计算机网络

- 1、概述
  - 主机之间的通信方式?
    - C/S客户端-服务器架构，P2P架构
    - 1、C/S分为服务请求方和服务提供方。
    - 客户：必须知道服务器的地址；不需要强大的硬件支持
    - 服务器：可同时处理多个客户的请求；不需要知道客户的地址，需要强大的硬件支持
    - 2、P2P不区分，支持大量对等用户同时工作，其实是特殊的C/S
  - 三种数据交换方式?
    - 电路交换：用于电话通信，实时通信；两用户通信要建立一条专用的物理链路；通信过程中路径被独占，通信结束后释放；
    - 报文交换：以报文为传输单位；时延较长
    - 分组交换：完整数据称为报文，将其分段；每一段加上首尾部称为分组，包含源地址、目的地址等控制信息；首部开销大
  - 计算机网络按拓扑结构可分为?
    - 总线型：用单根传输线将计算机连接起来。（优点是简单，增删结点方便；缺点是负载时通信效率不高，总线任意一处对故障敏感）

- 星型：每个计算机都用单独的线路与中央设备连接。（优点是便于集中控制和管理，缺点是成本高，中心节点对故障敏感）
- 环形：所有计算机接口设备连成一个环，可以使单环，也可以是双环，环中信号单向传输。
- 网状型：每个结点至少有两条路径与其他结点相连。（优点是可靠性高，缺点是控制复杂，成本高）

- 计算机网络按分布范围可分为?
  - 广域网：主要是用于提供长距离通信，覆盖范围通常为几十千米到几千千米。
  - 城域网：大多再用以太网技术，覆盖范围为几千米到几十千米。
  - 局域网：小范围内、计算机互联网络；以太网是应用最广泛的局域网，采用CSMA/CD技术；覆盖地理范围小、通信延迟短、可靠性高；覆盖范围为几十米到几千米。
  - 个人区域网：就是在个人工作的地方将设备用无线连接起来的网络；覆盖范围10米左右
- 计算机网络的功能?
  - 数据通信
  - 资源共享
  - 提高可靠性：计算机网络都是采用分布式控制方式，如果有部件或少量计算机发生故障，由于相同的资源可分布在不同的计算机上，这

样，网络可以通过不同的路由来访问这些资源，不影响用户对同类资源的访问。

- 促进分布式数据处理和分布式数据库的发展

- 网络性能指标
  - 时延
    - 排队时延：分组在路由器的输入队列或输出队列排队
    - 处理时延：路由器收到分组后的处理，分析首部、提取数据...
    - 传输时延：路由器将分组推出
    - 传播时延：电磁波在信道中传输
  - 带宽：单位时间内网络中某信道最大数据传输率，bit/s
  - 吞吐量：单位时间内通过某网络的数据量 吞返利
  - 往返时间：从发送方发送数据开始，到发送方收到接收方的确认总共的时延RTT
  - 利用率：有数据通过的时间/（有+无）数据通过的时间
- 网络协议三要素?
  - 语法：数据、控制信息的结构、格式
  - 语义：发什么控制信息、完成什么动作、怎么响应
  - 同步：说明事件顺序

- 七层模型及作用?
  - 应用层：为特定应用提供数据传输服务。报文
  - 表示层：数据加密，压缩
  - 会话层：服务器和客户端建立、维护会话
  - 传输层：主机中进程之间的通信
  - 网络层：分组在多个网络间传播
  - 数据链路层：分组在一个网络中传播
  - 物理层：怎样在传输媒体上传输比特流（多少伏代表0，多少伏代表1，用什么样的接口）
- 层次结构的特点?
  - 各层之间是独立的。某一层可以使用其下一层提供的服务而不需要知道服务是如何实现的。
  - 灵活性好。当某一层发生变化时，只要其接口关系不变，则这层以上或以下的各层均不受影响。
  - 易于实现和维护。将一个庞大复杂的系统分解成若干个相对独立的子系统，使实现和维护变得简单
  - 能促进标准化工作。每一层提供的功能和服务都已经有了精确地说明
- 数据封装过程?
  - 应用层：消息/报文message
  - 传输层：消息分段，加上TCP头——TCP segment

