BASICS OF NETWORK CONFIGURATIONS, FILES AND NETWORKING COMMANDS
Network Programming Lab (CS334)

March 30, 2021

Sheen Xavier A
Roll No : 57
University Roll No : TVE18CS058
Department of Computer Science and Engineering
College of Engineering, Trivandrum

Contents

Chapter 1

Basics of Network Configurations, Files and Networking Commands

1.1 Aim

To get started with basics of network configurations, files and networking commands in Linux.

1.2 Commands

1.2.1 ifconfig

Description

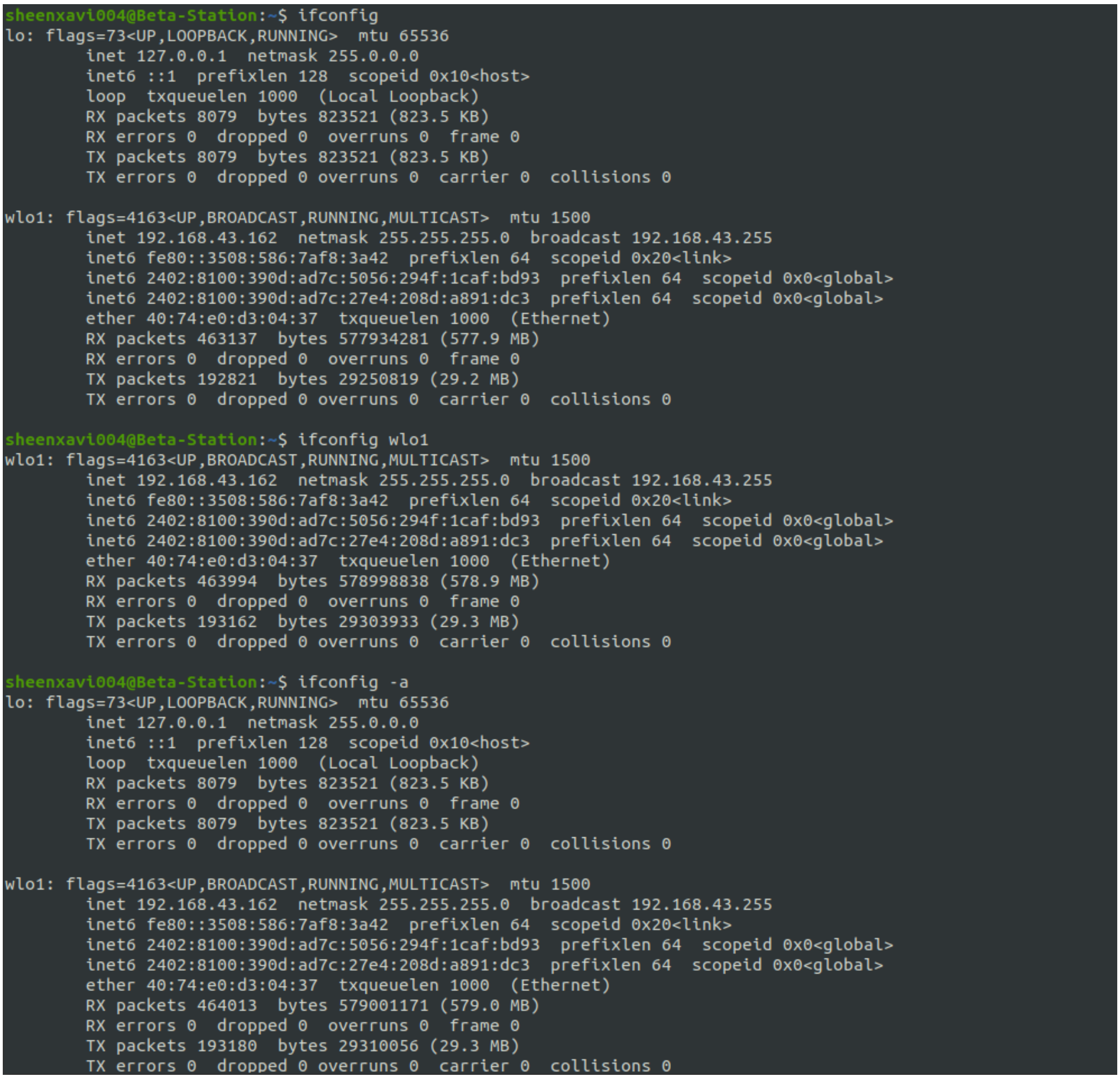
ifconfig is used to configure the kernel-resident network interfaces. It is used to initialize an interface, assign IP address to interface and enable or disable interface on demand. With this command you can view IP Address and Hardware / MAC address assign to interface and also MTU(Maximum transmission unit) size.

