1. 直链网络

1. **TCP/IP 四层模型 具体功能**

   应用层：数据表示、数据加密、会话控制

   传输层（TCP/UDP）：定义端到端协议，流量控制、拥塞控制

   网络层（IP）：实现端到端的通信，路由寻址转发

   子网层（以太网协议）：节点到节点的通信，比特流的传输

2. 错误检测

   - 差错检测：添加冗余信息来确定是否存在差错
   - 奇偶校验：d 比特信息和 1 比特校验位中 1 的总数为奇/偶数，可以检测奇数个比特差错（偶数个检查不出来）
   - 校验和：
     - 发送方：将数据所有字段以 16 位分割，用反码算数运算将所有 16 位数据相加（高位有进位则回卷到最低位），对结果取反码，即为校验和，同数据一起发送给接收方
     - 接收方：将所有 16 位加和（包括校验和），结果若全为 1，则认为无差错
   - 循环冗余校验：使用最少的冗余数校验最多错误

3. **TCP 可靠传输的实现：“确认+传输”的组合**

   - 自动请求重发 ARQ
     - 停等算法：发送方传输一帧之后，在传输下一帧之前等待一个 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
     - **滑动窗口算法：**通过窗口大小限制在途传输的数据帧个数
       - **流量控制**：接收方根据自身接收能力，控制发送方的发送速度
       - **拥塞避免**：发送方感知网络拥堵情况，主动放慢发送节奏

4. 媒体共享技术

   (1) 静态接入控制：

   ① 信道复用技术，为多个用户静态划分逻辑信道，相互不冲突

   ② 频分复用、时分复用、波分复用、码分复用（每个站分配的码片序列相互正交）

   (2) 动态接入控制：并不固定分配给用户，使用时动态接入

   ① 随机接入：节点按需随机接入，需解决碰撞问题

   1) ALOHA/时隙 ALOHA：为**无线网络**研制，用于任何传输介质，帧下来后立即发送，若碰撞以一定概率重传，一定概率等待一个传输时间

   2) 载波侦听多点接入 CSMA：**总线型网络**，多个节点以多点接入的方式连接在一个总线上，同一冲突域；载波侦听即节点再发送前先检测信道，是否有其他节点也在发送，若有则暂时不要发送数据，以免发生碰撞

   3) 带碰撞检测 CSMA/CD：先听再发，发的时候检测，撞了就停发、等一等再发

   4) 带碰撞避免 CSMA/CA：先听再发，发前先发信号预约信道，避免碰撞发生

   ② 受控接入：节点接入服从一定控制，入令牌环网

2. 网络互联

1. 交换机/网桥：靠 MAC 地址表过滤转发数据帧，只把帧法网目标节点所在的端口（非泛洪）
2. 节点位置：通过学习数据帧的源 MAC 记录节点位置
3. 生成树算法基本原理：阻断环路端口，避免帧广播风暴，让全网形成无环的树形转发路径
4. 地址分类
   ① ip 分类：把 IP 固定分类 A/B/C/D/ E 类，网段边界死板，地址浪费多
   ② 无类地址：打破固定分类，用**“子网掩码+前缀”**划分网段，按需分配地址节省 IP 资源
5. **路由协议 rip ospf 区别**

对比维度	RIP 距离矢量	OSPF 链路状态
协议基于类型	基于距离矢量	基于链路状态
交换内容	整表发送：向另据传输自身全部路由表	局部通告：尽向全网传输自身直连链路的状态
使用范围	小型局域网（跳数限制，最大 15 跳）	中大型/广域网（无跳数限制，支持大规模组网）
转发策略生成	从邻居路由表中，选跳数最少的路径作为最优	全网同步链路状态后，各自用 SPF 算法计算到各节点最短路径

