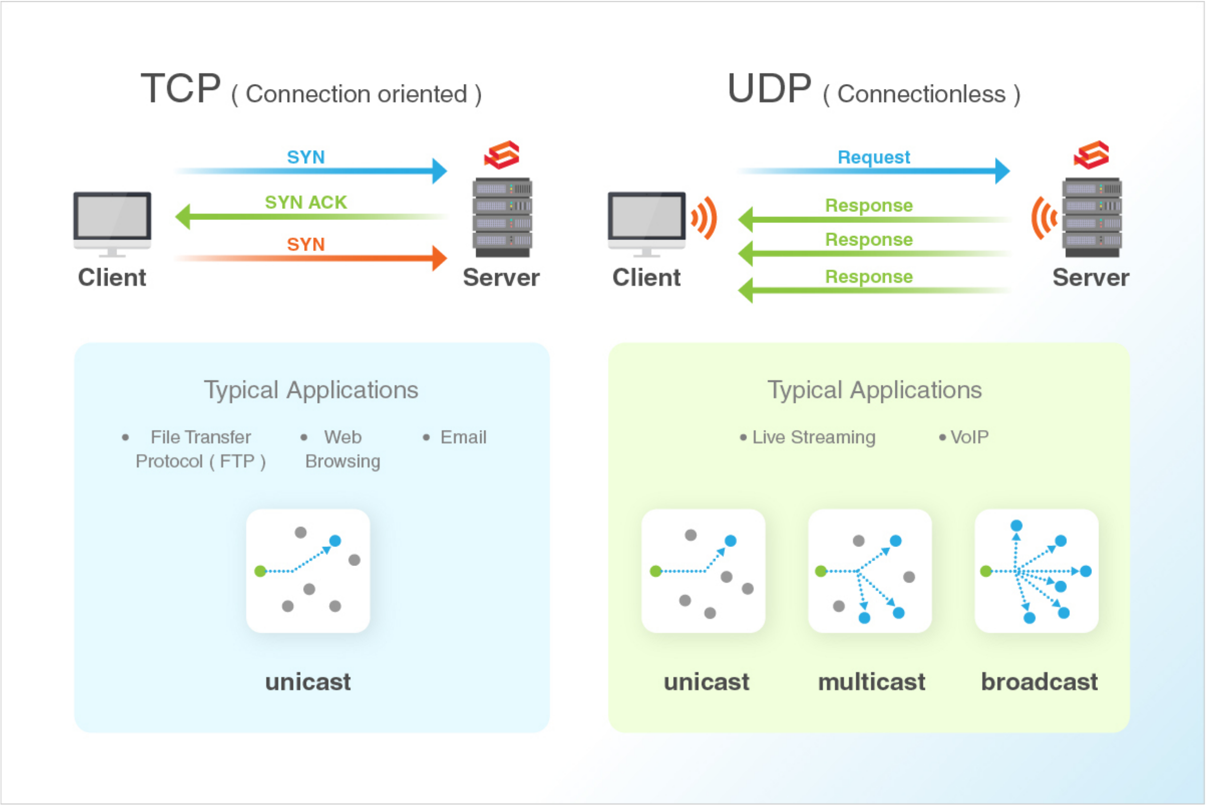
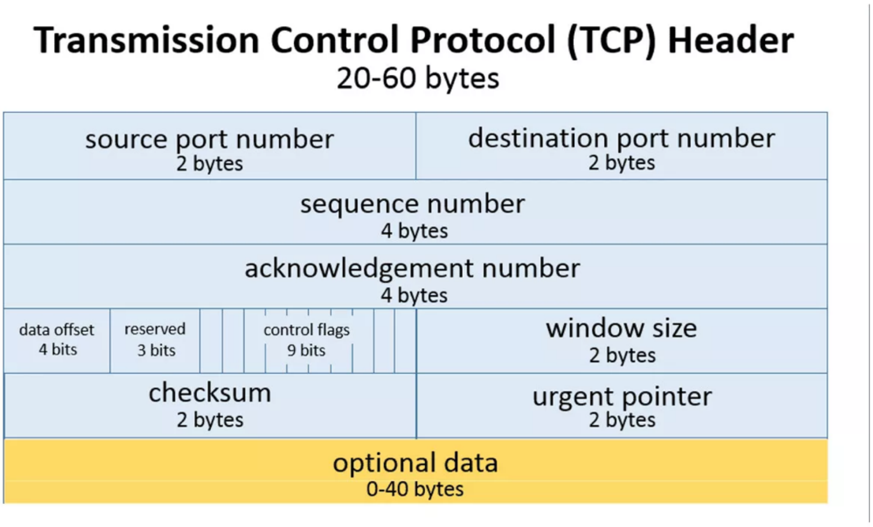
IT 307- Exploring the Networks
Handout 1

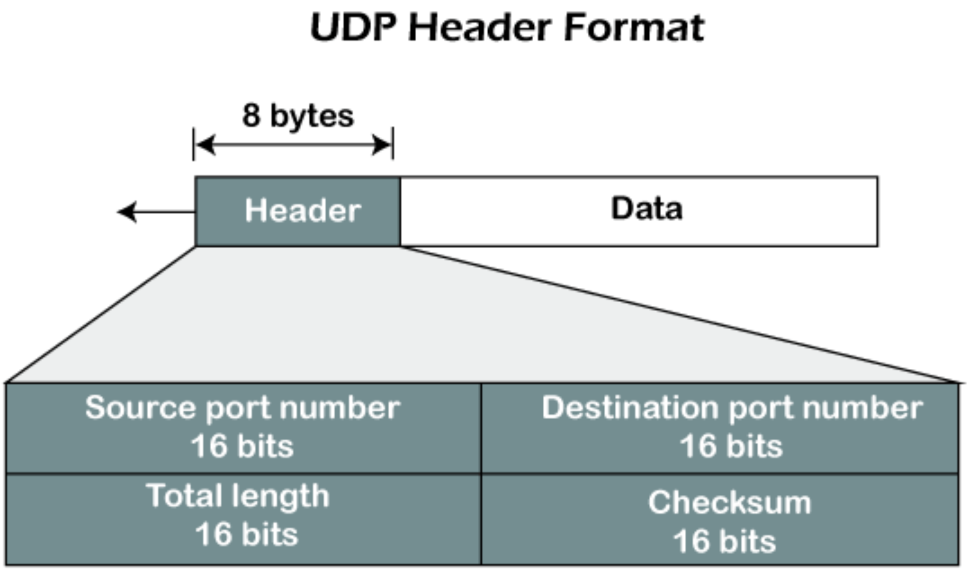
Observing TCP and UDP using Netstat
Explain common netstat command parameters and outputs.





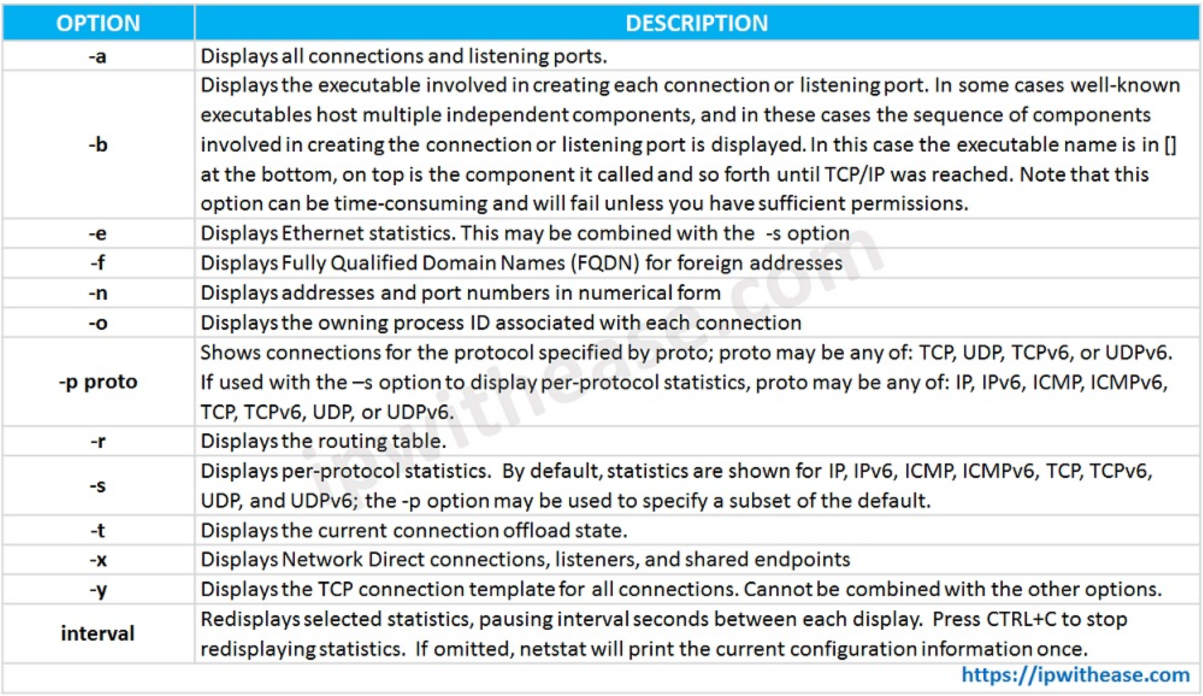
Transmission Control Protocol (TCP) Header
20-60 bytes

source port number 2 bytes	destination port number 2 bytes
sequence number 4 bytes	
acknowledgement number 4 bytes	
data offset 4 bits · reserved 3 bits · control flags 9 bits	window size 2 bytes
checksum 2 bytes	urgent pointer 2 bytes
optional data 0-40 bytes	



Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,

NETSTAT command table



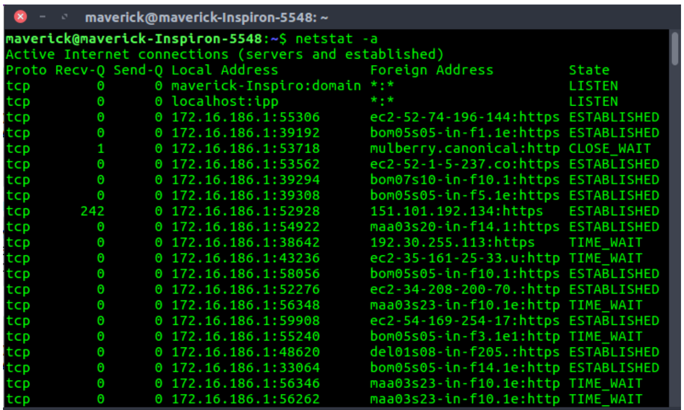
OPTION	DESCRIPTION
-a	Displays all connections and listening ports.
-b	Displays the executable involved in creating each connection or listening port. In some cases well-known executables host multiple independent components, and in these cases the sequence of components involved in creating the connection or listening port is displayed. In this case the executable name is in [] at the bottom, on top is the component it called and so forth until TCP/IP was reached. Note that this option can be time-consuming and will fail unless you have sufficient permissions.
-e	Displays Ethernet statistics. This may be combined with the -s option
-f	Displays Fully Qualified Domain Names (FQDN) for foreign addresses
-n	Displays addresses and port numbers in numerical form
-o	Displays the owning process ID associated with each connection
-p proto	Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the –s option to display per-protocol statistics, proto may be any of: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
-r	Displays the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6; the -p option may be used to specify a subset of the default.
-t	Displays the current connection offload state.
-x	Displays Network Direct connections, listeners, and shared endpoints
-y	Displays the TCP connection template for all connections. Cannot be combined with the other options.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, netstat will print the current configuration information once.

https://ipwithease.com

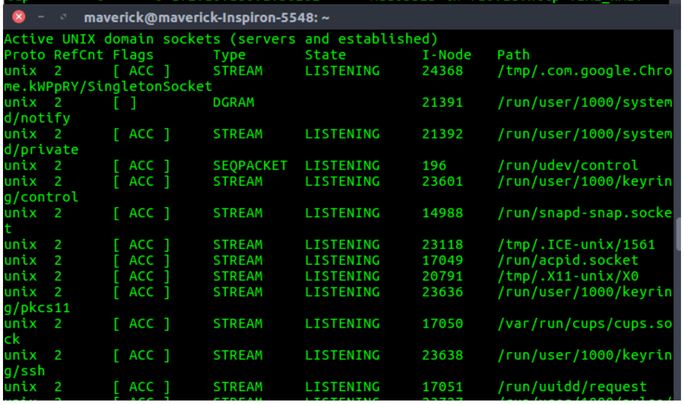
Examples of some practical netstat command :

1. **-a -all** : Show both listening and non-listening sockets. With the –interfaces option, show interfaces that are not up

2. **netstat -a | more :** To show both listening and non-listening sockets.

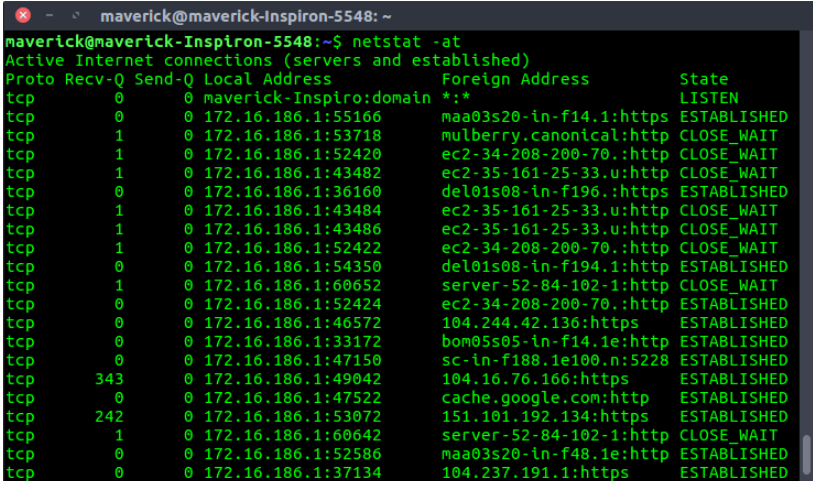


```
maverick@maverick-Inspiron-5548: ~
maverick@maverick-Inspiron-5548:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 maverick-Inspiro:domain *:*                     LISTEN
tcp        0      0 localhost:ipp           *:*                     LISTEN
tcp        0      0 172.16.186.1:55306      ec2-52-74-196-144:https ESTABLISHED
tcp        0      0 172.16.186.1:39192      bom05s05-in-f1.1e:https ESTABLISHED
tcp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
tcp        0      0 172.16.186.1:53562      ec2-52-1-5-237.co:https ESTABLISHED
tcp        0      0 172.16.186.1:39294      bom07s10-in-f10.1:https ESTABLISHED
tcp        0      0 172.16.186.1:39308      bom05s05-in-f5.1e:https ESTABLISHED
tcp      242      0 172.16.186.1:52928      151.101.192.134:https   ESTABLISHED
tcp        0      0 172.16.186.1:54922      maa03s20-in-f14.1:https ESTABLISHED
tcp        0      0 172.16.186.1:38642      192.30.255.113:https    TIME_WAIT
tcp        0      0 172.16.186.1:43236      ec2-35-161-25-33.u:http TIME_WAIT
tcp        0      0 172.16.186.1:58056      bom05s05-in-f10.1:https ESTABLISHED
tcp        0      0 172.16.186.1:52276      ec2-34-208-200-70.:http ESTABLISHED
tcp        0      0 172.16.186.1:56348      maa03s23-in-f10.1e:http TIME_WAIT
tcp        0      0 172.16.186.1:59908      ec2-54-169-254-17:https ESTABLISHED
tcp        0      0 172.16.186.1:55240      bom05s05-in-f3.1e1:http TIME_WAIT
tcp        0      0 172.16.186.1:48620      del01s08-in-f205.:https ESTABLISHED
tcp        0      0 172.16.186.1:33064      bom05s05-in-f14.1e:http ESTABLISHED
tcp        0      0 172.16.186.1:56346      maa03s23-in-f10.1e:http TIME_WAIT
tcp        0      0 172.16.186.1:56262      maa03s23-in-f10.1e:http TIME_WAIT
```



