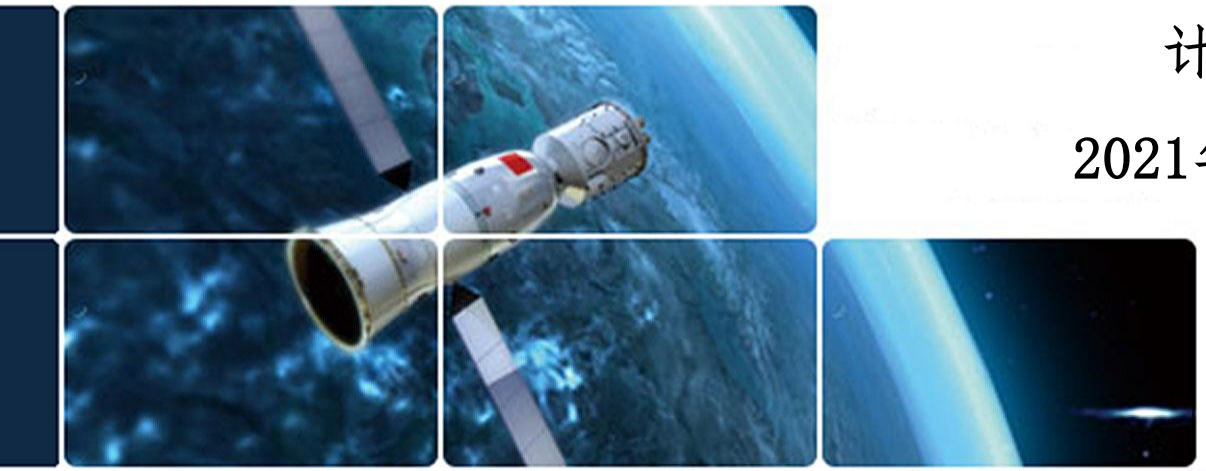
# 无线局域网（WLAN）技术



计算学部

2021年10月26日

# Question?

1. （1）移动互联网用户多址接入方式包括如下哪几种（　　）；（2）5G 移动通信网络最普遍采用的多址接入方式是（　　）。

（A）码分多址 CDMA　　（B）时分多址 TDMA

（C）频分多址 FDMA　　（D）空分多址 SDMA

2. （1）移动互联网接入技术包括如下哪几种（　　）；（2）你认为目前应用最普遍的移动互联网接入技术是（　　）；（3）为了快速访问校园网资源，哈工大校园内移动终端普遍采用接入技术是（　　）。

（A）无线局域网 WLAN 接入　　（B）无线个域网 WPAN 接入

（C）无线城域网 WMAN 接入　　（D）无线广域网 WWAN 接入

# 主要内容

- WLAN无线组网
- IEEE 802.11物理层
- IEEE 802.11MAC子层
- IEEE 802.11服务

# 无线局域网中用户的关注点

- 传输速度和人数
- 传输距离
- 是否支持漫游
- 认证方式

- 无线电辐射与干扰
- 是否安全
- 多信道干扰

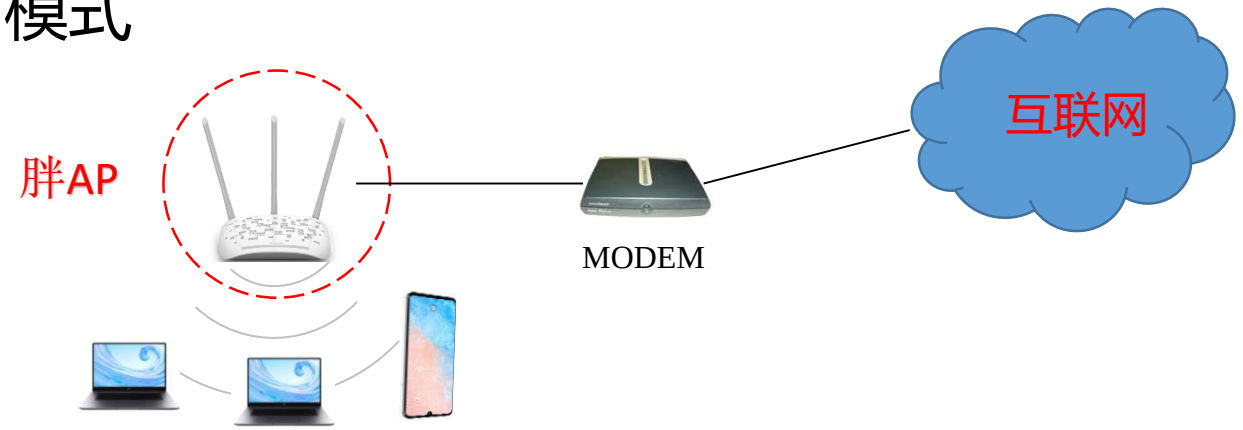
# 胖AP设备


- 天线
- 802.11 a/b/g/n/ac/ax
- 加密
- 802.1X认证
- 漫游
- 网管

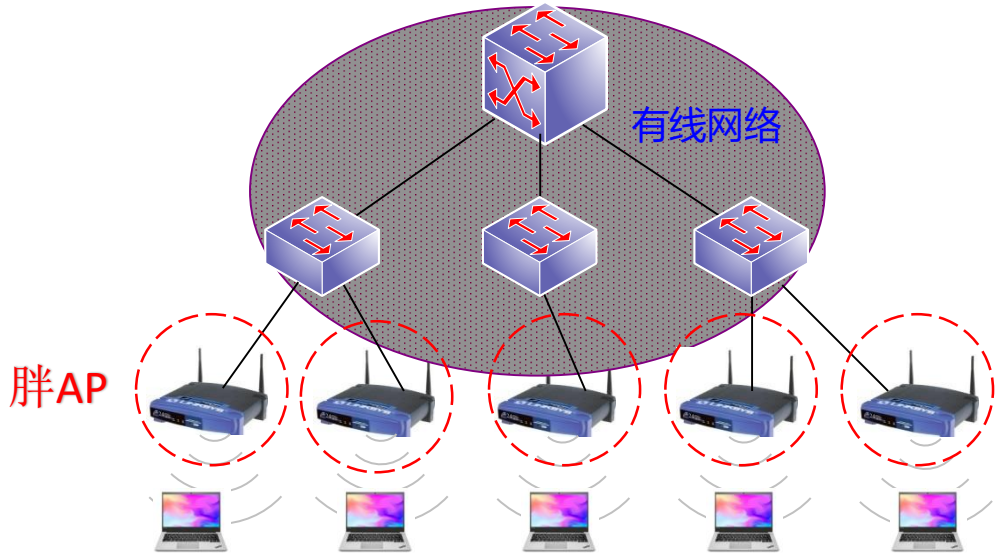
□胖*AP*集*WLAN*物理层、MAC层功能与一体，主要包括信号调制、信号发射、数据加密、用户认证、QOS、信号漫游、网络管理等功能

# 胖AP应用

1. 家庭或*SOHO*网络组网模式




2. 企业网络组网模式



# 胖AP的局限性

1. 利用胖***AP*** 组建大、中型无线网络时，配置工作量大

2. 对胖***AP*** 进行软件升级时，需要手工逐台进行升级，维护工作量大

3. 胖***AP***上保存着设备配置信息，当设备失窃时造成配置信息泄漏

4. 胖***AP*** 难于实现自动无线盲区修补、流氓***AP*** 检测等功能

**胖AP适用于小型无线网络部署，不适用于大规模网络部署！**

# WLAN产品架构的演进

瘦AP

瘦AP功能

802.11物理层功能

胖AP功能

802.11物理层功能

802.11MAC层功能

802.11 QOS功能

802.11 认证及加密功能

功能分离

胖AP

AC无线控制器功能

802.11MAC层功能

802.11 QOS功能

802.11 认证及加密功能

1. ***AP***控制与配置（**CAPWAP**）
2. ***AP*** 管理
3. 射频环境监控、射频配置
4. ***STA***数据管理
5. ***AC/AP***通信


**AC无线控制器**

# 为什么需要瘦AP

- 大型无线网络的挑战
  - 管理、监测及控制大量 ***AP***
  - 对大量 ***AP*** 配置及升级
  - ***WLAN*** 空口传输不稳定，易受干扰，需要对多AP之间无线干扰、信道转换、功率调整等进行集中控制，避免干扰，防止入侵，稳定整体性能
  - ***WLAN*** 安全要求提升

- 规模化组网运营必须采用瘦AP架构
  - 可集中完成AP配置更改、监控和管理，增强了对用户和业务的控制
  - 在各种组网模式下可实现对AP的统一管理，组网设计更灵活
  - 可整体降低网络故障率

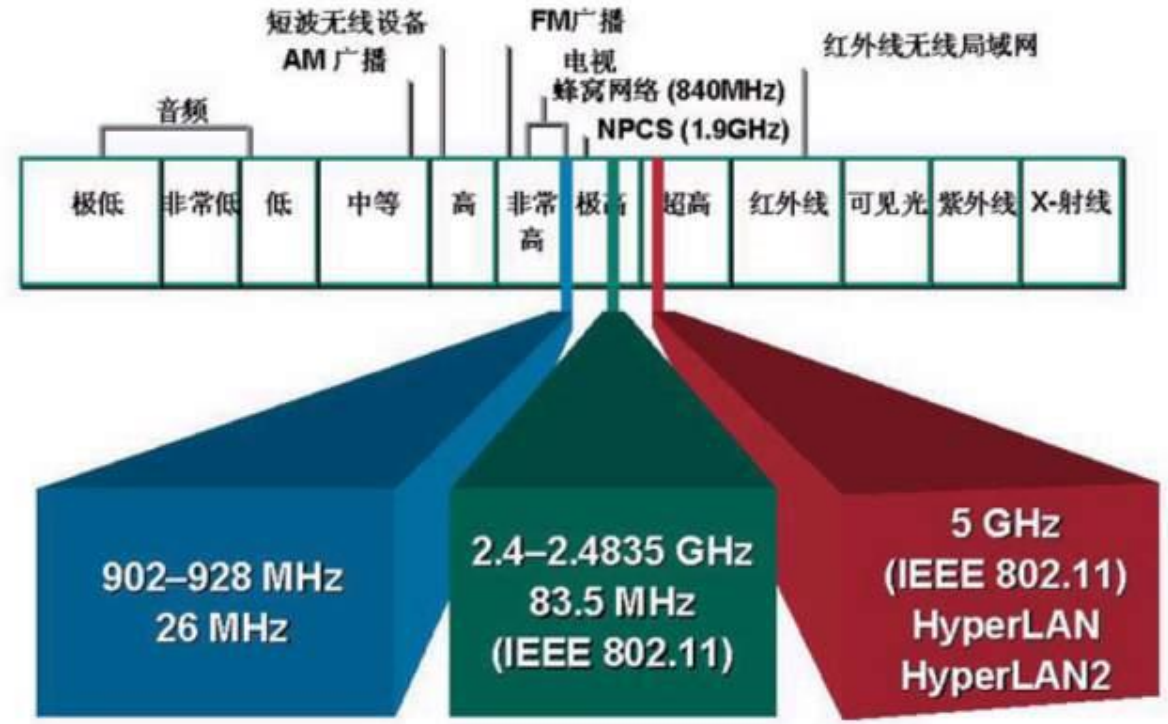
# 胖/瘦AP的比较

| | 胖AP方案 | 瘦 AP方案 |
|---|---|---|
| 技术模式 | 传统方式 | 增强管理 |
| 安全性 | 传统加密、认证方式，普通安全性 | 增加射频环境监控，基于用户位置安全策略，高安全性 |
| 网络管理 | 对每AP下发配置文件 | AC上分组批量配置，AP本身零配置 |
| WLAN组网规模 | 适合小规模组网 | 拓扑无关，适合大规模组网 |
| 增值业务能力 | 实现简单数据接入 | 可扩展更多丰富业务 |

