

# NETWORKS LAB EXPERIMENT – 1

YACHA VENKATA RAKESH

B180427CS

The screenshot shows two terminal windows side-by-side. Both windows have the title 'Terminal' and are running on a system with the user 'yachavenkatrakesh@pop-os'. The left terminal shows the output of a ping command to 'www.wikipedia.com'. It displays statistics for 4 packets transmitted, 4 received, 0% packet loss, and a round-trip time of 3003ms. The right terminal shows the output of a ping command to 'www.youtube.com'. It displays statistics for 6 packets transmitted, 6 received, 0% packet loss, and a round-trip time of 7055ms. Both terminals also show other network-related commands like 'ping -c 6 www.youtube.com' and 'ping -i 0.5 www.yahoo.com'.

```
yachavenkatrakesh@pop-os:~$ ping www.wikipedia.com
PING ncredir-lb.wikimedia.org (103.102.166.226) 56(84) bytes of data.
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=1 ttl=128 time=37.0 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=2 ttl=128 time=37.2 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=3 ttl=128 time=37.4 ms
64 bytes from ncredir-lb.eqsin.wikimedia.org (103.102.166.226): icmp_seq=4 ttl=128 time=36.8 ms
^C
--- ncredir-lb.wikimedia.org ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 36.802/37.099/37.370/0.220 ms
yachavenkatrakesh@pop-os:~$ 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=128 time=4.67 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=4.15 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=4.48 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=4.08 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=128 time=4.33 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 4.078/4.342/4.672/0.216 ms
yachavenkatrakesh@pop-os:~$ ping localhost
PING localhost(localhost (::1)) 56 data bytes
64 bytes from localhost (::1): icmp_seq=1 ttl=64 time=0.029 ms
64 bytes from localhost (::1): icmp_seq=2 ttl=64 time=0.041 ms
64 bytes from localhost (::1): icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from localhost (::1): icmp_seq=4 ttl=64 time=0.024 ms
64 bytes from localhost (::1): icmp_seq=5 ttl=64 time=0.040 ms
^C
--- localhost ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4073ms
rtt min/avg/max/mdev = 0.024/0.031/0.041/0.007 ms
yachavenkatrakesh@pop-os:~$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.024 ms
^C
--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2040ms
rtt min/avg/max/mdev = 0.024/0.029/0.037/0.005 ms
yachavenkatrakesh@pop-os:~$ ping 0
PING 0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.023 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.023 ms
^C
--- 0 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2048ms
rtt min/avg/max/mdev = 0.023/0.024/0.028/0.002 ms
yachavenkatrakesh@pop-os:~$ ping -c 6 www.youtube.com
PING youtube-ui.l.google.com (172.217.194.93) 56(84) bytes of data.
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=1 ttl=128 time=36.3 ms
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=2 ttl=128 time=36.1 ms
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=3 ttl=128 time=36.2 ms
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=4 ttl=128 time=36.3 ms
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=5 ttl=128 time=36.3 ms
64 bytes from 172.217.194.93 (172.217.194.93): icmp_seq=6 ttl=128 time=35.9 ms
^C
--- youtube-ui.l.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 7055ms
rtt min/avg/max/mdev = 36.892/36.170/36.315/0.150 ms
yachavenkatrakesh@pop-os:~$ ping -i 0.5 www.yahoo.com
PING new-fp-shed.wgt.b.yahoo.com (202.165.107.50) 56(84) bytes of data.
64 bytes from www.yahoo.com (202.165.107.50): icmp_seq=1 ttl=128 time=37.0 ms
64 bytes from www.yahoo.com (202.165.107.50): icmp_seq=2 ttl=128 time=36.8 ms
64 bytes from www.yahoo.com (202.165.107.50): icmp_seq=3 ttl=128 time=36.5 ms
64 bytes from www.yahoo.com (202.165.107.50): icmp_seq=4 ttl=128 time=36.4 ms
64 bytes from www.yahoo.com (202.165.107.50): icmp_seq=5 ttl=128 time=36.4 ms
^C
--- new-fp-shed.wgt.b.yahoo.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 36.356/36.603/37.012/0.253 ms
yachavenkatrakesh@pop-os:~$ ping -f -i 0.2 www.google.com
PING www.google.com (74.125.68.105) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 2611ms
rtt min/avg/max/mdev = 35.983/36.225/36.383/0.118 ms, ipg/ewma 200.880/36.262 ms
yachavenkatrakesh@pop-os:~$ ping -c 10 -q www.google.com
PING www.google.com (74.125.68.99) 56(84) bytes of data.
^C
--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 35.524/35.984/36.920/0.424 ms
yachavenkatrakesh@pop-os:~$ ping -c 20 www.youtube.com > ping.txt
yachavenkatrakesh@pop-os:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
yachavenkatrakesh@pop-os:~$ ping -6 www.wikipedia.com
ping: connect: Network is unreachable
yachavenkatrakesh@pop-os:~$ ping -D apple.com
PING apple.com (17.253.144.10) 56(84) bytes of data.
[1611510907.829335] 64 bytes from apple.com (17.253.144.10): icmp_seq=1 ttl=128 time=37.3 ms
^C
--- apple.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 37.283/37.283/37.283/0.000 ms
yachavenkatrakesh@pop-os:~$ ping -V www.google.com
ping from iputils s20700821
yachavenkatrakesh@pop-os:~$
```

## PING COMMAND

Ping command is a simple tool that can be used in troubleshooting network issues either connected to Local Area Network or the Internet and also test for network delay and packet losses or to test DNS issues such as name resolution. It works on network layer.

ICMP (Internet Control Message Protocol) echo request and the ICMP echo reply messages are commonly known as ping messages.

We can ping an IP address or domain name of a host. This host could be any network device such as computer, server, router or printer, whether its on local area network or in the internet. In terminal when we type ping [www.wikipedia.com](http://www.wikipedia.com) then domain name is sent to the dns server which maps this to the IP address of the server of that domain and send data packets to that server and then our computer wait for a response. Then the server will send the data packets back to us as a reply and these replies are called echo reply request and these replies inform you about what's happening with server we pinged.

If we received a reply then that means there is network connectivity between us and server. When we ping a server and get a message “request timed out” then that could mean that either server is powered down or server is up and running but it’s using a firewall that’s blocking all ping requests. When we ping a server and get a message “destination host unreachable” route to that destination can’t be found. That is the router

doesn't have information on how to route data to the destination or it could also mean remote server is down or disconnected to network or it could also mean that our system is not connected to the network.

### To test if network interface card is working

```
$ ping localhost or $ping 127.0.0.1
```

This is called a loopback test(will send out signals back to your system for testing)

### To test DNS name resolution issues

```
$ ping domainname
```

And if we get "ping request could not find host domain name. Please check and try again" could be because of DNS name resolution issues.

### Some other ping commands:

#### 1. \$ping Domainname or \$ping IPaddress

**from :** The destination domain name and it's ip address

IP address of the destination website might change based on our geographical location.

**icmp\_seq:** The sequence number of each ICMP packet. Increases for every subsequent echo request. It is also called as hop

**ttl :** The time to live value from 1 to 255. It can represents number of network hops a packet can take before router discards it.

A hop is occurred when a packet is passed from one network segment to another.

**time:** The time it took a packet to reach the destination and come back to source. It is expressed in milliseconds.

#### 2. \$ping -i 0.5 [www.wikipedia.com](http://www.wikipedia.com)

To increase time between two packets keep a number > 1

Else keep a number < 1 (minimum 0.2)

#### 3. \$ping -s 1000 [www.wikipedia.com](http://www.wikipedia.com)

To change packet size which is 64 bytes by default.

#### 4.\$ping -f -i 0.2 [www.wikipedia.com](http://www.wikipedia.com)

This prints '\_' for every sent packet and backspace for every received packets

#### 5.\$ping -c 10 -q [www.wikipedia.com](http://www.wikipedia.com)

This print only summary statistics without complete details

#### 6.\$ping -c 20 [www.wikipedia.com](http://www.wikipedia.com) > ping.txt

This saves the details of the ping data received into ping.txt file

#### 7.\$ping -v [www.wikipedia.com](http://www.wikipedia.com)

To display the version of this ping utility

```
Activities Terminal Jan 24 11:51 PM
yachavenkatarakesh@pop-os:~$ traceroute www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  1.040 ms  0.967 ms  0.912 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  * * *

yachavenkatarakesh@pop-os:~$ traceroute -I www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  0.830 ms  0.776 ms  0.735 ms
 2  dlinkrouter (192.168.0.1)  1.433 ms  1.960 ms  1.901 ms
 3  dns118.excellrbroadband.com (172.16.118.1)  2.782 ms  2.989 ms  2.948 ms
 4  175.101.137.1 (175.101.137.1)  6.218 ms  6.153 ms  6.300 ms
 5  125.21.210.73 (125.21.210.73)  6.450 ms  6.419 ms  6.340 ms
 6  182.79.141.36 (182.79.141.36)  6.755 ms  5.313 ms  5.233 ms
 7  182.79.161.171 (182.79.161.171)  7.249 ms  5.762 ms  6.237 ms
 8  162.158.53.22 (162.158.53.22)  5.601 ms  162.158.53.20 (162.158.53.20)  5.562 ms  162.158.53.3
 9  162.158.53.30 (162.158.53.30)  5.890 ms  162.158.53.39 (162.158.53.39)  5.866 ms  162.158.53.2
10  * * *
11  www.wikipedia.com (103.102.166.226)  38.646 ms  38.617 ms  37.834 ms

yachavenkatarakesh@pop-os:~$ traceroute -m 10 www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 10 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  1.047 ms  0.954 ms  0.909 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *

yachavenkatarakesh@pop-os:~$ traceroute -f 24 www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 24  * * *
 25  * * *
 26  * * *
 27  * * *
 28  * * *
 29  * * *
 30  * * *

yachavenkatarakesh@pop-os:~$ traceroute -I -n www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1  192.168.136.2  1.602 ms  1.573 ms  1.531 ms
 2  192.168.0.1  4.243 ms  4.189 ms  3.969 ms
 3  172.16.118.1  4.073 ms  4.734 ms  5.219 ms
 4  175.101.137.1  7.002 ms  6.952 ms  7.245 ms
 5  125.21.210.73  8.679 ms  22.639 ms  22.562 ms
 6  182.79.141.36  22.363 ms  21.068 ms  20.712 ms
 7  182.79.161.171  20.434 ms  19.707 ms  19.601 ms
 8  162.158.53.44  19.365 ms  162.158.53.39  19.281 ms  162.158.53.10  18.782 ms
 9  162.158.53.26  18.176 ms  162.158.53.5  20.886 ms  162.158.53.12  20.769 ms
10  * * *
11  103.102.166.226  36.896 ms  37.098 ms  37.070 ms

yachavenkatarakesh@pop-os:~$ traceroute -I -q 2 www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  0.774 ms  0.672 ms
 2  dlinkrouter (192.168.0.1)  1.560 ms  1.482 ms
 3  dns118.excellrbroadband.com (172.16.118.1)  2.162 ms  2.931 ms
 4  175.101.137.1 (175.101.137.1)  3.447 ms  4.279 ms
 5  125.21.210.73 (125.21.210.73)  5.248 ms  5.496 ms
 6  182.79.141.36 (182.79.141.36)  6.258 ms  6.266 ms
 7  182.79.161.171 (182.79.161.171)  28.945 ms  28.878 ms
 8  162.158.53.33 (162.158.53.33)  6.453 ms  162.158.53.37 (162.158.53.37)  6.406 ms
 9  162.158.53.37 (162.158.53.37)  4.995 ms  162.158.53.45 (162.158.53.45)  4.968 ms
10  * *
11  www.wikipedia.com (103.102.166.226)  38.036 ms  39.068 ms
```

## Traceroute

Traceroute is a command line utility that is used to show the exact route that is taken by the data packets as they travel across the internet to their destination. This tool is used to find problems like bottlenecks, such as why and where a connection to a server might be lagging.