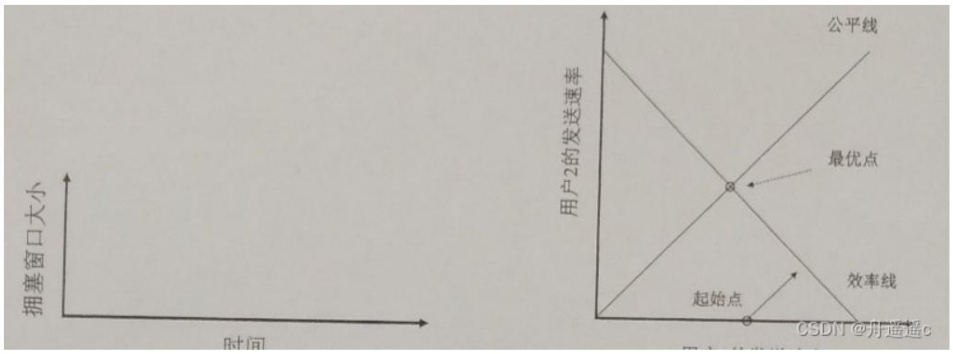
3. 网络传输

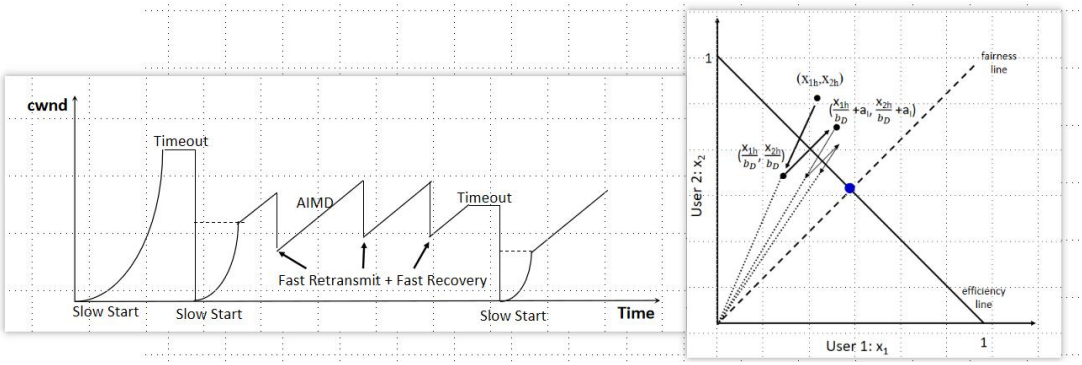
- UDP 特点：面向无连接的不可靠传输、丢失不重传、支持（一对一/一对多/多对一/多对多）的交互通信，轻量快传

- TCP 特点：面向连接的可靠传输、丢失重传、基于字节流的传输

1. **自适应重传**（基于超时的重传机制 快重传）拥塞控制 P30
   (1) **自适应重传**：基础是**超时重传**（发完等确认，超时就重传）；优化版**快重传**（没等超时，收到 3 个重复确认就直接重传），不用干等，提升效率
   (2) 发送方根据网络拥塞情况，动态调整发送窗口大小，避免网络堵死，核心是慢启动、拥塞避免、快重传、快恢复四步配合
2. **AIMD** 为什么能收敛 要会描述和绘制 P155
   (1) 网络空闲时加法增（每次加一点发送窗口，慢慢涨，不突然堵网）；检测到拥塞时乘法减（窗口直接减半，快速降速，立刻缓解拥堵）。一增一减的节奏，让全网所有发送方的发送速率慢慢趋于一致，最终适配网络总带宽，不会互相抢占导致全网拥塞，实现收敛

4. TCP通过AIMD（加性增，乘性减）机制来探测可用带宽和保障竞争流间的公平性。只考虑AIMD机制，试在如下图（a）中画出一个TCP流的拥塞窗口随时间变化的形状，并说明该形状的变化周期。对于两个竞争流，从如下图（b）中的起始点出发，在图中通信两个竞争流的发送速率收敛到最优点过程中的变化曲线。