If a single interface argument is given, it displays the status of the given interface only. If a single -a argument is given, it displays the status of all interfaces, even those that are down.

Syntax

```
ifconfig
ifconfig [interface]
ifconfig -a
```

Usage



```
sheenxavi004@Beta-Station:~$ ifconfig
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8079  bytes 823521 (823.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8079  bytes 823521 (823.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.162  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::3508:586:7af8:3a42  prefixlen 64  scopeid 0x20<link>
        inet6 2402:8100:390d:ad7c:5056:294f:1caf:bd93  prefixlen 64  scopeid 0x0<global>
        inet6 2402:8100:390d:ad7c:27e4:208d:a891:dc3  prefixlen 64  scopeid 0x0<global>
        ether 40:74:e0:d3:04:37  txqueuelen 1000  (Ethernet)
        RX packets 463137  bytes 577934281 (577.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 192821  bytes 29250819 (29.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sheenxavi004@Beta-Station:~$ ifconfig wlo1
wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.162  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::3508:586:7af8:3a42  prefixlen 64  scopeid 0x20<link>
        inet6 2402:8100:390d:ad7c:5056:294f:1caf:bd93  prefixlen 64  scopeid 0x0<global>
        inet6 2402:8100:390d:ad7c:27e4:208d:a891:dc3  prefixlen 64  scopeid 0x0<global>
        ether 40:74:e0:d3:04:37  txqueuelen 1000  (Ethernet)
        RX packets 463994  bytes 578998838 (578.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 193162  bytes 29303933 (29.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sheenxavi004@Beta-Station:~$ ifconfig -a
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8079  bytes 823521 (823.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8079  bytes 823521 (823.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.162  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::3508:586:7af8:3a42  prefixlen 64  scopeid 0x20<link>
        inet6 2402:8100:390d:ad7c:5056:294f:1caf:bd93  prefixlen 64  scopeid 0x0<global>
        inet6 2402:8100:390d:ad7c:27e4:208d:a891:dc3  prefixlen 64  scopeid 0x0<global>
        ether 40:74:e0:d3:04:37  txqueuelen 1000  (Ethernet)
        RX packets 464013  bytes 579001171 (579.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 193180  bytes 29310056 (29.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figure 1.1: Usage of ifconfig

1.2.2 ping

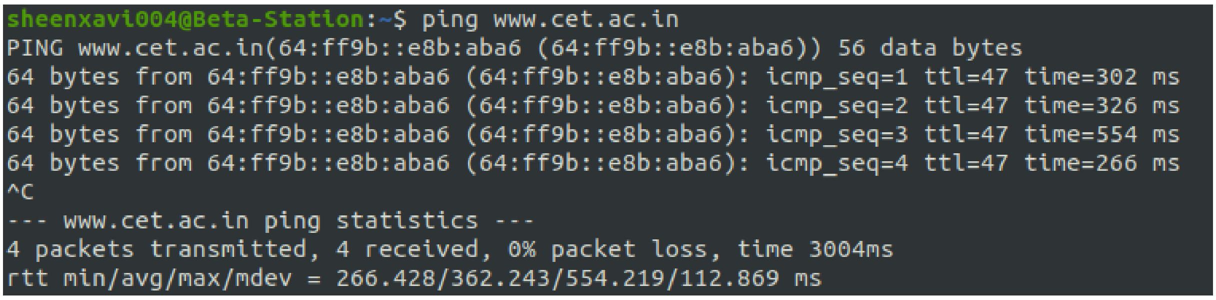
Description

ping (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. It uses the ICMP (Internet Control Message Protocol) and sends a series of ICMP echo request messages to the target host and waits for an ICMP echo reply. It also helps to calculate the package loss, round trip time of the packets, and whether the target host is reachable.

Syntax

