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 A
tcp 0 0 *:ssh *:*
                                                                                            Foreign Address
                                                                                                                                              State
                                                                                                                                              LISTEN
                                         localhost:ipp
                                                                                                                                              LISTEN
tcp
                      0
                                     0
                                     O localhost:mysql *:*
O hafizmaazahmad-P:domain *:*
                                                                                            *:*
                                                                                                                                              LISTEN
                      0
tcp
                                    0 hafizmaazahmad-P:dc

0 192.168.3.9:36466

0 192.168.3.9:58252

0 192.168.3.9:33928

0 192.168.3.9:38972

0 192.168.3.9:38972

0 192.168.3.9:56442

0 192.168.3.9:49710

0 192.168.3.9:49710

0 192.168.3.9:4576

0 192.168.3.9:54576

0 192.168.3.9:51260

0 192.168.3.9:51308

0 192.168.3.9:51262

0 192.168.3.9:51262

0 192.168.3.9:53260

0 192.168.3.9:53260

0 192.168.3.9:50308

0 192.168.3.9:50308
                      0
                                                                                                                                              LISTEN
tcp
                                                                                           fjr02s03-in-f10.1:https
fjr02s08-in-f2.1e:https
13.75.106.0:https
104.25.57.103:https
zrh04s08-in-f10.1:https
fjr02s04-in-f8.1e:https
                                                                                                                                              ESTABLISHED
                      0
tcp
                                                                                                                                              ESTABLISHED
                      0
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                                                                                                                                              ESTABLISHED
                      0
tcp
                                                                                           104.20.133.40:https
52.175.28.154:https
ws-in-f189.1e100.:https
                      0
                                                                                                                                              ESTABLISHED
tcp
                                                                                                                                              ESTABLISHED
                      0
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                                                                                           zrh04s07-in-f174.:https
zrh04s07-in-f174.:https
104.27.176.254:https
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                                                                                            zrh04s07-in-f174.:https
fjr02s08-in-f2.1e:https
fjr02s04-in-f14.1:https
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                      0
                                                                                                                                              ESTABLISHED
tcp
                                                                                            192.168.56.105:ssh
                                                                                                                                              ESTABLISHED
tcp
                                          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 A
tcp 0 0 *:ssh *:*
                                                                                                                       Foreign Address
                                                                                                                                                                                         State
                                                                                                                                                                                         LISTEN
                                                      localhost:ipp
tcp
                             0
                                                 0
                                                                                                                                                                                         LISTEN
                                                      localhost:mysql
tcp
                             0
                                                                                                                                                                                         LISTEN
                                               0 hafizmaazahmad-P:do
0 192.168.3.9:36466
0 192.168.3.9:58252
0 192.168.3.9:33928
0 192.168.3.9:38972
0 192.168.3.9:38972
0 192.168.3.9:56442
0 192.168.3.9:49710
0 192.168.3.9:43962
0 192.168.3.9:54576
0 192.168.3.9:51260
0 192.168.3.9:51260
0 192.168.3.9:51262
0 192.168.3.9:51262
0 192.168.3.9:53262
0 192.168.3.9:50262
0 192.168.3.9:50308
0 192.168.3.9:50308
                                                     hafizmaazahmad-P:domain *:*
tcp
                             0
                                                                                                                                                                                          LISTEN
                                                                                                                       #:#
fjr02s03-in-f10.1:https ESTABLISHED
fjr02s08-in-f2.1e:https ESTABLISHED
13.75.106.0:https ESTABLISHED
104.25.57.103:https ESTABLISHED
zrh04s08-in-f10.1:https ESTABLISHED
fjr02s04-in-f8.1e:https ESTABLISHED
tcp
                             0
tcp
                             0
tcp
tcp
                             0
tcp
                             0
tcp
                             0
                                                                                                                       104.20.133.40:https ESTABLISHED 52.175.28.154:https ESTABLISHED ws-in-f189.1e100.:https ESTABLISHED zrh04s07-in-f174.:https ESTABLISHED 2rh04s07-in-f174.:https ESTABLISHED 104.27.176.254:https ESTABLISHED 104.27.176.254:https ESTABLISHED ESTABLISHED
                             0
tcp
tcp
                             0
tcp
                             0
                             0
0
tcp
tcp
tcp
                             0
0
                                                                                                                        zrh04s07-in-f174.:https ESTABLISHED
tcp
                                                                                                                        fjr02s08-in-f2.1e:https ESTABLISHED
fjr02s04-in-f14.1:https ESTABLISHED
                             0
tcp
                             0
tcp
                             0
                                                                                                                        192.168.56.105:ssh
tcp
                                                                                                                                                                                         ESTABLISHED
                                                                                                                        1f.7d.089f.ip4.st:https ESTABLISHED
                                                 0 192.168.3.9:56594
```

(-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 A
udp 0 0 *:57399 *:*
udp 0 0 *:bootpc *:*
                                                             Foreign Áddress
                                                                                              State
               0
                        0 *:ipp
udp
                          *:mdns
               0
udp
               0
                         0 *:55213
udp
                           *:35010
               0
udp
               0
                         0 hafizmaazahmad-P:domain
udp
                        0 [::]:33152
0 [::]:mdns
                                                             [::]:*
[::]:*
udp6
udp6
               0
hafizmaazahmad@hafizmaazahmad-PC:~$
```