Traceroute not only pings the final destination, but it also pings each router on its way to the destination and measures the round trip time that the data packets took from each router and destination. Note that this shows route from source server or device to the destination server.

Each time three data packets are sent to each router on its way to the destination. This is just to ensure that if in case something strange happened resulting in a high round trip time for a packet but low round trip time for the other two packets.

First column shows number of hops or steps route took. Next three columns tells the round trip time each data packet took to each point and back to your computer. The last column shows IP address and also the domain name if its available.

Using traceroute we can know whether the problem is with LAN or server. High round trip time doesn't always mean there's a problem with router, it could just mean distance between certain routers are thousands of miles apart. Stars in between indicate that the router wasn't configured to return traceroute replies but still passed on data packets to next router.

**TTL** : It is a given value of maximum number of hops they can take before getting discarded.

By default it says over a maximum of 30 hops. So if datapackets don't reach destination after 30 hops, data packets are dropped. The reason for keeping a limit is to prevent data packets from travelling endlessly around internet trying to figure out its destination. This could happen, if certain routers in internet are misconfigured and the data packets could be caught in an endless loop.

In windows it is tracert not traceroute.

```

Activities Terminal - yachavenkatarakesh@pop-os:~ Jan 24 11:59 PM
yachavenkatarakesh@pop-os:~$ traceroute www.wikipedia.com 1000
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 1000 byte packets
 1  192.168.136.2 (192.168.136.2)  1.321 ms  1.287 ms  1.170 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  * * *

yachavenkatarakesh@pop-os:~$ traceroute -I www.wikipedia.com 1000
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 1000 byte packets
 1  192.168.136.2 (192.168.136.2)  0.801 ms  0.720 ms  0.687 ms
 2  dlinkrouter (192.168.0.1)  1.732 ms  1.946 ms  1.902 ms
 3  dns118.excelbroadband.com (172.16.118.1)  2.835 ms  3.548 ms  3.524 ms
 4  175.101.137.1 (175.101.137.1)  5.764 ms  5.741 ms  5.696 ms
 5  125.21.210.73 (125.21.210.73)  6.758 ms  6.924 ms  7.457 ms
 6  182.79.141.36 (182.79.141.36)  7.647 ms  5.319 ms  5.264 ms
 7  182.79.161.171 (182.79.161.171)  6.899 ms  7.542 ms  7.476 ms
 8  162.158.53.37 (162.158.53.37)  7.433 ms  7.366 ms  162.158.53.11 (162.158.53.11)  7.316 ms
 9  162.158.53.26 (162.158.53.26)  7.316 ms  162.158.53.36 (162.158.53.36)  7.278 ms  162.158.53.3
4 (162.158.53.34)  7.390 ms
10  * * *
11  www.wikipedia.com (103.102.166.226)  40.166 ms  40.211 ms  38.379 ms
yachavenkatarakesh@pop-os:~$ [REDACTED]
yachavenkatarakesh@pop-os:~$ traceroute -I -g www.google.com www.wikipedia.com
traceroute to www.wikipedia.com (103.102.166.226), 30 hops max, 72 byte packets
 1  192.168.136.2 (192.168.136.2)  0.601 ms  0.513 ms  0.488 ms
 2  dlinkrouter (192.168.0.1)  4.116 ms  4.396 ms  4.555 ms
 3  dns118.excelbroadband.com (172.16.118.1)  5.564 ms  5.505 ms  5.463 ms
 4  175.101.137.1 (175.101.137.1)  5.942 ms  5.908 ms  6.105 ms
 5  175.101.138.254 (175.101.138.254)  7.390 ms  7.348 ms  7.570 ms
 6  72.14.220.218 (72.14.220.218)  17.467 ms  5.278 ms  5.213 ms
 7  108.170.253.104 (108.170.253.104)  5.188 ms  5.726 ms  5.602 ms
 8  72.14.239.151 (72.14.239.151)  38.199 ms  38.162 ms  38.111 ms
 9  209.85.245.232 (209.85.245.232)  36.767 ms  36.725 ms  36.684 ms
10  108.170.233.49 (108.170.233.49)  41.568 ms  44.245 ms  44.208 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  sc-in-f106.1e100.net (74.125.68.106)  36.095 ms  36.068 ms  35.747 ms
yachavenkatarakesh@pop-os:~$ traceroute -I -F google.com
traceroute to google.com (74.125.24.138), 30 hops max, 60 byte packets
 1  192.168.136.2 (192.168.136.2)  0.557 ms  0.499 ms  0.460 ms
 2  dlinkrouter (192.168.0.1)  3.135 ms  3.833 ms  3.965 ms
 3  dns118.excelbroadband.com (172.16.118.1)  4.705 ms  4.681 ms  4.664 ms
 4  175.101.137.1 (175.101.137.1)  5.627 ms  5.600 ms  5.791 ms
 5  175.101.138.254 (175.101.138.254)  6.905 ms  6.870 ms  7.282 ms
 6  72.14.220.218 (72.14.220.218)  8.683 ms  3.874 ms  3.814 ms
 7  108.170.253.104 (108.170.253.104)  6.713 ms  5.624 ms  5.566 ms
 8  72.14.239.151 (72.14.239.151)  38.959 ms  38.925 ms  38.965 ms
 9  209.85.245.232 (209.85.245.232)  36.857 ms  36.832 ms  37.035 ms
10  172.253.68.247 (172.253.68.247)  37.476 ms  37.420 ms  37.485 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  74.125.24.138 (74.125.24.138)  36.653 ms  36.610 ms  36.583 ms
yachavenkatarakesh@pop-os:~$ [REDACTED]

```

## Traceroute

### Traceroute commands:

#### 1. traceroute domainname or IP address

Prints all the path travelled by the data packets to reach the given destination

#### 2. traceroute -m 40 [www.wikipedia.com](http://www.wikipedia.com)

Limits traceroute to 40 hops

#### 3. \$traceroute -f 10 wikipedia.com

This diplays only from hop\_count 10

#### 4. \$traceroute -n www.wikipedia.com

This prints ip addresses instead of domain names

#### 5. \$traceroute -I [www.wikipedia.com](http://www.wikipedia.com)

This try to print complete details instead of stars

## 6. \$traceroute -q 2 [www.wikipedia.com](http://www.wikipedia.com)

This limits number of datapackets per hop to 2

## 7. \$traceroute -g [www.wikipedia.com](http://www.wikipedia.com) [www.google.com](http://www.google.com)

To route a packet through this gate

## 8. \$traceroute -F [www.wikipedia.com](http://www.wikipedia.com)

To not fragment the packet

```
yachavenkatarakesh@pop-os:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.136.128 netmask 255.255.255.0 broadcast 192.168.136.255  
        ether fe80::b0b8:a04f:fe1df:9ba2 prefixlen 64 scopeid 0x20<link>  
    RX packets 341168 bytes 323667552 (323.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 163198 bytes 153542724 (153.5 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 2433 bytes 238190 (238.1 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2433 bytes 238190 (238.1 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
yachavenkatarakesh@pop-os:~$ sudo ifconfig ens33 down  
yachavenkatarakesh@pop-os:~$ 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 2441 bytes 238930 (238.9 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2441 bytes 238930 (238.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
yachavenkatarakesh@pop-os:~$ ifconfig -a  
ens33: flags=4098<BROADCAST,MULTICAST> mtu 1500  
    ether 00:0c:29:3e:3b:74 txqueuelen 1000 (Ethernet)  
    RX packets 341176 bytes 32368484 (323.0 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 163212 bytes 153544424 (153.5 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 2441 bytes 238930 (238.9 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2441 bytes 238930 (238.9 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
yachavenkatarakesh@pop-os:~$ sudo ifconfig ens33 up  
yachavenkatarakesh@pop-os:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.136.128 netmask 255.255.255.0 broadcast 192.168.136.255  
        ether fe80::b0b8:a04f:fe1df:9ba2 prefixlen 64 scopeid 0x20<link>  
    RX packets 380649 bytes 375773568 (375.7 MB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 170028 bytes 154666937 (154.6 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 2598 bytes 254042 (254.0 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2598 bytes 254042 (254.0 KB)
```

## Ifconfig

Ifconfig stands for interface configuration. It is used to view and change the configuration of network interface on system.

"ens0" -> Connected to wired (Ethernet)

"wlan0" -> Connected to wireless (router)

"lo" -> loop back interface, which system uses to communicate to itself.

Each of the network interface contains

1. Hwaddr (Mac address of the computer)
2. inet addr (Local IP address given to the computer) (LAN address)
3. Bcast (Broadcast address)
4. Mask (Subnet mask)
5. inet6 addr ( IPv6 address)

6. Rx packets -> Received packets
7. Tx packets -> Transmitted packets
  - At the time of execution of the command
8. mtu (Maximum Transmission Unit)
  - Size of each packet received by the ethernet card. Loop back interface will have larger packet size
9. txqueuelen this denotes the length of that transmitted queue of your device.
  - You can set it to smaller values for slower devices with high latency.
10. Collision ( >0 indicate that the packets are colliding while transferring your network which is sure sign of network cognition)

#### **ifconfig commands:**

1. \$ifconfig

Shows all the network interfaces which are active in the device

2. \$ifconfig interface\_name

Shows details of only that particular interface

3. \$sudo ifconfig ens33 down

This disables the ens33 interface

4. \$sudo ifconfig ens33 up

This enables the ens33 interface

5. \$ifconfig -a

Shows all network interfaces even if they are disabled.

6. \$ifconfig ens33 netmask some\_value

By this way we can edit the netmask values of that particular interface

7. \$ifconfig ens33 broadcast some\_value

8. \$ifconfig -s

Shows short list of all active network interfaces.