```
ping <URL/IP Address>
```

Usage



```
sheenxavi004@Beta-Station:~$ ping www.cet.ac.in
PING www.cet.ac.in(64:ff9b::e8b:aba6 (64:ff9b::e8b:aba6)) 56 data bytes
64 bytes from 64:ff9b::e8b:aba6 (64:ff9b::e8b:aba6): icmp_seq=1 ttl=47 time=302 ms
64 bytes from 64:ff9b::e8b:aba6 (64:ff9b::e8b:aba6): icmp_seq=2 ttl=47 time=326 ms
64 bytes from 64:ff9b::e8b:aba6 (64:ff9b::e8b:aba6): icmp_seq=3 ttl=47 time=554 ms
64 bytes from 64:ff9b::e8b:aba6 (64:ff9b::e8b:aba6): icmp_seq=4 ttl=47 time=266 ms
^C
--- www.cet.ac.in ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 266.428/362.243/554.219/112.869 ms
```

Figure 1.2: Usage of ping

1.2.3 traceroute

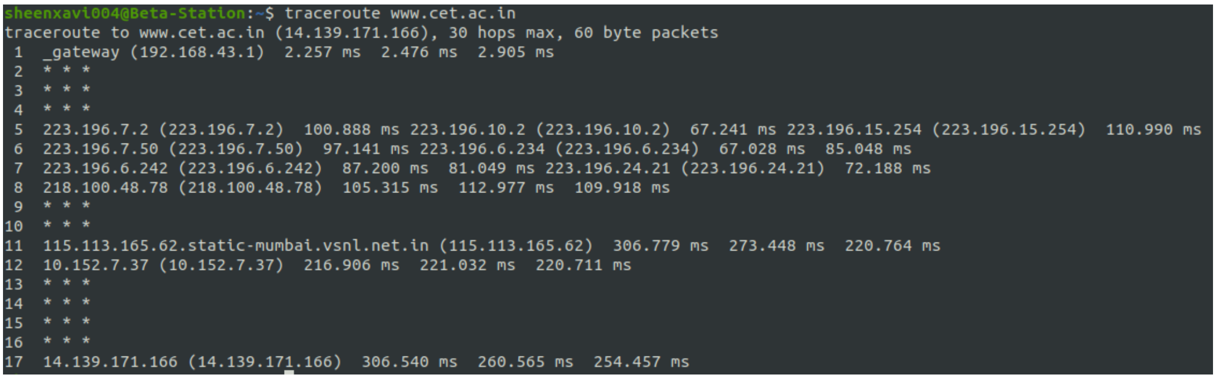
Description

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes.

Syntax

