

一、假定有一个通信协议，每个分组都引入 100 字节的开销用于头和成帧。现在使用这个协议发送 1M 字节的数据，然而在传送的过程中有一个字节被破坏了，因而包含该字节的那个分组被丢弃而造成重传该分组。试对于 1000、5000、10000 和 20000 字节的分组数据大小分别计算“开销+丢失”字节的总数目？分组数据大小的最佳值是多少？

答：假设一个分组中的数据大小为  $p$  字节，则共有分组数为  $\frac{1\text{MB}}{p}$  个，总的头部

代价为  $100 * \frac{1\text{MB}}{p}$ 。有一个字节被破坏，需要重传这个分组，这个分组大小

为  $p+100$ 。因此共传输数据为  $100 * \frac{1\text{MB}}{p} + p + 100\text{byte}$ 。而：

$$100 * \frac{1024 * 1024}{p} + p + 100 \geq \sqrt{\frac{100 * 1024 * 1024}{p}} + 100 = 20580\text{byte}$$

当且仅当  $\frac{100 * 1024 * 1024}{p} = p$  时成立，即  $p=10240\text{byte}$ 。

相应包括开销 1000---1101100，5000---1025100，20000---1025100，40000---1042600

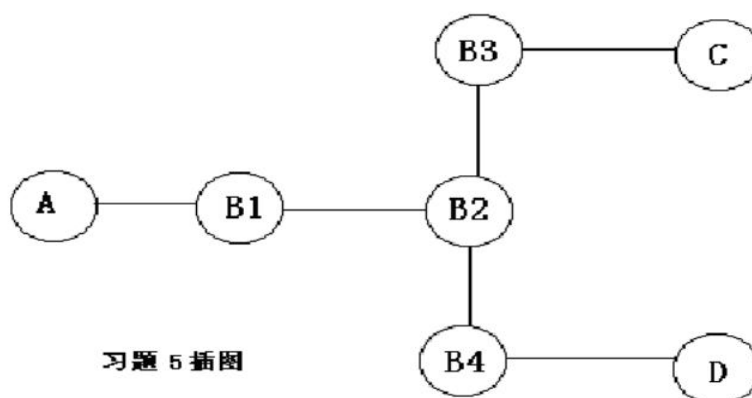
开销就减去 1000\*1000

二、考察下图中示出的透明桥接器的布局。假定开始时所有的转发表都是空的，试给出在下列的传输序列之后，桥接器 B1-B4 中的每一个的转发表的内容：

\*A 给 C 传送

\*C 给 A 传送

\*D 给 C 传送



要求在表中用可以从一个端口可以直接到达的那个邻居节点来标识该端口，例如，B1 的两个端口可标识为 B1 的 A 端口和 B1 的 B2 端口。

解答：当 A 给 C 传送时，所有的桥都看到了分组，知道 A 在哪里。然而，当随后 C 给 A 发送时，分组经过已知路径 B3-B2-B1 直接前往 A，B4 不知道 C 在哪里。类似地，当 D 给 C 发送时，分组经 B4 传播到 B2 后，经已知路径 B2-B3 直接前往 C，B1 不知道 D 在哪里。所以现在

桥接器 B1-B4 中的每一个的转发表的内容分别为：

桥 B1：目的地 A 一端口 A，目的地 C 一端口 B2（无 D）

桥 B2：目的地 A 一端口 B1，目的地 C 一端口 B3，目的地 D 一端口 B4

桥 B3：目的地 A 一端口 B2，目的地 C 一端口 C，目的地 D 一端口 B2

桥 B4：目的地 A 一端口 B2，目的地 D 一端口 D（无 C）

**三、什么是对称加密算法？什么是非对称加密算法？各自优缺点是什么？RSA 是对称加密算法还是非对称加密算法？假定在 RSA 算法中，两个质数  $p=3$ ， $q=5$ ，求解对明文 10 加解密的全过程。**

答：（1）对称加密算法：单密钥加密算法，用同一个密钥对信息进行加密和解密。

优点：加解密速度快。

缺点：密钥管理量大；密钥传输信道要求更高安全性；数字签名验证的问题

（2）非对称加密算法：有两个密钥，一个公钥，一个私钥，发信者用收信者的公钥加密的密文只有收信者的私钥可以解密，发信者用自己的私钥加密的数字签名只有拥有自己公钥的收信者才能解密以此验证数据是否被篡改。