4. 网络应用

1. **DNS　web（www）用户访问整个过程**（底层整个协议起了什么作用）

2017.1 试描述“在浏览器中输入网址，到取回网页”这段时间发生的网络操作。

答：1. 网址域名 DNS 查询，解析对应的 IP 地址。
2. 生成对应的 HTTP 请求，封装 TCP/IP 数据包。
3. 查询 IP 地址对应的网关和下一跳的 IP 地址。
4. 查询下一跳的 IP 地址对应的 Mac 地址。
5. 把数据转发给网关。
6. 经过路由寻址抵达网页服务器。
7. 网页服务器解析，返回所需具体页面。

3. **根域名服务器**的作用，**递归查询**和**迭代查询**的原理

(1) 根域名服务器：根域名服务器知道所有顶级域名服务器的域名和地址，本地域名服务器如果无法解析则需要求助于根域名服务器

(2) 递归查询（主机向本地域名服务器查询）：主机查询的本地域名服务器不知道被查询的域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文

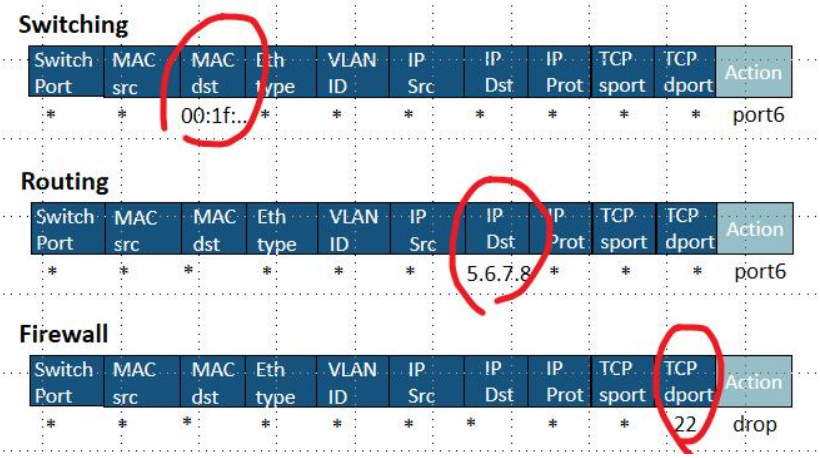
(3) 迭代查询（本地域名服务器向根域名服务器查询）：当根域名服务器收到本地域名服务器的迭代查询请求报文时，要么给出要查询的 IP 地址，要么告诉本地域名服务器下一步应当向哪一个域名服务器继续进行查询

4. DHCP 协议：动态主机配置协议

主机启动时广播发送 DHCP 发现报文，DHCP 服务器回答该报文，DHCP 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 地址池中取一个地址分配给该计算机

5. 软件定义网络：虚拟化技术（NFV 硬件虚拟化，复用提高效率；SDN 软件定义网络）

1. 什么是软件定义网络 SDN，如何实现管理：
   (1) 数据面和控制面物理分离的网络
   (2) 由逻辑上集中的控制面控制多个转发设备 ，统一编排控制策略
2. 网络三个平面：
   (1) 数据面：按照转发与处理规则，执行数据包处理与转发的平面
   (2) 控制面：计算转发与处理规则
   (3) 管理面：配置网络，设置路径权重影响控制面计算，从而实现特定目的（**流量工程**）
3. 流表要能看得懂实现了什么功能（交换 路由 防火墙功能）



