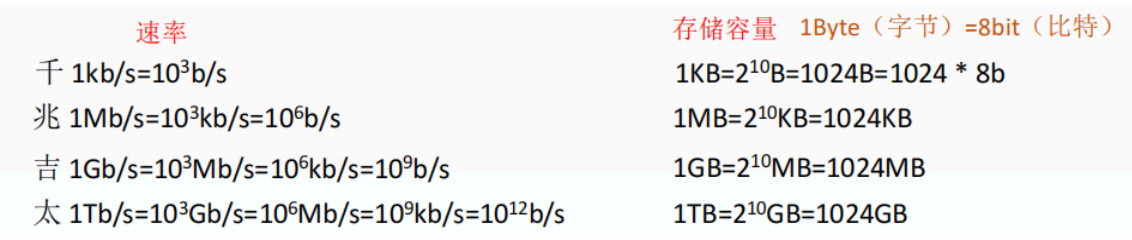
速率与容量的区别：



性能指标：速率 带宽 吞吐量（单位时间通过的数据量） 时延（从一端到另一端需要的时间，也叫延迟）

**时延带宽积：传播时延 X 带宽**

时延带宽积又称为以比特为单位的链路长度。即“某段链路现在有多少比特”。

**往返时延RTT：**从发送方发送数据开始，到发送方收到接收方的确认（接收方收到数据后立即发送确认），总共经历的时延

信道利用率：有数据通过时间/（有+无）数据通过时间

分层：强调对等实体的概念

实体:第n层中的活动元素称为n层实体。**同一层的实体叫对等实体**

协议:为进行网络中的**对等实体数据交换**而建立的规则、标准或约定称为网络协议

OSI参考模型：（从上到下）

**应用层**：所用能和用户交互产生网络流量的程序

**典型的应用层服务**： 文件传输FTP 电子邮件SMTP 万维网HTTP

**表示层**：用于处理在两个通信系统中交换信息的表示方式（语法和语义） **翻译官**

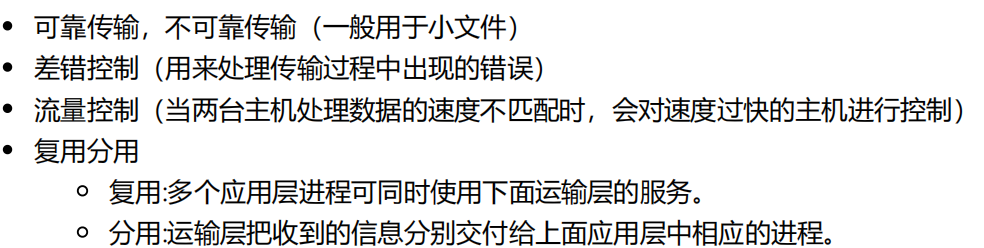
数据格式变换、数据加密解密、数据压缩恢复

**会话层**：向表示层实体/用户进程提供建立连接并在连接上有序地传输数据。这是会话，也是建立同步(SYN)

建立管理会话 **主要是同步和断点续传**

**传输层**：负责主机中两个进程的通信，即**端到端的通信**。传输单位是报文段或用户数据报

注意**复用分用功能**



**网络层**：把分组从源端传到目的端，为分组交换网上的不同主机提供通信服务

传输单位是数据报。把数据报进行切割后，就是分组

路由选择，流量控制，差错控制，拥塞控制

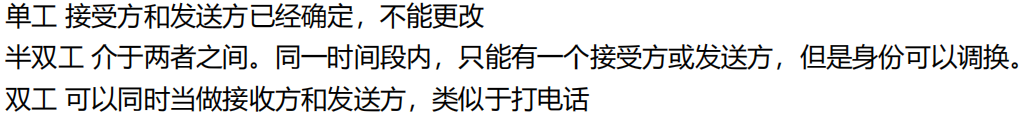
**链路层**：把网络层传下来的数据报组装成帧

成帧、差错控制、流量控制、访问控制（对信道） 传输单位是帧

**物理层**：在物理媒体上实现比特流的透明传输

透明传输:指不管所传数据是什么样的比特组合,都应当能够在链路上传送 单位是bit

接口特性，传输模式（单工，半双工，双工） 比特同步 比特编码



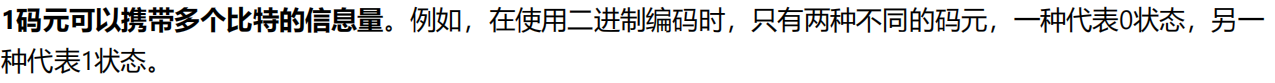
物理层：

接口特性（机械 电气 功能 规程）

串行传输：将表示一个字符的8位二进制数按由低位到高位的顺序依次发送——速度慢，费用低，适合远距离

并行传输：将表示一个字符的8位二进制数同时通过8条信道发送——速度快，费用高，适合近距离

**码元：**指用一个固定时长的信号波形（数字脉冲)，代表不同离散数值的基本波形



四进制码元：4种高低不同的信号波形 00、01、10、11

码元传播速率：波特为单位（Baud） 1波特表示数字通信系统每秒传输一个码元



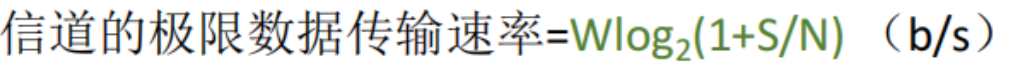
**奈氏准则:**在**理想低通**（无噪声，带宽受限)条件下，**为了避免码间串扰**，极限码元传输速率为**2W Baud**，W是信道带宽，**单位是Hz （只有在这俩公式下带宽才用hz）**

码间串扰:接收端收到的信号波形失去了码元之间清晰界限的现象

（如果信号在传输过程中“变质”了（比如通过带宽有限的信道、有噪声或多径反射），一个码元的波形会“拖尾巴”或“提前开始”，入侵到相邻码元的时间段。结果，接收端看到的信号波形就像模糊的涂鸦，码元之间没有了清晰的界限。）

