Computer Network

Assignment 1

GROUP — 3

Aditya Aggarwal	**2022028**
Piyush Narula	**2022354**

Ifconfig Command

```
piyush@piyush:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:b6:ce:35:35  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b4:45:06:c2:54:5e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 140662  bytes 20384382 (20.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 140662  bytes 20384382 (20.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.74  netmask 255.255.224.0  broadcast 192.168.63.255
        inet6 fe80::1bbe:84cf:df72:376c  prefixlen 64  scopeid 0x20<link>
        ether 38:d5:7a:57:3a:37  txqueuelen 1000  (Ethernet)
        RX packets 32853181  bytes 22675894890 (22.6 GB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 2374239  bytes 703239804 (703.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **ifconfig** is a command used to check the status of network interfaces. It also displays details like IP addresses, netmask, and broadcast addresses for the interfaces on your system.
- We can view all the interfaces using the command **ifconfig -a.**
- We can also activate and deactivate the interfaces using the ifconfig commands.
- Command **ifconfig <name> up** and **ifconfig <name> down** activate and deactivate the interfaces respectively.
- **inet** refers to IPv4 whereas **inet6** refers to IPv6.
- **TX** and **RX** refer to the number of packets transmitted and received by the network, respectively.

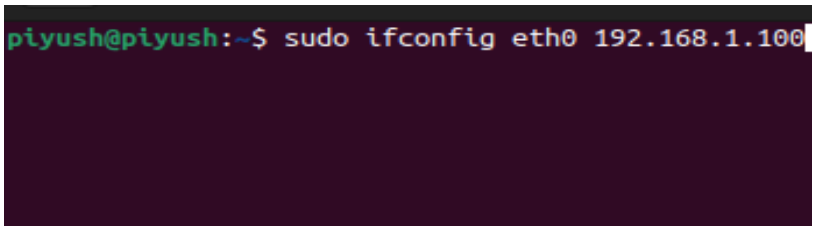
ifconfig -a

```
piyush@piyush:~$ ifconfig -a
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:b6:ce:35:35  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b4:45:06:c2:54:5e  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        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 141597  bytes 20508783 (20.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 141597  bytes 20508783 (20.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.42.74  netmask 255.255.224.0  broadcast 192.168.63.255
        inet6 fe80::1bbe:84cf:df72:376c  prefixlen 64  scopeid 0x20<link>
        ether 38:d5:7a:57:3a:37  txqueuelen 1000  (Ethernet)
        RX packets 33092468  bytes 22880724469 (22.8 GB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 2398811  bytes 712033347 (712.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

