

三次握手

1. 第一次握手

客户端向服务器发出连续请求报文，这报文首部中的同部位SYN=1；同时随机生成序列号seq=x；此时Tcp客户端进入了SYN-SENT(同步发送)状态。TCP规定SYN报文段（SYN=1）不能携带数据，但需要消耗掉一个序号。这个三次握手开始。表示客户端想要和服务端建立连接。

2. 第二次握手

TCP接受到请求报文后，则发出确定报文。确认报文中应该包含ACK = 1，SYN=1，确认号是ack = x + 1, 同时也要为自己初始化一个序列号seq = y, 此时服务器进入了SYN-RCVD（同步接受）状态。这个报文也不能携带数据，但是同样需要消耗掉一个序号。这个报文带有SYN（建立连接）和ACK（确认）标志，询问客户端是否准备好。

3. 第三次握手

TCP 客户端进程收到确认后，还要向服务器给出确认，确认报文的ACK = 1，ack = y+1；此时TCP连接建立，客户端进入ESTABLISHED（已建立连接）状态。TCP规定，ACK报文段可以携带数据，但是如果不携带数据则不消耗序号，这里客户端表示我已准备好。

为什么要三次握手？

举例：已失效的连接请求报文段。

client发送了一个连接请求的报文段，但是由于网络不好，这个请求并没有立即到达服务器。而是在某个网络节点滞留了，只带某个时间才到达server，本来这是个已失效的报文，但是server端接收到这个请求后，还是会向client发送确认报文，表示同意连接，假如不采用三次握手，那么只要server发出确认，新的连接就建立了。但其实这个请求是失败的请求，client不会理睬server的确认信息，也不会向服务器发送确认的请求，但是server认为新的请求已经建立起来了，并一直等待client发送过来的数据，这样server的很多资源就被白白浪费掉了，采用三次握手就可以防止这种情况的发生，server接受不到确认报文，就知道client并没有建立连接，这就是三次握手的作用。

四次挥手

1. 第一次挥手

TCP发送一个FIN（结束），用来关闭客户到服务器的连接。

客户端进程发出连接释放报文，并且停止发送数据。释放数据报文首部，FIN=1，其序列号为seq=u（等于前面已经传送过来的数据的最后一个字节的序号加1），此时，客户端进入FIN-WAIT-1（终止等待1）状态。TCP规定，FIN报文段即使不携带数据，也要消耗一个序号。

2. 第二次挥手

服务端收到这个FIN，他发回一个ACK(确认)，确认收到序号为收到序号+1，和SYN一样，一个FIN将占用一个序号。

服务器收到连接释放报文，发出确认报文，ACK=1，ack=u+1，并且带上自己的序列号seq=v，此时，服务端就进入了CLOSE-WAIT（关闭等待）状态。TCP服务器通知高层的应用进程，客户端向服务器的方向就释放了，这时候处于半关闭状态，即客户端已经没有数据要发送了，但是服务器若发送数据，客户端依然要接受。这个状态还要持续一段时间，也就是整个CLOSE-WAIT状态持续的时间。

3. 第三次挥手

服务端发送一个FIN(结束)到客户端，服务端关闭客户端的连接。

服务器将最后的数据发送完毕后，就向客户端发送连接释放报文，FIN=1，ack=u+1，由于在半关闭状态，服务器很可能又发送了一些数据，假定此时的序列号为seq=w，此时，服务器就进入了LAST-ACK（最后确认）状态，等待客户端的确认。

4. 第四次挥手

客户端发送ACK(确认)报文确认，并将确认的序号+1，这样关闭完成。

客户端收到服务器的连接释放报文后，必须发出确认，ACK=1，ack=w+1，而自己的序列号是seq=u+1，此时，客户端就进入了TIME-WAIT（时间等待）状态。注意此时TCP连接还没有释放，必须经过 $2 * MSL$ （最长报文段寿命）的时间后，当客户端撤销相应的TCB后，才进入CLOSED状态。服务器只要收到了客户端发出的确认，立即进入CLOSED状态。同样，撤销TCB后，就结束了这次的TCP连接。可以看到，服务器结束TCP连接的时间要比客户端早一些。

为什么要4次挥手？

关闭连接时，当收到对方的FIN报文通知时，它仅仅表示对方没有数据发送给你了；但未必你所有的数据都全部发送给对方了，所以你可以未必会马上会关闭SOCKET,也即你可能还需要发送一些数据给对方之后，再发送FIN报文给对方来表示你同意现在可以关闭连接了，所以它这里的ACK报文和FIN报文多数情况下都是分开发送的。可能有人会有疑问，tcp我握手的时候为何ACK(确认)和SYN(建立连接)是一起发送。挥手的时候为什么是分开的時候发送呢. 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。