# 主要内容

- WLAN无线组网
- IEEE 802.11物理层
- IEEE 802.11MAC子层
- IEEE 802.11服务

# 无线频段的分布




**ISM (*Industrial Scientific Medical*) 频段**

- ***ISM***：工业、科学和医疗频段，无需许可，需遵守一定发射功率，不干扰其它频段即可
- ***2.4GHz***为各国共同的***ISM***频段，无线网络均可工作在***2.4GHz***频段
- 我国***ISM***频段有***433.05~434.79MHz***、***2400~2483.5MHz***、***5725~5850MHz***

# 我国2.4GHz 信道划分

- 2.4GHz频段可用带宽为83.5MHz，划分为13个信道，每个信道带宽为22MHz

| 信道 | 中心频率（MHz） | 信道低端/高端频率（MHz） |
|---|---|---|
| 1 | 2412 | 2401/2423 |
| 2 | 2417 | 2406/2428 |
| 3 | 2422 | 2411/2433 |
| 4 | 2427 | 2416/2438 |
| 5 | 2432 | 2421/2443 |
| 6 | 2437 | 2426/2448 |
| 7 | 2442 | 2431/2453 |
| 8 | 2447 | 2426/2448 |
| 9 | 2452 | 2441/2463 |
| 10 | 2457 | 2446/2468 |
| 11 | 2462 | 2451/2473 |
| 12 | 2467 | 2456/2478 |
| 13 | 2472 | 2461/2483 |

# 我国5.8GHz 信道划分

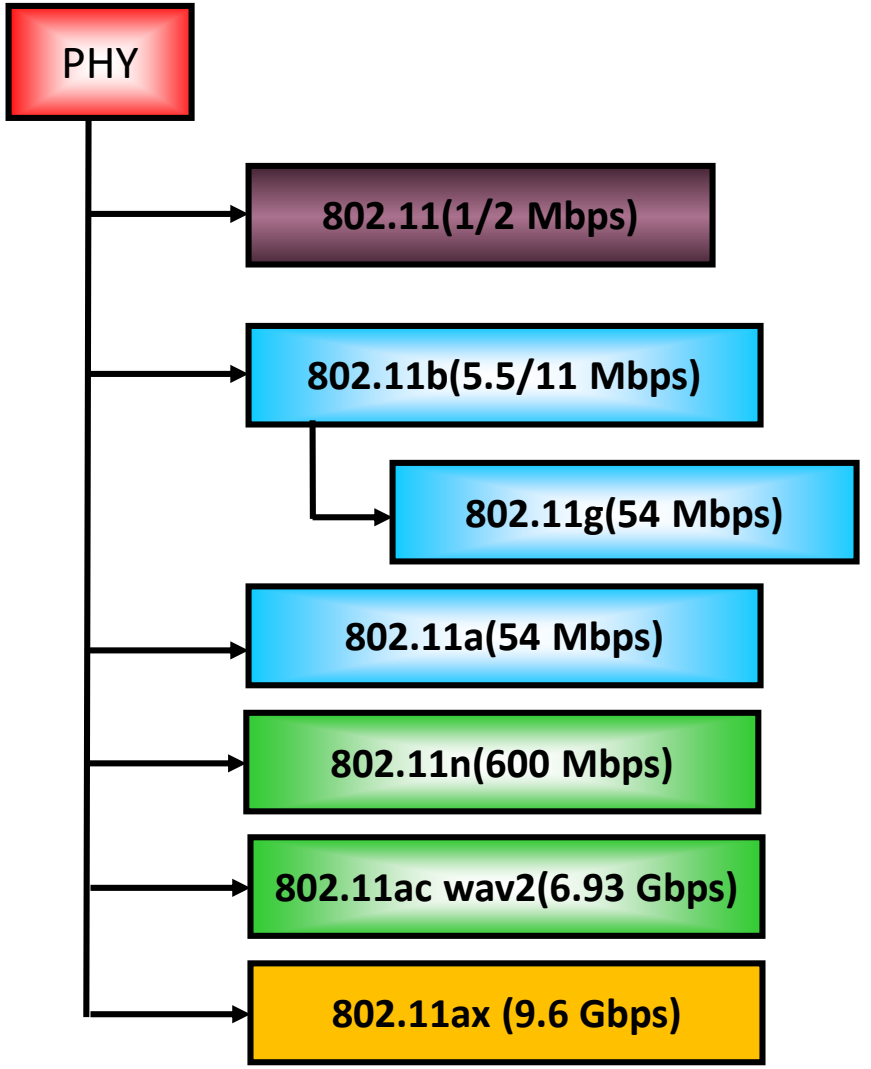
- 5.8GHz（5725~5850MHz）频段可用带宽为125MHz，划分为5个信道，每个信道带宽为20MHz

| 信道 | 中心频率（MHz） | 信道低端/高端频率（MHz） |
|---|---|---|
| 1 | 5745 | 5735/5755 |
| 2 | 5765 | 5755/5775 |
| 3 | 5785 | 5775/5795 |
| 4 | 5805 | 5795/5815 |
| 5 | 5825 | 5815/5835 |

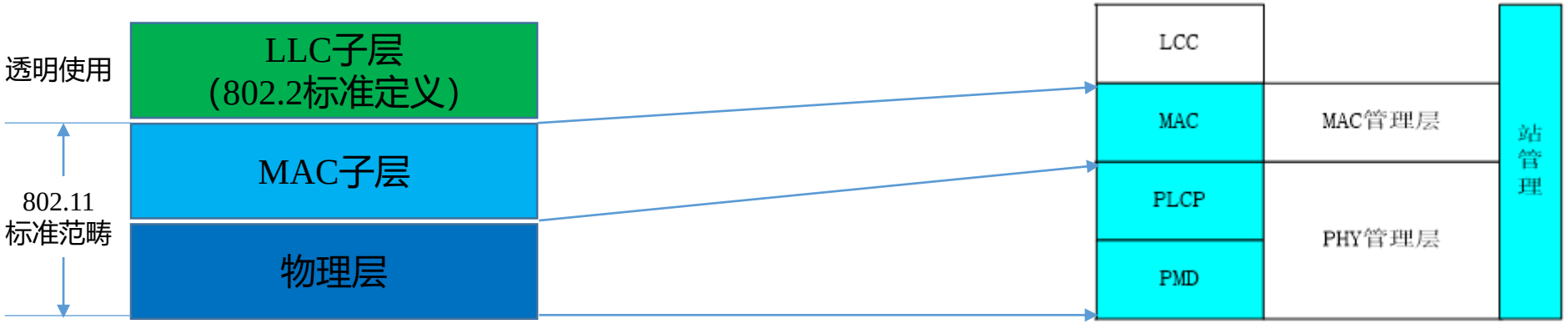
# IEEE 802.11标准演进

当前主流

| 标准号 | IEEE 802.11b | IEEE 802.11a | IEEE 802.11g | IEEE 802.11n | IEEE 802.11ac | IEEE 802.11ax |
|---|---|---|---|---|---|---|
| 标准时间 | 1999年9月 | 1999年9月 | 2003年6月 | 2009年9月 | 2013 Wave1<br>2016 Wave2 | 2019年9月 |
| 工作频率（GHz） | 2.4GHz | 5.0GHz | 2.4GHz | 2.4GHz<br>5.0GHz<br>（Wi-Fi 4） | 5.0GHz<br>（Wi-Fi 5） | 2.4GHz<br>5GHz<br>（Wi-Fi 6） |
| 物理速率（Mbps） | 11 | 54 | 54 | 600 | 6930 | 9600 |
| 实际吞吐量（Mbps） | 6 | 24 | 24 | 100以上 | 1300 | 数千兆 |
| 频宽（MHz） | 20 | 20 | 20 | 20/40 | 20/40/80/160 | 20/40/80/160 |
| 调制方式 | CCK/DSSS | OFDM | CCK/DSSS/OFDM | MIMO-OFDM/DSSS/CCK，64QAM | MIMO-OFDM/DSSS/CCK,256QAM | MIMO-OFDM/DSSS/CCK,1024QAM |
| 兼容性 | 802.11b | 802.11a | 802.11b/g | 802.11a/b/g/n | 802.11a/b/g/n | 802.11a/b/g/n/ac |



# IEEE 802.11协议栈




- 物理层分为三个子层： PMD协议（物理介质相关协议）、PLCP（物理层汇聚协议）和物理层管理子层
- MAC层（媒体接入控制层）分为MAC子层和MAC管理子层
- 还定义了一个站管理子层，它的主要任务是协调物理层和MAC层之间的交互

# 802.11 物理层关键技术

**1. MIMO**：从***802.11n***开始引入了单用户***MIMO***，后来发展到***11ac***的多用户***MIMO***，***802.11***支持下行链路的多用户MIMO，每个用户的最大通信速度没有增加，同一个AP同时可传输的用户数显著增加，提高了用户通信体验

