计算机保研面试 计算机网络常见题

计算机保研面试_计算机网络常见题

- 1 计算机网络体系结构
 - (1) OSI 和TCP/IP 模型各个层之间的协议和功能
 - (2) 计算机网络为什么要分层
 - (3) 时延有哪些
 - (4) 计算机网络和分布式系统的异同

2应用层

- (1) 网络应用模型有哪些,优缺点
- (2) DNS 域名解析的过程
- (3) 为什么 DNS 采用分布式层次数据库
- (4) HTTP 和 HTTPS
- (5) 点击一下网页会发生什么
- (6) Cookie 和 Session 有什么区别
- (7) 微信撤回机制

3 传输层

- (1) TCP 和UDP 的异同点
- (2) 三次握手和四次挥手的过程
- (3) 为什么握手要三次,挥手要四次
- (4) 为什么四次挥手时,客户端在发送 ACK 后需等待 2MSL
- (5) TCP 如何保证可靠传输
- (6) TCP 的流量控制
- (7) TCP 拥塞控制
- (8) TCP 的流量控制和拥塞控制有什么异同

4网络层

- (1) 路由器有什么作用
- (2) 路由算法有哪些
- (3) DHCP 协议
- (4) ICMP 协议
- (5) ipv6出现的动力是什么,报文头哪些字段发生了变化

5 数据链路层

- (1) IP 地址和 MAC 地址的区别
- (2) ARP 协议

1 计算机网络体系结构

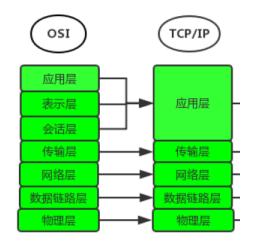
(1) OSI 和TCP/IP 模型各个层之间的协议和功能

- 应用层:为应用程序提供数据传输服务,数据单位为报文。协议有 HTTP、DNS、FTP、SMTP
- 传输层: 为进程提供端到端的数据传输服务,包括复用/分用、可靠数据传输、流量控制、差错控制等,数据单位为报文段。协议有TCP、UDP
- 网络层: 为**主机**提供数据传输服务,包括**IP选址、路由选择**等,数据单位为**数据报**。协议有 IP、ICMP
- 数据链路层:为**同一链路的主机**提供数据传输服务,包括**封装成帧、差错控制、流量控制**等,数据单位为**桢**,协议有 ARP、RARP
- 物理层:在物理介质上传输数据比特流,尽可能屏蔽传输媒介和通信手段的差异,使数据链路层感觉不到这些差异。协议有 IEEE 802

表示层: 数据压缩、加密以及数据描述,这使得应用程序不必关心在各台主机中数据内部格式不

同的问题

会话层:建立并管理会话



(2) 计算机网络为什么要分层

- **各层相互独立**,下层为上层提供服务,上层无需知道下层如何实现,只需使用下层提供的接口,这样可以将复杂的问题**分解**为多个容易处理的**子问题**
- 灵活性好, 当某层需要修改时, 只需保持接口不变, 不影响其他层的使用
- 易于**实现和维护**,整个系统被划分为多个独立的子系统
- 促进**标准化**工作,因为每层的功能及其提供的服务可以通过协议来说明,如RFC文档
- 分层使得计算机网络系统具有很强的可扩展性
- 分层网络协议的设计和实现使得网络运营商、网络设备供应商和网络应用开发商能够**各司其职**,功能分明,有益于网络的推广

(3) 时延有哪些

- 处理时延 (processing delay) : 检查分组头部、差错检测、路由等处理所需的时间
- 排队时延 (queuing delay) : 分组在链路上等待传输时所需的时间
- 传输时延(transmission delay):将所有分组的比特推向链路所需的时间
- 传播时延(propagation delay):从当前链路起点到下一个路由器传播所需要的时间

