# 2.计算机网络-数据链路层

1. 数据链路层服务：
   1. 负责结点-结点间数据传输
      1. 结点：主机、路由器、交换机
      2. 链路：连接相邻结点的通信信道
         1. 有线链路
         2. 无线链路
         3. 局域网
      3. 数据链路层负责通过一条链路从一个节点向另一个物理链路直接相连的相邻结点传送数据报
   2. 组帧
      1. 帧：链路层数据分组，封装网络层数据报
      2. 帧同步：从物理层接收的比特流中准确区分出一帧的开始与结束
         1. 字节计数法：数数
         2. 带字节填充的定界符法：利用特殊字节-定界符区分前后两个不同帧
            1. 有效载荷可能包含与定界符相同的位组合，怎么办？
         3. 带比特填充的定界符法：在有效载荷中与定界符相同的位组合处插入比特
         4. 物理层编码违例：将定界符设定为不会在数据部分出现的码字，例如：
            1. 4B/5B编码方案：直接选取未使用的码字
            2. 前导码：存在很长的前导码
            3. （差分）曼彻斯特编码：比特周期中间信号无跳变
   3. 物理寻址：MAC地址
   4. 流量控制
      1. 基于反馈的流量控制：接收方反馈，发送方调整
      2. 基于速率的流量控制：发送方根据内建机制自行限速
   5. 差错控制
   6. 访问控制
   7. 向下利用物理层提供的位流服务，向网络层提供服务接口
      1. 利用下层服务，为上层提供服务接口，这是中间层次的统一特征
   8. ps-链路层的具体实现：在适配器或芯片中同时实现物理层和数据链路层
2. 差错检测与纠正
   1. 差错编码：D->DR，其中R为纠正比特（冗余比特、监督位）
      1. 按功能可分为检错码和纠错码
      2. 按实现方式可分为分组码和卷积码，分组码又可分为线性或非线性分组码
      3. 差错编码并不能保证100%可靠
      4. 汉明距离：两个码字之间对应位不同的数目（按位异或，结果1的数目）
         1. 编码集的汉明距离：所有码字之间汉明距离的最小值
         2. 对于检错码，如果编码集的汉明距离为r+1，则该差错编码可以检测r位差错
         3. 对于纠错码，如果编码集的汉明距离为2r+1，则该差错编码可以纠正r位差错
         4. 例：{0000,0101,1010,1111}汉明距离为2；{000000,010101,101010,111111}汉明距离为3
   2. 奇偶校验：
      1. 1比特校验位：检测奇数位差错，50%准确率
      2. 二维奇偶校验：检测（同一行/列的）奇数位差错，部分偶数位差错
   3. Internet校验和（Checksum）：分组的校验和字段
      1. 发送端：将数据划分为16位整数序列，反码循环求和，再求反码
      2. 接收端：一样算，检测得到的checksum是否为16位全0或全1，是则无措；否则有错
   4. 循环冗余校验码（CRC）：
      1. 将数据比特D视为二进制数，选择一个r+1位的比特模式G，目标是找到r位的CRC比特R，使得<D,R>能够被G模2整除（即加法是按位异或）
      2. D左移r位，模2除以G，得到的余式即为R
      3. 可以检测所有突发长度小于r+1位差错：能力强大
      4. 广泛应用于实际网络应用（以太网、802.11WiFi、ATM等）
   5. 差错纠正：
      1. 前向纠错
         1. 纠错码
      2. 检错重发
         1. 停-等协议
         2. 滑动窗口协议
3. 可靠数据传输
   1. 可靠：不错、不丢、不乱、不多。信道的不可靠特性决定了可靠数据传输的复杂性
   2. 基本结构：发送方在传输层做完rdt的工作后将数据报交给下层，在不可靠信道上向接收方传输数据，接收方调用rdt响应处理到达的数据
   3. 渐进地设计可靠数据传输协议的发送方和接收方，只考虑单向数据传输（但控制信息双向流动）
   4. Rdt1.0：可靠信道上的可靠数据传输
      1. 底层信道完全可靠，不会发生错误，不会丢弃分组
