# 通俗理解TCP/IP协议三次握手与四次分手流程

2017年01月06日 14:07:54

阅读数：9447

三次握手流程

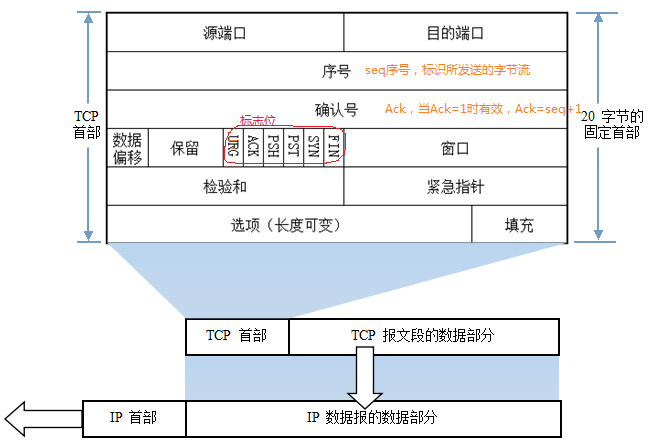
1. 客户端发个请求“开门呐，我要进来”给服务器
2. 服务器发个“进来吧，我去给你开门”给客户端
3. 客户端有很客气的发个“谢谢，我要进来了”给服务器

四次挥手流程

1. 客户端发个“时间不早了，我要走了”给服务器，等服务器起身送他
2. 服务器听到了，发个“我知道了，那我送你出门吧”给客户端，等客户端走
3. 服务器把门关上后，发个“我关门了”给客户端，然后等客户端走（尼玛~矫情啊）
4. 客户端发个“我知道了，我走了”，之后自己就走了

****TCP报文格式****

TCP/IP协议的详细信息参看《TCP/IP协议详解》三卷本。下面是TCP报文格式图：

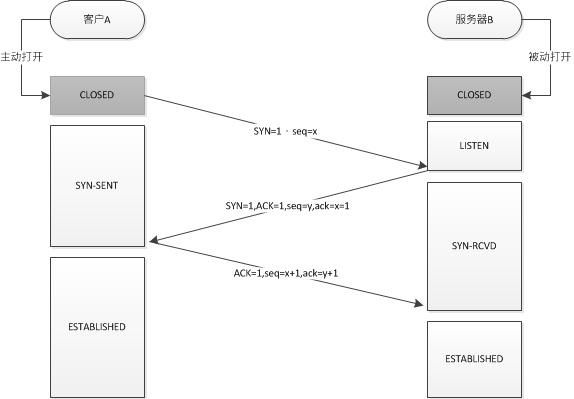


  上图中有几个字段需要重点介绍下：  
  （1）序号：Seq序号，占32位，用来标识从TCP源端向目的端发送的字节流，发起方发送数据时对此进行标记。  
  （2）确认序号：Ack序号，占32位，只有ACK标志位为1时，确认序号字段才有效，Ack=Seq+1。  
  （3）标志位：共6个，即URG、ACK、PSH、RST、SYN、FIN等，具体含义如下：  
  （A）URG：紧急指针（urgent pointer）有效。  
  （B）ACK：确认序号有效。  
  （C）PSH：接收方应该尽快将这个报文交给应用层。  
  （D）RST：重置连接。  
  （E）SYN：发起一个新连接。  
  （F）FIN：释放一个连接。

具体流程图如下：

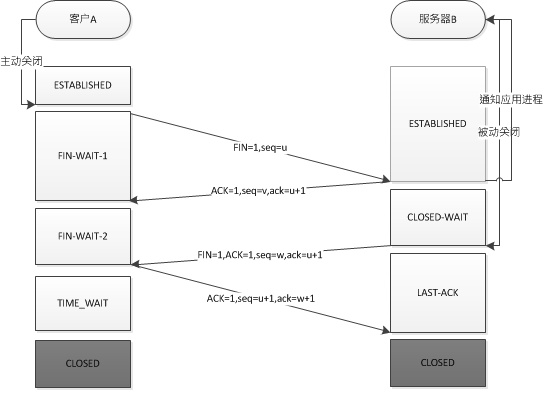
****三次握手的过程（客户端我们用A表示，服务器端用B表示）****

前提：A主动打开，B被动打开



****四次分手的过程（客户端我们用A表示，服务器端用B表示）****

前提：A主动关闭，B被动关闭



文字版解释：

第一次握手：建立连接时，[客户端](http://baike.baidu.com/view/930.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)发送[syn](http://baike.baidu.com/view/488528.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)包（syn=j）到[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)，并进入[SYN\_SENT](http://baike.baidu.com/view/840439.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)状态，等待服务器确认；SYN：同步序列编号（***Synchronize Sequence Numbers***）。