优点：加密和解密能力分开，私钥无法推出公钥；多个用户加密的消息只能由一个用户解读，从而实现公共网络中的保密通信；保证数字签名的验证使得用户能够知道数据是否被他人篡改；无需事先分配密钥，大大减少密钥持有量。

缺点：加解密速度慢。

**【附加】**相对于单钥加密，公钥加密需要保存的密钥数目非常少（只需要只需要保存自己的公私钥对就可以）；相对于公钥加密，单钥加密的效率非常的高。

（3）RSA 是非对称加密算法。

（4）公钥（ $e=11$ ,  $n=15$ ）私钥（ $d=3$ ,  $n=15$ ），密文  $C=10$

**【附加课件】**取  $p = 7$ ， $q = 11$ ； $n = p \times q = 77$ ， $z = (p-1) \times (q-1) = 60$

取  $e = 43$ ， $d = 7$  使得  $e \times d \bmod z = 301 \bmod 60 = 1$ ；得到公钥（ $e=43$ ， $n=77$ ），密钥（ $d=7$ ， $n=77$ ）  
设我们的明文为  $M = 42$ ；

加密  $C = M^e \bmod n = 42^{43} \bmod 77 = 14$ ；解密  $M = C^d \bmod n = 14^7 \bmod 77 = 42$

**RSA 算法：**

（1）选择两个大素数， $p$  和  $q$ ，均应大于  $10^{100}$

（2）计算  $n=p \times q$  和  $z=(p-1) \times (q-1)$

（3）选择一个与  $z$  互为质数的数，令其为  $d$

（4）找到一个  $e$  使其满足  $e \times d = 1 \bmod z$

有了这些预先计算好的参数，即可准备开始加密了。

把明文（看为一个比特串）划分为块，使得每个明文报文  $m$  落在  $0 \leq m \leq n$  之间。

这可以通过将明文分成每块有  $k$  位的组来实现，并且  $k$  是使得  $(2^k) < n$  成立的最大整数。

加密一个报文  $m$ ，需计算  $C=(M^e) \bmod n$ ，解密密文  $c$  要计算  $M=(C^d) \bmod n$

实施加密需要  $e$  和  $m$ ，实施解密需要  $d$  和  $m$ 。因此，公开密钥由（ $e$ ， $n$ ）构成，私密密钥由（ $d$ ， $n$ ）或只有  $d$  构成。 $N$  限制明文块的大小。

**四、CDN 通常根据客户端所使用的 DNS 服务器地址，来指定为客户端提供数据的 CDN 服务器，例如，根据？？自动配置的 DNS 服务器，为国科大怀柔校区的客户端选择位于**

怀柔数据中心的服务器,请分析这种用 DNS 服务器地址来为客户端选择 CDN 服务器的  
 优劣势以及如何改进来避免存在的劣势。

答: (1) **优势:** 当用户访问已经加入 CDN 服务的网站时, 首先通过 DNS 重定向技术确定最接近用户的最佳 CDN 节点, 同时将用户的请求指向该节点。可以减轻 local 服务器的负载, 也可以使用户更快速访问到需要的信息, 从而提升用户感知服务质量, 也可以节约成本。

**劣势:** 在 DNS 查询过程中有这样一个问题, 权威服务器接收请求的时候, 只能得到 local DNS 的 IP, 并不知道 client IP。一般如果 Local DNS 设置不当, 例如没有使用当前 ISP 提供的 Local DNS, 这种实现方法可能会误判用户的位置, 从而将用户误导到错误的 CDN 缓存节点, 造成加速效果差的问题。

(2) **避免:** 可以利用 end-user mapping 的技术, 通过 client IP 地址的前缀, 来对 client 进行表示识别。

**五、数据中心网络内部构成一个网络, 请从网络管理, 协议设计的角度, 定性对比数据中心网络和互联网网络。**

答:

互联网网络	数据中心网络
多个自治系统	一个管理域
分布式控制/路由	中心式控制和路由选择
单个最短路径路由	从源到目的有多个路径
难以测量	容易测量, 但是数据量巨大
标准化传输 (TCP、UDP)	多种传输方式 (DCTCP、pFabric、……)
改进需要达成共识	改进不需要达成共识
Network of networks	Backplane of gaint supercomputer

**六、(1) 什么是主动测量, 什么是被动测量, 它们各自的优缺点?**

(2) 什么是链路带宽, 什么是可用带宽?

