

## 第五章 传输层 TCP连接管理

TCP连接传输三个阶段：

- (1) 连接建立
- (2) 数据传送
- (3) 连接释放

TCP把连接作为最基本的抽象，每条TCP连接有两个端口，TCP连接的端点不是主机，不是主机的IP地址。不是应用程序，也不是传输层的协议端口。

TCP连接的端口称为套接字（Socket）或插口。

---

TCP连接的建立采用**客户服务器方式**，**主动发起连接建立的应用进程**叫做**客户**，而**被动等待连接建立的应用进程**叫**服务器**。

假设运行在一台主机（客户）上的一个进程想与另一台主机（服务器）上的一个进程建立一条连接，**客户应用进程首先通知客户TCP**，他**想建立一个与服务器上某个进程之间的连接**，**客户中的TCP**会用以下步骤与**服务器中的TCP**建立一条TCP连接。

TCP的连接建立过程：

连接的过程经历以下3个步骤，通常称为**三次握手**。

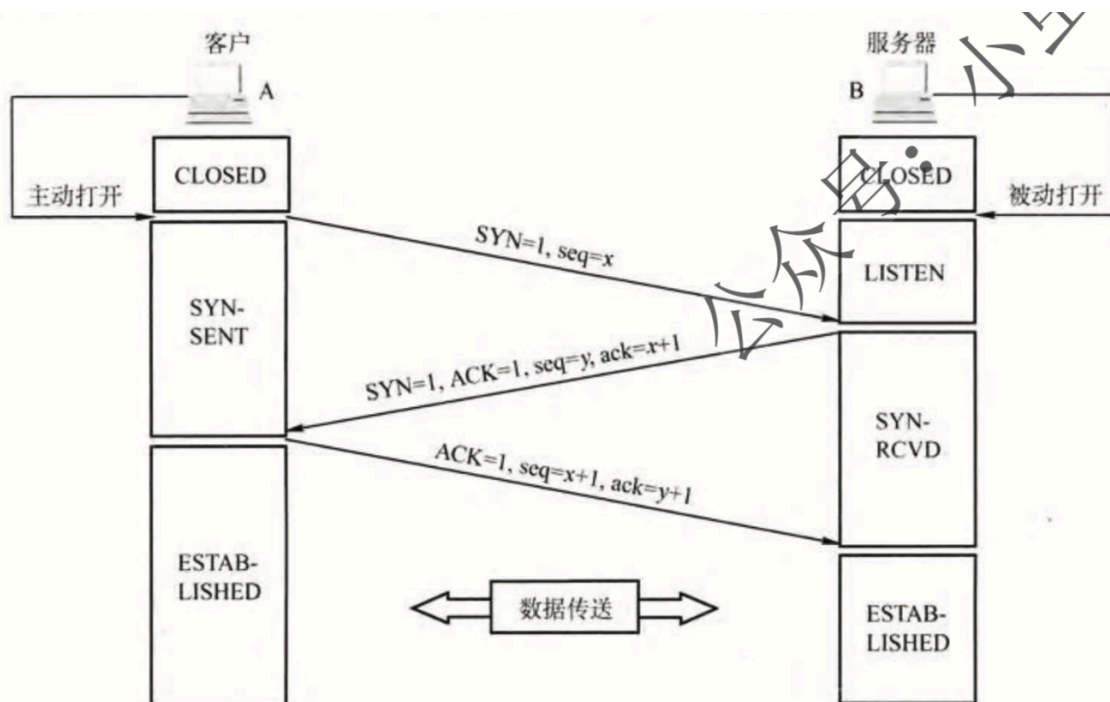


图 5.7 用“三次握手”建立 TCP 连接

### 三次握手的过程：

第一步：客户机的TCP首先向服务器的TCP发送一个连接请求报文段。这个特殊的报文段中**不含应用层数据**，其首部中的**SYN标志位被置为1**。另外客户会**随机选择一个起始序号seq=x**。

(连接请求报文**不携带数据**，但是要消耗一个序号)

$SYN=1$  ,  $seq=x$

第二步：服务器的TCP收到连接请求报文段后，如同意建立连接，就向客户机发回确认，并为该TCP连接分配TCP缓存和变量。在确认报文段中，SYN和ACK都被置为1，确认号字段ack的值为x+1.并且服务器随机产生起始序号seq=y。

(确认报文**不携带数据**，但也要消耗一个序号)

$SYN=1, ACK=1, seq=y, ack=x+1$

第三步：当客户机收到确认报文段后，还要向服务器给出确认，并且也要给该连接分配缓存和变量。这个报文段的ACK标志位被置1，序号字段为x+1，确认号字段ack=y+1。该**报文段可以携带数据**，**若不携带数据则不消耗序号**。

