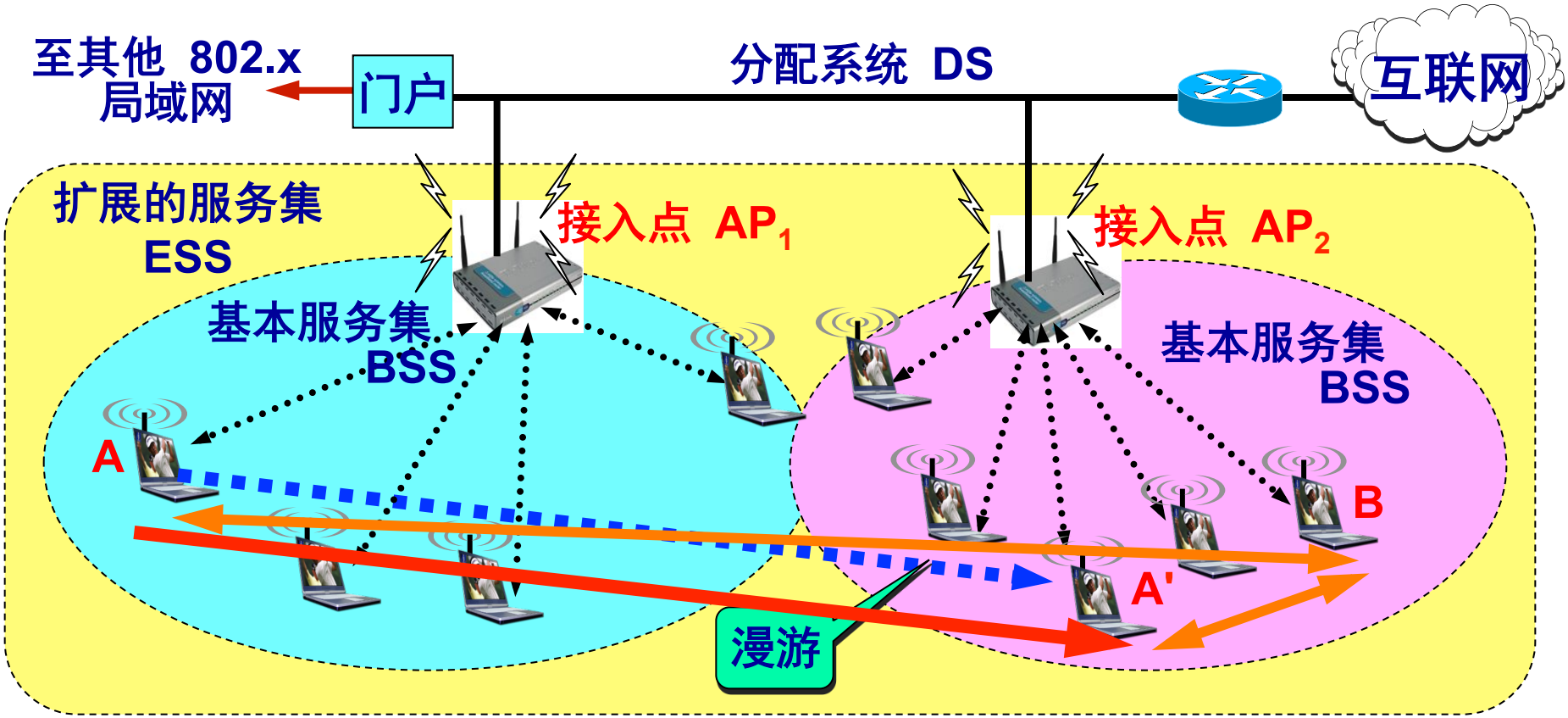
一个基本服务集可以是孤立的，也可通过接入点 AP
连接到一个主干分配系统 DS (Distribution System)，
然后再接入到另一个基本服务集，构成
扩展的服务集 ESS (Extended Service Set)



ESS 还可通过叫做门户 (portal) 为无线用户提供到非 802.11 无线局域网（例如，到有线连接的互联网）的接入。门户的作用就相当于一个网桥。



移动站 A 从某一个基本服务集**漫游**到
另一个基本服务集（到 A′ 的位置），
仍可保持与另一个移动站 B 进行通信。



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 (association)。
- 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。

