计算机网络

五层协议的体系结构分别是什么？每一层都有哪些协议?

- 技术点：网络模型、协议
- 思路：分条解释每层名字以及协议
- 参考回答：

    - 物理层
    - 数据链路层：逻辑链路控制LLC、媒体接入控制MAC
    - 网络层：IP协议、地址解析协议ARP、逆地址解析协议RARP、因特网控制报文协议ICMP
    - 传输层：传输控制协议TCP、用户数据报协议UDP
    - 应用层：文件传输协议FTP、远程登录协议TELNET、超文本传输协议HTTP、域名系统DNS、简单邮件协议SMTP、简单网络管理协议SNMP

TCP和UDP的区别?

- 技术点：传输层协议对比
- 参考回答：

    - TCP传输控制协议：面向连接；使用全双工的可靠信道；提供可靠的服务，即无差错、不丢失、不重复且按序到达；拥塞控制、流量控制、超时重发、丢弃重复数据等等可靠性检测手段；面向字节流；每条TCP连接只能是点到点的；用于传输可靠性要求高的数据
    - UDP用户数据报协议：无连接；使用不可靠信道；尽最大努力交付，即不保证可靠交付；无拥塞控制等；面向报文；支持一对一、一对多、多对一和多对多的交互通信；用于传输可靠性要求不高的数据

拥塞控制和流量控制都是什么，两者的区别?

- 技术点：拥塞控制、流量控制
- 参考回答：

    - 拥塞控制：对网络中的路由和链路传输进行速度限制，避免网络过载；包含四个过程：慢启动、拥塞避免、快重传和快恢复
    - 流量控制 ： 对点和点/发送方和接收方之间进行速度匹配，由于接收方的应用程序读取速度不一定很迅速，加上缓存有限，因此需要避免发送速度过快；相关技术：TCP滑动窗口、回退N针协议

谈谈TCP为什么要三次握手？为什么要四次挥手?

- 技术点：TCP可靠保证
- 参考回答：
- （1）建立TCP连接：TCP的三次握手

    - 客户端向服务端发送一个表示建立连接的报文段SYN报文段；一旦包含SYN报文段的IP数据报到达服务器主机，服务器从IP数据报中提取出TCP、SYN报文段，为该TCP连接分配需要的缓存和变量，并向客户端发送表示允许连接的报文段ACK；在收到ACK报文段之后，客户端也要给该连接分配缓存和变量，客户端向服务器再发送一个报文段ACK，表示对允许连接的报文段进行了确认。自此完成一次TCP连接。
    - 第三次握手可以避免由于客户端延迟的请求连接的请求，使得服务端无故再次建立连接。

- 断开TCP连接：TCP的四次挥手

    - 由于TCP连接是全双工的，因此每个方向都必须单独关闭。客户端在数据发送完毕后发送一个结束数据段FIN，且服务端也返回确认数据段ACK，此时结束了客户端到服务端的连接；然后客户端接收到服务端发送的FIN，且服务端也收到了ACK之后，自此双方的数据通信完全结束。简单说来是“先关读，后关写”，一共需要四个阶段：服务器读通道关闭->客户机写通道关闭->客户机读通道关闭->服务器写通道关闭。

播放视频用TCP还是UDP？为什么？

- 技术点：传输层协议适用场景
- 参考回答：播放视频适合用UDP。UDP适用于对网络通讯质量要求不高、要求网络通讯速度能尽量快的实时性应用；而TCP适用于对网络通讯质量有要求的可靠性应用。而且视频区分关键帧和普通帧，虽然UDP会丢帧但如果只是丢普通帧损失并不大，取而代之的是高速率和实时性。
- 引申：TCP、UDP适用的场景

Http，了解哪些响应状态码？

- 技术点：响应状态码
- 思路：
- 参考回答：状态码由三位数字组成，第一位数字表示响应的类型，常用的状态码有五大类：

    - 1xx：表示服务器已接收了客户端请求，客户端可继续发送请求
    - 2xx：表示服务器已成功接收到请求并进行处理

        - 200 OK：表示客户端请求成功

    - 3xx：表示服务器要求客户端重定向

    - 4xx：表示客户端的请求有非法内容

        - 400 Bad Request：表示客户端请求有语法错误，不能被服务器所理解
        - 401 Unauthonzed：表示请求未经授权，该状态代码必须与 WWW-Authenticate 报头域一起使用
        - 403 Forbidden：表示服务器收到请求，但是拒绝提供服务，通常会在响应正文中给出不提供服务的原因
        - 404 Not Found：请求的资源不存在，例如，输入了错误的URL

- 5xx：表示服务器未能正常处理客户端的请求而出现意外错误
    - 500 Internal Server Error：表示服务器发生不可预期的错误，导致无法完成客户端的请求
    - 503 Service Unavailable：表示服务器当前不能够处理客户端的请求，在一段时间之后，服务器可能会恢复正常

get和post的区别?

- 技术点：HTTP请求方法
- 参考回答：
    - GET：当客户端要从服务器中读取某个资源时使用GET；一般用于获取/查询资源信息；GET参数通过URL传递，传递的参数是有长度限制，不能用来传递敏感信息
    - POST：当客户端给服务器提供信息较多时可以使用POST；POST会附带用户数据，一般用于更新资源信息；POST将请求参数封装在HTTP 请求数据中，可以传输大量数据，传参方式比GET更安全

HTTP1.0、HTTP1.1、HTTP2.0的区别?

- 技术点：HTTP协议发展
- 参考回答：
- （1）HTTP1.0和HTTP1.1的区别：
    - HTTP1.0默认使用短连接，HTTP1.1开始默认使用长连接
    - HTTP1.1增加更多的请求头和响应头来改进和扩充HTTP1.0的功能，比如身份认证、状态管理和Cache缓存等
- （2）HTTP2.0和HTTP1.X相比的新特性：
    - 新的二进制格式：HTTP2.0的协议解析决定采用二进制格式，实现方便且健壮，不同于HTTP1.x的解析是基于文本
    - 多路复用：连接共享，即每一个request都是是用作连接共享机制的
    - 服务端推送：服务器主动向客户端推送消息

HTTP和TCP的区别

- 技术点：HTTP、TCP
- 参考回答：
    - TCP是传输层协议，定义数据传输和连接方式的规范。通过三次握手建立连接、四次挥手释放连接。
    - HTTP是应用层协议，定义的是传输数据的内容的规范。HTTP的连接使用"请求-响应"方式。基于TCP协议传输，默认端口号是80。

HTTP和HTTPS的区别

-技术点：HTTP、HTTPS - HTTP（超文本传输协议）：运行在TCP之上；传输的内容是明文；端口是80 -

HTTPS（安全为目标的HTTP）：运行在SSL/TLS之上，SSL/TLS运行在TCP之上；传输的内容经过加密；端口是443

HTTP和Socket的区别

- 技术点：HTTP、Socket
- 参考回答：
    - HTTP是应用层协议；基于TCP协议；使用“请求—响应”方式建立连接，在请求时需要先建立连接且客户端要先发出请求，可见服务器需要等到客户端发送一次请求后才能将数据传回给客户端
    - Socket（套接字）是对TCP/IP协议的封装，是接口而不是协议；创建Socket连接时可以指定传输层协议TCP或UDP；Socket建立连接过程三步骤：服务器监听->客户端请求->连接确认，可见服务器可以直接将数据传送给客户端（HTTP2.0也增加了服务端推送的功能）