计算机网络复习

一、绪论

Internet 基本概念

- 什么是 Internet（P1）：当前全球最大的、开放的、由众多网络相互连接而成的特定互连网，它采用 TCP/IP 协议族作为通信的规则，其前身是美国的 ARPANET
- 组成视角（P1）
  - 边缘部分：所有连接在互联网上的主机（端系统）构成，用户直接使用
  - 核心部分：大量通信链路和分组交换机（包括路由器和链路层交换机）构成，为边缘部分提供服务（连通性和交换）
- 服务视角（P1）
  - 根据基础设施向分布式应用程序提供的服务
  - 向 APP 提供从源点到目的地可信/最大努力的数据传输服务、保证时延和吞吐量
- 协议（P1）：协议定义了在两个或多个通信实体之间交换报文的格式和顺序，以及报文发送和/或接受一条保温或其他事件所采取的动作。
- 网络边缘（P2）：主机（端系统）
  - 客户/服务器模型
  - P2P 模型
- 网络接入（家庭、公司、无线）（P2）
  - 家庭接入：（P2）
    - 数字用户线（DSL）：利用电话公司现有的本地电话基础设施
    - 电缆：利用有线电视公司现有的优先电视基础设施
    - 光纤到户（FTTH）：光纤路径接入
    - 拨号、卫星
  - 公司（和家庭）接入：（P2）
    - 以太网：使用双绞铜线与一台以太网交换机相连，10Mbs、100Mbps、1Gbps、10Gbps 以太网
    - WiFi：IEEE 802.11
  - 广域无线接入：（P2）
    - WiFi、3G（分组交换广域无线因特网接入）、4G、5G、LTE
- 网络核心：互联因特网端系统的分组交换机和链路构成的网状网络（P3）
  - 分组交换、电路交换
  - 两个关键的网络层功能：路由和转发
- P3 的习题！
- 电路交换（P3）：预留了端系统间通信沿路径所需要的资源
  - 频分复用（FDM）：每条电路连续得到部分带宽
  - 时分复用（TDM）：每条电路在时隙中周期性得到所有带宽
  - Kbps=1000bit/s；Mbps=1000000bit/s
  - 带宽、交换能力、预留资源、有保证的表现、连接建立和取消
- 分组交换（P3）：存储转发、每一个包使用所有链路带宽
  - 核心技术：存储转发（交换机先存储整个分组，然后向输出链路转发）
  - N 条速率均为 R 的链路组成的路径，端到端时延是$N\frac{L}{R}$。*（计算）*

- 不预留端系统之间通信沿路径所需要的资源，每一个包使用所有链路带宽

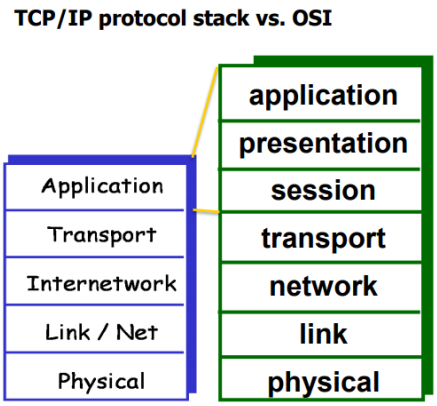
- 虚电路（P4）
  - 电路交换+分组交换

	电路交换	数据报分组交换	虚电路分组交换
传输通路	专用	非专用	非专用
连续性	连续传输	分组传输	分组传输
带宽	固定	动态使用	动态使用
路由	固定	动态	固定
时延	实时（只有呼叫建立时延）	分组传输时延	分组传输时延+呼叫建立时延
扩展性	差（接入用户有上限）	好（用户数量可动态扩充）	较好（用户数量动态，由拥塞控制来保证服务质量）

  - 路由器或主要通路是固定的、资源共享、拥塞控制、资源可被预留、连接建立和取消

协议体系结构（P4）

- 多层协议体系结构的必要性（P4）
  - 显式的体系结构结构允许复杂系统各层之间的保持结构上独立和相邻层之间灵活的调用关系
  - 模块化简化了体系结构维护和更新
- OSI 模型（P4）：开放系统互联模型，由 ISO 提出，是一个七层协议体系结构
  - 七层：应用层、表示层、会话层、运输层、网络层、数据链路层、物理层
- TCP/IP 模型（P6）：由全球互联网使用的五层协议体系结构
  - 五层：应用层、 运输层、网络层、链路层、 物理层
- 层次之间的关系及各层对应功能（P5）
  - 层次之间的关系（P5）
    - 每一层是所需求的通信功能的一个子集（subset）
    - 每一层依赖紧邻的下一个低层协议（rely on）
    - 每一层向紧邻的高层协议提供服务（provide）
    - 一层的变化不应导致其它层次的变化（changes not require changes）
  - 各层功能
    - 应用层：网络应用程序及它们的应用层协议存留的地方、应用层分组叫报文
    - 运输层：因特网的运输层在应用程序端点之间传送应用层报文、运输层分组叫报文段
    - 网络层：负责将数据报从一台主机移动到另一台主机、网络层分组叫数据报
    - 链路层：将网络层交下来的数据报组装成帧，在两个相邻节点间的链路上传送帧、链路层分组叫做帧
    - 物理层：将帧中的一个一个比特从一个结点移动到下一个结点、物理层所传数据的单位是比特
  - 对应关系：



二、链路层

—>PDU（P6）：协议数据单元，在传输系统的每一层，控制信息会被加入到用户数据当中来简化传输，从而形成一个协议数据单元。

链路层服务：（P7）：分帧、媒介访问控制、可靠交付、差错检测与纠正

- 分帧：将网络层数据报用链路层帧封装起来
  - 首部和尾部的作用：帧定界
- 媒介访问控制（MAC）：共享多址介质的协调访问，帧头部的 MAC 地址用于识别源和目的地，全称 Media Access Control Address
- 可靠交付：用于易于产生高差错率的链路，例如无线链路
- 差错检测和纠正
  - 发送控制器在帧首部设置差错校验比特、流控制
  - 接受控制器执行差错检测、流控制
  - 奇偶校验、因特网检验和的循环冗余校验
- *可靠性技术：流控制、检错/纠错
- *流控制方法：停止-等待、滑动窗口（成功发送/接收、尚未发送/接收 ACK、滑动窗口三大部分）