9. \$ifconfig interface add IPv6\_address

To add an IPv6 address

```

Activities Terminal ▾ Jan 25 12:35 AM yachavenkatarakesh@pop-os:~ yachavenkatarakesh@pop-os:~ yachavenkatarakesh@pop-os:~$ host www.wikipedia.com
www.wikipedia.com is an alias for ncredir-lb.wikimedia.org.
ncredir-lb.wikimedia.org has address 103.102.166.226
ncredir-lb.wikimedia.org has IPv6 address 2001:df2:e500:ed1a::3
yachavenkatarakesh@pop-os:~$ host www.google.com
www.google.com has address 74.125.68.106
www.google.com has address 74.125.68.99
www.google.com has address 74.125.68.104
www.google.com has address 74.125.68.147
www.google.com has address 74.125.68.105
www.google.com has address 74.125.68.103
www.google.com has IPv6 address 2404:6800:4003:c02::69
www.google.com has IPv6 address 2404:6800:4003:c02::63
www.google.com has IPv6 address 2404:6800:4003:c02::6a
www.google.com has IPv6 address 2404:6800:4003:c02::67
yachavenkatarakesh@pop-os:~$ host 8.8.8.8
8.8.8.8.in-addr.arpa domain name pointer dns.google.
yachavenkatarakesh@pop-os:~$ host -v www.wikipedia.com
Trying "www.wikipedia.com"
;; >>HEADER<- opcode: QUERY, status: NOERROR, id: 26271
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.wikipedia.com. IN A
;; ANSWER SECTION:
www.wikipedia.com. 5 IN CNAME ncredir-lb.wikimedia.org.
ncredir-lb.wikimedia.org. 4 IN A 103.102.166.226
Received 89 bytes from 127.0.0.53#53 in 44 ms
Trying "ncredir-lb.wikimedia.org"
;; >>HEADER<- opcode: QUERY, status: NOERROR, id: 29262
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;ncredir-lb.wikimedia.org. IN AAAA
;; ANSWER SECTION:
ncredir-lb.wikimedia.org. 5 IN AAAA 2001:df2:e500:ed1a::3
Received 70 bytes from 127.0.0.53#53 in 44 ms
Trying "ncredir-lb.wikimedia.org"
;; >>HEADER<- opcode: QUERY, status: NOERROR, id: 57327
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;ncredir-lb.wikimedia.org. IN MX
Received 42 bytes from 127.0.0.53#53 in 80 ms
yachavenkatarakesh@pop-os:~$ [REDACTED]

```

```

yachavenkatarakesh@pop-os:~$ host -a www.wikipedia.com
Trying "www.wikipedia.com"
;; >>HEADER<- opcode: QUERY, status: NOERROR, id: 61062
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.wikipedia.com. IN ANY
;; ANSWER SECTION:
www.wikipedia.com. 5 IN CNAME ncredir-lb.wikimedia.org.
Received 73 bytes from 127.0.0.53#53 in 92 ms
yachavenkatarakesh@pop-os:~$ host -t ns wikipedia.com
wikipedia.com name server ns1.wikimedia.org.
wikipedia.com name server ns2.wikimedia.org.
wikipedia.com name server ns0.wikimedia.org.
yachavenkatarakesh@pop-os:~$ host -t txt wikipedia.com
wikipedia.com descriptive text "v=spf1 -all"
yachavenkatarakesh@pop-os:~$ host -t SOA wikipedia.com
wikipedia.com has SOA record ns0.wikimedia.org. hostmaster.wikimedia.org. 2019120223 43200 7200
1209600 3600
yachavenkatarakesh@pop-os:~$ host -t C wikipedia.com
;; no response from 208.80.154.238
;; no response from 91.198.174.239
yachavenkatarakesh@pop-os:~$ host -R 3 google.com
google.com has address 74.125.24.102
google.com has address 74.125.24.138
google.com has address 74.125.24.100
google.com has address 74.125.24.139
google.com has address 74.125.24.101
google.com has address 74.125.24.113
google.com has IPv6 address 2404:6800:4003:c03::65
google.com has IPv6 address 2404:6800:4003:c03::71
google.com has IPv6 address 2404:6800:4003:c03::64
google.com has IPv6 address 2404:6800:4003:c03::8a
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
yachavenkatarakesh@pop-os:~$ host -t mx google.com
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
google.com mail is handled by 40 alt3.aspmx.l.google.com.
yachavenkatarakesh@pop-os:~$ [REDACTED]

```

Host is used to determine what domain a particular IP address resolves to. It gives information about domain servers IPv4, IPv6 addresses and mail server that domain uses.

## Host commands:

1. \$host [www.wikipedia.com](http://www.wikipedia.com) or \$host 8.8.8.8

Host some domain name or its IP address.

2. \$host -t ns [www.wikipedia.com](http://www.wikipedia.com)

Gives the appropriate name servers associated with the domain (i.e. they're the site's DNS providers)

3. \$host -t mx [www.wikipedia.com](http://www.wikipedia.com)

Gives the list of mail servers and their priorities. They can also be used for reverse lookup.

4. \$host -a [www.wikipedia.com](http://www.wikipedia.com)

It is used to specify the query type or enables the verbose output.

5. \$host -t txt [www.wikipedia.com](http://www.wikipedia.com)

It is used to print the txt record

6. \$host -t SOA [www.wikipedia.com](http://www.wikipedia.com)

It is used to print SOA record

7. \$host -R 3 [www.wikipedia.com](http://www.wikipedia.com)

Number of retries you can do in case of one try fails.

## 8. host -l [www.wikipedia.com](http://www.wikipedia.com)

To list all the hosts in that domain

The screenshot shows two terminal windows side-by-side. Both windows have the title 'Terminal' and are running on a 'pop-os' system. The left window shows the output of the command 'nslookup wikipedia.com'. It displays various DNS records for the domain, including A records for different IP addresses and CNAME records pointing to 'ncredir-lb.eqsin.wikimedia.org'. The right window shows the output of 'nslookup -type=ns wikipedia.com', which lists the nameservers for the domain: ns0.wikimedia.org, ns1.wikimedia.org, and ns2.wikimedia.org. Both windows also show other nslookup commands being run, such as '-type=mx' and '-type=txt'.

```
yachavenkatarakesh@pop-os:~$ nslookup wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: wikipedia.com
Address: 103.102.166.226
Name: wikipedia.com
Address: 2001:df2:e500:ed1a::3

yachavenkatarakesh@pop-os:~$ nslookup 103.102.166.226
226.166.102.103.in-addr.arpa name = ncredir-lb.eqsin.wikimedia.org.

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ nslookup -type=any wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: wikipedia.com
Address: 103.102.166.226
Name: wikipedia.com
Address: 2001:df2:e500:ed1a::3
wikipedia.com
origin = ns0.wikimedia.org
mail addr = hostmaster.wikimedia.org
serial = 2019120223
refresh = 43200
retry = 7200
expire = 1209600
minimum = 3600
wikipedia.com nameserver = ns1.wikimedia.org.
wikipedia.com nameserver = ns2.wikimedia.org.
wikipedia.com nameserver = ns0.wikimedia.org.

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ nslookup -type=a wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: wikipedia.com
Address: 103.102.166.226

yachavenkatarakesh@pop-os:~$ 
```

```
yachavenkatarakesh@pop-os:~$ nslookup -type=ns wikipedia.com
Jan 25 12:43 AM
yachavenkatarakesh@pop-os:~$ nslookup -type=ns wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
wikipedia.com nameserver = ns0.wikimedia.org.
wikipedia.com nameserver = ns1.wikimedia.org.
wikipedia.com nameserver = ns2.wikimedia.org.

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ nslookup -type=mx wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
*** Can't find wikipedia.com: No answer

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ nslookup -type=txt wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
wikipedia.com text = "v=spf1 -all"

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ nslookup -type=soa wikipedia.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
wikipedia.com
origin = ns0.wikimedia.org
mail addr = hostmaster.wikimedia.org
serial = 2019120223
refresh = 43200
retry = 7200
expire = 1209600
minimum = 3600

Authoritative answers can be found from:

yachavenkatarakesh@pop-os:~$ 
```

## nslookup

Nslookup 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.

### Nslookup Commands:

#### 1. \$nslookup [www.wikipedia.com](http://www.wikipedia.com)

It will give server IP address ( DNS server). Obviously they're found on port 53 and the domain names and their addresses will be displayed.

#### 2. \$nslookup 192.168.4.40

You can also do the reverse DNS lookup by providing the IP Address as argument

#### 3. nslookup -type=any [www.wikipedia.com](http://www.wikipedia.com)

Look up for any record

#### 4 nslookup -type=a [www.wikipedia.com](http://www.wikipedia.com)

## Lookup for an 'a' record

5. nslookup -type=ns [www.wikipedia.com](http://www.wikipedia.com)

Lookup for an ‘ns(name server)’ record

6. nslookup -type=SOA [www.wikipedia.com](http://www.wikipedia.com)

## Lookup for ‘soa’ record

7. nslookup -type=mx [www.wikipedia.com](http://www.wikipedia.com)

## Lookup for mail servers record

8. nslookup -type=txt [www.wikipedia.com](http://www.wikipedia.com)

## Lookup for txt record

```
Activities Terminal Jan 25 12:58 AM yachavenkatarakesh@pop-os:~ yachavenkatarakesh@pop-os:~
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com

```
; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 30628
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;wikipedia.com.      IN      A

;; ANSWER SECTION:
wikipedia.com.    1      IN      A      103.102.166.226

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 00:53:21 IST 2021
;; MSG SIZE rcvd: 58
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com +nocomments

```
; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com +nocomments
;; global options: +cmd
;wikipedia.com.      IN      A      103.102.166.226
;; Query time: 39 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 00:53:25 IST 2021
;; MSG SIZE rcvd: 58
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com -t mx

```
; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com -t mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 40293
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;wikipedia.com.      IN      MX

;; Query time: 103 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 00:53:33 IST 2021
;; MSG SIZE rcvd: 42
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com -t ns

```
; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com -t ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 17402
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;wikipedia.com.      IN      NS

;; ANSWER SECTION:
wikipedia.com.      5      IN      NS      ns2.wikimedia.org.
wikipedia.com.      5      IN      NS      ns0.wikimedia.org.
wikipedia.com.      5      IN      NS      ns1.wikimedia.org.

;; Query time: 95 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jan 25 00:57:19 IST 2021
;; MSG SIZE rcvd: 109
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com +trace

```
; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com +trace
;; global options: +cmd
.          5      IN      NS      a.root-servers.net.
.          5      IN      NS      b.root-servers.net.
.          5      IN      NS      c.root-servers.net.
.          5      IN      NS      d.root-servers.net.
.          5      IN      NS      e.root-servers.net.
.          5      IN      NS      f.root-servers.net.
.          5      IN      NS      g.root-servers.net.
.          5      IN      NS      h.root-servers.net.
.          5      IN      NS      i.root-servers.net.
.          5      IN      NS      j.root-servers.net.
.          5      IN      NS      k.root-servers.net.
.          5      IN      NS      l.root-servers.net.
.          5      IN      NS      m.root-servers.net.

;; Received 262 bytes from 127.0.0.53#53(127.0.0.53) in 27 ms

.          5      IN      NS      199.7.83.42#53(l.root-servers.net)
.          5      IN      NS      199.7.83.42#53(l.root-servers.net)

;; Received 31 bytes from 199.7.83.42#53(l.root-servers.net) in 771 ms
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com +short

```
103.102.166.226
```