```
traceroute <Host Address>
```

Usage



```
sheenxavi004@Beta-Station:~$ traceroute www.cet.ac.in
traceroute to www.cet.ac.in (14.139.171.166), 30 hops max, 60 byte packets
 1  _gateway (192.168.43.1)  2.257 ms  2.476 ms  2.905 ms
 2  * * *
 3  * * *
 4  * * *
 5  223.196.7.2 (223.196.7.2)  100.888 ms 223.196.10.2 (223.196.10.2)  67.241 ms 223.196.15.254 (223.196.15.254)  110.990 ms
 6  223.196.7.50 (223.196.7.50)  97.141 ms 223.196.6.234 (223.196.6.234)  67.028 ms  85.048 ms
 7  223.196.6.242 (223.196.6.242)  87.200 ms  81.049 ms 223.196.24.21 (223.196.24.21)  72.188 ms
 8  218.100.48.78 (218.100.48.78)  105.315 ms  112.977 ms  109.918 ms
 9  * * *
10  * * *
11  115.113.165.62.static-mumbai.vsnl.net.in (115.113.165.62)  306.779 ms  273.448 ms  220.764 ms
12  10.152.7.37 (10.152.7.37)  216.906 ms  221.032 ms  220.711 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  14.139.171.166 (14.139.171.166)  306.540 ms  260.565 ms  254.457 ms
```

Figure 1.3: Usage of traceroute

1.2.4 netstat

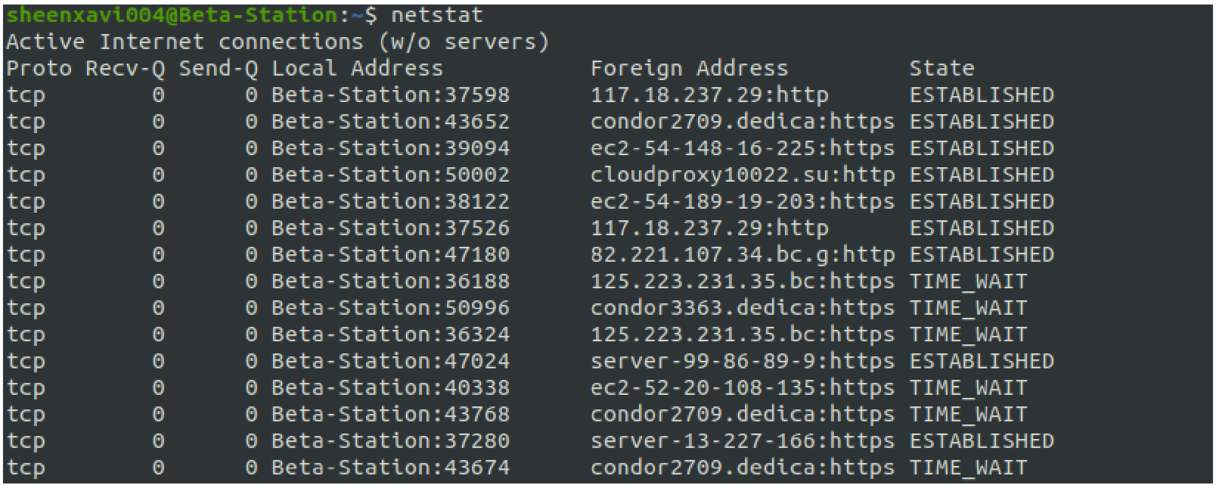
Description

Netstat(Network Statistics) command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships. When combined with -a it displays both listening and non listening sockets.

Syntax

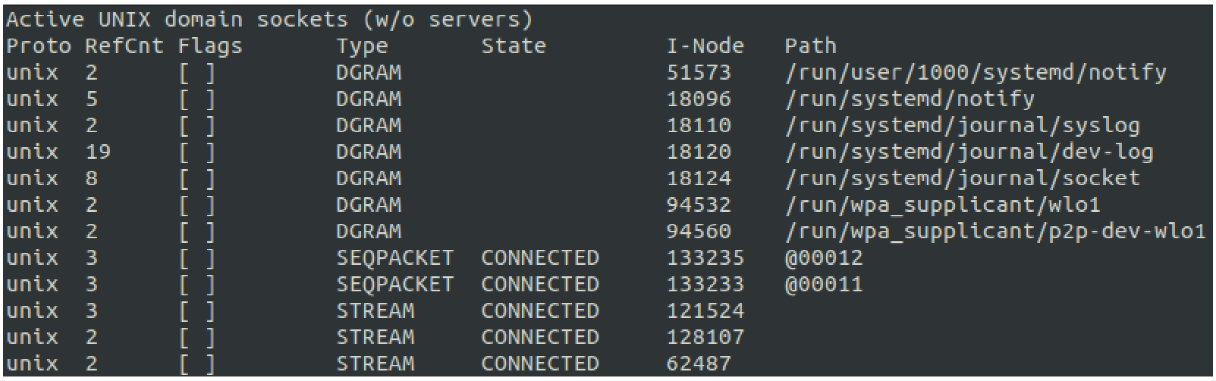
```
netstat
netstat -a
```

Usage



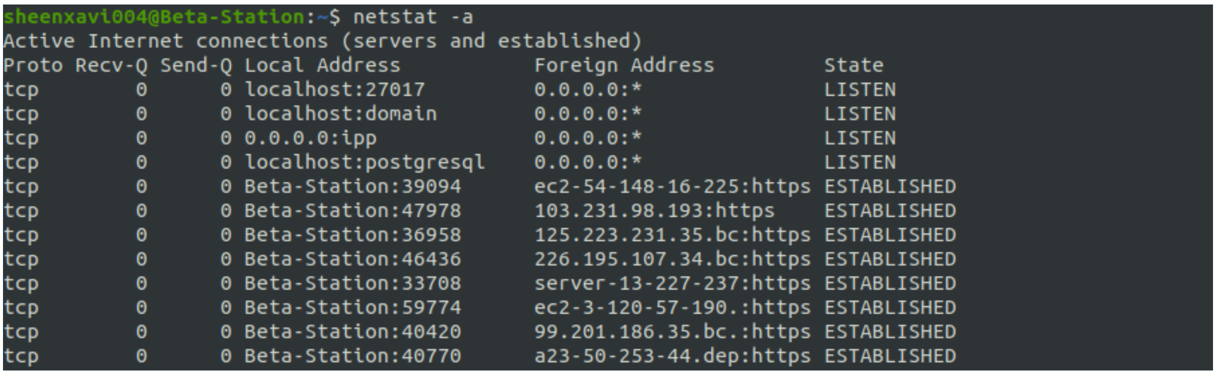
```
sheenxavi004@Beta-Station:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 Beta-Station:37598      117.18.237.29:http      ESTABLISHED
tcp        0      0 Beta-Station:43652      condor2709.dedica:https ESTABLISHED
tcp        0      0 Beta-Station:39094      ec2-54-148-16-225:https ESTABLISHED
tcp        0      0 Beta-Station:50002      cloudproxy10022.su:http ESTABLISHED
tcp        0      0 Beta-Station:38122      ec2-54-189-19-203:https ESTABLISHED