局域网：

- 局域网的构成（P8）：
  - 拓扑结构（P8）：总线型、环形、树形、星形
  - 传输媒介（P8-9）：双绞铜线、同轴电缆、光纤
- 网桥（P9）：
  - 网桥的作用：拓展单一 LAN，提供连接到其他 LANs（局域网）/WANs（广域网）的方式，任务是接受入链路层帧并将它们转发到出链路
  - 工作原理：对收到的帧根据其 MAC 帧的目的地址进行转发和过滤（网桥根据 MAC 地址转发，路由器根据网络地址如 IP 地址转发）
  - 网桥的要求（P9）：存储转发、透明、即插即用、自学习
    - 存储转发：读取在一个 LAN（局域网）中传送的帧、检查帧的首部 MAC 地址、有选择地存储 MAC 地址发往其它 LAN 的帧；使用第二个 LAN 的 MAC 协议，重新传输每个帧

- 透明：子网中的主机和路由器不知道网桥的存在
- 即插即用、自学习：网桥不需要提前设置

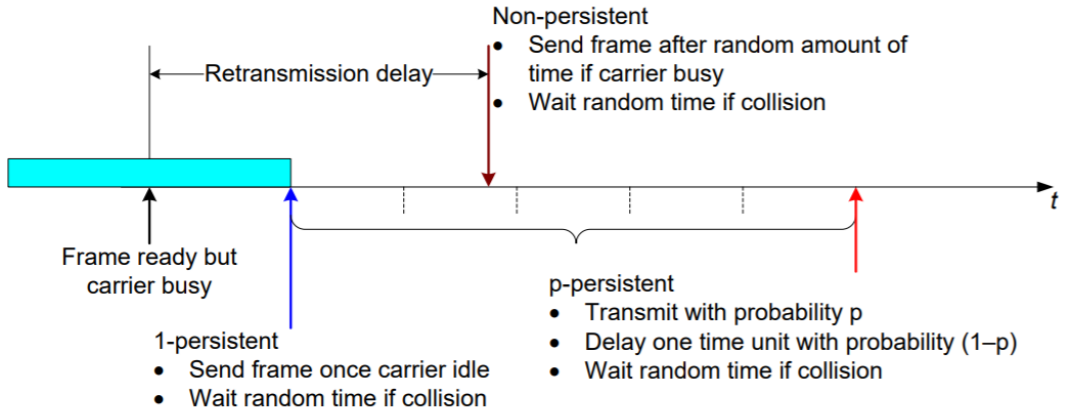
- 路由机制：网桥自动生成、更新转发表（P9）
  - 转发表（交换机表）：
    - MAC 地址
    - 通往该 MAC 地址的交换机接口
    - 表项放置在表中的时间
  - 地址学习：P10 的习题！
    - 交换机表初始为空
    - 每个接口接收到的每一个入帧，在交换机表中存储：
      - 该帧源地址字段中的 MAC 地址
      - 该帧到达的接口
      - 当前时间
    - 如果老化期过后，交换机没有接收到以该地址作为源地址的帧，就在表中删除这个地址
  - 生成树算法——使得每一个 LAN 到根网桥的路径代价和最小（习题 P11!）
    - 选根网桥
    - 对每一个网桥选根网口（各个端口到根网桥的代价最小）
    - 为每一个 LAN 选择指定的网桥（如果只有一个网桥连接到某 LAN，那么该网桥就是该 LAN 的指定网桥，否则到根网桥花费最小的网桥被选为该 LAN 的指定网桥）
    - 根网桥的网口和所有其它指定的网口设置为转发状态，其它设置为阻塞状态
  - 路由发现机制（P12）
    - 对一个目的地每一个站点发送一个单路由广播帧，帧访问每一个 LAN 一次并最终抵达目的地
    - 目的地向源地址回送全路由广播帧，源收集所有路由并选择最好的

- 二三层交换机，基本工作机理和比较：
  - Bridge 网桥：连接 LANs（局域网）：转发+地址自学习，共享媒介
  - Hub 集线器：像一个 Repeater，物理上是星形的，逻辑上是总线型的，每一个传输会占用所有带宽，所有其他站点都会收到；如果两个同时传就会发生碰撞；
  - Layer 2 Switch：连接主机或 LANs：网桥的功能（链路层的装置、透明、即插即用、自学习）+无碰撞。P14 习题！
  - Layer 3 Switch：使用到路由器功能的 Switch（交换机），填充了 packet-forwarding 的功能，在局域网上工作
  - Router：路由器，在公网或者局域网都能工作
  - 例如十个流，网桥的话每一个流只能占到 1/10，总共最多只能达到 100%，但是交换机总共能够达到 1000%的流量，集线器的话一个流会占用集线器所有资源。（P338/P23-25）
  - 现代交换机是全双工的
- 令牌环：基本工作原理（P15）图示 P16!
  - 当一个结点接收到令牌时。仅当它有一些帧要发送时，它才持有这个令牌，然后发送最大数目的帧数，最后往下一个节点转发令牌；否则它立即向下一个节点转发该令牌。