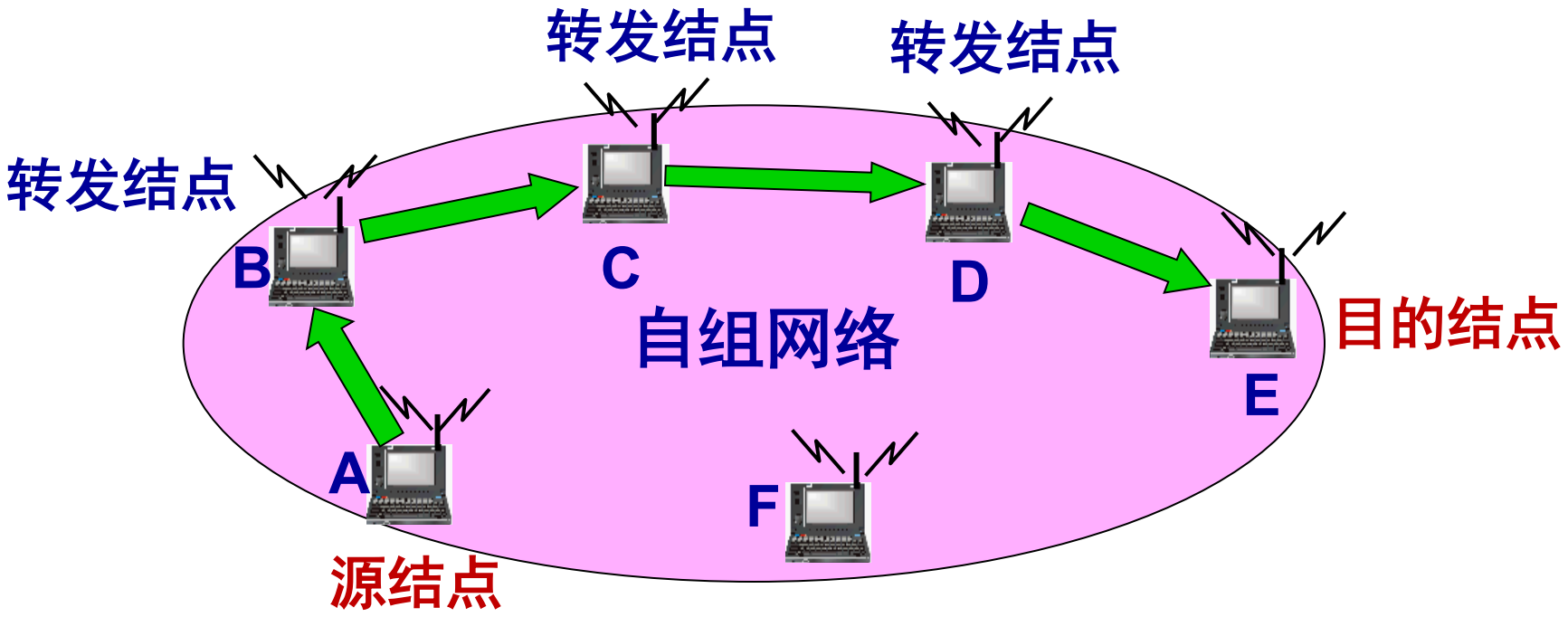
移动站与 AP 建立关联的方法

- 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)。

2. 移动自组网络

- 移动自组网络又称为自组网络 (ad hoc network)。
- 自组网络是没有固定基础设施（即没有 AP）的无线局域网。
- 这种网络是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。
- 自组网络的服务范围通常是受限的，而且一般也不和外界的其他网络相连接。
- 移动自组网络也就是移动分组无线网络。

2. 移动自组网络



三个主要问题：路由选择协议，多播，安全。

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，

无线传感器网络 WSN

- 无线传感器网络 WSN (Wireless Sensor Network) 是由大量传感器结点通过无线通信技术构成的自组网络。
- 无线传感器网络的应用是进行各种数据的采集、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须保持低功耗，以节省电池的消耗。
- 由于无线传感结点的存储容量受限，因此对协议栈的大小有严格的限制。
- 无线传感器网络还对网络安全性、结点自动配置、网络动态重组等方面有一定的要求。

无线传感器网络主要的应用领域

- 无线传感器网络主要的应用领域就是组成各种的物联网 IoT (Internet of Things)，例如：
  - 环境监测与保护（如洪水预报、动物栖息的监控）；
  - 战争中对敌情的侦查和对兵力、装备、物资等的监控；
  - 医疗中对病房的监测和对患者的护理；
  - 在危险的工业环境（如矿井、核电站等）中的安全监测；
  - 城市交通管理、建筑内的温度/照明/安全控制等。

移动自组网络不同于移动 IP

- 移动 IP 技术使漫游的主机可以用多种方式连接到互联网。
- 移动 IP 的核心网络功能仍然是基于在固定互联网中一直在使用的各种路由选择协议。
- 移动自组网络是将移动性扩展到无线领域中的自治系统，它具有自己特定的路由选择协议，并且可以不和互联网相连。

9.1.2 802.11 局域网的物理层

- 802.11 标准中物理层相当复杂。根据物理层的不同（如工作频段、数据率、调制方法等），对应的标准也不同。
- 最早流行的无线局域网是 802.11b，802.11a 和802.11g。2009年颁布了标准 802.11n
- 802.11 的物理层有以下几种实现方法：
  - 直接序列扩频 DSSS
  - 正交频分复用 OFDM
  - 跳频扩频 FHSS （已很少用）
  - 红外线 IR （已很少用）

几种常用的 802.11 无线局域网

标准	频段	数据速率	物理层	优缺点
802.11b (1999年)	2.4 GHz	最高11 Mbit/s	扩频	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍。
802.11a (1999年)	5 GHz	最高54 Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，价格最高，信号传播距离较短，且易受阻碍。
802.11g (2003年)	2.4 GHz	最高54 Mbit/s	OFDM	最高数据率较高，支持更多用户同时上网，信号传播距离最远，且不易受阻碍，价格比802.11b贵。
802.11n (2009年)	2.4 / 5 GHz	最高 600 Mbit /s	MIMO OFDM	使用多个发射和接收天线达到更高的数据传输率。当使用双倍带宽(40 MHz)时速率可达600 Mbit/s。

9.1.3 802.11 局域网的 MAC 层协议

1. CSMA/CA 协议

- 无线局域网不能简单地搬用 CSMA/CD 协议。这里主要有两个原因：
  - “碰撞检测”要求一个站点在发送本站数据的同时，还必须不间断地检测信道，但接收到的信号强度往往会远远小于发送信号的强度，在无线局域网的设备中要实现这种功能就花费过大。
  - 即使能够实现碰撞检测的功能，并且在发送数据时检测到信道是空闲的时候，在接收端仍然有可能发生碰撞。

CSMA/CA 协议的原理

- 欲发送数据的站先检测信道。在 802.11 标准中规定了在物理层的空中接口进行物理层的载波监听。
- 通过收到的相对信号强度是否超过一定的门限数值就可判定是否有其他的移动站在信道上发送数据。
- 当源站发送它的第一个 MAC 帧时，若检测到信道空闲，则在等待一段时间(DIFS)后就可发送。

为什么信道空闲还要再等待

- 这是考虑到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。

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间隔时间，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，为了避免几个站同时发送数据（一旦发送就要把一帧发送完，不能中途停止），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。

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 $\{0, 1, \ldots, 2^{2+i}-1\}$ 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。
- 当时隙编号达到 255 时（这对应于第 6 次退避）就不再增加了。
- 这里决定退避时间的变量 i 称为退避变量。

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。
- 这可能发生两种情况：
  - 若检测到信道空闲，退避计时器就继续倒计时。
  - 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。

冻结退避计时器剩余时间的做法是为了使协议对所有站点更加公平。

退避算法的使用情况

- 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：
  - 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。

