

链路和数据链路的概念有何不同？

数据链路层使用的信道

- 点对点信道：一对一点对点通信，对应PPP协议
  - 广播信道：一对多的广播通信，对应CSMA/CD协议
- 数据链路层负责相邻两个节点之间可靠的数据传输。  
(虽然目前协议都不是可靠传输)

数据链路层的基本问题

**封装成帧**

在一段数据前后添加**首部**和**尾部**

帧的长度：数据部分长度 + 首部 + 尾部

首部和尾部的作用：**帧定界**

每种链路层协议规定了帧的数据部分长度上限：**最大传输单元MTU**

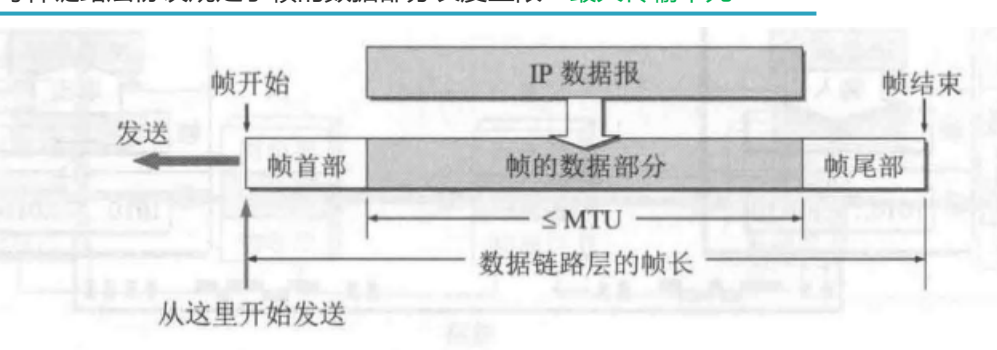


图 3-4 用帧首部和帧尾部封装成帧

举例：当数据是由ASCII码组成的文本文件时，可以使用帧定界符SOH和EOT  
SOH和EOT均为ASCII，编码分别为1H和0AH

作用：若传输中出错，发送端重新发送帧，则接收端会拿到两个帧，因为前面的帧没有EOT，所以无法。

透明：某个实际存在的东西，但是却好像不存在  
这里是指数据链路层对数据来说是透明的，即无论什么样的比特组合，都能够按照原样无差别地通过数据链路层。

问题：如果数据中出现帧首部或者尾部该如何处理？  
解决：插入转义字符，进行字节填充  
还是拿前面的SOH和EOT来举例，  
(1) 若数据中出现SOH或EOT，则在前面插入一个转义字符ESC，值为1B。  
(2) 若数据中出现整个ESC，则在前面再插入一个ESC  
这样，接收端每次看到ESC时就跳一个字节，即可保证透明传输

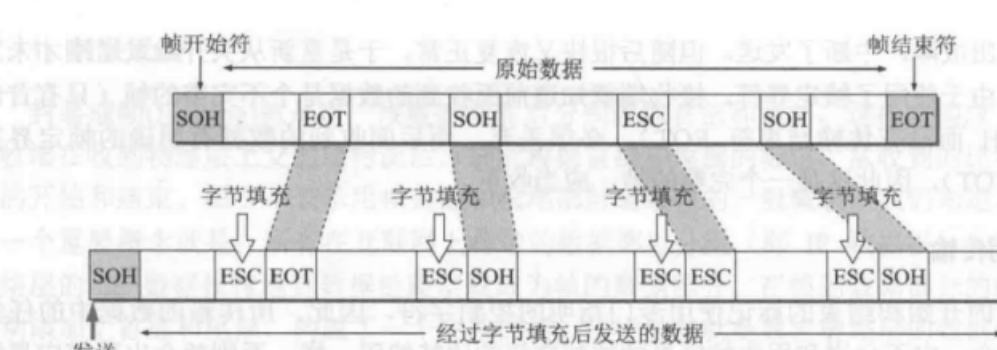


图 3-7 用字节填充法解决透明传输的问题

**差错检测**

1. 事先商定好分组：k个比特一组  
冗余码：n位  
除数：n+1位除数P  
把冗余码加在分组后面

2. 冗余码FCS的计算  
(1) 把数据M在模P位，得到k+n位数据  
(2) 拿到k+n位数据除以事先商定好的n+1位除数P；注意，是模2除法  
(3) 得到的n位余数即为FCS，加在k位数据M后面即可

3. 接收端的CRC校验：  
把收到的帧除以P，若余数为0，则说明未出错，否则说明出错，丢弃该帧。  
使用CRC校验可以保证无比特差错的传输，但并不是可靠传输！

可靠传输：数据链路层的发送端发什么，接收端就接收什么  
课本中的数据链路层协议都不是可靠传输的协议!!!