(3) 打开一个视频网站发现在线视频的加载速度通常达不到家里宽带带宽, 请分析各种可能的原因。

答: (1) **主动测量:** 指由测量用户主动发送探测数据测量, 将探测分组注入网络, 根据测量数据流的传送情况分析网络的性能。**优点: 更有针对性。**使用方便, 适合端到端的网络性能测量, 对于需要关心的内容只要在本地图发送测试包观察网络的响应即可; 由于该方法不涉及用户的网络信息, 所以对用户而言是很安全的。**缺点: 容易有偏采样, 探测数据也有可能对背景流量产生影响。**增加了网络潜在的负载, 尤其是如果测量未经准确设计, 使产生的流量达不到最小。可能会对网络造成较大的影响; 测量数据包对网络行为的影响。

• **被动测量:** 用户被动捕获数据进行测量。通过在网络中的链路或设备 (如路由器, 交换机等) 上借助包被动捕获数据的方式来记录网络流量, 分析流量, 获知网络的性能状况。**优点: 不会对网络背景流量产生影响。**测量的是网络上真正的流量; 能够达到对观察点网络

行为的详尽理解。**缺点：测量没有针对性。**被动测量方式可能要查看网络上的所有数据包，容易捕获网络中的敏感信息，给用户信息的保密和安全带来一定威胁；只能获得网络局部数据，无法了解网络整体状况；测受范围受限。

(2) **链路带宽（容量）**：指该链路上数据报文的最大传输速率，即每秒钟传输的最大字节数。

**可用带宽**：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。也就是指网络在不降低其它业务流的传输速率的情况下，所能提供给一个业务流的最大传输速率。

- (3) a. 该视频网站和家里宽带不是一个运营商，受到限制；  
b. 视频网站给用户做了限制以避免少数人占用了大多数人的资源；  
c. 服务器的带宽不够了；  
d. 其它进程占用了带宽；  
e. 电脑硬件读取和解析的能力限制了加载速度；

[附加]2017.2 请简述一种测量可用带宽的经典算法的工作原理。

1. 探测报文间隔模型：从发送端发送两个连续数据包，设数据包发送的时间间隔为  $T_{in}$ ，接收端接受这对数据包的时间间隔为  $T_{out}$ ，数据包大小为  $L$ ，网络最大带宽为  $C$ ，则可用带宽为  $A=C*(1-(T_{out}-T_{in})/T_{in})$ ；

2. 探测报文速率模型：当测试报文发送速率小于链路可用带宽时，传输时延相对固定，当传输报文发送速率大于链路可用带宽时，网络出现排队现象，传输时延增大，两种状态之间的那个点即为可用带宽。

七

表一、路由转发示意图

Entry No.	Prefix	Interface
1	192. 168. 128. 0/24	A
2	192. 168. 128. 0/20	B
3	192. 168. 192. 0/18	C
4	10. 10. 0. 0/16	D
5	*	E

给定一个路由器转发表如表一所示，路由器收到数据包后，按照最长前缀匹配的方式查找IP地址的相应转发端口，对于如下转发地址，请写出相应的IP转发端口：

- (1) 10. 1. 1. 1  
(2) 192. 168. 240. 1  
(3) 192. 168. 136. 1  
(4) 192. 168. 224. 1  
(5) 192. 168. 128. 1

7. (1) D (2)C (3)B (4)C (5)A

## 八、TCP/IP 体系结构对移动性支持不好的主要原因是什么？为什么？如何解决？

答：（1）原因：a. IP 地址的二义性，IP 地址即表示地址，又标识主机，即位置和身份的紧耦合；b. 不支持身份和地址的动态绑定，当移动后，IP 地址发生变化。

（2）因为连接和 IP 地址绑定，当 IP 地址变化时，连接只能断开。我们在移动的过程中会改变位置但不会改变身份，而 IP 由于位置和身份的紧耦合导致不能单独改变位置或者身份，又不能动态更新位置和身份的耦合关系，因此 TCP/IP 体系结构对移动性支持不好。