应答机制

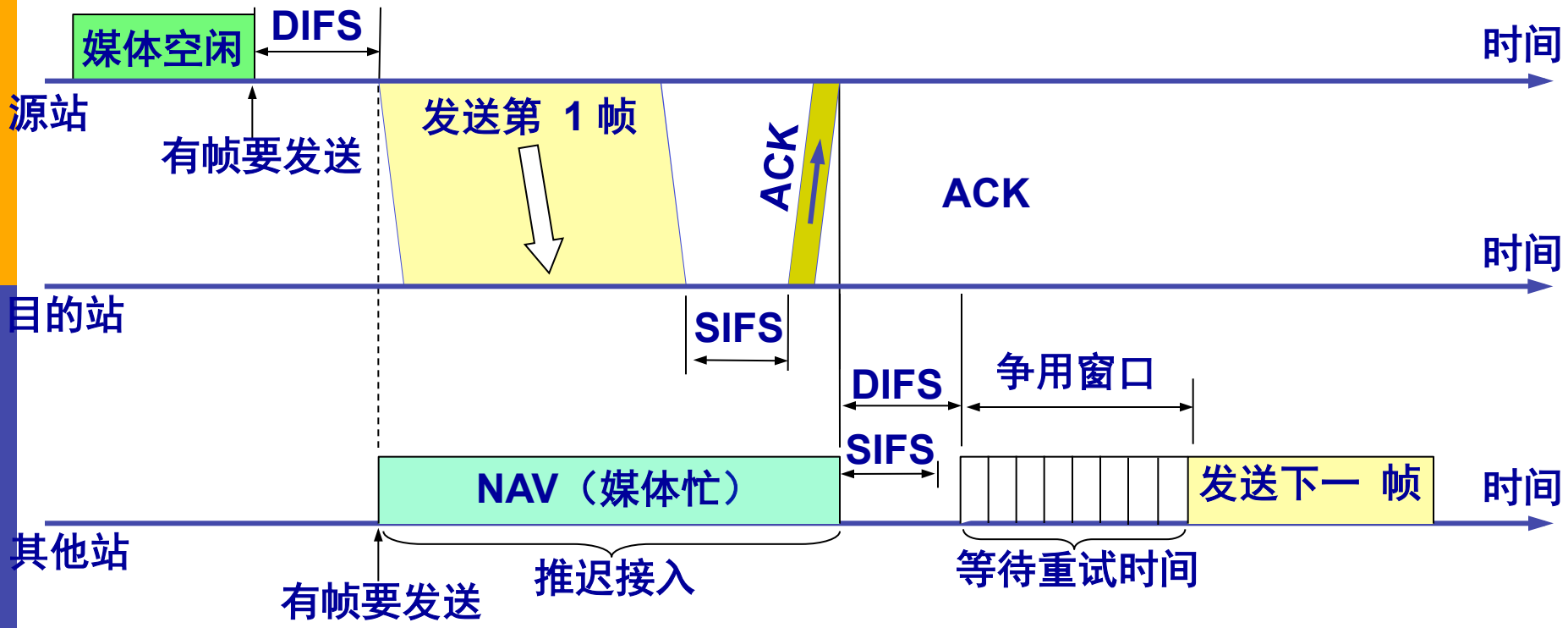
- 以太网没有应答机制（ACK）
- 但无线传输不可靠，需要ACK机制
- 停等式
  - 下一个数据要等到收到前一个数据的ACK才能发送
- 应答机制保证了数据产生的可靠性，那么不同数据的优先级又是如何保证的？
  - 数据的优先级高还是ACK的优先级高？

优先级：帧间间隔 IFS

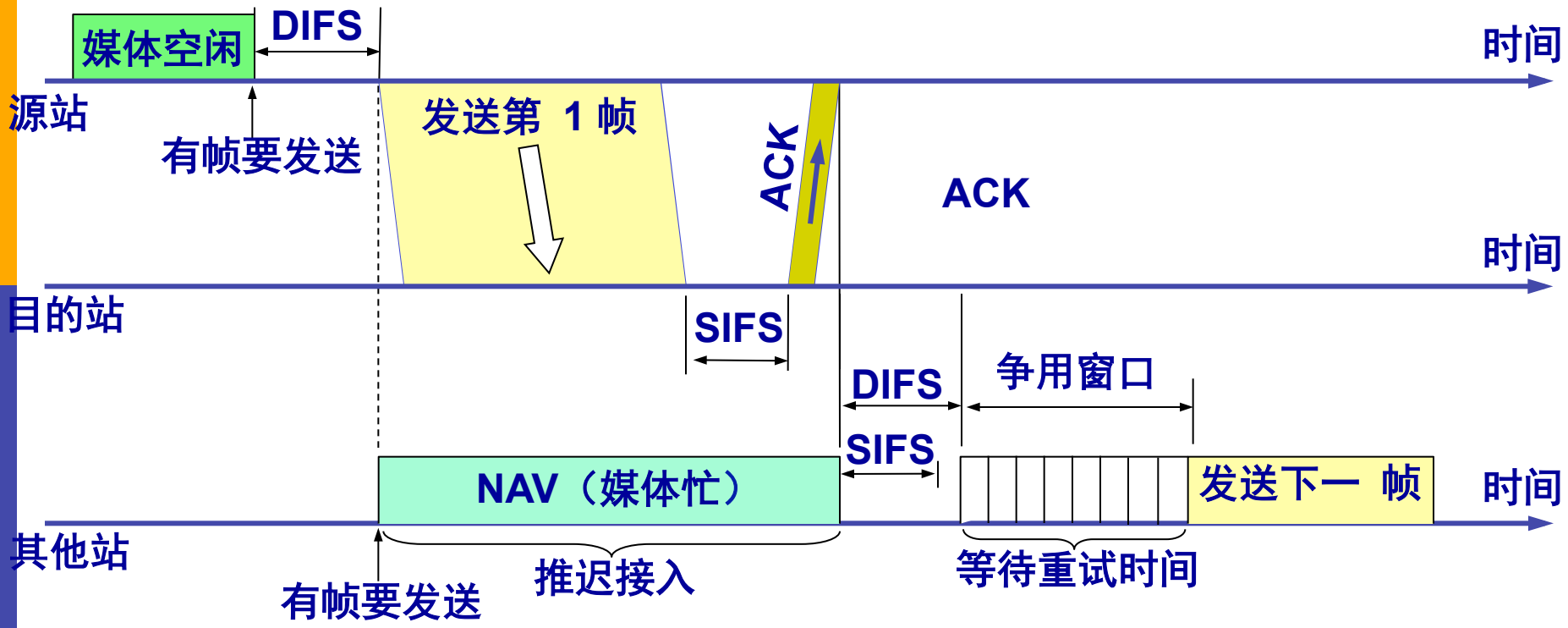
- 所有的站在完成发送后，必须再等待一段很短的时间（继续监听）才能发送下一帧。这段时间的通称是帧间间隔 IFS (InterFrame Space)。
- 帧间间隔长度取决于该站欲发送的帧的类型。高优先级帧需要等待的时间较短，因此可优先获得发送权。
- 若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态，因而低优先级帧就只能再推迟发送了。这样就减少了发生碰撞的机会。

