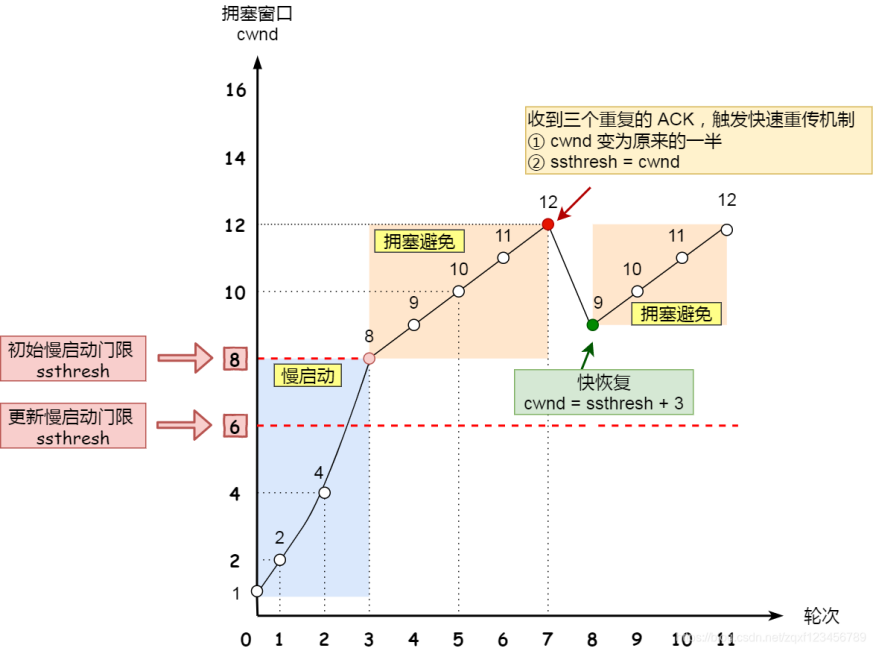
1. TCP/IP四层次的作用以及相应协议，原题
2. ABCD四个站的码片，发送的码片，计算ABCD各发送的消息
3. RIP OSPF BGP三个协议的不同
4. 最长匹配，选择路由，比较简单
5. TCP流量控制和拥塞控制的目的以及实现原理
6. 链路带宽、可用带宽是什么，测量这两种带宽的方法
7. 综合服务模型 区分服务模型有啥区别，RSVP工作原理，为啥逐跳路由
8. 对称加密算法和非对称加密算法是什么，优劣势，加密和签名过程
9. 根域名服务器的作用，递归查询和迭代查询的原理
10. 区块链的哈希链是啥，作用以及举例区块链的作用
11. 总线和无线使用的协议分别是啥，为啥不一样，我答的CSMA/CD和CSMA/CA以及区别

往年原题居多，部分新题，主要还是概念和原理，手写居多



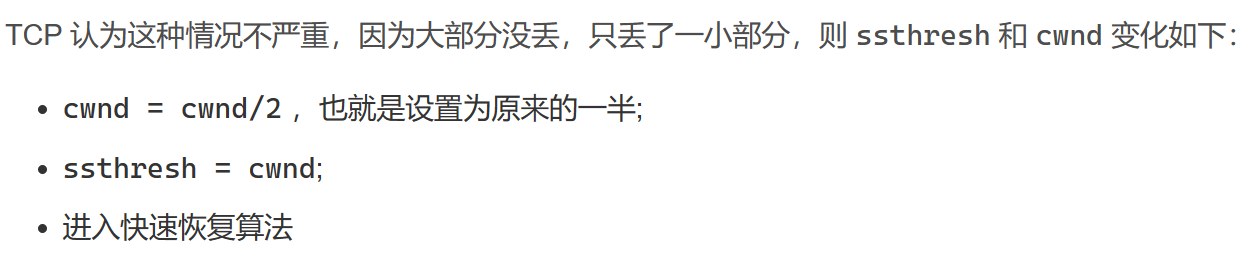
流量控制：避免「发送方」的数据填满「接收方」的缓存，但是并不知道网络中发生了什么。

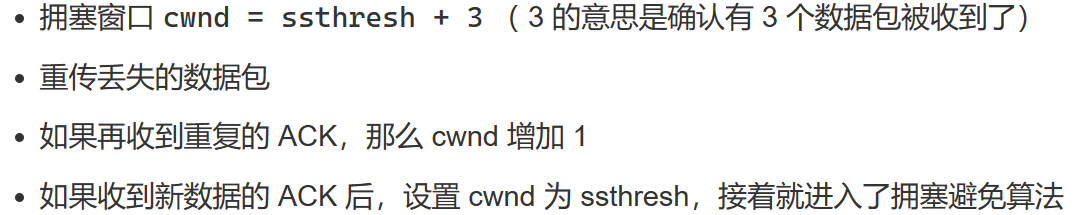
****拥塞控制：避免「发送方」的数据填满整个网络，避免更大的延迟以及更多的丢包****

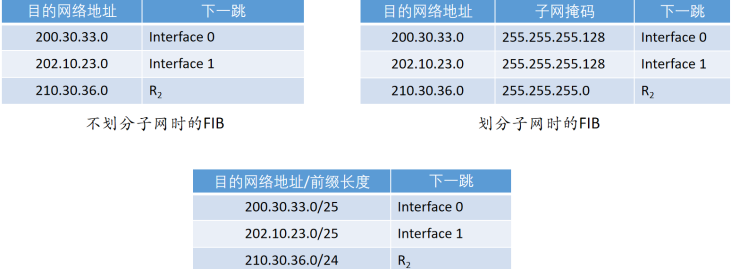
### 慢启动:当主机开始发送数据时，如果立即所大量数据字节注入到网络，那么就有可能引起网络拥塞，因为现在并不清楚网络的负荷情况。因此，较好的方法是先探测一下，即由小到大逐渐增大发送窗口

拥塞避免:让拥塞窗口cwnd缓慢地增大，即每经过一个往返时间RTT就把发送方的拥塞窗口cwnd加1，而不是加倍。这样拥塞窗口cwnd按线性规律缓慢增长，网络出现拥塞，把慢启动ssthresh设置为出现拥塞时的发送方窗口值的一半（但不能小于2）。然后把拥塞窗口cwnd重新设置为1，执行慢开始算法。迅速减少主机发送到网络中的分组数，使得发生拥塞的路由器有足够时间把队列中积压的分组处理完毕。

拥塞避免阶段将拥塞窗口控制为按线性规律增长，使网络比较不容易出现拥塞

快速重传：发送端在收到3个重复无序的ACK时候，它假定数据包丢失并重传该数据包，而无需等待重传计时器到期。

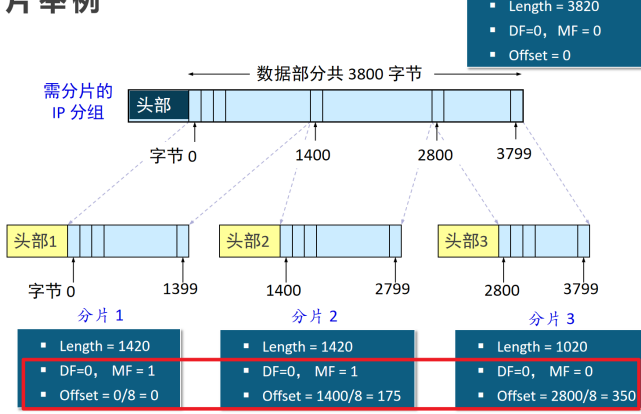




路由选择协议,路径选择

地址解析协议 ARP (Address Resolution Protocol)

实现IP地址与硬件地址的映射

网际控制报文协议 ICMP (Internet Control Message Protocol)

网络控制与诊断

网际组管理协议 IGMP (Internet Group Management Protocol)