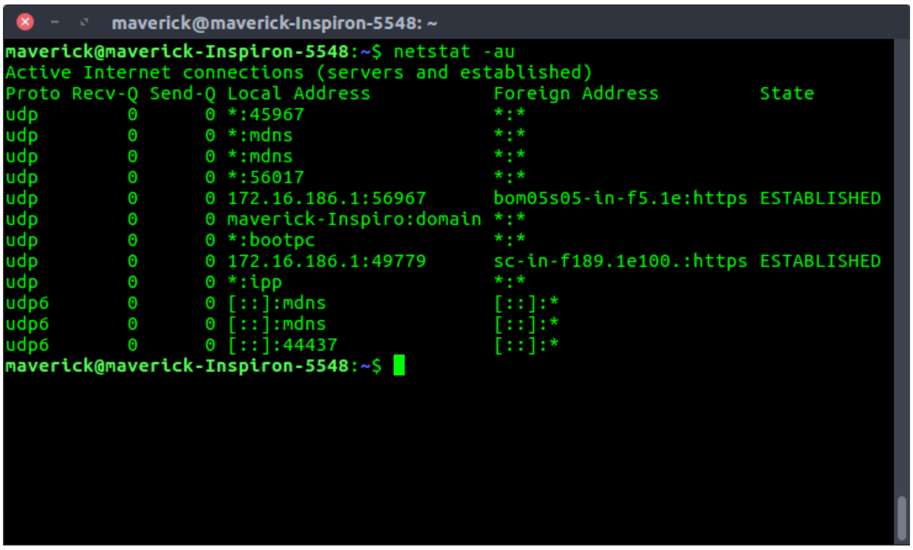
```
maverick@maverick-Inspiron-5548: ~
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     24368    /tmp/.com.google.Chro
me.kWPpRY/SingletonSocket
unix  2      [ ]         DGRAM                    21391    /run/user/1000/system
d/notify
unix  2      [ ACC ]     STREAM     LISTENING     21392    /run/user/1000/system
d/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     196      /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     23601    /run/user/1000/keyrin
g/control
unix  2      [ ACC ]     STREAM     LISTENING     14988    /run/snapd-snap.socke
t
unix  2      [ ACC ]     STREAM     LISTENING     23118    /tmp/.ICE-unix/1561
unix  2      [ ACC ]     STREAM     LISTENING     17049    /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     20791    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     23636    /run/user/1000/keyrin
g/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     17050    /var/run/cups/cups.so
ck
unix  2      [ ACC ]     STREAM     LISTENING     23638    /run/user/1000/keyrin
g/ssh
unix  2      [ ACC ]     STREAM     LISTENING     17051    /run/uuidd/request
```

3. **List all tcp ports.**
   # netstat -at : To list all tcp ports.



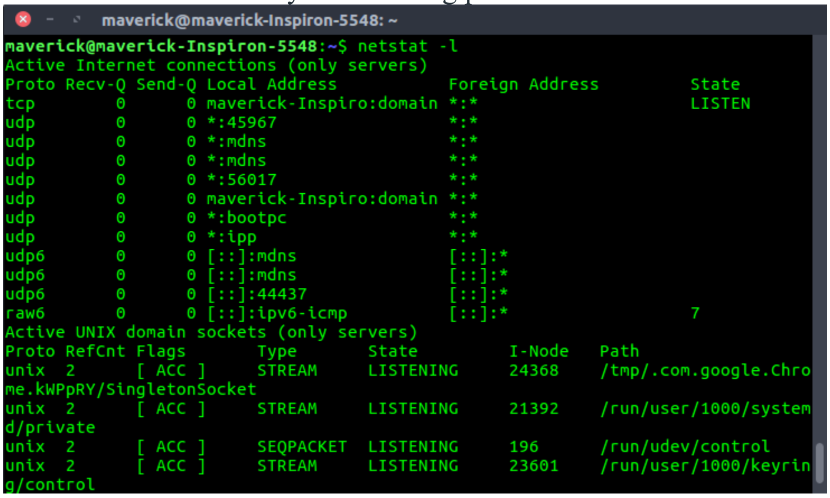
```
maverick@maverick-Inspiron-5548: ~
maverick@maverick-Inspiron-5548:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 maverick-Inspiro:domain *:*                     LISTEN
tcp        0      0 172.16.186.1:55166      maa03s20-in-f14.1:https ESTABLISHED
tcp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
tcp        1      0 172.16.186.1:52420      ec2-34-208-200-70.:http CLOSE_WAIT
tcp        1      0 172.16.186.1:43482      ec2-35-161-25-33.u:http CLOSE_WAIT
tcp        0      0 172.16.186.1:36160      del01s08-in-f196.:https ESTABLISHED
tcp        1      0 172.16.186.1:43484      ec2-35-161-25-33.u:http CLOSE_WAIT
tcp        1      0 172.16.186.1:43486      ec2-35-161-25-33.u:http CLOSE_WAIT
tcp        1      0 172.16.186.1:52422      ec2-34-208-200-70.:http CLOSE_WAIT
tcp        0      0 172.16.186.1:54350      del01s08-in-f194.1:http ESTABLISHED
tcp        1      0 172.16.186.1:60652      server-52-84-102-1:http CLOSE_WAIT
tcp        0      0 172.16.186.1:52424      ec2-34-208-200-70.:http ESTABLISHED
tcp        0      0 172.16.186.1:46572      104.244.42.136:https    ESTABLISHED
tcp        0      0 172.16.186.1:33172      bom05s05-in-f14.1e:http ESTABLISHED
tcp        0      0 172.16.186.1:47150      sc-in-f188.1e100.n:5228 ESTABLISHED
tcp      343      0 172.16.186.1:49042      104.16.76.166:https     ESTABLISHED
tcp        0      0 172.16.186.1:47522      cache.google.com:http   ESTABLISHED
tcp      242      0 172.16.186.1:53072      151.101.192.134:https   ESTABLISHED
tcp        1      0 172.16.186.1:60642      server-52-84-102-1:http CLOSE_WAIT
tcp        0      0 172.16.186.1:52586      maa03s20-in-f48.1e:http ESTABLISHED
tcp        0      0 172.16.186.1:37134      104.237.191.1:https     ESTABLISHED
```

4. **List all udp ports.**
   # netstat -au : To list all udp ports.



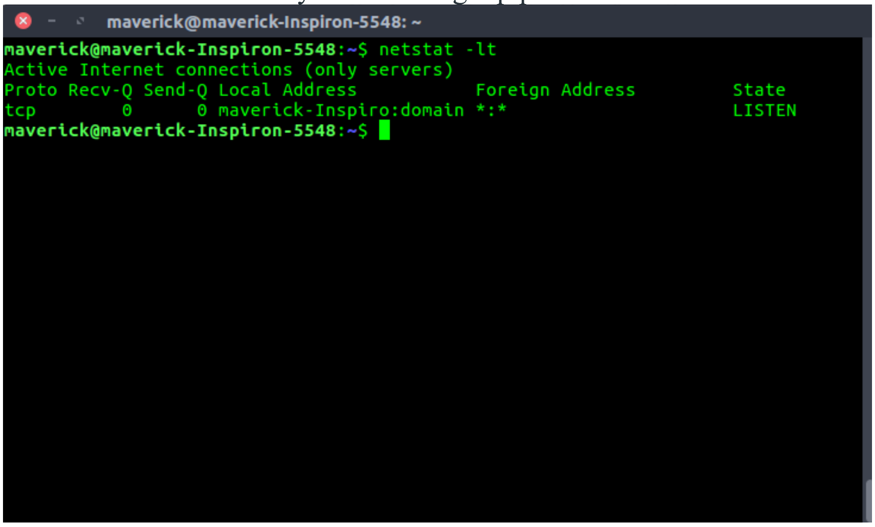
```
maverick@maverick-Inspiron-5548:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:45967                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:56017                 *:*
udp        0      0 172.16.186.1:56967      bom05s05-in-f5.1e:https ESTABLISHED
udp        0      0 maverick-Inspiro:domain *:*
udp        0      0 *:bootpc                *:*
udp        0      0 172.16.186.1:49779      sc-in-f189.1e100.:https ESTABLISHED
udp        0      0 *:ipp                   *:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:44437              [::]:*
maverick@maverick-Inspiron-5548:~$
```

5. **List only listening ports.**
   # **netstat -l :** To list only the listening ports.



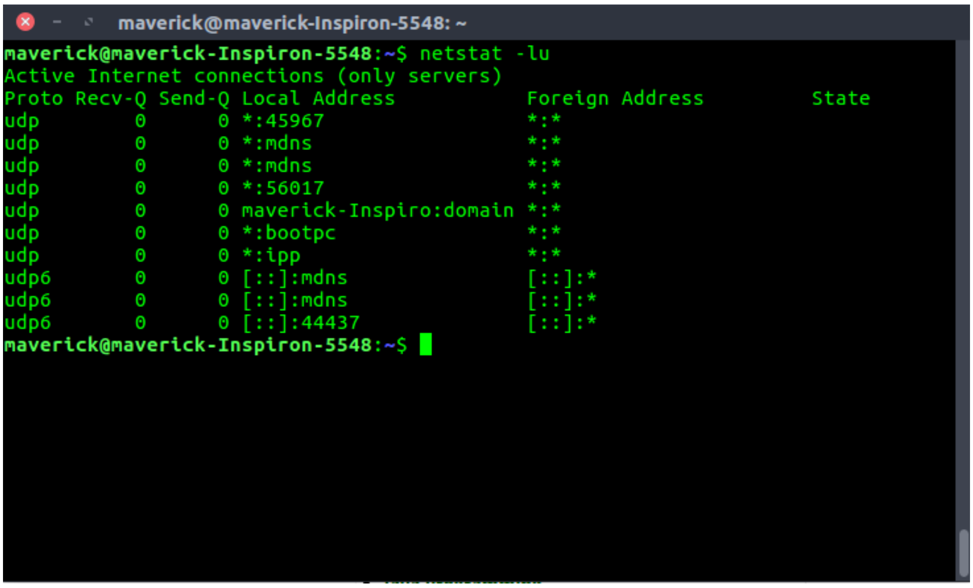
```
maverick@maverick-Inspiron-5548:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 maverick-Inspiro:domain *:*                     LISTEN
udp        0      0 *:45967                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:56017                 *:*
udp        0      0 maverick-Inspiro:domain *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:ipp                   *:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:44437              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     24368    /tmp/.com.google.Chro
me.kWPpRY/SingletonSocket
unix  2      [ ACC ]     STREAM     LISTENING     21392    /run/user/1000/system
d/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     196      /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     23601    /run/user/1000/keyrin
g/control
```

6. **List only listening TCP ports.**
   # **netstat -lt :** To list only the listening tcp ports.