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com +noall

yachavenkatarakesh@pop-os:~\$ dig wikipedia.com +noall +answer

```
wikipedia.com.      5      IN      A      103.102.166.226
```

yachavenkatarakesh@pop-os:~\$

dig

Resource 'A' means computer's IP address

‘NS’ means DNS name server for the named zone

‘MX’ means mail server

It displays domain name, TTL and then 'A' record and its IP address

Dig command gives IP addresses of servers hosted by that domain

## dig commands:

### 1. dig [www.wikipedia.com](http://www.wikipedia.com)

Returns domain name, TTL and then 'A' record and its IP address

### 2. dig [www.wikipedia.com](http://www.wikipedia.com) -t mx

For Mail servers

### 3. dig [www.wikipedia.com](http://www.wikipedia.com) -t ns

For name servers

```
Activities Terminal yachavenkatarakesh@pop-os:~ Jan 25 10:02 AM yachavenkatarakesh@pop-os:~ dig wikipedia.com ANY ; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com ANY ; global options: +cmd ; Got answer: ;-->HEADER<- opcode: QUERY, status: NOERROR, id: 17919 ; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1 ; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ; QUESTION SECTION: ;wikipedia.com. IN ANY ; ANSWER SECTION: wikipedia.com. 5 IN A 103.102.166.226 wikipedia.com. 5 IN SOA ns0.wikimedia.org. hostmaster.wikimedia.org. 2 01912023 43200 7200 1209600 3600 wikipedia.com. 5 IN NS ns1.wikimedia.org. wikipedia.com. 5 IN NS ns2.wikimedia.org. wikipedia.com. 5 IN NS ns0.wikimedia.org. ; Query time: 47 msec ; SERVER: 127.0.0.53#53(127.0.0.53) ; WHEN: Mon Jan 25 00:59:45 IST 2021 ; MSG SIZE rcvd: 172 yachavenkatarakesh@pop-os:~ dig wikipedia.com@8.8.8.8 ; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com@8.8.8.8 ; global options: +cmd ; Got answer: ;-->HEADER<- opcode: QUERY, status: NOERROR, id: 18945 ; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1 ; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ; QUESTION SECTION: ;wikipedia.com@8.8.8.8. IN A ; Query time: 75 msec ; SERVER: 127.0.0.53#53(127.0.0.53) ; WHEN: Mon Jan 25 01:00:17 IST 2021 ; MSG SIZE rcvd: 50 yachavenkatarakesh@pop-os:~ dig wikipedia.com NS ; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com NS ; global options: +cmd ; Got answer: ;-->HEADER<- opcode: QUERY, status: NOERROR, id: 32321 ; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ; QUESTION SECTION: ;wikipedia.com. IN NS ; ANSWER SECTION: wikipedia.com. 5 IN NS ns1.wikimedia.org. wikipedia.com. 5 IN NS ns2.wikimedia.org. wikipedia.com. 5 IN NS ns0.wikimedia.org. ; Query time: 127 msec ; SERVER: 127.0.0.53#53(127.0.0.53) ; WHEN: Mon Jan 25 01:00:52 IST 2021 ; MSG SIZE rcvd: 109 yachavenkatarakesh@pop-os:~ dig wikipedia.com +noall +answer +stats ; wikipedia.com. 5 IN A 103.102.166.226 ; SERVER: 127.0.0.53#53(127.0.0.53) ; WHEN: Mon Jan 25 01:01:15 IST 2021 ; MSG SIZE rcvd: 58 yachavenkatarakesh@pop-os:~ dig wikipedia.com MX ; <>> DiG 9.16.6-Ubuntu <>> wikipedia.com MX ; global options: +cmd ; Got answer: ;-->HEADER<- opcode: QUERY, status: NOERROR, id: 60000 ; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1 ; OPT PSEUDOSECTION: ; EDNS: version: 0, flags:; udp: 65494 ; QUESTION SECTION: ;wikipedia.com. IN MX ; Query time: 147 msec ; SERVER: 127.0.0.53#53(127.0.0.53) ; WHEN: Mon Jan 25 01:01:54 IST 2021 ; MSG SIZE rcvd: 42 yachavenkatarakesh@pop-os:~
```

### 4. dig [www.wikipedia.com](http://www.wikipedia.com) +short

To get only the relevant matter

### 5. dig [www.wikipedia.com](http://www.wikipedia.com) +nocomments

To get comment lines out

### 6. dig [www.wikipedia.com](http://www.wikipedia.com) +noall

To set or clear all display flags

### 7. dig [www.wikipedia.com](http://www.wikipedia.com) +noall +answer

To get detailed answer

## 8. dig [www.wikipedia.com](http://www.wikipedia.com) ANY

To get all DNS record types

## 9. dig [www.wikipedia.com](http://www.wikipedia.com) +trace

To trace the DNS path

## 10. dig [www.wikipedia.com](http://www.wikipedia.com) @ 8.8.8.8

To specify name servers

## 11. dig [www.wikipedia.com](http://www.wikipedia.com) +noall +answer +stats

To query the statistics section

The screenshot shows two terminal windows side-by-side. Both windows are titled 'Activities' and 'Terminal'. The left terminal window shows the output of a 'whois wikipedia.com' command. It provides detailed information about the domain, including its creation date (2001-01-13T00:12:14Z), last update (2021-01-25T02:01:46Z), and various registrars involved. It also lists the nameservers (NS0.WIKIMEDIA.ORG, NS1.WIKIMEDIA.ORG, NS2.WIKIMEDIA.ORG) and includes a notice from ICANN about whois accuracy. The right terminal window shows the output of a 'whois -h whois.markmonitor.com wikipedia.com' command. This version includes additional fields like 'Registrar Registration Expiration Date' (2022-01-09T00:00:00-0800) and 'Registrant Organization' (Wikimedia Foundation, Inc.). Both windows also contain a 'NOTICE' section at the bottom, which is identical in both outputs.

```
yachavenkatarakesh@pop-os:~$ whois wikipedia.com
Domain Name: WIKIPEDIA.COM
Registry Domain ID: 51687032_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-12-09T10:19:22Z
Creation Date: 2001-01-13T00:12:14Z
Registry Expiry Date: 2022-01-10T05:28:20Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: NS0.WIKIMEDIA.ORG
Name Server: NS1.WIKIMEDIA.ORG
Name Server: NS2.WIKIMEDIA.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-01-25T02:01:46Z <<

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. Users may consult the sponsoring registrar's Whois 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; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated 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

yachavenkatarakesh@pop-os:~$ whois -h whois.markmonitor.com wikipedia.com
Domain Name: wikipedia.com
Registry Domain ID: 51687032_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-12-09T02:19:22-0800
Creation Date: 2001-01-12T16:12:14-0800
Registrar Registration Expiration Date: 2022-01-09T00:00:00-0800
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registrant Organization: Wikimedia Foundation, Inc.
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/wikipedia.com
Admin Organization: Wikimedia Foundation, Inc.
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/wikipedia.com
Tech Organization: Wikimedia Foundation, Inc.
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/wikipedia.com
Name Server: ns0.wikimedia.org
Name Server: ns1.wikimedia.org
Name Server: ns2.wikimedia.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-01-24T17:57:26-0800 <<

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.
```

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

Domain Name: wikipedia.com

Registry Domain ID: 51687032\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.markmonitor.com

Registrar URL: http://www.markmonitor.com

Updated Date: 2020-12-09T02:19:22-0800

Creation Date: 2001-01-12T16:12:14-0800

Registrar Registration Expiration Date: 2022-01-09T00:00:00-0800

Registrar: MarkMonitor, Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2083895770

Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)

Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)

Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)

Registrant Organization: Wikimedia Foundation, Inc.

Registrant State/Province: CA

Registrant Country: US

Registrant Email: Select Request Email Form at <https://domains.markmonitor.com/whois/wikipedia.com>

Admin Organization: Wikimedia Foundation, Inc.

Admin State/Province: CA

Admin Country: US

Admin Email: Select Request Email Form at <https://domains.markmonitor.com/whois/wikipedia.com>

Tech Organization: Wikimedia Foundation, Inc.

Tech State/Province: CA

Tech Country: US

Tech Email: Select Request Email Form at <https://domains.markmonitor.com/whois/wikipedia.com>

Name Server: ns0.wikimedia.org

Name Server: ns1.wikimedia.org

Name Server: ns2.wikimedia.org

DNSSEC: unsigned

URL WHOIS: <http://wdprs.internic.net/>

>>> Last update of WHOIS database: 2021-01-24T17:57:26-0800 <<

For more information on WHOIS status codes, please visit:  
<https://www.icann.org/resources/pages/epp-status-codes>

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:  
<https://domains.markmonitor.com/whois>

Jan 25 7:38 AM

yachavenkatarakesh@pop-os:~

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)  
Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://www.markmonitor.com>  
Contact us at +1.8007459229  
In Europe, at +44.02032062220

--  
yachavenkatarakesh@pop-os:~\$ whois whois.godaddy.com  
No match for "WHOIS.GODADDY.COM".  
>>> Last update of whois database: 2021-01-25T02:07:18Z <<

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. Users may consult the sponsoring registrar's Whois 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; The Data in VeriSign Global Registry Services' ("VeriSign") Whois database is provided by VeriSign for information purposes only, and to assist persons in obtaining information about or related to a domain name registration record. VeriSign does not guarantee its accuracy. By submitting a Whois query, you agree to abide by the following terms of use: You agree that you may use this Data only for lawful purposes and that under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to VeriSign (or its computer systems). The compilation, repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated 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 Registrars.

yachavenkatarakesh@pop-os:~\$

## whois

whois is a query and response protocol widely used for querying databases that store the registered users or assignees of an Internet resource, such as domain name, an IP address block, or an autonomous system, but is also used for wider range of other information. The protocol stores and delivers db content in human readable format.

Whois method is used for checking information about ownership of a domain name like owner name, email, phone, address, domain created date, expire date, modification date, hosting server detail, domain IP. This protocol had its origin in ARPANET NICNAME protocol and was based on Name/Finger protocol. This is widely used by hackers for social engineering attacks and this also has a sister protocol Rwhois

There are two entities here Registries and Registrars. There are only few registries (Verisign) and thousands of registrars(eg : Godaddy, Tucows etc.,) and site owners has to buy it from registrars.

**Why didn't we get full whois record for a website?**

There are 2 types of whois while registries maintain thin records (only registrar's information) and registrars maintain thick record (registrant info in addition to registrar info).

If nothing about whois server mentioned, it returns whois information from registry database which is responsible for managing TLD(Top level domain). Some registrars explicitly block whois lookup from command line to prevent DOS attack.

```
Activities Terminal Jan 25 8:13 AM
yachavenkatarakesh@pop-os:~
```

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.136.2	0.0.0.0	UG	100	0	0	ens33
link-local	0.0.0.0	255.255.0.0	U	1000	0	0	ens33
192.168.136.0	0.0.0.0	255.255.255.0	U	100	0	0	ens33

yachavenkatarakesh@pop-os: \$ route -n

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.136.2	0.0.0.0	UG	100	0	0	ens33
169.254.0.0	0.0.0.0	255.255.0.0	U	1000	0	0	ens33
192.168.136.0	0.0.0.0	255.255.255.0	U	100	0	0	ens33

yachavenkatarakesh@pop-os: \$ route -Cn

Kernel IP cache

Source	Destination	Gateway	Flags	Metric	Ref	Use	Iface
yachavenkatarakesh@pop-os:	\$ ip -4 route						
default	via 192.168.136.2	dev ens33	proto dhcp	metric 100			
169.254.0.0/16	dev ens33	proto link	metric 1000				
192.168.136.0/24	dev ens33	proto kernel	scope link	src 192.168.136.128	metric 100		
yachavenkatarakesh@pop-os:	\$ ip -6 route						
::1	dev lo	proto kernel	metric 256	pref medium			
fe80::/64	dev ens33	proto kernel	metric 100	pref medium			
yachavenkatarakesh@pop-os:	\$ ip route						
default	via 192.168.136.2	dev ens33	proto dhcp	metric 100			
169.254.0.0/16	dev ens33	proto link	metric 1000				
192.168.136.0/24	dev ens33	proto kernel	scope link	src 192.168.136.128	metric 100		
yachavenkatarakesh@pop-os:	\$ ip route show table local						
broadcast	127.0.0.0	dev lo	proto kernel	scope link	src 127.0.0.1		
local	127.0.0.0/8	dev lo	proto kernel	scope host	src 127.0.0.1		
local	127.0.0.1	dev lo	proto kernel	scope host	src 127.0.0.1		
broadcast	127.255.255.255	dev lo	proto kernel	scope link	src 127.0.0.1		
broadcast	192.168.136.0	dev ens33	proto kernel	scope link	src 192.168.136.128		
local	192.168.136.128	dev ens33	proto kernel	scope host	src 192.168.136.128		
broadcast	192.168.136.255	dev ens33	proto kernel	scope link	src 192.168.136.128		

yachavenkatarakesh@pop-os: \$

## route

Route is used when required to work with IP/Kernel routing tables. Mainly used to setup static routes to specific hosts/networks via interface. Route is used for showing or updating IP/Kernel routing table. It contains details of destination IP address of server you're trying to connect, gateway IP address of router, then subnet mask, flags(probably two most common flags are U meaning router is up and running, G meaning gateway so this router uses a gateway, Iface is interface).

