1.Http协议

Http是应用层的传输协议，基于Tcp/Ip通信协议传递数据



2.特点

快速简单，发送请求只需要请求方法和路径，协议简单，通信速度块

可以传输任意类型对象，定义在content-type中

无连接无状态，每次只处理一个请求，断开连接就关闭会话，不会记录状态

3.URL与URI

URL是资源的绝对路径，而URI是相对路径，URI是标志一个资源，URL是对URI的具体定位，比如一个个人名片，上面有人名与详细地址，而URI就是人名，知道这个人的名字，但是如果想找到这个人，还需要URL详细地址

4.Http请求Request

4.1请求行（请求方法，协议版本）

4.2请求头部（附加信息，比如content-type，connection，user-agent）

4.3空行

4.4请求数据（详细内容）

5.Http请求Response

5.1状态行（协议版本号，状态码）

5.2消息头部（附加信息，比如content-type，date）

5.3空行

5.4响应正文

6.Http工作原理：

1.客户端通过Http客户端连接到服务器，建立TCP套接字连接

2.通过Tcp套接字发送Http请求报文4

3.服务器解析内容，返回响应报文，写到TCP套接字

4.判断connection方式，如果为close，服务器关闭TCP连接， 如果是keep-Alive会保持一段时间，该时间内可以继续接收请求，http 1.0中默认是：Connection: close；http 1.1中默认启用Keep-Alive，Keep-Alive功能使客户端到服务器端的连接持续有效，当出现对服务器的后继请求时，Keep-Alive功能避免了建立或者重新建立连接。启用Keep-Alive模式更高效，性能更高

5.客户端解析响应内容，反应到Http客户端浏览器上

7.Get/Post请求的区别

1.Get将请求的数据附加在URL之后，Post不会显示，

2.Get将请求写入了请求头部中，而Post则将请求放在请求内容中

3.Get请求提交的数据有限制（URL长度限制），Post没有限制

4.Get比Post安全性更差，请求可见

8.缺点

安全性低，传输消息，需要经过很多中转节点，路由器转发的时候容易被篡改，下面引入Https

8.Https（安全套接字层超文本传输协议HTTPS）

HTTP+SSL层。HTTPS的安全基础是SSL，因此加密的详细内容就需要SSL，在Http协议基础上面加上SSL协议，SSL协议依靠证书来验证服务器的身份，并为Web浏览器和服务器之间的通信加密，即需要CA证书

HTTPS协议的主要作用可分为两种：

　　　　1、建立一个信息安全通道，保证数据传输的安全。

　　　　2、确认网站的真实性。

9. HTTPS的工作原理

1、Client使用HTTPS的URL访问Web服务器，要求与Web服务器建立SSL连接。

　　　　2、Web服务器收到客户端请求后，会将网站的证书信息（证书中包含公钥）传送一份给客户端。

　　　　3、客户端的浏览器与Web服务器开始协商SSL连接的安全等级，也就是加密方式。

　　　　4、客户端的浏览器根据双方同意的安全等级，建立会话密钥，然后利用网站的公钥将会话密钥加密，并传送给网站。

　　　　5、Web服务器利用自己的私钥解密出会话密钥。

　　　　6、Web服务器利用会话密钥加密与客户端之间的通信。

了解SSL过程：

SSL依赖于TCP连接,所以在SSL交互之前需建立TCP连接

第一步，客户端给出协议版本号、一个客户端生成的随机数（Client random），以及客户端支持的加密方法。

第二步，服务端确认双方使用的加密方法，并给出数字证书、以及一个服务器生成的随机数（Server random）。

第三步，客户端确认数字证书有效，然后生成一个新的随机数（Premaster secret），并使用数字证书中的公钥，加密这个随机数，发给服务端。

第四步，服务端使用自己的私钥，获取客户端发来的随机数（即Premaster secret）。

第五步，客户端和服务端根据约定的加密方法，使用前面的三个随机数，生成"对话密钥"（session key），用来加密接下来的整个对话过程。

10. 为什么不能对每个客户端使用相同的秘钥（对称加密）

1.为客户端并不是固定的,所以要么只使用一种对称秘钥,所有客户端都一样

2.要么就先传输对称秘钥,然后在进行数据传输.安全性低

11.Https为什么需要第三方CA证书

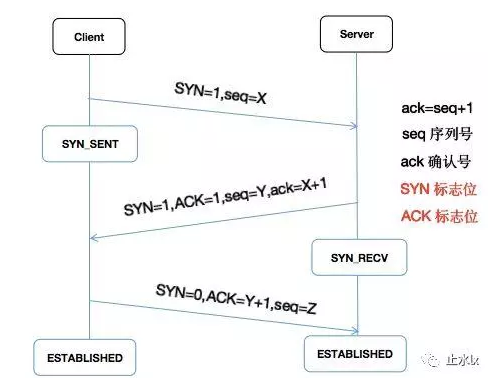
1.服务器将证书信息携带公钥如果被替换，客户端不知道是否是服务器返回的，那么这就表示不能直接将公钥传递给客户端，而是第三方机构使用它的私钥对我们的公钥进行加密后，再传给客户端。客户端再使用第三方机构的公钥进行解密，如果能解密，就说明这个公钥没有被中间人调包。因为如果中间人使用自己的私钥加密后的东西传给客户端，客户端是无法使用第三方的公钥进行解密的

12.Https为什么客户端需要数字证书

1. 第三方机构不可能只给你一家公司制作证书，它也可能会给中间人这样有坏心思的公司发放证书。这样的，中间人就有机会对你的证书进行调包，客户端在这种情况下是无法分辨出是接收的是你的证书，客户端内容生成证书编号，用于验证

13.Tcp三次握手四次挥手

三次握手建立连接：



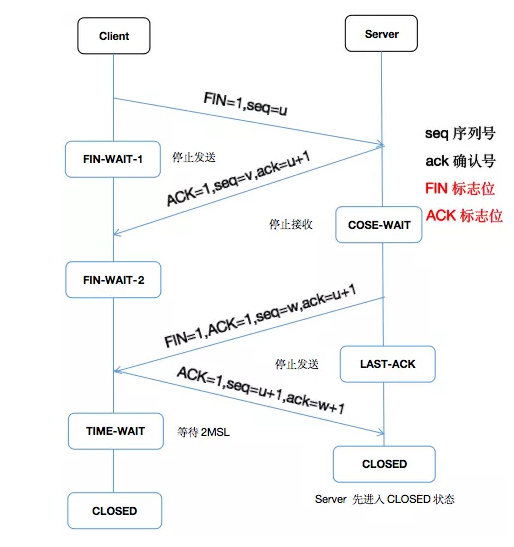
为什么需要三次握手：

前两次握手进行同步和准备，第三次握手进入状态

为什么不是2次握手呢？

如果一个连接请求在网络中跑得慢，超时了，这时客户端会重发请求，但这个跑的慢的客户端最后还是跑到了，然后服务端就接收了两个请求，然后全部回应就会创建两个连接，浪费资源。如果加入第三次验证，则客户端接收到一个服务端确认连接请求之后，后面再接收到确认连接请求就可以抛弃不管了。

四次挥手断开连接：



为什么4次挥手？

TCP 是双向的，所以需要在两个方向分别关闭，每个方向的关闭又需要请求和确认，所以一共就4次