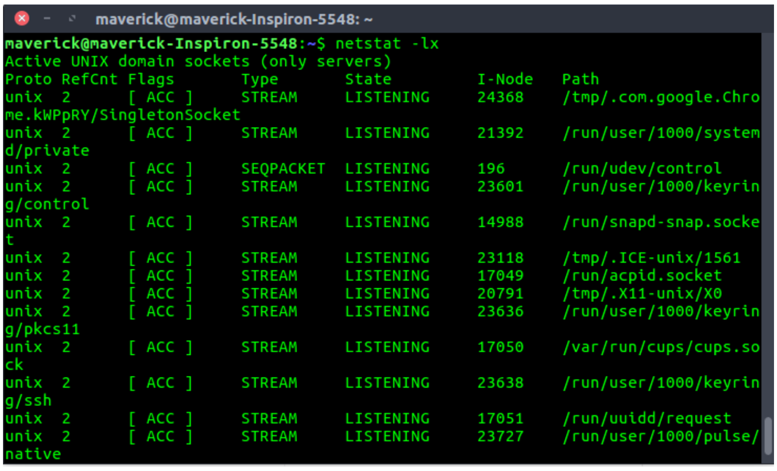
```
maverick@maverick-Inspiron-5548:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 maverick-Inspiro:domain *:*                     LISTEN
maverick@maverick-Inspiron-5548:~$
```

7. **List only listening UDP ports.**
   # **netstat -lu :** To list only the listening udp ports.



```
maverick@maverick-Inspiron-5548:~$ netstat -lu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 *:45967                 *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:mdns                  *:*
udp        0      0 *:56017                 *:*
udp        0      0 maverick-Inspiro:domain *:*
udp        0      0 *:bootpc                *:*
udp        0      0 *:ipp                   *:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:44437              [::]:*
maverick@maverick-Inspiron-5548:~$ 
```

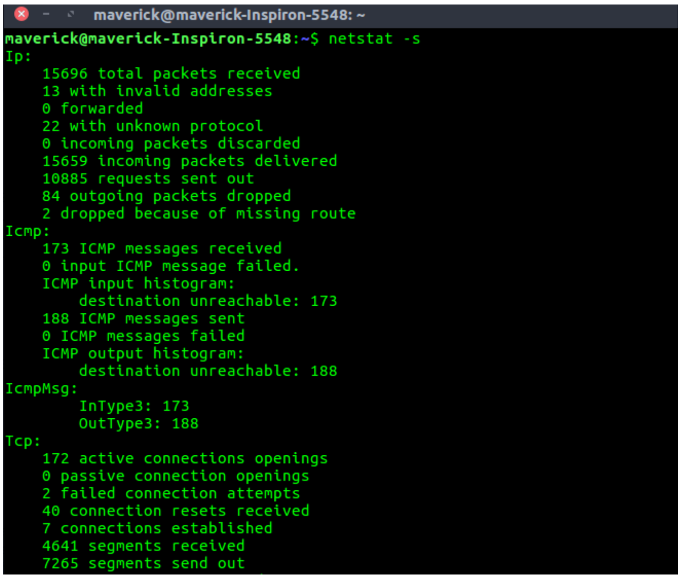
8. **List only the listening UNIX ports**
   # netstat -lx : To list only the listening UNIX ports.



```
maverick@maverick-Inspiron-5548:~$ netstat -lx
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     24368    /tmp/.com.google.Chro
me.kWPpRY/SingletonSocket
unix  2      [ ACC ]     STREAM     LISTENING     21392    /run/user/1000/system
d/private
unix  2      [ ACC ]     SEQPACKET  LISTENING     196      /run/udev/control
unix  2      [ ACC ]     STREAM     LISTENING     23601    /run/user/1000/keyrin
g/control
unix  2      [ ACC ]     STREAM     LISTENING     14988    /run/snapd-snap.socke
t
unix  2      [ ACC ]     STREAM     LISTENING     23118    /tmp/.ICE-unix/1561
unix  2      [ ACC ]     STREAM     LISTENING     17049    /run/acpid.socket
unix  2      [ ACC ]     STREAM     LISTENING     20791    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     23636    /run/user/1000/keyrin
g/pkcs11
unix  2      [ ACC ]     STREAM     LISTENING     17050    /var/run/cups/cups.so
ck
unix  2      [ ACC ]     STREAM     LISTENING     23638    /run/user/1000/keyrin
g/ssh
unix  2      [ ACC ]     STREAM     LISTENING     17051    /run/uuidd/request
unix  2      [ ACC ]     STREAM     LISTENING     23727    /run/user/1000/pulse/
native
```

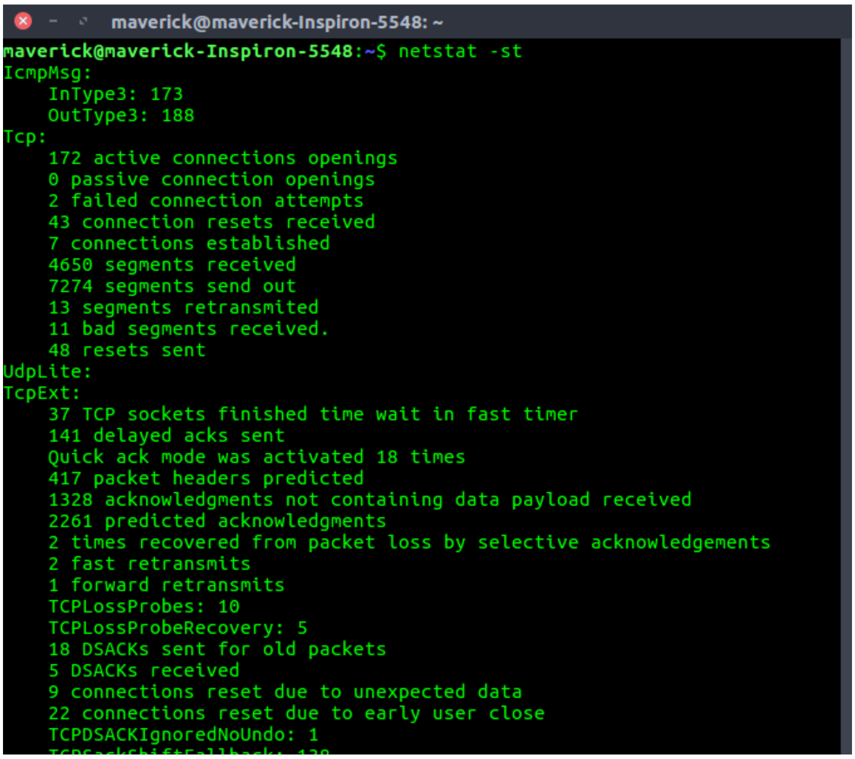
9. **List the statistics for all ports.**

# netstat -s : To list the statistics for all ports.



```
maverick@maverick-Inspiron-5548:~$ netstat -s
Ip:
    15696 total packets received
    13 with invalid addresses
    0 forwarded
    22 with unknown protocol
    0 incoming packets discarded
    15659 incoming packets delivered
    10885 requests sent out
    84 outgoing packets dropped
    2 dropped because of missing route
Icmp:
    173 ICMP messages received
    0 input ICMP message failed.
    ICMP input histogram:
        destination unreachable: 173
    188 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 188
IcmpMsg:
        InType3: 173
        OutType3: 188
Tcp:
    172 active connections openings
    0 passive connection openings
    2 failed connection attempts
    40 connection resets received
    7 connections established
    4641 segments received
    7265 segments send out
```