**香农定理：**噪声 （但是噪声的影响是相对的，若信号较强，那么噪声影响相对较小——所以有了**信噪比 信噪比=信号的平均功率/噪声的平均功率**，常记为S/N，并用分贝(dB）作为度量单位）





香农定理关注的是信息传输速率；奈氏准则是波特率！ 求速率——两者结合

基带信号 数字信道 基带传输

宽带信号 模拟信号 宽带传输 编码和调制

编码：

数字数据编码为数字信号：非归零编码（1就是1 0就是0）

曼彻斯特：将一个码元分成两个相等的间隔，前一个间隔为低电平后一个间隔为高电平表示码元1（当然反过来也行）

差分曼彻斯特：中间有反转 且若码元为1，则前半个码元的电平与上一个码元的后半个码元的电平相同，若为0，则相反

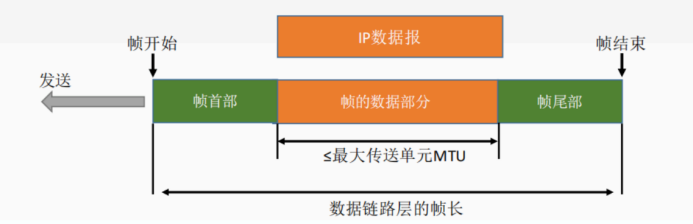
数字数据调制为模拟信号：

数字数据调制技术在发送端将数字信号转换为模拟信号，而在接收端将模拟信号还原为数字信号，分别对应于调制解调器的调制和解调过程。

中继器的功能:对信号进行再生和还原

集线器的功能:对信号进行再生放大转发（所以又称多口中继器）

数据链路层：



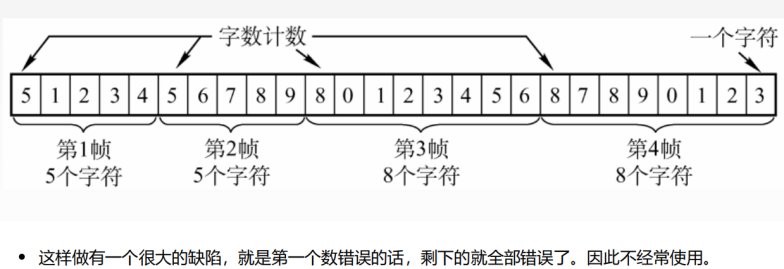
（非常直观的示意图）

透明传输是指不管所传数据是什么样的比特组合，都应当能够在链路上传送。因此，链路层就“看不见”有什么妨碍数据传输的东西。

**当所传数据中的比特组合恰巧与某一个控制信息完全一样时，就必须采取适当的措施，使收方不会将这样的数据误认为是某种控制信息**。这样才能保证数据链路层的传输是透明的。

组帧的四种方法: 1.字符计数法，2.字符(节）填充法，3.零比特填充法，4.违规编码法。

字符计数：

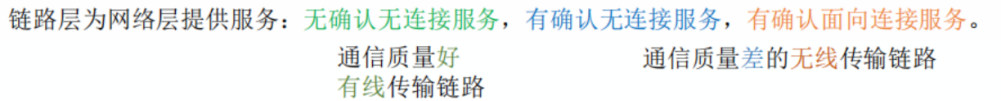


字符填充：插入转义字符（保证前面的透明传输）

零比特填充：在发送端，扫描整个信息字段，只要连续5个1，就立即填入1个0。（因为控制信息是01111110）

**保证了透明传输:在传送的比特流中可以传送任意比特组合，而不会引起对帧边界的判断错误**

差错控制（检错编码）：



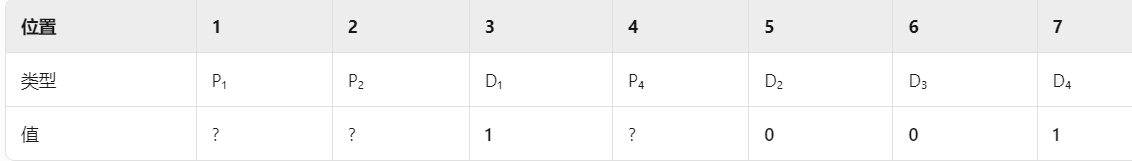
冗余编码 奇偶校验码 CRC循环



接收端如何检错 把收到的每一个帧都除以同样的除数，然后检查得到的余数R（余数为0代表正确）

差错控制（纠错编码——海明码） 纠正单比特错误

举个例子：4 位 D = 1001 P为检验位 D为数据位



第k为检验位覆盖位置（二进制第 k 位=1），比如P2： 2 3 6 7的倒数第二位为1，应该有：

