

HTTP/TCP

TCP三次握手四次挥手

三次握手的目的是建立可靠的通信信道，说到通讯，简单来说就是数据的发送与接收，而三次握手最主要的目的就是双方确认自己与对方的发送与接收是正常的。

断开，多一次是因为服务器再知道断开请求之后还会传完一小部分数据，然后在断开

在浏览器中输入url地址 ->> 显示主页的过程

总体来说分为以下几个过程:

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

http 1.0,1.1,2.0 以及https

在HTTP/1.0中，默认使用的是短连接，HTTP 1.1起，默认使用长连接

错误状态响应码 :在HTTP1.1中新增了24个错误状态响应码，如409（Conflict）表示请求的资源与资源的当前状态发生冲突

缓存处理 :在HTTP1.0中主要使用header里的If-Modified-Since,Expires来做为缓存判断的标准，HTTP1.1则引入了更多的缓存控制策略例如Entity tag

带宽优化及网络连接的使用 :HTTP1.0中，存在一些浪费带宽的现象，例如客户端只是需要某个对象的一部分，而服务器却将整个对象送过来了，并且不支持断点续传功能，HTTP1.1则在请求头引入了range头域，它允许只请求资源的某个部分，即返回码是206（Partial Content）

HTTP 2.0 vs HTTP 1.1

1. HTTP/2采用二进制格式而非文本格式
2. HTTP/2是完全多路复用的，而非有序并阻塞的——只需一个连接即可实现并行
3. 使用报头压缩，HTTP/2降低了开销
4. HTTP/2让服务器可以将响应主动“推送”到客户端缓存中

HTTP vs HTTPS

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. **安全性和资源消耗** : HTTP协议运行在TCP之上，所有传输的内容都是明文，客户端和服务端都无法验证对方的身份。HTTPS是运行在SSL/TLS之上的HTTP协议，SSL/TLS 运行在TCP之上。所有

传输的内容都经过加密，加密采用对称加密，但对称加密的密钥用服务器方的证书进行了非对称加密。所以说，HTTP 安全性没有 HTTPS高，但是 HTTPS 比HTTP耗费更多服务器资源。

https加密过程

todo , 非对称，对称分别用在哪里