无差错接受：凡是接受的帧均没有差错

比特差错

传输差错

- 帧丢失
- 帧差错
- 帧重复
- 帧失序

过去OS的措施：在CRC检错的基础上，增加**帧编号**、**确认**和**重传**机制  
目前已经采用区域针对性的方式。

点对点信道：点对点协议PPP

顾名思义，实现点对点信道的通信  
例：用户计算机与ISP进行通信时，数据链路层使用PPP协议

PPP协议的组成部分

- 一个将IP数据报封装到串行链路的方法
- 一个用来建立、配置和测试数据链路连接的链路控制协议LCP
- 一套网络控制协议NCP

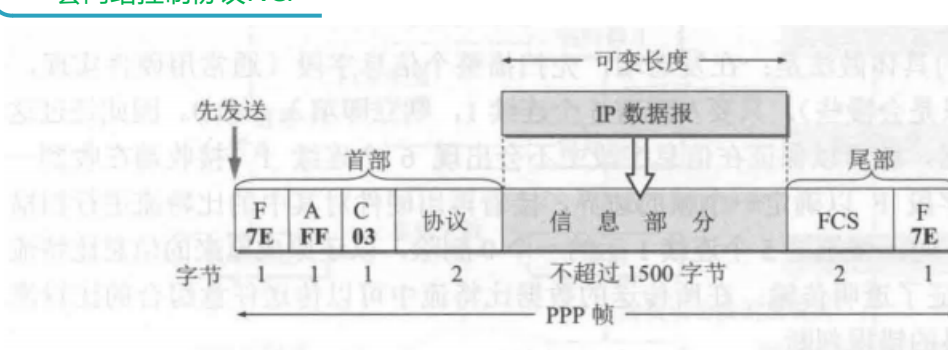


图 3-10 PPP 帧格式

标志字节F：规定为0x7E

地址字节A规定为0xFF，控制字节C规定为0x03；这两者皆无作用

协议字节：0x0021时，PPP帧的信息字段是IP数据报  
0x0021时，PPP帧的信息字段是LCP的数据  
0x8021时，PPP帧的信息字段是网络层的控制数据

信息字节：不超过1500字节

FCS：帧校验序列

**如何实现透明传输？**

字节填充（异步传输时使用）

- 转义字符为0x7D
- 1. 0x7D转换成 (0x7D, 0x5E)
- 2. 0x7D转换成 (0x7D, 0x5D)
- 3. 数值(小于0x20)的字符转义(0x7D, 0x20 + 字符)
- 如0x03转义(0x7D, 0x23)

零比特填充（同步传输时使用）

- 信息字段中，如果发现连续的五个1，则填充一个0。
- 因为0x7E中有连续的六个1，只要保证信息字段中不出现连续的六个1即可

**PPP协议的工作状态**

过程概述：

1. 用户拨号接入ISP，建立物理连接  
调制解调器发送载波信号，从链路静止进入链路建立状态
2. 用户电脑向ISP发送一系列的LCP分组（封装成多个PPP帧）  
发送LCP配置请求帧，链路另一端发送以下一种帧：  
(1) 配置确认帧(Configuration-Ack) 所有选项都被接受。  
(2) 配置否认帧(Configuration-Nak) 所有选项都理解但不能接受，它列出了不能接受的选项。  
(3) 配置拒绝帧(Configuration-Reject) 选项有的无法识别或不能接受，需要协商。  
确认后进入鉴别状态
3. 鉴别状态只允许发送LCP协议的分组、鉴别协议的分组、监测链路质量的分组  
可使用  
口令鉴别协议PAP（可多次尝试）  
口令握手鉴别协议CHAP（更安全）  
若鉴别失败，转入终止状态；否则转入网络层协议状态
4. 网络层协议状态：链路两端的网络控制协议NCP  
根据网络层的不同协议交换网络控制分组  
NCP给用户分配一个IP地址，进入链路打开状态

注意：

1. 用户通信完毕时，NCP释放网络层连接，收回IP地址；LCP释放数据链路层连接；最后释放物理层的连接。
2. PPP链路的起始机终止状态始终是链路静止状态
3. PPP协议不是纯粹的链路层协议，还包含物理层和网络层的内容