(4) 计算机网络和分布式系统的异同

- 同:
 - 分布式系统是建立在计算机网络之上的,他们在**物理结构**上基本相同
 - 他们都具有通信和资源共享的功能
- 异:
 - o 计算机网络是分布式系统的**基础**,分布式系统是计算机网络技术发展的高级阶段(**应用**)

他们的区别主要在高层软件上,分布式系统是建立在网络上的软件系统,用户不必关心网络环境中的资源分布和联网计算机的差异

2应用层

(1) 网络应用模型有哪些,优缺点

- C/S: 有一个主机作为服务器,负责接受客户端的请求
 - 优点:随时提供服务、方便管理
 - 缺点:可扩展性差、服务器压力、会出现单点失效问题
- P2P: 每个主机既是客户端, 又是服务器
 - 优点:减轻了服务器的压力,提高了资源利用效率;可扩展性好;网络鲁棒性强,不会出现单点 失效问题;去中心化
 - 缺点:消息延迟(消息是随机转发给其他节点,需多次转发才能到达)、消息重复(每个节点都转发,会重复收到消息)、不方便管理

(2) DNS 域名解析的过程

- 域名解析协议,将域名映射成为IP,基于 UDP 协议
 - 1. 客户端在**本地缓存**中查找,如果没有找到,则将查询请求发给 DNS 服务器

- 2. 首先发送给**本地 DNS 服务器**,本地 DNS 服务器先在管辖的记录表查找,再在缓存中查找。如果 找不到,则本地 DNS 服务器将请求发送给根域名服务器
- 3. 根域名服务器返回下一级域名服务器,再依次递归查询,得到域名对应的 IP 地址

(3) 为什么 DNS 采用分布式层次数据库

集中式的问题包括:单点故障、通信容量有限、远距离的集中式数据库查询慢、不便于维护、可扩展性差

(4) HTTP 和 HTTPS

- HTTP: 超文本传输协议,定义了浏览器怎样向万维网服务器**请求万维网文档**,以及服务器怎样把文档 传送给浏览器,基于 **TCP**
 - HTTP的特点: 无状态(不记录用户访问状态,一般用cookie记录)、可以是持久性连接(所有请求和响应经相同的 TCP 连接发送),也可以是非持久性连接(每个请求/响应对是经一个单独的TCP 连接发送)
- HTTPS: 使用 SSL 协议对 HTTP 传输的数据进行加密, 比较安全

(5) 点击一下网页会发生什么

- DNS 域名解析
- 通过**三次握手**建立 TCP 连接
- 客户端发起 HTTP 请求
- 服务器响应请求
- 浏览器解析 HTML 代码,并请求代码中的资源
- 通过四次挥手断开 TCP 连接

(6) Cookie 和 Session 有什么区别

- 存放位置不同: cookie存放在客户端; session存放在服务器
- 安全性不同: cookie不安全, 别人可以用本地的 cookie 进行非法登录
- 数据大小限制不同: cookie的大小有限制; session没有限制

(7) 微信撤回机制

3 传输层

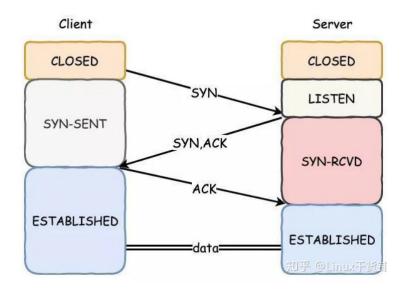
「提供服务:进程之间的逻辑通信、复用和分用、差错检测、面向连接的TCP和无连接的UDP **、特点: 无连接、首部开销小、最大努力交付,应用层要保证可靠性** 首部: 8B, 分别为源端口号、目的端口号、长度、校验和 UDP协议 【校验:采用首部、伪首部、数据进行二进制反码运算求和再取反 符点:有连接、一对一、提供可靠交付、全双工通信、面向字节流 首部: 20B, 源端口、目的端口、序号、确认号等控制信息 连接管理: 三次握手建立, 四次握手释放 (序号: 用来保证数据能有序提交给应用层 确认:确认号为期待收到的下一个报文段第一个字节的序号 传输层 (超时: 计时器到期还没收到确认则重传对应报文 冗余确认。当收到失序报文时向发送端发送冗余ACK TCP协议 流量控制:在确认报文中设置接收窗口rwnd的值来限制发送速率 「原理:根据自己估算的网络拥塞程度设置cwnd的值来限制发送速率 '慢开始: 当cwnd < ssthresh时,每收到一个报文段的确认cwnd加1 拥塞避免: 当cwnd>ssthresh时,每经过一个往返延时cwnd加1 拥塞控制。 快重传: 当收到连续的三个重复的ACK,直接重传对方期待的报文 快恢复: 当收到连续的三个冗余ACK, 令ssthresh=cwnd= cwnd 拥塞处理: ssthresh置为原cwnd的一半, cwnd置1