P₂ ⊕ 1 ⊕ 0 ⊕ 1 = 0 由此计算P2

海明码——》单比特纠错方案

怎么纠错？伴随式： 把上面的每个检验位P和真实计算的检验位异或后，重组，若错误位置 ！=0，将**该位置的比特翻转**即可纠正错误。

流量控制（停等协议和滑窗协议，滑窗又分为后退N帧和选择重传）：



停等：发一个数据，就要等接收方回一个ack，又有ack丢失，ack迟到，超时等情况

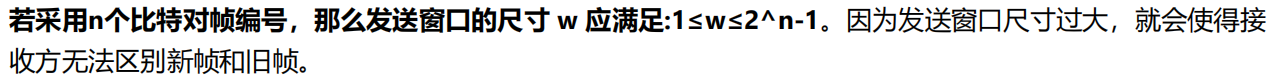
GBN：



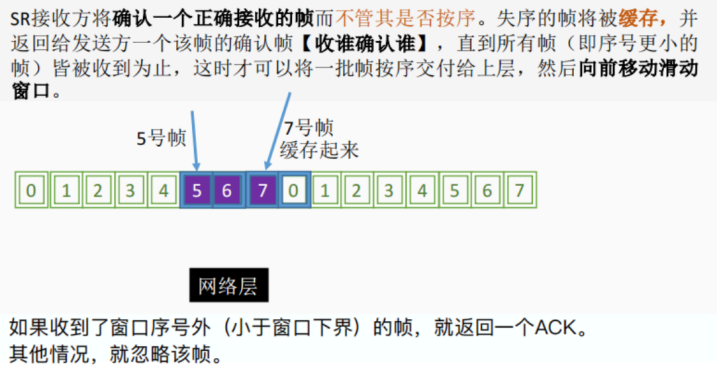
累积确认！对n号帧的确认采用累积确认的方式，标明接收方已经收到n号帧和它之前

的全部帧

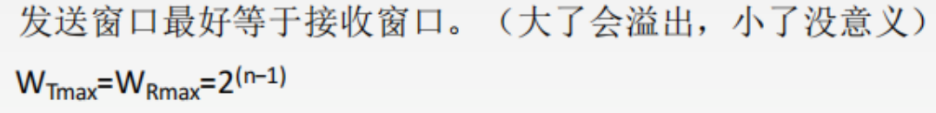
如果出现超时，发送方重传所有已发送但未被确认的帧。（即回退n帧，名字来源）



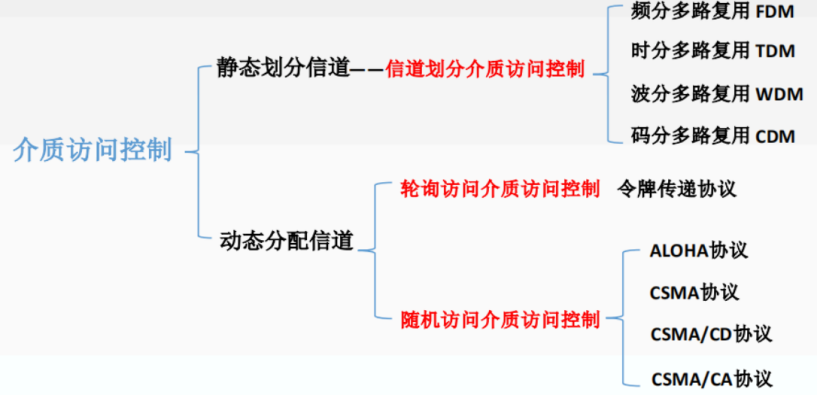
SR：加大接收窗口，设置接收缓存，缓存乱序到达的帧



来者不拒，收谁确认谁 超时：一次重传一个帧



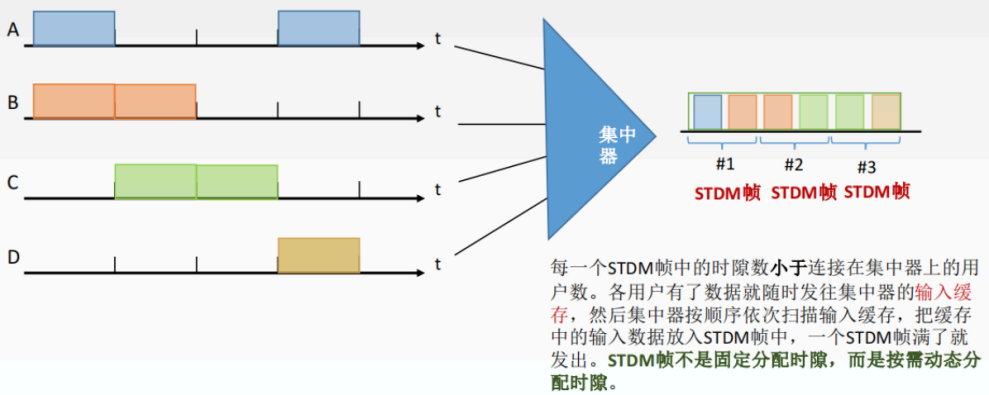
介质访问控制：经典大图梳理！



时分复用：将时间划分为一段段等长的时分复用帧（TDM帧)。每一个时分复用的用户在每一个TDM帧中占用固定序号的时隙，所有用户轮流占用信道

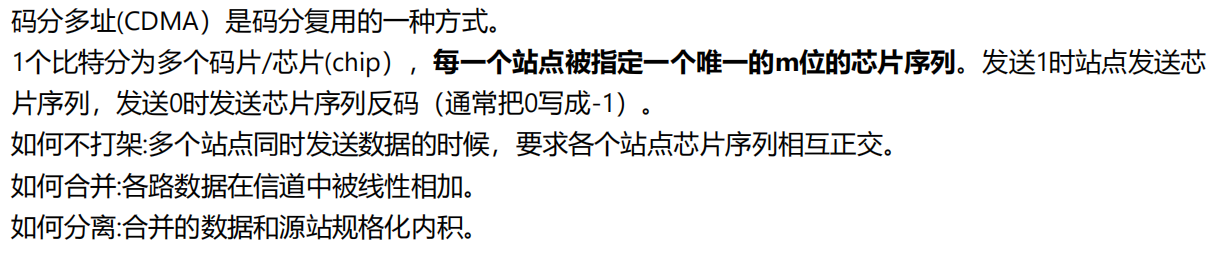
改进时分复用——统计时分复用STDM

ABCD中任何一个想传输数据时，直接发送即可。不用等到自己的时间段，信道利用率大大提高（相当于多加个缓存）



波分复用WDM：合波器 分波器

码分复用CDMA：

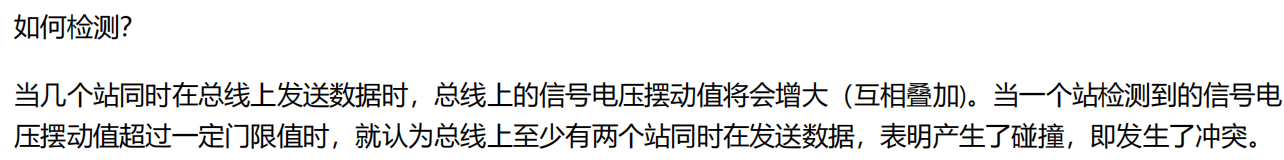


随机访问介质访问控制：即随时随地想用的时候分配（**ALOHA CSMA CSMA/CD CSMA/CA**）

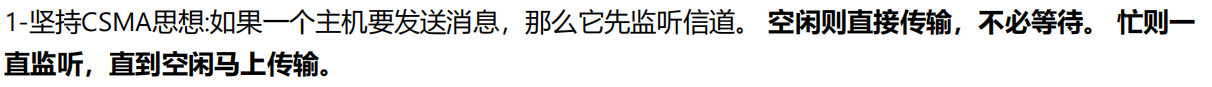
纯ALOHA：想发就发 冲突：超时后随机一段时间重传

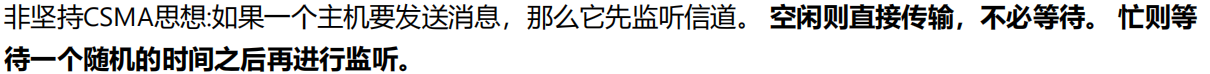
时隙ALOHA：控制想法就发的随意性 必须等到下一个时间片开始时刻再发送

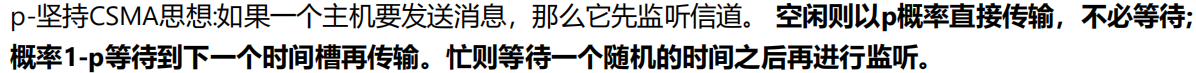
CSMA协议：CS:载波侦听/监听，每一个站在发送数据之前要检测一下总线上是否有其他计算机在发送数据（**核心：发送帧之前，监听信道**）



