C++研发高频笔/面试题目  
**笔试：**  
笔试这一块想不到特别好说的，很多时候只是公司筛选人的第一步，分数高低代表意义不大（尤其是大公司，现身说法，我的腾讯笔试真的是呵呵哒），当然笔试是一个门槛，不过后面很可能就不用谈了。我笔试经验也不足，感觉笔试考察最重点的就是算法的熟悉程度，代码能力，我笔试成绩通常不太高，原因是我编程题速度比较慢，往往都做不完。

（2） TCP/IP协议及其编程：计算机网络基础，socket编程，其中子网划分，七层协议（例如交换机属于数据链路层一类题目），五层协议，协议名称及其作用，常用端口号，https1.0 1.1特性与区别，三次握手四次挥手（可能出现的服务器攻击），加密（对称，非对称），IO复用等

1. 2计算机网络（TCP/IP）  
   （1） 建立TCP服务器的各个系统调用  
   （2） 继上一题，说明socket网络编程有哪些系统调用？其中close是一次就能直接关闭的吗，半关闭状态是怎么产生的？  
   （3） 对路由协议的了解与介绍。内部网关协议IGP包括RIP，OSPF，和外部网关协议EGP和BGP.  
   （4） 路由协议所使用的算法。  
   （5） TCP和UDP的区别  
   （6） TCP和UDP相关的协议与端口号  
   （7） TCP（UDP，IP）等首部的认识（http请求报文构成）  
   （8） 网页解析的过程与实现方法  
   （9）    在浏览器中输入URL后执行的全部过程（如[www.baidu.com](http://www.baidu.com)）  
   （10） 网络层分片的原因与具体实现  
   （11） TCP的三次握手与四次挥手的详细介绍（TCP连接建立与断开是热门问题）  
   （12） TCP握手以及每一次握手客户端和服务器端处于哪个状态（11种状态）  
   （13） 为什么使用三次握手，两次握手可不可以？  
   （14） TIME\_WAIT的意义（为什么要等于2MSL）  
   （15） 超时重传机制（不太高频）  
   （16） TCP怎么保证可靠性（面向字节流，超时重传，应答机制，滑动窗口，拥塞控制，校验等）？  
   （17） 流量控制的介绍，采用滑动窗口会有什么问题（死锁可能，糊涂窗口综合征）？  
   （18） tcp滑动窗口协议  
   （19） 拥塞控制和流量控制的区别  
   （20） TCP拥塞控制，算法名字？（极其重要）  
   （21） http协议与TCP联系  
   （22） http/1.0和http/1.1的区别  
   （23） http的请求方法有哪些？get和post的区别。  
   （24） http的状态码  
   （25） http和https的区别，由http升级为https需要做哪些操作  
   （26） https的具体实现，怎么确保安全性  
   （27） http中浏览器一个URL的流程，这个过程中浏览器做了什么，URL包括哪三个部分？  
   （28） 一个机器能够使用的端口号上限是多少，为什么？可以改变吗？那如果想要用的端口超过这个限制怎么办？  
   （29） 对称密码和非对称密码体系  
   （30） 数字证书的了解（高频）  
   （31） 客户端为什么信任第三方证书  
   （32） RSA加密算法，MD5原理（MD5不算加密算法）  
   （33） 单条记录高并发访问的优化  
   （34） 介绍一下ping的过程，分别用到了哪些协议

ping 的原理

ping 程序是用来探测主机到主机之间是否可通信，如果不能ping到某台主机，表明不能和这台主机建立连接。ping 使用的是ICMP协议，它发送icmp回送请求消息给目的主机。ICMP协议规定：目的主机必须返回ICMP回送应答消息给源主机。如果源主机在一定时间内收到应答，则认为主机可达。

ICMP协议通过IP协议发送的，IP协议是一种无连接的，不可靠的数据包协议。在Unix/Linux，序列号从0开始计数，依次递增。而Windows　ping程序的ICMP序列号是没有规律。

ICMP协议在实际传输中数据包：20字节IP首部 + 8字节ICMP首部+ 1472字节<数据大小>38字节

ICMP报文格式:IP首部(20字节)+8位类型+8位代码+16位校验和+(不同的类型和代码，格式也有所不同)

Ping工作过程——

假定主机A的IP地址是192.168.1.1，主机B的IP地址是192.168.1.2，都在同一子网内，则当你在主机A上运行“Ping 192.168.1.2”后，都发生了些什么呢?

首先，Ping命令会构建一个固定格式的ICMP请求数据包，然后由ICMP协议将这个数据包连同地址“192.168.1.2”一起交给IP层协议（和ICMP一样，实际上是一组后台运行的进程），IP层协议将以地址“192.168.1.2”作为目的地址，本机IP地址作为源地址，加上一些其他的控制信息，构建一个IP数据包，并在一个映射表中查找出IP地址192.168.1.2所对应的物理地址（也叫MAC地址，熟悉网卡配置的朋友不会陌生，这是数据链路层协议构建数据链路层的传输单元——帧所必需的），一并交给数据链路层。后者构建一个数据帧，目的地址是IP层传过来的物理地址，源地址则是本机的物理地址，还要附加上一些控制信息，依据以太网的介质访问规则，将它们传送出去。

其中映射表由ARP实现。ARP(Address Resolution Protocol)是地址解析协议,是一种将IP地址转化成物理地址的协议。ARP具体说来就是将网络层（IP层，也就是相当于OSI的第三层）地址解析为数据连接层（MAC层，也就是相当于OSI的第二层）的MAC地址。

主机B收到这个数据帧后，先检查它的目的地址，并和本机的物理地址对比，如符合，则接收；否则丢弃。接收后检查该数据帧，将IP数据包从帧中提取出来，交给本机的IP层协议。同样，IP层检查后，将有用的信息提取后交给ICMP协议，后者处理后，马上构建一个ICMP应答包，发送给主机A，其过程和主机A发送ICMP请求包到主机B一模一样。

即先由IP地址，在网络层传输，然后再根据mac地址由数据链路层传送到目的主机

（35） TCP/IP的分片粘包过程  
（36） 有没有抓过TCP包，描述一下  
（37） 一个ip配置多个域名，靠什么识别？  
（38） 服务器攻击（DDos攻击）