1. OSI与TSP/IP各层的结构与功能，都有哪些协议？
2. 计算机网络体系结构

应用层🡪表示层🡪会话层🡪运输层🡪网络层🡪数据链路层🡪物理层

1. TCP/IP的四层协议

应用层（FTP\SMTP）🡪运输层（TCP或UDP）🡪网络层IP🡪网络接口层

五层协议

1. **应用层🡪运输层🡪网络层🡪数据链路层🡪物理层**
   1. 应用层

任务是通过应用进程间的交互来完成特定网络应用。应用层协议定义的是应用进程间的通信和交互的规则。对于不同的网络应用需要不同的应用层协议。

在互联网中应用层协议很多，**如域名系统DNS，支持万维网应用的HTTP协议，支持电子邮件的SMTP协**议等等。

域名系统：将域名和IP地址相互映射的一个分布式数据库，能够使人更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

HTTP协议

超文本传输协议使互联网上应用最为广泛的一种网络协议。所有的万维网都必须遵循这个标准。

* 1. 运输层

运输层主要任务使负责两台主机进程之间的通信提供通用的数据传输服务。

使用以下两种协议：  
1. **传输控制协议TCP:**  提供面向链接的，可靠的数据传输服务，文本传输

2.  **用户数据协议UDP**: 提供无连接的，尽最大努力的数据传输服务，视频、语音

* 1. 网络层

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路，也可能经过很多通信子网。网络层的任务就是选择合适的网间路由和交换节点，确保数据及时传送。

网络层使用的是IP协议，因此也叫做IP数据报。

* 1. 数据链路层

在相邻节点之间传送数据时，数据链路层将网络层交下来的IP数据报组成帧。

* 1. 物理层

物理层的作用时实现相邻计算机节点之间的比特流的透明传送，尽可能屏蔽掉具体传输介质和物理设备的差异。

1. TCP三次握手和四次握手

2.1 TCP三次握手漫画图解

简单示意图：

客户端-发送带有SYN标志的数据包-一次握手-服务端

服务端-发送带有SYN/ACK标志的数据包-二次握手-客户端

客户端-发送带有ACK标志的数据包-三次握手-服务端

最主要的目的是 双方确认自己与对方的发送与接收是正常的

第二次握手：

传回ACK是为了告诉客户端，我接受的信息确实就是你所发送的信号了，表明客户端到服务端的通信是正常的

而回传SYN是为了建立并确认从服务端到客户端的通信

**2.2 断开一个TCP链接为什么要进行四次握手**

**-** 客户端 发送一个FIN，用来关闭客户端到服务器的数据传送

**- 服务器 收到这个FIN,它发回一个ACK，确认序号为收到的序号加1.**

**- 服务器 关闭与客户端的连接，发送一个FIN给客户端**

**- 客户端 发送ACK报文确认，并将确认序号设置为收到序号加1**

三、TCP、UDP协议的区别

**UDP** 在传送数据之前不需要先建立连接，远地主机在收到 UDP 报文后，不需要给出任何确认。**虽然 UDP 不提供可靠交付，但在某些情况下 UDP 确是一种最有效的工作方式（一般用于即时通信），比如： QQ 语音、 QQ 视频 、直播等等**

**TCP** **提供面向连接的服务**。在传送数据之前必须先建立连接，数据传送结束后要释放连接。 TCP 不提供广播或多播服务。由于 TCP 要提供可靠的，面向连接的传输服务（TCP的可靠体现在TCP在传递数据之前，会有三次握手来建立连接，而且在数据传递时，有确认、窗口、重传、拥塞控制机制，在数据传完后，还会断开连接用来节约系统资源），这一难以避免增加了许多开销，如确认，流量控制，计时器以及连接管理等。这不仅使协议数据单元的首部增大很多，还要占用许多处理机资源。**TCP 一般用于文件传输、发送和接收邮件、远程登录等场景。**

1. TCP协议如何保证可靠传输
2. 校验和：TCP将保持它首部和数据的校验和。这是一个端到端的校验和，目的是检测数据在传输过程中的任何变化。如果收到段的校验和有差错，TCP将丢弃这个报文段和不确认收到这个报文段。
3. 流量控制：TCP连接的每一方都有固定大小的缓冲空间，TCP的接收端只允许发送端发送接收端缓冲区能够接纳的数据。当接收方来不及处理发送方的数据，能提示发送方降低发送的速率，防止包丢失。TCP使用的流量控制协议是可变大小的滑动窗口协议。
4. 拥塞控制：当网络拥塞时，减少数据的发送。
5. ARQ协议：也是为了实现可靠传输，基本原理是就是发完每个分组就停止发送，等待对方确认。在收到确认后再发下一个分组。
6. 超时重传：

当TCP发出一个段后，它将启动一个定时器，等待目的段确认收到这个报文段。如果不能及时收到一个确认，将重发这个报文段。

1. 再浏览器输入url地址🡪显示主页的过程

过程：

1. 浏览器查找域名的IP地址

（域名🡪IP）

DNS查找过程：

浏览器缓存、路由器缓存、DNS缓存

1. 浏览器向web服务器发送一个HTTP请求
2. 服务器处理请求
3. 服务器发回一个HTML响应
4. 浏览器开始显示HTML

使用的协议：

DNS:获取域名对应的IP

TCP:与服务器简历TCP连接

IP: 建立TCP协议时，需要发送数据，发送数据再网络层使用IP协议

OPSE:IP数据包再路由器之间，路由选择使用OPSF协议

ARP：路由器再与服务器通信时，需要将ip地址转换为MAC地址，需要使用ARP协议

HTTP协议：在TCP建立完成后，使用HTTP协议访问网页

过程：

1. DNS解析
2. TCP连接
3. 发送HTTP请求
4. 服务器处理请求并返回HTTP报文
5. 浏览器解析渲染页面
6. 连接结束

七 URI和URL的区别时什么

URI(Uniform Resource Identifier) 是统一资源标志符，可以唯一标识一个资源。

URL(Uniform Resource Location) 是统一资源定位符，可以提供该资源的路径。它是一种具体的 URI，即 URL 可以用来标识一个资源，而且还指明了如何 locate 这个资源。

URI的作用像身份证号一样，URL的作用更像家庭住址一样。URL是一种具体的URI，它不仅唯一标识资源，而且还提供了定位该资源的信息。

八 HTTP和HTTPS的区别

1. 端口：HTTP的URL由“http://”起始且默认使用端口80，而HTTPS的URL由“https://”起始且默认使用端口443。
2. 安全和资源消耗

HTTP协议允许在TCP上，所有传输的内容都是明文，客户端和服务器端都无法验证对方的身份。

HTTPS是允许在SSL/TLS之上的HTTP协议，SSL/TLS运行在TCP之上。所有传输的内容都是加密的。HTTP安全性没有HTTPS高，但HTTPS比HTTP消耗更多的服务器资源。