

# **NETWORKS LAB**

## **CS3093D**

# **ASSIGNMENT 1**

Submitted by,  
Indrajith T S  
B180486CS  
S8 - Btech

# NETWORK COMMANDS

## 1. Ping

Ping sends ICMP ECHO\_REQUEST to network host specified by the address

ping 8.8.8.8 to ping to google's primary dns

ping www.google.com for pinging google using address

```
indrajith@indrajithb180486cs:~$ ping www.google.com
PING www.google.com (142.250.182.4) 56(84) bytes of data.
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=1 ttl=114 time=2730 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=2 ttl=114 time=1858 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=3 ttl=114 time=1243 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=4 ttl=114 time=274 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=5 ttl=114 time=874 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=6 ttl=114 time=2064 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=7 ttl=114 time=1067 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=8 ttl=114 time=1681 ms
^C
--- www.google.com ping statistics ---
9 packets transmitted, 8 received, 11.1111% packet loss, time 8585ms
rtt min/avg/max/mdev = 273.721/1473.749/2729.852/718.862 ms, pipe 3
indrajith@indrajithb180486cs:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=648 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=141 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=503 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=92.9 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4016ms
rtt min/avg/max/mdev = 92.897/346.113/648.095/235.609 ms
indrajith@indrajithb180486cs:~$
```

Here host address is specified using its name and ip.

Some other flags that can be used with the ping command are as follows

Flag -s size is used to specify the size of a packet

-c count is used to specify the no of packets

-q for quiet output which is only the summary

-i time for time interval

-t ttl to set time to live

-W timeout to set timeout in s in case of not reachable

```
terminal 58115 17:22
indrajith@indrajithb180486cs:~$ ping -q -i 2 -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 8027ms
rtt min/avg/max/mdev = 321.266/924.967/2701.890/898.252 ms, pipe 2
indrajith@indrajithb180486cs:~$
```

```
terminal 58115 17:22
indrajith@indrajithb180486cs:~$ ping -t 1 -W 1 -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 10.0.2.2 icmp_seq=1 Time to live exceeded
From 10.0.2.2 icmp_seq=2 Time to live exceeded
From 10.0.2.2 icmp_seq=3 Time to live exceeded
From 10.0.2.2 icmp_seq=4 Time to live exceeded
From 10.0.2.2 icmp_seq=5 Time to live exceeded

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 4086ms
indrajith@indrajithb180486cs:~$
```

## 2. tracert/traceroute

It tracks the route packets take from an ip network on their way to the given host destination.

```
terminal 58115 17:22
indrajith@indrajithb180486cs:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2)  0.758 ms  0.743 ms  0.785 ms
 2 * *
 3 * *
 4 * *
 5 * *
 6 * *
 7 * *
 8 * *
 9 * *
10 * *
11 * *
12 * *
13 * *
14 * *
15 * *
16 * *
17 * *
18 * *
19 * *
20 * *
21 * *
22 * *
23 * *
24 * *
25 * *
26 * *
27 * *
28 * *
29 * *
30 * *

indrajith@indrajithb180486cs:~$
```

This shows the only path that exits through the gateway of the virtual machine.

```
Command Prompt  
C:\Users\INDRAJITH T S>tracert 8.8.8.8  
Tracing route to dns.google [8.8.8.8]  
over a maximum of 30 hops:  
  
 1      3 ms      3 ms      3 ms  192.168.43.1  
 2      *          *          *      Request timed out.  
 3    370 ms     799 ms     598 ms  10.45.1.226  
 4    517 ms    1421 ms    1154 ms  10.45.8.178  
 5    757 ms     308 ms     256 ms  10.45.8.187  
 6    729 ms     785 ms       *      172.16.101.54  
 7      *          *          *      Request timed out.  
 8      *          *          1775 ms  117.216.207.222  
 9    270 ms     132 ms     130 ms  72.14.218.250  
10   1198 ms    1403 ms     321 ms  216.239.43.137  
11   1349 ms     602 ms     980 ms  74.125.253.17  
12   1818 ms       *      3474 ms  dns.google [8.8.8.8]  
  
Trace complete.  
C:\Users\INDRAJITH T S>
```

Tracert identifying all the routes from the host machine.

### 3. ifconfig/ipconfig

Ifconfig is used to show the network details in linux

- a for all list
- s for short list
- interface name for a specific interface details
- down for deactivating up for activating

```
Indrajith@indrajithb180486cs:~$ ifconfig -a
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::db6c:355a:51aa:3bd7 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:19:9e:0d txqueuelen 1000 (Ethernet)
            RX packets 141373 bytes 196173204 (196.1 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 68270 bytes 4530976 (4.5 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 750 bytes 77230 (77.2 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 750 bytes 77230 (77.2 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Indrajith@indrajithb180486cs:~$
```

For all interfaces

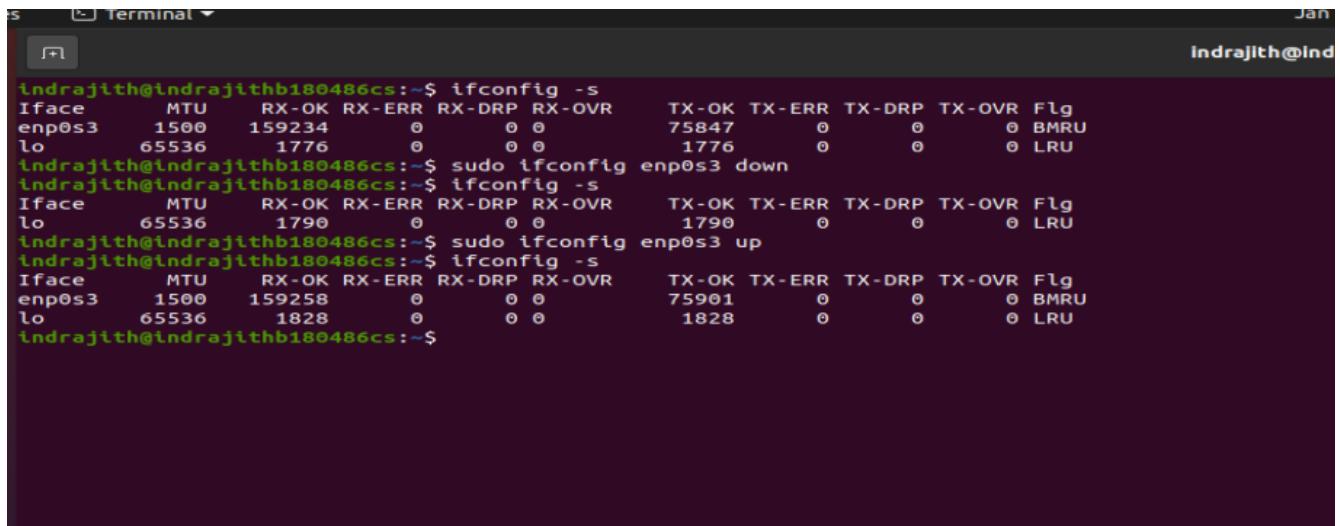
```
Indrajith@indrajithb180486cs:~$ ifconfig -s
Iface      MTU   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3     1500  142712      0      0 0       68799      0      0      0 BMRU
lo         65536     750      0      0 0       750       0      0      0 LRU
Indrajith@indrajithb180486cs:~$
```

Summary of interfaces

```
Indrajith@indrajithb180486cs:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fe80::db6c:355a:51aa:3bd7 prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:19:9e:0d txqueuelen 1000 (Ethernet)
            RX packets 145814 bytes 202466706 (202.4 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 70431 bytes 4660859 (4.6 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Indrajith@indrajithb180486cs:~$
```

