链滴

关于握手那些事

作者：vcjmhg

原文链接：https://ld246.com/article/1575208038691

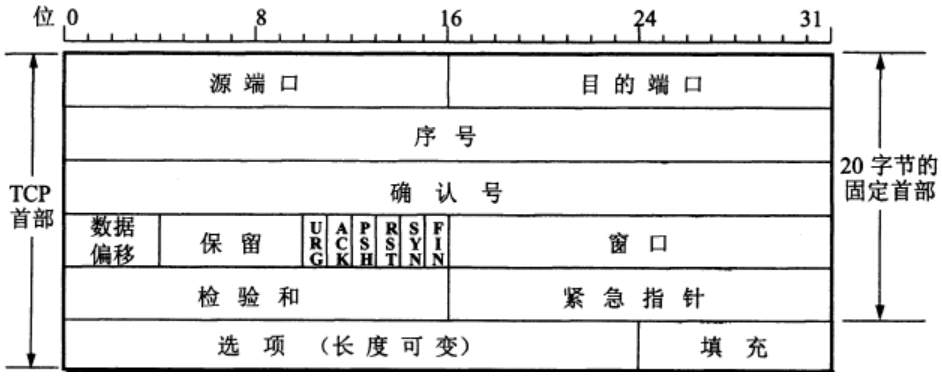
来源网站：链滴

缘起

可能学习过计算机网络的同学都知道TCP/IP在建立连接时需要进行三次握手，但不知大家是否考虑过何必须用三次握手来建立连接？是否可以通过两次握手就建立？为何中断连接的时候又必须进行四次手，而不能用三次握手？下边在这篇文章中我们对这些问题一一进行解答。

报文格式

握手建立TCP连接的过程，其本质就是连接双方达成传输规则的公式，而规则的达成势必少不了共同约定。而TCP报文便是TCP连接建立的共识。因此开始之前先了解TCP报文的格式是很有必要的。按谢希仁老师的教材，TCP的报文格式如下所示：



上图的字段是很多的，但在此处并不需要我们都了解，其中下边这几个字段和握手过程密切相关，需我们提前予以说明。

1. 序号：Seq序号，占32位，用来标识从TCP源端向目的端发送的字节流，发起方发送数据时对此进标记。

2. 确认号：Ack序号，占32位，只有ACK标志位为1时，确认序号字段才有效，Ack=Seq+1。

3. 标志位：共6个，即URG、ACK、PSH、RST、SYN、FIN等，具体含义如下：

（A）URG：紧急指针（urgent pointer）有效。

（B）ACK：仅当ACK=1时确认号字段才有效。当ACK=0时，确认号字段无效

（C）PSH：当两个应用进程进行交互通信时，有时一端的应用进行希望在键入一个命令后能够立即到对方的响应。在这种情况下，TCP就可以使用推送（PSH）操作。接受放在受到PSH=1的报文段后就会尽快交付给接受应用进程，而不在等到缓存填满之后再发送。