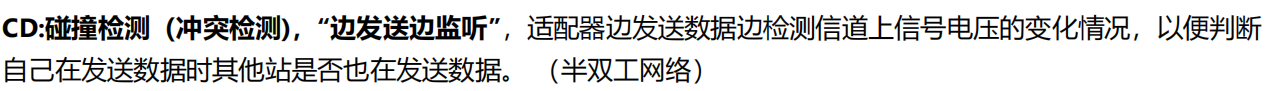
又分为：







CSMA/CD：

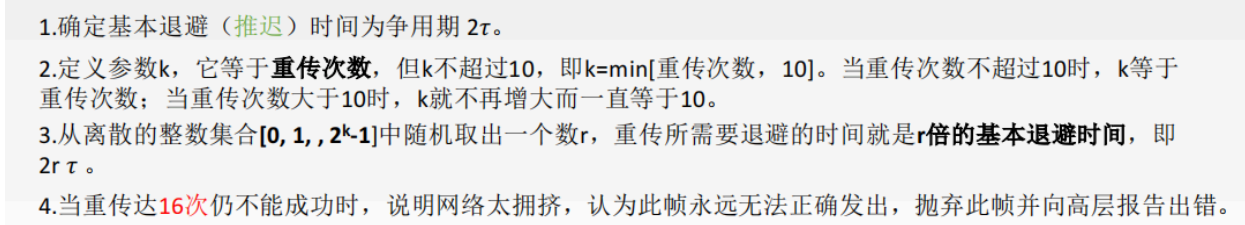


核心：边发送边监听！ 在发送数据之前以及发送数据时都要检测一下总线

问：监听之后为啥还会发生冲突呢？

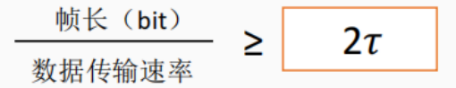
答：因为电磁波在总线上总是以有限的速率传播的。

总线的端到端往返传播时延只要经过2z时间还没有检测到碰撞，就能肯定这次发送不会发生碰撞

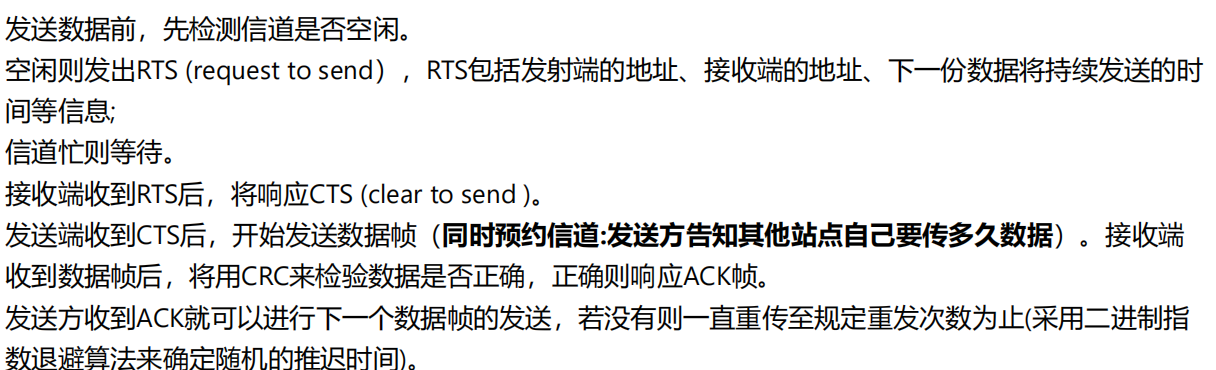


与前面不同，需要最小帧长！！！！

如果帧的长度太小，可能在站点停止传送之前，就已经传送完了。因此需要确定一个最小帧长

以太网的最小帧长：64B （即512b）

CSMA/CA协议：主要用于无线局域网 CSMA/CD用于有线局域网

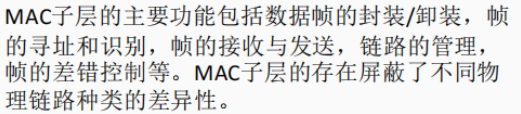


采用能量检测

轮训访问介质控制访问：轮询协议和令牌传递协议

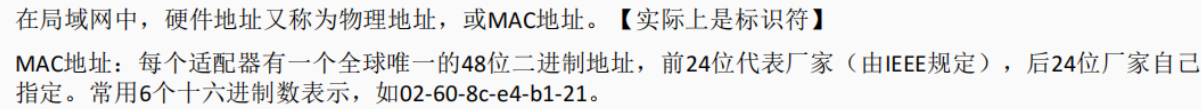
想起来前面的五层协议（GPT版本）：应用层 传输层 网络层 数据链路层 物理层

MAC和LLC（二者组成数据链路层）：



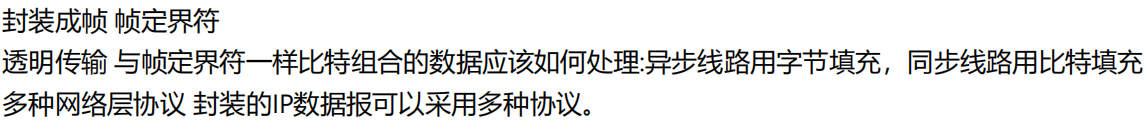
以太网：用的是CSMA/CD IEEE802.3 无连接不可靠 只实现无差错接收，不实现可靠传输

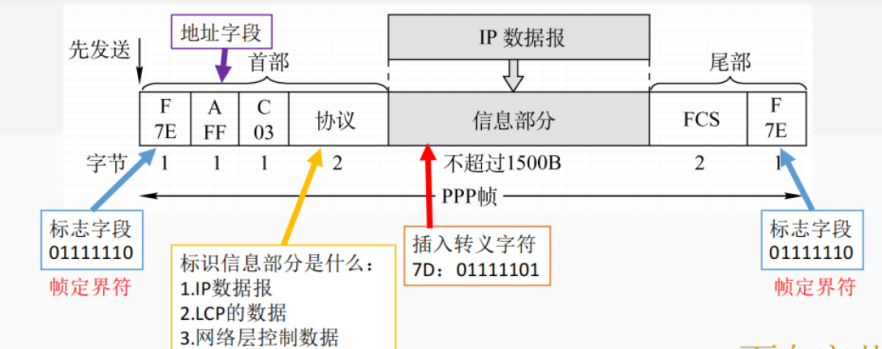
MAC地址：48位，6个16进制数



PPP协议：

点对点协议，是目前使用最广泛的数据链路层协议 **只支持全双工链路 面向字节**

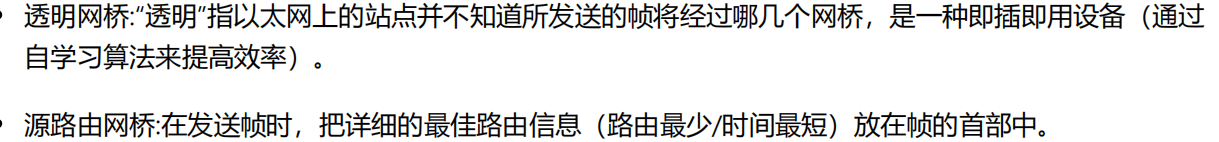




HDLC协议：高级数据链路控制 也是全双工 面向比特，透明传输使用0比特插入法，所有帧采用CRC校验

链路层设备：

网桥根据MAC帧的目的地址对帧进行转发和过滤。当网桥收到一个帧时，并不向所有接口转发此帧，而是先检查此帧的目的MAC地址，然后再确定将该帧转发到哪一个接口，或者是把它丢弃（即过滤）  **透明网桥与源路由网桥**