SIFS，即短 (Short) 帧间间隔，长度为 28 μs，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。

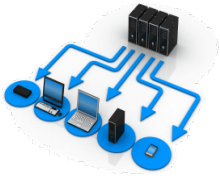
使用 SIFS 的帧类型有：ACK 帧、CTS 帧、由过长的 MAC 帧分片后的数据帧，以及所有回答 AP 探询的帧和在 PCF 方式中接入点 AP 发送出的任何帧。

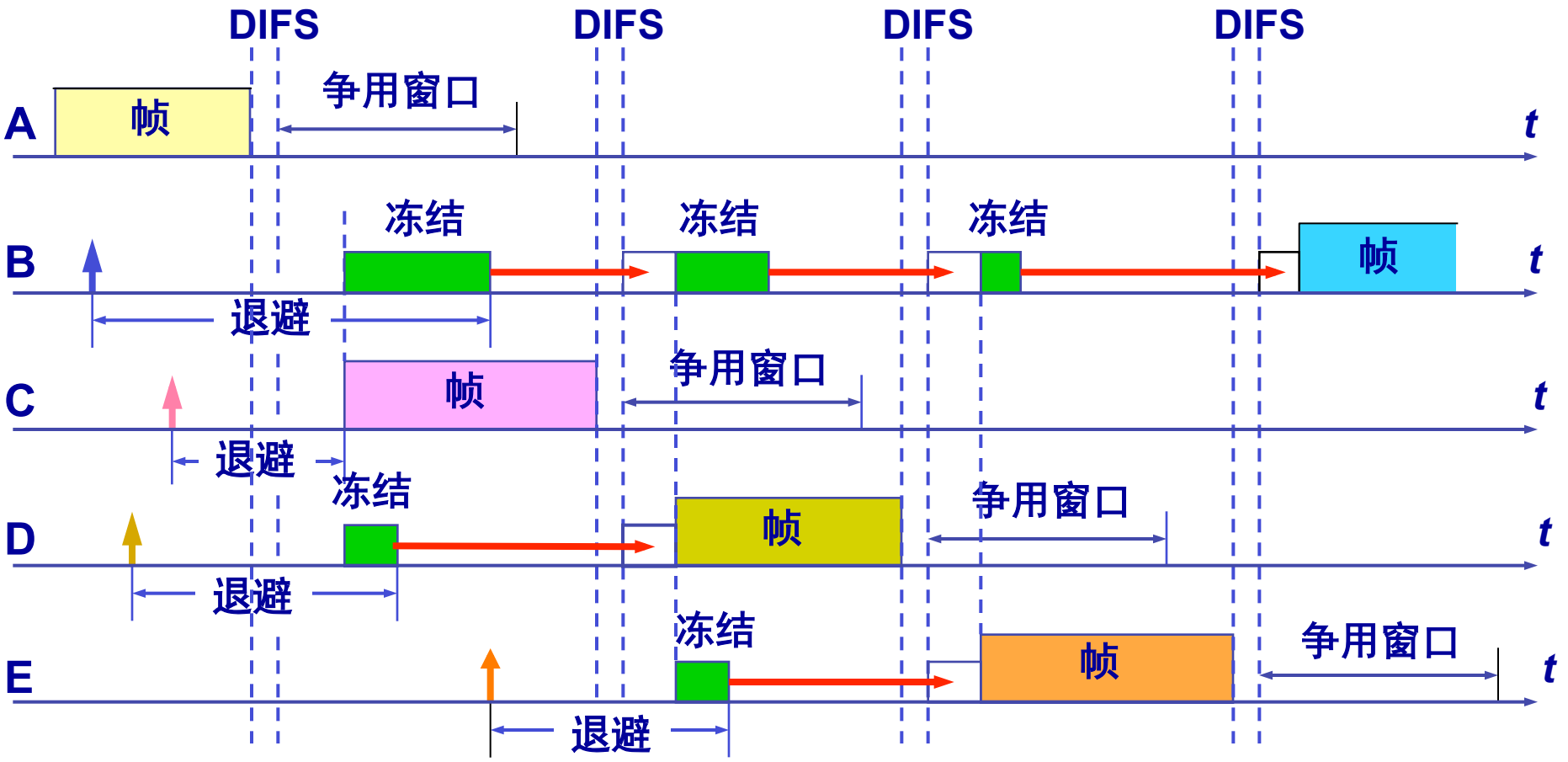


DIFS，即分布协调功能帧间间隔，它比 SIFS 的帧间间隔要长得多，长度为 128 μs。在 DCF 方式中，DIFS 用来发送数据帧和管理帧。



802.11 的退避机制+IFS





图例 ——— 检测到信道忙，冻结剩余的退避时间

打算发送数据

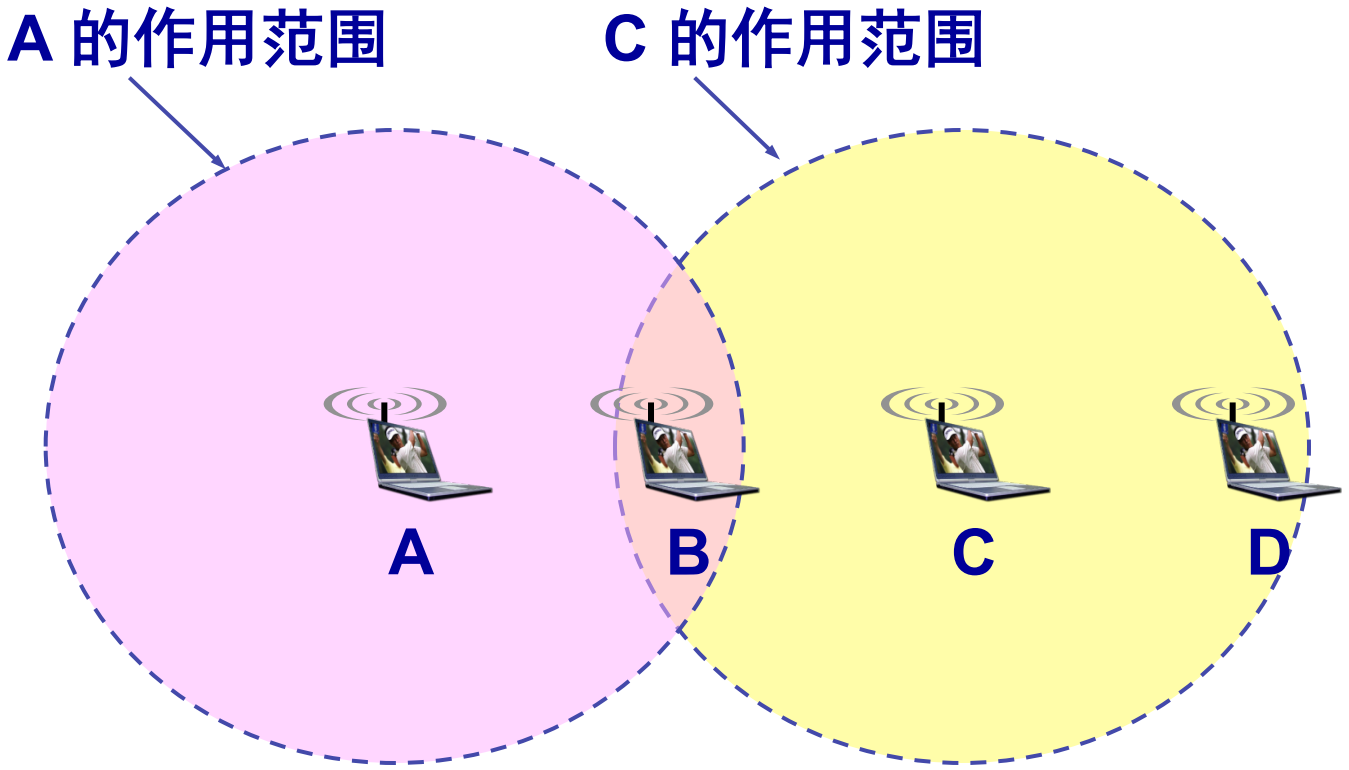
CSMA/CA 算法归纳

- (1) 若站点最初有数据要发送（而不是发送不成功再进行重传），且检测到信道空闲，在等待时间 DIFS 后，就发送整个数据帧。