**2. 信道绑定**：将两个信道绑定为一个信道使用，提供更大的带宽

**3. 更多子载波**：随着标准不断演进，OFDM支持更多的有效子载波，子载波并行传输，可获得更高的传输速率

**4. 更短GI**：通过缩短数据帧之间的保护间隔（***GI：Guard Interval***）提高吞吐量

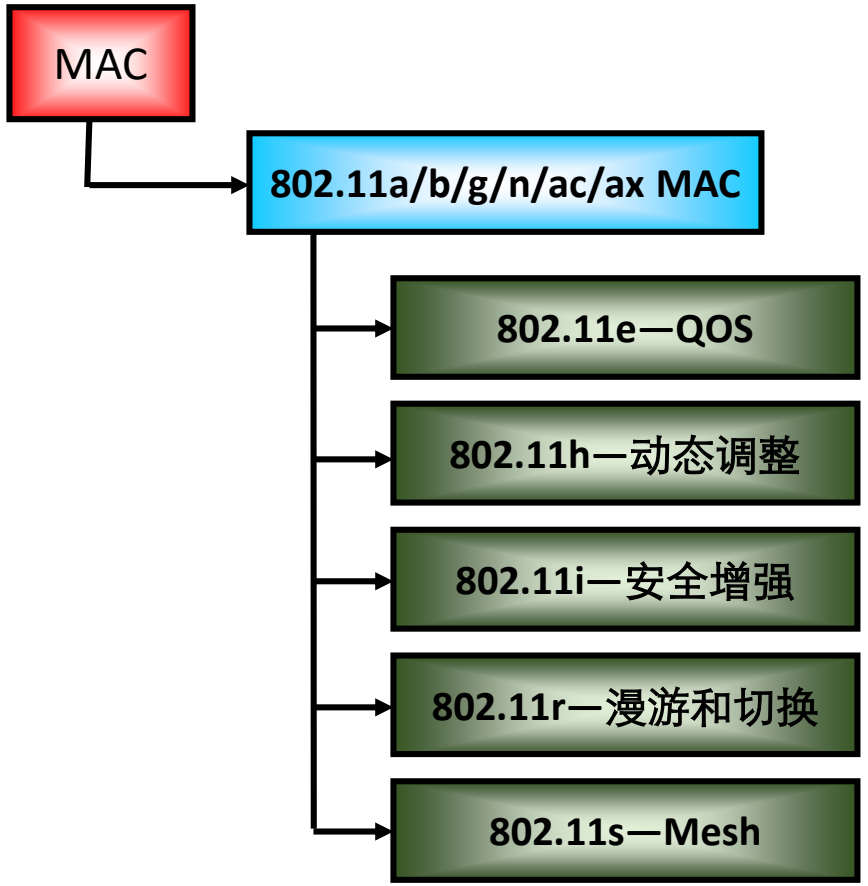
**5. FHSS和DSSS**：FHSS技术以某种随机样式在频率间不断跳换，每个子信道只进行瞬间的传输，提高系统抗干扰能力；DSSS技术将功率分散于较宽的频带，从而提高数据传输速率

# 主要内容

- WLAN无线组网
- IEEE 802.11物理层
- IEEE 802.11MAC子层
- IEEE 802.11服务

# 802.11MAC层相关协议

- 数据链路层包括*LLC*（逻辑链路控制）和*MAC*（媒体存取控制）功能




- *802.11e*：在无线网络中加入*QoS*特性和多媒体支持
- *802.11h*：用于频谱管理
- *802.11i*：用于用户端口身份验证和设备验证，使用高级加密标准（AES）分组密码。 该标准还增强了密钥管理、基于802.1X 的用户身份验证和头数据完整性
- *802.11r*：快速基础服务转移，主要是用来解决客户端在不同AP间切换时的延迟问题
- *802.11s*：拓扑发现、路径选择与转发、信道定位、安全、流量管理和网络管理

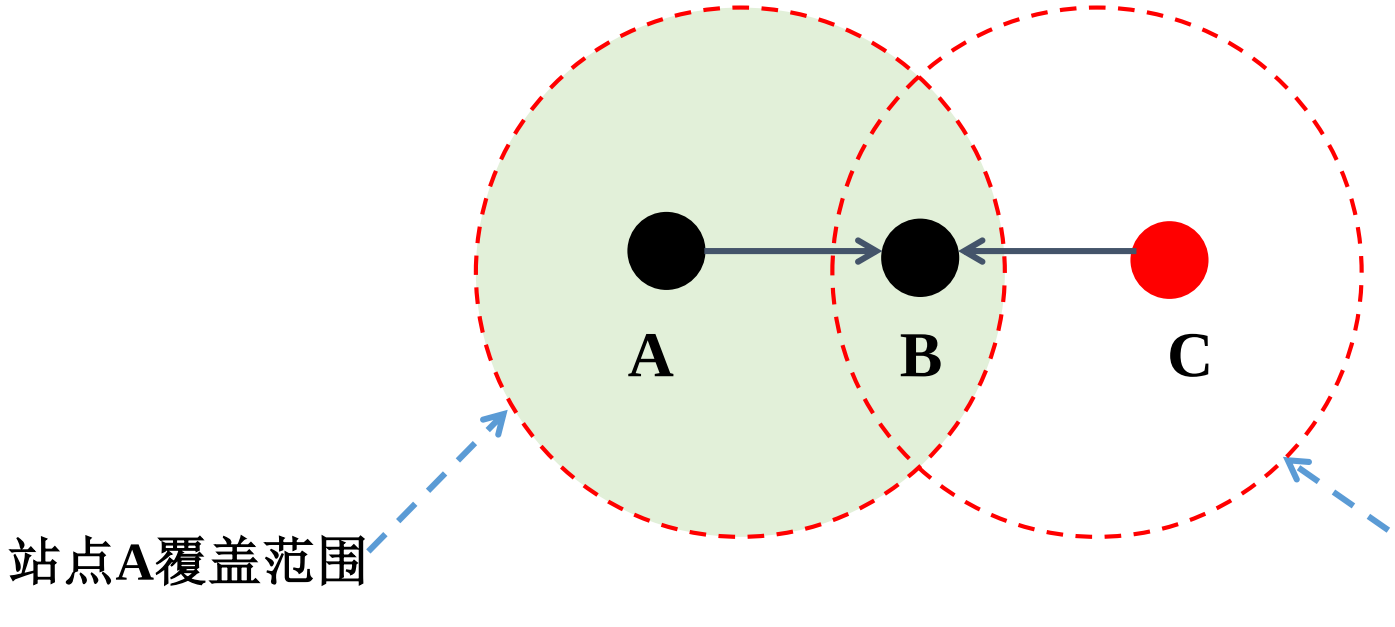
# MAC子层访问机制

- 为了尽量减少数据传输碰撞和重试发送，防止各站点无序争用信道，*WLAN*采用与以太网*CSMA/CD*(载波监听多路访问/冲突检测)相类似的*CSMA/CA*(载波监听多路访问/冲突防止)协议。*CSMA/CA*将时间域划分与帧格式紧密联系起来，保证某一时刻只有一个站点发送，实现了集中控制，*CSMA/CA*利用*ACK*信号避免冲突发生，只有当客户端收到返回的*ACK*信号后，才能确认送出的信号已经正确到达

- 在无线局域网的环境下，MAC子层协议须解决两个问题
  - 隐藏站问题
  - 暴露站问题

# 隐藏站问题

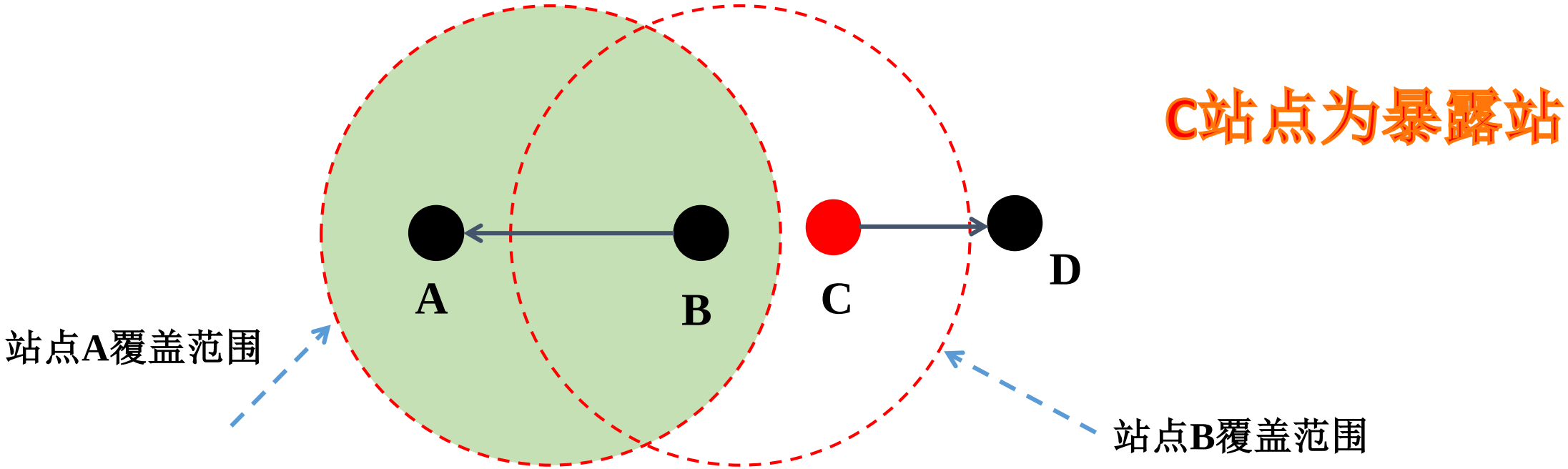
- 隐藏站：站点A向站点B发送信息，站点C未侦测到A也向B发送信息，故A和C同时将信号发送至B，引起信号冲突，最终导致发送至站点B的信号都丢失了。相对于站点A，站点C为隐藏站
- 隐藏站是指位于接收站点范围内和发送站点范围外的站点




