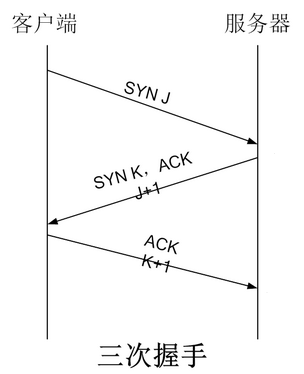
# 一、tcp协议格式



# 二、三次握手

在 TCP/IP 协议中，TCP 协议提供可靠的连接服务，采用[三次握手](http://baike.baidu.com/link?url=eZXiFRQOKsO6NUMErlv_ourWMexrPfxtUhSw1f5waWf_gVDDeOpI7xFga2VygpC-qZWFVkj-XTcQeKx7UQO7fq)建立一个连接。



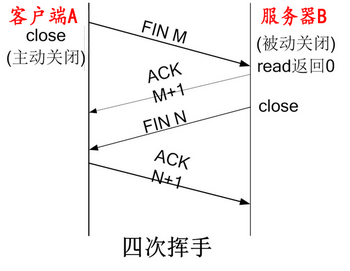
**第一次握手**：建立连接时，客户端发送 syn 包(tcp协议中syn位置1，序号为J)到服务器，并进入 SYN\_SEND 状态，等待服务器确认；

**第二次握手**：服务器收到 syn 包，必须确认客户的 SYN，同时自己也发送一个 SYN 包，即 SYN+ACK包（tcp协议中syn位置1，ack位置1，序号K，确定序号为J+1），此时服务器进入 SYN\_RECV 状态；

**第三次握手**：客户端收到服务器的 SYN＋ACK 包，向服务器发送确认包 ACK(tcp协议中ack位置1，确认序号K+1)，此包发送完毕，客户端和服务器进入 ESTABLISHED 状态，完成三次握手。

# 三、四次挥手

[TCP 的四次握手](http://baike.baidu.com/link?url=8_DsYi4pjWpNRFrSX10jiGxe0PLruypbRhv4o56eXOi07tQPokeFgnt1_leXVDy7ELc-uR4_E1cr1NfV3lJUYK)，**是为了保证通信双方都关闭了连接**，具体过程如下：



1）客户端 A 在应用层调用close时会激发底层发送一个 FIN（tcp协议中FIN位置1、序号为M，结合上图分析）请求，用来关闭客户 A 到服务器 B 的数据传送，客户端A此时处于半关闭状态（应用层无法接收数据但底层还可以接收数据）；

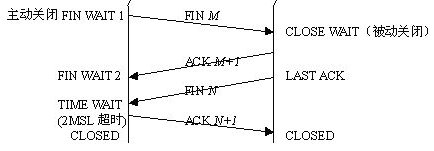
2）服务器 B 底层收到客户端A的FIN时会做两件事

2.1)第1件事：收到客户端A的FIN时底层会主动回发一个ACK（tcp协议中ACK位置1，确认序号M+1）

2.2)第2件事：收到客户端A的FIN时，导致服务器B的应用层read()返回0（告诉服务器B应用层：客户端A关闭了）

3）服务器B应用层调用close()激发底层给客户端 A 发送一个 FIN（tcp协议中FIN位置1、序号为N）,这是服务器B已处于半关闭状态;

4）客户端 A 底层回发 ACK（tcp协议中ACK位置1，确认序号N+1） 给服务器B，这是客户端A、服务器B都处于完全关闭状态，回收相应的资源。



**为什么 TIME\_WAIT 状态还需要等 2MS L后才能返回到 CLOSED 状态？**

是因为我们必须要假想网络是不可靠的，你无法保证你最后发送的 ACK 报文会一定被对方收到，因此对方处于 LAST\_ACK 状态下的 SOCKET 可能会因为超时未收到 ACK 报文，而重发 FIN 报文，所以这个 TIME\_WAIT 状态的作用就是用来重发可能丢失的 ACK 报文。