- (2) 否则，站点执行 CSMA/CA 协议的退避算法。一旦检测到信道忙，就冻结退避计时器。只要信道空闲，退避计时器就进行倒计时。
- (3) 当退避计时器时间减少到零时（这时信道只可能是空闲的），站点就发送整个的帧并等待确认。
- (4) 发送站若收到确认，就知道已发送的帧被目的站正确收到了。这时如果要发送第二帧，就要从上面的步骤 (2) 开始，执行 CSMA/CA 协议的退避算法，随机选定一段退避时间。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（再次使用 CSMA/CA 协议争用接入信道），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。

隐藏和暴露问题

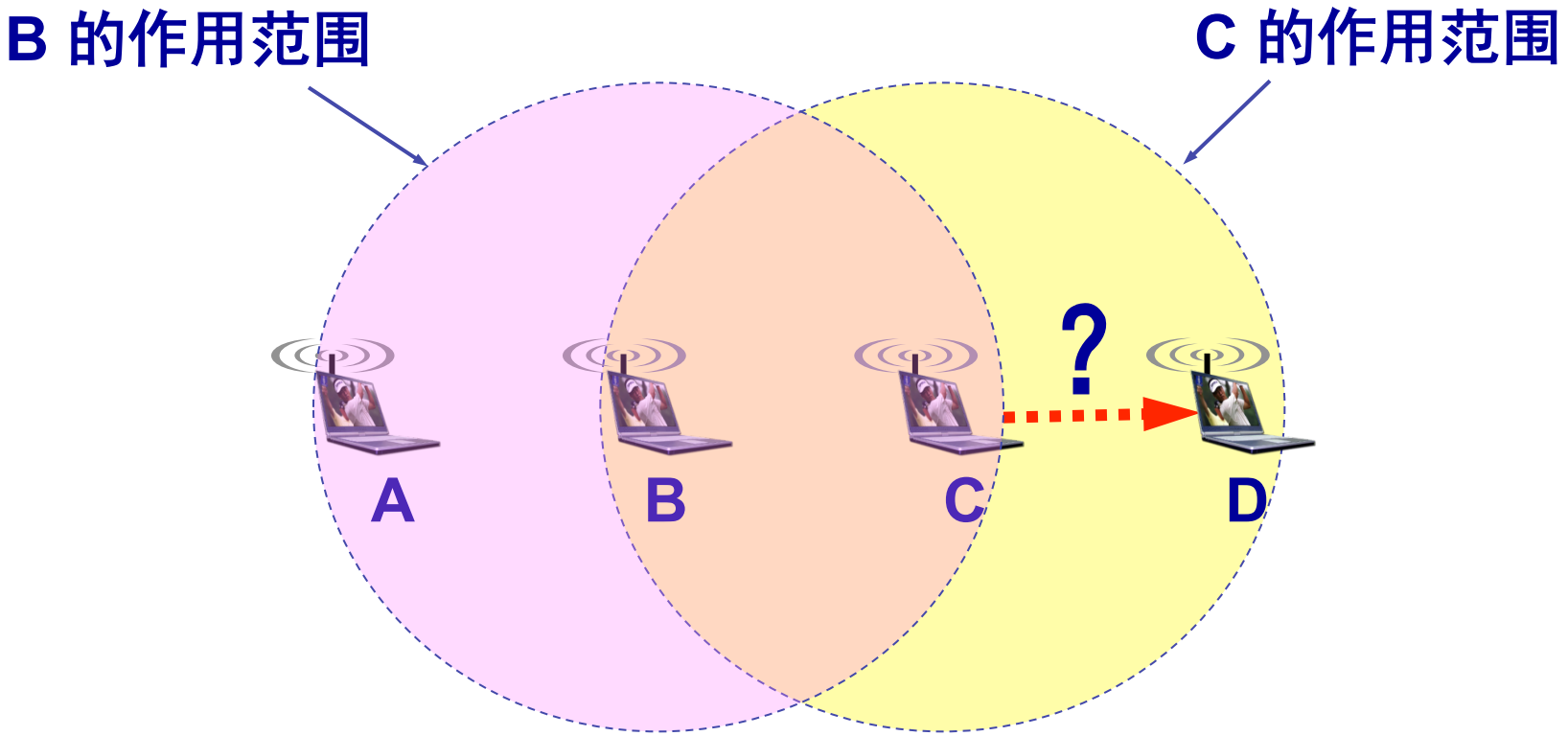
- 有了CSMA/CA是不是就万事大吉了？
  - 隐蔽站问题
  - 暴露站问题

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)



