# 无线局域网802.11

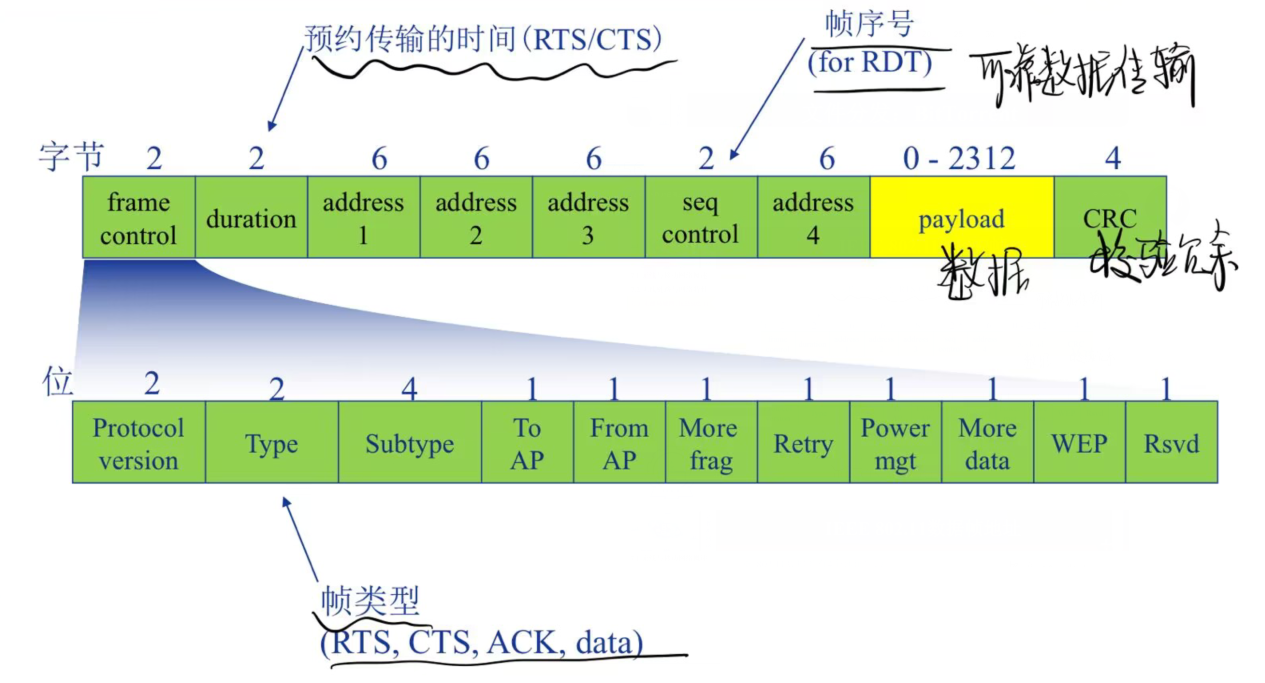
1. IEEE802.11无线局域网：按照不同频段可以做以下划分，最高速率从上至下递增
   1. 802.11b
      1. 物理层采用直接扩频序列（所有主机码片序列相同）--CDM也是这种技术，但码片序列正交
      2. 最高数据率较低，价格最低，信号传播距离最远，不易受阻
   2. 802.11a
      1. 最高数据率较高，价格最高，信号传播距离较短，易受阻，支持更多用户同时上网
   3. 802.11g
      1. 最高数据率较高，信号传播距离最远，不易受阻，支持更多用户同时上网，比b贵
   4. 802.11n（多天线MIMO）
      1. 使用多个发射和接收天线以允许更高的数据传输率，使用双倍带宽时速率很高
   5. 均使用**CSMA/CD**多路访问控制协议，均有**基础设施（基站）网络模式**和**特定网（自组织）网络模式**
2. 802.11 LAN 体系结构
   1. 无线主机与基站通信：基站=访问点（AP）
   2. 基本服务集BSS，也称为单元（cell）
      1. 基础设施网络模式/基站网络模式：无线主机+AP（基站）
      2. 自组织网络模式：只有主机
3. 802.11：信道与关联
   1. 频谱划分为不同频率的信道
      1. 每个AP选择一个频率（信道）
      2. 存在干扰可能，相邻的AP可能选择相同的信道
   2. 主机：必须与某个AP关联
      1. 扫描信道，监听包含AP名称和MAC地址的**信标帧**（AP会定期广播这种信标帧）
         1. **被动扫描**：AP发，主机收
            1. AP发送信标帧，主机向选择的AP发送关联请求帧，AP收到后向主机发送关联响应帧
         2. **主动扫描**：主机发，AP收
            1. 主机**广播**探测请求帧，AP发送探测响应帧，主机向选择的AP发送关联请求帧，AP向主机发送关联响应帧
      2. 选择一个AP进行关联
      3. 可能需要进行身份认证
      4. 回忆一下，DHCP动态获取IP地址的过程，很类似
4. **802.11 多路访问控制**
   1. CSMA：发送数据前监听信道，避免与传输中的其他结点冲突
      1. 难点：不能像CSMD/CD那样边发边听
         1. 无线信道中接收信号强度会被发射信号强度淹没
         2. 无法侦听到所有可能的冲突：**隐藏站**、信号衰落
      2. 目标：避免冲突——CSMA/CA
   2. **CSMA/CA**
      1. DIFS：分布式帧间间隔；SIFS：短帧帧间间隔
      2. 冲突避免基本过程
         1. 发送方：
            1. 监听到信道空闲了DIFS时间，则发送完整的帧（不同时检测冲突）
            2. 监听到信道忙，开始随机退避倒计时

