

netstat – network statistics

David Morgan

[Certain] Network statistics

“Print network connections, routing tables, interface statistics,
masquerade connections, and multicast memberships”

netstat man page

Example setting – 3 services/ports

- machine A, 192.168.3.12/CHANG
 - one service in its own right
 - ssh, tcp port 22
 - two services via superserver xinetd
 - echo, tcp port 7
 - chargen, udp port 19
- machine B, 192.168.3.10/monarch; ssh client

Options – a, ut, n, p

conducted thru ssh session from B (192.168.3.10) to A (192.168.3.12)

```

root@CHANG:~# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 176 192.168.3.12:ssh    192.168.3.10:53908     ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State         I-Node Path
unix    2      [ ]     DGRAM      923          @/org/kernel/udev/udev

root@CHANG:~# netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:*                    *:*                    LISTEN
tcp        0      0 *:ssh                  192.168.3.10:53908     LISTEN
tcp        0      0 192.168.3.12:ssh      192.168.3.10:53908     ESTABLISHED
udp        0      0 *:*                    *:*                    LISTEN
udp        0      0 *:chargen              *:*                    LISTEN

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State         I-Node Path
unix    2      [ ]     DGRAM      923          @/org/kernel/udev/udev

root@CHANG:~# netstat -a ut
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:*                    *:*                    LISTEN
tcp        0      0 *:ssh                  192.168.3.10:53908     LISTEN
udp        0      0 *:*                    *:*                    LISTEN

root@CHANG:~# netstat -n
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:7              0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*              LISTEN
tcp        0      0 192.168.3.12:22        192.168.3.10:53908     ESTABLISHED
udp        0      0 0.0.0.0:19            0.0.0.0:*              LISTEN

root@CHANG:~# netstat -a utp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:7              0.0.0.0:*              LISTEN     3551/xinetd
tcp        0      0 0.0.0.0:22             0.0.0.0:*              LISTEN     1615/sshd
udp        0      0 192.168.3.12:22        192.168.3.10:53908     ESTABLISHED 3501/0
udp        0      0 0.0.0.0:19            0.0.0.0:*              LISTEN     3551/xinetd
    
```

Annotations in the image:

- default: open sockets, all protocols (points to `netstat`)
- a(l): include listening (non-"open") (points to `netstat -a`)
- 3 services/ports HERE on A (points to the ssh, echo, and chargen entries in the `netstat -a` output)
- u,t: udp & tcp protocols, specifically & restrictively (points to `netstat -a ut`)
- n: numeric output (address/port/user) (points to `netstat -n`)
- p: PID/program that owns socket (points to `netstat -a utp`)

Mirrored by outside measurement

```
root@monarch:~  
File Edit View Terminal Tabs Help  
[root@monarch ~]# nmap -sTU 192.168.3.12  
  
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-08-02 21:45 PDT  
Interesting ports on CHANG (192.168.3.12):  
(The 3138 ports scanned but not shown below are in state: closed)  
PORT      STATE SERVICE  
7/tcp    open  echo  
19/udp   open  chargen  
22/tcp   open  ssh  
MAC Address: 00:02:B3:41:86:F9 (Intel)  
  
Nmap finished: 1 IP address (1 host up) scanned in 1462.138 seconds  
[root@monarch ~]#
```

same 3 services/ports detected THERE on A
by port scan from here on B

TCP connection states

conducted thru
hit-and-run ssh
command "session"

```
root@monarch:~  
File Edit View Terminal Tabs Help  
[root@monarch ~]# ssh 192.168.3.12 "netstat -pantu"  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name  
tcp        0      0 0.0.0.0:0:7             0.0.0.0:*                LISTEN      3551/xinetd  
tcp        0      0 0.0.0.0:0:22            0.0.0.0:*                LISTEN      1615/sshd  
tcp        0      0 192.168.3.12:22         192.168.3.10:53908      ESTABLISHED 3501/0  
tcp        0      0 192.168.3.12:22         192.168.3.10:45470      ESTABLISHED 3963/sshd: root@not  
udp        0      0 0.0.0.0:0:19           0.0.0.0:*                3551/xinetd  
[root@monarch ~]#  
[root@monarch ~]# netstat -pantu  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name  
tcp        0      0 0.0.0.0:0:32769         0.0.0.0:*                LISTEN      1804/rpc.statd  
tcp        0      0 0.0.0.0:0:111          0.0.0.0:*                LISTEN      1786/portmap  
tcp        0      0 0.0.0.0:0:6000         0.0.0.0:*                LISTEN      2627/X  
tcp        0      0 0.0.0.0:0:23           0.0.0.0:*                LISTEN      2227/xinetd  
tcp        0      0 127.0.0.1:631          0.0.0.0:*                LISTEN      2134/cupsd  
tcp        0      0 127.0.0.1:5335         0.0.0.0:*                LISTEN      2099/mDNSResponder  
tcp        0      0 127.0.0.1:25           0.0.0.0:*                LISTEN      2244/sendmail: acce  
tcp        0      0 192.168.3.10:45470     192.168.3.12:22        TIME_WAIT   -  
tcp        0      0 192.168.3.10:53908     192.168.3.12:22        ESTABLISHED 2789/ssh  
tcp        0      0 :::6000                 :::*                    LISTEN      2627/X  
tcp        0      0 :::22                   :::*                    LISTEN      2218/sshd  
udp        0      0 0.0.0.0:0:32768         0.0.0.0:*                1804/rpc.statd  
udp        0      0 0.0.0.0:0:708          0.0.0.0:*                1804/rpc.statd  
udp        0      0 0.0.0.0:0:5353         0.0.0.0:*                2099/mDNSResponder  
udp        0      0 0.0.0.0:0:111          0.0.0.0:*                1786/portmap  
udp        0      0 0.0.0.0:0:631          0.0.0.0:*                2134/cupsd  
[root@monarch ~]#
```