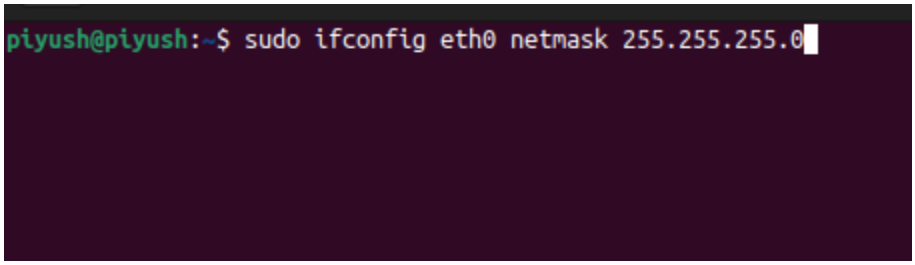
ifconfig <name> down & ifconfig <name> up

```
aytida@DESKTOP-J2KB0MD:~$ sudo ifconfig eth0 down
aytida@DESKTOP-J2KB0MD:~$ 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 246  bytes 21978 (21.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 246  bytes 21978 (21.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

aytida@DESKTOP-J2KB0MD:~$ sudo ifconfig eth0 up
aytida@DESKTOP-J2KB0MD:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1472
        inet 172.27.47.28  netmask 255.255.240.0  broadcast 172.27.47.255
        inet6 fe80::215:5dff:fe2b:e001  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:2b:e0:01  txqueuelen 1000  (Ethernet)
        RX packets 17912  bytes 91365304 (91.3 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4729  bytes 383581 (383.5 KB)
        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 246  bytes 21978 (21.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 246  bytes 21978 (21.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

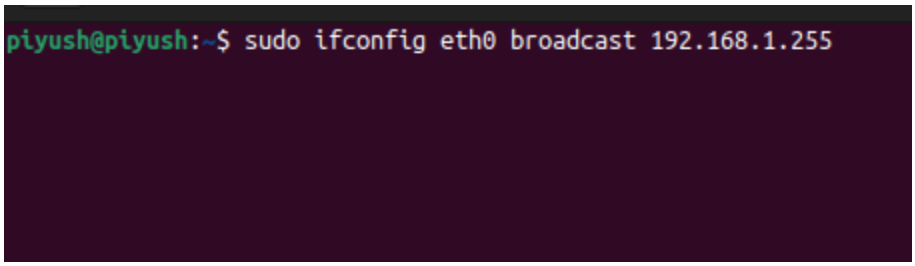
- **ifconfig <if-name> <new-ip-addr>** sets a new IP address for the specified network interface



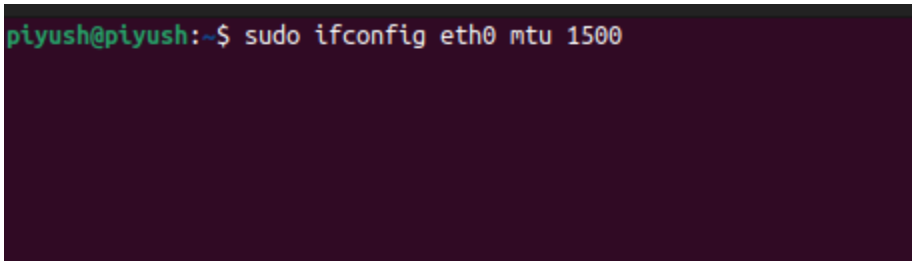
- **ifconfig <if-name> netmask <new-netmask>** assigns a new subnet mask to the specified network interface.



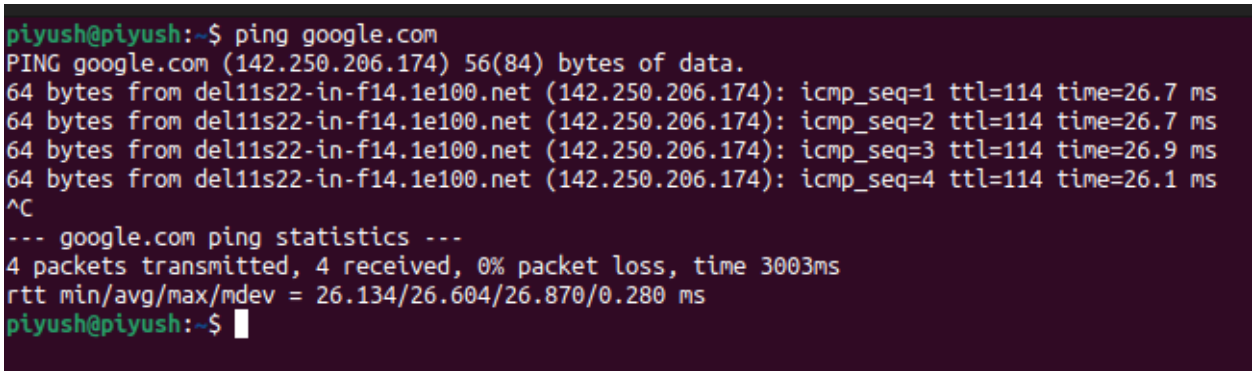
- **ifconfig <if-name> broadcast <new-broadcast>** sets a new broadcast address for the specified network interface.



- **ifconfig <if-name> mtu <new-mtu>** changes the Maximum Transmission Unit (MTU) size for the specified network interface.



Ping Command



- **ping** is the short form of Packet Internet Groper and it is used to check the connectivity between the host and server.
- It sends ICMP Echo Request packets to the target host and measures the time it takes for the Echo Reply packets to return, providing information on network connectivity and latency.
- You can also specify the number of echo requests to be sent by using the command **ping -c <number> <server>**
- You can also induce the time delay between every packet sent by using the command **ping -i <delay> <server>**
- You can also specify the number of data bytes to be sent by using the command **ping -s <bytes> <server>**
- You can also send packets from a particular interface using the command **ping -I <interface> <server>**

ping -c2 google.com

```
piyush@piyush:~$ ping -c2 google.com
PING google.com (142.250.206.174) 56(84) bytes of data.
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=1 ttl=114 time=26.7 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=114 time=38.1 ms

