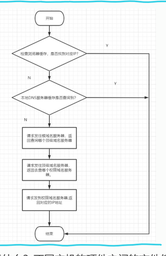
计算机网络
by:斐

应用层

存放产生流量的应用
常用协议：FTP,SMTP,HTTP
干什么？文件传输、邮件、虚拟机

- 两种网络应用模型
  - C/S模型　有中心节点
  - P2P模型　没有中心节点，每个机器都有上传下载功能
- DNS系统
  网络域名解析系统



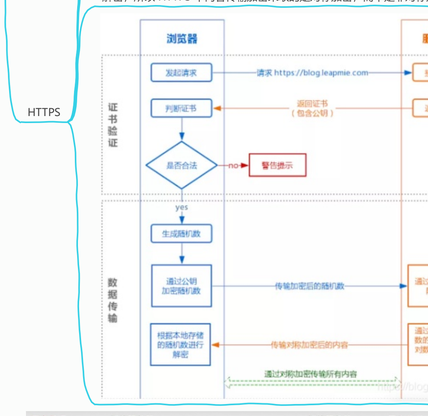
- FTP
  - 干什么？不同主机软硬件之间的文件传输
  - C/S模型，TCP
  - 是什么？简单邮件传输协议
- SMTP
  - 用什么？TCP，C/S模型，端口号25
  - 缺点？只能传英文，易长的这样
- POP3
  - 用什么？TCP，C/S模型，端口号110
  - 缺点？不方便
- IMAP（pop3的plus版本）
- 协议
  - HTTP
    - 干什么？定义了浏览器如何向www请求文档数据
    - 是什么？无状态的协议，浏览器不会记住你是谁

状态码	类型
1XX	信息性状态码
2XX	成功状态码
3XX	重定向状态码
4XX	客户端错误状态码
5XX	服务端错误状态码

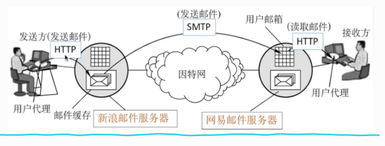
- 3XX
  - 301永久重定向
  - 302临时重定向
  - 400错误请求
- 4XX
  - 401未授权
  - 403服务器拒绝
  - 500服务器内部错误
- 5XX
  - 502网关错误
  - 503服务器不可用
  - 504网关超时

状态码详细信息：https://www.cnblogs.com/starof/p/5035119.html

  - HTTPS
    - 是什么？HTTP+SSL
      - 如何加密？服务器传递公钥给客户，但是私钥保留，客户端通过公钥加密新生成的密钥，传递给服务器，服务器用私钥解密密钥后通过密钥加密信息给客户端。
    - 对称加密　指加密解密都使用同一密钥
    - 非对称加密　反之，使用不同密钥
    - HTTPS协议之所以是安全的是因为 HTTPS 协议会对传输的数据进行加密，而加密过程是使用了非对称加密实现。但其实，HTTPS在内容传输的加密上使用的是对称加密，非对称加密只作用在证书协议环节。
    - 非对称加密的加解密效率是非常低的，而 http 的应用场景中通常端与端之间存在大量的交互，非对称加密的效率是无法接受的；
      另外，在 HTTPS 的证书中只有服务端保存了私钥，一对公私钥只能实现单向的加解密，所以 HTTPS 中内容传输加密采取的是对称加密，而不是非对称加密。



  - 邮件



时代发展后要新为使用http协议

  - cookie&session
    - 相同点　都是属于会话跟踪技术。
    - cookie
      - Cookie通过客户端记录信息确定用户身份，Session通过在服务器端记录信息确定用户身份。
      - Cookie实际上是一小段的文本信息。用来存放用户状态，可以被服务器修改。
      - cookie是不可跨域名的(浏览器可以在二级域名下使用)，也不支持修改端口，只能同名重置。
      - cookie普通过传输协议走的，使用http协议是可能导致数据在不加密的情况下被截获的，其中有一个secure字段可以控制只在https等安全协议里面传输cookie
    - session
      - Session机制决定了当前客户只会获取到自己的Session，而不会获取到别人的Session，各客户的Session创建过程是独立，互不可见。Session的使用以Cookie为使，但是过多的Session存储在服务器内存中，会对服务器造成压力。如果用户太多可能会导致内存溢出，所以session信息应该精简。为了减小服务器压力，会把超过session生存时间的session删除。
      - session正常运行需要客户端浏览器的支持，因为session需要cookie作为标识（http无状态，无法判断用户）。session会自动生成cookie一个专用的cookie来判断是否为同一个用户！禁用cookie会导致session失效。
    - 不同点　最大区别为生存周期，session会过期，同时浏览器的开关同样会导致session过期，cookie是预先设置的生存周期，或永久的保存于本地的文件。
- http协议的过程
  1. 使用DNS域名解析；
  2. 发起TCP的3次握手；
  3. 建立TCP连接后发起http请求；
  4. 服务器响应http请求，浏览器得到返回response；
  5. 浏览器解析response，并请求其它的资源（如js、css、图片等）；
  6. 浏览器对页面进行渲染。

