通信与网络

李凡、黎有琦

# 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

# 9.1 无线局域网 WLAN

# 9.1.1 无线局域网的组成

- **无线局域网 WLAN** (Wireless Local Area Network)：采用无线通信技术的局域网。
- **特点：**
  1. 提供了移动接入的功能
  2. 节省投资，建网速度较快
  3. 支持便携设备联网
- 由于手机普及率日益增高，通过无线局域网接入到互联网已成为当今上网的最常用的方式。

# 9.1.1 无线局域网的组成

- 便携站和移动站表示的意思并不一样。
- **便携站**：便于移动，但在工作时，其位置是固定不变的。
- **移动站**：不仅能够移动，还可以在移动的过程中进行通信。

# 9.1.1 无线局域网的组成

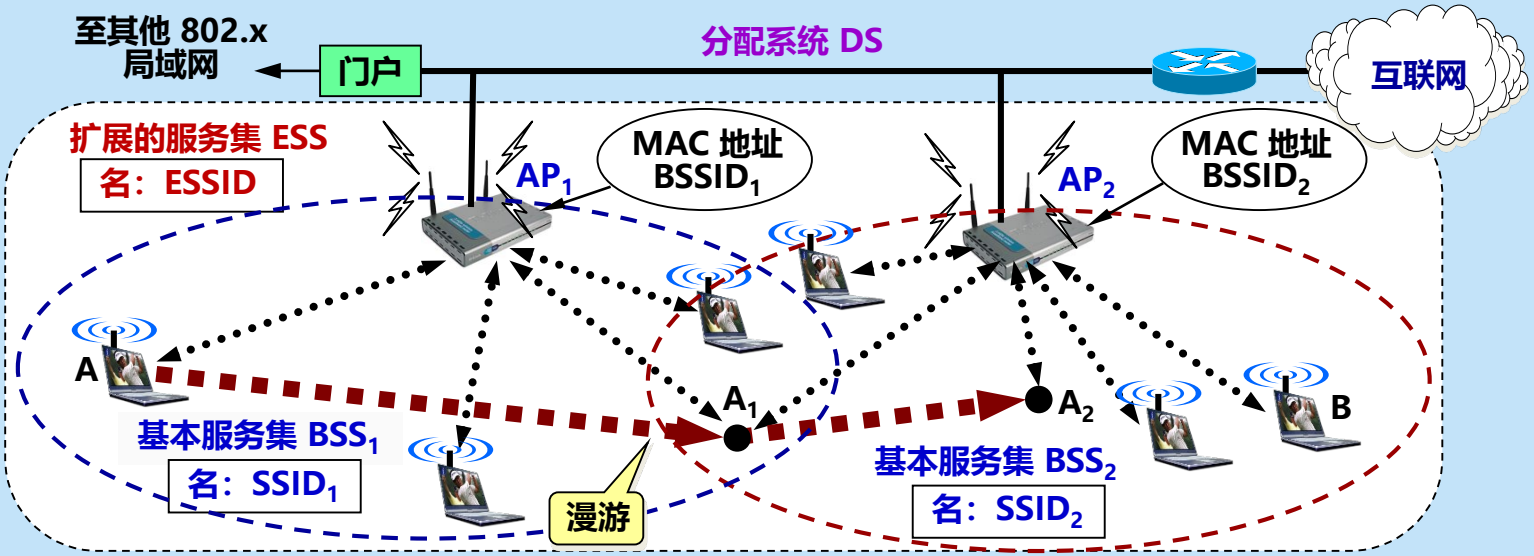
- 可分为**两大类**：
  1. 有固定基础设施的 WLAN
  2. 无固定基础设施的 WLAN
- 所谓“**固定基础设施**”是指预先建立起来的、能够覆盖一定地理范围的一批**固定基站**。

# 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。
  1. 使用星形拓扑，中心叫做**接入点 AP** (Access Point)。
     - AP 是无线局域网的**基础设施**，也是一个**链路层**的设备。
     - AP 也叫做**无线接入点 WAP** (Wireless Access Point)。
     - 无线局域网中的站点对网内或网外的通信**都必须通过 AP**。
  2. 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** 。

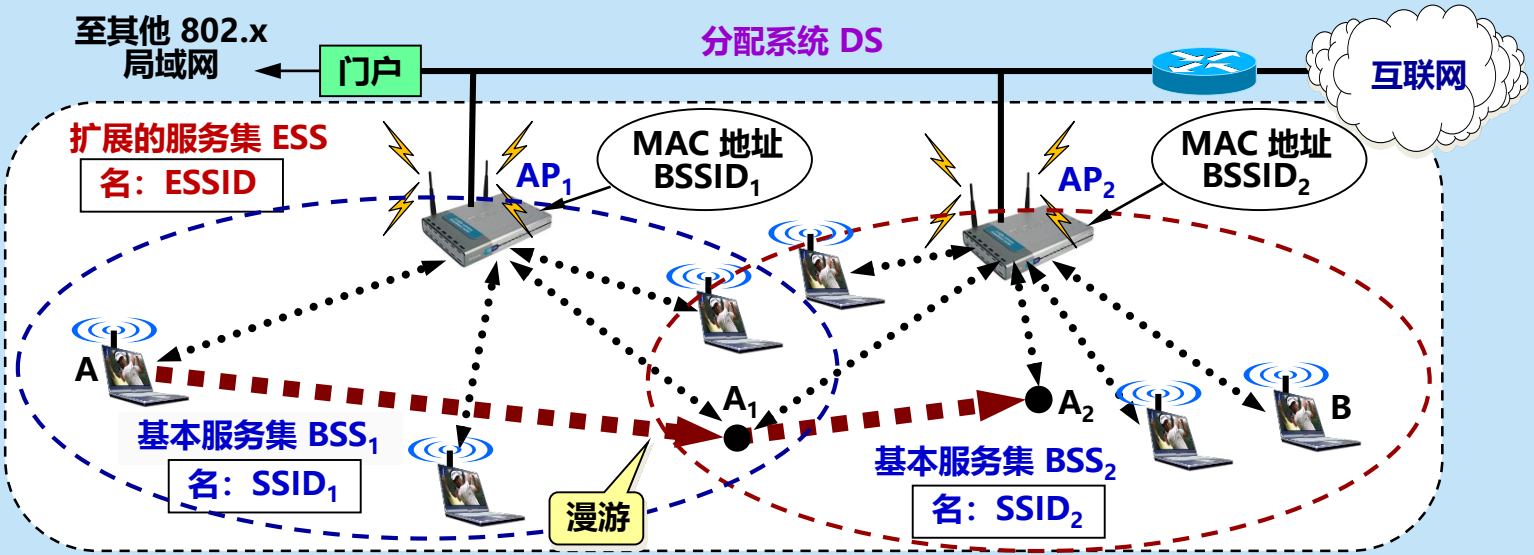
# 1. IEEE 802.11

## IEEE 802.11 的基本服务集 BSS 和扩展服务集 ESS



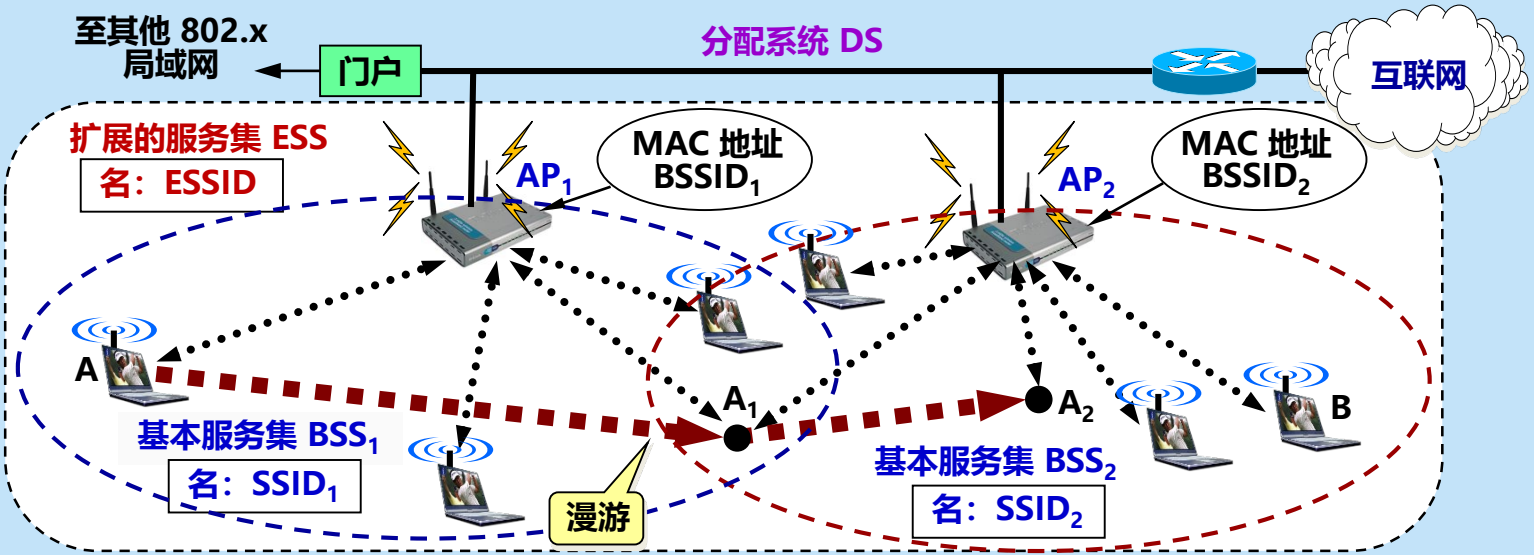
# 1. IEEE 802.11

基本服务集 BSS (Basic Service Set )是无线局域网的最小构件。
一个 BSS 包括一个接入点 AP 和若干个移动站。



# 1. IEEE 802.11

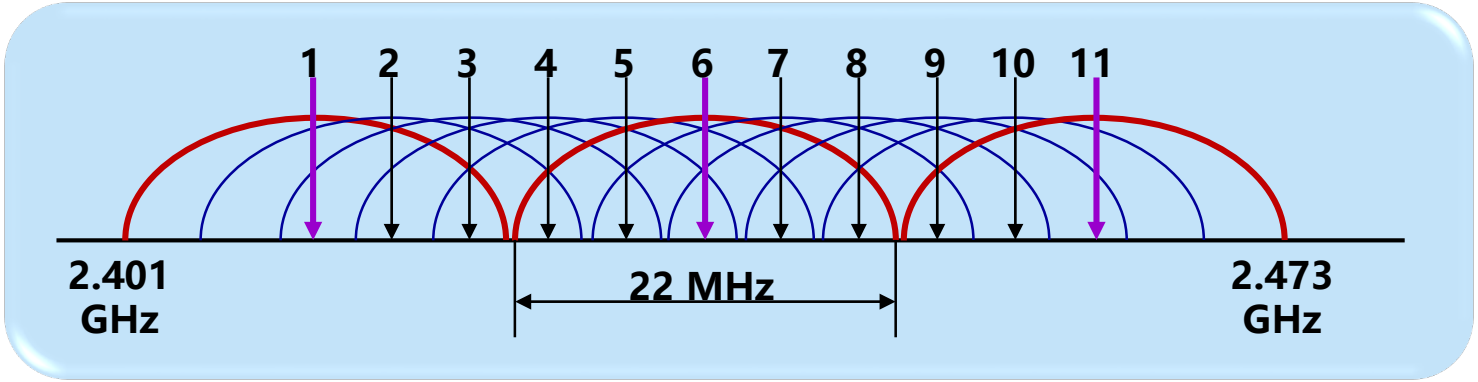
必须为该 AP 分配一个不超过 32 字节的服务集标识符 SSID (Service Set IDentifier)
（即该 AP 的无线局域网的名字）和一个通信信道。




一个 BSS 所覆盖的地理范围叫做一个基本服务区 BSA (Basic Service Area)。

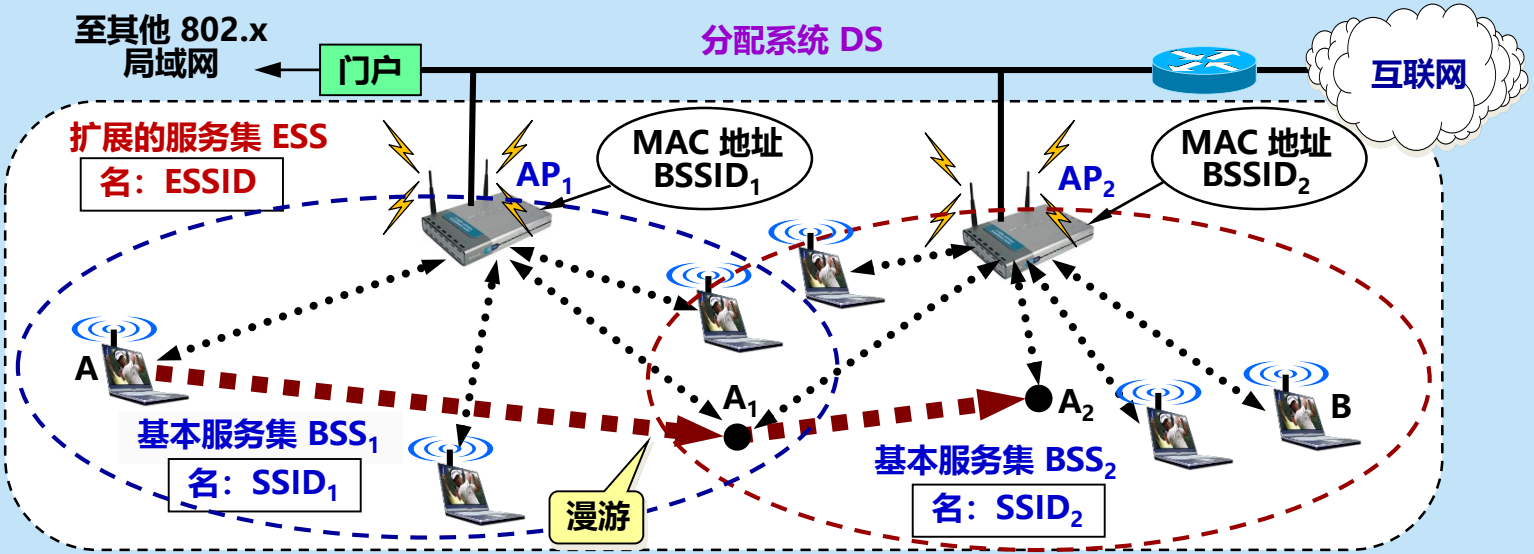
## 信道 (channel)

- 无线局域网通常使用 2.4 GHz 和 5 GHz 频段。每一个频段划分为若干个信道，供各无线局域网使用。
- 802.11b 使用 2.4 GHz 频段，带宽约 85 MHz。定义了 11 个部分重叠的信道集。相邻信道的中心频率相差 5 MHz，每个信道的带宽约为 22 MHz。



