**TCP三次握手**

作者：HioHio  
链接：https://www.zhihu.com/question/24853633/answer/573627478  
来源：知乎  
著作权归作者所有。商业转载请联系作者获得授权，非商业转载请注明出处。

TCP A TCP B

​

1. CLOSED LISTEN

​

2. SYN-SENT --> <SEQ=100><CTL=SYN> ...

​

3. (duplicate) ... <SEQ=90><CTL=SYN> --> SYN-RECEIVED

​

4. SYN-SENT <-- <SEQ=300><ACK=91><CTL=SYN,ACK> <-- SYN-RECEIVED

​

5. SYN-SENT --> <SEQ=91><CTL=RST> --> LISTEN

​

6. ... <SEQ=100><CTL=SYN> --> SYN-RECEIVED

​

7. SYN-SENT <-- <SEQ=400><ACK=101><CTL=SYN,ACK> <-- SYN-RECEIVED

​

8. ESTABLISHED --> <SEQ=101><ACK=401><CTL=ACK> --> ESTABLISHED

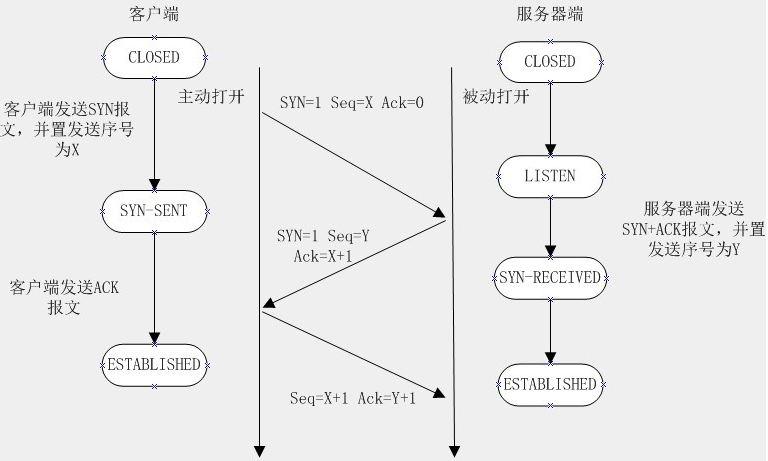
​

Recovery from Old Duplicate SYN

这是 复用连接时，旧在途包发往新连接中的例子。

* 3中，一个旧的重复的 SYN到达 B。
* 4中， B分别不出是否旧的，照样子正常回包。
* 5中，A检测到 B 返回的ACK不正确，所以返回 RST(reset)
* 6中，B接收到 RST(reset)信号，于是变成 LISTEN 状态。
* 7中，新连接正常的 SYN终于到达了，三次握手正常进行。

这种是简化的情况，但是可以看出 TCP 是如何处理复用旧链接的包到达的



TCP四次挥手

 第一次挥手(FIN=1，seq=x)

假设客户端想要关闭连接，客户端发送一个 FIN 标志位置为1的包，表示自己已经没有数据可以发送了，但是仍然可以接受数据。

发送完毕后，客户端进入 FIN\_WAIT\_1 状态。

 第二次挥手(ACK=1，ACKnum=x+1)

服务器端确认客户端的 FIN 包，发送一个确认包，表明自己接受到了客户端关闭连接的请求，但还没有准备好关闭连接。

发送完毕后，服务器端进入 CLOSE\_WAIT 状态，客户端接收到这个确认包之后，进入 FIN\_WAIT\_2 状态，等待服务器端关闭连接。

 第三次挥手(FIN=1，seq=y)