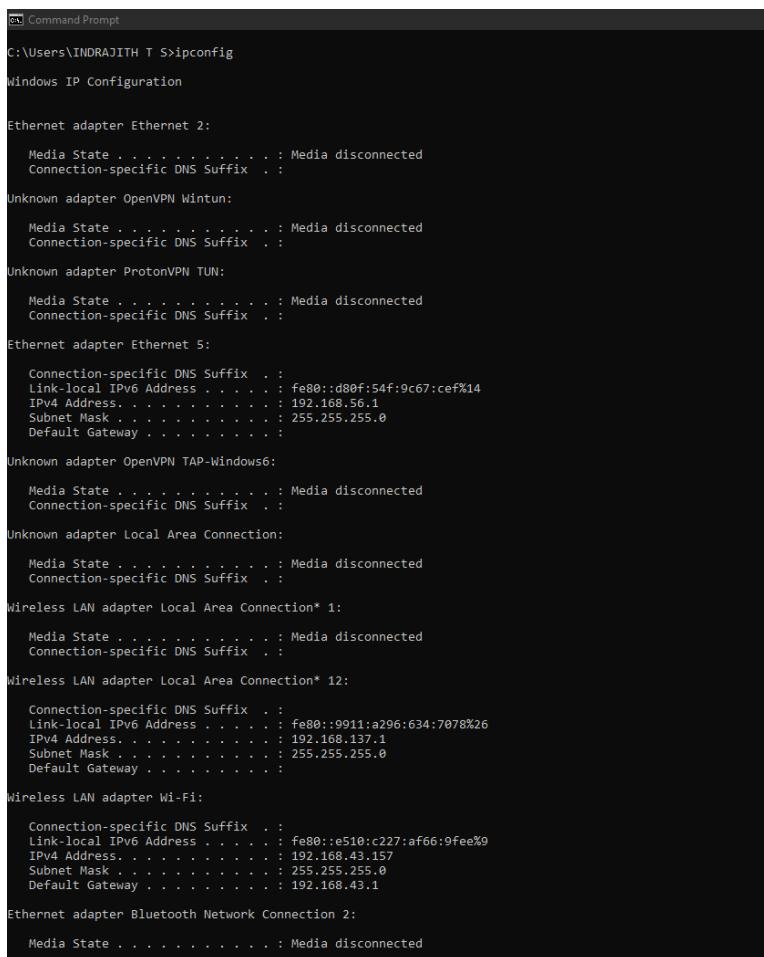
Detail of a specific interface



```
Jan
indrajith@indrajithb180486cs:~$ ifconfig -s
Iface      MTU   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3     1500  159234     0     0     0    75847     0     0     0 BMRU
lo        65536   1776     0     0     0    1776     0     0     0 LRU
indrajith@indrajithb180486cs:~$ sudo ifconfig enp0s3 down
indrajith@indrajithb180486cs:~$ ifconfig -s
Iface      MTU   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
lo        65536   1790     0     0     0    1790     0     0     0 LRU
indrajith@indrajithb180486cs:~$ sudo ifconfig enp0s3 up
indrajith@indrajithb180486cs:~$ ifconfig -s
Iface      MTU   RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3     1500  159258     0     0     0    75901     0     0     0 BMRU
lo        65536   1828     0     0     0    1828     0     0     0 LRU
indrajith@indrajithb180486cs:~$
```

## Changing the working status of interfaces

Ipconfig is the command used in windows



```
Command Prompt
C:\Users\INDRAJITH T S>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Unknown adapter OpenVPN Wintun:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Unknown adapter ProtonVPN TUN:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Ethernet adapter Ethernet 5:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::d80f:54f:9c67:cef%14
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Unknown adapter OpenVPN TAP-Windows6:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Unknown adapter Local Area Connection:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . .

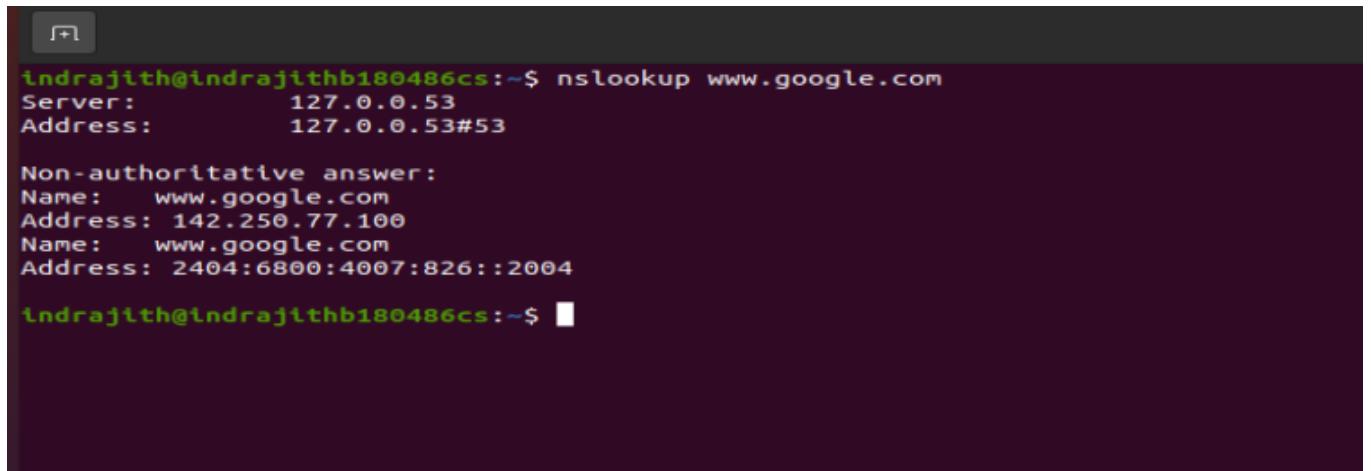
Wireless LAN adapter Local Area Connection* 12:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::9011:a296:634:7078%26
  IPv4 Address . . . . . : 192.168.137.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::e510:c227:af66:9fee%9
  IPv4 Address . . . . . : 192.168.43.157
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.43.1

Ethernet adapter Bluetooth Network Connection 2:
  Media State . . . . . : Media disconnected
```

#### 4. dig/nslookup/host

This is to query internet dns. This can be used to troubleshoot dns servers through interactive session.

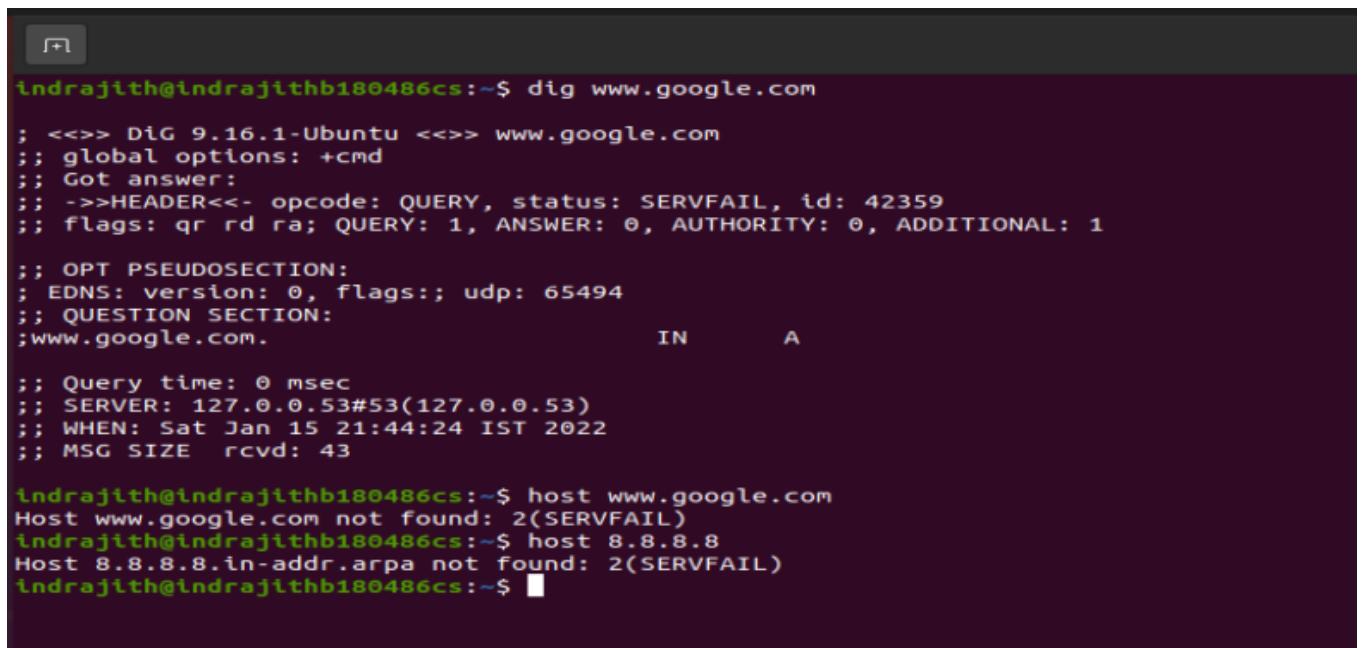


```
indrajith@indrajithb180486cs:~$ nslookup www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.77.100
Name:   www.google.com
Address: 2404:6800:4007:826::2004

indrajith@indrajithb180486cs:~$
```

