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.

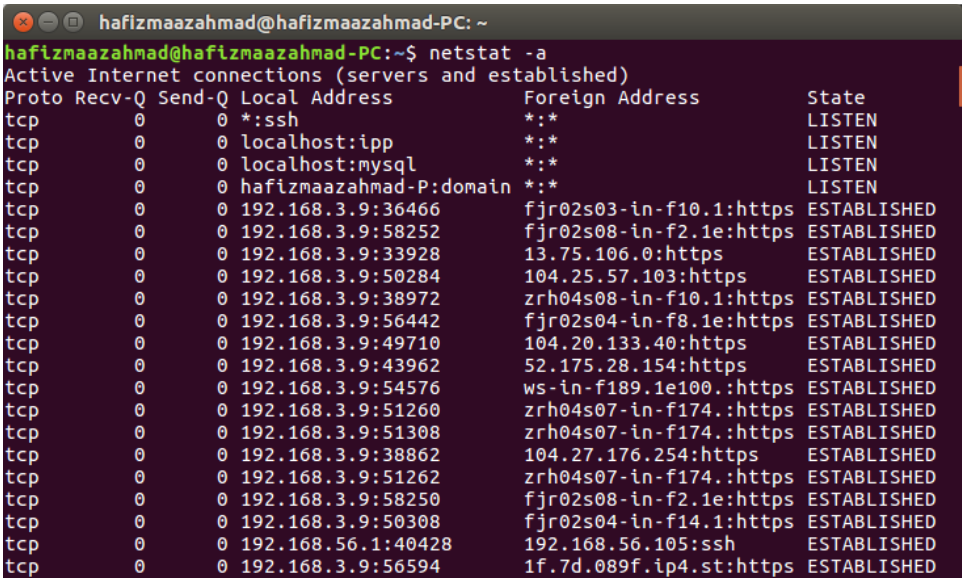
* For information about other switches see the man page of netstat. For Linux use command “man netstat”.

Experimentation

Here some executions of netstat command/utility are provided.