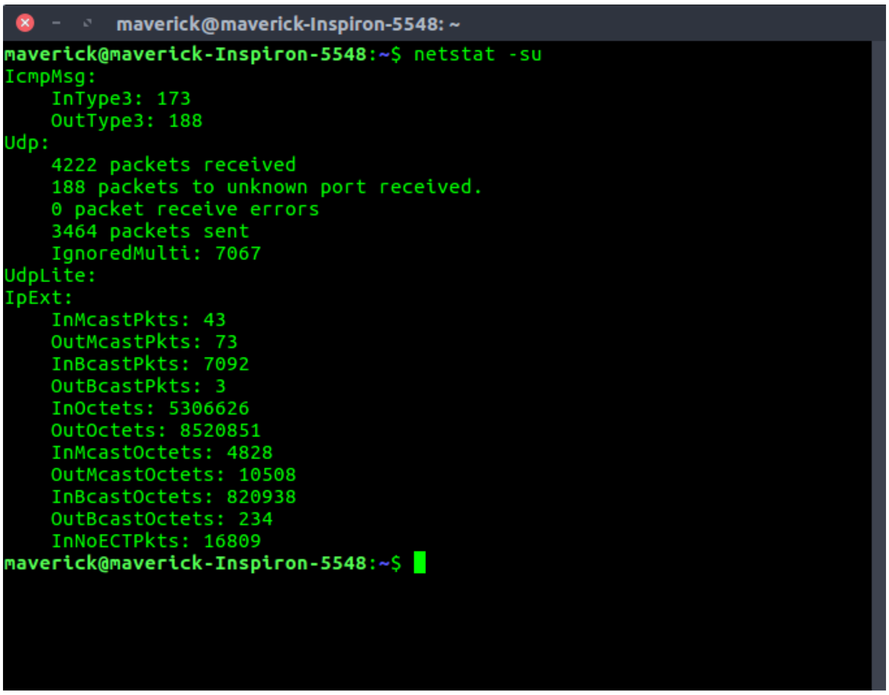
10. **List the statistics for TCP (or) UDP ports.**
# netstat -st(TCP) : To list the statistics for TCP ports.



maverick@maverick-Inspiron-5548: ~

```
maverick@maverick-Inspiron-5548:~$ netstat -st
IcmpMsg:
    InType3: 173
    OutType3: 188
Tcp:
    172 active connections openings
    0 passive connection openings
    2 failed connection attempts
    43 connection resets received
    7 connections established
    4650 segments received
    7274 segments send out
    13 segments retransmited
    11 bad segments received.
    48 resets sent
UdpLite:
TcpExt:
    37 TCP sockets finished time wait in fast timer
    141 delayed acks sent
    Quick ack mode was activated 18 times
    417 packet headers predicted
    1328 acknowledgments not containing data payload received
    2261 predicted acknowledgments
    2 times recovered from packet loss by selective acknowledgements
    2 fast retransmits
    1 forward retransmits
    TCPLossProbes: 10
    TCPLossProbeRecovery: 5
    18 DSACKs sent for old packets
    5 DSACKs received
    9 connections reset due to unexpected data
    22 connections reset due to early user close
    TCPDSACKIgnoredNoUndo: 1
    TCPSackShiftFallback: 138
```

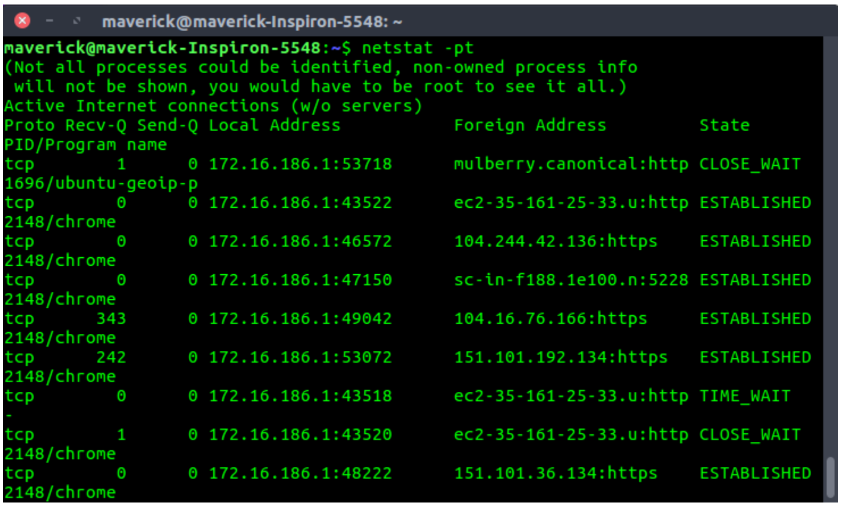
# netstat -su(UDP) : List the statistics for UDP ports.



maverick@maverick-Inspiron-5548: ~

```
maverick@maverick-Inspiron-5548:~$ netstat -su
IcmpMsg:
    InType3: 173
    OutType3: 188
Udp:
    4222 packets received
    188 packets to unknown port received.
    0 packet receive errors
    3464 packets sent
    IgnoredMulti: 7067
UdpLite:
IpExt:
    InMcastPkts: 43
    OutMcastPkts: 73
    InBcastPkts: 7092
    OutBcastPkts: 3
    InOctets: 5306626
    OutOctets: 8520851
    InMcastOctets: 4828
    OutMcastOctets: 10508
    InBcastOctets: 820938
    OutBcastOctets: 234
    InNoECTPkts: 16809
maverick@maverick-Inspiron-5548:~$ 
```

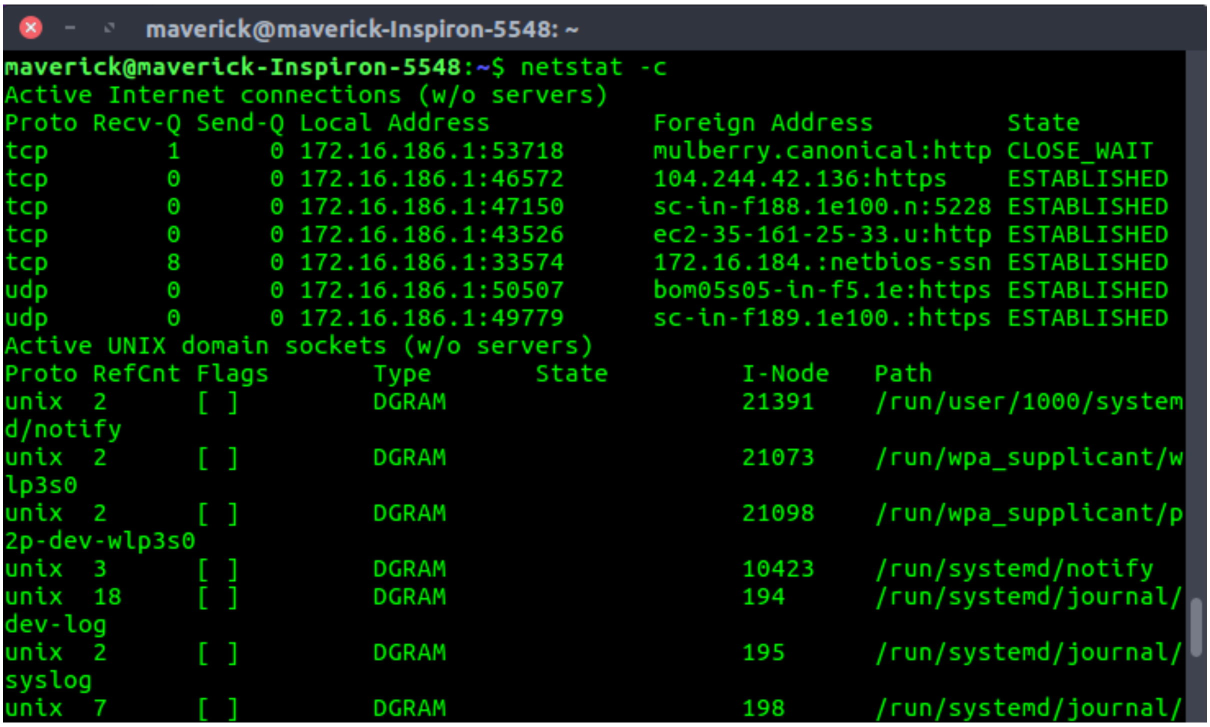
11. **Display PID and program names in the output.**
# netstat -pt : To display the PID and program names.



```
maverick@maverick-Inspiron-5548:~$ netstat -pt
(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 (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
1696/ubuntu-geoip-p
tcp        0      0 172.16.186.1:43522      ec2-35-161-25-33.u:http ESTABLISHED
2148/chrome
tcp        0      0 172.16.186.1:46572      104.244.42.136:https    ESTABLISHED
2148/chrome
tcp        0      0 172.16.186.1:47150      sc-in-f188.1e100.n:5228 ESTABLISHED
2148/chrome
tcp      343      0 172.16.186.1:49042      104.16.76.166:https     ESTABLISHED
2148/chrome
tcp      242      0 172.16.186.1:53072      151.101.192.134:https   ESTABLISHED
2148/chrome
tcp        0      0 172.16.186.1:43518      ec2-35-161-25-33.u:http TIME_WAIT
-
tcp        1      0 172.16.186.1:43520      ec2-35-161-25-33.u:http CLOSE_WAIT
2148/chrome
tcp        0      0 172.16.186.1:48222      151.101.36.134:https    ESTABLISHED
2148/chrome
```

