第8章 无线局域网(WLAN)

刘 轶
北京航空航天大学 计算机学院

局域网技术标准(第3章的一页PPT)

- **IEEE802**系列局域网标准
  - **IEEE 802.1a** 综述与体系结构
  - **IEEE 802.1b** 寻址、互联、管理
  - **IEEE 802.2** 逻辑链路控制(LLC)
  - **IEEE 802.3** CSMA/CD介质访问控制(MAC)与物理层技术规范
    - **IEEE 802.3u** 快速以太网(Fast Ethernet)
    - **IEEE 802.3z** 千兆以太网(Gigabit Ethernet)
  - **IEEE 802.4** Token Bus介质访问控制与物理层技术规范
  - **IEEE 802.5** Token Ring介质访问控制与物理层技术规范
  - **IEEE 802.11** 无线局域网介质访问控制与物理层技术规范

8.1 概述

8.2 IEEE802.11的物理层

8.3 IEEE802.11的MAC层

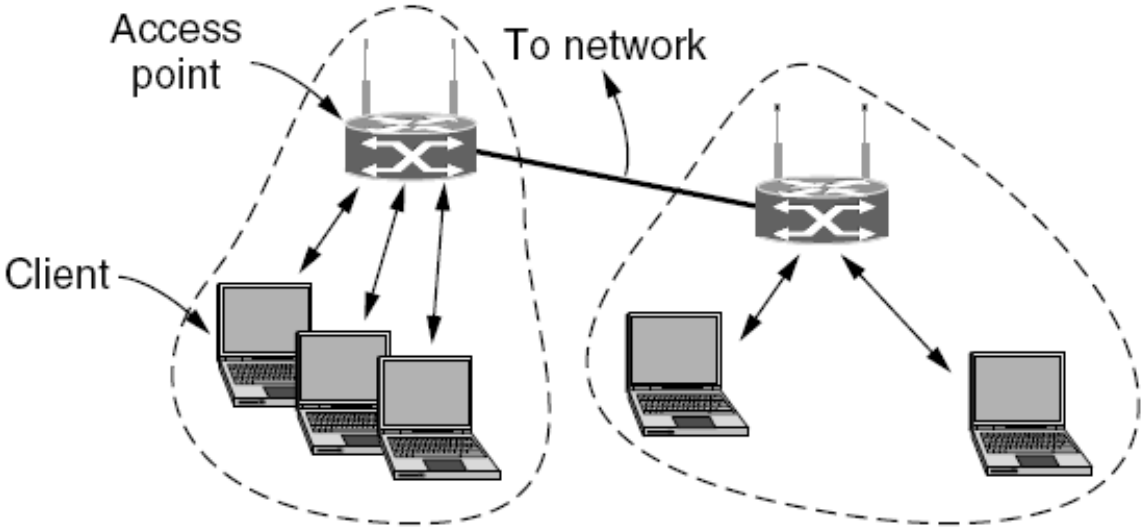
8.4 IEEE802.11的帧结构

8.5 IEEE802.11的安全性

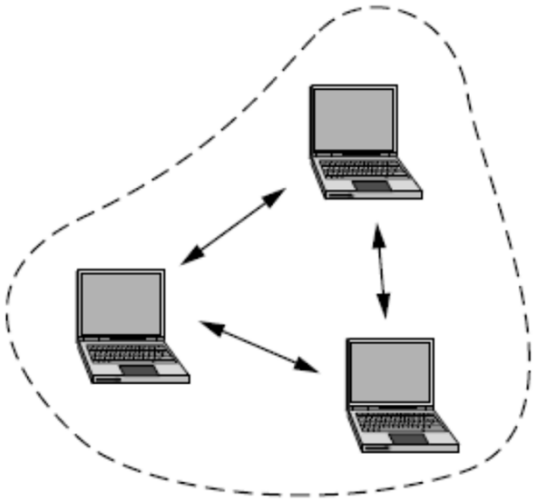
8.1 概 述

8.1 概述

- **802.11网络有两种使用模式**
  - **① 基础设施模式/有架构模式(Infrastructure mode)**
    - 每个客户端与一个接入点(AP—Access Point)连接，接入点与其他网络连接
    - 几个接入点可通过有线网络连接形成扩展的802.11网络
  - **② 自组织网络模式(ad hoc mode)**
    - 多台计算机相互连接形成网络，相互间发送帧
    - 无接入点



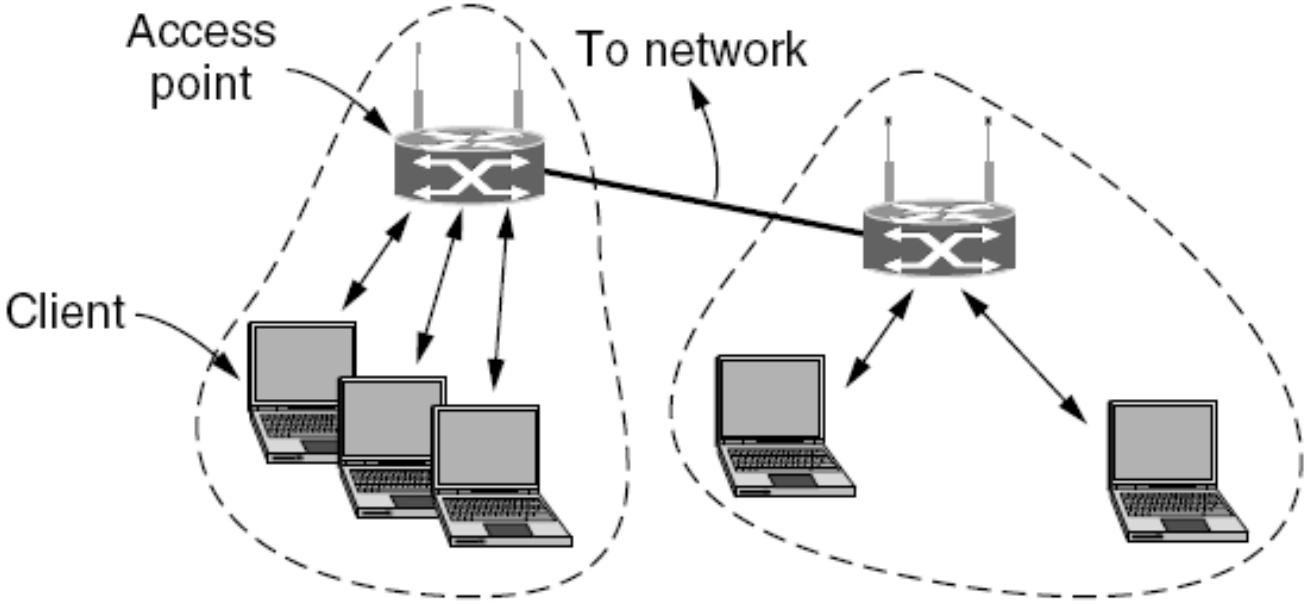
基础设施模式(Infrastructure mode)



自组织网络模式(ad hoc mode)

8.1 概述

- 基础设施模式/有架构模式(Infrastructure mode)
  - 基本服务集(BSS, Basic Service Set):
    一个基站(即AP) + 若干个移动站
  - BSS内的站之间可通信，与BSS外的通信需通过基站进行
  - 每个AP分配一个≤32 字节的服务集标识符SSID和一个信道
    SSID: Sevice Set Identifier ←相当于该基本服务集的名字