交换机：以太网交换机就是多端口的网桥 直通式 存储转发式

经典考点！！！！

 只有路由器才能隔离广播域！！！

网络层：

电路交换 报文交换 分组交换 数据报方式 虚电路方式

数据报无连接，基于路由协议和算法构建转发表，每个分组独立选路

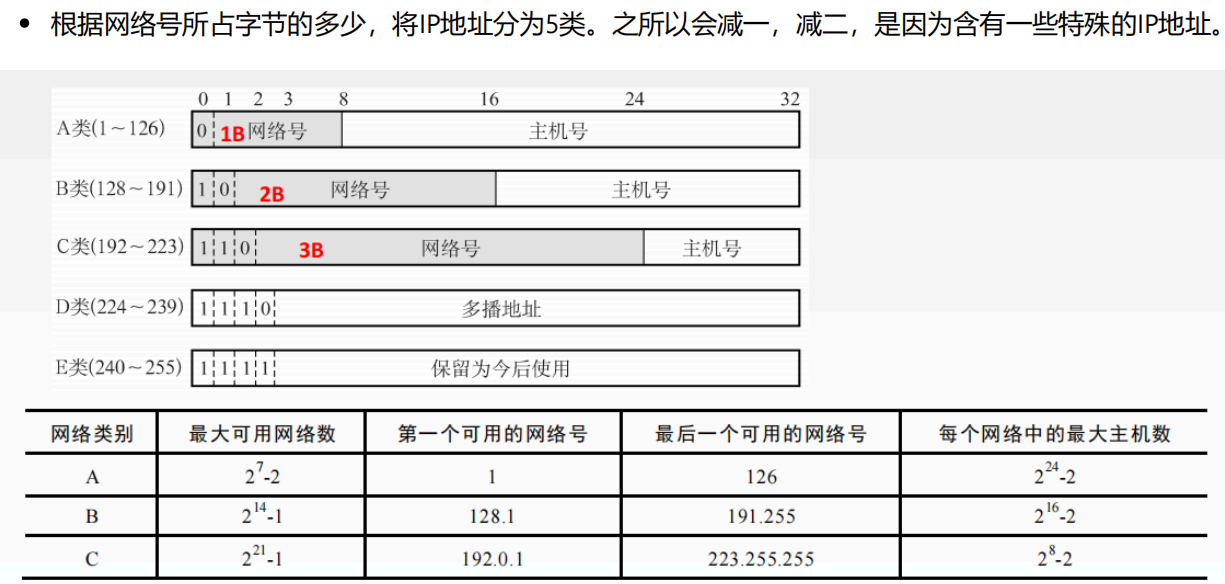


IP数据报：



片偏移以8B为单位

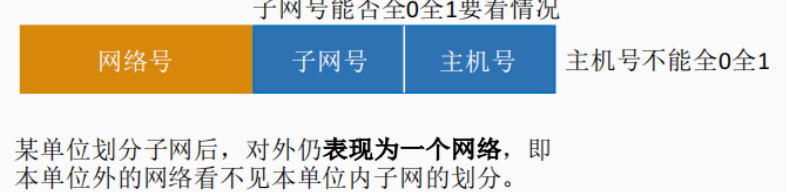
IP地址： **每一类8位为间隔**



网络地址转换NAT：

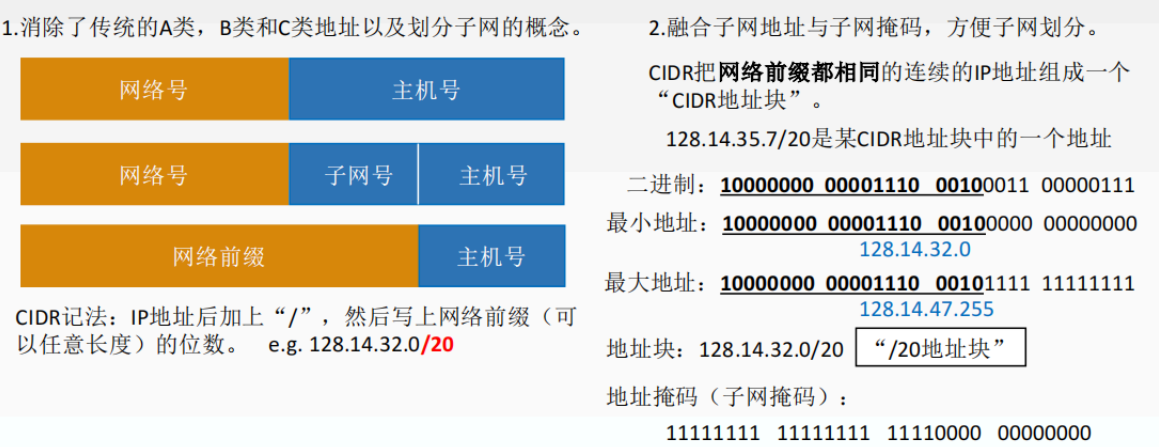
里边含有一张NAT转换表，包含局域网里边的主机和因特网里边的一个IP地址。局域网里边的主机请求数据时会进行IP地址转换

子网划分：两级IP地址变为三级IP地址



子网掩码与IP地址逐位相与，就得到子网网络地址

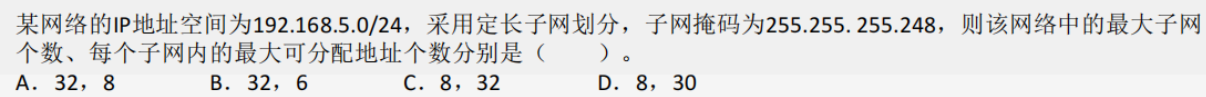
五分类变址CIDR：经典左图一眼看出区别！



超网：多个子网聚合成一个较大的子网，也称路由聚合 即将网络前缀缩短

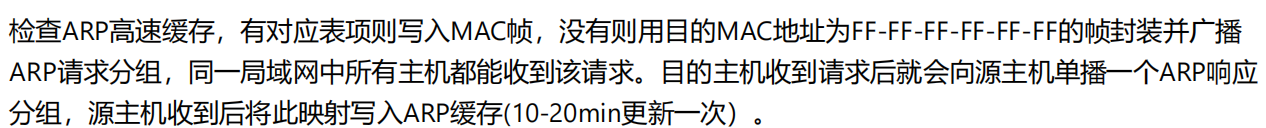
网络号+子网号=网络前缀 所以网络号可通过网络前缀-子网号来得到

**好题！**



前24位为网络前缀，后8位又进行了子网划分。通过子网掩码来确定子网掩码的位数。248转换为二进制为11111000。 子网位数为5，最大子网个数为 2^5 =32, 分配地址个数 为 2^3 -2=6。 (减2 是因为不能全为0或全为1)。

ARP协议 : 完成主机或路由器IP地址到MAC地址的映射



DHCP协议：

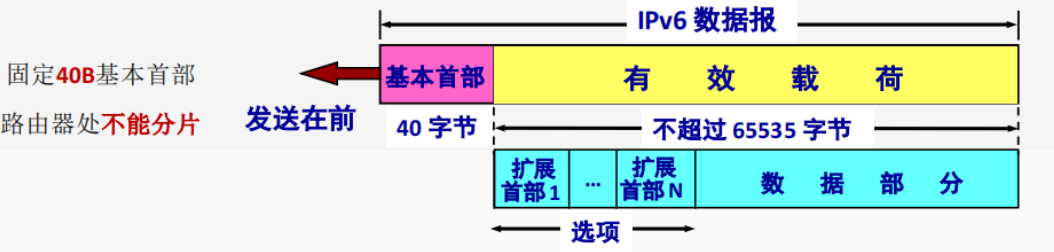
**是应用层协议**，使用客户/服务器方式，客户端和服务端通过广播方式进行交互，**基于UDP**。DHCP提供即插即用联网的机制，主机可以从服务器**动态**获取IP地址、子网掩码、默认网关、DNS服务器名称与IP地址,允许地址重用，支持移动用户加入网络，支持在用地址续租

ICMP协议： 经典应用是ping

和传输层紧密相连，作用就是为了更有效地转发IP数据报和提高交付成功的机会



IPv6：

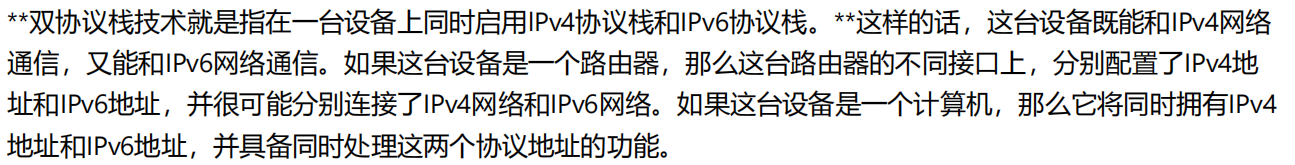


地址从32位（4B）扩大到==128位（16B） 同时移除了校验和字段 支持即插即用不需要DHCP 删掉了服务类型字段 将可选字段移出首部变为了扩展首部，基本首部40B固定