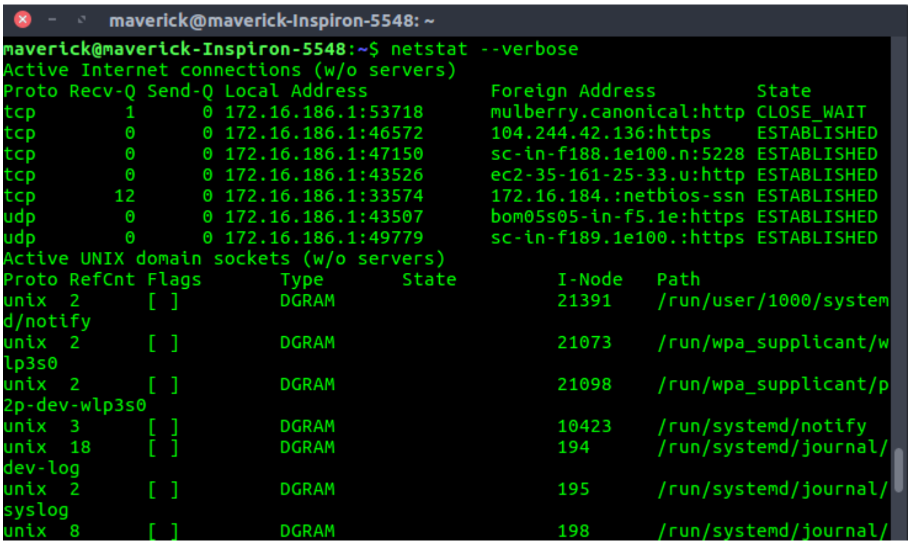
12. **Print the netstat information continuously.**
    netstat will print information continuously every few seconds.

    # netstat -c : To print the netstat information continuously.



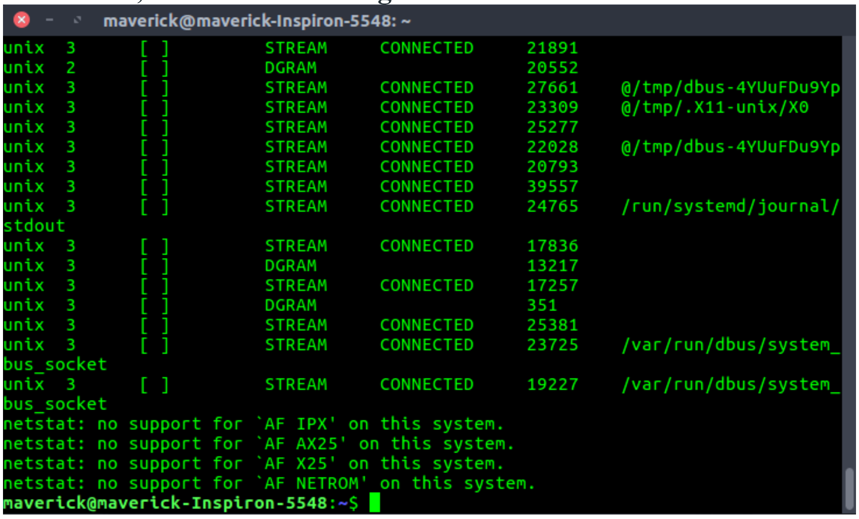
```
maverick@maverick-Inspiron-5548:~$ netstat -c
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
tcp        0      0 172.16.186.1:46572      104.244.42.136:https    ESTABLISHED
tcp        0      0 172.16.186.1:47150      sc-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 172.16.186.1:43526      ec2-35-161-25-33.u:http ESTABLISHED
tcp        8      0 172.16.186.1:33574      172.16.184.:netbios-ssn ESTABLISHED
udp        0      0 172.16.186.1:50507      bom05s05-in-f5.1e:https ESTABLISHED
udp        0      0 172.16.186.1:49779      sc-in-f189.1e100.:https ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    21391    /run/user/1000/system
d/notify
unix  2      [ ]         DGRAM                    21073    /run/wpa_supplicant/w
lp3s0
unix  2      [ ]         DGRAM                    21098    /run/wpa_supplicant/p
2p-dev-wlp3s0
unix  3      [ ]         DGRAM                    10423    /run/systemd/notify
unix  18     [ ]         DGRAM                    194      /run/systemd/journal/
dev-log
unix  2      [ ]         DGRAM                    195      /run/systemd/journal/
syslog
unix  7      [ ]         DGRAM                    198      /run/systemd/journal/
```

13. **The non-supportive address families in the system.**
    # netstat --verbose : To get the non-supportive address families in the system.



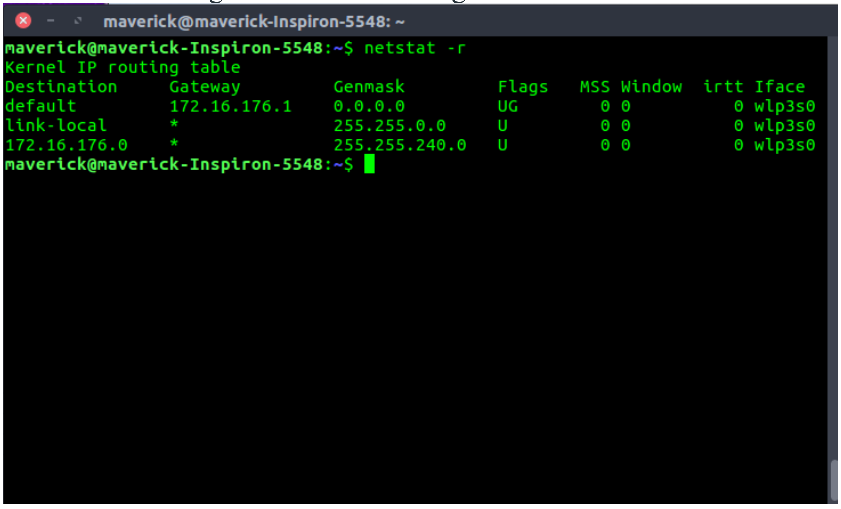
```
maverick@maverick-Inspiron-5548:~$ netstat --verbose
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        1      0 172.16.186.1:53718      mulberry.canonical:http CLOSE_WAIT
tcp        0      0 172.16.186.1:46572      104.244.42.136:https    ESTABLISHED
tcp        0      0 172.16.186.1:47150      sc-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 172.16.186.1:43526      ec2-35-161-25-33.u:http ESTABLISHED
tcp       12      0 172.16.186.1:33574      172.16.184.:netbios-ssn ESTABLISHED
udp        0      0 172.16.186.1:43507      bom05s05-in-f5.1e:https ESTABLISHED
udp        0      0 172.16.186.1:49779      sc-in-f189.1e100.:https ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    21391    /run/user/1000/system
d/notify
unix  2      [ ]         DGRAM                    21073    /run/wpa_supplicant/w
lp3s0
unix  2      [ ]         DGRAM                    21098    /run/wpa_supplicant/p
2p-dev-wlp3s0
unix  3      [ ]         DGRAM                    10423    /run/systemd/notify
unix  18     [ ]         DGRAM                    194      /run/systemd/journal/
dev-log
unix  2      [ ]         DGRAM                    195      /run/systemd/journal/
syslog
unix  8      [ ]         DGRAM                    198      /run/systemd/journal/
```

At the end, we have something like this :