# 1. IEEE 802.11

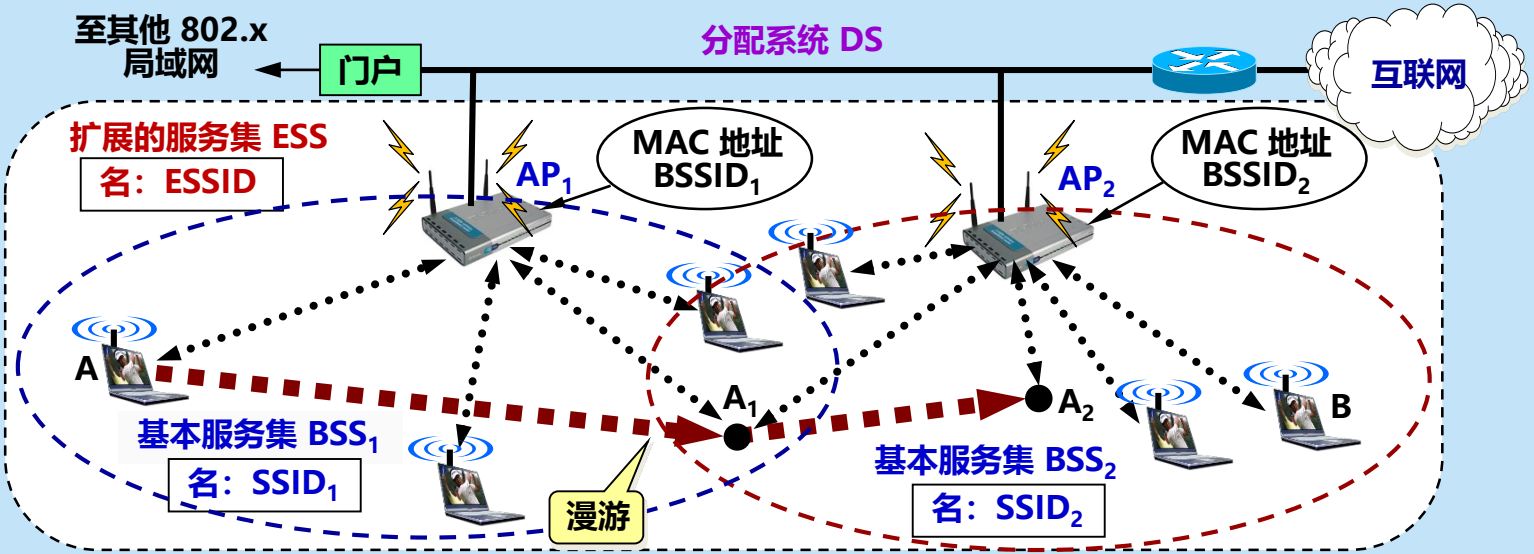
每个 AP 有一个唯一的 48 位 MAC 地址，名称是基本服务集标识符 BSSID。在无线局域网中传送的各种帧的首部中，都必须有节点的 MAC 地址（即 BSSID，但不是 SSID）。




用户通常都知道所连接的无线局域网 SSID，但可以不知道其 BSSID。

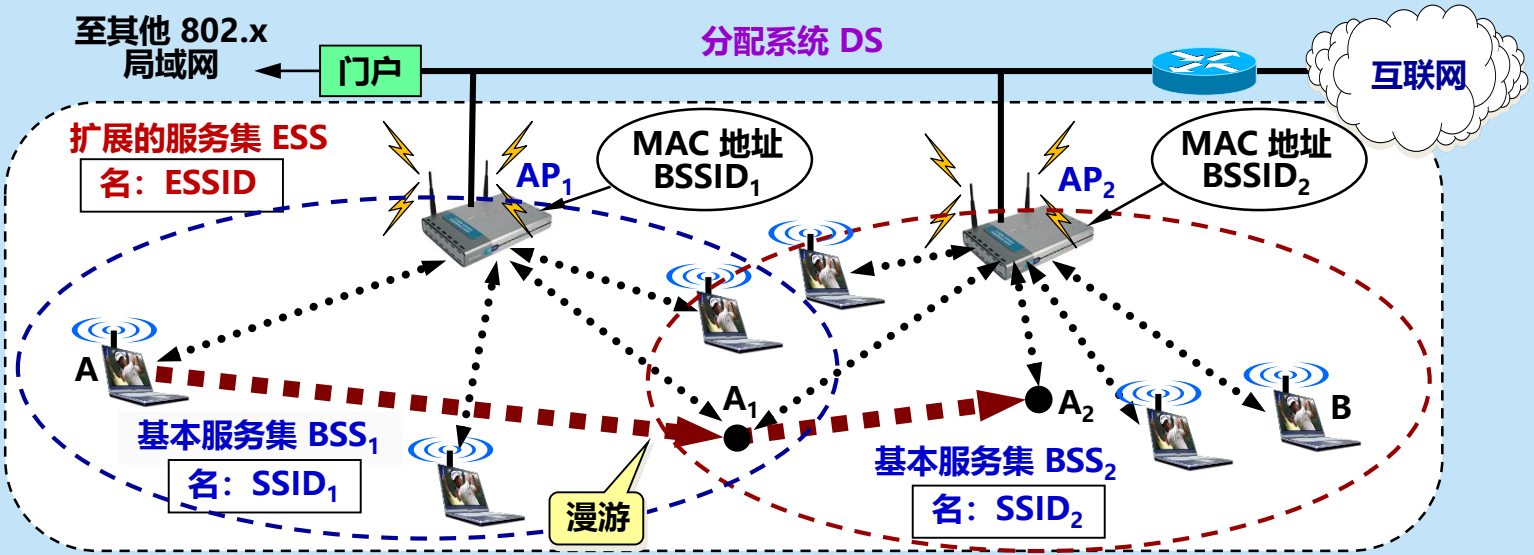
# 1. IEEE 802.11

一个 BSS 可以通过 AP 连接到一个分配系统 DS (Distribution System)，然后再连接到另一个 BSS，构成了一个扩展服务集 ESS (Extended Service Set)。



