计算机网络常见面试题总结

1. OSI ， TCP/IP ，五层协议的体系结构

OSI 分层（7 层）：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。

TCP/IP 分层（4 层）：网络接口层、网际层、运输层、应用层。

五层协议（5 层）：物理层、数据链路层、网络层、运输层、应用层。

每一层的作用如下：

物理层：激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。该层为上层协议提供了一个传输数据的物理媒体。

数据链路层：数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。

网络层：网络层负责对子网间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功能。

传输层：第一个端到端，即主机到主机的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。

会话层：会话层管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。

表示层：表示层对上层数据或信息进行变换以保证一个主机应用层信息可以被另一个主机的应用程序理解。表示层的数据转换包括数据的加密、压缩、格式转换等。

应用层：为操作系统或网络应用程序提供访问网络服务的接口。

2. IP 地址的分类

A 类地址：以 0 开头，第一个字节范围：0~127；

B 类地址：以 10 开头，第一个字节范围：128~191；

C 类地址：以 110 开头，第一个字节范围：192~223；

D 类地址：以 1110 开头，第一个字节范围为 224~239；

3. ARP 协议的工作原理

首先，每台主机都会在自己的 ARP 缓冲区中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址的对应关系。当源主机需要将一个数据包要发送到目的主机时，会首先检查自己 ARP 列表中是否存在该 IP 地址对应的 MAC 地址，如果有，就直接将数据包发送到这个 MAC 地址；如果没有，就向本地网段发起一个 ARP 请求的广播包，查询此目的主机对应的 MAC 地址。此 ARP 请求数据包里包括源主机的 IP 地址、硬件地址、以及目的主机的 IP 地址。网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的 IP 是否和自己的 IP 地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的 MAC 地址和 IP 地址添加到自己的 ARP 列表中，如果 ARP 表中已经存在该 IP 的信息，则将其覆盖，然后给源主机发送一个 ARP 响应数据包，告诉对方自己是它需要查找的 MAC 地址；源主机收到这个 ARP 响应数据包后，将得到的目的主机的 IP 地址和 MAC 地址添加到自己的 ARP 列表中，并利用此信息开始数据的传输。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败。