（3）解决方法：1）. Mobile IP 技术。假设移动主机有一个永久的 IP 地址，称为本地地址（home address），作为 identifier，与移动前的网络拥有相同的前缀。主机移动到新的网络时，获得新的 IP 地址，作为 locator。两个地址可以共存，locator 负责接收数据，identifier 负责解复用数据。2）. 连接和 IP 地址解绑定，当 IP 地址发生变化时，移动一方通告对方自己新的地址，两端的应用连接不断开。3）. 使用 NDN 等类似机制。

## 九、Timeout Retransmission（超时重传）对 TCP 传输性能的影响体现在哪几个方面？为什么说超时重传对?? 大宽、高延时（RTT）的网络影响最大？是否可以直接减小 RT0 时间来减小超时重传的影响？

答：[待校正]（1）RTO 可能是 RTT 的几个数量级以上，在 RTO 时间内不能传输数据，因此将会使发送端经较长时间等待才能发现报文段丢失，降低了连接数据传输的吞吐量。此外，超时重传会导致进入 slow start。

（2）TCP 根据得到的 RTT 值更新 RTO 值，发送端对每个发出的数据包进行计时，如果在 RTO 时间内没有收到所发出的数据包对应的 ACK，则任务数据包丢失，将重传数据，若 RTO 较大，则系统在长时间内无法发送数据包，此时若系统的带宽也很大，则造成了资源的大量浪费。

（3）不能直接减小。因为若 RTO 过小，发送端尽管可以很快得检测出报文段的丢失，但也可能将一些延迟大的报文段误认为是丢失，造成不必要的重传，浪费了网络资源。

## 十、考虑下图所示的子网，使用距离向量路由选择，下列向量刚刚被路由 C 收到：

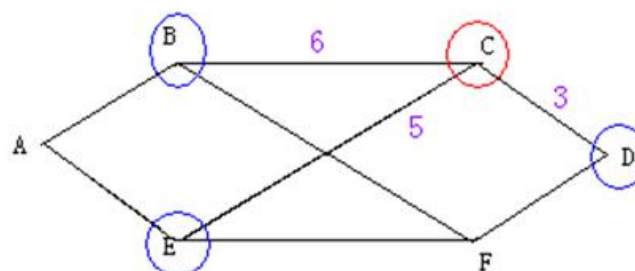
来自 B: (5, 0, 8, 12, 6, 2)

来自 D: (16, 12, 6, 0, 9, 10)

来自 E: (7, 6, 3, 9, 0, 4)

路由器 C 测量到达 B、D 和 E 的延时分别等于 6、3 和 5。试问路由器 C 的新路由表是什么？

请给出所使用的输入线路和所预期的延时。



答： 通过 B 给出 (11, 6, 14, 18, 12, 8)

通过 D 给出 (19, 15, 9, 3, 12, 13)

通过 E 给出 (12, 11, 8, 14, 5, 9)

取到每一个目的地的最小值 (C 除外) 得到: (11, 6, 0, 3, 5, 8)

所以 C 得路由表及输出路线和对应代价如下所示:

目的地	下一主机	代价	路径
A	B	11	C-B-A
B	B	6	C-B
C	C	0	C
D	D	3	C-D
E	E	5	C-E
F	B	8	C-B-F

**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。

**2017.2 一个“客户-服务器”系统的性能收到两个网络因素的影响: 网络带宽 (每秒传输多少位) 和延迟 (第 1 位从客户传播到服务器要花多少秒的时间)。(1) 带宽和延迟成反比关系吗? 如果是, 请阐述其关系; 如果不是, 请给出一个具有高带宽, 高延迟的网络的例子, 再给出一个具有低带宽低延迟的网络的例子。(2) 除了带宽和延迟, 还需要什么其他的参数, 才能很好的刻画一个用于视频传输网络所提供的服务质量?**

答: (1) 带宽与延迟不成反比。高带宽高延迟: 卫星链路; 低带宽低延迟: 56kbps 调制解调器。横贯大陆的光纤连接可以有很多千兆位/秒带宽, 但是由于光速度传送要越过数千公里, 时延将也高。相反, 使用 56 kbps 调制解调器呼叫在同样大楼内的计算机则有低带宽和较低的时延。