各种器件解析

**(网络) 适配器 (adapter)**

即网络接口卡，也叫网卡，上面装有处理器和存储器，且MAC地址固化在ROM中

工作层次：物理层和数据链路层

作用：

1. 进行数据串行传输和并行传输的转换。
2. 提供数据缓冲。
3. 从系统总线上把数据打包后发送到局域网。
4. 从局域网接受数据包解包后存放到存储器。

4. 实现以太网协议（如数据的封装、发送、地址的检查）。

MAC地址是计算机的硬件地址，存储在适配器的ROM中；而IP地址是计算机的软件地址，存储在计算机的存储器中

**转发器/中继器 (repeater)**

工作层次：物理层

作用：放大信号

**集线器 (hub)**

工作层次：物理层

作用：简单地转发信号（可以看作是多端口的转发器）

1. 使用集线器的以太网是星形拓扑，但在逻辑上仍然是总线型，尽管外表看上去是星形的。
2. 使用集线器的以太网仍然是同一广播域。

**网桥 (bridge)**

工作层次：数据链路层

作用：对收到的帧根据其MAC帧的目的地址进行转发和过滤，从而使各网段成为独立的广播域。

**以太网交换机 (switch/switching hub)**

工作层次：数据链路层

作用：多端口的网桥

特点：

1. 以太网交换机每个端口都与一个单独的主机或者另一个以太网交换机相连，每个端口和连接端口的主机都是独立的广播域。
2. 工作在全双工方式（不使用CSMA/CD协议！！），有并行性（网桥每次只能分析转发一个帧，交换机是多个）
3. 端口有存储器，可暂存帧。
4. 端口即用设备，帧交换表可通过自学习算法建立（P102）

数据链路层

**局域网分类 (按网络拓扑)**

- 星形网
- 环形网
- 总线网

**以太网：目前应用最广泛（垄断）的局域网技术**

两个标准  
DIX Ethernet V2  
IEEE 802.3

**局域网分层**

IEEE 802委员会曾经把局域网的数据链路层拆分成LLC和MAC两个子层  
但后来以太网发展到了垄断地位，以太网只有MAC协议，因此LLC层消失

局域网跨越了物理层和数据链路层

**简介**

第一代以太网使用总线网

标准以太网：10Base-5  
10Mbps 基带信号 500m

注意：以太网发送的数据都使用曼彻斯特编码的信号（每个比特对应两个码元！）

1. 采用较为灵活的光连接的工作方式  
尽量大努力的交付，而不是可靠交付！

2. 同一时间只能允许一台计算机发送数据！  
采用的协议：CSMA/CD协议

**以太网通信流程**

总结：先听后发；边听边发；碰撞停止；退避重发

多点接入，使用总线型网络

载波监听：注意以太网根本没有载波，因为都是数字信号。  
边发送边监听(载波监听和碰撞检测才是协议的实质！)

概念与常数

1. 电磁波在1km电缆的传播时延大概为5μs (2\*10<sup>8</sup>m/s)。
2. 使用CSMA/CD协议以太网只能进行半双工通信。
3. 单程端到端传播时延：t<sub>p</sub>，是最远的两端传播！
4. 争用期/碰撞窗口：2t<sub>p</sub>，标准以太网中为512比特时间 (51.2μs) 由10Mbps/5可以算出

1. 碰撞检测的过程：可以看到若发生碰撞，最多经过2t<sub>p</sub>，发送端即可检测到。  
检测到碰撞（A在发数据，同时又收到B的数据）后发送方立即停止发送！