- 关联(association)：移动站与AP建立连接，加入该基本服务集
- 移动站与AP建立关联的方法

  ① 被动扫描

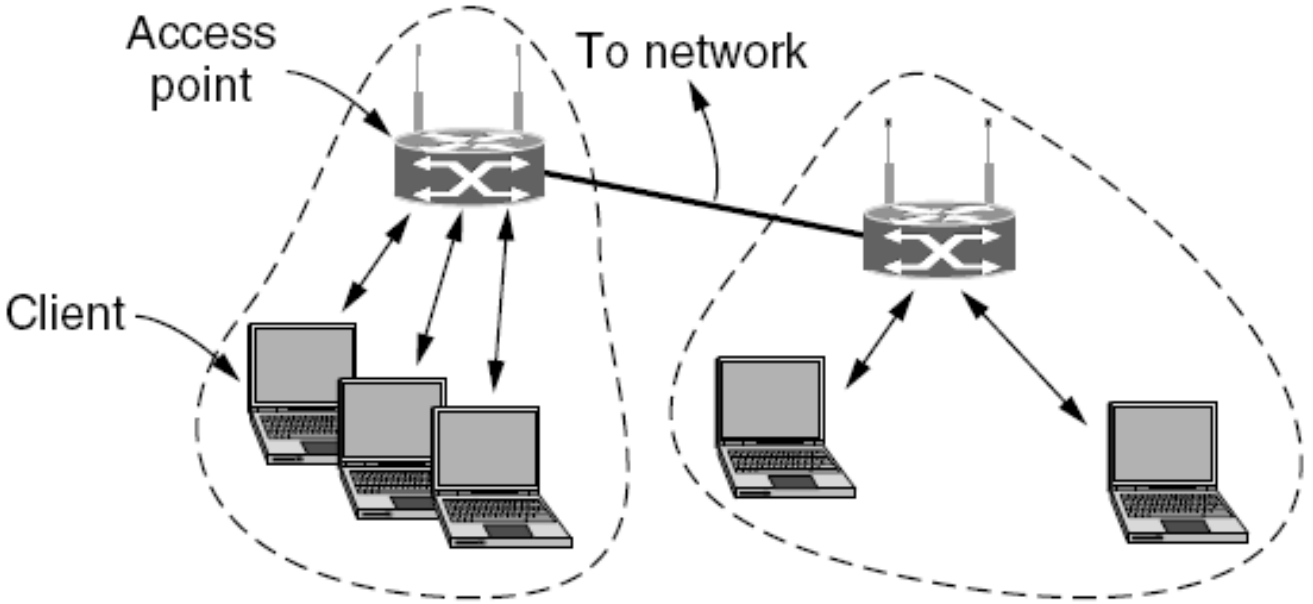
  – 移动站等待接收AP周期性发出的信标帧(beacon frame)

  – 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)

  ② 主动扫描

  – 移动站主动发出探测请求帧(probe request frame)，等待 AP 发回的探测响应帧(probe response frame)
- 重新关联(Reassociation)：移动站改变其首选AP，即加入另一BSS

  – 移动站从一个BSS漫游至另一个BSS时

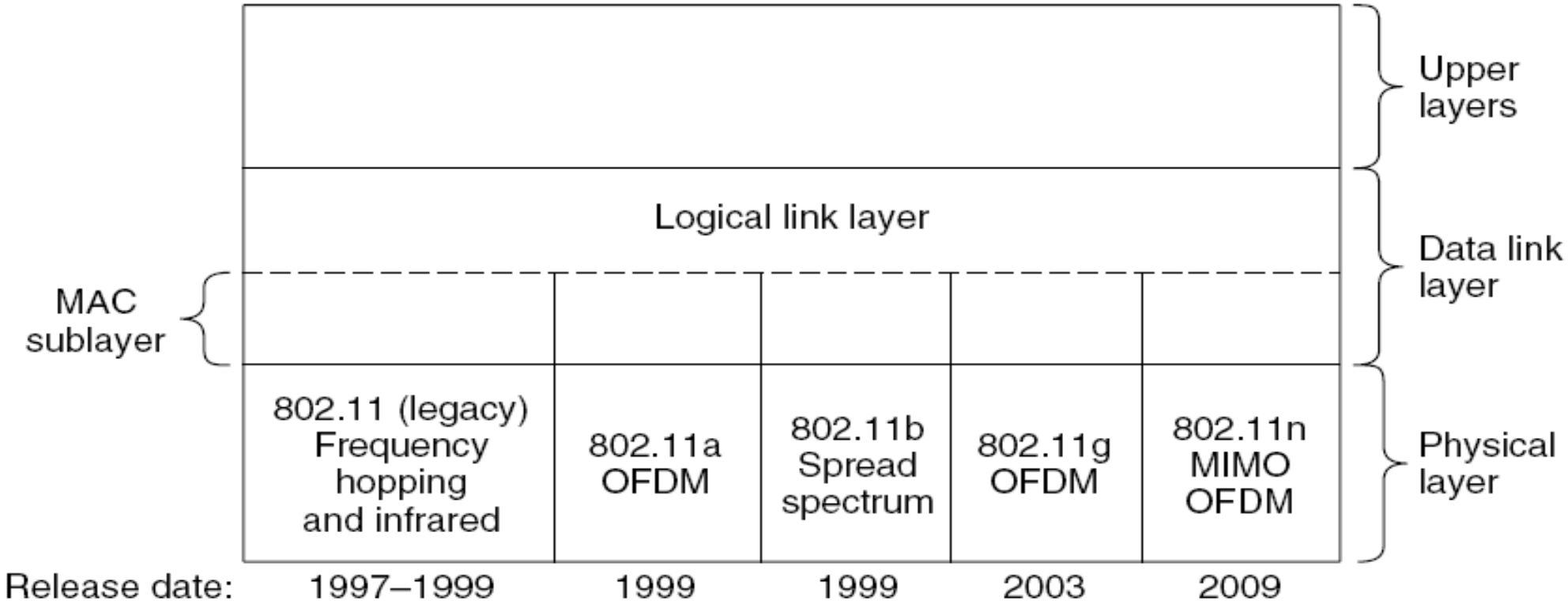


8.1 概述

- **Wi-Fi与802.11**
  - **Wireless fidelity(无线保真)的缩写**
  - **是一个无线网络通信技术的品牌，由Wi-Fi联盟(Wi-Fi Alliance)拥有**
  - **目的**
    改善基于IEEE 802.11的无线网络产品之间的互通性
  - **一般认为，使用IEEE 802.11系列协议的局域网就称为Wi-Fi**
  - **热点(Hotspot)**
    在公共场所提供Wi-Fi接入Internet服务的地点

8.1 概述

- **802.11协议栈 (与其他IEEE802协议类同)**
  - **客户端和AP的协议相同**
  - **MAC子层决定如何分配信道**
  - **LLC子层屏蔽IEEE802协议之间的差异，同时承上启下**