4. 路由设备与相关层

物理层：中继器（Repeater，也叫放大器），集线器。

数据链路层：网桥，交换机。

网络层：路由器。

网关：网络层以上的设备。

5. 常见的路由选择协议，以及它们的区别

常见的路由选择协议有：RIP 协议、OSPF 协议。

RIP 协议：底层是贝尔曼福特算法，它选择路由的度量标准（metric)是跳数，最大跳数是 15 跳，如果大于 15 跳，它就会丢弃数据包。

OSPF 协议：底层是迪杰斯特拉算法，是链路状态路由选择协议，它选择路由的度量标准是带宽，延迟。

6. TCP 与 UDP 的区别

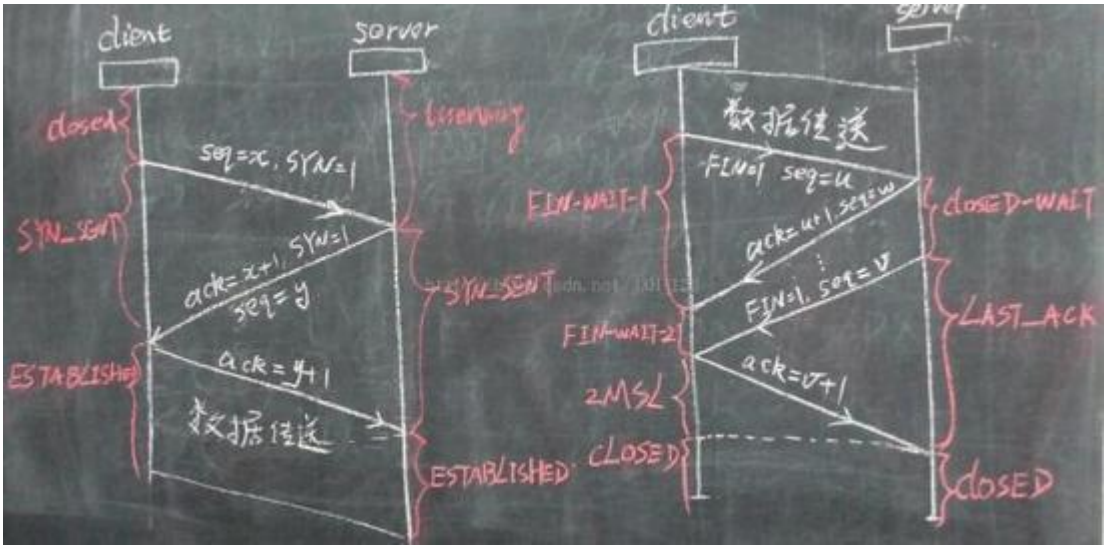
UDP 是面向无连接的，不可靠的数据报服务；

TCP 是面向连接的，可靠的字节流服务。

7. TCP 的可靠性如何保证？

TCP 的可靠性是通过顺序编号和确认（ACK）来实现的。

8. TCP 三次握手和四次挥手的全过程



10. 在浏览器中输入 www.baidu.com 后执行的全部过程

现在假设如果我们在客户端（客户端）浏览器中输入 http://www.baidu.com, 而 baidu.com 为要访问的服务器（服务器），下面详细分析客户端为了访问服务器而执行的一系列关于协议的操作：

1、客户端浏览器通过 DNS 解析到 www.baidu.com 的 IP 地址 220.181.27.48，通过这个 IP 地址找到客户端到服务器的路径。客户端浏览器发起一个 HTTP 会话到 220.161.27.48，然后通过 TCP 进行封装数据包，输入到网络层。

2、在客户端的传输层，把 HTTP 会话请求分成报文段，添加源和目的端口，如服务器使用 80 端口监听客户端的请求，客户端由系统随机选择一个端口如 5000，与服务器进行交换，服务器把相应的请求返回给客户端的 5000 端口。然后使用 IP 层的 IP 地址查找目的端。

3、客户端的网络层不用关系应用层或者传输层的东西，主要做的是通过查找路由表确定如何到达服务器，期间可能经过多个路由器，这些都是由路由器来完成的工作，我不作过多的描述，无非就是通过查找路由表决定通过那个路径到达服务器。

4、客户端的链路层，包通过链路层发送到路由器，通过邻居协议查找给定 IP 地址的 MAC 地址，然后发送 ARP 请求查找目的地址，如果得到回应后就可以使用 ARP 的请求应答交换的 IP 数据包现在就可以传输了，然后发送 IP 数据包到达服务器的地址。

11. HTTP 协议包括哪些请求？

GET：请求读取由 URL 所标志的信息。

POST：给服务器添加信息（如注释）。

PUT：在给定的 URL 下存储一个文档。

DELETE：删除给定的 URL 所标志的资源。

12. HTTP 中， POST 与 GET 的区别

(1)Get 是从服务器上获取数据，Post 是向服务器传送数据。

(2)Get 是把参数数据队列加到提交表单的 Action 属性所指向的 URL 中，值和表单内各个字段一一对应，在 URL 中科院看到。

(3)Get 传送的数据量小，不能大于 2KB；post 传送的数据量较大，一般被默认为不受限制。

(4)根据 HTTP 规范，GET 用于信息获取，而且应该是安全的和幂等的。

I.所谓 **安全的** 意味着该操作用于获取信息而非修改信息。换句话说，GET 请求一般不应产生副作用。就是说，它仅仅是获取资源信息，就像数据库查询一样，不会修改，增加数据，不会影响资源的状态。

II. **幂等** 的意味着对同一 URL 的多个请求应该返回同样的结果。

13. TCP/IP 中，每一层对应的协议

网络层 ：IP 协议、ICMP 协议、ARP 协议、RARP 协议。

传输层 ：UDP 协议、TCP 协议。

应用层 ：FTP（文件传送协议）、Telenet（远程登录协议）、DNS（域名解析协议）、SMTP（邮件传送协议），POP3 协议（邮局协议），HTTP 协议。

14. TCP 对应的协议和 UDP 对应的协议

TCP 对应的协议：

（1） FTP ：定义了文件传输协议，使用 21 端口。常说某某计算机开了 FTP 服务便是启动了文件传输服务。下载文件，上传主页，都要用到 FTP 服务。

（2） Telnet ：它是一种用于远程登陆的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于 DOS 模式下的通信服务。如以前的 BBS 是-纯字符界面的，支持 BBS 的服务器将 23 端口打开，对外提供服务。

（3） SMTP ：定义了简单邮件传送协议，现在很多邮件服务器都用的是这个协议，用于发送邮件。如常见的免费邮件服务中用的就是这个邮件服务端口，所以在电子邮件设置-中常看到有这么 SMTP 端口设置这个栏，服务器开放的是 25 号端口。