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。

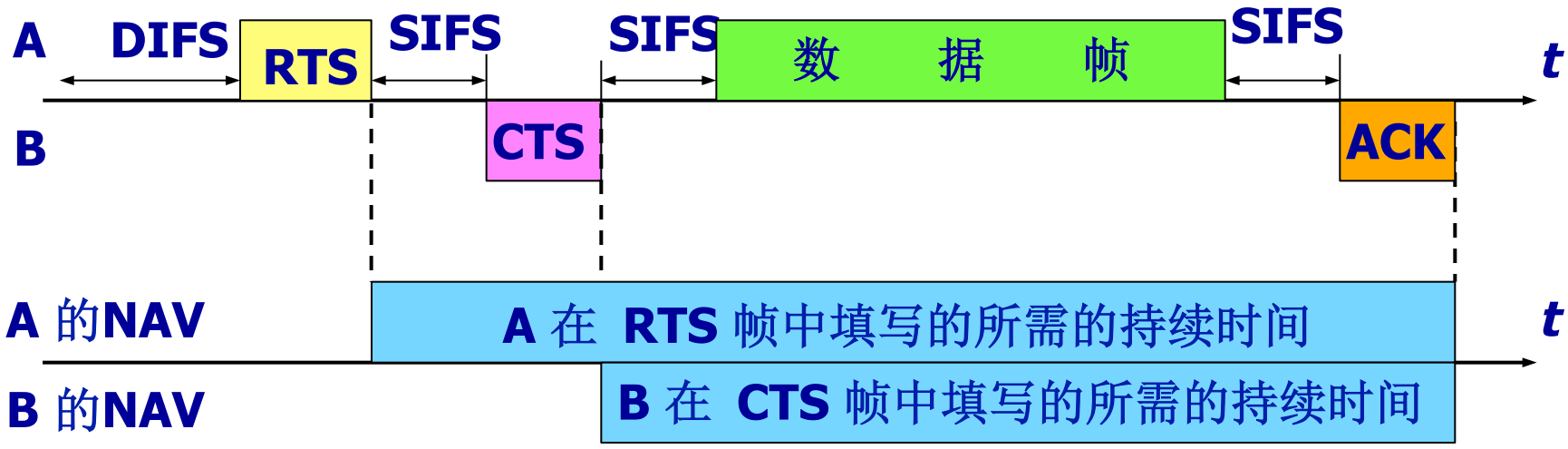
其实 B 向 A 发送数据并不影响 C 向 D 发送数据
这就是暴露站问题(exposed station problem)



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。

解决方案：对信道进行预约

- 为了更好地解决隐蔽站带来的碰撞问题，802.11允许要发送数据的站对信道进行预约。



2. 对信道进行预约

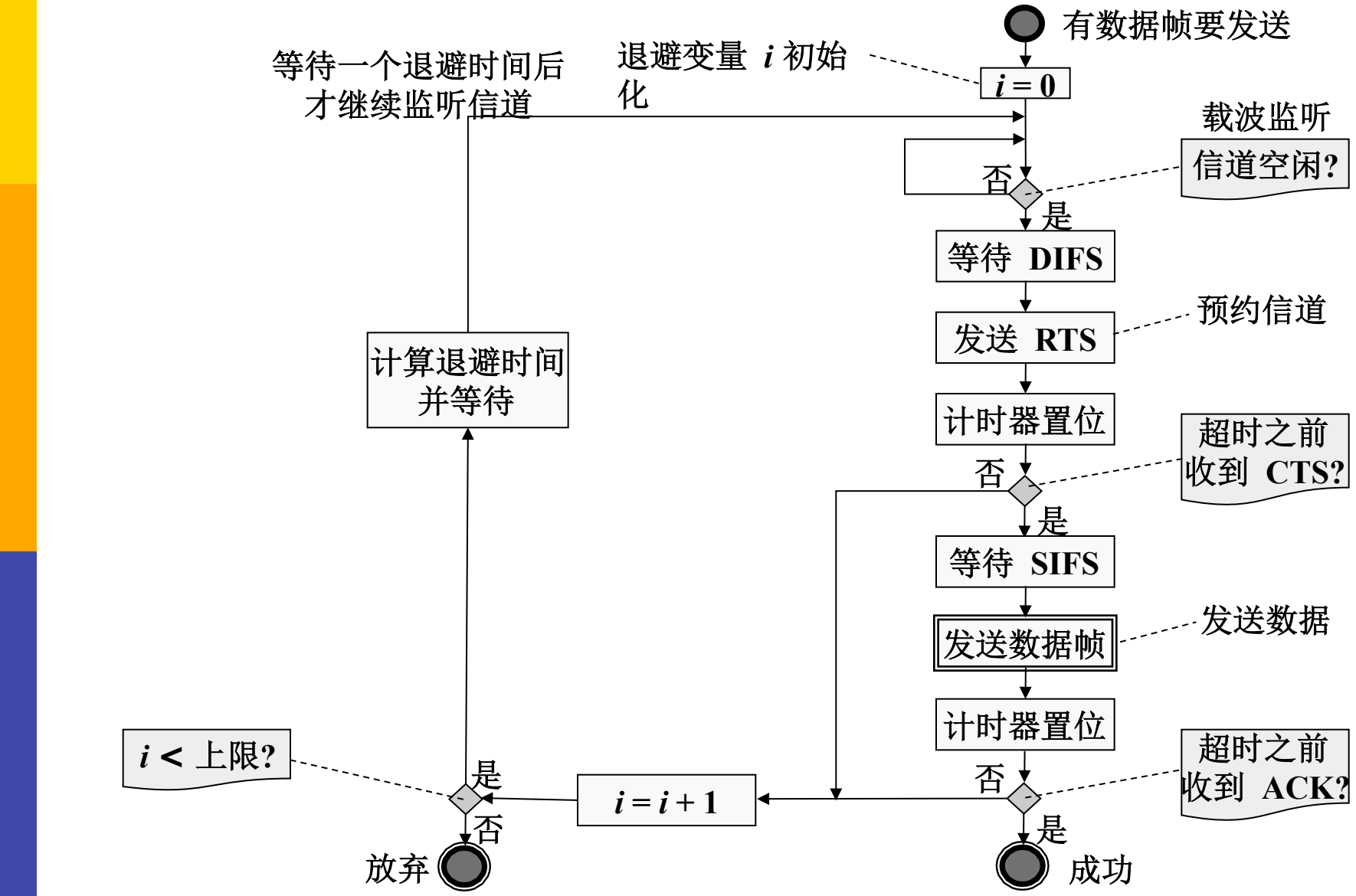
- 使用 RTS 帧和 CTS 帧会使整个网络的通信效率有所下降。但与数据帧相比，开销不算大。
- 相反，若不使用这种控制帧，则一旦发生碰撞而导致数据帧重发，则浪费的时间就更多。

