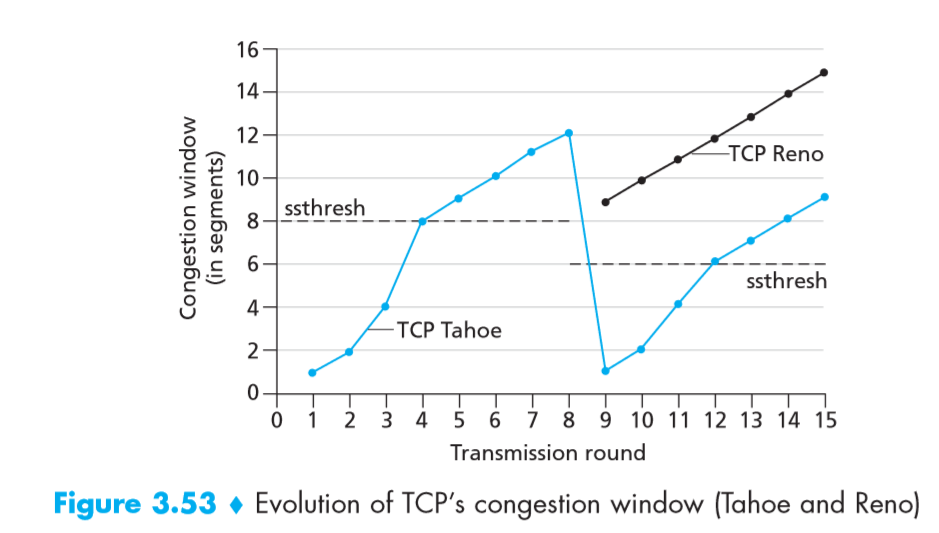


慢开始和拥塞避免：

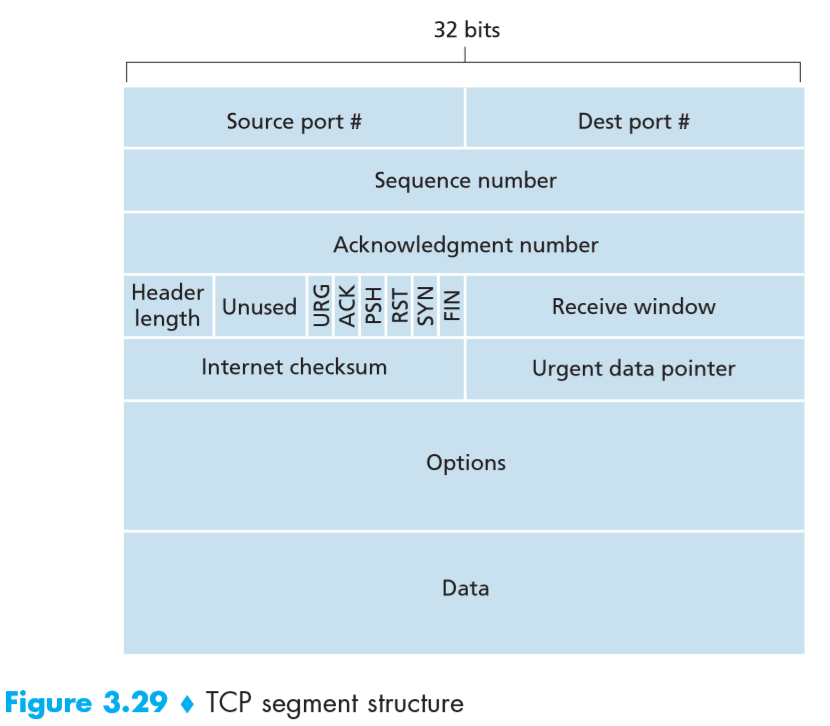
发送方维持一个叫做拥塞窗口（cwnd）的状态变量。拥塞窗口的大小取决于拥塞程度，动态变化。发送方让发送窗口等于拥塞窗口。开始拥塞窗口的值设置为一个最大报文段（MSS）的数值，记为1。如果没有出现拥塞，每经过一个传输轮次，cwnd变为原来的两倍。为了防止过快增加，设置了慢开始门限状态变量（ssthresh）。当检测到超时时，将ssthresh设为原先cwnd的一半，将cwnd置为1，重新开始慢启动，这个过程中当cwnd的大小等于ssthresh时，执行拥塞避免策略，每次cwnd的大小只增加1.