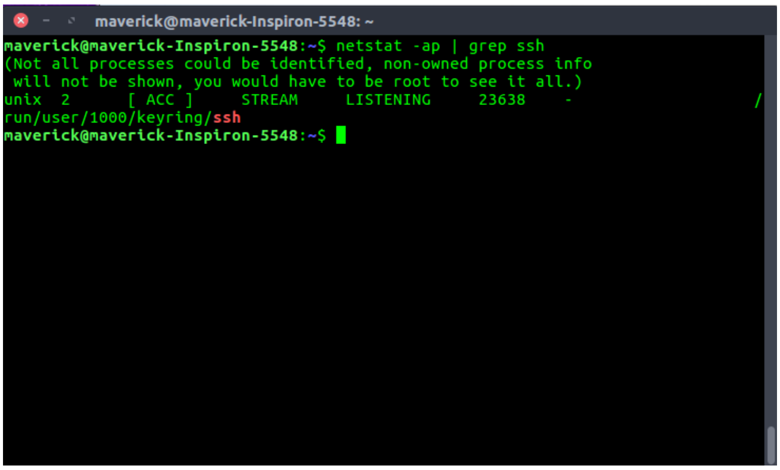
```
unix  3      [ ]         STREAM     CONNECTED     21891
unix  2      [ ]         DGRAM                    20552
unix  3      [ ]         STREAM     CONNECTED     27661    @/tmp/dbus-4YUuFDu9Yp
unix  3      [ ]         STREAM     CONNECTED     23309    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     25277
unix  3      [ ]         STREAM     CONNECTED     22028    @/tmp/dbus-4YUuFDu9Yp
unix  3      [ ]         STREAM     CONNECTED     20793
unix  3      [ ]         STREAM     CONNECTED     39557
unix  3      [ ]         STREAM     CONNECTED     24765    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     17836
unix  3      [ ]         DGRAM                    13217
unix  3      [ ]         STREAM     CONNECTED     17257
unix  3      [ ]         DGRAM                    351
unix  3      [ ]         STREAM     CONNECTED     25381
unix  3      [ ]         STREAM     CONNECTED     23725    /var/run/dbus/system_
bus_socket
unix  3      [ ]         STREAM     CONNECTED     19227    /var/run/dbus/system_
bus_socket
netstat: no support for `AF IPX' on this system.
netstat: no support for `AF AX25' on this system.
netstat: no support for `AF X25' on this system.
netstat: no support for `AF NETROM' on this system.
maverick@maverick-Inspiron-5548:~$ 
```

14. **The kernel routing information.**
    # netstat -r : To get the kernel routing information.



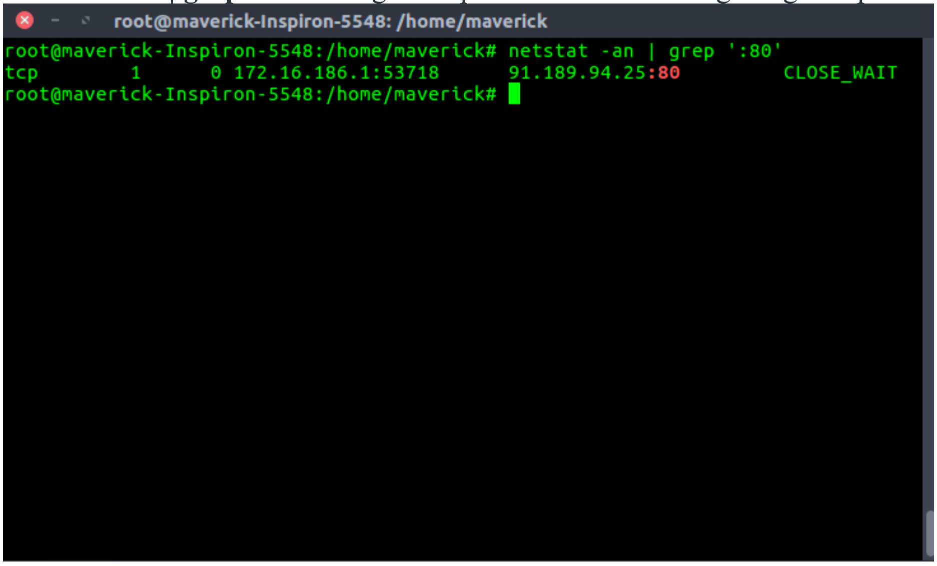
```
maverick@maverick-Inspiron-5548:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         172.16.176.1    0.0.0.0         UG        0 0          0 wlp3s0
link-local      *               255.255.0.0     U         0 0          0 wlp3s0
172.16.176.0    *               255.255.240.0   U         0 0          0 wlp3s0
maverick@maverick-Inspiron-5548:~$ 
```

15. **The port on which a program is running.**
    # netstat -ap | grep ssh : To get the port on which a program is running.



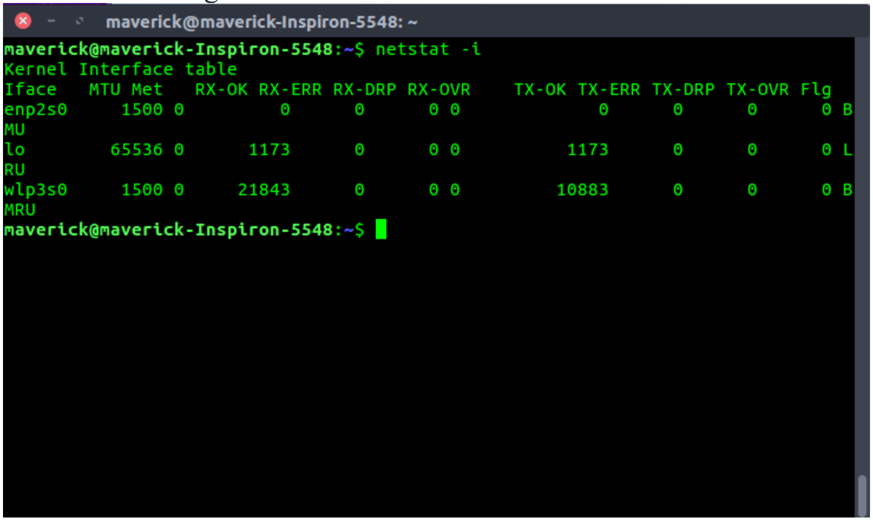
```
maverick@maverick-Inspiron-5548:~$ netstat -ap | grep ssh
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
unix  2      [ ACC ]     STREAM     LISTENING     23638    -                   /
run/user/1000/keyring/ssh
maverick@maverick-Inspiron-5548:~$ 
```

16. **Which process is using a particular port:**
    # netstat -an | grep ':80' : To get the process which is using the given port.



```
root@maverick-Inspiron-5548:/home/maverick# netstat -an | grep ':80'
tcp        1      0 172.16.186.1:53718      91.189.94.25:80         CLOSE_WAIT
root@maverick-Inspiron-5548:/home/maverick# 
```

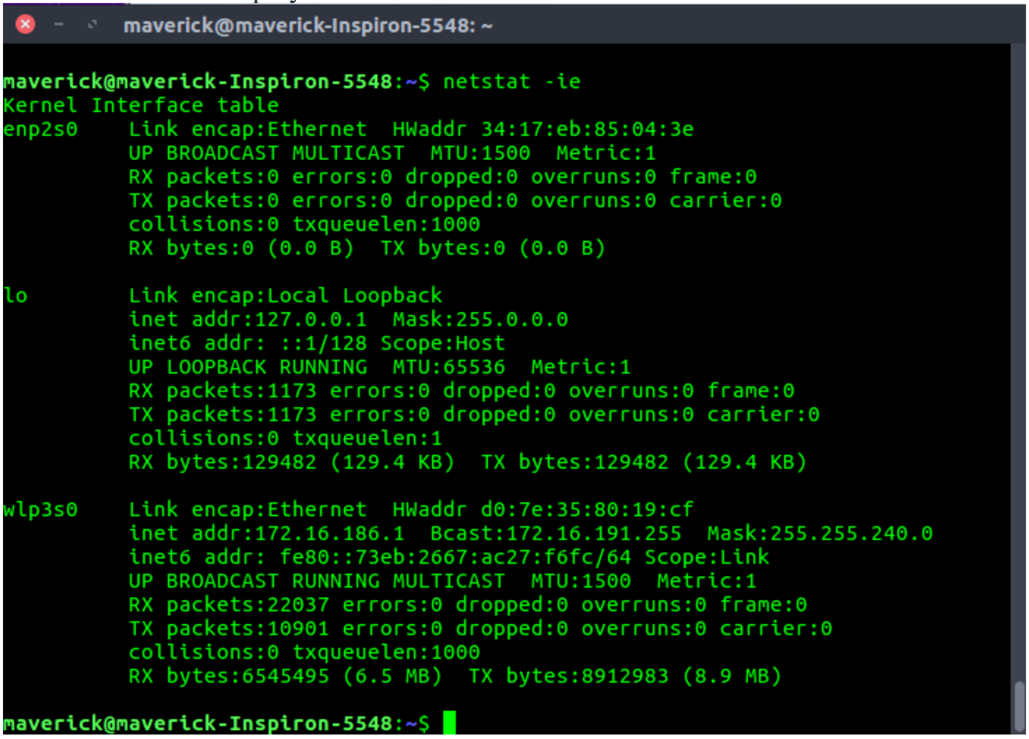
17. **List of network interfaces.**
    # netstat -i : To get the list of network interfaces.



```
maverick@maverick-Inspiron-5548:~$ netstat -i
Kernel Interface table
Iface   MTU Met   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp2s0     1500 0         0      0      0 0             0      0      0      0 B
MU
lo        65536 0      1173      0      0 0          1173      0      0      0 L
RU
wlp3s0     1500 0     21843      0      0 0         10883      0      0      0 B
MRU
maverick@maverick-Inspiron-5548:~$ 
```