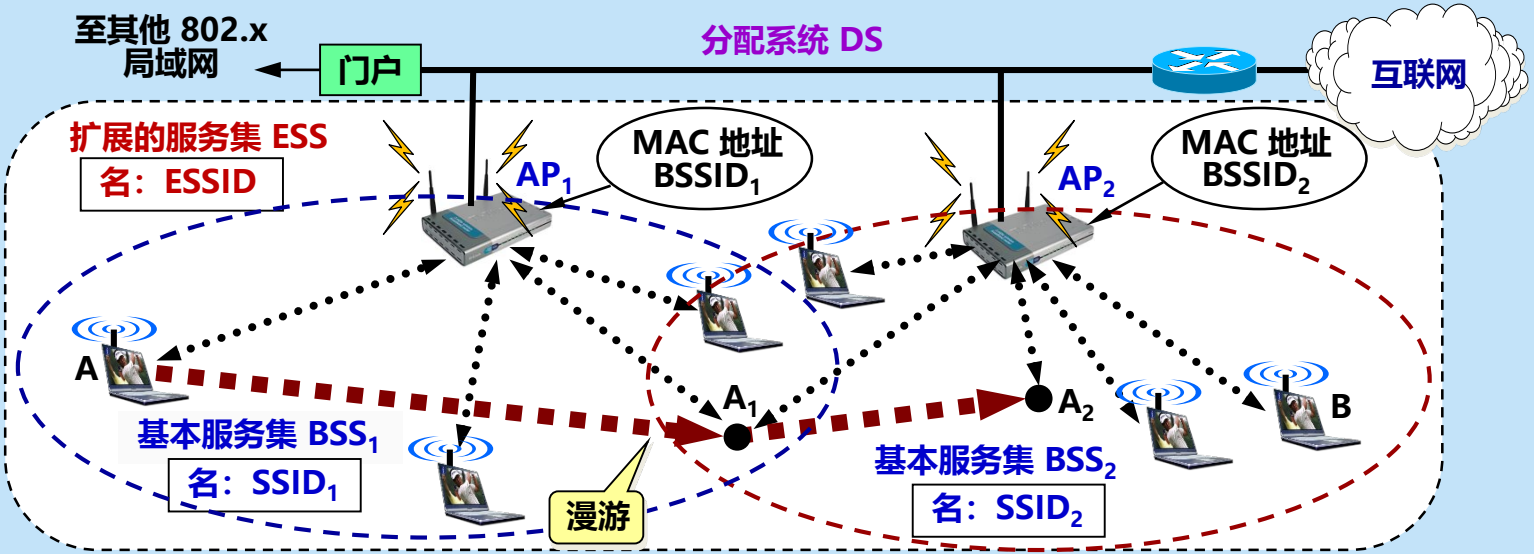
# 1. IEEE 802.11

ESS 也有个标识符，是不超过 32 字符的字符串名字 (不是地址)，叫做
扩展服务集标识符 ESSID。



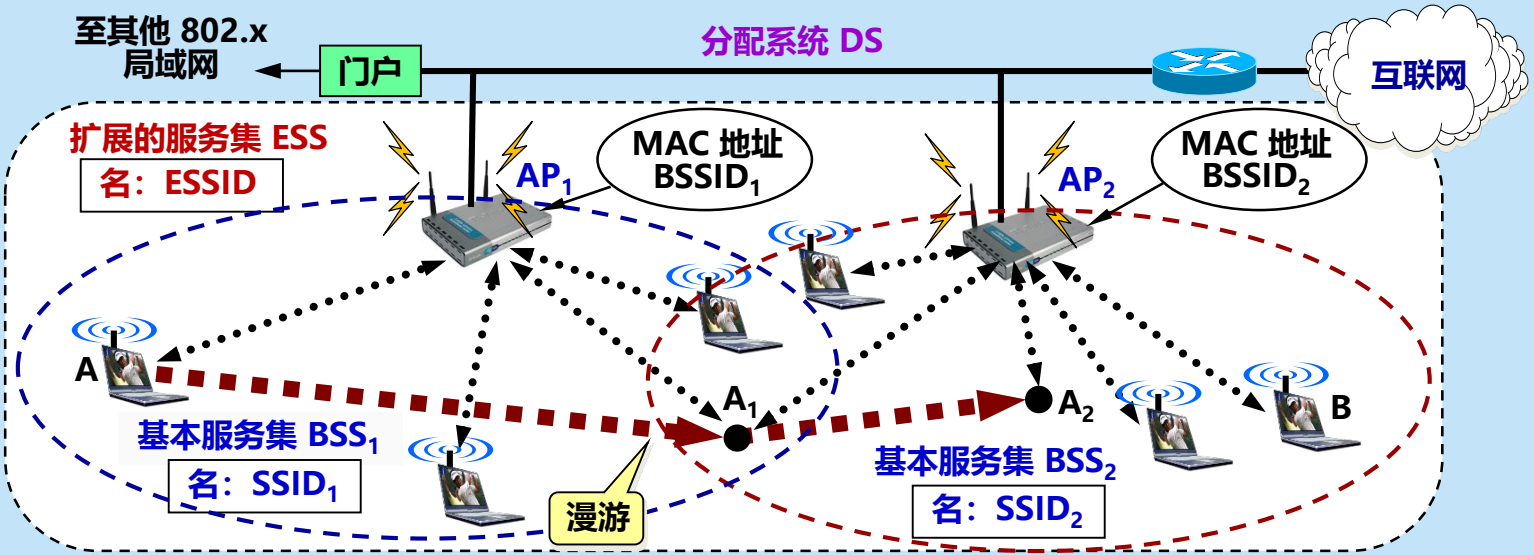
# 1. IEEE 802.11

DS 的作用：使 ESS 对上层的表现就像一个 BSS 一样。
DS 可以使用以太网（最常用）、点对点链路或其他无线网络。



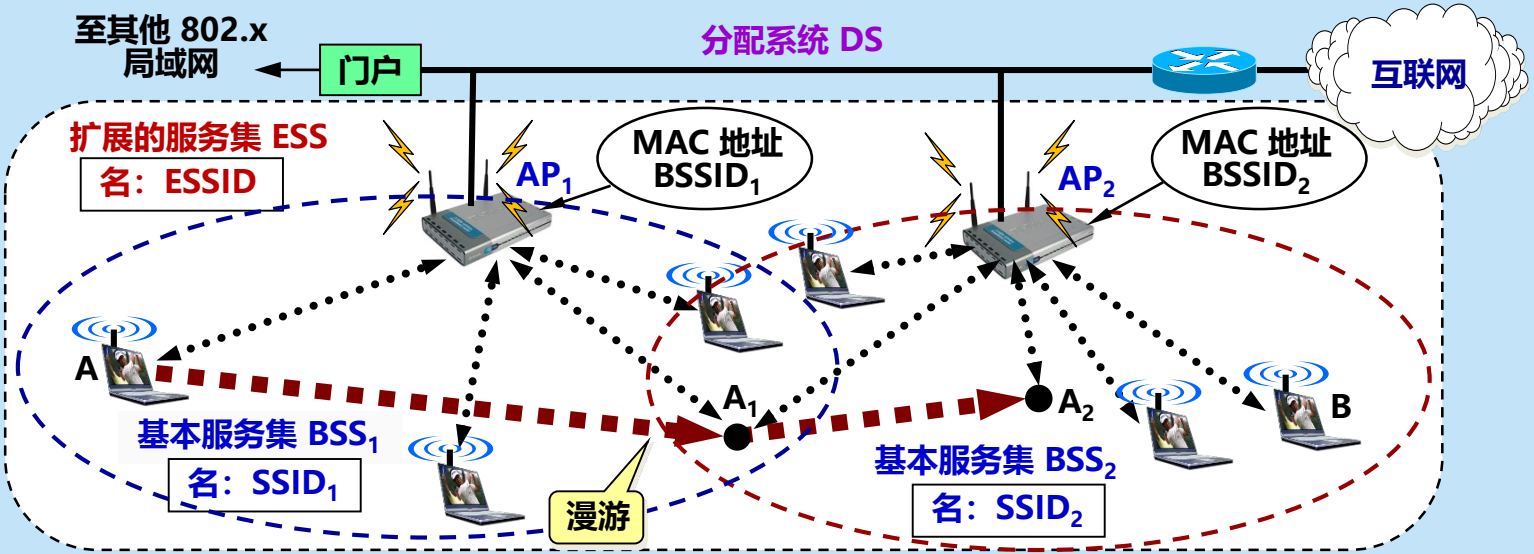
# 1. IEEE 802.11

ESS 还可为无线用户提供到 802.x 局域网（非802.11无线局域网）的接入。
通过门户 (Portal) 设备实现。门户相当于一个网桥。



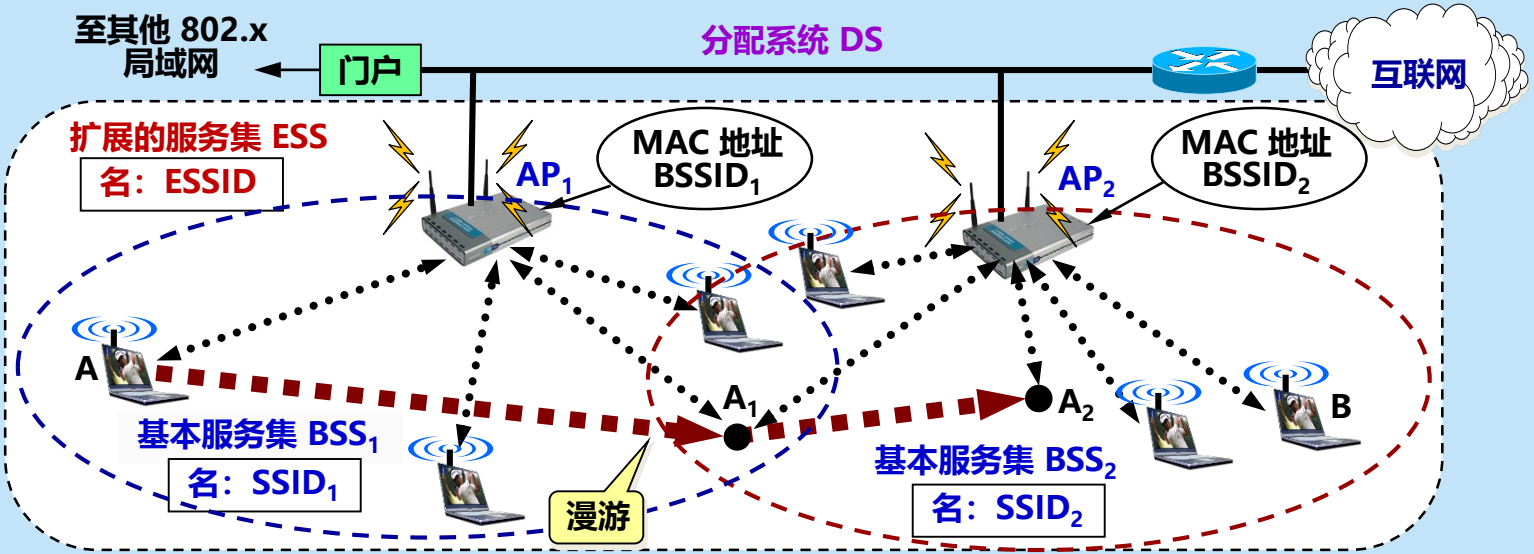
# 1. IEEE 802.11

移动站 A 如果要和另一个 BSS 中的移动站 B 通信，就必须经过两个接入点 $AP_1$ 和 $AP_2$，即 A→$AP_1$→$AP_2$→B。



# 1. IEEE 802.11

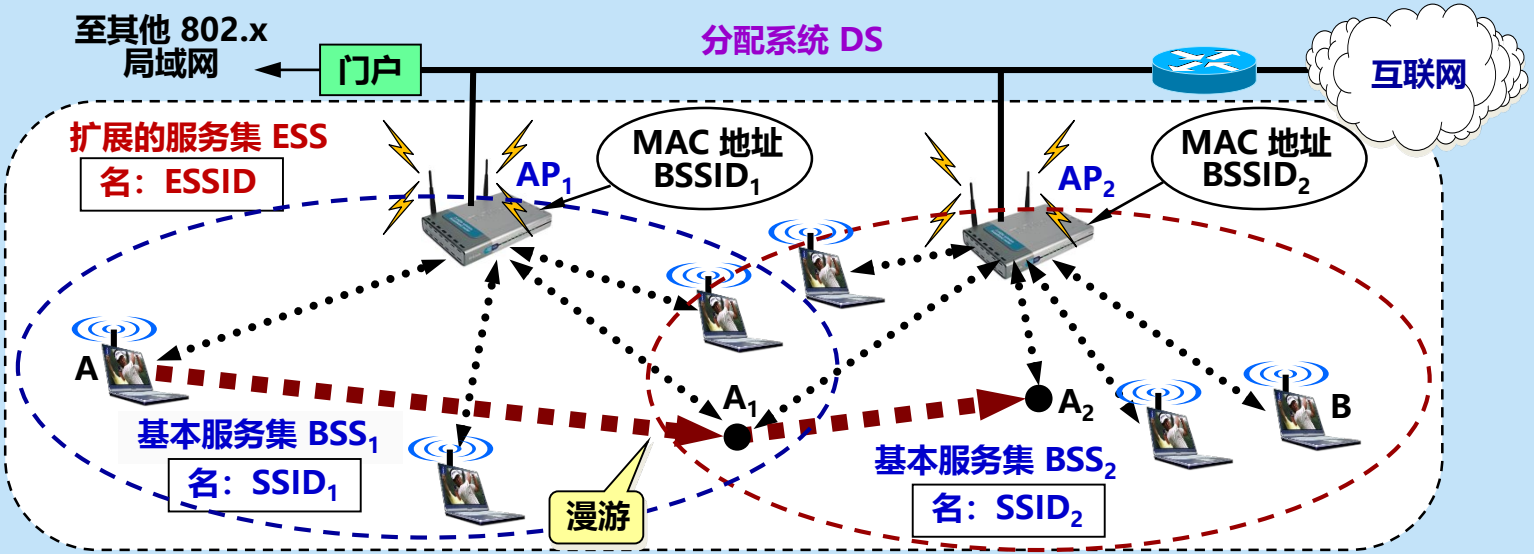
移动站 A 漫游到位置 $A_1$ 时，选择和信号较强的一个 AP 联系。当漫游到位置 $A_2$ 时，就只能和 $AP_2$ 联系了。




BSS 的服务范围是由 AP 所发射的电磁波的辐射范围确定的。

# 1. IEEE 802.11

移动站只要能够和其中一个 AP 联系上，就可以一直保持与另一个移动站 B 的通信。

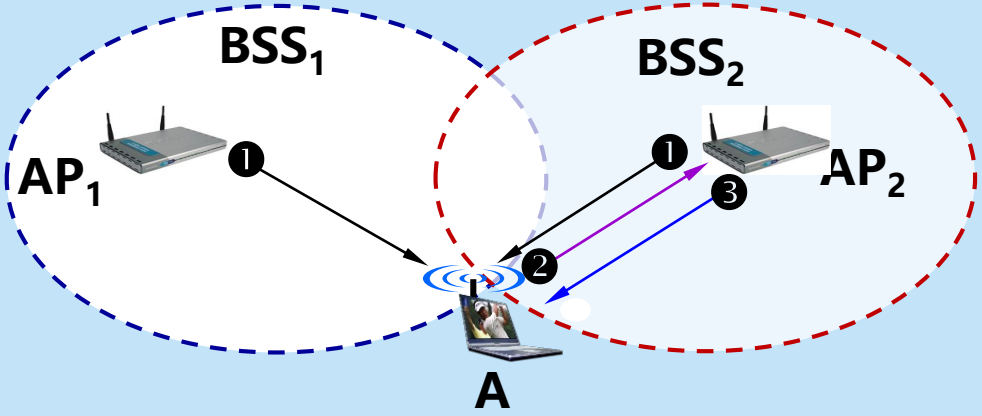



BSS 的服务范围是由 AP 所发射的电磁波的辐射范围确定的。

## 关联 (association)

- 一个移动站若要加入到一个 BSS，就必须先与某个 AP **建立关联**。
- **建立关联**：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 才能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。

# 建立关联的两种方法：(1) 被动扫描

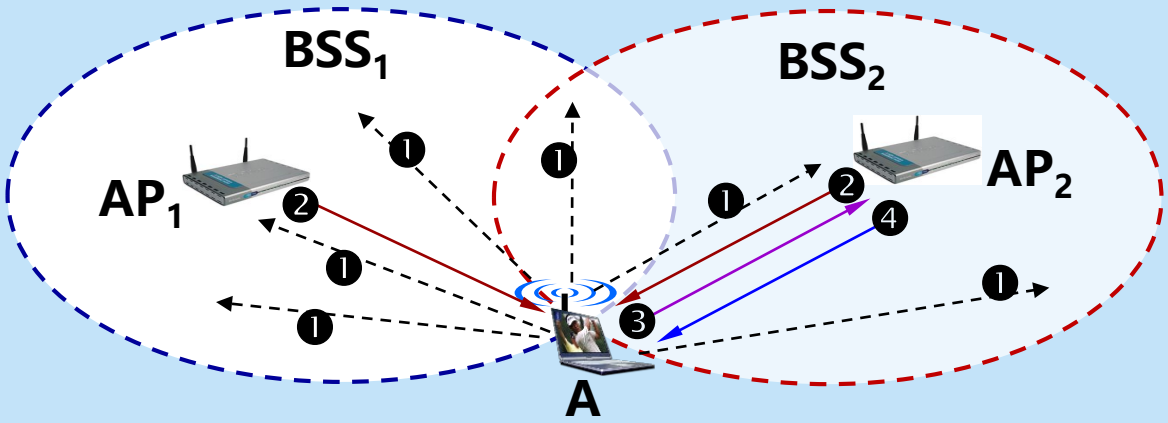



❶ AP 周期性发出信标帧 (beacon frame)，其中包含 SSID 、速率等系统参数。

❷ 移动站 A 扫描 11 个信道，选择加入到 $AP_2$ 所在的基本服务集 $BSS_2$，向 $AP_2$ 发出关联请求帧 (Association Request frame)。

❸ $AP_2$ 同意移动站 A 发来的关联请求，向移动站A发送关联响应帧 (Association Response frame)。

# 建立关联的两种方法：(2) 主动扫描




一个移动站可以同时进行主动扫描和被动扫描。

❶ 移动站 A 主动发出广播的探测请求帧 (Probe Request frame)，让所有能够收到此帧的接入点知道有移动站要求建立关联。

❷ 两个 AP 都回答探测响应帧 (Probe Response frame)。

❸ 移动站 A 向 $AP_2$ 发出关联请求帧 (Association Response frame)。

❹ $AP_2$ 向移动站 A 发送关联响应帧，与移动站 A 建立关联。

## 重建关联 (reassociation) 和分离 (dissociation)

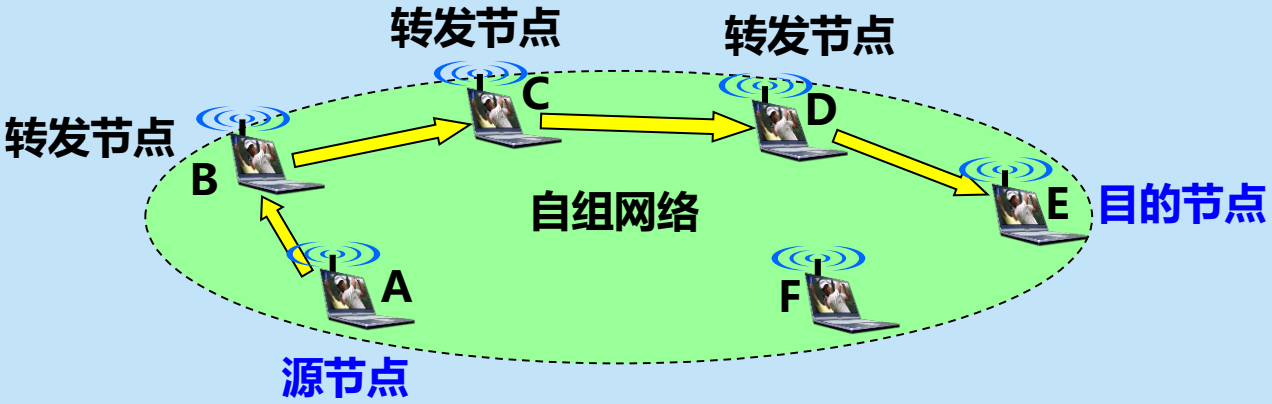
- 移动站使用**重建关联** (reassociation) 服务，可把这种关联转移到另一个接入点。
- 当使用**分离** (dissociation) 服务时，可终止这种关联。

## 安全地建立关联

- 用户在和附近的接入点 AP 建立关联时，一般还要键入用户密码。
- 初期加密方案：有线等效的保密 WEP (Wired Equivalent Privacy)。
- 现在加密方案：无线局域网受保护的接入 WPA (WiFi Protected Access) 或 WPA2 。

# 2. 移动自组网络

- 又称为**自组网络** (ad hoc network) 。
- 是没有固定基础设施（即没有 AP）的无线局域网。
- 移动站都处于平等状态。




**三个主要问题：**路由选择协议，多播，安全。

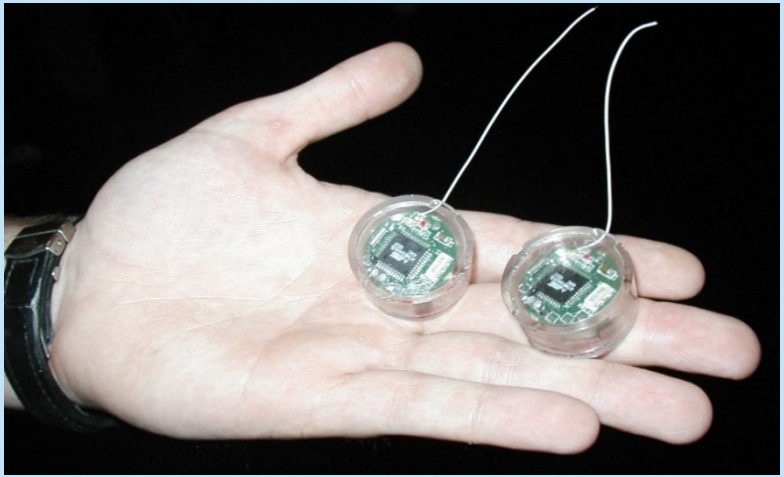
## 2. 移动自组网络

- 服务范围通常是受限的，一般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。
- 优点：
  - 方便灵活。
  - 生存性非常好。

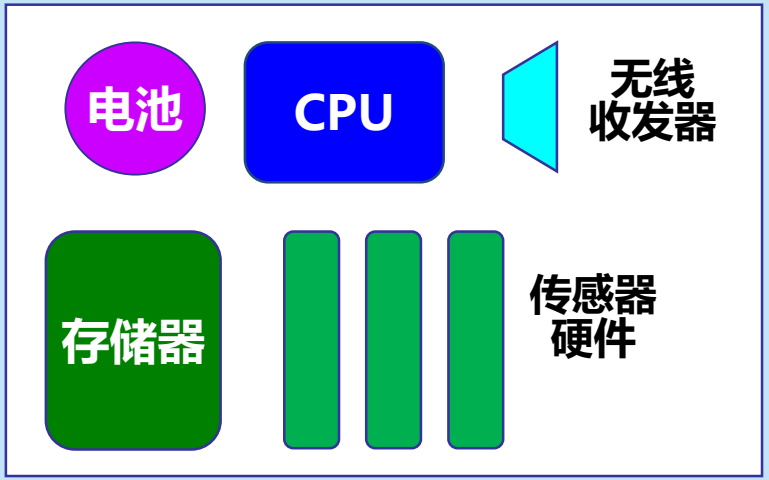
# 无线传感器网络 WSN

- **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**：进行各种数据的采集、处理和传输。
- **特点**：
  1. 不需要很高的带宽，但大部分时间必须保持低功耗。
  2. 对协议栈的大小有严格的限制。
  3. 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。

# 传感器结点的形状和组成



(a) 形状




(b) 组成

## 无线传感器网络主要的应用领域

- 组成各种物联网 IoT (Internet of Things)，例如：
  1. 环境监测与保护；
  2. 战争中对敌情的侦查和对兵力、装备、物资等的监控；
  3. 医疗中对病房的监测和对患者的护理；
  4. 在危险的工业环境中的安全监测；
  5. 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

- 漫游的主机可以用多种方式连接到互联网。
- 漫游的主机可以直接或通过无线链路连接到固定网络上的另一个子网。
- 需要地址管理和增加协议的互操作性。
- 核心网络功能仍然是各种路由选择协议。

## 移动自组网络

- 把移动性扩展到无线领域中的自治系统。
- 具有自己特定的路由选择协议，并且可以不和互联网相连。
- 即使和互联网相连时，移动自组网络也是以末梢网络 (stub network) 方式工作。
- **末梢网络：** 不允许外部通信量穿越该网络。

## 几种不同的接入

- **固定接入** (fixed access)：在作为网络用户期间，用户设置的地理位置保持不变。
- **移动接入** (mobility access)：用户设置能够以车辆速度移动时进行网络通信。当发生切换时，通信仍然是连续的。
- **便携接入** (portable access)：在受限的网络覆盖面积中，用户设备能够在以步行速度移动时进行网络通信，提供有限的切换能力。
- **游牧接入** (nomadic access)：用户设备的地理位置至少在进行网络通信时保持不变。如用户设备移动了位置，则再次进行通信时可能还要寻找最佳的基站。