站点C为隐藏站

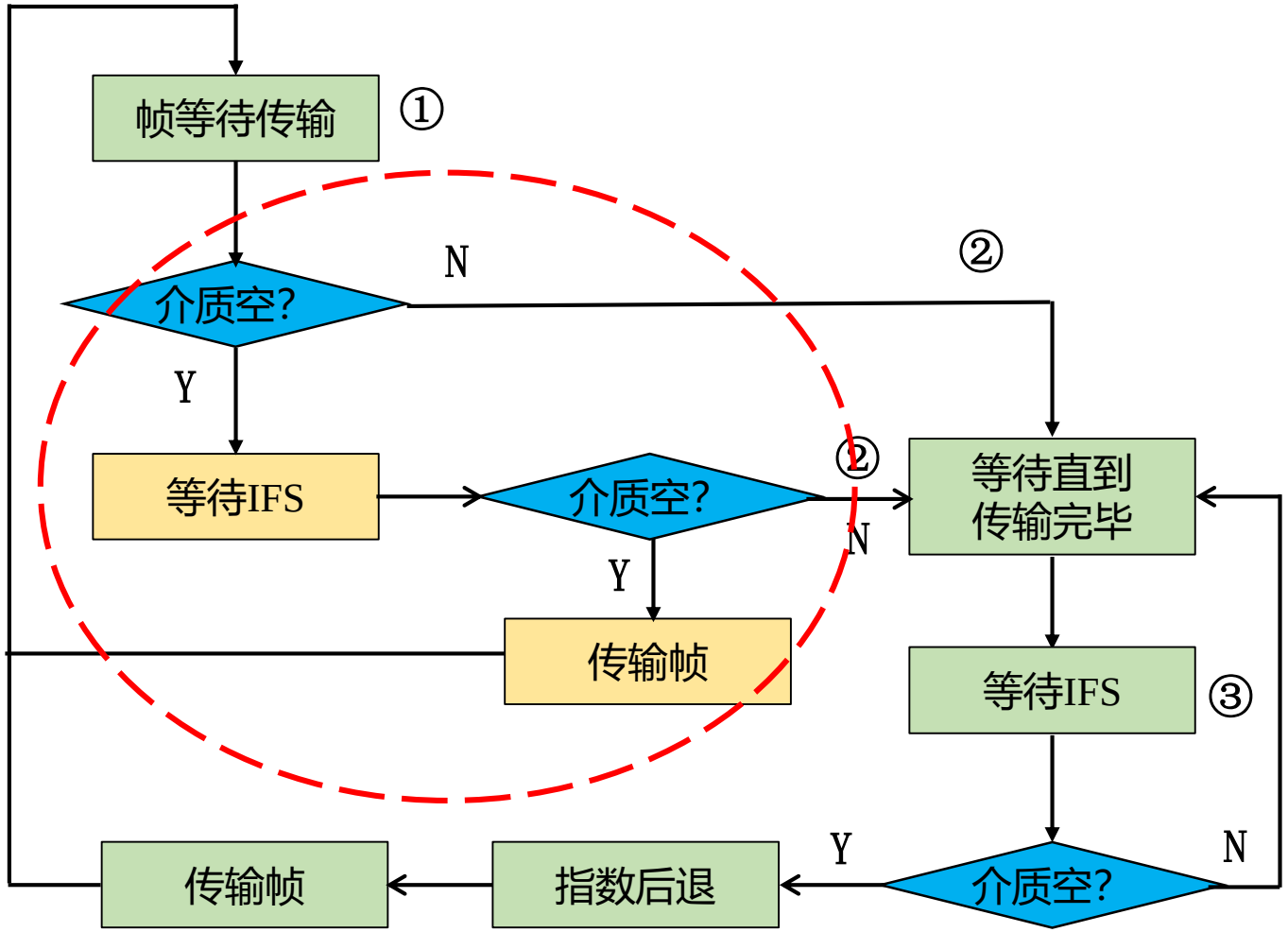
# 暴露站问题

- 暴露站：指位于发送站点范围内和接收站点范围外的站点，暴露站因侦听到发送站点的发送而延迟发送。从实际情况看，暴露站可能位于接收站点通信范围外，暴露站的发送不会造成冲突。引入了不必要的延时




C站点为暴露站

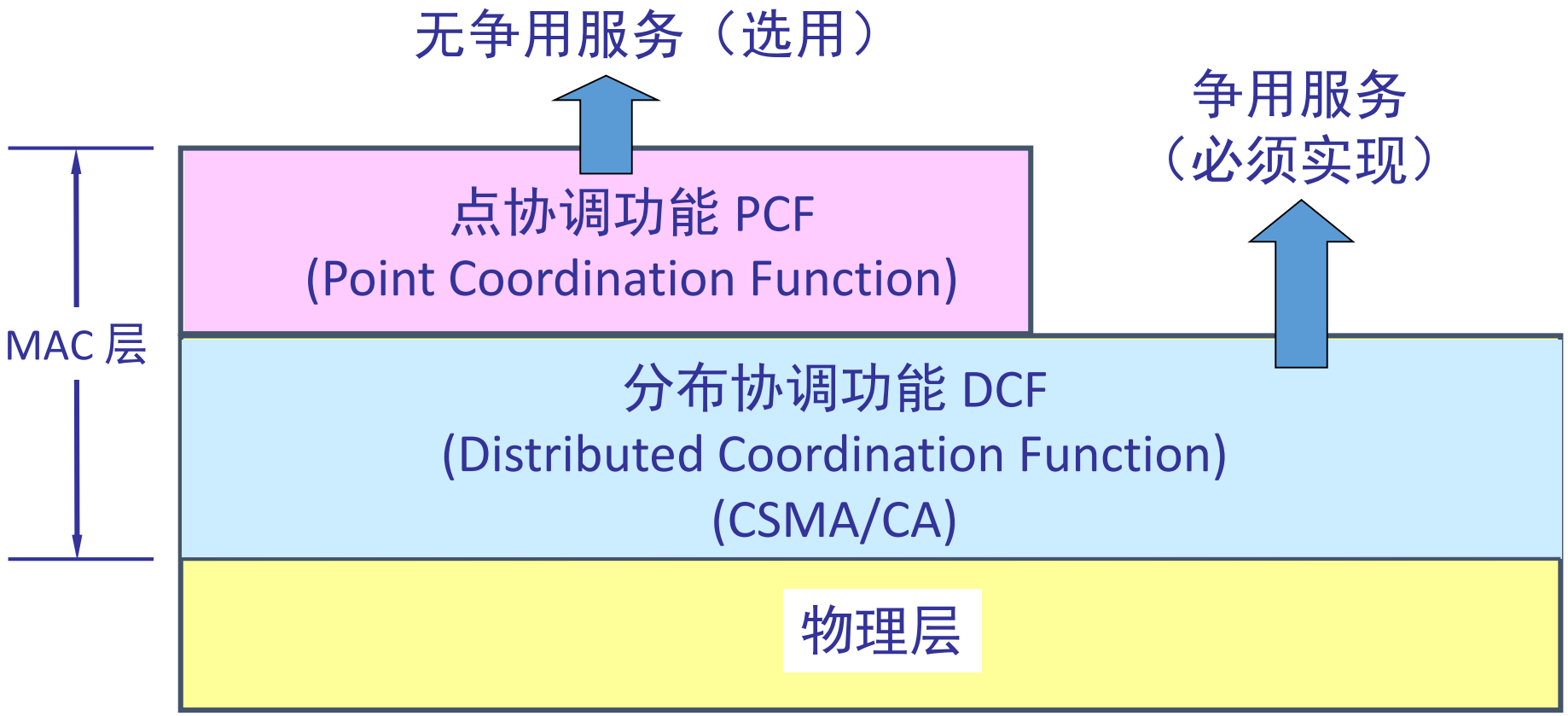
# CSMA/CA的工作流程




- 发送站点传送数据时，如未探测到网络正在传送数据，则等待一个时间间隔（帧间间隔IFS）后继续探测，如仍未探测到网络传送活动，就开始发送数据
- 接收站点如能收到发送站点送出的完整数据，则返回一个ACK数据报，如果该ACK数据报被发送站点收到，则数据发送完成；否则，发送站点等待一个时间后继续重传
- 这在一定程度上解决了隐藏站问题

# 802.11 MAC的协调功能

- MAC 层通过协调功能（点协调功能PCF或分布协调功能DCF）确定站点什么时间可发送数据或接收数据

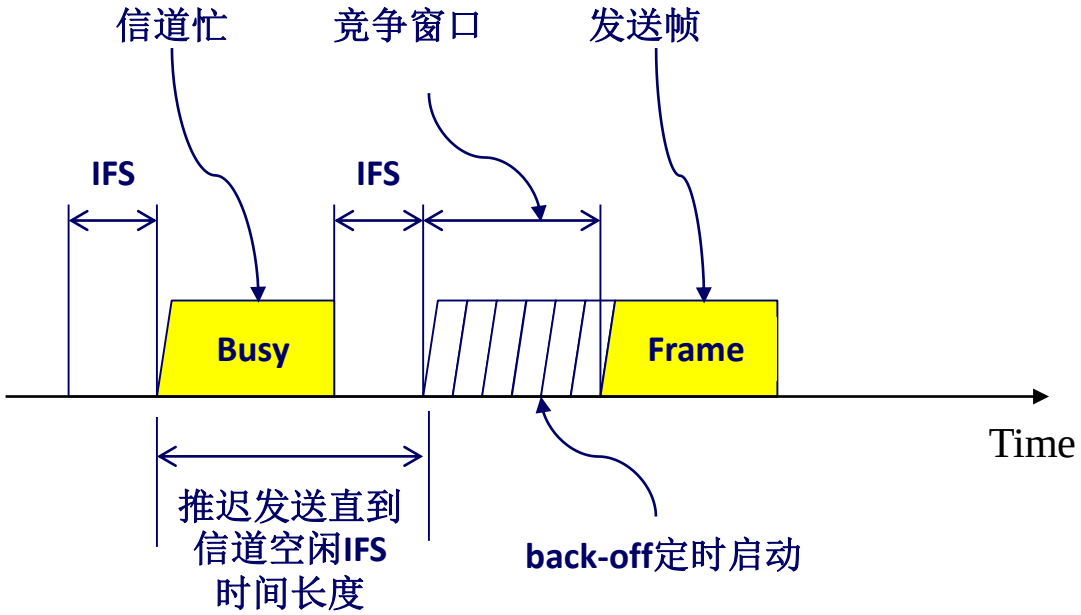


# 点协调功能：PCF

- PCF（*Point Coordination Function*）用接入点 AP 集中控制BSS内的活动
- PCF使用集中控制接入算法，把发送数据权轮流交给各子站，避免了碰撞的产生
  - 例如时间敏感的业务（如分组话音）应该使用无竞争服务的PCF
  - PCF协调功能为可选功能，对某些无线局域网，PCF可以没有

# MAC访问机制：DCF方式

- DCF (*Distributed Coordination Function*)不采用中心控制方式，各站点均使用CSMA/CA机制的分布式接入算法，通过争用信道来获取发送权



