HTTP协议版本

- HTTP/0.9

- 仅支持GET请求方式
- 仅能请求访问HTML格式的资源

- 只要不是1开头的都是Beta版本

- HTTP/1.0

- 增加POST和HEAD请求方式
- 支持多种数据格式的请求与访问
- 支持cache缓存功能
- 新增状态码、多字符集支持、内容编码等

- 早期HTTP/1.0不支持keep-alive长连接，只支持串行连接
- 后期HTTP/1.0增加Connection: keep-alive字段（非标准字段），开始支持长连接

- HTTP/1.1

- 增加持久连接（默认开启Connection: keep-alive）
- 增加管道机制（支持多个请求同时发送）
- 增加PUT/PATCH/OPTION/DELETE等请求方式
- 增加Host字段（指定服务器域名）-> 案例: 搜索百度 查看network
- 增加100状态码（Continue）,支持只发送头信息
- 增加身份认证机制
- 支持传送内容的一部分和文件断点续传
- 新增了24个错误状态码

- HTTP/2.0

- 增加双工模式（客户端同时发送多个请求，服务端同时处理多个请求）
- 服务器推送（服务器会把客户端需要的资源一起推送到客户端，合适加载静态资源）
- 头信息压缩机制（每次请求都会带上所有信息发送给服务端【HTTP协议不带状态】）

- 二进制协议（头信息与数据体使用二进制进行传输）
- 多工（先发送已处理好的部分，再响应其他请求，最后再解决没有处理好的部分）

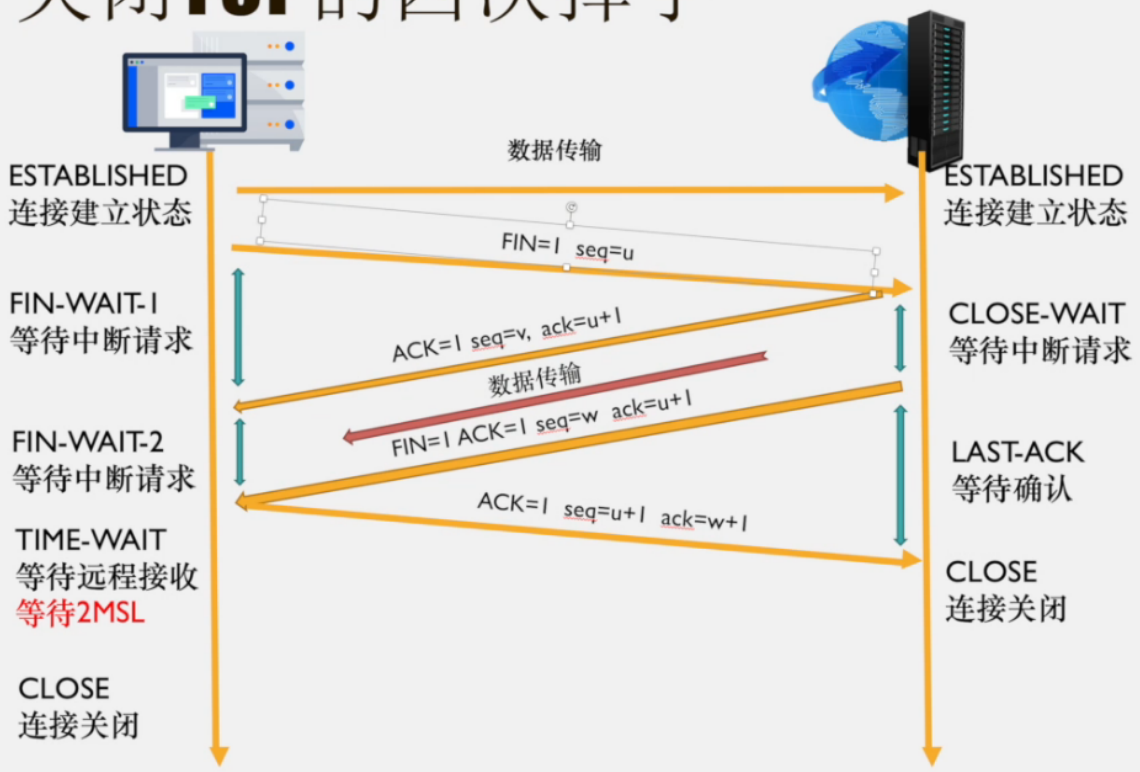
关闭TCP

关闭TCP连接的前奏

- FIN：finish 关闭连接

- 状态：
- FIN-WAIT-1 - 等待远程TCP的连接中断请求，或先前的连接中断请求的确认
  FIN-WAIT-2 - 从远程TCP等待连接中断请求
  CLOSE-WAIT - 等待从本地用户发来的连接中断请求
  LAST-ACK - 等待原来发向远程TCP的连接中断请求的确认
  TIME-WAIT -等待足够的时间以确保远程TCP接收到连接中断请求的确认
  CLOSED - 没有任何连接状态