# 9.1.2 802.11 局域网的物理层

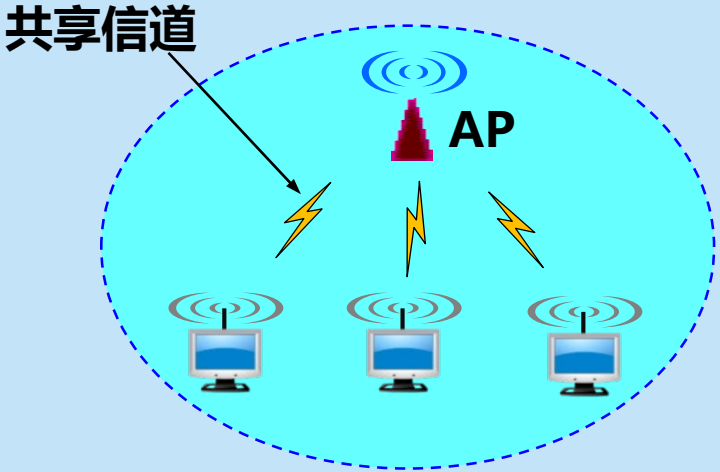
- 802.11 标准中物理层相当复杂。根据物理层的不同（如工作频段、数据率、调制方法等），对应的标准也不同。

| 标准 | 别名 | 频段 | 最高数据率 | 物理层 | 优缺点 |
|---|---|---|---|---|---|
| 802.11b (1999年) | Wi-Fi 1 | 2.4 GHz | 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) | Wi-Fi 2 | 5 GHz | 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) | Wi-Fi 3 | 2.4 GHz | 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) | Wi-Fi 4 | 2.4 / 5 GHz | 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。 |
| 802.11ac (2014年) | Wi-Fi 5 | 5 GHz | 7 Gbit/s | MIMO OFDM | 完全遵循 802.11i 安全标准的所有内容，使得无线连接能够在安全性方面达到企业级用户的需求。 |
| 802.11ax (2019年) | Wi-Fi 6 | 2.4 / 5 GHz | 9.6 Gbit/s | MIMO OFDM | 侧重解决密集环境下（如火车站、机场）提高吞吐量密度（即单位面积的吞吐量） |

## 802.11 的物理层的几种实现方法

- 802.11 的物理层有以下几种实现方法：
  1. 扩频
  2. 多入多出 MIMO (Multiple Input Multiple Output)
  3. 正交频分复用 OFDM (Orthogonal Frequency Division Multiplexing)
  4. 跳频扩频 FHSS （已很少用）
  5. 红外线 IR （已很少用）

# 9.1.3 802.11 局域网的 MAC 层协议

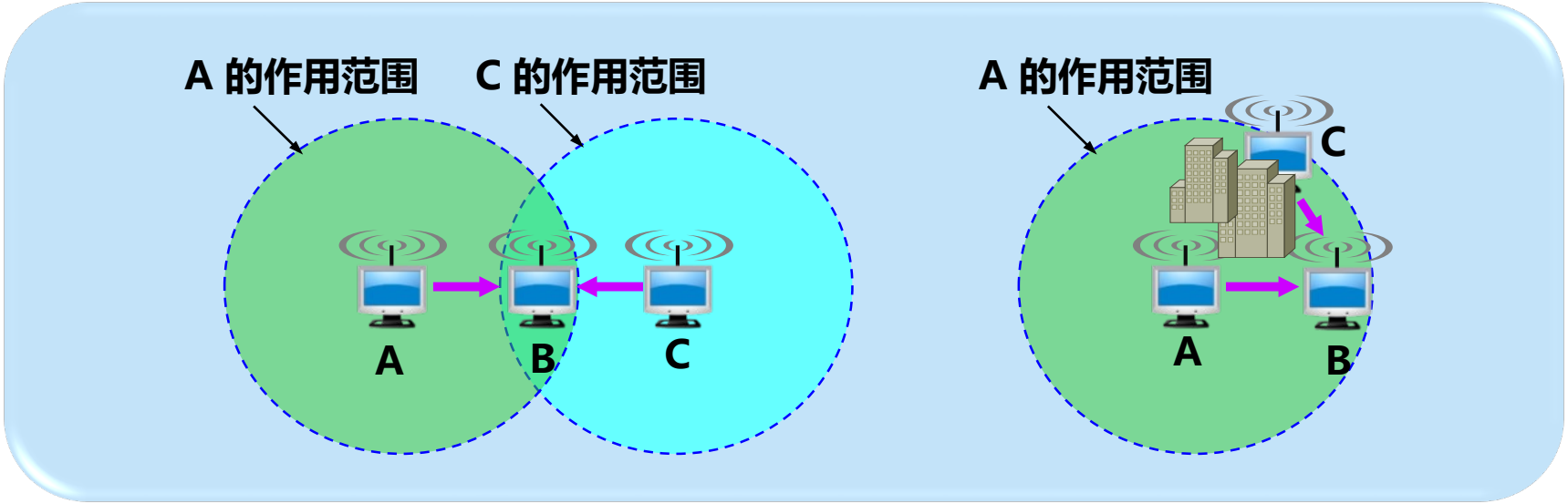



必须解决共享信道上的碰撞问题

# 1. CSMA/CA 协议

- 无线局域网**不能**简单地搬用 CSMA/CD 协议。因为：
  1. **碰撞检测（CD）**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**。
  2. 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**。

# 无线局域网的特殊问题




**隐蔽站问题** (hidden station problem)：由于无线信号覆盖范围和穿透能力有限，A 和 C 检测不到彼此的无线信号，都以为 B 是空闲的，因而都向 B 发送数据，结果发生碰撞。

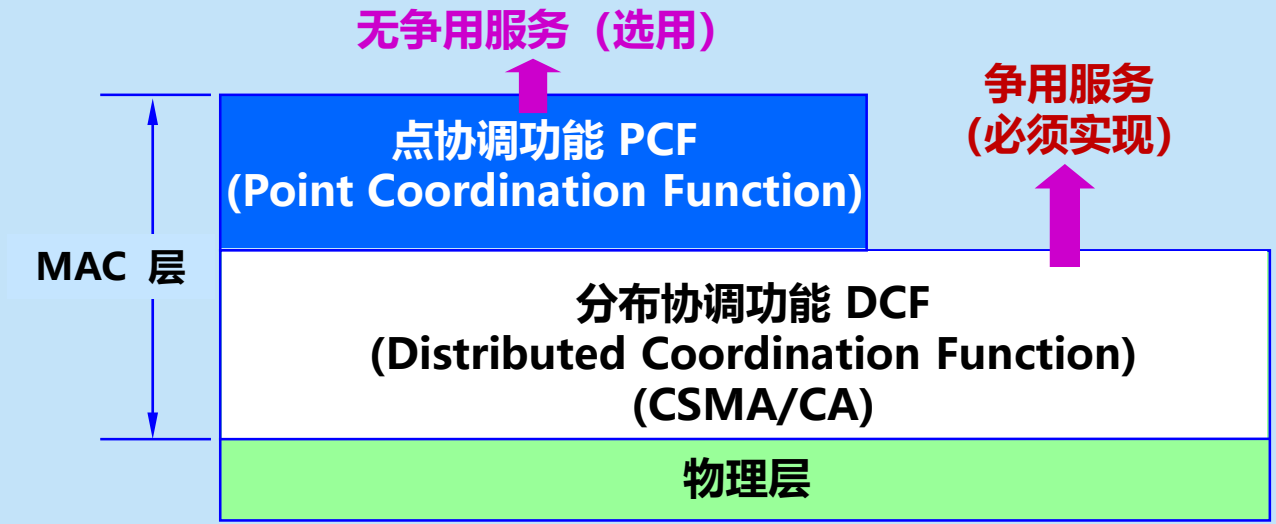
## 必须考虑的特点

1. 无线局域网的适配器**无法实现**碰撞检测；
2. 检测到信道空闲，其实信道**可能并不空闲**；
3. 即使能够在硬件上实现无线局域网的碰撞检测功能，也无法检测出**隐蔽站问题**带来的碰撞。

## CSMA/CA 协议

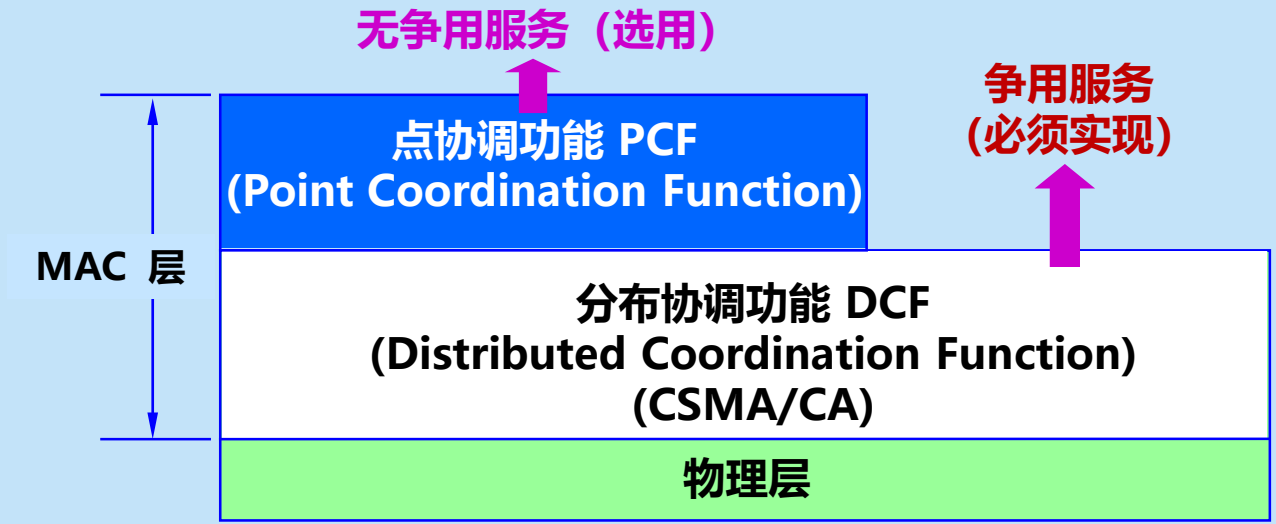
- 无线局域网不能使用 CSMA/CD。
- 但可以使用 CSMA 协议。
- 改进：
  - 增加碰撞避免 CA (Collision Avoidance)：尽量减少碰撞发生的概率。
  - 使用 CSMA/CA 的同时，使用停止等待协议：链路层确认，解决碰撞后重传。