2. 对信道进行预约

- 虽然如此，协议还是设有三种情况供用户选择：
  - (1) 使用 RTS 帧和 CTS 帧；
  - (2) 只有当数据帧的长度超过某一数值时才使用 RTS 帧和 CTS 帧（显然，当数据帧本身就很短时，再使用 RTS 帧和 CTS 帧只能增加开销）；
  - (3) 不使用 RTS 帧和 CTS 帧。

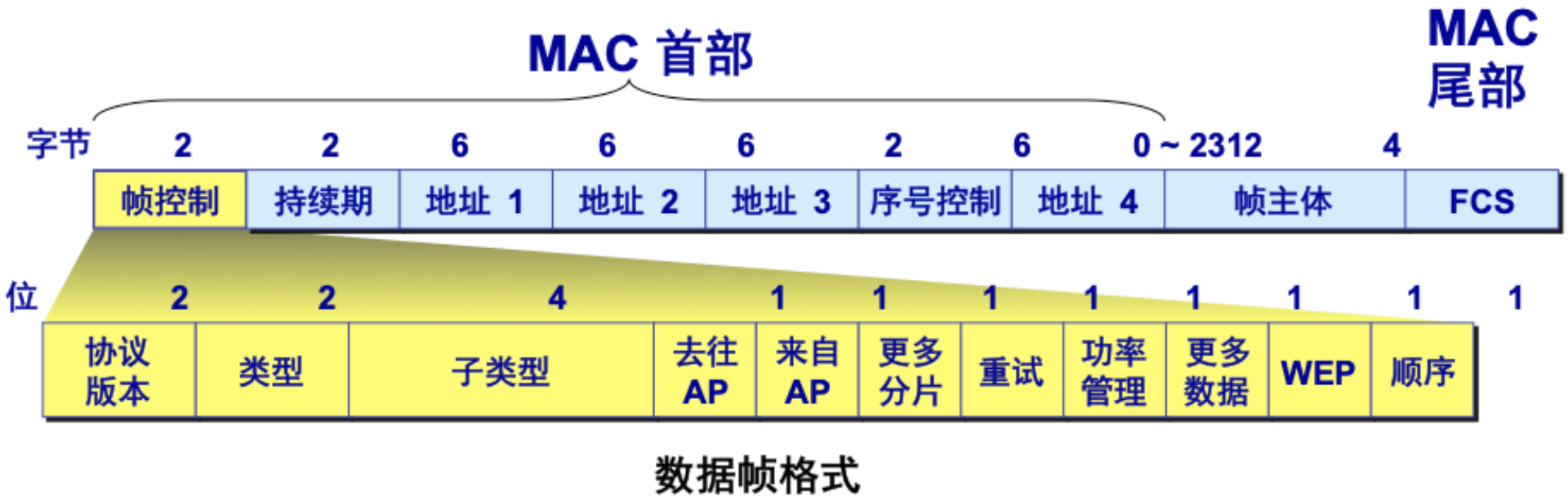
- 虽然协议经过了精心设计，但碰撞仍然会发生。

CSMA/CA 协议的基本流程图



9.1.4 802.11 局域网的 MAC 帧

- 802.11 帧共有三种类型：控制帧、数据帧和管理帧。

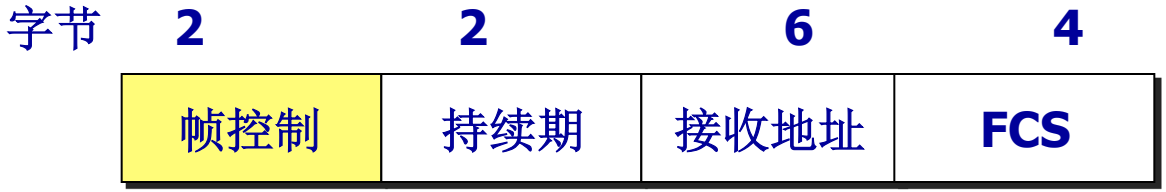


数据帧格式

9.1.4 802.11 局域网的 MAC 帧

- 802.11 帧共有三种类型：控制帧、数据帧和管理帧。

RTS帧格式（帧控制字段中的子类型为1011）



CTS 和 ACK 帧格式（帧控制字段中的子类型分别为1100和1101）

802.11 数据帧的三大部分

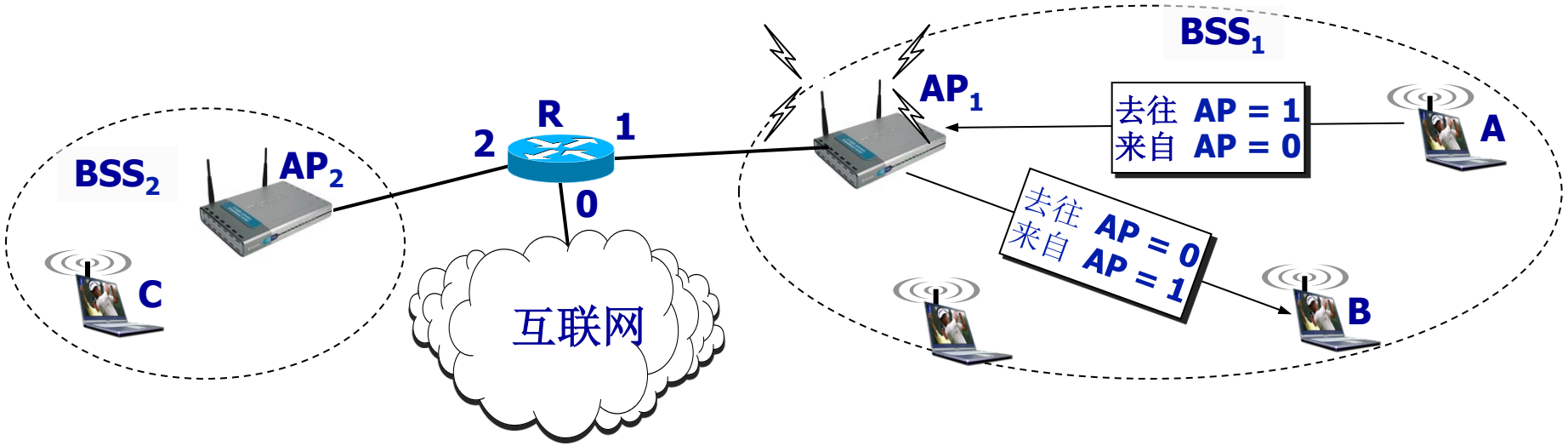
- MAC 首部，共 30 字节。帧的复杂性都在帧的首部。
- 帧主体，也就是帧的数据部分，不超过 2312 字节。这个数值比以太网的最大长度长很多。不过 802.11 帧的长度通常都是小于 1500 字节。
- 帧检验序列 FCS 是尾部，共 4 字节

