

NETSTAT Utility Tutorial

Course: Computer Networks (CS - 307) **Instructor:** Mr Ibrahim Nadir **Fall 2019**
National University of Computer and Emerging Sciences, Lahore

Introduction

Netstat utility is used to get information about network connections, routing tables and interface statistics. This utility is available cross platform, it can be found builtin on Windows, OS X and Linux. However there might be a slight difference in syntax of usage. This utility is considered very useful for network administrators to troubleshoot network related problems.

Usage

netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p protocol] [-r] [-s] [-t] [-x] [-y] [time_interval] [/?]

| Sr. | Switch | Description |
|-----|--------|---|
| 1 | a | Displays active TCP connections, TCP connections with the listening state, as well as UDP ports that are being listened to. |
| 2 | b | Display the process's actual file name associated with connection. |
| 3 | f | Display the Fully Qualified Domain Name (FQDN) for each foreign IP addresses when possible. |

* For information about other switches see the man page of netstat. For Linux use command “man netstat”.

Experimentation

Here some executions of netstat command/utility are provided.

1. Switch -a

(-a) All active TCP/UDP connections and their states.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -a  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 *:ssh                   *:                        LISTEN  
tcp        0      0 localhost:ipp           *:                        LISTEN  
tcp        0      0 localhost:mysql         *:                        LISTEN  
tcp        0      0 hafizmaazahmad-P:domain *:                        LISTEN  
tcp        0      0 192.168.3.9:36466       fjr02s03-in-f10.1:https ESTABLISHED  
tcp        0      0 192.168.3.9:58252       fjr02s08-in-f2.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:33928       13.75.106.0:https       ESTABLISHED  
tcp        0      0 192.168.3.9:50284       104.25.57.103:https     ESTABLISHED  
tcp        0      0 192.168.3.9:38972       zrh04s08-in-f10.1:https ESTABLISHED  
tcp        0      0 192.168.3.9:56442       fjr02s04-in-f8.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:49710       104.20.133.40:https     ESTABLISHED  
tcp        0      0 192.168.3.9:43962       52.175.28.154:https     ESTABLISHED  
tcp        0      0 192.168.3.9:54576       ws-in-f189.1e100.:https ESTABLISHED  
tcp        0      0 192.168.3.9:51260       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:51308       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:38862       104.27.176.254:https    ESTABLISHED  
tcp        0      0 192.168.3.9:51262       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:58250       fjr02s08-in-f2.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:50308       fjr02s04-in-f14.1:https ESTABLISHED  
tcp        0      0 192.168.56.1:40428       192.168.56.105:ssh      ESTABLISHED  
tcp        0      0 192.168.3.9:56594       1f.7d.089f.ip4.st:https ESTABLISHED
```

(-at) All active TCP connections and their states.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -at  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 *:ssh                   *:                        LISTEN  
tcp        0      0 localhost:ipp           *:                        LISTEN  
tcp        0      0 localhost:mysql         *:                        LISTEN  
tcp        0      0 hafizmaazahmad-P:domain *:                        LISTEN  
tcp        0      0 192.168.3.9:36466       fjr02s03-in-f10.1:https ESTABLISHED  
tcp        0      0 192.168.3.9:58252       fjr02s08-in-f2.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:33928       13.75.106.0:https       ESTABLISHED  
tcp        0      0 192.168.3.9:50284       104.25.57.103:https     ESTABLISHED  
tcp        0      0 192.168.3.9:38972       zrh04s08-in-f10.1:https ESTABLISHED  
tcp        0      0 192.168.3.9:56442       fjr02s04-in-f8.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:49710       104.20.133.40:https     ESTABLISHED  
tcp        0      0 192.168.3.9:43962       52.175.28.154:https     ESTABLISHED  
tcp        0      0 192.168.3.9:54576       ws-in-f189.1e100.:https ESTABLISHED  
tcp        0      0 192.168.3.9:51260       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:51308       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:38862       104.27.176.254:https    ESTABLISHED  
tcp        0      0 192.168.3.9:51262       zrh04s07-in-f174.:https ESTABLISHED  
tcp        0      0 192.168.3.9:58250       fjr02s08-in-f2.1e:https ESTABLISHED  
tcp        0      0 192.168.3.9:50308       fjr02s04-in-f14.1:https ESTABLISHED  
tcp        0      0 192.168.56.1:40428       192.168.56.105:ssh      ESTABLISHED  
tcp        0      0 192.168.3.9:56594       1f.7d.089f.ip4.st:https ESTABLISHED
```