# 802.11 的 MAC 层



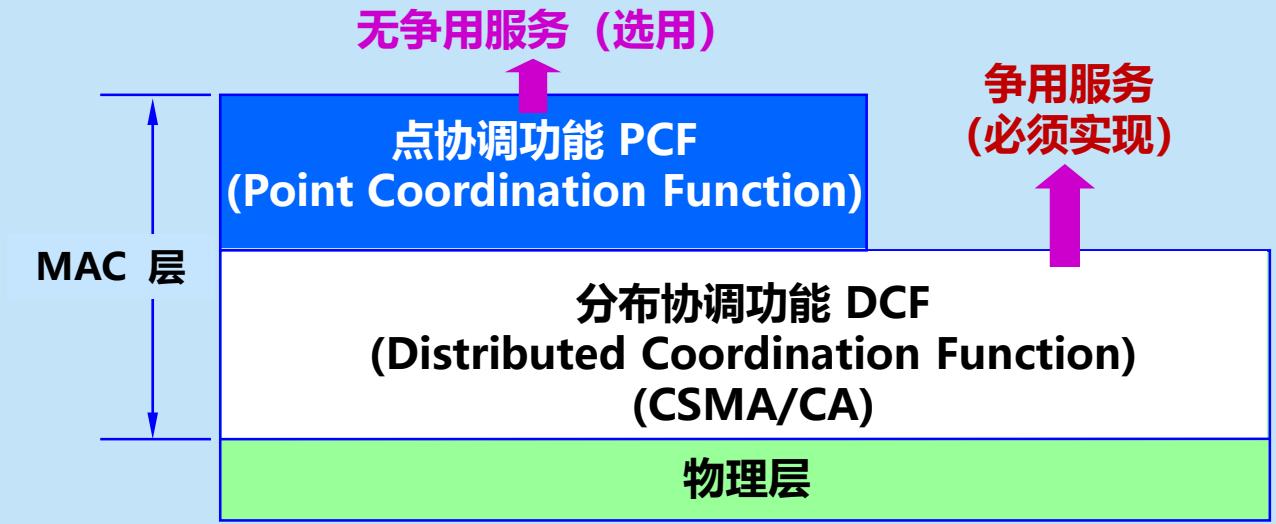

MAC 层通过**协调功能**来确定在基本服务集 BSS 中的移动站何时可以发送或接收数据。包括**两个子层**：DCF 和 PCF。

# 802.11 的 MAC 层：分布协调功能 DCF



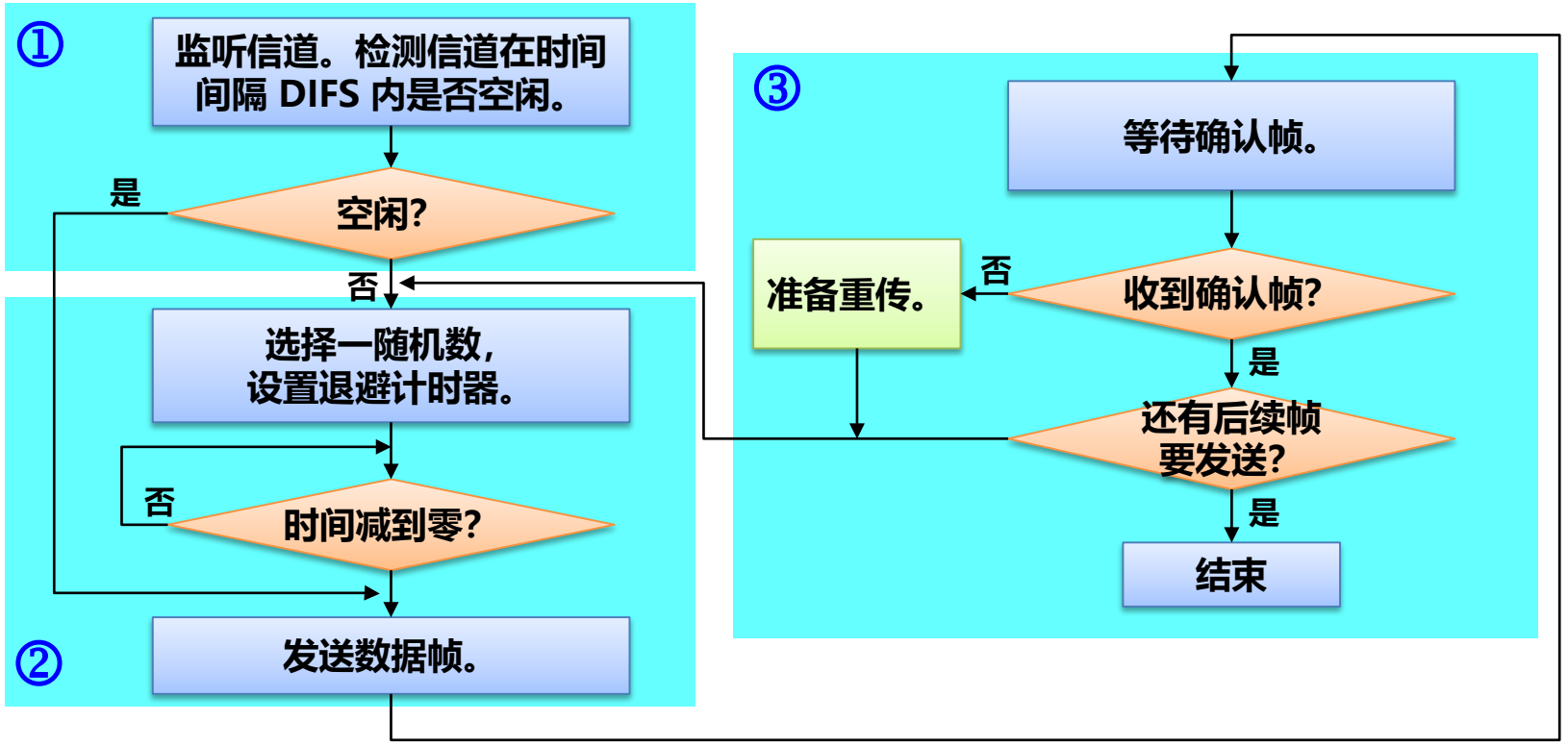

**DCF 子层：不采用任何中心控制。每个节点使用 CSMA/CA 机制的分布式接入算法，让各个站通过争用信道来获取发送权。因此 DCF 向上提供争用服务。所有实现都必须有 DCF 功能。**

# 802.11 的 MAC 层：点协调功能 PCF




**PCF 子层：** 可选。使用集中控制的接入算法，用类似于探询的方法把发送数据权轮流交给各个站，从而避免碰撞。自组网络没有 PCF 子层。
对时间敏感的业务，如分组话音，应使用提供无争用服务的 PCF。

# CSMA/CA 协议的要点



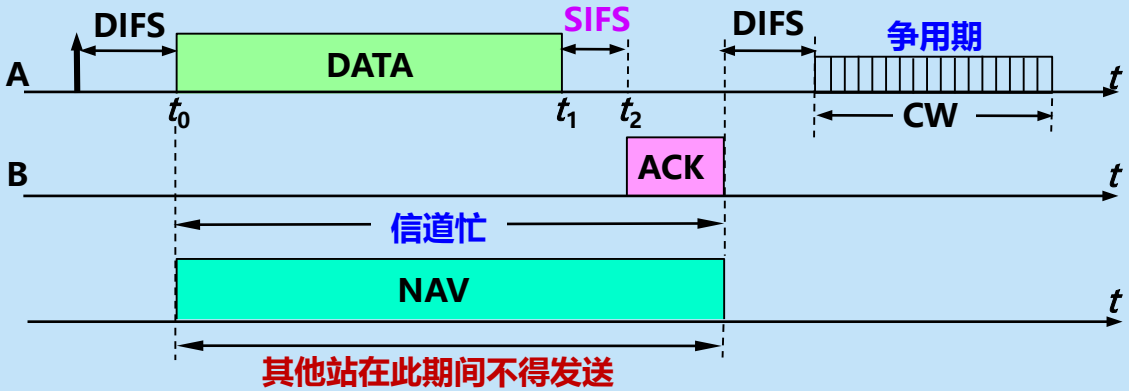
## 2. 时间间隔 DIFS 的重要性

- 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)。
- 两种常用的帧间间隔：
  - 分布协调功能帧间间隔 **DIFS**。
  - 短 (Short) 帧间间隔 **SIFS**。

# SIFS

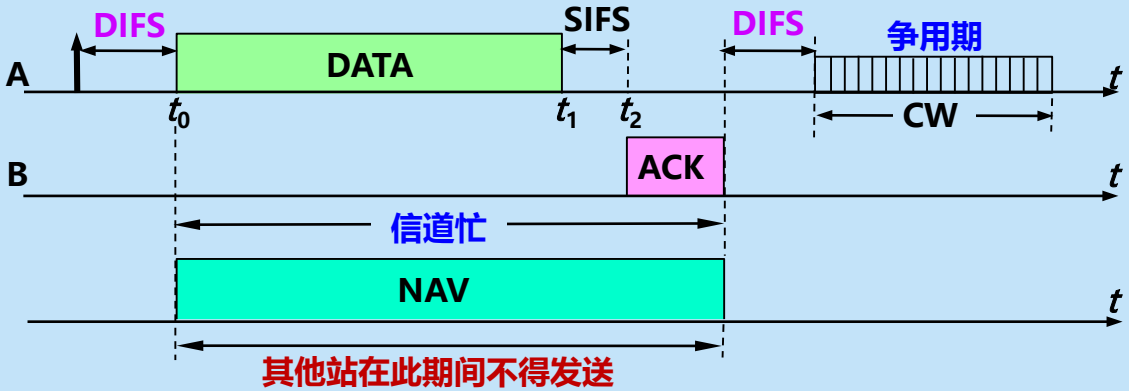
是最短的帧间间隔，用来分隔属于一次对话的各帧。
一个站应当能够在这段时间内从发送方式切换到接收方式。

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 探测请求帧和在 PCF 方式中接入点 AP 发送出的任何帧。



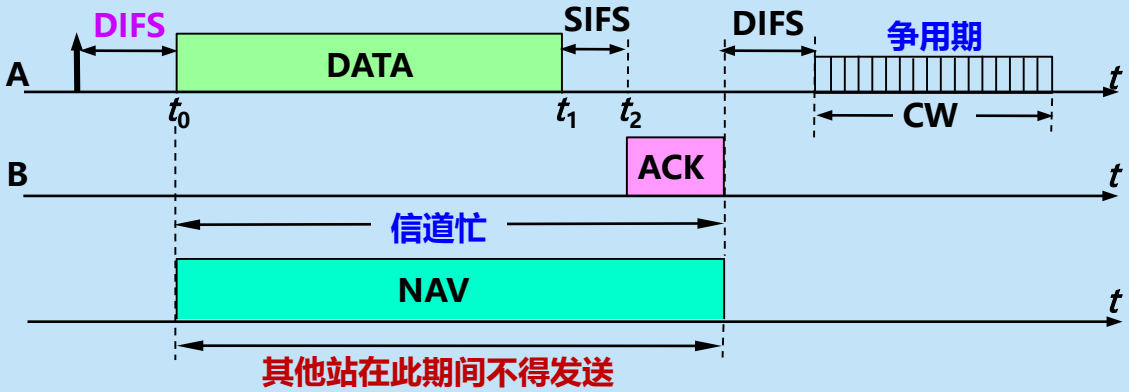
# DIFS

比 SIFS 的帧间间隔要长得多。在 DCF 方式中，DIFS 用来发送数据帧和管理帧。802.11 标准规定：凡在空闲时间想发送数据的站点，必须等待时间 DIFS 后才能发送。保证了确认帧 ACK 得以优先发送。



# DIFS 很重要

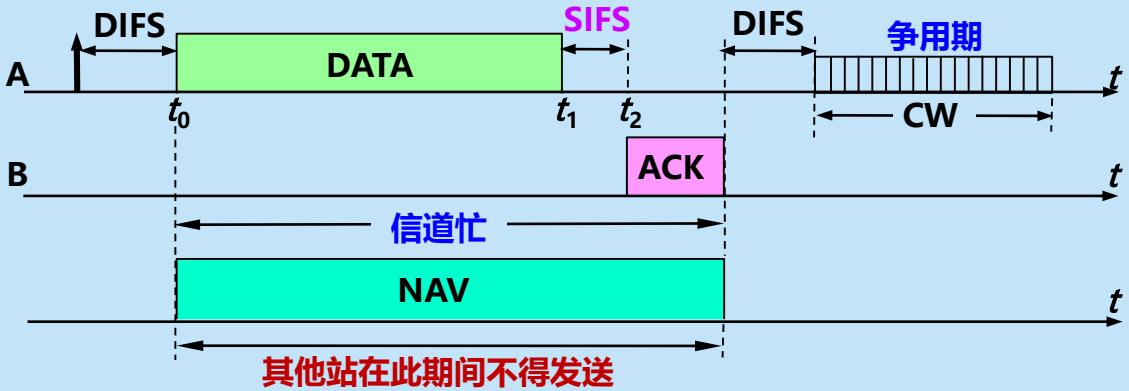
A 监听信道。若信道在时间间隔 DIFS 一直都是空闲的，A 就可以在 $t_0$ 时间发送数据帧 DATA。



# DIFS 很重要

B 收到数据帧后，必须进行 CRC 检验。若检验无差错，再从接收状态转为发送状态。经过时间间隔 SIFS 后，向 A 发送确认帧 ACK。

从 A 发送数据帧 DATA 开始，到收到确认 ACK 为止的这段时间 (DATA + SIFS + ACK) 内，必须不允许任何其他站发送数据，这样才不会发生碰撞。



# 避免发生碰撞的两种机制

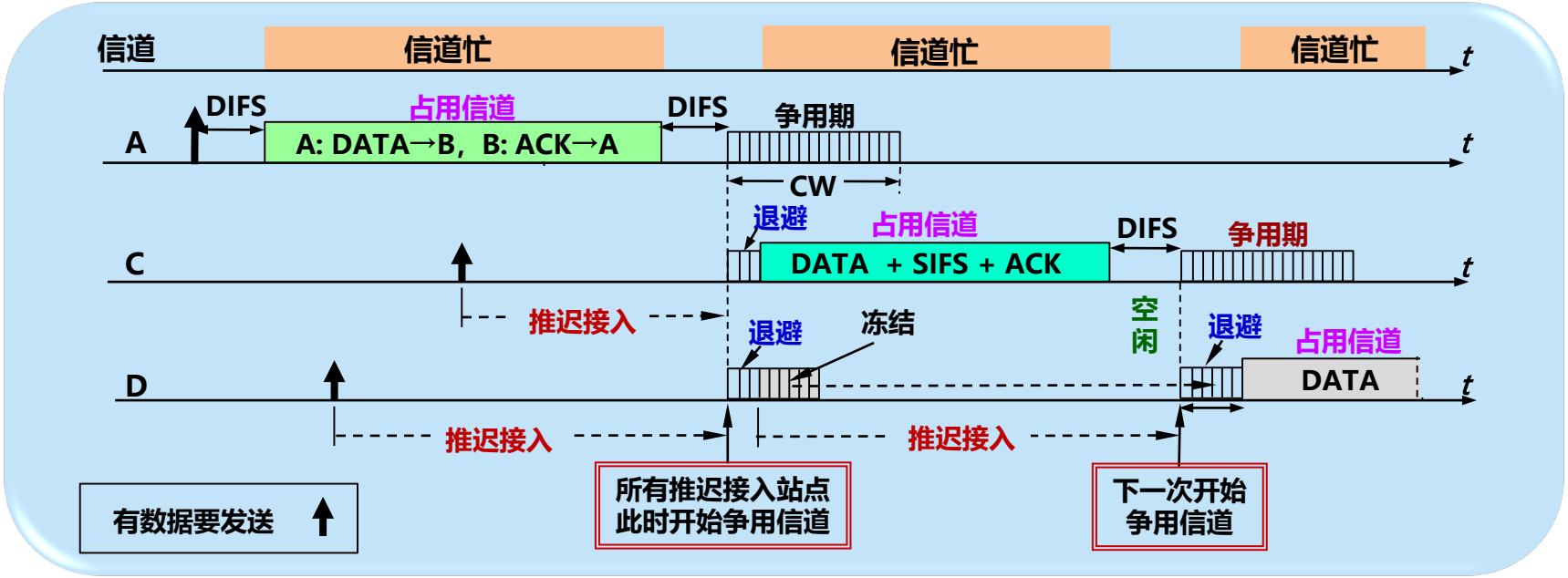
## 虚拟载波监听

- 软件实现。
- 源站 A 把要占用信道的时间（DATA + SIFS + ACK），写入其数据帧 DATA 的首部。
- 所有处在站点 A 的广播范围内的各站都能够收到这一信息，并创建自己的**网络分配向量 NAV** (Network Allocation Vector)。
- **NAV 指出**：信道忙的持续时间，意思是：“**其他站点不能在这段时间发送数据**”。

## 载波监听

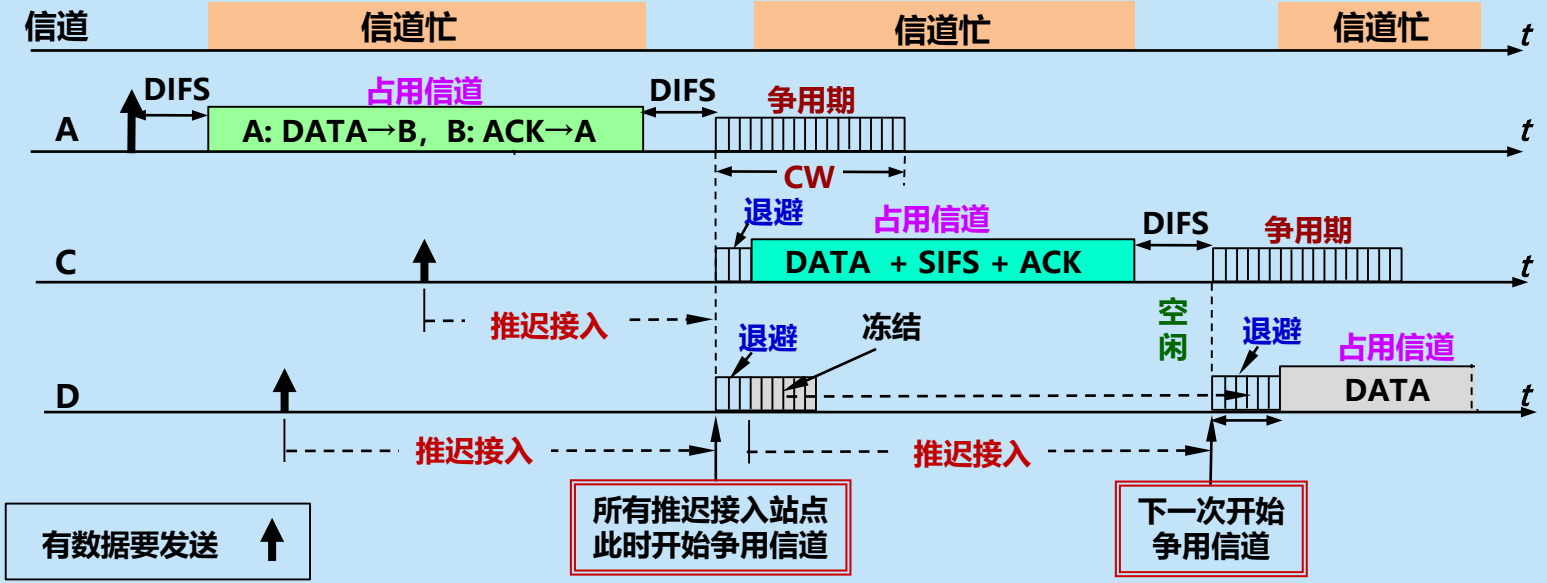
- 在物理层用硬件实现。
- 每个站检查收到的信号强度是否超过一定的门限数值，用此判断是否有其他移动站在信道上发送数据。
- 任何站要发送数据之前，必须监听信道。只要监听到信道忙，就不能发送数据。