- 网络层：加上IP头——IP数据包
- 数据链路层：加上MAC头——帧frame
- 物理层：比特

- TCP/IP协议栈？
  - 网际接口层：PPP
  - 网络层：IP、ARP、ICMP
  - 传输层：TCP、UDP
  - 应用层：FTP、DNS、TELNET、SMTP、POP3、IMAP4、HTTP
- TCP/IP模型
  - 应用层，传输层，网络层，网络接口层
- TCP/IP四层模型、OSI七层模型区别？
  - TCP/IP 先有协议后建立模型，没有对网络接口层进行细分；简化分层；只适用于TCP/IP网络
  - OSI先有模型再有规范；实现困难；适合各种网络
- 路由器和交换机的区别
  - 交换机：二层数据链路层设备；用于组建局域网；依靠MAC地址
  - 路由器：三层网络层设备；跨网段数据传输，路由选择最佳路径；依靠IP地址
- 交换机原理
  - 交换机内有一张MAC表，存放MAC地址到接口映射

- 根据收到的数据帧的首部信息内目的MAC地址在自己的表中查找，有转发，没有转发到全部端口上（泛洪）

- 路由器原理
  - 路由器内有一份路由表，里面有它的寻址信息
  - 收到网络层的数据报后，会根据路由表和选路算法将数据报转发到下一站（可能是路由器、交换机、目的主机）

- 2、物理层
- 物理层接口特性?
  - 机械特性：指明接线器所用的尺寸和大小，引脚数目和排列等等。
  - 电气特性：指明电缆的各条线上所出现的电压范围。
  - 功能特性：指明某条线上的某一电平下电压的意义。
  - 过程特性：指明各种可能事件发生的顺序。积淀功过
- 物理层三种通信方式?
  - 单工通信：只有一个方向的通信，没有反向的交互 ——一条信道
  - 半双工通信：通信双方都可以发送、接收信号，但任何一方不能同时发送、接收——两条信道

- 全双工通信：通信双方可以同时发送接收消息——两条信道
- 两种数据传输方式?
  - 串行传输：速度慢、费用低、适合远距离
  - 并行传输：速度快、费用高、适合近距离，用于计算机内部数据传输
- 奈氏准则、香农定理?
  - 奈氏准则：带宽受限、无噪声条件下，为了避免码间串扰，码元（一个基本波形）传输速率上限是2W Baud
  - 香农定理：带宽受限、有噪声条件下，为了不产生误差，信道的数据传输速率有上限值
- 什么是码间串扰?
  - 传输特性不理想、波形畸变、相邻码元波形之间发生部分重叠
- 基带信号、带通信号?
  - 基带信号：未经过任何处理的信号，一般传的不远，频率较低，比如说话的声波。
  - 带通信号：基带信号调制后的结果，频率较高，传得更远。
- 调制?
  - 将数字信号（比特流，取值离散）转化为连续的模拟信号
- 基本调制方法?

- 调幅AM：振幅有变化代表1，无变化代表0
- 调频FM：频率高代表1，频率低代表0
- 调相PM：正弦波代表1，余弦波代表0

- 信道复用技术（静态划分信道，物理层）
  - 频分复用FDM：所有主机在相同的时间占用不同的频率带宽资源。
  - 时分复用TDM：时间分片，所有主机在不同的时间片，占用相同的频率带宽资源，固定顺序（统计时分复用不固定用户顺序）
  - 波分复用WDN：光的频分复用
  - 码分复用CDM（为了安全）：各用户可以在同样时间使用同样的频带进行通信。特别地，各用户使用经过特殊挑选的不同码型，以使各用户之间不会造成干扰。
- 物理层设备？（不隔离冲突域）
  - 中继器：对衰减的信号进行放大，以增加信号传递的距离
  - 集线器：对衰减的信号放大，再转发到其他所有工作状态端口上（不能隔离冲突域）