      2. 发送方和接收方的FSM独立
   5. Rdt2.0：可能产生位错误的信道。“停-等协议”
      1. 底层信道可能翻转分组中的位：利用校验和检测位错误
      2. 使用确认机制（ACK），接收方显示地告知发送方分组已正确接收，发送方会等待接收方的反馈
      3. NAK：接收方显示告知发送方分组出错，发送方收到后重传分组
      4. 引入重传机制的rdt协议称为ARQ协议
      5. 缺陷：
         1. ACK/NAK消息可能坏掉，重传又可能产生重复分组
         2. 解决重复分组：发送方为每组增加序列号，接收方丢弃重复分组
   6. Rdt2.1：应对ACK/NAK被破坏
      1. 引入了序列号机制的Rdt。两个序列号就够用
      2. 若收到重复分组，即非期望收到的分组，丢弃后继续等待
   7. Rdt2.2：与Rdt2.1功能相同，但只使用ACK消息，抛弃了NAK
      1. 在ACK消息中显示加入了被确认分组的序列号
      2. 发送方收到重复ACK后重传当前分组
   8. Rdt3.0：引入定时器，发送方等待一定时间，超时则重传
      1. 工作正确，但太慢了--一直在等待
      2. 引入流水线机制
   9. 流水线协议：允许发送方在收到ACK之前连续发送多个分组
      1. 需要更大的序列号范围，发送方和接收方需要更大的存储空间缓存分组
   10. 滑动窗口协议
       1. 窗口：允许使用的序列号范围；窗口尺寸为N代表最多有N个等待确认的消息
       2. 滑动窗口：随着协议的进行，窗口在序列号空间内向前滑动
       3. 常见协议：GBN、SR
   11. GBN（Go Back N）协议：
       1. 分组头部包含k-bit序列号
       2. 累计确认：ACK（n）代表0到n均已经被正确接收
       3. 为空中的分组设置计时器，超时则重传序列号大于等于send\_base且还未收到ACK的所有分组
       4. 可能产生重复ACK，但只需要记住唯一的期望序列号（下一个想收到的）
       5. 乱序到达的分组：
          1. 接收窗口为1，接收方没有缓存，故要直接丢弃
          2. 重新确认序列号最大的按序到达的分组
       6. 缺点：重传太多，低效且浪费资源
   12. SR（Selective Repeat）协议：
       1. 接收方对每个分组单独确认
          1. 设置缓存机制，缓存乱序到达的分组
       2. 发送方只重传没收到ACK的分组
          1. 为每个分组设置定时器，同样的是超时则重传
       3. 发送方与接收方窗口不同步
          1. 发送方窗口：N个连续的序列号，限制已发送未确认的分组
          2. 接收方窗口：可以接收的无差错到达的分组序号
       4. 困境：若序列号设置过少，则可能导致接收方错误解析数据
          1. 发送窗口与接收窗口尺寸的和需要能用k位序列号空间表示
4. 多路访问控制（MAC）协议
   1. 多路访问控制协议：广播链路可能存在冲突，故需要采用分布式算法决策如何共享信道
   2. 理想MAC协议：只有一个结点希望传输数据时可以以全速发送，M个结点发送数据时带宽被均分
      1. 完全分散控制，无需特定结点协调，无需时钟、时隙同步
   3. MAC协议分类
      1. 信道划分MAC协议：多路复用技术、TDMA、FDMA、CDMA、WDMA等
         1. TDMA：时间上划分信道，每个站点周期性接入信道，占用固定长度的时隙，未用时隙空闲
         2. FDMA：频谱上划分信道，每个站点分配一个固定频带，无传输频带空闲
      2. 随机访问MAC协议：时隙ALOHA、ALOHA、CSMA、CSMA/CD、CSMA/CA等
         1. 信道不划分，允许冲突，采用冲突恢复机制
         2. 时隙ALOHA协议：
            1. 所有帧大小相同，时间划分为等长的时隙，结点间时钟同步且只能在时隙开始时刻发送帧
            2. 保证每个时隙可以传输1个帧，若两个或以上结点在同一时隙发送帧，则结点检测到冲突
            3. 结点有新的帧时：