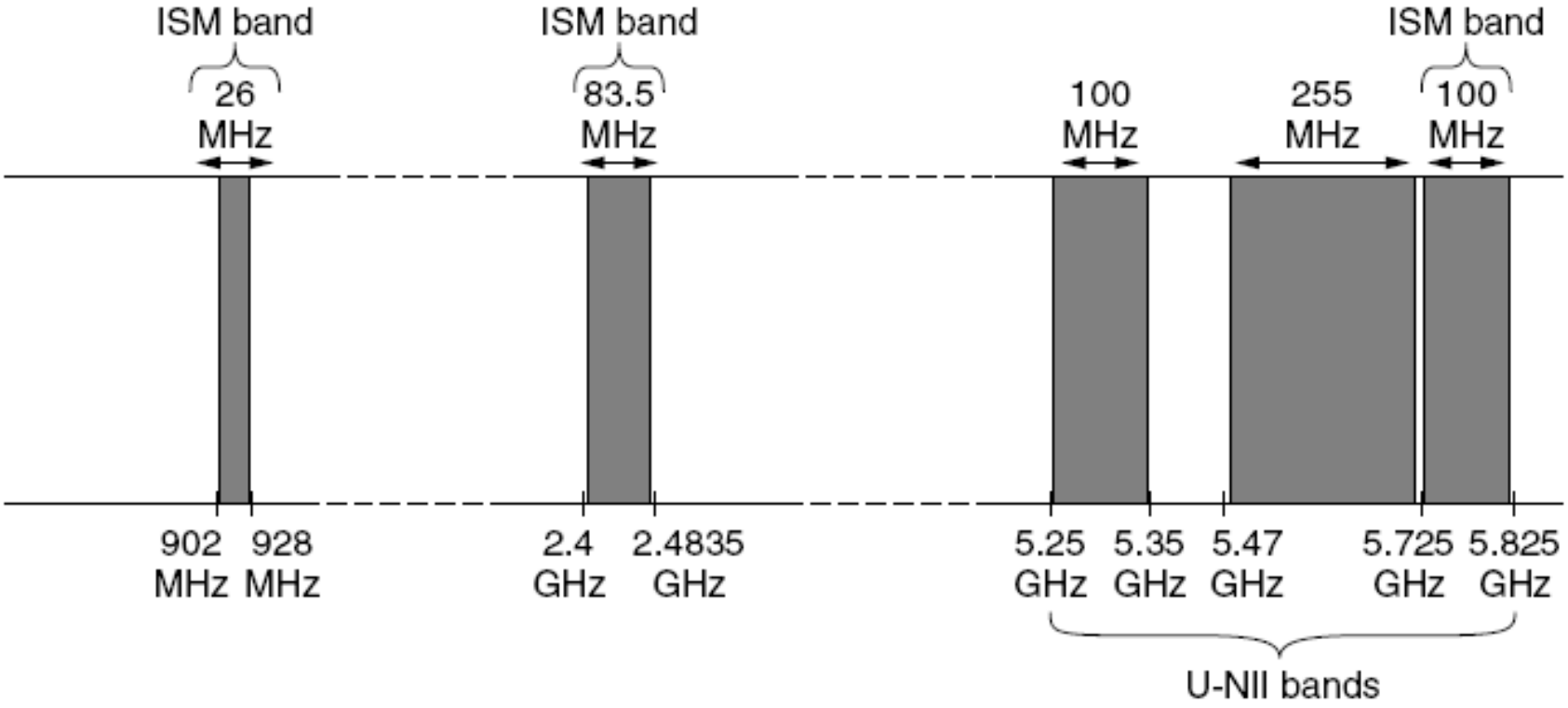


IEEE802.11协议栈

8.2 IEEE802.11的物理层

8.2 IEEE802.11的物理层

- 无线频段
  - 多数无线频段由政府管理和分配，需**license**才可使用
  - 预留了无需许可即可免费使用的频段
    - **ISM**频段：**ISM---Industrial, Scientific, Medical**
    - 限制：发射功率 < **1Watt (WLAN**一般不超过**50mW)**



未来可能增加**60GHz**频段用于家庭和个人无线应用

8.2 IEEE802.11的物理层

- **802.11物理层的几种实现方法：**
  - ① 红外IR
    早期，已很少使用
  - ② 2.4GHz跳频扩频FHSS
    早期，已很少使用
  - ③ 直序扩频DSSS
    IEEE80211b，速率11Mbps，广泛应用
  - ④ 正交频分复用(OFDM)
    2003年，IEEE802.11g，速率54Mbps
  - ⑤ 多入多出(MIMO)+OFDM
    2009年，IEEE802.11n，速率600Mbps

8.2 IEEE802.11的物理层

标准	频段	数据速率	物理层	优缺点
802.11b	**2.4GHz**	最高 **11 Mb/s**	**HR-DSSS**	数据速率较低 信号传播距离远，不易受阻碍
802.11a	**5 GHz**	最高 **54 Mb/s**	**OFDM**	数据速率较高 支持更多用户同时上网 信号传播距离较短，易受阻碍
802.11g	**2.4GHz**	最高 **54 Mb/s**	**OFDM**	数据速率较高 支持更多用户同时上网 信号传播距离远，不易受阻碍
802.11n	**2.4GHz** **5GHz**	最高 **600Mb/s**	**MIMO +** **OFDM**	数据速率最高

TP-LINK WDR6500

- 无线路由器
- 无线标准：IEEE 802.11b/g/n/…
- 无线传输速率(最高)：1300Mbps
- 1个10/100/1000M WAN口
- 4个10/100/1000M LAN口

华为E5573s-853

- 4G无线路由器(移动WiFi)
- 联通4G/电信4G
  - LTE/TD-SCDMA，最高150Mbps
- 无线标准：IEEE 802.11n
- 无线传输速率：150Mbps
- 产品净重：75g

8.3 IEEE802.11的MAC层

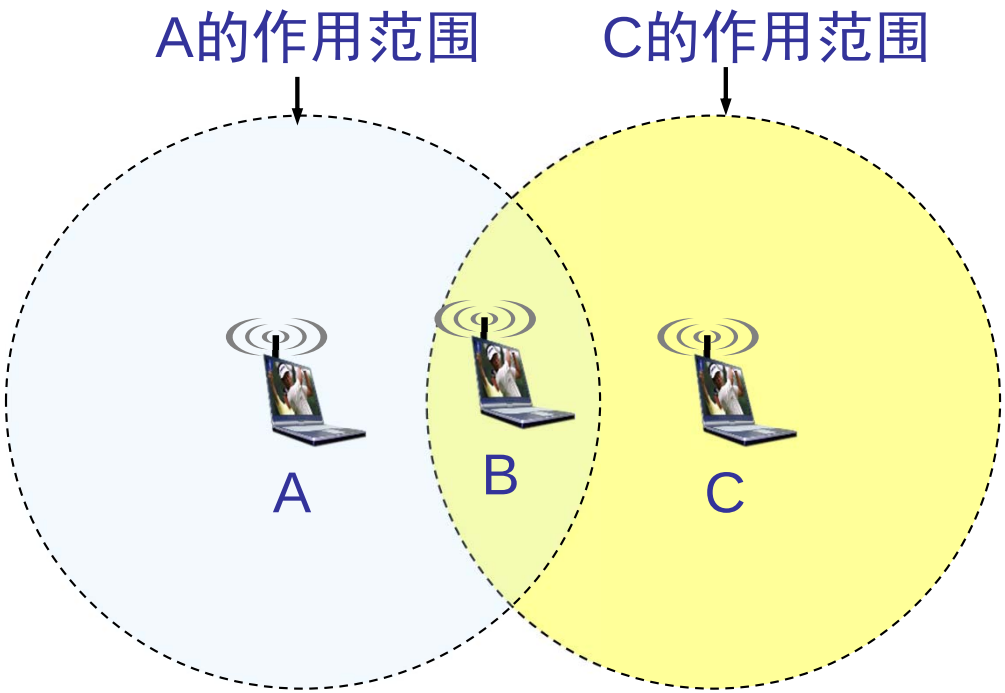
8.3 IEEE802.11的MAC层

- 以太网的CSMA/CD协议取得了巨大的成功
- WLAN与以太网同属IEEE802系列标准
- 无线网络的特点使得WLAN不能简单照搬CSMA/CD：
  - 无线网络适配器的接收信号强度远小于发送信号强度，像CSMA/CD协议那样进行碰撞检测(边发送边听)比较困难
  - 无线信号覆盖范围有限，即使能够进行碰撞检测，也可能检测不到碰撞 → 隐蔽站问题
- WLAN使用CSMA/CA协议