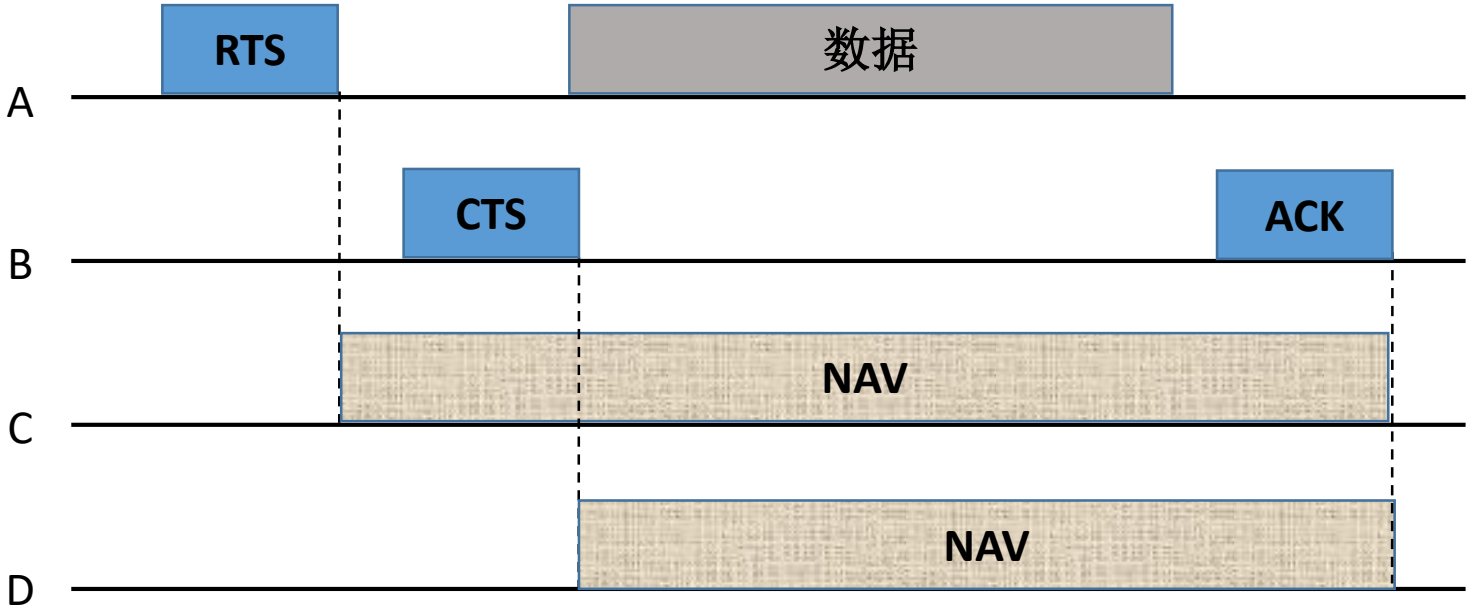

- DCF 使用物理信道监听手段和虚拟信道监听手段监听信道是否处于空闲状态，无论哪种手段监听到信道忙，均视为信道处于忙状态

# 物理信道监听和虚拟信道监听

- 物理信道监听
  - 站点发送数据帧的前提之一是信道空闲，需要先检测信道（进行载波监听）
  - 在数据帧传送过程中并不监听信道，而是直接送出整个帧

- 虚拟信道监听
  - 源站把要占用信道时间（包括目的站发回确认帧所需时间）写入发送数据帧头部“*Duration Time*”字段，以便使其它站在这一段时间都不要发送数据
  - 当站点检测到正在信道中传送的帧的“*Duration Time*”字段时，就调整自己的网络分配向量NAV，NAV指出了信道处于忙状态的持续时间

# 虚拟信道的监听方法




- 假设C处于A的无线范围内，但不在B的无线范围内，C监听到A发送的RTS就调整自己的网络分配向量NAV
- 假设D监听不到A，但监听到B发送的CTS，D也调整NAV

- A发送数据帧之前先发送一个控制帧（请求发送RTS：Request To Send），包括源地址、目的地址和这次通信（包括相应的确认帧）所需要的持续时间
- 若信道空闲，目的站B响应一个控制帧（允许发送CTS：Clear To Send），也包括这次通信所需要的持续时间
- A收到CTS后发送数据帧，目的站收到数据帧后通过确认帧ACK应答，传送成功

# 802.11帧分类

- 数据帧

  传送数据报文

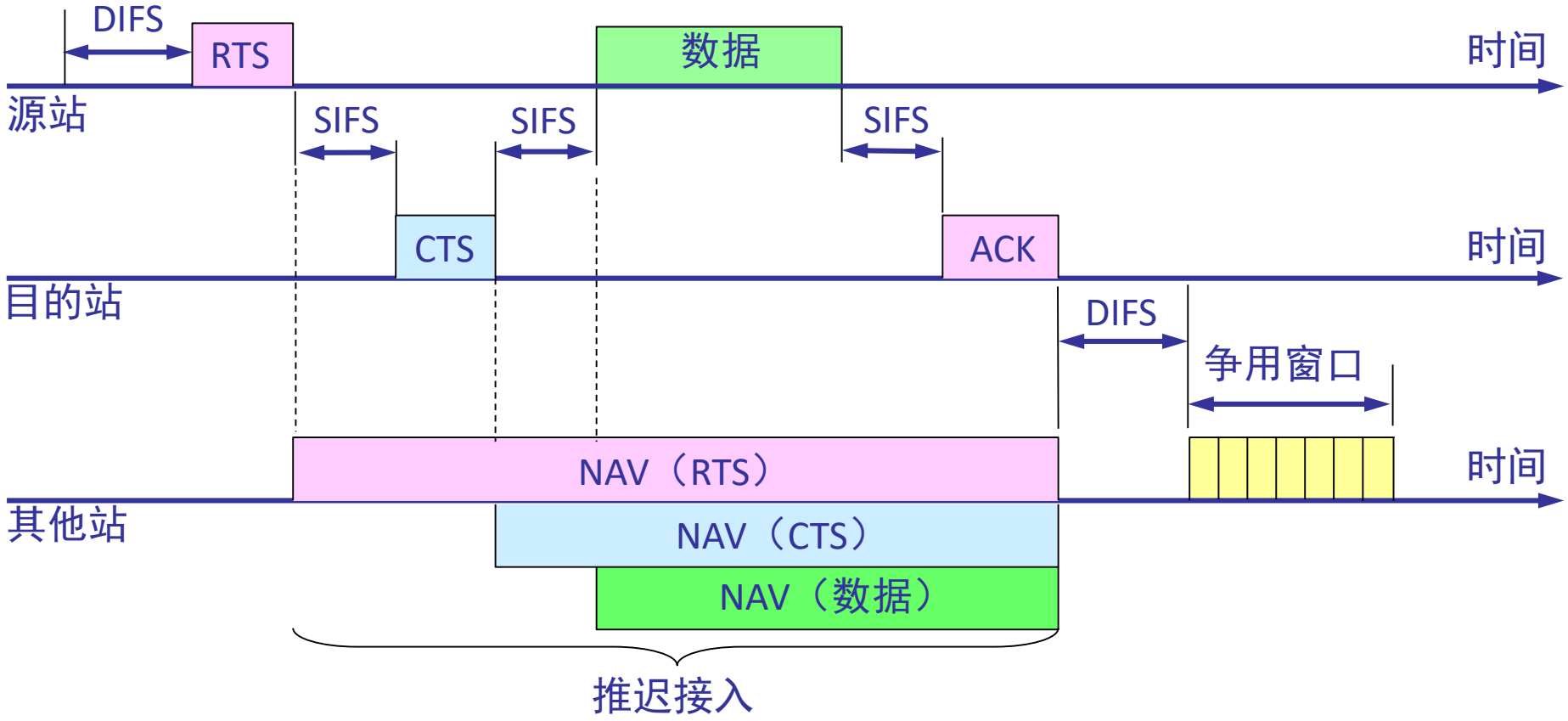
- 控制帧

  协助发送数据帧的控制报文，例如： RTS、CTS，ACK

- 管理帧

  负责站点（STA）和AP之间认证、关联等管理工作

# 不同帧之间的时序关系




- 帧和帧之间需要间隔一定的时间，称为帧间间隔***IFS***，***SIFS*** 表示短帧间间隔，***DIFS*** 表示分布协调帧间间隔），***PIFS*** 表示点协调帧间间隔

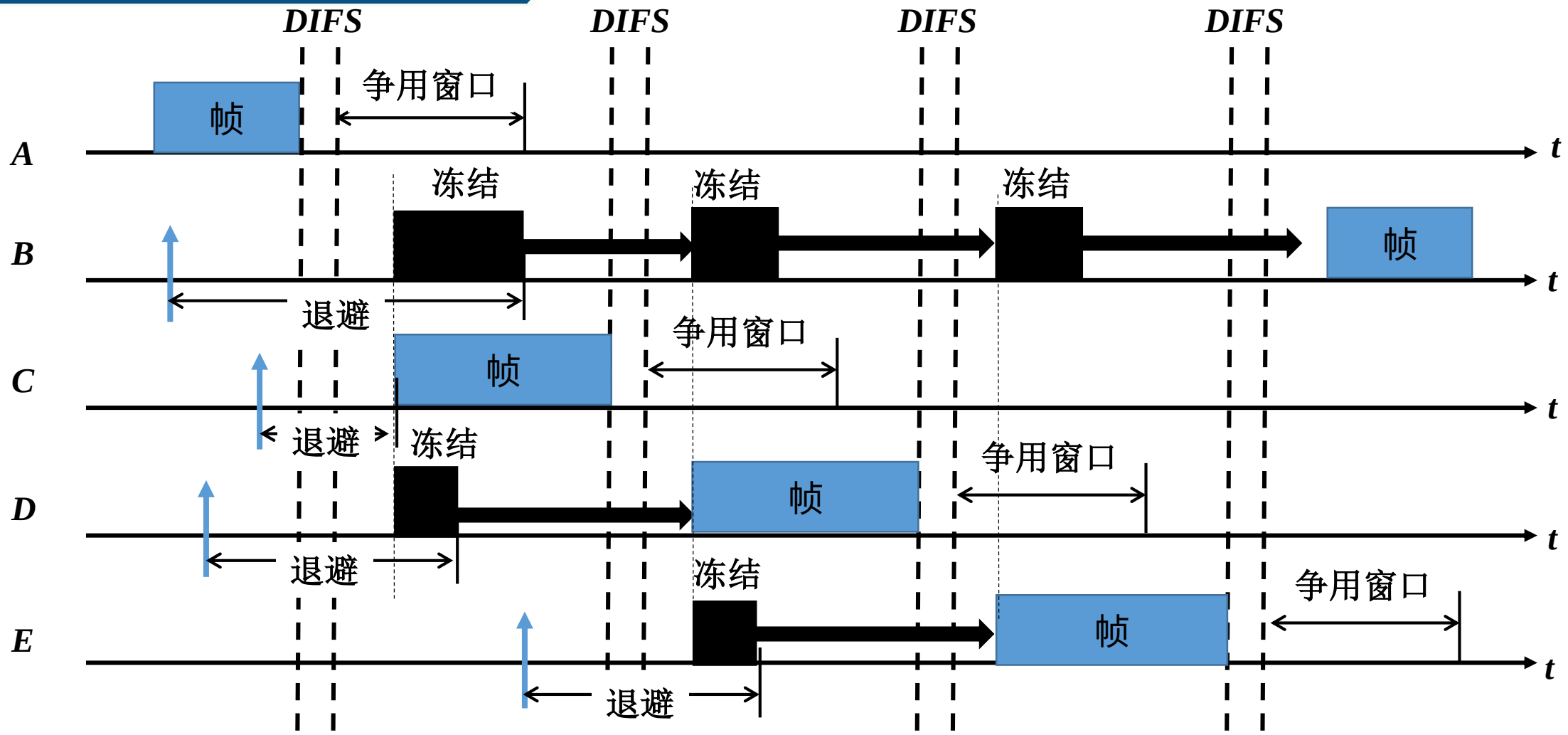
# 退避机制

- 为了尽量减少冲突，CSMA/CA采用了退避机制，当一个站点要发送数据帧时，如碰到如下几种情况下，必须进行退避：①发送第一帧之前检测到信道处于忙状态、②每一次重传、③发送下一帧前

