计算机网络总结

- 计算机网络概述
  - 发展历程
    - 第一阶段：从专用网络向互联网发展
    - 第二阶段：建成三级结构的Internet（有序）
    - 第三阶段：逐渐形成多层次ISP结构的Internet（无序）
  - 组成
    - 网络边缘：主机/端系统、接入网
    - 网络核心：分组交换机和链路构成的网状网络、向网络边缘的大量主机提供连通性
    - 如今：端-网-云
    - 网络协议=语法+语义+同步
  - 性能指标
    - 注：在计算机领域如存储，，在通信领域，
    - 速率 = （b/s, bps,...）
    - 带宽 bandwidth 数字信道能传送的**最高数据率** （kb/s, Mb/s=b/s）
    - 吞吐量(每秒实际传输的比特数)=
    - 时延/延迟=发送时延+传播时延+处理时延+排队时延
      - 从结点进入传输介质的时间—发送时延=
        - 我们能提高是仅是发送速率，提高链路带宽可以降低发送时延
      - 在信道中传播需要的时间—传播时延=
      - 主机或路由器在收到分组时必要的处理时间—处理时延
      - 结点缓存队列中分组排队的时间—排队时延
    - 时延带宽积=（b, Kb）
    - 信道利用率——并非越高越好，当信道利用率越大时，该信道的时延也会迅速增加
    - 网络利用率=全网络的信道利用率的加权平均
  - 分类
    - 直连网络
    - 交换网络
      - 交换技术的发展
        - 电路交换
          - 方式：面向连接，经过建立连接、通话、释放连接的三个步骤
          - 缺点：传输效率低，数据有突发性可能会导致资源浪费
        - 报文转发

        - 方式：以存储转发的形式将整个报文发值目的端
      - 分组交换
        - 方式：以存储转发的形式将分组逐跳转发至目的端
        - 优点：高效、灵活、迅速、可靠
        - 缺点：时延（处理时延和排队时延）、附加信息开销
    - 互联网
- 计算机网络体系结构和参考模型
  - 理论模型：OSI参考模型
    - 物理层（PDU:bits）：原始比特传输
    - 数据链路层（PDU:帧）：可靠的点对点数据帧传输
    - 网络层（PDU:IP分组）：网络互连的关键，分组交换，主机到主机的通信（尽力而为的交付）
      - 网络结点只有物理层+数据链路层+网络层
    - 传输层（PDU：传输层报文/消息）：端到端的数据传输
    - 会话层：进程管理、断点续发、双/单/半双工
    - 表示层：加解密、数据格式化
    - 应用层（PDU:数据）
  - 实际架构：TCP/IP体系结构
    - 子网层
    - IP层：实现主机到主机的通信
    - TCP/UDP层：端到端的协议
    - 应用层
  - 实际架构：细腰结构——IP为细腰
    - IP over Everything —— IP应用到各式各样的网络上
    - Everything over IP —— 各式各样的应用承载在IP上
- 直连网络（广播网络，可扩展性差）
  - 信道编码（物理层）
    - 基带信号编码
      - 非差分编码：0、1固定编码，无关联
      - 双相码：相位相关，有关联
        - 曼彻斯特码：一个周期的方波（Z走向）表示1，反向方波为0
        - 差分曼彻斯特码：采用差分码的概念，相邻周期的方波反相表示1，同向表示0
    - 数字信号调制
      - 幅度键控
      - 频移键控