（4） POP3 ：它是和 SMTP 对应，POP3 用于接收邮件。通常情况下，POP3 协议所用的是 110 端口。也是说，只要你有相应的使用 POP3 协议的程序（例如 Fo-xmail 或 Outlook），就可以不以 Web 方式登陆进邮箱界面，直接用邮件程序就可以收到邮件（如是 163 邮箱就没有必要先进入网易网站，再进入自己的邮-箱来收信）。

（5）HTTP 协议： 是从 Web 服务器传输超文本到本地浏览器的传送协议。

UDP 对应的协议：

（1） DNS ：用于域名解析服务，将域名地址转换为 IP 地址。DNS 用的是 53 号端口。

（2） SNMP ：简单网络管理协议，使用 161 号端口，是用来管理网络设备的。由于网络设备很多，无连接的服务就体现出其优势。

（3） TFTP (Trival File Transfer Protocal)，简单文件传输协议，该协议在熟知端口 69 上使用 UDP 服务。

15.特殊的 IP 地址

（1）网络地址

IP 地址由网络号（包括子网号）和主机号组成，网络地址的主机号为全 0，网络地址代表着整个网络。

（2）广播地址

广播地址通常称为直接广播地址，是为了区分受限广播地址。

广播地址与网络地址的主机号正好相反，广播地址中，主机号为全 1。当向某个网络的广播地址发送消息时，该网络内的所有主机都能收到该广播消息。

（3）组播地址

D 类地址就是组播地址。

先回忆下 A，B，C，D 类地址吧

A 类地址以 00 开头，第一个字节作为网络号，地址范围为：0.0.0.0~127.255.255.255；

B 类地址以 10 开头，前两个字节作为网络号，地址范围是：128.0.0.0~191.255.255.255;

C 类地址以 110 开头，前三个字节作为网络号，地址范围是：192.0.0.0~223.255.255.255。

D 类地址以 1110 开头，地址范围是 224.0.0.0~239.255.255.255，D 类地址作为组播地址（一对多的通信）；

E 类地址以 1111 开头，地址范围是 240.0.0.0~255.255.255.255，E 类地址为保留地址，供以后使用。

Notice：只有 A,B,C 有网络号和主机号之分，D 类地址和 E 类地址没有划分网络号和主机号。

（4）255.255.255.255

该 IP 地址指的是受限的广播地址。受限广播地址与一般广播地址（直接广播地址）的区别在于，受限广播地址之只能用于本地网络，路由器不会转发以受限广播地址为目的地址的分组；一般广播地址既可在本地广播，也可跨网段广播。例如：主机 192.168.1.1/30 上的直接广播数据包后，另外一个网段 192.168.1.5/30 也能收到该数据报；若发送受限广播数据报，则不能收到。

Notice：一般的广播地址（直接广播地址）能够通过某些路由器（当然不是所有的路由器），而受限的广播地址不能通过路由器。

（5）0.0.0.0

常用于寻找自己的 IP 地址，例如在我们的 RARP，BOOTP 和 DHCP 协议中，若某个未知 IP 地址的无盘机想要知道自己的 IP 地址，它就以 255.255.255.255 为目的地址，向本地范围（具体而言是被各个路由器屏蔽的范围内）的服务器发送 IP 请求分组。

（6）回环地址

127.0.0.0/8 被用作回环地址，回环地址表示本机的地址，常用于对本机的测试，用的最多的是 127.0.0.1。

（7）A、B、C 类私有地址

私有地址(private address)也叫专用地址，它们不会在全球使用，只具有本地意义。

A 类私有地址：10.0.0.0/8，范围是：10.0.0.0~10.255.255.255

B 类私有地址：172.16.0.0/12，范围是：172.16.0.0~172.31.255.255

C 类私有地址：192.168.0.0/16，范围是：192.168.0.0~192.168.255.255

15. NAT 协议、 DHCP 协议、 DNS 协议的作用

NAT 协议 ：网络地址转换(NAT,Network AddressTranslation)属接入广域网(WAN)技术，

是一种将私有（保留）地址转化为合法 IP 地址的转换技术，它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单，NAT 不仅完美地解决了 IP 地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。

DHCP 协议 ：动态主机设置协议（Dynamic Host ConfigurationProtocol, DHCP）

是一个局域网的网络协议，使用 UDP 协议工作，主要有两个用途：给内部网络或网络服务供应商自动分配 IP 地址，给用户或者内部网络管理员作为对所有计算机作中央管理的手段。

DNS 协议：DNS 是域名系统 (Domain Name System) 的缩写，是因特网的一项核心服务，它作为可以将域名和 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。