- 帧要绕一圈回到发送该帧的结点以后被吸收，在传送结束以后站点重新插入一个新的令牌

以太网：

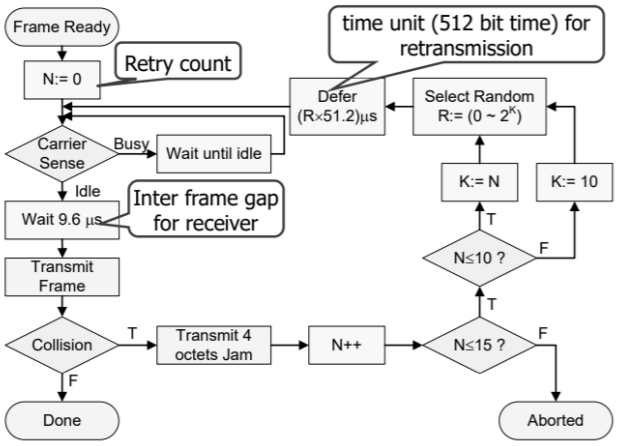
- 媒体接入控制：CSMA 的基本思想（P16-17）
  - CSMA：载波侦听多路访问
    - 传前听
    - 空闲传，忙时等一个合理时间，再听
    - 没 ACK 重传
  - 非持续的 CSMA：busy 后 idle 时会等待随机时延
  - 1-持续的 CSMA：busy 后 idle 时会立即重传
  - p-持续的 CSMA：空闲繁忙都要以概率 p 传输，概率 1-p 不传输



- CSMA/CD 的工作原理（P17）
  - 工作步骤
    - 步骤 1：如果媒介空闲，传输；否则前往步骤 2
    - 步骤 2：如果忙，等待空闲，然后立即传输
    - 步骤 3：如果遇到碰撞，发送 jam 信号，中止
    - 步骤 4：发送完 jam 信号以后等待一个随机时间量，然后返回步骤 2
  - 冲突检测的方式（P18）
    - 在基带总线上，碰撞产生的信号电压远高于单站信号，即如果电缆信号大于单站信号，则检测到碰撞。（因为信号会衰减，所以需要 jam 信号加强冲突，使其他设备易于检测）
    - 在星型拓扑上，超过一个端口活跃，则检测到碰撞
  - 冲突检测与传播/传输时延的关系
    - 最坏情况下为了确保发送站点在传输时能检测到可能存在的冲突，数据帧的传输时延至少要等于信号传播时延的 2 倍，即 RTT（或者总现的端到端往返传播时延）
  - 二进制指数退避算法：（P18）
    - 该帧经历了一连串 n 次碰撞后，结点随即从{0，1，2，…，2^n-1}中选择一个 K 值，等待 K*512bit（以太网争用期时间为 512 比特时间，51.2μs=RTT）时间，n 最大值不超过 10，超过 10 以后 k 不再增大而一直等于 10，最大只能到 15，若到 16 则丢弃该帧

- 最小帧长和最大范围：（P29）
  - 最小帧长：如果帧太短，发送方不知道该帧发生了碰撞，规定最短帧长为 64 字节即 512bit，对 10Mbit/s 的以太网，发送 512bit 需要 51.2μs，也即 RTT
  - 最大范围：最大范围不得超过网络距离约为 5km

IEEE 802.3 Transmission Algorithm



- IEEE 802.3 以太网规约
  - 以太网媒介
    - 向网络层提供无连接服务、不可靠服务
    - 同轴电缆、双绞线和光纤
  - 以太网帧格式（P19）

前同步码 (8Bytes)	目的地址 (6Bytes)	源地址 (6Bytes)	类型 (2Bytes)	数据 (46~1500Bytes)	CRC (4Bytes)

无线局域网

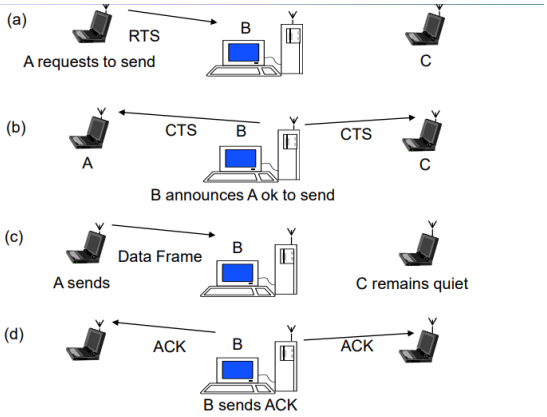
- 无线局域网的概念和应用
  - 概念：（P19）
    - 基站：一般连接到有线网络，负责向与之关联的无线主机发送和接收数据
    - 无线链路：一般用于连接移动终端和基站
    - 平滑切换（交付 handoff）：移动终端在移动切换基站的时候基站必须清楚这种变化
    - SNR 信噪比：收到的信号和噪声强度的相对测量
    - BER 比特差错率：接收方收到的有错传输比特与 SNR 之比
  - 和优先链路的区别：递减的信号强度、来自其他源的干扰、多径传播、鲁棒性和安全（P20）

—>移动自组织网络（Ad hoc）是一种自治、多跳网络，整个网络没有固定的基础设施，能够在不能利用或者不便利用现有网络基础设施(如基站、AP)的情况下，提供终端之间的相互通信。

  - 带来的问题：（P21）

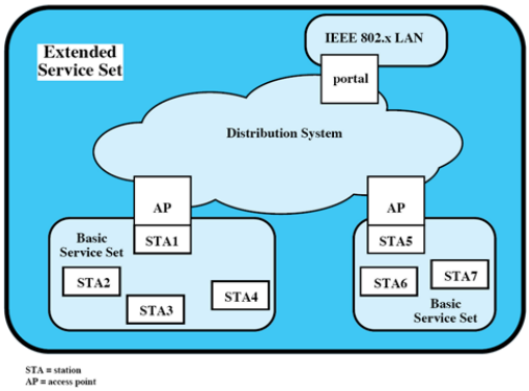
- 隐藏终端问题
- 暴露终端问题
- 信号衰减问题

- 处理隐藏终端问题：4 帧交换，使用 RTS 短请求发送控制帧和 CTS 短允许发送控制帧：流程：Src: RTS，Dest: CTS, Src: Data, Dest: ACK（P21）