        - 相移键控
    - 香农公式——信道容量与计算
        -
            - C—信道容量(bps)；W—信道带宽(Hz)；S—信号平均功率；N—高斯白噪声功率；S/N—信噪比（常表示为SNR(dB)，）
        - 增加信道宽带W并不能无限增大C，因为W↑，N∝W↑
- 组帧（链路层）
    - 面向字节的协议——把每一帧看成一个字节集
        - 起始标记法：用特定字符表示帧的开始和结束
        - 字节计数法：帧中字节数放在首部的一个字段中
    - 面向比特的协议
        - 用01111110（标志字段）作为开始和结束的标志
        - 比特填充法：未加上标志字段的比特流处理，只要发现5个连续的1就立即填上一个0
- 错误检测（链路层）
    - 基本思想：在数据帧中加入冗余信息来确定是否存在差错，**只能做到无差错接受**
    - 处理分为 重传 和 纠错
    - 奇偶校验
        - 单个位奇偶校验
        - 二维奇偶校验
    - 校验和 Checksum
        - 常用的：发送方数据分为16位序列相加（有进位，最高位进位回卷到最低位），结果取反码；接收方将所有16位序列相加，全为1则认为无差错
        - 特点：冗余少，检测能力较弱
    - 循环冗余校验CRC
        - 发送方：对于数据M，k+1比特的多项式C，实际发送的数据为
        - 接收方：校验是否成立：不是则判定出错，是判定无措（不一定无错）
- 可靠传输（链路层）
    - 基本机制——确认和超时的组合
    - 自动请求重发 ARQ
        - 停等算法 stop and wait
            - 发送方传输一帧之后在传输下一阵之前等待一个ACK；如果在某段时间之后ACK没有到达则发送方超时，重发原始帧
            - 增加1bit序列号的停等算法——每帧（序列号值）交替使用
            - 缺点：链路上只允许一个未确认的帧，可能不能保持管道满载
        - 滑动窗口算法 sliding window
            - 增加单位时间传输数据帧的数目，尽量保持管道满载

- 特点：可靠传输、高效传输、按序传送、流量控制
- 要求
- 发送方：能缓存SWS个帧；收到ACK则右移更新LAR，若窗口大小允许，发送新的帧，更新LFS；为每帧设置定时器，若超时则重传该帧
- 接收方：在接收窗口接收该帧；将收到的最大连续数据帧序号作为ACK回复
- 当数据帧丢失
  - ① 回退N机制回复丢包：接收方只对连续收到的数据帧回复ACK；发送方在超时后重传ACK+1到LFS之间的数据帧
  - ② 选择确认机制恢复丢包：接收方对每个接收的数据帧进行确认；发送方根据确认信息进行重传；效率高但实现复杂

- 介质访问控制（链路层）
  - 媒体共享技术
    - 静态划分信道——信道复用技术（强调公平性）
      - 频分复用FDM（共享带宽）：所有用户在相同的时间占用各自的带宽资源
      - 时分复用TDM：将时间划分为一段段等长的时分复用帧TDM帧，每个用户在TDM帧中有固定序号的时隙（同步时分复用）
      - 统计时分复用STDM：按需动态分配时隙（异步时分复用）
      - 波分复用WDM
      - 码分复用CDM：码分多址CDMA
        - 发送比特1（m bit码片序列），比特0（m bit码片序列的反码）
        - 码片是互相正交的，
    - 动态媒体接入控制，多点接入（强调自组织和带宽利用率）
      - 随机接入
        - ALOHA （信道利用率约18%）
          - 若碰撞结点立即以概率p重传，以概率1-p等待一个帧传输时间
        - 时隙ALOHA（信道利用率约37%）
          - 结点只在时隙开始传输帧，为避免一个帧快传完了时被别的结点发送的帧碰撞
        - CSMA 载波侦听多点接入
          - 非持续CSMA
          - 1-坚持CSMA
          - p-坚持CSMA
        - CSMA/CD 带碰撞检测的CSMA（有线网络）
          - 1-坚持CSMA+碰撞检测
          - 原则：帧必须足够长，最小帧长为2τ*带宽

