# 第一章

一、计算机网络简单定义：一些互相连接的、以共享资源为目的的、自治的计算机的集合。

二、什么是因特网

1. 构成描述
   1. 端系统
   2. 连接设备
      1. 通信链路
      2. 分组交换机
         1. 链路层交换机
         2. 分组交换机
   3. 分组交换技术
      1. 发送端将要发送的数据分成若干较小的块， 添加首部形成  
         分组（ 包packet） ， 分别发送到目的端， 再组装恢复原数据。
      2. 路径（ route或path） ： 一个分组从发送端系统传输到接收端  
         系统， 所经过的一系列通信链路和分组交换机
      3. 端系统之间通信的路径不专用。
      4. 多个通信端系统同时共享一条路径或一部分。
      5. 第一个分组交换网络：ARPA网， 产生于20 世纪70年代， 是因特网的“ 最早祖先” 。
   4. 因特网服务提供商ISP
      1. 一个由多个分组交换机和多段通信链路组成的网络。 端系统通过ISP接入因特网， 如住宅区ISP、 大学ISP、 公司ISP等。
2. 服务描述
   1. 提供网络应用基础架构  
      允许终端系统上运行分布式应用程序，并彼此交换数据:  
      如Web, email, games, e-commerce, database,  
      VOIP, P2P file sharing
   2. 为分布式应用程序提供的通信服务接口:
      1. 无连接服务connectionless
      2. 面向连接服务connection-oriented
      3. 不提供数据传递时间保证（发送端到接收端）的服务

三、网络协议

1. 什么是网络协议

定义了通信实体之间交换的报文的格式和传输顺序，以及在报文发送和/或接收或者其他事件方面所采取的行动（ 响应）

1. 因特网协议： TCP/IP协议。
   1. TCP（ Transmission Control Protocol） 传输控制协议
   2. IP （ Internet Protocol） 网际协议
2. 因特网标准： 由IETF制定的标准文档RFC。
   1. RFC（ Request For Comments ） ：请求评论
   2. IETF (Internet Engineering Task Force ) ： 因特网工程任务组。
   3. RFC有近6000个， 不断更新完善。

四、网络的两大部分

* 1. 网络边缘（资源子网）
  2. 网络核心（连接子网，无应用层）
     1. 边缘路由器：一台端系统到另一台端系统所经过的路径上的第一台路由器
     2. 接入网：端系统到边缘路由器上的通信链路

五、数据如何通过网络传送

* 1. 电路交换
     1. 特点
        1. 静默期长
        2. 需要预留端到端资源
        3. 传输速率恒定
     2. ·分类
        1. 时分复用
        2. 频分复用
  2. 分组交换
     1. 特点
        1. 每个分组使用链路全部带宽
        2. 不需要预留端到端资源，资源按需使用
     2. 工作过程
        1. 源端将报文划分为较小的数据块（分组packet），每个分组通过一系列链路和分组交换机传送，直到目的端目的端恢复原报文。
     3. 分类
        1. 虚电路网络
           1. 一定面向连接
        2. 数据报网络
           1. 可以面向连接也可以不面向连接
     4. 流量强度

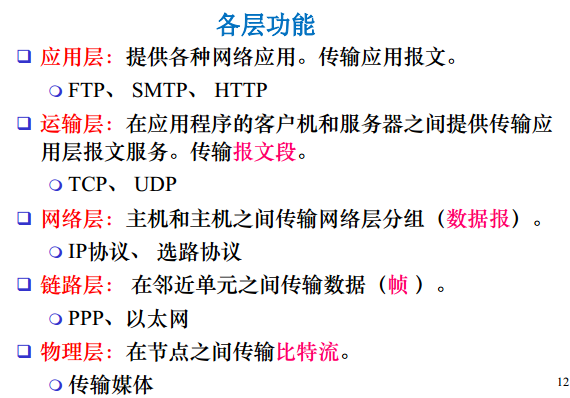
设， R= 链路速率 (bps)、 L= 分组长度 (比特)、 a= 平均分组到达速率（每秒分组， pkt/s则流量强度=La/R（比特到达队列速率是La bit/s