网络地址转换NAT (Network Address Translation):私有地址与全局地址之间的翻译



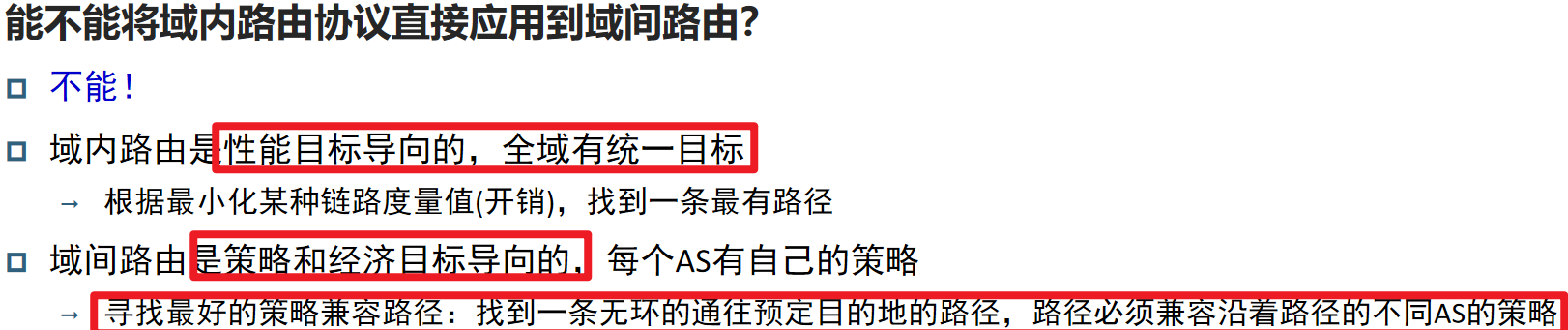
互联网采用两层的路由选择协议

域内 (Intra-Domain)路由协议，内部网关协议 (interior gateway protocol, IGP)：性能目标导向的，全域有统一目标

域间 (Inter-Domain)路由协议，外部网关协议(Exterior Gateway Protocol, EGP)：策略和经济目标导向的，每个AS有自己的策略

RIP距离向量算法：出现故障收敛慢，开销大，扩展性差

开放最短路径优先OSFP协议：使用最广泛的分布式链路状态(Link State, LS)路由协议，收敛速度快，支撑更大规模的网络路由



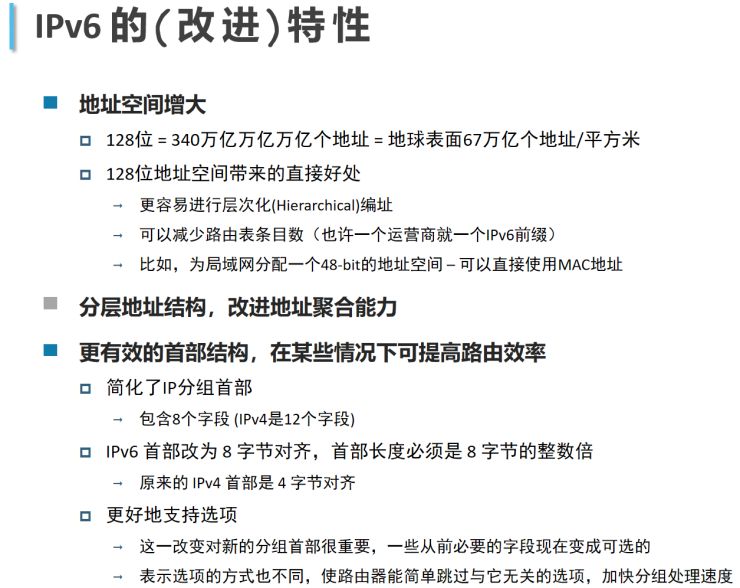
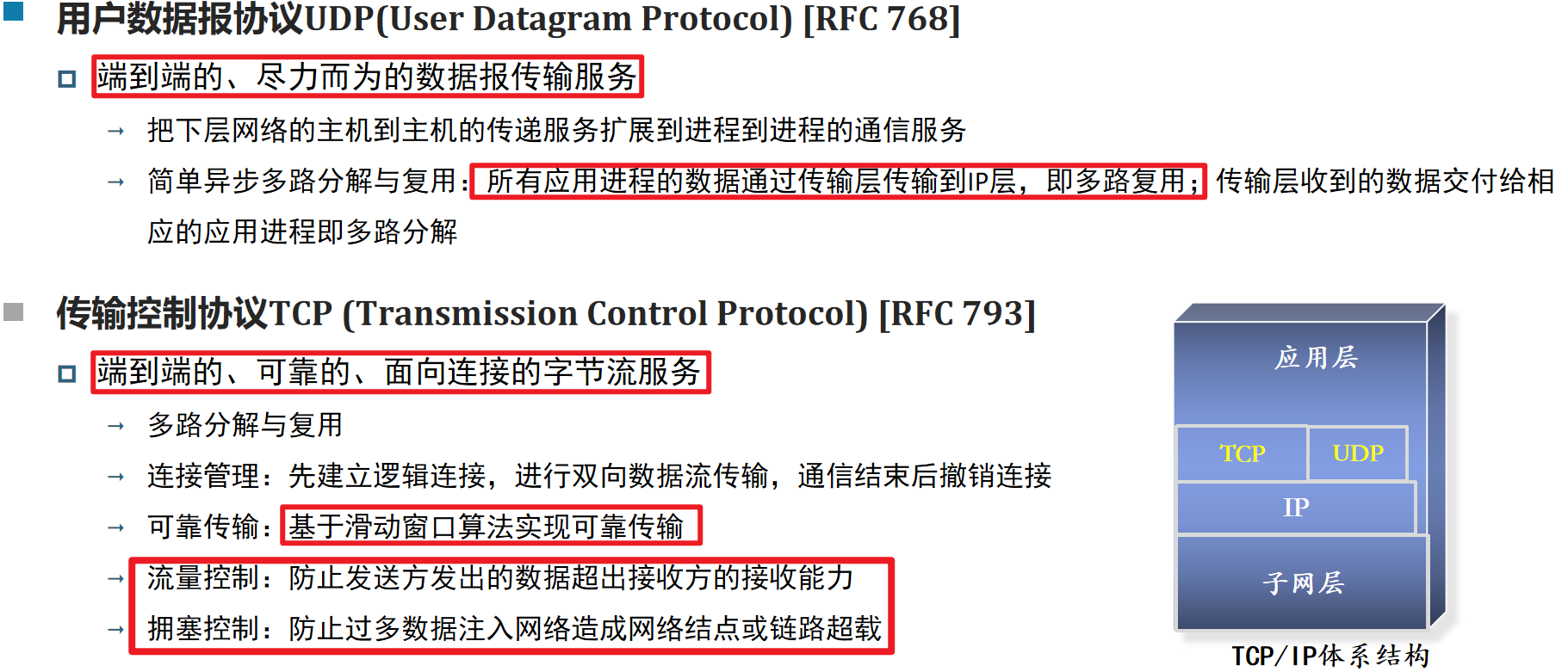
域间的对等点 (BGP发言人) 之间使用 TCP 连接

IP 地址的双重职责 (二义性)

标识符 (identifier)：移动过程中始终不应变

定位符 (locator)：应随着网络接入点的变化而变化

移动 IP (Mobile IP)技术，通过 IP-in-IP 隧道方式将发往移动节点家乡网络的数据包转发到移动节点的当前位置

与下层协议无关、对上层协议透明，独立于各种无线接入技术及具体上层业务，应用范围最广、应用效果最好

双协议栈技术 (Dual-Stack) 设备上同时支持IPv4和IPv6协议栈，其它过渡技术的基础隧道技术(Tunnel)