        - 端到端往返时延2τ为碰撞窗口/争用期，结点至多经过2τ（δ→0）可知是否有碰撞
      - CSMA/CA 带碰撞避免的CSMA（无线局域网）
        - 非持续CSMA+碰撞避免
    - 受控接入
  - 网络类型
    - 广域网WAN（交换技术）
    - 城域网MAN
    - 局域网LAN（广播技术）
      - 特点：覆盖范围小、高传输速率、低误码率、拓扑形状多、传输媒介有双绞线光纤等
      - 代表：以太网Ethernet，令牌环网
        - 以太网组成：传输介质，网络配适器，中继设备（中继器，集线器），交换设备（网桥，交换机）
        - 以太网地址（冒号相隔的6个数）：硬件地址/MAC地址/网卡的物理地址
        - 以太网提供的是不可靠的交付
        - 以太网扩展
          - 在物理层：光纤，多个Hub
          - 在链路层：网桥，二层交换机，演变成交换网络不再是广播域
    - 个域网PAN
- 交换网络（单播，可扩展性强但线性扩展；不支持多种异构网络）
  - 网桥
    - 在链路层扩展局域网，使各网段成为隔离开的碰撞域
    - 工作方式，基于转发数据库FBD/转发表
      - 过滤
      - 转发
    - 缺点：规模不能太大
  - 数据帧转发
    - FDB存储目的MAC到网桥端口的映射关系
      - （结点位置自学习）网桥每收到一个新的数据帧，记录源MAC地址和该网桥输入端口的映射关系
    - 对每个数据帧在FDB中做查找，假设数据帧来自端口
      - 若存在对应端口号且与接收端口一致丢弃
      - 若存在对应端口号但不同于接收端口，则从该端口将数据转发（单播）
      - 如果FDB不存在对应条目映射，将数据包从所有端口转发（广播）
  - 生成树协议
    - 提升网络健壮性（避免环路）：带环的图→生成树

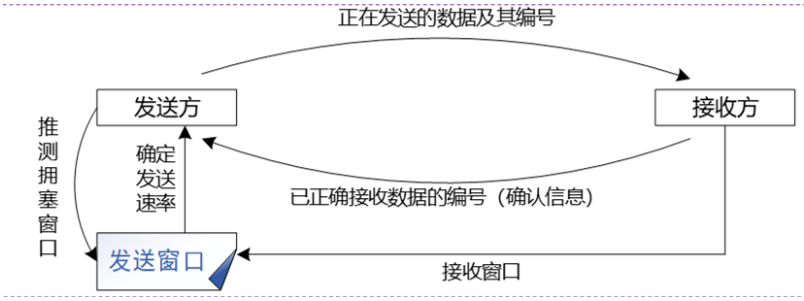
        - 算法思想
            - 选择一个网桥作为生成树的根，如最小序号的网桥（根网桥总在它所有的端口上转发分组）
            - 其他结点确定**根端口**，以到根路径最短的端口作为根端口
            - 为每个局域网选**指派网桥**（指派网桥负责向根网桥转发帧）
            - 网桥之间交换配置消息
                - 本网桥认定的根网桥标志符
                - 从本网桥到根网桥的距离
                - 自己的网桥标志符
            - 每个网桥收到配置消息时
                - 若优于自己的消息，更新自己的配置，距离加1，向消息接收端口之外的其他所有端口转发
                - 否则丢弃
    - 二层交换机（多接口网桥）
        - 用交换机扩展局域网
    - 虚拟局域网（VLAN）
        - 只是局域网提供的一种服务
- 网络互联（基于IP，连接各种异构网络，大规模路由）
    - 网络协议IP（中间转发设备功能简单，成本低，扩展性强）
        - IP向上提供最基本的、简单的、灵活的数据报传输服务（无连接、尽最大努力交付）
        - 互联结点是路由器/网关→转发（动作、局部）+路由选择（决策、全局）
            - 路由器总是有两个或两个以上的IP地址，每一个接口都有一个不同网络号的IP地址
        - IP的关键是建立可扩展的异构互连机制
        - IP地址（网络号+主机号）
            - 分类
                - A类，B类，C类为单播地址
                    - A类：0+7位网络号（1.~126.）+24位主机号
                        - 网络号全0和全1的IP地址保留
                    - B类：10+14位网络号（128.1~191.255）+16位主机号
                    - C类：110+21位网络号(192.0.1~223.255.255)+8位主机号
                - D类为组播地址
                    - D类：1110+多播地址
                - E类为保留地址
                    - E类：1111+保留
            - 特点