六、协议分层

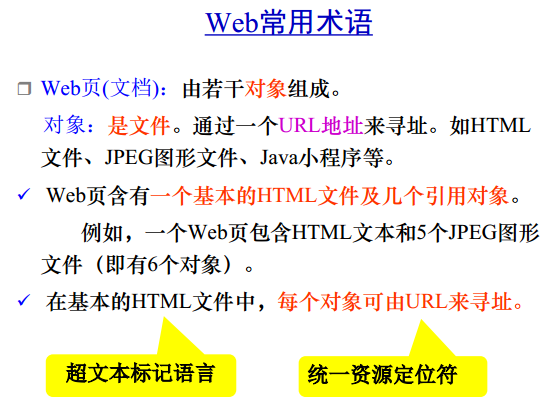


会话层的主要功能是在两个节点间建立、维护和释放面向用户的连接，并对会话进行管理和控制，保证会话数据可靠传送。

表示层主要是负责数据格式的转换，压缩与解压缩，加密与解密。



# 第二章





一、HTTP协议

1. 定义：HTTP定义了在浏览器程序和Web服务器程序间传输的报文格式和序列
2. 底层协议：TCP
   1. 工作过程
      1. 创建TCP连接->交换报文->关闭TCP连接
   2. TCP提供了可靠的传输服务
      1. TCP保证HTTP报文能够完整的到达对方
3. 特点·
   1. HTTP是无状态的协议服务器端不会保存关于客户端的任何信息
4. 分类
   1. 非持久HTTP连接
      1. 特点
         1. 每个TCP连接只传送一个web对象
         2. 每个web对象的时间=2\*RTT+文件传输时间
   2. 持久HTTP连接
      1. 特点
         1. 每个TCP连接可以传送多个web对象
      2. 分类
         1. 非流水线方式：客户机只能在接受到一个响应后再发送新的请求
         2. 流水线方式：可以连续产生请求，可能传输所有报文时间只需要一个RTT时延

二、FTP

1. 底层协议：TCP
2. 传输过程
   1. 建立控制连接->验证通过后建立数据连接（双向）->传输数据->关闭数据连接->关闭控制连接
3. 控制和数据连接
   1. 控制连接21号端口，持久
   2. 数据连接20端口，非持久，每传输一个web对象需要重新建立一个数据连接
4. 特点
   1. FTP是有状态的：服务器对每个活动用户会话的状态进行追踪，并保留；限制同时会话的总数。
   2. FTP控制信息带外传输，HTTP控制信息带内传输（请求头信息的控制信息）

三、邮件传输

1. 邮件服务进程端口号：25
2. 组成
   1. 用户代理：如outlook，基于web的QQ邮箱。用来编辑、查看邮件。
   2. 邮件服务器：只用来存和发邮件。
3. 邮件传输到读取的过程：
   1. 寄信方在用户代理写好邮件，通过SMTP或者HTTP传输邮件到寄信方邮件服务器
   2. 寄信方邮件服务器通过SMTP传输到收信方邮件服务器
   3. 收件方通过HTTP或POP3或IMAP获取从收件方邮件服务器获取邮件到收件方用户代理
4. SMTP
   1. 特点
      1. 持久连接
      2. 基于TCP
      3. SMTP不使用中间邮件服务器发送邮件， 即TCP 连接是从发送方到接收方的直接相连。如果接收方的邮件服务器没有开机，该邮件仍保留在发送方邮件服务器上，并在以后进行再次传送。邮件不会在某个中间邮件服务器停留。
      4. 把所有对象都放在一个报文里
   2. 编码方式
      1. 使用7为ASCII码编码方式，接收方需要编码解码
      2. HTTP没有该限制
5. MIME
   1. 为了解决SMTP的编码问题而出现的
   2. 用户->MIME->SMTP->SMTP->MIME->用户
6. POP3
   1. 无状态，功能简单
7. IMAP
   1. 有状态，功能多