  CSMA/CA: Carrier Sense Multiple Access / Collision Avoidance
  - 由于无线网络的特性，难以像有线网络那样检测冲突，因此着眼于避免冲突
  - 比CSMA/CD复杂得多

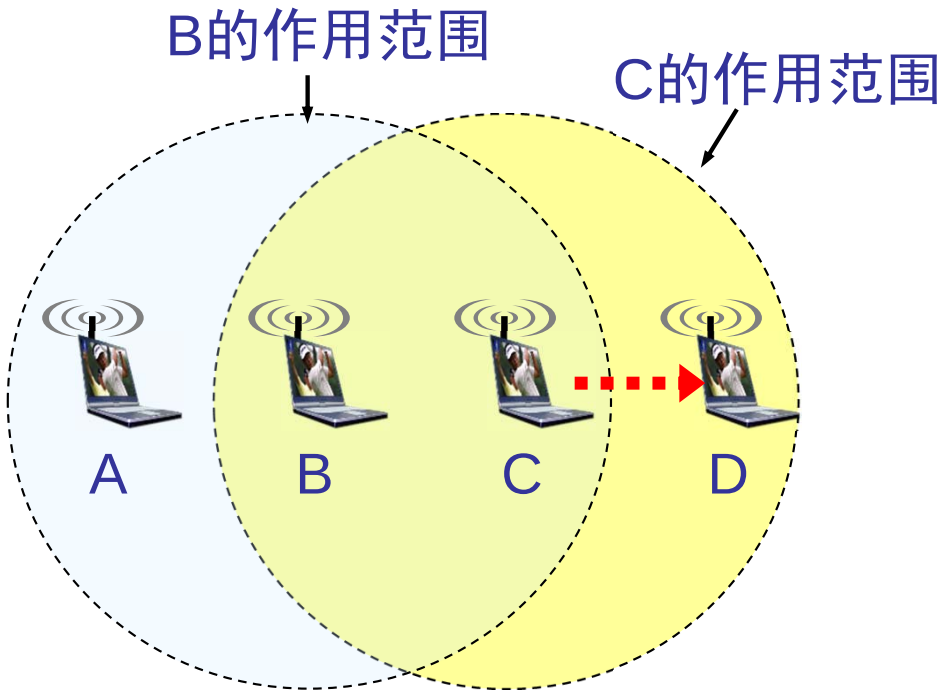
无线网络的隐藏站和暴露站问题使得无法沿用以太网的CSMA/CD协议

隐藏站问题
(hidden station problem)



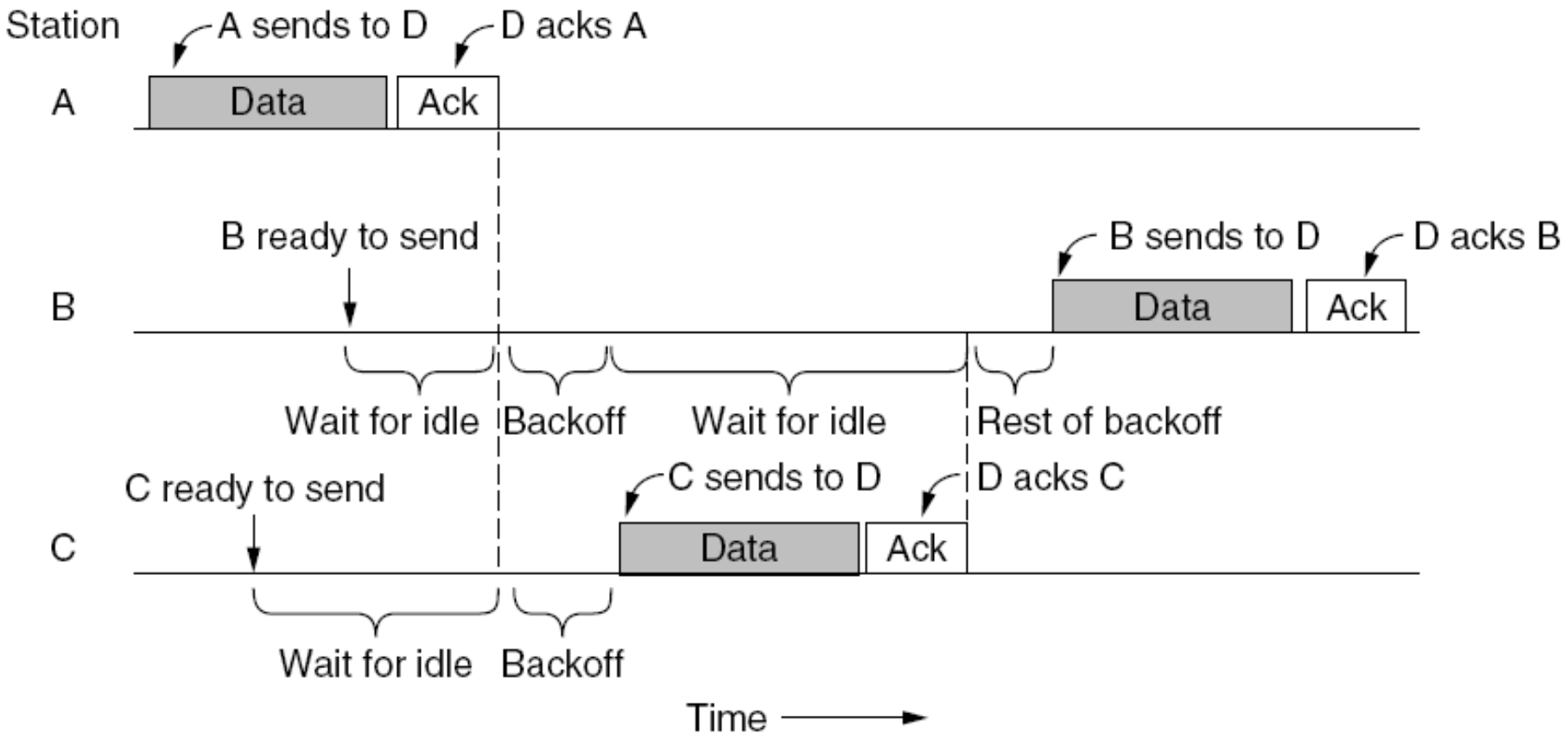
- A、C都向B发送数据，在B站发生碰撞，但A、C检测不到

暴露站问题
(exposed station problem)