$ACK=1, seq=x+1, ack=y+1$

成功进行以上三步，就建立了TCP连接，接下来就可以传送应用层数据。**TCP**提供的是全双工通信，因此通信双方的应用进程在任何时候都能发送数据。

另外，服务器端的资源是在完成第二次握手时分配的，而客户端的资源是在完成第三次握手时分配的，这就使得服务器易于收到SYN洪泛攻击。

## 2、TCP连接的释放

参与TCP连接的两个进程中的任何一个都能终止该连接。

TCP连接释放的过程通常称为**四次握手**。

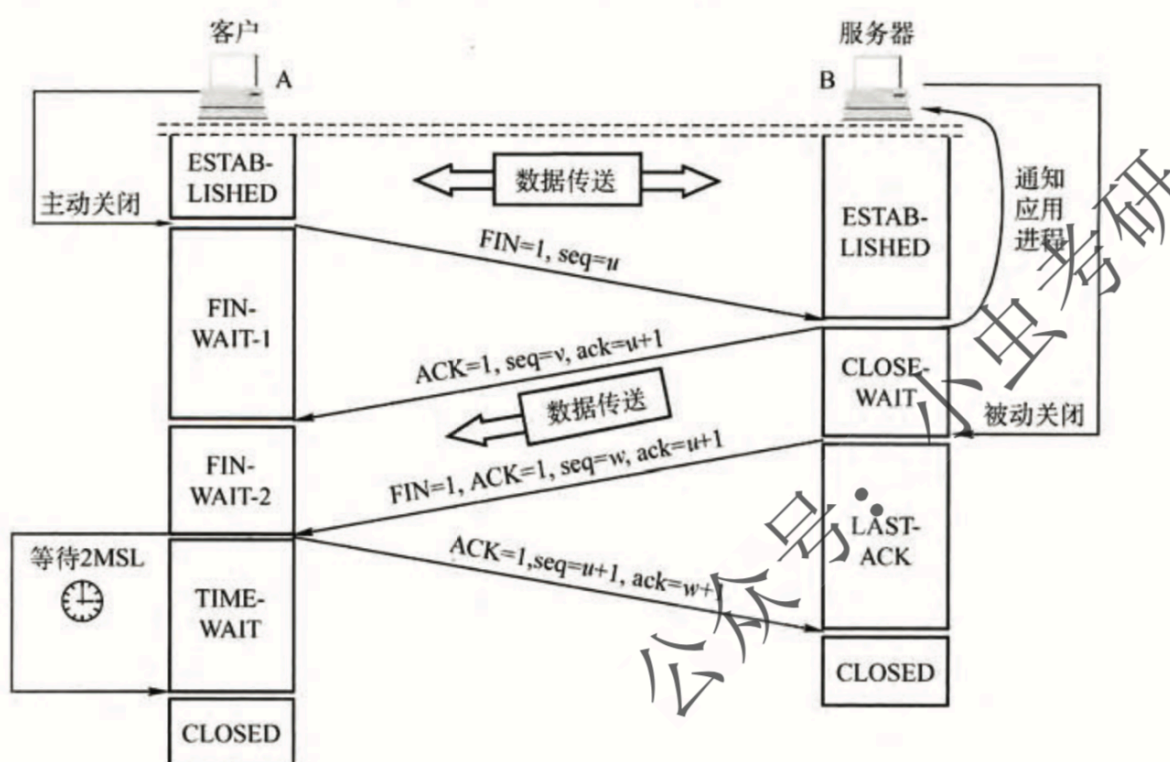


图 5.8 用“四次握手”释放 TCP 连接

四次握手的过程：

第一步：客户机打算关闭连接时，向其TCP**发送一个连接释放报文段**，并停止发送数据，主动关闭TCP连接，**该报文段的FIN标志位被置为1**，**seq=u**，它等于前面已发送过的数据的最后一个字节的序号+1（FIN报文段即使不携带数据，也要消耗一个序号）。

**FIN=1, seq=u**

TCP是全双工的，即可以想象为一条TCP连接上有两条数据通路。**发送**

FIN报文时，发送FIN的一端不能在发送数据，即关闭了其中一条数据通路了，但对方还可以发送数据。

第二步：服务器收到连接释放报文段后即发出确认，确认号是  $ack=u+1$ ，而这个报文段自己的序号是  $v$ ，等于他前面已传送的最后一个字节的序号+1。

$ACK=1, seq=v, ack=u+1$

此时，从客户机到服务器这个方向的连接就释放了，**TCP连接处于半关闭状态**。但服务器若发送数据，客户机仍要接收，即从服务器到客户机这个方向的连接并未关闭。

第三步：若服务器已经没有要向客户机发送的数据，就通知TCP释放连接，此时其发出  $FIN=1$  的连接释放报文段。

$FIN=1, ACK=1, seq=w, ack=u+1$

第四步：客户机收到连接释放报文段后，必须发出确认。在确认报文段中，**ACK字段被置为1，确认号  $ack=w+1$ ，序号  $seq=u+1$** 。此时TCP连接还未释放，必须经过时间等待计时器设置的时间  $2MSL$  后(最长报文段寿命)，**A才进入连接关闭状态**。

$ACK=1, seq=u+1, ack=w+1$

对上述 TCP 连接建立和释放的总结如下：

1) 连接建立。分为 3 步：

- ①  $SYN=1, seq=x$ 。
- ②  $SYN=1, ACK=1, seq=y, ack=x+1$ 。
- ③  $ACK=1, seq=x+1, ack=y+1$ 。

2) 释放连接。分为 4 步：

- ①  $FIN=1, seq=u$ 。
- ②  $ACK=1, seq=v, ack=u+1$ 。
- ③  $FIN=1, ACK=1, seq=w, ack=u+1$ 。
- ④  $ACK=1, seq=u+1, ack=w+1$ 。

选择题喜欢考查（关于连接和释放的题目，ACK、SYN、FIN 一定等于 1），请牢记。