5.3 TCP协议（中）


TCP连接管理
TCP连接的管理就是使运输连接的建立和释放都能正常进行
连接阶段
连接建立
数据传送
连接释放
TCP连接建立时面对的问题
要使每一方都能够确知对方的存在
要允许双方协商一些参数（如最大窗口值、是否使用窗口扩大选项、时间戳选项及服务质量等）
能够对运输实体资源（如缓存大小、连接表中的项目等）进行分配
连接的建立(三次握手）
客户机的TCP首先向服务器的TCP发送一个连接请求报文段
SYN=1
seq=x
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
SYN = 1
ACK = 1
ack= x+1
seq = y
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
ACK = 1
seq = x+1
ack = y+1
服务器易于受到syn洪泛攻击
连接的释放（四次挥手）
客户机向其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
FIN = 1
seq = u
服务器收到连接释放报文段后即发出确认
ACK =1
seq = v
ack = u+1
服务器通知客户端TCP释放连接
FIN = 1
ACK = 1
seq = w
ack = u+1
客户机受到连接释放报文后，发出确认
ACK = 1
seq = u+1
ack = w+1
SYN洪泛攻击
SYN洪泛攻击发生在OSI第四层，这种方式利用TCP协议的特性，就是三次握手
攻击者发送TCP SYN，SYN是TCP三次握手中的第一个数据包，而当服务器返回ACK后，该攻击者就不对其进行再确认
那这个TCP连接就处于挂起状态，也就是所谓的半连接状态，服务器收不到再确认的话，还会重复发送ACK给攻击者
影响
浪费服务器的资源
在服务器上，这些TCP连接会因为挂起状态而消耗CPU和内存，最后服务器可能死机