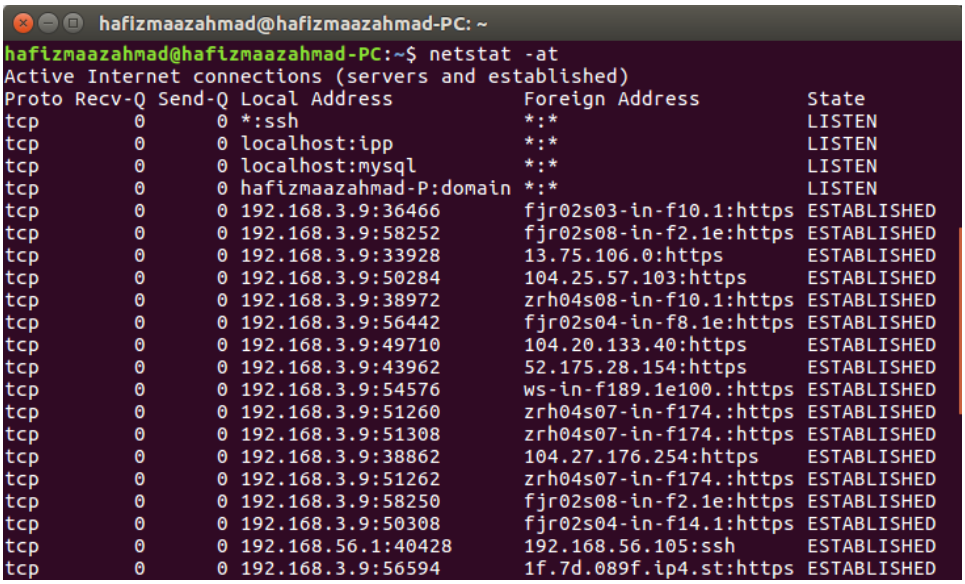
1. Switch -a

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



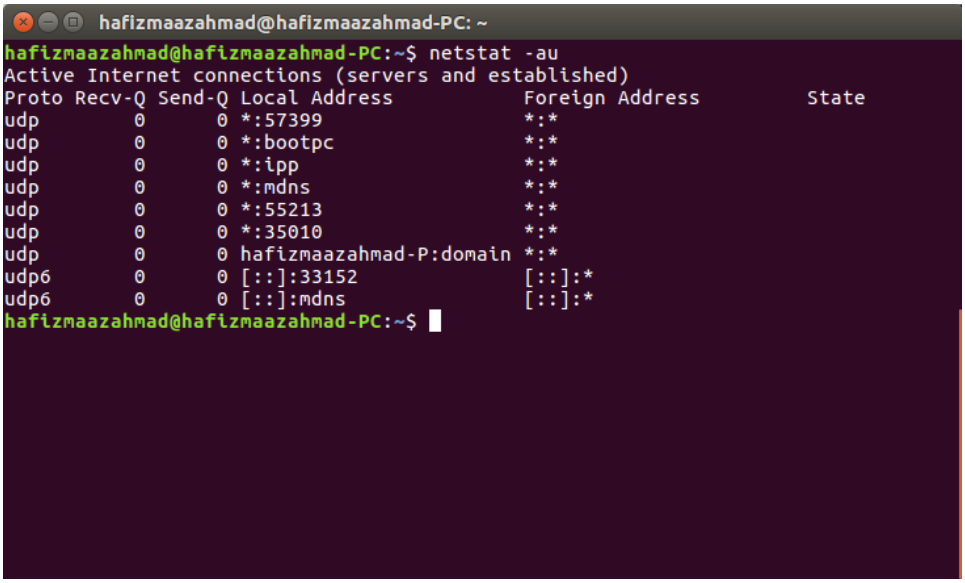
```
hafizmaazahmad@hafizmaazahmad-PC: ~
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        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.



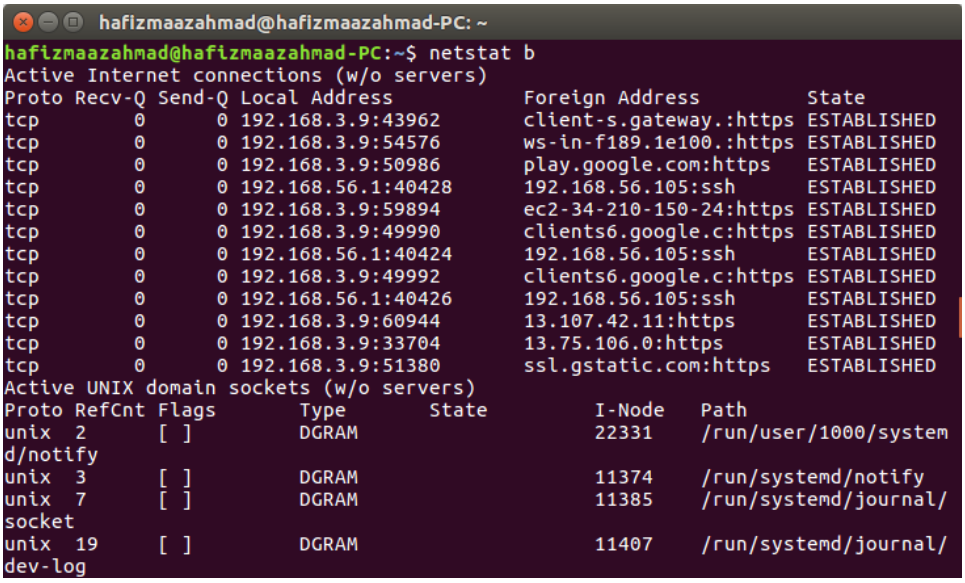
```
hafizmaazahmad@hafizmaazahmad-PC: ~
hafizmaazahmad@hafizmaazahmad-PC:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        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.