nslookup of google



```
indrajith@indrajithb180486cs:~$ dig www.google.com
; <>> DiG 9.16.1-Ubuntu <>> www.google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 42359
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.google.com.           IN      A
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sat Jan 15 21:44:24 IST 2022
;; MSG SIZE  rcvd: 43

indrajith@indrajithb180486cs:~$ host www.google.com
Host www.google.com not found: 2(SERVFAIL)
indrajith@indrajithb180486cs:~$ host 8.8.8.8
Host 8.8.8.8.in-addr.arpa not found: 2(SERVFAIL)
indrajith@indrajithb180486cs:~$
```

dig on google

```
indrajith@indrajithb180486cs:~$ nslookup -debug www.google.com
Server:      127.0.0.53
Address:     127.0.0.53#53

-----
    QUESTIONS:
        www.google.com, type = A, class = IN
    ANSWERS:
        -> www.google.com
            internet address = 142.250.67.36
            ttl = 46
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
-----
Non-authoritative answer:
Name:   www.google.com
Address: 142.250.67.36
-----
    QUESTIONS:
        www.google.com, type = AAAA, class = IN
    ANSWERS:
        -> www.google.com
            has AAAA address 2404:6800:4007:808::2004
            ttl = 258
    AUTHORITY RECORDS:
    ADDITIONAL RECORDS:
-----
Name:   www.google.com
Address: 2404:6800:4007:808::2004

indrajith@indrajithb180486cs:~$
```

debug on google

## 5. whois

This command provides details and information about the server that is provided.

```

Indrajith@Indrajithb180486cs: ~
lndrajith@Indrajithb180486cs: ~ whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: https://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 2007-09-15T04:00:00Z
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
Dnssec: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-01-15T07:25:33Z <<
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar, which may be longer or shorter. Please refer to the registrar's database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and automated except as reasonably necessary to register domain names or modify existing registrations. If you attempt to query our Whois Services ("VeriSign") Whois database by providing to VeriSign for information purposes only, and to assist persons in obtaining information about a domain name registrant's registration of a domain name, VeriSign reserves the right to limit your query to a maximum of 3 (three) requests per second. You further agree that you will not use this Data to: (i) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, fax, or other similar marketing tools and methods; or (ii) enable other individuals to do the same using your computer system through the use of scripts, programs, or other processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without VeriSign's prior written consent. You agree not to use electronic processes that are high-volume and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04+0000
Creation Date: 2007-09-15T04:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)

```

Flag -p for all mirrored databases

-c return the smallest ip range in with a reference to an irt object.

```

ls terminal ~
Indrajith@Indrajithb180486cs: ~ whois -a -c google.com
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
%
% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.
%
% Information related to 'Google.com'

inet-rtr:      Google.com
org:           ORG-NA1296-RIPE
local-as:      AS197267
ifaddr:        172.217.169.238 Masklen 0
ifaddr:        172.217.0.0 Masklen 0
admin-c:       AA37671-RIPE
tech-c:        AA37671-RIPE
mnt-by:        Jb71-mnt
created:       2021-06-10T15:02:02Z
last-modified: 2021-06-10T15:14:15Z
source:        RIPE

organisation:  ORG-NA1296-RIPE
org-name:      Nickb
org-type:      OTHER
address:       Hafez st
mnt-ref:      jb7-mnt
mnt-by:        jb7-mnt
mnt-by:        Jb70-mnt
created:       2021-06-10T06:33:51Z
last-modified: 2021-06-10T06:33:51Z
source:        RIPE # Filtered

role:          Admin
address:      Shariaty
nic-hdl:       AA37671-RIPE
mnt-by:        jb7-mnt
created:       2021-06-10T06:07:49Z
last-modified: 2021-06-10T06:07:49Z
source:        RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.102.2 (ANGUS)

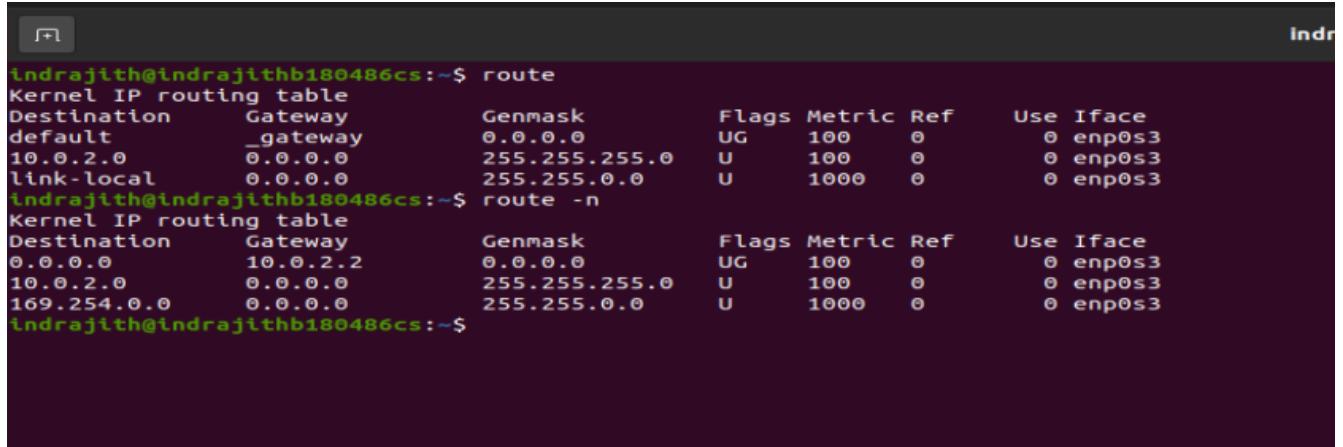
Indrajith@Indrajithb180486cs: ~

```

## 6. route

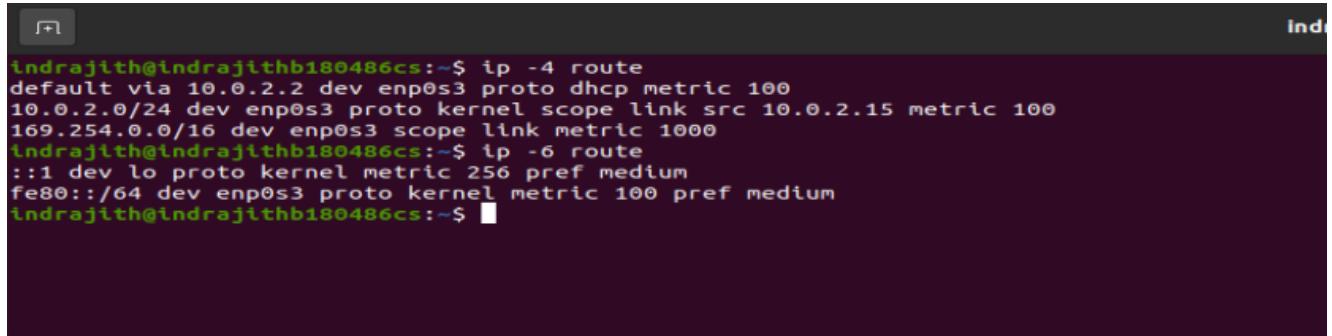
This command is used to see the routing tables that is already established or to add another route as we wish.