(2) 还需要启动时间、缓冲时间、卡顿率等。

丢包率, 网络中数据的传输是以发送和接收数据包的形式传输的, 理想状态下是发送了多少数据包就能接收到多少数据包, 但是由于信号衰减、网络质量等等诸多因素的影响下, 可由丢包率来判定视频传输质量, 丢包率越小, 则该网络质量越好。

**2017.3 在标准的 TCP 实现中, TCP 连接空闲多长时间就会在下次发送数据包时, 触发慢启动 (简称 SSAI)? 请简述此时重新从慢启动开始的原因。是否可以把 SSAI 直接关闭掉, 请简述原因。**

答: (1) 1 个 RTT。

(2) 重启慢启动是需要重新探索可用带宽。慢启动的目的是, 使 TCP 在用拥塞避免探寻更多可用带宽之前得到 cwnd 值, 以及帮助 TCP 建立 ACK 时钟。通常, TCP 在建立新连接时执行慢启动, 直至有丢包时, 执行拥塞避免算法进入稳定状态。在传输初始阶段, 由于未知网络传输能力, 需要缓慢探测可用传输资源, 防止短时间内大量数据注入导致拥塞。慢启动算法正是针对这一问题而设计。在数据传输之初或者重传计时器检测到丢包后, 需要执行慢启动。

(3) 两种答案: 1. 可以。因为这样可以节省吞吐率从 0 增长到可用带宽的时间。

2. 不可以。因为在一个 RTT 时间内, 有可能有新建的流占用了已有带宽, 这时用原来的窗口大小 (发送速率) 会导致拥塞。(回答一种即可)

2017.4 在数据中心网络中，多个发送端向一个接受端发送数据时，会带来 TCP Incast 问题。请简述 TCP Incast 问题发生的原因，以及可能的解决方案。

答：（1）TCP Incast 问题当多条并发流到达同一交换机设备时，突发流量容易造成丢包。

从根本上来讲是由于传统的 TCP/IP 协议在设计之初针对的是带宽较低、延迟较大、地理分布广泛而连接较为稀疏的互联网，而 TCP 协议不能很好地适应数据中心网络高带宽、低延时、地理分布集中而连接密集的特点。

（2）解决思路：1. 增加设备缓冲区的大小。

2. 往中间设备增加通知功能，通过显示通知发送方哪些数据包丢失，尽快回复丢包。

在数据中心的链路层，**拥塞通知**和**流控**是缓解 TCP Incast 问题的两个主要方法。

传输层缓解或解决 TCP Incast 问题的解决方案主要分为三大类：

（1）参数调整。改善 DCN 中 TCP 重传的机制，使得重传尽快执行，提升吞吐量。

（2）传输机制优化。通过改进拥塞控制，尽量避免或减少瓶颈链路交换机缓存区占满的情况，减少丢包，降低 TCP Incast 问题发生概率。

（3）协议替换。通过采用其他传输协议，从根本上解决该问题中 TCP 协议带来的弊端。

2017.5 下图是 OpenFlow 局域网络拓扑，S1 的流表包含一条转发规则，Controller 持有全局网络的拓扑信息，请描述 Packet 1 从 C1 到 H2 的转发过程，包含流表查询、流表安装流程以及具体的流表转发规则。