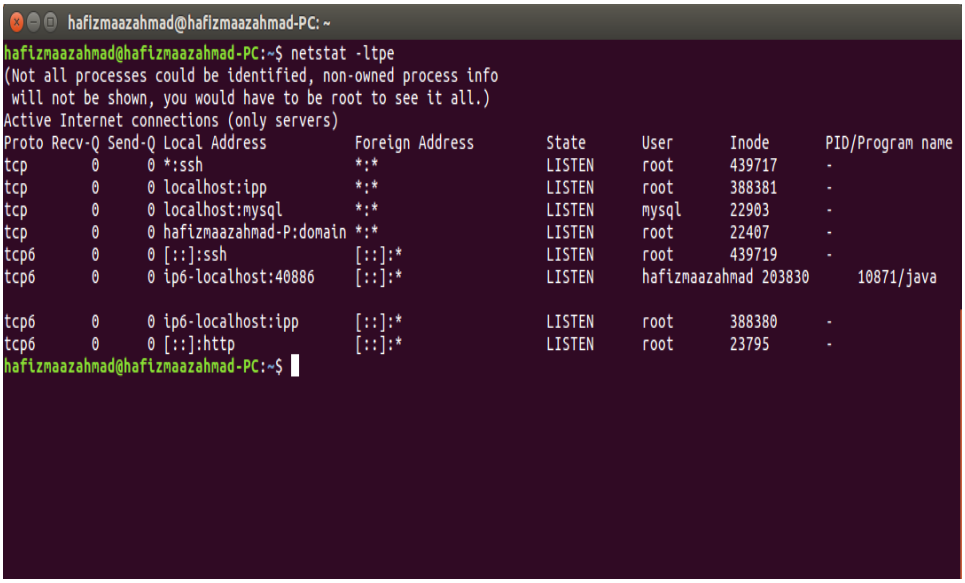


2- Switch -b

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

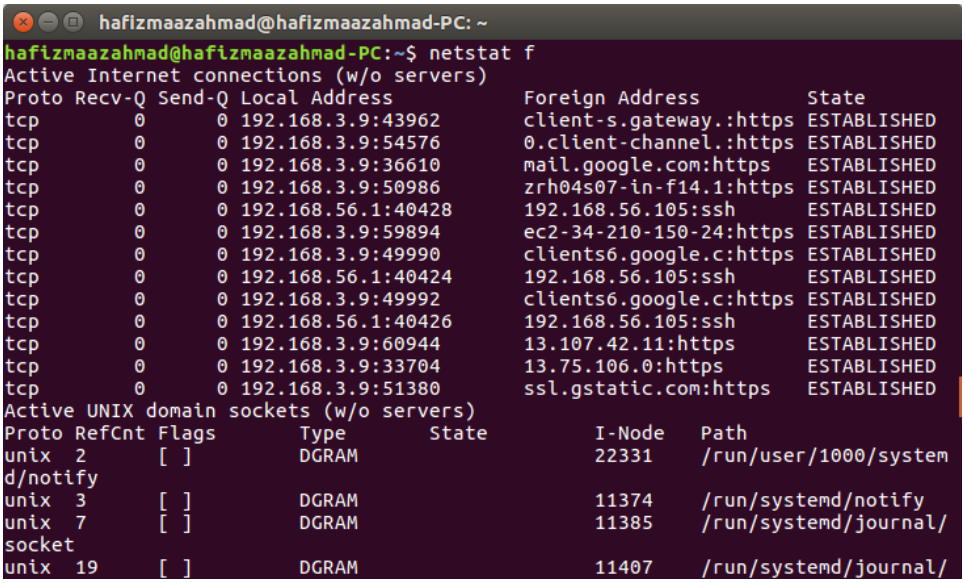


(-ltpe) Usernames and processes associated with connections.