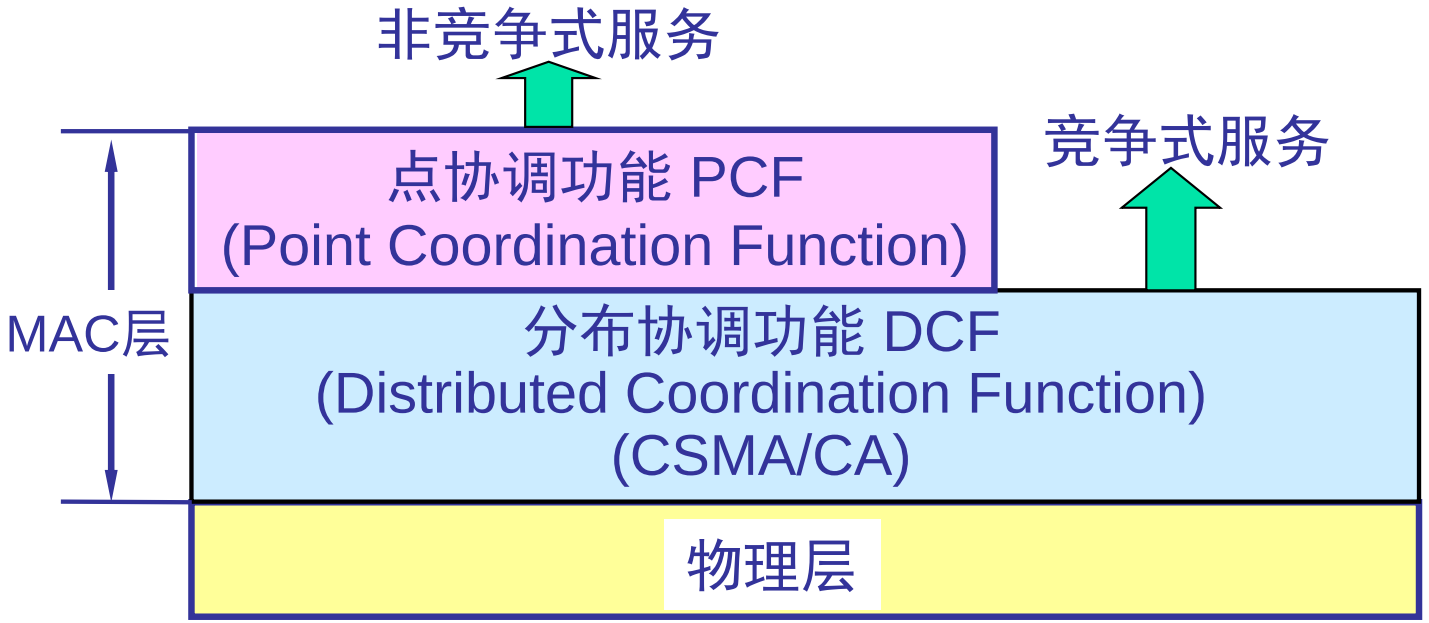
- B正向A发送时，C向D发送
- C检测到传输介质上有信号，于是等待
- C本不必等待

- 一个发送帧的时序例子：
  ① A正在向D发送帧，此时B、C也准备发送，它们检测到信道忙，于是等待
  ② A收到来自D的确认帧(ACK)，信道变为空闲
  ③ B、C不是立即发送导致冲突，而是先执行退避算法
  ④ C退避时间较短，先开始发送，B退避完成后发现信道忙，继续等待、退避
- 与CSMA/CD的两个重要区别：
  - 退避在前，有助于避免冲突 ← 无线网中冲突代价较大
  - 利用确认帧推断是否发生冲突 ← 无线网中检测冲突很困难



8.3 IEEE802.11的MAC层

- 802.11的MAC层提供两种服务
  - 分布协调功能 DCF：各站按照CSMA/CA协议竞争使用信道
  - 点协调功能 PCF：集中控制方法，由AP逐个轮询各站发送数据，避免了碰撞的产生
- 在实际应用中，DCF使用较多
  - DCF需要考虑的问题：如何尽可能减少冲突



8.3 IEEE802.11的MAC层

虚拟载波监听可减少移动站的能耗，有利于电池供电设备

- **802.11的载波监听机制**
  - ① 物理载波监听：简单地检查信道看是否存在有效的信号
  - ② 虚拟载波监听：**802.11**特有的机制
- **虚拟载波监听(Virtual Carrier Sense)**
  - 发送站将它要占用信道的时间放在发送帧中，其他站在收到该信息后，将不在这一段时间内发送数据 → 冲突概率大大减少
  - 该时间放置在**MAC**帧 “持续时间**(Duration)**”字段
    - 本帧结束后还要占用信道多少时间(单位: 微秒)，包括确认帧所需时间
  - “虚拟载波监听”的意思是：其他站并没有监听信道，而是在收到发送站的通知后才不发送数据
- **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 (Network Allocation Vector)**
  - **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。

- 使用CSMA/CA的虚拟信道监听
  - RTS/CTS机制与NAV配合使用，防止隐藏站在同一时间发送，减少冲突

① A向B发送数据帧之前，先发送一个RTS帧(请求发送)

② B如果收到此请求，返回一个CTS帧(允许发送)