Routing table in normal and complete numerical mode



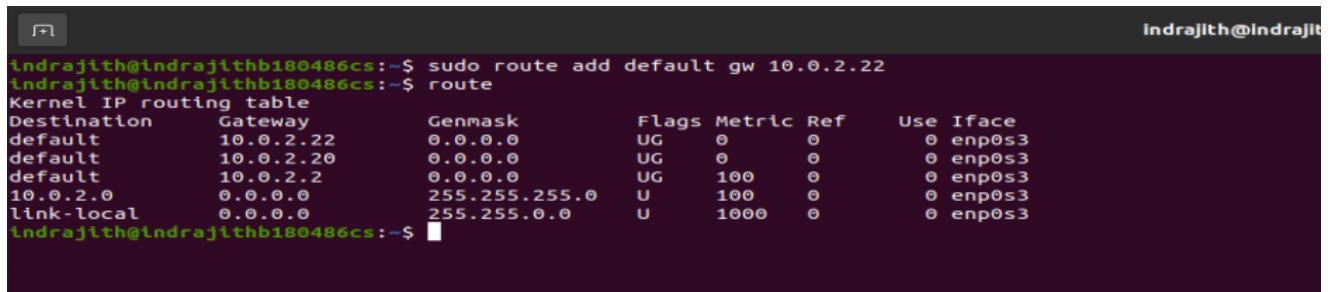
```
indrajith@indrajithb180486cs:~$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         _gateway       0.0.0.0        UG    100    0      0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0   U     100    0      0 enp0s3
link-local      0.0.0.0        255.255.0.0    U     1000   0      0 enp0s3
indrajith@indrajithb180486cs:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
0.0.0.0         10.0.2.2       0.0.0.0        UG    100    0      0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0   U     100    0      0 enp0s3
169.254.0.0     0.0.0.0        255.255.0.0    U     1000   0      0 enp0s3
indrajith@indrajithb180486cs:~$
```

-4 flag for ipv4 and -6 flag for ipv6 with ip



```
indrajith@indrajithb180486cs:~$ ip -4 route
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
indrajith@indrajithb180486cs:~$ ip -6 route
::1 dev lo proto kernel metric 256 pref medium
fe80::/64 dev enp0s3 proto kernel metric 100 pref medium
indrajith@indrajithb180486cs:~$
```

Adding new routes



```
indrajith@indrajithb180486cs:~$ sudo route add default gw 10.0.2.22
indrajith@indrajithb180486cs:~$ route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
default         10.0.2.22       0.0.0.0        UG    0      0      0 enp0s3
default         10.0.2.20       0.0.0.0        UG    0      0      0 enp0s3
default         10.0.2.2        0.0.0.0        UG    100    0      0 enp0s3
10.0.2.0        0.0.0.0        255.255.255.0   U     100    0      0 enp0s3
link-local      0.0.0.0        255.255.0.0    U     1000   0      0 enp0s3
indrajith@indrajithb180486cs:~$
```

## 7. tcpdump

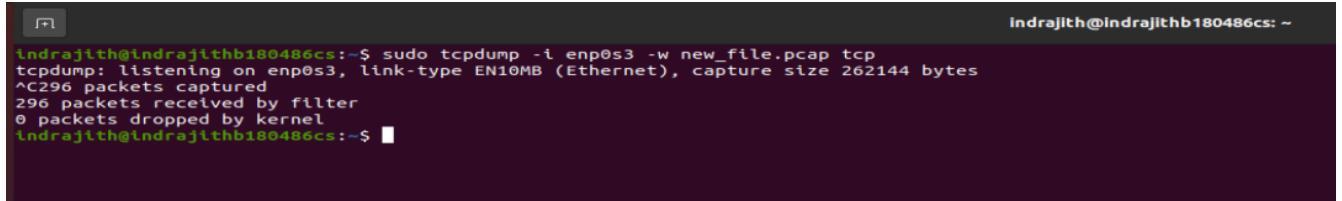
We need sudo permission to use this command. This command is used to listen to network traffic which prints the description of the contents of the packets.

```
Indrajith@Indrajithb180486cs:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:48:14.145631 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 08:00:27:19:9e:0d (oui Unknown), length 302
00:48:14.145813 IP gateway.bootps > Indrajithb180486cs.bootpc: BOOTP/DHCP, Reply, length 548
00:48:14.145906 ARP, Request who-has _gateway tell Indrajithb180486cs, length 28
00:48:14.145906 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
00:48:14.145909 IP Indrajithb180486cs > _gateway: ICMP Indrajithb180486cs udp port bootpc unreachable, length 556
00:48:14.149281 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:48:14.841423 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:48:27.209733 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:27.209744 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:27.209754 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:28.281322 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:29.305210 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:29.305236 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:30.330301 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:31.353191 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:32.377946 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:33.402065 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:34.425838 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:35.449382 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:36.473870 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:36.473912 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:37.497630 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:37.497650 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:38.521560 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:38.521579 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:39.545588 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:39.545747 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:40.560148 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:40.569349 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:41.593375 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:41.593392 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:42.617303 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:42.617515 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:43.641202 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:43.641228 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:44.665221 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:44.665249 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:45.689958 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:45.690056 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:46.713220 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:46.713248 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:47.737740 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:47.737767 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:48.761347 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:48.761371 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:49.785597 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:49.785628 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:50.800040 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:50.800145 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:51.833553 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:51.833721 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:52.857389 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:52.857413 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:53.881315 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:53.881335 ARP, Request who-has 10.0.2.22 tell Indrajithb180486cs, length 28
00:48:56.572447 IP 0.0.0.0.bootpc > 255.255.255.255.bootps: BOOTP/DHCP, Request from 08:00:27:19:9e:0d (oui Unknown), length 302
00:48:56.572661 IP gateway.bootps > Indrajithb180486cs.bootpc: BOOTP/DHCP, Reply, length 548
00:49:24.805266 ARP, Request _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
00:49:24.805281 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805294 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805306 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805318 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805330 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805342 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805354 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805366 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805378 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.805390 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
00:49:24.841677 IP6 Indrajithb180486cs > ff02::16: HBH ICMP6, multicast listener report v2, 2 group record(s), length 48
```

We can listen to any particular interface using -i interface name command.

```
Indrajith@Indrajithb180486cs:~$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:57:34.873720 IP Indrajithb180486cs.41178 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26609602, win 65535, length 0
00:57:34.873726 IP Indrajithb180486cs.41174 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26671335, win 65535, length 0
00:57:34.873726 IP Indrajithb180486cs.41174 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26623655, win 65535, length 0
00:57:34.873732 IP Indrajithb180486cs.41172 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26681091, win 65535, length 0
00:57:34.873737 IP Indrajithb180486cs.41170 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26759612, win 65535, length 0
00:57:34.873743 IP Indrajithb180486cs.41168 > server-65-8-80-2.maa51.r.cloudfront.net.https: Flags [.], ack 26816909, win 65535, length 0
00:57:34.874104 IP server-65-8-80-2.maa51.r.cloudfront.net.https > Indrajithb180486cs.41176: Flags [.], ack 1, win 65535, length 0
00:57:34.874112 IP server-65-8-80-2.maa51.r.cloudfront.net.https > Indrajithb180486cs.41178: Flags [.], ack 1, win 65535, length 0
00:57:34.874115 IP server-65-8-80-2.maa51.r.cloudfront.net.https > Indrajithb180486cs.41172: Flags [.], ack 1, win 65535, length 0
00:57:34.874116 IP server-65-8-80-2.maa51.r.cloudfront.net.https > Indrajithb180486cs.41170: Flags [.], ack 1, win 65535, length 0
00:57:34.874118 IP server-65-8-80-2.maa51.r.cloudfront.net.https > Indrajithb180486cs.41168: Flags [.], ack 1, win 65535, length 0
00:57:34.874780 IP Indrajithb180486cs.54411 > dns.google.domain: 6282+ [rau] PTR? 15.2.0.10.in-addr.arpa. (51)
00:57:34.894473 IP dns.google.domain > Indrajithb180486cs.54411: 6282 NXDomain 0/0 (51)
00:57:34.894566 IP Indrajithb180486cs.54411 > dns.google.domain: 6282+ PTR? 15.2.0.10.in-addr.arpa. (40)
00:57:34.914691 IP dns.google.domain > Indrajithb180486cs.54411: 6282 NXDomain 0/0 (40)
00:57:34.915376 IP Indrajithb180486cs.58343 > dns.google.domain: 19041+ [rau] PTR? 8.8.8.8.in-addr.arpa. (49)
00:57:34.935458 IP dns.google.domain > Indrajithb180486cs.58343: 19041 1/0 PTR dns.google. (73)
```

Filters can be applied to listening like specifying src and dst.  
We can also apply a tcp filter using tcp.