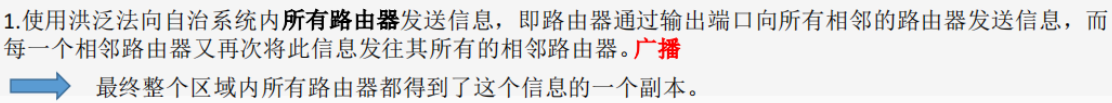
IPV4向V6过滤：

双栈协议和隧道技术



路由算法：  
OSPF：所有路由器掌握完整的网络拓扑和链路费用信息

使用分布式的链路状态协议 使用dijkstra



最终，所有路由器都能建立一个链路状态数据库，即全网拓扑图

不存在坏消息传的慢的问题，对**规模大的网络效果好**，直接使用**IP数据报传送**

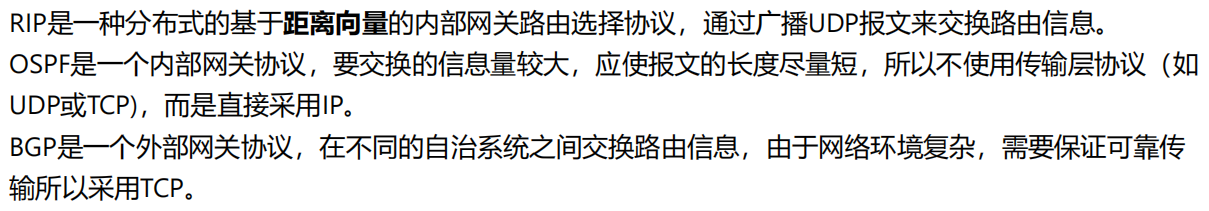
RIP ：路由器**只掌握物理相连**的邻居及链路费用

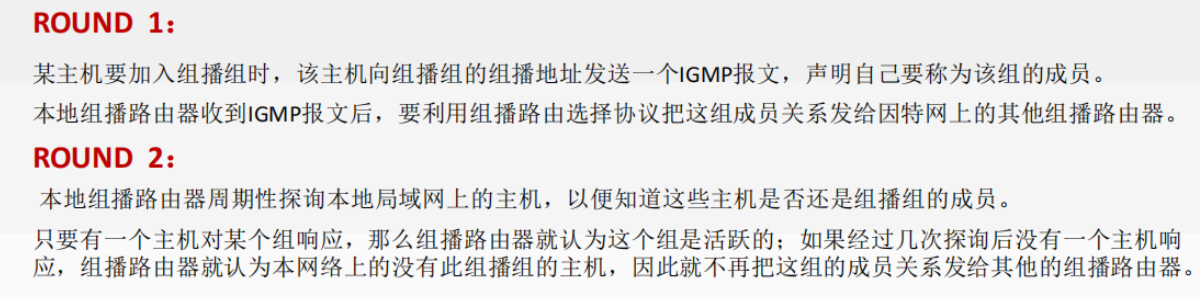
基于距离向量 跳数16表示不可达 慢收敛的特点 仅和相邻路由器交换信息！（交换自己的路由表）