- 3、数据链路层
- 数据链路层的功能？
  - 网络层传下来的IP数据报添加首部尾部，封装成帧

- 透明传输：帧使用首部、尾部定界，数据部分有相同内容，加上转义字符，用户察觉不到转义字符的存在
- 差错检测：CRC冗余检验

- 两种情况下的数据链路层
  - 使用点对点信道：ppp协议（点到点协议）
  - 使用广播信道：通信协议CSMA/CD
- 通信协议CSMA/CD（动态划分信道）？
  - 多点接入：多主机连到总线上
  - 载波监听：发数据前先检测总线上有无数据，有则不发
  - 碰撞检测：发送中，监听到信道已有其它主机正在发送数据，表示发生了碰撞。（提前监听，但电磁波有时延，还是可能会发生碰撞）
- PPP协议?
  - 点对点协议，用户拨号上网使用，只支持全双工链路
- MAC地址?
  - 物理地址，唯一标识网卡/网络适配器
- 以太网?
  - 星形拓扑局域网
- 虚拟局域网VLAN?
  - 出现原因：以太网扩大，广播域扩大，广播风暴

- 解决方法：虚拟局域网VLAN：同一VLAN可以广播通信，不同VLAN 不可广播通信
- 链路层设备？（隔离冲突域）
  - 网桥：根据MAC地址转发或过滤收到的帧（丢弃）
  - 交换机：
    - 是一种多接口的网桥
    - 接口处还有存储器，可以在繁忙时把帧进行缓存
    - 是一种即插即用的设备，内部的帧交换表具有自学习功能
    - 可以实现虚拟局域网VLAN
- 4、网络层
  - 分组交换的两种方式
    - 虚电路方式：面向连接；分组传输前先建立逻辑连接，按序发送
    - 数据报方式：无连接；每个分组独立发送、走不同路径；乱序
  - IP地址编址方式？
    - 分类编址：网络号+主机号，不同分类有不同的网络号长度
    - 子网划分：网络号+子网号+主机号，必须配置子网掩码（子网掩码与IP地址相与，得到主机号）

- 无分类编址CIDR：网络前缀号+主机号，
- IP地址32位,分四组十进制表示
- IP地址分类?
  - 主机号全0为网络地址，全为1为广播地址，不可分配
  - A类地址：0开头（第一字节0~127），网络号1字节，网络号0和127不指派
  - B类地址：10开头（128~191）网络号2字节
  - C类地址：110开头（192~223）网络号3字节
  - D类地址多播地址，E类地址保留
- 特殊IP地址?
  - 0.0.0.0所有不清楚源地址、目的地址的集合，默认路由
  - 255.255.255.255广播地址（路由器不转发）
  - 127.0.0.1本机地址
  - 10.X.X.X、172.16.X.X ~ 172.31.X.X、192.168.X.X私有地址 61
- 子网划分?
  - 必须配置子网掩码，IP地址与子网掩码相与得到主机号
  - 默认子网掩码：未划分子网时，网络号全为1
- 无分类编址?
  - 背景：子网数目继续扩充
  - 构造方式：网络位长度可以任意指定

CIDR使用“斜线记法”，或称CIDR记法。即在IPv4地址后面加上斜线“/”，在斜线后面写上网络前缀所占的比特数量。

- 构成超网：把许多小网合并成大网，通过找共同前缀实现
- ARP地址解析协议工作原理？
  - IP地址——>MAC地址
  - 每个主机上都有一个ARP高速缓存，有本局域网里，IP地址到MAC地址的映射表
  - （广播请求，单播响应）收到数据包，先查表，表中没有，广播发送ARP请求，目的主机收到请求，单播发送ARP响应给A，A将获得的关系写入缓存
- 网际控制报文协议ICMP？
  - 作用：用于在主机、路由器之间传递控制信息
  - 两种报文：询问报文、差错报告报文
  - 应用：跟踪路由traceroute（源主机到目的主机要经过哪些路由器）,ping测试连通性
- 虚拟专用网VPN作用？
  - 通过因特网，连接同机构不同网络
  - 各主机地址为，本机构可自由分配的，私有/专用地址（只能内部通信，不可与因特网其他主机通信）
- 网络地址转换协议NAT作用？转换，地址，安全
  - 专用网主机想和因特网主机通信，通过NAT路由器（维护一张NAT转换表：内网地址-外网地