        - 为两级的层次结构
        - 实际标识的是一个结点和一个链路的接口
        - 同一个网络上的结点IP地址的网络号必须一样
        - 所有分配到的网络号的网络都是平等的
    - 路由选择协议：RIP、OSPF、BGP
    - IP分组转发——查找路由表根据目的网络地址确定下一跳路由器
        - FIB路由表：网络号与下一跳地址的映射关系
    - 地址解析协议ARP（IP地址与硬件地址映射）（网络层）
        - 在ARP Cache中查是否有目的地址的IP地址，有则查出相应的硬件地址；否则在**局域网内广播**ARP请求询问目的地址的硬件地址。目的地址收到ARP请求后单播回复自己的硬件地址
    - IP报文格式
    - IP分片（连接异构网络）
        - 每片的长度必须是8的倍数，每个分段都要有IP数据包头（注意标识Identification，偏移offset，标志位flag，长度length，校验和checksum）
            - 标识：计数器，按序+1
            - 标志位：MF=1表示后面还有分片，MF=0表示这是最后一个；DF=0才允许分片（DF：Don't Fragment）
            - 偏移量：采用8字节为偏移单位，即偏移量的1表示8字节
        - 缺点
            - 不能充分利用网络资源
            - 端到端性能差，丢了一个其余皆丢弃
            - 可被利用来生成DoS攻击
- 划分子网
    - 基本思想：IP地址两级变三级（网络号+子网号+主机号）（子网号从主机号中取，至少借2位，至少留2位主机号）
    - 子网掩码：子网掩码&IP地址=子网的网络地址
    - 路由表FIB的变化：增加了子网掩码
        - 用本结点的各个网络子网掩码与目的主机IP地址相与，看是否相匹配
- 构造超网
    - 无分类域间路由CIDR：网络号长度不限制（网络前缀+主机号→IP地址/网络前缀位数）
    - 路由聚合/构成超网
    - 最长前缀匹配：从匹配成功结果中选择具有最长网络前缀的路由
- 网络控制与诊断—ICMP协议
    - 是IP层协议，但封装在IP数据报中
    - 报文类型

        - ICMP差错报告报文（IP分组传输中发生错误，ICMP发送差错报告通知**源主机**）
        - ICMP询问报文（管理员对某些网络问题进行判断可使用查询报文）
    - 应用
        - PING测试主机之间连通性：询问报文
        - Tracerout/tracert跟踪分组从源点到终点的路径：ICMP超时报文
        - 路径MTU发现：源主机向目的主机连续发送多个长度不同的数据报文
- IP路由协议
    - 路由器工作原理——路由生成、分组转发
    - 路由协议基本概念
        - 静态路由选择——集中式，非自适应路由选择
        - 动态路由选择——分布式，自适应路由选择
        - Internet采用两层路由选择协议：域内路由+域间路由
            - IGP内部网关协议：RIP、OSPF（性能目标导向）
            - EGP外部网关协议：BGP-4（策略和经济目标）
    - 内部网关协议RIP（UDP）
        - 基于距离向量算法
        - 范围：仅与相邻路由器交换路由信息
        - 消息：当前路由器所知道的全部信息（自己的路由表）（初识化每个路由表只知道一跳以内的路由信息）
        - 更新原则：**短优先，新优先**。定期或者触发交换路由信息
        - 缺点
            - 可扩展性不高，16即为无穷大
            - 不能带丢失率高的网络中使用
            - 不能动态地使用时延、负载等为依据选择路由
            - 开销较大
            - 收敛速度较慢
    - 内部网关协议OSPF（IP）
        - 基于链路状态，每个节点建立完整的网络图
        - 范围：向本自治系统内所有路由器发送消息（可靠机制）
        - 消息：只是与本路由器相邻的路由器之间链路状态
            - 链路状态：接口的IP地址、掩码+链路类型+开销+序列号+生存期（后面两个用于可靠扩散）
        - 更新：各个结点根据链路状态数据库单独计算到其他结点的最短路径。当链路状态发生变化了路由器用**洪泛法**向校园路由器发送变动信息
        - 分组类型
            - Hello分组