  - RTS：指示传输 DATA 帧和确认帧需要的总时间，用以警告所有不在源点范围内的站点此刻正在交换数据
  - CTS：给发送方明确的发送许可，也指示其他站点在预约期内不要发送
  - 但是 RTS 和 CTS 交换仅用于为长数据帧预约信道，在实际中，默认的 RTS 门限值大于最大帧长值，因而对于所有发送的 DATA 帧，RTS/CTS 序列都被跳过。

- IEEE 802.11 体系结构（P21）
  - 基本概念☆☆☆
    - AP：接入点。802.11 无线以太网标准中 BSS 星型拓扑的中央基站叫做接入点 AP
    - BSS：基本服务集。802.11 标准规定无线局域网的最小构件，一个基本服务集包括一个基站和若干移动站
    - SSID：服务集标识符
    - ESS：拓展服务集：由分配系统 DS 相连的多个基本服务集 BSS
    - DS：分配系统：用以连接一个基本服务集 BSS 的集合和不同的局域网构成一个拓展服务集 ESS 的系统，使拓展服务集 ESS 对上层的表现像一个基本服务集 BSS。DS 可以是一个交换机、有线网络或无线网络。
    - 分布式协调功能：DCF，用于传输异步数据，优先级最低
    - 点协调功能：PCF，集中式控制，用于发送实时数据，优先级仅次于控制帧
  - 体系结构图



- 媒体接入控制 CSMA/CA（P23）
- 3 层优先级：控制帧>点协调功能>分布式协调功能（P22）
  - SIFS：短帧间间隔，最高优先级，用于控制帧，如 ACK、LLC 逻辑链路控制子层（负责识别网络层协议，然后对它们进行封装。LLC 报头告诉数据链路层一旦帧被接收到时，应当对数据包做何处理）、PDU（协议数据单元）、轮询（Poll response）、CTS 帧等
  - PIFS：中等长度的帧间间隔，对应 PCF 轮询，用于使得 AP 等待 PIFS 而不是 DIFS 时间以访问信道，让 AP 总比普通节点具有更高的访问信道的优先级。
  - DIFS：分布式帧间间隔：最长的帧间间隔，对应 DCF，用于节点在开始发送数据之前监测信道是否空闲。如果信道已经空闲，则节点仍需等待 DIFS 段时间才开始发送数据；而如果在 DIFS 时间段内任一时刻信道被监测为忙，则节点不得不推迟它的数据发送。
  - DIFS=SIFS+2*slotTime
  - PIFS=SIFS+slotTime
- 与以太网的 CSMA/CD 相比较
  - 相同：都有 CSMA 即载波侦听多路访问，每个站点在传输之前侦听信道，并且一旦侦听到该信道忙就抑制传输
  - 不同：
    - 802.11 使用碰撞避免（CA），使用链路层确认/重传（ARQ）方案
      - 802.11 不使用碰撞检测的原因有：
        - 检测碰撞的能力要求站点具有同时发送和接收的能力，制造具有检测碰撞能力的硬件代价大
        - 适配器会因为隐藏终端问题和衰减问题而无法监测到所有的碰撞。
    - 以太网使用碰撞检测（CD）、不使用链路层确认机制
- 802.11b/g 频段及传输速率
  - 802.11b：频率范围 2.4~2.4835GHz，数据率最高为 11Mbps
  - 802.11a：频率范围 5.1~5.8GHz，数据率最高为 54Mbps
  - 802.11g：频率范围 2.4~2.485GHz，数据率最高为 54Mbps

网络性能分析

- 指标：
  - 网络时延：Delay，结点的时延、端到端时延
  - 丢包：到达一个满队列的路由器的分组将会被路由器丢弃
  - 吞吐量：比特从发送方到接收方传输的速率 bits/unit per time
    - 瞬时吞吐量：某一特定时间点比特传播速率（bps）
    - 平均吞吐量：某一段时间内比特传播的平均速率（bps）
      - e.g.：若该文件有 F 比特，主机 B 接收到所有 F 比特用去 T 秒，则文件传送的平均吞吐量为 F/T bps
- 四种时延：
  - 处理时延：检查比特差错、检查分组首部和决定将该分组导向何处
  - 排队时延：分组在输出链路上等待传输的时延，取决于路由器拥塞的程度
    - 估计排队时延：流量强度$\rho = \frac{L*a}{R}$，其中 a 是分组到达队列的平均速率（单位是 pkt/s），R 是传输速率，即从队列中推出比特的速率，假定所有分组由 L 比特

组成。

- 传输时延（ Transmission Delay）：将所有分组的比特推（传输）向链路所需要的时间
  - R：带宽（bps）
  - L：分组长度（bits）
  - 传输时延=L/R
- 传播时延（Propogation Delay）：从链路的起点到另一路由器传播所需要的时间，取决于链路的物理媒体
  - 传播时延=两台路由器的距离/传播速率

- 传输媒介利用率分析
  - 媒介利用率$U=\frac{帧的传输时间}{总时间（主要考虑传输+传播时间）}$
  - Point-to-point link
    - 定义：1：一般化的帧传输时间；a：端到端的传播时延；N：站点的个数
    - 最大利用率：$U=\frac{1}{1+a}$（无论 a 与 1 谁大谁小）
  - ALOHA：
    - 原理：节点一有帧就传输，if ACK 可以，if not ACK（噪声或碰撞），立即以概率 p 重传帧或者以概率 1-p 在另一个帧时间等待；
    - 效率：共有 N 个节点，一个给定节点成功传输一次的概率是$p(1-p)^{N-1}$，纯 ALOHA 协议的最大效率为$\frac{1}{2e}$。
  - Slotted ALOHA：
    - 原理：节点有帧就等待下一个时隙开始传输整个帧，if not ACK，在时隙结束之前检测到碰撞，以概率 p 在后续的每一个时隙当中重传帧，直到成功传输。帧有 L 比特，帧总是以信道的全部速率（R bps）发送，时间被划分为长度为 L/R 的帧。
    - 效率：一个给定节点成功传输一次的概率是$p(1-p)^{N-1}$，N 个活跃结点时，任意一个结点成功传送的概率是$Np(1-p)^{N-1}$，取 N->∞，得到时隙 ALOHA 协议的最大效率是$\frac{1}{e}$。
  - 令牌环：$U=\begin{cases}\frac{1}{1+a/N}, a<1\\ \frac{1}{a+a/N}, a>1\end{cases}$
  - CSMA/CD（ p-persistent ）的简单性能模型：$U=\frac{1}{1+4.44a}$