址），转换成临时公有IP地址

- 缓解IPv4地址空间耗尽问题
- NAT对外网主机屏蔽了内网主机的网络地址，可避免网络外部攻击

- 冲突域和广播域?
  - 冲突域：同一时间内、只能有一台设备、发送信息的范围，交换机每个端口自成一个冲突域
  - 广播域：收到同样广播消息的节点的集合，路由器上的每个端口自成一个广播域
- 隔离广播域?
  - 收到广播地址不转发
- IP数据报发送流程?
  - 主机发送，路由转发
  - 同一网络上的主机可以直接通信（直接交付），不同网络上主机通信要通过路由器（间接交付）
- 中继器、集线器、网桥、交换机、路由器区别?
  -

> 中继器和集线器工作在物理层，既不隔离冲突域也不隔离广播域。
>
> 网桥和交换机（多端口网桥）工作在数据链路层，可以隔离冲突域，不能隔离广播域。
>
> 路由器工作在网络层，既隔离冲突域，也隔离广播域。

- 路由配置方法?
  - 静态路由配置：人工配置路由表
  - 动态路由配置：由路由选择协议实现（内部网关协议： RIP/OSPF; 外部网关协议：BGP）

- RIP路由信息协议（应用层协议）
  - 认为好的路由是距离短的，即通过路由器数量最少的路由
  - 特点：周期性和相邻路由器交换路由表
  - 存在问题：路由环路（数据始终在网络中传输，无法到达目的地）
- OSPF开放最短路径优先协议（传输层协议）
  - 基于链路状态，采用迪杰斯特拉算法，无路由环路问题
  - 链路状态发生变化时、广播发送、与本路由器相邻所有路由器的链路状态
  - 链路状态：与哪些路由器相连，以及“代价”
- BGP外部网关协议
  - 与其他相邻自治系统BGP、交换网络可达性信息（到达某个网络要经过的一系列自治系统）
- RIP、OSPF、BGP的比较
  - RIP：基于距离向量的内部网关协议，广播UDP报文交换路由信息
  - OSPF：基于链路状态的内部网关协议，交换信息量大，报文要短，采用IP
  - BGP：外部网关协议，不同自治系统间交换路由信息，网络环境复杂，要保持可靠传输，采用TCP
- 网络层主要协议?

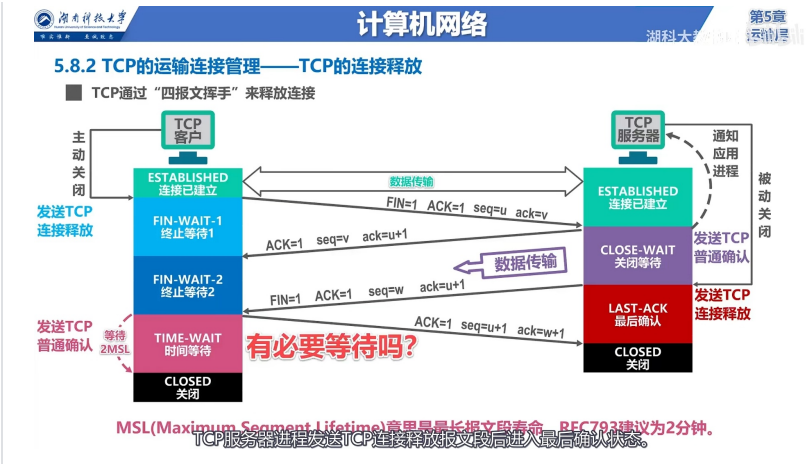
- IP；ARP, ICMP辅助IP；NAT不明确
- IPV4、IPv6（根本上解决IP地址耗尽问题）
  - IPV4 32位，点分十进制表示；IPv6地址扩大到128位，8个16进制块，用冒号分隔
  - IPV4：单播、多播、广播；IPV6：单播、多播、任播（地址类型）
    - 单播：点对点通信；多播（一点对多点通信，广播是多播的一个特例）；任播（终点是一组计算机，但只交付其中一个）
- 5、传输层
- 端对端通信、点对点通信?
  - 点对点通信是数据链路层提供的，是主机与主机之间的通信，一个点是指MAC地址或IP地址
  - 端到端通信传输提供的，指运行在不同主机之间两个进程之间的通信，一个进程由一个端口来标识。
- UDP和TCP区别?
  - 1、TCP先连接再传输，UDP直接传输
  - 2、TCP只能一对一传输，UDP多种模式
  - TCP面向字节流，UDP传整个包
  - 3、TCP可靠，不丢不重，按顺序，UDP不可靠，误码丢弃
  - TCP流量控制、差错检测，UDP传输速率不受网络影响，适合实时传输