若无冲突，下一个时隙继续发送新的帧

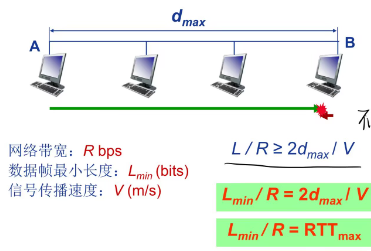
若有冲突，结点在下一个时隙以概率p重传该帧直至成功

* + - * 1. 优点：单结点可以以全部速率传输，思路简单，且高度分散化，只需同步时隙
        2. 缺点：易冲突，浪费时隙，且需要实现时钟同步的开销，且最大效率只有37%
      1. ALOHA协议：非时隙的ALOHA，更简单，无需同步时钟
         1. 在有新生成的帧时，立即发送——冲突可能性增大；效果比时隙ALOHA更差
      2. CSMA（载波监听多路访问）协议：引入了监听机制
         1. 发送帧之前监听信道，信道空闲则发送完整帧，否则推迟发送
         2. **CSMA/CD协议**：在监听基础上引入了冲突检测机制

边发边听，不发不听，可以在短时间内检测到冲突，冲突后传输中止

有线局域网易于实现，无线局域网则很难实现（接收信号强度被淹没）

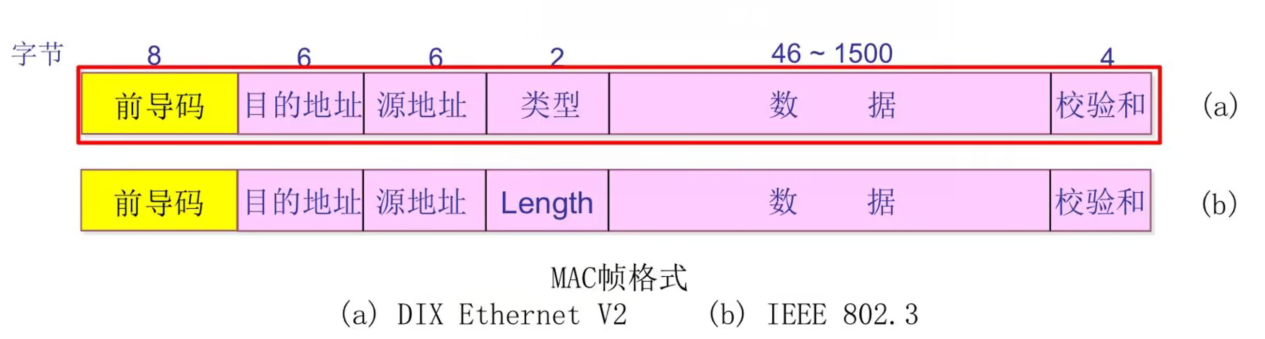
可以检测出冲突的前提是：



为什么是2d/V呢？设想一下，A发送数据经过d/V的时间到达B，此时B刚好开始发数据，检测到A发送的数据后B停止发送，B发送出的数据经过第二个d/V的时间到达A，此时A才知道发生了冲突。故若从A发送数据开始经过2d/V的时间还未冲突，则一定不会冲突

* + 1. 轮转MAC协议：结点轮流使用信道
       1. 综合了信道划分与随机访问两者的优点
       2. 轮询机制：主结点轮流邀请从属结点发送数据
       3. 令牌传递：控制令牌依次从一个结点传递到下一个结点（令牌：特殊帧）
       4. 比特映像介质访问控制协议：将时间划分为一系列的预约周期与数据传输周期，先预约
          1. 任意预约周期包括N个时隙，每个时隙1比特，对应一个站
          2. 任意一个站想发送数据，必须在它的时隙到来时发一个1
          3. 一轮预约周期后，所有站都知道谁要发数据，按照预约的顺序发送，永不冲突

1. 局域网技术
   1. 链路层寻址：MAC地址（LAN地址、以太网地址、物理地址）
   2. 局域网中的每一块网卡都有一个唯一的MAC地址
   3. 以太网
      1. 物理拓扑：总线/星型
      2. 无连接、不可靠、采用二进制指数退避算法的CSMA/CD协议
      3. 二进制指数退避：第m次连续冲突后，取n=min{m,10}，从0到2的n-1次幂选择一个数K，等待K\*512个比特的传输延迟时间，再返回监听信道尝试传输
      4. 以太网帧结构