2- Switch -b

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

```
🔊 🖨 🗊 hafizmaazahmad@hafizmaazahmad-PC: ~

        hafizmaazahmad@hafizmaazahmad-PC:~$ netsta

        Active Internet connections (w/o servers)

        Proto Recv-Q Send-Q Local Address

        tcp
        0
        192.168.3.9:43962

        tcp
        0
        192.168.3.9:54576

        tcp
        0
        192.168.3.9:50986

        tcp
        0
        192.168.56.1:40428

        tcp
        0
        192.168.3.9:59884

        tcp
        0
        192.168.3.9:49990

        tcp
        0
        192.168.3.9:49990

        tcp
        0
        192.168.3.9:49992

        tcp
        0
        192.168.3.9:49992

        tcp
        0
        192.168.3.9:60944

        tcp
        0
        192.168.3.9:53704

        tcp
        0
        0
        192.168.3.9:51380

        Active UNIX domain sockets (w/o servers)
        0

 hafizmaazahmad@hafizmaazahmad-PC:~$ netstat b
                                                                                                                            Foreign Address
                                                                                                                                                                                                State
                                                                                                                           client-s.gateway.:https ESTABLISHED
ws-in-f189.1e100.:https ESTABLISHED
                                                                                                                           play.google.com:https
192.168.56.105:ssh
ec2-34-210-150-24:https
                                                                                                                                                                                                ESTABLISHED
ESTABLISHED
                                                                                                                                                                                                ESTABLISHED
                                                                                                                            clients6.google.c:https
192.168.56.105:ssh
                                                                                                                                                                                                ESTABLISHED
                                                                                                                                                                                                ESTABLISHED
                                                                                                                           192.108.30.103.351
clients6.google.c:https
192.168.56.105:ssh
13.107.42.11:https
13.75.106.0:https
                                                                                                                                                                                               ESTABLISHED
                                                                                                                                                                                                ESTABLISHED
                                                                                                                                                                                                ESTABLISHED
                                                                                                                                                                                                ESTABLISHED
tcp 0 0 192.168.3.9:51380
Active UNIX domain sockets (w/o servers)
                                                                                                                            ssl.gstatic.com:https
                                                                                                                                                                                                ESTABLISHED
 Proto RefCnt Flags
                                                                                                     State
                                                                                                                                             I-Node
 unix
                                                                       DGRAM
                                                                                                                                             22331
                                                                                                                                                                      /run/user/1000/system
                                     [ ]
 d/notify
                                     [ ]
 unix 3
                                                                       DGRAM
                                                                                                                                             11374
                                                                                                                                                                       /run/systemd/notify
 unix
                                                                       DGRAM
                                                                                                                                             11385
                                                                                                                                                                      /run/systemd/journal/
 socket
 unix 19
                                     []
                                                                       DGRAM
                                                                                                                                             11407
                                                                                                                                                                      /run/systemd/journal/
```