- 4、TCP首部长，UDP短
- 5、TCP用于FTP/HTTP/HTTPS，UDP用于音视频，广播

- TCP三次握手过程?
  - ack确认号，seq序号
  - 确认ACK（=1时确认号有效），同步SYN在连接建立时用来同步序号
  - A发送连接请求报文：同步位SYN=1，ACK=0，seq=x（选一个自己的初始序列号）
  - B收到，同意连接，发送连接确认报文：SYN=1，ACK=1，seq=y（选一个自己的初始序列号），ack=x+1
  - A收到确认报文，确认收到：ACK=1，seq=x+1，ack=y+1（确认对方序列号）
  - B收到A确认，连接建立
- TCP四次挥手过程?
  - 双方都可请求释放连接，ACK始终为1
  - 序号seq自己发，确认ack都加1
  - A发送TCP连接释放报文段，进入FIN-WAIT：FIN=1 终止位，seq=u 自己发送数据最后一个字节的序号加1，ack=v 自己收到的数据最后一个字节的序号加1
  - B发送TCP普通确认报文段，进入CLOSE-WAIT：seq=v，ack=u+1(B可以向A发，A不可

以向B发)

- B不需要连接时，发送连接释放报文：FIN=1，seq=w可能又发送了一些数据，ack=u+1重复确认
- A收到，发出确认，进入TIME-WAIT状态，等待2MSL后关闭（最大报文存活时间）：seq=u+1, ack=w+1
- B收到确认关闭ACK=1



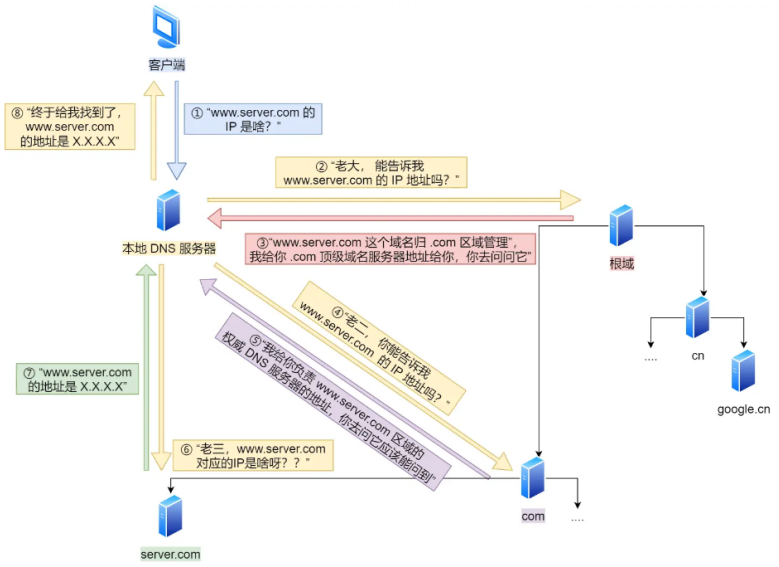
- 为什么要四次挥手？/为什么要有CLOSE-WAIT?
  - 客户端发送FIN=1的连接释放报文，服务器收到进入CLOSE-WAIT
  - 这个状态是让服务器发送未发送完的数据
- 为什么要有MSL/最后的TIME-WAIT?
  - 1、确认最后一个A给B的确认报文可以到达。B若未收到确认报文，会请求重传
  - 2、让本连接内所有报文从网络中消失，下次连接不会受旧报文干扰
- TCP可靠传输如何实现?