Display extended information on the interfaces (similar to ifconfig) using netstat -ie:

# **netstat -ie :** To display extended information on the interfaces



```
maverick@maverick-Inspiron-5548:~$ netstat -ie
Kernel Interface table
enp2s0    Link encap:Ethernet  HWaddr 34:17:eb:85:04:3e
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:129482 (129.4 KB)  TX bytes:129482 (129.4 KB)

wlp3s0    Link encap:Ethernet  HWaddr d0:7e:35:80:19:cf
          inet addr:172.16.186.1  Bcast:172.16.191.255  Mask:255.255.240.0
          inet6 addr: fe80::73eb:2667:ac27:f6fc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22037 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10901 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6545495 (6.5 MB)  TX bytes:8912983 (8.9 MB)

maverick@maverick-Inspiron-5548:~$
```

How to check if TCP / UDP port is open on Linux & Windows Cloud Servers

The following are the common port numbers:
Ports 0 to 1023 are Well-Known Ports
Ports 1024 to 49151 are Registered Ports (*Often registered by a software developer to designate a particular port for their application)
Ports 49152 to 65535 are Public Ports

20,21	FTP	TCP
22	SSH	TCP and UDP
23	Telnet	TCP
25	SMTP	TCP
50,51	IPSec	/
53	DNS	TCP and UDP
67,68	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
119	NNTP	TCP
123	NTP	TCP
135-139	NetBIOS	TCP and UDP
143	IMAP	TCP and UDP
161,162	SNMP	TCP and UDP
389	Lightweight Directory Access	TCP and UDP
443	HTTPS	TCP and UDP
465	SMTP over SSL	TCP
989	FTP Protocol (data) over TLS/SSL	TCP and UDP
990	FTP Protocol (data) over TLS/SSL	TCP and UDP

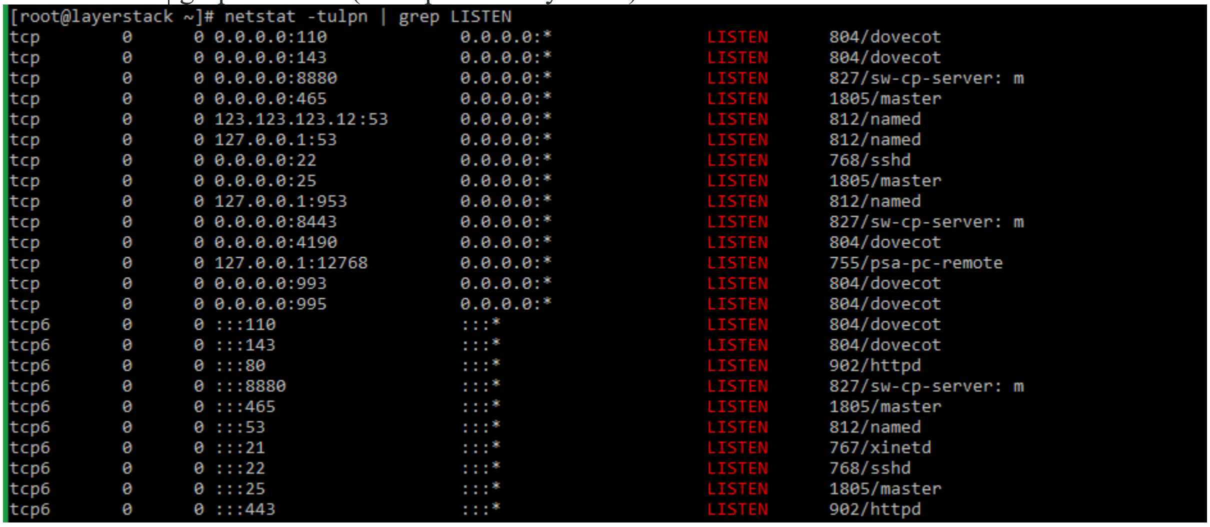
993	IMAP over SSL	TCP
995	POP3 over SSL	TCP
3389	Remote Desktop	TCP and UDP

Using netstat command

netstat (network statistics) is a command-line tool that can be used to monitor both incoming and outgoing network connections in a server.

The netstat command along with the grep command to check the listening services can be used in the below syntax

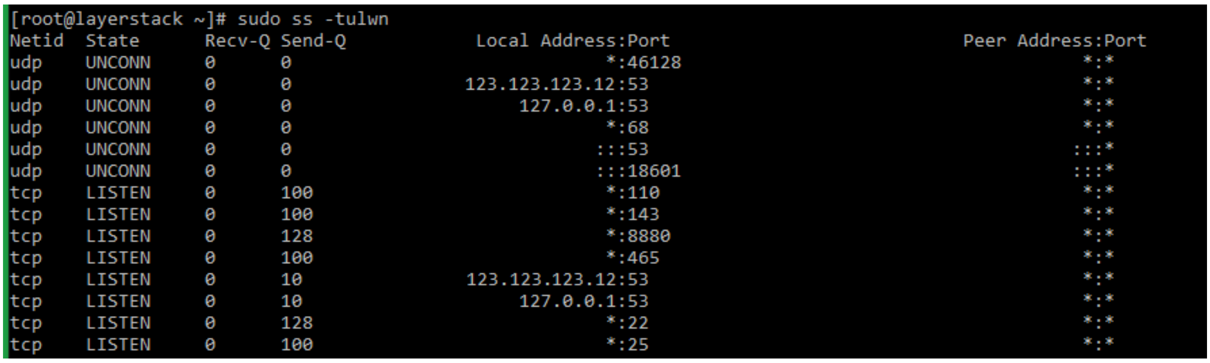
netstat -tulpn | grep LISTEN
# netstat -nat | grep LISTEN (for OpenBSD systems)



```
[root@layerstack ~]# netstat -tulpn | grep LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      804/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      804/dovecot
tcp        0      0 0.0.0.0:8880            0.0.0.0:*               LISTEN      827/sw-cp-server: m
tcp        0      0 0.0.0.0:465             0.0.0.0:*               LISTEN      1805/master
tcp        0      0 123.123.123.12:53       0.0.0.0:*               LISTEN      812/named
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN      812/named
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      768/sshd
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      1805/master
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN      812/named
tcp        0      0 0.0.0.0:8443            0.0.0.0:*               LISTEN      827/sw-cp-server: m
tcp        0      0 0.0.0.0:4190            0.0.0.0:*               LISTEN      804/dovecot
tcp        0      0 127.0.0.1:12768         0.0.0.0:*               LISTEN      755/psa-pc-remote
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN      804/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN      804/dovecot
tcp6       0      0 :::110                  :::*                    LISTEN      804/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      804/dovecot
tcp6       0      0 :::80                   :::*                    LISTEN      902/httpd
tcp6       0      0 :::8880                 :::*                    LISTEN      827/sw-cp-server: m
tcp6       0      0 :::465                  :::*                    LISTEN      1805/master
tcp6       0      0 :::53                   :::*                    LISTEN      812/named
tcp6       0      0 :::21                   :::*                    LISTEN      767/xinetd
tcp6       0      0 :::22                   :::*                    LISTEN      768/sshd
tcp6       0      0 :::25                   :::*                    LISTEN      1805/master
tcp6       0      0 :::443                  :::*                    LISTEN      902/httpd
```

netstat command has been deprecated in the latest versions of Linux distribution. The ss command has taken its place.

The syntax for using the ss command is as provided below:
# sudo ss -tulpn



```
[root@layerstack ~]# sudo ss -tulwn
Netid  State      Recv-Q Send-Q            Local Address:Port                          Peer Address:Port
udp    UNCONN     0      0                             *:46128                                    *:*
udp    UNCONN     0      0                123.123.123.12:53                                       *:*
udp    UNCONN     0      0                     127.0.0.1:53                                       *:*
udp    UNCONN     0      0                             *:68                                       *:*
udp    UNCONN     0      0                            :::53                                      :::*
udp    UNCONN     0      0                            :::18601                                   :::*
tcp    LISTEN     0      100                           *:110                                      *:*
tcp    LISTEN     0      100                           *:143                                      *:*
tcp    LISTEN     0      128                           *:8880                                     *:*
tcp    LISTEN     0      100                           *:465                                      *:*
tcp    LISTEN     0      10               123.123.123.12:53                                       *:*
tcp    LISTEN     0      10                    127.0.0.1:53                                       *:*
tcp    LISTEN     0      128                           *:22                                       *:*
tcp    LISTEN     0      100                           *:25                                       *:*
```

The switches for the ss command mean as follows:

t: Show only TCP sockets.
u: Show only UDP sockets.
l: Show listening sockets.
p: Show the name of the process that opened the socket.
n: Do not try to resolve service names.