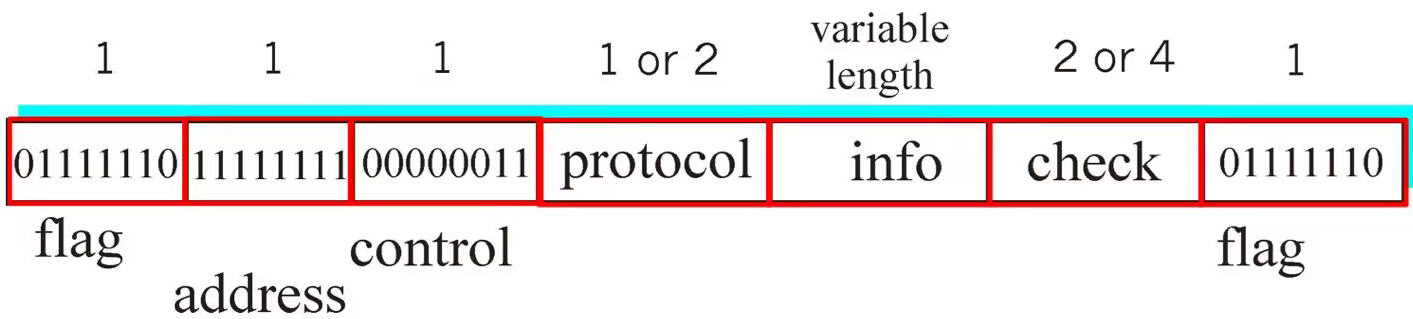


* + - 1. 前导码：前7个字节10101010，第8个字节为10101011，用于时钟同步，通常不计入帧长
      2. 目的地址、源地址：6B，用于寻址判断接收
      3. 类型：2B，指示帧中封装的是哪种高层协议分组（IP、NovellIPX、AppleTalk等）
      4. 数据：上层协议载荷
      5. 校验和：4B，CRC差错编码
    1. 标准最长以太网帧为1518B
  1. 以太网交换机
     1. 链路层设备
        1. 存储-转发以太网帧
        2. 检验到达帧的目的MAC地址，选择性向一个或多个输出链路转发
        3. 利用CSMA/CD访问链路，发送帧
     2. 透明：主机感知不到交换机的存在
     3. 即插即用
     4. 自学习：无需配置
        1. 可通过自学习获知到达主机的接口信息，自行维护交换表
        2. 目的MAC地址在表中，则将帧转发到该表中entry指向的接口，否则泛洪
     5. 主机利用独享链路直接连接交换机，交换机缓存帧，在每段链路上利用CSMA/CD收发帧
     6. 交换机的交换方式
        1. 存储转发模式：默认模式
        2. 直通模式：边收边发，接收到帧的目的地址即开始转发，不做缓存，相当于导线
        3. 无碎片模式：不做完整缓存，接收到帧的前64字节即开始转发
     7. 物理层、链路层和网络层设备比较



* 1. VLANs：虚拟局域网
     1. 较大规模的局域网中，用户改变接入点会带来安全隐私、效率和管理问题
     2. 虚拟局域网：逻辑上划分局域网络，可以在一个物理LAN架构上配置、定义多个VLAN
     3. 基于端口的VLAN：分组交换机端口划分
        1. 流量隔离：不同VLAN间流量隔离
        2. 动态成员：划分可变
        3. 在VLAN间转发：通过路由，就像在独立交换机之间（物理->逻辑）
     4. 跨越多交换机的VLAN：
        1. 多线缆连接：每个线缆连接一个VLAN
        2. 中继端口（trunk）：在跨越多个物理交换机定义的VLAN承载帧
           1. 传输802.1Q数据帧，去除/增加了额外的首部域，避免由于VLANID产生歧义
     5. 帧标记标准：
        1. 带VLAN标记的帧称为标记帧：在源地址字段和类型字段中间插入4B的VLAN标记
        2. 普通以太网帧称为无标记帧
     6. 其他划分方法：基于MAC地址的VLAN、基于协议的VLAN、基于子网的VLAN…

1. PPP协议
   1. 点对点数据链路控制：无需介质访问控制和明确的MAC寻址
   2. 常见的点对点数据链路控制协议：HDLC，PPP
   3. 设计需求
      1. 组帧：将上层数据报封装到数据链路层帧，可以同时承载任何网络层协议分组，向上层实现分用
      2. 比特透明传输：数据域支持承载任何比特模式
      3. 差错检测：无纠正
      4. 连接活性检测：检测、并向网络层通知链路状态（链路失效则停止工作）
      5. 网络层地址协商：端结点可以学习/配置彼此网络地址
      6. 无需支持差错纠正/恢复、流量控制、乱序交付、多点链路（由高层协议处理）
   4. PPP数据帧



* + 1. 标志：定界符，标识开始/结束（0x7E）
    2. 地址：无效，就是个选项
    3. 控制：无效，留着给未来开发新功能
    4. 协议：上层协议（IP，IPCP etc）
    5. 信息：上层协议分组数据
    6. 校验：CRC码
  1. 透明传输：PPP用定界符标识开始结束，可能存在歧义
     1. 异步传输时引入字节填充：
        1. 用一个转义字符0x7D，插入其中，使0x7E变成两字节（0x7D，0x7E）
        2. 原本信息字段中的0x7D用（0x7D，0x5D）表示
     2. 同步传输时用零比特填充：
        1. 信息字段中5个连续1后面插入一个0
        2. 接收时删去5个1后面的0
  2. 在交换网络层数据之前，PPP数据链路两端需要配置PPP链路，学习/配置网络层信息
  3. PPPoE：提供在以太网链路上的PPP连接
     1. 以太网无认证，而PPP点对点提供认证机制
     2. 工作过程：
        1. Discovery阶段：获取对方以太网地址
        2. Session阶段：协商与PPP数据报传输
        3. Terminate阶段：会话建立后的任意时刻，结束会话

1. 链路虚拟化（略）