- 超时重传机制，一个已经发送的报文段在超时时间内没有收到确认，那么就重传这个报文段
- RTT时间?
  - 往返时间(Round-Trip Time)：报文段从发送到接收到确认经过的时间
- TCP流量控制如何实现?
  - 滑动窗口
- 什么是滑动窗口?
  - 缓存的一部分，用来存放字节流
- 滑动窗口如何工作?
  - 发送方，接收方各有一个滑动窗口
  - 接收方通过 TCP 报文段中的窗口字段告诉发送方自己的窗口大小，发送方根据这个值和其它信息设置自己的窗口大小
  - 发送窗口：前面所有段都发送且收到确认，滑动到第一个字节不是已发送已确认的状态
  - 接收窗口：前面所有段都接收到，才会移动...接收窗口只会对窗口内最后一个按序到达的字节进行确认
  - （确认报文段中ack=31说明希望收到31号数据，发送方收到该数据，得知字节31之前都已经被接收）
- TCP四种算法实现拥塞控制?

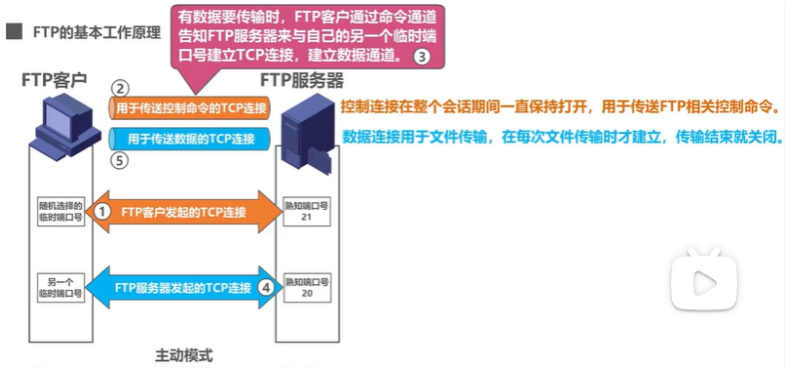
- 发送方维护一个状态变量：拥塞窗口cwnd，值随着网络拥塞程度动态变化
  - 窗口变化原则：无网络拥塞，增大窗口，出现拥塞，减小窗口
  - 网络拥塞如何判断？发生超时重传
- 发送方将拥塞窗口作为发送窗口
- 慢开始&拥塞避免算法
  - 刚开始执行慢开始算法，cwnd=1，收到确认后，每轮指数增长
  - 到慢开始门限，拥塞避免算法，cwnd线性增长加1
  - 发生超时重传，门限减半，窗口置1，重新慢开始算法
  - 再次到达门限，使用拥塞避免....
- 快重传&快恢复
  - 丢包导致超时重传，但并没有拥塞
  - 发送方收到三个重复确认，立刻重传（快重传）
  - 然后执行快恢复，慢开始门限，窗口减半，执行拥塞避免

- 6、应用层。
  - 域名系统协议DNS？
    - 作用：通过域名（网址）找到查到IP
    - 可以使用TCP或UDP传输，端口号53

- DNS域名解析过程？
  - 浏览器先看自身缓存有没有，没有向操作系统询问，操作系统查看自身缓存，没有向hosts文件询问，最后才会问本地DNS服务器
  - 按照本地域名服务器，根域名服务器，顶级域名服务器，权限域名服务器顺序请求
  - 图示