③ A开始发送数据帧，并启动一个ACK计时器

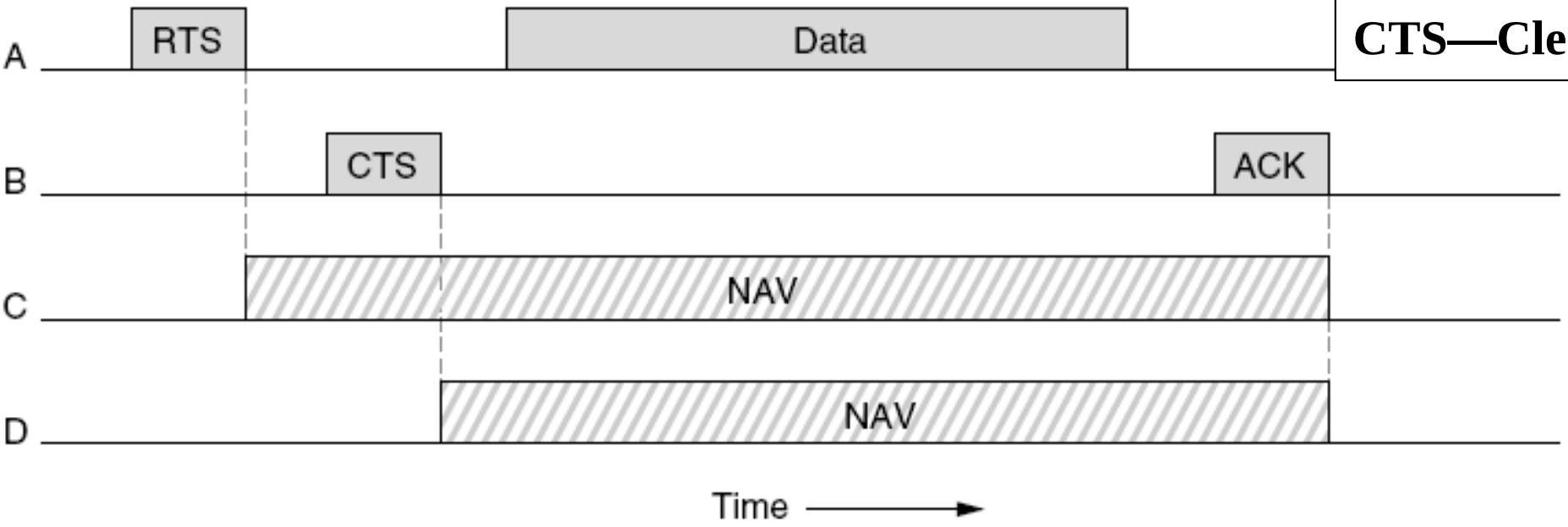
④ B收到数据帧后，返回一个ACK

⑤ 如果ACK计时器超时而未收到ACK，则认为发生了冲突，后退后重新启动发送

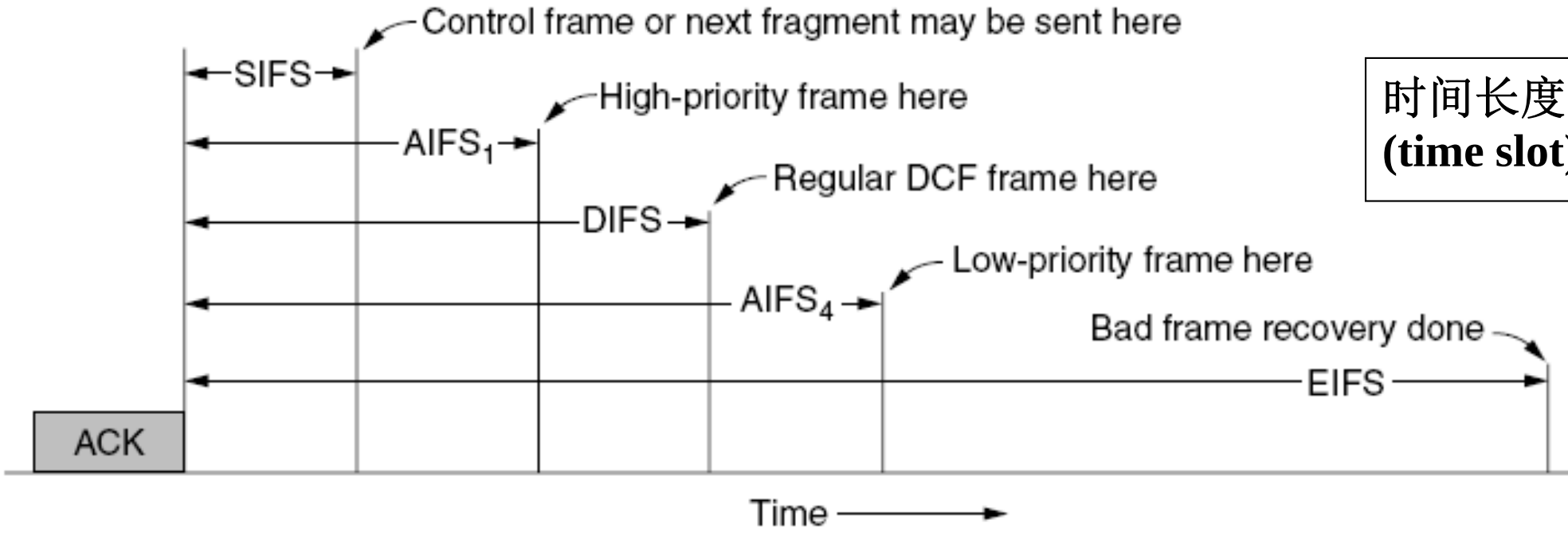
  - 如果C、D是隐藏站，就会收到RTS或CTS，由此更新自己的NAV，并在此段时间内停止发送

RTS—Ready to send

CTS—Clear to send



- **帧间间隔(InterFrame Space)**
  - **IEEE 802.11e，2005年，扩展了CSMA/CA**
  - 一帧发出后，需要保持一段时间的空闲，任何站才可以发送帧
  - 为不同类型的帧定义了不同的时间间隔
    - ① **SIFS: Short IFS**，短帧间间隔，用于**CTS、ACK**等帧
    - ② **DIFS: DCF IFS**，**DCF**帧间间隔，用于**DCF**模式下数据帧
    - ③ **AIFS1/AIFS4: Arbitration IFS**，不同优先级的帧
    - ④ **EIFS: Extended IFS**，收到坏帧时报告问题
  - 帧间间隔机制使得在竞争式发送时，高优先级帧可以优先发送