[第二次握手](http://baike.baidu.com/view/205949.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)：[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)收到[syn](http://baike.baidu.com/view/488528.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)包，必须确认客户的SYN（[ack](http://baike.baidu.com/view/204040.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入[SYN\_RECV](http://baike.baidu.com/view/1520054.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)状态；

第三次握手：[客户端](http://baike.baidu.com/view/930.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)收到[服务](http://baike.baidu.com/view/133203.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)器的SYN+ACK包，向[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)发送确认包ACK([ack](http://baike.baidu.com/view/204040.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)=k+1），此包发送完毕，客户端和服务器进入[ESTABLISHED](http://baike.baidu.com/view/1137549.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)（TCP连接成功）状态，完成三次握手。

完成三次握手，[客户端](http://baike.baidu.com/view/930.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)与服务器开始传送[数据](http://baike.baidu.com/view/38752.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)，在上述过程中，还有一些重要的概念：

未连接队列

在[三次握手协议](http://baike.baidu.com/view/2494361.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)中，[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)维护一个未连接队列，该队列为每个[客户端](http://baike.baidu.com/view/930.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)的SYN包（[syn](http://baike.baidu.com/view/488528.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)=j）开设一个条目，该条目表明服务器已收到SYN包，并向客户发出确认，正在等待客户的确认包。这些条目所标识的连接在[服务器](http://baike.baidu.com/view/899.htm" \t "https://blog.csdn.net/qq_18425655/article/details/_blank)处于SYN\_RECV状态，当服务器收到客户的确认包时，删除该条目，服务器进入ESTABLISHED状态。

关闭TCP连接：改进的三次握手

对于一个已经建立的连接，TCP使用改进的三次握手来释放连接（使用一个带有FIN附加标记的报文段）。TCP关闭连接的步骤如下：

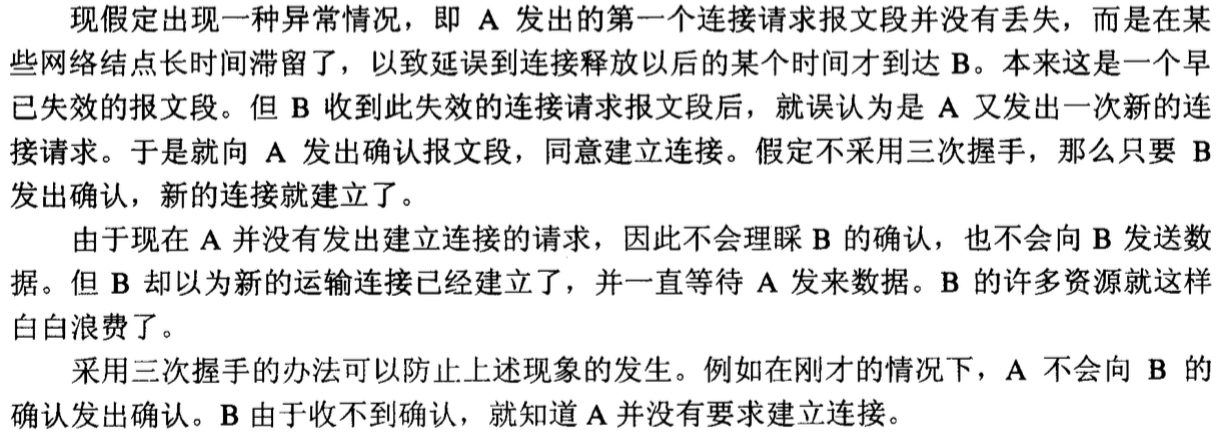
第一步，当主机A的应用程序通知TCP数据已经发送完毕时，TCP向主机B发送一个带有FIN附加标记的报文段（FIN表示英文finish）。