三、网络层

网络层服务：路由选择、转发、建立连接

- 路由选择：分组从发送方流向接收方的时候，网络层必须决定这些分组所采用的路由或路径

- 转发：当一个分组到达路由器的一条输入链路时，路由器必须将该分组移动到适当的输出链路
- 建立连接（虚电路）：某些网络层体系结构如 ATM、帧中继、MPLS 等，要求从源到目的地沿着所选择的路径彼此握手，以便在给定源到目的地连接中的网络层数据分组能够开始流动之前建立起状态。

*—>QoS：Quality of service，服务质量，指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力，是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术

*—>信令报文：端系统向网络发送指示虚电路启动与终止的报文，以及路由器之间传递的用于建立虚电路的报文

*—>信令协议：用以交换信令报文的协议

- 分组交换网络，基本思想

  对比：虚电路网络（ATM）和数据报网络（IP 网络）
  - 虚电路网络：仅在网络层提供连接服务的计算机网络，为每一个数据报流建立连接、终止连接、每一个数据报携带 VC 识别号，每一个在源-目的结点的路径上的交换机需要保持一个“状态”，路径上的资源需要分配给虚电路网络，笨拙的端系统。
  - 数据报网络：仅在网络层提供无连接服务的计算机网络，不需要建立连接，交换机不需要保持“状态”，报文转发用的是目的主机的地址，数据报可能走不同的路径，聪明的端系统。

- 分组交换网络中路由
  - 性能评估指标：
    - 最小跳数：
    - 最小代价：最小时延、最大吞吐量决定最小代价
  - 路由信息的更新方式
    - 本地的、相邻交换机、所有网络中的交换机
    - 周期性更新、依赖主要交换机和链路的更新、固定不变的

- 路由算法（P35 开始）
  - 集中式路由（P35）：固定的路径、最小代价算法、依赖网络拓扑中的主要改变而重新设置，Fixed
  - 分布式路由：（P36）
    - 洪泛：广播包，虽然很鲁棒，终点可达，所有交换机都被访问了，但是会形成很多副本，包也会转圈圈形成广播风暴
    - 随机行走：随机选择一个出口，对强连通网络有用，但是不是最优的，可能走环路。
    - 自适应路由//动态路由策略与算法：
  - 最小代价路由算法及其性能分析——一定要做题！！！！
    - Bellman-Ford（分布式、局部信息）-RIP，距离向量 DV 算法
      - 关键思想：1、2、……、k 条链路最小
      - 收敛较慢，且在收敛的时候会遇到路由选择环路
      - 问题：好消息传播得快，坏消息传播得慢的无穷计数问题：解决方案是增加毒性逆转（善意的谎言，z 到 x 经过 y，但是 z 告诉 y 它到 x

距离无穷大），但不能处理三个或更多节点的环路

- Dijkstra Algorithm（集中式、全局信息）-OSPF，链路状态 LS 算法
  - 关键思想：单源最短路的迪杰斯特拉算法
  - 实现一个要求 O(|N||E|)个报文的 O(N^2)算法
  - 问题：路由选择振荡：解决方案是非同步运行算法且链路代价更新随机化
- 第一、二、三代互联网路由算法之间的对比和改进

- 链路代价的计算

- 自治系统与路由方式
  - AS：自治系统，由单一 ISP 或大型组织管理的一组路由器和网络。
  - AS 由一组通常处在相同管理控制下的路由器组成，相同的 AS 当中全部运行同样的路由选择算法。
  - 有 AS 号
  - AS 的区域边界路由器：负责为流向该区域以外的分组提供路由选择
  - IRP(IGP) 与 ERP（EGP）概念
    - IRP(IGP)，Interior Gateway Protocol 内部网关协议，是在一个自治网络内网关（主机和路由器）间交换路由信息的协议。包括 RIP（DV），OSPF（LS），IGRP
    - ERP(EGP)，Exterior Gateway Protocol 外部网关协议，是一个在自治系统网络中两个邻近的网关主机间交换路由信息的协议。包括 BGP
  - 内部路由协议
    - 距离向量协议（RIP）与链路状态协议（OSPF）
    - RIP：Bellman-Ford 算法，距离向量，跳：经过的子网数量
    - OSPF：Dijkstra 算法，链路状态。优点：安全、多条费用相同的路径、对单薄、组播路由选择的综合支持、支持大范围内的层次式路由
      - IR：Internal Router：AS 内每一个区域内部，不和任何外面区域相连的路由器
      - ABR：Area Border Router：AS 内每一个区域边界的路由器
      - BR：Backbone Router，骨干路由，跑 OSPF 算法的路由器
      - ASB：AS Boundry Router，边界路由，跑 BGP 算法的路由器
    - 路由结构图与路由表的生成（P46）
  - BGP：边界网关协议子网使用 BGP 来向因特网的其余部分告知它的存在
    - 端口号固定 179，携带 AS-PATH 信息防止路由循环，可达性、CIDR
    - BGP 的功能：
      - 从相邻 AS 处获得子网可达性信息。
      - 向本 AS 内部所有路由器传播这些可达性信息。
      - 基于可达性信息和 AS 策略，决定到达子网的“好”路由
      - iBGP：在同一个 AS 当中两台路由器之间的 BGP 会话
      - eBGP：跨越两个 AS 的 BGP 会话
    - 基本报文类型和工作方式
      - OPEN、UPDATE、KEEP-ALIVE、NOTIFICATION
      - 工作方式:
        - 获知邻居：OPEN、KEEP-ALIVE 交换
        - 邻居可达性：互传 KEEP-ALIVE 和 UPDATE