- 只有当监听到信道处于空闲，且该数据帧是第一个数据帧时才不退避

- 标准规定，退避时间是整数倍时隙，CSMA/CA采用的二进制指数退避算法，第$i$次退避在$2^{2+i}$个(第1次8个，第2次16个,……)时隙中随机地选择一个，当使用退避算法选择了某个时隙后，就根据该时隙的位置设置一个退避计时器(backoff timer)，当退避计时器时间减小到零时，就开始发送数据，当退避计时器时间尚未减小到零时信道又转变为忙态，这时就冻结退避计时器的数值，重新等待信道变为空闲，再经过时间DIFS后，继续启动退避计时器(从剩下的时间开始)

# 退避机制示意图

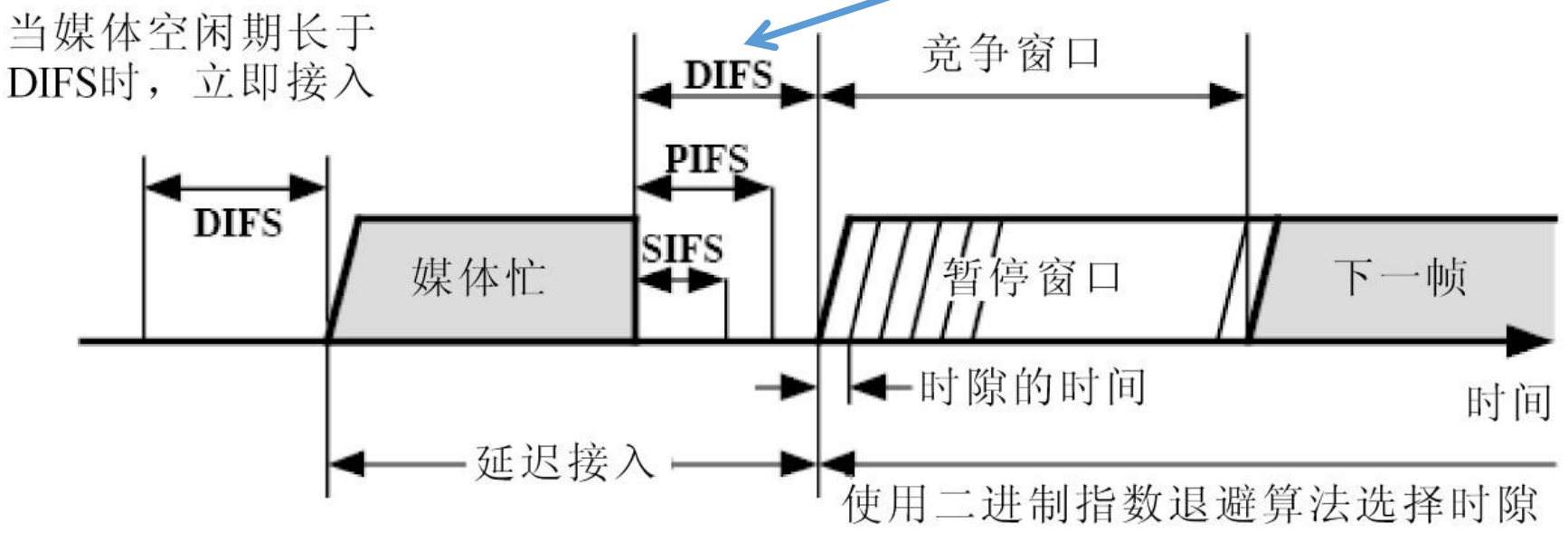



打算发送数据 冻结退避时间

# 帧间间隔

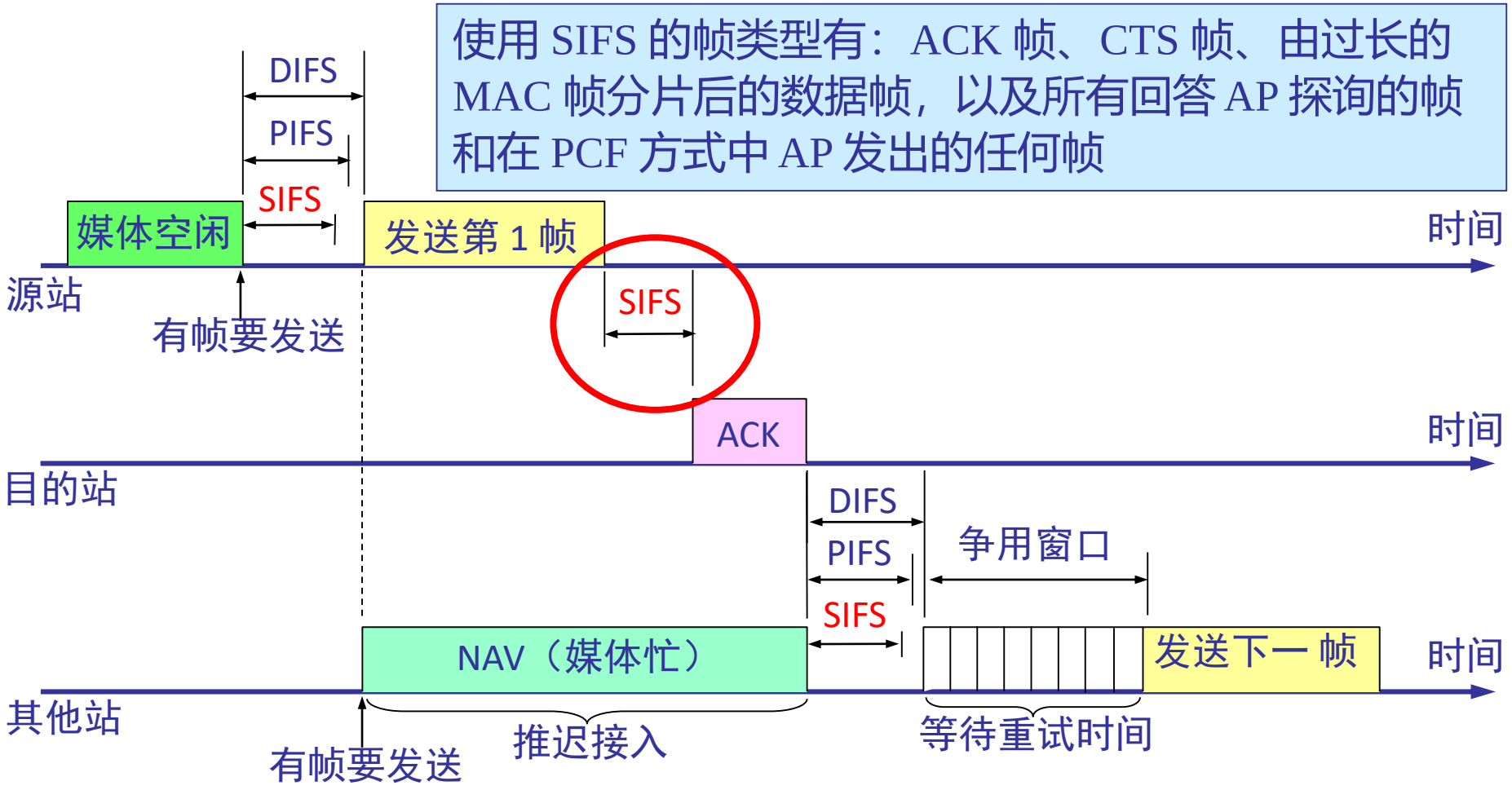
- 帧间间隔类型选择取决于发送帧类型。高优先级帧等待时间较短，优先获得发送权
- 若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙状态，低优先级帧继续推迟发送。这样可减少发生碰撞的机会
- 帧间间隔按照时间长短分为***SIFS***（短帧间间隔）、***PIFS***（点协调控制帧间间隔）、***DIFS***（分布协调功能帧间间隔）