把 IPv6 分组封装在 IPv4 分组中，IPv6 网络之间穿越 IPv4网络进行通信

互通技术NAT-PT (Network Address Translation –Protocol Translation)

在两种网络的相连处进行两种地址间的翻译，修改协议报头，使 IPv4 网络与 IPv6 网络能够互通

IP层：主机-主机的通信 传输层实现端系统上运行的应用进程间的逻辑通信，即端到端传输

传输层采用抽象定位符端口 (port)，使得进程间能够间接相互识别

<源主机IP、目的主机IP、源端口号、目的端口号> 四元组可唯一标识互联网中的 TCP 或 UDP 传输

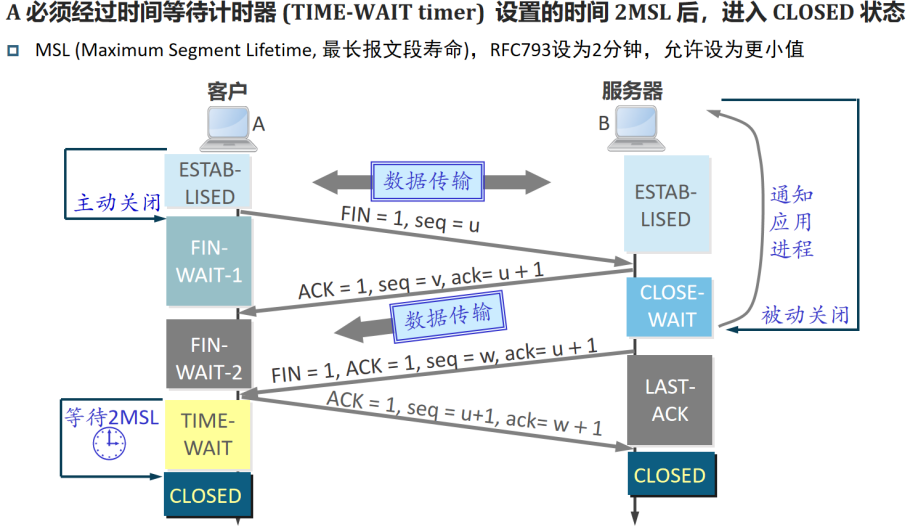
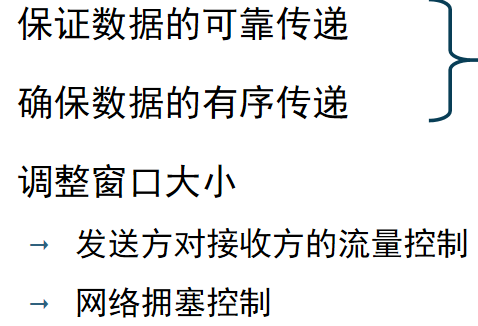
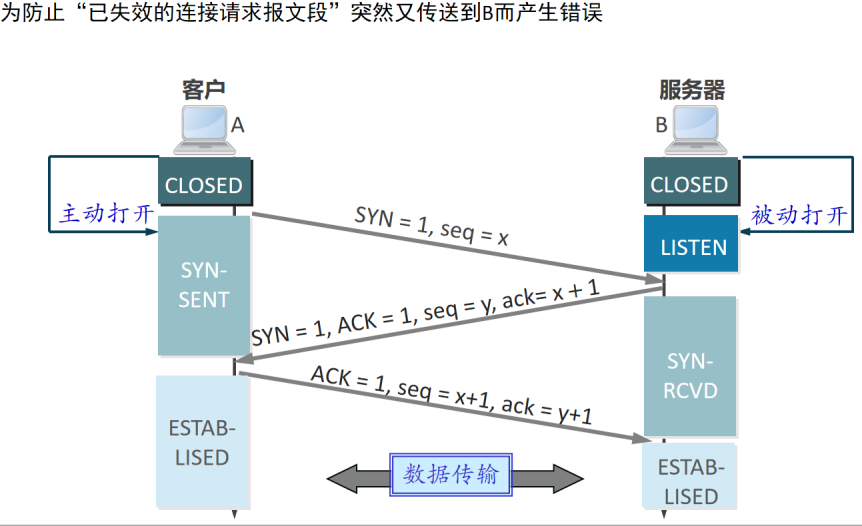
UDP:无连接的，无需建立连接，无需维护状态 减小开销和启动延迟，例如DNS 尽最大努力交付，不保证可靠传输