        - 数据库描述分组
        - 链路状态请求分组
        - 链路状态更新分组
        - 链路状态确认分组
      - 问题：存在短暂环路
    - 外部网关协议BGP（TCP）
      - BGP发言人：BGP边界路由器
      - 基于路径向量
  - IP多播
    - 多播地址：D类1110+多播地址（前五位不使用）
    - 实现的协议
      - 网际组管理协议IGMP（IP）：让连接在本地局域网的多播路由器知道自己所在的局域网上是否有主机
        - 主机加入多播组
        - 多播路由器确定本地组成员关系
      - 多播路由选择协议：找到以源主机为根节点的多播转发树
  - 虚拟专用网VPN
    - 采用IP隧道技术连接使用私有地址通信的内部网络，隧道两端是公有地址
  - 网络地址转换NAT
    - 负责私有地址与全局地址之间的翻译
    - NAT路由器：至少有一个有效的全局IP地址
- 端到端传输
  - 传输层协议概述
    - 实现应用进程之间端到端的通信（end-to-end）
    - 作用
      - 多路分解和复用（UDP、TCP）——<IP, 16位端口号>
        - 三类端口：熟知端口（0~1023）、登记端口（1024~49151）、客户端端口（49152~65535）
      - 连接管理
      - 可靠传输
      - 流量控制
      - 拥塞控制
  - 用户数据报协议 UDP
    - 应用：IP电话，视频直播（允许丢包，但时延敏感）
    - 特点：

    - 无连接，无需建立连接，无需维护状态）
    - 端到端的、尽力而为的数据报传输服务，不保证可靠传输
    - 面向报文，比IP数据报多了端口和差错检测的功能
    - 没有拥塞控制
    - 最基本的传输层协议，可按上层需求定制
  - 报文：伪首部+首部+数据（校验和是对于所有的内容）
- 传输控制协议 TCP



  - 特点
    - 端到端的、可靠的、面向连接的有序字节流服务
    - 点对点的双工通信，会将字节流写入发送/接收缓冲区
    - 多路分解与复用
    - 可靠传输
    - 流量控制
    - 拥塞控制
  - 滑动窗口算法是TCP的核心
    - 可靠和有序传输
    - 流量控制
    - 自适应重传
    - 拥塞控制
  - 报文段格式
    - 源端口和目的端口
    - 该报文段的数据流的第一个序号
    - 确认号：期待下一次报文段的数据的第一个序号
    - 6位标志字段
      - URG 紧急
      - ACK 确认，置1时确认号字段才有效
      - PSH 托送，置1表示发送方有push操作
      - RST 复位，置1表示TCP连接出现大差错
      - SYN 同步，置1表示这是请求/接受报文，SYN=1,ACK=0表示连接请求，SYN=1,ACK=1表示连接接受

        - FIN 终止，置1表示释放连接
    - 接收窗口：指明接收窗口大小
    - 校验和：计算整个TCP首部、数据、伪首部
    - 选项：最大报文段长度MSS，窗口扩大，时间戳，选择确认
- 多路复用（源、目的端口）
- 连接管理（SYN、FIN、ACK、序号、确认号）
    - 方式：客户-服务器方式（建立是非对称的）
    - 连接建立——三次握手
        - 客户向服务端应答第三个确认报文段
            - 为防止已经失效的连接请求报文段突然又传送到服务端产生错误
            - 已经失效 情况①：第一次握手确实丢失导致重新建立连接
            - 已经失效 情况②：第一次握手延迟到达导致重新建立连接
        - 连接释放
            - 任何一方都可以主动关闭连接（FIN报文），另一端可以继续发送数据
                - 客户最后等待2MSL时间的原因
                    - 确保客户发送的最后一个ACK报文能够到达服务端
                    - 防止已经失效的连接报文段出现在本连接/下个新连接中，2MSL可以使本连接持续时间内产生所有报文段从网络中消失
            - 任何一方都可以发送RST报文关闭连接
                - 请求连接不存在的端口
                - 某段TCP出现了混乱情况
                - 某段TCP发现连接另一端TCP空闲时间超长
- 滑动窗口
    - 发送窗口
        - 发送窗口上限值=Min(接收窗口，CongestionWindow)
        - 有效窗口=发送窗口上限值-（最后发送字节-最后被确认的字节）
    - 接收窗口
        - 根据本地缓存情况，确定发送窗口大小并通知发送方，实现流量控制
    - 选择确认SACK：确认收到的不连续的数据块的边界
    - 数据有序传递
    - 流量控制（接收窗口、选项）
        - 目的：防止快发送给慢接收造成接收崩溃，缓冲区溢出
        - 原理
            - 接收方确认接收窗口大小并通知发送方
            - 发送方确定发送窗口上限值