四、DNS

1. 端口号：53号端口
2. 底层协议
   1. DNS服务器间进行域传输的时候用TCP 53
   2. 客户端查询DNS服务器时用 UDP 53
3. 提供服务
   1. 主机IP地址映射
   2. 主机别名
   3. 邮件服务器别名
   4. 负载均衡
4. 特点
   1. DNS通常于其他应用层协议共同使用（如HTTP，SMTP）
5. 查询方式
   1. 递归查询
      1. 负载重
   2. 迭代查询
      1. 我不知道它在哪儿，不过你可以问xxx‘
6. 域名解析过程

1.客户机提出[域名解析](http://www.so.com/s?q=%E5%9F%9F%E5%90%8D%E8%A7%A3%E6%9E%90&ie=utf-8&src=internal_wenda_recommend_text" \t "_blank)请求,并将该请求发送给本地的[域名服务器](http://www.so.com/s?q=%E5%9F%9F%E5%90%8D%E6%9C%8D%E5%8A%A1%E5%99%A8&ie=utf-8&src=internal_wenda_recommend_text" \t "_blank)。  
2.当本地的域名服务器收到请求后,就先查询本地的缓存,如果有该纪录项,则本地的域名服务器就直接把查询的结果返回。  
3.如果本地的缓存中没有该纪录,则本地域名服务器就直接把请求发给根域名服务器,然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址。  
4.本地服务器再向上一步返回的域名服务器发送请求,然后接受请求的服务器查询自己的缓存,如果没有该纪录,则返回相关的下级的域名服务器的地址。  
5.重复第四步,直到找到正确的纪录。  
6.本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时还将结果返回给客户机。

五、浏览器输入[www.baidu.com](http://www.baidu.com)

事件顺序

(1) 浏览器获取输入的域名www.baidu.com

(2) 浏览器向DNS请求解析www.baidu.com的IP地址

(3) 域名系统DNS解析出百度服务器的IP地址

(4) 浏览器与该服务器建立TCP连接(默认端口号80)

(5) 浏览器发出HTTP请求，请求百度首页

(6) 服务器通过HTTP响应把首页文件发送给浏览器

(7) TCP连接释放

(8) 浏览器将首页文件进行解析，并将Web页显示给用户。

标准回答：

1、客户端浏览器通过DNS解析到[www.baidu.com](http://www.baidu.com/" \t "_blank) 的IP地址220.181.27.48，通过这个IP地址找到客户端到服务器的路径。客户端浏览器发起一个HTTP会话到220.181.27.48，然后通过TCP进行封装数据包，输入到网络层。  
2、在客户端的传输层，把HTTP会话请求分成报文段，添加源和目的端口，如服务器使用80端口监听客户端的请求，客户端由系统随机选择一个端口如5000，与服务器进行交换，服务器把相应的请求返回给客户端的5000端口。然后使用IP层的IP地址查找目的端。  
3、客户端的网络层不用关心应用层或者传输层的东西，主要做的是通过查找路由表确定如何到达服务器，期间可能经过多个路由器，这些都是由路由器来完成的工作，我不作过多的描述，无非就是通过查找路由表决定通过那个路径到达服务器。  
4、客户端的链路层，包通过链路层发送到路由器，通过邻居协议查找给定IP地址的MAC地址，然后发送ARP请求查找目的地址，如果得到回应后就可以使用ARP的请求应答交换的IP数据包现在就可以传输了，然后发送IP数据包到达服务器的地址。

# 第三章

一、套接字

1. 定义: 同一台主机内应用层与运输层之间的接口, 进程通过套接字在网络上发送和接收报文。
2. 分类
   1. UDP套接字：目的IP地址，目的端口号。
   2. TCP套接字：源IP地址，源端口号，目的IP地址，目的端口号。
3. 多线程web服务器
   1. Web服务器对每个连接的客户机具有不同的套接字
   2. 非持久HTTP将为每个请求具有不同的套接字