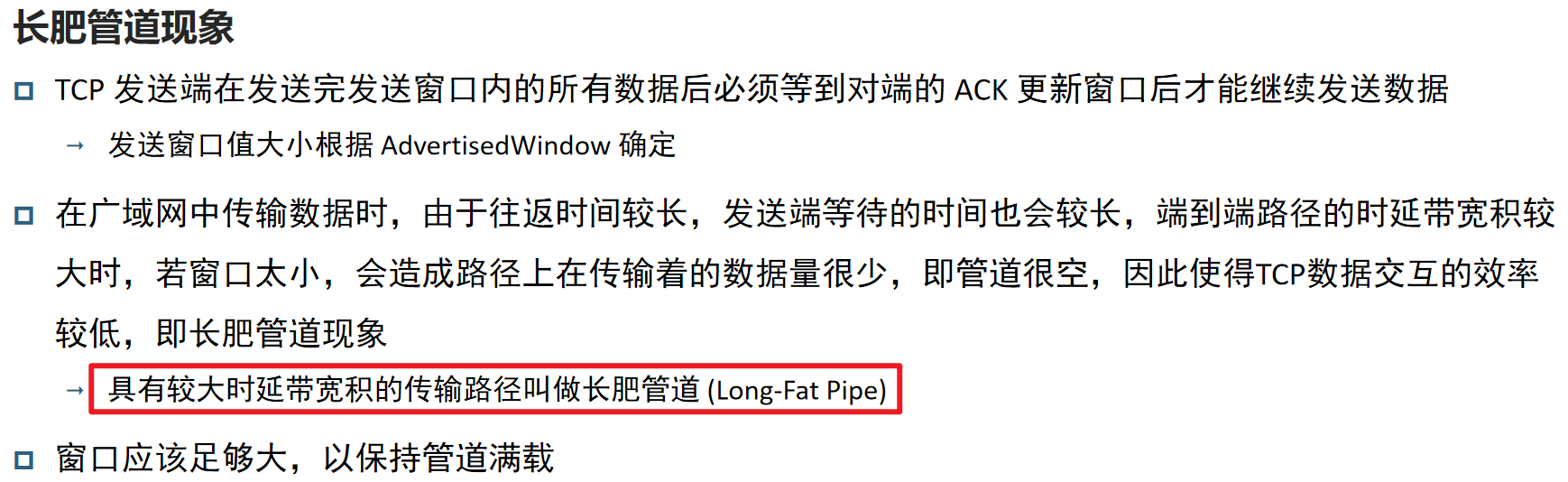
主机不需维持复杂的状态 没有拥塞控制

每条 TCP 连接是一对双向的点对点字节流，每条 TCP 连接两个端点

双方确定自己的初始序列号，并通知对端 两端的初始序列号相互独立，各自随机选择一初始序列号

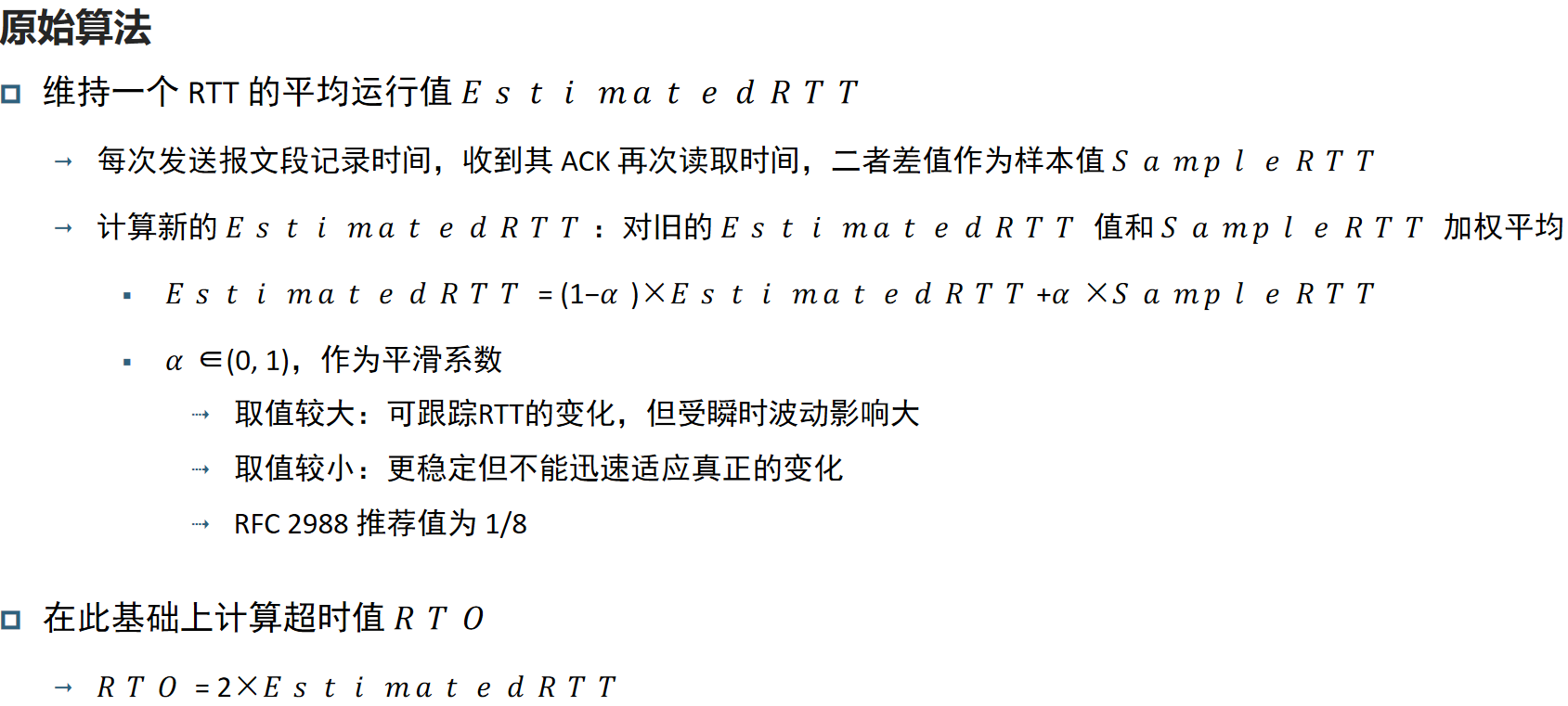
为什么随机选择，不从0开始？ 防止使用同一连接标识的两个不同实例，过快地重复使用同一个序号

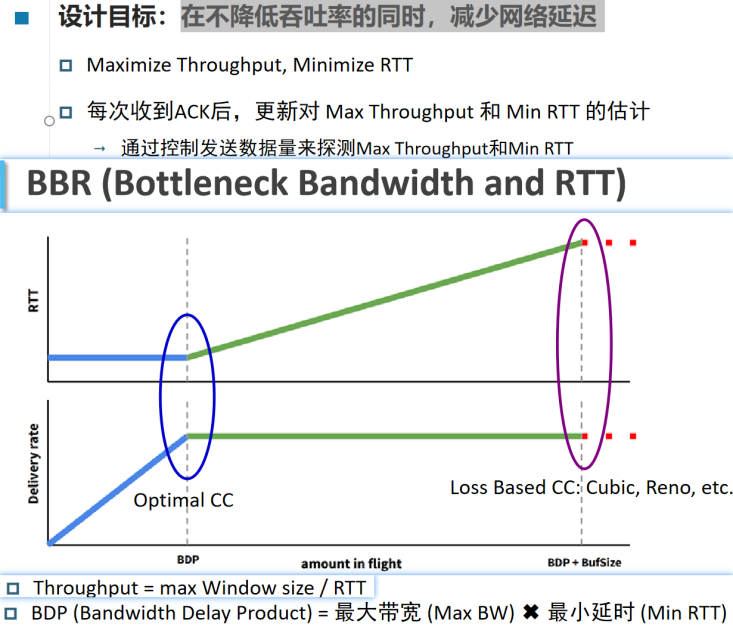


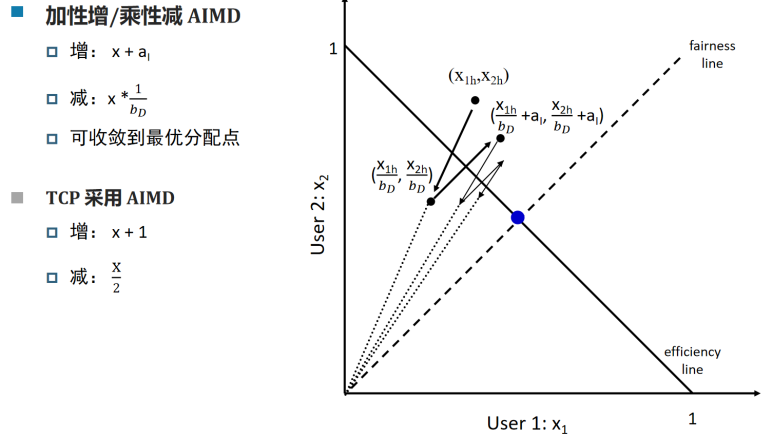




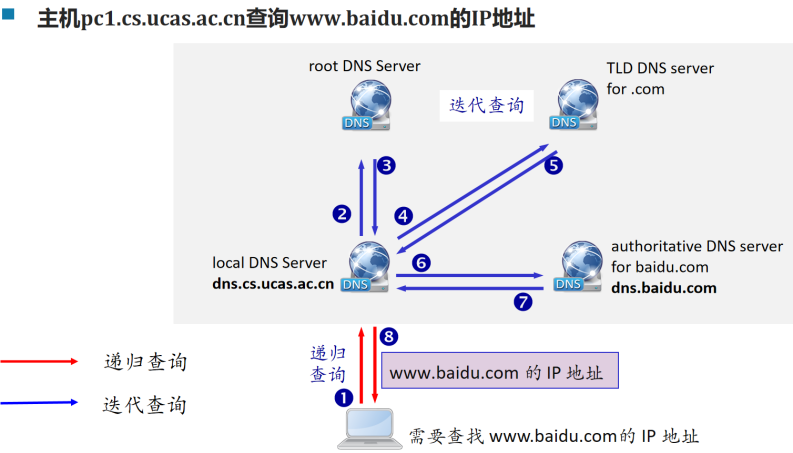
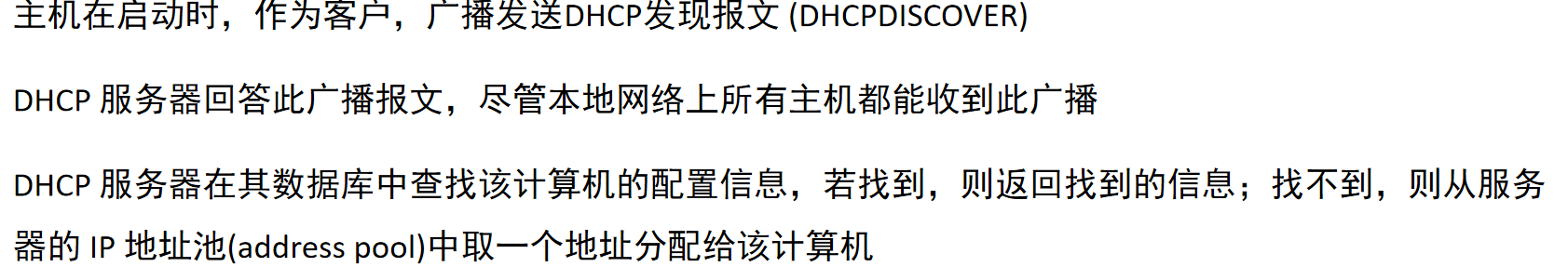
TCP 每发送一个报文段，就对这个报文段设置一定时器RTO,定时器到期，还没有收到确认，就重传该报文段