(but what's a state?)

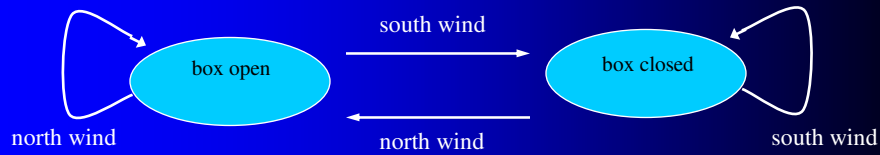
State machines in a nutshell

- a set of states
- a set of inputs (might be events)
- a transition function $f(s,i)$ of state, input
 - if you're in this state
 - and that input comes along
 - to which other state do you transition?
- describe operation of dynamic systems

State machines – example

- square box, lid hinged along south edge
- states – lid is open, lid is closed
- inputs – wind blows north, wind blows south
- transition function $F(\text{state}, \text{input})$
 - box open, wind north \rightarrow box open
 - box open, wind south \rightarrow box closed
 - box closed, wind north \rightarrow box open
 - box closed, wind south \rightarrow box closed

State diagram - example

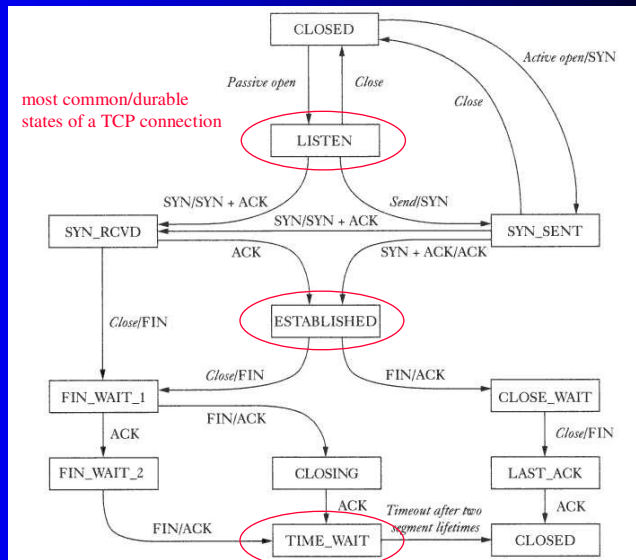


states – ovals

inputs –wind occurrences

transition function – the set of arrows

TCP state diagram



most common/durable states of a TCP connection

states – the rectangles

inputs –receipt of packets with the indicated flag-bit settings

transition function – the set of arrows

see rfc 793

TCP states... wait a minute!

machine A ->

```

root@monarch:~# ssh 192.168.3.12 "netstat -pantu"
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:7              0.0.0.0:*               LISTEN      3551/xinetd
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      1615/sshd
tcp        0      0 192.168.3.12:22       192.168.3.10:53908     ESTABLISHED 3501/0
tcp        0      0 192.168.3.12:22       192.168.3.10:45470     ESTABLISHED 3963/sshd: root@not
udp        0      0 0.0.0.0:19            0.0.0.0:*               LISTEN      3551/xinetd

```

hit-and-run ssh connection lasting a second

machine B ->

```

root@monarch:~# netstat -pantu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:32769         0.0.0.0:*               LISTEN      1804/rpc.statd
tcp        0      0 0.0.0.0:111          0.0.0.0:*               LISTEN      1786/portmap
tcp        0      0 0.0.0.0:6900         0.0.0.0:*               LISTEN      2627/X
tcp        0      0 0.0.0.0:23           0.0.0.0:*               LISTEN      2227/xinetd
tcp        0      0 127.0.0.1:631        0.0.0.0:*               LISTEN      2134/cupsd
tcp        0      0 127.0.0.1:5335       0.0.0.0:*               LISTEN      2099/mDNSResponder
tcp        0      0 127.0.0.1:25         0.0.0.0:*               LISTEN      2244/sendmail: acce
tcp        0      0 192.168.3.10:45470   192.168.3.12:22       TIME_WAIT   -
tcp        0      0 192.168.3.10:53908   192.168.3.12:22       ESTABLISHED 2789/ssh
tcp        0      0 0.0.0.0:8000         0.0.0.0:*               LISTEN      2627/X
tcp        0      0 0.0.0.0:22           0.0.0.0:*               LISTEN      2218/sshd
udp        0      0 0.0.0.0:32768       0.0.0.0:*               LISTEN      1804/rpc.statd
udp        0      0 0.0.0.0:708         0.0.0.0:*               LISTEN      1804/rpc.statd
udp        0      0 0.0.0.0:5353        0.0.0.0:*               LISTEN      2099/mDNSResponder
udp        0      0 0.0.0.0:111         0.0.0.0:*               LISTEN      1786/portmap
udp        0      0 0.0.0.0:631         0.0.0.0:*               LISTEN      2134/cupsd