表示层

处理两个网络通信系统的信息
常用功能：数据转换、数据加解密、数据压缩和恢复

- 表示层

会话层

建立连接、有序传输数据
常用功能：建立管理终止会话，从校验点恢复数据继续传输数据

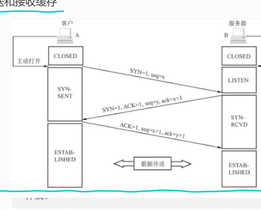
- 会话层

传输层
进程之间通信

两进程之间的通信，端到端的报文段传输
常用功能：可靠传输、差错控制、流量控制、复用分用
常用协议：TPC、UDP

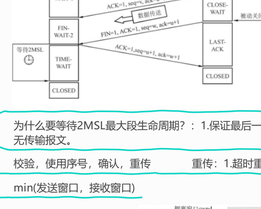
应用程序	FTP	TELNET	SMTP	DNS	TFTP	HTTP	SNMP
熟知端口号	21	23	25	53	69	80	161

- 端口号
  16bit
  - 服务端端口号
    - 知名端口号0-1023
    - 普通端口号1024-49151
    - 补充：https:443　socket：1080　mysql：3306
  - 客户端端口号　客户端口号49152-65535
- 协议
  - UDP
    - 无连接的，面向不可靠传输
    - 无拥塞控制（但是有校验和，校验不对的直接丢掉！），适合实时性的网络传输
    - 头部比TCP小（8B　20B）
    - 面向报文的，每一个UP把应用层的整个报文都接收并且封装，不会分片
  - TCP
    - 点对点，可靠有序不丢不重
    - 全双工，有发送和接收缓存
    - 三次握手



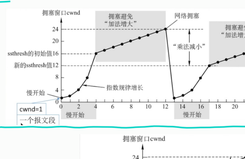
ROUND 1：客户端发送**连接请求报文段**，无应用层数据。
SYN=1，seq=x(随机)
ROUND 2：服务器端为该TCP连接**分配缓存和变量**，并向客户端返回**确认报文段**，允许连接，无应用层数据。
SYN=1，ACK=1，seq=y(随机)，ack=x+1
ROUND 3：客户端为该TCP连接**分配缓存和变量**，并向服务器端返回确认报文。可以携带数据。
SYN=0，ACK=1，seq=x+1，ack=y+1

    - 四次挥手

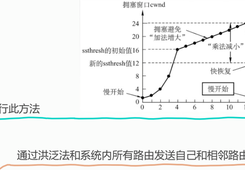


ROUND 1：客户端发送**连接释放报文段**，停止发送数据。主动关闭TCP连接。
FIN=1，seq=u
ROUND 2：服务器端回送一个确认报文段，客户到服务器这个方向连接释释放了——半关闭状态。
ACK=1，seq=v，ack=u+1
ROUND 3：服务器最后完成数据发送段，主动关闭TCP连接。
FIN=1，ACK=1，seq=w，ack=u+1
ROUND 4：客户端回送一个确认报文段，再等到时间等待计时器(2MSL：最长报文段寿命)，连接释放，关闭。

      - 为什么要等待2MSL最大段生命周期？：1.保证最后一个ACK报文可达，让链路中无传输报文。
    - 可靠传输　校验，使用序号，确认，重传　　重传：1.超时重传，收到三个相同ACK确认触时重传
    - 流量控制　min(发送窗口，接收窗口)
    - 拥塞控制



      - 慢开始，拥塞避免
      - 快重传，快回复
        三个冗余ACK收到触发执行此方法



网络层
主机之间通信

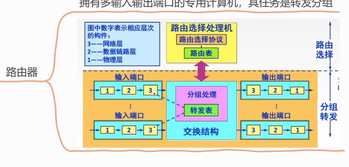
为了把分组从源传输到目的地，分组是数据包切割而成。
分组端到端传输，单位报文段
路由选择机制发，异构网络互联，拥塞控制
常用功能：路由选择，差错控制，流量控制，拥塞控制
常用协议：IP，ICMP，OSPF

