[**TCP端口状态说明ESTABLISHED、TIME\_WAIT**](http://www.cnblogs.com/jiunadianshi/articles/2981068.html)

TCP状态转移要点  
TCP协议规定，对于已经建立的连接，网络双方要进行四次握手才能成功断开连接，如果缺少了其中某个步骤，将会使连接处于假死状态，连接本身占用的资源不 会被释放。网络服务器程序要同时管理大量连接，所以很有必要保证无用连接完全断开，否则大量僵死的连接会浪费许多服务器资源。在众多TCP状态中，最值得 注意的状态有两个：CLOSE\_WAIT和TIME\_WAIT。    
  
1、LISTENING状态  
FTP服务启动后首先处于侦听（LISTENING）状态。

2、ESTABLISHED状态  
ESTABLISHED的意思是建立连接。表示两台机器正在通信。

3、CLOSE\_WAIT

    对方主动关闭连接或者网络异常导致连接中断，这时我方的状态会变成CLOSE\_WAIT 此时我方要调用close()来使得连接正确关闭

4、TIME\_WAIT

    我方主动调用close()断开连接，收到对方确认后状态变为TIME\_WAIT。TCP协议规定TIME\_WAIT状态会一直持续2MSL(即两倍的分 段最大生存期)，以此来确保旧的连接状态不会对新连接产生影响。处于TIME\_WAIT状态的连接占用的资源不会被内核释放，所以作为服务器，在可能的情 况下，尽量不要主动断开连接，以减少TIME\_WAIT状态造成的资源浪费。

    目前有一种避免TIME\_WAIT资源浪费的方法，就是关闭socket的LINGER选项。但这种做法是TCP协议不推荐使用的，在某些情况下这个操作可能会带来错误。

5、SYN\_SENT状态

　 　SYN\_SENT状态表示请求连接，当你要访问其它的计算机的服务时首先要发个同步信号给该端口，此时状态为SYN\_SENT，如果连接成功了就变为 ESTABLISHED，此时SYN\_SENT状态非常短暂。但如果发现SYN\_SENT非常多且在向不同的机器发出，那你的机器可能中了冲击波或震荡波 之类的病毒了。这类病毒为了感染别的计算机，它就要扫描别的计算机，在扫描的过程中对每个要扫描的计算机都要发出了同步请求，这也是出现许多 SYN\_SENT的原因。  
  
根 据TCP协议定义的3次握手断开连接规定,发起socket主动关闭的一方 socket将进入TIME\_WAIT状态,TIME\_WAIT状态将持续2个MSL(Max Segment Lifetime),在Windows下默认为4分钟,即240秒,TIME\_WAIT状态下的socket不能被回收使用. 具体现象是对于一个处理大量短连接的服务器,如果是由服务器主动关闭客户端的连接,将导致服务器端存在大量的处于TIME\_WAIT状态的socket, 甚至比处于Established状态下的socket多的多,严重影响服务器的处理能力,甚至耗尽可用的socket,停止服务. TIME\_WAIT是TCP协议用以保证被重新分配的socket不会受到之前残留的延迟重发报文影响的机制,是必要的逻辑保证.  
  
  
windows 机器设置  
在HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters,右键添加名为TcpTimedWaitDelay的  
DWORD键,设置为60,以缩短TIME\_WAIT的等待时间  
  
ubuntu机器设置

vi /etc/sysctl.conf

编辑文件，加入以下内容：  
net.ipv4.tcp\_syncookies = 1  
net.ipv4.tcp\_tw\_reuse = 1  
net.ipv4.tcp\_tw\_recycle = 1  
net.ipv4.tcp\_fin\_timeout = 30

然后执行 /sbin/sysctl -p 让参数生效。

net.ipv4.tcp\_syncookies = 1 表示开启SYN Cookies。当出现SYN等待队列溢出时，启用cookies来处理，可防范少量SYN攻击，默认为0，表示关闭；

net.ipv4.tcp\_tw\_reuse = 1 表示开启重用。允许将TIME-WAIT sockets重新用于新的TCP连接，默认为0，表示关闭；

net.ipv4.tcp\_tw\_recycle = 1 表示开启TCP连接中TIME-WAIT sockets的快速回收，默认为0，表示关闭。

net.ipv4.tcp\_fin\_timeout 修改系統默认的 TIMEOUT 时间

查看系统TCP连接资源命令

netstat

netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'

一般情况下，系统的socket资源默认5000个。（非官方）  
  
TCP协议中有TIME\_WAIT这个状态  
主要有两个原因  
1。防止上一次连接中的包，迷路后重新出现，影响新连接（经过2MSL，上一次连接中所有的重复包都会消失）  
2。可靠的关闭TCP连接。在主动关闭方发送的最后一个 ack(fin) ，有可能丢失，这时被动方会重新发  
fin, 如果这时主动方处于 CLOSED 状态 ，就会响应 rst 而不是 ack。所以主动方要处于 TIME\_WAIT 状态，而不能是 CLOSED 。