When there is no gateway it means that device is on same network as my own computer.

If final IP address matches for more than one rule then it chooses the one with longest subnet mask.

## tcpdump

It is a common packet analyzer runs under command line, it allows user to display tcp packets transmitted or received over a network to which the computer is attached.

## **tcpdump commands:**

## 1. \$sudo tcpdump

Shows all the network packets moving from that device.

2. \$sudo tcpdump -i ens33

Shows only those packets moving via ens33 network interface

3. \$sudo tcpdump -c n

To capture only n packets

4. \$sudo tcpdump -c 10 -A

To get in ASCII format

## 5. \$sudo tcpdump -D

To get list of all available interfaces

## 6. \$sudo tcpdump -n

To get packet transferring in IP address.

```

Activities Terminal Jan 25 8:50 AM
yachavenkatarakesh@pop-os:~$ sudo tcpdump -w test.pcap -c 10
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
203 packets received by filter
0 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ sudo tcpdump -r test.pcap
reading from file test.pcap, link-type EN10MB (Ethernet)
08:47:32.637176 IP 192.168.136.128.42926 > whatsapp-cdn-shv-01-any2.fcdn.net.https: Flags [P.], seq 616359061:616359092, ack 1381797247, win 65535, length 31
08:47:32.638381 IP Whatsapp-cdn-shv-01-any2.fcdn.net.https > 192.168.136.128.42926: Flags [.], ack 31, win 64240, length 0
08:47:32.981106 IP whatsapp-cdn-shv-01-any2.fcdn.net.https > 192.168.136.128.42926: Flags [P.], seq 1:39, ack 31, win 64240, length 38
08:47:32.981286 IP 192.168.136.128.42926 > whatsapp-cdn-shv-01-any2.fcdn.net.https: Flags [.], ack 39, win 65535, length 0
08:47:37.962679 IP 192.168.136.128.32787 > 192.168.136.2.domain: 33484+ A? i.ytimg.com. (29)
08:47:38.014673 IP 192.168.136.2.domain > 192.168.136.128.32787: 33484 1/0 A 172.217.194.119 (45)
08:47:38.016346 IP 192.168.136.128.35352 > 172.217.194.119.443: UDP, length 1350
08:47:38.057053 IP 172.217.194.119.443 > 192.168.136.128.35352: UDP, length 1350
08:47:38.057054 IP 172.217.194.119.443 > 192.168.136.128.35352: UDP, length 234
08:47:38.057055 IP 172.217.194.119.443 > 192.168.136.128.35352: UDP, length 63
yachavenkatarakesh@pop-os:~$ tcpdump -D
1.ens33 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
9.bluetooth0 (Bluetooth adapter number 0) [none]
yachavenkatarakesh@pop-os:~$ sudo tcpdump -c 4 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
08:48:57.635840 IP 192.168.136.128.42926 > whatsapp.https: Flags [P.], seq 616359185:616359216, ack 1381797399, win 65535, length 31
08:48:57.637381 IP whatsapp.https > 192.168.136.128.42926: Flags [.], ack 31, win 64240, length 0
08:48:57.930487 IP whatsapp.https > 192.168.136.128.42926: Flags [P.], seq 1:39, ack 31, win 64240, length 38
08:48:57.930724 IP 192.168.136.128.42926 > whatsapp.https: Flags [.], ack 39, win 65535, length 0
4 packets captured
4 packets received by filter
0 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ 

```

```

yachavenkatarakesh@pop-os:~$ sudo tcpdump -c 1 -xx
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
08:49:47.942047 IP 192.168.136.128.44014 > sb-in-f91.1e100.net.443: UDP, length 622
0x0000: 0050 56e7 2534 000c 293e 3b74 0800 4500
0x0010: 028a 5e8c 4000 4011 c399 c0a8 8880 447d
0x0020: 825b abee 01bb 0276 1889 47d6 8583 8210
0x0030: 3006 d8b8 daa9 9d30 9436 ff41 34c1 b66c
0x0040: cfbe 085e 04f3 3848 efc2 993f 1af9 e6ec
0x0050: fb0a 507e 56de 34ee 8de1 0404 1827 942f
0x0060: 35cc f2c7 6e6e adab 9b28 fbd8 c2ba 5b28
0x0070: fb7a e60d c120 ce5c 5a80 3b79 92f7 8703
0x0080: 5d3d bebb d533 2c00 af98 3888 665e 2377
0x0090: e18f 8848 daab 5aa2 6ba4 0aa4 ecfb d139
0x00a0: 3456 d974 3154 aa7d c0b4 8b64 18ed 0868
0x00b0: c9d4 71aa bf83 500f 5562 09c9 2f44 346d
0x00c0: 04cf 1fd9 5153 f62e e83a 5380 5a3a c767
0x00d0: 9f3d a3f8 4053 3c55 d154 93e4 4e8a 99eb
0x00e0: 4560 53b6 188f c871 0cff 2951 f340 3677
0x00f0: 3f15 b958 f46f 8112 96b1 4d4e 4400 0409
0x0100: 52e0 17d2 20ed 0ed5 ffa1 9155 1e59 6076
0x0110: a6b7 6412 ab52 f6e6 518f b163 f6f9 bbf5
0x0120: 50bc 64e5 45d2 59f3 4f38 bb11 980e c1ec
0x0130: d6a4 06e4 941a d55d 64c7 4bd7 b251 66da
0x0140: c757 a4d4 adbd 45c4 017e 1a7b 456e f5be
0x0150: 9c24 b7f6 f044 06c9 9ba6 3b34 0d79 080b
0x0160: 6be6 a441 b415 80c7 e536 473e 5d6d 6a3e
0x0170: ecdf 7d5f f8e9 3512 6149 1423 9936 3b27
0x0180: a739 96f3 a60a 0c21 d680 d92a 7540 3690
0x0190: 1f22 5d7b dbb4 9cf1 01fb 0a2e efaf 53f8
0x01a0: 4153 5e68 b59d 00ac dacf 41f7 e275 99f3
0x01b0: 4cdd ee51 c297 ebef 3844 7e65 30f8 dd30
0x01c0: 147d 3b1d fae9 162a a316 3d44 65c9 dd99
0x01d0: ac77 bdef 3691 5d93 74ed 1f3c b501 46d8
0x01e0: 0d79 1269 1d23 0658 f5a2 7558 ec30 96a0
0x01f0: 3de3 dfe2 2177 3647 3b61 4f2a d4a9 c1bd
0x0200: 511f 7114 17c5 9a8b efe9 e000 cd89 bd2b
0x0210: 1701 39fd 2561 c40e 76a8 6c6a 61cb d9d2
0x0220: 3517 f622 a50c 0a30 a0a3 1b60 5e93 c419
0x0230: 8a3e a8f4 e3ed 031e 625f 936e c8b5 343e
0x0240: d949 8843 a683 db64 098e b9d7 25f1 1735
0x0250: e207 dce2 3c00 8b4b 6986 49fb d759 c7ba
0x0260: 25ca 7349 0613 7911 a642 46b0 f92b 6d10
0x0270: zcf7 762b c59d feff f70e 87d9 40f5 0f5c
0x0280: a6d0 51d3 7145 90d1 3ec2 a848 0e18 9897
0x0290: df14 3782 8cb2 d7b8
1 packet captured
37 packets received by filter
5 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ 

```

## 7. \$tcpdump -w test.pcap

Save packets into the file test.pcap

## 8. \$tcpdump -r test.pcap

View saved packets from the file test.pcap

## 9. \$sudo tcpdump -c 10 -xx

To get in both ASCII and Hexa decimal format

## 10. \$sudo tcpdump tcp

To capture only based on some protocol

## 11. \$ sudo tcpdump port 2201

ping ssh [rakesh\\_b180427cs@athena.nitc.ac.in](mailto:rakesh_b180427cs@athena.nitc.ac.in) -p 2201

This is used to capture those packets via port 2201

## 12. \$sudo tcpdump src [www.wikipedia.com](http://www.wikipedia.com)

\$sudo tcpdump dst [www.wikipedia.com](http://www.wikipedia.com)

This is used to capture those packets via that domain name similarly ip addresses could also be given.

```

Activities Terminal Jan 29 8:53 AM
yachavenkatarakesh@pop-os:~$ sudo tcpdump port 2201 -c 6
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:51:55.707999 IP 192.168.136.128.34938 > athena.nitc.ac.in.2201: Flags [S], seq 40518052
03, win 64240, options [mss 1460,sACKoff,TS val 3687788278 ecr 0,nop,wscale 7], length 0
08:51:55.766490 IP athena.nitc.ac.in.2201 > 192.168.136.128.34938: Flags [S.], seq 6863960
0, ack 4051805294, win 64240, options [mss 1460], length 0
08:51:55.766647 IP 192.168.136.128.34938 > athena.nitc.ac.in.2201: Flags [.], ack 1, win 6
4240, length 0
08:51:55.767915 IP 192.168.136.128.34938 > athena.nitc.ac.in.2201: Flags [P.], seq 1:33, a
ck 1, win 64240, length 32
08:51:55.768962 IP athena.nitc.ac.in.2201 > 192.168.136.128.34938: Flags [.], ack 33, win
64240, length 0
08:51:55.833071 IP athena.nitc.ac.in.2201 > 192.168.136.128.34938: Flags [P.], seq 1:42, a
ck 33, win 64240, length 41
6 packets captured
7 packets received by filter
0 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ sudo tcpdump src wikipedia.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:52:22.093148 IP wikipedia.com > 192.168.136.128: ICMP echo reply, id 5, seq 1, length 6
4
08:52:23.098506 IP wikipedia.com > 192.168.136.128: ICMP echo reply, id 5, seq 2, length 6
4
08:52:24.098629 IP wikipedia.com > 192.168.136.128: ICMP echo reply, id 5, seq 3, length 6
4
^C
3 packets captured
8 packets received by filter
0 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ sudo tcpdump dst google.com
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
08:52:56.062566 IP 192.168.136.128 > 74.125.24.139: ICMP echo request, id 6, seq 1, length
64
08:52:57.063916 IP 192.168.136.128 > 74.125.24.139: ICMP echo request, id 6, seq 2, length
64
08:52:58.065855 IP 192.168.136.128 > 74.125.24.139: ICMP echo request, id 6, seq 3, length
64
08:52:59.068437 IP 192.168.136.128 > 74.125.24.139: ICMP echo request, id 6, seq 4, length
64
^C
4 packets captured
8 packets received by filter
0 packets dropped by kernel
yachavenkatarakesh@pop-os:~$ 
```