# 3. 争用信道的过程



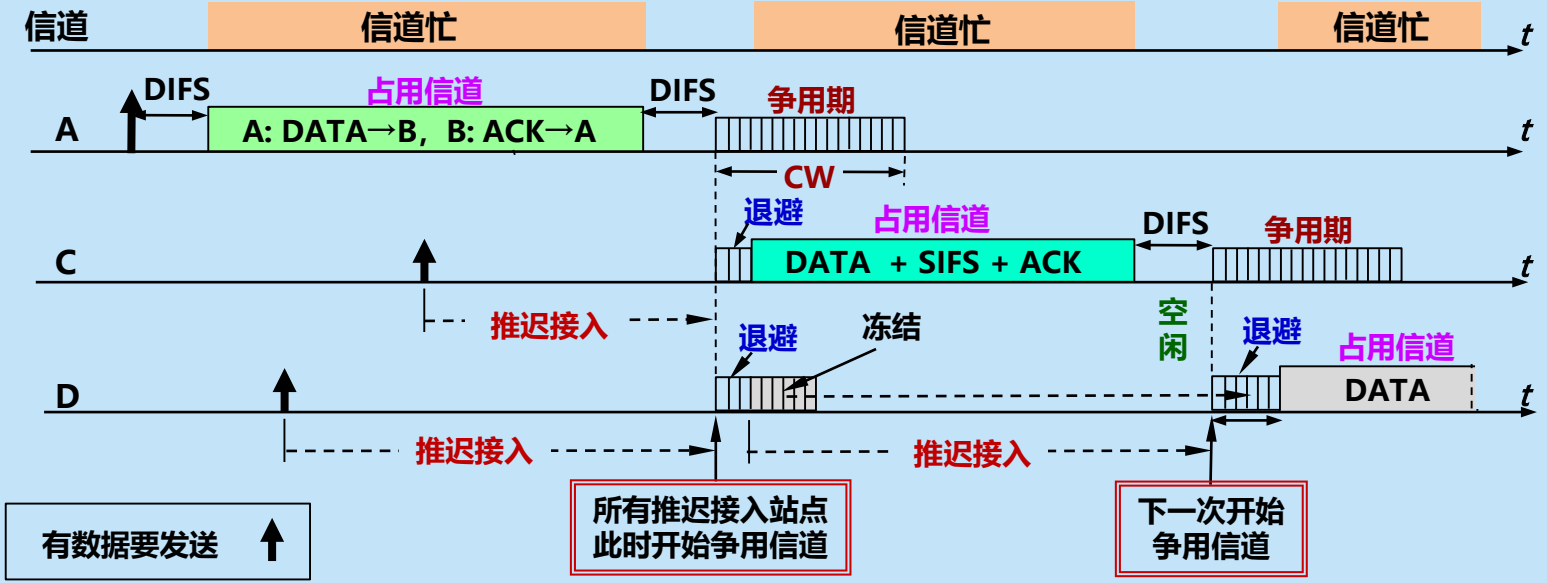

在站点 A 和 B 通信的过程中，站点 C 和 D 也要发送数据。但 C 和 D 检测到信道忙，因此必须**推迟接入**(defer access)，以免发生碰撞。

# 3. 争用信道的过程




在等待信道进入空闲状态后，都经过规定的时间间隔 DIFS 再同时发送数据必然产生碰撞。因此，CSMA/CA 规定：所有推迟接入的站都必须在**争用期**执行统一的**退避算法**开始**公平地争用信道**。

# 3. 争用信道的过程




争用期也叫做**争用窗口 CW** (Contention Window)。争用窗口由许多时隙 (time slot) 组成。例如，争用窗口 CW = 15 即窗口大小是 15 个时隙。

## 时隙长度的确定

- **方法：在下一个时隙开始时，每个站点都能检测出在前一个时隙开始时信道是否忙（这样就可采取适当对策）。**
- **时隙长短在不同 802.11 标准中可以有不同数值。**
- **例如：802.11g**
  - **一个时隙时间为 9us；**
  - **SIFS = 10 us；**
  - **DIFS = SIFS + (2 * Slot time) = 28us。**

## 退避算法

- 站点在**进入争用期**时，应在 0 ~ CW 个时隙中**随机**生成一个退避时隙数，并设置**退避计时器** (backoff timer)。
- 当几个站同时争用信道时，计时器**最先降为零**的站首先接入媒体，发送数据帧。这时信道转为忙，而其他正在退避的站则**冻结**其计时器，保留计时器的数值不变，推迟到下次争用信道时**接着倒计时。**
- 这样的规定对所有的站是**公平的。**

## “推迟接入”和“退避 (backoff)”的区别

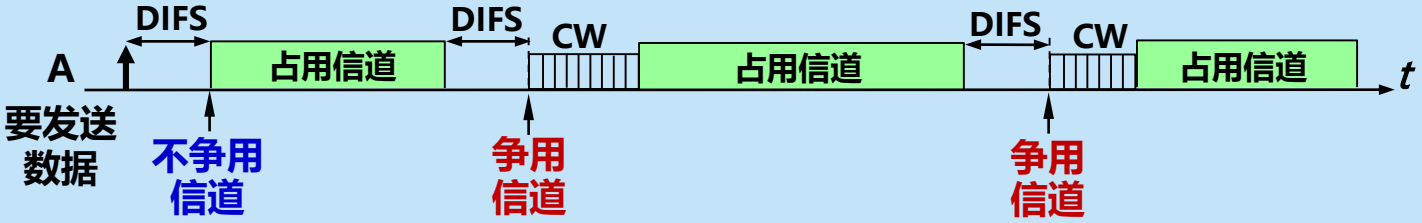
- **推迟接入：**
  - 发生在信道处于忙的状态，为的是等待争用期的到来，以便执行退避算法来争用信道。
  - 这时退避计时器处于冻结状态。
- **退避：**
  - 是争用期各站点执行的算法，退避计时器进行倒计时。
  - 这时信道是空闲的，并且总是出现在时间间隔 DIFS 的后面。

## 争用窗口

- **建议值：** 15 (最小) ≤ 争用窗口 CW ≤ 1023 (最大)。
- **CSMA/CA规定：** 如果未收到确认帧，则必须重传。但每重传一次，争用窗口的数值就近似加倍。
- **假定：** 选择初始争用窗口 CW = $2^4 - 1 = 15$，第 $i$ 次退避就在 $2^{4+i} - 1$ 个时隙中随机地选择一个，即：
  - 第 1 次重传时，随机退避的时隙数应在 0 ~ 31 之间生成。
  - 第 2 次重传时，随机退避的时隙数应在 0 ~ 63 之间生成。
  - 第 3 次重传时，随机退避的时隙数应在 0 ~ 127 之间生成。
  - 第 4 次重传时，随机退避的时隙数应在 0 ~ 255 之间生成。
  - 第 5 次重传时，随机退避的时隙数应在 0 ~ 511 之间生成。
  - 第 6 次以及 6 次以上重传时，随机退避的时隙数应在 0 ~ 1023 之间生成，争用窗口 CW 不再增大了。

## 退避算法的使用场景

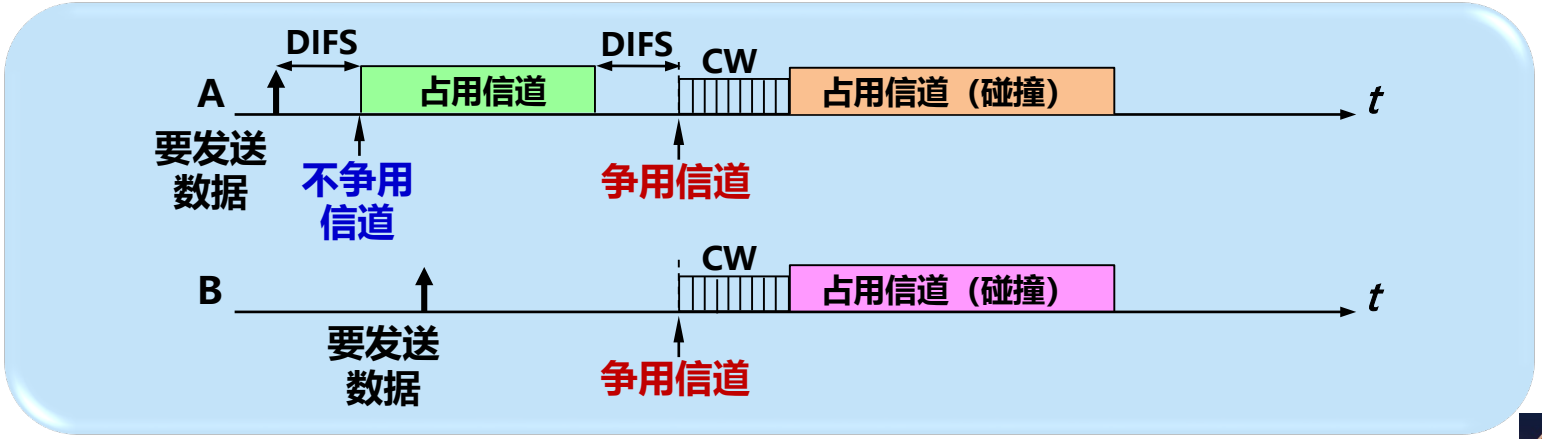
1. 要发送数据时检测到信道忙。
2. 已发出的数据帧未收到确认，重传数据帧。
3. 接着发送后续的数据帧（为了防止一个站长期垄断发送权）。



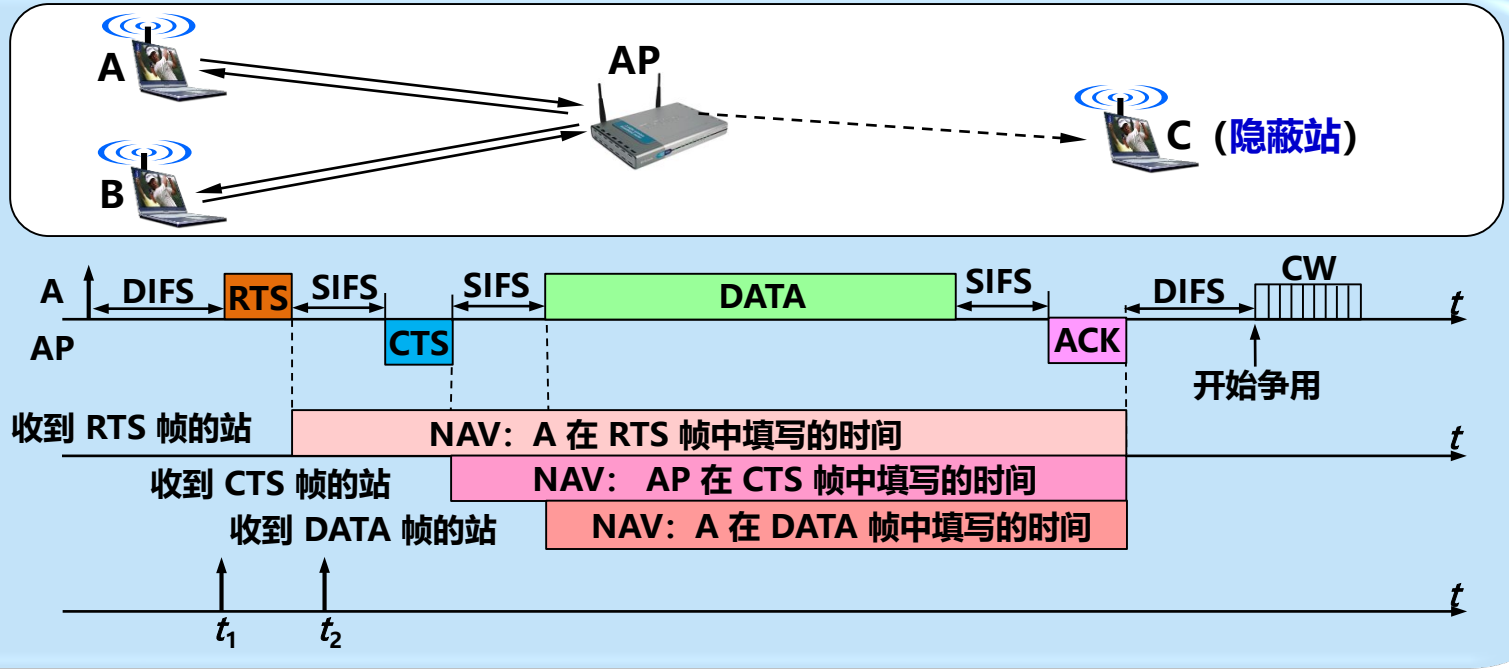

当站点想发送数据，并检测信道连续空闲时间超过 DIFS 时，即可立即发送数据，而不必经过争用期。

# 4. 对信道进行预约

- **假设：** B 站正好在 A 占用信道时要发送数据。B 检测到信道忙，于是推迟到争用信道时与 A 一起争用信道。但正巧 A 和 B 又生成了同样大小的随机退避时隙数。结果就发生了碰撞，A 和 B 都必须再重传。
- 为进一步减少碰撞，还需要再采用一些措施：**信道预约。**