- 网络可达性，一更新就 UPDATE

- IP 协议
  - IP 基本原理
    异构网络环境下，internet 协议的工作过程
  - 协议
    - 协议基本原语与相关参数
      - MTU：最大传送单元，一个链路层帧能承载的最大数据量
    - IPv4 首部格式（各字段含义和变化）
      - 注意 IP 是首部校验和
    - IP 地址的分类法，A、B、C、D 类划分标准和地址范围
      - A：0 开始，范围 1.x.x.x 到 126.x.x.x，划分是 1 位，7 位，24 位
      - B：10 开始，范围 128.0.x.x 到 191.255.x.x，划分是 2 位，14 位，16 位
      - C：110 开始，范围 192.0.0.x 到 223.255.255.x，划分是 3 位，21 位，8 位
      - D：1110 开始，代表组播地址
    - 子网划分/聚集
      - 子网掩码，左边的是子网地址，右边的是主机地址
    - CIDR 表达
      - CIDR：无类别域间路由选择，是因特网的地址分配策略
  - IPv6
    - 和 IPv4 的异同
      - 看习题!!! 习题有！记下来!!
    - 优点：扩充的地址空间、高效的 40 字节首部、校验和被移除从而减少了处理时延、流标签与优先级、支持资源分配、增加寻址灵活性……
    - 缺点：切换成本高、转变需要时间……

- NAT 原理及优缺点
  - NAT，网络地址转换，为内部和外部通信启用不同的 IP 地址集，提供内部因特网和更广域的因特网的交互
  - 优点：行使防火墙的功能、允许一个机构使用更多的内部 IP 地址，隔离 IP 更改
  - 缺点：端口号用于进程编址而非主机编址，妨碍 P2P 应用程序
- ARP 地址解析原理和流程
  - Address Resolution Protocol
  - 在局域网上，ARP 用一个主机/路由器的 IP 地址来获得它的 MAC 地址，过程见 P57，大概就是先查 ARP 表，没有就广播，收到以后返回 ARP 单播
- DHCP 动态地址获取的过程
  - DHCP：动态主机配置协议，即插即用
  - DHCP-Discover->DHCP-Offer->选择一个发包含 Server IP 的 DHCP-Request ->DHCP-ACK，最后客户根据 DHCP-ACK 配置完成所有自己的参数
  - 断开的时候发送 DHCP-Realease 报文
- ICMP：用于发送出错和控制信息，Ping 和 traceroute 的实现原理
  - Internet Control Message Protocol
  - PING：Echo Request->Echo Reply
  - Traceroute：关键是 TTL

*—>MTU：最大传输单元（Maximum Transmission Unit，MTU）是指一种通信协议的某一层上面所能通过的最大数据包大小（以字节为单位）

- Mobile IP
  - 概念：
    - 移动终端（节点）：可能将其连接点从一个网络更改为另一个网络的主机
    - 通信节点：向移动节点发送寻址数据包的主机
    - 归属代理：归属网络上维护已注册移动节点列表的节点。
    - 外部代理：帮助移动节点传送数据报的外部网络上的路由器
    - 隧道：包括 IP 的 IP 封装、最小封装和通用路由封装，它存在于本地代理和移动节点的关心地址之间。归属代理接收发送到移动节点的数据包，并通过 IP 隧道将数据包转发给外部代理。
  - 三角路由原理：……这个我觉得我应该理解了，就是通信节点发给移动终端的数据报要先经过归属代理和 IP 隧道发给外部代理，再给移动终端，然后移动终端通过外部代理直接响应通信节点这样

- IP 组播
  - 组播地址：D 类 IPv4 地址，224 开头及往上；组播 MAC 地址
  - 组播模型：主机将 IP 数据报编址到一个多播组，路由器将多播数据报转发给已加入该组播组的主机。
  - 组播组管理：IGMP 因特网组管理协议，主机和路由器在一个本地网络中交换多播组信息
    - 主机：发送报告给路由器以加入/退出一个组播组，但是主机不需要显式指出自己退出组播组，或者也可以由路由器 query 一下主机 Report 回应已经加入的组播组集合。
    - 路由器：固定时间间隔 Query 一下主机，希望继续留在组播组当中的主机需要回复这个 Query，否则会被路由器退出组播组

*—>软状态：在一个软状态协议当中，状态如果未被显式更新，则通过超时时间被删除

- 组播路由机制（Shared-tree, Source-based tree）
  - Shared-Tree：被所有组成员共享的生成树，MST（Steinner Tree），不实际使用
  - Source-based Tree：每一个不同的发送者都有自己的生成树，单源最短路，Dijkstra 算法，可能会包括那些并不在管辖主机不在组播组内的路由器；生成方法是看一下包的来源是不是上游，是就向下游广播，否则丢掉这个包，最后反向一下给到源点就是生成树了

四、传输层

网络层：主机之间逻辑连接；传输层：进程之间逻辑连接

- 传输层服务：
  - 编址：进程识别号、传输实体识别号、主机地址
  - 复用
    - 多路复用：在源主机从不同套接字收集数据块，并为每一个数据块封装上首部信息从而生成报文段，然后将报文段传递到网络层的工作
    - 多路分解：将运输层报文段中的数据交付到正确的套接字的工作（目的主机，