## tcpdump

```

Activities Terminal Jan 29 11:34 AM
yachavenkatarakesh@pop-os:~$ 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 localhost:ipp            0.0.0.0:*              LISTEN
tcp     0      0 192.168.136.128:56784   sin11s12-in-f14.1:https TIME_WAIT
tcp     0      0 192.168.136.128:53676   stats.g.doublecli:https TIME_WAIT
tcp     0      0 192.168.136.128:54982   74.125.24.84:https TIME_WAIT
tcp     0      0 192.168.136.128:50052   r3:https             TIME_WAIT
tcp     0      0 192.168.136.128:40308   172.217.194.119:https TIME_WAIT
tcp     0      0 192.168.136.128:45554   sa-in-f94.1e100.n:https TIME_WAIT
tcp     0      0 192.168.136.128:39498   ip173.208.100.17.:https TIME_WAIT
tcp     0      0 192.168.136.128:52712   cdnjs.cloudflare:https TIME_WAIT
tcp     0      0 192.168.136.128:41266   server-52-84-226.:https TIME_WAIT
tcp     0      0 192.168.136.128:53154   sin11s03-in-f46.1:https TIME_WAIT
tcp     0      0 192.168.136.128:33072   172.217.194.95:https TIME_WAIT
tcp     0      0 192.168.136.128:56482   hopenbid.pubmatrix:https TIME_WAIT
tcp     0      0 192.168.136.128:42090   74.125.24.95:https TIME_WAIT
tcp     0      0 192.168.136.128:33034   cdn.perfdrive.com:https TIME_WAIT
tcp     0      0 192.168.136.128:43016   117.18.237.66:https TIME_WAIT
tcp     0      0 192.168.136.128:39308   ads.us.e-planning:https TIME_WAIT
tcp     0      0 192.168.136.128:37316   spl.teozap.com:https TIME_WAIT
tcp     0      0 192.168.136.128:44986   sa-in-f132.1e100.:https TIME_WAIT
tcp     0      0 192.168.136.128:41544   jp:https             TIME_WAIT
tcp     0      0 192.168.136.128:34830   74.125.24.132:https TIME_WAIT
tcp6    0      0 localhost:ipp            [::]:*                LISTEN
udp     0      0 192.168.136.128:bootpc  192.168.136.254:bootps ESTABLISHED
udp     0      0 0.0.0.0:631            0.0.0.0:*
udp     0      0 0.0.0.0:41646        0.0.0.0:*
udp     0      0 0.0.0.0:mdns          0.0.0.0:*
udp6    0      0 [::]:mdns            [::]:*                *
raw6   0      0 [::]:ipv6-icmp       [::]:*                7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type      State      I-Node  Path
unix  2      [ ACC ]     SEQPACKET  LISTENING  31484  /run/udev/control
unix  2      [ ACC ]     STREAM    LISTENING  33190  /run/irqbalance/irqbalance816.sock
unix  2      [ ACC ]     STREAM    LISTENING  45418  /run/ircbalance/ircbalance81
unix  2      [ ]        DGRAM     45415   /run/user/1000/systemd/notif
y
unix  2      [ ACC ]     STREAM    LISTENING  45418   /run/user/1000/systemd/priva
te
unix  4      [ ]        DGRAM     31454   /run/systemd/notif
unix  2      [ ACC ]     STREAM    LISTENING  55058  @/dbus-vfs-daemon/socket-XlmUMs6y
unix  2      [ ACC ]     STREAM    LISTENING  50530  @/tmp/.ICE-unix/1750
unix  2      [ ACC ]     STREAM    LISTENING  42803  @/tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM    LISTENING  49181  /tmp/ssh-TVmp8L5cyvb/agent.1667
unix  2      [ ACC ]     STREAM    LISTENING  31457  /run/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING  31459  /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM    LISTENING  48306  @/tmp/dbus-F0cMkcun
unix  2      [ ACC ]     STREAM    LISTENING  31469  /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM    LISTENING  45423  /run/user/1000/bus
unix  2      [ ACC ]     STREAM    LISTENING  45424  /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM    LISTENING  31480  /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM    LISTENING  45425  /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING  45426  /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM    LISTENING  45427  /run/user/1000/gnupg/S.gpg-agent.cch
yachavenkatarakesh@pop-os:~$ netsstat -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 localhost:ipp            0.0.0.0:*              LISTEN
tcp     0      0 192.168.136.128:bootpc  192.168.136.254:bootps ESTABLISHED
yachavenkatarakesh@pop-os:~$ netsstat -au
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 localhost:ipp            0.0.0.0:*              LISTEN
tcp     0      0 192.168.136.128:bootpc  192.168.136.254:bootps ESTABLISHED
yachavenkatarakesh@pop-os:~$ netsstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0 localhost:domain          0.0.0.0:*              LISTEN
tcp     0      0 localhost:ipp            0.0.0.0:*              LISTEN
tcp6    0      0 localhost:ipp            [::]:*                LISTEN
yachavenkatarakesh@pop-os:~$ netsstat -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 localhost:ipp            0.0.0.0:*              LISTEN
tcp     0      0 192.168.136.128:bootpc  192.168.136.254:bootps ESTABLISHED
yachavenkatarakesh@pop-os:~$ netstat -a
Active UNIX domain sockets (only servers)
Proto Refcnt Flags       Type      State      I-Node  Path
unix  2      [ ACC ]     SEQPACKET  LISTENING  31484  /run/udev/control
unix  2      [ ACC ]     STREAM    LISTENING  33190  /run/irqbalance/irqbalance816.sock
unix  2      [ ACC ]     STREAM    LISTENING  45418  /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING  55058  @/dbus-vfs-daemon/socket-XlmUMs6y
unix  2      [ ACC ]     STREAM    LISTENING  50530  @/tmp/.ICE-unix/1750
unix  2      [ ACC ]     STREAM    LISTENING  42803  @/tmp/.X11-unix/X1
unix  2      [ ACC ]     STREAM    LISTENING  49181  /tmp/ssh-TVmp8L5cyvb/agent.1667
unix  2      [ ACC ]     STREAM    LISTENING  31457  /run/systemd/private
unix  2      [ ACC ]     STREAM    LISTENING  31459  /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM    LISTENING  48306  @/tmp/dbus-F0cMkcun
unix  2      [ ACC ]     STREAM    LISTENING  31469  /run/lvm/lvmpolld.socket
unix  2      [ ACC ]     STREAM    LISTENING  45423  /run/user/1000/bus
unix  2      [ ACC ]     STREAM    LISTENING  45424  /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM    LISTENING  31480  /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM    LISTENING  45425  /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM    LISTENING  45426  /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM    LISTENING  45427  /run/user/1000/gnupg/S.gpg-agent.cch
yachavenkatarakesh@pop-os:~$ 
```

## netstat

It is used for network and system management. It is a command line network utility tool that display network connections for DCP protocol, routing tables and number of other network interfaces and protocol statistics. It is also used to find out number of active connections in a computer and what connections/ services running

### netstat commands:

1. \$netstat -a

To show list of both listening and non-listening sockets

2. \$netstat -at

To list all tcp ports

3. \$netstat -au

To list all udp ports

4. \$netstat -l

To list only the listening sockets

```

Activities Terminal - Jan 25 11:35 AM
yachavenkatarakesh@pop-os:~                                     yachavenkatarakesh@pop-os:-
[Activity icon] [Terminal icon] [Search icon] [Minimize icon] [Maximize icon] [Close icon]
[Activity icon] [Terminal icon] [Search icon] [Minimize icon] [Maximize icon] [Close icon]

yachavenkatarakesh@pop-os:~$ netstat -a
unix 3      [ ]      STREAM  CONNECTED    33212
unix 3      [ ]      STREAM  CONNECTED    49158
unix 2      [ ]      DGRAM
unix 3      [ ]      STREAM  CONNECTED    50529
unix 3      [ ]      STREAM  CONNECTED    53402
unix 3      [ ]      STREAM  CONNECTED    46791
unix 3      [ ]      STREAM  CONNECTED    34378 /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED    49157
unix 2      [ ]      DGRAM   36704
unix 3      [ ]      DGRAM   36886
unix 3      [ ]      STREAM  CONNECTED    28880 /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED    50668
unix 3      [ ]      STREAM  CONNECTED    30347
unix 3      [ ]      STREAM  CONNECTED    53376
unix 3      [ ]      STREAM  CONNECTED    46027 /run/user/1000/bus
unix 3      [ ]      STREAM  CONNECTED    33213
unix 3      [ ]      STREAM  CONNECTED    34384 /run/systemd/journal/stdout
unix 3      [ ]      STREAM  CONNECTED    40632
unix 3      [ ]      STREAM  CONNECTED    50672
unix 3      [ ]      DGRAM   18166
unix 3      [ ]      STREAM  CONNECTED    46365
unix 3      [ ]      STREAM  CONNECTED    29343
yachavenkatarakesh@pop-os:~$ netstat -s
Ip:
Forwarding: 2
8752 total packets received
1 with invalid addresses
0 forwarded
0 incoming packets discarded
8749 incoming packets delivered
5119 requests sent out
20 outgoing packets dropped
Icmp:
47 ICMP messages received
0 input ICMP message failed
ICMP input histogram:
destination unreachable: 47
58 ICMP messages sent
0 ICMP messages failed
ICMP output histogram:
destination unreachable: 58
IcmpMsg:
InType3: 47
OutType3: 58
Tcp:
132 active connection openings
0 passive connection openings
8 failed connection attempts
22 connection resets received
yachavenkatarakesh@pop-os:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0  localhost:domain          0.0.0.0:*              LISTEN
tcp     0      0  localhost:ipp             0.0.0.0:*              LISTEN
tcp6    0      0  localhost:ipp             [::]:*                LISTEN
yachavenkatarakesh@pop-os:~$ netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp     0      0  localhost:domain          0.0.0.0:*              LISTEN
tcp     0      0  localhost:ipp             0.0.0.0:*              LISTEN
tcp6    0      0  localhost:ipp             [::]:*                LISTEN
yachavenkatarakesh@pop-os:~$ netstat -lx
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type            State         I-Node Path
unix  2      [ ACC ]     SEQPACKET  LISTENING   31484 /run/udev/control
unix  2      [ ACC ]     STREAM       LISTENING   33196 /run/irqbalance/irqbalance816.sock
unix  2      [ ACC ]     STREAM       LISTENING   45418 /run/user/1000/systemd/private
unix  2      [ ACC ]     STREAM       LISTENING   55058 @/dbus-vfs-daemon/socket-XlmUMs6y
unix  2      [ ACC ]     STREAM       LISTENING   50530 @/tmp/.ICE-unix/1750
unix  2      [ ACC ]     STREAM       LISTENING   42804 /tmp/X11-unix/X1
unix  2      [ ACC ]     STREAM       LISTENING   42803 @/tmp/X11-unix/X1
unix  2      [ ACC ]     STREAM       LISTENING   49181 /tmp/ssh-TVmpg8L5cyvb/agent.1667
unix  2      [ ACC ]     STREAM       LISTENING   50531 /tmp/.ICE-unix/1750
unix  2      [ ACC ]     STREAM       LISTENING   31457 /run/systemd/private
unix  2      [ ACC ]     STREAM       LISTENING   31459 /run/systemd/userdb/io.systemd.DynamicUser
unix  2      [ ACC ]     STREAM       LISTENING   48306 @/tmp/dbus-F0cMKun
unix  2      [ ACC ]     STREAM       LISTENING   31469 /run/lvm/lvmpoold.socket
unix  2      [ ACC ]     STREAM       LISTENING   45423 /run/user/1000/bus
unix  2      [ ACC ]     STREAM       LISTENING   45424 /run/user/1000/gnupg/S.dirmngr
unix  2      [ ACC ]     STREAM       LISTENING   31489 /run/systemd/journal/stdout
unix  2      [ ACC ]     STREAM       LISTENING   45425 /run/user/1000/gnupg/S.gpg-agent.browser
unix  2      [ ACC ]     STREAM       LISTENING   45426 /run/user/1000/gnupg/S.gpg-agent.extra
unix  2      [ ACC ]     STREAM       LISTENING   45427 /run/user/1000/gnupg/S.gpg-agent.ssh
unix  2      [ ACC ]     STREAM       LISTENING   30180 /var/run/vmware/guestServicePipe
unix  2      [ ACC ]     STREAM       LISTENING   45428 /run/user/1000/gnupg/S.gpg-agent
unix  2      [ ACC ]     STREAM       LISTENING   45429 /run/user/1000/pipewire-0
unix  2      [ ACC ]     STREAM       LISTENING   45430 /run/user/1000/kdeconnect-service