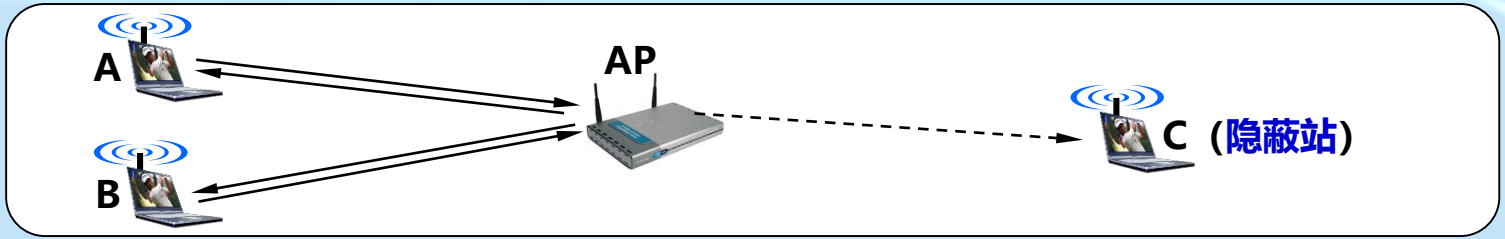


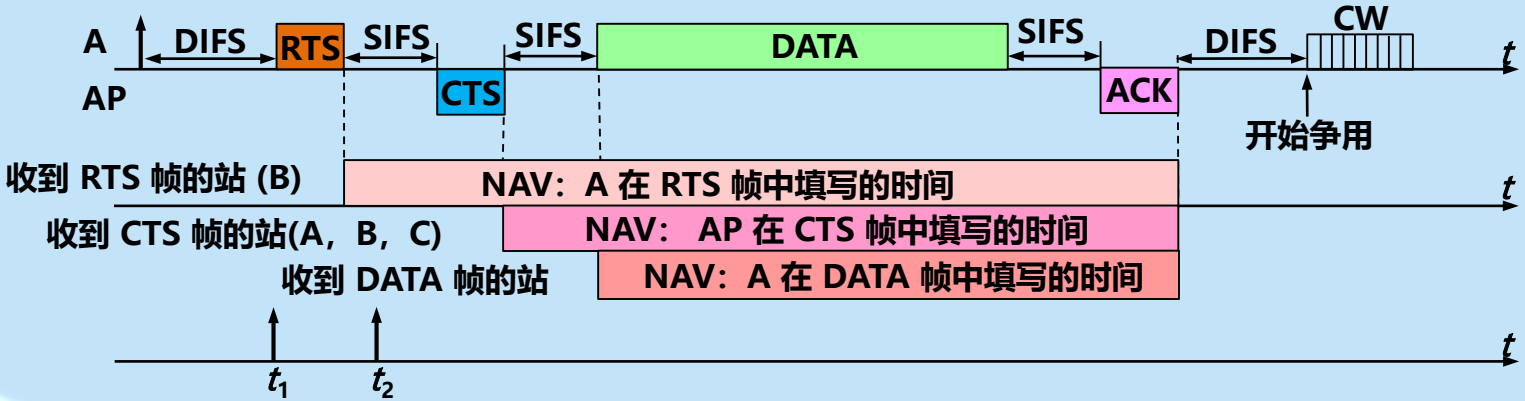
# 4. 对信道进行预约



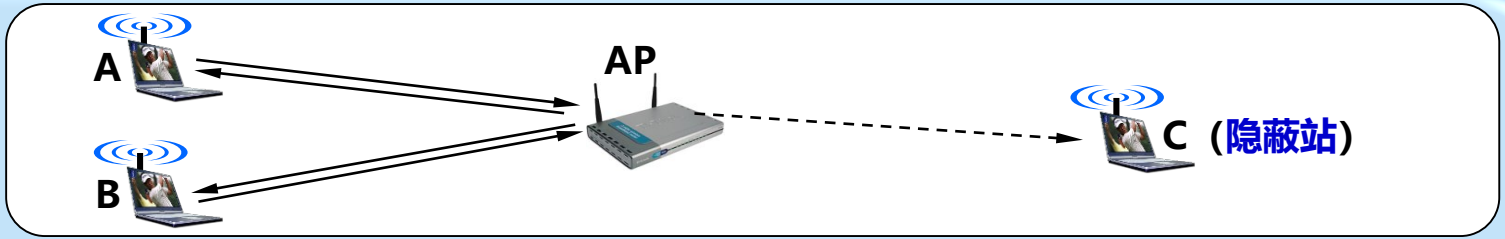

**隐蔽站问题：** A 站或 B 站向接入点 AP 发送数据时， C 站接收不到这些信号。C 站向 AP 发送的信号也传播不到远处的 A 站或 B 站。

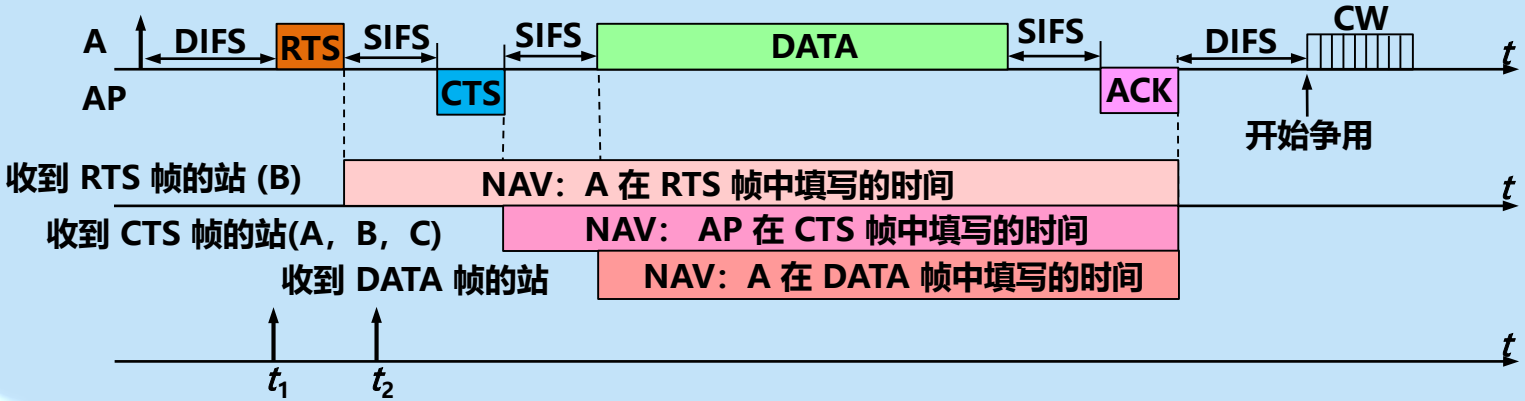
# 4. 对信道进行预约


A
B
AP
C（隐蔽站）

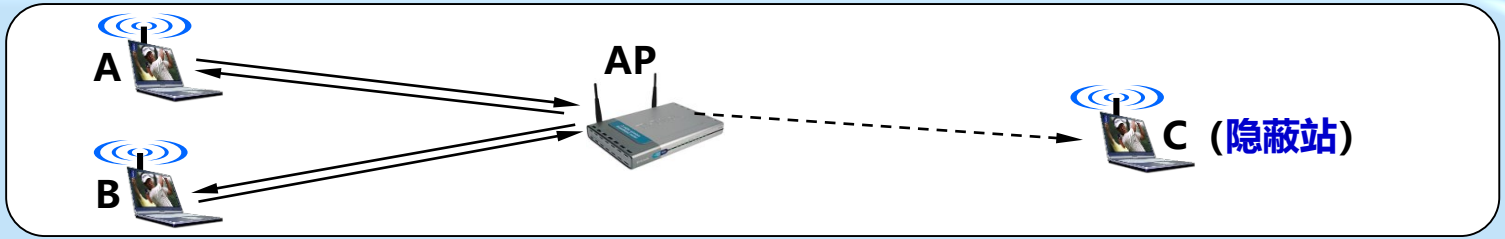

A
AP
DIFS
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
CW
开始争用
t
收到 RTS 帧的站 (B)
NAV：A 在 RTS 帧中填写的时间
收到 CTS 帧的站(A，B，C)
NAV： AP 在 CTS 帧中填写的时间
收到 DATA 帧的站
NAV：A 在 DATA 帧中填写的时间
t1
t2

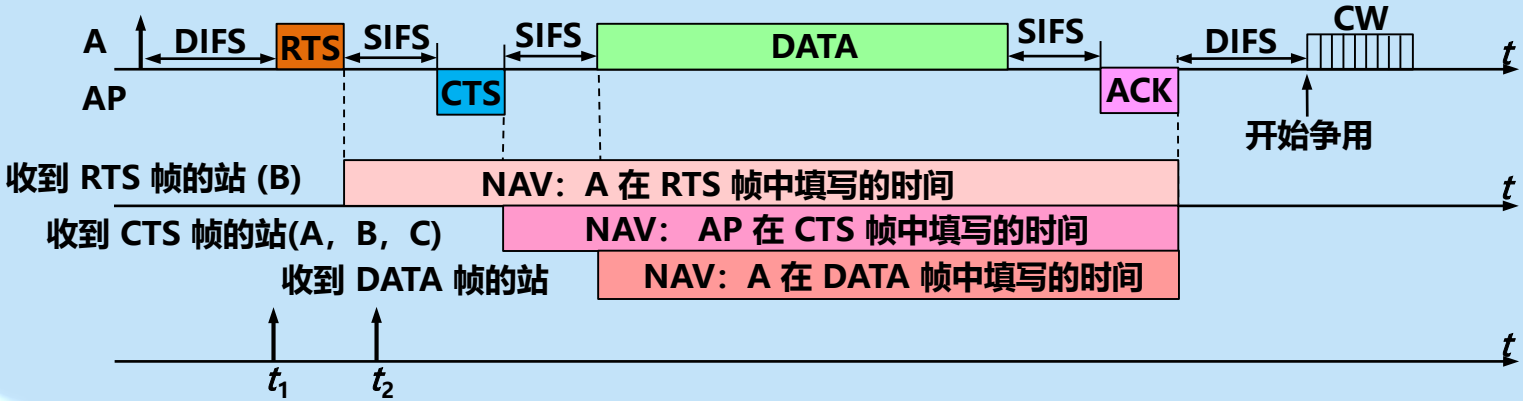
# 4. 对信道进行预约


A
B
AP
C（隐蔽站）


A
AP
DIFS
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
CW
开始争用
t
收到 RTS 帧的站 (B)
NAV：A 在 RTS 帧中填写的时间
收到 CTS 帧的站(A，B，C)
NAV： AP 在 CTS 帧中填写的时间
收到 DATA 帧的站
NAV：A 在 DATA 帧中填写的时间
t1
t2

# 4. 对信道进行预约




以上措施使得 A 站和接入点 AP（以及 A 站和 B 站）的通信过程中，发生碰撞的概率大大降低，特别是减少了隐蔽站的干扰问题。

## 信道预约

- 使用 RTS 帧和 CTS 帧会使整个网络的通信效率有所下降，多浪费信道的时间 [RTS + SIFS + CTS + SIFS]。
- 但与数据帧相比，开销不算大。这两种控制帧都很短，其长度分别为 20 字节和 14 字节。而数据帧最长可达 2346 字节。
- 若不使用这种控制帧，一旦发生碰撞而导致数据帧重发，浪费的时间就更多。

## 信道预约不能完全避免碰撞

- 即使使用了 RTS 和 CTS 对信道进行预约，但碰撞也有可能发生。
- 例如：有的站可能在时间 $t_1$ 或 $t_2$ 就发送了数据（这些站可能是没有收到 RTS 帧或 CTS 帧或 NAV），结果必定与 RTS 帧或 CTS 帧发生碰撞。
- A 站若收不到 CTS 帧，就不能发送数据帧，而必须重传 RTS 帧。
- A 站只有正确收到 CTS 帧后才能发送数据帧。

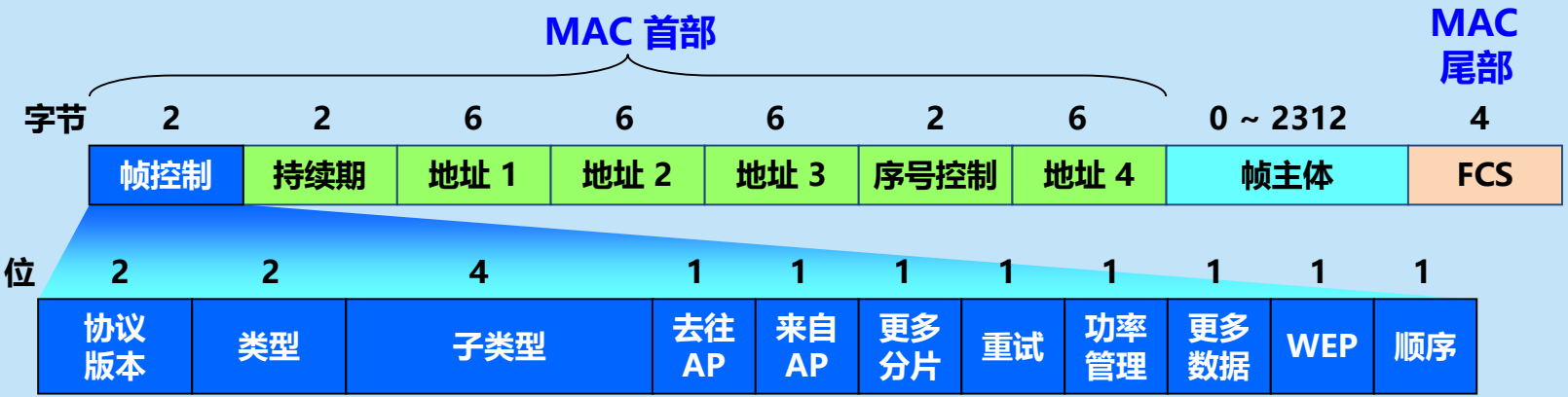
## 信道预约不是强制的

- 信道预约**不是强制性**规定。各站可以自己决定使用或不使用信道预约。
- 只有当数据帧的长度**超过**某一数值时，使用 RTS 帧和 CTS 帧才比较合适。
- 因为无线信道的误码率比有线信道的高得多，所以，无线局域网的 MAC 帧长一般应当短些，以便在出错重传时减小开销。

# 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）**

| 字节 | 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|---|
| | 帧控制 | 持续期 | 接收地址 | 发送地址 | FCS |

**CTS 和 ACK 帧格式（帧控制字段中的子类型分别为 1100 和 1101）**

| 字节 | 2 | 2 | 6 | 4 |
|---|---|---|---|---|
| | 帧控制 | 持续期 | 接收地址 | FCS |

## 802.11 数据帧的三大部分

- **MAC 首部**：共 30 字节。复杂。
- **帧主体**：数据部分，不超过 2312 字节。802.11 帧的长度通常都小于 1500 字节。
- **帧检验序列 FCS**：尾部，共 4 字节 。

# 1. 关于 802.11 数据帧的地址

- 数据帧有四个地址字段。

| 去往 AP | 来自 AP | 地址 1 | 地址 2 | 地址 3 | 地址 4 |
|---|---|---|---|---|---|
| | | 接收地址 | 发送地址 | ? | ? |

地址 1 永远是接收地址（即直接接收数据帧的节点地址）。

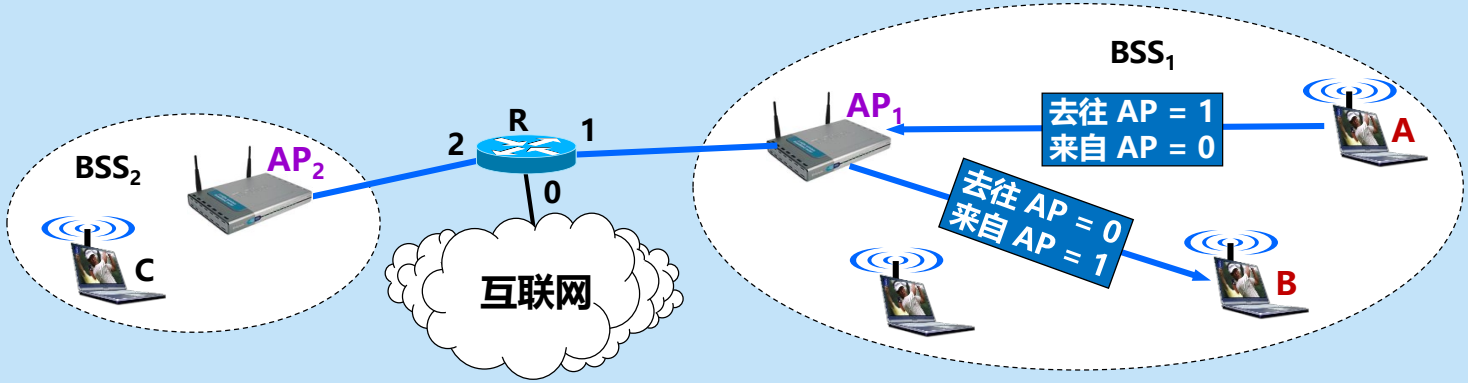
地址 2 永远是发送地址（即实际发送数据帧的节点地址）。

地址 3 和地址 4 取决于数据帧中的“来自AP”和“去往AP”这两个字段的数值。

注意：上述地址都是 MAC 地址，即硬件地址，而 AP 的 MAC 地址是 BSSID。

# 最常用的两种情况

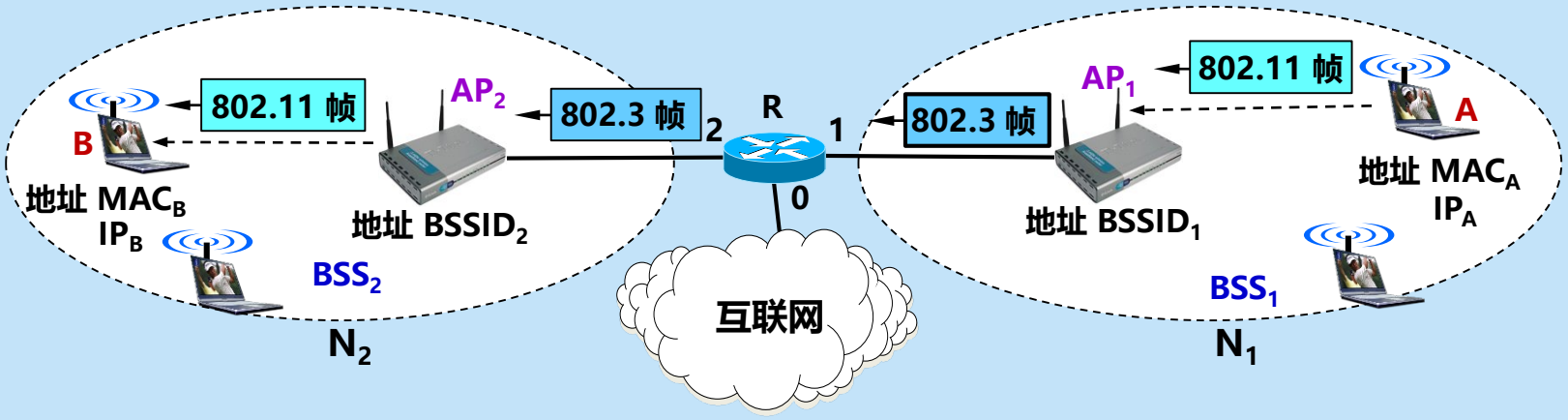
站点 A 向 B 发送数据帧，数据帧必须经过 $AP_1$ 转发。




| 数据报流向 | 去往 AP | 来自 AP | 地址 1 | 地址 2 | 地址 3 | 地址 4 |
|---|---|---|---|---|---|---|
| A → $AP_1$ | 1 | 0 | $AP_1$ 地址 | A 的地址 | B 的地址 | — |
| $AP_1$ → B | 0 | 1 | B 的地址 | $AP_1$ 地址 | A 的地址 | — |