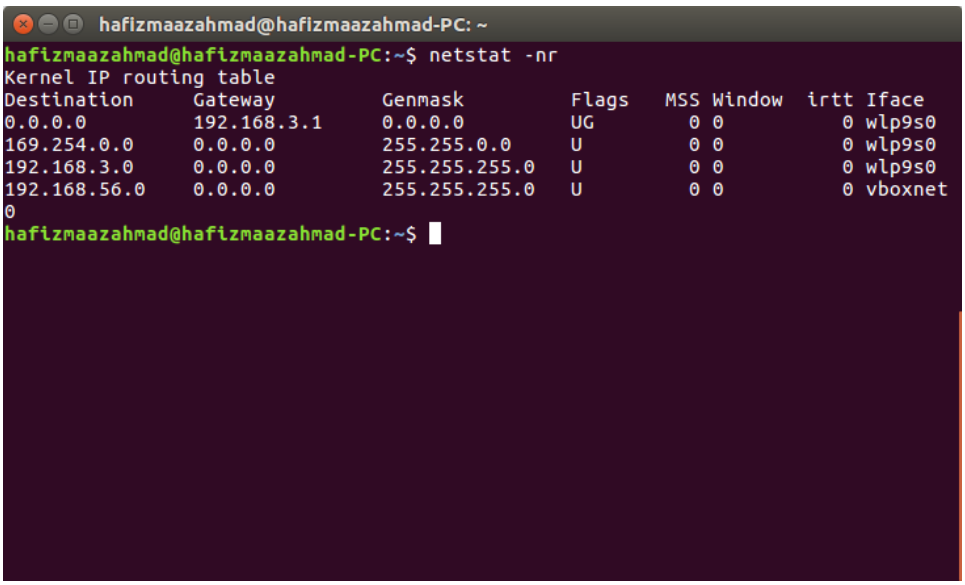
3- Switch -f

Displays FQDNs associated with foreign IPs (when possible).



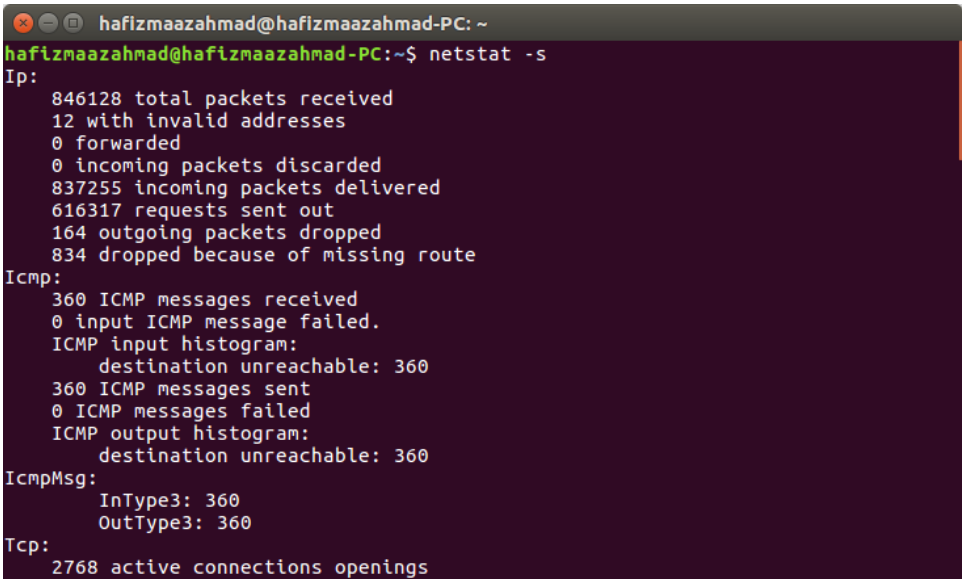
4- Switch -nr

Displays Kernel routing table of host machine.



5- Switch -s

Displays all network statistics.



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