说一下HTTP

HTTP概念

超文本：不仅仅是文本，还有图片，视频等等数据

传输：从一个点转移到另一个点

协议：两者或以上参与者之间的约定和规范

超文本传输协议：计算机世界中，将文本，视频、图片等数据从一个点转移到另一个点之间对的约定和协议

HTTP优缺点

优点：简单

缺点：不安全

- 双刃剑
  - 明文传输
    - 方便调试
    - 没有安全可言
  - 无状态
    - 不用多余字段记录状态，可以减轻网络负担
    - 导致每次进入一次网站就需要进行一次验证（携带cookie等方案可以解决）
- 不加密----可能造成数据泄漏
- 不校验身份----可能会上虚假网站
- 不校验信息----可能会造成网页广告泛滥

常见网络状态码

- 1XX：中间状态，表示还没完成
- 2XX：成功
  - 200：成功并正常返回
- 3XX：重定向
  - 301：永久重定向，表示这个url已经不对了
  - 304：缓存重定向，表示返回的数据无改变，直接可以请求缓存（通常在前一个请求返回200后出现）
- 4xx：客户端错误
  - 403：不允许访问，通常为权限不够
  - 404：资源不存在
- 5XX：服务器错误
  - 502：表示代理请求错误，代理访问器正常，但代理向后台服务器请求出错后，代理服务器返回
  - 503：网络不可用，通常是DOS攻击后出现

报文常见字段

- Host：客户端发请求时，用来指定服务器的域名
- Content-Length：服务器在返回数据时，用来表示这次响应数据的长度
- Content-Type：用于服务器响应时，告诉客户端，本次数据的类型
- Accept：客户端请求时，说明自己可以接受的数据类型
- Content-Encoding：说明数据的压缩方式，表示服务器返回数据的压缩方式
- Accept-Encoding：客户端可接收的压缩类型
- Connection：非标准字段，最常用于客户端要求服务器使用TCP长连接，以便其他请求复用

HTTP与HTTPS

区别

- http默认端口80，https默认端口443
- http是明文传输，https加密传输
- http三次握手后就可以进行数据传输，https在三次握手后还需要进行SSL/TSL握手
- https还需要向CA机构申请数字证书来保证服务器的可信性

HTTPS如何解决HTTP存在的问题

- 信息加密：采用对等加密和非对等加密的混合加密方式（密钥传输非对称加密，数据传输使用对称加密）
- 数字证书：保证网站是正规的
- 校验机制：使用摘要算法来保证数据完整性

从HTTP1.0到HTTP3.0

HTTP1.0

- 短连接

HTTP1.1

- 使用TCP长连接改善HTTP1.0的短连接造成的性能问题，keep-alive
- 采用管道网络传输，只要第一个请求发出去后，不用等返回，就可以直接发第二个请求，可以减少整体响应时间

还存在的问题

- 请求与响应的头部不压缩就发送，太大了
- 服务器按顺序响应请求，如果服务器慢,会造成请求不到数据（队头阻塞），也没有请求优先级控制。
- 请求只能从客户端开始，服务器只能被动响应

HTTP2.0

- 基于HTTPS，安全有保障
- 会压缩头部数据，HPACK算法
- 将1.1中纯文本格式的报文，改成二进制格式，减少解析时间，增加传输效率
- 数据包不按顺序发送，有优先级响应策略

还存在的问题

- 多个请求复用一个TCP连接，下层TCP协议不知道有几个HTTP协议，一旦发生丢包，就触发重传，整个TCP连接中的所有请求都要等待这个包被重传过来（想想HTTP1.1管道中一个请求阻塞，也会造成其他请求阻塞）

HTTP3.0

- 将2.0中底层的TCP更换成UDP，UDP不管顺序，也不管丢包，所以不会发生1.1中的队头阻塞，2.0的丢包重传问题的
- 基于QUIC可以实现保证传输的可靠性
- 头部压缩算法由Hpack改成Qpack