RIP和OSPF又称内部网关协议 BGP是外部网关协议

BGP：每个AS中会选一个路由作为BGP发言人

当BGP发言人互相交换了网络可达性的信息后，各BGP发言人就根据所采用的策略从收到的路由信息中找出到达各AS的较好路由

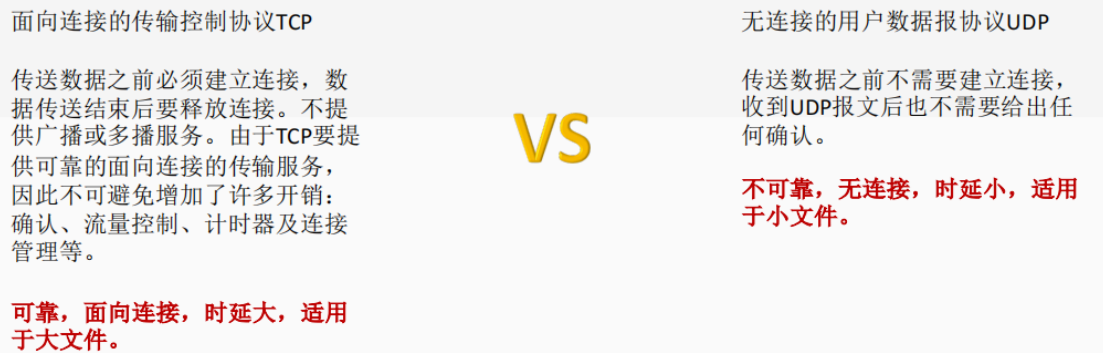


IGMP协议：——**和组播**相关！  


转发表：转发表必须包含完成转发功能所必需的信息，在转发表的每一行必须包含从要到达的目的网络到输出端口和某些MAC地址信息的映射

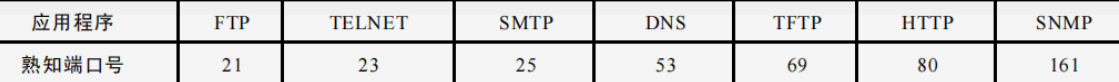
传输层：

主要是TCP和UDP，前者靠谱后者不靠谱



复用:应用层所有的应用进程都可以通过传输层再传输到网络层。

分用:传输层从网络层收到数据后交付指明的应用进程。

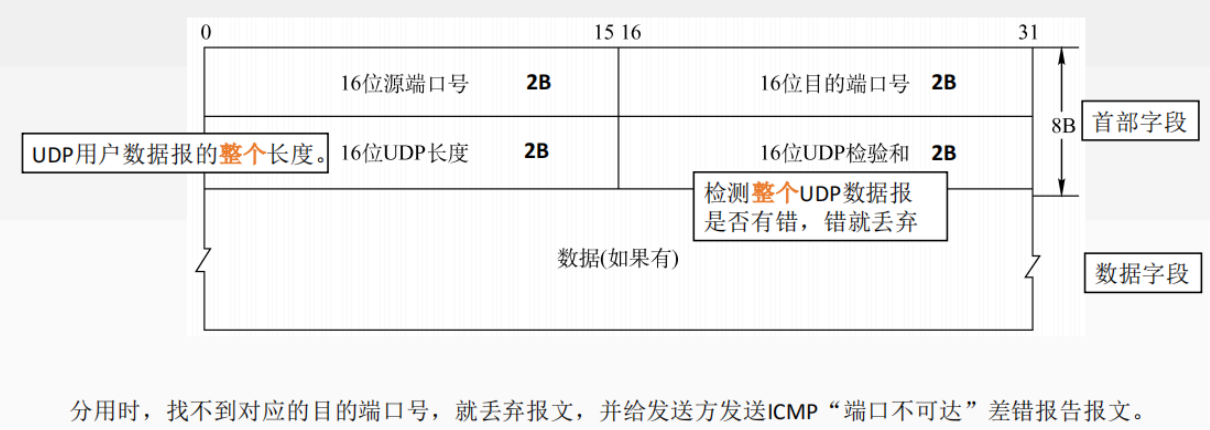


套接字**唯一标识了网络中的一个主机和它上面的一个进程**

Socket=（主机ip地址，端口号）

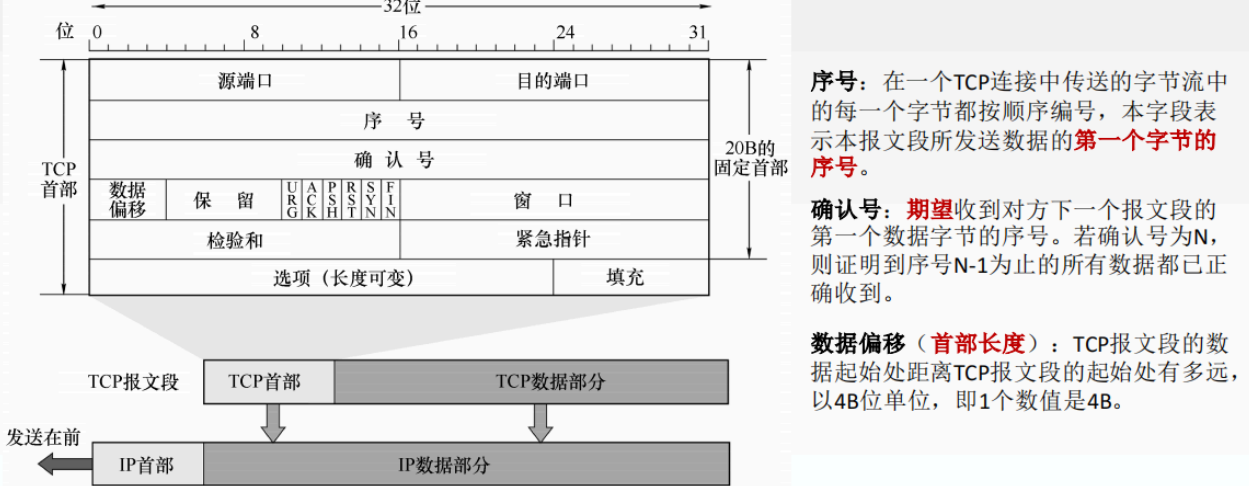
UDP协议：

无连接 不可靠 面向报文（适合一次性传输少量数据的网络应用） 无拥塞控制（适合实时应用）



TCP协议：

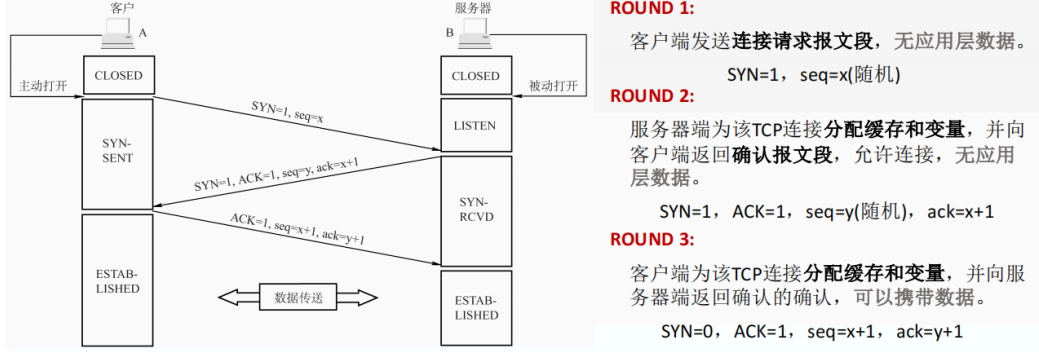
面向连接（点对点 虚连接！） **TCP提供服务：可靠有序，不丢不重 全双工通信 面向字节流**