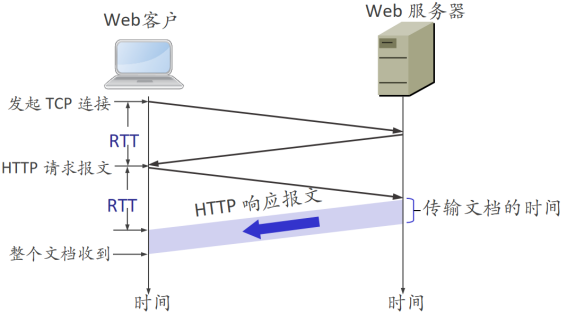
快速重传不能代替常规超时机制，仅是增强功能，在某些情况下可更早地触发重传丢失的报文段

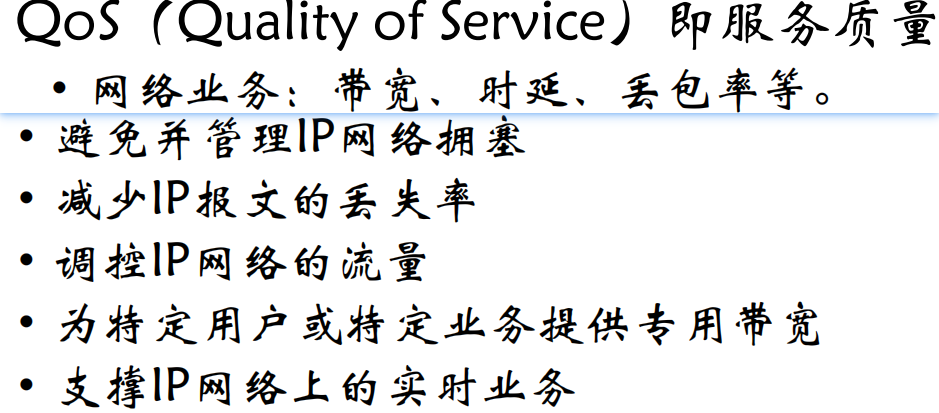


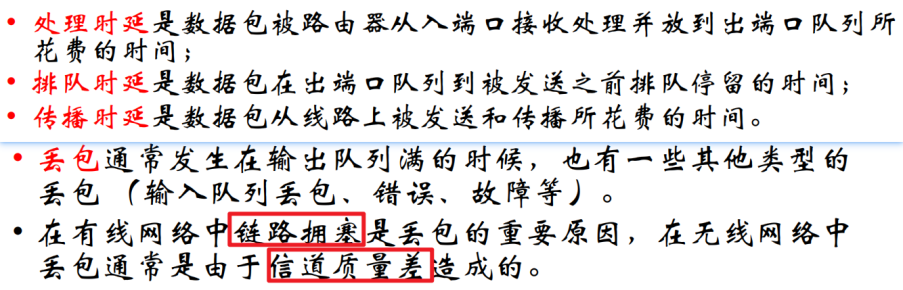
应用层协议 定义某一类网络应用的应用进程之间的通信规则

主机名 (域名)解析 (映射) 为IP地址









业务综合化 业务差异化

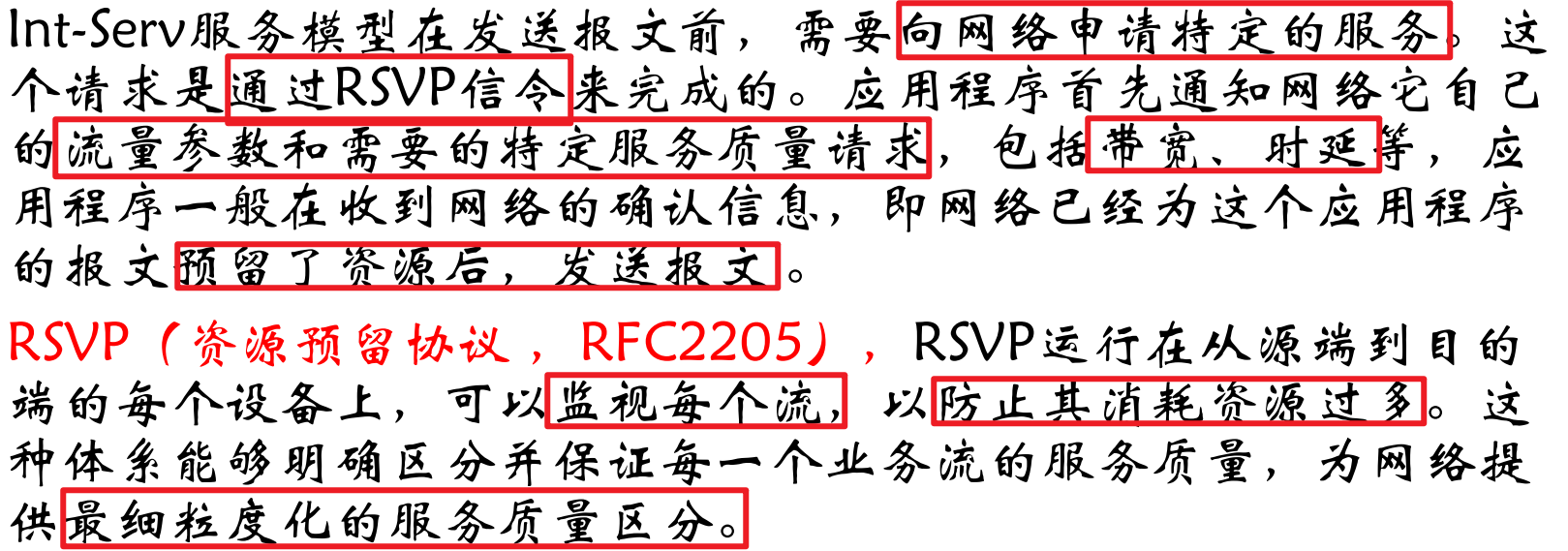
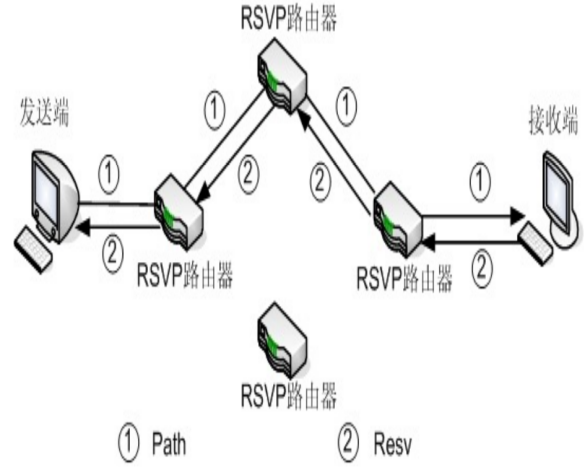
Best-Effort service（尽力而为服务模型） 单一的服务模型，也是最简单，网络尽最大的可能性来发送报文。但对时