根据不同传输需要选择不同帧间间隔



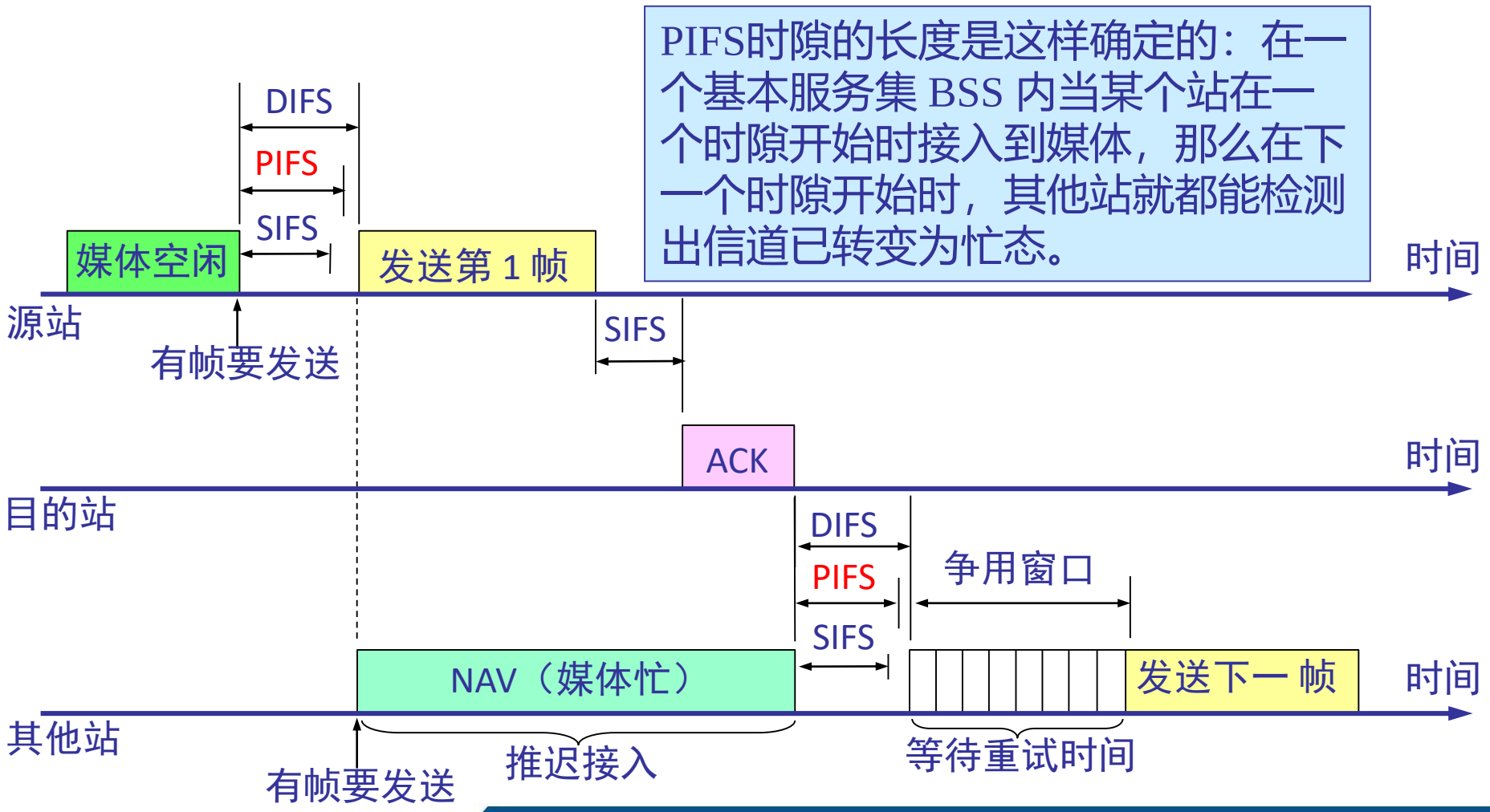
# 帧间间隔SIFS

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



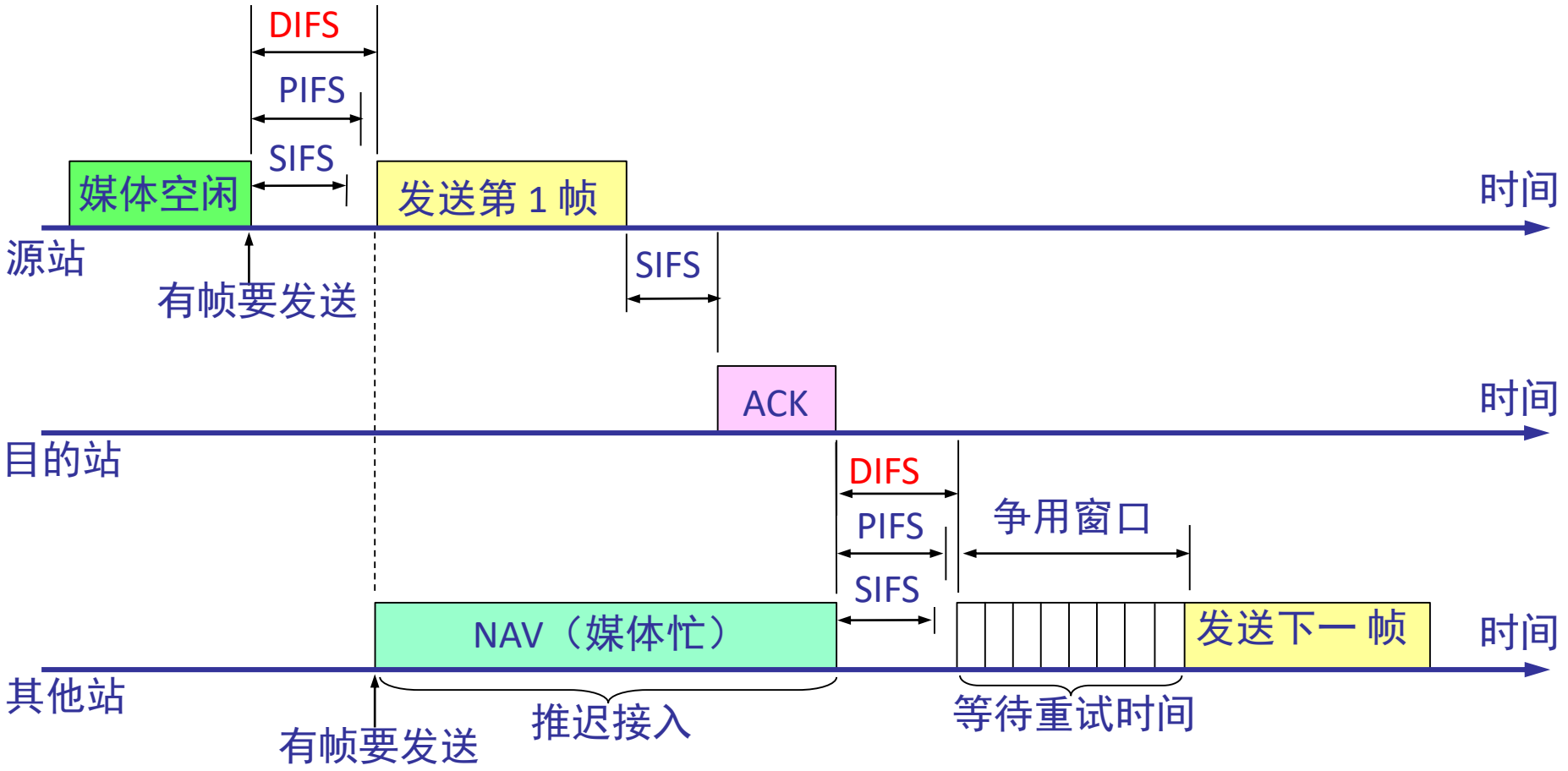
# 帧间间隔PIFS

- ***PIFS***，即点协调帧间间隔，它比 ***SIFS*** 长，是为了在开始使用 PCF 方式时优先获得接入到媒体。***PIFS*** 长度是 ***SIFS*** 加一个时隙长度。

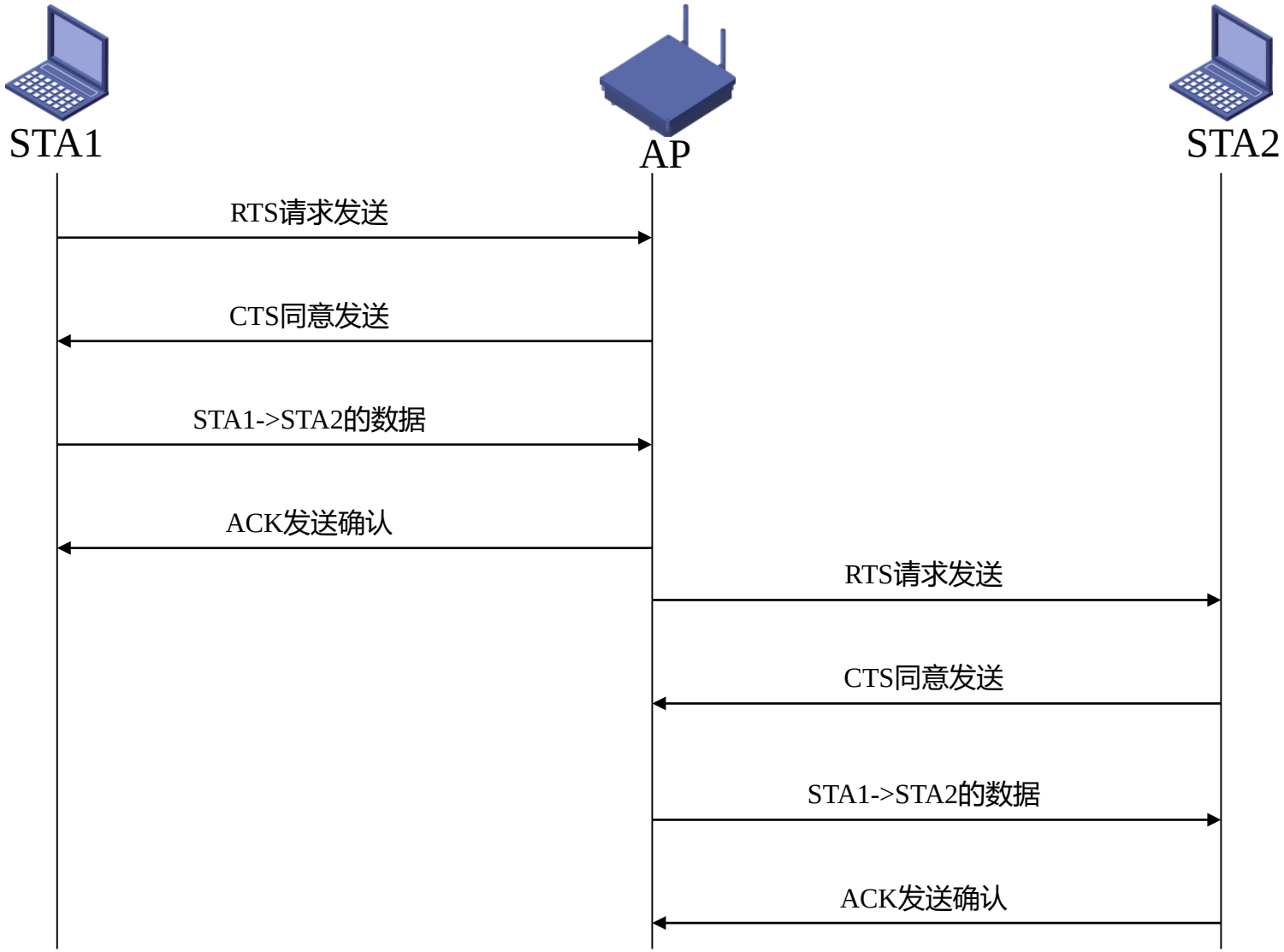


# 帧间间隔DIFS

- ***DIFS***，即分布协调帧间间隔（最长的 IFS），在 DCF 方式中用来发送数据帧和管理帧。***DIFS*** 的长度是 PIFS 再增加一个时隙长度