数据-交付->套接字）

- 流控制：发送方不会以太快的传输速度导致接收方的缓冲区溢出，用发送和接收窗口完成
- 面向连接：连接建立和终止（状态图会画了吗！）
- 可靠传输

- 可靠传输要解决的 7 个问题
  - 按序交付：序列号标识顺序
  - 重传策略：超时计时器 >RTT
  - 副本检测：以序列号区分，要求序列号空间足够大
  - 流量控制
    - 滑动窗口机制的设计：发送方的发送窗口不能超过接收方给出的接收窗口的数值，TCP 窗口单位是字节
    - 信用量窗口
    - TCP 复合的窗口管理方式
      - 基于接收方缓冲区
      - 基本机制和工作流程
  - 连接建立：三次握手
    - 为什么不两次握手？防止两次握手的情况下，滞后的 SYN 报文段带来错误
  - 连接终止：四次挥手
    - 为什么不两次挥手？因为可能在 CLOSE WAIT 状态的服务器向客户发送了最后一个数据段，并且这个数据段比服务器发送给客户的 FIN 早到达，结果客户关闭了 TCP 连接，导致最后一个数据段的数据丢失。
    - 可靠网络与不可靠网络下连接建立与终止的算法对比
    - 三次握手的流程图与其必要性
  - 崩溃恢复：
    - 计时器：当在(timeout)*(number of retries)超过以后仍然没有收到 ACK，就关闭连接
    - RST：重启的一方发送 RST i 用以回复任何到达的序列号为 i 的段，另一方可以确认 RST i 然后关闭连接

- 传输层协议：UDP，TCP
- UDP：无连接、尽最大努力交付、面向报文、无拥塞控制、首部开销小
- TCP 协议
  - 基本服务
    - 面向连接的运输层协议、只能有两个端点、可靠交付、全双工通信、面向字节流
  - 协议首部格式
    - 注意：IP 校验和只校验 20 字节的 IP 报头；TCP 校验和计算首部和数据两个部分，TCP 首部最小长度 20 字节，典型的 IP 数据报首部 20 字节
  - TCP 拥塞控制算法
    - RTT 报文段的往返时间（Round Trip Time）
    - RTO 超时重传时间，应该略大于 RTT
    - 时延 RTT 估计算法

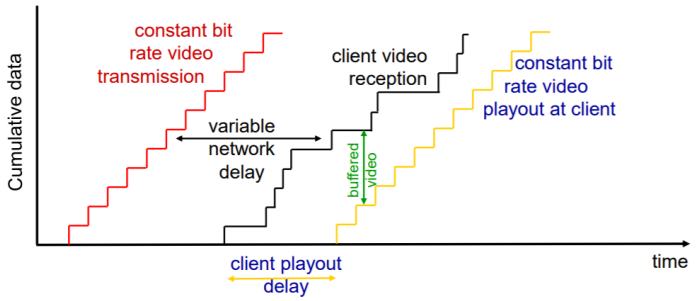
- 平均算法 $\mathrm{ARTT(k+1)}=\frac{1}{k+1}\sum_{i=1}^{k+1}RTT(i)$ or $\mathrm{ARTT(k+1)}=\frac{k}{k+1}ARTT(k)+\frac{1}{k+1}RTT(i)$
- 指数平均算法：$\mathrm{SRTT(k+1)}=\alpha*\mathrm{SRTT(k)}+(1-\alpha)*\mathrm{RTT(k+1)}=(1-\alpha)*\mathrm{RTT(k+1)}+\alpha(1-\alpha)*\mathrm{RTT(k)}+\cdots+\alpha^{k}(1-\alpha)*\mathrm{RTT(1)}$

◆ RTO 计时器管理算法看 P83!!!我没法打字了，有点麻烦，找个题目做一下？？

◆ Jacobson's Reno
- 慢启动
- 拥塞避免：窗口增长基本算法（AIMD）：加性增、乘性减
- 快重传：连续收到三个（对同一数据的）重复确认
- 快恢复

- 数据网络中的拥塞控制
  - 拥塞问题：通过网络传输的数据包数接近网络的数据包处理能力。
  - 网络拥塞和性能指标?
  - 拥塞情况下网络吞吐率特征
  - 拥塞控制方式
    - 抑制分组：在拥塞结点为每一个丢弃的分组产生，发送到源结点
    - 反压（逐跳）：从拥塞结点逐跳向源点反压，要求每一跳抑制传送速率
    - 警告位（在 Frame Relay 网络中）：在包头设置警告位警告后向（BECN，假定拥塞会爆发）或者前向（FECN,假定拥塞会逐渐积累）的端系统，让端系统减少提供的负载
    - 拥塞窗口（TCP）：将数据报的超时视为网络拥塞的一个信号
    - 随机早期丢弃（RED）：Random Early Discard，路由器在缓存变得很满之前随机丢弃一些包
    - 流量整形：通过平均数据速率将突发的流量整形成有固定速率的流量
      - 漏桶机制：输入空的时候什么都不做，输出速率则固定，像一个漏桶
      - 令牌桶机制：作业题有一题！会分析哦

- 网络服务质量



知道这个图怎么分析!

  - 不同类型应用对 QoS 要求
    - 弹性流量和非弹性流量：非弹性应用不会在拥挤的情况下减少需求，拒绝(流量)资源太少的服务请求。
    - 非弹性流量：实时音视频、存储音视频、交互游戏需要非弹性的流量