服务器端准备好关闭连接时，向客户端发送结束连接请求，FIN 置为1。

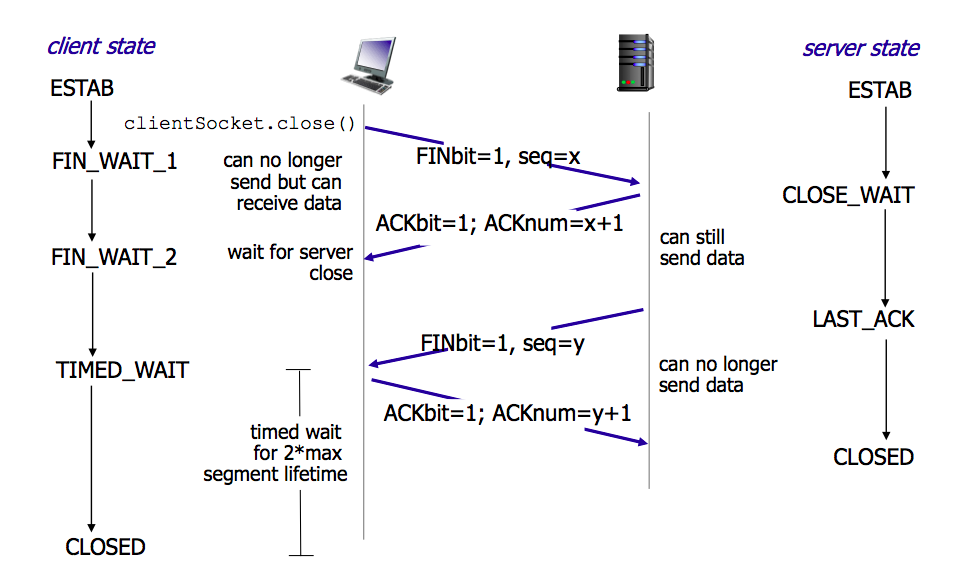
发送完毕后，服务器端进入 LAST\_ACK 状态，等待来自客户端的最后一个ACK。

 第四次挥手(ACK=1，ACKnum=y+1)

客户端接收到来自服务器端的关闭请求，发送一个确认包，并进入 TIME\_WAIT状态，等待可能出现的要求重传的 ACK 包。

服务器端接收到这个确认包之后，关闭连接，进入 CLOSED 状态。

客户端等待了某个固定时间（两个最大段生命周期，2MSL，2 Maximum Segment Lifetime）之后，没有收到服务器端的 ACK ，认为服务器端已经正常关闭连接，于是自己也关闭连接，进入 CLOSED 状态



**TCP和HTTP**

TCP是底层通讯协议，定义的是数据传输和连接方式的规范；  
HTTP是应用层协议，定义的是传输数据的内容的规范；  
HTTP协议中的数据是利用TCP协议传输的，所以支持HTTP也就一定支持TCP ；

**socket**

Socket是应用层与TCP/IP协议族通信的中间软件抽象层，它是一组接口。在设计模式中，Socket其实就是一个门面模式，它把复杂的TCP/IP协议族隐藏在Socket接口后面，对用户来说，一组简单的接口就是全部，让Socket去组织数据，以符合指定的协议。

**http https区别和联系**

 HTTP 明文传输，数据都是未加密的，安全性较差，HTTPS（SSL+HTTP） 数据传输过程是加密的，安全性较好。

 使用 HTTPS 协议需要到 CA（Certificate Authority，数字证书认证机构） 申请证书，一般免费证书较少，因而需要一定费用。证书颁发机构如：Symantec、Comodo、GoDaddy 和 GlobalSign 等。

 HTTP 页面响应速度比 HTTPS 快，主要是因为 HTTP 使用 TCP 三次握手建立连接，客户端和服务器需要交换 3 个包，而 HTTPS除了 TCP 的三个包，还要加上 ssl 握手需要的 9 个包，所以一共是 12 个包。

 http 和 https 使用的是完全不同的连接方式，用的端口也不一样，前者是 80，后者是 443。

 HTTPS 其实就是建构在 SSL/TLS 之上的 HTTP 协议，所以，要比较 HTTPS 比 HTTP 要更耗费服务器资源

7 应用层 6 表示层 5 会话层 4 传输层 3 网络层 2 数据链路层 1 物理层

TCP UDP区别

1） TCP提供面向连接的传输，通信前要先建立连接（三次握手机制）； UDP提供无连接的传输，通信前不需要建立连接。

2） TCP提供可靠的传输（有序，无差错，不丢失，不重复）； UDP提供不可靠的传输。

3） TCP面向字节流的传输，因此它能将信息分割成组，并在接收端将其重组； UDP是面向数据报的传输，没有分组开销。

4） TCP提供拥塞控制和流量控制机制； UDP不提供拥塞控制和流量控制机制。