延、可靠性等性能不提供任何保证。

是网络的缺省服务模型，通过FIFO队列来实现。适用于绝大多数网络应用

• Integrated service（综合服务模型，简称Int-Serv）

• Differentiated service（区分服务模型，简称Diff-Serv）



工作在IP协议之上，属于OSI模型的传输层

• 本身并不处理传输层的数据，是一个网络控制协议

• 可以在点对点单播或多点对多点的组播网络通信应用中进行资源预留

• 是一个单向的资源预留协议

• 面向接收端的资源预留协议，由会话的接收端发起资源预留请求

• 对不支持它的路由器提供透明的操作

优缺点：提供绝对有保证的QoS

• 可扩展性是Int-Serv结构最致命的一个问题，需要端到端信令，为每一个

会话预留软状态

• 对路由器的要求较高，要求路径上所有路由器必须支持RSVP

• 不适合于短生存期的流，包预留资源的开销很可能大于流中所有包的开销

是多服务模型，起源于IntServ，它可以满足粗粒度的QoS需求。

• 不需要使用RSVP，应用程序在发出报文前，不需要通知网络为其预留资源。

• 网络不需要为每个流维护状态，根据每个报文的差分服务类（IP报文头中的差分服务标记字段DS），来提供特定的服务



根据排队和出队的策略的不同，队列调度分为以下几种

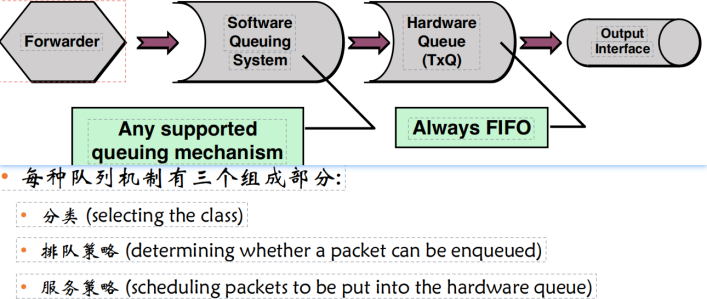
• FIFO（First In First Out）：先进先出队列

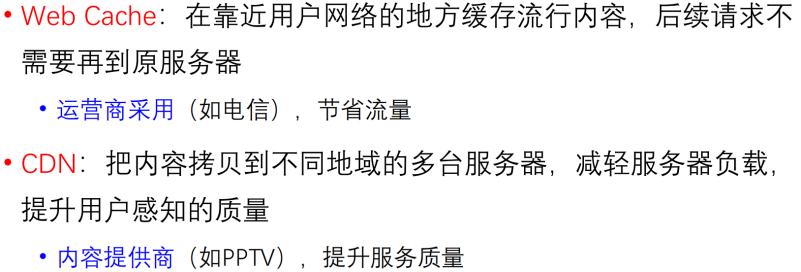
• PQ（Priority Queue）:优先级队列

• CQ（Custom Queue）：定制队列

• WFQ（Weighted Fair Queue）：加权公平队列

• CBWFQ（Class Based WFQ）：基于类的加权公平队列





EDNS：用户->CDN服务器的映射

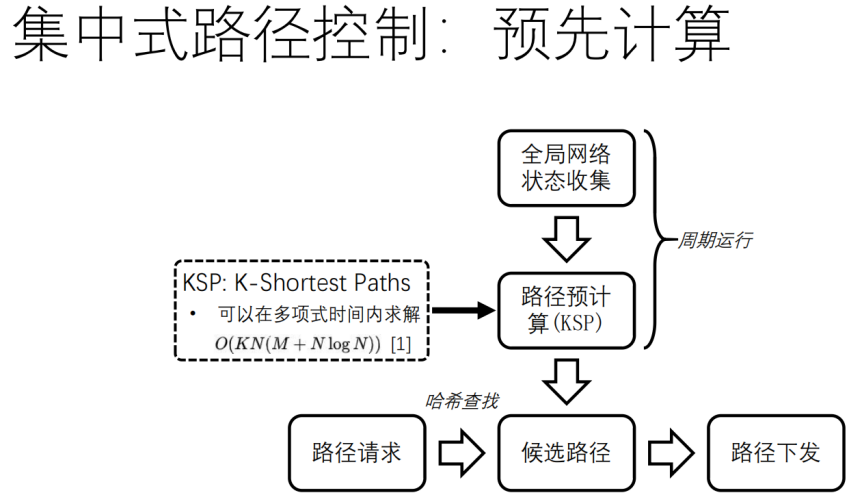


用早期流行度预测整个生命周期流行度 LSTM时间序列

找关联：• 电视剧的集• 视频网站的推荐视频 GNN空间关联

部分缓存 缓存替换

分块传输（chunk） 便于切换码率

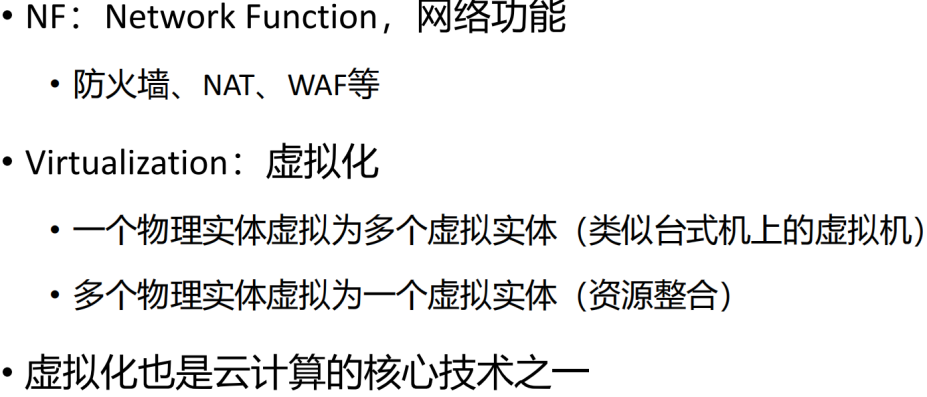


软件定义网络

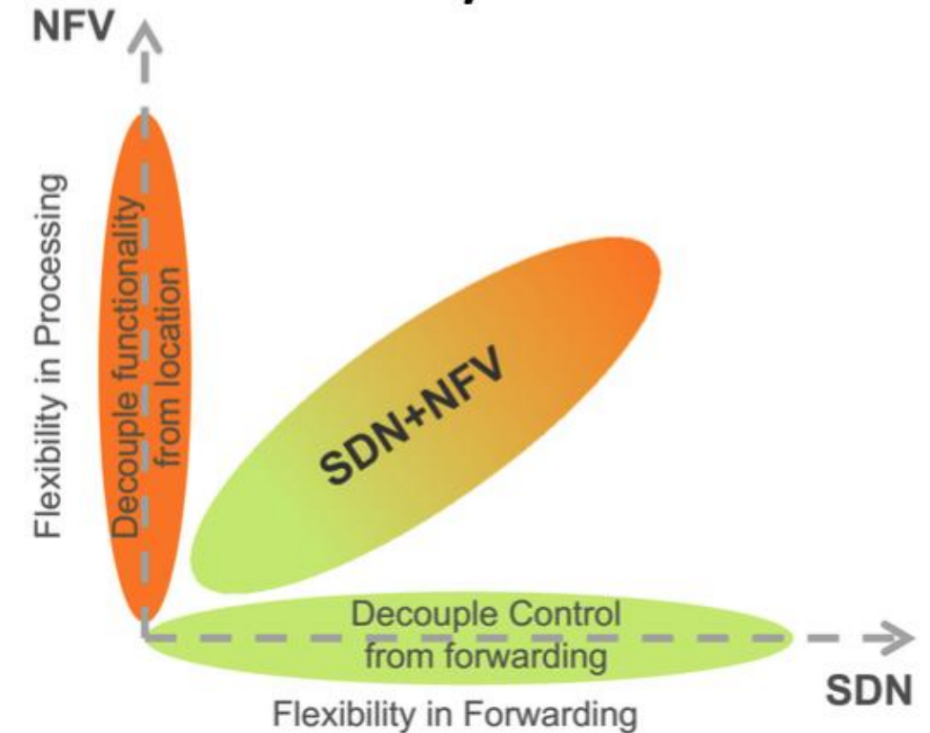
• 数据面（data plane）与控制面（control plane）物理分离的网络