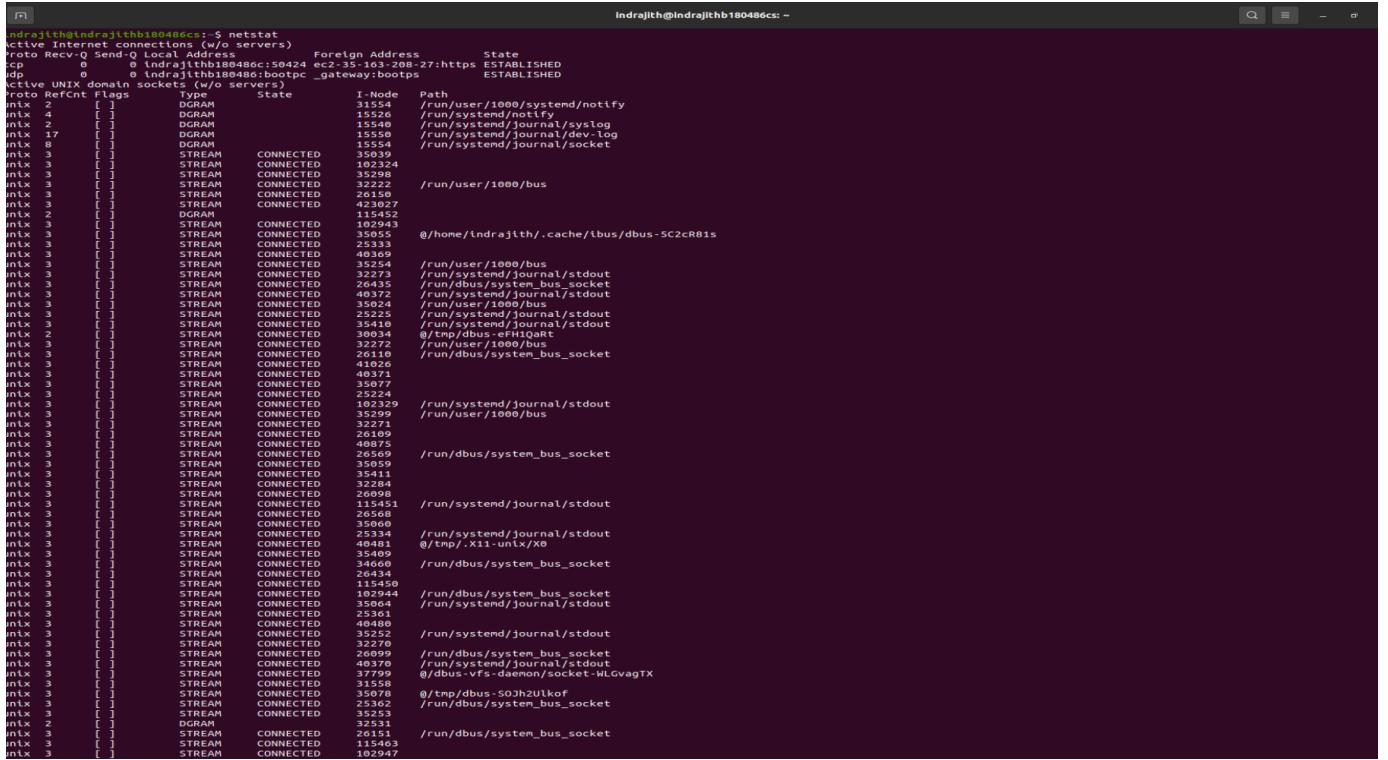


```
Indrajith@Indrajithb180486cs:~$ sudo tcpdump -i enp0s3 -w new_file.pcap tcp
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C296 packets captured
296 packets received by filter
0 packets dropped by kernel
Indrajith@Indrajithb180486cs:~$
```

Also we can save the captured info into file using -w filename.pcap

## 8. netstat/ss

This network command prints network connections , routing tables, interface statistics etc.



```
Indrajith@Indrajithb180486cs:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 Indrajithb180486cs:so424  ec2-35-163-208-27:https ESTABLISHED
tcp        0      0 Indrajithb180486cs:bootpc _gateway:bootps   ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State            I-Node Path
intx    2      [ ]          DGRAM     CONNECTED        31554  /run/user/1000/systemd/notify
intx    2      [ ]          DGRAM     CONNECTED        15549  /run/systemd/journal/stdout
intx    2      [ ]          DGRAM     CONNECTED        15549  /run/systemd/journal/syslog
intx   17      [ ]          DGRAM     CONNECTED        15550  /run/systemd/journal/dev-log
intx    8      [ ]          DGRAM     CONNECTED        15551  /run/systemd/journal/socket
intx    3      [ ]          STREAM    CONNECTED       35298
intx    3      [ ]          STREAM    CONNECTED       102324
intx    3      [ ]          STREAM    CONNECTED       35298
intx    3      [ ]          STREAM    CONNECTED       35298
intx    3      [ ]          STREAM    CONNECTED       26150
intx    3      [ ]          STREAM    CONNECTED       423027
intx    2      [ ]          DGRAM     CONNECTED       1152
intx    3      [ ]          STREAM    CONNECTED       102943
intx    3      [ ]          STREAM    CONNECTED       35055  @/home/Indrajith/.cache/libus/dbus-5C2cR81s
intx    3      [ ]          STREAM    CONNECTED       25333
intx    3      [ ]          STREAM    CONNECTED       4049
intx    3      [ ]          STREAM    CONNECTED       35254
intx    3      [ ]          STREAM    CONNECTED       32273  /run/user/1000/bus
intx    3      [ ]          STREAM    CONNECTED       2048  /run/systemd/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       40372  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       35024  /run/user/1000/bus
intx    3      [ ]          STREAM    CONNECTED       25225  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       35299  /run/user/1000/bus
intx    3      [ ]          STREAM    CONNECTED       30034  @/tmp/dbus-efH1QqRt
intx    3      [ ]          STREAM    CONNECTED       32272  /run/user/1000/bus
intx    3      [ ]          STREAM    CONNECTED       2048  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       41026
intx    3      [ ]          STREAM    CONNECTED       40371
intx    3      [ ]          STREAM    CONNECTED       35977
intx    3      [ ]          STREAM    CONNECTED       15524
intx    3      [ ]          STREAM    CONNECTED       102329  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       35299  /run/user/1000/bus
intx    3      [ ]          STREAM    CONNECTED       25225  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       26109
intx    3      [ ]          STREAM    CONNECTED       40875
intx    3      [ ]          STREAM    CONNECTED       2048  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       35059
intx    3      [ ]          STREAM    CONNECTED       35411
intx    3      [ ]          STREAM    CONNECTED       32284
intx    3      [ ]          STREAM    CONNECTED       26990
intx    3      [ ]          STREAM    CONNECTED       115451  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       26568
intx    3      [ ]          STREAM    CONNECTED       35060
intx    3      [ ]          STREAM    CONNECTED       35274  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       40481  @/tmp/.X11-unix/X0
intx    3      [ ]          STREAM    CONNECTED       35409
intx    3      [ ]          STREAM    CONNECTED       34659  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       26434
intx    3      [ ]          STREAM    CONNECTED       115450
intx    3      [ ]          STREAM    CONNECTED       10944  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       45064  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       25361
intx    3      [ ]          STREAM    CONNECTED       40480
intx    3      [ ]          STREAM    CONNECTED       35272  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       32276
intx    3      [ ]          STREAM    CONNECTED       26999  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       40481  /run/systemd/journal/stdout
intx    3      [ ]          STREAM    CONNECTED       37799  @/dbus-vfs-daemon/socket-MLGvagTX
intx    3      [ ]          STREAM    CONNECTED       31555
intx    3      [ ]          STREAM    CONNECTED       35078  @/tmp/dbus-50jh2ulkof
intx    3      [ ]          STREAM    CONNECTED       35252  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       35253
intx    2      [ ]          DGRAM     CONNECTED       32531
intx    3      [ ]          STREAM    CONNECTED       2048  /run/dbus/system_bus_socket
intx    3      [ ]          STREAM    CONNECTED       115463
intx    3      [ ]          STREAM    CONNECTED       102947
```

