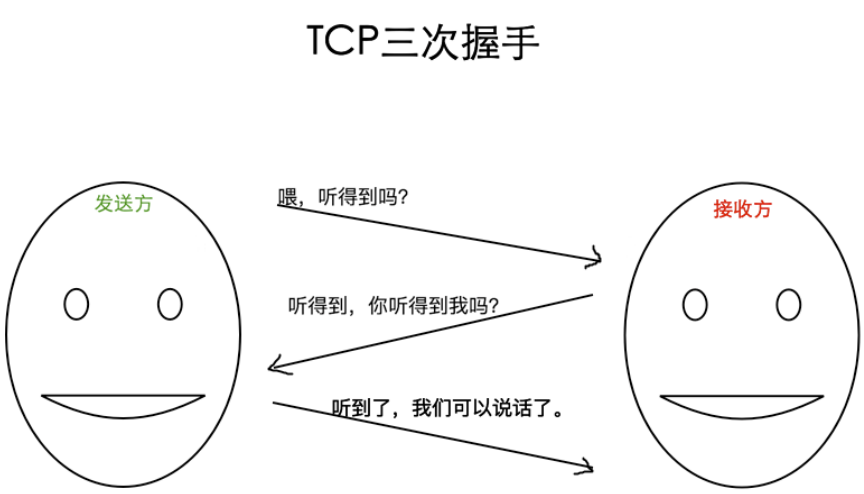
三次握手的过程

三次握手是为了确保双方能够达到沟通的基本保障，举个例子来说



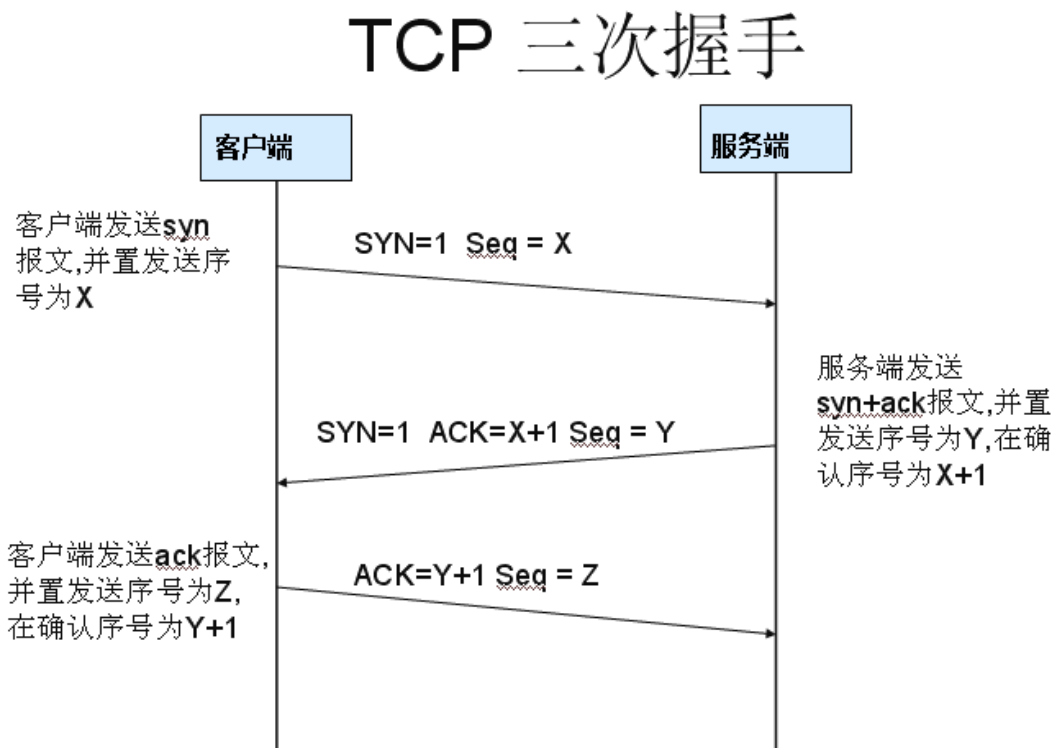
发送方 和 接收方都有两个职责，接受信息（电话听筒） 和 发送信息（麦克风），如果要保证正常的通话