--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 26.690/32.386/38.082/5.696 ms
piyush@piyush:~$
```

ping -i5 google.com

```
piyush@piyush:~$ ping -i5 google.com
PING google.com (142.250.206.174) 56(84) bytes of data.
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=1 ttl=114 time=26.5 ms
64 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=114 time=26.8 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 26.505/26.631/26.757/0.126 ms
piyush@piyush:~$
```

ping -s 1000 google.com

```
piyush@piyush:~$ ping -s 1000 google.com
PING google.com (142.250.206.174) 1000(1028) bytes of data.
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=1 ttl=114 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=2 ttl=114 (truncated)
76 bytes from del11s22-in-f14.1e100.net (142.250.206.174): icmp_seq=3 ttl=114 (truncated)
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 26.605/27.088/27.760/0.490 ms
```

ping -I 1000 google.com

```
aytida@DESKTOP-J2KB0MD:~$ ping -I eth0 google.com
PING google.com (142.250.194.206) from 172.27.47.28 eth0: 56(84) bytes of data.
64 bytes from del12s07-in-f14.1e100.net (142.250.194.206): icmp_seq=1 ttl=118 time=7.67 ms
64 bytes from del12s07-in-f14.1e100.net (142.250.194.206): icmp_seq=2 ttl=118 time=10.1 ms
64 bytes from del12s07-in-f14.1e100.net (142.250.194.206): icmp_seq=3 ttl=118 time=7.42 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.421/8.393/10.089/1.203 ms
aytida@DESKTOP-J2KB0MD:~$
```

Traceroute Command

```
piyush@piyush:~$ traceroute google.com
traceroute to google.com (142.250.206.174), 30 hops max, 60 byte packets
 1  192.168.32.254 (192.168.32.254)  21.243 ms  21.203 ms  21.625 ms
 2  auth.iiitd.edu.in (192.168.1.99)  11.826 ms  11.819 ms  11.850 ms
 3  103.25.231.1 (103.25.231.1)  12.891 ms  12.884 ms  12.876 ms
 4  * * *
 5  10.119.234.162 (10.119.234.162)  15.240 ms  20.132 ms  12.835 ms
 6  72.14.194.160 (72.14.194.160)  12.827 ms  8.275 ms  8.243 ms
 7  142.251.54.111 (142.251.54.111)  29.620 ms  30.377 ms  30.490 ms
 8  142.251.76.201 (142.251.76.201)  49.836 ms  49.892 ms 142.251.76.203 (142.251.76.203)  32.694 ms
 9  del11s22-in-f14.1e100.net (142.250.206.174)  28.100 ms  28.169 ms  29.109 ms
piyush@piyush:~$
```

- Traceroute is a command-line utility for tracing the full path from your local system to another network system.
- It tracks the path packets take from your computer to a destination host across a network.
- It shows each intermediate router (hop) along the route, along with the time taken for each hop, helping identify where delays or failures occur.
- The **asterisks “ * * * “** may indicate that the intermediate router is not responding to traceroute requests, possibly due to configuration or performance issues.
- Organizations may also configure their routers not to respond to traceroute because they don’t want to reveal details of their internal network.

Netstat Command