(1) TCP 和UDP 的异同点

- 同:都是传输层的协议,都是为进程间的端对端数据传输提供服务
- 异:
 - TCP 是面向连接的,需要通过三次握手建立连接,四次挥手接除连接;UDP 是无连接的,即发送数据之前不需要建立连接
 - TCP 是可靠数据传输,它通过超时重传、数据校验等方法来确保无差错; UDP 是不可靠的,会出现丢失、重复等差错
 - o TCP 的资源负载比较大,UDP 的资源负载比较小
 - TCP 由于有流量控制、拥塞控制、超时重传等机制,传输速度比 UDP 慢
 - TCP 的报文段的头部 (20bytes) 比 UDP (8bytes) 的长

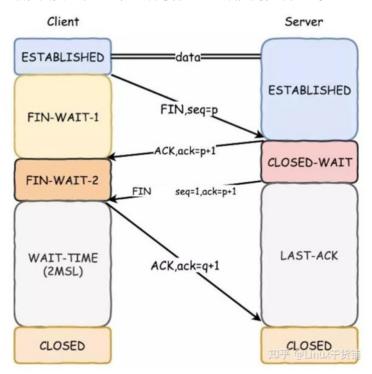
(2) 三次握手和四次挥手的过程

- 三次握手:
 - 。 客户端发送一个SYN报文段,发起TCP连接
 - 。 服务器在收到 SYN 后进行响应, 回复一个 SYN-ACK 报文段
 - 。 客户端在收到服务器的响应后, 回复一个 ACK 报文段, 表示收到



• 四次挥手:

- o 客户端发送 FIN, 准备断开连接
- 。 服务器在收到 FIN 后,回复一个 ACK ,进入**半关闭状态**
- o 待服务器没有向客户端发送的数据时,服务器发送 FIN
- 。 客户端收到 FIN 后,回复一个 ACK,然后等待 2MSL 后关闭,服务器收到 ACK 后也关闭



(3) 为什么握手要三次,挥手要四次

- 三次握手:要保证**连接是双工的**,**至少**要握手 **3 次**。如果握手 2 次,则只能保证服务器能收到客户端的信息,而不能保证客户端能收到服务器的信息;如果握手 4 次,则多余了。
- 四次挥手:还是因为**连接是双工**的,**前两次**只是保证了客户端发送的数据传输完了,**服务器需要等它发送的数据也传输完**,再断开连接。

(4) 为什么四次挥手时,客户端在发送 ACK 后需等待 2MSL

因为网络是不可靠的,客户端回复给服务器的 **ACK 可能会丢失**,如果丢失的话,服务器会重新发送 FIN,客户端需要等一会

MSL指一个片段在网络中最大的存活时间; 2MSL: 发送+回复所需的最大时间

(5) TCP 如何保证可靠传输

- **校验和**机制
- 序列号: TCP 将数据中的每个字节编上序号
- 累积确认:接收方收到数据后,都会发送一个带有期待下一次接收的序号的 ACK
- 超时重传: 发送方每发送一个报文段, 都要设置一次计时器, 如果到一定时间后还未收到 ACK, 则重传
 - 计时器重传间隔一般比 RTT 大一点,TCP 采用**指数加权移动平均**算法估算 RTT