1. 关于 802.11 数据帧的地址

- 802.11 数据帧最特殊的地方就是有四个地址字段。地址 4 用于自组网络。我们在这里只讨论前三种地址。

去往 AP	来自 AP	地址 1	地址 2	地址 3	地址 4
0	1	目的地址	AP 地址	源地址	——
1	0	AP 地址	源地址	目的地址	——

站点 A 向 B 发送数据帧，
或路由器 R 向 C 发送数据，
但数据帧必须经过 AP 转发。



1. 关于 802.11 数据帧的地址

数据报在路由器 R 与移动站 C 之间传送（表中地址都是MAC地址）

数据报流向	去往 AP	来自 AP	地址1	地址2	地址3	地址4
R接口2 → AP_2	1	0	AP_2地址	R接口2地址	C的地址	——
AP_2 → C	0	1	C的地址	AP_2地址	R接口2地址	——
C → AP_2	1	0	AP_2地址	C的地址	R接口2地址	——
AP_2 → R 接口 2	0	1	R接口2地址	AP_2地址	C的地址	——

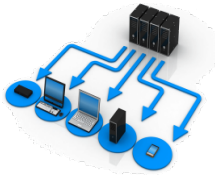
2. 序号控制、持续期和帧控制字段

- **序号控制**字段占 16 位，其中序号子字段占 12 位，分片子字段占 4 位。
- **持续期**字段占 16 位。
- **帧控制**字段共分为 11 个子字段：
  - **协议版本**字段现在是 0。
  - **类型**字段和**子类型**字段用来区分帧的功能。
  - **更多分片**字段置为 1 时表明这个帧属于一个帧的多个分片之一。
  - **有线等效保密**字段 WEP 占 1 位。若 WEP = 1，就表明采用了 WEP 加密算法。

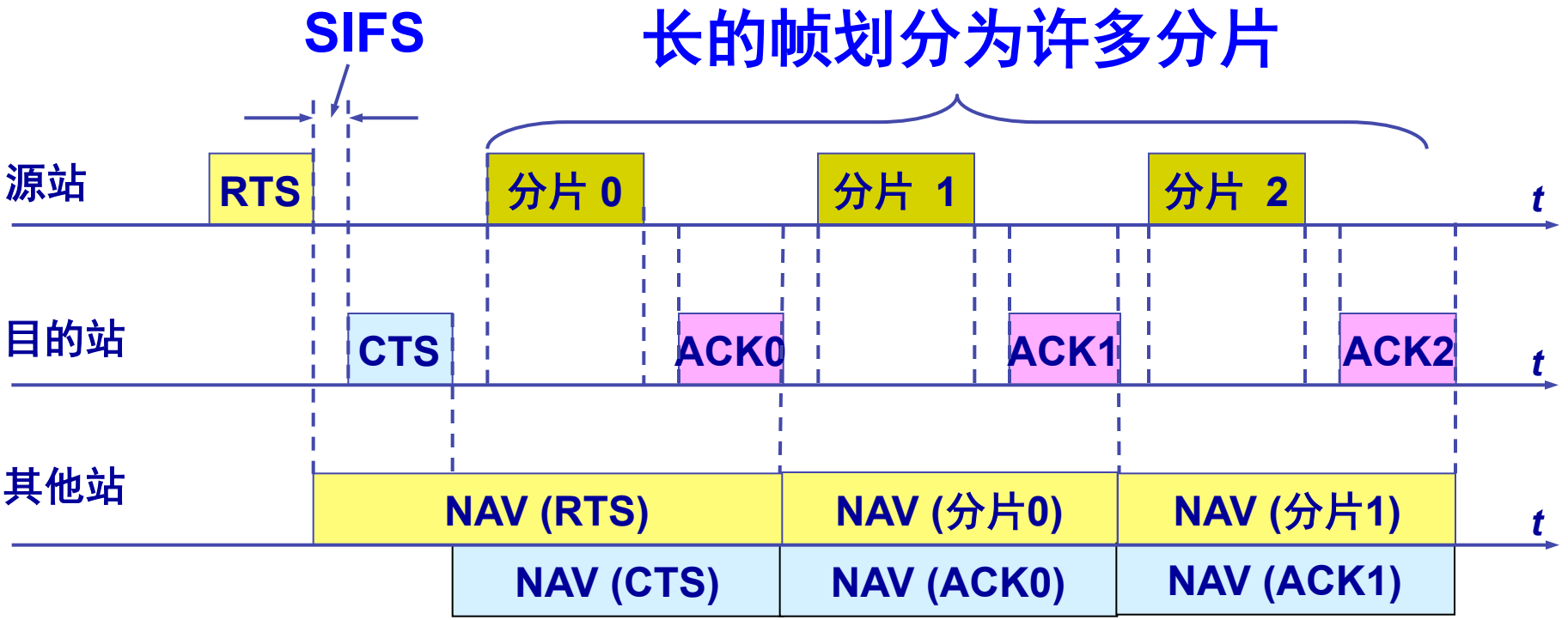
2. 序号控制、持续期和帧控制字段

- 序号控制字段占 16 位，其中序号子字段占 12 位，分片子字段占 4 位。
- 持续期字段占 16 位。
- 帧控制字段共分为 11 个子字段：
  - 协议版本字段现在是 0。
  - 类型字段和子类型字段用来区分帧的功能。
  - 更多分片字段置为 1 时表明这个帧属于一个帧的多个分片之一。
  - 有线等效保密字段 WEP 占 1 位。若 WEP = 1，就表明采用了 WEP 加密算法。

分片的发送举例



为了提高传输效率，在信道质量较差时，
需要把一个较长的帧划分为许多较短的分片。



作业

9-3，9-7，9-8，9-9，9-10，9-13，9-14，9-15