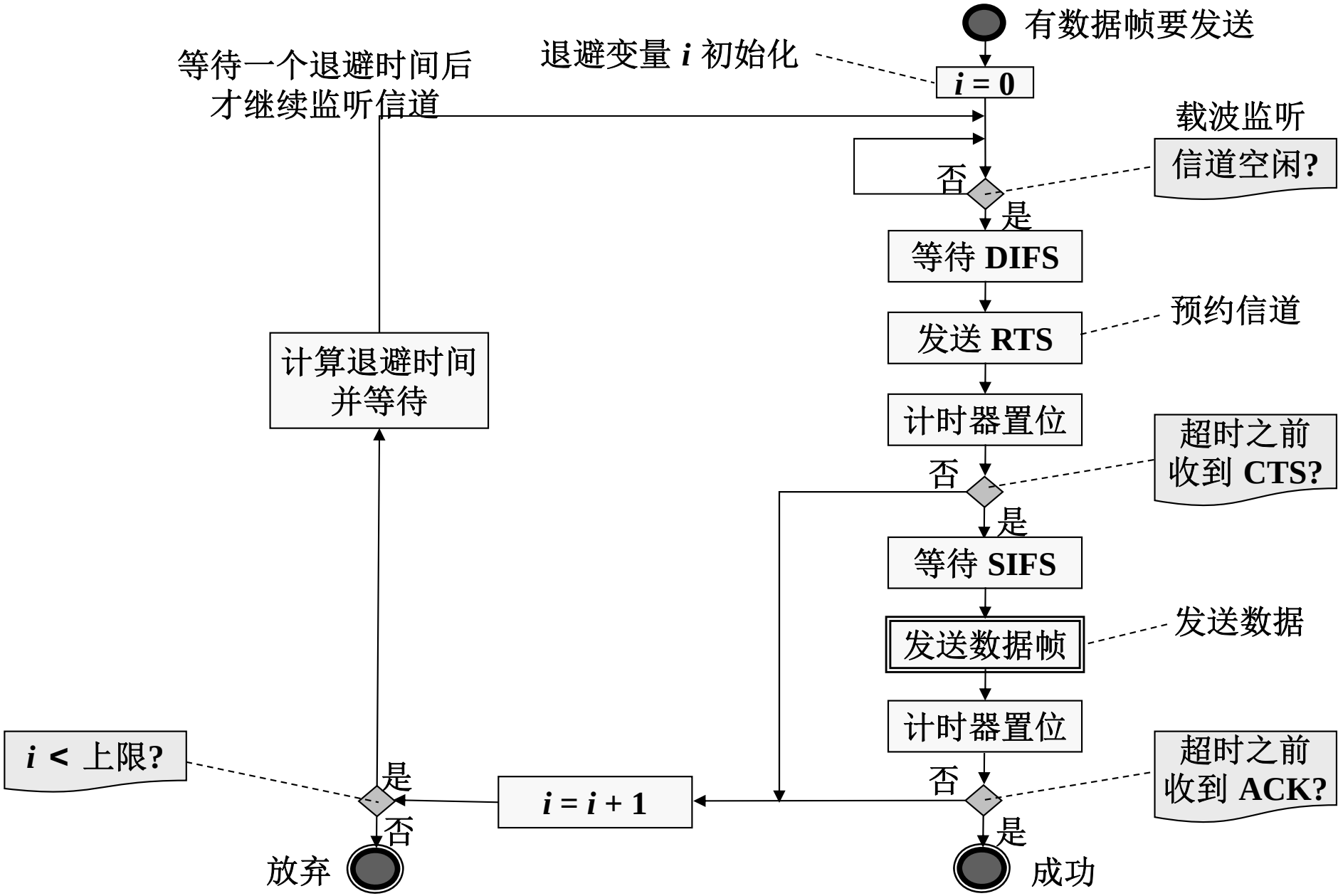
时间长度以时隙**(time slot)**为单位

8.3 IEEE802.11的MAC层

- **CSMA/CA的退避算法**
  - 一个站要发送数据时，检测到信道空闲后，退避一段时间再检测信道并发送 **(注：退避时间与帧间间隔不同)**
  - 使用二进制指数退避算法：

    第**i**次退避：在2^{2+i}个时隙中随机选择，即：**{0, 1, …, 2^{2+i-1}}**
    - 第**1**次退避：退避时间**0—7**个时隙
    - 第**2**次退避：退避时间**0—15**个时隙
  - 站点每过一个时隙就检测一次信道：
    - 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

CSMA/CA发送的基本流程图



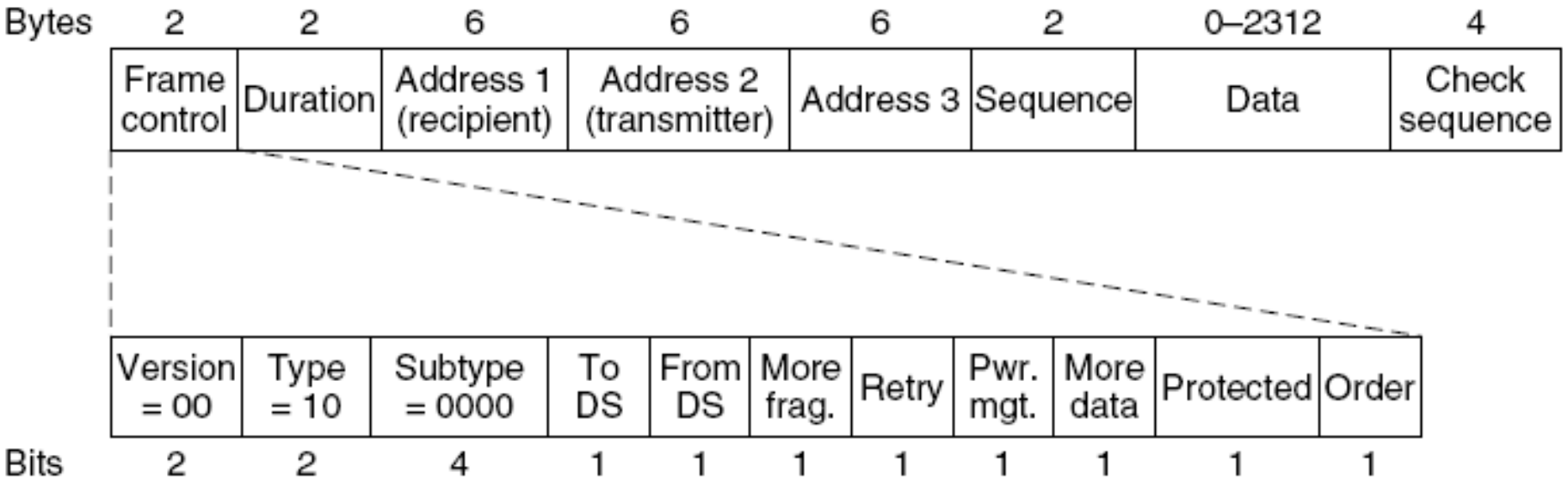
8.3 IEEE802.11的MAC层

- **CSMA/CA主要特性总结**
  - 发送前退避
    → 同时检测到信道空闲的站退避时间长度不同
  - 发送站/接收站之间**RTS/CTS**握手
    → 使隐藏站得知数据传输
  - 虚拟载波监听与**NAV**配合使用
    → 等待站无须持续监听信道
  - 接收站正确接收数据帧后，需返回**ACK**帧
    → 使发送站知道是否发生冲突
  - 不同类型的帧设置不同的帧间间隔
    → 控制帧等高优先级帧能更快地发送出去

问：按照CSMA/CA协议，网络中是否可能发生冲突？

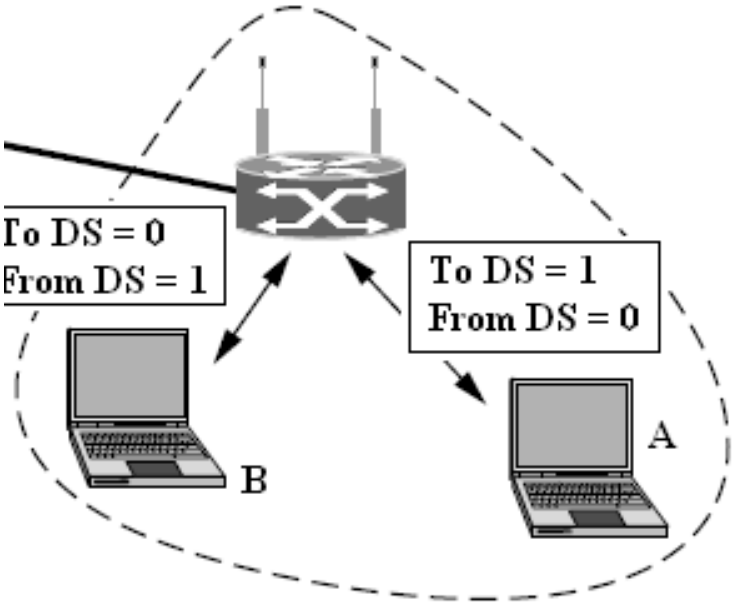
8.4 IEEE802.11的帧结构

- **802.11的帧分为三种类型：数据帧、控制帧、管理帧**
- **帧控制(Frame control)：包含11个子字段**
  - **Version:** 协议版本
  - **Type和Subtype:** 帧类型(数据、控制、管理)和子类型(如**RTS**、**CTS**等)
  - **To DS和From DS:** 该帧是发送到或是来自于**AP**连接的网络
  - **More Fragment:** 分片传输用
  - **Retry:** 是否是重传帧
  - **Power management:** 指明发送方进入节能模式
  - **More data:** 发送方还有更多的帧需要发送
  - **Protected frame:** 该帧数据部分是否被加密
  - **Order:** 告诉接收方高层是否按顺序处理帧序列