tcp        0      0 Beta-Station:37526      117.18.237.29:http      ESTABLISHED
tcp        0      0 Beta-Station:47180      82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 Beta-Station:36188      125.223.231.35.bc:https TIME_WAIT
tcp        0      0 Beta-Station:50996      condor3363.dedica:https TIME_WAIT
tcp        0      0 Beta-Station:36324      125.223.231.35.bc:https TIME_WAIT
tcp        0      0 Beta-Station:47024      server-99-86-89-9:https ESTABLISHED
tcp        0      0 Beta-Station:40338      ec2-52-20-108-135:https TIME_WAIT
tcp        0      0 Beta-Station:43768      condor2709.dedica:https TIME_WAIT
tcp        0      0 Beta-Station:37280      server-13-227-166:https ESTABLISHED
tcp        0      0 Beta-Station:43674      condor2709.dedica:https TIME_WAIT
```

Figure 1.4: Usage of netstat



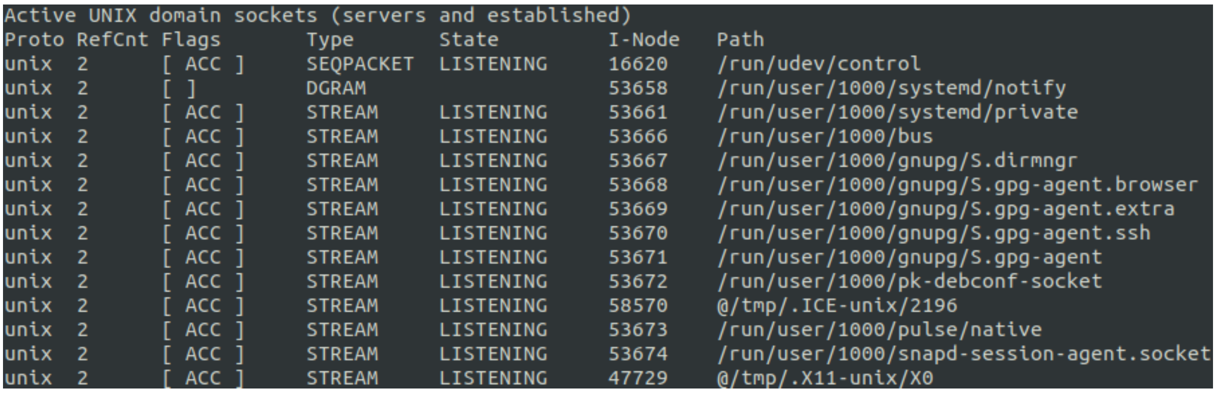
```
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    51573    /run/user/1000/systemd/notify
unix  5      [ ]         DGRAM                    18096    /run/systemd/notify
unix  2      [ ]         DGRAM                    18110    /run/systemd/journal/syslog
unix  19     [ ]         DGRAM                    18120    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM                    18124    /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    94532    /run/wpa_supplicant/wlo1
unix  2      [ ]         DGRAM                    94560    /run/wpa_supplicant/p2p-dev-wlo1
unix  3      [ ]         SEQPACKET  CONNECTED     133235   @00012
unix  3      [ ]         SEQPACKET  CONNECTED     133233   @00011
unix  3      [ ]         STREAM     CONNECTED     121524
unix  2      [ ]         STREAM     CONNECTED     128107
unix  2      [ ]         STREAM     CONNECTED     62487
```

Figure 1.5: Usage of netstat(contd...)