- 有效窗口大于0才能发更多数据
- 还必须保证发送缓冲区不溢出

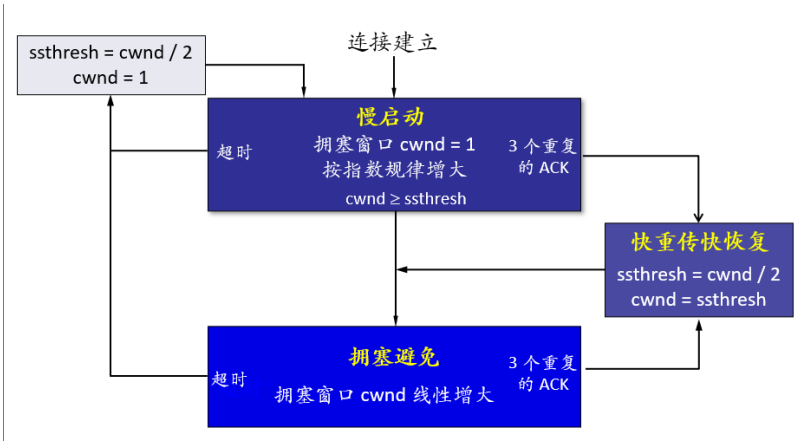
- 若发送方无法知道接收窗口为0
  - 情况：当接收方没有数据向发送方发送→陷入死锁
  - 解决：发送方主动定期探测。TCP每个连接设置一个持续计时器，当收到对方0窗口长度通知式启动计时器
- 接收窗口大小
  - 长肥管道现象
    - 具有较大时延带宽积的传输路径，但因为发送窗口小，TCP传输的数据少，传输路径很空
  - 最大值应能让发送方保持管道满载
  - 影响因素
    - 与时延带宽积相匹配（应该为多少）
    - 受缓存空间的限制（可以为多少）

- 触发传输
  - 触发机制——如何决定传输一个报文段
    - 空间驱动，缓存区存放数量达到MSS最大报文段长度
    - 业务驱动，进程要求，push操作
    - 时间驱动，计时器到齐
  - 当有窗口大小限制时
    - 一味地利用任何大小的发送窗口会导致糊涂窗口综合症
      - 发送方传送小报文段（效率低），接收方打开小窗口
    - 解决
      - 接收方等待一段时间再向发送端发确认报文段
      - Nagle算法（效率和公平性的平衡）
        - 引入一个定时器，接收方自计时
        - 窗口允许就发送满载报文段
        - 窗口不允许如果当前没有传输中的报文段也可以发一个小报文段
        - 如果有传输的报文段，发送方等到ACK到达之后才能发送下一个报文段
- 丢失恢复，可靠传输（ACK、确认号、选项）
  - （粗粒度）TCP每个报文段都有一个计时器，阈值RTO超时重传时间
    - 自适应重传
      - 原始算法：维持一个RTT的平均运行值ERTT
        - 更新：ERTT=（1-α）ERTT+α*样本值实际RTT
        - RTO=2*ERTT

- karn/Partridge算法
  - 每次超时重传一个报文段即停止计算RTT样本值，不重传才重新计算
  - 让TCP对超时的反应别太主动
- Jacobson/Karels算法
  - RTO=ERTT+4*RTT变化

- （更快些，辅助）快速重传
  - 重复确认触发重传
  - 接收方：当报文段到达，立即回复ACK，即使序号已被确认
  - 发送方：收到一个重复ACK就知道接收方必定收到乱序的报文段，前面分组可能丢失。收到一定数量的重复ACK立即触发重传