- 路由选择协议
  - 内部路由选择协议IGP
    - OSPF
      适合大网
      - 通过洪泛法和系统内所有路由发送自己和相邻路由器的链路状态信息
      - 只要网络有变动就会更新
      - 路由表中需要保存一个路由表，用来保存从自己到目的地址的最佳距离和下一跳ip
      - 注意如果超过16条就表示不可达。
      - 最开始的时候，每个路由把路由表只有自己，经过若干次和相邻路由表交换路由表信息后结果会收敛。
    - RIP
      适合小网
      - 应用层协议，使用UDP
      - 好消息传得快，坏消息传的慢，因为如果：
        信息传递会依照数跳中可达且距离最小的来更新
        在多次传递假网络之后才能发现当前是不可达。

  - 外部路由选择协议EGP　BGP
    - 和其他自治系统的边界路由器交换信息，交换和其他自治系统可达性的信息。
    - 应用层协议，TCP协议
- IP地址

NetID 网络号	HostID 主机号	本地地址（局部地址）	环回地址	描述
全0	全0	可以	不可以	本网络上的本主机，路由表中用于表示默认路由（有点像下面network的写法）
全0	特定值	不可以	可以	表示本网内某个特定主机
全1	全1	不可以	可以	本网广播地址（路由器不转发）
特定值	全0	不可以	不可以	网络地址，表示一个网络
特定值	全1	不可以	可以	直接广播地址，对特定网络上的所有主机进行广播
127	任何值（非全0/1）	可以	可以	用于本地软件自测试用，极为环回地址

  - 目的是把内网的ip和端口号，映射为外部互联网大网ip和路由器，达到和其他网络互联的目的。
  - NAT路由器：只需要使用NAT软件即可
  - NAT转换表：内网ip端口 <-> 外网ip端口
  - NAT网络地址转换协议
  - ARP协议
    ip地址到MAC地址的一个映射
    内网之间的一种协议，用来找目的地。　　通过广播自己的ip，期望ip，自己MAC地址，目的地收到后单播返回自己的MAC地址，建立起协议。
  - 协议
    - DHCP协议
      DHCP服务器有一个ip池，使用C/S方式，动态分配ip给新接入的设备。
      是应用层协议，但是是网络层基础，动态提供了当前网络的动态ip，通过广播通信
    - ICMP网际控制报文协议
      传递的是控制信息，例如网络不通，是否可达，路由是否可用等
      - ICMP差错控制报文
      - ICMP询问报文：例如ping命令
  - CIDR超网　就是把多个小子网，合并成一个大网
  - 设备　路由器



拥有多输入输出端口的专用计算机，其任务是转发分组

数据链路层

物理层plus版本：从物理连接改造成逻辑上无差错的数据链路
网络层信息是以太网帧。传输单位帧
常用功能：差错控制、流量控制、接入控制
常用协议：PPP

- 功能
  - 封装帧帧透明传输
    - 字符填充法
    - 零比特填充法：五个一填充/删除0
  - 流量控制
    接收方接收不下就不回复
    点对点
    - 停止等待
    - 滑动窗口
  - *差错控制
    主道P21
    - *奇偶校验码
    - *CRC
    - *海明码
- 协议
  - PPP协议：点对点协议，用来对两节点建立直接连接
  - HDLC协议：HDLC协议用以保证传送到下一层的数据在传输过程中能够准确地被接收。

  - CSMA/CD：检测碰撞
  - CSMA/CA：避免碰撞
- 数据链路层设备
  - 网桥：根据目的地址对帧进行过滤，自学习和隔断用分割了冲突域，因为会对帧进行过滤，所以分割。
  - 交换机(多口网桥)
    每个口都是一个冲突域，但是在同一个广播域

	能否隔离冲突域	能否隔离广播域
物理层设备【集线器】（中继器、集线器）	×	×
链路层设备【网桥】（网桥、交换机）	√	×
网络层设备【路由器】（路由器）	√	√

物理层

物理媒介上透明传输　　物理层设备
- 放大器：放大模拟信号
- 中继器：再生还原数字信号
- 集线器(多口中继器)：共享式设备通过广播