```
sheenxavi004@Beta-Station:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:27017         0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ipp             0.0.0.0:*               LISTEN
tcp        0      0 localhost:postgresql    0.0.0.0:*               LISTEN
tcp        0      0 Beta-Station:39094      ec2-54-148-16-225:https ESTABLISHED
tcp        0      0 Beta-Station:47978      103.231.98.193:https    ESTABLISHED
tcp        0      0 Beta-Station:36958      125.223.231.35.bc:https ESTABLISHED
tcp        0      0 Beta-Station:46436      226.195.107.34.bc:https ESTABLISHED
tcp        0      0 Beta-Station:33708      server-13-227-237:https ESTABLISHED
tcp        0      0 Beta-Station:59774      ec2-3-120-57-190.:https ESTABLISHED
tcp        0      0 Beta-Station:40420      99.201.186.35.bc.:https ESTABLISHED
tcp        0      0 Beta-Station:40770      a23-50-253-44.dep:https ESTABLISHED
```

Figure 1.6: Usage of netstat -a



```
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     SEQPACKET  LISTENING     16620    /run/udev/control
unix  2      [ ]         DGRAM                    53658    /run/user/1000/systemd/notify
unix  2      [ ACC ]     STREAM     LISTENING     53661    /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM     LISTENING     53666    /run/user/1000/bus
unix  2      [ ACC ]     STREAM     LISTENING     53667    /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM     LISTENING     53668    /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM     LISTENING     53669    /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM     LISTENING     53670    /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM     LISTENING     53671    /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM     LISTENING     53672    /run/user/1000/pk-debconf-socket
unix  2      [ ACC ]     STREAM     LISTENING     58570    @/tmp/.ICE-unix/2196
unix  2      [ ACC ]     STREAM     LISTENING     53673    /run/user/1000/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     53674    /run/user/1000/snapd-session-agent.socket
unix  2      [ ACC ]     STREAM     LISTENING     47729    @/tmp/.X11-unix/X0
```

Figure 1.7: Usage of netstat -a(contd...)

1.2.5 nslookup

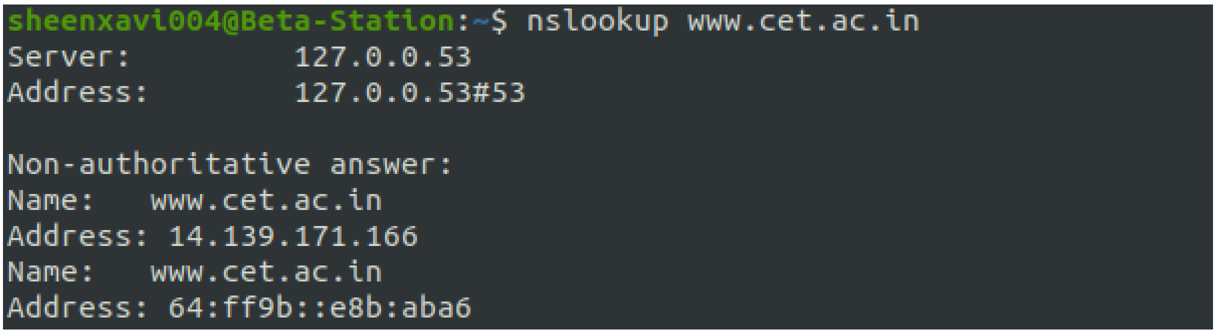
Description

nslookup(Name Server Lookup) is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems. Most operating systems come with built-in nslookup feature.

Syntax

```
nslookup <URL / IP Address>
```

Usage



```
sheenxavi004@Beta-Station:~$ nslookup www.cet.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.cet.ac.in
Address: 14.139.171.166
Name:   www.cet.ac.in
Address: 64:ff9b::e8b:aba6
```

Figure 1.8: Usage of nslookup

1.2.6 route

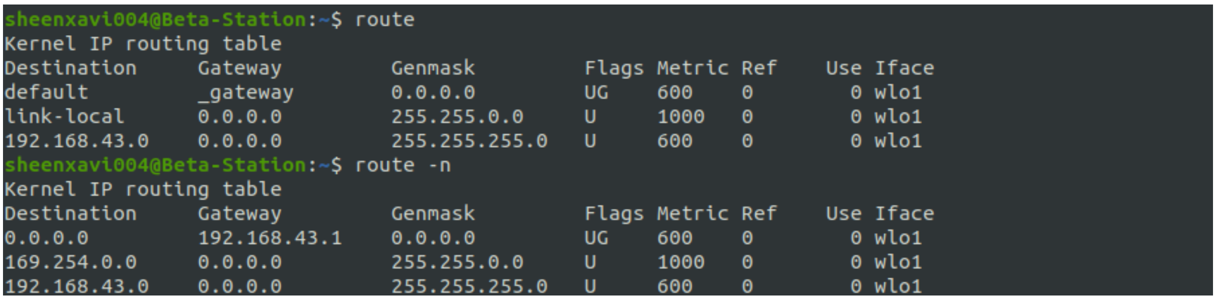
Description

route command in Linux is used when you want to work with the IP/kernel routing table. Its basic function is to show or manipulate IP routing tables. It can add and delete routes and default gateway. route command simply displays the IP/Kernel routing table. When combined with a -n it displays the full numeric form of the IP/Kernel routing table.

Syntax