```
piyush@piyush:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 piyush:36380           239.2.190.35.bc.g:https ESTABLISHED
tcp        0      0 piyush:42332           ec2-44-216-62-19.:https ESTABLISHED
tcp        0      0 piyush:34000           server-54-192-142:https ESTABLISHED
tcp        0      0 piyush:60798           172.64.155.209:https    ESTABLISHED
tcp        0      0 piyush:50758           whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 piyush:47416           whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 piyush:33736           104.18.35.227:https     ESTABLISHED
tcp        0      0 piyush:40248           31.234.186.35.bc.:https ESTABLISHED
tcp        0      1 piyush:58968           gladys.canonical.c:http SYN_SENT
tcp        0      0 piyush:54814           sh-in-f188.1e100.n:5228 ESTABLISHED
tcp        0      0 piyush:45758           172.64.155.209:https    ESTABLISHED
tcp        0      0 piyush:50124           ec2-34-224-14-144:https ESTABLISHED
tcp        0      0 piyush:42338           ec2-44-216-62-19.:https ESTABLISHED
udp        0      0 piyush:39699           del11s10-in-f4.1e:https ESTABLISHED
udp        0      0 piyush:39916           del11s18-in-f10.1:https ESTABLISHED
udp        0      0 piyush:60655           del12s04-in-f14.1:https ESTABLISHED
udp        0      0 piyush:60659           del11s18-in-f14.1:https ESTABLISHED
udp        0      0 localhost:57293        localhost:57293         ESTABLISHED
udp        0      0 piyush:bootpc          adc.iiitd.edu.in:bootps ESTABLISHED
udp        0      0 piyush:42040           del11s04-in-f10.1:https ESTABLISHED
udp        0      0 piyush:46301           del11s20-in-f10.1:https ESTABLISHED
udp        0      0 piyush:54724           del12s01-in-f14.1:https ESTABLISHED
udp        0      0 piyush:38855           del11s22-in-f14.1:https ESTABLISHED
Active UNIX domain sockets (w/o servers)
```

- **netstat** is the short form of the word network statistics.
- It displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.
- It provides information about active connections, listening ports, and network statistics, helping diagnose network issues and monitor network activity.
- **-a** flag is used to display all listening and non-listening socket connections. **-t** and **-u** flags display TCP and UDP connections, respectively.

```
aytida@DESKTOP-J2KB0MD:~$ netstat -t -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.255.255.254:domain   0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:domain       0.0.0.0:*               LISTEN
aytida@DESKTOP-J2KB0MD:~$ netstat -u -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 127.0.0.53:domain       0.0.0.0:*
udp        0      0 10.255.255.254:domain   0.0.0.0:*
udp        0      0 localhost:323           0.0.0.0:*
udp6       0      0 ip6-localhost:323       [::]:*
```

- **-r** flag displays the routing table, and **-i** flag shows all the information for the configured network interfaces.

```
aytida@DESKTOP-J2KB0MD:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         DESKTOP-J2KB0MD 0.0.0.0         UG        0 0          0 eth0
172.27.32.0     0.0.0.0         255.255.240.0   U         0 0          0 eth0
aytida@DESKTOP-J2KB0MD:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1472      467      0      0 0           319      0      0      0 BMRU
lo       65536      131      0      0 0           131      0      0      0 LRU
aytida@DESKTOP-J2KB0MD:~$
```

- **-p** flag, short for -program, displays the PID and name of the process using the socket.

```
aytida@DESKTOP-J2KB0MD:~$ netstat -p
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ]         DGRAM                    24585    -                    /var/run/chrony/chronyd.sock
unix  2      [ ]         DGRAM                    17676    426/systemd          /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM      CONNECTED     27673    -                    /run/systemd/notify
unix  2      [ ]         DGRAM                    27682    -                    /run/systemd/journal/syslog
unix  8      [ ]         DGRAM      CONNECTED     27690    -                    /run/systemd/journal/dev-log
unix  7      [ ]         DGRAM      CONNECTED     27692    -                    /run/systemd/journal/socket
unix  2      [ ]         DGRAM      CONNECTED     21700    426/systemd
unix  3      [ ]         STREAM     CONNECTED     34831    -                    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     23593    -
unix  3      [ ]         STREAM     CONNECTED     29706    -
unix  2      [ ]         DGRAM      CONNECTED     31797    -
unix  3      [ ]         STREAM     CONNECTED     29721    -                    /run/systemd/journal/stdout
```

- **-l** flag shows only listening socket connections.

```
aytida@DESKTOP-J2KB0MD:~$ netstat -l
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.255.255.254:domain   0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:domain       0.0.0.0:*               LISTEN
udp        0      0 127.0.0.53:domain       0.0.0.0:*
udp        0      0 10.255.255.254:domain   0.0.0.0:*
udp        0      0 localhost:323           0.0.0.0:*
udp6       0      0 ip6-localhost:323       [::]:*
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     17516    /run/WSL/2_interop
unix  2      [ ACC ]     STREAM     LISTENING     28       /run/WSL/1_interop
unix  2      [ ACC ]     STREAM     LISTENING     18898    /var/run/dbus/system_bus_socket
unix  2      [ ACC ]     SEQPACKET  LISTENING     27661    /mnt/wslg/weston-notify.sock
unix  2      [ ACC ]     STREAM     LISTENING     29702    /mnt/wslg/runtime-dir/wayland-0
unix  2      [ ACC ]     STREAM     LISTENING     29703    /tmp/.X11-unix/X0
unix  2      [ ACC ]     STREAM     LISTENING     23590    /mnt/wslg/runtime-dir/pulse/native
unix  2      [ ACC ]     STREAM     LISTENING     25709    /mnt/wslg/PulseAudioRDPSource
unix  2      [ ACC ]     STREAM     LISTENING     28734    /mnt/wslg/PulseAudioRDPSink
```

Name Server Lookup Command