- 文件传输协议FTP？
  - 客户机从FTP服务器上传或者下载文件，基于TCP，C/S架构
- FTP的两种模式？
  - 主动模式：建立数据通道时，服务器主动连接客户机



- 被动模式：建立数据通道时，客户机主动连接服务器
- 注意：两种模式命令通道的建立没有不同

- 动态主机配置协议DHCP?
  - 各主机通过DHCP动态获取网络配置信息，基于UDP
- 什么是中继代理?
  - 将一个局域网内的DHCP请求转发到其他局域网内的DHCP服务器上
- DHCP协议工作过程? fati 请确
  - 1、客户机广播发送DHCP发现报文，源IP为0.0.0.0，若客户机和服务器不在同一子网，需要中继代理
  - 2、DHCP服务器收到报文，广播发送DHCP提供报文给客户机
  - 3、客户机广播发送DHCP请求报文，告知是否使用对方作为DHCP服务器
  - 4、服务器发送DHCP确认报文，客户机可使用租用给它的IP
  - 5、租用期过半，客户机发送DHCP请求报文，请求续约
  - 6、客户机可随时停止租期
- 电子邮件协议有哪些?
  - SMTP简单邮件传送协议 邮件发送协议

- POP3邮局协议 邮件读取协议 基于TCP，C/S
- IMAP4因特网邮件访问协议 邮件读取 基于TCP，C/S

- SMTP特点?
  - 只能传送ASCII码文本数据
  - 通过MIME多用途因特网邮件扩展协议可传送非ASCII码文本数据
- SMTP工作原理?
  - 发送方邮件服务器周期性扫描缓存
  - 发现有邮件，主动与接收方邮件服务器建立连接
  - 接下来通过命令和应答的方式发送邮件
- POP3邮局协议特点?
  - 支持下载删除，下载保留方式从邮件服务器下载邮件到客户机
  - 不允许用户管理邮件
  - 端口110
- IMAP4因特网邮件访问协议特点?
  - 允许用户在自己计算机管理邮件服务器邮件，联机协议
  - 端口143
- 什么是万维网WWW?
  - 联机信息储藏所，不是某种计算机网络，是种应用

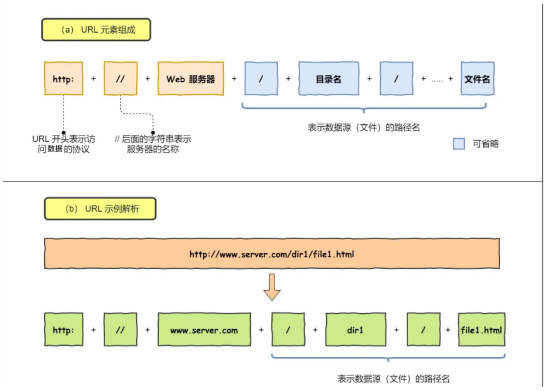
- 浏览器是万维网应用的客户进程。不同浏览器对网页内容解析有所不同，因为使用不同浏览器内核（渲染引擎）
- 什么是URL?
  - URL统一资源定位符，即网址。指明资源位置，<协议>://<主机>:<端口>/<路径>
- 什么是Cookie?
  - 服务器端保存客户端信息的文本文件
- 超链接的作用?
  - 通过超链接可以将网页连接成信息网
- 万维网文件类型?
  - HTML超文本标记语言，使用标签，描述网页结构和内容
  - CSS层叠样式表：描述网页样式
  - JavaScript：控制网页行为，与JAVA无关
- 万维网协议——HTTP协议
  - 超文本（音视频图文混合体）传输协议
  - 无状态协议，先建立TCP连接，再通过请求、响应报文交互，C/S模型
  - 两种报文（每个请求报文都会收到一个响应报文）
    - 请求报文：第一行有方法（常用方法：GET从URL标记处获取资源、POST向服务器提交数据）、URL、HTTP版本