当信道空闲且DIFS时间后，计时器倒计时（-1），否则不变

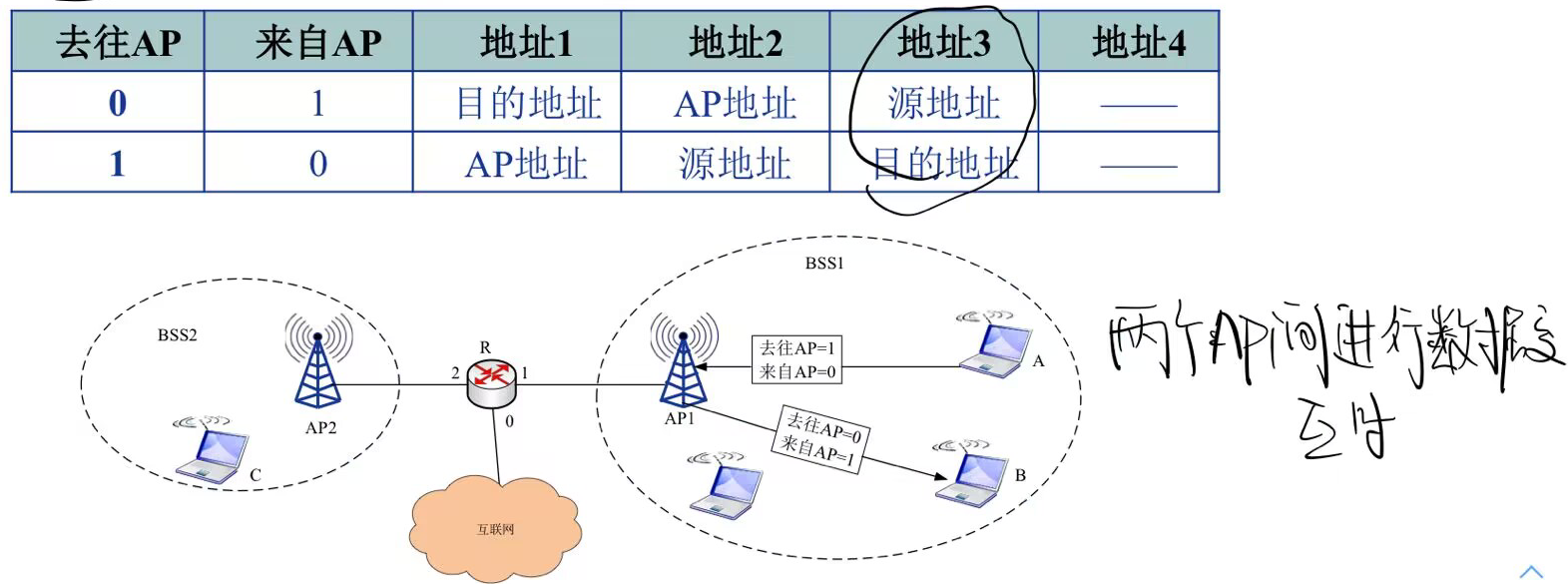
计时器超时，发送完整的帧

如果没有收到ACK，增加随机退避间隔时间（信道冲突，接着等），继续倒计时

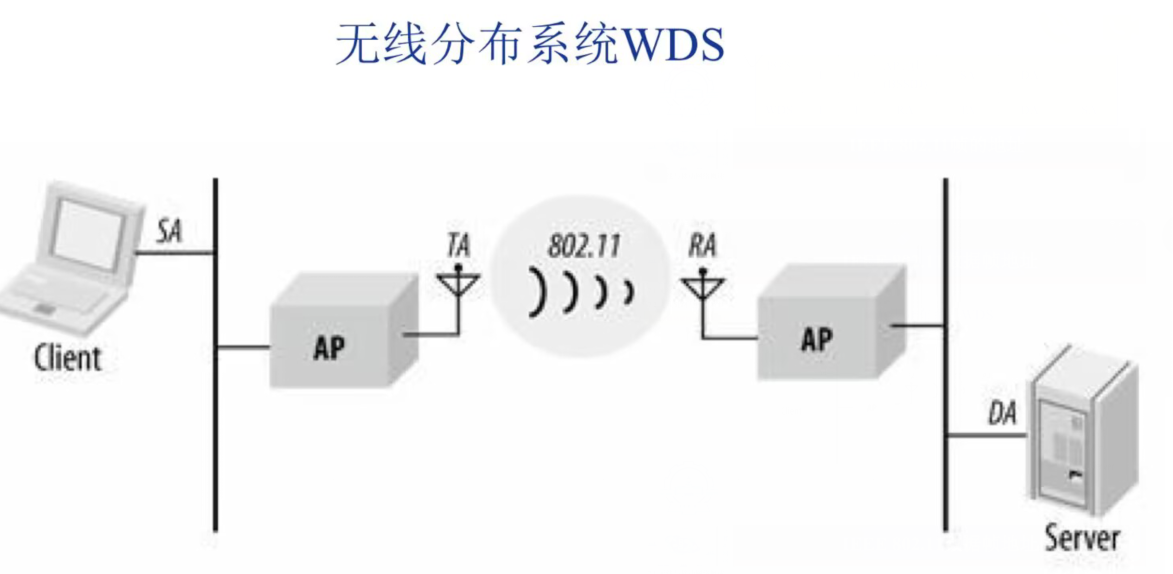
* + - 1. 接收方：
         1. 正确接收帧，则在延迟SIFS时间后（解决隐藏站问题），向发送方发送ACK
    1. 基本思想：允许发送方**预约**信道，而不是随机发送数据帧，从而避免长数据帧的冲突
    2. 预约过程
       1. 发送端首先向基站发送一个RTS帧（预约请求帧）
          1. RTS也可能冲突，但帧短，处理起来容易得多
       2. 基站广播一个CTS帧（预约响应帧）作为对RTS的响应
          1. 使用广播，CTS可以被所有基站接收，消除隐藏站影响，让其他站推迟发送数据
    3. 交换数据过程：
       1. 主机监听信道，空闲了DIFS后向基站发送一个RTS
       2. 基站收到RTS后，等待一个SIFS，向主机回复一个CTS
       3. 主机在收到基站回复的CTS后，延迟一个SIFS，开始向基站发送数据
       4. 基站接收数据，完毕后延迟一个SIFS，**广播**一个ACK，告知所有主机，这次数据传输完成
    4. 由以上过程可知，一个主机从期望开始发送数据开始，到确认数据被基站正确接受，最快需要DIFS+3SIFS（忽略传输时延、传播时延和处理时延）
  1. 802.11 MAC帧