```
route
route -n
```

Usage



```
sheenxavi004@Beta-Station:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlo1
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlo1
sheenxavi004@Beta-Station:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.43.1    0.0.0.0         UG    600    0        0 wlo1
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlo1
192.168.43.0    0.0.0.0         255.255.255.0   U     600    0        0 wlo1
```

Figure 1.9: Usage of route

1.2.7 dig

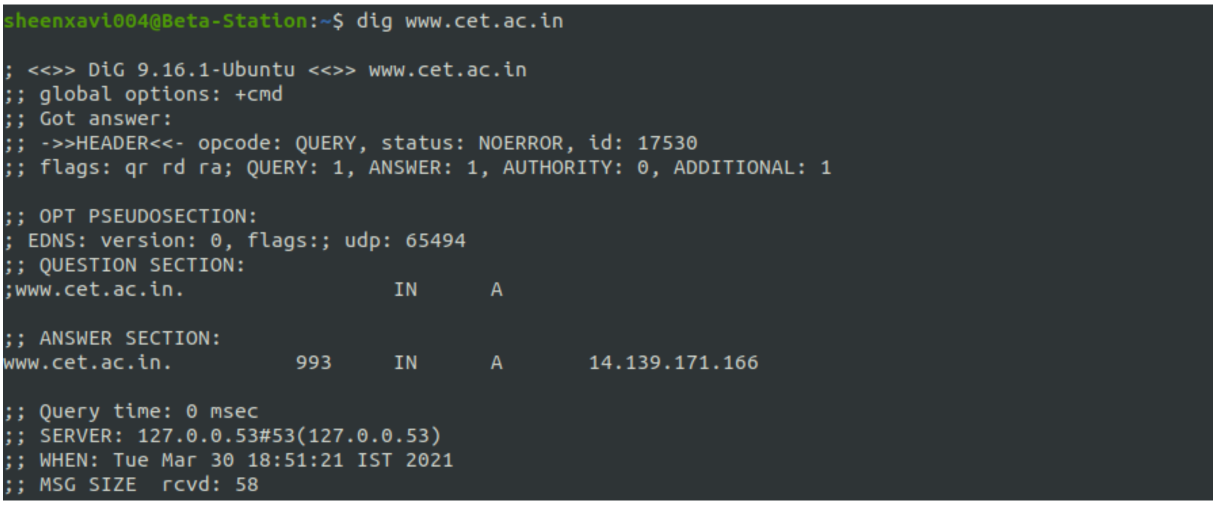
Description

dig (Domain Information Groper) is used for retrieving information about DNS name servers such as a record, CNAME, MX Record etc. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. A +short is included with the command to query domain "A" record. An MX is included with the command to display the MX record for the domain.

Syntax

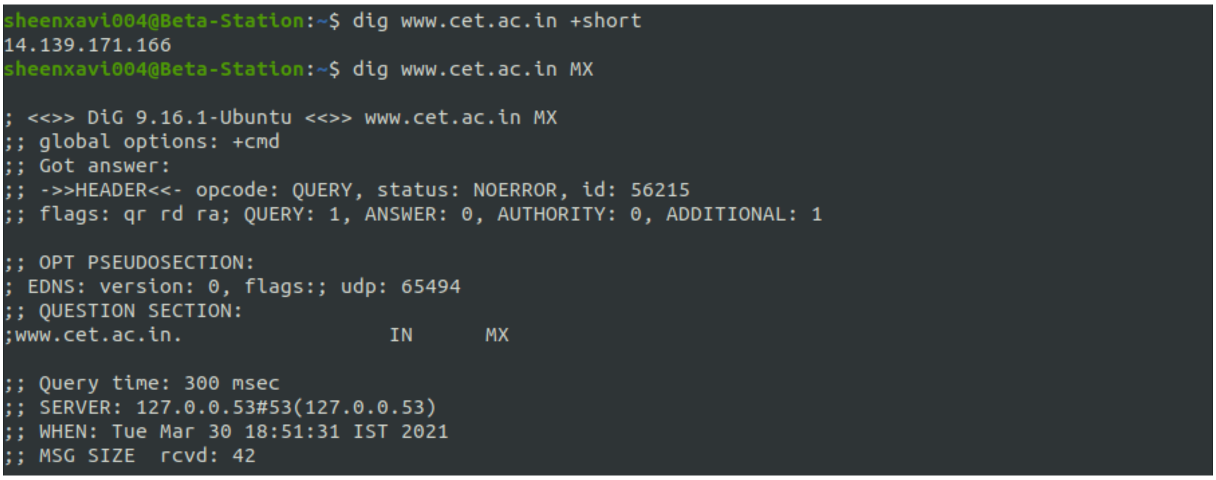
```
dig [URL]
dig [URL] +short
dig [URL] MX
```

Usage



```
sheenxavi004@Beta-Station:~$ dig www.cet.ac.in

; <<>> DiG 9.16.1-Ubuntu <<>> www.cet.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17530
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.cet.ac.in.                 IN      A

;; ANSWER SECTION:
www.cet.ac.in.          993     IN      A       14.139.171.166

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Mar 30 18:51:21 IST 2021
;; MSG SIZE  rcvd: 58
```

Figure 1.10: Usage of dig



```
sheenxavi004@Beta-Station:~$ dig www.cet.ac.in +short
14.139.171.166
sheenxavi004@Beta-Station:~$ dig www.cet.ac.in MX