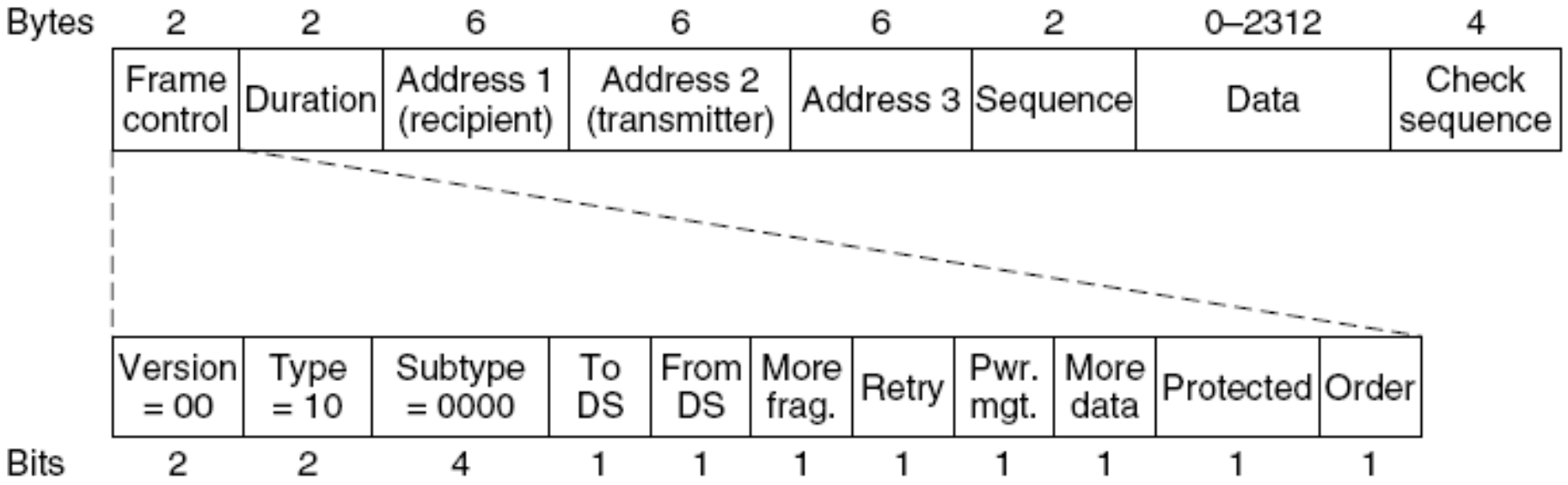


- 持续时间(Duration)
  - 本帧及ACK帧将占用信道时间(单位:微秒)
  - 其它站根据该字段调整NAV，进行虚拟载波监听
- 地址(Address)：
  - 连续3个字段，802标准地址(即MAC地址)
  - 网内两个站之间通信需通过AP，涉及三个地址

到 DS	从 DS	Address 1	Address 2	Address 3
0	1	目的地址	AP 地址	源地址
1	0	AP 地址	源地址	目的地址

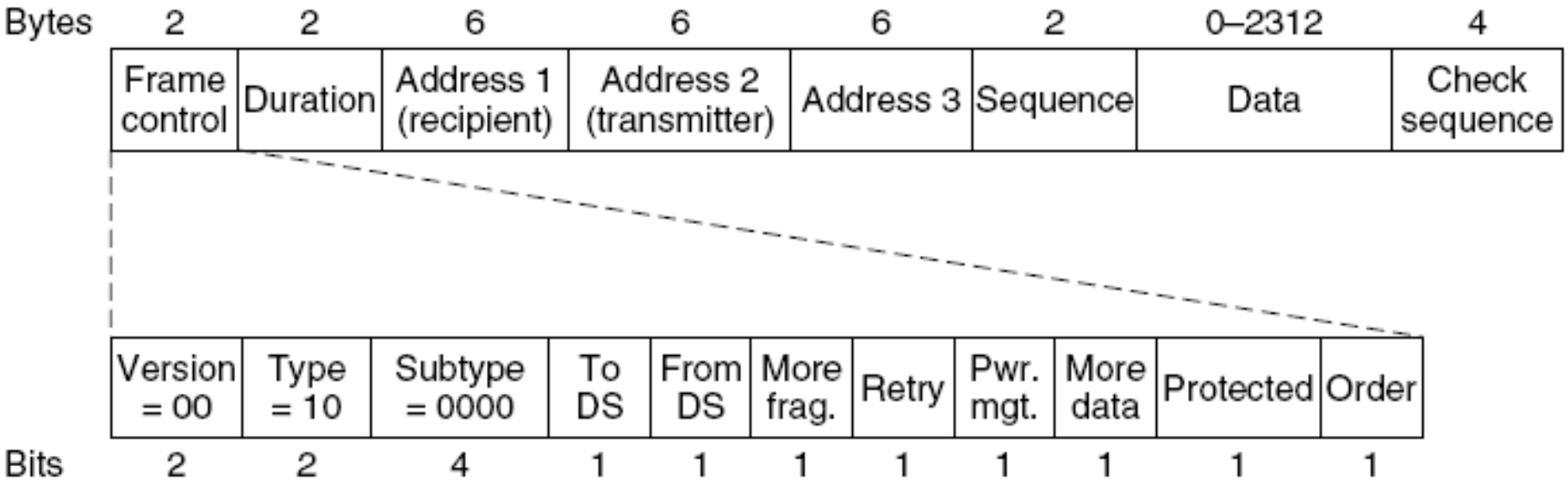


A向B发送帧需通过AP



8.4 IEEE802.11的帧结构

- 帧序号(Sequence)：2字节，用于重复帧的检测
- 数据(Data)：帧的有效载荷
  - 帧中数据最多2312字节
  - 一般小于1500字节
- 帧校验(Frame check sequence)：32位CRC校验
- 管理帧格式与数据帧相同，数据内容依管理帧类型而不同
- 控制帧较短，只有一个地址，没有数据



8.5 IEEE802.11的安全性

8.5 IEEE802.11的安全性

- 第一代安全协议：**WEP(Wired Equivalent Privacy)**
  - 各方面安全性都存在缺陷
    - 通过异或操作加密数据，密钥分配较弱导致输出经常重复
    - 通过32位CRC实现完整性保护，防攻击能力很弱
  - **2002**年被首次攻破
  - 目前使用免费软件可在很短时间内破解**WEP**
- 在此背景下，**802.11i**组仓促上马
  - **2003**年推出**WPA(WiFi Protected Access)**
  - **2004**年推出**WPA2**，成为正式标准
  - **WPA**是**802.11i**的子集
- 同一时期，中国推出了**WAPI(Wireless LAN Authentication and Privacy Infrastructure)**，强制性国家标准→原理与**802.11i**相似

8.5 IEEE802.11的安全性

- 移动站在通过AP发送帧之前须进行认证(authentication)
  - 如果802.11网络是开放(open)的
    - 可直接通信，无需认证
  - 否则必须进行认证
- WPA2的两种认证方式

  ① 有认证服务器
  - 配置认证服务器，存有用户名和口令数据库
  - 使用802.1x实现认证
  - 适用于企业

  ② 无认证服务器
  - 移动站和AP间使用预共享密钥(preshared key)进行认证
  - 适用于家庭和小型应用场合

- 认证握手过程：4次握手
  ① AP发出一个随机数(nonce)用于识别(nonce: 仅使用一次的临时值)
  ② 客户端选取自己的临时值nonce，并用其nonce、MAC地址、AP的MAC地址、主密钥作为参数计算会话密钥K_S，客户端将自己的临时值和消息完整性检查值(MIC)发送给AP
  ③ AP分发一个组密钥K_G，用于后续的广播和组播
  ④ 客户端确认组密钥
- 后续的通信使用AES算法加密，密钥为会话密钥K_S