(-au) All active UDP connections and their states.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -au  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
udp        0      0 *:57399                 *:                        *:*  
udp        0      0 *:bootpc                *:                        *:*  
udp        0      0 *:ipp                    *:                        *:*  
udp        0      0 *:mdns                   *:                        *:*  
udp        0      0 *:55213                  *:                        *:*  
udp        0      0 *:35010                  *:                        *:*  
udp        0      0 hafizmaazahmad-P:domain *:                        *:*  
udp6       0      0 [::]:33152              [::]:*                  [::]:*  
udp6       0      0 [::]:mdns                [::]:*                  [::]:*  
hafizmaazahmad@hafizmaazahmad-PC:~$
```

2- Switch -b

(-b) File names and relative paths to files associated with connections.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat b  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 192.168.3.9:43962       client-s.gateway.:https ESTABLISHED  
tcp        0      0 192.168.3.9:54576       ws-in-f189.1e100.:https ESTABLISHED  
tcp        0      0 192.168.3.9:50986       play.google.com:https  ESTABLISHED  
tcp        0      0 192.168.56.1:40428      192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:59894       ec2-34-210-150-24:https ESTABLISHED  
tcp        0      0 192.168.3.9:49990       clients6.google.c:https ESTABLISHED  
tcp        0      0 192.168.56.1:40424      192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:49992       clients6.google.c:https ESTABLISHED  
tcp        0      0 192.168.56.1:40426      192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:60944       13.107.42.11:https     ESTABLISHED  
tcp        0      0 192.168.3.9:33704       13.75.106.0:https      ESTABLISHED  
tcp        0      0 192.168.3.9:51380       ssl.gstatic.com:https  ESTABLISHED  
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags      Type       State       I-Node      Path  
unix    2      [ ]       DGRAM      -           22331       /run/user/1000/system  
d/notify  
unix    3      [ ]       DGRAM      -           11374       /run/systemd/notify  
unix    7      [ ]       DGRAM      -           11385       /run/systemd/journal/  
socket  
unix    19     [ ]       DGRAM      -           11407       /run/systemd/journal/  
dev-log
```

(-ltpe) Usernames and processes associated with connections.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -ltpe  
(Not all processes could be identified, non-owned process info  
will not be shown, you would have to be root to see it all.)  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User        Inode      PID/Program name  
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*                LISTEN      root        439717     -  
tcp        0      0 0.0.0.0:ipp             0.0.0.0:*                LISTEN      root        388381     -  
tcp        0      0 0.0.0.0:mysql             0.0.0.0:*                LISTEN      mysql       22903     -  
tcp        0      0 0.0.0.0:hafizmaazahmad-P:domain 0.0.0.0:*                LISTEN      root        22407     -  
tcp6       0      0 [::]:ssh               [::]:*                 LISTEN      root        439719     -  
tcp6       0      0 ip6-localhost:40886    [::]:*                 LISTEN      hafizmaazahmad 203830    10871/java  
  
tcp6       0      0 ip6-localhost:ipp      [::]:*                 LISTEN      root        388380     -  
tcp6       0      0 [::]:http              [::]:*                 LISTEN      root        23795     -  
hafizmaazahmad@hafizmaazahmad-PC:~$
```

3- Switch -f

Displays FQDNs associated with foreign IPs (when possible).

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -f  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 192.168.3.9:43962      client-s.gateway.:https ESTABLISHED  
tcp        0      0 192.168.3.9:54576      0.client-channel.:https ESTABLISHED  
tcp        0      0 192.168.3.9:36610      mail.google.com:https  ESTABLISHED  
tcp        0      0 192.168.3.9:50986      zrh04s07-in-f14.1:https ESTABLISHED  
tcp        0      0 192.168.56.1:40428     192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:59894      ec2-34-210-150-24:https ESTABLISHED  
tcp        0      0 192.168.3.9:49990      clients6.google.c:https ESTABLISHED  
tcp        0      0 192.168.56.1:40424     192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:49992      clients6.google.c:https ESTABLISHED  
tcp        0      0 192.168.56.1:40426     192.168.56.105:ssh     ESTABLISHED  
tcp        0      0 192.168.3.9:60944      13.107.42.11:https     ESTABLISHED  
tcp        0      0 192.168.3.9:33704      13.75.106.0:https      ESTABLISHED  
tcp        0      0 192.168.3.9:51380      ssl.gstatic.com:https  ESTABLISHED  
  
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags      Type       State       I-Node      Path  
unix    2      [ ]       DGRAM      -           22331       /run/user/1000/system  
d/notify  
unix    3      [ ]       DGRAM      -           11374       /run/systemd/notify  
unix    7      [ ]       DGRAM      -           11385       /run/systemd/journal/  
socket  
unix    19     [ ]       DGRAM      -           11407       /run/systemd/journal/
```

4- Switch -nr

Displays Kernel routing table of host machine.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -nr  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags      MSS  Window  irtt  Iface  
0.0.0.0          192.168.3.1     0.0.0.0          UG         0 0      0     wlp9s0  
169.254.0.0      0.0.0.0         255.255.0.0      U         0 0      0     wlp9s0  
192.168.3.0      0.0.0.0         255.255.255.0    U         0 0      0     wlp9s0  
192.168.56.0     0.0.0.0         255.255.255.0    U         0 0      0     vboxnet  
0  
hafizmaazahmad@hafizmaazahmad-PC:~$
```

5- Switch -s

Displays all network statistics.

```
hafizmaazahmad@hafizmaazahmad-PC: ~  
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -s  
Ip:  
  846128 total packets received  
  12 with invalid addresses  
  0 forwarded  
  0 incoming packets discarded  
 837255 incoming packets delivered  
 616317 requests sent out  
  164 outgoing packets dropped  
  834 dropped because of missing route  
Icmp:  
  360 ICMP messages received  
  0 input ICMP message failed.  
  ICMP input histogram:  
    destination unreachable: 360  
  360 ICMP messages sent  
  0 ICMP messages failed  
  ICMP output histogram:  
    destination unreachable: 360  
IcmpMsg:  
  InType3: 360  
  OutType3: 360  
Tcp:  
  2768 active connections openings
```

* It was an introductory tutorial, for detailed information read man page.