-a flag for all listening and non listening sockets.

```
Indrajith@indrajithb180486cs:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp   0      0 localhost:domain          0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:ssh              0.0.0.0:*               LISTEN
tcp   0      0 localhost:ipp             0.0.0.0:*               LISTEN
tcp   0      0 indrajithb180486c:48076 239.237.117.34.bc:https ESTABLISHED
tcp   0      0 indrajithb180486c:50424  ec2-35-163-208-27:https ESTABLISHED
tcp   0      0 indrajithb180486c:52264  102.115.120.34.bc:https ESTABLISHED
tcp6  0      0 [::]:http                [::]:*                  LISTEN
tcp6  0      0 [::]:ftp                 [::]:*                  LISTEN
tcp6  0      0 [::]:ssh                 [::]:*                  LISTEN
tcp6  0      0 [::]:ip6-localhost:ipp  [::]:*                  LISTEN
udp   0      0 0.0.0.0:631              0.0.0.0:*
udp   0      0 localhost:domain          0.0.0.0:*
udp   0      0 indrajithb180486:bootpc _gateway:bootps            ESTABLISHED
udp   0      0 0.0.0.0:45628             0.0.0.0:*
udp6  0      0 [::]:mdns                [::]:*                  *
udp6  0      0 [::]:39367               [::]:*                  *
raw6 0      0 [::]:ipv6-lcmpl          [::]:*                  7

Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type    State      I-Node Path
unix  2      [ ACC ] STREAM LISTENING  25398 @/tmp/dbus-FQWeXUL0
unix  2      [ ACC ] DGRAM  LISTENING  31514 /run/user/1000/systemd/notify
unix  2      [ ACC ] STREAM LISTENING  31557 /run/user/1000/systemd/private
unix  2      [ ACC ] STREAM LISTENING  31594 /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ] STREAM LISTENING  31595 /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ] STREAM LISTENING  31596 /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ] STREAM LISTENING  31597 /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ] STREAM LISTENING  31598 /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ] STREAM LISTENING  31599 /run/user/1000/pk-debconf-socket
unix  2      [ ACC ] STREAM LISTENING  34663 @/tmp/.ICE-unix/1491
unix  2      [ ACC ] STREAM LISTENING  31669 /run/user/1000/pulse/native
unix  2      [ ACC ] STREAM LISTENING  32601 @/run/user/1000/gpd-session-agent.socket
unix  2      [ ACC ] STREAM LISTENING  32646 @/tmp/.X11-unix/X0
unix  2      [ ACC ] STREAM LISTENING  31972 /run/user/1000/keyring/control
unix  2      [ ACC ] STREAM LISTENING  146583 /run/systemd/private
unix  2      [ ACC ] STREAM LISTENING  146592 /run/systemd/userdb/lo.systemd.DynamicUser
unix  2      [ ACC ] STREAM LISTENING  36037 /run/systemd/userdb/lo/systemd/pcss1
unix  2      [ ACC ] STREAM LISTENING  102155 /run/cups/cups.sock
unix  2      [ ACC ] STREAM LISTENING  34776 /run/user/1000/keyring ssh
unix  2      [ ACC ] STREAM LISTENING  21169 /run/acpid.socket
unix  2      [ ACC ] STREAM LISTENING  147378 /run/systemd/journal/to.systemd.journal
unix  2      [ ACC ] STREAM LISTENING  21179 /run/avahi-daemon/socket
unix  2      [ ACC ] STREAM LISTENING  23041 @/run/systemd/ibus/bus_socket
unix  2      [ ACC ] STREAM LISTENING  21203 /run/snapd.socket
unix  2      [ ACC ] STREAM LISTENING  21205 /run/snapd-snap.socket
unix  2      [ ACC ] STREAM LISTENING  21207 /run/uuid/request
unix  2      [ ACC ] STREAM LISTENING  32384 @/tmp/dbus-WV06JXyo
unix  2      [ ACC ] STREAM LISTENING  67095 @/run/systemd/journal/_journal.sock
unix  2      [ ACC ] STREAM LISTENING  105786 @/tmp/.ICE-unix/1491
unix  4      [ ]  DGRAM  LISTENING  15526 /run/systemd/notify
unix  2      [ ]  DGRAM  15540 /run/systemd/journal/syslog
unix  2      [ ]  DGRAM  LISTENING  15542 /run/systemd/fsck.progress
unix  17     [ ]  DGRAM  LISTENING  15550 /run/systemd/journal/dev-log
unix  2      [ ACC ] STREAM LISTENING  15552 /run/systemd/journal/stdout
unix  8      [ ]  DGRAM  LISTENING  15554 /run/udev/control
unix  2      [ ACC ] SEPACKET  LISTENING  15556 @/tmp/dbus-S0Jh2ulkof
unix  2      [ ACC ] STREAM LISTENING  34231 @/tmp/dbus-ZVpyg93X
unix  2      [ ACC ] STREAM LISTENING  32383 @/tmp/dbus-W96TJPLU
unix  2      [ ACC ] STREAM LISTENING  88858 @/tmp/.ICE-unix/1491
unix  2      [ ACC ] STREAM LISTENING  33047 @/tmp/.ICE-unix/1491
unix  2      [ ACC ] STREAM LISTENING  35007 @/home/Indrajith/.cache/ibus/dbus-5C2CR815
unix  2      [ ACC ] STREAM LISTENING  34119 @/tmp/ssh-KRpWAYTLBctj/agent.1374
unix  2      [ ACC ] STREAM LISTENING  34664 @/tmp/.ICE-unix/1491
unix  2      [ ACC ] STREAM LISTENING  25399 @/tmp/dbus-eFH1QaRT
unix  2      [ ACC ] STREAM LISTENING  76702 @/tmp/.ICE-unix/1491
unix  2      [ ACC ] STREAM LISTENING  104381 @/tmp/.ICE-unix/1491
unix  3      [ ]  STREAM CONNECTED  35039 @/tmp/.ICE-unix/1491
unix  3      [ ]  STREAM CONNECTED  162324 @/tmp/.ICE-unix/1491
unix  3      [ ]  STREAM CONNECTED  35298 @/tmp/.ICE-unix/1491
```

-at for all tcp and -au for udp etc.

```
Indrajith@indrajithb180486cs:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp   0      0 localhost:domain          0.0.0.0:*               LISTEN
tcp   0      0 0.0.0.0:ssh              0.0.0.0:*               LISTEN
tcp   0      0 localhost:ipp             0.0.0.0:*               LISTEN
tcp   0      0 indrajithb180486c:48076  239.237.117.34.bc:https ESTABLISHED
tcp   0      0 indrajithb180486c:50424  ec2-35-163-208-27:https ESTABLISHED
tcp   0      0 indrajithb180486c:52264  102.115.120.34.bc:https ESTABLISHED
tcp6  0      0 [::]:http                [::]:*                  LISTEN
tcp6  0      0 [::]:ftp                 [::]:*                  LISTEN
tcp6  0      0 [::]:ssh                 [::]:*                  LISTEN
tcp6  0      0 ip6-localhost:ipp        [::]:*                  LISTEN
Indrajith@indrajithb180486cs:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp   0      0 0.0.0.0:631              0.0.0.0:*
udp   0      0 0.0.0.0:mdns             0.0.0.0:*
udp   0      0 localhost:domain          0.0.0.0:*
udp   0      0 indrajithb180486:bootpc _gateway:bootps            ESTABLISHED
udp   0      0 0.0.0.0:45628             0.0.0.0:*
udp6  0      0 [::]:mdns                [::]:*                  *
udp6  0      0 [::]:39367               [::]:*                  *

Indrajith@indrajithb180486cs:~$
```

-s for statistics of all ports.

```
indrajith@indrajithb180486cs:~$ netstat -s
Indrajith@indrajithb180486cs:~
```

Ip:

```
Forwarding: 2
153906 total packets received
24 with invalid addresses
0 forwarded
0 incoming packets discarded
153879 incoming packets delivered
117052 requests sent out
20 outgoing packets dropped
169 dropped because of missing route
```