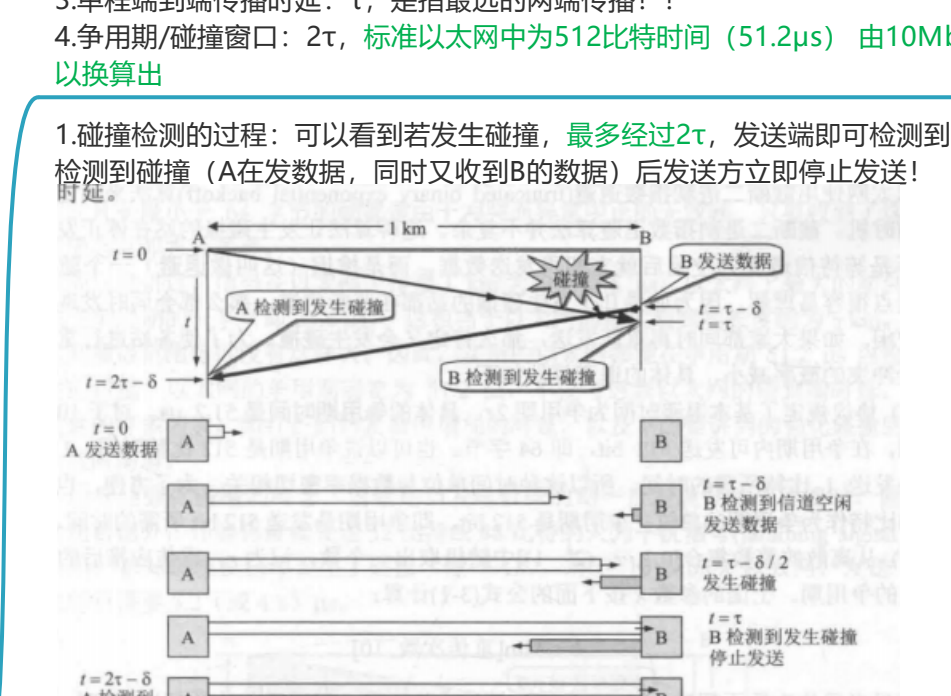


图 3-17 传播时延对载波监听的影响

2. 检测到碰撞，使用截断二进制指数退避算法

设k=min(重传次数, 10)，争用期2t<sub>p</sub>为512比特时间。  
每次重发从{0, 1, ..., (2<sup>k</sup>-1)-1}中取出一个数字乘以2t<sub>p</sub>

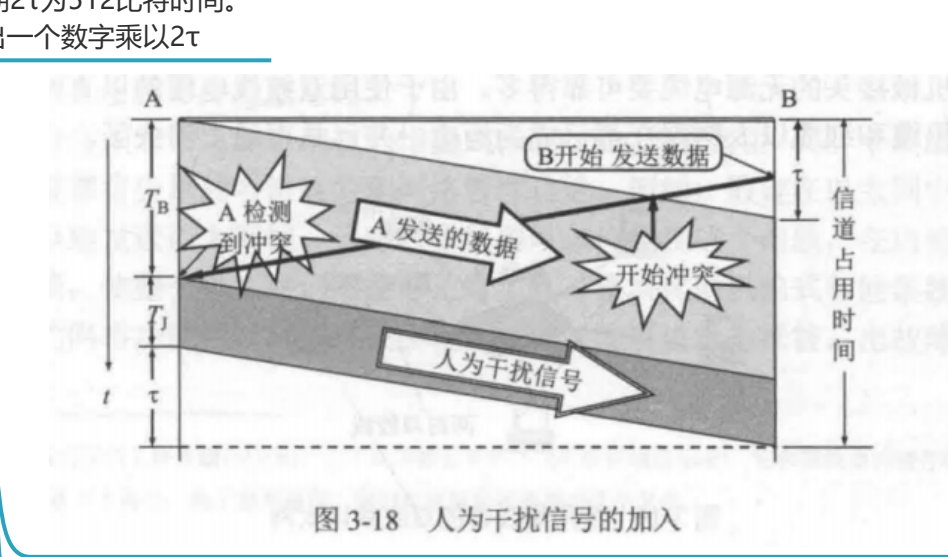


图 3-18 人为干扰信号的加入

总线被占用时间：T<sub>B</sub> + T<sub>J</sub> + t<sub>p</sub>

注意：发送完干扰信号之后才能执行退避算法！！  
执行退避算法就不需要再进行帧间隔了！！！！

3. 强化碰撞：发送数据的站一旦发现出现了碰撞，还要发送一个32/48比特的为人干扰信号，通知其他用户发生了碰撞。

4. 帧间最小间隔：96比特时间，9.6μs。帧与帧之间的发送间隔为96比特时间

**以太网的信号利用率**

定义参数a=τ/T<sub>0</sub>  
τ是帧到帧时延，T<sub>0</sub>是发送帧需要的时间（帧长除以发送速率 10Mbps/s）  
a越小，一旦发生碰撞就马上被检测出来，而立即停止发送，空信道资源浪费越少，信道利用率越大

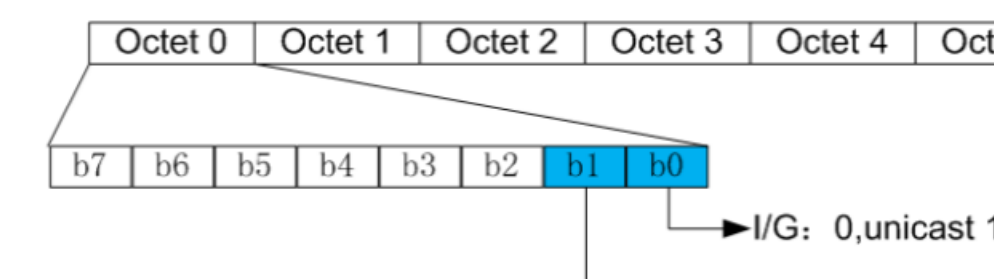
极限信道利用率：不发生故障，信道始终空闲  
S<sub>max</sub>=T<sub>0</sub>/(T<sub>0</sub>+τ)=1/(1+a)，看出a需要远远小于1