RTT: 往返时间,即一个报文发出的时间与收到对应ACK的时间的间隔

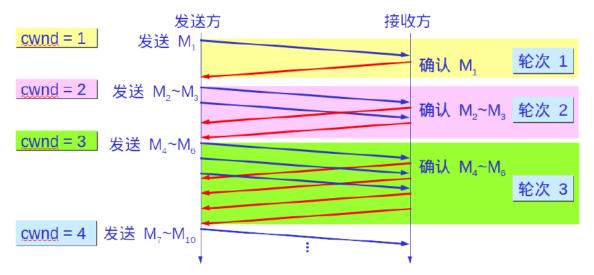
• 快速重传: 防止超时重传周期过大, 发送方如果收到 连续 3 个冗余的 ACK, 则立即重传

(6) TCP 的流量控制

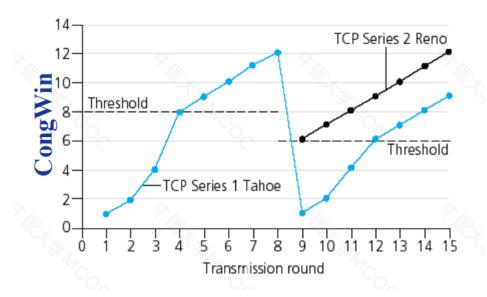
- 作用: 使发送方的发送速率与接收方的应用程序读取**速率相匹配, 防止发送方发得太快**
- 实现:接收方根据自己的接收缓存大小,通过报文段头部的**接收窗口** rwnd 字段,动态地调整发送方的发送速率

(7) TCP 拥塞控制

- 拥塞控制:发送方根据通信的时延,估算出网络的拥塞程度,计算一个**拥塞窗口** cwnd,来减小发送速率,**防止网络中的路由器或链路过载**
 - 慢启动: TCP 连接刚建立时,设置拥塞窗口为 1 MSS;之后每收到一个新的 ACK,拥塞窗口就加 1,这样的话,每个 RTT 内拥塞窗口就呈指数增加;当拥塞窗口达到一个阈值时,进入拥塞避免阶段



- 拥塞避免: 每经过一个往返时延RTT, 拥塞窗口就增加一个MSS, 即线性增长; 当出现超时(网络拥塞)时, 让慢启动阈值等于当前拥塞窗口的一半, 并进入慢启动阶段
- 快速恢复: 发送方收到**连续 3 个冗余ACK**时,让慢启动阈值等于当前拥塞窗口的一半,**当前窗口** 再减半,并进入**拥塞避免**阶段
- 快速重传: 防止超时重传周期过大, 发送方如果收到 连续 3 个冗余的 ACK, 则立即重传



(8) TCP 的流量控制和拥塞控制有什么异同

- 同:都是通过改变发送方的发送速率,以此达到控制的
- 异:
 - 流量控制解决的是发送方和接收方速率不匹配的问题,是通过接收窗口来实现的
 - 拥塞控制解决的是避免**网络负载过大**的问题,是通过拥塞窗口来实现的

