

本节内容

TCP连接管理

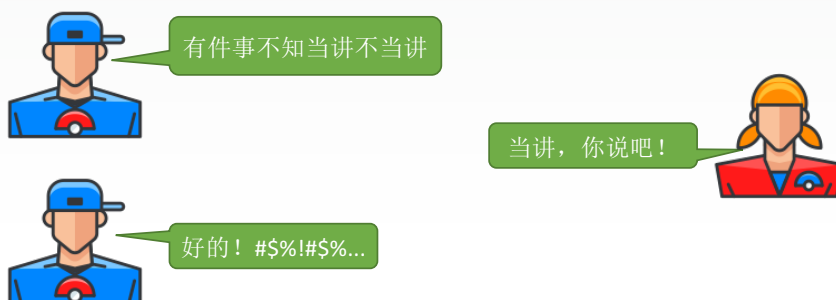
王道考研/CSKAOYAN.COM

TCP连接管理

TCP连接传输三个阶段：



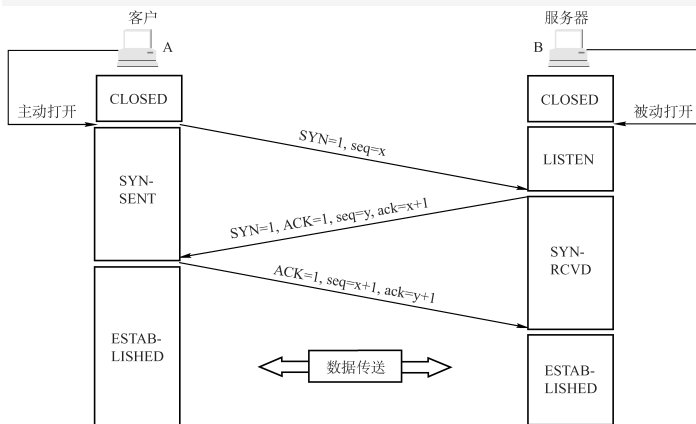
TCP连接的建立采用**客户服务器方式**，主动发起连接建立的应用进程叫做客户，而被动等待连接建立的应用进程叫服务器。



三次握手

王道考研/CSKAOYAN.COM

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：



ROUND 1:

客户端发送**连接请求报文段**，无应用层数据。

$SYN=1, seq=x(\text{随机})$

ROUND 2:

服务器端为该TCP连接**分配缓存和变量**，并向客户端返回**确认报文段**，允许连接，无应用层数据。

$SYN=1, ACK=1, seq=y(\text{随机}), ack=x+1$

ROUND 3:

客户端为该TCP连接**分配缓存和变量**，并向服务器端返回确认的确认，可以携带数据。

$SYN=0, ACK=1, seq=x+1, ack=y+1$

王道考研/CSKAOYAN.COM

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。这样更加会浪费服务器的资源。攻击者就对服务器发送非常大量的这种TCP连接，由于每一个都没法完成三次握手，所以在服务器上，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，就无法为正常用户提供服务了。

SYN cookie

王道考研/CSKAOYAN.COM



四次握手

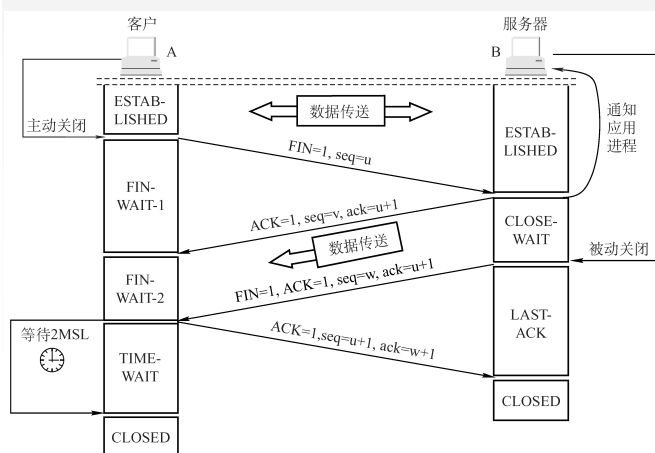


王道考研/CSKAQYAN.COM

TCP的连接释放



参与一条TCP连接的两个进程中的任何一个都能终止该连接，连接结束后，主机中的“资源”（缓存和变量）将被释放。



ROUND 1:

客户端发送**连接释放报文段**，停止发送数据，主动关闭TCP连接。

$FIN=1, seq=u$

ROUND 2:

服务器端回送一个确认报文段，客户到服务器这个方向的连接就释放了——半关闭状态。

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

ROUND 3:

服务器端发完数据，就发出连接释放报文段，主动关闭TCP连接。

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

ROUND 4:

客户端回送一个确认报文段，再等到时间等待计时器设置的2MSL（最长报文段寿命）后，连接彻底关闭。

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

王道考研/CSKAQYAN.COM