- 弹性流量：文件传输、E-mail、网络文件、即时通讯是需要弹性流量
- 综合服务体系（ISA）与区分服务（DS）
  - 基本思想和差别
    - ISA：将可区分的 IP 数据包流与一个流关联。定义在两个层级上：分别是不同的服务类别和每个类别内特定的流。
      - 资源预留：路由器维护每个会话分配的资源的状态信息。
      - RSVP：多媒体应用的 IP 信令协议（定义见上）。
        - Path 从源往下，存储每一跳路由器的路径状态，保留了上一跳路由器的地址，也可能收集 Qos 信息
        - Resv 从每一个 Receiver 往上
      - 软状态：一个软状态可以被 Path msg 或者 Resv msg 创建并周期性更新
      - RSVP 中资源是不断取最大值的过程，即 Reservation Merging
      - 缺点：高代价（要维持软状态）、复杂（结构复杂，需要支持这个复杂功能的路由器）、定义的服务级别很少而不灵活。
    - DS:
      - 优点：
        - 提供简单、易于实现、低开销的机制
        - 基于性能而区分的网络服务的支持范围
        - 网络核心功能简单，边缘路由器功能相对复杂
      - PHB：Per-Hop Behavior 每跳行为，对每一个 DS 域中的路由器，定义应用于具有特定 DS 的数据包的策略和优先级、导致不同可观察转发性能的结果。
        - 加速型转发：很难实现
        - 确保型转发：简单，尽最大努力服务、RED 随即早期丢弃算法
  - 区分服务中 SLA 的概念
    - Service Level Agreement：是关于网络服务供应商和客户间的一份合同，其中定义了服务类型、服务性能参数、流量配置文件等。
    - 边缘路由器的功能：分类、流量计、标记、整形、丢弃流速率过高的包
    - 内部路由器的功能：对 DS 代码点（code point）的一致解释、分类、队列管理

五、网络安全

- 被动攻击与主动攻击的概念
  - 被动攻击：窃听传送、流量分析；很难发现，但可以防止
  - 主动攻击：乔装（中间人）攻击、重放攻击、修改报文、拒绝服务攻击 Denial of Service；难以防止，但可检测到
- 加密、报文鉴别码 (Message Authentic Code (MAC) 经过特定算法后产生的一小段报文，检查某段报文的完整性，以及作身份验证)、数字签名
- 对称加密：发送者和接收者的密钥相同
  - 加密机制的组成元素：明文、加密算法、密钥、密文、解密算法
  - 对加密机制的要求
    - 强加密算法
    - 发送方和接收方必须安全地获取密钥-密钥分发

- 常见加密算法（一般了解）——看 PPT95 页开始，这里有的讲不清楚
  - 替代：
    - 凯撒密码：替代一位
    - 单表密码：随机的一个映射表
    - 维吉尼亚密码：一张 26*26 的映射表
  - 转置
    - 篱笆密码：将明文竖着写，然后横着读
    - 行列密码……
- 非对称加密算法：RSA 算法（重点）！
  - 公钥和私钥，用公钥加密，私钥解密
  - 密钥生成过程
    - 两个大素数 p、q
    - n=pq
    - z=(p-1)(q-1)
    - 选 e<N，且 gcd(e,n)=1
    - 求 d，使得 ed mod z=1
    - 公钥 K_B^+=（n,e），私钥 K_B^-=（n,d）
  - RSA 加密和解密计算过程
    - 密文 c=m^e mod n
    - 解密 m=c^d mod n
- 报文鉴别与散列函数
  - 报文鉴别码：MAC
  - 报文鉴别的可能方式和要求
    - 密码认证：CBC-MAC
    - 哈希认证：MD5、SHA-1 等
    - 要求：
      - 可操作性：任意输入长度、固定输出长度、容易计算
      - 安全性：单向的（X 找 Y，Y 难找 X）、弱碰撞的（X1 难找 X2）、强碰撞的（X1≠X2 时 MAX(X1)=MAC(X2)的概率很低）
- 公钥系统
  - 公钥加密机制的组成元素
    - 明文、加密算法、公钥和私钥、密文、解密算法
  - 加密和数字签名
    - 发送方数字签名，让接收方确认确实是发送方发送了报文
  - Diffie-Hellman 密钥交换过程：看 PPT102 页
    - 大概：
      - 首先有一个很大的 P 让全世界知道，然后有一个 $g \in Z_p^*$使得任意 $a \in Z_p^*$存在 k∈Z，a=g^k(mod P)
      - A 选 X∈1~P-1，计算 g^X(mod P)送 B
      - B 选 Y∈1~P-1，计算 g^Y(mod P)送 A
      - AB 都可以计算出 g^XY(mod P)，作为密钥
  - 数字证书的概念和构造，CA
    - CA：认证中心，用以证实一个实体的真实身份、生成一个把身份和实体的公钥绑定起来的证书

        - 证书：包含这个公钥和公钥所有者全局唯一的身份标识信息
    - 安全电子邮件系统设计：会画图!!
        - 安全性、发送方鉴别和报文完整性：自己的密钥、对方的公钥、新的对称密钥
- SSL（TLS）与 IPSEC
    - 所处的层次：
        - SSL：Secure Sockets Layer；TLS：Transport Layer Security，传输层
        - IPSec：IPSecurity，网络层
    - 基本功能与协议结构
        - SSL：
            - 四轮握手：建立安全能力、服务器鉴别与密钥交换、客户机鉴别与密钥交换、相互确认
            - 为什么要有不重数？假设 Trudy 第二天监听 Alice 和 Bob 之间的所有消息，Trudy 与 Bob 建立 TCP 连接，发送完全相同的记录序列，Bob(有可能是 Amazon)认为 Alice 要购买同样的东西。
            - 解决方案：Bob 为每个连接发送不同的随机值。这将导致加密密钥在两天内有所不同。
        - IPSec：网络层
            - 模式：见 PPT108 页
                - 传输模式：原 IP 头和 IP 数据之间插入 IPSec 头
                - 隧道模式：原 IP 头和 IP 数据作为新的 Payload，在新 Payload 之前加入 New IP 头和 IPSec 头
            - AH：Authentication Header，提供完整性、源认证，但不加密报文
            - ESP：Encapsulating Security Payload，与 AH 一起提供加密功能。
            - SA：Security Association 安全关联，定义了发送方和接收方之间的单向关系，全双工通信通常需要两个 SA。
                - SPI：Security Parameters Index 安全参数索引(SPI)告诉我们在什么 SA 下处理接收到的数据包。
            - IKE：Internet Key Exchange 因特网密钥交换，用于建立、修改和删除安全关联。