6. 未来互联网体系

1. 为什么会形成细腰结构
   (1) 网络层设计简洁清晰，业务和通信模式自由发展，符合最初主机互联和资源共享的需求
   (2) 在当前的 IP 网络体系结构中，认为细腰结构存在于 IP 层。然而由于网络中存在着大量的重复流量，因此在未来的互联网体系结构中，认为细腰结构应该上移，从而更多地面向网络服务。
2. 还会演进吗？未来互连网体系结构
   (1) NDN、SOFIA、LISP、MobilityFirst 等
   (2) NDN 基本思想：把基于 where 的 ip 模式 变为基于 data 的模型，网络通信属于 pull 模型，接收方发送指定内容的 interest 作为请求，一个 interest 触发最多一个 data 数据包，数据包沿 interest 请求路径返回（name 和位置无关，天然支持移动性）
   (3) 将 IP 传输方式变为网络内缓存（in-networking）好处：基本消除了冗余传输
3. **ip 二义性带来什么问题，为什么要把名字和路径分开：**
   移动性为例：IP 地址即表示位置（移动过程中改变），又表示身份（移动过程中不变），端到端连接绑定了地址，移动过程中地址切换，连接断开需要重新建立连接，服务质量下降，不改变 IP 地址的二义性就无法从根本上解决问题
4. 互连网体系结构的两个核心问题
   (1) 怎么命名 Naming：比如 IP 网络就是以 IP 地址命名主机
   (2) 如何路由 Routing：怎么用名字把数据包转发到目的地
5. 原地址 AIP 问题：

(1) 网络安全问题的根源之一：IP 层的名字没有任何安全绑定或属性
(2) AIP 核心思想：再命名上增加安全属性，使用自验证地址（实体公钥作为名字），摒弃 CIDR 前缀地址，采用多层级扁平地址结构，地址组件与公钥哈希绑定，实现自认证，无需全局可信机构验证
(3) 原 AIP 问题：用户没有隐私了，任何一个而数据包最终都能追溯到主机（人），AIP 实现问责制，网络运维者能知道每个数据包是由谁发的，源地址无法伪造，但又涉及用户隐私
(4) APIP：委托问责，通过端到端加密和地址转换，只有源端网络知道是谁发的，保护隐私，每个数据包都有一个问责地址

网络专题部分_孙毅老师

1.网络安全的定义以及五大要素?

2.加密技术的 3 种类型？对称密码算法的含义?非对称密码算法的含义?二者的优缺点比较。如何用非对称密码(公钥密码算法)进行数字签名?

3.DES 算法的基本原理?RSA 算法的基本原理?

4、基于单项校验和的身份验证的流程以及争议解决的方法及原理?

5.什么是主动攻击，什么是被动攻击?常见的主动被动攻击行为都有哪些?

6.什么是 DDos 攻击?

8.什么是大象流?什么是老鼠流?什么是乌龟流?什么是蜻蜓流?

7.网络测量的定义及应用?

9.网络测量的分类标准都有哪些?按照不同标准分类分别都分出那些具体的类别?

10.什么是主动测量?什么是被动测量?各自的优缺点是什么?

11.什么是链路的瓶颈带宽?什么是链路的可用带宽?二者的区别?

12.典型的可用带宽和瓶颈带宽的测量方法?

13、什么是别名解析?具体的别名解析方法及原理?

14.服务质量的概念和 IP Qos 的目标?

15.端到端时延包含哪些部分?其中每一部分的具体含义?

16.三种 Qos 模型及相互比较?

17.RSVP 协议的工作原理及协议特点?

18.区分服务模型的基本原理?

19.什么是队列调度?路由器出端口队列结构?

20.常见队列调度算法拥塞控制机制的原理?及各自的优缺点?

21.什么是整形?什么是限速?令牌桶算法的工作原理?

22.什么是 zip-f 定律?

23.Web 缓存的工作原理?及它的缺点?

24.CDN 的工作原理?及它的服务器选择的常见策略?

25.缓存容量受限时该如何管理(缓存内容选择和替换策略)缓存?

26.什么是 P2P 网络?

27.BitTorrent 协议的特点和原理?

28.基于 DHT 的 P2P 网络的特点?Chord 的原理?

29. 什么是区块链?其核心价值有哪些?

30.区块链系统的基本工作原理?

31.什么是区块?什么是 Hash 链?各自的作用是什么?

32.区块链与分布式数据库的区别?

33.生活中常见的区块链应用的案例?