4 网络层

′功能,异构网络互联、路由与转发、拥塞控制 路由算法 {静态:由网络管理员手工配置路由信息 动态:通过路由器间彼此交换的信息来构造路由表,分为距离-向量和链路状态算法 概念:将互联网分成许多较小的自治系统,系统有权决定自己内部采用什么路由协议 协议 {内部网关协议: 自治系统内部使用的网关协议,如RIP、OSPF 层次路由 外部网关协议:自治系统之间使用的网关协议,如BGP4 首部: 固定部分共20B, 其中首部长度、总长度和片偏移的基本单位分别为4B、1B、8B NAT: 实现专用网络地址和公用网络地址之间的相互转换 子网划分: 采用子网掩码对物理子网再一次进行子网划分 CIDR: 在变长子网掩码的基础上提出的一种消除传统A、B、C类网络划分 「概念:将网络前缀都相同的连续的IP地址组成"CIDR地址块" IPv4 路由聚合 {目的: 使得一个地址块可以表示很多地址,减少路由表表项和路由器间的信息交换 方法。把一串IP地址都写为二进制表示,取最长的公共前缀作为网络号 网络层 (ARP:对于特定的IP地址,查询其对应的物理地址 协议 ₹DHCP: 给网络中的主机动态的分配IP地址 (ICMP: 用来给主机或路由器报告差错和异常情况 IPv6: 首部40B, 地址长度16B, 主要用于解决IPv4的地址耗尽问题 AIGP RIP协议:基于距离向量路由选择协议,使用UDP,与相邻路由器交换整个路由表OSPF协议:基于链路状态路由算法,使用IP,与全部路由器交换相邻结点链路状态 (EGP:BGP协议:基于路径向量路由选择协议,使用TCP,寻找的并非最佳路由 IP组播:在发送者和每一接收者之间实现点对多点网络连接,应用UDP协议,使用D类地址 (概念: 移动节点以固定的网络IP地址,实现跨越不同网段的漫游功能 【组成: 移动结点、本地代理、外部代理 「特点:可以用来连接异构网络,完成路由转发,能隔离冲突域和广播域,依照IP地址转发 (控制部分:路由选择处理机,根据路由协议构造与维护路由表 分组转发部分:交换结构、一组输入端口和一组输出端口

(1) 路由器有什么作用

• 路由选择:根据路由协议构造出路由表,确定分组从源主机到目的主机的最佳路径

• 分组转发:根据转发表,将分组从路由器的输入端口转移到合适的输出端口

(2) 路由算法有哪些

- 链路状态路由算法 (如 OSPF 算法)
- 距离-矢量路由算法(如 RIP 算法)
- **层次路由**:将网络分为若干个自治系统,同一自治系统内的路由器运行相同的路由协议。每个自治系统有一些**网关路由器**,负责自治系统之间的路由。
 - o 内部网关协议: 自治系统内的路由协议, 如 OSPF、RIP
 - 。 外部网关协议: 自治系统间的路由协议, 如 BGP

(3) DHCP 协议

- 动态主机配置协议,即插即用,如手机带在身上,移动一定距离后,需要接入新的路由或者基站,IP 地址就自动更新了
- 协议过程: 手机先播 DHCP 发现报文,服务器响应一个DHCP提供报文,手机再请求 IP 地址,最后服务器发送一个 ACK,携带有分配的 IP 地址

(4) ICMP 协议

互联网控制报文协议,用于差错检验和网络探询,如 ping

(5) ipv6出现的动力是什么,报文头哪些字段发生了变化

- 动机: IPv4 的 IP 地址数量不够用了、改进报文头, 加快转发速率
- 报文头: 20字节-->40字节、源地址和目的地址从32位-->128位, 去除了校验和

5 数据链路层

(1) IP 地址和 MAC 地址的区别

- IP 地址是**网络**层的地址,是分层次的;MAC 地址是**数据链路**层的地址,是平面式的
- IP 地址是逻辑地址; MAC地址是物理地址
- IP 地址不具备唯一性; MAC**地址具有唯一**性
- MAC 帧中封装了 IP 数据报

(2) ARP 协议

- 解决的问题:在**同一个局域网**内,如何在**已知**目的接口的 **IP** 的情况下,**确定其 MAC** 地址
- ARP 是一个**即插即用**的协议,每个节点(主机或路由器)维护一个 ARP 表,存放节点的 **IP/MAC 映射 关系**;假设 A 要给 B 发一个数据,则 A **广播**一个分组,其中包含 B 的 IP,B 接收到后,IP 匹配成功,向 A 回复其 MAC 地址,A 将该 IP/MAC 映射信息记录下来。