(-ltpe) Usernames and processes associated with connections.

```
👂 🗎 🕦 hafizmaazahmad@hafizmaazahmad-PC: ~
 nafizmaazahmad@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

tcp 0 0 *:ssh

*:*
                                                                                            State
                                                                                                            User
                                                                                                                           Inode
                                                                                                                                           PID/Program name
                                                                                            LISTEN
                                                                                                                           439717
                                                                                                            root
                        0 localhost:ipp
                                                                                            LISTEN
                                                                                                                           388381
 tcp
                                                                                                            root
                        0 localhost:mysql
                                                                                            LISTEN
                                                                                                                           22903
 tcp
                                                                                                            mysql
                        0 hafizmaazahmad-P:domain *:*
                                                                                            LISTEN
                                                                                                                           22407
 tcp
                                                                                                            root
                        0 [::]:ssh
                                                                                            LISTEN
                                                                                                            root
                                                                                                                           439719
 tcp6
                        0 ip6-localhost:40886
                                                                                            LISTEN
                                                                                                            hafizmaazahmad 203830
                                                                                                                                                 10871/java
 tcp6
                        0 ip6-localhost:ipp
                                                                                            LISTEN
                                                                                                                           388380
 tcp6
                                                            [::]:*
[::]:*
                                                                                                            root
                                                                                            LISTEN
                                                                                                                           23795
tcp6
                        0 [::]:http
                                                                                                            root
  afizmaazahmad@hafizmaazahmad-PC:~$
```

3- Switch -f

Displays FQDNs associated with foreign IPs (when possible).

```
😑 🗊 hafizmaazahmad@hafizmaazahmad-PC: ~
  hafizmaazahmad@hafizmaazahmad-PC:~$ netstat f
hafizmaazahmad@hafizmaazahmad-PC:~$ netst:
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address
tcp 0 192.168.3.9:43962
tcp 0 0 192.168.3.9:54576
tcp 0 0 192.168.3.9:36610
tcp 0 0 192.168.3.9:50986
tcp 0 0 192.168.3.9:59894
tcp 0 0 192.168.3.9:59894
tcp 0 0 192.168.3.9:49990
tco 0 0 192.168.56.1:40424
                                                                                       Foreign Address
                                                                                                                                      State
                                                                                       client-s.gateway.:https
0.client-channel.:https
                                                                                                                                      ESTABLISHED
                                                                                                                                      ESTABLISHED
                                                                                       mail.google.com:https ESTABLISHED
zrh04s07-in-f14.1:https ESTABLISHED
192.168.56.105:ssh ESTABLISHED
ec2-34-210-150-24:https ESTABLISHED
                                                                                       clients6.google.c:https
192.168.56.105:ssh
                      0
                                                                                                                                      ESTABLISHED
                                   0 192.168.56.1:40424

0 192.168.39:49992

0 192.168.39:49992

0 192.168.3.9:60944

0 192.168.3.9:33704

0 192.168.3.9:51380
                                                                                                                                      ESTABLISHED
 tcp
                                                                                       clients6.google.c:https
192.168.56.105:ssh
13.107.42.11:https
                                                                                                                                      ESTABLISHED
                      0
 tcp
                      0
 tcp
                                                                                                                                      ESTABLISHED
                      0
                                                                                                                                      ESTABLISHED
 tcp
 tcp
                      0
                                                                                       13.75.106.0:https
                                                                                                                                      ESTABLISHED
                                                                                       ssl.gstatic.com:https
                                                                                                                                      ESTABLISHED
 tcp
                      0
 Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags
unix 2 []
                                                 Type
DGRAM
                                                                                                   I-Node
                                                                                                                     Path
                                                                       State
unix 2
d/notify
                                                                                                                     /run/user/1000/system
                                                                                                   22331
                                                                                                                     /run/systemd/notify
/run/systemd/journal/
unix 3
unix 7
                                                 DGRAM
                                                                                                   11374
                                                 DGRAM
                                                                                                   11385
 socket
                                                 DGRAM
                                                                                                                     /run/systemd/journal/
 unix
                                                                                                   11407
            19
```

4- Switch -nr

Displays Kernel routing table of host machine.

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