```

5. \$netstat -lu

To list only listening udp packets

6. \$netstar -lt

To list only listening TCP packets

## 7. \$netstat -lx

To list only the listening UNIX ports

## 8. \$netstat -s

To list the statistics from all the ports

## 9. \$netstat -pt

To display the PID and program names

## 10. \$netstat -c

To print the netstat information continuously

## 11. \$netstat -r

To get kernel routing information

## 12. \$netstat -i

To get the list of network interfaces.

```
yachavenkatarakesh@pop-os:~$ ss
Netid State      Recv-Q Send-Q          Peer Address:Port
                                         Local Address:Port
                                         Process
u_seq ESTAB      0      0              * 79779
                                         @00014 79778
u_seq ESTAB      0      0              * 79777
                                         @00013 79776
u_str ESTAB      0      0              * 48059
                                         * 50821
u_str ESTAB      0      0              * 49749
                                         * 48945
u_str ESTAB      0      0              * 47799
                                         /run/user/1000/bus 47800
u_str ESTAB      0      0              * 46801
                                         * 46045
u_str ESTAB      0      0              * 51524
                                         /run/user/1000/bus 45971
u_str ESTAB      0      0              * 44766
                                         * 48264
u_str ESTAB      0      0              * 86326
                                         @/tmp/.X11-unix/X1 82093
u_str ESTAB      0      0              * 54342
                                         * 49725
u_str ESTAB      0      0              * 48789
                                         /run/user/1000/bus 46800
u_str ESTAB      0      0              * 45945
                                         * 51300
u_str ESTAB      0      0              * 38253
                                         /run/dbus/system_bus_socket 30335
u_str ESTAB      0      0              * 86981
                                         /run/systemd/journal/stdout 87621
u_str ESTAB      0      0              * 50827
                                         * 50826
u_str ESTAB      0      0
                                         * 84065

yachavenkatarakesh@pop-os:~$ ss -a
Netid State      Recv-Q Send-Q          Peer Address:Port
                                         Local Address:Port
                                         Process
-Port
nl  UNCONN      0      0
evolution-calendaring/2019
nl  UNCONN      0      0
NetworkManager/807
nl  UNCONN      0      0
io.elementary.a/3157
nl  UNCONN      0      0
kernel
nl  UNCONN      0      0
goa-daemon/1611
nl  UNCONN      0      0
chrome/5751
nl  UNCONN      0      0
geoclue/1351
nl  UNCONN      0      0
chrome/5709
nl  UNCONN      0      0
evolution-addre/2049
nl  UNCONN      0      0
systemd-resolve/608
nl  UNCONN      0      0
avahi-daemon/800
nl  UNCONN      0      0
chrome/5751
nl  UNCONN      0      0
chrome/5709
nl  UNCONN      0      0
io.elementary.a/3157
nl  UNCONN      0      0
evolution-addre/2049
nl  UNCONN      0      0
evolution-calendaring/2019
nl  UNCONN      0      0
goa-daemon/1611
nl  UNCONN      0      0
geoclue/1351
nl  UNCONN      0      0
NetworkManager/807
nl  UNCONN      0      0
avahi-daemon/800
nl  UNCONN      0      0
systemd-resolve/608
nl  UNCONN      768  0
kernel
nl  UNCONN      4352  0
ss/8058
tcpdiag:
```

**ss**

ss tool is similar to the netstat command so it is also used for displaying network socket related information on a linux system. It displays more detailed information compared to that of netstat tool.

## ss commands:

## 1. ss

ss without any options simply lists all the connections regardless of the state they are in.

## 2. ss -a

This is used to retrieve both listening and non-listening ports

The screenshot shows a terminal window with two tabs. The left tab shows the output of `ss -l`, listing many UNCONN (non-listening) connections. The right tab shows the output of `ss -t`, listing listening connections (ESTAB) and non-listening connections (LISTEN). Below these, the left tab shows `ss -u` and the right tab shows `ss -lu`, both listing UDP connections. The bottom tab shows the output of `ss -p`, which lists processes by port number and pid.

```
yachavenkatarakesh@pop-os:~$ ss -l
Netid State Recv-Q Send-Q          Local Address:Port          Peer Address:Port
nl   UNCONN 0      0                *:*
nl   UNCONN 0      0                rtnl:evolution-calen/2019
nl   UNCONN 0      0                rtnl:NetworkManager/807
nl   UNCONN 0      0                rtnl:io.elementary.a/3157
nl   UNCONN 0      0                rtnl:kernel
nl   UNCONN 0      0                rtnl:goa-daemon/1611
nl   UNCONN 0      0                rtnl:chrome/5751
nl   UNCONN 0      0                rtnl:geoclue/1351
nl   UNCONN 0      0                rtnl:chrome/5709
nl   UNCONN 0      0                rtnl:evolution-addre/2049
nl   UNCONN 0      0                rtnl:systemd-resolve/608
nl   UNCONN 0      0                rtnl:avahi-daemon/800
nl   UNCONN 0      0                rtnl:chrome/5751
nl   UNCONN 0      0                rtnl:chrome/5709
nl   UNCONN 0      0                rtnl:io.elementary.a/3157
nl   UNCONN 0      0                rtnl:evolution-addre/2049
nl   UNCONN 0      0                rtnl:evolution-calen/2019
nl   UNCONN 0      0                rtnl:goa-daemon/1611
nl   UNCONN 0      0                rtnl:geoclue/1351
nl   UNCONN 0      0                rtnl:NetworkManager/807
nl   UNCONN 0      0                rtnl:avahi-daemon/800
nl   UNCONN 0      0                rtnl:systemd-resolve/608
nl   UNCONN 768     0                tcpdiag:kernel
nl   UNCONN 4352    0                tcpdiag:ss/8104
nl   UNCONN 0      0                selinux:kernel

yachavenkatarakesh@pop-os:~$ ss -t
State Recv-Q Send-Q          Local Address:Port          Peer Address:Port
CLOSE-WAIT 130     0      192.168.136.128:51816  216.239.32.116:https
CLOSE-WAIT 130     0      192.168.136.128:51390  172.217.194.94:https
ESTAB    0      0      192.168.136.128:57418  74.125.24.188:5228
LISTEN   0      4096   127.0.0.53%lo:domain  0.0.0.0:*
LISTEN   0      5      127.0.0.1:ipp  0.0.0.0:*
LISTEN   0      5      [:1]:ipp  [:1]:*
yachavenkatarakesh@pop-os:~$ ss -lt
State Recv-Q Send-Q          Local Address:Port          Peer Address:Port
LISTEN   0      4096   127.0.0.53%lo:domain  0.0.0.0:*
LISTEN   0      5      127.0.0.1:ipp  0.0.0.0:*
LISTEN   0      5      [:1]:ipp  [:1]:*
yachavenkatarakesh@pop-os:~$ ss -ua
State Recv-Q Send-Q          Local Address:Port          Peer Address:Port
UNCONN  0      0      127.0.0.53%lo:domain  0.0.0.0:*
UNCONN  0      0      0.0.0.0:631  0.0.0.0:*
UNCONN  0      0      0.0.0.0:41646  0.0.0.0:*
UNCONN  0      0      224.0.0.251:mdns  0.0.0.0:*
UNCONN  0      0      0.0.0.0:mdns  0.0.0.0:*
UNCONN  0      0      [:1]:mdns  [:1]:*
UNCONN  0      0      [:1]:54756  [:1]:*
yachavenkatarakesh@pop-os:~$ ss -lu
State Recv-Q Send-Q          Local Address:Port          Peer Address:Port
UNCONN  0      0      127.0.0.53%lo:domain  0.0.0.0:*
UNCONN  0      0      0.0.0.0:631  0.0.0.0:*
UNCONN  0      0      0.0.0.0:41646  0.0.0.0:*
UNCONN  0      0      224.0.0.251:mdns  0.0.0.0:*
UNCONN  0      0      0.0.0.0:mdns  0.0.0.0:*
UNCONN  0      0      [:1]:mdns  [:1]:*
UNCONN  0      0      [:1]:54756  [:1]:*
yachavenkatarakesh@pop-os:~$ ss -p
Netid State Recv-Q Send-Q          Port          Peer Address:Port          Local Address:
Process
u_seq ESTAB 0      0      79778          * 79779          @00014
users:(("chrome",pid=5709,fd=10))
u_seq ESTAB 0      0      79776          * 79777          @00013
users:(("chrome",pid=5709,fd=9))
u_str ESTAB 0      0      50821          * 48059          *
users:(("dconf-service",pid=2043,fd=5))
u_str ESTAB 0      0      48945          * 49749          *
users:(("vmtoolsd",pid=2108,fd=14))
u_str ESTAB 0      0      47800          * 47799          /run/user/1000/bus
users:(("dbus-daemon",pid=1557,fd=18))
u_str ESTAB 0      0      ....          *          *
.....          *          *
```

## 3. ss -l

To display only listening sockets

## 4. \$ss -t

To display all tcp connections

## 5. \$ss -lt

To display all listening tcp connections

## 6.\$ss -ua

To display all udp connections

## 7.\$ss -lu

To display all listening udp connections

## 8.\$ss -p

To display PID's of all sockets

## 9.\$ss -s

To list the summary statistics

10.\$ss -4

To list all IPv4 socket connections

11.\$ss -6

To list all IPv6 socket connections

Activities Terminal

yachavenkatarkesh@pop-os:~\$ dstat

You did not select any stats, using -cdngy by default.

	total-cpu-usage	-dsk/total	-net/total	--paging--	--system--	usr	sys	idl	wai	stl	read	writ	recv	send	in	out	int	csw
3	3	92	1	795	399						971	1348						
		99			120	120					253	448						
		100									242	488						
1	99			312	60	60					301	393						
	1	99			96	60					276	457						
		99									225	396						
		99			44						279	410						
		100									256	430						
		100			4096						218	365						
		100									210	367						
		99									211	366						
		99				60	300				238	391						
		100			12						228	374						
		99				60	60				233	372						
		100									197	337						
		100			8192	60	60				215	377						
		100									214	342						
		99			240						267	434						
		100									232	468						
6	2	92		32	180	240					1438	2680						
1	2	97		124							721	1389						
1	1	99				60					460	1078						
1	1	98			52						512	1200						
1	1	98									491	919						
2	1	97			76						497	735						
1	99					20					318	482						
1	99										283	422						
1	1	99				600	600				626	934						
2	2	96		44	191	60					912	1235						
3	5	92				60	60				1844	2563						
2	98			80	246	120					2089	1519						
5	2	94				120	120				873	1268						
1	1	98			24						892	1241						
1	99										338	481						
1	99				20						316	474						
1	99										271	425						
1	99					420	480				232	377						
1	99				12	60	60				347	584						
1	99										294	408						
1	99										344	518						
1	99					44	180	180			329	457						
1	99										339	554						
	procs	mem	swap	free	buff	cache	in	out	read	writ	int	csw	usr	sys	idl	wai	stl	
3.9	1738	860	126	1127									781	393	966	1336	3	3 92 1
	1738	860	126	1127									76	332	476			99
	1738	860	126	1127									310	483				99
1.0	1738	860	126	1127									20	379	551	1		99
	1735	863	126	1127									1735	2037	5	3	92	
	1735	863	126	1127									24	345	494	1		99
	1735	863	126	1127									356	528				99
	1735	863	126	1127									20	282	617			100
	1735	863	126	1127									255	616				99
	1735	863	126	1127									278	482	1			99
	1735	863	126	1127									12	391	471	1		99
	1735	863	126	1127									296	478	1	1		99
	1735	863	126	1127									44	368	514			99
	1735	863	126	1127									259	397				100
	1729	869	126	1127									84	545	809	1	1	98
	1729	869	126	1127									288	639				99
	1729	869	126	1127									24	307	610			99
	1729	869	126	1127									326	459	1			99
6.0	1729	869	126	1127									219	334				100
	1729	869	126	1127									430	710	1	1		99
	1729	869	126	1127									12	3448	1871	1	2	97
	1729	869	126	1127									1275	2015	6	3	91	
	1729	869	126	1127									28	634	920	1	1	98
	1729	869	126	1127									261	379				100
	1729	869	126	1127									12	266	380	1		99
	1729	869	126	1127									356	565	1			99
	process	idle	wait	stolen	user	system												
3	gnome-shell	0.7			1	93												
1	chrome	0.1			1	99												
1	kworker/3:0-0x1				1	98												
1	gnome-shell	0.2			1	98												
1	kworker/1:0-0x1				1	99												
1	gnome-terminal	0.4			1	98												
1	Xorg	1.5			3	4												
2	gnome-shell	1.5			2	2												
6	Xorg	3.0			3	9												
1	gnome-shell	0.2			1	98												
1	xwnc	0.1			1	99												