发送方： 麦克风正常、电话听筒正常
接收方： 麦克风正常、电话听筒正常

第一次握手：发送方发送消息给接收方，不确定 麦克风 是否正常，所以发出消息之后接收方需要进行应答。
第二次握手：接收方接到消息，能够说明发送方的麦克风正常，接收方的电话听筒正常。但是不能确定 接收方麦克风是否存在问题，所以作出应答的同时发出询问对方能够收到应答
第三次握手：发送方收到应答，这个时候能够证明 发送方 麦克风 和 电话听筒都是正常的，发送方作出应答 是为了告诉 接收方，接收方麦克风是正常的

tcp三次握手过程

第一次握手（syn）：Client随机产生一个值seq=x，发送给Server并且带有一些标识
第二次握手（syn/ack）：Server收到数据包后得知Client请求建立连接，将x+1，随机产生一个值seq=y，追加自己的标识，发送给Client
第三次握手(ack)：Client收到确认后，给 x 和 y 加 1 并发送握手期间的最后一个ack分组



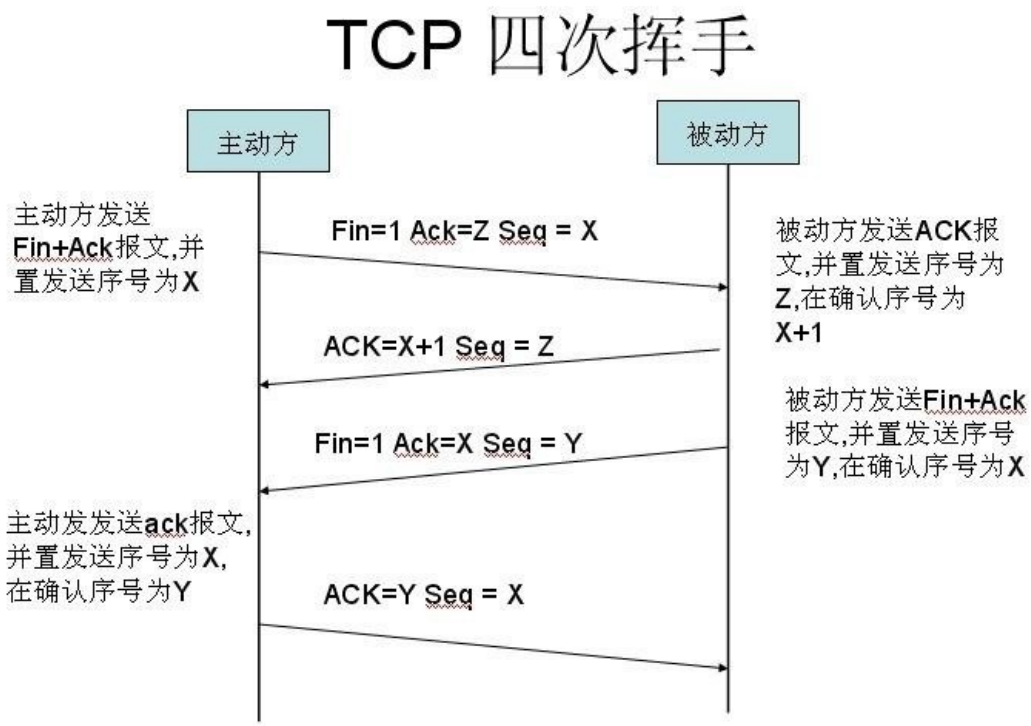
Server端易受到SYN攻击?

服务器端的资源分配是在二次握手时分配的，而客户端的资源是在完成三次握手时分配的，所以服务器容易受到SYN洪泛攻击，SYN攻击就是Client在短时间内伪造大量不存在的IP地址，并向Server不断地发送SYN包，Server则回复确认包，并等待Client确认，由于源地址不存在，因此Server需要不断重发直至超时，这些伪造的SYN包将长时间占用未连接队列，导致正常的SYN请求因为队列满而被丢弃，从而引起网络拥塞甚至系统瘫痪。

防范SYN攻击措施：降低主机的等待时间使主机尽快的释放半连接的占用，短时间受到某IP的重复SYN则丢弃后续请求

四次挥手过程

第一次挥手： Client数据发送完毕，Client向 Server 发送一个FIN，请求关闭数据传输
第二次挥手： 当Server 接收到 Client 的关闭请求时，很可能不是马上关闭请求（Server端还有数据没有发送完毕），向Client发送一个ACK，告诉Client，收到关闭请求
第三次挥手： Server向Client发送一个FIN，告诉Client应用程序关闭
第四次挥手： 当Client收到Server的FIN时，回复一个ACK给Server端，关闭连接



为什么需要四次挥手

第一次挥手：主动方 发起关闭，只能说明 主动方没有 数据要发送了

第二次挥手：被动方 接到关闭请求，很可能不能马上关闭，有可能还有数据没有发送完成，所以先回复一个关闭请求收到了，让主动方等待被动方通知关闭

第三次挥手：被动方 可以关闭了，发送关闭请求，不能马上关闭，要确认关闭被 主动方 收到

第四次挥手：主动方 收到关闭请求，给予回复 可以 关闭了。 断开连接