* + 1. 各字段的作用如上图所示，其中frame control字段还可按位划分
    2. **802.11数据帧地址**
       1. 地址1：主机或AP的MAC地址，指明帧的接收方
       2. 地址2：主机或AP的MAC地址，指明帧的发送方
       3. 地址3：最初源地址或最终目的地址（看在哪个阶段）
       4. 地址4：用于Ad-hoc或无线桥接







* 1. 802.11 同一子网内的移动性：交换机看到来自H1的帧并记住哪个交换机端口可以用于到达H1
  2. 802.11 高级功能
     1. 速率适应：
        1. 移动终端移动、SNR变化时，基站、移动终端会动态改变传输速率（通过物理层调制技术）
        2. 移动终端远离基站，SNR降低，BER（比特误码率）增加，此时切换到低传输速率以降低BER
     2. 功率管理（省电）：
        1. 结点到AP：
           1. 结点会休眠到下一个信标帧，此时AP就不向结点发送数据帧
           2. 结点会在下一个信标帧之前唤醒
        2. **信标帧**：包含了一个移动终端列表，AP**缓存**了等待发送给这些移动终端的帧
        3. 若AP到移动终端的帧将要发送，结点保持唤醒，否则休眠直到下一个信标帧
           1. 这波给我发数据，我就醒着，否则就下一波再说
  3. 个人局域网：蓝牙
     1. 典型的自组织网络
     2. 主设备/客户端设备：主设备轮询客户端，授予客户端传输请求
     3. 寄放模式：客户端可以进入寄放状态（睡眠）并稍后唤醒（省电）
     4. 自助：节点自组装，即插即用