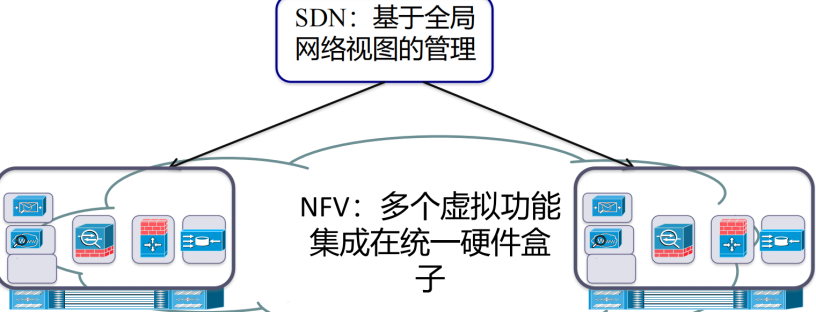
• 由（逻辑上）集中的控制面控制多个转发设备（如交换机）









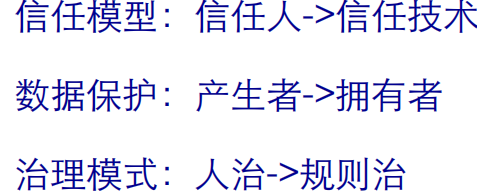


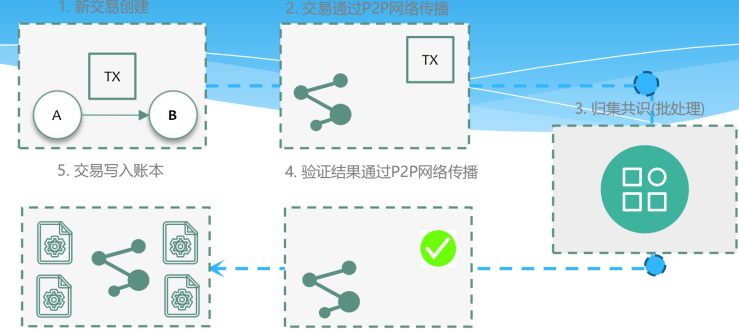
区块链通过去中心化的分布式记账方式实现了多方间的可信数据流转需求，成为构建web3.0时代不可或缺的关键技术

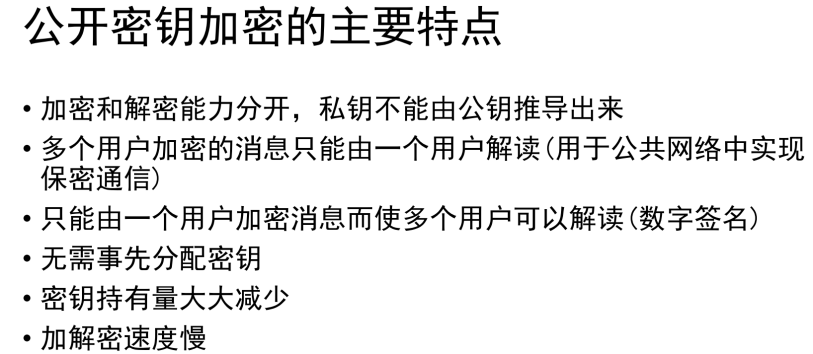
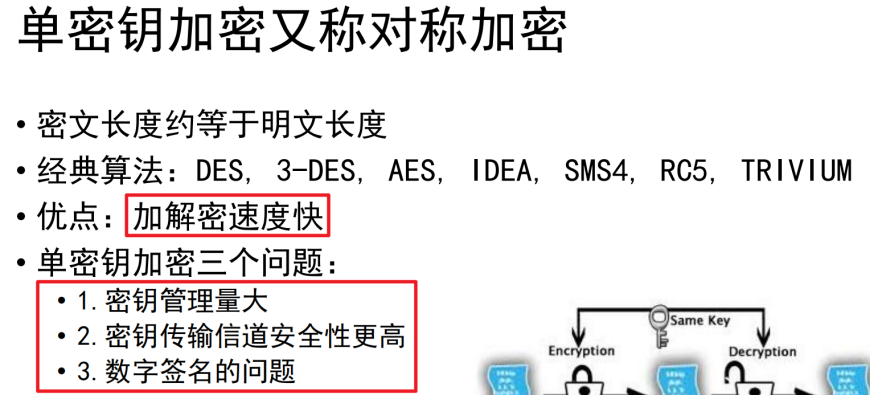
数据的不可伪造、不可篡改和可追溯特性， 消除了中心化方案下寡头操纵和单点故障的风险，增加了系统的鲁棒性

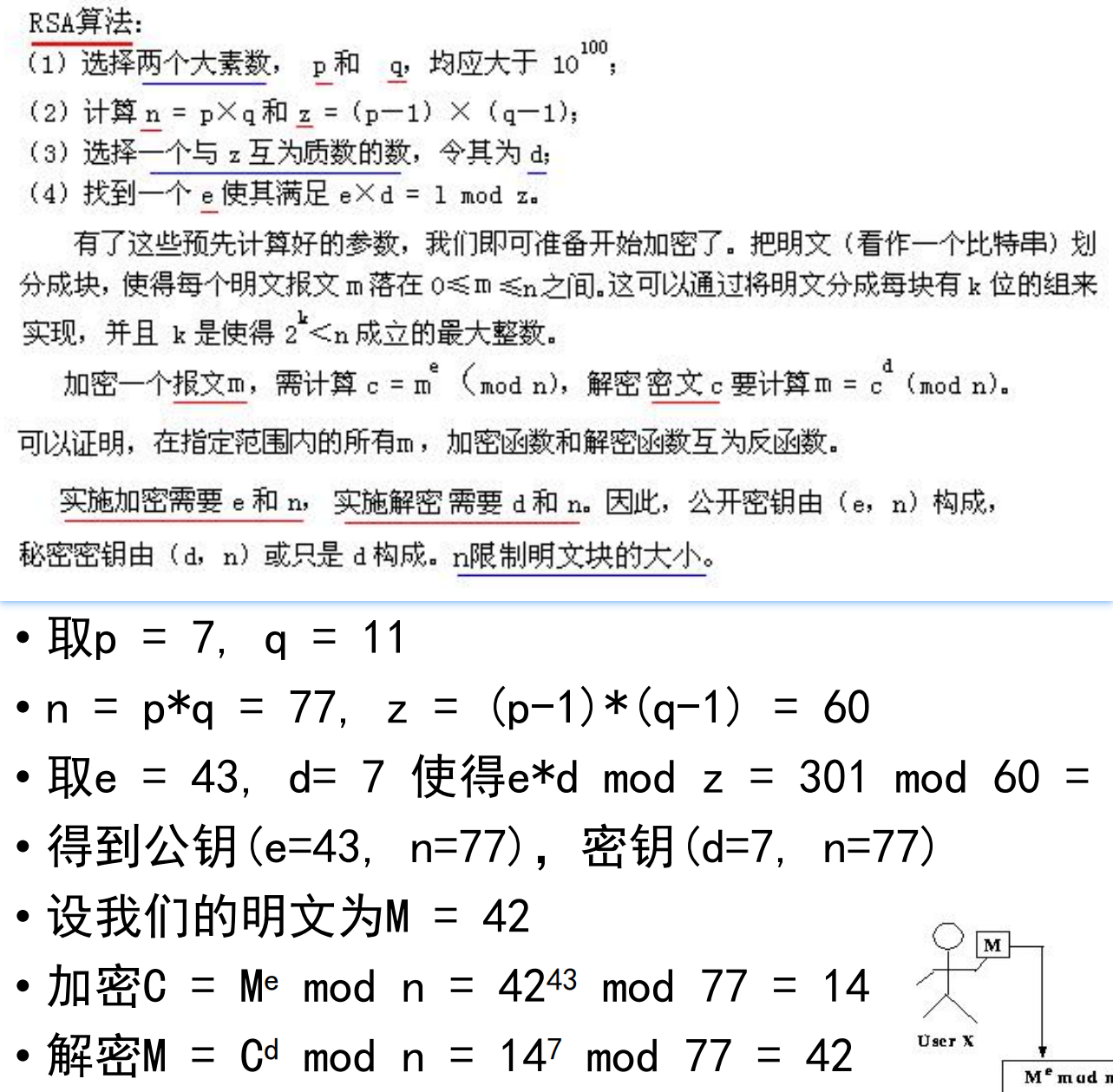
智能合约能够按照预先定义数据的访问和使用规则自动执行 任何组织或个人都无法干预数据的流转过程