```
aytida@DESKTOP-J2KB0MD:~$ nslookup www.facebook.com
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
www.facebook.com        canonical name = star-mini.c10r.facebook.com.
Name:   star-mini.c10r.facebook.com
Address: 163.70.146.35
Name:   star-mini.c10r.facebook.com
Address: 2a03:2880:f18a:8a:face:b00c:0:25de

aytida@DESKTOP-J2KB0MD:~$ nslookup 163.70.146.35
35.146.70.163.in-addr.arpa      name = edge-star-mini-shv-01-del2.facebook.com.

Authoritative answers can be found from:

aytida@DESKTOP-J2KB0MD:~$ nslookup  edge-star-mini-shv-01-del2.facebook.com.
Server:         10.255.255.254
Address:        10.255.255.254#53

Non-authoritative answer:
Name:   edge-star-mini-shv-01-del2.facebook.com
Address: 163.70.146.35

aytida@DESKTOP-J2KB0MD:~$
```

- **nslookup** is short for "Name Server Lookup."
- It is used to query the domain name system (DNS) to obtain domain name or IP address mapping information.
- **Forward Lookup** converts a domain name into its corresponding IP address using DNS.
- **Reverse Lookup** converts an IP address into its corresponding domain name. This is often used to ensure that the correct servers are being used.
- Specifying the DNS server allows querying specific servers.

```
aytida@DESKTOP-J2KB0MD:~$ nslookup www.google.com 1.1.1.1
Server:         1.1.1.1
Address:        1.1.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.77.196
Name:   www.google.com
Address: 2404:6800:4002:82c::2004
```

Dig Command

```
aytida@DESKTOP-J2KB0MD:~$ dig iiitd.ac.in

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> iiitd.ac.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44901
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;iiitd.ac.in.                   IN      A

;; ANSWER SECTION:
iiitd.ac.in.            86400   IN      A       103.25.231.30

;; Query time: 19 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sun Aug 25 17:02:09 IST 2024
;; MSG SIZE  rcvd: 56

aytida@DESKTOP-J2KB0MD:~$
```

- **dig** provides information regarding query time, response time, DNS server used, and the entire DNS response message. It is a more robust command than “nslookup.”
- The **dig MX** command sends a DNS query to the server, asking for the website's MX records.

```
aytida@DESKTOP-J2KB0MD:~$ dig iiitd.ac.in MX

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> iiitd.ac.in MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26230
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;iiitd.ac.in.                   IN      MX

;; ANSWER SECTION:
iiitd.ac.in.            86400   IN      MX      10 alt4.aspmx.l.google.com.
iiitd.ac.in.            86400   IN      MX      10 alt3.aspmx.l.google.com.
iiitd.ac.in.            86400   IN      MX      1 aspmx.l.google.com.
iiitd.ac.in.            86400   IN      MX      5 alt1.aspmx.l.google.com.
iiitd.ac.in.            86400   IN      MX      5 alt2.aspmx.l.google.com.