# 基于RTS / CTS机制的典型报文发送过程



# 主要内容

- 无线WLAN无线组网
- IEEE 802.11物理层
- IEEE 802.11MAC子层
- IEEE 802.11服务

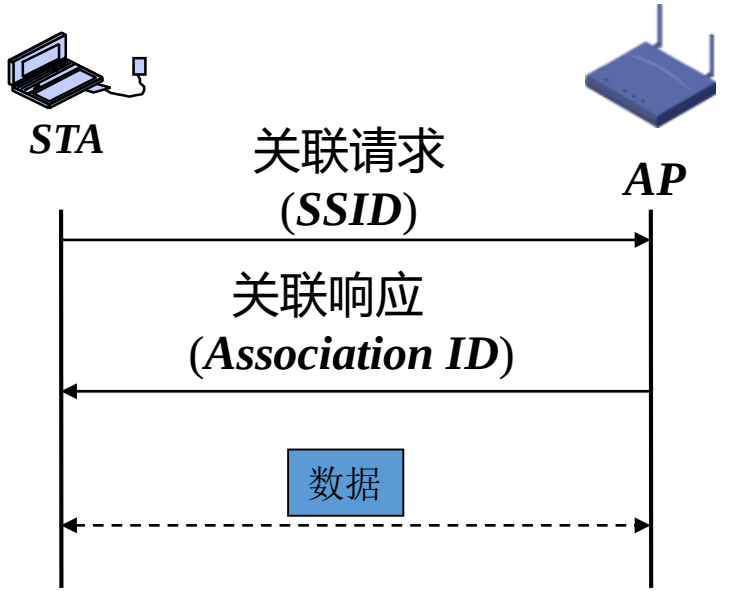
# IEEE 802.11的服务

- 标准WLAN必须提供9种服务，分为两类
- 5种分发服务：涉及到对BSS成员关系的管理，并且会影响到BSS之外的站点。分发服务由AP提供
  - 处理站点的移动性
  - 当站点进入BSS时，通过这些服务与AP关联起来
  - 当站点离开BSS时，通过这些服务与AP断开联系
- 4种站点服务：只与一个BSS内部的活动有关系，在BSS内部进行，在关联过程完成之后这些服务才能用到

# 分发服务-关联服务

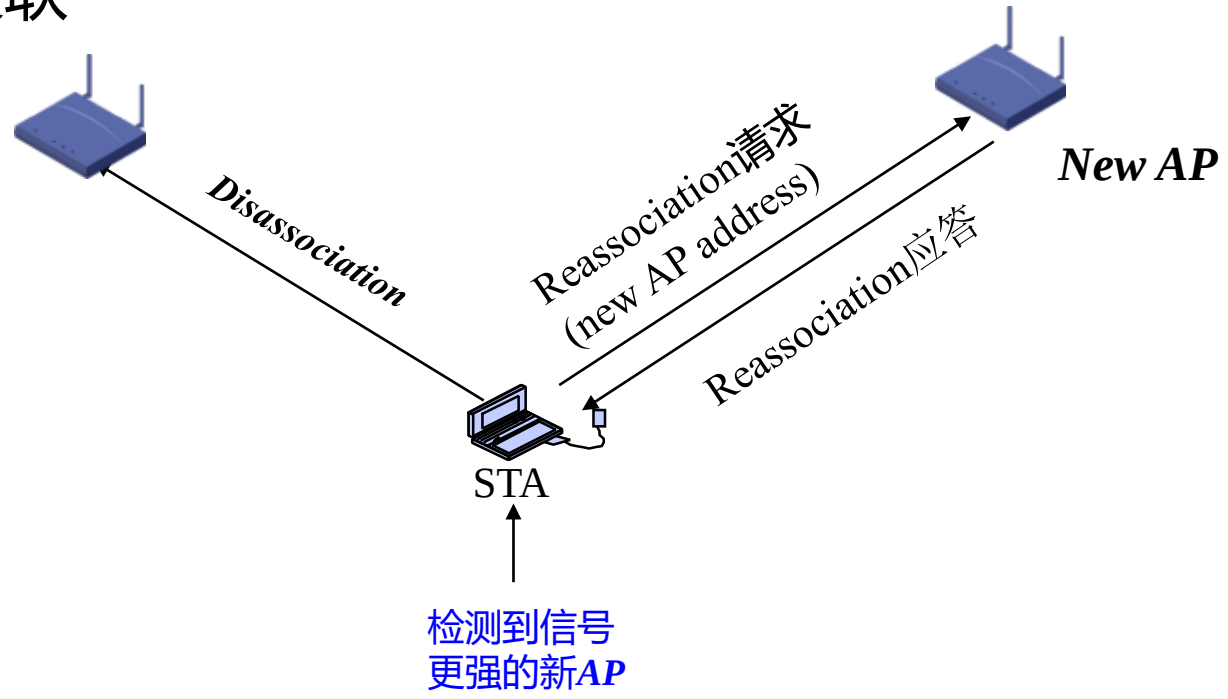
- 关联（*Association*）服务：站点利用该服务连接到*AP*上，当站点进入*AP* 范围之内时，该服务被用到

- 关联阶段分为两个步骤：
  - 站点向*AP* 发送关联请求
  - *AP* 向站点返回关联响应



# 分发服务-分离服务和重新关联服务

- 分离（*Disassociation*）服务：不管是站点还是*AP*，都可能解除关联关系，一个站点在离开或关闭之前，先使用该服务；*AP*在停机或维护之前也用到该服务
- 重新关联（*Resassociation*）服务：利用该服务，站点可以改变它的首选*AP*，该服务支持站点从一个*BSS*移动到另一个*BSS*， 站点从一个*AP*移动到另一个*AP*时，需要重新进行认证和关联



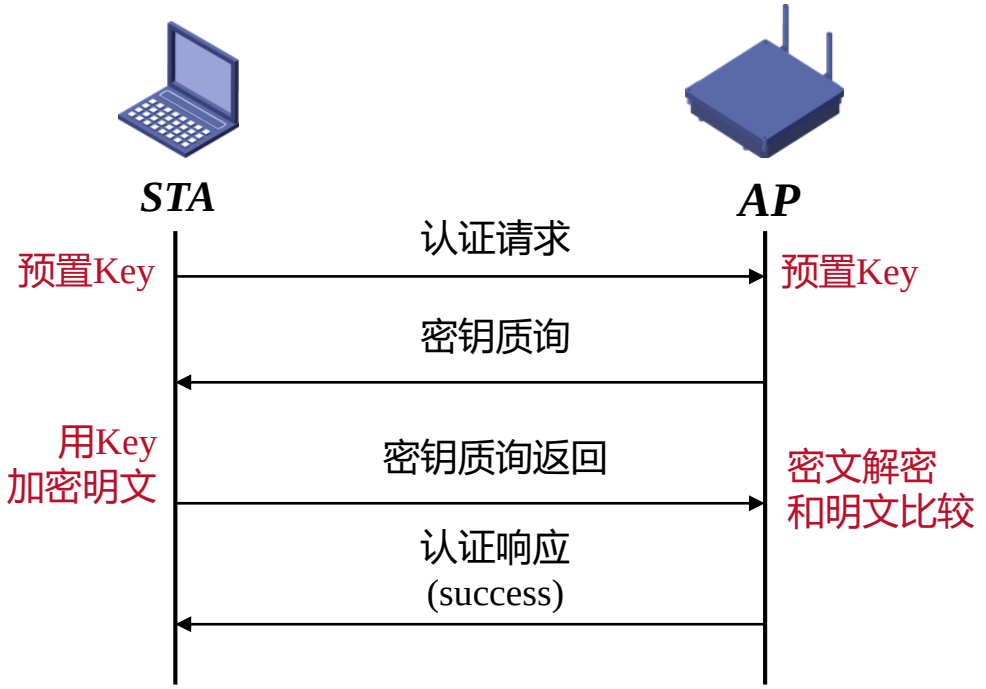
# 分发服务-分发服务和融合服务

- 分发（*Distribution*）服务：决定如何路由那些发送给*AP*的帧。如果帧的目标对于*AP*来说是本地的，则该帧将直接发送到空中，否则的话，它们必须通过*DS*（分布式系统）转发

- 融合（*Integration*）服务：如果一个帧需要通过一个非*IEEE 802.11*的网络来发送，并且该网络使用了不同的编址方案或者不同帧格式，该服务可以将*IEEE 802.11*格式帧翻译成目标网络所要求的帧格式

# 站点服务-认证服务

- 认证（***Authentication***）：任何一个站点必须证明自己的身份（认证通过）后才允许发送数据。站点向***AP***发出认证请求后，***AP*** 发送质询帧以确定该站点是否知道连接密钥（口令），站点用密钥加密质询帧送回到***AP***，若比对正确，表示站点认证通过
- 注意：开放系统不需要认证



# 站点服务-其它服务

- 解除认证（*Deauthentication*）：用于对已认证站点离开网络时提供解除认证服务
- 私密性（*Privacy*）：用于提供信息加密和解密服务
- 数据投递（*Data delivery*）：用于数据传送服务

# 无线接入过程的三个阶段

站点启动初始化并开始使用*AP*传送数据帧前，需经过三个阶段实现站点接入：


第一阶段　　第二阶段　　第三阶段

# 无线接入过程-扫描阶段

## 第一阶段：扫描（*SCAN*）阶段

- 无线站点接入 *AP* 前须通过*Scanning*搜索*AP*，可通过两种方式实现：
  - 主动扫描方式 （特点：能迅速找到）：站点依次在不同个信道发出*Probe Request*帧，寻找与站点有相同*SSID*的*AP*，若找不到相同*SSID*的*AP*，则一直扫描下去
  - 被动扫描方式（特点：查找时间长，站点节电）：站点被动等待*AP*定时送出的*Beacon*信标帧，该帧提供*AP*及所在*BSS*相关信息：“我在这里”…

## 第二阶段：认证（*Authentication*）阶段

- 当站点找到与其有相同*SSID*的*AP*，根据*AP*信号强度，选择信号最强*AP*，进入认证阶段，只有认证通过的站点才能进行无线接入访问
  - 开放系统身份认证(*open-system authentication*)：不认证也不加密
  - WEP共享密钥认证(*shared-key authentication*）：等效加密
  - WPA-PSK认证（*Pre-shared key*）：*WEP* 预分配共享密钥的认证方式，在加密方式和密钥的验证方式上作了修改，使其安全性更高，分为家用和企业两个版本
  - WPA2认证：*IEEE 802.11i*无线网络标准，有家用版本与企业版本，使用更安全的加密技术*AES (Advanced Encryption Standard)*，支持*802.1X EAP*扩展认证协议

# 无线接入过程-关联阶段

## 第三阶段：关联（*Association*）阶段

- 当*AP*向站点返回认证响应信息，身份认证获得通过后，进入关联阶段
  - 站点向*AP*发送关联请求
  - *AP*向站点返回关联响应
  - 接入过程完成，站点初始化完毕，开始向*AP*传送数据帧

# The End !