Icmp:

```
3105 ICMP messages received
327 input ICMP message failed
ICMP input histogram:
    destination unreachable: 3014
    timeout in transit: 32
    echo replies: 59
1551 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
    destination unreachable: 1375
    echo requests: 176
```

IcmpMsg:

```
InType0: 59
InType3: 3014
InType11: 32
OutType3: 1375
OutType8: 176
```

Tcp:

```
1490 active connection openings
0 passive connection openings
778 failed connection attempts
9 connection resets received
1 connections established
142167 segments received
104187 segments sent out
420 segments retransmitted
0 bad segments received
406 resets sent
```

Udp:

```
8287 packets received
318 packets to unknown port received
0 packet receive errors
11214 packets sent
0 receive buffer errors
0 send buffer errors
IgnoredMulti: 8
```

UdpExt:

```
197 TCP sockets finished time wait in fast timer
3746 delayed acks sent
130178 packet headers predicted
1234 acknowledgments not containing data payload received
2108 predicted acknowledgments
TCPLostRetransmit: 93
TCPTimeouts: 875
1 connections reset due to early user close
2 connections aborted due to timeout
TCPRecvCoalesce: 231
TCPFastOpenActiveFail: 226
TCPSpuriousRtxHostQueues: 455
TCPAutoCorking: 27
TCPSynRetrans: 420
TCPOrtgdataSent: 2754
TCPHystartTrainDetect: 3
TCPHystartTrainCwnd: 106
TCPWinProbe: 1
TCPKeepAlive: 595
TCPDelivered: 3126
TcptTimeoutRehash: 875
```

IpExt:

```
InMcastPkts: 161
```

## 9. Dstat

It is the tool used for generating system resource statistics.

```
indrajith@indrajithb180486cs:~$ dstat
You did not select any stats, using -cdnny by default.
--total-cpu-usage-- -dsk/total- -net/total- ---paging--- ---system---
usr sys idl wai stl| read  writ| recv  send| in    out| int   csw
 6  1  91  2  0| 66k  333k|     0  0| 38  105B| 507  446
 2  0  98  0  0|     0  0|     0  0| 0  0| 471  158
 1  0  99  0  0|     0  0|     0  0| 0  0| 561  124
 3  0  87  10  0|     0 100k|     0  0| 0  0| 457  185
 4  0  96  0  0|     0  0|     0  0| 0  0| 426  146
 1  1  98  0  0|     0 16k|     0  0| 0  0| 484  176
 3  0  97  0  0|     0  0|     0  0| 0  0| 452  144
 2  0  98  0  0|     0  0|     0  0| 0  0| 523  184
 2  0  98  0  0|     0  0|     0  0| 0  0| 511  444
17  2  72  9  0| 16k  44k|     0 216B| 0  0| 798 3571
57  6  28  9  0| 384k 36k| 14k 7368B| 0  0| 895 6959
71  7  22  0  0|     0  0|     0  0| 0  0| 715 8166
46  4  43  7  0| 36k 300k| 1414B 2848B| 0  0| 777 5451
66  6  6  22  0| 4344k 0| 68k 4613B| 0  0| 928 7559
66  7  0  27  0| 23M  0| 0  0| 0  0| 897 3530
80  2  0  18  0| 24M  0| 0  0| 0  0| 825 2193
96  0  0  4  0| 1036k  0| 0  0| 0  0| 571 2547
66  6  11  16  0| 2104k 396k| 3125B 521B| 0  0| 727 7392
35  5  60  0  0| 0  0| 0  0| 0  0| 727 5144
80  8  10  1  0| 8192B 80k| 34k 5744B| 0  0| 731 8217
74  5  21  0  0| 0 192k| 974B 1838B| 0  0| 755 6137
62 11  26  0  0| 4096B  0| 57k 2662B| 0  0| 784 6814
36  4  48  11  0| 352k 620k| 29k 8099B| 0  0| 901 4031
43  6  42  8  0| 408k 132k| 2072B 2141B| 0  0| 743 4263
14  6  67  13  0| 568k 2124k| 223B 100B| 0  0| 1032 3169
 2  1  97  0  0| 0  0| 0  0| 0  0| 557  592
 2  0  98  0  0| 0  0| 0  0| 0  0| 436  160
 4  0  96  0  0| 0  0| 0  0| 0  0| 501  249 ^C
indrajith@indrajithb180486cs:~$
```

-c flag is for cpu stats and -d for disk stats and also we can choose the top processes in cpu using –top-cpu flag

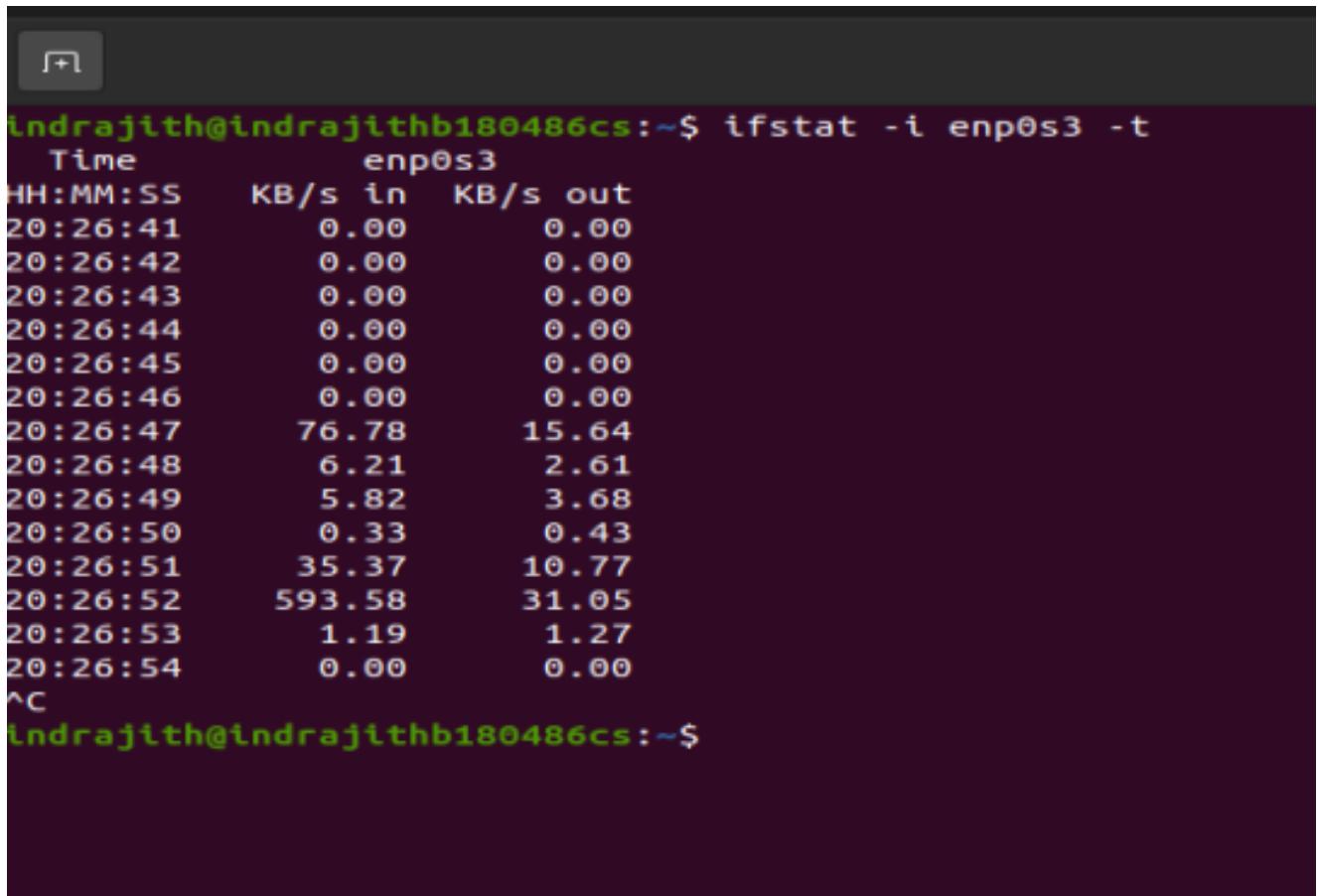
```
Indrajith@indrajithb180486cs:~$ dstat -c --top-cpu -d
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour of importlib;
import imp
--total-cpu-usage-- -most-expensive- -dsk/total-
usr sys idl wai stl|__cpu_process__| read writ
 6  1  91  2  0|gnome-shell  0.8| 68k  331k
 2  0  98  0  0|gnome-shell  1.0| 0   0
 3  0  97  0  0|gnome-shell  1.0| 0   0
 6  1  93  0  0|gnome-shell  2.0| 0   0
 2  0  98  0  0|accounts-daem 2.0| 0   0
 3  0  88  9  0|gnome-terminal 1.0| 0   16k
 3  1  96  0  0|gnome-shell  2.0| 0   0
 2  0  98  0  0|gnome-shell  1.0| 0   0
 2  2  96  0  0|gnome-terminal 1.0| 0   0
15 0  85  0  0|gnome-shell  12| 0   0
69 9  0  22  0|GeckoMain    31| 7856k  276k
64 9  0  27  0|GeckoMain    56| 1412k  440k
51 2  0  47  0|GeckoMain    36| 156k  0
71 10 0  18  0|GeckoMain    59| 1588k  336k
88 10 0  2  0|GeckoMain    48| 3632k  296k
88 12 0  0  0|GeckoMain    54| 124k  152k
88 12 0  0  0|GeckoMain    72| 40k  0
95 5  0  0  0|GeckoMain    58| 24k  204k
93 7  0  0  0|GeckoMain    65| 12k  204k
81 14 2  3  0|GeckoMain    62| 4096B  2936k
13 3  82  1  0|GeckoMain    11| 4096B  544k
21 1  78  0  0|GeckoMain    17| 0   0
53 6  34  7  0|GeckoMain    31| 0   84k
70 3  6  21  0|GeckoMain    39| 0   684k
58 6  35  0  0|GeckoMain    38| 0   12k
64 9  27  0  0|GeckoMain    43| 0   0
53 5  41  0  0|GeckoMain    21| 0   0
44 4  52  0  0|GeckoMain    18| 0   0
86 9  5  0  0|GeckoMain    46| 1812k  1688k
75 14 0  11  0|We          30| 2536k  264k
65 8  27  0  0|GeckoMain    30| 1128k  0
34 2  64  0  0|gnome-shell  18| 0   0
 5 0  95  0  0|Privilege   2.0| 0   0
 6 2  92  0  0|Privilege   1.0| 0   0 ^C
Indrajith@indrajithb180486cs:~$
```