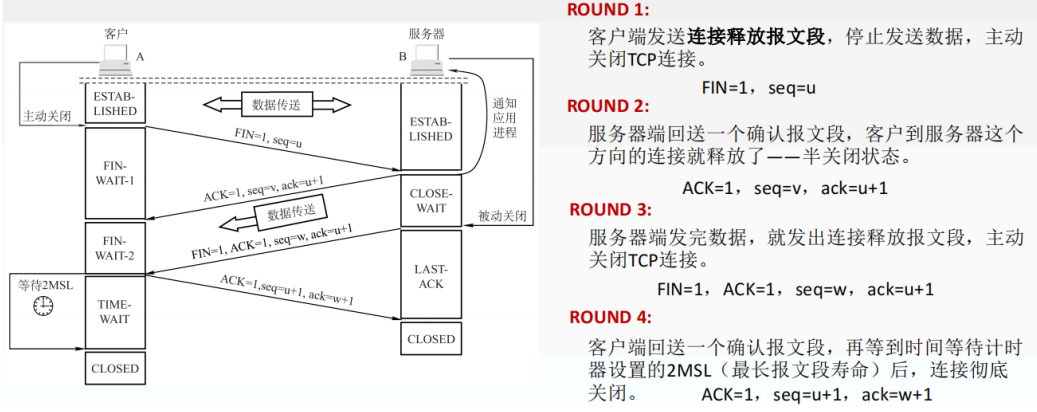
注意序号是第一个字节 偏移以4B为单位 端口长度和UDP一样都是16位

TCP的连接方式：客户/服务器

连接建立：

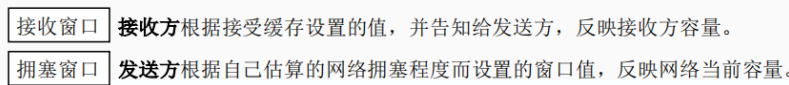


连接释放：**四次握手** 拆成两队来看



TCP协议实现可靠传输的机制：校验 序号 确认 重传

TCP流量控制：滑窗机制 拥塞控制是全局性的，流量控制是点对点的



拥塞控制算法：

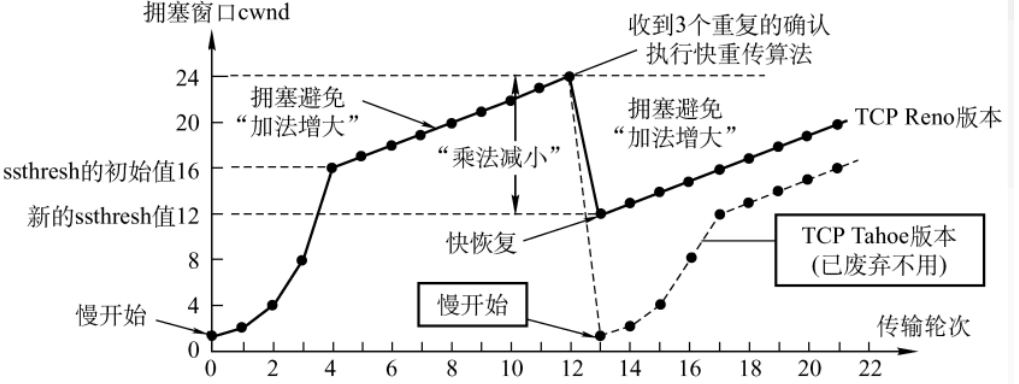
慢开始和拥塞避免：

刚开始进行指数增长，到达 ssthresh 之后，进行加法增长。

遇到网络拥塞之后，降到初始值，重复之前的步骤。新的 ssthresh 设为 拥塞时窗口大小的一半。

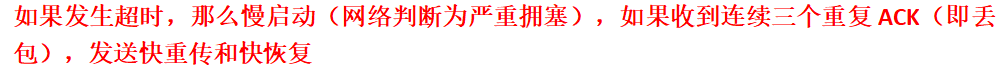


快重传和快恢复：

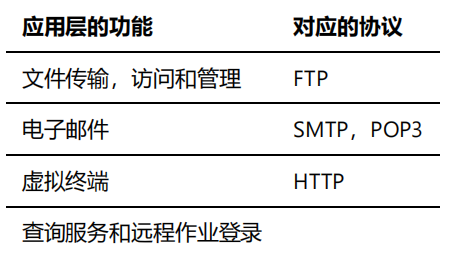


前面的步骤和之前一样。不同的是降低拥塞窗口的时机和大小不同

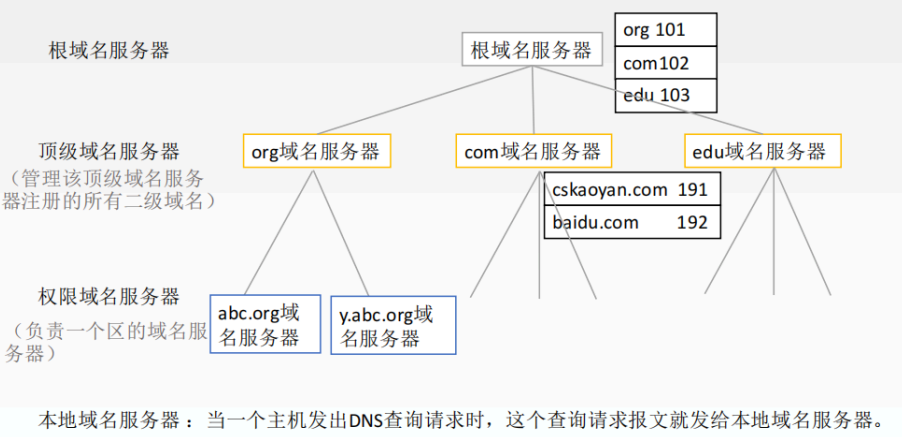
当收到3个重复的确认时，执行快重传算法，拥塞窗口降到原来的一半



应用层：



DNS系统：将域名解析成IP地址



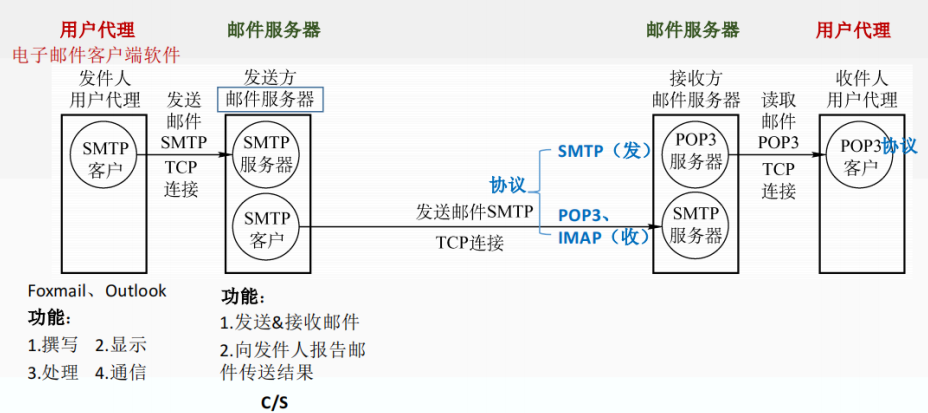
域名解析过程：递归和迭代 递归靠别人迭代靠自己

**文件传输协议FTP：**

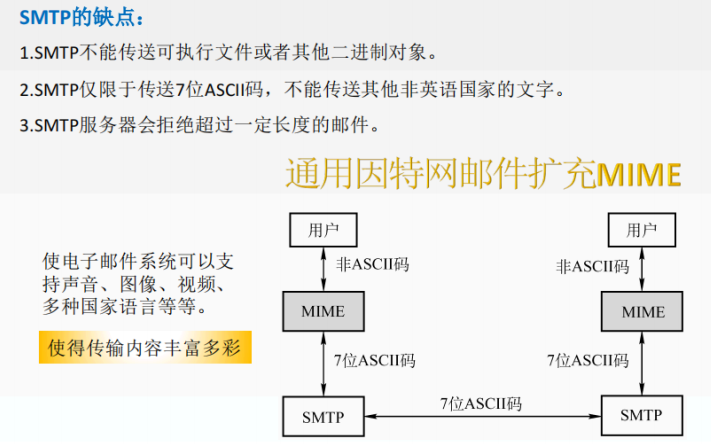
匿名服务器：向公众提供文件拷贝服务



电子邮件：SMAP和POP3 经典组成结构



MIME：



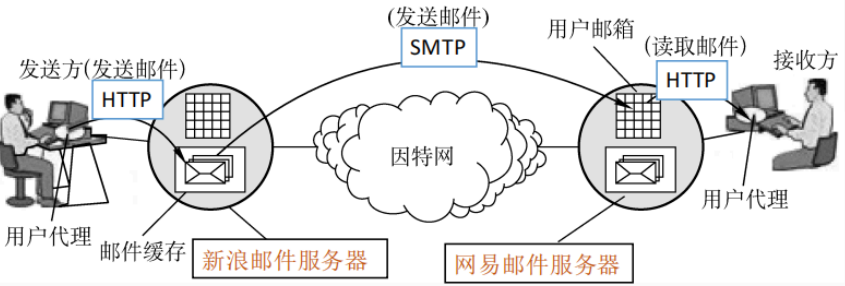
邮局协议POP3： 读邮件的 TCP连接，端口号110

国际报文存取协议 IMAP：POP3升级版

IMAP协议比POP协议复杂。当用户PC上的IMAP客户程序打开IMAP服务器的邮箱时，用户可以看到邮箱的首部，若用户需要打开某个邮件，该邮件才上传到用户的计算机上。

IMAP可以让用户在不同的地方使用不同的计算机随时上网阅读处理邮件，还允许只读取邮件中的某一个部分(先看正文，有WiFi的时候再下载附件）。

基于万维网的电子邮件协议：——利用HTTP发送邮件



万维网：

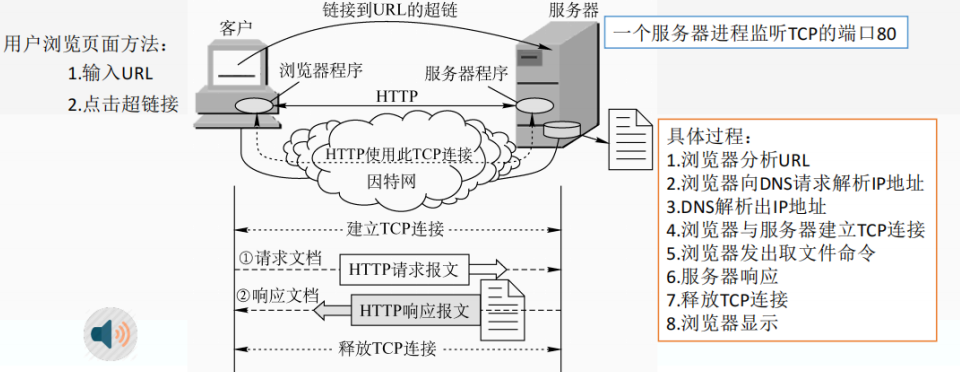
统一标识符URL

用户通过点击超链接(http:/www.baidu.com)获取资源，这些**资源通过超文本传输协议HTTP**传送给使用者。

万维网以**客户/服务器**方式工作，用户使用的浏览器就是万维网客户程序，万维网文档所驻留的主机运行服务器程序。

万维网使用超文本标记语言HTML，使得万维网页面设计者可以很方便地从一个界面的链接转到另一个界面，并能够在自己的屏幕上显示出来

HTTP协议：



HTTP本身是无状态的；但实际中一些万维网站点希望能识别用户——cookie（**存储在用户主机中的文本文件，记录一段时间内用户的访问记录**，目的在提供个性化服务）

**HTTP采用TCP做传输协议，但HTTP本身是无连接的**（通信双方在交换HTTP报文前不需要提前建立HTTP连接）