## dstat

dstat is used to retrieve information or statistics of the components of the system such as network connections, IO devices, CPU etc., It is generally used to retrieve a handful of information about the above mentioned components. Using this tool one can even see the throughput for block devices that makeup a single filesystem or storage system.

## **dstat commands:**

## 1. dstat

Display statistics of the major OS components

## 2. dstat –vmstat

Display information which is displayed by the vmstat tool

### 3. dstat –netstat

Display information which is displayed by the vmstat tool

### 4. dstat -c –top-cpu

Display stats of all process which are using most of the CPU

```
yachavenkatarakesh@pop-os:~$ dstat -d --top-mem
yachavenkatarakesh@pop-os:~$ dstat --list
internal:
yachavenkatarakesh@pop-os:~$ dstat --bits
yachavenkatarakesh@pop-os:~$ dstat --float
```

usr	sys	idl	wai	stl	read	writ	recv	send	in	out	int	csw	
3	3	93	1	5789	3023				926	1297			
					99		33	1440	960		323	484	
					99		480			314	455		
					1	99	1049	960	480		362	484	
					99		480			265	373		
					3	99	426	480			394	576	
					1	99		33	960	960	370	480	
					1	99				286	387		
					1	99				275	413		
					1	1	99		33		459	795	
					1	1	98		480		850	1282	
					1	1	99		98	480		426	555
					1	2	98		480		989	1363	
					1	1	99		66	480		420	544
					1	1	99		480			295	410
					1	1	99		480			259	379
					1	1	99					362	509
					1	1	99					260	372
					1	1	99					284	410
					1	1	99					261	400
					1	1	99		99			235	352
					1	1	99		1750	480		313	452
					1	1	98		819			480	831
					1	1	99		655			374	540
					1	1	98					600	782
					1	1	99					257	366

### 5. dstat -d –top-mem

Display stats of all process using most of the memory

### 6. dstat –list

Display list of all plugins

### 7. dstat –float

Will display accurate values instead of rounded

### 8. dstat –bits

Prints in bits

### 9. dstat –nocolor

Will not display any color

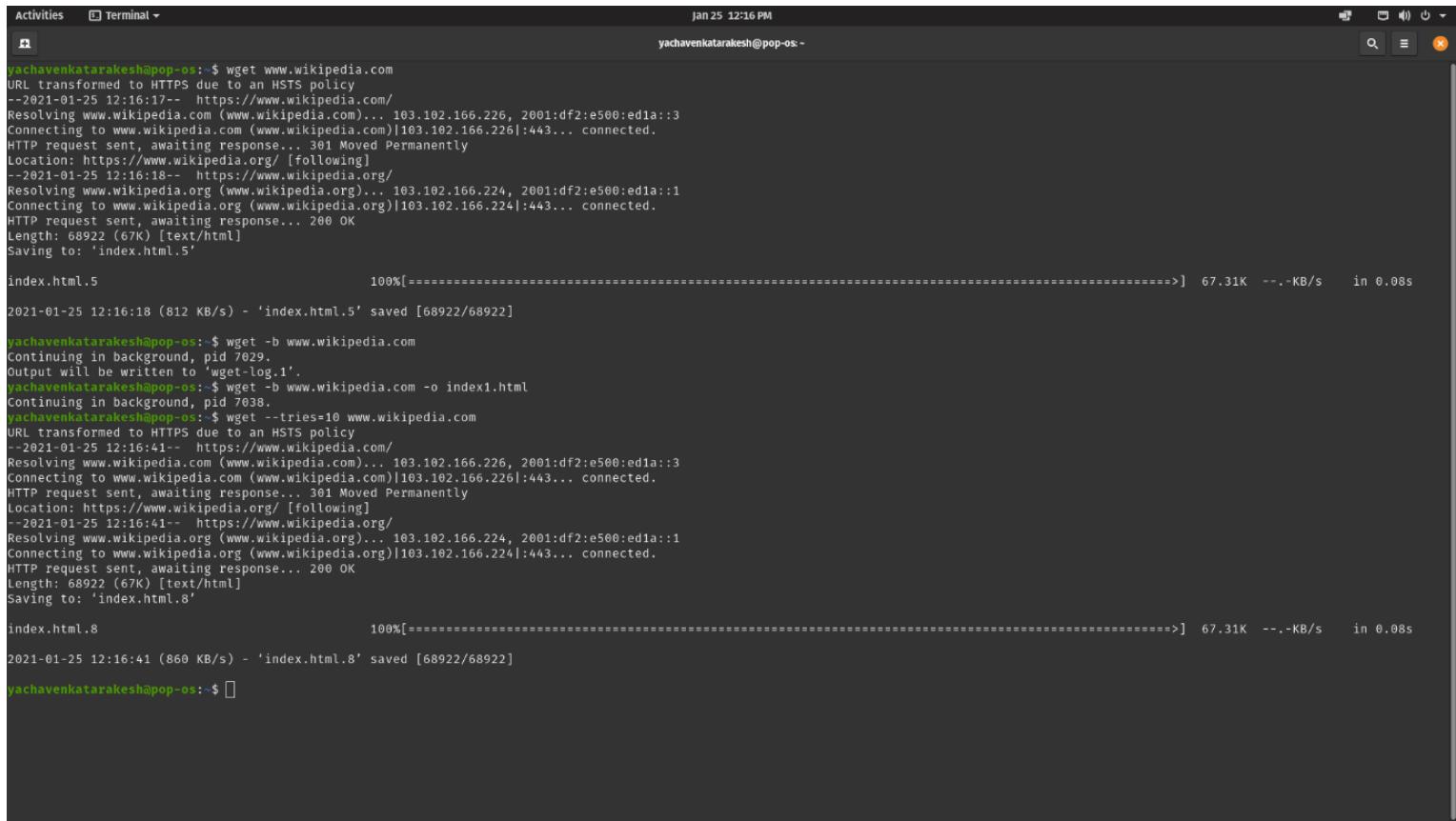
## Ifstat

It is used to report network interface statistics and displays in and out speeds of network's bandwidth consumption and speed at regular intervals of time. Also helpful in finding the network's bandwidth as we could find the average of all. It is similar to that of vmstat or iostat which reports io and virtual memory statistics respectively.

## Ifstat commands:

## 1. Sifstat

Displays network bandwidth consumption for various time intervals.



```
Activities Terminal Jan 25 12:16 PM
yachavenkatarakesh@pop-os:~
```

```
yachavenkatarakesh@pop-os:~$ wget www.wikipedia.com
URL transformed to HTTPS due to an HSTS policy
--2021-01-25 12:16:17-- https://www.wikipedia.com/
Resolving www.wikipedia.com (www.wikipedia.com)... 103.102.166.226, 2001:df2:e500:ed1a::3
Connecting to www.wikipedia.com (www.wikipedia.com)|103.102.166.226|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.wikipedia.org/ [following]
--2021-01-25 12:16:18-- https://www.wikipedia.org/
Resolving www.wikipedia.org (www.wikipedia.org)... 103.102.166.224, 2001:df2:e500:ed1a::1
Connecting to www.wikipedia.org (www.wikipedia.org)|103.102.166.224|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68922 (67k) [text/html]
Saving to: 'index.html.5'

index.html.5          100%[=====] 67.31K --.-KB/s in 0.08s

2021-01-25 12:16:18 (812 KB/s) - 'index.html.5' saved [68922/68922]

yachavenkatarakesh@pop-os:~$ wget -b www.wikipedia.com
Continuing in background, pid 7029.
Output will be written to 'wget-log.1'.
yachavenkatarakesh@pop-os:~$ wget -b www.wikipedia.com -o index1.html
Continuing in background, pid 7038.
yachavenkatarakesh@pop-os:~$ wget --tries=10 www.wikipedia.com
URL transformed to HTTPS due to an HSTS policy
--2021-01-25 12:16:41-- https://www.wikipedia.com/
Resolving www.wikipedia.com (www.wikipedia.com)... 103.102.166.226, 2001:df2:e500:ed1a::3
Connecting to www.wikipedia.com (www.wikipedia.com)|103.102.166.226|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.wikipedia.org/ [following]
--2021-01-25 12:16:41-- https://www.wikipedia.org/
Resolving www.wikipedia.org (www.wikipedia.org)... 103.102.166.224, 2001:df2:e500:ed1a::1
Connecting to www.wikipedia.org (www.wikipedia.org)|103.102.166.224|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68922 (67k) [text/html]
Saving to: 'index.html.8'

index.html.8          100%[=====] 67.31K --.-KB/s in 0.08s

2021-01-25 12:16:41 (860 KB/s) - 'index.html.8' saved [68922/68922]

yachavenkatarakesh@pop-os:~$ 
```

This is a very useful command to download the files from the server even when the user hasn't logged onto the system and can work in without use of any browser and also can work in background without hindering current process. It can also be used to get links in HTML, XHTML pages or can convert links to downloadable HTML files for offline viewing. This can be used to resume the download if it stopped due to network failure. Hence it is best useful for slow or unstable networks. It will keep retrying until the whole file is downloaded.

### wget commands:

1. [wget www.wikipedia.com](http://www.wikipedia.com)

Downloads the page into some default file. i.e. downloads the html file

2. [wget file\\_Link](#)

Downloads the file at this link

3. [\\$wget -b www.wikipedia.com](#)

Downloads in background, so we neednot resume our work until it gets downloaded.

4. [\\$wget -b www.wikipedia.com -o file.html](#)

Saves the text to our required file instead of some default files

5. [\\$wget --tries=10 www.wikipedia.com](#)

To try a given number of times in case of failures due to network issues

6. [\\$wget -c www.wikipedia.com](#)

To resume a partially downloaded file so that user need not again start from first if download failed due to some connectivity issues

**YACHA VENKATA RAKESH**

**B180427CS**

**NETWORKS LAB**

**WEEK 1 SUBMISSION**

**CSE 3<sup>RD</sup> YEAR A BATCH**