二、UDP

1. UDP报文
   1. 组成：UDP首部+应用层报文
   2. 特点
      1. 面向报文，应用层交下来的报文，在添加首部后就向下交付给IP层。
      2. UDP 对应用层交下来的报文， 既不合并， 也不拆分， 而是保留这些报文的边界。
      3. 应用层交给 UDP 多长的报文， UDP 就照样发送， 即一次发送一个报文。
      4. 接收方 UDP 对 IP 层交上来的 UDP 用户数据报， 在去除首部后就原封不动地交付上层的应用进程， 一次交付一个完整的报文。
      5. 应用程序必须选择合适大小的报文。
   3. UDP首部
      1. 长度：8字节
      2. 组成：源端口号+目的端口号+长度+校验和（2+2+2+2）
2. UDP特点
   1. 无连接
   2. 不可靠，不一定按序到达
   3. 无拥塞控制
   4. UDP 支持一对一、一对多、多对一和多对多的交互通信。

三、TCP

1. TCP特点
   1. 点到点通信：一个发送端一个接受端。
   2. 面向连接的服务
   3. 提供拥塞控制
   4. 提供流量控制
   5. 可靠有序的服务
   6. 全双工
2. TCP报文
   1. 固定长度：20字节
   2. 重点组成
      1. 序号（4字节）：表示这个TCP报文的首字节的序号
      2. 确认号（4字节）：表示期待的下一个TCP报文的首字节的序号
      3. 窗口字段：用于流量控制，用于指示作为接受方，愿意接受的字  
         节数量。
      4. ACK：只有当ACK=1是确认号字段才有效，ACK=0是确认号字段无效
      5. SYN：SYN=1表示这是一个连接请求或者连接接受报文
      6. FIN：FIN=1表示该报文的发送端的数据已经发送完毕，请求释放连接。
3. 可靠传输
   1. 快速重传
4. 三次握手：  
    第一次握手：客户端发送syn包(syn=x)到服务器，并进入SYN\_SEND状态，等待服务器确认；  
    第二次握手：服务器收到syn包，必须确认客户的SYN（ack=x+1），同时自己也发送一个SYN包（syn=y），即SYN+ACK包，此时服务器进入SYN\_RECV状态；  
    第三次握手：客户端收到服务器的SYN＋ACK包，向服务器发送确认包ACK(ack=y+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。  
    握手过程中传送的包里不包含数据，三次握手完毕后，客户端与服务器才正式开始传送数据。理想状态下，TCP连接一旦建立，在通信双方中的任何一方主动关闭连接之前，TCP 连接都将被一直保持下去。
5. 四次挥手  
    与建立连接的“三次握手”类似，断开一个TCP连接则需要“四次握手”。  
    第一次挥手：主动关闭方发送一个FIN，用来关闭主动方到被动关闭方的数据传送，也就是主动关闭方告诉被动关闭方：我已经不 会再给你发数据了(当然，在fin包之前发送出去的数据，如果没有收到对应的ack确认报文，主动关闭方依然会重发这些数据)，但是，此时主动关闭方还可 以接受数据。  
    第二次挥手：被动关闭方收到FIN包后，发送一个ACK给对方，确认序号为收到序号+1（与SYN相同，一个FIN占用一个序号）。  
    第三次挥手：被动关闭方发送一个FIN，用来关闭被动关闭方到主动关闭方的数据传送，也就是告诉主动关闭方，我的数据也发送完了，不会再给你发数据了。  
    第四次挥手：主动关闭方收到FIN后，发送一个ACK给被动关闭方，确认序号为收到序号+1，至此，完成四次挥手。
6. 流量控制
   1. 定义：发送方不能发送太多、太快的数据让接收方缓冲区溢出
7. 拥塞控制
   1. 定义：太多的源发送太多太快的数据，使网络来不及处理
   2. 过程
      1. 当CongWin < ssthresh时， 发送者处于慢启动阶段,CongWin指数增长
      2. 当CongWin > ssthresh时， 发送者处于拥塞避免阶段, CongWin线性增长
      3. 当出现3个冗余确认时,发送者处于快速恢复阶段。 阈值ssthresh设置为CongWin/2， 且CongWin设置为ssthresh+3\*MSS
      4. 当超时发生时，阈值ssthresh设置为CongWin/2，并且CongWin设置为1 MSS.
   3. 慢启动：收到一个ACK确认congwin+1
   4. 拥塞避免：一个RTT后congwin+1