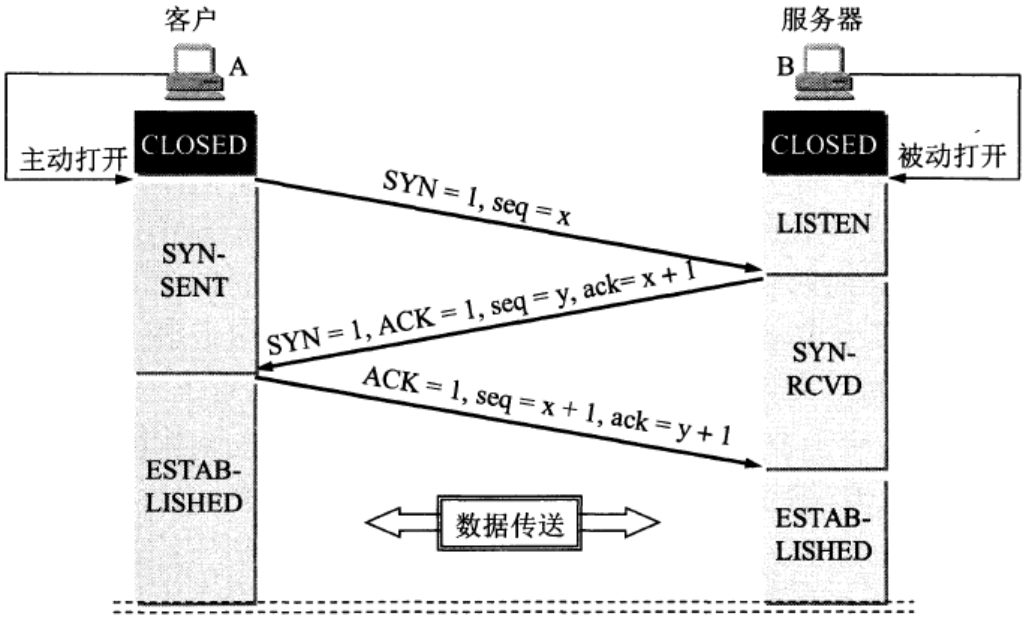
（D）RST：用于重置连接。当RST=1时，表明TCP连接中出现了严重差错，必须释放连接，然后重建立连接

（E）SYN：在建立连接时用来同步序号。

（F）FIN：用来释放一个连接。

三次握手

所谓三次握手指的就是TCP连接在建立时需要客户端和服务器总共发送3个数据包确认连接的建立。个流程如下所示：



操作	作用
第一次握手	客户端将标志位SYN置为1，随机产生一个值seq=x，将该数据包发送给服务器，客服端进入进入SYN_SEN状态，等待服务器端确认。
	客户端发信服务器收到，此时服务器就明白，客户端的发信能力和自己的接受能力没有问题
第二次握手	服务器收到数据包后由标志位SYN=1知道客户端请求立连接，服务器将标志位SYN和ACK都置为1，ack=x+，随机产生一个值seq=y，并将该数据包发送给客户端以确认连接请求，服务器进入SYN_CVD状态
	服务器发信客户端收到，此时客户端就会明白服务器端的信能力和收信能力都没问题，此时服务器还不知道自己的发信能力和客户端的收信能力如何，因此引了第三次握手
第三次握手	客户端收到确认后，检查ack是否为x+，ACK是否为1，如果正确则将标志位ACK置为1，ack=y+，并将该数据包发送给服务器，服务器检查ack是否为y+，ACK是否为1，如果正确则连接建立成功，客户端和服务器进入ESTABLISHED状态，完成三次握手

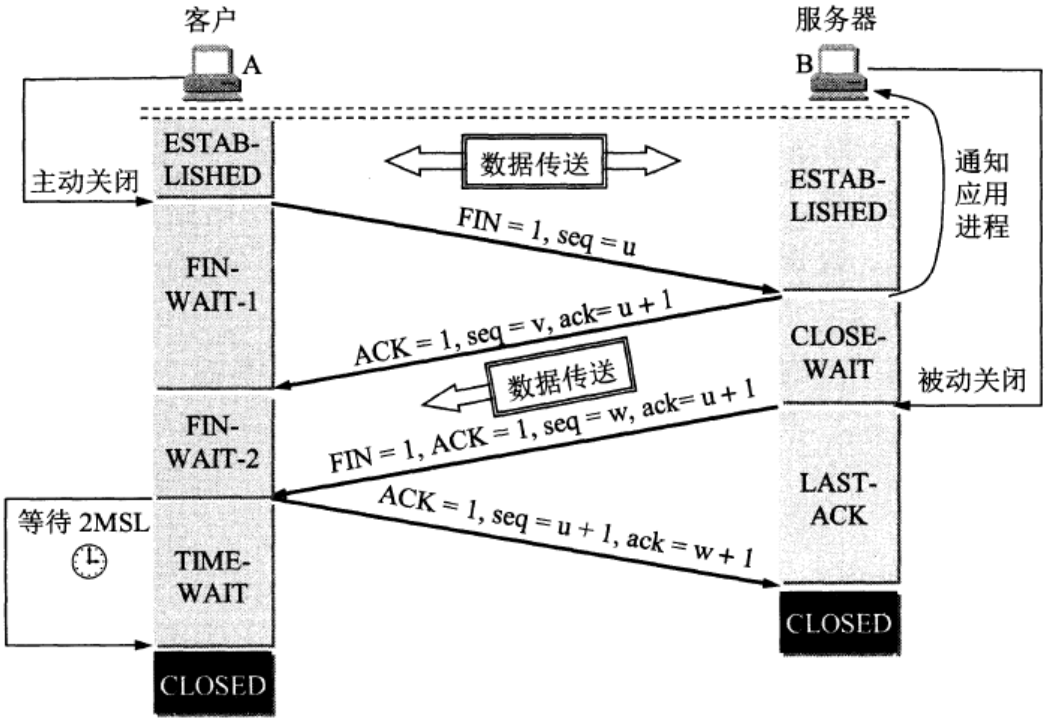
随后客户端与服务器之间可以开始传输数据了。 客户端发信服务器到信之后，就会明白自己的发信能力和客户端的收信能力都没有问题，两个都会明白彼此之间收发能都正常。可以进行数据传输 。