- 响应报文：第一行有HTTP版本、状态码（202接受、400错误请求、404找不到）、解释状态码短语

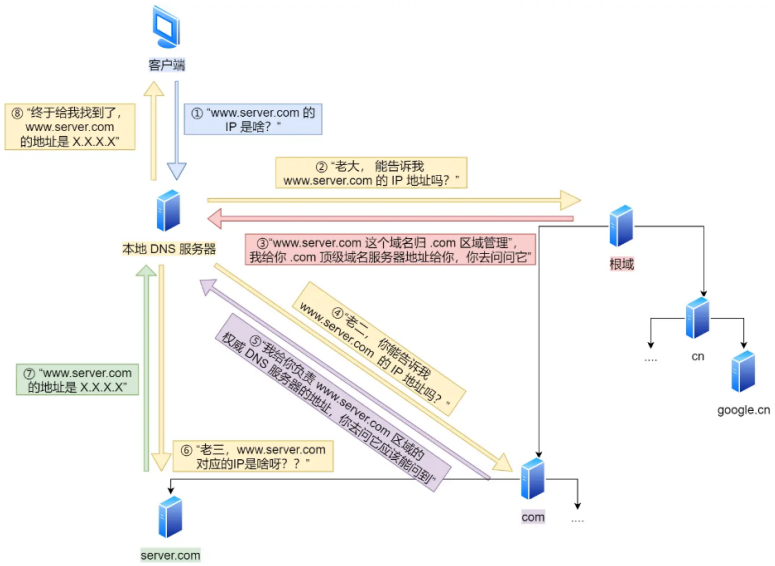
- HTTP/1.0和HTTP/1.1区别？
  - HTTP/1.0：每次请求都要建立连接，收到响应后关闭连接（每次都经历三次握手、四次挥手）
  - HTTP/1.1：引入持久链接，TCP连接默认不关闭，可被多个请求复用
- HTTP 2（基于SSL）优化了哪些？
  - 头部压缩：多个请求头部一样，消除重复
  - 报文采用二进制格式：提高数据传输效率
  - 并发传输：多个请求复用一条连接
  - 改进请求应答模式：服务器可以主动向客户端发送信息
- 什么是SOCKET？
  - SOCKET=IP+端口号，通过socket与其它主机应用建立通信
  - 端口号用来区分数据应该发送到哪一个应用上，将一条数据线插到不同主机应用的插槽上
- 应用层常见协议及端口号？
  - DNS域名解析协议，53
  - DHCP动态主机配置协议，67/68
  - FTP文件传输协议，控制连接21，数据传输20

- TELNET远程终端协议，23
- HTTP超文本传输协议，80
- SMTP简单邮件传送协议，25
- POP3邮件读取协议，110
- IMAP网际报文存取协议，143

- 从输入网址到显示网页的过程?
  - 解析URL获得web服务器域名（www. xxx. com ）和文件路径名
    - URL其实是在请求服务器中的文件，没有路径名时就会访问根目录下的默认文件



  - 生成HTTP请求消息
  - 查询服务器域名对应的IP地址： DNS服务器保存了web服务器和IP的对应关系
    - DNS地址解析过程



浏览器先看自身缓存有没有，没有向操作系统询问，操作系统查看自身缓存，没有向hosts文件询问，最后才会问本地DNS服务器

- **获得IP，将传输工作交给操作系统中的协议栈，生成TCP，IP报文，加上MAC头部**
- **网卡将数字信号转化成电信号，通过网线发送出去**
- **交换机接收电信号，转化为数字信号，直接缓存，查自己的MAC地址表（mac地址-端口），将包发送到对应端口，MAC地址表查不到就发送到所有端口上（局域网内）**
- **路由器接收以太网包（接收电信号，转化为数字信号，错误校验，查看是否是发给自己的包，缓存），查路由表（IP地址-端口号），转发到对应端口，网络包在路由器上传输...**
- **服务器收到请求，同样方式发包，客户端收到，渲染网页**

以上内容整理于 幕布文档