答：步骤如下：

1) 首先，数据从 C1 唯一的端口发出，发到 S1；

2) S1 查询流表，匹配不到对应条目，因此该数据包缓存下，并查询 Controller。

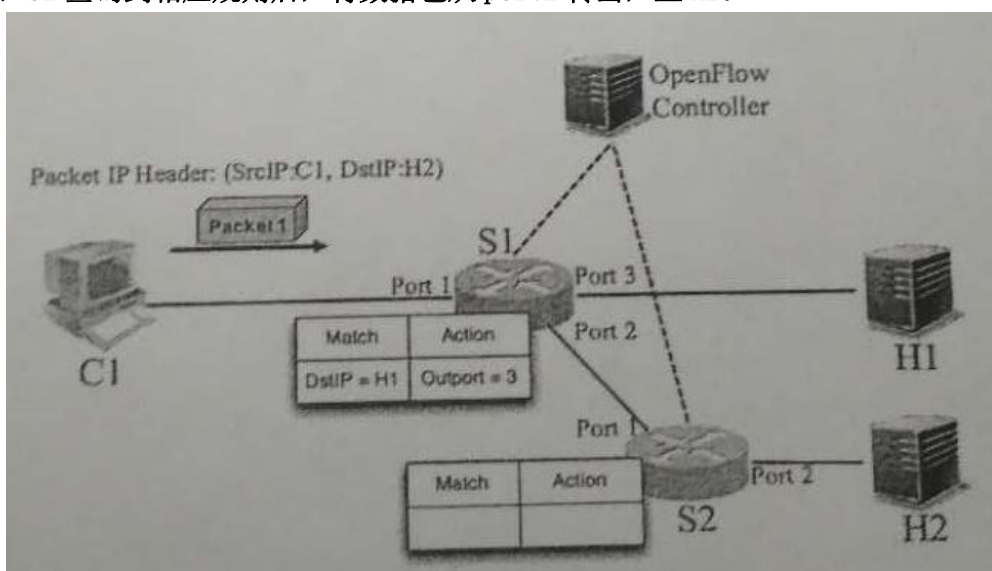
3) Controller 下发规则至 S1，规则内容为：“DstIP=H2, Outport=2”。

4) S1 按照相应规则，将数据包从 PORT2 转出，至 S2

5) S2 收到数据包后，找不到对应规则，因此也将该数据包缓存下，并查询 Controller

6) Controller 下发规则至 S2，规则内容为 DstIP=H2, output=2

7) S2 查询到相应规则后，将数据包从 port2 转出，至 H2。



**题目 2: 为什么 RSA 算法是有效的非对称加密算法? 什么是数字签名? 数字签名认证的过程是什么?**

**有效的非对称加密算法:** 因为即使我们有了公钥  $(e, n)$ , 我们很难找到其对应的私钥  $(d, n)$  要得到私钥, 我们需要知道  $z = (p-1)*(q-1)$ , 即必须将  $n$  分解为  $p*q$  而当  $p, q$  为大质数时, 除了试除法, 没有更有效的方法能将  $n$  分解. 大数分解难题产生的不对称性也就是 RSA 算法的理论基础

**数字签名:** 设计一个代替手迹签名的方案, 从根本上说, 我们需要这样一个系统, 一方通过该系统能以如下方式向另一方发送已签名的文件: (1) 接收方能够验证出发送方所宣称的身份; (2) 发送方以后不能否认报文是他发的; (3) 接收方不能伪造对报文的签名。

**过程:** 1. 共享你的公钥; 2. 对你的数据进行哈希; 3. 把哈希值用私钥进行加密; 4. 收信者对哈希值用私钥进行解密; 5. 把接收的数据进行哈希, 把解密后的哈希值对比, 判断数据是否被篡改。

**题目 3: 什么是 Qos? IP Qos 的目标是什么? Qos 有哪三种服务类型? 典型的 Qos 机制有哪些?**

**QoS (Quality of Service)** 即服务质量

网络业务: 带宽、时延、丢包率等。

**IP QoS 目标:** 避免并管理 IP 网络拥塞; 减少 IP 报文的丢失率; 调控 IP 网络的流量; 为特定用户或特定业务提供专用带宽; 支撑 IP 网络上的实时业务

通常 QoS 提供以下三种服务模型:

**Best-Effort service (尽力而为服务模型)** Best-Efforts 是一个单一的服务模型, 也是最简单的服务模型。对 Best-Effort 服务模型, 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。

**Integrated service (综合服务模型, 简称 Int-Serv)** Best-Effort 服务模型是网络的缺省服务模型, 通过 FIFO 队列来实现。它适用于绝大多数网络应用, 如 FTP、E-Mail 等。

优点: 能够提供绝对有保证的 QoS

缺点: 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

**Differentiated service (区分服务模型, 简称 Diff-Serv)** Best-Effort 服务模型实质上并不属于 QoS 的范畴, 因为在转发尽力而为的通信时, 并没有提供任何服务或者传送保证。优点: 扩展性好, 简单可实现, DS 标记只是规定了有限数量的业务级别, 状态信息的数量正比于业务级别, 而不是流的数量; 具有层次化结构, 不同区域有不同的服务提供策略; 不影响路由, 仅限于队列调度与缓冲管理