; <<>> DiG 9.16.1-Ubuntu <<>> www.cet.ac.in MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56215
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.cet.ac.in.                 IN      MX

;; Query time: 300 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Mar 30 18:51:31 IST 2021
;; MSG SIZE  rcvd: 42
```

Figure 1.11: Usage of dig with +short and MX options

1.2.8 arp

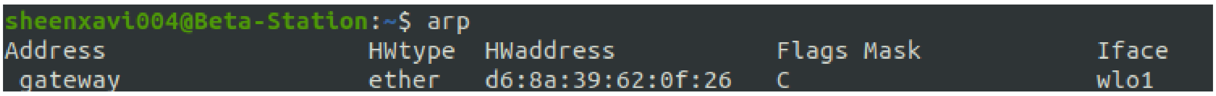
Description

arp(Address Resolution Protocol) command manipulates the System's ARP cache. It is a protocol used by network nodes to resolve IP addresses to their corresponding MAC addresses. It can also be used to add an address for which to proxy arp and to forcefully add permanent entries to the ARP table. Invoking the arp command without any options will display the contents of the arp cache table.

Syntax

```
arp
```

Usage



```
sheenxavi004@Beta-Station:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
 gateway                 ether   d6:8a:39:62:0f:26   C                     wlo1
```

Figure 1.12: Usage of arp

1.2.9 host

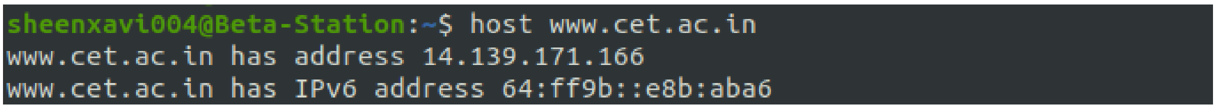
Description

host command in Linux system is used for DNS lookup operations. In simple words, this command is used to find the IP address of a particular domain name or if you want to find out the domain name of a particular IP address in IPv4 or IPv6.

Syntax

```
host <URL/IP Address>
```

Usage



```
sheenxavi004@Beta-Station:~$ host www.cet.ac.in
www.cet.ac.in has address 14.139.171.166
www.cet.ac.in has IPv6 address 64:ff9b::e8b:aba6
```

Figure 1.13: Usage of host

1.2.10 hostname

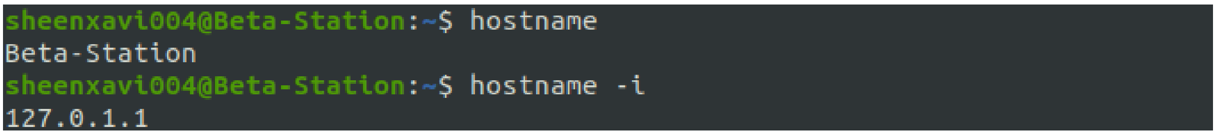
Description

hostname command in Linux is used to obtain the DNS(Domain Name System) name and set the system's hostname or NIS(Network Information System) domain name. A hostname is a name which is given to a computer and it attached to the network. Its main purpose is to uniquely identify over a network. The -i option is used to get the IP(network) addresses(works only if the hostname is resolvable).

Syntax

```
hostname
hostname -i
```

Usage



```
sheenxavi004@Beta-Station:~$ hostname
Beta-Station
sheenxavi004@Beta-Station:~$ hostname -i
127.0.1.1
```

Figure 1.14: Usage of hostname

1.2.11 ethtool

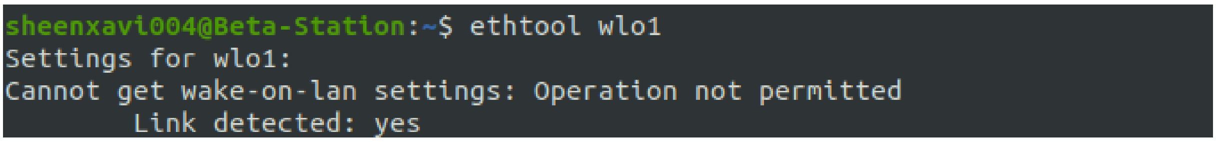
Description

ethtool command is used to display/change Ethernet adapter settings. You can change Network Interface Card speed, auto-negotiation, wake on LAN setting, duplex mode using this command.

Syntax

```
ethtool <devname>
```

Usage



```
sheenxavi004@Beta-Station:~$ ethtool wlo1
Settings for wlo1:
Cannot get wake-on-lan settings: Operation not permitted
        Link detected: yes
```

Figure 1.15: Usage of ethtool

1.3 Result

The basic commands pertaining to Network Configurations were studied. These commands were executed in a Linux Shell and the results were verified.