边缘计算将计算和存储功能由中心化服务器转移至更靠近网络边缘数据源的位置

区块链（Blockchain）是一种创新的分布式交易验证和数据共享技术



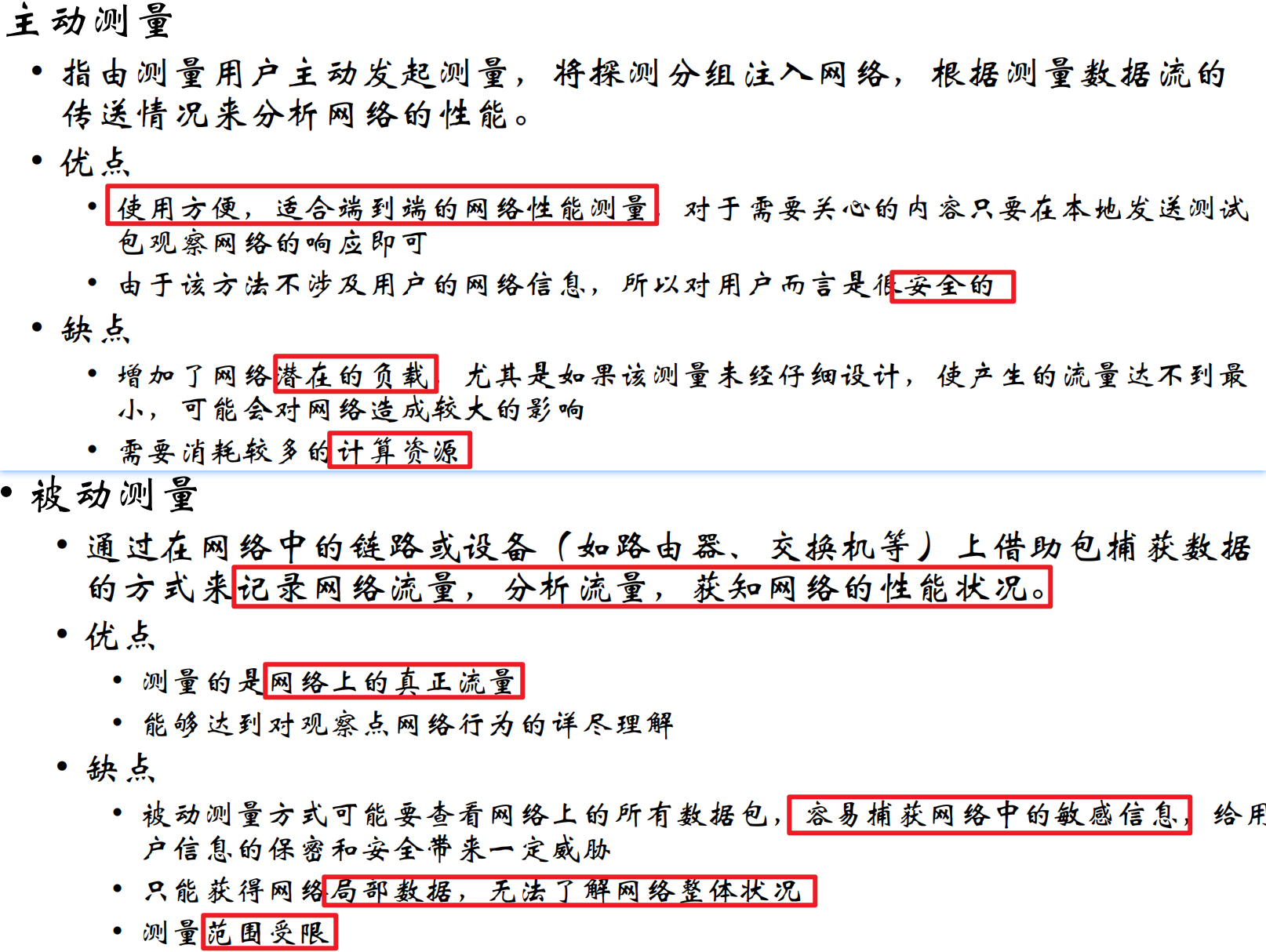




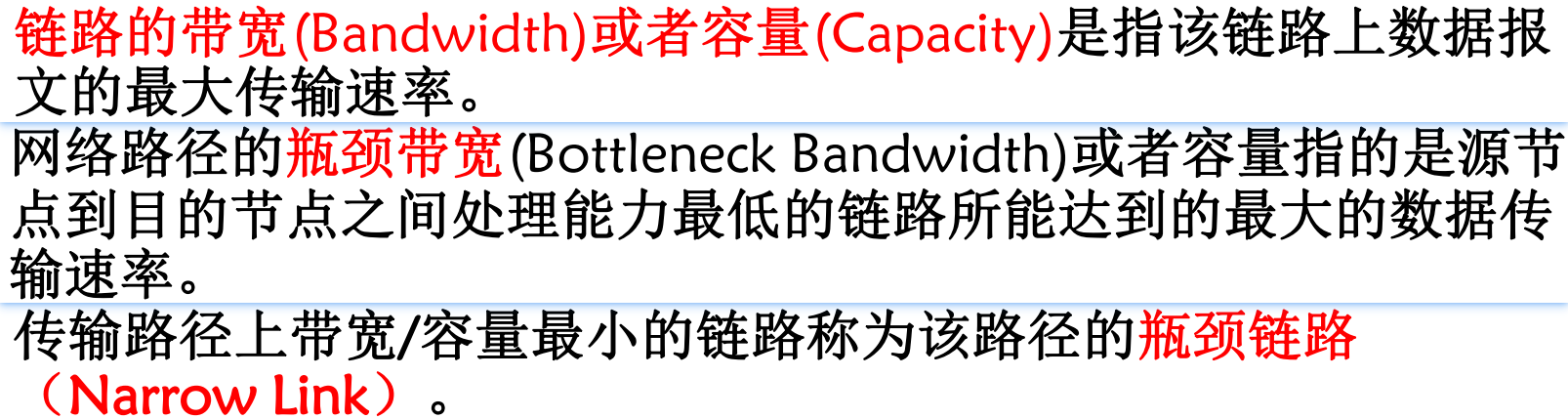
向目标网络发送大量数据包耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务停止响应甚至崩溃。

• DDoS：Distributed Denial of Service，即分布式拒绝服务攻击。借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。









可用带宽(Available Bandwidth)是指当应用程序和其它背景流(Cross Traffic)共享网络路径时，该应用程序所能得到的带宽