又称为物理地址或硬件地址  
实质上是一个“名字”

广播信道：以局域网为例

**以太网**

**MAC地址**



前三个字节为组织统一标识符OUI（向RA购买）；后三个字节为扩展标识符Extended Identifier

U/L: 0, unicast 1, multicast

U/L: 0, Universal Address 1, locally administered

**以太网的MAC层**

根据MAC帧中的目的地址，转发和过滤帧

适配器的特殊工作方式：混杂方式 只要听到帧就接收，而不管这些帧的目的地址

帧分类：其中广播地址和组播地址只用于目的地址；广播地址是48位全1！

- (1) 单播(unicast)帧（一对一），即收到的帧的 MAC 地址与本站的硬件地址相同。
- (2) 广播(broadcast)帧（一对全体），即发送给本局域网内所有站点的帧（全1 地址）。
- (3) 多播(multicast)帧（一对多），即发送给本局域网上一部分站点的帧。

**MAC帧的格式**

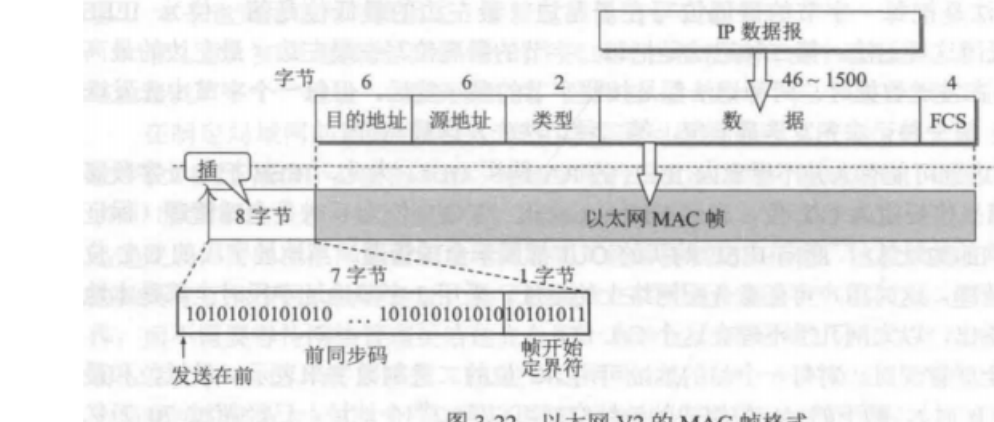


图 3-22 以太网 V2 的 MAC 帧格式

第一个字段：目的地址；  
第二个字段：源地址；（注意顺序！）  
第三个字段：类型、标志IP层使用的是什么协议  
第四字段：数据长度46~1500字节（46是最短帧长-18所得）  
第五个字段：FCS字段，用来进行CRC校验（只校验前述的五个字段！）

拿到物理层时，还要额外加8个字节，7字节的前同步码和1个字节的帧开始定界符

几个注意事项：

1. 帧填充，当数据不足46字节时进行帧填充，接收方会由IP协议首部的前总长度字段检测是否进行了填充，从而丢弃填充。
2. 为什么不用帧结束定界符？也不用保证透明传输吗？  
因为存在帧间最小间隔，接收方只要从检测到帧开始定界符起接收，到帧间隔为止（可以监测到发送方电压不变化），即可保证传输的正确性

**以太网的扩展**

物理层扩展：使用集线器

数据链路层扩展：使用以太网交换机

以太网的扩展

- 以太网交换机不通用CSMA/CD协议！工作在全双工方式！
- 以太网交换机的自学习功能
  - 初次广播
  - 记录后单播
  - 注意：
    1. 及时及时更改交换表中的项目
    2. 生成树协议STP在逻辑上切断某些链路，消除环路现象。
- 对比
  - 总线型以太网：CSMA/CD协议 半双工工作方式
  - 使用以太网交换机：不使用CSMA/CD协议 全双工工作方式
- 广播风暴
  - 以太网包含太多计算机的缺点
  - 对信息安全不利
- 虚拟局域网VLAN
  - 虚拟局域网VLAN定义
  - 虚拟局域网VLAN
  - 虚拟局域网的802.1Q帧
    - 802.1Q帧
    - 2字节标记的0x8100
    - 4字节
    - 12字节的VID
    - 以太网最大帧长为1518+4=1522字节
  - 发送的三种情况