# 第四章

一．网络层的功能

1. 转发
   1. 定义：将分组从路由器的一个输入端口转移到另一个输出端口的本地动作
2. 选路
   1. 定义：指确认分组从源到目的端的端到端路径的网络范围动作
3. 连接建立
   1. 运输层
      1. TCP三次握手
   2. 网络层
      1. 指分组的源端到目的端所经过的所有路由器相互握手建立连接状态
   3. 因特网
      1. 因特网网络层不建立连接，使用IP协议

二、分组交换机

* 1. 链路层交换机
     1. 根据链路层字段做转发决定的分组交换机
  2. 路由器
     1. 根据网络层字段做转发决定的分组交换机

三、虚电路和数据报

1. 任何网络的网络层只一同虚电路或数据报之一的服务
2. 虚电路
   1. 特点：逻辑上的专用线路（电路交换是实际电路）
   2. 组成
      1. 源和目的之间的一条路进
      2. VC号
      3. 路由转发表中的表项
   3. 工作原理：
      1. 在源和目的之间创建一个VC，源向该VC发送带有VC号的分组； 每经过一台中间路由器， 用新的VC号代替原VC号：从VC号转发表获得，分组在每条链路上的VC号不同， 依此规则，直到目的地。
   4. 信息维护
      1. 只要该路由器创建新的VC，其转发表中就增加一项；
      2. 终止一个VC，其转发表中就删除对应项。
      3. 路由器必须为正在进行的连接维护连接状态信息，直到该连接释放
   5. 网络层和运输层连接建立的区别
      1. 运输层的连接建立：  
         只涉及两个端系统，相互协商通信并共同确定连接的参数。网络中的路由器并不知道该运输层连接。
      2. 网络层虚电路建立：  
         沿两个端系统之间路径上的路由器都要参与虚电路的建立，且每个路由器都完全知道所经过的所有虚电路。
3. 数据报网络
   1. 传输过程
      1. 路由器转发方法
         1. 根据到达分组的目的地址在转发表中查询，找到相应的输出链路接口，并将分组转发出去
         2. 最长前缀匹配
      2. 传发表
         1. 每台路由器有一张。 目的地址与链路接口的映射表。
         2. 路由器转发表只维持转发状态信息；
         3. 转发表由选路算法修改（ 1～5分钟更新）
         4. 虚电路网络转发表随虚电路的建立和拆除更新。
      3. 不同路径
         1. 分组使用目的主机地址转发相同源和目的地的分组可能采用不同的路径
4. 对比
   1. 虚电路网络
      1. 网络功能复杂，端系统设备简单。
   2. 数据报网络
      1. 网络层服务模型简单
      2. 端系统功能强大：许多复杂功能，由端系统在协议栈的高层实现，如按序传送、可靠数据传输、拥塞控制与DNS名字解析等；
      3. 带来的结果：
         1. 因特网服务模型提供的服务保证最少（可能没有！），对网络层的需求最小，使得互连使用各种不同链路层技术的网络变得更加容易。
         2. 许多应用都在位于网络边缘的主机（服务器）上实现。

四、IPV4

1. IPV4数据报
   1. 固定长度20字节
   2. 标识字段
      1. MF=0表示分片结束
      2. DF=0表示可以分片
   3. 片偏移字段
      1. 使分片后的分组重新组装
2. IP地址编址
   1. IP地址分类：ABCDE目前在使用的只有ABCD，D类地址用于特殊的用途



