netstat - 打印网络连接/路由表/接口统计/伪装连接/多播成员。包含在net-tools工具包中

语法
netstat [option]

参数释义
当前开放的套接口信息
–route, -r　路由表信息
–groups, -g　多播组成员信息
–interfaces, -i　网卡接口信息
–masquerade, -M　伪装连接信息
–statistics, -s　各种协议的汇总信息
–numeric, -n　显示数字形式的主机/端口/用户名
–numeric-hosts　显示数字形式的主机名，不影响端口和用户名解析
–numeric-ports　显示数字形式的端口，不影响主机和用户名解析
–numeric-users　显示数字形式用户名(userID)，不影响主机和端口解析
–protocol=<family >, -A　IP层协议族。如IPv4-inet,IPv6-inet6
–continuous, -c　每秒都进行信息的连续打印
–extend, -e　显示额外的信息。User和Inode信息
–timers, -o　网络计时器信息。其中，第一列代表计时器类型，第二列代表对应的时间值。列表如下:

第一列:
keeplive - keeplive时间计时器
on - 重发时间计时
timewait - 等待时间计时
off - 没有时间计时
第二列(a/b/c):
a - 计与第一列的对应关系如下:
keeplive - keeplive时间，由tcp_keeplive_time确定
on - 重发时间
timewait - 等待时间
b - 已经重发的次数

c - keeplive已发送的probe探测包次数，由tcp_keeplive_probes决定上限

keeplive原理:

1.在tcp_keeplive_time时间内，如果期间发送数据互通，则重置到该值进行倒数；如超过该时间无数据互通，则进入probe探测包发送

2.probe探测包总共发射次数由tcp_keeplive_probes决定，并且发送时间间隔由tcp_keeplive_intvl决定

–programs, -p　套接字所属进程的PID和名称

–listening, -l　只显示正在侦听的套接字

–all, -a　显示所有正在或不在侦听的套接字

-F　显示FIB的路由信息

-C　显示路由缓存信息

TCP连接状态:

ESTABLISHED - 套接字的有效连接

SYN_SENT - 套接字尝试建立连接

SYN_RECV - 套接字接收到连接请求

FIN_WAIT1 - 主动结束方第一次发送FIN后的状态

FIN_WAIT2 - 主动结束方第一次收到ACK后的状态

TIME_WAIT - 主动结束方第一次接收到FIN后的状态

CLOSED - 套接字连接已被关闭

CLOSE_WAIT - 被动结束方第一次接收到FIN后的状态

LASTi_ACK - 被动结束方第一次发送FIN后的状态

LISTEN - 套接字侦听连接。需要指定-l或-a参数

CLOSING - 套接字都已关闭，但还未把所有数据发出

UNKNOWN - 套接字状态未知

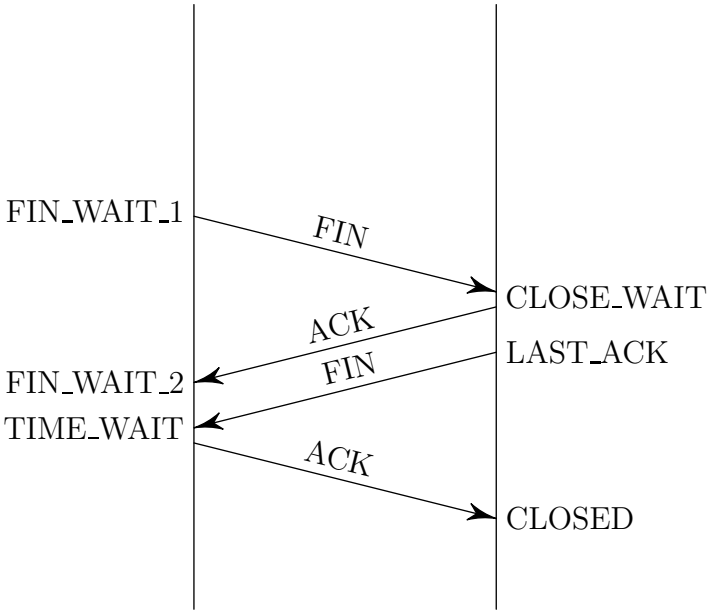
FIN_WAIT_1
FIN
CLOSE_WAIT
ACK
LAST_ACK
FIN_WAIT_2
FIN
TIME_WAIT
ACK
CLOSED

图 1: 四次握手图解