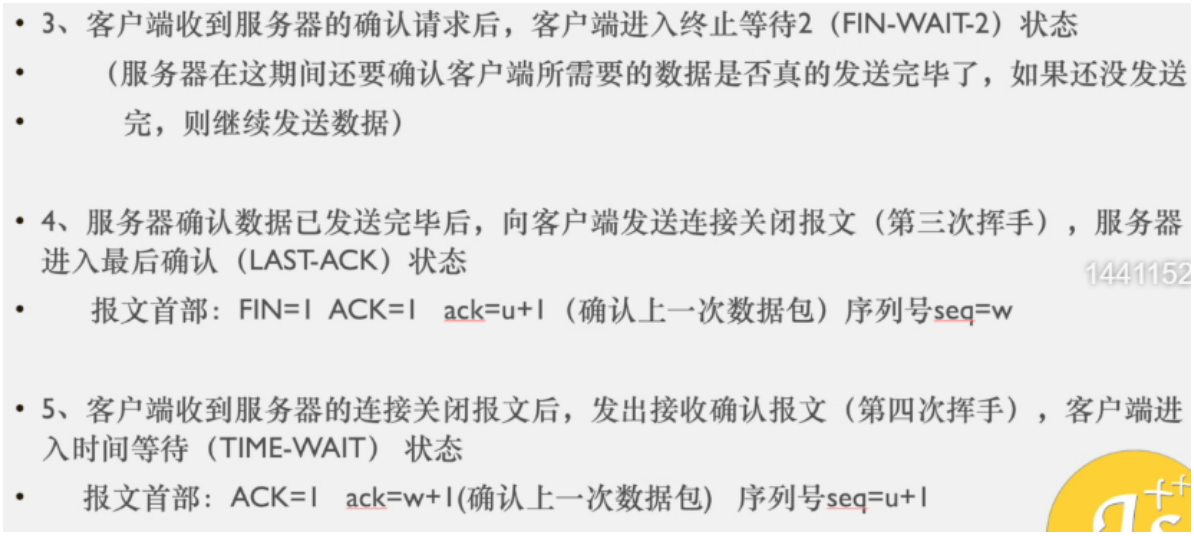
关闭TCP的四次挥手

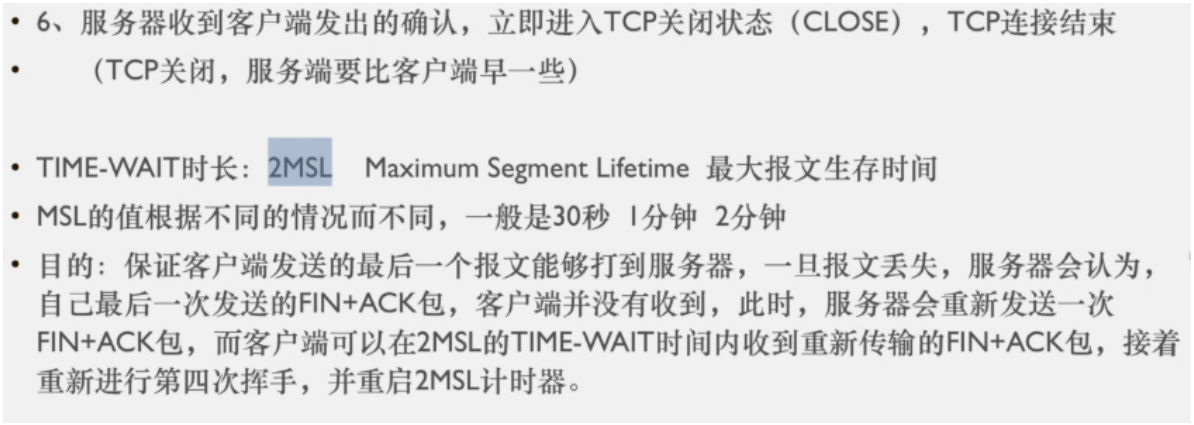


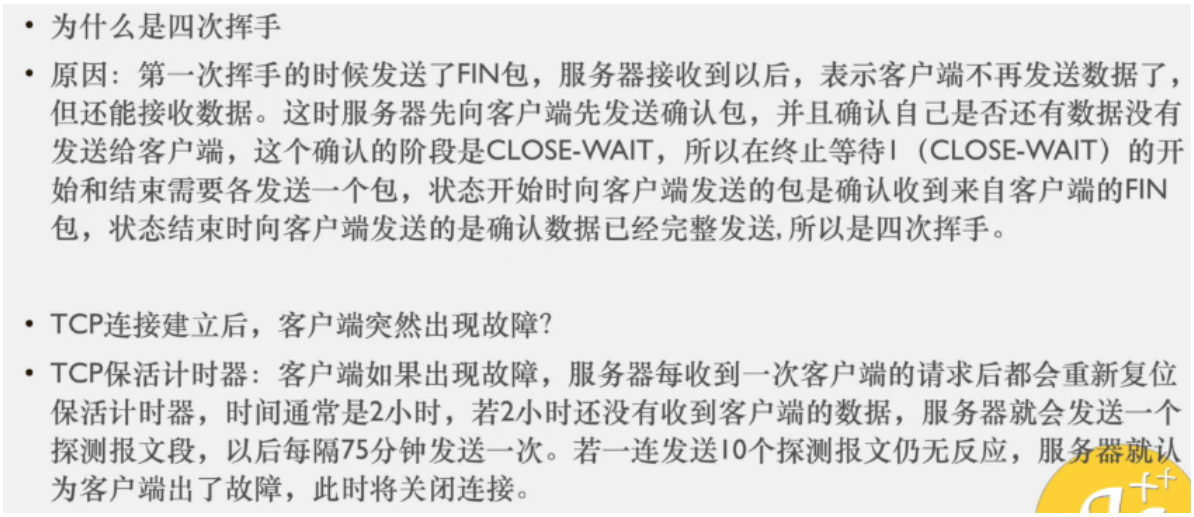
- 客户端进入 FIN-WAIT-2 的状态时，就不会在向服务端发送请求，但是能够接收到响应

- 1、客户端发送连接关闭报文（此时已停止发送数据）（第一次挥手）
- 报文首部：FIN=1（序列号seq=u）
- 此刻：客户端进入终止等待1（FIN-WAIT-1）状态

- 2、服务器收到连接关闭报文，并发送确认报文（第二次挥手）
- 报文首部：ACK=1 ack=u+1（确认FIN）（序列号seq=v）
- 此刻：服务端进入关闭等待（CLOSE-WAIT）状态
- 说明：连接半关闭状态，客户端没有数据要发送，但服务器如果还要发送数据，
- 客户端依然需要接受







- TCP 保活计时器 在任何TCP连接时都是存在的

同源策略

- 比3次握手4次挥手都重要的概念

- 同源策略 Same-Origin-Policy(SOP)
- web浏览器只允许在两个页面有相同的源时，第一个页面的脚本访问第二个页面里的数据。

- 第一个页面：http://test.jsplusplus.com/index.html AJAX请求 ->
- 第二个页面：http://study.jsplusplus.com/server.php

- 同源策略 Same-Origin-Policy(SOP)
- 报错： Access to XMLHttpRequest at 'http://study.jsplusplus.com/server.php' from origin 'http://test.jsplusplus.com' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.

- Access to XMLHttpRequest at：请求跨域
- 地址： http://study.jsplusplus.com/server.php