到这里可能会有人问了，两次握手之后客户端直接向服务器端直接发送数据，不也可以吗?

严格意义上讲，第二次握手之后，客户端直接发送数据也可以向服务器确定客户端的接受能力和自己发信能力。但是直接发送的话，可能由于服务器端没有准备就绪，从而造成数据包的丢失，也就是说三次的握手在一定程度上是提前让服务器做好接受数据的准备。

挥手道别

所谓四次握手就是指终止TCP连接的时候，需要客户端和服务器总共发送4个数据包以确认连接的断。整个过程如下图所示:



操作 **作用**

第一次挥手 客户端发送一个FIN，用来关闭客户端到服务器的数据送，客户端进入FIN_WAIT_1状态。
户端发信，服务器端到收信。客户端告知服务器端自己需要发送的数据已经发完，但服务器端不一定部收到

第二次挥手 服务器收到FIN后，发送一个ACK给客户端，确认序号收到序号+1（与SYN相同，一个FIN占用一个序号），服务器进入CLOSE_
AIT状态。 服务器端发信，客户端收信。服务器端告知客户端其发的数据自己已经全部收到了。但是服务器端不一定数据发送完毕

第三次挥手 服务器发送一个FIN，用来关闭服务器到客户端的数据送，服务器进入LAST_ACK状态。
务器端发信，客户端收信。服务器端告知客户端自己需要发送的数据以及发送完。但是客户端不一定到了所有数据

第四次挥手 客户端收到FIN后，进入TIME_
AIT状态，接着发送一个ACK给服务器端，确认序号为收到序号+
，服务器端进入CLOSED状态，完成四次挥手。 客户端发信，服务

原文链接：关于握手那些事

端收信。告知服务器端其发送的数据自己已经全部接收到了，双方可以释放连接了

到这里可能大家又有疑问了，为什么TCP在建立连接的时候需要三次握手就可以了，而分别的时候却挥手四次?

这是因为服务端在LISTEN状态下，收到建立连接请求的SYN报文后，把ACK和SYN放在一个报文里发给客户端。而关闭连接时，当收到对方的FIN报文时，仅仅表示对方不再发送数据了但是还能接收数，己方也未必全部数据都发送给对方了，所以己方可以立即close，也可以发送一些数据给对方后，发送FIN报文给对方来表示同意现在关闭连接，因此，己方ACK和FIN一般都会分开发送。

小结

到这里可能大家就明白了，TCP在建立连接时要进行三次主要是为了让双方都明确自身和对方收发能正常。而TCP在断开是进行四次挥手，主要是为了保证收发双方数据都发送完毕，并且对方都完全接到。