- 拥塞控制（协议未体现）
  - 网络拥塞的代价
    - 分组到达速率接近链路容量时，分组将经历巨大的排队时延
    - 发送方必须执行重传以补偿因为缓存溢出而丢弃的分组
    - 发送方在遇到大时延时，可能进行不必要的重传，从而引起路由器及其链路资源的浪费
    - 当一个分组沿一条路径传输过程中被丢弃时，每个上游路由器用于转发该分组而使用的传输容量最终被浪费掉了
  - 网络负载过大网络性能会下降，超过阈值急剧下降。大量未送达分组，大量重传分组
  - 端到端的拥塞控制（TCP √）
    - 端设备通过丢包，延时变化推测拥塞情况
    - 优点：中间设备设计简单
    - 缺点：当推测策略差时网络利用率低
    - TCP拥塞控制



    - 采用改变发送窗口大小来控制发送速率，MaxWindow=Min(CWND, 接收窗口大小)
    - 拥塞检测

- 报文段超时
- 收到多个重复的ACK
- 速率（拥塞窗口）调整
  - 当判断网络拥塞时，减慢发送速率
  - 当收到非重复的（新的）ACK时增大发送速率
  - 慢启动
    - CWND从很小的初始值开始快速增大（1个MSS数值），探测网络的负责能力
    - 慢启动门限：ssthresh
  - 拥塞避免——加性增/乘性减AIMD
    - TCP：增x+1，减x/2
    - ssthresh=max(cwnd/2,2)
- 快恢复——在快重传之后
  - ssthresh减小为CWND/2
  - 新CWND=ssthresh
  - 执行拥塞避免（AIMD）
  - 若出现超时CWND=1
- 网络辅助的拥塞控制
  - 网络设备对端系统提供反馈
  - 优点：更准确，网络利用率高
  - 缺点：中间设备设计复杂；每个传输流维护一个状态，扩展性差
  - 中间设备对TCP性能的影响
    - Buffer大小：过大会引起BufferBloat的问题（过多数据包导致了数据包延迟，降低了总吞吐量）
    - 队列调度：FIFO，公平排队
    - 丢弃策略：队尾丢弃，随机早检测（RED）

- 网络应用
  - 基本应用模型
    - CC模型（用户-用户）
      - 例如：（端服务系统）电子邮件，VPN，隧道通信；
        - 特点：部署可控、成本可控、数据可控、用户友好
      - 例如（中心服务系统）电商，即时通信应用
        - 特点：高成本、管理难、数据泄露
    - CS模型（用户-服务器）
      - 例如：Web，DNS，DHCP，SNMP（等加代理）

- 域名系统DNS
  - 将主机名/域名映射为IP地址，运行在UDP之上
  - 工作方式：客户/服务器方式
  - 层次化域名空间
  - 分布式、层次化的域名空间存储和管理
    - 根服务器 全球13个
    - 顶级域名服务器
    - 权威服务器
    - 本地域名服务器（递归服务器）
- 万维网
  - 工作方式：客户/服务器方式
  - 用URL唯一标识Web上的各种文档
    - <协议>://<主机/域名>:<端口>/<路径>
  - 基于HTTP实现Web客户程序与服务器程序之间的交互
    - HTTP面向事务的应用层协议，无连接，无状态
    - HTTP报文：请求和响应报文
- 电子邮件
  - 用户代理，邮件服务器
  - 发送邮件的协议：SMTP协议
    - TCP连接建立，邮件传送，TCP连接释放
  - 读取邮件的协议
    - 邮局协议版本3 POP3
    - 互联网报文存取协议 IMAP
  - 邮件信息格式
    - 互联网文本报文格式
    - 通用互联网邮件扩充 MIME
- 文件传送协议
  - 工作方式：客户/服务器方式
  - 文件传送协议FTP（基于TCP）
    - 减少不同系统下处理文件的不兼容性
    - 一个主进程（接受新请求）+多个从属进程（TCP连接，处理单个请求）
  - 简单文件传送协议TFTP（基于UDP）
- 远程终端协议 Telnet
  - 工作方式：客户/服务器方式
  - 用网络虚拟终端NVT屏蔽不同操作系统的差异

    - 动态主机配置协议DHCP
        - 工作方式：客户/服务器方式
    - 简单网络管理协议 SNMP
        - 工作方式：客户/服务器方式
        - 监视网络性能、检测分析网络差错、配置网络设备
        - 组成：SNMP，管理信息结构SMI，管理信息库MIB
    - 应用进程跨越网络的通信
- 网络安全
- IPv6