- from origin 'http://test.jsplusplus.com'
- 请求来自源 http://test.jsplusplus.com
- has been blocked by CORS policy
- 被跨域资源共享策略(Cross-origin resource sharing)阻止
- No 'Access-Control-Allow-Origin' header is present on the requested resource
- 在请求的资源中没有发现'允许跨域'头信息

- 同源策略 Same-Origin-Policy(SOP)
- http://www.jsplusplus.com

http://study.jsplusplus.com	不同源
http://www.jsplusplus.com:8080	不同源
https://www.jsplusplus.com	不同源
http://www.jsplusplus.com/course/index.html	同源
http://www.jsplusplus.com/index/course/index.html	同源

- 源(域名)：协议 + 域名 + 端口
- 同源：相同的协议 && 相同的域名 && 相同的端口
- 不同源（跨域）：不同的协议 || 不同的域名 || 不同的端口

- 将server.php放入test.jsplusplus.com/中

- 同源策略 Same-Origin-Policy(SOP)
- 跨域操作初试
- server.php: header('Access-Control-Allow-Origin: *');
- server.php: header('Access-Control-Allow-Origin: http://test.jsplusplus.com');
- 同源策略是浏览器的一个安全功能，不同源的客户端脚本在没有明确授权的情况下，不能读写对方资源。只有同一个源的脚本赋予dom、读写cookie、session、ajax等操作的权限。