## 10. ifstat

ifstat command monitors non-loop network interfaces that are active. Flag -a is used to enable monitoring for all the interfaces.

```
indrajith@indrajithb180486cs:~$ ifstat -a
      lo          enp0s3
KB/s in KB/s out   KB/s in KB/s out
 0.00    0.00    0.00    0.00
 0.00    0.00    0.00    0.00
 0.00    0.00    0.00    0.00
 0.74    0.74    0.64    3.04
 5.54    5.54   76.13   12.21
 0.58    0.58    6.99    2.58
 3.86    3.86   14.66    5.01
 2.21    2.21   295.31   19.00
 0.00    0.00   525.79   22.95
 1.72    1.72    9.11    3.69
 2.38    2.38   43.89   14.75
 1.19    1.19   434.69   18.68
 6.68    6.68   63.74   22.18
 1.20    1.20   58.49   29.55
12.11   12.11   55.50   16.18
 3.08    3.08   188.89   16.17
 2.87    2.87   49.87  105.96
 2.09    2.09   70.78   27.80
^C
indrajith@indrajithb180486cs:~$
```

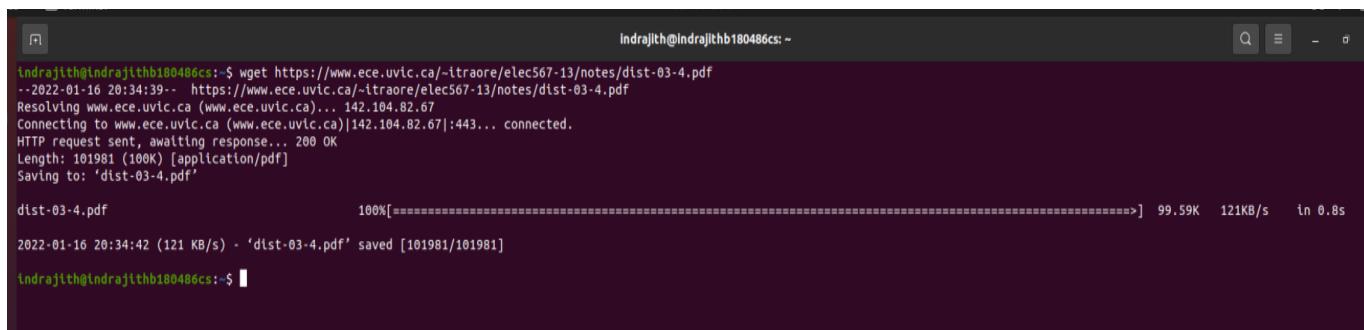
-i interface name is used to enable monitoring on a specific interface.  
-t to average over each second.



```
indrajith@indrajithb180486cs:~$ ifstat -i enp0s3 -t
      Time          enp0s3
HH:MM:SS    KB/s  in   KB/s  out
20:26:41      0.00  0.00
20:26:42      0.00  0.00
20:26:43      0.00  0.00
20:26:44      0.00  0.00
20:26:45      0.00  0.00
20:26:46      0.00  0.00
20:26:47     76.78 15.64
20:26:48      6.21  2.61
20:26:49      5.82  3.68
20:26:50      0.33  0.43
20:26:51     35.37 10.77
20:26:52    593.58 31.05
20:26:53      1.19  1.27
20:26:54      0.00  0.00
^C
indrajith@indrajithb180486cs:~$
```

## 11. wget

wget command is used to download files from the internet without the use of an interactive gui. We specify the url of the file to download.



```
indrajith@indrajithb180486cs:~$ wget https://www.ece.uvic.ca/~itraore/elec567-13/notes/dist-03-4.pdf
--2022-01-16 20:34:39-- https://www.ece.uvic.ca/~itraore/elec567-13/notes/dist-03-4.pdf
Resolving www.ece.uvic.ca (www.ece.uvic.ca)... 142.104.82.67
Connecting to www.ece.uvic.ca (www.ece.uvic.ca)|142.104.82.67|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 101981 (100K) [application/pdf]
Saving to: 'dist-03-4.pdf'

dist-03-4.pdf          100%[=====] 99.59K  121KB/s  in 0.8s

2022-01-16 20:34:42 (121 KB/s) - 'dist-03-4.pdf' saved [101981/101981]

indrajith@indrajithb180486cs:~$
```

We can add multiple file links to a txt file and then use the -i filename to download multiple files that is given in the txt file.

-nv flag can be used to turn off the verbose output when we need to see only the summary.

```
indrajith@indrajithb180486cs:~$ wget -nv -i links.txt
2022-01-16 20:36:50 URL:https://www.ece.uvic.ca/~itraore/elec567-13/notes/dist-03-4.pdf [101981/101981] -> "dist-03-4.pdf.1" [1]
2022-01-16 20:36:56 URL:http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf [7511126/7511126] -> "ComputerNetworks.pdf" [1]
FINISHED --2022-01-16 20:36:56--
Total wall clock time: 7.7s
Downloaded: 2 files, 7.3M in 5.6s (1.30 MB/s)
indrajith@indrajithb180486cs:~$
```

## 12. tracepath

This traces the path to the destination ip. This is similar to traceroute but with lesser options thus dont need sudo permission.

-m flag can be used to decide the maximum number of hops.

```
indrajith@indrajithb180486cs:~$ tracepath -m 5 www.google.com
1?: [LOCALHOST]                                pmtu 1500
1: _gateway                                     0.324ms
1: _gateway                                     0.265ms
2: no reply
3: no reply
4: no reply
5: no reply
      Too many hops: pmtu 1500
      Resume: pmtu 1500
indrajith@indrajithb180486cs:~$
```