快速重传和快速恢复：快速重传的策略已经在图中有解释。当发送方接收到3个冗余ACK时（但并没有超时），TCP对于这种事件反应没有超时那么激烈，此时执行快速恢复策略：将ssthresh设为原先cwnd的一半，再将cwnd的值减半，之后每次发送时cwnd的值再增加1。

一种称为TCP Tahoe的TCP早期版本没有快速恢复策略，不管是超时还是收到3个冗余ACK，均采用慢开始策略。而较新版本的TCP Reno，则综合了快速恢复。两者的区别如下图：



TCP报文段格式：

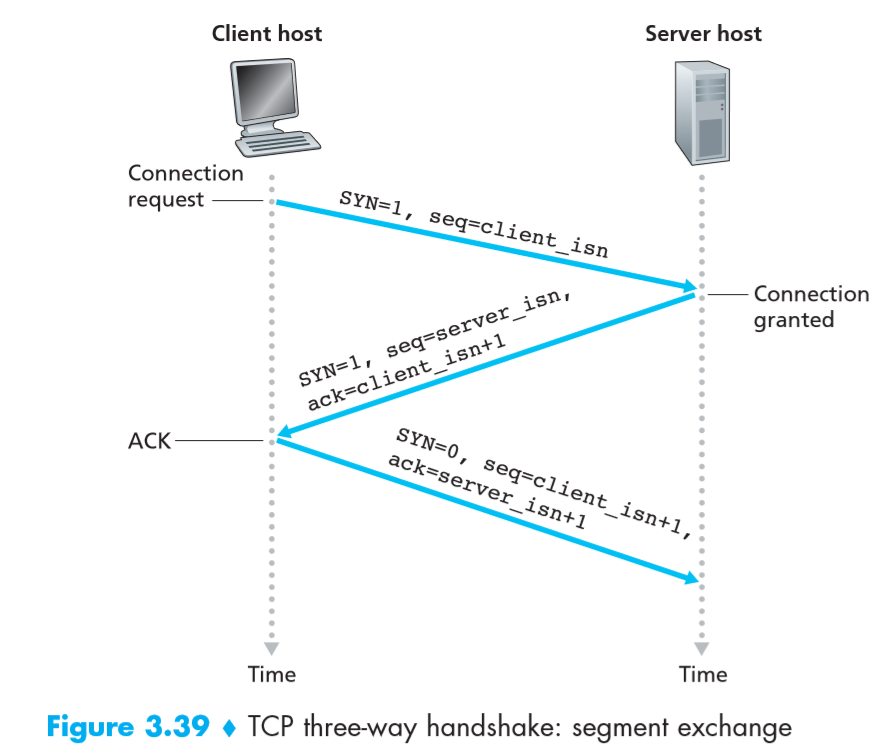


三次握手的过程：

第一次握手：客户端主机向服务器发送一个特殊的TCP报文段，该报文段不包含应用层数据，但是在报文段的首部中的SYN标志位置为1，代表请求建立连接，称为SYN报文段。客户端随机选择一个初始序号，并将此编号放在SYN报文段的序号字段。该报文段被封装在一个网络层数据报中，发送给服务器。

第二次握手：服务器接收到包含SYN报文段的IP数据报，提取出SYN报文段，为该TCP连接分配TCP缓存和变量，并向客户TCP发送允许连接的报文段。该报文段也不包含应用层数据，SYN标志位置为1，确认号字段为SYN报文段的编号+1，服务器选择主机的初始序号，并将其放置到TCP报文段首部的序号字段。这个报文段被称为SYNACK报文段。

第三次握手：客户端收到SYNACK报文段后，也要给该连接分配缓存和变量。同时再向服务器发送另外一个报文段，对于SYNACK报文段给以确认，这个报文段包含了应用层数据。



拓展知识：因为第二次握手（还没有正式开始传送数据）时，服务器就已经给TCP连接分配了缓存资源，这为经典的DoS攻击即SYN洪泛攻击（SYN flood attack）提供了环境。在这种攻击中，攻击者发送大量的TCP SYN报文段，而不完成第三次握手的步骤。随着这种SYN报文段纷至沓来，服务器不断为这些半开连接分配资源（但从未使用），导致服务器的连接资源被消耗殆尽。这种SYN洪泛攻击是被记载的众多DoS攻击中的第一种。

连接释放的过程：

客户端向服务器发送一个特殊的TCP报文段，该报文段FIN标志位置为1。服务器收到后，给发送方回送一个确认报文段。然后服务器发送它自己的终止报文段，其FIN比特被置为1.最后，客户端对服务器的终止报文段进行确认。