# 复杂情况：站点处在不同的两个子网中

站点 A 向 B 发送数据帧，必须经过路由器 R 和 $AP_2$ 向 B 转发。



# 复杂情况：站点处在不同的两个子网中

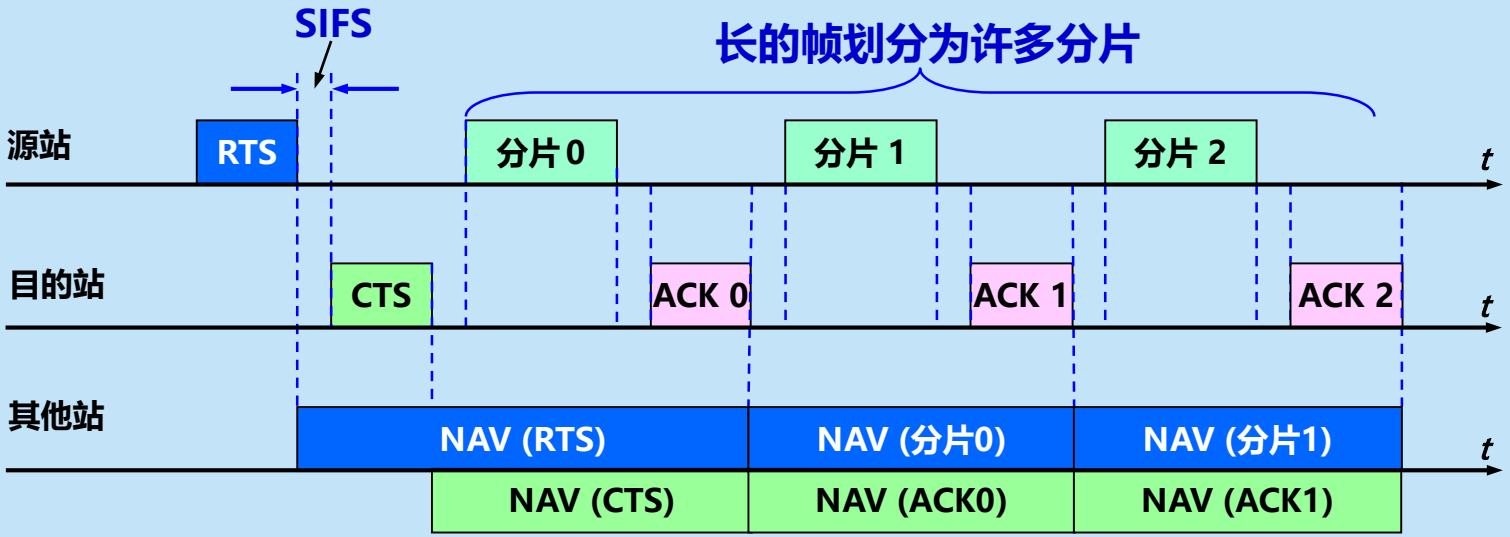
| 数据报流向 | 去往 AP | 来自 AP | 地址 1 | 地址 2 | 地址 3 | 地址 4 |
|---|---|---|---|---|---|---|
| A → $AP_1$ | 1 | 0 | $AP_1$ 地址的 $BSSID_1$ | A 的地址 $MAC_A$ | R 接口 1 地址 $MAC_{R-1}$ | —— |
| $AP_1$ → R (以太网帧) | 目的 MAC 地址 = $MAC_{R-1}$ | | 源 MAC 地址 = $MAC_A$ | | | |
| R → $AP_2$ (以太网帧) | 目的 MAC 地址 = $MAC_B$ | | 源 MAC 地址 = $MAC_{R-2}$ | | | |
| $AP_2$ → B | 0 | 1 | B 的地址 $MAC_B$ | $AP_2$ 的 $BSSID_2$ | R 接口 2 地址 $MAC_{R-2}$ | —— |

## 2. 序号控制字段、持续期字段和帧控制字段

- **序号控制**：占 16 位，其中序号子字段占 12 位，分片子字段占 4 位。
- **持续期**：占 16 位。
- **帧控制**：共分为 11 个子字段：
  1. **协议版本**：现在是 0。
  2. **类型**和**子类型**：用来区分帧的功能。
  3. **更多分片**：置为 1 时表明这个帧属于一个帧的多个分片之一。
  4. **功率管理**：占 1 位，用来指示移动站的功率管理模式。
  5. **WEP**：占 1 位。若 WEP = 1，表明对帧主体字段采用了加密算法。

# 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。



# 9.2 无线个人区域网WPAN

- **无线个人区域网 WPAN** (Wireless Personal Area Network)：在个人工作地方把属于个人使用的电子设备用无线技术连接起来**自组网络**，不需要使用接入点 AP。
- 整个网络的范围大约在 10 m 左右。
- WPAN 可以是一个人使用，也可以是若干人共同使用。
- 与**个人区域网 PAN** (Personal Area Network) 并不完全等同，因为 PAN 不一定都是使用无线连接的。

# WPAN 和 WLAN 不一样

- **WPAN：**
  - 是以个人为中心使用的无线个人区域网；
  - 实际上是一个低功率、小范围、低速率和低价格的电缆替代技术。
- **WLAN：**
  - 是同时为许多用户服务的无线局域网；
  - 是一个大功率、中等范围、高速率的局域网。

# WPAN 标准

- 由 IEEE 的 802.15 工作组制定，包括 MAC 层和物理层的标准。
- WPAN 都工作在 2.4 GHz 的 ISM 频段。
- 欧洲的 ETSI 标准则把无线个人区域网取名为 HiperPAN。

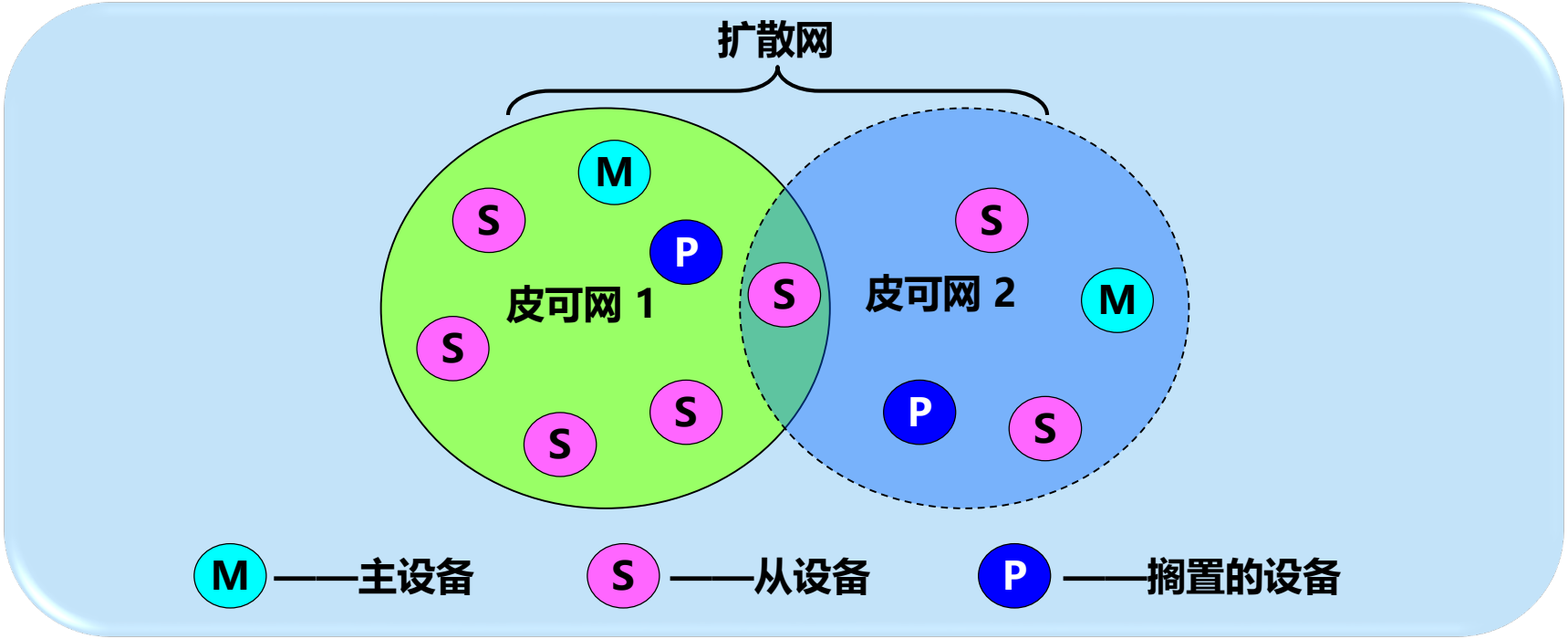
# 1. 蓝牙系统 (Bluetooth)

- 最早使用的 WPAN。
- 1994 年，由爱立信公司推出，其标准是 IEEE 802.15.1 。
- **第 1 代蓝牙**：数据率 = 720 kbit/s，通信范围 = 10 米左右。
- **蓝牙 4.0**：
  - **低耗能蓝牙 BLE** (Bluetooth Low Energy)：
    - 适用于数据量很小的节点，电池可以连续工作 4 ~ 5 年；
    - 距离增大到 30 m，数据率可达 1 Mbit/s。
  - **传统蓝牙** (classic Bluetooth)：
    - 数据率提高到 3 Mbit/s，传输距离可达 100 m。
- **蓝牙 5.0**：数据率上限达 24 Mbit/s，传输距离最高可达 300 m。

## 皮可网 (piconet)

- 蓝牙使用 TDM 方式和扩频跳频 FHSS 技术组成不用接入点 AP 的皮可网 (piconet)。
- 每一个皮可网有一个主设备 (Master) 和最多 7 个工作的从设备 (Slave)。
- 通过共享主设备或从设备，可以把多个皮可网链接起来，形成一个范围更大的扩散网 (scatternet)。

# 蓝牙系统中的皮可网和扩散网



## 2. 低速 WPAN

- 主要用于工业监控组网、办公自动化与控制等领域
- 速率是 2 ~ 250 kbit/s。
- 标准是 IEEE 802.15.4。新修订的标准是 IEEE 802.15.4-2006。
- 低速 WPAN 中最重要的就是 ZigBee。
- ZigBee 技术主要用于各种电子设备（固定的、便携的或移动的）之间的无线通信。

## ZigBee 的特点

- 通信距离短 (10 ~ 80 m)，传输数据速率低，成本低廉。
- 功耗非常低
  - 对于某些工作时间和总时间之比小于 1% 的情况，电池的寿命甚至可以超过 10 年。
- 网络容量大
  - 一个 ZigBee 的网络最多包括有 255 个结点，其中一个是主设备，其余则是从设备。
  - 若是通过网络协调器，整个网络最多可以支持超过 64000 个结点。

# ZigBee 标准与协议栈


在 IEEE 802.15.4 标准基础上发展而来。所有 ZigBee 产品也是 802.15.4 产品。IEEE 802.15.4 只是定义了 ZigBee 协议栈的**最低的两层**（物理层和 MAC 层），而上面的两层（网络层和应用层）则是由 ZigBee 联盟定义的。

# ZigBee 标准与协议栈

- IEEE 802.15.4 物理层使用的三个频段

| 频段 | 数据率 | 信道数 |
| --- | --- | --- |
| 2.4 GHz（全球） | 250 kbit/s | 16 |
| 915 MHz（美国） | 40 kbit/s | 10 |
| 868 MHz（欧洲） | 20 kbit/s | 1 |

- MAC 层主要沿用 802.11 无线局域网标准的 CSMA/CA 协议。
- 在网络层，ZigBee 可采用星形和网状拓扑，或两者的组合。

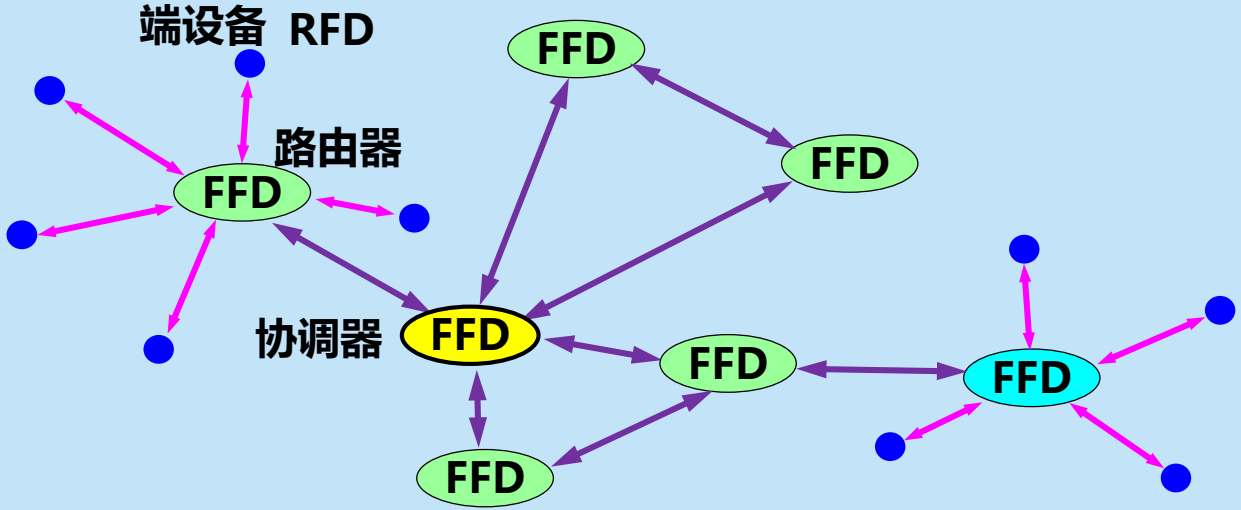
# ZigBee 的组网方式

- 一个 ZigBee 网络最多可以有 255 个节点。
- 节点按功能的强弱可划分为**两大类**：

1. **全功能设备** FFD (Full-Function Device)
   - ① 充当**协调器** (coordinator)，负责维护整个 ZigBee 网络的节点信息，同时还可以与其他 ZigBee 网络的协调器交换数据。
   - ② 通过各网络协调器的相互通信，可以得到覆盖更大范围、超过 65000 个节点的 ZigBee网络。
2. **精简功能设备** RFD (Reduced-Function Device)
   - ① 是 ZigBee 网络中数量最多的**端设备**。
   - ② 电路简单，存储容量较小，因而成本较低。
   - ③ RFD 结点**只能**与处在该星形网中心的 FFD 结点交换数据。

# ZigBee 的组网方式

有一个全功能设备 FFD 充当网络的协调器。
ZigBee 网络中数量最多的端设备是精简功能设备 RFD 结点。



# 3. 高速 WPAN

- 用于在便携式多媒体装置之间传送数据，支持11 ~ 55 Mbit/s 的数据率，标准是 802.15.3。
- IEEE 802.15.3a 工作组还提出了更高数据率的物理层标准的超高速 WPAN，使用超宽带 UWB 技术：
  - 工作在 3.1 ~ 10.6 GHz 微波频段，有非常高的信道带宽。
  - 信号的带宽应超过信号中心频率的 25% 以上，或信号的绝对带宽超过 500 MHz。
  - 使用了瞬间高速脉冲，可支持 100 ~ 400 Mbit/s 的数据率，可用于小范围内高速传送图像或 DVD 质量的多媒体视频文件。