```

residue of that connection, lasting a minute

same connection

local process "waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request." RFC793

Options – s, statistics (tcp)

```

root@monarch:~# netstat -st
Tcp:
 1 active connections openings
 1 passive connection openings
 0 failed connection attempts
 0 connection resets received
 0 connections established
 41 segments received
 41 segments send out
 0 segments retransmitted
 0 bad segments received.
 0 resets sent
TcpExt:
 1 TCP sockets finished time wait in fast timer
 2 delayed acks sent
 5 packets directly queued to recvng prequeue.
 293 packets directly received from prequeue
 12 packets header predicted
 4 packets header predicted and directly queued to user
 3 acknowledgments not containing data received
 15 predicted acknowledgments
 0 TCP data loss events

```

Options – s, statistics (udp)

```
root@monarch:~  
File Edit View Terminal Tabs Help  
[root@monarch ~]# netstat -su  
Udp:  
  24 packets received  
  0 packets to unknown port received.  
  0 packet receive errors  
  24 packets sent  
[root@monarch ~]#
```

Options – s, statistics (ip)

```
root@monarch:~  
File Edit View Terminal Tabs Help  
[root@monarch ~]# netstat -sw  
Ip:  
 38711 total packets received  
 0 forwarded  
 0 incoming packets discarded  
1031 incoming packets delivered  
1088 requests sent out  
38622 reassemblies required  
942 packets reassembled ok  
1000 fragments received ok  
Icmp:  
 964 ICMP messages received  
 0 input ICMP message failed.  
ICMP input histogram:  
  echo replies: 964  
  0 ICMP messages sent  
  0 ICMP messages failed  
ICMP output histogram:  
[root@monarch ~]#
```

Options – i, traffic measurement

```

root@monarch:~# netstat -l eth0
Kernel Interface table
Iface      MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500  0    12251      0      0      0    11279      0      0      0 BMRU

[root@monarch ~]# ping -f -c 100 192.168.3.12
PING 192.168.3.12 (192.168.3.12) 56(84) bytes of data.

--- 192.168.3.12 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 1599ms
rtt min/avg/max/mdev = 0.108/0.118/0.379/0.029 ms, pipe 2, ipg/ewma 16.153/0.116 ms

[root@monarch ~]# netstat -l eth0
Kernel Interface table
Iface      MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500  0    12351      0      0      0    11379      0      0      0 BMRU
    
```

← hundred pings, out and in

plus 100 in (RX)

plus 100 out (TX)

Options – i, traffic measurement

```

root@monarch:~# netstat -l eth0; netstat -sw
Kernel Interface table
Iface      MTU Met  RX OK RX ERR RX DRP RX OVR    TX OK TX ERR TX DRP TX OVR Flg
eth0      1500  0    77283      0      0      0    81991      0      0      0 BMRU

Ip:
77352 total packets received
0 forwarded
0 incoming packets discarded
1952 incoming packets delivered
2066 requests sent out
77285 reassemblies required
1885 packets reassembled ok
2000 fragments received ok

icmp:
1385 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
  echo replies: 1335
  0 ICMP messages sent
  0 ICMP messages failed
  ICMP output histogram:
    
```

before

```

root@monarch:~# ping -s 6000 -c 1000 192.168.3.2
PING 192.168.3.2 (192.168.3.2): 6000(6008) bytes of data.
.....
--- 192.168.3.2 ping statistics ---
1000 packets transmitted, 948 received, 5% packet loss, time 1308/ms
rtt min/avg/max/mdev = 15.217/22.474/42.749/5.368 ms, pipe 5, ipg/ewma 13.100/18.504 ms

root@monarch:~# netstat -l eth0; netstat -sw
Kernel Interface table
Iface      MTU Met  RX OK RX ERR RX DRP RX OVR    TX OK TX ERR TX DRP TX OVR Flg
eth0      1500  0    116162      0      0      0    122992      0      0      0 BMRU

Ip:
116220 total packets received
0 forwarded
0 incoming packets discarded
2600 incoming packets delivered
3066 requests sent out
116153 reassemblies required
2833 packets reassembled ok
3000 fragments received ok

icmp:
2833 ICMP messages received
0 input ICMP message failed.
ICMP input histogram:
  echo replies: 2633
  0 ICMP messages sent
  0 ICMP messages failed
  ICMP output histogram:
    
```

after

IP packets: 116220-77352=38868

ICMP messages: 2833-1885=948

messages split into 41 packets each (38868/948)

ethernet carries 1 packet per frame

1464-byte ave payload per frame (60028/41)

approximates ethernet's maximum