;; Query time: 30 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sun Aug 25 17:30:09 IST 2024
;; MSG SIZE  rcvd: 158
```

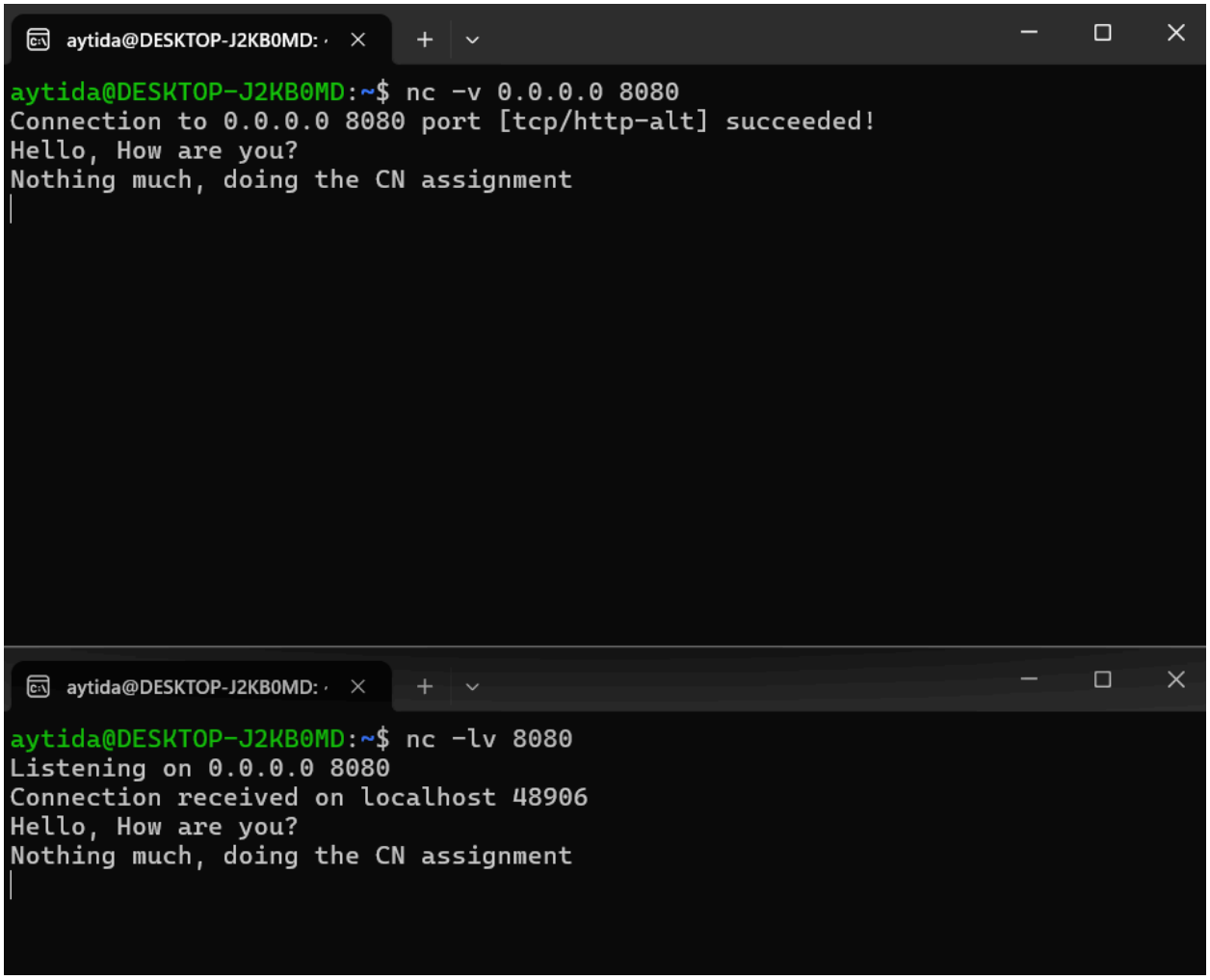
- The dig command can also be used to query a **specific DNS server**.

```
aytida@DESKTOP-J2KB0MD:~$ dig @8.8.8.8 youtube.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> @8.8.8.8 youtube.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40515
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;youtube.com.                   IN      A

;; ANSWER SECTION:
youtube.com.            1       IN      A       142.250.194.142

;; Query time: 0 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Aug 25 17:31:01 IST 2024
;; MSG SIZE  rcvd: 56
```

- **dig -x** command is used for reverse DNS lookup. It queries the DNS to find the domain name associated with a specific IP address.

```
aytida@DESKTOP-J2KB0MD:~$ dig -x 8.8.8.8

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35943
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   51069   IN      PTR     dns.google.

;; Query time: 20 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sun Aug 25 17:31:53 IST 2024
;; MSG SIZE  rcvd: 73
```

Netcat Command



- **nc,** short for **Netcat command**, is used for network communication.
- The **-l** flag enables listening mode for incoming connections.
- The **-v** flag enables verbose mode, which provides more detailed output about the connections and activities.
- To establish a connection, the **IP address** and **port number** are required.
- In the above image, 8080 is the port number, and 0.0.0.0 represents available network interfaces on the local machine. This establishes a communication network between two command line tabs on the local machine.