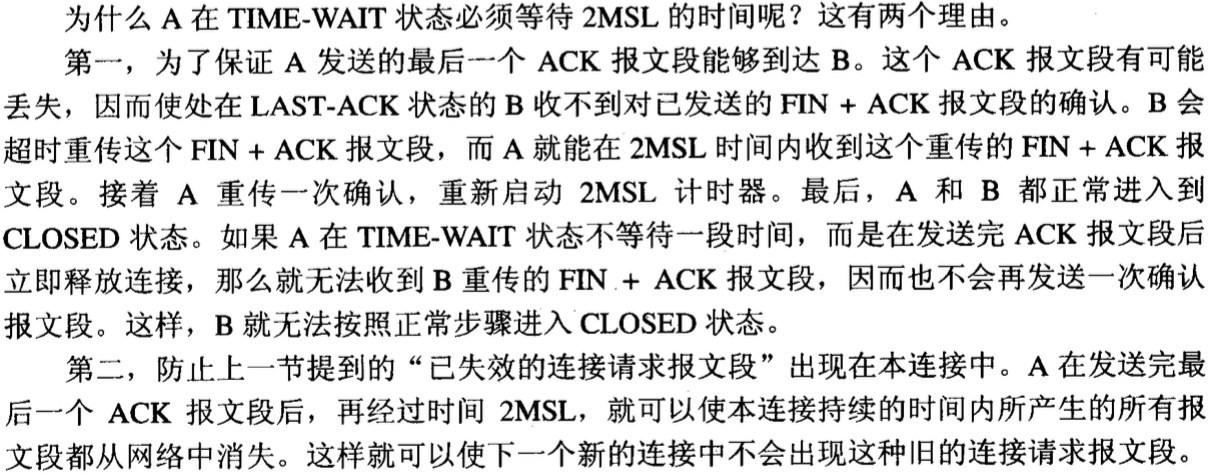
第二步，主机B收到这个FIN报文段之后，并不立即用FIN报文段回复主机A，而是先向主机A发送一个确认序号ACK，同时通知自己相应的应用程序：对方要求关闭连接（先发送ACK的目的是为了防止在这段时间内，对方重传FIN报文段）。

第三步，主机B的应用程序告诉TCP：我要彻底的关闭连接，TCP向主机A送一个FIN报文段。

第四步，主机A收到这个FIN报文段后，向主机B发送一个ACK表示连接彻底释放。

**为什么要采用三次握手，两次不行吗？**

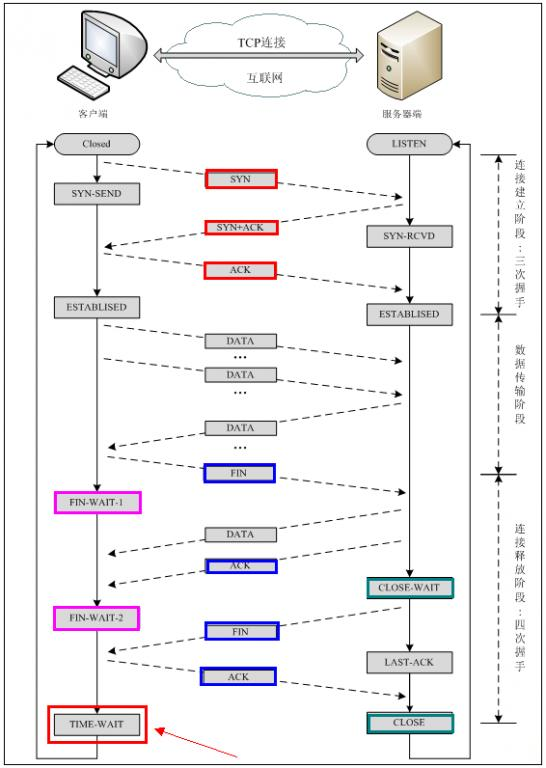




**保活计时器：**

*设想有这样的情况：客户端已主动与服务器建立了TCP连接，但后来客户端的主机突然出现故障。*

*通常设为2小时。若2小时没有收到客户端的数据，服务器就发送一个探测报文段，以后则每隔75分钟发送一次。若一连发送10个探测报文段后仍无客户端的响应，服务器就认为客户端出现了故障，接着就关闭这个连接。*



**为什么连接的时候是三次握手，关闭的时候却是四次握手？**

答：因为当Server端收到Client端的SYN连接请求报文后，可以直接发送SYN+ACK报文。其中ACK报文是用来应答的，SYN报文是用来同步的。但是关闭连接时，当Server端收到FIN报文时，很可能并不会立即关闭SOCKET，所以只能先回复一个ACK报文，告诉Client端，"你发的FIN报文我收到了"。只有等到我Server端所有的报文都发送完了，我才能发送FIN报文，因此不能一起发送。故需要四步握手。

**为什么TIME\_WAIT状态需要经过2MSL(最大报文段生存时间)才能返回到CLOSE状态？**

答：虽然按道理，四个报文都发送完毕，我们可以直接进入CLOSE状态了，但是我们必须假象网络是不可靠的，有可以最后一个ACK丢失。所以TIME\_WAIT状态就是用来重发可能丢失的ACK报文。

#### **如果已经建立了连接，但是客户端突然出现故障了怎么办？**

TCP还设有一个保活计时器，显然，客户端如果出现故障，服务器不能一直等下去，白白浪费资源。服务器每收到一次客户端的请求后都会重新复位这个计时器，时间通常是设置为2小时，若两小时还没有收到客户端的任何数据，服务器就会发送一个探测报文段，以后每隔75分钟发送一次。若一连发送10个探测报文仍然没反应，服务器就认为客户端出了故障，接着就关闭连接。