缺点: 仅实现粗略的分等级服务; 本质上是一种相对优先级策略, 不能保证端到端 QoS 性能; 组件分散, 需要协同一致、统一策略和管理

**Qos 模型选择:** IntServ: 精细粒度, 严格质量保证, 网络的核心复杂, 需要路由器之间的信令, 扩展性差, 面向连接的 QoS。 DiffServ: 粗略粒度, 相对质量保证, 网络的边缘复杂, 不需要信令, 扩展性好, 面向分组的 QoS

**典型的 QoS 机制:** 流量分类和标记; 拥塞管理和调度策略; 流量监管与流量整形

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

每个端口都有自己的软件队列和硬件队列。硬件队列 (transmit queue, or TxQ) 永远使用 FIFO 队列。软件队列根据不同的系统版本和硬件平台有不同的选择和配置。每种队列机制

有三个组成部分:分类 排队策略 服务策略

#### **题目 4: 什么是 RSVP 协议? 它的协议特点是什么?**

**RSVP** (资源预留协议, RFC2205), Int-Serv 服务模型在发送报文前, 需要向网络申请特定的服务。这个请求是通过 RSVP 信令来完成的。RSVP 运行在从源端到目的端的每个设备上, 可以监视每个流, 以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量, 为网络提供最细粒度化的服务质量区分。

**协议特点:** 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。

#### **题目 5: 什么是网络攻击? 网络攻击主要分为哪几种?**

**网络攻击**指的是利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及其系统中的数据进行攻击。

**主动攻击**会导致某些数据流的篡改和虚假数据流的产生。这类攻击可分为篡改、伪造消息数据和终端, 拒绝服务。

**被动攻击**中攻击者不对数据信息做任何修改, 截取/窃听是指在未经用户同意的情况下攻击者获得了信息。通常包括窃听、流量分析、破解弱加密的数据流等攻击方式。

**口令入侵**是指使用某些合法用户的帐号和口令登录到目的主机, 然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的帐号, 然后再进行合法用户口令的破译。

**特洛伊木马:** 放置特洛伊木马程序能直接侵入用户的计算机并进行破坏, 常被伪装成工具程式或游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载, 一旦用户打开了这些邮件的附件或执行了这些程序之后, 就会在自己的计算机启动时悄悄执行的程序。

**Web 欺骗**是一种电子信息欺骗, 攻击者在创造了整个 Web 世界的一个令人信服但是完全错误的拷贝。攻击者控制着错误的 Web 站点, 这样受攻击者浏览器和 Web 之间的所有网络信息完全被攻击者所截获。

**网络监听**是主机的一种工作模式, 在这种模式下, 主机能接收到本网段在同一条物理通道上传输的所有信息, 而不管这些信息的发送方和接收方是谁。

**DoS 攻击**是指故意的攻击网络协议实现的缺陷或直接通过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, 使目标系统服务系统停止响应甚至崩溃。

#### **题目 6: 什么是区块链? 它的技术本质与核心价值是什么? 核心特性? 应用范围?**

**区块链**是一种传递信任的技术体系, 是实现价值点对点传递及信任全网络多层级传递的技术体系, 由多中心网络取代中心机构进行记账, 是一种分布式记账, 不依赖单个中心。

**技术本质:** 区块链 (Block chain) 是一种创新的分布式交易验证和数据共享技术, 也被称为分布式账本技术。

**宏观本质:** 分布式平等部署系统; 全网节点协作完成交易验证和存储; 无单一控制中心;

**微观本质:** 数据存储于块 (Block) 中, 块在逻辑上串联起来构成链条 (Chain); 应用数字签名与完整性校验保证块数据的真实性、时序性、完整性; 在技术层面具有不可伪造、不可抵赖、不可篡改、不可撤销等属性, 在应用层面具有分布式的公开透明、交易可跟踪等特征; 区块链并非某项特定技术, 实际是一种技术组合, 是一种实践创新/组合创新/集成创新。

**核心价值:** 区块链通过构建 P2P 自组织网络、时间有序不可篡改的密码学共享账本、分布式共识机制, 从而实现去中心化信任。

**核心特性:** 多中心、共同维护、时序数据、安全可信、可编程、共建共享

**应用范围:** 金融领域、供应链管理、版权交易、物联网、医疗&慈善