1. 私有IP地址
   1. 私有地址（Private address，也可称为专网地址）属于非注册地址，专门为组织机构内部使用，它是局域网范畴内的，私有IP禁止出现在Internet中，在ISP连接用户的地方，将来自于私有IP的流量全部都会阻止并丢掉。
   2. 随着私有IP网络的发展，为节省可分配的注册IP地址，有一组IP地址被拿出来专门用于私有IP网络，称为私有IP地址。
   3. 私有IP地址范围：  
      A: 10.0.0.0~10.255.255.255 即10.0.0.0/8  
      B:172.16.0.0~172.31.255.255即172.16.0.0/12  
      C:192.168.0.0~192.168.255.255 即192.168.0.0/16
2. 子网划分
   1. 子网掩码：主机部分全0，网络部分全1

五、一些其他的协议

1. DHCP
   1. 需要 IP 地址的主机在启动时就向 DHCP 服务器广播发送发现报文（ DHCPDISCOVER） ， 这时该主机就成为DHCP 客户。本地网络上所有主机都能收到此广播报文，但只有 DHCP服务器才回答此广播报文。DHCP 服务器先在其数据库中查找该计算机的配置信息。若找到，则返回找到的信息。若找不到，则从服务器的 IP地址池(address pool)中取一个地址分配给该计算机。DHCP服务器的回答报文叫做提供报文（ DHCPOFFER）
   2. 并不是每个网络上都有 DHCP 服务器， 这样会使DHCP 服务器的数量太多。 现在是每一个网络至少有一个 DHCP 中继代理(通常是一台路由器)， 它配置了DHCP 服务器的 IP 地址信息。当 DHCP 中继代理收到主机发送的发现报文后， 就以单播方式向 DHCP 服务器转发此报文， 并等待其回答。 收到 DHCP 服务器回答的提供报文后， DHCP 中继代理再将此提供报文发回给主机。
2. NAT：网络地址转换(NAT,Network AddressTranslation)属接入广域网(WAN)技术，是一种将私有（保留）地址转化为合法IP地址的转换技术，它被广泛应用于各种类型Internet接入方式和各种类型的网络中。原因很简单，NAT不仅完美地解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。借助于NAT，私有（保留）地址的"内部"网络通过[路由器](http://baike.baidu.com/view/1360.htm)发送[数据包](http://baike.baidu.com/view/25880.htm)时，[私有地址](http://baike.baidu.com/view/39496.htm)被转换成合法的IP地址，一个局域网只需使用少量IP地址（甚至是1个）即可实现私有地址网络内所有计算机与Internet的通信需求。
3. ICMP：是(Internet Control Message Protocol)Internet控制[报文](https://baike.so.com/doc/6200132-6413395.html)协议。它是[TCP/IP协议族](https://baike.so.com/doc/1956074-2070055.html)的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指[网络通](https://baike.so.com/doc/7558016-7832109.html)不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。
4. ARP：地址解析协议的工作原理

答:1：首先，每个主机都会在自己的ARP缓冲区中建立一个ARP列表，以表示IP地址和MAC地址之间的对应关系。  
2：当源主机要发送数据时，首先检查ARP列表中是否有对应IP地址的目的主机的MAC地址，如果有，则直接发送数据，如果没有，就向本网段的所有主机发送ARP数据包，该数据包包括的内容有：源主机 IP地址，源主机MAC地址，目的主机的IP 地址。  
3：当本网络的所有主机收到该ARP数据包时，首先检查数据包中的IP地址是否是自己的IP地址，如果不是，则忽略该数据包，如果是，则首先从数据包中取出源主机的IP和MAC地址写入到ARP列表中，如果已经存在，则覆盖，然后将自己的MAC地址写入ARP响应包中，告诉源主机自己是它想要找的MAC地址。  
4：源主机收到ARP响应包后。将目的主机的IP和MAC地址写入ARP列表，并利用此信息发送数据。如果源主机一直没有收到ARP响应数据包，表示ARP查询失败。  
广播发送ARP请求，单播发送ARP响应。

六、选路算法

RIP协议：底层是贝尔曼福特算法，它选择路由的度量标准（metric)是跳数，最大跳数是15跳，如果大于15跳，它就会丢弃数据包。

OSPF协议：底层是迪杰斯特拉算法，是链路状态路由选择协议，它选择路由的度量标准是带宽，延迟。